



IBM eNetwork Firewall for Windows NT

參考手冊

版本 3 版次 2.1.1



IBM eNetwork Firewall for Windows NT

參考手冊

版本 3 版次 2.1.1

註

在使用本資訊及其支援的產品之前，請務必閱讀第145頁的『注意事項』中的一般資訊。

第二版 (1998 年 6 月)

本版次適用於版本 3 版次 2.1.1 的 IBM eNetwork Firewall for Windows (產品編號 5765-C16)。本版次取代 SC40-0214-00。

Portions Copyright © 1993, 1994 by NEC Systems Laboratory.

所包含的安全性軟體來自 RSA Data Security, Inc. Copyright 1990,1995 RSA Data Security, Inc. All rights reserved.

© Copyright International Business Machines Corporation 1994, 1998. All rights reserved.

目錄

關於本書	vii
必備的知識	vii
本版次中的功能	vii
Socks 通訊協定第 5 版	vii
網路位址轉換	viii
簡易的管理	viii
NT 的強化	viii
嚴密的鑑證	viii
報告公用程式	viii
警示、監督、及記載	viii
隔離多個網路	viii
國家語言支援	ix
輸入 IP 位址	ix
如何連絡 IBM 以尋求服務	ix
第1章 使用 IBM Firewall 命令行介面	1
架構伺服器	1
領域名稱服務程式	2
過濾	3
HTTP Proxy	3
介面	4
日誌保存程式	5
日誌檔管理	6
日誌監督程式	7
郵件	10
網路位址轉換	10
呼叫	13
呼叫器架構	14
電訊公司	14
數據機架構	16
測試呼叫器架構	16
多種呼叫器	17
使用者	17
第2章 使用報告公用程式	23
報告公用程式用法	23
IBM Firewall 日誌格式	24
從防火牆日誌檔產生訊息	25
產生資料庫匯入檔	25
透過報告公用程式使用資料庫	27
報告公用程式的使用者介面	28
SQL 表格	29

第3章 附加的 SafeMail 軟體開發套件	45
SafeMail 處理概觀	45
建立附加的 SafeMail 開道	45
撰寫原始程式	46
建立 DLL	46
安裝 DLL	46
第4章 附加的日誌保存程式軟體開發套件	47
如何建立附加的日誌保存程式	47
撰寫原始程式	47
建立 DLL	47
安裝 DLL	47
第5章 提供自己的鑑證方法	49
使用者提供的鑑證	49
使用「軟體開發套件 (SDK)」來建立使用者提供的鑑證計劃	49
防火牆鑑證處理的概觀	49
建立使用者提供的鑑證計劃	50
第6章 使用「建立密碼鎖檔案公用程式」(MKKF)	57
建立密碼鎖檔案	57
第7章 疑難排解與測試	65
安裝及設定	65
過濾支援失敗	65
遞送路徑問題	65
無法從防火牆 ping 主電腦	65
無法從安全主電腦 ping 非安全主電腦 (反之亦然)	67
DNS 問題	67
尚未架構 DNS	68
DNS 查詢失敗或逾時	68
nslookup www.ibm.com. nns.nns.nns.nns 失敗	68
nslookup www.ibm.com. 127.0.0.1 失敗	68
nslookup host.secure.company.com. sns.sns.sns.sns 失敗	69
nslookup www.ibm.com. sns.sns.sns.sns 失敗	69
架構從屬站	69
伺服器沒有回應	69
無法登入至「架構伺服器」	70
資料傳輸控制	70
對連線所做的變更未生效	70
Proxy 伺服器	70
未傳輸任何資料	70
無法連線至想要的主電腦	71
鑑證服務程式	71
無法鑑證 Windows NT 管理者帳戶	71
無法鑑證防火牆 proxy 使用者	71

網路位址轉換	72
NAT 連線不作用	72
如何為 NAT 封包建立路徑呢?	72
有哪些可用的偵錯工具可以用來協助使用 NAT?	72
日誌機能	72
日誌機能變更在伺服器上沒有生效	72
報告公用程式	73
存取檔案時發生錯誤:	73
匯入資料至資料庫時發生錯誤。	73
 附錄A. 訊息	 75
訊息標籤	75
訊息	75
 附錄B. 強化「Windows NT 系統架構」	 133
 附錄C. 取得備註的要求 (RFC)	 135
 附錄D. IBM eNetwork Firewall Socks5.conf 架構檔格式	 137
指定連接埠	137
指定主電腦	137
指定鑑證方法	138
鑑證項目	138
指定命令	139
載入模組	139
遞送路徑項目	139
變數項目	140
環境變數	140
Proxy 項目	141
存取控制項目	141
過濾	142
 參考書目	 143
IBM 出版品中的資訊	143
防火牆主題	143
Internet 及全球資訊網主題	143
一般安全性主題	143
企業出版品中的資訊	143
 注意事項	 145
註冊商標	145
 名詞解釋	 147
 索引	 149
 讀者意見表	 153

關於本書

本書是專為網路或系統安全管理者 (負責在 Windows NT** 上安裝、管理和使用 IBM eNetwork Firewall 3.2 版) 而寫的參考手冊。若要知道如何使用 Telnet 或 FTP 等從屬站程式，請參閱您的 TCP/IP 從屬站程式的使用手冊。

必備的知識

您必須具備 TCP/IP 及網路管理的知識，再安裝及架構 IBM eNetwork Firewall。因為您將設置和架構一個控制進出網路的防火牆，所以您必須先瞭解網路運作的情形。尤其，您需要瞭解 IP 位址的基本資訊、完整名稱和子網路遮罩。

有關 TCP/IP (涵蓋 netstat、arp、ifconfig、ping、nslookup、DNS、sendmail、routing 及其它資訊) 的優良書籍為 *TCP/IP Network Administration*。請參閱參考書目以取得詳細的資訊。

有關執行 UNIX 管理，並提供 TCP/IP 概觀 (包括遞送路徑、網路硬體、DNS 及 sendmail) 的優良書籍為 *UNIX System Administration Handbook*。請參閱參考書目以取得詳細的資訊。

本版次中的功能

IBM eNetwork Firewall for Windows NT 提供各式各樣的功能，並且包含防火牆的全部三個架構：

1. 應用程式 proxy

- FTP
- HTTP，包括 Gopher 及 WAIS
- Telnet
- SafeMail

HTTP、Telnet 及 FTP 都具有鑑證能力。

2. 透過「Socks 通訊協定第 5 版」的電路層閘道，一種 Internet 標準。

3. 過濾 -- 廣泛且健全的一組基準，可根據它來允許或拒絕資料傳輸。基準包括 TCP/IP 位址、連接埠、通訊協定、方向、配接卡 (安全/非安全) 及其它。

提供許多預先定義的服務程式會使設定作業更快速。

Socks 通訊協定第 5 版

「Socks 通訊協定第 5 版」除了簡單又具有彈性之外，它還提供下列優點：

- 部署鑑證及加密方法時非常簡單

- UDP 連結，會建立虛擬 proxy 電路，在 UDP 型的 proxy 電路上來回移動
- Socks V5 Watcher，會顯示即時 socks 效能資訊

網路位址轉換

隨著 Internet 蓬勃發展，突顯出 IP 位址殆盡的問題。網路位址轉換 (NAT) 根據位址重新使用，對此一問題提供了解決方案。

NAT 的好處是，透過式容許使用專用或非法位址的網路與 Internet 上的主電腦通信；並可以有效地讓專用網路擁有寬廣的位址空間。此外，若使用 NAT，則專用網路中的位址就會被隱藏起來，不會被外界看到，進而提供多一層的安全性。

簡易的管理

透過使用 Java** 應用程式來從遠端機器進行管理，您就可以輕鬆地更新防火牆架構。此外，可以為不同的管理者指派不同層次的權限，以進一步控制防火牆的存取。無論是「Windows NT Firewall」或是「AIX Firewall」，都可以用這種單純、易懂的使用者圖形介面 (GUI) 來管理。

NT 的強化

安裝防火牆時會停用非 TCP/IP 通訊協定、不需要的系統服務程式，以及非管理者帳戶的本端登入。

嚴密的鑑證

提供支援所有一般的記號型鑑證機制如 SecurID、SecureNet 密碼鎖、及其它。

報告公用程式

報告公用程式可讓您在系統日誌匯入到資料庫引擎之後執行 SQL 查詢。

警示、監督、及記載

廣泛且詳細的記載功能會併入所有的防火牆活動與 TCP/IP 位址、使用者 ID、TDD、檔案名稱、埠號等。所包括的「日誌監督程式」是用來注意可疑的活動，並在超過臨界值時給您警示。

隔離多個網路

使用防火牆中的多個「網路介面卡 (NIC)」，您就可以隔離多個子網路。

國家語言支援

國家語言支援有英文、日文、韓文、法文、簡體中文、繁體中文、義大利文、西班牙文及巴西的葡萄牙文。

輸入 IP 位址

架構防火牆時，會要求您鍵入 IP 位址。您必須以下面格式輸入一個具有全部 4 個八位元組的完整帶點十進數 IP 位址：

`nnn.nnn.nnn.nnn`

其中每一個 nnn 代表三個數字的組合，其範圍從 000 到 255。

如何連絡 IBM 以尋求服務

「IBM 支援中心」提供關於問題診斷和解決方面的電話協助。您可以隨時打電話給「IBM 支援中心」；您可以在 8 個小時的上班時間內收到回電（星期一至星期五，8:00 a.m.至 5:00 p.m.，當地時間）。連絡電話是 1-800-237-5511。

美國或波多黎各以外地區，請連絡當地 IBM 代表或授權的 IBM 供應商。

第1章 使用 IBM Firewall 命令行介面

本章討論您可以從 IBM eNetwork Firewall 命令行中使用的命令。

下列資訊適用於命令作業：

- 本書所列出的命令使用下列語法：
 - 加底線 表示為使用者輸入的資料。
 - [] 指參數為選用性的。
 - {} 指使用者可選擇的參數。
 - | 是用來區隔選項。
- 所有參數均使用 keyword=value (關鍵字=值) 的格式。
- 如果一個參數具有多個值，則值應該括在雙引號內，且應該以空格區隔它們，例如：
`secaddr="11.22.33.1 11.22.33.2"`
- 任何參數都不能包含空格，除非它在雙引號內。
- 如果您略過一個或多個必要參數，則命令行公用程式將列出遺漏的參數。
- 如果在參數中輸入了一個無效值，則命令行公用程式將報告這個錯誤。
- 某些防火牆服務程式會在它們的架構檔變更時，以動態方式更新它們的作用。某些需要 update 次命令。已將 update 次命令提供給那些需要它的防火牆服務程式。
- 只有主要的防火牆管理者可以從命令行中執行程式。
- 因為複雜性與檔案的交互相依性，**不要直接編輯任何架構檔**。

架構伺服器

fwcfigsrv 命令會列出或變更架構伺服器的選項。管理者必須擁有管理資料傳輸控制功能的權限，才能發出這個命令。

若要列出架構伺服器選項，請發出下列命令。

```
fwcfigsrv cmd=list
```

fwcfigsrv 命令的輸出結果會是下面這個樣子：

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

若要變更架構伺服器選項，請發出下列命令。

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

參數定義如下：

localonly

指定防火牆是否只能從本端機器來管理。有效值為 yes 或 no。

encryption

指出架構伺服器是否要透過 ssl 將送入的資料加密。有效值為 none 或 ssl。

sslfile 指定使用 ssl 密碼鎖檔案名稱來進行 ssl 加密。請參閱第57頁的『第6章 使用「建立密碼鎖檔案公用程式」(MKKF)』。

領域名稱服務程式

「領域名稱服務程式(DNS)」將提供完整領域名稱服務程式給安全網路內的主電腦使用，而提供最少的資訊給安全網路外的主電腦。若要完成此目標需有三個領域名稱伺服器：

- 一個在防火牆
- 一個在安全網路內
- 一個在安全網路外

相關資訊，請參閱 *IBM eNetwork Firewall 使用指南*。

註：

1. x.x.x.x 是一個帶點十進制格式的 IP 位址。
2. secaddr 與 remaddr 參數的值可以是單一 IP 位址或 IP 位址的列示。如果指定了 IP 位址的列示，則列示應該以空格區隔，並包含在雙引號內。
3. 重覆的位址將被偵測並標示為一個錯誤。
4. 第一次架構 DNS 時，fwdns cmd=change 將建立新檔案。防火牆將恆僅具有一個 DNS 架構記錄。值可能是空的。變更改命令足以變更 DNS 記錄中的任一或全部值。

下列命令列出目前的 DNS 架構。

```
fwdns cmd=list
```

若要變更 DNS 架構項目及建立新檔案，請輸入：

```
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"
```

參數定義如下：

secdomain=SecureDomainName

您的內部、安全網路的領域名稱

secaddr=SecureDNSaddr[,...]

您的安全領域名稱伺服器的 IP 位址

remaddr=NonSecureDNSaddr[,...]

您的 Internet 連線服務供應站所提供的安全網路外的領域名稱伺服器的 IP 位址。

過濾

請使用 **fwfilter** 命令來啟動及停止過濾規則。

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

參數定義如下：

fwfilter cmd=update

重新建置架構及啟動該規則集。

fwfilter cmd=verify

執行架構的「測試建置」，但不啟動任何變更。

fwfilter cmd=list

列示最近建置的架構

fwfilter cmd=shutdown

停用過濾機制

fwfilter cmd=startlog

將所選取的資料傳輸記載至防火牆日誌機能中

fwfilter cmd=stoplog

停止 firewall 過濾記載

HTTP Proxy

HTTP proxy 會透過 IBM Firewall 評估 socks 伺服器用來瀏覽 Web 的需求，來有效處理瀏覽器要求。使用者可以存取 Internet 上有用的資訊，而不會危及它們內部網路的安全，並且不需要變更它們的從屬站環境來執行 HTTP proxy。

fwhttp 命令可列出或變更現行的 HTTP proxy 架構。

若要列出目前的 HTTP proxy 架構，請使用下列命令。

```
fwhttp cmd=list
```

若要變更目前的 HTTP proxy 架構，請使用下列命令。

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

參數定義如下：

port HTTP proxy 服務程式所要傾聽的連接埠。

maxcontentlengthbuffer

要用來將文件傳回的最大緩衝區大小，以能夠將內容長度標頭的附加資訊傳回。

minactivethreads

在起始設定時啟動，並可在執行期間繼續活動的工作者緒最小數限制。

maxactivethreads

可隨時執行的工作者緒最大數限制。

idlethreadtimeout

將閒置緒保持在可用狀態的最長時間限制。

logging

指示是否要記載 HTTP 活動。參數值為 on 或 off。

authenticate

所要鑑證的使用者層次。參數值有 all、none 或 new。

authenticatetimeout

在建立持續性連線之後，要等待從屬站提出要求的時間長短。

maxpersistrequests

在持續性連線上所要接收的最大要求數目。

persisttimeout

維持持續性連線的時間。

介面

安全介面會將 IBM Firewall 主電腦連到您要保護之內部網路的主電腦網路。您至少需具備一個安全介面，防火牆才會作用。非安全介面會將 IBM Firewall 連到一或數個外部網路或 Internet。IBM Firewall 至少必須具備一個非安全介面。

此命令會列出防火牆的網路介面。管理者必須擁有管理介面功能的權限，才能發出這個命令。

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

管理者權限的相關資訊，請參閱 *IBM eNetwork Firewall 使用指南* 的「管理」一章。

參數定義如下：

addr=x.x.x.x

列出已架構在防火牆的所有網路介面，並識別每一個網路介面為安全或非安全介面。同時它也可以識別名稱。若指定選用性參數 **addr**，就只會列出這種介面。如果提供給 **addr** 的 IP 位址為帶點十進位數，列示就會包含位址、狀態及所指定之位址的名稱 (假定已將它架構至防火牆)。

此命令可讓您將您的網路介面定義至防火牆。管理者必須擁有管理介面功能的權限，才能發出這個命令。

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

參數定義如下：

addr=x.x.x.x

包含要變更之介面的帶點十進位數位址。如果沒有將該介面定義至防火牆，就會產生錯誤報告。

state={secure|nonsecure}

包含 "secure" 或 "nonsecure" 其中一個關鍵字，這二種關鍵字可將介面所屬的網路分類。

name 有意義的名稱，可用來識別其所屬的介面或網路。可包含空格，但必須用雙引號括起來。

雖然狀態及名稱參數都是選用性的，但是您必須指定其中一項。

日誌保存程式

下列命令會呼叫日誌檔保存程式，來維護已架構來用於保存的日誌機能。

```
fwlogmgmt -l 或 fwlogmgmt -a
```

在 Windows NT Scheduled Service 中放入這個命令會很管用。相關資訊，請參閱 *IBM eNetwork Firewall 使用指南*。

日誌檔管理

日誌檔管理可定義及管理您的日誌與保存檔。fwlog 命令可新增、修改及刪除日誌機能。

若要新增日誌機能，請使用下列命令。

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

facility 的有效值為：

- firewall (local4) - 一般防火牆日誌，包含過濾器記載功能
- alert (local1) - 用來顯示「警示」顯示畫面的日誌監督常駐程式及臨界值違規警告。
- adminaudit (local0) - 管理審核日誌
- mail - 郵件日誌

priority 的有效值為：

- debug
- info
- warning
- error
- crit

logfile 參數可指定應將防火牆日誌項目傳送至何處。logfile 的有效值為完整的檔案名稱 (格式為 (磁碟機:\目錄))，以指定要將日誌項目寫入到哪一個檔案。

註：為警示日誌或防火牆日誌機能識別的檔案應彼此相異，而且也必須與要用防火牆功能來處理之任何其他日誌機能的檔案不同。

注意，僅有防火牆日誌訊息會出現在報告公用程式的檔案輸入中。沒有其他機能應該導向至與防火牆日誌或警示日誌相同的檔案。

arcfile、logtime 及 arctime 皆為選用性參數，且只有當 logfile 參數有指定檔案名稱時才能生效。如果指定了任何一個參數，就必須指定所有三個參數。這些參數可控制日誌保存。若要使實際日誌保存出現，必須定期執行 fwlogmgmt 命令。請參閱第5頁的『日誌保存程式』。

在預設的狀況下，防火牆會使用這些參數來指示儲存保存日誌記錄的位置，以及多久要保存一次。您需要指定這三個參數，來啟用保存功能。

您可以撰寫附加的防火牆保存功能來取代該保存功能。請參閱第47頁的『第4章 附加的日誌保存程式軟體開發套件』。

arcfile 參數須含有完整路徑名稱。

logtime 參數可指定在移至保存檔之前，將防火牆日誌項目保留在日誌檔中的最少天數。

arctime 參數可指定在清除之前，將防火牆記載記錄保留在保存檔中的最少天數。

若要變更日誌機能，請使用下列命令。

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

如果變更（尤其是在起始案例中）無法建立一個語法正確的架構檔（例如，已建立的日誌檔定義遺漏了某些欄位），將發出一個警告，而且「防火牆」將不會記載資料。

若要執行記載但不要保存，僅需 **facility**、**priority** 與 **logfile** 參數即可。一旦啟動日誌保存，若要將它停止，請將 **archive**、**logtime** 及 **arctime** 參數留白。若您已經排定了保存工作，請將它刪除。

若要列出目前的日誌檔架構資料，請使用下列命令。

```
fwlog cmd=list
```

若要刪除 `fwlog cmd=list` 命令上的項目所傳回的索引號碼指定的防火牆日誌項目，請發出下列命令。

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

日誌監督程式

請使用「日誌監督程式命令」來告訴日誌監督程式，要於何時、如何觸發警示。在所指定的時間間隔中，當達到這個命令（或是相對應的架構從屬站畫面）所指定的臨界值時，就會出現這個警示。當警示出現時：

1. 會將記錄寫入防火牆警示機能及防火牆日誌機能
2. 會執行所指定的命令
3. 會將通知傳送至一或多個使用者 ID

4. 會將訊息傳送至呼叫裝置

最後三項動作是由這裡所指定的適當架構值來加以控制。

列出日誌監督程式設定值

```
fwlogmon cmd=list
```

指定當有任何警示出現時，要用來接收郵件通報的使用者 ID

若要指定當有任何警示出現時，要用來接收郵件通報的使用者（會將通知傳送到您所加入的每一個 ID）：

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

指定當有任何警示出現時，所要執行的命令

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

```
fwlogmon cmd=delete
          type=command
```

根據失敗的登入嘗試次數，指定在到達臨界值時應觸發警示

```
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
```

根據特定防火牆訊息 ID 出現的次數，指定在到達臨界值時應啟動警示

```
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=
```

參數定義如下：

- type** 識別所新增或修改的日誌監督程式命令性質的類型。
- 允用的值有 `id`、`command`、`msg`、`single`、`multi` 及 `host`。
- id** 指定要將通知傳送到哪一個使用者 ID。
- command** 指定要執行的命令。
- msg** 針對特定日誌訊息的監督工作。
- single** 對單一使用者 ID 監督工作。會為每一個嘗試失敗的 ID 保留一個計數器。當任一 ID 的計數器達到在此命令中指定的臨界值時，就會觸發警示。
- multi** 對多個使用者 ID 監督工作。如果嘗試失敗的所有使用者 ID 之計數器總數，達到在此命令中指定的臨界值時，就會觸發警示。
- host** 針對主電腦名稱來監督工作。會為每一個嘗試失敗的主電腦名稱保留一個計數器。當任一主電腦名稱的計數器達到在此命令中指定的臨界值時，就會觸發警示。
- username** 防火牆管理者或其他要接收警示通報之使用者的郵件 ID。您必須正確地架構安全端的郵件伺服器，才能順利地傳送警示通報。
- command** 當任何警示出現時，所要執行之命令的名稱。必須是執行檔的完整路徑名稱。它可以是 `.bat` 檔，執行該檔中的多項命令；但是如果該 `.bat` 檔會牽涉到其他檔案，也必須有那些檔案的完整路徑名稱。
- count** 設定失敗次數的臨界值，或是特定日誌訊息出現次數的臨界值，在達到臨界值時，會使用警示訊息。
- time** 以分鐘為單位來設定時間間隔。從第一次出現後，必須在這段時間間隔中達到該計數，才會觸發一個事件。發生在現行時間之前，比此間隔還早的事件，會從該計數刪除。

- pager** 指定在相關的臨界值觸發警示時，是否要使用呼叫。使用中的呼叫器架構會被用來傳送呼叫。
- tag** 要受監督的日誌訊息標籤 (訊息前置符號為 ICA)。無法監督 ICA 標籤少於 1000 的日誌監督程式訊息。

郵件

使用 `fwmail` 命令，來對映到公用及安全郵件領域。

```
fwmail cmd=list

fwmail cmd=add
    secdomain=
    mail=
    remdomain=

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

fwmail cmd=delete
    secdomain=
```

參數定義如下：

secdomain

讓在防火牆安全端的使用者知道所描述之郵件領域的名稱。

mail 郵件伺服器的位址。

remdomain

讓在防火牆非安全端的使用者知道所描述之郵件領域的名稱。

網路位址轉換

「網路位址轉換」(NAT) 可讓其他任何的 IP 網路重覆使用安全 IP 網路內的位址，以解決 IP 位址不夠用的問題。

NAT 支援四種類型的架構：

- Many-to-One 登記位址 - Many-to-One 轉換可轉換封包的安全位址及埠號，讓許多 (最多 65536) 內部位址共用一個已註冊的 IP 位址。這個供多者共用的已登記 IP 位址會將本端位址隱藏起來，但除了此 IP 位址之外，您必須要有另一個專門供 Firewall 使用的 Internet 登記位址。
- 轉換安全 IP 位址 - 轉換安全 IP 位址項目可定義一組需要 NAT 來執行 IP 位址轉換的安全網路位址。在預設的狀況下，「網路位址轉換程式」會在所有的安全 IP 位址上執行位址轉換。

- 排除安全 IP 位址 - 「排除安全 IP 位址」項目可定義一組不需 NAT 來執行 IP 位址轉換的安全網路位址。在預設的狀況下，「網路位址轉換程式」會在所有的安全 IP 位址上執行位址轉換，除非該位址在「排除安全 IP 位址」項目所指定的範圍內。
- 對映安全 IP 位址 - 「對映安全 IP 位址」項目可定義「安全 IP 位址」及「已登記的 IP 位址」之間的一對一對映。一對一式 IP 位址對映可讓外部應用程式從屬站（如 FTP 或 Telnet 從屬站）設定與安全網路內的伺服器機器之間的 TCP 階段作業。

NAT 命令的語法如下：

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

參數定義如下：

fwnat cmd=list

列示現行 NAT 架構

fwnat cmd=update

復新 NAT 引擎

fwnat cmd=verify

檢查架構語法

fwnat cmd=shutdown

停止所有位址轉換

fwnat cmd=startlog

啟動記載每一個已轉換的封包

fwnat cmd=stoplog

停止記載每一個已轉換的封包

若要將一個 many-to-one 項目加到 NAT 架構，請使用 **type=many-to-one**：

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

參數定義如下：

type=many-to-one

新增 many-to-one 項目

addr=Addr

識別已新增至已登記位址儲存區的已登記 IP 位址範圍的 IP 位址

timeout=minutes

在 NAT 可以釋出已登記 IP 位址之前，位址轉換可保持閒置的分鐘數。預設值為 15，範圍為 5-45。

若要修改 NAT 架構中的 many-to-one 項目，請使用下列語法：

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

參數定義如下：

index 當您執行 fwnat cmd=list 時，左邊的直欄中會出現特定 NAT 項目的號碼。請使用您的特定 NAT 項目的號碼來作為索引參數。

addr=Addr
識別已新增至已登記位址儲存區的已登記 IP 位址範圍的 IP 位址

timeout=minutes
在 NAT 可以釋出已登記 IP 位址之前，位址轉換可保持閒置的分鐘數。預設值為 15，範圍為 5-45。

若要將一個轉換項目加到 NAT 架構檔，請使用 **type=translate**，而若要自 NAT 架構檔排除一個項目，請使用 **type=exclude**：

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

參數定義如下：

type=translate
新增轉換項目

type=exclude
新增排除項目

addr=Addr
識別需要轉換的安全 IP 位址範圍的 IP 位址。

mask=Mask
識別 IP 位址範圍

若要修改 NAT 架構檔中的轉換或排除項目，請使用下列語法：

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

參數定義如下：

index 當您執行 fwnat cmd=list 時，左邊的直欄中會出現特定 NAT 項目的號碼。請使用您的特定 NAT 項目的號碼來作為索引參數。

addr=Addr
識別需要轉換的安全 IP 位址範圍的 IP 位址。

mask=Mask
識別 IP 位址範圍

若要將一個映射項目加到 NAT 架構，請使用 **type=map**：

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

參數定義如下：

type=map
新增對映項目

secaddr
應該轉換為指定的已登記位址的 IP 位址

remaddr
指出所指定的安全位址應該轉換為已登記位址

若要修改 NAT 架構中的對映項目，請使用下列語法：

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

參數定義如下：

index 當您執行 **fwnat cmd=list** 時，左邊的直欄中會出現特定 NAT 項目的號碼。請使用您的特定 NAT 項目的號碼來作為索引參數。

secaddr
應該轉換為指定的已登記位址的 IP 位址

remaddr
指出所指定的安全位址應該轉換為已登記位址

呼叫

您可以啟動呼叫器通報支援，在防火牆上有闖入警示時將訊息傳送到管理者的呼叫器，讓防火牆呼叫系統管理者。若要正確地運作，您必須用 **fwpgmr**、**fwcarrier** 及 **fwmodem** 命令來架構呼叫器、電訊公司服務及數據機。

呼叫器架構

fwpgr 命令可設定使用中之呼叫器的參數 (所謂使用中之呼叫器即是「防火牆」會以訊號通知的呼叫器)。

若要列出呼叫器，請使用下列命令。

```
fwpgr cmd=list
```

若要新增呼叫器，請使用下列命令。

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

若要修改呼叫器參數，請使用下列命令。

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

參數定義如下：

carrier 電訊公司服務程式名稱，與電訊公司資料庫中所定義的相同 (利用 **fwcarrier** 命令)。

modem
數據機名稱，與數據機資料庫中所定義的相同 (利用 **fwmodem** 命令)。

pagerid
由電訊公司所指定、特別用來識別您的呼叫裝置的號碼或名稱。

message
傳送到呼叫裝置並且會在呼叫裝置上顯示的訊息。根據您的電訊公司所提供的服務，該訊息可以是數字或文字。如果訊息超過電訊公司的長度設定 (比 200 個字元少)，或是超過 200 個字元，訊息會被截斷。

電訊公司

使用 **fwcarrier** 命令來設定您所使用之呼叫服務的參數。

若要列出電訊公司，請使用下列命令。

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

若要新增電訊公司，請使用下列命令。

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

若要修改電訊公司參數，請使用下列命令。

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

若要刪除電訊公司，請使用下列命令。

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

參數定義如下：

carrier 電訊公司的名稱。

dial 必須指定已訂約之 TAP 服務的電訊公司數據機電話號碼。

method
參數值必須為 TAP。

password
此為選用性的參數，除非電訊公司服務有要求。

length 電訊公司服務所允許的訊息長度上限。

baud 指定電訊公司服務所支援的最穩定傳輸速率。

parity 您電訊公司服務所支援的同位檢查類型。對 TAP 通訊協定而言，這通常是偶數同位檢查。

databits
您電訊公司服務所支援的資料位元數。對 TAP 通訊協定而言，這通常是 7。

stopbits
您電訊公司服務所支援的停止位元數。對 TAP 通訊協定而言，這通常是 1。

數據機架構

要設定通報支援時，您需要架構數據機。

請使用數據機命令來架構數據機，以傳送呼叫器要求給呼叫器的電訊公司。

若要列出數據機，請使用下列命令。

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

若要新增數據機，請使用下列命令。

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

若要修改數據機參數，請使用下列命令。

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

若要刪除數據機，請使用下列命令。

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

參數定義如下：

modem

數據機名稱。

comport

數據機所連接的 COM 序列埠。您必須在您的 Windows NT 系統上定義這個 COM 連接埠上的數據機。

initstring

數據機的起始設定字串。字串中的參數必須適合 AT 數據機命令，但是不能將 AT 併為字串的部份。所指定的參數必須與電訊公司數據機的通信需求配合。

outsideline

欲撥接外線時所使用的號碼。

測試呼叫器架構

若想確定您已正確地架構使用中的呼叫器，請使用下列命令。

```

pager
    carrier=
    modem=
    ID=
    msg=

```

參數定義可由 `fwpggr` 命令的參數來識別。

多種呼叫器

如果您必須常常變更您所使用的呼叫器，請執行下列作業：

- 確定您已定義所有必須的電訊公司及數據機。
- 使用 `fwpggr` 或架構從屬站來定義及儲存呼叫器架構
- 複製 `R00TDIR\config\pager.cfg` 檔案，並給它一個您能夠辨識的名稱
- 定義另一個呼叫器架構，並將它複製等等，直到您有所需的全部 `pager.cfg` 檔案備份為止
- 將您要使用的架構檔複製回 `R00TDIR\config\pager.cfg`

若您嘗試處理切換變更，請用 `Windows NT at` 命令來設定已排程的工作，以自動重複每次切換開始時的最後一個項目符號。

使用者

此命令新增一個使用者，或修改現存的防火牆使用者的一個或多個屬性。所有參數具有預設值，或在某些情況下不需要。對 `cmd=add` 而言，預設值將被儲存；對 `cmd=change` 而言，現存值將被保留。

```

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]
[mianother=MinNonAlphaChars]
[pwdwarntime=PasswordWarnTime]
    [userchg={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}]

```

基本參數

username

這個使用者的登入名稱。

fullname

使用者的全名，或某些其他屬於這個使用者的簡短 (線上) 資訊。如果空格將包括在這個值內，須以雙引號括住這個值。

level 預設值為 `proxy`，指出將建立的使用者為單純 `proxy` 或 `Socks` 使用者。管理函數群組與管理鑑證不適用於 `proxy` 使用者。

key 用來鑑證使用者的「Digital Pathways' SecureNet 密碼鎖」卡的密碼鎖。因為這個值必須含有空格，須以雙引號括住它。

鑑證

下列為鑑證字串及其相對應的鑑證方法。下面指出 `fwuser` 命令各種參數的鑑證字串用法。

- `permit-permit all`
- `deny-deny all`
- `password-Firewall password`
- `NT-NT logon password`
- `snk-SNK`
- `sdi-SDI`
- `user-user-supplied authentications`
- `userauth2-user-supplied authentications`

- userauth3-user-supplied authentications

secftp 從安全介面 FTP 登入的鑑證方法。有效值為 deny、permit、password、NT、snk、sdi、user、userauth2 及 userauth3。預設值為 deny。

remftp 從非安全介面 FTP 登入的鑑證方法。有效值為 deny、permit、password、NT、snk、sdi、user、userauth2 及 userauth3。預設值為 deny。

secauth
從安全介面 telnet 登入的鑑證方法。有效值為 deny、permit、password、NT、snk、sdi 與 user。預設值為 deny。

remauth
從非安全介面 telnet 登入的鑑證方法。有效值為 deny、permit、password、NT、snk、sdi、user、userauth2 及 userauth3。預設值為 deny。

secadmin
從安全介面「防火牆架構從屬站」登入的鑑證方法。有效值為 deny、permit、password、NT、snk、sdi、user、userauth2 及 userauth3。若為 proxy 使用者，則預設值為 deny；若為「主要防火牆」管理者，則預設值為 NT。

remadmin
從非安全介面「防火牆架構從屬站」登入的鑑證方法。有效值為 deny、permit、password、NT、snk、sdi、user、userauth2 及 userauth3。若為 proxy 使用者，則預設值為 deny；若為「主要防火牆」使用者，則預設值為 NT。

secsocks
來自防火牆的安全端之 Socks 從屬站連線的 Socks5 鑑證方法。有效值為 deny、permit、password、NT、snk、sdi、user、userauth2 及 userauth3。

如果 Socks5 伺服器是架構為使用者 ID/通行碼形式鑑證方法，而非「挑戰回應鑑證方法」(CRAM)，則 SNK 將不會運作，因為 Socks5 使用者 ID/通行碼通訊協定無法顯示 SNK 盤問。

預設值為 deny。

remsocks
來自防火牆的非安全端的 Socks 從屬站連線的 Socks5 鑑證方法。有效值為 deny、permit、password、NT、snk、sdi、user、userauth2 及 userauth3。

如果 Socks5 伺服器是架構為使用者 ID/通行碼形式鑑證方法，而非「挑戰回應鑑證方法」(CRAM)，則 SNK 將不會運作，因為 Socks5 使用者 ID/通行碼通訊協定無法顯示 SNK 盤問。

預設值為 deny。

sechttp

來自安全介面之 HTTP 要求的鑑證方法。有效值為 deny、permit、password、NT、sdi、user、userauth2 及 userauth3。

HTTP 通訊協定不支援 SNK，因為它沒有提供顯示 SNK 盤問的方法給使用者。它支援 SDI，但會提示使用者輸入「通行碼」(而非提示使用者輸入 SDI 通行碼)。使用者應該輸入 SDI 通行碼。

註: fwdfuser 不能在其鑑證方法欄位上設定 SNK 或「防火牆通行碼」。

防火牆通行碼參數**password**

指出是否將提示使用者輸入通行碼。依據預設值，如果指定任何鑑證方法，或預設須輸入通行碼，將給與您提示。

pwdvalue

大部份用於 script 程式設計，此參數容許在命令行上指定參數值。請注意，以清楚的文字輸入這個值，會將此值明確地告知竊聽者。沒有預設值。

userchng

決定要如何在使用者資料庫中設定「管理者變更旗號」。若設定為 yes，則「管理者變更旗號」就會在使用者第一次登入時，要求使用者變更通行碼。預設值為 No。只有在提供 password=yes 及 pwdvalue=" 參數時，此參數才有效。

pwlocked

指定是否要鎖定通行碼。當登入失敗的次數超過限制，或是未使用通行碼的週數達到「停工前的最長時間」所指定的週數時，就會將這個設定設為 yes。

histexpire

定義使用者無法要求通行碼的期間 (週)。這個值是整數字串。有效值為 0 - 52。0 指出未設定任何時間限制。預設值為 0。

histsize

定義使用者無法重新使用的先前通行碼的數目。這個值是整數字串。有效值為 0 - 20。只有在 histexpire=0 的情況下才有效。預設值為 5。

loginretries

定義上次在系統鎖定帳戶之前已順利登入後，所容許的不成功登入嘗試的數目。這個值是整數字串。有效值為 0 - 20。預設值為 10。零或負值指出沒有限制。一旦鎖定使用者的帳戶，使用者將無法登入，直到系統管理者將 pwlocked 設為 no。

maxage

定義通行碼的最長使用期限 (週)。此時，必須變更通行碼。這個值是整數字串。有效值為 0 - 52。0 指出沒有最長壽命。預設值為 13。

maxexpired

定義超出使用者可變更已過期通行碼的 maxage 值 (週) 的最大時間。在這個定義的時間後，僅有管理使用者可變更通行碼。這個值是整數字串。有效值為 -1 - 26。如果 maxexpired 屬性為 0，則在符合 maxage 值時，通行碼即到期。如果 maxage 屬性為 0，將忽略 maxexpired 屬性。預設值為 3。

maxrepeats

定義一個字元可在新通行碼重複的最大次數。有效值為 0 - 8，但值 0 無意義。值 8 指出沒有最大數目。預設值為 2。

minalpha

定義須在新通行碼中的字母字元的最少數目。這個值是整數字串。有效值為 0 - 8。0 指出沒有最少數目。預設值為 4。

mindiff 定義需在新通行碼但不在舊通行碼中的字元的最少數目。這個值是整數字串。有效值為 0 - 8。0 指出沒有最少數目。預設值為 3。

minlen 定義通行碼的最短長度。這個值是整數字串。有效值為 0 - 8。0 指出沒有最少數目。預設值為 8。

minother

定義須在新通行碼中的非字母字元的最少數目。這個值是整數字串。有效值為 0 - 8。0 指出沒有最少數目。預設值為 1。

pwdwarntime

定義一個天數，在這個天數後，系統將發出一個需要通行碼變更的警告。這個值是整數字串。有效值為 0 - 30。零或負值指出不發出任何訊息。預設值為 5。

管理函數群組

fg_all 如果容許這個管理者管理防火牆的所有層面，請輸入 yes。預設值為 no。

fg_dns 如果容許這個管理者管理「領域名稱服務程式」，請輸入 yes。預設值為 no。

fg_interfaces

如果容許這個管理者定義防火牆介面，請輸入 yes。預設值為 no。

fg_logmonitor

如果容許這個管理者管理「日誌監督程式」臨界值，請輸入 yes。預設值為 no。

fg_logs

如果容許這個管理者管理「日誌機能」，請輸入 yes。預設值為 no。

fg_mail

如果可以讓這個管理者管理防火牆郵件閘道，請輸入 yes。預設值為 no。

fg_netobjs1

如果可以讓這個管理者執行「網路物件」的基本管理，請輸入 yes。預設值為 no。

fg_netobjs2

如果可以讓這個管理者執行「網路物件」的進階管理，請輸入 yes。預設值為 no。

fg_pagers

如果可以讓這個管理者管理「呼叫器設置」，請輸入 yes。預設值為 no。

fg_proxyserver

如果可以讓這個管理者架構防火牆 proxy 常駐程式，請輸入 yes。預設值為 no。

fg_traffic

如果容許這個管理者管理「資料傳輸控制」，請輸入 yes。預設值為 no。

fg_user

如果容許這個管理者管理「防火牆使用者」，請輸入 yes。預設值為 no。

若要列示所有防火牆使用者或單一指定的防火牆使用者的所有屬性，請輸入：

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

type={short|long}

如果您使用一個使用者名稱，類型的預設值為 long。如果您未使用使用者名稱，預設值為 short。

若要從防火牆中除去一個使用者，請輸入：

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

第2章 使用報告公用程式

本章將探討如何使用 IBM Firewall 的報告公用程式。報告公用程式的主要目的在於依據防火牆日誌檔，產生管理資訊的表列化檔案。

可產生表列化的檔案，並將這些表格匯入至資料庫系統 (如 DB2/6000 或 DB2/2) 中的表格。然後，管理者就可使用「結構化查詢語言 (SQL)」，來查詢資料並產生報告。公用程式亦容許管理者建立防火牆日誌訊息的可讀取文字檔。

