McAfee VirusScan per Windows 95 e Windows 98

Manuale dell’utente

Network Associates
Italy
Centro Direzionale Summit
Palazzo D/1
Via Brescia 38
20063 Cermusco sul Naviglio
Milano
Italy

COPYRIGHT

CONTRATTO DI LICENZA

A TUTTI GLI UTENTI: SI INVITANO GLI UTENTI A LEGGERE ATTENTAMENTE IL SEGUENTE CONTRATTO LEGALE ("CONTRATTO"), CHE RIPORTA I TERMINI GENERALI DI LICENZA PER IL SOFTWARE NETWORK ASSOCIATES. PER I TERMINI SPECIFICI DELLA PROPRIA LICENZA, CONSULTARE IL DOCUMENTO README.1ST, LICENZA.TXT O ALTRA LICENZA CHE ACCOMPAGNA IL SOFTWARE COME FILE DI TESTO O COME PARTE DELLA CONFEZIONE DEL SOFTWARE STESSO. Qualora l'utente non accetti i termini del presente Contratto, NON DOVRÀ INSTALLARE IL SOFTWARE. (L'UTENTE POTRÀ EVENTUALMENTE RESTITUIRE IL PRODOTTO AL RIVENDITORE E OTTENERE IL RIMBORSO DEL PREZZO.)

1. **Concessione di licenza.** Previo pagamento delle quote di licenza richieste e nel rispetto delle condizioni e clausole del presente Contratto, Network Associates concede all'utente un diritto non esclusivo e non trasferibile all'uso di una copia della versione specificata del Software e della documentazione di accompagnamento (la "Documentazione"). La copia del Software può essere installata su computer, workstation, portatili, cercapersone, "telefoni intelligenti" o altri dispositivi elettronici per i quali il Software è stato progettato (le "periferiche client"). Se il Software è concesso in licenza all'interno di un insieme di prodotti o unitamente a più di un prodotto Software, la presente licenza si applica a tutti i prodotti Software soggetti ai vincoli o ai termini di utilizzo specificati per ogni singolo Software nella fattura o sulla confezione del prodotto.

   a. **Utilizzo.** Il Software è concesso in licenza come singolo prodotto; non può essere usato su più periferiche client o da più utenti contemporaneamente, fatta eccezione per quanto riportato nella presente Sezione 1. Il Software si intende "in uso" su di un computer quando esso è caricato sulla memoria temporanea (ossia RAM) o installato sulla memoria permanente (ad esempio su disco rigido, CD-ROM o altro dispositivo di memorizzazione) di quella periferica client. La presente licenza autorizza l'utente a produrre una copia del Software esclusivamente come copia di riserva e per scopi d'archivio, purché tale copia contenga tutte le informazioni relative al proprietario.

   b. **Utilizzo del server.** Conformemente a quanto specificato nella fattura o nella confezione del prodotto, è consentito installare e utilizzare il Software su una periferica client o su un server ("Server") all'interno di un ambiente per più utenti o di una rete ("Utilizzo del server") per (i) la connessione, diretta o indiretta, ad un numero di periferiche client o "postazioni" specificate che non superi il massimo consentito; oppure per (ii) la distribuzione di un numero di agenti (poller) che non superi il massimo specificato per la distribuzione. Se la fattura o la confezione del prodotto non specificano un massimo numero di periferiche client o poller, la presente licenza fornisce il permesso per l'uso di un singolo prodotto, conformemente a quanto previsto dalla precedente sottosezione (a). Un'apposita licenza è richiesta per ciascuna periferica client o postazione che può connettersi al Software in qualsiasi momento, indipendentemente dal fatto che le suddette periferiche client o postazioni dotate di licenza siano connesse al Software contemporaneamente o usino effettivamente il Software in ogni momento.

L’uso da parte dell’acquirente di software o hardware che riducono il numero di periferiche client o postazioni che si connettono al Software e lo utilizzano simultaneamente (ad esempio hardware e software "multiplexing" o "pooling") non riduce il numero totale di licenze che è necessario possedere. In particolare è necessario possedere un numero di licenze pari al numero di distinti input dati al software o all'hardware multiplexing o pooling "front end". Se il numero di periferiche client o postazioni che possono connettersi al Software può eccedere il numero di licenze acquistate, è necessario predisporre un valido meccanismo in grado di assicurare che l'uso del Software non ecceda i limiti di utilizzo specificati nella fattura o sulla confezione del prodotto. La presente licenza autorizza l'utente a creare o scaricare una copia della Documentazione per ogni periferica client o postazione dotata di licenza, purché ogni copia contenga tutte le informazioni relative al proprietario per la Documentazione.

c. **Utilizzo del volume.** Se il Software è concesso in licenza in base ai termini di utilizzo del volume specificati nella fattura o sulla confezione, è consentito produrre, utilizzare e installare tutte le copie addizionali del Software necessarie per le periferiche client specificate nei termini di utilizzo del volume. La presente licenza autorizza l'utente a produrre o scaricare una copia della Documentazione per ognuna delle copie del Software consentite dai termini di utilizzo del volume, purché ciascuna di esse contenga tutte le informazioni relative al proprietario per la Documentazione. è obbligatorio predisporre un valido meccanismo in grado di assicurare che il numero di periferiche client su cui il Software è installato non ecceda il numero di licenze acquistate.

2. **Risoluzione.** La presente licenza è valida per il periodo di tempo specificato nella fattura o sulla confezione del prodotto, oppure nel file README.1ST, LICENZA.TXT, o in altri file di testo che accompagnano il Software e hanno lo scopo di definire i termini del contratto di licenza. Dove le disposizioni del Contratto qui indicate entrano in conflitto con le disposizioni riportate nella fattura o sulla confezione del prodotto, il documento README.1ST, il documento LICENZA.TXT, la fattura, la confezione del prodotto o altri documenti di testo costituiranno i termini della licenza d'uso del Software. Sia l'utente, sia Network Associates possono sospendere la licenza prima del termine specificato nell'apposito documento e secondo i termini in esso indicati. Il presente Contratto e la licenza si ritengono automaticamente decaduti qualora l'utente non rispettasse uno qualsiasi dei limiti o delle altre richieste in esso descritte. Alla risoluzione del presente contratto, l'utente è tenuto a distruggere tutte le copie del Software e della Documentazione in suo possesso. L'utente può risolvere il presente Contratto in qualsiasi momento distruggendo il Software e la Documentazione, oltre a tutte le copie in suo possesso.
3. **Aggiornamenti.** Durante il periodo di validità della licenza, l'utente ha il diritto di scaricare revisioni, perfezionamenti e aggiornamenti del Software, quando Network Associates li pubblica sui propri servizi elettronici, siti Web o altri servizi in linea.
4. **Diritti di proprietà.** Il Software e la Documentazione sono protetti dalle leggi degli Stati Uniti e dagli accordi internazionali sul copyright. Network Associates possiede e mantiene pienamente qualsivoglia diritto, titolo e interesse relativamente al Software, inclusi tutti i diritti di copyright, brevetti, diritti al segreto commerciale, marchi commerciali e altri diritti di proprietà intellettuale connessi. L'utente riconosce che il possesso, l'installazione e l'uso del Software non trasferiscono alla sua persona la proprietà intellettuale del Software e che egli non acquisirà alcun diritto al Software, fatta

eccezione per quanto espressamente stabilito dal presente Contratto. L'utente accetta che ogni copia del Software e della Documentazione conterrà le stesse informazioni relative al proprietario che appaiono nel Software e nella Documentazione.

5. **Restrizioni.** Non è consentito affittare, noleggiare, prestare o rivendere il Software e neppure consentire a terze parti il beneficio dell'uso o delle funzionalità del Software condividendolo o consentendone l'uso attraverso servizi di alcun tipo o altri accordi. Non è consentito trasferire nessuno dei diritti che il presente contratto attribuisce all'utente. Non è consentito copiare la Documentazione del Software. Non è consentito elaborare, decompilare o disassemblare il Software, fatta eccezione per quanto consentito dalla legge in vigore. Non è consentito modificare o creare lavori derivati, basati sul Software integralmente o in parte. Non è consentito copiare il Software, fatta eccezione per i casi espressamente consentiti dalla Sezione 1 di cui sopra. Non è consentito rimuovere etichette o altre indicazioni relative al proprietario presenti sul Software. Tutti i diritti non espressamente elencati qui di seguito devono essere accordati da Network Associates. Network Associates si riserva il diritto di condurre controlli periodici, previo preavviso scritto, per verificare che vengano rispettati i termini del contratto di licenza.

6. **Garanzia ed esclusione di garanzia**

   a. **Garanzia limitata.** Network Associates garantisce che, per trenta (30) giorni dalla data dell'acquisto o della distribuzione originale, il supporto (ad esempio i dischetti) su cui il Software è registrato sarà privo di difetti di materiale e di fabbricazione.

   b. **Tutela del cliente.** La responsabilità di Network Associates e dei suoi fornitori, e unica forma di tutela per i clienti, sarà limitata, a discrezione di Network Associates, (i) alla restituzione dell'eventuale prezzo di acquisto pagato per la licenza oppure (ii) alla sostituzione del supporto difettoso su cui il Software è registrato con una copia non difettosa. Il supporto difettoso dovrà essere restituito a Network Associates dall'acquirente a proprie spese, unitamente a una copia della ricevuta d'acquisto. La presente garanzia limitata è nulla se il difetto è dovuto a incidente, abuso o uso erroneo. Qualsiasi supporto sostitutivo è garantito fino al completamento del periodo di garanzia iniziato con il precedente Software. Fuori dal territorio degli Stati Uniti il presente diritto non è garantito, date le restrizioni cui Network Associates è soggetta in materia di esportazione.

   Esclusione di garanzia. Conformemente a quanto consentito dalle leggi vigenti e fatta eccezione per la garanzia limitata di cui sopra, IL SOFTWARE È FORNITO TALE E QUAL È, SENZA ALCUNA GARANZIA ESPRESSA O IMPLICITA. SENZA ALCUN LIMITE ALLE SUDDETTE DISPOSIZIONI, L'ACQUIRENTE ASSUME LA PIENA RESPONSABILITÀ PER LA SCELTA DEL SOFTWARE AL FINE DI SVOLGERE DETERMINATE ATTIVITÀ E PER L'INSTALLAZIONE, L'USO E I RISULTATI OTTENUTI DAL SOFTWARE STESSO. SENZA ALCUN LIMITE ALLE SUDDETTE DISPOSIZIONI, NETWORK ASSOCIATES NON GARANTISCE IN ALCUN MODO CHE IL SOFTWARE SIA PRIVO DI ERRORI, INTERRUZIONI O ALTRI DIFETTI O CHE IL SOFTWARE SODDISFI LE ESIGENZE DELL'ACQUIRENTE. SECONDO QUANTO CONSENTITO DALLA LEGGE, NETWORK ASSOCIATES non riconosce alcuna altra garanzia, espressa o implicita, comprese, in via esemplificativa, la garanzia di commerciabilità ed idoneità per un fine particolare, relativamente al software e alLA DOCUMENTAZIONE di accompagnamento. L'apposizione di limiti alla garanzia implicita non è consentita in alcuni Stati o giurisdizioni; pertanto la limitazione di cui

sopra potrebbe non essere applicabile. I suddetti termini saranno applicabili conformemente a quanto consentito dalle leggi vigenti.

L'acquisto o il pagamento del Software potrebbero dare all'acquirente il diritto a ulteriori garanzie che Network Associates specificherà nella fattura o sulla confezione del prodotto ricevuto con l'acquisto o nei file README.1ST, LICENZA.TXT o altri file di testo che accompagnano il Software e hanno lo scopo di stabilire i termini del contratto di licenza. Dove le disposizioni del presente Contratto entrano in conflitto con le disposizioni riportate nella fattura o sulla confezione del prodotto, nel file README.1ST, LICENZA.TXT o in simili documenti, la fattura, la confezione o il file di testo faranno fede per i termini relativi al diritto di garanzia dell'acquirente in merito al Software.

7. **Limitazione di responsabilità.** IN NESSUN CASO E CONFORMEMENTE A NESSUNA TEORIA LEGALE, ANCHE SE IN CASO DI ILLECITO CIVILE, CONTRATTO, O IN ALTRO MODO, NETWORK ASSOCIATES O I SUOI FORNITORI SARANNO RESPONSABILI VERSO L'ACQUIRENTE O QUALSIASI ALTRA PERSONA PER QUALSIVOGLIA DANNO INDIRETTO, SPECIALE, INCIDENTALE O CONSEQUENZIALE DI OGNI SORTA, INCLUSI, SENZA ALCUNA LIMITAZIONE, DANNI PER LA MANCANZA DI BUONA VOLONTÀ, SOSPESO FUNZIONAMENTO, BLOCCO DEL COMPUTER O MALFUNZIONAMENTO, E PER QUALSIASI ALTRO POSSIBILE DANNO O PERDITA. IN NESSUN CASO NETWORK ASSOCIATES POTRÀ ESSERE RITENUTA RESPONSABILE PER DANNI CHE SUPERINO IL PREZZO DI LISTINO APPLICATO DA NETWORK ASSOCIATES PER LA LICENZA D'USO DEL SOFTWARE, ANCHE NEL CASO IN CUI NETWORK ASSOCIATES SIA STATA AVVERTITA DELLA POSSIBILITÀ DI TALI DANNI. QUESTA LIMITAZIONE DI RESPONSABILITÀ NON SI APPLICA ALLA RESPONSABILITÀ PER MORTE O INFORTUNIO ALLA PERSONA, CONFORMEMENTE AL DIVIETO DI TALI LIMITAZIONI IMPOSTO DALLE LEGGI VIGENTI. INOLTRE, DATO CHE ALCUNI STATI E GIURISDIZIONI NON CONSENTONO L'ESCLUSIONE O LIMITAZIONE DEI DANNI INCIDENTALI O CONSEQUENZIALI, TALE LIMITAZIONE O ESCLUSIONE POTREBBE NON APPLICARSI A TUTTI GLI UTENTI. I suddetti termini saranno applicabili conformemente a quanto consentito dalle leggi vigenti.
8. **Governo degli Stati Uniti.** Il Software e la Documentazione di accompagnamento sono considerati rispettivamente "software commerciale per computer" e "documentazione di software commerciale per computer", conformemente al DFAR Section 227.7202 e FAR Section 12.212, quando applicabili. Qualsiasi uso, modifica, riproduzione, dimostrazione, rappresentazione o presentazione del Software e della Documentazione di accompagnamento da parte del Governo degli Stati Uniti sarà regolamentata esclusivamente dai termini del presente Contratto e sarà vietata in tutti i casi, fatta eccezione per quanto espressamente consentito dai termini del presente Contratto.
9. **Controlli di esportazione.** Né il Software né la relativa Documentazione e le informazioni o tecnologie che vi stanno alla base possono essere scaricate o esportate in altro modo o riesportate (i) negli stati di (o a cittadini o residenti degli stati di) Cuba, Iran, Iraq, Libia, Corea del Nord, Sudan, Siria o qualsiasi altro paese a cui gli Stati Uniti abbiano imposto l'embargo dei beni; o (ii) agli stati che compaiono nell'elenco Specially Designated Nations del Ministero del Tesoro degli Stati Uniti o nella Table of Denial Orders del Ministero del Commercio degli Stati Uniti. Coloro che scaricano o usano il Software aderiscono automaticamente alle suddette disposizioni e garantiscono di non essere domiciliati in

nessuno di tali paesi o di trovarsi sotto il loro controllo o di non essere cittadini o residenti di nessuno di tali paesi e di non essere contemplati in nessuna delle suddette liste.

INOLTRE SI INFORMA CHE L'ESPORTAZIONE DEL SOFTWARE PUÓ ESSERE SOGGETTA AL RISPETTO DELLE NORME E REGOLAMENTAZIONI PROMULGATE PERIODICAMENTE DALL'UFFICIO DI AMMINISTRAZIONE DELLE ESPORTAZIONI, PRESSO IL MINISTERO DEL COMMERCIO DEGLI STATI UNITI, CHE LIMITA L'ESPORTAZIONE E LA RIESPORTAZIONE DI DETERMINATI PRODOTTI E DATI TECNICI. SE L'ESPORTAZIONE DEL SOFTWARE È CONTROLLATA DA QUESTE NORME E REGOLAMENTAZIONI, IL SOFTWARE NON VERRÀ ESPORTATO O RIESPORTATO, DIRETTAMENTE O INDIRETTAMENTE, (A) SENZA TUTTE LE LICENZE DI ESPORTAZIONE E RIESPORTAZIONE E LE APPROVAZIONI RICHIESTE DAGLI STATI UNITI O DA ALTRI GOVERNI CONFORMEMENTE ALLE LEGGI VIGENTI, O (B) IN VIOLAZIONE DI QUALSIASI DIVIETO APPLICABILE CONTRO L'ESPORTAZIONE O RIESPORTAZIONE DI QUALSIASI PARTE DEL SOFTWARE. ALCUNI PAESI IMPONGONO RESTRIZIONI ALL'USO DELLA CODIFICA ENTRO I LORO CONFINI O ALLA SUA IMPORTAZIONE O ESPORTAZIONE, ANCHE SE ESCLUSIVAMENTE PER USO TEMPORANEO E PER SCOPI PERSONALI O LAVORATIVI. L'UTENTE È CONSAPEVOLE CHE L'APPLICAZIONE DELLE SUDDETTE LEGGI NON È LA MEDESIMA IN TUTTI I PAESI. SEBBENE L'ELENCO DI PAESI CHE SEGUE NON SIA ESAURIENTE, POTREBBERO ESSERE IMPOSTI VINCOLI ALL'ESPORTAZIONE DELLA TECNOLOGIA DI CODIFICA VERSO, O ALL'IMPORTAZIONE DA: BELGIO, CINA (INCLUSA HONG KONG), FRANCIA, INDIA, INDONESIA, ISRAELE, RUSSIA, ARABIA SAUDITA, SINGAPORE E COREA DEL SUD. L'UTENTE È CONSAPEVOLE CHE È SUA RESPONSABILITÀ IL RISPETTO DI QUALSIASI LEGGE GOVERNATIVA DI ESPORTAZIONE E DELLE ALTRE LEGGI VIGENTI E CHE NETWORK ASSOCIATES NON È SOGGETTA A ULTERIORI RESPONSABILITÀ DOPO LA VENDITA INIZIALE ENTRO I CONFINI DEL PAESE DI ORIGINE.

10. **Attività ad alto rischio.** Il Software non possiede caratteristiche di fault tolerance e non è progettato o destinato all'uso in ambienti pericolosi, che richiedono prestazioni infallibili inclusi, senza limitazioni, il controllo di impianti nucleari, il pilotaggio di aeromobili o il controllo dei relativi sistemi di comunicazione, il controllo del traffico aereo, il controllo di sistemi di offesa, il controllo di macchine di ausilio alla vita o qualsiasi altra applicazione in cui errori del Software potrebbero causare direttamente la morte, l'infortunio o gravi danni fisici alla persona o alla proprietà (in generale "attività ad alto rischio"). Network Associates rifiuta espressamente di rilasciare qualsiasi garanzia espressa o implicita di attitudine del Software per attività ad alto rischio.
11. **Varie.** Il presente Contratto è regolato dalle leggi degli Stati Uniti e dello stato della California, senza riferimenti ai conflitti dei principi di legge. L'applicazione della United Nations Convention of Contracts for the International Sale of Goods è espressamente esclusa. Il Contratto qui riportato è di natura consultiva e non sostituisce le disposizioni di Contratto eventualmente riportate nei file README.1ST, LICENZA.TXT o altri file di testo che accompagnano il Software e hanno lo scopo di stabilire i termini del contratto di licenza dell'utente. Dove i termini previsti dal presente Contratto entrano in conflitto con quanto riportato nei documenti README.1ST o LICENZA.TXT, il documento di testo fa fede per i termini di concessione della licenza d'uso del Software. Il presente Contratto non può essere modificato se non per mezzo di un addendum scritto pubblicato da un rappresentante autorizzato di Network Associates. Nessun provvedimento qui riportato

dovrebbe essere ritenuto privo di validità, a meno che il documento che ne fa decadere la validità non sia in forma scritta e non porti la firma di Network Associates o di un rappresentante autorizzato di Network Associates. Se uno qualsiasi dei termini previsti dal presente Contratto viene dichiarato non valido, la parte rimanente del Contratto rimarrà pienamente vincolante ed efficace. Le parti confermano che, secondo il loro desiderio, il presente Contratto è stato scritto solo in lingua inglese.

12. **Servizio clienti Network Associates.** Per qualsiasi quesito riguardante i termini e le condizioni qui riportate o per contattare Network Associates per qualunque altra ragione, chiamare il numero (408) 988-3832, fax (408) 970-9727, scrivere a Network Associates International B.V., P.O. Box 898, 7301 BS Apeldoorn, Paesi Bassi, oppure visitare il sito Web di Network Associates all'indirizzo http://www.nai.com.

Sommario

Prefazione

I virus informatici

Coloro che hanno già avuto modo di sperimentare la perdita di importanti dati memorizzati sul disco rigido o di osservare impotenti l'arresto del computer mentre sul monitor compariva un messaggio di saluto o ancora di doversi scusare per l'invio di messaggi di posta elettronica indesiderati che in realtà non avevano mai inviato, conoscono già gli effetti e il potenziale distruttivo dei virus informatici e di altri programmi dannosi. Solo poche fortunate persone possono affermare di non essersi ancora imbattute in una "infezione" da virus. Oggi, tuttavia, con gli oltre 24.000 virus conosciuti in circolazione in grado di attaccare i sistemi basati su Windows e su DOS, il contagio da virus è diventato sempre più probabile.

Fortunatamente solo alcuni delle migliaia di virus in circolazione sono in grado di arrecare danni gravi ai dati. Il termine "virus informatico", infatti, comprende un'ampia gamma di programmi con un'unica caratteristica in comune: si "autoreplicano" automaticamente infettando un programma ospite o alcuni settori del disco del computer evitando di essere rilevati. La maggior parte dei virus causa problemi di natura relativamente innocua, con effetti semplicemente fastidiosi o talvolta addirittura insignificanti. Spesso, la conseguenza principale di un'infezione da virus è da ricercarsi nei costi derivanti dall'investimento di tempo o risorse nella ricerca dell'origine dell'infezione e nell'eliminazione di ogni traccia.

Perché preoccuparsi?

Ci si chiederà dunque perché preoccuparsi delle infezioni da virus se causano problemi così banali. Il problema non può risolversi così semplicemente. Innanzitutto, sebbene siano relativamente pochi i virus con effetti distruttivi, non si conosce la reale diffusione di quelli dannosi. In molti casi i virus con gli effetti più devastanti sono i più difficili da scoprire, in quanto frutto di uno sviluppo doloso e corredati di tutte le misure necessarie per evitarne il rilevamento. In secondo luogo, anche i virus relativamente "benigni" possono interferire con le normali attività del computer e causare un comportamento imprevedibile in altri programmi. Alcuni virus contengono dei bug, del codice scritto male oppure degli altri problemi in grado di causare l'arresto del sistema quando vengono eseguiti. In altri casi, si verificano problemi nell'esecuzione di programmi legittimi quando un virus, intenzionalmente o casualmente, altera i parametri del sistema o altri aspetti dell'ambiente di elaborazione.

Individuare l'origine dei blocchi e degli errori del sistema può essere un'operazione dispendiosa in termini di tempo e denaro che va a discapito di attività più produttive.

Al di là di queste difficoltà, esiste un problema di prospettiva: i computer infetti possono essere portatori dell'infezione ad altri computer. Se si scambiano regolarmente dati con colleghi o clienti, è possibile diventare la causa di un involontario contagio e provocare più danni alla propria reputazione o al proprio volume d'affari di quanti non ne subisca fisicamente il computer.

La minaccia dei virus e di altri programmi dannosi è reale ed è in continuo aumento. Secondo alcune stime i costi derivanti solo dal rilevamento e dall'eliminazione delle infezioni da virus, in termini di tempo e mancata produttività, ammontano a 1 miliardo di dollari all'anno, cifra da cui sono esclusi i costi della perdita e del ripristino dei dati nelle prime fasi dell'attacco del virus.

Da dove provengono i virus?

Molte persone, dopo aver subito l'attacco di un virus o aver sentito parlare della comparsa di nuovi programmi insidiosi all'interno dei programmi di uso comune, si saranno posti molte domande riguardo l'origine dei virus. Da dove vengono i virus e gli altri programmi dannosi? Chi li scrive? Per quale motivo tali sviluppatori tentano di interrompere le attività lavorative, distruggere i dati o causare costose perdite di tempo e denaro? In che modo è possibile fermarli?

Perché è successo a me?

Probabilmente non consolerà affatto sapere che chi ha scritto il virus che ha cancellato la tabella di allocazione dei file del disco rigido non aveva intenzione di colpire un'azienda in particolare. E neanche rallegrerà sapere che il problema dei virus probabilmente non sarà mai eliminato del tutto. Tuttavia può essere utile avere alcune nozioni sulla provenienza dei virus e sulle loro modalità di funzionamento per proteggersi in modo più efficace.

Preistoria dei virus

Gli storici dei virus hanno identificato numerosi programmi che disponevano di caratteristiche che oggi sono associate ai virus. Robert M. Slade, ricercatore e insegnante canadese, fa risalire l'origine dei virus a particolari programmi creati per ottimizzare l'uso dello spazio dei file e per eseguire altre utili attività al tempo delle prime reti di computer.

Slade ricorda che gli scienziati di un laboratorio di ricerca della Xerox Corporation avevano definito questi programmi come "worm" (vermi), un termine coniato quando tali scienziati avevano iniziato a notare la presenza di "buchi" negli stampati delle mappe della memoria dei computer che parevano frutto dell'azione di vermi. Questo termine è utilizzato ancora oggi per descrivere i programmi che si autoreplicano senza alterare il programma ospite.

Tra gli studenti universitari sopravvive una forte tradizione di scherzi informatici che probabilmente ha contribuito a sviluppare l'utilizzo delle tecniche di programmazione alla base dei programmi "worm" nella direzione di insidiose minacce piuttosto che in quella dei programmi di utilità. Per mettere alla prova la propria abilità, gli studenti di informatica costruivano spesso programmi "worm" e li rilasciavano affinché "lottassero" gli uni contro gli altri in una sorta di competizione che aveva lo scopo finale di valutare quale di essi era in grado di "sopravvivere" e di sterminare i rivali. Quegli stessi studenti utilizzavano anche i programmi "worm" per fare degli scherzi a ignari colleghi.

Alcuni di questi studenti scoprirono presto che alcune funzioni del sistema operativo ospite potevano essere utilizzate per ottenere accesso non autorizzato alle risorse del computer. Altri, approfittando della relativa incompetenza di alcuni utenti, sostituivano alcuni programmi di utilità di uso comune con programmi di loro creazione. Gli ignari utenti, eseguendo quelli che credevano essere i programmi utilizzati in precedenza, constatavano che i propri file non esistevano più, che le proprie password di account erano state rubate o incorrevano in altri spiacevoli incidenti. Questi programmi, denominati "cavalli di Troia" per la somiglianza metaforica con l'antico dono dei Greci alla città di Troia, costituiscono ancora oggi una seria minaccia per gli utenti di computer.

I virus e la rivoluzione dei PC

Ciò che oggi è considerato un vero virus informatico è comparso per la prima volta, secondo Robert Slade, subito dopo la diffusione dei personal computer nel mercato di massa nei primi anni ‘80. Altri ricercatori fanno risalire l'avvento dei programmi virus al 1986, in corrispondenza della comparsa del virus "Brain". Qualunque sia la data precisa, il collegamento tra la minaccia dei virus e i personal computer non è casuale. La diffusione dei computer su vasta scala ha reso possibile il dilagare dei virus in molti sistemi, mentre in precedenza il mondo dell'informatica era stato appannaggio esclusivo di poche grandi corporazioni e università che disponevano di grandi mainframe sottoposti a stretta sorveglianza. Non aveva senso impiegare nei PC le sofisticate misure di sicurezza utilizzate per proteggere i dati importanti in tali ambienti. Anzi, gli scrittori di virus vi trovarono un terreno particolarmente fertile servendosi proprio delle tecnologie PC per i propri scopi.

Infezione del settore di boot

Con i primi PC, ad esempio, il sistema operativo veniva caricato ("boot") con i dischi floppy. Gli autori del virus Brain scoprirono presto che potevano inserire il proprio programma al posto del codice eseguibile presente nel settore di boot di tutti i floppy disk formattati con MS-DOS, anche se non comprendente i file di sistema. In questo modo, gli utenti caricavano il virus nella memoria ogni volta che avviavano il computer con un disco floppy formattato nell'unità floppy. Una volta caricati nella memoria, i virus sono in grado di autoreplicarsi nei settori di boot di altri floppy o dischi rigidi. Gli ignari utenti che caricavano il virus Brain da un disco floppy infetto vedevano comparire la "pubblicità" di una società di consulenza informatica pakistana.

Con tale annuncio pubblicitario, il virus Brain è stato il precursore di un'altra caratteristica dei virus moderni: il carico utile. Per carico utile si intendono gli scherzi o i comportamenti dolosi i cui effetti possono spaziare dalla visualizzazione di messaggi indesiderati fino alla distruzione dei dati. È la caratteristica dei virus che suscita maggiore interesse - molti autori di virus scrivono oggi i propri virus con il chiaro intento di distribuire il carico utile nel maggior numero di computer possibile.

Per un certo periodo, i sofisticati discendenti del primo virus del settore di boot hanno rappresentato la minaccia più seria per gli utenti di computer. Esistono anche varianti dei virus del settore di boot che infettano il record MBR (Master Boot Record), nel quale vengono memorizzate le informazioni sulla partizione che sono necessarie affinché il computer riesca a trovare tutte le partizioni del disco rigido e lo stesso settore di boot.

In realtà, quasi tutte le fasi del processo di boot, dalla lettura del record MBR al caricamento del sistema operativo, sono vulnerabili nei confronti dei sabotaggi virali. Tra i diversi effetti dei virus più tenaci e devastanti ancora oggi è compresa la capacità di infettare il settore di boot o il record MBR del computer. Entrando in azione al momento dell'avvio, il virus dispone di molti vantaggi, fra cui la possibilità di infettare il sistema ancora prima che venga eseguito il codice di protezione antivirus in grado di rilevarlo. VirusScan anticipa questa possibilità consentendo di creare un disco di emergenza che è possibile utilizzare per eseguire il boot del computer e rimuovere le infezioni.

I virus del settore di boot e del record MBR hanno tuttavia un limite sostanziale: devono diffondersi per mezzo dei dischi floppy o di altri supporti rimovibili rimanendo confinati nella prima traccia del disco. Di pari passo con il sempre minore utilizzo dei dischetti e con la distribuzione del software tramite altri supporti, quali i CD-ROM, altri tipi di virus hanno preso il posto di quelli che costituivano una minaccia per il settore di boot. La diffusione di dischetti ad alta capacità, come i dischi Iomega Zip e prodotti simili di altri produttori, potrebbe tuttavia dare luogo a nuovi focolai di infezione.

Virus che infettano i file

Nello stesso periodo in cui gli autori del virus Brain scoprirono la vulnerabilità del settore di boot del DOS, altri autori scoprirono come utilizzare il software esistente per consentire la replicazione delle proprie creazioni. Uno dei primi esempi di questo tipo di virus è comparso nei computer della Lehigh University in Pennsylvania. Questo virus ha infettato l'interprete dei comandi DOS COMMAND.COM utilizzandolo per caricarsi nella memoria. Una volta entrato nel sistema, si diffondeva in altri file COMMAND.COM non infetti ogni volta che un utente immetteva un qualunque comando DOS standard che invocava l'accesso al disco. La diffusione di questo virus si è limitata ai dischi floppy che contenevano, solitamente, un intero sistema operativo.

I virus della successiva generazione hanno presto superato questo limite grazie anche a sofisticate tecniche di programmazione. I virus di questo tipo, ad esempio, aggiungono il proprio codice all'inizio di un file eseguibile in modo che tale codice venga eseguito immediatamente all'avvio del programma e restituiscono il controllo al programma legittimo, il quale continua le proprie operazioni come se non fosse successo niente di insolito. Una volta attivato, il virus "blocca" o "intrappola" le richieste che il programma legittimo invia al sistema operativo e inserisce le proprie risposte. Alcuni virus particolarmente astuti sono perfino in grado di sovvertire i tentativi di eliminarli dalla memoria intrappolando la sequenza di input per il riavvio a caldo CTRL+ALT+CANC e di fingere un riavvio. A volte l'unico segnale che indica la presenza del virus - ovviamente prima che esploda il carico utile - è una piccola variazione nella dimensione del file del programma contaminato.

Virus invisibili, mutanti, cifrati e polimorfi

Sebbene si tratti di segnali minimi, il cambiamento della dimensione del file e altri fattori di questo tipo sono indizi sufficienti per la maggior parte dei prodotti antivirus per individuare e rimuovere il codice responsabile dell'infezione. Per questo motivo, una delle principali preoccupazioni degli scrittori di virus è rappresentata dai metodi possibili per nascondere il proprio artefatto.

Inizialmente venivano utilizzate tecniche che costituivano un insieme di programmazione innovativa ed espedienti ovvii. Il virus Brain, ad esempio, reinstradava le richieste in modo da spostare un settore di boot di un dischetto dalla posizione attuale alla nuova posizione dei file di boot, che il virus aveva rimosso. Questa capacità di "invisibilità" gli consentiva, così come ad altri virus, di non essere rilevato con le tradizionali tecniche di ricerca.

Poiché i virus dovevano continuamente evitare di infettare i sistemi già contaminati, per evitare che le dimensioni dei file o l'utilizzo della memoria giungessero a punti tali da rendere facilmente rilevabile la presenza del virus, gli autori dovevano anche fornire l'istruzione di non toccare determinati file.

Per risolvere questo problema, facevano in modo che il virus scrivesse una "firma" in codice per contrassegnare i file contaminati che non dovevano più essere infettati. Questo espediente riuscì a impedire che il virus venisse rilevato immediatamente ma aprì anche la strada per la nascita del software antivirus che sfrutta proprio quelle firme codificate per rintracciare il virus.

Di conseguenza, gli scrittori di virus escogitarono diversi metodi per nascondere le firme codificate. Alcuni virus "mutano" o cambiano la firma ogni volta che infettano un file. Altri cifrano la firma in codice o il virus stesso, lasciando solo un paio di byte da utilizzare come chiave per decifrarli. I nuovi virus più sofisticati, utilizzando l'invisibilità, la mutazione e la codifica, appaiono sempre più diversificati e difficili da rilevare. La ricerca di questi virus "polimorfi" ha visto impegnati gli ingegneri informatici nello sviluppo di elaborate tecniche di programmazione nell'ambito del software antivirus.

Virus macro

Intorno al 1995, la lotta contro i virus è giunta a una svolta. Nascevano continuamente nuovi virus, in parte favoriti dalla disponibilità di "kit" virali preconfezionati che consentivano anche ad utenti non programmatori di creare un nuovo virus in brevissimo tempo. Ma molti dei prodotti antivirus in commercio procedevano facilmente di pari passo con aggiornamenti che rilevavano ed eliminavano le nuove varianti virali, che consistevano principalmente in errori di lieve entità in modelli già noti.

Tuttavia, il 1995 è stato anche l'anno della comparsa del virus Concept, che ha scritto una nuova sorprendente pagina nella storia dei virus. Prima di Concept, i file di dati, quali documenti, fogli di lavoro e oggetti di grafica creati con i più diffusi prodotti software, erano considerati immuni alle infezioni. I virus, dopo tutto, non sono altro che programmi e, come tali, dovevano essere eseguiti analogamente ai programmi eseguibili per poter evidenziare i propri effetti dannosi. I file di dati, invece, memorizzavano solo le informazioni immesse tramite il software durante la lavorazione.

Questa distinzione venne meno nel momento in cui la Microsoft aggiunse per la prima volta funzioni macro in Microsoft Word e Microsoft Excel, le applicazioni di punta della suite di Office. Utilizzando la versione semplificata del linguaggio Visual BASIC incluso nella suite, gli utenti potevano creare modelli di documenti che avrebbero formattato e aggiunto automaticamente alcune funzioni nei documenti creati con Microsoft Word e Microsoft Excel. Per gli scrittori di virus, si trattò di un'opportunità per nascondere e diffondere i virus nei documenti creati dall'utente stesso.

Con la crescente diffusione di Internet e di prodotti di posta elettronica che consentono di allegare file ai messaggi, si è creata la condizione ideale per una rapida e capillare diffusione dei virus macro. In meno di un anno, i virus macro sono diventati la minaccia più insidiosa dall'avvento dei virus.

Nuovi sviluppi

Mentre i virus diventano più sofisticati e continuano a minacciare l'integrità dei sistemi da cui dipendiamo, sono emersi altri pericoli da fonti non sospette: il World Wide Web. Dapprima depositario di documenti di ricerca e trattati accademici, il Web si è trasformato nel mezzo più versatile mai inventato per le comunicazioni e il commercio.

Per le sue vaste potenzialità, il Web ha attirato l'attenzione e le energie di sviluppo di quasi tutte le società di computer nell'industria. Le convergenze nelle tecnologie risultanti da questo luogo febbricitante di invenzioni fornisce ora ai progettisti di pagine Web gli strumenti per raccogliere e visualizzare informazioni in modi mai utilizzati prima. I siti Web sono ora in grado di inviare e ricevere posta elettronica, formulare ed eseguire interrogazioni in database utilizzando motori di ricerca avanzati, inviare e ricevere file audio e video e distribuire dati e risorse multimediali a un pubblico mondiale.

La maggior parte delle tecnologie che rendono possibili queste funzioni è costituita da programmi piccoli e facilmente scaricabili che interagiscono con il browser e, talvolta, con il software sul disco rigido. Questa strada può servire come punto di entrata nel sistema di computer di altri programmi meno benevoli.

Java e ActiveX

Questi programmi, benevoli o dannosi, hanno una varietà di formati. Alcuni di questi programmi sono applicazioni con scopi particolari, "applet" scritte in Java, il nuovo linguaggio di programmazione sviluppato dalla Sun Microsystems. Altri sono sviluppati utilizzando ActiveX, una tecnologia Microsoft che i programmatori possono utilizzare per scopi simili.

Sia Java che ActiveX fanno ampio uso di moduli software predefiniti, denominati "oggetti", che i programmatori possono scrivere o reperire da fonti esistenti e modellare in plug-in, applet, driver di periferiche e altro software necessario per il potenziamento del Web. Gli oggetti Java sono denominati "classi", mentre gli oggetti ActiveX sono denominati "controlli". La principale differenza tra questi sta nel modo in cui vengono eseguiti sul sistema. Le applet Java vengono eseguite su una "macchina virtuale" Java progettata per interpretare la programmazione in Java e convertirla in azioni sul sistema, mentre i controlli ActiveX vengono eseguiti come programmi nativi di Windows che collegano ed effettuano scambi di dati tra il software Windows esistente. La maggior parte di questi oggetti sono parti utili, persino

necessarie, di un sito Web interattivo. Nonostante gli sforzi degli ingegneri della Sun e della Microsoft nel progettare misure di sicurezza, alcuni programmatori utilizzano gli strumenti Java e ActiveX per inserire oggetti dannosi nei siti Web; tali oggetti si nascondono nei siti fino a quando visitatori inconsapevoli li scaricano su computer.

A differenza dei virus, gli oggetti Java e ActiveX dannosi di solito non si replicano. Il Web fornisce loro ampie opportunità di diffusione sui computer e, allo stesso tempo, le loro piccole dimensioni e la loro natura innocua ne rende difficoltoso il rilevamento. Infatti, a meno che non si specifichi esplicitamente al browser di bloccarli, gli oggetti Java e ActiveX vengono automaticamente scaricati sul sistema ogni volta che si visita un sito Web che li ospita.

Al contrario, gli oggetti dannosi si diffondono come carichi utili di virus. Ad esempio, i programmatori hanno sviluppato oggetti in grado di leggere i dati dal disco rigido e inviarli nuovamente al sito Web visitato, in grado di "appropriarsi" dell'account di posta elettronica e inviare messaggi offensivi a nome dell'utente o visualizzare dati inviati dal computer ad altri computer e viceversa.

Nuovi obiettivi dell’infezione

Il software dannoso ha iniziato a insinuarsi anche in ambiti che prima erano considerati inattaccabili. Gli utenti del client mIRC (Internet Relay Chat), ad esempio, hanno avuto esperienza di virus costruiti con il linguaggio procedurale mIRC. I virus procedurali vengono inviati come testo normale, una caratteristica che li escluderebbe generalmente dall’infezione da virus, ma le versioni precedenti del client mIRC interpretavano le istruzioni codificate nello script, causando così l'esecuzione degli effetti dannosi sul computer del destinatario. Nelle versioni aggiornate del prodotto è stata disabilitata questa capacità, ma il problema del mIRC è utile per confermare la regola generale che vede sempre qualcuno pronto ad approfittare dei punti non protetti all'interno del software.

I virus vengono sviluppati per ragioni molto diverse, dal puro divertimento al desiderio di notorietà nel gruppo dei pari o ancora per vendetta nei confronti di colleghi di lavoro o di persone che si ritengono ostili. Indipendentemente dalle singole motivazioni, gli scrittori continuano a sviluppare nuovi modi per arrecare danni al prossimo.

Come proteggersi

La protezione avanzata di VirusScan è uno strumento efficace per la prevenzione contro le infezioni e il danneggiamento dei dati. Tuttavia, è molto più efficace se utilizzata in combinazione con un programma di sicurezza completo comprendente una varietà di misure di sicurezza per la protezione dei dati. Inoltre, il software antivirus è tanto più efficace quanto più è aggiornato. Poiché vengono rilevati mensilmente dai 200 ai 300 nuovi virus e varianti di virus, i file di dati (.DAT) che consentono al software di Network Associates di rilevare ed eliminare i virus possono diventare rapidamente obsoleti.

Se non vengono aggiornati i file inizialmente forniti con il software, si corre il rischio di infezioni ad opera di nuovi virus. Poiché Network Associates ha riunito i più esperti ricercatori nell'ambito degli antivirus nella divisione McAfee Labs, i file aggiornati per combattere i nuovi virus sono disponibili sul mercato spesso anche prima che siano necessari.

La maggior parte delle altre misure di sicurezza sono dettate dal senso comune: è sempre consigliabile eseguire un controllo dei dischi che si ricevono da fonti sconosciute o di cui si dubita, tramite un software antivirus o un'utilità di verifica. I programmatori più subdoli utilizzano oggi programmi il cui aspetto ricorda quello dei programmi utilizzati per garantire la protezione dei computer, celando uno scopo disdicevole dietro un aspetto familiare. Insieme ai propri prodotti, VirusScan fornisce VALIDATE.EXE, un programma che consente di prevenire questo tipo di manipolazione, ma né questo né altri prodotti antivirus sono in grado di rilevare la sostituzione dei programmi shareware o delle utilità di uso comune con i cosiddetti "cavalli di Troia" non ancora identificati o con altri programmi dannosi.

L'accesso al World Wide Web e a Internet pone altri rischi. VirusScan consente di bloccare l’accesso a determinati siti Web pericolosi per impedire agli utenti di scaricare software dannosi; inoltre rileva la presenza di oggetti dannosi che vengono comunque scaricati. Disporre di un firewall completo per proteggere la rete e implementare altre misure di sicurezza rappresenta una necessità quando la rete è vulnerabile agli attacchi di pirati senza scrupoli che possono penetrare da qualunque parte del mondo per appropriarsi di dati sensibili o per insediare un codice dannoso.

È necessario anche assicurarsi che la rete non sia accessibile da parte di utenti non autorizzati e disporre di adeguati programmi di formazione per insegnare e mettere in atto le misure di sicurezza standard. Per informazioni sull'origine, il comportamento e altre caratteristiche di particolari virus, consultare la Virus Information Library disponibile presso il sito Web di Network Associates.

Altri prodotti di Network Associates sono compresi nella suite Total Virus Defense (TVD), la soluzione antivirus più completa attualmente disponibile, e in Total Network Security (TNS), la più avanzata suite di sicurezza antivirus di rete oggi sul mercato. Per entrambi Network Associates offre un eccellente servizio di assistenza tecnica, addestramento e una rete mondiale di ricercatori e sviluppatori. Per informazioni sulle capacità di Total Virus Defense, rivolgersi al rappresentante Network Associates locale oppure visitare il sito World Wide Web della Network Associates.

Come contattare il servizio clienti

Servizio clienti

Per ordinare i prodotti o avere informazioni su di essi, contattare il reparto Assistenza clienti di Network Associates al numero 39 (0)2 9214 1555 o scrivere al seguente indirizzo:

Network Associates Intwrnational B.V.
P.O. Box 898
7301 BS Apeldoorn
Paesi Bassi

Supporto tecnico

Network Associates è nota per il suo grande impegno nel cercare di soddisfare i propri clienti. Per continuare questa tradizione, abbiamo trasformato il nostro sito World Wide Web in una valida fonte informativa in materia di supporto tecnico. Consigliamo a tutti gli utenti di visitare il nostro sito Web per leggere le risposte alle domande frequenti, scaricare gli aggiornamenti ai software Network Associates e ottenere le notizie e le informazioni più aggiornate sui virus pubblicate da Network Associates.

World Wide Web	http://support.nai.com

Agli utenti che non dispongono dell'accesso al Web e a coloro che non trovano sul nostro sito ciò che desiderano, si consiglia l'utilizzo dei servizi automatici.

Automated Voice e Fax Response System	(408) 988-3034
Internet	support@nai.com
CompuServe	GO NAI
America Online	parola chiave NAI

Nel caso in cui nessuno dei servizi automatici fosse in grado di offrire le risposte desiderate, si consiglia di contattare Network Associates a uno dei seguenti numeri, dal lunedì al venerdì, dalle ore 6:00 alle ore 18:00 , ora locale della costa del Pacifico.

Per i clienti dotati di licenza aziendale:

Tel.	(408) 988-3832
Fax	(408) 970-9727

Per i clienti dotati di licenza personale:

Tel.	(972) 278-6100
Fax	(408) 970-9727

Per fornire le risposte agli utenti in modo rapido ed efficiente, il personale del supporto tecnico di Network Associates necessita di alcune informazioni sul computer e sul software in uso. Saranno necessarie le seguenti informazioni:

- Nome del prodotto e numero della versione in uso
- Marca e modello del computer in uso
- Eventuali hardware o periferiche aggiuntive collegate al computer
- Tipo di sistema operativo e numero della versione in uso
- Tipo e versione della rete, se il computer in uso è collegato a una rete
- Contenuto di AUTOEXEC.BAT e CONFIG.SYS e contenuto dello script di sistema LOGIN
- Precisi passaggi da svolgere perché si verifichi il problema

Addestramento Network Associates

Per informazioni sui programmi di addestramento in loco per i prodotti Network Associates, chiamare il numero (800) 338-8754.

Commenti e feedback

Network Associates apprezza i commenti forniti dagli utenti e si riserva il diritto di usare qualsiasi informazione fornita in qualunque modo ritenga appropriato, senza incorrere in alcuna obbligazione. Gli utenti sono pregati di inviare gli eventuali commenti sulla documentazione del prodotto antivirus di Network Associates all'indirizzo: Network Associates, Inc., 15220 NW Greenbrier Parkway, Suite 100, Beaverton, OR 97006-5762, U.S.A. È inoltre possibile inviare un fax al numero (503) 531-7655 oppure un messaggio di posta elettronica all'indirizzo tvd_documentation@nai.com.

Notifica di informazioni utili per l'aggiornamento dei file antivirus

Il software antivirus Network Associates offre all'utente le migliori funzioni disponibili per il rilevamento della presenza di virus e la loro rimozione, inclusa la scansione euristica avanzata in grado di individuare virus nuovi e ancora privi di un nome non appena emergono. In alcuni casi tuttavia potrebbe apparire nel proprio sistema un virus di tipo completamente nuovo che non costituisce una variante dei tipi esistenti e quindi non viene individuato. Poiché i ricercatori di Network Associates si impegnano per fornire strumenti efficaci e aggiornati per la protezione del sistema, tutti gli utenti sono invitati a notificare ai ricercatori eventuali nuove classi Java, controlli ActiveX, siti Web pericolosi o virus che il loro software non è stato in grado di rilevare. Network Associates si riserva il diritto di usare qualsiasi informazione fornita dagli utenti nei casi in cui lo ritenga opportuno, senza incorrere in alcuna obbligazione. Inviare gli eventuali suggerimenti all'indirizzo:

virus_research@nai.com	Si invitano gli utenti a utilizzare questo indirizzo per notificare nuovi tipi di virus, controlli ActiveX e classi Java dannosi e siti Internet pericolosi.

Per le notifiche al nostro ufficio di ricerca europeo, usare il seguente indirizzo di posta elettronica:

virus_research_europe@nai.com

Per le notifiche al nostro ufficio di ricerca per la zona Asia-Pacifico o al nostro ufficio in Giappone, usare uno dei seguenti indirizzi di posta elettronica:

avert-jp@nai.com	Utilizzare questo indirizzo per le notifiche al nostro ufficio in Giappone riguardanti oggetti dannosi.
avert_apac@nai.com	Usare questo indirizzo per le notifiche riguardanti oggetti dannosi al nostro ufficio per la zona Asia-Pacifico.

Informazioni relative ai contatti internazionali

Per contattare Network Associates all'esterno degli Stati Uniti, utilizzare gli indirizzi, i numeri di telefono e i numeri di fax riportati di seguito.

Network Associates
America Latina

150 South Pine Island Road, Suite 205
Plantation, Florida 33324
USA
Tel.: (954) 452-1731
Fax: (954) 236-8031

Network Associates
Australia

Level 1, 500 Pacific Highway
St. Leonards, NSW
Sydney, Australia 2065
Tel.: 61-2-8425-4200
Fax: 61-2-9439-5166

Network Associates
Austria

Pulvermuehlstrasse 17
Linz, Austria
Codice postale A-4040
Tel.: 43-732-757-244
Fax: 43-732-757-244-20

Network Associates
Belgio

Bessenveldtstraat 25a
Diegem
Belgio - 1831
Tel.: 32-2-716-4070
Fax: 32-2-716-4770

Network Associates Brasile

Rua Geraldo Flausino Gomez 78
Cj. - 51 Brooklin Novo - São Paulo
SP - 04575-060 - Brasile
Tel.: (55 11) 5505 1009
Fax: (55 11) 5505 1006

Network Associates Canada

139 Main Street, Suite 201
Unionville, Ontario
Canada L3R 2G6
Tel.: (905) 479-4189
Fax: (905) 479-4540

Network Associates Deutschland GmbH

Ohmstraße 1
D-85716 Unterschleißheim
Germany
Tel: 49 89 3707 0
Fax: 49 89 3707 1199

NA Network Associates Oy Finlandia

Sinikalliontie 9
02630 Espoo
Finlandia
Tel.: 358 9 5270 70
Fax: 358 9 5270 7100

Network Associates France S.A.

50 rue de Londres
75008 Parigi
Francia
Tel.: 33 1 44 908 737
Fax: 33 1 45 227 554

Network Associates Hong Kong

19/F, Matheson Centre
3 Matheson Street
Causeway Bay
Hong Kong
Tel.: 852-2832-9525
Fax: 852-2832-9530

Network Associates International B.V.

Gatwickstraat 25
1043 GL Amsterdam
Paesi Bassi
Tel.: 31 20 586 6100
Fax: 31 20 586 6101

Network Associates International Ltd.

Minton Place, Victoria Street
Windsor, Berkshire
SL4 1EG
Regno Unito
Tel.: 44 (0)1753 827 500
Fax: 44 (0)1753 827 520

Network Associates Srl Italia

Centro Direzionale Summit
Palazzo D/1
Via Brescia, 28
20063 - Cernusco sul Naviglio (MI)
Italia
Tel.: 39 (0)2 9214 1555
Fax: 39 (0)2 9214 1644

Network Associates Japan, Inc.

Toranomon 33 Mori Bldg.
3-8-21 Toranomon Minato-Ku
Tokyo 105-0001
Giappone
Tel.: 81 3 5408 0700
Fax: 81 3 5408 0781

Network Associates Messico

Andres Bello No. 10, 4 Piso
4th Floor
Col. Polanco
Città del Messico, Messico D.F. 11560
Tel.: (525) 282-9180
Fax: (525) 282-9183

Network Associates Portogallo

Av. de Liberdade, 114
1269-046 Lisboa
Portogallo
Tel.: 351 1 340 4543
Fax :351 1 340 4575

Network Associates Repubblica Popolare Cinese

New Century Office Tower, Room 1557
No. 6 Southern Road Capitol Gym
Pechino
Repubblica Popolare Cinese 100044
Tel.: 8610-6849-2650
Fax: 8610-6849-2069

Network Associates Spagna

Orense 4, 4th Floor
Edificio Trieste
28020 Madrid
Spagna
Tel.: 34 91 598 18 00
Fax: 34 91 556 14 04

Net Tools Network Associates Sudafrica

Bardev House, St. Andrews
Meadowbrook Lane
Epson Downs, P.O. Box 7062
Bryanston, Johannesburg
Sud Africa 2021
Tel.: 27 11 706-1629
Fax: 27 11 706-1569

Network Associates Sud-est asiatico

7 Temasek Boulevard
The Penthouse
#44-01, Suntec Tower One
Singapore 38987
Tel.: 65-430-6670
Fax: 65-430-6671

Network Associates Svezia

Datavägen 3A
Box 596
S-175 26 Järfälla
Svezia
Tel.: 46 (0) 8 580 88 400
Fax: 46 (0) 8 580 88 405

Network Associates AG Svizzera

Baeulerwisenstrasse 3
8152 Glattbrugg
Svizzera
Tel.: 0041 1 808 99 66
Fax: 0041 1 808 99 77

Informazioni su McAfee VirusScan 1

Cos'è VirusScan

VirusScan è l'elemento chiave nella suite di strumenti di sicurezza Network Associates Total Virus Defense. Funziona come un'instancabile sentinella in linea che difende il sistema dagli attacchi dei virus e lo protegge dal potenziale pericolo di altri software dannosi. Il suo potente gruppo di strumenti di scansione e altri miglioramenti lo rendono da sempre uno dei più importanti software antivirus, ma nell'ultima versione di VirusScan è stata aggiunta all'arsenale di protezione la tecnologia McAfee WebScanX che contribuisce a garantire la sicurezza del sistema contro i pericoli provenienti da Internet.

Le pagine Web più sofisticate, ad esempio, possono incorporare elementi interattivi creati con classi Java e controlli ActiveX. Inoltre, milioni di utenti oggi si scambiano messaggi, file e altri dati attraverso la posta elettronica, utilizzando spesso "allegati" costituiti da file eseguibili, modelli di documenti e altri dati. Ma queste utili tecnologie moderne possono nascondere nuovi pericoli. File eseguibili infetti da virus potrebbero essere in agguato sui siti Web, spesso all'insaputa dello stesso titolare del sito. Oppure potrebbero diffondersi attraverso la posta elettronica, anche quando non viene espressamente richiesto. Abili programmatori possono progettare applet Java o controlli ActiveX in grado di aggirare le funzioni di sicurezza incorporate nei browser degli utenti in modo da poter leggere i dati contenuti nel disco rigido, inviare messaggi di posta elettronica a nome di altri oppure procurare danni di altro genere.

In un ambiente in cui sono presenti questi pericoli, prendere precauzioni per proteggersi dai software maligni non è più un lusso ma una necessità. Si consideri l'importanza dei dati presenti nel proprio computer e il tempo, la fatica e il denaro che occorrerebbero per sostituire questi dati se andassero persi o se un'infezione da virus li rendesse inutilizzabili. È sufficiente confrontare questa eventualità con i tempi ridotti e il limitato sforzo necessario per predisporre alcune semplici misure di sicurezza, per capire l'utilità di proteggersi dalle infezioni.

La protezione del proprio computer dai virus è essenziale anche quando i dati presenti nel sistema non sono di fondamentale importanza. L'assenza di un'adeguata protezione potrebbe infatti permettere a un virus di insediarsi nel proprio computer e diffondersi poi alle macchine di collaboratori e colleghi. Controllando periodicamente il disco rigido con VirusScan, si riduce significativamente la propria vulnerabilità alle infezioni e si evitano inutili sprechi di tempo e denaro, oltre a dannose perdite di dati.

VirusScan fornisce tutti gli strumenti necessari per mantenere il sistema intatto e sicuro. Se usato correttamente, come parte di un completo programma di sicurezza che include backup, protezione tramite password, addestramento e consapevolezza, VirusScan può proteggere il computer da attacchi nocivi e impedire la diffusione di software dannosi nella propria rete.

I componenti di VirusScan

VirusScan include vari gruppi di componenti, formati da uno o più programmi collegati, ognuno caratterizzato da un ruolo preciso nella difesa del computer contro i virus e altri software dannosi. I gruppi di componenti sono:

- **Componenti comuni.** Questo gruppo include i file di dati e altri file di supporto condivisi da molti programmi di componenti VirusScan. Tra di essi ci sono i file di definizione del virus VirusScan virus (.DAT), i file di configurazione predefinita, i file di convalida e altri.

- **Scanner della riga di comando.** Questo gruppo include SCANPM.EXE, un agente di scansione potente per ambienti a 32 bit, e BOOTSCAN.EXE, uno scanner specifico più piccolo. Entrambi i programmi consentono di avviare operazioni di scansione mirata dalla finestra del prompt di MS-DOS o da modalità MS-DOS protetta. Normalmente si usa l'interfaccia utente grafica di VirusScan per eseguire la maggior parte delle procedure di scansione, ma quando non si riesce ad avviare Windows o i componenti dell'interfaccia grafica di VirusScan non funzionano nel proprio sistema, è possibile usare in sostituzione i programmi della riga di comando.

  SCANPM.EXE fornisce uno scanner completo per ambienti DOS con modalità protetta a 16 e 32 bit e include il supporto per assegnazioni di memoria estesa e memoria flessibile. Per utilizzare lo scanner, aprire una finestra del prompt di MS-DOS oppure riavviare il computer in modalità MS-DOS, quindi eseguire SCANPM.EXE dalla riga di comando, con le opzioni di scansione desiderate. Vedere Appendice E, "Utilizzo delle opzioni della riga di comando VirusScan", per l'elenco e la descrizione delle opzioni disponibili.

  VirusScan utilizza BOOTSCAN.EXE sul disco di emergenza per fornire un ambiente di avvio senza virus. Quando si esegue la procedura guidata per la creazione del Disco di emergenza, VirusScan copia BOOTSCAN.EXE, un determinato gruppo di file .DAT, e avvia i file a un solo floppy disk. Questo disco consente di avviare il computer, eseguire la scansione della memoria e del record MBR (Master Boot Record), del settore di boot e dei file di sistema sul disco rigido.

BOOTSCAN.EXE non rileva o pulisce i virus delle macro, ma rileva o pulisce altri virus che possono mettere a repentaglio l'installazione di VirusScan o infettare file all'avvio del sistema. Dopo aver identificato e risposto ai virus, è possibile eseguire VirusScan per pulire il resto del sistema, a condizione che nessun altro programma venga eseguito contemporaneamente.

- **VirusScan.** Questo componente offre un controllo estremamente completo sulle operazioni di scansione. è possibile avviare una scansione in qualsiasi momento (questa funzione è nota con il nome di "scansione su richiesta"), specificare come obiettivi della scansione dischi locali o dischi di rete, scegliere il modo in cui VirusScan dovrà rispondere a qualsiasi infezione rilevata e visualizzare report completi sulle azioni eseguite. È possibile iniziare con la modalità di configurazione base di VirusScan, quindi passare alla modalità avanzata per ottenere la massima flessibilità. Vedere "Uso di McAfee VirusScan" a pagina 153 per i dettagli.

- **VShield.** Questo componente fornisce una protezione costante dai virus contenuti in dischetti, contratti dalla propria rete o caricati in memoria. VShield viene avviato insieme al computer e rimane in memoria fino all'arresto del sistema. Un flessibile gruppo di pagine di proprietà permette di indicare a VShield le parti del sistema da scandire, il momento in cui scandirle, le parti da tralasciare e il modo in cui trattare i file infetti eventualmente rilevati. Inoltre VShield è in grado di avvertire l'utente quando rileva un virus e di generare report che riassumono tutte le azioni eseguite.

  L'ultima versione di VShield include la tecnologia per la protezione contro le applet Java e i controlli ActiveX ostili. Grazie a questa nuova funzionalità VShield scandisce automaticamente i messaggi di posta e gli allegati che l'utente riceve via Internet attraverso i programma Lotus cc:Mail, Microsoft Mail o altri client di posta che supportano lo standard Microsoft Messaging Application Programming Interface (MAPI). Inoltre può filtrare le classi Java e i controlli ActiveX ostili, confrontandoli con un proprio database interno di classi e controlli notoriamente dannosi. Quando rileva una corrispondenza con uno degli elementi del proprio database, VShield ne avverte l'utente oppure nega automaticamente agli oggetti dannosi l'accesso al sistema. VShield può inoltre impedire al computer di collegarsi a siti Internet pericolosi. è sufficiente indicare i siti che il proprio browser deve evitare di visitare e VShield impedirà automaticamente l'accesso a essi. La protezione di sicurezza tramite password per le proprie opzioni di configurazione impedisce agli altri utenti di effettuare modifiche non autorizzate. Dalla stessa finestra di dialogo è possibile impostare le opzioni di configurazione per tutti i moduli VShield. Per ulteriori dettagli Vedere "Uso di VShield" a pagina 81.

- **Scansione di cc:Mail.** Questo componente include una tecnologia ottimizzata per la scansione delle caselle di posta Lotus cc:Mail che non utilizzano lo standard MAPI. Si consiglia di installare e usare questo componente se il proprio gruppo di lavoro o la propria rete utilizza cc:Mail v6.x o una versione precedente. Vedere "Selezione delle opzioni di Rilevamento" a pagina 108 per ulteriori dettagli.

- **MAPI Scanner.** Questo componente consente di eseguire la scansione della Posta in arrivo e di un'altra casella di posta per le applicazioni client di posta elettronica che aderiscono allo standard MAPI. Si consiglia di usarlo come supplemento alla scansione continua in background che VShield fornisce per i client MAPI, quali Exchange e Outlook. Vedere "Scansione di posta elettronica in Microsoft Exchange e Outlook" a pagina 241

- **Pianificatore VirusScan.** Questo componente permette di definire le attività che VirusScan dovrà eseguire. Una "attività" può consistere in vari compiti, dalla scansione di un gruppo di dischi in un determinato momento o a intervalli prestabiliti, all'impostazione di VShield perché venga eseguito con determinate opzioni. Il Pianificatore contiene un elenco predefinito di attività che assicurano un livello di protezione minimo del proprio sistema. è possibile ad esempio scandire e ripulire immediatamente la propria unità C: o tutti i dischi del proprio computer e attivare o disattivare VShield. Vedere "Pianificazione delle attività di scansione" a pagina 183 per i dettagli.

- **McAfee ScreenScan.** Questo componente opzionale scandisce il computer quando lo screen saver è attivo, ovvero nei momenti in cui la macchina è accesa ma inattiva. Vedere "Uso di ScreenScan" a pagina 256 per i dettagli.

- **Documentazione.** La documentazione di VirusScan include:

  – Una *Guida introduttiva*, che presenta il prodotto, fornisce le istruzioni per l'installazione, spiega come agire quando si sospetta che il proprio computer sia stato infettato da un virus e fornisce una panoramica del prodotto. La *Guida introduttiva* è disponibile solo con le copia di VirusScan distribuite su dischi CD-ROM—non è possibile scaricarla dal sito web di Network Associates o da altri servizi elettronici.

  – Questo *Manuale dell'utente* è fornito sul CD-ROM di VirusScan o installato sul proprio disco rigido nel formato .PDF di Adobe Acrobat. Il *Manuale dell'utente* descrive nei dettagli le modalità di utilizzo di VirusScan e fornisce altre utili informazioni, dal background alle opzioni di configurazione avanzate. I file Acrobat .PDF sono flessibili documenti in linea contenenti collegamenti ipertestuali e altri strumenti che facilitano la navigazione del documento e il recupero delle informazioni.

Per ottenere i migliori risultati nell'apertura e nella stampa della *Guida dell'utente*, Network Associates consiglia di utilizzare Acrobat Reader 3.0—Reader versione 3.0.1 non riesce a stampare correttamente le immagini incluse nel file .PDF.

– Un file di guida in linea. La guida in linea fornisce all'utente un accesso rapido a consigli e suggerimenti sull'uso di VirusScan. Per aprire la guida in linea dall'interno di VirusScan o dall'interno di Pianificatore VirusScan, scegliere **Argomenti della Guida** dal menu **Guida**.

  VirusScan include inoltre una funzione di guida in linea sensibile al contesto. Per visualizzare gli argomenti di guida contestuali, fare clic con il pulsante destro del mouse su pulsanti, caselle di riepilogo o altri elementi presenti nelle finestre di dialogo. Per aprire il file di guida principale per un determinato argomento, fare clic sui pulsanti **Guida** quando sono presenti.

– Il file README.1ST o LICENSE.TXT. Questo file riporta i termini del contratto di licenza per l'uso di VirusScan. è indispensabile leggerlo con attenzione perché installando VirusScan l'utente accetta automaticamente tutti i termini di tale contratto.

– Il file WHATSNEW.TXT. Questo file contiene le ultime aggiunte e modifiche apportate alla documentazione del programma, elenca eventuali comportamenti del programma rilevati o altre questioni relative alla presente versione del prodotto e spesso descrive nuove funzioni del software incorporate negli aggiornamenti incrementali. Il file WHATSNEW.TXT si trova al livello principale del CD-ROM VirusScan o nella cartella di programma di VirusScan. È possibile aprirlo e stamparlo dal Blocco note di Windows e da quasi tutti gli elaboratori di testi.

Quando eseguire la scansione per la ricerca di virus

Perché l'ambiente di lavoro risulti sicuro, è necessario eseguire regolarmente scansioni per la ricerca di virus. La frequenza ottimale con cui eseguire tali scansioni dipende dalla frequenza con cui si scambiano dischetti con altri utenti, si condividono file sulla propria rete locale o si interagisce con altri computer attraverso Internet. In alcuni casi può essere sufficiente eseguire una scansione del sistema una volta al mese e in altri potrebbero essere necessarie più scansioni al giorno. Per la sicurezza del sistema, inoltre, è buona norma effettuare una scansione appena prima di eseguire il backup dei dati, prima di installare nuovi programmi o aggiornamenti, in particolare se sono stati scaricati da altri computer, e quotidianamente al momento dell'avvio e dell'arresto del sistema.

Si consiglia l'utilizzo di VShield per scandire la memoria del proprio computer e mantenere un livello di vigilanza costante fra una scansione e l'altra. Nella maggior parte dei casi questo dovrebbe essere sufficiente per preservare l'integrità del proprio sistema.

Se ci si connette a Internet con una certa frequenza o si scaricano spesso dei file, è utile affiancare alle scansioni regolari delle scansioni aggiuntive effettuate in corrispondenza di tali eventi. VirusScan include un gruppo predefinito di attività di scansione che aiutano l'utente a monitorare il sistema nei momenti in cui l'ingresso di virus è più probabile, ad esempio

- Quando si inserisce un floppy disk nell'unità floppy del computer
- Quando si avvia un'applicazione o si apre un file
- Quando ci si collega o si mappa un'unità di rete al proprio sistema

Anche la più completa scansione, tuttavia, potrebbe non riuscire a rilevare nuovi virus, se il software antivirus non è aggiornato. L'acquisto di VirusScan comporta per l'utente il diritto agli aggiornamenti gratuiti ai nuovi virus per l'intera vita del prodotto. Il programma quindi può essere continuamente aggiornato, affinché conservi appieno la propria efficacia. Se si installa il software client Network Associates SecureCast, VirusScan avverte l'utente quando è necessario aggiornare i file di dati e propone di scaricarli autonomamente. Per informazioni su come aggiornare il proprio sistema, vedere Appendice A, "Uso di SecureCast per l'aggiornamento del software" e "Configurazione delle opzioni di Aggiornamento automatico" a pagina 216.

Riconoscere quando non è presente alcun virus

I personal computer, nonostante la loro breve vita, si sono evoluti a tal punto da essere oggi macchine estremamente complesse che eseguono software sempre più sofisticati. Anche il più lungimirante fra i produttori dei primi PC non avrebbe mai potuto immaginare le attività per le quali i vari tipi di utenti, dagli scienziati ai grafici, sfruttano oggi la velocità, la flessibilità e la potenza dei moderni PC. Ma questa potenza comporta un prezzo: i conflitti hardware e software abbondano, le applicazioni e i sistemi operativi si bloccano con frequenza e centinaia di altri problemi possono verificarsi nei contesti più impensati. Tali problemi, in alcuni casi, possono ricordare gli effetti distruttivi derivanti da un'infezione da virus. Altri problemi, poi, sembrano privi di spiegazione logica o impossibili da diagnosticare, per cui gli utenti frustrati, forse come ultima risorsa, incolpano di tutto una misteriosa infezione da virus.

Ma quando la causa del problema è effettivamente un virus, di solito è possibile eliminare l'infezione in modo relativamente facile e rapido, in quanto i virus lasciano tracce nel sistema che possono essere individuate e rimosse.

Eseguendo una completa scansione del sistema con VirusScan vengono rilevate tutte le varianti di virus conosciute che possono infettare il computer, oltre ad alcune varianti prive di un nome noto o di un comportamento definito. Ciò non è di grande aiuto quando il problema deriva effettivamente da un conflitto di interrupt, ma se non altro permette di escludere una possibile causa. È possibile quindi proseguire la ricerca e risoluzione dei problemi del sistema con un'utility di diagnosi del sistema completa come McAfee Nuts & Bolts.

Più grave poi è la confusione generata dai programmi tipo virus, dai programmi che simulano virus e dai programmi che violano la sicurezza. I programmi antivirus non possono rilevare e reagire ad agenti di distruzione definiti "cavalli di Troia" che non sono mai apparsi prima. Inoltre non possono reagire ai programmi che violano la sicurezza, ovvero che permettono agli hacker di impedire l'accesso alla rete e bloccare i sistemi, e neppure possono reagire alla convinzione dell'utente che un virus sia presente nel sistema quando ciò non è vero.

Il modo migliore per scoprire se un blocco del computer dipende da un attacco da virus è effettuare una completa scansione e valutare con attenzione i risultati. Se VirusScan non rileva infezioni, le probabilità che il problema derivi da un virus sono molto limitate ed è consigliabile cercare altre cause. Inoltre, nella remota eventualità che VirusScan non riesca a rilevare un virus macro o un altro tipo di virus che ha effettivamente infettato il sistema, sono molto ridotte le probabilità che possano verificarsi a breve gravi problemi. Si può comunque confidare nel fatto che i ricercatori di Network Associates identificheranno immediatamente il nuovo virus, lo isoleranno e aggiorneranno VirusScan in modo che possa individuarlo e, se possibile, rimuoverlo quando lo incontra. Per informazioni su come aiutare i ricercatori a scoprire nuovi virus, vedere "Notifica di informazioni utili per l'aggiornamento dei file antivirus" a pagina xxiv.

Installazione di McAfee VirusScan 2

Prima di iniziare

Network Associates distribuisce McAfee VirusScan in due modi diversi: come file scaricabile dal sito Web di Network Associates o da altri servizi elettronici e come disco CD-ROM. Dopo aver scaricato un archivio VirusScan o inserito il disco di installazione del programma nell'unità CD-ROM, la procedura di installazione è identica per entrambi i tipi di distribuzione. Rivedere i requisiti di sistema indicati qui sotto per verificare che il sistema sia idoneo all'uso di VirusScan, quindi eseguire la procedura di installazione riportata a pagina 38.

❑ **NOTA:** Alcuni gruppi di componenti VirusScan sono disponibili solo nella versione su CD-ROM del prodotto. Per ulteriori dettagli, rivolgersi al proprio fornitore di fiducia.

Requisiti di sistema

VirusScan può essere installato ed eseguito su qualsiasi PC IBM o PC compatibile dotato di:

- Processore equivalente a Intel 80386 o superiore. Network Associates consiglia, come dotazione minima, un processore di classe Intel Pentium o compatibile.
- Unità CD-ROM. Se la copia di VirusScan è stata scaricata, l'unità CD-ROM non è richiesta.
- Come minimo 15MB di spazio libero su disco per l'installazione completa.
- Almeno 8MB di RAM.
- Microsoft Windows 95 o Microsoft Windows 98.

Altri suggerimenti

Per sfruttare pienamente le funzioni di aggiornamento automatico di VirusScan, è necessario disporre di una connessione a Internet. La connessione può essere attivata attraverso una rete locale oppure con un modem ad alta velocità e l'iscrizione a un provider di servizi Internet.

NOTA: Network Associates *non* fornisce connessioni a Internet. Contattare il centro assistenza locale per conoscere tariffe e condizioni di intervento oppure rivolgersi all'amministratore del sistema per informazioni sulla connessione a Internet tramite la rete aziendale.

La procedura di installazione

Scegliere il tipo di distribuzione proprio della copia di VirusScan di cui si dispone, quindi seguire i corrispondenti passaggi al fine di preparare i propri file per l'installazione.

- **Se la copia di VirusScan è stata scaricata** dal sito Web di Network Associates, da un server sulla rete locale oppure da un altro servizio elettronico, creare una cartella temporanea sul disco rigido e usare WinZip, PKZIP o un programma di utility analogo per estrarre i file di installazione di VirusScan nella cartella temporanea. I programmi di utility necessari possono essere scaricati da molti servizi in linea.

  IMPORTANTE: Se esiste il rischio che sul computer in uso sia presente un virus, evitare di scaricarvi i file di installazione di VirusScan. È necessario scaricare i file in un computer che ***non*** sia infetto. Installare la copia di VirusScan su questo computer, quindi usare il programma di utility McAfee Disco di soccorso durante l'installazione in modo da creare un disco che possa essere utilizzato per effettuare il boot del computer infetto e rimuovere il virus. Vedere "Quando si sospetta la presenza di un virus," a pagina 59 per ulteriori informazioni.

- **Se la copia di VirusScan disponibile è su CD-ROM**, inserire il disco nell'unità CD-ROM.

Quando si inserisce il CD-ROM, compare la schermata introduttiva di VirusScan, simile a quella mostrata alla Figura 2-1 a pagina 39.

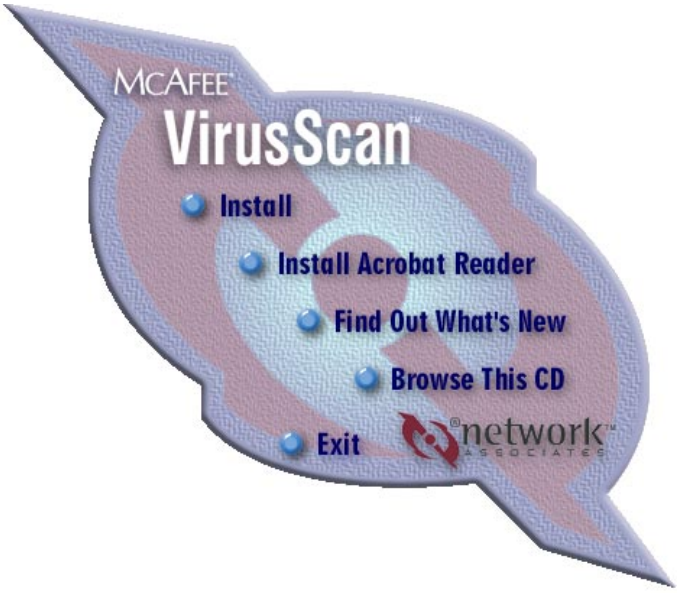

Figura 2-1. La finestra introduttiva di McAfee VirusScan

Per installare subito VirusScan, fare clic su **Installa VirusScan**, quindi passare al Passaggio 3 a pagina 40 per continuare l'installazione.

Se la schermata introduttiva non compare oppure se si installa VirusScan dai file scaricati, iniziare dal Passaggio 1.

Procedere come segue:

1. Scegliere **Esegui** dal menu **Avvio** nella barra delle applicazioni di Windows.

   Viene visualizzata la finestra di dialogo Esegui (Figura 2-2).

Figura 2-2. La finestra di dialogo Esegui

2. Digitare <X>:\SETUP.EXE nell'apposita casella di testo, quindi fare clic su **OK**.

   La <X> rappresenta la lettera della propria unità CD-ROM o il percorso della cartella contenente i file di VirusScan estratti. Per ricercare i file sul disco rigido o sul CD-ROM, fare clic su **Sfoglia**.

NOTA: Se la copia di VirusScan disponibile proviene da un CD-ROM VirusScan Security Suite o Total Virus Defense, è necessario indicare anche la cartella contenente VirusScan per Windows 95 e Windows 98. Per ulteriori dettagli, consultare il file SOMMARIO.TXT incluso nel CD-ROM.

Il programma di installazione avvia e visualizza la schermata introduttiva (Figura 2-3).

Figura 2-3. La finestra della funzione guidata di installazione

3. Fare clic su **Avanti>** per procedere.

   La successiva finestra della funzione guidata mostra il contratto di licenza per gli utenti di VirusScan. Leggere attentamente i termini dell'accordo. L'installazione di VirusScan comporta l'automatica accettazione del contratto.

4. Se non si intende accettare il contratto di licenza, fare clic su **No**. La procedura di installazione viene sospesa immediatamente. Se invece si intende accettare i termini del contratto di licenza, fare clic su **Sì** per procedere.

   Se si installa la nuova versione di VirusScan su una versione esistente del programma, il programma di installazione rileva la versione esistente e permette di rimuoverla dal computer (Figura 2-4).

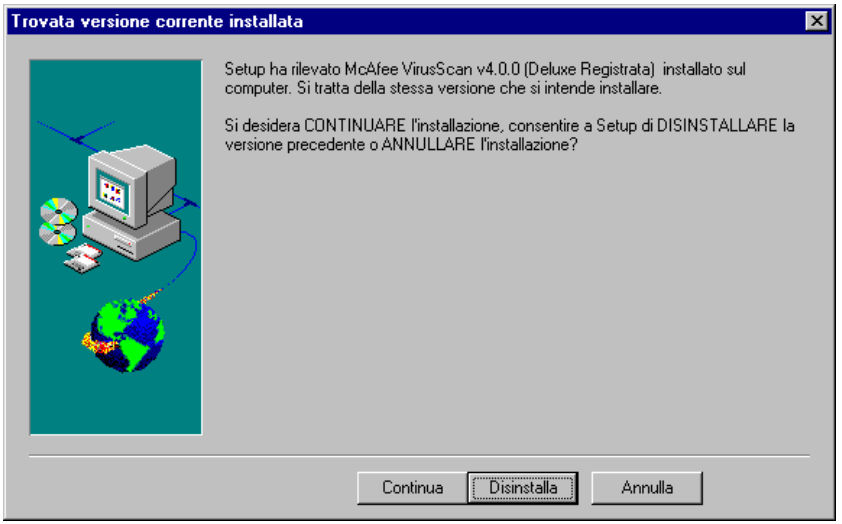

Figura 2-4. La finestra Rilevata versione già installata

5. Per continuare, è possibile

   - Fare clic su **Conserva** per mantenere le impostazioni scelte per l'installazione esistente di VirusScan. Il programma di installazione manterrà i file delle impostazioni ma rimuoverà i restanti file di programma di VirusScan.

     NOTA: Le impostazioni saranno mantenute solo per VirusScan versione 4.0.1 o successiva. Tenterà di mantenere le impostazioni di VirusScan v3.x, ma non quelle di VirusScan v2.x o WebScanX v3.1.6 o precedente.

   - Fare clic su **Rimuovi** per eliminare la versione di VirusScan esistente e tutte le relative impostazioni dal computer. Al termine dell'operazione, il programma di installazione visualizzerà la schermata mostrata nella Figura 2-5 a pagina 42. È possibile proseguire con il Passaggio 6.

- Fare clic su **Esci dall'installazione** per interrompere il processo. Se si effettua questa seconda scelta, verrà chiesto di confermare l'interruzione dell'installazione. Fare nuovamente clic su **Esci dall'installazione** per interrompere o su **Riprendi** per continuare l'installazione.

