MS81: WebSphere® MQ internet pass-thru Versión 1.2

SC10-3826-00

Aviso

Antes de utilizar esta información y el producto al que se refiere, lea la información general del apartado "Avisos" en la página vii.

Primera edición, marzo de 2002

Este manual es la traducción del original inglés *MS81 WebSphere MQ internet pass-thru Version 1.2* , SC34-6100-00.

Esta edición se aplica a la Versión 1.2 de MS81: WebSphere MQ internet pass-thru (número de programa 5639-L92) y a todos los releases y modificaciones posteriores hasta que se indique lo contrario en nuevas ediciones.

En la parte posterior de esta publicación se incluye una hoja para comentarios del lector. **Copyright International Business Machines Corporation 2000–2002. Reservados todos los derechos**. Derechos restringidos para los usuarios del gobierno de los EE.UU. - Documentación relacionada con derechos limitados - El uso, duplicación o divulgación están restringidos por GSA ADP Schedule Contract con IBM Corporation.

© Copyright International Business Machines Corporation 2000-2002. Reservados todos los derechos.

Contenido

© Copyright IBM Corp. 2000-2002

Figuras

© Copyright IBM Corp. 2000-2002

Avisos

El párrafo siguiente no se aplica al Reino Unido ni a ningún otro país en el que dichas disposiciones no sean compatibles con la legislación vigente.

INTERNATIONAL BUSINESS MACHINES CORPORATION FACILITA ESTA PUBLICACIÓN ″TAL CUAL″ SIN GARANTÍAS DE NINGÚN TIPO, NI EXPLÍCITAS NI IMPLÍCITAS, INCLUYENDO, PERO SIN LIMITARSE A, LAS GARANTÍAS IMPLÍCITAS DE NO INFRACCIÓN, COMERCIALIZACIÓN O ADECUACIÓN A UN FIN CONCRETO. Algunos estados o países no permiten la renuncia a las garantías explícitas o implícitas en ciertas transacciones, por tanto, es posible que esta declaración no resulte aplicable a su caso.

Las referencias realizadas en esta publicación a productos, programas o servicios IBM, no implican que IBM piense ponerlos a disposición en todos los países en los que IBM opera.

Las referencias a programas, productos o servicios de IBM hechas en esta publicación no pretenden establecer ni implicar que sólo puedan utilizarse los productos, programas o servicios de IBM. En lugar del producto de IBM se puede utilizar cualquier programa que sea funcionalmente equivalente y que no vulnere los derechos de propiedad intelectual. Será responsabilidad del usuario evaluar y verificar el funcionamiento con otros productos que no sean los designados explícitamente por IBM.

IBM puede tener patentes o solicitudes de patentes pendientes que cubran el tema principal descrito en esta información. La entrega de este documento no le otorga ninguna licencia sobre dichas patentes. Puede enviar consultas de licencias, por escrito, a IBM Director of Licensing, IBM Corporation, 500 Columbus Avenue, Thornwood, Nueva York 10594, EE.UU.

La información contenida en este documento no ha sido sometida a ninguna prueba oficial de IBM y se distribuye TAL CUAL. Queda bajo la responsabilidad del cliente el uso de la información o la implementación de cualquiera de estas técnicas y su evaluación e integración en el entorno operativo del cliente dependerán de la habilidad del mismo. Aunque IBM ha revisado la precisión de cada uno de los elementos en una situación específica, no se garantiza que puedan obtenerse los mismos resultados o resultados similares en otras situaciones. Los usuarios que intenten adaptar estas técnicas a sus propios entornos lo harán bajo su propio riesgo.

Marcas registradas

Los siguientes términos son marcas registradas de International Business Machines Corporation en Estados Unidos y en otros países:

AIX	FFST	First Failure Support Technology
IBM	IBMLink	MQSeries
SupportPac	WebSphere	

© Copyright IBM Corp. 2000-2002

Microsoft, Windows, Windows NT y el logotipo de Windows son marcas registradas de Microsoft Corporation en Estados Unidos o en otros países.

Otros nombres de empresas, productos y servicios pueden ser marcas comerciales o marcas de servicio de otras compañías.

Prefacio

Qué es internet pass-thru

Anteriormente, WebSphere MQ internet pass-thru se denominaba MQSeries internet pass-thru. En esta publicación, se hará referencia a MQSeries como WebSphere MQ. Tenga en cuenta que no todas las publicaciones de MQSeries cambiarán directamente el nombre a WebSphere MQ y que, por lo tanto, durante algún tiempo se hará referencia a MQSeries y a WebSphere MQ.

IBM® WebSphere MQ internet pass-thru:

- Es una extensión del producto base WebSphere MQ que se puede utilizar para implementar las soluciones de mensajería entre sitios remotos a través de Internet.
- Facilita la entrada y salida de un cortafuegos de los protocolos de WebSphere MQ y hace que resulten más manejables gracias a la función de túnel HTTP para protocolos o a que puede actuar como un servidor proxy.
- Funciona como un servicio autónomo que puede recibir y enviar flujos de mensajes de WebSphere MQ. No es necesario que el sistema en el que se ejecuta contenga un gestor de colas WebSphere MQ.
- Le permite proporcionar transacciones de empresa a empresa mediante WebSphere MQ.
- Permite utilizar las aplicaciones WebSphere MQ existentes, sin modificar, a través de un cortafuegos.
- Proporciona un solo punto de control del acceso a varios gestores de colas.
- Permite cifrar todos los datos.

En este manual, para facilitar su uso, se hace referencia a WebSphere MQ internet pass-thru como “MQIPT”.

A quién va dirigida esta publicación

Este manual va dirigido a diseñadores de sistemas, administradores técnicos de WebSphere MQ y administradores de redes y cortafuegos.

Conocimientos necesarios para comprender esta publicación

Deberá tener una sólida formación acerca de:

- La administración de los gestores de colas y canales de mensajes de WebSphere MQ, como se describe en las publicaciones *MQSeries Administración del sistema* y *MQSeries Intercommunication.*
- El modo en que se implementan los cortafuegos.
- El direccionamiento y los sistemas de redes de los protocolos de Internet.
- IBM Network Dispatcher para el equilibrio de carga y una mayor disponibilidad.
- IBM WebSphere Application Server.

Requisitos previos

Este release de internet pass-thru se ejecuta en estas plataformas:

- Windows NT® V4.0, con Service pack 6

© Copyright IBM Corp. 2000-2002

- Windows 2000
- Windows XP
- Sun Solaris
- AIX®
- HP-UX 11
- Linux

Nota: AIX y HP-UX estarán disponibles cuando haya un release de Java 1.4 para dichas plataformas.

El release de JDK debe ser del nivel 1.4.0 o un release superior compatible.

El único protocolo de red soportado es TCP/IP.

La ayuda del cliente de administración requiere un navegador Netscape.

Información sobre accesibilidad

La GUI del cliente de administrador se ha creado para mejorar la accesibilidad. Permite realizar directamente todas las funciones disponibles sin utilizar un ratón, simplemente con las combinaciones de teclas equivalentes. Puede desplazarse por la pantalla utilizando el tabulador, la tecla de mayúsculas más el tabulador, la tecla de control más el tabulador y las teclas del cursor, como se hace habitualmente. Se puede realizar la función equivalente a pulsar los botones si se selecciona el botón y luego se pulsa Intro.

Se pueden seleccionar las funciones de menú combinando el tabulador y las del cursor o utilizando las teclas de método abreviado que están disponibles para todas las opciones. Por ejemplo, la GUI se puede cerrar seleccionando alt-f y luego alt-q (Archivo->Salir). Cuando haya llegado a un elemento de menú, puede activarlo con la tecla Intro.

Puede desplazarse por el árbol utilizando las teclas del cursor. En especial, las teclas de derecha e izquierda del cursor se pueden utilizar para abrir o cerrar un nodo MQIPT, lo que permite mostrarlo u ocultarlo.

Se puede modificar el estado de los recuadros de selección con la tecla espaciadora. Con la tecla Intro, se pueden seleccionar los campos para editarlos.

Diseño

Lo ideal es que la GUI tenga el diseño del entorno. Pero como esto no siempre es posible, puede proporcionar un archivo de configuración que personalice el diseño de la GUI según sus necesidades. El nombre del archivo de configuración es "custom.properties" y debe ubicarse en el subdirectorio `bin`.

Utilice este archivo de configuración para configurar lo siguiente:

- El color de primer plano: el color del texto
- El color de fondo
- El font del texto
- El estilo del texto; ya sea sin formato, negrita, cursiva, o negrita y cursiva

Se proporciona un archivo de configuración de ejemplo "customSample.properties" que contiene comentarios sobre cómo puede modificarlo. Se le recomienda que copie este archivo en `bin/custom.properties` y que efectúe los cambios necesarios.

Bibliografía

Esta publicación está disponible en formato PDF y HTML como parte del producto instalado y se instala en los directorios que se indican en la Tabla 1. Antes de utilizar el cliente de administración, debe descomprimir el archivo que se encuentra en el subdirectorio `<idioma>/html`.

- PDF

  `doc\<idioma>\pdf\<nombrearchivo>.pdf`
- HTML (incluido en un archivo zip)

  `doc\<idioma>\html\<nombrearchivo>.zip`

La publicación se proporciona en varios idiomas. La tabla siguiente muestra el idioma y el nombre de archivo correspondiente:

Tabla 1. Resumen de idiomas y nombres de archivos

Idioma	Entorno nacional	Nombre del archivo PDF	Nombre del archivo HTML
Chino simplificado	zn_CN	amqyzb00.pdf	amqyzb00.zip
Alemán	de_DE	amqygb00.pdf	amqygb00.zip
Japonés	ja_JP	amqyjb00.pdf	amqyjb00.zip
Coreano	ko_KR	amqykb00.pdf	amqykb00.zip
Portugués del Brasil	pt_BR	amqybb00.pdf	amqybb00.zip
Español	es_ES	amqysb00.pdf	amqysb00.zip
Inglés americano	en_US	amqyab00.pdf	amqyab00.zip

También le resultarán útiles las publicaciones siguientes:

- *MQSeries Intercommunication*, SC33-1872
- *MQSeries Administración del sistema*, SC10-3081
- *MQSeries Clientes*, GC10-9654
- *MQSeries Queue Manager Clusters*, SC34-5349

En estas publicaciones se proporciona información sobre cómo definir los canales de WebSphere MQ y sus atributos, en especial, la definición de CONNAME.

Las publicaciones WebSphere MQ están disponibles en:

`http://www.ibm.com/software/ts/mqseries/library/`

© Copyright IBM Corp. 2000-2002

Resumen de cambios

Las mejoras de esta versión de WebSphere MQ internet pass-thru son:

- Configuraciones de ejemplo
- Rastreo SSL mejorado
- Java Security Manager
- Programa de utilidad KeyMan para gestionar certificados SSL y archivos de conjunto de claves
- Soporte de Linux, incluido Quality of Service para mensajes de WebSphere MQ
- Imagen de instalación de NLS disponible en plataformas Windows
- Ahora los nombres de propiedades no son sensibles a las mayúsculas y minúsculas
- Versión del servlet
- Soporte de servidor y cliente Socks
- Modalidad de proxy SSL
- Estado de semáforo para el cliente de administración
- Soporte de clúster de WebSphere MQ

© Copyright IBM Corp. 2000-2002

Capítulo 1. Introducción a WebSphere MQ internet pass-thru

WebSphere MQ internet pass-thru es una ampliación del producto WebSphere MQ base. Funciona como un servicio autónomo que puede recibir y enviar flujos de mensajes de WebSphere MQ, tanto entre dos gestores de colas de WebSphere MQ como entre un cliente de WebSphere MQ y un gestor de colas de WebSphere MQ. MQIPT permite realizar esta conexión cuando el cliente y servidor no están en la misma red física.

Se pueden colocar uno o varios MQIPT en la vía de comunicación entre dos gestores de colas de WebSphere MQ o entre un cliente de WebSphere MQ y un gestor de colas de WebSphere MQ. Los MQIPT permiten que dos sistemas WebSphere MQ intercambien mensajes sin necesidad de que haya una conexión TCP/IP directa entre ambos. Esto resulta útil si la configuración del cortafuegos no permite una conexión TCP/IP directa entre los dos sistemas.

MQIPT escucha en una o varias puertas TCP/IP las conexiones de entrada, las cuales pueden transportar mensajes de WebSphere MQ normales, mensajes de WebSphere MQ enviados en HTTP mediante la función de túnel, o mensajes cifrados mediante SSL (Secure Sockets Layer). Puede manejar varias conexiones simultáneas.

Se hace referencia al canal de WebSphere MQ que efectúa la petición de conexión TCP/IP inicial como el “canal de llamada”, al canal que está intentando realizar la conexión como el “canal de respuesta” y al gestor de colas con el que finalmente se está intentando contactar como el “gestor de colas de destino”.

Los usos previstos de MQIPT son:

- MQIPT se puede utilizar como un concentrador de canales, de modo que para un cortafuegos todos los canales dirigidos o procedentes de varios sistemas principales diferentes parecen proceder o dirigirse al mismo MQIPT. Esto facilita la definición y gestión de las normas de filtro del cortafuegos.

© Copyright IBM Corp. 2000-2002

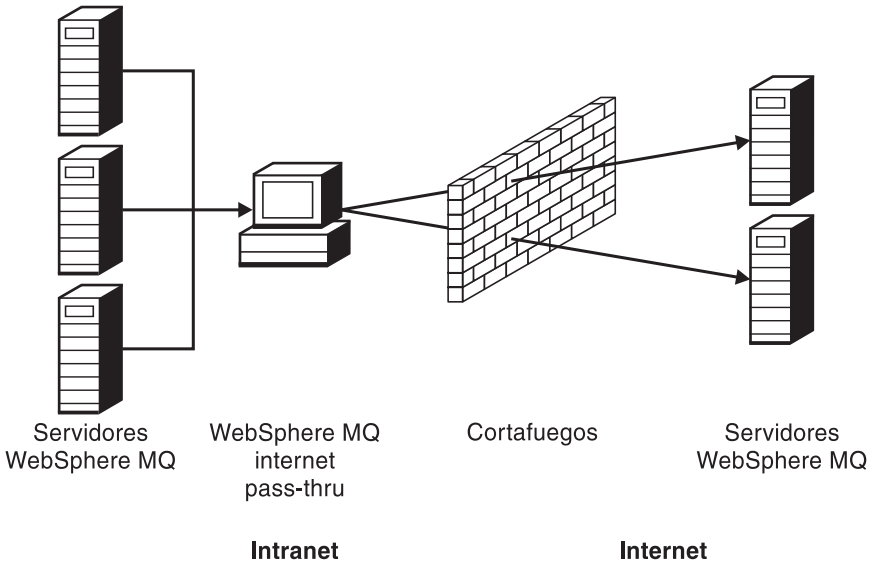

Figura 1. Ejemplo de MQIPT como un concentrador de canales

- Si MQIPT se coloca en la DMZ ("zona desmilitarizada") del cortafuegos, en una máquina con una dirección de protocolo de internet (IP) conocida y de confianza, se puede utilizar MQIPT para escuchar las conexiones de canales de WebSphere MQ de entrada que, a continuación, se pueden enviar a la intranet de confianza. El cortafuegos interno debe permitir que esta máquina de confianza realice conexiones de entrada. En esta configuración, MQIPT impide que las peticiones externas vean las direcciones IP reales de las máquinas de la intranet de confianza. De este modo, MQIPT proporciona un solo punto de acceso.

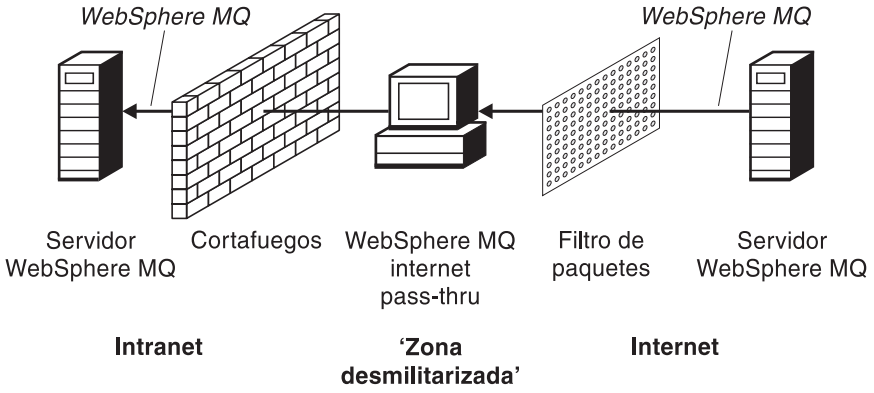

Figura 2. Ejemplo de MQIPT con una "zona desmilitarizada"

- Si se despliegan dos MQIPT en línea, se pueden comunicar utilizando HTTP o SSL. La función de túnel HTTP permite transmitir las peticiones a través de cortafuegos, mediante los servidores proxy HTTP existentes. El primer MQIPT inserta el protocolo de WebSphere MQ en HTTP y el segundo extrae el protocolo de WebSphere MQ del HTTP que lo encierra y lo dirige al gestor de colas de destino.

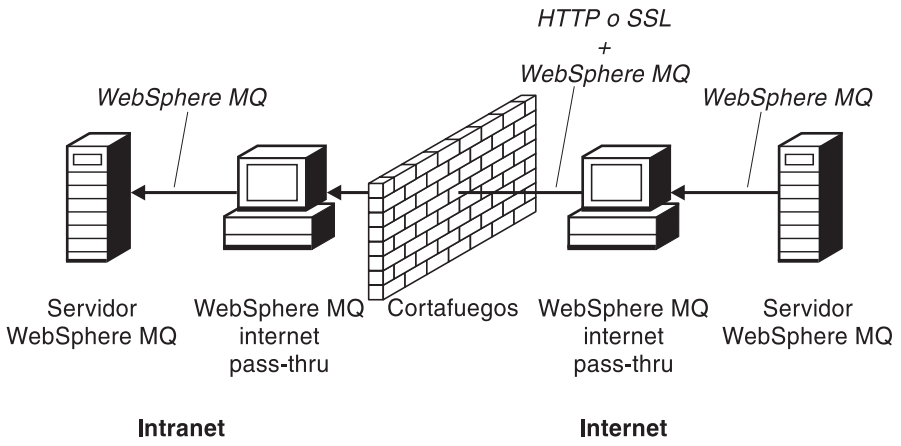

Figura 3. Ejemplo de MQIPT y la función de túnel HTTP

- Del mismo modo, se pueden cifrar las peticiones antes de transmitirlas a través de los cortafuegos. El primer MQIPT cifra los datos y el segundo los descifra utilizando SSL antes de enviarlos al gestor de colas de destino.

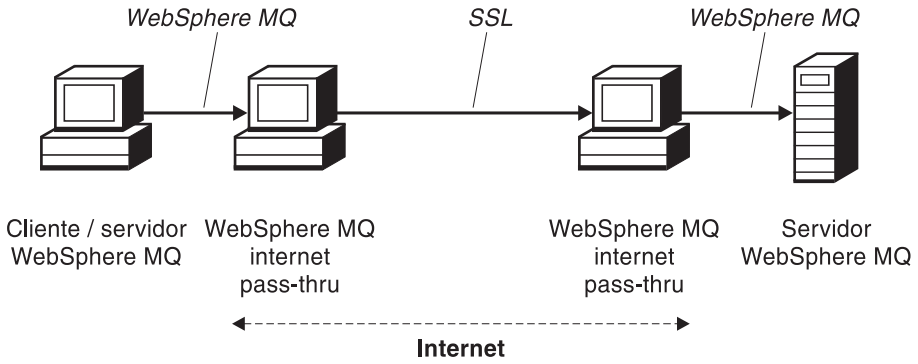

Figura 4. Ejemplo de MQIPT y SSL

MQIPT guarda los datos en la memoria mientras los envía desde el origen al destino. No se guardan datos en el disco (excepto la memoria que el sistema operativo pasa al disco). La única vez que MQIPT accede de forma explícita al disco es para leer su archivo de configuración y para grabar los registros de anotaciones y rastreo.

El rango completo de tipos de canales de WebSphere MQ puede pasarse a través de uno o varios MQIPT. La presencia de los MQIPT en una vía de comunicación no afecta a las características funcionales de los componentes de WebSphere MQ conectados, pero puede afectar al rendimiento de la transferencia de mensajes.

MQIPT se puede utilizar junto con WebSphere MQ Publish/Subscribe o con el intermediario de mensajes de WebSphere MQ.

En la Figura 5 en la página 4 se muestran todas las configuraciones posibles de los MQIPT en una topología de WebSphere MQ. Observe en la figura que el proxy HTTP, el proxy SOCKS y las máquinas MQIPT que hay detrás del cortafuegos del extremo de las “conexiones de salida” representan la posibilidad de encadenar varias máquinas en internet. Por ejemplo, una máquina MQIPT se puede comunicar a través de una o varias máquinas de proxy SOCKS o HTTP, o más máquinas MQIPT, antes de alcanzar el destino.

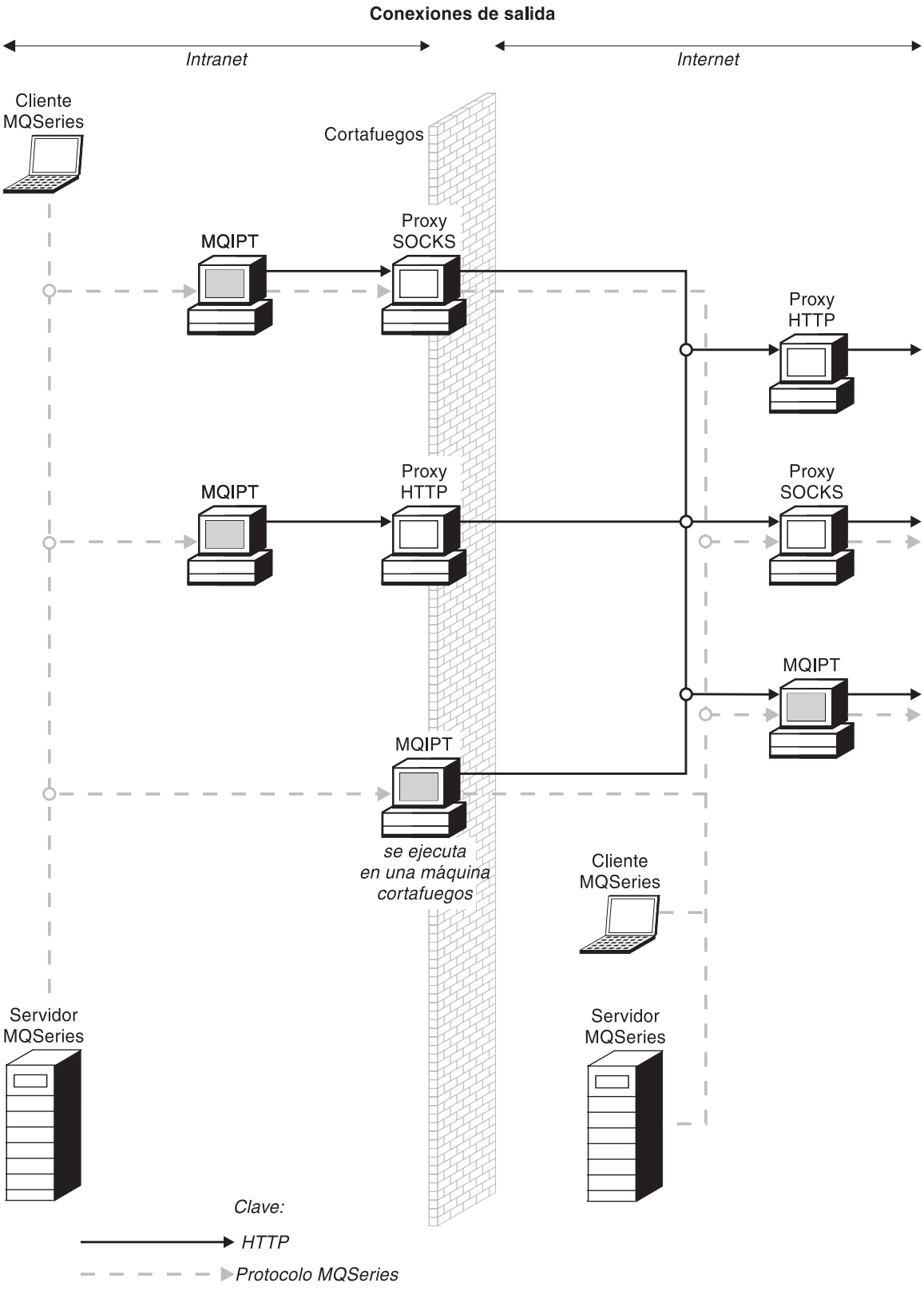

Figura 5. Topología WebSphere MQ que muestra las configuraciones posibles de MQIPT (Parte 1 de 2)

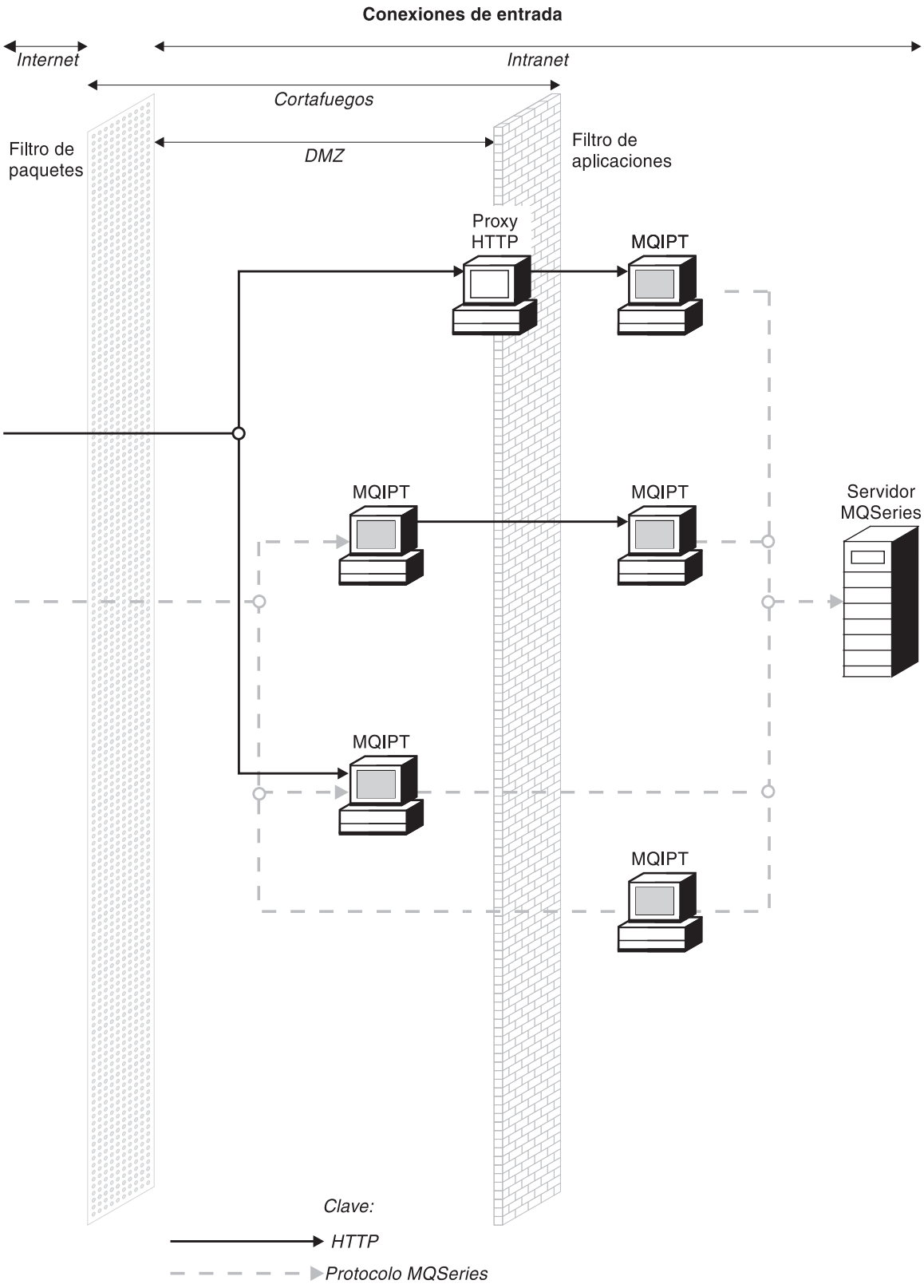

Figura 5. Topología WebSphere MQ que muestra las configuraciones posibles de MQIPT (Parte 2 de 2)

Capítulo 2. Cómo funciona internet pass-thru

En este capítulo se proporciona una visión general del funcionamiento de internet pass-thru y se describe detalladamente lo siguiente:

Visión general del funcionamiento de internet pass-thru

En la configuración más sencilla, MQIPT actúa como emisor del protocolo de WebSphere MQ. Escucha en una puerta TCP/IP y acepta las peticiones de conexión de los canales de WebSphere MQ. Si se recibe una petición con un formato válido, MQIPT establece una conexión TCP/IP adicional entre él mismo y el gestor de colas de WebSphere MQ de destino. A continuación, pasa todos los paquetes de protocolo que recibe de la conexión de entrada al gestor de colas de destino y devuelve los paquetes de protocolo del gestor de colas de destino en la conexión de entrada original.

No se realiza ningún cambio en el protocolo de WebSphere MQ (cliente/servidor o gestor de colas a gestor de colas) ya que ninguno de los extremos conoce directamente la existencia de un intermediario, por lo tanto, no se necesitan versiones nuevas del código de cliente o servidor de WebSphere MQ.

Para utilizar MQIPT, el canal de llamada debe configurarse de modo que utilice el nombre de sistema principal y la puerta de MQIPT y no el nombre de sistema principal y la puerta del gestor de colas de destino. Esto se define en la propiedad CONNAME del canal de WebSphere MQ. MQIPT no analiza el nombre de canal, sino que simplemente se pasa al gestor de colas de destino. Del mismo modo, también se pasan al gestor de colas de destino otros campos de configuración como, por ejemplo el ID de usuario y la contraseña de un canal de cliente/servidor.

MQIPT se puede utilizar para permitir el acceso a uno o varios gestores de colas de destino. Para que esto funcione, debe haber un mecanismo que indique a MQIPT con qué gestor ha de conectar, por lo que, como se describe en el párrafo siguiente, MQIPT utiliza el número de puerta TCP/IP de entrada para determinar con qué gestor de colas ha de conectar.

© Copyright IBM Corp. 2000-2002

Para permitir el acceso a más de un gestor de colas de destino, MQIPT puede configurarse de modo que escuche en varias puertas TCP/IP. Cada puerta de escucha se correlaciona con un gestor de colas a través de una "ruta" de MQIPT. El administrador de MQIPT puede definir un máximo de 100 rutas de este tipo, que asocian una puerta TCP/IP de escucha con el nombre de sistema principal y la puerta del gestor de colas de destino. Esto significa que el nombre de sistema principal (dirección IP) del gestor de colas de destino nunca puede visualizarse en el canal de origen. Toda ruta puede manejar varias conexiones entre su puerta de escucha y el destino y cada conexión actúa de modo independiente.

Soporte de HTTP

Opcionalmente, MQIPT se puede configurar de modo que los paquetes de datos que envía se codifiquen como peticiones de HTTP. MQIPT da soporte a los túneles HTTP con o sin fragmentación.

Debido a que los canales actuales no aceptan peticiones de HTTP, se necesita un segundo MQIPT para recibir las peticiones de HTTP y volver a convertirlas en paquetes de protocolo de WebSphere MQ normales. El segundo MQIPT separa la cabecera HTTP para volver a convertir el paquete de entrada en un paquete de protocolo de WebSphere MQ estándar, antes de pasarlo al gestor de colas de destino.

Cuando se utiliza la función de túnel HTTP sin fragmentación, para cada petición de HTTP se devuelve una respuesta HTTP al primer MQIPT. Esta respuesta puede ser la respuesta del gestor de colas de destino o un reconocimiento ficticio. Si uno de los sistemas WebSphere MQ ha de enviar una cadena de paquetes de protocolos de WebSphere MQ de forma continuada (como sucede cuando se transfiere un mensaje de gran tamaño), para transferir los datos se utilizan varios pares de petición/respuesta HTTP. Para ello, MQIPT inserta flujos de peticiones o de respuestas adicionales.

Cuando se utiliza la función de túnel HTTP con fragmentación, una cabecera HTTP sólo incluirá el primer paquete. Los paquetes medio y último tendrán cabeceras fragmentadas. Por lo tanto, no será necesario esperar un reconocimiento ficticio del segundo MQIPT y el rendimiento mejorará ligeramente en comparación con la función de túnel HTTP sin fragmentación.

Cuando se utiliza HTTP entre dos MQIPT, la conexión TCP/IP por la que fluyen las peticiones y respuestas HTTP será permanente y se mantendrá abierta mientras dure el ciclo de vida del canal de mensajes. Los MQIPT no cerrarán la conexión TCP/IP entre los pares de petición/respuesta.

Si dos MQIPT se comunican a través de HTTP, es posible que una petición de HTTP permanezca en estado pendiente durante un período de tiempo prolongado. Esto puede suceder, por ejemplo, en un canal de peticionario/servidor cuando el extremo del servidor espera la llegada de mensajes a su cola de transmisión. El protocolo de canal de WebSphere MQ proporciona un mecanismo de "pulsaciones" que requiere que el extremo que está a la espera envíe periódicamente mensajes de pulsaciones al otro extremo (el período de pulsaciones de canal por omisión es de 5 minutos) y MQIPT utiliza estas pulsaciones como la respuesta HTTP. No inhabilite este mecanismo de pulsaciones de canal ni lo establezca en un valor demasiado elevado, así se evitará problemas de tiempo excedido en algunos cortafuegos.

Algunos servidores proxy HTTP tienen sus propias propiedades para controlar las conexiones permanentes, por ejemplo, el número de peticiones que pueden realizarse en una conexión permanente. El proxy HTTP también debe soportar el protocolo HTTP 1.1. Cuando se utiliza el proxy de antememoria IBM WebSphere Caching Proxy, se deben restablecer las propiedades siguientes:

- MaxPersistenceRequest se debe establecer en un valor alto (por ejemplo, 5000)
- PersistentTimeout se debe establecer en un valor alto (por ejemplo, 12 horas)
- ProxyPersistence se debe establecer en `activado`

Soporte de SOCKS

Cuando se realizan conexiones de salida a través de un cortafuegos, se puede habilitar una aplicación para SOCKS de modo que todas las conexiones se realicen mediante un proxy SOCKS y, por lo tanto, quede habilitado un punto de control de salida a través del cortafuegos.

En los releases anteriores de MQIPT, para dar soporte a SOCKS se debían establecer las propiedades del sistema Java `SocksProxyHost` y `SocksProxyPort`, que afectaban a todas las conexiones realizadas mediante MQIPT con lo que se obligaba a que todas las rutas utilizaran el mismo proxy SOCKS. En este release de MQIPT se ha implementado el soporte SOCKS V5 pero únicamente con el soporte para las direcciones de formato IPV4 y sin autenticación de usuario.

Se puede configurar cada ruta de modo que se comunique con un proxy SOCKS diferente utilizando las propiedades `SocksClient`, `SocksProxy` y `SocksProxyPort`.

Asimismo, se pueden habilitar todas las rutas para que actúen como un servidor SOCKS (proxy) mediante la propiedad `SocksServer` y, de este modo, se permite que una aplicación WebSphere MQ habilitada para SOCKS pueda conectarse con el destino a través de MQIPT. Cuando se utiliza esta función, el destino y la puerta de destino se obtienen durante el reconocimiento, por lo tanto se ignoran las propiedades `Destination` y `DestinationPort` definidas en la ruta. Esta es una función clave para dar soporte a la agrupación en clúster de WebSphere MQ. Consulte el apartado “Agrupación en clúster” en la página 20 para obtener más información sobre cómo utilizar MQIPT con la agrupación en clúster de WebSphere MQ.

Soporte de SSL

El protocolo SSL proporciona seguridad en las conexiones a través de canales de comunicación que no son seguros y garantiza:

Confidencialidad en las comunicaciones
La conexión puede ser confidencial, ya que se pueden cifrar los datos que se intercambian el cliente y el servidor de modo que, por ejemplo, los datos sólo tengan sentido para ellos. Esto garantiza la transferencia segura de información privada como, por ejemplo, los números de tarjetas de crédito.

Integridad de las comunicaciones
La conexión es fiable. El transporte de mensajes incluye una comprobación de la integridad de los mensajes basada en una función hash segura.

Autenticación
El cliente puede autenticar al servidor y un servidor autenticado puede autenticar al cliente. Esto significa que se garantiza que la información

solamente se intercambiará entre las partes acordadas. El mecanismo de autenticación está basado en el intercambio de certificados digitales (certificados X.509v3).

El protocolo SSL puede utilizar diferentes algoritmos de firma digital para la autenticación de las partes involucradas en la comunicación. Las operaciones criptográficas que se utilizan en SSL, el cifrado que garantiza la confidencialidad de los datos y la utilización segura de hashque aporta integridad a los mensajes, se basan en que el cliente y el servidor compartan claves secretas. SSL proporciona diferentes mecanismos de intercambio de claves que permiten compartir las claves secretas. SSL puede utilizar varios algoritmos de cifrado y hash. Se da soporte a diferentes algoritmos criptográficos. Éstos se especifican mediante suites de cifrado SSL. Se da soporte a las siguientes suites de cifrado:

SSL_RSA_EXPORT_WITH_RC4_40_MD5
SSL_RSA_EXPORT_WITH_DES40_CBC_SHA
SSL_RSA_EXPORT_WITH_RC2_CBC_40_MD5#
SSL_RSA_WITH_3DES_EDE_CBC_SHA
SSL_RSA_WITH_NULL_MD5
SSL_RSA_WITH_NULL_SHA
SSL_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
SSL_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA
SSL_DHE_DSS_WITH_3DES__EDE_CBC_SHA
SSL_DHE_RSA_WITH_3DES__EDE_CBC_SHA
SSL_DH_anon_WITH_RC4_40_MD5
SSL_DH_anon_EXPORT_WITH_DES40_CBC_SHA
SSL_RSA_WITH_RC4_128_MD5
SSL_RSA_WITH_RC4_128_SHA
SSL_RSA_WITH_DES_CBC_SHA
SSL_DHE_RSA_WITH_DES_CBC_SHA
SSL_DHE_DSS_WITH_DES_CBC_SHA
SSL_DH_anon_WITH_3DES_EDE_CBC_SHA
SSL_DH_anon_WITH_RC4_128_MD5
SSL_DH_anon_WITH_DES_CBC_SHA

Reconocimiento SSL

El proceso de reconocimiento SSL se produce durante la petición de conexión inicial entre el servidor y el cliente SSL, cuando se realiza la autenticación y se negocian las suites de cifrado.