報告公用程式是由下列程式與檔案所構成：

fwlogtxt

依據防火牆日誌檔產生全文字訊息的程式

fwlogtbl

依據防火牆日誌與 su 日誌，產生資料庫匯入檔 (具有 DEL (有區隔字元) 格式) 的程式。

若要使用 fslogtbl 程式及 DDL、DML 與 DEL 檔，您應該具有某些關聯式資料庫的知識，並略懂如何使用適當的關聯式資料庫產品。

fwschema.ddl

「SQL 資料定義語言 (DDL)」陳述式的檔案，適合於定義資料庫表格

fwimport.dat

DB2 匯入陳述式的檔案，適合於將 DEL 檔匯入至資料庫表格中

fwqrysmpl.dml

「SQL 資料操控語言 (DML)」陳述式的檔案，適合於產生報告範例

fwlogcvrt

將 Windows NT 防火牆日誌格式轉換為 AIX 防火牆日誌格式的程式。這可讓其它廠商的報告工具像以前一般地運作，除了可能無法辨識新的訊息。

DDL 與 DML 檔是專供 DB2 系列使用，但可被修改，以便能與其他資料庫管理系統一起使用。DEL 格式檔可穩定地匯入 (載入) 至 DB2/6000、DB2/2 及其他資料庫及檔案系統。必要時，它們的簡單格式應該容許轉換為其他格式。

報告公用程式用法

此資訊將解釋如何從命令行使用報告公用程式如需從架構從屬站使用報告公用程式的相關資訊，請參閱 *IBM eNetwork Firewall 使用指南*。

若要從命令行查看防火牆日誌檔，請使用 **fwlogtxt** 公用程式。相關資訊，請參閱第25頁的『從防火牆日誌檔產生訊息』。

若要依據日誌資訊來產生報告，請：

1. 安裝關聯式資料庫產品。
2. 建立空的資料庫。
3. 在資料庫中建立空的防火牆日誌表格。
4. 欲產生製表檔，請從命令行執行 **fwlogtbl**。
5. 匯入結果檔案，將日誌資料移入資料庫表格中。
6. 經由執行 SQL 陳述式或 SQL 程式來產生報告。

註：前三個步驟只需要執行一次，然後，每一次有新的日誌資料可使用時，將重複其餘步驟。

IBM Firewall 日誌格式

防火牆日誌檔的每一個項目均具有如下格式：

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

其中

- 前三個欄位 **date**、**time** 與 **firewall-name** 是由防火牆日誌機能所新增。
- **year** 是四個字元的年。
- **pid** 是項目將套用的緒 ID。
- **Amsg_num** 是一個循序整數，「報告公用程式」將使用它，從 `fw_log.cat` 檔中存取適當、已轉換的訊息文字。而以數字表示的 `msg_num` 前面會有一個日誌層次指示器字母 (A)。這個指示器會分辨出產生日誌的平台，以及各種日誌格式的任何差異。
- **msg_ID** 是訊息的外部號碼 (如 ICA0001e)。
- **var_1-n** 代表訊息變數的值，其中 **n** 即是訊息定義中的變數數目。

註：不要將其他記錄引導至與防火牆日誌相同的檔案。因為這種記錄不遵守報告公用程式所需的格式，而產生無法預測的結果。

請使用命令 `fwlogcvrt` 將這個 Windows NT 版本日誌格式轉換成 AIX 日誌格式。您可能需要這樣處理，才能使用其他支援 IBM Firewall for AIX 日誌的廠商報告工具。這類轉換會移除出現在 `msg_num` 前面的 'A' 日誌層次指示器，並將兩個空白字元插入到 `firewall_name` 及年份間之冒號的兩邊。

參數包括：

input 從 Windows NT Firewall 日誌重新導向的標準輸入。

output 標準輸出，可重新導向至檔案。

fwlogcvrt 語法

fwlogcvrt

範例：

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

從防火牆日誌檔產生訊息

您可以使用命令 **fwlogtxt**，從防火牆日誌檔的項目中建立可讀取的訊息。

參數包括：

input 來自防火牆日誌檔的標準輸入

output 標準輸出

fwlogtxt 語法

fwlogtxt

範例：

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

沒有 fwlogtxt 的參數；它採用標準輸入的資訊，並將結果放至標準輸出中。

產生資料庫匯入檔

您可以使用命令 **fwlogtbl**，來建立、改寫或附加表列化檔案，然後從其中移出資料庫表格來產生報告。

參數包括：

input 防火牆日誌檔。

output 檔案名稱：

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

fwlogtbl 語法

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

範例：

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

- w** 指定應該置換現存的輸出檔。如果檔案不存在，fwlogtbl 將建立它。
- a** 指定所產生的檔案應該附加至現存的輸出檔中。如果檔案不存在，fwlogtbl 將建立它。
- d** 識別輸出目錄。
- OutDir** 指定將儲存輸出檔的目錄。如果未指定任何目錄，輸出檔將儲存在現行目錄中。
- su** 指定 LogName 為 AIX su 日誌檔的名稱。這樣，您的 Windows NT Firewall 就可以處理先前舊版之 AIX Firewall 的防火牆及 su 日誌檔。

LogName

指定防火牆日誌檔或 AIX su 日誌檔。

雖然輸出檔是預先定義的，但在執行 fwlogtbl 後，可對它進行複製或更名。輸出檔案的格式為具有區隔字元的 ASCII (DEL) 檔案格式，沒有字串區隔字元，而是以分號 (;) 作為直欄的區隔字元。

關於訊息的詳細資訊，請參閱第75頁的『附錄A. 訊息』。

透過報告公用程式使用資料庫

本段將描述與防火牆一起提供的檔案，這些檔案將用來建立資料庫、將資訊匯入資料庫，以及查詢報告。如果您有 DB2，db2 這個命令可以用在這些檔案上。(類似於 db2 命令的功能可能存在於其他資料庫管理系統中。這些檔案可能需要變更，方可與如此的功能一起使用。)

若要執行 db2 命令，您必須安裝 DB2，並定義一個「案例」。請參閱 DB2 安裝手冊。首先，您必須使用 DB2 的建立資料庫命令，來建立一個空的資料庫。(建議您將它命名為 'fwlog')。若要執行這個動作，請在命令行上輸入如下的命令：

```
db2cmd
```

然後在 DB2 命令結果視窗中輸入：

```
db2 create database fwlog
```

然後，您必須連接至 fwlog 資料庫：

```
db2 connect to fwlog
```

db2 命令的 -vf 選項的使用方式如下：

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

下列各段將有這些步驟的詳細說明。在任何情況下，使用者應該仔細檢查標準輸出 (在每一個範例中，已重新導向至檔案)。對匯入作業而言，同時也需要檢查每一個個別匯入陳述式所產生的 .msg 檔。

建立表格

db2 -vf fwschema.ddl > schema.out 這個命令會建立所有必須的表格及索引。最好是在安裝防火牆不久之後，發出這個命令一次。當這個範例正在執行時所用的現行使用者 ID 將是表格的建立者 ID。在稍後的 SQL 陳述式中，這個 ID 可能需要作為表格名稱的限定元 (如 creatorid.tableName)，除非它們正在建立者 ID 下執行。因此，如果未使用建立者的 ID，則使用者將需要編輯 fwimport.dat 與 fwqrysmp.dml 檔，以便將建立者 ID 置於每一個表格名稱之前。

ROOTDIR\sample\report\fwschema.ddl 含有可建立資料庫表格的 DDL 陳述式，有了這些資料庫表格，就可以接受來自 fwlogtbl 所建立的表列化檔案的記錄。ROOTDIR 為您在進行安裝作業時，所選定的 IBM Firewall 目標位置目錄。您應該查閱 schema.out，以判斷您的作業是否順利。fwschema.ddl 檔案中的陳述式可按原狀使用，或略作修改以適用於不同資料庫系統。(使用者不應該變更表格與直欄名稱。)

匯入資料

db2 -vf fwimport.dat > import.out 這個命令會將資料從所有 DEL 檔案載入至 **db2-vf fwschema.ddl** 命令所建立的表格中。

ROOTDIR\sample\report\fwimport.dat 檔案含有範例陳述式，它會將 *.tbl 檔的資料匯入至 DB2 資料庫。如 第27頁的『建立表格』所提一般，如果匯入的使用者不是表格的建立者，則建立者 ID 必須置於每一個表格名稱之前。

每一個匯入陳述式將在標準輸出中產出資訊，而在 tblname.msg 檔中產生其他資訊，其中 tblname 對於每一個匯入陳述式而言將是特定的。使用者應該檢查這兩種輸出格式，來判斷是否順利完成匯入。當透過如 DB2 的程式，執行這個檔案中的所有匯入陳述式時，使用者應該將標準輸出引導至檔案，然後檢查該檔案與每一個 .msg 檔。每一個匯入命令均會產生個別的 .msg 檔。此外，每當它們有新日誌將反映在資料庫時，使用者應該重新發出 **db2 -vf fwimport.dat > import.out** 命令。

當匯入大日誌檔時，您可能會收到 SQL 錯誤號碼，其說明指出需要更多的記憶體或磁碟空間。例如，訊息可能是「資料堆空間或異動日誌空間不足」。這些錯誤需要調整資料庫產品或 fwlog 資料庫的參數設定。請參閱 DB2 文件，取得詳細資訊。另一種調整 DB2 參數設定的暫代方式就是將大的日誌或大的表列化檔案分成較小的檔案。

執行範例查詢

db2 -vf fwqrysmp.dml > report.out 命令會執行範例查詢。ROOTDIR:\sample\report\fwqrysmp.dml 檔案含有 SQL 陳述式範例，它可依據某些查詢需求，提供有用的報告資料。您可以使用這些範例來建立您自己的報告。如 第27頁的『建立表格』所提一般，如果匯入的使用者不是表格的建立者，則建立者 ID 必須置於每一個表格名稱之前。

當從命令行中執行查詢時，DB2 將配置它可能對每一個輸出直欄需要的最大空間。這可能會造成不易閱讀的報告。您可以透過在每一個查詢中要求更少的直欄，或透過將這些查詢陳述式內含在您可以更容易控制呈現方式的程式內，來達成更滿意的結果。

報告公用程式的使用者介面

「報告公用程式」將安裝為防火牆安裝的一部份。它們也可以個別安裝，並在非防火牆主電腦上執行。架構從屬站或 fwlogtbl 命令可用來在防火牆上執行報告公用程式。在非防火牆上，請使用命令行。

SQL 表格

本段將定義 SQL 表格的佈置。

每一個防火牆日誌訊息或 AIX su 日誌訊息都將對映到下列其中一個 SQL 表格：

```
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
```

您不應該變更表格與直欄名稱。然而，如果您發現它的某些值被截斷的話，您可以增加字元直欄的寬度。

索引

代表特殊防火牆事件的日誌記錄應該僅在資料庫中出現一次。如果管理者多次匯入同一個表列化檔案，或如果匯入從同一個日誌檔案衍生出來的另一個表列化檔案，則一個日誌記錄可能出現多次。

若要避免這個問題，資料庫定義範例檔案 (fwschema.dll) 將使用這三個欄位，在每一個表格上定義一個唯一索引：

- 為這個記錄的來源的日誌檔的檔案名稱 (LOG_FILE)
- 這個記錄在該日誌檔中的行號 (LINE_NUM)
- 這個字行的重複次數，是依據系統日誌的「上一個訊息已重複 n 次」訊息 (REPEAT_NUM) 而來

這個索引可阻止您從相同名稱的檔案中載入相同行號多次。這個措施加上小心管理您的日誌檔名稱，應可避免在您的資料庫中重複出現日誌事件。

將其他索引加至您的資料庫可加強您最常用查詢的效能。請參閱您的資料庫文件，取得詳細資訊。

表格說明

本段將使防火牆日誌訊息對映至表格與直欄，並指向您想要查詢作為您的報告的資訊。將對映至特殊表格的所有訊息將列示在表格尾端的附註中。提供資料給特殊直欄的訊息將列示在該直欄的說明。這些表格中含有 IBM Firewall for AIX 及 IBM Firewall for NT 的個別訊息，以及這兩個防火牆共用的訊息。

關於防火牆日誌訊息的詳細資訊，請參閱第75頁的『附錄A. 訊息』。

在下列說明的「資料類型」直欄中，'int' 暗指 DB2 的 SMALLINT 直欄類型；'long int' 暗指 DB2 INTEGER 類型。「日期時間」資料類型暗指 DB2 TIMESTAMP。在時間標記中，微秒值將恆為 "000000"。

如果說明標示為必要，必須指定一個值，方可在表格中輸入記錄。

在這些表格說明中，將省略充當唯一索引的三個直欄以及接收日誌層次指示器的直欄，因為它們的定義相同，且通常沒有理由查詢它們。

表 1. ADMIN_ALERT. 這個表格含有與來自 a_alert.tbl 檔的侵入警示有關的訊息。

直欄	資料類型	簡短說明
DATE_TIME	date_time	動作的日期與時間 (必要)
FIREWALL	char(100)	防火牆機器的完整名稱 (必要)
PID	int	AIX 處理 ID、NT 緒 ID (必要)
MSG_NUM	int	訊息號碼 (必要)
USERID	char(16)	使用者 ID (ICA0001、ICA0002、ICA0003、ICA0004、ICA2001、ICA2002、ICA2003、ICA2026、ICA2043、ICA2068、ICA2167、ICA2168、ICA 2170、ICA2173、ICA3001、ICA3012、ICA3018)
ACTION	char(7)	連線 (ICA3012) 或連結 (ICA3018)
NUM_COUNT	int	鑑證失敗數目 (ICA0001、ICA0002、ICA0003)；TAG_MSG_NUM 的日誌項目數目 (ICA0004)；天數 (ICA9000)
TAG_MSG_NUM	char(8)	標示訊息號碼 (ICA0004)
SRC_IP	char(15)	來源 IP 位址 (ICA2001、ICA2028、ICA2079、ICA2167、ICA3012、ICA3018)
DST_IP	char(15)	目的地 IP 位址 (ICA2028、ICA2079、ICA3012、ICA3018)

表 1. *ADMIN_ALERT* (繼續). 這個表格含有與來自 *a_alert.tbl* 檔的侵入警示有關的訊息。

直欄	資料類型	簡短說明
AUTH_METHOD	char(20)	鑑證方法 (ICA2002、ICA2167、ICA2170)
NETWORK	char(25)	網路名稱 (ICA2001、ICA2002、ICA2167)
HOST_NAME	char(100)	主電腦名稱 (ICA0003、ICA2002)
TIMEOUT_SEC	int	逾時秒數 (ICA2026)
CONN_USERID	char(16)	Socks 連線使用者名稱 (ICA3001)
APPLICATION	char(30)	應用程式名稱如 telnet、ftp、... (ICA2167、ICA2168、ICA2170、ICA3012)
註: 相關訊息: 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		

表 2. *FILTER_ACTIVE_RULE*. 本表格含有來自 *f_rule.tbl* 檔的現行「過濾器」規則。

直欄	資料類型	簡短說明
DATE_TIME	date_time	動作的日期與時間 (必要)
FIREWALL	char(100)	防火牆機器的完整名稱 (必要)
PID	int	AIX 處理 ID、NT 緒 ID (必要)
MSG_NUM	int	訊息號碼 (必要)
RULE_NUM	int	規則號碼 (必要)
RULE	char(150)	規則 (必要)
註: 相關訊息: ICA1037		

表 3. *FILTER_INFO*. 本表格含有與來自 *f_info.tbl* 檔的「過濾器」有關的錯誤或一般資訊訊息。

直欄	資料類型	簡短說明
DATE_TIME	date_time	動作的日期與時間 (必要)
FIREWALL	char(100)	防火牆機器的完整名稱 (必要)
PID	int	AIX 處理 ID、NT 緒 ID (必要)
MSG_NUM	int	訊息號碼 (必要)
RULE_NUM	int	過濾規則號碼 (ICA1005)

表 3. *FILTER_INFO* (繼續). 本表格含有與來自 *f_info.tbl* 檔的「過濾器」有關的錯誤或一般資訊訊息。

直欄	資料類型	簡短說明
ERROR_NUM	int	系統錯誤號碼 -- AIX 錯誤號碼或 Windows NT 最後一個錯誤 (ICA1007, ICA1008, ICA1009, ICA1011 ICA1013, ICA1015, ICA1021, ICA1023, ICA1024) 對應於這個錯誤號碼的文字可透過 <code>_strerror</code> 函數來取得。 「Windows NT 最後一個錯誤」的文字可透過「格式訊息」功能，或在 Win32 Programmer's Reference Volume 2 的 Appendix A 中取得。
LOAD_PATH	char(100)	核心程式擴充載入路徑 (ICA1011、ICA1012)
DVC_DRV	char(25)	裝置驅動程式 (ICA1021)
TERM_SIG	char(25)	終止信號 (ICA1260)
FILE_NAME	char(100)	檔案名稱 (ICA1024)
RC	int	內部防火牆回覆碼 (ICA1019)
註: 相關訊息: ICA1001 ICA1002 ICA1003 ICA1005 ICA1007 ICA1008 ICA1009 ICA1011 ICA1012 ICA1013 ICA1014 ICA1015 ICA1016 ICA1017 ICA1019 ICA1021 ICA1022 ICA1023 ICA1024 ICA1200 ICA1260		

表 4. *FILTER_MATCH*. 這個表格含有來自 *f_match.tbl* 檔的相符過濾規則。

直欄	資料類型	簡短說明
DATE_TIME	date_time	動作的日期與時間 (必要)
FIREWALL	char(100)	防火牆機器的完整名稱 (必要)
PID	int	AIX 處理 ID、NT 緒 ID (必要)
MSG_NUM	int	訊息號碼 (必要)
RULE_NUM	int	規則號碼 (必要)
ACTION	char(6)	規則類型: 容許、拒絕等。
DIRECTION	char(8)	封包的傳送方向為入埠或離埠 (必要的)
SRC_IP	char(15)	傳送者的 IP 位址 (必要)
DST_IP	char(15)	收件者的 IP 位址 (必要)
PROTOCOL	char(7)	高階通訊協定如 UDP、IP、ICMP、TCP 或 TCP/ACK (必要)
SRC_PORT	int	<ul style="list-style-type: none"> ICMP 的 IP 封包類型 其他的資源通訊協定埠號 (必要的)
DST_PORT	int	<ul style="list-style-type: none"> ICMP 的 IP 封包碼 其他的目的地通訊協定埠號 (必要的)
ROUTING	char(5)	封包的遞送範圍: 遞送或區域 (必要)
INTERFACE	char(10)	介面類型: 安全或非安全性 (必要)

表 4. *FILTER_MATCH* (繼續). 這個表格含有來自 *f_match.tbl* 檔的相符過濾規則。

直欄	資料類型	簡短說明
FRAGMENT	char(8)	識別封包為片段或非片段 (必要)
TUNNEL_ID	int	通道 ID (必要)
ENCRYPTION	char(7)	加密演算法：DES_CBC 或 CDMF 或無
BYTES	long int	特定封包的長度 (必要)
註：相關訊息：ICA1036		

表 5. *FILTER_STATUS*. 這個表格含有關於來自 *f_stat.tbl* 檔的過濾器的狀態變更的資訊。

直欄	資料類型	簡短說明
DATE_TIME	date_time	動作的日期與時間 (必要)
FIREWALL	char(100)	防火牆機器的完整名稱 (必要)
PID	int	AIX 處理 ID、NT 緒 ID (必要)
MSG_NUM	int	訊息號碼 (必要)
DAEMON	char(25)	AIX 過濾記載常駐程式 (ICA1004)，或 Windows NT 過濾記載服務程式。
VERSION	int	版本號碼 (ICA1004、ICA1033)
RELEASE	int	版次號碼 (ICA1004、ICA1033)
PACKET_LOGGING	char(8)	啟用或停用封包記載的狀態 (ICA1035)
註：相關訊息：ICA1004 ICA1032 ICA1033 ICA1034 ICA1035。過濾規則更新 (ICA1032) 的明細可從 FILTER_ACTIVE_RULE 表格中取得。		

表 6. *INTERFACES*. 此表格包含 *interface.tbl* 檔案中的介面 (配接卡) 架構訊息資訊。

直欄	資料類型	簡短說明
DATE_TIME	date_time	動作的日期與時間 (必要)
FIREWALL	char(100)	防火牆機器的完整名稱 (必要)
PID	int	AIX 處理 ID、NT 緒 ID (必要)
MSG_NUM	int	訊息號碼 (必要)
IP	char(15)	配接卡的 IP 位址 (ICA9038、ICA9039、ICA9040)
OLD_MASK	char(15)	先前的遮罩值 (ICA9040)
NEW_MASK	char(15)	新的遮罩值 (ICA9040)
註：相關訊息：ICA9037、ICA9038、ICA9039、ICA9040、ICA9041		

表 7. *NAT_INFO*. 本表格含有來自 *nat_info.tbl* 檔的「網路位址轉換」訊息資訊。

直欄	資料類型	簡短說明
DATE_TIME	date_time	動作的日期與時間 (必要)
FIREWALL	char(100)	防火牆機器的完整名稱 (必要)

表 7. NAT_INFO (繼續). 本表格含有來自 nat_info.tbl 檔的「網路位址轉換」訊息資訊。

直欄	資料類型	簡短說明
PID	int	AIX 處理 ID、NT 緒 ID (必要)
MSG_NUM	int	訊息號碼 (必要)
VERSION	int	NAT 版本號碼 (ICA9033)
RELEASE	int	NAT 版次號碼 (ICA9033)
IP	char(15)	IP 位址 (ICA9035、ICA9036)
註: 相關訊息: ICA9032、ICA9033、ICA9034、ICA9035、ICA9036		

表 8. PAGER_INFO. 本表格含有與 Firewall 的呼叫功能有關的資訊 (來自 pgr_info.tbl 檔)。

直欄	資料類型	簡短說明
DATE_TIME	date_time	動作的日期與時間 (必要)
FIREWALL	char(100)	防火牆機器的完整名稱 (必要)
PID	int	AIX 處理 ID、NT 緒 ID (必要)
MSG_NUM	int	訊息號碼 (必要)
USERID	char(16)	使用者 ID (ICA4036、ICA4174、ICA4175)
ERROR_NUM	int	系統錯誤號碼 - AIX 錯誤號碼或 Windows NT 最後一個錯誤 (ICA4371)
PROGRAM	char(25)	程式名稱 (ICA4000)
SIGNAL	int	終止信號 (ICA4000)
ID	int	識別碼 (ICA4036)
PRIORITY	int	優先順序 (ICA4036)
PERIOD	int	時期 (ICA4036)
RETRY_COUNT	int	重試次數 (ICA4036、ICA4313、ICA4314、ICA4364、ICA4365)
FROM_ENTRY	char(15)	函數名稱 (ICA4036)
HOST_NAME	char(100)	主電腦名稱 (ICA4174、ICA4175)
MESSAGE_TEXT	char(250)	頁面的文字 (ICA4036、ICA4353 - 4360、ICA4368、ICA4372)
SERVICE	char(25)	服務程式名稱 (ICA4017)
SOCKET	int	Socket 號碼 (ICA4017)
FILENAME	char(100)	檔案名稱 (ICA4154、ICA4351、ICA4352)
註: 相關訊息: ICA4000 ICA4001 ICA4007 ICA4017 ICA4036 ICA4154 ICA4168 ICA4174 ICA4175、ICA4300 - 4303、ICA4305 - 4315、ICA4351 - 4360、ICA4362 - 4372)		

表 9. *PROXY_FTP*. 這個表格含有來自 *p_fip.tbl* 檔的 *FTP* 階段作業的 *FTP* 動作資訊。

直欄	資料類型	簡短說明
DATE_TIME	date_time	動作的日期與時間 (必要)
FIREWALL	char(100)	防火牆機器的完整名稱 (必要)
PID	int	AIX 處理 ID、NT 緒 ID (必要)
MSG_NUM	int	訊息號碼 (必要)
USERID	char(16)	使用者 ID (必要)
SRC_IP	char(15)	使用者的 IP 位址 (必要)
DST_IP	char(15)	遠端機器的 IP 位址 (必要)
ACTION	char(5)	檔案轉送動作：存放或取得 (必要)
FILE_NAME	char(100)	檔案名稱
BYTES	long int	資料的轉送數量
SID	long int	唯一階段作業 ID (必要)
註：相關訊息：ICA2075		

表 10. *PROXY_HTTP*. 本表格含有來自 *p_http.tbl* 檔的 *Proxy* 階段作業的 *HTTP* 動作資訊。

直欄	資料類型	簡短說明
DATE_TIME	date_time	動作的日期與時間 (必要)
FIREWALL	char(100)	防火牆機器的完整名稱 (必要)
PID	int	AIX 處理 ID、NT 緒 ID (必要)
MSG_NUM	int	訊息號碼 (必要)
STATUS	int	狀態 (必要)
SRC_IP	char(15)	使用者的 IP 位址 (必要)
REQUEST	char(250)	HTTP 要求的內容 (必要)
BYTES	long int	資料的轉送數量。
註：相關訊息：ICA2099		

表 11. *PROXY_INFO*. 本表格含有與來自 *p_info.tbl* 檔的 *Proxy* 有關的錯誤或一般資訊訊息。

直欄	資料類型	簡短說明
DATE_TIME	date_time	動作的日期與時間 (必要)
FIREWALL	char(100)	防火牆機器的完整名稱 (必要)
PID	int	AIX 處理 ID、NT 緒 ID (必要)
MSG_NUM	int	訊息號碼 (必要)
USERID	char(16)	使用者 ID (ICA2018、ICA2019、ICA2057、ICA2058、ICA2166、ICA2177、ICA2172)

表 11. *PROXY_INFO* (繼續). 本表格含有與來自 *p_info.tbl* 檔的 *Proxy* 有關的錯誤或一般資訊訊息。

直欄	資料類型	簡短說明
ERROR_NUM	int	系統錯誤號碼 - AIX 錯誤號碼或 Windows NT 最後一個錯誤 (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) 錯誤號碼的文字 (AIX 系統錯誤) 可透過 <code>_strerror</code> 函數來取得。「Windows NT 最後一個錯誤」的文字可透過「格式訊息」功能，或在 Win32 Programmer's Reference Volume 2 的 Appendix A 中取得。
OPTION_VAL	char(20)	選項旗標或參數值 (ICA2014、ICA2015、ICA2049、ICA2050)
TIME	char(15)	無效的時間間隔 (ICA2044、ICA2202)
RC	int	內部防火牆回覆碼 (ICA2007、ICA2030、ICA2031、ICA2033、ICA2034、ICA2054、ICA2057、ICA2058、ICA2065、ICA2120、ICA2166、ICA2203)
INVOC_NAME	char(20)	發生系統錯誤時 socket 或連接埠的呼叫名稱 (ICA2055、ICA2056)
AUDIT_TYPE	char(7)	不明審核類型 (7 個十六進位數字) (ICA2004)
HOST_NAME	char(100)	主電腦名稱 (ICA2106、ICA2107、ICA2126)
FILE_NAME	char(100)	檔案名稱 (ICA2029、ICA2030、ICA2072、ICA2183、ICA2204、ICA2205、ICA2206、ICA2207)
LINE_NUM	int	行號 (ICA2029、ICA2030)
PROTOCOL	char(25)	無效通訊協定名稱 (ICA2112、ICA2116)
CUSTOMIZED_ATTR	char(25)	行號 (ICA2105、ICA2106、ICA2125、ICA2166)
ODM_ERR_NUM	int	來自「物件資料管理系統」的錯誤號碼 (ICA2102、ICA2103、ICA2104、ICA2105、ICA2107、ICA2108、ICA2109、ICA2125)
APPLICATION (僅限 NT)	char(30)	應用程式名稱 (ICA2200、ICA2201、ICA2202、ICA2203、ICA2204、ICA2205、ICA2206、ICA2207)

表 11. *PROXY_INFO* (繼續). 本表格含有與來自 *p_info.tbl* 檔的 *Proxy* 有關的錯誤或一般資訊訊息。

直欄	資料類型	簡短說明
CALLER (僅限 NT)	char(25)	呼叫函數 (ICA2200、ICA2201、ICA2202、ICA2203、ICA2204、ICA2205、ICA2206、ICA2207)
FAILED_IN (僅限 NT)	char(25)	失敗函數 (ICA2201、ICA2203)
註: 相關訊息: 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		

表 12. *PROXY_LOGIN*. 本表格含有關於來自 *p_login.tbl* 檔的順利 *Proxy* 登入的資訊 (主要關於鑑證)。

直欄	資料類型	簡短說明
DATE_TIME	date_time	動作的日期與時間 (必要)
FIREWALL	char(100)	防火牆機器的完整名稱 (必要)
PID	int	AIX 處理 ID、NT 緒 ID (必要)
MSG_NUM	int	訊息號碼 (必要)
USERID	char(16)	使用者 ID (必要)
APPLICATION	char(30)	應用程式名稱 - telnet、ftp、.... (必要)
AUTH_METHOD	char(15)	鑑證方法 (必要)
NETWORK	char(25)	網路 (安全/非安全 -也可能具有其他資訊) (必要)
HOST_NAME	char(100)	主電腦名稱 (必要)
註: 相關訊息: ICA2024 ICA2025 ICA2169		

表 13. *PROXY_STATUS*. 本表格含有來自 *p_stat.tbl* 檔的 *PROXY* 狀態資訊。

直欄	資料類型	簡短說明
DATE_TIME	date_time	動作的日期與時間 (必要)
FIREWALL	char(100)	防火牆機器的完整名稱 (必要)
PID	int	AIX 處理 ID、NT 緒 ID (必要)
MSG_NUM	int	訊息號碼 (必要)
USERID	char(16)	使用者 ID (ICA2008、ICA2016、ICA2021)
SRC_IP	char(15)	來源 IP 位址 (ICA2000、ICA2008、ICA2010、ICA2011、ICA2012、ICA2013、ICA2141、ICA2180)

表 13. *PROXY_STATUS* (繼續). 本表格含有來自 *p_stat.tbl* 檔的 *PROXY* 狀態資訊。

直欄	資料類型	簡短說明
DST_IP	char(15)	目的地 IP 位址 (ICA2000、ICA2010、ICA2011、ICA2012、ICA2013)
REMOTE_HOST	char(100)	遠端主電腦名稱 (從防火牆機器的觀點來看) (ICA2021、ICA2022、ICA2027)
SID (僅限 NT)	int	階段作業識別碼 (ICA2177、ICA2180、ICA2181 ICA2182)
SOCKET (僅限 NT)	char(25)	Socket 名稱 (ICA2177)
RC (僅限 NT)	int	回覆碼或原因碼 (ICA2181、ICA2182)
CMD (僅限 NT)	char(36)	SMTP 卡 (ICA2182)
註: 相關訊息: ICA2000 ICA2010 ICA2011 ICA2012 ICA2013 ICA2016 ICA2021 ICA2022 ICA2027 ICA2097 ICA2098 ICA2141 ICA2163 ICA2164 ICA2165 ICA2177 ICA2180 ICA2181 ICA2182		

表 14. *SERVER_INFO*. 本表格含有關於來自 *srv_info.tbl* 檔的「架構伺服器」狀態與活動的資訊。

直欄	資料類型	簡短說明
DATE_TIME	date_time	動作的日期與時間 (必要)
FIREWALL	char(100)	防火牆機器的完整名稱 (必要)
PID	int	AIX 處理 ID、NT 緒 ID (必要)
MSG_NUM	int	訊息號碼 (必要)
USERID	char(16)	使用者 ID (ICA9003、ICA9004)
ERROR_NUM	int	系統錯誤號碼 - AIX 錯誤號碼或 Windows NT 最後一個錯誤 (ICA9008、ICA9009) 錯誤號碼的文字 (AIX 系統錯誤) 可透過 <code>strerror</code> 函數來取得。「Windows NT 最後一個錯誤」的文字可透過「格式訊息」功能,或在 Win32 Programmer's Reference Volume 2 的 Appendix A 中取得。
註: 相關訊息: ICA9003 ICA9004 ICA9005 ICA9006 ICA9007 ICA9008 ICA9009 ICA9010 ICA9011 ICA9012 ICA9013 ICA9014 ICA9015		

表 15. *SESSION*. 這個表格含有來自 *session.tbl* 檔的 *SOCKS* 與 *PROXY* 階段作業啟動/停止資訊。

直欄	資料類型 (長度)	簡短說明
DATE_TIME	date_time	動作的日期與時間 (必要)
FIREWALL	char(100)	防火牆機器的完整名稱 (必要)
PID	int	AIX AIX 處理 ID、NT 緒 ID、NT 緒 ID (必要)
MSG_NUM	int	訊息號碼 (必要)
USERID	char(16)	使用者 ID (必要)
SERVICE_TYPE	char(10)	服務程式類型: socks 或 proxy (必要)

表 15. *SESSION* (繼續). 這個表格含有來自 *session.tbl* 檔的 *SOCKS* 與 *PROXY* 階段作業啟動/停止資訊。

直欄	資料類型 (長度)	簡短說明
APPLICATION	char(30)	應用程式名稱 - telnet、ftp、.... (必要)
SRC_IP	char(15)	使用者的 IP 位址 (必要)
DST_IP	char(15)	遠端機器的 IP 位址 (必要)
SESSION_EVENT	char(5)	<ul style="list-style-type: none"> 當建立階段作業時開始。 當終止階段作業時結束 (必要)
BYTES	long int	在階段作業期間已轉送的資料數量。若應用程式為 Telnet，此值應為 0。
SID	long int	「防火牆」所產生的唯一階段作業識別碼，以時間為基礎。
註: 相關訊息： <ul style="list-style-type: none"> Safemail 階段作業啟動：ICA2178 Safemail 階段作業停止：ICA2179 Socks 階段作業啟動：ICA3011 Socks 階段作業停止：ICA3015 Proxy Telnet 階段作業啟動：ICA2036 (AIX 日誌) ICA2208、ICA2218 (NT 日誌) Proxy Telnet 階段作業停止：ICA2077 (AIX 日誌) ICA2209、ICA2219 (NT 日誌) Proxy FTP 階段作業啟動：ICA2041 (AIX 日誌) ICA2208、ICA2218 (NT 日誌) Proxy FTP 階段作業停止：ICA2076 (AIX 及 NT 日誌) Socks FTP 階段作業動作的明細位在 SOCKS_FTP 表格中。 Proxy FTP 階段作業動作的明細位在 PROXY_FTP 中。		

表 16. *SOCKS_FTP*. 本表格含有來自 *sftp.tbl* 檔的 *FTP* 階段作業的 *SOCKS FTP* 動作資訊。

直欄	資料類型	簡短說明
DATE_TIME	date_time	動作的日期與時間 (必要)
FIREWALL	char(100)	防火牆機器的完整名稱 (必要)
PID	int	AIX AIX 處理 ID、NT 緒 ID (必要)
MSG_NUM	int	訊息號碼 (必要)
USERID	char(16)	使用者 ID (必要)
SRC_IP	char(15)	使用者的 IP 位址 (必要)
DST_IP	char(15)	遠端機器的 IP 位址 (必要)

表 16. *SOCKS_FTP* (繼續). 本表格含有來自 *s_ftp.tbl* 檔的 *FTP* 階段作業的 *SOCKS FTP* 動作資訊。

直欄	資料類型	簡短說明
DATA_BIND	char(5)	<ul style="list-style-type: none"> 當建立資料連結時 '啟動'。(ICA3010) 當終止資料連結時 '停止'。(ICA3014) (必要)
BYTES	long int	資料的轉送數量。
註: 相關訊息: ICA3010 ICA3014		