Se si continua, il programma di installazione rimuoverà la versione esistente di VirusScan, mantenendo le impostazioni precedenti, se è stata scelta questa opzione. Al termine dell'operazione, sarà visualizzata la schermata relativa al tipo di installazione (Figura 2-5).

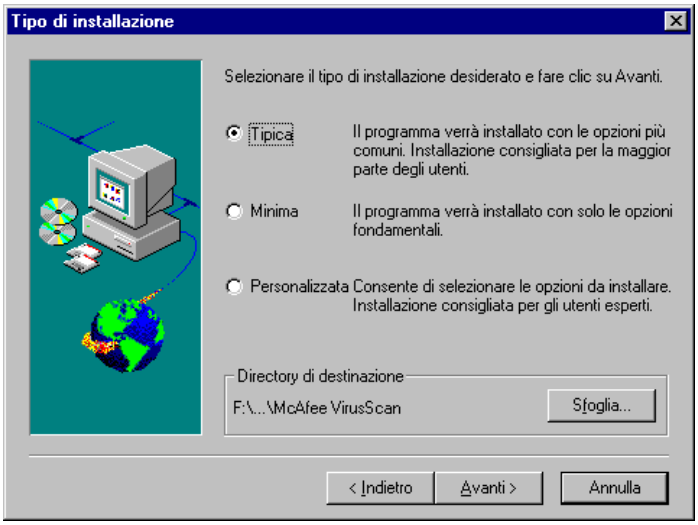

Figura 2-5. La finestra Tipo di installazione

6. Selezionare i gruppi di componenti di VirusScan che si desidera installare. è possibile scegliere fra le seguenti opzioni:

   - **Tipica.** Selezionare questa opzione per installare la funzione di scansione della riga di comando di VirusScan; la funzione di scansione su richiesta di VirusScan; la funzione di scansione all'eccesso VShield; la funzione di scansione del client MAPI; il Pianificatore VirusScan e file comuni utilizzati da tutti i componenti dei programmi. Network Associates consiglia questo tipo di installazione per la maggior parte degli utenti.

   - **Minima.** Scegliere questa opzione per installare le funzioni di scansione della riga di comando di VirusScan, la funzione di scansione all'accesso VShield e la funzione di scansione su richiesta di VirusScan. Network Associates consiglia questo tipo di installazione se lo spazio libero su disco è ridotto o se sono presenti altri vincoli relativi al sistema.

- **Personalizzata.** Scegliere questa opzione per installare, a scelta, i componenti desiderati di VirusScan. Come impostazione predefinita, l'opzione Personalizzata installa gli stessi componenti dell'opzione Tipica, ma si può anche scegliere di installare cc:Mail Scan, un'opzione plug-in che consente a VShield di cercare i virus in Posta in arrivo di Lotus cc:Mail (Vedere "Selezione delle opzioni di Rilevamento" a pagina 108 per i dettagli) e ScreenScan, un'utility di scansione che esamina il sistema alla ricerca di virus ogni volta che è attivo lo screen saver.

7. Fare clic su **Sfoglia** per individuare la cartella che si desidera usare per l'installazione. In base all'impostazione predefinita, VirusScan viene installato nel seguente percorso:

   C:\Programmi\Network Associates\McAfee VirusScan

8. Dopo avere scelto il gruppo di componenti che si desidera installare e avere specificato una destinazione, fare clic su **Avanti>** per procedere.

   - **Se si è scelto un gruppo di componenti dell'installazione Tipica o Minima**, viene visualizzata una finestra della funzione guidata che elenca i componenti scelti e la cartella di destinazione specificata. In base all'impostazione predefinita, il programma di installazione, prima di installare VirusScan, ricerca eventuali virus esistenti nelle partizioni e nei settori di boot del disco rigido oltre che nella memoria del computer. Inoltre, aggiunge il comando **Ricerca di virus** ai menu di scelta rapida che appaiono quando si fa clic con il pulsante destro del mouse sugli oggetti disposti sul desktop e in Gestione risorse (Windows 95) o Esplora risorse (Windows 98).

     Se le opzioni elencate sono quelle che effettivamente si intende scegliere, fare clic su **Avanti>**. Diversamente, fare clic su **<Indietro** per modificare le scelte. **Passare al** Passaggio 9 a pagina 44.

   - **Se è stato scelto un gruppo di componenti dell'installazione Personalizzata**, viene visualizzata una finestra nella quale sono elencati i componenti che possono essere installati (Figura 2-6 a pagina 44). Selezionare i componenti che si desidera aggiungere e deselezionare le caselle di controllo dei componenti che si desidera escludere dall'installazione.

     Selezionando i componenti, la relativa descrizione viene visualizzata nella parte inferiore della finestra. Una volta terminate le selezioni, fare clic su **Avanti>**.

Figura 2-6. La finestra Selezione componenti

In base all'impostazione predefinita, il programma di installazione, prima di completare l'installazione, ricerca attraverso VirusScan eventuali virus presenti nelle partizioni e nei settori di boot del disco rigido oltre che nella memoria del computer. Inoltre, aggiunge il comando per la ricerca di virus ai menu di scelta rapida che appaiono quando si fa clic con il pulsante destro del mouse sugli oggetti presenti sul desktop e in Gestione risorse (Windows 95) o Esplora risorse (Windows 98). Fare clic su **Avanti>** nella parte inferiore di ciascuna delle due finestre per continuare.

Se si preferisce che il programma di installazione non esegua queste operazioni, deselezionare tutte le caselle di controllo, quindi fare clic su **Avanti >** per continuare.

Il programma di installazione avvierà rapidamente VirusScan per ricercare virus sul disco rigido e nella memoria prima di proseguire.

9. Se il sistema risulta essere esente da virus, fare clic su **OK** per procedere. Se viene rilevata un'infezione da virus, uscire immediatamente dal programma di installazione. Vedere "Quando si sospetta la presenza di un virus," a pagina 59 per informazioni su come procedere in questa situazione.

10. Il programma di installazione inizia a copiare i file di VirusScan sul computer. Quando la copia dei file è quasi terminata, il programma chiede se si desidera creare un disco di emergenza (Figura 2-7).

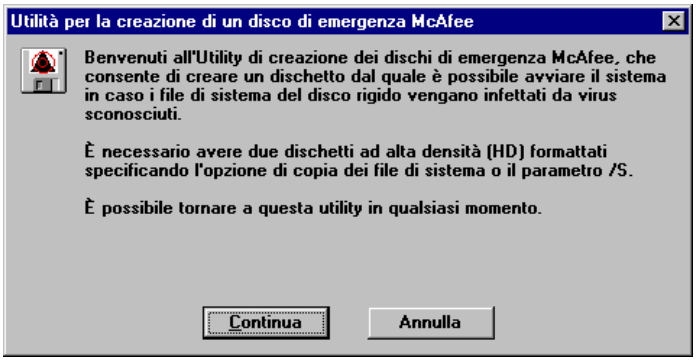

Figura 2-7. Finestra della funzione guidata di creazione del disco di emergenza

11. Per tralasciare questo passaggio, fare clic su **Annulla**, quindi passare al Passaggio 16. Sarà possibile creare un disco di emergenza dopo l'installazione. Per creare un disco di emergenza ora, fare clic su **Avanti>**.

NOTA: Network Associates consiglia comunque di creare un disco di emergenza durante l'installazione, ma dopo che VirusScan ha analizzato il sistema per la ricerca di virus. Se VirusScan rileva la presenza di un virus nel sistema, occorre *evitare assolutamente* di creare un disco di emergenza sul computer infetto.

---

12. Viene visualizzata la finestra successiva della procedura guidata (vedere Figura 2-8 a pagina 46). Sono disponibili due scelte:

    - Se si dispone di un dischetto *formattato ed esente da virus* che contiene solo file di sistema DOS o Windows, inserirlo nell'unità floppy. Quindi selezionare la casella di controllo **Non formattare** e fare clic su **Avanti>** per continuare.

      In questo modo la funzione guidata Disco di emergenza copia sul dischetto solo il componente della riga di comando VirusScan e i relativi file di supporto. Andare al Passaggio 13 a pagina 47 per continuare.

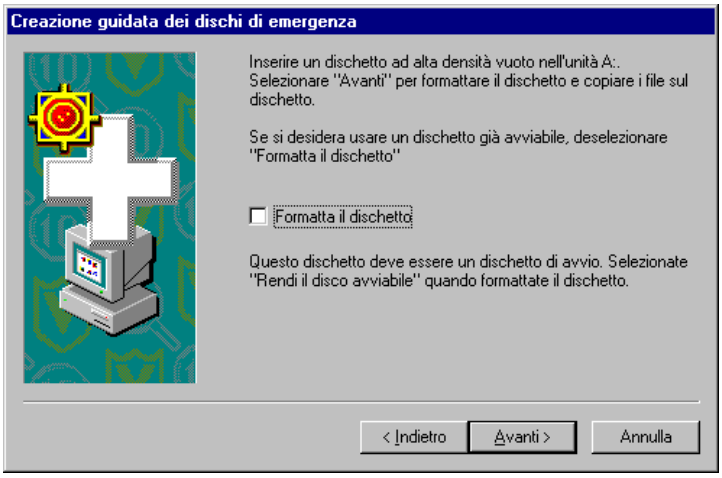

Figura 2-8. Seconda finestra di creazione guidata del disco di emergenza

- Se *non* si dispone di un dischetto formattato ed esente da virus con i file di sistema DOS o Windows, è necessario crearne uno al fine di utilizzare il disco di emergenza per avviare il computer. Procedere come segue:

  a. Inserire un dischetto *non formattato* nell'unità floppy.

  b. Verificare che la casella di controllo **Non formattare** non sia selezionata.

  c. Fare clic su **Avanti>**.

     Viene visualizzata la finestra di dialogo di formattazione del disco di Windows (Figura 2-9 a pagina 47).

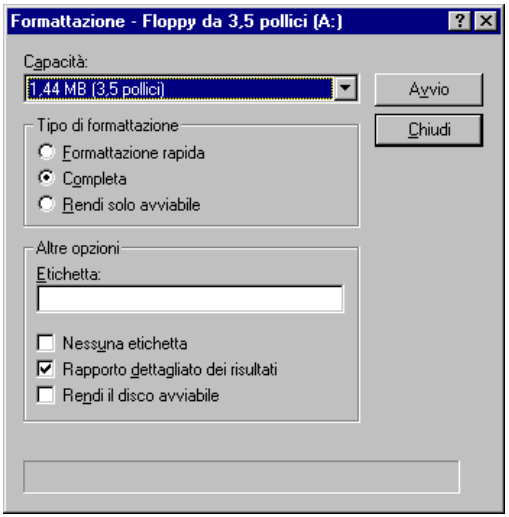

Figura 2-9. Finestra di dialogo di formattazione di Windows

d. Verificare che la casella di controllo **Completa** nella sezione **Tipo di formattazione** e la casella di controllo **Copia file di sistema** nella sezione **Altre opzioni** siano entrambe selezionate. Fare clic sul pulsante **Avvio**.

   Windows formatterà il dischetto e copierà i file di sistema necessari per avviare il computer.

e. Al termine della formattazione del disco, fare clic su **Chiudi**. Fare clic nuovamente su **Chiudi** per tornare alla finestra Disco di emergenza.

13. Fare clic su **Avanti>** per procedere. Il programma di installazione scandisce nuovamente il disco formattato per cercare eventuali virus (Figura 2-10 a pagina 48).

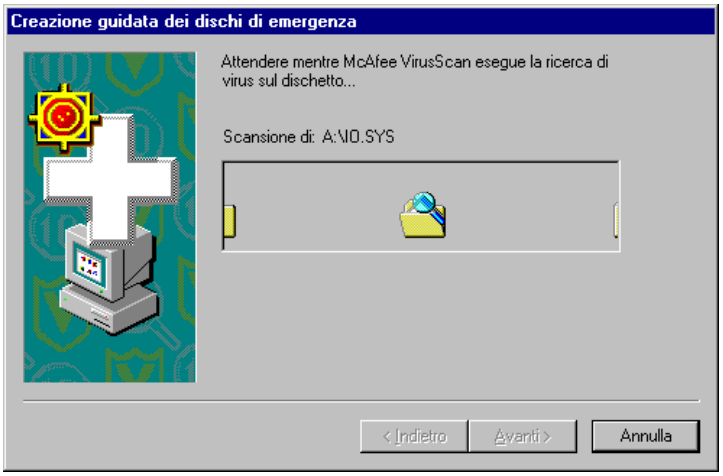

Figura 2-10. Scansione antivirus del disco di emergenza

Se VirusScan non rileva alcun virus durante la scansione, il programma di installazione copia immediatamente BOOTSCAN.EXE e i file di supporto sul dischetto creato. Se VirusScan *rileva* un virus, chiudere immediatamente il programma di installazione. Vedere "Quando si sospetta la presenza di un virus," a pagina 59 per informazioni su come procedere.

14. Quando la funzione guidata ha finito di copiare i file del disco di emergenza, visualizza la finestra finale della procedura guidata (Figura 2-11).

Figura 2-11. Finestra finale della creazione guidata del disco di emergenza

15. Fare clic su **Fine** per tornare al programma di installazione. Rimuovere il disco di emergenza dall'unità floppy, etichettarlo e riporlo in un luogo sicuro.

> **NOTA:** Un dischetto è protetto quando sul lato opposto a quello dello sportellino metallico sono aperte entrambe le finestrelle. Se è aperta una sola di esse, aprire anche l'altra spostando il cursore che scorre all'interno fino a quando si blocca in posizione aperta.

Il programma di installazione finirà la copia dei file di installazione di VirusScan sul disco rigido, quindi elencherà i nomi dei file di sistema che ha modificato. Viene incluso anche il file AUTOEXEC.BAT perché ad esso è stata aggiunta una riga per indicare a VirusScan di eseguire le operazioni di scansione ogni volta che si avvia il computer. Il programma di installazione crea una copia del file AUTOEXEC.BAT originale e la rinomina, aggiungendo un'estensione diversa, nel caso si rendesse necessario ripristinare il file precedente.

16. Prendere nota del nome utilizzato dal programma di installazione per rinominare il file AUTOEXEC.BAT per riferimento futuro, quindi fare clic su **Avanti >** per proseguire.

17. Il programma di installazione richiede di riavviare il computer per completare l'installazione di VirusScan. Ciò garantisce inoltre che il componente VShield inizi la scansione antivirus immediatamente. Se vi sono lavori urgenti da svolgere, selezionare **No, riavvierò il computer in seguito**, quindi fare clic su **Fine**. Altrimenti selezionare **Sì, riavvia il computer ora**, quindi fare clic su **Fine** per riavviare il sistema.

> **IMPORTANTE:** Network Associates consiglia comunque di riavviare subito il computer, al fine di attivare immediatamente la protezione antivirus di VShield. Se la copia di VirusScan è stata scaricata e si desidera convalidarla, farlo *prima* di riavviare. Vedere "Convalida dei file"per informazioni su come effettuare questo controllo.

Esecuzione di un'installazione in background

Se si gestisce una rete e si intende impiegare VirusScan come applicazione antivirus standard, è possibile utilizzare la funzione di installazione in background del programma per installare VirusScan su ogni nodo della rete senza o con scarsa interazione da parte dell'utente finale. Durante tale processo, il programma di installazione non visualizza alcun pannello o finestra di funzione guidata né offre all'utente finale opzioni di configurazione.

L'impostazione di tali opzioni e l'esecuzione del programma di installazione avvengono in background su ciascuna workstation di destinazione. Se lo si desidera, è addirittura possibile installare VirusScan su workstation incustodite, senza che l'utente finale ne sia a conoscenza, purché si disponga di tutti i privilegi di amministrazione necessari.

Un'installazione in background è costituita da due passaggi principali. Innanzi tutto, è necessario installare sul computer o sul server di amministrazione gli stessi componenti VirusScan che saranno installati su ogni singola workstation di destinazione. Una speciale modalità del programma di installazione registra le scelte effettuate durante l'installazione e le mantiene in un file di configurazione denominato SETUP.ISS. Quindi è necessario utilizzare una modalità diversa per installare una configurazione di VirusScan identica su ciascun sistema di destinazione. Il programma di installazione utilizzerà il file SETUP.ISS creato nel primo passaggio per guidare ciascuna installazione successiva.

Registrazione delle preferenze

Per registrare le preferenze di installazione, procedere nel modo seguente:

1. Cercare un file SETUP.ISS esistente nella cartella \WINDOWS del computer o del server di amministrazione. Se si trova un file con tale nome nella cartella di WINDOWS, rinominarlo oppure cancellarlo.

   Quando si registrano le preferenze, il programma di installazione le salva in un nuovo file SETUP.ISS nella stessa posizione.

2. Scegliere **Esegui** dal menu **Avvio** sulla barra delle applicazioni di Windows.

   Viene visualizzata la finestra di dialogo Esegui (Figura 2-12).

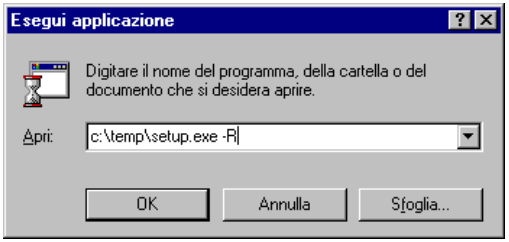

Figura 2-12. La finestra di dialogo Esegui

3. Digitare `<X>:\SETUP.EXE -R` nell'apposita casella di testo, quindi fare clic su **OK**.

   La `<X>` rappresenta la lettera dell'unità CD-ROM o il percorso della cartella contenente i file di VirusScan estratti. Il `-R` indica al programma di installazione l'esecuzione in modalità "registrazione".

NOTA: Se la copia di VirusScan fa parte di VirusScan Security Suite oppure del CD-ROM Total Virus Defense, è necessario specificare anche quale cartella contiene VirusScan per Windows 95 e Windows 98. Per ulteriori dettagli, leggere il file CONTENTS.TXT incluso con l'uno o l'altro pacchetto.

   Per cercare il file SETUP.EXE sul disco rigido o sul CD-ROM, fare clic su **Sfoglia**. Verificare di aggiungere il `-R` all'istruzione di esecuzione se si utilizza questa opzione.

4. Seguire i passaggi di installazione descritti alle pagine 41 a 49 per scegliere i componenti e le impostazioni da assegnare a ciascuna workstation di destinazione.

   Il programma di installazione annota le scelte fatte a ogni passaggio e le registra nel file SETUP.ISS.

IMPORTANTE: Prestare particolare attenzione durante l'installazione iniziale per rispondere alle domande che compaiono nelle finestre della procedura guidata della configurazione e seguire i passaggi di installazione nella sequenza presentata, altrimenti l'installazione in background che verrà eseguita in seguito sarà annullata. Non è possibile tornare indietro durante l'installazione per cambiare le impostazioni.

Per specificare opzioni diverse, è necessario iniziare nuovamente l'installazione affinché il programma di installazione possa registrare correttamente le scelte fatte. Se si intende installare VirusScan su workstation non custodite, verificare di specificare opzioni che non richiedono l'interazione dell'utente—ad esempio, non chiedere al programma di installazione di creare un disco d'emergenza.

L'installazione sarà annullata anche se VirusScan rileva la presenza di un virus sul computer o sul server.

5. Al termine dell'installazione, fare clic su **Fine** per uscire dal programma di installazione.

Modifica del file SETUP.ISS per specificare una directory di installazione

Se si desidera installare VirusScan in una directory specifica, è necessario modificare il file SETUP.ISS creato al momento dell'installazione di VirusScan sul computer o sul server di amministrazione. Per semplificare l'amministrazione della rete, ad esempio, è possibile installare tutte le copie di VirusScan nella stessa directory su ciascun nodo della rete stessa.

Il file SETUP.ISS è un file di testo con formattazione speciale simile ai file di configurazione WIN.INI o SYSTEM.INI ed è possibile aprirlo con qualsiasi editor di testo e modificarlo in base alle proprie esigenze.

NOTA: Network Associates consiglia di limitare le modifiche al file SETUP.ISS. Se si desidera il controllo completo del processo di installazione oppure si intende specificare in anticipo le opzioni di configurazione per ogni copia di VirusScan, è possibile utilizzare ISeamless, un potente strumento di scripting di Network Associates progettato espressamente a questo scopo. Contattare il Supporto tecnico di Network Associates per i dettagli.

SETUP.ISS specifica la directory di installazione come valore per la variabile **szDir,** elencata sotto l'intestazione **[SdSetupType-0]**. Come impostazione predefinita, la voce appare come segue:

```
[SdSetupType-0]
szDir=C:\Program Files\Network Associates\McAfee VirusScan\
Result=403
```

Per specificare una directory di installazione diversa, sostituire il percorso mostrato con quello desiderato. La directory di installazione specificata in questo punto avrà la precedenza sulla directory di installazione predefinita su ciascun sistema di destinazione.

IMPORTANTE: Il programma di installazione crea un file SETUP.ISS esclusivo per ogni prodotto Network Associates su ciascuna piattaforma. È necessario utilizzare il file che corrisponde al sistema operativo installato sulla workstation di destinazione. Ad esempio, non è possibile utilizzare un file SETUP.ISS creato durante l'installazione di VirusScan per Windows 95 per controllare un'installazione di VirusScan per Windows NT.

6. Salvare il file in formato testo, quindi uscire dall'editor di testo.

IMPORTANTE: Network Associates consiglia di utilizzare il file SETUP.ISS creato per eseguire un'installazione di prova su una singola workstation prima di usarlo per l'installazione di VirusScan in rete.

Esecuzione di un'installazione in background

Se esiste un file SETUP.ISS che elenca tutti i componenti e tutte le impostazioni che si desidera assegnare a ciascuna workstation della rete, è possibile duplicare tali impostazioni esattamente per ogni copia di VirusScan che si installa. Vedere "Registrazione delle preferenze" a pagina 50 per informazioni sulla creazione del file SETUP.ISS.

È possibile eseguire un'installazione in background in molti modi e con livelli diversi di interazione con gli utenti della rete. Ad esempio, è possibile creare uno script per gli utenti che esegua un'installazione in background di VirusScan non appena essi si collegano a un server di autenticazione, senza nessun'altra interazione a parte le operazioni necessarie per il login. Inoltre, è possibile chiedere agli utenti di eseguire l'installazione da un server designato. Altre opzioni ancora includono l'uso di VirusScan tramite un'applicazione di gestione di rete quale Zero Administration Client (ZAC) di Network Associates, System Management Server (SMS) di Microsoft o pacchetti simili.

Qualunque metodo si scelga, innanzi tutto è necessario preparare il pacchetto VirusScan per l'installazione, quindi eseguire il programma di installazione in modalità background.

Procedere come segue:

1. Copiare i file di installazione di VirusScan dal CD-ROM di VirusScan o dalla relativa cartella del computer di amministrazione in cui sono memorizzati nella directory VirusScan su un server centrale. Gli utenti o l'applicazione di gestione della rete installerà VirusScan su questo server.

2. Individuare il file SETUP.ISS memorizzato nella directory VirusScan sul server centrale. Rinominarlo o eliminarlo.

3. Copiare il file SETUP.ISS creato durante l'esecuzione dell'installazione registrata sul computer di amministrazione nella directory VirusScan sul server centrale. Il file necessario si trova nella directory WINDOWS sul computer di amministrazione. Vedere "Registrazione delle preferenze" a pagina 50 per sapere come registrare l'installazione.

   Al termine di questo passaggio, gli utenti o l'applicazione di gestione di rete eseguirà il programma di installazione in modalità background per duplicare l'installazione registrata.

Per eseguire il programma di installazione in modalità background, includere la riga `<X>:\SETUP.EXE -S` in qualsiasi script di login o istruzione per gli utenti che descriva come eseguire tale programma. In questa riga, `<X>` rappresenta il percorso della cartella sul server che contiene i file di installazione di VirusScan e il file SETUP.ISS creato. Il `-S` indica al programma di installazione l'esecuzione in modalità background. Per impostazione predefinita, il programma di installazione riavvia la workstation al termine dell'installazione dei file.

Se non si desidera che il programma di installazione riavvii ciascuna workstation di destinazione, è necessario modificare il file SETUP.ISS creato durante l'installazione registrata. Modificare il valore della voce **BootOption** sotto l'intestazione **[sdFinishReboot - 0]** dal valore corrente a zero (0). In questo modo, si indica al programma di installazione di non forzare il riavvio della workstation di destinazione.

Come ulteriore passo verso l'implementazione di una strategia antivirus coerente su tutta la rete, è possibile copiare un file di configurazione con le opzioni che gli utenti devono avere nella directory di installazione su ciascuna workstation. Inoltre, è possibile utilizzare la protezione tramite password per impedire le modifiche non autorizzate alle impostazioni di configurazione prescelte. Vedere "Uso dei menu di VirusScan" a pagina 155 per informazioni sul salvataggio delle impostazioni in un file di configurazione. Per sapere come proteggere le impostazioni tramite password, vedere "Attivazione della protezione tramite password" a pagina 181.

❑ **NOTA:** Per preimpostare le opzioni di configurazione in modo che VirusScan le installi già nella opposizione corretta, utilizzare il programma di utility ISeamless di Network Associates che fornisce controllo completo sulle opzioni di installazione e configurazione. Per ulteriori dettagli, contattare il rivenditore o il supporto tecnico Network Associates.

Convalida dei file

Lo scaricamento e la copia dei file da qualsiasi fonte esterna espone il computer al rischio, seppur limitato, di infezioni da virus. Lo scaricamento di software antivirus non fa eccezione a questa regola. Network Associates utilizza severe e complete misure di sicurezza per garantire l'integrità, l'affidabilità e l'immunità da virus dei prodotti acquistati e scaricati dal suo sito Web e dagli altri suoi servizi elettronici. Ma il software antivirus attira l'attenzione degli scrittori di programmi virus e di software cosiddetti "cavalli di Troia", alcuni dei quali si divertono a inviare copie infette di software commerciali o a usare gli stessi nomi di file per camuffare il loro lavoro.

È possibile proteggersi da questa evenienza oppure prevenire la possibilità che i file scaricati vengano corrotti facendo attenzione a:

- scaricare i file solo dal sito di Network Associates e
- convalidare i file scaricati.

Network Associates include una copia di VALIDATE.EXE, il proprio software di convalida, in ogni pacchetto VirusScan.

Per convalidare i propri file, procedere come segue:

1. Installare VirusScan con la procedura descritta in "La procedura di installazione" alle pagine 38 a 49.
2. Fare clic sul pulsante **Avvio** (Windows 95) o su **Start** (Windows 98) sulla barra delle applicazioni, scegliere **Programmi**, quindi **Prompt di MS-DOS**.
3. Nella finestra che appare, modificare la riga di comando in modo che porti alla directory contenente i file di VirusScan installati. Se sono state scelte le opzioni di installazione predefinite, il percorso dei file è il seguente:

   C:\Programmi\Network Associates\McAfee VirusScan

Per accedere a questa directory, digitare `cd progra~1\networ~1\mcafee~1` nella riga di comando, quindi premere INVIO. Se VirusScan è stato installato in un'altra directory, digitare il percorso corretto di quella directory.

4. Eseguire VALIDATE.EXE. Per farlo, digitare `validate *.*` nella riga di comando.

   VALIDATE.EXE scandisce tutti i file contenuti nella directory del programma VirusScan, quindi genera un elenco di tali file che ne indica i nomi, le dimensioni in byte, la data e l'ora di creazione e due codici di convalida in colonne diverse.

   Per utilizzare VALIDATE.EXE al fine di esaminare singoli file, è sufficiente far seguire alla parola `validate` il nome del file che si desidera verificare. È possibile inoltre usare i caratteri jolly del DOS `?` e `*` per specificare un gruppo di file.

   ❑ **NOTA:** Network Associates consiglia di inviare alla stampante i risultati di VALIDATE.EXE, per crearne una copia su carta, più facile da consultare. Se la stampante in uso è impostata per accettare i documenti prodotti dai programmi MS-DOS, è sufficiente digitare `validate *.* >lpt1` nella riga di comando. Per informazioni su come impostare la stampante affinché possa stampare dai programmi MS-DOS, consultare la documentazione di Windows.

   Per accertarsi di disporre esattamente degli stessi file usati dagli ingegneri che hanno preparato la copia di VirusScan, è necessario confrontare i codici di convalida con la packing list fornita con il programma. La packing list è un file di testo contenente i codici di convalida che gli ingegneri di Network Associates hanno generato da processi di controllo indipendente di tipo CRC (cyclical redundancy check) durante la preparazione di VirusScan per la commercializzazione. Questo metodo garantisce un alto livello di sicurezza e impedisce qualsiasi manomissione.

5. Per visualizzare la packing list, digitare `type packing.lst` al prompt della riga di comando, quindi premere INVIO.

   ❑ **NOTA:** Network Associates consiglia, anche questa volta, di inviare alla stampante i risultati di PACKING.LST. Per farlo, digitare `type packing.lst>lpt1` al prompt della riga di comando.

   ---

6. Confrontare i risultati di VALIDATE.EXE a quelli di PACKING.LST. Le dimensioni, le date e ore di modifica e i codici di convalida per tutti i file dovrebbero essere esattamente gli stessi. In caso contrario, eliminare immediatamente il file: *evitare assolutamente* di aprire il file o esaminarlo con qualsiasi altro programma di utility; questo potrebbe esporre il sistema al rischio di infezioni da virus.

IMPORTANTE: Il controllo della propria installazione di VirusScan con VALIDATE.EXE non *garantisce* che la copia del programma in uso sia esente da difetti, errori di copia, infezioni da virus o manomissioni. Tuttavia le funzioni di sicurezza presenti nel programma rendono estremamente improbabile che qualcuno abbia manomesso i file quando i codici di convalida sono corretti. Consultare i file LICENZA.TXT o LEGGIMI.1ST inclusi nella copia di VirusScan per apprendere i termini del contratto di licenza relativi all'uso del programma.

Verifica di funzionamento del programma installato

Una volta installato, VirusScan è pronto a scandire il sistema per la ricerca di file infetti. È possibile testare se l'installazione è corretta e verificare che sia possibile eseguire la scansione antivirus in modo appropriato implementando un test sviluppato da EICAR (European Institute of Computer Anti-virus Research), una coalizione di produttori di soluzioni antivirus, come metodo offerto ai clienti per verificare l'installazione del software antivirus.

Per verificare il funzionamento del programma installato, procedere come segue:

1. Aprire un editor di testo per Windows standard, ad esempio il Blocco note e digitare:

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-
TEST-FILE!$H+H*
```

NOTA: L'intera stringa va digitata su una *sola riga* nella finestra dell'editor di testi. Gli utenti che leggono questo manuale dal computer possono copiare la stringa nel Blocco note direttamente dal file di Acrobat.

---

2. Salvare il file con il nome EICAR.COM. La dimensione del file dovrebbe essere pari a 69 o 70 byte.

3. Avviare VirusScan e scandire la directory contenente EICAR.COM. Quando VirusScan esamina questo file, rileva il virus EICAR-STANDARD-AV-TEST-FILE.

IMPORTANTE: Questo file *non è un virus*—: non può diffondersi o infettare altri file e neppure danneggiare in altri modi il sistema. Eliminare il file una volta terminata la verifica dell'installazione, per evitare di allarmare gli atri utenti.

Rimozione delle infezioni dal sistema 3

Quando si sospetta la presenza di un virus,

Per prima cosa evitare di farsi prendere dal panico! Sebbene siano tutt'altro che innocui, *la maggior parte* dei virus che possono infettare un computer non distruggono i dati e neppure causano danni tali da rendere inutilizzabile la macchina. Anche i virus più distruttivi, relativamente rari, di solito producono dei danni in risposta a un evento scatenante. Nella maggior parte dei casi, quando non esistono ancora prove visibili dei danni, si può ancora intervenire ed eliminare l'infezione. In ogni caso la sola presenza nel computer di queste piccole sezioni di codice indesiderato può comunque interferire con le normali attività della macchina: i virus possono occupare risorse di sistema e causare altri effetti sgradevoli. Quindi è necessario affrontare seriamente il problema dei virus e cercare di rimuoverli non appena si incontrano.

Un secondo concetto da tenere ben presente è che uno strano comportamento del computer, un blocco inspiegabile del sistema o altri eventi imprevedibili potrebbero originare da cause diverse da un virus. Quando si verificano problemi di questo genere, effettuare una scansione per la ricerca di virus generalmente non serve a risolvere la situazione. È utile però al fine di escludere una delle potenziali cause.

La migliore iniziativa per la sicurezza del computer è installare VirusScan ed effettuare un'immediata e completa scansione del sistema.

In fase di installazione, VirusScan esamina la memoria del computer e i settori di boot del disco per verificare che non vi siano infezioni che potrebbero danneggiare i file installati. Se in fase di installazione VirusScan non rileva la presenza di alcun virus nel sistema, è possibile continuare tranquillamente l'installazione. Si effettuerà una scansione completa del sistema in seguito, non appena si riavvierà il computer dopo aver terminato l'installazione: in qualche angolo remoto potrebbero essere in agguato virus che non si caricano nella memoria del computer o che si nascondono nei blocchi di boot del disco. Vedere il Capitolo 2, "Installazione di McAfee VirusScan," per informazioni sulla scansione del sistema in fase di installazione. Per informazioni sulle modalità di esecuzione di una scansione completa del sistema, vedere Capitolo 5, "Uso di McAfee VirusScan,".

Se VirusScan rileva la presenza di un virus durante la procedura di installazione, è indispensabile rimuovere il virus dal sistema prima di installare il programma. La procedura necessaria è riportata a pagina 60.

IMPORTANTE: Per la massima sicurezza, la stessa procedura va eseguita se VirusScan rileva un virus nella memoria del computer una volta effettuata l'installazione.

Se VirusScan ha rilevato un'infezione durante l'installazione, procedere esattamente come segue:

1. Uscire immediatamente dal programma di installazione, quindi arrestare il sistema.

   Assicurarsi di spegnere completamente il computer. *Evitare assolutamente* di premere la combinazione di tasti **CTRL+ALT+CANC** o il pulsante Reset della macchina per riavviare il sistema: alcuni virus rimangono intatti durante questo tipo di reboot "a caldo".

2. Se la copia di VirusScan include un disco di emergenza, inserirlo nell'unità floppy.

   NOTA: Se la copia in uso di VirusScan non è dotata del Disco di emergenza McAfee, o comunque il Disco di emergenza non è a portata di mano, è necessario creare un nuovo disco in un computer che *non sia infetto.* Accedere a un computer immune da virus e svolgere la procedura descritta nella sezione "Creazione di un disco di emergenza" a pagina 62.

3. Avviare nuovamente il computer infetto.

   Il disco di emergenza riavvia il computer e lancia immediatamente BOOTSCAN.EXE, un programma speciale di scansione dalla riga di comando. Il programma chiede se il computer è stato spento prima dell'avvio con il disco di emergenza. Se è così, premere il tasto S della tastiera e continuare con il Passaggio 4. In caso contrario, premere il tasto N, quindi arrestare il sistema, spegnere il computer e ripetere l'operazione.

   Una volta avviato, BootScan visualizza un report dell'andamento della scansione e tenta di rimuovere interamente i codici dei virus da tutti i file infetti che rileva. Una volta completata l'analisi, mostra all'utente l'esito finale della scansione: numero di file scanditi, numero di file infetti rilevati, presenza di virus in memoria o nei blocchi di boot del disco e altre informazioni.

4. Quando BootScan termina l'analisi del sistema, è possibile procedere in uno dei modi seguenti:

   - **A questo punto, è possibile continuare il lavoro al proprio computer.** Se BootScan non ha rilevato alcun virus, o ha ripulito tutti i file infetti trovati, rimuovere il disco di emergenza dall'unità floppy, quindi riavviare il computer secondo la normale procedura. Se l'installazione di VirusScan sul computer è stata interrotta quando il programma di installazione ha rilevato l'infezione, ora è possibile completarla.

   - **Si può provare comunque a ripulire o eliminare da sé i file infetti.** Se BootScan rileva un virus che non riesce a rimuovere, identifica i file infetti e informa l'utente che non riesce a disinfettarli o che non dispone di uno strumento di rimozione del virus.

     A questo punto, è possibile

     – **Individuare ed eliminare il file o i file infetti.** Per ripristinare qualsiasi file eliminato, sarà necessario ricorrere alle copie di backup. è importante analizzare anche i file di backup, per verificare che non siano infetti, ed eliminare eventuali infezioni esistenti.

     – **Si può provare inoltre a rimuovere da sé un'infezione.** Network Associates mette a disposizione le informazioni e i suggerimenti per rimuovere i virus dai file infetti nella propria Virus Information Library. Per visualizzare queste informazioni, avviare un browser web e digitare il seguente indirizzo:

       http://www.nai.com/vinfo/<numero documento>.asp

       Nell'indirizzo sopra riportato, <numero documento> rappresenta un documento tecnico della Virus Information Library. Sostituire <numero documento> con uno dei seguenti numeri:

       0013 0319 0322 0323 0327 1145

       ❑ **NOTA:** I numeri dei documenti potrebbero cambiare. Vedere il sommario della Virus Information Library in linea, per avere informazioni aggiornate.

Creazione di un disco di emergenza

Se il Disco di emergenza originale di VirusScan non è disponibile, o perché è stato smarrito, o perché la copia di VirusScan in uso è stata scaricata da uno dei servizi elettronici Network Associates, è necessario creare da sé un disco di emergenza.

AVVERTENZA: Se VirusScan rileva un virus in fase di installazione, è indispensabile installare l'applicazione in un computer *che non sia infetto*, quindi creare un disco di emergenza su quel sistema. A questo punto è possibile avviare il sistema infetto utilizzando il disco di emergenza, rimuovere l'infezione e solo allora installare VirusScan. è necessario rimuovere la copia di VirusScan dal sistema non infetto utilizzato per l'emergenza, se non si dispone di una licenza per l'uso di più copie del programma.

Per creare un disco di emergenza con la procedura guidata di VirusScan, procedere come segue:

1. Inserire nell'unità floppy del computer un dischetto da 1,44MB vuoto e *non formattato.*
2. Fare clic su **Avvio** nella barra delle applicazioni di Windows, puntare su **Programmi**, quindi su **McAfee VirusScan**. Scegliere **Crea disco di emergenza**.

   Viene visualizzato il primo pannello della procedura guidata per la creazione del disco di emergenza (Figura 3-1 a pagina 62).

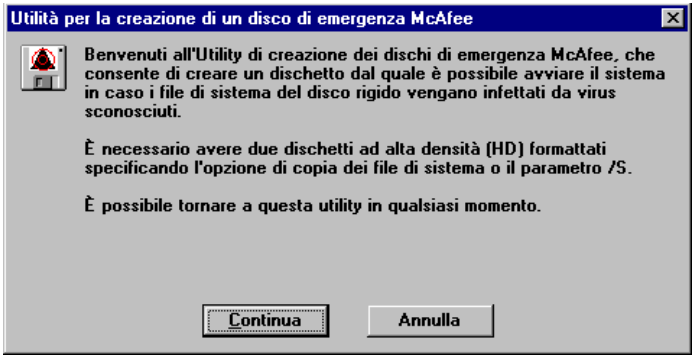

Figura 3-1. Finestra della funzione guidata di creazione del disco di emergenza

3. Fare clic su **Avanti>** per visualizzare il pannello successivo (Figura 3-2 a pagina 63). Sono possibili due scelte:

   - Se si dispone di un floppy *privo di virus formattato* che contiene solo file di sistema DOS o Windows, inserirlo nell'unità floppy. Selezionare quindi la casella di controllo **Non formattare**, quindi fare clic su **Avanti>** per continuare.

     In tal modo, la procedura guidata Disco di emergenza copia solo il componente della riga di comando di VirusScan e i relativi file di supporto sul floppy. Per continuare, passare al Passaggio 5 a pagina 65.

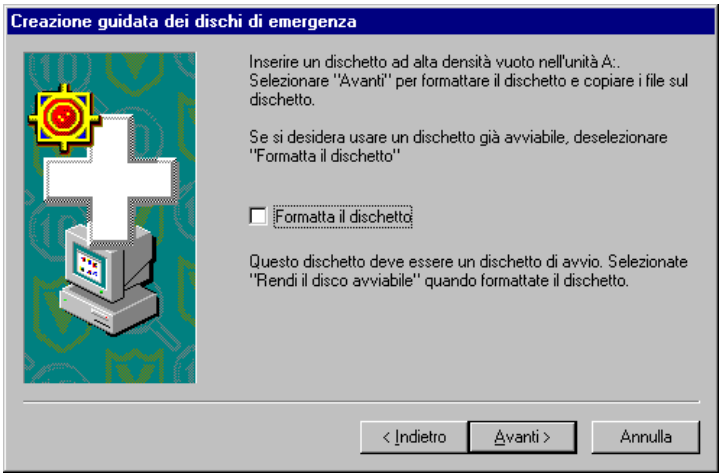

Figura 3-2. Secondo pannello della procedura guidata Disco di emergenza

   - Se *non* si dispone di un floppy privo di virus formattato con file di sistema DOS o Windows, è necessario crearne uno da utilizzare con il disco di emergenza per avviare il computer.

     Procedere come segue:

     a. Inserire un dischetto *non formattato* nell'unità floppy.

     b. Verificare che la casella di controllo **Non formattare** non sia selezionata.

     c. Fare clic su **Avanti>**.

Viene visualizzata la finestra di dialogo di formattazione del disco di Windows (Figura 3-3).

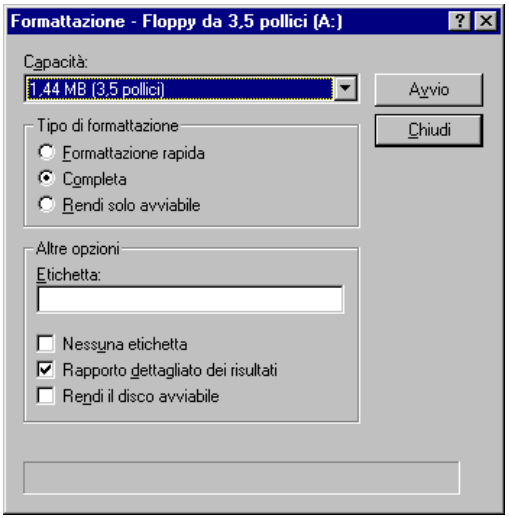

Figura 3-3. Finestra di dialogo di formattazione di Windows

d. Verificare che la casella di controllo **Completa** nella sezione **Tipo di formattazione** e la casella di controllo **Copia file di sistema** nella sezione **Altre opzioni** siano entrambe selezionate. Fare clic sul pulsante **Avvio**.

   Windows formatterà il dischetto e copierà i file di sistema necessari per avviare il computer.

e. Al termine della formattazione del disco, fare clic su **Chiudi**. Fare clic nuovamente su **Chiudi** per tornare alla finestra Disco di emergenza.

4. Fare clic su **Avanti>** per continuare. In questo modo la funzione guidata Disco di emergenza copia sul dischetto di boot creato solo il componente della riga di comando VirusScan e i relativi file di supporto.

5. Quando la funzione guidata ha finito di copiare i file del disco di emergenza, fare clic su **Fine** per tornare al programma di installazione. Incollare un'etichetta di identificazione sul dischetto, attivare la protezione da scrittura e riporre il dischetto in un posto sicuro.

NOTA: Un dischetto è protetto quando sul lato opposto a quello dello sportellino metallico sono aperte entrambe le finestrelle. Se è aperta una sola di esse, aprire anche l'altra spostando il cursore che scorre all'interno. Trascinare il cursore fino a quando si blocca in posizione aperta. In un disco protetto nessun software può essere salvato, quindi i file registrati nel disco non potranno venire infettati da virus.

Creazione di un disco di emergenza senza il programma di utility apposito

Quando non è possibile usare il programma di utility per la creazione del disco di emergenza, o perché VirusScan non è ancora installato o perché in fase di installazione è stato rilevato un virus, è possibile creare un disco di emergenza con la seguente procedura: Procedere come segue:

AVVERTENZA: Se VirusScan ha individuato un virus in fase di installazione nel computer, è indispensabile creare il disco di emergenza in un computer *che non sia infetto.*

---

1. Aprire la finestra del Prompt di MS-DOS o effettuare il reboot del computer in modalità DOS. Per informazioni su questa procedura, consultare la documentazione di Windows.

2. Inserire nell'unità floppy del computer un dischetto da 1,44MB vuoto e *non formattato.*

3. Digitare questo comando al prompt di MS-DOS:

   ```
   format <drive>: /s/u/v
   ```

   Sostituire la lettera per l'unità floppy al posto di `<drive>` nel comando mostrato. Quindi, premere **INVIO.** Quindi premere INVIO. Il dischetto inserito viene formattato e qualsiasi informazione eventualmente contenuta viene sovrascritta. In esso vengono copiati i file di sistema DOS per l'avvio del computer, dopodiché viene richiesto di immettere un'etichetta di volume per il disco.

4. Quando il DOS chiede un'etichetta di volume, immettere un nome di massimo 11 per distinguere questo disco dagli altri.

5. Se VirusScan è installato nel computer e si trova nella directory di programma predefinita, passare alla directory corretta digitando il seguente comando al prompt di MS-DOS:

   ```
   cd\progra~1\networ~1\mcafee~1
   ```

   Se invece VirusScan non è installato, passare alla directory che contiene i file di VirusScan estratti o alla directory VirusScan sull'unità CD-ROM.

6. Digitare questi comandi al prompt di MS-DOS per copiare i file corretti nel disco di emergenza. Sostituire la lettera per l'unità floppy al posto di `<drive>` nei comandi mostrati:

   ```
   copy bootscan.exe <drive>:
   ```

   ```
   copy scan.dat <drive>:
   ```

   ```
   copy names.dat <drive>:
   ```

   ```
   copy clean.dat <drive>:
   ```

   copy license.dat <drive>:

   copy messages.dat <drive>:

   copy edwiz16.exe <drive>:

7. Copiare nel disco di emergenza tutti gli altri programmi di utility DOS necessari per avviare il computer, per effettuare il debug del software di sistema, per gestire l'eventuale memoria estesa o espansa disponibile e per svolgere tutte le altre consuete attività di avvio. Se normalmente si usa un programma di utility per la compressione dei file registrati sul disco, copiare anche i driver necessari per decomprimere gli archivi.

8. Terminata la copia dei file sul disco di emergenza, incollare sul dischetto un'etichetta di identificazione, attivare la protezione da scrittura e riporre il dischetto in un posto sicuro.

❑ **NOTA:** Un dischetto è protetto quando sul lato opposto a quello dello sportellino metallico sono aperte entrambe le finestrelle. Se è aperta una sola di esse, aprire anche l'altra spostando il cursore che scorre all'interno. Trascinare il cursore fino a quando si blocca in posizione aperta. In un disco protetto nessun software può essere salvato, quindi i file registrati nel disco non potranno venire infettati da virus.

Risposta ai virus e ai software dannosi

VirusScan è composto da più programmi, quindi in un determinato momento potrebbero essere attivi più programmi diversi. Per questo la possibile risposta a un'infezione da virus o alla presenza di altri software dannosi dipenderà da quale di questi programmi rileva l'oggetto pericoloso, da come è configurato il programma relativamente alla risposta ai virus e da altri fattori ancora. Le sezioni che seguono presentano una panoramica delle risposte predefinite disponibili in ognuno dei programmi di VirusScan. Per informazioni sulle altre possibili risposte, vedere i capitoli del manuale dedicati ai singoli componenti.

Risposta alla presenza di software dannosi rilevati da VShield

VShield è composto da quattro moduli collegati che forniscono una protezione ininterrotta, realizzata attraverso una continua scansione in background per la ricerca di virus, oggetti Java e ActiveX dannosi e siti Web pericolosi. Un quinto modulo controlla le impostazioni di sicurezza per gli altri quattro. è possibile configurare e attivare separatamente ogni modulo oppure usare i moduli insieme per il massimo livello di protezione. Vedere Capitolo 4, "Uso di VShield," per informazioni sulle opzioni di configurazione di ciascun modulo. Poiché ogni modulo rileva oggetti diversi o scandisce punti diversi di ingresso di virus, ognuno presenta un proprio gruppo di risposte predefinite.

Modulo Scansione sistema

In base all'impostazione predefinita, questo modulo effettua una ricerca dei virus ogniqualvolta si esegue, si copia, si crea o si rinomina qualsiasi file nel sistema oppure quando si leggono dati da un dischetto. Quindi, Scansione sistema può fungere da backup qualora altri moduli VShield non rilevino un virus scaricato ad esempio con un'applicazione FTP client. Nella configurazione iniziale, quando il modulo individua un virus durante una di queste operazioni, impedisce l'apertura, il salvataggio oppure la copia del file infetto e chiede cosa fare del virus (vedere Figura 3-4).

Le opzioni di risposta visualizzate in questa finestra di dialogo derivano dalle scelte predefinite o da quelle effettuate nella Pagina Azione del modulo Scansione sistema. Vedere "Scegliere le opzioni Azione" a pagina 97 per sapere come scegliere quali opzioni debbano essere visualizzate in questa finestra.

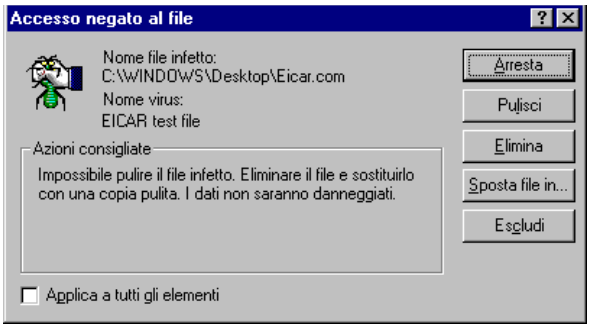

Figura 3-4. Opzioni di risposta iniziali di Scansione sistema

Se è stata selezionata la casella di controllo **Continua accesso** nella Pagina Azione del modulo sarà visualizzato invece un avviso a tutto schermo con le opzioni di risposta (Figura 3-5).

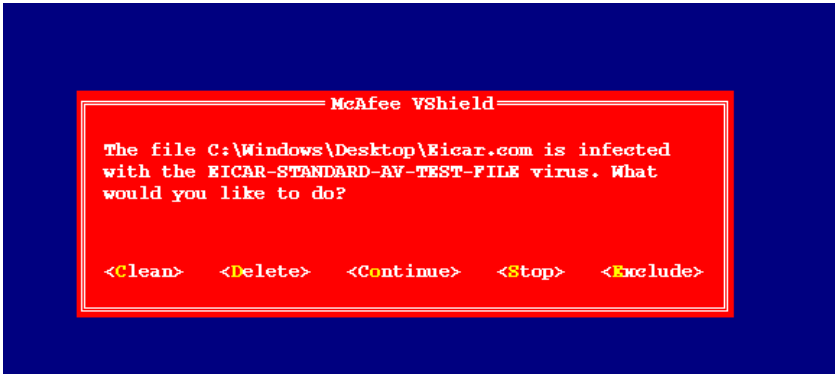

Figura 3-5. Opzioni di risposta disponibili da Scansione sistema

Per selezionare una delle azioni elencate, fare clic su un pulsante della finestra di dialogo oppure digitare la lettera evidenziata in giallo quando viene visualizzato l'avviso a tutto schermo. Se si desidera applicare la stessa risposta a tutti i file infetti rilevati da VShield durante la scansione, selezionare **Applica a tutti gli elementi** nella finestra di dialogo. Le scelte disponibili sono:

- **Pulisci file.** Fare clic su **Pulisci** nella finestra di dialogo oppure digitare C quando viene visualizzato l'avviso a tutto schermo per indicare a VShield di tentare di rimuovere il codice del virus dal file infetto. Se VShield riesce a rimuovere il codice del virus, il file torna allo stato originale.

  Se VShield non riesce a rimuovere il codice del virus, o perché non dispone di uno strumento di rimozione adeguato o perché il virus ha danneggiato il file in modo irreparabile, annota questo risultato nel suo file di log e non esegue altre azioni. Nella maggior parte dei casi questi file andrebbero eliminati e ripristinati dalle copie di backup.

- **Elimina file.** Fare clic su **Elimina** nella finestra di dialogo oppure digitare D quando viene visualizzato l'avviso a tutto schermo per indicare a VShield di eliminare immediatamente il file infetto. In base all'impostazione predefinita, VShield annota il nome del file infetto nel suo file di log, al fine di fornire all'utente un elenco dei file infetti rilevati. è possibile ripristinare i file eliminati dalle copie di backup.

- **Spostare il file in una nuova posizione.** Fare clic su **Sposta il file in** nella finestra di dialogo. Si apre una finestra che può essere utilizzata per individuare la cartella di quarantena oppure un'altra cartella in cui isolare il file infetto. Dopo aver selezionata la cartella, VShield vi sposta immediatamente il file infetto.

- **Continua accesso.** Digitare O quando viene visualizzato l'avviso a tutto schermo per indicare a VShield di continuare l'attività con il file e di non adottare alcuna azione. Normalmente si usa questa opzione per tralasciare l'analisi di file che per certo non contengono virus. Se è stata abilitata l'opzione per la registrazione degli eventi, VShield annoterà ogni infezione rilevata nel suo file di log.

- **Interrompi scansione.** Fare clic su **Interrompi** nella finestra di dialogo oppure digitare S quando viene visualizzato l'avviso a tutto schermo per indicare a VShield di negare qualsiasi accesso al file ma di non adottare alcuna azione. La negazione dell'accesso al file impedisce all'utente di aprire, salvare, copiare o rinominare il file. Per proseguire è necessario fare clic su **OK**. Se è stata abilitata l'opzione per la registrazione degli eventi, VShield annoterà ogni infezione rilevata nel suo file di log.

- **Escludi il file dalla scansione.** Fare clic su **Escludi** nella finestra di dialogo oppure digitare E quando viene visualizzato l'avviso a tutto schermo per indicare a VShield di escludere il file in questione dalle future operazioni di scansione. Normalmente si usa questa opzione per tralasciare l'analisi di file che per certo non contengono virus.

Modulo Scansione posta

Questo modulo effettua una ricerca dei virus nei messaggi di posta elettronica ricevuti dai sistemi di posta aziendali quali cc:Mail e Microsoft Exchange. Nella configurazione iniziale, il modulo chiede all'utente di scegliere una risposta fra tre opzioni disponibili, ogniqualvolta rileva un virus (vedere Figura 3-6). Una quarta opzione fornisce informazioni aggiuntive.

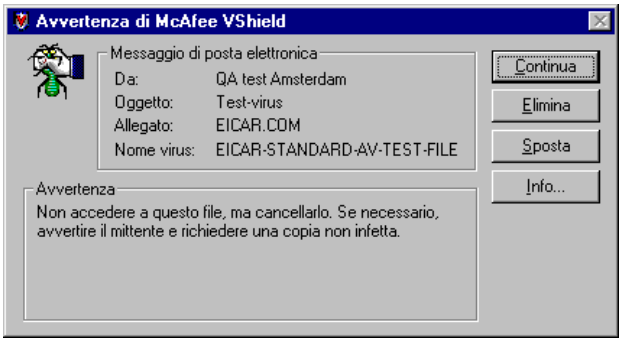

Figura 3-6. Opzioni di risposta disponibili da Scansione posta

Fare clic sul pulsante corrispondente alla risposta desiderata. Le scelte disponibili sono:

- **Continua.** Fare clic su questo pulsante affinché VShield non effettui alcuna azione contro il virus rilevato e riprenda la scansione. VShield continuerà finché non trova un altro virus sul sistema o finché non termina l'operazione di scansione. Normalmente si usa questa opzione per tralasciare l'analisi di file che per certo non contengono virus, o se si prevede di lasciare il computer incustodito mentre si scarica la posta elettronica. VShield annota ogni virus rilevato nel suo file di log.
- **Elimina.** Fare clic su questo pulsante affinché VShield elimini il file allegato infetto dal messaggio di posta elettronica ricevuto. Come impostazione predefinita, VShield annota il nome dell'allegato nel proprio file di log.

- **Sposta.** Fare clic su questo pulsante affinché VShield crei una directory di quarantena dove ha rilevato il virus e quindi sposti in essa i file infetti. Se ad esempio sono in uso Microsoft Exchange, Microsoft Outlook o altri client di posta che supportano lo standard MAPI, la directory di quarantena apparirà come cartella denominata INFECTED nella casella postale dell'utente o sul server di posta. Se invece è in uso un client di posta che supporta lo standard POP-3 o simile, la directory di quarantena apparirà al livello principale del disco rigido non appena si scarica un file infetto.
- **Info.** Fare clic su questo pulsante per collegarsi alla Virus Information Library di Network Associates. Questa scelta non esegue alcuna azione contro il virus rilevato da VShield. Vedere "Visualizzazione di informazioni sui file infetti e sui virus" a pagina 77 per ulteriori dettagli.

Quando l'utente sceglie l'azione desiderata, VShield la esegue e aggiunge una nota nella parte iniziale del messaggio di posta elettronica che conteneva l'allegato infetto. La nota include il nome del file infetto, il nome del virus responsabile dell'infezione e una descrizione dell'azione che VShield ha eseguito in risposta.

Modulo Scansione scaricamento

Questo modulo ricerca i virus nei messaggi di posta elettronica e in altri file ricevuti via Internet attraverso un browser web o altri programmi client di posta elettronica quali Eudora Light, Netscape Mail, Outlook Express e così via. Il modulo *non* rileverà i file scaricati con applicazioni client FTP, applicazioni per terminali o tramite canali simili. Nella configurazione iniziale, il modulo chiede all'utente di scegliere una risposta fra tre opzioni disponibili, ogniqualvolta rileva un virus (vedere Figura 3-7). Una quarta opzione fornisce informazioni aggiuntive.

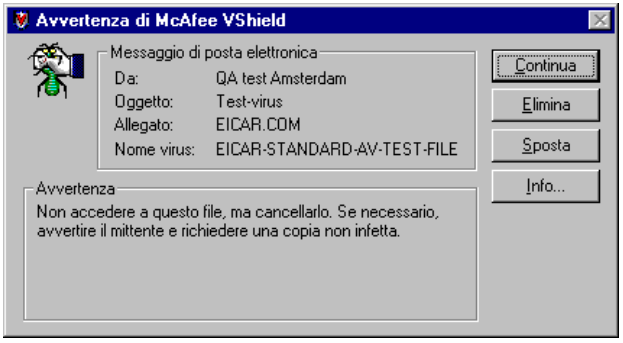

Figura 3-7. Opzioni di risposta disponibili da Scansione scaricamento

Fare clic sul pulsante corrispondente alla risposta desiderata. Le scelte disponibili sono:

- **Continua.** Fare clic su questo pulsante affinché VShield non effettui alcuna azione contro il virus rilevato e riprenda la scansione. VShield continuerà finché non trova un altro virus sul sistema o finché non ha concluso l'operazione di scansione. Normalmente si usa questa opzione per tralasciare l'analisi di file che per certo non contengono virus, o se si prevede di lasciare il computer incustodito mentre si scarica la posta elettronica. VShield annota ogni infezione rilevata nel proprio file di log.
- **Elimina.** Fare clic su questo pulsante affinché VShield elimini il file allegato infetto dal messaggio di posta elettronica ricevuto. Per impostazione predefinita, VShield annota il nome del file infetto nel proprio file di log.
- **Sposta.** Fare clic su questo pulsante affinché VShield crei una directory di quarantena dove ha rilevato il virus e quindi sposti in essa i file infetti. Se invece è in uso un client di posta che supporta lo standard POP-3 o simile, la directory di quarantena apparirà al livello principale del disco rigido non appena si scarica un file infetto.
- **Informazioni.** Fare clic su questa opzione per collegarsi alla Virus Information Library di Network Associates. Questa scelta non esegue alcuna azione contro il virus rilevato da VShield. Vedere "Visualizzazione di informazioni sui file infetti e sui virus" a pagina 77 per ulteriori dettagli.

Quando l'utente sceglie l'azione desiderata, VShield la esegue e aggiunge una nota nella parte iniziale del messaggio di posta elettronica che conteneva l'allegato infetto. La nota include il nome del file infetto, il nome del virus responsabile dell'infezione e una descrizione dell'azione che VShield ha eseguito in risposta.

Modulo Filtro Internet

Questo modulo ricerca classi Java o controlli ActiveX ostili, ogniqualvolta si visita un sito Web o si scaricano file da Internet. Il modulo inoltre può essere usato per impedire al browser in uso di connettersi a siti Internet pericolosi. Nella configurazione iniziale, ogniqualvolta il modulo incontra un oggetto potenzialmente dannoso, chiede all'utente se desidera **Negare** all'oggetto l'accesso al proprio sistema o se desidera **Continuare** e consentire l'accesso all'oggetto. Il modulo offre la stessa scelta quando l'utente tenta di accedere a un sito Web potenzialmente pericoloso (Figura 3-8 a pagina 73).

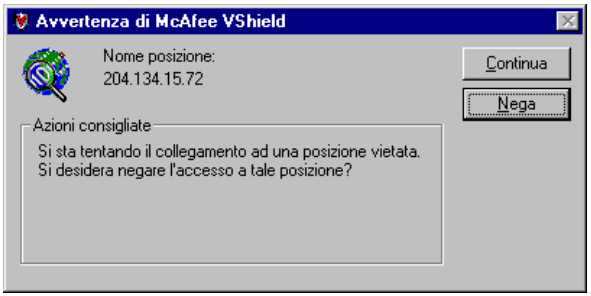

Figura 3-8. Opzioni di risposta disponibili da Filtro Internet

Risposta alla presenza di un virus rilevato da VirusScan

Quando si installa VirusScan e si avvia per la prima volta una scansione, il programma analizza tutti i file presenti nell'unità C: che siano suscettibili di infezioni da virus. Questa funzione fornisce un livello di protezione base, che può essere esteso configurando VirusScan secondo le proprie esigenze specifiche. Nella configurazione iniziale, viene chiesto all'utente di scegliere una risposta quando il programma rileva un virus (Figura 3-9).

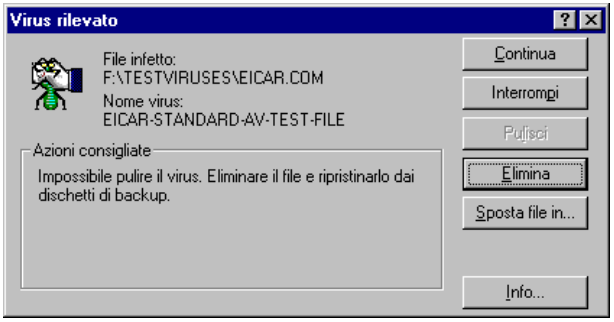

Figura 3-9. Opzioni di risposta disponibili da VirusScan

Per rispondere all'infezione, fare clic su uno dei pulsanti indicati. è possibile scegliere fra le seguenti alternative:

- **Continua.** Fare clic su questo pulsante per proseguire con l'operazione di scansione e fare in modo che VirusScan elenchi ogni file infetto nella parte inferiore della finestra principale (Figura 3-10 a pagina 74), registri ogni rilevamento nel proprio file di log ma non adotti alcuna azione per rispondere al virus. Quando VirusScan termina l'analisi del sistema, è possibile fare clic con il pulsante destro del mouse su ognuno dei file infetti elencati nella finestra principale, quindi selezionare una risposta specifica per il singolo file dal menu di scelta rapida che appare.

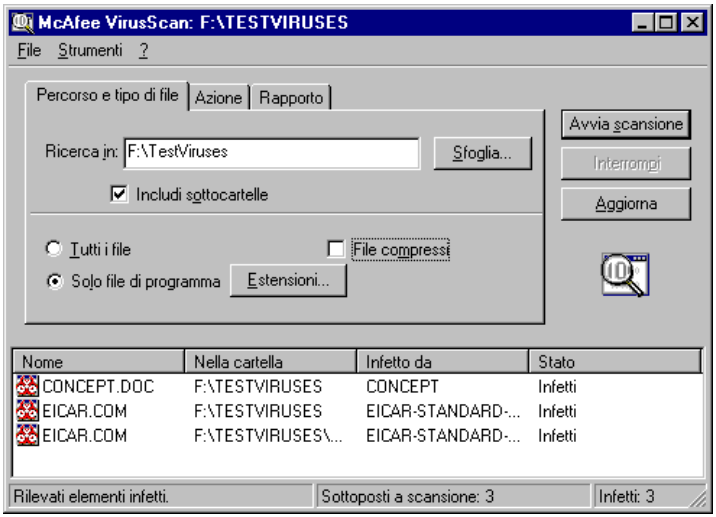

Figura 3-10. Finestra principale di VirusScan

- **Interrompi.** Fare clic su questo pulsante per interrompere immediatamente l'operazione di scansione. Nella parte inferiore della finestra principale vengono elencati i file infetti trovati fino a quel momento (Figura 3-10) e ogni infezione rilevata viene registrata nel file di log, ma il programma non effettua alcuna azione in risposta ai virus. Fare clic con il pulsante destro del mouse su ognuno dei file infetti elencati nella finestra principale, quindi selezionare una risposta specifica per il singolo file dal menu di scelta rapida che appare.

- **Ripulisci.** Fare clic su questo pulsante per fare in modo che VirusScan tenti di rimuovere il codice del virus dal file infetto. Se non riesce a ripulire il file, o perché non dispone di uno strumento di rimozione adeguato o perché il virus ha danneggiato il file in modo irreparabile, annota questo risultato nel suo file di log e suggerisce risposte alternative. Nell'esempio della Figura 3-9, VirusScan non è riuscito a rimuovere Eicar Test Virus, un virus "simulato", scritto appositamente per testare la corretta installazione dei software antivirus. In questo caso non è disponibile l'opzione **Ripulisci** fra le possibili risposte. Nella maggior parte dei casi questi file andrebbero eliminati e ripristinati dalle copie di backup.

- **Elimina.** Fare clic su questo pulsante per eliminare immediatamente il file dal sistema. In base all'impostazione predefinita, VirusScan registra il nome del file infetto nel suo file di log affinché l'utente possa ripristinarlo da una copia di backup.

- **Sposta il file in.** Fare clic su questo pulsante per aprire una finestra di dialogo che può essere utilizzata per selezionare la cartella di quarantena o un'altra cartella adatta. Una volta individuata la cartella corretta, fare clic su **OK** per trasferire il file in quella posizione.
- **Info.** Fare clic su questo pulsante per collegarsi alla Virus Information Library di Network Associates. Questa scelta non esegue alcuna azione contro il virus rilevato da VirusScan. Vedere "Visualizzazione di informazioni sui file infetti e sui virus" a pagina 77 per ulteriori dettagli.

Risposta da fornire quando Scansione posta rileva un virus

Il componente Scansione posta permette di scandire, su iniziativa dell'utente, i messaggi di posta elettronica in entrata pervenuti da Microsoft Exchange o Microsoft Outlook. Può essere avviato da entrambi i client di posta e usato come supplemento alla scansione continua in background della posta elettronica effettuata da VShield. Scansione posta consente inoltre di pulire gli allegati infetti o di interrompere la scansione, possibilità che completa la fuzione di monitoraggio continuo di VShield. Nella configurazione iniziale, Scansione posta chiede all'utente di scegliere una risposta quando rileva un virus (Figura 3-11).

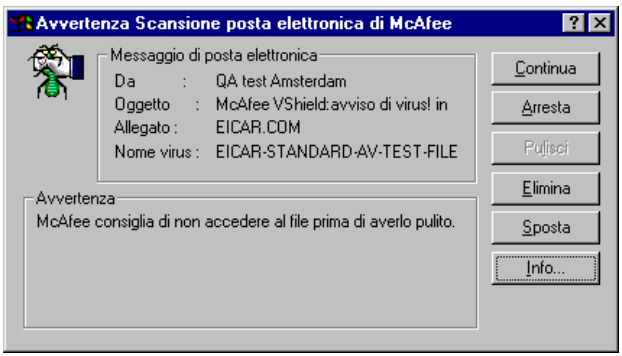

Figura 3-11. Opzioni di risposta disponibili da Scansione posta

Per rispondere all'infezione, fare clic su uno dei pulsanti indicati. È possibile scegliere fra le seguenti alternative:

- **Continua.** Scansione scambio procede all'analisi, elenca nella parte inferiore della finestra principale tutti i file infetti trovati (vedere Figura 3-12) e registra ogni infezione rilevata nel suo file di log, ma non effettua alcuna azione per rispondere ai virus. Scansione posta continua finché non trova un altro virus sul sistema oppure fino al termine dell'operazione di scansione. Quando VirusScan termina l'analisi del sistema, è possibile fare clic con il pulsante destro del mouse su ognuno dei file infetti elencati nella finestra principale, quindi selezionare una risposta specifica per il singolo file dal menu di scelta rapida che appare.
- **Interrompi.** Scansione posta interrompe immediatamente la scansione. Nella parte inferiore della finestra principale vengono elencati i file infetti trovati fino a quel momento (Figura 3-12) e ogni infezione rilevata viene registrata nel file di log, ma il programma non effettua alcuna azione in risposta ai virus. Fare clic con il pulsante destro del mouse su ognuno dei file infetti elencati nella finestra principale, quindi selezionare una risposta specifica per il singolo file dal menu di scelta rapida che appare.

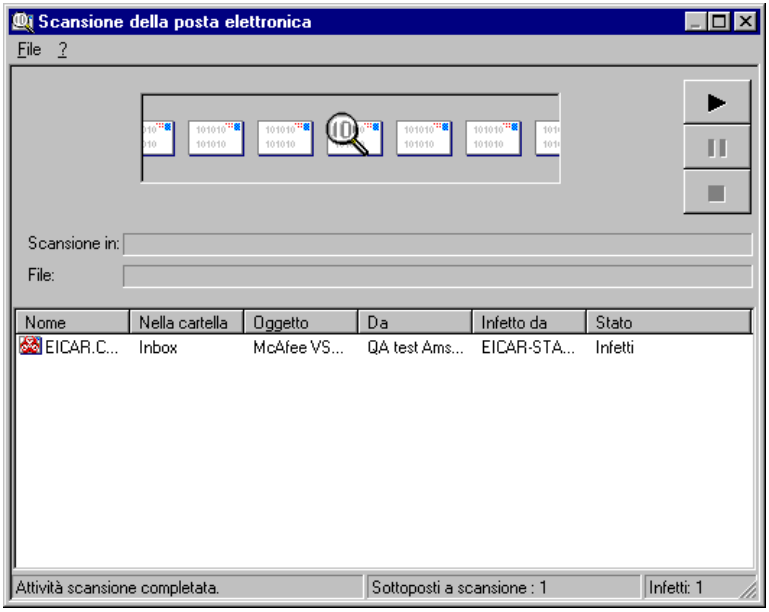

Figura 3-12. Finestra Scansione posta

- **Ripulisci.** Scansione scambio tenta di rimuovere il codice del virus dal file infetto. Se non riesce a ripulire il file, o perché non dispone di uno strumento di rimozione adeguato o perché il virus ha danneggiato il file in modo irreparabile, annota questo risultato nel suo file di log e suggerisce risposte alternative. Nell'esempio della Figura 3-11 non è disponibile l'opzione **Pulisci** fra le possibili risposte. Nella maggior parte dei casi questi file andrebbero eliminati e ripristinati dalle copie di backup.

- **Elimina.** Scansione posta elimina immediatamente il file dal sistema. In base all'impostazione predefinita, Scansione posta registra il nome del file infetto nel suo file di log, affinché l'utente possa ripristinarlo da una copia di backup.
- **Sposta.** Scansione posta apre una finestra di dialogo che può essere usata per individuare la propria cartella di quarantena o altra cartella adeguata. Una volta individuata la cartella corretta, fare clic su **OK** per trasferire il file in quella posizione.
- **Info.** Scansione posta apre una finestra di dialogo che mostra informazioni sul file infetto o sul virus responsabile dell'infezione. Questa scelta consente al programma di non intraprendere alcuna azione contro il virus rilevato. Vedere "Visualizzazione di informazioni sui file infetti e sui virus" per ulteriori dettagli.

Visualizzazione di informazioni sui file infetti e sui virus

Facendo clic su **Info** in una delle finestre di dialogo di risposta, ci si collega alla Virus Information Library in linea di Network Associates, a condizione che sul computer sia disponibile un collegamento Internet e il software del browser web (Figura 3-13).

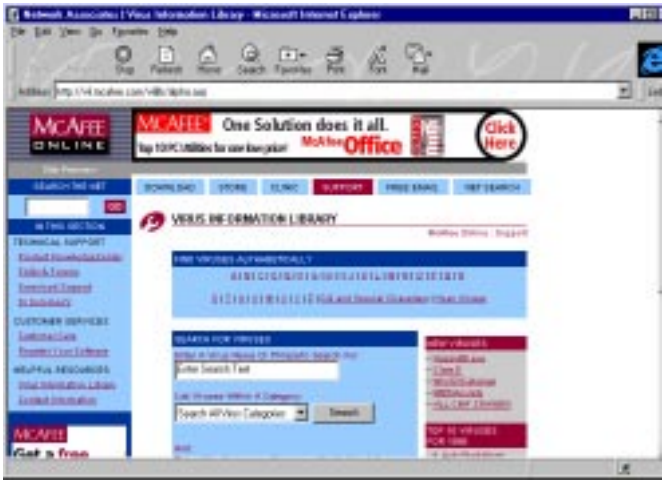

Figura 3-13. Virus Information Library in linea

La Virus Information Library contiene documenti che offrono una panoramica dettagliata di ogni virus che VirusScan è in grado di rilevare ed eliminare. Le informazioni includono le modalità di infezione e di alterazione dei file, l'ordinamento dei carichi utili, le modalità di riconoscimento delle infezioni ed altri dati. La Library fornisce anche consigli sulla prevenzione delle infezioni da virus e sulla rimozione di virus che VirusScan non può rimuovere.

Se si sceglie **File Info** dal menu **File** nella finestra principale di VirusScan (vedere Figura 3-10 a pagina 74) oppure fare clic con il pulsante destro del mouse su un file elencato nella finestra principale di VirusScan oppure nella finestra Scansione posta (vedere Figura 3-12 a pagina 76), quindi **Informazioni sul file** dal menu di scelta rapida che viene visualizzato, VirusScan aprirà la finestra di dialogo Informazioni elemento infetto che assegna un nome al file, elenca il tipo e le dimensioni in byte, attribuisce le date di creazione e modifica e descrive i relativi attributi (vedere Figura 3-14).

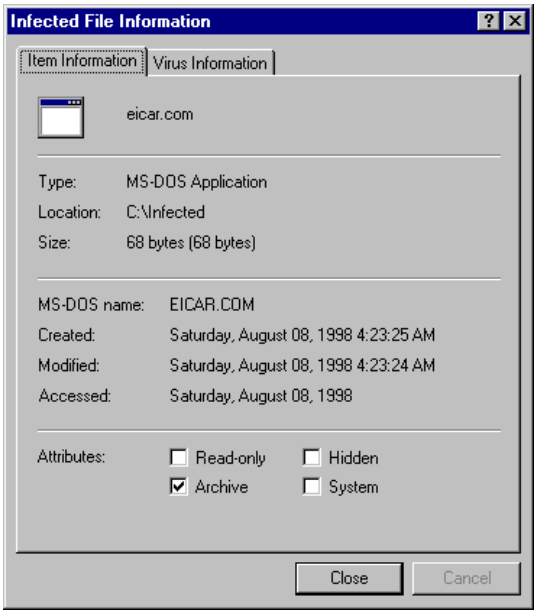

Figura 3-14. La pagina di proprietà Informazioni file infetto

Come capire le false rilevazioni

Una falsa rilevazione si verifica quando VirusScan invia un messaggio di avviso per la presenza di un virus che in realtà non c'è o effettua una registrazione nel suo file di log che identifica un virus che in realtà non esiste. è più probabile che si verifichino false rilevazioni quando sono installati nel computer software antivirus di più produttori, perché alcuni di questi software registrano in memoria, senza protezione, le firme in codice che usano per rilevare i virus.

Il modo migliore di procedere quando compare un messaggio d'avviso o una nuova registrazione nel file di log, è agire come se si trattasse effettivamente di un virus, svolgendo le operazioni appropriate per rimuovere il virus dal sistema. Quando invece si è certi che VirusScan abbia effettuato una falsa rilevazione, ad esempio perché indica come infetto un file che si usa senza problemi da anni, prima di rivolgersi al personale di assistenza tecnica, accertarsi che non sussista una delle seguenti situazioni:

- **sono in uso più programmi antivirus.** In questo caso VirusScan potrebbe aver rilevato la firma in codice non protetta in uso da parte di un altro programma antivirus e averla identificata come virus. Per evitare questo problema, configurare il computer per l'esecuzione di un solo programma antivirus, quindi arrestare il sistema e spegnere il computer. Attendere alcuni secondi prima di riavviare il computer, in modo che il sistema possa cancellare dalla memoria le stringhe delle firme in codice degli altri programmi antivirus.
- **è in uso un chip BIOS dotato di funzioni antivirus.** Alcuni chip BIOS sono dotati di funzioni antivirus che possono causare false rilevazioni quando si esegue VirusScan. Consultare il Manuale dell'utente del computer per informazioni su come funzionano le proprietà antivirus della macchina e come disabilitarle se necessario.
- **è in uso un vecchio PC Hewlett-Packard o Zenith.** Alcuni dei modelli più vecchi di questi produttori modificano i settori di boot sui loro dischi rigidi a ogni avvio. VirusScan potrebbe rilevare queste modifiche come virus, mentre non lo sono. Consultare il Manuale dell'utente del computer per vedere se la macchina usa un codice di boot automodificante. Per risolvere il problema usare la versione per la riga di comando di VirusScan e aggiungere informazioni di convalida agli stessi file di avvio. Questo metodo non registra informazioni relative al settore di boot o al record di boot principale.
- **è in uso un software protetto da copia.** A seconda del tipo di protezione da copia usato, VirusScan potrebbe individuare un virus nel settore di boot o nel record di boot principale, su alcuni dischetti o altri supporti.

Se nessuna di queste condizioni sussiste, contattare il supporto tecnico di Network Associates o inviare un messaggio di posta elettronica all'indirizzo AVresearch@nai.com con una spiegazione chiara e dettagliata del problema.

Uso di VShield 4

Le funzioni di VShield

VShield scandisce il sistema in background, durante il normale lavoro con i file, per proteggere il sistema dai virus che potrebbero provenire dai dischetti, dalla rete a cui il sistema è connesso, dai file allegati in arrivo con i messaggi di posta elettronica e dai virus caricati in memoria. VShield viene avviato quando si accende il computer e rimane in memoria fino all'arresto del sistema. VShield include inoltre la tecnologia per la protezione del sistema dagli applet Java e dai controlli ActiveX ostili, che impedisce al computer di connettersi a siti Internet pericolosi. La protezione di sicurezza tramite password per le proprie opzioni di configurazione impedisce agli altri utenti di effettuare modifiche non autorizzate.

Perché usare VShield

VShield presenta capacità uniche che rendono questo componente una parte integrante di VirusScan, un completo pacchetto di sicurezza antivirus. Fra queste capacità compaiono le seguenti:

- **Accesso, scansione.** Grazie a questa capacità VShield scandisce per la ricerca di virus i file che vengono aperti, copiati, salvati o modificati in altro modo e i file che vengono letti o scritti nei dischetti. Esso quindi può individuare e bloccare i virus non appena compaiono nel sistema. Questa funzione fornisce una misura ulteriore di protezione antivirus fra una procedura di scansione e l'altra.

- **Individuazione e blocco degli oggetti dannosi.** VShield può impedire agli oggetti Java e ActiveX dannosi di accedere al sistema, prima che essi possano diventare una minaccia. VShield svolge questa funzione scandendo le centinaia di oggetti che vengono scaricati quando ci si connette al Web o ad altri siti Internet e i file allegati che vengono ricevuti con la posta elettronica. Il programma confronta questi elementi con un proprio elenco interno aggiornato di oggetti dannosi e blocca quelli che potrebbero causare problemi.

- **Filtro dei siti Internet.** VShield include un elenco di siti Web o Internet pericolosi, siti cioè che rappresentano una minaccia per il sistema in quanto potrebbero contenere software da scaricare dannosi. A questo elenco predefinito è possibile aggiungere qualsiasi altro sito per impedire al browser in uso di accedervi, o aggiungendo l'indirizzo Internet Protocol (IP) del sito o aggiungendo il suo nome di dominio.

- **Funzionamento automatico.** VShield si integra con numerosi browser e applicazioni client di posta elettronica basati sullo standard Microsoft Messaging Application Programming Interface (MAPI). Questa integrazione permette a VShield di accedere ai messaggi di posta elettronica e scandire i file allegati per la ricerca di virus, prima che questi raggiungano il computer.

Browser e client di posta elettronica supportati da VShield

VShield funziona in modo perfettamente integrato con molti dei più diffusi browser Web e delle più diffuse applicazioni client di posta disponibili per la piattaforma Windows. Una volta connesso il computer a Internet, VShield non richiede alcuna configurazione ulteriore per il corretto funzionamento con il browser in uso. È necessario invece configurare VShield perché funzioni correttamente con il software client di posta elettronica in uso. Vedere "Uso della procedura guidata per la configurazione di VShield" a pagina 83 o "Impostazione delle proprietà di VShield" a pagina 90 per informazioni su come effettuare la configurazione richiesta.

I browser Web che sono stati testati e funzionano correttamente con VShield sono i seguenti:

- Netscape Navigator v3.x
- Netscape Navigator v4.0.x (v4.0.6 esclusa)
- Microsoft Internet Explorer v3.x
- Microsoft Internet Explorer v4.x

I client di posta elettronica che sono stati testati e funzionano correttamente con il modulo Scansione scaricamento di VShield sono i seguenti:

- Microsoft Outlook Express
- Qualcomm Eudora v3.x e v4.x
- Netscape Mail (incluso in molte versioni di Netscape Navigator e Netscape Communicator)
- America Online mail v3.0 e v4.0

Per poter lavorare con il modulo Scansione posta di VShield, occorre usare particolari versioni di Lotus cc:Mail oppure il software client di posta elettronica deve supportare lo standard MAPI di Microsoft. I client che sono stati testati e funzionano correttamente con il modulo Scansione posta sono i seguenti:

- Microsoft Exchange v4.0, v5.0 e v5.5
- Microsoft Outlook 97 e Microsoft Outlook 98
- Lotus cc:Mail v6.x e v7.x (che non supporta lo standard MAPI)
- cc:Mail v8.0 e v8.01 (solo versione che supporta lo standard MAPI)

Altri software client che supportano lo standard MAPI potrebbero funzionare in modo corretto con VShield ma Network Associates non garantisce la compatibilità di VShield con i software client che non compaiono nell'elenco riportato sopra.

Uso della procedura guidata per la configurazione di VShield

Dopo avere installato VirusScan e riavviato il computer, VShield viene caricato immediatamente in memoria e inizia a lavorare con un gruppo di opzioni predefinite che attivano una protezione antivirus di base. Se VShield non viene disattivato o non viene disattivato uno dei suoi moduli, o ancora se VShield non viene completamente terminato, non occorre in alcun caso preoccuparsi di avviare VShield o pianificare attività di scansione per esso.

Per ottenere un livello di sicurezza superiore a quello minimo occorre configurare VShield affinché funzioni correttamente con il software client di posta in uso ed esamini accuratamente il traffico Internet del sistema alla ricerca di eventuali virus e software dannosi. La procedura guidata per la configurazione di VShield può essere d'aiuto nella corretta impostazione di queste opzioni. In seguito, quando si sarà acquisita una maggiore familiarità con VShield e una migliore conoscenza delle aree del sistema maggiormente soggette al rischio di ricevere danni da software pericolosi, sarà possibile adattare meglio il programma al proprio ambiente di lavoro.

Per avviare la procedura guidata per la configurazione di VShield, procedere in uno dei modi seguenti:

- Avviare Pianificatore VirusScan, quindi selezionare l'icona di VShield nella barra delle applicazioni. Quindi, fare clic su nella barra delle applicazioni del Pianificatore. Per sapere come avviare e utilizzare il Pianificatore VirusScan, vedere "Avvio dell'Utilità di pianificazione di VirusScan" a pagina 184 oppure.
- Localizzare l'icona di VShield nel system tray di Windows, quindi fare clic su essa con il pulsante destro del mouse. Puntare su **Proprietà** nel menu di scelta rapida che appare, quindi scegliere **Scansione sistema**.

Con entrambi i metodi si apre la finestra di dialogo Proprietà VShield (Figura 4-1).

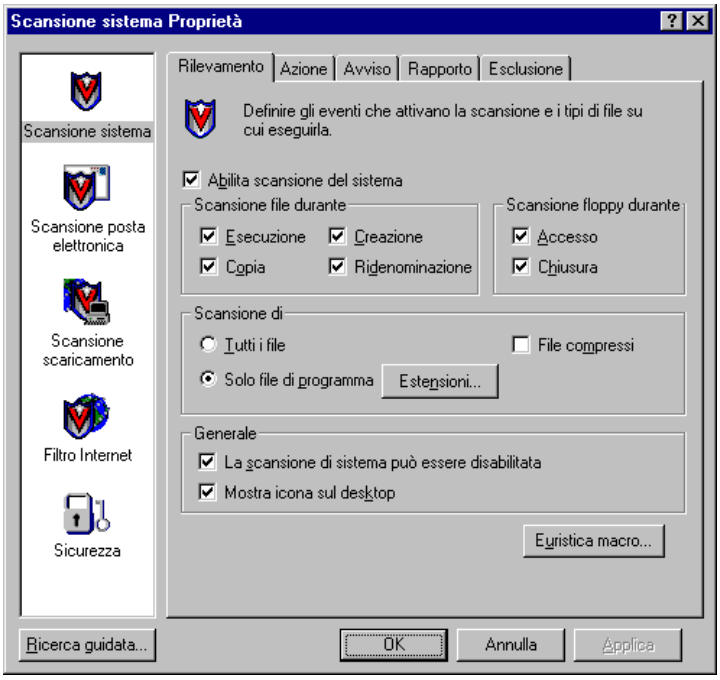

Figura 4-1. La finestra di dialogo Proprietà VShield

Fare clic su **Procedura guidata** nell'angolo inferiore sinistro della finestra di dialogo, per visualizzare il primo pannello della procedura guidata di configurazione (Figura 4-2 a pagina 85).

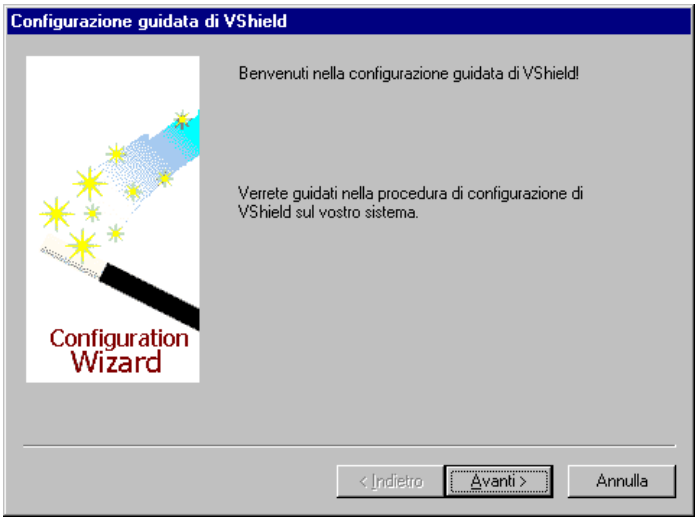

Figura 4-2. Finestra introduttiva della procedura guidata per la configurazione di VShield

Fare clic su **Avanti>** per visualizzare il pannello di configurazione di Scansione sistema (Figura 4-3).

Figura 4-3. Procedura guidata per la configurazione di VShield - Pannello Scansione sistema

In questo pannello è possibile impostare VShield affinché ricerchi i virus nei file soggetti al rischio di infezioni ogni qualvolta vengono aperti, eseguiti, copiati, salvati o modificati in altro modo. Fra i file soggetti al rischio di virus compaiono vari tipi di file eseguibili e file di documenti con macro incorporate, come ad esempio file di Microsoft Office. VShield scandirà inoltre i file registrati nei dischetti ogni qualvolta verranno lette o scritte informazioni sui dischetti stessi e all'arresto del computer.

Se rileva la presenza di un virus, VShield emette un segnale acustico di avviso e chiede all'utente di scegliere una risposta. Il programma inoltre registra le proprie azioni e riepiloga le proprie impostazioni correnti in un file di registro che l'utente può visualizzare in seguito.

Per attivare queste funzioni, selezionare **Sì**, quindi fare clic su **Avanti>**. Diversamente, selezionare **No**, quindi fare clic su **Avanti>** per proseguire.

Compare sullo schermo il pannello Scansione posta della procedura guidata (Figura 4-4).

Figura 4-4. Procedura guidata per la configurazione di VShield - Pannello Scansione posta

Se non si usa la posta elettronica o non si dispone di una connessione a Internet, selezionare la casella di controllo **Non uso la posta elettronica**, quindi fare clic su **Avanti>** per proseguire. Diversamente, selezionare la casella di controllo che corrisponde al tipo di client di posta elettronica in uso. Le scelte disponibili sono:

- **Attiva posta aziendale.** Selezionare questa casella di controllo se si usa un sistema di posta elettronica proprietario al lavoro o in un ambiente di rete. La maggior parte di questi sistemi usano un server di rete centrale per la ricezione e la distribuzione della posta che i singoli utenti inviano dalle applicazioni client. Questi sistemi potrebbero inviare e ricevere posta dall'esterno della rete o da Internet, ma generalmente lo fanno attraverso un'applicazione "gateway" eseguita dal server.

  VShield supporta sistemi di posta elettronica aziendali che rientrano in due categorie generali:

  - **Client di posta che supportano lo standard MAPI.** Selezionare questo pulsante se si usa un client di posta elettronica che aderisce allo standard MAPI. Fra i client di questo tipo compaiono Microsoft Exchange, Microsoft Outlook e la versione 8.0 o superiore di Lotus cc:Mail.

  - **Lotus cc:Mail.** Selezionare questo pulsante se si usa cc:Mail versioni 6.x o 7.x che supportano un protocollo Lotus proprietario per l'invio e la ricezione della posta.

- **Client di posta Internet.** Selezionare questa casella di controllo se si usa un client di posta elettronica che supporta il protocollo Post Office Protocol (POP-3) o Simple Mail Transfer Protocol (SMTP) e invia e riceve posta Internet standard direttamente o attraverso una connessione telefonica. Selezionare questa opzione se si invia e si riceve posta elettronica da casa e si usano Netscape Mail, America Online o client di posta diffusi quali Qualcomm Eudora o Microsoft Outlook.

Dopo avere specificato quale sistema di posta elettronica è in uso, fare clic su **Avanti>** per proseguire.

NOTA: Se si usano entrambi i tipi di sistemi di posta, selezionare entrambe le caselle di controllo. Si noti tuttavia che VShield supporta solo due tipi di sistemi di posta elettronica *aziendale* alla volta. Per avere informazioni sul sistema di posta elettronica in uso nel proprio ufficio, rivolgersi all'amministratore della rete aziendale.

È importante inoltre distinguere fra Microsoft Outlook e Microsoft Outlook Express. Sebbene i due programmi presentino nomi simili, Outlook 97 e Outlook 98 sono sistemi di posta elettronica aziendale che supportano lo standard MAPI mentre Outlook Express invia e riceve la posta elettronica attraverso i protocolli POP-3 e SMTP. Per ulteriori informazioni su questi programmi, consultare la documentazione Microsoft.

Nel successivo pannello della procedura guidata è possibile impostare le opzioni per il modulo Scansione scaricamento di VShield (Figura 4-5).

Figura 4-5. Procedura guidata per la configurazione di VShield - Pannello Scansione scaricamento

Affinché VShield analizzi per la ricerca di virus ogni file scaricato da Internet, selezionare la casella di controllo **Sì, scandisci i miei file scaricati per la ricerca di virus**, quindi fare clic su **Avanti>** per proseguire. VShield analizzerà per la ricerca di virus i file maggiormente soggetti al rischio di infezione e scandirà i file compressi al momento della ricezione.

Diversamente, selezionare la casella di controllo **No, non attivare la scansione scaricamento**, quindi fare clic su **Avanti>** per proseguire.

Nel successivo pannello della procedura guidata è possibile impostare le opzioni per il modulo Filtro Internet di VShield (vedere Figura 4-6 a pagina 89).

Figura 4-6. Procedura guidata per la configurazione di VShield - Pannello Filtro Internet

Selezionare **Sì, attiva protezione per applet ostili divieto di accesso ai siti non sicuri**, quindi fare clic su **Avanti>** affinché VShield blocchi gli applet Java e i controlli ActiveX che possono danneggiare il sistema. Questa opzione inoltre impedirà al browser Web di connettersi a siti Web o Internet potenzialmente pericolosi. VShield gestisce un elenco degli oggetti e dei siti dannosi utilizzata per controllare i siti visitati e gli oggetti incontrati. Se rileva una corrispondenza al proprio elenco interno, può o impedire automaticamente l'accesso al sito o offrire all'utente la scelta di consentire o impedire l'accesso.

Per disattivare questa funzione, selezionare **No, non attivare protezione per applet ostili e divieto di accesso ai siti non sicuri** , quindi fare clic su **Avanti>** per proseguire.

Il pannello finale della procedura guidata riassume le opzioni scelte (Figura 4-7).

Figura 4-7. Procedura guidata per la configurazione di VShield - Pannello di riepilogo

Se l'elenco di riepilogo riflette correttamente le scelte effettuate, fare clic su **Fine** per salvare le modifiche e tornare alla finestra di dialogo Proprietà VShield. Diversamente fare clic su **<Indietro** per cambiare qualsiasi opzione scelta o su **Annulla** per tornare alla finestra di dialogo Proprietà VShield senza salvare alcuna delle modifiche effettuate.

Impostazione delle proprietà di VShield

Perché siano garantite prestazioni ottimali in un determinato computer o ambiente di rete, è necessario indicare a VShield cosa scandire, cosa fare se rileva un virus o altri software dannosi e come comunicare all'utente l'individuazione di un problema . È possibile usare la procedura guidata per la configurazione per attivare la maggior parte delle opzioni di protezione di VShield ma se si desidera un completo controllo sul comportamento del programma e la capacità di adattarlo alle proprie esigenze, occorre scegliere le opzioni desiderate nella finestra di dialogo Proprietà VShield.

La finestra di dialogo Proprietà VShield consiste di una serie di pagine di proprietà che controllano le impostazioni per ogni programma componente. Per scegliere le opzioni desiderate, fare clic sull'icona del programma componente, quindi fare clic sulle singole schede della finestra di dialogo Proprietà VShield.

Per aprire la finestra di dialogo Proprietà VShield, procedere in uno dei seguenti modi:

- Avviare il Pianificatore VirusScan, quindi selezionare l'icona di VShield nella barra delle applicazioni. Quindi, fare clic su nella barra delle applicazioni del Pianificatore. Per sapere come avviare e utilizzare il Pianificatore VirusScan, vedere "Avvio dell'Utilità di pianificazione di VirusScan" a pagina 184 oppure
- Localizzare l'icona di VShield nel system tray di Windows, quindi fare clic su essa con il pulsante destro del mouse. Puntare su **Proprietà** nel menu di scelta rapida che appare, quindi scegliere **Scansione sistema**.

Con entrambi i metodi si apre la finestra di dialogo Proprietà VShield (Figura 4-8).

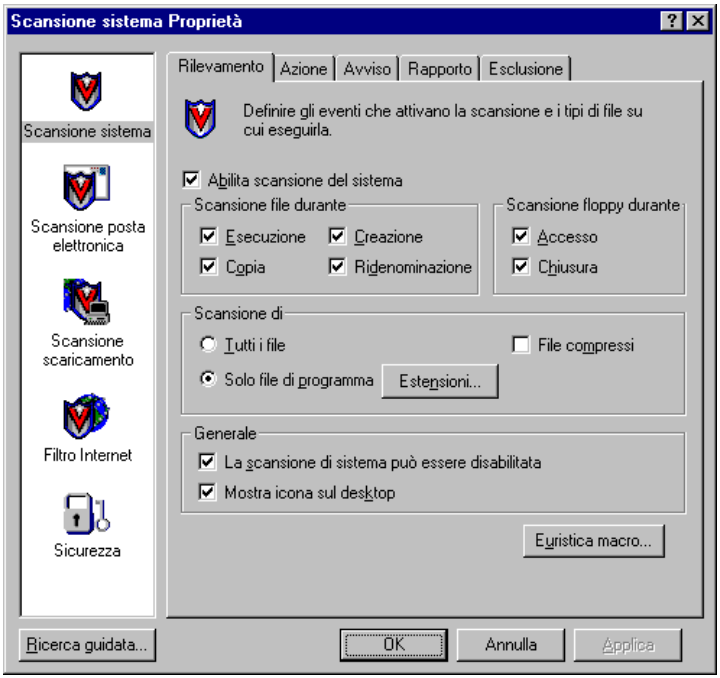

Figura 4-8. La finestra di dialogo Proprietà Scansione sistema - Pagina Rilevamento

Configurazione del modulo Scansione sistema

Il modulo Scansione sistema di VShield può controllare il sistema per la presenza di virus ogni qualvolta i file presenti nel disco vengono aperti, eseguiti, salvati o modificati e ogni qualvolta si leggono o si scrivono informazioni in un dischetto . Per scegliere le opzioni desiderate fare clic sull'icona Scansione sistema, sul lato sinistro della finestra di dialogo Proprietà VShield, per visualizzare le pagine delle proprietà di questo modulo. Le opzioni disponibili sono descritte nelle sezioni che seguono.

Selezione delle opzioni di Rilevamento

VShield inizialmente presume che l'utente desideri effettuare una scansione per la ricerca di virus ogni qualvolta viene usato un qualsiasi file soggetto al rischio di infezioni, sia presente sul disco sia su dischetti (vedere Figura 4-8 a pagina 91). Sebbene queste opzioni predefinite offrano un buon equilibrio fra efficienza della scansione e sicurezza, il proprio ambiente potrebbe richiedere impostazioni diverse.

Per modificare queste impostazioni, verificare che sia selezionata la casella di controllo Attiva Scansione sistema, quindi procedere come segue:

1. Indicare a VShield quando e dove dovrà effettuare la scansione per la ricerca di virus. È possibile scegliere fra le opzioni seguenti

   - **Scandire i file quando si lavora con essi.** Ogni qualvolta i file sul disco vengono aperti, copiati, salvati, rinominati o usati in altro modo, il codice virus può eseguirsi e trasmettere le infezioni ad altri file. Per evitare questo, selezionare una qualsiasi combinazione delle caselle di controllo **Esegui**, **Copia**, **Crea** e **Rinomina**; selezionando tutte le opzioni si ottiene il massimo livello di sicurezza. VShield ritarderà leggermente ogni operazione del sistema in quanto dovrà scandire i file.

   - **Scandire i file sui dischetti.** Virus del settore di boot possono nascondersi nei blocchi di boot di qualsiasi dischetto formattato e quindi venire caricati in memoria quando il computer legge l'unità floppy. Selezionare la casella di controllo **Accesso** affinché VShield esamini i dischetti ogni qualvolta il computer legge informazioni da essi. Selezionare la casella di controllo **Arresto** affinché VShield scandisca qualsiasi dischetto lasciato nell'unità quando si arresta il computer. Questo assicura che nessun virus possa essere caricato quando il computer legge l'unità floppy all'avvio.

2. Specificare i tipi di file che VShield dovrà esaminare. È possibile

   - Scansione di file compressi. Selezionare la casella di dialogo **File compressi** per fare in modo che il modulo Scansione sistema ricerchi i file compressi con LZEXE e PKLite. Anche se fornisce una protezione migliore, la scansione dei file compressi aumenta il tempo necessario per tale operazione.

   - **Scelta dei tipi di file da sottoporre a scansione.** Normalmente i virus non possono infettare i file di dati o i file che contengono un codice non eseguibile. Per questa ragione è possibile eseguire le operazioni di scansione solo sui file maggiormente esposti all'infezione del virus in modo da velocizzare le operazioni di scansione. Per fare questo, selezionare il pulsante **Solo file di programma**. Per vedere o specificare le estensioni dei nomi dei file che VShield esaminerà, fare clic su **Estensioni** per aprire la finestra di dialogo Estensioni file di programmi (Figura 4-9).

Figura 4-9. Finestra di dialogo Estensioni file di programma

Per impostazione predefinita, VShield analizza per la ricerca di virus i file che presentano le estensioni .EXE, .COM, .DO?, .XL?, .RTF, .BIN, .SYS, .MD? e .OBD. I file con estensione .DO?, .XL?, .RTF, .MD? e .OBD sono file di Microsoft Office e tutti possono contenere infezioni di virus macro. Il carattere? è un carattere jolly che consente a VShield di scandire sia i file di documenti sia i modelli.

NOTA: VShield scandisce automaticamente determinati file di programmi inclusi in un elenco predefinito di estensioni. Questo elenco è diverso da quello di VirusScan, in quanto la scansione dei file .DLL e .VXD, file comuni usati costantemente da Windows, rallenterebbe molto il sistema. Affinché VShield scandisca questi tipi di file, aggiungere le loro estensioni nella finestra di dialogo. In alternativa, si consideri la possibilità di eseguire frequenti operazioni di scansione con VirusScan, se è necessario scandire regolarmente file di questo tipo.

– Per aggiungere estensioni all'elenco fare clic su **Aggiungi**, quindi digitare le estensioni dei file che VShield dovrà scandire nella finestra di dialogo che appare.

– Per eliminare un'estensione dall'elenco, selezionarla, quindi fare clic su **Elimina**.

– Fare clic su **Predefinito** per ripristinare l'elenco nella sua forma originaria.

Una volta terminata quest'operazione , fare clic su **OK** per chiudere la finestra di dialogo.

- **Scandire tutti i file.** Affinché VShield esamini tutti i file del sistema, in qualsiasi modo vengano usati e qualunque estensione presentino, selezionare il pulsante **Tutti i file**. Questa opzione rallenta notevolmente il sistema ma assicura la massima protezione da virus.

3. Scegliere i tipi di scansione euristica da attivare. Fare clic su **Euristica delle macro** per aprire la finestra di dialogo Impostazioni di scansione euristica delle macro (Figura 4-10).

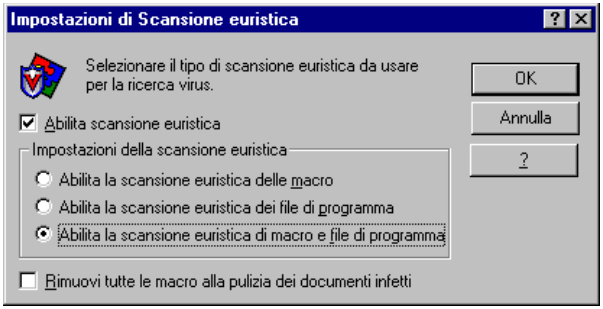

Figura 4-10. Finestra di dialogo Impostazioni di scansione euristica delle macro

La tecnologia della scansione euristica permette a VShield di riconoscere i virus macro sulla base della loro somiglianza a virus simili noti al programma. A tale scopo, il programma cerca determinate caratteristiche "simili a virus" nei file da scandire. La presenza di un numero sufficiente di tali caratteristiche in un file fa sì che VShield lo identifichi come potenzialmente infetto con un virus nuovo o non identificato in precedenza.

Dato che VShield cerca contemporaneamente caratteristiche del file che presentano la possibilità di infezione da virus, raramente fornisce una falsa indicazione di un'infezione. A meno che non si sia certi che il file *non* contiene un virus, trattare le infezioni "probabili" con la stessa attenzione richiesta per le infezioni certe.

Per attivare la scansione euristica, procedere come segue:

a. Selezionare la casella di controllo **Attiva scansione euristica**. Le opzioni rimanenti della finestra di dialogo si attivano.

b. Selezionare il tipo di scansione euristica che VShield deve utilizzare. Le scelte disponibili sono:

   - **Attiva scansione euristica delle macro.** Scegliere questa opzione affinché VShield identifichi tutti i file di Microsoft Word, Microsoft Excel e altri file di Microsoft Office che includono delle macro e quindi confronti il codice della macro con il database delle firme dei virus. Quando VShield identifica un virus il cui nome corrisponde esattamente a un elemento del proprio database interno o individua firme in codice che somigliano a virus esistenti comunica all'utente di avere rilevato un "probabile" virus macro.

   - **Attiva la scansione euristica dei file di programma.** Scegliere questa opzione per fare in modo che VShield individui nuovi virus nei file di programmi esaminandone le caratteristiche e confrontandoli con una lista di caratteristiche di virus note. VShield identificherà i file con un numero sufficiente di queste caratteristiche come virus potenziali.

   - **Attiva la scansione euristica delle macro e dei file di programma.** Scegliere questa opzione per fare in modo che VShield utilizzi entrambi i tipi di scansione euristica. Network Associates consiglia di utilizzare questa opzione per una protezione antivirus totale.

c. Determinare la modalità di trattamento dei file macro infetti. Selezionare **Rimuovi macro durante la pulizia dei documenti infetti** per eliminare tutti i codici infetti dal documento e lasciare solo i dati. Per rimuovere solo il codice virus dalle macro del documento, non selezionare questa casella di controllo.

> **AVVERTENZA:** Utilizzare questa funzione con cautela: la rimozione di tutte le macro da un documento può provocare la perdita o il danneggiamento dei dati e l'impossibilità di utilizzarli.

d. Fare clic su **OK** per salvare le impostazioni e tornare alla finestra di dialogo Proprietà VShield.

4. Scegliere le opzioni di gestione di VShield. Con queste impostazioni è possibile controllare l'interazione fra l'utente e VShield. È possibile

   - **Disattivare il modulo Scansione sistema a piacere.** Selezionare la casella di controllo **Scansione sistema può essere disattivato** per avere la possibilità di disattivare questo modulo. Si noti che Network Associates consiglia di lasciare attivata la funzione Scansione sistema per la massima protezione. Quando questa casella di controllo è deselezionata, vengono rimossi il comando di disattivazione nel menu di scelta rapida di VShield e il pulsante di disattivazione dalla finestra di dialogo Stato di VShield.

     > **SUGGERIMENTO:** Per accertarsi che nessun altro utente del proprio computer possa disattivare VShield e per rinforzare la politica di sicurezza antivirus fra gli utenti di VirusScan della propria rete, disattivare questa casella di controllo, quindi proteggere le impostazioni con una password. Questo impedirà agli altri utenti di disabilitare VShield dal Pianificatore VirusScan o dalla finestra di dialogo Proprietà VShield. Vedere "Configurazione del modulo Sicurezza" a pagina 142 per i dettagli.

   - **Visualizzare l'icona di VShield nel system tray di Windows.** Selezionare la casella di controllo **Mostra icona nella barra delle applicazioni** affinché VShield mostri questa icona nel system tray. Facendo doppio clic sull'icona si apre la finestra di dialogo Stato di VShield. Facendo clic con il pulsante destro del mouse sull'icona si apre un menu di scelta rapida. Vedere "Uso del menu di scelta rapida di VShield" a pagina 146 e "Registrazione delle informazioni di stato di VShield" a pagina 150 per ulteriori dettagli.

5. Fare clic sulla scheda Azione per scegliere ulteriori opzioni di VShield. Per salvare le modifiche senza chiudere la finestra di dialogo Proprietà Scansione sistema, fare clic su **Applica**. Per salvare le modifiche e chiudere la finestra di dialogo, fare clic su **OK**. Fare clic su **Annulla** per chiudere la finestra di dialogo senza salvare le modifiche.

NOTA: Facendo clic su **Annulla** non è possibile ripristinare le modifiche salvate facendo clic su **Applica**.

Scegliere le opzioni Azione

Quando VShield rileva la presenza di un virus, può rispondere o chiedendo all'utente cosa fare con il file infetto o eseguendo automaticamente un'azione che è stata scelta in origine dall'utente stesso. Usare la pagina delle proprietà Azione per specificare quali opzioni di risposta si desidera che VShield fornisca quando rileva un virus o quali azioni si desidera che VShield esegua automaticamente.

Procedere come segue:

1. Fare clic sulla scheda Azione del modulo Scansione sistema per visualizzare la corretta pagina di proprietà (Figura 4-11).

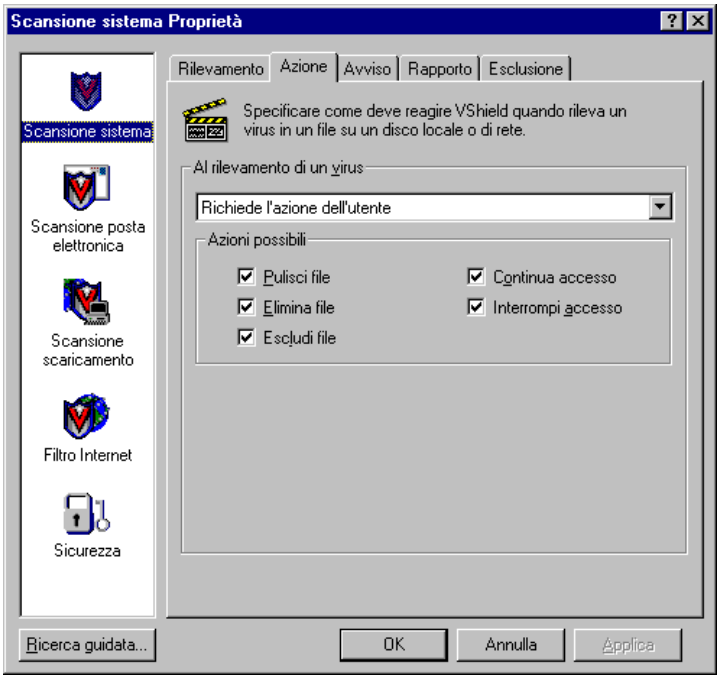

Figura 4-11. La finestra di dialogo Proprietà Scansione sistema - Pagina Azione

2. Selezionare una risposta dall'elenco **Al rilevamento di un virus**. L'area immediatamente al di sotto dell'elenco cambia per visualizzare opzioni aggiuntive per ciascuna selezione.

Le scelte disponibili sono:

- **Richiedi azione.** Scegliere questa risposta per fare in modo che VShield chieda cosa fare qualora venga rilevato un virus—il programma visualizzerà un messaggio di avviso e offrirà una serie di possibili risposte. Selezionare le opzioni da visualizzare nel messaggio di avviso:
  - **Pulisci file.** Con questa opzione VShield tenta di rimuovere il codice virus dal file infetto.
  - **Elimina file.** Con questa opzione VShield elimina immediatamente il file infetto.
  - **Escludi file.** Con questa opzione VShield non scandirà più il file in futuro.
  - **Continua accesso.** Con questa opzione VShield consente all'utente di continuare il lavoro al file e non esegue altre azioni. Se sono attivate le opzioni di reporting del programma, VShield annota l'incidente nel proprio file di registro. Questa opzione fa in modo che VShield visualizzi un avviso a tutto schermo anziché una finestra di dialogo quando viene rilevato un virus. Vedere "Risposta alla presenza di software dannosi rilevati da VShield" a pagina 67 per i dettagli.
  - **Interrompi accesso.** Con questa opzione VShield nega all'utente l'accesso al file ma non esegue altre azioni. La negazione dell'accesso al file impedisce all'utente di aprire, salvare, copiare o rinominare il file. Per proseguire è necessario fare clic su **OK**. Se è stata attivata la funzione di reporting, VShield registra l'incidente.
- **Sposta i file infetti automaticamente.** Con questa opzione VShield sposta i file infetti in una directory di quarantena non appena li rileva. Per impostazione predefinita, VShield sposta questi file in una cartella denominata INFECTED che il programma crea al livello radice dell'unità in cui rileva il virus. Se ad esempio VShield rileva un file infetto nell'unità T:\RISORSE DEL COMPUTER ed era stata specificata INFECTED come directory di quarantena, VShield copia il file in T:\INFECTED.

  È possibile immettere un altro nome e percorso nell'apposita casella di testo o fare clic su **Sfoglia** per localizzare una cartella adatta sul proprio disco rigido.

- **Pulisci automaticamente i file infetti.** Usare questa opzione affinché VShield rimuova il codice virus dal file infetto non appena lo rileva. Se VShield non riesce a rimuovere il virus, lo notifica nell'area messaggio; se sono attivate le funzioni di reporting del programma, VShield annota l'incidente nel proprio file di registro. Per ulteriori dettagli, vedere "Selezione delle opzioni di Rapporto" a pagina 101.
- **Elimina automaticamente i file infetti.** Scegliere questa risposta per fare in modo che VShield elimini immediatamente ogni file rilevato. Verificare di attivare la funzione di reporting per scoprire quali file VShield ha eliminato. Sarà necessario ripristinare i file eliminati da copie di backup.
- **Nega l'accesso ai file infetti e continua.** Scegliere questa risposta per fare in modo che VShield contrassegni il file come "off limits" e continui la normale procedura di scansione. Usare questa opzione solo se si prevede di lasciare il computer incustodito per lunghi periodi. Se inoltre sono attivate le funzioni di reporting di VShield (vedere "Selezione delle opzioni di Rapporto" a pagina 101 per i dettagli), il programma registrerà i nomi di tutti i virus rilevati e i nomi dei file infetti affinché sia possibile eliminarli in seguito.

3. Fare clic sulla scheda Avviso per scegliere ulteriori opzioni di VShield. Per salvare le modifiche senza chiudere la finestra di dialogo Proprietà Scansione sistema, fare clic su **Applica**. Per salvare le modifiche e chiudere la finestra di dialogo, fare clic su **OK**. Fare clic su **Annulla** per chiudere la finestra di dialogo senza salvare le modifiche.

❑ **NOTA:** Facendo clic su **Annulla** non è possibile ripristinare le modifiche salvate facendo clic su **Applica**.

Selezione delle opzioni di Avviso

Una volta configurato il programma con le opzioni di risposta desiderate, è possibile lasciare che VShield ricerchi i virus nel sistema e li rimuova automaticamente, quando li rileva, senza quasi nessun intervento ulteriore. Se invece si desidera che VShield informi immediatamente l'utente quando rileva un virus, affinché questi possa scegliere l'azione più opportuna, è possibile configurare il programma perché invii un messaggio d'avviso all'utente principale o ad altri in vari modi. Utilizzare la pagina di proprietà Avvisi per scegliere i metodi di avviso che si desidera utilizzare.

Procedere come segue:

1. Fare clic sulla scheda Avviso del modulo Scansione sistema per visualizzare la corretta pagina di proprietà (Figura 4-12).

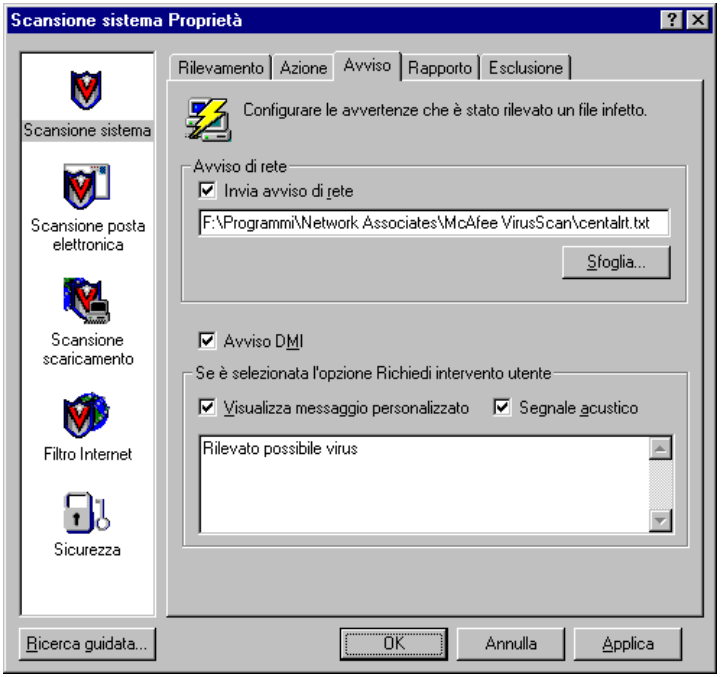

Figura 4-12. La finestra di dialogo Proprietà Scansione sistema - Pagina Avviso

2. Affinché VShield invii un messaggio d'avviso a un server che usa NetShield, una soluzione antivirus prodotta da Network Associates, selezionare la casella di controllo **Invia avviso alla rete**, quindi immettere il percorso della cartella di avviso NetShield della propria rete o fare clic su **Sfoglia** per localizzare la cartella corretta.

❑ **NOTA:** La cartella scelta deve contenere CENTALRT.TXT, il file di avviso centralizzato NetShield. NetShield raccoglie i messaggi di avviso provenienti da VShield e da altri software Network Associates e quindi li passa agli amministratori della rete perché prendano i necessari provvedimenti. Per ulteriori informazioni sull'Avviso centralizzato, vedere il *Manuale dell'utente* di NetShield.

---

3. Affinché VShield invii i messaggi di avviso per i virus attraverso la DMI Component Interface alle applicazioni della scrivania e alle applicazioni di gestione della rete che si eseguono sulla rete, selezionare la casella di controllo **Avviso DMI**.

   ❑ **NOTA:** DMI (Desktop Management Interface) è uno standard per informazioni sulle richieste di gestione delle comunicazioni e le informazioni di avviso tra i componenti hardware e software dei computer o collegati ad essi e le applicazioni utilizzate per la loro gestione. Per ulteriori informazioni sull'uso di questo metodo di avviso, rivolgersi all'amministratore della rete.

4. Se era stata scelta l'opzione **Richiedi azione dell'utente** come risposta nella pagina Azione (vedere "Scegliere le opzioni Azione" a pagina 97 per i dettagli), è possibile inoltre fare in modo che VShield emetta un segnale acustico di avviso e mostri un messaggio personalizzato quando rileva un virus. Per effettuare quest'operazione, selezionare la casella di controllo **Visualizza messaggio personalizzato**, quindi digitare il messaggio che si desidera visualizzare nella relativa casella di controllo—è possibile digitare fino a 225 caratteri. Selezionare poi la casella di controllo **Avviso sonoro**.

5. Fare clic sulla scheda Report per scegliere ulteriori opzioni di VShield. Per salvare le modifiche senza chiudere la finestra di dialogo Proprietà Scansione sistema, fare clic su **Applica**. Per salvare le modifiche e chiudere la finestra di dialogo, fare clic su **OK**. Fare clic su **Annulla** per chiudere la finestra di dialogo senza salvare le modifiche.

   ❑ **NOTA:** Facendo clic su **Annulla** non è possibile ripristinare le modifiche salvate facendo clic su **Applica**.

Selezione delle opzioni di Rapporto

Il modulo Scansione sistema di VShield elenca le proprie impostazioni correnti e riepiloga tutte le azioni eseguite durante le operazioni di scansione in un file di registro denominato VSHLOG.TXT. È possibile fare in modo che VShield scriva il proprio registro su questo file oppure è possibile usare qualsiasi editor di testo per creare un file che possa essere utilizzato dal programma a questo scopo. Il file di registro può essere aperto e stampato in seguito con qualsiasi editor di testo e usato quindi come documento di riferimento.

Il file VSHLOG.TXT può servire all'utente come un importante strumento di gestione in cui vedere le registrazioni delle attività legate ai virus e le impostazioni utilizzate per rilevare e rispondere alle infezioni individuate da VShield. È possibile anche utilizzare i rapporti degli incidenti registrati nel file per determinare quali file è necessario sostituire dalle copie di backup, esaminarlo in quarantena, o eliminarlo dal computer. Usare la pagina delle proprietà Report per determinare quali informazioni VShield dovrà includere nel proprio file di registro.

Per impostare VShield affinché annoti in un file di registro le azioni eseguite, procedere come segue:

1. Fare clic sulla scheda Report del modulo Scansione sistema per visualizzare la corretta pagina di proprietà (Figura 4-13).

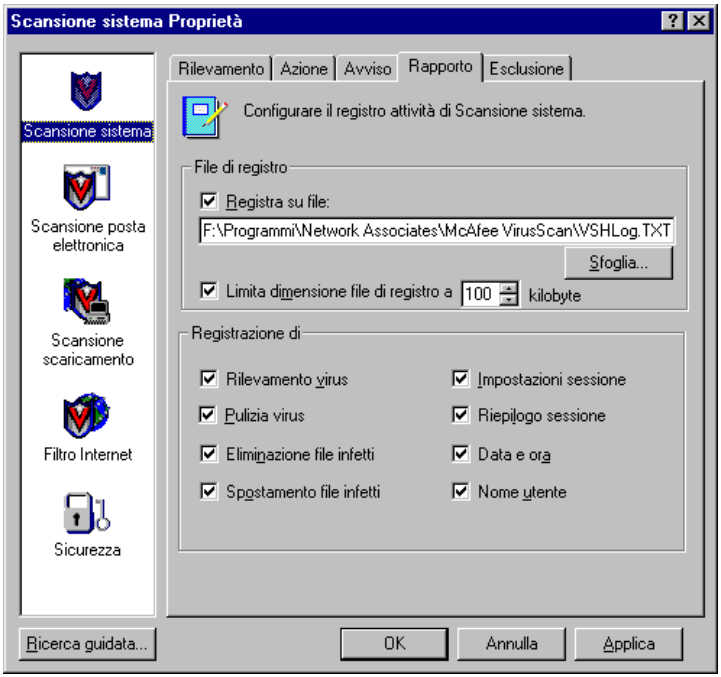

Figura 4-13. La finestra di dialogo Proprietà Scansione sistema - Pagina Report

2. Selezionare la casella di controllo **Registra su file**.

   Per impostazione predefinita, VShield scrive le informazioni di registro nel file WEBFLTR.TXT contenuto nella directory del programma VirusScan. È possibile immettere un altro nome e percorso nell'apposita casella di testo o fare clic su **Sfoglia** per localizzare un file adatto in qualsiasi altra posizione del proprio disco o della propria rete.

3. Per ridurre al minimo le dimensioni del file di registro, selezionare la casella di controllo **Limita dimensioni del file di registro a**, quindi immettere un valore per le dimensioni in kilobyte del file nella relativa casella di testo.

