IBM eNetwork Firewall per Windows NT

Manuale di riferimento

Versione 3 Rilascio 2.1.1

SC13-2750-01

IBM eNetwork Firewall per Windows NT

Manuale di riferimento

Versione 3 Rilascio 2.1.1

SC13-2750-01

NOTA:

Prima di utilizzare queste informazioni e il prodotto supportato, consultare “Informazioni particolari” a pagina v.

Seconda edizione (giugno 1998)

Questa pubblicazione si riferisce a IBM eNetwork Firewall per Windows NT Versione 3 Rilascio 2.1.1 (numero programma 5765-C16). Questa edizione sostituisce SC13-2750-00.

Richieste di ulteriori copie di questo prodotto o informazioni tecniche sullo stesso vanno indirizzate ad un rivenditore autorizzato o ad un rappresentante commerciale IBM. Le pubblicazioni non sono disponibili all'indirizzo di seguito riportato.

Come ultima pagina del manuale è stato predisposto un foglio riservato ai commenti del lettore. Se il modulo è stato rimosso, indirizzare i commenti a:

SELFIN S.p.A.
Translation assurance
Via F. Giordani, 7
80122 Napoli

Tutti i commenti ed i suggerimenti potranno essere utilizzati dall'IBM e dalla Selfin e diventeranno esclusiva delle stesse.

Indice

Informazioni particolari

I riferimenti contenuti in questa pubblicazione relativi a prodotti, programmi o servizi IBM non implicano che l'IBM intenda renderli disponibili in tutti i paesi in cui opera.

Qualsiasi riferimento a programmi su licenza d'uso o ad altri prodotti IBM contenuto in questa pubblicazione non significa che soltanto tali programmi e/o prodotti possano essere usati.

In sostituzione a quelli forniti dall'IBM, possono essere usati prodotti, programmi o servizi funzionalmente equivalenti che non comportino violazione dei diritti di proprietà intellettuale o di altri diritti dell'IBM.

È responsabilità dell'utente valutare e verificare la possibilità di utilizzare altri programmi e/o prodotti, fatta eccezione per quelli espressamente indicati dall'IBM.

L'IBM può avere brevetti o domande di brevetto in corso relativi a quanto trattato nella presente pubblicazione. La fornitura di questa pubblicazione non implica la concessione di alcuna licenza su di essi. Chi desiderasse ricevere informazioni relative a licenze può rivolgersi per iscritto a:

Director of Commercial Relations IBM Europe
IBM Corporation
D-7030 Boeblingen
Deutschland

Coloro che detengono la licenza su questo programma e desiderano avere informazioni su di esso allo scopo di consentire: (i) uno scambio di informazioni tra programmi indipendenti ed altri (compreso questo) e (ii) l'uso reciproco di tali informazioni, dovrebbero rivolgersi:

IBM Corporation
P.O. Box 12195
3039 Cornwallis Road
Research Triangle Park, NC 27709-2195
USA

Queste informazioni possono essere rese disponibili, secondo condizioni contrattuali appropriate, compreso, in alcuni casi, l'addebito di un canone.

Il programma su licenza descritto in questo manuale e tutto il materiale su licenza ad esso relativo sono forniti dall'IBM nel rispetto delle condizioni previste dalla licenza d'uso.

Questa pubblicazione non deve essere riprodotta e viene fornita senza alcuna garanzia, esplicita o implicita. Essa è inoltre da considerarsi solo una guida generale e a titolo indicativo. La IBM Italia si riserva di modificare le caratteristiche tecniche e fisiche nonché i nomi dei prodotti ivi citati, declinando ogni responsabilità per danni diretti o indiretti derivanti da eventuali modifiche.

Questo prodotto comprende software sviluppato dall'Università della California, di Berkeley e dei suoi collaboratori.

Marchi

I seguenti termini, contrassegnati in questa pubblicazione da un asterisco (*), sono marchi dell'IBM Corporation:

- Common User Access
- DB2
- eNetwork
- IBM
- OS/2

Microsoft, Windows, Windows NT ed il logo di Windows 95 sono marchi della Microsoft Corporation.

UNIX è esclusivamente un marchio su licenza della X/Open Company Limited.

Java e HotJava sono marchi della Sun Microsystems, Inc.

Nomi di altri prodotti, società e servizi, che potrebbero essere contrassegnati da un doppio asterisco (**), possono essere marchi di altre società.

Introduzione

Questo manuale è rivolto ai responsabili della sicurezza di rete o di sistema che installano, gestiscono e utilizzano IBM eNetwork Firewall per Windows NT** Versione 3.2. Per utilizzare i programmi client, quali Telnet o FTP, consultare la guida per l'utente relativa ai programmi client TCP/IP.

Conoscenze di base

È importante avere una buona conoscenza di TCP/IP e della gestione di rete prima di installare e configurare IBM eNetwork Firewall. Dal momento che si è in procinto di installare e configurare un firewall che controlla gli accessi alla rete in entrata e in uscita, è indispensabile avere una conoscenza di base del funzionamento di una rete. In particolare è necessaria una buona familiarità con i principi fondamentali relativi a indirizzi IP, nomi completi e maschere di sottorete.

Un eccellente manuale su TCP/IP, relativo a netstat, arp, ifconfig, ping, nslookup, DNS, sendmail, instradamento e molto altro ancora è *TCP/IP Network Administration*. Per ulteriori dettagli, consultare la *Bibliografia*.

Un eccellente manuale per i gestori di UNIX, che fornisce anch'esso una panoramica completa su TCP/IP, instradamento, hardware di rete, DNS, e sendmail è *UNIX System Administration Handbook*. Per ulteriori dettagli, consultare la *Bibliografia*.

Funzioni di questo rilascio

IBM eNetwork Firewall per Windows NT offre una grande varietà di funzioni ed include le tre architetture del firewall:

1. Proxy di applicazione
   - FTP
   - HTTP, incluso Gopher e WAIS
   - Telnet
   - SafeMail

   HTTP, Telnet e FTP hanno funzioni di autenticazione.
2. Gateway a livello di circuito tramite il Socks Protocol Versione 5, uno standard di Internet
3. Filtro - un completo ed efficace insieme di criteri secondo i quali è possibile negare o consentire il traffico. I criteri includono l'indirizzo TCP/IP, la porta, il protocollo, la direzione, l'adattatore (sicuro/non sicuro) e così via.

   Molti servizi predefiniti rendono più rapida la procedura di impostazione.

Socks Protocol Versione 5

Oltre alla sua semplicità e flessibilità, il Socks Protocol Versione 5 presenta i seguenti vantaggi:

- Installazione semplificata dei metodi di autenticazione e crittografia
- Associazione UDP, che crea un circuito proxy virtuale per il passaggio dei circuiti proxy basati su UDP
- Socks V5 Watcher, che consente di visualizzare le informazioni sull'esecuzione di socks in tempo reale

NAT (Network Address Translation)

Con lo sviluppo sempre crescente di Internet, il problema dell'esaurimento degli indirizzi IP è diventato rilevante. Network address translation (Network Address Translation) fornisce una soluzione al problema dell'esaurimento degli indirizzi IP basata sul riutilizzo degli indirizzi.

Il vantaggio di NAT sta nel fatto che consente in modo trasparente ad una rete di utilizzare indirizzi privati o non validi per comunicare con gli host presenti su Internet, facendo in modo che le reti private possano effettivamente disporre di un vasto spazio per gli indirizzi. Se viene utilizzato NAT, inoltre, gli indirizzi presenti nella rete privata vengono nascosti all'esterno e viene garantito un livello supplementare di sicurezza.

Gestione semplificata

Con l'utilizzo di un'applicazione Java**, che è possibile gestire da una macchina remota, si possono eseguire facilmente gli aggiornamenti alla configurazione del firewall. È possibile assegnare diversi livelli di autorizzazione a vari responsabili per favorire il controllo dell'accesso al firewall. Questa singola GUI (graphical user interface), facile da comprendere, può essere utilizzata per gestire entrambi i firewall Windows NT ed AIX.

Hardening di NT

Quando il firewall viene installato, vengono disabilitati i protocolli che non sono TCP/IP, i servizi di sistema non necessari ed i login locali dei codici di contabilizzazione degli utenti non responsabili.

Autenticazione più efficace

Viene fornito un supporto per tutti i meccanismi di autenticazione a base token comuni, quali SecurID, SecureNet Key e così via.

Programmi di utilità per i prospetti

I programmi di utilità per i prospetti consentono di eseguire un'interrogazione SQL per il log di sistema una volta esportato in un processo del database.

Avvisi, controllo e log

Un log completo e dettagliato comprende tutte le attività del firewall più l'indirizzo TCP/IP, gli ID utente, TOD, i nomi file, i numeri di porta e così via. Viene fornito il controllo log per verificare tutte le attività sospette e per avvisare che le soglie sono state superate.

Isolamento di più reti

Utilizzando più NIC (Network Interface Cards) sul firewall, è possibile isolare più sottoreti.

Supporto per la lingua nazionale

Il supporto di lingua nazionale viene offerto per l'inglese, il giapponese, il coreano, il francese, il cinese semplificato, il cinese tradizionale, l'italiano, lo spagnolo ed il portoghese brasiliano.

Immissione degli indirizzi IP

Quando si configura il firewall, viene richiesta l'immissione degli indirizzi IP. È possibile immettere un indirizzo IP decimale con punti, con quattro ottetti, nel formato:

```
nnn.nnn.nnn.nnn
```

dove ogni `nnn` è un insieme di tre numeri compresi nell'intervallo 000–255.

Assistenza tecnica IBM

Il centro di assistenza tecnica IBM fornisce assistenza telefonica per l'individuazione e la risoluzione dei problemi. È possibile chiamare il centro di assistenza tecnica IBM in qualsiasi momento; si riceverà una risposta telefonica entro le successive 8 ore lavorative (lunedì–venerdì, 8:00–17:00, ora locale del cliente). Il numero di telefono da chiamare è il seguente: 167-820094.

In alternativa è possibile contattare il rappresentate IBM o il rivenditore autorizzato IBM.

Capitolo 1. Utilizzo dell'interfaccia riga comandi di IBM Firewall

Questo capitolo descrive i comandi che possono essere utilizzati da una riga comandi di IBM eNetwork Firewall.

Le seguenti informazioni fanno riferimento ai comandi:

- I comandi citati in questo manuale utilizzano la seguente sintassi:
  - la *sottolineatura* indica i dati immessi dall'utente.
  - [] indica che un parametro è facoltativo.
  - {} indica che l'utente ha una scelta di parametri.
  - ‘ separa le scelte.
- Tutti i parametri utilizzano il formato `parola chiave=valore`.
- Se un parametro è composto da più valori, questi devono essere racchiusi tra virgolette e delimitati da spazi vuoti, ad esempio:

  ```
  secaddr="11.22.33.1 11.22.33.2"
  ```

- Non includere spazi all'interno della stringa relativa al parametro a meno che non sia racchiusa tra virgolette.
- Se uno o più parametri obbligatori vengono omessi, il programma di utilità della riga comandi elenca i parametri mancanti.
- Se viene immesso un valore non valido per il parametro, il programma di utilità della riga comandi notifica questo errore.
- Alcuni servizi del firewall vengono aggiornati dinamicamente in base alle modifiche apportate ai file di configurazione. Altri richiedono un sottocomando update. Viene fornito un sottocomando `update` per i servizi del firewall che richiedono istruzioni.
- Soltanto i responsabili principali del firewall possono eseguire i programmi dalla riga comandi.
- A causa della complessità e dell'interdipendenza dei file, si consiglia di **non editare direttamente nessun file di configurazione**.

Server di configurazione

Il comando `fwcfgsrv` elenca o modifica le opzioni del server di configurazione. Per poter eseguire questo comando, un responsabile deve essere autorizzato a gestire le funzioni di controllo del traffico.

Per elencare le opzioni del server di configurazione, immettere il seguente comando.

```
fwcfgsrv cmd=list
```

L'emissione del comando `fwcfgsrv` viene visualizzata nel seguente modo:

```
localonly = yes/no
encryption = none/ssl
sslfile = filename if one is defined
```

Per modificare le opzioni del server di configurazione, immettere il seguente comando.

```
fwcfgsrv cmd=change
         [localonly={yes‘no}]
         [encryption={none‘ssl}]
         [sslfile=]
```

Le definizioni dei parametri sono:

localonly Indica se il firewall può essere gestito soltanto da una macchina locale. I valori validi sono yes o no.

encryption Indica se il server di configurazione prevede che i dati in arrivo vengano crittografati tramite ssl. I valori validi sono none o ssl.

sslfile Indica il nome del file di chiavi ssl da utilizzare per la crittografia ssl. Consultare il Capitolo 6, “Utilizzo del programma di utilità MKKF (Make Key File)” a pagina 59.

DNS (Domain Name Service)

Il DNS (Domain Name Service) fornisce un servizio del nome dominio completo agli host interni alla rete sicura fornendo contemporaneamente informazioni minime agli host esterni alla rete sicura. Per ottenere tale scopo sono necessari tre server nomi dominio:

- uno sul firewall
- uno all'interno della rete sicura
- uno all'esterno della rete sicura

Per ulteriori informazioni, consultare *IBM eNetwork Firewall - Guida per l'utente*.

Nota:

1. x.x.x.x indica un indirizzo IP in formato decimale con punti.
2. Il valore per i parametri secaddr e remaddr può essere un singolo indirizzo IP o un elenco di indirizzi IP. Se viene specificato un elenco di indirizzi IP, questo deve essere delimitato da spazi e racchiuso tra virgolette.
3. Gli indirizzi duplicati vengono rilevati e contrassegnati come errori.
4. La prima volta che viene configurato il DNS, `fwdns cmd=change` crea il nuovo file. Il firewall ha sempre un solo record di configurazione DNS. È possibile che i valori non risultino specificati. Il sottocomando change è sufficiente per modificare uno o tutti i valori nel record DNS.

Il seguente comando elenca la configurazione corrente del DNS.

```
fwdns cmd=list
```

Per modificare l'entrata della configurazione del DNS e creare un file nuovo:

```
fwdns cmd=change
    secdomain=SecureDomainName
    secaddr=x.x.x.x ‘ "x.x.x.x  x.x.x.x  x.x.x.x"
    remaddr=x.x.x.x ‘ "x.x.x.x  x.x.x.x  x.x.x.x"
```

Le definizioni dei parametri sono:

secdomain=*NomeDominioSicuro* Il nome dominio della rete interna sicura

secaddr=*IndDNSSicuro[,...]* L'indirizzo IP dei server nomi dominio

remaddr=*IndDNSNonSicuro[,...]* Gli indirizzi IP dei server nomi dominio esterni alla rete sicura ricevuti dal fornitore dei servizi del collegamento ad Internet.

Filtri

Utilizzare il comando `fwfilter` per attivare e disattivare le regole di filtro.

```
fwfilter cmd=update ‘ verify ‘ list ‘ shutdown ‘ startlog ‘
stoplog
```

Le definizioni dei parametri sono i seguenti:

fwfilter cmd=update ricrea la configurazione ed attiva l'insieme di regole.

fwfilter cmd=verify esegue una "creazione di prova" per la configurazione ma non attiva le modifiche.

fwfilter cmd=list elenca l'ultima configurazione creata

fwfilter cmd=shutdown disattiva il meccanismo dei filtri

fwfilter cmd=startlog registra il traffico selezionato nella funzione `log firewall`

fwfilter cmd=stoplog arresta il log dei filtri del firewall

Proxy HTTP

Il proxy HTTP gestisce in modo efficiente le richieste del browser tramite IBM Firewall permettendo così di fare a meno di un server Socks per la visualizzazione del Web. Gli utenti possono accedere ad informazioni utili su Internet senza compromettere la sicurezza delle loro reti interne e senza modificare il loro ambiente client per implementare il proxy HTTP.

Il comando `fwhttp` elenca o modifica la configurazione del proxy HTTP corrente.

Per elencare la configurazione del proxy HTTP corrente, utilizzare il seguente comando.

```
fwhttp cmd=list
```

Per modificare la configurazione del proxy HTTP corrente, utilizzare il seguente comando.

```
fwhttp cmd=change
       [port=]
       [maxcontentlengthbuffer=]
        [minactivethreads=]
        [maxactivethreads=]
        [idlethreadtimeout=]
        [logging=]
        [authenticate=]
        [authenticatetimeout=]
        [maxpersistrequests=]
        [persisttimeout=]
```

Le definizioni dei parametri sono:

port La porta su cui il servizio proxy http è in ascolto.

maxcontentlengthbuffer L'ampiezza massima di un buffer per la restituzione dei documenti e di un'intestazione aggiuntiva relativa alla lunghezza del contenuto.

minactivethreads Il numero minimo di thread attivi da avviare al momento dell'inizializzazione e da conservare in fase di esecuzione.

maxactivethreads Il numero massimo di thread attivi che possono essere eseguiti in qualsiasi momento.

idlethreadtimeout Il periodo di tempo per conservare i thread inattivi disponibili.

logging Indica se si desidera eseguire il log per le attività HTTP. I valori validi sono on e off.

authenticate Il livello degli utenti da autenticare. I valori validi sono all, none o new.

authenticatetimeout Il periodo di tempo entro il quale attendere una richiesta client dopo aver stabilito un collegamento permanente.

maxpersistrequests Il numero massimo di richieste da ricevere su un collegamento permanente.

persisttimeout Il periodo di tempo per conservare un collegamento permanente.

Interfacce

Le interfacce sicure collegano l'host IBM Firewall alla rete di host della rete interna, vale a dire la rete che si desidera proteggere. **Il funzionamento del firewall richiede almeno un'interfaccia sicura.** Le interfacce non sicure collegano IBM Firewall ad una o più reti esterne oppure ad Internet. IBM Firewall deve avere almeno un'interfaccia non sicura.

Questo comando elenca le interfacce di rete del firewall. Per poter eseguire questo comando, un responsabile deve essere autorizzato a gestire le funzioni delle interfacce.

```
fwinterface cmd=list
                    [addr=x.x.x.x]
```

Per ulteriori informazioni sull'autorizzazione del responsabile, consultare *IBM eNetwork Firewall - Guida per l'utente*.

Le definizioni dei parametri sono:

addr=x.x.x.x Elenca tutte le interfacce di rete che sono state configurate sul firewall e le identifica come interfacce sicure o non sicure. Anche un nome può essere identificato. Se viene specificato il parametro facoltativo `addr`, viene elencata soltanto l'interfaccia correlata. Se viene fornito un indirizzo IP decimale con punti per `addr`, l'elenco conterrà l'indirizzo, lo stato ed il nome solo dell'indirizzo specificato, presumendo che sia stato configurato sul firewall.

Questo comando consente di definire le interfacce di rete sul firewall. Per poter eseguire questo comando, un responsabile deve essere autorizzato a gestire le funzioni delle interfacce.

```
fwinterface cmd=change
            addr=x.x.x.x
            [state={secure|nonsecure}]
            [name=]
```

Le definizioni dei parametri sono:

addr=x.x.x.x Contiene l'indirizzo decimale con punti dell'interfaccia da modificare. Se l'interfaccia non è definita sul firewall, viene restituito un errore.

state={secure|nonsecure} Contiene una delle due parole chiave "secure" o "nonsecure" che identificano la rete collegata all'interfaccia specificata.

name È un nome valido che identifica l'interfaccia o la rete a cui è collegato. Gli spazi sono consentiti, se correttamente racchiusi tra doppi apici.

Sebbene entrambi i parametri sono facoltativi, occorre specificarne almeno uno.

Programma di archiviazione dei log

Il seguente comando richiama il programma di archiviazione dei file di log per conservare le funzioni di log configurate per l'archiviazione.

```
fwlogmgmt -1 o fwlogmgmt -a
```

È utile inserire questo comando in un servizio pianificato Windows NT. Per ulteriori informazioni, consultare *IBM eNetwork Firewall - Guida per l'utente*.

Gestione dei file di log

La gestione dei file di log consente di definire e gestire i file di log e di archivio. Il comando fwlog aggiunge, modifica ed elimina le funzioni di log.

Per aggiungere le funzioni di log, immettere il seguente comando.

```
fwlog cmd=add
      facility=Facility
      priority=Priority
      logfile=LogFileName
       [arcfile=ArchivePath
      logtime=DaysToKeepInLog
      arctime=DaysToKeepInArchive
```

I valori validi per **facility**:

- firewall (local4) - log generale del firewall compreso il log di filtro
- alert (local1) - lo stato del daemon di controllo log e le avvertenze delle violazioni di soglia forniti nella Visualizzazione Avvisi
- adminaudit (local0) - log del controllo di gestione
- mail - log di posta

I valori validi per **priority**:

- debug
- informazione
- avvertenza
- errore
- condizione critica

Il parametro logfile indica dove inviare le entrate di log del firewall. Il valore valido per logfile è un nome completo (con il formato drive:\directory) che indica il file in cui scrivere le entrate di log.

Nota: I file identificati per le funzioni `log avvisi` o `log firewall` devono essere differenti da quelli delle altre funzioni di log, se utilizzate per elaborare questi file.

È importante che vengano visualizzati SOLTANTO i messaggi di log del firewall nei file dei programmi di utilità per i prospetti. Nessun'altra funzione deve essere indirizzata allo stesso file del log avvisi o log firewall.

I parametri arcfile, logtime e arctime sono facoltativi e sono validi solo quando il parametro logfile specifica un nome file. Se viene specificato uno di questi parametri, occorre specificare anche gli altri. Questi parametri controllano l'archiviazione dei log. Per eseguire l'archiviazione, immettere il comando `fwlogmgmt` periodicamente. Consultare “Programma di archiviazione dei log” a pagina 5.

Per impostazione assunta, il firewall utilizza questi parametri per indicare dove memorizzare i record del log di archivio e la frequenza con cui eseguire la funzione di archiviazione. È necessario specificare questi tre parametri per abilitare l'archiviazione.

La funzione di archiviazione può essere modificata scrivendo un plugin di archiviazione del firewall. Consultare Capitolo 4, “Kit di sviluppo software del plugin Log Archiver” a pagina 47.

Il parametro **arcfile** deve contenere un nome percorso completo.

Il parametro **logtime** indica il numero minimo di giorni per cui un'entrata di log del firewall resta nel file di log prima di essere spostata nel file di archivio.

Il parametro **arctime** indica il numero minimo di giorni per cui un record di log del firewall resta nel file di archivio prima che venga eliminato.

Per modificare le funzioni di log, immettere il seguente comando.

```
fwlog cmd=change
        index=Index
        [facility=Facility]
        [priority=Priority]
        [logfile=LogFileName]
        [arcfile=ArchiveFileName]
        [logtime=DaysToKeepInLog]
        [arctime=DaysToKeepInArchive]
```

Se una modifica, specialmente alla prima ricorrenza, non riesce a creare un file di configurazione corretto nella sintassi (ad esempio, la definizione del file di log creato ha campi mancanti), viene emesso un messaggio di avvertenza ed il firewall non esegue il log dei dati.

Per eseguire il log ma non l'archiviazione, vengono richiesti solo i parametri **facility**, **priority** e **logfile**. Per disabilitare l'archiviazione dei log una volta avviata, eliminare i parametri **archive**, **logtime** e **arctime**. Se è stato pianificato un lavoro di archiviazione, annullarlo.

Per elencare i dati di configurazione correnti del file di log, immettere il seguente comando.

```
fwlog cmd=list
```

Per eliminare l'entrata di log del firewall specificata dal numero di indice restituito per l'entrata sul comando fwlog cmd=list, immettere il seguente comando.

```
fwlog cmd=delete
      index=index of entry to delete
```

Controllo log

Utilizzare questo comando per indicare quando e come il controllo log attiva gli avvisi. Gli avvisi si verificano quando vengono raggiunti i valori di soglia specificati in questo comando (o nel pannello del client di configurazione corrispondente) in un intervallo di tempo specificato. Quando si verifica un avviso:

1. Viene scritto un record nella funzione avvisi del firewall ed in quella di log del firewall
2. Viene eseguito un comando specificato
3. Viene inviata una notifica ad uno o più ID utente
4. Viene inviato un messaggio ad un cercapersone

Le ultime tre azioni sono controllate dalla configurazione dei valori specificata in questo punto.

Elenco delle impostazioni del controllo log

```
fwlogmon cmd=list
```

Specifica degli ID utente che devono ricevere le notifiche di posta quando si verifica un avviso

Per specificare gli ID utente che devono ricevere le notifiche di posta quando si verifica un avviso (la notifica viene inviata ad ogni ID aggiunto):

```
fwlogmon cmd=add‘delete
         type=id
         username=
         [comment=]
```

Specifica di un comando da eseguire quando si verifica un avviso

```
fwlogmon cmd=add‘change
         type=command
         command=
         [comment=]

fwlogmon cmd=delete
         type=command
```

Specifica di una soglia raggiunta la quale deve essere attivato un avviso in base al numero di tentativi di login non riusciti

```
fwlogmon cmd=add
         type=single‘multi‘host
         count=
         time=
         pager=
         [comment=]

fwlogmon cmd=change
         type=single‘multi‘host
         [count=]
         [time=]
         [pager=]
         [comment=]

fwlogmon cmd=delete
         type=single‘multi‘host
```

Specifica di una soglia raggiunta la quale deve essere attivato un avviso in base al numero di ricorrenze di uno specifico ID di messaggio del firewall

```
fwlogmon cmd=add
         type=msg
         tag=
         count=
         time=
         pager=
         [comment=]

fwlogmon cmd=change
         type=msg
         tag=
         [count=]
         [time=]
         [pager=]
         [comment=]
```

```
fwlogmon cmd=delete
         type=msg
         tag=
```

Le definizioni dei parametri sono:

type Identifica le caratteristiche del comando di controllo log che vengono aggiunte o modificate.

I valori validi sono id, command, msg, single, multi e host.

id Indica l'ID utente a cui inviare gli avvisi.

command Specifica un comando da eseguire.

msg Indica il controllo di un messaggio di log specifico.

single Indica il controllo in base a singoli id utente. Viene tenuto un conteggio di ogni ID per cui si è verificato un tentativo non riuscito. Se il conteggio di un qualsiasi ID raggiunge il valore di soglia specificato in questo comando, viene attivato un avviso.

multi Indica il controllo in base a più id utente. Se il totale dei conteggi di tutti gli ID utente per i quali sono stati eseguiti tentativi non riusciti raggiunge il valore di soglia specificato in questo comando, viene attivato un avviso.

host Indica il controllo in base ai nomi host. Viene tenuto un conteggio di ogni nome per cui si è verificato un tentativo non riuscito. Se il conteggio di un qualsiasi nome raggiunge il valore di soglia specificato in questo comando, viene attivato un avviso.

username L'ID posta di un responsabile del firewall o di un altro utente a cui notificare un avviso. Le notifiche degli avvisi vengono inviate con esito positivo solo se il server di posta del sito sicuro è stato configurato correttamente.

command Il nome del comando da eseguire quando si verifica un avviso. Deve essere il nome di percorso completo di un file eseguibile. Può essere un file .bat, che consente l'esecuzione di più comandi dall'interno del file, tuttavia se il file .bat fa riferimento ad altri file, devono essere specificati anche i nomi di percorso completo di questi file.

count Imposta la soglia per il numero di errori o per le ricorrenze di un particolare messaggio di log, raggiunta la quale viene attivato un avviso.

time Imposta l'intervallo di tempo in minuti. Perché venga attivato un evento, il conteggio deve essere raggiunto entro questo intervallo di tempo a partire dalla prima ricorrenza. Le ricorrenze precedenti a questo intervallo vengono eliminate dal conteggio prima dell'ora corrente.

pager Specifica se utilizzare o meno un cercapersone, quando la soglia associata attiva un avviso. La configurazione del cercapersone attivo viene utilizzata per inviare la chiamata.

tag Una tag di messaggio del log (con il prefisso ICA) da controllare. I messaggi del controllo log (tag ICA inferiori a 1000) non possono essere controllati.

Gestione della posta

Utilizzare il comando `fwmail` per mappare i domini di posta sicuri.

```
fwmail cmd=list

fwmail cmd=add
        secdomain=
        mail=
        remdomain=

fwmail cmd=change
        secdomain=
        [mail=]
        [remdomain=]

fwmail cmd=delete
        secdomain=
```

Le definizioni dei parametri sono:

secdomain Il nome con cui il dominio di posta che viene descritto è noto agli utenti della parte sicura del firewall.

mail Indirizzo del server di posta.

remdomain Il nome con cui il dominio di posta che viene descritto è noto agli utenti della parte non sicura del firewall.

NAT (Network Address Translation)

Il programma di conversione degli indirizzi di rete (NAT, Network Address Translation), rappresenta una soluzione al problema dell'esaurimento degli indirizzi IP, in quanto consente il riutilizzo degli indirizzi interni alla rete IP sicura da parte di qualsiasi altra rete IP.

NAT supporta quattro tipi di configurazione:

- Indirizzo registrato di tipo Unificare - La conversione di tipo Unificare comporta la conversione dell'indirizzo sicuro e del numero di porta di un pacchetto in modo che diversi indirizzi interni (fino a 65536) possano condividere un unico indirizzo IP registrato. L'indirizzo IP registrato condiviso univoco nasconderà gli indirizzi locali, ma, oltre ad esso, sarà necessario un altro indirizzo Internet registrato unicamente per il Firewall.
- indirizzi IP sicuri di tipo Convertire - Un indirizzo IP sicuro di tipo Convertire definisce una serie di indirizzi di rete sicuri che richiedono NAT per eseguire la conversione degli indirizzi IP. Per impostazione assunta, NAT esegue la conversione degli indirizzi su tutti gli indirizzi IP sicuri.
- Indirizzi IP sicuri di tipo Escludere - Un indirizzo IP sicuro di tipo Escludere definisce una serie di indirizzi di rete sicuri che non richiedono NAT per eseguire la conversione degli indirizzi IP. Per impostazione assunta, NAT esegue la conversione degli indirizzi su tutti gli indirizzi IP sicuri, a meno che l'indirizzo non sia compreso nell'intervallo specificato da un'entrata di indirizzi IP sicuri di tipo Escludere.
- Indirizzo IP sicuro di tipo Mappare - Un indirizzo IP sicuro di tipo Mappare definisce una mappatura uno-a-uno da un indirizzo IP sicuro ad un indirizzo IP

registrato. Questa mappatura uno-a-uno di indirizzi IP consente ai client di applicazioni esterne, quali FTP o Telnet, di impostare delle sessioni TCP con le macchine server appartenenti alla rete sicura.

La sintassi del comando NAT è la seguente:

```
fwnat cmd=list | update | verify |shutdown | startlog | stoplog
```

Le definizioni dei parametri sono:

fwnat cmd=list Elenca la configurazione NAT corrente

fwnat cmd=update Aggiorna il processo NAT

fwnat cmd=verify Controlla la sintassi della configurazione

fwnat cmd=shutdown Arresta la conversione di tutti gli indirizzi

fwnat cmd=startlog Avvia il log dei pacchetti convertiti

fwnat cmd=stoplog Arresta il log dei pacchetti convertiti

Per aggiungere l'entrata Unificare nella configurazione NAT, utilizzare **type=many-to-one**:

```
fwnat cmd=add
        type=many-to-one
        addr=Addr
        [timeout=minutes]
```

Le definizioni dei parametri sono:

type=many-to-one Aggiunge un'entrata `Unificare`

addr=*Addr* L'indirizzo IP che identifica un intervallo di indirizzi IP registrati aggiunti al gruppo di indirizzi registrati

timeout=*minutes* Il numero di minuti per cui una conversione di indirizzo può restare inattiva prima che NAT possa liberare l'indirizzo IP registrato. Il valore assunto è 15 e l'intervallo è 5–45.

Per modificare un'entrata Unificare nella configurazione NAT utilizzare la seguente sintassi:

```
fwnat cmd=change
      index=
        [addr=Addr]
        [timeout=minutes]
```

Le definizioni dei parametri sono:

index Quando viene eseguito `fwnat cmd=list`, sono presenti dei numeri nella colonna a sinistra per entrate NAT specifiche. Utilizzare il numero dell'entrata NAT specifica per il parametro index.

addr=*Addr* L'indirizzo IP che identifica un intervallo di indirizzi IP registrati aggiunti al gruppo di indirizzi registrati

timeout=*minutes* il numero di minuti per cui una conversione di indirizzo può restare inattiva prima che NAT possa liberare l'indirizzo IP registrato. Il valore assunto è 15 e l'intervallo è 5–45.

Per aggiungere un'entrata Convertire al file di configurazione NAT, utilizzare **type=translate**; per eliminare un'entrata dallo stesso file, immettere **type=exclude**:

```
fwnat cmd=add
        type={translate‘exclude}
        addr=Addr
        mask=Mask
```

Le definizioni dei parametri sono:

type=translate Aggiunge un'entrata `Convertire`

type=exclude Aggiunge un'entrata `Escludere`

addr=*Addr* L'indirizzo IP che identifica un intervallo di indirizzi IP sicuri che richiedono la conversione

mask=*Mask* Identifica un intervallo di indirizzi IP

Per modificare un'entrata Convertire o Escludere nel file di configurazione NAT utilizzare la seguente sintassi:

```
fwnat cmd=change
      index=
        [addr=Addr]
        [mask=Mask]
```

Le definizioni dei parametri sono:

index Quando viene eseguito `fwnat cmd=list`, sono presenti dei numeri nella colonna a sinistra per entrate NAT specifiche. Utilizzare il numero dell'entrata NAT specifica per il parametro index.

addr=*Addr* L'indirizzo IP che identifica un intervallo di indirizzi IP sicuri che richiedono la conversione

mask=*Mask* Identifica un intervallo di indirizzi IP

Per aggiungere l'entrata Mappare alla configurazione NAT utilizzare **type=map**:

```
fwnat cmd=add
      type=map
      secaddr=SecureAddr]
      remaddr=RegisteredAddr]
```

Le definizioni dei parametri sono:

type=map Aggiunge un'entrata `Mappare`

secaddr L'indirizzo IP che deve essere convertito in uno specifico indirizzo IP registrato

remaddr L'indirizzo registrato in cui deve essere convertito l'indirizzo sicuro specificato

Per modificare un'entrata Mappare nel file di configurazione NAT utilizzare la seguente sintassi:

```
fwnat cmd=change
      index=
      [secaddr=SecureAddr]
      [remaddr=RegisteredAddr]
```

Le definizioni dei parametri sono:

index Quando viene eseguito `fwnat cmd=list`, sono presenti dei numeri nella colonna a sinistra per entrate NAT specifiche. Utilizzare il numero dell'entrata NAT specifica per il parametro index.

secaddr L'indirizzo IP che deve essere convertito in uno specifico indirizzo IP registrato

remaddr L'indirizzo registrato in cui deve essere convertito l'indirizzo sicuro specificato

Cercapersone

È possibile attivare il supporto di notifica del cercapersone in modo che il firewall possa contattare un responsabile di sistema inviandogli un segnale sonoro nel caso di minacce alla sicurezza del firewall. Per questo motivo, occorre configurare il cercapersone, la portante ed un modem utilizzando i comandi `fwpgr`, `fwcarrier` e `fwmodem`.

Configurazione del cercapersone

Il comando `fwpgr` imposta i parametri per il cercapersone attivo a cui il firewall invia i segnali.

Per elencare un cercapersone, immettere il seguente comando.

```
fwpgr cmd=list
```

Per aggiungere un cercapersone, immettere il seguente comando.

```
fwpgr cmd=add
        carrier=
        modem=
        pagerid=
        message=
```

Per modificare i parametri del cercapersone, immettere il seguente comando.

```
fwpgr cmd=change
        [carrier=]
        [modem=]
        [pagerid=]
        [message=]
```

Le definizioni dei parametri sono:

carrier Un nome per il servizio della portante, come definito nel database delle portanti (comando `fwcarrier`).

modem Un nome per il modem, come definito nel database dei modem (comando `fwmodem`).

pagerid Il numero o il nome di identificazione univoco del cercapersone assegnato dalla portante.

message Il messaggio da inviare e visualizzare sul cercapersone. Può essere un numero o un testo, a seconda del servizio fornito dalla portante. Il messaggio verrà troncato se eccede l'impostazione di lunghezza minima per la portante o 200 caratteri.

Portante

Utilizzare il comando `fwcarrier` per impostare i parametri dei cercapersone utilizzati.

Per elencare una portante, immettere il seguente comando.

```
fwcarrier cmd=list
        carrier=
```

Per aggiungere una portante, immettere il seguente comando.

```
fwcarrier cmd=add
        carrier=
          dial=
          method=
          [password=]
          length=
        baud=
        parity=
        databits=
        stopbits=
```

Per modificare i parametri della portante, immettere il seguente comando.

```
fwcarrier cmd=change
        carrier=
          [dial=]
          [method=]
          [password]
          [length=]
          [baud]
        [parity=]
        [databits=]
        [stopbits=]
```

Per eliminare una portante, immettere il seguente comando.

```
fwcarrier cmd=delete
        carrier=
```

Le definizioni dei parametri sono:

carrier Il nome della portante.

dial Specificare il numero di telefono del modem della portante per il servizio TAP prescelto.

method Il valore deve essere TAP.

password È facoltativo, a meno che non sia necessario per il servizio della portante.

length La lunghezza massima del messaggio consentita dal servizio della portante.

baud Specificare la velocità in baud più affidabile del servizio della portante.

parity Il tipo di controllo di parità supportato dal servizio della portante. In genere, è 'pari' per il protocollo TAP.

databits Il numero di bit di dati supportato dal servizio della portante. Di solito è 7 per il protocollo TAP.

stopbits Il numero di bit di stop supportato dal servizio della portante. Di solito è 1 per il protocollo TAP.

Configurazione del modem

Per impostare il supporto di notifica del cercapersone, è necessario configurare il modem.

Utilizzare il comando modem se di desidera configurare un modem per inviare le richieste del cercapersone alla portante.

Per elencare un modem, immettere il seguente comando.

```
fwmodem cmd=list
        modem=
```

Per aggiungere un modem, immettere il seguente comando.

```
fwmodem cmd=add
        modem=
        comport=
        initsting=
        outsideline=
```

Per modificare i parametri del modem, immettere il seguente comando.

```
fwmodem cmd=change
        modem=
        [comport=]
        [initstring=]
        [outsideline=]
```

Per eliminare un modem, immettere il seguente comando.

```
fwmodem cmd=delete
        modem=
```

Le definizioni dei parametri sono:

modem Un nome per il modem.

comport La porta COM seriale a cui viene collegato il modem. Il modem su questa porta seriale COM deve essere definito per il sistema Windows NT.

initstring La stringa di inizializzazione per il modem. I parametri nella stringa devono essere validi per il comando del modem AT, ma AT non deve essere incluso nella stringa. I parametri specificati devono essere coordinati con i requisiti di comunicazione del modem della portante.

outsideline Il numero da comporre per ottenere la linea esterna.

Verifica della configurazione del cercapersone

Per assicurarsi di aver configurato in modo corretto il cercapersone attivo, utilizzare il seguente comando.

```
pager
        carrier=
        modem=
    ID=
    msg=
```

Le definizioni dei parametri sono identiche a quelle del comando `fwpgr`.

Vari cercapersone

Se si desidera modificare regolarmente il cercapersone attivo, attenersi alla seguente procedura:

- Assicurarsi di aver definito tutte le portanti ed i modem necessari
- Utilizzare `fwpgr` o il client di configurazione per definire e salvare una configurazione del cercapersone
- Copiare il file `ROOTDIR\config\pager.cfg` ed attribuirgli un nome riconoscibile
- Definire un'altra configurazione del cercapersone e copiarla, continuare così finché non vengono copiati tutti i file pager.cfg necessari
- Ricopiare il file di configurazione che si desidera attivare in `ROOTDIR\config\pager.cfg`

Se vengono eseguite più modifiche, impostare un lavoro pianificato utilizzando il comando `at` di Windows NT in modo da ripetere automaticamente l'ultima sequenza all'inizio di ogni modifica.

Utenti

Questo comando aggiunge un nuovo utente oppure modifica uno o più attributi di un utente del firewall già esistente. Tutti i parametri hanno valori assunti o non sono necessari in determinate circostanze. Per `cmd=add`, i valori assunti vengono memorizzati; per `cmd=change`, i valori esistenti vengono conservati.

```
fwuser cmd={add|change}
username=LoginName
[fullname="UsersRealName"]
[password={yes|no}]
[pwdvalue=Password]
[level={proxy|admin}]
       [secftp=SecureFTPauthentication]
       [remftp=NonSecureFTPauthentication]
       [secauth=SecureTelnetAuthentication]
[remauth=NonSecureTelnetAuthentication]
       [secadmin=SecureAdminAuthentication]
[remadmin=NonSecureAdminAuthentication]
       [secsocks=SecureSocks]
       [remsocks=NonSecureSocks]
       [sechttp=SecureHTTP]
[key="SecureNet Key Code"]
[histexpire=HistoryExpiration]
[histsize=HistorySize]
[loginretries=LoginRetries]
[maxage=MaxAge]
[maxexpired=MaxExpiredAge]
[maxrepeats=MaxRepeatChars]
[minalpha=MinAlphaChars]
[mindiff=MinDifferentChars]
[minlen=MinLength]
[minother=MinNonAlphaChars]
[pwdwarntime=PasswordWarnTime]
       [userchng={yes|no}]
       [pwlocked={yes‘no}]
[fg_all={yes|no}]
[fg_dns={yes|no}]
[fg_interfaces={yes|no}]
[fg_logmonitor={yes|no}]
[fg_logs={yes|no}]
[fg_mail={yes|no}]
[fg_netobjs1={yes|no}]
[fg_netobjs2={yes|no}]
[fg_pagers={yes|no}]
[fg_proxyserver={yes|no}]
[fg_user={yes|no}]
[fg_traffic={yes|no}]
```

Parametri fondamentali

username Nome di login per questo utente.

fullname Il nome completo dell'utente o qualche altra breve informazione (una riga) relativa a questo utente. Se contiene degli spazi, il valore deve essere racchiuso tra virgolette.

level Il valore assunto è proxy ed indica che l'utente creato è un utente proxy semplice o un utente Socks. Le autenticazioni di gestione ed i gruppi con funzione di gestione non vengono applicati agli utenti proxy.

key La chiave utilizzata per autenticare la scheda Digital Pathways' SecureNet Key dell'utente. Se il valore contiene degli spazi, racchiuderlo tra virgolette.

Autenticazioni

Di seguito sono riportati i metodi di autenticazione e le corrispondenti stringhe di autenticazione. L'utilizzo delle stringhe di autenticazione per i vari parametri del

Authentication Methods), SNK non funzionerà perché il protocollo Parola d'ordine/ID utente Socks5 non può visualizzare la domanda SNK.

L'impostazione assunta è deny.

sechttp Il metodo di autenticazione per le richieste HTTP da un'interfaccia sicura. I valori validi sono deny, permit, password, NT, sdi, user, userauth2 e userauth3.

SNK non è supportato dal protocollo HTTP perché non fornisce alcuna modalità di visualizzazione della domanda SNK all'utente. SDI è supportato ma all'utente verrà richiesta una parola d'ordine invece di un codice di accesso SDI. L'utente deve immettere il codice di accesso SDI personale.