表 17. *SOCKS_INFO*. 本表格含有與來自 *s_info.tbl* 檔的 *Socks* 有關的錯誤或一般資訊訊息。

直欄	資料類型	簡短說明
DATE_TIME	date_time	動作的日期與時間 (必要)
FIREWALL	char(100)	防火牆機器的完整名稱 (必要)
PID	int	AIX 處理 ID、NT 緒 ID (必要)
MSG_NUM	int	訊息號碼 (必要)
USERID	char(16)	使用者 ID (ICA3044、ICA3045、ICA3046、ICA3047、ICA3049)
ACTION	char(7)	連線 (ICA3044、ICA3049) 或 連結 (ICA3046、ICA3047)
ERROR_NUM	int	系統錯誤號碼 - AIX 錯誤號碼 (ICA3013、ICA3019、ICA3031、ICA3032、ICA3040、ICA3044、ICA3101、ICA3102、ICA3103、ICA3104、ICA3106、ICA3107、ICA3108、ICA3122、ICA3124、ICA3125、ICA3126、ICA3128)
SRC_HOST	char(25)	來源主電腦名稱 (ICA3019、ICA3035)
DST_HOST	char(25)	目的地主電腦名稱 (ICA3016、ICA3045)
SRC_IP	char(15)	來源位址 (ICA3042、ICA3043、ICA3044、ICA3045、ICA3046、ICA3047、ICA3049)
DST_IP	char(15)	目的地位址 (ICA3044、ICA3045、ICA3046、ICA3047、ICA3049)
LINE_NUM	int	行號 (ICA3022、ICA3023、ICA3024、ICA3025、ICA3026、ICA3109、ICA3110、ICA3111、ICA3112、ICA3115、ICA3116、ICA3117、ICA3118、ICA3119、ICA3120); 或行數 (ICA3113)
EXEC_STATUS	int	執行狀態 (ICA3027)

表 17. *SOCKS_INFO* (繼續). 本表格含有與來自 *s_info.tbl* 檔的 *Socks* 有關的錯誤或一般資訊訊息。

直欄	資料類型	簡短說明
CMD	char(36)	如登入的命令 (ICA3027、ICA3039、ICA3042、ICA3044、ICA3048) 附註：對 ICA3042 而言，命令的格式為十六進位格式
FILE_NAME	char(100)	檔案名稱 (ICA3030、ICA3032、ICA3105、ICA3109、ICA3110、ICA3111、ICA3112、ICA3113、ICA3114、ICA3115、ICA3116、ICA3117、ICA3118、ICA3119、ICA3120)
APPLICATION	char(30)	應用程式名稱 - telnet、ftp、.... (ICA3044、ICA3045、ICA3049)
VERSION	char(10)	以十六進位表示的 Socks 版本號碼 (ICA3043)
註：相關訊息：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		

表 18. *SSL_INFO*. 本表格含有關於來自 *ssl_info.tbl* 檔的 *SSL* 狀態與活動的資訊。

直欄	資料類型	簡短說明
DATE_TIME	date_time	動作的日期與時間 (必要)
FIREWALL	char(100)	防火牆機器的完整名稱 (必要)
PID	int	AIX 處理 ID、NT 緒 ID (必要)
MSG_NUM	int	訊息號碼 (必要)
Client_IP	char(15)	從屬站的 IP 位址
註：相關訊息：ICA5015 ICA5022 ICA5023 ICA5028 ICA5029 ICA5036 ICA5039 ICA5060 ICA5063 ICA5082 ICA5120		

表 19. *SU*. 本表格含有關於 *su.tbl* 檔的 *SU* 活動的明細 (如果您正在載入 AIX *su* 日誌)。

直欄	資料類型	簡短說明
DATE_TIME	date_time	動作的日期與時間 (必要) 因為 AIX 不會在 <i>su</i> 日誌檔中記錄年，DATE_TIME 直欄的年部份將設定為今年或前一年，視月/日設定而定 (如果月/日晚於現行月/日，將假定它是上一年。)
FROM_USERID	char(16)	使用者 ID (必要)
TO_USERID	char(16)	使用者 ID (必要)
LOGIN_STATUS	char(7)	登入嘗試的狀態：成功或失敗 (必要)

表 20. *TUNNEL_CONTEXT*. 本表格含有來自 *t_cntxt.tbl* 檔的現行「通道範圍」設定。

直欄	資料類型	簡短說明
DATE_TIME	date_time	動作的日期與時間 (必要)
FIREWALL	char(100)	防火牆機器的完整名稱 (必要)
PID	int	AIX 處理 ID、NT 緒 ID (必要)
MSG_NUM	int	訊息號碼 (必要)
TUNNEL_ID	long int	通道 ID (必要)
SRC_IP	char(15)	來源 IP 位址 (必要)
DST_IP	char(15)	目的地 IP 位址 (必要)
ENCRYPTION	char(7)	加密演算法 DES_CBC 或 CDMF
註: 相關訊息: ICA1043		

表 21. *TUNNEL_POLICY*. 本表格含有來自 *t_policy.tbl* 檔的「通道策略」陳述式。

直欄	資料類型	簡短說明
DATE_TIME	date_time	動作的日期與時間 (必要)
FIREWALL	char(100)	防火牆機器的完整名稱 (必要)
PID	int	AIX 處理 ID、NT 緒 ID (必要)
MSG_NUM	int	訊息號碼 (必要)
POLICY	char(60)	從 fwpolicy 檔讀取策略陳述式 (必要)
註: 相關訊息: ICA1040		

表 22. *TUNNEL_STATUS*. 本表格含有關於來自 *t_stat.tbl* 的「通道」狀態變更的資訊。

直欄	資料類型	簡短說明
DATE_TIME	date_time	動作的日期與時間 (必要)
FIREWALL	char(100)	防火牆機器的完整名稱 (必要)
PID	int	AIX 處理 ID、NT 緒 ID (必要)
MSG_NUM	int	訊息號碼 (必要)
SESSION_SCKT	long int	階段作業 socket 連接埠 (ICA1038)
MASTER_SCKT	long int	主要 socket 連接埠 (ICA1038)
TUNNEL_ID	long int	已刪除通道 ID (ICA1041)

表 22. *TUNNEL_STATUS* (繼續). 本表格含有關於來自 *t_stat.tbl* 的「通道」狀態變更的資訊。

直欄	資料類型	簡短說明
<p>註:</p> <p>相關訊息：ICA1038 ICA1039 ICA1041 ICA1042</p> <ul style="list-style-type: none"> 已定義的策略 (ICA1039) 的明細可從 TUNNEL_POLICY 表格取得。 已定義的通道範圍 (ICA1042) 的詳細資訊，可從 TUNNEL_CONTEXT 表格中取得。 		

第3章 附加的 SafeMail 軟體開發套件

IBM Firewall SafeMail 閘道的主要目的，是要在安全及非安全性網路之間轉送郵件，並隱藏安全網路上的主電腦名稱。

SafeMail 閘道本身並不提供任何的內容過濾處理。但是，您可以編寫 SafeMail Content Screener (內容審查程式)，並將它安裝在「防火牆」上，以作為附加的 SafeMail 閘道。您附加的 SafeMail 閘道可以檢視整個 E-mail 訊息，並可根據您所建立的基準來審查 E-mail。附加的 SafeMail 閘道可以告訴 SafeMail 閘道要禁止訊息的轉送，或是要允許訊息通過閘道。

SafeMail 處理概觀

當 SMTP 從屬站連接到 SafeMail 閘道時，SafeMail 閘道會連線到目的地 SMTP 伺服器，而且當 SafeMail 閘道收到來自從屬站具有數行文字的 E-mail 時，會從從屬站一次傳送一行文字的 e-mail 訊息到目的地伺服器。SafeMail 閘道會依需要改寫 E-mail 的某些表頭字行，以隱藏安全網路主電腦的名稱。

如果已安裝附加的「內容審查程式」，則當每一行 E-mail 訊息傳過 SafeMail 閘道時，SafeMail 閘道就會呼叫內容審查程式。SafeMail 閘道也會傳遞 E-mail 訊息的來源及目的地的相關及其他資訊，這樣內容審查程式才可以讓各個呼叫彼此產生關聯。如果必須先分析整個訊息，內容審查程式才能決定是否要讓該訊息通過「防火牆」的話，在這種情況之下，這會很有用。

如果 SafeMail 閘道必須改寫任何表頭，以隱藏安全網路上的主電腦名稱，在改寫該表頭之前，會先呼叫附加的「內容審查程式」。

建立附加的 SafeMail 閘道

若要建立並安裝附加的 SafeMail 閘道，您必須：

- 編寫附加 DLL 的原始程式
- 建立 DLL
- 將 DLL 安裝在「防火牆」上

ROOTDIR\samples\safemail 包含附加的內容審查程式的範例程式碼、必要表頭檔及 IBM Visual Age 和 Microsoft Visual C++ 的 make 檔範例。ROOTDIR 為您在進行安裝作業時，所選定的 IBM Firewall 目標位置目錄。

撰寫原始程式

附加的內容審查程式必須執行一個叫做 `UsrCheck` 的函數，這個函數具有下列原型：

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

當 SafeMail 開道有一行 E-mail 訊息準備要讓內容審查程式檢查時，此為 SafeMail 開道呼叫的進入點。此函數負責檢查這一行 E-mail 訊息；如果它要讓 E-mail 訊息繼續通過 SafeMail 開道，就會傳回 0；如果它要 SafeMail 開道拒絕繼續處理此訊息，則傳回非零值。

請參閱 `ROOTDIR\samples\safemail` 的 `usrcheck.c` 中的範例程式碼，以取得介於 SafeMail 開道及內容審查程式之間的介面的完整說明。

`Check` 函數上的 `pCheckData` 參數為 `ROOTDIR\samples\safemail` 的 `usrcheck.h` 中所說明的 C 結構。此結構包含正在處理之 E-mail 訊息的相關重要資訊，例如：SMTP 伺服器的來源及目的地位址，以及執行傳送及接收動作之 SMTP 伺服器的網路類型（安全或非安全）。該結構同時也包含一個對談關聯性程式，可讓內容審查程式使數個呼叫與同一個 E-mail 訊息產生關聯。

建立 DLL

在您寫好附加的「內容審查程式」的原始程式後，您必須將它編譯，並且鏈結至 DLL。該 DLL 必須命名為 `smusr.dll`。並且必須從該 DLL 匯出 `UsrCheck` 進入點。請參閱 `ROOTDIR\samples\safemail` 中的 `make` 檔範例，取得適當的編譯及鏈結切換範例，以正確地建立 DLL。所提供的 `make` 檔範例適用於 IBM VisualAge C++ 及 Microsoft Visual C。

安裝 DLL

一旦您建立 `smusr.dll` 成功，您必須將它安裝在「防火牆」上。將 `smusr.dll` 複製到「防火牆」的 `\bin` 目錄中。然後使用 Windows NT「控制台」中的「服務控制管理系統」，關閉並重新啟動 IBM Firewall SafeMail 伺服器，以載入附加的程式。

IBM Firewall 提供 `smusr.dll` 的範例，位於「防火牆」的 `\bin` 目錄中。請先將這個 DLL 更名，再把您的 `smusr.dll` 複製到該目錄中，以便將來把您的附加程式移除時，能夠將它還原。

本章及下二章中的編譯器名稱會依各種範例而有所不同。但這三章皆參照二個相同的編譯器。

第4章 附加的日誌保存程式軟體開發套件

IBM Firewall 日誌常駐程式會將所記載的資訊寫入您在架構從屬站的日誌機能對話框中所指定的檔案中。然後您可以使用 `fwlogmgmt` 命令，定期保存舊的日誌記錄。一般而言，您可以從 Windows NT 的「排程式」來執行 `fwlogmgmt` 命令。在預設的狀況下，`fwlogmgmt` 命令會將舊的日誌記錄保存在一個目錄中，並且會用 Windows NT 的壓縮命令來將日誌記錄壓縮。但是，您可以撰寫附加的「日誌保存程式」，以取代預設的保存動作。

如何建立附加的日誌保存程式

欲建立附加的「日誌保存程式」，您必須：

1. 編寫附加 DLL 的原始程式
2. 建立 DLL
3. 將 DLL 安裝在「防火牆」上

`ROOTDIR\sample\logarch` 目錄包含附加的「日誌保存程式」的範例程式，其複製「防火牆」的預設動作及 IBM Visual Age for C++ 的 `make` 檔。`ROOTDIR` 為您在進行安裝作業時，所選定的 IBM Firewall 目標位置目錄。

撰寫原始程式

附加的「日誌保存程式」必須執行一組「防火牆」用來執行保存功能的函數。這些函數的原型範例皆定義在 `ROOTDIR\sample\logarch` 目錄的 `fwarch.h` 中。

這些函數會執行基本的保存功能，例如：將檔案新增至保存檔中、從保存檔中擷取檔案、復新保存檔及列出保存檔中的檔案。

這些函數的相關詳細資訊，請參閱 `ROOTDIR\sample\logarch` 目錄中 `fwarch.c` 的範例。

建立 DLL

在您寫好附加的「日誌保存程式」的原始程式後，您必須將它編譯，並且鏈結至 DLL。該 DLL 必須命名為 `fwarch.dll`。在 `fwarch.h` 中列出的所有函數都必須從該 DLL 匯出。

`ROOTDIR\sample\logarch` 目錄提供一 IBM VisualAge for C++ 的 `make` 檔範例，可用來將範例程式碼建立到適當的 DLL 中。

安裝 DLL

在您成功地建立 `fwarch.dll` 後，請將它安裝在「防火牆」上。將 `fwarch.dll` 複製到 `ROOTDIR\bin` 目錄中。

「防火牆」的預設 `fwarch.dll` 也在此目錄中。所以在您將您所建立的 DLL 複製到此目錄前，請先將此預設的 DLL 備份或更名。

同時，請確定目前並沒有執行 `fwlogmgmt` 命令，並且在您置換預設的 DLL 時，請確定沒有執行 IBM Firewall 日誌常駐程式。請使用「服務控制管理系統」來關閉 IBM Firewall 日誌常駐程式，然後再置換 DLL，並重新啟動。

第5章 提供自己的鑑證方法

本章將為您說明如何提供自己的鑑證方法之相關資訊。

使用者提供的鑑證

我們提供了位於 `ROOT_DIR\bin\authsdk` 目錄的使用者鑑證範例。檔案包括：

- `authschm.h` - 介面定義檔
- `authus.cpp` - 範例計劃的原始檔
- `gwauth4.lib` - 防火牆的程式庫
- `msvc++.mak` - Microsoft Visual C Make file
- `schmname.h` - 介面定義檔
- `vac++.mak` - IBM Visual Age Make file

使用下列命令來編譯 IBM Visual Age 的使用者鑑證範例。

- `nmake -f vac++.mak` - 建置 DLL
- `nmake -f vac++.mak install` - 建置並安裝 DLL
- `nmake -f vac++.mak clean` - 清除本端目錄

使用下列命令來編譯 Mircrosoft Visual C 的使用者鑑證範例。

- `nmake -f msvc++.mak` - 建置 DLL
- `nmake -f msvc++.mak install` - 建置並安裝 DLL
- `nmake -f msvc++.mak clean` - 清除本端目錄

使用「軟體開發套件 (SDK)」來建立使用者提供的鑑證計劃

IBM Firewall 提供可外掛的介面，來整合協力廠商的鑑證安全性產品。可撰寫附加在 Firewall 鑑證計劃介面的鑑證計劃 `.dll`，來執行此項作業。

防火牆鑑證處理的概觀

下列防火牆服務程式必須鑑證使用者，才可讓它們存取防火牆服務程式：

- IBM Firewall 架構伺服器
- IBM Firewall Proxy FTP 常駐程式
- IBM Firewall Proxy HTTP 常駐程式
- IBM Firewall Telnet 常駐程式
- IBM Firewall Socks 伺服器

Firewall 提供下列鑑證計劃：

全部拒絕

拒絕使用者存取服務程式。

全部允許

允許使用者存取服務程式，而不需要加以鑑證。

Firewall 通行碼

提示使用者輸入已定義在「防火牆使用者」資料庫中的通行碼。

NT 登入通行碼

提示使用者輸入「Windows NT 登入通行碼」。

SecureNetKey

使用「AssureNet Pathways SecureNet Key」鑑證使用者。

SecurID 卡

使用 Security Dynamics SecurID 安全卡來鑑證使用者。

所使用的鑑證計劃可以定義在每一個使用者或每一個服務程式基礎上。例如，可以架構 Firewall，讓使用者 *John* 試圖登入 IBM Firewall 架構伺服器時提示他輸入「Windows NT 登入通行碼」。但是當 *John* 要使用 IBM Firewall Telnet Proxy 時，則會使用他的「SecurID 卡」來鑑證他。其間，當使用者 *Mary* 試圖登入「IBM Firewall 架構伺服器」時，則會提示她輸入「防火牆通行碼」。Firewall 所提供的鑑證計畫，以及如何為使用者定義鑑證計畫的相關資訊，請參閱 *IBM eNetwork Firewall 使用指南* 的「管理」一章。

除了 IBM Firewall 提供的鑑證計劃，您最多可安裝三個使用者提供的鑑證計劃。您可以根據現有的安全基礎來撰寫這些計劃；或者，您可以從協力廠商取得安全計劃，將他們的產品與「防火牆」整合。

「防火牆」中的每一個鑑證計劃（包括使用者提供的鑑證計劃）是由執行鑑證計劃 API 的 DLL 代表。此 API 是定義鑑證計劃如何使用「防火牆」來登記自己，以及「防火牆」如何將鑑證要求傳遞給它。

建立使用者提供的鑑證計劃

建立使用者提供的鑑證計劃是由下列步驟組成：

- 撰寫原始程式來執行鑑證計劃 API
- 編譯及鏈結原始程式到 DLL
- 將 DLL 安裝在「防火牆」上

建立使用者提供之鑑證計劃所需的 C 原始表頭檔及程式庫檔案，以及 Microsoft Visual C++ 及 IBM Visual Age for C++ 的範例程式及範例 make 檔案都可在 ROOTDIR\bin\authsdk 中找到。

撰寫原始程式

所有鑑證計劃必須執行兩件事：

1. 使用「防火牆」登記它們自己
2. 執行 AuthSchmFn

向 Firewall 登記： 啟動「防火牆」服務程式之前，「防火牆」會試圖載入它在 `\bin\authschm` 子目錄中找到的每一個 DLL。載入每一個 DLL 時，它的起始設定常式必須呼叫「防火牆」中的 `registerAuthSchm` 函數，才能使用「防火牆」登記它自己。

`registerAuthSchm` 函數原型是定義在 `authschm.h` 表頭檔中。它會採用指向 `AuthSchmInfo` 結構 (也定義在 `authschm.h` 中) 的單一參數。The `AuthSchmInfo` 結構會連結鑑證計劃與「防火牆」應該呼叫之適當 `AuthSchmFn` 的位址，以便將鑑證要求傳遞給鑑證計劃。

使用者提供的鑑證計劃必須使用下列三個名稱中的其中一個：

1. `user`
2. `userauth2`
3. `userauth3`

表頭檔 `schmname.h` 中，有定義給這些名稱的符號名稱。使用者提供的鑑證計劃的設計應該讓一般使用者都可以指定要使用這三個名稱中的哪一個，以便讓多個使用者提供的鑑證計劃可以安裝在同一個「防火牆」上，而不需要擔心兩個不同的計劃會有同樣的名稱。

DLL 起始設定常式順利呼叫登記 `AuthSchm` 並傳回呼叫程式之後，會準備 DLL 來處理鑑證要求。基於這個原因，可能也需要在 DLL 起始設定常式中執行任何的計劃特定起始設定。

執行 AuthSchmFn： 每一個鑑證計劃 DLL 必須使用定義在 `authschm.h` 中的原型，來執行 `AuthSchmFn` 函數。`AuthSchmFn` 函數具有一個指向 `AuthReq` 結構的參數。`AuthReq` 結構是一個簡單的 C 結構，其中包含現行鑑證要求的相關資訊。`AuthReq` 是定義在 `authschm.h` 中。`AuthReq` 結構包含要鑑證之使用者的名稱、要求鑑證的「防火牆」元件/服務程式，以及該要求的其它相關資訊。如需 `AuthReq` 結構之資訊的完整列示及說明，請參閱 `authschmh` 中有關它的說明。

除了使用者名稱及防火牆元件之外，`AuthReq` 結構中還有三個參數在執行鑑證計劃時特別重要：

gwaput

這是「防火牆」提供之回覆常式的位址，在它需要傳送訊息給使用者時可以使用該鑑證計劃。例如，如果鑑證計劃需要發出一個提示訊息給使用者的話，則它會呼叫 `gwaput` 參數提供的登錄點。`gwaput` 回覆功能是以 `authschm.h` 中的 `AuthSchmPut` typedef 為原型。請參閱 `AuthSchmPut` typedef 上的說明，即可取得 `AuthSchmFn` 必須在此呼叫上傳遞的參數完整列示。

gwaget

這是「防火牆」提供之回覆常式的位址，在它需要從鑑證的使用者擷取回應時可以使用該鑑證計劃。例如，如果鑑證計劃需要從使用者取得通行碼的話，則它會呼叫 gwaget 參數提供的登錄點。gwaget 回覆功能是以 authschm.h 中的 AuthSchmGet typedef 為原型。請參閱 AuthSchmGet typedef 上的說明，即可取得 AuthSchmFn 必須在此呼叫上傳遞的參數完整列示。特別重要的一個參數為 echo 參數。AuthSchmFn 可以使用此參數來指示使用者的回應是否應傳回給他。

opaque_data

opaque_data 欄位是「防火牆」用來讓對 AuthSchmFn 的呼叫與對其回覆常式之呼叫產生關聯。呼叫 gwaget 或 gwaput 常式時，則 AuthSchmFn 應該會使用在 AuthReq 結構上傳遞給它的相同 opaque_data 值來傳遞。

請注意：鑑證計劃必須能夠與所有的「防火牆」元件互動。某些「防火牆」元件可以支援與一般使用者的多個提示/回應對話。這些元件稱之為交談式「防火牆」元件。某些「防火牆」元件因為它們通訊協定的本質，所以只支援單一的提示/回應。這些稱為非交談式「防火牆」元件。

使用者提供的鑑證計劃必須能夠根據呼叫它的「防火牆」元件來修改它的行為，如 AuthReq 結構的元件欄位所指示的一樣。元件欄位的有效值是定義在 authschm.h 中。元件欄位目前的有效值如下：

表 23. 元件欄位的有效值

AuthSchm.h 中的元件符號	「防火牆」元件	交談式/非交談式
AUTHSCHM_UNKNOWN	新的或無法辨識的「防火牆」元件	假設它是交談式
AUTHSCHM_REMADMIN	架構伺服器	交談式
AUTHSCHM_FTP	FTP Proxy	非交談性
AUTHSCHM_TELNET	Telnet Proxy	交談式
AUTHSCHM_HTTP	HTTP Proxy	交談式
AUTHSCHM_SOCKS_PWD	使用通行碼鑑證的 Socks 伺服器	非交談性
AUTHSCHM_SOCKS_CRAM	使用 CRAM 鑑證的 Socks 伺服器	交談式
AUTHSCHM_REMIPSEC	「遠端從屬站 IPSEC」伺服器 (目前在 Windows NT 上無法使用)	交談式

AuthSchmFn 已經完成它的處理時，它必須以其中一個 GWA 回覆碼 (定義在 authschm.h 中) 來傳回給呼叫程式。此回覆碼是用來指示鑑證使用者是否順利，以及在處理期間是否發生錯誤。

表 24. GWA 回覆碼

回覆碼	表示
GWA_OK	處理期間沒有發生錯誤，而且順利鑑證使用者
GWA_DENY	處理期間沒有發生錯誤，但使用者無法鑑證本身
GWA_IOFAILURE	試圖傳送提示給使用者，或試圖取得使用者的回應時發生錯誤。一般而言，回覆常式中有錯誤發生時就會傳回這個回覆碼。
GWA_BUFFERTOOSMALL	AuthSchmFn 函數無法從使用者擷取回應，因為它無法配置一個夠大的緩衝區來接收該回應。
GWA_NOAUTHFN	錯誤 - 與鑑證計劃無關
GWA_FNNOTREG	錯誤 - 與鑑證計劃無關
GWA_RSVNAME	錯誤 - 包含保留名稱且無法用於此鑑證計劃的鑑證要求
GWA_BADNETTYPE	錯誤 - 與鑑證計劃無關
GWA_BADAPP	錯誤 - 與鑑證計劃無關
GWA_BADADDR	錯誤 - 鑑證要求上提供的位址無效
GWA_MEMSHORTAGE	錯誤 - 因為無法配置記憶體，所以無法處理鑑證要求
GWA_USERDBFAIL	錯誤 - 無法查詢所需的資料庫
GWA_REGFAILED	錯誤 - 與鑑證計劃無關
GWA_AUTHERROR	錯誤 - 鑑證計劃特定錯誤狀況
GWA_INTERNAL	錯誤 - 鑑證計劃中的其他錯誤狀況

當 AuthSchmFn 傳回「防火牆」時，如果回覆碼為 GWA_OK，則會考慮鑑證使用者，並讓該使用者可以存取所要求的服務程式。GWA_DENY 被視為非錯誤狀況，但拒絕該使用者存取所要求的服務程式。所有其它的回覆碼都是錯誤狀況，而且拒絕該使用者存取所要求的服務程式。

編譯及鏈結到原始程式： 編譯及鏈結原始程式到 DLL 時，您必須使用 \bin\authsdk 目錄中提供的 gwauth4.lib，將 DLL 鏈結到 gwauth4.dll，以便解析定義在 authschm.h 中的登錄點名稱。此外，AuthSchmFn 不是從 DLL 匯出的，此點相當重要。IBM VisualAge for C++ 及 Microsoft Visual C++ 的範例 make 檔案可在 \bin\authsdk 目錄中找到。

安裝 DLL： DLL 已順利建置好時，請將它複製到 R00TDIR\bin\authschm 目錄中，然後重新啟動「防火牆」機器。為了讓防火牆能載入 DLL 並登記 DLL 的鑑證計劃，必須重新啟動「防火牆」機器。

將它放在一起：第54頁的圖 1 會顯示如何載入鑑證計劃，以及顯示如何在鑑證要求處理期間呼叫主要函數。

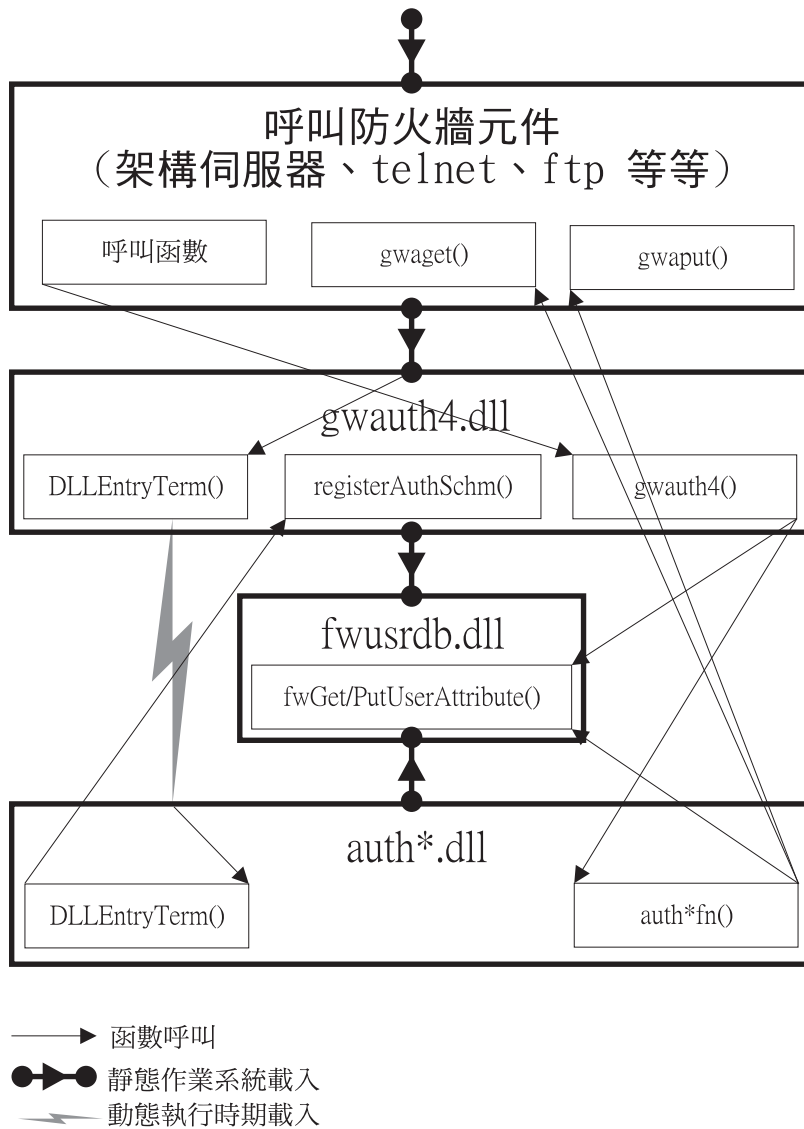


圖 1. DLL 起始設定與登記

需要使用鑑證服務程式的「防火牆」元件會鏈結到稱之為 gwauth4 的「防火牆」DLL。載入 gwauth4 dll 時，則會呼叫它的 DLLEntryTerm 常式，而且會試圖進行執行時期載入，

載入 R00TDIR\bin\authschm 中所有的 DLL。如果鑑證 DLL 無法載入，則它不會被視為一個載入 gwauth4 dll 的錯誤。gwauth4 dll 仍會繼續嘗試載入。

當鑑證計劃的 DLEntryTerm 常式執行時，它們會負責使用 gwauth4.dll 登記鑑證計劃。呼叫 registerAuthSchm 即會完成此項作業。authschm dll 需要為 DLL 支援的每一個鑑證計劃呼叫一次 registerAuthSchm。在 registerAuthSchm 函數上傳遞的 AuthSchmInfo 結構會將鑑證計劃的名稱 (儲存在使用者資料庫中) 與 AuthSchmFn 函數的登錄點連結。registration 函數會將其結構的拷貝傳遞給它，以便讓 authschm dll 可以在需要時重新使用，修改這個結構。鑑證計劃 DLL 也會負責釋放 AuthSchmInfo 結構。

registerAuthSchm 函數是負責建置鏈結的列示 (代表所有登記的鑑證計劃)。gwauth4 的 DLEntryTerm 常式會將列示錨點起始設定為空值。然後，當 authschm DLL 呼叫 registerAuthSchm 函數時，它會執行下列事項：

1. 在鑑證計劃列示中掃描，以搜尋一個名稱與傳遞名稱相同的項目。如果存在的話，請將它從列示中移除，並刪除它所有相關的儲存體。
2. 根據 AuthSchmInfo 結構建置 AuthSchmEntry 結構，並將它新增到鑑證計劃列示中。
3. 將登記作業成功 (GWA_OK) 或失敗 (GWA_REGFAILED) 的指示傳回給呼叫程式。

當 gwauth4 的 DLEntryTerm 已在每一個 authschm dll 上執行了執行時載入，而且 authschm DLL 已登記它們的鑑證計劃之後，gwauth4 的 DLEntryTerm 常式會傳回給呼叫程式。此時，其它元件可以開始呼叫 gwauth4 函數，來要求鑑證服務程式。

當 gwauth4.dll 卸載時，則會重新呼叫 DLEntryTerm 常式，以終止處理。為了終止而呼叫時，此常式將會刪除 AuthSchmList 上的 AuthSchmEntry 項目，及其相關的儲存體。因為會完成此項作業，所以鑑證計劃就不需要從「防火牆」取消登記它們自己。

鑑證要求處理： 當「防火牆」服務程式需要鑑證使用者時，它會呼叫 gwauth4.dll 中的函數。gwauth4 會從呼叫元件擷取資訊，並查詢「防火牆」使用者資料庫來決定要用來處理要求的鑑證計劃名稱。

gwauth4 已決定鑑證計劃的名稱時，它會掃描已登記鑑證計劃的列示，以取得相同名稱的計劃。如果它依據相同名稱尋找登記的計劃，則它會建置 AuthReq 結構來代表目前的要求，並呼叫鑑證計劃 DLL (與該名稱相關) 中的登錄點。

gwauth4 所呼叫的 AuthSchmFn 函數會處理要求並在需要與使用者互動時，呼叫 gwaget 與 gwaput 回覆常式。當它完成處理時，它會以適當的回覆碼將控制傳回給 gwauth4。

gwauth4 會撰寫適當的日誌記錄來記載鑑證要求，然後返回發出要求及收到鑑證計劃 DLL 之回覆碼的防火牆元件。

第6章 使用「建立密碼鎖檔案公用程式」(MKKF)

安全 SSL 網路連線要求您具備：

- 架構您的架構伺服器，供 SSL 使用
- 建立一個密碼鎖，供安全通信使用
- 指定為您的伺服器上可靠的主密碼
- 隱藏您的密碼鎖檔案通行碼

使用 MKKF 以建立起始伺服器密碼鎖、鎖環檔及認證要求。MKKF 也將用來接收鎖環內的起始認證，以及隱藏您的密碼鎖檔案通行碼。

建立密碼鎖檔案

執行此公用程式時，您必須使用 Windows NT 管理者帳戶登入。

1. 進入 ROOTDIR\config 目錄，並請輸入下列命令，以啟動密碼鎖公用程式：

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

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

2. 建立一個新鎖環檔。

```
鎖環功能表  
目前選取的鎖環：(無)
```

```
N - 建立新鎖環檔  
O - 開啓鎖環檔  
X - 結束
```

輸入一個命令：**n**

如上所示輸入 'n'，來建立一個新密碼鎖檔案。

將提示您輸入一個將供密碼鎖檔案使用的檔案名稱。您可以使用任何檔案名稱，但它須以 .kyr 結尾。依據預設值，防火牆將尋找名為 fwkey.kyr 的檔案。

輸入鎖環檔的名稱，或是按下 ENTER 鍵，接受 **fwkey.kyr** 的預設值

MKKF 將建立一個新密碼鎖檔案，並顯示鎖環功能表。請注意，密碼鎖檔案將列示為目前選取的鎖環。

3. 建立一個新密碼鎖與認證要求。

鎖環功能表
目前選取的鎖環：fwkey.kyr

- N - 建立新鎖環檔
- O - 開啓鎖環檔
- S - 儲存鎖環檔
- A - 將鎖環檔儲存為另一個檔案
- P - 設定鎖環檔的通行碼
- C - 建立鎖環檔的隱藏檔
- R - 在鎖環檔內接收認證
- W - 使用密碼鎖與認證
- X - 結束

輸入一個命令：w

如上所示輸入 'w'，跳至「密碼鎖」功能表。

密碼鎖功能表
目前選取的鎖環：fwkey.kyr
選取的密碼鎖項目：(無)

- L - 列示/選取將使用的密碼鎖
- C - 建立新密碼鎖與認證要求
- I - 從「防護」密碼鎖檔案中匯入一個密碼鎖
- X - 結束這個功能表

輸入一個命令：c

如上所示輸入 'c'，來建立一個新密碼鎖。

在可以將密碼鎖儲存在密碼鎖檔案之前，密碼鎖檔案必須要有通行碼的保護。MKKF 將提示您輸入一個用來保護密碼鎖檔案的通行碼。當您輸入通行碼時，它不會顯示出來。MKKF 也會詢問通行碼是否要設定到期天數。輸入如下所示的 'n'。

輸入將用於密碼鎖檔案的通行碼：
通行碼
重新輸入通行碼，進行驗證：**通行碼**
通行碼過期了嗎？
輸入 Y 代表是，或輸入 N 代表否：
n
已順利設定通行碼。
按 ENTER 鍵，繼續作業

MKKF 將給與您可建立的密碼鎖類型的提示。

選擇認證類型功能表
S - PEM 認證要求格式（專用增強訊息）
P - PKCS10 認證要求格式
C - 取消

輸入一個命令：s

如上所示輸入 's'，來建立 PEM 認證。MKKF 將產生一個空認證：

撰寫安全伺服器認證功能表

現行認證資訊

密碼鎖名稱：(無)

密碼鎖大小：0

伺服器名稱：(無)

組織：(無)

組織單位：(無)

城市/地區：(無)

州/省：(無)

郵遞區號：(無)

國家：(無)

M - 修改認證欄位

R - 準備建立密碼鎖與認證要求

C - 取消

輸入一個命令：m

輸入 'm'，修改空認證。將提示您輸入關於新認證的資訊：

- 輸入一個將使用的名稱。這個名稱可以是任何字串，且僅被 MKKF 公用程式使用：

輸入一個將用在密碼鎖項目使用的名稱：

防火牆密碼鎖

- 輸入密碼鎖的大小。IBM Firewall 只提供可匯出的 MKKF 版本。最大的密碼鎖大小為 1024。

1: 508

2: 512

3: 768

4: 896

5: 1024

輸入與您想要之密碼鎖大小對應的數字：

2

- 輸入防火牆的完整 TCP/IP 主電腦名稱 (例如，jupiter.raleigh.ibm.com)：

輸入伺服器的完整 TCP/IP 領域名稱，或按下 Enter 鍵，使欄位留白

jupiter.raleigh.ibm.com

- 輸入與認證有關聯的組織名稱。(例如，公司名稱)：

輸入要進行認證的「組織名稱」，或自行按下 ENTER 鍵，使欄位留白。

AAA Inc.

- 輸入組織單位名稱。(例如，部門名稱)：

輸入要進行認證的「組織單位名稱」或自行按下 ENTER 鍵，使欄位留白。

網路安全產品

- 輸入將在其中使用認證的城市：

輸入要進行認證的「當地/城市名稱」，或自行按下 ENTER 鍵，使欄位留白。

RTP

- 輸入省。

註：因為認證規格，所以這個欄位最少須有三個字元，因此兩個字母的州縮寫無效。

輸入要進行認證的「州/省名稱」，或自行按下 ENTER 鍵，使欄位留白。
「省」最少須有三個字元。

N.C.

- 輸入與認證有關聯的郵遞區號。(這同於郵政編碼)：

輸入要進行認證的「郵遞區號」，或自行按下 ENTER 鍵，使欄位留白。

27709

- 請輸入兩個字母的國碼：

輸入要進行認證的「國碼」，或自行按下 ENTER 鍵，使欄位留白。
國碼僅能有兩個字母。

US

MKKF 從您那裡收集到所有資訊後，將顯示認證：

撰寫安全伺服器認證功能表

現行認證資訊

密碼鎖名稱：防火牆密碼鎖

密碼鎖大小：512

伺服器名稱：jupiter.raleigh.ibm.com

組織：AAA Inc.