   Immettere un valore compreso tra 10KB e 999KB. Per impostazione predefinita, VShield limita la dimensione del file a 100KB. Se i dati del file di registro eccedono la dimensione di file specificata, VShield cancella il registro esistente e riprende dal punto di interruzione.

4. Selezionare le caselle di controllo corrispondenti alle informazioni che VShield dovrà annotare nel proprio file di registro. È possibile scegliere di registrare queste informazioni:

   - **Rilevamento virus.** Selezionare questa casella di controllo affinché VShield annoti il numero dei file infetti rilevati durante la corrente sessione di scansione.
   - **Pulizia virus.** Selezionare questa casella di controllo affinché VShield annoti il numero dei file infetti da cui è riuscito a rimuovere il virus.
   - **Eliminazione file infetto.** Selezionare questa casella di controllo affinché VShield annoti il numero dei file infetti che ha eliminato dal sistema.
   - **Spostamento file infetti.** Selezionare questa casella di controllo affinché VShield annoti il numero dei file infetti spostati nella directory di quarantena.
   - **Impostazioni sessione.** Selezionare questa casella di controllo affinché VShield elenchi le opzioni scelte nella finestra di dialogo Proprietà Scansione sistema per ogni sessione di scansione.
   - **Riepilogo sessione.** Selezionare questa casella di controllo affinché VShield crei un riepilogo delle azioni eseguite durante ogni sessione di scansione. Le informazioni di riepilogo includono il numero dei file scanditi da VShield, il numero e il tipo dei virus rilevati, il numero dei file spostati o eliminati e altri dati.
   - **Data e ora.** Selezionare questa casella di controllo affinché VShield accodi la data e l'ora a ogni immissione di registro effettuata.
   - **Nome utente.** Selezionare questa casella di controllo affinché VShield accodi il nome utente immesso nel computer a ogni immissione di registro effettuata.

5. Fare clic sulla scheda Esclusione per scegliere ulteriori opzioni di VShield. Per salvare le modifiche senza chiudere la finestra di dialogo Proprietà Scansione sistema, fare clic su **Applica**. Per salvare le modifiche e chiudere la finestra di dialogo, fare clic su **OK**. Fare clic su **Annulla** per chiudere la finestra di dialogo senza salvare le modifiche.

❑ **NOTA:** Facendo clic su **Annulla** non è possibile ripristinare le modifiche salvate facendo clic su **Applica**.

Scelta opzioni Esclusione

Molti dei file memorizzati nel computer non sono vulnerabili a infezioni da virus. L'analisi di questi file da parte di VShield può richiedere molto tempo e produrre risultati di scarsa utilità. È possibile rendere più rapide le operazioni di scansione richiedendo a VShield di analizzare solo i tipi di file maggiormente soggetti al rischio di infezioni (vedere "Selezione delle opzioni di Rilevamento" a pagina 92 per i dettagli) oppure è possibile indurre VShield a ignorare interi file o intere cartelle la cui immunità da virus è certa.

Una volta utilizzato VirusScan per scandire il sistema in modo completo, è possibile indurre VShield a ignorare i file e le cartelle che non cambiano o che normalmente non sono vulnerabili da infezioni da virus. Per fare in modo che VShield escluda dalla scansione determinati file o cartelle, procedere come segue:

1. Fare clic sulla scheda Esclusione del modulo Scansione sistema per visualizzare la corretta pagina di proprietà (Figura 4-14).

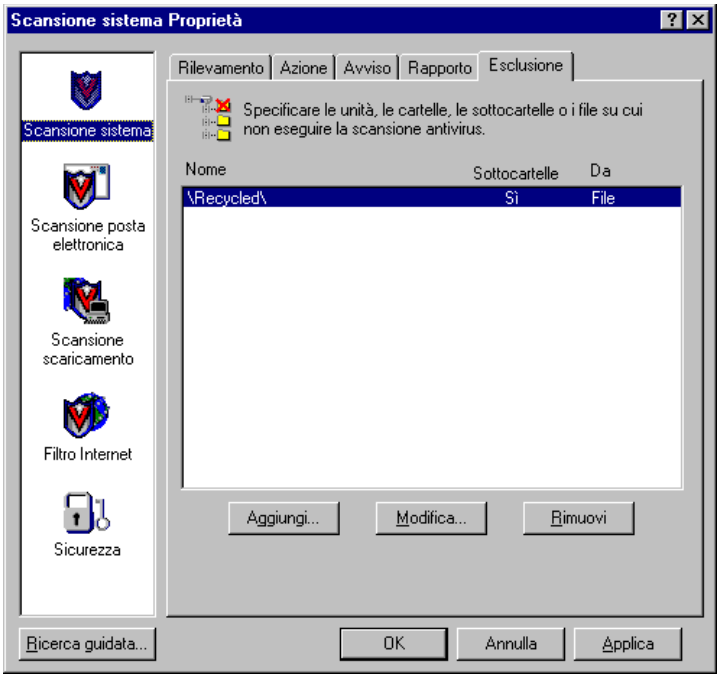

Figura 4-14. La finestra di dialogo Proprietà Scansione sistema - Pagina Esclusione

La pagina Esclusione elenca inizialmente solo il contenuto del cestino. VShield esclude il Cestino dalle operazioni di scansione in quanto Windows non esegue i file che si trovano in esso.

2. Specificare gli elementi che si desidera escludere. È possibile

   - **Aggiungere alla lista di esclusione file, cartelle o volumi.** Fare clic su **Aggiungi** per aprire la finestra di dialogo Aggiungi elemento da escludere (Figura 4-15).

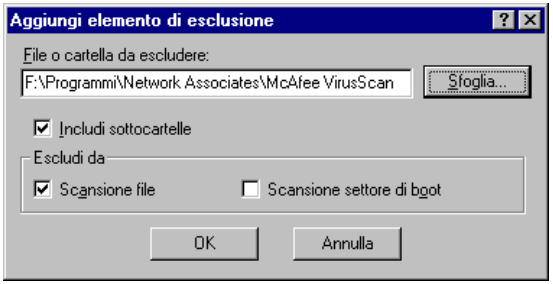

Figura 4-15. Finestra di dialogo Aggiungi elemento da escludere

   a. Digitare il volume, il percorso del file o il percorso della cartella che si desidera escludere dalla scansione o fare clic su **Sfoglia** per localizzare il file o la cartella sul proprio computer.

      NOTA: Se era stata scelta l'opzione di spostare automaticamente i file infetti in una cartella di quarantena, VShield non scandirà quella cartella.

   b. Selezionare la casella di controllo **Includi sottocartelle** per escludere dalla scansione tutte le sottocartelle interne alla cartella specificata.

   c. Selezionare la casella di controllo **Scansione file** affinché VShield, in fase di scansione, ometta di ricercare nei file o nelle cartelle escluse eventuali virus dei file.

   d. Selezionare la casella di controllo **Scansione settore di boot** affinché VShield, in fase di scansione, ometta di ricercare nei file o nelle cartelle escluse eventuali virus del settore di boot. Utilizzare questa opzione per escludere dalle operazioni di scansione i file di sistema, come ad esempio COMMAND.COM.

      AVVERTENZA: Network Associates consiglia di *non* escludere i file di sistema dalla scansione per la ricerca di virus.

e. Per salvare le modifiche apportate e chiudere la finestra di dialogo, fare clic su **OK**.

f. Ripetere i passi da a. a d. fino a quando non sono stati elencati tutti i file e le cartelle che non si desidera sottoporre a scansione.

- **Modificare l'elenco di esclusione.** Per cambiare le impostazioni di un elemento escluso, selezionarlo nell'elenco Esclusioni, quindi fare clic su **Modifica** per aprire la finestra di dialogo Modifica elemento escluso. Effettuare le modifiche desiderate, quindi fare clic su **OK** per chiudere la finestra di dialogo.
- **Rimuovere un elemento dall'elenco.** Per eliminare un elemento escluso, selezionarlo nell'elenco, quindi fare clic su **Rimuovi**. VShield scandirà questo file o cartella nelle successive operazioni di scansione.

3. Fare clic su un'altra scheda per cambiare qualsiasi impostazione di Scansione sistema o fare clic su una delle icone lungo il lato della finestra di dialogo Proprietà Scansione sistema al fine di scegliere opzioni per un altro modulo.

   Per salvare le modifiche eseguite nel modulo Scansione sistema senza chiudere la sua finestra di dialogo, fare clic su **Applica**. Per salvare le modifiche e chiudere la finestra di dialogo, fare clic su **OK**. Fare clic su **Annulla** per chiudere la finestra di dialogo senza salvare le modifiche.

NOTA: Facendo clic su **Annulla** non è possibile ripristinare le modifiche salvate facendo clic su **Applica**.

Configurazione del modulo Scansione posta

Il modulo Scansione posta di VShield ricerca i virus nei file allegati ai messaggi di posta elettronica ricevuti tramite il sistema di posta aziendale, come ad esempio Microsoft Exchange, Microsoft Outlook, oppure Lotus cc:Mail, o ancora tramite programmi di posta client POP-3 o SMTP Eudora, Netscape Mail o Microsoft Outlook Express. VShield si concentra sui file allegati inclusi nei messaggi in quanto i messaggi stessi, tranne qualche rara eccezione, non sono soggetti ai virus. Dato che scandisce la posta elettronica non appena arriva sul server di posta o sul desktop, VShield può intercettare i virus prima che possano diffondersi.

Per scegliere le opzioni desiderate fare clic sull'icona Scansione posta, sul lato sinistro della finestra di dialogo Proprietà VShield al fine di visualizzare le pagine delle proprietà di questo modulo. Le opzioni disponibili sono descritte nelle sezioni che seguono.

Selezione delle opzioni di Rilevamento

VShield non attiva il modulo Scansione posta per impostazione predefinita, in quanto è necessario specificare quale sistema di posta elettronica è in uso attraverso la procedura guidata di configurazione del programma.

Per attivare e configurare la scansione della posta elettronica, procedere come segue:

1. Selezionare la casella di controllo **Attiva scansione degli allegati di posta**.

   Vengono attivate le altre opzioni presenti nella pagina delle proprietà (Figura 4-16).

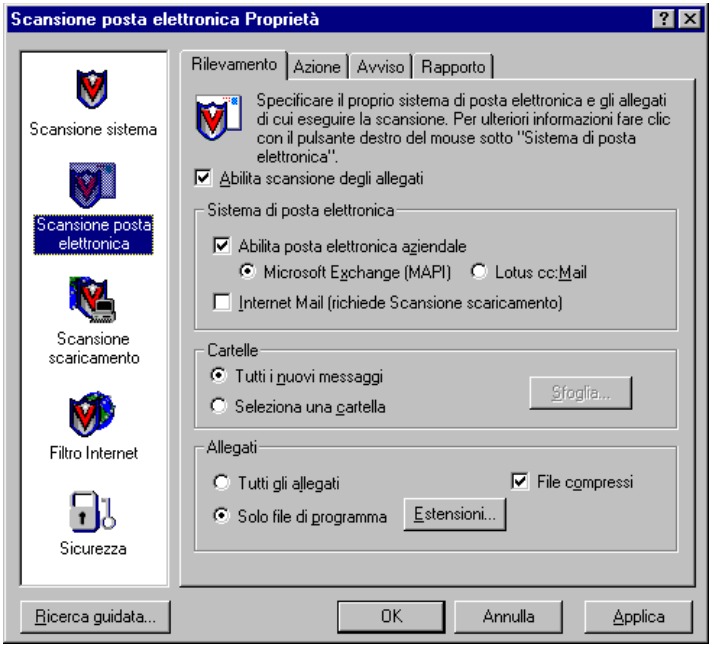

Figura 4-16. La finestra di dialogo Proprietà Scansione posta - Pagina Rilevamento

2. Selezionare il tipo di sistema di posta elettronica in uso. Le opzioni disponibili sono:

   - **Attiva posta aziendale.** Selezionare questa casella di controllo affinché VShield scandisca la posta ricevuta attraverso il sistema di posta utilizzato dalla rete aziendale. Questi sistemi generalmente usano un protocollo di posta proprietario e dispongono di un server di posta centrale a cui viene inviata tutta la posta che in seguito viene distribuita. Questi sistemi spesso inviano e ricevono posta Internet ma generalmente lo fanno attraverso un'applicazione gateway. Il modulo Scansione posta supporta due tipi di sistemi di posta aziendali:

     – **Microsoft Exchange (MAPI).** Selezionare questo pulsante se si usa un sistema di posta elettronica che invia e riceve la posta attraverso Messaging Application Programming Interface di Microsoft, un protocollo di posta per Windows. Ne sono esempi Microsoft Exchange, Microsoft Outlook 97, Microsoft Outlook 98, Lotus cc:Mail 8.0 e Lotus cc:Mail 8.01.

     – **Lotus cc:Mail.** Selezionare questo pulsante se si usa cc:Mail 6.x or 7.x. Questi sistemi usano un protocollo Lotus proprietario per l'invio e la ricezione della posta. È possibile inoltre installare cc:Mail versione 8.0 o superiore in modo tale che usi lo stesso protocollo delle versioni precedenti di cc:Mail. Per avere informazioni sul sistema di posta elettronica in uso nel proprio ufficio, rivolgersi all'amministratore della rete aziendale.

     NOTA: Per vedere l'opzione **Lotus cc:Mail**, è necessario utilizzare l'opzione di installazione Personalizzata di VirusScan per installare lo scanner cc:Mail di VirusScan. Per ulteriori dettagli, vedere Capitolo 2, pagina 42. È possibile selezionare un solo sistema di posta elettronica *aziendale* alla volta, ma è possibile fare in modo che VShield scandisca sia il sistema di posta aziendale che il sistema di posta Internet se sono entrambi in uso.

   - **Posta Internet (richiede scansione allo scaricamento).** Selezionare questa casella di controllo affinché VShield scandisca la posta Internet che viene inviata e ricevuta attraverso il protocollo Post Office Protocol (POP-3) o Simple Mail Transfer Protocol (SMTP). Scegliere questa opzione se si lavora a casa o attraverso una connessione telefonica a un provider Internet gestita da un software quale Qualcomm Eudora Pro, Microsoft Outlook Express o Netscape Mail.

> **IMPORTANTE:** Poiché la posta Internet viene ricevuta dalla stessa "linea" da cui si scaricano gli altri file di siti Web e di altre fonti, VShield usa le opzioni di rilevamento, azione, avviso e reporting impostate nel modulo Scansione scaricamento per determinare come rispondere alla posta Internet in arrivo. Per scandire la posta Internet quindi occorre attivare anche il modulo Scansione scaricamento e usare le sue pagine di proprietà per scegliere le impostazioni desiderate.

3. Indicare a VShield quale fonti di posta deve controllare.

   - Se si sceglie **Microsoft Mail (MAPI)** come sistema di posta aziendale, le opzioni disponibili sono:

     – **Tutta la nuova posta.** Selezionare questo pulsante per fare in modo che VShield cerchi i virus nei file allegati a ciascun messaggio di posta che arriva nella casella MAPI o tramite altri servizi MAPI. Scegliere questa opzione se si riceve posta da più fonti—ad esempio, tramite il sistema di posta aziendale e un client a POP-3 o SMTP—oppure se il sistema di posta ha più di una casella postale.

     > **IMPORTANTE:** Dato che questa opzione indica a VShield di scandire gli allegati di file solo nei nuovi messaggi di posta, non sarà rilevato alcun virus nei messaggi già memorizzati sul computer o sul server di posta. Per garantire una protezione totale, eseguire una scansione completa della posta con il componente Scansione posta di VirusScan. Per ulteriori dettagli, vedere Capitolo 7, "Utilizzo di strumenti specifici per la scansione,".

     – **Selezionare Cartella.** Selezionare questo pulsante per designare una cartella specifica per la scansione da parte di VShield. Scegliere questa opzione se il sistema di posta elettronica utilizzato invia i messaggi in una posizione specifica del server di posta o del proprio computer. Quindi fare clic su **Sfoglia** per aprire una finestra di dialogo in cui individuare la cartella che VShield deve scandire.

Se è già stato eseguito il collegamento al sistema di posta elettronica, la finestra di dialogo mostrerà le caselle postali disponibili e altre cartelle del sistema. Se non è stato eseguito il collegamento, VShield tenterà di utilizzare il profilo MAPI predefinito per farlo. Scegliere la cartella che VShield deve scandire, quindi fare clic su **OK** per chiudere la finestra di dialogo.

- Se si sceglie **Lotus cc:Mail** come sistema di posta elettronica aziendale, è necessario indicare a VShield la frequenza di scansione di Posta in arrivo di Lotus cc:Mail (Figura 4-17).

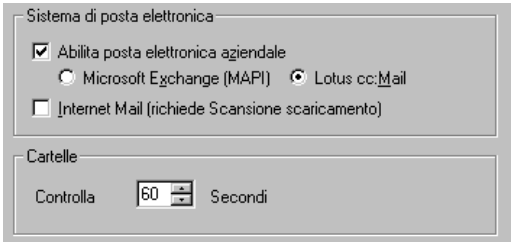

Figura 4-17. Pagina Rilevamento con l'opzione cc:Mail selezionata

Nell'area **Cartelle**, immettere il numero di secondi che VShield dovrà attendere prima di avviare la ricerca dei virus. Per impostazione predefinita, il programma effettua un controllo ogni minuto. Accertarsi di impostare un intervallo più breve di quello specificato per la ricezione della posta, affinché VShield possa rilevare qualsiasi virus prima che raggiunga il computer.

4. Specificare il tipo di allegati di posta elettronica che VShield dovrà esaminare. È possibile

   - **Scansione di file compressi.** Selezionare la casella di controllo **File compressi** per fare in modo che Scansione posta ricerchi i virus nei file compressi dei seguenti formati: .??_, .CAB, LZEXE, LZH, PKLite, .TD0 e .ZIP. Sebbene garantisca il massimo livello di protezione, la scansione dei file compressi può rallentare le attività di scansione, in particolare quando vengono analizzati grossi volumi di posta.

   - **Scelta dei tipi di file da sottoporre a scansione.** Normalmente i virus non possono infettare i file di dati o i file che contengono un codice non eseguibile. Quindi, è possibile restringere la portata delle operazioni di scansione ai file più suscettibili alle infezioni dei virus. Ciò consente di ridurre i tempi delle operazioni di scansione in caso di grandi volumi di posta.

Per fare questo, selezionare il pulsante **Solo file di programma**. Per vedere o specificare le estensioni dei nomi dei file che VShield esaminerà, fare clic su **Estensioni** per aprire la finestra di dialogo Estensioni file di programmi (Figura 4-18).

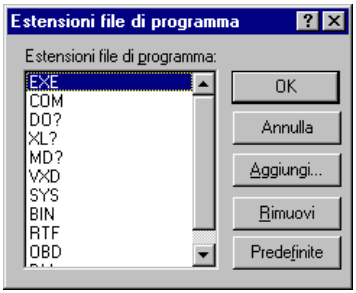

Figura 4-18. Finestra di dialogo Estensioni file di programma

Per impostazione predefinita, VShield analizza per la ricerca di virus i file che presentano le estensioni .EXE, .COM, .DO?, .XL?, .RTF, .BIN, .SYS, .MD? e .OBD. I file con estensione .DO?, .XL?, .RTF, .MD? e .OBD sono file di Microsoft Office e tutti possono contenere infezioni di virus macro. Il carattere? è un carattere jolly che consente a VShield di scandire sia i file di documenti sia i modelli.

- Per aggiungere estensioni all'elenco fare clic su **Aggiungi**, quindi digitare le estensioni dei file che VShield dovrà scandire nella finestra di dialogo che appare.
- Per eliminare un'estensione dall'elenco, selezionarla, quindi fare clic su **Elimina**.
- Fare clic su **Predefinito** per ripristinare l'elenco nella sua forma originaria.

Una volta terminata quest'operazione , fare clic su **OK** per chiudere la finestra di dialogo.

- **Scandire tutti gli allegati.** Affinché VShield esamini tutti gli allegati che arrivano con i messaggi si posta elettronica, qualunque sia la loro estensione, selezionare il pulsante **Tutti gli allegati**. Questa scelta potrebbe rallentare l'elaborazione della posta elettronica se si ricevono grossi volumi di posta ma garantisce la massima protezione antivirus.

5. Fare clic sulla scheda Azione per scegliere ulteriori opzioni di VShield. Per salvare le modifiche senza chiudere la finestra di dialogo Proprietà Scansione posta, fare clic su **Applica**. Per salvare le modifiche e chiudere la finestra di dialogo, fare clic su **OK**. Fare clic su **Annulla** per chiudere la finestra di dialogo senza salvare le modifiche.

❑ **NOTA:** Facendo clic su **Annulla** non è possibile ripristinare le modifiche salvate facendo clic su **Applica**.

Scegliere le opzioni Azione

Quando VShield rileva un virus in un allegato di posta, può rispondere o chiedendo all'utente cosa fare con il file infetto o eseguendo automaticamente un'azione che l'utente ha scelto in origine. Usare la pagina delle proprietà Azione per specificare quali opzioni di risposta si desidera che VShield fornisca quando rileva un virus o quali azioni si desidera che VShield esegua automaticamente.

Procedere come segue:

1. Fare clic sulla scheda Report del modulo Scansione posta per visualizzare la corretta pagina di proprietà (Figura 4-19).

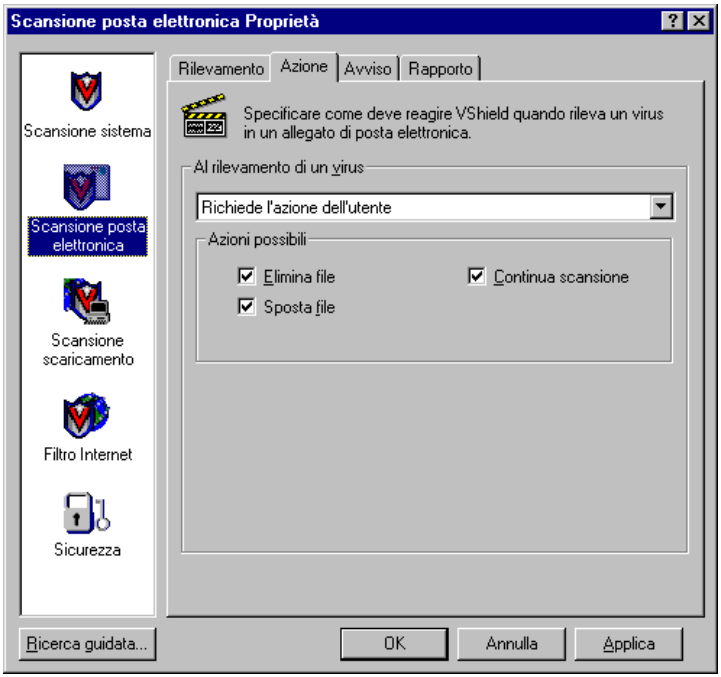

Figura 4-19. finestra di dialogo Proprietà Scansione posta - Pagina Azione

2. Selezionare una risposta dall'elenco **Al rilevamento di un virus**. L'area immediatamente al di sotto dell'elenco cambia per visualizzare opzioni aggiuntive per ciascuna selezione. Le scelte disponibili sono:

   - **Richiedi azione.** Usare questa opzione se si desidera che VShield chieda all'utente cosa fare quando rileva un virus: verrà visualizzato un messaggio d'avviso e verranno proposte una serie di risposte possibili. Selezionare le opzioni che si desidera vedere nel messaggio di avviso:

     – **Elimina file.** Con questa opzione VShield elimina immediatamente i file allegati infetti. VShield conserva il messaggio di posta elettronica a cui il file era allegato.

     – **Sposta file.** Con questa opzione VShield sposta il file infetto in una directory di quarantena selezionata precedentemente.

     – **Continua scansione.** Con questa opzione VShield continua la scansione senza effettuare altre azioni. Se sono attivate le opzioni di reporting del programma, VShield annota l'incidente nel proprio file di registro.

- **Sposta file infetti in una cartella.** Con questa opzione VShield sposta i file infetti in una directory di quarantena non appena li rileva. Per impostazione predefinita, VShield sposta questi file in una cartella denominata INFECTED.

  Se si usa un sistema di posta aziendale, VShield crea la cartella INFECTED sul server di posta della rete. Non è possibile specificare un'altra cartella o cambiare il nome della cartella. A seconda dell'accesso disponibile al proprio server di posta, attraverso il proprio client di posta potrebbe essere possibile vedere o eliminare i file in quella cartella.

  Se si utilizza un client di posta Internet, VShield creerà la cartella denominata INFECTED a livello radice dell'unità su cui si scarica la posta. Ad esempio, se la casella della posta in entrata del client è sull'unità D: e VShield trova un allegato infetto nella posta elettronica, creerà la directory D:\INFECTED e vi copierà il file.

  È possibile cambiare il nome e la posizione della cartella in cui VShield deposita i file Internet infetti, ma per farlo è necessario passare al modulo Scansione scaricamento e fare clic sulla scheda Azione da esso. Vedere "Scegliere le opzioni Azione" a pagina 125 per i dettagli.

- **Elimina file infetti.** Scegliere questa opzione per fare in modo che VShield elimini immediatamente ogni file infetto rilevato. Accertarsi di attivare le funzioni di reporting di VShield, in modo da avere una registrazione di quali file VShield ha eliminato. Sarà necessario ripristinare i file eliminati da copie di backup. Per ulteriori dettagli, vedere "Selezione delle opzioni di Rapporto" a pagina 119.

- **Scansione continua.** Scegliere questa risposta per fare in modo che VShield continui la scansione senza adottare alcuna azione contro i virus rilevati. Se inoltre sono attivate le funzioni di reporting di VShield (vedere "Selezione delle opzioni di Rapporto" a pagina 119 per i dettagli), il programma registrerà i nomi di tutti i virus rilevati e i nomi dei file infetti affinché sia possibile eliminarli in seguito.

3. Fare clic sulla scheda Avviso per scegliere ulteriori opzioni di VShield. Per salvare le modifiche senza chiudere la finestra di dialogo Proprietà Scansione posta, fare clic su **Applica**. Per salvare le modifiche e chiudere la finestra di dialogo, fare clic su **OK**. Fare clic su **Annulla** per chiudere la finestra di dialogo senza salvare le modifiche.

NOTA: Facendo clic su **Annulla** non è possibile ripristinare le modifiche salvate facendo clic su **Applica**.

Selezione delle opzioni di Avviso

Una volta configurato il programma con le opzioni di risposta desiderate, è possibile lasciare che VShield ricerchi i virus nella posta in arrivo e li rimuova automaticamente, quando li rileva, senza quasi nessun intervento ulteriore. Se invece si desidera che VShield informi immediatamente l'utente quando rileva un virus, affinché questi possa scegliere l'azione più opportuna, è possibile configurare il programma perché invii un messaggio d'avviso all'utente principale o ad altri in vari modi. Utilizzare la pagina di proprietà Avvisi per scegliere i metodi di avviso che si desidera utilizzare.

Procedere come segue:

1. Fare clic sulla scheda Report del modulo Scansione posta per visualizzare la corretta pagina di proprietà (Figura 4-20).

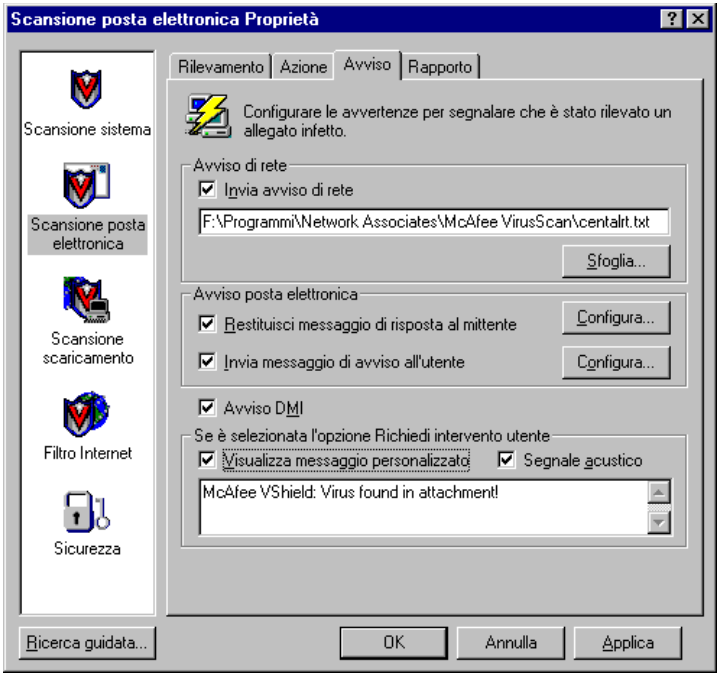

Figura 4-20. finestra di dialogo Proprietà Scansione posta - Pagina Avviso

2. Affinché VShield invii un messaggio d'avviso a un server che usa NetShield, una soluzione antivirus prodotta da Network Associates, selezionare la casella di controllo **Invia avviso alla rete**, quindi immettere il percorso della cartella di avviso NetShield della propria rete o fare clic su **Sfoglia** per localizzare la cartella corretta.

NOTA: La cartella scelta deve contenere CENTALRT.TXT, il file di avviso centralizzato NetShield. NetShield raccoglie i messaggi di avviso provenienti da VShield e da altri software Network Associates e quindi li passa agli amministratori della rete perché prendano i necessari provvedimenti. Per ulteriori informazioni sull'Avviso centralizzato, vedere il *Manuale dell'utente* di NetShield.

3. Selezionare la casella di controllo **Invia posta al mittente** per inviare un messaggio di avviso al mittente dell'allegato di posta infetto. È possibile poi comporre una risposta standard da inviare. Procedere come segue:

   a. Per aprire un messaggio di posta standard, fare clic su **Configura**.

   b. Specificare l'oggetto quindi aggiungere qualsiasi commento desiderato nel corpo del messaggio, sotto una notifica di infezione standard che VShield fornisce automaticamente. È possibile aggiungere fino a 1024 caratteri di testo.

   c. Per inviare una copia del messaggio ad un altro utente, digitare l'indirizzo di posta elettronica nella casella di testo **cc:** oppure fare clic su **cc:** per selezionare un destinatario nella directory dell'utente del sistema di posta o nella rubrica.

      NOTA: Per trovare un indirizzo nella directory dell'utente del sistema di posta, è necessario memorizzare informazioni sugli indirizzi in una directory, in un database o in una rubrica dell'utente conforme allo standard MAPI o in una directory equivalente di Lotus cc:Mail. Se non è ancora stato eseguito il collegamento al sistema di posta, VShield tenta di utilizzare il profilo MAPI predefinito per collegarsi ai sistemi conformi a tale standard oppure chiede di fornire un nome utente, una password e un percorso per la casella di posta di Lotus cc:Mail. Digitare le informazioni richieste e premere **OK** per continuare.

   d. Fare clic su **OK** per salvare il messaggio.

Ogni qualvolta rileva un virus, VShield invia una copia di questo messaggio a ogni persona da cui l'utente riceve posta contenente allegati infetti. Nell'indirizzo del destinatario vengono inserite le informazioni rilevate nell'intestazione originale del messaggio e nell'area al di sotto della riga dell'oggetto viene identificato il virus e il file infetto. Se sono attivate le funzioni di reporting del programma, VShield registra inoltre tutti gli invii dei messaggi d'avviso.

4. Per inviare messaggi di posta per avvisare della presenza di allegati infetti, selezionare la casella di controllo **Invia avviso all'utente**. È possibile quindi scrivere una risposta standard da inviare a uno o più destinatari, ad esempio un amministratore di rete, ogni qualvolta VShield rileva un allegato di posta elettronica infetto. Procedere come segue:

   a. Per aprire un messaggio di posta standard, fare clic su **Configura**.

   b. Digitare un indirizzo di posta elettronica nella casella di testo **A:** oppure fare clic su **A:** per selezionare un destinatario nella directory dell'utente del sistema di posta o nella rubrica. Ripetere l'operazione nella casella di testo **cc:** per inviare una copia del messaggio ad altri utenti.

   ❑ **NOTA:** Per trovare un indirizzo nella directory dell'utente del sistema di posta, è necessario memorizzare informazioni sugli indirizzi in una directory, in un database o in una rubrica dell'utente conforme allo standard MAPI o in una directory equivalente di Lotus cc:Mail. Se non è ancora stato eseguito il collegamento al sistema di posta, VShield tenta di utilizzare il profilo MAPI predefinito per collegarsi ai sistemi conformi a tale standard oppure chiede di fornire un nome utente, una password e un percorso per la casella di posta di Lotus cc:Mail. Digitare le informazioni richieste da VShield e premere **OK** per continuare.

   ---

   c. Compilare la riga dell'oggetto, quindi aggiungere i commenti desiderati nel corpo del messaggio al di sotto dell'avviso di infezione. È possibile aggiungere fino a 1024 caratteri di testo.

   d. Fare clic su **OK** per salvare il messaggio.

   Ogni qualvolta rileva un virus, VShield invia una copia di questo messaggio a ognuno degli indirizzi immessi al Passaggio b. Nell'area immediatamente al di sotto della riga dell'oggetto vengono aggiunte le informazioni per l'identificazione del virus e del file infetto. Se sono attivate le funzioni di reporting del programma, VShield registra inoltre tutti gli invii dei messaggi d'avviso.

5. Affinché VShield invii i messaggi di avviso per i virus attraverso la DMI Component Interface alle applicazioni della scrivania e alle applicazioni di gestione della rete che si eseguono sulla rete, selezionare la casella di controllo **Avviso DMI**.

> **NOTA:** DMI (Desktop Management Interface) è uno standard per informazioni sulle richieste di gestione delle comunicazioni e le informazioni di avviso tra i componenti hardware e software dei computer o collegati ad essi e le applicazioni utilizzate per la loro gestione. Per ulteriori informazioni sull'uso di questo metodo di avviso, rivolgersi all'amministratore della rete.

6. Se era stata scelta l'opzione **Richiedi azione dell'utente** come risposta nella pagina Azione (vedere "Scegliere le opzioni Azione" a pagina 113 per i dettagli), è possibile inoltre fare in modo che VShield emetta un segnale acustico di avviso e mostri un messaggio personalizzato quando rileva un virus. Per effettuare quest'operazione, selezionare la casella di controllo **Visualizza messaggio personalizzato**, quindi digitare il messaggio che si desidera visualizzare nella relativa casella di controllo—è possibile digitare fino a 225 caratteri. Selezionare poi la casella di controllo **Avviso sonoro**.
7. Fare clic sulla scheda Report per scegliere ulteriori opzioni di VShield. Per salvare le modifiche senza chiudere la finestra di dialogo Proprietà Scansione posta, fare clic su **Applica**. Per salvare le modifiche e chiudere la finestra di dialogo, fare clic su **OK**. Fare clic su **Annulla** per chiudere la finestra di dialogo senza salvare le modifiche.

> **NOTA:** Facendo clic su **Annulla** non è possibile ripristinare le modifiche salvate facendo clic su **Applica**.

Selezione delle opzioni di Rapporto

Il modulo Scansione posta di VShield elenca le proprie impostazioni correnti e riepiloga tutte le azioni effettuate durante le operazioni di scansione in un file di registro denominato WEBEMAIL.TXT. È possibile fare in modo che VShield scriva il proprio registro in questo file o usare qualsiasi editor di testo per creare un file che possa essere utilizzato dal programma a questo scopo. Il file di registro può essere aperto e stampato in seguito con qualsiasi editor di testo e usato quindi come documento di riferimento.

Il file WEBEMAIL.TXT può servire all'utente come un importante strumento di gestione in cui vedere le registrazioni delle attività legate ai virus e le impostazioni utilizzate per rilevare e rispondere alle infezioni individuate da VShield. È possibile anche utilizzare i rapporti degli incidenti registrati nel file per determinare quali file è necessario sostituire dalle copie di backup, esaminarlo in quarantena, o eliminarlo dal computer. Usare la pagina delle proprietà Report per determinare quali informazioni VShield dovrà includere nel proprio file di registro.

Per impostare VShield affinché annoti in un file di registro le azioni eseguite, procedere come segue:

1. Fare clic sulla scheda Avviso del modulo Scansione posta per visualizzare la corretta pagina di proprietà (vedere Figura 4-21).

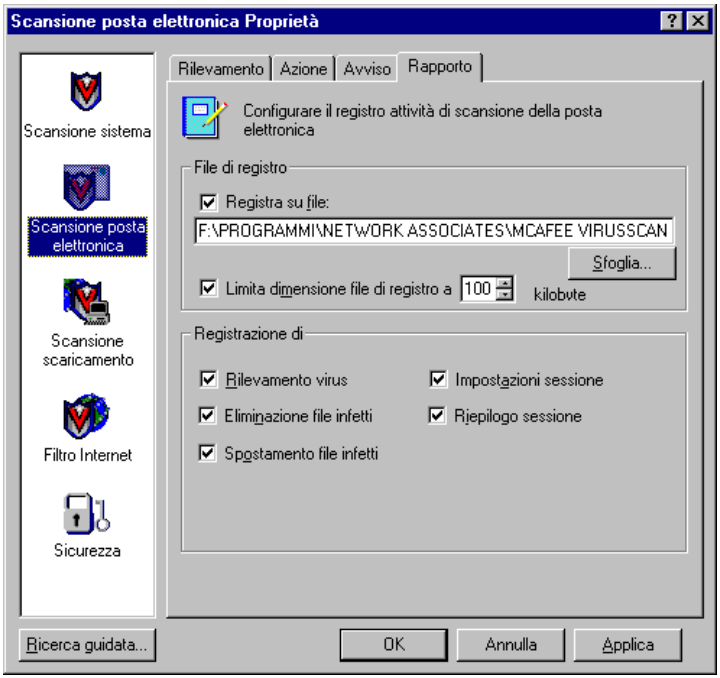

Figura 4-21. finestra di dialogo Proprietà Scansione posta - Pagina Report

2. Selezionare la casella di controllo **Registra su file**.

   Per impostazione predefinita, VShield scrive le informazioni di registro nel file WEBEMAIL.TXT contenuto nella directory del programma VirusScan. È possibile immettere un altro nome e percorso nell'apposita casella di testo o fare clic su **Sfoglia** per localizzare un file adatto in qualsiasi altra posizione del proprio disco o della propria rete.

3. Per ridurre al minimo le dimensioni del file di registro, selezionare la casella di controllo **Limita dimensioni del file di registro a**, quindi immettere un valore per le dimensioni in kilobyte del file nella relativa casella di testo.

   Immettere un valore compreso tra 10KB e 999KB. Per impostazione predefinita, VShield limita la dimensione del file a 100KB. Se i dati del file di registro eccedono la dimensione di file specificata, VShield cancella il registro esistente e riprende dal punto di interruzione.

4. Selezionare le caselle di controllo corrispondenti alle informazioni che VShield dovrà annotare nel proprio file di registro. È possibile selezionare la registrazione di queste informazioni:

   - **Rilevamento virus.** Selezionare questa casella di controllo affinché VShield annoti il numero dei file infetti rilevati in fase di analisi della posta elettronica.
   - **Eliminazione file infetto.** Selezionare questa casella di controllo affinché VShield annoti il numero dei file infetti eliminati in fase di analisi della posta elettronica.
   - **Spostamento file infetti.** Selezionare questa casella di controllo affinché VShield annoti il numero dei file infetti spostati nella directory di quarantena.
   - **Impostazioni sessione.** Selezionare questa casella di controllo affinché VShield elenchi le opzioni scelte nella finestra di dialogo Proprietà Scansione posta per ogni sessione di scansione.
   - **Riepilogo sessione.** Selezionare questa casella di controllo affinché VShield crei un riepilogo delle azioni eseguite durante ogni sessione di scansione. Le informazioni di riepilogo includono il numero dei file scanditi da VShield, il numero e il tipo dei virus rilevati, il numero dei file spostati o eliminati e altri dati.

5. Fare clic su un'altra scheda per cambiare qualsiasi impostazione di Scansione posta o fare clic su una delle icone lungo il lato della finestra di dialogo Proprietà Scansione posta al fine di scegliere opzioni per un altro modulo.

   Per salvare le modifiche nel modulo Scansione posta senza chiudere la sua finestra di dialogo fare clic su **Applica**. Per salvare le modifiche e chiudere la finestra di dialogo, fare clic su **OK**. Fare clic su **Annulla** per chiudere la finestra di dialogo senza salvare le modifiche.

   NOTA: Facendo clic su **Annulla** non è possibile ripristinare le modifiche salvate facendo clic su **Applica**.

Configurazione del modulo Scansione scaricamento

Il modulo Scansione scaricamento di VShield può controllare i file scaricati da Internet quando vengono visitati siti Web, siti FTP e altri siti Internet. Questo modulo inoltre è la sede in cui impostare le opzioni di risposta agli allegati di posta infetti ricevuti attraverso i programmi client di posta POP-3 o SMTP quali Eudora, Netscape Mail o Microsoft Outlook Express. Per attivare questa funzione, occorre inoltre scegliere un sistema di posta appropriato nella pagina Rilevamento del modulo Scansione posta. Vedere "Selezione delle opzioni di Rilevamento" a pagina 108 per i dettagli.

Per impostare VShield affinché scandisca i file scaricati, fare clic sull'icona Scansione scaricamento sul lato sinistro della finestra di dialogo Proprietà VShield al fine di visualizzare le pagine delle proprietà di questo modulo. Le opzioni disponibili sono descritte nelle sezioni che seguono.

Selezione delle opzioni di Rilevamento

VShield inizialmente presume che l'utente desideri effettuare una scansione per la ricerca di virus ogni qualvolta viene scaricato da Internet un file soggetto al rischio di infezioni (vedere Figura 4-22). Queste opzioni predefinite forniscono un livello di sicurezza eccellente, ma il proprio ambiente di lavoro potrebbe richiedere impostazioni diverse.

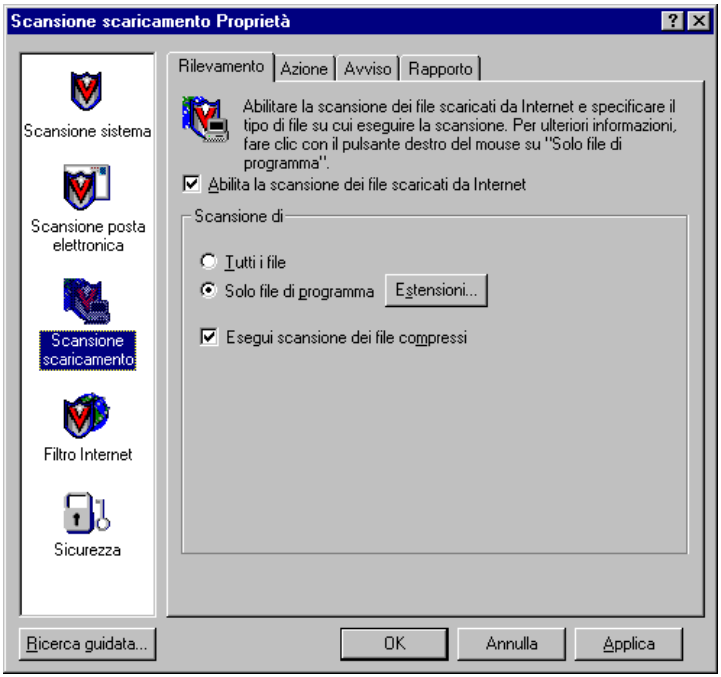

Figura 4-22. La finestra di dialogo Proprietà Scansione scaricamento - Pagina Rilevamento

Per modificare queste impostazioni, accertarsi che sia selezionata la casella di controllo Attiva scansione scaricamento da Internet, quindi procedere come segue:

1. Specificare i tipi di file che VShield dovrà esaminare. È possibile

   - **Scelta dei tipi di file da sottoporre a scansione.** Normalmente i virus non possono infettare i file di dati o i file che contengono un codice non eseguibile. È possibile quindi ridurre con sicurezza il raggio d'azione delle attività di scansione ai soli file maggiormente soggetti al rischio di infezioni da virus, al fine di rendere più rapide le operazioni di scaricamento, in particolare con i file grandi o i gruppi numerosi di file. Per fare questo, selezionare il pulsante **Solo file di programma**. Per vedere o specificare le estensioni dei nomi dei file che VShield esaminerà, fare clic su **Estensioni** per aprire la finestra di dialogo Estensioni file di programmi (Figura 4-23).

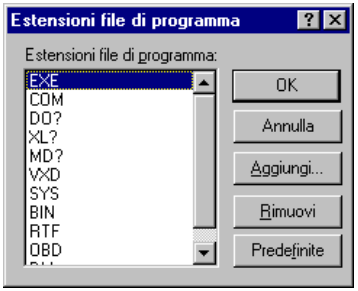

Figura 4-23. Finestra di dialogo Estensioni file di programma

Per impostazione predefinita, VShield analizza per la ricerca di virus i file che presentano le estensioni .EXE, .COM, .DO?, .XL?, .RTF, .BIN, .SYS, .MD? e .OBD. I file con estensione .DO?, .XL?, .RTF, .MD? e .OBD sono file di Microsoft Office e tutti possono contenere infezioni di virus macro. Il carattere? è un carattere jolly che consente a VShield di scandire sia i file di documenti sia i modelli.

- Per aggiungere estensioni all'elenco fare clic su **Aggiungi**, quindi digitare le estensioni dei file che VShield dovrà scandire nella finestra di dialogo che appare.
- Per eliminare un'estensione dall'elenco, selezionarla, quindi fare clic su **Elimina**.
- Fare clic su **Predefinito** per ripristinare l'elenco nella sua forma originaria.

Una volta terminata quest'operazione , fare clic su **OK** per chiudere la finestra di dialogo.

- **Scandire tutti i file.** Affinché VShield esamini tutti i file scaricati, qualunque sia l'estensione, selezionare il pulsante **Tutti i file**. Questo potrebbe rallentare il funzionamento del sistema, ma assicura l'immunità da virus.
- **Scansione di file compressi.** Selezionare la casella di controllo **File compressi** per fare in modo che il modulo Scansione scaricamento ricerchi i virus nei file compressi dei seguenti formati: .??_, .CAB, LZEXE, LZH, PKLite, .TD0 e .ZIP. Sebbene garantisca una migliore protezione, la scansione dei file compressi in fase di scaricamento può rallentare lo scaricamento.

2. Fare clic sulla scheda Azione per scegliere ulteriori opzioni di VShield. Per salvare le modifiche senza chiudere la finestra di dialogo Proprietà Scansione scaricamento, fare clic su **Applica**. Per salvare le modifiche e chiudere la finestra di dialogo, fare clic su **OK**. Fare clic su **Annulla** per chiudere la finestra di dialogo senza salvare le modifiche.

❑ **NOTA:** Facendo clic su **Annulla** non è possibile ripristinare le modifiche salvate facendo clic su **Applica**.

Scegliere le opzioni Azione

Quando VShield rileva la presenza di un virus, può rispondere o chiedendo all'utente cosa fare con il file infetto o eseguendo automaticamente un'azione che è stata scelta in origine dall'utente stesso. Usare la pagina delle proprietà Azione per specificare quali opzioni di risposta si desidera che VShield fornisca quando rileva un virus o quali azioni si desidera che VShield esegua automaticamente.

Procedere come segue:

1. Fare clic sulla scheda Azione nel modulo Scansione scaricamento per visualizzare la corretta pagina di proprietà (Figura 4-24).

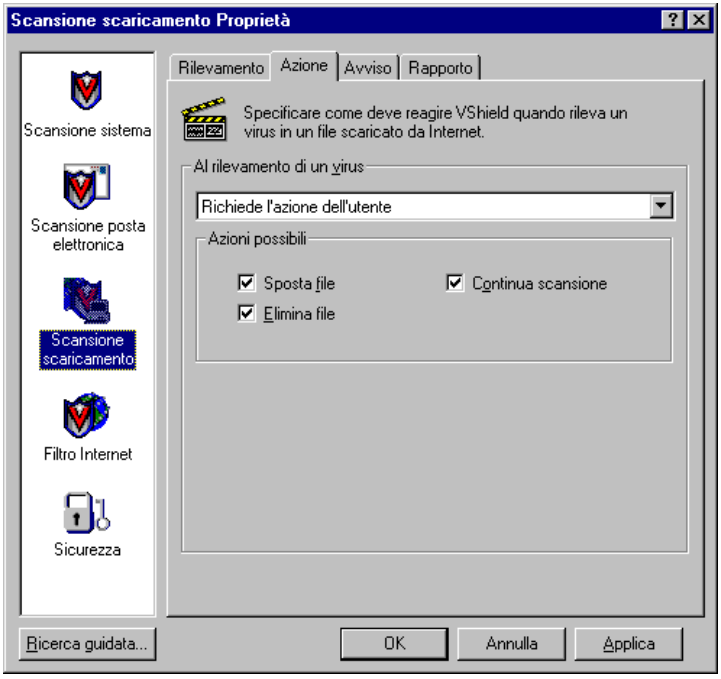

Figura 4-24. La finestra di dialogo Proprietà Scansione scaricamento - Pagina Azione

2. Selezionare una risposta dall'elenco **Al rilevamento di un virus**. L'area immediatamente al di sotto dell'elenco cambia per visualizzare opzioni aggiuntive per ciascuna selezione. Le scelte disponibili sono:

   - **Richiedi azione.** Scegliere questa risposta per fare in modo che VShield chieda cosa fare qualora venga rilevato un virus—il programma visualizzerà un messaggio di avviso e offrirà una serie di possibili risposte. Selezionare le opzioni da visualizzare nel messaggio di avviso:

     – **Sposta file.** Con questa opzione VShield sposta il file infetto in una directory di quarantena selezionata precedentemente.

     – **Elimina file.** Con questa opzione VShield elimina immediatamente il file infetto.

– **Continua scansione.** Con questa opzione VShield continua la scansione senza effettuare altre azioni. Se sono attivate le opzioni di reporting del programma, VShield annota l'incidente nel proprio file di registro.

- **Sposta file infetti in una cartella.** Con questa opzione VShield sposta i file infetti in una directory di quarantena non appena li rileva. Per impostazione predefinita, VShield sposta questi file in una cartella denominata INFECTED che il programma crea al livello radice del disco in cui si salvano i file scaricati.

  Se ad esempio VShield rileva un virus in un file scaricato in E:\RISORSE DEL COMPUTER ed era stata specificata INFECTED come directory di quarantena, VShield copia il file in E:\INFECTED.

  È possibile immettere un altro nome e percorso nell'apposita casella di testo o fare clic su **Sfoglia** per localizzare una cartella adatta sul proprio disco rigido.

- **Elimina file infetti.** Scegliere questa risposta per fare in modo che VShield elimini ogni file infetto scaricato. Accertarsi di attivare le funzioni di reporting di VShield, in modo da avere una registrazione di quali file VShield ha eliminato.

- **Scansione continua.** Scegliere questa risposta per fare in modo che VShield continui la scansione senza adottare alcuna azione contro i virus rilevati. Se inoltre sono attivate le funzioni di reporting di VShield (vedere "Selezione delle opzioni di Rapporto" a pagina 130 per i dettagli), il programma registrerà i nomi di tutti i virus rilevati e i nomi dei file infetti affinché sia possibile eliminarli in seguito.

3. Fare clic sulla scheda Avviso per scegliere ulteriori opzioni di VShield. Per salvare le modifiche senza chiudere la finestra di dialogo Proprietà Scansione scaricamento, fare clic su **Applica**. Per salvare le modifiche e chiudere la finestra di dialogo, fare clic su **OK**. Fare clic su **Annulla** per chiudere la finestra di dialogo senza salvare le modifiche.

❑ **NOTA:** Facendo clic su **Annulla** non è possibile ripristinare le modifiche salvate facendo clic su **Applica**.

Selezione delle opzioni di Avviso

Una volta configurato il programma con le opzioni di risposta desiderate, è possibile lasciare che VShield ricerchi i virus nei file scaricati e li rimuova automaticamente, quando li rileva, senza quasi nessun intervento ulteriore. Se invece si desidera che VShield informi immediatamente l'utente quando rileva un virus, affinché questi possa scegliere l'azione più opportuna, è possibile configurare il programma perché invii un messaggio d'avviso all'utente principale o ad altri in vari modi. Utilizzare la pagina di proprietà Avvisi per scegliere i metodi di avviso che si desidera utilizzare.

Procedere come segue:

1. Fare clic sulla scheda Avviso del modulo Scansione scaricamento per visualizzare la corretta pagina di proprietà (Figura 4-25).

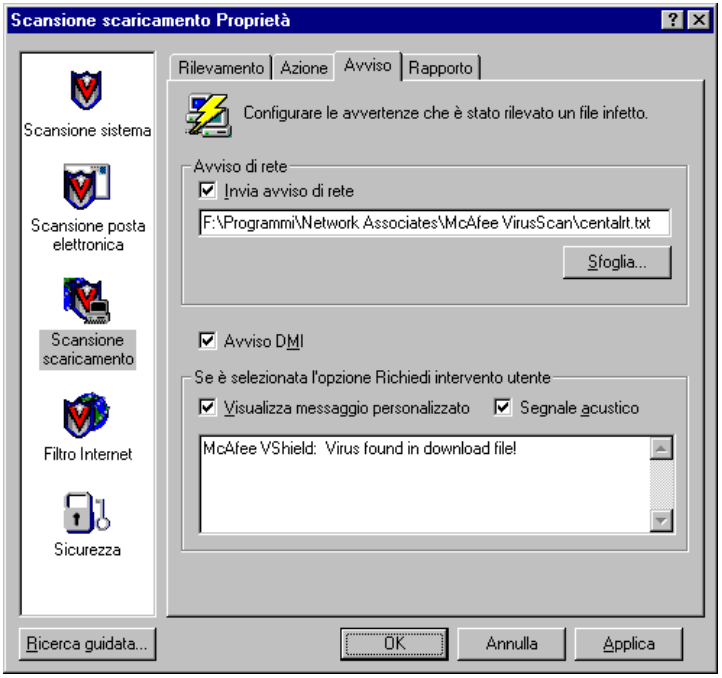

Figura 4-25. La finestra di dialogo Proprietà Scansione scaricamento - Pagina Avviso

2. Affinché VShield invii un messaggio d'avviso a un server che usa NetShield, una soluzione antivirus prodotta da Network Associates, selezionare la casella di controllo **Invia avviso alla rete**, quindi immettere il percorso della cartella di avviso NetShield della propria rete o fare clic su **Sfoglia** per localizzare la cartella corretta.

   NOTA: La cartella scelta deve contenere CENTALRT.TXT, il file di avviso centralizzato NetShield. NetShield raccoglie i messaggi di avviso provenienti da VShield e da altri software Network Associates e quindi li passa agli amministratori della rete perché prendano i necessari provvedimenti. Per ulteriori informazioni sull'Avviso centralizzato, vedere il *Manuale dell'utente* di NetShield.

3. Affinché VShield invii i messaggi di avviso per i virus attraverso la DMI Component Interface alle applicazioni della scrivania e alle applicazioni di gestione della rete che si eseguono sulla rete, selezionare la casella di controllo **Avviso DMI**.

   NOTA: DMI (Desktop Management Interface) è uno standard per informazioni sulle richieste di gestione delle comunicazioni e le informazioni di avviso tra i componenti hardware e software dei computer o collegati ad essi e le applicazioni utilizzate per la loro gestione. Per ulteriori informazioni sull'uso di questo metodo di avviso, rivolgersi all'amministratore della rete.

4. Se era stata scelta l'opzione **Richiedi azione dell'utente** come risposta nella pagina Azione (vedere "Scegliere le opzioni Azione" a pagina 125 per i dettagli), è possibile inoltre fare in modo che VShield emetta un segnale acustico di avviso e mostri un messaggio personalizzato quando rileva un virus. Per effettuare quest'operazione, selezionare la casella di controllo **Visualizza messaggio personalizzato**, quindi digitare il messaggio che si desidera visualizzare nella relativa casella di controllo—è possibile digitare fino a 225 caratteri. Selezionare poi la casella di controllo **Avviso sonoro**.

5. Fare clic sulla scheda Report per scegliere ulteriori opzioni di VShield. Per salvare le modifiche senza chiudere la finestra di dialogo Proprietà Scansione scaricamento, fare clic su **Applica**. Per salvare le modifiche e chiudere la finestra di dialogo, fare clic su **OK**. Fare clic su **Annulla** per chiudere la finestra di dialogo senza salvare le modifiche.

   NOTA: Facendo clic su **Annulla** non è possibile ripristinare le modifiche salvate facendo clic su **Applica**.

Selezione delle opzioni di Rapporto

Il modulo Scansione scaricamento di VShield elenca le proprie impostazioni correnti e riepiloga le azioni eseguite durante le operazioni di scansione in un file di registro denominato WEBINET.TXT. È possibile fare in modo che VShield scriva il proprio registro in questo file o usare qualsiasi editor di testo per creare un file che possa essere utilizzato dal programma a questo scopo. Il file di registro può essere aperto e stampato in seguito con qualsiasi editor di testo e usato quindi come documento di riferimento. Usare la pagina delle proprietà Report per determinare quali informazioni VShield dovrà includere nel proprio file di registro.

Per impostare VShield affinché annoti in un file di registro le azioni eseguite, procedere come segue:

1. Fare clic sulla scheda Report nel modulo Scansione scaricamento per visualizzare la corretta pagina di proprietà (Figura 4-26).

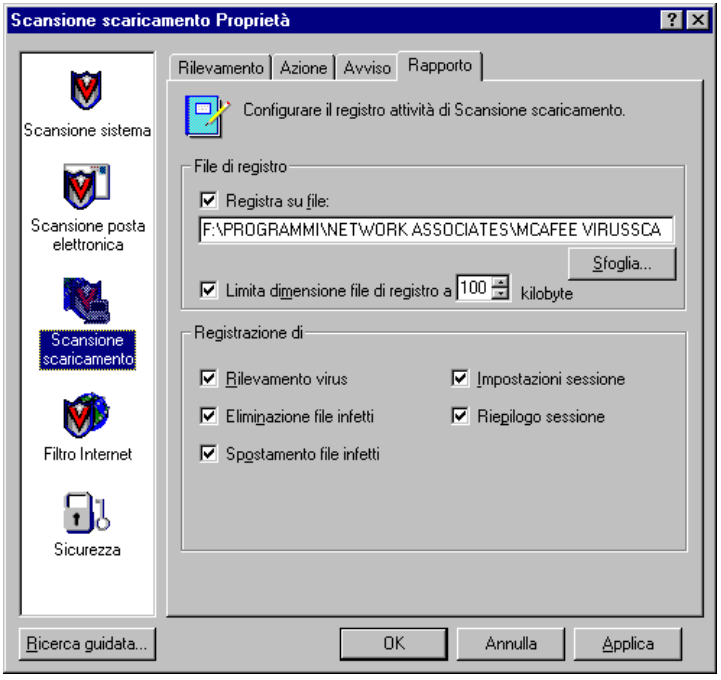

Figura 4-26. La finestra di dialogo Proprietà Scansione scaricamento - Pagina Report

2. Selezionare la casella di controllo **Registra su file**.

   Per impostazione predefinita, VShield scrive le informazioni di registro nel file WEBFLTR.TXT contenuto nella directory del programma VirusScan. È possibile immettere un altro nome e percorso nell'apposita casella di testo o fare clic su **Sfoglia** per localizzare un file adatto in qualsiasi altra posizione del proprio disco o della propria rete.

3. Per ridurre al minimo le dimensioni del file di registro, selezionare la casella di controllo **Limita dimensioni del file di registro a**, quindi immettere un valore per le dimensioni in kilobyte del file nella relativa casella di testo.

   Immettere un valore compreso tra 10KB e 999KB. Per impostazione predefinita, VShield limita la dimensione del file a 100KB. Se i dati del file di registro eccedono la dimensione di file specificata, VShield cancella il registro esistente e riprende dal punto di interruzione.

4. Selezionare le caselle di controllo corrispondenti alle informazioni che VShield dovrà annotare nel proprio file di registro. È possibile scegliere di registrare queste informazioni:

   - **Rilevamento virus.** Selezionare questa casella di controllo affinché VShield annoti il numero dei file infetti rilevati in fase di scaricamento.
   - **Eliminazione file infetto**. Selezionare questa casella di controllo affinché VShield annoti il numero dei file infetti rilevati in fase di scaricamento.
   - **Spostamento file infetti.** Selezionare questa casella di controllo affinché VShield annoti il numero dei file infetti spostati nella directory di quarantena.
   - **Impostazioni sessione.** Selezionare questa casella di controllo affinché VShield elenchi le opzioni scelte nella finestra di dialogo Proprietà Scansione scaricamento per ogni sessione di scansione.
   - **Riepilogo sessione.** Selezionare questa casella di controllo affinché VShield crei un riepilogo delle azioni eseguite durante ogni sessione di scansione. Le informazioni di riepilogo includono il numero dei file scanditi da VShield, il numero e il tipo dei virus rilevati, il numero dei file spostati o eliminati e altri dati.

5. Fare clic su un'altra scheda per cambiare qualsiasi impostazione di Scansione scaricamento o fare clic su una delle icone lungo il lato della finestra di dialogo Proprietà Scansione scaricamento al fine di scegliere opzioni per un altro modulo.

   Per salvare le modifiche nel modulo Scansione scaricamento senza chiudere la sua finestra di dialogo fare clic su **Applica**. Per salvare le modifiche e chiudere la finestra di dialogo, fare clic su **OK**. Fare clic su **Annulla** per chiudere la finestra di dialogo senza salvare le modifiche.

❑ **NOTA:** Facendo clic su **Annulla** non è possibile ripristinare le modifiche salvate facendo clic su **Applica**.

Configurazione del modulo Filtro Internet

Sebbene sia gli oggetti Java sia gli oggetti ActiveX includono sicure funzioni di protezione progettate per impedire danni ai computer, alcuni programmatori hanno sviluppato oggetti che sfruttano le misteriose funzioni Java e ActiveX per causare vari tipi di danni ai sistemi.

Oggetti pericolosi come questi sono spesso in agguato sui siti Web in attesa di essere scaricati nei computer degli utenti che visitano il sito, i quali di solito non si accorgono neppure della loro presenza. Molti browser includono una funzione che permette di bloccare completamente gli applet Java o i controlli ActiveX o di attivare opzioni di protezione che autenticano gli oggetti prima di scaricarli nel sistema. Ma questi approcci possono privare l'utente dei vantaggi dati dall'interattività dei siti Web visitati, bloccando indiscriminatamente tutti gli oggetti, pericolosi e non.

VShield consente un approccio più giudizioso. Il programma usa un proprio database aggiornato di oggetti notoriamente dannosi per analizzare le classi Java e i controlli ActiveX incontrati durante la navigazione in Internet.

Per impostare VShield affinché blocchi gli oggetti dannosi e filtri i siti Internet pericolosi, fare clic sull'icona Filtro Internet sul lato sinistro della finestra di dialogo Proprietà VShield, per visualizzare le pagine delle proprietà di questo modulo. Le opzioni disponibili sono descritte nelle sezioni che seguono.

Selezione delle opzioni di Rilevamento

VShield per impostazione predefinita blocca tutti gli oggetti e i siti dannosi elencati nel database, per evitare che l'utente li incontri accidentalmente (Figura 4-27).

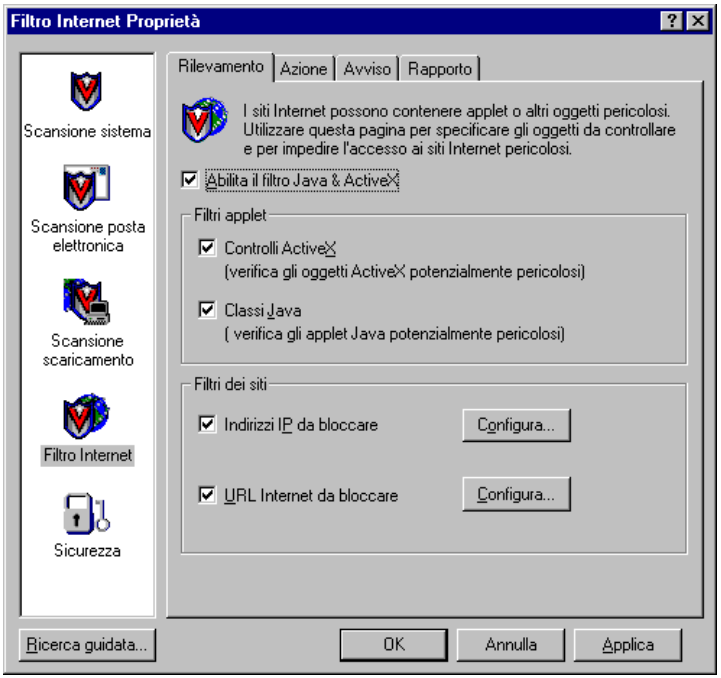

Figura 4-27. Proprietà Filtro Internet - Pagina Rilevamento

Per cambiare questa impostazione predefinita, verificare che sia selezionata la casella di controllo Attiva flirto Java e ActiveX, quindi procedere come segue:

1. Indicare a VShield quali oggetti filtrare. Le opzioni disponibili sono:

   - **Controlli ActiveX.** Selezionare questa casella di controllo affinché VShield ricerchi e blocchi i controlli dannosi ActiveX o .OCX.
   - **Classi Java.** Selezionare questa casella di controllo affinché VShield ricerchi e blocchi le classi Java, o applet dannose scritte in Java.

VShield confronta gli oggetti incontrati quando vengono visitati i siti Internet con un proprio database interno in cui sono elencate le caratteristiche degli oggetti che notoriamente causano danni. Quando rileva una corrispondenza, VShield può avvertire l'utente e permettere a questi di decidere cosa fare, oppure può impedire automaticamente lo scaricamento dell'oggetto. Vedere "Scegliere le opzioni Azione" a pagina 137 per ulteriori dettagli.

2. Indicare a VShield quali siti filtrare. Il programma usa un elenco di siti Internet pericolosi per decidere a quali impedire l'accesso da parte del browser in uso. è possibile attivare questa funzione e aggiungere elementi all'elenco dei siti "proibiti" in due modi:

   - **Indirizzi IP da bloccare.** Selezionare questa casella di controllo affinché VShield identifichi i siti Internet pericolosi utilizzando i loro indirizzi Internet Protocol (IP). Per vedere o specificare gli indirizzi che VShield dovrà proibire, fare clic su **Configura** per aprire la finestra di dialogo Indirizzi IP proibiti (Figura 4-28).

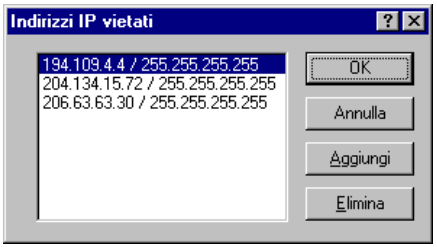

Figura 4-28. La finestra di dialogo Indirizzi IP proibiti

Gli indirizzi dei protocolli Internet sono costituiti da quattro gruppi di tre numeri ciascuno, formattati nel modo seguente:

123.123.123.123

Ogni gruppo di numeri può variare da zero a 255. VShield può utilizzare questo numero per identificare un computer o una rete di computer specifici in Internet e impedire al browser di collegarsi ad essi. In Figura 4-28, ogni indirizzo presenta due gruppi di numeri IP. Il primo è l'indirizzo di dominio del sito proibito, ovvero il numero utilizzato per trovarlo su Internet, e il secondo è una "subnet mask."

Una subnet mask è un modo per “rimappare” una serie di indirizzi di computer in una rete interna. VShield mostra la subnet mask predefinita 255.255.255.255. Nella maggior parte dei casi non è necessario cambiare questo numero. Ma se un particolare nodo di rete di un sito a cui accedere fosse una fonte certa di pericolo, può essere necessario immettere una subnet mask per tutelare la sicurezza di accesso alle altre macchine di quel sito.

– Per aggiungere elementi all’elenco dei siti proibiti, fare clic su **Aggiungi**, quindi digitare gli indirizzi che VShield dovrà bloccare nella finestra di dialogo che appare (Figura 4-29).

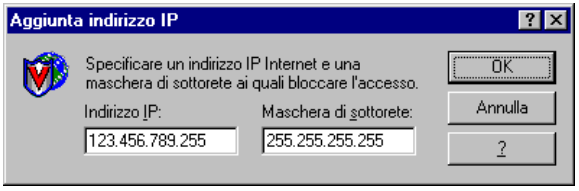

Figura 4-29. La finestra di dialogo Aggiungi indirizzo IP

Accertarsi di immettere ogni indirizzo nella forma corretta. Se si conosce il valore della subnet mask per il sito che si desidera evitare, immetterlo nella casella di testo sotto. Diversamente, lasciare attivato il valore predefinito. Fare clic su **OK** per salvare l’indirizzo e tornare alla finestra di dialogo Indirizzi IP proibiti. Per aggiungere un altro indirizzo all’elenco ripetere questi passaggi.

– Per rimuovere un indirizzo dall’elenco degli indirizzi proibiti, selezionarlo, quindi fare clic su **Elimina**.

Terminate le modifiche all’elenco fare clic su **OK** per salvare le modifiche e tornare alla finestra di dialogo Proprietà Filtro Internet. Fare clic su **Annulla** per chiudere la finestra di dialogo senza salvare le modifiche.

• **URL Internet da bloccare.** Selezionare questa casella di controllo affinché VShield identifichi i siti Internet pericolosi utilizzando il loro indirizzo Uniform Resource Locator. Per vedere o specificare gli indirizzi che VShield dovrà proibire, fare clic su **Configura** per aprire la finestra di dialogo URL proibiti (Figura 4-30 a pagina 136).

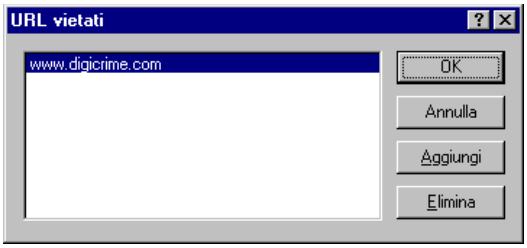

Figura 4-30. La finestra di dialogo URL proibiti

A volte utilizzato come sinonimo di "nome di dominio" o "nome host", un URL specifica il nome e la posizione di un computer in Internet, generalmente insieme al "protocollo di trasferimento" che si desidera usare per richiedere una risorsa di quel computer. Un URL completo per un sito Web ad esempio potrebbe presentarsi come segue:

http://www.dominiopericoloso.it

L'URL completo indica al browser di richiedere la risorsa attraverso il protocollo HyperText Transport Protocol ("http://") di un computer "www" che si trova su una rete denominata "dominiopericoloso.it". Altri protocolli di trasferimento sono ad esempio "ftp://" e "gopher://." Il sistema Domain Name Server di Internet converte gli URL nei corretti indirizzi IP utilizzando un database aggiornato, centralizzato e incrociato.

– Per aggiungere elementi all'elenco dei siti proibiti, fare clic su **Aggiungi**, quindi digitare gli indirizzi che VShield dovrà bloccare nella finestra di dialogo che appare (Figura 4-31).

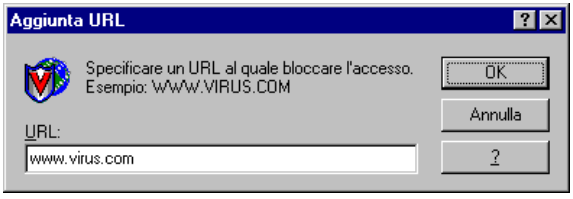

Figura 4-31. La finestra di dialogo Aggiungi URL

Accertarsi di immettere ogni indirizzo nella forma corretta. Per indicare un sito Web a cui impedire l'accesso è possibile immettere *solo il nome di dominio* se il protocollo è HyperText Transport Protocol. Fare clic su **OK** per salvare l'indirizzo e tornare alla finestra di dialogo Indirizzi IP proibiti. Per aggiungere un altro indirizzo all'elenco ripetere questi passaggi.

– Per rimuovere un indirizzo dall'elenco degli indirizzi proibiti, selezionarlo, quindi fare clic su **Elimina**.

Terminate le modifiche all'elenco fare clic su **OK** per salvare le modifiche e tornare alla finestra di dialogo Proprietà Filtro Internet. Fare clic su **Annulla** per chiudere la finestra di dialogo senza salvare le modifiche.

3. Fare clic sulla scheda Azione per scegliere ulteriori opzioni di VShield. Per salvare le modifiche senza chiudere la finestra di dialogo Proprietà Filtro Internet fare clic su **Applica**. Per salvare le modifiche e chiudere la finestra di dialogo, fare clic su **OK**. Fare clic su **Annulla** per chiudere la finestra di dialogo senza salvare le modifiche.

❑ **NOTA:** Facendo clic su **Annulla** non è possibile ripristinare le modifiche salvate facendo clic su **Applica**.

Scegliere le opzioni Azione

Quando VShield incontra un oggetto pericoloso o un sito proibito può rispondere o chiedendo all'utente se bloccare l'oggetto o il sito o effettuando automaticamente il blocco. Usare la pagina delle proprietà Azione per specificare quali delle seguenti azioni VShield dovrà eseguire.

Per impostazione predefinita, VShield lascia decidere all'utente cosa fare (Figura 4-32 a pagina 138).

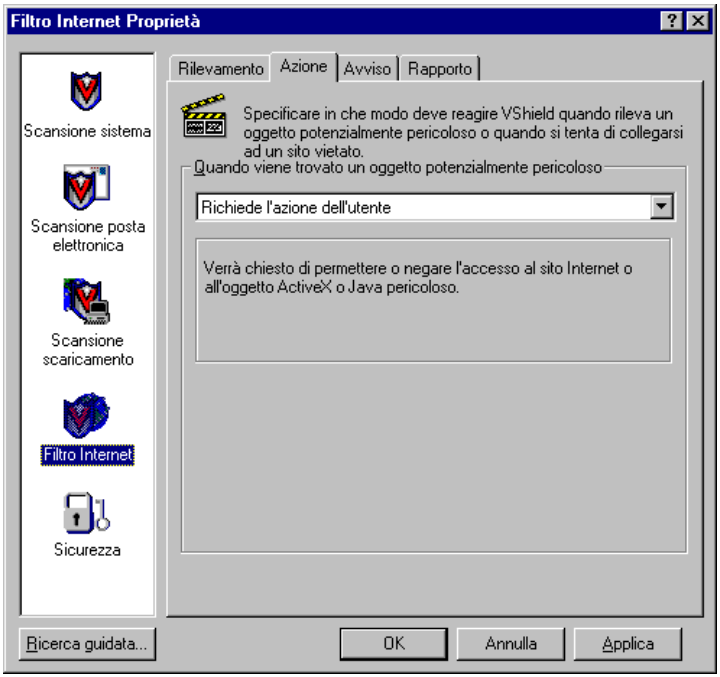

Figura 4-32. La finestra di dialogo Proprietà Filtro Internet - Pagina Azione

Scegliere una risposta dall'elenco **Quando viene rilevato un oggetto potenzialmente dannoso**. Le scelte disponibili sono:

- **Richiedi azione.** Scegliere questa risposta per fare in modo che VShield chieda se bloccare un oggetto o un sito dannoso o se consentirvi l'accesso.
- **Nega accesso all'oggetto.** Scegliere questa opzione affinché VShield blocchi automaticamente gli oggetti o i siti dannosi. Il programma agirà in base al contenuto del proprio database interno e alle informazioni sui siti aggiunte dall'utente. Vedere "Selezione delle opzioni di Rilevamento" a pagina 133 per i dettagli.

Fare clic sulla scheda Avviso per scegliere ulteriori opzioni di VShield. Per salvare le modifiche senza chiudere la finestra di dialogo Proprietà Filtro Internet fare clic su **Applica**. Per salvare le modifiche e chiudere la finestra di dialogo, fare clic su **OK**. Fare clic su **Annulla** per chiudere la finestra di dialogo senza salvare le modifiche.

NOTA: Facendo clic su **Annulla** non è possibile ripristinare le modifiche salvate facendo clic su **Applica**.

Selezione delle opzioni di Avviso

Una volta configurato il programma con le opzioni di risposta desiderate, è possibile lasciare che VShield ricerchi e blocchi gli oggetti o i siti Internet dannosi, senza quasi nessun intervento ulteriore. Se invece si desidera che VShield informi immediatamente l'utente quando incontra tali oggetti o siti, affinché questi possa scegliere l'azione più opportuna, è possibile configurare il programma perché invii un messaggio d'avviso all'utente principale o ad altri in vari modi. Utilizzare la pagina di proprietà Avvisi per scegliere i metodi di avviso che si desidera utilizzare.

Procedere come segue:

1. Fare clic sulla scheda Avviso del modulo Filtro Internet per visualizzare la corretta pagina di proprietà (Figura 4-33).

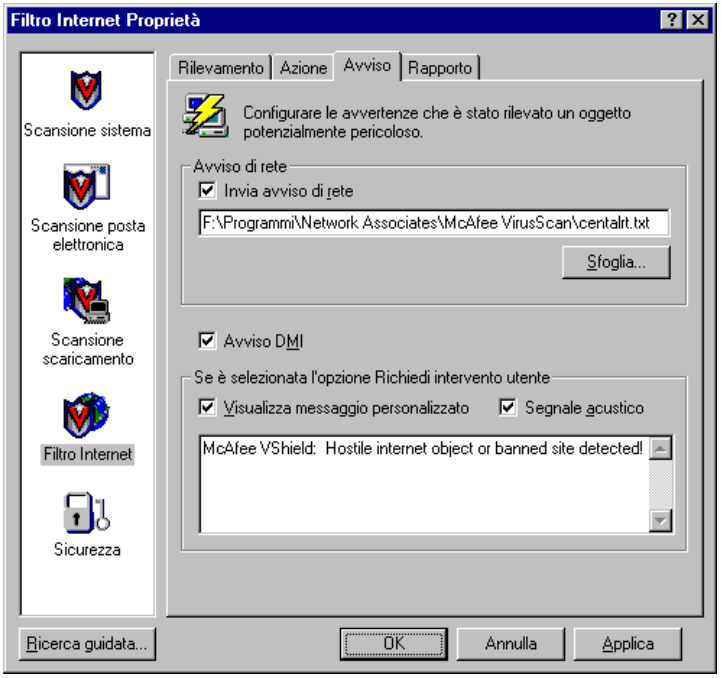

Figura 4-33. La finestra di dialogo Proprietà Filtro Internet - Pagina Avviso

2. Affinché VShield invii un messaggio d'avviso a un server che usa NetShield, una soluzione antivirus prodotta da Network Associates, selezionare la casella di controllo **Invia avviso alla rete**, quindi immettere il percorso della cartella di avviso NetShield della propria rete o fare clic su **Sfoglia** per localizzare la cartella corretta.

   NOTA: La cartella scelta deve contenere CENTALRT.TXT, il file di avviso centralizzato NetShield. NetShield raccoglie i messaggi di avviso provenienti da VShield e da altri software Network Associates e quindi li passa agli amministratori della rete perché prendano i necessari provvedimenti. Per ulteriori informazioni sull'Avviso centralizzato, vedere il *Manuale dell'utente* di NetShield.

3. Affinché VShield invii i messaggi di avviso per i virus attraverso la DMI Component Interface alle applicazioni della scrivania e alle applicazioni di gestione della rete che si eseguono sulla rete, selezionare la casella di controllo **Avviso DMI**.

   NOTA: DMI (Desktop Management Interface) è uno standard per informazioni sulle richieste di gestione delle comunicazioni e le informazioni di avviso tra i componenti hardware e software dei computer o collegati ad essi e le applicazioni utilizzate per la loro gestione. Per ulteriori informazioni sull'uso di questo metodo di avviso, rivolgersi all'amministratore della rete.

4. Se era stata scelta l'opzione **Richiedi azione dell'utente** come risposta nella pagina Azione (vedere "Scegliere le opzioni Azione" a pagina 137 per i dettagli), è possibile inoltre fare in modo che VShield emetta un segnale acustico di avviso e mostri un messaggio personalizzato quando rileva un virus. Per effettuare quest'operazione, selezionare la casella di controllo **Visualizza messaggio personalizzato**, quindi digitare il messaggio che si desidera visualizzare nella relativa casella di controllo—è possibile digitare fino a 225 caratteri. Selezionare poi la casella di controllo **Avviso sonoro**.

5. Fare clic sulla scheda Report per scegliere ulteriori opzioni di VShield. Per salvare le modifiche senza chiudere la finestra di dialogo Proprietà Filtro Internet fare clic su **Applica**. Per salvare le modifiche e chiudere la finestra di dialogo, fare clic su **OK**. Fare clic su **Annulla** per chiudere la finestra di dialogo senza salvare le modifiche.

   NOTA: Facendo clic su **Annulla** non è possibile ripristinare le modifiche salvate facendo clic su **Applica**.

Selezione delle opzioni di Rapporto

Il modulo Filtro Internet di VShield annota il numero degli oggetti Java e ActiveX e il numero di oggetti a cui ha impedito di accedere al computer in un file di registro denominato WEBFLTR.TXT. Lo stesso file registra il numero di siti Internet visitati mentre VShield era attivo e il numero dei siti pericolosi a cui il programma ha impedito l'accesso da parte del browser.

È possibile fare in modo che VShield scriva il proprio registro nel proprio file predefinito o usare qualsiasi editor di testo per creare un file che possa essere utilizzato dal programma a questo scopo. Il file di registro può essere aperto e stampato in seguito con qualsiasi editor di testo e usato quindi come documento di riferimento. Usare la pagina delle proprietà Report per indicare il file che si desidera usare come registro per la funzione Filtro Internet di VShield e per determinare la massima dimensione ammessa per il file stesso.

Per impostare VShield affinché annoti in un file di registro le azioni eseguite, procedere come segue:

1. Fare clic sulla scheda Report nel modulo Filtro Internet per visualizzare la corretta pagina di proprietà (Figura 4-34).

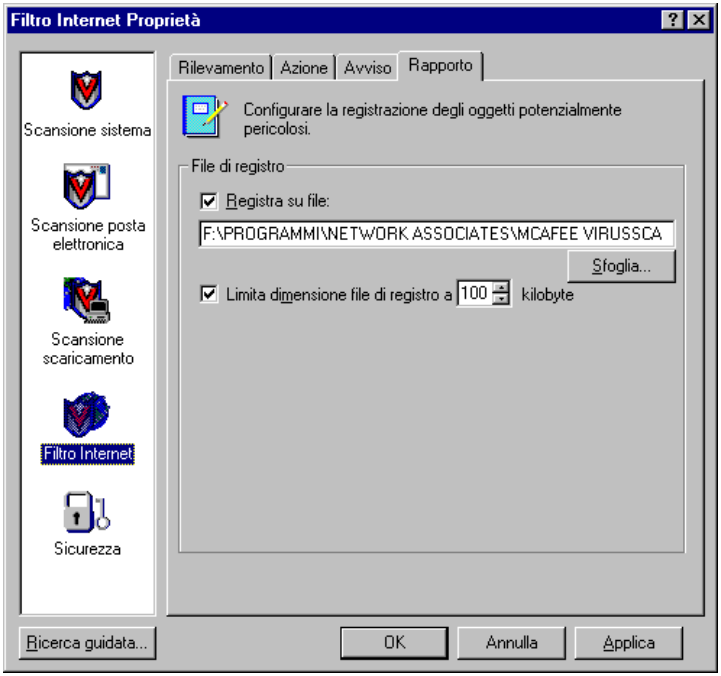

Figura 4-34. La finestra di dialogo Proprietà Filtro Internet - Pagina Report

2. Selezionare la casella di controllo **Registra su file**.

   Per impostazione predefinita, VShield scrive le informazioni di registro nel file WEBFLTR.TXT contenuto nella directory del programma VirusScan. È possibile immettere un altro nome e percorso nell'apposita casella di testo o fare clic su **Sfoglia** per localizzare un file adatto in qualsiasi altra posizione del proprio disco o della propria rete.

3. Per ridurre al minimo le dimensioni del file di registro, selezionare la casella di controllo **Limita dimensioni del file di registro a**, quindi immettere un valore per le dimensioni in kilobyte del file nella relativa casella di testo.

   Immettere un valore compreso tra 10KB e 999KB. Per impostazione predefinita, VShield limita la dimensione del file a 100KB. Se i dati del file di registro eccedono la dimensione di file specificata, VShield cancella il registro esistente e riprende dal punto di interruzione.

4. Fare clic su un'altra scheda per cambiare qualsiasi impostazione di Filtro Internet o fare clic su una delle icone lungo il lato della finestra di dialogo Proprietà Filtro Internet al fine di scegliere opzioni per un altro modulo.

   Per salvare le modifiche nel modulo Filtro Internet senza chiudere la sua finestra di dialogo fare clic su **Applica**. Per salvare le modifiche e chiudere la finestra di dialogo, fare clic su **OK**. Fare clic su **Annulla** per chiudere la finestra di dialogo senza salvare le modifiche.

NOTA: Facendo clic su **Annulla** non è possibile ripristinare le modifiche salvate facendo clic su **Applica**.

Configurazione del modulo Sicurezza

Per proteggere da modifiche non autorizzate le impostazioni scelte per i singoli moduli VShield è possibile assegnare una password alle pagine di proprietà desiderate o a tutte le pagine. Gli amministratori di sistemi possono usare questa funzione insieme alla capacità di VShield di salvare le proprie impostazioni in un file .VSH per ripetere le proprie opzioni di configurazione in tutti i computer client della rete. Impedire la disattivazione di VShield (vedere Passaggio 4 a pagina 96 per i dettagli) e proteggere questa impostazione con una password, è un modo facile ed efficace per rinforzare una stretta politica di sicurezza antivirus per tutti gli utenti della rete.

Usare il modulo Sicurezza per assegnare una password e scegliere quali pagine proteggere.

Attivazione della protezione tramite password

VShield non attiva il modulo Sicurezza per impostazione predefinita, in quanto è necessario che venga specificata la password con cui proteggere le impostazioni.

Per attivare e configurare la protezione tramite password di VShield, procedere come segue:

1. Selezionare la casella di controllo **Attiva protezione tramite password**.

   Vengono attivate le altre opzioni presenti nella pagina delle proprietà (Figura 4-35).

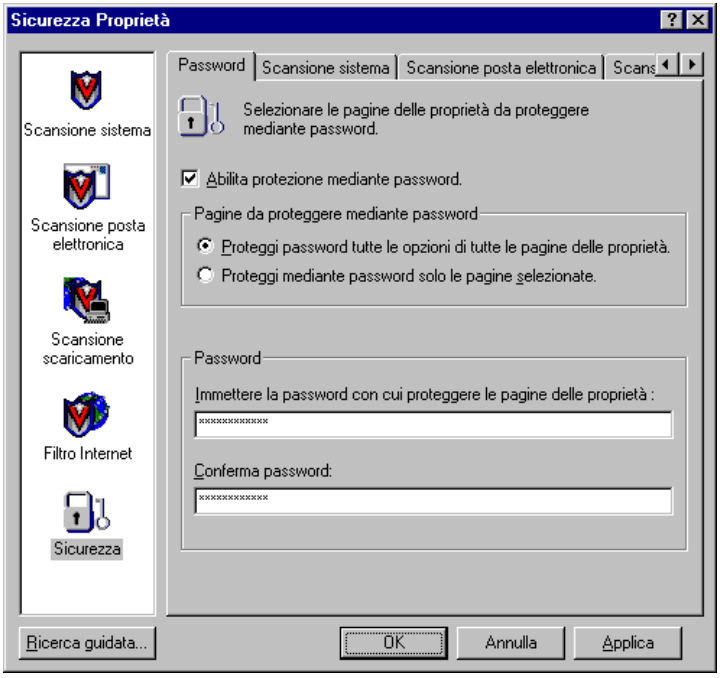

Figura 4-35. La finestra di dialogo Proprietà Sicurezza - Pagina Password

2. Scegliere se si desidera proteggere le pagine delle proprietà di tutti i moduli VShield o solo determinate pagine. Le scelte disponibili sono:

   - **Protezione password di tutte le opzioni in tutte le pagine delle proprietà.** Selezionare questo pulsante per proteggere tutte le impostazioni con una sola operazione.

- **Protezione password delle pagine di proprietà selezionate.** Selezionare questo pulsante per scegliere quali pagine di proprietà proteggere nei singoli moduli. Le altre schede della finestra di dialogo Proprietà Sicurezza permettono di indicare singole pagine.

3. Immettere la password con cui proteggere le impostazioni. Digitare una qualsiasi combinazione di 20 caratteri al massimo nella casella di testo superiore dell'area **Password** quindi immettere esattamente la stessa combinazione nella casella di testo sottostante per confermare la password scelta.

IMPORTANTE: La protezione tramite password di VShield è diversa dalla protezione tramite password che può essere assegnata a VirusScan. Scegliendo una password per un componente, questa non viene assegnata anche agli altri ma è necessario immettere una password per ogni componente da proteggere.

---

4. Fare clic su una qualsiasi altra scheda del modulo Sicurezza per proteggere le singole pagine delle proprietà. Per salvare la password immessa senza chiudere la finestra di dialogo Proprietà Sicurezza fare clic su **Applica**. Se era stata effettuata la scelta di proteggere tutte le pagine di proprietà in tutti i moduli e si desidera chiudere la finestra di dialogo, fare clic su **OK**. Per chiudere la finestra di dialogo senza salvare alcuna modifica fare clic su **Annulla**.

NOTA: Facendo clic su **Annulla** non è possibile ripristinare le modifiche salvate facendo clic su **Applica**.

Quando le impostazioni sono state protette con una password, VShield richiederà di immettere la password assegnata ogni qualvolta si aprirà la finestra di dialogo Proprietà VShield (Figura 4-36).

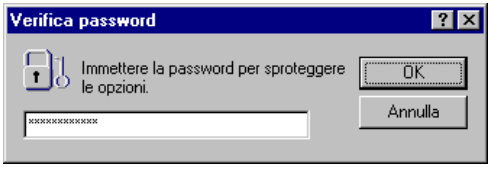

Figura 4-36. La finestra di dialogo Verifica password

Immettere la password scelta nell'apposita casella di testo, quindi fare clic su **OK** per accedere alla finestra di dialogo Proprietà VShield.

Protezione delle singole pagine di proprietà

Se era stata scelta l'opzione **Protezione password delle pagine di proprietà selezionate, nella pagina Password** del modulo Sicurezza, è possibile scegliere quale opzione di configurazione proteggere.

Procedere come segue:

1. Fare clic sulla scheda del *modulo* di cui proteggere le impostazioni. Se la scheda desiderata non è visibile, fare clic su ◄ o ► per portarle in superficie. Un esempio di pagine è riportato in Figura 4-37.

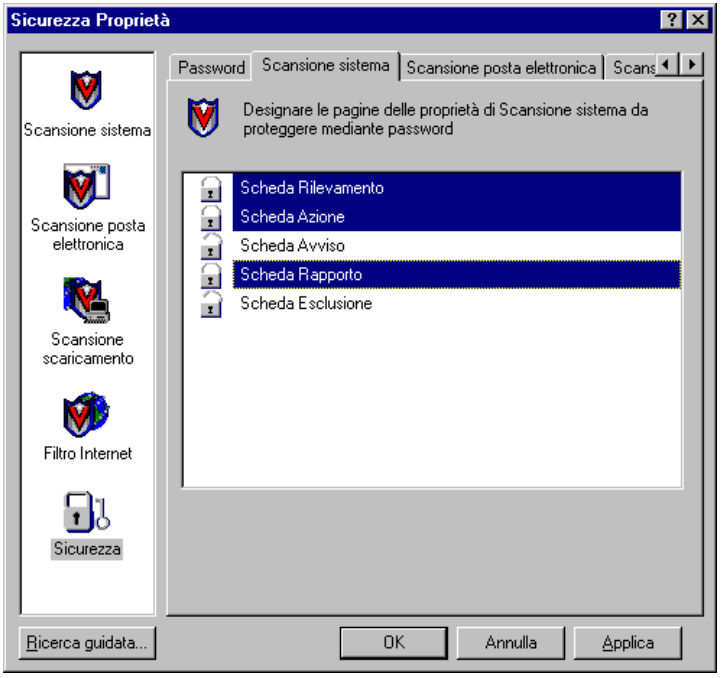

Figura 4-37. Opzioni di sicurezza Scansione sistema

2. Dall'elenco visualizzato, selezionare le impostazioni che si desidera proteggere.

   È possibile proteggere le pagine di proprietà desiderate o tutte le pagine del modulo. Le pagine di proprietà protette mostrano l'icona di un lucchetto chiuso nell'elenco di sicurezza rappresentato in Figura 4-37. Per rimuovere la protezione da una pagina di proprietà, fare clic sull'icona del lucchetto chiuso al fine di aprirlo.

3. Selezionare tutte le pagine di proprietà che si desidera proteggere in ogni modulo.

4. Per salvare la password immessa senza chiudere la finestra di dialogo Proprietà Sicurezza fare clic su **Applica**. Per salvare le modifiche e chiudere la finestra di dialogo, fare clic su **OK**. Per chiudere la finestra di dialogo senza salvare alcuna modifica fare clic su **Annulla**.

> **NOTA:** Facendo clic su **Annulla** non è possibile ripristinare le modifiche salvate facendo clic su **Applica**.

Uso del menu di scelta rapida di VShield

VShield raggruppa molti dei comandi più comuni in un menu di scelta rapida associato alla sua icona del system tray. Fare doppio clic su questa icona per visualizzare la finestra di dialogo Stato di VShield. Fare clic sull'icona con il pulsante destro del mouse per visualizzare i seguenti comandi:

- **Stato.** Scegliere questa opzione per aprire la finestra di dialogo Stato di VShield.
- **Proprietà.** Puntare su questa opzione quindi scegliere uno dei moduli di VShield che compaiono nel sottomenu per aprire la finestra di dialogo Proprietà VShield alla pagina delle proprietà del modulo scelto.
- **Attiva.** Puntare su questa opzione quindi scegliere uno dei moduli di VShield che compaiono nel sottomenu per attivarlo o disattivarlo. I moduli che nel menu sono contrassegnati da un segno di spunta sono attivi, gli altri sono inattivi.
- **Informazioni.** Scegliere questa opzione per visualizzare il numero di versione e il numero di serie di VShield, il numero di versione e la data di creazione dei file .DAT in uso al momento e una nota di copyright di Network Associates.
- **Esci.** Scegliere questa opzione per interrompere le scansioni di tutti i moduli VShield e scaricare VShield dalla memoria.

Disattivare o terminare VShield

Una volta avviato VShield compare una piccola icona del programma nel system tray di Windows. *Disattivando* VShield il programma continua a eseguirsi in memoria, ma smette di eseguire ogni scansione. Quando si disattivano tutti i suoi moduli, VShield lascia l'icona "annullato" nel system tray di Windows ed è possibile usarla per attivare di nuovo il programma.

Terminando VShield il programma viene completamente rimosso dalla memoria e scompare anche l'icona dal system tray di Windows. Per riattivare il programma a questo punto, è necessario aprire la finestra di dialogo Proprietà VShield e attivare di nuovo ogni modulo singolarmente (vedere "Impostazione delle proprietà di VShield" a pagina 90 per i dettagli) oppure avviarlo nuovamente dal Pianificatore VirusScan.

È possibile disattivare o terminare VShield in quattro modi diversi:

- **Dal menu di scelta rapida di VShield.** Fare clic con il pulsante destro del mouse sull'icona di VShield nel system tray di Windows per visualizzare il relativo menu di scelta rapida, quindi scegliere **Esci**.

  VShield si interrompe immediatamente, viene scaricato dalla memoria e rimuove la propria icona dal system tray di Windows.

  Per disattivare i singoli moduli di VShield, fare clic con il pulsante destro del mouse sull'icona di VShield, puntare su **Attiva**, quindi scegliere i singoli moduli uno a uno. I moduli che nel menu sono contrassegnati da un segno di spunta sono attivi, gli altri sono inattivi.

  > **NOTA:** Vedere "Uso del menu di scelta rapida di VShield" a pagina 146 Per ulteriori informazioni sulle altre opzioni disponibili nel menu.

- **Dalla finestra di dialogo Stato di VShield.** Fare doppio clic sull'icona di VShield nel system tray di Windows per visualizzare la finestra di dialogo Stato di VShield (Figura 4-38).

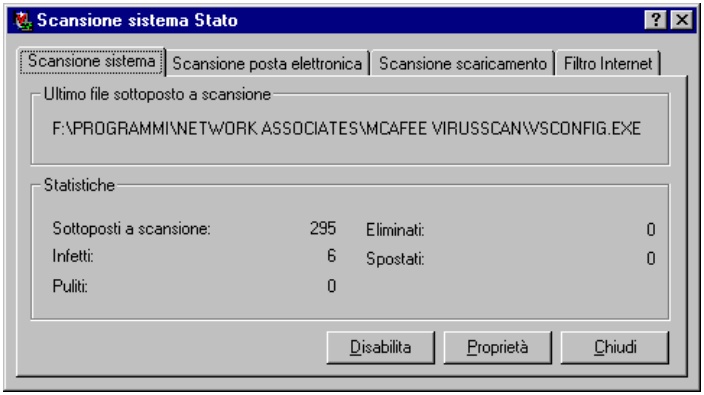

Figura 4-38. La finestra di dialogo Stato di VShield

Per ogni modulo che si desidera disattivare fare clic sulla scheda corrispondente, quindi fare clic su **Disattiva**. VShield disattiva immediatamente il modulo. Quando tutti i moduli sono stati disattivati, VShield mostra nel system tray di Windows. Per attivare di nuovo ogni singolo modulo, aprire la finestra di dialogo Stato, quindi fare clic su **Attiva** nelle singole pagine delle proprietà.

- **Dalla finestra di dialogo Proprietà VShield.** Fare clic sull'icona di VShield con il pulsante destro del mouse nel system tray di Windows, puntare su **Proprietà**, quindi scegliere **Scansione sistema** dal menu di scelta rapida che appare per visualizzare la finestra di dialogo Proprietà VShield (Figura 4-39).

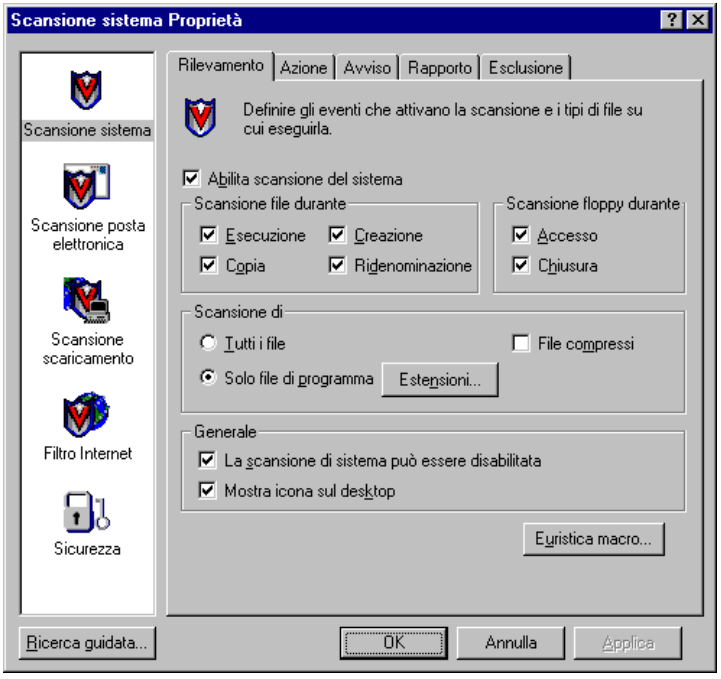

Figura 4-39. La finestra di dialogo Proprietà VShield

Per ogni modulo che si desidera disattivare fare clic sulla corrispondente icona sul lato sinistro della finestra di dialogo, quindi fare clic sulla scheda Rilevamento. Quindi deselezionare la casella di controllo **Attiva** nella parte superiore di ogni pagina. Con questa operazione VShield disattiva il modulo. Quando tutti i moduli vengono disattivati, VShield mostra l'icona nel system tray di Windows, se non è stata disattivata la casella di controllo **Visualizza icona sul desktop**.

Per attivare di nuovo ogni singolo modulo, aprire la finestra di dialogo Proprietà VShield quindi selezionare la casella di controllo **Attiva** nella pagina Rilevamento di ogni modulo.

- **Dal Pianificatore VirusScan.** Fare clic su **Avvio** nella barra delle attività di Windows, puntare su **Programmi**, quindi su **McAfee VirusScan**. Poi scegliere **Pianificatore McAfee VirusScan** per aprire la finestra del Pianificatore (Figura 4-40).

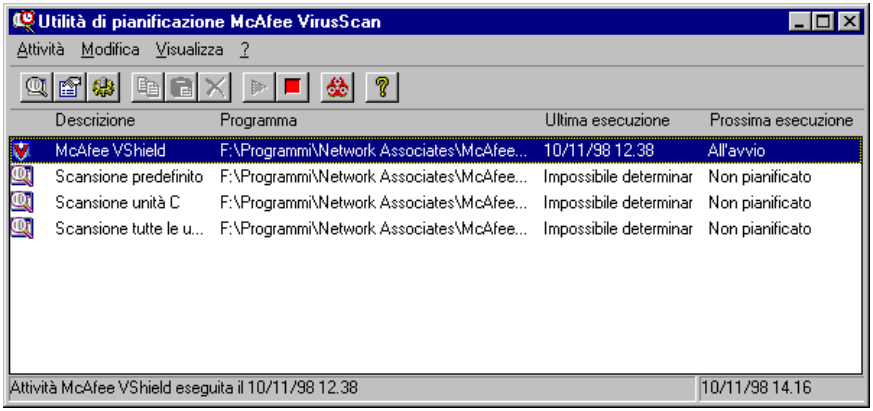

Figura 4-40. La finestra Pianificatore VirusScan

Selezionare **McAfee VShield** nell'elenco, quindi scegliere **Disattiva** nel menu **Attività**. VShield disattiva tutti i moduli VShield e visualizza l'icona nel system tray di Windows. Per avviare di nuovo VShield, selezionare l'attività VShield, quindi scegliere **Attiva** nel menu **Attività**.