Todas las suites de cifrado SSL mencionadas anteriormente, con la excepción de las suites de cifrado anónimas, requieren la autenticación del servidor y permiten la autenticación del cliente: se puede configurar el servidor para que solicite la autenticación del cliente. En SSL, la autenticación en las comunicaciones de igual está basada en la criptografía de claves públicas y en los certificados digitales X.509v3. Un sitio que deba autenticarse en el protocolo SSL necesita una clave privada y un certificado digital que contenga la clave pública correspondiente junto con información acerca de la identidad del sitio y el tiempo de validez del certificado. Los certificados los firma una autoridad de certificación y este tipo de certificados se denominan certificados de autoridades de certificación. Un certificado seguido de uno o varios certificados constituye una cadena de certificados. Una cadena de certificados se caracteriza por el hecho que, comenzando a partir del primer certificado (el certificado del sitio), la firma de cada certificado de la cadena se puede verificar utilizando la clave pública contenida en el siguiente certificado de la autoridad de certificación.

Cuando se establece una conexión segura que requiere la autenticación del servidor, éste envía al cliente una cadena de certificados para demostrar su identidad. El cliente SSL continuará estableciendo la conexión con el servidor solamente si puede autenticar el servidor como, por ejemplo, si puede verificar la firma del certificado del sitio del servidor. Para poder verificar dicha firma, el cliente SSL debe confiar en el propio sitio del servidor o como mínimo en una de las autoridades de certificación de la cadena de certificados que proporciona el servidor. Los certificados de los sitios y de las autoridades de certificación de confianza se deben mantener en el extremo del cliente para poder realizar esta verificación.

El cliente SSL inspecciona la cadena de certificados del servidor, comenzando por el certificado del sitio y considera la firma del certificado del sitio como válida si el certificado del sitio está en el depósito de certificados de autoridades de certificación o sitios de confianza o si un certificado de autoridad de certificación de la cadena se puede validar basándose en su depósito de certificados de autoridades de certificación. En este último caso, el cliente SSL comprueba que la cadena de certificados tenga las firmas correctas, comenzando por el certificado de la autoridad de certificación de confianza hasta el certificado del sitio del servidor. También se comprueba que todo certificado involucrado en este proceso tenga el formato y las fechas de validez correctas. Si no es así, se rechaza la conexión con el servidor. Después de comprobar el certificado del servidor, el cliente utiliza la clave pública intercalada en dicho certificado en los pasos siguientes del protocolo SSL. La conexión SSL solamente se puede establecer si el servidor realmente tiene la clave privada correspondiente.

La autenticación del cliente sigue el mismo procedimiento; si un servidor SSL necesita autenticación del cliente, éste envía al servidor una cadena de certificados para demostrar su identidad y el servidor comprueba que dicha cadena esté basada en su depósito de certificados de autoridades de certificación y sitios de confianza. Después de comprobar el certificado del cliente, el servidor utiliza la clave pública intercalada en dicho certificado en los pasos siguientes del protocolo SSL. La conexión SSL solamente se puede establecer si el cliente realmente tiene la clave privada correspondiente.

El protocolo SSL propiamente dicho proporciona un alto nivel de seguridad en las comunicaciones. Sin embargo, el protocolo funciona basándose en la información que proporciona la aplicación. Solamente si esta base de información se mantiene de forma segura, se puede alcanzar el objeto global de garantizar que las comunicaciones sean seguras. Por ejemplo, si el depósito de certificados de autoridades de certificación y sitios de confianza no ofrece seguridad, podría establecer una conexión segura con un destino que no es nada seguro.

MQIPT y SSL

Se ha implementado SSL V3.0, mediante las señales PKCS12 (Public Key Cryptography Standards) de los archivos de conjunto de claves (cuyos tipos de archivo son .p12 o .pfx), que contienen certificados X509.V3.

Un MQIPT puede actuar como un cliente SSL o como un servidor SSL dependiendo del extremo que inicie la conexión. El cliente inicia una conexión y el servidor acepta la petición de conexión. Una ruta MQIPT puede actuar como cliente y como servidor, aunque en este caso se recomienda utilizar la modalidad de proxy SSL, por motivos de rendimiento. Toda ruta MQIPT se puede configurar de forma independiente con su propio conjunto de propiedades SSL. Consulte el

apartado “Información de consulta relacionada con la sección de ruta” en la página 58 para obtener información detallada.

Valores de trust

Un archivo de conjunto de claves contiene un certificado personal que incluye el certificado de la autoridad certificadora o una cadena de certificados de la autoridad certificadora. Para habilitar la autenticación cuando se realiza una conexión, es necesario que el certificado contenga un valor de tipo trust. Hay dos tipos de valores para trust:

Trust as peer
Significa que el certificado es de confianza pero no lo será cualquier otro certificado firmado por este certificado.

Trust as Certificate Authority (CA)
Significa que cualquier certificado que venga firmado por este certificado es un certificado de confianza.

El archivo de conjunto de claves del extremo del servidor SSL, identificado mediante la propiedad SSLServerKeyRing debe contener su certificado personal. Un segundo archivo de conjunto de claves, identificado mediante la propiedad SSLServerCAKeyRing, debe contener un certificado de confianza (CA o Peer). El archivo de conjunto de claves del extremo del cliente SSL, identificado mediante la propiedad SSLClientKeyRing contiene su certificado personal. Un segundo archivo de conjunto de claves, identificado mediante la propiedad SSLClientCAKeyRing, debe contener un certificado de confianza (CA o Peer). Un archivo de conjunto de claves también puede contener una lista de las CRL (listas de revocación de certificados).

Asimismo, se pueden utilizar certificados autofirmados que son similares a los del archivo de conjunto de claves de ejemplo (sslSample.pfx) que se proporcionan con MQIPT.

Se puede utilizar el programa de utilidad KeyMan (situado en el subdirectorio ssl) para crear certificados autofirmados y gestionar los archivos de conjunto de claves y los certificados. Para obtener más información, consulte el apartado “KeyMan” en la página 15.

Debe proteger los archivos de contraseñas y de conjunto de claves con las funciones de seguridad del sistema operativo para que no se acceda de forma no autorizada a los mismos.

Comprobación de SSL

En el Capítulo 10, “Iniciación a internet pass-thru” en la página 67 se describen las tareas que se pueden realizar para comprobar una conexión SSL.

Hay diferentes proveedores que ofrecen certificados y tecnologías de gestión de certificados, por ejemplo:

- RSA Security (www.rsasecurity.com)
- Entrust Technologies (www.entrust.com)
- VeriSign (www.verisign.com)

Mensajes de error de SSL

Si se utiliza un valor de parámetro no válido en una de las llamadas al método SSL o si se proporcionan datos erróneos al protocolo SSL, pueden visualizarse los

siguientes códigos de error en una excepción SSLRuntimeException.

Tabla 2. Mensajes de error SSLRuntimeException

ID	Descripción
1	Se ha utilizado un método erróneamente o uno o varios de los parámetros de entrada estaban fuera de los límites.
2	Los datos proporcionados no se pueden procesar.
3	La firma de los datos proporcionados no se puede verificar.
10	El nombre del asunto del certificado de la autoridad certificadora no coincide con el nombre del emisor del certificado.
11	No se da soporte al tipo de un certificado.
12	Se está utilizando un certificado antes de su período de validez.
13	Un certificado ha caducado.
14	No puede verificarse la firma de un certificado.
15	No se puede utilizar un certificado.
20	El servidor no da soporte a ninguna de las suites de cifrado que ha propuesto el cliente.
21	El servidor no da soporte a ninguno de los métodos de compresión que ha propuesto el cliente.
22	No hay ningún certificado disponible.
23	No se da soporte a un algoritmo o tipo de formato.
24	Se rechaza la información obsoleta.
25	Se revoca un certificado.
26	Un conjunto de CRL está incompleto (faltan algunas CRL delta).
27	Ya existe el nombre del certificado.
28	La clave pública que se ha de certificar ya existe.
29	Algún número de serie o alguna clave (certificado, CRL) no son correctos.

Se genera una SSLException si finaliza la excepción del protocolo de reconocimiento SSL.

Tabla 3. Mensajes de error de SSLException

ID	Descripción
3	El tiempo de espera de conexión definido en SSLContext ha caducado y no se ha recibido ninguna respuesta del igual.
2	El igual ha cancelado anormalmente la conexión durante un reconocimientoSSL sin ninguna indicación de error adicional.
10	Se ha recibido un mensaje inesperado.
20	Se ha recibido un mensaje con un MAC de registro erróneo.
30	Anomalía de descompresión.
40	Anomalía de reconocimiento.
41	El igual no ha enviado ningún certificado.
42	Se ha recibido un certificado erróneo.
43	Se ha recibido un certificado no soportado.
44	Se ha recibido un certificado revocado.
45	Se ha recibido un certificado caducado.

Tabla 3. Mensajes de error de SSLException (continuación)

46	Se ha recibido un certificado desconocido.
47	Se ha detectado un parámetro no permitido.

Calidad de servicio (QoS)

IBM WebSphere Edge Server proporciona una solución de gestión de ancho de banda mediante la conexión (plugin) de Transactional Quality of Service para la plataforma Linux. Transactional Quality of Service (TQoS) hace referencia al servicio global, en cuanto a elementos como el rendimiento y el retardo, que se proporciona a los usuarios de una red. Se pueden establecer atributos que permitan garantizar la calidad de servicio asociada a los datos de salida que se envían en una conexión. De este modo, el administrador de políticas puede definir normas que permitan identificar el tráfico relacionado con servidores y acciones de política específicos con diferentes controles de servicio exclusivos para este tráfico. Por ejemplo, una instalación puede definir una política que especifique un trato preferente para un tráfico de salida asociado al tráfico del servidor que da soporte a una venta de una cantidad determinada de artículos y no así para el tráfico del servidor que da soporte a un cliente que navega por la red. MQIPT sólo requiere que se instale y se ejecute Policy Agent (pagent) para poder implementar Quality of Service (QoS).

Las políticas de TQoS se definen en un archivo de configuración de políticas (`pagent.conf`) o mediante un servidor LDAP. Pagent de TQoS puede acceder al archivo de configuración de políticas o ir a un servidor LDAP, o a ambos para recuperar las entradas de política de TQoS. Si desea obtener más información, consulte la publicación *IBM Edge Server Administration Guide* que se puede encontrar en el URL siguiente:

`http://www-3.ibm.com/software/webservers/edgeserver/library.html`

Desde este sitio puede ver el archivo HTML en línea o descargar la versión en formato PDF; en cualquiera de estos formatos puede buscar información sobre TQoS.

Para obtener información detallada sobre cómo descargar WES con TQoS, consulte el archivo Readme.txt de MQIPT.

MQIPT se proporciona con una biblioteca ficticia denominada `libmqiptqos.so`, que se encuentra en el subdirectorio lib. Después de instalar TQoS, debe editar el script mqipt del subdirectorio bin y cambiar la variable de entorno LD_LIBRARY_PATH para que apunte al subdirectorio lib de WES.

Para poder implementar Quality of Service (QoS), MQIPT sólo requiere que se instale y se ejecute pagent. Con MQIPT, se puede establecer una prioridad de aplicación para el flujo de datos de una ruta en ambas direcciones, hecho que, por supuesto, afectará a todos los canales que utilicen dicha ruta. La prioridad se define utilizando las propiedades de MQIPT `QosToCaller` y `QosToDest` (consulte el apartado “Información de consulta relacionada con la sección de ruta” en la página 58 para obtener más información) y los valores que se utilicen aquí deberán coincidir con una definición de políticas de ApplicationPriority en el archivo de control `pagent.conf`. Si pagent no encuentra una política coincidente, no se asignará ninguna prioridad a los datos. Los cambios que se efectúen en una política no quedarán reflejados en MQIPT hasta que se reinicie pagent. Consulte el

apartado “Configuración de la calidad de servicio (QoS)” en la página 79 para obtener más información sobre las definiciones de políticas.

Servlet

Ahora hay una versión de servlet de MQIPT (llamada MQIPTServlet) que puede desplegarse en un servidor de aplicaciones. Funciona de modo similar al MQIPT ″normal″ pero actúa como si únicamente tuviera una ruta. Una petición de conexión de entrada para iniciar un canal de WebSphere MQ la maneja una instancia de MQIPTServlet y cada instancia mantiene una conexión permanente con el gestor de colas de destino. Los flujos de datos posteriores se mantienen en el mismo canal utilizando el ID de sesión que se ha creado durante la primera petición de conexión.

En el subdirectorio web se puede encontrar un archivo archivador de aplicación web llamado `MQIPTServlet.war`. Este archivo .war debe importarse al servidor de aplicaciones.

Se puede configurar MQIPTServlet estableciendo las propiedades en el archivo web.xml, situado en el subdirectorio WEB-INF del servidor de aplicaciones. Solamente se puede aplicar un subconjunto de las propiedades de MQIPT actuales a MQIPTServlet. Las propiedades siguientes se pueden utilizar con MQIPTServlet:

- ClientAccess
- ConnectionLog
- MaxLogfileSize
- QMgrAccess
- Trace

Los archivos de rastreo y de anotaciones de conexión se graban en un directorio con una propiedad nueva denominada LogDir. Se recomienda definir esta propiedad antes de iniciar MQIPTServlet.

Para controlar la cantidad de recursos que utiliza MQIPTServlet, puede establecer el número máximo de sesiones activas o el número de instancias del servlet en el servidor de aplicaciones.

MQIPTServlet se puede comprobar con IBM WebSphere Application Server 4.0, Tomcat 3.3 y Tomcat 4.0.

Consulte el apartado “Configuración del servlet MQIPT” en la página 90 para obtener una configuración de ejemplo.

KeyMan

Junto con MQIPT se envía ahora el programa de utilidad autónomo KeyMan que permite gestionar los certificados SSL y los archivos de conjunto de claves. En el subdirectorio ssl se puede encontrar un archivo zip que contiene KeyMan. Para instalar KeyMan, descomprima el archivo en un directorio temporal y siga las instrucciones que contiene el archivo README.txt. KeyMan tiene muchas funciones, pero en este apartado nos limitaremos a las relacionadas con la creación de certificados y la gestión de archivos de conjunto de claves que contienen señales PKCS12.

KeyMan es una herramienta de gestión para el extremo del cliente de PKI (Infraestructura de claves públicas). KeyMan gestiona claves, certificados, CRL

(listas de revocación de certificados), y sus depósitos respectivos para almacenar y recuperar estos elementos. Se da soporte al ciclo de vida completo de los certificados y a los procesos necesarios para manejar los certificados de usuarios.

KeyMan gestiona depósitos que contienen agrupaciones de claves, certificados y listas de revocación. Un depósito se denomina una señal. Una señal consta de los valores de confianza (trust) para una aplicación determinada, por ejemplo, MQIPT. Generalmente, una señal contiene claves privadas y las cadenas de certificados asociadas que permiten autenticar a un usuario en otros sitios. Además, una señal contiene certificados de socios de comunicaciones de confianza y de autoridades de certificación (CA).

Tipos de señales soportados

KeyMan da soporte a diferentes tipos de señales. Las señales son depósitos que contienen claves, certificados, CRL y valores de confianza (trust). Algunas señales solamente pueden almacenar un subconjunto de estos tipos de elementos.

Señal PKCS7
Contiene un conjunto de certificados y opcionalmente las CRL asociadas. No se pueden almacenar claves en este tipo de depósito. Este depósito no requiere autenticación. Los certificados y las CRL están protegidos mediante una firma. Sin embargo, un usuario malintencionado podría cambiar el modo en que se ha almacenado el conjunto de elementos de una señal PKCS7. Este tipo de señal se utiliza cuando se define el conjunto de elementos mediante algún tipo de contexto.

Señal PKCS12
Contiene claves privadas, certificados y las CRL asociadas. El contenido se protege mediante una frase de contraseña del usuario. Los elementos públicos (los certificados y las CRL) y los elementos privados (las claves) se pueden proteger mediante algoritmos con diferentes niveles de protección.

Depósitos PKCS11 (CryptoKi)
PKCS11 define una interfaz para las señales criptográficas. Estas señales pueden almacenar claves y certificados. No se pueden almacenar las CRL. El acceso a una señal está protegido mediante un número de identificación personal (PIN). Debe especificar la DLL de PKCS11 que utiliza KeyMan para acceder a la señal.

KeyMan da soporte a las DLL de PKCS11 versión 2.01 y 2.10.

PKCS7 y PKCS12 son señales de software y pueden recuperarse desde soportes diferentes (por ejemplo, archivos, URI y el portapapeles).

KeyMan puede crear señales PKCS7 a partir de datos con un formato desconocido. Explora los datos y con los certificados X.509 y las CRL que detecta crea una señal PKCS7. Si tiene mensajes de correo electrónico que contienen certificados o CRL puede abrir la carpeta email de KeyMan y este programa intentará extraer los elementos X.509. Por supuesto, los datos no se pueden volver a almacenar en su formato original. Los datos extraídos se pueden almacenar en un archivo con el formato PKCS7.

Formatos de datos estándar soportados

KeyMan da soporte a varios formatos de datos estándar. Las siguientes son descripciones de su significado y el contexto de uso:

PKCS7

Este formato de datos es un conjunto de certificados y CRL. El conjunto de certificados y CRL como lo describe PKCS7 no está protegido. Sin embargo, cada certificado y CRL individual están protegidos por una firma. PKCS7 se utiliza siempre que el conjunto de certificados y CRL que se espera se ha definido mediante contexto. En los sistemas Windows, los sufijos de archivo estándar para los archivos PKCS7 son .p7r y .p7b.

PKCS10

PKCS10 define un mensaje de petición de certificado. Contiene la clave pública y la información acerca del nombre del solicitante de X.500. El mensaje está firmado con la clave privada correspondiente. Los mensajes PKCS10 se pueden generar en formato binario y con estructura ASCII. El mensaje se debe someter a una autoridad de certificación (CA).

PKCS12

PKCS12 lo utilizan los navegadores y servidores web para importar y exportar las claves privadas y los certificados asociados. KeyMan puede leer y grabar estos archivos PKCS12. Estos programas solamente comprenden un perfil muy especifico de PKCS12 pero KeyMan puede generar archivos PKCS12 más generales. KeyMan puede almacenar conjuntos de claves privadas, certificados, CRL y los valores de confianza correspondientes en un solo archivo PKCS12. Los archivos PKCS12 están protegidos mediante una frase de contraseña. Normalmente, una señal PKCS12 contiene la política de confianza de una aplicación determinada. En el caso de IBM BlueZ SSLite, se utilizarán las claves y las cadenas de certificados asociadas para la autenticación del cliente y del servidor. Otros certificados representan la CA de confianza o los servidores de confianza dependiendo de sus respectivos valores de confianza (trust). En los sistemas Windows, los sufijos de archivo estándar para los archivos PKCS12 son .p12 y .pfx.

SPKAC

SignedPublicKeyAndChallenge (SPKAC) es un formato de datos para solicitar certificados de una CA. Este formato concreto lo genera Netscape cuando se utiliza el código HTML <keygen>. Contiene la clave pública firmada y el desafío. Este formato de datos lo puede generar KeyMan en formato binario y Base64.

certificados X.509 V3

KeyMan puede leer certificados X.509 V3 en formato binario o encerrado en una estructura ASCII. Estos archivos se pueden importar o abrir con KeyMan. También se pueden escribir certificados individuales a partir de una señal con estos dos formatos (**Detalles de certificado -> Guardar icono**). En los sistemas Windows los sufijos de archivo estándar para los archivos de certificados X.509 son .crt, .cer y .der.

Listas de revocación de certificados (CRL) X.509 V2

KeyMan puede leer las CRL X.509 V2 en formato binario o encerradas en una estructura ASCII. Se puede abrir una CRL individual. KeyMan sólo importa las CRL a señales que ya contienen el certificado de la CA asociado. Se puede escribir una CRL individual en formato binario o encerrada en una estructura ASCII (**Detalles de certificados -> Detalles de CRL -> Guardar icono**). En los sistemas Windows el sufijo de archivo estándar para los archivos de CRL X.509 es .crl.

Preguntas frecuentes acerca de KeyMan

Para cuestiones generales acerca de criptografía y términos relacionados consulte a los laboratorios RSA cuáles son sus ″preguntas frecuentes acerca de la criptografía actual″. Las preguntas frecuentes que se presentan a continuación describen cuestiones relacionadas con KeyMan.

¿Puede leer KeyMan archivos PKCS12 generados por Netscape o Internet Explorer?

KeyMan puede leer los archivos PKCS12 generados por el navegador Netscape o Internet Explorer siempre que conozca la contraseña que protege su contenido.

¿Puede KeyMan crear archivos PKCS12 que puedan leerse mediante Netscape o Internet Explorer?

El estándar PKCS12 permite mucha libertad de selección de algoritmos y de disposición de contenido. Los navegadores solamente aceptan un perfil muy específico de todas las opciones posibles. KeyMan puede generar archivos PKCS12 que se pueden leer mediante Netscape e Internet Explorer. Dado que KeyMan le permite hacer muchas más cosas con PKCS12 puede crear archivos que estos navegadores no comprendan. El perfil común de los navegadores es similar al siguiente: el cifrado público/privado (vea **Opciones de menú -> Valores PKCS12**) debe ser ″RC2 (40 bits)″/″DES (168 bits)″, respectivamente. Debe haber exactamente un certificado privado en la señal PKCS12.

¿Qué es un certificado privado?

Si KeyMan detecta una clave y un certificado coincidentes combina estos dos elementos en un certificado privado. Esto significa que para cualquier certificado privado también poseerá la clave privada correspondiente. Si importa los certificados a una señal, KeyMan comprobará si hay una clave privada coincidente y automáticamente combinará la clave y el certificado importado como un certificado privado. Si esto ocurre, KeyMan se lo notificará con un diálogo.

¿Qué es un certificado de CA o de igual (″Peer″)?

Los certificados que contiene una señal establecen un nivel de confianza. Definen en quién confía. El significado de la confianza y la evaluación exacta de los certificados dependerá de la aplicación que utiliza la señal. Con KeyMan puede definir dos tipos de confianza para los certificados: CA e igual (″Peer″). Si acepta un certificado de confianza CA, implícitamente considerará de confianza cualquier certificado que esté firmado directa o indirectamente por dicha CA. Si establece el nivel de confianza en igual (″Peer″) solamente confiará en ese certificado concreto. Los certificados firmados por un certificado de igual (″Peer″) no serán de confianza.

¿Qué son los certificados que ni son privados, ni de CA ni de igual (″Peer″)?

Para cada cadena completa, KeyMan intenta almacenar la cadena completa hasta el certificado raíz. No es necesario que estos certificados sean de confianza y, por lo tanto, no aparecerán entre los certificados CA o de igual (″Peer″). Puede encontrar estos certificados si selecciona el conjunto de claves ″Todos los elementos de certificados″. Los certificados que no son de confianza no poseen un icono.

¿Qué es una señal?

Una señal es un conjunto de claves, certificados y CRL. Una señal se almacena en algún soporte (por ejemplo, un archivo, un URL o un componente de hardware). Hay varios tipos de señales con posibilidades

diferentes: señales de software, señales de hardware, señales no protegidas y señales protegidas mediante contraseñas o PIN.

¿Qué es un conjunto de claves?
Una señal consta de varios conjuntos de claves. Un conjunto de claves determinado identifica un conjunto de elementos específico (por ejemplo, los certificados del mismo nivel de confianza o los certificados de los que es el propietario de la clave privada o claves sin certificados coincidentes).

Soporte de Network Dispatcher

Se puede utilizar MQIPT con IBM Network Dispatcher para proporcionar una mayor disponibilidad y equilibrio de carga entre muchos servidores, mediante el uso de asesores personalizados. En este apartado se presupone que está familiarizado con Network Dispatcher y con los asesores personalizados.

Con MQIPT se proporcionan dos asesores personalizados, ubicados en el subdirectorio `lib`. Siga las instrucciones de la publicación *Network Dispatcher User's Guide* (GC31-8496) para instalar los asesores personalizados. En la Figura 6 se muestra un ejemplo de cómo utilizar Network Dispatcher para supervisar la dirección de puerta 1414 para MQIPT. Tenga en cuenta que todo MQIPT debe tener el mismo archivo de configuración.

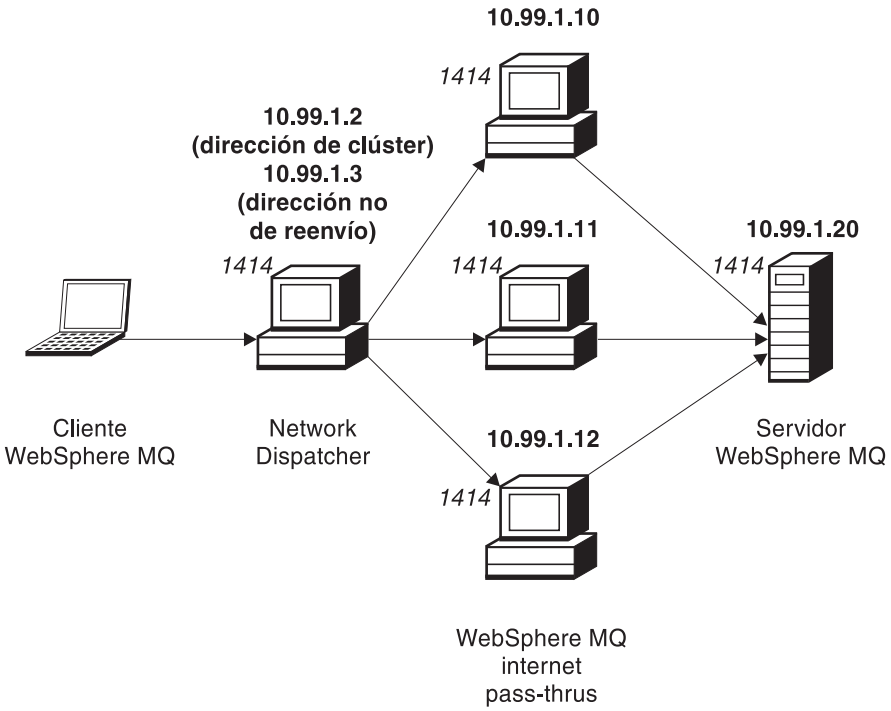

Figura 6. Utilización de Network Dispatcher con MQIPT

Siga las instrucciones del capítulo 5 de la publicación *Network Dispatcher User's Guide* para configurar el componente del distribuidor para definir la puerta 1414 y las máquinas de servidor con equilibrio de carga. Puede utilizar las opciones de menú del cliente de administración o la modalidad de línea de mandatos "ndcontrol". Por ejemplo:

```
ndcontrol port add 10.99.1.2 : 1414
ndcontrol server add 10.99.1.2 : 1414 : 10.99.1.10
ndcontrol server add 10.99.1.2 : 1414 : 10.99.1.11
ndcontrol server add 10.99.1.2 : 1414 : 10.99.1.12
```

La definición de ruta del archivo de configuración de MQIPT debe ser similar a la siguiente:

```
[route]
ListenerPort=1414
Destination=10.99.1.20
DestinationPort=1414
NDAdvisor=true
```

Puede iniciar y detener un asesor personalizado desde la línea de mandatos. Por ejemplo:

```
ndcontrol advisor start mqipt_normal 1414
```

Este mandato inicia el asesor de MQIPT en modalidad “normal”, en la que el asesor base realiza su propia temporización para calcular los factores de peso de cada MQIPT. Para utilizar el asesor de MQIPT en modalidad de sustitución (“replace”), añada esta línea a la definición de ruta de MQIPT:

```
NDAdvisorReplaceMode=true
```

También debe iniciar el asesor personalizado `mqipt_replace` en lugar de `mqipt_normal`. Por ejemplo:

```
ndcontrol advisor start mqipt_replace 1414
```

Cuando utilice un asesor para la puerta del escucha SSL (es decir, `SSLServer=true` en el archivo de configuración `mqipt.conf`), debe colocar un archivo archivador en el directorio de trabajo de Network Dispatcher. Este archivo archivador tiene un nombre específico, relacionado con la ruta que se está supervisando. Por ejemplo, si la ruta 1414 se ha establecido en `SSLServer=true`, debe colocarse un archivo `mqipt1414.ssl` en el directorio `c:\winnt\system32` (en Windows NT). Consulte el archivo `mqipt1414Sample.ssl` para obtener más información.

Agrupación en clúster

Se pueden utilizar los clústeres de WebSphere MQ con MQIPT habilitando para SOCKS todo gestor de colas del clúster que abarque Internet y habilitando MQIPT para que actúe como proxy SOCKS. Dado que hay muchos modos diferentes de configurar el gestor de colas en un clúster, la descripción siguiente está basada en las tareas descritas en la publicación *MQSeries Queue Manager Clusters*, SC34-5349, 1ª Parte, Capítulo 3. El diagrama siguiente es una ampliación del definido en la Tarea 2, "Adición de un gestor de colas nuevo al clúster". NEWYORK y CHICAGO están en un clúster llamado HOME y ambos contienen depósitos completos. NEWYORK, LONDON y PARIS están en otro clúster llamado INVENTORY. Tenga en cuenta que no es necesario que habilite CHICAGO para SOCKS ya que está en un clúster que no necesita un MQIPT.

En la práctica, todo gestor de colas del clúster INVENTORY está "oculto" detrás de un MQIPT. Dado que el gestor de colas se ha habilitado para SOCKS, cuando se inicia un canal emisor del clúster, la petición se envía a su destino, utilizando MQIPT como proxy SOCKS. Normalmente, se utiliza la definición de CONNAME de un canal receptor del clúster para identificar al gestor de colas local, pero cuando se utiliza con MQIPT, CONNAME debe identificar el MQIPT local y su puerta de escucha de entrada. En el diagrama siguiente, todas las direcciones de puertas de escucha de entrada son 1414 y las direcciones de puerta de escucha de salida son 1415.

Existen dos métodos para ejecutar un gestor de colas habilitado para SOCKS. El primero es habilitar para SOCKS toda la máquina en la que está ejecutándose el

gestor de colas. El segundo es habilitar para SOCKS simplemente el gestor de colas. Cuando utilice cualquiera de estos métodos, debe configurar el cliente SOCKS de modo que solamente efectúe conexiones remotas utilizando MQIPT como proxy SOCKS y debe inhabilitar la autenticación de usuarios. Hay varios productos en el mercado que permiten proporcionar el soporte de SOCKS. Debe elegir uno que soporte el protocolo SOCKS V5. Consulte el apartado "Soporte de SOCKS" en la página 9 para obtener más información acerca del soporte de SOCKS en MQIPT.

Consulte el apartado "Configuración del soporte de agrupación en clúster de MQIPT" en la página 92 para obtener un ejemplo de cómo configurar una red de clústeres.

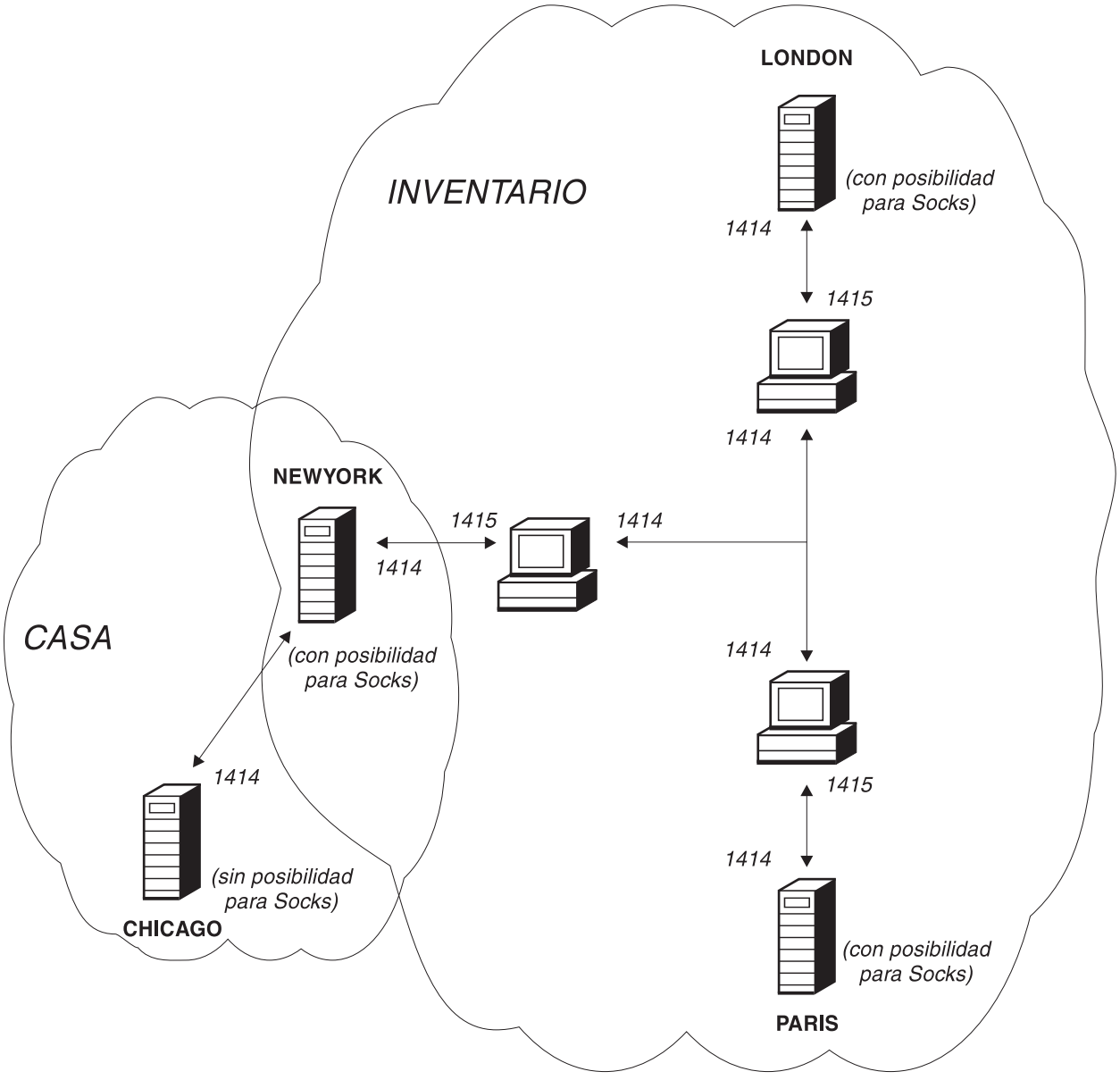

Figura 7. Soporte de la agrupación en clúster de MQIPT

Configuraciones de canales soportadas

Se da soporte a todos los tipos de canales de WebSphere MQ, pero la configuración está limitada a las conexiones TCP/IP. Para un cliente o un gestor de colas de WebSphere MQ, MQIPT parece su gestor de colas de destino. Donde la configuración de canal requiere un sistema principal de destino y un número de puerta, se especifican el nombre de sistema principal MQIPT y el número de puerta de escucha.

Canales cliente/servidor
MQIPT escucha las peticiones de conexión de cliente de entrada y luego las direcciona (utilizando la función de túnel HTTP, SSL o los paquetes de protocolos de WebSphere MQ estándar). Si MQIPT utiliza la función de túnel HTTP o SSL las dirige a una conexión con un segundo MQIPT. Si no utiliza la función de túnel HTTP, las dirige a una conexión con lo que considera el gestor de colas de destino (aunque éste puede ser un MQIPT adicional). Cuando el gestor de colas de destino acepta la conexión de cliente, los paquetes se transmiten entre el cliente y el servidor.

Canales emisor/receptor del clúster
Si MQIPT recibe una petición de entrada de un canal emisor del clúster, presupone que el gestor de colas se ha habilitado para SOCKS y la dirección de destino real se obtiene durante el proceso de reconocimiento SOCKS. A continuación, envía la petición al MQIPT siguiente o al gestor de colas de destino, exactamente del mismo modo que lo hace para los canales de conexión de cliente. Esto también incluye los canales de clúster emisor definidos automáticamente.

Emisor/receptor
Si MQIPT recibe una petición de entrada de un canal emisor, la dirige al siguiente MQIPT o al gestor de colas de destino, exactamente del mismo modo que se hace para los canales de conexión de cliente. El gestor de colas de destino valida la petición de entrada e inicia el canal receptor según convenga. Todas las comunicaciones entre el canal emisor y receptor (incluidos los flujos de seguridad) se transmiten.

Peticionario/servidor
Esta combinación se maneja del mismo modo que los tipos mencionados anteriormente. La validación de la petición de conexión la realiza el canal servidor en el gestor de colas de destino.

Peticionario/emisor
La configuración de 'devolución de llamada' puede resultar útil si dos gestores de colas no pueden establecer conexiones directas entre sí, pero ambos pueden conectarse con MQIPT y aceptar las conexiones procedentes del mismo.

Servidor/peticionario y servidor/receptor
Estos los maneja MQIPT exactamente igual que la configuración emisor/receptor.

Java Security Manager

La implementación original del soporte de Java Security Manager con la función de modalidad de proxy SSL estaba destinada a gestionar el control de las conexiones de sockets, pero también se puede utilizar con cualquier otra característica MQIPT para proporcionar otro nivel de seguridad.

MQIPT utiliza Java Security Manager por omisión, como está definido en la clase `java.lang.SecurityManager`. La característica Java Security Manager en MQIPT se

puede habilitar o inhabilitar utilizando la propiedad global SecurityManager, consulte el apartado "Información de consulta relacionada con la sección global" en la página 57 para obtener más información.

Java Security Manager utiliza dos archivos de políticas por omisión. Todas las instancias de una máquina virtual de un sistema principal utilizan un archivo de políticas de sistema global llamado $JREHOME/lib/security/java.policy (donde $JREHOME es el directorio que contiene el entorno de ejecución Java). En el directorio inicial del usuario puede haber un segundo archivo de políticas, específico del usuario, llamado .java.policy. También se puede utilizar un archivo de políticas MQIPT adicional, consulte el apartado "Información de consulta relacionada con la sección global" en la página 57 para obtener más información. Para utilizar un archivo de políticas adicional, asegúrese de que la propiedad policy.allowSystemProperty se haya establecido en true en el archivo de políticas del sistema global (java.security).