組織單位：網路安全產品
城市/當地：RTP
省：N.C.
郵遞區號：27709
國家：US

M - 修改認證欄位
R - 準備建立密碼鎖與認證要求
C - 取消

輸入一個命令：**r**

如果在認證資訊中有任何錯誤，您可以輸入 'm'，來進行更正。如果資訊是正確的，請輸入 'r' 來建立新密碼鎖及其相關的密碼鎖檔案。

MKKF 將提示您提供一個儲存認證的檔案。您可以使用任何檔案名稱，但最好使用相同的基本名稱作為密碼鎖檔案，並加入 .cert 作為副檔名：

輸入將儲存下列的認證要求的檔案：

fwkey.cert
正在建立專屬密碼鎖...
已順利建立專屬密碼鎖。
正在建立認證要求...
已順利建立認證要求
正在將新密碼鎖加到密碼鎖檔案中
已順利建立新密碼鎖與認證要求。
按 ENTER 鍵，繼續作業

4. 使新建立的密碼鎖成為預設值。

在建立了密碼鎖與認證後，將顯示「密碼鎖」功能表。新建立的密碼鎖將列示為「選取的密碼鎖項目」：

密碼鎖功能表
目前選取的鎖環：fwkey.kyr
選取的密碼鎖項目：防火牆密碼鎖

L - 列示/選取將使用的密碼鎖
S - 顯示關於選取的密碼鎖的資訊
D - 刪除選取的密碼鎖
C - 建立新密碼鎖與認證要求
I - 從「防護密碼鎖檔案」匯入一個密碼鎖
E - 將選取的密碼鎖匯出至「防護密碼鎖檔案」
F - 使選取的密碼鎖作為這個鎖環的預設密碼鎖
U - 取消標示選取的密碼鎖的授權者名稱狀態
R - 建立選取的密碼鎖的認證要求
X - 結束這個功能表

輸入一個命令：**f**

您必須使新建立的密碼鎖成為密碼鎖檔案中的預設密碼鎖。輸入先前範例中所示的 'f'。
將提示您確認動作：

密碼鎖功能表

目前選取的密碼鎖：防火牆密碼鎖

您確定想要使這個密碼鎖成為預設值嗎？

輸入 Y 代表是，或輸入 N 代表否：

y

已將密碼鎖設定成為預設密碼鎖。

按 ENTER 鍵，繼續作業

在密碼鎖已標示為預設值後，「密碼鎖功能表」即會顯示出來：

密碼鎖功能表

目前選取的鎖環：fwkey.kyr

選取的密碼鎖項目：防火牆密碼鎖

- L - 列示/選取將使用的密碼鎖
- S - 顯示關於選取的密碼鎖的資訊
- D - 刪除選取的密碼鎖
- C - 建立新密碼鎖與認證要求
- I - 從「防護密碼鎖檔案」匯入一個密碼鎖
- E - 將選取的密碼鎖匯出至「防護密碼鎖檔案」
- F - 使選取的密碼鎖作為這個鎖環的預設密碼鎖
- U - 取消標示選取的密碼鎖的授權者名稱狀態
- R - 建立選取的密碼鎖的認證要求
- X - 結束這個功能表

輸入一個命令：**x**

輸入 'x'，結束「密碼」功能表。

5. 接收鎖環檔內的認證。

「鎖環」功能表將顯示出來：

鎖環功能表

目前選取的鎖環：fwkey.kyr

- N - 建立新鎖環檔
- O - 開啓鎖環檔
- S - 儲存鎖環檔
- A - 將鎖環檔儲存為另一個檔案
- P - 設定鎖環檔的通行碼
- C - 建立鎖環檔的隱藏檔
- R - 在鎖環檔內接收認證
- W - 使用密碼鎖與認證
- X - 結束

輸入一個命令：**r**

註：既然防火牆不會為了執行認證而使用 SSL，所以認證單位(CA)不必簽署您的認證。

輸入檔案名稱，或按下 ENTER 來取得 Cert.txt。

fwkey.cert

這是自我簽署的認證。要將它加到密碼鎖檔案中嗎？

輸入 Y 代表是，或輸入 N 代表否：

y

認證已新增至鎖環。

按 ENTER 鍵，繼續作業

6. 建立密碼鎖檔案的隱藏檔。

在認證已新增至鎖環後，「鎖環功能表」即會顯示出來：

鎖環功能表

目前選取的鎖環：fwkey.kyr

- N - 建立新鎖環檔
- O - 開啓鎖環檔
- S - 儲存鎖環檔
- A - 將鎖環檔儲存為另一個檔案
- P - 設定鎖環檔的通行碼
- C - 建立鎖環檔的隱藏檔
- R - 在鎖環檔內接收認證
- W - 使用密碼鎖與認證
- X - 結束

輸入一個命令：**c**

您需要建立密碼鎖檔案的隱藏檔。如先前範例中所示，輸入 'c'。MKKF 將使用相同的基本名稱作為密碼鎖檔案，並使用 .sth 作為副檔名：

隱藏的密碼鎖檔案已儲存至 fwkey.sth

按 ENTER 鍵，繼續作業

在已建立隱藏檔後，「鎖環功能表」即會顯示出來：

鎖環功能表

目前選取的鎖環：fwkey.kyr

- N - 建立新鎖環檔
- O - 開啓鎖環檔
- S - 儲存鎖環檔
- A - 將鎖環檔儲存為另一個檔案
- P - 設定鎖環檔的通行碼
- C - 建立鎖環檔的隱藏檔
- R - 在鎖環檔內接收認證
- W - 使用密碼鎖與認證
- X - 結束

輸入一個命令：**x**

現在可使用您的密碼鎖檔案。如上所示輸入 'x'，結束 MKKF，以及輸入 'y'，按照所示的方式將變更儲存至您的密碼鎖檔案中：

鎖環檔已變更。要儲存嗎？
輸入 Y 代表是，或輸入 N 代表否：
y
鎖環已儲存至 fwkey.kyr
按 ENTER 鍵，繼續作業
#

7. 更新架構檔。

在建立檔案後，您須使用 `fwcfgsrv` 命令，在架構伺服器參數檔中指定密碼鎖檔案名稱。

如果您要對架構伺服器使用 SSL 加密，您也須使用 `fwcfgsrv` 命令來設定 `encryption=ssl` 選項。

使用 `fwcfgsrv` 命令之後，請停止並重新啓動伺服器服務程式。

第7章 疑難排解與測試

本章告訴您當設定和架構 IBM Firewall 時，如何解決一些常見的問題。

如果您遇到問題，首先請用偵錯優先順序建立一個防火牆日誌，來增加傳送至您的日誌的資訊。請參閱第6頁的『日誌檔管理』，取得相關資訊。

安裝及設定

過濾支援失敗

問題說明

您接收錯誤訊息。

過濾支援驗證失敗。Socket 建立呼叫失敗。
路徑名稱中的檔案或目錄不存在。

本問題是因在安裝後並未重新啟動防火牆所致。

建議動作

請重新啟動您的防火牆並重試程序。

遞送路徑問題

IBM Firewall 會在安全策略對話框上，提供一個標題名稱為 *測試 IP 遞送路徑* 的功能，這個功能對與遞送路徑有關之問題的除錯相當有用。啟動這個勾選框，啟動您的「連線」架構，並啟動「連線規則記載」。然後檢查您的防火牆日誌，檢視關於所有通過您防火牆之封包的詳細資訊。

首先使用 IP 位址，然後使用主電腦名稱，來執行這些測試。如果您的資料傳輸遞送路徑雖正確使用位址但未使用名稱，請參閱第67頁的『DNS 問題』，取得相關資訊。

無法從防火牆 ping 主電腦

問題說明

您的網路介面並未正確架構。

建議動作

請參閱作業系統文件。

問題說明

您連接至非安全網路的連線並未正確架構。

建議動作

請連絡您的「Internet 服務提供者」，取得協助。

問題說明

如果您的安全網路是隔離在路由器之後，則您的防火牆必須有至該路由器的靜態遞送路徑。使用 `netstat -rn`，驗證靜態遞送路徑：

```
netstat -rn
```

以「通訊協定系列 2」而言，此輸出應如下所示：

目的地 設定值	閘道	旗號
nnn.nnn.nnn	nrr.nrr.nrr.nrr	UG	
sss.sss.sss	nnn.nnn.nnn.nnn	U	
ssl.ssl.ssl	srr.srr.srr.srr	UG	
127	127.0.0.1	U	

圖 2. 的範例輸出 `netstat -rn`.

nrr.nrr.nrr.nrr

代表您連接 Internet 的路由器並且是預設遞送路徑。預設遞送路徑是靜態遞送路徑 (Flag=UG)。

nnn.nnn.nnn

代表您的非安全領域。這是一個介面遞送路徑 (Flag=U)。

nnn.nnn.nnn.nnn

代表您的非安全介面。

sss.sss.sss

代表您的安全領域。這是一個介面遞送路徑 (Flag=U)。

sss.sss.sss.sss

代表您的安全介面。

ssl.ssl.ssl

代表網路安全端的子領域，而 `srr.srr.srr.srr` 代表這個子領域的路由器。這是一個靜態遞送路徑 (Flag=UG)。

127.0.0.1

是回路或區域主電腦。這是一個介面遞送路徑 (Flag=U)。

您必須有每個介面的介面遞送路徑，而且您的預設遞送路徑必須指向「防火牆」非安全端的路由器。

建議動作

將靜態遞送路徑新增到您的路由器中。請連絡路由器管理者。請使用 `route add` 命令。

問題說明

您的安全介面或您正在嘗試連線之主電腦上的子網路遮罩可能不正確。

建議動作

請使用您的從屬站架構公用程式，來更正遮罩設定。

無法從安全主電腦 ping 非安全主電腦 (反之亦然)

問題說明

每一個鄰近防火牆的路由器都須包含靜態遞送路徑，將防火牆指定為閘道，以便傳送資料到防火牆外的目的地網路。

建議動作

請與您的路由器管理者連絡。

問題說明

如果您的安全網路使用未登記且可在非安全網路上遞送的位址，包括 RFC 1597 中所指定的專用位址，則封包不會遞回給傳送者。

建議動作

請使用具有已登記位址的從屬站。

DNS 問題

防火牆 DNS 將會透過查詢安全名稱伺服器來解析名稱。安全名稱伺服器將解析安全網路中的所有名稱。安全名稱伺服器會向防火牆名稱伺服器提出非安全名稱的要求。防火牆名稱伺服器會查詢非安全名稱伺服器，來解析要求。

DNS 問題會影響其它區域的防火牆作業。即使問題與 DNS 的關係並不明顯，但是您最好還是要檢查 DNS。

以下是一些範例，帶您逐步了解這個方法，以便使用 nslookup 公用程式，來隔離問題。在這些範例中，我們將使用下列值：

www.ibm.com

代表非安全網路上的任意主電腦名稱

nns.nns.nns.nns

代表非安全名稱伺服器的位址

sns.sns.sns.sns

代表安全名稱伺服器的位址

host.secure.company.com

代表您安全網路內任意主電腦的名稱

127.0.0.1

代表您防火牆上的迴圈位址

這些值可從「架構從屬站」的**領域名稱服務程式**對話框中取得。當您練習這些作業時，將需要這些值。

註: nslookup 命令需要主電腦名稱加上一個句點，以避免 nslookup 附加您的安全領域名稱。

尚未架構 DNS

問題說明

您尚未架構防火牆的 DNS 機能。

建議動作

請完成**領域名稱服務**對話框。

DNS 查詢失敗或逾時

問題說明

防火牆資料傳輸控制不容許 DNS 封包流過。

建議動作

請進入**安全策略**對話框，啟動“允許 DNS 查詢”勾選框，然後重新啟動您的資料傳輸控制。

nslookup www.ibm.com. nns.nns.nns.nns 失敗

問題說明

非安全名稱伺服器未使用所指出的位址，或並未正確架構。

建議動作

請與您的 DNS 服務供應者連絡，取得有效的名稱伺服器位址。

nslookup www.ibm.com. 127.0.0.1 失敗

問題說明

Microsoft DNS 服務程式可能目前不在執行中。請到服務程式控制管理系統，來判斷它是否正在執行。

建議動作

請使用服務程式控制管理系統來啟動 DNS。

nslookup host.secure.company.com. sns.sns.sns.sns 失敗

問題說明

您的安全名稱伺服器已關閉。

建議動作

請重新啟動您的名稱伺服器。

nslookup www.ibm.com. sns.sns.sns.sns 失敗

問題說明

您的安全名稱伺服器並未正確架構，所以無法與 IBM Firewall 交談。

建議動作

架構的必備條件，請參閱 *IBM eNetwork Firewall 使用指南*。

架構從屬站

伺服器沒有回應

問題說明

架構從屬站及架構伺服器正在使用不同的語言。

建議動作

在架構從屬站登入畫面上，請選取防火牆已經安裝的語言。

問題說明

SSL 加密可能並未正確架構。

建議動作

請確定已在從屬站登入畫面中選取 SSL。請使用服務程式控制管理系統，來停止及重新啟動防火牆架構伺服器。

問題說明

防火牆的架構伺服器可能已停用。

建議動作

確定防火牆架構伺服器正在執行中。

問題說明

防火牆的架構伺服器可能正在監督非標準連接埠。

建議動作

請檢查 c:\winnt\system32\drivers\etc\services，並確定它含有字行 ibmfwrcs 1014/tcp。如果您想要使用另一個連接埠上的伺服器，請根據您的需求編輯 ibmfwrcs 1014/tcp，並確定您已在從屬站的登入畫面中指定新連接埠。請使用服務程式控制管理系統，來停止及重新啟動架構伺服器。

問題說明

防火牆的資料傳輸控制可能不允許與「架構伺服器」進行雙向通信。此動作僅影響在遠端主電腦上執行的「架構從屬站」。

建議動作

請在執行「架構從屬站」的機器與防火牆之間建立一個連線。「架構從屬站」應該是連線的來源，而防火牆應為目的地。請重新建立並啟動您的變更。相關資訊，請參閱 *IBM eNetwork Firewall 使用指南*。

問題說明

「架構伺服器」可能未架構，來容許從遠端主電腦進行登入。

建議動作

請使用 `fwcfgsrv` 命令，來驗證 `localonly` 參數是否設定為 `no`。

無法登入至「架構伺服器」

問題說明

每一個已在防火牆中鑑證的使用者名稱被架構來使用數個鑑證方法的任一個。`Denyall` 是用來禁止對該使用者使用某一個特定的服務程式。

建議動作

請檢查正在使用的使用者名稱之「安全管理」與「非安全管理」欄位。這些欄位僅對「管理者」有效，對防火牆使用者則無效。

資料傳輸控制

對連線所做的變更未生效

問題說明

對任何「資料傳輸控制」元件所做的變更在它們啟動之前並不會立即生效。包括「系統管理」下的**安全策略**對話框。

建議動作

請使用**連線啟動**對話框，重新建立並啟動您的架構。

Proxy 伺服器

未傳輸任何資料

問題說明

防火牆的 `proxy` 服務程式會在安裝後重新啟動機器時啟動。

建議動作

重新啟動機器。

問題說明

必須架構防火牆的「資料傳輸控制」，才能允容許封包在 proxy 處理中來回傳輸，而不直接通過防火牆。

建議動作

按照 *IBM eNetwork Firewall 使用指南* 中所說明，架構 proxy 連線的每一半。

儘可能使用預先定義的服務程式，特別是對 FTP 資料傳輸更應如此。

無法連線至想要的主電腦

問題說明

如果資料在 proxy 處理中來回流動，但未連接主電腦，則您的從屬站可能無法正確分辨主電腦名稱。

建議動作

請確定已在**安全策略**對話框上啟用允許 DNS 查詢，而且已啟動您的連線架構。請參閱第67頁的『DNS 問題』，取得相關資訊。

問題說明

在防火牆中，由任一防火牆服務程式鑑證的每個使用者名稱，可被架構為要使用其中任一鑑證方法。Deny all 是用來禁止對該使用者使用某一個特定的 proxy。

建議動作

檢查「架構從屬站」上，**使用者**對話框中的使用者帳戶鑑證設定。

鑑證服務程式

無法鑑證 Windows NT 管理者帳戶

問題說明

Windows NT 管理者帳戶的防火牆屬性會儲存在 fwdadm 下的防火牆使用者資料庫中。

建議動作

請驗證 fwdadm 是否已為您試圖使用的服務程式設定正確的驗證方法。

無法鑑證防火牆 proxy 使用者

問題說明

如果防火牆 proxy 使用者是定義在防火牆使用者資料庫中，則 fwduser 名稱是用來定義使用者的屬性。

建議動作

請驗證 fwduser 的鑑證方法是否正確定義給您試圖存取的服務程式。

網路位址轉換

NAT 連線不作用

問題說明

已設定並啟動 NAT，但連線還是不作用。

建議動作

可能是路由表有問題，或是 NAT 架構問題。

如何為 NAT 封包建立路徑呢？

問題說明

沒有為 NAT 封包建立路徑。

建議動作

使用 NAT 位址的目的地或防火牆的閘道，將路由器上的靜態路徑新增在防火牆的前面。

有哪些可用的偵錯工具可以用來協助使用 NAT？

問題說明

有哪些可用的偵錯工具可以用來協助使用 NAT？

建議動作

「NAT 記載功能」可讓您追蹤管理動態登記的位址。

日誌機能

日誌機能變更在伺服器上沒有生效

問題說明

刪除或變更日誌機能時，它看起來似乎可在 GUI 上作用，但在伺服器上卻沒有生效。

建議動作

重新啟動您的系統。

報告公用程式

存取檔案時發生錯誤：

問題說明

在使用下列任一命令後，會看到上述錯誤：

```
db2 -vf fwschema.d11 > schema.out
           db2 -vf fwimport.dat > import.out
db2 -vf fwqrysmp.dml > sample.out
```

建議動作

提供 .ddl、.dat 或 .dml 檔的正確完整檔案名稱。

匯入資料至資料庫時發生錯誤。

問題說明

自 db2 -vf fwimport.dat>import.out 命令產生的 import.out 檔中有訊息指出其中的匯入作業失敗或僅部份成功。

建議動作

檢查相對於出現問題之匯入陳述式的 .msg 檔案。其將提供關於問題的詳細資訊。請查看對應 .tbl 檔的相關記錄以檢查輸入資料及判定問題所在。例如，資料庫中的目標直欄是否過長？目標直欄類型的資料類型是否合宜？如果輸入資料看似錯誤，您可能必須找出原始的日誌檔記錄來確定 fwlogtbl 正確地產生 .tbl 檔記錄。

若無法解決問題，請先儲存 import.out 檔、.msg 檔、相關的 .tbl 檔及原來的日誌檔，然後再連絡 IBM 服務人員。

附錄A. 訊息

此附錄包含 IBM Firewall for AIX 及 IBM Firewall for NT 的各自的訊息，以及這兩個防火牆共用的訊息。它也提供下列 IBM Firewall 訊息的相關資訊：

- 形成訊息的方式
- 訊息的嚴重性層次
- 訊息及其解釋

如果您已看過訊息及其解釋，但仍需要進一步資訊的話，請參閱第65頁的『第7章 疑難排解與測試』。

訊息標籤

- ICA** 前 3 個固定字元。
- xxxx** 範圍從 0000 - 9999 中的號碼。
- a** 嚴重性指標。訊息以嚴重性層次來分類。
- i - 參考用資訊
 - w - 警告
 - e - 錯誤
 - s - 嚴重

號碼 0000 - 9999 細分如下：

- 0000 - 0999 入侵警示
- 1000 - 1999 過濾器
- 2000 - 2999 Proxy
- 3000 - 3999 Socks
- 4000 - 4999 呼叫器
- 5000 - 8999 可使用的項目
- 9000 - 9999 一般/其他

訊息

ICA0001 警告 - 計數 個鑑證失敗。

解說： 已達鑑證失敗的臨界值條件。

ICA0002 警告 - 使用者 使用者名稱 已有 計數 次鑑證失敗。

解說： 已達偵測特定日誌訊息的臨界值條件。

ICA0003 警告 - 計數 來自主電腦 主電腦 IP 位址的鑑證失敗。

解說: 已達來自任何特定主電腦的鑑證失敗的臨界值條件。

ICA0004 警告 - 標籤 訊息 ID 具有 計數 個 日誌項目。

解說: 已達偵測特定日誌訊息的臨界值條件。

ICA0005 日誌監督程式 - 記憶體不足。

解說: 處理已將記憶體用盡。

ICA0006 日誌監督程式 - 無法存取服務程式檔案: 錯誤碼

解說: 在 /etc/services 中找不到 fwlogmond 的項目。

ICA0007 日誌監督程式 - 無法建立 socket : 錯誤碼

解說: 無法開啓 socket - 請參閱錯誤訊息。

ICA0008 日誌監督程式 - bind() 已失敗: 錯誤碼

解說: 無法連結 socket - 請參閱錯誤訊息。

ICA0009 無法開啓臨界值定義檔: 錯誤碼

解說: 存取臨界值定義檔時, 發生問題 - 請參閱錯誤訊息。

ICA0010 日誌監督程式 - 嚴重的讀取錯誤: 錯誤碼

解說: 從 socket 讀取資料時, 發生問題 - 請參閱錯誤訊息。

ICA0011 無法取得臨界值定義檔的狀態: 錯誤碼

解說: 存取臨界值定義檔時, 發生問題 - 請參閱錯誤訊息。

ICA0012 正在關閉日誌監督常駐程式。

解說: 常駐程式正在異常中止或已收到終止信號。先前的日誌訊息將提供詳細資訊。

ICA0013 日誌監督程式取得終止信號。

解說: 常駐程式已收到終止信號, 且將關閉。

ICA0014 啓動日誌監督常駐程式。

解說: 已啓動常駐程式。

ICA0015 無法為日誌監督建立常駐程式: 錯誤碼

解說: 無法建立常駐程式 - 請參閱錯誤訊息。

ICA0016 無法開啓 處理 ID 檔案 - 常駐程式可能已在使用中。

解說: 常駐程式無法開啓處理 id 檔。

ICA0017 無法將處理 id (處理 ID) 寫入 檔案。

解說: 常駐程式無法將處理 ID 寫入至檔案。

ICA0018 日誌監督程式 - 讀取不到任何資料。

解說: 收到沒有資料的封包 - 已捨棄。

ICA0019 日誌監督程式 - 短讀取。已捨棄標籤。

解說: 收到沒有足夠資料的封包 - 已捨棄。

ICA0020 日誌監督程式 - ICA 標籤格式不對。

解說： 收到的封包格式錯誤的資料 - 已捨棄。

ICA0021 日誌監督程式 - 鑑證資料格式不對。

解說： 收到的封包格式錯誤的資料 - 已捨棄。

ICA0022 臨界值定義檔中語法無效 (無效的輸入值)。

解說： 臨界值檔中所指出的項目發生語法錯誤。

ICA0023 無法開啓 fwmail.conf 檔案。

解說： 開啓 fwmail.conf 檔案失敗或檔案是空的

ICA0024 無法連線至 SMTP 伺服器。

解說： SMTP 伺服器忙線中或拒絕連線

ICA0025 警示訊息 Email 失敗。

解說： 無法將日誌監督程式警示訊息 E-mail 到指定位址。

ICA0051 保存在日誌檔 日誌檔名稱 的天數必須是無正負符號的短整數值。

解說： 保存在日誌檔的天數必須是有效的整數值。

ICA0052 保存在保存檔 日誌檔名稱 的天數必須是無正負符號的短整數值。

解說： 保存在保存檔的天數必須是有效的整數值。

ICA0053 一個日誌檔 日誌檔名稱 存在有多個項目在 logmgmt.cfg 是不被允許。

解說： 一個日誌檔有多個項目在 logmgmt.cfg 是不被允許。

ICA0054 無法開啓 \$ 變數：檔。

解說： 無法開啓 logmgmt.cfg 檔案。

ICA0055 logmgmt.cfg 檔無有效項目。

解說： logmgmt.cfg 檔無有效項目。

ICA0056 日誌訊息 "\$ 變數 : " 無效

解說： 日誌訊息無效

ICA1001 無法以我們的處理 ID 來建立檔案

解說： 寫入檔案 fwlogd.pid 時過濾器記載常駐程式發現錯誤。

使用者回應： 檢查目錄 /etc/security 常駐其中的檔案系統。可能空間不足。

ICA1002 無法與 cfgfilt 程式通信

解說： 由於沒有建立 fwlogd.pid 檔，所以 fwlogd 常駐程式和 cfgfilt 應用程式 (過濾控制所需) 之間無法通信。

使用者回應： 檢查目錄 /etc/security 常駐其中的檔案系統。可能空間不足。

ICA1003 繼續記載常駐程式起始設定

解說： fwlogd 常駐程式將繼續啟動處理。

ICA1004 已於 日期 時間 時，起始設定過濾器記載常駐程式 fwlogd (層次 版本. 版次)

解說： 已啟動 IP 封包記載常駐程式。如果啓用封包記載，常駐程式 fwlogd 會將所需的記錄寫入 syslog (local4 檔)。

ICA1005 因為緩衝區溢位，所以抑制 `filter_rule_no` 封包訊息的記載。

解說： `fwlogd` 常駐程式過濾日誌緩衝區已溢位。無法記載已指定過濾規則的封包。

使用者回應： 檢查日誌。您的防火牆可能被拒絕服務，或者您可能正在記載不必要的訊息。例如，廣播訊息必須有一條日誌控制設定為否 (l=n) 的拒絕規則，以避免填滿日誌。

ICA1006 嚴重的 `fwlogd` 錯誤 - 失敗的函數：錯誤訊息

解說： `fwlogd` 伺服器在所指出的函數中失敗，已終止常駐程式。

使用者回應： 請更正所指出的系統問題，並重新啟動 `fwlogd`。

ICA1007 無法分割子處理：錯誤碼

解說： 啟動過濾器記載常駐程式期間，發生所指出的系統錯誤。

使用者回應： 根據已顯示的錯誤，採取更正動作。

ICA1008 從 `setpggrp` 常式傳回的錯誤：錯誤碼

解說： 啟動過濾器記載常駐程式期間，發生所指出的系統錯誤。

ICA1009 無法分割衍生第二個子處理：錯誤碼

解說： 啟動過濾器記載常駐程式期間，發生所指出的系統錯誤。

ICA1010 必須有 `Root` 權限才能執行這個常駐程式

解說： 必須在 `Root` 權限之下才能啟動過濾器記載常駐程式

使用者回應： 以 `Root` 權限重新啟動。

ICA1011 查詢核心程式擴充 `load_path` 的 `sysconfig` 呼叫失敗：錯誤碼

解說： 啟動過濾器記載常駐程式期間，發生所指出的系統錯誤。

ICA1012 未載入 `AIX` 核心程式擴充 `netinet` -- 無法繼續

解說： `netinet` 裝置驅動程式未含過濾器支援。

使用者回應： 安裝「防火牆」字碼。可能已安裝字碼，但尚未重新開機。

ICA1013 `Socket` 建立呼叫失敗：錯誤碼

解說： 啟動過濾器記載常駐程式期間，發生所指出的系統錯誤。

ICA1014 `AIX` `netinet` 裝置驅動程式不在所要求的層次上

解說： `netinet` 裝置驅動程式和 `fwlogd` 常駐程式不是相同層次。

使用者回應： 解除這個衝突；在安裝新層次的「防火牆」後，可能需要重新開機。

ICA1015 在 `ioctl()` 呼叫 (`SIOCGFWLOG`) 上發生錯誤：錯誤碼

解說： 啟動過濾器記載常駐程式期間，發生所指出的系統錯誤。

ICA1016 無法取得現行擱置的日誌佇列

解說： 日誌訊息之前緊連著其他資訊。

ICA1017 從 `SIOCGFWLOG` `ioctl()` 呼叫傳回錯誤

解說： 啟動過濾器記載常駐程式期間，發生所指出的系統錯誤。

ICA1018 嚴重的 fwlogd 錯誤 - 失敗的函數：系統錯誤訊息

解說：fwlogd 伺服器在所指出的函數中失敗，已終止常駐程式。

使用者回應：請更正所指出的系統問題，並重新啟動 fwlogd。

ICA1019 異常錯誤結束，rc
internal_fw_return_code

解說：啟動過濾器記載常駐程式期間，發生所指出的系統錯誤。

ICA1020 嚴重的 fwlogd 錯誤 - 失敗的函數：回覆碼 = 0x 函數回覆碼

解說：fwlogd 伺服器在所指出的函數中失敗，已終止常駐程式。

使用者回應：請更正所指出的系統問題，並重新啟動 fwlogd。

ICA1021 開啓 /dev/ipsppoif 時，發生錯誤：錯誤碼

解說：未安裝指定的裝置驅動程式。

使用者回應：若已安裝「防火牆」字碼，請檢查 /tmp/rc/net.out 檔，找出可能的錯誤訊息。

ICA1022 無法驗證過濾器支援

解說：在這個訊息之前已產生錯誤記錄，因此無法驗證過濾器支援。

ICA1023 在 ioctl() 呼叫 (SIOCGFWLVL) 上發生錯誤：錯誤碼

解說：啟動過濾器記載常駐程式期間，發生所指出的系統錯誤。

使用者回應：請執行下列其中一項：

- 若為 AIX：請驗證是否已安裝正確層次的「防火牆 netinet」裝置驅動程式，且在安裝後，是否已重新開機。
- 若為 OS/390：:p.請驗證是否已安裝正確層次的 TCP/IP，且是否以 IPCONFIG FIREWALL 架構陳述式來啟動。

ICA1024 寫入檔案 /etc/security/fwlogd.pid 時，發生錯誤：錯誤碼

解說：由於指出的系統錯誤碼，所以 fwlogd 無法寫入指定檔案。

使用者回應：更正指出的問題，然後重新啟動過濾器記載常駐程式。

ICA1032 已於 日期, 時間，更新過濾規則

解說：已更新 IP 封包過濾規則。

ICA1033 已於 日期, 時間，起始設定過濾支援 (層次版本.版次)

解說：已起始設定防火牆過濾器支援。

ICA1034 已於 日期, 時間 時，停止過濾支援

解說：IP 封包過濾處理目前正在使用預設的過濾規則，而非使用 /etc/security/filters.cfg 檔案中所定義的規則。

ICA1035 已於 日期, 時間，將封包記載狀態設定為啓用/停止

解說：已變更封包記載狀態。訊息指出時間戳記的現行狀態。

ICA1036 *#:rule_noR: rule_type 方向： 介面
s:src_addr d: dst_addr p: 通訊協定
標籤： scr_port/icmp_type tag:
dst_port/icmp_code r:已遞送/本端 a:
secure/non_secure f:yes/no T:tunnel_id
e:C/D/n l:packet_length*

解說： 日誌記錄指出所處理的 IP 封包及其符合的過濾規則。若要寫入此記錄，該符合的過濾規則的日誌控制必須設定為 yes。如果符合此規則的 IP 封包是一個片段，就會顯示表頭封包的 ports/icmp type/code 資訊，但如果不是表頭封包，則會顯示零。

ICA1037 *#:rule_no action src_addr src_mask
dst_addr dst_mask 通訊協定
logical_op value logical_op value
interface_type 遞送方向l= log_control
f=fragment_controlt= tunnel_ID
enc_alg auth_alg*

解說： 當更新過濾規則時，會將已啟動的規則寫入日誌。 這個日誌訊息說明其中一條已啟動的規則。

ICA1038 已啟動「階段作業密碼鎖」引擎，使用階段作業 **socket** 連接埠：埠號
與主要 **socket** 連接埠 埠號

解說： 如 /etc/services 上的定義，使用指定的 UDP 連接埠號碼啟動加密通道。

ICA1039 策略已 (重新) 定義為：

解說： 策略快取已使用 /etc/security/fwpolicy 檔案來 (重新) 定義。下列字行會顯示新的策略快取。

ICA1040 >策略陳述式： *tunnel_origin
tunnel_end tunnel_ID
encrypt_flag/authenticate_flag*

解說： 所記錄的字行讀取自 /etc/security/fwpolicy 檔案。

ICA1041 已為通道通道 ID 刪除範圍設定 >

解說： 已列出之 ID 的通道範圍不再有效。

ICA1042 已定義下列通道範圍設定：

解說： 如下列日誌記錄所列示，定義通道範圍設定。

ICA1043 >tunnel_ID:數字, src_addr:IP 位址, dst_addr:IP 位址, 加密: 演算法

解說： 訊息列示已啟動通道範圍的特定屬性。

ICA1044 主電腦計數器警告：IP(IP 位址) 超出限制

解說： 試圖與「防火牆」機器連線的安全主電腦太多

系統動作： 傳遞連線

ICA1045 TCP 超出限制：IP 位址(連接埠)->IP 位址(連接埠) 已被拒絕

解說： 通過「防火牆」機器的 TCP 階段作業太多

系統動作： 拒絕連線

ICA1046 UDP 超出限制：IP 位址(連接埠)->IP 位址(連接埠) 已被拒絕。

解說： 通過「防火牆」機器的 UDP 階段作業太多

系統動作： 拒絕連線

ICA1047 寬限期警告：已傳遞過多的 TCP 階段作業，IP 位址(連接埠)->IP 位址(連接埠)

解說： 通過「防火牆」機器的 TCP 階段作業太多

系統動作： 傳遞連線

ICA1048 寬限期警告：已傳遞太多 UDP 階段作業，IP 位址(連接埠)->IP 位址(連接埠)

解說： 通過「防火牆」機器的 UDP 階段作業太多

ICA1049 無效的 ipsec 套裝軟體：s:IP 位址 d:IP 位址 通訊協定：通訊協定 spi: 安全性參數索引

解說： 正在接收的防火牆無法解開 ipsec 套裝軟體的封裝。

使用者回應： 請確定通道定義已正確匯出，並且已在每一個防火牆上啟動。

ICA1050 已為通道 *tunnel_ID* 刪除設定

解說： 已列出之 ID 的通道設定不再有效。

ICA1051 已定義下列通道設定：

解說： 如下列日誌記錄所列示，定義通道設定。

ICA1052 >tunnel_ID:號碼,
src_addr:IP_address,
dst_addr:IP_address, src_enc:演算法
rem_enc:演算法 src_mac:演算法
rem_mac:演算法 src_enc_mac:
演算法 rem_enc_mac:演算法
src_pol:策略 rem_pol:策略 模態：
transport_mode

解說： 訊息列示已啟動通道的特定屬性。

ICA1200 由於上述錯誤而終止記載常駐程式

解說： 由於這個訊息前面所記錄的錯誤，因此終止 fwlogd 常駐程式。

系統動作： 不啟動 IP 過濾器記載。

使用者回應： 更正所指出的錯誤，並重新啟動 fwlogd。

ICA1260 於 日期, 時間 終止過濾記載常駐程式，因為收到 *termination* 信號所致

解說： fwlogd 常駐程式接收到指定的終止信號而停止。

ICA1305 \不明["]

解說： 替 syslog 製作 IP 封包的格式時，發現不明通訊協定規格的記錄。可辨識的通訊協定為 IP、ICMP、TCP、UDP 與 IPSP。請注意，IPSP 是 IBM 設計來透過通道傳遞加密封包。

ICA1400 嚴重的 fwtimernat 錯誤 - 失敗的函數：系統錯誤訊息

解說： fwtimernat 伺服器在所指出的函數中失敗，已終止 fwtimernat 伺服器。

使用者回應： 請更正所指出的系統問題，並重新啟動 fwtimernat。

ICA1401 嚴重的 fwtimernat 錯誤 - 失敗的函數：回覆碼 = 0x 函數回覆碼

解說： fwtimernat 伺服器在所指出的函數中失敗，已終止 fwtimernat 伺服器。

使用者回應： 請更正所指出的系統問題，並重新啟動 fwtimernat。

ICA1402 嚴重的 fwtimernat 錯誤 - 失敗的函數：錯誤訊息

解說： fwtimernat 伺服器在所指出的函數中失敗，已終止 fwtimernat 伺服器。

使用者回應： 請更正所指出的系統問題，並重新啟動 fwtimernat。

ICA2000 從 IP 位址 (非安全站台) 傳送新的 FTP 階段作業至 IP 位址。

解說： 正從非安全站台啟動新的 FTP 階段作業。

ICA2001 鑑證失敗，因 *net ftp* 的使用者 名稱 (不明)：IP 位址。

解說：一位沒有帳戶的使用者嘗試從網路上使用 FTP proxy。

使用者回應：請連絡您的防火牆管理者設定 proxy 帳戶。

ICA2002 使用者 名稱 的鑑證失敗，鑑證方法 為 網路：主電腦名稱 的 鑑證方法。

解說：「防火牆」無法使用指定的鑑證方法來鑑證指示的使用者名稱。

使用者回應：請洽詢您的「防火牆」管理者。

ICA2003 沒有 shell 是針對 使用者名稱 而架構的。

解說：已識別的使用者嘗試 proxy 登入，但沒有定義登入 shell。

使用者回應：請洽詢「防火牆」管理者，更正這個使用者登入設定檔。

ICA2004 收到不明的審核事件 *0xhex_value*。

解說：模組 tcpip_audit.c 接收到一不明審核要求。

ICA2005 將資料寫入從屬站時，發生錯誤：錯誤碼。

解說：無法與從屬站通信；請查看記載的系統訊息。

ICA2006 *ptelnetd: auditproc:* 錯誤碼。

解說：telnet 審核處理傳回指定錯誤。系統檔案的潛在訛誤。

ICA2007 *ptelnetd:* 緊急狀況=參數值。

解說：偵測到不明錯誤。系統檔案的潛在訛誤。

ICA2008 來自：IP 位址 而使用 telnet 進入 的非防火牆使用者 名稱。

解說：沒有防火牆帳戶的使用者嘗試使用 telnet proxy。

系統動作：假設已使用「一般鑑證」。

ICA2009 */bin/login:* 錯誤碼。

解說：系統登入期間發生嚴重錯誤。請參閱指出的系統錯誤訊息。

ICA2010 從 IP 位址 (非安全) 連線至 IP 位址。

解說：透過非安全性介面已成功建立指定 IP 位址之間的連線。

ICA2011 從 IP 位址 (安全) 連線至 IP 位址。

解說：透過安全性介面已成功建立指定 IP 位址之間的連線。

ICA2012 從 IP 位址 (安全站台) 傳送到 IP 位址 的新 FTP 階段作業。

解說：正在啟動新的 FTP 階段作業。

ICA2013 從 IP 位址 傳送到 IP 位址 的新 Telnet 階段作業。

解說：已建立新的 Telnet 階段作業。

ICA2014 不支援選項 *value*。

解說：不支援所指出的旗號，請參閱先前的訊息。

ICA2015 不支援選項 *-value*。

解說：不支援所指出的旗號，請參閱先前的訊息。

ICA2016 遠端使用者 ID \ "名稱"。

解說: 所指定之使用者的 FTP 連線要求。

ICA2017 偵錯 - 在 行數。

ICA2018 找不到使用者 名稱 的 SNK 密碼鎖。

解說: 找不到所指定之使用者 ID SecureNetKey 值。

使用者回應: 請與「防火牆管理者」連絡, 找出可能的登入架構問題。

ICA2019 未正確讀取使用者 名稱 的 SNK 密碼鎖。

解說: 無法將 SecureNetKey 值讀取為所指定之使用者 ID 的八進位數值。

使用者回應: 請與「防火牆管理者」連絡, 找出可能的登入架構問題。

ICA2020 /usr/bin/fwuserau 或 /usr/bin/fwuserpt 不存在。

解說: 所使用使用者提供的鑑證方法已異常中止。

系統動作: 鑑證已異常中止。

使用者回應: 確定有 /usr/bin/fwuserau 及 /usr/bin/fwuserpt 存在, 且擁有者是 root。如果執行檔不存在, 使用者必須使用與防火牆作業系統相容的編譯器, 來產生執行檔, 然後將其名稱指定為 /usr/bin/fwuserau 或 /usr/bin/fwuserpt。

