

IBM eNetwork Firewall para Windows NT



Manual de consulta

Versión 3 Release 2.1.1

IBM eNetwork Firewall para Windows NT



Manual de consulta

Versión 3 Release 2.1.1

Nota: Antes de utilizar esta información y el producto al que da soporte, lea cuidadosamente la información general que encontrará en "Avisos" en la página 165.

Segunda edición (junio de 1998)

Esta edición se aplica a la Versión 3 Release 2.1.1 del IBM eNetwork Firewall para Windows NT (número de producto 5765-C16). Esta edición substituye SC31-8659-00.

Portions Copyright © 1993, 1994 by NEC Systems Laboratory.

Contiene software de seguridad de RSA Data Security, Inc. Copyright © 1990, 1995 RSA Data Security, Inc. Reservados todos los derechos.

© Copyright International Business Machines Corporation 1994, 1998. Reservados todos los derechos.

Contenido

Acerca de este manual	v
Conocimientos previos	v
Características de este release	v
Protocolo Socks, Versión 5	vi
Conversión de dirección de red	vi
Sencilla administración	vi
Delimitación de NT	vi
Autenticación consolidada	vi
Programas de utilidad de informes	vi
Alertas, supervisión y registro	vi
Aislamiento de varias redes	vii
Soporte al idioma nacional	vii
Especificación de direcciones IP	vii
Cómo ponerse en contacto con IBM para recibir servicio	vii
 Capítulo 1. Utilización de la Interfaz de línea de mandatos de IBM	 1
Servidor de configuración	1
Servicios de denominación de dominios	2
Filtros	3
Proxy HTTP	3
Interfaces	4
Archivador de registros	5
Gestión de Archivos de Registro	6
Supervisor de registro	8
Correo	10
Conversión de dirección de red	11
Notificación al buscapersonas	14
Usuarios	17
 Capítulo 2. Utilización de los programas de utilidad de informes	 23
Utilización de los programas de utilidad de informes	24
Formato de registro de IBM Firewall	24
 Capítulo 3. Kit de desarrollo de software del "Plug-in" de SafeMail	 45
Visión general del proceso de SafeMail	45
Creación de un "Plug-in" de la pasarela SafeMail	45
 Capítulo 4. Kit de desarrollo de software del "plug-in" del archivador de registro	 47
Cómo crear un "plug-in" de archivador de registro	47
 Capítulo 5. Cómo suministrar sus propios métodos de autenticación	 49
Autenticación suministrada por el usuario	49
Utilización del Kit para el desarrollo del software para crear un esquema de autenticación suministrada por el usuario	49
 Capítulo 6. Utilización del Programa de utilidad de creación de archivo de claves (MKKF)	 59
Creación de un archivo de claves	59

Capítulo 7. Resolución de problemas y comprobación	67
Instalación y puesta a punto	67
Problemas de direccionamiento	67
Problemas DNS	69
Cliente de configuración	70
Control del tráfico	71
Servidores proxy	72
Servicios de autenticación	72
Conversión de dirección de red	73
Recursos de registro	73
Programas de utilidad de informes	73
 Apéndice A. Mensajes	75
Código de los mensajes	75
Mensajes	75
 Apéndice B. Delimitación de la configuración del sistema Windows NT	151
 Apéndice C. Obtención de Peticiones de comentarios (RFC)	153
 Apéndice D. Formato del archivo de configuración Socks5.conf de IBM eNetwork Firewall	155
Especificación de puertas	155
Especificación de sistema principales	155
Especificación de métodos de autenticación	156
Entradas de autenticación	157
Especificación de mandatos	157
Carga de módulos	157
Direccionamiento de entradas	158
Entradas de variables	158
Entradas proxy	160
Entradas de control de acceso	160
Filtros	161
 Bibliografía	163
Información en publicaciones de IBM	163
Información en publicaciones especializadas	163
 Avisos	165
Marcas registradas	165
 Glosario	167
 Índice	169

Acerca de este manual

Este manual tiene como finalidad servir de consulta a los administradores de la red o de la seguridad del sistema que se encargan de instalar, administrar y utilizar IBM eNetwork Firewall Versión 3.2 en una máquina con Windows NT**. Para utilizar programas de cliente, como Telnet o FTP, consulte la guía del usuario de los programas de cliente TCP/IP.

Conocimientos previos

Antes de instalar y configurar IBM eNetwork Firewall, es importante disponer de amplios conocimientos acerca de TCP/IP y de la administración de la red. Puesto que definirá y configurará un cortafuegos que controla el acceso dentro y fuera de la red, primero debe entender el funcionamiento de la red. En especial, debe entender los aspectos básicos de las direcciones IP, nombres calificados al completo y máscaras de subred.

Un excelente manual sobre TCP/IP que explica netstat, arp, ifconfig, ping, nslookup, DNS, sendmail, el direccionamiento y muchas más materias es *TCP/IP Network Administration*. Consulte el apartado *Bibliografía* para obtener más detalles.

Un excelente manual para quienes se encargan de realizar la administración UNIX, que también ofrece una excelente visión general de TCP/IP y del direccionamiento, del hardware de red, DNS y de sendmail es *UNIX System Administration Handbook*. Consulte el apartado *Bibliografía* para obtener más detalles.

Características de este release

IBM eNetwork Firewall para Windows NT ofrece una rica selección de características e incluye las tres arquitecturas del cortafuegos:

1. Proxies de aplicación

- FTP
- HTTP, incluyendo Gopher y WAIS
- Telnet
- SafeMail

HTTP, Telnet y FTP tienen posibilidad de autenticación.

2. Pasarela a nivel de circuito a través del protocolo Socks versión 5, un estándar de Internet
3. Filtrado—un amplio y sólido conjunto de criterios sobre qué tráfico puede permitirse o denegarse. Los criterios incluyen la dirección TCP/IP, la puerta, el protocolo, la dirección, el adaptador (seguro/no seguro), entre otros.

Existen numerosos servicios predefinidos que hacen que la configuración resulte más rápida.

Protocolo Socks, Versión 5

Además de su simplicidad y flexibilidad, el protocolo Socks, versión 5, ofrece las ventajas siguientes:

- Fácil desarrollo de los métodos de autenticación y cifrado
- Asociación UDP, que crea un circuito proxy virtual para atravesar circuitos proxy basados en UDP
- Socks V5 Watcher, que muestra información del rendimiento del socks en tiempo real

Conversión de dirección de red

Con el impresionante crecimiento de Internet, el agotamiento de direcciones IP se ha convertido en un problema importante. Conversión de direcciones de red (NAT) constituye una solución para el problema del agotamiento de direcciones IP que se basa en la reutilización de direcciones.

La ventaja de NAT es que permite claramente que una red que utilice direcciones privadas o no permitidas se comunique con sistemas principales de Internet, de modo que la red privada disponga de un amplio espacio de direcciones. Es más, mediante NAT, las direcciones de la red privada permanecen ocultas del mundo externo, lo cual supone un mayor grado de seguridad.

Sencilla administración

Mediante la utilización de una aplicación Java**, que puede administrarse desde una máquina remota, puede realizar fácilmente actualizaciones en la configuración del cortafuegos. Y es posible asignar a los distintos administradores distintos niveles de autorización para ejercer mayor control sobre el acceso al cortafuegos. Esta interfaz gráfica de usuario (GUI) sencilla y fácil de entender puede utilizarse para administrar el Windows NT Firewall y el AIX Firewall.

Delimitación de NT

Cuando se instala el cortafuegos, ningún protocolo TCP/IP está inhabilitado, los servicios del sistema que no se necesitan no están habilitados y los registros locales de cuentas que no son el administrador también están inhabilitados.

Autenticación consolidada

Se ofrece soporte para todos los mecanismos de autenticación basados en contraseñas más conocidos, como SecurID, Clave SecureNet y otros.

Programas de utilidad de informes

Los programas de utilidad de informes le permiten ejecutar una consulta SQL en el registro del sistema tras su exportación a un intérprete de bases de datos.

Alertas, supervisión y registro

El extenso y detallado registro incluye toda la actividad del cortafuegos y las direcciones TCP/IP, ID de usuarios, TOD, nombres de archivos, números de puertas, etc. Se incluye un Supervisor de registro para observar actividades sospechosas y enviarle alertas cuando se han excedido los umbrales.

Aislamiento de varias redes

Mediante la utilización de varias Tarjetas de interfaz de red (NIC) en el cortafuegos, puede aislar varias subredes.

Soporte al idioma nacional

Se ofrece soporte al idioma nacional para el inglés, japonés, coreano, francés, chino simplificado, chino tradicional, italiano, español y portugués de Brasil.

Especificación de direcciones IP

Cuando configure el cortafuegos, se le solicitará que especifique direcciones IP. Debe especificar una dirección IP con puntos decimales completa, compuesta de 4 octetos, en el formato:

`nnn.nnn.nnn.nnn`

donde cada nnn es un grupo de tres números comprendidos en el rango 000–255.

Cómo ponerse en contacto con IBM para recibir servicio

El Centro de soporte de IBM ofrece ayuda telefónica para el diagnóstico y resolución de problemas. Puede llamar al Centro de soporte de IBM en cualquier momento; volverán a llamarle dentro de las siguientes ocho horas laborables (Lunes a viernes, de las 08:00 a las 17:00 horas, horario local del cliente). El número al que puede llamar es el 1-800-237-5511.

Si se encuentra fuera de los Estados Unidos o de Puerto Rico, póngase en contacto con el representante de IBM o proveedor de IBM autorizado de su localidad.

Capítulo 1. Utilización de la Interfaz de línea de mandatos de IBM

En este capítulo se explican los mandatos que puede utilizar desde una línea de mandatos de IBM Firewall.

A los mandatos se aplica la información siguiente:

- Los mandatos que se listan en este manual utilizan la siguiente sintaxis:
 - subrayado indica que se trata de datos entrados por el usuario.
 - [] indica que un parámetro es opcional.
 - {} indica que el usuario puede elegir entre varios parámetros.
 - | separa opciones.
- Todos los parámetros utilizan el formato palabra clave=valor.
- Si un parámetro dispone de varios valores, tales valores deben especificarse entre comillas dobles y separarse con espacios en blanco, por ejemplo:
secaddr="11.22.33.1 11.22.33.2"
- No incluya espacios en ningún parámetro a menos que se hayan especificado entre comillas dobles.
- Si omite uno o más parámetros obligatorios, en el programa de utilidad de la línea de mandatos se listarán los parámetros que faltan.
- Si se especifica un valor no válido para un parámetro, el programa de utilidad de la línea de mandatos informará acerca de la existencia de este error.
- Algunos servicios del cortafuegos actualizan dinámicamente su comportamiento cuando cambian sus archivos de configuración. Algunos necesitan un submandato de actualización. Los servicios del cortafuegos que necesitan una instrucción cuentan con un submandato update.
- Sólo los administradores del cortafuegos primario pueden ejecutar programas desde la línea de mandatos.
- Debido a la complejidad e interdependencias entre los archivos, **no edite directamente ningún archivo de configuración.**

Servidor de configuración

El mandato `fwcfgsrv` lista o cambia las opciones del servidor de configuración. Para poder emitir este mandato, el administrador debe tener autorización para administrar funciones de control del tráfico.

Para que se listen las opciones del servidor de configuración, emita el mandato siguiente.

```
fwcfgsrv cmd=list
```

La salida del mandato `fwcfgsrv` tiene el aspecto siguiente:

```
localonly = yes/no
encryption = none/ssl
sslfile = nombre de archivo si se ha definido uno
```

Para cambiar las opciones del servidor de configuración, emita el mandato siguiente.

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

Las definiciones de los parámetros son las siguientes:

localonly Indica si el cortafuegos sólo puede administrarse desde una máquina local. Los valores válidos son yes o no (sí o no).

encryption Indica si el servidor de configuración espera datos de entrada que han de cifrarse a través de ssl o no. Los valores válidos son none o ssl (ninguno o ssl).

sslfile Indica el nombre de archivo ssl que ha de utilizarse para el cifrado ssl. Consulte el apartado Capítulo 6, “Utilización del Programa de utilidad de creación de archivo de claves (MKKF)” en la página 59.

Servicios de denominación de dominios

El Servicio de denominación de dominios (DNS) ofrece servicio completo de denominación de dominios a los sistemas principales del interior de una red segura, mientras que proporciona información mínima a los sistemas principales que se encuentran en el exterior de la red segura. Para ello se necesitan tres servidores de denominación de dominios:

- Uno en el cortafuegos
- Uno en el interior de la red segura
- Uno en el exterior de la red segura.

Consulte el manual *IBM eNetwork Firewall - Guía del usuario* para obtener más información.

Nota:

1. Las x.x.x.x son una dirección IP en su formato que contiene puntos decimales.
2. El valor de los parámetros secaddr y remaddr puede ser una única dirección IP o una lista de direcciones IP. Si se especifica una lista de direcciones IP, ésta deberá limitarse utilizando espacios y deberá especificarse entre comillas dobles.
3. Las direcciones duplicadas se detectan y se marcan como un error.
4. La primera vez que se configuran los DNS, fwdns cmd=change crea el nuevo archivo. El cortafuegos siempre tendrá exactamente un registro de configuración de DNS. Los valores pueden estar vacíos. El submandato change es suficiente para cambiar cualquiera o todos los valores del registro DNS.

El mandato siguiente lista la configuración DNS actual.

```
fwdns cmd=list
```

Para cambiar la entrada de configuración DNS y crear un nuevo archivo:

```
fwdns cmd=change
    secdomain=Nombre dominio seguro
    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"
```

Las definiciones de los parámetros son las siguientes:

secdomain=Nombre dominio seguro nombre de dominio de la red segura interna

secaddr=Dirección DNS segura[,...] dirección IP de los servidores de nombres de dominios seguros

remaddr=Dirección DNS no segura[,...] dirección IP de los servidores de nombres de dominios que se encuentran fuera de la red segura y que proporciona el proveedor de servicio de conexión a Internet.

Filtros

Utilice el mandato **fwfilter** para activar y desactivar normas de los filtros.

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

Las definiciones de los parámetros son:

fwfilter cmd=update vuelve a crear la configuración y activa ese conjunto de normas.

fwfilter cmd=verify realiza una "creación de prueba" de la configuración, pero no activa ningún cambio.

fwfilter cmd=list lista la configuración que se ha creado más recientemente

fwfilter cmd=shutdown desactiva el mecanismo de filtrado

fwfilter cmd=startlog registra el tráfico seleccionado en el recurso registro del cortafuegos

fwfilter cmd=stoplog detiene el registro de filtros del cortafuegos

Proxy HTTP

proxy HTTP gestiona con eficacia las peticiones del navegador a través de IBM Firewall, eliminando la necesidad de un servidor socks para navegar por la Web. Los usuarios pueden acceder a la útil información de Internet, sin comprometer la seguridad de sus redes internas y sin alterar sus entornos de cliente para la implementación de un proxy HTTP.

El mandato **fwhttp** lista o cambia la configuración actual del proxy.

Para listar la configuración actual del proxy HTTP, utilice el mandato siguiente.

```
fwhttp cmd=list
```

Para cambiar la configuración actual del proxy HTTP, utilice el mandato siguiente.

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

Las definiciones de los parámetros son las siguientes:

- port** La puerta a la que atenderá el servicio del proxy http.
- maxcontentlengthbuffer** El tamaño máximo de un almacenamiento intermedio para la devolución de documentos para permitir la adición de una cabecera de longitud de contenido que ha de devolverse.
- minactivethreads** El número mínimo de hebras de trabajo que han de iniciarse durante la inicialización y mantenerse activas en tiempo de ejecución.
- maxactivethreads** El número máximo de hebras de trabajo que pueden estar en ejecución en cualquier momento.
- idlethreadtimeout** El período de tiempo que deben conservarse disponibles las hebras desocupadas.
- logging** Indica si se desea el registro para la actividad HTTP. Los valores son on u off (activar o desactivar).
- authenticate** El nivel de los usuarios a autenticar. Los valores son all, none o new (todos, ninguno, nuevos).
- authentikatimeout** El tiempo que ha de esperarse una petición del cliente tras establecerse una conexión continua.
- maxpersistrequests** El número máximo de peticiones a recibir en una conexión continua.
- persisttimeout** El tiempo que ha de mantenerse una conexión continua.

Interfaces

Las interfaces seguras conectan el sistema principal del IBM Firewall a la red de sistemas principales de la red interna, la red que desea proteger. **Como mínimo, debe disponer de una interfaz segura para que el cortafuegos pueda funcionar.** Las interfaces no seguras conectan IBM Firewall a una o más redes externas o a Internet. IBM Firewall debe tener, como mínimo, una interfaz no segura.

Este mandato muestra una lista de las interfaces de red del cortafuegos. Para poder emitir este mandato, el administrador debe disponer de autorización para administrar funciones de interfaz.

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

Consulte el capítulo Administración del manual *IBM eNetwork Firewall - Guía del usuario* para obtener más información acerca de la autorización del administrador.

Las definiciones de los parámetros son las siguientes:

addr=x.x.x.x Muestra una lista con todas las interfaces de red que se han configurado para el cortafuegos e identifica a cada una de ellas como interfaz segura o no segura. También podría identificarse un nombre. Si se especifica el parámetro opcional **addr**, sólo se listará esa interfaz. Si se especifica una dirección IP con puntos decimales para **addr**, la lista contendrá la dirección, estado y nombre sólo de la dirección especificada, dando por supuesto que ésta se ha configurado para el cortafuegos.

Este mandato le permite definir las interfaces de red para el cortafuegos. Para poder emitir este mandato, el administrador debe disponer de autorización para administrar funciones de interfaz.

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

Las definiciones de los parámetros son las siguientes:

addr=x.x.x.x Contiene la dirección con puntos decimales de la interfaz que va a cambiarse. Si esa interfaz no se ha definido para el cortafuegos, se informará un error.

state={secure|nonsecure} Contiene una de las dos palabras clave, "secure" o "nonsecure", que califican a la red que está conectada a la interfaz especificada.

name Es un nombre significativo que identifica a la interfaz o a la red a la que se conecta. Pueden incluirse espacios, siempre que también se especifiquen las comillas dobles correspondientes.

Aunque el estado y el nombre son parámetros opcionales, deberá especificarse uno de ellos.

Archivador de registros

El mandato siguiente invoca el archivador de archivos de registro para mantener los recursos de Registro que se han configurado para la tarea de archivar.

```
fwlogmgmt -l o fwlogmgmt -a
```

Colocar este mandato en un Servicio planificado Windows NT da resultados satisfactorios. Consulte el manual *IBM eNetwork Firewall - Guía del usuario* para obtener más información.

Gestión de Archivos de Registro

La Gestión de Archivos de Registro define y gestiona los archivos de registro y los archivos archivador. El mandato fwlog añade, modifica y suprime recursos de registro.

Para añadir recursos del registro, emita el mandato siguiente.

```
fwlog cmd=add
      facility=Recurso
      priority=Prioridad
      logfile=Nombre archivo registro
      [arcfile=Vía acceso archivador
      logtime=Días a conservar en registro
      arctime=Días a conservar en archivador
```

Valores válidos para el **recursos**:

- firewall (local4) - registros del cortafuegos generales, incluido el registro del filtros
- alert (local1) - estado del daemon del supervisor de registro y advertencias de violación de umbral que se utilizan para poblar la Visualización de alertas
- adminaudit (local0) - registro de comprobación administrativa
- mail - registros de correo

Valores válidos para la **prioridad**:

- depuración
- información
- advertencia
- error
- crítico

El parámetro logfile indica a dónde deben enviarse las entradas de registro del cortafuegos. El valor válido para logfile es un nombre de archivo calificado al completo (con el formato unidad:\directorio) que indique el archivo en el que deben grabarse las entradas del registro.

Nota: Los archivos que se identifican para los recursos registro de alertas o registro del cortafuegos deben ser distintos entre sí y distintos de los archivos de cualquier otro registro si las funciones del cortafuegos van a utilizarse para procesar tales archivos.

Es muy importante que SÓLO aparezcan mensajes del cortafuegos en la entrada de los archivos de los programas de utilidad de informes. No deberá dirigirse ningún otro recurso al mismo archivo que el registro del cortafuegos o registro de alertas.

Los parámetros arcfile, logtime y arctime son opcionales y sólo son válidos cuando el parámetro logfile especifica un nombre de archivo. Si se especifica alguno de ellos, también deberán especificarse todos los demás, los tres. Estos parámetros controlan la tarea de archivar registros. Para que tenga lugar la tarea de archivar

real, ejecute el mandato `fwlogmgmt` periódicamente. Consulte el apartado “Archivador de registros” en la página 5.

Como valor por omisión, el cortafuegos utiliza estos parámetros para indicar dónde almacenar los registros de anotaciones de archivador y con qué frecuencia debe realizarse el archivo. Deberá especificar los tres parámetros para habilitar el archivo.

La función de archivar puede sustituirse escribiendo una conexión de archivo al cortafuegos. Consulte el apartado Capítulo 4, “Kit de desarrollo de software del “plug-in” del archivador de registro” en la página 47.

El parámetro **arcfile** debe contener una vía de acceso totalmente calificada.

El parámetro **logtime** indica el número mínimo de días que una entrada de registro del cortafuegos permanecerá en el archivo de registro antes de moverse al archivador.

El parámetro **arctime** indica el número mínimo de días que un registro de anotaciones del cortafuegos permanecerá en el archivador antes de depurarse.

Para cambiar recursos del registro, emita el mandato siguiente.

```
fwlog cmd=change
      index=Índice
      [facility=Recurso]
      [priority=Prioridad]
      [logfile=Nombre archivo registro]
      [arcfile=Nombre archivo archivador]
      [logtime=Días a conservar en registro]
      [arctime=Días a conservar en archivador]
```

Si un cambio, en particular en la instancia inicial, impide la creación de un archivo de configuración sintácticamente correcto (por ejemplo, al archivo de registro que se ha creado le faltan campos), se emitirá una advertencia y el cortafuegos no registrará datos.

Para llevar a cabo el registro pero no el archivo, sólo hacen falta los parámetros **facility**, **priority** y **logfile**. Para inhabilitar el archivo del registro una vez iniciado, elimine el contenido de los parámetros **archive**, **logtime** y **arctime**. Si ha planificado un trabajo de archivo, suprávalo.

Para que se listen los datos actuales de configuración del archivo de registro, emita el mandato siguiente.

```
fwlog cmd=list
```

Para suprimir la entrada de registro del cortafuegos especificada mediante el número de índice devuelto para la entrada en el mandato `fwlog cmd=list`, emita el mandato siguiente.

```
fwlog cmd=delete
      index=índice de entrada a suprimir
```

Supervisor de registro

Utilice el mandato del supervisor de registro para indicarle a éste cuándo y cómo activar alertas. Las alertas se producen cuando se alcanzan los valores de umbral especificados en este mandato (o en el panel de cliente de configuración correspondiente) dentro de un periodo determinado. Cuando se produce una alerta:

1. Se graba un registro en el recurso de alertas y en el de registro del cortafuegos
2. Se ejecuta un mandato especificado
3. Se envía una notificación a uno o más ID de usuario
4. Se envía un mensaje a un dispositivo de notificación al buscapersonas

Los tres últimas acciones se controlan configurando adecuadamente los valores que se especifican a continuación.

Listing the Log Monitor Setting (Listar los valores del supervisor de registro)

```
fwlogmon cmd=list
```

Specifying User IDs to Receive Mail Notifications when any Alert Occurs (Especificar que los ID de usuario reciban notificaciones de correo cuando se produzca una alerta)

Para especificar que los ID de usuario reciban notificaciones de correo cuando se produzca una alerta (la notificación se enviará a cada id que añada):

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

Specifying a Command to be Run when any Alert Occurs (Especificar que se ejecute un mandato cuando se produzca una alerta)

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

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

Specifying a Threshold at which an Alert Should be Triggered Based on the Number of Unsuccessful Login Attempts (Especificar un umbral que, una vez alcanzado, debe activar una alerta según el número de intentos de conexión no satisfactorios)

```
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
```

Specifying a Threshold at which an Alert Should be Triggered Based on Number of Occurrences of a Specific Firewall Message ID (Especificar un umbral que, una vez alcanzado, debe activar una alerta según el número de ocurrencias de un ID de mensaje de cortafuegos específico)

```
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=
```

Las definiciones de los parámetros son las siguientes:

- type** Identifica el tipo de características del mandato del supervisor de registro que se ha añadido o modificado.
- Los valores permitidos son id, command, msg, single, multi y host.
- id** Afecta al id de usuario al que se envían notificaciones.
- command** Especifica el mandato que va a ejecutarse.
- msg** Afecta a la supervisión de un mensaje de registro específico.
- single** Afecta a la supervisión basada en un solo id de usuario. Para cada id se establece un número de intentos no satisfactorios. Cuando este número coincide con el valor de umbral especificado en este mandato, se activa una alerta.
- multi** Afecta a la supervisión basada en varios id de usuario. Cuando el número total de intentos no satisfactorios para todos los id coincide con el valor de umbral especificado en este mandato, se activa una alerta.

host	Afecta a la supervisión basada en los nombres de sistema personal. Para cada sistema personal se establece un número de intentos no satisfactorios. Cuando este número coincide con el valor de umbral especificado en este mandato, se activa una alerta.
username	El id de correo de un administrador de cortafuegos o de otro usuario al que se le notificará de la existencia de una alerta. Las notificaciones de alerta se enviarán satisfactoriamente sólo si ha configurado adecuadamente un servidor de correo seguro.
command	El nombre del mandato que se ha de ejecutar cuando se produce una alerta. Debe ser la vía de acceso completa de un archivo ejecutable. Puede ser un archivo .bat, que permite que varios mandatos se ejecuten desde el archivo mismo; sin embargo, si el archivo .bat hace referencia a otros archivos, éstos también deben tener vías de acceso completas.
count	Establece el umbral en el número de intentos fallidos o de ocurrencias de un mensaje de registro determinado; alcanzado dicho número, se activará una alerta.
time	Establece un periodo de tiempo en minutos. Para que se active un evento, debe alcanzarse un número de ocurrencias dentro de este periodo de tiempo a partir de la primera ocurrencia. Las ocurrencias que se producen después de este periodo antes de la hora actual no se tienen en cuenta.
pager	Cuando el umbral asociado activa una alerta, este parámetro especifica si usted va a utilizar o no un buscapersonas. Para enviar la notificación se utiliza la configuración activa del buscapersonas.
tag	El identificador de mensajes de registro (que incluye el prefijo ICA) que se ha de supervisar. Los mensajes de supervisión de registro (aquellos cuyos identificadores ICA son inferiores a 1000) no pueden supervisarse.

Correo

Utilice el mandato `fwmail` para correlacionar dominios de correo públicos y seguros.

```
fwmail cmd=list

fwmail cmd=add
    secdomain=
    mail=
    remdomain=

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

fwmail cmd=delete
    secdomain=
```

Las definiciones de los parámetros son las siguientes:

secdomain El nombre por el que los usuarios conocen el dominio de correo que está describiéndose en la ubicación segura del cortafuegos.

mail Dirección de un servidor de correo.

remdomain El nombre por el que los usuarios conocen el dominio de correo que está describiéndose en la ubicación no segura del cortafuegos.

Conversión de dirección de red

La Conversión de dirección de red (NAT) ofrece una solución al problema de la limitación de las direcciones IP, pues permite que cualquier otra red IP pueda utilizar las direcciones del interior de la red IP segura.

NAT soporta cuatro tipos de configuración:

- Dirección registrada de varias en una - La conversión de varias en una consiste en convertir la dirección segura de un paquete y el número de puerta de tal modo que muchas direcciones internas (hasta 65536) puedan compartir una dirección IP registrada. Esta dirección IP registrada oculta las direcciones locales, pero además será necesario disponer de otra dirección registrada de Internet sólo para el cortafuegos.
- Convertir direcciones IP seguras - Una entrada Convertir direcciones IP seguras define una serie de direcciones de red seguras que requieren NAT para realizar la conversión de direcciones IP. Como valor por omisión, la conversión de direcciones de red realiza la conversión de las direcciones de todas las direcciones IP seguras.
- Excluir direcciones IP seguras Una entrada Excluir direcciones IP seguras define un conjunto de direcciones de red seguras que no necesita la NAT para realizar la conversión de direcciones IP. Como valor por omisión, la conversión de direcciones de red realiza la conversión de direcciones de todas las direcciones IP seguras, a menos que la dirección se encuentre dentro del rango que especifica una entrada Excluir direcciones IP seguras.
- Correlacionar direcciones IP seguras Una entrada Correlacionar direcciones IP seguras define una correlación exacta de una dirección IP segura con una dirección IP registrada. Esta correlación exacta de direcciones IP permite a los clientes de aplicaciones externas, como los clientes FTP o Telnet, establecer sesiones TCP con máquinas de servidor que residen dentro de la red segura.

La sintaxis del mandato de NAT es la siguiente:

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

Las definiciones de los parámetros son las siguientes:

fwnat cmd=list Lista la configuración de NAT actual

fwnat cmd=update Renueva el motor de la NAT

fwnat cmd=verify Comprueba la sintaxis de la configuración

fwnat cmd=shutdown Detiene la conversión de todas las direcciones

fwnat cmd=startlog Inicia el registro de cada paquete convertido

fwnat cmd=stoplog Detiene el registro de cada paquete convertido

Para añadir una entrada varias en una a la configuración de NAT, utilice **type=many-to-one**:

```
fwnat cmd=add
      type=many-to-one
      addr=Dirección
      [timeout= minutos]
```

Las definiciones de los parámetros son las siguientes:

type=many-to-one Añade una entrada many-to-one

addr=Dirección Dirección IP que identifica un rango de las direcciones IP registradas que se han añadido a la agrupación de direcciones registradas

timeout= minutos Número de minutos que una conversión de direcciones puede permanecer desocupada antes de que la NAT pueda liberar la dirección IP registrada. El valor por omisión es 15 y el rango es 5–45.

Para modificar una entrada de varias en una en la configuración de la NAT utilice la siguiente sintaxis:

```
fwnat cmd=change
      index=
      [addr=Dirección]
      [timeout= minutos]
```

Las definiciones de los parámetros son las siguientes:

index Cuando ejecuta `fwnat cmd=list`, se muestran números en la columna de la izquierda para las entradas específicas de la NAT. Utilice el número de su entrada de NAT específica para el parámetro index.

addr=Dirección Dirección IP que identifica un rango de las direcciones IP registradas que se han añadido a la agrupación de direcciones registradas

timeout= minutos número de minutos que una conversión de direcciones puede permanecer desocupada antes de que la NAT pueda liberar la dirección IP registrada. El valor por omisión es 15 y el rango es 5–45.

Para añadir una entrada de conversión o de exclusión al archivo de configuración de la NAT, escriba **type=translate** y para excluir una entrada del archivo de configuración de la NAT utilice **type=exclude**:

```
fwnat cmd=add
      type={translate|exclude}
      addr=Dirección
      mask=Máscara
```

Las definiciones de los parámetros son las siguientes:

type=translate Añade una entrada translate

type=exclude Añade una entrada exclude

addr=Dirección Dirección IP que identifica un rango de las direcciones IP seguras que necesitan conversión.

mask=Máscara Identifica un rango de direcciones IP

Para modificar una entrada de conversión o exclusión del archivo de configuración de la NAT utilice la siguiente sintaxis:

```
fwnat cmd=change
      index=
        [addr=Dirección]
        [mask=Máscara]
```

Las definiciones de los parámetros son las siguientes:

index Cuando ejecuta `fwnat cmd=list`, se muestran números en la columna de la izquierda para las entradas específicas de la NAT. Utilice el número de su entrada de NAT específica para el parámetro `index`.

addr=Dirección Dirección IP que identifica un rango de las direcciones IP seguras que necesitan conversión.

mask=Máscara Identifica un rango de direcciones IP

Para añadir una entrada correlacionada a la configuración de NAT, utilice **type=map**:

```
fwnat cmd=add
      type=map

      secaddr=Dirección segura]

      remaddr=Dirección registrada]
```

Las definiciones de los parámetros son las siguientes:

type=map Añade una entrada map

secaddr Dirección IP que debe convertirse en una dirección registrada especificada

remaddr Dirección registrada a la que debe convertirse la dirección segura especificada

Para modificar una entrada de correlación en la configuración de la NAT utilice la siguiente sintaxis:

```
fwnat cmd=change
      index=
        [secaddr=Dirección segura]
        [remaddr=Dirección registrada]
```

Las definiciones de los parámetros son las siguientes:

index Cuando ejecuta `fwnat cmd=list`, se muestran números en la columna de la izquierda para las entradas específicas de la NAT. Utilice el número de su entrada de NAT específica para el parámetro `index`.

secaddr Dirección IP que debe convertirse en una dirección registrada especificada

remaddr Dirección registrada a la que debe convertirse la dirección segura especificada

Notificación al buscapersonas

Puede activar el soporte de notificación al buscapersonas para que el cortafuegos notifique a un administrador del sistema enviando un mensaje al buscapersonas del administrador cuando se produzcan alertas en el cortafuegos. Para que esto funcione adecuadamente, debe configurar el buscapersonas, el servicio de telefonía y un módem utilizando los mandatos fwpgr, fwcarrier y fwmodem.

Configuración del buscapersonas

El mandato fwpgr le permite establecer parámetros para el buscapersonas activo; el que identificará el cortafuegos.

Para listar un buscapersonas, emita el mandato siguiente.

```
fwpgr cmd=list
```

Para añadir un buscapersonas, emita el mandato siguiente.

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

Para modificar parámetros del buscapersonas, emita el mandato siguiente.

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

Las definiciones de los parámetros son las siguientes:

- | | |
|----------------|---|
| carrier | Un nombre para el servicio de telefonía, tal como se ha definido en la base de datos de portadoras (mediante el mandato fwcarrier). |
| modem | Un nombre para el módem, tal como se ha definido en la base de datos de modems (mediante el mandato fwmodem). |
| pagerid | El número de identificación o el nombre exclusivos asignados al proveedor de telefonía para el dispositivo de notificación al buscapersonas. |
| message | El mensaje que se ha de enviar al dispositivo de notificación al buscapersonas y visualizar en dicho dispositivo. Dependiendo del servicio que el proveedor de telefonía proporcione, puede ser un número o texto. Se truncará si es más largo del valor de longitud mínimo para el proveedor de telefonía o de 200 caracteres. |

Proveedor de telefonía

Emita el mandato fwcarrier para establecer parámetros para los servicios de notificación al buscapersonas que utilice.

Para listar un proveedor de telefonía, emita el mandato siguiente.

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


Para añadir un proveedor de telefonía, emita el mandato siguiente.

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

Para modificar parámetros de proveedor de telefonía, emita el mandato siguiente.

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

Para suprimir un proveedor de telefonía, emita el mandato siguiente.

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

Las definiciones de los parámetros son las siguientes:

- | | |
|-----------------|---|
| carrier | El nombre del proveedor de telefonía. |
| dial | Debe especificar el número de proveedor de telefonía para el servicio TAP que ha contratado. |
| method | El valor debe ser TAP. |
| password | Es optativa, a menos que la necesite para el servicio del proveedor de telefonía. |
| length | La longitud máxima del mensaje que permite el servicio del proveedor de telefonía. |
| baud | Especifique la velocidad en baudios más fiable que el servicio del proveedor de telefonía soporta. |
| parity | El tipo de comprobación de paridad que el servicio del proveedor de telefonía soporta. Suele ser un número par para el protocolo TAP. |
| databits | El número de bits de datos que el servicio del proveedor de telefonía soporta. Suele ser 7 para el protocolo TAP. |
| stopbits | El número de bits de parada que el servicio del proveedor de telefonía soporta. Suele ser 1 para el protocolo TAP. |

Configuración del módem

Para definir el soporte de notificación al buscapersonas, deberá configurar el módem.

Utilice el mandato modem si desea configurar un módem para enviar peticiones de buscapersonas al proveedor de telefonía del buscapersonas.

Para listar un módem, emita el mandato siguiente.

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

Para añadir un módem, emita el mandato siguiente.

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

Para modificar parámetros de módem, emita el mandato siguiente.

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

Para suprimir un módem, emita el mandato siguiente.

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

Las definiciones de los parámetros son las siguientes:

modem Un nombre para el módem.

comport La puerta COM serie a la que se conecta el módem. El módem que está conectado en esta puerta COM no debe estar definido para el sistema Windows NT.

initstring La serie de inicialización del módem. Los parámetros de la serie debe ser los adecuados para un mandato AT de módem, pero AT no debe incluirse en la serie. Los parámetros especificados deben estar coordinados con los requisitos de comunicación del módem de los proveedores de telefonía.

outsideline El número que ha de marcarse para tener línea externa.

Comprobación de la configuración del buscapersonas

Para asegurarse de que ha configurado correctamente el buscapersonas activo, utilice el mandato siguiente.

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

Las definiciones de los parámetros son idénticas a las del mandato `fwpggr`.

Varios buscapersonas

Si tiene que cambiar el buscapersonas activo de manera habitual, haga lo siguiente:

- Asegúrese de que ha definido todos los proveedores de telefonía y modems necesarios.
- Utilice `fwpggr` o el cliente de configuración para definir y guardar una configuración de buscapersonas.
- Copie el archivo `ROOTDIR\config\pager.cfg` dándole un nombre que le permita identificarlo.
- Defina otra configuración de buscapersonas y cópiela; repita este procedimiento hasta que tenga copias de todos los archivos `pager.cfg` que necesite.
- Copie el archivo de configuración que desea activar en `ROOTDIR\config\pager.cfg`

Si intenta manejar cambios de desplazamiento, establezca un trabajo planificado utilizando el mandato `at` de Windows NT para repetir automáticamente el último indicador de párrafo al principio de cada desplazamiento.

Usuarios

Este mandato añade un nuevo usuario o modifica uno o más atributos de un usuario del cortafuegos existente. Todos los parámetros disponen de valores por omisión o bien no se necesitan cuando se dan determinadas circunstancias. Para `cmd=add`, los valores por omisión se almacenarán; para `cmd=change`, se conservarán los valores existentes.

```

fwuser cmd={add|change}
      username=Nombre de conexión
      [fullname="Nombre real de los usuarios"]
      [password={yes|no}]
      [pwdvalue=Contraseña]
      [level={proxy|admin}]
      [secftp=Autenticación de FTP protegido]
      [remftp=Autenticación de FTP no seguro]
      [secauth=Autenticación de Telnet seguro]
[remauth=Autenticación Telnet no Seguro]
      [secadmin=Autenticación de administración segura]
[remadmin=Autenticación Admin no Segura]
      [secsocks=Socks seguro]
      [remsocks=Socks no seguro]
      [sechttp=HTTP seguro]
      [key="Código de clave SecureNet"]
      [histexpire=Caducidad histórico]
      [histsize=Tamaño histórico]
      [loginretries=Reintentos de conexión]
      [maxage=Antigüedad máxima]
      [maxexpired=Antigüedad caducidad máxima]
      [maxrepeats=Caracteres repetidos máximos]
      [minalpha=Caracteres alfabéticos mínimos]
      [mindiff=Caracteres distintos mínimos]
      [minlen=Longitud mínima]
      [minother=Caracteres no alfabéticos mínimos]
      [pwdwarntime=Tiempo para advertencia de contraseña]
      [userchgng={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}]

```

Parámetros básicos

username Nombre de conexión de este usuario.

fullname El nombre completo del usuario o información concisa (una línea) acerca de este usuario. Si van a incluirse espacios en este valor, el valor deberá especificarse entre comillas dobles.

level El valor por omisión es proxy, lo que indica que el usuario que se está creando es un simple usuario proxy o Socks. Los grupos de funciones administrativas y las autenticaciones de administración no se aplican a los usuarios de proxy.

key Clave utilizada para autenticar la Tarjeta de claves SecureNet de Digital Pathways del usuario. Puesto que este valor debe contener espacios, deberá especificarse entre comillas dobles.

Autenticaciones

A continuación se muestran cadenas de autenticación y sus métodos de autenticación correspondientes. A continuación se indica cómo utilizar las cadenas de autenticación para los diferentes parámetros del mandato `fwuser`.

- `permit`—permitir todo
- `deny`—denegar todo
- `password`—contraseña de cortafuegos
- `NT`—contraseña de conexión NT
- `snk`—SNK
- `sdi`—SDI
- `user`—autenticaciones suministradas por el usuario
- `userauth2`—autenticaciones suministradas por el usuario
- `userauth3`—autenticaciones suministradas por el usuario

secftp Método de autenticación que se utiliza para las conexiones FTP desde una interfaz segura. Los valores válidos son `deny`, `permit`, `password`, `NT`, `snk`, `sdi`, `user`, `userauth2` y `userauth3`. El valor por omisión es `deny`.

remftp Método de autenticación que se utiliza para las conexiones FTP desde una no interfaz segura. Los valores válidos son `deny`, `permit`, `password`, `NT`, `snk`, `sdi`, `user`, `userauth2` y `userauth3`. El valor por omisión es `deny`.

secauth Método de autenticación que se utiliza para las conexiones Telnet desde una interfaz segura. Los valores válidos son `deny`, `permit`, `password`, `NT`, `snk`, `sdi` y `user`. El valor por omisión es `deny`.

remauth Método de autenticación que se utiliza para las conexiones Telnet desde una interfaz no segura. Los valores válidos son `deny`, `permit`, `password`, `NT`, `snk`, `sdi`, `user`, `userauth2` y `userauth3`. El valor por omisión es `deny`.

secadmin Método de autenticación que se utiliza para las conexiones del Cliente de configuración remoto desde una interfaz segura. Los valores válidos son `deny`, `permit`, `password`, `NT`, `snk`, `sdi`, `user`, `userauth2` y `userauth3`. El valor por omisión es `deny` para los usuarios del proxy y `NT` para los administradores del cortafuegos primario.

remadmin Método de autenticación que se utiliza para las conexiones del Cliente de configuración remoto desde una interfaz no segura. Los valores válidos son `deny`, `permit`, `password`, `NT`, `snk`, `sdi`, `user`, `userauth2` y `userauth3`. El valor por omisión es `deny` para los usuarios del proxy y `NT` para los usuarios del cortafuegos primario.

secsocks Método de autenticación de Socks5 para las conexiones del cliente Socks que proceden de la ubicación no segura del cortafuegos. Los valores válidos son `deny`, `permit`, `password`, `NT`, `snk`, `sdi`, `user`, `userauth2` y `userauth3`.

Si el servidor Socks5 V5 se configura para utilizar métodos de autenticación de tipo ID de usuario/Contraseña en lugar de para los métodos Challenge Response Authentication Methods (CRAM), SNK no funcionará porque el protocolo ID de usuario/Contraseña de Socks5 no puede visualizar la solicitud SNK.

El valor por omisión es deny.

remsocks Método de autenticación de Socks5 para las conexiones del cliente Socks que proceden de la ubicación no segura del cortafuegos. Los valores válidos son deny, permit, password, NT, snk, sdi, user, userauth2 y userauth3.

Si el servidor Socks5 V5 se configura para utilizar métodos de autenticación de tipo ID de usuario/Contraseña en lugar de para los métodos Challenge Response Authentication Methods (CRAM), SNK no funcionará porque el protocolo ID de usuario/Contraseña de Socks5 no puede visualizar la solicitud SNK.

El valor por omisión es deny.

sechttp Método de autenticación para las peticiones HTTP procedentes de una interfaz segura. Los valores válidos son deny, permit, password, NT, sdi, user, userauth2 y userauth3.

SNK no recibe el soporte del protocolo HTTP porque no ofrece ninguna forma de mostrar al usuario la solicitud SNK. SDI recibe soporte, pero al usuario se le solicitará que especifique una contraseña en lugar de un código passcode SDI. El usuario debe escribir su código passcode SDI.

Nota: Para fwdfuser no puede establecerse SNK o Contraseña del cortafuegos en ninguno de sus campos de método de autenticación.

Parámetros de las contraseñas del cortafuegos

password Indica si al usuario se le solicitará una contraseña. Como valor por omisión, se le solicitará si se especifica algún método de autenticación o se le permitirá tomar la contraseña por omisión.

pwdvalue El parámetro pwdvalue, que se utiliza principalmente para la programación de scripts, permite especificar el valor de un parámetro en la línea de mandatos. Tenga en cuenta que este valor se escribe en texto normal y no presenta ninguna dificultad para las escuchas ilegales. No tiene ningún valor por omisión.

userchng Determina la forma en que se establecerá el distintivo change del administrador en la base de datos del usuario. Un valor yes establece el distintivo change del administrador, que necesita que el usuario cambie su contraseña la primera vez que se conecta. El valor por omisión es no. Este parámetro sólo es válido si se especifican los parámetros password=yes y pwdvalue=".

pwlocked Indica si la contraseña se ha bloqueado o no. Se establece en yes, cuando se excede el número máximo de conexiones anómalas o cuando no se ha utilizado la contraseña durante el número de semanas que se ha especificado para el tiempo máximo antes del bloqueo.

histexpire Define el período de tiempo (en semanas) durante el cual un usuario no puede volver a utilizar una contraseña. El valor es una serie de enteros. Los valores válidos son 0 a 52. El valor 0 indica que no se ha establecido ningún límite de tiempo. El valor por omisión es 0.

histsize Define el número de contraseñas anteriores que un usuario puede volver a utilizar. El valor es una serie de enteros. Los valores válidos son 0 a 20. Sólo es válido si histexpire=0. El valor por omisión es 5.