Per terminare completamente VShield, selezionare **McAfee VShield** nell'elenco delle attività, quindi fare clic su nella barra degli strumenti Pianificatore. VShield si interrompe immediatamente, viene scaricato dalla memoria e rimuove la propria icona dal system tray di Windows. Per attivare di nuovo il programma, selezionare l'attività VShield, quindi fare clic su .

Registrazione delle informazioni di stato di VShield

Una volta attivato e configurato, VShield opera costantemente in background, analizzando e scandendo la posta elettronica ricevuta, i file eseguiti o scaricati o gli oggetti Java e ActiveX incontrati.

Per vedere un riepilogo dello stato di avanzamento:

1. Aprire una finestra di dialogo Stato di VShield. È possibile farlo in due modi diversi:

   - Fare doppio clic sull'icona del system tray di VShield; per aprire la finestra di dialogo Stato mostrata in Figura 4-38 a pagina 147; oppure
   - Aprire il Pianificatore VirusScan, selezionare l'attività VShield nell'elenco delle attività, quindi fare clic sulla barra degli strumenti Pianificatore per visualizzare la finestra di dialogo Proprietà dell'attività mostrata in Figura 4-41.

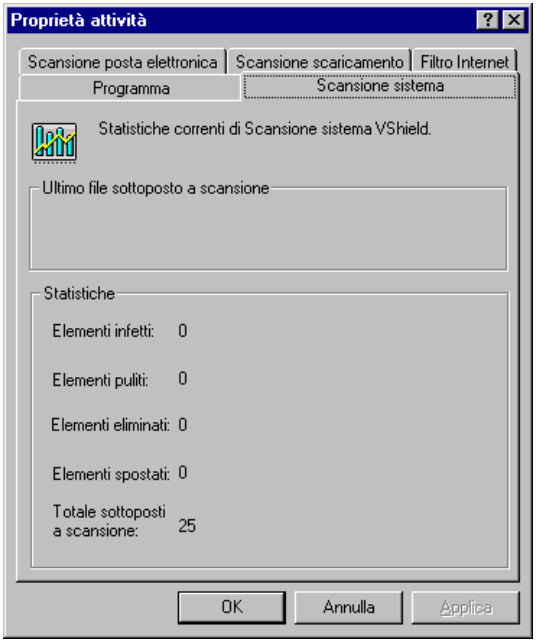

Figura 4-41. Finestra di dialogo Proprietà dell'attività di VShield

2. Fare clic sulla scheda corrispondente al programma che si desidera attivare o disattivare o di cui si desidera controllare i progressi.

   Per il modulo Scansione sistema VShield riporta il numero dei file scanditi, il numero dei file infetti rilevati e il numero dei file puliti, spostati ed eliminati. Per i moduli Scansione posta e Scansione scaricamento, rileva il numero dei file scanditi, il numero di infezioni rilevate e il numero dei file spostati o eliminati. Per gli applet Java e ActiveX o per i siti Internet, VShield riporta il numero di elementi scanditi e il numero di nuovi elementi classificati come “proibiti” o a cui è stato impedito l’accesso.

   Se sono attivate le funzioni di reporting del programma, VShield annota le stesse informazioni anche nei file di registro dei singoli moduli.

Se per aprire una finestra di dialogo Stato si sceglie il primo metodo descritto in Passaggio 1 a pagina 150, è anche possibile attivare o disattivare VShield oppure aprire la finestra di dialogo Proprietà VShield. È possibile:

- Fare clic sulla scheda che corrisponde al componente del programma da attivare o disattivare, quindi fare clic su **Attiva** per avviare il componente del programma. Fare clic su **Disattiva** per disattivarlo. Vedere "Disattivare o terminare VShield" a pagina 146 per apprendere altri metodi per disattivare o attivare VShield.
- Fare clic su **Proprietà** per aprire la finestra di dialogo Proprietà VShield in cui impostare le opzioni che indicano a VShield come eseguire ogni tipo di scansione. Vedere "Impostazione delle proprietà di VShield" a pagina 90 per sapere come scegliere le opzioni di configurazione nella finestra di dialogo Proprietà VShield.

Uso di McAfee VirusScan 5

Cos'è VirusScan

Il nome VirusScan si riferisce sia all'intera serie dei componenti del programma antivirus del desktop descritti in questo *Manuale dell'utente*, sia a un particolare componente della serie: SCAN32.EXE o scanner "su richiesta" di VirusScan. La definizione "Su richiesta" significa che l'utente controlla l'inizio e la fine di un'operazione di scansione di VirusScan, gli obiettivi esaminati, le operazioni eseguite quando viene rilevato un virus o altri aspetti del funzionamento del programma. Gli altri componenti di VirusScan, invece, si attivano automaticamente o seguendo una pianificazione impostata dall'utente. In origine, VirusScan era costituito unicamente da uno scanner su richiesta — le caratteristiche integrate nel programma forniscono attualmente un cluster di funzioni antivirus che consente la massima protezione dalle infezioni da virus e dagli attacchi di software dannosi.

Il componente su richiesta di VirusScan funziona in due modalità: l'interfaccia VirusScan "Classico" consente di utilizzare immediatamente il programma, impostando un numero minimo di opzioni di configurazione e avendo, tuttavia, la possibilità di sfruttare al massimo il motore di scansione e rilevamento virus di VirusScan; la modalità avanzata di VirusScan aggiunge flessibilità alle opzioni di configurazione del programma, tra le quali la possibilità di eseguire contemporaneamente più operazioni di scansione.

Questo capitolo descrive come utilizzare VirusScan nelle modalità Classica e Avanzata.

Finalità delle operazioni di scansione su richiesta

Poiché il componente VShield fornisce la funzione di scansione in background, l'uso di VirusScan per eseguire la scansione del sistema potrebbe sembrare ridondante. Tuttavia, misure di sicurezza antivirus efficaci includono scansioni del sistema approfondite e regolari in quanto:

- **La scansione in background controlla i file nel momento in cui vengono eseguiti.** VShield ricerca il codice del virus quando si avviano i file eseguibili o durante la lettura dei dischetti, ma VirusScan può verificare le strutture dei codici nei file memorizzati sul disco rigido. Se un file infetto viene eseguito raramente, può succedere che VShield non rilevi il virus fino a quando non utilizza il carico utile. VirusScan, tuttavia, è in grado di rilevare la presenza di un virus in attesa di essere eseguito.

- **I virus sono nascosti.** Se accidentalmente viene lasciato un dischetto nell'unità all'avvio del computer, è possibile che un virus venga caricato in memoria prima di caricare VShield. Questa eventualità può presentarsi in particolare se VShield non è configurato per sottoporre a scansione i dischetti. Una volta in memoria, un virus può infettare quasi tutti i programmi, incluso VShield.
- **La scansione con VShield richiede tempo e risorse.** La scansione per la ricerca dei virus durante le operazioni di esecuzione, copia o salvataggio di file può ritardare leggermente i tempi di avvio del software e altre operazioni. A seconda della situazione, questo tempo prezioso potrebbe essere impiegato in modo più utile. Nonostante l'impatto sia molto leggero, si può essere tentati e disabilitare VShield per impiegare ogni bit disponibile per operazioni particolarmente impegnative. In tal caso, l'esecuzione delle regolari operazioni di scansione durante i periodi di inattività può salvaguardare il sistema da infezioni senza comprometterne le prestazioni.
- **Un livello di sicurezza ridondante è un buon livello di sicurezza.** Nel mondo delle reti e del Web, in cui opera la maggior parte degli utenti, è possibile scaricare un virus in pochi secondi, senza rendersi neanche conto della sua provenienza. Se un conflitto software disabilita la scansione in background oppure se la scansione in background non è configurata per il controllo di un punto di ingresso vulnerabile, un virus può entrare nel sistema. Le regolari operazioni di scansione possono spesso rilevare infezioni prima che queste si diffondano o danneggino il sistema.

VirusScan in modalità Classica presenta una singola operazione di scansione predefinita, preconfigurata e pronta all'esecuzione. È possibile avviare questa operazione di scansione per rilevare virus sull'unità C: oppure configurare ed eseguire le operazioni di scansione secondo le proprie necessità. Anche VirusScan in modalità Avanzata presenta una singola operazione di scansione preconfigurata, che sottopone a scansione tutti i dischi rigidi locali.

Avvio di VirusScan

Per avviare VirusScan,

- Fare clic su **Avvio** sulla barra delle applicazioni di Windows, scegliere **Programmi**, quindi **McAfee VirusScan**. Selezionare quindi **McAfee VirusScan** dall'elenco visualizzato; oppure
- Fare clic su **Avvio**, quindi selezionare **Esegui** dal menu visualizzato. Digitare SCAN32.EXE nella finestra di dialogo Esegui, quindi fare clic su **OK**.

Entrambi i metodi consentono di aprire la finestra di VirusScan in modalità Classica (Figura 5-1).

Figura 5-1. La finestra VirusScan in modalità Classica

Fare clic su **Avvia scansione** nel lato destro della finestra per avviare subito l'attività di scansione predefinita oppure configurare, secondo le proprie necessità, un'attività di scansione selezionando le schede nella parte superiore della finestra e attivando le opzioni in ciascuna pagina delle proprietà.

Uso dei menu di VirusScan

I menu presenti nella parte superiore della finestra di VirusScan consentono di modificare alcune caratteristiche delle operazioni del programma. È possibile:

- **Salvare o ripristinare le impostazioni predefinite.** In base alle impostazioni predefinite, VirusScan in modalità Classica ricerca i virus nei file maggiormente esposti al rischio di infezioni. Analizza le aree della memoria e del sistema, esamina l'unità C: e tutte le sottocartelle di tale unità, quindi emette un segnale acustico di avviso e richiede all'utente di scegliere una risposta se rileva la presenza di un virus. Il programma inoltre registra le proprie azioni e riepiloga le impostazioni correnti in un file di registro che l'utente può visualizzare in seguito.

  Se si modificano le impostazioni e si desidera salvare come predefinite le modifiche apportate, selezionare **Salva come predefinite** dal menu **File**, oppure selezionare il pulsante **Nuova scansione** sul lato destro della finestra di VirusScan in modalità Classica. VirusScan richiederà all'utente la conferma per sostituire il file che registra le impostazioni predefinite. Fare clic su **Sovrascrivi** oppure su **OK** per continuare. VirusScan registrerà le opzioni impostate e le utilizzerà per tutte le operazioni di scansione eseguite successivamente.

NOTA: Se si sono modificate le impostazioni predefinite, ma l'utente desidera ripristinare le impostazioni originali, utilizzare Gestione risorse per individuare ed eliminare il file DEFAULT.VSC nella directory del programma VirusScan. Quando si riavvia VirusScan, le impostazioni predefinite verranno ripristinate e salvate nel nuovo file DEFAULT.VSC. Per ottenere maggiori informazioni sul formato .VSC del file, consultare Appendice C, "Comprensione del formato di file .VSC".

- **Salvare le nuove impostazioni.** Se sono necessarie configurazioni diverse di VirusScan per eseguire varie operazioni di scansione o se si desidera eseguire un'operazione di scansione con la stessa configurazione su più computer, è possibile salvare le opzioni di configurazione personalizzate in un file formato .VSC con un nome specifico. Un file formato .VSC è un file di testo che registra le opzioni di configurazione di VirusScan, proprio come i file .INI di Windows registrano le opzioni di avvio del programma.

  Per salvare le impostazioni personalizzate, configurare innanzitutto VirusScan con le opzioni desiderate, quindi scegliere **Salva impostazioni** dal menu **File**. Digitare un nome descrittivo nella finestra di dialogo Salva impostazioni scansione con nome, scegliere un'ubicazione sul disco rigido per il file, quindi fare clic su **Salva**. È possibile copiare questo file su un altro computer perché utilizzi le stesse impostazioni. Vedere "Configurazione di VirusScan in modalità Classica" a pagina 158 oppure "Configurazione di VirusScan in modalità Avanzata" a pagina 165 per ulteriori dettagli.

  Per eseguire VirusScan con queste impostazioni, è sufficiente individuare il file .VSC salvato, selezionarlo e fare doppio clic. Questa procedura avvia VirusScan con le impostazioni caricate.

- **Aprire il registro attività di VirusScan.** Scegliere **Visualizza registro attività** dal menu **File** per aprire il file di registro utilizzato da VirusScan per registrare le azioni e le impostazioni.

  Il file di registro verrà aperto in una finestra del Blocco appunti (Figura 5-2 a pagina 157). È possibile stampare, modificare e copiare questo file, trattandolo come un comune file di testo. Per ulteriori informazioni sui record del file di registro, consultare "Selezione delle opzioni di Rapporto" a pagina 176.

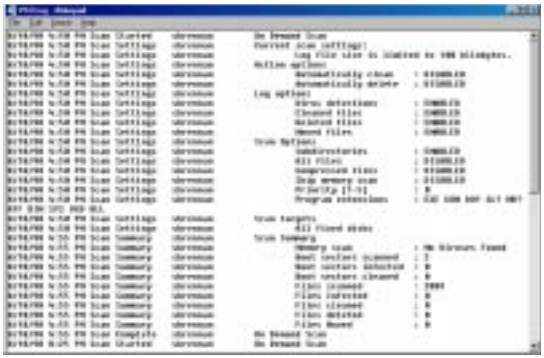

Figura 5-2. Registro attività di VirusScan

- **Uscire da VirusScan.** Selezionare **Chiudi** dal menu **File** per uscire da VirusScan. L'uscita da VirusScan determina l'arresto di qualsiasi operazione di scansione attiva, ma *non* influenza le operazioni di VShield che proseguono in background. Se non vengono salvate, le opzioni di configurazione selezionate non vengono conservate dopo l'uscita da VirusScan.
- **Modifica delle modalità di VirusScan.** Selezionare **Avanzata** dal menu **Strumenti** per passare dalla modalità VirusScan Classica ad Avanzata. Per passare dalla modalità Avanzata alla modalità Classica, scegliere **Classica** dal menu **Strumenti**.
- **Attivazione della protezione tramite password.** Scegliere **Protetto da password** dal menu **Strumenti** per aprire una finestra di dialogo nella quale scegliere le opzioni di configurazione di VirusScan che si desidera bloccare per prevenire modifiche non autorizzate. Vedere "Attivazione della protezione tramite password" a pagina 181 per ulteriori dettagli.
- **Avvio dell'utilità di pianificazione di VirusScan.** Scegliere **Utilità di pianificazione** dal menu **Strumenti** per aprire l'utilità di pianificazione VirusScan, un'utilità che consente di configurare ed eseguire operazioni di scansione non assistite. Per ulteriori informazioni sull'utilizzo dell'utilità di pianificazione, consultare "Pianificazione delle attività di scansione" a pagina 183.

- **Aprire il file della guida in linea.** Scegliere **Guida in linea** dal menu **?** per visualizzare un elenco degli argomenti della guida di VirusScan. Per visualizzare una descrizione sensibile al contesto di pulsanti, elenchi e di altre voci nella finestra di VirusScan, scegliere **Guida rapida** dal menu **?**, quindi selezionare una voce con il pulsante sinistro del mouse dopo che il cursore del mouse viene modificato in . È possibile visualizzare gli stessi argomenti della guida facendo clic con il tasto destro su un elemento nella finestra di VirusScan, quindi scegliendo **Guida rapida** nel menu visualizzato.

Configurazione di VirusScan in modalità Classica

Per eseguire un'operazione di scansione, è necessario specificare a VirusScan cosa sottoporre a scansione, cosa fare in caso di rilevamento di virus e in che modo comunicare all'utente il rilevamento di virus. Inoltre, l'utente può impostare VirusScan in modo che tenga traccia delle azioni eseguite. Una serie di pagine delle proprietà controlla le opzioni relative a ciascuna operazione: fare clic su una delle schede nella finestra di VirusScan in modalità Classica per impostare VirusScan per l'attività desiderata.

Scelta delle opzioni Percorso e tipo di file

VirusScan inizialmente presume che l'utente desideri sottoporre a scansione l'unità C: e tutte le sottocartelle e limita la scansione solo ai file maggiormente esposti all'infezione (Figura 5-3).

Figura 5-3. Finestra VirusScan in modalità Classica - pagina Percorso e tipo di file

Per modificare queste opzioni, attenersi alla seguente procedura:

1. Scegliere un volume o una cartella nel sistema o nella rete che si desidera sottoporre a scansione per la ricerca di virus con VirusScan.

   È possibile digitare un percorso per il volume o la cartella da sottoporre a scansione nella casella di testo **Ricerca in** oppure fare clic su **Sfoglia** per aprire la finestra di dialogo Sfoglia per cartelle (Figura 5-4).

Figura 5-4. Finestra di dialogo Sfoglia per cartelle

   Fare clic su ⊞ per visualizzare l'intero elenco di voci visualizzato nella finestra di dialogo. Fare clic su ⊟ per ridurre una voce. È possibile selezionare i dischi rigidi, le cartelle o i file come obiettivi di scansione, sia sul sistema sia su altri computer della rete. Non è possibile selezionare Risorse del computer, Risorse di rete o più volumi come obiettivi di scansione da VirusScan in modalità Classica: per scegliere questi oggetti come obiettivi di scansione, è necessario utilizzare VirusScan in modalità Avanzata.

   Una volta selezionato l'obiettivo di scansione, fare clic su **OK** per ritornare alla finestra di VirusScan in modalità Classica.

2. Selezionare la casella di controllo **Includi sottocartelle** per consentire a VirusScan di cercare i virus in tutte le cartelle contenute nell'obiettivo di scansione.

3. Specificare il tipo di file che VirusScan deve sottoporre a scansione. È possibile

- **Eseguire la scansione di file compressi.** Selezionare la casella di controllo **File compressi** per consentire a VirusScan di cercare i virus nei file compressi con i seguenti formati: .??_, .CAB, LZEXE, LZH, PKLite, .TD0, e .ZIP. Nonostante garantisca una maggiore protezione, la scansione di file compressi dilata i tempi necessari a tale operazione.

- **Scegliere il tipo di file da sottoporre a scansione.** Normalmente i virus non sono in grado di attaccare i file di dati o i file che non contengono un codice eseguibile. Per questa ragione è possibile limitare le operazioni di scansione solo ai file maggiormente esposti alle infezioni dei virus, in modo da velocizzare le operazioni di scansione. A tal fine, selezionare il pulsante **Solo file di programma**. Per visualizzare o indicare le estensioni dei nomi di file che saranno analizzati da VirusScan, fare clic su **Estensioni** per aprire la finestra di dialogo Estensioni file di programma (Figura 5-5).

Figura 5-5. Finestra di dialogo Estensioni file di programma

Secondo le impostazioni predefinite, VirusScan cerca i virus nei file con le estensioni .EXE, .COM, .DO?, .XL?, .MD?, .VXD, .SYS, .BIN, .RTF, .OBD e .DLL. I file con estensione .DO?, .XL?, .RTF, .MD?, e .OBD sono file di Microsoft Office. Tutti questi file possono essere infettati da virus macro. Il ? è un carattere jolly che abilita la scansione di file di documento e di modello da parte di VirusScan.

  – Per aggiungere estensioni all'elenco, fare clic su **Aggiungi**, quindi digitare le estensioni dei file che si desidera VirusScan sottoponga a scansione nella finestra di dialogo visualizzata.

  – Per eliminare un'estensione dall'elenco, selezionarla, quindi fare clic su **Rimuovi**.

  – Fare clic su **Predefinite** per ripristinare l'elenco nella sua forma originaria.

Al termine, scegliere **OK** per chiudere la finestra di dialogo.

Per far sì che VirusScan esamini tutti i file sul sistema, indipendentemente dall'estensione, selezionare il pulsante **Tutti i file**. Questa operazione rallenta notevolmente il sistema, ma garantisce la completa eliminazione dei virus.

4. Fare clic sulla scheda Azione per scegliere le opzioni aggiuntive di VirusScan.

   Per avviare immediatamente un'operazione di scansione con le opzioni appena selezionate, fare clic su **Avvia scansione**. Per salvare le modifiche come opzioni di scansione predefinite, selezionare **Salva come predefinite** dal menu **File** oppure fare clic su **Nuova scansione**. Per salvare le impostazioni in un nuovo file, scegliere **Salva impostazioni** dal menu **File**, attribuire un nome al file nella finestra di dialogo visualizzata, quindi scegliere **Salva**.

Scelta delle opzioni Azione

Quando VirusScan rileva un virus può chiedere all'utente quale operazione eseguire sul virus infetto, oppure può eseguire automaticamente un'azione precedentemente impostata. Utilizzare la pagina proprietà Azione per specificare le opzioni di risposta o le azioni che si desidera VirusScan esegua quando rileva un virus.

Procedere come segue:

1. Fare clic sulla scheda Azione nella finestra di VirusScan in modalità Classica per visualizzare la pagina delle proprietà appropriata (Figura 5-6).

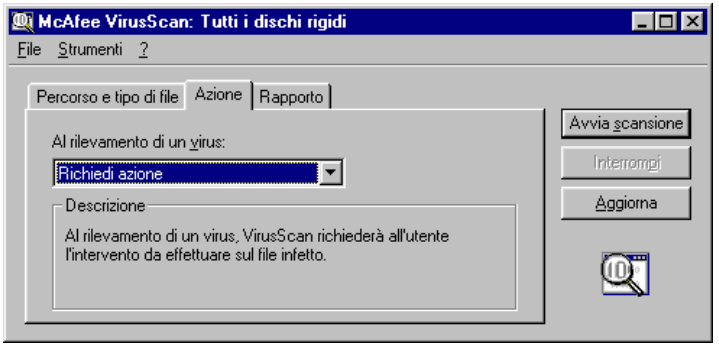

Figura 5-6. Finestra VirusScan in modalità Classica - pagina Azione

2. Selezionare una risposta dall'elenco **Al rilevamento di un virus**. L'area immediatamente al di sotto dell'elenco cambia per visualizzare opzioni aggiuntive per ciascuna risposta. Le scelte disponibili sono:

   - **Richiedi azione.** Scegliere questa risposta se si prevede di assistere all'operazione di scansione eseguita da VirusScan: VirusScan visualizza un messaggio di avviso quando rileva la presenza di un virus e consente all'utente di utilizzare l'ampia gamma di risposte disponibili.
   - **Sposta file infetti automaticamente**. Scegliere questa risposta per consentire a VirusScan di spostare i file infetti eventualmente rilevati in una directory di quarantena. In base alle impostazioni predefinite, VirusScan sposta questi file in una cartella denominata INFECTED (infetti), creata al livello principale dell'unità in cui viene rilevata la presenza del virus. Ad esempio, se VirusScan rileva un file infetto in T:\MY DOCUMENTS e si è specificato INFECTED come directory di quarantena, VirusScan copierà il file in T:\INFECTED.

     È possibile immettere un nome diverso nella casella di testo fornita, o fare clic su **Sfoglia** per individuare una cartella adeguata sul disco rigido.
   - **Pulisci automaticamente i file infetti.** Scegliere questa risposta per indicare a VirusScan di rimuovere il codice del virus dal file infetto appena ne rileva la presenza. Se VirusScan non è in grado di eliminare il virus, prenderà nota del virus rilevato nel file di registro. Per ulteriori dettagli, vedere "Selezione delle opzioni di Rapporto" a pagina 176.
   - **Elimina automaticamente i file infetti.** Utilizzare questa opzione per indicare a VirusScan di eliminare immediatamente i file infetti rilevati. Attivare la funzione di notifica in modo da registrare i file eliminati da VirusScan. Sarà necessario ripristinare i file eliminati da copie di backup. Se VirusScan non è in grado di eliminare un file infetto, prenderà nota del virus nel file di registro.

- **Continua scansione.** Utilizzare questa opzione solo se si prevede di non assistere alle operazioni di scansione di VirusScan. Se viene attivata anche la funzione di notifica di VirusScan (vedere "Selezione delle opzioni di Rapporto" a pagina 176 per i dettagli), il programma registra il nome dei virus rilevati e il nome dei file infetti in modo tale che sia possibile eliminarli alla prima occasione.

3. Fare clic sulla scheda Rapporto per scegliere le opzioni aggiuntive di VirusScan.

   Per avviare immediatamente un'operazione di scansione con le opzioni appena selezionate, fare clic su **Avvia scansione**. Per salvare le modifiche come opzioni di scansione predefinite, selezionare **Salva come predefinite** dal menu **File** oppure fare clic su **Nuova scansione**. Per salvare le impostazioni in un nuovo file, scegliere **Salva impostazioni** nel menu **File**, attribuire un nome al file nella finestra di dialogo visualizzata, quindi scegliere **Salva**.

Selezione delle opzioni di Rapporto

In base alle impostazioni predefinite, VirusScan emette una segnalazione acustica quando rileva la presenza di un virus. È possibile utilizzare la pagina Rapporto per attivare o disattivare questo avviso o per aggiungere un messaggio di avviso alla finestra di dialogo Virus rilevato visualizzata quando VirusScan rileva un file infetto. Questo messaggio di avviso può contenere qualsiasi tipo di informazione, da un semplice avviso alle istruzioni sulle modalità di notifica del virus all'amministratore di rete.

Questa pagina determina inoltre le dimensioni e la posizione del file di registro di VirusScan. In base alle impostazioni predefinite, il programma elenca le impostazioni correnti e riassume tutte le azioni che esegue durante le operazioni di scansione in un file di registro denominato VSCLOG.TXT. È possibile fare in modo che VirusScan registri i virus in questo file o utilizzare un editor di testi per creare un file di testo da utilizzare con VirusScan. Quindi è possibile aprire e stampare il file di registro per visionarlo successivamente da VirusScan o da un editor di testo.

Per scegliere le opzioni di avviso e registro di VirusScan, procedere come segue:

1. Fare clic sulla scheda Rapporto nella finestra di VirusScan in modalità Classica per visualizzare la pagina delle proprietà corretta (Figura 5-7).

Figura 5-7. Finestra VirusScan in modalità Classica - pagina Rapporto

2. Scegliere i metodi di avviso che si desidera siano utilizzati da VirusScan quando viene rilevata la presenza di un virus. Con VirusScan è possibile:

   - **Visualizzare un messaggio personalizzato.** Selezionare la casella di controllo **Messaggio**, quindi specificare il messaggio che si desidera visualizzare nell'apposita casella di testo. È possibile immettere un messaggio di massimo 225 caratteri.

     NOTA: Per indicare a VirusScan di visualizzare i messaggi, è necessario selezionare **Richiedi azione** come risposta nella pagina Azione (per ulteriori dettagli, vedere "Scelta delle opzioni Azione" a pagina 171).

   - **Segnale acustico.** Selezionare la casella di controllo **Segnale acustico**.

3. Selezionare la casella di controllo **Registra su file**.

   In base alle impostazioni predefinite, VirusScan scrive le informazioni di registro nel file VSCLOG.TXT nella directory di programma di VirusScan. È possibile immettere un altro nome e percorso nell'apposita casella di testo o fare clic su **Sfoglia** per localizzare un file adatto in qualsiasi altra posizione del disco o della rete.

4. Per ridurre al minimo le dimensioni del file di registro, selezionare la casella di controllo **Limita dimensioni del file di registro a**, quindi immettere un valore per le dimensioni del file, in kilobyte, nella relativa casella di testo.

   Immettere un valore compreso tra 10KB e 999KB. In base alle impostazioni predefinite, VirusScan limita la dimensione del file a 100KB. Se i dati nel file di registro superano le dimensioni del file impostate, VirusScan cancella la registrazione esistente e ricomincia dal punto in cui ha smesso.

5. Fare clic su una scheda diversa per modificare alcune impostazioni di VirusScan.

   Per avviare immediatamente un'operazione di scansione con le opzioni appena selezionate, fare clic su **Avvia scansione**. Per salvare le modifiche come opzioni di scansione predefinite, selezionare **Salva come predefinite** dal menu **File** oppure fare clic su **Nuova scansione**. Per salvare le impostazioni in un nuovo file, scegliere **Salva impostazioni** nel menu **File**, attribuire un nome al file nella finestra di dialogo visualizzata, quindi scegliere **Salva**.

Configurazione di VirusScan in modalità Avanzata

VirusScan in modalità Avanzata offre maggiore flessibilità nelle opzioni di configurazione rispetto a VirusScan in modalità Classica, inclusa la possibilità di eseguire simultaneamente più operazioni di scansione, di escludere elementi dalle operazioni di scansione e di attivare la capacità di rilevamento euristico di VirusScan.

Avvio di VirusScan in modalità Avanzata

Per avviare VirusScan in modalità Avanzata, procedere come segue:

1. Fare clic su **Avvio** sulla barra delle applicazioni di Windows, scegliere **Programmi**, quindi **McAfee VirusScan**. Selezionare quindi **McAfee VirusScan** dall'elenco visualizzato.

   Questa operazione apre la finestra VirusScan in modalità Classica (vedere Figura 5-1 a pagina 155).

2. Selezionare **Avanzata** dal menu **Strumenti** nella finestra VirusScan in modalità Classica per passare alla modalità avanzata di VirusScan.

Come in VirusScan in modalità Classica, anche in VirusScan in modalità Avanzata una serie di pagine delle proprietà controlla le opzioni per ciascuna attività. Fare clic su ciascuna scheda nella finestra VirusScan in modalità Avanzata per impostare VirusScan per le attività prescelte. Le sezioni successive descrivono le opzioni disponibili.

Selezione delle opzioni di Rilevamento

Inizialmente VirusScan effettua la scansione di tutti i dischi rigidi del computer, inclusi quelli mappati dalle unità di rete e limita la scansione solo ai file maggiormente esposti all'infezione (Figura 5-8).

Figura 5-8. finestra VirusScan in modalità Avanzata - pagina Rilevamento

Per modificare queste opzioni e aggiungerne altre, procedere come segue:

1. Selezionare le parti del sistema o della rete che si desidera siano sottoposte a scansione da VirusScan. È possibile:

   - **Aggiungere obiettivi da sottoporre a scansione.** Fare clic su **Aggiungi** per aprire la finestra di dialogo Aggiungi elemento di scansione (Figura 5-9 a pagina 167).

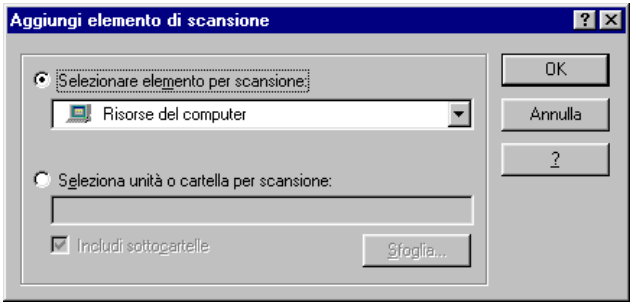

Figura 5-9. Finestra di dialogo Aggiungi elemento di scansione

Perché VirusScan esamini tutto il computer oppure un sottoinsieme di unità del sistema o della rete, fare clic sul pulsante **Selezionare elemento per scansione**, quindi selezionare l'obiettivo di scansione dall'elenco fornito.

Le scelte disponibili sono:

- **Risorse del computer.** VirusScan sottopone a scansione tutte le unità collegate fisicamente al computer o mappate logicamente mediante Gestione risorse di Windows ad una lettera di unità sul computer.
- **Tutti i supporti rimovibili.** VirusScan sottopone a scansione soltanto i CD-ROM, i dischi Iomega Zip o supporti di memorizzazione simili collegati fisicamente al computer.
- **Tutti i dischi rigidi.** VirusScan sottopone a scansione i dischi rigidi collegati fisicamente al computer.
- **Tutte le unità di rete.** VirusScan sottopone a scansione tutte le unità mappate logicamente mediante Gestione risorse di Windows ad una lettera di unità sul computer.

Per far sì che VirusScan esamini un particolare disco o cartella del sistema, fare clic sul pulsante **Seleziona unità o cartella per scansione**. Digitare quindi nella casella di testo fornita la lettera dell'unità o il percorso della cartella che si desidera sottoporre a scansione oppure fare clic su **Sfoglia** per localizzare l'obiettivo di scansione sul computer. Selezionare la casella di controllo **Includi sottocartelle** per consentire a VirusScan di rilevare i virus anche nelle cartelle contenute nell'obiettivo di scansione. Per chiudere la finestra di dialogo, fare clic su **OK**.

- **Modificare gli obiettivi di scansione.** Selezionare uno degli obiettivi di scansione elencati, quindi fare clic su **Modifica** per aprire la finestra di dialogo Modifica elemento di scansione (Figura 5-10).

Figura 5-10. Finestra di dialogo Modifica elemento di scansione

Viene visualizzata la finestra di dialogo con l'obiettivo di scansione esistente specificato. Selezionare o immettere un nuovo obiettivo di scansione, quindi fare clic su **OK** per chiudere la finestra di dialogo.

- **Rimuovere gli obiettivi di scansione.** Selezionare uno degli obiettivi di scansione elencati, quindi fare clic su **Rimuovi** per eliminarlo.

2. Specificare il tipo di file che si desidera VirusScan sottoponga a scansione. È possibile:

   - **Eseguire la scansione di file compressi.** Selezionare la casella di controllo **File compressi** per consentire a VirusScan di cercare i virus nei file compressi con i seguenti formati: .??_, .CAB, LZEXE, LZH, PKLite, .TD0, e .ZIP. Nonostante garantisca una maggiore protezione, la scansione di file compressi può aumentare il tempo necessario per tale operazione.

   - **Scegliere il tipo di file da sottoporre a scansione.** Normalmente i virus non sono in grado di attaccare i file di dati o i file che non contengono un codice eseguibile. Per questa ragione è possibile limitare le operazioni di scansione solo ai file maggiormente esposti alle infezioni dei virus, in modo da velocizzare le operazioni di scansione. A tal fine, selezionare il pulsante **Solo file di programma**. Per visualizzare o indicare le estensioni dei nomi di file che saranno analizzati da VirusScan, fare clic su **Estensioni** per aprire la finestra di dialogo Estensioni file di programma (Figura 5-11 a pagina 169).

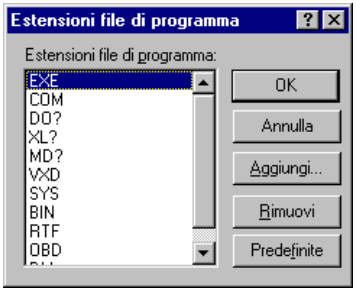

Figura 5-11. Finestra di dialogo Estensioni file di programma

In base alle impostazioni predefinite, VirusScan cerca i virus nei file con le estensioni .EXE, .COM, .DO?, .XL?, .RTF, .BIN, .SYS, .MD?, .VXD, .OBD e .DLL. I file con estensione .DO?, .XL?, .RTF, .MD? e .OBD sono file di Microsoft Office. Tutti questi file possono essere infettati da virus macro. Il ? è un carattere jolly che abilita la scansione di file di documento e di modello da parte di VirusScan.

- Per aggiungere estensioni all'elenco, fare clic su **Aggiungi**, quindi digitare le estensioni dei file che si desidera VirusScan sottoponga a scansione nella finestra di dialogo visualizzata.
- Per eliminare un'estensione dall'elenco, selezionarla, quindi fare clic su **Rimuovi**.
- Fare clic su **Predefinite** per ripristinare l'elenco nella sua forma originaria.

Al termine, scegliere **OK** per chiudere la finestra di dialogo.

Per far sì che VirusScan esamini tutti i file sul sistema, indipendentemente dall'estensione, selezionare il pulsante **Tutti i file**. Questa operazione rallenta notevolmente il sistema, ma garantisce la completa eliminazione dei virus.

- **Attivare la scansione euristica**. Fare clic su **Euristica macro** per aprire la finestra di dialogo Impostazioni di scansione dell'euristica della macro (Figura 5-12 a pagina 170).

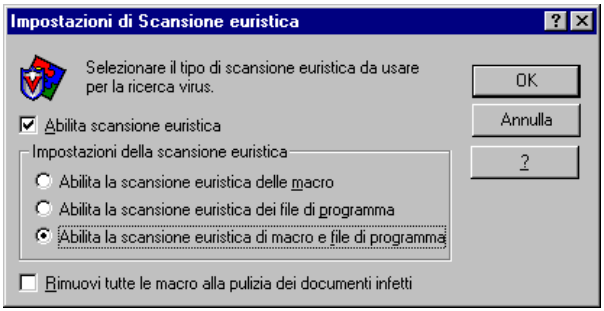

Figura 5-12. Finestra di dialogo Impostazioni di scansione dell'euristica della macro

La tecnologia di scansione euristica consente a VirusScan di riconoscere nuovi virus macro in base alla loro somiglianza con virus simili già conosciuti. A tal fine, il programma cerca le caratteristiche di "virus simili" in file già sottoposti a scansione. La presenza di un numero sufficiente di tali caratteristiche consente a VirusScan di identificare il file come potenzialmente infetto da un nuovo virus o da uno precedentemente non identificato.

Poiché VirusScan ricerca simultaneamente le caratteristiche dei file che escludono la possibilità di infezione da virus, raramente darà indicazioni errate su un'infezione da virus. Quindi, a meno che non si sia certi che il file *non* contiene un virus, trattare le infezioni "probabili" con la stessa attenzione richiesta dalle infezioni certe.

Per attivare la scansione euristica, procedere come segue:

a. Selezionare la casella di controllo **Abilita scansione euristica macro**. Vengono attivate le altre opzioni della finestra di dialogo.

b. Selezionare il tipo di scansione euristica che si desidera che VirusScan utilizzi. Le scelte disponibili sono:

   - **Abilita scansione euristica macro**. Scegliere questa opzione per consentire a VirusScan di identificare tutti i file di Microsoft Word, Microsoft Excel e altri file di Microsoft Office che presentano macro incorporate e quindi di confrontare il codice macro al database di firme virus. VirusScan identifica le corrispondenze esatte in base al nome del virus; le firme in codice che somigliano a virus esistenti consentono a VirusScan di segnalare la presenza di un "probabile" virus macro.

- **Attiva scansione euristica del file di programma.** Scegliere questa opzione per consentire a VirusScan di individuare nuovi virus nei file di programma esaminandone le caratteristiche e confrontandole con l'elenco delle caratteristiche dei virus noti. VirusScan identificherà i file con un numero sufficiente di queste caratteristiche come virus probabili.
- **Attiva scansione euristica dei file di programma e di macro.** Scegliere questa opzione per consentire a VirusScan di utilizzare entrambi i tipi di scansione euristica. Network Associates consiglia di utilizzare questa opzione per una protezione antivirus completa.

c. Determinare la modalità di trattamento dei file macro infetti. Selezionare **Rimuovi tutte le macro alla pulizia dei documenti infetti** per eliminare tutti i codici infetti dal documento e lasciare solo i dati. Per rimuovere solo il codice virus dalle macro del documento, non selezionare questa casella di controllo.

> **AVVERTENZA:** Utilizzare questa funzione con cautela: la rimozione di tutte le macro da un documento può provocare la perdita o il danneggiamento dei dati e l'impossibilità di utilizzarli.

d. Scegliere **OK** per salvare le impostazioni e tornare alla finestra VirusScan in modalità Avanzata.

3. Fare clic sulla scheda Azione per scegliere le opzioni aggiuntive di VirusScan.

   Per avviare immediatamente un'operazione di scansione con le opzioni appena selezionate, fare clic su **Avvia scansione**. Per salvare le modifiche come opzioni di scansione predefinite, selezionare **Salva come predefinite** dal menu **File** oppure fare clic su **Nuova scansione**. Per salvare le impostazioni in un nuovo file, scegliere **Salva impostazioni** nel menu **File**, attribuire un nome al file nella finestra di dialogo visualizzata, quindi scegliere **Salva**.

Scelta delle opzioni Azione

Quando VirusScan rileva un virus può chiedere all'utente quale operazione eseguire sul virus infetto, oppure può eseguire automaticamente un'azione precedentemente impostata. Utilizzare la pagina delle proprietà Azione per specificare le opzioni di risposta o le azioni che si desidera VirusScan esegua quando rileva un virus.

Procedere come segue:

1. Fare clic sulla scheda Azione nella finestra VirusScan in modalità Avanzata per visualizzare la pagina delle proprietà corretta (Figura 5-13).

Figura 5-13. VirusScan in modalità Avanzata - pagina Azione

2. Selezionare una risposta dall'elenco **Al rilevamento di un virus**. L'area immediatamente al di sotto dell'elenco cambia per visualizzare opzioni aggiuntive per ciascuna risposta. Le scelte disponibili sono:

   - **Richiedi azione.** Scegliere questa risposta se si prevede di assistere all'operazione di scansione eseguita da VirusScan: il programma visualizza un messaggio di avviso quando rileva un virus e offre all'utente una gamma di risposte possibili. Selezionare le opzioni di risposta che si desidera visualizzare nel messaggio di avviso:

     – **Pulisci infezione.** Questa opzione indica a VirusScan di tentare di rimuovere il codice del virus dal file infetto.

     – **Elimina file.** Questa opzione indica a VirusScan di eliminare immediatamente il file infetto.

     – **Escludi elemento.** Questa opzione indica a VirusScan di tralasciare il file durante le operazioni di scansione successive. Questa è l'unica opzione non selezionata per impostazione predefinita.

     – **Continua scansione.** Questa opzione indica a VirusScan di continuare la scansione senza intraprendere alcun'altra azione. Se è stata abilitata l'opzione per la registrazione degli eventi, VirusScan registra l'infezione rilevata nel file di registro.

  - **Interrompi scansione.** Questa opzione indica a VirusScan di interrompere l'operazione di scansione immediatamente. Per continuare la scansione, fare clic su **Avvia scansione** per riavviare l'operazione.

  - **Sposta file.** Questa opzione indica a VirusScan di spostare il file infetto in una cartella di quarantena.

- **Sposta file infetti automaticamente**. Scegliere questa risposta per consentire a VirusScan di spostare i file infetti eventualmente rilevati in una directory di quarantena. In base alle impostazioni predefinite, VirusScan sposta questi file in una cartella denominata INFECTED (infetti), creata al livello principale dell'unità in cui viene rilevata la presenza del virus. Ad esempio, se VirusScan rileva un file infetto in T:\MY DOCUMENTS e si è specificato INFECTED come directory di quarantena, VirusScan copierà il file in T:\INFECTED.

  È possibile immettere un nome diverso nella casella di testo fornita, o fare clic su **Sfoglia** per individuare una cartella adeguata sul disco rigido.

- **Pulisci file infetti automaticamente.** Scegliere questa risposta per consentire a VirusScan di rimuovere il codice del virus dal file infetto non appena ne rileva la presenza. Se VirusScan non è in grado di eliminare il virus, prenderà nota del virus nel suo file di registro, se si sono abilitate le funzioni di registrazione. Per ulteriori dettagli, vedere "Selezione delle opzioni di Rapporto" a pagina 176.

- **Elimina file infetti automaticamente.** Scegliere questa risposta per consentire a VirusScan di eliminare immediatamente ogni file infetto. Attivare la funzione di notifica in modo da registrare i file eliminati da VirusScan. Sarà necessario ripristinare i file eliminati da copie di backup.

- **Continua scansione.** Scegliere questa risposta solo se si prevede di non assistere alle operazioni di scansione di VirusScan. Se viene attivata anche la funzione di notifica di VirusScan (vedere "Selezione delle opzioni di Rapporto" a pagina 176 per i dettagli), il programma registra il nome dei virus rilevati e il nome dei file infetti in modo tale che sia possibile eliminarli alla prima occasione.

3. Fare clic sulla scheda Avviso per scegliere le opzioni di configurazione aggiuntive di VirusScan.

Per avviare immediatamente un'operazione di scansione con le opzioni appena selezionate, fare clic su **Avvia scansione**. Per salvare le modifiche come opzioni di scansione predefinite, selezionare **Salva come predefinite** dal menu **File** oppure fare clic su **Nuova scansione**. Per salvare le impostazioni in un nuovo file, scegliere **Salva impostazioni** nel menu **File**, attribuire un nome al file nella finestra di dialogo visualizzata, quindi scegliere **Salva**.

Selezione delle opzioni di Avviso

Una volta configurato con le opzioni di risposta desiderate, VirusScan ricerca ed elimina i virus dal sistema automaticamente, appena ne rileva la presenza, senza ulteriori interventi da parte dell'utente. Tuttavia, se l'utente desidera che VirusScan lo informi immediatamente quando rileva un virus per agire in modo appropriato, è possibile configurarlo in diversi modi. Utilizzare la pagina delle proprietà Avviso per scegliere i metodi di avviso che si desidera utilizzare.

Procedere come segue:

1. Fare clic sulla scheda Avviso nella finestra VirusScan in modalità Avanzata per visualizzare la pagina delle proprietà corretta (Figura 5-14).

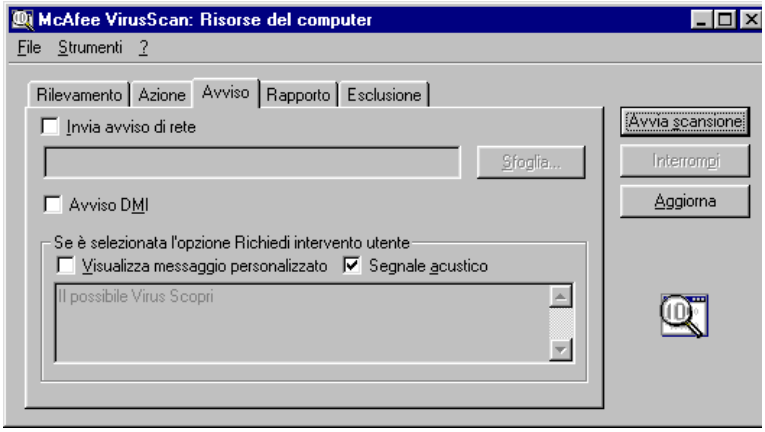

Figura 5-14. VirusScan in modalità Avanzata - pagina Avviso

2. Per indicare a VirusScan di inviare un messaggio di avviso ad un server che esegue NetShield, la soluzione antivirus di Network Associates per i server, selezionare la casella di controllo **Invia avviso di rete**, quindi immettere il percorso per la cartella di avviso di NetShield nella rete, oppure fare clic su **Sfoglia** per individuare la cartella appropriata.

NOTA: La cartella scelta deve contenere CENTALRT.TXT, il file di avviso centralizzato di NetShield. NetShield raccoglie i messaggi di avviso inviati da VirusScan e da altri programmi Network Associates, quindi li trasferisce agli amministratori di rete perché intraprendano le azioni necessarie. Per ulteriori informazioni sull'Avviso centralizzato, consultare il *Manuale dell'utente* di NetShield.

3. Per consentire a VirusScan di inviare messaggi di avviso di virus attraverso l'interfaccia del componente DMI alle applicazioni del desktop e di gestione della rete in esecuzione, selezionare la casella di controllo **Avviso DMI**.

   NOTA: DMI (Desktop Management Interface) è uno standard per la comunicazione di richieste di gestione e informazioni di avviso tra i componenti hardware e software dei computer o collegati ad essi e le applicazioni utilizzate per la loro gestione. Per ulteriori informazioni sul metodo di avviso, contattare l'amministratore della rete.

4. Se si sceglie **Richiedi azione** come risposta nella pagina Azione (vedere "Scelta delle opzioni Azione" a pagina 171 per i dettagli), è possibile anche indicare a VirusScan di emettere un segnale acustico e visualizzare un messaggio personalizzato al rilevamento di un virus. Per effettuare quest'operazione, selezionare la casella di controllo **Visualizza messaggio personalizzato**, quindi digitare il messaggio che si desidera visualizzare nella relativa casella di testo: è possibile digitare fino a 225 caratteri. Selezionare quindi la casella di controllo **Segnale acustico**.

5. Fare clic sulla scheda Rapporto per scegliere le opzioni di configurazione aggiuntive di VirusScan.

   Per avviare immediatamente un'operazione di scansione con le opzioni appena selezionate, fare clic su **Avvia scansione**. Per salvare le modifiche come opzioni di scansione predefinite, selezionare **Salva come predefinite** dal menu **File** oppure fare clic su **Nuova scansione**. Per salvare le impostazioni in un nuovo file, scegliere **Salva impostazioni** nel menu **File**, attribuire un nome al file nella finestra di dialogo visualizzata, quindi scegliere **Salva**.

Selezione delle opzioni di Rapporto

VirusScan elenca le impostazioni correnti e riassume tutte le azioni eseguite durante le operazioni di scansione in un file di registro denominato VSCLOG.TXT. VirusScan può registrare i virus in questo file, oppure è possibile utilizzare qualunque editor di testi per creare un file di testo utilizzato da VirusScan. Quindi è possibile aprire e stampare il file di registro per esaminarlo in seguito, sia da VirusScan che da un editor di testo.

Il file VSCLOG.TXT può essere utilizzato come importante strumento di gestione per controllare l'attività dei virus nel sistema e prendere nota delle impostazioni utilizzate per rilevare e rispondere alle infezioni rilevate da VirusScan. È possibile anche utilizzare i rapporto degli incidenti registrati nel file per determinare quali file è necessario sostituire dalle copie di backup, esaminare in quarantena, o eliminare dal computer. Utilizzare la pagina delle proprietà Rapporto per determinare le informazioni da includere nel file di registro di VirusScan.

Per impostare VirusScan per la registrazione delle azioni in un file di registro, procedere come segue:

1. Fare clic sulla scheda Rapporto nella finestra VirusScan in modalità Avanzata per visualizzare la pagina delle proprietà appropriata (Figura 5-15).

Figura 5-15. VirusScan in modalità Avanzata - pagina Rapporto

2. Selezionare la casella di controllo **Registra su file**.

   In base alle impostazioni predefinite, VirusScan scrive le informazioni di registro nel file VSCLOG.TXT nella directory di programma di VirusScan. É possibile digitare un nome diverso nella relativa casella di testo o fare clic su **Sfoglia** per individuare un file adatto in un'altra directory sul disco rigido o in rete.

3. Per ridurre al minimo le dimensioni del file di registro, selezionare la casella di controllo **Limita dimensione file di registro a**, quindi immettere un valore per le dimensioni del file, in kilobyte, nella relativa casella di testo.

   Immettere un valore compreso tra 10KB e 999KB. In base alle impostazioni predefinite, VirusScan limita la dimensione del file a 100KB. Se i dati nel file di registro superano le dimensioni del file impostate, VirusScan cancella la registrazione esistente e ricomincia dal punto in cui ha smesso.

4. Selezionare le caselle di controllo corrispondenti alle informazioni che si desidera VirusScan registri nel file di registro. È possibile registrare una qualsiasi delle seguenti informazioni:

   - **Rilevamento virus.** Selezionare questa casella di controllo perché VirusScan riporti il numero dei file infetti rilevati durante la sessione di scansione.
   - **Pulizia virus**. Selezionare questa casella di controllo perché VirusScan riporti il numero dei file infetti dai quali ha rimosso il virus.
   - **Eliminazione file infetti.** Selezionare questa casella di controllo perché VirusScan riporti il numero dei file infetti eliminati dal sistema.
   - **Spostamento file infetti.** Selezionare questa casella di controllo perché VirusScan riporti il numero dei file infetti spostati nella directory di quarantena.
   - **Impostazioni sessione.** Selezionare questa casella di controllo perché VirusScan riporti le opzioni selezionate nella finestra di dialogo Proprietà McAfee VirusScan per ogni sessione di scansione.
   - **Riepilogo sessione.** Selezionare questa casella di controllo perché VirusScan riassuma le azioni eseguite durante ciascuna sessione di scansione. Le informazioni di riepilogo includono il numero di file sottoposti a scansione, il numero e il tipo di virus rilevati, il numero di file spostati o eliminati e altre informazioni.

- **Data e ora.** Selezionare questa casella di controllo perché VirusScan riporti la data e l'ora di ciascuna voce annotata nel file di registro.
- **Nome utente.** Selezionare questa casella di controllo perché VirusScan riporti il nome dell'utente utilizzato per il collegamento al computer nel momento della registrazione delle voci nel file di registro.

Per vedere i contenuti del file di registro, avviare VirusScan, quindi scegliere **Visualizza registro attività** dal menu **File**. Per ulteriori informazioni, consultare "Uso dei menu di VirusScan" a pagina 155.

5. Selezionare la scheda Esclusione per scegliere le opzioni di configurazione aggiuntive di VirusScan.

   Per avviare immediatamente un'operazione di scansione con le opzioni appena selezionate, fare clic su **Avvia scansione**. Per salvare le modifiche come opzioni di scansione predefinite, selezionare **Salva come predefinite** dal menu **File** oppure fare clic su **Nuova scansione**. Per salvare le impostazioni in un nuovo file, scegliere **Salva impostazioni** nel menu **File**, attribuire un nome al file nella finestra di dialogo visualizzata, quindi scegliere **Salva**.

Scelta opzioni Esclusione

Molti dei file memorizzati nel computer non sono vulnerabili a infezioni da virus. Le operazioni di scansione che esaminano questi file possono richiedere molto tempo e produrre scarsi risultati. È possibile accelerare le operazioni di scansione indicando a VirusScan di cercare solo i tipi di file esposti (vedere "Selezione delle opzioni di Rilevamento" a pagina 166 per i dettagli), oppure indicando a VirusScan di ignorare interi file o cartelle sicuramente immuni da virus.

Una volta eseguita la scansione completa del sistema, è possibile escludere i file e le cartelle che non si modificano o che non sono normalmente vulnerabili a infezioni da virus. È possibile anche fare affidamento su VShield per assicurare la protezione tra le operazioni di scansione pianificate. Operazioni di scansione eseguite regolarmente, con l'esame di tutte le aree del computer, forniscono la migliore protezione dai virus.

Per escludere file o cartelle dalle operazioni di scansione, procedere come segue:

1. Fare clic sulla scheda Esclusione nella finestra VirusScan in modalità Avanzata per visualizzare la pagina delle proprietà corretta (Figura 5-16).

Figura 5-16. Finestra VirusScan in modalità Avanzata - pagina Esclusione

La pagina Esclusione elenca inizialmente solo il contenuto del cestino. VirusScan esclude il cestino dalle operazioni di scansione perché Windows non esegue i file memorizzati in quest'area.

2. Specificare gli elementi che si desidera escludere. È possibile:

   - **Aggiungere alla lista di esclusione file, cartelle o volumi.** Fare clic su **Aggiungi** per aprire la finestra di dialogo Aggiungi elemento di esclusione (Figura 5-17).

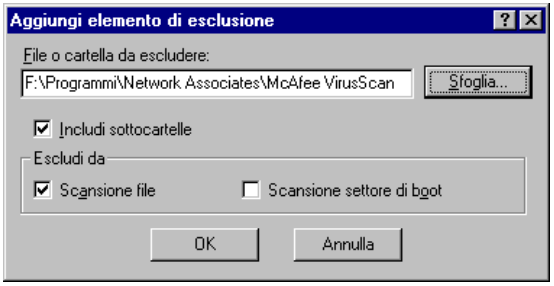

Figura 5-17. Finestra di dialogo Aggiungi elemento di esclusione

a. Digitare il volume, il percorso del file o il percorso della cartella che si desidera escludere dalla scansione o fare clic su **Sfoglia** per localizzare il file o la cartella sul proprio computer.

NOTA: Se si è scelto di spostare automaticamente i file infetti in una cartella di quarantena, il programma esclude tale cartella dalle operazioni di scansione.

---

b. Selezionare la casella di controllo **Includi sottocartelle** per escludere dalla scansione tutte le sottocartelle interne alla cartella specificata.

c. Selezionare la casella di controllo **Scansione file** perché VirusScan non rilevi virus nei file o nelle cartelle escluse.

d. Selezionare la casella di controllo **Scansione settore di boot** perché VirusScan non ricerchi virus nei settori di boot dei file o delle cartelle escluse. Utilizzare questa opzione per escludere dalle operazioni di scansione i file di sistema, come ad esempio COMMAND.COM.

AVVERTENZA: Network Associates consiglia di *non* escludere i file di sistema dalla scansione per la ricerca di virus.

---

e. Per salvare le modifiche apportate e chiudere la finestra di dialogo, fare clic su **OK**.

f. Ripetere i punti da a. a d. fino a quando non sono stati elencati tutti i file e le cartelle che non si desidera sottoporre a scansione.

- **Modificare l'elenco di esclusione.** Per cambiare le impostazioni di un elemento escluso, selezionarlo nell'elenco Esclusioni, quindi fare clic su **Modifica** per aprire la finestra di dialogo Modifica elemento di esclusione. Effettuare le modifiche desiderate, quindi fare clic su **OK** per chiudere la finestra di dialogo.
- **Rimuovere un elemento dall'elenco.** Per eliminare un elemento escluso, selezionarlo nell'elenco, quindi fare clic su **Rimuovi**. VirusScan effettuerà la scansione di questo file o cartella durante la successiva operazione di scansione.

3. Fare clic su una scheda diversa per modificare alcune impostazioni di configurazione di VirusScan.

   Per avviare immediatamente un'operazione di scansione con le opzioni appena selezionate, fare clic su **Avvia scansione**. Per salvare le modifiche come opzioni di scansione predefinite, selezionare **Salva come predefinite** dal menu **File** oppure fare clic su **Nuova scansione**. Per salvare le impostazioni in un nuovo file, scegliere **Salva impostazioni** nel menu **File**, attribuire un nome al file nella finestra di dialogo visualizzata, quindi scegliere **Salva**.

Attivazione della protezione tramite password

VirusScan consente di impostare una password per proteggere da modifiche non autorizzate le impostazioni scelte in ciascuna pagina delle proprietà. Questa funzione si rivela particolarmente utile per gli amministratori di sistema che non intendono consentire agli utenti eventuali variazioni alle misure di sicurezza modificando le impostazioni di VirusScan. Utilizzare la pagina delle proprietà Sicurezza per bloccare le proprie impostazioni.

Per attivare la protezione tramite password per VirusScan in modalità avanzata, procedere come segue:

1. Scegliere **Protetto da password** dal menu **Strumenti** nella finestra VirusScan in modalità Avanzata per aprire la finestra di dialogo Password di protezione (Figura 5-18).

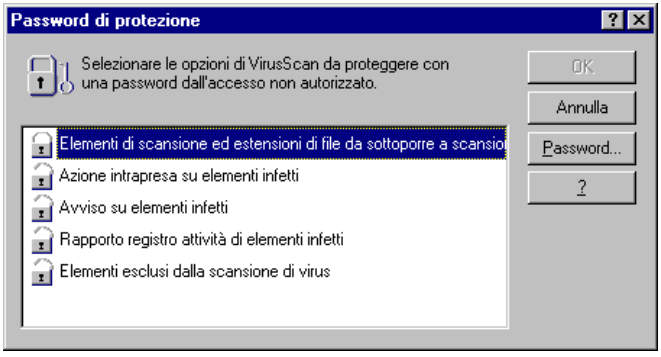

Figura 5-18. Finestra di dialogo Password di protezione

2. Dall'elenco visualizzato, selezionare le impostazioni che si desidera proteggere.

   È possibile proteggere qualsiasi pagina o tutte le pagine delle proprietà di VirusScan. Le pagine di proprietà protette mostrano l'icona di un lucchetto chiuso nell'elenco di sicurezza rappresentato in Figura 5-18. Per rimuovere la protezione da una pagina di proprietà, fare clic sull'icona del lucchetto chiuso al fine di aprirlo.

3. Fare clic su **Password** per aprire la finestra di dialogo Specifica password (Figura 5-19).

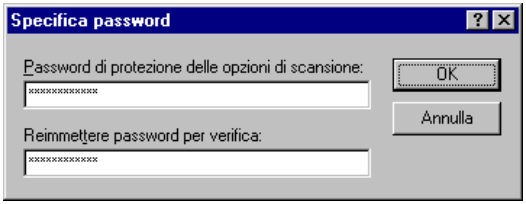

Figura 5-19. Finestra di dialogo Specifica password

   a. Immettere una password nella prima casella di testo visualizzata, quindi immettere nuovamente la password nella casella di testo sottostante per confermare la scelta.

   b. Fare clic su **OK** per chiudere la finestra di dialogo Specifica password.

4. Fare clic su **OK** per tornare alla finestra VirusScan in modalità Avanzata.

Pianificazione delle attività di scansione 6

Funzioni dell'utilità di pianificazione di VirusScan

L'utilità di pianificazione di VirusScan esegue operazioni di scansione e altre attività pianificate dall'utente. È possibile utilizzare l'utilità di pianificazione di VirusScan, insieme ad altre attività pianificate, per eseguire operazioni di scansione non assistite in modo da non interrompere il proprio lavoro.

Perché è utile pianificare le operazioni di scansione

Sebbene VirusScan contenga dei componenti che controllano di continuo il computer per rilevare la presenza di virus e che consentono all'utente di eseguire in qualunque momento la scansione del sistema, è possibile pianificare le operazioni di scansione e altre attività di VirusScan per

- **Impostare uno schema per la scansione del sistema.** Se si desidera controllare il computer o la rete per rilevare l'attività di virus, è possibile pianificare la scansione completa del sistema a intervalli di tempo regolari. Le funzioni di notifica di VirusScan consentono di ottenere dei rapporti completi relativi al numero, al tipo, alle dimensioni e ad altre caratteristiche di qualunque virus rilevato sul sistema.
- **Disporre di uno strumento aggiuntivo per la scansione all'accesso.** Network Associates consiglia l'utilizzo di VShield per la scansione continua del sistema; tuttavia, se l'ambiente operativo non consente di utilizzare VShield o se si ritiene che l'utilizzo del programma possa diminuire le prestazioni del sistema, è preferibile pianificare operazioni di scansione frequenti per evitare le infezioni da virus. Se si utilizza VShield di frequente, è comunque utile pianificare scansioni complete del sistema per evitare che i file infetti da virus non vengano rilevati.
- **Eseguire differenti operazioni di scansione.** La funzione di pianificazione delle operazioni di scansione consente di scegliere fra diversi tipi di attività da eseguire in momenti diversi. Ad esempio, è possibile programmare VShield per la scansione continua del sistema e la scansione meno frequente di un'unità di rete.

L'utilità di pianificazione viene fornita con un insieme di attività già configurate ma non ancora pianificate. Tali attività comprendono l'esecuzione automatica di VShield quando si avvia il computer, la scansione predefinita del sistema, la scansione dell'unità C, la scansione di tutte le unità disco del sistema e l'aggiornamento dei file di dati di VirusScan e dei componenti del programma. È possibile abilitare le attività predefinite desiderate oppure si possono definire le attività più adatte al proprio ambiente di lavoro.

Avvio dell'Utilità di pianificazione di VirusScan

Per avviare l'utilità di pianificazione di VirusScan,

- Fare clic sul pulsante **Avvio** (Windows 95) o **Start** (Windows 98), scegliere **Programmi**, quindi **McAfee VirusScan**. Scegliere, quindi, **Utilità di pianificazione di VirusScan McAfee** dall'elenco che viene visualizzato; oppure
- Avviare VirusScan in modalità Classica, quindi selezionare **Utilità di pianificazione** dal menu **Strumenti**. Per ottenere informazioni relative all'avvio di VirusScan, vedere Capitolo 5, "Uso di McAfee VirusScan".

Entrambi i metodi consentono di aprire la finestra Utilità di pianificazione (Figura 6-1). Una volta avviato, l'utilità di pianificazione visualizza anche una piccola icona nell'area messaggi di Windows. Fare doppio clic su questa icona per visualizzare la finestra Utilità di pianificazione.

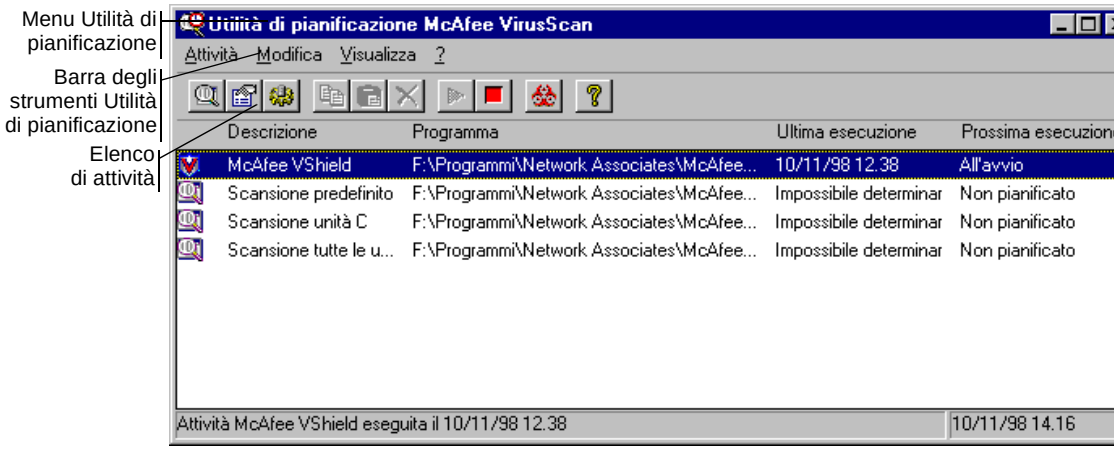

Figura 6-1. La finestra Utilità di pianificazione di VirusScan

La finestra Utilità di pianificazione mostra inizialmente un insieme di attività predefinite fornite con l'utilità di pianificazione, già preconfigurate e pronte all'utilizzo. Un'attività è un insieme di istruzioni per eseguire un programma particolare, in una determinata configurazione e in uno specifico momento. L'elenco di attività dell'Utilità di pianificazione indica il programma che eseguirà l'attività: l'utente pianifica VShield o SCAN32.EXE per l'esecuzione di molte attività; visualizza la data e l'ora dell'ultima esecuzione dell'attività e indica quando è necessario impostarla di nuovo. Ciascuna nuova attività creata viene visualizzata nella parte inferiore dell'elenco di attività.

La barra degli strumenti visualizzata nella parte superiore della finestra Utilità di pianificazione fornisce un accesso rapido ai comandi più comuni del programma. Per visualizzare unicamente i pulsanti di comando della barra degli strumenti, fare clic su **Visualizza**, scegliere **Barra degli strumenti**, quindi selezionare **Pulsanti standard**. Per aggiungere testo ai pulsanti, fare clic su **Visualizza**, scegliere **Barra degli strumenti**, quindi selezionare **Etichette di testo**. È possibile attivare entrambe le opzioni contemporaneamente: un segno di spunta accanto alla voce di menu indica quale visualizzazione è attiva. È possibile ritrovare la maggior parte dei comandi della barra degli strumenti nei menu situati nella parte superiore della finestra Utilità di pianificazione e nei menu di scelta rapida visualizzati quando si fa clic con il tasto destro del mouse su un'attività in elenco.

Nella barra di stato visualizzata nella parte inferiore della finestra Utilità di pianificazione è indicato il numero di attività elencate. Quando si seleziona un'attività elencata, la barra di stato indica l'ultima attività eseguita. Nella barra di stato viene visualizzata anche una breve descrizione di ciascun pulsante della barra degli strumenti quando il cursore del mouse passa su di questi. Per visualizzare o nascondere ciascun elemento della finestra, scegliere **Barra del titolo** oppure **Barra di stato** dal menu **Visualizza**.

Utilizzo della finestra Utilità di pianificazione

Dalla finestra Utilità di pianificazione è possibile:

- **Creare una nuova attività.** Selezionare **Nuova attività** dal menu **Attività** oppure fare clic su  nella barra degli strumenti dell'Utilità di pianificazione. Viene visualizzata una finestra di dialogo delle proprietà dell'attività. Per informazioni sulle modalità di definizione delle azioni da eseguire, vedere "Creazione di nuove attività" a pagina 189.

- Pianificare e avviare un'attività. Selezionare una delle attività elencate nella finestra Utilità di pianificazione, quindi scegliere **Proprietà** dal menu **Attività** oppure fare clic su  nella barra degli strumenti dell'Utilità di pianificazione. Viene visualizzata una finestra di dialogo delle proprietà dell'attività. Per informazioni sulle modalità di definizione delle opzioni che si desidera selezionare per avviare l'attività, vedere "Abilitazione delle attività" a pagina 191.

- Configurare il programma per le attività. Selezionare una delle attività elencate nella finestra Utilità di pianificazione, quindi fare clic su  nella barra degli strumenti dell'Utilità di pianificazione per visualizzare una pagina delle proprietà per il componente VirusScan che eseguirà l'attività. La modalità di visualizzazione di questa pagina delle proprietà dipende dal componente VirusScan eseguito. Per informazioni sulle modalità di scelta delle opzioni per la scansione, vedere "Configurazione delle opzioni delle attività" a pagina 195.

  > **NOTA:** È possibile configurare unicamente quei programmi utilizzati per l'aggiornamento di VirusScan oppure i programmi che eseguono un'operazione di scansione: vale a dire, VShield o VirusScan (SCAN32.EXE). Sebbene sia possibile utilizzare l'Utilità di pianificazione di VirusScan per pianificare altri programmi da eseguire, non è tuttavia possibile utilizzarla per *configurare* altri programmi.

- **Copiare un'attività.** Selezionare una delle attività elencate nella finestra Utilità di pianificazione, quindi selezionare **Copia** dal menu **Modifica** oppure fare clic su  nella barra degli strumenti dell'Utilità di pianificazione. L'attività viene copiata negli Appunti di Windows. Quindi, fare clic sulla finestra Utilità di pianificazione, selezionare **Incolla** dal menu **Modifica** oppure fare clic su  nella barra degli strumenti dell'Utilità di pianificazione per incollare l'attività copiata nell'elenco dell'Utilità di pianificazione. Utilizzare questa funzione per copiare le impostazioni di un'attività che si desidera utilizzare come modello per altre attività simili.

- **Cancellare un'attività.** Selezionare una delle attività elencate nella finestra Utilità di pianificazione, quindi selezionare **Elimina** dal menu **Attività** oppure fare clic su  nella barra degli strumenti dell'Utilità di pianificazione.

  > **NOTA:** È possibile cancellare solo le attività create dall'utente; non è possibile cancellare le attività predefinite fornite con l'utilità di pianificazione. Tuttavia, possono essere disattivate le attività predefinite che non si desidera eseguire. Per ulteriori dettagli, vedere "Abilitazione delle attività" a pagina 191.

- **Avviare un'attività.** Selezionare una delle attività elencate nella finestra Utilità di pianificazione, quindi selezionare **Avvia** dal menu **Attività** oppure fare clic su  nella barra degli strumenti dell'Utilità di pianificazione. L'attività selezionata viene avviata immediatamente con le opzioni selezionate. Per abilitare le funzioni di scansione di VShield, selezionare McAfee VShield nell'elenco delle attività, quindi selezionare **Abilita** dal menu **Attività**. Per avviare VShield e caricarlo in memoria, selezionare l'attività VShield, quindi fare clic su  nella barra degli strumenti dell'Utilità di pianificazione.

- **Interrompere un'attività.** Selezionare una delle attività elencate nella finestra dell'Utilità di pianificazione, quindi selezionare **Interrompi** dal menu **Attività** oppure fare clic su  nella barra degli strumenti dell'Utilità di pianificazione. Per interrompere l'esecuzione di VShield, selezionare McAfee VShield nell'elenco delle attività, quindi fare clic su  nella barra degli strumenti dell'Utilità di pianificazione. Per disattivare semplicemente VShield, selezionare l'attività VShield, quindi selezionare **Disabilita** dal menu **Attività**. Per ottenere informazioni sulle modalità da seguire per terminare completamente VShield e rimuoverlo dalla memoria, vedere "Disattivare o terminare VShield" a pagina 146.

- **Collegamento alla Virus Information Library di Network Associates.** Selezionare **Elenco virus** dal menu **Visualizza** oppure fare clic su  nella barra degli strumenti dell'Utilità di pianificazione. VirusScan avvierà l'applicazione browser desiderata e si collegherà al sito Web di Network Associates. Per ulteriori informazioni sul contenuto della libreria, vedere "Visualizzazione di informazioni sui file infetti e sui virus" a pagina 77.

  NOTA: Per collegarsi alla Virus Information Library, è necessario disporre di una connessione a Internet e di un software di esplorazione del Web installato sul computer.

- **Aprire il file della guida in linea.** Selezionare **Guida in linea** dal menu **?** oppure fare clic su  nella barra degli strumenti dell'Utilità di pianificazione per visualizzare un elenco di argomenti dalla guida di VirusScan.

- **Visualizzare un Registro attività.** Selezionare una delle attività elencate nella finestra Utilità di pianificazione, quindi scegliere **Visualizza registro attività** dal menu **Attività**. Non è possibile associare un file di registro a tutte le attività; in ogni caso VirusScan aprirà il file di registro delle relative attività in una finestra del Blocco appunti (vedere Figura 5-2 a pagina 157). È possibile stampare, modificare e copiare questo file, trattandolo come un comune file di testo. Per ulteriori informazioni sui record del file di registro, consultare Capitolo 4, "Uso di VShield," e Capitolo 5, "Uso di McAfee VirusScan".

- **Avviare l'Utilità di pianificazione di VirusScan automaticamente.** Scegliere **Carica all'avvio** dal menu **Visualizza** per avviare l'Utilità di pianificazione di VirusScan all'avvio del computer. Nell'Utilità di pianificazione questa opzione è attivata per impostazione predefinita. Dato che per eseguire un'attività pianificata è indispensabile che l'Utilità di pianificazione sia attiva, è consigliabile predisporne l'avvio automatico in modo tale da consentire l'avvio delle attività pianificate all'ora stabilita.
- **Uscire dall'Utilità di pianificazione di VirusScan.** Scegliere **Esci** dal menu **Attività** per uscire dall'Utilità di pianificazione. Se vi sono attività in sospeso, è preferibile ridurre ad icona l'utilità di pianificazione invece di chiuderla. Per ulteriori informazioni su come avviare nuovamente l'Utilità di pianificazione, consultare "Avvio dell'Utilità di pianificazione di VirusScan" a pagina 184.

Gestione delle attività predefinite

Subito dopo aver installato VirusScan e riavviato il computer, VShield inizia immediatamente la scansione del sistema, utilizzando una configurazione predefinita che fornisce un livello di protezione di base del sistema. Le altre attività elencate nella finestra Utilità di pianificazione sono state impostate secondo una configurazione predefinita, ma queste attività restano inattive fino a quando non vengono abilitate. Per ulteriori dettagli, vedere "Abilitazione delle attività" a pagina 191.

Le attività predefinite sono:

- **VShield.** Per impostazione predefinita, questa attività viene eseguita automaticamente all'avvio del computer. Non è possibile pianificare una nuova esecuzione di VShield, ma è possibile scegliere fra differenti opzioni di scansione Vedere "Impostazione delle proprietà di VShield" a pagina 90 e sapere quali opzioni sono disponibili.
- **Scansione tutte le unità.** Questa attività sottopone a scansione tutti i dischi rigidi e i supporti rimovibili del sistema, oltre alla memoria RAM e ai settori di boot del disco rigido. Attivare questa attività perché possa essere avviata. È possibile eseguire questa attività secondo la configurazione predefinita oppure impostare opzioni di configurazione personalizzate: vedere "Configurazione di VirusScan per la scansione pianificata" a pagina 196.
- **Scansione unità C:.** Questa attività sottopone a scansione l'unità C:, la memoria RAM e i settori di boot del disco rigido per impostazione predefinita. Attivare questa attività perché possa essere avviata. È possibile eseguire questa attività secondo la configurazione predefinita oppure impostare opzioni di configurazione personalizzate: vedere "Configurazione di VirusScan per la scansione pianificata" a pagina 196.

- **Scansione predefinita.** Questa attività costituisce un modello che può essere utilizzato per la creazione di altre attività. Per impostazione predefinita, viene sottoposta a scansione l'unità C:, la memoria RAM e i settori di boot del disco. Attivare questa attività perché possa essere avviata. È possibile eseguire questa attività secondo la configurazione predefinita oppure impostare opzioni di configurazione personalizzate: vedere "Configurazione di VirusScan per la scansione pianificata" a pagina 196.
- **Aggiornamento automatico.** Questa attività consente la connessione ad un server o ad un sito del protocollo FTP (File Transfer Protocol) designato per aggiornare i file di dati VirusScan (.DAT). L'attività è configurata per effettuare il collegamento ad un server Network Associates, tuttavia è necessario pianificare e attivare l'attività per ottenere l'aggiornamento dei file. È inoltre possibile configurare l'attività per collegarsi a un server centrale o ad un sito FTP della propria rete per l'aggiornamento dei file. Vedere "Configurazione delle opzioni di Aggiornamento automatico" a pagina 216 per informazioni sulle modalità di configurazione dell'attività in base alle proprie esigenze.
- **Upgrade automatico.** Questa attività consente la connessione ad un server o ad un sito FTP designato allo scopo di aggiornare i componenti del programma VirusScan in base alle più recenti versioni. Per collegarsi a un particolare server o ad un sito FTP è necessario configurare l'attività, quindi pianificare e attivare l'attività per ottenere l'aggiornamento dei file. Vedere "Configurazione delle opzioni di Upgrade automatico" a pagina 228 per informazioni sulle modalità di configurazione dell'attività in base alle proprie esigenze.

Creazione di nuove attività

Sebbene le attività predefinite possano fornire una protezione adeguata al sistema, sarà probabilmente necessario creare e avviare attività personalizzate una volta acquisita una certa esperienza con VirusScan e con i tempi e le modalità di scansione.

Per creare una nuova attività, procedere come segue:

1. Selezionare **Nuova attività** dal menu **Attività** nella finestra Utilità di pianificazione oppure fare clic su  nella barra degli strumenti dell'Utilità di pianificazione.

   Viene visualizzata la finestra di dialogo Proprietà attività (Figura 6-2 a pagina 190).

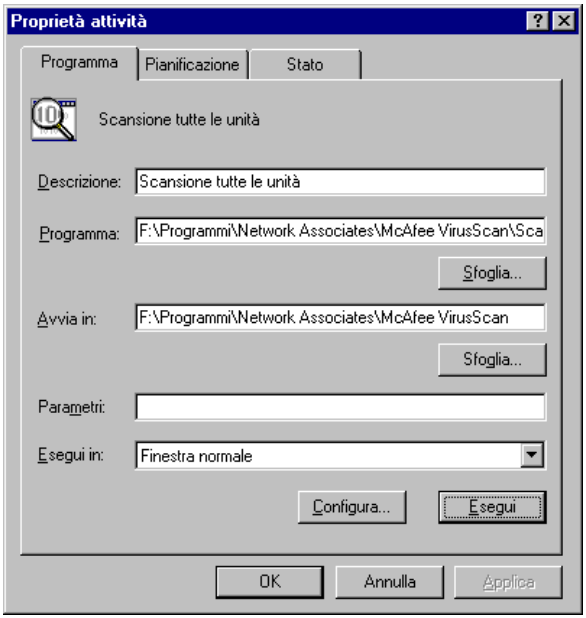

Figura 6-2. Finestra Proprietà attività - pagina Programma

2. Digitare un nome per l'attività nella casella di testo **Descrizione**. Assicurarsi che il nome descriva chiaramente l'attività così da poterla distinguere da altre presenti nella finestra Utilità di pianificazione.

3. Digitare il percorso completo e il nome del file del programma con il quale si desidera avviare l'attività nella casella di testo **Programma** oppure fare clic su **Sfoglia** per individuare il programma sul disco rigido.

   Per impostazione predefinita, l'utilità di pianificazione seleziona VirusScan come programma per l'esecuzione dell'attività e lo individua nel seguente percorso:

   C:\Program Files\Network Associates\McAfee VirusScan\SCAN32.EXE

   Dall'utilità di pianificazione di VirusScan può essere avviato qualsiasi programma eseguibile; tuttavia, è possibile configurare le opzioni di programma soltanto per VirusScan, VShield Aggiornamento automatico e Upgrade automatico. Per ulteriori dettagli, vedere "Configurazione delle opzioni delle attività" a pagina 195.

4. Perché il programma selezionato al Passaggio 3 ricerchi in una particolare cartella i file di dati, i file .INI o altri file richiesti per l'avvio, digitare il percorso della cartella appropriata nella casella di testo **Avvia in** oppure fare clic su **Sfoglia** per individuarlo sul disco rigido. Di solito, un programma ricerca i file necessari nella propria cartella.

5. Digitare qualsiasi parametro che si desidera utilizzare all'avvio del programma. Per la maggior parte dei programmi, i parametri consentiti includono le opzioni disponibili dalla riga di comando o i file che si desidera aprire all'avvio del programma.

6. Selezionare **Finestra normale** dall'elenco **Esegui in** per visualizzare il programma nella relativa finestra predefinita all'avvio. Selezionare **Finestra ingrandita** per espandere la finestra alle massime dimensioni. Selezionare **Finestra ridotta a icona** per ridurre la finestra ad un'icona della barra delle applicazioni.