Nota: Per `fwdfuser` non è possibile impostare SNK o la parola d'ordine del firewall in nessuno dei suoi campi relativi al metodo di autenticazione.

Parametri della parola d'ordine del firewall

password Indica se all'utente viene richiesta una parola d'ordine. Per impostazione assunta, la parola d'ordine viene richiesta se non è stato specificato alcun metodo di autenticazione o se non è consentita come valore assunto.

pwdvalue Utilizzato soprattutto per la programmazione degli script, pwdvalue consente che il valore di un parametro possa essere specificato sulla riga comandi. Questo valore viene immesso in testo visibile non codificato ed è pertanto leggibile da eventuali intrusi. Nessun valore assunto.

userchng Determina come viene impostato l'indicatore di modifica responsabile nel database utente. Il valore yes imposta l'indicatore di modifica responsabile che richiede all'utente di modificare la propria parola d'ordine la prima volta che effettua il collegamento. No è il valore assunto. Questo parametro è valido solo se sono supportati i parametri password=yes e pwdvalue=''.

pwlocked Indica se la parola d'ordine è stata bloccata. Yes indica che il numero massimo di tentativi di login è stato superato e che la parola d'ordine non è stata utilizzata, una volta trascorso il numero di settimane specificato dal periodo di tempo massimo prima del blocco.

histexpire Definisce il periodo di tempo (in settimane), trascorso il quale un utente non può riutilizzare una parola d'ordine. Il valore è una stringa di numeri interi. I valori validi sono compresi tra 0 e 52. Il valore 0 indica che non è stato impostato alcun limite di tempo. Il valore assunto è 0.

histsize Definisce il numero di parole d'ordine precedenti che un utente non può riutilizzare. Il valore è una stringa di numeri interi. I valori validi sono compresi tra 0 e 20. Valido solo se viene specificato `histexpire=0`. Il valore assunto è 5.

loginretries Definisce il numero di tentativi di login non riusciti consentiti a partire dall'ultimo tentativo riuscito prima che il sistema blocchi il codice di contabilizzazione. Il valore è una stringa di numeri interi. I valori validi sono compresi tra 0 e 20. Il valore assunto è 10. Uno zero o un valore negativo indica che non esiste alcun limite. Una volta bloccato il codice

di contabilizzazione, l'utente non può più eseguire il login finché il responsabile di sistema non reimposta `pwlocked` su no.

maxage Definisce il periodo massimo di validità (in settimane) di una parola d'ordine. La parola d'ordine deve essere modificata entro questo periodo. Il valore è una stringa di numeri interi. I valori validi sono compresi tra 0 e 52. Il valore 0 indica che non è stato impostato alcun periodo massimo di validità. Il valore assunto è 13.

maxexpired Definisce il periodo di tempo massimo (in settimane), oltre al valore maxage, entro il quale un utente può modificare una parola d'ordine scaduta. Trascorso questo periodo, soltanto il responsabile può modificare la parola d'ordine. Il valore è una stringa di numeri interi. I valori validi sono compresi tra -1 e 26. Se l'attributo maxexpired è 0, la parola d'ordine scade quando viene raggiunto il valore maxage. Se l'attributo maxage è 0, maxexpired viene ignorato. Il valore assunto è 3.

maxrepeats Definisce il numero massimo di volte in cui è possibile ripetere un carattere della nuova parola d'ordine. I valori validi sono compresi tra 0 e 8, ma il valore 0 non è indicativo di nulla. Il valore 8 indica che non esiste un numero massimo. Il valore assunto è 2.

minalpha Definisce il numero minimo di caratteri alfabetici che devono essere specificati per una nuova parola d'ordine. Il valore è una stringa di numeri interi. I valori validi sono compresi tra 0 e 8. Il valore 0 indica che non è specificato alcun numero minimo. Il valore assunto è 4.

mindiff Definisce il numero minimo di caratteri alfabetici richiesti in una nuova parola d'ordine e non presenti in quella vecchia. Il valore è una stringa di numeri interi. I valori validi sono compresi tra 0 e 8. Il valore 0 indica che non è specificato alcun numero minimo. Il valore assunto è 3.

minlen Definisce la lunghezza minima di una parola d'ordine. Il valore è una stringa di numeri interi. I valori validi sono compresi tra 0 e 8. Il valore 0 indica che non è specificato alcun numero minimo. Il valore assunto è 8.

minother Definisce il numero minimo di caratteri non alfabetici che devono essere specificati per una nuova parola d'ordine. Il valore è una stringa di numeri interi. I valori validi sono compresi tra 0 e 8. Il valore 0 indica che non è specificato alcun numero minimo. Il valore assunto è 1.

pwdwarntime Definisce il numero di giorni prima che il sistema emetta un messaggio di avvertenza con il quale viene richiesta la modifica della parola d'ordine. Il valore è una stringa di numeri interi. I valori validi sono compresi tra 0 e 30. Uno zero o un valore negativo indica che non viene emesso alcun messaggio. Il valore assunto è 5.

Gruppi funzionali di gestione

fg_all Immettere yes se al responsabile è consentito gestire tutti gli aspetti del firewall. Il valore assunto è no.

fg_dns Immettere yes se al responsabile è consentito gestire il DNS (Domain Name Service). Il valore assunto è no.

fg_interfaces Immettere yes se al responsabile è consentito definire le interfacce del firewall. Il valore assunto è no.

fg_logmonitor Immettere yes se al responsabile è consentito gestire le soglie del controllo log. Il valore assunto è no.

fg_logs Immettere yes se al responsabile è consentito gestire le funzioni di log. Il valore assunto è no.

fg_mail Immettere yes se al responsabile è consentito gestire il gateway di posta del firewall. Il valore assunto è no.

fg_netobjs1 Immettere yes se al responsabile è consentito eseguire la gestione di base degli oggetti di rete. Il valore assunto è no.

fg_netobjs2 Immettere yes se al responsabile è consentito eseguire la gestione avanzata degli oggetti di rete. Il valore assunto è no.

fg_pagers Immettere yes se al responsabile è consentito gestire l'impostazione cercapersone. Il valore assunto è no.

fg_proxyserver Immettere yes se al responsabile è consentito configurare i daemon proxy del firewall. Il valore assunto è no.

fg_traffic Immettere yes se al responsabile è consentito gestire il controllo del traffico. Il valore assunto è no.

fg_user Immettere yes se al responsabile è consentito gestire gli utenti del firewall. Il valore assunto è no.

Per elencare gli attributi di tutti o di un singolo utente firewall specificato:

```
fwuser cmd=list
       [username=username]
       [type={short|long}]
```

type={short|long} Se viene utilizzato un nome utente, il valore assunto per il tipo è long. Se non viene utilizzato un nome utente, il valore assunto è short.

Per rimuovere un utente dal firewall:

```
fwuser cmd=delete
       username=username
```

Capitolo 2. Utilizzo dei programmi di utilità per i prospetti

Questo capitolo descrive l'utilizzo dei programmi di utilità per i prospetti di IBM Firewall. Lo scopo principale dei programmi di utilità per i prospetti è creare dei file disposti in tabelle contenenti informazioni di gestione dai file di `log firewall`.

I file di testo disposti in tabelle possono essere creati ed importati in un sistema di database, quale DB2/6000 o DB2/2 . Il responsabile può quindi utilizzare SQL (Structured Query Language) per interrogare i dati e generare i prospetti. I programmi di utilità consentono al responsabile di creare un file di testo leggibile dei messaggi di log del firewall.

I programmi di utilità per i prospetti sono costituiti da programmi e file:

fwlogtxt Il programma utilizzato per generare i messaggi di testo completo da un file di log del firewall

fwlogtbl Il programma utilizzato per creare i file di importazione del database, in formato DEL (delimitato) da un log del firewall o da un log su.

Per utilizzare il programma fwlogtbl ed i file DEL, DML e DDL, viene richiesta una conoscenza di base dei database relazionali e dell'utilizzo di un prodotto appropriato del database relazionale.

fwschema.ddl Il file di istruzioni DDL (Data Definition Language) SQL, utilizzato per definire le tabelle del database

fwimport.dat Il file delle istruzioni di importazione DB2, utilizzato per importare i file DEL nelle tabelle del database

fwqrysmp.dml Il file di istruzioni DML (Data Manipulation Language) SQL, utilizzato per generare prospetti di esempio

fwlogcvrt Il programma per convertire il formato log del firewall Windows NT in un formato AIX. Ciò consente ai tool di riferimento di altri fornitori di agire come descritto in precedenza, ad eccezione del fatto che i nuovi messaggi possono non essere riconosciuti.

I file DDL e DML sono specifici per la famiglia DB2, ma possono essere modificati per altri sistemi di gestione del database. I file in formato DEL possono essere facilmente importati (caricati) nel DB2/6000, DB2/2 ed in altri database e sistemi di file. La semplicità del loro formato consente la conversione in altri formati, se necessario.

Utilizzo dei programmi di utilità per i prospetti

Queste informazioni descrivono come utilizzare i programmi di utilità per i prospetti dalla riga comandi. Per ulteriori informazioni sull'utilizzo dei programmi di utilità per i prospetti dal client di configurazione, consultare *IBM eNetwork Firewall - Guida per l'utente*.

Per visualizzare i file di log del firewall dalla riga comandi, utilizzare il programma di utilità **fwlogtxt**. Per ulteriori informazioni, consultare “Creazione dei messaggi dal file di log del firewall” a pagina 25.

Per generare i prospetti in base alle informazioni di log:

1. Installare il prodotto del database relazionale.
2. Creare un database vuoto.
3. Creare tabelle di log del firewall vuote nel database.
4. Per creare dei file disposti in tabelle, eseguire **fwlogtbl** dalla riga comandi.
5. Importare i file risultanti per compilare le tabelle del database con i dati di log.
6. Creare dei prospetti eseguendo le istruzioni o i programmi SQL.

Nota: I primi tre passi vengono eseguiti una sola volta, gli altri passi invece vengono ripetuti ogni volta che sono disponibili nuovi dati di log.

Formato del log di IBM Firewall

Ogni entrata del file di log del firewall ha il seguente formato:

```
Date Time firewall_name:year;pid:Amsg_num; msg_ID;var_1;...;var_n;
```

dove

- i primi tre campi, **date, time, firewall-name** vengono aggiunti dalla funzione di log del firewall.
- **year** indica l'anno a quattro caratteri.
- **pid** è l'ID thread a cui viene applicata l'entrata.
- **Amsg_num** è un numero intero sequenziale che i programmi di utilità per i prospetti utilizzano per accedere al testo appropriato del messaggio convertito dal file fw_log.cat. msg_num è preceduto da una lettera (A) che indica il livello di log. Questo indicatore distingue entrambe le piattaforme che hanno generato il log e le differenze del formato di log.
- **msg_ID** è il numero esterno del messaggio (ad esempio, ICA0001e).
- **var_1-n** rappresenta i valori delle variabili di messaggio, dove **n** è il numero di variabili nella definizione del messaggio.

Nota: Non indirizzare altri record allo stesso file di log del firewall. Tali record non sono conformi al formato richiesto dai programmi di utilità per i prospetti e pertanto possono verificarsi risultati imprevisti.

Utilizzare il comando `fwlogcvrt` per convertire il formato log del rilascio Windows NT in un log AIX. È necessario eseguire questa conversione per utilizzare i tool che supportano IBM Firewall per i log AIX. La conversione elimina l'indicatore di livello log 'A' che precede msg_num ed inserisce due spazi vicino ai due punti tra firewall_name e year.

I parametri includono:

input L'immissione standard reindirizzata da un log del firewall Windows NT.

output L'emissione standard, che può essere reindirizzata ad un file.

Sintassi di fwlogcvrt

```
fwlogcvrt
```

Esempio:

```
fwlogcvrt < fw980212.log >logcvrt.out
```

Creazione dei messaggi dal file di log del firewall

Utilizzare il comando **fwlogtxt** per creare dei messaggi leggibili dalle entrate di un file di log del firewall.

I parametri includono:

input L'immissione standard da un file di log del firewall

output L'emissione standard

Sintassi di fwlogtxt

```
fwlogtxt
```

Esempio:

```
fwlogtxt < fw980212.log >logtxt.out
        fwlogtxt < my.log ‘ find "ICA0"
```

Non sono specificati parametri per fwlogtxt; le informazioni vengono raccolte dall'immissione standard ed i risultati vengono aggiunti all'emissione standard.

Creazione dei file di importazione del database

Utilizzare il comando **fwlogtbl** per creare, sovrascrivere o accodare i file disposti in tabelle che vengono utilizzati dall'utente per compilare le tabelle del database per la creazione dei prospetti.

I parametri includono:

input File di log del firewall

output Nomi file:

a_alert.tbl
f_rule.tbl
f_info.tbl
f_match.tbl
f_stat.tbl
interfaces.tbl
nat_info.tbl
p_info.tbl
p_ftp.tbl
p_http.tbl
p_info.tbl
p_login.tbl
p_stat.tbl
server_info.tbl
session.tbl

s_ftp.tbl
s_info.tbl
ssl_info.tbl

Sintassi di fwlogtbl

```
      fwlogtbl  -w [-d OutDir]  [-su]LogName
                 ‘
-a
```

Esempio:

```
              fwlogtbl -a  -d :c\reports fw961031.log
```

-w Specifica che il file di emissione esistente deve essere sostituito. Se il file non esiste, fwlogtbl lo crea.

-a Specifica che il file creato deve essere accodato al file di emissione esistente. Se il file non esiste, fwlogtbl lo crea.

-d Identifica l'indirizzario di emissione.

OutDir Specifica l'indirizzario in cui memorizzare tutti i file di emissione. Se l'indirizzario non è specificato, i file di emissione vengono memorizzati nell'indirizzario corrente.

-su Specifica che LogName è il nome di un file di log su AIX. Quindi il firewall Windows NT può elaborare i file di log su ed i file di log del firewall dai precedenti firewall AIX.

LogName Specifica un file di log del firewall o un file di log su AIX.

I nomi dei file di emissione sono predefiniti, ma possono essere copiati o ridenominati dopo l'esecuzione di fwlogtbl. I file di emissione hanno il formato del file ASCII delimitato (DEL), senza delimitatori della stringa di caratteri ed utilizzano il punto e virgola (;) come delimitatore di colonna.

Per ulteriori informazioni sui messaggi, consultare l'Appendice A, “Messaggi” a pagina 75 .

Utilizzo del database con i programmi di utilità per i prospetti

Questa sezione descrive i file forniti con il firewall per la creazione del database, l'importazione delle informazioni nel database e l'interrogazione dei prospetti. Se si dispone del DB2, è possibile utilizzare il comando db2 con questi file. È possibile che esistano funzioni simili al db2 in altri programmi di gestione del database. Per poter utilizzare i file con queste funzioni, può essere necessario modificare questi file.

Per eseguire il comando db2, è necessario che il DB2 sia installato e che sia stata definita un'istanza. Consultare la documentazione relativa all'installazione del DB2. Inizialmente, utilizzare il comando Creare database del DB2 per creare un database vuoto (denominarlo 'fwlog'). Per eseguire questa operazione, digitare dalla riga comandi:

```
db2cmd
```

Poi immettere nella finestra risultante dal comando DB2:

```
db2 create database fwlog
```

Quindi, collegarsi al database fwlog:

```
db2 connect to fwlog
```

Le opzioni -vf del comando db2 possono essere utilizzate nel seguente modo:

```
db2 -vf fwschema.ddl > schema.out
                       db2 -vf fwimport.dat > import.out
                       db2 -vf fwqrysmp.dml > report.out
```

Questi passi sono descritti in modo dettagliato nelle sezioni successive. In ciascun caso, l'utente deve controllare attentamente l'emissione standard (reindirizzata ad un file per ogni esempio). Per l'importazione, è anche necessario controllare il file .msg prodotto da ogni singola istruzione di importazione.

Creazione delle tabelle

Il comando **db2 -vf fwschema.ddl > schema.out** crea tutte le tabelle e gli indici necessari. Eseguire questo comando una volta, preferibilmente subito dopo l'installazione del firewall. L'ID utente corrente al momento dell'esecuzione di questo esempio sarà l'ID autore delle tabelle. È possibile che sia necessario utilizzare questo ID come qualificatore del nome tabella (ad esempio, creatorid.tableName) nelle successive istruzioni SQL, a meno che queste non vengano eseguite con l'ID autore. Se non viene utilizzato l'ID autore, è necessario editare i file fwimport.dat e fwqrysmp.dml per posizionare l'ID autore davanti ad ogni nome di tabella.

Il file `ROOTDIR\sample\report\fwschema.ddl`, contiene le istruzioni DDL per creare le tabelle del database necessarie per accettare i record dai file disposti in tabelle creati da **fwlogtbl**. *ROOTDIR* è l'indirizzario selezionato durante il processo di installazione come ubicazione di destinazione per IBM Firewall. Consultare schema.out per verificare la riuscita dell'operazione. Le istruzioni `fwschema.ddl` possono essere utilizzate così come sono o possono essere modificate per gestire vari sistemi di database. Gli utenti non devono modificare i nomi di tabella e di colonna.

Importazione dei dati

Il comando **db2 –vf fwimport.dat > import.out** carica i dati da tutti i file DEL nelle tabelle create dal comando **db2-vf fwschema.ddl**.

Il file `ROOTDIR\sample\report\fwimport.dat` contiene istruzioni di esempio per l'importazione dei dati dai file *.tbl nel database DB2. Come indicato nella sezione “Creazione delle tabelle”, se l'utente delle importazioni non è l'autore delle tabelle, l'ID autore deve essere posizionato davanti ad ogni nome di tabella.

Ogni istruzione di importazione fornisce informazioni all'emissione standard ed al file `tblname.msg`, dove tblname è specifico per ogni istruzione di importazione. L'utente deve controllare i due formati di emissione per determinare se l'importazione è stata eseguita correttamente. Quando vengono eseguite tutte le istruzioni di importazione in questo file con un programma come il DB2, l'utente deve indirizzare l'emissione standard ad un file e controllare tale file ed ogni file .msg. Ciascun comando di importazione genera un singolo file .msg. Inoltre, l'utente deve rieseguire il comando **db2 –vf fwimport.dat > import.out** in qualsiasi momento si desideri riportare un nuovo log nel database.

Durante l'importazione dei file di log di grandi dimensioni, è possibile ricevere dei codici di errore SQL con le descrizioni che indicano una richiesta di memoria o di spazio su disco. Ad esempio, il messaggio può essere `spazio log di transazione` o `spazio memoria riservata insufficiente`. Questi errori richiedono la correzione delle impostazioni dei parametri per il prodotto del database o per il database fwlog. Per ulteriori informazioni, consultare la documentazione relativa al DB2. Un metodo di correzione temporaneo per le impostazioni dei parametri DB2 è quello di suddividere i file disposti in tabelle o file di log di grandi dimensioni in file più piccoli.

Esecuzione delle interrogazioni di esempio

Il comando **db2 -vf fwqrysmp.dml > report.out** esegue le interrogazioni di esempio. Il file `ROOTDIR:\sample\report\fwqrysmp.dml` contiene istruzioni SQL di esempio che possono fornire dati utili per i prospetti, in base ad alcuni requisiti delle interrogazioni. È possibile utilizzare questi esempi per creare dei prospetti personalizzati. Come indicato nella sezione “Creazione delle tabelle” a pagina 27, se l'utente delle importazioni non è l'autore delle tabelle, l'ID autore deve essere posizionato davanti ad ogni nome di tabella.

Quando le interrogazioni vengono eseguite dalla riga comandi, il DB2 assegna lo spazio massimo necessario per ogni colonna di emissione. Ciò può causare delle difficoltà nella lettura di un prospetto. Per ottenere risultati più soddisfacenti, richiedere un numero minore di colonne in ogni interrogazione oppure inserire le istruzioni delle interrogazioni in un programma da cui è possibile controllare meglio la presentazione.

L'interfaccia utente nei programmi di utilità per i prospetti

I programmi di utilità per i prospetti sono installati come parte dell'installazione del firewall. È anche possibile installarli separatamente ed eseguirli su un host non firewall. È possibile utilizzare il client di configurazione o il comando `fwlogtbl` per eseguire i programmi di utilità per i prospetti sul firewall. Su una macchina non firewall, utilizzare la riga comandi.

Tabelle SQL

Questa sezione descrive la struttura delle tabelle SQL.

Ogni messaggio di log del firewall o su AIX è mappato ad una delle seguenti tabelle SQL:

```
ADMIN_ALERT
FILTER_INFO
FILTER_MATCH
FILTER_ACTIVE_RULE
FILTER_STATUS
INTERFACES
NAT_INFO
PAGER_INFO
PROXY_FTP
PROXY_HTTP
PROXY_INFO
PROXY_LOGIN
PROXY_STATUS
SERVER_INFO
SESSION
SOCKS_FTP
SOCKS_INFO
SSL_INFO
SU
TUNNEL_CONTEXT
TUNNEL_POLICY
TUNNEL_STATUS
```

Non modificare i nomi di tabella e di colonna. Tuttavia, è possibile aumentare la dimensione della colonna dei caratteri nel caso in cui alcuni valori vengano troncati.

Indici

Il record di log che rappresenta un particolare evento del firewall deve essere visualizzato soltanto una volta nel database. Se un responsabile importa più volte lo stesso file disposto in tabelle oppure se viene importato un altro file disposto in tabelle appartenente allo stesso file di log, è possibile che il record di log venga visualizzato più volte.

Per evitare questa situazione, il file di esempio delle definizioni del database, fwschema.dll, definisce un indice univoco in ogni tabella utilizzando i seguenti tre campi:

- il nome file del file di log che era l'origine di questo record (LOG_FILE)
- il numero di riga del record in questo file di log (LINE_NUM)
- Il numero di ripetizioni per questa riga, in base al messaggio 'ultimo messaggio ripetuto n volte' (REPEAT_NUM)

Questo indice impedisce di caricare più volte lo stesso numero di righe dallo stesso file denominato. Questa funzione, insieme ad una gestione attenta dei nomi file di log, impedisce che vengano duplicati gli eventi dei log nel database.

Aggiungendo altri indici al database, è possibile migliorare le prestazioni delle interrogazioni più comuni. Per ulteriori informazioni, consultare la documentazione relativa al database.

Descrizione della tabella

Questa sezione mappa i messaggi di log del firewall alle tabelle e colonne ed indica le informazioni che si desidera interrogare per i propri prospetti. Tutti i messaggi mappati ad una particolare tabella sono elencati nella nota alla fine della tabella. I messaggi che forniscono dati per particolari colonne sono elencati nella parte destinata alla descrizione della colonna. Le tabelle contengono messaggi per IBM Firewall per AIX, IBM Firewall per NT e alcuni messaggi comuni per entrambi i firewall.

Per ulteriori informazioni sui messaggi di log del firewall, consultare Appendice A, “Messaggi” a pagina 75.

Nella colonna Tipo di dati, riportata nella seguente descrizione, 'int' indica il tipo di colonna SMALLINT per DB2 e 'long int' il tipo DB2 INTEGER. Il tipo di dati date_time indica DB2 TIMESTAMP. Per data/ora, il valore in microsecondi è sempre "000000".

Se una descrizione è contrassegnata da *richiesto*, indica che deve essere specificato un valore per immettere il record nella tabella.

Le tre colonne per l'indice univoco e la colonna per la ricezione dell'indicatore del livello log sono state omesse da queste descrizioni di tabella, in quanto le loro definizioni sono identiche e di solito non esiste alcun motivo per interrogarle.

Tabella 1 (Pagina 1 di 2). ADMIN_ALERT. Questa tabella contiene i messaggi che fanno riferimento agli avvisi di intrusioni del file a_alert.tbl.

Colonna	Tipo di dati	Breve descrizione
DATE_TIME	date_time	Data e ora per l'azione (richiesto)
FIREWALL	char(100)	Nome completo della macchina firewall (richiesto)
PID	int	ID processo AIX, ID thread NT (richiesto)
MSG_NUM	int	Numero di messaggio (richiesto)
USERID	char(16)	ID utente (ICA0001, ICA0002, ICA0003, ICA0004, ICA2001, ICA2002, ICA2003, ICA2026, ICA2043, ICA2068, ICA2167, ICA2168, ICA 2170, ICA2173, ICA3001, ICA3012, ICA3018)
ACTION	char(7)	collegamento (ICA3012) o bind (ICA3018)
NUM_COUNT	int	Numero dell'errore di autenticazione (ICA0001, ICA0002, ICA0003); numero delle entrate di log per TAG_MSG_NUM (ICA0004); numero di giorni (ICA9000)
TAG_MSG_NUM	char (8)	Tag di messaggio (ICA0004)
SRC_IP	char(15)	Indirizzo IP di origine (ICA2001, ICA2028, ICA2079, ICA2167, ICA3012, ICA3018)
DST_IP	char(15)	Indirizzo IP di destinazione (ICA2028, ICA2079, ICA3012, ICA3018)
AUTH_METHOD	char(20)	Metodo di autenticazione (ICA2002, ICA2167, ICA2170)

Tabella 1 (Pagina 2 di 2). ADMIN_ALERT. Questa tabella contiene i messaggi che fanno riferimento agli avvisi di intrusioni del file a_alert.tbl.

Colonna	Tipo di dati	Breve descrizione
NETWORK	char(25)	Nome rete (ICA2001, ICA2002, ICA2167)
HOST_NAME	char(100)	Nome host (ICA0003, ICA2002)
TIMEOUT_SEC	int	Secondi di timeout (ICA2026)
CONN_USERID	char(16)	Nome utente di collegamento socks (ICA3001)
APPLICATION	char(30)	Nome applicazione - telnet, ftp, ... (ICA2167, ICA2168, ICA2170, ICA3012)

Nota: Messaggi correlati: ICA0001 ICA0002 ICA0003 ICA0004 ICA0005 ICA0006 ICA0007 ICA0008 ICA0009 ICA0010 ICA0011 ICA0012 ICA0013 ICA0014 ICA0015 ICA0016 ICA0017 ICA0018 ICA0019 ICA0020 ICA0021 ICA0022 ICA1010 ICA2001 ICA2002 ICA2003 ICA2020 ICA2026 ICA2028 ICA2037 ICA2040 ICA2042 ICA2043 ICA2079 ICA2167 ICA2168 ICA2170 ICA2173 ICA3001 ICA3012 ICA3018 ICA9000 ICA9001

Tabella 2. FILTER_ACTIVE_RULE. Questa tabella contiene le regole di filtro attive del file f_rule.tbl.

Colonna	Tipo di dati	Breve descrizione
DATE_TIME	date_time	Data e ora per l'azione (richiesto)
FIREWALL	char(100)	Nome completo della macchina firewall (richiesto)
PID	int	ID processo AIX, ID thread NT (richiesto)
MSG_NUM	int	Numero di messaggio (richiesto)
RULE_NUM	int	Numero della regola (richiesto)
RULE	char(150)	Regola (richiesto)

Nota: Messaggio correlato: ICA1037

Tabella 3 (Pagina 1 di 2). FILTER_INFO. Questa tabella contiene messaggi informativi generici o di errore correlati ai filtri del file f_info.tbl.

Colonna	Tipo di dati	Breve descrizione
DATE_TIME	date_time	Data e ora per l'azione (richiesto)
FIREWALL	char(100)	Nome completo della macchina firewall (richiesto)
PID	int	ID processo AIX, ID thread NT (richiesto)
MSG_NUM	int	Numero di messaggio (richiesto)
RULE_NUM	int	Numero regola di filtro (ICA1005)

Tabella 3 (Pagina 2 di 2). FILTER_INFO. Questa tabella contiene messaggi informativi generici o di errore correlati ai filtri del file f_info.tbl.

Colonna	Tipo di dati	Breve descrizione
ERROR_NUM	int	Numero Errore di sistema -- errno AIX o Ultimo errore Windows NT (ICA1007, ICA1008, ICA1009, ICA1011 ICA1013, ICA1015, ICA1021, ICA1023, ICA1024) È possibile richiamare il testo corrispondente a questo numero di errore utilizzando la funzione _strerror. Il testo per Ultimo errore Windows NT è disponibile mediante la funzione relativa al formato dei messaggi oppure nell'Appendice A di Win32 Programmer's Reference Volume 2.
LOAD_PATH	char(100)	Percorso di caricamento dell'estensione kernel (ICA1011, ICA1012)
DVC_DRV	char(25)	Programma di controllo unità (ICA1021)
TERM_SIG	char(25)	Segnale di arresto (ICA1260)
FILE_NAME	char(100)	Nome file (ICA1024)
RC	int	Codice di errore interno del firewall (ICA1019)
Nota: Messaggi correlati: ICA1001 ICA1002 ICA1003 ICA1005 ICA1007 ICA1008 ICA1009 ICA1011 ICA1012 ICA1013 ICA1014 ICA1015 ICA1016 ICA1017 ICA1019 ICA1021 ICA1022 ICA1023 ICA1024 ICA1200 ICA1260		

Tabella 4 (Pagina 1 di 2). FILTER_MATCH. Questa tabella contiene le regole di filtro mappate del file f_match.tbl.

Colonna	Tipo di dati	Breve descrizione
DATE_TIME	date_time	Data e ora per l'azione (richiesto)
FIREWALL	char(100)	Nome completo della macchina firewall (richiesto)
PID	int	ID processo AIX, ID thread NT (richiesto)
MSG_NUM	int	Numero di messaggio (richiesto)
RULE_NUM	int	Numero della regola (richiesto)
ACTION	char(6)	Tipo di regola: permit, deny, etc.
DIRECTION	char (8)	Direzione del pacchetto 'in arrivo' o 'in partenza' (richiesto)
SRC_IP	char(15)	Indirizzo IP del mittente (richiesto)
DST_IP	char(15)	Indirizzo IP del destinatario (richiesto)
PROTOCOL	char(7)	Protocollo di alto livello, ad esempio UDP, IPIP, ICMP, TCP o TCP/ACK (richiesto)
SRC_PORT	int	• Tipo di pacchetto IP per ICMP • Numero di porta del protocollo di origine per altri protocolli (richiesto)

Tabella 4 (Pagina 2 di 2). FILTER_MATCH. Questa tabella contiene le regole di filtro mappate del file f_match.tbl.

Colonna	Tipo di dati	Breve descrizione
DST_PORT	int	• Codice del pacchetto IP per ICMP • Numero di porta del protocollo di destinazione per altri protocolli (richiesto)
ROUTING	char(5)	Connessione di instradamento dei pacchetti: instradamento o locale (richiesto)
INTERFACE	char(10)	Tipo di interfaccia: sicura o non sicura (richiesto)
FRAGMENT	char (8)	Identifica il pacchetto come frammentato o non frammentato (richiesto)
TUNNEL_ID	int	ID tunnel (richiesto)

Tabella 6 (Pagina 2 di 2). INTERFACES. Questa tabella contiene le informazioni sui messaggi di configurazione dell'interfaccia (adattatore) del file interface.tbl.

Colonna	Tipo di dati	Breve descrizione
MSG_NUM	int	Numero di messaggio (richiesto)
IP	char(15)	Indirizzo IP per l'adattatore (ICA9038, ICA9039, ICA9040)
OLD_MASK	char(15)	valore maschera precedente (ICA9040)
NEW_MASK	char(15)	valore nuova maschera (ICA9040)
Nota: Messaggi correlati: ICA9037, ICA9038, ICA9039, ICA9040, ICA9041		

Tabella 7. NAT_INFO. Questa tabella contiene informazioni sui messaggi NAT (Network Address Translation) del file nat_info.tbl.

Colonna	Tipo di dati	Breve descrizione
DATE_TIME	date_time	Data e ora per l'azione (richiesto)
FIREWALL	char(100)	Nome completo della macchina firewall (richiesto)
PID	int	ID processo AIX, ID thread NT (richiesto)
MSG_NUM	int	Numero di messaggio (richiesto)
VERSION	int	Numero di versione NAT (ICA9033)
RELEASE	int	Numero di rilascio NAT (ICA9033)
IP	char(15)	Indirizzo IP (ICA9035, ICA9036)
Nota: Messaggi correlati: ICA9032, ICA9033, ICA9034, ICA9035, ICA9036		

Tabella 8 (Pagina 1 di 2). PAGER_INFO. Questa tabella contiene le informazioni relative alla funzione del cercapersone del firewall, dal file pgr_info.tbl.

Colonna	Tipo di dati	Breve descrizione
DATE_TIME	date_time	Data e ora per l'azione (richiesto)
FIREWALL	char(100)	Nome completo della macchina firewall (richiesto)
PID	int	ID processo AIX, ID thread NT (richiesto)
MSG_NUM	int	Numero di messaggio (richiesto)
USERID	char(16)	ID utente (ICA4036, ICA4174, ICA4175)
ERROR_NUM	int	Numero errore di sistema - errno AIX o Ultimo errore Windows NT (ICA4371)
PROGRAM	char(25)	Nome del programma (ICA4000)
SIGNAL	int	Segnale di arresto (ICA4000)
ID	int	Identificativo (ICA4036)
PRIORITY	int	Priorità (ICA4036)
PERIOD	int	Periodo (ICA4036)

Tabella 8 (Pagina 2 di 2). PAGER_INFO. Questa tabella contiene le informazioni relative alla funzione del cercapersone del firewall, dal file pgr_info.tbl.

Colonna	Tipo di dati	Breve descrizione
RETRY_COUNT	int	Numero di tentativi (ICA4036, ICA4313, ICA4314, ICA4364, ICA4365)
FROM_ENTRY	char(15)	Nome della funzione (ICA4036)
HOST_NAME	char(100)	Nome host (ICA4174, ICA4175)
MESSAGE_TEXT	char(250)	Testo della chiamata (ICA4036, ICA4353 - 4360, ICA4368, ICA4372)
SERVICE	char(25)	Nome del servizio (ICA4017)
SOCKET	int	Numero di socket (ICA4017)
FILENAME	char(100)	Nome file (ICA4154, ICA4351, ICA4352)
Nota: Messaggi correlati: ICA4000 ICA4001 ICA4007 ICA4017 ICA4036 ICA4154 ICA4168 ICA4174 ICA4175, ICA4300 - 4303, ICA4305 - 4315, ICA4351 - 4360, ICA4362 - 4372)		

Tabella 9. PROXY_FTP. Questa tabella contiene le informazioni sull'azione FTP dalle sessioni FTP del file p_ftp.tbl.

Colonna	Tipo di dati	Breve descrizione
DATE_TIME	date_time	Data e ora per l'azione (richiesto)
FIREWALL	char(100)	Nome completo della macchina firewall (richiesto)
PID	int	ID processo AIX, ID thread NT (richiesto)
MSG_NUM	int	Numero di messaggio (richiesto)
USERID	char(16)	ID utente (richiesto)
SRC_IP	char(15)	Indirizzo IP dell'utente (richiesto)
DST_IP	char(15)	Indirizzo IP della macchina remota (richiesto)
ACTION	char(5)	Azione di trasferimento file: put o get (richiesto)
FILE_NAME	char(100)	Nome file
BYTES	long int	Quantità di dati trasferiti
SID	long int	ID sessione univoco (richiesto)
Nota: Messaggio correlato: ICA2075		

Tabella 10 (Pagina 1 di 2). PROXY_HTTP. Questa tabella contiene le informazioni sull'azione HTTP dalle sessioni proxy del file p_http.tbl.

Colonna	Tipo di dati	Breve descrizione
DATE_TIME	date_time	Data e ora per l'azione (richiesto)
FIREWALL	char(100)	Nome completo della macchina firewall (richiesto)
PID	int	ID processo AIX, ID thread NT (richiesto)
MSG_NUM	int	Numero di messaggio (richiesto)

Tabella 10 (Pagina 2 di 2). PROXY_HTTP. Questa tabella contiene le informazioni sull'azione HTTP dalle sessioni proxy del file p_http.tbl.

Colonna	Tipo di dati	Breve descrizione
STATUS	int	Stato (richiesto)
SRC_IP	char(15)	Indirizzo IP dell'utente (richiesto)
REQUEST	char(250)	Contenuto della richiesta HTTP (richiesto)
BYTES	long int	Quantità di dati trasferiti
Nota: Messaggio correlato: ICA2099		

Tabella 11 (Pagina 1 di 2). PROXY_INFO. Questa tabella contiene messaggi informativi generici o di errore correlati ai proxy del file p_info.tbl.

Colonna	Tipo di dati	Breve descrizione
DATE_TIME	date_time	Data e ora per l'azione (richiesto)
FIREWALL	char(100)	Nome completo della macchina firewall (richiesto)
PID	int	ID processo AIX, ID thread NT (richiesto)
MSG_NUM	int	Numero di messaggio (richiesto)
USERID	char(16)	ID utente (ICA2018, ICA2019, ICA2057, ICA2058, ICA2166, ICA2177, ICA2172)
ERROR_NUM	int	Numero errore di sistema - errno AIX o Ultimo errore Windows NT (ICA2005, ICA2006, ICA2009, ICA2029, ICA2035, ICA2038, ICA2039, ICA2052, ICA2054, ICA2055, ICA2056, ICA2057, ICA2058, ICA2059, ICA2063, ICA2064, ICA2065, ICA2066, ICA2067, ICA2068, ICA2069, ICA2069, ICA2070, ICA2071, ICA2074, ICA2110, ICA2111, ICA2113, ICA2114, ICA2115, ICA2118, ICA2119, ICA2121, ICA2122, ICA2123, ICA2124, ICA2200, ICA2201, ICA2202, ICA2203) Per richiamare il testo relativo al numero dell'errore (Errori di sistema AIX) utilizzare la funzione _strerror. Il testo per Ultimo errore Windows NT è disponibile mediante la funzione relativa al formato dei messaggi oppure nell'Appendice A di Win32 Programmer's Reference Volume 2.
OPTION_VAL	char(20)	Indicatore dell'opzione o valore del parametro (ICA2014, ICA2015, ICA2049, ICA2050)
TIME	char(15)	Intervallo di tempo non valido (ICA2044, ICA2202)
RC	int	Codice di errore interno del firewall (ICA2007, ICA2030, ICA2031, ICA2033, ICA2034, ICA2054, ICA2057, ICA2058, ICA2065, ICA2120 ICA2166, ICA2203)

Tabella 11 (Pagina 2 di 2). PROXY_INFO. Questa tabella contiene messaggi informativi generici o di errore correlati ai proxy del file p_info.tbl.

Colonna	Tipo di dati	Breve descrizione
INVOC_NAME	char(20)	Nome di richiamo per il socket o la porta al momento in cui si è verificato l'errore di sistema (ICA2055, ICA2056)
AUDIT_TYPE	char(7)	Tipo di controllo sconosciuto (7 cifre esadecimali) (ICA2004)
HOST_NAME	char(100)	Nome host (ICA2106, ICA2107, ICA2126)
FILE_NAME	char(100)	Nome file (ICA2029, ICA2030, ICA2072, ICA2183, ICA2204, ICA2205, ICA2206, ICA2207)
LINE_NUM	int	Numero di riga (ICA2029, ICA2030)
PROTOCOL	char(25)	Nome protocollo non valido (ICA2112, ICA2116)
CUSTOMIZED_ATTR	char(25)	Numero di riga (ICA2105, ICA2106, ICA2125, ICA2166)
ODM_ERR_NUM	int	Numero di errore da ODM (Object Data Manager) (ICA2102, ICA2103, ICA2104, ICA2105, ICA2107, ICA2108, ICA2109,ICA2125)
APPLICATION (solo NT)	char(30)	Nome applicazione (ICA2200, ICA2201, ICA2202, ICA2203, ICA2204, ICA2205, ICA2206, ICA2207)
CALLER (solo NT)	char(25)	Funzione di chiamata (ICA2200, ICA2201, ICA2202, ICA2203, ICA2204, ICA2205, ICA2206, ICA2207)
FAILED_IN (solo NT)	char(25)	Funzione errata (ICA2201, ICA2203)

Nota: Messaggi correlati: ICA2004 ICA2005 ICA2006 ICA2007 ICA2009 ICA2014 ICA2015 ICA2018 ICA2019 ICA2023 ICA2029 ICA2030 ICA2031 ICA2032 ICA2033 ICA2034 ICA2035 ICA2038 ICA2039 ICA2044 ICA2045 ICA2046 ICA2047 ICA2048 ICA2049 ICA2050 ICA2051 ICA2052 ICA2053 ICA2054 ICA2055 ICA2056 ICA2057 ICA2058 ICA2059 ICA2060 ICA2061 ICA2062 ICA2063 ICA2064 ICA2065 ICA2066 ICA2067 ICA2068 ICA2069 ICA2070 ICA2071 ICA2072 ICA2073 ICA2074 ICA2100 ICA2102 ICA2103 ICA2104 ICA2105 ICA2109 ICA2110 ICA2111 ICA2112 ICA2113 ICA2114 ICA2115 ICA2116 ICA2117 ICA2118 ICA2119 ICA2120 ICA2121 ICA2122 ICA2123 ICA2124 ICA2125 ICA2126 ICA2127 ICA2166 ICA2171 ICA2172 ICA2183 ICA2200 ICA2201 ICA2202 ICA2203 ICA2204 ICA2205 ICA2206 ICA2207

Tabella 12 (Pagina 1 di 2). PROXY_LOGIN. Questa tabella contiene le informazioni (principalmente relative all'autenticazione) sui login PROXY eseguiti correttamente del file p_login.tbl.

Colonna	Tipo di dati	Breve descrizione
DATE_TIME	date_time	Data e ora per l'azione (richiesto)
FIREWALL	char(100)	Nome completo della macchina firewall (richiesto)
PID	int	ID processo AIX, ID thread NT (richiesto)
MSG_NUM	int	Numero di messaggio (richiesto)
USERID	char(16)	ID utente (richiesto)

Tabella 12 (Pagina 2 di 2). PROXY_LOGIN. Questa tabella contiene le informazioni (principalmente relative all'autenticazione) sui login PROXY eseguiti correttamente del file p_login.tbl.

Colonna	Tipo di dati	Breve descrizione
APPLICATION	char(30)	Nome applicazione - telnet, ftp, ... (richiesto)
AUTH_METHOD	char(15)	Metodo di autenticazione (richiesto)
NETWORK	char(25)	Rete (sicura/non sicura - potrebbe contenere ulteriori informazioni) (richiesto)
HOST_NAME	char(100)	Nome host (richiesto)
Nota: Messaggi correlati: ICA2024 ICA2025 ICA2169		

Tabella 13. PROXY_STATUS. Questa tabella contiene le informazioni relative allo stato del proxy dal file p_stat.tbl.