- loginretries** Define el número permitido de intentos de conexión no satisfactorios tras la última conexión satisfactoria antes de que el sistema bloquee la cuenta o perfil. El valor es una serie de enteros. Los valores válidos son 0 a 20. El valor por omisión es 10. Un valor de cero o negativo indica que no existe ningún límite. Cuando la cuenta del usuario se bloquee, éste no podrá conectarse hasta que el administrador del sistema establezca `pwlocked` en no.
- maxage** Define la antigüedad máxima (en semanas) de una contraseña. La contraseña deberá cambiarse llegado ese momento. El valor es una serie de enteros. Los valores válidos son 0 a 52. El valor 0 indica que no existe antigüedad máxima. El valor por omisión es 13.
- maxexpired** Define el tiempo máximo (en semanas), pasado el valor de la antigüedad máxima, de que dispone un usuario para cambiar una contraseña caducada. Transcurrido el tiempo definido, sólo el administrador podrá cambiar la contraseña. El valor es una serie de enteros. Los valores válidos son -1 a 26. Si el atributo de `maxexpired` es 0, la contraseña caducará cuando se alcance el valor de `maxage`. Si el atributo de `maxage` es 0, el atributo de `maxexpired` se pasará por alto. El valor por omisión es 3.
- maxrepeats** Define el número máximo de veces que puede repetirse un carácter en una nueva contraseña. Los valores válidos son 0 a 8, pero un valor de 0 carece de sentido. El valor 8 indica que no existe ningún número máximo. El valor por omisión es 2.
- minalpha** Define el número mínimo de caracteres alfabéticos que debe incluir una nueva contraseña. El valor es una serie de enteros. Los valores válidos son 0 a 8. El valor 0 indica que no existe número máximo. El valor por omisión es 4.
- mindiff** Define el número mínimo de caracteres obligatorios en una nueva contraseña que no deben ser iguales a los de la contraseña antigua. El valor es una serie de enteros. Los valores válidos son 0 a 8. El valor 0 indica que no existe número máximo. El valor por omisión es 3.
- minlen** Define la longitud mínima de una contraseña. El valor es una serie de enteros. Los valores válidos son 0 a 8. El valor 0 indica que no existe número máximo. El valor por omisión es 8.
- minother** Define el número mínimo de caracteres no alfabéticos que debe contener una contraseña nueva. El valor es una serie de enteros. Los valores válidos son 0 a 8. El valor 0 indica que no existe número máximo. El valor por omisión es 1.
- pwdwarntime** Define el número de días que precede al momento en el que el sistema emitirá una advertencia para indicar que se necesita un cambio de contraseña. El valor es una serie de enteros. Los valores válidos son 0 a 30. Un valor de cero o negativo indica que no se emitirá ningún mensaje. El valor por omisión es 5.

Grupos funcionales administrativos

- fg_all** Escriba yes (sí) si este administrador tiene permiso para administrar todos los aspectos del cortafuegos. El valor por omisión es no.
- fg_dns** Escriba yes (sí) si este administrador tiene permiso para administrar los Servicios de denominación de dominios. El valor por omisión es no.

- fg_interfaces** Escriba yes (sí) si este administrador tiene permiso para definir interfaces de cortafuegos. El valor por omisión es no.
- fg_logmonitor** Escriba yes (sí) si este administrador tiene permiso para administrar los umbrales del Supervisor de registro. El valor por omisión es no.
- fg_logs** Escriba yes (sí) si este administrador tiene permiso para administrar los Recursos de registro. El valor por omisión es no.
- fg_mail** Escriba yes (sí) si este administrador tiene permiso para administrar la pasarela de correo del cortafuegos. El valor por omisión es no.
- fg_netobjs1** Escriba yes (sí) si este administrador tiene permiso para realizar la administración básica de los Objetos de red. El valor por omisión es no.
- fg_netobjs2** Escriba yes (sí) si este administrador tiene permiso para realizar la administración avanzada de los Objetos de red. El valor por omisión es no.
- fg_pagers** Escriba yes (sí) si este administrador tiene permiso para administrar la Configuración de buscapersonas. El valor por omisión es no.
- fg_proxyserver** Escriba yes (sí) si este administrador tiene permiso para configurar los daemons del proxy del cortafuegos. El valor por omisión es no.
- fg_traffic** Escriba yes (sí) si este administrador tiene permiso para administrar el Control del tráfico. El valor por omisión es no.
- fg_user** Escriba yes (sí) si este administrador tiene permiso para administrar los usuarios del cortafuegos. El valor por omisión es no.

Para que se listen todos los atributos de todos los usuarios del cortafuegos o de un usuario del cortafuegos específico:

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

type={short|long} El valor por omisión para "type" es "long" si utiliza un nombre de usuario. Si no utiliza un nombre de usuario, el valor por omisión es "short".

Para eliminar un usuario del cortafuegos:

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

Capítulo 2. Utilización de los programas de utilidad de informes

En este capítulo se describe la utilización de los programas de utilidad de informes de IBM Firewall. La finalidad principal de los programas de utilidad de informes es generar archivos tabulados de información administrativa a partir de los archivos del registro del cortafuegos.

Los archivos de texto tabulados pueden generarse e importarse como tablas a un sistema de bases de datos, como DB2/6000 o DB2/2 . Entonces, el administrador puede utilizar el Lenguaje de consulta estructurada (SQL) para consultar los datos y generar informes. Los programas de utilidad también permiten al administrador crear un archivo de texto legible de los mensajes de registro del cortafuegos.

Los programas de utilidad de informes se componen de los programas y archivos siguientes:

fwlogtxt Programa para generar mensajes de texto a partir de un archivo de registro del cortafuegos

fwlogtbl Programa para generar archivos de importación de bases de datos, en formato DEL (delimitado), a partir de un registro del cortafuegos y un registro su.

Para utilizar el programa fwlogtbl y los archivos DDL, DML y DEL, debe tener conocimientos sobre las bases de datos relacionales y sobre la utilización de un producto de bases de datos relacionales apropiado.

fwschema.ddl Archivo de sentencias de Lenguaje de Definición de Datos (DDL) SQL, apropiado para la definición de tablas de bases de datos

fwimport.dat Archivo de sentencias de importación DB2, apropiado para importar los archivos DEL en las tablas de bases de datos

fwqrysmpl.dml Archivo de sentencias de Lenguaje de Manipulación de Datos (DML) SQL, apropiado para generar informes de muestra

fwlogcvrt Programa para convertir un formato de registro del cortafuegos Windows NT en un formato de registro del cortafuegos AIX. Esto permite que las herramientas de generación de informes de otros proveedores puedan funcionar como antes, a excepción de que es posible que los nuevos mensajes no se reconozcan.

Los archivos DDL y DML son específicos de la familia DB2, pero pueden modificarse para su utilización con otros sistemas de gestión de bases de datos. Los archivos en formato DEL pueden importarse (cargarse) fácilmente en DB2/6000, DB2/2 y en otros sistemas de archivos y de bases de datos. Su sencillo formato permitirá la conversión a otros formatos, si es necesario.

Utilización de los programas de utilidad de informes

Con esta información se explica la utilización de los programas de utilidad de informes desde la línea de mandatos. Consulte el manual *IBM eNetwork Firewall - Guía del usuario* para obtener información acerca de la utilización de los programas de utilidad de informes desde el cliente de configuración.

Para ver el archivo de registro del cortafuegos desde la línea de mandatos, utilice el programa de utilidad **fwlogtxt**. Consulte el apartado “Generación de mensajes desde el archivo de registro del cortafuegos” en la página 25 para obtener más información.

Para generar informes basados en la información del registro:

1. Instale el producto de base de datos relacional.
2. Cree una base de datos vacía.
3. Cree tablas de registro del cortafuegos vacías en la base de datos.
4. Para generar los archivos tabulados, ejecute **fwlogtbl** desde la línea de mandatos.
5. Importe los archivos resultantes para rellenar las tablas de bases de datos con los datos del registro.
6. Genere los informes ejecutando sentencias SQL o programas SQL.

Nota: Los tres primeros pasos sólo se realizan una vez, mientras que los demás pasos se repiten cada vez que existen nuevos datos de registro disponibles.

Formato de registro de IBM Firewall

Cada entrada del archivo de registro del cortafuegos tiene el formato:

```
Fecha Hora nombre_cortafuegos:año;pid:Anúm_msj;  
ID_msj;var_1;...;var_n;
```

donde

- Los tres primeros campos, **fecha, hora y nombre_cortafuegos** los añade el recurso de registro del cortafuegos.
- **año** es el año, con cuatro caracteres.
- **pid** es el ID de hebra al que se aplica la entrada.
- **Anúm_msj** es un entero secuencial que los programas de utilidad de informes utilizan para acceder al texto de mensaje convertido apropiado a partir del archivo fw_log.cat. El número del mensaje (núm_msj) va inmediatamente precedido de un indicador del nivel del registro (la letra A). Este indicador distingue tanto la plataforma que originó el registro como cualquier diferencia en el formato del mismo.
- **ID_mensaje** es el número externo del mensaje (como ICA0001e).
- **var_1-n** representa los valores de las variables de los mensajes, donde **n** es el número de variables de la definición del mensaje.

Nota: No dirija otros registros al mismo archivo que el registro del cortafuegos. Tales registros no se ajustarán al formato que necesitan los programas de utilidad de informes y los resultados serán impredecibles.

Utilice el mandato **fwlogcvrt** para convertir este formato de registro del release de Windows NT a un registro de AIX. Puede que tenga que hacerlo para utilizar herramientas de informes de otro proveedor que soportan el IBM Firewall para registros AIX. Al efectuar la conversión se eliminará el indicador 'A' del nivel del registro que precede al número de mensaje y se insertarán dos caracteres en blanco alrededor de los dos puntos que hay entre el nombre del cortafuegos y el año.

Los parámetros son:

input Entrada estándar redirigida desde un registro Windows NT Firewall.

output Salida estándar, que puede redirigirse a un archivo.

fwlogcvrt syntax

```
fwlogcvrt
```

Ejemplo:

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

Generación de mensajes desde el archivo de registro del cortafuegos

Utilice el mandato **fwlogtxt** para generar mensajes legibles a partir de las entradas de un archivo de registro del cortafuegos.

Los parámetros incluyen:

input Entrada estándar de un archivo de registro del cortafuegos

output Salida estándar

sintaxis de fwlogtxt

```
fwlogtxt
```

Ejemplo:

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

No existen parámetros para **fwlogtxt**; toma la información de la entrada estándar y coloca los resultados en la salida estándar.

Generación de archivos de importación de bases de datos

Utilice el mandato **fwlogtbl** para crear, sobregrabar o realizar adiciones en los archivos tabulados que el usuario puede utilizar para rellenar las tablas de bases de datos para la generación de informes.

Los parámetros incluyen:

input Archivo de registro del cortafuegos.

output Nombres de archivo:

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

sintaxis de fwlogtbl

```
fwlogtbl  -w [-d DirSalida] [-su]NombreRegistro  
           |  
           -a
```

Ejemplo:

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

-w Especifica que el archivo de salida existente debe sustituirse. Si el archivo no existe, fwlogtbl lo crea.

-a Especifica que el archivo generado debe añadirse al archivo de salida existente. Si el archivo no existe, fwlogtbl lo crea.

-d Identifica el directorio de salida.

DirSalida Especifica el directorio en el que van a almacenarse todos los archivos de salida. Si no se especifica ningún directorio, los archivos de salida se almacenarán en el directorio actual.

-su Especifica que NombreRegistro es el nombre de un archivo de registro de AIX. De este modo, Windows NT Firewall puede procesar archivos de registro su y del cortafuegos de los AIX Firewalls anteriores.

NombreRegistro Especifica un archivo de registro del cortafuegos o un archivo de registro su de AIX.

Los nombres de los archivos de salida están predefinidos, pero pueden copiarse o cambiarse sus nombres tras ejecutar fwlogtbl. Los archivos de salida tienen formato de archivo delimitado (DEL) de ASCII, sin delimitadores de caracteres, y utilizan el punto y la coma (;) como delimitadores de columna.

Para obtener más información acerca de los mensajes, consulte el Apéndice A, "Mensajes" en la página 75.

Utilización de una base de datos con programas de utilidad de informes

En este apartado se describen los archivos que se facilitan con el cortafuegos para la creación de la base de datos, importación de información a la base de datos y consulta de informes. Si dispone de DB2, el mandato db2 puede utilizarse con estos archivos. (Puede que existan funciones similares al mandato db2 en otros gestores de bases de datos. Puede que los archivos deban alterarse para utilizarlos con tales funciones.)

Para ejecutar el mandato db2, deberá haber instalado DB2 y deberá existir una 'instancia' definida. Consulte la documentación de la instalación de DB2. Para empezar, debe utilizar el mandato "create database" de DB2 para crear una base de datos vacía. (El nombre sugerido es 'fwlog'.) Para ello, escriba lo siguiente en la línea de mandatos:

```
db2cmd
```

En la ventana de mandatos DB2 que se muestra, escriba:

```
db2 create database fwlog
```

A continuación, debe conectarse a la base de datos fwlog:

```
db2 connect to fwlog
```

Las opciones -vf del mandato db2 pueden utilizarse como se indica a continuación:

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

Estos pasos se describen más detalladamente en los apartados siguientes. En cada caso, el usuario debe comprobar cuidadosamente la salida estándar (redirigida a un archivo en cada uno de los ejemplos). Para la importación, también es necesario comprobar el archivo .msg generado individualmente por cada sentencia de la importación.

Creación de las tablas

El mandato **db2 -vf fwschema.ddl > schema.out** crea todas las tablas e índices necesarios. Emita este mandato una vez, preferiblemente justo después de haber instalado el cortafuegos. El ID de usuario actual que esté utilizándose en el momento de ejecutarse este ejemplo será el ID de creador de las tablas. Puede que este ID tenga que utilizarse como calificador del nombre de la tabla (como idcreador.Nombretabla) en sentencias SQL posteriores, a menos que se ejecuten bajo el ID del creador. Así, si no se utiliza el ID del creador, el usuario tendrá que editar los archivos fwimport.dat y fwqrysmp.dml para colocar el ID del creador delante de cada nombre de tabla.

El archivo, `ROOTDIR/sample/report/fwschema.ddl` contiene las sentencias DDL para crear las tablas de bases de datos necesarias para aceptar registros de los archivos tabulados creadas por el mandato **fwlogtbl**. **ROOTDIR** es el directorio que ha seleccionado durante el proceso de instalación como ubicación de destino para IBM Firewall. Deberá comprobar schema.out para determinar si la operación ha resultado satisfactoria. Las sentencias del archivo fwschema.ddl pueden utilizarse tal cual o modificarse para trabajar con diversos sistemas de bases de datos. (Los usuarios no deben cambiar los nombres de las tablas ni de las columnas.)

Importación de los datos

El mandato **db2 -vf fwimport.dat > import.out** carga datos de todos los archivos DEL en las tablas creadas por el mandato **db2-vf fwschema.ddl**.

El archivo R00TDIR/sample/report/fwimport.dat contiene sentencias de ejemplo para importar los datos de los archivos *.tbl a la base de datos DB2. Como se mencionó en el apartado “Creación de las tablas” en la página 27, si el usuario de las importaciones no es el creador de las tablas, el ID del creador deberá colocarse delante de cada nombre de tabla.

Cada una de las sentencias de importación genera información en la salida estándar e información adicional en un archivo tblname.msg, donde tblname es específico de cada sentencia de importación. El usuario debe comprobar ambas formas de salida para determinar si la importación ha resultado satisfactoria. Cuando se ejecutan todas las sentencias de importación de este archivo con un programa como db2, el usuario debe dirigir la salida estándar a un archivo y, a continuación, comprobar ese archivo y cada uno de los archivos .msg. Cada mandato de importación genera un archivo .msg separado. Además, el usuario debe emitir nuevamente el mandato **db2 -vf fwimport.dat > import.out** siempre que exista un nuevo registro a reflejar en la base de datos.

Cuando importe archivos de registro grandes, puede que reciba códigos de error SQL con descripciones que indiquen que se necesita más memoria o más espacio de disco. Por ejemplo, el mensaje podría ser espacio de área de almacenamiento insuficiente o espacio de registro de transacción insuficiente. Estos errores requieren ajustar de los valores de los parámetros para el producto de bases de datos o para la base de datos fwlog. Consulte la documentación de DB2 para obtener más información. Una alternativa temporal al ajuste de los valores de los parámetros DB2 es dividir los registros grandes o los archivos tabulados grandes en archivos más pequeños.

Ejecución de consultas de ejemplo

El mandato **db2 -vf fwqrysmpl.dml > report.out** ejecuta consultas de ejemplo. El archivo R00TDIR:\sample\report\fwqrysmpl.dml contiene sentencias SQL de ejemplo que pueden proporcionar útiles datos de informes, en base a algunas de las necesidades de consulta. Puede basarse en estos ejemplos para crear sus propios informes. Como se mencionó en el apartado “Creación de las tablas” en la página 27, si el usuario de las importaciones no es el creador de las tablas, el ID del creador deberá colocarse delante de cada nombre de tabla.

Cuando las consultas se ejecutan desde la línea de mandatos, DB2 asigna el máximo espacio que podría necesitar para cada columna de salida. Ello podría dar como resultado un informe de difícil lectura. Puede que obtenga mejores resultados solicitando menos columnas en cada consulta o incorporando estas sentencias de consulta a un programa que le permita controlar mejor la presentación.

Interfaz de usuario en los programas de utilidad de informes

Los programas de utilidad de informes se instalan como parte de la instalación del cortafuegos. También pueden instalarse por separado y ejecutarse en un sistema principal que no sea cortafuegos. Para ejecutar programas de utilidad de informes en el cortafuegos puede utilizarse el cliente de configuración o el mandato fwlogtbl. En un sistema principal que no sea cortafuegos, se utilizará la línea de mandatos.

Tablas SQL

Esta sección define el diseño de las tablas SQL

Cada mensaje de registro del cortafuegos o mensaje de registro su de AIX se correlaciona con una de las tablas SQL siguientes:

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

No debe cambiar los nombres de las tablas ni de las columnas. Sin embargo, puede incrementar la anchura de una columna de caracteres si comprueba que están truncándose algunos de sus valores.

Índices

Un registro de anotaciones que represente un suceso del cortafuegos en particular sólo debe aparecer una vez en la base de datos. Si el administrador importa el mismo archivo tabulado varias veces o si se importa otro archivo tabulado que procede del mismo archivo de registro, puede que un registro de anotaciones aparezca más de una vez.

Como ayuda para evitar este problema, el archivo de ejemplo de definición de bases de datos, fwschema.dll, define un índice exclusivo en cada una de las tablas, utilizando estos tres campos:

- Nombre de archivo del archivo de registro que era el origen de este registro (LOG_FILE)
- El número de línea de este registro en ese archivo de registro (LINE_NUM)
- El número de repetición de esta línea, que se basa en el mensaje 'último mensaje repetido n veces' de syslog (REPEAT_NUM)

Este índice evita que se cargue más de una vez el mismo número de línea del mismo archivo especificado. Esto, combinado con una gestión cuidadosa de los nombres de los archivos de registro, debe evitar la duplicación de sucesos de registro en la base de datos.

La adición de otros índices a la base de datos puede mejorar el rendimiento de las consultas más comunes. Consulte la documentación de la base de datos para obtener más información.

Descripciones de tabla

En este apartado, los mensajes del registro del cortafuegos se correlacionan con tablas y columnas y se indica la información que puede que desee consultar para los informes. Todos los mensajes correlacionados con una tabla determinada se listan en la nota que aparece al final de la tabla. Los mensajes que proporcionan datos para columnas en particular se listan en la descripción de esa columna. Las tablas contienen mensajes para IBM Firewall para AIX, mensajes para IBM Firewall para NT y mensajes comunes a ambos cortafuegos.

Para obtener información acerca de los mensajes del cortafuegos, consulte el Apéndice A, "Mensajes" en la página 75.

En la columna Tipo de datos de las descripciones siguientes, 'int' significa el tipo de columna SMALLINT para DB2; 'long int' significa el tipo INTEGER de DB2. Un Tipo de Datos de date_time significa TIMESTAMP de DB2. En la indicación de fecha y hora, el valor en microsegundos siempre será "000000".

Si una descripción se marca como *obligatoria*, debe especificarse un valor para que el registro se coloque en la tabla.

Las tres columnas que sirven de índice exclusivo y la columna para recibir el indicador del nivel del registro se han omitido de estas definiciones de tabla porque sus definiciones son idénticas y, por lo general, no suele haber ninguna razón para consultarlas.

Tabla 1 (Página 1 de 2). ADMIN_ALERT. Esta tabla contiene los mensajes relacionados con las alertas de intrusión del archivo a_alert.tbl.

Columna	Tipo de datos	Breve descripción
DATE_TIME	date_time	Fecha y hora de la acción (obligatoria)
FIREWALL	char(100)	Nombre calificado al completo de la máquina cortafuegos (obligatoria)
PID	int	ID de proceso AIX, ID de hebra NT (obligatoria)
MSG_NUM	int	Número de mensaje (obligatoria)
USERID	char(16)	ID de usuario (ICA0001, ICA0002, ICA0003, ICA0004, ICA2001, ICA2002, ICA2003, ICA2026, ICA2043, ICA2068, ICA2167, ICA2168, ICA2170, ICA2173, ICA3001, ICA3012, ICA3018)
ACTION	char(7)	"connect" (ICA3012) o "bind" (ICA3018)
NUM_COUNT	int	Número de autenticaciones anómalas (ICA0001, ICA0002, ICA0003); número de entradas de registro para TAG_MSG_NUM (ICA0004); número de días (ICA9000)
TAG_MSG_NUM	char(8)	Número de mensaje de código (ICA0004)
SRC_IP	char(15)	Dirección IP de origen (ICA2001, ICA2028, ICA2079, ICA2167, ICA3012, ICA3018)

Tabla 1 (Página 2 de 2). ADMIN_ALERT. Esta tabla contiene los mensajes relacionados con las alertas de intrusión del archivo a_alert.tbl.

Columna	Tipo de datos	Breve descripción
DST_IP	char(15)	Dirección IP de destino (ICA2028, ICA2079, ICA3012, ICA3018)
AUTH_METHOD	char(20)	Método de autenticación (ICA2002, ICA2167, ICA2170)
NETWORK	char(25)	Nombre de la red (ICA2001, ICA2002, ICA2167)
HOST_NAME	char(100)	Nombre del sistema principal (ICA0003, ICA2002)
TIMEOUT_SEC	int	Tiempo de espera en segundos (ICA2026)
CONN_USERID	char(16)	Nombre de usuario de conexión Socks (ICA3001)
APPLICATION	char(30)	Nombre de la aplicación, como "telnet", "ftp", ... (ICA2167, ICA2168, ICA2170, ICA3012)
Nota: Mensajes relacionados: 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		

Tabla 2. FILTER_ACTIVE_RULE. Esta tabla las contiene normas de FILTRO activas del archivo f_rule.tbl.

Columna	Tipo de datos	Breve descripción
DATE_TIME	date_time	Fecha y hora de la acción (obligatoria)
FIREWALL	char(100)	Nombre calificado al completo de la máquina cortafuegos (obligatoria)
PID	int	ID de proceso AIX, ID de hebra NT (obligatoria)
MSG_NUM	int	Número de mensaje (obligatoria)
RULE_NUM	int	Número de norma (obligatoria)
RULE	char(150)	Norma (obligatoria)
Nota: Mensaje relacionado: ICA1037		

Tabla 3 (Página 1 de 2). FILTER_INFO. Esta tabla contiene los mensajes de información general o de errores relacionados con los FILTROS del archivo f_info.tbl.

Columna	Tipo de datos	Breve descripción
DATE_TIME	date_time	Fecha y hora de la acción (obligatoria)
FIREWALL	char(100)	Nombre calificado al completo de la máquina cortafuegos (obligatoria)
PID	int	ID de proceso AIX, ID de hebra NT (obligatoria)
MSG_NUM	int	Número de mensaje (obligatoria)

Tabla 3 (Página 2 de 2). FILTER_INFO. Esta tabla contiene los mensajes de información general o de errores relacionados con los FILTROS del archivo f_info.tbl.

Columna	Tipo de datos	Breve descripción
RULE_NUM	int	Número de norma de filtro (ICA1005)
ERROR_NUM	int	Número de Error del sistema -- Número de error de AIX o Último error de Windows NT (ICA1007, ICA1008, ICA1009, ICA1011 ICA1013, ICA1015, ICA1021, ICA1023, ICA1024) El texto que corresponde a este número de error puede obtenerse a través de la función _strerror. El texto para el último error de Windows NT está disponible a través de la función Formatear Mensaje o en el Apéndice A de la publicación Win32 Programmer's Reference Volume 2.
LOAD_PATH	char(100)	Vía de acceso de carga de extensión del kernel (ICA1011, ICA1012)
DVC_DRV	char(25)	Controlador de dispositivo (ICA1021)
TERM_SIG	char(25)	Señal de terminación (ICA1260)
FILE_NAME	char(100)	Nombre de archivo (ICA1024)
RC	int	Código de retorno interno del cortafuegos (ICA1019)
Nota: Mensajes relacionados: ICA1001 ICA1002 ICA1003 ICA1005 ICA1007 ICA1008 ICA1009 ICA1011 ICA1012 ICA1013 ICA1014 ICA1015 ICA1016 ICA1017 ICA1019 ICA1021 ICA1022 ICA1023 ICA1024 ICA1200 ICA1260		

Tabla 4 (Página 1 de 2). FILTER_MATCH. Esta tabla contiene las normas de filtro comparadas del archivo f_match.tbl.

Columna	Tipo de datos	Breve descripción
DATE_TIME	date_time	Fecha y hora de la acción (obligatoria)
FIREWALL	char(100)	Nombre calificado al completo de la máquina cortafuegos (obligatoria)
PID	int	ID de proceso AIX, ID de hebra NT (obligatoria)
MSG_NUM	int	Número de mensaje (obligatoria)
RULE_NUM	int	Número de norma (obligatoria)
ACTION	char(6)	Tipo de norma: permitir, denegar, etc.
DIRECTION	char(8)	Dirección del paquete, de entrada o de salida (obligatoria)
SRC_IP	char(15)	Dirección IP del remitente (obligatoria)
DST_IP	char(15)	Dirección IP del destinatario (obligatoria)
PROTOCOL	char(7)	Protocolo de alto nivel como, por ejemplo, UDP, IPIP, ICMP, TCP o TCP/ACK (obligatoria)

Tabla 4 (Página 2 de 2). FILTER_MATCH. Esta tabla contiene las normas de filtro comparadas del archivo f_match.tbl.

Columna	Tipo de datos	Breve descripción
SRC_PORT	int	<ul style="list-style-type: none"> Tipo de Paquete IP para ICMP Número de puerta del protocolo de recursos para otros (obligatoria)
DST_PORT	int	<ul style="list-style-type: none"> Código de Paquete IP para ICMP Número de puerta del protocolo de destino para otros (obligatoria)
ROUTING	char(5)	Afiliación de direccionamiento de los paquetes: direccionado o local (obligatoria)
INTERFACE	char(10)	Tipo de interfaz: segura o no segura (obligatoria)
FRAGMENT	char(8)	Identifica si el paquete es de tipo fragmento o no de fragmento (obligatoria)
TUNNEL_ID	int	ID del túnel (obligatoria)
ENCRYPTION	char(7)	Algoritmo de cifrado: DES_CBC o CDMF o ninguno
BYTES	long int	Longitud del paquete específico (obligatoria)
Nota: Mensaje relacionado: ICA1036		

Tabla 5. FILTER_STATUS. Esta tabla contiene información acerca de los cambios en el estado de los filtros del archivo f_stat.tbl.

Columna	Tipo de datos	Breve descripción
DATE_TIME	date_time	Fecha y hora de la acción (obligatoria)
FIREWALL	char(100)	Nombre calificado al completo de la máquina cortafuegos (obligatoria)
PID	int	ID de proceso AIX, ID de hebra NT (obligatoria)
MSG_NUM	int	Número de mensaje (obligatoria)
DAEMON	char(25)	Daemon de registro de filtros de AIX (ICA1004) o servicio de registro de filtros de Windows NT.
VERSION	int	Número de versión (ICA1004, ICA1033)
RELEASE	int	Número de release (ICA1004, ICA1033)
PACKET_LOGGING	char(8)	Estado del registro de paquetes, habilitado o inhabilitado (ICA1035)
Nota: Mensajes relacionados: ICA1004 ICA1032 ICA1033 ICA1034 ICA1035. Los detalles de las actualizaciones de normas de filtro (ICA1032) pueden obtenerse de la tabla FILTER_ACTIVE_RULE.		

Tabla 6. INTERFACES. Esta tabla contiene información de los mensajes de configuración de la interfaz (adaptador) del archivo interface.tbl.

Columna	Tipo de datos	Breve descripción
DATE_TIME	date_time	Fecha y hora de la acción (obligatoria)
FIREWALL	char(100)	Nombre calificado al completo de la máquina cortafuegos (obligatoria)
PID	int	ID de proceso AIX, ID de hebra NT (obligatoria)
MSG_NUM	int	Número de mensaje (obligatoria)
IP	char(15)	Dirección IP del adaptador (ICA9038, ICA9039, ICA9040)
OLD_MASK	char(15)	valor de la máscara anterior (ICA9040)
NEW_MASK	char(15)	valor de la máscara nueva (ICA9040)
Nota: Mensajes relacionados: ICA9037, ICA9038, ICA9039, ICA9040, ICA9041		

Tabla 7. NAT_INFO. Esta tabla contiene información de los mensajes de conversión de dirección de red del archivo nat_info.tbl.

Columna	Tipo de datos	Breve descripción
DATE_TIME	date_time	Fecha y hora de la acción (obligatoria)
FIREWALL	char(100)	Nombre calificado al completo de la máquina cortafuegos (obligatoria)
PID	int	ID de proceso AIX, ID de hebra NT (obligatoria)
MSG_NUM	int	Número de mensaje (obligatoria)
VERSION	int	Número de versión de NAT (ICA9033)
RELEASE	int	Número de release de NAT (ICA9033)
IP	char(15)	Dirección IP (ICA9035, ICA9036)
Nota: Mensajes relacionados: ICA9032, ICA9033, ICA9034, ICA9035, ICA9036		

Tabla 8 (Página 1 de 2). PAGER_INFO. Esta tabla contiene información relacionada con la función de envío de mensajes al buscapersonas del cortafuegos, del archivo pgr_info.tbl.

Columna	Tipo de datos	Breve descripción
DATE_TIME	date_time	Fecha y hora de la acción (obligatoria)
FIREWALL	char(100)	Nombre calificado al completo de la máquina cortafuegos (obligatoria)
PID	int	ID de proceso AIX, ID de hebra NT (obligatoria)
MSG_NUM	int	Número de mensaje (obligatoria)
USERID	char(16)	ID de usuario (ICA4036, ICA4174, ICA4175)
ERROR_NUM	int	Número de Error del sistema - Número de error de AIX o último error de Windows NT (ICA4371)

Tabla 8 (Página 2 de 2). *PAGER_INFO*. Esta tabla contiene información relacionada con la función de envío de mensajes al buscapersonas del cortafuegos, del archivo *pgr_info.tbl*.

Columna	Tipo de datos	Breve descripción
PROGRAM	char(25)	Nombre del programa (ICA4000)
SIGNAL	int	Señal de terminación (ICA4000)
ID	int	Identificador (ICA4036)
PRIORITY	int	Prioridad (ICA4036)
PERIOD	int	Período (ICA4036)
RETRY_COUNT	int	Número de reintentos (ICA4036, ICA4313, ICA4314, ICA4364, ICA4365)
FROM_ENTRY	char(15)	Nombre de la función (ICA4036)
HOST_NAME	char(100)	Nombre del sistema principal (ICA4174, ICA4175)
MESSAGE_TEXT	char(250)	Texto de la página (ICA4036, ICA4353 - 4360, ICA4368, ICA4372)
SERVICE	char(25)	Nombre del servicio (ICA4017)
SOCKET	int	Número de socket (ICA4017)
FILENAME	char(100)	Nombre del archivo (ICA4154, ICA4351, ICA4352)
Nota: Mensajes relacionados: ICA4000 ICA4001 ICA4007 ICA4017 ICA4036 ICA4154 ICA4168 ICA4174 ICA4175, ICA4300 - 4303, ICA4305 - 4315, ICA4351 - 4360, ICA4362 - 4372)		

Tabla 9. *PROXY_FTP*. Esta tabla contiene información de las acciones FTP de las sesiones FTP del archivo *p_ftp.tbl*.

Columna	Tipo de datos	Breve descripción
DATE_TIME	date_time	Fecha y hora de la acción (obligatoria)
FIREWALL	char(100)	Nombre calificado al completo de la máquina cortafuegos (obligatoria)
PID	int	ID de proceso AIX, ID de hebra NT (obligatoria)
MSG_NUM	int	Número de mensaje (obligatoria)
USERID	char(16)	ID de usuario (obligatoria)
SRC_IP	char(15)	Dirección IP del usuario (obligatoria)
DST_IP	char(15)	Dirección IP de la máquina remota (obligatoria)
ACTION	char(5)	Acción de transferencia de archivos: put o get (obligatoria)
FILE_NAME	char(100)	Nombre del archivo
BYTES	long int	Cantidad de datos transferidos.
SID	long int	ID de sesión exclusivo (obligatoria)
Nota: Mensaje relacionado: ICA2075		

Tabla 10. *PROXY_HTTP*. Esta tabla contiene información de las acciones HTTP de las sesiones Proxy del archivo *p_http.tbl*.

Columna	Tipo de datos	Breve descripción
DATE_TIME	date_time	Fecha y hora de la acción (obligatoria)
FIREWALL	char(100)	Nombre calificado al completo de la máquina cortafuegos (obligatoria)
PID	int	ID de proceso AIX, ID de hebra NT (obligatoria)
MSG_NUM	int	Número de mensaje (obligatoria)
STATUS	int	Estado (obligatoria)
SRC_IP	char(15)	Dirección IP del usuario (obligatoria)
REQUEST	char(250)	Contenido de la petición HTTP (obligatoria)
BYTES	long int	Cantidad de datos transferidos.

Nota: Mensaje relacionado: ICA2099

Tabla 11 (Página 1 de 2). *PROXY_INFO*. Esta tabla contiene los mensajes de información general y de errores relacionados con *PROXY* del archivo *p_info.tbl*.

Columna	Tipo de datos	Breve descripción
DATE_TIME	date_time	Fecha y hora de la acción (obligatoria)
FIREWALL	char(100)	Nombre calificado al completo de la máquina cortafuegos (obligatoria)
PID	int	ID de proceso AIX, ID de hebra NT (obligatoria)
MSG_NUM	int	Número de mensaje (obligatoria)
USERID	char(16)	ID de usuario (ICA2018, ICA2019, ICA2057, ICA2058, ICA2166, ICA2177, ICA2172)
ERROR_NUM	int	Número de Error del sistema - Número de error de AIX o último error de Windows NT (ICA2005, ICA2006, ICA2009, ICA2029, ICA2035, ICA2038, ICA2039, ICA2052, ICA2054, ICA2055, ICA2056, ICA2057, ICA2058, ICA2059, ICA2063, ICA2064, ICA2065, ICA2066, ICA2067, ICA2068, ICA2069, ICA2069, ICA2070, ICA2071, ICA2074, ICA2110, ICA2111, ICA2113, ICA2114, ICA2115, ICA2118, ICA2119, ICA2121, ICA2122, ICA2123, ICA2124, ICA2200, ICA2201, ICA2202, ICA2203) El texto del número de error (Errores del sistema AIX) puede obtenerse a través de la función <code>_strerror</code> . El texto para el último error de Windows NT está disponible a través de la función <code>Formatear Mensaje</code> o en el Apéndice A de la publicación <code>Win32 Programmer's Reference Volume 2</code> .
OPTION_VAL	char(20)	Distintivo de opción o valor de parámetro (ICA2014, ICA2015, ICA2049, ICA2050)

Tabla 11 (Página 2 de 2). PROXY_INFO. Esta tabla contiene los mensajes de información general y de errores relacionados con PROXY del archivo p_info.tbl.

Columna	Tipo de datos	Breve descripción
TIME	char(15)	Intervalo de tiempo no válido (ICA2044, ICA2202)
RC	int	Código de retorno interno del cortafuegos (ICA2007, ICA2030, ICA2031, ICA2033, ICA2034, ICA2054, ICA2057, ICA2058, ICA2065, ICA2120 ICA2166, ICA2203)
INVOC_NAME	char(20)	Nombre de la invocación para el socket o la puerta en el momento de producirse el error (ICA2055, ICA2056)
AUDIT_TYPE	char(7)	Tipo de comprobación desconocido (7 dígitos hexadecimales) (ICA2004)
HOST_NAME	char(100)	Nombre del sistema principal (ICA2106, ICA2107, ICA2126)
FILE_NAME	char(100)	Nombre del archivo (ICA2029, ICA2030, ICA2072, ICA2183, ICA2204, ICA2205, ICA2206, ICA2207)
LINE_NUM	int	Número de la línea (ICA2029, ICA2030)
PROTOCOL	char(25)	Nombre de protocolo no válido (ICA2112, ICA2116)
CUSTOMIZED_ATTR	char(25)	Número de la línea (ICA2105, ICA2106, ICA2125, ICA2166)
ODM_ERR_NUM	int	Número de error del Gestor de Datos de Objetos (ICA2102, ICA2103, ICA2104, ICA2105, ICA2107, ICA2108, ICA2109, ICA2125)
APPLICATION (sólo NT)	char(30)	Nombre de la aplicación (ICA2200, ICA2201, ICA2202, ICA2203, ICA2204, ICA2205, ICA2206, ICA2207)
CALLER (sólo NT)	char(25)	Función que llama (ICA2200, ICA2201, ICA2202, ICA2203, ICA2204, ICA2205, ICA2206, ICA2207)
FAILED_IN (sólo NT)	char(25)	Función anómala (ICA2201, ICA2203)
Nota: Mensajes relacionados: 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		

Tabla 12. PROXY_LOGIN. Esta tabla contiene información (principalmente relacionada con la autenticación) acerca de las conexiones satisfactorias de PROXY del archivo p_login.tbl.

Columna	Tipo de datos	Breve descripción
DATE_TIME	date_time	Fecha y hora de la acción (obligatoria)
FIREWALL	char(100)	Nombre calificado al completo de la máquina cortafuegos (obligatoria)
PID	int	ID de proceso AIX, ID de hebra NT (obligatoria)
MSG_NUM	int	Número de mensaje (obligatoria)
USERID	char(16)	ID de usuario (obligatoria)
APPLICATION	char(30)	Nombre de la aplicación - telnet, ftp, ... (obligatoria)
AUTH_METHOD	char(15)	Método de autenticación (obligatoria)
NETWORK	char(25)	Red (segura/no segura - también puede tener información adicional) (obligatoria)
HOST_NAME	char(100)	Nombre del sistema principal (obligatoria)
Nota: Mensajes relacionados: ICA2024 ICA2025 ICA2169		

Tabla 13 (Página 1 de 2). PROXY_STATUS. Esta tabla contiene la información de estado de PROXY del archivo p_stat.tbl.

Columna	Tipo de datos	Breve descripción
DATE_TIME	date_time	Fecha y hora de la acción (obligatoria)
FIREWALL	char(100)	Nombre calificado al completo de la máquina cortafuegos (obligatoria)
PID	int	ID de proceso AIX, ID de hebra NT (obligatoria)
MSG_NUM	int	Número de mensaje (obligatoria)
USERID	char(16)	ID de usuario (ICA2008, ICA2016, ICA2021)
SRC_IP	char(15)	Dirección IP de origen (ICA2000, ICA2008, ICA2010, ICA2011, ICA2012, ICA2013, ICA2141, ICA2180)
DST_IP	char(15)	Dirección IP de destino (ICA2000, ICA2010, ICA2011, ICA2012, ICA2013)
REMOTE_HOST	char(100)	Nombre del sistema principal remoto (desde la perspectiva de la máquina cortafuegos (ICA2021, ICA2022, ICA2027)
SID (sólo NT)	int	Identificador de la sesión (ICA2177, ICA2180, ICA2181 ICA2182)
SOCKET (sólo NT)	char(25)	Nombre del socket (ICA2177)
RC (sólo NT)	int	Código de retorno o de razón (ICA2181, ICA2182)
CMD (sólo NT)	char(36)	Tarjeta SMTP (ICA2182)

Tabla 13 (Página 2 de 2). PROXY_STATUS. Esta tabla contiene la información de estado de PROXY del archivo p_stat.tbl.

Columna	Tipo de datos	Breve descripción
Nota: Mensajes relacionados: ICA2000 ICA2010 ICA2011 ICA2012 ICA2013 ICA2016 ICA2021 ICA2022 ICA2027 ICA2097 ICA2098 ICA2141 ICA2163 ICA2164 ICA2165 ICA2177 ICA2180 ICA2181 ICA2182		

Tabla 14. SERVER_INFO. Esta tabla contiene información acerca del estado y actividades del Servidor de Configuración del Archivo srv_info.tbl.

Columna	Tipo de datos	Breve descripción
DATE_TIME	date_time	Fecha y hora de la acción (obligatoria)
FIREWALL	char(100)	Nombre calificado al completo de la máquina cortafuegos (obligatoria)
PID	int	ID de proceso AIX, ID de hebra NT (obligatoria)
MSG_NUM	int	Número de mensaje (obligatoria)
USERID	char(16)	ID de usuario (ICA9003, ICA9004)
ERROR_NUM	int	Número de Error del sistema - Número de error de AIX o Último error de Windows NT (ICA9008, ICA9009) El texto del número de error (Errores del sistema AIX) puede obtenerse con la función strerror. El texto para el último error de Windows NT está disponible a través de la función Formatear Mensaje o en el Apéndice A de la publicación Win32 Programmer's Reference Volume 2.
Nota: Mensajes relacionados: ICA9003 ICA9004 ICA9005 ICA9006 ICA9007 ICA9008 ICA9009 ICA9010 ICA9011 ICA9012 ICA9013 ICA9014 ICA9015		

Tabla 15 (Página 1 de 2). SESSION. Esta tabla contiene información de inicio/detención de la sesión SOCKS y PROXY del archivo session.tbl.

Columna	Tipo de datos (longitud)	Breve descripción
DATE_TIME	date_time	Fecha y hora de la acción (obligatoria)
FIREWALL	char(100)	Nombre calificado al completo de la máquina cortafuegos (obligatoria)
PID	int	ID de proceso AIX, ID de hebra NT (obligatoria)
MSG_NUM	int	Número de mensaje (obligatoria)
USERID	char(16)	ID de usuario (obligatoria)
SERVICE_TYPE	char(10)	Tipo de servicio: socks o proxy (obligatoria)
APPLICATION	char(30)	Nombre de la aplicación - telnet, ftp, (obligatoria)

Tabla 15 (Página 2 de 2). *SESSION*. Esta tabla contiene información de inicio/detención de la sesión *SOCKS* y *PROXY* del archivo *session.tbl*.

Columna	Tipo de datos (longitud)	Breve descripción
SRC_IP	char(15)	Dirección IP del usuario (obligatoria)
DST_IP	char(15)	Dirección IP de la máquina remota (obligatoria)
SESSION_EVENT	char(5)	<ul style="list-style-type: none"> • empezar cuando se establece una sesión. • finalizar cuando se termina una sesión. (obligatorio)
BYTES	long int	Cantidad de datos transferidos durante la sesión. Si la aplicación es telnet, será 0.
SID	long int	Identificador de sesión exclusivo, generado por el cortafuegos, en base a la hora del reloj.