La sintaxis del archivo de políticas es muy compleja y aunque se puede modificar utilizando un editor de texto, se le recomienda que utilice el programa de utilidad policytool que se proporciona con Java para realizar los cambios. El programa de utilidad policytool se puede encontrar en el directorio $JREHOME/bin y está totalmente documentado en la documentación de Java.

Con MQIPT se proporciona un archivo de políticas de ejemplo (mqiptSample.policy) para mostrar los permisos necesarios para ejecutar MQIPT. Solamente se han añadir/modificar/suprimir las entradas java.net.SocketPermission, para adaptarlas a sus propios requisitos, y así poder controlar quién se puede conectar a MQIPT y a quién puede conectarse MQIPT. En este archivo de ejemplo se presupone que MQIPT se ha instalado en el directorio inicial por omisión, por ejemplo, c:\Archivos de programa\IBM\WebSphere MQ internet pass-thru\. Si ha instalado MQIPT en otra ubicación, esto debe quedar reflejado en las definiciones de codeBase y java.io.FilePermission.

Normalmente, los permisos se definen con tres atributos y los valores para controlar las conexiones de sockets son:

class permission
: java.net.SocketPermission

name to control
: Se crea con el formato nombresistpral:puerta, donde cada componente del nombre se puede especificar con un comodín. El nombre de sistema principal puede ser un nombre de dominio o una dirección IP. La posición más a la izquierda del nombre de sistema principal se especifica mediante un asterisco. Por ejemplo, harry.company1.com coincidirá con las cadenas de caracteres siguientes:

  - harry
  - harry.company1.com
  - *.company1.com
  - *
  - 123.456.789 (suponiendo que se trata de la dirección IP de harry.company1.com)

  El componente de puerta del nombre se puede especificar como una dirección de puerta individual o como un rango de direcciones de puertas, por ejemplo:

  - 1414 (solamente la puerta 1414)

- 1414- (todas las direcciones de puerta superiores o igual a 1414)
- -1414 (todas las direcciones de puertas inferiores o iguales a 1414)
- 1-1414 (todas las direcciones de puertas que oscilen entre 1 y 1414, inclusive)

allowed action

Las acciones que utiliza `java.net.SocketPermission` son:

- accept. Permite aceptar las conexiones procedentes del destino especificado.
- connect. Permite la conexión con el destino especificado.
- listen. Permite escuchar las peticiones de conexión en la puerta o puertas especificadas.
- resolve. Permite utilizar el servicio de nombres DNS para resolver los nombres de dominio como direcciones IP.

También se puede controlar Java Security Manager mediante las propiedades del sistema Java `java.security.manager` y `java.security.policy`, pero se le recomienda que utilice las propiedades SecurityManager y SecurityManagerPolicy para controlar MQIPT.

Finalización normal y condiciones de error

Cuando MQIPT detecta que un canal de WebSphere MQ se cierra (de forma normal o anómala) propaga el cierre del canal. Si el administrador cierra una ruta mediante MQIPT, todos los canales que pasan por dicha ruta se cerrarán.

MQIPT proporciona una función de tiempo excedido de conexión desocupada. Si MQIPT detecta que un canal ha estado desocupado durante un período de tiempo que supera el valor de tiempo excedido, inmediatamente concluye las dos conexiones implicadas.

Los dos sistemas WebSphere MQ de cada extremo del canal contemplan estas condiciones de finalización anormal como errores de red o como si fuera el otro extremo el que ha finalizado el canal. A continuación, los canales implicados pueden reiniciar y recuperar la conexión (si el error sucede cuando el protocolo está en período de duda) del mismo modo que lo hacen cuando no se utilizan los MQIPT.

Seguridad de los mensajes

Cuando se utilizan mensajes de WebSphere MQ rápidos y no permanentes, si la ruta MQIPT falla o se reinicia cuando hay un WebSphere MQ en tránsito, se podría perder el mensaje. Antes de reiniciar la ruta, asegúrese de que todos los canales de WebSphere MQ que utilicen la ruta de MQIPT estén inactivos.

Consulte la publicación *MQSeries Intercommunication*, SC33-1872 para obtener más información sobre los canales y mensajes de WebSphere MQ.

Anotaciones de conexión

MQIPT proporciona un recurso de anotaciones de conexión que contiene listas de todos los intentos de conexión satisfactorios o no. Se controla mediante las propiedades `ConnectionLog` y `MaxLogFileSize`. Consulte el apartado “Información de consulta relacionada con la sección global” en la página 57 para obtener información más detallada.

Cada vez que se inicia MQIPT, se crea una anotación de conexión nueva y para facilitar su identificación el nombre de archivo incluye la indicación de la hora actual. Por ejemplo:

```
mqiptAAAAMMDDHHmmSS.log
```

donde

- `AAAA` es el año
- `MM` es el mes
- `DD` es el día
- `HH` es la hora
- `mm` son los minutos
- `SS` son los segundos

A efectos de auditoría, estos archivos de anotaciones no se borran nunca. El administrador de MQIPT es el responsable de gestionar y suprimir estos archivos cuando ya no son necesarios.

Otras consideraciones de seguridad

Si opta por no utilizar SSL, MQIPT permite los flujos de seguridad de canal, de modo que pueden utilizarse las salidas de los canales de WebSphere MQ para proporcionar seguridad de un extremo a otro del canal.

MQIPT tiene varias funciones adicionales que pueden ayudar a los diseñadores a desarrollar una solución segura:

- Si una red interna tiene muchos clientes y todos intentan realizar conexiones de salida, se pueden dirigir todas a través de un MQIPT situado dentro del cortafuegos. El administrador del cortafuegos debe otorgar acceso externo solamente a la máquina de MQIPT.
- MQIPT solamente puede conectar con los gestores de colas para los que se ha configurado explícitamente en su archivo de configuración, a menos que MQIPT actúe como proxy SOCKS.
- MQIPT verifica que los mensajes que recibe y transmite sean válidos y se ajusten al protocolo de WebSphere MQ. Esto impide que los MQIPT se utilicen en ataques de seguridad fuera del protocolo de WebSphere MQ. Si MQIPT actúa como proxy SSL, una vez cifrados todos los protocolos y datos de WebSphere MQ, MQIPT solamente puede garantizar el reconocimiento SSL. En esta situación se recomienda utilizar Java Security Manager. Consulte el apartado “Java Security Manager” en la página 22.
- Permite que las salidas de canal ejecuten sus propios protocolos de seguridad de un extremo a otro.
- MQIPT permite limitar el número total de conexiones de entrada estableciendo la propiedad `MaxConnectionThreads`. Esto ayuda a proteger un gestor de colas interno vulnerable a los ataques de denegación de servicio.

Debe proteger el archivo de configuración de MQIPT, `mqipt.conf`, ya que este archivo controla el acceso a los sistemas principales internos, y debe impedir que se acceda de forma no autorizada a la puerta de mandatos (si está habilitada) ya que este tipo de acceso permite que una persona externa concluya MQIPT.

Capítulo 3. Actualización desde la versión anterior

Para actualizar MQIPT de la Versión 1.1 a la Versión 1.2, siga estos pasos:

1. Efectúe una copia del archivo de configuración `mqipt.conf` y guárdelo en una ubicación diferente del directorio inicial de MQIPT.
2. Detenga MQIPT ejecutando el mandato:

   ```
   mqiptAdmin -stop
   ```
3. Si ha instalado MQIPT como un servicio, debe suprimirlo antes de desinstalar MQIPT:

   ```
   mqiptService -remove
   ```
4. Ejecute el programa de desinstalación para MQIPT.
5. Una vez instalado MQIPT V1.2, vuelva a copiar el archivo de configuración guardado en el directorio inicial de MQIPT. El archivo es compatible con la Versión 1.2. El nuevo archivo `mqiptSample.conf` le muestra las nuevas propiedades que probablemente desee utilizar.
6. Se le recomienda que utilice la GUI de administración MQIPT para gestionar los cambios realizados en MQIPT. El archivo de configuración de la Versión 1.1 es compatible con la GUI.

Nuevas opciones de configuración

Las propiedades siguientes son nuevas en la Versión 1.2:

LogDir
QoS
QosToDest
QosToCaller
SecurityManager
SecurityManagerPolicy
ServletClient
SocksClient
SocksServer
SocksProxyHost
SocksProxyPort
SSLProxyMode
UriName

Para obtener información acerca de todas las propiedades, consulte el apartado “Información de consulta relacionada con la configuración” en la página 54.

© Copyright IBM Corp. 2000-2002

Capítulo 4. Instalación de internet pass-thru en Windows

En este capítulo se describe cómo instalar MQIPT en un sistema Windows NT, Windows 2000 o Windows XP:

Descarga e instalación de los archivos

Puede descargar MQIPT desde la página web de SupportPac de WebSphere MQ:
`http://www.ibm.com/software/ts/mqseries/downloads`

Siga las instrucciones para descargar los archivos.

Abra un indicador de mandatos y desempaquete `ms81_nt.zip` en un directorio temporal. Ejecute el archivo `setup.exe` y siga las instrucciones en línea.

MQIPT debe instalarlo un usuario que tenga autorización de administrador.

MQIPT contiene los archivos que se muestran en la tabla siguiente y los archivos para la GUI del cliente de administración, que se proporciona como una característica que puede instalar por separado. En la tabla siguiente se muestran todos estos archivos.

Archivo	**Finalidad**
Readme.txt	La información más reciente que no se incluye en las publicaciones.
mqiptSample.conf	Archivo de configuración de ejemplo.
ssl\sslSample.pfx	Archivo de conjunto de claves de prueba.
ssl\sslSample.pwd	Archivo de contraseña para el archivo de conjunto de claves de prueba.
ssl\sslCAdefault.pfx	Archivo de conjunto de claves para la autoridad de certificación (CA) de ejemplo.
ssl\sslCAdefault.pwd	Archivo de contraseña para el archivo de conjunto de claves CA de ejemplo.
ssl\KeyMan.zip	Programa de utilidad KeyMan.
lib\MQipt.jar	Contiene los archivos de tiempo de ejecución, de clases y de propiedades.
lib\ADV_mqipt_normal. class	Asignador de tareas de Network Dispatcher para la modalidad "normal".

© Copyright IBM Corp. 2000-2002

Archivo	Finalidad
lib\ADV_mqipt_replace. class	Asignador de tareas de Network Dispatcher para la modalidad de “sustitución”.
lib\mqipt1414Sample.ssl	Archivo archivador de ejemplo para el asignador de tareas de Network Dispatcher.
bin\mqipt.bat	Método abreviado para ejecutar MQIPT desde la línea de mandatos.
bin\mqiptAdmin.bat	Método abreviado para detener MQIPT y renovar la información de archivos.
bin\mqiptservice.exe	Añadir o suprimir MQIPT en el administrador de control de servicios de Windows.
bin\mqiptVersion.bat	Muestra el número de versión de MQIPT.
web\MQIPTServlet.war	Archivo archivador web para la versión del servlet.
doc\<idioma>\pdf\ <nombrearchivo>.pdf	La publicación *internet pass-thru* en formato PDF. Consulte el apartado “Bibliografía” en la página xi para obtener más información sobre cómo obtener la documentación en copia impresa.
doc\<idioma>\html\ <nombrearchivo>.zip	Archivo maestro de la publicación *internet pass-thru* en formato HTML. Consulte el apartado “Bibliografía” en la página xi para obtener más información sobre cómo obtener la documentación en copia impresa.

Los archivos asociados con la característica de la GUI del cliente de administración son:

Archivo	Finalidad
lib\guiadmin.jar	Contiene los archivos de tiempo de ejecución, de clases y de propiedades.
bin\mqiptGui.bat	Método abreviado para ejecutar el cliente de administración desde la línea de mandatos.
bin\customSample. properties	Archivo de ejemplo para personalizar el diseño y, por lo tanto, el acceso del cliente de administración.

El programa de instalación actualiza la variable de entorno CLASSPATH con la ubicación de los archivos `MQipt.jar` y `guiadmin.jar`.

Preparación de internet pass-thru

Antes de iniciar MQIPT por primera vez, copie el archivo de configuración de ejemplo, `mqiptSample.conf` en `mqipt.conf`. Consulte el Capítulo 9, “Administración y configuración de internet pass-thru” en la página 49 para obtener información acerca de las tareas de configuración y administración.

Inicio de internet pass-thru desde la línea de mandatos

Abra un indicador de mandatos, vaya al directorio `bin` y ejecute `mqipt`. Por ejemplo:

```
c:
cd \mqipt\bin
mqipt ..
```

También puede iniciar MQIPT en Windows desde el menú Inicio -> Programas.

Si ejecuta el script `mqipt` sin ninguna opción, se utilizará la ubicación por omisión "." para el archivo de configuración (`mqipt.conf`). Para especificar una ubicación diferente:

```
mqipt <nombre_directorio>
```

Aparecerán mensajes en la consola que mostrarán el estado de MQIPT. Si se produce un error, consulte el apartado "Determinación de problemas" en la página 99. Los siguientes mensajes son un ejemplo de que MQIPT se ha iniciado correctamente:

```
5639-L92 (C) Copyright IBM Corp. 2000-2002 All Rights Reserved
MQCPI001 WebSphere MQ internet pass-thru Version 1.2 starting
MQCPI004 Reading configuration information from c:\mqipt\mqipt.conf
MQCPI008 Listening for control commands on port 1881
MQCPI011 The path c:\mqipt\logs will be used to store the log files
MQCPI006 Route 1418 has started and will forward messages to :
MQCPI034 ....mqserver.company4.com(1414)
MQCPI035 ....using MQ protocols
MQCPI006 Route 1415 has started and will forward messages to :
MQCPI034 ....mqipt.company2.com(1415)
MQCPI035 ....using MQ protocols
MQCPI036 ....SSL Client side enabled with properties :
MQCPI031 ......cipher suites <null>
MQCPI032 ......keyring file c:\mqipt\KeyMan.pfx
MQCPI038 ......distinguished name(s) CN=*Doe O=IBM OU=* L=* ST=* C=*
```

Cuando se invoca por primera vez MQIPT, se crean automáticamente los subdirectorios siguientes del directorio inicial `mqipt`:

- Un directorio ″logs″ en el que se guardan las anotaciones cronológicas de conexión.
- Un directorio ″errors″ en el que se graban los registros de rastreo y FFST™ (First Failure Support Technology™).

Inicio del cliente de administración desde la línea de mandatos

Abra un indicador de mandatos, vaya al directorio `bin` y ejecute `mqiptGui`. Por ejemplo:

```
c:
cd \mqipt\bin
mqiptGui
```

Para que el cliente de administración pueda realizar una conexión de salida a través de un cortafuegos con un MQIPT mediante un proxy SOCKS, especifique el nombre de sistema principal o la dirección y el número de puerta:

```
mqiptGui <NombreSistpralsocks <Puertasocks>>
```

El valor por omisión para `Puertasocks` es 1080.

En la ventana principal del cliente de administración aparecen mensajes que indican el estado del cliente de administración.

Utilización de un programa de control de servicios de Windows

Se proporciona por separado un programa de control de servicios, `mqiptservice.exe`, que permite gestionar e iniciar MQIPT como un servicio de Windows.

El programa `mqiptservice.exe` toma los siguientes argumentos de línea de mandatos:

mqiptservice -install ***vía de acceso***
Instala y registra el servicio, de modo que aparezca en el panel de servicios de Windows como un servicio manual. Vaya al panel de servicios y cambie el valor a "automático" para que MQIPT se inicie de forma automática cuando se inicie el sistema. Después de instalar este servicio, deberá reiniciar Windows. El parámetro de vía de acceso, que debe indicarse, es la vía de acceso totalmente calificada del directorio que contiene el archivo de configuración `mqipt.conf`. Indique entre comillas el nombre de vía de acceso si contiene espacios en blanco.

mqiptservice -remove
Suprime el servicio y éste desaparece del panel de servicios.

mqiptservice ?
Muestra mensajes de ayuda en inglés de EE.UU. con una lista de los argumentos válidos.

Si se especifica install y remove en el mismo mandato, se genera un error.

Internamente, Windows invoca `mqiptservice` sin argumentos. Si lo invoca desde la línea de mandatos sin argumentos, el programa sobrepasa el tiempo de espera y devuelve un error.

Cuando se inicia el servicio MQIPT, se inician todas las rutas activas de MQIPT. Cuando se detiene, se concluyen de forma inmediata todas las rutas.

Nota: La variable de entorno PATH debe contener la ubicación de las bibliotecas de tiempo de ejecución JNI. El archivo `jvm.dll` se puede encontrar en el subdirectorio `classics` de JDK.

Desinstalación de internet pass-thru como un servicio de Windows

Desinstale MQIPT como un servicio, deteniéndolo en el panel de servicios de Windows. A continuación, abra un indicador de mandatos, vaya al subdirectorio `bin` de MQIPT y escriba:

```
mqiptservice -remove
```

Desintalación de internet pass-thru

Antes de desinstalar MQIPT del sistema, suprímalo como un servicio de Windows, tal y como se ha descrito anteriormente. A continuación, ejecute el proceso de desintalación desde el menú Inicio de Windows.

Capítulo 5. Instalación de internet pass-thru en Sun Solaris

En este capítulo se describe cómo instalar MQIPT en un sistema Sun Solaris:

Descarga e instalación de los archivos

Puede descargar MQIPT desde la página web de SupportPac de WebSphere MQ:

```
http://www.ibm.com/software/ts/mqseries/downloads
```

Siga las instrucciones para descargar los archivos.

Inicie la sesión como usuario `root`, descomprima y desempaquete el archivo `ms81_sol.tar.Z` en un directorio temporal. Ejecute el mandato `pkgadd` como se muestra en el ejemplo siguiente:

```
login root
cd /tmp
uncompress -fv ms81_sol.tar.Z
tar xvf ms81_sol.tar
pkgadd -d . mqipt
```

En el ejemplo se presupone que `ms81_sol.tar.Z` está en el directorio /tmp.

MQIPT contiene los archivos que se muestran en la tabla siguiente, incluidos los archivos para la GUI del cliente de administración.

Archivo	**Finalidad**
Readme.txt	La información más reciente que no se incluye en las publicaciones.
mqiptSample.conf	Archivo de configuración de ejemplo.
ssl/sslSample.pfx	Archivo de conjunto de claves de prueba.
ssl/sslSample.pwd	Archivo de contraseña para el archivo de conjunto de claves de prueba.
ssl/sslCAdefault.pfx	Archivo de conjunto de claves para la autoridad de certificación (CA) de ejemplo.
ssl/sslCAdefault.pwd	Archivo de contraseña para el archivo de conjunto de claves CA de ejemplo.
ssl/KeyMan.zip	Programa de utilidad KeyMan.
lib/MQipt.jar	Contiene los archivos de tiempo de ejecución, de clases y de propiedades.
lib/ADV_mqipt_normal. class	Asignador de tareas de Network Dispatcher para la modalidad "normal".
lib/ADV_mqipt_replace. class	Asignador de tareas de Network Dispatcher para la modalidad de "sustitución".

© Copyright IBM Corp. 2000-2002

Archivo	Finalidad
lib/mqipt1414Sample.ssl	Archivo archivador de ejemplo para el asignador de tareas de Network Dispatcher.
bin/mqipt	Método abreviado para ejecutar MQIPT desde la línea de mandatos.
bin/mqiptAdmin	Método abreviado para detener MQIPT y renovar la información de archivos.
bin/mqiptVersion	Muestra el número de versión de MQIPT.
bin/mqiptService	Instalar MQIPT de modo que se inicie automáticamente cuando se arranque el sistema.
bin/mqiptEnv	Define la ubicación del archivo `mqipt.jar` y lo utilizan únicamente los demás scripts.
web/MQIPTServlet.war	Archivo archivador web para la versión del servlet.
doc/<idioma>/pdf/ <nombrearchivo>.pdf	La publicación *internet pass-thru* en formato PDF. Consulte el apartado "Bibliografía" en la página xi para obtener más información sobre cómo obtener la documentación en copia impresa.
doc/<idioma>/html/ <nombrearchivo>.zip	Archivo maestro de la publicación *internet pass-thru* en formato HTML. Consulte el apartado "Bibliografía" en la página xi para obtener más información sobre cómo obtener la documentación en copia impresa.
lib/mqiptGui.jar	Contiene los archivos de tiempo de ejecución, de clases y de propiedades de la GUI del cliente de administración.
bin/mqiptGui	Método abreviado para ejecutar el cliente de administración desde la línea de mandatos.
bin/customSample. properties	Archivo de ejemplo para personalizar el diseño y, por lo tanto, el acceso del cliente de administración.

Preparación de internet pass-thru

Antes de iniciar MQIPT por primera vez, copie el archivo de configuración de ejemplo, `mqiptSample.conf` en `mqipt.conf`. Consulte el Capítulo 9, "Administración y configuración de internet pass-thru" en la página 49 para obtener información acerca de las tareas de configuración y administración.

Inicio de internet pass-thru desde la línea de mandatos

Inicie la sesión como usuario `root` y vaya al directorio `bin`. Por ejemplo:

```
cd /opt/mqipt/bin
mqipt ..
```

Si ejecuta el script `mqipt` sin ninguna opción se utilizará la ubicación por omisión "." para el archivo de configuración (`mqipt.conf`). Para especificar una ubicación diferente:

```
mqipt <nombre_directorio>
```

Aparecerán mensajes en la consola que mostrarán el estado de MQIPT. Si se produce un error, consulte el apartado "Determinación de problemas" en la página 99. Los siguientes mensajes son un ejemplo de que MQIPT se ha iniciado correctamente:

```
5639-L92 (C) Copyright IBM Corp. 2000-2002 All Rights Reserved
MQCPI001 WebSphere MQ internet pass-thru Version 1.2 starting
MQCPI004 Reading configuration information from /opt/mqipt/mqipt.conf
MQCPI008 Listening for control commands on port 1881
MQCPI011 The path /opt/mqipt/logs will be used to store the log files
MQCPI006 Route 1418 has started and will forward messages to :
MQCPI034 ....mqserver.company4.com(1414)
MQCPI035 ....using MQ protocols
MQCPI006 Route 1415 has started and will forward messages to :
MQCPI034 ....mqipt.company2.com(1415)
MQCPI035 ....using MQ protocols
MQCPI036 ....SSL Client side enabled with properties :
MQCPI031 ......cipher suites <null>
MQCPI032 ......keyring file /opt/mqipt/KeyMan.pfx
MQCPI038 ......distinguished name(s) CN=*Doe O=IBM OU=* L=* ST=* C=*
```

Cuando se invoca por primera vez MQIPT, se crean automáticamente los subdirectorios siguientes del directorio inicial `mqipt`:

- Un directorio ″logs″ en el que se guardan las anotaciones cronológicas de conexión.
- Un directorio ″errors″ en el que se graban los registros de rastreo y FFST (First Failure Support Technology).

Inicio automático de internet pass-thru

Para que MQIPT se inicie de forma automática cuando arranque el sistema, ejecute el script `mqiptService`. Por ejemplo:

```
cd /opt/mqipt/bin
mqiptService -install
```

Para que MQIPT no se inicie automáticamente:

```
cd /opt/mqipt/bin
mqiptService -remove
```

Inicio del cliente de administración desde la línea de mandatos

Abra un indicador de mandatos, vaya al directorio `bin` y ejecute `mqiptGui`. Por ejemplo:

```
cd /opt/mqipt/bin
mqiptGui
```

Para que el cliente de administración pueda realizar una conexión de salida a través de un cortafuegos con un MQIPT, especifique el nombre de sistema principal o la dirección y el número de puerta:

```
mqiptGui <NombreSistpralsocks <Puertasocks>>
```

El valor por omisión para `Puertasocks` es 1080.

En la ventana principal del cliente de administración aparecen mensajes que indican el estado del cliente de administración.

Desintalación de internet pass-thru

Antes de desinstalar MQIPT del sistema, impida que se inicie automáticamente como se describe en el apartado “Inicio automático de internet pass-thru”. Inicie la sesión como usuario `root` y ejecute el mandato `pkgrm`:

```
pkgrm mqipt
```

Capítulo 6. Instalación de internet pass-thru en AIX

En este capítulo se describe cómo instalar MQIPT en un sistema AIX:

Descarga e instalación de los archivos

Puede descargar MQIPT desde la página web de SupportPac de WebSphere MQ:

`http://www.ibm.com/software/ts/mqseries/downloads`

Siga las instrucciones para descargar los archivos.

Inicie la sesión como usuario `root`, descomprima y desempaquete el archivo `ms81_aix.tar.Z` en un directorio temporal. Ejecute el mandato `installp` como se muestra en el ejemplo siguiente:

```
cd /tmp
uncompress -fv ms81_aix.tar.Z
tar xvf ms81_aix.tar
installp -d . -a mqipt-RT
```

En el ejemplo se presupone que `ms81_aix.tar.Z` está en el directorio /tmp.

MQIPT contiene los archivos que se muestran en la tabla siguiente, incluidos los archivos para la GUI del cliente de administración.

Archivo	**Finalidad**
Readme.txt	La información más reciente que no se incluye en las publicaciones.
mqiptSample.conf	Archivo de configuración de ejemplo.
ssl/sslSample.pfx	Archivo de conjunto de claves de prueba.
ssl/sslSample.pwd	Archivo de contraseña para el archivo de conjunto de claves de prueba.
ssl/sslCAdefault.pfx	Archivo de conjunto de claves para la autoridad de certificación (CA) de ejemplo.
ssl/sslCAdefault.pwd	Archivo de contraseña para el archivo de conjunto de claves CA de ejemplo.
ssl/KeyMan.zip	Programa de utilidad KeyMan.
lib/MQipt.jar	Contiene los archivos de tiempo de ejecución, de clases y de propiedades.
lib/ADV_mqipt_normal. class	Asignador de tareas de Network Dispatcher para la modalidad "normal".
lib/ADV_mqipt_replace. class	Asignador de tareas de Network Dispatcher para la modalidad de "sustitución".

© Copyright IBM Corp. 2000-2002

Archivo	Finalidad
lib/mqipt1414Sample.ssl	Archivo archivador de ejemplo para el asignador de tareas de Network Dispatcher.
bin/mqipt	Método abreviado para ejecutar MQIPT desde la línea de mandatos.
bin/mqiptAdmin	Método abreviado para detener MQIPT y renovar la información de archivos.
bin/mqiptVersion	Muestra el número de versión de MQIPT.
bin/mqiptService	Instalar MQIPT de modo que se inicie automáticamente cuando se arranque el sistema.
bin/mqiptEnv	Define la ubicación del archivo `mqipt.jar` y lo utilizan únicamente los demás scripts.
web/MQIPTServlet.war	Archivo archivador web para la versión del servlet.
doc/<idioma>/pdf/ <nombrearchivo>.pdf	La publicación *internet pass-thru* en formato PDF. Consulte el apartado "Bibliografía" en la página xi para obtener más información sobre cómo obtener la documentación en copia impresa.
doc/<idioma>/html/ <nombrearchivo>.zip	Archivo maestro de la publicación *internet pass-thru* en formato HTML. Consulte el apartado "Bibliografía" en la página xi para obtener más información sobre cómo obtener la documentación en copia impresa.
lib/mqiptGui.jar	Contiene los archivos de tiempo de ejecución, de clases y de propiedades.
bin/mqiptGui	Método abreviado para ejecutar el cliente de administración desde la línea de mandatos.
bin/customSample. properties	Archivo de ejemplo para personalizar el diseño y, por lo tanto, el acceso del cliente de administración.

Preparación de internet pass-thru

Antes de iniciar MQIPT por primera vez, copie el archivo de configuración de ejemplo, `mqiptSample.conf` en `mqipt.conf`. Consulte el Capítulo 9, "Administración y configuración de internet pass-thru" en la página 49 para obtener información acerca de las tareas de configuración y administración.

Inicio de internet pass-thru desde la línea de mandatos

Inicie la sesión como usuario `root` y vaya al directorio `bin`. Por ejemplo:

```
cd /usr/opt/mqipt/bin
mqipt ..
```

Si ejecuta el script `mqipt` sin ninguna opción se utilizará la ubicación por omisión "." para el archivo de configuración (`mqipt.conf`). Para especificar una ubicación diferente:

```
mqipt <nombre_directorio>
```

Aparecerán mensajes en la consola que mostrarán el estado de MQIPT. Si se produce un error, consulte el apartado "Determinación de problemas" en la página 99. Los siguientes mensajes son un ejemplo de que MQIPT se ha iniciado correctamente:

```
5639-L92 (C) Copyright IBM Corp. 2000-2002 All Rights Reserved
MQCPI001 WebSphere MQ internet pass-thru Version 1.2 starting
MQCPI004 Reading configuration information from /usr/opt/mqipt/mqipt.conf
MQCPI008 Listening for control commands on port 1881
MQCPI011 The path /usr/opt/mqipt/logs will be used to store the log files
MQCPI006 Route 1418 has started and will forward messages to :
MQCPI034 ....mqserver.company4.com(1414)
MQCPI035 ....using MQ protocols
MQCPI006 Route 1415 has started and will forward messages to :
MQCPI034 ....mqipt.company2.com(1415)
MQCPI035 ....using MQ protocols
MQCPI036 ....SSL Client side enabled with properties :
MQCPI031 ......cipher suites <null>
MQCPI032 ......keyring file /usr/opt/mqipt/KeyMan.pfx
MQCPI038 ......distinguished name(s) CN=*Doe O=IBM OU=* L=* ST=* C=*
```

Cuando se invoca por primera vez MQIPT, se crean automáticamente los subdirectorios siguientes del directorio inicial `mqipt`:

- Un directorio ″logs″ en el que se guardan las anotaciones cronológicas de conexión.
- Un directorio ″errors″ en el que se graban los registros de rastreo y FFST (First Failure Support Technology).

Inicio automático de internet pass-thru

Para que MQIPT se inicie de forma automática cuando arranque el sistema, ejecute el script `mqiptService` para añadir una entrada a `inittab`. Por ejemplo:

```
cd /usr/opt/mqipt/bin
../mqiptService -install
```

Para que MQIPT no se inicie automáticamente y para suprimir su entrada en `inittab`:

```
cd /usr/opt/mqipt/bin
../mqiptService -remove
```

Inicio del cliente de administración desde la línea de mandatos

Abra un indicador de mandatos, vaya al directorio `bin` y ejecute `mqiptGui`. Por ejemplo:

```
cd /usr/opt/mqipt/bin
../mqiptGui
```

Para que el cliente de administración pueda realizar una conexión de salida a través de un cortafuegos con un MQIPT, especifique el nombre de sistema principal o la dirección y el número de puerta:

```
mqiptGui <NombreSistpralsocks <Puertasocks>>
```

El valor por omisión para `Puertasocks` es 1080.

En la ventana principal del cliente de administración aparecen mensajes que indican el estado del cliente de administración.

Desintalación de internet pass-thru

Antes de desinstalar MQIPT del sistema, impida que se inicie automáticamente como se describe en el apartado “Inicio automático de internet pass-thru” en la página 39. Inicie la sesión como usuario `root` y ejecute el mandato `installp`:

```
installp -u mqipt-RT
```

Capítulo 7. Instalación de internet pass-thru en HP-UX

En este capítulo se describe cómo instalar MQIPT en un sistema HP-UX:

Descarga e instalación de los archivos

Puede descargar MQIPT desde la página web de SupportPac de WebSphere MQ:

```
http://www.ibm.com/software/ts/mqseries/downloads
```

Siga las instrucciones para descargar los archivos.

Inicie la sesión como usuario `root`, descomprima y desempaquete el archivo `ms81_hp11.tar.Z` en un directorio temporal. Ejecute el mandato `swinstall` como se muestra en el ejemplo siguiente:

```
login root
cd /tmp
uncompress -fv ms81_hp11.tar.Z
tar xvf ms81_hp11.tar
swinstall -s /tmp MQIPT.MQIPT-RT
```

En el ejemplo se presupone que `ms81_hp11.tar.Z` está en el directorio /tmp.

MQIPT contiene los archivos que se muestran en la tabla siguiente, incluidos los archivos para la GUI del cliente de administración.

Archivo	**Finalidad**
Readme.txt	La información más reciente que no se incluye en las publicaciones.
mqiptSample.conf	Archivo de configuración de ejemplo.
ssl/sslSample.pfx	Archivo de conjunto de claves de prueba.
ssl/sslSample.pwd	Archivo de contraseña para el archivo de conjunto de claves de prueba.
ssl/sslCAdefault.pfx	Archivo de conjunto de claves para la autoridad de certificación (CA) de ejemplo.
ssl/sslCAdefault.pwd	Archivo de contraseña para el archivo de conjunto de claves CA de ejemplo.
ssl/KeyMan.zip	Programa de utilidad KeyMan.
lib/MQipt.jar	Contiene los archivos de tiempo de ejecución, de clases y de propiedades.
lib/ADV_mqipt_normal. class	Asignador de tareas de Network Dispatcher para la modalidad "normal".
lib/ADV_mqipt_replace. class	Asignador de tareas de Network Dispatcher para la modalidad de "sustitución".

© Copyright IBM Corp. 2000-2002

Archivo	Finalidad
lib/mqipt1414Sample.ssl	Archivo archivador de ejemplo para el asignador de tareas de Network Dispatcher.
bin/mqipt	Método abreviado para ejecutar MQIPT desde la línea de mandatos.
bin/mqiptAdmin	Método abreviado para detener MQIPT y renovar la información de archivos.
bin/mqiptVersion	Muestra el número de versión de MQIPT.
bin/mqiptService	Instalar MQIPT de modo que se inicie automáticamente cuando se arranque el sistema.
bin/mqiptEnv	Define la ubicación del archivo `mqipt.jar` y lo utilizan únicamente los demás scripts.
bin/mqiptFork	Se utiliza para iniciar MQIPT durante el arranque del sistema.
web/MQIPTServlet.war	Archivo archivador web para la versión del servlet.
doc/<idioma>/pdf/ <nombrearchivo>.pdf	La publicación *internet pass-thru* en formato PDF. Consulte el apartado "Bibliografía" en la página xi para obtener más información sobre cómo obtener la documentación en copia impresa.
doc/<idioma>/html/ <nombrearchivo>.zip	Archivo maestro de la publicación *internet pass-thru* en formato HTML. Consulte el apartado "Bibliografía" en la página xi para obtener más información sobre cómo obtener la documentación en copia impresa.
lib/mqiptGui.jar	Contiene los archivos de tiempo de ejecución, de clases y de propiedades de la GUI del cliente de administración.
bin/mqiptGui	Método abreviado para ejecutar el cliente de administración desde la línea de mandatos.
bin/customSample. properties	Archivo de ejemplo para personalizar el diseño y, por lo tanto, el acceso del cliente de administración.

Preparación de internet pass-thru

Antes de iniciar MQIPT por primera vez, copie el archivo de configuración de ejemplo, `mqiptSample.conf` en `mqipt.conf`. Consulte el Capítulo 9, "Administración y configuración de internet pass-thru" en la página 49 para obtener información acerca de las tareas de configuración y administración.

Inicio de internet pass-thru desde la línea de mandatos

Inicie la sesión como usuario `root` y vaya al directorio `bin`. Por ejemplo:

```
cd /opt/mqipt/bin
mqipt ..
```

Si ejecuta el script `mqipt` sin ninguna opción se utilizará la ubicación por omisión "." para el archivo de configuración (`mqipt.conf`). Para especificar una ubicación diferente:

```
mqipt <nombre_directorio>
```

Aparecerán mensajes en la consola que mostrarán el estado de MQIPT. Si se produce un error, consulte el apartado "Determinación de problemas" en la página 99. Los siguientes mensajes son un ejemplo de que MQIPT se ha iniciado correctamente:

```
5639-L92 (C) Copyright IBM Corp. 2000-2002 All Rights Reserved
MQCPI001 WebSphere MQ internet pass-thru Version 1.2 starting
MQCPI004 Reading configuration information from /opt/mqipt/mqipt.conf
MQCPI008 Listening for control commands on port 1881
MQCPI011 The path /opt/mqipt/logs will be used to store the log files
MQCPI006 Route 1418 has started and will forward messages to :
MQCPI034 ....mqserver.company4.com(1414)
MQCPI035 ....using MQ protocols
MQCPI006 Route 1415 has started and will forward messages to :
MQCPI034 ....mqipt.company2.com(1415)
MQCPI035 ....using MQ protocols
MQCPI036 ....SSL Client side enabled with properties :
MQCPI031 ......cipher suites <null>
MQCPI032 ......keyring file /opt/mqipt/KeyMan.pfx
MQCPI038 ......distinguished name(s) CN=*Doe O=IBM OU=* L=* ST=* C=*
```

Cuando se invoca por primera vez MQIPT, se crean automáticamente los subdirectorios siguientes del directorio inicial `mqipt`:

- Un directorio "logs" en el que se guardan las anotaciones cronológicas de conexión.
- Un directorio "errors" en el que se graban los registros de rastreo y FFST (First Failure Support Technology).

Inicio automático de internet pass-thru

Para que MQIPT se inicie de forma automática cuando arranque el sistema, ejecute el script `mqiptService`. Por ejemplo:

```
cd /opt/mqipt/bin
mqiptService -install
```

Se presupone que JDK 1.4 ya está instalado en un directorio llamado `/opt/java1.4`. Si no es así, edite el archivo `mqipt.ske` y cambie la variable PATH de modo que apunte a la ubicación de JDK. Debe aplicar este cambio antes de ejecutar el mandato `mqiptService -install`.

Cuando se inicia MQIPT como un servicio, graba un archivo `console.log` en el subdirectorio `logs`. Este subdirectorio se crea la primera vez que se ejecuta MQIPT, por lo tanto, debe haber iniciado MQIPT una vez como mínimo antes de intentar iniciarlo como un servicio.

Para que MQIPT no se inicie automáticamente:

```
cd /opt/mqipt/bin
mqiptService -remove
```

Inicio del cliente de administración desde la línea de mandatos

Abra un indicador de mandatos, vaya al directorio `bin` y ejecute `mqiptGui`. Por ejemplo:

```
cd /opt/mqipt/bin
mqiptGui
```

Para que el cliente de administración pueda realizar una conexión de salida a través de un cortafuegos con un MQIPT, especifique el nombre de sistema principal o la dirección y el número de puerta:

```
mqiptGui <NombreSistpralsocks <Puertasocks>>
```

El valor por omisión para `Puertasocks` es 1080.

En la ventana principal del cliente de administración aparecen mensajes que indican el estado del cliente de administración.