Colonna	Tipo di dati	Breve descrizione
DATE_TIME	date_time	Data e ora per l'azione (richiesto)
FIREWALL	char(100)	Nome completo della macchina firewall (richiesto)
PID	int	ID processo AIX, ID thread NT (richiesto)
MSG_NUM	int	Numero di messaggio (richiesto)
USERID	char(16)	ID utente (ICA2008, ICA2016, ICA2021)
SRC_IP	char(15)	Indirizzo IP di origine (ICA2000, ICA2008, ICA2010, ICA2011, ICA2012, ICA2013, ICA2141, ICA2180)
DST_IP	char(15)	Indirizzo IP di destinazione (ICA2000, ICA2010, ICA2011, ICA2012, ICA2013)
REMOTE_HOST	char(100)	Nome host remoto (per la macchina firewall) (ICA2021, ICA2022, ICA2027)
SID (solo NT)	int	Identificativo sessione (ICA2177, ICA2180, ICA2181 ICA2182)
SOCKET (solo NT)	char(25)	Nome socket (ICA2177)
RC (solo NT)	int	Codice di errore o motivo (ICA2181, ICA2182)
CMD (solo NT)	char(36)	Scheda SMTP (ICA2182)
Nota: Messaggi correlati: ICA2000 ICA2010 ICA2011 ICA2012 ICA2013 ICA2016 ICA2021 ICA2022 ICA2027 ICA2097 ICA2098 ICA2141 ICA2163 ICA2164 ICA2165 ICA2177 ICA2180 ICA2181 ICA2182		

Tabella 14 (Pagina 1 di 2). SERVER_INFO. Questa tabella contiene informazioni sullo stato e le attività del server di configurazione del file srv_info.tbl.

Colonna	Tipo di dati	Breve descrizione
DATE_TIME	date_time	Data e ora per l'azione (richiesto)
FIREWALL	char(100)	Nome completo della macchina firewall (richiesto)

Tabella 14 (Pagina 2 di 2). SERVER_INFO. Questa tabella contiene informazioni sullo stato e le attività del server di configurazione del file srv_info.tbl.

Colonna	Tipo di dati	Breve descrizione
PID	int	ID processo AIX, ID thread NT (richiesto)
MSG_NUM	int	Numero di messaggio (richiesto)
USERID	char(16)	ID utente (ICA9003, ICA9004)
ERROR_NUM	int	Numero errore di sistema – errno AIX o Ultimo errore Windows NT (ICA9008, ICA9009) Per richiamare il testo relativo al numero dell'errore (Errori di sistema AIX) utilizzare la funzione strerror. Il testo per Ultimo errore Windows NT è disponibile mediante la funzione relativa al formato dei messaggi oppure nell'Appendice A di Win32 Programmer's Reference Volume 2.
Nota: Messaggi correlati: ICA9003 ICA9004 ICA9005 ICA9006 ICA9007 ICA9008 ICA9009 ICA9010 ICA9011 ICA9012 ICA9013 ICA9014 ICA9015		

Tabella 15 (Pagina 1 di 2). SESSION. Questa tabella contiene le informazioni relative all'avvio ed all'arresto delle sessioni SOCKS e PROXY del file session.tbl.

Colonna	Tipo di dati (lunghezza)	Breve descrizione
DATE_TIME	date_time	Data e ora per l'azione (richiesto)
FIREWALL	char(100)	Nome completo della macchina firewall (richiesto)
PID	int	ID processo AIX, ID thread NT (richiesto)
MSG_NUM	int	Numero di messaggio (richiesto)
USERID	char(16)	ID utente (richiesto)
SERVICE_TYPE	char(10)	Tipo di servizio: socks o proxy (richiesto)
APPLICATION	char(30)	Nome applicazione - telnet, ftp, ... (richiesto)
SRC_IP	char(15)	Indirizzo IP dell'utente (richiesto)
DST_IP	char(15)	Indirizzo IP della macchina remota (richiesto)
SESSION_EVENT	char(5)	• iniziano quando viene stabilita una sessione. • terminano quando viene arrestata una sessione. (richiesto)
BYTES	long int	La quantità di dati trasferiti durante la sessione. Se l'applicazione è telnet, questa sarà 0.
SID	long int	Identificativo di sessione univoco, generato dal firewall, in base all'ora.

Tabella 15 (Pagina 2 di 2). SESSION. Questa tabella contiene le informazioni relative all'avvio ed all'arresto delle sessioni SOCKS e PROXY del file session.tbl.

Colonna	Tipo di dati (lunghezza)	Breve descrizione

Nota:

Messaggi correlati:

- Avvio sessione Safemail: ICA2178
- Arresto sessione Safemail: ICA2179
- Avvio sessione Socks: ICA3011
- Arresto sessione Socks: ICA3015
- Avvio sessione Telnet proxy: ICA2036 (Log AIX) ICA2208, ICA2218 (Log NT)
- Arresto sessione Telnet proxy: ICA2077 (Log AIX) ICA2209, ICA2219 (Log NT)
- Avvio sessione FTP proxy: ICA2041 (Log AIX) ICA2208, ICA2218 (Log NT)
- Arresto sessione FTP proxy: ICA2076 (Log AIX e NT)

Per ulteriori dettagli sulle azioni della sessione FTP Socks, consultare la tabella SOCKS_FTP. Le informazioni relative alle azioni della sessione FTP Proxy sono contenute nella tabella PROXY_FTP.

Tabella 16. SOCKS_FTP. Questa tabella contiene le informazioni sull'azione FTP SOCKS dalle sessioni FTP del file s_ftp.tbl.

Colonna	Tipo di dati	Breve descrizione

Tabella 17 (Pagina 1 di 2). SOCKS_INFO. Questa tabella contiene messaggi informativi generici o di errore correlati al Socks del file s_info.tbl.

Colonna	Tipo di dati	Breve descrizione
DATE_TIME	date_time	Data e ora per l'azione (richiesto)
FIREWALL	char(100)	Nome completo della macchina firewall (richiesto)
PID	int	ID processo AIX, ID thread NT (richiesto)
MSG_NUM	int	Numero di messaggio (richiesto)
USERID	char(16)	ID utente (ICA3044, ICA3045, ICA3046, ICA3047, ICA3049)
ACTION	char(7)	collegamento (ICA3044, ICA3049) o bind (ICA3046, ICA3047)
ERROR_NUM	int	Numero errore di sistema - errno AIX (ICA3013, ICA3019, ICA3031, ICA3032, ICA3040, ICA3044, ICA3101, ICA3102, ICA3103, ICA3104, ICA3106, ICA3107, ICA3108, ICA3122, ICA3124, ICA3125, ICA3126, ICA3128)
SRC_HOST	char(25)	Nome host di origine (ICA3019, ICA3035)
DST_HOST	char(25)	Nome host di destinazione (ICA3016, ICA3045)
SRC_IP	char(15)	Indirizzo di origine (ICA3042, ICA3043, ICA3044, ICA3045, ICA3046, ICA3047, ICA3049)
DST_IP	char(15)	Indirizzo di destinazione (ICA3044, ICA3045, ICA3046, ICA3047, ICA3049)
LINE_NUM	int	Numero di riga (ICA3022, ICA3023, ICA3024, ICA3025, ICA3026, ICA3109, ICA3110, ICA3111, ICA3112, ICA3115, ICA3116, ICA3117, ICA3118, ICA3119, ICA3120); Numero di righe (ICA3113)
EXEC_STATUS	int	Stato di esecuzione (ICA3027)
CMD	char(36)	Comando, ad esempio, login (ICA3027, ICA3039, ICA3042, ICA3044, ICA3048) nota: per ICA3042, il comando è nel formato esadecimale
FILE_NAME	char(100)	Nome file (ICA3030, ICA3032, ICA3105, ICA3109, ICA3110, ICA3111, ICA3112, ICA3113, ICA3114, ICA3115, ICA3116, ICA3117, ICA3118, ICA3119, ICA3120)
APPLICATION	char(30)	Nome applicazione - telnet, ftp... (ICA3044, ICA3045, ICA3049)
VERSION	char(10)	Numero della versione Socks in formato esadecimale (ICA3043)

Tabella 17 (Pagina 2 di 2). SOCKS_INFO. Questa tabella contiene messaggi informativi generici o di errore correlati al Socks del file s_info.tbl.

Colonna	Tipo di dati	Breve descrizione
Nota: Messaggi correlati: ICA3013 ICA3016 ICA3017 ICA3019 ICA3022 ICA3023 ICA3024 ICA3025 ICA3026 ICA3027 ICA3030 ICA3031 ICA3032 ICA3033 ICA3035 ICA3039 ICA3040 ICA3041 ICA3042 ICA3043 ICA3044 ICA3045 ICA3046 ICA3047 ICA3048 ICA3049 ICA3052 ICA3101 ICA3102 ICA3103 ICA3104 ICA3105 ICA3106 ICA3107 ICA3108 ICA3109 ICA3110 ICA3111 ICA3112 ICA3113 ICA3114 ICA3115 ICA3116 ICA3117 ICA3118 ICA3119 ICA3120 ICA3121 ICA3122 ICA3123 ICA3124 ICA3125 ICA3126 ICA3127 ICA3128		

Tabella 18. SSL_INFO. Questa tabella contiene informazioni sullo stato e sulle attività SSL del file ssl_info.tbl.

Colonna	Tipo di dati	Breve descrizione
DATE_TIME	date_time	Data e ora per l'azione (richiesto)
FIREWALL	char(100)	Nome completo della macchina firewall (richiesto)
PID	int	ID processo AIX, ID thread NT (richiesto)
MSG_NUM	int	Numero di messaggio (richiesto)
Client_IP	char(15)	Indirizzo IP del client
Nota: Messaggi correlati: ICA5015 ICA5022 ICA5023 ICA5028 ICA5029 ICA5036 ICA5039 ICA5060 ICA5063 ICA5082 ICA5120		

Tabella 19. SU. Questa tabella contiene i dettagli sulle attività SU del file su.tbl, quando viene caricato un log SU AIX.

Colonna	Tipo di dati	Breve descrizione
DATE_TIME	date_time	Data e ora per l'azione (richiesto) Poiché AIX non registra l'anno nel file di log su, la parte dell'anno relativa alla colonna DATE_TIME viene impostata sull'anno corrente o sull'anno precedente, in base alle impostazioni mese/giorno (se l'impostazione mese/giorno è successiva a quella corrente, questa parte viene impostata sull'anno precedente).
FROM_USERID	char(16)	ID utente (richiesto)
TO_USERID	char(16)	ID utente (richiesto)
LOGIN_STATUS	char(7)	Stato del tentativo di collegamento: riuscito o non riuscito (richiesto)

Tabella 20 (Pagina 1 di 2). TUNNEL_CONTEXT. Questa tabella contiene le specifiche di contesto del TUNNEL attivo del file t_cntxt.tbl.

Colonna	Tipo di dati	Breve descrizione
DATE_TIME	date_time	Data e ora per l'azione (richiesto)

Tabella 20 (Pagina 2 di 2). TUNNEL_CONTEXT. Questa tabella contiene le specifiche di contesto del TUNNEL attivo del file t_cntxt.tbl.

Colonna	Tipo di dati	Breve descrizione
FIREWALL	char(100)	Nome completo della macchina firewall (richiesto)
PID	int	ID processo AIX, ID thread NT (richiesto)
MSG_NUM	int	Numero di messaggio (richiesto)
TUNNEL_ID	long int	ID tunnel (richiesto)
SRC_IP	char(15)	Indirizzo IP di origine (richiesto)
DST_IP	char(15)	Indirizzo IP di destinazione (richiesto)
ENCRYPTION	char(7)	Algoritmo di crittografia DES_CBC o CDMF
Nota: Messaggio correlato: ICA1043		

Tabella 21. TUNNEL_POLICY. Questa tabella contiene le istruzioni per la politica del TUNNEL del file t_policy.tbl.

Colonna	Tipo di dati	Breve descrizione
DATE_TIME	date_time	Data e ora per l'azione (richiesto)
FIREWALL	char(100)	Nome completo della macchina firewall (richiesto)
PID	int	ID processo AIX, ID thread NT (richiesto)
MSG_NUM	int	Numero di messaggio (richiesto)
POLICY	char(60)	Lettura dell'istruzione per la politica dal file fwpolicy (richiesto)
Nota: Messaggio correlato: ICA1040		

Tabella 22 (Pagina 1 di 2). TUNNEL_STATUS. Questa tabella contiene le informazioni sulle modifiche dello stato dei TUNNEL dal file t_stat.tbl.

Colonna	Tipo di dati	Breve descrizione
DATE_TIME	date_time	Data e ora per l'azione (richiesto)
FIREWALL	char(100)	Nome completo della macchina firewall (richiesto)
PID	int	ID processo AIX, ID thread NT (richiesto)
MSG_NUM	int	Numero di messaggio (richiesto)
SESSION_SCKT	long int	Porta socket di sessione (per ICA1038)
MASTER_SCKT	long int	Porta socket principale (per ICA1038)
TUNNEL_ID	long int	ID tunnel eliminato (per ICA1041)

Tabella 22 (Pagina 2 di 2). TUNNEL_STATUS. Questa tabella contiene le informazioni sulle modifiche dello stato dei TUNNEL dal file t_stat.tbl.

Colonna	Tipo di dati	Breve descrizione

Nota:

Messaggi correlati: ICA1038 ICA1039 ICA1041 ICA1042

- I dettagli sulla politica definita (ICA1039) si trovano nella tabella TUNNEL_POLICY.
- I dettagli sul tunnel definito (ICA1042) si trovano nella tabella TUNNEL_CONTEXT.

Capitolo 3. Kit di sviluppo software del plugin SafeMail

Lo scopo principale del gateway SafeMail di IBM Firewall è scambiare la posta tra reti sicure e non sicure nascondendo contemporaneamente i nomi degli host della rete sicura.

Il gateway SafeMail non fornisce però funzioni di filtro del contenuto. Tuttavia, è possibile scrivere un programma per filtrare il contenuto ed installarlo sul firewall come un plugin del gateway SafeMail. Questo plugin del gateway SafeMail è in grado di visualizzare l'intero messaggio di posta elettronica e di filtrarlo secondo i criteri stabiliti. Il plugin può indicare al gateway SafeMail di interrompere il trasferimento di un messaggio oppure può consentire al messaggio di passare attraverso il gateway.

Panoramica dell'elaborazione SafeMail

Quando un client SMTP si collega al gateway SafeMail, quest'ultimo si collega al server di destinazione SMTP e passa il messaggio di posta elettronica una riga per volta dal client al server di destinazione man mano che riceve le righe di posta elettronica dal client. Il gateway SafeMail riscrive alcune righe di intestazione del messaggio, se necessario, per oscurare i nomi degli host della rete sicura.

Se viene installato un plugin del programma di filtro del contenuto, il gateway SafeMail richiama questo programma ad ogni riga del messaggio di posta elettronica che passa attraverso il gateway. Inoltre, il gateway SafeMail passa le informazioni relative all'origine ed alla destinazione del messaggio di posta elettronica ed altre informazioni in modo che il programma di filtro del contenuto possa mettere in correlazione le varie chiamate. È utile nel caso in cui l'intero messaggio deve essere analizzato prima che il programma di filtro del contenuto determini se consentire o meno al messaggio di passare attraverso il firewall.

Se il gateway SafeMail deve riscrivere una qualsiasi intestazione allo scopo di nascondere i nomi degli host della rete sicura, il plugin del programma di filtro del contenuto verrà richiamato prima che l'intestazione venga riscritta.

Creazione di un plugin del gateway SafeMail

Per creare ed installare un plugin del gateway SafeMail è necessario:

- Scrivere il codice di origine per la DLL del plugin
- Creare la DLL
- Installare la DLL sul firewall

`ROOTDIR\samples\safemail` contiene codici di esempio per un plugin del programma di filtro del contenuto, i file di intestazioni necessari ed i makefile di esempio per IBM Visual Age e Microsoft Visual C++. *ROOTDIR* è l'indirizzario selezionato durante il processo di installazione come ubicazione di destinazione per IBM Firewall.

Scrittura del codice di origine

Il plugin del programma di filtro del contenuto deve implementare una funzione denominata UsrCheck, che ha il seguente prototipo:

```
int _Export UsrCheck(pCheckData Data);
```

Questo è il punto di entrata che il gateway SafeMail richiama quando una riga del messaggio di posta elettronica è pronta per essere esaminata dal programma di filtro del contenuto. Questa funzione esamina la riga del messaggio di posta elettronica e restituisce 0, se consente al messaggio di passare attraverso il gateway SafeMail, o un valore diverso da zero per indicare a SafeMail di interrompere l'elaborazione del messaggio.

Per una descrizione completa dell'interfaccia tra il gateway SafeMail ed il programma di filtro del contenuto, consultare il codice di esempio in usrcheck.c, nell'indirizzario `ROOTDIR\samples\safemail`.

Il parametro pCheckData della funzione di controllo è una struttura C documentata in usrcheck.h, nell'indirizzario `ROOTDIR\samples\safemail`. Questa struttura contiene importanti informazioni sul messaggio di posta elettronica che viene elaborato, ad esempio gli indirizzi di origine e destinazione dei server SMTP ed i tipi di rete (sicura e non sicura) per i server SMTP di invio e ricezione. Inoltre, questa struttura contiene un correlatore di conversazione, che consente al programma di filtro del contenuto di mettere in correlazione varie chiamate con lo stesso messaggio di posta elettronica.

Creazione della DLL

Dopo aver scritto il codice di origine per il plugin del programma di filtro del contenuto, compilarlo e collegarlo ad una DLL. La DLL deve essere denominata smusr.dll. Il punto di entrata UsrCheck deve essere esportato dalla DLL. Consultare i makefile di esempio nell'indirizzario `ROOTDIR\samples\safemail`, per informazioni sulle alternanze tra compilazione e collegamento necessarie per creare la DLL in modo corretto. I makefile di esempio sono forniti per IBM VisualAge C++ e Microsoft Visual C.

Installazione della DLL

Dopo aver creato correttamente smusr.dll, installarlo sul Firewall. Copiare smusr.dll nell'indirizzario `\bin` del firewall. Quindi utilizzare il programma di gestione dei servizi dal pannello di controllo di Windows NT per arrestare e riavviare il server SafeMail di IBM Firewall in modo da caricare il plugin.

IBM Firewall contiene un file smusr.dll di esempio nell'indirizzario `\bin` del firewall. Ridenominare questa DLL prima di copiare il proprio file smusr.dll nell'indirizzario indicato in modo da poterlo ripristinare se in futuro verrà rimosso il plugin.

I nomi del programma di compilazione variano a seconda del tipo in questo capitolo e nei successi due capitoli. I tre capitoli fanno riferimento agli stessi due programmi di compilazione.

Capitolo 4. Kit di sviluppo software del plugin Log Archiver

Il daemon di log di IBM Firewall scrive le informazioni di log su file che vengono specificati con la casella di dialogo del client di configurazione **Funzioni di log**. Utilizzare il comando `fwlogmgmt` per archiviare periodicamente i vecchi record di log. Di solito, il comando `fwlogmgmt` viene eseguito dal programma di pianificazione di Windows NT. Per impostazione assunta, il comando `fwlogmgmt` archivia i vecchi record di log in un indirizzario e li comprime utilizzando l'appropriato comando di Windows NT. Tuttavia, è possibile scrivere un plugin Log Archiver per sostituire le condizioni di archiviazione assunte.

Creazione di un plugin Log Archiver

Per creare un plugin Log Archiver, attenersi alla seguente procedura:

1. Scrivere il codice di origine per la DLL del plugin
2. Creare la DLL
3. Installare la DLL sul firewall

L'indirizzario `ROOTDIR\sample\logarch` contiene il codice di esempio per il plugin Log Archiver che duplica le caratteristiche del firewall ed un makefile per IBM Visual Age per C++. *ROOTDIR* è l'indirizzario selezionato durante il processo di installazione come ubicazione di destinazione per IBM Firewall.

Scrittura del codice di origine

Il plugin Log Archiver deve supportare una serie di funzioni che il firewall utilizza per eseguire la funzione di archiviazione. I prototipi di queste funzioni sono definiti in fwarch.h, nell'indirizzario `ROOTDIR\sample\logarch`.

Queste funzioni supportano le funzioni di archiviazione di base quali aggiungere un file in un archivio, estrarre un file da un archivio, aggiornare un archivio ed elencare i file in un archivio.

Per ulteriori informazioni su queste funzioni, consultare il codice di esempio in fwarch.c, nell'indirizzario `ROOTDIR\sample\logarch`.

Creazione della DLL

Dopo aver scritto il codice di origine per il plugin Log Archiver, compilarlo e collegarlo ad una DLL. La DLL deve essere denominata fwarch.dll. Tutte le funzioni elencate in fwarch.h devono essere esportate dalla DLL.

Nell'indirizzario `ROOTDIR\sample\logarch` viene fornito un makefile di esempio per IBM VisualAge per C++ per creare un codice di esempio nella DLL appropriata.

Installazione della DLL

Dopo aver creato correttamente fwarch.dll, installarlo sul Firewall. Copiare fwarch.dll nell'indirizzario `ROOTDIR\bin`.

Anche il file assunto del firewall fwarch.dll è ubicato in questo indirizzario. Eseguire la copia di riserva o ridenominare questa DLL prima di copiare la DLL sostitutiva nell'indirizzario.

Inoltre, assicurarsi che il comando `fwlogmgmt` non sia correntemente in esecuzione e che il daemon di log di IBM Firewall non venga eseguito quando viene sostituita la DLL assunta. Utilizzare il programma di gestione dei servizi per arrestare il daemon di log di IBM Firewall e riavviarlo dopo aver sostituito la DLL.

Capitolo 5. Metodi di autenticazione personalizzati

Questo capitolo fornisce le informazioni su come personalizzare i metodi di autenticazione.

Autenticazione fornita dall'utente

Viene fornito un esempio di autenticazione utente ubicato nell'indirizzario `ROOT_DIR\bin\authsdk`. I file inclusi sono:

- authschm.h - file di definizione interfacce
- authus.cpp - file di origine per lo schema di esempio
- gwauth4.lib - libreria del firewall
- msvc++.mak - makefile di Microsoft Visual C
- schmname.h - file di definizione interfacce
- vac++.mak - makefile di IBM Visual Age

Utilizzare i seguenti comandi per compilare l'esempio di autenticazione utente per Visual Age IBM:

- nmake -f vac++.mak - crea la DLL
- nmake -f vac++.mak install - crea ed installa la DLL
- nmake -f vac++.mak clean - ripulisce l'indirizzario locale

Utilizzare i seguenti comandi per compilare l'esempio di autenticazione utente per Visual C Microsoft:

- nmake -f msvc++.mak - crea la DLL
- nmake -f msvc++.mak install - crea ed installa la DLL
- nmake -f msvc++.mak clean - ripulisce l'indirizzario locale

Utilizzo del kit di sviluppo del software per creare uno schema dell'autenticazione fornita dall'utente

IBM Firewall fornisce un'interfaccia plugin per consentire l'integrazione dei prodotti di sicurezza per l'autenticazione distribuiti da altri produttori. Ciò viene eseguito scrivendo uno schema di autenticazione .dll che si collega all'interfaccia dello schema di autenticazione del firewall.

Panoramica del processo di autenticazione del firewall

I seguenti servizi del firewall devono eseguire l'autenticazione degli utenti prima che questi possano aver accesso al firewall:

- Server di configurazione di IBM Firewall
- Daemon FTP proxy di IBM Firewall
- Daemon HTTP proxy di IBM Firewall
- Daemon Telnet di IBM Firewall

- Server Socks di IBM Firewall

Il firewall fornisce i seguenti schemi di autenticazione:

Negare tutto All'utente viene sempre negato l'accesso al servizio.

Consentire tutto All'utente viene consentito l'accesso al servizio senza che gli venga richiesta alcuna informazione.

Parola d'ordine firewall All'utente viene richiesta una parola d'ordine che sia definita nel database utente del firewall.

Parola d'ordine per accesso a NT All'utente viene richiesta la parola d'ordine per l'accesso a Windows NT.

SecureNetKey L'utente viene autenticato utilizzando AssureNet Pathways SecureNet Key.

Scheda SecurID L'utente viene autenticato utilizzando la scheda di sicurezza Security Dynamics SecurID.

Lo schema di autenticazione utilizzato può essere definito in base all'utente o al servizio. Ad esempio, il firewall può essere configurato in modo che quando un utente, *John*, tenta di collegarsi al server di configurazione di IBM Firewall, gli viene richiesta la parola d'ordine per l'accesso a Windows NT. Ma quando *John* desidera utilizzare il proxy Telnet di IBM Firewall, viene autenticato utilizzando la sua scheda SecurID. Intanto, se un altro utente, *Mary*, tenta di collegarsi al server di configurazione di IBM Firewall, gli viene richiesta la parola d'ordine del firewall. Per ulteriori informazioni sugli schemi di autenticazione forniti dagli utenti e su come vengono definiti per ciascun utente, consultare il capitolo relativo alla gestione del manuale *IBM eNetwork Firewall - Guida per l'utente*.

Oltre agli schemi di autenticazione forniti da IBM Firewall, è possibile installare un massimo di tre schemi di autenticazione forniti dagli utenti. Questi schemi possono essere scritti per interagire con l'infrastruttura di sicurezza esistente oppure possono essere richiesti ai fornitori di altre case di produzione per integrare i loro prodotti con il firewall.

Ogni schema di autenticazione nel firewall, incluse le autenticazioni fornite dagli utenti, è rappresentato da una DLL che implementa l'API dello schema di autenticazione. Tale API definisce come lo schema di autenticazione viene registrato con il firewall ed il modo in cui il firewall gli trasmette le richieste di autenticazione.

Creazione di uno schema di autenticazione fornito dall'utente

La creazione di uno schema di autenticazione fornito dall'utente è costituita dai seguenti passi:

- scrittura del codice di origine per supportare l'API dello schema di autenticazione
- collegamento e compilazione del codice di origine in una DLL
- installazione della DLL sul firewall

I file di intestazione di origine C ed i file di libreria necessari per creare uno schema di autenticazione fornito dall'utente, ad esempio i makefile per Microsoft Visual C++ e IBM Visual Age per C++, sono contenuti in `ROOTDIR\bin\authsdk`.

Scrittura del codice di origine

Tutti gli schemi di autenticazione devono:

1. registrarsi con il firewall
2. supportare AuthSchmFn

Registrazione con il firewall: Prima che i servizi del firewall vengano avviati, il firewall tenta di caricare tutte le DLL trovate nel sottoindirizzario `\bin\authschm`. Man mano che ciascuna DLL viene caricata, la relativa routine di inizializzazione deve richiamare una funzione del firewall denominata registerAuthSchm in modo che venga registrata con il firewall.

Il prototipo della funzione registerAuthSchm è definito nel file di intestazione authschm.h. Viene utilizzato un solo parametro che rappresenta un puntatore alla struttura AuthSchmInfo, anch'essa definita in authschm.h. La struttura AuthSchmInfo associa un nome dello schema di autenticazione all'indirizzo di AuthSchmFn che il firewall deve richiamare per poter passare le richieste di autenticazione allo schema di autenticazione.

Gli schemi di autenticazione forniti dall'utente devono utilizzare uno dei seguenti nomi:

1. user
2. userauth2
3. userauth3

Sono stati definiti dei nomi simbolici per questi nomi nel file di intestazione schmname.h. Gli schemi di autenticazione forniti dall'utente devono essere concepiti in modo tale da consentire all'utente finale di specificare quale di questi tre nomi viene utilizzato, in modo da poter installare più schemi sullo stesso firewall indipendentemente dal fatto che due schemi diversi richiedano lo stesso nome.

Dopo che la routine di inizializzazione della DLL ha richiamato correttamente la funzione registrAuthSchm ed è stata restituita al richiedente, la DLL deve essere preparata per elaborare le richieste di autenticazione. Per questo motivo, può essere necessario eseguire ogni inizializzazione specifica degli schemi nella routine di inizializzazione della DLL.

Supporto di AuthSchmFn: Ogni DLL dello schema di autenticazione deve supportare una funzione denominata AuthSchmFn utilizzando il prototipo definito in authschm.h. La funzione AuthSchmFn ha un parametro, un puntatore ad una struttura AuthReq. AuthReq è una semplice struttura C che contiene tutte le informazioni relative alla richiesta di autenticazione corrente. AuthReq è definito in authschm.h. La struttura di AuthReq contiene il nome dell'utente che viene

gwaput Rappresenta l'indirizzo di una routine callback fornita dal firewall, che lo schema di autenticazione può utilizzare quando desidera inviare un messaggio all'utente. Ad esempio, se lo schema di autenticazione emette un messaggio di richiesta all'utente, deve richiamare il punto di entrata fornito nel parametro gwaput. Il prototipo della funzione callback gwaput è la definizione AuthSchmPut contenuta in authschm.h. Per un elenco completo dei parametri che AuthSchmFn deve passare su questa chiamata, consultare i commenti relativi alla definizione AuthSchmPut.

gwaget Rappresenta l'indirizzo di una routine callback fornita dal firewall, che lo schema di autenticazione può utilizzare quando richiede una risposta all'utente finale che viene autenticato. Ad esempio, se lo schema di autenticazione richiede una parola d'ordine dall'utente, deve richiamare il punto di entrata fornito nel parametro gwaget. Il prototipo della funzione callback gwaget è la definizione AuthSchmGet contenuta in authschm.h. Per un elenco completo dei parametri che AuthSchmFn deve passare su questa chiamata, consultare i commenti relativi alla definizione AuthSchmGet. Un parametro particolarmente importante è echo. AuthSchmFn può utilizzare questo parametro per indicare se la risposta dell'utente deve essere rinviata o meno.

opaque_data Il campo opaque_data viene utilizzato dal firewall per mettere in correlazione le chiamate tra AuthSchmFn e le routine callback. Quando vengono richiamate le routine gwaget e gwaput, la funzione AthSchmFn deve trasferire lo stesso valore opaque_data della struttura AuthReq.

Gli schemi di autenticazione devono poter interagire con tutti i componenti del firewall. Alcuni componenti del firewall possono supportare più caselle di dialogo di domanda/risposta con l'utente finale. Questi componenti vengono denominati componenti del firewall interattivi. Alcuni componenti del firewall, a causa del tipo di protocollo, possono supportare solo una singola domanda/risposta. Questi sono denominati componenti non interattivi.

Lo schema di autenticazione fornito dall'utente deve essere in grado di adattarsi ad ogni tipo di componente del firewall che viene richiamato, come indicato dal campo Componente della struttura AuthReq. I valori validi del campo Componente vengono definiti in authschm.h. I valori validi correnti del campo Componente sono:

Tabella 23. Valori validi del campo Componente

Simbolo componente da AuthSchm.h	**Componente del firewall**	**Interattivo/Non interattivo**
AUTHSCHM_UNKNOWN	Componente del firewall nuovo o non riconosciuto	Considerato interattivo
AUTHSCHM_REMADMIN	Server di configurazione	interattivo
AUTHSCHM_FTP	Proxy FTP	non interattivo
AUTHSCHM_TELNET	Proxy Telnet	interattivo
AUTHSCHM_HTTP	Proxy HTTP	interattivo
AUTHSCHM_SOCKS_PWD	Server Socks che utilizza l'autenticazione della parola d'ordine	non interattivo
AUTHSCHM_SOCKS_CRAM	Server Socks che utilizza l'autenticazione CRAM	interattivo
AUTHSCHM_REMIPSEC	Server IPSEC del client remoto (correntemente non disponibile su Windows NT)	interattivo

Quando AuthSchmFn ha completato l'elaborazione, deve ritornare al chiamante con uno dei codici di errore GWA definiti in authschm.h. Questo codice di errore viene utilizzato per indicare se l'utente è stato autenticato correttamente oppure se si sono verificati errori durante l'elaborazione:

Tabella 24. Codici di errore GWA

Codice di errore	Significato
GWA_OK	Nessun errore durante l'elaborazione, l'utente è stato autenticato correttamente
GWA_DENY	Nessun errore durante l'elaborazione ma l'utente non è riuscito ad eseguire l'autenticazione
GWA_IOFAILURE	Si è verificato un errore durante il tentativo di inviare le richieste all'utente o di ricevere una risposta dall'utente. Di solito viene restituito quando ci sono errori nelle routine callback.
GWA_BUFFERTOOSMALL	La funzione AuthSchmFn non è riuscita a ricevere una risposta dall'utente, perché non è stato possibile allocare un buffer sufficientemente grande.
GWA_NOAUTHFN	Errore - Non importante per l'autenticazione degli schemi
GWA_FNNOTREG	Errore - Non importante per l'autenticazione degli schemi
GWA_RSVNAME	Errore - La richiesta di autenticazione contiene un nome riservato e non può essere utilizzato per questo schema di autenticazione
GWA_BADNETTYPE	Errore - Non importante per l'autenticazione degli schemi
GWA_BADAPP	Errore - Non importante per l'autenticazione degli schemi
GWA_BADADDR	Errore - L'indirizzo fornito nella richiesta di autenticazione non era valido
GWA_MEMSHORTAGE	Errore - Non è stato possibile elaborare la richiesta di autenticazione perché la memoria non poteva essere allocata
GWA_USERDBFAIL	Errore - Non è stato possibile interrogare un database richiesto
GWA_REGFAILED	Errore - Non importante per l'autenticazione degli schemi
GWA_AUTHERROR	Errore - Condizione di errore specifica dello schema di autenticazione
GWA_INTERNAL	Errore - Più condizioni di errore nello schema di autenticazione

Quando la funzione AuthSchmFn viene restituita al firewall, se il codice di errore è GWA_OK, l'utente può essere autenticato e gli viene consentito l'accesso al servizio richiesto. GWA_DENY non è considerato come una condizione errore, ma all'utente viene negato l'accesso al servizio richiesto. Tutti gli altri codici di errore sono condizioni di errore ed all'utente viene negato l'accesso al servizio richiesto.

Compilazione e collegamento al codice di origine: Durante la compilazione ed il collegamento al codice di origine in una DLL, è necessario collegare la DLL a gwauth4.dll utilizzando il gwauth4.lib fornito nell'indirizzario `\bin\authsdk`, per risolvere i nomi del punto di entrata definiti in authschm.h. Inoltre, è importante che AuthSchmFn non sia esportato dalla DLL. I makefile di esempio per IBM VisualAge per C++ e Microsoft Visual C++ vengono forniti nell'indirizzario `\bin\authsdk`.

Installazione della DLL: Dopo aver creato correttamente la DLL, copiarla nell'indirizzario `ROOTDIR\bin\authschm` e rieseguire il boot della macchina firewall. L'esecuzione del boot è necessaria affinché il firewall possa caricare la DLL e registrare gli schemi di autenticazione della DLL.

Raggruppamento: La Figura 1 a pagina 56 indica come vengono caricati gli schemi di autenticazione ed il modo in cui la funzione chiave esegue le chiamate durante l'elaborazione della richiesta di autenticazione.

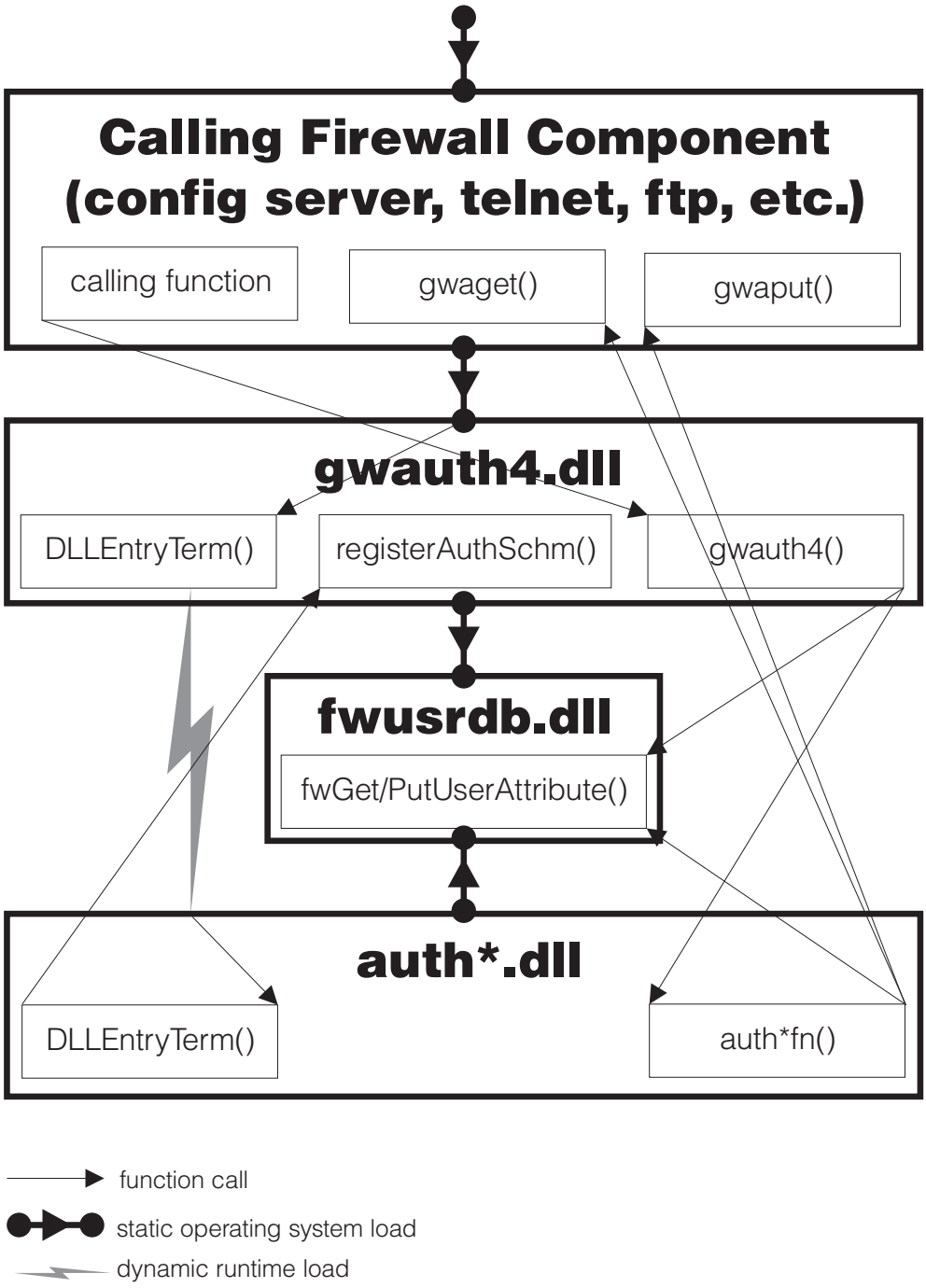

Figura 1. Registrazione ed inizializzazione della DLL

I componenti del firewall che richiedono di utilizzare i servizi di autenticazione si collegano ad una DLL del firewall denominata gwauth4. Quando la DLL gwauth4 viene caricata, la routine DLLEntryTerm viene richiamata e viene eseguito un tentativo di caricamento runtime di tutte le DLL in `ROOTDIR\bin\authschm`. Se una DLL dello schema di autenticazione non viene caricata correttamente, non verrà considerata come errore per il caricamento della dll gwauth4. La dll gwauth4 raggruppa questi tentativi di caricamento.

Quando viene eseguita la routine DLLEntryTerm degli schemi di autenticazione, questi ultimi vengono registrati con gwauth4.dll. Ciò avviene richiamando

registerAuthSchm. La dll authschm deve richiamare registerAuthSchm per ogni schema di autenticazione supportato dalla DLL. La struttura AuthSchmInfo passata sulla funzione registerAuthSchm associa il nome dello schema di autenticazione come memorizzato nel database utente con il punto di entrata della funzione AuthSchmFn. La funzione di registrazione effettua delle copie della struttura passata, in modo che la dll authschm possa riutilizzarla o, se necessario, modificarla. La DLL dello schema di autenticazione è anche responsabile della liberazione della struttura AuthSchmInfo.

La funzione registerAuthSchm è responsabile della creazione di un elenco collegato che rappresenta tutti gli schemi di autenticazione registrati. La routine DLLEntryTerm di gwauth4 inizializza l'ancora dell'elenco su NULL. Quindi, quando le DLL authschm richiamano la funzione registerAuthSchm:

1. Eseguire la scansione dell'elenco degli schemi di autenticazione in cerca di un'entrata che abbia lo stesso nome di quella trasferita. Se ne esiste una, eliminarla dall'elenco e cancellare tutta la memoria associata.
2. Creare una struttura AuthSchmEntry in base alla struttura AuthSchmInfo ed aggiungerla all'elenco degli schemi di autenticazione.
3. Restituire al chiamante un indicatore che notifichi se la registrazione è stata eseguita correttamente (GWA_OK) o meno (GWA_REGFAILED).

Dopo che la routine DLLEntryTerm di gwauth4 ha eseguito un caricamento runtime di ogni dll authschm e dopo che le DLL hanno registrato i propri schemi di autenticazione, la routine DLLEntryTerm di gwauth4 verrà restituita al chiamante. A questo punto gli altri componenti possono iniziare a richiedere i servizi di autenticazione richiamando la funzione gwauth4.

Quando gwauth4.dll viene scaricato, la routine DLLEntryTerm verrà richiamata ancora per l'elaborazione finale. Quando questa routine viene richiamata per l'elaborazione finale, verranno eliminate tutte le voci AuthSchmEntry su AuthSchmList e la memoria associata. In questa situazione, non è necessario cancellare la registrazione degli schemi di autenticazione dal firewall.

Elaborazione della richiesta di autenticazione: Quando un servizio del firewall deve autenticare un utente, richiama le funzioni contenute in gwauth4.dll. gwauth4 raccoglie le informazioni da questo componente ed interroga il database utente del firewall per ottenere il nome dello schema di autenticazione da utilizzare per elaborare la richiesta.

Una volta individuato il nome dello schema di autenticazione, gwauth4 esegue la scansione dell'elenco degli schemi di autenticazione registrati per trovarne uno con lo stesso nome. Dopo averlo trovato, crea una struttura AuthReq per rappresentare la richiesta corrente e richiama il punto di entrata nella DLL dello schema di autenticazione associata a quel nome.

La funzione AuthSchmFn richiamata da gwauth4 elabora la richiesta e richiama le routine callback gwaget e gwaput, a seconda dei casi, per interagire con l'utente finale. Quando l'elaborazione viene completata, restituisce il controllo a gwauth4 con il codice di errore appropriato.

gwauth4 scrive i record di log appropriati per documentare la richiesta di autenticazione e ritorna al componente del firewall che ha effettuato la richiesta, trasmettendo il codice di errore ricevuto dalla DLL dello schema di autenticazione.

Capitolo 6. Utilizzo del programma di utilità MKKF (Make Key File)

Per un collegamento di rete SSL sicuro è necessario che:

- sia stato configurato il server di configurazione per SSL
- sia stata creata una chiave per le comunicazioni sicure
- l'utente sia stato designato come root sicuro sul server
- sia stata nascosta la parola d'ordine del file di chiavi

Utilizzare MKKF per creare la chiave del server iniziale, il file di chiavi e la richiesta di certificato. MKKF viene utilizzato anche per ricevere il certificato iniziale in un file di chiavi e per nascondere la parola d'ordine del file di chiavi.

Creazione di un file di chiavi

Quando viene eseguito questo programma di utilità, è necessario che l'utente si sia collegato utilizzando il codice di contabilizzazione del responsabile di Windows NT.

1. Andare all'indirizzario ROOTDIR\config ed avviare il programma di utilità relativo alle chiavi immettendo:

   ```
   c:\program files\IBM\Firewall\config > mkkf

   MKKF Key Manager
   Copyright IBM Corp. 1996
   All Rights Reserved
   ```

2. Creare un nuovo file di chiavi.

   ```
   Key Ring Menu
   Currently Selected Key Ring: (none)

   N - Create New Key Ring File
   O - Open Key Ring File
   X - Exit

   Enter a command: n
   ```

   Immettere 'n' come indicato precedentemente per creare un nuovo file di chiavi.