Nota:

Mensajes relacionados:

- Inicio de sesión Safemail: ICA2178
- Detención de sesión Safemail: ICA2179
- Inicio de sesión Socks: ICA3011
- Detención de sesión Socks: ICA3015
- Inicio de sesión de Proxy Telnet: ICA2036 (Registros AIX) ICA2208, ICA2218 (Registros NT)
- Detención de sesión Proxy Telnet: ICA2077 (Registros AIX) ICA2209, ICA2219 (Registros NT)
- Inicio de sesión de Proxy FTP: ICA2041 (Registros AIX) ICA2208, ICA2218 (Registros NT)
- Detención de sesión Proxy FTP: ICA2076 (Registros AIX y NT)

Los detalles de las acciones de la sesión Socks FTP se encuentran en la tabla *SOCKS_FTP*.
Los detalles de las acciones Proxy FTP se encuentran en *PROXY_FTP*.

Tabla 16 (Página 1 de 2). *SOCKS_FTP*. Esta tabla contiene la información de las acciones *SOCKS FTP* de las sesiones FTP del archivo *s_ftp.tbl*.

Columna	Tipo de datos	Breve descripción
DATE_TIME	date_time	Fecha y hora de la acción (obligatoria)
FIREWALL	char(100)	Nombre calificado al completo de la máquina cortafuegos (obligatoria)
PID	int	ID de proceso AIX, ID de hebra NT (obligatoria)
MSG_NUM	int	Número de mensaje (obligatoria)
USERID	char(16)	ID de usuario (obligatoria)
SRC_IP	char(15)	Dirección IP del usuario (obligatoria)
DST_IP	char(15)	Dirección IP de la máquina remota (obligatoria)

Tabla 16 (Página 2 de 2). SOCKS_FTP. Esta tabla contiene la información de las acciones SOCKS FTP de las sesiones FTP del archivo s_ftp.tbl.

Columna	Tipo de datos	Breve descripción
DATA_BIND	char(5)	<ul style="list-style-type: none"> 'iniciar' cuando se establece el vínculo de datos. (ICA3010) 'detener' cuando finaliza el vínculo de datos. (ICA3014) (obligatoria)
BYTES	long int	Cantidad de datos transferidos.
Nota: Mensajes relacionados: ICA3010 ICA3014		

Tabla 17 (Página 1 de 2). SOCKS_INFO. Esta tabla contiene los mensajes de información general y de errores relacionados con Socks del archivo s_info.tbl.

Columna	Tipo de datos	Breve descripción
DATE_TIME	date_time	Fecha y hora de la acción (obligatoria)
FIREWALL	char(100)	Nombre calificado al completo de la máquina cortafuegos (obligatoria)
PID	int	ID de proceso AIX, ID de hebra NT (obligatoria)
MSG_NUM	int	Número de mensaje (obligatoria)
USERID	char(16)	ID de usuario (ICA3044, ICA3045, ICA3046, ICA3047, ICA3049)
ACTION	char(7)	"connect" (ICA3044, ICA3049) o "bind" (ICA3046, ICA3047)
ERROR_NUM	int	Número de Error del sistema - Número de error de AIX (ICA3013, ICA3019, ICA3031, ICA3032, ICA3040, ICA3044, ICA3101, ICA3102, ICA3103, ICA3104, ICA3106, ICA3107, ICA3108, ICA3122, ICA3124, ICA3125, ICA3126, ICA3128)
SRC_HOST	char(25)	Nombre del sistema principal de origen (ICA3019, ICA3035)
DST_HOST	char(25)	Nombre del sistema principal de destino (ICA3016, ICA3045)
SRC_IP	char(15)	Dirección de origen (ICA3042, ICA3043, ICA3044, ICA3045, ICA3046, ICA3047, ICA3049)
DST_IP	char(15)	Dirección de destino (ICA3044, ICA3045, ICA3046, ICA3047, ICA3049)
LINE_NUM	int	Número de línea (ICA3022, ICA3023, ICA3024, ICA3025, ICA3026, ICA3109, ICA3110, ICA3111, ICA3112, ICA3115, ICA3116, ICA3117, ICA3118, ICA3119, ICA3120); o Número de líneas (ICA3113)
EXEC_STATUS	int	Estado de la ejecución (ICA3027)

Tabla 17 (Página 2 de 2). SOCKS_INFO. Esta tabla contiene los mensajes de información general y de errores relacionados con Socks del archivo s_info.tbl.

Columna	Tipo de datos	Breve descripción
CMD	char(36)	Mandato, como login (ICA3027, ICA3039, ICA3042, ICA3044, ICA3048) nota: para ICA3042, el mandato está en formato hexadecimal
FILE_NAME	char(100)	Nombre del archivo (ICA3030, ICA3032, ICA3105, ICA3109, ICA3110, ICA3111, ICA3112, ICA3113, ICA3114, ICA3115, ICA3116, ICA3117, ICA3118, ICA3119, ICA3120)
APPLICATION	char(30)	Nombre de la aplicación - telnet, ftp, ... (ICA3044, ICA3045, ICA3049)
VERSION	char(10)	Número de la versión de Socks en hexadecimal (ICA3043)
Nota: Mensajes relacionados: 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		

Tabla 18. SSL_INFO. Esta tabla contiene información acerca de las actividades y el estado de SSL del archivo ssl_info.tbl.

Columna	Tipo de datos	Breve descripción
DATE_TIME	date_time	Fecha y hora de la acción (obligatoria)
FIREWALL	char(100)	Nombre calificado al completo de la máquina cortafuegos (obligatoria)
PID	int	ID de proceso AIX, ID de hebra NT (obligatoria)
MSG_NUM	int	Número de mensaje (obligatoria)
Client_IP	char(15)	Dirección IP del cliente
Nota: Mensajes relacionados: ICA5015 ICA5022 ICA5023 ICA5028 ICA5029 ICA5036 ICA5039 ICA5060 ICA5063 ICA5082 ICA5120		

Tabla 19. SU. Esta tabla contiene detalles acerca de las actividades SU del archivo su.tbl si se está cargando un registro su.

Columna	Tipo de datos	Breve descripción
DATE_TIME	date_time	Fecha y hora de la acción (obligatoria) Puesto que AIX no registra el año en el archivo de registro su, la parte del año de la columna DATE_TIME se establece en el año actual o en el año anterior, en base a los valores de mes/día (si mes/día es posterior al mes/día actual, se da por supuesto que se trata del año anterior.)
FROM_USERID	char(16)	ID de usuario (obligatoria)
TO_USERID	char(16)	ID de usuario (obligatoria)
LOGIN_STATUS	char(7)	Estado del intento de conexión: satisfactorio o anómalo (obligatoria)

Tabla 20. TUNNEL_CONTEXT. Esta tabla contiene las especificaciones del contexto de TÚNEL activo del archivo t_cntxt.tbl.

Columna	Tipo de datos	Breve descripción
DATE_TIME	date_time	Fecha y hora de la acción (obligatoria)
FIREWALL	char(100)	Nombre calificado al completo de la máquina cortafuegos (obligatoria)
PID	int	ID de proceso AIX, ID de hebra NT (obligatoria)
MSG_NUM	int	Número de mensaje (obligatoria)
TUNNEL_ID	long int	ID del túnel (obligatoria)
SRC_IP	char(15)	Dirección IP de origen (obligatoria)
DST_IP	char(15)	Dirección IP de destino (obligatoria)
ENCRYPTION	char(7)	Algoritmo de cifrado DES_CBC o CDMF

Nota: Mensaje relacionado: ICA1043

Tabla 21 (Página 1 de 2). TUNNEL_POLICY. Esta tabla contiene las sentencias de la política de TÚNEL del archivo t_policy.tbl.

Columna	Tipo de datos	Breve descripción
DATE_TIME	date_time	Fecha y hora de la acción (obligatoria)
FIREWALL	char(100)	Nombre calificado al completo de la máquina cortafuegos (obligatoria)
PID	int	ID de proceso AIX, ID de hebra NT (obligatoria)
MSG_NUM	int	Número de mensaje (obligatoria)

Tabla 21 (Página 2 de 2). TUNNEL_POLICY. Esta tabla contiene las sentencias de la política de TÚNEL del archivo t_policy.tbl.

Columna	Tipo de datos	Breve descripción
POLICY	char(60)	Lectura de la sentencia de política del archivo fwpolicy (obligatoria)
Nota: Mensaje relacionado: ICA1040		

Tabla 22. TUNNEL_STATUS. Esta tabla contiene información acerca de los cambios en el estado de los TÚNELES del archivo t_stat.tbl.

Columna	Tipo de datos	Breve descripción
DATE_TIME	date_time	Fecha y hora de la acción (obligatoria)
FIREWALL	char(100)	Nombre calificado al completo de la máquina cortafuegos (obligatoria)
PID	int	ID de proceso AIX, ID de hebra NT (obligatoria)
MSG_NUM	int	Número de mensaje (obligatoria)
SESSION_SCKT	long int	Puerta del socket de la sesión (para ICA1038)
MASTER_SCKT	long int	Puerta del socket maestro (para ICA1038)
TUNNEL_ID	long int	ID de túnel suprimido (para ICA1041)
Nota: Mensajes relacionados: ICA1038 ICA1039 ICA1041 ICA1042 <ul style="list-style-type: none"> Los detalles de la política definida (ICA1039 pueden obtenerse de la tabla TUNNEL_POLICY. Los detalles del contexto de túnel definido (ICA1042) pueden obtenerse de la tabla TUNNEL_CONTEXT. 		

Capítulo 3. Kit de desarrollo de software del "Plug-in" de SafeMail

La finalidad básica de la pasarela SafeMail del IBM Firewall es enviar correo entre las redes protegidas y no protegidas a la vez que se ocultan los nombres de los sistemas principales de la red protegida.

La pasarela SafeMail no proporciona ninguna capacidad de filtrado de contenidos propia. Si embargo, puede grabar un Visualizador de contenidos de SafeMail e instalarlo en el cortafuegos como un "plug-in" de la pasarela SafeMail. El "plug-in" de su pasarela de SafeMail tiene la capacidad de ver todo el mensaje de correo electrónico y discriminar el correo electrónico según los criterios que establezca. El "plug-in" de la pasarela SafeMail puede indicar a la pasarela SafeMail que cancele la transferencia de un mensaje o permita que el mensaje circule a través de la pasarela.

Visión general del proceso de SafeMail

Cuando un cliente SMTP se conecta a la pasarela SafeMail, la pasarela SafeMail se conecta al servidor SMTP de destino y pasa el mensaje de correo electrónico línea a línea cada vez desde el cliente al servidor de destino según recibe las líneas de correo electrónico del cliente. La pasarela de SafeMail reescribirá algunas líneas de encabezados del correo electrónico según haga falta para ocultar los nombres de los sistemas principales de la red protegida.

Si un "plug-in" del discriminador de contenidos está instalado, la pasarela de SafeMail llamará al discriminador de contenidos con cada línea del mensaje de correo electrónico según pasa a través de la pasarela. La pasarela de SafeMail también pasa información sobre el origen y el destino del mensaje de correo electrónico y otras informaciones, de forma que el discriminador de contenidos pueda correlacionar las varias llamadas con cada otro. Esto puede ser útil en los casos en que hay que analizar todo el mensaje antes de que el discriminador de contenidos pueda tomar una decisión sobre si permite que el mensaje circule a través de este cortafuegos o no.

Si la pasarela SafeMail debe volver a escribir cualquiera de los encabezados para esconder los nombres de los sistemas principales de la red protegida, el "plug-in" del discriminador de contenidos se llamará antes de que se haya vuelto a escribir el encabezado.

Creación de un "Plug-in" de la pasarela SafeMail

Para crear e instalar un "plug-in" de la pasarela de SafeMail deberá:

- Escribir el código fuente para la DLL del "plug-in"
- Crear la DLL
- Instalar la DLL en el cortafuegos

ROOTDIR\samples\safemail contiene código de muestra para el "plug-in" de un discriminador de contenidos, los archivos de encabezados necesarios y makefiles de ejemplo para IBM Visual Age y Microsoft Visual C++. ROOTDIR es el directorio

que ha seleccionado durante el proceso de instalación como ubicación de destino para IBM Firewall.

Grabación del código fuente

El "plug-in" del discriminador de contenidos debe incorporar una función denominada `UsrCheck`, que tiene el siguiente prototipo:

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

Este es el punto de entrada que llama la pasarela de SafeMail cuando tiene una línea de correo electrónico lista para que la compruebe el discriminador de contenidos. Esta función es responsable del examen de la línea del mensaje de correo electrónico y de devolver 0 si quiere que el mensaje de correo electrónico siga su curso a través de la pasarela de SafeMail o no cero si quiere que SafeMail cancele el proceso del mensaje.

Consulte el código de muestra de `usrcheck.c` en `R00TDIR\samples\safemail` para obtener una descripción completa de la interfaz entre la pasarela de SafeMail y el discriminador de contenidos.

El parámetro `pCheckData` de la función de comprobación es una estructura de C documentada en `usrcheck.h` en `R00TDIR\samples\safemail`. Esta estructura contiene información importante sobre el mensaje de correo electrónico que se procesa, como las direcciones de origen y destino de los servidores SMTP y los tipos de redes (protegidas y no protegidas) para los servidores SMTP que envían y reciben. Esta estructura también contiene un correlacionador de conversación que permitirá al discriminador de contenidos correlacionar varias llamadas con el mismo mensaje de correo electrónico.

Creación de la DLL

Cuando haya escrito el código fuente del "plug-in" del supervisor de contenidos, deberá compilarlo y vincularlo en una DLL. La DLL debe tener el nombre `smusr.dll`. Y el punto de entrada `UsrCheck` debe exportarse desde la DLL. Consulte los `makefiles` de muestra en `R00TDIR\samples\safemail` para obtener ejemplos de los conmutadores de compilación y vinculación necesarios para crear la DLL correctamente. Se suministran `makefiles` de muestra para IBM VisualAge C++ y Microsoft Visual C.

Instalación de la DLL

Cuando haya creado satisfactoriamente `smusr.dll`, instálelo en el cortafuegos. Copie `smusr.dll` en el directorio `\bin` del cortafuegos. A continuación utilice el Gestor de control de servicios del panel de control de Windows NT para detener y reiniciar el servidor SafeMail de IBM Firewall para que se cargue el "plug-in".

El IBM Firewall incluye el `smusr.dll` de muestra del directorio `\bin` del cortafuegos. Cambie el nombre de esta DLL antes de copiar `smusr.dll` en ese directorio para que pueda restaurarla si elimina su plug-in en el futuro.

Los nombres del compilador varían de instancia a instancia en este y los siguientes dos capítulos. Los tres capítulos se refieren a los dos mismos compiladores.

Capítulo 4. Kit de desarrollo de software del "plug-in" del archivador de registro

El daemon de registro del IBM Firewall guarda la información de registro en los archivos que especifica con el cuadro de diálogo **Recursos de registro** del cliente de configuración. A continuación use el mandato `fwlogmgmt` para archivar periódicamente los registros antiguos. Normalmente ejecuta el mandato `fwlogmgmt` desde el Scheduler de Windows NT. Por omisión, el mandato `fwlogmgmt` archiva registros antiguos y los comprime usando el mandato `compact` de Windows NT. Sin embargo, puede escribir un "plug-in" de archivador de registro para reemplazar el comportamiento del archivador por omisión.

Cómo crear un "plug-in" de archivador de registro

Para crear un "plug-in" del archivador de registro debe:

1. Escribir el código fuente para la DLL del "plug-in"
2. Crear la DLL
3. Instalar la DLL en el cortafuegos

El directorio `R00TDIR\sample\logarch` contiene código de muestra para un "plug-in" del archivador del registro que duplica el comportamiento por omisión del cortafuegos y un makefile para IBM Visual Age para C++. `R00TDIR` es el directorio que ha seleccionado durante el proceso de instalación como ubicación de destino para IBM Firewall.

Grabación del código fuente

El "plug-in" del archivador de registro debe incorporar un conjunto de funciones que el cortafuegos utiliza para llevar a cabo la función de archivado. Los prototipos de estas funciones se definen en `fwarch.h` en el directorio `R00TDIR\sample\logarch`.

Estas funciones incorporan funciones de archivado básicas como la adición de un archivo a un archivador, la extracción de un archivo de un archivador, la revocación de un archivador y el listado de los archivos de un archivador.

Consulte el código de muestra de `fwarch.c` en el directorio `R00TDIR\sample\logarch` para obtener más detalles sobre estas funciones.

Creación de la DLL

Cuando haya escrito el código fuente para el "plug-in" del archivador de registro, deberá compilarlo y vincularlo a una DLL. La DLL debe tener el nombre `fwarch.dll`. Todas las funciones listadas en `fwarch.h` deben exportarse desde la DLL.

Se proporciona un makefile de muestra para IBM VisualAge para C++ para construir el código de muestra en las DLL adecuadas en el directorio `R00TDIR\sample\logarch`.

Instalación de la DLL

Cuando haya creado satisfactoriamente fwarch.dll, instálelo en el cortafuegos. Copie fwarch.dll en el directorio R00TDIR\bin.

El archivo fwarch.dll por omisión del cortafuegos también se encuentra en este directorio. Haga una copia de seguridad de esta DLL o cámbiele el nombre antes de copiar su DLL en este directorio.

Igualmente, asegúrese de que el mandato fwlogmgt no se está ejecutando actualmente y de que el daemon de registro del IBM Firewall no se está ejecutando cuando reemplaza la DLL por omisión. Utilice el Gestor del control de servicios para detener el daemon de registro de IBM Firewall y a continuación reiniciarla cuando haya reemplazado la DLL.

Capítulo 5. Cómo suministrar sus propios métodos de autenticación

Este capítulo ofrece información sobre cómo suministrar sus propios métodos de autenticación.

Autenticación suministrada por el usuario

Se facilita una autenticación de usuario de ejemplo, que se encuentra en el directorio `ROOT_DIR\bin\authsdk`. Los archivos que se incluyen son:

- `authschm.h` - archivos de definición de interfaz
- `authus.cpp` - archivo fuente para el esquema de ejemplo
- `gwauth4.lib` - biblioteca del Cortafuegos
- `msvc++.mak` - Creación de archivos de Microsoft Visual C
- `schmname.h` - archivos de definición de interfaz
- `vac++.mak` - Creación de archivos de IBM Visual Age

Utilice los mandatos siguientes para compilar la autenticación de usuario de ejemplo para Visual Age de IBM:

- `nmake -f vac++.mak` - crea la DLL
- `nmake -f vac++.mak install` - crea e instala la DLL
- `nmake -f vac++.mak clean` - borra el directorio local

Utilice los mandatos siguientes para compilar la autenticación de usuario de ejemplo para Visual C de Microsoft:

- `nmake -f msvc++.mak` - crea la DLL
- `nmake -f msvc++.mak install` - crea e instala la DLL
- `nmake -f msvc++.mak clean` - borra el directorio local

Utilización del Kit para el desarrollo del software para crear un esquema de autenticación suministrada por el usuario

IBM Firewall proporciona una interfaz de conexión para habilitar la integración de productos de seguridad de autenticación de otras empresas. Lo consigue grabando una `.dll` de esquema de autenticación que se conecta a la interfaz del esquema de autenticación del cortafuegos.

Visión general del proceso de autenticación del cortafuegos

Los siguientes servicios de cortafuegos deben autenticar a los usuarios para que puedan acceder a los servicios de cortafuegos:

- Servidor de configuración de IBM Firewall
- Daemon del proxy FTP de IBM Firewall
- Daemon del proxy HTTP de IBM Firewall

- Daemon Telnet de IBM Firewall
- Servidor socks de IBM Firewall

El cortafuegos proporciona los esquemas de autenticación siguientes:

Denegar todo Al usuario siempre se le niega el acceso al servicio.

Permitir todo Al usuario se le permite acceder al servicio directamente.

Contraseña del cortafuegos Al usuario se le solicita una contraseña que se define en la base de datos Usuario del Cortafuegos.

Contraseña de conexión NT Al usuario se le solicita su Contraseña de conexión de Windwos NT.

Clave SecureNet El usuario se autentifica con la Clave AssureNet Pathways SecureNet.

Tarjeta SecurID El usuario se autentifica con la tarjeta de seguridad Security Dinamics SecurID.

El esquema de autenticación utilizado puede definirse para cada usuario o para cada servicio. Por ejemplo, el cortafuegos puede configurarse para que cuando el usuario *Roberto* intente conectarse al servidor de configuración de IBM Firewall tenga que especificar su Contraseña de conexión de Windows NT. Pero cuando *Roberto* desee utilizar el Proxy Telnet de IBM Firewall, se autentificará utilizando su tarjeta SecurID. Entretanto, cuando la usuaria *María* intente conectarse al Servidor de configuración de IBM Firewall se le solicitará su Contraseña del cortafuegos. Consulte el capítulo Administración del manual *IBM eNetwork Firewall - Guía del usuario* para obtener más información acerca de los esquemas que facilita el cortafuegos y acerca de cómo definirlos para cada usuario.

Además de los esquemas de autenticación que proporciona IBM Firewall, puede instalar hasta tres esquemas de autenticación suministrados por el usuario. Puede grabar estos esquemas para que interactúen con la infraestructura de seguridad existente o puede obtenerlos de otros proveedores de seguridad para integrar sus productos al cortafuegos.

Cada esquema de autenticación del cortafuegos, incluyendo los esquemas de autenticación suministrados por el usuario, se representa mediante una DLL que implementa la API del esquema de autenticación. Esta API define la forma en que el esquema de autenticación se autorregistra en el cortafuegos y cómo éste le pasa las peticiones de autenticación.

Creación de un esquema de autenticación suministrada por el usuario

La creación de un esquema de autenticación suministrada por el usuario se compone de los pasos siguientes:

- Grabación del código fuente para implantar la API del esquema de autenticación
- Compilación y enlace del código fuente en una DLL
- Instalación de la DLL en el cortafuegos

Los archivos fuente C de cabeceras y de bibliotecas necesarios para crear un esquema de autenticación suministrado por el usuario, así como el código de

ejemplo y la creación de archivos de ejemplo para Microsoft Visual C++ e IBM Visual Age para C++, pueden encontrarse en R00TDIR\bin\authsdk.

Grabación del código fuente

Todos los esquemas de autenticación debe hacer dos cosas:

1. Registrarse en el cortafuegos
2. Implementar AuthSchmFn

Registro con el cortafuegos: Antes de que se inicien los servicios del cortafuegos, éste intenta cargar todas las DLL que encuentran en el subdirectorio \bin\authschm. A medida que se carga cada DLL, su rutina de inicialización debe llamar a una función del cortafuegos denominada registerAuthSchm para que pueda autorregistrarse en el cortafuegos.

El prototipo de la función registerAuthSchm se define en el archivo de cabeceras authschm.h. Toma un único parámetro que es un puntero a una estructura AuthSchmInfo, que también se define en authschm.h. La estructura AuthSchmInfo asocia un nombre de esquema de autenticación a la dirección de AuthSchmFn correspondiente que el cortafuegos debe llamar para pasar las peticiones de autenticación al esquema de autenticación.

Los esquemas de autenticación suministrada por el usuario deben utilizar uno de estos tres nombres:

1. user
2. userauth2
3. userauth3

En el archivo de cabeceras schmname.h existen nombres simbólicos definidos para estos nombres. Tenga en cuenta que los esquemas de autenticación suministrada por el usuario deben diseñarse para permitir al usuario final especificar cuál de estos tres nombres se utiliza, para que puedan instalarse en el mismo cortafuegos varios esquemas de autenticación suministrada por el usuario sin tener que preocuparse de si dos esquemas distintos necesitan el mismo nombre.

Cuando la rutina de inicialización de la DLL ha llamado satisfactoriamente al registro AuthSchm y ha vuelto al emisor, la DLL debe prepararse para procesar las peticiones de autenticación. Por este motivo, puede que también sea necesario realizar una inicialización específica del esquema en la rutina de inicialización de la DLL.

Implementación de AuthSchmFn: Cada DLL del esquema de autenticación debe implementar una función denominada AuthSchmFn utilizando el prototipo que se define en authschm.h. La función AuthSchmFn tiene un parámetro, un puntero a una estructura AuthReq. La estructura AuthReq es una estructura C sencilla que contiene toda la información que pertenece a la petición de autenticación actual. La estructura AuthReq se define en authschm.h y contiene el nombre del usuario que está autenticándose, la petición de componente/servicio del cortafuegos y otras informaciones acerca de la petición. Para obtener una lista completa y la explicación de la información de la estructura AuthReq, consulte los comentarios acerca de ello en authschm.h.

Además del nombre del usuario y del componente del cortafuegos, la estructura `AuthReq` tiene tres parámetros que son especialmente importantes para la implementación de un esquema de autenticación:

- gwaput** Es la dirección de una rutina de llamada de retorno que proporciona el cortafuegos, que el esquema de autenticación puede utilizar siempre que necesite enviar un mensaje al usuario. Por ejemplo, si el esquema de autenticación necesita emitir un mensaje de solicitud para el usuario, para ello llamaría al punto de entrada que se facilita en el parámetro `gwaput`. La función de llamada de retorno `gwaput` es un prototipo creado por `AuthSchmPut` typedef en `authschm.h`. Consulte los comentarios de `AuthSchmPut` typedef para obtener una lista completa de los parámetros que `AuthSchmFn` debe pasar en esta llamada.
- gwaget** Es la dirección de una rutina de llamada de retorno que proporciona el cortafuegos, que el esquema de autenticación puede utilizar siempre que necesite recuperar una respuesta del usuario final que está autenticándose. Por ejemplo, si el esquema de autenticación necesita que el usuario le proporcione una contraseña, para ello llamaría al punto de entrada que se facilita en el parámetro `gwaget`. La función de llamada de retorno `gwaget` es un prototipo creado por `AuthSchmGet` typedef en `authschm.h`. Consulte los comentarios de `AuthSchmGet` typedef para obtener una lista completa de los parámetros que `AuthSchmFn` debe pasar en esta llamada. Un parámetro especialmente importante es el parámetro `echo`. `AuthSchmFn` puede utilizar este parámetro para indicar si la respuesta del usuario debe devolverse a éste visualizándose en forma de caracteres o no.
- opaque_data** El cortafuegos utiliza el campo `opaque_data` para correlacionar las llamadas a `AuthSchmFn` con las llamadas a sus rutinas de llamada de retorno. Cuando llama a las rutinas `gwaget` o `gwaput`, `AuthSchmFn` debe pasar en el mismo valor `opaque_data` que se le ha pasado en la estructura `AuthReq`.

Tenga en cuenta que los esquemas de autenticación deben ser capaces de interactuar con todos los componentes del cortafuegos. Algunos de los componentes del cortafuegos pueden dar soporte a varios diálogos de solicitud/respuesta con el usuario final. Estos componentes se denominan componentes del cortafuegos interactivos. Algunos componentes del cortafuegos, debido a la naturaleza de sus protocolos, sólo pueden dar soporte a una única solicitud/respuesta. Estos componentes se denominan componentes de cortafuegos no interactivos.

El esquema de autenticación suministrado por el usuario debe ser capaz de modificar su comportamiento en base al componente del cortafuegos que lo llama, como indica el campo de componente de la estructura `AuthReq`. Los valores válidos para el campo de componente se definen en `authschm.h`. y son los siguientes:

<i>Tabla 23. Valores válidos para el campo de componente</i>		
Símbolo de componente de AuthSchm.h	Componente del cortafuegos	Interactivo/No interactivo
AUTHSCHM_UNKNOWN	Componente del cortafuegos nuevo o no reconocido	Se da por supuesto que es interactivo
AUTHSCHM_REMADMIN	Servidor de configuración	interactivo
AUTHSCHM_FTP	Proxy FTP	no interactivo
AUTHSCHM_TELNET	Proxy Telnet	interactivo
AUTHSCHM_HTTP	Proxy HTTP	interactivo
AUTHSCHM_SOCKS_PWD	Servidor Socks con autenticación de contraseña	no interactivo
AUTHSCHM_SOCKS_CRAM	Servidor Socks con autenticación CRAM	interactivo
AUTHSCHM_REMIPSEC	Servidor IPSEC de cliente remoto (Actualmente no disponible en Windows NT)	interactivo

Cuando AuthSchmFn ha completado su proceso, debe volver al emisor con uno de los códigos de retorno GWA definidos en authschm.h. Este código de retorno se utiliza para indicar si el usuario se ha autenticado correctamente y si se ha producido o no algún error durante el proceso:

Tabla 24. Códigos de retorno GWA	
Código de retorno	Significado
GWA_OK	No se han producido errores durante el proceso y el usuario se ha autenticado correctamente
GWA_DENY	No se han producido errores durante el proceso, pero el usuario no ha podido autenticarse
GWA_IOFAILURE	Se ha producido un error mientras se intentaba enviar las solicitudes al usuario o al intentar obtener una respuesta del usuario. Por lo general, este código suele devolverse cuando existen errores en las rutinas de llamada de retorno.
GWA_BUFFERTOOSMALL	La función AuthSchmFn no ha podido recuperar una respuesta el usuario porque no ha podido asignar un almacenamiento intermedio lo suficientemente grande para recibir la respuesta.
GWA_NOAUTHFN	Error - No relacionado con los esquemas de autenticación
GWA_FNNOTREG	Error - No relacionado con los esquemas de autenticación
GWA_RSVNAME	Error- La petición de autenticación contenía un nombre reservado que no puede utilizarse para este esquema de autenticación
GWA_BADNETTYPE	Error - No relacionado con los esquemas de autenticación
GWA_BADAPP	Error - No relacionado con los esquemas de autenticación
GWA_BADADDR	Error - La dirección suministrada en la petición de autenticación no era válida
GWA_MEMSHORTAGE	Error - La petición de autenticación no ha podido procesarse porque no ha sido posible asignarle memoria
GWA_USERDBFAIL	Error - No ha podido consultarse a una base de datos obligatoria
GWA_REGFAILED	Error - No relacionado con los esquemas de autenticación
GWA_AUTHERROR	Error - Condición de error específica del esquema de autenticación
GWA_INTERNAL	Error - Condición de error de tipo diverso en el esquema de autenticación

Cuando AuthSchmFn vuelve al cortafuegos, si el código de retorno es GWA_OK, el usuario se considera autenticado y recibe acceso al servicio solicitado. GWA_DENY se trata como una condición que no es un error, pero se deniega el acceso del usuario al servicio solicitado. Todos los demás códigos de retorno son condiciones de error y al usuario se le deniega el acceso al servicio solicitado.

Compilación y enlace al código fuente: Cuando se compila y enlaza el código fuente a una DLL, debe enlazar la DLL a gwauth4.dll utilizando la gwauth4.lib que se facilita en el directorio \bin\authsdk para poder resolver los nombres de puntos finales definidos en authschm.h. Además, es importante que AuthSchmFn no se exporte de la DLL. La creación de archivos de ejemplo para IBM VisualAge para C++ y Microsoft Visual C++ para se facilitan en el directorio \bin\authsdk.

Instalación de la DLL: Cuando la DLL se haya creado satisfactoriamente, cópiela en el directorio ROOTDIR\bin\authschm y vuelva a arrancar la máquina cortafuegos. El rearranque es necesario para que el cortafuegos intente cargar la DLL y registrar los esquemas de autenticación de la DLL.

Organización: Figura 1 en la página 56 muestra cómo se cargan los esquemas de autenticación y las llamadas a las funciones clave durante el proceso de petición de autenticación.

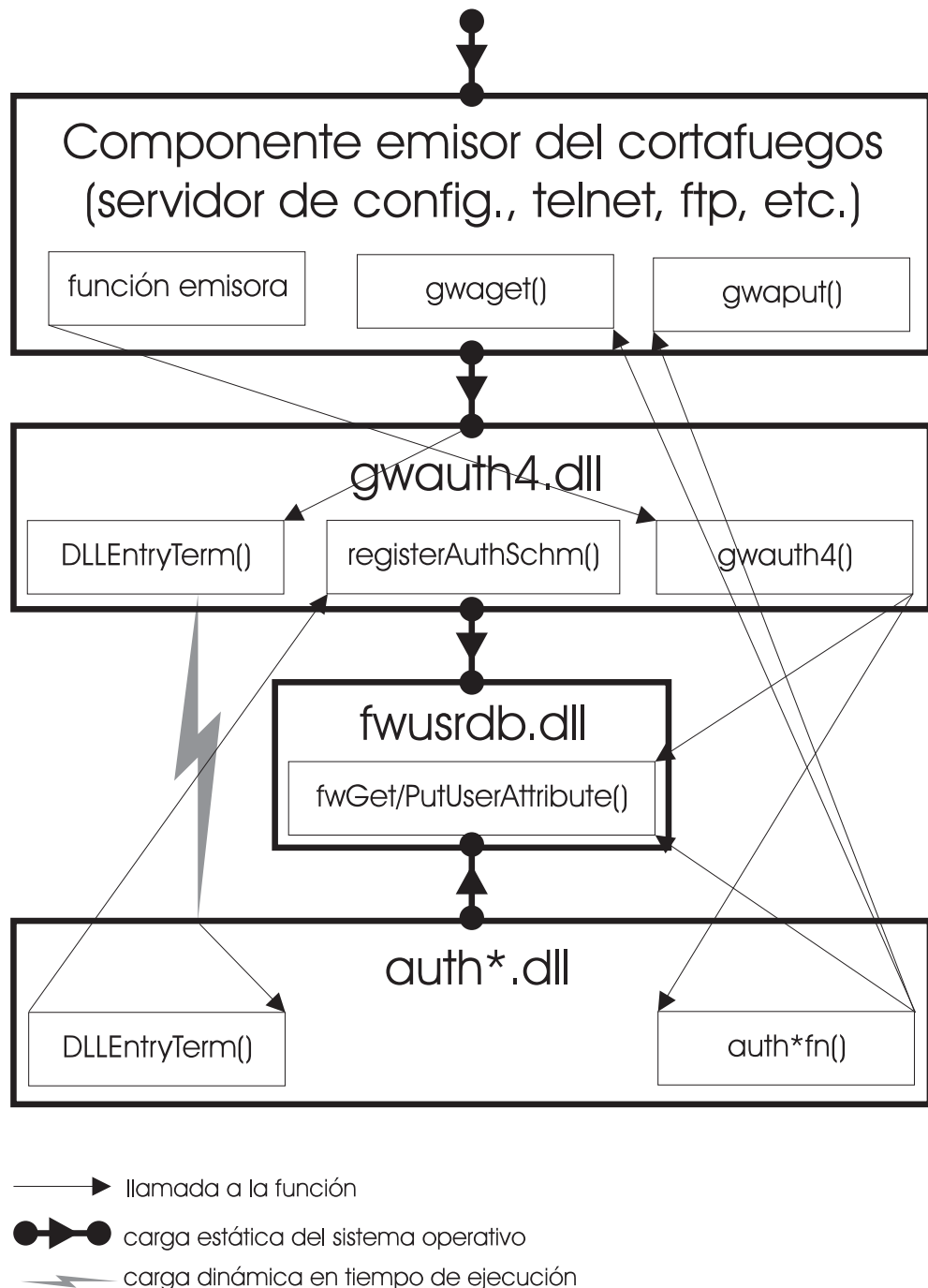


Figura 1. Inicialización y registro de DLL

Los componentes del cortafuegos que necesitan utilizar los servicios de autenticación se enlazan a una DLL del cortafuegos denominada gwauth4. Cuando se carga la dll gwauth4, se invoca su rutina DLLEntryTerm y se intenta la carga en tiempo de ejecución de todas las DLL de R00TDIR\bin\authschm. Si una DLL del esquema de autenticación no puede cargarse, no se considera un error para la carga de la dll gwauth4. La dll gwauth4 crea una serie con estos intentos de carga.

Cuando se ejecuta la rutina DLLEntryTerm de los esquemas de autenticación, éstos son los responsables del registro de los esquemas de autenticación con gwauth4.dll. Ello tiene lugar llamando a registerAuthSchm. La dll authschm nece-

sita llamar a `registerAuthSchm` una vez por cada esquema de autenticación al que la DLL da soporte. La estructura `AuthSchmInfo` que se pasa en la función `registerAuthSchm` asocia el nombre del esquema de autenticación como se ha almacenado en la base de datos de usuarios con el punto de entrada de la función `AuthSchmFn`. La función de registro realizará copias de la estructura que se le ha pasado, para que la dll `authschm` pueda volver a utilizar o modificar esta estructura en función de las necesidades. La DLL del esquema de autenticación también es responsable de liberar la estructura `AuthSchmInfo`.

La función `registerAuthSchm` es responsable de crear una lista enlazada que representa todos los esquemas de autenticación registrados. La rutina `DLLEntryTerm` de `gwauth4` inicializará el ancla o fijación de la lista hasta `NULL`. A continuación, cuando las DLL de `authschm` DLL llamen a la función `registerAuthSchm`, realizará lo siguiente:

1. Explorar la lista de esquemas de autenticación en busca de una entrada que tenga el mismo nombre que el nombre que se ha pasado. Si encuentra una, elimínala de la lista y suprima todo el almacenamiento que se le asocia.
2. Crear una estructura `AuthSchmEntry` basándose en la estructura `AuthSchmInfo` y añadirla a la lista de esquemas de autenticación.
3. Devolver al emisor una indicación que muestre si el registro ha resultado satisfactorio (`GWA_OK`) o no (`GWA_REGFAILED`).

Cuando `DLLEntryTerm` de `gwauth4` haya realizado una carga en tiempo de ejecución en cada una de las dll `authschm` y éstas hayan registrado sus esquemas de autenticación, la rutina `DLLEntryTerm` de `gwauth4` volverá al emisor. Llegado este punto, otros componentes pueden iniciar la petición de servicios de autenticación llamando a la función `gwauth4`.

Cuando `gwauth4.dll` se descargue, volverá a llamarse a la rutina `DLLEntryTerm` para el proceso de terminación. Cuando se llame para la terminación, esta rutina suprimirá todos los elementos `AuthSchmEntry` de `AuthSchmList` y el almacenamiento que se les asocia. Esto es así para que los esquemas de autenticación no tengan que encargarse de anular su registro del cortafuegos.

Proceso de petición de autenticación: Cuando un servicio del cortafuegos tiene que autenticar a un usuario, llama a las funciones de `gwauth4`. `gwauth4` toma información del componente que llama y consulta la base de datos de usuarios del cortafuegos para determinar el nombre del esquema de autenticación que debe utilizarse para procesar la petición.

Cuando `gwauth4` ha determinado el nombre del esquema de autenticación, explora su lista de esquemas de autenticación registrados en busca de un esquema que tenga el mismo nombre. Si encuentra un esquema registrado con el mismo nombre, crea una estructura `AuthReq` para representar la petición actual y llama al punto de entrada de la DLL del esquema de autenticación que se asocia al nombre.

La función `AuthSchmFn` que `gwauth4` ha llamado procesa la petición y llama a las llamadas de retorno `gwaget` y `gwput` según sea necesario para interactuar con el usuario final. Cuando completa su proceso, devuelve el control a `gwauth4` con el código de retorno correspondiente.

gwauth4 graba los registros de anotaciones correspondientes para documentar la petición de autenticación y, a continuación, vuelve al componente del cortafuegos que ha originado la petición, difundiendo el código de retorno que ha recibido de la DLL del Esquema de autenticación.

Capítulo 6. Utilización del Programa de utilidad de creación de archivo de claves (MKKF)

Una conexión de red SSL segura requiere que haya:

- Configurado el servidor de configuración para SSL
- Creado una clave para las comunicaciones seguras
- Recibido la designación de usuario raíz fiable en el servidor
- Ocultado la contraseña del archivo de claves

Utilice el MKKF para crear la clave de servidor inicial, el archivo de juego de claves y la petición de certificado. El MKKF también se utiliza para recibir el certificado inicial en un juego de claves y ocultar la contraseña del archivo de claves.

Creación de un archivo de claves

Cuando ejecute este programa de utilidad, deberá conectarse usando una cuenta del administrador de Windows NT.

1. Diríjase al directorio ROOTDIR\config e inicie el programa de utilidad de claves escribiendo:

```
c:\archivos de programa\IBM\Firewall\config > mkkf
```

```
Gestor de claves MKKF  
Copyright IBM Corp. 1996  
Reservados todos los derechos
```

2. Cree un nuevo archivo de juego de claves.

```
Menú Juego de claves  
Juego de claves actualmente seleccionado: (ninguno)
```

```
N - Crear un nuevo archivo de juego de claves  
O - Abrir archivo de juego de claves  
X - Salir
```

```
Escriba un mandato: n
```

Para crear un nuevo archivo de claves, escriba 'n', tal como se ha indicado.

Se le solicitará el nombre del archivo que ha de utilizarse para el archivo de juego de claves. Puede utilizar cualquier nombre de archivo, pero deberá finalizar con .kyr. Como valor por omisión, el cortafuegos busca un archivo denominado fwkey.kyr.

Escriba un nombre para el archivo de juego de claves o pulse INTRO para aceptar el valor por omisión, **fwkey.kyr**

El MKKF creará un nuevo archivo de claves y visualizará el menú del juego de claves. Observe que el archivo de claves aparecerá como el juego de claves actualmente seleccionado.

3. Cree una nueva clave y petición de certificado.

Menú Juego de claves

Juego de claves actualmente seleccionado: fwkey.kyr

- N - Crear un nuevo archivo de juego de claves
- O - Abrir archivo de juego de claves
- S - Guardar archivo de juego de claves
- A - Guardar juego de claves como otro archivo
- P - Establecer contraseña para archivo de juego de claves
- C - Crear archivo oculto para archivo de juego de claves
- R - Recibir un certificado en un archivo de juego de claves
- W - Trabajar con claves y certificados
- X - Salir

Escriba un mandato: **w**

Para ir al menú Clave, escriba 'w', tal como se ha indicado.

Menú Clave

Juego de claves actualmente seleccionado: fwkey.kyr

Entrada de clave seleccionada: (ninguna)

- L - Listar/Seleccionar una clave con la que trabajar
- C - Crear una nueva clave y petición de certificado
- I - Importar una clave de un Archivo de claves blindado
- X - Salir de este menú

Escriba un mandato: **c**

Para crear una nueva clave, escriba 'c', tal como se ha indicado.

Para que una clave pueda almacenarse en un archivo de claves, el archivo de claves debe protegerse por contraseña. El MKKF le solicitará que escriba la contraseña que ha de utilizarse para proteger el archivo de claves. La contraseña no se visualizará cuando la escriba. El MKKF también preguntará si la contraseña debe caducar. Escriba 'n', como se muestra a continuación:

Escriba

la contraseña que va a utilizar para el archivo de claves:

contraseña

Vuelva a escribir la contraseña para verificarla: **contraseña**

¿Debe caducar la contraseña?

Escriba S para sí o N para no:

n

La contraseña se ha establecido satisfactoriamente.

Pulse INTRO para continuar

El MKKF le preguntará el tipo de clave que ha de crearse.

Elija el Menú Tipo de certificado

- S - Formato de petición de certificado PEM (Private Enhanced Message)
- P - Formato de petición de certificado PKCS10
- C - Cancelar

Escriba un mandato: **s**

Para crear un Formato de petición de certificado PEM, escriba 's', tal como se ha indicado. El MKKF generará un certificado vacío:

Menú Componer certificado de servidor seguro

Información del certificado actual

Nombre de clave: (ninguno)

Tamaño de clave: 0

Nombre del servidor: (ninguno)

Organización: (ninguna)

Unidad de la organización: (ninguna)

Ciudad/Localidad: (ninguna)

Estado/Provincia: (ninguno)

Código postal: (ninguno)

País: (ninguno)

M - Modificar los campos del certificado

R - Preparado para crear petición de clave y certificado

C - Cancelar

Escriba un mandato: **m**

Para modificar el certificado vacío, escriba 'm'. Se le solicitará que escriba la información del nuevo certificado:

- Escriba el nombre que ha de utilizarse. Este nombre puede ser cualquier serie de caracteres y sólo lo utilizará el programa de utilidad MKKF:

Escriba el nombre a utilizar para la entrada de clave:

Clave del cortafuegos

- Especifique el tamaño de la clave. IBM Firewall sólo incluye la versión exportable del MKKF. El tamaño de clave máximo es 1024.

1: 508

2: 512

3: 768

4: 896

5: 1024

Escriba el número que corresponde al tamaño de clave deseado:

2

- Escriba el nombre del sistema principal TCP/IP calificado al completo el cortafuegos (por ejemplo, jupiter.raleigh.ibm.com):

Escriba

el nombre del dominio TCP/IP calificado al completo del servidor o pulse Intro para dejar el campo en blanco

jupiter.raleigh.ibm.com

- Escriba el nombre de la organización que ha de asociarse al certificado. (Por ejemplo, el nombre de la empresa):

Escriba el
Nombre de la organización para el certificado
o pulse INTRO para dejar el campo en blanco.

AAA Inc.

- Escriba el nombre de la unidad de la organización. (Por ejemplo, el nombre de un departamento):

Escriba el Nombre de la unidad de la organización para el certificado
o pulse INTRO para dejar el campo en blanco.