A questo punto, sono state immesse informazioni sufficienti per creare l'attività, ma non è stata ancora pianificata per eseguire le opzioni di programma selezionate. È possibile:

- Fare clic su **Applica** per salvare le modifiche senza chiudere la finestra di dialogo Proprietà dell'attività, quindi fare clic sulla scheda Pianificazione. Per informazioni sulle modalità di pianificazione di un'attività, vedere "Abilitazione delle attività."

- Fare clic su **OK** per salvare le modifiche e tornare alla finestra Utilità di pianificazione di VirusScan. In seguito sarà necessario pianificare l'attività per l'esecuzione. Per questa operazione, selezionare l'attività dall'elenco nella finestra Utilità di pianificazione, quindi fare clic su  per aprire la finestra di dialogo Proprietà attività.

- Fare clic su **Annulla** per chiudere la finestra di dialogo senza creare un'attività.

Abilitazione delle attività

Abilitare un'attività significa pianificarla e attivare la pianificazione in modo che l'attività venga eseguita quando è necessario. Per eseguire le attività che utilizzano VirusScan, non VShield, per sottoporre a scansione il sistema, è necessario configurare la scansione per l'avvio automatico. Vedere Passaggio 4 a pagina 203 per ulteriori dettagli.

Per abilitare un'attività, procedere come segue:

1. Se non è stata già aperta la finestra di dialogo Proprietà attività, fare doppio clic su una delle attività elencate nella finestra Utilità di pianificazione oppure selezionare un'attività e fare clic su nella barra degli strumenti dell'Utilità di pianificazione.

   Viene visualizzata la finestra di dialogo Proprietà attività (vedere Figura 6-2 a pagina 190). Selezionando VShield, Aggiornamento automatico o Upgrade automatico nell'elenco delle attività dell'Utilità di pianificazione, la finestra di dialogo Proprietà attività avrà un aspetto diverso rispetto a quello visualizzato nella Figura 6-2.

2. Fare clic sulla scheda Pianificazione per visualizzare la pagina delle proprietà appropriata (Figura 6-3).

NOTA: La finestra di dialogo Proprietà attività di VShield non conterrà una pagina delle proprietà Pianificazione, ma includerà schede di stato per ciascuno dei moduli di scansione di VShield. Le finestre di dialogo Proprietà attività di Aggiornamento automatico e Upgrade automatico, invece, non conterranno schede di stato.

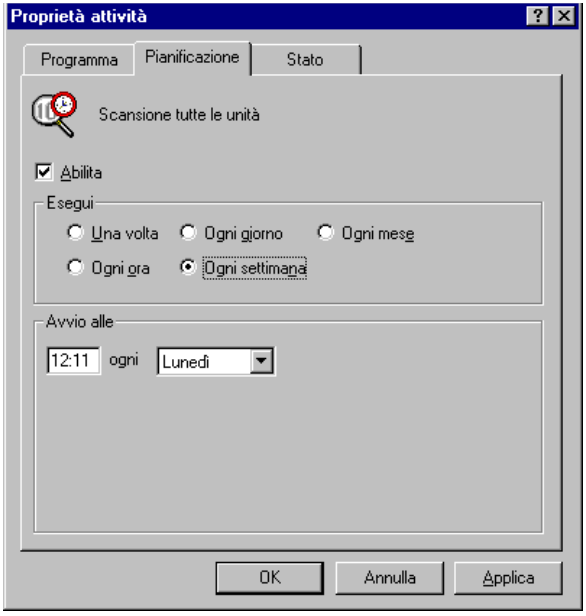

Figura 6-3. Finestra di dialogo Proprietà attività - pagina Pianificazione

3. Selezionare la casella di controllo **Abilita**. Le opzioni nelle aree **Esegui** e **Avvio alle** diventeranno attive.

4. Selezionare la frequenza con la quale eseguire l'attività nell'area **Esegui**. In base all'intervallo selezionato, l'area **Avvio alle** fornisce un insieme diverso di scelte per la pianificazione delle attività. Le scelte sono:

   - **Una volta.** L'attività viene eseguita una sola volta alla data e all'ora specificati. Immettere l'ora nella casella di testo all'estrema sinistra nell'area **Avvio alle**, quindi selezionare un mese dall'elenco a destra. Quindi, immettere la data e l'anno nelle apposite caselle di testo.

   - **Ogni ora.** L'attività viene eseguita ogni ora finché il computer è acceso e l'utilità di pianificazione è in esecuzione. Specificare nell'apposita casella di testo il numero di minuti di attesa dopo ogni ora, prima che l'utilità di pianificazione avvii di nuovo l'attività.

   - **Ogni giorno**. L'attività viene eseguita una sola volta all'ora specificata nei giorni indicati. Immettere l'ora nella casella di testo fornita, quindi selezionare le caselle di controllo per ciascun giorno in cui si desidera avviare l'attività.

   - **Ogni settimana.** L'attività viene eseguita una sola volta ogni settimana al giorno e all'ora specificati. Immettere l'ora nella casella di testo fornita, quindi scegliere un giorno dall'elenco a destra.

   - **Ogni mese.** L'attività viene eseguita una sola volta ogni mese al giorno e all'ora specificati. Immettere l'ora nella casella di testo all'estrema sinistra, quindi immettere il giorno del mese in cui si desidera avviare l'attività.

   NOTA: Immettere tutte le ore pianificate, ad eccezione dell'intervallo tra le ore, utilizzando un formato di 24 ore. Se si desidera eseguire l'attività alle 9:30 della sera, ad esempio, immettere 21:30.

   ---

5. Selezionare la casella di controllo **Esecuzione casuale entro un'ora** per avviare l'attività in un momento qualsiasi entro 60 minuti dall'ora prescelta come ora di esecuzione pianificata. Ad esempio, supponendo che sia stato scelto un intervallo giornaliero e che l'esecuzione dell'attività sia stata impostata alle 1:15 a.m. ogni giorno. Scegliendo questa opzione, si indica all'Utilità di pianificazione di eseguire l'attività in un momento qualsiasi fra la 1:15 a.m. e le 2:14 a.m.

Attivando tale opzione, è possibile creare e distribuire in rete un comune file di configurazione di VirusScan (.VSC), pianificare lo stesso insieme di attività da eseguire contemporaneamente e tuttavia mantenere la quantità di traffico in rete ad un livello gestibile in ogni punto. Non attivando tale opzione, l'utilizzo del medesimo file .VSC in tutti i computer della rete potrebbe determinare la contemporanea attivazione di un'attività di scansione o di aggiornamento su ogni computer, il che andrebbe a discapito della larghezza di banda disponibile della rete.

6. A questo punto è stata pianificata l'attività per l'esecuzione all'ora prevista. Fare clic su **OK** per chiudere la finestra di dialogo Proprietà attività oppure fare clic su **Applica** per salvare le impostazioni senza chiudere la finestra di dialogo. Fare clic su **Annulla** per chiudere la finestra di dialogo senza salvare le modifiche.

NOTA: Per avviare l'attività, il computer deve essere acceso e l'Utilità di pianificazione di VirusScan deve essere in esecuzione. Se il computer è spento o se l'utilità di pianificazione non è in esecuzione al momento in cui l'attività deve essere eseguita, l'attività viene avviata alla successiva ora pianificata. È possibile ridurre ad icona l'utilità di pianificazione in modo da visualizzarla soltanto come icona nella barra delle applicazioni di Windows.

Se si pianifica un'attività di scansione di VirusScan su un computer non assistito, è necessario configurare il programma perché avvii automaticamente l'operazione di scansione. Per ulteriori dettagli, vedere Passaggio 4 a pagina 203.

Verifica dello stato delle attività

La finestra Utilità di pianificazione di VirusScan riporta la data e l'ora dell'ultima esecuzione delle attività e della successiva pianificazione; tali informazioni sono visualizzate a destra di ciascuna attività elencata. Per visualizzare i risultati per ciascuna attività, il numero di file sottoposti a scansione, i file infetti eventualmente rilevati e le azioni intraprese in risposta alle infezioni rilevate, procedere come segue per aprire la finestra di dialogo Proprietà dell'attività alla pagina Stato.

1. Se non è stata già aperta la finestra di dialogo Proprietà dell'attività, fare doppio clic su una delle attività elencate nella finestra Utilità di pianificazione oppure selezionare un'attività e fare clic su  nella barra degli strumenti dell'Utilità di pianificazione.

2. Viene visualizzata la finestra di dialogo Proprietà dell'attività (vedere Figura 6-2 a pagina 190). Fare clic sulla scheda Stato per visualizzare la pagina delle proprietà appropriata (Figura 6-4 a pagina 195).

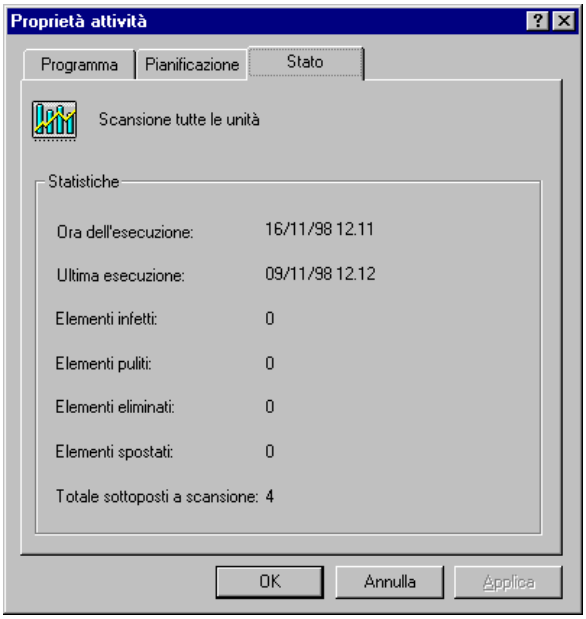

Figura 6-4. Finestra di dialogo Proprietà dell'attività - pagina Stato

La scheda Stato elencherà i risultati dell'ultima operazione di scansione effettuata e il nome dell'ultimo file sottoposto a scansione. Fare clic su **OK** o su **Annulla** per chiudere la finestra di dialogo.

NOTA: La finestra di dialogo Proprietà dell'attività per VShield conterrà le schede Stato per tutti i moduli di scansione di VShield. La finestra di dialogo Proprietà dell'attività per l'Aggiornamento automatico e l'Upgrade automatico non conterrà schede Stato. Per ulteriori informazioni sulle modalità di reperimento delle informazioni di stato di VShield, vedere "Registrazione delle informazioni di stato di VShield" a pagina 150.

Configurazione delle opzioni delle attività

Quando si crea e pianifica un'attività, l'Utilità di pianificazione di VirusScan eseguirà il programma specificato nella finestra di dialogo Proprietà dell'attività con un insieme predefinito di opzioni. Nella maggior parte dei casi, questo insieme predefinito sarà in grado di fornire al computer una protezione sufficiente dai virus e da altri programmi software sospetti o aggiornerà i file di dati dal server corretto, ma è possibile selezionare opzioni personalizzate che rispondano al meglio alle esigenze lavorative e di sicurezza dell'utente.

NOTA: È possibile utilizzare l'utilità di pianificazione per configurare soltanto il componente VirusScan. Per configurare qualsiasi programma software che si desidera eseguire con l'utilità di pianificazione, è necessario utilizzare gli strumenti appropriati per configurare separatamente tali programmi. Per i dettagli, consultare la documentazione relativa al software.

Di solito, VirusScan viene utilizzato per eseguire le attività di scansione pianificate. Sebbene sia possibile configurare VShield per eseguire varie attività di scansione, non è possibile specificarne i tempi di esecuzione: VShield viene eseguito all'avvio del computer e interrotto alla chiusura del sistema. VShield può essere disabilitato e abilitato nuovamente nell'Utilità di pianificazione, ma non è possibile creare una seconda attività VShield.

Configurazione di VirusScan per la scansione pianificata

Perché VirusScan esegua una scansione pianificata, è necessario indicare gli elementi da sottoporre a scansione e quelli da ignorare, le azioni da intraprendere e le modalità di avviso in caso di rilevamento di virus. È possibile anche specificare che venga conservato un record delle azioni intraprese e impedire che vengano modificate le impostazioni. Una serie di pagine delle proprietà consente di controllare le opzioni di ciascuna attività: fare clic su ciascuna scheda nella finestra di dialogo Proprietà di McAfee VirusScan per impostare VirusScan per l'esecuzione dell'attività.

Per gestire le pagine delle proprietà di VirusScan, selezionare una delle attività di scansione elencate nella finestra Utilità di pianificazione, quindi fare clic su  nella barra degli strumenti dell'Utilità di pianificazione.

NOTA: L'attività selezionata deve essere configurata per l'esecuzione di VirusScan. È possibile modificare una delle attività predefinite o configurare l'attività creata. Per informazioni sulle modalità di definizione dei programmi che eseguiranno le attività di scansione, vedere "Creazione di nuove attività" a pagina 189.

Viene visualizzata la pagina di dialogo Proprietà di McAfee VirusScan (Figura 6-5).

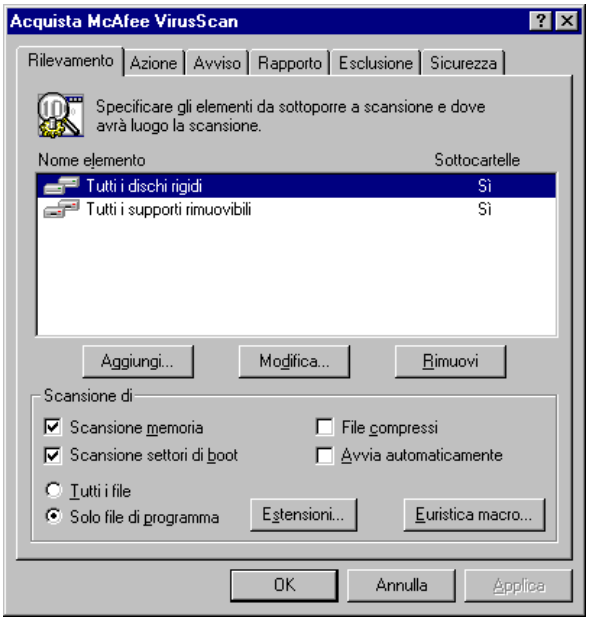

Figura 6-5. Finestra di dialogo Proprietà di VirusScan - pagina Rilevamento

Scelta delle opzioni di rilevamento

Se si decide di configurare un'attività appena creata, VirusScan inizialmente presume che l'utente desideri effettuare una scansione dell'unità C: e della memoria del computer, per rilevare eventuali virus nei settori di boot e limitare la scansione soltanto a quei file che possono essere colpiti da infezione da virus. Se si decide di configurare una delle attività predefinite, le opzioni iniziali potranno variare.

Per modificare le opzioni iniziali delle attività, procedere come segue:

1. Selezionare le parti del sistema o della rete che si desidera siano sottoposte a scansione da VirusScan. È possibile:

   - **Aggiungere obiettivi da sottoporre a scansione.** Fare clic su **Aggiungi** per aprire la finestra di dialogo Aggiungi elemento di scansione (Figura 6-6).

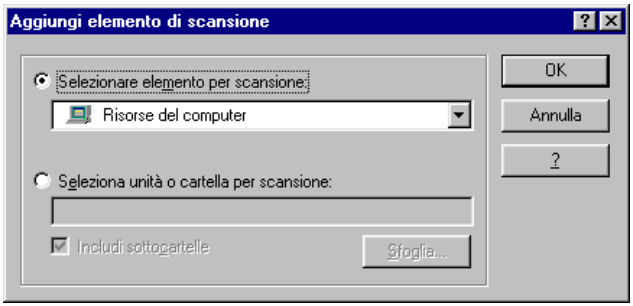

Figura 6-6. Finestra di dialogo Aggiungi elemento di scansione

Perché VirusScan esamini tutto il computer oppure un sottoinsieme di unità del sistema o della rete, fare clic sul pulsante **Seleziona elemento per scansione**, quindi selezionare l'obiettivo di scansione dall'elenco fornito. Le scelte disponibili sono:

- **Risorse del computer.** VirusScan sottopone a scansione tutte le unità collegate fisicamente al computer o mappate logicamente mediante Gestione risorse di Windows ad una lettera di unità sul computer.
- **Tutti i supporti rimovibili.** VirusScan sottopone a scansione soltanto i dischi CD, le cartucce Syquest e Iomega o i supporti di memorizzazione simili collegati fisicamente al computer.
- **Tutti i dischi rigidi.** VirusScan sottopone a scansione i dischi rigidi collegati fisicamente al computer.
- **Tutte le unità di rete.** VirusScan sottopone a scansione tutte le unità mappate logicamente mediante Gestione risorse di Windows ad una lettera di unità sul computer.

Per far sì che VirusScan esamini un particolare disco o cartella del sistema, fare clic sul pulsante **Seleziona unità o cartella per scansione**. Quindi, digitare nella casella di testo fornita la lettera di unità o il percorso alla cartella che si desidera sottoporre a scansione oppure fare clic su **Sfoglia** per localizzare l'obiettivo di scansione sul computer. Selezionare la casella di controllo **Includi sottocartelle** per consentire a VirusScan di rilevare i virus anche nelle cartelle contenute nell'obiettivo di scansione. Per chiudere la finestra di dialogo, fare clic su **OK** .

- **Modificare gli obiettivi di scansione.** Selezionare uno degli obiettivi di scansione elencati, quindi fare clic su **Modifica** per aprire la finestra di dialogo Modifica elemento di scansione (Figura 6-7).

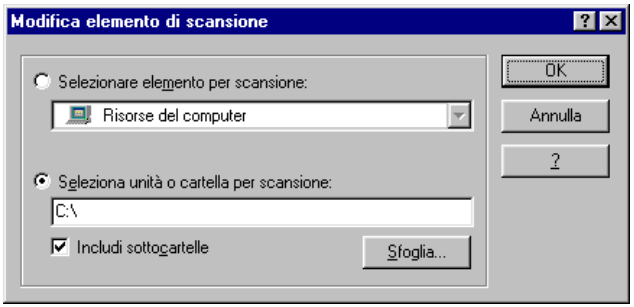

Figura 6-7. Finestra di dialogo Modifica elemento di scansione

Viene visualizzata la finestra di dialogo con l'obiettivo di scansione esistente specificato. Selezionare o immettere un nuovo obiettivo di scansione, quindi fare clic su **OK** per chiudere la finestra di dialogo.

- **Rimuovere gli obiettivi di scansione.** Selezionare uno degli obiettivi di scansione elencati, quindi fare clic su **Rimuovi** per eliminarlo.

2. Specificare il tipo di file che si desidera VirusScan sottoponga a scansione. È possibile:

   - **Eseguire la scansione di file compressi.** Selezionare la casella di controllo **File compressi** per consentire a VirusScan di cercare i virus nei file compressi con i seguenti formati: .??_, .CAB, LZEXE, LZH, PKLite, .TD0 e .ZIP. Nonostante garantisca una maggiore protezione, la scansione di file compressi dilata i tempi necessari a tale operazione.

- **Scegliere il tipo di file da sottoporre a scansione.** Normalmente i virus non sono in grado di attaccare i file di dati o i file che non contengono un codice eseguibile. Per questa ragione è possibile limitare le operazioni di scansione solo ai file maggiormente esposti alle infezioni dei virus, in modo da velocizzare le operazioni di scansione. A tal fine, selezionare il pulsante **Solo file di programma**. Per visualizzare o indicare le estensioni dei nomi file che saranno analizzati da VirusScan, fare clic su **Estensioni** per aprire la finestra di dialogo Estensioni file di programma (Figura 6-8).

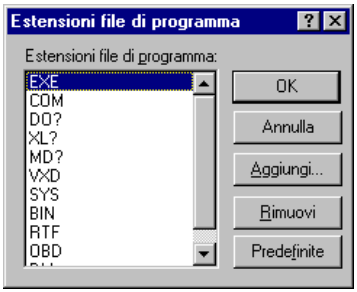

Figura 6-8. Finestra di dialogo Estensioni file di programma

Per impostazione predefinita, VirusScan cerca i virus nei file con le estensioni .EXE, .COM, .DO?, .XL?, .RTF, .BIN, .SYS, .MD?, .VXD, .OBD e .DLL. I file con estensione .DO?, .XL?, .RTF e .OBD sono file di Microsoft Office. Tutti questi file possono essere infettati da virus macro. Il ? è un carattere jolly che abilita la scansione di file di documento e di modello da parte di VirusScan.

- Per aggiungere estensioni all'elenco, fare clic su **Aggiungi**, quindi digitare le estensioni dei file che si desidera VirusScan sottoponga a scansione nella finestra di dialogo visualizzata.
- Per eliminare un'estensione dall'elenco, selezionarla, quindi fare clic su **Rimuovi**.
- Fare clic su **Predefinite** per ripristinare l'elenco nella sua forma originaria.

Al termine, scegliere **OK** per chiudere la finestra di dialogo.

Per far sì che VirusScan esamini tutti i file sul sistema, indipendentemente dall'estensione, selezionare il pulsante **Tutti i file**. Questa operazione rallenta notevolmente il sistema, ma garantisce la completa eliminazione dei virus.

- **Attivare la scansione euristica**. Fare clic su **Euristica macro** per aprire la finestra di dialogo Impostazioni di scansione dell'euristica della macro (Figura 6-9).

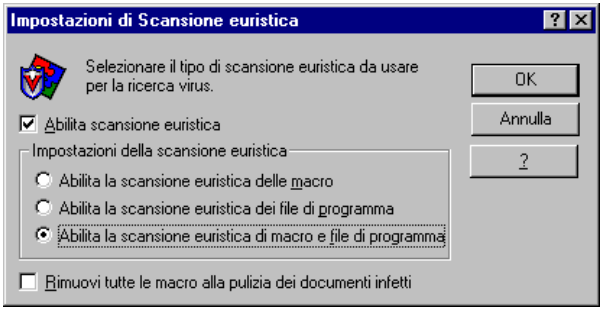

Figura 6-9. Finestra di dialogo Impostazioni di scansione dell'euristica della macro

La tecnologia di scansione euristica consente a VirusScan di riconoscere nuovi virus macro in base alla loro somiglianza con virus simili già conosciuti. A tal fine, il programma cerca le caratteristiche di "virus simili" in file già sottoposti a scansione. La presenza di un numero sufficiente di tali caratteristiche consente a VirusScan di identificare il file come potenzialmente infetto da un nuovo virus o da uno precedentemente non identificato.

Poiché VirusScan ricerca simultaneamente le caratteristiche dei file che escludono la possibilità di infezione da virus, raramente darà indicazioni errate su un'infezione da virus. Quindi, a meno che non si sia certi che il file *non* contiene un virus, trattare le infezioni "probabili" con la stessa attenzione richiesta dalle infezioni certe.

Per attivare la scansione euristica, procedere come segue:

a. Selezionare la casella di controllo **Abilita scansione euristica macro**. Vengono attivate le altre opzioni della finestra di dialogo.

b. Selezionare il tipo di scansione euristica che si desidera che VirusScan utilizzi. Le scelte disponibili sono:

- **Abilita scansione euristica macro**. Scegliere questa opzione per consentire a VirusScan di identificare tutti i file di Microsoft Word, Microsoft Excel e altri file di Microsoft Office che presentano macro incorporate e quindi di confrontare il codice macro con il database di firme virus. VirusScan identifica le corrispondenze esatte in base al nome del virus; le firme in codice che somigliano a virus esistenti consentono a VirusScan di segnalare la presenza di un "probabile" virus macro.
- **Attiva scansione euristica del file di programma.** Scegliere questa opzione per consentire a VirusScan di individuare nuovi virus nei file di programma esaminandone le caratteristiche e confrontandole con l'elenco delle caratteristiche dei virus noti. VirusScan identificherà i file con un numero sufficiente di queste caratteristiche come virus probabili.
- **Attiva scansione euristica dei file di programma e di macro.** Scegliere questa opzione per consentire a VirusScan di utilizzare entrambi i tipi di scansione euristica. Network Associates consiglia di utilizzare questa opzione per una protezione antivirus completa.

c. Determinare la modalità di trattamento dei file macro infetti. Selezionare **Rimuovi tutte le macro alla pulizia dei documenti infetti** per eliminare tutti i codici infetti dal documento e lasciare solo i dati. Per rimuovere solo il codice virus dalle macro del documento, non selezionare questa casella di controllo.

> **AVVERTENZA:** Utilizzare questa funzione con cautela: la rimozione di tutte le macro da un documento può provocare la perdita o il danneggiamento dei dati e l'impossibilità di utilizzarli.

d. Fare clic su **OK** per salvare le impostazioni personalizzate e tornare alla finestra di dialogo Proprietà di McAfee VirusScan.

3. Selezionare altre opzioni di scansione. I virus che colpiscono i settori di boot vengono caricati nella memoria del computer e si annidano nei blocchi di boot o nel record di avvio principale del disco rigido locale. Per rilevare questi virus, selezionare le caselle di controllo **Scansione memoria** e **Scansione settori di boot**.

4. Se sono state pianificate operazioni di scansione da eseguire in modalità non assistita, selezionare la casella di controllo **Avvia automaticamente** perché VirusScan possa iniziare la scansione subito dopo essere stato avviato. Se non si seleziona questa casella di controllo, l'utilità di pianificazione avvia VirusScan, ma VirusScan attenderà la selezione dell'opzione **Avvia scansione** prima di avviare la scansione. Se la casella di controllo non viene selezionata, è possibile annullare l'operazione di scansione se questa interferisce con l'attività dell'utente.

5. Fare clic sulla scheda Azione per scegliere le opzioni aggiuntive di VirusScan. Per salvare le modifiche senza chiudere la finestra di dialogo delle proprietà di VirusScan, fare clic su **Applica**. Per salvare le modifiche e ritornare alla finestra Utilità di pianificazione, fare clic su **OK**. Per tornare alla finestra Utilità di pianificazione senza salvare le modifiche, fare clic su **Annulla**.

> **NOTA:** Facendo clic su **Annulla** non sarà possibile ripristinare le modifiche già salvate se si è fatto clic su **Applica**.

Scelta delle opzioni di azione

Quando VirusScan rileva un virus può chiedere all'utente quale operazione eseguire sul virus infetto, oppure può eseguire automaticamente un'azione precedentemente impostata. Utilizzare la pagina delle proprietà Azione per specificare le opzioni di risposta o le azioni che si desidera VirusScan esegua quando rileva un virus.

Procedere come segue:

1. Per l'avvio dalla finestra Utilità di pianificazione, selezionare l'attività creata nel relativo elenco, quindi fare clic su  nella barra degli strumenti dell'Utilità di pianificazione.

2. Viene visualizzata la finestra di dialogo Proprietà di McAfee VirusScan (vedere Figura 6-5 a pagina 197). Fare clic sulla scheda Azione per visualizzare la pagina delle proprietà appropriata (Figura 6-10 a pagina 204).

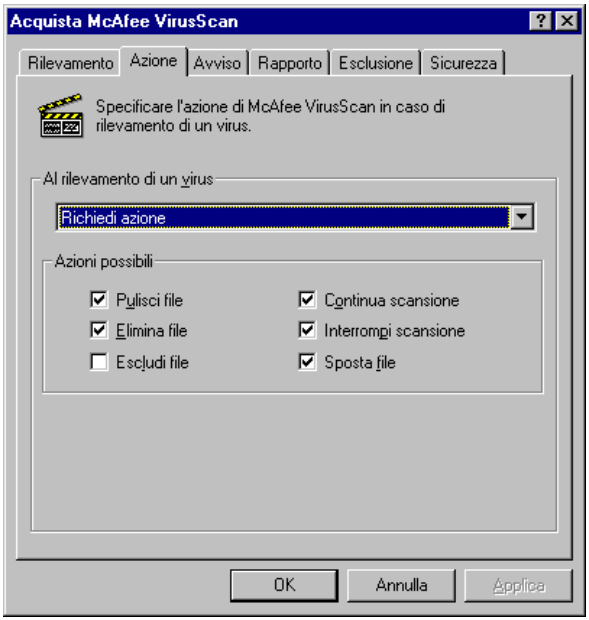

Figura 6-10. Finestra di dialogo Proprietà di VirusScan - pagina Azione

3. Per definire il tipo di risposta da parte di VirusScan qualora rilevasse un virus, selezionare una risposta dall'elenco **Al rilevamento di un virus**. L'area immediatamente al di sotto dell'elenco cambia per visualizzare opzioni aggiuntive per ciascuna selezione. Le scelte disponibili sono:

   - **Richiedi azione.** Utilizzare quest'opzione se si prevede di assistere all'operazione di scansione eseguita da VirusScan—il programma visualizza un messaggio di avviso quando rileva un virus e offre all'utente una gamma di risposte disponibili. Selezionare le opzioni di risposta che si desidera visualizzare nel messaggio di avviso:

     – **Pulisci file.** Questa opzione indica a VirusScan di tentare di rimuovere il codice del virus dal file infetto.

     – **Elimina file.** Questa opzione indica a VirusScan di eliminare immediatamente il file infetto.

     – **Escludi file.** Questa opzione indica a VirusScan di tralasciare il file durante le operazioni di scansione successive. Questa è l'unica opzione non selezionata per impostazione predefinita.

  - **Continua scansione.** Questa opzione indica a VirusScan di continuare la scansione senza intraprendere alcun'altra azione. Se è stata abilitata l'opzione per la registrazione degli eventi, VirusScan registra l'infezione rilevata nel file di registro.
  - **Interrompi scansione.** Questa opzione indica a VirusScan di interrompere l'operazione di scansione immediatamente. Per continuare, avviare nuovamente l'operazione dall'utilità di pianificazione o da VirusScan.
  - **Sposta file.** Questa opzione indica a VirusScan di spostare il file infetto in una cartella di quarantena.

- **Sposta file infetti automaticamente**. Utilizzare questa opzione per consentire a VirusScan di spostare i file infetti in una directory di quarantena appena ne rileva la presenza. In base alle impostazioni predefinite, VirusScan sposta questi file in una cartella denominata INFECTED (infetti), creata al livello principale dell'unità in cui viene rilevata la presenza del virus. Ad esempio, se VirusScan rileva un file infetto in T:\MY DOCUMENTS e si è specificato INFECTED come directory di quarantena, VirusScan copierà il file in T:\INFECTED.

  È possibile immettere un nome diverso nella casella di testo fornita, o fare clic su **Sfoglia** per individuare una cartella adeguata sul disco rigido.

- **Pulisci file infetti automaticamente.** Utilizzare questa opzione per comunica a VirusScan di rimuovere il codice del virus dal file infetto appena ne rileva la presenza. Se VirusScan non può rimuovere il virus, avverte l'utente nella sua area di messaggio e, se le funzioni di notifica sono attivate, prende nota del virus nel suo file di registro. Per ulteriori dettagli, vedere "Scelta delle opzioni di rapporto" a pagina 208.

- **Elimina file infetti automaticamente.** Utilizzare questa opzione per indicare a VirusScan di eliminare immediatamente i file infetti rilevati. Attivare la funzione di notifica in modo da registrare i file eliminati da VirusScan. Sarà necessario ripristinare i file eliminati da copie di backup.

- **Continua scansione.** Utilizzare questa opzione solo se si prevede di non assistere alle operazioni di scansione di VirusScan. Se viene attivata anche la funzione di notifica di VirusScan (vedere "Scelta delle opzioni di rapporto" a pagina 208 per i dettagli), il programma registra il nome dei virus rilevati e il nome dei file infetti in modo tale che sia possibile eliminarli alla prima occasione.

4. Fare clic sulla scheda Avviso per scegliere le opzioni aggiuntive di VirusScan. Per salvare le modifiche senza chiudere la finestra di dialogo delle proprietà di VirusScan, fare clic su **Applica**. Per salvare le modifiche e ritornare alla finestra Utilità di pianificazione, fare clic su **OK**. Per tornare alla finestra Utilità di pianificazione senza salvare le modifiche, fare clic su **Annulla**.

   NOTA: Facendo clic su **Annulla** non sarà possibile ripristinare le modifiche già salvate se si è fatto clic su **Applica**.

Scelta delle opzioni di avviso

Una volta configurato con le opzioni di risposta desiderate, VirusScan ricerca ed elimina i virus dal sistema automaticamente, appena ne rileva la presenza, senza ulteriori interventi da parte dell'utente. Tuttavia, se l'utente desidera che VirusScan lo informi immediatamente quando rileva un virus per agire in modo appropriato, è possibile configurarlo in diversi modi. Utilizzare la pagina delle proprietà Avviso per scegliere i metodi di avviso che si desidera utilizzare.

Procedere come segue:

1. Per l'avvio dalla finestra Utilità di pianificazione, selezionare l'attività creata nel relativo elenco, quindi fare clic su  nella barra degli strumenti dell'Utilità di pianificazione.

2. Viene visualizzata la finestra di dialogo Proprietà di McAfee VirusScan (vedere Figura 6-5 a pagina 197). Fare clic sulla scheda Avviso per visualizzare la pagina delle proprietà appropriata (Figura 6-11 a pagina 207).

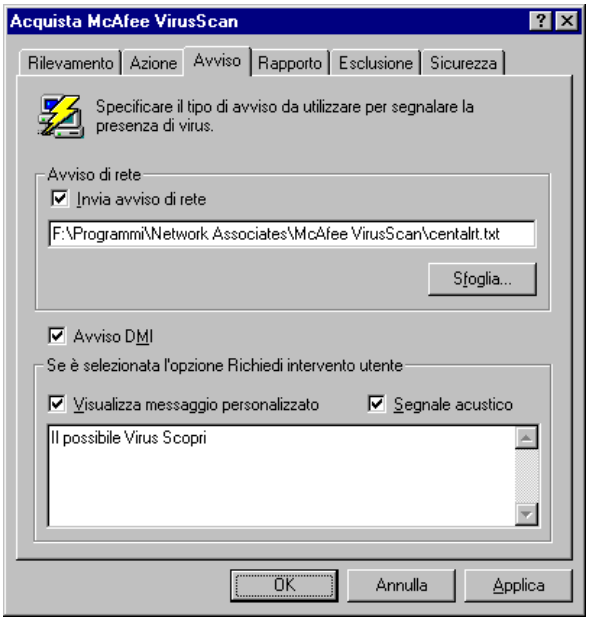

Figura 6-11. Finestra di dialogo Proprietà di VirusScan - pagina Avviso

3. Per indicare a VirusScan di inviare un messaggio di avviso ad un server che esegue NetShield, la soluzione antivirus di Network Associates per i server, selezionare la casella di controllo **Invia avviso di rete**, quindi immettere il percorso per la cartella di avviso di NetShield nella rete, oppure fare clic su **Sfoglia** per individuare la cartella appropriata.

   NOTA: La cartella scelta deve contenere CENTALRT.TXT, il file di avviso centralizzato di NetShield. NetShield raccoglie i messaggi di avviso inviati da VirusScan e da altri programmi Network Associates, quindi li trasferisce agli amministratori di rete perché intraprendano le azioni necessarie. Per ulteriori informazioni sull'Avviso centralizzato, consultare il *Manuale dell'utente* di NetShield.

   ---

4. Per consentire a VirusScan di inviare messaggi di avviso di virus attraverso l'interfaccia del componente DMI alle applicazioni del desktop e di gestione della rete in esecuzione, selezionare la casella di controllo **Avviso DMI**.

> **NOTA:** DMI (Desktop Management Interface) è uno standard per la comunicazione di richieste di gestione e informazioni di avviso tra i componenti hardware e software dei computer o collegati ad essi e le applicazioni utilizzate per la loro gestione. Per ulteriori informazioni sul metodo di avviso, contattare l'amministratore della rete.

5. Se si sceglie **Richiedi azione** come risposta nella pagina Azione (vedere "Scelta delle opzioni di azione" a pagina 203 per i dettagli), è possibile anche indicare a VirusScan di emettere un segnale acustico e visualizzare un messaggio personalizzato al rilevamento di un virus. Per effettuare quest'operazione, selezionare la casella di controllo **Visualizza messaggio personalizzato**, quindi digitare il messaggio che si desidera visualizzare nella relativa casella di testo: è possibile digitare fino a 225 caratteri. Selezionare quindi la casella di controllo **Segnale acustico**.

6. Fare clic sulla scheda Rapporto per scegliere le opzioni aggiuntive di VirusScan. Per salvare le modifiche senza chiudere la finestra di dialogo delle proprietà di VirusScan, fare clic su **Applica**. Per salvare le modifiche e ritornare alla finestra Utilità di pianificazione, fare clic su **OK**. Per tornare alla finestra Utilità di pianificazione senza salvare le modifiche, fare clic su **Annulla**.

> **NOTA:** Facendo clic su **Annulla** non sarà possibile ripristinare le modifiche già salvate se si è fatto clic su **Applica**.

Scelta delle opzioni di rapporto

VirusScan elenca le impostazioni correnti e riassume tutte le azioni eseguite durante le operazioni di scansione in un file di registro denominato VSCLOG.TXT. VirusScan può registrare i virus in questo file, oppure è possibile utilizzare qualunque editor di testi per creare un file di testo utilizzato da VirusScan. Quindi è possibile aprire e stampare il file di registro per visionarlo successivamente da VirusScan o da un editor di testo.

Il file VSCLOG.TXT può essere utilizzato come importante strumento di gestione per controllare l'attività dei virus nel sistema e prendere nota delle impostazioni utilizzate per rilevare e rispondere alle infezioni rilevate da VirusScan. È possibile anche utilizzare il rapporto degli incidenti registrati nel file per determinare quali file è necessario sostituire dalle copie di backup, esaminare in quarantena, o eliminare dal computer. Utilizzare la pagina delle proprietà Rapporto per determinare le informazioni da includere nel file di registro di VirusScan.

Per impostare VirusScan per la registrazione delle azioni in un file di registro, procedere come segue:

1. Per l'avvio dalla finestra Utilità di pianificazione, selezionare l'attività creata nel relativo elenco, quindi fare clic su nella barra degli strumenti dell'Utilità di pianificazione.

2. Viene visualizzata la finestra di dialogo Proprietà di McAfee VirusScan (vedere Figura 6-5 a pagina 197). Fare clic sulla scheda Rapporto per visualizzare la pagina delle proprietà appropriata (Figura 6-12).

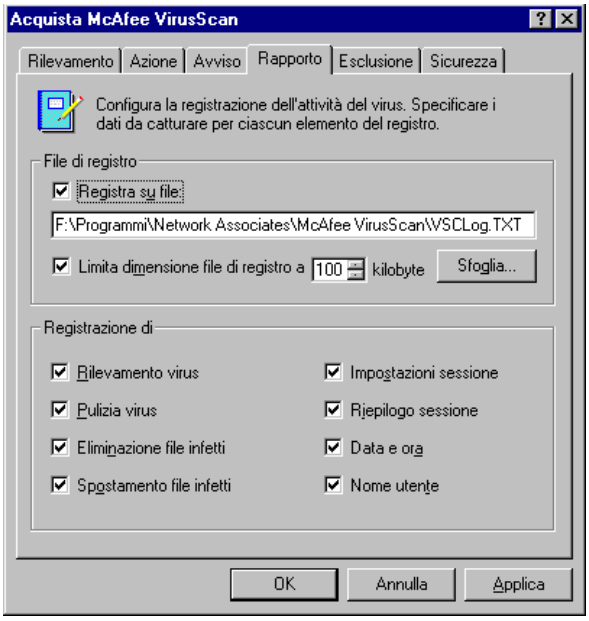

Figura 6-12. Proprietà di VirusScan - pagina Rapporto

3. Selezionare la casella di controllo **Registra su file**.

   In base alle impostazioni predefinite, VirusScan scrive le informazioni di registro nel file VSCLOG.TXT nella directory di programma di VirusScan. É possibile digitare un nome diverso nella relativa casella di testo o fare clic su **Sfoglia** per individuare un file adatto in un'altra directory sul disco rigido o in rete.

4. Per ridurre al minimo le dimensioni del file di registro, selezionare la casella di controllo **Limita dimensione file di registro a**, quindi immettere un valore per le dimensioni del file, in kilobyte, nella relativa casella di testo.

Immettere un valore compreso tra 10KB e 999KB. In base alle impostazioni predefinite, VirusScan limita la dimensione del file a 100KB. Se i dati nel file di registro superano le dimensioni del file impostate, VirusScan cancella la registrazione esistente e ricomincia dal punto in cui ha smesso.

5. Selezionare le caselle di controllo corrispondenti alle informazioni che si desidera VirusScan registri nel file di registro. Si può scegliere di registrare tutte le seguenti informazioni:

   - **Rilevamento virus.** Selezionare questa casella di controllo perché VirusScan riporti il numero dei file infetti rilevati durante la sessione di scansione.
   - **Pulizia virus.** Selezionare questa casella di controllo perché VirusScan riporti il numero dei file infetti dai quali ha rimosso il virus.
   - **Eliminazione file infetti.** Selezionare questa casella di controllo per indicare a VirusScan di annotare il numero dei file infetti eliminati dal sistema.
   - **Spostamento file infetti.** Selezionare questa casella di controllo perché VirusScan riporti il numero dei file infetti spostati nella directory di quarantena.
   - **Impostazioni sessione.** Selezionare questa casella di controllo perché VirusScan riporti le opzioni selezionate nella finestra di dialogo Proprietà McAfee VirusScan per ogni sessione di scansione.
   - **Riepilogo sessione.** Selezionare questa casella di controllo perché VirusScan riassuma le azioni eseguite durante ciascuna sessione di scansione. Le informazioni di riepilogo includono il numero di file sottoposti a scansione, il numero e il tipo di virus rilevati, il numero di file spostati o eliminati e altre informazioni.
   - **Data e ora.** Selezionare questa casella di controllo perché VirusScan riporti la data e l'ora di ciascuna voce annotata nel file di registro.
   - **Nome utente.** Selezionare questa casella di controllo perché VirusScan riporti il nome dell'utente utilizzato per il collegamento al computer nel momento della registrazione delle voci nel file di registro.

Per visualizzare il contenuto del file di registro dell'Utilità di pianificazione di VirusScan, selezionare l'attività creata nell'elenco delle attività, quindi scegliere **Visualizza registro attività** dal menu **Attività**. È inoltre possibile avviare VirusScan e selezionare **Visualizza registro attività** dal menu **File**. Per ulteriori informazioni, consultare "Uso dei menu di VirusScan" a pagina 155.

6. Fare clic sulla scheda Esclusione per scegliere le opzioni aggiuntive di VirusScan. Per salvare le modifiche senza chiudere la finestra di dialogo delle proprietà di VirusScan, fare clic su **Applica**. Per salvare le modifiche e tornare alla finestra Utilità di pianificazione, fare clic su **OK**. Per tornare alla finestra Utilità di pianificazione senza salvare le modifiche, fare clic su **Annulla**.

> **NOTA:** Facendo clic su **Annulla** non vengono ripristinate le modifiche salvate facendo clic su **Applica**.

Scelta delle opzioni di esclusione

Molti dei file memorizzati nel computer non sono vulnerabili a infezioni da virus. Le operazioni di scansione che esaminano questi file possono richiedere molto tempo e produrre scarsi risultati. È possibile accelerare le operazioni di scansione indicando a VirusScan di cercare solo i tipi di file esposti (vedere "Scelta delle opzioni di rilevamento" a pagina 197 per i dettagli), oppure indicando a VirusScan di ignorare interi file o cartelle sicuramente immuni da virus.

Una volta eseguita la scansione completa del sistema, è possibile escludere i file e le cartelle che non si modificano o che non sono normalmente esposti a infezioni da virus. È possibile anche fare affidamento su VShield per assicurare la protezione tra le operazioni di scansione pianificate. Operazioni di scansione eseguite regolarmente, con l'esame di tutte le aree del computer, forniscono la migliore protezione dai virus.

Per escludere file o cartelle dalle operazioni di scansione, procedere come segue:

1. Per l'avvio dalla finestra Utilità di pianificazione, selezionare l'attività creata nel relativo elenco, quindi fare clic su  nella barra degli strumenti dell'Utilità di pianificazione.

2. Viene visualizzata la finestra di dialogo Proprietà di McAfee VirusScan (vedere Figura 6-5 a pagina 197). Fare clic sulla scheda Esclusione per visualizzare la pagina delle proprietà appropriata. (Figura 6-13).

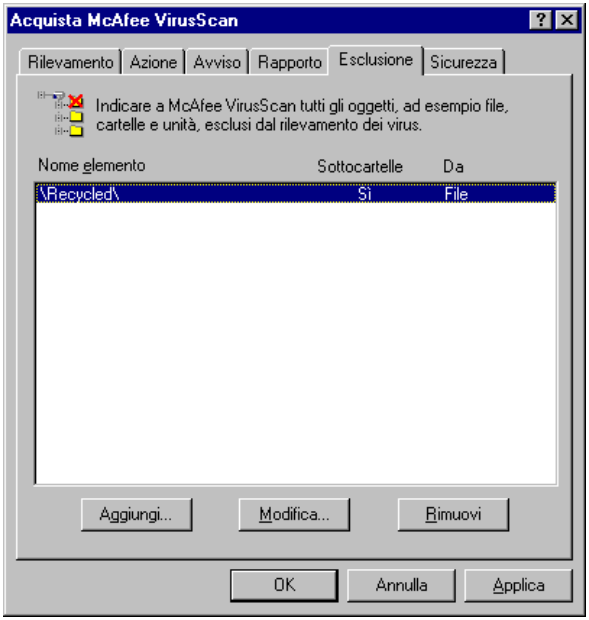

Figura 6-13. Finestra di dialogo Proprietà di VirusScan - pagina Esclusione

La pagina Esclusione elenca inizialmente solo il contenuto del cestino. VirusScan esclude il cestino dalle operazioni di scansione perché Windows non esegue i file memorizzati in quest'area.

3. Specificare gli elementi che si desidera escludere. È possibile:

   - **Aggiungere all'elenco di esclusione file, cartelle o volumi.** Fare clic su **Aggiungi** per aprire la finestra di dialogo Aggiungi elemento di esclusione (Figura 6-14 a pagina 213).

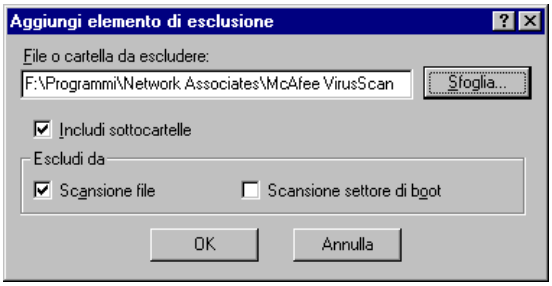

Figura 6-14. Finestra di dialogo Aggiungi elemento di esclusione

a. Digitare il volume, il percorso del file o il percorso della cartella che si desidera escludere dalla scansione o fare clic su **Sfoglia** per localizzare il file o la cartella sul proprio computer.

> **NOTA:** Se si è scelto di spostare automaticamente i file infetti in una cartella di quarantena, il programma esclude tale cartella dalle operazioni di scansione.

b. Selezionare la casella di controllo **Includi sottocartelle** per escludere dalla scansione tutte le sottocartelle interne alla cartella specificata.

c. Selezionare la casella di controllo **Scansione file** affinché VirusScan non ricerchi i virus nei file o nelle cartelle escluse.

d. Selezionare la casella di controllo **Scansione settore di boot** affinché VirusScan non ricerchi virus nei settori di boot dei file o delle cartelle escluse. Utilizzare questa opzione per escludere dalle operazioni di scansione i file di sistema, come ad esempio COMMAND.COM.

> **AVVERTENZA:** Network Associates consiglia di *non* escludere i file di sistema dalla scansione per la ricerca di virus.

e. Per salvare le modifiche apportate e chiudere la finestra di dialogo, fare clic su **OK**.

f. Ripetere i punti da a. a d. fino a quando non sono stati elencati tutti i file e le cartelle che non si desidera sottoporre a scansione.

- **Modificare l'elenco di esclusione.** Per modificare le impostazioni per un elemento di esclusione, selezionare l'elemento dall'elenco quindi fare clic su **Modifica** per aprire la finestra di dialogo Modifica elemento di esclusione. Effettuare le modifiche desiderate, quindi fare clic su **OK** per chiudere la finestra di dialogo.
- **Rimuovere un elemento dall'elenco.** Per eliminare un elemento escluso, selezionarlo nell'elenco, quindi fare clic su **Rimuovi**. VirusScan effettuerà la scansione di questo file o cartella durante la successiva operazione di scansione.

4. Fare clic sulla scheda Sicurezza per scegliere le opzioni aggiuntive di VirusScan. Per salvare le modifiche senza chiudere la finestra di dialogo delle proprietà di VirusScan, fare clic su **Applica**. Per salvare le modifiche e tornare alla finestra Utilità di pianificazione, fare clic su **OK**. Per tornare alla finestra Utilità di pianificazione senza salvare le modifiche, fare clic su **Annulla**.

NOTA: Facendo clic su **Annulla** non vengono ripristinate le modifiche salvate facendo clic su **Applica**.

Scelta delle opzioni di sicurezza

VirusScan consente di impostare una password per proteggere da modifiche non autorizzate le impostazioni scelte in ciascuna pagina delle proprietà. Questa funzione si rivela particolarmente utile per gli amministratori di sistema che non intendono consentire agli utenti eventuali variazioni alle misure di sicurezza modificando le impostazioni di VirusScan. Utilizzare la pagina delle proprietà Sicurezza per bloccare le proprie impostazioni.

Procedere come segue:

1. Per l'avvio dalla finestra Utilità di pianificazione, selezionare l'attività creata nel relativo elenco, quindi fare clic su  nella barra degli strumenti dell'Utilità di pianificazione.

2. Viene visualizzata la finestra di dialogo Proprietà di McAfee VirusScan (vedere Figura 6-5 a pagina 197). Fare clic sulla scheda Sicurezza per visualizzare la pagina delle proprietà appropriata. (Figura 6-15).

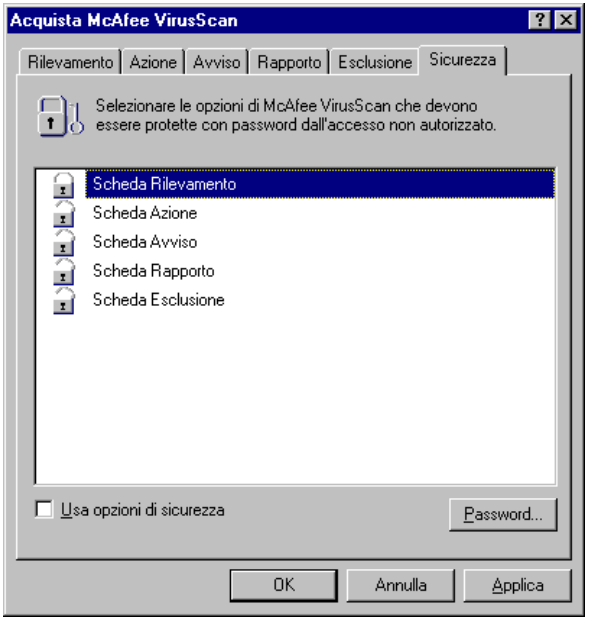

Figura 6-15. Finestra di dialogo Proprietà di VirusScan - pagina Sicurezza

3. Dall'elenco visualizzato, selezionare le impostazioni che si desidera proteggere.

   È possibile proteggere qualsiasi pagina o tutte le pagine delle proprietà di VirusScan. Le pagine delle proprietà protette visualizzano l'icona di un lucchetto chiuso nell'elenco di sicurezza rappresentato nella Figura 6-15. Per rimuovere la protezione da una pagina delle proprietà, fare clic sull'icona del lucchetto per sbloccarla.

4. Fare clic su **Password** per aprire la finestra di dialogo Specifica password (Figura 6-16 a pagina 216).

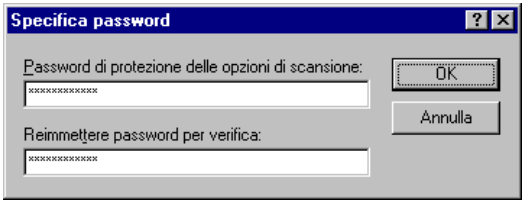

Figura 6-16. Finestra di dialogo Specifica password

a. Immettere una password nella prima casella di testo visualizzata, quindi immettere nuovamente la password nella casella di testo sottostante per confermare la scelta.

b. Fare clic su **OK** per chiudere la finestra di dialogo Specifica password.

5. Se si desidera creare altre attività di scansione copiando questa (per i dettagli, vedere pagina 186), è possibile assicurarsi che le impostazioni di sicurezza compaiano come impostazione predefinita nell'attività copiata selezionando la casella di controllo **Applica opzioni di sicurezza**. Se si configura l'attività Scansione predefinita con questa opzione, tutte le nuove attività create selezionando **Nuova attività** dal menu **Attività** o facendo clic su  acquisiranno le impostazioni di sicurezza scelte per l'attività Scansione predefinita.

6. Fare clic su una scheda diversa per modificare alcune impostazioni di VirusScan. Per salvare le modifiche senza chiudere la finestra di dialogo delle proprietà di VirusScan, fare clic su **Applica**. Per salvare le modifiche e tornare alla finestra Utilità di pianificazione, fare clic su **OK**. Per tornare alla finestra Utilità di pianificazione senza salvare le modifiche, fare clic su **Annulla**.

NOTA: Facendo clic su **Annulla** non vengono ripristinate le modifiche salvate facendo clic su **Applica**.

Configurazione delle opzioni di Aggiornamento automatico

Per funzionare al massimo dell'efficienza, VirusScan necessita della regolare immissione dei file di definizione dei nuovi virus, di aggiornamenti del database relativi a oggetti e a siti Internet pericolosi e di altri aggiornamenti tecnici. In mancanza di file aggiornati, VirusScan non sarebbe in grado di individuare nuove forme di software dannoso o di rilevare nuovi tipi di virus qualora vi entri in contatto.

Network Associates, attraverso la divisione McAfee Labs, aggiorna con regolarità i file critici e rende disponibili i file modificati sui propri server FTP (File Transfer Protocol) come pacchetti di file di dati (.DAT). Un pacchetto .DAT è composto da un file di archivio con estensione .ZIP denominato DAT-XXXX.ZIP. Le XXXX del nome del file rappresentano un numero di serie che varia ad ogni versione dei file .DAT.

❑ **NOTA:** "Aggiornare" VirusScan significa scaricare e installare nuove versione dei file .DAT; Eseguire l'"upgrade" di VirusScan significa invece scaricare e installare revisioni della versione del prodotto, file eseguibili e , in alcuni casi, file .DAT. Network Associates fornisce aggiornamenti gratuiti dei file .DAT per tutta la durata del prodotto. Questo non garantisce però che i file .DAT siano sempre compatibili con le versioni precedenti del prodotto.

Il diritto di scaricare gratuitamente gli upgrade di VirusScan dipende dai termini della licenza o dai termini del contratto di vendita stipulato all'acquisto. Per qualsiasi quesito riguardante i suddetti termini, consultare i documenti LICENSE.TXT o README.1ST inclusi nella copia di VirusScan oppure consultare il proprio rivenditore autorizzato. Network Associates consente di scaricare gratuitamente i file di aggiornamento e altri servizi dai propri siti FTP in base alla durata della licenza. L'Utilità di pianificazione di VirusScan utilizza un'attività diversa, l'Upgrade automatico, per controllare quando e con quale frequenza vengono scaricati i nuovi file di VirusScan. Vedere "Configurazione delle opzioni di Upgrade automatico" a pagina 228 per informazioni sulle modalità di configurazione di questa attività.

In base alle impostazioni predefinite, l'attività Aggiornamento automatico inclusa nell'Utilità di pianificazione di VirusScan è configurata per scaricare i più recenti aggiornamenti dei file .DAT direttamente dal sito FTP di Network Associates. Tale configurazione può semplificare notevolmente l'amministrazione delle reti di piccole dimensioni o di singole installazioni di VirusScan. Se si gestisce una rete di ampie dimensioni, tuttavia, mantenere questa configurazione può seriamente gravare sull'ampiezza di banda esterna se, come accade se si lascia attivata la configurazione predefinita, tutti i nodi di rete tentano di aggiornare i file .DAT contemporaneamente.

Piuttosto, Network Associates consiglia di utilizzare l'Aggiornamento automatico in associazione al servizio annesso, Enterprise SecureCast, in base a un perfetto accordo di azione congiunta. Una volta installato il software client su un server amministrativo, SecureCast può inviare, o "spingere" automaticamente i file aggiornati, non appena McAfee Labs li rende disponibili. Vedere "Installazione di Enterprise SecureCast" a pagina 280 per maggiori dettagli.

Se, quindi, tali file aggiornati vengono resi disponibili su uno o più server centrali delle rete e i rimanenti nodi di rete vengono configurati per "estrarre" i file aggiornati dai server, sarà possibile:

- Pianificare l'estensione dei file .DAT a tutta la rete nei momenti più appropriati e con minimo intervento sia da parte degli amministratori che degli utenti della rete. Con la finestra di dialogo delle Proprietà dell'attività dell'Utilità di pianificazione di VirusScan, è possibile stabilire quando ciascun nodo di rete riceverà dal server i file aggiornati.

  È possibile, ad esempio, indicare l'ora desiderata per effettuare l'aggiornamento quando si utilizza VirusScan per la prima volta, ma impostare l'Aggiornamento automatico affinché si azioni secondo un intervallo di tempo casuale entro 60 minuti dall'ora prestabilita, oppure impostare una pianificazione che programma o fa ruotare gli aggiornamenti dei file .DAT su tutta la rete. Per informazioni sulle modalità di pianificazione dell'Aggiornamento automatico o su altre attività, vedere "Abilitazione delle attività" a pagina 191.

- Ripartizione dei compiti amministrativi di estensione fra server o controller di dominio differenti, fra zone diverse delle reti geografiche o fra le altre divisioni della rete. Mantenere fondamentalmente interno il traffico degli aggiornamenti può altresì ridurre le possibilità di violazioni della sicurezza di rete.

- Riduzione delle probabilità di attesa per scaricare i nuovi file .DAT. Il traffico sui server Network Associates aumenta considerevolmente ogniqualvolta i file .DAT vengono pubblicati. Evitare la competizione per la larghezza di banda della rete consente di utilizzare l'aggiornamento con interruzioni minime.

Altre opzioni avanzate di Aggiornamento automatico consentono di eseguire il backup dei file .DAT esistenti, installare il file .DAT aggiornato, riavviare il computer aggiornato, se necessario, oppure eseguire particolari programmi dopo aver effettuato gli aggiornamenti. Un gruppo di pagine delle proprietà relative all'Aggiornamento automatico controlla le opzioni di tale attività: fare clic sulle singole schede della finestra di dialogo Proprietà Aggiornamento automatico per configurarle.

Per configurare l'Aggiornamento automatico, procedere come segue:

1. Selezionare l'attività Aggiornamento automatico visualizzata nella finestra Utilità di pianificazione, quindi fare clic su  nella barra degli strumenti dell'Utilità di pianificazione.

NOTA: L'Aggiornamento automatico verrà eseguito secondo la pianificazione impostata nella finestra di dialogo Proprietà attività. Per aprire la finestra di dialogo Proprietà attività, invece, selezionare l'attività Aggiornamento automatico, quindi fare clic su nella barra degli strumenti Utilità di pianificazione. Per informazioni sull'impostazione della pianificazione di un'attività, vedere "Abilitazione delle attività" a pagina 191.

Sarà visualizzata la finestra di dialogo Aggiornamento automatico (vedere Figura 6-17).

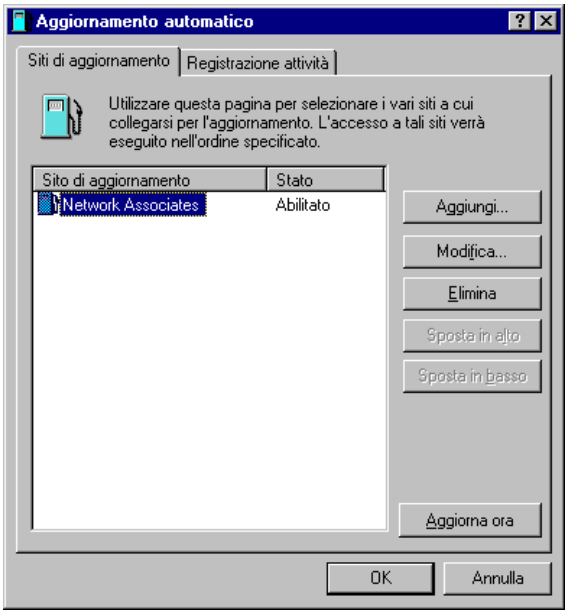

Figura 6-17. Finestra di dialogo Aggiornamento automatico - pagina Siti aggiornamento

In tale finestra, Aggiornamento automatico riporta i siti da cui scaricherà i nuovi file .DAT. Inizialmente, Aggiornamento automatico viene configurato per collegarsi unicamente con il sito FTP Network Associates. Da questa finestra di dialogo, è possibile aggiungere tutti i siti necessari e modificare l'ordine secondo cui Aggiornamento automatico tenta di connettersi ad essi. Le opzioni disponibili sono:

- **Aggiungi nuovo sito.** Fare clic su **Aggiungi** per aprire la finestra di dialogo Proprietà Aggiornamento automatico (Figura 6-18). Per informazioni sulle modalità di specifica delle opzioni per il nuovo sito, vedere "Configurazione delle opzioni di aggiornamento" a pagina 222.

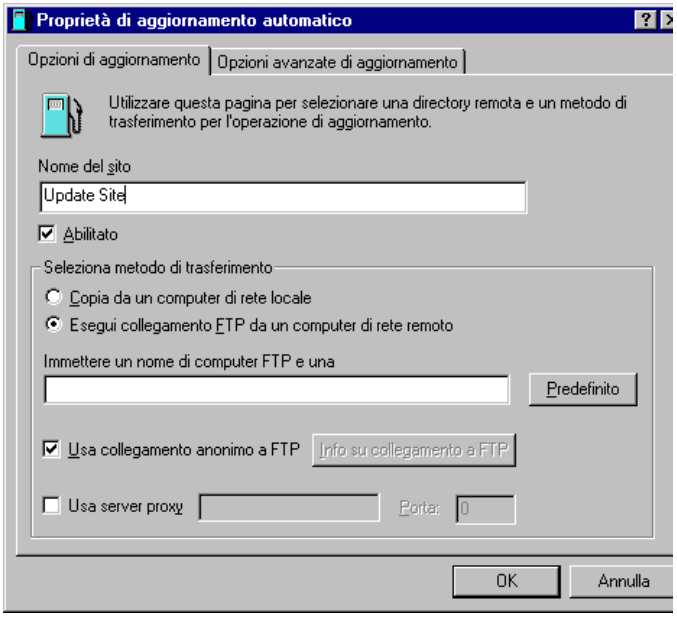

Figura 6-18. Finestra di dialogo Proprietà Aggiornamento automatico Pagina Opzioni aggiornamento

- **Modificare le opzioni per un sito esistente.** Selezionare uno dei siti visualizzati nell'elenco, quindi fare clic su **Modifica** per aprire la finestra di dialogo Proprietà Aggiornamento automatico (vedere Figura 6-18). Effettuare le modifiche desiderate, quindi fare clic su **OK** per chiudere la finestra di dialogo. Per le descrizioni e le istruzioni relative alla configurazione delle opzioni disponibili, vedere "Configurazione delle opzioni di aggiornamento" a pagina 222.
- **Rimozione di un sito esistente.** Selezionare uno dei siti visualizzati nell'elenco, quindi fare clic su **Rimuovi** per eliminarlo.
- **Modificare l'ordine di ricerca per i siti esistenti.** Per modificare l'ordine in base al quale Aggiornamento automatico si connette ai siti elencati nella finestra di dialogo, selezionare il sito di cui si desidera modificare la priorità, quindi fare clic su **Sposta su** per riservare al sito una priorità più alta oppure **Sposta giù** per riservargli una priorità più bassa.

- **Aggiornamento immediato dei file .DAT.** Fare clic su **Aggiorna ora** per consentire ad Aggiornamento automatico di connettersi immediatamente al primo sito dell'elenco e di ricercare nuovi file .DAT. Per utilizzare tale funzione, è necessario configurare le opzioni appropriate perché Aggiornamento automatico individui il sito elencato e, se necessario, si colleghi ad esso. Per informazioni sulle modalità di specifica delle opzioni necessarie, vedere "Configurazione delle opzioni di aggiornamento" a pagina 222.

  Se Aggiornamento automatico dopo tre tentativi effettuati non riesce a collegarsi al sito in elenco oppure se non trova nuovi file .DAT, si collegherà ad ognuno degli altri siti in elenco fino al reperimento dei file .DAT più recenti disponibili. Se è stata selezionata l'opzione **Aggiorna subito**, Aggiornamento automatico scaricherà tutti i file .DAT presenti sul primo sito a cui ha avuto accesso. Vedere "Configurazione delle opzioni di aggiornamento avanzate" a pagina 225 per ulteriori dettagli.

2. Fare clic sulla scheda Registra attività per visualizzare la successiva pagina delle proprietà (Figura 6-19).

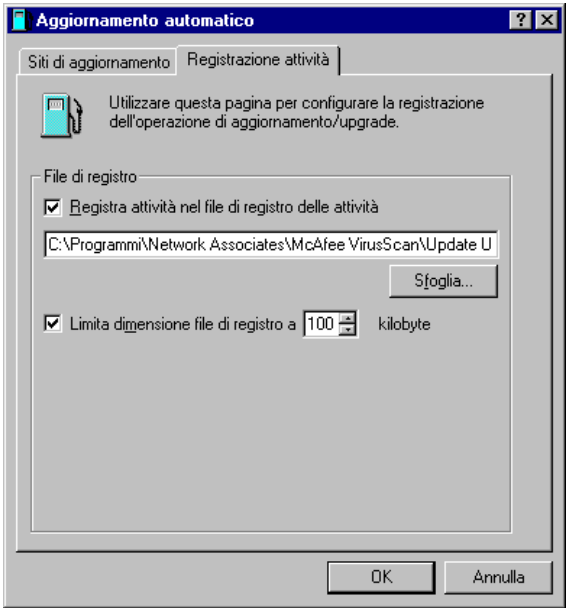

Figura 6-19. Finestra di dialogo Aggiornamento automatico - Pagina Registra attività

3. Selezionare la casella di controllo **Registra attività nel file di registro attività**.

   Per impostazione predefinita, Aggiornamento automatico registra ciò che avviene durante i tentativi di aggiornamento effettuati e salva il record nel file UPDATE UPGRADE ACTIVITY LOG.TXT memorizzato nella directory del programma VirusScan. È possibile immettere un altro nome e percorso nell'apposita casella di testo o fare clic su **Sfoglia** per localizzare un file adatto in qualsiasi altra posizione del disco o della rete.

4. Per ridurre al minimo le dimensioni del file di registro, selezionare la casella di controllo **Limita dimensioni del file di registro a**, quindi immettere un valore per le dimensioni in kilobyte del file nella relativa casella di testo.

   Immettere un valore compreso tra 10KB e 999KB. Per impostazione predefinita, VShield limita la dimensione del file a 100KB. Se i dati del file di registro eccedono la dimensione di file specificata, Aggiornamento automatico cancella il registro esistente e riprende dal punto di interruzione. Per visualizzare il contenuto del file di registro dell'Utilità di pianificazione di VirusScan, selezionare l'attività Aggiornamento automatico nell'elenco delle attività, quindi scegliere **Visualizza registro attività** dal menu **Attività**.

5. Per salvare le modifiche apportate e chiudere la finestra di dialogo Aggiornamento automatico, fare clic su **OK** . Fare clic su **Annulla** per chiudere la finestra di dialogo senza salvare le modifiche. Aggiornamento automatico salva tutte le modifiche effettuate nella finestra di dialogo Aggiornamento automatico in UPDATE.INI, un file memorizzato nella directory del programma VirusScan. Per adottare le stesse impostazioni in rete, copiare UPDATE.INI nella directory del programma VirusScan su ciascun nodo di rete.

Configurazione delle opzioni di aggiornamento

Per creare un nuovo sito per l'aggiornamento o modificare le impostazioni di un sito esistente, fare clic su **Aggiungi** nella finestra di dialogo Aggiornamento automatico (vedere Figura 6-17 a pagina 219), oppure selezionare un sito in elenco, quindi fare clic su **Modifica**. Entrambe le azioni apriranno la finestra di dialogo Proprietà Aggiornamento automatico (Figura 6-20 a pagina 223).

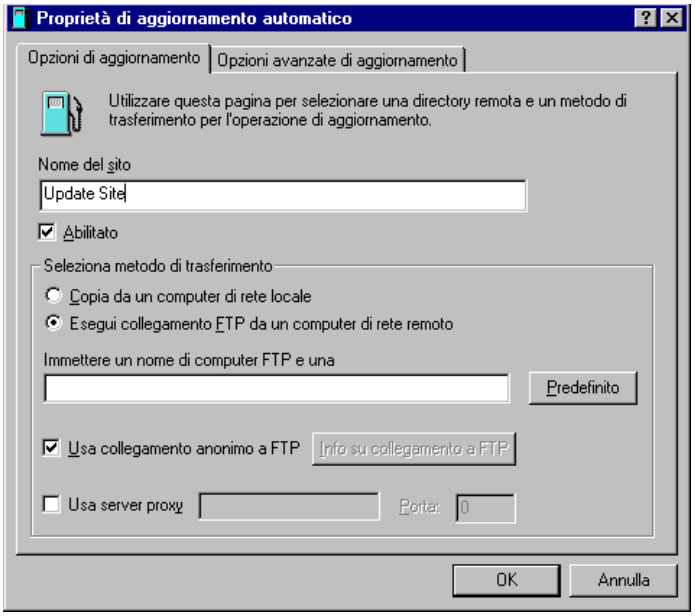

Figura 6-20. Finestra di dialogo Proprietà Aggiornamento automatico - Pagina Opzioni aggiornamento

Procedere quindi come riportato di seguito:

1. Digitare il nome del sito nell'apposita casella di testo. Scegliere un nome descrittivo riconoscibile nell'elenco dei siti.

2. Fare clic su **Abilitato** perché Aggiornamento automatico si colleghi al sito all'ora pianificata. Quando la casella di controllo è deselezionata le opzioni configurate vengono mantenute, ma Aggiornamento automatico non controllerà il sito.

   Aggiornamento automatico effettuerà fino a tre tentativi di connessione al sito durante ciascuna operazione di aggiornamento pianificata. Quando si collega e scarica il nuovo pacchetto dei file .DAT, Aggiornamento automatico estrae anche i file e li installa nella directory del programma VirusScan.

3. Scegliere il metodo che si desidera utilizzare per connettersi al server di destinazione. Le scelte disponibili sono:

- **Copiare da un computer di rete locale**. Selezionare questa opzione per trasferire semplicemente i file di aggiornamento da un computer di rete tramite un qualsiasi protocollo di rete comune attivo. Le impostazioni di tale protocollo regoleranno le modalità di connessione di Aggiornamento automatico e la lunghezza del periodo di timeout prima che Aggiornamento automatico interrompa il tentativo di connessione.

  Immettere il nome del computer secondo la notazione dell'Universal Naming Convention (UNC) nell'apposita casella di testo oppure fare clic su **Sfoglia** per individuare il computer sulla rete. Le rimanenti opzioni della finestra di dialogo cesseranno di essere disponibili.

- **FTP da un computer remoto di rete**. Selezionare tale opzione per trasferire i file di aggiornamento tramite File Transfer Protocol (FTP). Per utilizzare questa opzione, è indispensabile che il server di destinazione disponga di un servizio FTP attivo.

  Aggiornamento automatico utilizza la propria implementazione FTP per connettersi al server, ma il periodo di timeout del tentativo di connessione dipenderà dalle impostazioni del protocollo di rete esistente.

  Immettere quindi il nome del dominio del server di destinazione, insieme a tutte le altre informazioni necessarie relative alla directory, nell'apposita casella di testo. Facendo clic su **Predefinito** si immetterà il server FTP di Network Associates.

  Se il server di destinazione accetta login FTP anonimi, selezionare la casella di controllo **Usa login FTP anonimo**. Se invece si utilizza un account FTP specifico che richiede nome utente e password, deselezionare la casella di controllo, quindi fare clic su **Informazioni sul login FTP**. Questo pulsante aprirà una finestra di dialogo in cui è possibile immettere il nome utente e la password. Immettere di nuovo la password per confermarla, quindi fare clic su **OK** per chiudere la finestra di dialogo.

4. Se si indirizzano le richieste FTP della rete tramite un server proxy, selezionare la casella di controllo **Usa server proxy**, quindi immettere il nome del server proxy nell'apposita casella di testo. È possibile immettere il nome nella notazione UNC oppure un nome di dominio, purché sia compatibile con l'ambiente operativo. Di seguito, immettere nella rimanente casella di testo la porta logica del server proxy alla quale l'Aggiornamento automatico dovrebbe indirizzarsi con la richiesta FTP.

5. Per selezionare ulteriori opzioni, fare clic sulla scheda Aggiornamento avanzato. Per salvare le modifiche e tornare alla finestra di dialogo Aggiornamento automatico, fare clic su **OK**. Aggiornamento automatico salva tutte le modifiche effettuate nella finestra di dialogo Aggiornamento automatico in UPDATE.INI, un file memorizzato nella directory del programma VirusScan. Fare clic su **Annulla** per chiudere la finestra di dialogo senza salvare le modifiche.

Configurazione delle opzioni di aggiornamento avanzate

Per completare l'attività Aggiornamento automatico, è necessario immettere unicamente un server di destinazione, una modalità di connessione e tutte le informazioni necessarie relative al login. Quindi, una volta abilitata l'attività e impostata una pianificazione, Aggiornamento automatico scaricherà i file appropriati dal server di destinazione, li estrarrà dall'archivio .ZIP e li installerà nella directory del programma VirusScan.

Per fare in modo che Aggiornamento automatico esegua operazioni di pre o post-elaborazione sui file o che esegua altre azioni, selezionare la scheda Opzioni di aggiornamento avanzate per visualizzare la corretta pagina delle proprietà (Figura 6-21).

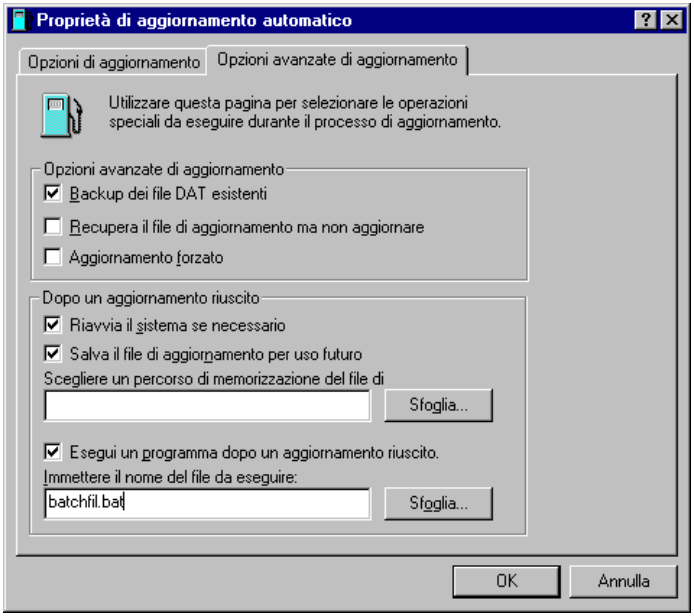

Figura 6-21. Finestra di dialogo Proprietà Aggiornamento automatico Pagina Opzioni di aggiornamento avanzate

Procedere quindi come riportato di seguito:

1. Indicare ad Aggiornamento automatico le azioni da eseguire prima o durante l'esecuzione di un aggiornamento. Le opzioni disponibili sono:

   - **Creare copie di backup dei file .DAT esistenti.** Selezionare questa casella di controllo perché Aggiornamento automatico rinomini i file .DAT di VirusScan esistenti prima di installare i nuovi file. Per rinominare i file, Aggiornamento automatico accoda l'estensione .SAV al nome del file e all'estensione esistenti. CLEAN.DAT, ad esempio, diverrà CLEAN.DAT.SAV.

   - **Richiamare il file di aggiornamento senza eseguire l'aggiornamento**. Selezionare questa casella di controllo perché Aggiornamento automatico scarichi l'archivio .ZIP che contiene i nuovi file .DAT e li salvi semplicemente in una posizione indicata anziché estrarli e installarli.

     La selezione di questa casella di controllo comporta anche la selezione della casella di controllo **Salva i file di aggiornamento per un successivo utilizzo** nell'area **Dopo un aggiornamento**. Per indicare ad Aggiornamento automatico dove salvare il pacchetto dei file .DAT, immettere un percorso e il nome di una cartella nella casella di testo sotto la casella di controllo oppure fare clic su **Sfoglia** per individuare una cartella adeguata.

     Questa opzione viene utilizzata per scaricare i nuovi file .DAT in un server centrale della rete e per consentire ai singoli computer client di scaricare, estrarre e installare localmente i nuovi file.

   - **Aggiorna subito.** Selezionare questa casella di controllo per indicare ad Aggiornamento automatico di scaricare e installare qualsiasi pacchetto di file .DAT rilevi sul server di destinazione, sia nel caso che il pacchetto sia più recente dei file .DAT esistenti, sia in caso contrario. Questa opzione viene utilizzata per aggiornare periodicamente i file .DAT contenuti nella directory del programma VirusScan, nel caso in cui i file esistenti siano stati danneggiati. Questa opzione consentirà, inoltre, di aggirare i messaggi di errore che VirusScan potrebbe inviare, nel caso in cui non rilevi nuovi file sul server di destinazione nell'ora stabilita per l'attività di aggiornamento.

     AVVERTENZA: Network Associates consiglia di utilizzare con estrema cautela quest'opzione. Se l'attività di Aggiornamento automatico è stata configurata per collegarsi ad un server che contiene versioni precedenti dei file .DAT, è possibile ridurre l'efficacia di VirusScan ed esporre il computer o la rete al rischio di infezioni da virus nuovi e di altro software

dannoso. L'aggiornamento dei componenti del programma VirusScan può inoltre determinare incompatibilità con le versioni precedenti dei file .DAT. Tale incompatibilità può, a sua volta, determinare comportamenti imprevedibili da parte di VirusScan.

2. Indicare ad Aggiornamento automatico le operazioni da compiere dopo aver scaricato, estratto e installato i nuovi file .DAT. Le opzioni disponibili sono:

   - **Riavviare il sistema, se necessario, dopo un aggiornamento**. Selezionare questa casella di controllo perché Aggiornamento automatico riavvii il sistema dopo l'installazione dei nuovi file .DAT.

     Sebbene VirusScan e VShield richiedano il riavvio del sistema per caricare i nuovi file .DAT, può essere consigliabile effettuare tale operazione solo durante le ore di inattività in modo tale da non interferire con l'attività produttiva. Se si pianifica l'esecuzione di un programma dopo aver aggiornato i file .DAT, sarà necessario deselezionare tale casella di controllo.

     NOTA: Questa opzione è valida solo per le operazioni di aggiornamento pianificate. Se si fa clic su **Aggiorna ora** nella finestra di dialogo Aggiornamento automatico, Aggiornamento automatico chiederà se si desidera riavviare il computer al termine dell'installazione dei nuovi file .DAT, che si selezioni o meno tale opzione.

- **Salva i file di aggiornamento per un successivo utilizzo.** Selezionare questa casella di controllo affinché Aggiornamento automatico salvi una copia non estratta del pacchetto dei file .DAT nella posizione specificata. Aggiornamento automatico estrae quindi i file .DAT dal pacchetto degli aggiornamenti e procede con l'installazione. Al contrario, l'opzione **Richiamare il file di aggiornamento ma non effettuare l'aggiornamento** salva il file non estratto, ma non installa i nuovi file .DAT.

  Per indicare ad Aggiornamento automatico dove salvare il pacchetto dei file .DAT, immettere un percorso e il nome di una cartella nella casella di testo sotto la casella di controllo oppure fare clic su **Sfoglia** per individuare una cartella adeguata.

- **Esegui programma dopo l'aggiornamento.** Selezionare questa casella di controllo perché Aggiornamento automatico avvii un altro programma una volta installati i nuovi file .DAT. Tale opzione si utilizzerà, ad esempio, per avviare un programma client di posta elettronica o un'utilità per i messaggi di rete che comunichi all'amministratore del sistema che l'operazione di aggiornamento è stata condotta a termine.

  Immettere quindi il percorso e il nome del file del programma che si desidera eseguire oppure fare clic su **Sfoglia** per individuare il programma sul disco rigido.

3. Per salvare le modifiche e tornare alla finestra di dialogo Aggiornamento automatico, fare clic su **OK**. Aggiornamento automatico salva tutte le modifiche effettuate nella finestra di dialogo Aggiornamento automatico in UPDATE.INI, un file memorizzato nella directory del programma VirusScan. Fare clic su **Annulla** per chiudere la finestra di dialogo senza salvare le modifiche.

Configurazione delle opzioni di Upgrade automatico

Network Associates revisiona di frequente VirusScan per aggiungere nuove capacità di rilevamento e ripristino, nuove funzioni di gestione e flessibilità e altri potenziamenti che migliorano la sicurezza del prodotto. L'utilità Upgrade automatico di VirusScan è stata progettata specificamente per ricercare e scaricare le nuove versioni non appena esse sono disponibili.

NOTA: "Aggiornare" VirusScan significa scaricare e installare nuove versione dei file .DAT; Eseguire l'"upgrade" di VirusScan significa invece scaricare e installare revisioni della versione del prodotto, file eseguibili e, in alcuni casi, file .DAT. Network Associates fornisce aggiornamenti gratuiti dei file .DAT per tutta la durata del prodotto. Questo non garantisce però che i file .DAT siano sempre compatibili con le versioni precedenti del prodotto.

Il diritto di scaricare gratuitamente gli upgrade di VirusScan dipende dai termini della licenza o dai termini del contratto di vendita stipulato all'acquisto. Per qualsiasi quesito riguardante i suddetti termini, consultare i documenti LICENSE.TXT o README.1ST inclusi nella copia di VirusScan oppure consultare il proprio rivenditore autorizzato. Network Associates consente di scaricare gratuitamente i file di aggiornamento e altri servizi dai propri siti FTP in base alla durata della licenza. L'Utilità di pianificazione di VirusScan utilizza un'attività diversa, l'Upgrade automatico, per controllare quando e con quale frequenza vengono scaricati i nuovi file di VirusScan. Vedere "Configurazione delle opzioni di Upgrade automatico" a pagina 228 per informazioni sulle modalità di configurazione di questa attività.

Per impostazione predefinita, l'attività Upgrade automatico inclusa nell'Utilità di pianificazione di VirusScan non è configurata con le informazioni riguardanti il sito necessarie a scaricare le nuove versioni di VirusScan. Gli utenti di VirusScan registrati possono ottenere tali informazioni dai rivenditori autorizzati o presso altre fonti di Network Associates.

Network Associates consiglia di utilizzare Upgrade automatico in associazione al servizio annesso Enterprise SecureCast, in base a un perfetto accordo di azione congiunta. Una volta installato il software client su un server amministrativo, SecureCast può inviare, o "spingere" automaticamente i file aggiornati, non appena Network Associates li rende disponibili. Vedere "Installazione di Enterprise SecureCast" a pagina 280 per maggiori dettagli.

Se, quindi, tali file aggiornati vengono resi disponibili su uno o più server centrali delle rete e i rimanenti nodi di rete vengono configurati per "estrarre" i file aggiornati dai server, sarà possibile:

- Pianificare l'estensione delle nuove versioni di VirusScan a tutta la rete nei momenti più appropriati e con minimo intervento sia da parte degli amministratori che degli utenti della rete. Con la finestra di dialogo delle Proprietà dell'attività dell'Utilità di pianificazione di VirusScan, è possibile stabilire quando ciascun nodo di rete riceverà dal server i file aggiornati.

È possibile, ad esempio, indicare l'ora desiderata per effettuare l'Upgrade automatico quando si utilizza VirusScan per la prima volta, ma impostare il programma in maniera tale che si azioni secondo un intervallo di tempo casuale entro 60 minuti dall'ora prestabilita, oppure impostare una pianificazione che programma o fa ruotare gli upgrade su tutta la rete. Per informazioni sulle modalità di pianificazione di Upgrade automatico o di altre attività, vedere "Abilitazione delle attività" a pagina 191.

- Ripartizione dei compiti amministrativi di estensione fra server o controller di dominio differenti, fra zone diverse delle reti geografiche o fra le altre divisioni della rete. Mantenere fondamentalmente interno il traffico degli aggiornamenti può altresì ridurre le possibilità di violazioni della sicurezza di rete.
- Riduzione delle probabilità di attesa per scaricare le nuove versioni di VirusScan. Il traffico sui server Network Associates aumenta considerevolmente quando vengono rilasciate nuove versioni di VirusScan. Evitare la competizione per la larghezza di banda della rete consente di implementare le nuove versioni con interruzioni minime.

> **IMPORTANTE:** Se i nuovi file di upgrade di VirusScan vengono collocati in un server che utilizza nomi di file sensibili alla differenza tra maiuscole e minuscole, è necessario rinominare il file PKGDESC.INI, contenuto negli upgrade di VirusScan, perché utilizzi solo lettere minuscole. In caso contrario, l'Upgrade automatico non individuerà il file sul server e di conseguenza non installerà la nuova versione di VirusScan sui computer client.

Altre opzioni avanzate di Upgrade automatico consentono di riavviare il sistema o di salvare il pacchetto degli aggiornamenti per un successivo utilizzo. Un gruppo di pagine di proprietà di Upgrade automatico controlla le opzioni di tale attività: per configurarle, fare clic su ciascuna scheda nella finestra di dialogo Proprietà Upgrade automatico.

Per configurare Upgrade automatico, procedere come segue:

1. Selezionare l'attività Upgrade automatico visualizzata nella finestra Utilità di pianificazione, quindi fare clic su  nella barra degli strumenti dell'Utilità di pianificazione.

NOTA: L'Upgrade automatico verrà eseguito in base alla pianificazione impostata nella finestra di dialogo Proprietà attività. Per aprire invece la finestra di dialogo Proprietà attività, selezionare l'attività Upgrade automatico, quindi fare clic su nella barra degli strumenti dell'Utilità di pianificazione. Per informazioni sull'impostazione della pianificazione di un'attività, vedere "Abilitazione delle attività" a pagina 191.

Sarà visualizzata la finestra di dialogo Upgrade automatico (vedere Figura 6-22).

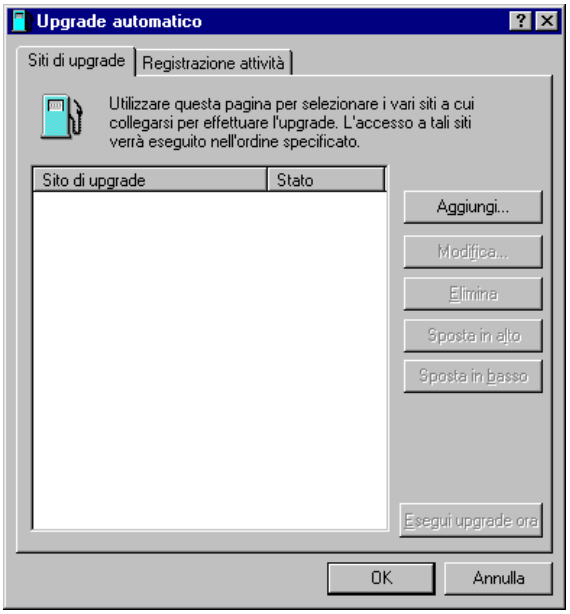

Figura 6-22. Finestra di dialogo Upgrade automatico - Pagina Siti di aggiornamento

In questa pagina, Upgrade automatico elenca i siti dai quali scaricherà i nuovi file .DAT. Inizialmente, nell'elenco non sarà visualizzato alcun sito, poiché l'Upgrade automatico non è configurato per connettersi ai siti di aggiornamento. È possibile ricercare i siti desiderati dalle informazioni ricevute al momento dell'acquisto di VirusScan. In questa finestra di dialogo è possibile aggiungere tutti i siti necessari e modificare l'ordine secondo cui Upgrade automatico tenta di connettersi ad essi. Le opzioni disponibili sono:

- **Aggiungi nuovo sito.** Fare clic su **Aggiungi** per aprire la finestra di dialogo Proprietà Upgrade automatico (Figura 6-23). Per informazioni sulle modalità di specifica delle opzioni per il nuovo sito, vedere "Configurazione delle opzioni di upgrade" a pagina 234.

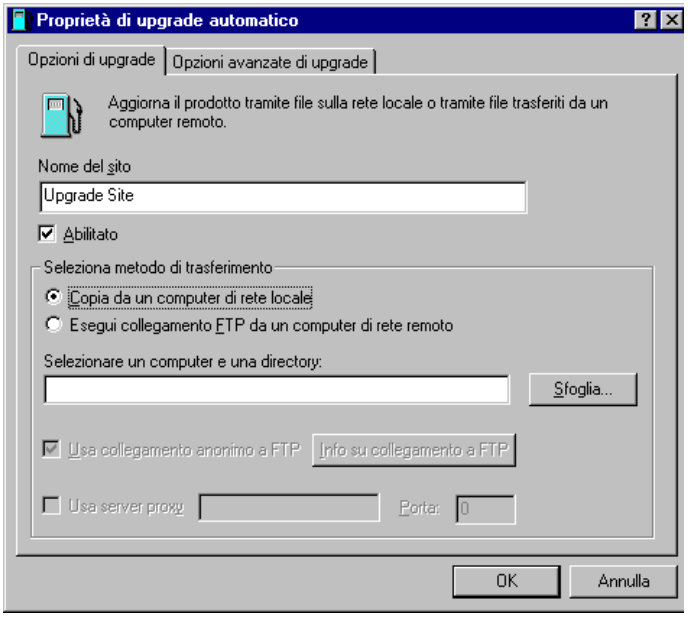

Figura 6-23. Finestra di dialogo Proprietà Upgrade automatico - Pagina Opzioni di aggiornamento

- **Modificare le opzioni per un sito esistente.** Selezionare uno dei siti presenti nell'elenco, quindi fare clic su **Modifica** per aprire la finestra di dialogo Proprietà Upgrade automatico (vedere Figura 6-23). Effettuare le modifiche desiderate, quindi fare clic su **OK** per chiudere la finestra di dialogo. Per le descrizioni e le istruzioni relative alla configurazione delle opzioni disponibili, vedere "Configurazione delle opzioni di upgrade" a pagina 234.
- **Rimozione di un sito esistente.** Selezionare uno dei siti visualizzati nell'elenco, quindi fare clic su **Rimuovi** per eliminarlo.
- **Modificare l'ordine di ricerca per i siti esistenti.** Per modificare l'ordine in base al quale Upgrade automatico si connette a ciascun sito, selezionare il sito di cui si desidera modificare la priorità, quindi fare clic su **Sposta su** per riservare al sito una priorità più alta oppure **Sposta giù** per riservargli una priorità più bassa.

- **Upgrade automatico immediato dei file di VirusScan.** Fare clic su **Esegui upgrade ora** perché Upgrade automatico si connetta immediatamente al primo sito presente nell'elenco e ricerchi una nuova versione di VirusScan. Per utilizzare tale funzione, è necessario configurare le opzioni necessarie di Upgrade automatico per individuare il sito in elenco e, se necessario, collegarsi ad esso. Vedere "Configurazione delle opzioni di upgrade" a pagina 234 per informazioni sulle modalità di specifica delle opzioni desiderate.

  Se Upgrade automatico dopo tre tentativi effettuati non riesce a collegarsi al sito in elenco o se non individua nuovi file di VirusScan, accederà ad ognuno degli altri siti in elenco fino al reperimento della versione di VirusScan più recente disponibile.

2. Fare clic sulla scheda Registra attività per visualizzare la successiva pagina delle proprietà (Figura 6-24).

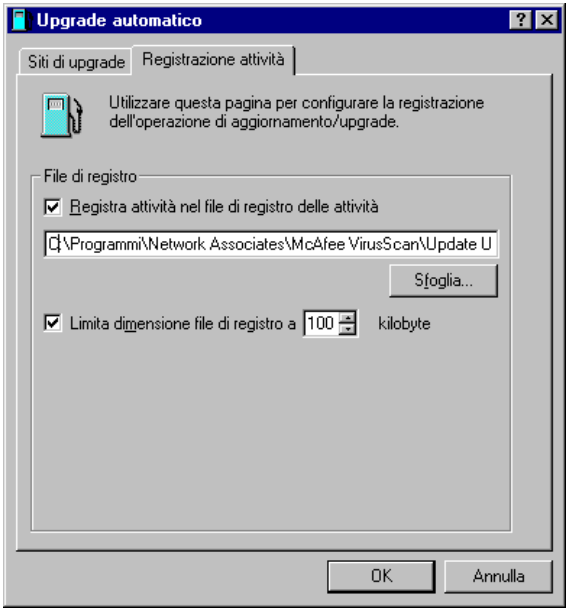

Figura 6-24. Finestra di dialogo Upggrade automatico - Pagina Registra attività

3. Selezionare la casella di controllo **Registra attività nel file di registro attività**.

   Per impostazione predefinita, Upgrade automatico registra ciò che avviene durante i tentativi di aggiornamento effettuati e salva il record nel file UPDATE UPGRADE ACTIVITY LOG.TXT contenuto nella directory del programma VirusScan. È possibile immettere un altro nome e percorso nell'apposita casella di testo o fare clic su **Sfoglia** per localizzare un file adatto in qualsiasi altra posizione del disco o della rete.

4. Per ridurre al minimo le dimensioni del file di registro, selezionare la casella di controllo **Limita dimensioni del file di registro a**, quindi immettere un valore per le dimensioni in kilobyte del file nella relativa casella di testo.