   Viene richiesto di specificare un nome file per il file di chiavi. È possibile utilizzare un qualsiasi nome file che termini in .kyr. Per impostazione assunta, il firewall ricerca il file denominato fwkey.kyr.

   Immettere un nome per il file di chiavi oppure premere INVIO, se si accetta il valore assunto **fwkey.kyr**

   MKKF crea un nuovo file di chiavi e visualizza il relativo menu. Il file di chiavi viene elencato come il file di chiavi selezionato correntemente.

3. Creare un nuovo file di chiavi e la richiesta di certificato.

```
Key Ring Menu
Currently Selected Key Ring: fwkey.kyr

N - Create New Key Ring File
O - Open Key Ring File
S - Save Key Ring File
A - Save Key Ring as Another File
P - Set Password for Key Ring File
C - Create Stash File for Key Ring File
R - Receive a Certificate into a Key Ring File
W - Work with Keys and Certificates
X - Exit

Enter a command: w
```

Immettere 'w', come indicato, per andare al menu Chiave.

```
Key Menu
Currently Selected Key Ring: fwkey.kyr
Selected Key Entry: (none)

L - List/Select a key to work with
C - Create a New Key and Certificate Request
I - Import a key from an Armored key file
X - Exit this menu

Enter a command: c
```

Immettere 'c', come indicato precedentemente, per creare una nuova chiave.

Prima che una chiave possa essere memorizzata in un file di chiavi, questo deve essere protetto da una parola d'ordine. MKKF richiede all'utente di immettere una parola d'ordine da utilizzare per la protezione del file di chiavi. La parola d'ordine non viene visualizzata quando la si digita. MKKF richiede all'utente se desidera stabilire una data di scadenza per la parola d'ordine. Immettere 'n' come indicato di seguito:

```
Enter password to use for the key file:
password
Enter the password again for verification: password
Should the password expire?
Enter Y for yes or N for no:
n
Password successfully set.
Press ENTER to continue
```

MKKF richiede all'utente il tipo di chiave da creare.

```
Choose Certificate Type Menu
S - PEM Certificate Request Format (Private Enhanced Message)
P - PKCS10 Certificate Request Format
C - Cancel

Enter a command: s
```

Immettere 's', come indicato precedentemente, per creare un formato di richiesta certificato PEM. MKKF crea un certificato vuoto:

```
Compose Secure Server Certificate Menu

Current Certificate Information
Key Name: (none)
Key Size: 0
Server Name: (none)
Organization: (none)
Organization Unit: (none)
City/Locality: (none)
State/Province: (none)
Postal Code: (none)
Country: (none)

M - Modify the Certificate Fields
R - Ready To Create Key and Certificate Request
C - Cancel

Enter a command: m
```

Immettere 'm' per modificare il certificato vuoto. Vengono richieste ulteriori informazioni sul nuovo certificato:

- Immettere un nome da utilizzare. Questo nome può essere una qualsiasi stringa e viene utilizzato solo dal programma di utilità MKKF:

  ```
  Enter a name to use for the key entry:

  Firewall Key
  ```

- Immettere la dimensione della chiave. IBM Firewall invia solo la versione esportabile di MKKF. La dimensione massima della chiave è 1024.

  ```
  1:   508
  2:   512
  3:   768
  4:   896
  5:   1024
  Enter the number corresponding to the key size you want:

  2
  ```

- Immettere il nome host TCP/IP completo per il firewall (Ad esempio, jupiter.raleigh.ibm.com):

  ```
  Enter the server's fully qualified TCP/IP domain name or press
  Enter by itself to leave the field blank

  jupiter.raleigh.ibm.com
  ```

- Immettere un nome di organizzazione da associare al certificato, ad esempio, il nome della società:

  ```
  Enter Organization Name for the certificate
  or press ENTER by itself to leave the field blank.

  AAA Inc.
  ```

- Immettere il nome di un'unità organizzativa, ad esempio, il nome di un reparto:

  ```
  Enter Organizational Unit Name for the certificate
  or press ENTER by itself to leave the field blank.
  ```

  Network Security Products

- Immettere il nome della città in cui viene utilizzato il certificato:

  ```
  Enter Locality/City Name for the certificate
  or press ENTER by itself to leave the field blank.
  ```

  RTP

- Immettere lo stato o la provincia.

  Nota: In base alle specifiche per i certificati, questo campo deve essere composto da almeno tre caratteri, pertanto le abbreviazioni relative allo stato formate da due lettere non sono valide.

  ```
  Enter State/Province Name for the certificate
  or press ENTER by itself to leave the field blank.
  State/Province must be at least three characters long.
  ```

  N.C.

- Immettere un codice postale da associare al certificato.

  ```
  Enter Postal Code for the certificate
  or press ENTER by itself to leave the field blank.
  ```

  27709

- Immettere il codice del paese a due cifre:

  ```
  Enter Country Code for the certificate
  or press ENTER by itself to leave the field blank.
  Country code must be exactly two characters long.
  ```

  US

Dopo che MKKF ha raccolto tutte le informazioni, il certificato viene visualizzato:

```
Compose Secure Server Certificate Menu

Current Certificate Information
Key Name: Firewall Key
Key size: 512
Server Name: jupiter.raleigh.ibm.com
Organization: AAA Inc.
Organizational Unit: Network Security Products
City/Locality: RTP
State/Province N.C.
Postal Code: 27709
Country: US

M - Modify the Certificate Fields
R - Ready To Create Key and Certificate Request
C - Cancel

Enter a command: r
```

Se alcune informazioni del certificato sono errate, è possibile immettere 'm' per correggerle. Se le informazioni sono corrette, immettere 'r' per creare la nuova chiave ed il file di chiavi associato.

MKKF richiede all'utente un file in cui memorizzare il certificato. È possibile scegliere un qualsiasi nome file, ma si consiglia di utilizzare lo stesso nome di base del file di chiavi con l'aggiunta dell'estensione .cert:

```
Enter file to store the certificate request in:
fwkey.cert
Creating Private Key...
Private key was successfully created.
Creating certificate request...
certificate request was successfully created
Adding new key to key file.
The new key and certificate request were created successfully.
Press ENTER to continue
```

4. Utilizzare la chiave appena creata come valore assunto.

   Dopo aver creato la chiave ed il certificato, viene visualizzato il menu Chiave. La chiave appena creata viene elencata come entrata chiave selezionata:

```
Key Menu
Currently Selected Key Ring: fwkey.kyr
Selected Key Entry: Firewall Key

L - List/Select a Key To Work With
S - Show Information about Selected Key
D - Delete Selected key
C - Create a New Key and Certificate Request
I - Import a Key From an Armored Key File
E - Export Selected Key To an Armored Key File
F - Make Selected Key the Default Key for this Key Ring
U - Unmark Selected Key's Trusted Root Status
R - Create A Certificate Request for Selected Key
X - Exit This Menu

Enter a command: f
```

Utilizzare la chiave appena creata come chiave assunta nel file di chiavi. Immettere 'f' come indicato nell'esempio precedente. Viene richiesto di confermare l'azione:

```
Key Menu
Currently selected key: Firewall Key
Are you sure you want to make this key the default?
Enter Y for yes or N for No:
y
Key was made the default key.
Press ENTER to continue
```

Dopo che la chiave è stata contrassegnata come valore assunto, viene visualizzato il menu Chiave:

```
Key menu
Currently Selected Key Ring: fwkey.kyr
Selected Key Entry: Firewall Key

L - List/Select a Key To Work With
S - Show Information about Selected Key
D - Delete Selected key
C - Create a New Key and Certificate Request
I - Import a Key From an Armored Key File
E - Export Selected Key To an Armored Key File
F - Make Selected Key the Default Key for this Key Ring
U - Unmark Selected Key's Trusted Root Status
R - Create A Certificate Request for Selected Key
X - Exit This Menu

Enter a command: x
```

Uscire dal menu Chiave digitando 'x'.

5. Ricevere il certificato nel file di chiavi.

   Viene visualizzato il menu File di chiavi:

   ```
   Key Ring Menu
   Currently Selected Key Ring: fwkey.kyr

   N - Create New Key Ring File
   O - Open Key Ring File
   S - Save Key Ring File
   A - Save Key Ring as Another File
   P - Set Password for Key Ring File
   C - Create Stash File for Key Ring File
   R - Receive a Certificate into a Key Ring File
   W - Work with Keys and Certificates
   X - Exit

   Enter a command: r
   ```

   Nota: Poiché il firewall non utilizza SSL per l'autenticazione, non è necessario che il certificato venga rilasciato da un ente per la certificazione.

```
Enter file name or press ENTER for Cert.txt.
fwkey.cert
This is a self-signed certificate. Add it to the key file?
Enter Y for yes or N for no:
y
Certificate added to key ring.
Press ENTER to continue
```

6. Creare un file stash per il file di chiavi.

   Dopo che il certificato è stato aggiunto al file di chiavi, viene visualizzato il menu File di chiavi:

   ```
   Key Ring Menu
   Currently Selected Key Ring: fwkey.kyr

   N - Create New Key Ring File
   O - Open Key Ring File
   S - Save Key Ring File
   A - Save Key Ring as Another File
   P - Set Password for Key Ring File
   C - Create Stash File for Key Ring File
   R - Receive a Certificate into a Key Ring File
   W - Work with Keys and Certificates
   X - Exit

   Enter a command: c
   ```

   È necessario creare un file stash per il file di chiavi. Immettere 'c' come indicato nell'esempio precedente. MKKF utilizza lo stesso nome di base del file di chiavi con l'aggiunta dell'estensione .sth:

   ```
   Stashed password file saved to fwkey.sth
   Press ENTER to continue
   ```

   Dopo aver creato il file stash, viene visualizzato il menu File di chiavi:

   ```
   Key Ring Menu
   Currently Selected Key Ring: fwkey.kyr

   N - Create New Key Ring File
   O - Open Key Ring File
   S - Save Key Ring File
   A - Save Key Ring as Another File
   P - Set Password for Key Ring File
   C - Create Stash File for Key Ring File
   R - Receive a Certificate into a Key Ring File
   W - Work with Keys and Certificates
   X - Exit

   Enter a command: x
   ```

   Il file di chiavi è pronto per l'utilizzo. Immettere 'x', come indicato precedentemente, per uscire da MKKF e 'y' per salvare le modifiche apportate al file di chiavi:

```
Key ring file has been changed. Save?
Enter Y for yes or N for no:
y
Key ring saved to fwkey.kyr
Press ENTER to continue
#
```

7. Aggiornamento del file di configurazione.

   Dopo aver creato il file di chiavi, è necessario specificarne il nome nel file dei parametri del server di configurazione utilizzando il comando `fwcfgsrv`.

   Se viene utilizzata la crittografia SSL per il server di configurazione, occorre anche impostare l'opzione encryption=ssl utilizzando il comando `fwcfgsrv`.

   Dopo aver utilizzato il comando `fwcfgsrv`, arrestare e riavviare il servizio del server.

Capitolo 7. Prova e risoluzione dei problemi

Questo capitolo indica come risolvere alcuni dei problemi più comuni che possono verificarsi durante l'installazione e la configurazione di IBM Firewall.

Nel caso in cui si verifichi un problema, creare innanzitutto un `log firewall`, a priorità `debug`, per aumentare la quantità di informazioni inviate ai propri log. Per ulteriori informazioni, consultare “Gestione dei file di log” a pagina 5.

Installazione ed impostazione

Supporto filtro non riuscito

Spiegazione del problema Vengono ricevuti questi messaggi di errore.

```
Verifica del supporto filtro non riuscita.
Chiamata per la creazione del socket non riuscita.
Un file o un indirizzario del nome percorso non esiste.
```

Questo problema si è verificato perché non è stato rieseguito il boot del firewall dopo l'installazione.

Azione consigliata Rieseguire il boot del firewall e ritentare la procedura.

Problemi di instradamento

IBM Firewall fornisce una funzione nella casella di dialogo **Politica di sicurezza** denominata *Provare l'instradamento IP*, che può risultare utile per risolvere i problemi di instradamento. Abilitare questa casella di spunta, attivare la configurazione del collegamento e il log delle regole di collegamento. Quindi esaminare il `log firewall` per visualizzare le informazioni dettagliate su tutti i pacchetti che passano attraverso il firewall.

Eseguire queste prove utilizzando prima gli indirizzi IP e poi i nomi host. Se il traffico viene instradato in modo corretto utilizzando gli indirizzi ma non i nomi, consultare “Problemi relativi al DNS” a pagina 69 per ulteriori informazioni.

Impossibile eseguire il ping degli host dal firewall

Spiegazione del problema L'interfaccia di rete non è configurata in modo corretto.

Azione consigliata Consultare la documentazione relativa al sistema operativo.

Spiegazione del problema Il collegamento alla rete non sicura non è configurato in modo corretto.

Azione consigliata Contattare il fornitore dei servizi Internet.

Spiegazione del problema Se la rete sicura è isolata dietro ad un router, il firewall deve avere un instradamento statico al router. Utilizzare `netstat -rn` per verificare l'instradamento statico:

```
netstat -rn
```

L'emissione per il Protocollo di Famiglia 2 deve essere simile al seguente:

```
Destinazione  Gateway          Indicatori     ....
valore ass.  nrr.nrr.nrr.nrr  UG
nnn.nnn.nnn  nnn.nnn.nnn.nnn  U
sss.sss.sss  sss.sss.sss.sss  U
ss1.ss1.ss1  srr.srr.srr.srr  UG
127          127.0.0.1        U
```

Figura 2. Esempio di emissione di netstat -rn.

nrr.nrr.nrr.nrr rappresenta il router per Internet ed è l'instradamento assunto. L'instradamento assunto è un instradamento statico (Indicatore=UG).

nnn.nnn.nnn rappresenta il dominio non sicuro. Si tratta di un'interfaccia di instradamento (Indicatore=U).

nnn.nnn.nnn.nnn rappresenta l'interfaccia non sicura.

sss.sss.sss rappresenta il dominio sicuro. Si tratta di un'interfaccia di instradamento (Indicatore=U).

sss.sss.sss.sss rappresenta l'interfaccia sicura.

ss1.ss1.ss1 rappresenta un sottodominio all'estremità sicura della rete e srr.srr.srr.srr rappresenta il router a tale sottodominio. Si tratta di un'instradamento statico (Indicatore=UG).

127.0.0.1 è l'invio/ricezione o l'host locale. Si tratta di un'interfaccia di instradamento (Indicatore=U).

È necessario che ogni interfaccia abbia un instradamento e che l'instradamento assunto punti al router che si trova all'estremità non sicura del firewall.

Azione consigliata Aggiungere un instradamento statico al router. Contattare il responsabile del router. Utilizzare il comando `route add`.

Spiegazione del problema La maschera di sottorete sull'interfaccia sicura o l'host a cui l'utente sta tentando di collegarsi può non essere corretto.

Azione consigliata Utilizzare i programmi di utilità di configurazione del client per correggere le impostazioni della maschera.

Impossibile eseguire il ping degli host non sicuri dagli host sicuri (e viceversa)

Spiegazione del problema Ogni router adiacente al firewall deve contenere un instradamento statico che specifichi il firewall come gateway per le reti di destinazione al di là del firewall.

Azione consigliata Contattare il responsabile del router.

Spiegazione del problema Se la rete sicura utilizza indirizzi che non sono registrati e che non possono essere instradati sulla rete non sicura, inclusi gli indirizzi privati come specificato nella documentazione RFC 1597, i pacchetti non verranno reinstradati al mittente.

Azione consigliata Utilizzare un client con un indirizzo registrato.

Problemi relativi al DNS

Il DNS del firewall risolve i nomi interrogando il server nomi sicuro. Il server nomi sicuro risolve tutti i nomi nella rete sicura. Il server nomi sicuro invia le richieste per i nomi non sicuri al server nomi del firewall. Il server nomi del firewall interroga il server nomi non sicuro per risolvere la richiesta.

I problemi relativi al DNS possono influenzare altre aree operative del firewall. È buona norma controllare il DNS anche quando il problema non è esplicitamente collegato al DNS.

Di seguito sono riportati degli esempi che guidano l'utente attraverso tutte le fasi di questo metodo utilizzando il programma di utilità `nslookup` allo scopo di isolare il problema. In questi esempi vengono utilizzati i seguenti valori:

www.ibm.com rappresenta un nome host arbitrario sulla rete non sicura

nns.nns.nns.nns rappresenta l'indirizzo del server nomi non sicuro

sns.sns.sns.sns rappresenta l'indirizzo del server nomi sicuro

host.secure.company.com rappresenta il nome di un host arbitrario all'interno della rete sicura

127.0.0.1 rappresenta l'indirizzo di invio/ricezione del firewall.

Questi valori si trovano nella casella di dialogo **Servizi Nomi Dominio** del client di configurazione. Questi valori sono necessari quando si eseguono tali operazioni.

Nota: Il comando `nslookup` richiede il punto dopo il nome host per impedire che `nslookup` accodi il nome dominio sicuro dell'utente.

Il DNS non è stato ancora configurato

Spiegazione del problema Le funzioni DNS del firewall non sono state ancora configurate.

Azione consigliata Completare la casella di dialogo **Servizi Nomi Dominio**.

Errore o timeout delle interrogazioni DNS

Spiegazione del problema Il controllo del traffico del firewall non consente il flusso dei pacchetti DNS.

Azione consigliata Andare alla casella di dialogo **Politica di sicurezza**, selezionare la casella di spunta *Consentire interrogazioni DNS* e riattivare il controllo del traffico.

nslookup www.ibm.com. nns.nns.nns.nns non è riuscito

Spiegazione del problema Il server nomi non sicuro non sta utilizzando l'indirizzo indicato oppure non è configurato in modo corretto.

Azione consigliata Contattare il fornitore dei servizi DNS per un indirizzo del server nomi valido.

nslookup www.ibm.com. 127.0.0.1 non è riuscito

Spiegazione del problema È possibile che il `servizio DNS Microsoft` non sia in esecuzione. Andare al programma di gestione di controllo dei servizi per controllare se il servizio è in esecuzione.

Azione consigliata Utilizzare il programma di gestione di controllo dei servizi per avviare DNS.

nslookup host.secure.company.com. sns.sns.sns.sns non è riuscito

Spiegazione del problema Il server nomi sicuro non è attivo.

Azione consigliata Riavviare il server nomi.

nslookup www.ibm.com. sns.sns.sns.sns non è riuscito

Spiegazione del problema Il server nomi sicuro non è configurato in modo corretto per interagire con IBM Firewall.

Azione consigliata Per ulteriori informazioni sui requisiti di configurazione, consultare *IBM eNetwork Firewall - Guida per l'utente*.

Client di configurazione

Il server non risponde

Spiegazione del problema Il client ed il server di configurazione utilizzano linguaggi differenti.

Azione consigliata Nel pannello di logon del client di configurazione, selezionare il linguaggio con cui il firewall è stato installato.

Spiegazione del problema È possibile che la crittografia SSL non sia stata configurata in modo corretto.

Azione consigliata Assicurarsi che sia stata selezionata la crittografia SSL nel pannello di logon del client. Arrestare e riavviare il server di configurazione del firewall utilizzando il programma di gestione di controllo dei servizi.

Spiegazione del problema È possibile che il server di configurazione del firewall sia disabilitato.

Azione consigliata Assicurarsi che il server di configurazione del firewall sia in esecuzione.

Spiegazione del problema È possibile che il server di configurazione del firewall stia controllando una porta non standard.

Azione consigliata Esaminare `c:\winnt\system32\drivers\etc\services` ed assicurarsi che contenga la riga `ibmfwrcs 1014/tcp`. Se si desidera utilizzare il server su un'altra porta, editare `ibmfwrcs 1014/tcp` ed assicurarsi che la nuova porta venga specificata nel pannello di logon del client. Arrestare e riavviare il server di configurazione utilizzando il programma di gestione di controllo dei servizi.

Spiegazione del problema È possibile che al momento il controllo del traffico del firewall non consenta le comunicazioni da e verso il server di configurazione. Questo problema interessa soltanto i client di configurazione in esecuzione su un host remoto.

Azione consigliata Codificare un collegamento tra la macchina, su cui è in esecuzione il client di configurazione, ed il firewall. Il client di configurazione deve indicare l'origine del collegamento ed il firewall la destinazione. Ritentare l'operazione dopo aver attivato le modifiche. Per ulteriori informazioni, consultare *IBM eNetwork Firewall - Guida per l'utente*.

Spiegazione del problema È possibile che il server di configurazione non sia configurato per consentire il login da un host remoto.

Azione consigliata Utilizzare il comando `fwcfgsrv` per verificare che il parametro `localonly` sia impostato su no.

Impossibile collegarsi al server di configurazione

Spiegazione del problema Ogni nome utente autenticato sul firewall viene configurato per utilizzare uno qualsiasi dei diversi metodi di autenticazione. `Deny all` è utilizzato per negare l'utilizzo di un determinato servizio ad un utente.

Azione consigliata Esaminare i campi Gestione sicura e Gestione non sicura del nome utente che viene utilizzato. Questi campi sono validi solo per i responsabili e non per gli utenti del firewall.

Controllo del traffico

Mancata applicazione delle modifiche ai collegamenti

Spiegazione del problema modifiche apportate ai componenti del controllo del traffico non vengono applicate fin quando non saranno attivate, inclusa la casella di dialogo **Politica di sicurezza** sotto Gestione del sistema.

Azione consigliata Utilizzare la casella di dialogo **Attivazione collegamento** per rigenerare ed attivare la configurazione.

Server proxy

Nessun dato trasmesso

Spiegazione del problema I servizi proxy del firewall non vengono avviati fin quando non viene rieseguito il boot della macchina dopo l'installazione.

Azione consigliata Rieseguire il boot della macchina.

Spiegazione del problema Il controllo del traffico del firewall deve essere configurato per gestire il flusso dei pacchetti da e verso il processo proxy, non direttamente attraverso il firewall.

Azione consigliata Configurare ciascuna metà del collegamento proxy come descritto nel manuale *IBM eNetwork Firewall - Guida per l'utente*.

Utilizzare i servizi predefiniti quando è possibile, in modo particolare con il traffico FTP.

Impossibile collegarsi all'host desiderato

Spiegazione del problema Se i dati vengono trasmessi da e verso il proxy, ma l'utente non riesce a collegarsi all'host, è possibile che il client non stia risolvendo i nomi host in modo corretto.

Azione consigliata Assicurarsi che *Consentire interrogazioni DNS* sia abilitato nella casella di dialogo **Politica di sicurezza** e che sia stata attivata la configurazione del collegamento. Per ulteriori informazioni, consultare “Problemi relativi al DNS” a pagina 69.

Spiegazione del problema Ogni nome utente autenticato sul firewall dai servizi del firewall può essere configurato per utilizzare un qualsiasi metodo di autenticazione. `Deny all` è utilizzato per negare l'utilizzo di un particolare proxy ad un utente.

Azione consigliata Esaminare le impostazioni di autenticazione del codice di contabilizzazione nella casella di dialogo **Utenti** del client di configurazione.

Servizi di autenticazione

Il codice di contabilizzazione di un responsabile Windows NT non può essere autenticato

Spiegazione del problema Gli attributi del firewall per il codice di contabilizzazione del responsabile Windows NT sono memorizzati nel database dell'utente firewall sotto `fwdfadm`.

Azione consigliata Verificare che `fwdfadm` abbia impostato l'appropriato metodo di autenticazione per il servizio che si tenta di utilizzare.

L'utente proxy del firewall non può essere autenticato

Spiegazione del problema Se l'utente proxy del firewall non è definito nel database dell'utente firewall, il nome `fwdfuser` viene utilizzato per definire gli attributi dell'utente.

Azione consigliata Verificare che il metodo di autenticazione di `fwdfuser` sia definito correttamente per il servizio che l'utente sta tentando di utilizzare.

NAT (Network Address Translation)

Il collegamento NAT non funziona

Spiegazione del problema È stata impostata ed attivata la funzione NAT ma il collegamento non funziona.

Azione consigliata Esiste un problema relativo alle tabelle di instradamento o alla configurazione NAT.

Come stabilire un instradamento per i pacchetti NAT

Spiegazione del problema Non è stato stabilito alcun instradamento per i pacchetti NAT.

Azione consigliata Aggiungere un instradamento statico sul router davanti al firewall con la destinazione, l'indirizzo NAT ed il gateway del firewall.

Tool di debug disponibili per eseguire la funzione NAT

Spiegazione del problema Quali tool di debug sono disponibili per eseguire NAT?

Azione consigliata Il log di NAT, che consente di tracciare la gestione degli indirizzi registrati dinamici.

Funzioni di log

Le modifiche delle funzioni di log non sono valide per il server

Spiegazione del problema L'eliminazione o la modifica di una funzione di log viene eseguita sulla GUI, pertanto non è valida sul server.

Azione consigliata Rieseguire il boot del sistema.

Programmi di utilità per i prospetti

Errore nell'accesso al file:

Spiegazione del problema È possibile visualizzare l'errore utilizzando uno dei seguenti comandi:

```
db2 -vf fwschema.dll > schema.out
db2 -vf fwimport.dat > import.out
db2 -vf fwqrysmp.dml > sample.out
```

Azione consigliata Fornire i nomi file completi corretti per il file .ddl, .dat o .dml.

Errore durante l'importazione dei dati nel database

Spiegazione del problema Il file import.out generato dal comando `db2 -vf fwimport.dat>import.out` contiene messaggi indicanti che una delle importazioni non è stata eseguita correttamente o che è stata eseguita solo in parte.

Azione consigliata Controllare il file .msg corrispondente all'istruzione di importazione che ha determinato la notifica del problema. Verranno fornite ulteriori informazioni. Ricercare i record correlati nel file .tbl corrispondente per controllare i dati di immissione e per individuare la causa dell'errore. Ad esempio, la stringa di dati è troppo lunga per la colonna di destinazione del database? Il tipo di dati è appropriato per il

tipo di colonna di destinazione? Se i dati di immissione non sono corretti, è necessario localizzare il record del file di log originario per assicurarsi che `fwlogtbl` abbia generato il record del file .tbl in modo corretto.

Se il problema persiste, salvare i file import.out e .msg, il file .tbl associato ed il file di log originario prima di contattare l'assistenza IBM.

Appendice A. Messaggi

Questa appendice contiene messaggi per IBM Firewall per AIX, IBM Firewall per NT e alcuni messaggi comuni per entrambi i firewall. Fornisce anche le seguenti informazioni sui messaggi di IBM Firewall :

- Come vengono formattati i messaggi
- I livelli di gravità dei messaggi
- I messaggi e le relative spiegazioni

Se dopo aver letto il messaggio e la relativa spiegazione sono necessarie ulteriori informazioni, fare riferimento al Capitolo 7, “Prova e risoluzione dei problemi” a pagina 67.

Tag di messaggio

ICA I primi 3 byte fissi.

xxxx Un numero compreso tra 0000 e 9999.

a Un indicatore di gravità. I messaggi vengono classificati in base al livello di gravità.

- i – info
- w – avvertenza
- e – errore
- s – grave

I numeri da 0000 a 9999 vengono classificati ulteriormente nelle seguenti categorie:

- da 0000 a 0999 Segnale di intrusione
- da 1000 a 1999 Filtri
- da 2000 a 2999 Proxy
- da 3000 a 3999 Socks
- da 4000 a 4999 Cercapersone
- da 5000 a 8999 Messaggi disponibili
- da 9000 a 9999 Messaggi generici

Messaggi

ICA0001 ATTENZIONE - *numero* **errori di autenticazione**

Spiegazione: Le condizioni di soglia per gli errori di autenticazione sono state soddisfatte.

ICA0002 ATTENZIONE - *numero* **errori di autenticazione per utente** *nome_utente***.**

Spiegazione: Le condizioni di soglia per il rilevamento di un determinato messaggio di log sono state soddisfatte.

ICA0003 ATTENZIONE - *numero* **errori di autenticazione dall'host** *indirizzo IP dell'host***.**

Spiegazione: Le condizioni di soglia per gli errori di autenticazione da un determinato host sono state soddisfatte.

ICA0004 ATTENZIONE - Tag *id_messaggio* **con** *numero* **entrate di log.**

Spiegazione: Le condizioni di soglia per il rilevamento di un determinato messaggio di log sono state soddisfatte.

ICA0005 Controllo log - memoria esaurita.

Spiegazione: Il processo ha esaurito la memoria.

ICA0006 Controllo log - errore di accesso al file di servizi:*errno*

Spiegazione: Non è stato possibile trovare l'entrata per fwlogmond in /etc/services.

ICA0007 Controllo log - creazione del socket non riuscita: *errno*

Spiegazione: Non è stato possibile aprire il socket - fare riferimento al messaggio di errore.

ICA0016 Non è stato possibile aprire *file id processo* **- è possibile che il daemon sia già attivo.**

Spiegazione: Il daemon non è riuscito ad aprire il file id processo.

ICA0017 Non è stato possibile scrivere l'id processo (*id processo***) su** *file***.**

Spiegazione: Il daemon non è riuscito a scrivere l'id processo sul file.

ICA0018 Controllo log - lettura vuota.

Spiegazione: È stato ricevuto un pacchetto che non conteneva dati - è stato eliminato.

ICA0019 Controllo log - lettura breve. Tag eliminata.

Spiegazione: È stato ricevuto un pacchetto che conteneva un numero insufficiente di dati - è stato eliminato.

ICA0020 Controllo log - formato della tag ICA errato.

Spiegazione: È stato ricevuto un pacchetto che presentava dati in formato errato - è stato eliminato.

ICA0021 Controllo log - formato dei dati di autenticazione errato.

Spiegazione: È stato ricevuto un pacchetto che presentava dati in formato errato - è stato eliminato.

ICA0022 Sintassi non valida nel file di definizione della soglia (*entrata non valida***).**

Spiegazione: La sintassi dell'entrata indicata nel file della soglia non è corretta.

ICA0023 Impossibile aprire il file fwmail.conf.

Spiegazione: L'apertura del file fwmail.conf non è riuscita o il file è vuoto.

ICA0024 Impossibile eseguire il collegamento al server SMTP.

Spiegazione: Il server SMTP è in esecuzione o rifiuta il collegamento.

ICA0025 Invio del messaggio di attenzione non riuscito.

Spiegazione: Non è stato possibile inviare il messaggio di attenzione del controllo log all'indirizzo specificato.

ICA0051 Il numero di giorni per la conservazione nel file di log, *nome file log***, deve essere un numero intero piccolo senza segno.**

Spiegazione: Il numero di giorni per la conservazione nel file di log deve essere un numero intero valido.

ICA0052 Il numero di giorni per la conservazione in archivio, *nome file log***, deve essere un numero intero piccolo senza segno.**

Spiegazione: Il numero di giorni per la conservazione in archivio deve essere un numero intero valido.

ICA0053 Non sono consentite più entrate per il file di log, *nome file log***, in logmgmt.cfg.**

Spiegazione: Non sono consentite più entrate per il file di log in logmgmt.cfg.

ICA0054 Impossibile aprire il file *$ Variabili :***.**

Spiegazione: Impossibile aprire il file logmgmt.cfg.

ICA0055 Nessuna entrata valida nel file logmgmt.cfg.

Spiegazione: Nessuna entrata valida nel file logmgmt.cfg.

ICA0056 Il messaggio di log,"*$ Variabili :***", non è valido**

Spiegazione: Il messaggio di log non è valido.

ICA1001 Impossibile creare il file con l'ID processo

Spiegazione: Il daemon di log del filtro ha rilevato un errore durante la scrittura del file fwlogd.pid.

Risposta dell'utente: Controllare il sistema di file in cui risiede l'indirizzario /etc/security. È possibile che si sia verificata una condizione di spazio esaurito.

ICA1002 Comunicazione con il programma cfgfilt impossibile

Spiegazione: Poiché il file fwlogd.pid non è stato creato, la comunicazione tra il daemon fwlogd e l'applicazione fgfilt (richiesta per il controllo del filtro) non può essere stabilita.

Risposta dell'utente: Controllare il sistema di file in cui risiede l'indirizzario /etc/security. È possibile che si sia verificata una condizione di spazio esaurito.

ICA1003 Continuazione dell'inizializzazione del daemon di log

Spiegazione: Il daemon fwlogd continua l'elaborazione di avvio.

ICA1004 Daemon di log del filtro *fwlogd* **(livello** *versione***.***rilascio***) inizializzato alle** *ora* **del** *data*

Spiegazione: Il daemon di log del pacchetto IP è stato avviato. Se il log del pacchetto è abilitato, il daemon fwlogd scrive i record richiesti su syslog, local4, file.

ICA1005 Log dei messaggi di pacchetto *numero_regola_filtro* **soppresso a causa di eccedenza del buffer**

Spiegazione: Il buffer di log del filtro del daemon fwlogd è in eccedenza. Impossibile eseguire il log di un pacchetto per la regola di filtro specificata.

Risposta dell'utente: Controllare il log. È possibile che sia stato tentato un accesso non autorizzato al firewall o che siano stati registrati dei messaggi non richiesti. Ad esempio, i messaggi broadcast devono avere una regola 'deny' ed il controllo log impostato su no (l=n), per impedire la registrazione nel log.

ICA1006 Errore grave di fwlogd - *funzione errata***:** *messaggio di errore*

Spiegazione: Il server fwlogd non è riuscito ad eseguire la funzione indicata, il daemon è stato arrestato.

Risposta dell'utente: Correggere l'errore di sistema indicato e riavviare fwlogd.

ICA1007 Impossibile eseguire fork sul processo child: *errno*

Spiegazione: Durante l'avvio del daemon di log del filtro, si è verificato l'errore di sistema indicato.

Risposta dell'utente: In base all'errore visualizzato, eseguire la correzione appropriata.

ICA1008 Errore restituito dalla routine setpgrp: *errno*

Spiegazione: Durante l'avvio del daemon di log del filtro si è verificato l'errore di sistema indicato.

ICA1009 Impossibile eseguire fork sul secondo processo child: *errno*

Spiegazione: Durante l'avvio del daemon di log del filtro si è verificato l'errore di sistema indicato.

ICA1010 Questo daemon deve essere eseguito con autorizzazione di root

Spiegazione: Il daemon di log del filtro deve essere avviato con l'autorizzazione di root.

Risposta dell'utente: Riavviarlo con l'autorizzazione di root.

ICA1011 Chiamata sysconfig per interrogare l'estensione kernel *percorso_caricamento* **non riuscita:** *errno*

Spiegazione: Durante l'avvio del daemon di log del filtro, si è verificato l'errore di sistema indicato.

ICA1012 Estensione kernel AIX *netinet* **non caricata -- impossibile continuare**

Spiegazione: Il programma di controllo unità **netinet** non ha il supporto filtro.

Risposta dell'utente: Installare il programma del firewall. Potenzialmente, il programma è stato installato ma non è stato rieseguito il *boot*.

ICA1013 Chiamata per la creazione del socket non riuscita: *errno*

Spiegazione: Durante l'avvio del daemon di log del filtro, si è verificato l'errore di sistema indicato.

ICA1014 Programma di controllo unità netinet di AIX non al livello richiesto

Spiegazione: Il programma di controllo unità netinet ed il daemon fwlogd non sono allo stesso livello.

Risposta dell'utente: Risolvere il conflitto, è possibile che occorra rieseguire il boot dopo l'installazione del nuovo livello del firewall.

ICA1015 Errore restituito dalla chiamata ioctl() (SIOCGFWLOG): *errno*

Spiegazione: Durante l'avvio del daemon di log del filtro, si è verificato l'errore di sistema indicato.

ICA1016 Impossibile richiamare la coda di log corrente differita

Spiegazione: Ulteriori informazioni sono associate al precedente messaggio di log.

ICA1017 Errore restituito dalla chiamata SIOCGFWLOG ioctl()

Spiegazione: Durante l'avvio del daemon di log del filtro, si è verificato l'errore di sistema indicato.

ICA1018 Errore grave di fwlogd - *funzione errata***:** *messaggio di errore di sistema*

Spiegazione: Il server fwlogd non è riuscito ad eseguire la funzione indicata, il daemon è stato arrestato.

Risposta dell'utente: Correggere l'errore di sistema indicato e riavviare fwlogd.

ICA1019 Uscita per errore imprevisto con rc *codice_errore_fw_interno*

Spiegazione: Durante l'avvio del daemon di log del filtro, si è verificato l'errore di sistema indicato.

ICA1020 Errore grave di fwlogd - *funzione in errore***: codice di errore = 0x***codice di errore della funzione*

Spiegazione: Il server fwlogd non è riuscito ad eseguire la funzione indicata, il daemon è stato arrestato.

Risposta dell'utente: Correggere l'errore di sistema indicato e riavviare fwlogd.

ICA1021 Errore nell'apertura di */dev/ipsp_poif***:** *errno*

Spiegazione: Il programma di controllo unità non è stato installato.

Risposta dell'utente: Se il programma del firewall è stato installato, controllare il file /tmp/rc/net.out per possibili messaggi di errore.

ICA1022 Verifica del supporto filtro non riuscita

Spiegazione: A causa di un errore registrato prima di questo messaggio, il supporto filtro non può essere verificato.

ICA1023 Errore nella chiamata ioctl() (SIOCGFWLVL): *errno*

Spiegazione: Durante l'avvio del daemon di log del filtro, si è verificato l'errore di sistema indicato.

Risposta dell'utente: Eseguire una delle seguenti operazioni:

- Per AIX: Verificare che sia stato installato il livello corretto del programma di controllo unità netinet e che sia stato rieseguito il boot della macchina dopo l'installazione.
-

ICA1036 *#:rule_noR: rule_type direction: interface s:src_addr d: dst_addr p: protocol tag: scr_port/icmp_type tag: dst_port/icmp_code r:routed/local a: secure/non_secure f:yes/no T:tunnel_id e:C/D/n l:packet_length*

Spiegazione: Il record di log che indica un pacchetto IP elaborato e la regola di filtro corrispondente. Per eseguire la scrittura del record, il controllo log della regola di filtro mappata deve essere impostato su *sì*. Se il pacchetto IP corrispondente a questa regola è un frammento, le informazioni relative al tipo/codice porte/icmp vengono visualizzate per il pacchetto delle intestazioni, mentre per gli altri pacchetti viene visualizzato zero.

ICA1037 *#:rule_no action src_addr src_mask dst_addr dst_mask protocol logical_op value logical_op value interface_type routing directionl= log_control f=fragment_controlt= tunnel_ID enc_alg auth_alg*

Spiegazione: Quando le regole di filtro vengono aggiornate, quelle attive vengono scritte nel log. Questo messaggio di log descrive una delle regole attivate.

ICA1038 **Processo delle Chiavi di Sessione avviato, utilizzate la porta del socket di sessione:***num_porta* **e la porta del socket principale:***num_porta*

Spiegazione: Il tunnel di crittografia è stato avviato utilizzando i numeri di porta UDP specificati, come definito in /etc/services.

ICA1039 **(Ri)definizione in corso della politica come:**

Spiegazione: La cache della politica viene (ri)definita utilizzando il file /etc/security/fwpolicy. Le seguenti righe indicano la nuova cache della politica.

ICA1040 >**Istruzione per la politica:** *origine_tunnel fine_tunnel ID_tunnel indicatore_crittografia/indicatore_autenticazione*

Spiegazione: La riga registrata è stata letta dal file /etc/security/fwpolicy.

ICA1041 **Specifica di contesto eliminato per il tunnel:** *ID_tunnel*

Spiegazione: Il contesto del tunnel, per l'ID indicato, non è più operativo.

ICA1042 **Vengono definite le seguenti specifiche di contesto del tunnel:**

Spiegazione: Le specifiche di contesto vengono definite come indicato nei seguenti record di log.

ICA1043 >**ID_tunnel:***numero***, indirizzo_origine:***indirizzo_IP***, indirizzo_destinazione:***indirizzo_IP***, crittografia** *algoritmo*

Spiegazione: Il messaggio elenca gli attributi specifici del contesto del tunnel attivato.

ICA1044 **Avvertenza numero di host: limite IP(***indirizzo IP***) superato**

Spiegazione: Troppi host sicuri tentano di collegarsi alla macchina firewall.

Azione del sistema: Accettare i collegamenti.

ICA1045 **Limite TCP superato:** *indirizzo IP***(***Porta***)->***indirizzo IP***(***Porta***) rifiutato**

Spiegazione: Troppe sessioni TCP tentano di passare attraverso la macchina firewall.

Azione del sistema: Rifiutare i collegamenti.

ICA1046 Limite UDP superato: *indirizzo IP*(*Porta*)->*indirizzo IP*(*Porta*) **rifiutato.**

Spiegazione: Troppe sessioni UDP tentano di passare attraverso la macchina firewall.

Azione del sistema: Rifiutare i collegamenti.

ICA1047 Avvertenza periodo di deroga : troppe sessioni TCP, *indirizzo IP*(*Porta*)->*indirizzo IP*(*Porta*) **passate**

Spiegazione: Troppe sessioni TCP tentano di passare attraverso la macchina firewall.

Azione del sistema: Accettare i collegamenti.

ICA1048 Avvertenza periodo di deroga : troppe sessioni UDP, *indirizzo IP*(*Porta*)->*indirizzo IP*(*Porta*) **passate**

Spiegazione: Troppe sessioni UDP tentano di passare attraverso la macchina firewall.

ICA1049 Pacchetto ipsec non valido: s:*indirizzo IP* **d:***indirizzo IP* **protocollo:***protocollo* **spi:***indice parametri di sicurezza*

Spiegazione: Il pacchetto ipsec non può essere decapsulato dal firewall ricevente.

Risposta dell'utente: Assicurarsi che la definizione di tunnel sia stata esportata correttamente ed attivata su ogni firewall.

ICA1050 Specifica eliminata per il tunnel:*tunnel_ID*

Spiegazione: La specifica del tunnel, per l'ID indicato, non è più operativa.

ICA1051 Vengono definite le seguenti specifiche del tunnel:

Spiegazione: Le specifiche del tunnel vengono definite come indicato nei seguenti record di log.

ICA1052 >**ID_tunnel:***numero*, **indirizzo_origine:***indirizzo_IP*, **indirizzo_destinazione:***indirizzo_IP*, **crittografia_origine:***algoritmo* **crittografia_remota:***algoritmo***macchina_origine:***algoritmo* **macchina_remota:***algoritmo***macchina_crittografia_origine:***algoritmo* **macchina_crittografia_remota:***algoritmo* **politica_origine:***politica***politica_remota:***politica* **modo:***modo_trasporto*

Spiegazione: Il messaggio elenca gli attributi specifici del tunnel attivato.

ICA1200 Accesso in corso del daemon di log a causa degli errori riportati precedentemente

Spiegazione: A causa degli errori riportati precedentemente, il daemon fwlogd viene arrestato.

Azione del sistema: Il log del filtro IP non verrà attivato.

Risposta dell'utente: Correggere gli errori indicati e riavviare fwlogd.

ICA1260 Arresto in corso del daemon di log alle *ore* **del** *data* **per ricezione segnale** *arresto*

Spiegazione: Il daemon fwlogd che ha ricevuto il segnale di arresto indicato viene arrestato.