Productos para la seguridad de la red

- Escriba la ciudad en la que se utilizará el certificado:

Escriba
el Nombre de la localidad/ciudad para el certificado
o pulse INTRO para dejar el campo en blanco.

RTP

- Escriba un estado o provincia.

Nota: Debido a las especificaciones de los certificados, este campo debe tener un mínimo de tres caracteres, por lo tanto, no se pueden utilizar abreviaturas de dos letras para los estados.

Escriba
el Nombre del estado/provincial para el certificado
o pulse INTRO para dejar el campo en blanco.
Estado/Provincia deben tener, como mínimo, una longitud de tres caracteres.

N.C.

- Escriba el código postal que ha de asociarse al certificado. (Se trata del código postal que utilizamos para el correo tradicional):

Escriba el Código postal para el certificado
o pulse INTRO para dejar el campo en blanco.

27709

- Escriba un código de país de dos letras:

Escriba el Código
del país para el certificado
o pulse INTRO para dejar el campo en blanco.
El código del país debe tener exactamente una longitud de dos
caracteres.

US

Cuando el MKKF haya recopilado toda la información que ha especificado, se
visualizará el certificado:

Menú Componer certificado de servidor seguro

Información del certificado actual
Nombre de clave: Clave del cortafuegos
Tamaño de clave: 512
Nombre del servidor: jupiter.raleigh.ibm.com
Organización: AAA Inc.
Unidad de la organización: Productos para la seguridad de la red
Ciudad/Localidad: RTP
Estado/Provincia: N.C.
Código postal: 27709
País: US

M - Modificar los campos del certificado
R - Preparado para crear petición de clave y certificado
C - Cancelar

Escriba un mandato: **r**

Si existe algún error en la información del certificado, puede escribir 'm' para
realizar las correcciones. Si la información es correcta, escriba 'r' para crear la
nueva clave y su archivo de claves asociado.

El MKKF le preguntará el archivo en el que almacenar el certificado. Puede
utilizar cualquier nombre de archivo pero, como práctica a seguir, se aconseja
utilizar el mismo nombre que el utilizado para el archivo de claves y añadirle la
extensión .cert:

Escriba el archivo en el que almacenar la
petición de certificado:

fwkey.cert

Creando clave privada...

La clave privada se ha creado satisfactoriamente.

Creando petición de certificado...

La petición de certificado se ha creado satisfactoriamente

Añadiendo nueva clave a archivo de claves.

La nueva clave y la petición de certificado se han creado
satisfactoriamente.

Pulse INTRO para continuar

4. Especifique la clave que acaba de crearse como el valor por omisión.

Tras crearse la clave y el certificado, se visualizará el menú Clave. La clave
recientemente creada aparecerá como la Entrada de clave seleccionada:

Menú Clave

Juego de claves actualmente seleccionado: fwkey.kyr

Entrada de clave seleccionada: Clave del cortafuegos

- L - Listar/Seleccionar una clave con la que trabajar
- S - Mostrar información acerca de la clave seleccionada
- D - Suprimir la clave seleccionada
- C - Crear una nueva clave y petición de certificado
- I - Importar una clave de un Archivo de claves blindado
- E - Exportar la clave seleccionada a un Archivo de claves blindado
- F - Especificar la clave seleccionada como la clave por omisión para este juego de claves
- U - Quitar marca del estado de raíz fiable de la clave seleccionada
- R - Crear una petición de certificado para la clave seleccionada
- X - Salir de este menú

Escriba un mandato: **f**

Debe especificar la clave recientemente creada como la clave por omisión en el archivo de claves. Escriba 'f', tal como se indicaba en el ejemplo anterior. Se le solicitará que confirme la acción:

Menú Clave

Clave actualmente seleccionada: Clave del cortafuegos

¿Está seguro de que desea que esta clave sea el valor por omisión?

Escriba S para sí o N para no:

y

La clave ahora es la clave por omisión.

Pulse INTRO para continuar

Tras haber especificado la clave como el valor por omisión, se visualizará el

Menú Clave:

Menú clave

Juego de claves actualmente seleccionado: fwkey.kyr

Entrada de clave seleccionada: Clave del cortafuegos

- L - Listar/Seleccionar una clave con la que trabajar
- S - Mostrar información acerca de la clave seleccionada
- D - Suprimir la clave seleccionada
- C - Crear una nueva clave y petición de certificado
- I - Importar una clave de un Archivo de claves blindado
- E - Exportar la clave seleccionada a un Archivo de claves blindado
- F - Especificar la clave seleccionada como la clave por omisión para este juego de claves
- U - Quitar marca del estado de raíz fiable de la clave seleccionada
- R - Crear una petición de certificado para la clave seleccionada
- X - Salir de este menú

Escriba un mandato: **x**

Salga del menú Clave escribiendo una 'x'.

5. Reciba el certificado en el archivo de juego de claves.

Se visualizará el menú Juego de claves:

Menú Juego de claves
Juego de claves actualmente seleccionado: fwkey.kyr

N - Crear un nuevo archivo de juego de claves
O - Abrir archivo de juego de claves
S - Guardar archivo de juego de claves
A - Guardar juego de claves como otro archivo
P - Establecer contraseña para archivo de juego de claves
C - Crear archivo oculto para archivo de juego de claves
R - Recibir un certificado en un archivo de juego de claves
W - Trabajar con claves y certificados
X - Salir

Escriba un mandato: **r**

Nota: Puesto que el cortafuegos no utiliza la SSL en la autenticación, no será necesario que una autoridad certificadora firme el certificado.

Escriba el nombre del archivo o pulse INTRO
para Cert.txt.

fwkey.cert

Éste es un certificado que incluye firma. ¿Añadirlo al archivo de claves?
Escriba S para sí o N para no:

y

El certificado se ha añadido al juego de claves.
Pulse INTRO para continuar

6. Cree un archivo oculto para el archivo de claves.

Tras haberse añadido el certificado al juego de claves, se visualizará el Menú Juego de claves:

Menú Juego de claves
Juego de claves actualmente seleccionado: fwkey.kyr

N - Crear un nuevo archivo de juego de claves
O - Abrir archivo de juego de claves
S - Guardar archivo de juego de claves
A - Guardar juego de claves como otro archivo
P - Establecer contraseña para archivo de juego de claves
C - Crear archivo oculto para archivo de juego de claves
R - Recibir un certificado en un archivo de juego de claves
W - Trabajar con claves y certificados
X - Salir

Escriba un mandato: **c**

Debe crear un archivo oculto para el archivo de claves. Escriba 'c', tal como se indicaba en el ejemplo anterior. El MKKF utilizará el mismo nombre que el utilizado para el nombre del archivo de claves y añadirá la extensión .sth:

El archivo de contraseñas oculto se ha guardado en fwkey.sth
Pulse INTRO para continuar

Tras haberse creado el archivo oculto, se visualizará el Menú Juego de claves:

Menú Juego de claves

Juego de claves actualmente seleccionado: fwkey.kyr

N - Crear un nuevo archivo de juego de claves

O - Abrir archivo de juego de claves

S - Guardar archivo de juego de claves

A - Guardar juego de claves como otro archivo

P - Establecer contraseña para archivo de juego de claves

C - Crear archivo oculto para archivo de juego de claves

R - Recibir un certificado en un archivo de juego de claves

W - Trabajar con claves y certificados

X - Salir

Escriba un mandato: **x**

Ahora, el archivo de claves está preparado para utilizarse. Escriba una 'x', como se ha indicado anteriormente, para salir del MKKF y escriba una 's' para guardar los cambios en el archivo de claves, tal como se ha explicado:

El archivo de juego de claves se ha cambiado. ¿Guardar?

Escriba S para sí o N para no:

y

El juego de claves se ha guardado en fwkey.kyr

Pulse INTRO para continuar

#

7. Actualización del archivo de configuración.

Después de crear el archivo de claves, debe especificar el nombre del archivo de claves en el archivo de parámetros del servidor de configuración utilizando el mandato fwcfgsrv.

Si está utilizando el cifrado SSL para el servidor de configuración, puede que también tenga que definir la opción encryption=ssl utilizando el mandato fwcfgsrv.

Tras haber utilizado el mandato fwcfgsrv, detenga y vuelva a arrancar el servicio del servidor.

Capítulo 7. Resolución de problemas y comprobación

En este capítulo se explica cómo resolver algunos de los problemas más comunes que se detectan al definir y configurar IBM Firewall.

Si está experimentando problemas, en primer lugar debe crear un registro del cortafuegos, con prioridad de depuración, para que la información que se envía a los registros sea más completa. Consulte el apartado “Gestión de Archivos de Registro” en la página 6 para obtener más información.

Instalación y puesta a punto

Soporte de filtros anómalo

Explicación del problema Recibirá estos mensajes de error.

La verificación del soporte de filtros ha resultado anómala. La llamada para la creación del socket ha resultado anómala.
Un archivo o directorio del nombre de la vía de acceso no existe.

Este problema se debe a que no se ha arrancado el cortafuegos tras realizar la instalación.

Acción recomendada Vuelva a arrancar el cortafuegos e intente nuevamente el procedimiento.

Problemas de direccionamiento

IBM Firewall proporciona una función en el recuadro de diálogo **Política de seguridad** titulada *Probar direccionamiento IP*, que puede resultar de gran utilidad para depurar problemas de direccionamiento. Habilite este cuadro de selección, active la configuración Conexión y habilite Registro de normas de conexión. A continuación, examine el registro del cortafuegos para ver información detallada acerca de todos los paquetes que fluyen a través del cortafuegos.

Realice estas tareas utilizando primero las direcciones IP y, a continuación, utilizando los nombres de los sistemas principales. Si el tráfico se direcciona correctamente utilizando las direcciones pero no utilizando los nombres, consulte el apartado “Problemas DNS” en la página 69 para obtener más información.

No puede ejecutarse ping para los sistemas principales desde el cortafuegos

Explicación del problema La interfaz de la red no se ha configurado correctamente.

Acción recomendada Consulte la documentación del sistema operativo.

Explicación del problema La conexión de la red no segura no se ha configurado correctamente.

Acción recomendada Póngase en contacto con el suministrador de servicio para obtener ayuda.

Explicación del problema Si la red segura se ha aislado detrás de un direccionador, el cortafuegos debe tener una ruta estática a ese direccionador. Utilice `netstat -rn` para verificar el direccionamiento estático:

```
netstat -rn
```

La salida debe ser la siguiente para Protocol Family 2:

Destino por omisión	Pasarela nrr.nrr.nrr.nrr	Distintivos UG
nnn.nnn.nnn	nnn.nnn.nnn.nnn	U
sss.sss.sss	sss.sss.sss.sss	U
ss1.ss1.ss1	srr.srr.srr.srr	UG
127	127.0.0.1	U

Figura 2. Salida de ejemplo de netstat -rn.

nrr.nrr.nrr.nrr representa el direccionador a Internet y es la ruta por omisión. La ruta por omisión es una ruta estática (Distintivo=UG).

nnn.nnn.nnn representa el dominio no seguro. Se trata de una ruta de interfaz (Distintivo=U).

nnn.nnn.nnn.nnn representa la interfaz no segura.

sss.sss.sss representa el dominio seguro. Se trata de una ruta de interfaz (Distintivo=U).

sss.sss.sss.sss representa la interfaz segura.

ss1.ss1.ss1 representa un subdominio en la ubicación segura de la red y **srr.srr.srr.srr** representa la ruta a ese subdominio. Se trata de una ruta estática (Distintivo=UG).

127.0.0.1 es el bucle de retorno o sistema principal local. Se trata de una ruta de interfaz (Distintivo=U).

Debe disponer de una ruta de interfaz para cada interfaz y la ruta por omisión debe señalar al direccionador de la ubicación no segura del cortafuegos.

Acción recomendada Añada una ruta estática al direccionador. Póngase en contacto con el administrador de los direccionadores. Utilice el mandato `route add`.

Explicación del problema Puede que la máscara de subred de la interfaz segura o el sistema principal con el que está intentando establecer contacto sean incorrectos.

Acción recomendada Utilice los programas de utilidad de configuración del cliente para corregir los valores de la máscara.

No puede ejecutarse ping para los sistemas principales no seguros desde sistemas principales seguros (o viceversa)

Explicación del problema Cada direccionador contiguo al cortafuegos debe tener una ruta estática que identifique al cortafuegos como pasarela para las redes de destino externas al cortafuegos.

Acción recomendada Póngase en contacto con el administrador del direccionador.

Explicación del problema Si la red segura utiliza direcciones que no se han registrado y no pueden direccionarse en la red segura, incluidas las direcciones privadas tal como especifica la RFC 1597, los paquetes no volverán a direccionarse al remitente.

Acción recomendada Utilice un cliente con una dirección registrada.

Problemas DNS

El DNS del cortafuegos resuelve los nombres consultando al servidor de nombres seguro. El servidor de nombres seguro resuelve todos los nombres de la red segura. El servidor de nombres seguro reenvía las peticiones de los nombres no seguros al servidor de nombres del cortafuegos. El servidor de nombres del cortafuegos consulta al servidor de nombres no seguro para solucionar la petición.

Los problemas DNS pueden tener un impacto en otras áreas de funcionamiento del cortafuegos. Lo recomendado es comprobar el DNS, incluso si el problema no está claramente relacionado con el DNS.

A continuación se muestran algunos ejemplos con los pasos que debe seguir para este método utilizando el programa de utilidad `nslookup` para aislar el problema. En estos ejemplos, se utilizan los valores siguientes:

www.ibm.com representa un nombre de sistema principal arbitrario en la red no segura

nns.nns.nns.nns representa la dirección del servidor de nombres no seguro

sns.sns.sns.sns representa la dirección del servidor de nombres seguro

host.secure.company.com representa el nombre de un sistema principal arbitrario que se encuentra en el interior de la red segura

127.0.0.1 representa la dirección del bucle de retorno del cortafuegos.

Estos valores pueden obtenerse en el recuadro de diálogo **Servicios de denominación de dominios** en el Cliente de configuración. Para trabajar con estos ejercicios necesitará estos valores.

Nota: El mandato `nslookup` necesita un punto adicional a continuación del nombre del sistema principal para evitar que `nslookup` añada su nombre de dominio seguro.

DNS todavía no se ha configurado

Explicación del problema Todavía no ha configurado los recursos DNS del cortafuegos.

Acción recomendada Complete el recuadro de diálogo **Servicios de denominación de dominios**.

Las consultas DNS resultan anómalas o se excede el tiempo de espera

Explicación del problema El control de tráfico del cortafuegos no permite el flujo de los paquetes DNS.

Acción recomendada Vaya al recuadro de diálogo **Política de seguridad**, active el recuadro de selección *Permitir consultas DNS* y vuelva a activar el control del tráfico.

nslookup www.ibm.com. nns.nns.nns.nns es anómala

Explicación del problema El servidor de nombres no seguro no utiliza la dirección indicada o no se ha configurado correctamente.

Acción recomendada Póngase en contacto con el proveedor de servicio DNS para obtener una dirección de servidor de nombres válida.

nslookup www.ibm.com. 127.0.0.1 es anómala

Explicación del problema Puede que el Servicio DNS de Microsoft no esté en ejecución. Diríjase al gestor de control de servicios para determinar si está ejecutándose.

Acción recomendada Utilice el gestor de control de servicios para iniciar el DNS.

nslookup host.secure.company.com. sns.sns.sns.sns resulta anómalo

Explicación del problema El servidor de nombres seguro está desconectado.

Acción recomendada Vuelva a arrancar el servidor de nombres.

nslookup www.ibm.com. sns.sns.sns.sns resulta anómalo

Explicación del problema El servidor de nombre seguro no se ha configurado correctamente para interactuar con IBM Firewall.

Acción recomendada Consulte el manual *IBM eNetwork Firewall - Guía del usuario* para conocer los requisitos de la configuración.

Cliente de configuración

El servidor no responde

Explicación del problema El cliente de configuración y el servidor de configuración utilizan idiomas distintos.

Acción recomendada En el panel de conexión del cliente de configuración, seleccione el idioma en el que se ha instalado el cortafuegos.

Explicación del problema Puede que el cifrado SSL no se haya configurado correctamente.

Acción recomendada Asegúrese de haber seleccionado SSL en el panel de conexión del cliente. Detenga y vuelva a arrancar el servidor de configuración del cortafuegos utilizando el gestor de control de servicios.

Explicación del problema Puede que el servidor de configuración del cortafuegos esté inhabilitado.

Acción recomendada Asegúrese de que el servidor de configuración del cortafuegos esté ejecutándose.

Explicación del problema Puede que el servidor de configuración del cortafuegos esté supervisando una puerta no estándar.

Acción recomendada Examine `c:\winnt\system32\drivers\etc\services` y asegúrese de que contiene la línea `ibmfwrccs 1014/tcp`. Si desea utilizar el servidor en una puerta distinta, edite `ibmfwrccs 1014/tcp` y asegúrese de especificar la nueva puerta en el panel de conexión del cliente. Detenga y vuelva a arrancar el servidor de configuración utilizando el gestor de control de servicios.

Explicación del problema Puede que el control del tráfico del cortafuegos no permita las comunicaciones que proceden de y se dirigen al Servidor de configuración. Esto sólo afecta a los Clientes de configuración que se ejecutan en un sistema principal remoto.

Acción recomendada Codifique una conexión entre la máquina que ejecuta el Cliente de configuración y el cortafuegos. El Cliente de configuración debe ser el origen de la conexión y el cortafuegos el destino. Vuelva a generar los cambios y actívelos. Consulte el manual *IBM eNetwork Firewall - Guía del usuario* para obtener más información.

Explicación del problema Puede que el Servidor de configuración no se haya configurado para permitir conexiones desde un sistema principal remoto.

Acción recomendada Utilice el mandato `fwcfgsrv` para verificar que el parámetro `localonly` se ha establecido en "no".

No puede conectarse al Servidor de configuración

Explicación del problema Cada nombre de usuario autenticado en el cortafuegos está configurado para utilizar cualquiera de los distintos métodos de autenticación existentes. Denegar todo se utiliza para que un usuario no pueda utilizar un servicio determinado.

Acción recomendada Examine los campos Administración segura y Administración no segura del nombre de usuario que está utilizándose. Estos campos sólo son válidos para los Administradores, no para los usuarios del cortafuegos.

Control del tráfico

Los cambios realizados en las Conexiones no entran en vigor

Explicación del problema Los cambios que se realizan en cualquiera de los componentes del Control del tráfico no entran en vigor hasta que se activan. Esto incluye el recuadro de diálogo **Política de seguridad** de Administración del sistema.

Acción recomendada Utilice el recuadro de diálogo **Activación de la conexión** para volver a generar y activar la configuración.

Servidores proxy

No se ha transmitido ningún dato

Explicación del problema Los servicios del proxy del cortafuegos no se inician hasta rearrancar la máquina tras la instalación.

Acción recomendada Vuelva a arrancar la máquina.

Explicación del problema El Control del tráfico del cortafuegos debe configurarse para permitir el flujo de paquetes hacia y desde el proceso proxy, no directamente a través del cortafuegos.

Acción recomendada Configure ambas partes de la conexión del proxy como se describe en el manual *IBM eNetwork Firewall - Guía del usuario*.

Utilice los servicios predefinidos siempre que sea posible, en especial con el tráfico FTP.

No puede establecerse conexión con el sistema principal deseado

Explicación del problema Si los datos fluyen hacia y desde el proxy, pero no puede establecerse contacto con el sistema principal, puede que el cliente no resuelva correctamente los nombres de los sistemas principales.

Acción recomendada Asegúrese de que *Permitir consultas DNS* esté habilitado en el recuadro de diálogo **Política de seguridad** y que la configuración de la conexión esté activada. Consulte el apartado “Problemas DNS” en la página 69 para obtener más información.

Explicación del problema Cada nombre de usuario que se autentifica en el cortafuegos mediante cualquiera de los servicios del cortafuegos puede configurarse para utilizar cualquiera de los distintos métodos de autenticación. Denegar todo se utiliza para que un usuario no pueda utilizar un proxy determinado.

Acción recomendada Examine los valores de autenticación de la cuenta en el recuadro de diálogo **Usuarios** del Cliente de configuración.

Servicios de autenticación

Una cuenta de administrador de Windows NT no puede autenticarse

Explicación del problema Los atributos del cortafuegos para una cuenta de administrador de Windows NT se almacenan en la base de datos de usuarios del cortafuegos en fwdadm.

Acción recomendada Verifique que fwdadm tenga el método de autenticación correcto que se ha establecido para el servicio que está intentando utilizar.

El usuario del proxy del cortafuegos no puede autenticarse

Explicación del problema Si el usuario del proxy del cortafuegos no se ha definido en la base de datos de usuarios del cortafuegos, para definir los atributos del usuario se utiliza el nombre fwdfuser.

Acción recomendada Verifique que el método de autenticación de fwdfuser se haya definido correctamente para el servicio al que el usuario intenta acceder.

Conversión de dirección de red

La conexión NAT no funciona

Explicación del problema Ha configurado y activado la NAT, pero la conexión no funciona.

Acción recomendada Existe un problema en las tablas de direccionamiento o un problema de configuración de NAT.

Cómo establecer una ruta para los paquetes NAT

Explicación del problema No existe ninguna ruta establecida para los paquetes NAT.

Acción recomendada Añada una ruta estática en el direccionador que aparece para el cortafuegos con la dirección o direcciones NAT de destino y la pasarela del cortafuegos.

Herramientas de ayuda para la depuración disponibles con la NAT

Explicación del problema ¿De qué herramientas de ayuda para la depuración dispone la NAT?

Acción recomendada Registro NAT, que le permite realizar el rastreo de la gestión de las direcciones dinámicas registradas.

Recursos de registro

Los cambios en el recurso de registro no entran en vigor en el servidor

Explicación del problema Cuando se suprime o cambia un recurso de registro, parece funcionar en la GUI, pero no entra en vigor en el servidor.

Acción recomendada Vuelva a arrancar el sistema.

Programas de utilidad de informes

Se ha producido un error al acceder al archivo:

Explicación del problema El error anterior puede verse tras utilizar cualquiera de los mandatos siguientes:

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

Acción recomendada Especifique nombres de archivos calificados al completo correctos para los archivos .ddl, .dat o .dml.

Se han producido errores al importar datos a la base de datos.

Explicación del problema El archivo import.out que se obtiene después de emitir un mandato db2 -vf fwimport.dat>import.out contiene mensajes que indican que una de las importaciones resultó anómala o sólo fue parcialmente satisfactoria.

Acción recomendada Compruebe el archivo .msg correspondiente a la sentencia de importación para la que se ha notificado el problema. Dicho archivo proporcionará información más detallada sobre el problema. Busque los registros relacionados en el archivo .tbl correspondiente para ver los datos de entrada y determine dónde está el error. Por ejemplo, ¿es demasiado largo para su columna de destino de la base de datos? ¿Es el tipo de datos adecuado para el tipo de columna de destino? Si el aspecto de los datos de entrada no es satisfactorio, tal vez debería localizar el registro del archivo de anotaciones original para asegurarse de que fwlogtbl generó el registro del archivo .tbl correctamente.

Si no puede solucionar este problema guarde el archivo import.out, el archivo .msg, el archivo .tbl asociado y el archivo de anotaciones original antes de ponerse en contacto con el Centro de servicio de IBM.

Apéndice A. Mensajes

Este apéndice contiene los mensajes para IBM Firewall para AIX, mensajes para IBM Firewall para NT y mensajes comunes a ambos cortafuegos. En este apéndice también se proporciona la siguiente información acerca de los mensajes de IBM Firewall :

- Formato de los mensajes
- Niveles de gravedad de los mensajes
- Mensajes y sus explicaciones

Si ha consultado un mensaje y su explicación y necesita obtener más información, consulte Capítulo 7, “Resolución de problemas y comprobación” en la página 67.

Código de los mensajes

ICA	Los 3 primeros bytes fijos.
xxxx	Un número que se encuentra en el rango 0000 a 9999.
a	Un indicador de gravedad. Los mensajes se clasifican por nivel de gravedad. <ul style="list-style-type: none"> • i – informativo • w– advertencia • e – error • s – grave

Los números 0000 – 9999 también se clasifican en las categorías siguientes:

- 0000 – 0999 Alarma de intrusión
- 1000 – 1999 Filtros
- 2000 – 2999 Proxy
- 3000 – 3999 Socks
- 4000 – 4999 Buscapersonas
- 5000 – 8999 Disponibilidad
- 9000 – 9999 General/Otros

Mensajes

ICA0001 ALERTA - %1\$s anomalías de autenticación.

Explicación: Se han satisfecho las condiciones de umbral para las anomalías de autenticación.

ICA0002 ALERTA - %1\$s anomalías de autenticación para el usuario %2\$s.

Explicación: Se han satisfecho las condiciones de umbral para la detección de un mensaje de registro específico.

ICA0003 ALERTA - %1\$s anomalías de autenticación del sistema principal %2\$s.

Explicación: Se han satisfecho las condiciones de umbral para las anomalías de autenticación de cualquier sistema principal específico.

ICA0004 ALERTA - Código %1\$s con %2\$s entradas de registros.

Explicación: Se han satisfecho las condiciones de umbral para la detección de un mensaje de registro específico.

ICA0005 Supervisor de registro - memoria insuficiente.

Explicación: El proceso no dispone de suficiente memoria.

ICA0006 Supervisor de registro - anomalía al acceder al archivo de servicios: %1\$s

Explicación: No ha podido encontrarse la entrada para fwlogmond en /etc/services.

ICA0007 Supervisor de registro - creación del socket anómala: %1\$s

Explicación: No ha podido abrirse el socket - consulte el mensaje de error.

ICA0008 Supervisor de registro - bind() anómalo: %1\$s

Explicación: No ha podido ejecutarse bind para el socket - consulte el mensaje de error.

ICA0009 No ha podido abrirse el archivo de definición de umbral: %1\$s

Explicación: Problema al acceder al archivo de definición de umbral - consulte el mensaje de error.

ICA0010 Supervisor de registro - error de lectura muy grave: %1\$s

Explicación: Problema al leer del socket - consulte el mensaje de error.

ICA0011 No ha podido obtenerse el estado del archivo de definición de umbral: %1\$s

Explicación: Problema al acceder al archivo de definición de umbral - consulte el mensaje de error.

ICA0012 El daemon del supervisor de registro está concluyendo.

Explicación: El daemon está finalizando de forma anómala o recibiendo una señal de terminación. Encontrará más detalles en los mensaje de registro anteriores.

ICA0013 El supervisor de registro ha recibido una señal de terminación.

Explicación: El daemon ha recibido una señal de terminación y va a concluir.

ICA0014 Iniciando daemon del supervisor de registro.

Explicación: El daemon se ha iniciado.

ICA0015 No ha podido crearse el daemon para el supervisor de registro: %1\$s

Explicación: La creación del daemon ha resultado anómala - consulte el mensaje de error.

ICA0016 No ha podido abrirse %1\$s - puede que el daemon ya esté activo.

Explicación: El daemon no ha podido abrir el archivo de ID de proceso.

ICA0017 No ha podido grabarse el ID de proceso (%1\$s) en %2\$s.

Explicación: El daemon no ha podido grabar el ID de proceso en el archivo.

ICA0018 Supervisor de registro - lectura vacía.

Explicación: Se ha recibido un paquete sin datos - se descarta.

ICA0019 Supervisor de registro - lectura insuficiente. Se descarta el código.

Explicación: El paquete recibido no tiene datos suficientes - se descarta.

ICA0020 Supervisor de registro - código ICA mal formateado.

Explicación: Se ha recibido un paquete con datos mal formateados - se descarta.

ICA0021 Supervisor de registro - datos de autenticación mal formateados.

Explicación: Se ha recibido un paquete con datos mal formateados - se descarta.

ICA0022 Sintaxis no válida en archivo de definición de umbral (%1\$s).

Explicación: La entrada indicada en el archivo de umbral es sintácticamente incorrecto.

ICA0023 No ha podido abrirse el archivo fwmail.conf.

Explicación: La apertura del archivo fwmail.conf ha resultado anómala o el archivo está vacío

ICA0024 No puede conectarse con el Servidor SMTP.

Explicación: El Servidor SMTP está ocupado o rechaza la conexión

ICA0025 El envío electrónico del mensaje de alerta ha resultado anómalo.

Explicación: No ha podido enviarse electrónicamente el mensaje de alerta del supervisor de registro a la dirección especificada.

ICA0051 Los días a conservar en el archivo de registro, %1\$s, debe ser un valor entero corto sin signo.

Explicación: Los días a conservar en el archivo de registro debe ser un entero válido.

ICA0052 Los días a conservar en los archivadores, %1\$s, debe ser un valor entero corto sin signo.

Explicación: Los días a conservar en los archivadores debe ser un entero válido.

ICA0053 No se permiten varias entradas para el archivo de registro, %1\$s, en logmgmt.cfg.

Explicación: No se permiten varias entradas para un archivo de registro en logmgmt.cfg.

ICA0054 No se puede abrir el archivo %1\$s.

Explicación: No ha podido abrirse el archivo logmgmt.cfg.

ICA0055 No existe ninguna entrada válida en el archivo logmgmt.cfg.

Explicación: No existe ninguna entrada válida en el archivo logmgmt.cfg.

ICA0056 El mensaje de registro,"%1\$s", no es válido

Explicación: El mensaje del registro no es válido

ICA1001 No ha podido crearse el archivo con nuestro ID de proceso

Explicación: El daemon del registro de filtros ha detectado un error al grabar el archivo fwlogd.pid.

Respuesta del Usuario: Compruebe el sistema de archivos en que reside el directorio /etc/security. Existe una posible condición de insuficiencia de espacio.

ICA1002 Las comunicaciones con el programa cfgfilt no son posibles

Explicación: Debido a que no se ha creado el archivo fwlogd.pid, las comunicaciones entre el daemon fwlogd y la aplicación cfgfilt (necesaria para el control de filtros) no es posible.

Respuesta del Usuario: Compruebe el sistema de archivos en que reside el directorio /etc/security. Existe una posible condición de insuficiencia de espacio.

ICA1003 Continuando con la inicialización del daemon de registro

Explicación: El daemon fwlogd continuará el proceso de arranque.

ICA1004 El daemon del registro de filtros %1\$s (nivel %2\$s.%3\$s) se ha inicializado a las %4\$s del %5\$s

Explicación: Se ha iniciado el daemon de registro del paquete IP. Cuando/si el registro de paquetes está habilitado, el daemon fwlogd grabará los registros necesarios en el archivo syslog, local4.

ICA1005 Se ha suprimido el registro de mensaje(s) del paquete %1\$s debido a un desbordamiento del almacenamiento intermedio

Explicación: Se ha desbordado el almacenamiento intermedio del registro de filtros del daemon fwlogd. No puede registrarse un paquete para la norma de filtro especificada.

Respuesta del Usuario: Compruebe el registro. Puede que el cortafuegos esté bajo un ataque de denegación de servicio o puede que esté registrando mensajes que no se necesitan. Por ejemplo, los mensajes de difusión general deben tener una norma de denegación, con el control de registro establecido en no (l=n), para impedir que se llene el registro.

ICA1006 Error muy grave de fwlogd - %1\$s: %2\$s

Explicación: El servidor fwlogd no ha podido realizar satisfactoriamente la función indicada, el daemon ha finalizado.

Respuesta del Usuario: Corrija el problema del sistema que se indica y vuelva a arrancar fwlogd.

ICA1007 No ha podido ejecutarse fork para el proceso inferior: %1\$s

Explicación: Durante el arranque del daemon de registro de filtros, se ha detectado el error del sistema indicado.

Respuesta del Usuario: Basándose en el error que se visualiza, realice la acción correctiva.

ICA1008 Retorno de error en la rutina setpgrp: %1\$s

Explicación: Durante el arranque del daemon de registro de filtros, se ha detectado el error del sistema indicado.

ICA1009 No ha podido ejecutarse fork para el segundo proceso inferior: %1\$s

Explicación: Durante el arranque del daemon de registro de filtros, se ha detectado el error del sistema indicado.

ICA1010 Este daemon debe ejecutarse con autorización de raíz

Explicación: El daemon del registro de filtros debe arrancarse con autorización de usuario raíz.

Respuesta del Usuario: Vuelva a arrancarlo con autorización de usuario raíz.

ICA1011 La llamada de sysconfig para consultar la extensión kernel %1\$s ha resultado anómala: %2\$s

Explicación: Durante el arranque del daemon de registro de filtros, se ha detectado el error del sistema indicado.

ICA1012 La extensión kernel de AIX %1\$s no se ha cargado -- no puede continuarse

Explicación: El controlador de dispositivos **netinet** no contiene soporte de filtros.

Respuesta del Usuario: Instale el código del cortafuegos. En teoría, el código se ha instalado, pero no se ha realizado el *rearranque*.

ICA1013 La llamada de creación de socket ha resultado anómala: %1\$s

Explicación: Durante el arranque del daemon de registro de filtros, se ha detectado el error del sistema indicado.

ICA1014 El controlador de dispositivos netinet de AIX no se encuentra en el nivel necesario

Explicación: El controlador de dispositivos **netinet** y el daemon **fwlogd** no tienen el mismo nivel.

Respuesta del Usuario: Solucione el conflicto; es posible que sea necesario rearrancar tras instalar el nuevo nivel del cortafuegos.

ICA1015 Error en llamada ioctl() (SIOCGFWLOG): %1\$s

Explicación: Durante el arranque del daemon de registro de filtros, se ha detectado el error del sistema indicado.

ICA1016 No puede obtenerse la cola de registros diferidos actual

Explicación: Existe información adicional que se asocia al mensaje de registro inmediatamente anterior.

ICA1017 Retorno de error de la llamada SIOCGFWLOG ioctl()

Explicación: Durante el arranque del daemon de registro de filtros, se ha detectado el error del sistema indicado.

ICA1018 Error muy grave de fwlogd - %1\$s: %2\$s

Explicación: El servidor **fwlogd** no ha podido realizar satisfactoriamente la función indicada, el daemon ha finalizado.

Respuesta del Usuario: Corrija el problema del sistema que se indica y vuelva a arrancar **fwlogd**.

ICA1019 Salida errónea no esperada con rc %1\$s

Explicación: Durante el arranque del daemon de registro de filtros, se ha detectado el error del sistema indicado.

ICA1020 Error muy grave de fwlogd - %1\$s: código de retorno = 0x%2\$s

Explicación: El servidor fwlogd no ha podido realizar satisfactoriamente la función indicada, el daemon ha finalizado.

Respuesta del Usuario: Corrija el problema del sistema que se indica y vuelva a arrancar fwlogd.

ICA1021 Error en %1\$s abierto: %2\$s

Explicación: El controlador de dispositivos indicado no se ha instalado.

Respuesta del Usuario: Si se ha instalado el código del cortafuegos, compruebe el archivo /tmp/rc/net.out para verificar si existen posibles mensajes de error.

ICA1022 La verificación del soporte de filtros no ha resultado satisfactoria

Explicación: Debido a un error registrado con anterioridad a este mensaje, no puede verificarse el soporte de filtros.

ICA1023 Error en llamada ioctl() (SIOCGFWLVL): %1\$s

Explicación: Durante el arranque del daemon de registro de filtros, se ha detectado el error del sistema indicado.

Respuesta del Usuario: Efectúe una de las acciones siguientes:

- Para AIX: :p.Verifique si se ha instalado en nivel correcto del controlador de dispositivos netinet del cortafuegos y si la máquina se ha rearrancado tras realizarse la instalación.
- Para OS/390: :p.Verifique si se ha instalado en nivel correcto de TCP/IP y si se ha iniciado con la sentencia de configuración **IPCONFIG FIREWALL**.

ICA1024 Error al grabar el archivo %1\$s: %2\$s

Explicación: Debido al n de error del sistema indicado, fwlog no ha podido grabar el archivo especificado.

Respuesta del Usuario: Corrija el problema que se indica y vuelva a arrancar el daemon del registro de filtros.

ICA1032 Normas de filtro actualizadas a las %1\$s del %2\$s

Explicación: Las normas de filtrado del paquete IP se han actualizado.

ICA1033 El soporte de filtros (nivel %1\$s.%2\$s) ha sido inicializado a las %3\$s del %4\$s

Explicación: El soporte de filtros del cortafuegos se ha inicializado.

ICA1034 El soporte de filtros se ha desactivado a las %1\$s del %2\$s

Explicación: El filtrado de paquetes IP ahora está utilizando las normas de filtro por omisión en lugar de las que se han definido en el archivo /etc/security/fwfilters.cfg.

ICA1035 El estado del registro de paquetes se ha establecido en %1\$s a las %2\$s del %3\$s

Explicación: El estado del registro de paquetes ha cambiado. El mensaje indica el estado actual y la indicación de la hora.

ICA1036 #:n_norma R: dirección_tipo_norma: interfaz
s: direc_orig d: direc_destino p: protocolo código: puerta_orig/tipo_icmp código:
puerta_dest/código_icmp r: direccionado/local a: protegido/no_protegido f: sí/no
T: id_túnel e: C/D/n l: longitud_paquete

Explicación: Anotación del registro que indica un paquete IP procesado y la norma de filtro correspondiente con la que coincidía. Para que se escriba esta anotación, la norma de registro coincidente debe tener el control de registro fijado a sí. Si el paquete IP que coincidía con esta norma es un fragmento, la información de puertas/icmp tipo/código aparece para el paquete de cabecera pero se muestra como cero para los paquetes que no sean el paquete de cabecera.

ICA1037 #:n norma acción direc_orig máscara_orig direc_dest máscara_dest protocolo
valor op_lógica valor op_lógica tipo_interfaz direccionamiento dirección=
control_registro f=control_fragmentot= ID_túnel alg_cifr alg_aut

Explicación: Cuando se actualizan las normas de filtro, las normas activadas se graban en el registro. Este mensaje de registro describe una de las normas activadas.

ICA1038 El intérprete de claves de sesión se ha iniciado, utilizando la puerta de socket de sesión: %1\$s y la puerta de socket maestro: %2\$s

Explicación: El túnel de cifrado se ha iniciado utilizando los números de puertas UDP especificados, tal como se ha definido en /etc/services.

ICA1039 La política está (re)definiéndose como:

Explicación: La antememoria de política está (re)definiéndose utilizando el archivo /etc/security/fwppolicy. Las líneas siguientes muestran la nueva antememoria de política.

ICA1040 >Sentencia de política: %1\$s

Explicación: La línea registrada se ha leído del archivo /etc/security/fwppolicy.

ICA1041 Se ha suprimido la especificación de contexto para el túnel: %1\$s

Explicación: El contexto de túnel, para el ID especificado, ya no está operativo.

ICA1042 Se define la especificación(ones) de contexto de túnel siguiente(s):

Explicación: Las especificaciones de contexto de túnel están definiéndose, tal como se indica en los registros de anotaciones siguientes.

ICA1043 >ID_túnel: %1\$s, direc_orig: %2\$s, direc_destino: %3\$s, cifrado: %4\$s

Explicación: El mensaje lista los atributos específicos del contexto de túnel activado.

ICA1044 Advertencia del contador del sistema principal: Límite IP(%1\$s) excedido

Explicación: Existen demasiados sistemas principales seguros que intentan conectarse con la máquina cortafuegos

Acción del Sistema: pasar las conexiones

ICA1045 Límite TCP excedido: %1\$s(%2\$s)->%3\$s(%4\$s) rechazadas

Explicación: Existen demasiadas sesiones TCP a través de la máquina cortafuegos

Acción del Sistema: rechazar las conexiones

ICA1046 Límite UDP excedido: %1\$s(%2\$s)->%3\$s(%4\$s) rechazadas.

Explicación: Existen demasiadas sesiones UDP a través de la máquina cortafuegos

Acción del Sistema: rechazar las conexiones

**ICA1047 Advertencia de período de gracia: demasiadas sesiones
TCP,%1\$s(%2\$s)->%3\$s(%4\$s) pasadas**

Explicación: Existen demasiadas sesiones TCP a través de la máquina cortafuegos

Acción del Sistema: pasar las conexiones

**ICA1048 Advertencia de período de gracia: demasiadas sesiones
UDP,%1\$s(%2\$s)->%3\$s(%4\$s) pasadas**

Explicación: Existen demasiadas sesiones UDP a través de la máquina cortafuegos

ICA1049 Paquete ipsec no válido: s:%1\$s d:%2\$s protocolo:%3\$s spi:%4\$s

Explicación: El cortafuegos receptor no puede eliminar la encapsulación del paquete ipsec.

Respuesta del Usuario: Asegúrese de que la definición del túnel se haya exportado correctamente y activado en cada cortafuegos.

ICA1050 Se ha suprimido la especificación para el túnel:%1\$s

Explicación: La especificación del túnel, para el ID especificado, ya no está operativa.

ICA1051 Se define la(s) especificación(ones) de túnel siguiente(s):

Explicación: Las especificaciones de túnel están definiéndose, tal como se indica en los registros de anotaciones siguientes.

**ICA1052 >ID_túnel:%1\$s, direc_orig:%2\$s, direc_dest:%3\$s, cifr_orig:%4\$s
elim_cifr:%5\$s máq_orig:%6\$s elim_máq:%7\$s máq_cifr_orig:%8\$s
elim_máq_cifr:%9\$s pol_orig:%10\$s elim_pol:%11\$s modalidad:%12\$s**

Explicación: El mensaje lista los atributos específicos del túnel activado.

ICA1200 Finalizando daemon de registro debido a los errores anteriores

Explicación: Debido a los errores grabados con anterioridad a este mensaje, el daemon fwlogd está finalizando.

Acción del Sistema: El registro de filtros IP no se activará.

Respuesta del Usuario: Corrija los errores indicados y vuelva a arrancar fwlogd.

**ICA1260 Finalizando daemon de registro de filtros a las %1\$s del %2\$s debido a la
recepción de la señal %3\$s**

Explicación: El daemon fwlogd ha recibido la señal de terminación indicada y está deteniéndose.

ICA1305 \"desconocido\"

Explicación: Al formatearse un paquete IP para syslog, se detectó un registro con una especificación de protocolo desconocida. Los protocolos IP, ICMP, TCP, UDP e IPSP son los protocolos reconocidos. Tenga en cuenta que IPSP es la designación de IBM para los paquetes cifrados que pasan a través de un túnel.

ICA1400 Error muy grave de fwtimernat - %1\$s: %2\$s

Explicación: El servidor fwtimernat no ha podido realizar satisfactoriamente la función indicada. El servidor fwtimernat ha sido interrumpido.

Respuesta del Usuario: Corrija el problema del sistema que se indica y vuelva a arrancar fwtimernat.

ICA1401 Error muy grave de fwtimernat - %1\$s: código de retorno = 0x%2\$s

Explicación: El servidor fwtimernat no ha podido realizar satisfactoriamente la función indicada. El servidor fwtimernat ha sido interrumpido.

Respuesta del Usuario: Corrija el problema del sistema que se indica y vuelva a arrancar fwtimernat.

ICA1402 Error muy grave de fwtimernat - %1\$s: %2\$s

Explicación: El servidor fwtimernat no ha podido realizar satisfactoriamente la función indicada. El servidor fwtimernat ha sido interrumpido.

Respuesta del Usuario: Corrija el problema del sistema que se indica y vuelva a arrancar fwtimernat.

ICA2000 Nueva sesión FTP en %1\$s desde %2\$s (ubicación no segura).

Explicación: Iniciándose una nueva sesión ftp desde una ubicación no segura.

ICA2001 Autenticación anómala para el usuario %1\$s (desconocido) desde %2\$s:%3\$s.

Explicación: Un usuario que no disponía de cuenta ha intentado utilizar el proxy ftp desde la red.

Respuesta del Usuario: Solicite al administrador del cortafuegos que defina una cuenta proxy.

ICA2002 Autenticación anómala para el usuario %1\$s con %2\$s desde %3\$s:%4\$s.

Explicación: El cortafuegos no puede autenticar el nombre del usuario indicado utilizando el método de autenticación especificado.

Respuesta del Usuario: Consulte al administrador del cortafuegos.

ICA2003 No se han configurado shells para %1\$s.

Explicación: El usuario identificado ha intentado una conexión con el proxy y no se ha definido ningún shell de conexión.

Respuesta del Usuario: Solicite al administrador del cortafuegos que corrija el perfil conexión de este usuario.

ICA2004 Se ha recibido un evento de comprobación desconocido de 0x%1\$s.

Explicación: El módulo tcpip_audit.c. ha recibido una petición de comprobación desconocida.

ICA2005 Error al grabar en el cliente: %1\$s.

Explicación: No es posible establecer comunicaciones con el cliente, consulte el mensaje del sistema registrado.

ICA2006 ptelnetd: auditproc: %1\$s.

Explicación: El proceso de comprobación telnet ha devuelto el error indicado. Es posible que los archivos del sistema se hayan dañado.