ICA2021 正在嘗試以使用者 ID 名稱, 連線至遠端主電腦 名稱。

解說: 正在嘗試建立新的 FTP 連線。

ICA2022 正嘗試連線到遠端主電腦 名稱。

解說: 正在嘗試建立新的 FTP 連線。

ICA2023 用法: ptelnetd [-n] [-s]。

解說: 啟動 ptelnet 常駐程式時指定不明旗號。

使用者回應: 僅使用旗號 -n 及/或 -s。

ICA2024 已順利使用 方法 鑑證方法, 從 網路: 主電腦名稱 中, 鑑證使用者 名稱。

解說: FW 已使用指定的鑑證方法, 確認指出的使用者名稱。

ICA2025 使用者 名稱 已順利使用 方法 鑑證方法, 從 網路: 主電腦名稱 中登入。

解說: FTP 使用者已登入。

ICA2026 經過 n 秒後, 使用者 名稱 已在 目前時間 發生逾時。

解說: 指定使用者的連線嘗試逾時。可能是網路遞送問題或是無法使用遠端主電腦。

ICA2027 於 時間 從 遠端主電腦 連線。

解說: 已與「防火牆」建立 Net FTP 連線。

ICA2028 已經拒絕從 IP 位址 到 IP 位址 的 FTP 連線。此機器不支援從非安全站台 FTP 連線。

解說: 一般說來, 這表示嘗試通過非安全介面來與「防火牆」建立 FTP 連線。

系統動作: 拒絕連線。

ICA2029 系統錯誤, 錯誤碼 = - 在 位置 第 行號 行。

解說: 執行系統呼叫時, 系統呼叫發生問題。

系統動作: 系統執行終止

使用者回應: 請取得日誌，找出錯誤號碼的意義，然後設法解決問題。若無法解決此問題，請連絡 IBM 服務人員。

ICA2030 **函數呼叫，回覆碼 = - 在 位置 第 行號 行。**

解說: 函數呼叫發生問題。

系統動作: 傳回錯誤

使用者回應: 取得日誌，了解回覆碼並嘗試解決此問題。若無法解決此問題，請連絡 IBM 服務人員。

ICA2031 **sdi 函數呼叫 creadcfg() rc = -。**

解說: 函數呼叫發生問題。

系統動作: 傳回錯誤

使用者回應: 請參閱 sdi 參考手冊的說明。

ICA2032 **失去連線。**

解說: 失去 FTP 連線。

使用者回應: 重新建立階段作業。

ICA2033 **sdi 函數呼叫 sd_init rc = -。**

解說: 函數呼叫發生問題。

系統動作: 傳回錯誤

使用者回應: 請參閱 sdi 參考手冊的說明。

ICA2034 **sdi 函數呼叫 sd_check rc = -。**

解說: 函數呼叫發生問題。

系統動作: 傳回錯誤

使用者回應: 請參閱 sdi 參考手冊的說明。

ICA2035 **setsockopt(): 錯誤訊息代碼。**

解說: setsockopt 呼叫上的系統錯誤。

ICA2036 **已為使用者 使用者 ID 啟動 Telnet 階段作業 階段作業 ID (來源 IP 位址:目的 IP 位址)。**

解說: 在啟動每一個 Telnet 階段作業時，均會產生訊息。當使用者 ID、來源 ip 與目的地 ip 防火牆都認識時，即開始階段作業。階段作業 ID 是防火牆所產生的唯一識別碼。

ICA2037 **使用者 fwdfuser 或 fwdpuser 已嘗試登入，但不被容許。**

解說: fwdfuser 與 fwdpuser 為保留的使用者，不可以使用。

系統動作: 已拒絕登入。

使用者回應: 管理者應該調查誰正在使用這個使用者名稱。

ICA2038 **ttloop: 同層級處理已停止：錯誤碼。**

解說: 沖寫網路輸出緩衝區時，發生錯誤。同層級處理停止。

ICA2039 **ttloop: 讀取：錯誤碼。**

解說: 沖寫網路輸出緩衝區時，發生錯誤。

ICA2040 **使用者 ID fwdfuser 不能讓鑑證設定成 password、none 或 snk。**

解說: fwdfuser 為已保留的使用者 ID，不可使用 password 或 none 來作為鑑證方法。

系統動作: 已拒絕登入。

使用者回應: 管理者應該變更使用者 ID fwdfuser 的鑑證方法。

ICA2041 已啟動 使用者 ID 的 FTP 階段作業
階段作業 ID (來源 IP 位址;目的 IP
位址)。

解說: 在啟動每一個 FTP 階段作業時, 均會產生訊息。當使用者 ID、來源 ip 與目的地 ip 防火牆都認識時, 即開始階段作業。階段作業 ID 是防火牆所產生的唯一識別碼。

ICA2042 req_rsp_code 已誤設為
FW_AUTH_REQ。

解說: 不容許 fw_tn_authenticate 將 req_rsp_code 設定為 FW_AUTH_REQ。

系統動作: 終止鑑證。

使用者回應: 變更 fw_tn_authenticate, 重新製作 (make) 程式庫 fwuser.o, 然後將它放入「防火牆」中。

ICA2043 無法取得 使用者名稱 的通行碼。

解說: 這個使用者的鑑證類型是「通行碼」, 但找不到任何通行碼。

使用者回應: 請洽詢您的「防火牆」管理者。

ICA2044 -t 時間指定錯誤 (值)。

解說: 所顯示的時間值含有在數值範圍 0 至 9 外的字元, 或超出所容許的最大值。

ICA2045 防火牆不支援選項 -T。

解說: 不支援指示的選項。

ICA2046 防火牆不支援選項 -k。

解說: 不支援指示的選項。

ICA2047 防火牆不支援選項 -s。

解說: 不支援指示的選項。

ICA2048 防火牆不支援選項 -u。

解說: 不支援指示的選項。

ICA2049 旗號 -參數值 不明, 不予處理。

解說: 已指示的旗號, 但無法辨識該旗號。

ICA2050 參數 參數值 不明。

解說: 無法辨識指定為選項的值。

ICA2051 位址的 adapt_addr 轉換錯誤。

解說: 已顯示的 IP 位址是無效的。

使用者回應: 可能是 /etc/security/fwsecadpt.cfg 檔案的訛誤。請移除檔案, 重新架構您的安全介面, 然後重新起始設定過濾器。

ICA2052 afopen 無法開啓
/etc/security/login.cfg: 錯誤碼。

解說: 無法鑑證使用者; 所指定的檔案發生開啓錯誤。

ICA2053 無法開啓安全介面檔。

解說: 尚未架構安全性介面。

使用者回應: 如果必須定義安全介面, 請使用「防火牆」命令/smit 畫面來定義安全介面。

ICA2054 enduserdb rc=值, 錯誤碼。

解說: 當嘗試擷取使用者登入設定檔資訊時, 收到所指出的系統錯誤碼。

使用者回應: 請與您的「防火牆管理者」連絡, 以驗證您的登入帳戶。

ICA2055 getpeername() (呼叫名稱): 錯誤
碼。

解說: 當 FTP 常駐程式試圖取得 socket 名稱時, 發生系統錯誤。

ICA2056 **t)esockme()** (呼叫名稱): 錯誤碼。

解說: 當 FTP 常駐程式試圖取得連接埠名稱時，發生系統錯誤。

ICA2057 使用者 ID 的 **getuser** 非安全
Shell rc=值, 錯誤碼。

解說: 試圖從「防火牆」的非安全端擷取連線的 Shell 名稱時，收到所指出的系統錯誤碼。

使用者回應: 請與您的「防火牆管理者」連絡，為您的使用者登入設定檔設定一個 shell。

ICA2058 使用者 ID 的 **getuser** 安全 shell
rc=值, 錯誤碼。

解說: 試圖從「防火牆」的安全端擷取連線的 Shell 名稱時，收到所指出的系統錯誤碼。

使用者回應: 請與您的「防火牆管理者」連絡，為您的使用者登入設定檔設定一個 shell。

ICA2059 **ioctl()**: 錯誤碼

解說: 在 SIOCSPGRP 的 ioctl() 呼叫上，發生系統錯誤。

ICA2060 **ptelnetd: ftok** 要求共用的記憶體失敗。

解說: 無法配置共用記憶體區段。

使用者回應: 請與「防火牆管理者」連絡，很顯然這是記憶體的問題。

ICA2061 **ptelnetd: shmat** 要求共用的記憶體失敗。

解說: 無法配置共用記憶體區段。

使用者回應: 請與「防火牆管理者」連絡，很顯然這是記憶體的問題。

ICA2062 **ptelnetd: shmget** 要求共用的記憶體失敗。

解說: 無法配置共用記憶體區段。

使用者回應: 請與「防火牆管理者」連絡，很顯然這是記憶體的問題。

ICA2063 **setsockopt()** (SO_DEBUG): 錯誤碼。

解說: 所指出的錯誤訊息是由叫做 'setsockopt' 的系統傳回。

ICA2064 **setsockopt()** (SO_KEEPAIVE): 錯誤碼。

解說: 所指出的錯誤訊息是由叫做 'setsockopt' 的系統傳回。

ICA2065 **setuser rc=值**, 錯誤碼。

解說: 因上述原因，所以收到系統呼叫的不正確回覆碼。

ICA2066 **signal()**: 錯誤碼。

解說: 當 FTP 常駐程式試圖建立信號處理器時，發生系統錯誤。

ICA2067 嚴重的 **pftpd** 起始設定錯誤 -
bind(): 錯誤碼

解說: pftpd 伺服器起始設定失敗，已終止常駐程式。

使用者回應: 請更正所指出的系統問題，並重新啟動 pftpd。這個錯誤的最可能原因是另一個 FTP 常駐程式已在標準 FTP 連接埠 (21) 上進行傾聽。

ICA2068 嚴重的 **pftpd** 起始設定錯誤 -
listen(): 錯誤碼

解說: pftpd 伺服器起始設定失敗，已終止常駐程式。

使用者回應: 請更正所指出的系統問題, 並重新啟動 pftpd。

ICA2069 嚴重的 pftpd 錯誤 - 主要 accept(): 錯誤碼

解說: pftpd 伺服器的主要常式失效, 已終止常駐程式。

使用者回應: 請更正所指出的系統問題, 並重新啟動 pftpd。

ICA2070 嚴重的 pftpd 起始設定錯誤 - socket(): 錯誤碼

解說: pftpd 伺服器起始設定失敗, 已終止常駐程式。

使用者回應: 請更正所指出的系統問題, 並重新啟動 pftpd。

ICA2071 連線拒絕, 已達最大連線數。

解說: pftpd 伺服器無法建立另一個 FTP 階段作業, 因為已達階段作業的最大限制數。

系統動作: 拒絕連線。

使用者回應: 請等現存的連線結束後, 再重試要求。

ICA2072 無法使用 ftp 架構檔 (檔案名稱)。

解說: FTP 常駐程式嘗試開啓所指定的 FTP 架構檔, 但檔案不是不存在, 就是無法開啓。

系統動作: FTP 常駐程式處理使用預設架構。

使用者回應: 無; 除非檔案應該存在。若是檔案應該存在, 即須建立檔案, 或將檔案移至訊息中所指定的位置。

ICA2073 無法取得 FTP 語言表格的儲存體。

解說: 無法取得代表 FTP 架構檔中的 REPLYLANGUAGE 陳述式所需的儲存體。

系統動作: 繼續進行處理。

使用者回應: 在架構檔中增加區域大小或減少項目。

ICA2074 FTP 架構陳述式的處理已完成: 架構陳述式

解說: FTP 已處理所指出的架構陳述式。

系統動作: 繼續進行處理。

使用者回應: 無

ICA2075 使用者 ID 的 FTP (來源 IP 位址: 目的 IP 位址), 作業 檔案名稱, 位元組數 個位元組。 sid: 階段作業 id。

解說: 開啓 FTP 階段作業時對每個檔案傳送產生此訊息。sid 是防火牆在階段作業啓動時, 所產生的唯一識別碼。

ICA2076 使用者 id 的 FTP 階段作業 階段作業 id (來源 IP 位址: 目的 IP 位址) 已經結束, 歷時 歷時 秒, 位元組數 個位元組。

解說: 每個 FTP 常駐程式階段作業結束時產生此訊息。sid 是防火牆在階段作業啓動時, 所產生的唯一識別碼。

ICA2077 使用者 ID 的 Telnet 階段作業 階段作業 ID (來源 IP 位址: 目的 IP 位址), 位元組數 個位元組。

解說: 每個 Telnet 階段作業結束時產生此訊息。sid 是防火牆在階段作業啓動時, 所產生的唯一識別碼。

ICA2078 已經中斷 proxy 使用者 使用者 - 閒置了 時間 分鐘。

解說: 使用者的階段作業已超過最大容許閒置時間。

ICA2079 **注意 - 未經授權便試圖從 IP 位址連線至 IP 位址。**

解說: 一般說來，這表示嘗試透過非安全介面來建立與 Firewall 的連線。

系統動作: 拒絕連線。

ICA2080 **FTP 架構檔第 行數 行中，靠近直欄直欄 的語法錯誤 (原因): 架構陳述式**

解說: 位在指定行的 FTP 架構陳述式有錯誤。系統將提供發生錯誤的理由與偵測到該錯誤的位置。

系統動作: 陳述式已被忽略。

使用者回應: 請更正 FTP 架構檔中的陳述式。

ICA2081 **FTP 架構陳述式提供的訊息目錄無法使用。**

解說: 試圖開啓 REPLYLANGUAGE FTP 架構陳述式所提供訊息目錄失敗。沒有從屬站訊息目錄可以使用。

系統動作: 從屬站訊息目錄被迫為 C 目錄中的英文。

使用者回應: 請確定在與 FTP 架構 REPLYLANGUAGE 陳述式中的語言目錄相關的每一個目錄中，均有目錄檔。亦請檢查是否已正確設定 NLSPATH 環境變數，以容許替代來自 LANG 環境變數與目錄名稱 (%N) (%L) 的次目錄。

ICA2082 **無法將 ftp LANG 環境變數設定為子目錄名稱, 原因: 原因**

解說: 當 FTP 常駐程式試圖將 LANG 環境變數的設定變更為所指定的次目錄時，發生系統錯誤 (「原因」所提供的錯誤)。

系統動作: 繼續進行處理。恢復可能會產生其他訊息。

使用者回應: 使用所提供的理由，決定這是系統錯誤或程式設計錯誤。

ICA2083 **無法開啓 子目錄名稱 目錄中的 ftp 從屬站訊息目錄，原因: 原因**

解說: ftp 常駐程式無法開啓指定次目錄中的訊息目錄。所給與的理由是從 catopen() 傳回的錯誤號碼。

系統動作: 繼續進行處理。恢復可能會產生其他訊息。

使用者回應: 請確定在目錄中有一個與所提供的語言目錄相連結的目錄。請檢查是否已正確設定 NLSPATH 環境變數，以容許替代次目錄 (%L) 與目錄名稱 (%N)。

ICA2084 **強制透過 C 子目錄將 FTP 從屬站訊息目錄設成英文。**

解說: 因為先前列示的錯誤，ftp 常駐程式已使用 C 次目錄，迫使從屬站訊息目錄以英文顯示。

系統動作: 如果語言可以被迫成為 C 訊息目錄，則處理將繼續；否則，程式將跳出。

使用者回應: 請更正先前訊息的錯誤。如果程式亦存在，請在 C 次目錄中建立訊息目錄，並正確設定 NLSPATH 環境變數。

ICA2085 **pid 處理 ID (來源 IP 位址) 的 Telnet 階段作業已經結束。**

解說: 每個 Telnet 階段作業結束時產生此訊息。

ICA2086 **使用者檔案架構錯誤: 使用者 使用者 沒有密碼鎖 (密碼鎖)。**

解說: ftpd 已在使用者檔案中找到所要求的使用者，但找不到密碼鎖 - 架構了錯誤的使用者檔案。

使用者回應: 請使用「防火牆」命令/smit 畫面，來更正這個問題。

ICA2087 **ftpd 在使用者架構檔中，找不到所指定的使用者 使用者名稱。**

解說: 所指定的使用者名稱尚未架構，或 user.cfg 檔已損毀。

使用者回應： 請使用「防火牆」命令/smit 畫面，來更正這個問題。

ICA2088 ftpd 無法開啓使用者架構檔。

解說： ftpd 對 fopen 所做的呼叫已失敗，因為它無法開啓使用者架構檔。

使用者回應： 確定使用者架構檔 (依據預設值，指的是 user.cfg) 可供使用；請使用「防火牆」命令/smit 畫面

ICA2089 在表格 (struct tab2 authtab[]) 中，找不到任何與使用者檔案的授權類型 (授權類型) 相符的項目。

解說： 所指定使用者的權限類型 (從 user.cfg 傳回的) 不符合任何支援的類型 (如 deny、none、snk、sdi、password 等。)

使用者回應： 請檢查 user.cfg 檔的完整性或架構；使用「防火牆」命令/smit 來更正這個問題。

ICA2090 使用者 '使用者名稱' 無法通過 從屬站 IP 的鑑證，原因是 KEY=DENY 在 user.cfg 檔案中。

解說： 鑑證已失敗，因為「防火牆」管理者所設定的 user.cfg 檔案規格所致。

使用者回應： 請洽詢您的「防火牆」管理者。

ICA2091 不容許使用者 '使用者名稱' ftp 至非安全連接埠 (防火牆 IP)。

解說： 使用者嘗試利用 FTP 透過非安全連接埠 (nsp) 來進入防火牆伺服器 - 所有 nsp 使用者都必須正確地將 'fwnsftp' 密碼鎖架構為有效的權限類型 (在 user.cfg 檔中)。

使用者回應： 請檢查 user.cfg 檔的完整性或架構；使用「防火牆」命令/smit 來更正這個問題。

ICA2092 內部錯誤：nt_gwauth() 失敗。

解說： nt_gwauth() 通常會傳回下列三個值之一 (AUTHENTICATED、NOT_AUTHENTICATED 或 DENY) 在這個案例中，nt_gwauth 傳回了一些無效的整數。

ICA2093 不容許使用者 '使用者名稱' FTP 至安全連接埠 (埠號)。

解說： 使用者嘗試透過安全連接埠 (sp) 用 FTP 進入防火牆伺服器 - 所有 sp 使用者必須正確地將他們的 'fwsftp' 密碼鎖架構為有效的權限類型 (在 user.cfg 檔中)。

使用者回應： 請檢查 user.cfg 檔的完整性或架構；使用「防火牆」命令/smit 來更正這個問題。

ICA2094 登入失敗：預期的格式："PASS <通行碼>" 在 "USER <使用者名稱>" 後面；收到 無效的命令。

解說： 鑑證失敗，因為 FTP 從屬站未傳送預期的格式 (每一 RFC959 要有一個 PASS '通行碼')。

使用者回應： 輸入 "user <username>"；輸入正確的通行碼。請洽詢您的「防火牆」管理者。

ICA2095 登入失敗：(透過 鑑證方法 方法) 使用者 '使用者名稱' 無法通過 從屬站 IP (從屬站站台) 的鑑證。

解說： 鑑證失敗，因為輸入無效 (由從屬站所輸入的值來指定鑑證類型) - 例如使用者輸入無效的通行碼、snk 密碼鎖等。

使用者回應： 請洽詢您的「防火牆」管理者。

ICA2096 已鑑證：(使用的方法為 鑑證方法) 使用者 '使用者名稱' 已經通過 從屬站 IP (從屬站站台) 的鑑證。

解說： 已順利鑑證

ICA2097 **httpd --> 正在啓動 HTTP proxy 伺服器版本 HTTP Proxy 版本。**

解說: 正在啓動 WWW 存取的 HTTP Proxy 。

ICA2098 **httpd --> 正在關閉 HTTP proxy 伺服器。**

解說: 正在關閉 WWW 存取的 HTTP Proxy 。

ICA2099 **httpd --> 狀態: <HTTP 狀態碼>; 從屬站 <IP 位址>要求<" HTTP GET 要求">; <位元組數>個位元組。**

解說: 透過 proxy 進行從屬站 HTTP 要求某些檔案的狀態。「狀態」編碼值的相關資訊,請參閱 HTTP 1.0(RFC 1945) 或 HTTP 1.1(RFC 2068) 說明文件 (或是替代的 RFC), 您可以在 Internet 上的各種站台找到這些文件, 包括 ds.internic.net 。

ICA2100 **Socket 位址等於零。**

解說: 在區域要求中, 發現無效的目的地位址。

ICA2101 **Socket 位址系列錯誤: *sin_family_type* 。**

解說: 在區域要求中, 找到無效的位址系列類型。

ICA2102 **起始設定 odm 時, 發生錯誤: *odm* 錯誤碼。**

解說: 發生了 ODM (物件資料管理系統) 的 *odm_initialize()* 錯誤。

ICA2103 **設定 odm 預設路徑時, 發生錯誤: *odm* 錯誤碼。**

解說: 發生了 ODM (物件資料管理系統) 的 *odm_set_path()* 錯誤。物件類別, OCSvhost 。

ICA2104 **鎖定 odm 資料庫時, 發生錯誤: *odm* 錯誤碼。**

解說: 發生了 ODM (物件資料管理系統) 的 *odm_lock()* 錯誤。

ICA2105 **開啓 odm 物件 自訂的屬性 時, 發生錯誤: *odm* 錯誤碼。**

解說: 發生了 ODM (物件資料管理系統) 的 *odm_open_class()* 錯誤。

ICA2106 **搜尋 odm 物件 OCS 虛擬主電腦 時, 發生錯誤: *odm* 錯誤碼。**

解說: 發生了 ODM (物件資料管理系統) 的 *odm_get_first()* 錯誤。物件類別, OCSvhost 。

ICA2107 **關閉 odm 物件 OCS 虛擬主電腦 時, 發生錯誤: *odm* 錯誤碼。**

解說: 發生了 ODM (物件資料管理系統) 的 *odm_close_class()* 錯誤。物件類別, OCSvhost 。

ICA2108 **解除鎖定 odm 資料庫時, 發生錯誤: *odm* 錯誤碼。**

解說: 發生了 ODM (物件資料管理系統) 的 *odm_unlock()* 錯誤。

ICA2109 **終止 odm 時, 發生錯誤: *odm* 錯誤碼。**

解說: 發生了 ODM (物件資料管理系統) 的 *odm_terminate()* 錯誤。

ICA2110 **依據名稱取得伺服器時, 發生錯誤: 錯誤碼。**

解說: 發生了 *getservbyname()* 錯誤。在 /etc/services 檔中, 未正確指定主電腦「登入監督程式」服務程式 *lm* 。

ICA2111 **byname() 錯誤：錯誤碼。**

解說： 發生了 gethostbyname() 錯誤。在 /etc/hosts 中，未正確指定主電腦機器名稱。

ICA2112 **通訊協定名稱無效：通訊協定名稱。**

解說： 不支援 ODM 物件類別 OCSvhost 中所指定的通訊協定名稱。

ICA2113 **開啓 socket 至 LM 時，發生錯誤：錯誤碼。**

解說： 在「登入監督程式」常駐的主電腦機器中，發生 socket() 錯誤。

ICA2114 **連結區域位址時，發生錯誤：錯誤碼。**

解說： 使用這個 OCS 節點的區域位址時，發生 bind() 錯誤。

ICA2115 **將 socket 連線到 LM 時，發生錯誤：錯誤碼。**

解說： 在「登入監督程式」常駐的主電腦機器中，發生 connect() 錯誤。

ICA2116 **通訊協定類型錯誤：通訊協定類型。**

解說： 用來與主電腦「登入監督程式」通信的虛擬終端機通訊協定類型無效。

ICA2117 **LM 訊息發生 Malloc 錯誤。**

解說： 以動態方式配置可變長度「登入監督程式」訊息的空間時，發生了 malloc() 錯誤。

ICA2118 **傳輸訊息至 LM 時，發生錯誤：錯誤碼。**

解說： 當傳送一個要求給「登入監督程式」，要求開啓正確的主電腦裝置時，發生了 send() 錯誤。

ICA2119 **從 LM 接收到訊息時，發生錯誤：錯誤碼。**

解說： 當「登入監督程式」傳回認可時，發生了 recv() 錯誤。

ICA2120 **LM 的狀態錯誤：狀態。**

解說： 來自「登入監督程式」的認可指出，並「未」順利開啓主電腦裝置。

ICA2121 **開啓 OCS 管理裝置時，發生錯誤：錯誤碼。**

解說： 未順利開啓 OCS 管理裝置。

ICA2122 **無法將 IP 位址轉換為 TBM ID：錯誤碼。**

解說： 發生了 ioctl() OCS_GET_TBMID 錯誤。ioctl 命令 OCS_GET_TBMID 無法在 OCS 管理裝置上使用。

ICA2123 **由 rlogin 指出連接 TBM 時發生錯誤：錯誤碼。**

解說： 發生了 ioctl() OCS_IS_TBM_CONNECTED 錯誤。ioctl 命令 OCS_IS_TBM_CONNECTED 無法在 OCS 管理裝置上使用。

ICA2124 **未連接任何主電腦節點：錯誤碼。**

解說： 沒有任何主電腦節點連線到來自可能的主電腦節點列示之此 OCS 節點。

ICA2125 **取得 ODM (物件資料管理系統) 的列示時，發生錯誤：自訂的屬性：odm 錯誤碼。**

解說： 發生了 ODM 物件類別，CuAt(自行設定的屬性) 的 odm_get_list() 錯誤。

ICA2126 沒有任何相關的 **OCS** 主電腦節點名稱：要連結的主電腦節點。

解說： 找到了 CuAt (自行設定的屬性) 項目，但沒有相符的主電腦節點/ocs 節點。

ICA2127 在「主電腦」陣列上發生 **Malloc** 錯誤。

解說： 以動態方式配置可能的主電腦名稱陣列空間時，發生了 malloc() 錯誤。

ICA2128 在鑑證前，從屬站 IP (從屬站站台) 的使用者 (不明) 嘗試執行命令 '無效的命令'。

解說： 在輸入使用者名稱與通行碼來進行鑑證前，使用者已嘗試一些動作 - 在繼續任何進一步的處理之前，必須先鑑證使用者。

使用者回應： 請以 USER 與 PASS 登入

ICA2129 **gethostbyname** (*invocation name*) : *errno*

解說： 當 ftpd 嘗試取得對應於主電腦名稱的主電腦資訊時，發生了系統錯誤。

ICA2130 從屬站 IP (從屬站站台) 的使用者 (使用者名稱) 試圖執行命令 '無效的命令'。

解說： 所指定的使用者嘗試進行無效的命令。

使用者回應： 在您指定 "quote site destination" 之前，只容許 USER、QUOTE SITE 與 QUIT 命令。

ICA2131 從屬站 IP 的使用者 '使用者名稱' 無法通過鑑證，原因是 **user.cfg** 檔案發生錯誤。

解說： 鑑證已失敗，因為「防火牆管理者」所設定的 user.cfg 檔案規格所致 (請查看先前的日誌)。

使用者回應： 請洽詢您的「防火牆」管理者。

ICA2132 IP 從屬站 IP (從屬站站台) 的使用者 '使用者' 試圖執行無效的指令 '無效的指令'。

解說： 使用者嘗試進行無效的命令。此時有效的命令僅為 SITE、USER 與 QUIT。

ICA2133 錯誤：函數 呼叫無法使用於案例中：行，WSAGetLastError

解說： 一般錯誤訊息：請檢查日誌

ICA2134 注意：ftpd: connect() (於 案例) 無法與 IP 連線，WSAGetLastError。

解說： Connect() 找不到所要求的位址；請檢查 WSAGetLastError 結果。

使用者回應： 請仔細複查您的位址 - 可能是 DNS 或網路錯誤

ICA2135 資料轉送完成：收到 位元組 個位元組 (來自 來源 IP)；傳送 位元組 個位元組 (至 目的地 IP)。

解說： 這項資訊反映在特定 FTP 階段作業時的單一資料轉送。但是請注意：可能是資料轉送不成功 \ (請查看日誌檔中失敗的接收 (recv) 或傳送 (send) 呼叫)。

ICA2136 錯誤：CreateThread() 無法使用於案例：errno。

解說： ftpd 無法建立緒。

ICA2137 已建立資料連線；伺服器：來源 IP 從屬站：目的地 IP。

解說： 已順利完成資料連線。

ICA2138 記憶體不足：pftpd: malloc(位元組)
傳回 NULL 於函數 案例。

解說： 無法配置足夠的記憶體 - malloc 傳回 NULL。

ICA2139 LogonUser() 失敗：原因。

解說： Windows NT (SAM) API LogonUser (用於通行碼鑑證) 因上述理由而失敗。

使用者回應： 請連絡「防火牆」管理者。

ICA2140 httpd --> HTTP Proxy 鑑證 結果；使用者 <使用者>；在 <使用者 IP> 上；透過 網路 ... RC：<原因>。

解說： HTTP Proxy 嘗試鑑證使用者。其成功或失敗的原因都會在這裡報告。

使用者回應： 請連絡「防火牆」管理者。

ICA2141 終止由 IP 位址 至 IP 位址 的 FTP 階段作業。

解說： 終止連線到防火牆的 FTP 階段作業。

ICA2142 fw_tn_authenticate 已順利鑑證 使用者 ID。

ICA2143 fw_tn_authenticate 無法鑑證 使用者 ID。

解說： fw_tn_authenticate 無法鑑證所指定的使用者 ID。

系統動作： 已拒絕登入。

使用者回應： 如果 fw_tn_authenticate 具有任何記載機能，則管理者應該查閱日誌檔，以找出原因。

ICA2144 fw_tn_authenticate 並未順利傳回。

解說： fw_tn_authenticate 所傳回的值不是零。函數 fw_tn_authenticate 可能遺漏了。

系統動作： 已拒絕登入。

使用者回應： 小心查閱 fw_tn_authenticate，查看是否曾經傳回非零值；若曾傳回非零值，請加以更正。若是如此，請重新製作 (make) 程式庫 fwuser.o，並將其放入「防火牆」中。

ICA2145 系統已傳回回覆碼 rc，位在檔案 檔案名稱 的第 行號 行。

解說： 系統呼叫失敗。可能缺程式庫 fwuser.o。

系統動作： 鑑證已異常中止。

使用者回應： 請確定 /usr/lib/fwuser.o 存在。如果存在，請與您的 IBM 代表連絡。

ICA2146 未置換 IBM 提供的 fwuser.o。

解說： 您正在使用 IBM 提供的 fwuser.o，因為您並未用自己的 fwuser.o 加以取代。

系統動作： 鑑證已異常中止。

使用者回應： 如果您定義任何使用者，來使用「使用者提供的」鑑證，您就應該撰寫並編譯自己的鑑證方法。IBM 提供的 fwuser.o 將會拒絕所有至「非 AIX」及「非防火牆」使用者的存取。

ICA2147 fwtnet：使用者 使用者 ID 已經啟動從 來源 IP 位址 (安全端) 到 目的 IP 位址 的透通式 telnet 階段作業。

解說： 在啟動每一個透通式 proxy 階段作業時，即產生訊息。當使用者 ID、來源 IP 與目的地 IP 防火牆都認識時，即開始階段作業。僅限從安全端啟動的階段作業。

系統動作： 容許透通式 telnet。

ICA2148 注意 -- 不允許使用者 使用者 ID 未經授權便試圖從 來源 IP 位址 (非安全端) 連線到 目的 IP 位址。

解說: 一般說來, 這表示嘗試透過非安全介面來建立與 Firewall 的連線。

系統動作: 拒絕連線。

使用者回應: 您應該使用透過 proxy, 從安全端進行 telnet。

ICA2149 **fwtelnet:** 啟動從 來源 IP 位址 至 目的 IP 位址 的透過式 telnet 階段作業時, 發生 **LOGIN_ADAPTER_ERROR**。

解說: 呼叫 q_check_secure(0) 時, 發生了 LOGIN_ADAPTER_ERROR。

系統動作: 拒絕連線。

使用者回應: 請檢查安全配接卡。

ICA2150 **Pftpd 錯誤 - 失敗的函數: 回覆碼 = 0x**函數回覆碼

解說: pftpd 伺服器偵測到所指出的函數中有錯誤。常駐程式終止。

使用者回應: 請更正所指出的系統問題, 並重新啟動 pftpd。

ICA2151 拒絕登入。

解說: 這則訊息將顯示給嘗試登入但不被容許的使用者。

ICA2152 **fwlogin:** 寫入 裝置 失敗。

解說: 無法寫入裝置。

ICA2153 **fwlogin:** 讀取 裝置 失敗。

解說: 無法讀取裝置。

ICA2154 連接埠名稱 中有錯誤, 原因。

解說: 這個「防火牆」發生問題。

ICA2155 **Pftpd 錯誤 - 失敗的函數: 系統錯誤訊息**

解說: pftpd 伺服器偵測到所指出的函數中有錯誤。常駐程式終止。

使用者回應: 請更正所指出的系統問題, 並重新啟動 pftpd。

ICA2156 注意 -- 使用者 使用者 ID 試圖使用透過式 ftp 從「非安全端」來源 IP 位址 連線到 目的 IP 位址, 但不被容許。

解說: 一般說來, 這表示嘗試透過非安全介面來建立與 Firewall 的連線。

系統動作: 拒絕連線。

使用者回應: 您應該使用透過式 proxy, 從安全端進行 FTP。

ICA2157 來源 IP 位址 的使用者 使用者 ID 不能使用透過式 proxy 來連接 目的 IP 位址。

解說: 一般說來, 這表示在未架構透過式 proxy 的情況下, 嘗試建立與「防火牆」的連線。

系統動作: 拒絕連線。

使用者回應: 開啓 fwtp proxy ftp = on

ICA2158 所指定的選項 參數值 不正確。

解說: 所指出的旗號指定錯誤。

ICA2159 未指定 -t 選項的逾時值。

解說: 必須提供 -t 選項的逾時值。

ICA2160 已變更 網路：主電腦名稱 使用者
使用者 ID 的通行碼。

解說： FTP 使用者已順利變更通行碼資料庫中的通行碼。

系統動作： 無

使用者回應： 無

ICA2161 使用者 使用者 ID 試圖使用 網路：
主電腦名稱 的過期通行碼來登入。

解說： FTP 使用者試圖使用過期的通行碼來建立與「防火牆」的連線。

系統動作： FTP 登入驗證失敗，使用者將回到 FTP 命令 shell。

使用者回應： 使用者必須用 FTP USER 命令，或重新建立 FTP 連線並傳遞通行碼字符串格式 "old_password/new_password/new_password"，再一次進行驗證。

ICA2162 變更 網路：主電腦名稱 使用者 使
用者 ID 的通行碼失敗。

解說： FTP 使用者嘗試變更通行碼，而通行碼驗證常式失敗。可能的失敗原因包括：- 所指定的 "舊" 通行碼錯誤、- 只有指定一次 "新" 通行碼、- 所指定的二次 "新" 通行碼不相符，或者 - 用來分隔通行碼的定界符號不是 "/"。

系統動作： FTP 通行碼驗證失敗，使用者將回到 FTP 命令 shell。

使用者回應： 嘗試重新驗證 FTP 伺服器，查看所輸入的通行碼是否正確。如果還是有問題，則請連絡服務代表。

ICA2163 已啟動 safemaid。

解說： 正在啟動 safemaid。

ICA2164 停止 safemaid。

解說： 正在停止 safemaid。

ICA2165 已中斷 telnet 階段作業。

解說： 正在結束 Telnet 階段作業，但無法從管道中擷取階段作業資訊。在啟動期間，從屬站可能已中斷階段作業，因此並未完全起始設定階段作業。

ICA2166 無法擷取使用者 使用者 ID 的屬性
屬性。回覆碼 = 回覆碼。

解說： 「鑑證服務程式」無法為所指出的使用者從「使用者資料庫」擷取所指出的屬性。系統動作：使用者鑑證失敗。

使用者回應： 請連絡系統管理者，以更正使用者資料庫記錄。

ICA2167 使用者 ID 要求 服務程式 時，鑑證
失敗；所使用的鑑證方法為 網路類
型 上之 從屬站位址 的 鑑證計劃。

解說： 所指出的使用者欲要求所指出的服務程式，並且使用所指出的鑑證方法來鑑證使用者，但是失敗了。而該使用者是從所指出的位址及網路類型要求該服務程式。系統動作：使用者鑑證失敗。