Desintalación de internet pass-thru

Antes de desinstalar MQIPT del sistema, impida que se inicie automáticamente como se describe en el apartado “Inicio automático de internet pass-thru” en la página 43. Inicie la sesión como usuario `root` y ejecute el mandato `swremove`:

```
swremove MQIPT
```

Capítulo 8. Instalación de internet pass-thru en Linux

En este capítulo se describe cómo instalar MQIPT en un sistema Linux:

Descarga e instalación de los archivos

Puede descargar MQIPT desde la página web de SupportPac de WebSphere MQ:

```
http://www.ibm.com/software/ts/mqseries/downloads
```

Siga las instrucciones para descargar los archivos.

Inicie la sesión como usuario `root`, descomprima y desempaquete el archivo `ms81_linux.tar.gz` en un directorio temporal. Ejecute el mandato `rpm` como se muestra en el ejemplo siguiente:

```
login root
cd /tmp
gunzip -fv ms81_linux.tar.gz
tar xvf mq81_linux.tar
cd i386
rpm -i WebSphereMQ-IPT-1.2.0-0.i386.rpm
```

En el ejemplo se presupone que `ms81_linux.tar.gz` está en el directorio /tmp.

MQIPT contiene los archivos que se muestran en la tabla siguiente, incluidos los archivos para la GUI del cliente de administración.

Archivo	**Finalidad**
Readme.txt	La información más reciente que no se incluye en las publicaciones.
mqiptSample.conf	Archivo de configuración de ejemplo.
ssl/sslSample.pfx	Archivo de conjunto de claves de prueba.
ssl/sslSample.pwd	Archivo de contraseña para el archivo de conjunto de claves de prueba.
ssl/sslCAdefault.pfx	Archivo de conjunto de claves para la autoridad de certificación (CA) de ejemplo.
ssl/sslCAdefault.pwd	Archivo de contraseña para el archivo de conjunto de claves CA de ejemplo.
ssl/KeyMan.zip	Programa de utilidad KeyMan.
lib/MQipt.jar	Contiene los archivos de tiempo de ejecución, de clases y de propiedades.
lib/ADV_mqipt_normal. class	Asignador de tareas de Network Dispatcher para la modalidad "normal".

© Copyright IBM Corp. 2000-2002

Archivo	Finalidad
lib/ADV_mqipt_replace. class	Asignador de tareas de Network Dispatcher para la modalidad de “sustitución”.
lib/mqipt1414Sample.ssl	Archivo archivador de ejemplo para el asignador de tareas de Network Dispatcher.
lib/libiptqos.so	Biblioteca de tiempo de ejecución para el soporte de calidad de servicio.
bin/mqipt	Método abreviado para ejecutar MQIPT desde la línea de mandatos.
bin/mqiptAdmin	Método abreviado para detener MQIPT y renovar la información de archivos.
bin/mqiptVersion	Muestra el número de versión de MQIPT.
bin/mqiptService	Instalar MQIPT de modo que se inicie automáticamente cuando se arranque el sistema.
bin/mqiptEnv	Define la ubicación del archivo `mqipt.jar` y lo utilizan únicamente los demás scripts.
web/MQIPTServlet.war	Archivo archivador web para la versión del servlet.
doc/<land>/pdf/ <nombrearchivo>.pdf	La publicación *internet pass-thru* en formato PDF. Consulte el apartado “Bibliografía” en la página xi para obtener más información sobre cómo obtener la documentación en copia impresa.
doc/<idioma>/html/ <nombrearchivo>.zip	Archivo maestro de la publicación *internet pass-thru* en formato HTML. Consulte el apartado “Bibliografía” en la página xi para obtener más información sobre cómo obtener la documentación en copia impresa.
lib/mqiptGui.jar	Contiene los archivos de tiempo de ejecución, de clases y de propiedades de la GUI del cliente de administración.
bin/mqiptGui	Método abreviado para ejecutar el cliente de administración desde la línea de mandatos.
bin/customSample. properties	Archivo de ejemplo para personalizar el diseño y, por lo tanto, el acceso del cliente de administración.

Preparación de internet pass-thru

Antes de iniciar MQIPT por primera vez, copie el archivo de configuración de ejemplo, `mqiptSample.conf` en `mqipt.conf`. Consulte el Capítulo 9, “Administración y configuración de internet pass-thru” en la página 49 para obtener información acerca de las tareas de configuración y administración.

Inicio de internet pass-thru desde la línea de mandatos

Inicie la sesión como usuario `root` y vaya al directorio `bin`. Por ejemplo:

```
cd /opt/mqipt/bin
mqipt ..
```

Si ejecuta el script `mqipt` sin ninguna opción se utilizará la ubicación por omisión “.” para el archivo de configuración (`mqipt.conf`). Para especificar una ubicación diferente:

```
mqipt <nombre_directorio>
```

Aparecerán mensajes en la consola que mostrarán el estado de MQIPT. Si se produce un error, consulte el apartado “Determinación de problemas” en la página 99. Los siguientes mensajes son un ejemplo de que MQIPT se ha iniciado correctamente:

```
5639-L92 (C) Copyright IBM Corp. 2000-2002 All Rights Reserved
MQCPI001 WebSphere MQ internet pass-thru Version 1.2 starting
MQCPI004 Reading configuration information from /opt/mqipt/mqipt.conf
MQCPI008 Listening for control commands on port 1881
MQCPI011 The path /opt/mqipt/logs will be used to store the log files
MQCPI006 Route 1418 has started and will forward messages to :
MQCPI034 ....mqserver.company4.com(1414)
MQCPI035 ....using MQ protocols
MQCPI006 Route 1415 has started and will forward messages to :
MQCPI034 ....mqipt.company2.com(1415)
MQCPI035 ....using MQ protocols
MQCPI036 ....SSL Client side enabled with properties :
MQCPI031 ......cipher suites <null>
MQCPI032 ......keyring file /opt/mqipt/KeyMan.pfx
MQCPI038 ......distinguished name(s) CN=*Doe O=IBM OU=* L=* ST=* C=*
```

Cuando se invoca por primera vez MQIPT, se crean automáticamente los subdirectorios siguientes del directorio inicial `mqipt`:

- Un directorio ″logs″ en el que se guardan las anotaciones cronológicas de conexión.
- Un directorio ″errors″ en el que se graban los registros de rastreo y FFST (First Failure Support Technology).

Inicio automático de internet pass-thru

Para que MQIPT se inicie de forma automática cuando arranque el sistema, ejecute el script `mqiptService`. Por ejemplo:

```
cd /opt/mqipt/bin
mqiptService -install
```

Cuando se inicia MQIPT como un servicio, graba un archivo `console.log` en el subdirectorio `logs`. Este subdirectorio se crea la primera vez que se ejecuta MQIPT, por lo tanto, debe haber iniciado MQIPT una vez como mínimo antes de intentar iniciarlo como un servicio.

Para que MQIPT no se inicie automáticamente:

```
cd /opt/mqipt/bin
mqiptService -remove
```

Inicio del cliente de administración desde la línea de mandatos

Abra un indicador de mandatos, vaya al directorio `bin` y ejecute `mqiptGui`. Por ejemplo:

```
cd /opt/mqipt/bin
mqiptGui
```

Para que el cliente de administración pueda realizar una conexión de salida a través de un cortafuegos con un MQIPT, especifique el nombre de sistema principal o la dirección y el número de puerta:

```
mqiptGui <NombreSistpralsocks <Puertasocks>>
```

El valor por omisión para `Puertasocks` es 1080.

En la ventana principal del cliente de administración aparecen mensajes que indican el estado del cliente de administración.

Desintalación de internet pass-thru

Antes de desinstalar MQIPT del sistema, impida que se inicie automáticamente como se describe en el apartado “Inicio automático de internet pass-thru” en la página 47. Inicie la sesión como usuario `root` y ejecute el mandato `swremove`:

```
rpm -e WebSphereMQ-IPT-1.2.0-0
```

Capítulo 9. Administración y configuración de internet pass-thru

MQIPT se configura modificando el archivo de configuración `mqipt.conf`. Para ello se utiliza el cliente de administración, el cual es el método recomendado, o el editor que desee. En la información de este capítulo se describen ambos métodos junto con la información relacionada:

- "Utilización del cliente de administración de internet pass-thru"
- "Utilización de los mandatos de internet pass-thru en modalidad de línea de mandatos" en la página 53
- "Información de consulta relacionada con la configuración" en la página 54

Utilización del cliente de administración de internet pass-thru

Puede utilizar el cliente de administración para configurar y actualizar uno o varios MQIPT. Muestra las propiedades globales de un MQIPT y las propiedades específicas de la ruta.

Los únicos datos que se almacenan localmente en el cliente de administración es la lista de los MQIPT, que se encuentra en el archivo `client.conf`. Antes de mostrarse las propiedades globales y de rutas en el cliente de administración, éstas se recuperan siempre de MQIPT.

Inicio del cliente de administración

Inicie el cliente de administración utilizando el script `mqiptGui` que se encuentra en el subdirectorio `bin` de MQIPT. Consulte el capítulo de instalación de cada plataforma para obtener información sobre cómo iniciar el cliente de administración.

La primera vez que se inicia el cliente de administración, se muestra un cuadro de diálogo que le solicita información sobre la conexión con un MQIPT. La información que necesita es:

Nombre de MQIPT
El nombre utilizado para describir este MQIPT. Aunque esta información no es esencial, se recomienda que la proporcione.

Dirección de red
La dirección del sistema en que reside MQIPT; puede ser un nombre reconocido por el servidor de nombres, una dirección decimal con puntos, un sistema principal local (si MQIPT está en la misma máquina que el cliente).

Puerta de mandatos
El número de la puerta en la que MQIPT escucha los mandatos.

Tiempo de espera
El número de segundos que el cliente de administración esperará una conexión con MQIPT. Mantenga este valor lo más bajo posible para disminuir el tiempo de renovación de la ventana.

Contraseña de acceso
La contraseña que se utiliza para las comunicaciones con MQIPT. Rellene este campo solamente si la comprobación de contraseñas está en vigor. La

© Copyright IBM Corp. 2000-2002

comprobación de contraseñas está en vigor si se proporciona AccessPW en el archivo de configuración MQIPT y su valor no es una serie de caracteres nula.

Guardar contraseña
Si se deja en blanco este recuadro de selección, se recordará mientras dure la sesión o hasta que se suprima MQIPT. Si se selecciona el recuadro, la contraseña se guardará para las próximas sesiones.

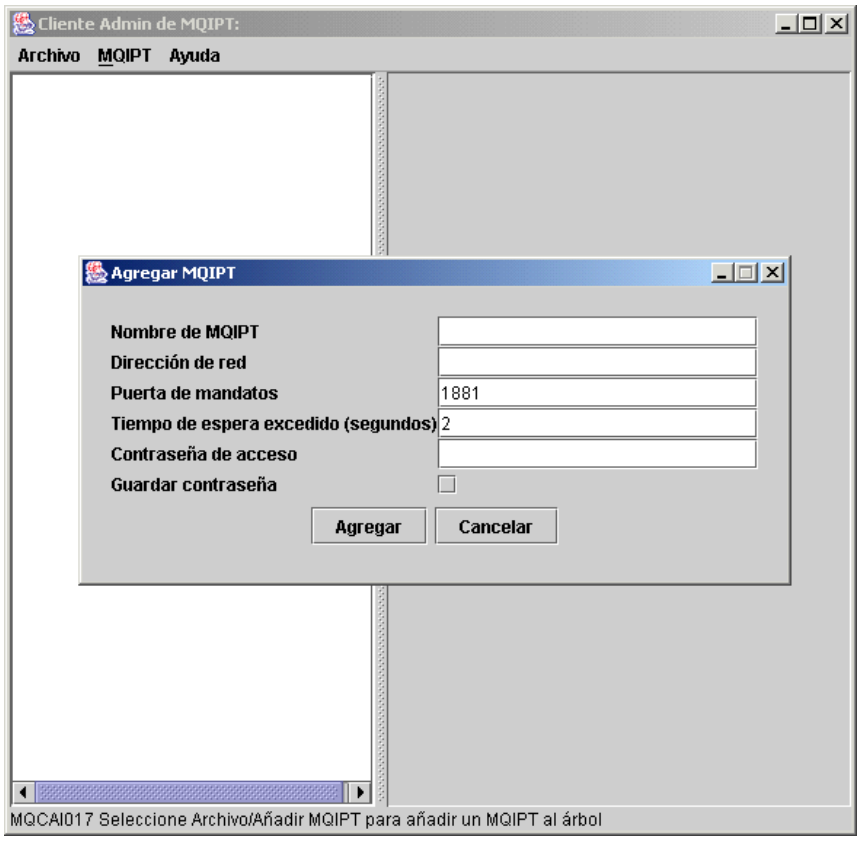

Figura 8. Ventana para acceder por primera vez a un MQIPT

Administración de un MQIPT

Sólo se puede actualizar un MQIPT cada vez, por lo tanto, si se selecciona otro MQIPT de la lista, los cambios pendientes deberán aplicarse antes de continuar. Los cambios que se realicen a las propiedades no afectarán a MQIPT hasta que se utilice la opción de menú “Aplicar“.

Si selecciona un MQIPT de la lista se recuperan las propiedades globales y de rutas de MQIPT. Si MQIPT no está ejecutándose o si se ha especificado un valor incorrecto para CommandPort, se emite un mensaje de error. El nombre de sistema principal y el valor de CommandPort se pueden modificar con la opción de menú “Conexión”.

Si pulsa dos veces en un MQIPT de la lista se muestra una lista de las rutas. Al seleccionar una ruta, se muestran sus propiedades. Puede personalizar las propiedades según sus requisitos.

Si utiliza un archivo de configuración (`mqipt.conf`) de MQSeries internet pass-thru Versión 1.0, no verá un nombre de ruta. Puede añadir un nombre de ruta actualizando el campo Nombre.

Cuando se aplican los cambios se añade una indicación de la hora al archivo de configuración y se devuelve a MQIPT; los cambios entran en vigor de forma inmediata. Las líneas de comentarios que haya en el archivo se perderán.

Se puede añadir una ruta utilizando la opción de menú "Agregar ruta". Se mostrará un conjunto de las propiedades por omisión de esta ruta nueva, según se haya definido mediante las propiedades globales.

Herencia de las propiedades

En el cliente de administración, las propiedades de los MQIPT y de las rutas se pueden establecer dentro de una jerarquía de métodos:

1. Toda propiedad tiene un valor por omisión y si la propiedad no se menciona en el archivo de configuración o si el usuario no la ha establecido específicamente en el cliente de administración, se presupone el valor por omisión.
2. Se presupone que las propiedades globales que se establecen para cada MQIPT son también las de cada ruta de dicho MQIPT, a menos que haya una información de ruta específica que indique lo contrario. En el archivo de configuración, esto significa que las propiedades que se establecen en la sección global se propagan a todas las rutas, a menos que se establezcan propiedades adicionales en las secciones de rutas. Las propiedades que establece el usuario del cliente de administración en un MQIPT se propagan a todas las rutas, a menos que se establezca específicamente una propiedad en una ruta.
3. Independientemente de los valores por omisión y de los valores globales, los valores que se establezcan para una ruta se mantendrán para la misma.

Opciones del menú Archivo

La mayor parte de las opciones relacionadas con la gestión del árbol se muestran cuando se selecciona el menú Archivo.

Agregar MQIPT
Muestra el mismo diálogo que aparece cuando se utiliza por primera vez el cliente, como se describe en el apartado "Inicio del cliente de administración" en la página 49.

Quitar MQIPT
Suprime solamente el MQIPT que está resaltado del árbol del cliente de administración. No afecta a la ejecución de MQIPT.

Guardar configuración
Guarda los nodos MQIPT del árbol en el archivo de configuración del cliente de administración, de modo que puedan volver a leerse la próxima vez que se inicie. Solamente se guardan los nodos MQIPT. Las propiedades globales y de rutas siempre se recuperan de MQIPT.

Salir
Detiene la ejecución del cliente de administración. Sin embargo, el cliente de administración comprueba en primer lugar si el árbol o el MQIPT actual se han modificado; si uno de ellos o los dos se han modificado, se visualizará uno o varios diálogos en que se le preguntará si desea guardar el cliente, aplicar los cambios a MQIPT o ambas cosas.

Opciones de menú de MQIPT

Conexión
Cambia los parámetros de acceso de un MQIPT. Los cambios se reflejan en la vista de árbol. Muestra una ventana similar a la que se describe en el apartado "Inicio del cliente de administración" en la página 49.

Contraseña
Cambia la propiedad de la contraseña del MQIPT remoto. Esta acción hace que se visualice un diálogo de contraseña donde debe realizar las entradas siguientes:

- **Contraseña actual**: para comprobar que no está haciendo un uso indebido, debe demostrar que sabe cuál es la contraseña antes de modificarla. Si no hay ninguna contraseña en vigor, este campo se deja en blanco.
- **Contraseña nueva**: la contraseña nueva o en blanco, si desea interrumpir el uso de contraseñas en este MQIPT.
- **Volver a entrar contraseña nueva**: impide que escriba errores tipográficos en el campo anterior y le solicita que repita la misma información.
- **Guardar contraseña**: se utiliza para determinar si la contraseña nueva se guardará localmente, junto con otras propiedades de acceso de este MQIPT.

Agregar ruta
Agrega una ruta del MQIPT seleccionado. Consulte la Figura 9 para obtener información detallada. Cada ruta debe tener un valor exclusivo de ListenerPort para MQIPT.

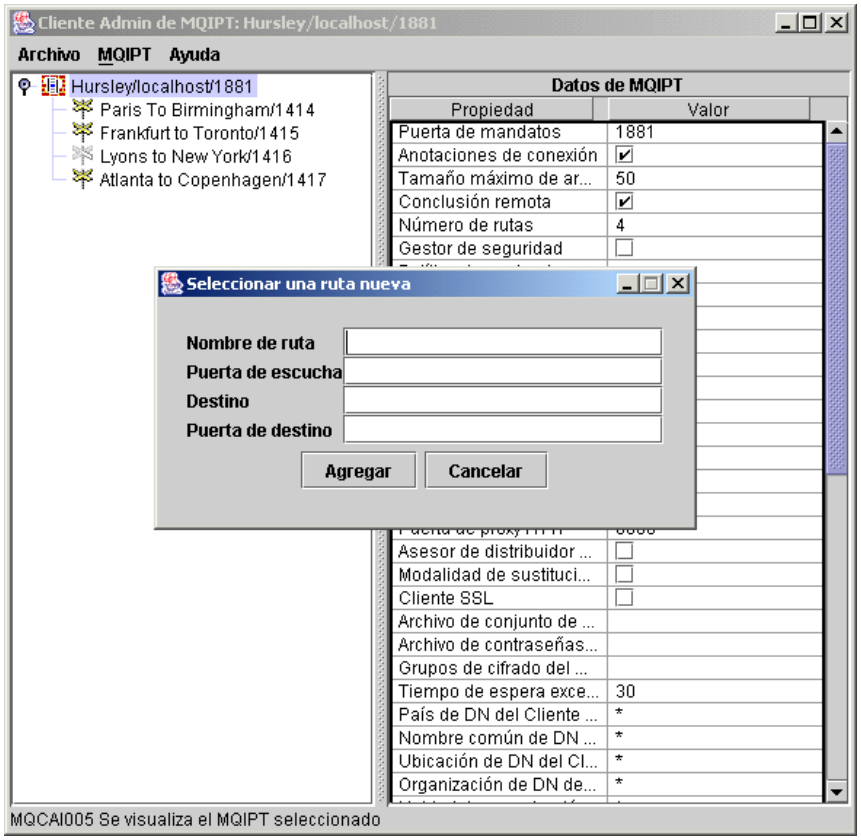

Figura 9. Adición de una ruta

Eliminar ruta
Suprime la ruta seleccionada del MQIPT. La supresión no afecta al MQIPT hasta que se utiliza la opción de menú "Aplicar".

Aplicar
Cuando esté satisfecho con los cambios que ha realizado en la configuración del MQIPT, esta opción envía un archivo de configuración nuevo al MQIPT, que lo guarda. Los nuevos valores entran en vigor de forma inmediata.

Renovar
Lee el archivo de configuración del MQIPT seleccionado y renueva la pantalla.

Detener
Envía un mandato de detención al MQIPT para indicarle que detenga su ejecución. Después de este mandato, perderá el contacto con el MQIPT. Este mandato se ignora a menos que la propiedad RemoteShutdown esté activada.

Se puede actualizar la información de las rutas del mismo modo que la información global de MQIPT: Cuando cambie las propiedades de una ruta, tendrá que aplicar los cambios para que entren en vigor. Puede hacerlo seleccionando la opción de menú "MQIPT/Aplicar" o respondiendo ″Sí″ cuando se le pregunte si desea guardar la configuración.

Opciones del menú Ayuda

Ayuda
Utiliza Netscape para mostrar información sobre cómo utilizar el cliente de administración; seleccione ″Administración y configuración de internet pass-thru″ en el panel de la izquierda. Antes de utilizar el cliente de administración, debe descomprimir el archivo que se encuentra en el subdirectorio `<idioma>/html`.

Acerca de
Muestra una ventana con información acerca de la versión del cliente de administración.

Utilización de los mandatos de internet pass-thru en modalidad de línea de mandatos

Si decide que no desea utilizar el cliente de administración, puede utilizar la modalidad de línea de mandatos para administrar y configurar internet pass-thru.

Administración de internet pass-thru mediante la modalidad de línea de mandatos

Con el editor de texto que prefiera, cambie el archivo de configuración, `mqipt.conf`, de modo que se ajuste a sus requisitos. Consulte el apartado "Información de consulta relacionada con la configuración" en la página 54 para obtener una lista de las propiedades que puede modificar.

Si la sección global del archivo `mqipt.conf` especifica un valor para `CommandPort`, MQIPT escuchará en esta puerta los siguientes mandatos de administración ASCII:

```
mqiptAdmin -refresh {nombresistpral {puerta} }      envía el mandato refresh
mqiptAdmin -stop    {nombresistpral {puerta} }      envía el mandato stop
```

El script `mqiptAdmin` está en el subdirectorio `bin`.

Si no se proporciona, el nombre de sistema principal toma el valor por omisión de `localhost` y la puerta `1881`.

STOP
MQIPT cierra todas las conexiones, deja de escucha las conexiones de entrada y, después, sale. Con la opción de menú "MQIPT/Detener" del cliente de administración, se realiza la misma acción. Este mandato se ignora a menos que el archivo `mqipt.conf` especifique `RemoteShutDown=true`.

REFRESH
MQIPT vuelve a leer `mqipt.conf`. Si encuentra que:

- Hay rutas activas en este momento que ahora están marcadas como inactivas (o ya no figuran en el archivo), las cierra y deja de escuchar las conexiones de entrada de esas rutas.
- Hay rutas marcadas como activas que no están ejecutándose en este momento, las inicia.
- Hay parámetros de configuración de una ruta que está ejecutándose en este momento que se han modificado, aplica los valores modificados a dichas rutas. Siempre que es posible, (por ejemplo, cuando se realiza un cambio en el valor del rastreo), efectúa la acción sin interrumpir las conexiones que están ejecutándose. Pero cuando se modifican algunos parámetros, por ejemplo, cuando se modifica un destino, MQIPT tiene que cerrar todas las conexiones y reiniciar la ruta para que el cambio surta efecto.

Con la opción de menú "MQIPT/Aplicar" del cliente de administración, se realiza la misma acción, siempre que cliente de administración no haya modificado ninguno de los valores de MQIPT.

En Windows, estas funciones de administración también están disponibles desde el menú Inicio -> Programas.

Información de consulta relacionada con la configuración

Si desea obtener información sobre cómo realizar algunas configuraciones sencillas, consulte el Capítulo 10, "Iniciación a internet pass-thru" en la página 67. Para consultar una configuración de ejemplo, vea el archivo `mqiptSample.conf` en el directorio inicial de MQIPT.

El archivo `mqipt.conf` consta de un conjunto de secciones. Hay una sección global y una sección adicional para cada ruta que se ha definido mediante MQIPT. En esta configuración sencilla, solamente hay una ruta, por lo tanto, el archivo contiene dos secciones, una sección global y una sección de ruta.

Cada sección contiene pares de propiedades de nombre/valor. Algunas propiedades pueden aparecer únicamente en las secciones globales, algunas pueden aparecer solamente en las secciones de rutas y otras pueden aparecer en ambas secciones. Si una propiedad no aparece ni en la sección de ruta ni en la sección global, el valor de la propiedad en la sección de la ruta reemplazará al valor de la sección global, pero solamente para esta ruta concreta. De este modo, se puede utilizar la sección global para establecer los valores por omisión que se han de utilizar para las propiedades que no se han establecido en las secciones de cada ruta individual.

La sección global comienza por una línea que contiene los caracteres `[global]` y finaliza cuando comienza la primera sección de ruta. La sección global debe ir antes que todas las secciones de ruta del archivo. Toda sección de ruta comienza

por una línea que contiene los caracteres [route] y acaba cuando comienza la siguiente sección de ruta o cuando se llega al final del archivo.

Se ignorará cualquier nombre de palabra clave no reconocido, es decir, cualquier par de nombre/valor cuyo nombre no sea uno de los nombres definidos en este documento. Si un par de nombre/valor que aparece en una sección de ruta tiene un nombre reconocido pero un valor que no es válido, por ejemplo, MinConnectionThreads=x o HTTP=unsure, se inhabilitará dicha ruta, esto es, no se escucharán las conexiones de entrada. Si aparece un par de nombre/valor en la sección global con un nombre reconocido y un valor no válido, se inhabilitarán todas las rutas y MQIPT no se iniciará. Cuando una propiedad figure con los valores true y false, se puede utilizar cualquier combinación de mayúsculas y minúsculas.

Resumen de las propiedades

En la Tabla 4 se muestra lo siguiente:

- Todas las propiedades.
- Si la propiedad se aplica a la sección global, a la sección de ruta o ambas secciones.
- Valores por omisión.

Si falta una propiedad en la sección de ruta y en la sección global, se utilizan los valores por omisión que se muestran en la tabla.

Tabla 4. Resumen de las propiedades de configuración

Nombre de la propiedad	Global	Ruta	Valor por omisión
AccessPW	yes		<null>
Active	yes	yes	true
ClientAccess	yes	yes	false
CommandPort	yes		<null>[1]
ConnectionLog	yes		true
Destination		yes	<null>
DestinationPort		yes	1414
HTTP[6,7]	yes	yes	false
HTTPChunking[1]	yes	yes	false
HTTPProxy[1]	yes	yes	<null>
HTTPProxyPort[1]	yes	yes	8080
IdleTimeout	yes	yes	0
ListenerPort		yes	<null>
LogDir (sólo es válido para MQIPTServlet)			<null>
MaxConnectionThreads	yes	yes	100
MaxLogFileSize	yes		50
MinConnectionThreads	yes	yes	5
Name		yes	<null>
NDAdvisor	yes	yes	false
NDAdvisorReplaceMode[4]	yes	yes	false
QMgrAccess	yes	yes	true

Tabla 4. Resumen de las propiedades de configuración (continuación)

Nombre de la propiedad	Global	Ruta	Valor por omisión
QoS (sólo puede utilizarse en Linux)	yes	yes	false
QosToCaller[9]	yes	yes	1
QosToDest[9]	yes	yes	1
RemoteShutdown	yes		false
SecurityManager	yes		false
SecurityManagerPolicy	yes		<null>
ServletClient[1]	yes	yes	false
SocksClient	yes	yes	false
SocksProxyHost[8]	yes	yes	<null>
SocksProxyPort[8]	yes	yes	1080
SocksServer[7]	yes	yes	false
SSLClient	yes	yes	false
SSLClientCipherSuites[2]	yes	yes	<null>
SSLClientConnectTimeout[2]	yes	yes	30
SSLClientDN_C[2]	yes	yes	*[5]
SSLClientDN_CN[2]	yes	yes	*[5]
SSLClientDN_L[2]	yes	yes	*[5]
SSLClientDN_O[2]	yes	yes	*[5]
SSLClientDN_OU[2]	yes	yes	*[5]
SSLClientDN_ST[2]	yes	yes	*[5]
SSLClientKeyRing[2]	yes	yes	<null>
SSLClientKeyRingPW[2]	yes	yes	<null>
SSLProxyMode	yes	yes	false
SSLServer[6]	yes	yes	false
SSLServerAskClientAuth[3]	yes	yes	false
SSLServerCipherSuites[3]	yes	yes	<null>
SSLServerDN_C[3]	yes	yes	*[5]
SSLServerDN_CN[3]	yes	yes	*[5]
SSLServerDN_L[3]	yes	yes	*[5]
SSLServerDN_O[3]	yes	yes	*[5]
SSLServerDN_OU[3]	yes	yes	*[5]
SSLServerDN_ST[3]	yes	yes	*[5]
SSLServerKeyRing[3]	yes	yes	<null>
SSLServerKeyRingPW[3]	yes	yes	<null>
Trace	yes	yes	0
UriName (consulte la página 65 para obtener información detallada acerca de los valores por omisión).[1]	yes	yes	

Notas:

1. Establezca HTTP en true para que estas propiedades surtan efecto.
2. Establezca SSLClient en true para que estas propiedades surtan efecto.
3. Establezca SSLServer en true para que estas propiedades surtan efecto.
4. Establezca NDAdvisor en true para que estas propiedades surtan efecto.
5. El símbolo "*" representa un comodín.
6. HTTP y SSLServer no se pueden utilizar juntos. La propiedad HTTP sólo se utiliza para definir la conexión de salida. Los datos de entrada en ListenerPort se detectan automáticamente, si se establece SSLServer se generará una excepción de tiempo de ejecución.
7. HTTP y SocksServer no se pueden utilizar juntos. La propiedad HTTP sólo se utiliza para definir la conexión de salida. Los datos de entrada en ListenerPort se detectan automáticamente, si se establece SocksServer se generará una excepción de tiempo de ejecución.
8. Establezca SocksClient en true para que estas propiedades surtan efecto.
9. Establezca QoS en true para que estas propiedades surtan efecto.

Información de consulta relacionada con la sección global

La sección global puede contener las propiedades siguientes y todas las propiedades del apartado "Información de consulta relacionada con la sección de ruta" en la página 58, a excepción de ListenerPort, Destination, DestinationPort y Name.

AccessPW
La contraseña que se utiliza cuando el controlador de administración envía mandatos a MQIPT. Si no existe esta propiedad o si se establece en blanco, no se lleva a cabo ninguna comprobación.

CommandPort
La puerta TCP/IP en que MQIPT escucha los mandatos de configuración del programa de utilidad `mqiptAdmin` o del cliente de administración. Puede cambiar la puerta de mandatos del cliente de administración del mismo modo que cualquier otra propiedad. Tenga en cuenta que no modifica las propiedades de la conexión. Cuando aplica la configuración nueva a MQIPT, el cliente de administración modifica automáticamente las propiedades de la conexión.

Si la propiedad `CommandPort` no está presente, MQIPT no escuchará los mandatos de configuración. Si desea que la escucha se realice en la puerta de mandatos, se le aconseja que utilice 1881. El cliente de administración no tiene un valor por omisión para CommandPort, pero 1881 es el valor por omisión cuando se utiliza la modalidad de línea de mandatos.

ConnectionLog
Puede ser `true` o `false`. Cuando es true, MQIPT anota cronológicamente todos los intentos de conexión (satisfactorios o no) en el subdirectorio `logs` y los sucesos de desconexión en el archivo `mqiptAAAAMMDDHHmmSS.log`. El valor por omisión es true. Cuando se modifica esta propiedad de `true` a `false`, MQIPT cierra el archivo de anotaciones actual y crea uno nuevo. Este nuevo es el que se utilizará cuando se vuelva a establecer la propiedad en `true`.

MaxLogFileSize
El tamaño máximo (especificado en KB) del archivo de anotaciones de conexión `mqipt.log`. Cuando se aumenta el tamaño del archivo `mqipt.log` por encima de este valor máximo, se crea una copia de seguridad `mqipt.back` y se inicia un nuevo archivo. Solamente se mantiene un archivo de copia de

seguridad. Cada vez que el archivo de anotaciones principal alcanza el valor máximo, las copias de seguridad anteriores se borran. El valor por omisión es 50, el valor mínimo permitido es 5.

RemoteShutDown
Puede ser `true` o `false`. Cuando se establece en true (y cuando existe una puerta de mandatos) MQIPT concluirá cada vez que se reciba un mandato STOP en la puerta de mandatos. El valor por omisión es false.

SecurityManager
Establezca esta propiedad en true para habilitar Java Security Manager para esta instancia de MQIPT. Para ello es necesario que se hayan otorgado los permisos correctos. Consulte el apartado "Java Security Manager" en la página 22 para obtener más información. El valor por omisión de esta propiedad es false.

SecurityManagerPolicy
El nombre de archivo totalmente calificado de un archivo de políticas. Si esta propiedad no se establece, solamente se utilizan los archivos de políticas de usuario y del sistema por omisión. Si Java Security Manager ya está habilitado, las modificaciones que se realicen en esta propiedad no surtirán efecto hasta que se inhabilite y se vuelva a habilitar Java Security Manager.

Información de consulta relacionada con la sección de ruta

La sección de ruta puede contener las propiedades siguientes:

Active
La ruta acepta las conexiones de entrada solamente si Active se establece en `true`. Esto significa que puede cerrar el acceso al destino de forma temporal estableciendo `Active=false`, sin tener que suprimir la sección de ruta del archivo de configuración. Si cambia esta propiedad a `false`, la ruta se detendrá cuando se emita un mandato REFRESH. Todas las conexiones a esta ruta finalizarán.

ClientAccess
La ruta acepta conexiones de entrada de canales de clientes solamente si se establece ClientAccess en `true`. Tenga en cuenta que potencialmente puede configurar los MQIPT para que acepten solamente peticiones de clientes, peticiones de gestores de colas o ambos tipos de peticiones. Utilice esta propiedad junto con la propiedad QMgrAccess. Si cambia esta propiedad a `false`, la ruta se detendrá y se reiniciará cuando se emita el mandato REFRESH. Todas las conexiones a esta ruta finalizarán.

Destination
El nombre de sistema principal (o una dirección IP decimal con puntos) del gestor de colas (o MQIPT posterior) al que se ha de conectar esta ruta. Toda sección de ruta **debe** contener un valor explícito para Destination. Se pueden tener varias secciones de rutas que apunten al mismo Destination. Si un cambio en esta propiedad afecta a una ruta, ésta se detendrá y se reiniciará cuando se emita el mandato REFRESH. Todas las conexiones a esta ruta finalizarán.

DestinationPort
La puerta del sistema principal especificado en Destination a la que se conectará esta ruta. Más de una ruta pueden apuntar a la misma combinación de Destination y DestinationPort. Toda sección de ruta **debe** contener un valor explícito para DestinationPort. Si un cambio en esta propiedad afecta a una ruta, ésta se detendrá y se reiniciará cuando se emita el mandato REFRESH. Todas las conexiones a esta ruta finalizarán.

HTTP
Establezca esta propiedad en `true` para las rutas que deben realizar las peticiones de túnel HTTP de salida (es decir, que se comunican con otro MQIPT a través de HTTP). Establézcala en `false` para las rutas dirigidas a los gestores de colas de WebSphere MQ. Si cambia esta propiedad a `false`, la ruta se detendrá y se reiniciará cuando se emita el mandato REFRESH. Todas las conexiones a esta ruta finalizarán. Para utilizar la fragmentación HTTP, establezca esta propiedad en `true`. Esta propiedad no se puede utilizar con:

- QoS
- SocksClient
- SSLClient
- SSLProxyMode

HTTPChunking
Establezca esta propiedad en `true` para las rutas que deben realizar las peticiones de salida utilizando la función de túnel HTTP con fragmentación. La propiedad HTTP también debe establecerse en `true`. Establezca la propiedad en `false` cuando no utilice la fragmentación HTTP. Si cambia esta propiedad a `false`, la ruta se detendrá y se reiniciará cuando se emita el mandato REFRESH. Todas las conexiones a esta ruta finalizarán.

HTTPProxy
El nombre de sistema principal (o una dirección IP decimal con puntos) del proxy HTTP que utilizarán todas las conexiones a esta ruta. Si cambia esta propiedad, la ruta se detendrá y se reiniciará cuando se emita el mandato REFRESH. Todas las conexiones a esta ruta finalizarán.

HTTPProxyPort
La dirección de la puerta que se ha de utilizar en el proxy HTTP. El valor por omisión es `8080`. Si cambia esta propiedad, la ruta se detendrá y se reiniciará cuando se emita el mandato REFRESH. Todas las conexiones a esta ruta finalizarán.

IdleTimeout
La hora, en minutos, después de la cual se cerrará una conexión que esté desocupada. Tenga en cuenta que los canales de gestor de colas a gestor de colas también tienen la propiedad DISCINT. Si establece el parámetro IdleTimeout, tome nota de la propiedad DISCINT. Si el valor es 0 significa que no hay un tiempo excedido de conexión desocupada. Los cambios en esta propiedad surten efecto solamente cuando se reinicia la ruta.

ListenerPort
El número de puerta en la que la ruta debe escuchar las peticiones de entrada. Toda sección de ruta **debe** contener un valor explícito para ListenerPort y además, los valores de ListenerPort que se establezcan en cada sección deben ser diferentes. Se puede utilizar cualquier número de puerta válida, incluidas las puertas 80 y 443, siempre que las puertas seleccionadas no estén siendo utilizadas por otro escucha TCP/IP que se ejecute en el mismo sistema principal.

LogDir
Utilice esta propiedad para definir el nombre de directorio para los archivos de anotaciones y de rastreo. Los cambios que se realicen en esta propiedad no surtirán efecto hasta que se haya detenido y reiniciado MQIPTServlet. El valor por omisión es <null>. Esta propiedad sólo es válida para MQIPTServlet.

MaxConnectionThreads
El número máximo de hebras de conexión y, por lo tanto, el número máximo

de conexiones simultáneas que puede manejar esta ruta. Si se alcanza este límite, el valor de `MaxConnectionThreads` también indica el número de conexiones que se pondrán en cola cuando estén utilizándose todas las hebras. Superado este número, se rechazarán las peticiones de conexión posteriores. El valor mínimo permitido es mayor que 1 o el valor de MinConnectionThreads. Si un cambio en esta propiedad afecta a una ruta, se utilizará el nuevo valor cuando se emita el mandato REFRESH. Todas las conexiones adoptarán el nuevo valor de forma inmediata. La ruta no se finalizará.

MinConnectionThreads
El número mínimo de hebras de conexión (las hebras que manejan las conexiones de entrada de esta ruta). Este es el número de hebras que se asigna cuando se inicia la ruta y el número total de hebras asignado no queda por debajo de este valor mientras la ruta está activa. El valor mínimo permitido es 0 y debe ser menor que el especificado para MaxConnectionThreads. Los cambios en esta propiedad surten efecto solamente cuando se reinicia la ruta.