ICA2007 ptelnetd: estado de alarma=%1\$s.

Explicación: Se ha detectado un error desconocido. Es posible que los archivos del sistema se hayan dañado.

ICA2008 El usuario sin cortafuegos %1\$s desde :%2\$s ha utilizado telnet.

Explicación: Un usuario que no disponía de cuenta para el cortafuegos ha intentado utilizar el proxy telnet.

Acción del Sistema: Se da por supuesto que se ha utilizado la Autenticación genérica.

ICA2009 /bin/login: %1\$s.

Explicación: Se ha producido un error muy grave durante la conexión del sistema. Consulte el mensaje de error del sistema que se indica.

ICA2010 Conexión a %1\$s desde %2\$s (no segura).

Explicación: Conexión satisfactoria entre las direcciones IP indicadas a través de la interfaz no segura.

ICA2011 Conexión a %1\$s desde %2\$s (segura).

Explicación: Conexión satisfactoria entre las direcciones IP indicadas a través de la interfaz segura.

ICA2012 Nueva sesión FTP en %1\$s desde %2\$s (ubicación segura).

Explicación: Iniciándose una nueva sesión ftp.

ICA2013 Nueva sesión Telnet en %1\$s desde %2\$s.

Explicación: Se ha establecido una nueva sesión telnet.

ICA2014 La opción %1\$s no recibe soporte.

Explicación: El distintivo indicado no recibe soporte, consulte el mensaje anterior.

ICA2015 La opción -%1\$s no recibe soporte.

Explicación: El distintivo indicado no recibe soporte, consulte el mensaje anterior.

ICA2016 ID de usuario remota \"%1\$s\".

Explicación: Petición de conexión ftp para el usuario indicado.

ICA2017 Depurar %1\$s %2\$s %3\$s.

ICA2018 No se ha encontrado la clave SNK para el usuario %1\$s.

Explicación: No se ha encontrado el valor SecureNetKey para el ID de usuario indicado.

Respuesta del Usuario: Consulte al administrador del cortafuegos para determinar si existe algún problema en la configuración de la conexión.

ICA2019 La clave SNK no se ha leído correctamente para el usuario %1\$s.

Explicación: El valor SecureNetKey no ha podido leerse como dígitos octales para el ID de usuario indicado.

Respuesta del Usuario: Consulte al administrador del cortafuegos para determinar si existe algún problema en la configuración de la conexión.

ICA2020 /usr/bin/fwuserau o /usr/bin/fwuserpt no existe.

Explicación: Se ha cancelado anormalmente la autenticación que utiliza el método de autenticación suministrado por el usuario.

Acción del Sistema: La autenticación se ha cancelado anormalmente.

Respuesta del Usuario: Asegúrese de que /usr/bin/fwuserau y /usr/bin/fwuserpt existen y que el propietario es el usuario raíz. Si el ejecutable no existe, el usuario debe crearlo utilizando un compilador compatible con el sistema de operación del cortafuegos y ponerle el nombre /usr/bin/fwuserau o /usr/bin/fwuserpt.

ICA2021 Intentando conectar a sistema principal remoto %1\$s con ID de usuario %2\$s.

Explicación: Intentando establecer una nueva conexión ftp.

ICA2022 Intentando conectar a sistema principal remoto %1\$s.

Explicación: Intentando establecer una nueva conexión ftp.

ICA2023 Utilización: ptelnetd -n -s .

Explicación: Se ha especificado un distintivo desconocido al iniciar el daemon ptelnet.

Respuesta del Usuario: Utilice sólo los distintivos -n y/o -s.

ICA2024 El usuario %1\$s ha sido autenticado satisfactoriamente utilizando la autenticación de %2\$s desde %3\$s:%4\$s.

Explicación: El cortafuegos ha autenticado el nombre de usuario indicado utilizando el método de autenticación especificado.

ICA2025 El usuario %1\$s se ha conectado utilizando la autenticación de %2\$s desde %3\$s:%4\$s.

Explicación: El usuario ftp se ha conectado.

ICA2026 El usuario %1\$s ha sobrepasado el tiempo de espera tras %2\$s segundos a las %3\$s.

Explicación: El intento de conexión ha excedido el tiempo de espera para el usuario especificado. Es posible que exista un problema de direccionamiento de la red o que el sistema principal remoto no esté disponible.

ICA2027 Conexión desde %1\$s a las %2\$s.

Explicación: Se ha establecido la conexión ftp de la red con el cortafuegos.

ICA2028 Se ha rechazado el intento de conexión FTP a %1\$s desde %2\$s. Esta máquina no da soporte a FTP desde la ubicación no segura.

Explicación: Por lo general indica un intento de establecer una conexión ftp con el cortafuegos a través de la interfaz no segura.

Acción del Sistema: Rechazar la conexión.

ICA2029 Error del sistema con número de error = %1\$s en %2\$s línea %3\$s.

Explicación: La llamada al sistema detecta un problema al ejecutar una llamada al sistema.

Acción del Sistema: La ejecución del sistema se ha detenido

Respuesta del Usuario: Consulte el registro, averigüe el significado del número de error e intente solucionar el problema. Si no puede resolverse, solicite asistencia técnica a IBM.

ICA2030 Llamada a función con código de retorno = %1\$s en %2\$s línea %3\$s.

Explicación: La llamada a la función detecta un problema.

Acción del Sistema: Se ha devuelto un error

Respuesta del Usuario: Consulte el registro, averigüe el significado del código de retorno e intente solucionar el problema. Si no puede resolverse, solicite asistencia técnica a IBM.

ICA2031 Llamada a función sdi creadcfg() rc = %1\$s.

Explicación: La llamada a la función detecta un problema.

Acción del Sistema: Se ha devuelto un error

Respuesta del Usuario: Lea la consulta sdi para conocer la explicación.

ICA2032 Se ha perdido la conexión.

Explicación: Se ha perdido la conexión ftp.

Respuesta del Usuario: Vuelva a establecer la sesión.

ICA2033 Llamada a función sdi sd_init rc = %1\$s.

Explicación: La llamada a la función detecta un problema.

Acción del Sistema: Se ha devuelto un error

Respuesta del Usuario: Lea la consulta sdi para conocer la explicación.

ICA2034 Llamada a función sdi sd_check rc = %1\$s.

Explicación: La llamada a la función detecta un problema.

Acción del Sistema: Se ha devuelto un error

Respuesta del Usuario: Lea la consulta sdi para conocer la explicación.

ICA2035 setsockopt(): %1\$s.

Explicación: Error del sistema en la llamada setsocketopt.

ICA2036 Se ha iniciado la sesión Telnet %1\$s para el usuario %2\$s (%3\$s:%4\$s).

Explicación: Mensaje que se genera al inicio de cada sesión Telnet. Una sesión empieza cuando el cortafuegos conoce el ID de usuario, la dirección IP de origen y la dirección IP de destino. El ID de sesión es un identificador exclusivo que el cortafuegos genera.

ICA2037 El usuario fwdfuser o fwdpuser ha intentado conectarse, no tiene permiso.

Explicación: fwdfuser y fwdpuser son usuarios reservados y no deberían usarse.

Acción del Sistema: Se ha rechazado la conexión.

Respuesta del Usuario: El administrador debería investigar quién está utilizando este usuario.

ICA2038 ttloop: similar finalizado: %1\$s.

Explicación: Se ha producido un error al vaciar el almacenamiento intermedio de salida de la red. Parece que el proceso similar ha finalizado.

ICA2039 ttloop: lectura: %1\$s.

Explicación: Se ha producido un error al vaciar el almacenamiento intermedio de salida de la red.

ICA2040 La autenticación establecida en contraseña, ninguna o snk no está permitida para el ID de usuario fwdfuser.

Explicación: fwdfuser es un ID de usuario reservado y no debería usar una contraseña o ninguno como método de autenticación.

Acción del Sistema: Se ha rechazado la conexión.

Respuesta del Usuario: El administrador debería cambiar el método de autenticación para el ID de usuario fwdfuser.

ICA2041 Se ha iniciado la sesión FTP %1\$s para %2\$s (%3\$s:%4\$s).

Explicación: Mensaje generado al inicio de cada sesión FTP. Una sesión empieza cuando el cortafuegos conoce el ID de usuario, la dirección IP de origen y la dirección IP de destino. El ID de sesión es un identificador exclusivo que el cortafuegos genera.

ICA2042 req_rsp_code se ha establecido incorrectamente en FW_AUTH_REQ.

Explicación: fw_tn_authenticate no puede establecer req_rsp_code en FW_AUTH_REQ.

Acción del Sistema: Cancelar anormalmente la autenticación.

Respuesta del Usuario: Cambie fw_tn_authenticate, vuelva a crear la biblioteca fwuser.o y colóquela en el cortafuegos.

ICA2043 No ha podido obtenerse la contraseña para %1\$s.

Explicación: El tipo de autenticación para este usuario es 'contraseña' y no se ha encontrado ninguna contraseña.

Respuesta del Usuario: Consulte al administrador del cortafuegos.

ICA2044 Se ha especificado una hora incorrecta (%1\$s) para -t.

Explicación: El valor de la hora que se muestra contiene caracteres fuera del rango numérico de 0 a 9 o excede el valor máximo permitido.

ICA2045 La opción -T no recibe soporte en el cortafuegos.

Explicación: La opción indicada no recibe soporte.

ICA2046 La opción -k no recibe soporte en el cortafuegos.

Explicación: La opción indicada no recibe soporte.

ICA2047 La opción -s no recibe soporte en el cortafuegos.

Explicación: La opción indicada no recibe soporte.

ICA2048 La opción -u no recibe soporte en el cortafuegos.

Explicación: La opción indicada no recibe soporte.

ICA2049 El distintivo desconocido -%1\$s ha sido ignorado.

Explicación: El distintivo mencionado se ha especificado y no se reconoce.

ICA2050 Parámetro desconocido %1\$s.

Explicación: El valor indicado, especificado como una opción, no es reconocido.

ICA2051 Error de conversión adapt_addr en dirección.

Explicación: La dirección IP mostrada no es válida.

Respuesta del Usuario: Es posible que se haya dañado el archivo /etc/security/fwsecadpt.cfg. Elimine el archivo, vuelva a configurar la interfaz o interfaces seguras y reinicialice los filtros.

ICA2052 afopen no ha podido abrir /etc/security/login.cfg: %1\$s.

Explicación: No se puede autenticar el usuario, error al abrir el archivo indicado.

ICA2053 No ha podido abrirse el archivo de interfaz segura.

Explicación: No se ha configurado una interfaz segura.

Respuesta del Usuario: Si debe definirse una interfaz segura, utilice los paneles smit/mandatos del cortafuegos para definir la interfaz o interfaces seguras.

ICA2054 enduserdb rc=%1\$s, %2\$s.

Explicación: Se ha recibido el código de error del sistema indicado al intentar recuperar la información del perfil de conexión del usuario.

Respuesta del Usuario: Consulte al administrador del cortafuegos para verificar su cuenta de conexión.

ICA2055 getpeername() (%1\$s): %2\$s.

Explicación: Se ha producido un error del sistema cuando el daemon ftp intentaba obtener el nombre del socket.

ICA2056 getsockname() (%1\$s): %2\$s.

Explicación: Se ha producido un error del sistema cuando el daemon ftp intentaba obtener el nombre de la puerta.

ICA2057 Shell no seguro de getuser rc=%1\$s para %2\$s, %3\$s.

Explicación: Se ha recibido el código de error del sistema indicado al intentar recuperar el nombre del shell para la conexión desde la ubicación no segura del cortafuegos.

Respuesta del Usuario: Consulte al administrador del cortafuegos para establecer un shell para su perfil de conexión de usuario.

ICA2058 Shell seguro de getuser rc=%1\$s para %2\$s, %3\$s.

Explicación: Se ha recibido el código de error del sistema indicado al intentar recuperar el nombre del shell para la conexión desde la ubicación segura del cortafuegos.

Respuesta del Usuario: Consulte al administrador del cortafuegos para utilizar un shell para su perfil de conexión de usuario.

ICA2059 ioctl(): %1\$s

Explicación: Error del sistema en la llamada ioctl() para SIOCSPGRP.

ICA2060 ptelnetd: ftok para la memoria compartida ha resultado anómalo.

Explicación: No se puede asignar el segmento de memoria compartida.

Respuesta del Usuario: Póngase en contacto con el administrador del cortafuegos; aparentemente se trata de un problema de memoria.

ICA2061 ptelnetd: shmat para la memoria compartida ha resultado anómalo.

Explicación: No se puede asignar el segmento de memoria compartida.

Respuesta del Usuario: Póngase en contacto con el administrador del cortafuegos; aparentemente se trata de un problema de memoria.

ICA2062 ptelnetd: shmget para la memoria compartida ha resultado anómalo.

Explicación: No se puede asignar el segmento de memoria compartida.

Respuesta del Usuario: Póngase en contacto con el administrador del cortafuegos; aparentemente se trata de un problema de memoria.

ICA2063 setsockopt() (SO_DEBUG): %1\$s.

Explicación: El mensaje de error indicado lo ha devuelto la llamada al sistema 'setsockopt'.

ICA2064 setsockopt() (SO_KEEPALIVE): %1\$s.

Explicación: El mensaje de error indicado lo ha devuelto la llamada al sistema 'setsockopt'.

ICA2065 setuser rc=%1\$s, %2\$s.

Explicación: Se ha recibido un código de retorno erróneo en una llamada del sistema por la razón indicada.

ICA2066 señal(): %1\$s.

Explicación: Se ha producido un error del sistema cuando el daemon ftp intentaba establecer un manejador de señal.

ICA2067 Error de inicialización de pftpd muy grave - bind(): %1\$s

Explicación: La inicialización del servidor pftpd ha resultado anómala, el daemon ha terminado.

Respuesta del Usuario: Corrija el problema del sistema que se indica y vuelva a arrancar pftpd. La causa más probable de este error es que otro daemon ftp ya está atendiendo a la puerta ftp estándar (21).

ICA2068 Error de inicialización de pftpd muy grave - listen(): %1\$s

Explicación: La inicialización del servidor pftpd ha resultado anómala, el daemon ha terminado.

Respuesta del Usuario: Corrija el problema del sistema que se indica y vuelva a arrancar pftpd.

ICA2069 Error pftpd muy grave - main accept(): %1\$s

Explicación: La rutina principal del servidor pftpd ha resultado anómala, el daemon ha terminado.

Respuesta del Usuario: Corrija el problema del sistema que se indica y vuelva a arrancar pftpd.

ICA2070 Error de inicialización de pftpd muy grave - socket(): %1\$s

Explicación: La inicialización del servidor pftpd ha resultado anómala, el daemon ha terminado.

Respuesta del Usuario: Corrija el problema del sistema que se indica y vuelva a arrancar pftpd.

ICA2071 Conexión rechazada, se ha alcanzado el número máximo de conexiones.

Explicación: El servidor pftpd no puede crear otra sesión FTP porque ya se ha alcanzado el número máximo de sesiones.

Acción del Sistema: La conexión se rechaza.

Respuesta del Usuario: Espere a que finalicen las conexiones existentes y, a continuación, intente de nuevo la solicitud.

ICA2072 El archivo de configuración ftp (%1\$s) no está disponible.

Explicación: El daemon ftp ha intentado abrir el archivo de configuración de ftp especificado pero no existe o no se ha podido abrir.

Acción del Sistema: El proceso del daemon ftp utiliza la configuración por omisión

Respuesta del Usuario: Ninguna, a no ser que el archivo deba existir, en cuyo caso debería crearse o moverse a la ubicación especificada en el mensaje.

ICA2073 No ha podido obtenerse almacenamiento para la tabla de lenguaje ftp.

Explicación: No se ha podido obtener el almacenamiento necesario para representar una sentencia REPLYLANGUAGE en el archivo de configuración de ftp.

Acción del Sistema: El proceso continúa.

Respuesta del Usuario: Aumente el tamaño de la región o reduzca las entradas del archivo de configuración.

ICA2074 El proceso para la sentencia de configuración ftp se ha completado: %1\$s

Explicación: ftp ha procesado la sentencia de configuración indicada.

Acción del Sistema: El proceso continua.

Respuesta del Usuario: Ninguna

ICA2075 FTP para %1\$s (%2\$s:%3\$s), %4\$s %5\$s, %6\$s bytes. sid: %7\$s.

Explicación: Mensaje generado para cada transferencia de archivos en sesiones FTP abiertas. El sid es un identificador exclusivo generado por el cortafuegos en el inicio de la sesión.

ICA2076 Ha finalizado la sesión FTP %1\$s para %2\$s (%3\$s:%4\$s), %5\$s segundos, %6\$s bytes.

Explicación: Mensaje generado al final de cada sesión del daemon FTP. El sid es un identificador exclusivo generado por el cortafuegos en el inicio de la sesión.

ICA2077 Ha finalizado la sesión Telnet %1\$s para %2\$s (%3\$s:%4\$s), %5\$s bytes.

Explicación: Mensaje generado al final de cada sesión Telnet. El sid es un identificador exclusivo generado por el cortafuegos en el inicio de la sesión.

ICA2078 Usuario Proxy desconectado %1\$s - desocupado durante %2\$s minutos.

Explicación: La sesión del usuario ha excedido el tiempo de espera máximo que se permite.

ICA2079 Atención - Intento de conexión no autorizado a %1\$s desde %2\$s.

Explicación: Generalmente indica un intento de establecer una conexión al cortafuegos a través de una interfaz no segura.

Acción del Sistema: Rechazar la conexión.

ICA2080 Error de sintaxis (%1\$s) junto a la columna %2\$s en la línea del archivo de configuración ftp %3\$s: %4\$s

Explicación: La sentencia de configuración ftp de la línea especificada es errónea. Se proporciona la razón del error y la ubicación donde se ha detectado.

Acción del Sistema: Se pasa por alto la sentencia.

Respuesta del Usuario: Corrija la sentencia en el archivo de configuración ftp.

ICA2081 Las sentencias de configuración ftp no han proporcionado ningún catálogo de mensajes que pueda utilizarse.

Explicación: Los intentos por abrir los catálogos de mensajes proporcionados por las sentencias de configuración de ftp REPLYLANGUAGE han resultado anómalos. No se puede usar ningún catálogo de mensajes de cliente.

Acción del Sistema: El catálogo de mensajes del cliente está forzado a inglés en el subdirectorío C.

Respuesta del Usuario: Asegúrese de que hay archivos de catálogo en cada uno de los directorios que se asocian a los directorios de lenguaje en las sentencias REPLYLANGUAGE de configuración ftp. Compruebe también que la variable de entorno NLSPATH esté establecida correctamente para permitir la substitución del subdirectorío de la variable de entorno LANG (%L) y el nombre de catálogo (%N).

ICA2082 La variable de entorno LANG ftp no ha podido establecerse en %1\$s, razón: %2\$s

Explicación: Se ha producido un error del sistema (dado por la razón) mientras el daemon ftp intentaba cambiar el valor de la variable de entorno LANG al subdirectorio especificado.

Acción del Sistema: El proceso continua. La recuperación puede generar otros mensajes.

Respuesta del Usuario: Utilice la razón especificada para determinar si se trata de un error de sistema o de un error de programación.

ICA2083 No ha podido abrirse el catálogo de mensajes de cliente ftp en el directorio: %1\$s, razón: %2\$s

Explicación: El daemon ftp no ha podido abrir el catálogo de mensajes en el subdirectorio especificado. La razón especificada es el número de error que ha devuelto catopen().

Acción del Sistema: El proceso continua. La recuperación puede generar otros mensajes.

Respuesta del Usuario: Asegúrese de que hay un catálogo en el directorio asociado con el directorio de lenguaje proporcionado. Compruebe que la variable de entorno NLSPATH esté establecida correctamente para permitir la substitución del subdirectorio (%L) y el nombre de catálogo (%N).

ICA2084 Forzando catálogo de mensajes de cliente ftp a inglés a través del subdirectorio C.

Explicación: Debido a los errores listados anteriormente, el daemon ftp ha forzado el catálogo de mensajes de cliente a inglés utilizando el subdirectorio C.

Acción del Sistema: Si se puede forzar el lenguaje al catálogo de mensajes de C, el proceso continúa. Si no se puede, el programa finaliza.

Respuesta del Usuario: Corrija el error del mensaje anterior. Si el programa también existía, cree el catálogo de mensajes en el subdirectorio C y establezca la variable de entorno NLSPATH correctamente.

ICA2085 Ha finalizado la sesión Telnet para el pid %1\$s (%2\$s).

Explicación: Mensaje generado al final de cada sesión Telnet.

ICA2086 Archivo de usuario incorrectamente configurado; el usuario %1\$s no tiene ninguna clave (%2\$s).

Explicación: ftpd ha encontrado el usuario solicitado en el archivo de usuario, pero no ha podido encontrar la clave - archivo de usuario incorrectamente configurado.

Respuesta del Usuario: Utilice los paneles smit/mandatos del cortafuegos para corregir este problema.

ICA2087 ftpd no ha podido encontrar el usuario especificado %1\$s en el archivo de configuración del usuario.

Explicación: El nombre de usuario especificado no se ha configurado o el archivo user.cfg está dañado.

Respuesta del Usuario: Utilice los paneles smit/mandatos del cortafuegos para corregir este problema.

ICA2088 ftpd no ha podido abrir el archivo de configuración de usuario.

Explicación: ftpd ha hecho una llamada a fopen que ha resultado anómala porque no ha podido abrir el archivo de configuración de usuario.

Respuesta del Usuario: Asegúrese de que el archivo de configuración del usuario (user.cfg por omisión) está disponible; utilice los paneles smit/mandatos del cortafuegos

ICA2089 El tipo de autorización del archivo de usuario (%1\$s) no coincidía con ninguna de las entradas de la tabla (struct tab2 authtab).

Explicación: El tipo de autorización del usuario especificado (devuelto de user.cfg) no coincide con los tipos admitidos (tales como deny,none,snk,sdi,password,etc.)

Respuesta del Usuario: Compruebe la integridad o la configuración del archivo user.cfg; utilice los paneles smit/mandatos del cortafuegos para corregir este problema.

ICA2090 La autenticación ha resultado anómala para el usuario '%1\$s' de %2\$s porque se ha especificado KEY=DENY en el archivo user.cfg.

Explicación: La autenticación ha resultado anómala debido a las especificaciones del archivo user.cfg establecidas por el administrador del cortafuegos.

Respuesta del Usuario: Consulte al administrador del cortafuegos.

ICA2091 El usuario '%1\$s' no tiene permiso para ftp para la puerta no segura (%2\$s).

Explicación: El usuario ha intentado utilizar ftp para el servidor del cortafuegos a través de una puerta no segura (nsp) - todos los usuarios nsp deben tener la clave 'fwnsftp' correctamente configurada para un tipo de autorización válida (en el archivo user.cfg).

Respuesta del Usuario: Compruebe la integridad o la configuración del archivo user.cfg; utilice los paneles smit/mandatos del cortafuegos para corregir este problema.

ICA2092 Error interno: nt_gwauth() ha resultado anómalo.

Explicación: nt_gwauth() normalmente devuelve uno de los tres valores (AUTHENTICATED,NOT_AUTHENTICATED o DENY) en este caso \ nt_gwauth ha devuelto algún entero no válido.

ICA2093 El usuario '%1\$s' no tiene permiso para ftp para la puerta segura (%2\$s).

Explicación: El usuario ha intentado utilizar ftp para el servidor del cortafuegos a través de una puerta segura (sp) - todos los usuarios sp deben tener la clave 'fwsftp' correctamente configurada para un tipo de autorización válida (en el archivo user.cfg).

Respuesta del Usuario: Compruebe la integridad o la configuración del archivo user.cfg; utilice los paneles smit/mandatos del cortafuegos para corregir este problema.

ICA2094 Conexión anómala: formato esperado: "PASS <contraseña>" a continuación: "USER <%1\$s>"; recibido %2\$s.

Explicación: La autenticación ha resultado anómala porque el cliente ftp no ha enviado el formato esperado (PASS 'contraseña' por RFC959)

Respuesta del Usuario: Escriba "user <nombre de usuario>"; entre la contraseña correcta. Consulte al administrador del cortafuegos.

ICA2095 Conexión anómala: (mediante método %1\$s) autenticación anómala de usuario '%2\$s' de %3\$s (ubicación de cliente).

Explicación: La autenticación ha sido anómala debido a una entrada no válida (por el cliente para el tipo de autenticación especificado); por ejemplo, el usuario ha entrado una contraseña o clave snk no válida, etc.

Respuesta del Usuario: Consulte al administrador del cortafuegos.

ICA2096 Autenticado: (mediante método %1\$s) autenticación satisfactoria de usuario '%2\$s' de %3\$s (ubicación de cliente).

Explicación: Autenticación satisfactoria

ICA2097 httpd --> Iniciando versión del servidor Proxy HTTP %1\$s.

Explicación: Iniciando Proxy HTTP para acceso a WWW.

ICA2098 httpd --> Concluyendo servidor Proxy HTTP.

Explicación: Concluyendo Proxy HTTP para acceso a WWW.

ICA2099 httpd --> Estado: <%1\$s> del cliente <%2\$s>, que ha solicitado <\"%3\$s\"> para <%4\$s> bytes.

Explicación: Estado de la petición HTTP del cliente para algunos archivos a través del Proxy. Para obtener más información acerca del valor del código "Estado", consulte los documentos HTTP 1.0(RFC 1945) o HTTP 1.1(RFC 2068) (o RFC relacionadas) que están disponibles en diversas ubicaciones de Internet, incluida ds.internic.net.

ICA2100 La dirección del socket es igual a cero.

Explicación: Se ha encontrado una dirección de destino que no es válida en la petición local.

ICA2101 Error en la familia de direcciones de socket: %1\$s.

Explicación: Se ha encontrado un tipo de familia de destino que no es válido en la petición local.

ICA2102 Error al inicializar odm: %1\$s.

Explicación: Se ha producido un error en odm_initialize() para ODM (Gestor de datos de objetos).

ICA2103 Error al establecer la vía de acceso por omisión de odm: %1\$s.

Explicación: Se ha producido un error en odm_set_path() para ODM (Gestor de Datos de Objetos). Clase de objeto, OCSvhost.

ICA2104 Error al bloquear base de datos odm: %1\$s.

Explicación: Se ha producido un error de odm_lock() para ODM (Gestor de datos de objetos).

ICA2105 Error al abrir el objeto odm %1\$s: %2\$s.

Explicación: Se ha producido un error en odm_open_class() para ODM (Gestor de datos de objetos).

ICA2106 Error al buscar el objeto odm %1\$s: %2\$s.

Explicación: Se ha producido un error en odm_get_first() para ODM (Gestor de datos de objetos). Clase de objeto, OCSvhost.

ICA2107 Error al cerrar el objeto odm %1\$s: %2\$s.

Explicación: Se ha producido un error en odm_close_class() para ODM (Gestor de datos de objetos). Clase de objeto, OCSvhost.

ICA2108 Error al desbloquear base de datos odm: %1\$s.

Explicación: Se ha producido un error en odm_unlock() error para ODM (Gestor de Datos de Objetos).

ICA2109 Error al finalizar odm: %1\$s.

Explicación: Se ha producido un error en odm_terminate() para ODM (Gestor de datos de objetos).

ICA2110 Error al obtener servidor por nombre: %1\$s.

Explicación: Se ha producido un error en getservbyname(). El servicio de supervisión de la conexión del sistema principal, lm, no está especificado correctamente en el archivo /etc/services.

ICA2111 byname() error: %1\$s.

Explicación: Se ha producido un error en gethostbyname(). El nombre de la máquina del sistema principal no se ha definido correctamente en /etc/hosts.

ICA2112 Nombre de protocolo no válido: %1\$s.

Explicación: El nombre de protocolo especificado en la clase de objeto ODM, OCSvhost, no está admitido.

ICA2113 Error al abrir socket para LM: %1\$s.

Explicación: Se ha producido un error en socket() para la máquina de sistema principal en la que se encuentra el supervisor de conexión.

ICA2114 Error al vincular dirección local: %1\$s.

Explicación: Se ha producido un error en bind() al usar la dirección local para este nodo OCS.

ICA2115 Error al conectar socket para LM: %1\$s.

Explicación: Se ha producido un error en connect() para la máquina del sistema en la que se encuentra el supervisor de conexión.

ICA2116 Error de tipo de protocolo: %1\$s.

Explicación: El tipo de protocolo de terminal virtual utilizado para la comunicación con el supervisor de conexión del sistema principal no es válido.

ICA2117 Error Malloc en mensaje LM.

Explicación: Se ha producido un error malloc() cuando se ha asignado dinámicamente el espacio para la variable de longitud del mensaje del supervisor de conexión.

ICA2118 Error al transmitir mensaje a LM: %1\$s.

Explicación: Se ha producido un error en send() al enviar una petición al supervisor de conexión para abrir el dispositivo del sistema principal correcto.

ICA2119 Error al recibir mensaje de LM: %1\$s.

Explicación: Se ha producido un error en recv() cuando el supervisor de conexión ha devuelto un acuse de recibo.

ICA2120 Error de estado de LM: %1\$s.

Explicación: El acuse de recibo del supervisor de conexión indica que el dispositivo del sistema principal NO se ha abierto satisfactoriamente.

ICA2121 Error al abrir dispositivo de administración OCS: %1\$s.

Explicación: El dispositivo de administración OCS no se ha abierto satisfactoriamente.

ICA2122 No ha podido convertirse la dirección IP para el ID de TMB: %1\$s.

Explicación: Se ha producido un error en ioctl() OCS_GET_TBMID. El mandato ioctl OCS_GET_TBMID ha resultado anómalo en el dispositivo de administración OCS.

ICA2123 Error al conectar TMB determinado por rlogin: %1\$s.

Explicación: Se ha producido un error en ioctl() OCS_IS_TBM_CONNECTED. El mandato ioctl OCS_IS_TBM_CONNECTED ha resultado anómalo en el dispositivo de administración de OCS.

ICA2124 No se ha conectado ningún nodo del sistema principal: %1\$s.

Explicación: No hay ningún nodo conectado a este nodo de OCS de la lista de nodos de sistema principal posibles.

ICA2125 Error al obtener la lista para ODM (Gestor de datos de objetos): %1\$s: %2\$s.

Explicación: Se ha producido un error en odm_get_list() para la clase de objetos de ODM, CuAt(Atributo personalizado).

ICA2126 No se ha asociado ningún nodo del sistema principal OCS con: %1\$s.

Explicación: La entrada del CuAt (Atributo personalizado) se ha encontrado pero no había ninguna correspondencia con el nodo del sistema principal o el nodo OCS.

ICA2127 Error Malloc en matriz del sistema principal.

Explicación: Se ha producido un error en malloc() al asignar dinámicamente el espacio para la matriz de nombres de sistema principal posibles.

ICA2128 El usuario (desconocido) de %1\$s (ubicación de cliente) ha intentado un mandato '%2\$s' antes de la autenticación.

Explicación: Un usuario ha intentado llevar a cabo acciones antes de entrar el nombre de usuario y la contraseña para la autenticación; los usuarios deben autenticarse primero antes de que pueda continuar otro proceso.

Respuesta del Usuario: Conéctese con USER y PASS

ICA2129 gethostbyname (%1\$s): %2\$s

Explicación: Se ha producido un error del sistema cuando ftpd intentaba obtener la información del sistema principal que corresponde al nombre del sistema principal.

ICA2130 El usuario (%1\$s) de %2\$s (ubicación de cliente) ha intentado un mandato '%3\$s'.

Explicación: El usuario especificado ha intentado un mandato no válido.

Respuesta del Usuario: Sólo los mandatos USER, QUOTE SITE y QUIT se permiten hasta que especifique "quote site destination".

ICA2131 La autenticación ha resultado anómala para el usuario '%1\$s' de %2\$s debido a un error en el archivo user.cfg.

Explicación: La autenticación ha resultado anómala debido a las especificaciones del archivo user.cfg establecidas por el administrador del cortafuegos (compruebe los registros anteriores).

Respuesta del Usuario: Consulte al administrador del cortafuegos.

ICA2132 El usuario '%1\$s' de ip %2\$s (ubicación de cliente) ha intentado el mandato no válido '%3\$s'.

Explicación: El usuario ha intentado un mandato no válido. Los únicos mandatos válidos llegado este punto son SITE, USER y QUIT.

ICA2133 Error: la llamada de %1\$s ha resultado anómala en %2\$s:%3\$s, %4\$s

Explicación: Mensaje de error general; compruebe los registros

ICA2134 Aviso: ftpd: connect() (en %1\$s) no ha podido conectarse con %2\$s, %3\$s.

Explicación: Connect() no ha podido encontrar la dirección solicitada; compruebe el resultado de WSAGetLastError.

Respuesta del Usuario: Compruebe su dirección por duplicado; puede ser un error de DNS o de red

ICA2135 Transferencia de datos finalizada: %1\$s bytes recibidos (de %2\$s); %3\$s bytes enviados (a %4\$s).

Explicación: Esta información refleja una única transferencia de datos durante una sesión ftp particular. \ Sin embargo, tenga en cuenta que es posible que la transferencia de datos no se haya completado satisfactoriamente \ (compruebe el registro para verificar si existe una llamada de recepción o de envío anómala).

ICA2136 Error: CreateThread() ha resultado anómalo en %1\$s: %2\$s.

Explicación: ftpd no ha podido crear una hebra

ICA2137 Se ha establecido la conexión de datos; servidor: %1\$s cliente: %2\$s.

Explicación: Conexión de datos satisfactoria.

ICA2138 No existe suficiente memoria: pftpd: malloc(%1\$s) ha devuelto NULL en la función %2\$s.

Explicación: No se puede asignar suficiente memoria; malloc ha devuelto NULL.

ICA2139 LogonUser() ha resultado anómalo: %1\$s.

Explicación: LogonUser de la API de Windows NT (SAM) (para autenticación de contraseñas) ha resultado anómalo debido a las razones especificadas.

Respuesta del Usuario: Póngase en contacto con el administrador del cortafuegos.

ICA2140 httpd --> Autenticación de Proxy HTTP %1\$s para el usuario <%2\$s>, en <%3\$s>, mediante %4\$s ... RC:<%5\$s>.

Explicación: El Proxy HTTP ha intentado realizar la autenticación del usuario. La razón que aquí se informa indica si ha resultado satisfactoria o no.

Respuesta del Usuario: Póngase en contacto con el administrador del cortafuegos.

ICA2141 La sesión FTP en %1\$s desde %2\$s finalizará.

Explicación: La sesión ftp en el cortafuegos finaliza.

ICA2142 fw_tn_authenticate ha autenticado %1\$s satisfactoriamente.**ICA2143 La autenticación de fw_tn_authenticate para %1\$s ha resultado anómala.**

Explicación: fw_tn_authenticate no puede autenticar el ID de usuario especificado.

Acción del Sistema: Se ha rechazado la conexión.

Respuesta del Usuario: Si fw_tn_authenticate no tiene recursos de registro, el administrador debería examinar el archivo de registro para determinar la causa.

ICA2144 fw_tn_authenticate no ha devuelto un valor satisfactorio.

Explicación: El valor devuelto por fw_tn_authenticate no es cero. Podría faltar la función fw_tn_authenticate.

Acción del Sistema: Se ha rechazado la conexión.

Respuesta del Usuario: Examine fw_tn_authenticate con atención para ver si devuelve un valor que no sea cero y corríjalo si sucede esto. Si es el caso, vuelva a crear la biblioteca fwuser.o y colóquela en el cortafuegos.

ICA2145 El sistema ha devuelto el código de retorno %1\$s en el archivo %2\$s en la línea %3\$s.

Explicación: Una llamada del sistema ha resultado anómala. Puede que falte la biblioteca fwuser.o.

Acción del Sistema: La autenticación se ha cancelado anormalmente.

Respuesta del Usuario: Asegúrese de que /usr/lib/fwuser.o esté presente. Si lo está, póngase en contacto con su representante de IBM.

ICA2146 El fwuser.o suministrado por IBM no se ha sustituido.

Explicación: Está usando el fwuser.o suministrado por IBM porque no lo ha sustituido por su propio fwuser.o.

Acción del Sistema: La autenticación se ha cancelado anormalmente.

Respuesta del Usuario: Debería escribir y compilar su propia autenticación si ha definido un usuario para que use la autenticación suministrada por el usuario. El fwuser.o suministrado por IBM deniega el acceso a todos los usuarios que no lo sean de AIX y del cortafuegos.

ICA2147 fwtelnet: el usuario %1\$s ha iniciado una sesión transparente desde %2\$s (ubicación segura) a %3\$s.

Explicación: Mensaje generado al inicio de cada sesión del proxy transparente (fwtelnet). Una sesión empieza cuando el cortafuegos conoce el ID de usuario, el IP de origen y el IP de destino. Sólo se permite la sesión iniciada desde la ubicación segura.

Acción del Sistema: Permitir telnet transparente.

ICA2148 Atención -- Intento de conexión no autorizada para el usuario %1\$s desde %2\$s (ubicación no segura) a %3\$s, no está permitido.

Explicación: Generalmente indica un intento de establecer una conexión al cortafuegos a través de una interfaz no segura.

Acción del Sistema: Rechazar la conexión.

Respuesta del Usuario: Debería utilizar telnet desde la ubicación segura usando un Proxy transparente.

ICA2149 fwtelnet: se ha producido un LOGIN_ADAPTER_ERROR al iniciar una sesión telnet transparente desde %1\$s a %2\$s.

Explicación: Se ha producido un LOGIN_ADAPTER_ERROR al llamar a q_check_secure(0).

Acción del Sistema: Rechazar la conexión.

Respuesta del Usuario: Compruebe el adaptador seguro.

ICA2150 Error de Pftpd - %1\$s: código de retorno = 0x%2\$s

Explicación: El servidor pftpd ha detectado un error en la función indicada. El daemon está finalizando.

Respuesta del Usuario: Corrija el problema del sistema que se indica y vuelva a arrancar pftpd.

ICA2151 Conexión rechazada.

Explicación: Este mensaje debe mostrarse al usuario que intenta conectarse pero no está autorizado.

ICA2152 fwlogin: la grabación a %1\$s ha resultado anómala.

Explicación: No se puede grabar en el dispositivo.

ICA2153 fwlogin: la lectura de %1\$s ha resultado anómala.

Explicación: No se puede leer del dispositivo.

ICA2154 error en %1\$s con %2\$s.

Explicación: Este cortafuegos ha encontrado un problema.

ICA2155 Error de Pftpd - %1\$s: %2\$s

Explicación: El servidor pftpd ha detectado un error en la función indicada. El daemon está finalizando.

Respuesta del Usuario: Corrija el problema del sistema que se indica y vuelva a arrancar pftpd.

ICA2156 **Atención -- El usuario %1\$s ha intentado utilizar un ftp transparente desde la ubicación NO SEGURA %2\$s a %3\$s, no se ha permitido.**

Explicación: Generalmente indica un intento de establecer una conexión al cortafuegos a través de una interfaz no segura.

Acción del Sistema: Rechazar la conexión.

Respuesta del Usuario: Debería utilizar el ftp desde la ubicación segura usando un proxy transparente.

ICA2157 **El usuario %1\$s de %2\$s no tiene permitido utilizar proxy transparente para %3\$s.**

Explicación: Generalmente indica un intento de establecer una conexión con un cortafuegos mientras el Proxy transparente no está configurado.

Acción del Sistema: Rechazar la conexión.

Respuesta del Usuario: Active fwtp proxy ftp =

ICA2158 **La opción %1\$s se ha especificado incorrectamente.**

Explicación: El distintivo mencionado se ha especificado incorrectamente.

ICA2159 **No se ha especificado el valor de tiempo de espera de la opción -t.**

Explicación: Se debe suministrar un valor de tiempo de espera para la opción -t.

ICA2160 **Ha cambiado la contraseña del usuario %1\$s de %2\$s :%3\$s.**

Explicación: Un usuario FTP ha cambiado su contraseña satisfactoriamente en la base de datos de contraseñas.

Acción del Sistema: Ninguna

Respuesta del Usuario: Ninguna

ICA2161 **El usuario %1\$s ha intentado conectarse utilizando una contraseña caducada desde %2\$s :%3\$s.**

Explicación: Un usuario FTP ha intentado establecer una conexión con el cortafuegos utilizando una contraseña caducada.

Acción del Sistema: La validación de la conexión FTP no es satisfactoria y el usuario es devuelto al shell de mandatos FTP.

Respuesta del Usuario: El usuario debe volver a intentar validar a través del mandato USER de FTP o volviendo a establecer la conexión FTP y transmitir la cadena de la contraseña de la forma "antigua_contraseña/nueva_contraseña/nueva_contraseña".

ICA2162 **No se ha podido cambiar la contraseña del usuario %1\$s de %2\$s :%3\$s.**

Explicación: Un usuario FTP ha intentado cambiar su contraseña y la rutina de validación de la contraseña ha resultado anómala. Entre las posibles razones de la anomalía se incluye: - Se ha especificado una contraseña "antigua" no válida, - Sólo se ha especificado una aparición de la "nueva" contraseña, - Dos de las apariciones de la "nueva" contraseña no coinciden, o - El delimitador que se ha utilizado para separar las contraseñas no era "/".

Acción del Sistema: La validación de contraseña FTP resulta anómala y el usuario vuelve al shell de mandatos FTP.

Respuesta del Usuario: Intente volver a validarla con el servidor FTP, verificando que las contraseñas están escribiéndose correctamente. Si el problema persiste, póngase en contacto con el servicio técnico.

ICA2163 Se ha iniciado safemaid.

Explicación: Iniciando safemaid.

ICA2164 Se ha detenido safemaid.

Explicación: Deteniendo safemaid.

ICA2165 Sesión telnet interrumpida.

Explicación: La sesión Telnet está finalizando, pero no puede recuperar su información de la sesión desde el conducto. Probablemente, la sesión se ha interrumpido durante el arranque del cliente y por lo tanto no se ha inicializado completamente.

ICA2166 No se ha podido recuperar el atributo %1\$s del usuario %2\$s. Código de retorno = %3\$s.

Explicación: El servicio de autenticación no ha podido recuperar el atributo especificado de la base de datos de usuarios para el usuario especificado. Acción del sistema : La autenticación del usuario resulta anómala.

Respuesta del Usuario: Póngase en contacto con el administrador del sistema para corregir el registro de la base de datos del usuario.

ICA2167 La autenticación de %1\$s ha resultado anómala para %2\$s utilizando %3\$s desde %4\$s en %5\$s

Explicación: El usuario especificado no ha podido autenticarse para el servicio especificado mediante el método de autenticación especificado. El usuario ha solicitado el servicio desde la dirección y el tipo de red que se indican. Acción del sistema : La autenticación del usuario resulta anómala.

Respuesta del Usuario: Póngase en contacto con el administrador del sistema.

ICA2168 La autenticación de %1\$s ha resultado anómala para %2\$s debido a que no existía suficiente almacenamiento.

Explicación: El ID de usuario no ha podido autenticarse para el servicio porque se ha producido una anomalía de asignación de memoria durante el proceso de autenticación. Acción del sistema : La autenticación del usuario resulta anómala.

Respuesta del Usuario: Póngase en contacto con el administrador del sistema.

ICA2169 Autenticación satisfactoria del usuario %1\$s para %2\$s utilizando %3\$s desde %4\$s:%5\$s

Explicación: El cortafuegos ha autenticado el nombre del usuario indicado para el servicio solicitado utilizando el esquema de autenticación especificado.

ICA2170 La autenticación de %1\$s ha resultado anómala para %2\$s. %3\$s no está registrado al cortafuegos.

Explicación: El ID de usuario no ha podido autenticarse para el servicio. El método de autenticación solicitado no se ha registrado en el cortafuegos. Acción del sistema : La autenticación del usuario resulta anómala.

Respuesta del Usuario: Póngase en contacto con el administrador del sistema.

ICA2171 La cuenta %1\$s se ha bloqueado debido a que la contraseña ha caducado.

Explicación: La contraseña ha caducado y no se ha cambiado. Esta cuenta está bloqueada.

Acción del Sistema: La cuenta está bloqueada y las autenticaciones de contraseña del cortafuegos no resultarán satisfactorias. Respuesta del usuario

ICA2172 La cuenta %1\$s está bloqueada.

Explicación: Esta cuenta está bloqueada.

Acción del Sistema: La cuenta está bloqueada. Las autenticaciones de contraseña del cortafuegos no resultarán satisfactorias.

Respuesta del Usuario: Solicite al administrador del cortafuegos que desbloquee la cuenta.

ICA2173 El usuario ha intentado conectarse utilizando el nombre de usuario reservado %1\$s.

Explicación: El ID que ha especificado el usuario está reservado para que lo utilice el cortafuegos.

Acción del Sistema: Se ha rechazado la conexión.