使用者回應： 請連絡系統管理者。

ICA2168 使用者 ID 要求 服務程式 時，因儲
存體不足而鑑證失敗。

解說： 在鑑證資料時，記憶體配置失敗，因此無法鑑證「使用者 ID」來要求服務程式。系統動作：使用者鑑證失敗。

使用者回應： 請連絡系統管理者。

ICA2169 使用者 名稱 要求 服務程式 鑑證成
功；鑑證方法為 網路：主電腦名稱
的 方法。

解說： FW 已使用所指出的鑑證方法來鑑證所指出的使用者名稱，以提供該使用者所要求的服務程式。

ICA2170 使用者 ID 要求 服務程式 鑑證失敗。未使用「防火牆」來登記 鑑證方法。

解說： 無法鑑證「使用者 ID」來要求服務程式。所要求的鑑證方法未使用「防火牆」來登記。系統動作：使用者鑑證失敗。

使用者回應： 請連絡系統管理者。

ICA2171 通行碼過期，已鎖定帳戶 使用者名稱。

解說： 通行碼已過期，且尚未變更。已鎖定此帳戶。

系統動作： 已鎖定此帳戶，「防火牆」通行碼鑑證失敗。UserRes

ICA2172 已鎖定帳戶 使用者名稱。

解說： 已鎖定此帳戶。

系統動作： 已鎖定此帳戶。「防火牆」通行碼鑑證失敗。

使用者回應： 請與「防火牆管理者」連絡，以找出未鎖定的帳戶。

ICA2173 使用者嘗試使用已保留的使用者名稱 使用者 ID 來登入。

解說： 使用者所提供的 ID 已被防火牆保留。

系統動作： 已拒絕登入。

使用者回應： 管理者應該調查誰正在使用這個使用者名稱。

ICA2174 內部處理發生錯誤，因此 使用者 ID 要求 服務程式 鑑證失敗；所使用的 鑑證方法為 網路類型 上之 從屬站位址 的 鑑證計劃。

解說： 所指出的使用者欲要求所指出的服務程式，並且使用所指出的鑑證方法來鑑證使用者，但是失敗了。而該使用者是從所指出的位址及網路類型要求

該服務程式。由於內部處理發生錯誤，鑑證要求失敗。系統動作：使用者鑑證失敗。

使用者回應： 請連絡系統管理者。

ICA2175 使用者 使用者名稱 的 Windows NT LogonUser 呼叫失敗。最後錯誤為 最後錯誤。

解說： 用 Windows NT LogonUser API 呼叫來鑑證所指出的使用者名稱失敗。LogonUser 失敗後，Windows NT 報告最後錯誤。系統動作：使用者鑑證失敗。

使用者回應： 請連絡系統管理者。

ICA2176 使用者名稱 使用 網路 的 元件時，被定義來鑑證使用者的鑑證計劃 鑑證計劃 不明。

解說： 當使用者使用所指出之網路的防火牆元件時，定義使用所指出的鑑證計劃來鑑證所指出的使用者，但是目前該鑑證計劃尚未用防火牆來登記。系統動作：使用者鑑證要求失敗。

使用者回應： 請連絡系統管理者。

ICA2177 收到來自 socket 對等名稱 的 SafeMail 連線 0x階段作業 ID。

解說： SafeMail 收到所列出之同等名稱的 \入埠連線。所指出的連線 ID 號碼 \已被用作追蹤的目的。(偵錯層次)

系統動作： 已指派一緒來處理這個 \連線。

ICA2178 已建立從 送件者的 IP 位址 到 接收者的 IP 位址 的 SafeMail 階段作業 0x階段作業 ID。

解說： SafeMail 已建立與接收者郵件伺服器的連接，\並且準備轉送郵件。(資訊層次)

系統動作： 將開始轉送資料。

ICA2179 **SafeMail 已為連線 0x階段作業 ID 從 傳送伺服器的位址 轉送了 訊息 位元組數 位元組到 接收伺服器的位址。**

解說： SafeMail 已成功地在所列出的二台郵件伺服器之間轉送訊息。在 ICA2166 訊息中就已識別 \這個階段作業。此訊息包含所指出的 \位元組數。(資訊層次)

ICA2180 **SafeMail 終止來自 送件者的位址 的階段作業 0x階段作業 ID。**

解說： SafeMail 拒絕轉送在所指出之階段作業中 \所傳送的郵件。(資訊層次)

系統動作： 此階段作業已終止。

使用者回應： 增加記載優先順序的層次，以取得 \較詳細的診斷資訊。

ICA2181 **SafeMail 終止階段作業 0x階段作業 ID，原因碼為 原因碼。**

解說： 因為偵測到主要的錯誤狀況，SafeMail 的主要處理器終止了所指出的階段作業。原因碼包含：\01 - 找不到接收者郵件伺服器 \02 - 送件者試圖在兩台非安全伺服器之間遞送郵件 \03 - 接收者郵件伺服器拒絕連線，可能已當機 \04 - 接收者郵件伺服器拒絕接受郵件 \05 - 一個或多個連線逾時；送件者或接收者郵件伺服器可能已當機 \06 - recv() 傳回 0 位元組；送件者或接收者郵件伺服器可能已當機 \07 - recv() 傳回負數；送件者或接收者郵件伺服器可能已當機 \08 - 收到太多錯誤命令 \09 - select() 傳回負數；送件者或接收者郵件伺服器可能已當機 \這個訊息記載於「偵錯」層次。

系統動作： 此連線已終止。

ICA2182 **由於 SMTP 命令 命令無效， SafeMail 拒絕階段作業 0x階段作業 ID，原因碼為 原因碼。**

解說： SafeMail 的命令驗證次常式偵測到 \無效或危險的命令。這些原因碼依各種 SMTP 命令 \而有所不同。現行值的相關資訊，請參閱 IBM Firewall Support \網頁。(偵錯層次)

系統動作： 此連線已終止。

使用者回應： 更正傳送郵件的從屬站或傳送郵件的伺服器，\以傳送安全且有效的資訊。

ICA2183 **httpd --> 無法使用 HTTP Proxy 架構檔 (檔案名稱)。**

解說： HTTP proxy 常駐程式嘗試開啓所指定的架構檔，但是檔案不存在或是無法開啓。

系統動作： HTTP Proxy 沒有啓動

使用者回應： 透過 GUI 或 fwhttp 命令來架構 proxy，然後重新啓動 proxy。

ICA2184 **signal() 發生錯誤，訊號為 訊號號碼。safemaid 結束。**

解說： 當 safemaid 常駐程式試圖建立信號處理程式時，發生系統錯誤。

ICA2185 **無法開啓 socket。 safemaid 結束**

解說： 開啓 socket 失敗。

ICA2186 **無法將 socket 連結至連接埠。 safemaid 結束**

解說： 將 socket 連結至連接埠時失敗。

ICA2187 **無法接受新的連線。safemaid 重試**

解說： 接受新連線時失敗。

ICA2188 -I 時間指定錯誤 (值)。

解說： 所顯示的時間值含有在數值範圍 0 至 9 外的字元，或超出所容許的最大值。

ICA2189 未對 -I 選項指定逾時值。

解說： 必須對 -1 選項提供一個逾時值。

ICA2200 (服務程式：函數) **WinSocket** 起始
設定錯誤： *WSAGetLastError*

解說: 起始設定 WinSocket 時，發生錯誤。

使用者回應: 更正 WSAGetLastError 所指出的系統問題，並重新啟動所指出的服務程式（第一個參數）。

ICA2201 (服務程式：呼叫函數) 失敗的函數
在行 行號 失敗：WSAGetLastError

解說：所指出的「網路」元件失敗。

使用者回應: 更正 WSAGetLastError 所指出的系統問題，並重新啟動所指出的服務程式（第一個參數）。

ICA2202 (服務程式：呼叫函數) 在
WSAGetLastError 秒後，逾時 逾時：

解說：所指出的函數在閒置了所指出的秒數後，發生逾時。

使用者回應: 重新連接所指出的服務程式，並在所指出的逾時時間內回應。

ICA2203 (服務程式：呼叫函數) 記憶體錯誤；
失敗的函數 在行 行號 傳回 傳回
值： *WSAGetLastError*

解說： 發生記憶體錯誤，通常是記憶體不足；請檢查 WSAGetLastError

使用者回應： 清出磁碟空間 - 請洽詢「系統管理者」

ICA2204 (服務程式：呼叫函數) 檔案名稱 發生錯誤：存取遭拒或建立失敗。

解說： 試圖存取或建立所指出的檔案或與檔案參數有關的檔案時，所指出的服務程式發生錯誤。

使用者回應： 請確定所指出的檔案名稱存在且有正確的存取權。

ICA2205 (服務程式：呼叫函數) 找不到所需要的檔案 檔案名稱。

解說：所指定的檔案不存在。造成失敗的原因，很有可能是因為「防火牆」的預設架構被消除了。請從目前的備份將檔案還原。

使用者回應: 請驗證架構檔是否存在。架構程式會預期這個檔案存在。如果沒有備份版本，請連絡您的服務代表。

ICA2206 (服務程式：呼叫函數) 架構檔 檔案名稱 已損毀。

解說： 所指出之架構檔的格式不正確。其內容已損毀。造成損毀的原因，很有可能是因為該檔案是以手動編輯，且加入了無效的資料。

使用者回應: 必須以正確的方式重新建立架構檔。先取得該檔案 (或建立一可檢視的備份), 然後將原來的檔案消除。使用適當的防火牆架構命令來重新架構這個檔案 (若有需要, 可參考原來的檔案)。

ICA2207 (服務程式：呼叫函數) 架構檔 檔案名稱 是空的。

解說：找不到所指出的架構檔，或是雖然找到了，但是是空的。找不到檔案的原因，很有可能是因為尚未執行所指出之服務程式的架構。

使用者回應: 請驗證架構檔的狀態。如果檔案存在，架構命令會預期這個檔案包含資料。相關資訊，請參閱使用指南。

ICA2208 服務程式 為 使用者 ID 從非安全配接卡啟動階段作業 階段作業 ID (來源 IP 位址;目的 IP 位址)。

解說: 這是在每個所指出的階段作業開始時所產生的訊息。

ICA2209 服務程式 已為非安全配接卡上的 使用者 ID 結束階段作業 階段作業 ID (來源 IP 位址;目的 IP 位址); 位元組數 位元組總數。

解說: 在每個所指出的階段作業結束時，會產生訊息。「位元組總數」是指在階段作業期間，所轉送的位元組總數。不支援「位元組總數」的服務程式 (即 ptelnetd) 會顯示「零」。

ICA2210 (服務程式) 使用者 使用者 ID 企圖使用已過期的通行碼，以從 來源 IP 位址 (非安全) 登入。

解說: 所指出的使用者試圖從非安全配接卡上的來源 IP，使用所指出的過期通行碼，來建立與「防火牆」的連線。

使用者回應: 所提供的通行碼已過期。請連絡您的系統管理者。

ICA2211 (服務程式) 使用者 使用者 ID 企圖使用已過期的通行碼，以從 來源 IP 位址 (安全) 登入。

解說: 所指出的使用者試圖從安全配接卡上的來源 IP，使用所指出的過期通行碼，來建立與「防火牆」的連線。

使用者回應: 所提供的通行碼已過期。請連絡您的系統管理者。

ICA2212 (服務程式) 來源 IP 位址 (安全) 上的使用者 名稱 已順利通過鑑證。

解說: FW 已鑑證所指出的使用者名稱，該使用者來自所指出之安全配接卡上的來源 IP。

ICA2213 (服務程式) 來源 IP 位址 (非安全) 上的使用者 名稱 已順利通過鑑證。

解說: FW 已鑑證所指出的使用者名稱，該使用者來自所指出之非安全配接卡上的來源 IP。

ICA2214 (服務程式) 來源 IP 位址 (非安全) 上的使用者 名稱 鑑證失敗。

解說: 所指出的使用者名稱沒有通過 FW 鑑證，該使用者來自所指出之非安全配接卡上的來源 IP。

使用者回應: 導致失敗的原因，很有可能是因為您所鍵入的使用者名稱或通行碼不正確；使用者名稱及通行碼皆需區分大小寫 (請檢查是否啓用了 Caps Lock 鍵)。

ICA2215 (服務程式) 來源 IP 位址 (安全) 上的使用者 名稱 鑑證失敗。

解說: 所指出的使用者名稱沒有通過 FW 鑑證，該使用者來自所指出之安全配接卡上的來源 IP。

使用者回應: 導致失敗的原因，很有可能是因為您所鍵入的使用者名稱或通行碼不正確；使用者名稱及通行碼皆需區分大小寫 (請檢查是否啓用了 Caps Lock 鍵)。

ICA2216 (服務程式) 來自 來源 IP 位址 (非安全) 的使用者 名稱 沒有輸入相符的 (驗證) 通行碼。

解說: 所指出的使用者要求變更通行碼，但是所輸入二次通行碼不相符；該使用者來自所指出的之非安全配接卡上的來源 IP。使用者的鑑證資料沒有變更。

使用者回應: 若您要變更通行碼，必須輸入二次通行碼，第二次是爲了驗證；導致失敗的原因，很有可能是因為所輸入的驗證通行碼不正確。

ICA2217 (服務程式) 來自 來源 IP 位址 (安全) 的使用者 名稱 沒有輸入相符的 (驗證) 通行碼。

解說：所指出的使用者要求變更通行碼，但是所輸入二次通行碼不相符；該使用者來自所指出的之安全配接卡上的來源 IP。使用者的鑑證資料沒有變更。

使用者回應：若您要變更通行碼，必須輸入二次通行碼，第二次是爲了驗證；導致失敗的原因，很有可能是因爲所輸入的驗證通行碼不正確。

ICA2218 服務程式 已為安全配接卡上的 使用者 ID 啟動階段作業 階段作業 ID (來源 IP 位址:目的 IP 位址)。

解說：這是在每個所指出的階段作業開始時所產生的訊息。

ICA2219 服務程式 已為安全配接卡上的 使用者 ID 結束階段作業 階段作業 ID (來源 IP 位址:目的 IP 位址)；位元組數 位元組總數。

解說：在每個所指出的階段作業結束時，會產生訊息。「位元組總數」是指在階段作業期間，所轉送的位元組總數。不支援「位元組總數」的服務程式 (即 ptnetd) 會顯示「零」。

ICA2220 (服務程式) 使用者 使用者 ID 啟動了一個從 來源 IP 位址 (安全端) 到 目的 IP 位址 的透通式 proxy 階段作業。

解說：這是在啟動每一個透通式 proxy 階段作業時所產生的訊息。當防火牆識別出使用者 ID、來源 IP 與目的地 IP 時，即開始階段作業。僅限從安全端啟動的階段作業。

系統動作：允許透通式 proxy。

ICA2221 (服務程式) 警告：在「控制」線路之對等端上的 IP (控制 IP 位址) 不等於「資料」線路之對等端上的 IP (資料 IP 位址)。

解說：爲確保「安全性」(即「反侵入」)，請確定「控制連線 socket」所連接的對等端 IP 位址，與「資料連線 socket」所連接的對等端 IP 位址相同。但是如果使用「網路分派程式」，或是目的地已使用多個配接卡，這些情況便會有所不同。

系統動作：請檢查「目的地 FTP 伺服器」是否有使用數個配接卡，或是檢查是否已使用「網路分派程式」。請確定過濾器只允許有效的 IP 位址通過第 20 及第 21 號連接埠。

ICA2222 (服務程式) 警告！通訊協定違規。收到「非 RFC」相容命令 無效字串；預期為 通訊協定字串。

解說：所指出的服務程式收到異常字串，該字串與相關之 RFC 不相容；可能是網路駭客。

系統動作：使用與 RFC 相容的「從屬站」來要求所指出的服務程式。

ICA3001 *警告*：真正的使用者是 識別使用者名稱，而不是 Socks 連線使用者名稱

解說：可能有破壞安全性的企圖；未鑑證使用者名稱。

ICA3006 計數 個位元組來自 從屬站，計數 個位元組來自 伺服器

解說：訊息指出 sockd 常駐程式及其個別的從屬站和伺服器主電腦之間轉送的位元組數目。

ICA3007 由於超過最大連線計數被拒絕連線。

解說：socks 伺服器的架構只能接受某一從屬站階段作業的最大限制數。當已到達該臨界值，又有額外的連線要求傳來時，就會產生此訊息。

系統動作：關閉新發出的連線。

使用者回應： 並行連線的最大數限制是由 socks5.conf 中的 SOCKS5_MAXCHILD 參數所決定。 增加此設定值，並復新伺服器。相關詳細資訊，請參閱 IBM Firewall 參考手冊。 start unused

ICA3010 已連線 -- 從 使用者
(*real_user*)@*src_addr* 連結至
dst_addr (目的地連接埠)

解說： 建立連線。

ICA3011 已連線 -- 從 使用者
(*real_user*)@*src_addr* 連線至
dst_addr (應用程式)

解說： 用 socket 連線至外界成功。

ICA3012 遭拒絕 -- 從 使用者
(*real_user*)@*src_addr* 連線至
dst_addr (應用程式)

解說： 遠端主電腦已拒絕連線。

ICA3013 **select()** 錯誤碼

解說： 系統發生錯誤。

ICA3014 已終止 -- 從 使用者
(*real_user*)@*src_addr* 連結至
dst_addr (目的地連接埠)。 (自 從屬
站 接收 計數 個位元組，自 伺服器)
接收 計數 個位元組。

解說： 連線終止。

ICA3015 已終止 -- 從 使用者
(*real_user*)@*src_addr* 連線至
dst_addr (目的地主電腦)。 (自 從
屬站 接收 計數 個位元組，自 伺
服器 接收 計數 個位元組)

解說： 已終止與伺服器的連線。

ICA3016 ***找不到可與 目的地主電腦 通信的
適當介面

解說： 檔案 /etc/sockd.route 不包括為所指出的目的地主電腦的遞送資訊。

ICA3017 無法執行 *pid sockd* 處理 的 **shell**
命令

解說： Sockd 常駐程式無法執行 /bin/sh 命令。

使用者回應： 驗證 /bin/sh shell 可在系統上使用。

ICA3018 遭拒絕 -- 從 使用者
(*real_user*)@*src_addr* 連結至
dst_addr

解說： 遠端主電腦已拒絕連線。

ICA3019 來自主電腦 *socks_src_name*: 錯誤碼
的 **GetDst()** 錯誤

解說： 在解析所要求之連線的目的地位址時，發生錯誤。

ICA3022 第 行號 行的 **?=** 欄位無效

解說： 在 /etc/sockd.conf 檔案中發現無效的項目。

ICA3023 無效的比較，位在第 行號 行

解說： 在 /etc/sockd.conf 檔案中發現無效的項目。

ICA3024 無效的項目，位在第 行號 行

解說： 在 /etc/sockd.route 檔案中發現無效的項目。

ICA3025 無效的允許/拒絕欄位，位在第 行號
行

解說： 在 /etc/sockd.conf 檔案中發現無效的項目。

ICA3026 無效的埠號，位在第 行號 行

解說： 在 /etc/sockd.conf 檔案中發現無效的項目。

ICA3027 `\\"cmd\\"" 的 Shell 命令已失敗 (執行狀態)`

解說: 所顯示的 Shell 命令失敗。

使用者回應: 驗證系統上有 Shell 處理器。

ICA3030 無法開啓架構檔 (`/etc/sockd.conf`)

解說: 要求開啓所指出的檔案失敗。

ICA3031 無法開啓路由檔 (`/etc/sockd.route`) : 錯誤碼

解說: 要求開啓所指出的檔案失敗。

使用者回應: 請洽詢您的「防火牆」管理者。在「防火牆」安裝時已提供預設檔。

ICA3032 無法開啓使用者檔案 (使用者名稱檔案): 錯誤碼

解說: 在准許的規則中找不到對 `*=userlist` 指定的檔案名稱。

ICA3033 `Validate()` 傳回異常的結果

解說: 已指定使用者名稱的 `Identd` 驗證, 但 `Identd` 的回應為異常的結果。

ICA3035 無法連線到 從屬站主電腦 上的 `identd`

解說: 已指定使用者名稱的 `Identd` 驗證, 但 `Identd` 沒有回應。

ICA3039 錯誤 -- `shell` 命令 `\\"cmd\\"" 沒有包含英數字元。`

解說: `Shell` 命令無效, 請參閱日誌訊息。

ICA3040 錯誤 -- `shell_cmd fork()` 錯誤碼

解說: `Sockd` 常駐程式無法透過 `'fork()'` 切換至子處理。

ICA3041 錯誤 -- 無法取得從屬站位址。

解說: 從 `'getpeername()'` 呼叫傳回的錯誤。

使用者回應: 檢查遞送和 DNS 架構。

ICA3042 錯誤 -- 主電腦 從屬站位址 傳送了未定義的命令 (`0xhex-command-received`)

解說: 接收來自從屬站應用程式的無效命令。

使用者回應: 可能是從屬站架構有問題, 或是從屬站和「防火牆」支援層次不符。

ICA3043 錯誤 -- 主電腦 從屬站位址 的版本錯誤 (`0xhex-version-number`)

解說: 「防火牆」支援 Socks 4.2 版本。

使用者回應: 可能是從屬站架構有問題, 或是從屬站和「防火牆」支援層次不符。

ICA3044 失敗 -- 從 使用者 (`real_user`)@`src_addr` 連線到 `dst_addr` (應用程式)。錯誤碼: 命令造成的失敗 錯誤碼。

解說: 連線要求失敗。

ICA3045 失敗 -- 從 `user(real_user)`@`src_addr` 連結至 `dst_addr`。錯誤: 已連線到錯誤主電腦 `dst_name` (`dst_port` (`application`))。

解說: 連結要求失敗。

ICA3046 失敗 -- 從 `user(real_user)`@`src_addr` 連結至 `dst_addr`。錯誤碼: 命令造成的失敗 錯誤碼。

解說: 連結要求失敗。

ICA3047 逾時 -- 從 *user{real_user}@src_addr*
連結至 *dst_addr*

解說: 連線逾時。

ICA3048 **Shell** 命令太長: *command...*

解說: 來自 */etc/sockd.conf* 檔的執行命令太長。

ICA3049 逾時 -- 從 *user{real_user}@src_addr*
連線到 *dst_addr (application)*

解說: 連線逾時。

ICA3050 相符的 *sockd.conf* 過濾規則

解說: 來自 */etc/sockd.conf* 檔的過濾規則, 符合
socks 連線。

ICA3051 **AIX sockd_route()** 找不到 *remote*
address 的介面。

解說: 找不到介面遞送路徑資訊。

ICA3052 將使用者 ID 設定為 "*nobody*" 時,
發生錯誤。

解說: 無法將子項 *sockd* 處理的使用者 ID 設定為
"*nobody*"。

ICA3053 **popen (AIX 遞送路徑 script)** 發生
錯誤: 系統錯誤訊息

解說: 無法執行 *script* 尋找遞送路徑資訊。

ICA3054 在 **AIX sockd_route()** 發生嚴重的
記憶體配置錯誤。

解說: 試圖收集遞送資訊, 發生記憶體配置失敗。

ICA3055 **AIX sockd_route()** 解析 輸入行 中
的第一個空間時, 發生嚴重錯誤

解說: 解析系統遞送路徑資訊時, 發生錯誤。

ICA3056 **AIX sockd_route()** 解析 輸入行 中
的第二個空間時, 發生嚴重錯誤

解說: 解析系統遞送路徑資訊時, 發生錯誤。

ICA3057 **AIX sockd_route()** 讀取遞送路徑
script 輸出時, 發生嚴重錯誤:
system error message

解說: 讀取 *script* 輸出時, 發生錯誤。

ICA3058 **popen (AIX 配接卡 script)** 發生錯
誤: 系統錯誤訊息

解說: 無法執行 *script* 尋找介面資訊。

ICA3101 傳送資料時, 發生 **Sockd** 錯誤 -
select(): 系統錯誤訊息

解說: (SOCKS422) 傳送資料時, 發生錯誤。

ICA3102 傳送資料時, 發生 **Sockd** 錯誤 -
write(): (系統錯誤訊息

解說: (SOCKS422) 傳送資料時, 發生錯誤。

ICA3103 接收資料時, 發生 **Sockd** 錯誤 -
select(): 系統錯誤訊息

解說: (SOCKS422) 接收資料時, 發生錯誤。

ICA3104 接收資料時, 發生 **Sockd** 錯誤 -
read(): 系統錯誤訊息

解說: (SOCKS422) 接收資料時, 發生錯誤。

ICA3105 無法建立處理 **id** 檔 檔案名稱。

解說: (SOCKS422) 無法建立/寫入處理 *id* 檔。

ICA3106 **Sockd** 分割子項失敗：系統錯誤訊息

解說： (SOCKS422) 分割子項來處理 SOCKS 要求的嘗試失敗。

ICA3107 設定入埠 **socket SO_LINGER** 選項失敗：系統錯誤訊息

解說： (SOCKS422) 不是嚴重的錯誤

ICA3108 設定離埠 **socket SO_LINGER** 選項失敗：系統錯誤訊息

解說： (SOCKS422) 不是嚴重的錯誤

ICA3109 檔案 檔案名稱 第 行號 行的項目無效。

解說： (SOCKS422) 錯誤的架構項目語法。

ICA3110 檔案 檔案名稱 第 行號 行的介面欄位無效。

解說： (SOCKS422) 錯誤的架構項目語法。

ICA3111 檔案 檔案名稱 第 行號 行的目的地 IP 不正確。

解說： (SOCKS422) 錯誤的架構項目語法。

ICA3112 檔案 檔案名稱 第 行號 行的目的地遮罩不正確。

解說： (SOCKS422) 錯誤的架構項目語法。

ICA3113 已解析檔案 檔案名稱 中的第 行號 行。

解說： (SOCKS422) 錯誤的架構項目語法。

ICA3114 在檔案 檔案名稱 中找不到任何有效字行。

解說： (SOCKS422) 架構檔是空的，或語法不對。

使用者回應： 請更正所指出的架構檔。

ICA3115 檔案 檔案名稱 第 行號 行的 '許可/拒絕' 欄位無效。

解說： (SOCKS422) 錯誤的架構項目語法。

ICA3116 檔案 檔案名稱 第 行號 行的 '?=' 欄位無效。

解說： (SOCKS422) 錯誤的架構項目語法。

ICA3117 檔案 檔案名稱 第 行號 行的來源 IP 不正確。

解說： (SOCKS422) 錯誤的架構項目語法。

ICA3118 檔案 檔案名稱 第 行號 行的來源遮罩不正確。

解說： (SOCKS422) 錯誤的架構項目語法。

ICA3119 檔案 檔案名稱 第 行號 行的比較無效。

解說： (SOCKS422) 錯誤的架構項目語法。

ICA3120 檔案 檔案名稱 第 行號 行的埠號無效。

解說： (SOCKS422) 錯誤的架構項目語法。

ICA3121 收到 **SIGUSR1** - 正在傾出 **socks** 架構。

解說： (SOCKS422) 發生信號將現行的架構傾出至日誌檔，在這個訊息之後。

ICA3122 Sockd 無法分割常駐程式：系統錯誤訊息

解說： (SOCKS422) 無法分割以起始設定 sockd 常駐程式。

使用者回應： 請更正所指出的系統問題，並重新啟動 sockd。

ICA3123 正在啟動 Sockd 伺服器。

解說： (SOCKS422) Sockd 已順利起始設定，並等待連線。

ICA3124 嚴重的 sockd 起始設定錯誤 - bind(): 系統錯誤訊息

解說： (SOCKS422) 無法起始設定 Sockd 伺服器，已終止常駐程式。

使用者回應： 請更正所指出的系統問題，並重新啟動 sockd。

ICA3125 嚴重的 sockd 起始設定錯誤 - listen(): 系統錯誤訊息

解說： (SOCKS422) 無法起始設定 Sockd 伺服器，已終止常駐程式。

使用者回應： 請更正所指出的系統問題，並重新啟動 sockd。

ICA3126 嚴重的 sockd 錯誤 - main accept(): 系統錯誤訊息

解說： (SOCKS422) Sockd 伺服器主要常式已失敗，已終止常駐程式。

使用者回應： 請更正所指出的系統問題，並重新啟動 sockd。

ICA3127 Sockd 伺服器收到終止信號。

解說： root 或 nobody 刪除處理，已終止常駐程式。

使用者回應： 如果管理者想重新啟動 sockd，請重新啟動（輸入 "sockd"）。

ICA3128 嚴重的 sockd 起始設定錯誤 - socket(): 系統錯誤訊息

解說： Sockd 伺服器起始設定失敗，已終止常駐程式。

使用者回應： 請更正所指出的系統問題，並重新啟動 sockd。

ICA3129 嚴重的 sockd 起始設定錯誤 - 失敗的函數：系統錯誤訊息

解說： 無法在所指出的函數中起始設定 Sockd 伺服器，已終止常駐程式。

使用者回應： 請更正所指出的系統問題，並重新啟動 sockd。

ICA3130 Sockd 錯誤 - 失敗的函數：系統錯誤訊息

解說： sockd 伺服器偵測到所指出函數中的錯誤。常駐程式將繼續執行，但連線可能會被拒絕或終止。

使用者回應： 如果問題持續，請停止 sockd，請更正所指出的系統問題，然後重新啟動 sockd。

ICA3131 讀取 檔案名稱 時，發生錯誤。將使用先前放入快取記憶體中的資料。

解說： 無法讀取檔案，或檔案含有不正確的資料。先前的訊息應該會說明問題。 Sockd 將繼續以快取記憶體中自先前版本檔案的資料來進行作業。

使用者回應： 請更正所指出檔案中的錯誤。

ICA3132 不明旗號 - 參數值。

解說： 無法辨識所指出的旗號，已終止常駐程式。

使用者回應： 請更正語法，並重新啟動 sockd。

ICA3133 不明參數 參數值。

解說: 無法辨識所指出的參數，已終正常駐程式。

使用者回應: 請更正語法，並重新啟動 sockd。

ICA3134 選項 *option1* 與 *option2* 衝突。

解說: 無法同時指定所指出的選項，已終正常駐程式。

使用者回應: 請更正語法，並重新啟動 sockd。

ICA3135 **Sockd 錯誤 - 失敗的函數: 回覆碼 = 0x**功能回覆碼

解說: sockd 伺服器偵測到所指出函數中的錯誤。常駐程式終止。

使用者回應: 請更正所指出的系統問題，並重新啟動 sockd。

ICA3700 **WinSocket 起始設定發生錯誤:**
WinSocket 錯誤

解說: 起始設定 WinSocket 時，發生錯誤。

使用者回應: 請更正所指出的系統問題，並重新啟動 sockd。

ICA4000 程式 - 警告: 收到訊號 訊號，正在終止 ...