Name
Un nombre opcional que sirve para identificar la ruta. Aparece en los mensajes de la consola y en la información de rastreo. Los cambios en esta propiedad surten efecto solamente cuando se reinicia la ruta.

NDAdvisor
Establezca esta propiedad en `true` para las rutas gestionadas por Network Dispatcher para que puedan responder a las peticiones procedentes del asesor personalizado. Si cambia esta propiedad a `false`, la ruta se detendrá cuando se emita un mandato REFRESH. Todas las conexiones a esta ruta finalizarán. Para utilizar la propiedad NDAdvisorReplaceMode, establezca esta propiedad en `true`.

NDAdvisorReplaceMode
Establezca esta propiedad en `true` para utilizar la modalidad de sustitución (“replace”) del asesor de Network Dispatcher personalizado. Deberá haber iniciado el asesor personalizado `mqipt_replace` en la dirección ListenerPort de esta ruta. Establezca esta propiedad en `false` para utilizar la modalidad “normal”. Para poder utilizar esta propiedad, debe establecer la propiedad NDAdvisor en `true`.

QMgrAccess
La ruta permite conexiones de entrada del canal del gestor de colas (por ejemplo, de canales emisores) solamente si se establece el valor QMgrAccess en `true`. Si cambia esta propiedad a `false`, la ruta se detendrá cuando se emita un mandato REFRESH. Todas las conexiones a esta ruta finalizarán.

QoS
Establezca esta propiedad en `true` para habilitar la calidad de servicio (Quality of Service) para todas las conexiones de esta ruta. Esta propiedad solamente se puede habilitar en Linux. Si cambia esta propiedad, la ruta se detendrá y se reiniciará cuando se emita el mandato REFRESH. Todas las conexiones a esta ruta finalizarán. Esta propiedad no se puede utilizar con:

- HTTP
- SSLClient
- SSLProxyMode
- SSLServer

QosToCaller
Esta propiedad establece la prioridad de todo el tráfico procedente de la máquina de MQIPT al iniciador de la conexión. Establezca la propiedad en 1

para prioridad baja, 2 para prioridad media y 3 para prioridad alta (el valor por omisión es 1). Si cambia esta propiedad (y QoS se establece en true), la ruta se detendrá y se reiniciará cuando se emita el mandato REFRESH. Todas las conexiones a esta ruta finalizarán.

QosToDest
Esta propiedad establece la prioridad de todo el tráfico de la máquina MQIPT al destino de la conexión (que se ha definido mediante la propiedad Destination). Establezca la propiedad en 1 para prioridad baja, 2 para prioridad media y 3 para prioridad alta (el valor por omisión es 1). Si cambia esta propiedad (y QoS se establece en true), la ruta se detendrá y se reiniciará cuando se emita el mandato REFRESH. Todas las conexiones a esta ruta finalizarán.

ServletClient
Establezca esta propiedad en true cuando se conecte al servlet MQIPT. La propiedad HTTP también debe establecerse en true. Si cambia esta propiedad (y HTTP se establece en true), la ruta se detendrá y se reiniciará cuando se emita el mandato REFRESH.

SocksClient
Establezca esta propiedad en true para que la ruta actúe como un cliente Socks y defina todas las conexiones que se realizarán a través del proxy Socks con las propiedades SocksProxyHost y SocksProxyPort. Si cambia esta propiedad, la ruta se detendrá y se reiniciará cuando se emita el mandato REFRESH. Todas las conexiones a esta ruta finalizarán. Esta propiedad no se puede utilizar con:

- HTTP
- SocksServer
- SSLClient
- SSLProxyMode

SocksProxyHost
El nombre de sistema principal (o una dirección IP decimal con puntos) del proxy Socks que utilizarán todas las conexiones de esta ruta. Si cambia esta propiedad (y SocksClient se establece en true), la ruta se detendrá y se reiniciará cuando se emita el mandato REFRESH. Todas las conexiones a esta ruta finalizarán.

SocksProxyPort
La dirección de la puerta que se ha de utilizar en un proxy Socks. El valor por omisión es 1080. Si cambia esta propiedad (y SocksClient se establece en true), la ruta se detendrá y se reiniciará cuando se emita el mandato REFRESH. Todas las conexiones a esta ruta finalizarán.

SocksServer
Establezca esta propiedad en true para que la ruta actúe como un cliente Socks y acepte todas las conexiones de clientes Socks. Si cambia esta propiedad, la ruta se detendrá y se reiniciará cuando se emita el mandato REFRESH. Todas las conexiones a esta ruta finalizarán. Esta propiedad no se puede utilizar con:

- SocksClient
- SSLProxyMode
- SSLServer

SSLClient
Establezca esta propiedad en true para que la ruta actúe como un cliente SSL y acepte todas las conexiones de salida de clientes Socks. Si la establece en true el destino será otro MQIPT que actúa como un servidor SSL. Si cambia esta

propiedad, la ruta se detendrá y se reiniciará cuando se emita el mandato REFRESH. Todas las conexiones a esta ruta finalizarán. Esta propiedad no se puede utilizar con:

- HTTP
- QoS
- SSLProxyMode

SSLClientCipherSuites
El nombre de la suite de cifrado SSL que se ha de utilizar en el extremo del cliente SSL. Pueden ser una o varias suites de cifrado soportadas. Si deja en blanco este campo, el cliente SSL utiliza las suites de cifrado soportadas de SSLClientKeyRing. Si cambia esta propiedad, la ruta se detendrá y se reiniciará cuando se emita el mandato REFRESH. Todas las conexiones a esta ruta finalizarán.

SSLClientConnectTimeout
Establezca esta propiedad en el número de segundos que esperará un cliente SSL a que se acepte una conexión SSL. Si un cambio en esta propiedad afecta a una ruta, se utilizará el nuevo valor cuando se emita el mandato REFRESH. La ruta no se finalizará.

SSLClientDN_C
Utilice esta propiedad para aceptar los certificados recibidos del servidor SSL de este país. El nombre puede tener un asterisco (*) como prefijo o sufijo para ampliar su ámbito. Si no especifica esta propiedad, se presuponen “todos los nombres de empresa”. Si cambia esta propiedad, la ruta se detendrá y se reiniciará cuando se emita el mandato REFRESH. Todas las conexiones a esta ruta finalizarán.

SSLClientDN_CN
Utilice esta propiedad para aceptar los certificados recibidos del servidor SSL de este nombre común. El nombre puede tener un asterisco (*) como prefijo o sufijo para ampliar su ámbito. Si no especifica esta propiedad, se presuponen “todos los nombres comunes”. Si cambia esta propiedad, la ruta se detendrá y se reiniciará cuando se emita el mandato REFRESH. Todas las conexiones a esta ruta finalizarán.

SSLClientDN_L
Utilice esta propiedad para aceptar los certificados recibidos del servidor SSL de esta ubicación. El nombre puede tener un asterisco (*) como prefijo o sufijo para ampliar su ámbito. Si no especifica esta propiedad, se presuponen “todas las ubicaciones”. Si cambia esta propiedad, la ruta se detendrá y se reiniciará cuando se emita el mandato REFRESH. Todas las conexiones a esta ruta finalizarán.

SSLClientDN_O
Utilice esta propiedad para aceptar los certificados recibidos del servidor SSL de esta organización. El nombre puede tener un asterisco (*) como prefijo o sufijo para ampliar su ámbito. Si no especifica esta propiedad, se presuponen “todas las organizaciones”. Si cambia esta propiedad, la ruta se detendrá y se reiniciará cuando se emita el mandato REFRESH. Todas las conexiones a esta ruta finalizarán.

SSLClientDN_OU
Utilice esta propiedad para aceptar los certificados recibidos del servidor SSL de este nivel de organización. El nombre puede tener un asterisco (*) como prefijo o sufijo para ampliar su ámbito. Si no especifica esta propiedad, se

presuponen “todas las unidades organizativas”. Si cambia esta propiedad, la ruta se detendrá y se reiniciará cuando se emita el mandato REFRESH. Todas las conexiones a esta ruta finalizarán.

SSLClientDN_ST
Utilice esta propiedad para aceptar los certificados recibidos del servidor SSL de este estado. El nombre puede tener un asterisco (*) como prefijo o sufijo para ampliar su ámbito. Si no especifica esta propiedad, se presuponen “todos los estados”. Si cambia esta propiedad, la ruta se detendrá y se reiniciará cuando se emita el mandato REFRESH. Todas las conexiones a esta ruta finalizarán.

SSLClientKeyRing
El nombre de archivo totalmente calificado del archivo que contiene el certificado de cliente. En las plataformas **Windows**, debe utilizar una barra doble invertida (\\) como separador de archivos. Debe especificar SSLClientKeyRing si establece SSLClient en `true`. Si cambia esta propiedad, la ruta se detendrá y se reiniciará cuando se emita el mandato REFRESH. Todas las conexiones a esta ruta finalizarán.

SSLClientKeyRingPW
El nombre de archivo totalmente calificado que contiene la contraseña para abrir el conjunto de claves. En las plataformas **Windows**, debe utilizar una barra doble invertida (\\) como separador de archivos. Debe especificar SSLClientKeyRingPW si establece SSLClient en `true`. Si cambia esta propiedad, la ruta se detendrá y se reiniciará cuando se emita el mandato REFRESH. Todas las conexiones a esta ruta finalizarán.

SSLProxyMode
Establezca esta propiedad en `true` para habilitar la ruta de modo que sólo acepte peticiones de conexión de clientes SSL y dirija la petición, mediante la función de túnel, directamente al destino. Si cambia esta propiedad, la ruta se detendrá y se reiniciará cuando se emita el mandato REFRESH. Todas las conexiones a esta ruta finalizarán. Esta propiedad no se puede utilizar con:

- HTTP
- QoS
- SocksClient
- SSLClient
- SSLServer

SSLServer
Establezca esta propiedad en `true` para que la ruta actúe como un servidor SSL y acepte todas las conexiones SSL de entrada. Si la establece en `true`, el que solicita la conexión de entrada será otro MQIPT que actúa como un cliente SSL. Si cambia esta propiedad, la ruta se detendrá y se reiniciará cuando se emita el mandato REFRESH. Todas las conexiones a esta ruta finalizarán. Esta propiedad no se puede utilizar con:

- QoS
- SocksServer
- SSLProxyMode

SSLServerAskClientAuth
Utilice esta propiedad para que el servidor SSL solicite la autenticación de los clientes SSL. El cliente SSL deberá tener su propio certificado para enviarlo al servidor SSL. El certificado se recupera del archivo de conjunto de claves. Si cambia esta propiedad, la ruta se detendrá y se reiniciará cuando se emita el mandato REFRESH. Todas las conexiones a esta ruta finalizarán.

SSLServerCipherSuites
El nombre de la suite de cifrado SSL que se ha de utilizar en el extremo del servidor SSL. Pueden ser una o varias suites de cifrado soportadas. Si deja en blanco este campo, el servidor SSL utiliza las suites de cifrado soportadas de SSLServerKeyRing. Si cambia esta propiedad, la ruta se detendrá y se reiniciará cuando se emita el mandato REFRESH. Todas las conexiones a esta ruta finalizarán.

SSLServerDN_C
Utilice esta propiedad para aceptar los certificados recibidos del cliente SSL de este país. El nombre puede tener un asterisco (*) como prefijo o sufijo para ampliar su ámbito. Si no especifica esta propiedad, se presuponen "todos los nombres de empresa". Si cambia esta propiedad, la ruta se detendrá y se reiniciará cuando se emita el mandato REFRESH. Todas las conexiones a esta ruta finalizarán.

SSLServerDN_CN
Utilice esta propiedad para aceptar los certificados recibidos del cliente SSL de este nombre común. El nombre puede tener un asterisco (*) como prefijo o sufijo para ampliar su ámbito. Si no especifica esta propiedad, se presuponen "todos los nombres comunes". Si cambia esta propiedad, la ruta se detendrá y se reiniciará cuando se emita el mandato REFRESH. Todas las conexiones a esta ruta finalizarán.

SSLServerDN_L
Utilice esta propiedad para aceptar los certificados recibidos del cliente SSL de esta ubicación. El nombre puede tener un asterisco (*) como prefijo o sufijo para ampliar su ámbito. Si no especifica esta propiedad, se presuponen "todas las ubicaciones". Si cambia esta propiedad, la ruta se detendrá y se reiniciará cuando se emita el mandato REFRESH. Todas las conexiones a esta ruta finalizarán.

SSLServerDN_O
Utilice esta propiedad para aceptar los certificados recibidos del cliente SSL de esta organización. El nombre puede tener un asterisco (*) como prefijo o sufijo para ampliar su ámbito. Si no especifica esta propiedad, se presuponen "todas las organizaciones". Si cambia esta propiedad, la ruta se detendrá y se reiniciará cuando se emita el mandato REFRESH. Todas las conexiones a esta ruta finalizarán.

SSLServerDN_OU
Utilice esta propiedad para aceptar los certificados recibidos del cliente SSL de esta unidad de organización. El nombre puede tener un asterisco (*) como prefijo o sufijo para ampliar su ámbito. Si no especifica esta propiedad, se presuponen "todas las unidades organizativas". Si cambia esta propiedad, la ruta se detendrá y se reiniciará cuando se emita el mandato REFRESH. Todas las conexiones a esta ruta finalizarán.

SSLServerDN_ST
Utilice esta propiedad para aceptar los certificados recibidos del cliente SSL de este estado. El nombre puede tener un asterisco (*) como prefijo o sufijo para ampliar su ámbito. Si no especifica esta propiedad, se presuponen "todos los estados". Si cambia esta propiedad, la ruta se detendrá y se reiniciará cuando se emita el mandato REFRESH. Todas las conexiones a esta ruta finalizarán.

SSLServerKeyRing
El nombre de archivo totalmente calificado del archivo que contiene el certificado del servidor. En las plataformas **Windows**, debe utilizar una barra doble invertida (\\) como separador de archivos. Debe especificar

SSLServerKeyRing si establece SSLServer en `true`. Si cambia esta propiedad, la ruta se detendrá y se reiniciará cuando se emita el mandato REFRESH. Todas las conexiones a esta ruta finalizarán.

SSLServerKeyRingPW
El nombre de archivo totalmente calificado que contiene la contraseña para abrir el conjunto de claves del servidor. En las plataformas **Windows**, debe utilizar una barra doble invertida (`\\`) como separador de archivos. Debe especificar SSLServerKeyRingPW si establece SSLServer en `true`. Si cambia esta propiedad, la ruta se detendrá y se reiniciará cuando se emita el mandato REFRESH. Todas las conexiones a esta ruta finalizarán.

Trace
El nivel de rastreo necesario se puede especificar mediante un entero de 0 a 5. Si el valor es 0 significa que se realizará el rastreo y si es 5 el rastreo será completo.

Si un cambio en esta propiedad afecta a una ruta, se utilizará el nuevo valor cuando se emita el mandato REFRESH. Todas las conexiones adoptarán el nuevo valor de forma inmediata. La ruta no se finalizará.

UriName
Esta propiedad se puede utilizar para cambiar el nombre del URI (Uniform Resource Identifier) del recurso cuando se utiliza un proxy HTTP o el servlet MQIPT, aunque los valores por omisión serán suficientes para la mayor parte de las configuraciones. El valor por omisión para el proxy HTTP es:

```
HTTP://<destino>:<puerta_destino>/mqipt
```

El valor por omisión para el servlet MQIPT es:

```
HTTP://<destino>:<puerta_destino>/MQIPTServlet
```

Si cambia esta propiedad y HTTP o ServletClient se establecen en `true`, la ruta se detendrá y se reiniciará cuando se emita el mandato REFRESH.

Capítulo 10. Iniciación a internet pass-thru

En este capítulo le iniciaremos en la utilización de MQIPT; le indicaremos cómo realizar algunas configuraciones sencillas que le permitan confirmar que el producto se ha instalado correctamente.

Este capítulo tiene los apartados siguientes:

Supuestos

Para cada ejemplo, se presupone lo siguiente:

- Está utilizando Windows NT, (aunque estos ejemplos se pueden ejecutar en cualquiera de las plataformas soportadas).
- Sabe cómo definir gestores de colas, colas y canales en WebSphere MQ.
- Ya tiene instalado un cliente y un servidor de WebSphere MQ.
- MQIPT está instalado en un directorio llamado `C:\mqipt` (en Windows).
- El cliente, el servidor y cada MQIPT están instalados en máquinas diferentes.
- Sabe colocar mensajes en una cola utilizando el mandato `amqsputc`.
- Sabe obtener mensajes de una cola utilizando el mandato `amqsgetc`.

En el servidor de WebSphere MQ ha realizado lo siguiente:

- Ha definido un gestor de colas llamado `MQIPT.QM1`.
- Ha definido un canal de conexión de servidor llamado `MQIPT.CONN.CHANNEL`.
- Ha definido una cola local llamada `MQIPT.LOCAL.QUEUE`.
- Ha iniciado un escucha TCP/IP para `MQIPT.QM1` en la puerta 1414.

Solamente una aplicación puede escuchar en una dirección de puerta determinada en la misma máquina. Si la puerta 1414 ya está utilizándose, seleccione una dirección de puerta que esté libre y sustitúyala en los ejemplos

© Copyright IBM Corp. 2000-2002

Cuando haya realizado esto, puede probar la ruta desde el cliente de WebSphere MQ al gestor de colas, colocando un mensaje en la cola local del gestor de colas mediante el mandato `amqsputc` y recuperándolo con el mandato `amqsgetc`.

Configuraciones de ejemplo

Los ejemplos siguientes se representan como diagramas e instrucciones paso a paso. Puede utilizar los recuadros de selección que hay a la derecha de cada diagrama para ver de qué modo progresa por el ejemplo. En algunos ejemplos se le solicitará que edite el archivo `mqipt.conf`, que encontrará en el directorio inicial de MQIPT.

Antes de comenzar, asegúrese de que:

- Ha copiado `mqiptSample.conf` en `mqipt.conf`
- Ha editado `mqipt.conf` y suprimido todas las rutas
- Ha cambiado la entrada de `ClientAccess` por `true`
- Ha cambiado el destino de `mqserver.company2.com` por el de su gestor de colas
- Ha cambiado la dirección de DestinationPort por la que utiliza su gestor de colas
- Ha leído el apartado “Supuestos” en la página 67

Prueba de verificación de la instalación

Ésta es una configuración sencilla que le permite asegurarse de que MQIPT se ha instalado correctamente.

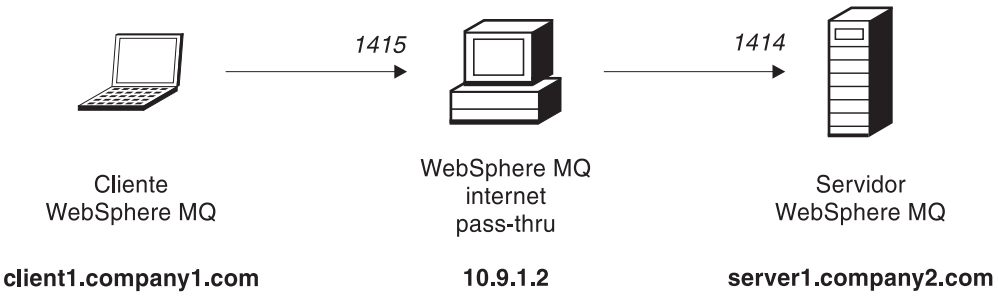

Figura 10. Diagrama de la red IVT

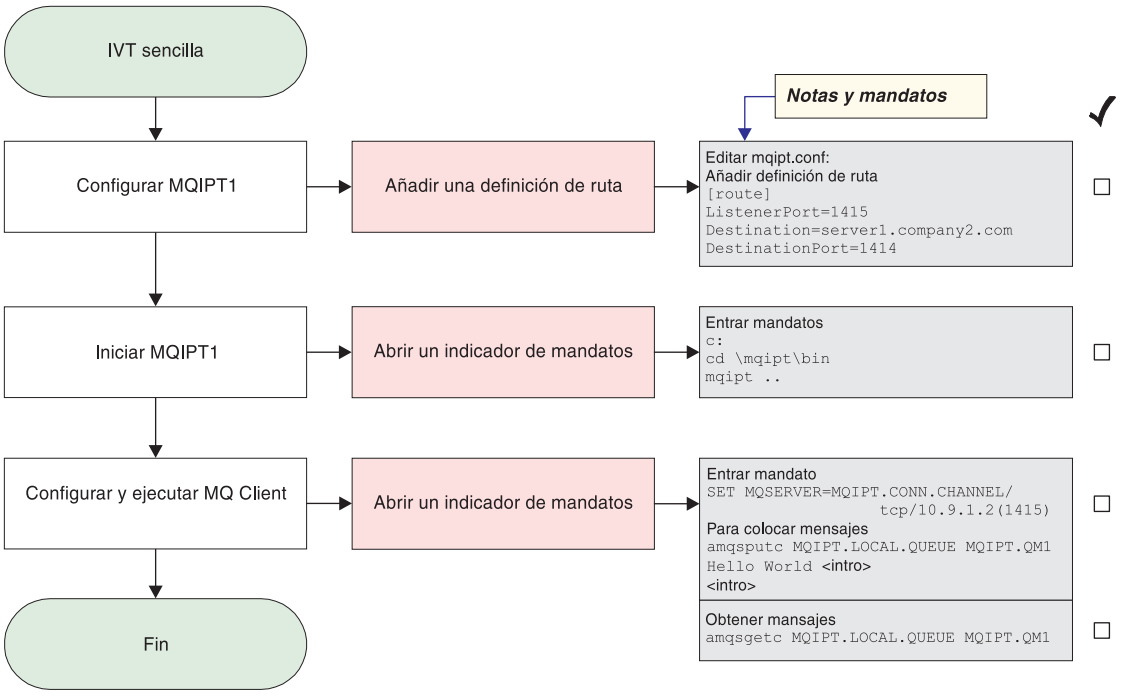

Figura 11. Configuración de IVT

Antes de comenzar:

1. Configure MQIPT1.

   Edite el archivo `mqipt.conf` y añada una definición de ruta:

   ```
   [route]
   ListenerPort=1415
   Destination=server1.company2.com
   DestinationPort=1414
   ```

2. Inicie MQIPT1.

   Abra un indicador de mandatos y escriba lo siguiente:

   ```
   c:
   cd \mqipt\bin
   mqipt ..
   ```

   El mensaje siguiente indica que se ha realizado correctamente:

   ```
   5639-L92 (C) Copyright IBM Corp. 2000-2002 All Rights Reserved
   MQCPI001 WebSphere MQ internet pass-thru Version 1.2 starting
   MQCPI004 Reading configuration information from C:\mqipt\mqipt.conf
   MQCPI011 The path C:\mqipt\logs will be used to store the log files
   MQCPI006 Route 1415 has started and will forward messages to :
   MQCPI034 ....server1.company2.com(1414)
   MQCPI035 ....using MQ protocols
   ```

3. En un indicador de mandatos de la máquina cliente de WebSphere MQ, escriba lo siguiente:

   ```
   SET MQSERVER=MQIPT.CONN.CHANNEL/tcp/10.9.1.2(1415)
   ```

4. Coloque un mensaje mediante el mandato siguiente:

   ```
   amqsputc MQIPT.LOCAL.QUEUE MQIPT1.QM1
   Hola amigos <Intro>
    <Intro>
   ```

5. Obtenga el mensaje mediante el mandato siguiente:

   ```
   amqsgetc MQIPT.LOCAL.QUEUE MQIPT1.QM1
   ```

Verá el texto ″Hola amigos″.

Autenticación del servidor SSL

En este ejemplo comprobará una conexión SSL utilizando el certificado de prueba de ejemplo (el archivo de conjunto de claves `sslsample.pfx`) conectando un cliente de WebSphere MQ a un servidor de WebSphere MQ mediante dos MQIPT. Durante el reconocimiento SSL, el servidor enviará su certificado de prueba al cliente. El cliente utilizará su copia del certificado (con el distintivo ″trust-as-peer″) para autenticar al servidor. Se utilizará una suite de cifrado por omisión, SSL_RSA_WITH_RC4_128_MD5. (En base al archivo `mqipt.conf` creado en el apartado “Prueba de verificación de la instalación” en la página 68.) Para obtener información detallada sobre cómo crear un certificado de prueba para utilizarlo en este ejemplo, consulte el apartado “Creación de certificados de prueba SSL” en la página 89.

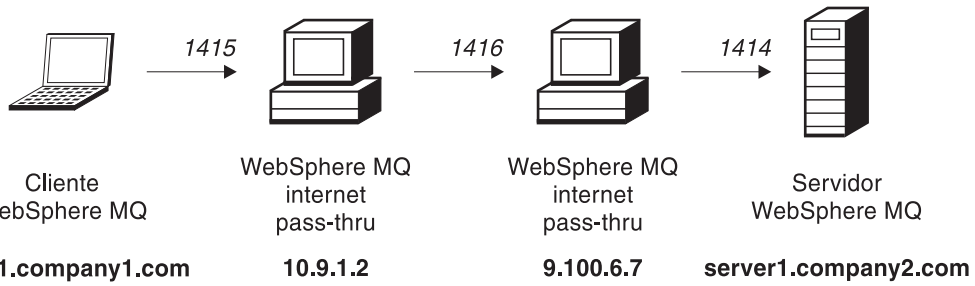

Figura 12. Diagrama de red del servidor SSL

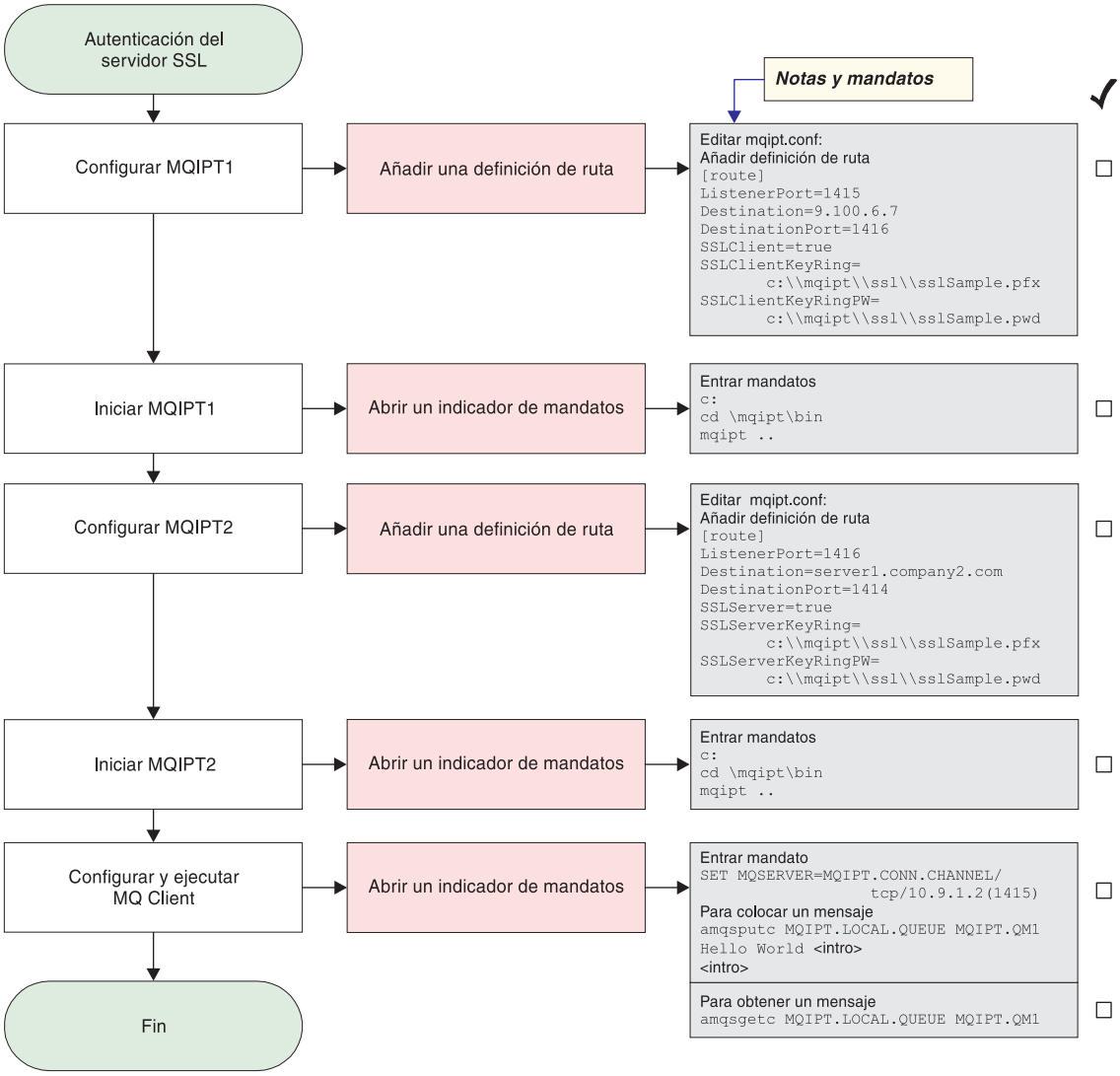

Figura 13. Autenticación del servidor SSL

1. Configure MQIPT1.

   Edite el archivo `mqipt.conf` y añada una definición de ruta:

   ```
   [route]
   ListenerPort=1415
   Destination=9.100.6.7
   DestinationPort=1416
   SSLClient=true
   SSLClientKeyRing=C:\\mqipt\\sslSample.pfx
   SSLClientKeyRingPW=C:\\mqipt\\sslSample.pwd
   ```

2. Inicie MQIPT1.

   Abra un indicador de mandatos y escriba lo siguiente:

   ```
   c:
   cd \mqipt\bin
   mqipt ..
   ```

   El mensaje siguiente indica que se ha realizado correctamente:

   ```
   5639-L92 (C) Copyright IBM Corp. 2000-2002 All Rights Reserved
   MQCPI001 WebSphere MQ internet pass-thru Version 1.2 starting
   MQCPI011 The path c:\mqipt\logs will be used to store the log files
   MQCPI006 Route 1415 has started and will forward messages to :
   ```

```
MQCPI034 ....9.100.6.7(1416)
MQCPI035 ....using MQ protocols
MQCPI036 ....SSL Client side enabled with properties :
MQCPI031 ......cipher suites <null>
MQCPI032 ......keyring file c:\mqipt\sslSample.pfx
MQCPI047 ......CA keyring file <null>
MQCPI038 ......distinguished name(s) CN=* O=* OU=* L=* ST=* C=*
```

3. Configure MQIPT2.

   Edite el archivo `mqipt.conf` y añada una definición de ruta:

   ```
   [route]
   ListenerPort=1416
   Destination=Server1.company2.com
   DestinationPort=1414
   SSLClient=true
   SSLServerKeyRing=C:\\mqipt\\sslSample.pfx
   SSLServerKeyRingPW=C:\\mqipt\\sslSample.pwd
   ```

4. Inicie MQIPT2.

   Abra un indicador de mandatos y escriba lo siguiente:

   ```
   c:
   cd \mqipt\bin
   mqipt
   ```

   El mensaje siguiente indica que se ha realizado correctamente:

   ```
   5639-L92 (C) Copyright IBM Corp. 2000-2002 All Rights Reserved
   MQCPI001 WebSphere MQ internet pass-thru Version 1.2 starting
   MQCPI011 The path c:\mqipt\logs will be used to store the log files
   MQCPI006 Route 14196 has started and will forward messages to :
   MQCPI034 ....server1.company2.com(1414)
   MQCPI035 ....using MQ protocols
   MQCPI037 ....SSL Server side enabled with properties :
   MQCPI031 ......cipher suites <null>
   MQCPI032 ......keyring file c:\mqipt\sslSample.pfx
   MQCPI047 ......CA keyring file <null>
   MQCPI038 ......distinguished name(s) CN=* O=* OU=* L=* ST=* C=*
   MQCPI033 ......client authentication set to false
   ```

5. En un indicador de mandatos de la máquina cliente de WebSphere MQ, escriba lo siguiente:

   ```
   SET MQSERVER=MQIPT.CONN.CHANNEL/tcp/10.9.1.2(1415)
   ```

6. Coloque un mensaje mediante el mandato siguiente:

   ```
   amqsputc MQIPT.LOCAL.QUEUE MQIPT1.QM1
   Hola amigos <Intro>
    <Intro>
   ```

7. Obtenga el mensaje mediante el mandato siguiente:

   ```
   amqsgetc MQIPT.LOCAL.QUEUE MQIPT1.QM1
   ```

Verá el texto ″Hola amigos″.

Autenticación del cliente SSL

En este ejemplo comprobará una conexión SSL utilizando el certificado de prueba de ejemplo. Se realizará una autenticación del servidor y del cliente. Durante el reconocimiento SSL, el servidor enviará su certificado de prueba al cliente. El cliente utilizará su copia del certificado, con el distintivo ″trust-as-peer″, para autenticar al servidor. A continuación, el cliente enviará su certificado de prueba al servidor. El servidor utilizará su copia del certificado, con el distintivo ″trust-as-peer″, para autenticar al cliente. Se utilizará una suite de cifrado por

omisión, SSL_RSA_WITH_RC4_128_MD5. (En base al archivo `mqipt.conf` creado en el apartado “Prueba de verificación de la instalación” en la página 68.)

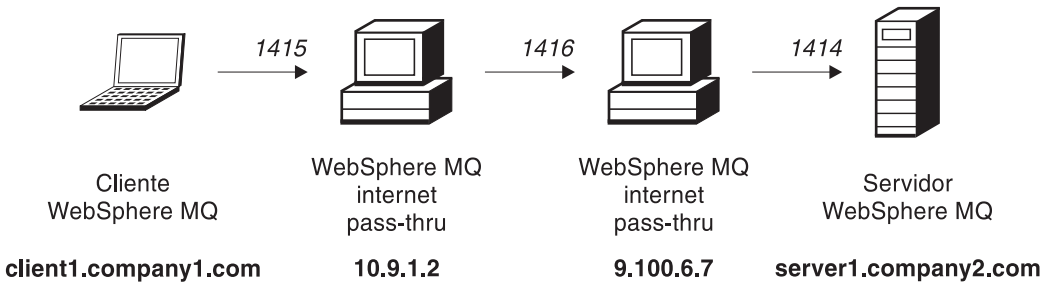

Figura 14. Diagrama de red del cliente SSL

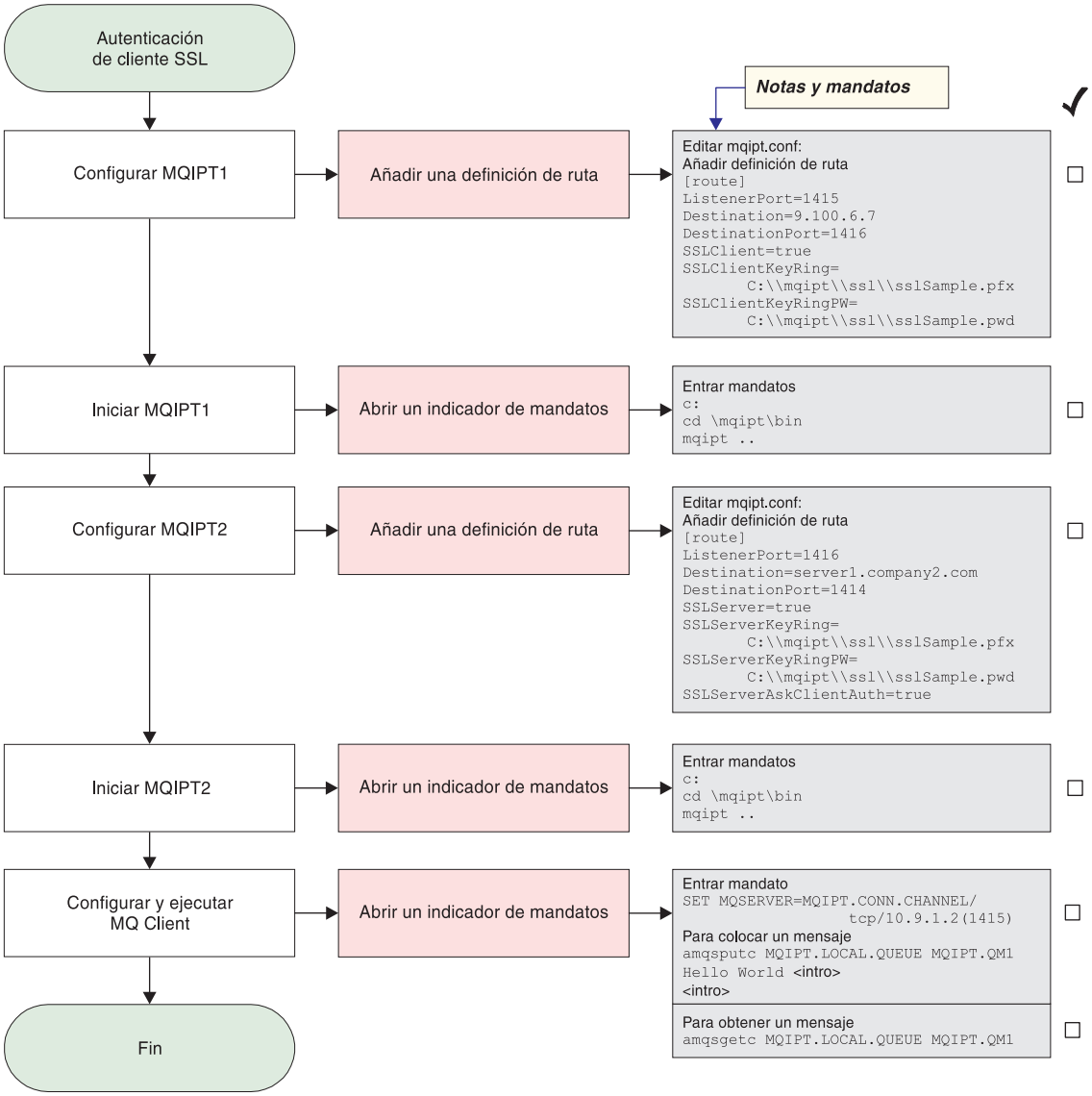

Figura 15. Autenticación del cliente SSL

1. Configure MQIPT1.
   Edite el archivo `mqipt.conf` y añada una definición de ruta:

```
[route]
ListenerPort=1415
Destination=9.100.6.7
DestinationPort=1416
SSLClient=true
SSLClientKeyRing=C:\\mqipt\\sslSample.pfx
SSLClientKeyRingPW=C:\\mqipt\\sslSample.pwd
```

2. Inicie MQIPT1.

   Abra un indicador de mandatos y escriba lo siguiente:

   ```
   c:
   cd \mqipt\bin
   mqipt ..
   ```

   El mensaje siguiente indica que se ha realizado correctamente:

   ```
   5639-L92 (C) Copyright IBM Corp. 2000-2002 All Rights Reserved
   MQCPI001 WebSphere MQ internet pass-thru Version 1.2 starting
   MQCPI011 The path c:\mqipt\logs will be used to store the log files
   MQCPI006 Route 1415 has started and will forward messages to :
   MQCPI034 ....9.100.6.7(1416)
   MQCPI035 ....using MQ protocols
   MQCPI036 ....SSL Client side enabled with properties :
   MQCPI031 ......cipher suites <null>
   MQCPI032 ......keyring file c:\mqipt\sslSample.pfx
   MQCPI047 ......CA keyring file <null>
   MQCPI038 ......distinguished name(s) CN=* O=* OU=* L=* ST=* C=*
   ```

3. Configure MQIPT2.

   Edite el archivo `mqipt.conf` y añada una definición de ruta:

   ```
   [route]
   ListenerPort=1416
   Destination=Server1.company2.com
   DestinationPort=1414
   SSLClient=true
   SSLServerKeyRing=C:\\mqipt\\sslSample.pfx
   SSLServerKeyRingPW=C:\\mqipt\\sslSample.pwd
   ```

4. Inicie MQIPT2.

   Abra un indicador de mandatos y escriba lo siguiente:

   ```
   c:
   cd \mqipt\bin
   mqipt
   ```

   El mensaje siguiente indica que se ha realizado correctamente:

   ```
   5639-L92 (C) Copyright IBM Corp. 2000-2002 All Rights Reserved
   MQCPI001 WebSphere MQ internet pass-thru Version 1.2 starting
   MQCPI011 The path c:\mqipt\logs will be used to store the log files
   MQCPI006 Route 1416 has started and will forward messages to :
   MQCPI034 ....server1.company2.com(1414)
   MQCPI035 ....using MQ protocols
   MQCPI037 ....SSL Server side enabled with properties :
   MQCPI031 ......cipher suites <null>
   MQCPI032 ......keyring file c:\mqipt\sslSample.pfx
   MQCPI047 ......CA keyring file <null>
   MQCPI038 ......distinguished name(s) CN=* O=* OU=* L=* ST=* C=*
   MQCPI033 ......client authentication set to true
   ```

5. En un indicador de mandatos de la máquina cliente de WebSphere MQ, escriba lo siguiente:

   ```
   SET MQSERVER=MQIPT.CONN.CHANNEL/tcp/10.9.1.2(1415)
   ```

6. Coloque un mensaje mediante el mandato siguiente:

```
amqsputc MQIPT.LOCAL.QUEUE MQIPT1.QM1
Hola amigos <Intro>
 <Intro>
```

7. Obtenga el mensaje mediante el mandato siguiente:

```
amqsgetc MQIPT.LOCAL.QUEUE MQIPT1.QM1
```

Verá el texto ″Hola amigos″.