Respuesta del Usuario: El administrador debería averiguar quién está utilizando este nombre de usuario.

ICA2174 La autenticación de %1\$s ha resultado anómala para %2\$s utilizando %3\$s desde %4\$s en %5\$s a causa de un error de proceso interno.

Explicación: El usuario especificado no ha podido autenticarse para el servicio especificado mediante el método de autenticación especificado. El usuario ha solicitado el servicio desde la dirección y el tipo de red que se indican. La petición de autenticación ha resultado anómala debido a un error de proceso interno. Acción del sistema : La autenticación del usuario resulta anómala.

Respuesta del Usuario: Póngase en contacto con el administrador del sistema.

ICA2175 La llamada de conexión de usuario de Windows NT ha resultado anómala para el usuario %1\$s. El último error ha sido %2\$s.

Explicación: La llamada a la API de conexión de usuario de Windows NT no ha podido autenticar el nombre del usuario especificado. Windows NT ha informado el último error tras producirse la conexión de usuario anómala. Acción del sistema : La autenticación del usuario resulta anómala.

Respuesta del Usuario: Póngase en contacto con el administrador del sistema.

ICA2176 El esquema de autenticación desconocido %1\$s ha sido definido para %2\$s utilizando %3\$s desde %4\$s.

Explicación: Se ha definido el esquema de autenticación especificado para el usuario indicado cuando se utilizaba el componente del cortafuegos señalado desde la red especificada, pero el esquema de autenticación no está actualmente registrado en el cortafuegos. Acción del sistema : La petición de autenticación del usuario resulta anómala.

Respuesta del Usuario: Póngase en contacto con el administrador del sistema.

ICA2177 La conexión SafeMail 0x%1\$s ha sido recibida desde %2\$s.

Explicación: SafeMail ha recibido una conexión de entrada del \nombre similar que se indica. El número de ID de conexión que se indica se \ha asignado para la realización del seguimiento. (Nivel de depuración)

Acción del Sistema: Se ha enviado una hebra para manejar esta \conexión.

ICA2178 Se ha establecido la sesión SafeMail 0x%1\$s de %2\$s a %3\$s.

Explicación: SafeMail ha establecido contacto con el servidor de correo \destinatario y está preparado para transferir correo. (Nivel de información)

Acción del Sistema: La transferencia de datos está a punto de empezar.

ICA2179 SafeMail ha reenviado %1\$s bytes en la conexión 0x%2\$s de %3\$s a %4\$s.

Explicación: SafeMail ha reenviado satisfactoriamente un mensaje entre los \dos servidores de correo que se indican. Esta sesión se identificó anteriormente en \un mensaje ICA2166. Este mensaje contenía el número de bytes \que se indica. (Nivel de información)

ICA2180 SafeMail ha finalizado la sesión 0x%1\$s de %2\$s.

Explicación: SafeMail ha rechazado la transferencia del correo que estaba enviándose en \la sesión indicada. (Nivel de información)

Acción del Sistema: La sesión ha finalizado.

Respuesta del Usuario: Aumente el nivel de prioridad del registro para obtener \información de diagnóstico más detallada .

ICA2181 SafeMail ha finalizado la sesión 0x%1\$s por el código de razón %2\$s.

Explicación: El procesador principal de SafeMail ha finalizado la sesión indicada \porque se ha detectado una condición de error primario. Entre los códigos de razón se incluyen: \01 - no es posible localizar el servidor de correo destinatario \02 - el remitente ha intentado direccionar el correo entre dos servidores no seguros \03 - el servidor de correo destinatario ha rechazado la conexión, podría estar desconectado \04 - el servidor de correo ha rechazado el correo \05 - se ha excedido el tiempo de espera de una o más conexiones; o el servidor de correo destinatario o \el servidor de correo remitente podría estar inactivo \06 - rcv() ha devuelto 0 bytes; o el servidor de correo destinatario o \el servidor de correo remitente podría estar inactivo \08 - se han recibido demasiados mandatos de error \09 - select() ha devuelto un valor negativo; o el servidor de correo destinatario o \el servidor de correo remitente podría estar inactivo \Este mensaje está registrado en el Nivel de depuración.

Acción del Sistema: La conexión ha finalizado.

ICA2182 SafeMail ha rechazado la sesión 0x%1\$s a causa de un comando %2\$s no válido, código de razón %3\$s.

Explicación: La subrutina de validación de mandatos de SafeMail ha detectado un \mandato no válido o peligroso. Estos códigos de razón varían para cada \mandato SMTP. Consulte la página de presentación de IBM Firewall Support para conocer los valores \actuales. (Nivel de depuración)

Acción del Sistema: La conexión ha finalizado.

Respuesta del Usuario: Corrija el cliente de correo remitente o el servidor de correo remitente \para que se envíe información válida y segura.

ICA2183 httpd --> El archivo de configuración del proxy HTTP (%1\$s) no está disponible.

Explicación: El daemon del proxy HTTP ha intentado abrir el archivo de configuración especificado, pero o no existe o no ha podido abrirse.

Acción del Sistema: El Proxy HTTP no se inicia

Respuesta del Usuario: Configure el proxy utilizando la GUI o el mandato fwhttp y vuelva a iniciar el proxy.

ICA2184 error signal() con señal %1\$s. Salida de safemaid.

Explicación: Se ha producido un error del sistema cuando el daemon safemaid intentaba establecer un manejador de señal.

ICA2185 El socket no ha podido abrirse. Salida de safemaid

Explicación: Anomalía al abrir el socket.

ICA2186 No ha podido vincularse el socket a la puerta. Salida de safemaid

Explicación: Anomalía al vincular el socket a la puerta.

ICA2187 No pueden aceptarse nuevas conexiones. Nuevo intento de safemaid

Explicación: Se ha producido una anomalía al aceptar una conexión nueva.

ICA2188 Se ha especificado una hora incorrecta (%1\$s) para -l.

Explicación: El valor de la hora que se muestra contiene caracteres fuera del rango numérico de 0 a 9 o excede el valor máximo permitido.

ICA2189 No se ha especificado el valor de tiempo de espera para la opción -l.

Explicación: Se debe especificar un valor de tiempo de espera para la opción -l.

ICA2200 (%1\$s:%2\$s) Error de inicialización de WinSocket : %3\$s

Explicación: Se ha producido un error al inicializar WinSocket.

Respuesta del Usuario: Corrija el problema del sistema que indica WSAGetLastError y vuelva a iniciar el servicio indicado (Primer parámetro).

ICA2201 (%1\$s:%2\$s) %3\$s ha resultado anómalo en la línea %4\$s : %5\$s

Explicación: El componente de Red especificado ha resultado anómalo

Respuesta del Usuario: Corrija el problema del sistema que indica WSAGetLastError y vuelva a iniciar el servicio indicado (Primer parámetro).

ICA2202 (%1\$s:%2\$s) %3\$s ha superado el tiempo de espera tras %4\$s segundos: %5\$s

Explicación: La función indicada ha excedido el tiempo de espera tras estar desocupada durante el período de tiempo especificado.

Respuesta del Usuario: Vuelva a establecer la conexión con el servicio indicado y dé una respuesta antes de que se exceda el tiempo indicado

ICA2203 (%1\$s:%2\$s) Error de memoria; %3\$s ha devuelto %4\$s en la línea %5\$s: %6\$s

Explicación: Se ha producido un error de memoria, generalmente por ser ésta insuficiente; WSASGetLastError

Respuesta del Usuario: Libere espacio de disco - consulte al Administrador del sistema

ICA2204 (%1\$s:%2\$s) error %3\$s: se ha denegado el acceso o la creación ha resultado anómala.

Explicación: El servicio indicado ha detectado un error al intentar acceder o crear el archivo especificado o el archivo que se asocia al parámetro del archivo.

Respuesta del Usuario: Asegúrese de que el nombre de archivo indicado exista y de que tenga los permisos correctos.

ICA2205 (%1\$s:%2\$s) El archivo %3\$s es necesario, pero no ha podido encontrarse.

Explicación: El archivo especificado no existe. La razón más probable de la anomalía es que se ha borrado la configuración por omisión del cortafuegos. Restaure el archivo a partir de una copia de seguridad actualizada.

Respuesta del Usuario: Verifique que no exista el archivo especificado. El programa de configuración espera este archivo para salir. Si no dispone de una versión de seguridad, póngase en contacto con el servicio técnico.

ICA2206 (%1\$s:%2\$s) El archivo de configuración %3\$s está corrupto.

Explicación: El archivo de configuración indicado no tiene un formato que pueda utilizarse. El contenido se ha dañado. La razón más probable de los daños es que el archivo se ha editado manualmente y se han añadido datos no válidos.

Respuesta del Usuario: Será necesario volver a crear el archivo de configuración correctamente. En primer lugar, catalogue el archivo (o cree una copia que pueda visualizarse) y, a continuación, borre el archivo original. Vuelva a configurar el archivo ejecutando el mandato de configuración del cortafuegos adecuado, utilizando el archivo original como referencia, si es necesario.

ICA2207 (%1\$s:%2\$s) El archivo de configuración %3\$s está vacío.

Explicación: El archivo de configuración indicado no se ha encontrado o se ha encontrado pero estaba vacío. La razón más probable que explique por qué no ha podido encontrarse el archivo es que no se ha realizado la configuración del servicio indicado.

Respuesta del Usuario: Verifique el estado del archivo de configuración. Si el archivo existe, el mandato de configuración espera que este archivo contenga datos. Consulte el manual para obtener información adicional.

ICA2208 %1\$s La sesión %2\$s se ha iniciado para %3\$s desde un adaptador no seguro (%4\$s:%5\$s).

Explicación: Mensaje que se genera al inicio de cada sesión indicada.

ICA2209 %1\$s La sesión %2\$s ha finalizado para %3\$s desde un adaptador no seguro (%4\$s:%5\$s); bytes %6\$s.

Explicación: Mensaje que se genera al final de cada sesión indicada. Los Bytes en total indican el número de bytes que se han transferido durante la sesión. Los servicios (por ejemplo, ptelnetd) que no den soporte a Bytes en total indicarán cero.

ICA2210 (%1\$s) El usuario %2\$s ha intentado conectarse utilizando una contraseña caducada desde %3\$s (no seguro).

Explicación: El usuario indicado ha intentado establecer una conexión con el cortafuegos utilizando la contraseña caducada indicada desde el IP de origen indicado en un adaptador no seguro.

Respuesta del Usuario: La contraseña indicada ha caducado por el conjunto de normas de contraseña. Póngase en contacto con el administrador del sistema.

ICA2211 (%1\$s) El usuario %2\$s ha intentado conectarse utilizando una contraseña caducada desde %3\$s (seguro).

Explicación: El usuario indicado ha intentado establecer una conexión con el cortafuegos utilizando la contraseña caducada indicada desde el IP de origen indicado en un adaptador seguro.

Respuesta del Usuario: La contraseña indicada ha caducado por el conjunto de normas de contraseña. Póngase en contacto con el administrador del sistema.

ICA2212 (%1\$s) El usuario %2\$s ha sido autenticado satisfactoriamente desde was %3\$s (seguro).

Explicación: El cortafuegos ha autenticado el nombre del usuario indicado desde el IP de origen indicado en un adaptador seguro.

ICA2213 (%1\$s) El usuario %2\$s ha sido autenticado satisfactoriamente desde was %3\$s (no seguro).

Explicación: El cortafuegos ha autenticado el nombre del usuario indicado desde el IP de origen indicado en un adaptador no seguro.

ICA2214 (%1\$s) La autenticación del usuario %2\$s ha resultado anómalo desde %3\$s (no seguro).

Explicación: El cortafuegos no ha autenticado satisfactoriamente el nombre del usuario indicado desde el IP de origen indicado en un adaptador no seguro.

Respuesta del Usuario: La causa más probable es que se ha escrito incorrectamente el nombre del usuario o la contraseña; los nombres de los usuarios y las contraseñas son sensibles a las mayúsculas y minúsculas (compruebe Bloq Mayús).

ICA2215 (%1\$s) La autenticación del usuario %2\$s ha resultado anómalo desde %3\$s (seguro).

Explicación: El cortafuegos no ha autenticado satisfactoriamente el nombre del usuario indicado desde el IP de origen indicado en un adaptador seguro.

Respuesta del Usuario: La causa más probable es que se ha escrito incorrectamente el nombre del usuario o la contraseña; los nombres de los usuarios y las contraseñas son sensibles a las mayúsculas y minúsculas (compruebe Bloq Mayús).

ICA2216 (%1\$s) El usuario %2\$s de %3\$s (no seguro) no ha escrito contraseñas coincidentes (verificación).

Explicación: Se ha solicitado, o era necesario, un cambio de contraseña y el usuario indicado del IP de origen que se especifica, en un adaptador no seguro, ha escrito contraseñas que no coincidían. Los datos de autenticación del usuario no han cambiado.

Respuesta del Usuario: El cambio de las contraseñas requiere la escritura de la contraseña dos veces, la segunda vez para verificarla; la causa más probable es que se ha escrito la verificación de la contraseña de forma incorrecta.

ICA2217 (%1\$s) El usuario %2\$s de %3\$s (seguro) no ha escrito contraseñas coincidentes (verificación).

Explicación: Se ha solicitado, o era necesario, un cambio de contraseña y el usuario indicado del IP de origen que se especifica, en un adaptador seguro, ha escrito contraseñas que no coincidían. Los datos de autenticación del usuario no han cambiado.

Respuesta del Usuario: El cambio de las contraseñas requiere la escritura de la contraseña dos veces, la segunda vez para verificarla; la causa más probable es que se ha escrito la verificación de la contraseña de forma incorrecta.

ICA2218 %1\$s La sesión %2\$s se ha iniciado para %3\$s desde un adaptador seguro (%4\$s:%5\$s).

Explicación: Mensaje que se genera al inicio de cada sesión indicada.

ICA2219 %1\$s La sesión %2\$s ha finalizado para %3\$s desde un adaptador seguro (%4\$s:%5\$s); bytes %6\$s.

Explicación: Mensaje que se genera al final de cada sesión indicada. Los Bytes en total indican el número de bytes que se han transferido durante la sesión. Los servicios (por ejemplo, ptelnetd) que no den soporte a Bytes en total indicarán cero.

ICA2220 (%1\$s) El usuario %2\$s ha iniciado una sesión proxy transparente desde %3\$s (ubicación segura) a %4\$s.

Explicación: Mensaje que se genera al inicio de cada sesión de proxy transparente. Una sesión empieza cuando el cortafuegos conoce el ID de usuario, el IP de origen y el IP de destino. Sólo se permite la sesión iniciada desde la ubicación segura.

Acción del Sistema: Permita el proxy transparente.

ICA2221 (%1\$s) Advertencia: El IP (%2\$s) del fin de línea de Control del similar no era igual al IP (%3\$s) del fin de línea de Datos del similar.

Explicación: Su finalidad es la Seguridad (es decir, la antipiratería) Asegúrese de que la Dirección IP del similar al que se conecta el socket de Conexión de control sea igual al IP del similar al que se conecta el socket de Conexión de datos. Pueden ser distintos si se utiliza el Asignador de tareas de la red o si el destino ha utilizado varios adaptadores

Acción del Sistema: Compruebe si el Servidor FTP de destino está utilizando varios adaptadores o si está utilizándose el Asignador de tareas de la red. Asegúrese de que los filtros sólo permitan direcciones IP válidas a través de las puertas 20 y 21.

ICA2222 (%1\$s) ¡Atención! Violación de protocolo. Se ha recibido un mandato no compatible con RFC %2\$s; Esperado %3\$s.

Explicación: El servicio indicado ha recibido una serie no esperada que no es compatible con la RFC asociada; posible presencia de un pirata.

Acción del Sistema: Utilice un Cliente que cumpla con la RFC del servicio indicado

ICA3001 *Alerta*: el usuario real es %1\$s, no %2\$s

Explicación: Posible intento de vulnerabilidad de la seguridad, el nombre de usuario no se ha autenticado.

ICA3006 %1\$s bytes de %2\$s, %3\$s bytes de %4\$s

Explicación: Mensaje que indica el número de bytes transferidos entre el daemon sockd y sus sistemas principales de cliente y servidor respectivos.

ICA3007 Se ha rechazado una conexión debido a que se ha excedido el número máximo de conexiones.

Explicación: El servidor de socks se ha configurado para aceptar sólo un número máximo determinado de sesiones de cliente. Este mensaje se genera cuando se ha alcanzado ese umbral y se reciben peticiones de conexión adicionales.

Acción del Sistema: Se cierra la conexión que se ha intentado más recientemente.

Respuesta del Usuario: El número máximo de conexiones simultáneas lo determina el parámetro SOCKS5_MAXCHILD en socks5.conf. Aumente este valor y renueve el servidor. Lea el manual de consulta del IBM Firewall para obtener más información. start unused

ICA3010 conectado -- Vincular desde %1\$s(%2\$s)@%3\$s para %4\$s (%5\$s)

Explicación: Se ha establecido la conexión.

ICA3011 conectado -- Conectar de %1\$s(%2\$s)@%3\$s a %4\$s (%5\$s)

Explicación: Conexión de socket satisfactoria con el exterior.

ICA3012 rechazado -- Conectar de %1\$s(%2\$s)@%3\$s a %4\$s (%5\$s)

Explicación: El sistema principal remoto ha rechazado la conexión.

ICA3013 select() %1\$s

Explicación: Error del sistema.

ICA3014 finalizado -- Vincular desde %1\$s(%2\$s)@%3\$s para %4\$s (%5\$s).(%6\$s bytes de %7\$s, %8\$s bytes de %9\$s)

Explicación: La conexión ha finalizado.

ICA3015 finalizado -- Conectar de %1\$s(%2\$s)@%3\$s a %4\$s (%5\$s).(%6\$s bytes de %7\$s, %8\$s bytes de %9\$s)

Explicación: La conexión al servidor ha finalizado.

ICA3016 *No puede encontrarse una interfaz adecuada para comunicarse con %1\$s**

Explicación: El archivo /etc/sockd.route no contiene información de direccionamiento para el sistema principal de destino especificado.

ICA3017 No puede ejecutarse el mandato de shell para pid %1\$s

Explicación: El daemon sockd no puede ejecutar un mandato /bin/sh.

Respuesta del Usuario: Compruebe que el shell /bin/sh esté disponible en el sistema.

ICA3018 rechazado -- Vincular desde %1\$s(%2\$s)@%3\$s para %4\$s

Explicación: El sistema principal remoto ha rechazado la conexión.

ICA3019 Error en GetDst() del sistema principal %1\$s: %2\$s

Explicación: Error al resolver la dirección de destino para la conexión solicitada.

ICA3022 Campo ?= no válido en la línea %1\$s

Explicación: Se ha encontrado una entrada no válida en el archivo /etc/sockd.conf.

ICA3023 Comparación no válida en la línea %1\$s

Explicación: Se ha encontrado una entrada no válida en el archivo `/etc/sockd.conf`.

ICA3024 Entrada no válida en la línea %1\$s

Explicación: Se ha encontrado una entrada no válida en el archivo `/etc/sockd.route`.

ICA3025 Campo permitir/denegar no válido en la línea %1\$s

Explicación: Se ha encontrado una entrada no válida en el archivo `/etc/sockd.conf`.

ICA3026 Número de puerta no válido en la línea %1\$s

Explicación: Se ha encontrado una entrada no válida en el archivo `/etc/sockd.conf`.

ICA3027 El mandato de shell ha resultado anómalo (%1\$s) para \"%2\$s\"

Explicación: El mandato de shell mostrado ha sido anómalo.

Respuesta del Usuario: Compruebe que el procesador del shell esté disponible en el sistema.

ICA3030 No ha podido abrirse el archivo de configuración (%1\$s)

Explicación: La petición de apertura del archivo indicado ha sido anómala.

ICA3031 No ha podido abrirse el archivo de direccionamiento (%1\$s): %2\$s

Explicación: La petición de apertura del archivo indicado ha sido anómala.

Respuesta del Usuario: Consulte al administrador del cortafuegos. Durante la instalación del cortafuegos se ha proporcionado un archivo por omisión.

ICA3032 No puede abrirse el archivo de usuario (%1\$s): %2\$s

Explicación: El nombre de archivo especificado para `*=userlist` en una norma de permiso no se ha podido encontrar.

ICA3033 Resultado no esperado de Validate()

Explicación: Se ha especificado la verificación de `Identd` del nombre de usuario, `Identd` ha respondido con un resultado no esperado.

ICA3035 No puede conectarse a identd en %1\$s

Explicación: Se ha especificado la verificación de `Identd` del nombre de usuario, pero `Identd` no ha respondido.

ICA3039 Error -- el mandato de shell \"%1\$s\" no contiene ningún carácter alfanumérico.

Explicación: Mandato del shell no válido, consulte el mensaje del registro.

ICA3040 Error -- shell_cmd fork() %1\$s

Explicación: El daemon `sockd` no ha podido cambiar al proceso inferior mediante `'fork()'`

ICA3041 Error -- no puede obtenerse la dirección del cliente.

Explicación: Retorno de error de la llamada `'getpeername()'`.

Respuesta del Usuario: Compruebe el direccionamiento y la configuración del DNS.

ICA3042 Error -- mandato no definido (0x%1\$s) del sistema principal %2\$s

Explicación: Se ha recibido un mandato no válido de la aplicación del cliente.

Respuesta del Usuario: Posible problema de configuración del cliente o discrepancia en el nivel de soporte del cliente y del cortafuegos.

ICA3043 Error -- versión errónea (0x%1\$s) del sistema principal %2\$s.

Explicación: El cortafuegos admite la versión 4.2. de socks

Respuesta del Usuario: Posible problema de configuración del cliente o discrepancia en el nivel de soporte del cliente y del cortafuegos.

ICA3044 Error -- Conectar de %1\$s(%2\$s)@%3\$s a %4\$s (%5\$s). Código de error: %6\$s %7\$s.

Explicación: Error en la petición de conexión.

ICA3045 Error -- Vincular desde %1\$s(%2\$s)@%3\$s para %4\$s. Error: conectado a sistema principal erróneo %5\$s (%6\$s).

Explicación: Error en la petición de vinculación.

ICA3046 Error -- Vincular desde %1\$s(%2\$s)@%3\$s para %4\$s. Código de error: %5\$s %6\$s.

Explicación: Error en la petición de vinculación.

ICA3047 Tiempo de espera excedido -- Vincular desde %1\$s(%2\$s)@%3\$s para %4\$s

Explicación: La conexión ha excedido el tiempo de espera.

ICA3048 El mandato de shell es demasiado largo: %1\$s...

Explicación: El mandato que se debe ejecutar, del archivo /etc/sockd.conf, es demasiado largo.

ICA3049 Tiempo de espera excedido -- Conectar de %1\$s(%2\$s)@%3\$s a %4\$s (%5\$s)

Explicación: La conexión ha excedido el tiempo de espera.

ICA3050 %1\$s

Explicación: Norma de filtro del archivo /etc/sockd.conf que coincide con la conexión socks.

ICA3051 AIX sockd_route() no puede encontrar la interfaz para %1\$s.

Explicación: No se ha podido encontrar la información de direccionamiento de interfaz.

ICA3052 Error al establecer el ID de usuario en "nadie".

Explicación: No se ha podido establecer el id de usuario del proceso sockd inferior en "nadie".

ICA3053 Error en popen (script de direccionamiento de AIX): %1\$s

Explicación: Error al ejecutar el script para encontrar la información de direccionamiento.

ICA3054 Anomalía de asignación de memoria muy grave en AIX sockd_route().

Explicación: Anomalía de asignación de memoria al intentar reunir información de direccionamiento.

ICA3055 Error AIX sockd_route() muy grave al analizar el primer espacio en: %1\$s

Explicación: Error al analizar la información de direccionamiento del sistema.

ICA3056 Error AIX sockd_route() muy grave al analizar el segundo espacio en: %1\$s

Explicación: Error al analizar la información de direccionamiento del sistema.

ICA3057 Error muy grave en AIX sockd_route() al leer salida de script de direccionamiento: %1\$s

Explicación: Error al leer la salida del script.

ICA3058 Error en popen (script de adaptador de AIX): %1\$s

Explicación: Error al ejecutar el script para encontrar la información de la interfaz.

ICA3101 Error de sockd al enviar datos - select(): %1\$s

Explicación: (SOCKS422) Error al enviar datos.

ICA3102 Error de sockd al enviar datos - write(): %1\$s

Explicación: (SOCKS422) Error al enviar datos.

ICA3103 Error de sockd al recibir datos - select(): %1\$s

Explicación: (SOCKS422) Error al recibir datos.

ICA3104 Error de sockd al recibir datos - read(): %1\$s

Explicación: (SOCKS422) Error al recibir datos.

ICA3105 No puede crearse el archivo de ID de proceso %1\$s.

Explicación: (SOCKS422) Error en la creación/escritura del archivo de id de proceso.

ICA3106 Sockd no ha podido ejecutar fork para el inferior: %1\$s

Explicación: (SOCKS422) Error en el intento de ejecutar fork para el inferior para manejar una petición SOCKS.

ICA3107 La opción de definición de socket de entrada SO_LINGER ha resultado anómala: %1\$s

Explicación: (SOCKS422) no crítico

ICA3108 La opción de definición de socket de salida SO_LINGER ha resultado anómala: %1\$s

Explicación: (SOCKS422) no crítico

ICA3109 Entrada no válida en la línea %1\$s en el archivo %2\$s.

Explicación: (SOCKS422) Sintaxis de entrada de configuración incorrecta.

ICA3110 Campo de interfaz no permitido en la línea %1\$s en el archivo %2\$s.

Explicación: (SOCKS422) Sintaxis de entrada de configuración incorrecta.

ICA3111 IP de destino no permitido en la línea %1\$s en el archivo %2\$s.

Explicación: (SOCKS422) Sintaxis de entrada de configuración incorrecta.

ICA3112 Máscara de destino no permitida en la línea %1\$s en el archivo %2\$s.

Explicación: (SOCKS422) Sintaxis de entrada de configuración incorrecta.

ICA3113 Se han analizado %1\$s líneas en el archivo %2\$s.

Explicación: (SOCKS422) Sintaxis de entrada de configuración incorrecta.

ICA3114 No se ha encontrado ninguna línea válida en el archivo %1\$s.

Explicación: (SOCKS422) Archivo de configuración vacío o sintaxis incorrecta.

Respuesta del Usuario: Corrija el archivo de configuración indicado.

ICA3115 Campo 'permitir/denegar' no válido en la línea %1\$s en el archivo %2\$s.

Explicación: (SOCKS422) Sintaxis de entrada de configuración incorrecta.

ICA3116 Campo '?=' no válido en la línea %1\$s en el archivo %2\$s.

Explicación: (SOCKS422) Sintaxis de entrada de configuración incorrecta.

ICA3117 IP de origen no permitido en la línea %1\$s en el archivo %2\$s.

Explicación: (SOCKS422) Sintaxis de entrada de configuración incorrecta.

ICA3118 Máscara de origen no permitida en la línea %1\$s en el archivo %2\$s.

Explicación: (SOCKS422) Sintaxis de entrada de configuración incorrecta.

ICA3119 Comparación no válida en la línea %1\$s en el archivo %2\$s.

Explicación: (SOCKS422) Sintaxis de entrada de configuración incorrecta.

ICA3120 Número de puerta no válido en la línea %1\$s en el archivo %2\$s.

Explicación: (SOCKS422) Sintaxis de entrada de configuración incorrecta.

ICA3121 Se ha recibido SIGUSR1 - volcando configuración de socks.

Explicación: (SOCKS422) Señal para volcar la configuración activa al archivo de registro después de este mensaje.

ICA3122 Sockd no ha podido ejecutar fork para daemon: %1\$s

Explicación: (SOCKS422) Error en fork para inicializar el daemon sockd.

Respuesta del Usuario: Corrija el problema de sistema indicado y reinicie sockd.

ICA3123 Servidor sockd iniciándose.

Explicación: (SOCKS422) Sockd se ha inicializado satisfactoriamente y está esperando las conexiones.

ICA3124 Error de inicialización de sockd muy grave - bind(): %1\$s

Explicación: (SOCKS422) La inicialización del servidor sockd ha terminado.

Respuesta del Usuario: Corrija el problema de sistema indicado y reinicie sockd.

ICA3125 Error de inicialización de sockd muy grave - listen(): %1\$s

Explicación: (SOCKS422) La inicialización del servidor sockd ha terminado.

Respuesta del Usuario: Corrija el problema de sistema indicado y reinicie sockd.

ICA3126 Error sockd muy grave - main accept(): %1\$s

Explicación: (SOCKS422) La rutina principal del servidor sockd ha resultado anómala, el daemon ha finalizado.

Respuesta del Usuario: Corrija el problema de sistema indicado y reinicie sockd.

ICA3127 El servidor sockd ha recibido una señal de terminación.

Explicación: El usuario raíz o nadie ha matado el proceso, daemon terminado.

Respuesta del Usuario: Reinicie sockd si el administrador así lo quiere (escriba "sockd").

ICA3128 Error de inicialización de sockd muy grave - socket(): %1\$s

Explicación: La inicialización del servidor sockd ha resultado anómala, el daemon ha finalizado.

Respuesta del Usuario: Corrija el problema de sistema indicado y reinicie sockd.

ICA3129 Error de inicialización muy grave de sockd - %1\$s: %2\$s

Explicación: La inicialización del servidor sockd ha resultado anómala en la función indicada, el daemon ha finalizado.

Respuesta del Usuario: Corrija el problema de sistema indicado y reinicie sockd.

ICA3130 Error de Sockd - %1\$s: %2\$s

Explicación: El servidor sockd ha detectado un error en la función indicada. El daemon continúa, pero las conexiones pueden ser rechazadas o finalizadas.

Respuesta del Usuario: Si el problema persiste, detenga sockd, corrija el problema del sistema indicado y reinicie sockd.

ICA3131 Error al leer %1\$s. Se utilizarán los datos colocados anteriormente en la antememoria.

Explicación: No se ha podido leer el archivo o contiene datos incorrectos. Un mensaje anterior debería describir este problema. Sockd seguirá funcionando con los datos almacenados en la antememoria de la versión anterior del archivo.

Respuesta del Usuario: Corrija el error en el archivo indicado.

ICA3132 Distintivo desconocido -%1\$s.

Explicación: No se reconoce el distintivo mencionado, el daemon finalizará.

Respuesta del Usuario: Corrija la sintaxis y reinicie sockd.

ICA3133 Parámetro desconocido %1\$s.

Explicación: No se reconoce el parámetro mencionado, el daemon finalizará.

Respuesta del Usuario: Corrija la sintaxis y reinicie sockd.

ICA3134 Opciones en conflicto %1\$s y %2\$s.

Explicación: Las opciones indicadas no se pueden especificar juntas, el daemon ha terminado.

Respuesta del Usuario: Corrija la sintaxis y reinicie sockd.

ICA3135 Error de Sockd - %1\$s: código de retorno = 0x%2\$s

Explicación: El servidor sockd ha detectado un error en la función indicada. El daemon está finalizando.

Respuesta del Usuario: Corrija el problema de sistema indicado y reinicie sockd.

ICA3700 Error de inicialización de WinSocket : %1\$s

Explicación: Se ha producido un error al inicializar WinSocket.

Respuesta del Usuario: Corrija el problema de sistema indicado y reinicie sockd.

ICA4000 %1\$s - Advertencia: Se ha recibido la señal %2\$s, finalizando...

Explicación: Finalización debida a la recepción de la señal.

ICA4001 PARAR %1\$s como PID %2\$s

Explicación: Se muestra la conclusión del daemon. Mensaje informativo.

ICA4002 ID temporal

Explicación: Mensaje informativo.

ICA4003 Problema con el proceso inferior %1\$s.

Explicación: No se ha podido crear un proceso inferior.

ICA4004 Error muy grave. Finalizando fwpagerd con la señal %1\$s.

Explicación: Manejador de señal.

ICA4005 No existe ningún daemon fwpagerd en ejecución, %1\$s no se ha encontrado.

Explicación: No se ha podido enviar un mensaje a un buscapersonas porque el daemon no estaba activo.

ICA4006 No existe ningún daemon fwpagerd en ejecución con el ID de proceso %1\$s.

Explicación: No se ha podido encontrar el ID de proceso del proceso del daemon.

ICA4007 INICIAR %1\$s como PID %2\$s

Explicación: Se muestra la información de inicio. Mensaje informativo.

ICA4008 No ha podido establecerse sigignore para SIGPIPE.

Explicación: Anomalía durante la configuración para ignorar la señal de conducto interrumpido.

ICA4009 No ha podido establecerse sigset para SIGCHLD.

Explicación: Anomalía durante la configuración para retener una señal inferior que se desvanece.

ICA4010 No ha podido establecerse el proceso de terminación.

Explicación: Anomalía para establecer la señal para retener la señal de terminación.

ICA4011 El socket no ha podido abrirse.

Explicación: Anomalía al abrir el socket.

ICA4012 No ha podido establecerse sigset para SIGTERM.

Explicación: Anomalía durante la configuración para retener las señales SIGTERM y SIGINT.

ICA4013 No ha podido establecerse la opción de reutilización del socket.

Explicación: Anomalía al establecer la opción de reutilización del socket.

ICA4014 No ha podido establecerse la opción linger para el socket.

Explicación: Anomalía al establecer la opción linger del socket.

ICA4015 No ha podido vincularse el socket a la puerta.

Explicación: Anomalía al vincular el socket a la puerta.

ICA4016 No ha podido establecerse la opción listen en el socket.

Explicación: Anomalía durante la configuración para la opción listen en el socket.

ICA4017 El servicio %1\$s está utilizando el socket TCP %2\$s.

Explicación: Mensaje informativo.

ICA4018 La llamada a la función select() ha resultado anómala.

Explicación: Anomalía en la llamada a la función interna.

ICA4019 Error grave de new_work().

Explicación: Error grave interno de la rutina new_work.

ICA4020 Error(%1\$s): No ha podido grabarse en el socket de corriente: %2\$s

Explicación: Posible error del sistema.

Respuesta del Usuario: Compruebe el uso el socket.

ICA4021 Problema al recibir la respuesta.

Explicación: Problema al recibir la respuesta del módem.

Respuesta del Usuario: Compruebe las conexiones del módem y la cadena de inicialización.

ICA4022 La petición ha resultado satisfactoria.

Explicación: Mensaje informativo.

ICA4023 La petición no ha resultado satisfactoria.

Explicación: La petición para enviar un mensaje a un buscapersonas ha resultado anómala.

ICA4024 Error(%1\$s): La prioridad está fuera de rango (%2\$s - %3\$s).

Explicación: Rango de prioridad incorrecto.

Respuesta del Usuario: Rango de prioridad correcto. Los valores válidos van de -1 a 5.

ICA4025 Error(%1\$s): La dirección debe tener el formato ID@proveedor_de_telefonía cuando se utiliza la opción -n.

Explicación: Sintaxis de uso de mandato incorrecta.

Respuesta del Usuario: Sintaxis de utilización de mandato incorrecta.

ICA4026 Error(%1\$s): Sistema principal desconocido %2\$s

Explicación: No se ha podido resolver el nombre de sistema principal.

Respuesta del Usuario: Compruebe el nombre de sistema principal.

ICA4027 Error(%1\$s): No ha podido abrirse el socket de corriente: %2\$s

Explicación: No se ha podido crear un nuevo socket.

ICA4028 Error(%1\$s): No han podido establecerse las opciones de socket: %2\$s

Explicación: No ha podido establecerse la opción linger para el socket.

ICA4029 Error(%1\$s): No ha podido conectarse a %2\$s : %3\$s.

Explicación: No ha podido conectarse al sistema principal.

Respuesta del Usuario: Compruebe la configuración de la puerta serie y que exista el archivo controlador del dispositivo.

ICA4030 Error(%1\$s): No ha podido grabarse en el socket de corriente: %2\$s.

Explicación: No ha podido grabarse en el socket de corriente.

ICA4031 Problema al recibir la respuesta. La condición del mensaje se desconoce.

Explicación: Problema al recibir la respuesta del módem.

ICA4032 El mensaje se ha enviado satisfactoriamente a la cola.

Explicación: Mensaje informativo. El mensaje se ha enviado a la cola.

ICA4033 El mensaje ha resultado anómalo. No se ha enviado ningún mensaje.

Explicación: No ha podido enviarse el mensaje a la cola del buscapersonas.

ICA4034 %1\$s Erróneo (ID %2\$s Pri %3\$s Seg %4\$s Intent %5\$s) %6\$s %7\$s: %8\$s.

Explicación: Este mensaje se visualiza cuando el mensaje no se ha enviado satisfactoriamente al buscapersonas.

ICA4035 No se ha podido recolocar el mensaje en fila de espera %1\$s de %2\$s a %3\$s.

Explicación: No ha podido enviarse a la cola del buscapersonas.

ICA4036 SATISFACTORIO (ID %1\$s Pri %2\$s Seg %3\$s Intent %4\$s) %5\$s %6\$s: %7\$s.

Explicación: Este mensaje se visualiza cuando el mensaje se ha enviado satisfactoriamente al buscapersonas. Mensaje informativo.

ICA4037 VUELCO en %1\$s (ID %2\$s Pri %3\$s Seg %4\$s Intent %5\$s) %6\$s %7\$s: %8\$s.

Explicación: Los mensajes a un buscapersonas que no se envían inmediatamente se vuelcan a un archivo para intentarlo más tarde.

ICA4038 No ha podido grabarse en el archivo de vuelco %1\$s.

Explicación: No se puede grabar en el archivo de vuelco.

Respuesta del Usuario: Compruebe los permisos del sistema de archivos.

ICA4039 IpcKey: 0x%1\$s

Explicación: Mensaje informativo.

ICA4040 Tiempo de reintento de %1\$s minutos excedido.

Explicación: No ha podido inicializarse el módem transcurridos los minutos especificados.

Respuesta del Usuario: Compruebe la cadena de inicialización.

ICA4041 Se ha encontrado un mensaje alfanumérico para un buscapersonas numérico.

Explicación: Los buscapersonas numéricos no pueden contener datos alfanuméricos.

Respuesta del Usuario: Realice las correcciones utilizando el menú smitty/SMIT.

ICA4042 La persona no puede recibir mensajes en el buscapersonas.

Explicación: Probablemente el buscapersonas no está activado.

Respuesta del Usuario: Compruebe si el buscapersonas está activado.

ICA4043 El proveedor de telefonía %1\$s no existe.

Explicación: El proveedor de telefonía especificado no existe.

Respuesta del Usuario: Realice las correcciones utilizando el menú smitty/SMIT.

ICA4044 El proveedor de telefonía %1\$s no tiene ningún número de teléfono DTMF.

Explicación: El proveedor de telefonía no tiene ningún número de teléfono DTMF.

Respuesta del Usuario: Realice las correcciones utilizando el menú smitty/SMIT.

ICA4045 El número del buscapersonas %1\$s es demasiado largo para el máximo del proveedor de telefonía de %2\$s.

Explicación: El número del buscapersonas es demasiado largo para el máximo del proveedor de telefonía.

Respuesta del Usuario: Utilice otro número de buscapersonas más corto que el máximo del proveedor de telefonía.

ICA4046 El número del buscapersonas %1\$s es demasiado largo para la longitud por omisión de %2\$s.

Explicación: Este mensaje se produce cuando la longitud por omisión es demasiado pequeña.

Respuesta del Usuario: Realice las correcciones utilizando el menú smitty/SMIT. Aumente la longitud por omisión.

ICA4047 Problema en la línea %1\$s del archivo del módem %2\$s.

Explicación: El archivo de definición del módem contiene un carácter que no es válido.

Respuesta del Usuario: Realice las correcciones utilizando el menú smitty/SMIT.

ICA4048 El módem no ha podido abrirse en el dispositivo /dev/%1\$s.

Explicación: No ha podido abrirse el módem en el dispositivo especificado.

Respuesta del Usuario: Compruebe o vuelva a configurar la puerta serie. Compruebe el dispositivo.

ICA4049 Módem abierto en /dev/%1\$s.

Explicación: Mensaje informativo. El módem se ha detectado satisfactoriamente en la puerta serie.

ICA4050 No han podido establecerse las características del módem.

Explicación: Anomalía al intentar establecer las características del módem.

Respuesta del Usuario: Compruebe la cadena de inicialización del módem.

ICA4051 El módem no ha podido inicializarse tras %1\$s reintentos.

Explicación: El módem no se ha podido inicializar.

Respuesta del Usuario: Compruebe la cadena de inicialización del módem y la configuración de la puerta serie.

ICA4052 No ha podido marcarse el número del buscapersonas %1\$s

Explicación: No se puede marcar el número del buscapersonas.

Respuesta del Usuario: Compruebe la validez del número del buscapersonas.

ICA4053 No se ha podido colgar el módem.

Explicación: No se ha podido colgar el módem.

Respuesta del Usuario: Compruebe la cadena de inicialización del módem y el mandato para colgar.

ICA4054 No ha podido marcarse el mensaje %1\$s

Explicación: No ha podido marcarse el mensaje.

ICA4055 Problema en la línea %1\$s en el archivo del módem %2\$s.

Explicación: El archivo de definición del módem no es válido.

Respuesta del Usuario: Realice las correcciones utilizando el menú smitty/SMIT.

ICA4056 No ha podido marcarse el número DTMF del proveedor de telefonía %1\$s (%2\$s).

Explicación: Es posible que se haya cambiado el número DTMF o que sea incorrecto para este proveedor de telefonía.

Respuesta del Usuario: Realice las correcciones utilizando el menú smitty/SMIT.

ICA4057 El bloque no ha podido transmitirse.

Explicación: Anomalía al intentar transmitir el bloque.

Respuesta del Usuario: Compruebe los parámetros del proveedor de telefonía utilizando el menú smitty/SMIT.

ICA4058 No existe ninguna respuesta para el bloque transmitido.

Explicación: No se ha podido establecer una respuesta del proveedor de telefonía después de transmitir el bloque.

Respuesta del Usuario: Compruebe los parámetros del proveedor de telefonía utilizando el menú smitty/SMIT.

ICA4059 No ha podido recibirse la respuesta a la entrega del mensaje.

Explicación: No se ha podido obtener una respuesta del proveedor de telefonía después de la entrega del mensaje.

Respuesta del Usuario: Compruebe los parámetros del proveedor de telefonía utilizando el menú smitty/SMIT.

ICA4060 El id del buscapersonas no ha podido transmitirse.

Explicación: El id del buscapersonas no ha podido transmitirse.

Respuesta del Usuario: Compruebe el número de buscapersonas y los parámetros del proveedor de telefonía utilizando el menú smitty/SMIT.

ICA4061 No ha podido transmitirse el fin de <CR> de la petición de modalidad automática.

Explicación: No ha podido transmitirse el fin de <CR> de la petición de modalidad automática.

Respuesta del Usuario: Compruebe los parámetros del proveedor de telefonía utilizando el menú smitty/SMIT.

ICA4062 No ha podido transmitirse la petición de modalidad automática.

Explicación: No ha podido transmitirse la señal de la petición de modalidad automática.

Respuesta del Usuario: Compruebe los parámetros del proveedor de telefonía utilizando el menú smitty/SMIT.

ICA4063 No ha podido recibirse la indicación de continuación del proveedor de telefonía %1\$s tras %2\$s reintentos.

Explicación: El proveedor puede estar ocupado en este momento.

Respuesta del Usuario: Compruebe los parámetros del proveedor de telefonía utilizando el menú smitty/SMIT e inténtelo más tarde.

ICA4064 Error de comunicaciones durante la solicitud con el proveedor de telefonía %1\$s.

Explicación: El error de comunicaciones se puede deber a varias razones. Inténtelo más tarde.

Respuesta del Usuario: Compruebe los parámetros del proveedor de telefonía utilizando el menú smitty/SMIT e inténtelo más tarde.

ICA4065 No ha podido recibirse la respuesta a la conexión.

Explicación: El módem no ha podido recibir la respuesta a la conexión.

Respuesta del Usuario: Compruebe la cadena de inicialización del módem y los parámetros del proveedor de telefonía.

ICA4066 El proveedor de telefonía %1\$s no ha respondido al intento de conexión.

Explicación: El proveedor de telefonía no ha respondido al intento de conexión.

Respuesta del Usuario: Compruebe los parámetros del proveedor de telefonía utilizando el menú smitty/SMIT e inténtelo más tarde.

ICA4067 El proveedor de telefonía %1\$s ha dicho %2\$s.

Explicación: El proveedor de telefonía ha transmitido algún mensaje de error o mensaje de ocupado.

Respuesta del Usuario: Compruebe los parámetros del proveedor de telefonía utilizando el menú smitty/SMIT e inténtelo más tarde.

ICA4068 El proveedor de telefonía %1\$s ha forzado una desconexión durante la conexión.