解說: 由於接收到信號而終止。

ICA4001 「停止」 程式 作為 PID 處理 ID

解說: 列印常駐程式結束的完成訊息。參考訊息。

ICA4002 暫時性 ID

解說: 參考訊息。

ICA4003 子處理 處理 ID 發生問題。

解說: 無法建立子處理。

ICA4004 嚴重錯誤。正在刪除訊號 訊號 上的 fwpagerd。

解說: 訊號處理程式。

ICA4005 沒有執行任何 fwpagerd 常駐程式，找不到 程式。

解說: 常駐程式不在作用中，無法傳送呼叫。

ICA4006 沒有任何用處理 ID 處理 ID 來執行的 fwpagerd 常駐程式。

解說: 找不到常駐程式處理程序的處理 Id。

ICA4007 「啟動」程式 作為 PID 處理 ID

解說: 列印啟動資訊。參考訊息。

ICA4008 無法設定 SIGPIPE 的 **sigignore**。

解說: 進行設定以忽略損毀的管道信號時失敗。

ICA4009 無法設定 SIGCHLD 的 **sigset**。

解說: 抓取漸弱子信號的設定失敗。

ICA4010 無法設定終止處理。

解說: 抓取終止處理的信號設定失敗。

ICA4011 無法開啓 socket。

解說: 開啓 socket 失敗。

ICA4012 無法設定 SIGTERM 的 **sigset**。

解說: 進行設定以快取 SIGTERM 與 SIGINT 信號時失敗。

ICA4013 無法設定 socket 重新使用選項。

解說: 設定 socket 重新使用選項失敗。

ICA4014 無法設定 **socket** 滯留選項。

解說： 設定 **socket** 滯留選項失敗。

ICA4015 無法將 **socket** 連結至連接埠。

解說： 將 **socket** 連結至連接埠時失敗。

ICA4016 無法設定傾聽 **socket**。

解說： 傾聽 **socket** 的設定失敗。

ICA4017 使用 **TCP socket** *socket* 的服務程式
servName 。

解說： 這是參考訊息。

ICA4018 函數呼叫 **select()** 失敗。

解說： 內部函數呼叫失敗。

ICA4019 **new_work()** 發生嚴重錯誤。

解說： 來自 **new_work** 常式的嚴重錯誤。

ICA4020 錯誤(程式)：無法寫入串流 **socket**：
socket

解說： 可能系統發生錯誤。

使用者回應： 檢查 **socket** 用法。

ICA4021 接收回應發生問題。

解說： 接收來自數據機的回應有問題。

使用者回應： 檢查數據機連線和起始設定字串。

ICA4022 要求成功。

解說： 參考訊息。

ICA4023 要求失敗。

解說： 要求傳送呼叫失敗。

ICA4024 錯誤(程式)：優先順序超出範圍
(*minpri* - *maxpri*)。

解說： 錯誤的優先順序範圍。

使用者回應： 請輸入正確的優先順序範圍。有效值是
從 -1 到 5。

ICA4025 錯誤(程式)：使用 **-n** 選項時，位址的
格式必須是 **ID@carrier**。

解說： 錯誤的命令用法語法。

使用者回應： 更正命令使用語法。

ICA4026 錯誤(程式)：不明主電腦 主電腦名稱

解說： 無法分辨主電腦名稱。

使用者回應： 檢查主電腦名稱。

ICA4027 錯誤(程式)：無法開啓串流 **socket**：
錯誤碼

解說： 無法建立新 **socket**。

ICA4028 錯誤(程式)：無法設定 **socket** 選
項：錯誤碼

解說： 無法設定 **socket** **linger** 選項。

ICA4029 錯誤(程式)：無法連線到 主電腦：錯
誤碼。

解說： 無法連線到主電腦。

使用者回應： 檢查序列連接埠架構和裝置驅動程式檔
的存在。

ICA4030 錯誤(程式)：無法寫入串流 **socket**：
錯誤碼。

解說： 無法寫入資料流 **socket**。

ICA4031 接收回應發生問題。訊息的狀況不明。

解說: 接收來自數據機的回應有問題。

ICA4032 已成功地將訊息傳送到佇列。

解說: 參考訊息。已將訊息傳送到佇列。

ICA4033 訊息失敗。未傳送任何訊息。

解說: 無法傳送訊息到呼叫器佇列。

ICA4034 日期 失敗 (ID ID 優先順序 優先順序 秒數 期間 嘗試次數 重試次數) [fromEntry] 人名: 訊息。

解說: 傳送呼叫失敗時, 就會顯示這個訊息。

ICA4035 無法重新排列從 程式 傳送到 人稱 的訊息 訊息。

解說: 無法傳送到呼叫佇列。

ICA4036 成功 (ID ID 優先順序 優先順序 秒數 期間 嘗試次數 重試次數) [fromEntry] 人名: 訊息。

解說: 傳送呼叫成功時, 就會顯示這個訊息。此為參考訊息。

ICA4037 傾出至 傾出檔 (ID ID 優先順序 優先順序 秒數 期間 嘗試次數 重試次數) [fromEntry] 人名: 訊息。

解說: 沒有立刻傳送的呼叫會被傾出到檔案, 供稍後再試。

ICA4038 無法寫入傾出檔 傾出檔案。

解說: 無法寫入傾出檔。

使用者回應: 檢查檔案系統許可權。

ICA4039 **lpcKey: 0xIpcKey**

解說: 參考訊息。

ICA4040 重試時間超過 重試時間 分鐘。

解說: 指定分鐘後無法起始設定數據機。

使用者回應: 檢查起始設定字串。

ICA4041 發現傳送給數字型呼叫器的訊息為英數訊息。

解說: 數字型呼叫器不能包含英數資料。

使用者回應: 用 smitty/SMIT 功能表來更正。

ICA4042 對方無法接收呼叫。

解說: 可能沒有啟動呼叫器。

使用者回應: 檢查呼叫器是否啟動。

ICA4043 載波 載波 不存在。

解說: 沒有指定的載波。

使用者回應: 用 smitty/SMIT 功能表來更正。

ICA4044 載波 載波 沒有 DTMF 電話號碼。

解說: 所指出的載波沒有 DTMF 電話號碼。

使用者回應: 用 smitty/SMIT 功能表來更正。

ICA4045 呼叫器號碼 呼叫器號碼 太長, 超出 載波的 載波最長限制 上限。

解說: 呼叫器號碼太長, 超出載波的最長限制。

使用者回應: 使用其他小於載波最長限制之較短的呼叫器號碼。

ICA4046 呼叫器號碼 呼叫器號碼 太長, 超出 預設長度 預設載波長度。

解說: 當預設長度太短時, 將發出這則訊息。

使用者回應： 用 smitty/SMIT 功能表來更正。 增加預設長度。

ICA4047 數據機檔案 數據機檔路徑名稱 的第
行號 行有問題。

解說： 數據機定義檔含有一個無效字元。

使用者回應： 用 smitty/SMIT 功能表來更正。

ICA4048 無法開啓裝置 /dev/裝置名稱 上的數
據機。

解說： 無法開啓所指出之裝置上的數據機。

使用者回應： 檢查或重新架構列序連接埠。檢查裝置。

ICA4049 已開啓 /dev/裝置名稱 上的數據機。

解說： 參考訊息。 已成功地在序列埠上偵測到數據機。

ICA4050 無法設定數據機性質。

解說： 嘗試設定數據機性質時失敗。

使用者回應： 檢查數據機起始設定字串。

ICA4051 重試 嘗試起始設定次數 次之後無法
起始設定數據機。

解說： 無法起始設定數據機。

使用者回應： 檢查數據機起始設定字串和序列埠架構。

ICA4052 無法撥接呼叫器號碼 呼叫器號碼

解說： 無法撥接呼叫器號碼。

使用者回應： 檢查呼叫器號碼的有效性。

ICA4053 無法掛斷數據機。

解說： 無法掛斷數據機。

使用者回應： 檢查所使用的數據機起始設定字串和掛斷命令。

ICA4054 無法撥接訊息 訊息

解說： 無法撥接訊息。

ICA4055 數據機檔案 檔案名稱 的第 行號 行
有問題。

解說： 無效的數據機定義檔。

使用者回應： 用 smitty/SMIT 功能表來更正。

ICA4056 無法撥接載波 載波 的 DTMF 號碼
(DTMF 號碼)。

解說： DTMF 號碼已變更，或該號碼對這個載波而言不正確。

使用者回應： 用 smitty/SMIT 功能表來更正。

ICA4057 無法傳輸區塊。

解說： 嘗試傳輸區塊時失敗。

使用者回應： 用 smitty/SMIT 功能表來檢查載波參數。

ICA4058 沒有回應至已傳輸的區塊。

解說： 傳輸區塊後，無法從載波得到回應。

使用者回應： 用 smitty/SMIT 功能表來檢查載波參數。

ICA4059 傳送訊息後，收不到回應。

解說： 訊息傳遞之後，無法從載波得到回應。

使用者回應： 用 smitty/SMIT 功能表來檢查載波參數。

ICA4060 無法傳輸呼叫器 ID。

解說： 無法傳輸呼叫器 ID。

使用者回應: 用 smitty/SMIT 功能表來檢查呼叫器號碼及載波參數。

ICA4061 無法傳輸自動模態要求的結尾
<CR>。

解說: 無法傳輸自動模態要求的結尾 <CR>。

使用者回應: 用 smitty/SMIT 功能表來檢查載波參數。

ICA4062 無法傳輸自動模態要求。

解說: 無法傳輸自動模態要求信號。

使用者回應: 用 smitty/SMIT 功能表來檢查載波參數。

ICA4063 重試 嘗試次數 次之後，無法接收載波 載波 的 go-head。

解說: 此時載波可能忙線。

使用者回應: 用 smitty/SMIT 功能表來檢查載波參數，稍後再試。

ICA4064 在以載波 載波 提供提示時，發生通信錯誤。

解說: 可能因某些原因而發生通信錯誤。請稍後再試。

使用者回應: 用 smitty/SMIT 功能表來檢查載波參數，稍後再試。

ICA4065 無法接收登入的回應。

解說: 數據機無法接收登入的回應。

使用者回應: 檢查數據機起始設定字串和載波參數。

ICA4066 載波 載波 未回應登入的動作。

解說: 載波沒有回應登入提示。

使用者回應: 用 smitty/SMIT 功能表來檢查載波參數，稍後再試。

ICA4067 載波 載波 表示 接收資料字串。

解說: 載波傳回某些錯誤訊息或忙線訊息。

使用者回應: 用 smitty/SMIT 功能表來檢查載波參數，稍後再試。

ICA4068 在登入時，載波 載波 已強制切斷連線。

解說: 登入期間載波強制切斷連線。

使用者回應: 用 smitty/SMIT 功能表來檢查載波參數。

ICA4069 正在將訊息傾出到因重試 最大重試 連線 次迴路所造成的載波 載波。

解說: 若載波忙線中，則程式會傾出呼叫並且稍候再試。

ICA4070 略過因重試 最大重試總數 次階段作業連線而造成的載波 載波。

解說: 經過幾次嘗試後仍然無法接觸載波。

使用者回應: 檢查載波參數，稍後再試。

ICA4071 錯誤(程式): 無法配置記憶體，以供載波重試使用: 錯誤碼。

解說: 可能是系統或記憶體配置發生錯誤。

ICA4072 錯誤(程式): 無法新增至載波重試列示: 錯誤碼。

解說: 可能沒有載波。

使用者回應: 檢查載波有效性然後再試。

ICA4073 重試 重試次數 次之後，資料無法透過 電話號碼 連線至載波 載波。

解說: 資料連線失敗。

使用者回應: 請使用 smitty/SMIT 功能表來檢查數據機連線及載波參數。

ICA4074 重試 嘗試次數 次之後，未收到載波 載波 要求輸入 ID 的提示。

解說： 載波未能回應 ID 或認可提示。

使用者回應： 請確定載波使用 TeleAlphanumeric 通訊協定。

ICA4075 透過載波 載波 登入時，發生通信錯誤。

解說： 可能由於幾個原因而發生通信錯誤。

使用者回應： 用 smitty/SMIT 功能表來檢查載波參數。

ICA4076 已超出載波 載波 的登入嘗試次數上限。

解說： 載波未能在指定嘗試內回應。

使用者回應： 檢查載波參數，稍後再試。

ICA4077 未從載波 載波 中收到繼續進行的訊息。

解說： 載波未能以「繼續進行」提示來回應。

使用者回應： 檢查載波參數，稍後再試。

ICA4078 無法建立區塊。

解說： 載波無法建立傳輸的區塊。

使用者回應： 用 smitty/SMIT 功能表來檢查載波參數。

ICA4079 載波 載波 未回應訊息傳遞。

解說： 載波在傳遞訊息時有困難。

使用者回應： 用 smitty/SMIT 功能表來檢查載波參數。

ICA4080 在傳遞訊息期間，載波 載波 已強制切斷連線。

解說： 傳遞訊息期間，載波強制切斷連線。

使用者回應： 檢查載波參數和數據機起始設定字串。

ICA4081 載波 載波 拒絕訊息或「呼叫器 ID」。

解說： 載波拒絕呼叫器訊息或呼叫器 ID。

使用者回應： 檢查呼叫器 ID 的有效性、呼叫器啟動與否及載波參數。

ICA4082 在訊息傳遞至載波 載波 時，發生通信錯誤。

解說： 可能因某些原因而發生通信錯誤。

使用者回應： 用 smitty/SMIT 功能表來檢查載波參數。

ICA4083 重試 最大嘗試次數 之後，無法接收載波 載波 的確認。

解說： 若載波忙線或無法建立連線時，則會發生這個訊息。

使用者回應： 用 smitty/SMIT 功能表來檢查載波參數，過幾分鐘後再試一次。

ICA4084 無法傳輸 <EOT>。

解說： 數據機無法傳輸 <EOT>。

使用者回應： 檢查數據機連線和起始設定字串。

ICA4085 無法收到 <EOT> 的回應。

解說： 數據機無法收到 <EOT> 的回應。

使用者回應： 檢查數據機連線和起始設定字串。

ICA4086 **載波 載波 未回應 <EOT>。**

解說： 載波無法回應傳輸的資料。

使用者回應： 檢查載波有效性和數據機連線。

ICA4087 **載波 載波 資料無法接受的錯誤來回應，因為內容有問題。**

解說： 載波無法回應傳輸的資料。

使用者回應： 用 smitty/SMIT 功能表來檢查載波參數。

ICA4088 **無法開啓預設檔 預設路徑名稱。**

解說： 可能沒有數據機預設檔或具有錯誤許可權。

使用者回應： 檢查是否含有檔案和許可權。

ICA4089 **不完整的預設檔 預設路徑名稱。**

解說： 數據機預設檔有遺漏資料。

使用者回應： 用 smitty/SMIT 功能表來更正。

ICA4090 **預設檔 預設路徑名稱 第 行號 行的外線號碼無效。**

解說： 載波資料庫檔有無效的行號。

使用者回應： 清除載波資料庫檔。

ICA4091 **預設檔 預設檔案 第 行號 行的傳輸速率值無效。**

解說： 載波資料庫檔有一個無效的傳輸速率。

使用者回應： 清除載波資料庫檔。

ICA4092 **預設檔 預設檔案 第 行號 行的資料位元值無效。**

解說： 載波資料庫檔有一個無效的資料位元值。

使用者回應： 清除載波資料庫檔。

ICA4093 **預設檔 預設檔案 第 行號 行的同位值無效。**

解說： 載波資料庫檔有一個無效的同位元值。

使用者回應： 清除載波資料庫檔。

ICA4094 **預設檔 預設檔案 第 行號 行的停止位元值無效。**

解說： 載波資料庫檔有一個無效的停止位元值。

使用者回應： 清除載波資料庫檔。

ICA4095 **無法識別預設檔 預設檔案 第 行號 行的標籤 標籤 ID。**

解說： 載波資料庫檔有一個無效標籤。

使用者回應： 清除載波資料庫檔。

ICA4096 **參數數目錯誤。**

解說： 參考訊息。

ICA4097 **錯誤(程式): 無法建立載波列示。記憶體發生問題。**

解說： 可能是系統或記憶體有問題。

ICA4098 **錯誤(程式): 在進行載波檔 載波檔 呼叫時，發生錯誤。**

解說： 載波資料庫檔有一些無效資料。

使用者回應： 檢查載波資料庫檔內是否有無效標籤。

ICA4099 **錯誤(程式): 無法取得 IPC 記號 錯誤碼。**

ICA4100 **錯誤(程式): 無法建立重試列示。可能是記憶體發生問題。**

解說： 可能是系統發生錯誤或記憶體有問題。

ICA4101	錯誤(載波): 無法建立佇列, <code>page_q_err</code> : 呼叫佇列錯誤。
ICA4102	錯誤(程式): 無法為 <code>SIGTERM/SIGINT</code> 設定信號攔取: 錯誤碼。
解說: 可能系統發生錯誤。	
ICA4103	錯誤(程式): 無法設定載波 載波 的數據機性質。
解說: 無法設定數據機。	
使用者回應: 檢查序列埠架構和起始設定字串。	
ICA4104	遺失載波 載波 的標籤 標籤。
解說: 遺失數據機資訊。標籤可能是傳輸速率、外線...等等。	
使用者回應: 檢查數據機架構檔是否有無效字元。	
ICA4105	載波 載波 至少要列出一個電話號碼。
解說: 載波必須包含電話號碼。	
使用者回應: 用 <code>smitty/SMIT</code> 功能表來新增電話號碼。	
ICA4106	無法開啓檔案 載波檔案名稱。
解說: 必須有載波資料庫檔。	
使用者回應: 如果不存在, 請使用 <code>smitty/SMIT</code> 功能表來建立。	
ICA4107	第 行號 行太長。
解說: 載波資料庫檔內的行太長。	
使用者回應: 檢查載波資料庫檔是否有無效行。	

ICA4108	第 行號 行的標籤不明。
解說: 載波資料庫檔內有不明標籤。	
使用者回應: 檢查載波資料庫檔是否有無效標籤。	
ICA4109	第 行號 行的順序無效。
解說: 載波資料庫檔內有無效順序。	
使用者回應: 檢查載波資料庫檔內是否有無效順序。	
ICA4110	載波 載波 無效, 不予處理。
解說: 載波無法用於呼叫。	
使用者回應: 檢查載波的有效性。	
ICA4111	無法新增載波到列示。
解說: 無法新增載波到列示。	
使用者回應: 檢查載波有效性和電話號碼。	
ICA4112	第 行號 行漏掉載波名稱或者載波名稱太長。
解說: 遺失載波名稱。	
使用者回應: 用 <code>smitty/SMIT</code> 功能表來新增載波。	
ICA4113	無法配置新的呼叫載波: 載波。
解說: 無法配置載波到列示。	
使用者回應: 檢查載波有效性和電話號碼。	
ICA4114	第 行號 行的值太長。
解說: 載波資料庫檔有一行太長。	
使用者回應: 清理載波資料庫檔上過長的字行。	
ICA4115	第 行號 行的標籤 標籤 重複, 不予處理。
解說: 發現重複標籤。	
使用者回應: 從載波資料庫檔移除重複標籤。	

ICA4116 第 行號 行的值不存在。

解說： 發現空白欄位。

使用者回應： 使用 smitty/SMIT 在空白欄位中加入一個值。

ICA4117 第 行號 行的值必須是 Y、Yes、N 或 No。

解說： 這個欄位需要 Y、Yes、N 或 No。

使用者回應： 用 smitty/SMIT 來新增或變更有效的資料。

ICA4118 第 行號 行的值必須大於 0。

解說： 這個欄位必須是正值。

使用者回應： 用 smitty/SMIT 將一個值變更為相反的值。

ICA4119 第 行號 行的值無效。

解說： 指定行上有一個無效值。

使用者回應： 用 smitty/SMIT 功能表來變更值。

ICA4120 載波 名稱 無效而被略過。

解說： 發現無效載波。

使用者回應： 用 smitty/SMIT 功能表來新增有效的載波。

ICA4121 無法新增載波到列示。

解說： 無法新增載波到呼叫列示。

使用者回應： 檢查載波有效性。

ICA4122 第 行號 行的標籤 標籤 重複，不予處理。

解說： 在載波段落上發現重複標籤。

使用者回應： 清理包含重複值的載波段落。

ICA4123 錯誤(程式): 無法取得 IPC 記號：錯誤碼

解說： 程式無法取得 IPC 記號。

ICA4124 錯誤(程式): 讀取佇列時，發生錯誤
呼叫佇列錯誤。

解說： 程式無法讀取佇列。

ICA4125 計數 個佇列項目。

解說： 參考訊息。

ICA4126 已刪除 ID 為 id 的訊息。

解說： 參考訊息。

ICA4127 ID id 不在佇列中。

解說： 參考訊息。

ICA4128 錯誤(程式): 嘗試刪除 ID id 時，發生錯誤
呼叫佇列錯誤。

解說： 嘗試刪除佇列的 ID。

ICA4129 密碼鎖為：entryKey 內容為 @ ptr: ptr。

解說： 僅為參考訊息。

ICA4130 數據機性質：

解說： 數據機起始設定資訊。

ICA4131 名稱：數據機名稱

解說： 數據機起始設定資訊。

ICA4132 Init: initString

解說： 數據機起始設定資訊。

ICA4133 命令狀態：命令

解說：數據機起始設定資訊。

ICA4134 命令終結字元：0x終結字元

解說：數據機起始設定資訊。

ICA4135 撥接：撥接

解說：數據機起始設定資訊。

ICA4136 撥接暫停：暫停

解說：數據機起始設定資訊。

ICA4137 撥號：diallb

解說：數據機起始設定資訊。

ICA4138 撥接 *：dialstar

解說：數據機起始設定資訊。

ICA4139 掛斷：掛斷

解說：數據機起始設定資訊。

ICA4140 有效的命令回應：validCommandresp

解說：數據機起始設定資訊。

ICA4141 有效連線：validConnect

解說：數據機起始設定資訊。

ICA4142 回響：echo

解說：數據機起始設定資訊。

ICA4143 數據機除錯記錄：PUTS(id) txd->
outStr

解說：數據機訊號交換資訊。

ICA4144 數據機除錯記錄：PUTC(id) txd->
outStr

解說：數據機訊號交換資訊。

ICA4145 數據機除錯記錄：GET rxd-> 記錄
id

解說：數據機訊號交換資訊。

ICA4146 數據機除錯記錄：INPUT(記錄 id

解說：數據機訊號交換資訊。

ICA4147 數據機除錯記錄：) rxd->

解說：數據機訊號交換資訊。

ICA4148 數據機除錯記錄：WAITFOR(記錄 id

解說：數據機訊號交換資訊。

ICA4149 無法取消鎖定子訊號。

解說：取消鎖定 SIGCHLD 訊號。

ICA4150 無法鎖定子訊號。

解說：鎖定 SIGCHLD 訊號。

ICA4151 暖開機檔案 filePathname 不存在。

解說：參考訊息。

ICA4152 無法開啓暖開機檔案 filePathname

解說：參考訊息。

ICA4153 暖開機檔案 filePathname 的指令行太
長。

解說：暖開機檔包含某些無效字元。

ICA4154 暖開機檔案 檔案路徑名稱 中有未使用的資料。

解說: 參考訊息。

ICA4155 暖開機檔案 檔案路徑名稱 沒有任何資料。

解說: 參考訊息。

ICA4156 暖開機檔案 檔案路徑名稱 第 行號 行的收件者 位址 錯誤, 不予處理。

解說: 暖開機檔有一些無效字元。參考訊息。

ICA4157 暖開機檔案 檔案路徑名稱 第 行號 行的格式錯誤, 不予處理。

解說: 暖開機檔有一些無效字元。參考訊息。

ICA4158 暖開機檔案 檔案路徑名稱 第 行號 行沒有訊息, 不予處理。

解說: 暖開機檔沒有訊息。參考訊息。

ICA4159 排列暖開機檔案 檔案路徑名稱 的第 行號 行發生錯誤, 不予處理。

解說: 暖開機檔有一些無效字元。參考訊息。

ICA4160 已完成檔案 檔案路徑名稱 的 計數 項訊息暖開機。

解說: 參考訊息。

ICA4161 錯誤(程式): 連續子項錯誤太多。

解說: 一列中有太多子錯誤。若載波或數據機定義檔有一些無效字元, 則會發生這種錯誤。

使用者回應: 用 smitty/SMIT 功能表來檢查載波資料庫檔及數據機定義檔。

ICA4162 子項無法執行 程式: 錯誤碼。

解說: 可能系統發生錯誤。

ICA4163 錯誤(錯誤碼): 子項無法分割子項: 程式名稱。

解說: 可能系統發生錯誤。

ICA4164 無法建立呼叫載波列示。

解說: 內部程式發生錯誤。

ICA4165 進行載波檔 *carrierFile* 呼叫時, 發生錯誤

解說: 載波資料庫包含一些無效資料。

使用者回應: 用 smitty/SMIT 功能表來檢查載波資料庫檔案。

ICA4166 參考訊息。IPC 密碼鎖為: *0xIpcKey*。

解說: 參考訊息。

ICA4167 無法建立佇列, *page_q_err: pageQerr*。

解說: 嘗試建立佇列時失敗。

ICA4168 已在 時間 建立「呼叫暖開機」檔案

解說: 參考訊息。

ICA4169 優先順序 *-p priority numPager*, 來自 *objfrom message*

解說: 參考訊息。

ICA4170 優先順序 *-p priority alpaPager@carrier*, 來自 *from message*

解說: 參考訊息。

ICA4171 優先順序 `-p priority -n numPager@carrier`，來自 `from message`

解說： 參考訊息。

ICA4172 呼叫器暖開機檔案的結尾。

解說： 參考訊息。 表示結束訊息。

ICA4173 無法寫入暖開機檔 `warmstrtFile` 中。

解說： 可能沒有暖開機檔。

ICA4174 時間 **STATUS-REQUEST** 來自 `user@主電腦`

解說： 顯示狀態要求資訊。

ICA4175 時間 **SUMMARY-REQUEST** 來自 `user@主電腦`。

解說： 顯示摘要要求資訊。

ICA4176 計數 個佇列項目。

解說： 計算呼叫器佇列上的佇列項目數目。

ICA4177 最舊的項目：ID `id`，收到時間 時間。

解說： 顯示佇列上最舊的項目。

ICA4178 擴充後再連接記憶體失敗。

解說： 可能系統發生錯誤。

ICA4179 擴展之後重新附加記憶體，對齊失敗。

解說： 可能系統發生錯誤。

ICA4180 無法關閉 `page_q_print()` 中的 **PAGE_Q** 信號：錯誤碼。

解說： 可能系統發生錯誤。

ICA4181 無法啟動 `page_q_print()` 中的 **PAGE_Q** 信號：錯誤碼。

解說： 可能系統發生錯誤。

ICA4182 鏈結 `headLink ->` 訊息 ID：`id`。

解說： 參考訊息。

ICA4183 優先順序：`priority`。

解說： 參考訊息。

ICA4184 人員：名稱。

解說： 參考訊息。

ICA4185 載波：`carrier`。

解說： 參考訊息。

ICA4186 訊息：`message`。

解說： 參考訊息。

ICA4187 無法取得共用的 **RAM**：錯誤碼。

解說： 可能系統發生錯誤。

ICA4188 無法取得附加的共用 **RAM**：錯誤碼。

解說： 可能系統發生錯誤。

ICA4189 無法取得 **PAGE_Q** 信號。

解說： 可能系統發生錯誤。

ICA4190 無法起始設定 `page_q_create()` 中的 `PAGE_Q` 信號：錯誤碼。

解說： 可能系統發生錯誤。

ICA4191 無法設定 `page_q_create()` 中的 `PAGE_Q` 信號：錯誤碼。

解說： 可能系統發生錯誤。

ICA4192 無法關閉 `page_q_empty()` 中的 `PAGE_Q` 信號：錯誤碼。

解說： 可能系統發生錯誤。

ICA4193 無法啟動 `page_q_empty()` 中的 `PAGE_Q` 信號：錯誤碼。

解說： 可能系統發生錯誤。

ICA4194 無法關閉 `page_q_enq(名稱, message)` 中的 `PAGE_Q` 信號：錯誤碼。

解說： 可能系統發生錯誤。

ICA4195 無法啟動 `page_q_enq()` 中的 `PAGE_Q` 信號：錯誤碼。

解說： 可能系統發生錯誤。

ICA4196 `page_q_enq()`: `ID(id)` 優先順序 (`priority`) 人員(名稱) 訊息(`message`)。

解說： 參考訊息。

ICA4197 無法關閉 `page_q_head()` 中的 `PAGE_Q` 信號：錯誤碼。

解說： 可能系統發生錯誤。

ICA4198 無法啟動 `page_q_head()` 中的 `PAGE_Q` 信號：錯誤碼。

解說： 可能系統發生錯誤。

ICA4199 無法關閉 `page_q_first()` 中的 `PAGE_Q` 信號：錯誤碼。

解說： 可能系統發生錯誤。

ICA4200 無法啟動 `page_q_first()` 中的 `PAGE_Q` 信號：錯誤碼。

解說： 可能系統發生錯誤。

ICA4201 無法關閉 `page_q_next()` 中的 `PAGE_Q` 信號：錯誤碼。

解說： 可能系統發生錯誤。

ICA4202 無法啟動 `page_q_next()` 中的 `PAGE_Q` 信號：錯誤碼。

解說： 可能系統發生錯誤。

ICA4203 無法關閉 `page_q_tail()` 中的 `PAGE_Q` 信號：錯誤碼。

解說： 可能系統發生錯誤。

ICA4204 無法啟動 `page_q_tail()` 中的 `PAGE_Q` 信號：錯誤碼。

解說： 可能系統發生錯誤。

ICA4205 無法關閉 `page_q_del()` 中的 `PAGE_Q` 信號：錯誤碼。

解說： 可能系統發生錯誤。

ICA4206 無法啟動 `page_q_del()` 中的 `PAGE_Q` 信號：錯誤碼。

解說： 可能系統發生錯誤。

ICA4207 **page_q_del(*ID*)**。

解說： 除錯資訊。

ICA4208 無法關閉 **page_q_deq()** 中的
PAGE_Q 信號：錯誤碼。

解說： 可能系統發生錯誤。

ICA4209 無法啟動 **page_q_deq()** 中的
PAGE_Q 信號：錯誤碼。

解說： 可能系統發生錯誤。

ICA4210 **page_q_del()**: **ID(*id*)** 優先順序
(*priority*) 人員(*名稱*) 訊息(*message*)。

解說： 參考訊息。

ICA4211 無法關閉 **page_q_walk()** 中的
PAGE_Q 信號：錯誤碼。

解說： 可能系統發生錯誤。

ICA4212 無法啟動 **page_q_walk()** 中的
PAGE_Q 信號：錯誤碼。

解說： 可能系統發生錯誤。

ICA4213 **PAGE_Q** 已滿。

解說： 呼叫佇列已滿。

使用者回應： 在一段時間後傳送呼叫。

ICA4300 正在掛斷。

解說： 正在掛斷電話。

ICA4301 正在起始設定數據機 ..

解說： 正在以起始字串起始設定數據機。

ICA4302 正在撥接

解說： 正在撥接電話。

ICA4303 正在等待連線。

解說： 正在等待數據機連線。

ICA4304 已經連線 速度

解說： 正在以指定的速度 (傳輸速率) 連線

ICA4305 已經連線!!!!!!!

解說： 已連線至呼叫器服務供給者

ICA4306 正在要求「自動模態」的提示。

解說： 正在要求自動模態的提示。正在等待 "ID="

ICA4307 提示 OK.....

解說： 從供給者取回 "ID="。

ICA4308 正在傳送「自動模態要求」。

解說： 正在將 ID 與 SST 傳送給呼叫器服務供給者

ICA4309 傳送「自動模態要求」OK!

解說： 已取得 [p;，表示通信順利

ICA4310 正在送出訊息

解說： 正在送出訊息區塊

ICA4311 正在等待結果

解說： 正在等待確認

ICA4312 已經收到 **Ack**。呼叫成功。

ICA4313 收到 **Nak**，重新傳送區塊。嘗試 *NakTries*

解說：已收到 **Nak**。呼叫器供給者正要求重新傳送

ICA4314 異動發生錯誤。重新傳送區塊。嘗試 *RsTries*

解說：異動發生錯誤。重新傳送區塊。

ICA4315 載波終止連線。

解說：呼叫器供給者已終止交談。打電話給供給者，請求解決問題。

ICA4350 **fwpage** [電訊公司="..."] [數據機="..."] [ID="..."] [msg="..."]

解說：**fwpage** 用法。請檢查您的參數，然後再試一次。

ICA4351 此 檔案不存在

解說：請檢查檔案，查看是否位在正確的目錄下。在使用這個字碼之前，必須先建立 **carriers.cfg**、**modems.cfg** 與 **pager.cfg**。

ICA4352 *What* 檔案損毀。

解說：使用者已修改檔案，但非 **stanze**。所有屬性均應透過 **GUI** 來輸入。

ICA4353 *What* 太長，請縮減後再試一次。

解說：'**What**' 參數太長。請加以縮短，再試一次。

ICA4354 *What* 錯誤。

解說：如果是傳輸速率錯誤，有效的選項為：600、1200、2400、4800、9600、14400；如果是每一位元組的資料位元錯誤，有效選項為：7、8；如果是停止位元錯誤，有效選項為：1、2；如果是外

線前置符號錯誤，您只能輸入號碼；如果是呼叫方法錯誤，本版只支援 **TAP**；如果是呼叫器 **ID** 錯誤，請檢查一下，查看它是否全為數字；如果是同位檢查錯誤，有效選項為：**O**(單數)、**E**(雙數)、**N**(無)、**S**(空格)、**M**(標示)；如果是 **COM** 連接埠錯誤，有效選項為：**COM1**、**COM2**，在這個版本中，**COM** 連接埠應該少於 10；如果是訊息字元錯誤，請檢查訊息，查看其中是否有特殊字元。

ICA4355 在 *where* 中設定參數時，發生錯誤。

解說：無法在 (**where**) 中設定參數。請檢查參數，然後再試一次。

ICA4356 當 *When* 時，**COM** 連接埠發生讀取錯誤。

解說：**COM** 連接埠發生讀取錯誤。將數據機回響設定為開啓，再試一次

ICA4357 當 *Where* 時 **COM** 連接埠發生寫入錯誤。

解說：**COM** 連接埠在寫入資料時，發生錯誤。

ICA4358 設定 *What* 錯誤

解說：依 '**What**' 所指出，設定錯誤。請檢查日誌檔，並找出錯誤所在。

ICA4359 *Where* 超出嘗試次數上限。中止程式

解說：嘗試在 60 分鐘內，開啓 **Com** 連接埠 60 次，且全部失敗。如果發生這種情形，請檢查硬體連線。嘗試在 10 分鐘內傳送呼叫器訊息 10 次，且全部失敗。如果發生這種情形，可能是因為呼叫提供者當機了。

ICA4360 在「載波」電話號碼中有不明字元：
 **pCarrierPhoneNum*

解說： 在載波電話號碼中，找到無法辨識的字元。
請檢查號碼，然後再試一次。

ICA4361 警告!!! 在一般情況下，傳呼提供廠
 商的數據機應該小於 2400。

解說： 這僅是一個警告而已。廣播供給者的數據機速
度的設定值通常應少於 2400。

ICA4362 無法起始設定數據機

解說： 變更數據機起始設定字串，然後再試一次。

ICA4363 數據機傳回錯誤。

解說： 數據機通信錯誤

ICA4364 *tries* 試圖開啓 Com 連接埠時，發
 生錯誤。在 1 分鐘內重試

解說： 開啓 com 連接埠時，發生錯誤。可能是另一
個程式正在使用它。 在 1 分鐘內自動重試。

ICA4365 在 *tries* 嘗試時，無法傳送呼叫。在
 1 分鐘內重試。

解說： 無法傳送呼叫。請檢查日誌檔，找出真正的原因。

ICA4366 訊息太長，已被截斷。

解說： 僅是一個警告。訊息長度太長，所以截斷，以
便放入所提供空間。

ICA4367 將「最長訊息限制」重設為內部定義
 值：訊息長度

解說： 將「最長訊息限制」重設為預設長度，因為使
用者定義的訊息長度大於內部定義的長度 80。

ICA4368 動作：Where 錯誤

解說： 如果是開啓 COM 連接埠時，發生錯誤，請
檢查架構，再試一次；如果是關閉 COM 處理時，發
生錯誤，這是系統問題；如果是清除 COM 時，發生
錯誤，這是系統問題；如果是傳送撥接命令時，發
生錯誤，這是撥接命令問題，請檢查一下，看它是
否為 Haye 相容數據機；如果是傳送 ID 要求時，發
生錯誤，請檢查呼叫器提供者是否支援 TAP 通訊協
定；如果是傳送自動提示時，發生錯誤，請檢查呼
叫器服務是否運作正常；如果是傳送訊息時，發生
錯誤，請檢查日誌檔，找出失敗的原因；如果是提
示錯誤，將無法從呼叫器提供者處取得一個提示。

ICA4369 錯誤太多。正在中止

解說： 錯誤太多，中止這個嘗試。

ICA4370 收到太多的 Nak，正在中止程式

解說： 已從呼叫器供給者處收到過多的 Nak，中止這
個嘗試。

ICA4371 COM 連接埠上的 *szComPort*，函數
 為 函數名稱，傳回 錯誤號碼

解說： 請檢查參數，然後再試一次。

ICA4372 數據機傳回錯誤訊息.....。傳回的訊息

解說： 訊息為：沒有連線、鈴響但沒有連線、沒有載
波、沒有撥號聲、忙線、沒有回答。

ICA4373 (函數名稱) 從數據機或載波傳回不明
 的回覆碼： *char1*、*char2*。

解說： 這個訊息是從數據機或載波的回應，通知您
「防火牆」的呼叫功能無法辨識。 *char1* 及 *char2* 為
回應中前二個字元的 *ascii* (*hex*) 字碼。

使用者回應： 您可在參照數據機說明或載波時，使用
這個資訊，以判斷不明回應的意義。

ICA5005 **SKIT** 起始設定失敗。回覆碼為：回覆碼

解說：安全 socket 起始設定失敗，顯示 SKIT 的回覆碼。

ICA5014 「遠端從屬站通道伺服器」正在傾聽連接埠 伺服器連接埠 #

解說：顯示為 sslrctd 架構的埠號。

ICA5015 已接受來自 *chp0.chp1.chp2.chp3* 的連線

解說：顯示從屬站的IP 位址。

ICA5017 無法取得安全的 socket。函數 **skit_secure_soc_init** retcode 為：函數 *retcode*

解說：無法取得安全 socket，因為 skit_secure_soc_init() 失敗了。

ICA5018 所使用的從屬伺服器加密規格是 *spec1 spec2 spec3*

解說：顯示密碼規格。

ICA5019 無法取得 Free Homenet IP 儲存區。

解說：動態過濾器的問題。

ICA5020 無法開啓遠端用戶端架構檔。

解說：無法取得 /etc/security/rcsfile.cfg。

使用者回應：請檢查檔案是否存在，並檢查其內容。

ICA5021 找不到 '關鍵字' 關鍵字。

解說：/etc/security/rcsfile.cfg 檔案中沒有此關鍵字。

使用者回應：檢查並更正 /etc/security/rcsfile.cfg。

ICA5024 常式名稱 中的函數 **skit_secure_soc_write** 錯誤。

解說：此常式中的 skit_secure_soc_write() 錯誤。

ICA5025 **ACKClient()** 中的函數 **skit_secure_soc_write()** 錯誤。

解說：ACKClient() 常式中的 skit_secure_soc_write() 錯誤。

ICA5026 從 常式名稱 中的「從屬站」接收到無效的回覆碼。

解說：從此常式中的從屬站接收到異常的回覆碼。

ICA5027 從 常式名稱 中的「從屬站」接收到錯誤要求的回覆碼。

解說：在此常式中，回覆碼訊息中的要求程式碼異常。

ICA5028 無效的登入要求。

解說：登入要求訊息的格式無效。

ICA5030 不明的遠端從屬站 ID：遠端從屬站 ID

解說：防火牆機器不認得此使用者 ID。

使用者回應：請更正此遠端從屬站的使用者資訊。

ICA5031 **RCTLoginPhase** 中的函數 **skit_secure_soc_write** 錯誤。

解說：登入階段的 skit_secure_soc_write() 錯誤。

ICA5035 無效的登出要求。

解說：登出要求訊息的格式無效。

ICA5067 取得無效的封包。

解說：所收到的封包格式無效。

ICA5078 在 `SvrReqHandler()` 中取得無法辨識的要求

解說: 無法識別所收到的要求, 將忽略該要求。

ICA5082 已切斷與從屬站 遠端從屬站 ID 的通道。

解說: 已切斷此遠端從屬站 ID 的通道。

ICA5086 ID: 使用者 ID 尚未定義。

解說: 防火牆機器上沒有此使用者 ID。

ICA5087 '使用者 ID' 無法通過鑑證。

解說: 此使用者 ID 的鑑證失敗。

ICA5089 函數 `rcFilterClear()` 失敗。回覆碼為 回覆碼。

解說: `rcFilterClear()` 失敗, 回覆碼如上所述。

使用者回應: 請檢查 IPSEC LAN 從屬站是否存在。這些產品不可並存。

ICA5090 函數 `rcFilterInit()` 失敗。回覆碼為 回覆碼

解說: `rcFilterInit()` 失敗, 回覆碼如上所述。

ICA5091 函數 `TunnelUp()` 無法執行可執行檔 命令行。

解說: 所顯示之命令行的 `system()` 呼叫失敗。

ICA5092 無法取得 `recoverstash` 函數呼叫的鎖環通行碼。

解說: 無法恢復隱藏檔的鎖環通行碼。

ICA8001 **SYSLOG/udp**: 不明的服務程式

ICA8002 函數名稱 函數失敗 - 錯誤碼,
`errno2 = 0xerrno2`

解說: 處理終止, 因為 `syslogd` 無法執行所指定的函數。該錯誤碼資訊附加在錯誤訊息上。

使用者回應: 請聯絡系統程式設計師。系統程式設計師: 使用該錯誤碼資訊來判定造成失敗的原因。

ICA8004 在 `AF_INET socket` 上偵測到錯誤, `\ slogd` 不再監督 `socket`

ICA8006 不明的優先順序名稱 \"優先順序\"

解說: 在架構檔中找到一個無效的優先順序名稱。

使用者回應: 請聯絡系統程式設計師。系統程式設計師: 檢查架構檔。

ICA8007 不明的機能名稱 \"機能\"

解說: 在架構檔中找到一個無效的機能名稱。

使用者回應: 請聯絡系統程式設計師。系統程式設計師: 檢查架構檔。

ICA8008 在 時間標記 收到來自 `SYSLOG@` 主電腦名稱 的訊息...