Configuración del proxy HTTP

En este ejemplo comprobará la conexión utilizando un proxy HTTP (IBM Caching Proxy). El nivel de CP debe ser 3.6 o superior. También debe comprobar lo siguiente:

- `ProxyPersistance` debe estar `activado`, de este modo se permite que las conexiones sean permanentes.
- `MaxPersistRequest` debe establecerse en 5000; y éste será el número de peticiones permitidas en una sola conexión antes de que se interrumpa la conexión.
- `PersistTimeout` debe establecerse en 12 horas; y éste será el período de tiempo que puede existir la conexión.

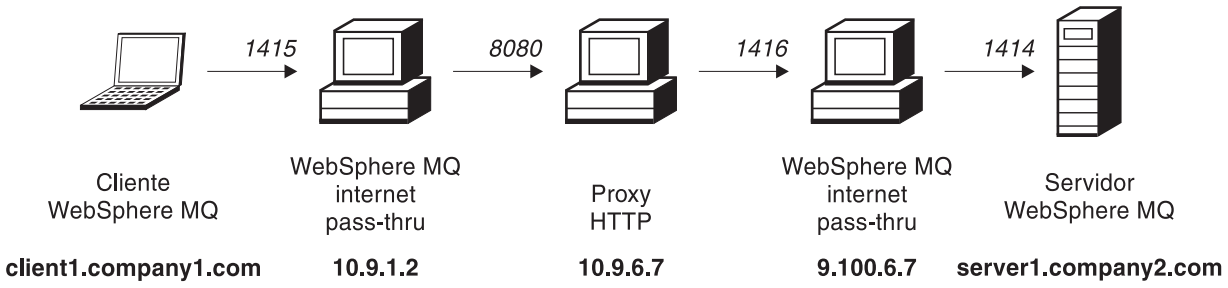

Figura 16. Diagrama de red del proxy HTTP

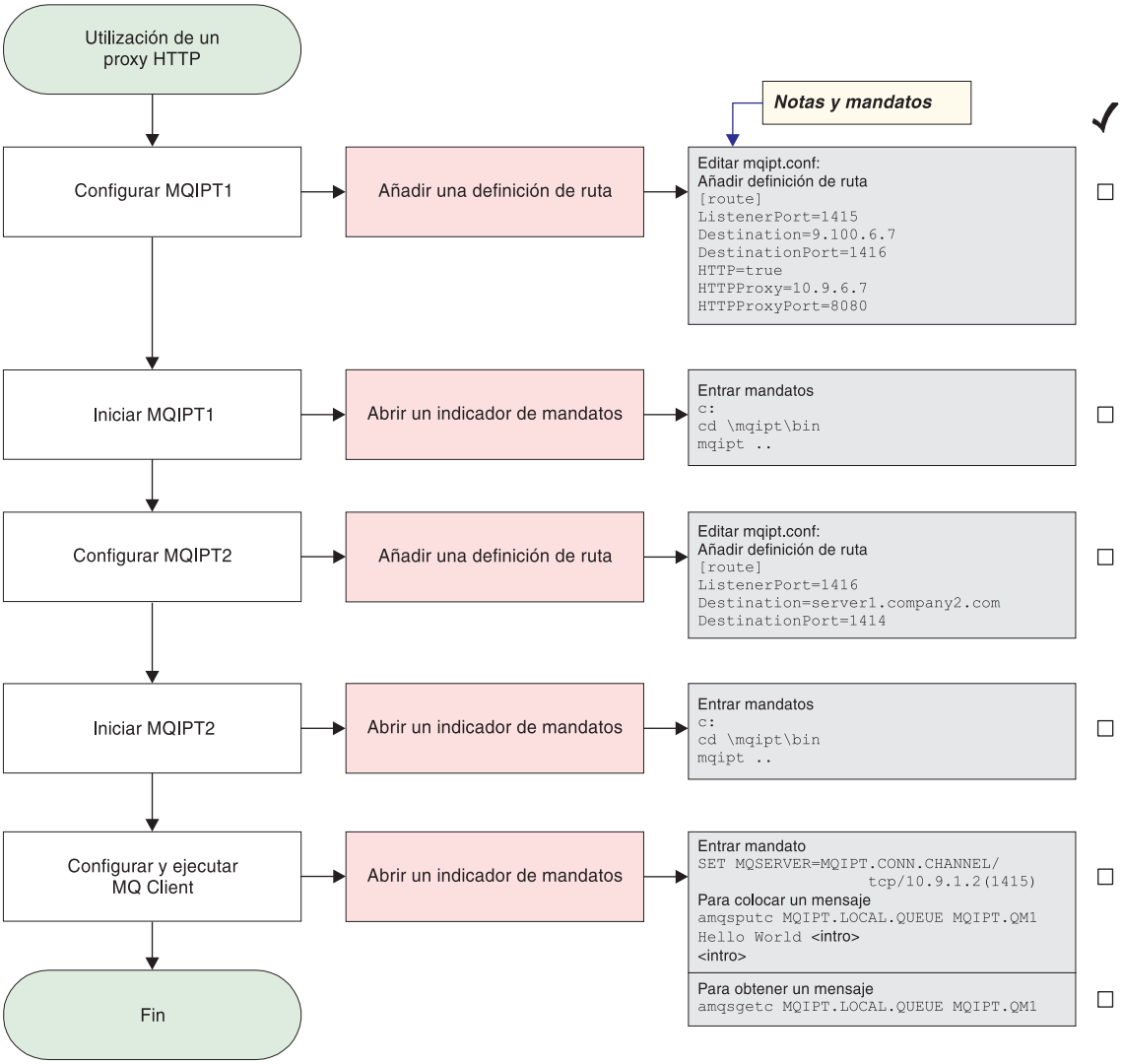

Figura 17. Configuración del proxy HTTP

1. Configure MQIPT1.

   Edite el archivo `mqipt.conf` y añada una definición de ruta:

   ```
   [route]
   ListenerPort=1415
   Destination=9.100.6.7
   DestinationPort=1416
   HTTP=true
   HTTPProxy=true
   HTTPProxyPort=8080
   ```

2. Inicie MQIPT1.

   Abra un indicador de mandatos y escriba lo siguiente:

   ```
   c:
   cd \mqipt\bin
   mqipt ..
   ```

   El mensaje siguiente indica que se ha realizado correctamente:

   ```
   5639-L92 (C) Copyright IBM Corp. 2000-2002 All Rights Reserved
   MQCPI001 WebSphere MQ internet pass-thru Version 1.2 starting
   MQCPI004 Reading configuration information from C:\mqipt\mqipt.conf
   MQCPI011 The path C:\mqipt\logs will be used to store the log files
   ```

```
MQCPI006 Route 1415 has started and will forward messages to :
MQCPI034 ....9.100.6.7(1416)
MQCPI035 ....using HTTP
MQCPI024 ....and HTTP proxy at 10.9.6.7(1080)
```

3. Configure MQIPT2.

   Edite el archivo `mqipt.conf` y añada una definición de ruta:

   ```
   [route]
   ListenerPort=1416
   Destination=Server1.company2.com
   DestinationPort=1414
   ```

4. Inicie MQIPT2.

   Abra un indicador de mandatos y escriba lo siguiente:

   ```
   c:
   cd \mqipt\bin
   mqipt
   ```

   El mensaje siguiente indica que se ha realizado correctamente:

   ```
   5639-L92 (C) Copyright IBM Corp. 2000-2002 All Rights Reserved
   MQCPI001 WebSphere MQ internet pass-thru Version 1.2 starting
   MQCPI004 Reading configuration information from C:\mqipt\mqipt.conf
   MQCPI011 The path C:\mqipt\logs will be used to store the log files
   MQCPI006 Route 1416 has started and will forward messages to :
   MQCPI034 ....server1.company2.com(1414)
   MQCPI035 ....using MQ protocols
   ```

5. En un indicador de mandatos de la máquina cliente de WebSphere MQ, escriba lo siguiente:

   ```
   SET MQSERVER=MQIPT.CONN.CHANNEL/tcp/10.9.1.2(1415)
   ```

6. Coloque un mensaje mediante el mandato siguiente:

   ```
   amqsputc MQIPT.LOCAL.QUEUE MQIPT1.QM1
   Hola amigos <Intro>
    <Intro>
   ```

7. Obtenga el mensaje mediante el mandato siguiente:

   ```
   amqsgetc MQIPT.LOCAL.QUEUE MQIPT1.QM1
   ```

Verá el texto ″Hola amigos″.

Configuración del control de acceso

En este ejemplo configurará MQIPT de modo que sólo acepte conexiones de clientes específicos añadiendo comprobaciones de seguridad a la puerta del escucha de MQIPT mediante Java Security Manager.

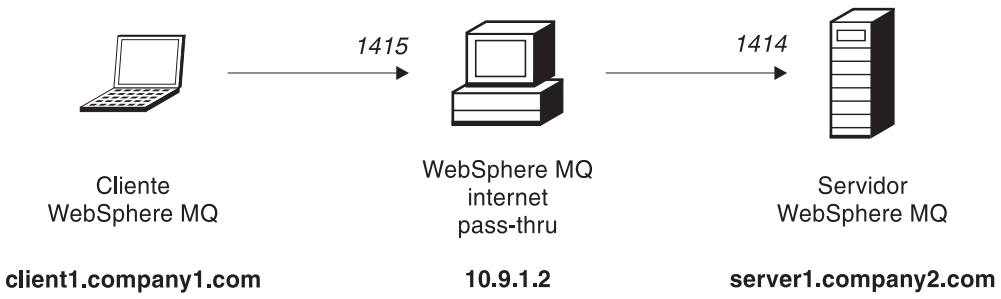

Figura 18. Diagrama de red de control de acceso

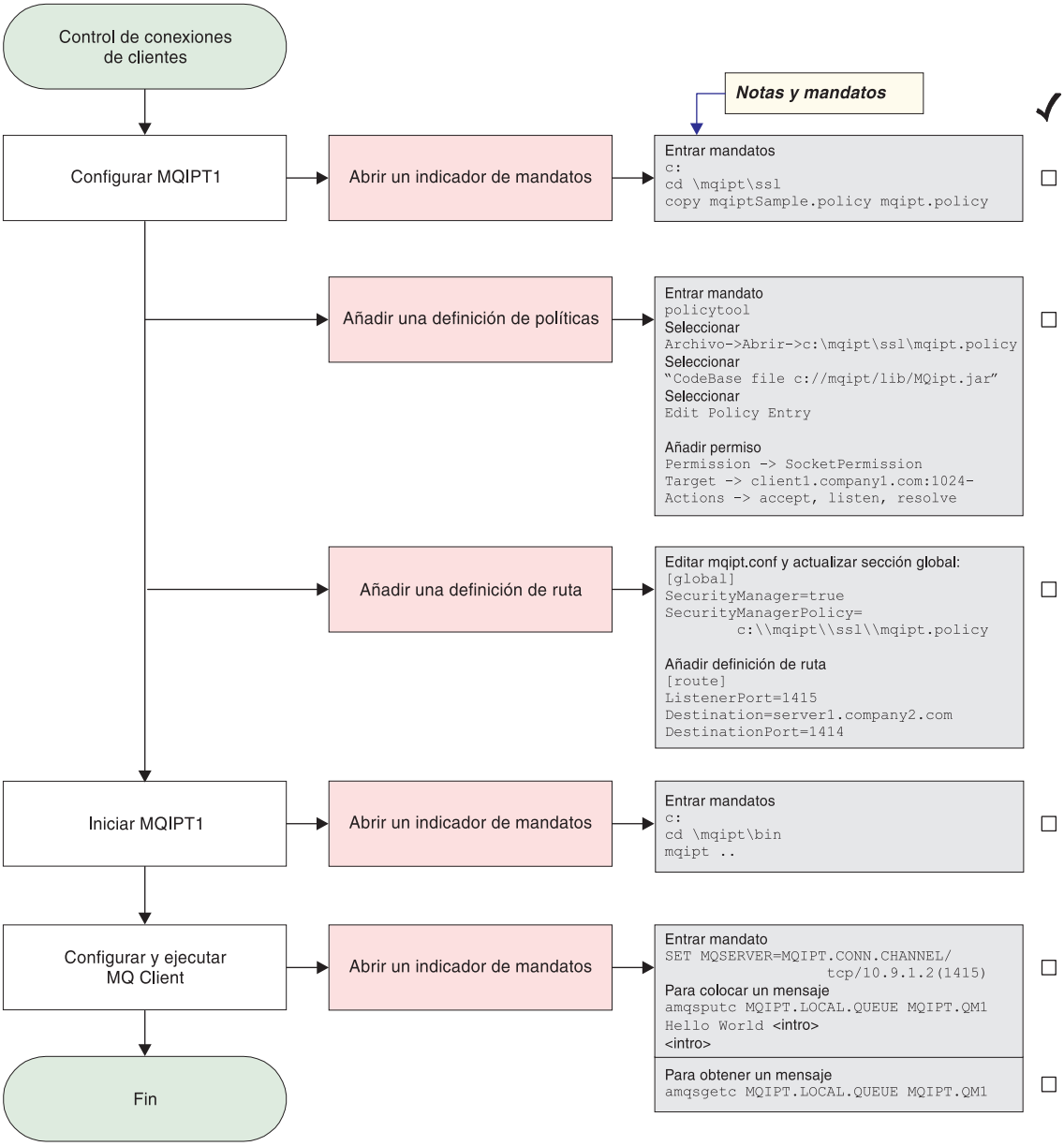

Figura 19. Configuración del control de acceso

1. Configure MQIPT1.
   a. Abra un indicador de mandatos y escriba lo siguiente:

      ```
      c:
      cd \mqipt\ssl
      copie c:\mqipt\ssl\mqiptSample.policy en mqipt.policy
      ```

   b. Añada una definición de políticas mediante el mandato siguiente:

      ```
      policytool
      ```

      1) Seleccione Archivo -> Abrir -> `c:\mqipt\ssl\mqipt.policy`
      2) Seleccione:

         ```
         file://C:/Archivos de programa/IBM/WebSphere MQ internet pass-thru/lib/MQipt.jar
         ```

      3) Cambie la base de código de:

         ```
         file://C:/Archivos de programa/IBM/WebSphere MQ internet pass-thru/lib/MQipt.jar
         ```

a:

```
file://C:/mqipt/lib/MQipt.jar
```

4) Cambie todos los permisos de:

```
C:\\Archivos de programa\\IBM\\WebSphere MQ internet pass-thru
```

a:

```
C:\\mqipt
```

5) Añada SocketPermission:

```
Permission=SocketPermission
Target=client1.company1.com:1024-
Acitons=accept, listen, resolve
```

c. Edite el archivo `mqipt.conf` y añada:

1) Dos propiedades a la sección global:

```
[global]
SecurityManager=true
SecurityManagerPolicy=c:\\mqipt\\ssl\\mqipt.policy
```

2) Una definición de ruta:

```
[route]
ListenerPort=1415
Destination=server1.company2.com
DestinationPort=1414
```

2. Inicie MQIPT1.

   Abra un indicador de mandatos y escriba lo siguiente:

```
c:
cd \mqipt\bin
mqipt ..
```

   El mensaje siguiente indica que se ha realizado correctamente:

```
5639-L92 (C) Copyright IBM Corp. 2000-2002 All Rights Reserved
MQCPI001 WebSphere MQ internet pass-thru Version 1.2 starting
MQCPI004 Reading configuration information from C:\mqipt\mqipt.conf
MQCPI055 Setting the java.security.policy to c:\mqipt\mqipt.policy
MQCPI053 Starting the Java Security Manager
MQCPI011 The path C:\mqipt\logs will be used to store the log files
MQCPI006 Route 1415 has started and will forward messages to :
MQCPI034 ....server1.company2.com(1414)
MQCPI035 ....using MQ protocols
```

3. En un indicador de mandatos de la máquina cliente de WebSphere MQ, escriba lo siguiente:

```
SET MQSERVER=MQIPT.CONN.CHANNEL/tcp/10.9.1.2(1415)
```

4. Coloque un mensaje mediante el mandato siguiente:

```
amqsputc MQIPT.LOCAL.QUEUE MQIPT1.QM1
Hola amigos <Intro>
 <Intro>
```

5. Obtenga el mensaje mediante el mandato siguiente:

```
amqsgetc MQIPT.LOCAL.QUEUE MQIPT1.QM1
```

Verá el texto ″Hola amigos″.

Configuración de la calidad de servicio (QoS)

En este ejemplo, se presupone que TQoS ya se ha instalado en la misma máquina que MQIPT.

En este ejemplo aplicará una calidad de servicio (QoS) a todos los canales de una ruta MQIPT. Esto solamente puede implementarse cuando se ejecuta MQIPT en la plataforma Linux. En este ejemplo se establecerá una prioridad ″average″ (media) para todos los datos que se envíen desde MQIPT al cliente de WebSphere MQ y una prioridad ″good″ (buena) para todos los datos que se envíen al servidor de WebSphere MQ. Utilizando las políticas de ejemplo de pagent que se listan a continuación, se pueden aplicar las prioridades siguientes a `QosToCaller` y a `QosToDest`:

- 1 - average (media)
- 2 - good (buena)
- 3 - very good (muy buena)

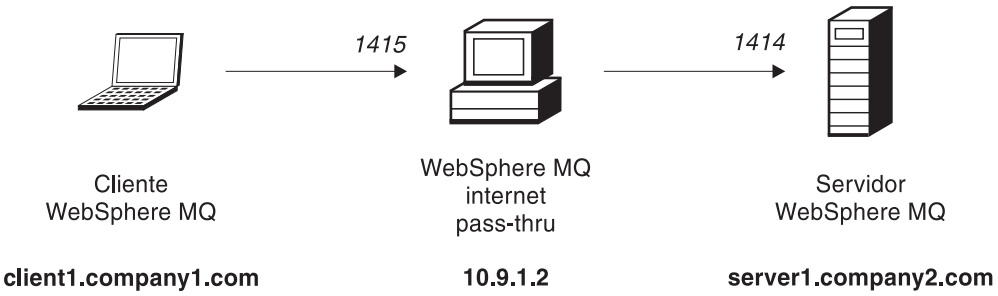

Figura 20. Diagrama de red de QoS

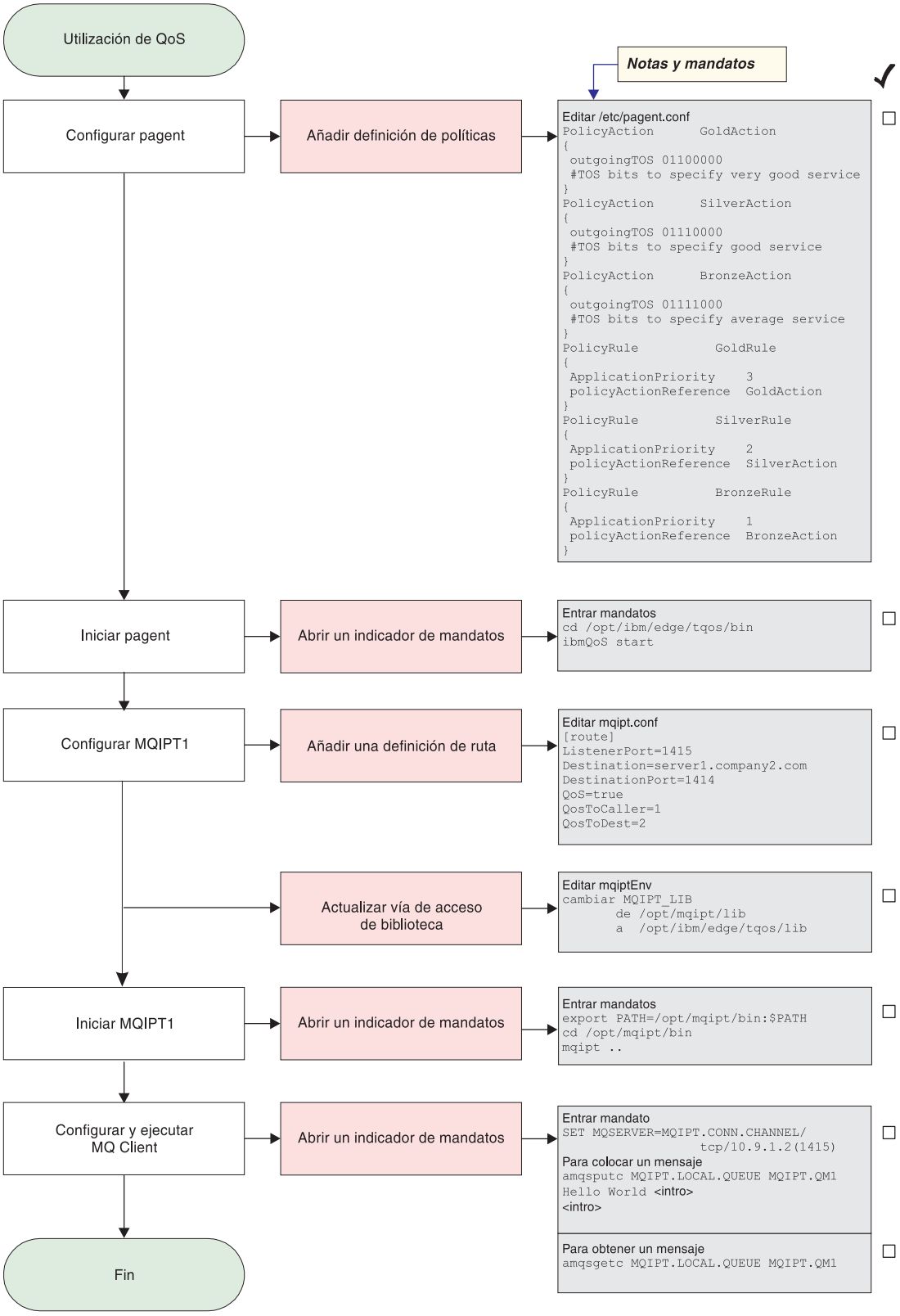

Figura 21. Configuración de QoS

1. Configure pagent.
   Edite el archivo `/etc/pagent.conf` y añada lo siguiente:

```
PolicyAction      GoldAction
{
 outgoingTOS 01100000
 #TOS bits to specify very good service
}
PolicyAction      SilverAction
{
 outgoingTOS 01110000
 #TOS bits to specify good service
}
PolicyAction      BronzeAction
{
 outgoingTOS 01111000
 #TOS bits to specify average service
}
PolicyRule          GoldRule
{
 ApplicationPriority    3
 policyActionReference  GoldAction
}
PolicyRule          SilverRule
{
 ApplicationPriority    2
 policyActionReference  SilverAction
}
PolicyRule          BronzeRule
{
 ApplicationPriority    1
 policyActionReference  BronzeAction
}
```

2. Inicie pagent.

   Abra un indicador de mandatos y escriba lo siguiente:

   ```
   cd  /opt/ibm/edge/tqos/bin
   ibmQoS start
   ```

3. Configure MQIPT1.

   Edite el archivo `mqipt.conf` y añada una definición de ruta:

   ```
   [route]
   ListenerPort=1415
   Destination=server1.company2.com
   DestinationPort=1414
   QoS=true
   QosToCaller=1
   QosToDest=2
   ```

4. Actualice la vía de acceso de biblioteca.

   Edite `mqiptEnv` (lo encontrará en `/opt/mqipt/bin`) y cambie MQIPT_LIB de:

   ```
   /opt/mqipt/lib
   ```

   a:

   ```
   /opt/ibm/edge/tqos/lib
   ```

5. Inicie MQIPT1.

   Abra un indicador de mandatos y escriba lo siguiente:

   ```
   export PATH=/opt/mqipt/bin:$PATH
   cd /opt/mqipt/bin
   mqipt ..
   ```

   El mensaje siguiente indica que se ha realizado correctamente:

   ```
   5639-L92 (C) Copyright IBM Corp. 2000-2002 All Rights Reserved
   MQCPI001 WebSphere MQ internet pass-thru Version 1.2 starting
   MQCPI004 Reading configuration information from /opt/mqipt/mqipt.conf
   MQCPI011 The path /opt/mqipt/logs will be used to store the log files
   ```

```
MQCPI006 Route 1415 has started and will forward messages to :
MQCPI034 ....server1.company2.com(1414)
MQCPI035 ....using MQ protocols
MQCPI049 ....QoS priority to dest = 2, to caller = 1
```

6. En un indicador de mandatos de la máquina cliente de WebSphere MQ, escriba lo siguiente:

```
SET MQSERVER=MQIPT.CONN.CHANNEL/tcp/10.9.1.2(1415)
```

7. Coloque un mensaje mediante el mandato siguiente:

```
amqsputc MQIPT.LOCAL.QUEUE MQIPT1.QM1
Hola amigos <Intro>
 <Intro>
```

8. Obtenga el mensaje mediante el mandato siguiente:

```
amqsgetc MQIPT.LOCAL.QUEUE MQIPT1.QM1
```

Verá el texto ″Hola amigos″.

Configuración del proxy SOCKS

En este ejemplo puede hacer que MQIPT actúe como un proxy SOCKS. El cliente de WebSphere MQ se debe habilitar para SOCKS antes de ejecutar este ejemplo y la configuración de SOCKS debe apuntar a MQIPT como el proxy SOCKS. Las propiedades Destination y DestinationPort de MQIPT pueden tener cualquier definición ya que el destino real se obtiene del cliente de WebSphere MQ durante el proceso de reconocimiento.

Antes de empezar, debe habilitar para SOCKS toda la máquina o simplemente la aplicación de cliente de WebSphere MQ (amqsputc/amqsgetc). También debe configurar el cliente de SOCKS para que:

- Apunte a MQIPT como el proxy Socks.
- Habilite el soporte de Socks V5.
- Inhabilite la autenticación de usuarios.
- Únicamente efectúe conexiones con la dirección de red de MQIPT.

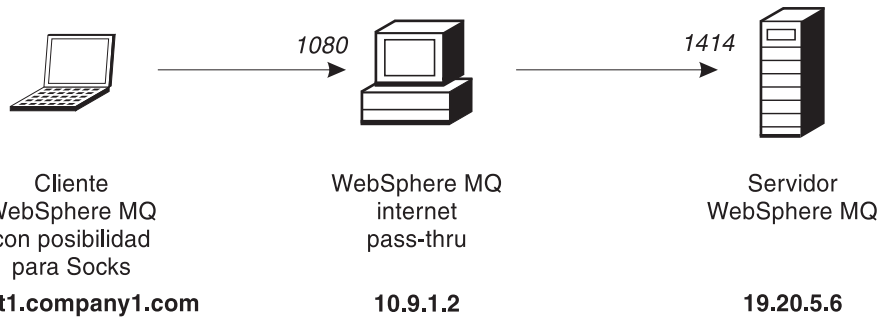

Figura 22. Diagrama de red del proxy SOCKS

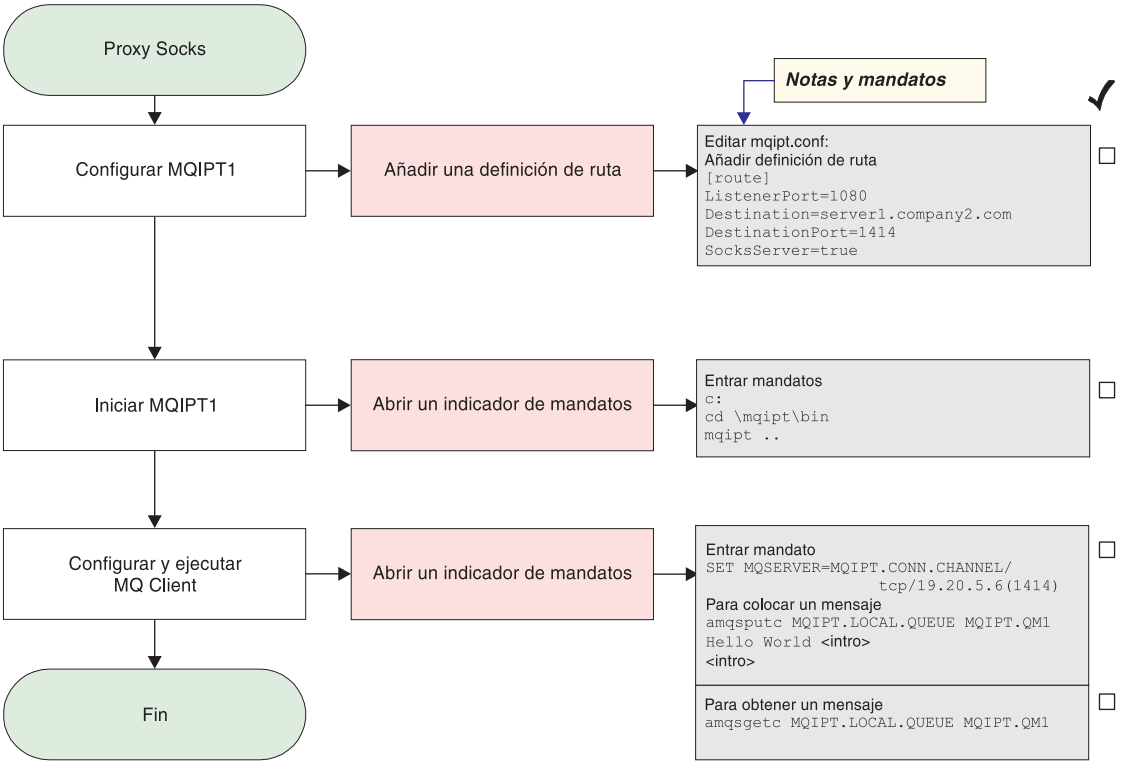

Figura 23. Configuración del proxy SOCKS

1. Configure MQIPT1.

   Edite el archivo `mqipt.conf` y añada una definición de ruta:

   ```
   [route]
   ListenerPort=1080
   Destination=server1.company2.com
   DestinationPort=1414
   SocksServer=true
   ```

2. Inicie MQIPT1.

   Abra un indicador de mandatos y escriba lo siguiente:

   ```
   c:
   cd \mqipt\bin
   mqipt ..
   ```

   El mensaje siguiente indica que se ha realizado correctamente:

   ```
   5639-L92 (C) Copyright IBM Corp. 2000-2002 All Rights Reserved
   MQCPI001 WebSphere MQ internet pass-thru Version 1.2 starting
   MQCPI004 Reading configuration information from C:\mqipt\mqipt.conf
   MQCPI011 The path C:\mqipt\logs will be used to store the log files
   MQCPI006 Route 1080 has started and will forward messages to :
   MQCPI034 ....server1.company2.com(1414)
   MQCPI035 ....using MQ protocols
   MQCPI052 ....Socks server side enabled
   ```

3. En un indicador de mandatos de la máquina cliente de WebSphere MQ, escriba lo siguiente:

   ```
   SET MQSERVER=MQIPT.CONN.CHANNEL/tcp/19.20.5.6(1414)
   ```

4. Coloque un mensaje mediante el mandato siguiente:

   ```
   amqsputc MQIPT.LOCAL.QUEUE MQIPT1.QM1
   Hola amigos <Intro>
    <Intro>
   ```

5. Obtenga el mensaje mediante el mandato siguiente:

   ```
   amqsgetc MQIPT.LOCAL.QUEUE MQIPT1.QM1
   ```

Verá el texto ″Hola amigos″.

Configuración del cliente SOCKS

En este ejemplo ejecutará MQIPT como si se hubiera habilitado para SOCKS, utilizando un proxy SOCKS existente. Es similar al procedimiento descrito en el apartado “Configuración del proxy SOCKS” en la página 83, excepto que es MQIPT el que realiza una conexión habilitada para SOCKS, en lugar del cliente de WebSphere MQ.

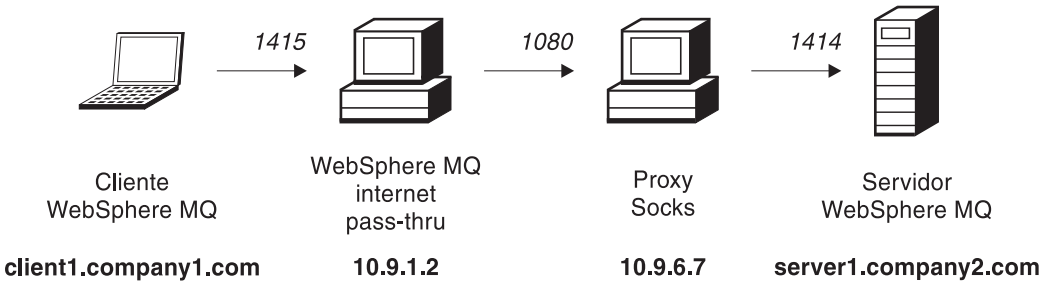

Figura 24. Diagrama de red del cliente SOCKS

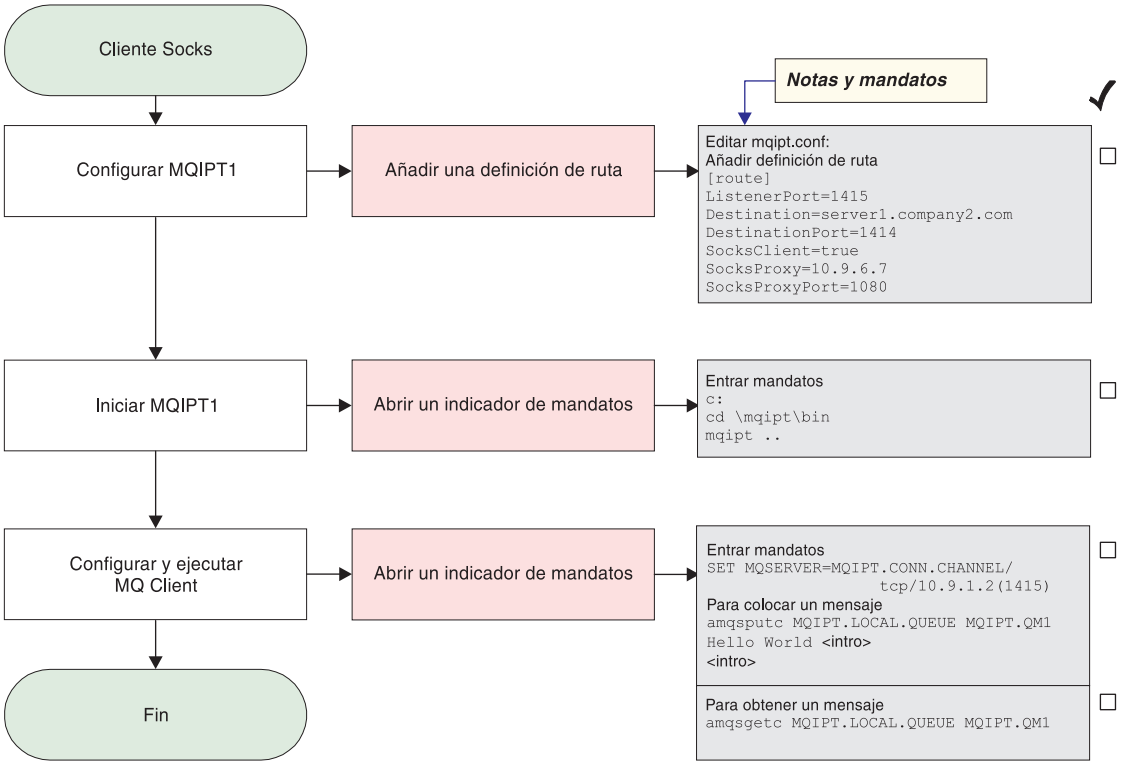

Figura 25. Configuración del cliente SOCKS

1. Configure MQIPT1.

   Edite el archivo `mqipt.conf` y añada una definición de ruta:

```
[route]
ListenerPort=1415
Destination=server1.company2.com
DestinationPort=1414
SocksClient=true
SocksProxy=10.9.6.7
SocksProxyPort=1080
```

2. Inicie MQIPT1.

   Abra un indicador de mandatos y escriba lo siguiente:

   ```
   c:
   cd \mqipt\bin
   mqipt ..
   ```

   El mensaje siguiente indica que se ha realizado correctamente:

   ```
   5639-L92 (C) Copyright IBM Corp. 2000-2002 All Rights Reserved
   MQCPI001 WebSphere MQ internet pass-thru Version 1.2 starting
   MQCPI004 Reading configuration information from C:\mqipt\mqipt.conf
   MQCPI022 Password checking has been disabled on the command port
   MQCPI011 The path C:\mqipt\logs will be used to store the log files
   MQCPI006 Route 1415 has started and will forward messages to :
   MQCPI034 ....server1.company2.com(1414)
   MQCPI035 ....using MQ protocols
   MQCPI039 ....and Socks proxy at 10.9.6.7(1080)
   ```

3. En un indicador de mandatos de la máquina cliente de WebSphere MQ, escriba lo siguiente:

   ```
   SET MQSERVER=MQIPT.CONN.CHANNEL/tcp/10.9.1.2(1415)
   ```

4. Coloque un mensaje mediante el mandato siguiente:

   ```
   amqsputc MQIPT.LOCAL.QUEUE MQIPT1.QM1
   Hola amigos <Intro>
    <Intro>
   ```

5. Obtenga el mensaje mediante el mandato siguiente:

   ```
   amqsgetc MQIPT.LOCAL.QUEUE MQIPT1.QM1
   ```

Verá el texto "Hola amigos".