Explicación: El proveedor de telefonía ha forzado una desconexión durante la conexión.

Respuesta del Usuario: Compruebe los parámetros del proveedor de telefonía utilizando el menú smitty/SMIT.

ICA4069 Vuelco de mensajes al proveedor de telefonía %1\$s debido a %2\$s bucles de reintento.

Explicación: Si el proveedor de telefonía está ocupado, el programa vuelca los mensajes del buscapersonas y lo intenta más tarde.

ICA4070 Salto de mensajes al proveedor de telefonía %1\$s debido a %2\$s intentos de conexión de sesión.

Explicación: No puede contactarse con el proveedor de telefonía después de varios intentos.

Respuesta del Usuario: Compruebe los parámetros del proveedor de telefonía e inténtelo más tarde.

ICA4071 Error(%1\$s): No ha podido asignarse memoria para el reintento del proveedor de telefonía: %2\$s.

Explicación: Es posible que haya errores del sistema o de asignación de memoria.

ICA4072 Error(%1\$s): No ha podido añadirse a la lista de reintentos del proveedor de telefonía: %2\$s.

Explicación: Posiblemente el proveedor de telefonía no exista.

Respuesta del Usuario: Compruebe la validez del proveedor de telefonía y vuelva a intentarlo.

ICA4073 La conexión de datos al proveedor de telefonía %1\$s del %2\$s ha resultado anómala tras %3\$s reintentos.

Explicación: La conexión de datos ha resultado anómala.

Respuesta del Usuario: Compruebe las conexiones del módem y los parámetros del proveedor de telefonía utilizando el menú smitty/SMIT.

ICA4074 La solicitud de ID del proveedor de telefonía %1\$s no se ha recibido tras %2\$s reintentos.

Explicación: El proveedor de telefonía no ha podido responder con una solicitud de ID o de acuse de recibo.

Respuesta del Usuario: Asegúrese de que el proveedor de telefonía utilice el protocolo TeleAlfanumérico.

ICA4075 Error de comunicaciones durante la conexión con el proveedor de telefonía %1\$s.

Explicación: El error de comunicaciones se puede deber a varias razones.

Respuesta del Usuario: Compruebe los parámetros del proveedor de telefonía utilizando el menú smitty/SMIT.

ICA4076 Se ha excedido el máximo de intentos de conexión para el proveedor de telefonía %1\$s.

Explicación: El proveedor no ha respondido durante los intentos especificados.

Respuesta del Usuario: Compruebe los parámetros del proveedor de telefonía e inténtelo más tarde.

ICA4077 No se ha recibido el mensaje de continuación del proveedor de telefonía %1\$s.

Explicación: El proveedor no ha respondido con una petición de continuación.

Respuesta del Usuario: Compruebe los parámetros del proveedor de telefonía e inténtelo más tarde.

ICA4078 No han podido crearse los bloques.

Explicación: El proveedor de telefonía no ha podido crear bloques para la transmisión.

Respuesta del Usuario: Compruebe los parámetros del proveedor de telefonía utilizando el menú smitty/SMIT.

ICA4079 El proveedor de telefonía %1\$s no ha respondido a la entrega del mensaje.

Explicación: El proveedor de telefonía ha tenido problemas al entregar el mensaje.

Respuesta del Usuario: Compruebe los parámetros del proveedor de telefonía utilizando el menú smitty/SMIT.

ICA4080 El proveedor de telefonía %1\$s ha forzado una desconexión durante la entrega del mensaje.

Explicación: El proveedor de telefonía ha forzado una desconexión durante la entrega del mensaje.

Respuesta del Usuario: Compruebe los parámetros del proveedor de telefonía y la cadena de inicialización del módem.

ICA4081 El proveedor de telefonía %1\$s ha rechazado el mensaje o el ID del buscapersonas.

Explicación: El proveedor de telefonía ha rechazado el mensaje o el id del buscapersonas.

Respuesta del Usuario: Compruebe la validez del id del buscapersonas, la activación del buscapersonas y los parámetros del proveedor de telefonía.

ICA4082 Error de comunicaciones durante la entrega del mensaje al proveedor de telefonía %1\$s.

Explicación: El error de comunicaciones se puede deber a varias razones.

Respuesta del Usuario: Compruebe los parámetros del proveedor de telefonía utilizando el menú smitty/SMIT.

ICA4083 No ha podido recibirse la confirmación del proveedor de telefonía %1\$s tras %2\$s reintentos.

Explicación: Este mensaje se produce si el proveedor de telefonía está ocupado o no se puede establecer una conexión.

Respuesta del Usuario: Compruebe los parámetros del proveedor de telefonía utilizando el menú smitty/SMIT y vuelva a intentarlo después de unos minutos.

ICA4084 No ha podido transmitirse <EOT>.

Explicación: El módem no ha podido transmitir <EOT>.

Respuesta del Usuario: Compruebe las conexiones del módem y la cadena de inicialización.

ICA4085 No ha podido recibirse la respuesta a <EOT>.

Explicación: El módem no ha podido recibir la respuesta a <EOT>.

Respuesta del Usuario: Compruebe las conexiones del módem y la cadena de inicialización.

ICA4086 El proveedor de telefonía %1\$s no ha respondido a <EOT>.

Explicación: El proveedor de telefonía no ha podido responder a los datos transmitidos.

Respuesta del Usuario: Compruebe la validez del proveedor de telefonía y las conexiones del módem.

ICA4087 El proveedor de telefonía %1\$s ha respondido con un error no aceptable de datos debido a los contenidos.

Explicación: El proveedor de telefonía no ha podido responder a los datos transmitidos.

Respuesta del Usuario: Compruebe los parámetros del proveedor de telefonía utilizando el menú smitty/SMIT.

ICA4088 No ha podido abrirse el archivo de valores por omisión %1\$s.

Explicación: Es posible que el archivo de valores por omisión del módem no exista o tenga permisos incorrectos.

Respuesta del Usuario: Compruebe los permisos y que el archivo exista.

ICA4089 Archivo de valores por omisión %1\$s incompleto.

Explicación: Faltan datos en el archivo de valores por omisión.

Respuesta del Usuario: Realice las correcciones utilizando el menú smitty/SMIT.

ICA4090 El número de línea externa no es válido en el archivo de valores por omisión %1\$s en la línea %2\$s.

Explicación: El archivo de la base de datos del proveedor de telefonía tiene un número de línea externa que no es válido.

Respuesta del Usuario: Limpie el archivo de la base de datos del proveedor de telefonía.

ICA4091 Valor de velocidad en baudios no válido en el archivo de valores por omisión %1\$s en la línea %2\$s.

Explicación: El archivo de la base de datos del proveedor de telefonía tiene una velocidad en baudios que no es válida.

Respuesta del Usuario: Limpie el archivo de la base de datos del proveedor de telefonía.

ICA4092 Valor de bits de datos no válido en el archivo de valores por omisión %1\$s en la línea %2\$s.

Explicación: El archivo de la base de datos del proveedor de telefonía tiene un valor de bits de datos que no es válido.

Respuesta del Usuario: Limpie el archivo de la base de datos del proveedor de telefonía.

ICA4093 Valor de paridad no válido en el archivo de valores por omisión %1\$s en la línea %2\$s.

Explicación: El archivo de la base de datos del proveedor de telefonía tiene un valor de paridad no válido.

Respuesta del Usuario: Limpie el archivo de la base de datos del proveedor de telefonía.

ICA4094 Valor de bit de parada en el archivo de valores por omisión %1\$s en la línea %2\$s.

Explicación: El archivo de la base de datos del proveedor de telefonía tiene un valor de bit de parada que no es válido.

Respuesta del Usuario: Limpie el archivo de la base de datos del proveedor de telefonía.

ICA4095 Código no reconocido %1\$s en el archivo de valores por omisión %2\$s en la línea %3\$s.

Explicación: El archivo de la base de datos del proveedor de telefonía tiene un código no válido.

Respuesta del Usuario: Limpie el archivo de la base de datos del proveedor de telefonía.

ICA4096 Número incorrecto de parámetros.

Explicación: Mensaje informativo.

ICA4097 Error(%1\$s): No ha podido crearse la lista de proveedores de telefonía.Existen problemas de memoria.

Explicación: Es posible que existan problemas de memoria o de sistema.

ICA4098 Error(%1\$s): Errores en el archivo del proveedor de telefonía del buscapersonas %2\$s.

Explicación: El archivo de la base de datos del proveedor de telefonía tiene algunos datos no válidos.

Respuesta del Usuario: Compruebe en el archivo de la base de datos del proveedor de telefonía los códigos no válidos.

ICA4099 Error(%1\$s): No ha podido obtenerse el símbolo IPC %2\$s.

ICA4100 Error(%1\$s): No ha podido crearse la lista de reintentos. Posibles problemas de memoria.

Explicación: Es posible que existan problemas de memoria o de sistema.

ICA4101 Error(%1\$s): No ha podido crearse la cola, page_q_err: %2\$s.

ICA4102 Error(%1\$s): No ha podido definirse el retén de señal para SIGTERM/SIGINT: %2\$s.

Explicación: Posible error del sistema.

ICA4103 Error(%1\$s): No han podido establecerse las características del módem para el proveedor de telefonía %2\$s.

Explicación: El módem no ha podido configurarse.

Respuesta del Usuario: Compruebe la configuración de la puerta serie y la cadena de inicialización.

ICA4104 Falta el código %1\$s para el proveedor de telefonía %2\$s.

Explicación: Falta información del módem. Un código podría ser una velocidad en baudios, una línea exterior ...

Respuesta del Usuario: Compruebe si hay caracteres no válidos en la configuración del módem.

ICA4105 El proveedor de telefonía %1\$s debe contener en su lista un número de teléfono como mínimo.

Explicación: El proveedor de telefonía debe contener el número de teléfono.

Respuesta del Usuario: Añada el número de teléfono utilizando el menú smitty/SMIT.

ICA4106 No puese abrirse el archivo %1\$s.

Explicación: El archivo de la base de datos del proveedor debe existir.

Respuesta del Usuario: Si todavía no existe, cree uno utilizando el menú smitty/SMIT.

ICA4107 La línea %1\$s es demasiado larga.

Explicación: La línea de la base de datos del proveedor de telefonía es demasiado larga.

Respuesta del Usuario: Compruebe si hay líneas no válidas en el archivo de la base de datos del proveedor de telefonía.

ICA4108 Código desconocido en la línea %1\$s.

Explicación: Existe un código desconocido en el archivo de la base de datos del proveedor de telefonía.

Respuesta del Usuario: Compruebe si hay un código no válido en el archivo de la base de datos del proveedor de telefonía.

ICA4109 Secuencia no válida en la línea %1\$s.

Explicación: Existe una secuencia no válida en el archivo de la base de datos del proveedor de telefonía.

Respuesta del Usuario: Compruebe si existe una secuencia no válida en el proveedor de telefonía.

ICA4110 El proveedor de telefonía %1\$s no es válido y se salta.

Explicación: El proveedor no se puede usar para enviar mensajes a buscapersonas.

Respuesta del Usuario: Compruebe la validez del proveedor.

ICA4111 No ha podido añadirse el proveedor de telefonía a la lista.

Explicación: No ha podido añadirse el proveedor de telefonía a la lista.

Respuesta del Usuario: Compruebe la validez del proveedor de telefonía y los números de teléfono.

ICA4112 Falta el nombre del proveedor de telefonía o es demasiado largo en la línea %1\$s.

Explicación: Falta el nombre del proveedor de telefonía.

Respuesta del Usuario: Añada un proveedor de telefonía utilizando el menú smitty/SMIT.

ICA4113 No ha podido asignarse el nuevo proveedor de telefonía del buscapersonas: %1\$s.

Explicación: El proveedor de telefonía no se ha podido asignar a la lista.

Respuesta del Usuario: Compruebe la validez del proveedor de telefonía y los números de teléfono.

ICA4114 El valor de la línea %1\$s es demasiado largo.

Explicación: Se ha encontrado una línea que es demasiado larga en el archivo de la base de datos del proveedor.

Respuesta del Usuario: Borre el nombre largo del archivo de la base de datos del proveedor de telefonía.

ICA4115 El código duplicado %1\$s de la línea %2\$s se ha pasado por alto.

Explicación: Se ha encontrado un código duplicado.

Respuesta del Usuario: Elimine el código duplicado del archivo de la base de datos del proveedor de telefonía.

ICA4116 El valor de la línea %1\$s no existe.

Explicación: Se ha encontrado un campo en blanco.

Respuesta del Usuario: Utilice smitty/SMIT para añadir un valor al campo que está en blanco.

ICA4117 El valor debe ser Y, Yes, N o No en la línea %1\$s.

Explicación: Este campo requiere un Y, Yes, N o No.

Respuesta del Usuario: Utilice smitty/SMIT para añadir o cambiar datos válidos.

ICA4118 El valor debe ser mayor que 0 en la línea %1\$s.

Explicación: Este campo debe ser positivo.

Respuesta del Usuario: Cambie el valor utilizando smitty/SMIT para que se especifique un valor positivo.

ICA4119 Valor no válido en la línea %1\$s.

Explicación: Se ha encontrado un valor que no es válido en la línea especificada.

Respuesta del Usuario: Cambie el valor utilizando el menú smitty/SMIT.

ICA4120 El proveedor de telefonía %1\$s no es válido y se salta.

Explicación: Se ha encontrado un proveedor de telefonía que no es válido.

Respuesta del Usuario: Añada un proveedor de telefonía utilizando el menú smitty/SMIT.

ICA4121 No ha podido añadirse el proveedor de telefonía a la lista.

Explicación: No ha podido añadirse el proveedor de telefonía a la lista de buscapersonas.

Respuesta del Usuario: Compruebe la validez del proveedor de telefonía.

ICA4122 El código duplicado %1\$s de la línea %2\$s se ha pasado por alto.

Explicación: Se ha encontrado un código duplicado en una stanza del proveedor de telefonía.

Respuesta del Usuario: Borre la stanza del proveedor de telefonía que contiene valores duplicados.

ICA4123 Error(%1\$s): No ha podido obtenerse el símbolo de IPC: %2\$s

Explicación: El programa no ha podido obtener el símbolo IPC.

ICA4124 Error(%1\$s): Error %2\$s al leer la cola.

Explicación: El programa no ha podido leer la cola.

ICA4125 %1\$s entradas en la cola.

Explicación: Mensaje informativo.

ICA4126 El mensaje con el ID %1\$s se ha suprimido.

Explicación: Mensaje informativo.

ICA4127 El ID %1\$s no se encuentra en la cola.

Explicación: Mensaje informativo.

ICA4128 Error(%1\$s): Error %2\$s al intentar suprimir el ID %3\$s.

Explicación: Se ha intentado suprimir un ID de la cola.

ICA4129 La clave es: %1\$s el contenido es @ %2\$s: %3\$s.

Explicación: Mensaje solamente informativo.

ICA4130 Características del módem:

Explicación: Información de inicialización del módem.

ICA4131 Nombre: %1\$s

Explicación: Información de inicialización del módem.

ICA4132 Inic: %1\$s

Explicación: Información de inicialización del módem.

ICA4133 Modalidad de mandatos: %1\$s

Explicación: Información de inicialización del módem.

ICA4134 Terminador de mandatos: 0x%1\$s

Explicación: Información de inicialización del módem.

ICA4135 Marcar: %1\$s

Explicación: Información de inicialización del módem.

ICA4136 Pausa en marcación: %1\$s

Explicación: Información de inicialización del módem.

ICA4137 Marcar #: %1\$s

Explicación: Información de inicialización del módem.

ICA4138 Marcar *: %1\$s

Explicación: Información de inicialización del módem.

ICA4139 Colgar: %1\$s

Explicación: Información de inicialización del módem.

ICA4140 Respuesta de mandato válida: %1\$s

Explicación: Información de inicialización del módem.

ICA4141 Conexión válida: %1\$s

Explicación: Información de inicialización del módem.

ICA4142 Eco: %1\$s

Explicación: Información de inicialización del módem.

ICA4143 Registro de depuración del módem: PUTS(%1\$s) txd-> %2\$s

Explicación: Información de sincronización del módem.

ICA4144 Registro de depuración del módem: PUTC(%1\$s) txd-> %2\$s

Explicación: Información de sincronización del módem.

ICA4145 Registro de depuración del módem: GET rxd-> %1\$s

Explicación: Información de sincronización del módem.

ICA4146 Registro de depuración del módem: INPUT(%1\$s

Explicación: Información de sincronización del módem.

ICA4147 Registro de depuración del módem:) rxd->

Explicación: Información de sincronización del módem.

ICA4148 Registro de depuración del módem: WAITFOR(%1\$s

Explicación: Información de sincronización del módem.

ICA4149 No ha podido desbloquearse la señal inferior.

Explicación: Desbloquea la señal SIGCHLD.

ICA4150 No ha podido bloquearse la señal inferior.

Explicación: Bloquea la señal SIGCHLD.

ICA4151 El archivo de inicio en caliente %1\$s no existe.

Explicación: Mensaje informativo.

ICA4152 No ha podido abrirse el archivo de inicio en caliente %1\$s

Explicación: Mensaje informativo.

ICA4153 La línea es demasiado larga en el archivo de inicio en caliente %1\$s.

Explicación: El archivo de inicio en caliente contiene algunos caracteres que no son válidos.

ICA4154 El archivo de inicio en caliente %1\$s contiene datos que no se usan.

Explicación: Mensaje informativo.

ICA4155 El archivo de inicio en caliente %1\$s está vacío.

Explicación: Mensaje informativo.

ICA4156 La línea %1\$s del archivo de inicio en caliente %2\$s tiene un destinatario incorrecto %3\$s, se ha pasado por alto.

Explicación: El archivo de inicio en caliente contiene algunos caracteres que no son válidos. Mensaje informativo.

ICA4157 La línea %1\$s del archivo de inicio en caliente %2\$s tiene un formato incorrecto, se ha pasado por alto.

Explicación: El archivo de inicio en caliente contiene algunos caracteres que no son válidos. Mensaje informativo.

ICA4158 La línea %1\$s del archivo de inicio en caliente %2\$s no tiene mensaje, se ha pasado por alto.

Explicación: El archivo de inicio en caliente no tiene ningún mensaje. Mensaje informativo.

ICA4159 Error en la línea de la cola %1\$s del archivo de inicio en caliente %2\$s, se ha pasado por alto.

Explicación: El archivo de inicio en caliente contiene algunos caracteres que no son válidos. Mensaje informativo.

ICA4160 Ha finalizado el inicio en caliente de %1\$s mensajes del archivo %2\$s.

Explicación: Mensaje informativo.

ICA4161 Error(%1\$s): Existen demasiados errores consecutivos de inferior.

Explicación: Demasiados errores de inferior en una fila. Se produce si el proveedor de telefonía o el archivo de definición del módem tienen algunos caracteres que no son válidos.

Respuesta del Usuario: Compruebe el archivo de la base de datos del proveedor de telefonía y el archivo de definición del módem utilizando el menú smitty/SMIT.

ICA4162 No se puede ejecutar inferior %1\$s : %2\$s.

Explicación: Posible error del sistema.

ICA4163 Error(%1\$s): El inferior no puede ejecutar fork para el inferior: %2\$s.

Explicación: Posible error del sistema.

ICA4164 No ha podido crearse la línea de proveedores de telefonía.

Explicación: Error interno del programa.

ICA4165 Errores en el archivo del proveedor de telefonía del buscapersonas %1\$s

Explicación: La base de datos del proveedor de telefonía contiene algunos caracteres que no son válidos.

Respuesta del Usuario: Compruebe el archivo de la base de datos del proveedor de telefonía utilizando el menú smitty/SMIT.

ICA4166 Mensaje informativo. La clave IPC es: 0x%1\$s.

Explicación: Mensaje informativo.

ICA4167 No ha podido crearse la cola, page_q_err: %1\$s.

Explicación: Error al intentar crear la cola.

ICA4168 El archivo de inicio en caliente del buscapersonas se ha creado a las %1\$s

Explicación: Mensaje informativo.

ICA4169 prioridad -p %1\$s %2\$s de %3\$s %4\$s

Explicación: Mensaje informativo.

ICA4170 prioridad -p %1\$s %2\$s@%3\$s de %4\$s %5\$s

Explicación: Mensaje informativo.

ICA4171 prioridad -p %1\$s -n %2\$s@%3\$s de %4\$s %5\$s

Explicación: Mensaje informativo.

ICA4172 Fin de archivo de inicio en caliente del buscapersonas.

Explicación: Mensaje informativo. Denota el fin del mensaje.

ICA4173 No ha podido grabarse en el archivo de inicio en caliente %1\$s.

Explicación: Es posible que el archivo de inicio en caliente no exista.

ICA4174 %1\$s PETICIÓN-ESTADO de %2\$s@%3\$s

Explicación: Muestra información de petición de estado.

ICA4175 %1\$s PETICIÓN-RESUMEN de %2\$s@%3\$s.

Explicación: Muestra la información de petición de resumen.

ICA4176 %1\$s entradas en la cola.

Explicación: Cuenta el número de entradas de cola en la cola del buscapersonas.

ICA4177 Entrada más antigua: El ID %1\$s se ha recibido a las %2\$s.

Explicación: Muestra la entrada más antigua de la cola.

ICA4178 La nueva conexión de memoria tras la expansión ha resultado anómala.

Explicación: Posible error del sistema.

ICA4179 La nueva conexión de memoria tras la expansión no ha podido alinearse.

Explicación: Posible error del sistema.

ICA4180 No ha podido descenderse el semáforo PAGE_Q en page_q_print() : %1\$s.

Explicación: Posible error del sistema.

ICA4181 No ha podido ascenderse el semáforo PAGE_Q en page_q_print() : %1\$s.

Explicación: Posible error del sistema.

ICA4182 enlace %1\$s -> ID de mensaje: %2\$s.

Explicación: Mensaje informativo.

ICA4183 Prioridad: %1\$s.

Explicación: Mensaje informativo.

ICA4184 Persona: %1\$s.

Explicación: Mensaje informativo.

ICA4185 Proveedor de telefonía: %1\$s.

Explicación: Mensaje informativo.

ICA4186 Mensaje: %1\$s.

Explicación: Mensaje informativo.

ICA4187 No ha podido obtenerse RAM compartida : %1\$s.

Explicación: Posible error del sistema.

ICA4188 No ha podido obtenerse RAM compartida conectada : %1\$s.

Explicación: Posible error del sistema.

ICA4189 No ha podido obtenerse el semáforo PAGE_Q.

Explicación: Posible error del sistema.

ICA4190 No ha podido inicializarse el semáforo PAGE_Q en page_q_create() : %1\$s.

Explicación: Posible error del sistema.

ICA4191 No ha podido establecerse el semáforo PAGE_Q en page_q_create() : %1\$s.

Explicación: Posible error del sistema.

ICA4192 No ha podido descenderse el semáforo PAGE_Q en page_q_empty() : %1\$s.

Explicación: Posible error del sistema.

ICA4193 No ha podido ascenderse el semáforo PAGE_Q en page_q_empty() : %1\$s.

Explicación: Posible error del sistema.

ICA4194 No ha podido descenderse el semáforo PAGE_Q en page_q_enq(%1\$s,%2\$s) : %3\$s.

Explicación: Posible error del sistema.

ICA4195 No ha podido ascenderse el semáforo PAGE_Q en page_q_enq() : %1\$s.

Explicación: Posible error del sistema.

ICA4196 page_q_enq(): ID(%1\$s) Pri(%2\$s) Persona(%3\$s) Mensaje(%4\$s).

Explicación: Mensaje informativo.

ICA4197 No ha podido descenderse el semáforo PAGE_Q en page_q_head() : %1\$s.

Explicación: Posible error del sistema.

ICA4198 No ha podido ascenderse el semáforo PAGE_Q en page_q_head() : %1\$s.

Explicación: Posible error del sistema.

ICA4199 No ha podido descenderse el semáforo PAGE_Q en page_q_first() : %1\$s.

Explicación: Posible error del sistema.

ICA4200 No ha podido ascenderse el semáforo PAGE_Q en page_q_first() : %1\$s.

Explicación: Posible error del sistema.

ICA4201 No ha podido descenderse el semáforo PAGE_Q en page_q_next() : %1\$s.

Explicación: Posible error del sistema.

ICA4202 No ha podido ascenderse el semáforo PAGE_Q en page_q_next() : %1\$s.

Explicación: Posible error del sistema.

ICA4203 No ha podido descenderse el semáforo PAGE_Q en page_q_tail() : %1\$s.

Explicación: Posible error del sistema.

ICA4204 No ha podido ascenderse el semáforo PAGE_Q en page_q_tail() : %1\$s.

Explicación: Posible error del sistema.

ICA4205 No ha podido descenderse el semáforo PAGE_Q en page_q_del() : %1\$s.

Explicación: Posible error del sistema.

ICA4206 No ha podido ascenderse el semáforo PAGE_Q en page_q_del() : %1\$s.

Explicación: Posible error del sistema.

ICA4207 page_q_del(%1\$s).

Explicación: Información de depuración.

ICA4208 No ha podido descenderse el semáforo PAGE_Q en page_q_deq() : %1\$s.

Explicación: Posible error del sistema.

ICA4209 No ha podido ascenderse el semáforo PAGE_Q en page_q_deq() : %1\$s.

Explicación: Posible error del sistema.

ICA4210 **page_q_del(): ID(%1\$s) Pri(%2\$s) Persona(%3\$s) Mensaje(%4\$s).**

Explicación: Mensaje informativo.

ICA4211 **No ha podido descenderse el semáforo PAGE_Q en page_q_walk() : %1\$s.**

Explicación: Posible error del sistema.

ICA4212 **No ha podido ascenderse el semáforo PAGE_Q en page_q_walk() : %1\$s.**

Explicación: Posible error del sistema.

ICA4213 **PAGE_Q está llena.**

Explicación: La cola del buscapersonas está llena.

Respuesta del Usuario: Envíe el mensaje al buscapersonas más tarde.

ICA4300 **Colgando.**

Explicación: Colgando la pantalla.

ICA4301 **Inicializando módem ..**

Explicación: Inicializando el módem con la cadena de inicialización.

ICA4302 **Marcando**

Explicación: Marcando el número de teléfono.

ICA4303 **En espera de conexión.**

Explicación: Esperando la conexión del módem

ICA4304 **CONECTADO %1\$s**

Explicación: Conectando a |velocidad| baudios

ICA4305 **CONECTADO!!!!!!**

Explicación: Conectado al proveedor del servicio del buscapersonas

ICA4306 **Solicitando petición de modalidad automática.**

Explicación: Solicitando petición de modalidad automática. Esperando "ID="

ICA4307 **Solicitud correcta.....**

Explicación: Se ha obtenido "ID=" del proveedor.

ICA4308 **Enviando petición de modalidad automática.**

Explicación: Enviando ID y SST al proveedor del servicio de buscapersonas

ICA4309 **Enviar petición de modalidad automáticaOK!**

Explicación: Se ha recibido p. Lo que significa que la comunicación es satisfactoria.

ICA4310 **Enviando mensaje**

Explicación: Enviando bloque de mensaje

ICA4311 En espera del resultado

Explicación: En espera de la confirmación

ICA4312 Recibido acuse de recibo. Mensaje al buscapersonas satisfactorio.**ICA4313 Recibido acuse de recibo negativo, Volver a enviar bloque. Intento %1\$s**

Explicación: Se han recibido acuses de recibo negativos. El proveedor del buscapersonas solicita que se vuelva a enviar.

ICA4314 Error de transacción. Volver a enviar bloque. Intento %1\$s

Explicación: Error de transacción. Volviendo a enviar el bloque.

ICA4315 Conexión finalizada por el proveedor de telefonía.

Explicación: El proveedor del buscapersonas ha finalizado la conversación. Consulte al proveedor de telefonía para solucionar el problema

ICA4350 fwpage proveedor de telefonía="..." módem="..." ID="..." mensaje="..."

Explicación: Uso de fwpage. Compruebe los parámetros y vuélvalo a probar.

ICA4351 El archivo %1\$s no existe

Explicación: Compruebe el archivo para ver si se encuentra en el directorio correcto. Hay que crear carriers.cfg, modems.cfg, y pager.cfg antes de usar este código.

ICA4352 El archivo %1\$s está dañado

Explicación: El archivo ha sido modificado por el usuario y no está en el formato de stanza. Todos los atributos deberían entrarse a través de la GUI.

ICA4353 %1\$s es demasiado largo, acórtelo y vuelva a intentarlo.

Explicación: [Qué] demasiado largo. Acórtelo y vuelva a intentarlo.

ICA4354 %1\$s incorrecto.

Explicación: Si la velocidad en baudios es errónea, las opciones válidas son: 600, 1200, 2400, 4800, 9600, 14400. Si los bits de datos por byte son erróneos, las opciones válidas son: 7, 8. Si los bits de parada son erróneos, las opciones válidas son: 1, 2. Si el prefijo de la línea de salida es erróneo, las entradas deben ser sólo números. Si el método de mensajes del buscapersonas es erróneo, esta versión sólo da soporte a TAP. Si hay un error de ID de buscapersonas, compruebe si tiene todos los números. Si la paridad es errónea, las opciones válidas son: O(impar), E(par), N(ninguno), S(espacio), M(marca). Si la puerta COM es errónea, las opciones válidas son: COM1, COM2 La puerta COM debería ser menor que 10 en esta versión. Si los caracteres del mensaje son erróneos, compruebe el mensaje para ver si contiene caracteres especiales.

ICA4355 Error de Establecer parámetros en %1\$s.

Explicación: No se puede establecer parámetros en [dónde]. Compruebe los parámetros y vuelva a probarlo.

ICA4356 cuando %1\$s, error de lectura de la puerta COM.

Explicación: Error de lectura de la puerta COM. Establezca el eco de módem en on y vuelva a intentarlo

ICA4357 cuando %1\$s, error de grabación en la puerta COM.

Explicación: Error de grabación en la puerta COM.

ICA4358 Error en Establecer %1\$s

Explicación: Error en Establecer [Qué]. Compruebe el archivo de registro y localice el error.

ICA4359 Se ha superado el número máximo de reintentos en %1\$s. Cancelar anormalmente el programa...

Explicación: Intente abrir la puerta COM 60 veces en 60 minutos. Todo ha resultado anómalo. Si es éste el caso, compruebe las conexiones del hardware. Intente enviar un mensaje al buscapersonas 10 veces en 10 minutos. Todo ha resultado anómalo. Si éste es el caso, puede que el proveedor de telefonía del buscapersonas esté desconectado.

ICA4360 Carácter desconocido en el número de teléfono del proveedor de telefonía: %1\$s

Explicación: Se ha encontrado un carácter no reconocido en el número de teléfono del proveedor. Compruebe el número y vuelva a intentarlo.

ICA4361 Advertencia!!! El módem del proveedor del buscapersonas suele ser menor a 2400.

Explicación: Esto es sólo una advertencia. La velocidad del módem del proveedor del buscapersonas normalmente se establece en menos de 2400.

ICA4362 No ha podido inicializarse el módem

Explicación: Cambie la cadena de inicialización del módem y vuelva a intentarlo.

ICA4363 El módem ha devuelto un Error.

Explicación: Error de comunicación del módem

ICA4364 Error en el intento %1\$s de abrir la puerta Com. Vuelva a intentarlo dentro de 1 minuto

Explicación: Error en la apertura de la puerta Com. Probablemente lo está usando otro programa. Se volverá a intentar automáticamente dentro de 1 minuto

ICA4365 Envío de mensaje al buscapersonas anómalo en el intento %1\$s. Vuelva a intentarlo dentro de 1 minuto

Explicación: Error al enviar un mensaje al buscapersonas. Compruebe el archivo de registro para averiguar la razón exacta.

ICA4366 El mensaje es demasiado largo, se ha truncado

Explicación: Esto es sólo una advertencia. El mensaje es demasiado largo. Trúnquelo para que tenga la longitud correcta.

ICA4367 Restablecer la Longitud máxima del mensaje al valor definido internamente:%1\$s

Explicación: Se restablece la longitud máxima del mensaje a los valores por omisión porque la longitud definida por el usuario es mayor que la definida internamente, que es de 80.

ICA4368 Acción: error en %1\$s

Explicación: Si se trata de un error al abrir la puerta COM, compruebe la configuración y vuelva a intentarlo. Si es un error de manejo de cierre de COM, se trata de un error del sistema. Si es un error de depuración de COM, se trata de un problema del sistema. Si se trata de un error del envío del mandato de marcación, es un problema del mandato de marcación. Compruebe si el módem es compatible con Hayes. Si se trata de un error de envío de petición de ID, compruebe si el proveedor de telefonía del buscapersonas da soporte al protocolo TAP. Si se trata de un error de solicitud de envío automático, compruebe si el servicio del buscapersonas funciona correctamente. Si es un error de envío del mensaje, compruebe el archivo de registro para localizar la causa de la anomalía. Si es un error de solicitud, no se puede obtener una respuesta de solicitud del proveedor del buscapersonas.

ICA4369 Existen demasiados errores de transacción. Cancelando anormalmente

Explicación: Existen demasiados errores de transacción, cancele este intento.

ICA4370 Se han recibido anormalmente demasiados acuses de recibo negativos, cancelando anormalmente el programa

Explicación: Se han recibido demasiados acuses de recibo negativos del proveedor del buscapersonas, cancele el intento.

ICA4371 %1\$s en la puerta COM con la función %2\$s ha devuelto %3\$s

Explicación: Compruebe los parámetros y vuelva a intentarlo.

ICA4372 Mensaje de error de retorno del módem..... %1\$s

Explicación: Los mensajes son. No conectado, Llamando pero no conectado, Sin proveedor de telefonía, Sin tono de marcación, Ocupado, Sin respuesta.

ICA4373 (%1\$s) Código de respuesta desconocido desde módem o proveedor de telefonía: %2\$s, %3\$s.

Explicación: Este mensaje informa la respuesta del módem o del proveedor de telefonía, que la función de envío de mensajes al buscapersonas del cortafuegos no reconoce. car1 y car2 son los códigos ascii (hex) para los 2 primeros caracteres de la respuesta.

Respuesta del Usuario: Utilice esta información cuando consulte las instrucciones del módem o al proveedor de telefonía para determinar el significado de las respuesta desconocida.

ICA5005 La inicialización de SKIT ha resultado anómala. El código de retorno es: %1\$s

Explicación: La inicialización del socket seguro ha resultado anómala; se visualiza el código de retorno de SKIT.

ICA5014 El Servidor de túneles del cliente remoto está atendiendo a la puerta %1\$s

Explicación: Se visualiza el número de puerta que se ha configurado para sslrctd.

ICA5015 Conexión aceptada de %1\$s.%2\$s.%3\$s.%4\$s

Explicación: Se visualiza la dirección IP del cliente.

ICA5017 No ha podido obtenerse el socket seguro. El código de retorno de la función skit_secure_soc_init es:%1\$s

Explicación: No ha podido obtenerse el socket seguro porque skit_secure_soc_init() ha resultado anómala.

ICA5018 Las especificaciones de cifrado del servidor esclavo que se han utilizado son %1\$s %2\$s %3\$s

Explicación: Se visualizan las especificaciones de cifrado.

ICA5019 No puede obtenerse la agrupación Free Homenet IP.

Explicación: Problema de los filtros dinámicos.

ICA5020 No ha podido abrirse el archivo de configuración del cliente remoto.

Explicación: El archivo /etc/security/rcsfile.cfg no está disponible.

Respuesta del Usuario: Compruebe si existe el archivo y su contenido.

ICA5021 No se puede encontrar la palabra clave '%1\$s'.

Explicación: El archivo /etc/security/rcsfile.cfg no tiene esta palabra clave.

Respuesta del Usuario: Compruebe y corrija el archivo /etc/security/rcsfile.cfg.

ICA5024 Error de función skit_secure_soc_write() en %1\$s.

Explicación: skit_secure_soc_write() ha resultado anómala en esta rutina.

ICA5025 Error de función skit_secure_soc_write() en ACKClient().

Explicación: skit_secure_soc_write() ha resultado anómala en la rutina ACKClient().

ICA5026 Se ha recibido un código de retorno no válido del Cliente en %1\$s.

Explicación: Se ha recibido un código de retorno no esperado del cliente en esta rutina.

ICA5027 Se ha recibido un código de retorno para una petición errónea del Cliente en %1\$s.

Explicación: El código de petición del mensaje de código de retorno no se espera en esta rutina.

ICA5028 Petición de conexión no válida.

Explicación: El formato del mensaje de petición de conexión no es válido.

ICA5030 ID de cliente remoto desconocido : %1\$s

Explicación: La máquina cortafuegos no conoce este ID de usuario.

Respuesta del Usuario: Corrija la información del usuario para este cliente remoto.

ICA5031 Error de función skit_secure_soc_write en RCTLoginPhase.

Explicación: skit_secure_soc_write() ha resultado anómala en la fase de conexión.

ICA5035 Petición de desconexión no válida.

Explicación: El formato del mensaje de petición de desconexión no es válido.

ICA5067 Se ha recibido un paquete no válido.

Explicación: El formato del paquete recibido no es válido.

ICA5078 Obtención de petición no reconocida en SvrReqHandler()

Explicación: Se ha recibido una petición no reconocida; se pasará por alto.

ICA5082 Se ha desconectado el túnel al cliente %1\$s.

Explicación: Se ha desconectado el túnel para el cliente remoto que tiene este ID.

ICA5086 ID: %1\$s no definido.

Explicación: Este ID de usuario no existe en la máquina cortafuegos.

ICA5087 La autenticación ha resultado anómala para '%1\$s'.

Explicación: La autenticación de este ID de usuario ha resultado anómala.

ICA5089 La función rcFilterClear() ha resultado anómala. El código de retorno es %1\$s.

Explicación: rcFilterClear() ha resultado anómala y ha devuelto este código de retorno.

Respuesta del Usuario: Compruebe si existe el cliente de la LAN IPSEC. Estos productos no son compatibles.

ICA5090 La función rcFilterInit() ha resultado anómala. El código de retorno es %1\$s

Explicación: rcFilterInit() ha resultado anómala y ha devuelto este código de retorno.

ICA5091 La función TunnelUp() no puede ejecutar el archivo ejecutable %1\$s.

Explicación: Se visualiza la llamada al sistema() anómala de la línea de mandatos.

ICA5092 No ha podido obtenerse la contraseña del juego de claves de la llamada a función recoverstash.

Explicación: No puede recuperarse la contraseña del juego de claves del archivo oculto.

ICA8001 SYSLOG/udp: servicio desconocido

ICA8002 La función %1\$s ha resultado anómala - %2\$s, errno2 = 0x%3\$s

Explicación: El proceso ha finalizado porque syslogd no ha podido llevar a cabo la función especificada. La información de errno se añade al mensaje de error.

Respuesta del Usuario: Póngase en contacto con el programador del sistema. Programador del sistema: utilice la información de errno para determinar la causa de la anomalía.

ICA8004 Se ha detectado un error en el socket AF_INET, \slogd ya no supervisará el socket

ICA8006 Nombre de prioridad desconocido \"%1\$s\"

Explicación: Un nombre de prioridad que se ha hallado en el archivo de configuración no es válido.

Respuesta del Usuario: Póngase en contacto con el programador del sistema. Programador del sistema: Compruebe el archivo de configuración.

ICA8007 Nombre de recurso desconocido \"%1\$s\"

Explicación: Un nombre de recurso que se ha hallado en el archivo de configuración no es válido.

Respuesta del Usuario: Póngase en contacto con el programador del sistema. Programador del sistema: Compruebe el archivo de configuración.

ICA8008 \bMensaje de SYSLOG@%1\$s a las %2\$.24s ...

Explicación: El archivo de configuración del daemon syslog contiene una entrada para enviar mensajes del registro del sistema a todos los usuarios conectados. Este mensaje sólo se enviará a todos los usuarios que están conectados actualmente al sistema en el que se está ejecutando el daemon syslog.

Respuesta del Usuario: Ningún programador del sistema: ninguno

ICA8009 SYSLOGD saliendo con la señal %1\$s

Explicación: El daemon syslog ha recibido una señal que ha provocado que el syslog saliera.

Respuesta del Usuario: Ningún programador del sistema: ninguno

ICA8010 SYSLOGD reiniciado**ICA8012 SYSLOGD no ha podido grabar en SMF - %1\$s**

Explicación: Se ha producido un error al grabar un registro en SMF. La información del texto de error se añade al mensaje de error.

Respuesta del Usuario: Póngase en contacto con el programador del sistema. Programador del sistema: Utilice la información del texto de error para determinar la causa del error de grabación en SMF.

ICA8013 La actualización del estado del proceso ha resultado anómala, código de retorno = 0x%1\$s

Explicación: Se ha producido un error al intentar actualizar el estado del proceso syslogd para el proceso kernel del cortafuegos. El código de retorno hace una breve descripción del error específico revuelto de la llamada de estado del proceso de actualización.

Respuesta del Usuario: Póngase en contacto con el programador del sistema. Programador del sistema: Póngase en contacto con el representante de asistencia técnica.

ICA8014 Opción desconocida (-%1\$s) especificada en la invocación de SYSLOGD

Explicación: Se ha producido un error al intentar iniciar el proceso del daemon syslogd. La opción especificada no recibe soporte de la invocación de syslogd.

Respuesta del Usuario: Compruebe las opciones de arranque y reinicie el daemon syslogd. Programador del sistema: si el problema persiste, póngase en contacto con el representante de asistencia técnica.

ICA8015 La entrada del archivo de configuración (%1\$s) no es válida

Explicación: Se ha producido un error al intentar analizar una entrada de configuración del archivo de configuración SYSLOG.

Respuesta del Usuario: Compruebe las entradas del archivo de configuración y reinicie el daemon syslogd. Programador del sistema: si el problema persiste, póngase en contacto con el representante de asistencia técnica.

ICA8016 %1\$s ha resultado anómalo para %2\$s - %3\$s

Explicación: Se ha producido un error al intentar llevar a cabo la función especificada para el dispositivo especificado. La información de error se añade al mensaje de error.

Respuesta del Usuario: Compruebe que el dispositivo especificado exista y vuelva a intentar la petición. Si el problema persiste, póngase en contacto con el programador del sistema. Programador del sistema: si el problema persiste, póngase en contacto con el representante de asistencia técnica.

ICA8050 %1\$s ha resultado anómalo. %2\$s

Explicación: Se ha hallado un error al ejecutar la función que aparece en el mensaje. El texto de error proporciona información adicional acerca del error.

Respuesta del Usuario: Corrija el error indicado en el mensaje y, si es necesario, vuelva a intentar la operación.

ICA8051 %1\$s ha resultado anómalo: código de retorno = 0x%2\$s

Explicación: Se ha hallado un error al ejecutar la función que aparece en el mensaje. También se muestra el código de retorno de la función indicada.

Respuesta del Usuario: Corrija el error indicado en el mensaje y, si es necesario, vuelva a intentar la operación.

ICA8052 FWSTACKD activando registro de filtros para %1\$s.

Explicación: FWSTACKD intenta activar el registro de filtros del paquete.

Acción del Sistema: El programa continúa.

ICA8053 FWSTACKD no puede activar el registro de filtros para %1\$s. %2\$s

Explicación: La activación del registro de filtros del paquete ha resultado anómala por la razón descrita en el mensaje de error adjunto.

Acción del Sistema: No se realizará el registro de filtros.

Respuesta del Usuario: Consulte el mensaje de error para corregir el error y, a continuación, vuelva a activar el registro de filtros con **fwfilter cmd=startlog**.

ICA8054 FWSTACKD activando registro de NAT para %1\$s.

Explicación: FWSTACKD intenta activar el registro de la conversión de dirección de red (NAT).

Acción del Sistema: El programa continúa.

ICA8055 FWSTACKD no puede activar el registro de NAT para %1\$s. %2\$s

Explicación: La activación del registro de la conversión de dirección de red (NAT) ha resultado anómala por la razón descrita en el mensaje de error adjunto.

Acción del Sistema: No se realizará el registro de la conversión de dirección de red.

Respuesta del Usuario: Consulte el mensaje de error para corregir el error y, a continuación, vuelva a activar el registro de la conversión de dirección de red con **fwnat cmd=startlog**.

ICA8056 FWSTACKD está activando NAT para %1\$s.

Explicación: FWSTACKD intenta activar la conversión de dirección de red (NAT).

Acción del Sistema: El programa continúa.

ICA8057 FWSTACKD no puede activar NAT para %1\$s. %2\$s

Explicación: La activación de la conversión de dirección de red (NAT) ha resultado anómala por la razón descrita en el mensaje de error adjunto.

Acción del Sistema: No se realizará la conversión de dirección de red.

Respuesta del Usuario: Consulte el mensaje de error para corregir el error y, a continuación, vuelva a activar la conversión de dirección de red con **fwnat cmd=update**.