   Immettere un valore compreso tra 10KB e 999KB. Per impostazione predefinita, Upgrade automatico limita la dimensione del file a 100KB. Se i dati del file di registro eccedono la dimensione del file specificata, Upgrade automatico cancella il registro esistente e riprende dal punto di interruzione. Per visualizzare il contenuto del file di registro dell'Utilità di pianificazione di VirusScan, selezionare l'attività Upgrade automatico nell'elenco delle attività, quindi scegliere **Visualizza registro attività** dal menu **Attività**.

5. Per salvare le modifiche apportate e chiudere la finestra di dialogo Upgrade automatico, fare clic su **OK**. Fare clic su **Annulla** per chiudere la finestra di dialogo senza salvare le modifiche. Aggiornamento automatico salva tutte le modifiche effettuate nella finestra di dialogo Upgrade automatico in UPGRADE.INI, un file memorizzato nella directory del programma VirusScan. Per adottare le stesse impostazioni in rete, copiare UPGRADE.INI nella directory del programma VirusScan su ciascun nodo di rete.

Configurazione delle opzioni di upgrade

Per creare un nuovo sito di upgrade o per modificare le impostazioni di un sito esistente, fare clic su **Aggiungi** nella finestra di dialogo Upgrade automatico (vedere Figura 6-22 a pagina 231), oppure selezionare un sito in elenco, quindi fare clic su **Modifica**. Entrambe le azioni apriranno la finestra di dialogo Proprietà Upgrade automatico (Figura 6-25 a pagina 235).

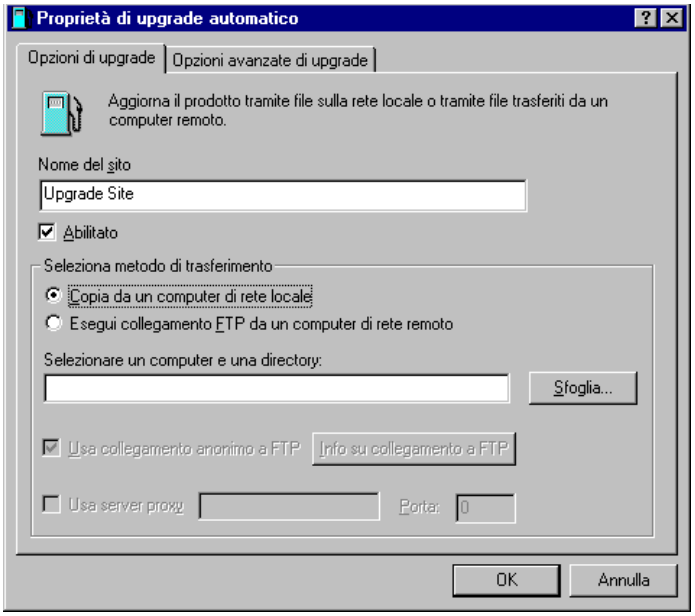

Figura 6-25. Finestra di dialogo Proprietà Upgrade automatico - Pagina Opzioni di aggiornamento

Procedere quindi come riportato di seguito:

1. Digitare il nome del sito nell'apposita casella di testo. Scegliere un nome descrittivo riconoscibile nell'elenco dei siti.

2. Fare clic su **Abilitato** per comunicare ad Upgrade automatico di connettersi al sito all'ora pianificata. Quando la casella di controllo è deselezionata, le opzioni configurate vengono mantenute, ma Upgrade automatico non controllerà il sito.

   Upgrade automatico effettuerà fino a tre tentativi di connessione al sito durante ciascuna operazione di aggiornamento pianificata. Quando si collega e scarica una nuova versione di VirusScan, Upgrade automatico estrae anche i file e li installa nella directory del programma VirusScan.

3. Scegliere il metodo che si desidera utilizzare per connettersi al server di destinazione. Le scelte disponibili sono:

- **Copiare da un computer di rete locale**. Selezionare questa opzione per trasferire semplicemente i file di aggiornamento da un computer di rete tramite un qualsiasi protocollo di rete comune attivo. Le impostazioni di tale protocollo regoleranno le modalità di connessione di Upgrade automatico e la lunghezza del periodo di timeout necessario prima che Upgrade automatico interrompa il tentativo di connessione.

  Immettere il nome del computer secondo la notazione dell'Universal Naming Convention (UNC) nell'apposita casella di testo oppure fare clic su **Sfoglia** per individuare il computer sulla rete. Le rimanenti opzioni della finestra di dialogo cesseranno di essere disponibili.

- **FTP da un computer remoto di rete**. Selezionare tale opzione per trasferire i file di aggiornamento tramite File Transfer Protocol (FTP). Per utilizzare questa opzione, è indispensabile che il server di destinazione disponga di un servizio FTP attivo.

  Upgrade automatico utilizza la propria implementazione FTP per connettersi al server, ma il periodo di timeout del tentativo di connessione dipenderà dalle impostazioni del protocollo di rete esistente.

  Di seguito, immettere nell'apposita casella di testo il nome del dominio del server di destinazione, insieme a tutte le altre informazioni necessarie relative alla directory oppure fare clic su **Sfoglia** per individuare il server sulla rete.

  Se il server di destinazione accetta login FTP anonimi, selezionare la casella di controllo **Usa login FTP anonimo**. Se invece si utilizza un account FTP specifico che richiede nome utente e password, deselezionare la casella di controllo, quindi fare clic su **Informazioni sul login FTP**. Questo pulsante aprirà una finestra di dialogo in cui è possibile immettere il nome utente e la password. Immettere di nuovo la password per confermarla, quindi fare clic su **OK** per chiudere la finestra di dialogo.

4. Se si indirizzano le richieste FTP della rete tramite un server proxy, selezionare la casella di controllo **Usa server proxy**, quindi immettere il nome del server proxy nell'apposita casella di testo. È possibile immettere il nome nella notazione UNC oppure un nome di dominio, purché sia compatibile con l'ambiente operativo. Di seguito, immettere nella rimanente casella di testo la porta logica del server proxy alla quale Upgrade automatico dovrebbe indirizzarsi con la richiesta FTP.

5. Per selezionare ulteriori opzioni, fare clic sulla scheda Upgrade avanzato. Per salvare le modifiche e tornare alla finestra di dialogo Upgrade automatico, fare clic su **OK**. L'Upgrade automatico salva tutte le modifiche effettuate nella finestra di dialogo Upgrade automatico in UPGRADE.INI, un file memorizzato nella directory del programma VirusScan. Fare clic su **Annulla** per chiudere la finestra di dialogo senza salvare le modifiche.

Configurazione delle opzioni di upgrade avanzato

Per completare l'attività Upgrade automatico, è necessario immettere solo un server di destinazione, un metodo di connessione e tutte le informazioni necessarie relative al login. Quindi, una volta abilitata l'attività e impostata una pianificazione, Upgrade automatico scaricherà i file appropriati dal server di destinazione, li estrarrà e li installerà nella directory del programma VirusScan.

Affinché Upgrade automatico intraprenda altre azioni prima o dopo l'individuazione di nuovi file, fare clic sulla scheda Opzioni di upgrade avanzate per visualizzare la pagina delle proprietà appropriata (Figura 6-26).

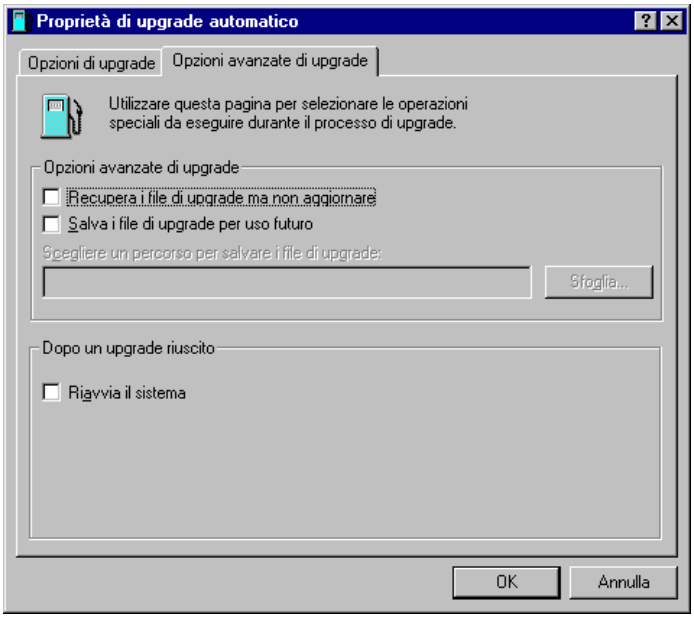

Figura 6-26. Finestra di dialogo Proprietà Upgrade automatico - Pagina Opzioni di aggiornamento avanzate

Procedere quindi come riportato di seguito:

1. Indicare ad Upgrade automatico in che modo procedere con i file scaricati. Le opzioni disponibili sono:

   - **Richiamare i file di upgrade ma non effettuare l'upgrade**. Selezionare questa casella di controllo per consentire ad Upgrade automatico di scaricare la nuova versione di VirusScan e salvarla semplicemente in una determinata posizione invece di installarla.

     Selezionando questa casella di controllo si seleziona anche la casella di controllo **Salva i file di aggiornamento per un successivo utilizzo**. Per indicare ad Upgrade automatico in quale posizione salvare i nuovi file, immettere un percorso e il nome della cartella nella casella di testo sotto la casella di controllo oppure fare clic su **Sfoglia** per individuare una cartella appropriata.

     Questa opzione viene utilizzata per scaricare i nuovi file di VirusScan in un server centrale della rete e per consentire ai singoli computer client di scaricare e installare localmente i nuovi file.

   - **Salvare i file di upgrade per un utilizzo successivo.** Selezionare questa casella di controllo per consentire ad Upgrade automatico di salvare una copia non estratta dei nuovi file di VirusScan in una determinata posizione. Upgrade automatico procederà quindi con l'installazione. Al contrario, l'opzione **Richiama i file di upgrade ma non effettuare l'upgrade** consente di salvare il file non estratto, ma non installa la nuova versione di VirusScan.

2. Indicare ad Upgrade automatico come procedere dopo aver scaricato e installato una nuova versione di VirusScan. Le opzioni disponibili sono:

   - **Riavviare il sistema dopo l'upgrade**. Selezionare questa casella di controllo perché Upgrade automatico riavvii il sistema dopo aver installato i nuovi file di VirusScan.

     Sebbene VirusScan e VShield richiedano il riavvio del sistema dopo le relative installazioni, può essere consigliabile effettuare tale operazione solo durante le ore di inattività, in modo tale da non interferire con l'attività produttiva.

❑ **NOTA:** Questa opzione è valida unicamente per operazioni di upgrade pianificate. Se si fa clic su **Esegui upgrade ora** nella finestra di dialogo Upgrade automatico, Upgrade automatico chiederà se si desidera riavviare il computer al termine dell'installazione della nuova versione di VirusScan, che l'opzione sia stata selezionata o meno.

---

3. Per salvare le modifiche e tornare alla finestra di dialogo Upgrade automatico, fare clic su **OK**. L'Upgrade automatico salva tutte le modifiche effettuate nella finestra di dialogo Upgrade automatico in UPGRADE.INI, un file memorizzato nella directory del programma VirusScan. Fare clic su **Annulla** per chiudere la finestra di dialogo senza salvare le modifiche.

Configurazione delle opzioni per altri programmi

È possibile utilizzare l'utilità di pianificazione per eseguire altri programmi secondo tempi prestabiliti, ma, a meno che il programma che si desidera eseguire non sia un prodotto antivirus della Network Associates, non è possibile eseguire l'utilità di pianificazione per configurare tale programma per l'esecuzione con particolari opzioni. Per questa operazione, è necessario aprire e preconfigurare il programma da soli: l'utilità di pianificazione eseguirà semplicemente il programma al momento specificato, così come è stato configurato. Tuttavia, è possibile utilizzare l'utilità di pianificazione per aprire la finestra di dialogo delle proprietà di VShield in modo da configurare VShield per l'esecuzione con particolari opzioni di scansione. Per informazioni sulle modalità di esecuzione di questa operazione, vedere Capitolo 4, "Uso di VShield".

Utilizzo di strumenti specifici per la scansione 7

Scansione di posta elettronica in Microsoft Exchange e Outlook

Oltre alla scansione continua in background fornita da VShield mediante il modulo per la scansione della posta elettronica, VirusScan include un componente completo del programma progettato in modo specifico per la ricerca di virus nelle caselle di posta elettronica in Microsoft Exchange e Microsoft Outlook o nei server di posta MAPI (Messaging Application Programming Interface) compatibili. Il programma di scansione della posta elettronica fornisce la possibilità di effettuare la scansione dei server di posta secondo le modalità e i tempi desiderati. Un'architettura di attivazione non intrusiva fornisce l'accesso al programma di scansione direttamente all'interno delle applicazioni client di Exchange o Outlook.

Se VirusScan è stato installato con l'opzione di installazione Tipica (per ulteriori dettagli, vedere pagina 42), è già possibile accedere al programma di scansione della posta elettronica.

Per utilizzare le impostazioni predefinite del programma di scansione della posta elettronica, avviare il software del client di Microsoft Exchange o Microsoft Outlook, quindi

1. collegarsi normalmente al server di posta elettronica.
2. Selezionare **Scansione** nel menu **Strumenti** o fare clic su  nella barra degli strumenti di Exchange o Outlook.

> **NOTA:** Se si utilizza Microsoft Exchange 5.0, una limitazione nella modalità di aggiornamento della barra degli strumenti da parte del programma impedisce che la scansione della posta elettronica visualizzi immediatamente i pulsanti. Per aggiungere il pulsante Scansione alla barra degli strumenti, selezionare **Personalizza barra degli strumenti** nel menu **Strumenti**, quindi aggiungere i pulsanti per la scansione della posta dall'elenco dei pulsanti disponibili nella finestra di dialogo Personalizza barra degli strumenti.

Una volta avviato, Scansione posta comincia immediatamente ad effettuare la scansione della casella di posta in Exchange o Outlook per rilevare la presenza di virus (vedere Figura 7-1).

In base alle impostazioni predefinite, la scansione della posta esamina *tutti* i messaggi di posta memorizzati nella casella Posta in arrivo sul server di posta, ricercando gli allegati che potrebbero essere infettati da virus. Se è presente un numero elevato di messaggi memorizzati che non sono stati ancora scaricati, l'operazione di scansione può durare a lungo. Per sospendere l'operazione, fare clic su ⏸. Per interromperla del tutto, fare clic su ■. Per riprendere l'operazione, fare clic su ▶.

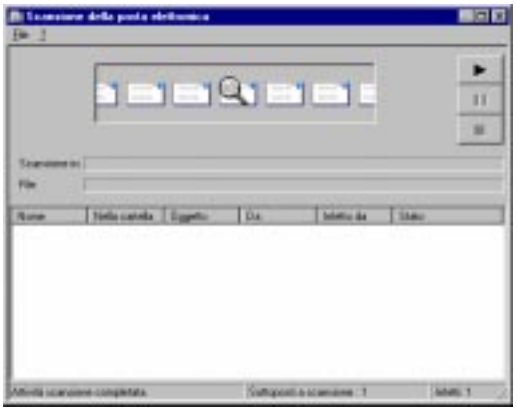

Figura 7-1. Scansione posta in corso

Se Scansione posta rileva un file infetto, richiede quale operazione intraprendere. Vedere "Risposta da fornire quando Scansione posta rileva un virus" a pagina 75 per ulteriori informazioni.

Configurazione del programma Scansione posta

Sebbene le impostazioni predefinite di Scansione posta forniscano un buon livello di protezione contro le infezioni diffuse tramite la posta elettronica in Exchange o Outlook, tuttavia potrebbero non essere adatte all'ambiente di lavoro.

Per modificare le opzioni di configurazione di Scansione posta, procedere come segue:

1. Avviare il software client di Exchange o Outlook, quindi collegarsi al server di posta elettronica.

   NOTA: Se l'utente è già collegato al dominio di rete del server di posta elettronica, non è necessario collegarsi direttamente al server; è sufficiente invece avviare Exchange o Outlook. Per informazioni sui requisiti per il collegamento al server, consultare l'amministratore della rete.

2. Selezionare **Proprietà di Scansione posta** dal menu **Strumenti** nel programma o fare clic su nella barra degli strumenti di Exchange o Outlook.

   Viene visualizzata la finestra di dialogo Proprietà di Scansione posta (vedere Figura 7-2). La finestra di dialogo Proprietà è costituita da una serie di pagine di proprietà per il controllo delle impostazioni di Scansione posta; fare clic sulle relative schede per impostare il programma in base alle proprie necessità.

Figura 7-2. Finestra di dialogo Proprietà di Scansione posta - pagina Rilevamento

Selezione delle opzioni di Rilevamento

L'impostazione predefinita iniziale di Scansione posta è la scansione di tutti i messaggi di posta elettronica nel server Exchange o Outlook e la limitazione della scansione ai soli file suscettibili di infezione da virus (vedere Figura 7-2 a pagina 243).

Per modificare queste impostazioni, seguire la procedura illustrata:

1. Selezionare il tipo di messaggi di posta elettronica che si desidera sottoporre a scansione in Scansione posta. Le scelte disponibili sono:

   - **Tutti i messaggi.** Fare clic su questo pulsante per fare in modo che Scansione posta controlli tutti i messaggi memorizzati nel server Exchange. L'operazione di scansione completa può richiedere molto tempo.
   - **Solo messaggi non letti.** Fare clic su questo pulsante per fare in modo che Scansione posta esamini solo quei messaggi contrassegnati come "non letti". Una volta completata la scansione di tutta la casella di posta, selezionare quest'opzione per rendere più rapide le operazioni di scansione, mantenendo una protezione antivirus completa per il computer.

     ❑ **NOTA:** Una volta scaricata la posta nel computer, VirusScan considera la cartella personale o il file di archivio come qualsiasi altro file, a meno che non venga esclusa dalle operazioni di scansione. Quest'opzione consente di aggiungere un ulteriore livello di protezione dai virus.

2. Selezionare il tipo di allegati che si desidera esaminare in Scansione posta. È possibile:

   - **Eseguire la scansione di file compressi.** Selezionare la casella di controllo **File compressi** per fare in modo che Scansione posta cerchi i virus nei file compressi con i seguenti formati: .??_, .CAB, LZEXE, LZH, PKLite, .TD0, e .ZIP. Nonostante garantisca una maggiore protezione, la scansione di file compressi dilata i tempi necessari a tale operazione.

- **Scegliere il tipo di file da sottoporre a scansione.** Normalmente i virus non sono in grado di attaccare i file di dati o i file che non contengono un codice eseguibile. Si può, quindi, restringere l'ambito delle operazioni di scansione in modo che Scansione posta verifichi solo gli allegati esposti maggiormente al rischio di infezioni. A tal fine, selezionare il pulsante **Solo file di programma**. Per visualizzare o indicare le estensioni dei nomi file che verranno esaminati da Scansione posta, fare clic su **Estensioni** per aprire la casella di controllo Estensioni file di programma (Figura 7-3).

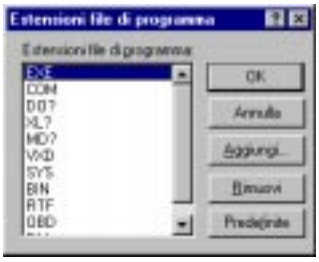

Figura 7-3. Finestra di dialogo Estensioni file di programma

Per valore predefinito, Scansione posta rileva i virus nei file con estensione .EXE, .COM, .DO?, .XL?, .RTF, .BIN, .SYS, .MD?, .VXD, .OBD e .DLL. I file con estensione .DO?, .XL?, .RTF e .OBD sono file di Microsoft Office. Tutti questi file possono essere infettati da virus macro. Il ? è un carattere jolly che abilita la scansione di file di documento e di modello da parte di Scansione.

- Per aggiungere un'estensione all'elenco, fare clic su **Aggiungi**, quindi digitare l'estensione che si desidera sottoporre a scansione nella finestra di dialogo di Scansione posta visualizzata.
- Per eliminare un'estensione dall'elenco, selezionarla, quindi fare clic su **Rimuovi**.
- Fare clic su **Predefinite** per ripristinare l'elenco nella sua forma originaria.

Al termine, scegliere **OK** per chiudere la finestra di dialogo.

Per fare in modo che Scansione posta esamini tutti i file del sistema, indipendentemente dall'estensione, fare clic sul pulsante **Esamina tutti gli allegati**. Questa operazione rallenta notevolmente il sistema, ma garantisce la completa eliminazione dei virus.

- **Attivare la scansione euristica**. Fare clic su **Euristica macro** per aprire la finestra di dialogo Impostazioni di scansione dell'euristica della macro(Figura 7-4).

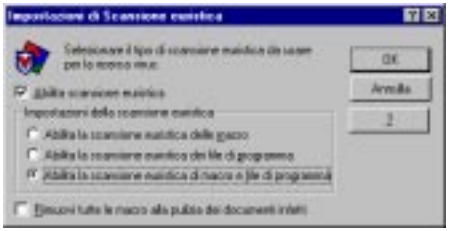

Figura 7-4. Finestra di dialogo Impostazioni di scansione dell'euristica della macro

La tecnologia di scansione euristica abilita il riconoscimento di nuovi virus da parte di Scansione posta sulla base della somiglianza con altri virus noti. A tal fine, il programma cerca le caratteristiche di "virus simili" in file già sottoposti a scansione. La presenza di un numero sufficiente di tali caratteristiche in un file consente a Scansione posta di individuare il file come potenzialmente infetto da un nuovo virus o da uno precedentemente non identificato.

Poiché Scansione posta ricerca simultaneamente le caratteristiche dei file che escludono la possibilità di infezione da virus, raramente darà indicazioni errate su un'infezione da virus. Quindi, a meno che non si sia certi che il file *non* contiene un virus, trattare le infezioni "probabili" con la stessa attenzione richiesta dalle infezioni certe.

Per attivare la scansione euristica, procedere come segue:

a. Selezionare la casella di controllo **Abilita scansione euristica macro**. Vengono attivate le altre opzioni della finestra di dialogo.

b. Selezionare il tipo di scansione euristica che si desidera che Scansione posta utilizzi. Le scelte disponibili sono:

   - **Abilita scansione euristica macro**. Scegliere questa opzione per consentire a Scansione posta di identificare tutti i file di Microsoft Word, Microsoft Excel e altri file di Microsoft Office che presentano macro incorporate e quindi di confrontare il codice macro al database di firme virus. Scansione posta identifica le corrispondenze esatte in base al nome del virus; le firme in codice che somigliano a virus esistenti consentono a Scansione posta di segnalare la presenza di un probabile virus macro.

- **Attiva scansione euristica del file di programma.** Scegliere questa opzione per consentire a Scansione posta di individuare nuovi virus nei file di programma esaminandone le caratteristiche e confrontandole con l'elenco delle caratteristiche dei virus noti. Scansione posta identificherà i file con un numero sufficiente di queste caratteristiche come virus probabili.
- **Attiva scansione euristica dei file di programma e di macro.** Scegliere questa opzione per consentire a Scansione posta di utilizzare entrambi i tipi di scansione euristica. Network Associates consiglia di utilizzare questa opzione per una protezione antivirus completa.

c. Determinare la modalità di trattamento dei file macro infetti. Selezionare **Rimuovi tutte le macro durante la pulizia di documenti infetti** per eliminare tutti i codici suscettibili di infezione dal documento e lasciare solo i dati. Per rimuovere solo il codice virus dalle macro del documento, non selezionare questa casella di controllo.

> **AVVERTENZA:** Utilizzare questa funzione con cautela: la rimozione di tutte le macro da un documento può provocare la perdita o il danneggiamento dei dati e l'impossibilità di utilizzarli.

d. Fare clic su **OK** per salvare le impostazioni e tornare alla finestra di dialogo Proprietà di Scansione posta.

3. Fare clic sulla scheda Azione per scegliere opzioni aggiuntive di Scansione posta. Per salvare le modifiche senza chiudere la finestra di dialogo Proprietà di Scansione posta, fare clic su **Applica**. Per salvare le modifiche e chiudere la finestra di dialogo, fare clic su **OK**. Fare clic su **Annulla** per chiudere la finestra di dialogo senza salvare le modifiche.

> **NOTA:** Facendo clic su **Annulla** non vengono ripristinate le modifiche salvate facendo clic su **Applica**.

Scelta delle opzioni Azione

Quando Scansione posta rileva un virus, richiede all'utente quale azione effettuare sul file infetto o esegue automaticamente l'azione determinata in precedenza. Utilizzare la pagina delle proprietà Azione per specificare le opzioni di risposta di Scansione posta al rilevamento di un virus o le azioni di risposta automatiche.

Procedere come segue:

1. Fare clic sulla scheda Azione nella finestra di dialogo Proprietà di Scansione posta per visualizzare la pagina delle proprietà appropriata (Figura 7-5).

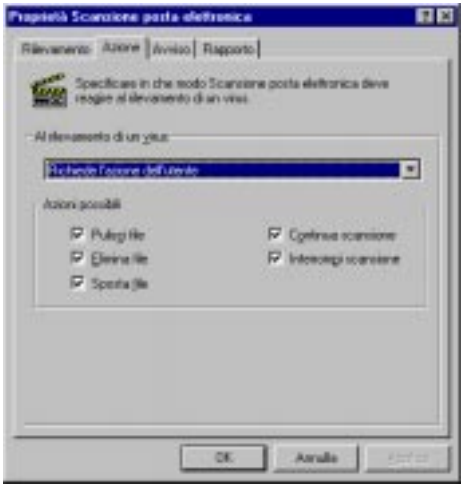

Figura 7-5. Finestra di dialogo Proprietà di Scansione posta - pagina Azione

2. Selezionare una risposta dall'elenco **Al rilevamento di un virus**. L'area immediatamente al di sotto dell'elenco cambia per visualizzare opzioni aggiuntive per ciascuna selezione. Le scelte disponibili sono:

   - **Richiedi azione.** Utilizzare quest'opzione se si prevede di assistere all'esame del disco da parte di Scansione posta: il programma visualizza un messaggio di avvertimento quando rileva un virus e consente di effettuare una serie di operazioni. Selezionare le opzioni di risposta che si desidera visualizzare nel messaggio di avviso:

     – **Pulisci file.** Quest'opzione fa in modo che Scansione posta rimuova il codice del virus dal file infetto.

     – **Elimina file.** Selezionare quest'opzione per eliminare immediatamente il file infetto in Scansione posta.

     – **Sposta file.** Selezionare quest'opzione per spostare il file infetto in una cartella di quarantena in Scansione posta.

     – **Continua scansione.** Selezionare quest'opzione per continuare la scansione senza effettuare altre operazioni in Scansione posta. Se le opzioni di registrazione sono abilitate, Scansione documento registra l'evento nel file di registro.

  - **Interrompi scansione.** Selezionare quest'opzione per interrompere immediatamente l'operazione di scansione in Scansione posta. Per continuare la scansione, fare clic su **Avvia scansione** per riavviare l'operazione.

- **Sposta automaticamente l'allegato infetto**. Selezionare quest'opzione per spostare i file infetti in una directory di quarantena di nome INFECTED in Scansione posta. Scansione posta crea la cartella INFECTED nel server di posta Exchange o Outlook.

  Non è possibile indicare una cartella diversa o cambiare il nome della cartella, ma la cartella INFECTED verrà visualizzata sotto la cartella di posta elettronica. É possibile aprire la cartella e visualizzare i messaggi in essa contenuti, ma quest'operazione potrebbe esporre il computer all'infezione da virus.

- **Pulisci automaticamente l'allegato infetto.** Selezionare quest'opzione per rimuovere il codice virus dall'allegato appena viene rilevato in Scansione posta. Se Scansione posta non è in grado di eliminare il virus, viene visualizzato un messaggio nell'area relativa e, se le funzioni di registrazione sono abilitate, l'evento viene memorizzato nel file registro. Per ulteriori dettagli, vedere "Selezione delle opzioni di Rapporto" a pagina 253.

- **Elimina automaticamente l'allegato infetto.** Selezionare quest'opzione per cancellare immediatamente gli allegati infetti rilevati in Scansione posta. Abilitare la funzione di rapporto per disporre di un registro degli allegati eliminati in Scansione posta. Sarà necessario ripristinare i file eliminati da copie di backup.

  AVVERTENZA: Scansione posta *non* tenta di spezzare i messaggi codificati per effettuarne la scansione. Se un file infetto contiene una struttura digitale, Scansione posta *rimuove* la firma digitale per ripulire o eliminare il file infetto.

- **Continua scansione.** Selezionare quest'opzione solo se si prevede di non assistere alle operazioni di Scansione posta. Se si attiva anche la funzione di rapporto di Scansione posta (per ulteriori dettagli, vedere "Selezione delle opzioni di Rapporto" a pagina 253), il programma visualizzerà un rapporto sui nomi di tutti i virus rilevati e dei nomi dei file infetti in modo che sia possibile eliminarli in futuro.

3. Fare clic sulla scheda Avviso per selezionare le opzioni aggiuntive di Scansione posta. Per salvare le modifiche senza chiudere la finestra di dialogo Proprietà di Scansione posta, fare clic su **Applica**. Per salvare le modifiche e chiudere la finestra di dialogo, fare clic su **OK**. Fare clic su **Annulla** per chiudere la finestra di dialogo senza salvare le modifiche.

> **NOTA:** Facendo clic su **Annulla** non vengono ripristinate le modifiche salvate facendo clic su **Applica**.

Selezione delle opzioni di Avviso

Una volta configurato con le opzioni di risposta desiderate, Scansione posta ricerca ed elimina i virus dal sistema automaticamente, appena ne rileva la presenza, senza ulteriori interventi da parte dell'utente. Tuttavia, se l'utente desidera che Scansione posta lo informi immediatamente quando rileva un virus per agire in modo appropriato, è possibile configurarlo per l'invio di messaggi in vari modi. Utilizzare la pagina delle proprietà Avviso per scegliere i metodi di avviso che si desidera utilizzare.

Procedere come segue:

1. Fare clic sulla scheda Avviso nella finestra di dialogo Proprietà Scansione posta per visualizzare la pagina delle proprietà appropriata (Figura 7-6).

Figura 7-6. Finestra di dialogo Proprietà Scansione posta - pagina Avviso

2. Per attivare l'invio di un messaggio di avviso da parte di Scansione posta a un server su cui è in esecuzione NetShield, una soluzione antivirus per server di Network Associates, selezionare la casella di controllo **Invia avviso di rete**, quindi digitare il percorso alla cartella dell'avviso di NetShield in rete o fare clic su **Sfoglia** per individuare la cartella appropriata.

   NOTA: La cartella scelta deve contenere CENTALRT.TXT, il file di avviso centralizzato di NetShield. NetShield raccoglie i messaggi di avviso inviati da Scansione posta e da altro software di Network Associates, quindi li trasferisce agli amministratori di rete per le opportune azioni Per ulteriori informazioni sull'Avviso centralizzato, consultare il *Manuale dell'utente* di NetShield.

3. Selezionare la casella di controllo **Invia posta al mittente** per inviare un messaggio di avviso al mittente dell'allegato di posta infetto. É possibile quindi comporre una risposta standard da inviare. Procedere come segue:

   a. Per aprire un messaggio di posta standard, fare clic su **Configura**.

   b. Compilare la riga dell'oggetto, quindi aggiungere i commenti desiderati nel corpo del messaggio, sotto l'avviso di infezione fornito da Scansione posta. É possibile aggiungere fino a 1024 caratteri di testo.

   c. Per inviare una copia di questo messaggio ad altri, immettere un indirizzo di posta elettronica nella casella di testo o fare clic su **Cc:** per selezionare un destinatario nella directory dell'utente del sistema di posta o nella rubrica.

   d. Fare clic su **OK** per salvare il messaggio.

   Ogni volta che rileva un virus, Scansione posta invia una copia del messaggio a tutti coloro che inviano allegati di posta elettronica infetti. Nell'indirizzo del destinatario vengono inserite le informazioni rilevate nell'intestazione originale del messaggio e nell'area al di sotto della riga dell'oggetto viene identificato il virus e il file infetto. Se è stata attivata la funzione di rapporto, Scansione posta registra anche ciascuna istanza di invio di messaggi di avviso.

4. Per inviare messaggi di posta per avvisare della presenza di allegati infetti, selezionare la casella di controllo **Invia avviso all'utente**.
   É possibile quindi comporre una risposta standard da inviare a uno o più destinatari: ad esempio, un amministratore di rete, ogni volta che Scansione posta rileva un allegato di posta elettronica infetto. Procedere come segue:

a. Per aprire un messaggio di posta standard, fare clic su **Configura**.

b. Digitare un indirizzo di posta elettronica nella casella di testo, o fare clic su **A:** per selezionare un destinatario nella directory dell'utente del sistema di posta o nella rubrica. Ripetere l'operazione nella casella di testo **Cc:** per inviare una copia del messaggio ad altri utenti.

> **NOTA:** Per ricercare un indirizzo di posta elettronica in questo modo, è necessario disporre dell'accesso alla directory dell'utente MAPI compatibile. Se si sta lavorando non in linea e ancora non ci si è collegati al sistema di posta elettronica, Scansione posta richiede di selezionare un profilo utente da usare per il collegamento al sistema. Digitare le informazioni richieste e premere **OK** per continuare.

c. Compilare la riga dell'oggetto, quindi aggiungere i commenti desiderati nel corpo del messaggio al di sotto dell'avviso di infezione. É possibile aggiungere fino a 1024 caratteri di testo.

d. Fare clic su **OK** per salvare il messaggio.

Ogni volta che rileva un virus, Scansione posta invia una copia del messaggio a tutti gli indirizzi digitati al Passaggio b. Nell'area immediatamente al di sotto della riga dell'oggetto vengono aggiunte le informazioni per l'identificazione del virus e del file infetto. Se è stata attivata la funzione di rapporto, Scansione posta registra anche ciascuna istanza di invio di messaggi di avviso.

5. Per inviare messaggi di avviso con Scansione posta tramite l'interfaccia del componente DMI ad applicazioni per la gestione del desktop e della rete in esecuzione sulla propria rete, selezionare la casella di controllo **Avviso DMI**.

> **NOTA:** DMI (Desktop Management Interface) è uno standard per la comunicazione di richieste di gestione e informazioni di avviso tra i componenti hardware e software dei computer o collegati ad essi e le applicazioni utilizzate per la loro gestione. Per ulteriori informazioni sul metodo di avviso, contattare l'amministratore della rete.

6. Se nella pagina Azione è stata selezionata la risposta **Richiedi azione** (per ulteriori dettagli, vedere pagina 248), è anche possibile fare in modo che Scansione posta emetta un segnale acustico e visualizzi un messaggio personalizzato quando rileva un virus. Per effettuare quest'operazione, selezionare la casella di controllo **Visualizza messaggio personalizzato**, quindi digitare il messaggio che si desidera visualizzare nella relativa casella di testo: è possibile digitare fino a 225 caratteri. Selezionare poi la casella di controllo **Segnale acustico**.

7. Fare clic sulla scheda Rapporto per selezionare le opzioni aggiuntive di Scansione posta. Per salvare le modifiche senza chiudere la finestra di dialogo Proprietà di Scansione posta, fare clic su **Applica**. Per salvare le modifiche e chiudere la finestra di dialogo, fare clic su **OK**. Fare clic su **Annulla** per chiudere la finestra di dialogo senza salvare le modifiche.

> **NOTA:** Facendo clic su **Annulla** non vengono ripristinate le modifiche salvate facendo clic su **Applica**.

Selezione delle opzioni di Rapporto

Scansione posta elenca le impostazioni correnti e riporta tutte le azioni effettuate durante la scansione in un file registro denominato MAILSCAN.TXT. É possibile impostare la scrittura in questo file da parte di Scansione posta o utilizzare un editor di testo qualsiasi per creare un file di testo da utilizzare in Scansione posta. É possibile aprire e stampare il file registro per una revisione successiva dall'interno di Scansione posta o con un editor di testo.

Utilizzare la pagina delle proprietà Rapporto per determinare quali informazioni includere nel file di registro di Scansione posta.

Per impostare la registrazione delle azioni di Scansione posta in un file di registro, procedere come segue:

1. Fare clic sulla scheda Rapporto nella finestra di dialogo Proprietà di Scansione posta per visualizzare la pagina delle proprietà appropriata (Figura 7-7 a pagina 254).

Figura 7-7. Finestra di dialogo Proprietà di Scansione posta - pagina Rapporto

2. Selezionare la casella di controllo **Registra su file**.

   Per valore predefinito, Scansione posta memorizza le informazioni di registrazione nel file MAILSCAN.TXT nella directory del programma VirusScan. É possibile digitare un nome diverso nella relativa casella di testo o fare clic su **Sfoglia** per individuare un file adatto in un'altra directory sul disco rigido o in rete.

3. Per ridurre al minimo le dimensioni del file di registro, selezionare la casella di controllo **Limita dimensione file di registro a**, quindi immettere un valore per le dimensioni in kilobyte del file nella relativa casella di testo.

   Immettere un valore compreso tra 10KB e 999KB. Per valore predefinito, Scansione posta limita le dimensioni del file a 100KB. Se i dati contenuti nella registrazione superano le dimensioni del file impostate, Scansione posta cancella il file esistente e ricomincia dal punto in cui ha interrotto il file.

4. Selezionare le caselle di controllo corrispondenti alle informazioni che si desidera registrare nel file di registro di Scansione posta. Si può scegliere di registrare tutte le seguenti informazioni:

   - **Rilevamento virus.** Selezionare questa casella di controllo per annotare il numero dei file infetti rilevati durante la scansione in Scansione posta.
   - **Pulizia virus.** Selezionare questa casella di controllo per annotare il numero dei file infetti dai quali è stato rimosso il virus in Scansione posta.
   - **Eliminazione di file infetti.** Selezionare questa casella di controllo per annotare il numero dei file infetti cancellati dal server di posta elettronica in Scansione posta.
   - **Spostamento file infetti.** Selezionare questa casella di controllo per annotare il numero di file infetti spostati nella directory di quarantena del server di posta elettronica in Scansione posta.
   - **Impostazioni sessione.** Selezionare questa casella di controllo per elencare le opzioni selezionate nella finestra di dialogo Proprietà di Scansione per ciascuna sessione di scansione in Scansione posta.
   - **Riepilogo sessione.** Selezionare questa casella di controllo per riepilogare le azioni di Scansione posta durante ciascuna sessione di scansione. Le informazioni di riepilogo includono il numero di file sottoposti a scansione, il numero e il tipo di virus rilevati, il numero di file spostati o eliminati e altre informazioni.
   - **Data e ora.** Selezionare questa casella di controllo per aggiungere la data e l'ora a ciascuna registrazione in Scansione posta.
   - **Nome utente.** Selezionare questa casella di controllo per aggiungere il nome utente collegato al server di posta elettronica nel momento in cui vengono effettuate le singole registrazioni.

5. Fare clic su una scheda diversa per modificare le impostazioni di Scansione posta. Per salvare le modifiche senza chiudere la finestra di dialogo Proprietà di Scansione posta, fare clic su **Applica**. Per salvare le modifiche e chiudere la finestra di dialogo, fare clic su **OK**. Fare clic su **Annulla** per chiudere la finestra di dialogo senza salvare le modifiche.

❑ **NOTA:** Facendo clic su **Annulla** non vengono ripristinate le modifiche salvate facendo clic su **Applica**.

Scansione di cc:Mail

VirusScan include il supporto per l'ultima generazione di software client per posta elettronica basato su standard MAPI per Microsoft, compresi i client Exchange e Outlook di Microsoft e la versione 8.0 e successive di cc:Mail di Lotus Development. Se si utilizzano versioni precedenti di cc:Mail, la versione 6.0 o la 7.0, è necessario installare il componente cc:Mail di VirusScan per effettuare la ricerca di virus in Posta in arrivo.

IMPORTANTE: Per installare il componente Scansione cc:Mail, selezionare l'opzione di installazione Personalizzata durante l'installazione, poiché l'installazione di questo componente in VirusScan non è predefinita. Per ulteriori dettagli, vedere pagina 43.

Una volta installata, Scansione cc:Mail si collega a VShield e accede al sistema cc:Mail, quindi effettua la scansione in background, controllando i nuovi messaggi nella Posta in arrivo di cc:Mail. Quando si ricevono nuovi messaggi, Scansione cc:Mail richiama VShield per l'esame di eventuali allegati infetti prima che il software del client li scarichi sul computer.

La sola reale interazione con Scansione cc:Mail avviene tramite la scelta dei sistemi di posta aziendali che si desidera che VShield sottoponga a scansione per la ricerca dei virus. Per ulteriori informazioni su come specificare cc:Mail come sistema di posta aziendale, consultare Capitolo 4, pagina 108.

Se l'utente non è ancora collegato al server cc:Mail, Scansione cc:Mail potrebbe chiedere di specificare il nome dell'utente e la password nella schermata di collegamento in modo che VShield possa accedere al server cc:Mail e sottoporre a scansione la posta in arrivo. Immettere il nome utente e la password cc:Mail, come se ci si volesse collegare direttamente a cc:Mail, quindi fare clic su **OK** per continuare. Avviare quindi l'applicazione client cc:Mail e impostare l'intervallo di polling del server cc:Mail su un periodo superiore a cinque minuti. Ciò consente a VShield di esaminare la posta elettronica prima che essa venga richiamata dal software del client.

Il componente cc:Mail si scollega dal server di posta elettronica quando si esce dal software del client senza salvare.

Uso di ScreenScan

Il componente ScreenScan di VirusScan fornisce una scansione per la ricerca di virus in background quando viene attivato lo screen saver del computer. Con questo componente, è possibile attivare il periodo di inattività del computer impostando il controllo automatico delle infezioni da virus. ScreenScan non effettua azioni sui virus rilevati, ma registra i risultati della scansione in un file di registro che è possibile visualizzare quando si desidera.

Per utilizzare ScreenScan, selezionare l'opzione di installazione Personalizzata durante l'installazione, poiché l'installazione di questo componente in VirusScan non è predefinita. Per ulteriori dettagli, vedere pagina 42. Una volta installato, ScreenScan visualizza una pagina delle proprietà nella finestra di dialogo Proprietà - Schermo di Windows. In questa pagina è possibile selezionare le opzioni di rilevamento e di rapporto che si desidera utilizzare in ScreenScan.

Per configurare ScreenScan, procedere come segue:

1. Fare clic sul pulsante **Avvio** (Windows 95) o su **Start** (Windows 98) sulla barra delle applicazioni, scegliere **Programmi**, quindi **Prompt di MS-DOS**.

2. Fare doppio clic su Schermo in Pannello di controllo per aprire la finestra di dialogo Proprietà - Schermo. Fare quindi clic sulla scheda McAfee ScreenScan per visualizzare la pagina delle proprietà appropriata (consultare Figura 7-8).

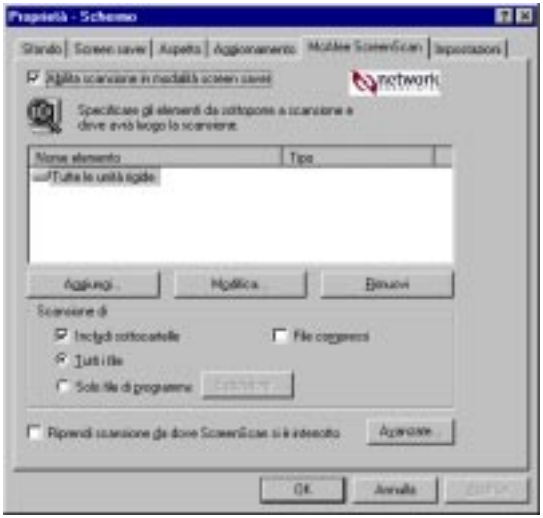

Figura 7-8. Finestra di dialogo Proprietà - Schermo -pagina McAfee ScreenScan

3. Selezionare la casella di controllo **Abilita scansione in modalità screen saver** per attivare le opzioni nel resto della pagina delle proprietà.

4. Selezionare le parti del sistema che si desidera siano controllate per rilevare virus da ScreenScan. È possibile:

- **Aggiungere obiettivi da sottoporre a scansione.** Fare clic su **Aggiungi** per aprire la finestra di dialogo Aggiungi elemento di scansione (Figura 7-9).

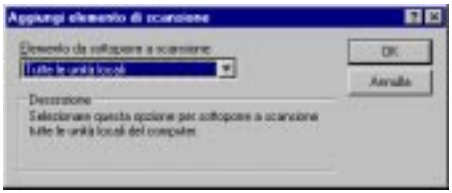

Figura 7-9. Finestra di dialogo Aggiungi elemento di scansione

Selezionare quindi l'obiettivo da sottoporre a scansione nell'elenco. Le scelte disponibili sono:

  - **Tutte le unità locali.** Selezionando quest'opzione, ScreenScan effettua la scansione di tutte le unità, dischi rigidi e dischetti, collegati fisicamente al computer o inseriti nell'unità a dischetti. Quest'opzione è la più sicura e completa disponibile in ScreenScan.
  - **Tutte le unità disco rigido.** ScreenScan sottopone a scansione solo i dischi rigidi collegati fisicamente al computer.
  - **Unità o cartella.** ScreenScan sottopone a scansione un disco o una cartella particolare del computer. Digitare quindi nella casella di testo fornita la lettera di unità o il percorso alla cartella che si desidera sottoporre a scansione oppure fare clic su **Sfoglia** per localizzare l'obiettivo di scansione sul computer. Per chiudere la finestra di dialogo, fare clic su **OK**.

    IMPORTANTE: Per effettuare la scansione di tutte le sottocartelle nell'obiettivo di scansione, selezionare la casella di controllo **Includi sottocartelle** nell'area **Oggetto da scandire** della pagina delle proprietà di ScreenScan.

- **Cambia obiettivi di scansione.** Selezionare uno degli obiettivi di scansione in elenco, quindi fare clic su **Modifica** per aprire la finestra di dialogo Modifica elemento di scansione (Figura 7-10 a pagina 259).

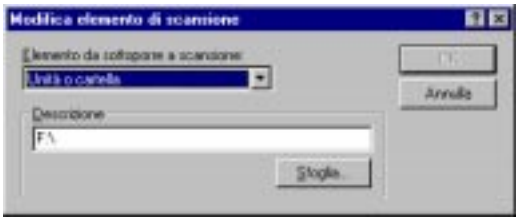

Figura 7-10. Finestra di dialogo Modifica elemento di scansione

Viene visualizzata la finestra di dialogo con l'obiettivo di scansione esistente specificato. Selezionare o immettere un nuovo obiettivo di scansione, quindi fare clic su **OK** per chiudere la finestra di dialogo.

- **Rimuovere gli obiettivi di scansione.** Selezionare uno degli obiettivi di scansione elencati, quindi fare clic su **Rimuovi** per eliminarlo.

5. Specificare il tipo di file che si desidera siano sottoposti a scansione da ScreenScan. È possibile:

   - **Eseguire la scansione di file compressi.** Selezionare la casella di controllo **File compressi** per effettuare la ricerca di virus con ScreenScan nei file compressi nei formati .CAB, .LZH o ZIP.

   - **Scegliere il tipo di file da sottoporre a scansione.** Normalmente i virus non sono in grado di attaccare i file di dati o i file che non contengono un codice eseguibile. Si può, quindi, restringere l'ambito delle operazioni di scansione in modo che ScreenScan verifichi solo i file esposti maggiormente al rischio di infezioni. A tal fine, selezionare il pulsante **Solo file di programma**. Per visualizzare o indicare le estensioni dei nomi file che saranno analizzati da ScreenScan, fare clic su **Estensioni** per aprire la finestra di dialogo Estensioni file di programma (Figura 7-11).

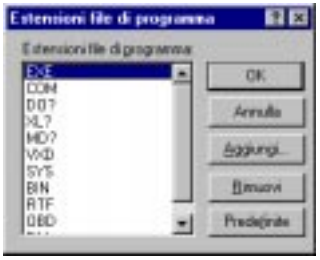

Figura 7-11. Finestra di dialogo Estensioni file di programma

In base alle impostazioni predefinite, ScreenScan cerca i virus nei file con le estensioni .EXE, .COM, .DO?, .XL?, .RTF, .BIN, .SYS, .MD?, .VXD, .OBD e .DLL. I file con estensione .DO?, .XL?, .RTF e .OBD sono file di Microsoft Office. Tutti questi file possono essere infettati da virus macro. Il ? è un carattere jolly che abilita la scansione di file di documento e di modello da parte di ScreenScan.

- Per effettuare aggiunte all'elenco, fare clic su **Aggiungi**, successivamente digitare le estensioni che ScreenScan deve sottoporre a scansione nella finestra di dialogo che viene visualizzata.
- Per eliminare un'estensione dall'elenco, selezionarla, quindi fare clic su **Elimina**.
- Fare clic su **Predefinite** per ripristinare l'elenco nella sua forma originaria.

Al termine, scegliere **OK** per chiudere la finestra di dialogo.

Per far sì che ScreenScan esamini tutti i file sul sistema, indipendentemente dall'estensione, selezionare il pulsante **Tutti i file**. Questa operazione rallenta notevolmente il sistema, ma garantisce la completa eliminazione dei virus.

6. Determinare le modalità delle operazioni di scansione di ScreenScan rispetto ad altre operazioni prioritarie del computer. Fare clic su **Avanzate** per aprire la finestra di dialogo Impostazioni di scansione avanzate (Figura 7-12).

Figura 7-12. Finestra di dialogo Impostazioni di scansione avanzate

Trascinare la barra di scorrimento verso sinistra per assegnare a ScreenScan una priorità più bassa rispetto ad altri programmi in esecuzione sul computer, incluso lo screen saver. Quest'opzione provoca il rallentamento della scansione del sistema da parte di ScreenScan, ma consente di eseguire altri programmi in modo uniforme. Trascinare la barra di scorrimento verso destra per assegnare a ScreenScan una priorità relativamente alta per le attività di scansione. L'operazione di scansione viene completata più rapidamente, ma l'esecuzione contemporanea di altri programmi non è uniforme come nel caso precedente.

7. Abilitazione della funzione di rapporto di ScreenScan.

   Selezionare la casella di controllo **Abilita registrazione delle attività di ScreenScan su file**. Per impostazione predefinita, ScreenScan registra le azioni in un file di testo denominato SCREENSCAN ACTIVITY LOG.TXT. Per selezionare un file di testo diverso da utilizzare come file di rapporto di ScreenScan, immettere il percorso e il nome file nella casella di testo fornita o fare clic su **Sfoglia** per individuare un file adatto sul disco rigido.

   ❑ **NOTA:** ScreenScan non crea nuovi file di rapporto. Per fare in modo che il programma utilizzi un file di registro diverso, selezionare un file di testo esistente che ScreenScan possa aprire e modificare.

   Per salvare le modifiche apportate e chiudere la finestra di dialogo, fare clic su **OK**. Fare clic su **Annulla** per chiudere la finestra di dialogo senza salvare le modifiche.

8. Per avviare la scansione dal punto in cui era stata interrotta da ScreenScan, selezionare la casella di controllo **Riprendi scansione dopo interruzione di ScreenScan**. Se non si seleziona questa casella di controllo, ScreenScan comincia la scansione dalla prima voce nell'elenco degli obiettivi da sottoporre a scansione, indipendentemente dal completamento della scansione sull'obiettivo.

9. Per salvare le modifiche senza chiudere la finestra di dialogo Proprietà-Schermo, fare clic su **Applica**. Per salvare le modifiche e chiudere la finestra di dialogo, fare clic su **OK**. Fare clic su **Annulla** per chiudere la finestra di dialogo senza salvare le modifiche.

> **NOTA:** Facendo clic su **Annulla** non vengono ripristinate le modifiche salvate facendo clic su **Applica.**

ScreenScan viene eseguito alla successiva entrata in modalità screen saver. Se si modificano gli screen saver, è necessario configurare nuovamente le opzioni di ScreenScan.

Uso di SecureCast per l'aggiornamento del software A

Introduzione a SecureCast

Con il servizio SecureCast di Network Associates è possibile scaricare facilmente gli ultimi aggiornamenti del prodotto e dei file di dati direttamente sul proprio desktop. Grazie a tale servizio, è possibile infatti ricevere via Internet gli aggiornamenti del proprio software in licenza Network Associates a scadenze regolari e in modo totalmente automatico. Per poter utilizzare questa opzione, è necessario installare il software client SecureCast e abbonarsi al canale Home SecureCast (nel caso di privati) o al canale Enterprise SecureCast (nel caso di aziende).

I privati, tra le altre cose, hanno la possibilità di scaricare i nuovi file su segnalazione del software solo e se decidono di aggiornare il proprio sistema. Chi lavora presso un'azienda (ma non come amministratore) deve invece chiedere al proprio amministratore quando è necessario aggiornare i file oppure utilizzare la funzione di Aggiornamento automatico, se inclusa nel prodotto.

Scegliere una delle opzioni di aggiornamento illustrate in questa appendice per proteggere in modo efficace tutto il proprio sistema, dalla rete al desktop. Con SecureCast è possibile avere le ultime versioni dei file di dati e di programma non appena questi diventano disponibili. Ogni mese vengono introdotti oltre 200 tra nuovi virus e altri agenti dannosi: allora perché rischiare di vedere danneggiati i propri dati o diventare inaccessibile la propria rete solo per aver dimenticato di aggiornare il software antivirus?

❑ **NOTA:** Con il termine "aggiornamento", si intende l'integrazione del prodotto esistente con le nuove versioni dei file di dati (.DAT). Con il termine "perfezionamento", si intendono le revisioni del prodotto, i file eseguibili e i file di dati. Network Associates fornisce aggiornamenti gratuiti dei file .DAT per tutta la durata del prodotto. Questo non garantisce però che i file .DAT siano sempre compatibili con le versioni precedenti del prodotto. Aggiornando regolarmente il proprio software all'ultima versione del prodotto e dei file .DAT mediante SecureCast, ci si assicura la completa protezione per tutta la durata dell'abbonamento o del piano di manutenzione.

Perché aggiornare i propri file di dati

Per fornire la migliore protezione possibile, Network Associates aggiorna continuamente i file di dati che rilevano i nuovi virus e altri agenti dannosi. È vero che il software si basa su una tecnologia in grado di rilevare famiglie di virus e codici dannosi fino a quel momento sconosciuti, tuttavia vengono continuamente introdotti nuovi tipi di virus e altri agenti. Il software esistente spesso non può rilevare questi intrusi proprio perché i file di dati sono diventati obsoleti. È il software stesso a segnalare periodicamente di aggiornare tali file. Per la massima protezione, Network Associates consiglia di aggiornare regolarmente i propri file.

Quali file di dati vengono scaricati mediante SecureCast

Con SecureCast vengono scaricati automaticamente i seguenti file di dati comuni:

- NAMES.DAT - contiene i nomi dei virus e altri dettagli che l'utente può consultare visualizzando la finestra Elenco virus.
- SCAN.DAT - contiene i dati relativi alle stringhe di rilevamento per tutti i virus rilevati.
- CLEAN.DAT - contiene i dati relativi alle stringhe di rimozione per tutti i virus rimossi.

Oltre ai comuni file .DAT sopra elencati, è anche possibile ricevere alcuni dei seguenti file aggiuntivi, a seconda dei prodotti antivirus o di sicurezza utilizzati:

- WEBSCANX.DAT o INTERNET.DAT - contengono i dati relativi alle stringhe di rilevamento per applet Java e controlli ActiveX dannosi. Questi file sono utilizzati da WebShieldX e VirusScan.
- MCALYZE.DAT - contiene i dati relativi alle stringhe di rilevamento per virus polimorfi complessi. Questo file è utilizzato dai prodotti Network Associates a 32 bit con motore dalla versione 3.0.0 alla versione 3.1.4.
- POLYSCAN.DAT - contiene i dati relativi alle stringhe di rilevamento per virus polimorfi complessi. Questo file è utilizzato dai prodotti Network Associates a 32 bit con motore 3.1.5 e versioni successive.

Requisiti di sistema

- Windows 95 o versioni successive oppure Windows NT
- Almeno 100MB di spazio libero su disco: Home SecureCast (client e canale) 7MB, più da 3 a 6MB per scaricamento. Enterprise SecureCast (client e canale) 15MB, più da 6 a 6,5MB per scaricamento.
- Una connessione a Internet attiva, diretta o con chiamata telefonica, per almeno un'ora a settimana.

Caratteristiche di SecureCast

- SecureCast utilizza software client sviluppato con tecnologie BackWeb.
- Con SecureCast non è più necessario scaricare file di aggiornamento dai servizi elettronici di Network Associates.
- SecureCast funziona in modo invisibile in background, lasciando la priorità ad altre applicazioni e utilizzando la connessione a Internet quando è inattiva. È anche possibile configurare il proprio client desktop in modo da assegnare una priorità più alta agli scaricamenti mediante SecureCast.
- SecureCast interagisce con la maggior parte dei firewall aziendali.
- SecureCast supporta connessioni TCP/IP a 32 bit per gli abbonati ai canali Enterprise SecureCast e Home SecureCast e fornisce connessioni non Internet per i privati che si collegano con chiamata telefonica tramite modem asincrono.
- SecureCast scarica i file .ZIP, .EXE e .DAT direttamente sul desktop dell'utente come InfoPak BackWeb.

Servizi gratuiti

- Scaricamento automatico dei file .DAT. I nuovi file .DAT in genere sono disponibili intorno al 15 del mese.
- Segnalazione della scoperta di nuovi virus dannosi.
- Annuncio di nuove versioni del software e dei prodotti associati.

Canale Home SecureCast

I privati possono installare il software client SecureCast dal CD-ROM Network Associates.

Funzionamento di SecureCast

I privati possono utilizzare il servizio di scaricamento, puntuale e gratuito, di SecureCast nei seguenti modi:

- per ricevere automaticamente via Internet gli ultimi aggiornamenti del software in licenza Network Associates, installare il client SecureCast e abbonarsi al canale Home SecureCast, oppure
- per aggiornare il software quando lo desiderano, utilizzando il programma di utility apposito incluso quando il software ne segnala la necessità.

Scaricamento automatico

Installazione di Home SecureCast

Per abbonarsi al canale Home SecureCast, procedere come segue:

1. Installare il software client BackWeb dal CD-ROM Network Associates.

   Si riceverà un InfoPak introduttivo a conferma che la connessione al canale Home SecureCast funziona. Un InfoPak può contenere, tra l'altro, suoni, animazioni e pagine Web. Quando si riceve un nuovo InfoPak da Home SecureCast, compare automaticamente come oggetto animato sul desktop finché non viene aperto. Per aprire un InfoPak, fare doppio clic su di esso.

2. Completare la registrazione al canale mediante la finestra di dialogo User Registration Information (che verrà visualizzata nel primo o nel secondo InfoPak che si riceve), quindi fare clic su **Next**.

   Nella finestra di dialogo Online Activity Status è indicato lo stato della trasmissione dati.

3. Al termine, prendere nota del proprio numero di registrazione e fare clic su **Finish**.

Uso di Home SecureCast

Si è ora pronti a ricevere periodici avvisi di virus, nonché gli aggiornamenti del prodotto. Nel giro di qualche giorno si riceveranno ulteriori InfoPak. Fare doppio clic su di essi per estrarre e installare gli aggiornamenti che contengono.

Annullamento dell'abbonamento a Home SecureCast

Per annullare il servizio in qualsiasi momento, procedere come segue:

1. Fare doppio clic sull'icona del client SecureCast nella barra delle applicazioni di Windows.
2. Fare clic con il pulsante destro del mouse sul pulsante del canale **Home**.

   Comparirà un menu di scelta rapida.
3. Fare clic su **Annulla abbonamento**, quindi fare clic su **OK** per confermare.

Avvio di uno scaricamento

Aggiornamento del software registrato

Il software Network Associates comprende una funzione che segnala periodicamente di effettuare l'aggiornamento. Se sono trascorsi diversi mesi dall'installazione iniziale del software, Network Associates consiglia di utilizzare le opzioni di aggiornamento descritte nelle sezioni che seguono per essere certi di avere le ultime versioni disponibili dei file di dati e del prodotto.

Aggiornamento dopo l'installazione

Dopo l'installazione del software antivirus o di sicurezza, la finestra introduttiva (Figura A-1 a pagina 268) richiede di effettuare l'aggiornamento. Tale finestra compare anche quando si avvia un sistema con il software Network Associates precaricato per la quinta volta. McAfee VirusScan ad esempio visualizza il seguente avviso:

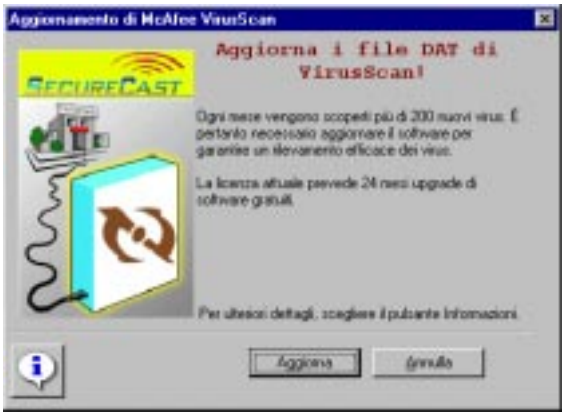

Figura A-1. Finestra introduttiva

1. Fare clic su **Aggiorna** per ricevere gratuitamente l'ultima versione del software.

   Verrà visualizzata la finestra di dialogo Internet Access (Figura A-2).

Figura A-2. Finestra di dialogo Internet Access

2. Se si ha l'accesso diretto a Internet, selezionare **Yes**, quindi fare clic su **Next**. in caso contrario selezionare **No**, quindi fare clic su **Next**.

   - Se si è selezionato **Yes**, verrà visualizzata la finestra di dialogo User Registration (Figura A-3 a pagina 269).

Figura A-3. Finestra di dialogo User Registration

Specificare le informazioni richieste. Per spostarsi tra le varie caselle di testo, premere il tasto TAB. Una volta terminata l'immissione delle informazioni, fare clic su **Next>**.

- Se si è selezionato **No**, verrà visualizzata la finestra di dialogo del server di scaricamento (Figura A-4). In tale finestra immettere o verificare l'indicativo del proprio paese e quello della propria località, quindi selezionare il server più vicino.

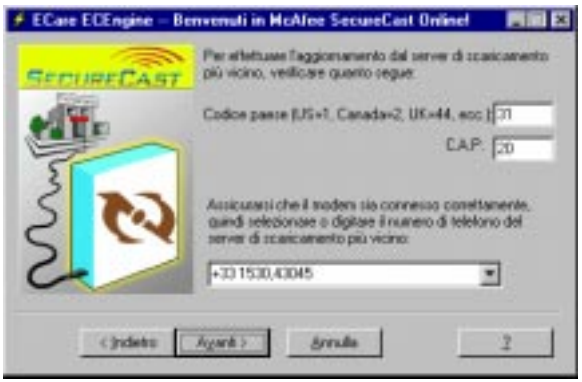

Figura A-4. Finestra di dialogo Server

> **NOTA:** Lo scaricamento dei file .DAT da server Network Associates con chiamata telefonica può comportare costi elevati dovuti alla tariffa interurbana.

Una volta terminata l'immissione delle informazioni, fare clic su **Next>** per continuare.

Il sistema si connetterà a un server Network Associates.

- Se sul server non vi sono nuovi aggiornamenti dei file .DAT o del software, la finestra di dialogo Online Activity Status (Figura A-5) indicherà che i file di cui si dispone sono aggiornati.

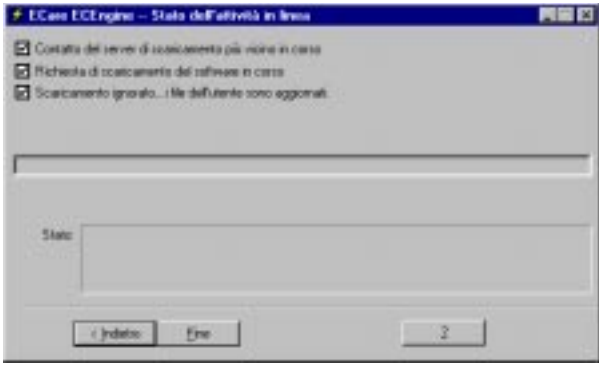

Figura A-5. Finestra di dialogo Online Activity Status (Nessuno scaricamento)

Fare clic su **Finish** per disconnettersi dal server.

- Se sul server vi sono nuovi file .DAT, la finestra di dialogo Online Activity Status (Figura A-6 a pagina 271) indicherà che è in corso lo scaricamento automatico sul sistema del file .EXE contenente i file .DAT.

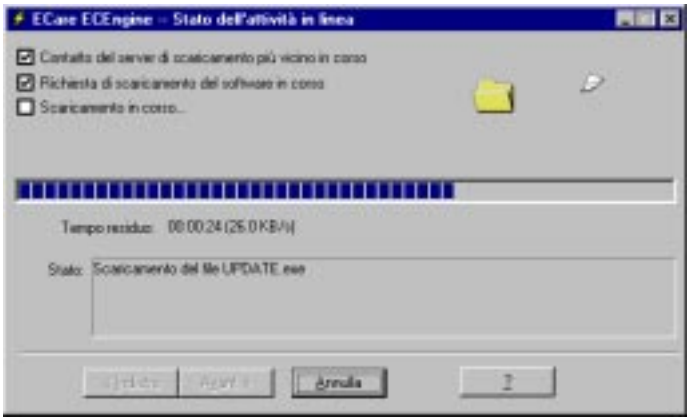

Figura A-6. Finestra di dialogo Online Activity Status

a. Al termine dello scaricamento, fare clic su **Next**. Verrà visualizzata la finestra di dialogo Online Activity Complete (Figura A-7).

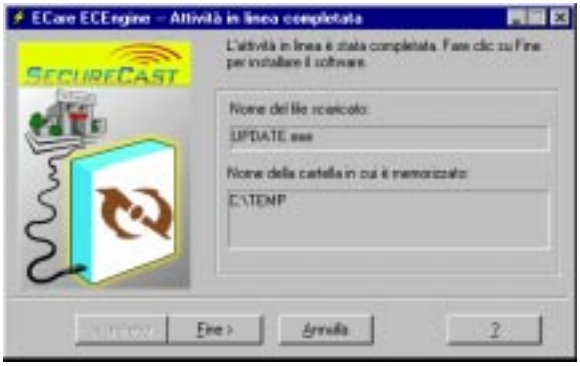

Figura A-7. Finestra di dialogo Online Activity Complete

b. Fare clic su **Finish** per installare i nuovi aggiornamenti dei file .DAT.

- Se sul server è presente una versione del prodotto più recente di quella di cui si dispone, verrà visualizzata la finestra di dialogo Newer Component Found (Figura A-8). Per scaricare solo gli ultimi file .DAT invece dell'intero prodotto, selezionare **DAT files only**, quindi fare clic su **Next**. Per scaricare una nuova versione del prodotto, fare clic su **Next**.

Figura A-8. Finestra di dialogo Newer Component Found

Nella finestra di dialogo Online Activity Status (vedere la Figura A-6 a pagina 271) verrà indicato lo stato dello scaricamento. Al termine dello scaricamento, fare clic su **Next** per continuare.

La finestra di dialogo Online Activity Complete (Figura A-9) confermerà che lo scaricamento è terminato.

Figura A-9. Finestra di dialogo Online Activity Complete

3. Prendere nota del nome e dell'ubicazione del file scaricato, quindi fare clic su **Finish** per installare il software.

Aggiornamento a intervalli periodici

A intervalli di 30 giorni la finestra di dialogo Aggiorna (Figura A-10) segnala di aggiornare il software.

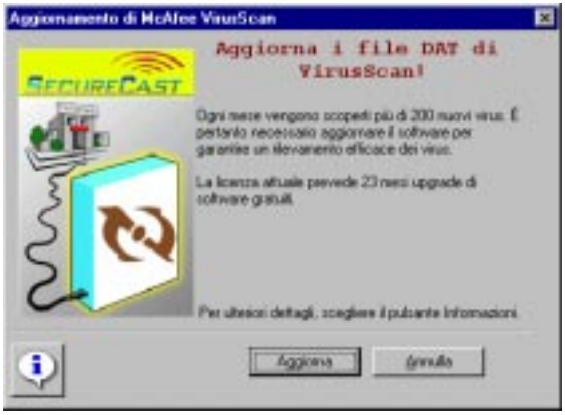

Figura A-10. Finestra di dialogo Aggiorna

Se l'utente è registrato, procedere come segue per ricevere gratuitamente le ultime versioni dei file di dati. Ripetere tale procedura tutti i mesi, quando il software lo segnala, in modo da avere sempre file aggiornati.

NOTA: In quanto utenti registrati, è possibile continuare a ricevere gli aggiornamenti dei file .DAT per tutta la durata del prodotto. Network Associates non può tuttavia garantire la compatibilità tra i futuri aggiornamenti dei file .DAT e le versioni più vecchie del prodotto. Ottenendo l'ultima versione del software mediante SecureCast ci si assicura una protezione completa dai virus per tutta la durata dell'abbonamento al software o del piano di manutenzione.

---

1. Fare clic su **Update** per ricevere gratuitamente le ultime versioni dei file di dati.

   Verrà visualizzata la finestra di dialogo Internet Access (vedere la Figura A-2 a pagina 268).

2. Se si ha l'accesso diretto a Internet, selezionare **Yes**, quindi fare clic su **Next**. Se non si ha l'accesso diretto a Internet, selezionare **No**, quindi fare clic su **Next**.

Verrà visualizzata la finestra di dialogo Server (vedere la Figura A-4 a pagina 269). Se si è selezionato **Yes**, la casella del numero telefonico da chiamare non sarà disponibile; se invece si è selezionato **No**, tale casella sarà accessibile.

3. Se si ha l'accesso diretto a Internet, verificare l'identificativo del proprio paese e quello della propria località, quindi fare clic su **Next**. Se non si ha l'accesso diretto a Internet, verificare l'identificativo del proprio paese e quello della propria località, selezionare il numero di un modem a chiamata telefonica, quindi fare clic su **Next**.

   Il sistema si connetterà a un server Network Associates.

   - Se sul server non vi sono nuovi aggiornamenti dei file .DAT o del software, la finestra di dialogo Online Activity Status (vedere la Figura A-5 a pagina 270) indicherà che i file di cui si dispone sono aggiornati. Fare clic su **Finish** per disconnettersi dal server.
   - Se sul server vi sono nuovi file .DAT, la finestra di dialogo Online Activity Status (vedere la Figura A-6 a pagina 271) indicherà che è in corso lo scaricamento automatico sul sistema del file .EXE contenente i file .DAT.

     Al termine dello scaricamento, fare clic su **Next**. Verrà visualizzata la finestra di dialogo Online Activity Complete (vedere la Figura A-7 a pagina 271).

4. Fare clic su **Finish** per installare i nuovi aggiornamenti dei file .DAT.

Se sul server è presente una versione del *prodotto* più recente di quella di cui si dispone, verrà visualizzata la finestra di dialogo Newer Component Found (vedere la Figura A-8 a pagina 272).

1. Per scaricare solo gli ultimi file .DAT invece dell'intero prodotto, selezionare **DAT files only**, quindi fare clic su **Next**. Per scaricare una nuova versione del prodotto, fare clic su **Next**.
2. Nella finestra di dialogo Online Activity Status (vedere la Figura A-6 a pagina 271) verrà indicato lo stato dello scaricamento. Al termine dello scaricamento, fare clic su **Next** per continuare.

La finestra di dialogo Online Activity Complete (Figura A-11) confermerà che lo scaricamento è terminato.

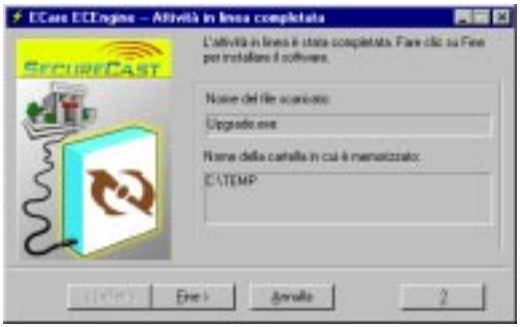

Figura A-11. Finestra di dialogo Online Activity Complete

3. Prendere nota del nome e dell'ubicazione del file scaricato, quindi fare clic su **Finish** per installare il software.

Registrazione del software di valutazione

Se si sta utilizzando una versione di valutazione di 30 giorni del software Network Associates, verrà visualizzata la finestra di dialogo Acquisto (Figura A-12). Tale finestra di dialogo viene visualizzata anche scegliendo **Acquisto** dal menu **File** del prodotto software Network Associates.

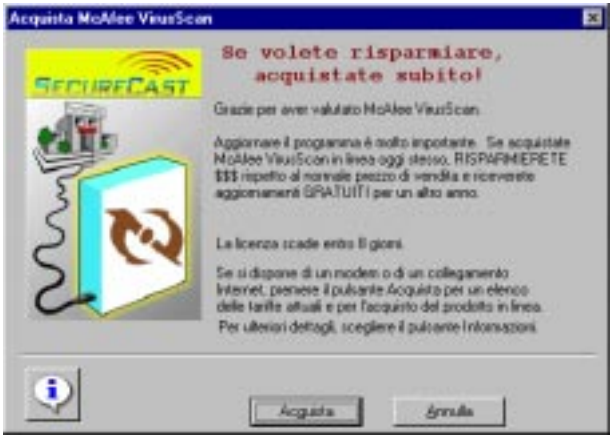

Figura A-12. Finestra di dialogo Acquisto

Se si continua a utilizzare copie di valutazione del software Network Associates dopo la scadenza delle relative licenze da 30 giorni, compariranno sempre più di frequente avvisi di registrazione del software. Network Associates consiglia di procedere nel seguente modo per essere certi di utilizzare le ultime versioni disponibili dei file di dati e del prodotto:

1. Nella finestra di dialogo Acquisto (Figura A-12 a pagina 275) fare clic su **Acquisto** per avviare la registrazione elettronica della propria copia di valutazione del software antivirus.

   Verrà visualizzata la finestra di dialogo Internet Access (vedere la Figura A-2 a pagina 268).

2. Se si ha l'accesso diretto a Internet, selezionare **Yes**, quindi fare clic su **Next**. Se non si ha l'accesso diretto a Internet, selezionare **No**, quindi fare clic su **Next**.

   Verrà visualizzata la finestra di dialogo Server (vedere la Figura A-4 a pagina 269). Se si è selezionato **Yes**, la casella del numero telefonico da chiamare non sarà disponibile; se invece si è selezionato **No**, tale casella sarà accessibile.

3. Se si ha l'accesso diretto a Internet, verificare l'identificativo del proprio paese e quello della propria località, quindi fare clic su **Next**. Se non si ha l'accesso diretto a Internet, verificare l'identificativo del proprio paese e quello della propria località, selezionare il numero di un modem a chiamata telefonica, quindi fare clic su **Next**.

   Il sistema si connetterà a un server Network Associates.

   - Se sul server non vi sono nuovi aggiornamenti dei file .DAT o del software, la finestra di dialogo Online Activity Status (vedere la Figura A-5 a pagina 270) indicherà che i file di cui si dispone sono aggiornati. Fare clic su **Finish** per disconnettersi dal server.
   - Se sul server vi sono nuovi file .DAT, la finestra di dialogo Online Activity Status (vedere la Figura A-6 a pagina 271) indicherà che è in corso lo scaricamento automatico sul sistema del file .EXE contenente i file .DAT.

     Al termine dello scaricamento, fare clic su **Next**. Verrà visualizzata la finestra di dialogo Online Activity Complete (vedere la Figura A-7 a pagina 271).

4. Fare clic su **Finish** per installare i nuovi aggiornamenti dei file .DAT.

Se sul server è presente una versione del prodotto più recente di quella di cui si dispone, verrà visualizzata la finestra di dialogo Newer Component Found (vedere la Figura A-8 a pagina 272). Per scaricare solo gli ultimi file .DAT invece dell'intero prodotto, selezionare **DAT files only**, quindi fare clic su **Next**.

Per scaricare una nuova versione del prodotto, procedere come segue:

1. Fare clic su **Next**.

   Se non si ha più diritto a ricevere gli aggiornamenti gratuiti del software, verrà visualizzata una seconda finestra di dialogo Newer Component Found (Figura A-13).

Figura A-13. Seconda finestra di dialogo Newer Component Found

> **NOTA:** La dimensione dei file e le tariffe vengono generate dinamicamente. I dati che compaiono durante lo scaricamento, pertanto, potrebbero variare rispetto a quelli della Figura A-13.

2. Fare clic su **Next>** per proseguire con lo scaricamento.

Verrà visualizzata la finestra di dialogo Enter Credit Card Information (Figura A-14).

Figura A-14. Finestra di dialogo Enter Credit Card Information

3. Immettere l'indirizzo di riferimento, il numero di conto e la data di scadenza della propria carta di credito. Fare clic su **Next>** per continuare.

NOTA: I dati relativi alla propria carta di credito vengono trasmessi in modo sicuro e riservato mediante una transazione protetta.

Verrà visualizzata la finestra di dialogo Online Purchase Authorization (Figura A-15).

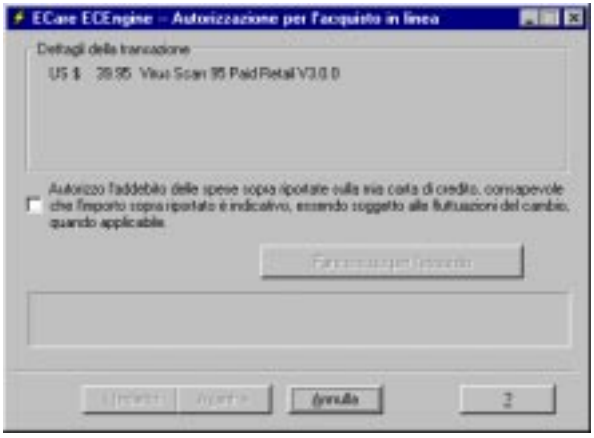

Figura A-15. Finestra di dialogo Online Purchase Authorization

4. Selezionare la casella di controllo per autorizzare l'addebito della transazione sulla propria carta di credito, quindi fare clic su Click Here to Buy per avviare lo scaricamento.

   NOTA: Network Associates effettuerà l'addebito sulla carta di credito solo se lo scaricamento viene completato correttamente.

   Nella finestra di dialogo Online Activity Status (vedere la Figura A-6 a pagina 271) verrà indicato lo stato dello scaricamento.

5. Al termine dello scaricamento, prendere nota del numero di transazione risultante dal proprio acquisto, quindi fare clic su **Next>** per continuare.

   La finestra di dialogo Online Activity Complete (vedere la Figura A-9 a pagina 272) confermerà il completamento della transazione.

6. Prendere nota del nome e dell'ubicazione del file scaricato, quindi fare clic su **Finish** per installare il software.

Canale Enterprise SecureCast

I responsabili della gestione di una rete aziendale possono scaricare il software client BackWeb dal sito per aziende di Network Associates (http://www.nai.com) e installarlo su un server di rete. Enterprise SecureCast è destinato ai soli amministratori e non ai normali utenti finali di un'azienda.

NOTA: Quando arriva il primo InfoPak, fare doppio clic su di esso per aprirlo, quindi completare la registrazione al canale mediante le finestre di dialogo Customer Registration Information. Quando si ricevono successivi InfoPak da Enterprise SecureCast, Network Associates consiglia di distribuirli ai singoli desktop secondo le necessità, in modo da preservare la larghezza di banda della rete.

Vantaggi

- Facilità d'uso

  Non è più necessario ricercare e scaricare gli aggiornamenti dai servizi di distribuzione Network Associates. Gli aggiornamenti, infatti, arriveranno automaticamente in formato compresso, pronti per essere testati e installati in loco.

- Protezione costante e continuata nel tempo

  Network Associates garantisce una protezione costante inviando, a scadenze regolari, gli aggiornamenti dei file .DAT e del prodotto direttamente sul desktop del computer. Il trasferimento inizia non appena gli aggiornamenti vengono resi disponibili sul server SecureCast.

- Avvisi di virus

  Si riceveranno avvisi della presenza di virus pericolosi, con suggerimenti sul modo migliore di evitare l'infezione. Inoltre, si risparmierà tempo prezioso grazie ad avvisi in grado di distinguere tra falsi allarmi e vere e proprie minacce per il sistema.

- Aggiornamenti per più piattaforme

  Abbonandosi a Enterprise SecureCast si riceveranno gli aggiornamenti ai prodotti per più piattaforme. Si potranno ricevere infatti, direttamente sul proprio desktop, gli aggiornamenti dei file di dati e dei prodotti Network Associates per Windows 95, Windows 98, Windows NT, Windows 3.*x*, DOS, OS/2 e Mac OS.

- Versioni in più lingue

  Abbonandosi si riceveranno gli aggiornamenti dei file .DAT non solo per più piattaforme, ma anche nella lingua desiderata.

- Supporto a HTTP nel software client

  Enterprise SecureCast supporta il protocollo HTTP (Hypertext Transfer Protocol) per la trasmissione dei file ai server SecureCast attraverso il firewall dell'utente.

  ❑ **NOTA:** Considerazioni sui firewall: se è installato un firewall, utilizzare il protocollo HTTP. In caso contrario, utilizzare il protocollo UDP. Se si sta utilizzando il software Firewall-1™ Check Point, si noterà che BackWeb è un tipo di trasmissione predefinito.

Installazione di Enterprise SecureCast

Per avere il client BackWeb gli utenti devono disporre di un numero di concessione (numero seriale della licenza del prodotto) per iscriversi a Enterprise SecureCast.

- Se non si dispone di tale numero, contattare il proprio responsabile degli acquisti, il proprio rivenditore o l'Assistenza clienti Network Associates al numero (408) 988-3832.

- Se si è già un utente Network Associates registrato e non si conosce il proprio numero di concessione, inoltrare il relativo modulo di richiesta in linea:

  http://www.nai.com/products/securecast/esc/grantreq.asp

OPPURE

Inviare un messaggio di posta elettronica all'indirizzo appropriato:

ESCRegistration@nai.com (Stati Uniti)

ESC-Registration-Europe@nai.com (Europa)

ESC-Registration-Asia@nai.com (Asia)

Per installare Enterprise SecureCast, procedere nel seguente modo:

1. Scaricare il client BackWeb Enterprise SecureCast (circa 2MB). Tale software client è configurato specificamente per operare in ambiente aziendale, con supporto alla trasmissione di file tramite HTTP.
2. Installare il software client Enterprise SecureCast.

   Si riceverà un InfoPak introduttivo a conferma che la connessione al canale Enterprise SecureCast funziona.
3. Iniziare la registrazione al canale immettendo i dati relativi alla propria azienda nelle finestre di dialogo Customer Registration Information (che compariranno nel primo o nel secondo InfoPak che si riceve).

   Dopo aver fatto clic su **Next** nell'ultima finestra di registrazione, nella finestra Online Activity Status verrà indicato lo stato della trasmissione dati.
4. Al termine, prendere nota del proprio numero di registrazione e fare clic su **Finish**.

   Il proprio browser Web si avvierà visualizzando un modulo di abbonamento al prodotto.
5. Selezionare il software, le piattaforme e la lingua in cui si desidera ricevere gli aggiornamenti.
6. Inoltrare il modulo di abbonamento al prodotto.

Uso di Enterprise SecureCast

Si è ora pronti a ricevere periodici avvisi di virus, nonché gli aggiornamenti del prodotto. Nel giro di qualche giorno si riceveranno ulteriori InfoPak. Un InfoPak può contenere, tra l'altro, suoni, animazioni e pagine Web. Quando si riceve un nuovo InfoPak da Enterprise SecureCast, compare automaticamente come oggetto animato sul desktop finché non viene aperto. Per aprire un InfoPak, fare doppio clic su di esso.

Una volta scaricati sul sistema, gli aggiornamenti devono essere distribuiti alle varie stazioni di lavoro sulla rete. Gli InfoPak ricevuti fungono anche da pacchetti di distribuzione per McAfee Enterprise (Me!). Con Me! è possibile gestire gli aggiornamenti software, l'inventario, la distribuzione, la contabilizzazione dell'utilizzo e gli avvisi centralizzati. Per ulteriori informazioni su Me!, contattare il rappresentante Network Associates.

Risoluzione dei problemi di Enterprise SecureCast

Problemi di registrazione

Se si tenta di registrarsi in un'ora di intenso traffico sul Web, possono verificarsi dei ritardi quando il server tenta di elaborare la richiesta di registrazione. Se si riceve il messaggio di errore "1105 Error" o "Database Error: Unable to connect to the data source", vi è un problema con il database sul server SecureCast. Provare a inoltrare di nuovo il modulo o ritentare la registrazione in un altro momento. Se si continua ad avere problemi a registrarsi al canale Enterprise SecureCast, contattare il centro di supporto per gli scaricamenti di Network Associates (dal lunedì al venerdì, dalle 8.00 alle 20.00 - ora degli Stati Uniti centrali) al numero (972) 278-6100 per avere assistenza.