ICA1305 \"sconosciuto\"

Spiegazione: Durante la formattazione di un pacchetto IP per syslog, è stato trovato un record con la specifica di protocollo sconosciuta. I protocolli IP, ICMP, TCP, UDP e IPSP sono protocolli riconosciuti. IPSP è designato dall'IBM per i pacchetti codificati che passano attraverso un tunnel.

ICA1400 Errore grave di fwtimernat - *funzione errata***:** *messaggio di errore di sistema*

Spiegazione: Il server fwtimernat non è riuscito ad eseguire la funzione indicata. Il server fwtimernat è stato terminato.

Risposta dell'utente: Correggere l'errore di sistema indicato e riavviare fwtimernat.

ICA1401 Errore grave di fwtimernat - *funzione errata***:** *messaggio di errore di sistema*

Spiegazione: Il server fwtimernat non è riuscito ad eseguire la funzione indicata. Il server fwtimernat è stato terminato.

Risposta dell'utente: Correggere l'errore di sistema indicato e riavviare fwtimernat.

ICA1402 Errore grave di fwtimernat - *funzione errata***:** *messaggio di errore*

Spiegazione: Il server fwtimernat non è riuscito ad eseguire la funzione indicata. Il server fwtimernat è stato terminato.

Risposta dell'utente: Correggere l'errore di sistema indicato e riavviare fwtimernat.

ICA2000 Nuova sessione FTP a *indirizzo_IP* **da** *indirizzo_IP* **(sito non sicuro).**

Spiegazione: Avvio di una nuova sessione ftp da un sito non sicuro.

ICA2001 Autenticazione non riuscita per utente *nome* **(sconosciuto) da** *ftp di rete***:***indirizzo_IP***.**

Spiegazione: Un utente, senza codice di contabilizzazione, ha tentato di utilizzare il proxy ftp dalla rete.

Risposta dell'utente: Contattare il responsabile del firewall per impostare il codice di contabilizzazione del proxy.

ICA2002 Autenticazione non riuscita per utente *nome* **con** *metodo di autenticazione* **da** *rete***:** *nome host***.**

Spiegazione: Il firewall non può eseguire l'autenticazione del nome utente indicato con il metodo di autenticazione specificato.

Risposta dell'utente: Contattare il responsabile del firewall.

ICA2003 Nessuna shell configurata per *nome utente***.**

Spiegazione: L'utente identificato ha tentato di eseguire un login al proxy ma non è stata definita alcuna shell.

Risposta dell'utente: Contattare il responsabile del firewall per correggere questo profilo di login utente.

ICA2004 Ricevuto evento di controllo sconosciuto di 0x*valore_esadecimale***.**

Spiegazione: È stata ricevuta una richiesta di controllo sconosciuta dal modulo tcpip_audit.c.

ICA2005 Errore nella scrittura al client: *errno***.**

Spiegazione: Impossibile comunicare con il client, consultare i messaggi di sistema registrati.

ICA2006 ptelnetd: auditproc: *errno***.**

Spiegazione: L'errore indicato è stato restituito dal processo di controllo telnet. Possibile danneggiamento dei file di sistema.

ICA2007 ptelnetd: errore grave stato=*valore***.**

Spiegazione: Rilevato errore sconosciuto. Possibile danneggiamento dei file di sistema.

ICA2008 Un utente non firewall *nome* **da :***indirizzo IP* **ha tentato di utilizzare il proxy telnet.**

Spiegazione: Un utente, senza codice di contabilizzazione, ha tentato di utilizzare il proxy telnet.

Azione del sistema: Utilizzare l'autenticazione generica.

ICA2009 /bin/login: *errno***.**

Spiegazione: Errore grave durante il login di sistema. Consultare i messaggi di errore del sistema indicati.

ICA2010 Collegamento a *indirizzo_IP* **da** *indirizzo_IP* **(non sicuro).**

Spiegazione: Collegamento riuscito tra gli indirizzi IP indicati attraverso l'interfaccia non sicura.

ICA2011 Collegamento a *indirizzo_IP* **da** *indirizzo_IP* **(sicuro).**

Spiegazione: Collegamento riuscito tra gli indirizzi IP indicati attraverso l'interfaccia sicura.

ICA2012 Nuova sessione FTP a *indirizzo_IP* **da** *indirizzo_IP* **(sito sicuro).**

Spiegazione: Avvio di una nuova sessione ftp.

ICA2013 Nuova sessione Telnet a *indirizzo_IP* **da** *indirizzo_IP***.**

Spiegazione: Stabilita una nuova sessione telnet.

ICA2014 Opzione *valore* **non supportata.**

Spiegazione: Questo indicatore non è supportato, fare riferimento al messaggio precedente.

ICA2015 Opzione -*valore* **non supportata.**

Spiegazione: Questo indicatore non è supportato, fare riferimento al messaggio precedente.

ICA2016 ID utente remoto \"*nome***\".**

Spiegazione: Richiesta di collegamento ftp per l'utente indicato.

ICA2017 Debug - *alla riga***.**
ICA2018 Chiave SNK non trovata per utente *nome***.**

Spiegazione: Il valore SecureNetKey non è stato trovato per l'ID utente indicato.

Risposta dell'utente: Contattare il responsabile del firewall per possibili problemi di configurazione del login.

ICA2019 Chiave SNK non letta correttamente per utente *nome***.**

Spiegazione: Il valore SecureNetKey non è stato letto come cifra ottale per l'ID utente indicato.

Risposta dell'utente: Contattare il responsabile del firewall per possibili problemi di configurazione del login.

ICA2020 /usr/bin/fwuserau o /usr/bin/fwuserpt non esiste.

Spiegazione: Il metodo di autenticazione fornito dall'utente si è interrotto.

Azione del sistema: L'autenticazione viene interrotta.

Risposta dell'utente: Assicurarsi che /usr/bin/fwuserau e /usr/bin/fwuserpt esistano e che il proprietario sia root. Se l'eseguibile non esiste, l'utente deve crearlo utilizzando un programma di compilazione compatibile con il sistema operativo del firewall e denominarlo /usr/bin/fwuserau o /usr/bin/fwuserpt.

ICA2021 Tentativo di collegamento all'host remoto *nome* **con ID utente** *nome***.**

Spiegazione: Viene eseguito il tentativo di stabilire un nuovo collegamento ftp.

ICA2022 Tentativo di collegamento all'host remoto *nome***.**

Spiegazione: Viene eseguito il tentativo di stabilire un nuovo collegamento ftp.

ICA2023 Uso: ptelnetd [-n] [-s].

Spiegazione: È stato specificato un indicatore sconosciuto durante l'avvio del daemon ptelnet.

Risposta dell'utente: Utilizzare solo gli indicatori -n e/o -s.

ICA2024 Utente *nome* **autenticato correttamente mediante** *metodo* **autenticazione da** *rete***:** *nome host***.**

Spiegazione: Il firewall ha eseguito l'autenticazione del nome utente indicato utilizzando il metodo di autenticazione specificato.

ICA2025 Utente *nome* **collegato mediante** *metodo* **autenticazione da** *rete***:** *nome host***.**

Spiegazione: Utente ftp collegato.

ICA2026 Timeout dell'utente *nome* **dopo** *n* **secondi alle** *ora corrente***.**

Spiegazione: Timeout del tentativo di collegamento per l'utente specificato. È possibile che ci sia un problema di instradamento della rete o che l'host remoto non sia disponibile.

ICA2027 Collegamento da *host remoto* **alle** *ora***.**

Spiegazione: È stato stabilito il collegamento ftp di rete al firewall.

ICA2028 Tentativo di collegamento FTP a *indirizzo_IP* **da** *indirizzo_IP* **rifiutato. Questa macchina non supporta FTP da siti non sicuri.**

Spiegazione: Generalmente indica il tentativo di stabilire un collegamento ftp al firewall mediante l'interfaccia non sicura.

Azione del sistema: Rifiutare il collegamento.

ICA2029 Errore di sistema con errno = - **in** *in* **linea** *linea***.**

Spiegazione: È stato rilevato un problema durante l'esecuzione di una chiamata di sistema.

Azione del sistema: L'esecuzione di sistema è stata arrestata.

Risposta dell'utente: Richiamare il log, determinare la causa dell'errore e cercare di risolvere il problema. Se il problema persiste, contattare l'assistenza IBM.

ICA2030 Chiamata di funzione con codice di errore = - **in** *in* **linea** *linea***.**

Spiegazione: La chiamata di funzione ha riscontrato un problema.

Azione del sistema: L'errore viene restituito.

Risposta dell'utente: Richiamare il log, determinare la causa dell'errore e cercare di risolvere il problema. Se il problema persiste, contattare l'assistenza IBM.

ICA2031 Chiamata di funzione sdi creadcfg() rc = -**.**

Spiegazione: La chiamata di funzione ha riscontrato un problema.

Azione del sistema: L'errore viene restituito.

Risposta dell'utente: Per ulteriori informazioni, consultare il manuale che fa riferimento a sdi.

ICA2032 Collegamento interrotto.

Spiegazione: Il collegamento ftp è stato interrotto.

Risposta dell'utente: Ristabilire la sessione.

ICA2033 Chiamata di funzione sdi sd_init rc = -**.**

Spiegazione: La chiamata di funzione ha riscontrato un problema.

Azione del sistema: L'errore viene restituito.

Risposta dell'utente: Per ulteriori informazioni, consultare il manuale che fa riferimento a sdi.

ICA2034 Chiamata di funzione sdi sd_check rc = -**.**

Spiegazione: La chiamata di funzione ha riscontrato un problema.

Azione del sistema: L'errore viene restituito.

Risposta dell'utente: Per ulteriori informazioni, consultare il manuale che fa riferimento a sdi.

ICA2035 setsockopt(): *errno***.**

Spiegazione: Errore di sistema nella chiamata setsocketopt.

ICA2036 Sessione Telnet *ID sessione* **avviata per utente** *ID utente* **(***indirizzo IP origine***:***indirizzo IP destinazione***).**

Spiegazione: Questo messaggio viene generato all'avvio di ogni sessione Telnet. Una sessione viene avviata quando l'ID utente, l'indirizzo IP di origine e quello di destinazione sono noti al firewall. L'ID sessione è un identificativo univoco generato dal firewall.

ICA2037 Tentativo di collegamento dell'utente fwdfuser o fwdpuser non consentito.

Spiegazione: fwdfuser e fwdpuser sono utenti riservati e non devono essere utilizzati.

Azione del sistema: Collegamento rifiutato.

Risposta dell'utente: Il responsabile deve individuare chi sta utilizzando questo utente.

ICA2038 ttloop: peer arrestato: *errno***.**

Spiegazione: Si è verificato un errore durante lo svuotamento del buffer di emissione della rete. È possibile che il processo peer si sia arrestato.

ICA2039 ttloop: lettura: *errno***.**

Spiegazione: Si è verificato un errore durante lo svuotamento del buffer di emissione della rete.

ICA2040 L'autenticazione impostata su password, none o snk non è consentita per l'ID utente fwdfuser.

Spiegazione: fwdfuser è un ID utente riservato e non deve utilizzare password o none come metodo di autenticazione.

Azione del sistema: Collegamento rifiutato.

Risposta dell'utente: Il responsabile deve modificare il metodo di autenticazione per l'ID utente fwdfuser.

ICA2041 Sessione FTP *ID sessione* **avviata per** *ID utente* **(***indirizzo IP origine***:***indirizzo IP destinazione***).**

Spiegazione: Questo messaggio viene generato all'avvio di ogni sessione FTP. Una sessione viene avviata quando l'ID utente, l'indirizzo IP di origine e quello di destinazione sono noti al firewall. L'ID sessione è un identificativo univoco generato dal firewall.

ICA2042 req_rsp_code impostato in modo errato su FW_AUTH_REQ.

Spiegazione: fw_tn_authenticate non è consentito per impostare req_rsp_code su FW_AUTH_REQ.

Azione del sistema: Interrompere l'autenticazione.

Risposta dell'utente: Modificare fw_tn_authenticate, ricreare la libreria fwuser.o ed inserirla nel firewall.

ICA2043 Non è stato possibile richiamare la parola d'ordine per *nome_utente***.**

Spiegazione: Il tipo di autenticazione per questo utente è 'password' ma non è stata trovata alcuna parola d'ordine.

Risposta dell'utente: Contattare il responsabile del firewall.

ICA2044 Tempo (*valore***) specificato per -t errato.**

Spiegazione: Il valore di tempo indicato contiene dei caratteri che non sono compresi nell'intervallo da 0 a 9 o supera il valore massimo consentito.

ICA2045 Opzione -T non supportata sul firewall.

Spiegazione: L'opzione indicata non è supportata.

ICA2046 Opzione -k non supportata sul firewall.

Spiegazione: L'opzione indicata non è supportata.

ICA2047 Opzione -s non supportata sul firewall.

Spiegazione: L'opzione indicata non è supportata.

ICA2048 Opzione -u non supportata sul firewall.

Spiegazione: L'opzione indicata non è supportata.

ICA2049 Indicatore sconosciuto -*valore* **ignorato.**

Spiegazione: L'indicatore specificato non è noto.

ICA2050 Parametro sconosciuto *valore***.**

Spiegazione: Il valore indicato, specificato come opzione, non è stato riconosciuto.

ICA2051 Errore di conversione adapt_addr per indirizzo.

Spiegazione: L'indirizzo IP indicato non è valido.

Risposta dell'utente: Possibile danneggiamento del file /etc/security/fwsecadpt.cfg. Eliminare il file, riconfigurare l'interfaccia sicura ed inizializzare nuovamente i filtri.

ICA2052 afopen non è riuscito ad aprire /etc/security/login.cfg: *errno***.**

Spiegazione: Impossibile eseguire l'autenticazione dell'utente, errore di apertura nel file indicato.

ICA2053 Non è stato possibile aprire il file di interfaccia sicura.

Spiegazione: L'interfaccia sicura non è stata configurata.

Risposta dell'utente: Per definire un'interfaccia sicura, utilizzare i comandi del firewall o i pannelli SMIT.

ICA2054 enduserdb rc=*valore***,** *errno***.**

Spiegazione: Il codice di errore di sistema indicato è stato ricevuto durante il tentativo di richiamare le informazioni sul profilo di login dell'utente.

Risposta dell'utente: Contattare il responsabile del firewall per verificare il codice di contabilizzazione di login.

ICA2055 getpeername() (*nome chiamata***):** *errno***.**

Spiegazione: Si è verificato un errore di sistema quando il daemon ftp ha tentato di richiamare il nome socket.

ICA2056 getsockname() (*nome chiamata***):** *errno***.**

Spiegazione: Si è verificato un errore di sistema quando il daemon ftp ha tentato di richiamare il nome porta.

ICA2057 rc=*valore* di getuser shell non sicura per *ID utente*, *errno*.

Spiegazione: Il codice di errore di sistema indicato è stato ricevuto durante il tentativo di richiamare il nome shell per il collegamento da un lato non sicuro del firewall.

Risposta dell'utente: Contattare il responsabile del firewall per impostare una shell per il profilo di login dell'utente.

ICA2058 rc=*valore* di getuser shell sicura per *ID utente*, *errno*.

Spiegazione: Il codice di errore di sistema indicato è stato ricevuto durante il tentativo di richiamare il nome shell per il collegamento da un lato sicuro del firewall.

Risposta dell'utente: Contattare il responsabile del firewall per visualizzare una shell per il profilo di login dell'utente.

ICA2059 ioctl(): *errno*

Spiegazione: Errore di sistema restituito dalla chiamata ioctl() per SIOCSPGRP.

ICA2060 ptelnetd: ftok per memoria condivisa non riuscito.

Spiegazione: Impossibile assegnare il segmento di memoria condivisa.

Risposta dell'utente: Contattare il responsabile del firewall, possibile problema di memoria.

ICA2061 ptelnetd: shmat per memoria condivisa non riuscito.

Spiegazione: Impossibile assegnare il segmento di memoria condivisa.

Risposta dell'utente: Contattare il responsabile del firewall, possibile problema di memoria.

ICA2062 ptelnetd: shmget per memoria condivisa non riuscito.

Spiegazione: Impossibile assegnare il segmento di memoria condivisa.

Risposta dell'utente: Contattare il responsabile del firewall, possibile problema di memoria.

ICA2063 setsockopt() (SO_DEBUG): *errno*.

Spiegazione: Il messaggio di errore indicato è stato restituito dalla chiamata di sistema 'setsockopt'.

ICA2064 setsockopt() (SO_KEEPALIVE): *errno*.

Spiegazione: Il messaggio di errore indicato è stato restituito dalla chiamata di sistema 'setsockopt'.

ICA2065 setuser rc=*valore*, *errno*.

Spiegazione: È stato ricevuto un codice di errore errato durante la chiamata di sistema per il motivo indicato.

ICA2066 signal(): *errno*.

Spiegazione: Si è verificato un errore di sistema quando il daemon ftp ha tentato di stabilire il programma di gestione dei segnali.

ICA2067 Errore grave di inizializzazione di pftpd - bind(): *errno*

Spiegazione: L'inizializzazione del server pftpd non è riuscita, il daemon è stato arrestato.

Risposta dell'utente: Correggere l'errore di sistema indicato e riavviare pftpd. La causa più probabile di questo errore può essere dovuta ad un altro daemon ftp in ascolto sulla porta ftp standard (21).

ICA2068 Errore grave di inizializzazione di pftpd - listen(): *errno*

Spiegazione: L'inizializzazione del server pftpd non è riuscita, il daemon è stato arrestato.

Risposta dell'utente: Correggere l'errore di sistema indicato e riavviare pftpd.

ICA2069 Errore grave pftpd - tentativo principale di accept(): *errno*

Spiegazione: La routine principale del server pftpd non è riuscita, il daemon viene arrestato.

Risposta dell'utente: Correggere l'errore di sistema indicato e riavviare pftpd.

ICA2070 Errore grave di inizializzazione di pftpd - socket(): *errno*

Spiegazione: L'inizializzazione del server pftpd non è riuscita, il daemon è stato arrestato.

Risposta dell'utente: Correggere l'errore di sistema indicato e riavviare pftpd.

ICA2071 Collegamento rifiutato, raggiunto il numero massimo di collegamenti.

Spiegazione: Il server pftpd non può creare un'altra sessione FTP, perché il numero massimo di sessioni è stato già raggiunto.

Azione del sistema: Il collegamento viene rifiutato.

Risposta dell'utente: Attendere che i collegamenti esistenti terminino, e ritentare l'operazione.

ICA2072 File di configurazione ftp (*nome file***) non disponibile.**

Spiegazione: Il daemon ftp ha tentato di aprire il file di configurazione FTP specificato ma questo non esiste o non può essere aperto.

Azione del sistema: L'elaborazione del daemon ftp utilizza la configurazione assunta

Risposta dell'utente: Nessuna, a meno che il file non sia necessario; in tal caso il file deve essere creato o spostato nell'ubicazione specificata nel messaggio.

ICA2073 Impossibile ottenere memoria per la tabella di lingua ftp.

Spiegazione: Non è stato possibile ottenere la memoria richiesta per rappresentare un'istruzione REPLYLANGUAGE nel file di configurazione ftp.

Azione del sistema: L'elaborazione continua.

Risposta dell'utente: Aumentare la dimensione o ridurre le entrate del file di configurazione.

ICA2074 Elaborazione completa per l'istruzione di configurazione ftp: *istruzione di configurazione*

Spiegazione: ftp ha elaborato l'istruzione di configurazione indicata.

Azione del sistema: L'elaborazione continua.

Risposta dell'utente: Nessuna

ICA2075 FTP per *id utente* **(***ind IP origine***:***ind IP dest***),** *operazione nome file***,** *byte* **byte. sid:** *id sessione***.**

Spiegazione: Messaggio generato per ogni trasferimento di file nelle sessioni FTP aperte. Il sid è un identificativo univoco generato dal firewall all'avvio della sessione.

ICA2076 Sessione FTP *id sessione* **terminata per** *id utente* **(***indirizzo IP origine***:***indirizzo IP destinazione***),** *durata* **secondi,** *byte* **byte.**

Spiegazione: Questo messaggio viene generato alla fine di ogni sessione FTP. Il sid è un identificativo univoco generato dal firewall all'avvio della sessione.

ICA2077 Sessione Telnet per *id sessione* **terminata per** *id utente* **(***ind IP origine***:***ind IP dest***),** *byte* **byte.**

Spiegazione: Questo messaggio viene generato alla fine di ogni sessione Telnet. Il sid è un identificativo univoco generato dal firewall all'avvio della sessione.

ICA2078 Utente proxy *utente* **scollegato - inattivo per** *numero* **minuti.**

Spiegazione: La sessione dell'utente ha superato il periodo massimo di inattività consentito.

ICA2079 Attenzione - Tentativo di collegamento non autorizzato a *indirizzo_IP* **da** *indirizzo_IP***.**

Spiegazione: Generalmente indica il tentativo di stabilire un collegamento al firewall mediante l'interfaccia non sicura.

Azione del sistema: Rifiutare il collegamento.

ICA2080 Errore di sintassi (*causa***) vicino alla colonna** *colonna* **della riga del file di configurazione ftp** *riga***:** *istruzione di configurazione*

Spiegazione: L'istruzione di configurazione ftp alla riga indicata è in errore. Vengono fornite la causa dell'errore e l'ubicazione in cui si è verificato l'errore.

Azione del sistema: L'istruzione viene ignorata.

Risposta dell'utente: Correggere l'istruzione nel file di configurazione ftp.

ICA2081 Nessun catalogo dei messaggi fornito dalle istruzioni di configurazione ftp è utilizzabile.

Spiegazione: Il tentativo di aprire i cataloghi dei messaggi forniti dalle istruzioni di configurazione REPLYLANGUAGE ftp non è riuscito. Non è possibile utilizzare alcun catalogo dei messaggi del client.

Azione del sistema: Il catalogo dei messaggi del client viene forzato nella lingua inglese, indirizzario C.

Risposta dell'utente: Assicurarsi che ci siano dei file di catalogo in ogni indirizzario associati agli indirizzari di lingua nelle istruzioni di configurazione ftp REPLYLANGUAGE. Controllare anche che la variabile di ambiente NLSPATH sia impostata in modo corretto per consentire la sostituzione del sottoindirizzario dalla variabile di ambiente LANG (%L) e del nome di catalogo (%N).

ICA2082 Impossibile impostare la variabile di ambiente ftp LANG su *sottoindirizzario***, motivo:** *motivo*

Spiegazione: Si è verificato un errore di sistema (indicato dal motivo) quando il daemon ftp stava tentando di modificare l'impostazione della variabile di ambiente LANG nel sottoindirizzario specificato.

Azione del sistema: L'elaborazione continua. La correzione può generare altri messaggi.

Risposta dell'utente: Utilizzare il motivo indicato per determinare se si tratta di un errore di sistema o di programmazione.

ICA2083 Impossibile aprire il catalogo dei messaggi del client ftp nell'indirizzario: *sottoindirizzario***, motivo:** *motivo*

Spiegazione: Il daemon ftp non ha potuto aprire il catalogo dei messaggi nel sottoindirizzario specificato. Il motivo fornito è il numero dell'errore restituito da catopen().

Azione del sistema: L'elaborazione continua. La correzione può generare altri messaggi.

Risposta dell'utente: Assicurarsi che ci sia un catalogo nell'indirizzario associato a quello della lingua fornito. Controllare che la variabile di ambiente NLSPATH sia impostata in modo corretto per consentire la sostituzione del sottoindirizzario (%L) e del nome di catalogo (%N).

ICA2084 Catalogo dei messaggi del client ftp forzato in inglese mediante il sottoindirizzario C.

Spiegazione: A causa degli errori precedentemente elencati, il daemon ftp ha forzato il catalogo dei messaggi del client nella lingua inglese utilizzando il sottoindirizzario C.

Azione del sistema: Se la lingua può essere forzata nel catalogo dei messaggi C, l'elaborazione continua. Altrimenti, il programma viene terminato.

Risposta dell'utente:

ICA2089 Il tipo di autorizzazione del file utente (*tipo autorizzazione***) non corrisponde a nessuna entrata della tabella (struct tab2 authtab “).**

Spiegazione: Il tipo di autorizzazione dell'utente specificato (restituito da user.cfg) non è compreso tra quelli supportati (quali deny,none,snk,sdi,password,etc.)

Risposta dell'utente: Controllare la configurazione o l'integrità del file user.cfg; per risolvere questo problema, utilizzare i comandi del firewall o i pannelli SMIT.

ICA2090 Autenticazione non riuscita per l'utente '*nome utente***' da** *IP client* **poiché è specificato KEY=DENY nel file user.cfg.**

Spiegazione: L'autenticazione non è riuscita a causa delle specifiche del file user.cfg impostate dal responsabile del firewall.

Risposta dell'utente: Contattare il responsabile del firewall.

ICA2091 ftp non consentito all'utente '*nome utente***' mediante la porta non sicura (***ip firewall***).**

Spiegazione: L'utente ha tentato di eseguire ftp sul server del firewall mediante una porta non sicura - tutti gli utenti della porta non sicura devono aver configurato la propria chiave 'fwnsftp' in modo corretto con un tipo di autorizzazione valido (nel file user.cfg).

Risposta dell'utente: Controllare la configurazione o l'integrità del file user.cfg; per risolvere questo problema, utilizzare i comandi del firewall o i pannelli SMIT.

ICA2092 Errore interno: nt_gwauth() non riuscito.

Spiegazione: nt_gwauth() restituisce normalmente uno dei tre valori (AUTHENTICATED,NOT_AUTHENTICATED o DENY), in questo caso nt_gwauth ha restituito alcuni numeri interi non validi.

ICA2093 ftp non consentito all'utente '*nome utente***' mediante la porta sicura (***numero porta***).**

Spiegazione: L'utente ha tentato di eseguire ftp sul server del firewall mediante una porta sicura - tutti gli utenti della porta sicura devono aver configurato la propria chiave 'fwsftp' in modo corretto con un tipo di autorizzazione valido (nel file user.cfg).

Risposta dell'utente: Controllare la configurazione o l'integrità del file user.cfg; per risolvere questo problema, utilizzare i comandi del firewall o i pannelli SMIT.

ICA2094 Login non riuscito: formato previsto: "PASS <password>" dopo: "USER <*nome utente***>"; ricevuto** *comando non valido***.**

Spiegazione: L'autenticazione non è riuscita perché il client ftp non ha inviato il formato previsto (PASS 'password' per RFC959).

Risposta dell'utente: Digitare "user <nome utente>"; immettere la parola d'ordine corretta. Contattare il responsabile del firewall.

ICA2095 Login non riuscito: (mediante metodo *metodo di autenticazione***) autenticazione utente '***nome utente***' da** *ip client* **(sito client) non riuscita.**

Spiegazione: L'autenticazione non è riuscita a causa di un'immissione non valida (dal client per il tipo di autenticazione specificato) - ad esempio, l'utente ha immesso una parola d'ordine o una chiave snk non valida.

Risposta dell'utente: Contattare il responsabile del firewall.

ICA2096 Autenticato: (mediante metodo *metodo di autenticazione***) autenticazione utente '***nome utente***' da** *ip client* **(sito client) eseguita correttamente.**

Spiegazione: Autenticazione eseguita correttamente.

ICA2097 httpd --> Avvio del server proxy HTTP, versione *versione proxy HTTP* **in corso.**

Spiegazione: Viene avviato il proxy HTTP per l'accesso WWW.

ICA2098 httpd --> Chiusura del server proxy HTTP in corso.

Spiegazione: Viene disattivato il proxy HTTP per l'accesso WWW.

ICA2099 httpd --> Stato: <*stato HTTP*> **del client** <*indirizzo IP*>**, che ha richiesto** <**\"** *richiesta GET HTTP***\"**> **per** <*numero di byte*> **byte.**

Spiegazione: Stato della richiesta HTTP del client di alcuni file mediante il proxy. Per ulteriori informazioni sul valore del codice "Stato", consultare i documenti HTTP 1.0(RFC 1945) o HTTP 1.1(RFC 2068) (o gli RFC successivi) disponibili su diversi siti Internet, incluso ds.internic.net.

ICA2100 Indirizzo socket uguale a zero.

Spiegazione: È stato rilevato un indirizzo di destinazione non valido nella richiesta locale.

ICA2101 Errore nella famiglia di indirizzi socket: *tipo_famiglia_sin***.**

Spiegazione: È stato rilevato un tipo di famiglia di indirizzi non valido nella richiesta locale.

ICA2102 Errore nell'inizializzazione di odm: *errno odm***.**

Spiegazione: Si è verificato un errore odm_initialize() per ODM (Object Data Manager).

ICA2103 Errore nell'impostazione del percorso assunto di odm: *errno odm***.**

Spiegazione: Si è verificato un errore odm_set_path() per ODM (Object Data Manager). Classe dell'oggetto, OCSvhost.

ICA2104 Errore nel blocco del database di odm: *errno odm***.**

Spiegazione: Si è verificato un errore odm_lock() per ODM (Object Data Manager).

ICA2105 Errore nell'apertura dell'oggetto odm *Customized_Attribute***:** *errno odm***.**

Spiegazione: Si è verificato un errore odm_open_class() per ODM (Object Data Manager).

ICA2106 Errore nella ricerca dell'oggetto odm *host_virtuale_OCS***:** *errno odm***.**

Spiegazione: Si è verificato un errore odm_get_first() per ODM (Object Data Manager). Classe dell'oggetto, OCSvhost.

ICA2107 Errore nella chiusura dell'oggetto odm *host_virtuale_OCS***:** *errno odm***.**

Spiegazione: Si è verificato un errore odm_close_class() per ODM (Object Data Manager). Classe dell'oggetto, OCSvhost.

ICA2108 Errore nello sblocco del database di odm: *errno odm***.**

Spiegazione: Si è verificato un errore odm_unlock() per ODM (Object Data Manager).

ICA2109 Errore nell'arresto di odm: *errno odm***.**

Spiegazione: Si è verificato un errore odm_terminate() per ODM (Object Data Manager).

ICA2110 Errore nel richiamo del server per nome: *errno***.**

Spiegazione: Si è verificato un errore getservbyname(). Il servizio Controllo login dell'host non è specificato in modo corretto nel file /etc/services.

ICA2111 Errore byname(): *errno***.**

Spiegazione: Si è verificato un errore gethostbyname(). Il nome della macchina host non è stato specificato in modo corretto in /etc/hosts.

ICA2112 Nome protocollo non valido: *nome protocollo***.**

Spiegazione: Il nome del protocollo specificato nella classe dell'oggetto ODM, OCSvhost, non è supportato.

ICA2113 Errore nell'apertura del socket su LM: *errno***.**

Spiegazione: Si è verificato un errore socket() sulla macchina host in cui si trova il Controllo login.

ICA2114 Errore di bind dell'indirizzo locale: *errno***.**

Spiegazione: Si è verificato un errore bind() utilizzando l'indirizzo locale per questo nodo OCS.

ICA2115 Errore nel collegamento del socket a LM: *errno***.**

Spiegazione: Si è verificato un errore connect() sulla macchina host in cui si trova il Controllo login.

ICA2116 Errore nel tipo di protocollo: *tipo protocollo***.**

Spiegazione: Il tipo di protocollo del terminale virtuale utilizzato per comunicare con il Controllo login dell'host non è valido.

ICA2117 Errore malloc su messaggio LM.

Spiegazione: Si è verificato un errore malloc() durante l'assegnazione dinamica dello spazio per il messaggio Controllo login a lunghezza variabile.

ICA2118 Errore nella trasmissione del messaggio a LM: *errno***.**

Spiegazione: Si è verificato un errore send() quando al Controllo login è stata inviata la richiesta di aprire l'unità host corretta.

ICA2119 Errore nella ricezione del messaggio da LM: *errno***.**

Spiegazione: Si è verificato un errore recv() quando il Controllo login ha restituito una conferma di ricezione.

ICA2120 Errore di stato da LM: *stato***.**

Spiegazione: La conferma di ricezione del Controllo login indica che l'unità host non è stata aperta correttamente.

ICA2121 Errore nell'apertura dell'unità di gestione OCS: *errno***.**

Spiegazione: L'unità di gestione OCS non è stata aperta correttamente.

ICA2122 Conversione dell'indirizzo IP in ID TBM: *errno***.**

Spiegazione: Si è verificato un errore OCS_GET_TBMID ioctl(). Il comando OCS_GET_TBMID ioctl non è stato eseguito correttamente sull'unità di gestione OCS.

ICA2123 Errore nel collegamento a TBM determinato da rlogin: *errno***.**

Spiegazione: Si è verificato un errore OCS_IS_TBM_CONNECTED ioctl(). Il comando OCS_IS_TBM_CONNECTED ioctl non è stato eseguito correttamente sull'unità di gestione OCS.

ICA2124 Nessun nodo host collegato: *errno***.**

Spiegazione: Non ci sono nodi host collegati a questo nodo OCS dall'elenco dei possibili nodi host.

ICA2125 Errore nel richiamo dell'elenco per ODM (Object Data Manager): *Customized_Attribute***:** *errno odm***.**

Spiegazione: Si è verificato un errore odm_get_list() per la classe dell'oggetto ODM, CuAt(Customized Attribute).

ICA2126 Nessun nome di nodo host OCS associato a: *nodohost_da_connettere***.**

Spiegazione: L'entrata CuAt(Customized Attribute) è stata trovata ma non c'è corrispondenza tra il nodo host ed il nodo OCS.

ICA2127 Errore malloc nell'assieme di host.

Spiegazione: Si è verificato un errore malloc() durante l'assegnazione dinamica dello spazio per l'assieme di nomi host possibili.

ICA2128 Utente (sconosciuto) da *ip client* **(sito client) ha tentato un comando '***comando non valido***' prima dell'autenticazione.**

Spiegazione: Un utente ha tentato di eseguire delle attività prima di immettere il nome utente e la parola d'ordine per l'autenticazione - è necessario eseguire l'autenticazione degli utenti prima che ulteriori elaborazioni possano continuare.

Risposta dell'utente: Eseguire il login con USER e PASS.

ICA2129 gethostbyname (*nome richiamo***):** *errno*

Spiegazione: Si è verificato un errore di sistema quando ftpd ha tentato di richiamare le informazioni corrispondenti al nome host.

ICA2130 Utente (*nome utente***) da** *ip client* **(sito client) ha tentato un comando '***comando non valido***'.**

Spiegazione: L'utente specificato ha eseguito un comando non valido.

Risposta dell'utente: Sono consentiti solo i comandi USER, QUOTE SITE e QUIT fino a quando non si specifica "quote site destination".

ICA2131 Autenticazione non riuscita per l'utente '*nome utente***' da** *IP client* **a causa di un errore nel file user.cfg.**

Spiegazione: L'autenticazione non è riuscita a causa delle specifiche del file user.cfg impostate dal responsabile del firewall (controllare i log precedenti).

Risposta dell'utente: Contattare il responsabile del firewall.

ICA2132 Utente '*utente***' da IP** *ip client* **(sito client) ha tentato un comando '***comando non valido***'.**

Spiegazione: L'utente ha eseguito un comando non valido. Gli unici comandi validi sono SITE, USER e QUIT.

ICA2133 Errore: chiamata *funzione* **non riuscita in** *istruzione***:***riga***,** *WSAGetLastError*

Spiegazione: Messaggio di errore generale; controllare i log.

ICA2134 Avviso: ftpd: connect() (in *istruzione***) non è riuscito a raggiungere** *IP***,** *WSAGetLastError***.**

Spiegazione: Connect() non è riuscito a trovare l'indirizzo richiesto; controllare il risultato WSAGetLastError.

Risposta dell'utente: Controllare l'indirizzo - possibili errori di rete o DNS.

ICA2135 Trasferimento dati completato: ricevuti *byte* **byte (da** *IP origine***); inviati** *byte* **byte (a** *IP destinazione***).**

Spiegazione: Queste informazioni fanno riferimento ad un singolo trasferimento di dati durante una particolare sessione ftp. Tuttavia, è possibile che il trasferimento dei dati non è stato completato correttamente (controllare il log per una chiamata di invio o ricezione non riuscita).

ICA2136 Errore: CreateThread() non riuscito in *istruzione***:** *errno***.**

Spiegazione: ftpd non ha potuto creare un thread.

ICA2137 Collegamento dati stabilito; server: *ip origine* **client:** *ip destinazione***.**

Spiegazione: Collegamento dati eseguito correttamente.

ICA2138 Memoria insufficiente: pftpd: malloc(*byte***) ha restituito NULL nella funzione** *istruzione***.**

Spiegazione: Impossibile assegnare memoria sufficiente - malloc ha restituito NULL.

ICA2139 LogonUser() non riuscito: *motivo***.**

Spiegazione: LogonUser API (SAM) Windows NT (per l'autenticazione della parola d'ordine) non è riuscito a causa dei motivi specificati.

Risposta dell'utente: Contattare il responsabile del firewall.

ICA2140 httpd --> Autenticazione proxy HTTP *risultato* **per utente** < *utente*>**, su** < *ip utente*>**, tramite** *rete* **... RC:**< *motivo*>**.**

Spiegazione: Il proxy HTTP ha tentato di eseguire l'autenticazione dell'utente. Il risultato è riportato qui per il motivo specificato.

Risposta dell'utente: Contattare il responsabile del firewall.

ICA2141 Sessione FTP a *indirizzo IP* **da** *indirizzo IP* **terminata.**

Spiegazione: La sessione ftp al firewall è terminata.

ICA2142 fw_tn_authenticate ha autenticato *id utente* **correttamente.**
ICA2143 Autenticazione fw_tn_authenticate per *id utente* **non riuscita.**

Spiegazione: fw_tn_authenticate non può eseguire l'autenticazione dell'ID utente specificato.

Azione del sistema: Collegamento rifiutato.

Risposta dell'utente: Se fw_tn_authenticate dispone di tutte le funzioni di log, il responsabile deve esaminare il file di log per individuare la causa del problema.

ICA2144 fw_tn_authenticate non ha restituito un valore corretto.

Spiegazione: Il valore restituito da fw_tn_authenticate non è zero. È possibile che la funzione fw_tn_authenticate non sia definita.

Azione del sistema: Collegamento rifiutato.

Risposta dell'utente: Esaminare attentamente fw_tn_authenticate per controllare se viene restituito un valore diverso da zero ed in tal caso correggerlo. Quindi, ricreare la libreria fwuser.o ed inserirla nel firewall.

ICA2145 Il sistema ha restituito il codice di errore *rc* **nel file** *nome file* **alla riga** *numero riga***.**

Spiegazione: Una chiamata di sistema non è riuscita. È possibile che la libreria fwuser.o non esista.

Azione del sistema: L'autenticazione viene interrotta.

Risposta dell'utente: Assicurarsi che /usr/lib/fwuser.o esista. In tal caso, contattare il proprio rappresentante IBM.

ICA2146 La libreria fwuser.o fornita dall'IBM non è stata sostituita.

Spiegazione: Viene utilizzata la libreria fwuser.o fornita dall'IBM perché l'utente non l'ha sostituita con la propria fwuser.o.

Azione del sistema: L'autenticazione viene interrotta.

Risposta dell'utente: È necessario scrivere e compilare la propria autenticazione se un qualsiasi utente può utilizzare l'autenticazione fornita dall'utente. La libreria fwuser.o fornita dall'IBM nega l'accesso a tutti gli utenti non AIX e non Firewall.

ICA2147 fwtelnet: l'utente *id utente* **ha avviato una sessione telnet trasparente da** *indirizzo IP origine* **(sito sicuro) a** *indirizzo IP destinazione***.**

Spiegazione: Questo messaggio viene generato all'inizio di ogni sessione proxy trasparente (fwtelnet). Una sessione viene avviata quando l'ID utente, l'indirizzo IP di origine e quello di destinazione sono noti al firewall. Sono consentite solo le sessioni avviate da un sito sicuro.

Azione del sistema: Consentire la sessione telnet trasparente.

ICA2148 Attenzione -- Tentativo di collegamento non autorizzato per l'utente *id utente* **da** *ind IP origine* **(sito non sicuro) a** *ind IP destinazione***, non consentito.**

Spiegazione: Generalmente indica il tentativo di stabilire un collegamento al firewall mediante l'interfaccia non sicura.

Azione del sistema: Rifiutare il collegamento.

Risposta dell'utente: È necessario eseguire la sessione telnet da un sito sicuro utilizzando il proxy trasparente.

ICA2149 fwtelnet: si è verificato un errore LOGIN_ADAPTER_ERROR durante l'avvio di una sessione telnet trasparente da *indirizzo IP origine* **a** *indirizzo IP destinazione***.**

Spiegazione: Si è verificato un errore LOGIN_ADAPTER_ERROR durante la chiamata q_check_secure(0).

Azione del sistema: Rifiutare il collegamento.

Risposta dell'utente: Controllare l'adattatore sicuro.

ICA2150 Errore Pftpd - *funzione in errore***: codice di errore = 0x***codice di errore della funzione*

Spiegazione: Il server pftpd ha rilevato un errore nella funzione indicata. Il daemon si arresta.

Risposta dell'utente: Correggere l'errore di sistema indicato e riavviare pftpd.

ICA2151 Login rifiutato.

Spiegazione: Questo messaggio viene visualizzato per gli utenti che tentano di collegarsi ma non sono autorizzati.

ICA2152 fwlogin: scrittura su *unità* **non riuscita.**

Spiegazione:

ICA2157 All'utente *id utente* **da** *indirizzo IP origine* **non viene consentito di utilizzare il proxy trasparente per** *indirizzo IP destinazione***.**

Spiegazione: Generalmente indica il tentativo di stabilire un collegamento al firewall mentre il proxy trasparente non è configurato.

Azione del sistema: Rifiutare il collegamento.

Risposta dell'utente: Attivare fwtpproxy ftp.

ICA2158 Opzione *valore* **specificata in modo errato.**

Spiegazione: Questo indicatore non è stato specificato in modo corretto.

ICA2159 Valore di timeout non specificato per l'opzione -t.

Spiegazione: Deve essere fornito un valore timeout per l'opzione -t.

ICA2160 Parola d'ordine modificata per l'utente *ID utente* **da** *rete* **:***nome host***.**

Spiegazione: Un utente FTP ha modificato correttamente la parola d'ordine nel database delle parole d'ordine.

Azione del sistema: Nessuna

Risposta dell'utente: Nessuna

ICA2161 L'utente *ID utente* **ha tentato di eseguire il login utilizzando la parola d'ordine scaduta da** *rete* **:***nome host***.**

Spiegazione: Un utente FTP ha tentato di stabilire un collegamento al firewall utilizzando la parola d'ordine scaduta.

Azione del sistema: La convalida del login FTP non è riuscita e l'utente viene restituito alla shell di comandi FTP.

Risposta dell'utente: L'utente deve tentare nuovamente la convalida utilizzando il comando USER FTP oppure stabilendo un nuovo collegamento FTP ed immettendo la stringa della parola d'ordine nel seguente formato "vecchia_parola_d'ordine/nuova_parola_d'ordine/nuova_parola_d'ordine".