解說: 系統日誌常駐程式架構檔包含一個項目, 可將系統日誌訊息傳送給所有已登入的使用者。此訊息會傳送給所有目前登入系統日誌常駐程式所正在執行之系統的使用者。

使用者回應: 非系統程式設計師: 無

ICA8009 收到訊號 訊號 後結束 **SYSLOG**

解說: 系統日誌常駐程式收到已造成系統日誌常駐程式結束的訊號。

使用者回應: 非系統程式設計師: 無

ICA8010 已經重新啟動 SYSLOGD

ICA8012 SYSLOGD 無法記錄到 SMF - 錯誤本文

解說: 將記錄寫入 SMF 時，發生錯誤。該錯誤本文資訊附加在錯誤訊息上。

使用者回應: 請聯絡系統程式設計師。系統程式設計師：使用該錯誤本文資訊來判定造成 SMF 寫入失敗的原因。

ICA8013 更新處理狀態失敗，回覆碼 = 0x回覆碼

解說: 嘗試為「防火牆」核心處理更新 syslogd 處理的狀態時，發生錯誤。回覆碼描述出從更新處理狀態呼叫傳回的特定錯誤。

使用者回應: 請聯絡系統程式設計師。系統程式設計師：聯絡服務代表。

ICA8014 在 SYSLOGD 呼叫指定的選項 (-startup_option) 不明

解說: 嘗試啟動 syslogd 常駐程式處理時，發生錯誤。syslogd 的呼叫不支援所指定的選項。

使用者回應: 請檢查啟動選項，並重新啟動 syslogd 常駐程式。系統程式設計師：如果還是有問題，則請連絡服務代表。

ICA8015 架構檔項目 (架構資料) 無效

解說: 嘗試解析 SYSLOG 架構檔的架構項目時，發生錯誤。

使用者回應: 請檢查架構檔項目，並重新啟動 syslogd 常駐程式。系統程式設計師：如果還是有問題，則請連絡服務代表。

ICA8016 檔案名稱 的 函數名稱 失敗 - 錯誤碼

解說: 嘗試執行所指定之裝置的函數時，發生錯誤。該錯誤碼資訊附加在錯誤訊息上。

使用者回應: 請驗證所指定的裝置是否存在，並重試要求。如果還是有問題，則請連絡系統程式設計師。系統程式設計師：如果還是有問題，則請連絡服務代表。

ICA8050 函數 失敗。error_text

解說: 執行訊息中所顯示的函數時，發生錯誤。該錯誤的更多資訊是由錯誤訊息所提供。

使用者回應: 更正訊息中所指定的錯誤；必要時，重試此作業。

ICA8051 函數 失敗：回覆碼 = 0xreturn_code

解說: 執行訊息中所顯示的函數時，發生錯誤。來自指定的函數之回覆碼也在訊息中顯示出。

使用者回應: 更正訊息中所指定的錯誤；必要時，重試此作業。

ICA8052 FWSTACKD 正在為 stack_name 啟動過濾器記載。

解說: FWSTACKD 正在嘗試啟動封包過濾器記載。

系統動作: 程式繼續執行。

ICA8053 FWSTACKD 無法為 stack_name 啟動過濾器記載。error_text

解說: 無法啟動封包過濾器記載，其原因說明於所附的錯誤訊息中。

系統動作: 不執行過濾器記載。

使用者回應: 使用錯誤訊息來更正該錯誤，然後以 **fwfilter cmd=startlog** 重新啟動過濾器記載。

ICA8054 FWSTACKD 正在為 *stack_name* 啟動 NAT 記載。

解說： FWSTACKD 正在嘗試啟動網路位址轉換 (NAT) 記載。

系統動作： 程式繼續執行。

ICA8055 FWSTACKD 無法為 *stack_name* 啟動 NAT 記載。 *error_text*

解說： 無法啟動網路位址轉換 (NAT) 記載，其原因說明於所附的錯誤訊息中。

系統動作： 不執行網路位址轉換記載。

使用者回應： 使用錯誤訊息來更正該錯誤，然後以 **fwnat cmd=startlog** 重新啟動網路位址轉換記載。

ICA8056 FWSTACKD 正在為 *stack_name* 啟動 NAT。

解說： FWSTACKD 正在嘗試啟動網路位址轉換 (NAT)。

系統動作： 程式繼續執行。

ICA8057 FWSTACKD 無法為 *stack_name* 啟動 NAT。 *error_text*

解說： 無法啟動網路位址轉換 (NAT)，其原因說明於所附的錯誤訊息中。

系統動作： 不執行網路位址轉換。

使用者回應： 使用錯誤訊息來更正該錯誤，然後以 **fwnat cmd=update** 重新啟動網路位址轉換。

ICA8058 FWSTACKD 正在為 *stack_name* 重新啟動通道定義。

解說： FWSTACKD 正在嘗試啟動通道定義，這些定義在系統關閉時仍可使用。

系統動作： 程式繼續執行。

ICA8059 FWSTACKD 無法為 *stack_name* 重新啟動通道定義。 *error_text*

解說： 無法啟動通道定義，其原因說明於所附的錯誤訊息中。

系統動作： 尚未啟動通道定義。

使用者回應： 使用錯誤訊息來更正該錯誤，然後以 **fwtunnel cmd=activate** 重新啟動通道定義。

ICA8060 FWSTACKD 正在為 *stack_name* 啟動過濾及 Socks 規則。

解說： FWSTACKD 正在嘗試啟動目前的封包過濾規則及 Socks 規則集。

系統動作： 程式繼續執行。

ICA8061 FWSTACKD 無法為 *stack_name* 啟動過濾及 Socks 規則。 *error_text*

解說： 無法啟動過濾規則及 Socks 規則，其原因說明於所附的錯誤訊息中。

系統動作： 預設過濾規則將生效。則會允許本端存取，而拒絕所有其他的存取。

使用者回應： 使用錯誤訊息來更正該錯誤，然後以 **fwfilter cmd=update** 重新啟動過濾及 Socks 規則。

ICA8062 FWSTACKD 正在為 *stack_name* 啟動 RealAudio 支援。

解說： FWSTACKD 正在嘗試啟動 Real Audio 支援。

系統動作： 程式繼續執行。

ICA8063 FWSTACKD 無法為 *stack_name* 啟動 RealAudio 支援。 *error_text*

解說： 無法啟動 Real Audio 支援，其原因說明於所附的錯誤訊息中。

系統動作： RealAudio 服務程式仍不可用。

使用者回應: 使用錯誤訊息來識別該錯誤，修正該錯誤，然後以 **fwaudio cmd=change** 啟動 Real Audio。

ICA8064 函數 失敗。 *error_text*

解說: 執行訊息中所顯示的函數時，發生錯誤。該錯誤的更多資訊是由錯誤訊息所提供。

使用者回應: 更正訊息中所指定的錯誤；必要時，重試此作業。

ICA9000 **IBM Firewall 評估版將在 天數 天後過期。**

解說: 這個軟體被標示為評估版，顧名思義，其本身是無效的。

ICA9001 「檔案系統完整性檢查程式」警告 - 警告說明本文

解說: fwfschk 在檔案系統中發現矛盾 - 潛在的威脅

ICA9002 最後的訊息重複了 %1\$d 次

解說: 當記載相同訊息，且沒有任何介入訊息時，AIX syslogd 所產生的訊息。訊息將保存在這裡，以供「日誌監督程式」夠偵測到狀況。這個訊息的語言必須是寫入真正 syslogd 訊息時所用的語言。

ICA9003 使用者 名稱 無法通過架構伺服器的鑑證。

解說: FW 架構伺服器無法鑑證所指出的使用者。

使用者回應: 請洽詢您的 FW 管理者。

ICA9004 使用者 名稱 順利通過架構伺服器的鑑證。

解說: FW 架構伺服器已鑑證所指出的使用者。

ICA9005 正在啟動遠端架構伺服器。

解說: 已啟動架構伺服器。

ICA9006 正在結束遠端架構伺服器。

解說: 正在結束架構伺服器。

ICA9007 遠端架構伺服器無法開啓訊息目錄。

解說: 遠端架構伺服器所使用的一個或多個訊息目錄可能已遺失。

使用者回應: 請洽詢您的 FW 管理者。

ICA9008 遠端架構伺服器在 **getpeername()** 時失敗：錯誤 錯誤碼。

解說: 架構伺服器無法取得本身的相關資訊。

使用者回應: 請洽詢您的 FW 管理者。

ICA9009 遠端架構伺服器在 **getsockname()** 時失敗：錯誤 錯誤碼。

解說: 架構伺服器無法取得關於自己的資訊。

使用者回應: 請洽詢您的 FW 管理者。

ICA9010 遠端架構伺服器無法取得配接卡資訊。

解說: 架構伺服器無法取得配接卡資訊。

使用者回應: 請洽詢您的 FW 管理者。

ICA9011 沒有為遠端架構啟動架構伺服器。

解說: 架構伺服器在它的架構檔中具有 local=yes 的設定，且從屬站是在遠端機器上。

使用者回應: 請洽詢您的 FW 管理者。

ICA9012 遠端架構伺服器無法讀取登入要求。

解說: 架構伺服器無法讀入從屬站登入要求。

使用者回應: 請洽詢您的 FW 管理者。

ICA9013 遠端架構伺服器收到錯誤的登入要求。

解說：登入要求含有不正確的資訊。

使用者回應：請洽詢您的 FW 管理者。

ICA9014 遠端架構伺服器無法建立管道。

解說：架構伺服器無法建立鑑證管道。

使用者回應：請洽詢您的 FW 管理者。

ICA9015 遠端架構伺服器無法建立處理。

解說：架構伺服器無法建立鑑證處理。

使用者回應：請洽詢您的 FW 管理者。

ICA9016 正在啟動 EFM 常駐程式。

解說：已在受管理的防火牆上，啟動 EFM 常駐程式。

ICA9017 正在結束 EFM 常駐程式；rc = 參數值。

解說：正在以所指定的回覆碼結束 EFM 常駐程式。

ICA9018 EFM 常駐程式無法開啓訊息目錄。

解說：EFM 所使用的一個或多個訊息目錄可能已遺失。

使用者回應：請洽詢您的 FW 管理者。

ICA9020 無法切換執行中的使用者 ID。

解說：無法產生系統呼叫，來切換執行中的使用者 ID。

使用者回應：請洽詢您的 FW 管理者。

ICA9021 這個防火牆不支援 *logon* 模式。

解說：這個防火牆不支援這個特定模式。

使用者回應：請洽詢您的 FW 管理者。

ICA9022 使用者 未經授權，不能以 登入 模式登入防火牆。

解說：這個使用者名稱未取得授權，無法使用這個特殊模式來登入。

使用者回應：請洽詢您的 FW 管理者。

ICA9023 無法載入 EFM DLL。

解說：無法載入 efm dll。

使用者回應：請洽詢您的 FW 管理者。

ICA9024 將 使用者 所啟動的要求轉送至防火牆 機器。

解說：已啟動轉送要求。

ICA9025 轉送要求已結束，回覆碼為 回覆碼。

解說：轉送作業完成。

ICA9026 於 時間 時，在防火牆 機器 上收到 使用者 的轉送要求。

解說：已在上述時間啟動了轉送作業。

ICA9027 函數 函數 中的檔案 檔案名稱 已新增至轉送要求中。

解說：將轉送所指定的檔案。

ICA9028 將 使用者 所啓始的要求啓動至防火牆 機器。

解說：已開始啓動作業。

ICA9029 啓動要求結束，回覆碼為 回覆碼。

解說：已完成啓動作業。

ICA9030 於 時間 時，在防火牆 機器 上收到使用者 的啟動要求。

解說： 已在上述時間啟動了啟動作業。

ICA9031 已結束啟動函數 函數 ，回覆碼為回覆碼。

解說： 已完成啟動所指定的函數。

ICA9032 已於 日期 時間 更新 NAT 架構。

解說： NAT 架構已更新。

ICA9033 已於 日期 時間 起始設定 NAT 支援 (層次 版本.版次)。

解說： 已起始設定防火牆 NAT 支援。

ICA9034 已於 日期 時間 停止 NAT 支援。

解說： 已停用 NAT 支援。

ICA9035 NAT 無法為「安全位址」安全 IP 位址 配置「已登記的位址」。

解說： 未轉換「安全的位址」，因為「已登記的 IP 位址」儲存區中沒有可用的位址。

ICA9036 NAT 將「已登記的位址」已登記的位址 釋放至位址儲存區。

解說： 「已登記的位址」已釋放至已登記的 IP 位址儲存區。

ICA9037 已於 時間及日期 自動更新防火牆介面。

解說： 「防火牆」起始設定程式已呼叫 **UpdateInterfaces()**，以觸發「防火牆」介面檔案 fwadpt.cfg 的自動更新功能。

系統動作： 無

使用者回應： 無

ICA9038 已將介面 位址 從「防火牆」架構移除。

解說： 已將所列出的「帶點十進位數位址」列示在「防火牆」架構檔案 fwadpt.cfg 中，但是 TCP 堆疊並不知道，因此，已從該架構檔移除。

系統動作： 無

使用者回應： 無

ICA9039 已將介面 位址 新增至「防火牆」架構中。

解說： TCP 堆疊已找到所列出的「帶點十進位數位址」，但是在「防火牆」架構檔案 fwadpt.cfg 中並沒有發現，因此，已新增至該架構檔。

系統動作： 無

使用者回應： 無

ICA9040 介面 位址 遮罩已由 舊遮罩 改為新遮罩。

解說： fwadpt.cfg 檔案中的遮罩與硬體上所安裝的遮罩不符。已將正確的遮罩欄位更新在 fwadpt.cfg 檔案中。

系統動作： 無

使用者回應： 無

ICA9041 在這台機器上找不到介面。

解說： 在這台機器上找不到配接卡介面。

系統動作： 無

使用者回應： 無

ICA9042 NAT 以作用中的 many-to-one 位址 many-to-one 位址 來啟動。

解說： NAT 已成功地起始設定，現在可使用。但若位址為 0，即意味仍不可使用 many-to-one 轉換。

系統動作： 無

使用者回應: 無

ICA9043 NAT 無法起始設定，回覆碼 rc。

解說: NAT 無法起始設定，現在仍不可用。

系統動作: 不會呼叫任何 NAT 函數。

使用者回應: 若使用者想要 NAT 函數，查看回覆碼並加以調整更正。若無法解決此問題，請連絡 IBM 服務人員。

ICA9044 停用 NAT。

解說: NAT 已成功停用，現在非使用中。

系統動作: 無

使用者回應: 無

ICA9045 NAT 已為安全位址：連接埠 安全位址：連接埠 配置位址：連接埠位址：連接埠

解說: NAT 已為安全主電腦配置位址儲存區中的位址：連接埠。

系統動作: 無

使用者回應: 無

ICA9046 NAT 無法為安全位址 安全位址 配置 many-to-one 位址。

解說: NAT 已用盡 many-to-one 位址的連接埠。

系統動作: 已捨棄本端主電腦的封包。

使用者回應: 意味著，有太多正在等待的連線。管理者可能需要縮短 many-to-one 位址連結的逾時，以便更快除去閒置轉換表格項目。

ICA9047 NAT 已從安全位址：連接埠 安全位址：連接埠 取消配置位址：連接埠位址：連接埠。

解說: NAT 已將所指定的位址：連接埠組退回可用的儲存區。

系統動作: 無

使用者回應: 無

ICA9048 NAT 偵測到通訊協定：通訊協定 位址：連接埠 位址：連接埠 安全位址：連接埠安全位址：連接埠之片段封包。

解說: NAT 偵測到片段的 FTP 控制封包或是片段的 ICMP 錯誤訊息。雖然未檢查資料欄 (payload)，NAT 仍會轉換片段的 FTP 控制封包。若是片段的 PORT 命令，因為訊息所含的 IP 位址尚未轉換，FTP 資料將會失敗。若封包是片段的 ICMP 錯誤訊息，則會被捨棄。

系統動作: 請參閱解說。

使用者回應: 如果重複發生這情況，請通報 IBM 服務人員。

ICA9049 NAT 偵測到脫序的片段，無法轉換來源位址 到 目的地位址。

解說: NAT 偵測到片段的資料包，其較資料包第一個片段先到達。

系統動作: NAT 無法正確轉換該片段，因而捨棄該資料包。

使用者回應: 如果重複發生這情況，請通報 IBM 服務人員。

ICA9050 NAT 無法轉換來自位址：連接埠 位址：連接埠 通訊協定 通訊協定 之封包到安全位址：連接埠 安全位址：連接埠，回覆碼為 rc。

解說: NAT 無法轉換封包。

系統動作: 已捨棄封包。

使用者回應: 如果重複發生這情況，請通報 IBM 服務人員。

ICA9051 **NAT** 偵測到來自安全位址：連接埠
安全位址：連接埠 通訊協定 通訊協定
之封包到達位址：連接埠 位址：
連接埠

解說： NAT 偵測到封包到達。

系統動作： 無

使用者回應： 無

ICA9052 **NAT** 偵測到來自安全位址：連接埠
安全位址：連接埠 通訊協定 通訊協定
之封包正要前往位址：連接埠 位
址：連接埠

解說： NAT 偵測到封包離埠。

系統動作： 無

使用者回應： 無

ICA9053 %3\$d 中有 字串值 檔案名稱

解說： 偵錯中

系統動作： 無

使用者回應： 無

ICA9054 **IP** 位址 位址 不可既是
many-to-one 位址同時又是非安全/
安全位址。

解說： 兩者不可相同。

系統動作： 不執行所要求的動作。

使用者回應： 請選擇不同的非安全/安全位址或是不同 many-to-one 位址。

ICA9055 **NAT** 偵測到脫序的片段，可轉換 來
源位址 到 目的地位址。

解說： NAT 偵測到抵達時脫序的內部或最終資料包
片段。

系統動作： NAT 可正確轉換該片段，所以並未捨棄
該資料包。

使用者回應： 無

ICA9060 嚴重的架構伺服器起始設定錯誤 -
socket()：系統錯誤訊息

解說： 架構伺服器起始設定失敗，已終止常駐程式。

使用者回應： 請更正所指出的系統問題，並重新啟動
架構伺服器。

ICA9061 嚴重的架構伺服器起始設定錯誤 -
listen()：系統錯誤訊息

解說： 架構伺服器起始設定失敗，已終止常駐程式。

使用者回應： 請更正所指出的系統問題，並重新啟動
架構伺服器。

ICA9062 嚴重的架構伺服器錯誤 - **main**
accept()：系統錯誤訊息

解說： 架構伺服器的主要常式失效，已終止常駐程
式。

使用者回應： 請更正所指出的系統問題，並重新啟動
架構伺服器。

ICA9063 架構伺服器錯誤 - 失敗的函數：回覆
碼 = 0x函數回覆碼

解說： 架構伺服器偵測到所指出函數中的錯誤。 常
駐程式終止。

使用者回應： 請更正所指出的系統問題，並重新啟動
架構伺服器。

ICA9064 選項 -參數值 不明，不予處理。

解說： 已指示的選項，但無法辨識該旗號。

ICA9065 **架構伺服器錯誤 - 失敗的函數: 系統錯誤訊息**

解說: 架構伺服器偵測到所指出函數中的錯誤。常駐程式終止。

使用者回應: 請更正所指出的系統問題，並重新啟動架構伺服器。

ICA9066 **記憶體不足：架構伺服器：
malloc(位元組) 傳回 NULL 於函數
function_name。**

解說: 無法配置足夠的記憶體 - malloc 傳回 NULL。

ICA9067 **連結失敗，位址：連接埠 已在使用中。**

解說: 給定的連接埠位址目前在使用中。

系統動作: 已終止架構伺服器。

使用者回應: 請使用不同的連接埠位址，連線到「架構伺服器」，或請聯絡您的「防火牆」管理者。

ICA9068 **-參數值 選項失敗或指定錯誤。**

解說: 所指出的選項失敗，或指定錯誤。

系統動作: 已終止架構伺服器。

使用者回應: 請更正所指出的選項用法，重新啟動架構伺服器。

ICA9069 **SSL 起始設定失敗。**

解說: 無法起始設定 SSL 加密環境，或是與夥伴訊號交換失敗。

系統動作: 已終止架構伺服器。

使用者回應: 請洽詢「防火牆」管理者，驗證 SSL 環境。

附錄B. 強化「Windows NT 系統架構」

強化是一種處理，它能夠經由關閉不必要的常駐程式及停用沒有授權的使用者 ID，發揮最大的安全效果與工作效率。強化是 IBM Firewall 軟體安裝作業的一部份，可編輯危及安全性的系統資源。

將會停用 IBM Firewall 架構不需要的服務程式及可能威脅安全性的服務程式。並且會刪除所有非 TCP/IP 通訊協定。

附錄C. 取得備註的要求 (RFC)

「備註的要求 (RFC)」為新通訊協定與建立 Internet 通訊協定套組標準的文件。所有 RFC 的相關書籍皆可向 Network Information Center (NIC) 單獨購買或以訂閱的方式取得。您可以從下列位置中取得這些文件：

Government Systems, Inc.
Attn: Network Information Center
14200 Park Meadow Drive
Suite 200
Chantilly, VA 22021

您可以從這個 URL 存取 RFC：

<http://www.cis.ohio-state.edu/hypertext/information/rfc.html>.

可使用 FTP 連線至 `ds.internic.net`，從 NIC 取得線上拷貝。您可以使用下列格式來轉送檔案：

RFC:RFCnnnn.TXT
RFC:RFCnnnn.PS

其中：

nnnn RFC 號碼

TXT 為文字格式

PS 為 PostScript 格式

RFC 索引的格式為：

RFC:RFC-INDEX.TXT

註：很多 RFC 都只有文字格式。因此，在您索取 PostScript 檔案之前，請先查看「RFC 索引」，以確定 RFC 有該格式的檔案。您也可以利用電子郵件，將訊息傳送至 `mailserv@ds.internic.net`，以向自動化 NIC 郵件伺服器要求 RFC 的線上拷貝。您必須在您的附註主體中，包括下列其中一個命令：

SEND RFCnnnn.TXT
或
SEND RFCnnnn.PS

其中：

nnnn RFC 號碼

TXT 為文字格式

PS 爲 PostScript 格式

假設您要索取文字格式的 RFC 812，您就要在您的郵件本文中指定：

SEND RFC812.TXT

欲索取 RFC 索引的線上拷貝，則在您的郵件本文中併入下列命令：

SEND RFC-INDEX.TXT

附錄D. IBM eNetwork Firewall Socks5.conf 架構檔格式

在預設的狀況下，架構檔 **socks5.conf** 會位於 IBM Firewall 的安裝程式目錄下。若有需要，您可以使用文字編輯程式來編輯這個檔案。

在第一次呼叫伺服器時，會讀取 **socks5.conf** 架構檔。(若要在不關閉的情況下復新，請鍵入 **socks5.config**。) 此檔包含 IBM Firewall 在決定要使用哪一個介面以到達特定位址（無論是直接連線至特定位址或是使用 proxy 伺服器）時，所需的全部資訊，以及符合 proxy 連線所需的基本條件。

架構檔中將出現下列部份：

- 別名
- 變數
- 模組
- 鑑證
- 遞送路徑
- Proxies
- 存取控制

在「鑑證」、「遞送路徑」、Proxies 及「存取控制」部份中，將依序讀取行，直至該部份符合的行：行的順序是非常重要的。針對欲符合的行，該行中的每一項目均需符合。

指定連接埠

可以使用名稱、號碼或範圍來指定連接埠。範圍以 [或 (為開始，且以) 或] 為結束，視範圍是否包含在內而定。範圍之內，定界符號應為兩個連接埠指定元（名稱與號碼），以逗點隔開。指定連接埠的方法及稱為連接埠型樣。

指定主電腦

經常需要主電腦位址與網路遮罩來指定引用於特定規則的主電腦。指定主電腦的方法及稱為主電腦型樣。有數種方式可用於指定 host/mask 組合：

參數	說明
hostIP/ mask	具有遮罩的主電腦位址 "ANDed" 必需與具有遮罩的主電腦 IP "ANDed" 相同。一般用於從網路或子網路部份遮罩掉位址的主電腦部份。
-	全部都符合。允許所有主電腦。

參數	說明
n1	相等於 n1.0.0.0/255.0.0.0。
n1.n2	相等於 n1.n2.0.0/255.255.0.0。
n1.n2.n3	相等於 n1.n2.n3.0/255.255.255.0。
.domain.name	主電腦名稱必須以字串 .domain.name 為結束。
a.host.name	主電腦名稱必須完全符合 a.host.name。

也不支援較舊的主電腦型樣語法，說明如下。但是，建議您採用較新的方法且其較易閱讀。

參數	說明
hostIP/a	全部都符合（與 "-" 相同）。允許所有主電腦。
hostIP/n	網路符合。遮罩掉主電腦及位址的子網路部份，僅留網路部份。用於執行此項作業的遮罩依據主電腦 IP 位址的類別而有不同。
hostIP/s	子網路符合。遮罩掉位址的主電腦部份，僅留子網路及網路部份。用於執行此項作業的遮罩依據主電腦 IP 位址的類別而有不同。
hostIP/h	主電腦符合。相等於主電腦 IP。

指定鑑證方法

我們所提供的鑑證方法有 *ibmcram* 及 *ibmpwd*。您可以增加其他鑑證方法。

您可以利用逗點隔開鑑證方法來指定一列示的鑑證方法。所選擇的鑑證方法必須符合列示中出現的其中一種方法。此語法即稱為鑑證型樣。在預設的狀況下，將定義鑑證方法為 NULL。藉由載入適宜模組，可以併入其他方法。 "-" 表示接受任何鑑證方法（包含 NULL）。

鑑證項目

鑑證項目指出可使用鑑證的類型。其格式如下：

```
auth/ban source-address source-port
auth-methods
```

參數	說明
auth/ban	無論鑑證項目已授權 (auth) 或未授權 (ban)。
source-address	有效的主電腦型樣。

參數	說明
source-port	有效的連接埠型樣。
auth-methods	有效的驗證型樣。

關鍵字 "ban" 指出不應嘗試鑑證此主電腦且該特定伺服器無有效的使用。

若未指定 `auth/ban` 行時，其預設為任何鑑證方法均可接受。若將連線的權限設定成 `deny`（預設值），直到引用鑑證之後，才會拒絕連線。在 `SOCKS5` 通訊協定中，鑑證發生於授權之前。您必須完全依據主電腦來決定如何鑑證主電腦。

指定命令

亦可以逗號隔開命令來指定一列示的命令。此語法，即稱為命令型樣。已定義的命令為：`connect`、`bind`、`udp`、`ping` 及 `traceroute`。您可利用模組來新增其他命令。"`-`"（破折號）表示可接受任何命令。

載入模組

利用模組可讓您新增鑑證方法、命令、權限檢查及內容過濾器來自行擴展伺服器的功能性。其格式如下：`module stub filename options`

參數	說明
module	載入的模組識別碼。
stub	存取功能名稱的模組相關名稱之前置符號。
filename	載入的模組檔案名稱。
options	模組特定的架構資訊（若有的話）。

模組可定義用於各處的欄位，所以最好先存放模組行。例如，鑑證模組定義使用於 `auth` 與 `permit` 行的鑑證方法名稱。

遞送路徑項目

在具有多重網路介面（因此，也具有多重 IP 位址）的機器上，請確定特定的網路介面是與特定的位址相關連的。藉由確定內部機器使用內部網路介面，而外部機器使用外部網路介面，可防止 "IP 詐騙"（網路外的機器假冒為網路內的機器）。`SOCKS` 伺服器在接受 `BIND` 要求或是發出 `SENDTO` 要求時，也可利用它來決定所要連結的網路介面。若無符合的項目，將使用 `INADDR_ANY` 來連結，且在任何介面上接收連線。單一網路的主電腦無需遞送路徑項目：其僅在具有一個網路介面以上的機器，才是必須的。其格式如下：`route dest-address dest-port interface-address`

參數	說明
route	用以指出遞送路徑項目的關鍵字。
dest-address	有效的主電腦型樣。
dest-port	有效的連接埠型樣。
interface-address	網路介面卡的 IP 位址，或網路介面的名稱（例如，elink31）。

變數項目

架構檔中的某些變數及旗號可以控制記載與參考訊息的數量及類型。格式為：**set** *variable value*

參數	說明
set	用來設定供本端使用的環境變數之關鍵字。
variable	有效的環境變數。請參閱下面的第140頁的『環境變數』，取得可用變數的列示。
value	指派的值。

環境變數

環境變數	說明
SOCKS5_BINDPORT [port]	將 IBM Firewall 架構為使用指定的連接埠，而不是使用連接埠 1080 的預設值。
SOCKS5_RECVFROMANYONE	如果啓用 UPD 支援，其允許 UPD 從屬站接收來自不明送件者的訊息。
SOCKS5_USECLIENTSPORT	只在 IBM Firewall 可連結至與從屬站用來傳送訊息的同一連接埠時，才將 IBM Firewall 架構成 proxy。當伺服器傳輸資料至從屬站時（在從屬站傳送訊息至伺服器之前傳送訊息至從屬站），proxying UDP 連線是必要的。這個用法的範例為 RealAudio。
SOCKS5_MAXCHILD	並行緒的最大數。
SOCKS5_NOREVERSEMAP	停用 IP 位址至主電腦名稱的對映。若在架構檔中指派別名，此舉將增加記載資訊的效能。
SOCKS5_NOSERVICENAME	停用埠號至服務程式名稱的對映。若在架構檔中指派別名，此舉將增加記載資訊的效能。

環境變數	說明
SOCKS5_NOIDENT	即使在編譯中，請停用 IDENT 要求。當您至從屬站的鏈結較慢且非使用 IDENTD，其為有用的。此舉將減少逾時期間。
SOCKS5_DEMAND_IDENT	若無來自從屬站的 IDENT 回應，請將 NULL 鑑證架構成失敗。其在確定使用者名稱永遠與連線要求相關連上非常有效。

Proxy 項目

Proxy 項目說明 SOCKS proxy 伺服器的位址。這些行告之伺服器如何連絡特定的主電腦。若無行符合主電腦，將直接連絡主電腦。其格式如下：*proxy-type dest-addr dest-port proxy-addr proxy-port*

參數	說明
proxy_type	proxy 伺服器的類型。有效的項目為： <ul style="list-style-type: none"> socks5 socks4 no proxy
dest-address	有效的主電腦型樣。
dest-port	有效的連接埠型樣。
proxy-address	IP 位址或 proxy 伺服器的名稱。
proxy-port	proxy 伺服器位於接受連線的 SOCKS 常駐程式上。

存取控制項目

存取控制部份決定允許或拒絕建立連線的要求。其有兩種類型，分別為允許行及拒絕行。行中的每一項目必須符合欲符合的整行。其格式如下：

```
permit auth cmd src-host dest-host src-port dest-port [userlist]
deny auth cmd src-host dest-host src-port dest-port [userlist]
```

參數	說明
auth	鑑證方法的列示，由有效的鑑證型樣及項目所指定。
cmd	符合此行所指定命令的有效命令型樣。
scr-host	來源主電腦的有效主電腦型樣。
dest-host	目的地主電腦的有效主電腦型樣。

參數	說明
scr-port	來源主電腦的有效連接埠型樣。
dest-port	目的地主電腦的有效連接埠型樣。
userlist	有效的使用者型樣。

過濾

過濾器指引執行透過載入模組的過濾處理。其格式如下：

```
filter name auth cmd src-host dest-host src-port dest-port [userlist]
```

參數	說明
name	過濾器模組的識別碼。
auth	鑑證方法的列示，由有效的鑑證型樣及項目所指定。
cmd	符合此行所指定命令的有效命令型樣。
scr-host	來源主電腦的有效主電腦型樣。
dest-host	目的地主電腦的有效主電腦型樣。
scr-port	來源主電腦的有效連接埠型樣。
dest-port	目的地主電腦的有效連接埠型樣。
userlist	有效的使用者型樣。

參考書目

Internet 安全性的相關資訊，請造訪 IBM Firewall 首頁：

<http://www.software.ibm.com/enetwork/firewall>。

IBM 出版品中的資訊

防火牆、Internet 安全性及一般安全性主題之相關資訊的其他 IBM 來源列於此處。

防火牆主題

您可在 IBM Firewall CD-ROM 及 IBM eNetwork Firewall 首頁取得下列文件。

- *IBM eNetwork Firewall 使用指南*, GC40-0213
- *IBM eNetwork Firewall 參考手冊*, SC40-0214
- *Guarding the Gates Using the IBM eNetwork Firewall for NT 3.2*, SG24-5209

Internet 及全球資訊網主題

- *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

一般安全性主題

- *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

企業出版品中的資訊

這些企業出版品均與 sendmail、TCP/IP 及 UNIX 有關：

- 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)
- 這些企業出版品均與 Internet 中的防火牆與安全性有關：
- 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)

注意事項

本書在提及一些 IBM 產品、程式或服務時，不暗示 IBM 會在有業務營運的所有國家發行這些產品、程式或服務。在提及 IBM 產品、程式或服務時，不表示或暗示只能使用 IBM 的產品、程式或服務。只要不侵害到 IBM 智慧財產權或其他受到法律保護的權利，凡是功能相等的產品、程式或服務程式，都可以代替 IBM 產品、程式或服務程式。其他產品在運作上的評價與驗證，除非 IBM 特別指示，其責任屬於使用者。

本文件所涵蓋的主要項目，IBM 已有專利或正在申請專利。使用者不享有本書內容之專利權。關於軟體授權若有任何問題，請以書面方式寄到：

台北市基隆路一段 206 號
台灣國際商業機器股份有限公司
法務部

本程式的合法使用者若想要 (i) 在獨立建立的程式和其它程式 (包括本程式) 之間交換資訊，以及 (ii) 共同使用交換的資訊，請連絡：

台北市基隆路一段 206 號
台灣國際商業機器股份有限公司
法務部

上述資訊需要在適當的條件和狀況下才可取得，包括可能需要付費。

本文件所描述的授權程式及其所有可用的授權資料，是由 IBM 根據「IBM 客戶契約」的條款規定而提供的。

本文件不專供生產使用且不提供任何保證，包括銷售性保證及特定用途的適用性。

這個產品包含由加洲大學柏克萊分校及其贊助者共同發展的軟體。

註冊商標

下列詞彙是 IBM 公司在美國或其它國家，或兩者所使用的註冊商標：

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

Microsoft、Windows、Windows NT 和 Windows 95 標誌都是 Microsoft 公司的商標或註冊商標。

UNIX 是在美國和其它國家的一個註冊商標，由 X/Open Company Limited 獨家授權。

Java 及 HotJava 是 Sun Microsystems, Inc. 的註冊商標。

用雙星號 (**) 表示的其它公司、產品及服務程式名稱，可能是其它公司的商標或服務標記。

名詞解釋

您可以於下列網址存取 IBM 軟體名詞解釋：
<http://www.networking.ibm.com/nsg/nsgmain.htm>。

索引

索引順序以中文字，英文字，及特殊符號之次序排列。

〔四劃〕

介面 4
公用程式，報告 23
方法，鑑證 49
日誌監督程式 7
日誌機能 72
日誌檔管理 6
日誌，防火牆 23

〔五劃〕

功能群組，管理 21

〔六劃〕

全球資訊網頁面 143
名稱服務程式，領域 2
安全 IP 位址，排除 11
安全 IP 位址，對映 11
安全 IP 位址，轉換 10

〔七劃〕

位址，排除安全 IP 11
位址，對映安全 IP 11
位址，轉換安全 IP 10
防火牆日誌 23

〔八劃〕

使用者提供的鑑證 49
使用建立密碼鎖檔案公用程式 (MKKF) 57
命令行介面 1
服務程式，領域名稱 2
表格，SQL 29

〔九劃〕

建立密碼鎖檔案 57
架構伺服器 1

查詢，範例 28

〔十劃〕

訊息 75
訊息，產生 25

〔十一劃〕

參考書目 143
參照 143
參數，基本 18
基本參數 18
密碼鎖檔案，建立 57
密碼鎖檔案，建立一個 57
強化 133
授權合約 145
排除安全 IP 位址 11
產生訊息 25

〔十二劃〕

備註的要求 (RFC) 135
報告公用程式 23, 73
報告公用程式用法 23
登記位址，Many-to-One 10

〔十三劃〕

群組，管理功能 21
資料傳輸控制 70
過濾 3

〔十四劃〕

對映 安全 IP 位址 11
疑難排解及測試 65
管理函數群組 21
管理，日誌檔 6
網路位址轉換 10
領域名稱服務程式 2

〔十五劃〕

範例查詢 28

〔十七劃〕

檔案管理, 日誌 6

〔十八劃〕

轉換安全 IP 位址 10

〔二十二劃〕

鑑證方法 49

鑑證, 使用者提供的 49

A

ADMIN_ALERT 29

a_alert.tbl 25

D

DB2 27

DB2/6000 或 DB2/2 23

DNS 問題 67

F

FILTER_ACTIVE_RULE 29

FILTER_INFO 29

FILTER_MATCH 29

FILTER_STATUS 29

fwfilter 3

fwimport.dat 23

fwinterface 5

fwlog 6

fwlogcvrt 23

fwlogmon 8

fwlogtbl 23, 24

fwlogtxt 23

fwmail 10

fwnat 11

fwqrysmpl.dml 23

fwschema.ddl 23, 27

fwuser 18

f_info.tbl 25

f_match.tbl 25

f_rule.tbl 25

f_stat.tbl 26

H

HTTP proxy 3

I

INTERFACES 29

interfaces.tbl 26

IP 位址, 排除安全 11

IP 位址, 對映安全 11

IP 位址, 轉換安全 10

M

Many-to-One 登記位址 10

N

NAT 72

NAT_INFO 29

nat_info.tbl 26

P

PAGER_INFO 29

Proxy 伺服器 70

proxy, HTTP 3

PROXY_FTP 29

PROXY_HTTP 29

PROXY_INFO 29

PROXY_LOGIN 29

PROXY_STATUS 29

p_ftp.tbl 26

p_http.tbl 26

p_info.tbl 26

p_login.tbl 26

p_stat.tbl 26

S

SERVER_INFO 29

server_info.tbl 26

SESSION 29

session.tbl 26
SOCKS_FTP 29
SOCKS_INFO 29
SQL 表格 29
SSL_INFO 29
ssl_info.tbl 26
SU 29
s_ftp.tbl 26
s_info.tbl 26

T

TUNNEL_CONTEXT 29
TUNNEL_POLICY 29
TUNNEL_STATUS 29

U

URL 143
(MKKF), 使用建立密碼鎖檔案公用程式 57
(RFC), 備註的要求 135

讀者意見表

爲使本書盡善盡美，本公司極需您寶貴的意見；懇請您使用過後，撥冗填寫下表，惠予指教。

請於下表適當空格內，填入記號（✓）；我們會在下一版中，作適當修訂，謝謝您的合作！

評估項目	評 估 意 見	備 註
正 確 性	內容說明與實際程序是否符合 <input type="checkbox"/> 是 <input type="checkbox"/> 否	
	參考書目是否正確 <input type="checkbox"/> 是 <input type="checkbox"/> 否	
一 致 性	文句用語及風格，前後是否一致 <input type="checkbox"/> 是 <input type="checkbox"/> 否	
	實際畫面訊息與本書所提之畫面訊息是否一致 <input type="checkbox"/> 是 <input type="checkbox"/> 否	
完 整 性	是否遺漏您想知道的項目 <input type="checkbox"/> 是 <input type="checkbox"/> 否	
	字句、章節是否有遺漏 <input type="checkbox"/> 是 <input type="checkbox"/> 否	
術語使用	術語之使用是否恰當 <input type="checkbox"/> 是 <input type="checkbox"/> 否	
	術語之使用，前後是否一致 <input type="checkbox"/> 是 <input type="checkbox"/> 否	
可 讀 性	文句用語是否通順 <input type="checkbox"/> 是 <input type="checkbox"/> 否	
	有否不知所云之處 <input type="checkbox"/> 是 <input type="checkbox"/> 否	
內容說明	內容說明是否詳盡 <input type="checkbox"/> 是 <input type="checkbox"/> 否	
	例題說明是否詳盡 <input type="checkbox"/> 是 <input type="checkbox"/> 否	
排版方式	本書的形狀大小，版面安排是否方便使用 <input type="checkbox"/> 是 <input type="checkbox"/> 否	
	字體大小，顏色編排，是否有助於閱讀 <input type="checkbox"/> 是 <input type="checkbox"/> 否	
目錄索引	目錄內容之編排，是否便於查考 <input type="checkbox"/> 是 <input type="checkbox"/> 否	
	索引語錄之排定，是否便於查考 <input type="checkbox"/> 是 <input type="checkbox"/> 否	
	※評估意見為 "否" 者，請於備註欄說明。	

其他：（篇幅不夠時，請另紙說明。）

[illegible]

上述改正意見，一經採用，本公司有合法之使用及發佈權利，特此聲明。

IBM eNetwork Firewall for Windows NT
參考手冊

SC40-0214-00

版本 3.2.1.1

折疊線

台北市基隆路一段二百零六號十七樓

臺灣國際商業機器股份有限公司
中文技術研究中心 啟



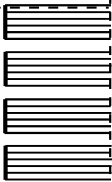
廣告回信
台灣地區郵政管理局 登記
北台字第 0587 號

(免貼郵票)

收件人 姓名：
地址：

寄

折疊線





Printed in Australia

SC40-0214-00