Problemi con i firewall

La maggior parte dei firewall che consentono l'esplorazione del Web permette anche di ricevere gli InfoPak SecureCast. Alcuni firewall però possono causare problemi di connessione al server SecureCast. Quando si completa il modulo di registrazione e si scarica il software, inizialmente si scarica un client SecureCast basato su BackWeb versione 1.2. Poiché la versione 1.2 non supporta determinati protocolli di comunicazione, quando la si utilizza, potrebbe comparire un errore di "mancata connessione alla rete". Per ovviare a questo problema, scaricare l'ultima versione del client SecureCast, la quale è stata sviluppata con BackWeb versione 3.0.

NOTA: È necessario sovrascrivere il client che utilizza la versione 1.2 di BackWeb con il software client che utilizza la versione 3.0 di BackWeb. *Non* disinstallare prima la versione più vecchia. In questo modo il nuovo client SecureCast conserverà le stesse preferenze per il canale.

Per installare e configurare il nuovo software client SecureCast, procedere nel seguente modo:

1. Installare BackWeb versione 3.0 su BackWeb versione 1.2.
2. Avviare il client SecureCast.
3. Per configurare il metodo di comunicazione del client SecureCast in base alle proprie informazioni di rete, scegliere **Opzioni globali** dal menu **Preferenze**.
4. Cambiare l'impostazione della modalità di accesso di BackWeb attraverso il server proxy da **Polite Agent** a **HTTP**. Quindi, fare clic su **Installazione proxy HTTP** e immettere le informazioni sulla rete richieste.

   NOTA: Le informazioni sul server proxy sono specifiche della rete. Per altri quesiti, contattare il proprio amministratore del sistema.

Annullamento dell'abbonamento a Enterprise SecureCast

Per annullare l'abbonamento a questo servizio in qualunque momento, procedere nel seguente modo:

1. Fare doppio clic sull'icona del client SecureCast nella barra delle applicazioni di Windows.
2. Fare clic con il pulsante destro del mouse sul pulsante del canale **Azienda**.

   Comparirà un menu di scelta rapida.
3. Fare clic su **Annulla abbonamento**, quindi fare clic su **OK** per confermare.

Risorse di supporto

SecureCast

Per ulteriori dubbi o quesiti su SecureCast, fare riferimento alla pagina SecureCast FAQ:

http://www.nai.com/products/securecast/esc/enterprise_faq.asp

BackWeb

- Per una descrizione generale di BackWeb e degli InfoPak, fare riferimento alla pagina BackWeb Overview:

  http://www.nai.com/products/securecast/securedetail.asp

- Per una guida completa su BackWeb (inclusi ulteriori suggerimenti per la risoluzione dei problemi), fare riferimento al BackWeb User's Manual:

  http://www.backweb.com/doc/version20/Client95/

OPPURE

- scaricare il relativo file .PDF:

  http://www.backweb.com/doc/version20/bwuser.pdf

- Per le soluzioni a seri problemi di funzionamento di BackWeb, contattare il centro di supporto per gli scaricamenti di Network Associates (dal lunedì al venerdì, dalle 8.00 alle 20.00 - ora degli Stati Uniti centrali) al numero (972) 278-6100.

Network Associates Servizi di assistenza

B

La scelta dell'antivirus e del software di protezione di Network Associates assicura il funzionamento uniforme ed efficace della tecnologia informativa. Il piano di assistenza di Network Associates consente di estendere la protezione ottenuta dal software fornendo agli utenti le informazioni tecniche necessarie per l'installazione, il monitoraggio, la manutenzione e l'aggiornamento del sistema con la tecnologia d'avanguardia di Network Associates. Un piano di assistenza personalizzato per le particolari necessità dell'utente consentirà di ottenere un sistema o una rete che opera in modo affidabile nell'ambiente di elaborazione per mesi o per anni.

I piani di assistenza di Network Associates si dividono in due sezioni principali. Le aziende possono scegliere fra i tre livelli di assistenza del programma PrimeSupport di Network Associates. I proprietari di prodotti Network Associates acquistati presso punti di vendita al dettaglio possono scegliere dal programma Personal Support un piano adeguato alle proprie necessità.

Opzioni PrimeSupport per le aziende

Il programma PrimeSupport di Network Associates dispone delle opzioni Basic, Extended e Anytime. Ciascuna opzione dispone di una gamma di funzioni che forniscono assistenza tempestiva ed economica adeguata alle necessità dell'utente.

PrimeSupport Basic

L'opzione Basic di PrimeSupport fornisce l'accesso tramite telefono all'assistenza di base per i prodotti fornita da personale esperto del supporto tecnico di Network Associates. Se il prodotto Network Associates è stato acquistato con una licenza di abbonamento, l'opzione Basic di PrimeSupport viene fornita come parte del pacchetto per la durata di due anni dalla data di acquisto. Se il prodotto Network Associates è stato acquistato con una licenza senza scadenza, è possibile rinnovare il piano PrimeSupport Basic con una spesa annuale.

PrimeSupport Basic include i seguenti servizi:

- Assistenza tecnica telefonica disponibile dalle 8.00 alle 20.00 (ora degli Stati Uniti centrali), dal lunedì al venerdì.

- Accesso illimitato alle informazioni di supporto di Network Associates, disponibile 24 ore su 24 tramite il sito Web di Network Associates.
- Aggiornamenti ai file di dati e ai prodotti tramite il sito Web di Network Associates.

PrimeSupport Extended

PrimeSupport Extended fornisce un'assistenza preventiva e personalizzata da parte di un rappresentante del supporto tecnico. Si entrerà in contatto con un professionista con una conoscenza approfondita del prodotto Network Associates che contatterà l'utente con una frequenza prestabilita per fornirgli assistenza nell'utilizzo e nella manutenzione dei prodotti Network Associates. Attraverso questo sistema di contatto regolare, il tecnico assegnato a PrimeSupport Extended fornisce la possibilità di prevenire i problemi prima ancora che questi si verifichino. Se tuttavia si verificasse un'emergenza, PrimeSupport Extended fornisce un tempo di risposta previsto che indica all'utente quanto dovrà attendere per ottenere un aiuto. È possibile acquistare PrimeSupport Extended su base annuale quando si acquista un prodotto Network Associates sia con licenza di abbonamento che con licenza senza scadenza.

PrimeSupport Extended include i seguenti servizi:

- Contatto con un rappresentante del supporto tecnico.
- Contatti di assistenza preventiva tramite telefono o posta elettronica da parte del tecnico assegnato ad intervalli prestabiliti.
- Tempi di risposta previsti: il rappresentante del supporto tecnico risponderà entro un'ora alle chiamate effettuate tramite cerca persone, entro quattro ore a chiamate effettuate tramite casella vocale e entro 12 ore a chiamate effettuate tramite posta elettronica.
- Assistenza tecnica telefonica disponibile dalle 7.00 alle 19.00 (ora degli Stati Uniti centrali), dal lunedì al venerdì.
- Accesso illimitato alle informazioni di supporto di Network Associates, disponibile 24 ore su 24 tramite il sito Web di Network Associates.
- Aggiornamenti ai file di dati e ai prodotti tramite il sito Web di Network Associates.
- Possibilità di designare un massimo di cinque persone all'interno dell'azienda per il contatto con i clienti.

PrimeSupport Anytime

PrimeSupport Anytime fornisce l'assistenza preventiva personalizzata 24 ore su 24 per i prodotti Network Associates utilizzati nei sistemi informativi aziendali a tutti i livelli. PrimeSupport Anytime fornisce gli stessi servizi di PrimeSupport Extended 24 ore su 24, sette giorni su sette con tempi di risposta previsti più brevi. È possibile acquistare PrimeSupport Anytime su base annuale quando si acquista un prodotto Network Associates sia con licenza di abbonamento che con licenza senza scadenza.

PrimeSupport Anytime include i seguenti servizi:

- Contatto con un rappresentante del supporto tecnico.
- Contatti di assistenza preventiva tramite telefono o posta elettronica da parte del tecnico assegnato ad intervalli prestabiliti.
- Tempi di risposta previsti: il rappresentante del supporto tecnico risponderà entro mezz'ora alle chiamate effettuate tramite cerca persone, entro un'ora a chiamate effettuate tramite casella vocale ed entro quattro ore a chiamate effettuate tramite posta elettronica.
- Assistenza tecnica telefonica disponibile 24 ore su 24, sette giorni su sette.
- Accesso illimitato alle informazioni di supporto di Network Associates, disponibile 24 ore su 24 tramite il sito Web di Network Associates.
- Aggiornamenti ai file di dati e ai prodotti tramite il sito Web di Network Associates.
- Possibilità di designare un massimo di dieci persone all'interno dell'azienda per il contatto con i clienti.

Tabella B-1. Panoramica di PrimeSupport

Caratteristiche	Basic	Extended	Anytime
Supporto tecnico telefonico	Dal lunedì al venerdì, dalle 8.00 alle 20.00	Dal lunedì al venerdì, dalle 7.00 alle 19.00	24 ore su 24, sette giorni su sette
Supporto tecnico tramite sito Web	Sì	Sì	Sì
Aggiornamenti software	Sì	Sì	Sì
Tecnico di supporto assegnato	—	Sì	Sì

Tabella B-1. Panoramica di PrimeSupport

Caratteristiche	Basic	Extended	Anytime
Contatto di assistenza preventiva	—	Sì	Sì
Contatti cliente designati	—	5	10
Tempo di risposta previsto	—	Cerca persone: 1 ora Casella vocale: 4 ore Posta elettronica: 12 ore	Cerca persone: 30 minuti Casella vocale: 1 ora Posta elettronica: 4 ore

Per ordinare PrimeSupport

Per ordinare PrimeSupport Basic, PrimeSupport Extended o PrimeSupport Anytime per i prodotti Network Associates:

- Contattare il rappresentante autorizzato, oppure
- Contattare i servizi di assistenza Network Associates al numero 1-800-988-5737 o al numero 1-650-473-2000 dalle 6.00 alle 17.00 (orario del Pacifico), dal lunedì al venerdì.

NOTA: Il programma PrimeSupport descritto in questo manuale è disponibile solo in America del Nord. Per informazioni relative alle opzioni del programma PrimeSupport disponibili fuori dall'America del Nord contattare l'ufficio vendite della propria zona. Le informazioni relative ai contatti sono riportate sulla copertina del manuale.

Servizi di assistenza per privati

Tutti coloro che hanno acquistato prodotti Network Associates presso punti vendita al dettaglio o dal sito Web di Network Associates hanno diritto ad alcuni servizi di assistenza compresi nell'acquisto del prodotto. Il livello di assistenza previsto dipende dal prodotto acquistato. Esempi dei servizi previsti sono:

- Aggiornamenti gratuiti ai file di dati (.DAT) per la durata del prodotto tramite il sito Web di Network Associates, la funzione di Aggiornamento automatico del prodotto o il servizio SecureCast (per informazioni, vedere l'Appendice A, "Uso di SecureCast per l'aggiornamento del software".). È possibile aggiornare i file di dati anche utilizzando il proprio browser Web per visitare il sito che si trova al seguente indirizzo:

  http://www.nai.com/download/updates/updates.asp

- Aggiornamenti gratuiti al programma (file eseguibile) per un anno tramite il sito Web di Network Associates, la funzione di Aggiornamento automatico del prodotto o il servizio SecureCast (per informazioni, vedere l'Appendice A, "Uso di SecureCast per l'aggiornamento del software".). Se è stata acquistata una versione "Deluxe" di un prodotto Network Associates, sono previsti aggiornamenti gratuiti del programma per due anni. È possibile aggiornare il software anche utilizzando il proprio browser Web per visitare il sito che si trova al seguente indirizzo:

  http://www.nai.com/download/upgrades/upgrades.asp

- Accesso gratuito 24 ore su 24, sette giorni su sette, all'assistenza in linea o elettronica tramite il sistema voce e fax di Network Associates, il sito Web di Network Associates e attraverso altri servizi elettronici quali America Online e CompuServe.

  Per contattare i servizi elettronici di Network Associates, selezionare una delle seguenti opzioni:

  – Sistema fax e voce automatico: (408) 988-3034
  – Sito Web di Network Associates: http://support.nai.com
  – CompuServe GO NAI
  – America Online: parola chiave MCAFEE

- 90 giorni di supporto tecnico gratuito da parte dei rappresentati del supporto disponibile nelle normali ore di ufficio, dalle 8.00 alle 20.00 (ora degli Stati Uniti centrali), dal lunedì al venerdì.

Al termine del periodo di assistenza gratuita, è possibile usufruire di una gamma di opzioni di assistenza personalizzata specifiche per le singole esigenze. Contattare l'Assistenza clienti di Network Associates al numero (972) 278-6100 per ulteriori informazioni sulle opzioni disponibili, oppure visitare il sito web di Network Associates all'indirizzo:

http://www.nai.com/services/support/support.asp

Consulenza e addestramento di Network Associates

Network Associates fornisce consulenza di esperti e addestramento completo per aumentare ai massimi livelli la protezione e le prestazioni della rete attraverso il programma Total Service Solutions.

Servizi di consulenza professionale

I servizi di consulenza professionale di Network Associates forniscono un'assistenza per tutte le fasi della crescita della rete, a partire dalla pianificazione e la progettazione, durante l'implementazione e per la gestione. I consulenti di Network Associates rappresentano una risorsa supplementare esperta con una linea di azione indipendente nella risoluzione dei problemi. Sarà possibile ottenere assistenza per l'integrazione dei prodotti Network Associates nel proprio ambiente, insieme all'assistenza per la risoluzione dei problemi o l'individuazione delle linee base per le prestazioni della rete. Inoltre, i consulenti di Network Associates sviluppano e forniscono ai clienti soluzioni per il raggiungimento degli scopi prefissati nei progetti, a partire dalla durata e dalle implementazioni su larga scala fino alla risoluzione rapida dei problemi.

Servizi di addestramento completo

I servizi di addestramento completo di Network Associates forniscono addestramento basilare e avanzato per i professionisti che operano sulle reti attraverso istruzioni pratiche che possono essere utilizzate immediatamente. Il programma dei servizi di addestramento completo verte sui malfunzionamenti della rete, sulla gestione delle prestazioni e sulla risoluzione dei problemi a tutti i livelli. Network Associates offre inoltre un addestramento modulare sui prodotti che consente di conoscere le caratteristiche e le funzionalità del proprio software.

È possibile iscriversi ai servizi di addestramento completo in qualsiasi periodo dell'anno presso i centri di addestramento di Network Associates oppure è possibile seguire dei corsi personalizzati a domicilio. Tutti i corsi garantiscono un apprendimento in varie fasi che consente di raggiungere i massimi livelli di conoscenza. Network Associates è un membro fondatore del consorzio CNX (Certified Network Expert).

Per ulteriori informazioni su questi programmi, contattare il rivenditore autorizzato oppure contattare Total Service Solutions al numero 1-800-395-3151.

Comprensione del formato di file .VSC

C

Salvataggio delle impostazioni di VirusScan

Una volta scelte le opzioni di configurazione di VirusScan, il programma salva le impostazioni nel file DEFAULT.VSC, nella directory di programma VirusScan. DEFAULT.VSC è un file di testo di configurazione che contiene le impostazioni di VirusScan. Il file è formattato in modo simile ai file .INI di Windows e aprendolo con un editor di testi, ad esempio Blocco note di Windows, è possibile variare direttamente le opzioni contenute. Se le impostazioni di VirusScan sono protette da password, il programma codifica il file DEFAULT.VSC per evitarne la manomissione. Per poterlo modificare, è necessario rimuovere la protezione.

Ciascuna variabile del file ha un nome seguito dal segno di uguale (=) e da un valore numerico. I valori corrispondono alle impostazioni selezionate durante la configurazione di VirusScan. Nel file DEFAULT.VSC, le variabili sono suddivise in otto gruppi identificati dalle rispettive intestazioni. Le tabelle riportate alle pagine seguenti elencano tutte le variabili, i rispettivi valori predefiniti e i valori impostabili.

❑ **NOTA:** Le variabili booleane possono avere come unico valore 0 o 1. Il valore 0 disabilita l'impostazione di VirusScan, mentre il valore 1 la abilita.

È possibile distribuire copie del file DEFAULT.VSC modificato agli utenti di VirusScan su altri computer, sovrascrivere i relativi file DEFAULT.VSC e copiare le impostazioni di VirusScan in modo che gli altri possano utilizzarle. VirusScan consente inoltre di salvare i file .VSC con il nome desiderato. Se si distribuiscono i file, gli altri utenti possono individuarli e, facendo doppio clic su di essi, avviare VirusScan applicando le opzioni che vi sono contenute.

Network Associates fornisce inoltre ISeamless, uno strumento completo di configurazione e di distribuzione che consente di mantenere il controllo completo sui file di configurazione di VirusScan, compresi DEFAULT.VSH, DEFAULT.VSC, UPGRADE.INI, UPDATE.INI e gli altri file speciali di configurazione creati dall'utente. Per ulteriori informazioni su ISeamless e gli altri strumenti di gestione di Network Associates, contattare il rappresentante di vendita o l'Assistenza clienti Network Associates.

ScanOptions

Variabile	Descrizione
bAutoStart	Tipo: Booleana (0/1) Abilita VirusScan ad avviare automaticamente la scansione all'avvio Valore predefinito: 0
bAutoExit	Tipo: Booleana (0/1) Indica l'uscita automatica da VirusScan al termine della scansione se non sono stati rilevati dei virus Valore predefinito: 0
bAlwaysExit	Tipo: Booleana (0/1) Indica l'uscita automatica da VirusScan al termine della scansione anche se sono stati rilevati dei virus Valore predefinito: 0
bSkipMemoryScan	Tipo: Booleana (0/1) Abilita VirusScan a non eseguire la scansione della memoria Valore predefinito: 0
bSkipBootScan	Tipo: Booleana (0/1) Abilita VirusScan a non eseguire la scansione dei settori di boot Valore predefinito: 0
bSkipSplash	Tipo: Booleana (0/1) Abilita VirusScan a non visualizzare lo schermo introduttivo all'avvio Valore predefinito: 0

DetectionOptions

Variabile	Descrizione
bScanAllFiles	Tipo: Booleana (0/1) Abilita VirusScan ad eseguire la scansione di tutti i tipi di file Valore predefinito: 0
bScanCompressed	Tipo: Booleana (0/1) Abilita VirusScan ad eseguire la scansione dei file compressi Valore predefinito: 1
szProgramExtensions	Tipo: Stringa Specifica quali estensioni di file verranno sottoposte a scansione da VirusScan Valore predefinito: EXE COM DO? XL?
szDefaultProgram Extensions	Tipo: Stringa Specifica il valore predefinito di szProgramExtensions Valore predefinito: EXE COM DO? XL?

AlertOptions

Variabile	Descrizione
bNetworkAlert	Tipo: Booleana (0/1) Abilita VirusScan ad inviare un file di avviso (.ALR) ad un percorso di rete controllato da NetShield per l'avviso centralizzato quando viene rilevato un virus Valore predefinito: 0
bSoundAlert	Tipo: Booleana (0/1) Abilita VirusScan ad emettere un segnale acustico di avviso quando viene rilevato un virus Valore predefinito: 1
szNetworkAlertPath	Tipo: Stringa Specifica il percorso di avviso di rete controllato da NetShield per l'avviso centralizzato. La cartella specificata da questo percorso deve contenere il file di avviso centralizzato CENTALRT.TXT Valore predefinito: Nessuno

ActionOptions

Variabile	Descrizione
bDisplayMessage	Tipo: Booleana (0/1) Abilita VirusScan a visualizzare un messaggio quando rileva un virus Valore predefinito: 0
ScanAction	Tipo: Numero intero (0-5) Indica a VirusScan di eseguire l'azione specificata quando viene rilevato un virus Valori possibili: 0 - Richiedi azione 1 - Sposta automaticamente 2 - Pulisci automaticamente 3 - Elimina automaticamente 4 - Continua Valore predefinito: 0
bButtonClean	Tipo: Booleana (0/1) Abilita VirusScan a visualizzare il pulsante Pulisci se ScanAction=0 Valore predefinito: 1
bButtonDelete	Tipo: Booleana (0/1) Abilita VirusScan a visualizzare il pulsante Elimina se ScanAction=0 Valore predefinito: 1
bButtonExclude	Tipo: Booleana (0/1) Abilita VirusScan a visualizzare il pulsante Escludi se ScanAction=0 Valore predefinito: 1
bButtonMove	Tipo: Booleana (0/1) Abilita VirusScan a visualizzare il pulsante Sposta se ScanAction=0 Valore predefinito: 1
bButtonContinue	Tipo: Booleana (0/1) Abilita VirusScan a visualizzare il pulsante Continua se ScanAction=0 Valore predefinito: 1

Variabile	Descrizione
bButtonStop	Tipo: Booleana (0/1) Abilita VirusScan a visualizzare il pulsante Interrompi se ScanAction=0 Valore predefinito: 1
szMoveToFolder	Tipo: Stringa Indica dove devono essere spostati i file infetti Valore predefinito: \Infetti
szCustomMessage	Tipo: Stringa Indica il messaggio di testo da visualizzare al rilevamento di virus Valore predefinito: Rilevato possibile virus

ReportOptions

Variabile	Descrizione
bLogToFile	Tipo: Booleana (0/1) Abilita VirusScan a registrare su file l'attività di scansione Valore predefinito: 1
bLimitSize	Tipo: Booleana (0/1) Abilita VirusScan a limitare le dimensioni del file di log Valore predefinito: 1
uMaxKilobytes	Tipo: Numero intero (10-999) Specifica le dimensioni massime in kilobyte del file di log Valore predefinito: 10
bLogDetection	Tipo: Booleana (0/1) Abilita VirusScan a registrare il rilevamento dei virus Valore predefinito: 1
bLogClean	Tipo: Booleana (0/1) Abilita VirusScan a registrare la pulizia dei virus Valore predefinito: 1
bLogDelete	Tipo: Booleana (0/1) Abilita VirusScan a registrare le eliminazioni dei file Valore predefinito: 1

Variabile	Descrizione
bLogMove	Tipo: Booleana (0/1) Abilita VirusScan a registrare gli spostamenti dei file Valore predefinito: 1
bLogSettings	Tipo: Booleana (0/1) Abilita VirusScan a registrare le impostazioni di sessione Valore predefinito: 1
bLogSummary	Tipo: Booleana (0/1) Abilita VirusScan a registrare i riepiloghi di sessione Valore predefinito: 1
bLogDateTime	Tipo: Booleana (0/1) Abilita VirusScan a registrare la data e l'ora dell'attività di scansione Valore predefinito: 1
bLogUserName	Tipo: Booleana (0/1) Abilita VirusScan a registrare il nome utente Valore predefinito: 1
szLogFileName	Tipo: Stringa Specifica il percorso per il file di log Valore predefinito: C:\Program Files\Network Associates\McAfee Viruscan\VSCLOG.TXT

ScanItems

Variabile	Descrizione
ScanItem_x, dove x è un indice a base zero	Tipo: Stringa Abilita VirusScan ad eseguire la scansione dell'elemento Valore predefinito: `C:|1 *` * La stringa è suddivisa in campi tramite il carattere pipe (|): Campo 1: percorso dell'elemento da sottoporre a scansione. Campo 2: booleano (1/0) Valori possibili: 1 - Abilita VirusScan ad eseguire la scansione delle sottocartelle dell'elemento 2 - Abilita VirusScan a non eseguire la scansione delle sottocartelle dell'elemento

SecurityOptions

Variabile	Descrizione
szPasswordProtect	Tipo: Stringa Questa variabile non è configurabile dall'utente. Valore predefinito: 0
szPasswordCRC	Tipo: Stringa Questa variabile non è configurabile dall'utente. Valore predefinito: 0
szSerialNumber	Tipo: Stringa Questa variabile non è configurabile dall'utente. Valore predefinito: 0

ExcludedItems

Variabile	Descrizione
NumExcludeItems	Tipo: Numero intero (0-n) Definisce il numero di elementi esclusi dalla scansione Valore predefinito: 1
ExcludedItem_x, dove x è un indice a base zero	Tipo: Stringa Abilita VirusScan ad escludere l'elemento dalla scansione Valore predefinito: `\Recycled|*.*|1|1 *` * La stringa è suddivisa in campi tramite il carattere pipe (|): Campo 1: cartella dell'elemento da escludere. Lasciare vuoto nel caso di file singoli nel sistema. Campo 2: file dell'elemento da escludere. Non immettere nessun valore nel campo se viene esclusa dalla scansione una directory senza un nome file. Campo 3: numero intero (1-3) Valori possibili: 1 - Esclude dalla scansione di file 2 - Esclude dalla scansione del record di boot 3 - Esclude sia dalla scansione del record di boot che dalla scansione di file Campo 4: booleano (1/0) Valori possibili: 1 - Abilita VirusScan ad escludere le sottocartelle dell'elemento escluso 2 - Abilita VirusScan a non escludere le sottocartelle

Comprensione del formato di file .VSH D

Salvataggio delle opzioni di configurazione di VShield

Quando si scelgono le opzioni di configurazione di VShield, VirusScan salva le impostazioni nel file DEFAULT.VSH che si trova nella directory di programma di VirusScan. DEFAULT.VSH è un file di testo di configurazione che riassume le impostazioni di VShield. È formattato in modo simile ai file .INI di Windows e aprendolo con un editor di testi, ad esempio Blocco note di Windows, è possibile variare direttamente le opzioni contenute. Se le impostazioni di VShield sono protette da password, VirusScan codifica il file DEFAULT.VSH per evitarne la manomissione. Per poterlo modificare, è necessario rimuovere la protezione.

Ciascuna variabile del file ha un nome seguito dal segno di uguale (=) e da un valore numerico. I valori corrispondono alle impostazioni selezionate durante la configurazione di VShield. Le variabili sono suddivise in 24 gruppi identificati dalle rispettive intestazioni e inclusi nel file DEFAULT.VSH. La maggior parte delle intestazioni corrisponde a un modulo di VShield. Le tabelle riportate nelle pagine seguenti elencano le opzioni, i rispettivi valori predefiniti e i possibili valori che possono essere impostati dall'utente.

❑ **NOTA:** Le variabili booleane possono avere come unico valore 0 o 1. Il valore 0 disabilita l'impostazione in VShield mentre il valore 1 la abilita.

È possibile distribuire copie del file DEFAULT.VSH modificato agli utenti di VShield su altri computer, sovrascrivere i relativi file DEFAULT.VSH e copiare le impostazioni di VShield in modo che gli altri possano utilizzarle. Network Associates fornisce inoltre ISeamless, uno strumento completo di configurazione e di distribuzione che consente di mantenere il controllo completo sui file di configurazione di VirusScan, compresi DEFAULT.VSH, DEFAULT.VSC, UPGRADE.INI, UPDATE.INI e gli altri file speciali di configurazione creati dall'utente.

Per ulteriori informazioni su ISeamless e gli altri strumenti di gestione di Network Associates, contattare il rappresentante di vendita o l'Assistenza clienti Network Associates.

Modulo Scansione sistema

General

Variabile	Descrizione
bEnabled	Tipo: Booleana (1/0) Abilita Scansione sistema Valore predefinito: 1
bCanBeDisabled	Tipo: Booleana (1/0) Definisce se VShield può essere disattivato Valore predefinito: 1
bShowTaskbarIcon	Tipo: Booleana (1/0) Definisce se l'icona della barra delle applicazioni di VShield viene visualizzata Valore predefinito: 1

DetectionOptions

Variabile	Descrizione
bProgFileHeurisitcs	Tipo: Booleana (1/0) Abilita VShield ad eseguire la scansione euristica dei file di programma Valore predefinito: 0
bMacroHeuristics	Tipo: Booleana (1/0) Abilita VShield ad eseguire la scansione euristica delle macro Valore predefinito: 0
bDetectTrojans	Tipo: Booleana (1/0) Abilita VShield ad eseguire la scansione per la ricerca di virus Trojan Valore predefinito: 1
bDetectJoke	Tipo: Booleana (1/0) Abilita VShield ad eseguire la scansione per la ricerca di virus Joke Valore predefinito: 1
bDetectCorrupted	Tipo: Booleana (1/0) Abilita VShield ad eseguire la scansione per la ricerca di file danneggiati Valore predefinito: 0

Variabile	Descrizione
bDetectMaybe	Tipo: Booleana (1/0) Abilita VShield ad eseguire la scansione per la ricerca di varianti di virus conosciuti Valore predefinito: 1
bRemoveAllMacros	Tipo: Booleana (1/0) Abilita VShield ad eliminare tutte le macro dai file infetti Valore predefinito: 0
bScanOnExecute	Tipo: Booleana (1/0) Abilita VShield ad eseguire la scansione quando i file vengono eseguiti Valore predefinito: 1
bScanOnOpen	Tipo: Booleana (1/0) Abilita VShield ad eseguire la scansione quando i file vengono aperti Valore predefinito: 1
bScanOnCreate	Tipo: Booleana (1/0) Abilita VShield ad eseguire la scansione quando i file vengono creati Valore predefinito: 1
bScanOnRename	Tipo: Booleana (1/0) Abilita VShield ad eseguire la scansione quando i file vengono rinominati Valore predefinito: 1
bScanOnShutdown	Tipo: Booleana (1/0) Abilita VShield ad eseguire la scansione del record di boot dell'unità A allo spegnimento del sistema Valore predefinito: 1
bScanOnBootAccess	Tipo: Booleana (1/0) Abilita VShield ad eseguire la scansione del record di boot di un dischetto appena inserito nell'unità floppy prima di consentirvi l'accesso. Valore predefinito: 1
bScanAllFiles	Tipo: Booleana (1/0) Abilita VShield ad eseguire la scansione di tutti i file, indipendentemente dall'estensione. Valore predefinito: 0

Variabile	Descrizione
bScanCompressed	Tipo: Booleana (1/0) Abilita il programma ad eseguire la scansione dei file compressi Valore predefinito: 1
szProgramExtensions	Tipo: Stringa Definisce le estensioni dei file da scandire. Valore predefinito: EXE COM DO? XL? MD?, SYS BIN RTF OBD (il carattere ? è un carattere jolly)
szDefaultProgram Extensions	Tipo: Stringa Definisce le estensioni da utilizzare come estensioni di programma predefinite durante la configurazione di scansione Valore predefinito: EXE COM DO? XL? MD?, SYS BIN RTF OBD (il carattere ? è un carattere jolly)

AlertOptions

Variabile	Descrizione
bDMIAlert	Tipo: Booleana (1/0) Abilita gli avvisi DMI (Desktop Management Interface) Valore predefinito: 0
bSoundAlert	Tipo: Booleana (1/0) Abilita il programma ad emettere un segnale acustico di avviso quando viene rilevato un virus Valore predefinito: 1
bNetworkAlert	Tipo: Booleana (1/0) Abilita l'Avviso centralizzato Valore predefinito: 0
szNetworkAlertPath	Tipo: Stringa Specifica la cartella degli avvisi centralizzati su un server Valore predefinito: Nessuno

ActionOptions

Variabile	Descrizione
bDisplayMessage	Tipo: Booleana (1/0) Definisce se visualizzare il messaggio personalizzato nella finestra di dialogo Richiedi azione al rilevamento di un virus Valore predefinito: 0
uVshieldAction	Tipo: Numero intero (1-5) Abilita VShield ad eseguire l'azione specificata quando viene rilevato un virus Valori possibili: 1 - Richiedi azione 2 - Sposta automaticamente i file infetti 3 - Pulisci file infetti automaticamente (L'accesso è impedito se i file non possono essere puliti) 4 - Elimina file infetti automaticamente 5 - Nega l'accesso ai file infetti e continua. Valore predefinito: 1
bButtonClean	Tipo: Booleana (1/0) Abilita VShield a fornire all'utente l'opzione di pulire il file se Richiedi azione è selezionata e viene rilevato un virus Valore predefinito: 1
bButtonDelete	Tipo: Booleana (1/0) Abilita VShield a fornire all'utente l'opzione di eliminare il file se Richiedi azione è selezionata e viene rilevato un virus Valore predefinito: 1
bButtonExclude	Tipo: Booleana (1/0) Abilita VShield a fornire all'utente l'opzione di escludere il file se Richiedi azione è selezionata e viene rilevato un virus Valore predefinito: 1
bButtonContinue	Tipo: Booleana (1/0) Abilita VShield a fornire all'utente l'opzione di continuare l'evento intercettato se Richiedi azione è selezionata e viene rilevato un virus Valore predefinito: 0

Variabile	Descrizione
bButtonStop	Tipo: Booleana (1/0) Abilita VShield a fornire all'utente l'opzione di impedire l'accesso al file infetto se Richiedi azione è selezionata e viene rilevato un virus Valore predefinito: 1
szMoveToFolder	Tipo: Stringa Definisce la cartella in cui spostare i file infetti Valore predefinito: \Infetti
szCustomMessage	Tipo: Stringa Definisce il messaggio personalizzato da visualizzare al rilevamento di un virus se l'azione è impostata su Richiedi azione Valore predefinito: Nessuno

ReportOptions

Variabile	Descrizione
bLogToFile	Tipo: Booleana (1/0) Definisce se i risultati devono essere registrati nel file di log Valore predefinito: 1
bLimitSize	Tipo: Booleana (1/0) Definisce se le dimensioni del file devono essere limitate Valore predefinito: 1
uMaxKilobytes	Tipo: Numero intero (10-999) Definisce le dimensioni massime in kilobyte del file di log Valore predefinito: 100
bLogDetection	Tipo: Booleana (1/0) Abilita VShield a registrare i nomi dei virus rilevati Valore predefinito: 1
bLogClean	Tipo: Booleana (1/0) Definisce se i risultati della pulizia devono essere registrati Valore predefinito: 1

Variabile	Descrizione
bLogDelete	Tipo: Booleana (1/0) Definisce se le operazioni di eliminazione dei file infetti devono essere registrate Valore predefinito: 1
bLogMove	Tipo: Booleana (1/0) Definisce se le operazioni di spostamento dei file infetti devono essere registrate Valore predefinito: 1
bLogSettings	Tipo: Booleana (1/0) Abilita VShield a scrivere un record delle impostazioni in uso durante la scansione immediatamente precedente allo spegnimento del sistema o allo scaricamento di VShield. Valore predefinito: 1
bLogSummary	Tipo: Booleana (1/0) Abilita VShield a scrivere un riepilogo delle rilevazioni e delle azioni della scansione immediatamente precedente allo spegnimento del sistema o allo scaricamento di VShield. Valore predefinito: 1
bLogDateTime	Tipo: Booleana (1/0) Definisce se la data e l'ora di un evento devono essere registrate Valore predefinito: 1
bLogUserName	Tipo: Booleana (1/0) Definisce se il nome utente deve essere registrato Valore predefinito: 1
szLogFileName	Tipo: Stringa Definisce il nome del file di log Valore predefinito: C:\Program Files\Network Associates\McAfee VirusScan\VSHLog.TXT

ExclusionOptions

Variabile	Descrizione
szExclusionsFileName	Tipo: Stringa Valore predefinito: C:\Program Files\Network Associates\McAfee VirusScan\VSHLog.TXT

ExcludedItems

Variabile	Descrizione
NumExcludedItems	Tipo: Numero intero (0-n) Definisce il numero di elementi esclusi dalla scansione all'accesso Valore predefinito: 1
ExcludedItem_x, dove x è un indice a base zero	Tipo: Stringa Abilita VShield ad escludere l'elemento dalla scansione all'accesso Valore predefinito: \Recycled|*.*|1|1 * * La stringa è suddivisa in campi tramite il carattere pipe (|): Campo 1: cartella dell'elemento da escludere. Lasciare vuoto nel caso di file singoli nel sistema. Campo 2: file dell'elemento da escludere. Lasciare vuoto se si esclude una cartella senza specificare il nome del file. Campo 3: numero intero (1-3) Valori possibili: 1 - Esclude dalla scansione di accesso ai file 2 - Esclude dalla scansione del record di boot 3 - Esclude sia dalla scansione del record di boot che dalla scansione di accesso ai file Campo 4: booleano (1/0) Valori possibili: 1 - Abilita VShield ad escludere le sottocartelle dell'elemento escluso 0 - Abilita VShield a non escludere le sottocartelle

Modulo Scansione posta

EMailGeneralOptions

Variabile	Descrizione
bMailType	Tipo: Booleana (1/0) Definisce il tipo di server di posta, MAPI o cc:Mail. Valore predefinito: 1 (MAPI)
bCanBeDisabled	Tipo: Booleana (1/0) Impedisce la disabilitazione della scansione della posta Valore predefinito: 1
bEnabled	Tipo: Booleana (1/0) Abilita la scansione della posta Valore predefinito: 0
bEnabledDummy=0	Tipo: Booleana (1/0) Seleziona automaticamente Posta Internet sulla pagina delle proprietà di Scansione posta quando è abilitata la Scansione scaricamento Valore predefinito: 0

EMailDetectionOptions

Variabile	Descrizione
bScanAllMails	Tipo: Booleana (1/0) Abilita VShield ad eseguire la scansione di tutta la nuova posta Valore predefinito: 0
bScanInternetMail	Tipo: Booleana (1/0) Abilita VShield ad eseguire la scansione della posta Internet Valore predefinito: 0
bScanAllFiles	Tipo: Booleana (1/0) Abilita VShield ad eseguire la scansione di tutti i file Valore predefinito: 0
bScanCompressed	Tipo: Booleana (1/0) Abilita VShield ad eseguire la scansione dei file compressi Valore predefinito: 1

Variabile	Descrizione
szProgramExtensions	Tipo: Stringa Definisce le estensioni dei file da scandire. Valore predefinito: EXE, COM, DO?, XL?, RTF, BIN, SYS, OBD, VXD, MD?, DLL (il carattere ? è un carattere jolly)
szDefaultProgram Estensioni	Tipo: Stringa Definisce le estensioni da utilizzare come estensioni di programma predefinite durante la configurazione di scansione Valore predefinito: EXE, COM, DO?, XL?, RTF, BIN, SYS, OBD, VXD, MD?, DLL (il carattere ? è un carattere jolly)
uPollInterval	Tipo: Integer (60-999) Definisce l'intervallo, in secondi, per il controllo della nuova posta ricevuta tramite cc:Mail Valore predefinito: 60
bDetectTrojans	Tipo: Booleana (1/0) Abilita VShield ad eseguire la scansione per la ricerca di virus Trojan Valore predefinito: 1
bDetectJoke	Tipo: Booleana (1/0) Abilita VShield ad eseguire la scansione per la ricerca di virus Joke Valore predefinito: 1
bDetectCorrupted	Tipo: Booleana (1/0) Abilita VShield ad eseguire la scansione per la ricerca di file danneggiati Valore predefinito: 0
bDetectMaybe	Tipo: Booleana (1/0) Abilita VShield ad eseguire la scansione per la ricerca di varianti di virus conosciuti Valore predefinito: 1
bProgFileHeuristics	Tipo: Booleana (1/0) Abilita VShield ad eseguire la scansione euristica dei file di programma Valore predefinito: 0
bMacroHeuristics	Tipo: Booleana (1/0) Abilita VShield ad eseguire la scansione euristica delle macro Valore predefinito: 0

EMailActionOptions

Variabile	Descrizione
szMoveFolder	Tipo: Stringa Definisce la cartella in cui devono essere spostati allegati di posta MAPI Valore predefinito: \Infetti
CC_szMoveFolder	Tipo: Stringa Definisce la cartella in cui devono essere spostati allegati di posta cc:Mail Valore predefinito: \Infetti
bDisplayMessage	Tipo: Booleana (1/0) Definisce se visualizzare il messaggio personalizzato nella finestra di dialogo Richiedi azione al rilevamento di un virus Valore predefinito: 0
uScanAction	Tipo: Numero intero (0/3) Abilita VShield ad eseguire l'azione specificata quando viene rilevato un virus Valori possibili: 0 - Richiedi azione. 1 - Sposta automaticamente i file infetti 2 - Elimina file infetti automaticamente 3 - Continua la scansione
bButtonDelete	Tipo: Booleana (1/0) Abilita VShield a fornire all'utente l'opzione di eliminare il file se Richiedi azione è selezionata e viene rilevato un virus Valore predefinito: 1
bButtonExclude	Tipo: Booleana (1/0) Abilita VShield a fornire all'utente l'opzione di escludere il file se Richiedi azione è selezionata e viene rilevato un virus Valore predefinito: 0
bButtonMove	Tipo: Booleana (1/0) Abilita VirusScan a fornire all'utente l'opzione di spostare il file infetto se è selezionata l'opzione Richiedi azione e viene rilevato un virus Valore predefinito: 1

Variabile	Descrizione
bButtonContinue	Tipo: Booleana (1/0) Abilita VShield a fornire all'utente l'opzione di continuare l'evento intercettato se Richiedi azione è selezionata e viene rilevato un virus Valore predefinito: 1
bButtonStop	Tipo: Booleana (1/0) Abilita VShield a fornire all'utente l'opzione di impedire l'accesso al file infetto se Richiedi azione è selezionata e viene rilevato un virus Valore predefinito: 0

EMailAlertOptions

Variabile	Descrizione
bDMIAlert	Tipo: Booleana (1/0) Abilita gli avvisi DMI (Desktop Management Interface) Valore predefinito: 0
bNetworkAlert	Tipo: Booleana (1/0) Abilita l'Avviso centralizzato Valore predefinito: 0
szNetworkAlertPath	Tipo: Stringa Specifica la cartella degli avvisi centralizzati su un server Valore predefinito: Nessuno
szCustomMessage	Tipo: Stringa Definisce il messaggio personalizzato da visualizzare al rilevamento di un virus se l'azione è impostata su Richiedi azione Valore predefinito: McAfee VShield: Rilevato un virus nell'allegato!
bReturnMail	Tipo: Booleana (1/0) Abilita VShield a informare il mittente che è stata ricevuta posta infetta tramite un client MAPI Valore predefinito: 0

Variabile	Descrizione
szReturnCc	Tipo: Stringa Identifica il destinatario della copia di notifica inviata al mittente per la posta infetta ricevuta tramite un client MAPI Valore predefinito: Nessuno
szReturnSubject	Tipo: Stringa Consente l'inserimento di un testo alla riga Oggetto che informa il mittente della ricezione di posta infetta tramite un client MAPI Valore predefinito: Nessuno
szReturnBody	Tipo: Stringa Consente l'inserimento di un messaggio in formato testo che informa il mittente della ricezione di posta infetta tramite un client MAPI Valore predefinito: Nessuno
bSendMailToUser	Tipo: Booleana (1/0) Abilita VShield a informare altri utenti che è stata ricevuta posta infetta tramite un client MAPI Valore predefinito: 0
szSendTo	Tipo: Stringa Identifica altri utenti a cui inviare l'avviso che è stata ricevuta posta infetta tramite un client MAPI Valore predefinito: Nessuno
szSendCc	Tipo: Stringa Identifica le persone che devono ricevere copia dell'avviso ad altri utenti riguardante il fatto che è stata ricevuta posta infetta tramite un client MAPI Valore predefinito: Nessuno
szSendSubject	Tipo: Stringa Consente l'inserimento di un testo alla riga Oggetto che informa altri utenti della ricezione di posta infetta tramite un client MAPI Valore predefinito: Nessuno
szSendBody	Tipo: Stringa Consente l'inserimento di un messaggio in formato testo che informa altri utenti della ricezione di posta infetta tramite un client MAPI Valore predefinito: Nessuno

Variabile	Descrizione
CC_bReturnMail	Tipo: Booleana (1/0) Abilita VShield a informare il mittente della posta infetta ricevuta tramite un client cc:Mail Valore predefinito: 0
CC_bSendMailToUser	Tipo: Booleana (1/0) Abilita VShield a informare altri utenti della ricezione di posta infetta tramite un client cc:Mail Valore predefinito: 0
CC_szReturnCc	Tipo: Stringa Identifica il destinatario della copia di notifica inviata al mittente per la posta infetta ricevuta tramite un client cc:Mail Valore predefinito: Nessuno
CC_szReturnSubject	Tipo: Stringa Consente l'inserimento di un testo alla riga Oggetto che informa il mittente della ricezione di posta infetta tramite un client cc:Mail Valore predefinito: Nessuno
CC_szReturnBody	Tipo: Stringa Consente l'inserimento di un messaggio in formato testo che informa il mittente della ricezione di posta infetta tramite un client cc:Mail Valore predefinito: Nessuno
CC_szSendTo	Tipo: Stringa Identifica altri utenti a cui inviare l'avviso che è stata ricevuta posta infetta tramite un client cc:Mail Valore predefinito: Nessuno
CC_szSendCc	Tipo: Stringa Identifica le persone che devono ricevere copia dell'avviso ad altri utenti riguardante il fatto che è stata ricevuta posta infetta tramite un client cc:Mail Valore predefinito: Nessuno

Variabile	Descrizione
CC_szSendSubject	Tipo: Stringa Consente l'inserimento di un testo alla riga Oggetto che informa altri utenti della ricezione di posta infetta tramite un client cc:Mail Valore predefinito: Nessuno
CC_szSendBody	Tipo: Stringa Consente l'inserimento di un messaggio in formato testo che informa altri utenti della ricezione di posta infetta tramite un client cc:Mail Valore predefinito: Nessuno

EMailReport Options

Variabile	Descrizione
bLogToFile	Tipo: Booleana (1/0) Definisce se i risultati della scansione devono essere registrati nel file di log Valore predefinito: 1
bLimitSize	Tipo: Booleana (1/0) Definisce se le dimensioni del file devono essere limitate Valore predefinito: 1
uMaxKilobytes	Tipo: Numero intero (10-999) Definisce le dimensioni massime in kilobyte del file di log Valore predefinito: 100
bLogDetection	Tipo: Booleana (1/0) Abilita VShield a registrare i nomi dei virus rilevati Valore predefinito: 1
bLogClean	Tipo: Booleana (1/0) Definisce se i risultati della pulizia devono essere registrati Valore predefinito: 1
bLogDelete	Tipo: Booleana (1/0) Definisce se le operazioni di eliminazione dei file infetti devono essere registrate Valore predefinito: 1

Variabile	Descrizione
bLogMove	Tipo: Booleana (1/0) Definisce se le operazioni di spostamento dei file infetti devono essere registrate Valore predefinito: 1
bLogSettings	Tipo: Booleana (1/0) Abilita VShield a scrivere un record delle impostazioni in uso durante la scansione immediatamente precedente allo spegnimento del sistema o allo scaricamento di VShield. Valore predefinito: 1
bLogSummary	Tipo: Booleana (1/0) Abilita VShield a scrivere un riepilogo delle rilevazioni e delle azioni della scansione immediatamente precedente allo spegnimento del sistema o allo scaricamento di VShield. Valore predefinito: 1
bLogDateTime	Tipo: Booleana (1/0) Definisce se la data e l'ora di un evento devono essere registrate Valore predefinito: 1
bLogUserName	Tipo: Booleana (1/0) Definisce se il nome utente deve essere registrato Valore predefinito: 1
szLogFileName	Tipo: Stringa Definisce il nome del file di log Valore predefinito: C:\Program Files\Network Associates\McAfee VirusScan\WebEmail.txt

Modulo Scansione scaricamento

DownloadGeneralOptions

Variabile	Descrizione
bEnabled	Tipo: Booleana (1/0) Abilita la scansione dei file scaricati Valore predefinito: 1
bCanBeDisabled	Tipo: Booleana (1/0) Impedisce la disabilitazione della scansione dei file scaricati Valore predefinito: 1

DownloadDetectionOptions

Variabile	Descrizione
bScanAllFiles	Tipo: Booleana (1/0) Abilita VShield ad eseguire la scansione di tutti i file Valore predefinito: 0
bScanCompressed	Tipo: Booleana (1/0) Abilita VShield ad eseguire la scansione dei file compressi Valore predefinito: 1
bDetectTrojans	Tipo: Booleana (1/0) Abilita VShield ad eseguire la scansione per la ricerca di virus Trojan Valore predefinito: 1
bDetectJoke	Tipo: Booleana (1/0) Abilita VShield ad eseguire la scansione per la ricerca di virus Joke Valore predefinito: 1
bDetectCorrupted	Tipo: Booleana (1/0) Abilita VShield ad eseguire la scansione per la ricerca di file danneggiati Valore predefinito: 0
bDetectMaybe	Tipo: Booleana (1/0) Abilita VShield ad eseguire la scansione per la ricerca di varianti di virus conosciuti Valore predefinito: 1

Variabile	Descrizione
bProgFileHeuristics	Tipo: Booleana (1/0) Abilita VShield ad eseguire la scansione euristica dei file di programma Valore predefinito: 0
bMacroHeuristics	Tipo: Booleana (1/0) Abilita VShield ad eseguire la scansione euristica delle macro Valore predefinito: 0
szProgramExtensions	Tipo: Stringa Definisce le estensioni dei file da scandire. Valore predefinito: EXE, COM, DO?, XL?, RTF, BIN, SYS, OBD, VXD, MD?, DLL (il carattere ? è un carattere jolly)

DownloadActionOptions

Variabile	Descrizione
szMoveToFolder	Tipo: Stringa Definisce la cartella in cui spostare i file infetti Valore predefinito: \Infetti
szCustomMessage	Tipo: Stringa Definisce il messaggio personalizzato da visualizzare al rilevamento di un virus se l'azione è impostata su Richiedi azione Valore predefinito: McAfee VShield: Rilevato un virus nel file scaricato!
uScanAction	Tipo: Numero intero (0/3) Abilita VShield ad eseguire l'azione specificata quando viene rilevato un virus Valore predefinito: 0 Valori possibili: 0 - Richiedi azione. 1 - Sposta automaticamente i file infetti 2 - Elimina file infetti automaticamente 3 - Continua la scansione

Variabile	Descrizione
bButtonClean	Tipo: Booleana (1/0) Abilita VShield a fornire all'utente l'opzione di pulire il file se Richiedi azione è selezionata e viene rilevato un virus Valore predefinito: 1
bButtonDelete	Tipo: Booleana (1/0) Abilita VShield a fornire all'utente l'opzione di eliminare il file se Richiedi azione è selezionata e viene rilevato un virus Valore predefinito: 1
bButtonExclude	Tipo: Booleana (1/0) Abilita VShield a fornire all'utente l'opzione di escludere il file se Richiedi azione è selezionata e viene rilevato un virus Valore predefinito: 0
bButtonMove	Tipo: Booleana (1/0) Abilita VirusScan a fornire all'utente l'opzione di spostare il file infetto se Richiede azione è selezionata e viene rilevato un virus Valore predefinito: 1
bButtonContinue	Tipo: Booleana (1/0) Abilita VShield a fornire all'utente l'opzione di continuare l'evento intercettato se Richiedi azione è selezionata e viene rilevato un virus Valore predefinito: 1
bButtonStop	Tipo: Booleana (1/0) Abilita VShield a fornire all'utente l'opzione di impedire l'accesso al file infetto se Richiedi azione è selezionata e viene rilevato un virus Valore predefinito: 0

DownloadAlertOptions

Variabile	Descrizione
bDMIAlert	Tipo: Booleana (1/0) Abilita gli avvisi DMI (Desktop Management Interface) Valore predefinito: 0
bNetworkAlert	Tipo: Booleana (1/0) Abilita l'Avviso centralizzato Valore predefinito: 0
szNetworkAlertPath	Tipo: Stringa Specifica la cartella degli avvisi centralizzati su un server Valore predefinito: Nessuno
bSoundAlert	Tipo: Booleana (1/0) Abilita il programma ad emettere un segnale acustico di avviso quando viene rilevato un virus Valore predefinito: 1
bDisplayMessage	Tipo: Booleana (1/0) Definisce se visualizzare un messaggio personalizzato nella finestra di dialogo Richiedi azione al rilevamento di controlli ActiveX o applet Java ostili oppure durante un tentativo di connessione a un URL o indirizzo IP proibito. Valore predefinito: 0

DownloadReportOptions

Variabile	Descrizione
bLogToFile	Tipo: Booleana (1/0) Definisce se i risultati della scansione devono essere registrati nel file di log Valore predefinito: 1
bLimitSize	Tipo: Booleana (1/0) Definisce se le dimensioni del file devono essere limitate Valore predefinito: 1

Variabile	Descrizione
uMaxKilobytes	Tipo: Numero intero (10-999) Definisce le dimensioni massime in kilobyte del file di log Valore predefinito: 100
bLogDetection	Tipo: Booleana (1/0) Abilita VShield a registrare controlli ActiveX o applet Java ostili rilevati oppure i tentativi di collegamento a URL o indirizzi IP proibiti. Valore predefinito: 1
bLogClean	Tipo: Booleana (1/0) Definisce se i risultati della pulizia devono essere registrati Valore predefinito: 1
bLogDelete	Tipo: Booleana (1/0) Definisce se le operazioni di eliminazione dei file infetti devono essere registrate Valore predefinito: 1
bLogMove	Tipo: Booleana (1/0) Definisce se le operazioni di spostamento dei file infetti devono essere registrate Valore predefinito: 1
bLogSettings	Tipo: Booleana (1/0) Abilita VShield a scrivere un record delle impostazioni in uso durante la scansione immediatamente precedente allo spegnimento del sistema o allo scaricamento di VShield. Valore predefinito: 1
bLogSummary	Tipo: Booleana (1/0) Abilita VShield a scrivere un riepilogo delle rilevazioni e delle azioni della scansione immediatamente precedente allo spegnimento del sistema o allo scaricamento di VShield. Valore predefinito: 1
bLogDateTime	Tipo: Booleana (1/0) Definisce se la data e l'ora di un evento devono essere registrate Valore predefinito: 1

Variabile	Descrizione
bLogUserName	Tipo: Booleana (1/0) Definisce se il nome utente deve essere registrato Valore predefinito: 1
szLogFileName	Tipo: Stringa Definisce il nome del file di log Valore predefinito: C:\Program Files\Network Associates\McAfee VirusScan\WebInet.txt

Modulo Filtro Internet

INetFltrGeneralOptions

Variabile	Descrizione
bEnabled	Tipo: Booleana (1/0) Abilita la scansione dei file scaricati Valore predefinito: 1
bCanBeDisabled	Tipo: Booleana (1/0) Impedisce la disabilitazione della scansione dei file scaricati Valore predefinito: 1

INetFltrDetectionOptions

Variabile	Descrizione
bScanIP	Tipo: Booleana (1/0) Abilita VShield a bloccare gli indirizzi IP specificati Valore predefinito: 1
bScanHost	Tipo: Booleana (1/0) Abilita VShield a bloccare gli URL specificati Valore predefinito: 1
bScanJava	Tipo: Booleana (1/0) Abilita VShield ad eseguire la scansione per la ricerca di applet Java potenzialmente ostili Valore predefinito: 1

Variabile	Descrizione
bScanActiveX	Tipo: Booleana (1/0) Abilita VShield ad eseguire la scansione per la ricerca di oggetti ActiveX potenzialmente ostili Valore predefinito: 1
bDetectTrojans	Tipo: Booleana (1/0) Abilita VShield ad eseguire la scansione per la ricerca di virus Trojan Valore predefinito: 1
bDetectJoke	Tipo: Booleana (1/0) Abilita VShield ad eseguire la scansione per la ricerca di virus Joke Valore predefinito: 1
bDetectCorrupted	Tipo: Booleana (1/0) Abilita VShield ad eseguire la scansione per la ricerca di file danneggiati Valore predefinito: 0
bDetectMaybe	Tipo: Booleana (1/0) Abilita VShield ad eseguire la scansione per la ricerca di varianti di virus conosciuti Valore predefinito: 1
bProgFileHeuristics	Tipo: Booleana (1/0) Abilita VShield ad eseguire la scansione euristica dei file di programma Valore predefinito: 0
bMacroHeuristics	Tipo: Booleana (1/0) Abilita VShield ad eseguire la scansione euristica delle macro Valore predefinito: 0

INetFltrActionOptions

Variabile	Descrizione
uScanAction	Tipo: Integer (0/1) Abilita VShield ad adottare l'azione specificata nel caso vengano rilevati URL o indirizzi IP proibiti oppure controlli ActiveX o applet Java ostili Valore predefinito: 0 Valori possibili: 0 - Richiedi azione. 1 - Nega accesso all'oggetto.

INetFltrAlertOptions

Variabile	Descrizione
bDMIAlert	Tipo: Booleana (1/0) Abilita gli avvisi DMI (Desktop Management Interface) Valore predefinito: 0
bNetworkAlert	Tipo: Booleana (1/0) Abilita l'Avviso centralizzato Valore predefinito: 0
szNetworkAlertPath	Tipo: Stringa Specifica la cartella degli avvisi centralizzati su un server Valore predefinito: Nessuno
bDisplayMessage	Tipo: Booleana (1/0) Definisce se visualizzare il messaggio personalizzato nella finestra di dialogo Richiedi azione al rilevamento di un virus Valore predefinito: 0

Variabile	Descrizione
bSoundAlert	Tipo: Booleana (1/0) Abilita VShield ad emettere un segnale acustico nel caso vengano rilevati URL o indirizzi IP proibiti oppure controlli ActiveX o applet Java ostili Valore predefinito: 1
szCustomMessage	Tipo: Stringa Se l'azione è impostata su Richiedi azione, questa variabile definisce il messaggio personalizzato da visualizzare al rilevamento di controlli ActiveX o applet Java ostili oppure durante un tentativo di connessione a un URL o indirizzo IP proibito. Valore predefinito: McAfee VShield: Rilevati oggetti Internet o siti proibiti!

INetFltrReportOptions

Variabile	Descrizione
bButtonDeny	Tipo: Booleana (1/0) Abilita VShield a fornire all'utente l'opzione di negare l'accesso ai siti in cui siano rilevati oggetti potenzialmente pericolosi Valore predefinito: 1
bButtonContinue	Tipo: Booleana (1/0) Abilita VirusScan a fornire all'utente l'opzione di proseguire l'evento intercettato anche se è stata selezionata Richiede azione ed è stato rilevato un indirizzo URL o IP proibiti oppure controlli ActiveX o applet Java ostili. Valore predefinito: 1
bLogToFile	Tipo: Booleana (1/0) Definisce se i risultati della scansione devono essere registrati nel file di log Valore predefinito: 1
bLimitSize	Tipo: Booleana (1/0) Definisce se le dimensioni del file devono essere limitate Valore predefinito: 1

Variabile	Descrizione
uMaxKilobytes	Tipo: Numero intero (10-999) Definisce le dimensioni massime in kilobyte del file di log Valore predefinito: 100
bLogDetection	Tipo: Booleana (1/0) Abilita VShield a registrare i nomi dei virus rilevati Valore predefinito: 1
bLogSettings	Tipo: Booleana (1/0) Abilita VShield a scrivere un record delle impostazioni in uso durante la scansione immediatamente precedente allo spegnimento del sistema o allo scaricamento di VShield. Valore predefinito: 1
bLogSummary	Tipo: Booleana (1/0) Abilita VShield a scrivere un riepilogo delle rilevazioni e delle azioni della scansione immediatamente precedente allo spegnimento del sistema o allo scaricamento di VShield. Valore predefinito: 1
bLogDateTime	Tipo: Booleana (1/0) Definisce se la data e l'ora di un evento devono essere registrate Valore predefinito: 1
bLogUserName	Tipo: Booleana (1/0) Definisce se il nome utente deve essere registrato Valore predefinito: 1
szLogFileName	Tipo: Stringa Definisce il nome del file di log Valore predefinito: C:\Program Files\Network Associates\McAfee VirusScan\WebFiltr.txt

Modulo Sicurezza

SecurityOptions

Variabile	Descrizione
bPasswordEnabled	Tipo: Booleana (1/0) Definisce se la protezione password è abilitata Valore predefinito: 0
szPasswordCRC	Riservati. Non modificare
bProtectAllOptions	Tipo: Booleana (1/0) Definisce se tutte le pagine delle proprietà devono essere protette da password Valore predefinito: 1
szPasswordProtect	Riservati. Non modificare

Impostazioni generali

AVCONFILE

Variabile	Descrizione
AVCONFILE	Tipo: Stringa Specifica il percorso di accesso a AVCONSOLE Valore predefinito: C:\Program Files\Network Associates\McAfee VirusScan\avconsol.ini
SEZIONE	Tipo: Stringa Specifica la sede del rapporto in AVCONSOL.INI Valore predefinito: Item_0

Utilizzo delle opzioni della riga di comando VirusScan E

Esecuzione della riga di comando VirusScan

È possibile eseguire la riga di comando VirusScan da una finestra Prompt di MS-DOS o riavviando il computer in modalità DOS. Per ottenere migliori prestazioni, Network Associates consiglia di riavviare il computer in modalità DOS. Per informazioni sulla procedura per il riavvio del computer in modalità DOS, consultare la documentazione Microsoft Windows.

Per utilizzare la riga di comando VirusScan, procedere come segue:

1. Aprire una finestra Prompt di MS-DOS da Windows o riavviare il computer in modalità DOS.
2. Accedere alla directory di programma VirusScan. Se VirusScan è stato installato con le opzioni predefinite, immettere la seguente riga al prompt dei comandi per individuare la directory corretta:

   ```
   C:\progra~1\networ~1\mcafee~1
   ```

3. Digitare `scan` e poi le opzioni di scansione che si desidera utilizzare, al prompt dei comandi.

   La riga di comando VirusScan avvia immediatamente la scansione del sistema con le opzioni selezionate. Al termine della procedura, visualizza i risultati dell'operazione di scansione e poi ritorna al prompt dei comandi.

4. Per eseguire un'altra operazione di scansione, ripetere Passaggio 3. Per chiudere la finestra Prompt di MS-DOS, digitare `exit` al prompt dei comandi. Se il computer è stato riavviato in modalità DOS, digitare `win` per avviare Windows; in caso contrario, riavviare il computer normalmente.

Le tabelle delle pagine seguenti elencano tutte le opzioni disponibili di VirusScan.

NOTA: Quando si specifica un nome di file come parte di un'opzione di una riga di comando, è necessario includere il percorso intero del file se questo non è presente nella directory di programma VirusScan.

Opzioni della riga di comando

Opzione della riga di comando	Limitazioni	Descrizione
Tutte le opzioni riportate di seguito consentono di configurare sia le scansioni su richiesta sia le scansioni all'accesso, salvo indicazioni diverse.		
/? o /HELP	Nessuno	Visualizza una lista di opzioni della riga di comando VirusScan, ciascuna con una breve descrizione.
/ADL	Solo opzione Scansione su richiesta.	Esegue la scansione di tutte le unità locali, incluse le unità compresse e le schede PC, ma non i dischi, oltre a tutte le altre unità specificate sulla riga di comando. Per eseguire la scansione di unità disco sia locali che di rete, utilizzare insieme i comandi /ADL e /ADN nella stessa riga di comando. OS/2: /ADL include nella scansione l'unità CD-ROM, se utilizzata con /NODDA.
/ADN	Solo opzione Scansione su richiesta.	Esegue la scansione per la ricerca di virus su tutte le unità di rete, incluse le unità CD-ROM, oltre a tutte le altre unità specificate sulla riga di comando. *Nota:* Per eseguire la scansione di unità disco sia locali che di rete, utilizzare insieme i comandi /ADL e /ADN nella stessa riga di comando.
/ALERTPATH *<dir>*	Solo opzione Scansione su richiesta.	Indica la directory *<dir>* come percorso di rete controllato dall'Avviso centralizzato.
/ALL	Solo opzione Scansione su richiesta.	Annulla l'impostazione di scansione predefinita eseguendo la scansione di tutti i file infettabili—indipendentemente dalla loro estensione. *Note:* L'utilizzo dell'opzione /ALL aumenta notevolmente il tempo richiesto per la scansione. Utilizzare questa opzione solo se si è rilevato un virus o se se ne sospetta l'esistenza. In base alle impostazioni predefinite, VirusScan esegue la scansione solo dei file che hanno le seguenti estensioni: .EXE, .COM, .SYS, .BIN, .OVL, .DLL, .DOC, .DOT, .XLA, .XLS, .XLT, .RTF, e .VXD. Questi sono i tipi di file maggiormente esposti al rischio di infezioni.

Opzione della riga di comando	Limitazioni	Descrizione
/ANALYZE	Solo opzione Scansione su richiesta. È necessaria la memoria estesa.	Abilita VirusScan a utilizzare tutte le scansioni euristiche, di programma e di macro. *Nota:* /MANALYZE ricerca solo i virus macro, mentre /PANALYZE ricerca i virus di programma.
/ANYACCESS	Solo opzione Scansione all'accesso.	Esegue la scansione di: * il settore di boot quando un dischetto viene letto o inciso * eseguibili * qualsiasi nuovo file.
/APPEND	Solo opzione Scansione su richiesta.	Utilizzare con /REPORT per aggiungere un messaggio di testo al file di rapporto specificato anziché sovrascriverlo.
/BOOT	Solo opzione Scansione su richiesta.	Scansione del settore di boot e del record di boot principale.
/BOOTACCESS	Solo opzione Scansione all'accesso.	Esegue la scansione del settore di boot di un dischetto per la ricerca di virus quando si accede a un dischetto (incluse le operazioni di lettura/scrittura).
/CLEAN	Solo opzione Scansione su richiesta.	Elimina i virus da tutti i file infetti e dalle aree del sistema.
/CLEANDOCALL	Solo opzione Scansione su richiesta.	Come misura di precauzione contro i virus macro, /CLEANDOCALL ripulisce tutte le macro dai documenti Microsoft Word e Office. ***Nota:*** Questa opzione elimina tutte le macro, incluse le macro non infette da virus.
/CONTACT *<messaggio>*	Solo opzione Scansione all'accesso.	Visualizza il messaggio specificato quando rileva un virus. Il messaggio non può superare i 255 caratteri.

Opzione della riga di comando	Limitazioni	Descrizione
/CONTACTFILE *<filename>*	Nessuno	Visualizza i contenuti di *<filename>* quando viene rilevato un virus. È un'opportunità di fornire informazioni sui contatti ed istruzioni all'utente quando viene rilevato un virus. Questa opzione è particolarmente utile negli ambienti di rete, poiché consente di conservare il messaggio in un file centrale invece che su ogni workstation. ***Nota:*** Qualunque carattere è valido in un messaggio di contatto tranne un backslash (\). I messaggi che cominciano con uno slash (/) o una linetta (-) devono essere messi tra virgolette.
/DEL	Solo opzione Scansione su richiesta.	Elimina i file infetti.
/EXCLUDE *<filename>*	Solo opzione Scansione su richiesta.	Non sottoporre a scansione né aggiungere codici di convalida ai file elencati in *<filename>*. Utilizzare questa opzione per: * Escludere file specifici da una scansione. Elencare il percorso completo per ciascun file che si desidera escludere sulla sua stessa riga. È possibile utilizzare caratteri jolly * e ?
/FILEACCESS	Solo opzione Scansione all'accesso.	Esegue la scansione dei file eseguibili all'accesso e all'esecuzione. ***Nota****:* Questa scansione *non* controlla il settore di boot.
/FREQUENCY <*n* >	Solo opzione Scansione su richiesta.	Non eseguire la scansione <*n*> ore dopo la scansione precedente. In ambienti dove esiste un rischio molto basso di infezione virale, utilizzare questa opzione per evitare scansioni inutili. Una scansione eseguita con frequenza assicura un livello maggiore di protezione contro le infezioni.
/GUIDA o /?	Nessuno	Visualizza una lista di opzioni della riga di comando VirusScan, ciascuna con una breve descrizione.
/IGNORE *<drive(s)>*	Solo opzione Scansione all'accesso.	Non controlla i file caricati da unità specificate.

Opzione della riga di comando	Limitazioni	Descrizione
/LOAD *<filename>*	Solo opzione Scansione su richiesta.	Carica le opzioni di scansione dal file nominato. Utilizzare questa opzione per eseguire una scansione già configurata attraverso il caricamento di impostazioni personalizzate salvate in un file formattato ASCII.
/LOCK	Non disponibile in ambienti con scarsa memoria	Quando l'opzione /LOCK viene attivata, VirusScan ferma e blocca il sistema quando rileva un virus. /LOCK è utile negli ambienti di rete altamente vulnerabili, ad esempio i laboratori informatici aperti a tutti. È consigliabile utilizzare /LOCK con l'opzione /CONTACTFILE per indicare all'utente cosa fare o chi contattare se VirusScan blocca il sistema.
/MANALYZE	Solo opzione Scansione su richiesta. È necessaria la memoria estesa.	Imposta le funzioni di scansione euristica di VirusScan in modo da ricercare solo i virus macro. *Nota:* /PANALYZE ricerca solo i virus di programma; /ANALYZE ricerca sia i virus di programma sia i virus macro.
/MANY	Solo opzione Scansione su richiesta.	Esegue la scansione consecutiva di più dischetti su una singola unità. VirusScan richiederà ciascun minidisco. Utilizzare questa opzione per controllare più dischetti rapidamente. Non è possibile utilizzare l'opzione /MANY se si esegue VirusScan da un dischetto di boot e si dispone di una sola unità floppy.
/MAXFILESIZE *<xxx.x>*	Solo opzione Scansione su richiesta.	Scandisce solo i file non più grandi di *<xxx.x>* megabyte.
/MEMEXCL		Esclude dalla scansione l'indirizzo di memoria A0000:0000.

Opzione della riga di comando	Limitazioni	Descrizione
/MOVE *<dir>* o *.???	Solo opzione Scansione su richiesta.	*/MOVE <directory>:* Sposta tutti i file infetti rilevati durante una scansione nella directory specificata, preservando la lettera di unità e la struttura di directory. *Nota:* Questa opzione non ha effetto se l'MBR (Master Boot Record) o il settore di boot è infettato, in quanto questi non sono i file reali. */MOVE*.???:* VirusScan modificherà l'estensione dei file infettati ma non li sposterà. Ad esempio, se si usa l'opzione /MOVE*.BAD, eventuali file infetti saranno semplicemente rinominati con l'estensione .BAD ma non saranno fisicamente spostati.
/NOBEEP	Solo opzione Scansione su richiesta.	Disattiva il segnale acustico che viene emesso ogni volta che VirusScan trova un virus.
/NOBREAK	Solo opzione Scansione su richiesta.	Disabilita CTRL-C e CTRL-BREAK durante le operazioni di scansione. Gli utenti non saranno in grado di interrompere le operazioni di scansione in corso quando si utilizza l'opzione /NOBREAK.
/NOCOMP	Solo opzione Scansione su richiesta. È necessaria la memoria estesa.	Tralascia il controllo dei file eseguibili compressi creati con i programmi di compressione file LZEXE o PkLite. Ciò consente di ridurre il tempo di scansione quando non è necessario effettuare un'operazione di scansione completa. In caso contrario, per valore predefinito VirusScan controlla il contenuto dei file eseguibili oppure dei file di decompressione automatica, eseguendo la decompressione di ciascun file nella memoria e la ricerca delle firme dei virus. VirusScan continuerà la ricerca delle modifiche nei file eseguibili compressi controllando nel caso in cui contengano codici di convalida VirusScan.

Opzione della riga di comando	Limitazioni	Descrizione
/NODDA	Solo opzione Scansione su richiesta.	Non si ha l'accesso diretto al disco. Ciò impedisce a VirusScan di accedere al record di boot. Questa funzione è stata aggiunta per consentire l'esecuzione di VirusScan in Windows NT. Può essere necessario utilizzare questa opzione su alcune unità dipendenti da periferiche. Se si utilizza /NODDA con le opzioni /ADN o /ADL, possono essere generati errori durante l'accesso a periferiche CD-ROM vuote o a unità Zip vuote. Se si verifica ciò, per continuare la scansione, immettere F (per Fail) come risposta ai messaggi di errore.
/NODISK	Solo opzione Scansione all'accesso.	Non esegue la scansione del settore di boot durante il caricamento di VShield.
/NODOC	Solo opzione Scansione su richiesta.	Non esegue la scansione dei file Microsoft Office.
/NOEMS	Solo opzione Scansione all'accesso.	Disabilita VShield dall'uso della memoria estesa (EMS).
/NOEXPIRE	Solo opzione Scansione su richiesta.	Disattiva il messaggio relativo alla "data di scadenza" se i file di dati di VirusScan non sono aggiornati.
/NOMEM	Nessuno	Non esegue la scansione della memoria. Ciò consente di ridurre i tempi di scansione. Utilizzare /NOMEM soltanto quando si è assolutamente certi dell'assenza di virus nel computer.
/NOREMOVE	Solo opzione Scansione all'accesso.	Evita la rimozione di VShield dalla memoria utilizzando l'opzione /REMOVE
/NOWARMBOOT	Solo opzione Scansione all'accesso.	Non esegue sul settore di boot del dischetto nell'unità A: la ricerca dei virus durante l'avvio a caldo (riavvio del sistema o CTRL+ALT+CANC).
/NOXMS	Solo opzione Scansione all'accesso.	Non utilizza l'XMS (extended memory).
/ONLY *<unità>*	Solo opzione Scansione all'accesso.	Controlla solo i programmi caricati dall'unità specificata.

Opzione della riga di comando	Limitazioni	Descrizione
/PANALYZE	Solo opzione Scansione su richiesta. È necessaria la memoria estesa.	Abilita VirusScan a eseguire la scansione utilizzando l'euristica di programma. *Nota:* /MANALYZE ricerca solo i virus macro; /ANALYZE ricerca sia i virus di programma sia i virus macro.
/PAUSE	Solo opzione Scansione su richiesta.	Attiva la pausa dello schermo. Quando VirusScan riempie lo schermo di messaggi, viene visualizzata anche la richiesta "Premere un tasto per continuare". Altrimenti, in base all'impostazione predefinita, VirusScan riempie e fa scorrere lo schermo in modo continuo e senza interruzioni, consentendo così l'esecuzione su PC con varie unità o con gravi infezioni senza richiedere interventi da parte dell'utente. Quando si utilizzano la opzioni di rapporto (/REPORT, /RPTCOR e /RPTERR), si consiglia di non specificare /PAUSE.
/PLAD	Solo opzione Scansione su richiesta.	Mantiene le ultime date di accesso alle unità Novell NetWare. In genere, le unità di rete di proprietà esclusiva aggiornano la data dell'ultimo accesso quando VirusScan apre ed esamina un file. Tuttavia, alcuni sistemi di backup a nastro utilizzano questa data per decidere se è necessario eseguire il backup del file. Utilizzare /PLAD per evitare che la data dell'ultimo accesso venga modificata dalla scansione.
/RECONNECT	Solo opzione Scansione all'accesso.	Ripristina VShield dopo che è stato disabilitato da determinati driver o programmi residenti in memoria.
/REMOVE	Solo opzione Scansione all'accesso.	Scarica VShield dalla memoria.

Opzione della riga di comando	Limitazioni	Descrizione
/REPORT *<nomefile>*	Solo opzione Scansione su richiesta.	Crea un rapporto di file infetti e di errori di sistema e salva i dati in *<filename>* in formato ASCII. Se esiste già un file *<filename>*, /REPORT lo sovrascrive. Per evitare la sovrascrittura, utilizzare l'opzione /APPEND con l'opzione /REPORT: VirusScan aggiungerà informazioni sul rapporto alla fine del file, invece di eseguire la sovrascrittura. Per aggiungere al rapporto i file sottoposti a scansione, i file danneggiati, i file modificati e gli errori di sistema, è possibile utilizzare le opzioni /RPTALL, /RPTCOR e /RPTERR. È possibile includere l'unità e la directory di destinazione (ad esempio, D:\VSREPRT\ALL.TXT); tuttavia se la destinazione è un'unità di rete, è necessario disporre dei diritti per la creazione o la cancellazione dei file su questa unità. Quando si utilizzano le opzioni di rapporto, si sconsiglia l'uso di /PAUSE.
/RPTALL	Solo opzione Scansione su richiesta.	Include tutti i file sottoposti a scansione nel file /REPORT. Quando utilizzata con /REPORT, questa opzione aggiunge i nomi dei file danneggiati nel file di rapporto. È possibile utilizzare l'opzione /RPTCOR con /RPTERR sulla riga di comando. Quando si utilizzano le opzioni di rapporto, si sconsiglia l'uso di /PAUSE.
/RPTCOR	Solo opzione Scansione su richiesta.	Include i file danneggiati nel file /REPORT. Quando utilizzata con /REPORT, questa opzione aggiunge i nomi dei file danneggiati nel file di rapporto. I file danneggiati rilevati da VirusScan potrebbero essere stati danneggiati da un virus. È possibile utilizzare l'opzione /RPTCOR con /RPTERR sulla riga di comando. Alcuni file che richiedono un file sovrapposto o eseguibile per funzionare correttamente (Ossia, quei file che non sono eseguibili da soli) potrebbero causare letture errate. Quando si utilizzano le opzioni di rapporto, si sconsiglia l'uso di /PAUSE.

Opzione della riga di comando	Limitazioni	Descrizione
/RPTERR	Solo opzione Scansione su richiesta.	Include gli errori nel file /REPORT. Quando utilizzata con l'opzione /REPORT, questa opzione aggiunge un elenco di errori di sistema al file di rapporto. /LOCK è utile negli ambienti di rete altamente vulnerabili, ad esempio i laboratori informatici aperti a tutti. È possibile utilizzare l'opzione /RPTCOR con /RPTERR sulla riga di comando. Gli errori di sistema possono includere problemi di lettura e scrittura su un dischetto o sul disco rigido, problemi al file system o alla rete, problemi di creazione di rapporti ed altri problemi correlati. Quando si utilizzano le opzioni di rapporto, si sconsiglia l'uso di /PAUSE.
/SAVE	Solo opzione Scansione all'accesso.	Salva le opzioni della riga di comando nel file VSHIELD.INI.
/SUB	Solo opzione Scansione su richiesta.	Esegue la scansione delle sottodirectory all'interno di una directory. Per valore predefinito, quando si specifica una directory piuttosto che un'unità per l'esecuzione della scansione, VirusScan esaminerà solo i file della directory e non quelli della sottodirectory. Utilizzare l'opzione /SUB per eseguire la scansione di tutte le sottodirectory all'interno delle directory specificate. Se si sta effettuando la scansione di un'intera unità, non è necessario utilizzare l'opzione /SUB.
/UNZIP	Solo opzione Scansione su richiesta. È necessaria la memoria estesa.	Scansione di file compressi.

Opzione della riga di comando	Limitazioni	Descrizione
/VIRLIST	Solo opzione Scansione su richiesta.	Visualizza il nome e una breve descrizione di ogni virus rilevato da VirusScan. Per leggere la lista dei virus una schermata per volta, è possibile utilizzare le opzioni /PAUSE e /VIRLIST. *Per indirizzare l'uscita di /VIRLIST in un file di testo:* Al prompt di comando, digitare: scan /VIRLIST> filename.txt VirusScan è in grado di rilevare molti virus, pertanto questo file è lungo più di 250 pagine. Poiché le dimensioni sono eccessive per poterlo aprire con il programma "Edit" di MS-DOS, si consiglia di utilizzare Notepad o un altro editor di testo.
/XMSDATA	Solo opzione Scansione all'accesso.	Carica i file di dati di VShield nella memoria XMS.

Indice

A

B

C

D

E

F

G

H

I

L

M

N

O

P

Q

R

S

T

U

V

W

Z