ICA2162 Errore nella modifica della parola d'ordine per l'utente *ID utente* **da** *rete* **:***nome host***.**

Spiegazione: Un utente FTP ha tentato di modificare la parola d'ordine e la routine di convalida della parola d'ordine non è riuscita. Le cause possibili di questo errore sono: - Specificata parola d'ordine "precedente" non corretta - Specificata una sola ricorrenza della "nuova" parola d'ordine - Le due ricorrenze della "nuova" parola d'ordine non corrispondono - Il delimitatore utilizzato per separare le parole d'ordine non era "/".

Azione del sistema: La convalida della parola d'ordine FTP non è riuscita e l'utente viene restituito alla shell di comandi FTP.

Risposta dell'utente: Tentare di eseguire nuovamente la convalida con il server FTP verificando che le parole d'ordine vengano immesse correttamente. Se il problema persiste, contattare il rappresentante del servizio.

ICA2163 safemaild avviato.

Spiegazione: Avvio di safemaild in corso.

ICA2164 safemaild arrestato.

Spiegazione: Arresto di safemaild in corso.

ICA2165 Sessione telnet interrotta.

Spiegazione: La sessione telnet sta terminando, ma non è possibile richiamare le relative informazioni dalla pipe. La sessione è stata probabilmente interrotta durante l'avvio eseguito dal client, pertanto la sessione non era stata completamente inizializzata.

ICA2166 Non è stato possibile richiamare l'attributo *attributo* **per l'utente** *id utente***. Codice di errore =** *codice di errore***.**

Spiegazione: Il servizio di autenticazione non è riuscito a richiamare l'attributo specificato dal database utente per l'utente specificato.

Azione del sistema: L'autenticazione dell'utente non è riuscita.

Risposta dell'utente: Contattare il responsabile di sistema per correggere il record del database dell'utente.

ICA2167 L'autenticazione di *id utente* **non è riuscita per** *servizio* **utilizzando** *schema autenticazione* **da** *indirizzo client* **su** *tipo di rete*

Spiegazione: Non è stato possibile eseguire l'autenticazione dell'utente specificato per il servizio indicato con il metodo di autenticazione specificato. L'utente stava richiedendo il servizio dall'indirizzo e tipo di rete indicati.

Azione del sistema: L'autenticazione dell'utente non è riuscita.

Risposta dell'utente: Contattare il responsabile di sistema.

ICA2168 L'autenticazione di *id utente* **non è riuscita per** *servizio* **a causa di insufficienza di memoria.**

Spiegazione: Non è stato possibile eseguire l'autenticazione dell'ID utente a causa di una insufficienza di memoria durante il processo di autenticazione.

Azione del sistema: L'autenticazione dell'utente non è riuscita.

Risposta dell'utente: Contattare il responsabile di sistema.

ICA2169 Utente *nome* **autenticato correttamente per** *servizio* **utilizzando** *metodo* **da** *rete***:***nome host***.**

Spiegazione: Il firewall ha eseguito l'autenticazione del nome utente indicato per il servizio richiesto utilizzando lo schema di autenticazione specificato.

ICA2170 L'autenticazione di *id utente* **non è riuscita per** *servizio***.** *metodo autenticazione* **non registrato con il firewall.**

Spiegazione: Non è stato possibile eseguire l'autenticazione dell'ID utente per il servizio. Il metodo di autenticazione richiesto non è registrato con il firewall.

Azione del sistema: L'autenticazione dell'utente non è riuscita.

Risposta dell'utente: Contattare il responsabile di sistema.

ICA2171 Il codice di contabilizzazione *nome_utente* **è stato bloccato a causa di una parola d'ordine scaduta.**

Spiegazione: La parola d'ordine è scaduta e non è stata modificata. Questo codice di contabilizzazione è stato bloccato.

Azione del sistema: Il codice di contabilizzazione è bloccato e l'autenticazione delle parole d'ordine del firewall non verrà eseguita correttamente.

ICA2172 Il codice di contabilizzazione *nome_utente* **è bloccato.**

Spiegazione: Questo codice di contabilizzazione è stato bloccato.

Azione del sistema: Il codice di contabilizzazione è bloccato. L'autenticazione delle parole d'ordine del firewall non verrà eseguita correttamente.

Risposta dell'utente: Contattare il responsabile del firewall per sbloccare il codice di contabilizzazione.

ICA2173 L'utente ha tentato di eseguire il login utilizzando il nome utente riservato *id utente***.**

Spiegazione: L'ID fornito dall'utente è riservato all'utilizzo del firewall.

Azione del sistema: Collegamento rifiutato.

Risposta dell'utente: Il responsabile deve individuare chi sta utilizzando questo nome utente.

ICA2174 L'autenticazione di *id utente* **non è riuscita per** *servizio* **utilizzando** *schema autenticazione* **da** *indirizzo client* **su** *tipo di rete* **a causa di un errore interno di elaborazione.**

Spiegazione: Non è stato possibile eseguire l'autenticazione dell'utente specificato per il servizio indicato con il metodo di autenticazione specificato. L'utente stava richiedendo il servizio dall'indirizzo e tipo di rete indicati. La richiesta di autenticazione non è riuscita a causa di un errore interno di elaborazione.

Azione del sistema: L'autenticazione dell'utente non è riuscita.

Risposta dell'utente: Contattare il responsabile di sistema.

ICA2175 Chiamata di LogonUser per Windows NT non riuscita per l'utente *nome utente***. L'ultimo errore era** *ultimo errore***.**

Spiegazione: Il nome utente specificato non è stato autenticato dalla chiamata dell'API LogonUser per Windows NT. Windows NT ha notificato l'ultimo errore dopo che il LogonUser non è riuscito.

Azione del sistema: L'autenticazione dell'utente non è riuscita.

Risposta dell'utente: Contattare il responsabile di sistema.

ICA2176 Definito schema di autenticazione sconosciuto *schema autenticazione* **per** *nome utente* **utilizzando** *componente* **da** *rete***.**

Spiegazione: Lo schema di autenticazione indicato è stato definito per l'utente specificato utilizzando il componente del firewall specificato dalla rete indicata, ma lo schema di autenticazione non è correntemente registrato con il firewall.

Azione del sistema: La richiesta di autenticazione dell'utente non è riuscita.

Risposta dell'utente: Contattare il responsabile di sistema.

ICA2177 Collegamento SafeMail 0x*ID sessione* **ricevuto da** *nome peer socket***.**

Spiegazione: SafeMail ha ricevuto un collegamento in arrivo dal nome peer elencato. Il numero ID del collegamento indicato è stato assegnato per la traccia. (Livello debug)

Azione del sistema: È stato inviato un thread per gestire questo collegamento.

ICA2178 La sessione SafeMail 0x*ID sessione* **è stata stabilita da** *indirizzo IP del mittente* **a** *indirizzo IP del destinatario***.**

Spiegazione: SafeMail ha stabilito un collegamento con il server di posta del destinatario ed è pronto per il trasferimento della posta. (Livello informativo)

Azione del sistema: Il trasferimento dei dati sta per iniziare.

ICA2179 SafeMail ha inoltrato *dimensione messaggio* **byte per il collegamento 0x***ID sessione* **da** *indirizzo server del mittente* **a** *indirizzo server del destinatario***.**

Spiegazione: SafeMail ha inoltrato un messaggio correttamente tra i due server di posta indicati. Questa sessione è stata precedentemente identificata nel messaggio ICA2166. Questo messaggio contiene il numero di byte specificato. (Livello informativo)

ICA2180 SafeMail ha terminato la sessione 0x*ID sessione* **da** *indirizzo del mittente***.**

Spiegazione: SafeMail ha rifiutato di trasferire la posta inviata nella sessione indicata. (Livello informativo)

Azione del sistema: La sessione è stata arrestata.

Risposta dell'utente: Aumentare il livello di priorità del log per ottenere ulteriori informazioni sulla diagnostica.

ICA2181 SafeMail ha terminato la sessione 0x*ID sessione* **per il codice motivo** *codice motivo***.**

Spiegazione: Il processore principale di SafeMail ha arrestato la sessione indicata, perché è stata rilevata una condizione di errore primaria. I codici motivo includono: \01 - impossibile localizzare il server di posta del destinatario \02 - il mittente ha tentato di instradare la posta tra due server non sicuri \03 - il server di posta del destinatario ha rifiutato il collegamento, è possibile che sia disattivato \04 - il server di posta del destinatario ha rifiutato di accettare la posta \05 - uno o più collegamenti in timeout; è possibile che il server di posta di ricezione o quello di invio sia disattivato \06 - recv() ha restituito 0 byte; è possibile che il server di posta di invio o quello di ricezione sia disattivato \07 - recv() ha restituito un valore negativo; è possibile che il server di posta di invio o quello di ricezione sia disattivato \08 - ricevuti troppi comandi errati \09 - select() ha restituito un valore negativo; è possibile che il server di posta di invio o quello di ricezione sia disattivato. Questo messaggio viene registrato con il livello Debug.

Azione del sistema: Il collegamento è stato arrestato.

ICA2182 SafeMail ha rifiutato la sessione 0x*ID sessione* **a causa di un comando non valido** *comando SMTP***, codice motivo** *codice motivo***.**

Spiegazione: La sottoroutine di convalida del comando di SafeMail ha rilevato un comando non valido o pericoloso. I codici motivo variano per ogni comando SMTP. Consultare la pagina web IBM Firewall Support per i valori correnti. (Livello debug)

Azione del sistema: Il collegamento è stato arrestato.

Risposta dell'utente: Risolvere il problema relativo al client o al server di posta del mittente, in modo che le informazioni valide e sicure possano essere inviate.

ICA2183 httpd --> File di configurazione HTTP (*nome file***) non disponibile.**

Spiegazione: Il daemon proxy HTTP ha tentato di aprire il file di configurazione specificato ma questo non esiste o non può essere aperto.

Azione del sistema: Il proxy HTTP non viene avviato

Risposta dell'utente: Configurare il proxy tramite GUI o con il comando fwhttp e riavviarlo.

ICA2184 Errore signal() con segnale *numero segnale***. Uscita da safemaild.**

Spiegazione: Si è verificato un errore di sistema quando il daemon safemaild ha tentato di stabilire il programma di gestione dei segnali.

ICA2185 Impossibile aprire il socket. Uscita da safemaild

Spiegazione: Errore durante l'apertura del socket.

ICA2186 Impossibile eseguire il bind del socket alla porta. Uscita da safemaild

Spiegazione: Errore durante il tentativo di eseguire il bind del socket alla porta.

ICA2187 Impossibile accettare il nuovo collegamento. Tentare di nuovo safemaild

Spiegazione: Errore nell'accettare un nuovo collegamento.

ICA2188 Tempo (*valore***) specificato per -l errato.**

Spiegazione: Il valore di tempo indicato contiene dei caratteri che non sono compresi nell'intervallo da 0 a 9 o supera il valore massimo consentito.

ICA2189 Valore di timeout non specificato per l'opzione -l.

Spiegazione: Un valore timeout deve essere fornito per l'opzione -l.

ICA2200 (*servizio***:***funzione***) Errore di inizializzazione WinSocket :** *WSAGetLastError*

Spiegazione: Si è verificato un errore durante l'inizializzazione di WinSocket.

Risposta dell'utente: Correggere l'errore di sistema indicato da WSAGetLastError e riavviare il servizio specificato (primo parametro).

ICA2201 (*servizio***:***funzione di chiamata***) Errore** *funzione errata* **alla riga** *numero riga* **:** *WSAGetLastError*

Spiegazione: Il componente Networking specificato non è riuscito

Risposta dell'utente: Correggere l'errore di sistema indicato da WSAGetLastError e riavviare il servizio specificato (primo parametro).

ICA2202 (*servizio***:***funzione di chiamata***) Timeout di** *timeout* **dopo** *WSAGetLastError* **secondi :**

Spiegazione: Timeout della funzione indicata dopo il periodo di inattività specificato.

Risposta dell'utente: Ricollegarsi al servizio indicato e rispondere prima del timeout indicato.

ICA2203 (*servizio***:***funzione di chiamata***) Errore di memoria;** *funzione errata* **restituito** *valore restituito* **alla riga** *numero riga***:** *WSAGetLastError*

Spiegazione: Si è verificato un errore di memoria, normalmente è un problema di memoria esaurita; controllare WSAGetLastError.

Risposta dell'utente: Liberare spazio su disco - contattare il responsabile di sistema.

ICA2204 (*servizio***:***funzione di chiamata***) Errore** *nome file***: accesso negato o creazione non riuscita.**

Spiegazione: Il servizio indicato ha rilevato un errore nel tentativo di accedere o creare il file specificato o il file associato al parametro.

Risposta dell'utente: Assicurarsi che il nome file indicato esista e che abbia le autorizzazioni appropriate.

ICA2205 (*servizio***:***funzione di chiamata***) Il file** *nome file* **richiesto non è stato trovato.**

Spiegazione: Il file specificato non esiste. La causa più probabile dell'errore è che la configurazione assunta del firewall è stata eliminata. Ripristinare il file da una copia di riserva corrente.

Risposta dell'utente: Verificare che il file di configurazione non esista. Il programma di configurazione prevede l'esistenza del file. Se la versione di riserva non è disponibile, contattare il rappresentante del servizio.

ICA2206 (*servizio***:***funzione di chiamata***) Il file di configurazione** *nome file* **è danneggiato.**

Spiegazione: Il formato del file di configurazione indicato non è corretto. Il contenuto è stato danneggiato. La causa più probabile del danneggiamento è che il file è stato editato manualmente e che sono stati aggiunti dati non validi.

Risposta dell'utente: È necessario creare di nuovo il file di configurazione in modo corretto. Tagliare il file (o creare una copia visualizzabile) ed eliminare l'originale. Riconfigurare il file utilizzando il comando di configurazione del firewall appropriato con il file originale come riferimento, se necessario.

ICA2207 (*servizio***:***funzione di chiamata***) Il file di configurazione** *nome file* **è vuoto.**

Spiegazione: Il file di configurazione indicato non è stato trovato oppure è stato trovato ma era vuoto. La causa più probabile può essere dovuta al fatto che la configurazione per il servizio indicato non è stata eseguita.

Risposta dell'utente: Verificare lo stato del file di configurazione. Se il file esiste, il comando di configurazione prevede che questo file contenga dei dati. Per ulteriori informazioni, consultare il manuale.

ICA2208 *servizio* **Sessione** *id sessione* **avviata per** *id utente* **da un adattatore non sicuro (***indirizzo IP origine***:***indirizzo IP destinazione***).**

Spiegazione: Questo messaggio viene generato all'inizio di ogni sessione indicata.

ICA2209 *servizio* **Sessione** *id sessione* **terminata per** *id utente* **da un adattatore non sicuro (***indirizzo IP origine***:***indirizzo IP destinazione***); byte** *byte totali***.**

Spiegazione: Questo messaggio viene generato alla fine di ogni sessione indicata. Byte Totali indica il numero di byte trasferiti durante la sessione. I servizi (ad esempio, ptelnetd) che non supportano Byte Totali indicheranno zero.

ICA2210 (*servizio***) L'utente** *id utente* **ha tentato il login utilizzando la parola d'ordine scaduta da** *indirizzo IP origine* **(non sicuro).**

Spiegazione: L'utente indicato ha tentato di stabilire un collegamento al firewall utilizzando la parola d'ordine scaduta dall'IP di origine specificato su un adattatore non sicuro.

Risposta dell'utente: La parola d'ordine fornita è scaduta in base all'insieme di regole delle parole d'ordine. Contattare il responsabile di sistema.

ICA2211 **(***servizio***) L'utente** *id utente* **ha tentato il login utilizzando la parola d'ordine scaduta da** *indirizzo IP origine* **(sicuro).**

Spiegazione: L'utente indicato ha tentato di stabilire un collegamento al firewall utilizzando la parola d'ordine scaduta dall'IP di origine specificato su un adattatore sicuro.

Risposta dell'utente: La parola d'ordine fornita è scaduta in base all'insieme di regole delle parole d'ordine. Contattare il responsabile di sistema.

ICA2212 **(***servizio***) L'utente** *nome* **è stato autenticato correttamente da** *indirizzo IP origine* **(sicuro).**

Spiegazione: Il firewall ha eseguito l'autenticazione del nome utente dall'IP di origine indicato su un adattatore sicuro.

ICA2213 **(***servizio***) L'utente** *nome* **è stato autenticato correttamente da** *indirizzo IP origine* **(non sicuro).**

Spiegazione: Il firewall ha eseguito l'autenticazione del nome utente dall'IP di origine indicato su un adattatore non sicuro.

ICA2214 **(***servizio***) L'autenticazione dell'utente** *nome* **non è riuscita da** *indirizzo IP origine* **(non sicuro).**

Spiegazione: Il firewall non è riuscito ad eseguire l'autenticazione del nome utente specificato dall'IP di origine indicato su un adattatore non sicuro.

Risposta dell'utente: Probabilmente il nome utente o la parola d'ordine non sono stati digitati in modo corretto; i nomi utente e le parole d'ordine sono sensibili al maiuscolo/minuscolo (controllare il tasto delle maiuscole).

ICA2215 **(***servizio***) L'autenticazione dell'utente** *nome* **non è riuscita da** *indirizzo IP origine* **(sicuro).**

Spiegazione: Il firewall non è riuscito ad eseguire l'autenticazione del nome utente specificato dall'IP di origine indicato su un adattatore sicuro.

Risposta dell'utente: Probabilmente il nome utente o la parola d'ordine non sono stati digitati in modo corretto; i nomi utente e le parole d'ordine sono sensibili al maiuscolo/minuscolo (controllare il tasto delle maiuscole).

ICA2216 **(***servizio***) L'utente** *nome* **da** *indirizzo IP origine* **(non sicuro) non ha immesso parole d'ordine corrispondenti (verifica).**

Spiegazione: È stata richiesta una modifica della parola d'ordine e l'utente indicato dall'indirizzo IP di origine specificato su un adattatore non sicuro ha immesso delle parole d'ordine non corrispondenti. I dati di autenticazione dell'utente non sono stati modificati.

Risposta dell'utente: La modifica richiede che la parola d'ordine venga immessa due volte, la seconda per la verifica. Probabilmente la parola d'ordine per la verifica è stata digitata in modo non corretto.

ICA2217 **(***servizio***) L'utente** *nome* **da** *indirizzo IP origine* **(sicuro) non ha immesso parole d'ordine corrispondenti (verifica).**

Spiegazione: È stata richiesta una modifica della parola d'ordine e l'utente indicato dall'indirizzo IP di origine specificato su un adattatore sicuro ha immesso delle parole d'ordine non corrispondenti. I dati di autenticazione dell'utente non sono stati modificati.

Risposta dell'utente: La modifica richiede che la parola d'ordine venga immessa due volte, la seconda per la verifica. Probabilmente la parola d'ordine per la verifica è stata digitata in modo non corretto.

ICA2218 *servizio* **Sessione** *id sessione* **avviata per** *id utente* **da un adattatore sicuro (***indirizzo IP origine***:***indirizzo IP destinazione***).**

Spiegazione: Questo messaggio viene generato all'inizio di ogni sessione indicata.

ICA2219 *servizio* **Sessione** *id sessione* **terminata per** *id utente* **da un adattatore sicuro (***indirizzo IP origine***:***indirizzo IP destinazione***); byte** *byte totali***.**

Spiegazione: Questo messaggio viene generato alla fine di ogni sessione indicata. Byte Totali indica il numero di byte trasferiti durante la sessione. I servizi (ad esempio, ptelnetd) che non supportano Byte Totali indicheranno zero.

ICA2220 **(***servizio***) L'utente** *id utente* **ha avviato una sessione proxy trasparente da** *indirizzo IP origine* **(sito sicuro) a** *indirizzo IP destinazione***.**

Spiegazione: Questo messaggio viene generato all'inizio di ogni sessione proxy trasparente. Una sessione viene avviata quando l'ID utente, l'indirizzo IP di origine e quello di destinazione sono noti al firewall. Sono consentite solo le sessioni avviate da un sito sicuro.

Azione del sistema: Consentire il proxy trasparente.

ICA2221 **(***servizio***) Avvertenza: L'IP (***indirizzo IP controllo***) all'estremità peer della riga di controllo non era uguale all'IP (***indirizzo IP dati***) all'estremità peer della riga dei dati.**

Spiegazione: Assicurarsi che l'indirizzo IP del peer a cui è collegato il socket Collegamento di controllo sia uguale a quello a cui è collegato il socket Collegamento di dati, per garantire la sicurezza contro eventuali intrusioni. Questa condizione cambia nel caso in cui viene utilizzato il programma di distribuzione di rete o se la destinazione ha utilizzato più adattatori.

Azione del sistema: Controllare se il server FTP di destinazione sta utilizzando più adattatori o se è in esecuzione il programma di distribuzione di rete. Assicurarsi che i filtri consentano solo agli indirizzi validi di passare attraverso le porte 20 e 21.

ICA2222 **(***servizio***) Avvertenza! Violazione di protocollo. Ricevuto comando RFC non compatibile** *stringa non valida***; Previsto** *stringa protocollo***.**

Spiegazione: Il servizio indicato ha ricevuto una stringa imprevista non compatibile con RFC; possibile intruso.

Azione del sistema: Utilizzare un client compatibile con RFC per il servizio indicato.

ICA3001 ***ATTENZIONE*: L'utente reale è** *id nome utente***, non** *nome utente di collegamento al socks*

Spiegazione: Possibile tentativo di violazione della sicurezza; nome utente non autenticato.

ICA3006 *numero* **byte da** *client***,** *numero* **byte da** *server*

Spiegazione: Questo messaggio indica il numero di byte trasferiti tra il daemon sockd ed i rispettivi host del server e del client.

ICA3007 **Collegamento rifiutato per il superamento del numero massimo di collegamenti.**

Spiegazione: Il server Socks è configurato per accettare soltanto un determinato numero massimo di sessioni client. Questo messaggio viene generato quando viene raggiunta questa soglia e continuano ad arrivare altre richieste di collegamento.

Azione del sistema: Il collegamento appena tentato viene interrotto.

Risposta dell'utente: Il numero massimo di collegamenti simultanei è determinato dal parametro SOCKS5_MAXCHILD in socks5.conf. Aumentare il valore di questa impostazione

ed aggiornare il server. Per ulteriori informazioni consultare il manuale di riferimento relativo ad IBM Firewall.

ICA3010 collegato -- Bind da *utente***(***real_user***)@***src_addr* **per** *dst_addr* **(***porta di destinazione***)**

Spiegazione: Collegamento stabilito.

ICA3011 collegato -- Collegamento da *utente***(***real_user***)@***src_addr* **a** *dst_addr* **(***applicazione***)**

Spiegazione: Il collegamento socket ad un sito esterno è stato eseguito correttamente.

ICA3012 Rifiutato -- Collegamento da *utente***(***real_user***)@***src_addr* **a** *dst_addr* **(***applicazione***)**

Spiegazione: L'host remoto ha rifiutato il collegamento.

ICA3013 select() *errno*

Spiegazione: Errore di sistema.

ICA3014 Terminato -- Bind da *utente***(***real_user***)@***src_addr* **per** *dst_addr* **(** *porta di destinazione***).(***numero* **byte da** *client***,** *numero* **byte da** *server***)**

Spiegazione: Collegamento terminato.

ICA3015 Terminato -- Collegamento da *utente***(***real_user***)@***src_addr* **a** *dst_addr* **(***host di destinazione***).(***numero* **byte da** *client***,** *numero* **byte da** *server***)**

Spiegazione: Collegamento al server terminato.

ICA3016 ***Impossibile trovare l'interfaccia appropriata per la comunicazione con *host di destinazione*

Spiegazione: Il file /etc/sockd.route non contiene informazioni di instradamento per l'host di destinazione specificato.

ICA3017 Impossibile eseguire il comando shell per pid *processo sockd*

Spiegazione: Il daemon Sockd non è in grado di eseguire un comando /bin/sh.

Risposta dell'utente: Verificare che la shell /bin/sh sia disponibile sul sistema.

ICA3018 Rifiutato -- Bind da *utente***(***real_user***)@***src_addr* **per** *dst_addr*

Spiegazione: L'host remoto ha rifiutato il collegamento.

ICA3019 Errore in GetDst() da host *socks_src_name***:** *errno*

Spiegazione: Errore nella risoluzione dell'indirizzo di destinazione per il collegamento richiesto.

ICA3022 Campo ?= non valido alla riga *numero riga*

Spiegazione: È stata trovata un'entrata non valida nel file /etc/sockd.conf.

ICA3023 Confronto non valido alla riga *numero riga*

Spiegazione: È stata trovata un'entrata non valida nel file /etc/sockd.conf.

ICA3024 Entrata non valida alla riga *numero riga*

Spiegazione: È stata trovata un'entrata non valida nel file /etc/sockd.route.

ICA3025 Campo permit/deny non valido alla riga *numero riga*

Spiegazione: È stata trovata un'entrata non valida nel file /etc/sockd.conf.

ICA3026 Numero di porta non valido alla riga *numero riga*

Spiegazione: È stata trovata un'entrata non valida nel file /etc/sockd.conf.

ICA3027 Comando shell non riuscito (*stato di esecuzione***) per \"***cmd***\"**

Spiegazione: Il comando shell visualizzato non è stato eseguito correttamente.

Risposta dell'utente: Verificare che il processore della shell sia disponibile sul sistema.

ICA3030 Impossibile aprire il file di configurazione (*/etc/sockd.conf***)**

Spiegazione: La richiesta di apertura per il file indicato non è stata eseguita correttamente.

ICA3031 Impossibile aprire il file di instradamento (*/etc/sockd.route***):** *errno*

Spiegazione: La richiesta di apertura per il file indicato non è stata eseguita correttamente.

Risposta dell'utente: Contattare il responsabile del firewall. È stato fornito un file assunto durante l'installazione del firewall.

ICA3032 Impossibile aprire il file utente (*nome file utente***):** *errno*

Spiegazione: Non è stato possibile trovare il nome file specificato per *=userlist in una regola permit.

ICA3033 Risultato imprevisto da Validate()

Spiegazione: È stata specificata la verifica Identd del nome utente, Identd ha restituito risultati imprevisti.

ICA3035 Impossibile collegarsi a identd su *host client*

Spiegazione: È stata specificata la verifica Identd del nome utente, Identd non ha risposto.

ICA3039 Errore -- il comando shell \"*cmd***\" non contiene caratteri alfanumerici.**

Spiegazione: Comando shell non valido, fare riferimento al messaggio di log.

ICA3040 Errore -- shell_cmd fork() *errno*

Spiegazione: Il daemon Sockd non è in grado di passare al processo child tramite 'fork()'.

ICA3041 Errore: impossibile richiamare l'indirizzo client.

Spiegazione: Errore restituito dalla chiamata 'getpeername()'.

Risposta dell'utente: Controllare l'instradamento e la configurazione DNS.

ICA3042 **Errore -- comando non definito (0x***ricevuto-comando-esa***) ricevuto dall'host** *indirizzo client*

Spiegazione: Ricevuto comando non valido dall'applicazione client.

Risposta dell'utente: È possibile che si sia verificato un problema di configurazione del client o una mancata corrispondenza del livello di supporto tra client e firewall.

ICA3043 **Errore -- versione errata (0x***num-versione-esa***) ricevuta dall'host** *indirizzo client***.**

Spiegazione: Il firewall supporta la versione socks 4.2.

Risposta dell'utente: È possibile che si sia verificato un problema di configurazione del client o una mancata corrispondenza del livello di supporto tra client e firewall.

ICA3044 **Non riuscito -- Collegamento da** *utente***(***real_user***)@***src_addr* **a** *dst_addr* **(***applicazione***). Codice di errore:** *comando errato errno***.**

Spiegazione: Richiesta di collegamento non riuscita.

ICA3045 **Non riuscito -- Bind da** *utente***(***real_user***)@***src_addr* **per** *dst_addr***. Errore: collegato ad host errato** *dst_name* **(***dst_port (application)***).**

Spiegazione: Richiesta di bind non riuscita.

ICA3046 **Non riuscito -- Bind da** *utente***(***real_user***)@***src_addr* **per** *dst_addr***. Codice di errore:** *comando errato errno***.**

Spiegazione: Richiesta di bind non riuscita.

ICA3047 **Timeout -- Bind da** *utente***(***real_user***)@***src_addr* **per** *dst_addr*

Spiegazione: Timeout del collegamento.

ICA3048 **Comando shell troppo lungo:** *comando***...**

Spiegazione: Il comando che deve essere eseguito, dal file /etc/sockd.conf, è troppo lungo.

ICA3049 **Timeout -- Collegamento da** *utente***(***real_user***)@***src_addr* **a** *dst_addr* **(***applicazione***)**

Spiegazione: Timeout del collegamento.

ICA3050 *regola di filtro sockd.conf corrisposta*

Spiegazione: La regola di filtro del file /etc/sockd.conf corrispondente al collegamento socks.

ICA3051 **sockd_route() AIX non può trovare l'interfaccia per** *indirizzo remoto***.**

Spiegazione: Impossibile trovare le informazioni sull'instradamento dell'interfaccia.

ICA3052 **Errore nell'impostazione dell'ID utente su "nobody".**

Spiegazione: Impossibile impostare l'ID utente del processo child sockd su "nobody".

ICA3053 **Errore nel popen (script di instradamento AIX):** *messaggio di errore di sistema*

Spiegazione: Errore nell'esecuzione dello script per trovare le informazioni di instradamento.

ICA3054 Errore grave di assegnazione della memoria in sockd_route() AIX.

Spiegazione: Errore di assegnazione di memoria nel tentativo di raccogliere informazioni di instradamento.

ICA3055 Errore grave nell'analisi sintattica di sockd_route() AIX per il primo spazio in: *riga di immissione*

Spiegazione: Errore durante l'analisi delle informazioni sull'instradamento di sistema.

ICA3056 Errore grave nell'analisi sintattica di sockd_route() AIX per il secondo spazio in: *riga di immissione*

Spiegazione: Errore durante l'analisi delle informazioni sull'instradamento di sistema.

ICA3057 Errore grave nella lettura sockd_route() AIX dell'emissione script di instradamento: *messaggio di errore di sistema*

Spiegazione: Errore durante la lettura dell'emissione script.

ICA3058 Errore nel popen (script dell'adattatore AIX): *messaggio di errore di sistema*

Spiegazione: Errore nell'esecuzione dello script per trovare le informazioni sull'interfaccia.

ICA3101 Errore sockd durante l'invio dei dati - select(): *messaggio di errore di sistema*

Spiegazione: (SOCKS422) Errore durante l'invio dei dati.

ICA3102 Errore sockd durante l'invio dei dati - write(): *messaggio di errore di sistema*

Spiegazione: (SOCKS422) Errore durante l'invio dei dati.

ICA3103 Errore sockd durante la ricezione dei dati - select(): *messaggio di errore di sistema*

Spiegazione: (SOCKS422) Errore durante la ricezione dei dati.

ICA3104 Errore sockd durante la ricezione dei dati - read(): *messaggio di errore di sistema*

Spiegazione: (SOCKS422) Errore durante la ricezione dei dati.

ICA3105 Impossibile creare il file di ID processo *nome file***.**

Spiegazione: (SOCKS422) Creazione/scrittura del file di ID processo non riuscita.

ICA3106 Fork di sockd al child non riuscito: *messaggio di errore di sistema*

Spiegazione: (SOCKS422) Il tentativo di eseguire la fork sul child per gestire una richiesta SOCKS non è riuscito.

ICA3107 Impostazione dell'opzione SO_LINGER del socket in arrivo non riuscita: *messaggio di errore di sistema*

Spiegazione: (SOCKS422) Errore non grave.

ICA3108 Impostazione dell'opzione SO_LINGER del socket in partenza non riuscita: *messaggio di errore di sistema*

Spiegazione: (SOCKS422) Errore non grave.

ICA3109 Entrata non valida alla riga *numero riga* **del file** *nome file***.**

Spiegazione: (SOCKS422) Sintassi dell'entrata di configurazione non corretta.

ICA3110 Campo di interfaccia non valido alla riga *numero riga* **del file** *nome file***.**

Spiegazione: (SOCKS422) Sintassi dell'entrata di configurazione non corretta.

ICA3111 Destinazione IP non valida alla riga *numero riga* **del file** *nome file***.**

Spiegazione: (SOCKS422) Sintassi dell'entrata di configurazione non corretta.

ICA3112 Maschera di destinazione non valida alla riga *numero riga* **del file** *nome file***.**

Spiegazione: (SOCKS422) Sintassi dell'entrata di configurazione non corretta.

ICA3113 Analizzate *numero* **righe del file** *nome file***.**

Spiegazione: (SOCKS422) Sintassi dell'entrata di configurazione non corretta.

ICA3114 Righe non valide rilevate nel file *nome file***.**

Spiegazione: (SOCKS422) File di configurazione vuoto o sintassi non corretta.

Risposta dell'utente: Correggere il file di configurazione indicato.

ICA3115 Campo 'permit/deny' non valido alla riga *numero riga* **del file** *nome file***.**

Spiegazione: (SOCKS422) Sintassi dell'entrata di configurazione non corretta.

ICA3116 Campo '?=' non valido alla riga *numero riga* **del file** *nome file***.**

Spiegazione: (SOCKS422) Sintassi dell'entrata di configurazione non corretta.

ICA3117 IP di origine non valido alla riga *numero riga* **del file** *nome file***.**

Spiegazione: (SOCKS422) Sintassi dell'entrata di configurazione non corretta.

ICA3118 Maschera di origine non valida alla riga *numero riga* **del file** *nome file***.**

Spiegazione: (SOCKS422) Sintassi dell'entrata di configurazione non corretta.

ICA3119 Confronto non valido alla riga *numero riga* **del file** *nome file***.**

Spiegazione: (SOCKS422) Sintassi dell'entrata di configurazione non corretta.

ICA3120 Numero di porta non valido alla riga *numero riga* **del file** *nome file***.**

Spiegazione: (SOCKS422) Sintassi dell'entrata di configurazione non corretta.

ICA3121 Ricevuto SIGUSR1 - dump della configurazione socks.

Spiegazione: (SOCKS422) Il segnale per eseguire il dump della configurazione attiva al file di log, dopo questo messaggio.

ICA3122 Sockd non ha potuto eseguire il fork del daemon: *messaggio di errore di sistema*

Spiegazione: (SOCKS422) Il comando fork per inizializzare il daemon sockd non è riuscito.

Risposta dell'utente: Correggere l'errore di sistema indicato e riavviare sockd.

ICA3123 Avvio del server Sockd in corso.

Spiegazione: (SOCKS422) Il server Sockd è stato inizializzato correttamente ed è in attesa dei collegamenti.

ICA3124 Errore grave di inizializzazione di sockd - bind(): *messaggio di errore di sistema*

Spiegazione: (SOCKS422) L'inizializzazione del server Sockd non è riuscita, il daemon è stato arrestato.

Risposta dell'utente: Correggere l'errore di sistema indicato e riavviare sockd.

ICA3125 Errore grave di inizializzazione di sockd - listen(): *messaggio di errore di sistema*

Spiegazione: (SOCKS422) L'inizializzazione del server Sockd non è riuscita, il daemon è stato arrestato.

Risposta dell'utente: Correggere l'errore di sistema indicato e riavviare sockd.

ICA3126 Errore grave di sockd - tentativo principale di accept(): *messaggio di errore di sistema*

Spiegazione: (SOCKS422) La routine principale del server Sockd non è riuscita, il daemon è stato arrestato.

Risposta dell'utente: Correggere l'errore di sistema indicato e riavviare sockd.

ICA3127 Il server sockd ha ricevuto il segnale di arresto.

Spiegazione: root o nobody ha arrestato il processo, il daemon è stato arrestato.

Risposta dell'utente: Riavviare il server sockd se richiesto dal responsabile (tipo "sockd").

ICA3128 Errore grave di inizializzazione di sockd - socket(): *messaggio di errore di sistema*

Spiegazione: L'inizializzazione del server Sockd non è riuscita, il daemon è stato arrestato.

Risposta dell'utente: Correggere l'errore di sistema indicato e riavviare sockd.

ICA3129 Errore grave di inizializzazione di sockd - *funzione errata***:** *messaggio di errore di sistema*

Spiegazione: L'inizializzazione del server Sockd non è riuscita per la funzione indicata, il daemon è stato arrestato.

Risposta dell'utente: Correggere l'errore di sistema indicato e riavviare sockd.

ICA3130 Errore di sockd - *funzione errata***:** *messaggio di errore di sistema*

Spiegazione: Il server sockd ha rilevato un errore nella funzione indicata. Il daemon continua, ma i collegamenti possono essere rifiutati o interrotti.

Risposta dell'utente: Se il problema persiste, arrestare sockd, correggere l'errore di sistema indicato e riattivarlo.

ICA3131 Errore nella lettura di *nome file***. Vengono utilizzati i dati precedentemente memorizzati nella cache.**

Spiegazione: Non è stato possibile leggere il file o questo conteneva dati non corretti. Un messaggio precedente fa riferimento al problema. Sockd continuerà a funzionare con i dati memorizzati nella cache dalla versione precedente del file.

Risposta dell'utente: Correggere l'errore nel file indicato.

ICA3132 Indicatore sconosciuto -*valore***.**

Spiegazione: L'indicatore non è stato riconosciuto, il daemon viene arrestato.

Risposta dell'utente: Correggere la sintassi e riavviare sockd.

ICA3133 Parametro sconosciuto *valore***.**

Spiegazione: Il parametro indicato non è stato riconosciuto, il daemon viene arrestato.

Risposta dell'utente: Correggere la sintassi e riavviare sockd.

ICA3134 Conflitto delle opzioni *opzione1* **e** *opzione2***.**

Spiegazione: Le opzioni indicate non possono essere specificate insieme, il daemon è stato arrestato.

Risposta dell'utente: Correggere la sintassi e riavviare sockd.

ICA3135 Errore Sockd - *funzione in errore***: codice di errore = 0x***codice di errore della funzione*

Spiegazione: Il server sockd ha rilevato un errore nella funzione indicata. Il daemon si arresta.

Risposta dell'utente: Correggere l'errore di sistema indicato e riavviare sockd.

ICA3700 Errore di inizializzazione WinSocket : *errore WinSocket*

Spiegazione: Si è verificato un errore durante l'inizializzazione di WinSocket.

Risposta dell'utente: Correggere l'errore di sistema indicato e riavviare sockd.

ICA4000 *programma* **- Avvertenza: ricevuto segnale** *segnale***, arresto dell'elaborazione in corso...**

Spiegazione: Arresto dovuto alla ricezione del segnale.

ICA4001 Arresto di *programma* **come PID** *ID processo*

Spiegazione: Visualizza la fine del processo di completamento del daemon. Messaggio informativo.

ICA4002 ID temporaneo

Spiegazione: Messaggio informativo.

ICA4003 Problema con il processo child *ID processo***.**

Spiegazione: Non è stato possibile creare un processo child.

ICA4004 Errore grave. Arresto di fwpagerd al segnale *segnale***.**

Spiegazione: Programma di gestione dei segnali.

ICA4005 Nessun daemon fwpagerd in esecuzione, *programma* **non trovato.**

Spiegazione: Non è stato possibile inviare la chiamata perché il daemon non era attivo.

ICA4006 Nessun daemon fwpagerd in esecuzione con id processo *ID processo***.**

Spiegazione: Non è stato possibile trovare l'ID processo del daemon.

ICA4007 Avvio di *programma* **come PID** *ID processo*

Spiegazione: Visualizza le informazioni all'avvio. Messaggio informativo.

ICA4008 Impossibile impostare sigignore per SIGPIPE.

Spiegazione: Errore durante l'impostazione per ignorare il segnale di pipe spezzata.

ICA4009 Impossibile impostare sigset per SIGCHILD.

Spiegazione: Errore durante l'impostazione per catturare il segnale di child interrotto.

ICA4010 Impossibile impostare il processo di arresto.

Spiegazione: Errore durante l'impostazione del segnale per la cattura del processo di arresto.

ICA4011 Impossibile aprire il socket.

Spiegazione: Errore durante l'apertura del socket.

ICA4012 Impossibile impostare sigset per SIGTERM.

Spiegazione: Errore durante l'impostazione per catturare i segnali SIGTERM e SIGINT.

ICA4013 Impossibile impostare l'opzione di riutilizzo del socket.

Spiegazione: Errore durante l'impostazione dell'opzione di riutilizzo del socket.

ICA4014 Impossibile impostare l'opzione di ritardo del socket.

Spiegazione: Errore durante l'impostazione dell'opzione di ritardo del socket.

ICA4015 Impossibile eseguire il bind del socket alla porta.

Spiegazione: Errore durante il tentativo di eseguire il bind del socket alla porta.

ICA4016 Impossibile impostare l'ascolto sul socket.

Spiegazione: Errore durante l'impostazione di ascolto sul socket.

ICA4017 Il servizio *nome servizio* **che sta utilizzando il socket TCP** *socket***.**

Spiegazione: Messaggio informativo.

ICA4018 Chiamata di funzione select() non riuscita.

Spiegazione: Errore nella chiamata di funzione interna.

ICA4019 Errore grave da new_work().

Spiegazione: Errore grave interno dalla routine new_work.

ICA4020 Errore(*programma***): Non è stato possibile scrivere sul socket di flusso:** *socket*

Spiegazione: Possibile errore di sistema.

Risposta dell'utente: Controllare l'utilizzo del socket.

ICA4021 Problema nella ricezione della risposta.

Spiegazione: Problema nella ricezione della risposta dal modem.

Risposta dell'utente: Controllare i collegamenti al modem e la stringa di inizializzazione.

ICA4022 Richiesta eseguita correttamente.

Spiegazione: Messaggio informativo.

ICA4023 Richiesta non riuscita.

Spiegazione: La richiesta di invio della chiamata non è stata eseguita correttamente.

ICA4024 Errore(*programma***): Priorità fuori intervallo (***priorità minima* **-** *priorità massima***).**

Spiegazione: Intervallo di priorità non corretto.

Risposta dell'utente: Correggere l'intervallo di priorità. I valori validi sono compresi tra -1 e 5.

ICA4025 Errore(*programma***): L'indirizzo deve avere il formato ID@carrier quando si utilizza l'opzione -n.**

Spiegazione: Sintassi di utilizzo del comando non corretta.

Risposta dell'utente: Correggere la sintassi di utilizzo del comando.

ICA4026 Errore(*programma***): Host** *nome host* **sconosciuto**

Spiegazione: Non è stato possibile risolvere il nome host.

Risposta dell'utente: Controllare il nome host.

ICA4027 Errore(*programma***): Non è stato possibile aprire il socket di flusso:** *errno*

Spiegazione: Non è stato possibile creare un nuovo socket.

ICA4028 Errore(*programma***): Non è stato possibile impostare le opzioni del socket:** *errno*

Spiegazione: Non è stato possibile impostare l'opzione di ritardo del socket.

ICA4029 Errore(*programma***): Non è stato possibile effettuare il collegamento a** *host* **:** *errno***.**

Spiegazione: Non è stato possibile collegarsi all'host.

Risposta dell'utente: Controllare la configurazione della porta seriale e l'esistenza del file del programma di controllo unità.

ICA4030 Errore(*programma***): Non è stato possibile scrivere sul socket di flusso:** *errno***.**

Spiegazione: Non è stato possibile scrivere al socket di flusso.

ICA4031 Problema nella ricezione della risposta. Condizione del messaggio sconosciuta.