Configuración del proxy SSL

En este ejemplo, ejecutará MQIPT en modalidad de proxy SSL, de modo que acepte una petición de conexión SSL procedente de un cliente SSL y la envíe a través de túnel a un servidor SSL.

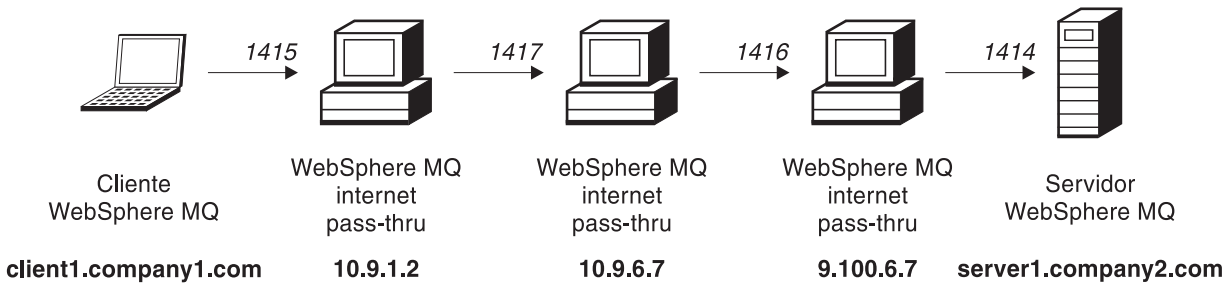

Figura 26. Diagrama de red del proxy SSL

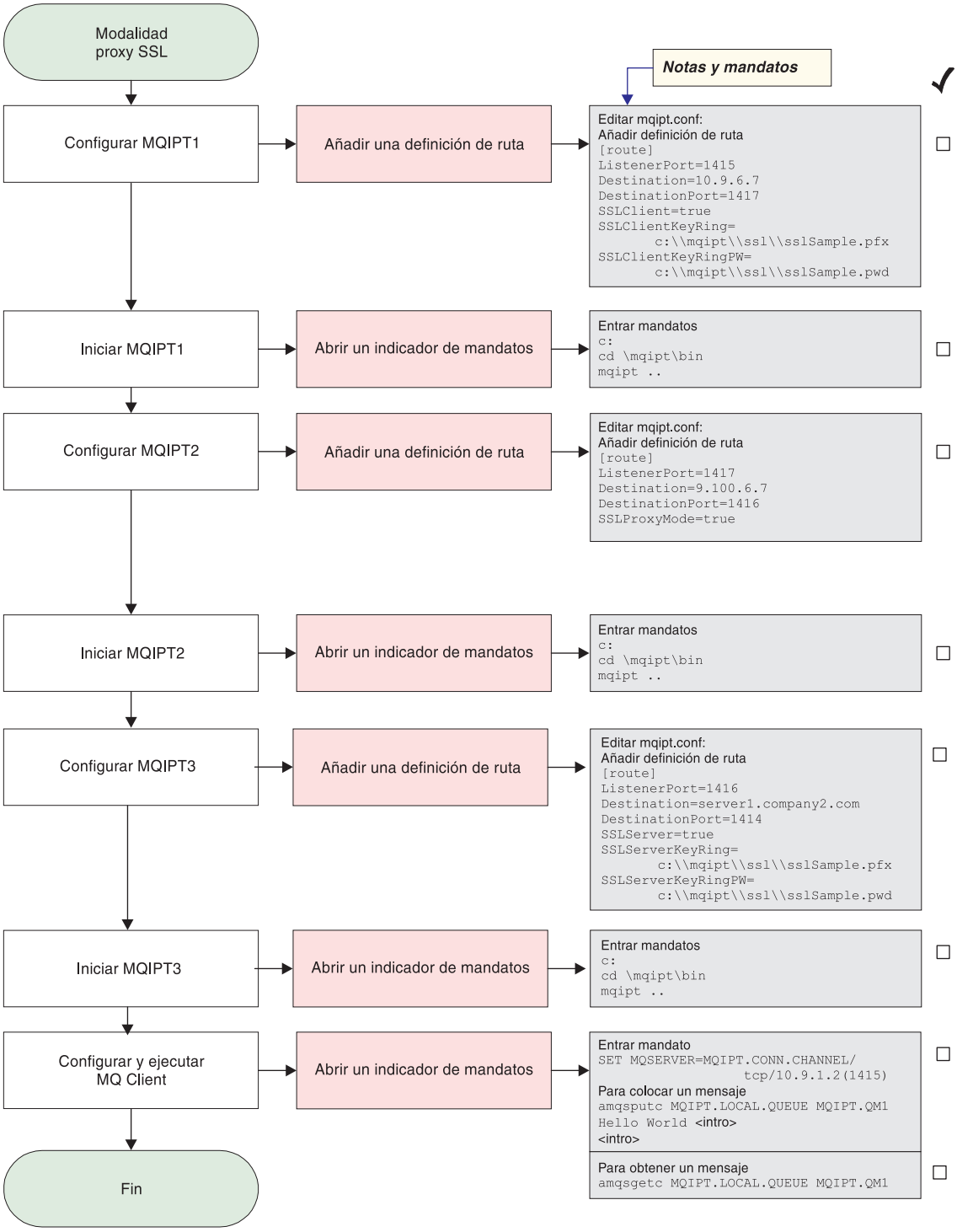

Figura 27. Configuración del proxy SSL

1. Configure MQIPT1.

   Edite el archivo `mqipt.conf` y añada una definición de ruta:

   ```
   [route]
   ListenerPort=1415
   Destination=10.9.6.7
   DestinationPort=1417
   ```

```
SSLClient=true
SSLClientKeyRing=c:\\mqipt\\ssl\\sslSample.pfx
SSLClientKeyRingPW=c:\\mqipt\\ssl\\sslSample.pwd
```

2. Inicie MQIPT1.

   Abra un indicador de mandatos y escriba lo siguiente:

   ```
   c:
   cd \mqipt\bin
   mqipt ..
   ```

   El mensaje siguiente indica que se ha realizado correctamente:

   ```
   5639-L92 (C) Copyright IBM Corp. 2000-2002 All Rights Reserved
   MQCPI001 WebSphere MQ internet pass-thru Version 1.2 starting
   MQCPI004 Reading configuration information from C:\mqipt\mqipt.conf
   MQCPI011 The path C:\mqipt\logs will be used to store the log files
   MQCPI006 Route 1415 has started and will forward messages to :
   MQCPI034 ....10.9.6.7(1417)
   MQCPI035 ....using MQ protocols
   MQCPI036 ....SSL Client side enabled with properties :
   MQCPI031 ......cipher suites <null>
   MQCPI032 ......keyring file c:\mqipt\ssl\sslSample.pfx
   MQCPI047 ......CA keyring file <null>
   MQCPI038 ......distinguished name(s) CN=* O=* OU=* L=* ST=* C=*
   ```

3. Configure MQIPT2.

   Edite el archivo `mqipt.conf` y añada una definición de ruta:

   ```
   [route]
   ListenerPort=1417
   Destination=9.100.6.7
   DestinationPort=1416
   SSLProxyMode=true
   ```

4. Inicie MQIPT2.

   Abra un indicador de mandatos y escriba lo siguiente:

   ```
   c:
   cd \mqipt\bin
   mqipt
   ```

   El mensaje siguiente indica que se ha realizado correctamente:

   ```
   5639-L92 (C) Copyright IBM Corp. 2000-2002 All Rights Reserved
   MQCPI001 WebSphere MQ internet pass-thru Version 1.2 starting
   MQCPI004 Reading configuration information from C:\mqipt\mqipt.conf
   MQCPI011 The path C:\mqipt\logs will be used to store the log files
   MQCPI006 Route 1417 has started and will forward messages to :
   MQCPI034 ....9.100.6.7(1416)
   MQCPI035 ....using SSLProxyMode
   ```

5. Configure MQIPT3.

   Edite el archivo `mqipt.conf` y añada una definición de ruta:

   ```
   [route]
   ListenerPort=1416
   Destination=server1.company2.com
   DestinationPort=1414
   SSLServer=true
   SSLServerKeyRing=c:\\mqipt\\ssl\\sslSample.pfx
   SSLServerKeyRingPW=c:\\mqipt\\ssl\\sslSample.pwd
   ```

6. Inicie MQIPT3.

   Abra un indicador de mandatos y escriba lo siguiente:

   ```
   c:
   cd \mqipt\bin
   mqipt
   ```

El mensaje siguiente indica que se ha realizado correctamente:

```
5639-L92 (C) Copyright IBM Corp. 2000-2002 All Rights Reserved
MQCPI001 WebSphere MQ internet pass-thru Version 1.2 starting
MQCPI004 Reading configuration information from C:\mqipt\mqipt.conf
MQCPI011 The path C:\mqipt\logs will be used to store the log files
MQCPI006 Route 1416 has started and will forward messages to :
MQCPI034 ....server1.company2.com(1414)
MQCPI035 ....using MQ protocols
MQCPI037 ....SSL Server side enabled with properties :
MQCPI031 ......cipher suites <null>
MQCPI032 ......keyring file c:\mqipt\ssl\sslSample.pfx
MQCPI047 ......CA keyring file <null>
MQCPI038 ......distinguished name(s) CN=* O=* OU=* L=* ST=* C=*
MQCPI033 ......client authentication set to false
```

7. En un indicador de mandatos de la máquina cliente de WebSphere MQ, escriba lo siguiente:

   ```
   SET MQSERVER=MQIPT.CONN.CHANNEL/tcp/10.9.1.2(1415)
   ```

8. Coloque un mensaje mediante el mandato siguiente:

   ```
   amqsputc MQIPT.LOCAL.QUEUE MQIPT1.QM1
   Hola amigos <Intro>
    <Intro>
   ```

9. Obtenga el mensaje mediante el mandato siguiente:

   ```
   amqsgetc MQIPT.LOCAL.QUEUE MQIPT1.QM1
   ```

Verá el texto ″Hola amigos″.

Creación de certificados de prueba SSL

En este ejemplo le mostraremos cómo crear un certificado autofirmado que puede utilizarse para comprobar las rutas MQIPT. El certificado tendrá activado el distintivo trust-as-peer.

1. Inicie KeyMan.
2. Seleccione ″Crear nuevo...″.
3. Seleccione ″Señal PKCS″.
4. Seleccione ″Acción -> Generar clave″.

   Aparecerá un nuevo par de claves en la lista ″RSA / 1024-bit″.
5. Seleccione el nuevo par de claves.
6. Seleccione ″Acción -> Crear certificado″.
7. Seleccione ″Certificado autofirmado″.
8. Escriba los detalles del certificado.

   Verá un diálogo que describe el certificado privado que se unirá a la clave. Especificar una etiqueta es una tarea opcional.
9. Seleccione el nuevo certificado.
10. Visualice los detalles del certificado.
11. Cambie las propiedades del certificado.
12. Active el distintivo trust-as-peer.
13. Cierre el diálogo. Seleccione ″Archivo -> Guardar″.
14. Escriba una frase para la contraseña, por ejemplo, Micontraseña.
15. Escriba un nombre de archivo para el nuevo archivo de conjunto de claves, por ejemplo, c:\mqipt\ssl\testRoute1414.pfx).

    Debe mantener el formato de archivo como PKCS#12 / PFX; **no ponga una marca de selección** en ″Incluir conjunto de claves en una clase Java″.

16. Cree un archivo de texto que contenga la frase de la contraseña (Micontraseña) que ha utilizando anteriormente.

    Por ejemplo, c:\mqipt\ssl\testRoute1414.pwd.

Este archivo de conjunto de claves se podrá utilizar ahora en el ejemplo del apartado "Autenticación del servidor SSL" en la página 70.

Configuración del servlet MQIPT

En este ejemplo se utiliza Tomcat Application Server y se presupone que ya se ha instalado en un directorio llamado `c:\jakarta-tomcat-4.0.1`.

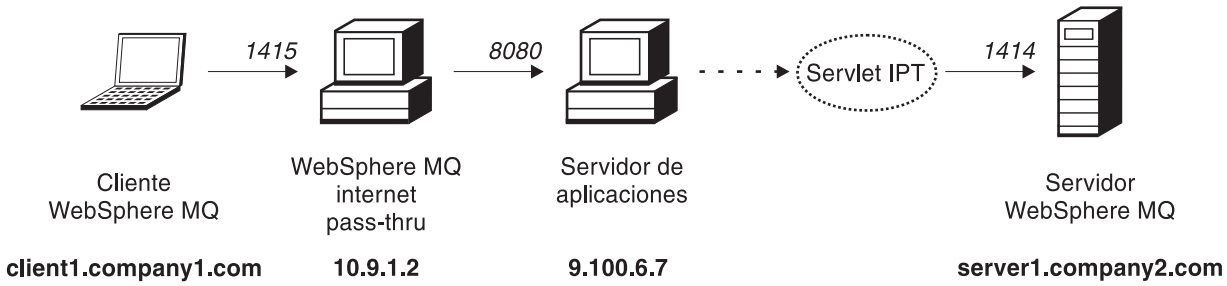

Figura 28. Diagrama de red del servlet

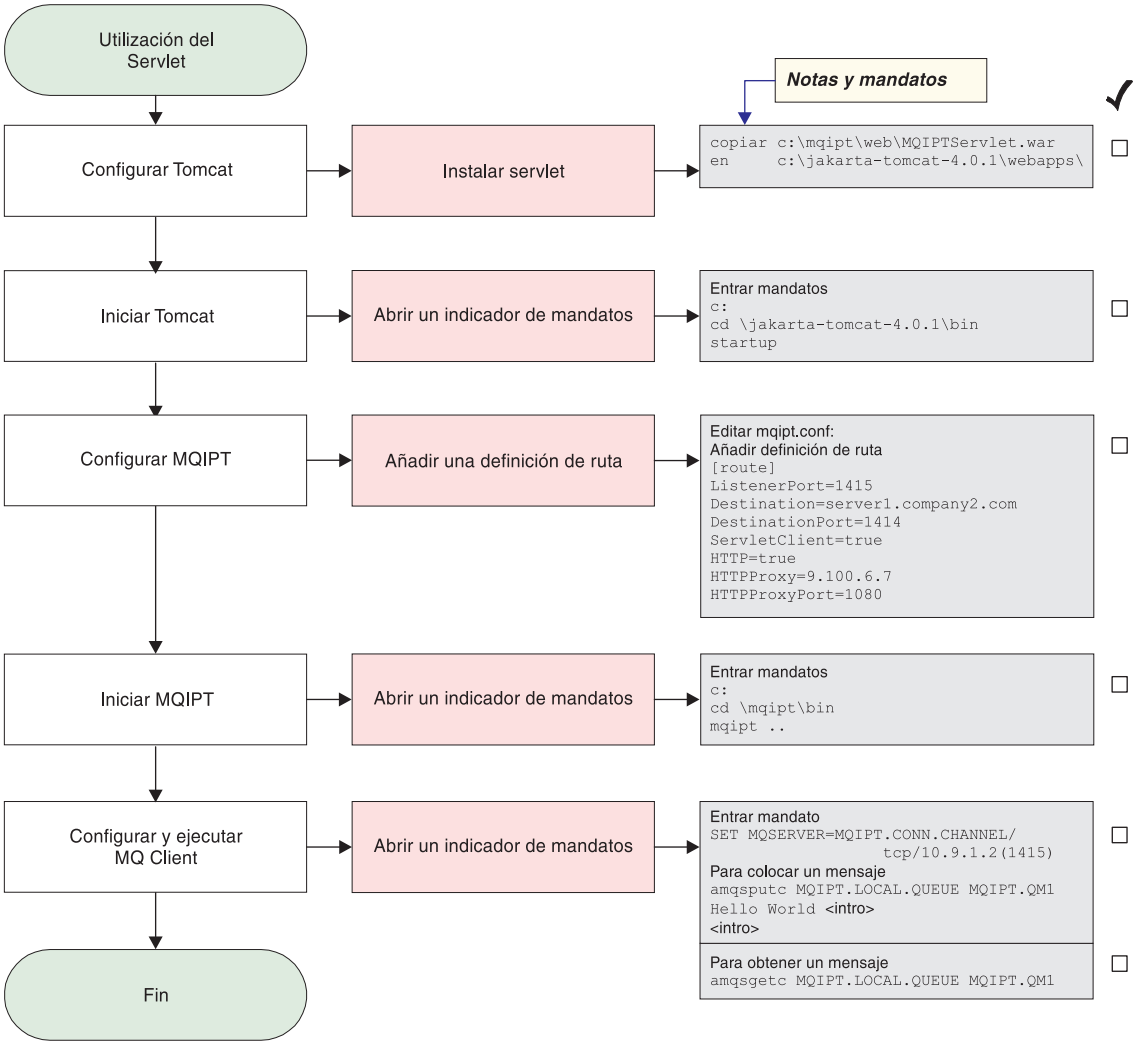

Figura 29. Configuración del servlet

1. Configure Tomcat.

   copie:

   ```
   c:\mqipt\web\MQIPTServlet.war
   ```

   en:

   ```
   c:\jakarta-tomcat-4.0.1\webapps
   ```

2. Inicie Tomcat

   Abra un indicador de mandatos y escriba lo siguiente:

   ```
   c:
   cd \jakarta-tomcat-4.0.1\bin
   startup
   ```

3. Configure MQIPT1.

   Edite el archivo `mqipt.conf` y añada una definición de ruta:

   ```
   [route]
   ListenerPort=1415
   Destination=server1.company2.com
   DestinationPort=1414
   ```

```
ServletClient=true
HTTP=true
HTTPProxy=9.100.6.7
HTTPProxyPort=8080
```

4. Inicie MQIPT1

   Abra un indicador de mandatos y escriba lo siguiente:

   ```
   c:
   cd \mqipt\bin
   mqipt ..
   ```

   El mensaje siguiente indica que se ha realizado correctamente:

   ```
   5639-L92 (C) Copyright IBM Corp. 2000-2002 All Rights Reserved
   MQCPI001 WebSphere MQ internet pass-thru Version 1.2 starting
   MQCPI004 Reading configuration information from C:\mqipt\mqipt.conf
   MQCPI011 The path C:\mqipt\logs will be used to store the log files
   MQCPI006 Route 1415 has started and will forward messages to :
   MQCPI034 ....server1.company2.com(1414)
   MQCPI035 ....using HTTP
   MQCPI024 ....and HTTP proxy at 9.100.6.7(8080)
   MQCPI059 ....servlet client enabled
   ```

5. En un indicador de mandatos de la máquina cliente de WebSphere MQ, escriba lo siguiente:

   ```
   SET MQSERVER=MQIPT.CONN.CHANNEL/tcp/10.9.1.2(1415)
   ```

6. Coloque un mensaje mediante el mandato siguiente:

   ```
   amqsputc MQIPT.LOCAL.QUEUE MQIPT1.QM1
   Hola amigos <Intro>
    <Intro>
   ```

7. Obtenga el mensaje mediante el mandato siguiente:

   ```
   amqsgetc MQIPT.LOCAL.QUEUE MQIPT1.QM1
   ```

Verá el texto ″Hola amigos″.

Configuración del soporte de agrupación en clúster de MQIPT

En este ejemplo, además de lo descrito en el apartado “Supuestos” en la página 67, también deberá haber hecho lo siguiente.

En el servidor de WebSphere MQ LONDON deberá:

- Definir un gestor de colas llamado LONDON.
- Definir un canal de conexión de servidor llamado MQIPT.CONN.CHANNEL.
- Iniciar un escucha TCP/IP para LONDON en la puerta 1414.
- Habilitar para SOCKS el gestor de colas.

En el servidor de WebSphere MQ NEWYORK deberá:

- Definir un gestor de colas llamado NEWYORK.
- Definir un canal de conexión de servidor llamado MQIPT.CONN.CHANNEL.
- Iniciar un escucha TCP/IP para NEWYORK en la puerta 1414.
- Habilitar para SOCKS el gestor de colas.

Para habilitar para SOCKS el gestor de colas, puede habilitar toda la máquina para SOCKS o simplemente la aplicación de servidor de WebSphere MQ. Configure el cliente de SOCKS de modo que:

- Apunte a MQIPT como el proxy SOCKS.
- Habilite el soporte de SOCKS V5.

- Inhabilite la autenticación de usuarios.
- Únicamente efectúe conexiones con MQIPT.

Sólo una aplicación puede escuchar en una dirección de puerta determinada en la misma máquina. Si la puerta 1414 ya está utilizándose, seleccione una dirección de puerta libre y sustitúyala en los ejemplos. Cuando haya realizado esto, puede comprobar las rutas entre los gestores de colas, colocando un mensaje en la cola local de LONDON y recuperándolo desde NEWYORK.

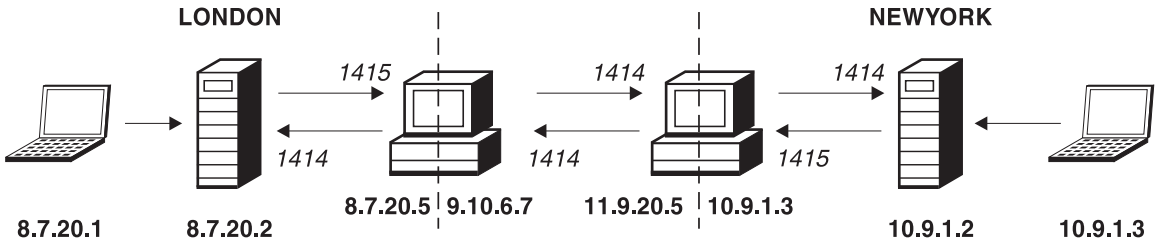

Figura 30. Diagrama de red de la agrupación en clúster

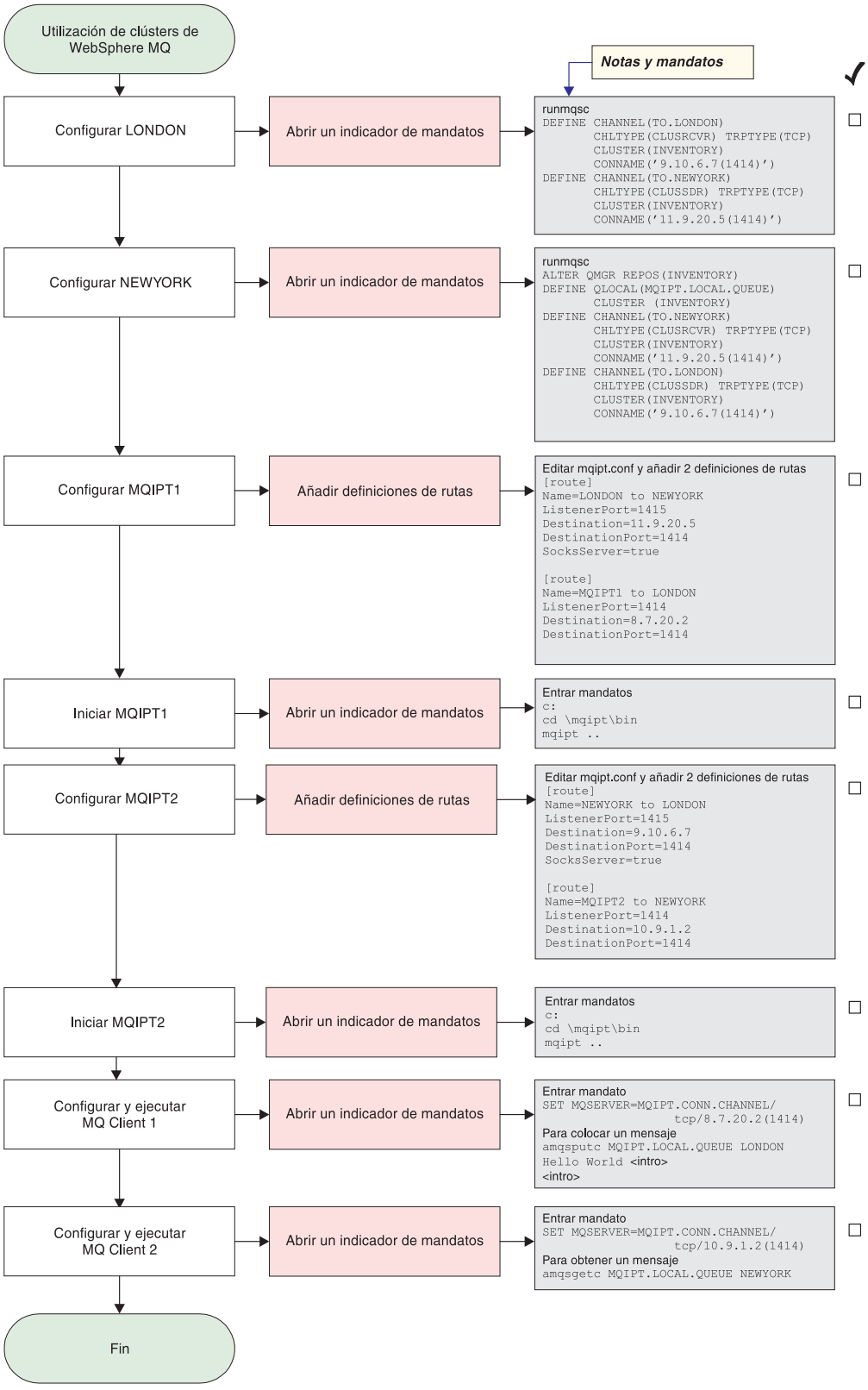

Figura 31. Configuración de la agrupación en clúster

1. Configure LONDON.
   Abra un indicador de mandatos y escriba lo siguiente:

```
runmqsc
DEFINE CHANNEL(TO.LONDON) +
       CHLTYPE(CLUSRCVR) TRPTYPE(TCP) +
       CLUSTER(INVENTORY) +
       CONNAME('9.10.6.7(1414)')
DEFINE CHANNEL(TO.NEWYORK) +
       CHLTYPE(CLUSSDR) TRPTYPE(TCP) +
       CLUSTER(INVENTORY) +
       CONNAME('11.9.20.5(1414)')
```

2. Configure NEWYORK.

   Abra un indicador de mandatos y escriba lo siguiente:

```
runmqsc
ALTER QMGR REPOS(INVENTORY)
DEFINE QLOCAL(MQIPT.LOCAL.QUEUE) +
       CLUSTER(INVENTORY)
DEFINE CHANNEL(TO.NEWYORK) +
       CHLTYPE(CLUSRCVR) TRPTYPE(TCP) +
       CLUSTER(INVENTORY) +
       CONNAME('11.9.20.5(1414)')
DEFINE CHANNEL(TO.LONDON) +
       CHLTYPE(CLUSSDR) TRPTYPE(TCP) +
       CLUSTER(INVENTORY) +
       CONNAME('9.10.6.7(1414)')
```

3. Configure MQIPT1.

   Edite el archivo `mqipt.conf` y añada dos definiciones de ruta:

```
[route]
Name=LONDON to NEWYORK
ListenerPort=1415
Destination=11.9.20.5
DestinationPort=1414
SocksServer=true
```

```
[route]
Name=MQIPT1 to LONDON
ListenerPort=1414
Destination=8.7.20.2
DestinationPort=1414
```

4. Inicie MQIPT1

   Abra un indicador de mandatos y escriba lo siguiente:

```
c:
cd \mqipt\bin
mqipt ..
```

   El mensaje siguiente indica que se ha realizado correctamente:

```
5639-L92 (C) Copyright IBM Corp. 2000-2002 All Rights Reserved
MQCPI001 WebSphere MQ internet pass-thru Version 1.2 starting
MQCPI004 Reading configuration information from C:\mqipt\mqipt.conf
MQCPI011 The path C:\mqipt\logs will be used to store the log files
MQCPI006 Route 1415 has started and will forward messages to :
MQCPI034 ....11.9.20.5(1414)
MQCPI035 ....using MQ protocols
MQCPI052 ....Socks server side enabled
MQCPI006 Route 1414 has started and will forward messages to :
MQCPI034 ....8.7.20.2(1414)
MQCPI035 ....using MQ protocols
```

5. Configure MQIPT2.

   Edite el archivo `mqipt.conf` y añada dos definiciones de ruta:

```
[route]
Name=NEWYORK to LONDON
ListenerPort=1415
Destination=9.10.6.7
DestinationPort=1414
SocksServer=true
[route]
Name=MQIPT2 to NEWYORK
ListenerPort=1414
Destination=10.9.1.2
DestinationPort=1414
```

6. Inicie MQIPT2

   Abra un indicador de mandatos y escriba lo siguiente:

   ```
   c:
   cd \mqipt\bin
   mqipt ..
   ```

   El mensaje siguiente indica que se ha realizado correctamente:

   ```
   5639-L92 (C) Copyright IBM Corp. 2000-2002 All Rights Reserved
   MQCPI001 WebSphere MQ internet pass-thru Version 1.2 starting
   MQCPI004 Reading configuration information from C:\mqipt\mqipt.conf
   MQCPI011 The path C:\mqipt\logs will be used to store the log files
   MQCPI006 Route 1415 has started and will forward messages to :
   MQCPI034 ....9.10.6.7(1414)
   MQCPI035 ....using MQ protocols
   MQCPI052 ....Socks server side enabled
   MQCPI006 Route 1414 has started and will forward messages to :
   MQCPI034 ....10.9.1.2(1414)
   MQCPI035 ....using MQ protocols
   ```

7. En un indicador de mandatos de la primera máquina cliente de WebSphere MQ (8.7.20.1), escriba lo siguiente:

   ```
   SET MQSERVER=MQIPT.CONN.CHANNEL/TCP/8.7.20.2(1414)
   ```

8. Coloque un mensaje mediante el mandato siguiente:

   ```
   amqsputc MQIPT.LOCAL.QUEUE LONDON
   Hola amigos <Intro>
    <Intro>
   ```

9. En un indicador de mandatos de la segunda máquina cliente de WebSphere MQ (10.9.1.3), escriba lo siguiente:

   ```
   SET MQSERVER=MQIPT.CONN.CHANNEL/TCP/10.9.1.2(1414)
   ```

10. En la segunda máquina cliente de WebSphere MQ, obtenga el mensaje mediante el mandato siguiente:

    ```
    amqsgetc MQIPT.LOCAL.QUEUE NEWYORK
    ```

Verá el texto ″Hola amigos″.

Creación de un archivo de conjunto de claves

Este ejemplo presupone que ha solicitado un certificado nuevo de una CA de confianza utilizando Keyman y que el certificado personal se le ha devuelto en un archivo (por ejemplo, `server.cer`). Esto será suficiente para realizar la autenticación del servidor. Si necesita autenticación del cliente necesitará solicitar un segundo certificado (por ejemplo, `client.cer`) y efectuar dos veces los pasos siguientes, para crear dos archivos de conjunto de claves.

1. Inicie KeyMan.
2. Seleccione ″Crear nuevo...″.
3. Seleccione ″Señal PKCS″.
4. Seleccione ″Acción -> Generar clave″.

Aparecerá un nuevo par de claves en la lista ″RSA / 1024-bit″.

5. Seleccione el nuevo par de claves.
6. Seleccione ″Acción -> Solicitar certificado″.

   Siga las instrucciones en línea.
7. Seleccione ″Archivo -> Guardar″.
8. Escriba la contraseña.
9. Escriba el nombre de archivo el nuevo archivo de conjunto de claves.

   Por ejemplo, `c:\mqipt\ssl\myServer.pfx`.
10. Debe mantener el formato de archivo como PKCS12 / PFX; **no ponga una marca de selección** en `"Incluir conjunto de claves en una clase Java"`.
11. Seleccione ″Archivo -> Salir″.
12. Cree un archivo de texto que contenga la frase de la contraseña (Micontraseña) que ha utilizando anteriormente.

    Por ejemplo, `c:\mqipt\ssl\myServer.pwd`.

Cuando le devuelvan el certificado, abra el archivo de conjunto de claves original `myServer.pfx`). A continuación:

1. Inicie KeyMan
2. Seleccione ″Abrir existente...″.
3. Seleccione ″Recurso local″.
4. Seleccione ″Abrir un archivo...″.
5. Escriba el nombre de archivo del archivo de certificado personal.

   Por ejemplo, `c:\mqipt\ssl\myServer.pfx`.
6. Escriba una frase para la contraseña.
7. Seleccione ″Archivo -> Importar″.
8. Seleccione ″Recurso local″.
9. Seleccione ″Abrir un archivo...″.
10. Escriba server.cer.

    Verá un diálogo en el que se describe el certificado privado que se unirá a la clave.
11. Seleccione ″Archivo -> Guardar″.
12. Seleccione ″Archivo -> Salir″.

Repita estos pasos para crear un archivo `myClient.pfx` a partir del archivo `client.cer`. Mediante KeyMan, compruebe el contenido del archivo de conjunto de claves de la CA de ejemplo, `sslCAdefault.pfx`, para ver si los certificados personales los había firmado una de las CA listadas. Si es así, puede utilizar el archivo de conjunto de clave de la CA de ejemplo. De no ser así, necesitará crear un archivo de conjunto de claves que contenga el certificado público de la CA que ha firmado sus certificados personales. Es posible que se lo devuelvan con su certificado personal. De no ser así, tendrá que solicitar el certificado de la CA a la misma CA que le ha proporcionado los certificados personales y deberá importarlo a `sslCAdefault.pfx`. El archivo de conjunto de claves de la CA se puede utilizar tanto en el extremo del cliente como en el extremo del servidor. Para utilizar estos nuevos archivos de conjunto de claves para la autenticación del servidor, consulte el ejemplo del apartado “Autenticación del servidor SSL” en la página 70, y establezca las siguientes propiedades de ruta:

```
SSLClientCAKeyRing=c:\\mqipt\\ssl\\sslCAdefault.pfx
SSLClientCAKeyRingPW=c:\\mqipt\\ssl\\sslCAdefault.pwd
SSLServerKeyRing=c:\\mqipt\\ssl\\myServer.pfx
```

```
SSLServerKeyRingPW=c:\\mqipt\\ssl\\myServer.pwd
SSLServerCAKeyRing=c:\\mqipt\\ssl\\sslCAdefault.pfx
SSLServerCAKeyRingPW=c:\\mqipt\\ssl\\sslCAdefault.pwd
```

Para utilizar estos nuevos archivos de conjunto de claves para la autenticación del cliente y del servidor, consulte el ejemplo del apartado “Autenticación del cliente SSL” en la página 72 y establezca las siguientes propiedades de ruta:

```
SSLClientKeyRing=c:\\mqipt\\ssl\\myClient.pfx
SSLClientKeyRingPW=c:\\mqipt\\ssl\\myClient.pwd
SSLClientCAKeyRing=c:\\mqipt\\ssl\\sslCAdefault.pfx
SSLClientCAKeyRingPW=c:\\mqipt\\ssl\\sslCAdefault.pwd
SSLServerKeyRing=c:\\mqipt\\ssl\\myServer.pfx
SSLServerKeyRingPW=c:\\mqipt\\ssl\\myServer.pwd
SSLServerCAKeyRing=c:\\mqipt\\ssl\\sslCAdefault.pfx
SSLServerCAKeyRingPW=c:\\mqipt\\ssl\\sslCAdefault.pwd
```

Capítulo 11. Mantenimiento de internet pass-thru

En este capítulo se describe cómo mantener internet pass-thru en ejecución y contiene los apartados siguientes:

- "Mantenimiento"
- "Determinación de problemas"
- "Ajuste del rendimiento" en la página 102

Mantenimiento

Regularmente, debe realizar una copia de seguridad de los siguientes archivos como parte de sus procedimientos de copia de seguridad habituales:

- El archivo de configuración `mqipt.conf`.
- El archivo de conjunto de claves SSL de `mqipt.conf` como se ha definido en las propiedades siguientes:
  - `SSLClientKeyRing`
  - `SSLClientCAKeyRing`
  - `SSLServerKeyRing`
  - `SSLServerCAKeyRing`
- Los archivos de contraseñas de conjunto de claves SSL de `mqipt.conf`, como se ha definido en las propiedades siguientes:
  - `SSLClientKeyRingPW`
  - `SSLClientCAKeyRingPW`
  - `SSLServerKeyRingPW`
  - `SSLServerCAKeyRingPW`
- El archivo de configuración del cliente de administración, `client.conf`, que contiene información acerca de la conexiones de todos los MQIPT que conoce el cliente de administración.

Determinación de problemas

Si encuentra algún problema, deberá comprobar en primer lugar algunos errores comunes:

- Se acaba de instalar el sistema MQIPT y no se ha reiniciado.
- Se ha establecido HTTP en `true` en una ruta que está conectada directamente con un gestor de colas.
- Se ha establecido SSLClient en `true` en una ruta que está conectada directamente con un gestor de colas.
- La variable CLASSPATH no se ha establecido correctamente.
- La variable PATH no se ha establecido correctamente.
- Las contraseñas almacenadas para los archivos de conjunto de claves son sensibles a las mayúsculas y minúsculas.

El paso siguiente es seguir el diagrama de flujo de la Figura 32 en la página 100. Los números hacen referencia a las notas siguientes.