ICA8058 FWSTACKD está reactivando las definiciones de túnel para %1\$s.

Explicación: FWSTACKD intenta reactivar las definiciones de túnel que estaban activas cuando se paró el sistema.

Acción del Sistema: El programa continúa.

ICA8059 FWSTACKD no puede reactivar las definiciones de túnel para %1\$s. %2\$s

Explicación: La activación de las definiciones de túnel ha resultado anómala por la razón descrita en el mensaje de error adjunto.

Acción del Sistema: Las definiciones de túneles no están activadas.

Respuesta del Usuario: Consulte el mensaje de error para corregir el error y, a continuación, vuelva a activar las definiciones de túnel con **fwtnnl cmd=activate**.

ICA8060 FWSTACKD está activando las normas de filtros y socks para %1\$s.

Explicación: FWSTACKD intenta activar el conjunto actual de normas de filtros del paquete y de normas de socks.

Acción del Sistema: El programa continúa.

ICA8061 FWSTACKD no puede activar las normas de filtros y socks para %1\$s. %2\$s

Explicación: La activación de las normas de filtros y de socks ha resultado anómala por la razón descrita en el mensaje de error adjunto.

Acción del Sistema: Entrarán en operación las normas de filtros por omisión. Se permitirá el acceso local, pero no otro tipo de accesos.

Respuesta del Usuario: Consulte el mensaje de error para corregir el error y, a continuación, vuelva a activar las normas de filtros y socks con **fwfilter cmd=update**.

ICA8062 FWSTACKD está activando el soporte RealAudio para %1\$s.

Explicación: FWSTACKD intenta activar el soporte RealAudio.

Acción del Sistema: El programa continúa.

ICA8063 FWSTACKD no puede activar el soporte RealAudio para %1\$s. %2\$s

Explicación: La activación del soporte RealAudio ha resultado anómala por la razón descrita en el mensaje de error adjunto.

Acción del Sistema: Los servicios RealAudio no están disponibles.

Respuesta del Usuario: Consulte el mensaje de error para identificar el error, arréglo y active RealAudio con **fwaudio cmd=change**.

ICA8064 %1\$s ha resultado anómalo. %2\$s

Explicación: Se ha hallado un error al ejecutar la función que aparece en el mensaje. El texto de error proporciona información adicional acerca del error.

Respuesta del Usuario: Corrija el error indicado en el mensaje y, si es necesario, vuelva a intentar la operación.

ICA9000 La evaluación de IBM Firewall caduca dentro de %1\$s días.

Explicación: Este software es una copia de evaluación y se inhabilitará él mismo tal y como se indica.

ICA9001 Advertencia de la comprobación de la integridad del sistema de archivos - %1\$s

Explicación: fwfschk ha encontrado una discrepancia en el sistema de archivos - se trata de una posible amenaza contra la seguridad

ICA9002 El último mensaje se repite %1\$d veces

Explicación: Mensaje generado por el syslogd de AIX cuando se registra un mensaje idéntico sin ningún mensaje que intervenga. El mensaje se guarda aquí para que el supervisor del registro pueda detectar la condición. Este mensaje debe estar en el idioma en el que se escriba el mensaje del syslogd real.

ICA9003 Autenticación anómala para el usuario %1\$s en el servidor de configuración.

Explicación: El servidor de configuración del cortafuegos no puede autenticar el usuario indicado.

Respuesta del Usuario: Consulte con el administrador del cortafuegos.

ICA9004 El usuario %1\$s se ha autenticado satisfactoriamente en el servidor de configuración.

Explicación: El servidor de configuración del cortafuegos ha autenticado el usuario indicado.

ICA9005 Iniciando servidor de configuración remota.

Explicación: Se ha iniciado el servidor de configuración.

ICA9006 Finalizando servidor de configuración remota.

Explicación: El servidor de configuración remota está finalizando.

ICA9007 El servidor de configuración remota no ha podido abrir el catálogo de mensajes.

Explicación: Es posible que falten uno o más catálogos de mensajes usados por el servidor de configuración remota.

Respuesta del Usuario: Consulte con el administrador del cortafuegos.

ICA9008 El servidor de configuración remota ha resultado anómalo en getpeername(): error %1\$s.

Explicación: El servidor de configuración remota no puede obtener información sobre el cliente.

Respuesta del Usuario: Consulte con el administrador del cortafuegos.

ICA9009 El servidor de configuración remota ha resultado anómalo en getsockname(): error %1\$s.

Explicación: El servidor de configuración remota no puede obtener información sobre él mismo.

Respuesta del Usuario: Consulte con el administrador del cortafuegos.

ICA9010 El servidor de configuración remota no ha podido obtener información del adaptador.

Explicación: El servidor de configuración no ha podido obtener información del adaptador.

Respuesta del Usuario: Consulte con el administrador del cortafuegos.

ICA9011 El servidor de configuración no está habilitado para la configuración remota.

Explicación: El servidor de configuración tiene establecido local=yes en su archivo de configuración y el cliente está en la máquina remota.

Respuesta del Usuario: Consulte con el administrador del cortafuegos.

ICA9012 El servidor de configuración remota no ha podido leer la petición de conexión.

Explicación: El servidor de configuración no puede leer la petición de conexión del cliente.

Respuesta del Usuario: Consulte con el administrador del cortafuegos.

ICA9013 El servidor de configuración remota ha recibido una petición de conexión incorrecta.

Explicación: La petición de conexión contenía información incorrecta.

Respuesta del Usuario: Consulte con el administrador del cortafuegos.

ICA9014 El servidor de configuración no ha podido crear la conexión.

Explicación: El servidor de configuración no puede crear una conexión para la autenticación.

Respuesta del Usuario: Consulte con el administrador del cortafuegos.

ICA9015 El servidor de configuración remota no ha podido crear el proceso.

Explicación: El servidor de configuración no puede crear un proceso para la autenticación.

Respuesta del Usuario: Consulte con el administrador del cortafuegos.

ICA9016 Iniciando daemon EFM.

Explicación: Se ha iniciado el daemon EFM en el cortafuegos gestionado.

ICA9017 Finalizando daemon EFM; rc = %1\$s.

Explicación: El daemon EFM está finalizando con el código de retorno especificado.

ICA9018 El daemon EFM no ha podido abrir el catálogo de mensajes.

Explicación: Es posible que falten uno o más catálogos de mensajes usados por el daemon EFM.

Respuesta del Usuario: Consulte con el administrador del cortafuegos.

ICA9020 No ha podido conmutarse el ID de usuario en ejecución.

Explicación: No se ha podido realizar la llamada del sistema para conmutar el ID de usuario en ejecución.

Respuesta del Usuario: Consulte con el administrador del cortafuegos.

ICA9021 Este cortafuegos no da soporte a la modalidad %1\$s.

Explicación: Este cortafuegos no da soporte a esta modalidad en particular.

Respuesta del Usuario: Consulte con el administrador del cortafuegos.

ICA9022 %1\$s no dispone de autorización para conectarse al cortafuegos en la modalidad %2\$s.

Explicación: Este nombre de usuario no está autorizado a conectarse usando esta modalidad particular.

Respuesta del Usuario: Consulte con el administrador del cortafuegos.

ICA9023 No ha podido cargarse la DLL de EFM.

Explicación: No ha podido cargarse la dll de EFM.

Respuesta del Usuario: Consulte con el administrador del cortafuegos.

ICA9024 Petición de transferencia iniciada por %1\$s para el cortafuegos %2\$s.

Explicación: Se ha iniciado la opción de transferencia.

ICA9025 La petición de transferencia ha terminado con el código de retorno %1\$s.

Explicación: La operación de transferencia se ha completado.

ICA9026 Se ha recibido la petición de transferencia de %1\$s en el cortafuegos %2\$s a %3\$s.

Explicación: La operación de transferencia se ha iniciado a la hora especificada.

ICA9027 El archivo %1\$s de la función %2\$s se ha añadido a la petición de transferencia.

Explicación: El archivo especificado va a transferirse.

ICA9028 Petición de activación iniciada por %1\$s para el cortafuegos %2\$s.

Explicación: Se ha iniciado la operación de activación.

ICA9029 La petición de activación ha terminado con el código de retorno %1\$s.

Explicación: La operación de activación se ha completado.

ICA9030 Se ha recibido la petición de activación de %1\$s en el cortafuegos %2\$s a %3\$s.

Explicación: La operación de activación se ha iniciado a la hora especificada.

ICA9031 La activación de la función %1\$s ha finalizado con el código de retorno %2\$s.

Explicación: La activación de la función especificada se ha completado.

ICA9032 Configuración de NAT actualizada a las %1\$s del %2\$s.

Explicación: La configuración de NAT ha sido actualizada.

ICA9033 El soporte de NAT (nivel %1\$s.%2\$s) ha sido inicializado a las %3\$s del %4\$s.

Explicación: Se ha inicializado el soporte de la NAT del cortafuegos.

ICA9034 El soporte de NAT se ha desactivado a las %1\$s del %2\$s.

Explicación: Se ha inhabilitado el soporte de NAT.

ICA9035 La NAT no ha podido asignar la dirección registrada para la dirección segura %1\$s.

Explicación: La Dirección segura no se ha convertido porque no existen direcciones disponibles en la agrupación de direcciones registradas.

ICA9036 NAT ha liberado la dirección registrada %1\$s para la agrupación de direcciones.

Explicación: La dirección registrada ha sido liberada a la agrupación de direcciones IP registradas.

ICA9037 Las interfaces del cortafuegos se actualizan automáticamente a %1\$s.

Explicación: El programa de inicialización del cortafuegos ha llamado a **UpdateInterfaces()** para desencadenar la actualización automática del archivo de interfaces del cortafuegos, fwadpt.cfg.

Acción del Sistema: Ninguna

Respuesta del Usuario: Ninguna

ICA9038 La interfaz %1\$s se ha eliminado de las configuraciones del cortafuegos.

Explicación: La dirección con puntos decimales que se muestra aparecía en el archivo de configuración del cortafuegos fwadpt.cfg, pero no se había dado a conocer a la pila TCP y, por ese motivo, se ha eliminado del archivo de configuración.

Acción del Sistema: Ninguna

Respuesta del Usuario: Ninguna

ICA9039 La interfaz %1\$s se ha añadido a la configuración del cortafuegos.

Explicación: La pila TCP ha encontrado la dirección con puntos decimales que se muestra, pero no se ha encontrado en el archivo de configuración del cortafuegos fwadpt.cfg y, por ese motivo, se ha añadido al archivo de configuración.

Acción del Sistema: Ninguna

Respuesta del Usuario: Ninguna

ICA9040 La máscara %1\$s de la interfaz ha sido actualizada de %2\$s a %3\$s.

Explicación: La máscara del archivo fwadpt.cfg no coincidía con lo instalado en el hardware. El campo de máscara correcto se ha actualizado en el archivo fwadpt.cfg.

Acción del Sistema: Ninguna

Respuesta del Usuario: Ninguna

ICA9041 No se ha encontrado ninguna interfaz en esta máquina.

Explicación: No se ha encontrado ninguna interfaz de adaptador en esta máquina.

Acción del Sistema: Ninguna

Respuesta del Usuario: Ninguna

ICA9042 NAT activada con una dirección varias en una %1\$s en operación.

Explicación: NAT se ha inicializado satisfactoriamente y ahora está activa. Si la dirección es 0, significa que la conversión varias en una está inactiva.

Acción del Sistema: Ninguna

Respuesta del Usuario: Ninguna

ICA9043 NAT no ha podido inicializarse, con código de retorno %1\$s.

Explicación: NAT no ha podido inicializarse y está inactiva.

Acción del Sistema: No se invocará ninguna función de NAT.

Respuesta del Usuario: Si el usuario quiere disponer de la funcionalidad NAT, consulte el código de retorno y realice las correcciones necesarias. Si el problema persiste, póngase en contacto con el servicio de IBM.

ICA9044 NAT desactivada.

Explicación: NAT se ha desactivado satisfactoriamente y ahora está inactiva.

Acción del Sistema: Ninguna

Respuesta del Usuario: Ninguna

ICA9045 NAT ha asignado la dirección:puerta %1\$s:%2\$s para la dirección:puerta segura %3\$s:%4\$s

Explicación: NAT ha asignado la dirección:puerta de la agrupación de direcciones en nombre del sistema principal seguro.

Acción del Sistema: Ninguna

Respuesta del Usuario: Ninguna

ICA9046 NAT no ha podido asignar la dirección varias en una para la dirección segura %1\$s

Explicación: NAT se ha quedado sin puertas con dirección varias en una.

Acción del Sistema: Se ha desactivado el paquete del sistema principal local.

Respuesta del Usuario: Esto indica que hay demasiadas conexiones pendientes. Es posible que un administrador decida reducir el tiempo de espera asociado con la dirección varias en una para intentar eliminar las entradas desocupadas de la tabla de conversión de forma más rápida.

ICA9047 NAT ha desasignado la dirección:puerta %1\$s:%2\$s de la dirección:puerta segura %3\$s:%4\$s.

Explicación: NAT ha devuelto la pareja dirección:puerta especificada a la agrupación disponible.

Acción del Sistema: Ninguna

Respuesta del Usuario: Ninguna

ICA9048 NAT ha detectado un paquete fragmentado con protocolo:%1\$s dirección:puerta %2\$s:%3\$s dirección:puerta segura %4\$s:%5\$s.

Explicación: NAT ha detectado un paquete de control FTP fragmentado o un mensaje de error de ICMP fragmentado. NAT convertirá un paquete de control FTP fragmentado, aunque no se examinen los campos de información. Si se trata de un mandato PORT fragmentado, los datos FTP serán anómalos, ya que la dirección IP del mensaje no se convierte. Si el paquete es un mensaje de error ICMP fragmentado, será desactivado.

Acción del Sistema: Véase una descripción más detallada.

Respuesta del Usuario: Si ocurre constantemente, avise al servicio de IBM.

ICA9049 NAT ha detectado un fragmento desordenado de %1\$s a %2\$s que no se ha podido convertir.

Explicación: NAT ha detectado un datagrama fragmentado que ha llegado antes que el primer fragmento del datagrama.

Acción del Sistema: NAT no puede convertir el fragmento correctamente y el datagrama es desactivado.

Respuesta del Usuario: Si ocurre constantemente, avise al servicio de IBM.

ICA9050 NAT no ha podido convertir un paquete con protocolo:%1\$s para dirección:puerta %2\$s:%3\$s de dirección:puerta segura %4\$s:%5\$hd con código de retorno %6\$s.

Explicación: NAT no ha podido convertir un paquete.

Acción del Sistema: el paquete es desactivado.

Respuesta del Usuario: Si ocurre constantemente, avise al servicio de IBM.

ICA9051 NAT ha detectado un paquete que ha llegado con protocolo:%1\$s a dirección:puerta %2\$s:%3\$s de dirección:puerta segura %4\$s:%5\$s

Explicación: NAT ha detectado la llegada de un paquete.

Acción del Sistema: Ninguna

Respuesta del Usuario: Ninguna

ICA9052 NAT ha detectado un paquete que ha salido con protocolo:%1\$s a dirección:puerta %2\$s:%3\$s de dirección:puerta segura %4\$s:%5\$s

Explicación: NAT ha detectado la salida de un paquete.

Acción del Sistema: Ninguna

Respuesta del Usuario: Ninguna

ICA9053 %1\$s %2\$s en %3\$d

Explicación: depuración

Acción del Sistema: Ninguna

Respuesta del Usuario: Ninguna

ICA9054 La dirección IP:%1\$s no puede utilizarse como dirección de interfaz no segura y dirección varias en una simultáneamente.

Explicación: No pueden ser idénticas.

Acción del Sistema: No se realiza la acción solicitada.

Respuesta del Usuario: Elija una otra dirección no segura u otra dirección varias en una.

ICA9060 Error de inicialización del servidor de configuración muy grave - socket(): %1\$s

Explicación: La inicialización del servidor de configuración ha resultado anómala, el daemon ha finalizado.

Respuesta del Usuario: Corrija el problema del sistema que se indica y vuelva a arrancar el servidor de configuración.

ICA9061 Error de inicialización del servidor de configuración muy grave - listen(): %1\$s

Explicación: La inicialización del servidor de configuración ha resultado anómala, el daemon ha finalizado.

Respuesta del Usuario: Corrija el problema del sistema que se indica y vuelva a arrancar el servidor de configuración.

ICA9062 Error del servidor de configuración muy grave - main accept(): %1\$s

Explicación: La rutina principal del servidor de configuración ha resultado anómala, el daemon ha terminado.

Respuesta del Usuario: Corrija el problema del sistema que se indica y vuelva a arrancar el servidor de configuración.

ICA9063 Error del servidor de configuración - %1\$s: código de retorno = 0x%2\$s

Explicación: El servidor de configuración ha detectado un error en la función indicada. El daemon está finalizando.

Respuesta del Usuario: Corrija el problema del sistema que se indica y vuelva a arrancar el servidor de configuración.

ICA9064 Opción desconocida -%1\$s ignorada.

Explicación: La opción mencionada se ha especificado y no se reconoce.

ICA9065 Error del servidor de configuración - %1\$s: %2\$s

Explicación: El servidor de configuración ha detectado un error en la función indicada. El daemon está finalizando.

Respuesta del Usuario: Corrija el problema del sistema que se indica y vuelva a arrancar el servidor de configuración.

ICA9066 No existe suficiente memoria: servidor de configuración: malloc(%1\$s) ha devuelto NULL en la función %2\$s.

Explicación: No se puede asignar suficiente memoria; malloc ha devuelto NULL.

ICA9067 El vínculo ha resultado anómalo, la dirección: %1\$s ya está en uso.

Explicación: La dirección de puerta indicada está en uso.

Acción del Sistema: El servidor de configuración finaliza.

Respuesta del Usuario: Conéctese al servidor de configuración con otra dirección de puerta, o póngase en contacto con el administrador del cortafuegos.

ICA9068 La opción `-%1$s` ha resultado anómala o se ha especificado incorrectamente.

Explicación: La opción indicada ha resultado anómala o se ha especificado incorrectamente.

Acción del Sistema: El servidor de configuración finaliza.

Respuesta del Usuario: Corrija el uso de la opción indicada y reinicie el servidor de configuración.

ICA9069 La inicialización de SSL ha resultado anómala.

Explicación: El entorno de cifrado SSL no se ha podido inicializar o el procedimiento de saludo con el otro sistema ha resultado anómalo.

Acción del Sistema: El servidor de configuración finaliza.

Respuesta del Usuario: Consulte al administrador del cortafuegos para verificar el entorno SSL.

Apéndice B. Delimitación de la configuración del sistema Windows NT

La delimitación es un proceso que maximiza la seguridad y la eficacia desactivando los daemons que no se necesitan e inhabilitando los ID de usuarios sin autorización. La delimitación forma parte de la instalación del software de IBM Firewall y edita los recursos del sistema que podrían comprometer la seguridad.

Los servicios que no se necesitan para la configuración del IBM Firewall y que constituyen una amenaza potencial para la seguridad se inhabilitan. Todos los protocolos que no son TCP/IP se suprimen.

Apéndice C. Obtención de Peticiones de comentarios (RFC)

Peticiones de comentarios (RFC) son documentos que presentan nuevos protocolos y establecer estándares para la suite de protocolos de Internet. Las copias impresas de las RFC pueden obtenerse en el Network Information Center (NIC), individualmente o como suscripción. También puede obtener estos documentos de:

Government Systems, Inc.
Attn: Network Information Center
14200 Park Meadow Drive
Suite 200
Chantilly, VA 22021

Puede acceder a las RFC desde este URL:

<http://www.cis.ohio-state.edu/hypertext/information/rfc.html>.

Existen copias en línea de NIC que pueden obtenerse utilizando el FTP para conectarse a `ds.internic.net`. Puede transferir los archivos utilizando el formato siguiente:

RFC:RFC`nnnn`.TXT
RFC:RFC`nnnn`.PS

Donde:

`nnnn` Es el número de RFC
TXT Es el formato de texto
PS Es el formato PostScript

El formato para los índices de RFC es:

RFC:RFC-INDEX.TXT

Nota: Muchas RFC sólo están disponibles en formato de texto. Antes de solicitar un archivo PostScript, compruebe primero el índice de RFC para asegurarse de que la RFC está disponible en ese formato. También puede solicitar copias en línea de las RFC a través del correo electrónico, desde el servidor de correo del NIC automatizado, enviando un mensaje a `mailserv@ds.internic.net`. En el cuerpo de la nota, debe incluir uno de los mandatos siguientes:

SEND RFC`nnnn`.TXT
o
SEND RFC`nnnn`.PS

Donde:

`nnnn` Es el número de RFC
TXT Es el formato de texto
PS Es el formato PostScript

Por ejemplo, para solicitar el formato de texto de la RFC 812, debe especificar en el cuerpo de la nota:

SEND RFC812.TXT

Para solicitar una copia en línea del índice de RFC, incluya el mandato siguiente en el cuerpo de la nota:

SEND RFC-INDEX.TXT

Apéndice D. Formato del archivo de configuración Socks5.conf de IBM eNetwork Firewall

El archivo de configuración **socks5.conf** se encuentra, por omisión, en el directorio de instalación de IBM Firewall. Si lo desea, puede editar este archivo mediante un editor de texto.

El archivo de configuración **socks5.conf** se lee cuando se invoca el servidor por primera vez. (Para realizar la renovación sin detener el tipo `socks5.config`). Este archivo contiene toda la información que IBM Firewall necesita para determinar qué interfaz se ha de utilizar para acceder a una dirección determinada, si se puede establecer una conexión directamente con una dirección determinada o se ha de utilizar otro servidor proxy y qué requisitos se necesitan para establecer una conexión proxy.

Los siguientes apartados forman parte del archivo de configuración:

- Alias
- Variables
- Módulos
- Autentificación
- Direccionamiento
- Proxis
- Control de acceso

En los apartados de Autentificación, Direccionamiento, Proxis y Control de acceso, las líneas se leen en orden hasta que se encuentra una coincidencia para ese apartado: el orden de las líneas es muy importante. Para que una línea coincida, cada entrada de la línea debe coincidir.

Especificación de puertas

Para especificar puertas puede utilizarse un nombre, número o rango. Los rangos empiezan con un [o (y terminan con un) o] dependiendo de si son o no inclusivos. Los delimitadores de rango deben incluir dos indicadores de puerta (nombres o números), separados por una coma. Al método de especificación de puertas se hace referencia como *patrón de puertas*.

Especificación de sistema principales

Las direcciones de sistema principal y las máscaras de red suelen ser necesarias para especificar qué sistema principal se aplica para una norma determinada. Al método de especificación de sistemas principales se hace referencia como patrón de sistemas principales. Existen varias maneras de especificar la pareja sistema principal/máscara:

Parámetro	Descripción
IP de sistema principal/máscara	Una dirección de sistema principal "ANDed" con la máscara debe ser la misma que una IP de sistema principal "ANDed" con la máscara. Esto suele utilizarse para eliminar de la parte de red o subred la máscara de la parte de sistema principal.
-	Todo coincide. Están permitidos todos los sistemas principales.
n1	Equivalente a n1.0.0.0/255.0.0.0.
n1.n2	Equivalente a n1.n2.0.0/255.255.0.0.
n1.n2.n3	Equivalente a n1.n2.n3.0/255.255.255.0.
.nombre.de.dominio	El nombre de sistema principal debe terminar con la cadena <i>.nombre.de.dominio</i> .
un.nombre.de.sistema.principal	El nombre de sistema principal debe coincidir exactamente con <i>un.nombre.de.sistema.principal</i> .

También se da soporte a la sintaxis más antigua del patrón de sistemas principales, tal como se describe a continuación. Si embargo, se recomienda el método más reciente, que es más fácil de leer.

Parámetro	Descripción
IP de sistema principal/a	Todo coincide (lo mismo que "-"). Están permitidos todos los sistemas principales.
IP de sistema principal/n	Coincidencia de red. Elimina la máscara de la parte de sistema principal y de subred de la dirección, dejando sólo la parte de red. La máscara utilizada para hacer esto depende de la clase de direcciones IP del sistema principal.
IP de sistema principal/s	Coincidencia de subred. Elimina la máscara de la parte de sistema principal de la dirección, dejando sólo la parte de subred y de red. La máscara utilizada para hacer esto depende de la clase de direcciones IP del sistema principal.
IP de sistema principal/h	Coincidencia de sistema principal. Equivalente a IP de sistema principal.

Especificación de métodos de autenticación

Los métodos de autenticación que se suministran son *ibmcram* y *ibmpwd*. Se pueden añadir otros.

Los métodos de autenticación pueden especificarse como una lista en la que dichos métodos están separados por una coma. Para que una línea coincida, el método de autenticación que elija tiene que ser uno de los métodos de esta lista. A esta sintaxis se hace referencia como patrón de autenticación. El método de

autenticación NULL es el que se ha definido por omisión. Pueden incluirse otros métodos cargando el módulo o los módulos adecuados. A "-" indica que se acepta cualquier método de autenticación, incluido NULL.

Entradas de autenticación

Las entradas de autenticación indican el tipo o los tipos de autenticación que pueden utilizarse. El formato es:

```
auth/ban  dirección_origen  puerta_origen
métodos_autenticación
```

Parámetro	Descripción
auth/ban	Indica si las entradas de autenticación se han autorizado (auth) o no (ban).
dirección_origen	Un patrón de sistema principal válido.
puerta_origen	Un patrón de puerta válido.
métodos_autenticación	Un patrón de autenticación válido.

La palabra clave "ban" indica que la autenticación no debe intentarse en ningún caso con este sistema principal y que no es válida para el servidor especificado.

Si no se ha especificado ninguna línea auth/ban, el valor por omisión es que cualquier método de autenticación es válido. Si el permiso para la conexión se ha establecido en *deny* (el valor por omisión), la conexión no podría rechazarse hasta después de haber aplicado la autenticación. En el protocolo SOCKS5, la autenticación tiene lugar después de la autorización. Basándose únicamente en el sistema principal, debe decidir cómo se va a autenticar dicho sistema principal.

Especificación de mandatos

Los mandatos también pueden especificarse como una lista en la que dichos mandatos están separados por una coma. A esta sintaxis se hace referencia como patrón de mandato. Los mandatos definidos son: connect, bind, udp, ping y traceroute. Pueden añadirse otros mandatos mediante módulos. A "-" (raya) indica que se acepta cualquier mandato.

Carga de módulos

Los módulos permiten personalizar las funciones del servidor al añadir métodos de autenticación, mandatos, comprobaciones de autorización y filtros de contenido nuevos. El formato es: *módulo sub nombre_archivo opciones*

Parámetro	Descripción
módulo	El identificador del módulo que se ha de cargar.
stub	Un prefijo que depende del módulo, que se utiliza para acceder a nombres de función.
nombre_archivo	El nombre de archivo del módulo que se ha de cargar.
opciones	Información de configuración específica del módulo, si la hay.

Los módulos pueden definir campos usados en cualquier sitio, por lo que es mejor colocar líneas de módulo en primer lugar. Por ejemplo, los módulos de autenticación definen métodos de autenticación utilizados en las líneas auth y permit.

Direccionamiento de entradas

En máquinas con varias interfaces de red (por lo tanto, con varias direcciones IP), es aconsejable asegurarse de que determinadas interfaces de red se utilicen junto con determinadas direcciones. Esto impide la "simulación de IP" (máquinas que están fuera de la red aparentan ser máquinas que están dentro de la red), al garantizar que las máquinas de dentro de la red utilizan la interfaz de red interna y que la máquinas de fuera de la red utilizan la interfaz de red externa. También lo utiliza el servidor SOCKS para determinar la interfaz de red que se ha de enlazar al aceptar una petición de BIND o cuando se emite una petición SENDTO. Si no coincide ninguna entrada, se utiliza INADDR_ANY para enlazar y puede recibirse una conexión en cualquier interfaz. Los sistemas principales con una sola dirección no tienen entradas de direccionamiento; sólo son necesarios para máquinas con más de una interfaz de red. El formato es: **route** *dirección_destino* *puerta_destino* *dirección_interfaz*

Parámetro	Descripción
route	Palabra clave que indica las entradas de direccionamiento.
dirección_destino	Un patrón de sistema principal válido.
puerta_destino	Un patrón de puerta válido.
dirección_interfaz	La dirección IP de una tarjeta de la interfaz de la red o bien el nombre de la interfaz de la red (por ejemplo, elnk31).

Entradas de variables

El número y el tipo de mensajes de registros e informativos puede controlarse mediante diferentes variables e identificadores en el archivo de configuración. El formato es: **set** *valor de variable*

Parámetro	Descripción
set	Palabra clave para establecer la entradas de variables de entorno para uso local.
variable	Una variable de entorno válida. Consulte el apartado “Variables de entorno” en la página 159 siguiente para obtener una lista de las variables disponibles.
valor	El valor que se ha de asignar.

Variables de entorno

Variable de entorno	Descripción
SOCKS5_BINDPORT [puerta]	Configura IBM Firewall para que utilice la puerta especificada, en lugar de la puerta por omisión 1080.
SOCKS5_RECVFROMANYONE	Si el soporte UDP está habilitado, esta variable permite a los clientes de UDP recibir mensajes de remitentes desconocidos.
SOCKS5_USECLIENTSPORT	Configura IBM Firewall para Proxy sólo si puede enlazarse con la misma puerta que el cliente utiliza para enviar mensajes. Es necesaria para establecer conexiones UDP de proxy cuando el servidor está enviando datos al cliente en modalidad continua (es decir, envía mensajes al cliente antes de que éste envíe mensajes al servidor). Un ejemplo de esto es RealAudio.
SOCKS5_MAXCHILD	Número máximo de hebras simultáneas.
SOCKS5_NOREVERSEMAP	Inhabilita la correlación de direcciones IP con los nombres de sistema principal. Si se han asignado alias en el archivo de configuración, aumentaría el rendimiento a costa de la información de registro.
SOCKS5_NOSERVICENAME	Inhabilita la correlación de números de puerta con nombres de servicio. Si se han asignado alias en el archivo de configuración, aumentaría el rendimiento a costa de la información de registro.
SOCKS5_NOIDENT	Inhabilita peticiones IDENT, incluso si se han compilado. Es la adecuada cuando el enlace con los clientes es lento y éstos no utilizan IDENTD. Reduce intervalos de espera.
SOCKS5_DEMAND_IDENT	Configura la autenticación NULL para que sea anómala si no hay una respuesta IDENT por parte de los clientes. Es la adecuada para garantizar que un nombre de usuario esté siempre asociado con una petición de conexión.

Entradas proxy

Las entradas proxy describen las direcciones de los servidores proxy SOCKS. Estas líneas indican al servidor cómo debe ponerse en contacto con un sistema principal determinado. Si ninguna línea coincide con un sistema principal, la conexión con el sistema principal tiene lugar directamente. El formato es:
tipo_proxy dirección_destino puerta_destino dirección_proxy puerta_proxy

Parámetro	Descripción
tipo_proxy	El tipo del servidor proxy. Las entradas válidas son: <ul style="list-style-type: none">• socks5• socks4• no proxy
dirección_destino	Un patrón de sistema principal válido.
puerta_destino	Un patrón de puerta válido.
dirección_proxy	La dirección IP o bien el nombre del servidor proxy.
puerta_proxy	La puerta del servidor proxy en la que el daemon SOCKS acepta conexiones.

Entradas de control de acceso

El apartado de control de acceso determina si se permite o deniega una petición para establecer una conexión. Hay dos tipos de líneas: permit y deny. Cada una de las entradas de la línea deben coincidir para que toda la línea coincida. El formato es:

```
permit auth cmd sist_pral_origen sist_pral_destino  
puerta_origen puerta_destino [lista_usuarios]  
deny auth cmd sist_pral_origen sist_pral_destino  
puerta_origen puerta_destino [lista_usuarios]
```

Parámetro	Descripción
auth	Una lista de métodos de autenticación, especificada mediante una patrón auth y una entrada auth válidos.
cmd	Un patrón de mandatos válido que especifica los mandatos que coinciden en esta línea.
sist_pral_origen	Un patrón de sistema principal válido para el sistema principal de origen.
sist_pral_destino	Un patrón de sistema principal válido para el sistema principal de destino.
puerta_origen	Un patrón de puerta válido para la puerta de sistema principal de origen.
puerta_destino	Un patrón de puerta válido para la puerta de sistema principal de destino.
lista_usuarios	Un patrón de usuario válido.

Filtros

El filtrado mediante un módulo cargado se lleva a cabo aplicando la norma filter. El formato es:

```
filter nombre auth cmd sist_pral_origen sist_pral_destino  
puerta_origen puerta_destino [lista_usuarios]
```

Parámetro	Descripción
nombre	El identificador del módulo de filtro.
auth	Una lista de métodos de autenticación, especificada mediante una patrón auth y una entrada auth válidos.
cmd	Un patrón de mandatos válido que especifica los mandatos que coinciden en esta línea.
sist_pral_origen	Un patrón de sistema principal válido para el sistema principal de origen.
sist_pral_destino	Un patrón de sistema principal válido para el sistema principal de destino.
puerta_origen	Un patrón de puerta válido para la puerta de sistema principal de origen.
puerta_destino	Un patrón de puerta válido para la puerta de sistema principal de destino.
lista_usuarios	Un patrón de usuario válido.

Bibliografía

Para obtener información adicional acerca de la seguridad en Internet, visite la página de presentación de IBM Firewall en la dirección <http://www.software.ibm.com/enetwork/firewall>.

Información en publicaciones de IBM

A continuación se listan otras fuentes de información de IBM acerca de los cortafuegos, la seguridad en Internet y temas que tratan la seguridad general.

Temas acerca de cortafuegos

Los documentos siguientes están disponibles en el CD-ROM del IBM Firewall y en la página de presentación del IBM eNetwork Firewall.

- *IBM eNetwork Firewall - Guía del usuario*, GC31-8658
- *IBM eNetwork Firewall - Manual de consulta*, SC31-8659
- *Vigilar las puertas con IBM eNetwork Firewall para NT 3.2*, SG24-5209

Temas acerca de Internet y de la World Wide Web

- *A Guide to the Internet Connection Servers*, SG24-4805
- *Accessing CICS Business Applications from the World Wide Web*, SG24-4547
- *Accessing OS/390 OpenEdition MVS from the Internet*, SG24-4721
- *Accessing the Internet*, SG24-2597
- *Building the Infrastructure for the Internet*, SG24-4824
- *Cool Title about the AS/400 and Internet*, SG24-4815
- *The Domino Defense: Security in Lotus Notes and the Internet*, SG24-4848
- *Examples of Using MQSeries on WWW*, SG24-4882
- *How to Secure the Internet Connection Server for MVS/ESA*, SG24-4803
- *Lotus Domino Server Release 4.5 on AIX Systems: Installation, Customization, and Administration*, SG24-4694

- *Netscape Proxy Server*, SK2T-7444
- *Running CICS Transactions through the Web: The CICS Internet Gateway to VSE/ESA*, SG24-4799
- *Safe Surfing: How to Build a Secure World Wide Web Connection*, SG24-4564
- *Teach Yourself CGI Programming with PERL in a Week*, SR23-7343
- *Using the Information Super Highway*, GG24-2499
- *World Wide Web Access to DB2*, SG24-4716

Temas acerca de la seguridad general

- *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

Información en publicaciones especializadas

Las publicaciones especializadas siguientes pertenecen a sendmail, TCP/IP y UNIX:

- Albitz, Paul, and Cricket Liu. *DNS and BIND*. Sebastopol, CA: O'Reilly and Associates, 1997. (ISBN: 1-56592-236-0)
- Costales, Brian with Eric Allman. *Sendmail* O'Reilly and Associates, Inc. (ISBN: 1-56592-222-0)
- Hunt, Craig. *TCP/IP Network Administration* O'Reilly and Associates, Inc. (ISBN: 0-937175-82-X)
- Nemeth, Snyder, et al. *UNIX System Administration Handbook* Prentice Hall. (ISBN: 0-13-151051-7)

Las publicaciones especializadas siguientes están relacionadas con los cortafuegos y con la seguridad en Internet:

- Ahuja, Vijay. *Network and Internet Security*. Boston: Academic Press Professional, 1996. (ISBN: 0120455951)
- Ahuja, Vijay. *Secure Commerce on the Internet*. Boston: Academic Press Professional, 1997. (ISBN: 0120455978)
- Anderson, Bart, et al. *The Waite Group's UNIX Communications and the Internet*. Indianapolis, IN: Sams Pub., 1995. (ISBN: 0672305372)
- Atkins, Derek, et al. *Internet Security: Professional Reference*. Indianapolis, IN: New Riders Publishing, 1996. (ISBN: 1562055577)
- Chapman, D. Brent, and Elizabeth D. Zwicky. *Building Internet Firewalls*. Sebastopol, CA: O'Reilly and Associates, 1995. (ISBN: 1565921240)
- Cheswick, William 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)

Avisos

Las referencias que se hacen en esta publicación a productos, programas o servicios de IBM no implican que IBM tenga intención de comercializarlos en todos los países en los que opera. Cualquier referencia a un producto, programa o servicio de IBM no pretende indicar ni implica que sólo pueda utilizarse ese producto, programa o servicio de IBM. De acuerdo con la propiedad intelectual vigente de IBM u otros derechos con protección legal, podrá utilizarse cualquier producto, programa o servicio funcionalmente equivalente en lugar del producto, programa o servicio de IBM. La valoración y verificación de su funcionamiento conjuntamente con otros productos, a excepción de los que IBM designa de forma expresa, son responsabilidad del usuario.

IBM podría tener patentes o solicitudes de patentes pendientes acerca del tema que se describe en este documento. La posesión de este documento no otorga ninguna licencia sobre tales patentes. Puede solicitar licencias, por escrito, a:

IBM Director of Licensing
IBM Corporation
500 Columbus Avenue
Thornwood, NY 10594
USA

Los propietarios de licencias de este programa que deseen recibir información acerca de la misma con la finalidad de permitir: (i) el intercambio de información entre programas creados independientemente y otros programas (incluido éste) y (ii) la mutua utilización de la información que se ha intercambiado, deben ponerse en contacto con:

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

Tal información podría estar disponible, de acuerdo con los términos y condiciones que se aplican, incluyendo, en algunos casos, el pago de una tarifa.

El programa bajo licencia que se describe en este documento y todo el material bajo licencia disponible para el mismo lo facilita IBM según los términos del IBM Customer Agreement.

Este documento no se destina a la utilización productiva y se adquiere tal cual, sin garantías de ningún tipo, y por la presente, se renuncia a todas las garantías, incluidas las garantías de comercialización y adecuación a una finalidad determinada.

Este producto incluye software desarrollado por la University of California, Berkeley y sus colaboradores.

Marcas registradas

Los términos siguientes son marcas registradas de IBM Corporation en los Estados Unidos y/o en otros países:

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

Microsoft, Windows, Windows NT y el logotipo de Windows 95 son marcas registradas o nombres comerciales registrados de Microsoft Corporation.

UNIX es una marca registrada en los Estados Unidos y otros países que se obtiene bajo licencia exclusivamente de X/Open Company Limited.

Java y HotJava son marcas registradas de Sun Microsystems, Inc.

Los otros nombres de empresas, productos o servicios, que podrían indicarse mediante un doble asterisco (**), pueden ser marcas registradas o marcas de servicio de otros.

Glosario

Puede acceder al glosario IBM Software en la dirección:
<http://www.networking.ibm.com/nsg/nsgmain.htm>.

Índice

Caracteres Especiales

(MKKF), Utilización del Programa de utilidad de creación de archivo de claves 59
(RFC), Peticiones de comentarios 153

A

a_alert.tbl 26
acuerdo de licencia 165
ADMIN_ALERT 29
archivo de claves, creación de un 59
Autenticación suministrada por el usuario 49
Autenticación, suministrada por el usuario 49

B

bibliografía 163

C

Centro de soporte de IBM vii
Centro de soporte, de IBM vii
consultas 163
Consultas de ejemplo 28
Consultas, ejemplo 28
Control del tráfico 71
Conversión de dirección de red 11
conversión de direcciones de red vi
Convertir direcciones IP seguras 11
Correlacionar direcciones IP seguras 11
Creación de un archivo de claves 59

D

DB2 27
DB2/6000 o DB2/2 23
delimitación 151
Dirección registrada de varias en una 11
direcciones de red, conversión vi
Direcciones IP seguras, convertir 11
Direcciones IP seguras, correlacionar 11
Direcciones IP seguras, excluir 11
direcciones IP, cómo especificarlas vii
Direcciones IP, convertir seguras 11
Direcciones IP, correlacionar seguras 11
Direcciones IP, excluir seguras 11
Direcciones, convertir IP seguras 11
Direcciones, correlacionar IP seguras 11
Direcciones, excluir IP seguras 11

E

especificación de direcciones IP, cómo realizarla vii
Excluir direcciones IP seguras 11

F

f_info.tbl 26
f_match.tbl 26
f_rule.tbl 26
f_stat.tbl 26
FILTER_ACTIVE_RULE 29
FILTER_INFO 29
FILTER_MATCH 29
FILTER_STATUS 29
Filtros 3
fwfilter 3
fwimport.dat 23
fwinterface 4
fwlog 6
fwlogcvrt 23
fwlogmon 8
fwlogtbl 23, 24
fwlogtxt 23, 24
fwmail 10
fwnat 11
fwqrysmp.dml 23
fwschema.ddl 23, 27
fwuser 18

G

Generación de mensajes 25
Gestión de Archivos de Registro 6
Gestión de archivos, de registro 6
Gestión, archivos de registro 6
Grupos funcionales administrativos 21
Grupos funcionales, administrativos 21
Grupos, funcionales administrativos 21

I

Interfaces 4, 29
interfaces.tbl 26
Interfaz de línea de mandatos 1

M

mensajes 75
Mensajes, generación 25
métodos de autenticación 49
métodos, autenticación 49

N

NAT vi, 73
NAT_INFO 29
nat_info.tbl 26

P

p_ftp.tbl 26
p_http.tbl 26
p_info.tbl 26
p_login.tbl 26
p_stat.tbl 26
PAGER_INFO 29
página Web 163
Parámetros básicos 18
Parámetros, básicos 18
Peticiones de comentarios (RFC) 153
Problemas DNS 69
programas de utilidad de informes 23, 73
programas de utilidad, informes 23
proxy HTTP 3
PROXY_FTP 29
PROXY_HTTP 29
PROXY_INFO 29
PROXY_LOGIN 29
PROXY_STATUS 29
proxy, HTTP 3

R

Recursos de registro 73
red, conversión de direcciones vi
registro del cortafuegos 23
registro, cortafuegos 23
Resolución de problemas y comprobación 67

S

s_ftp.tbl 26
s_info.tbl 26
SERVER_INFO 29
server_info.tbl 26
Servicios de denominación de dominios 2
Servicios de denominación, dominios 2
Servicios, denominación de dominios 2
Servidor de configuración 1
Servidores proxy 72
SESSION 29
session.tbl 26
SOCKS_FTP 29
SOCKS_INFO 29
SSL_INFO 29
ssl_info.tbl 26
SU 29
Supervisor de registro 8

T

Tablas SQL 29
Tablas, SQL 29
TUNNEL_CONTEXT 29
TUNNEL_POLICY 29
TUNNEL_STATUS 29

U

un archivo de claves, creación 59
URL 163
Utilización de los programas de utilidad de informes 23
Utilización del Programa de utilidad de creación de archivo de claves (MKKF) 59

V

Varias en una, dirección registrada 11

Hoja de Comentarios

IBM eNetwork Firewall para Windows NT

Manual de consulta

Versión 3 Release 2.1.1

Número de Publicación SC10-3280-01

En general, ¿está Ud. satisfecho con la información de este libro?

	Muy satisfecho	Satisfecho	Normal	Insatisfecho	Muy insatisfecho
Satisfacción general	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

¿Cómo valora los siguientes aspectos de este libro?

	Muy bien	Bien	Acep- table	Insatisfecho	Muy insatisfecho
Organización	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Información completa y precisa	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Información fácil de encontrar	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Utilidad de las ilustraciones	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Claridad de la redacción	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Calidad de la edición	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Adaptación a los formatos, unidades, etc. del país	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Comentarios y sugerencias:

Nombre

Dirección

Compañía u Organización

Teléfono



Dóblese por la línea de puntos

Por favor no lo grape

Dóblese por la línea de puntos

PONER
EL
SELLO
AQUÍ

IBM, S.A.
National Language Solutions Center
Av. Diagonal, 571
08029 Barcelona
España

Dóblese por la línea de puntos

Por favor no lo grape

Dóblese por la línea de puntos



Printed in the United States of America
on recycled paper containing 10%
recovered post-consumer fiber.

SC10-3280-01