Spiegazione: Problema nella ricezione della risposta dal modem.

ICA4032 Messaggio inviato in coda correttamente.

Spiegazione: Messaggio informativo. Il messaggio è stato inviato alla coda.

ICA4033 Errore nel messaggio. Nessun messaggio inviato.

Spiegazione: Non è stato possibile inviare il messaggio alla coda del cercapersone.

ICA4034 *data* **Non riuscito (ID** *ID* **Priorità** *priorità* **Secondi** *periodo* **Tentativi** *tentativi***) [***fromEntry***]** *nome persona***:** *messaggio***.**

Spiegazione: Visualizza questo messaggio quando la chiamata non viene inviata correttamente.

ICA4035 Impossibile reinserire in coda il messaggio *messaggio* **da** *programma* **a** *persona***.**

Spiegazione: Non è stato possibile inviare il messaggio alla coda del cercapersone.

ICA4036 Riuscito (ID *ID* **Priorità** *priorità* **Secondi** *periodo* **Tentativi** *tentativi***) [***fromEntry***]** *nome persona***:** *messaggio***.**

Spiegazione: Visualizza questo messaggio quando la chiamata viene inviata correttamente.

ICA4037 Dump in *file dump* **(ID** *ID* **Priorità** *priorità* **Secondi** *periodo* **Tentativi** *tentativi***) [***fromEntry***]** *nome persona***:** *messaggio***.**

Spiegazione: Viene eseguito il dump in un file delle chiamate che non vengono inviate immediatamente per tentativi futuri.

ICA4038 Impossibile scrivere nel file di dump *file di dump***.**

Spiegazione: Non è possibile eseguire la scrittura nel file di dump.

Risposta dell'utente: Controllare le autorizzazioni del sistema di file.

ICA4039 IpcKey: 0x/*pcKey*

Spiegazione: Messaggio informativo.

ICA4040 Tempo per ripetizione tentativi di *numero* **minuti scaduto.**

Spiegazione: Non è stato possibile inizializzare il modem dopo il numero di minuti specificati.

Risposta dell'utente: Controllare la stringa di inizializzazione.

ICA4041 Rilevato messaggio alfanumerico per cercapersone numerico.

Spiegazione: I cercapersone numerici non possono contenere dati alfanumerici.

Risposta dell'utente: Correggere l'errore utilizzando il menu smitty/SMIT.

ICA4042 La persona non riceve le chiamate.

Spiegazione: È possibile che il cercapersone non sia attivo.

Risposta dell'utente: Verificare che il cercapersone sia attivo.

ICA4043 La portante *portante* non esiste.

Spiegazione: La portante specificata non esiste.

Risposta dell'utente: Correggere l'errore utilizzando il menu smitty/SMIT.

ICA4044 La portante *portante* non dispone di un numero di telefono DTMF.

Spiegazione: La portante specificata non dispone del numero di telefono DTMF.

Risposta dell'utente: Correggere l'errore utilizzando il menu smitty/SMIT.

ICA4045 Numero del cercapersone *numero cercapersone* troppo lungo; lunghezza massima della portante di *Lung. portante*.

Spiegazione: Il numero del cercapersone è troppo esteso per la portante.

Risposta dell'utente: Utilizzare un altro numero di cercapersone la cui lunghezza sia inferiore a quella massima della portante.

ICA4046 Numero del cercapersone *numero cercapersone* troppo lungo; la lunghezza assunta è di *Lung. assunta portante*.

Spiegazione: Questo messaggio si presenta quando la lunghezza assunta è inferiore.

Risposta dell'utente: Correggere l'errore utilizzando il menu smitty/SMIT. Aumentare la lunghezza assunta.

ICA4047 Problema alla riga *numero riga* del file del modem *nome file modem*.

Spiegazione: Il file di definizione del modem contiene un carattere non valido.

Risposta dell'utente: Correggere l'errore utilizzando il menu smitty/SMIT.

ICA4048 Impossibile aprire il modem sull'unità /dev/*NomeUnità*.

Spiegazione: Non è stato possibile aprire il modem sull'unità specificata.

Risposta dell'utente: Controllare o riconfigurare la porta seriale. Controllare l'unità.

ICA4049 Modem aperto su /dev/*nome unità*.

Spiegazione: Messaggio informativo. Il modem è stato aperto correttamente sulla porta seriale.

ICA4050 Impossibile impostare le caratteristiche del modem.

Spiegazione: Errore durante il tentativo di impostazione delle caratteristiche del modem.

Risposta dell'utente: Controllare la stringa di inizializzazione del modem.

ICA4051 Impossibile inizializzare il modem dopo *numero* tentativi.

Spiegazione: Non è stato possibile inizializzare il modem.

Risposta dell'utente: Controllare la stringa di inizializzazione del modem e la configurazione della porta seriale.

ICA4062 Impossibile trasmettere la richiesta di modo automatico.

Spiegazione: Impossibile trasmettere il segnale della richiesta di modo automatico.

Risposta dell'utente: Controllare i parametri della portante utilizzando il menu smitty/SMIT.

ICA4063 Segnale di proseguimento dalla portante *portante* **dopo** *numero* **tentativi non ricevuto.**

Spiegazione: È possibile che al momento la portante sia occupata.

Risposta dell'utente: Controllare i parametri della portante utilizzando il menu smitty/SMIT e ritentare l'operazione successivamente.

ICA4064 Errore di comunicazione durante la richiesta comandi con la portante *portante***.**

Spiegazione: È possibile che l'errore di comunicazione si sia verificato per una serie di motivi. Tentare di nuovo l'operazione successivamente.

Risposta dell'utente: Controllare i parametri della portante utilizzando il menu smitty/SMIT e ritentare l'operazione successivamente.

ICA4065 Impossibile ricevere risposte alla richiesta di collegamento.

Spiegazione: Il modem non può ricevere risposte alla richiesta di collegamento.

Risposta dell'utente: Controllare la stringa di inizializzazione del modem ed i parametri della portante.

ICA4066 La portante *portante* **non ha risposto al tentativo di collegamento.**

Spiegazione: La portante non ha risposto al tentativo di collegamento.

Risposta dell'utente: Controllare i parametri della portante utilizzando il menu smitty/SMIT e ritentare l'operazione successivamente.

ICA4067 La portante *portante*

ICA4071 Errore(*programma***): Impossibile assegnare memoria per nuovo tentativo della portante:** *errno***.**

Spiegazione: Possibili errori di assegnazione della memoria o di sistema.

ICA4072 Errore(*programma***): Impossibile effettuare l'aggiunta all'elenco di nuovi tentativi della portante** *errno***.**

Spiegazione: È possibile che la portante non esista.

Risposta dell'utente: Controllare la validità della portante e ritentare l'operazione.

ICA4073 Collegamento dati alla portante *portante* **al** *numero di telefono* **non riuscito dopo** *numero* **tentativi.**

Spiegazione: Il collegamento dati non è riuscito.

Risposta dell'utente: Controllare i collegamenti al modem ed i parametri della portante utilizzando il menu smitty/SMIT.

ICA4074 Richiesta di ID dalla portante *portante* **non ricevuta dopo** *numero* **tentativi.**

Spiegazione: La portante non ha risposto con una richiesta di ID o di conferma ricezione.

Risposta dell'utente: Assicurarsi che la portante utilizzi il protocollo TAP (TeleAlphanumeric Protocol).

ICA4075 Errore di comunicazione durante il collegamento con la portante *portante***.**

Spiegazione: È possibile che l'errore di comunicazione si sia verificato per una serie di motivi.

Risposta dell'utente: Controllare i parametri della portante utilizzando il menu smitty/SMIT.

ICA4076 Numero massimo di tentativi di collegamento alla portante *portante* **superato.**

Spiegazione: La portante non è riuscita ad inviare una risposta rispettando il numero di tentativi specificato.

Risposta dell'utente: Controllare i parametri della portante e tentare di nuovo l'operazione.

ICA4077 Segnale di proseguimento del messaggio non ricevuto dalla portante *portante***.**

Spiegazione: La portante non è riuscita ad inviare la richiesta di proseguimento.

Risposta dell'utente: Controllare i parametri della portante e tentare di nuovo l'operazione.

ICA4078 Impossibile creare blocchi.

Spiegazione: La portante non è riuscita a creare dei blocchi per la trasmissione.

Risposta dell'utente: Controllare i parametri della portante utilizzando il menu smitty/SMIT.

ICA4079 La portante *portante* **non ha risposto alla consegna del messaggio.**

Spiegazione: La portante ha riscontrato dei problemi nella consegna del messaggio.

Risposta dell'utente: Controllare i parametri della portante utilizzando il menu smitty/SMIT.

ICA4080 Scollegamento forzato della portante *portante* **durante la consegna del messaggio.**

Spiegazione: Scollegamento forzato della portante durante la consegna del messaggio.

Risposta dell'utente: Controllare i parametri della portante e la stringa di inizializzazione del modem.

ICA4081 Messaggio o ID cercapersone rifiutato dalla portante *portante***.**

Spiegazione: Il messaggio o l'ID cercapersone è stato rifiutato dalla portante.

Risposta dell'utente: Controllare la validità dell'ID cercapersone, l'attivazione del cercapersone ed i parametri della portante.

ICA4082 Errore di comunicazione durante la consegna del messaggio alla portante *portante***.**

Spiegazione: È possibile che l'errore di comunicazione si sia verificato per una serie di motivi.

Risposta dell'utente: Controllare i parametri della portante utilizzando il menu smitty/SMIT.

ICA4083 Conferma dalla portante *portante* **dopo** *numero massimo* **tentativi non riuscita.**

Spiegazione: Questo messaggio si verifica quando la portante è occupata o se non è possibile stabilire un collegamento.

Risposta dell'utente: Controllare i parametri della portante utilizzando il menu smitty/SMIT e ripetere l'operazione dopo alcuni minuti.

ICA4084 Impossibile trasmettere <**EOT**>**.**

Spiegazione: Il modem non può trasmettere <EOT>.

Risposta dell'utente: Controllare i collegamenti del modem e la stringa di inizializzazione.

ICA4085 Impossibile ricevere risposta a <**EOT**>**.**

Spiegazione: Il modem non può ricevere risposte a <EOT>.

Risposta dell'utente: Controllare i collegamenti del modem e la stringa di inizializzazione.

ICA4086 La portante *portante* **non ha risposto a** <**EOT**>**.**

Spiegazione: La portante non può rispondere ai dati trasmessi.

Risposta dell'utente: Controllare la validità della portante ed i collegamenti del modem.

ICA4087 La portante *portante* **ha risposto con un errore di dati inaccettabile a causa del contenuto.**

Spiegazione: La portante non può rispondere ai dati trasmessi.

Risposta dell'utente: Controllare i parametri della portante utilizzando il menu smitty/SMIT.

ICA4088 Impossibile aprire il file dei valori assunti *nome percorso assunto***.**

Spiegazione: È possibile che il file dei valori assunti del modem non esista o che abbia autorizzazioni non corrette.

Risposta dell'utente: Controllare l'esistenza e le autorizzazioni del file.

ICA4089 File dei valori assunti *nome percorso assunto* **incompleto.**

Spiegazione: Il file dei valori assunti del modem non contiene tutti i dati.

Risposta dell'utente: Correggere l'errore utilizzando il menu smitty/SMIT.

ICA4090 Numero di linea esterna non valido nel file di valori assunti *nome percorso assunto* **alla riga** *numero riga***.**

Spiegazione: Il numero di linea esterna del file di database della portante non è valido.

Risposta dell'utente: Eliminare il file di database della portante.

ICA4091 Valore per la velocità in baud non valido nel file dei valori assunti *nome file* **alla riga** *numero riga***.**

Spiegazione: Il valore per la velocità in baud del file di database della portante non è valido.

Risposta dell'utente: Eliminare il file di database della portante.

ICA4092 Valore per i bit di dati non valido nel file dei valori assunti *nome file* **alla riga** *numero riga***.**

Spiegazione: Il valore per i bit di dati nel file di database della portante non è valido.

Risposta dell'utente: Eliminare il file di database della portante.

ICA4093 Valore per la parità non valido nel file dei valori assunti *nome file* **alla riga** *numero riga***.**

Spiegazione: Il valore per la parità del file di database della portante non è valido.

Risposta dell'utente: Eliminare il file di database della portante.

ICA4094 Valore per i bit di stop non valido nel file dei valori assunti *nome file* **alla riga** *numero riga***.**

Spiegazione: Il valore per i bit di stop nel file di database della portante non è valido.

Risposta dell'utente: Eliminare il file di database della portante.

ICA4095 Tag *ID tag* **sconosciuta nel file dei valori assunti** *nome file* **alla riga** *numero riga***.**

Spiegazione: Il valore della tag nel file di database della portante non è valido.

Risposta dell'utente: Eliminare il file di database della portante.

ICA4096 Numero di parametri errato.

Spiegazione: Messaggio informativo.

ICA4097 Errore(*programma***): Impossibile creare l'elenco delle portanti. Problemi di memoria.**

Spiegazione: Passibili problemi di memoria o di sistema.

ICA4098 Errore(*programma***): Errori nel file delle portanti del cercapersone** *file delle portanti***.**

Spiegazione: I dati del file di database della portante non sono validi.

Risposta dell'utente: Controllare che il file di database della portante non abbia tag non valide.

ICA4099 Errore(*programma***): Impossibile richiamare il token IPC** *errno***.**
ICA4100 Errore(*programma***): Impossibile richiamare l'elenco dei tentativi. Possibili problemi di memoria.**

Spiegazione: Possibili problemi di memoria o errori di sistema.

ICA4101 Errore(*portante***): Impossibile creare la coda, page_q_err:** *pageQErr***.**
ICA4102 Errore(*programma***): Impossibile impostare la cattura del segnale per SIGTERM/SIGINT:** *errno***.**

Spiegazione: Possibile errore di sistema.

ICA4103 Errore(*programma***): Impossibile impostare le caratteristiche del modem per la portante** *portante***.**

Spiegazione: Non è stato possibile impostare il modem.

Risposta dell'utente: Controllare la configurazione della porta seriale e la stringa di inizializzazione.

ICA4104 Tag *tag* **mancante per la portante** *portante***.**

Spiegazione: Informazioni sul modem mancanti. La tag può far riferimento alla velocità in baud, alla linea esterna, ecc.

Risposta dell'utente: Controllare che i caratteri del file di configurazione del modem siano validi.

ICA4105 La portante *portante* **deve avere almeno un numero di telefono nell'elenco.**

Spiegazione: La portante deve contenere il numero di telefono.

Risposta dell'utente: Aggiungere il numero di telefono utilizzando il menu smitty/SMIT.

ICA4106 Impossibile aprire il file *nome file portanti***.**

Spiegazione: Il file di database della portante deve esistere.

Risposta dell'utente: Se non esiste già, crearlo utilizzando il menu smitty/SMIT.

ICA4107 Riga *numero riga* **troppo lunga.**

Spiegazione: La riga del file di database della portante è troppo lunga.

Risposta dell'utente: Controllare che le righe del file di database della portante siano valide.

ICA4108 Tag sconosciuta alla riga *numero riga***.**

Spiegazione: Esiste una tag sconosciuta nel file di database della portante.

Risposta dell'utente: Controllare che le tag del file di database della portante siano valide.

ICA4109 Sequenza non valida alla riga *numero riga***.**

Spiegazione: Esiste una sequenza non valida nel file di database della portante.

Risposta dell'utente: Controllare che le sequenze del file di database della portante siano valide.

ICA4110 La portante *portante* **non è valida e verrà tralasciata.**

Spiegazione: La portante non può essere utilizzata per il cercapersone.

Risposta dell'utente: Controllare la validità della portante.

ICA4111 Impossibile aggiungere la portante all'elenco.

Spiegazione: La portante non può essere aggiunta all'elenco.

Risposta dell'utente: Controllare la validità della portante ed i numeri di telefono.

ICA4112 Nome della portante mancante o troppo lungo alla riga *numero riga***.**

Spiegazione: Il nome della portante manca.

Risposta dell'utente: Aggiungere la portante utilizzando il menu smitty/SMIT.

ICA4113 Errore: Impossibile assegnare una nuova portante di cercapersone: *portante***.**

Spiegazione: La portante non può essere assegnata all'elenco.

Risposta dell'utente: Controllare la validità della portante ed i numeri di telefono.

ICA4114 Il valore della riga *numero riga* **è troppo lungo.**

Spiegazione: È stata rilevata una riga troppo lunga nel file di database della portante.

Risposta dell'utente: Eliminare la riga lunga del file di database della portante.

ICA4115 Tag *tag* **duplicata alla riga** *numero riga* **ignorata.**

Spiegazione: È stata rilevata una tag duplicata.

Risposta dell'utente: Rimuovere la tag duplicata dal file di database della portante.

ICA4116 Valore inesistente alla riga *numero riga***.**

Spiegazione: È stato rilevato un campo vuoto.

Risposta dell'utente: Utilizzare smitty/SMIT per aggiungere un valore nel campo vuoto.

ICA4117 Il valore della riga deve essere *numero riga* **Y, Yes, N, No.**

Spiegazione: Questo campo richiede Y, Yes, N o No.

Risposta dell'utente: Utilizzare smitty/SMIT per aggiungere o modificare i dati validi.

ICA4118 Il valore della riga *numero riga* **deve essere maggiore di 0.**

Spiegazione: Questo campo deve essere positivo.

Risposta dell'utente: Modificare il valore in uno positivo utilizzando smitty/SMIT.

ICA4119 Valore non valido alla riga *numero riga***.**

Spiegazione: È stato rilevato un valore non valido alla riga specificata.

Risposta dell'utente: Modificare il valore utilizzando il menu smitty/SMIT.

ICA4120 La portante *nome* **non è valida e verrà tralasciata.**

Spiegazione: È stata rilevata una portante non valida.

Risposta dell'utente: Aggiungere una portante valida utilizzando il menu smitty/SMIT.

ICA4121 Impossibile aggiungere la portante all'elenco.

Spiegazione: Non è possibile aggiungere la portante all'elenco del cercapersone.

Risposta dell'utente: Controllare la validità della portante.

ICA4122 Tag *tag* **duplicata alla riga** *numero riga* **ignorata.**

Spiegazione: È stata rilevata una tag duplicata in una stanza della portante.

Risposta dell'utente: Eliminare la stanza della portante che contiene i valori duplicati.

ICA4123 Errore(*programma***): Non è stato possibile richiamare il token IPC:** *errno*

Spiegazione: Il programma non è riuscito a richiamare il token IPC.

ICA4124 Errore(*programma***): Errore** *pageqErr* **durante la lettura della coda.**

Spiegazione: Il programma non è riuscito a leggere la coda.

ICA4125 *numero* **entrate di coda.**

Spiegazione: Messaggio informativo.

ICA4126 Messaggio con ID *id* **eliminato.**

Spiegazione: Messaggio informativo.

ICA4127 ID *id* **non in coda.**

Spiegazione: Messaggio informativo.

ICA4128 Errore(*programma***): Errore** *pageqErr* **durante il tentativo di eliminazione dell'ID** *id***.**

Spiegazione: Tentativo di eliminazione di un ID della coda.

ICA4129 La chiave è: *entryKey***, il contenuto è @** *ptr***:** *ptr***.**

Spiegazione: Messaggio informativo.

ICA4130 Caratteristiche del modem:

Spiegazione: Informazioni sull'inizializzazione del modem.

ICA4131 Nome: *nomeModem*

Spiegazione: Informazioni sull'inizializzazione del modem.

ICA4132 Iniz: *stringaIniz*

Spiegazione: Informazioni sull'inizializzazione del modem.

ICA4133 Modo comando: *comando*

Spiegazione: Informazioni sull'inizializzazione del modem.

ICA4137 Cancelletto (#): *diallb*

Spiegazione: Informazioni sull'inizializzazione del modem.

ICA4138 Asterisco (*): *dialstar*

Spiegazione: Informazioni sull'inizializzazione del modem.

ICA4139 Riagganciare: *comando per riagganciare*

Spiegazione: Informazioni sull'inizializzazione del modem.

ICA4140 Risposta per comando valido: *risposta per comando valido*

Spiegazione: Informazioni sull'inizializzazione del modem.

ICA4141 Collegamento valido: *collegamento valido*

Spiegazione: Informazioni sull'inizializzazione del modem.

ICA4142 Eco: *eco*

Spiegazione: Informazioni sull'inizializzazione del modem.

ICA4143 Record di debug del modem: PUTS(*id***) txd-**> *outStr*

Spiegazione: Informazioni sull'handshaking del modem.

ICA4144 Record di debug del modem: PUTC(*id***) txd-**> *outStr*

Spiegazione: Informazioni sull'handshaking del modem.

ICA4145 Record di debug del modem: GET rxd-> *id record*

Spiegazione: Informazioni sull'handshaking del modem.

ICA4146 Record di debug del modem: INPUT(*id record*

Spiegazione: Informazioni sull'handshaking del modem.

ICA4147 Record di debug del modem:) rxd->

Spiegazione: Informazioni sull'handshaking del modem.

ICA4148 Record di debug del modem: WAITFOR(*id record*

Spiegazione: Informazioni sull'handshaking del modem.

ICA4149 Non è stato possibile sbloccare il segnale child.

Spiegazione: Sblocca il segnale SIGCHLD.

ICA4150 Non è stato possibile bloccare il segnale child.

Spiegazione: Blocca il segnale SIGCHLD.

ICA4151 Il file di avvio a caldo *nome precorso file* **non esiste.**

Spiegazione: Messaggio informativo.

ICA4152 Impossibile aprire il file di avvio a caldo *nome percorso file*

Spiegazione: Messaggio informativo.

ICA4153 Riga troppo lunga nel file di avvio a caldo *nome percorso file***.**

Spiegazione: Il file di avvio a caldo contiene caratteri non validi.

ICA4154 Il file di avvio a caldo *nome precorso file* **contiene dati non utilizzati.**

Spiegazione: Messaggio informativo.

ICA4155 Il file di avvio a caldo *nome percorso file* **è vuoto.**

Spiegazione: Messaggio informativo.

ICA4156 La riga *numero riga* **del file di avvio a caldo** *nome percorso file* **contiene destinatario** *indirizzo* **errato, ignorata.**

Spiegazione: Il file di avvio a caldo contiene caratteri non validi. Messaggio informativo.

ICA4157 La riga *numero riga* **del file di avvio a caldo** *nome percorso file* **ha un formato errato, ignorata.**

Spiegazione: Il file di avvio a caldo contiene caratteri non validi. Messaggio informativo.

ICA4158 La riga *numero riga* **del file di avvio a caldo** *nome percorso file* **non contiene messaggi, ignorata.**

Spiegazione: Il file di avvio a caldo non contiene messaggi. Messaggio informativo.

ICA4159 Errore nell'accodamento della riga *numero riga* **del file di avvio a caldo** *nome percorso file***, ignorata.**

Spiegazione: Il file di avvio a caldo contiene caratteri non validi. Messaggio informativo.

ICA4160 Avvio a caldo di *numero* **messaggi dal file** *nome percorso file* **completato.**

Spiegazione: Messaggio informativo.

ICA4161 Errore(*programma***): Troppi errori child consecutivi.**

Spiegazione: Troppi errori child in una riga. Ciò si verifica se la portante o il file di definizione del modem contiene caratteri non validi.

Risposta dell'utente: Controllare il file di database della portante ed il file di definizione del modem utilizzando il menu smitty/SMIT.

ICA4162 Il child non può eseguire *programma* **:** *errno***.**

Spiegazione: Possibile errore di sistema.

ICA4163 Errore(*errno***): Il child non può eseguire il fork sul child :** *nome programma***.**

Spiegazione: Possibile errore di sistema.

ICA4164 Non è stato possibile creare l'elenco delle portanti del cercapersone.

Spiegazione: Errore di programma interno.

ICA4165 Errori nel file delle portanti del cercapersone *file delle portanti***.**

Spiegazione: Il database della portante contiene dati non validi.

Risposta dell'utente: Controllare il file di database della portante utilizzando il menu smitty/SMIT.

ICA4166 Messaggio informativo. La chiave IPC è: 0x*ChiaveIpc***.**

Spiegazione: Messaggio informativo.

ICA4167 Non è stato possibile creare la coda, page_q_err: *pageQerr***.**

Spiegazione: Errore nel tentativo di creare la coda.

ICA4168 File di avvio a caldo del cercapersone creato alle *ora*

Spiegazione: Messaggio informativo.

ICA4169 priorità -p *priorità numPager* **da** *messaggio objfrom*

Spiegazione: Messaggio informativo.

ICA4170 priorità -p *priorità alpaPager@portante* **da** *da messaggio*

Spiegazione: Messaggio informativo.

ICA4171 priorità -p *priorità* **-n** *numero cercapersone@portante* **da** *da messaggio*

Spiegazione: Messaggio informativo.

ICA4172 Fine del file di avvio a caldo del cercapersone.

Spiegazione: Messaggio informativo. Indica la fine del messaggio.

ICA4173 Impossibile scrivere nel file di avvio a caldo *nome file***.**

Spiegazione: È possibile che il file di avvio a caldo non esista.

ICA4174 *ora* **RICHIESTA-STATO da** *utente@host*

Spiegazione: Visualizza le informazioni sulla richiesta di stato.

ICA4175 *ora* **RICHIESTA-RIEPILOGO da** *utente@host*

Spiegazione: Visualizza le informazioni sulla richiesta di riepilogo.

ICA4176 *numero* **entrate di coda.**

Spiegazione: Indica il numero di entrate della coda del cercapersone.

ICA4177 Entrata meno recente: ID *id* **ricevuto alle** *ora***.**

Spiegazione: Visualizza l'entrata meno recente della coda.

ICA4178 Ricollegamento della memoria dopo l'espansione non riuscito.

Spiegazione: Possibile errore di sistema.

ICA4179 Ricollegamento della memoria dopo l'allineamento dell'espansione non riuscito.

Spiegazione: Possibile errore di sistema.

ICA4180 Non è stato possibile disattivare il semaforo PAGE_Q in page_q_print() : *errno***.**

Spiegazione: Possibile errore di sistema.

ICA4181 Non è stato possibile attivare il semaforo PAGE_Q in page_q_print() : *errno***.**

Spiegazione: Possibile errore di sistema.

ICA4182 collegamento *collegamento* **-> ID messaggio:** *id***.**

Spiegazione: Messaggio informativo.

ICA4183 Priorità: *priorità***.**

Spiegazione: Messaggio informativo.

ICA4184 Persona: *nome***.**

Spiegazione: Messaggio informativo.

ICA4185 Portante: *portante***.**

Spiegazione: Messaggio informativo.

ICA4186 Messaggio: *messaggio***.**

Spiegazione: Messaggio informativo.

ICA4187 Non è stato possibile richiamare la RAM condivisa : *errno***.**

Spiegazione: Possibile errore di sistema.

ICA4188 Non è stato possibile richiamare la RAM condivisa collegata: *errno***.**

Spiegazione: Possibile errore di sistema.

ICA4189 Non è stato possibile richiamare il semaforo PAGE_Q.

Spiegazione: Possibile errore di sistema.

ICA4190 Non è stato possibile inizializzare il semaforo PAGE_Q in page_q_create() : *errno***.**

Spiegazione: Possibile errore di sistema.

ICA4191 Non è stato possibile impostare il semaforo PAGE_Q in page_q_create() : *errno***.**

Spiegazione: Possibile errore di sistema.

ICA4192 Non è stato possibile disattivare il semaforo PAGE_Q in page_q_empty() : *errno***.**

Spiegazione: Possibile errore di sistema.

ICA4193 **Non è stato possibile attivare il semaforo PAGE_Q in page_q_empty() :** *errno***.**

Spiegazione: Possibile errore di sistema.

ICA4194 **Non è stato possibile disattivare il semaforo PAGE_Q in page_q_enq(***nome***,***messaggio***) :** *errno***.**

Spiegazione: Possibile errore di sistema.

ICA4195 **Non è stato possibile attivare il semaforo PAGE_Q in page_q_enq() :** *errno***.**

Spiegazione: Possibile errore di sistema.

ICA4196 **page_q_enq(): ID(***id***) Priorità(***priorità***) Persona(***nome***) Messaggio(***messaggio***).**

Spiegazione: Messaggio informativo.

ICA4197 **Non è stato possibile disattivare il semaforo PAGE_Q in page_q_head() :** *errno***.**

Spiegazione: Possibile errore di sistema.

ICA4198 **Non è stato possibile attivare il semaforo PAGE_Q in page_q_head() :** *errno***.**

Spiegazione: Possibile errore di sistema.

ICA4199 **Non è stato possibile disattivare il semaforo PAGE_Q in page_q_first() :** *errno***.**

Spiegazione: Possibile errore di sistema.

ICA4200 **Non è stato possibile attivare il semaforo PAGE_Q in page_q_first() :** *errno***.**

Spiegazione: Possibile errore di sistema.

ICA4201 **Non è stato possibile disattivare il semaforo PAGE_Q in page_q_next() :** *errno***.**

Spiegazione: Possibile errore di sistema.

ICA4202 **Non è stato possibile attivare il semaforo PAGE_Q in page_q_next() :** *errno***.**

Spiegazione: Possibile errore di sistema.

ICA4203 **Non è stato possibile disattivare il semaforo PAGE_Q in page_q_tail() :** *errno***.**

Spiegazione: Possibile errore di sistema.

ICA4204 **Non è stato possibile attivare il semaforo PAGE_Q in page_q_tail() :** *errno***.**

Spiegazione: Possibile errore di sistema.

ICA4205 **Non è stato possibile disattivare il semaforo PAGE_Q in page_q_del() :** *errno***.**

Spiegazione: Possibile errore di sistema.

ICA4206 Non è stato possibile attivare il semaforo PAGE_Q in page_q_del() : *errno***.**

Spiegazione: Possibile errore di sistema.

ICA4207 page_q_del(*ID***).**

Spiegazione: Informazioni di debug.

ICA4208 Non è stato possibile disattivare il semaforo PAGE_Q in page_q_deq() : *errno***.**

Spiegazione: Possibile errore di sistema.

ICA4209 Non è stato possibile attivare il semaforo PAGE_Q in page_q_deq() : *errno***.**

Spiegazione: Possibile errore di sistema.

ICA4210 page_q_del(): ID(*id***) Priorità(***priorità***) Persona(***nome***) Messaggio(***messaggio***).**

Spiegazione: Messaggio informativo.

ICA4211 Non è stato possibile disattivare il semaforo PAGE_Q in page_q_walk() : *errno***.**

Spiegazione: Possibile errore di sistema.

ICA4212 Non è stato possibile attivare il semaforo PAGE_Q in page_q_walk() : *errno***.**

Spiegazione: Possibile errore di sistema.

ICA4213 PAGE_Q piena.

Spiegazione: La coda del cercapersone è piena.

Risposta dell'utente: Inviare la chiamata successivamente.

ICA4300 Interruzione chiamata in corso.

Spiegazione: Interruzione della chiamata.

ICA4301 Inizializzazione modem in corso ...

Spiegazione: Inizializzazione del modem con una stringa di inizializzazione.

ICA4302 Composizione in corso .....

Spiegazione: Composizione del numero di telefono in corso.

ICA4303 Attesa collegamento in corso.

Spiegazione: Attesa del collegamento del modem in corso.

ICA4304 COLLEGATO *velocità*

Spiegazione: Collegamento alla velocità indicata (velocità in baud).

ICA4305 COLLEGATO!!!!!!!

Spiegazione: Collegato al fornitore di servizio del cercapersone.

ICA4306 Richiesta comandi per Modo automatico.

Spiegazione: Richiesta comandi per modo automatico. In attesa di "ID=".

ICA4307 Richiesta comandi OK.....

Spiegazione: Ricevuto "ID=" dal fornitore.

ICA4308 Invio richiesta Modo automatico in corso.

Spiegazione: Invio dell'ID e SST al fornitore di servizio del cercapersone in corso.

ICA4354 *What* **errato.**

Spiegazione: Se la velocità in baud è errata, le opzioni valide sono: 600, 1200, 2400, 4800, 9600, 14400. Se i bit di dati per byte sono errati, le opzioni valide sono: 7, 8 Se i bit di stop sono errati, le opzioni valide sono: 1, 2 Se il prefisso linea esterna è errato, le immissioni devono essere solo numeri. Se il metodo del cercapersone è errato, questa versione supporta solo TAP. Se l'ID del cercapersone è errato, controllare tutti i numeri. Se la parità è errata, le opzioni valide sono: O(odd), E(even), N(none), S(space), M(mark). Se la porta COM è errata, le opzioni valide sono: COM1, COM2 .... In questa versione, la porta COM non deve superare 10. Se un carattere del messaggio è errato, controllare che il messaggio non contenga caratteri speciali.

ICA4355 Errore nell'impostazione dei parametri in *where***.**

Spiegazione: Impossibile impostare i paramtri in (where). Controllare i parametri e ritentare l'operazione.

ICA4356 Quando *when***, errore nella lettura della porta COM.**

Spiegazione: Errore nella lettura della porta COM. Impostare l'eco del modem e ritentare l'operazione.

ICA4357 Quando *Where***, errore di scrittura della porta COM.**

Spiegazione: Errore di scrittura della porta COM.

ICA4358 Errore nell'impostazione di *What*

Spiegazione: Impostare l'errore indicato da 'What'. Controllare il file di log e correggere l'errore.

ICA4359 Numero massimo di tentativi superato in *Where***. Interrompere il programma .....**

Spiegazione: Si è tentato di aprire la porta com 60 volte in 60 minuti. Tutti i tentativi non sono riusciti. In tal caso, controllare il collegamento hardware. Si è tentato di inviare il messaggio al cercapersone 10 volte in 10 minuti. Tutti i tentativi non sono riusciti. In tal caso, è possibile che il fornitore della chiamata non sia attivo.

ICA4360 Carattere sconosciuto nel numero di telefono della portante: **pNumTelefonoPortante*

Spiegazione: È stato rilevato un carattere sconosciuto nel numero di telefono della portante. Controllare il numero e riprovare.

ICA4361 Avvertenza!!! La velocità del modem del fornitore del cercapersone deve essere generalmente inferiore a 2400.

Spiegazione: Questa è soltanto un'avvertenza. Di solito, la velocità del modem del fornitore del cercapersone è inferiore a 2400.

ICA4362 Impossibile inizializzare il modem

Spiegazione: Modificare la stringa di inizializzazione del modem e ritentare l'operazione.

ICA4363 Il modem ha restituito un errore.

Spiegazione: Errore di comunicazione del modem.

ICA4364 Errore nel tentativo *tentativi* **di apertura della porta Com. Ritentare fra 1 minuto**

Spiegazione: Errore nell'apertura della porta COM. Probabilmente un altro programma la sta utilizzando. Ritentare automaticamente fra 1 minuto.

ICA4365 Invio della chiamata non riuscito al *tentativi* **tentativo. Ritentare fra 1 minuto**

ICA4373 (*nome funzione***) Codice di risposta sconosciuto dal modem o dalla portante** *char1***,** *char2***.**

Spiegazione: Questo messaggio contiene la risposta del modem o della portante, che il dispositivo cercapersone del firewall non riconosce. char1 e char2 sono i codici ascii (esadecimali) per i primi due caratteri della risposta.

Risposta dell'utente: Utilizzare queste informazioni quando si consultano le istruzioni del modem o della portante per determinare il significato di risposta sconosciuta.

ICA5005 Inizializzazione di SKIT non riuscita. Il codice di errore è: *codice di errore*

Spiegazione: L'inizializzazione del socket sicuro non è riuscita, viene visualizzato il codice di errore da SKIT.

ICA5014 Server del tunnel del client remoto in ascolto alla porta *porta server #*

Spiegazione: Viene visualizzato il numero di porta configurato per sslrctd.

ICA5015 Collegamento accettato da *chp0.chp1.chp2.chp3*

Spiegazione: Viene visualizzato l'indirizzo IP del client.

ICA5017 Impossibile richiamare il socket sicuro. Il codice di errore della funzione skit_secure_soc_init è:*codice di errore della funzione*

Spiegazione: Non è possibile richiamare il socket sicuro, perché skit_secure_soc_init() non è riuscito.

ICA5018 Le specifiche di cifra del server slave utilizzate sono *spec1 spec2 spec3*

Spiegazione: Vengono visualizzate le specifiche di cifra.

ICA5019 Impossibile richiamare il lotto Free Homenet IP.

Spiegazione: Problema relativo ai filtri dinamici.

ICA5020 Impossibile aprire il file di configurazione del client remoto.

Spiegazione: Il file /etc/security/rcsfile.cfg non è disponibile.

Risposta dell'utente: Controllare l'esistenza del file ed il suo contenuto.

ICA5021 Impossibile trovare la parola chiave '*parola chiave***'.**

Spiegazione: Il file /etc/security/rcsfile.cfg non contiene questa parola chiave.

Risposta dell'utente: Controllare e correggere il file /etc/security/rcsfile.cfg.

ICA5024 Errore della funzione skit_secure_soc_write() in *nome routine***.**

Spiegazione: skit_secure_soc_write() non è riuscito in questa routine.

ICA5025 Errore della funzione skit_secure_soc_write() in ACKClient().

Spiegazione: La funzione skit_secure_soc_write() non è riuscita nella routine ACKClient().

ICA5026 Ricevuto codice di errore non valido dal client in *routine***.**

Spiegazione: Ricevuto codice di errore non valido dal client in questa routine.

ICA5027 Ricevuto codice di errore per richiesta errata dal client in *nome routine***.**

Spiegazione: Ricevuto codice di errore imprevisto per la richiesta in questa routine.

ICA5028 Richiesta di login non valida.

Spiegazione: Il formato del messaggio per la richiesta di login non è valido.

ICA5030 ID client remoto sconosciuto : *ID client remoto*

Spiegazione: Questo ID utente è sconosciuto per la macchina firewall.

Risposta dell'utente: Correggere le informazioni dell'utente per questo client remoto.

ICA5031 Funzione skit_secure_soc_write, errore in RCTLoginPhase.

Spiegazione: La funzione skit_secure_soc_write() non è riuscita per la fase di login.

ICA5035 Richiesta di logout non valida

Spiegazione: Il formato del messaggio per la richiesta di logout non è valido.

ICA5067 Ricevuto pacchetto non valido.

Spiegazione: Il formato del pacchetto ricevuto non è valido.

ICA5078 Richiamare richiesta non riconosciuta in SvrReqHandler()

Spiegazione: La richiesta ricevuta non è stata riconosciuta, pertanto verrà ignorata.

ICA5082 Il tunnel al client *ID client remoto* **è stato scollegato.**

Spiegazione: Il tunnel per il client remoto con questo ID è stato scollegato.

ICA5086 ID: *id utente* **non definito.**

Spiegazione: Questo ID utente non esiste sulla macchina firewall.

ICA5087 Autenticazione non riuscita per '*id utente***'.**

Spiegazione: L'autenticazione non è riuscita per questo ID utente.

ICA5089 Funzione rcFilterClear() non riuscita. Il codice di errore è *codice di errore***.**

Spiegazione: La funzione rcFilterClear() non è riuscita ed è stato restituito questo codice di errore.

Risposta dell'utente: Controllare se il client IPSEC LAN è presente. Questi prodotti non possono coesistere.

ICA5090 Funzione rcFilterInit() non riuscita. Il codice di errore è *codice di errore***.**

Spiegazione: La funzione rcFilterInit() non è riuscita restituendo questo codice di errore.

ICA5091 La funzione TunnelUp() non può eseguire il file eseguibile *riga comandi***.**

Spiegazione: La riga comandi visualizzata non è riuscita ad eseguire la chiamata system().

ICA5092 Impossibile richiamare la parola d'ordine del file di chiavi dalla chiamata della funzione recoverstash.

Spiegazione: Impossibile richiamare la parola d'ordine del file di chiavi dal file stash.

ICA8001 SYSLOG/udp: servizio sconosciuto
ICA8002 La funzione *nome_funzione* **non è riuscita -** *errno***, errno2 = 0x***errno2*

Spiegazione: L'elaborazione termina perché syslogd non è riuscito ad eseguire la funzione specificata. Le informazioni sul numero degli errori sono accodate al messaggio di errore.

Risposta dell'utente: Contattare il programmatore di sistema. Programmatore di sistema: Utilizzare le informazioni sul numero degli errore per determinare la causa del problema.

ICA8004 Errore rilevato nel socket AF_INET, \ slogd non controlla più il socket
ICA8006 Nome priorità \"*priorità***\" sconosciuto**

Spiegazione: Nel file di configurazione è stato trovato un nome priorità non valido.

Risposta dell'utente: Contattare il programmatore di sistema. Programmatore di sistema: Controllare il file di configurazione.

ICA8007 Nome funzione \"*funzione***\" sconosciuto**

Spiegazione: Nel file di configurazione è stato trovato un nome funzione non valido.

Risposta dell'utente: Contattare il programmatore di sistema. Programmatore di sistema: Controllare il file di configurazione.

ICA8008 Massaggi da SYSLOG@*nome host* **a** *timestamp* **...**

Spiegazione: Il file di configurazione del daemon syslog conteneva un'entrata per inviare i messaggi syslog a tutti gli utenti collegati. Questo messaggio verrà inviato a tutti gli utenti collegati correntemente al sistema su cui viene eseguito il daemon syslog.

Risposta dell'utente: Nessun programmatore di sistema.

ICA8009 SYSLOGD in uscita al segnale *segnale*

Spiegazione: Il daemon syslog ha ricevuto un segnale che ne ha determinato l'uscita.

Risposta dell'utente: Nessun programmatore di sistema.

ICA8010 SYSLOGD riavviato
ICA8012 SYSLOGD non può registrare su SMF - *testo_errore*

Spiegazione: Si è verificato un errore durante la scrittura di un record su SMF. Le informazioni sul testo dell'errore sono accodate al messaggio di errore.

Risposta dell'utente: Contattare il programmatore di sistema. Programmatore di sistema: Utilizzare le informazioni sul testo dell'errore per determinare la causa del problema di scrittura SMF.

ICA8013 Aggiornamento dello stato del processo non riuscito, codice di errore = 0x*codice_errore*

Spiegazione: Si è verificato un errore nel tentativo di aggiornare lo stato del processo syslogd per il processo kernel del firewall. Il codice di errore traccia l'errore specifico restituito dalla chiamata dello stato del processo di aggiornamento.

Risposta dell'utente: Contattare il programmatore di sistema. Programmatore di sistema: Rivolgersi all'assistenza IBM.

ICA8014 Opzione (-*opzione_avvio*) sconosciuta, specificata al richiamo di SYSLOGD

Spiegazione: Si è verificato un errore durante il tentativo di avviare il processo del daemon syslogd. L'opzione specificata non è supportata durante il richiamo di syslogd.

Risposta dell'utente: Controllare le opzioni di avvio e riavviare il daemon syslogd. Programmatore di sistema: Se il problema persiste, rivolgersi all'assistenza IBM.

ICA8015 L'entrata (*dati_config*) del file di configurazione non è valida

Spiegazione: Si è verificato un errore nel tentativo di analizzare un'entrata di configurazione dal file di configurazione SYSLOG.

Risposta dell'utente: Controllare le entrate del file di configurazione e riavviare il daemon syslogd. Programmatore di sistema: Se il problema persiste, rivolgersi all'assistenza IBM.

ICA8016 Funzione *nome_funzione* non riuscita per *nome file* - *errno*

Spiegazione: Si è verificato un errore nel tentativo di eseguire la funzione indicata per l'unità specificata. Le informazioni sul numero degli errori sono accodate al messaggio di errore.

Risposta dell'utente: Verificare che l'unità specificata esista e ritentare la richiesta. Se il problema persiste, rivolgersi all'assistenza IBM. Programmatore di sistema: Se il problema persiste, rivolgersi all'assistenza IBM.

ICA8050 *funzione* **non riuscita.** *testo_errore*

Spiegazione: Si è verificato un errore durante l'esecuzione della funzione visualizzata nel messaggio. Ulteriori informazioni sull'errore vengono fornite dal testo del messaggio di errore.

Risposta dell'utente: Correggere l'errore specificato nel messaggio e, se necessario, ritentare l'operazione.

ICA8051 *funzione* **non riuscita: codice di errore = 0x***codice_errore*

Spiegazione: Si è verificato un errore durante l'esecuzione della funzione visualizzata nel messaggio. Viene visualizzato anche il codice di errore della funzione specificata.

Risposta dell'utente: Correggere l'errore specificato nel messaggio e, se necessario, ritentare l'operazione.

ICA8052 FWSTACKD sta attivando il log del filtro per *nome_stack*.

Spiegazione: FWSTACKD sta tentando di attivare il log del filtro del pacchetto.

Azione del sistema: Il programma continua.

ICA8053 FWSTACKD non può attivare il log del filtro per *nome_stack*. *testo_errore*

Spiegazione: L'attivazione del log del filtro del pacchetto non è riuscita per il motivo descritto nel relativo messaggio di errore.

Azione del sistema: Il log del filtro non verrà eseguito.

Risposta dell'utente: Per correggere l'errore, utilizzare il relativo messaggio, quindi riattivare il log dei filtri con **fwfilter cmd=startlog**.

ICA8054 FWSTACKD sta attivando il log di NAT per *nome_stack*.

Spiegazione: FWSTACKD sta tentando di attivare il log di NAT (Network Address Translation).

Azione del sistema: Il programma continua.

ICA8055 FWSTACKD non può attivare il log di NAT per *nome_stack***.** *testo_errore*

Spiegazione: L'attivazione del log di NAT (Network Address Translation) non è riuscita per il motivo descritto nel relativo messaggio di errore.

Azione del sistema: Il log di NAT non verrà eseguito.

Risposta dell'utente: Per correggere l'errore, utilizzare il relativo messaggio, quindi riattivare il log di NAT con **fwnat cmd=startlog**.

ICA8056 FWSTACKD sta attivando NAT per *nome_stack***.**

Spiegazione: FWSTACKD sta tentando di attivare NAT (Network Address Translation).

Azione del sistema: Il programma continua.

ICA8057 FWSTACKD non può attivare NAT per *nome_stack***.** *testo_errore*

Spiegazione: L'attivazione di NAT (Network Address Translation) non è riuscita per il motivo descritto nel relativo messaggio di errore.

Azione del sistema: NAT non verrà eseguito.

Risposta dell'utente: Per correggere l'errore, utilizzare il relativo messaggio, quindi riattivare NAT con **fwnat cmd=update**.

ICA8058 FWSTACKD sta riattivando le definizioni di tunnel per *nome_stack***.**

Spiegazione: FWSTACKD sta tentando di riattivare le definizioni di tunnel che erano attive quando il sistema è stato arrestato.

Azione del sistema: Il programma continua.

ICA8059 FWSTACKD non può riattivare le definizioni di tunnel per *nome_stack***.** *testo_errore*

Spiegazione: L'attivazione delle definizioni di tunnel non è riuscita per il motivo descritto nel relativo messaggio di errore.

Azione del sistema: Le definizioni di tunnel non vengono attivate.

Risposta dell'utente: Per correggere l'errore, utilizzare il relativo messaggio, quindi riattivare le definizioni di tunnel con **fwtunnl cmd=activate**.

ICA8060 FWSTACKD sta attivando le regole di filtro e le regole Socks per *nome_stack***.**

Spiegazione: FWSTACKD sta tentando di attivare l'insieme corrente delle regole di filtro e delle regole Socks del pacchetto.

Azione del sistema: Il programma continua.

ICA8061 FWSTACKD non può attivare le regole di filtro e le regole Socks per *nome_stack***.** *testo_errore*

Spiegazione: L'attivazione delle regole di filtro e delle regole Socks non è riuscita per il motivo descritto nel relativo messaggio di errore.

Azione del sistema: Verranno utilizzate le regole di filtro assunte. L'accesso locale sarà consentito ma verranno negati tutti gli altri accessi.

Risposta dell'utente: Per correggere l'errore, utilizzare il relativo messaggio, quindi riattivare le regole di filtro e le regole Socks con **fwfilter cmd=update**.

ICA8062 FWSTACKD sta attivando il supporto RealAudio per *nome_stack***.**

Spiegazione: FWSTACKD sta tentando di attivare il supporto RealAudio.

Azione del sistema: Il programma continua.

ICA8063 FWSTACKD non può attivare il supporto RealAudio per *nome_stack***.** *testo_errore*

Spiegazione: L'attivazione del supporto RealAudio non è riuscita per il motivo descritto nel relativo messaggio di errore.

Azione del sistema: I servizi RealAudio non sono disponibili.

Risposta dell'utente: Per identificare l'errore, utilizzare il relativo messaggio, quindi correggere l'errore ed attivare RealAudio con **fwaudio cmd=change**.

ICA8064 *funzione* **non riuscita.** *testo_errore*

Spiegazione: Si è verificato un errore durante l'esecuzione della funzione visualizzata nel messaggio. Ulteriori informazioni sull'errore vengono fornite dal testo del messaggio di errore.

Risposta dell'utente: Correggere l'errore specificato nel messaggio e, se necessario, ritentare l'operazione.

ICA9000 Il periodo di valutazione di IBM Firewall scade nell'arco di *numero* **giorni.**

Spiegazione: Questo software è contrassegnato come copia di valutazione e scadrà dopo il periodo di tempo indicato.

ICA9001 Avvertenza del programma di verifica dell'integrità del sistema di file - *testo descrittivo di avvertenza*

Spiegazione: fwfschk ha rilevato una discrepanza nel sistema di file, possibile threat.

ICA9002 Ultimo messaggio ripetuto %1$d volte

Spiegazione: Questo messaggio viene generato da syslogd di AIX quando un messaggio identico viene registrato nel log senza che venga visualizzato alcun messaggio di errore. Il messaggio viene conservato in modo che il Controllo log possa rilevare la condizione. Questo messaggio deve essere scritto nella stessa lingua del messaggio syslogd.

ICA9003 Autenticazione non riuscita per utente *nome* **sul server di configurazione.**

Spiegazione: Il server di configurazione del firewall non è in grado di eseguire l'autenticazione dell'utente indicato.

Risposta dell'utente: Contattare il responsabile del firewall.

ICA9004 Utente *nome* **autenticato correttamente sul server di configurazione.**

Spiegazione: Il server di configurazione del firewall ha eseguito l'autenticazione dell'utente indicato.

ICA9005 Avvio del server di configurazione remota.

Spiegazione: Il server di configurazione è stato attivato.

ICA9006 Chiusura del server di configurazione remota.

Spiegazione: Il server di configurazione viene chiuso.

ICA9007 Impossibile aprire il catalogo dei messaggi sul server di configurazione remota

Spiegazione: È possibile che manchino uno o più cataloghi di messaggi utilizzati dal server di configurazione remota.

Risposta dell'utente: Contattare il responsabile del firewall.

ICA9008 Funzione getpeername() non riuscita sul server di configurazione remota: errore *errno***.**

Spiegazione: Il server di configurazione del firewall non può ottenere informazioni sul client.

Risposta dell'utente: Contattare il responsabile del firewall.

ICA9009 Funzione getsockname() non riuscita sul server di configurazione remota: errore *errno***.**

Spiegazione: Il server di configurazione non può ottenere informazioni ad esso associate.

Risposta dell'utente: Contattare il responsabile del firewall.

ICA9010 Il server di configurazione remota non è riuscito ad ottenere informazioni sull'adattatore.

Spiegazione: Il server di configurazione del firewall non può ottenere informazioni sull'adattatore.

Risposta dell'utente: Contattare il responsabile del firewall.

ICA9011 Il server di configurazione non è abilitato per la configurazione remota.

Spiegazione: Nel file di configurazione, il server di configurazione è impostato in locale mentre il client si trova su una macchina remota.

Risposta dell'utente: Contattare il responsabile del firewall.

ICA9012 Impossibile leggere la richiesta di collegamento dal server di configurazione remota.

Spiegazione: Il server di configurazione non può leggere la richiesta di collegamento del client.

Risposta dell'utente: Contattare il responsabile del firewall.

ICA9013 Il server di configurazione remota ha ricevuto una richiesta di collegamento errata.

Spiegazione: La richiesta di collegamento conteneva informazioni errate.

Risposta dell'utente: Contattare il responsabile del firewall.

ICA9014 Impossibile creare un simbolo pipe dal server di configurazione remota.

Spiegazione: Il server di configurazione non può creare un simbolo pipe per l'autenticazione.

Risposta dell'utente: Contattare il responsabile del firewall.

ICA9015 Impossibile creare un processo dal server di configurazione remota.

Spiegazione: Il server di configurazione non può creare un processo per l'autenticazione.

Risposta dell'utente: Contattare il responsabile del firewall.

ICA9016 Avvio del daemon EFM.

Spiegazione: Il daemon EFM è stato avviato sul firewall gestito.

ICA9017 Chiusura del daemon EFM; rc = *valore***.**

Spiegazione: Il daemon EFM viene chiuso con il codice di errore specificato.

ICA9018 Impossibile aprire il catalogo dei messaggi dal daemon EFM.

Spiegazione: È possibile che manchino uno o più cataloghi di messaggi utilizzati dal daemon EFM.

Risposta dell'utente: Contattare il responsabile del firewall.

ICA9020 Impossibile passare all'ID utente in esecuzione.

Spiegazione: Non è stato possibile effettuare la chiamata di sistema per passare all'ID utente in esecuzione.

Risposta dell'utente: Contattare il responsabile del firewall.

ICA9021 Questo firewall non supporta il modo *logon***.**

Spiegazione: Questo firewall non supporta questo particolare modo.

Risposta dell'utente: Contattare il responsabile del firewall.

ICA9022 *utente* **non è autorizzato ad eseguire il collegamento al firewall in modo** *logon***.**

Spiegazione: Questo nome utente non è autorizzato ad eseguire il collegamento utilizzando questo particolare modo.

Risposta dell'utente: Contattare il responsabile del firewall.

ICA9023 Impossibile caricare la DLL di EFM.

Spiegazione: Errore nel caricare la DLL di EFM.

Risposta dell'utente: Contattare il responsabile del firewall.

ICA9024 Richiesta di trasferimento avviata da *utente* **al firewall** *macchina***.**

Spiegazione: L'operazione di trasferimento è stata avviata.

ICA9025 Richiesta di trasferimento terminata con il codice di errore *codice di errore***.**

Spiegazione: L'operazione di trasferimento è stata completata.

ICA9026 Richiesta di trasferimento ricevuta da *utente* **sul firewall** *macchina* **alle** *ora***.**

Spiegazione: L'operazione di trasferimento è stata avviata all'ora specificata.

ICA9027 Il file *nome file* **nella funzione** *funzione* **è stato aggiunto alla richiesta di trasferimento.**

Spiegazione: Il file specificato deve essere trasferito.

ICA9028 Richiesta di attivazione avviata da *utente* **sul firewall** *macchina***.**

Spiegazione: L'operazione di attivazione è stata avviata.

ICA9029 Richiesta di attivazione terminata con codice di errore *codice di errore***.**

Spiegazione: L'operazione di attivazione è stata completata.

ICA9030 Richiesta di attivazione ricevuta da *utente* **sul firewall** *macchina* **alle** *ora***.**

Spiegazione: L'operazione di attivazione è stata avviata all'ora specificata.

ICA9031 Attivazione della funzione *funzione* **terminata con il codice di errore** *codice di errore***.**

Spiegazione: L'attivazione della funzione specificata è stata completata.

ICA9032 Configurazione NAT aggiornata alle *ora* **del** *data***.**

Spiegazione: La configurazione NAT è stata aggiornata.

ICA9033 Supporto NAT (livello *versione.rilascio***) inizializzato alle** *ora* **del** *data***.**

Spiegazione: Il supporto NAT del firewall è stato inizializzato.

ICA9034 Supporto NAT disattivato alle *ora* **del** *data***.**

Spiegazione: Il supporto NAT è stato disabilitato.

ICA9035 NAT non può allocare l'indirizzo registrato per l'indirizzo sicuro *indirizzo IP sicuro***.**

Spiegazione: L'indirizzo sicuro non è stato convertito perché non ci sono indirizzi disponibili nel lotto di indirizzi registrati.

ICA9036 NAT ha rilasciato l'indirizzo registrato *indirizzo IP registrato* **nel lotto di indirizzi.**

Spiegazione: L'indirizzo registrato è stato rilasciato nel gruppo di indirizzi IP registrati.

ICA9037 Aggiornamento automatico delle interfacce del firewall alle *ora e data***.**

Spiegazione: Il programma di inizializzazione del firewall è stato denominato **UpdateInterfaces()** per eseguire il trigger automatico del file delle interfacce, fwadpt.cfg.

Azione del sistema: Nessuna

Risposta dell'utente: Nessuna

ICA9038 L'interfaccia *indirizzo* **è stata eliminata dalle configurazioni del firewall.**

Spiegazione: L'indirizzo decimale con punti specificato è stato elencato nel file di configurazione del firewall, fwadpt.cfg, ma non è noto allo stack TCP. Per questo motivo, è stato eliminato dal file di configurazione.

Azione del sistema: Nessuna

Risposta dell'utente: Nessuna

ICA9039 L'interfaccia *indirizzo* **è stata aggiunta alla configurazione del firewall.**

Spiegazione: L'indirizzo decimale con punti è stato trovato dallo stack TCP ma non nel file di configurazione del firewall, fwadpt.cfg, pertanto è stato aggiunto a tale file.

Azione del sistema: Nessuna

Risposta dell'utente: Nessuna

ICA9040 La maschera dell'interfaccia *indirizzo* **è stata aggiornata da** *maschera precedente* **a** *nuova maschera***.**

Spiegazione: La maschera nel file fwadpt.cfg non corrispondeva a quella installata sull'hardware. Il campo maschera corretto è stato aggiornato nel file fwadpt.cfg.

Azione del sistema: Nessuna

Risposta dell'utente: Nessuna

ICA9041 Nessuna interfaccia trovata su questa macchina.

Spiegazione: Nessuna interfaccia dell'adattatore è stata trovata su questa macchina.

Azione del sistema: Nessuna

Risposta dell'utente: Nessuna

ICA9042 NAT attivato con indirizzo unificato *indirizzo unificato***.**

Spiegazione: NAT è stato correttamente inizializzato ed ora è attivo. Se l'indirizzo è 0, ciò significa che la conversione di tipo Unificare è inattiva.

Azione del sistema: Nessuna

Risposta dell'utente: Nessuna

ICA9043 Impossibile inizializzare NAT con codice di errore *rc***.**

Spiegazione: NAT non è stato inizializzato ed è inattivo.

Azione del sistema: Non verrà richiamata nessuna funzione di NAT.

Risposta dell'utente: Se si desidera che NAT sia operativo, controllare il codice di errore e correggerlo. Se il problema persiste, contattare l'assistenza IBM.

ICA9044 NAT disattivato.

Spiegazione: NAT è stato correttamente disattivato ed ora è inattivo.

Azione del sistema: Nessuna

Risposta dell'utente: Nessuna

ICA9045 NAT ha allocato indirizzo:porta *indirizzo***:***porta* **per indirizzo sicuro:porta** *indirizzo sicuro***:***porta*

Spiegazione: NAT ha allocato l'indirizzo:porta dal gruppo di indirizzi per l'host sicuro.

Azione del sistema: Nessuna

Risposta dell'utente: Nessuna

ICA9046 NAT non può allocare indirizzo unificato per indirizzo sicuro *indirizzo sicuro*

Spiegazione: NAT ha esaurito le porte con indirizzo unificato.

Azione del sistema: Il pacchetto dell'host locale è stato tralasciato.

Risposta dell'utente: Ciò significa che ci sono troppi collegamenti in sospeso. È possibile che un responsabile desideri ridurre il timeout associato utilizzando l'indirizzo unificato nel tentativo di eliminare più rapidamente le entrate inattive della tavola di conversione.

ICA9047 NAT ha deallocato indirizzo:porta *indirizzo*:*porta* **da indirizzo sicuro:porta** *indirizzo sicuro*:*porta*.

Spiegazione: NAT ha restituito la coppia indirizzo:porta specificata al gruppo disponibile.

Azione del sistema: Nessuna

Risposta dell'utente: Nessuna

ICA9048 NAT ha individuato un pacchetto frammentato arrivato con protocollo:*protocollo* **indirizzo:porta** *indirizzo*:*porta* **indirizzo sicuro:porta** *indirizzo sicuro*:*porta*.

Spiegazione: NAT ha individuato un pacchetto di controllo FTP frammentato o un messaggio di errore ICMP frammentato. NAT convertirà il pacchetto di controllo FTP frammentato, ma il carico non verrà esaminato. Se si tratta di un comando PORT frammentato, i dati FTP non potranno essere utilizzati, in quanto l'indirizzo IP contenuto nel messaggio non viene convertito. Se il pacchetto è un messaggio di errore ICMP frammentato, verrà tralasciato.

Azione del sistema: Consultare la relativa spiegazione.

Risposta dell'utente: Se ciò si verifica ripetutamente, rivolgersi all'assistenza IBM.

ICA9049 NAT ha individuato un pacchetto fuori dall'ordine da *indirizzo origine* **a** *indirizzo destinazione* **impossibile da convertire.**

Spiegazione: NAT ha individuato un datagram frammentato che è arrivato prima del primo frammento del datagram.

Azione del sistema: NAT non può convertire il frammento correttamente, per cui il datagram viene tralasciato.

Risposta dell'utente: Se ciò si verifica ripetutamente, rivolgersi all'assistenza IBM.

ICA9050 NAT non è riuscito a convertire un pacchetto con protocollo:*protocollo*, **indirizzo origine:porta** *indirizzo*:*porta*, **indirizzo destinazione:porta** *indirizzo sicuro*:*porta*, **con codice di errore** *rc*.

Spiegazione: NAT non è riuscito a convertire il pacchetto.

Azione del sistema: Il pacchetto viene tralasciato.

Risposta dell'utente: Se ciò si verifica ripetutamente, rivolgersi all'assistenza IBM.

ICA9051 NAT ha individuato un pacchetto arrivato con protocollo:*protocollo* **a indirizzo:porta** *indirizzo*:*porta* **da indirizzo sicuro:porta** *indirizzo sicuro*:*porta*

Spiegazione: NAT ha individuato l'arrivo di un pacchetto.

Azione del sistema: Nessuna

Risposta dell'utente: Nessuna

ICA9052 NAT ha individuato un pacchetto in partenza con protocollo:*protocollo* **a indirizzo:porta** *indirizzo*:*porta* **da indirizzo sicuro:porta** *indirizzo sicuro*:*porta*

Spiegazione: NAT ha individuato la partenza di un pacchetto.

Azione del sistema: Nessuna

Risposta dell'utente: Nessuna

ICA9053 *Valore stringa nome file* **in %3$d**

Spiegazione: debug in corso

Azione del sistema: Nessuna

Risposta dell'utente: Nessuna

ICA9054 Impossibile utilizzare contemporaneamente indirizzo IP:*indirizzo* **come indirizzo di interfaccia sicura/non sicura e indirizzo unificato.**

Spiegazione: Tali indirizzi non possono essere identici.

Azione del sistema: L'azione richiesta non viene eseguita.

Risposta dell'utente: Scegliere un indirizzo sicuro/non sicuro o un indirizzo unificato diverso.

ICA9055 NAT ha individuato un pacchetto fuori dall'ordine da *indirizzo origine* **a** *indirizzo destinazione* **che è possibile convertire.**

Spiegazione: NAT ha individuato un frammento di datagram interno o finale arrivato fuori dall'ordine.

Azione del sistema: NAT è stato in grado di convertire il frammento correttamente per cui non ha tralasciato il datagram.

Risposta dell'utente: Nessuna

ICA9060 Errore grave di inizializzazione del server di configurazione - socket(): *messaggio di errore di sistema*

Spiegazione: L'inizializzazione del server di configurazione non è riuscita, il daemon è stato arrestato.

Risposta dell'utente: Correggere l'errore di sistema indicato e riavviare il server di configurazione.

ICA9061 Errore grave di inizializzazione del server di configurazione - listen(): *messaggio di errore di sistema*

Spiegazione: L'inizializzazione del server di configurazione non è riuscita, il daemon è stato arrestato.

Risposta dell'utente: Correggere l'errore di sistema indicato e riavviare il server di configurazione.

ICA9062 Errore grave del server di configurazione - tentativo principale di accept(): *messaggio di errore di sistema*

Spiegazione: La routine principale del server di configurazione non è riuscita, il daemon viene arrestato.

Risposta dell'utente: Correggere l'errore di sistema indicato e riavviare il server di configurazione.

ICA9063 Errore del server di configurazione - *funzione errata***: codice di errore = 0x***codice di errore della funzione*

Spiegazione: Il server di configurazione ha rilevato un errore nella funzione indicata. Il daemon si arresta.

Risposta dell'utente: Correggere l'errore di sistema indicato e riavviare il server di configurazione.

ICA9064 Opzione sconosciuta -*valore* ignorato.

Spiegazione: L'opzione indicata è stata specificata e non viene riconosciuta.

ICA9065 Errore del server di configurazione - *funzione errata*: *messaggio di errore di sistema*

Spiegazione: Il server di configurazione ha rilevato un errore nella funzione indicata. Il daemon si arresta.

Risposta dell'utente: Correggere l'errore di sistema indicato e riavviare il server di configurazione.

ICA9066 Memoria insufficiente: server di configurazione: malloc(*byte*) ha restituito NULL nella funzione *nome_funzione*.

Spiegazione: Impossibile assegnare memoria sufficiente - malloc ha restituito NULL.

ICA9067 Bind non riuscito, indirizzo: *porta* già in uso.

Spiegazione: L'indirizzo di porta fornito è attualmente in uso.

Azione del sistema: Il server di configurazione viene terminato.

Risposta dell'utente: Collegarsi al server di configurazione utilizzando un indirizzo di porta diverso oppure contattare il responsabile del Firewall.

ICA9068 Opzione *valore* non riuscita o specificata in modo errato.

Spiegazione: L'opzione indicata non è riuscita oppure è stata specificata in modo errato.

Azione del sistema: Il server di configurazione viene terminato.

Risposta dell'utente: Correggere l'uso dell'opzione indicata e riavviare il server di configurazione.

ICA9069 Inizializzazione SSL non riuscita.

Spiegazione: Non è stato possibile inizializzare l'ambiente di crittografia SSL oppure il collegamento con il partner non è riuscito.

Azione del sistema: Il server di configurazione viene terminato.

Risposta dell'utente: Contattare il responsabile del firewall per verificare l'ambiente SSL.

Appendice B. Hardening per la configurazione del sistema Windows NT

Hardening è il processo che ottimizza la sicurezza e l'efficienza disattivando i daemon non necessari e disabilitando gli ID utente non autorizzati. Hardening è una parte del processo di installazione del software IBM Firewall ed edita le risorse di sistema che possono compromettere la sicurezza.

I servizi, che non sono necessari per la configurazione di IBM Firewall e che costituiscono una minaccia per la sicurezza, vengono disabilitati. Tutti i protocolli non TCP/IP vengono eliminati.

Appendice C. RFC (Requests for Comment)

RFC (Requests for comments) sono dei documenti che presentano nuovi protocolli e stabiliscono gli standard per l'insieme di protocolli Internet. Copie cartacee di tutti i documenti RFC sono disponibili presso il NIC (Network Information Center), su base singola o tramite abbonamento. Per ottenere questi documenti, rivolgersi a:

Government Systems, Inc.
Attn: Network Information Center
14200 Park Meadow Drive
Suite 200
Chantilly, VA 22021

È possibile accedere ai documenti RFC dal seguente URL:

http//www.cis.ohio-state.edu/hypertext/information/rfc.html.

Le copie in linea sono disponibili presso il NIC utilizzando FTP per collegarsi a `ds.internic.net`. Questi file possono essere trasferiti utilizzando il seguente formato:

```
RFC:RFCnnnn.TXT
RFC:RFCnnnn.PS
```

Dove:

nnnn è il numero RFC

`TXT` è il formato del testo

`PS` è il formato PostScript

Il formato per l'indice RFC è:

```
RFC:RFC-INDEX.TXT
```

Nota: Molti RFC sono disponibili in formato testo. Prima di richiedere un file PostScript, controllare l'indice RFC per assicurarsi che il documento RCF sia disponibile in quel formato. È anche possibile richiedere le copie in linea dei documenti RFC tramite posta elettronica, dal server di posta NIC automatizzato, inviando un messaggio a `mailserv@ds.internic.net`. Includere uno dei seguenti comandi nella nota:

```
SEND RFCnnnn.TXT
```

o

```
SEND RFCnnnn.PS
```

Dove:

nnnn è il numero RFC

`TXT` è il formato del testo

`PS` è il formato PostScript

Ad esempio, per richiedere il formato testo RFC 812, specificare:

```
SEND RFC812.TXT
```

Per richiedere una copia in linea dell'indice RFC, includere il seguente comando nella nota:

```
SEND RFC-INDEX.TXT
```

Appendice D. Formato del file di configurazione Socks5.conf di IBM eNetwork Firewall

Per impostazione assunta, il file di configurazione **socks5.conf** è ubicato nell'indirizzario di installazione di IBM Firewall. Se necessario, è possibile editare questo file utilizzando un editor di testo.

Il file di configurazione **socks5.conf** viene letto la prima volta che viene richiamato il server. Per eseguire l'aggiornamento senza arrestare il sistema, immettere `socks5.config`. Questo file contiene le informazioni necessarie ad IBM Firewall per determinare l'interfaccia da utilizzare per raggiungere un determinato indirizzo, per stabilire se collegarsi direttamente ad un determinato indirizzo o se utilizzare un altro server proxy nonché i requisiti da soddisfare per stabilire un collegamento proxy.

Il file di configurazione contiene le seguenti sezioni:

- Alias
- Variabili
- Moduli
- Autenticazione
- Instradamento
- Proxy
- Controllo accessi

Nelle sezioni Autenticazione, Instradamento, Proxy e Controllo accessi, le righe vengono lette rispettando l'ordine finché non viene stabilita una corrispondenza con una determinata sezione: l'ordine delle righe è molto importante. Affinché venga stabilita una corrispondenza tra le righe, tutte le entrate della riga devono corrispondere.

Specifica delle porte

Le porte possono essere specificate utilizzando il nome, il numero o l'intervallo. Gli intervalli iniziano con [o (e terminano con) o] a seconda se l'intervallo sia o

Parametro	Descrizione
hostIP/ mask	Un indirizzo host collegato mediante "AND" con la maschera deve essere lo stesso dell'IP host collegato mediante "AND" con la maschera. Di solito viene utilizzato per mascherare la parte host dell'indirizzo da una parte della rete o sottorete.
-	Corrisponde tutto. Sono consentiti tutti gli host.
n1	Equivale a n1.0.0.0/255.0.0.0.
n1.n2	Equivale a n1.n2.0.0/255.255.0.0.
n1.n2.n3	Equivale a n1.n2.n3.0/255.255.255.0.
.domain.name	Il nome host deve terminare con la stringa *.domain.name.*
a.host.name	Il nome host deve corrispondere esattamente a *a.host.name.*

Esiste anche un supporto per la sintassi del modello host precedente. Tuttavia, il nuovo metodo è consigliato ed è più semplice da leggere.

Parametro	Descrizione
hostIP/a	Corrisponde tutto (come "-"). Sono consentiti tutti gli host.
hostIP/n	Corrispondenza di rete. Maschera le parti host e della sottorete dell'indirizzo, lasciando solo la parte di rete. La maschera utilizzata a tale scopo dipende dalla classe dell'indirizzo IP dell'host.
hostIP/s	Corrispondenza di sottorete. Maschera la parte host dell'indirizzo, lasciando solo la parte di rete e sottorete. La maschera utilizzata a tale scopo dipende dalla classe dell'indirizzo IP dell'host.
hostIP/h	Corrispondenza degli host. Equivale all'IP host.

Specifica dei metodi di autenticazione

I metodi di autenticazione che vengono inviati sono *ibmcram* e *ibmpwd*. È possibile aggiungerne altri.

I metodi di autenticazione possono essere specificati come un elenco di metodi separati da virgole. Per la corrispondenza delle righe, il metodo di autenticazione deve essere rappresentato da uno dei metodi appartenenti all'elenco. Questa sintassi viene denominata modello di autenticazione. Il metodo di autenticazione NULL viene definito per impostazione assunta. Gli altri metodi di autenticazione possono essere inclusi caricando i moduli appropriati. "-" indica che qualsiasi metodo di autenticazione è valido, incluso NULL.

Entrate di autenticazione

Le entrate di autenticazione indicano il tipo di autenticazione che può essere utilizzato. Il formato è:

```
auth/ban   source-address  source-port
auth-methods
```

Parametro	Descrizione
auth/ban	Indica se le entrate di autenticazione sono autorizzate (auth) o meno (ban).
source-address	Un modello host valido.
source-port	Un modello di porta valido.
auth-methods	Un modello di autenticazione valido.

La parola chiave "ban" indica che l'autenticazione non deve essere tentata con questo host e che non è utilizzabile per il server specificato.

Se non è specificata alcuna riga auth/ban, il valore assunto indica che è valido qualsiasi metodo di autenticazione. Se le autorizzazioni al collegamento sono impostate su *deny* (valore assunto), il collegamento non verrà rifiutato dopo che l'autenticazione è stata applicata. Nel protocollo SOCKS5, l'autenticazione precede l'autorizzazione. Stabilire il metodo di autenticazione in base al tipo di host.

Specifica dei comandi

Anche i comandi possono essere specificati come un elenco separato da virgole. Fare riferimento a questa sintassi come ad un modello di comando. I comandi definiti sono: connect, bind, udp, ping e traceroute. È possibile aggiungere altri comandi tramite i moduli. Un trattino ("-") indica che è valido qualsiasi comando.

Caricamento dei moduli

I moduli consentono l'espansione personalizzata della funzionalità del server aggiungendo nuovi metodi di autenticazione, comandi, controlli dell'autorizzazione e filtri del contenuto. Il formato è: *module stub filename options*

Parametro	Descrizione
module	L'identificativo del modulo da caricare.
stub	Un prefisso del nome dipendente dal modulo per accedere ai nomi delle funzioni.
filename	Il nome file del modulo da caricare.
options	Le eventuali informazioni di configurazione per uno specifico modulo.

I moduli possono definire i campi utilizzati altrove, pertanto si consiglia di immettere per prima cosa le righe dei moduli. Ad esempio, i moduli di autenticazione definiscono i nomi dei metodi di autenticazione utilizzati nelle righe auth e permit.

Entrate di instradamento

Sulle macchine a più interfacce di rete (e quindi con più indirizzi IP), assicurarsi che determinate interfacce di rete vengano utilizzate insieme a determinati indirizzi. Ciò impedisce il verificarsi di un'"indicazione di falsi indirizzi IP" (per le macchine al di fuori delle rete che pretendono di accedervi), assicurando che le macchine all'interno della rete utilizzino l'interfaccia di rete interna e che quelle al di fuori utilizzino l'interfaccia di rete esterna. Viene anche utilizzato dal server SOCKS per

Variabile di ambiente	Descrizione
SOCKS5_BINDPORT [porta]	Configura IBM Firewall per utilizzare la porta specificata, invece del valore assunto della porta 1080.
SOCKS5_RECVFROMANYONE	Se il supporto UPD è abilitato, questa variabile consente ai client UPD di ricevere messaggi da mittenti sconosciuti.
SOCKS5_USECLIENTSPORT	Configura IBM Firewall al proxy solo se può collegarsi alla stessa porta che il server utilizza per inviare i messaggi. Questa variabile è necessaria per eseguire il proxy dei collegamenti UDP quando il server invia i dati al client (i messaggi vengono inviati al client prima che il client li invii al server). Un esempio può essere il sistema RealAudio.
SOCKS5_MAXCHILD	Il numero massimo di thread simultanei.
SOCKS5_NOREVERSEMAP	Disabilita la mappatura degli indirizzi IP ai nomi host. Se nel file di configurazione vengono assegnati degli alias, questa variabile aumenta le prestazioni a discapito delle informazioni di registrazione.
SOCKS5_NOSERVICENAME	Disabilita la mappatura dei numeri di porta ai nomi dei servizi. Se nel file di configurazione vengono assegnati degli alias, questa variabile aumenta le prestazioni a discapito delle informazioni di registrazione.
SOCKS5_NOIDENT	Disabilita la richiesta IDENT, anche se compilata. È utile quando il collegamento ai client è lento ed i client non utilizzano IDENTD. Questa variabile riduce i periodi di timeout.
SOCKS5_DEMAND_IDENT	Configura l'autenticazione NULL in modo da non riuscire, se non è stata ricevuta alcuna risposta IDENT dai client. È utile per assicurare che un nome utente venga sempre associato ad una richiesta di collegamento.

Entrate proxy

Le entrate proxy descrivono gli indirizzi dei server proxy SOCKS. Queste righe indicano al server come contattare un determinato host. Se nessuna riga corrisponde ad un host, l'host viene contattato direttamente. Il formato è: *proxy-type dest-addr dest-port proxy-addr proxy-port*

Parametro	Descrizione
proxy_type	Il tipo di server proxy. Le entrate valide sono: • socks5 • socks4 • no proxy
dest-address	Un modello host valido.
dest-port	Un modello di porta valido.
proxy-address	L'indirizzo IP o il nome del server proxy.
proxy-port	La porta del server proxy su cui il daemon SOCKS sta accettando i collegamenti.

Entrate del controllo accessi

La sezione relativa al controllo accessi determina se viene consentita o negata una richiesta per stabilire un collegamento. Esistono due tipi di righe, permit e deny. Tutte le voci sulla riga devono corrispondere. Il formato è:

```
permit auth cmd src-host dest-host src-port dest-port [userlist]
deny auth cmd src-host dest-host src-port dest-port [userlist]
```

Parametro	Descrizione
auth	Un elenco di metodi di autenticazione, specificato da un'entrata e da un modello auth validi.
cmd	Un modello di comando valido che specifica i comandi corrispondenti a questa riga.
scr-host	Un modello host valido per l'host di origine.
dest-host	Un modello host valido per l'host di destinazione.
scr-port	Un modello di porta valido per la porta dell'host di origine.
dest-port	Un modello di porta valido per la porta dell'host di destinazione.
userlist	Un modello utente valido.

Filtri

La funzione di filtro attraverso un modulo caricato viene eseguita dalla direttiva del filtro. Il formato è:

```
filter  name auth cmd src-host dest-host src-port dest-port [userlist]
```

Parametro	Descrizione
name	L'identificativo del modulo di filtro.
auth	Un elenco di metodi di autenticazione, specificato da un'entrata e da un modello auth validi.
cmd	Un modello di comando valido che specifica i comandi corrispondenti a questa riga.
scr-host	Un modello host valido per l'host di origine.
dest-host	Un modello host valido per l'host di destinazione.
scr-port	Un modello di porta valido per la porta dell'host di origine.
dest-port	Un modello di porta valido per la porta dell'host di destinazione.
userlist	Un modello utente valido.

Appendice E. Bibliografia

Per ulteriori informazioni relative alla sicurezza su Internet, visitare la home page di IBM Firewall **http://www.software.ibm.com/enetwork/firewall**.

Informazioni contenute nelle pubblicazioni IBM

Di seguito sono riportate ulteriori fonti di informazioni IBM sui firewall, sulla sicurezza Internet e su argomenti relativi alla sicurezza in generale.

Argomenti relativi al firewall

Questi documenti sono disponibili sul CD-ROM di IBM Firewall e sulle home page di IBM eNetwork Firewall.

- *IBM eNetwork Firewall - Guida per l'utente*, GC13-2748-01
- *IBM eNetwork Firewall - Manuale di riferimento*, SC13-2750-00
- *Guarding the Gates Using the IBM eNetwork Firewall for NT 3.2*, SG24-5209

Argomenti relativi ad Internet e Web (World Wide Web)

- *A Guide to the Internet Connection Servers*, SG24-4805
- *Accessing CICS Business Applications from the World Wide Web*, SG24-4547
- *Accessing OS/390 OpenEdition MVS from the Internet*, SG24-4721
- *Accessing the Internet*, SG24-2597
- *Building the Infrastructure for the Internet*, SG24-4824
- *Cool Title about the AS/400 and Internet*, SG24-4815
- *The Domino Defense: Security in Lotus Notes and the Internet*, SG24-4848
- *Examples of Using MQSeries on WWW*, SG24-4882
- *How to Secure the Internet Connection Server for MVS/ESA*, SG24-4803
- *Lotus Domino Server Release 4.5 on AIX Systems: Installation, Customization, and Administration*, SG24-4694
- *Netscape Proxy Server*, SK2T-7444
- *Running CICS Transactions through the Web: The CICS Internet Gateway to VSE/ESA*, SG24-4799
- *Safe Surfing: How to Build a Secure World Wide Web Connection*, SG24-4564
- *Teach Yourself CGI Programming with PERL in a Week*, SR23-7343
- *Using the Information Super Highway*, GG24-2499
- *World Wide Web Access to DB2*, SG24-4716

Argomenti relativi alla sicurezza

- *The Basics of IP Network Design*, SG24-2580
- *Elements of Security: AIX V4.1*, GG24-4433
- *Enterprise-Wide Security Architecture and Solutions Presentation Guide*, SG24-4579
- *HACMP/6000 Customization Examples*, SG24-4498
- *IBM Global Network (IGN) Security Policy*, GC34-2206
- *IBM Security Architecture: Securing the Open Client/Server Distributed Enterprise*, SC24-8135
- *IBM Systems Monitor: Anatomy of a Smart Agent*, SG24-4398
- *Security Overview of Open Systems Networking*, GG24-3815
- *Systems Monitor for AIX User's Guide*, SC31-8173
- *TCP/IP Tutorial and Technical Overview*, GG24-3376

Informazioni contenute in altre pubblicazioni

Queste pubblicazioni fanno riferimento a sendmail, TCP/IP e UNIX:

- Albitz, Paul, and Cricket Liu. *DNS and BIND*. Sebastopol, CA: O'Reilly and Associates, 1997. (ISBN: 1-56592-236-0)
- Costales, Brian with Eric Allman. *Sendmail* O'Reilly and Associates, Inc. (ISBN: 1-56592-222-0)
- Hunt, Craig. *TCP/IP Network Administration* O'Reilly and Associates, Inc. (ISBN: 0-937175-82-X)
- Nemeth, Snyder, et al. *UNIX System Administration Handbook* Prentice Hall. (ISBN: 0-13-151051-7

Le seguenti pubblicazioni fanno riferimento ai firewall ed alla sicurezza su Internet:

- Ahuja, Vijay. *Network and Internet Security*. Boston: Academic Press Professional, 1996. (ISBN: 0120455951)
- Ahuja, Vijay. *Secure Commerce on the Internet*. Boston: Academic Press Professional, 1997. (ISBN: 0120455978)
- Anderson, Bart, et al. *The Waite Group's UNIX Communications and the Internet*. Indianapolis, IN: Sams Pub., 1995. (ISBN: 0672305372)
- Atkins, Derek, et al. *Internet Security: Professional Reference*. Indianapolis, IN: New Riders Publishing, 1996. (ISBN: 1562055577)
- Chapman, D. Brent, and Elizabeth D. Zwicky. *Building Internet Firewalls*. Sebastopol, CA: O'Reilly and Associates, 1995. (ISBN: 1565921240)
- Cheswick, Willam R., and Steven M. Bellovin. *Firewalls and Internet Security*. New York: Addison-Wesley, 1994. (ISBN: 0201633574)
- Cooper, Frederic J., et al. *Implementing Internet Security*. Indianapolis, IN: New Riders Publishing, 1995. (ISBN: 1562054716)

- Curry, David. *UNIX System Security: Guide for Users and Systems Administrators*. Sebastopol, CA: O'Reilly and Associates, 1994. (ISBN: 0201563274)
- Garfinkel, Simson, and Gene Spafford. *Practical UNIX Security*. Sebastopol, CA: O'Reilly and Associates, 1991. (ISBN: 0937175722)
- Garfinkel, Simson, and Gene Spafford. *Practical UNIX and Internet Security*. Sebastopol, CA: O'Reilly and Associates, 1996. (ISBN: 1565921488)
- Hare, Chris, and Karanjit Siyan. *Internet Firewalls and Network Security*. Indianapolis, IN: New Riders Publishing, 1996. (ISBN: 1562056328)
- Randall, Neil. *Teach Yourself the Internet in a Week*. Indianapolis, IN: Sams.Net, 1995. (ISBN: 0672307359)
- Stallings, William. *Internet Security Handbook*. Foster City, CA: IDG Books, 1995. (ISBN: 0077092546)
- Stevens, W. Richard. *TCP/IP Illustrated*. Reading, MA: Addison-Wesley, 1994. (ISBN: 0201634953)

Appendice F. Glossario

Per accedere al glossario software IBM, consultare:
http://www.networking.ibm.com/nsg/nsgmain.htm.

Indice analitico

N

P

R

S

T

U

Riservato ai commenti del lettore

IBM eNetwork Firewall per Windows NT
Manuale di riferimento
Versione 3.2.1 **SC13-2750-01**

Commenti relativi alla pubblicazione in oggetto potranno contribuire a migliorarla.
Si invita il lettore ad usare lo spazio sottostante citando, ove possibile, i riferimenti alla pagina ed al paragrafo; i suggerimenti ed i commenti inviati potranno essere usati liberamente dall'IBM e dalla Selfin e diventeranno proprietà esclusiva delle stesse.
Si prega di non utilizzare questo foglio per richiedere informazioni tecniche su sistemi, programmi o pubblicazioni; per tali esigenze si consiglia di rivolgersi al punto di vendita o alla filiale IBM interessata.

Commenti:

. . . . . .

. . . . . .

. . . . . .

. . . . . .

. . . . . .

. . . . . .

. . . . . .

. . . . . .

. . . . . .

. . . . . .

. . . . . .

. . . . . .

. . . . . .

. . . . . .

. . . . . .

. . . . . .

Nome . . . . . .

Mansione/Titolo . . . . . .

Indirizzo . . . . . .

. . . . . Piegare . . . . . Piegare . . . . . .

. . . . . Piegare . . . . . Piegare . . . . . .

SELFIN S.p.A.

Translation Assurance

via F. Giordani, 7

80122 - N A P O L I

Printed in the European Union

SC13-2750-01