© Copyright IBM Corp. 2000-2002

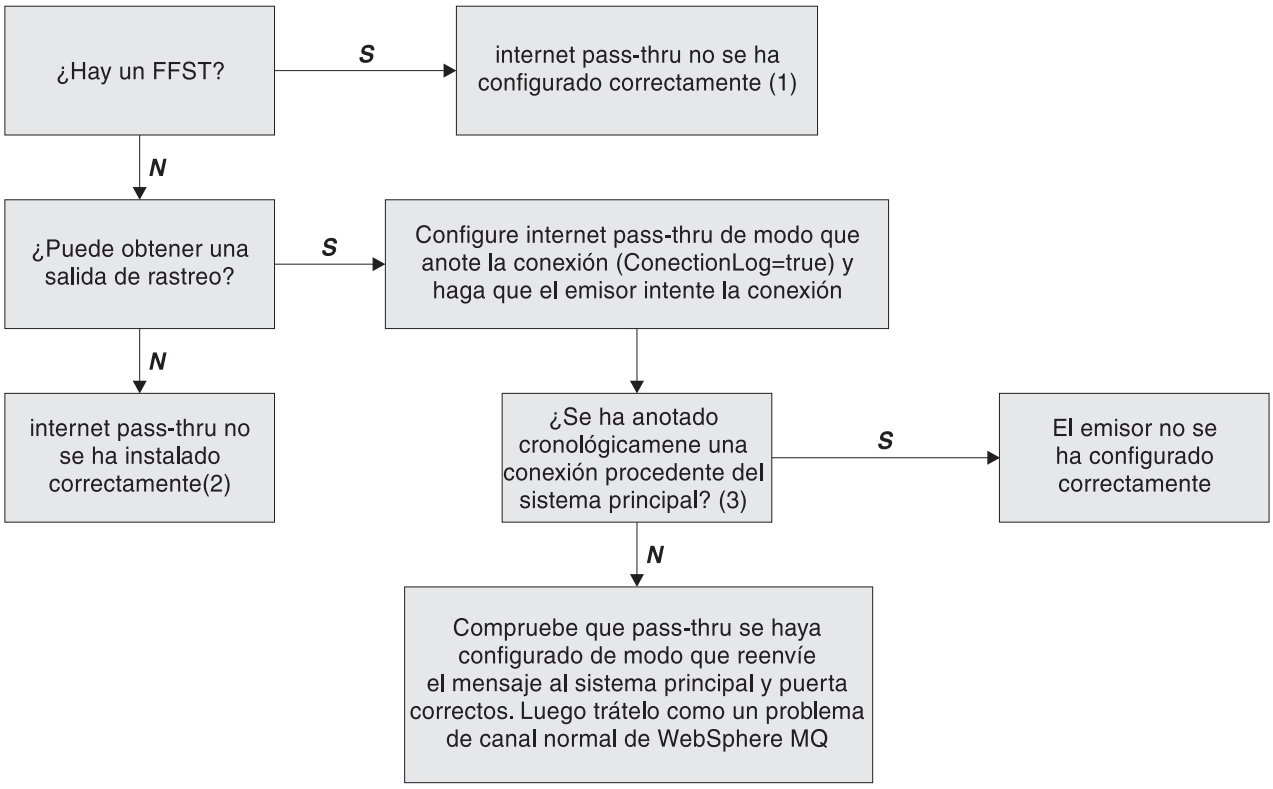

Figura 32. Diagrama de flujo de determinación de problemas

Notas:

1. Si encuentra informes FFST (en el subdirectorio de errores), puede estar seguro de que MQIPT se ha instalado correctamente. Es posible que haya habido un problema con la configuración.

   Cada informe FFST informa acerca de un problema que ha hecho que MQIPT o una ruta finalicen el proceso de arranque. Solucione el problema que ha generado los FFST. A continuación, suprima los FFST antiguos y reinicie o renueve MQIPT.
2. Si MQIPT no se ha instalado correctamente, compruebe que todos los archivos se hayan colocado en el lugar correcto y que la variable CLASSPATH se haya actualizado. Para comprobar que esto es correcto, vuelva a iniciar MQIPT manualmente.
3. Para iniciar manualmente MQIPT:

   Abra un indicador de mandatos. Vaya al subdirectorio `bin` y escriba:

   ```
   mqipt xxx
   ```

   donde *xxx* es el directorio inicial de MQIPT; en este caso es "`..`".

   Esto iniciará MQIPT y buscará la configuración en el directorio inicial. Busque los mensajes de error y los FFST en el subdirectorio `errors`.

   Compruebe si en la salida de texto de MQIPT hay mensajes de error y corrija los errores. Compruebe si hay FFST y corrija los errores. MQIPT no se iniciará si hay algún problema en la sección global del archivo de configuración. Una ruta no se iniciará si hay algún problema en la sección de ruta del archivo de configuración.

Inicio automático de internet pass-thru

Si instala MQIPT como un servicio de Windows NT y tiene que cambiar su arranque a modalidad automática, se iniciará cuando se inicie el sistema. Siempre inicie MQIPT manualmente una vez antes de intentar instalar MQIPT como un servicio de Windows NT para asegurarse de que la instalación se haya realizado correctamente. Consulte el apartado "Utilización de un programa de control de servicios de Windows" en la página 31 para obtener información detallada.

Si recibe un mensaje de error en el que se indica que no se ha podido localizar la DLL, está utilizando el programa `mqiptService` incorrecto o no ha configurado la variable de entorno PATH del sistema correctamente. La variable PATH debe contener la ubicación de las bibliotecas de tiempo de ejecución JNI. Este archivo (`jvm.dll`) se puede encontrar en el subdirectorio cliente de JDK.

Comprobación de la conectividad de extremo a extremo

Si se instala MQIPT correctamente, el paso siguiente es comprobar que las rutas se hayan establecido correctamente.

En el archivo de configuración, `mqipt.conf`, establezca la propiedad `ConnectionLog` en true. Inicie o renueve MQIPT e intente una conexión. Las anotaciones de conexión se crean en el subdirectorio logs del directorio inicial. Si no se crea, ya sabe que MQIPT no se ha instalado correctamente. Si no se registran intentos de conexión, el emisor no se ha establecido correctamente. Si se registran los intentos, compruebe que MQIPT esté enviando los mensajes a la dirección correcta.

Errores de rastreo

MQIPT proporciona un recurso de rastreo de ejecución detallado, que se controla mediante el atributo de rastreo. Cada ruta se puede rastrear de forma independiente. Los archivos de rastreo se graban en el directorio *xxx*`\errors` (donde *xxx* es el directorio que contiene `mqipt.conf`). Cada archivo de rastreo tiene un nombre con el formato siguiente:

`iptroute`*nnnnn*`.trc`

donde *nnnnn* es el número de puerta en la que está escuchando la ruta. La salida de rastreo de las hebras que no están asociadas directamente con una ruta determinada (por ejemplo, la entrada del mandato de manejo de hebras) se graba en un archivo diferente llamado `iptmain.trc`.

Los errores fatales inesperados se graban como registros FFST en un archivo de anotaciones de error, situado en el directorio *xxx*`\errors` (donde *xxx* es el directorio que contiene `mqipt.conf`). Los archivos FFST tienen el formato siguiente:

`ipt`*xxx*`.FFST`

donde *xxx* es la secuencia en que se ha generado el FFST (1 es el más antiguo). En un sistema de ejecución prolongada, puede alcanzar el número máximo que puede generar el sistema. En este caso, los FFST que se generan se graban en el archivo `mqipt0.FFST`. Si se crea el archivo `mqipt0.FFST`, debe detener y reiniciar MQIPT lo antes posible y suprimir los archivos antiguos.

Informe de problemas

Si tiene que informar acerca de un problema al centro de servicio de IBM, proporcione la información siguiente para que puedan ayudarle a resolver el problema con más rapidez:

- Proporcione un sencillo de diagrama de red de las máquinas que se utilizan, incluidas las direcciones IP.
- Si se está utilizando más de un MQIPT, sincronice el reloj del sistema en cada máquina MQIPT, de este modo, las entradas de rastreo serán coincidentes en cada MQIPT.
- Borre los archivos de rastreo antiguos.
- Ejecute el cliente para generar el problema, de modo que los archivos de rastreo solamente contengan una instancia del problema.
- Envíe una copia de todos los archivos .trc y .log de MQIPT.

Ajuste del rendimiento

Los siguientes son indicadores útiles para el ajuste del sistema.

Gestión de la agrupación de hebras

El rendimiento relativo de cada ruta se puede ajustar mediante una combinación de una agrupación de hebras y una especificación de tiempo excedido de conexión desocupada.

Hebras de conexión

A toda ruta MQIPT se le asigna una agrupación de hebras que se ejecutan al mismo tiempo y que manejan peticiones de comunicaciones de entrada. Durante la inicialización, se crea una agrupación de hebras (del tamaño especificado en el atributo de hebra `MinConnectionThreads`) y se asigna una hebra para que maneje la primera petición de entrada. Cuando se recibe esta petición, se establece la hebra para que maneje de forma inmediata la petición y la hebra siguiente queda asignada como preparada para la petición de entrada siguiente. Cuando se ha asignado trabajo a todas las hebras, se crea una nueva hebra, se añade a la agrupación y se le asigna trabajo. De este modo, la agrupación crece hasta que se alcanza el valor de `MaxConnectionThreads`. Cuando el número de hebras en ejecución alcanza el valor de `MaxConnectionThreads`, la petición de entrada siguiente espera a que se vuelva a liberar una hebra de la agrupación que hay en ejecución. Esta es la capacidad máxima de trabajo de la hebra, superada la cual ya no se pueden aceptar peticiones adicionales. Cuando finaliza una conversación o cuando ha transcurrido el período de tiempo de espera de conexión desocupada, se pueden volver a liberar hebras para la agrupación.

Tiempo de espera de conexión desocupada

Por omisión, las hebras en ejecución no se finalizan porque no haya actividad. Cuando una hebra se asigna a una conversación, permanece asignada a dicha conversación hasta que se cierra con normalidad, se desactiva la ruta o se concluye MQIPT. Opcionalmente, se puede especificar un intervalo de tiempo de espera de conexión desocupada, por el que se finaliza cualquier hebra que esté inactiva durante el período de tiempo especificado (en minutos). Una hebra de supervisión comprueba con regularidad los períodos de tiempo de conexión desocupada y finaliza las que han sobrepasado el umbral. Las hebras se reciclan y se vuelven a colocar en la agrupación de trabajo.

Capítulo 12. Mensajes

Cuando se ejecuta desde la línea de mandatos, MQIPT muestra un número reducido de mensajes informativos y de error en la consola, solamente en inglés de Estados Unidos.

Tenga en cuenta que:

- Los mensajes MQCAxxxx son los mensajes del cliente de administración.
- Los mensajes MQCPxxxx son mensajes de MQIPT.
- Los mensajes MQCxIxxx son mensajes informativos.
- Los mensajes MQCxExxx son mensajes de error.

MQCAE001 Unknown host: {0}

Explicación: No se puede encontrar el sistema principal MQIPT.

Respuesta del Usuario: Compruebe que haya especificado correctamente el nombre del sistema principal donde está ubicado MQIPT.

MQCAE002 The following error was reported by the system: {0}

Explicación: Se ha producido un error. Se ha informado acerca de un error producido después de un mandato del sistema.

MQCAE005 No valid destination address has been defined

Explicación: Al añadir una ruta, el campo de destino se ha dejado en blanco.

Respuesta del Usuario: Escriba una dirección de destino válida.

MQCAE006 No valid destination port has been defined

Explicación: Al añadir una ruta, el campo de dirección de puerta de destino se ha dejado en blanco.

Respuesta del Usuario: Escriba una dirección de puerta de destino válida.

MQCAE007 No valid listener port has been defined

Explicación: Al añadir una ruta, el campo de dirección de puerta de escucha se ha dejado en blanco.

Respuesta del Usuario: Escriba una dirección de puerta de escucha válida, con un valor entre 1 y 65535.

MQCAE008 No valid network address has been defined

Explicación: Al añadir un MQIPT, el campo de dirección de red se ha dejado en blanco.

Respuesta del Usuario: Escriba una dirección de red válida.

MQCAE009 No valid command port has been defined

Explicación: Al añadir un MQIPT, se ha utilizado una dirección de puerta de mandatos que no era válida.

Respuesta del Usuario: Escriba una dirección de puerta de mandatos que sea válida, con un valor entre 1 y 65535.

MQCAE010 Could not show online help

Explicación: El archivo para la ayuda en línea estaba disponible pero no se ha podido visualizar.

Respuesta del Usuario: Asegúrese de que Acrobat Reader esté disponible en la variable PATH del sistema.

MQCAE011 Could not parse parameter

Explicación: Se ha producido un error interno que ha hecho que se intentara actualizar un parámetro no existente en la tabla.

Respuesta del Usuario: Si el error continúa, póngase en contacto con el servicio de soporte técnico de IBM.

MQCAE012 Could not find file for online help

Explicación: No se ha podido encontrar el archivo ″guiadmin.pdf″.

Respuesta del Usuario: Asegúrese de que este archivo esté accesible en el subdirectorio doc.

© Copyright IBM Corp. 2000-2002

MQCAE013 Interrupted while trying to show online help

Explicación: Se ha producido un error del sistema cuando se visualizaba la ayuda en línea.

Respuesta del Usuario: Vuelva intentarlo. Si el error continúa, póngase en contacto con el servicio de soporte técnico de IBM.

MQCAE015 The password you have just entered has not been recognized

Explicación: MQIPT espera una contraseña válida, la que ha utilizado para el último mandato no es correcta. Debe coincidir con la que está definida en el archivo de configuración.

Respuesta del Usuario: Cambie la contraseña utilizando el panel **MQIPT->Conexión** y vuelva a intentar el último mandato.

MQCAE016 Node mismatch

Explicación: Hay una incoherencia interna entre el nodo seleccionado en el árbol y los datos que contiene la memoria.

Respuesta del Usuario: Cierre el cliente de administración y vuelva a intentar el mandato. Si el error continúa, póngase en contacto con el servicio de soporte técnico de IBM.

´MCAE017 Could not create NLS text for message {0}

Explicación: No se ha encontrado texto NLS para el número de mensaje definido.

Respuesta del Usuario: Es posible que el archivo ″guiadmin.properties″ esté dañado y que no se encuentre el número de mensaje especificado. Compruebe lo siguiente:

- El archivo Readme por si hay un mensaje nuevo.
- Que el archivo ″guideadmin.jar″ esté en la variable CLASSPATH del sistema.
- Que el archivo ″guideadmin.properties″ esté en el archivo ″guideadmin.jar″.
- Que el número de mensaje esté en el archivo ″guideadmin.properties″.

MQCAE018 Could not create NLS text for message MQCAE017

Explicación: El número de mensaje {0} no se ha podido encontrar en la lista de propiedades del sistema.

Respuesta del Usuario: Es posible que el archivo ″guideadmin.properties″ esté dañado. Compruebe lo siguiente:

- Que el archivo ″guideadmin.jar″ esté en la variable CLASSPATH del sistema.
- Que el archivo ″guideadmin.properties″ esté en el archivo ″guideadmin.jar″.
- Que el número de mensaje esté en el archivo ″guideadmin.properties″.

MQCAE019 You have failed to repeat your proposed new password

Explicación: Al cambiar la contraseña, no se ha entrado dos veces para su verificación.

Respuesta del Usuario: Vuelva a escribir la contraseña en el campo correspondiente.

MQCAE020 Failed to change MQIPT access parameters

Explicación: Se ha detectado un error interno cuando se intentaban cambiar los parámetros de acceso de MQIPT.

Respuesta del Usuario: Cierre el cliente de administración y vuelva a intentar el mandato. Si el error continúa, póngase en contacto con el servicio de soporte técnico de IBM.

MQCAE021 Internal failure to identify MQIPT

Explicación: Se ha detectado un error interno cuando se intentaba guardar un archivo de configuración en un MQIPT.

Respuesta del Usuario: Cierre el cliente de administración y vuelva a intentar el mandato. Si el error continúa, póngase en contacto con el servicio de soporte técnico de IBM.

MQCAE022 Internal failure to save MQIPT configuration

Explicación: Se ha detectado un error interno cuando se intentaba guardar un archivo de configuración en un MQIPT.

Respuesta del Usuario: Cierre el cliente de administración y vuelva a intentar el mandato. Si el error continúa, póngase en contacto con el servicio de soporte técnico de IBM.

MQCAE023 MQIPT {0} did not recognize your password.

Explicación: MQIPT espera una contraseña válida, la que ha utilizado para el último mandato no es correcta. Debe coincidir con la que está definida en el archivo de configuración.

Respuesta del Usuario: Cambie la contraseña utilizando el panel del menú **MQIPT->Conexión** y vuelva a intentar el mandato.

MQCAE024 MQIPT {0} has not recognized the command.

Explicación: El cliente de administración ha enviado un mandato a MQIPT, que éste no ha reconocido.

Respuesta del Usuario: Asegúrese de que la versión del código que utiliza el cliente de administración sea la misma que la de MQIPT.

MQCAE025 MQIPT {0} has failed to send configuration file.

Explicación: MQIPT ha intentado enviar el archivo de configuración, pero ha fallado.

Respuesta del Usuario: Cierre el cliente de administración y vuelva a intentar el mandato. Si no funciona, detenga y reinicie MQIPT.

MQCAE026 Remote shutdown is disabled on MQIPT {0}.

Explicación: Un intento de conclusión de MQIPT de forma remota no se ha ejecutado correctamente debido a que no estaba habilitada la conclusión remota en el archivo de configuración.

Respuesta del Usuario: Para habilitar la conclusión remota de MQIPT, edite el archivo de configuración y establezca la propiedad RemoteShutDown en true.

MQCAE027 Look and feel {0} is not supported.

Explicación: No está disponible el aspecto recomendado para la plataforma que está utilizando.

Respuesta del Usuario: El proceso continúa con el aspecto por omisión del sistema.

MQCAE028 Look and feel class {0} cannot be found.

Explicación: No está disponible el aspecto recomendado para la plataforma que está utilizando.

Respuesta del Usuario: El proceso continúa con el aspecto por omisión del sistema.

MQCAE029 Minimum Connection Threads must be non-negative and no bigger than Maximum Connection Threads

Explicación: El valor de Mínimo de hebras de conexión debe ser menor o igual que el valor de Máximo de hebras de conexión.

Respuesta del Usuario: Cambie el valor como corresponda.

MQCAE030 Maximum Connection Threads must be greater than zero and at least as big as Minimum Connection Threads

Explicación: El valor de Máximo de hebras de conexión debe ser mayor que el valor de Mínimo de hebras de conexión.

Respuesta del Usuario: Cambie el valor como corresponda.

MQCAE031 Port numbers must be in the range 0 to 65535

Explicación: Está intentando establecer un valor que no cumple con la especificación.

Respuesta del Usuario: Cambie el valor como corresponda.

MQCAE032 Trace must be in the range 0 to 5

Explicación: Está intentando establecer un valor que no cumple con la especificación.

Respuesta del Usuario: Cambie el valor como corresponda.

MQCAE033 Max Log file size must be in the range 5 to 50

Explicación: Está intentando establecer un valor que no cumple con la especificación.

Respuesta del Usuario: Cambie el valor como corresponda.

MQCAE049 No route has been selected on any MQIPT

Explicación: Se ha intentado suprimir una ruta sin seleccionar antes la ruta que debe suprimirse.

Respuesta del Usuario: Seleccione una ruta y vuelva a intentar el mandato.

MQCAE050 Could not connect to MQIPT {0}

Explicación: El cliente de administración no se ha podido conectar con el MQIPT especificado.

Respuesta del Usuario: Esto puede ser debido a una de las causas siguientes:

- MQIPT no está ejecutándose.
- MQIPT no está escuchando en su puerta de mandatos.
- Sólo un cliente de administración está utilizando la puerta de mandatos de MQIPT.
- La petición ha sobrepasado el tiempo de espera.

MQCAE051 Could not read reply from MQIPT {0}

Explicación: Se ha recibido una respuesta desde MQIPT que no se ajustaba al protocolo esperado.

Respuesta del Usuario: Asegúrese de que la versión del código que utiliza el cliente de administración sea la misma que la de MQIPT.

MQCAE052 Configuration has not been saved

Explicación: Se ha recibido una respuesta válida de MQIPT pero posteriormente no ha podido guardar el archivo de configuración.

Respuesta del Usuario: Compruebe que MQIPT tenga acceso de escritura en el archivo de configuración.

MQCAE053 MQIPT has not confirmed saving of configuration

Explicación: Se ha enviado el archivo de configuración a MQIPT pero MQIPT no lo ha reconocido.

Respuesta del Usuario: Esto puede ser debido a una de las causas siguientes:

- MQIPT no está ejecutándose.
- MQIPT no está escuchando en su puerta de mandatos.
- Sólo un cliente de administración está utilizando la puerta de mandatos de MQIPT.
- La petición ha sobrepasado el tiempo de espera.

MQCAE054 MQIPT data has not been refreshed

Explicación: Se ha establecido contacto con MQIPT pero el cliente de administración no ha podido leer el archivo de configuración.

Respuesta del Usuario: Esto puede ser debido a una de las causas siguientes:

1. MQIPT no se ha podido ejecutar correctamente.
2. La petición ha sobrepasado el tiempo de espera.

MQCAE055 No MQIPT or route on an MQIPT has been selected

Explicación: Ha seleccionado una opción de menú que no puede llevarse a cabo debido a que no se ha seleccionado un MQIPT ni una ruta.

Respuesta del Usuario: Seleccione una ruta o un MQIPT correctos y vuelva a intentarlo.

MQCAE056 Duplicate listener port has been rejected

Explicación: La puerta de escucha seleccionada se ha rechazado porque ya la está utilizando otra ruta.

Respuesta del Usuario: Seleccione una puerta de escucha diferente y vuelva a intentarlo.

MQCAI002 The MQIPT has been removed from display

Explicación: El MQIPT cuyo nodo ha seleccionado en el árbol se ha suprimido de la memoria del cliente.

MQCAI003 New route added to the display

Explicación: La nueva ruta que acaba de especificar se ha añadido al MQIPT actual.

MQCAI004 Route has been removed from the display

Explicación: La ruta que ha seleccionado en el árbol se ha suprimido de la memoria del cliente.

MQCAI005 Selected MQIPT is being displayed

Explicación: Los parámetros globales del MQIPT que ha seleccionado en el árbol se están visualizando en la tabla.

MQCAI006 Selected route is being displayed

Explicación: Los parámetros globales de la ruta que ha seleccionado en el árbol se están visualizando en la tabla.

MQCAI007 Client configuration has been saved

Explicación: Los parámetros de acceso para todos los MQIPT del árbol se han guardado.

MQCAI008 Display of online help succeeded

Explicación: La ayuda en línea se está visualizando como se había solicitado.

MQCAI009 Table has been updated

Explicación: El valor que acaba de entrar en la tabla se ha utilizado para actualizar el modelo que hay en la memoria.

MQCAI010 No MQIPT or route has been selected.

Explicación: No se lleva a cabo ninguna acción porque no hay información suficiente sobre dónde actuar.

MQCAI011 User Action has been cancelled

Explicación: Ha cancelado una acción iniciada anteriormente mediante una ventana emergente.

MQCAI014 Configuration has been saved on MQIPT

Explicación: Se ha guardado un archivo de configuración nuevo en el MQIPT que está seleccionado actualmente en el árbol y se ha utilizado para reiniciar MQIPT.

MQCAI015 Online help has terminated

Explicación: Se ha visualizado la ayuda en línea tal y como se había solicitado y, a continuación, se ha cerrado.

MQCAI017 Select File/Add MQIPT to add an MQIPT to the tree

Explicación: Este mensaje aparece cuando no hay ningún MQIPT en el árbol. Indica que debe añadir uno.

MQCAI018 New MQIPT added to display

Explicación: Se ha añadido un MQIPT nuevo tal y como se había indicado.

MQCAI019 MQIPT access parameters have been changed

Explicación: Se han modificado los parámetros de acceso del MQIPT que actualmente está seleccionado en el árbol.

MQCAI021 Select an MQIPT or route on the tree to display its contents

Explicación: Este mensaje aparece cuando no se muestra información en la tabla y le indica cómo puede visualizarla.

MQCAI022 The command port has changed

Explicación: Se ha solicitado que se modificara la puerta de mandatos de un MQIPT y la acción se ha llevado a cabo.

MQCAI023 The password has changed

Explicación: Para las comunicaciones futuras con el MQIPT que acaba de modificar debe utilizar la nueva contraseña.

MQCAI025 MQIPT {0} has been refreshed.

Explicación: La información que contiene el MQIPT se ha actualizado mediante la lectura de su archivo de configuración.

MQCAI026 MQIPT {0} has received shutdown request.

Explicación: El MQIPT ha reconocido que ha recibido una petición de conclusión y ahora concluirá.

MQCAI027 Client configuration has been refreshed

Explicación: La información que aparece en el cliente de administración se ha renovado a partir del archivo ″client.conf″ local.

MQCAI028 MQIPT {0} is active

Explicación: El MQIPT ha respondido satisfactoriamente a una solicitud ping.

MQCAI029 MQIPT {0} is not active

Explicación: El MQIPT no ha respondido a una solicitud ping dentro del tiempo especificado.

Respuesta del Usuario: Esto puede ser debido a una de las causas siguientes:

- MQIPT no está ejecutándose.
- MQIPT no está escuchando en su puerta de mandatos.
- La petición ha sobrepasado el tiempo de espera. El tiempo de espera se puede aumentar modificando la propiedad de tiempo excedido (timeout) en la información de conexión de MQIPT.

MQCAI030 Route {0} is active

Explicación: El MQIPT ha respondido satisfactoriamente a una solicitud ping.

MQCAI031 Route {0} is not active

Explicación: La ruta de MQIPT no ha respondido a una solicitud ping dentro del tiempo especificado.

Respuesta del Usuario: Esto puede ser debido a una de las causas siguientes:

- MQIPT no está ejecutándose.
- MQIPT no está escuchando en su puerta de mandatos.
- La petición ha sobrepasado el tiempo de espera. El tiempo de espera se puede aumentar modificando la propiedad de tiempo excedido (timeout) en la información de conexión de MQIPT.

MQCAI100 This script is used to start the Administration Client for {0}. Specifying a SOCKS proxy will allow the Administrator Client to talk to an MQIPT through a firewall.

Explicación: Información de ayuda en línea para el script mqiptGui.

MQCAI101 Format of command is:

Explicación: Información de ayuda en línea para el script mqiptGui.

MQCAI102 mqiptGui {socks_host{socks_port}}

Explicación: Información de ayuda en línea para el script mqiptGui.

MQCAI103 socks_host-host name of SOCKS proxy (optional)

Explicación: Información de ayuda en línea para el script mqiptGui.

MQCAI104 socks_port-SOCKS proxy port address (optional-default 1080)

Explicación: Información de ayuda en línea para el script mqiptGui.

MQCPE000 Could not locate message data when handling message {0}

Explicación: El número de mensaje {0} no se ha podido encontrar en la lista de propiedades del sistema.

Respuesta del Usuario: El archivo ″mqipt.properties″ está dañado y no se ha encontrado el número de mensaje especificado. Compruebe lo siguiente:

- Que el archivo ″MQipt.jar″ esté en la variable CLASSPATH del sistema.
- Que el archivo ″mqipt.properties″ esté en el archivo ″MQipt.jar″.
- Que el número de mensaje esté en el archivo ″mqipt.properties″.

MQCPE001 Directory does not exist or is not a directory

Explicación: Durante la inicialización, no se ha podido encontrar un directorio necesario. Este mensaje hace referencia a un directorio especificado en el archivo de configuración MQIPT, mqipt.conf o en las opciones de arranque de línea de mandatos de MQIPT del directorio por omisión.

Respuesta del Usuario: Especifique el directorio correcto y vuelva a intentar el mandato.

MQCPE004 Route startup failed on port {0}

Explicación: No se ha podido iniciar la ruta con el número de ListenerPort especificado.

Respuesta del Usuario: Se ha producido un error de E/S durante el arranque de la ruta. Compruebe si hay otros mensajes de error y registros de anotaciones adyacentes para obtener información adicional acerca del problema.

MQCPE005 The configuration file {0} could not be found

Explicación: No se ha podido encontrar el archivo de configuración de MQIPT ″mqipt.conf″ en el directorio especificado.

Respuesta del Usuario: Especifique el directorio correcto y vuelva a intentar el mandato.

MQCPE006 The number of routes has exceeded {0}. MQIPT will start but this configuration is unsupported.

Explicación: La configuración ha sobrepasado el número máximo soportado de rutas para una instancia de MQIPT. La operación no se detendrá pero es posible que como resultado el sistema se sobrecargue o presente alguna inestabilidad. No se dará soporte a las configuraciones que sobrepasen el número máximo de rutas indicado.

Respuesta del Usuario: Puede iniciar instancias adicionales de MQIPT que contengan menos rutas por instancia.

MQCPE007 Route not restarted on listener port {0}

Explicación: En una operación REFRESH, la ruta que estaba funcionando en el ListenerPort especificado no se ha reiniciado en la nueva configuración.

Respuesta del Usuario: Compruebe si hay otros mensajes de error para obtener información adicional acerca del problema.

MQCPE008 Duplicate route defined for listener port {0}

Explicación: Se ha definido más de una ruta con el mismo valor de ListenerPort.

Respuesta del Usuario: Suprima la ruta duplicada del archivo de configuración y vuelva a intentar el mandato.

MQCPE009 LogPath parameter {0} is not valid.

Explicación: La vía de acceso de anotaciones que se muestra en el texto no existe o no está accesible en este momento.

Respuesta del Usuario: Compruebe que exista el directorio y que MQIPT pueda acceder al mismo.

MQCPE010 Listener or command port number {0} is not valid

Explicación: El número de puerta proporcionado para el parámetro de puerta de mandatos o de puerta de escucha no es válido.

Respuesta del Usuario: Especifique un número de puerta válida que esté libre para poder utilizarla. Para obtener ayuda sobre cómo utilizar los números de puertas de la red, consulte al administrador de la red.

MQCPE011 The trace level {0} is outside the valid range 0 - 5

Explicación: Se ha solicitado la opción de rastreo especificada pero no estaba dentro del rango válido de 0-5.

Respuesta del Usuario: Especifique un valor de rastreo de 0–5.

MQCPE012 The value {0} is not valid for the attribute {1}

Explicación: Se ha especificado un valor de propiedad no válido.

Respuesta del Usuario: Consulte esta guía del usuario para obtener detalles adicionales sobre los valores válidos para cada parámetro de control.

MQCPE013 ListenerPort property was not found in route {0}

Explicación: MQIPT ha detectado una ruta en el archivo de configuración que no contiene una propiedad de ListenerPort. La propiedad ListenerPort es el identificador principal y exclusivo para cada ruta y, por lo tanto, es obligatorio.

Respuesta del Usuario: Especifique un valor de ListenerPort válido para la ruta especificada.

MQCPE014 ListenerPort property value {0} is not valid

Explicación: Se ha especificado una dirección de puerta no válida para la propiedad ListenerPort de una ruta.

Respuesta del Usuario: Una dirección de puerta debe estar dentro del rango de 1024–65535. Compruebe cada ListenerPort en el archivo de configuración.

MQCPE015 No text was found for message number {0}

Explicación: Se ha encontrado un error interno para el que no hay disponible una descripción.

Respuesta del Usuario: El archivo ″mqipt.properties″ está dañado y no se ha encontrado el número de mensaje especificado. Compruebe lo siguiente:

- El archivo Readme por si hay un mensaje nuevo.
- Que el archivo ″MQipt.jar″ esté en la variable CLASSPATH del sistema.
- Que el archivo ″mqipt.properties″ esté en el archivo ″MQipt.jar″.
- Que el número de mensaje esté en el archivo ″mqipt.properties″.

MQCPE016 The maximum number of connection threads is {0} but this is less than the minimum number of connection threads, which is {1}

Explicación: Su configuración ha especificado el número mínimo de hebras de conexión con un valor que supera el número máximo de hebras de conexión.

Respuesta del Usuario: Esto puede ser un error en una sola ruta, un conflicto entre una propiedad global y una propiedad de ruta que altere temporalmente los valores por omisión del sistema. Consulte los capítulos anteriores de esta guía del usuario para obtener información detallada acerca de los valores válidos y los valores por omisión aplicables.

MQCPE017 The exception {0} was thrown, causing MQIPT to shut down

Explicación: MQIPT ha finalizado de forma anormal y se ha concluido. Esto puede ser debido a limitaciones o condiciones del entorno del sistema como, por ejemplo, un desbordamiento de la memoria.

Respuesta del Usuario: Si el error continúa, póngase en contacto con el servicio de soporte técnico de IBM.

MQCPE018 The ListenerPort property is blank - the route will not start

Explicación: Se ha omitido el número de ListenerPort en una ruta.

Respuesta del Usuario: Edite el archivo de configuración y añada un ListenerPort válido.

MQCPE019 The stanza {0} was not found before the following: {1}

Explicación: Se ha producido un error de secuencia en el archivo de configuración.

Respuesta del Usuario: Edite el archivo de configuración y asegúrese de que todas las entradas [route] vayan después de las entradas [global].

MQCPE020 The new value for MaxConnectionThreads is {0}. This must be greater than the current value {1}

Explicación: Una vez iniciada la ruta, la propiedad MaxConnectionThread sólo puede aumentarse.

Respuesta del Usuario: Edite el archivo de configuración y cambie la propiedad MaxConnectionThread.

MQCPE021 The property Destination was not supplied for route {0}

Explicación: El destino de la propiedad en una ruta es obligatorio, pero se ha omitido en la ruta especificada.

Respuesta del Usuario: Edite el archivo de configuración y añada una propiedad de destino para la ruta especificada.

MQCPE022 The CommandPort value {0} is outside the valid range 1 - 65535.

Explicación: La propiedad CommandPort estaba fuera del rango de 1-65535.

Respuesta del Usuario: Edite el archivo de configuración y cambie la propiedad CommandPort por una dirección de puerta válida.

MQCPE023 Request for shutdown from Administration Client {0} is ignored because it is disabled.

Explicación: Un intento de conclusión de MQIPT de forma remota no se ha ejecutado correctamente debido a que no estaba habilitada la conclusión remota en el archivo de configuración.

Respuesta del Usuario: Para habilitar la conclusión remota de MQIPT, edite el archivo de configuración y establezca la propiedad RemoteShutDown en true.

MQCPE024 The command received by the MQIPT controller has not been recognized.

Explicación: MQIPT ha recibido un mandato que no reconoce a través de su puerta de mandatos.

Respuesta del Usuario: Compruebe en el archivo ″mqipt.log″ la identidad del mandato.

MQCPE025 Failed to connect to server on host {0}, port {1}.

Explicación: El cliente de administración de modalidad de línea (no de GUI) no se ha podido comunicar con MQIPT.

Respuesta del Usuario: Asegúrese de que se haya especificado la propiedad CommandPort como {1} en el archivo de configuración y que MQIPT esté ejecutándose en {0}.

MQCPE026 No reply received from server on host {0}, port {1}.

Explicación: El cliente de administración de modalidad de línea (no de GUI) se ha conectado con MQIPT pero no ha recibido ninguna respuesta.

Respuesta del Usuario: Esto indica que la petición ha sobrepasado el tiempo de espera o que MQIPT tiene algún problema.

MQCPE027 Reply from MQIPT not recognized.

Explicación: El cliente de administración de modalidad de línea (no de GUI) ha recibido una respuesta de MQIPT que no reconoce.

Respuesta del Usuario: Compruebe que el script mqiptAdmin esté utilizando la misma versión del archivo ″MQipt.jar″ que MQIPT.

MQCPE028 Invalid stanza detected: {0}

Explicación: Se ha encontrado una sección no reconocida en el archivo de configuración.

Respuesta del Usuario: Solamente son válidas las secciones [global] y [route] en el archivo de configuración.

MQCPE029 Was not able to flush log output.

Explicación: Es posible que algunos mensajes no se hayan grabado en las anotaciones debido a que el almacenamiento intermedio no se ha podido vaciar.

Respuesta del Usuario: Compruebe si hay un disco de directorio inicial de MQIPT que no esté lleno y si MQIPT sigue teniendo acceso al subdirectorio de las anotaciones.

MQCPE030 {0} not found in CLASSPATH.

Explicación: El archivo jar especificado no se ha encontrado en la variable de entorno CLASSPATH.

Respuesta del Usuario: Añada el archivo especificado a la variable CLASSPATH del sistema.

MQCPE031 {0} class not found.

Explicación: Este mensaje se genera cuando se visualiza el número de versión de MQIPT. La clase especificada no se ha podido encontrar en el archivo jar de MQIPT o la variable de entorno CLASSPATH del sistema está dañada.

Respuesta del Usuario: Compruebe que el archivo de clase especificado esté en el archivo ″MQipt.jar″ y que

el archivo ″MQipt.jar″ esté en la variable CLASSPATH del sistema.

MQCPE033 Failed to send configuration file to Administration Client at {0}

Explicación: Se ha producido un error al enviar el archivo de configuración al cliente de administración.

Respuesta del Usuario: Compruebe que el archivo de configuración esté en el directorio inicial de MQIPT y que otro proceso no esté compartiéndolo.

MQCPE034 Administration Client at {0} did not supply the correct password.

Explicación: La propiedad AccessPW del archivo de configuración no coincide con la que ha proporcionado el cliente de administración.

Respuesta del Usuario: Cambie la propiedad AccessPW en el archivo de configuración o la contraseña guardada en el cliente de administración.

MQCPE035 Failed to start command listener on port {0}

Explicación: Se ha producido un error de E/S al iniciar el escucha de mandatos en la dirección de puerta especificada.

Respuesta del Usuario: Compruebe en el archivo de configuración la dirección de la puerta especificada para la propiedad CommandPort.

MQCPE038 MQIPT has not started as expected

Explicación: Este mensaje lo genera el proceso mqiptFork que inicia MQIPT como un servicio del sistema.

Respuesta del Usuario: Consulte las anotaciones de error para obtener más información. Puede intentar aumentar el tiempo de inactividad que utiliza IPTFork antes de que compruebe si MQIPT está ejecutándose. Edite el script mqiptFork y aumente el parámetro que se pasa a IPTFork.

MQCPE039 I/O error occurred running mqipt script

Explicación: Se ha producido un error al iniciar MQIPT desde el proceso fork.

Respuesta del Usuario: Compruebe si la variable de entorno PATH contiene la ubicación de JDK y si el script mqipt tiene autorización de ejecución.

MQCPE040 Interruption occurred running mqipt script

Explicación: Se ha producido un error después de iniciar MQIPT desde el proceso Fork.

Respuesta del Usuario: Consulte las anotaciones de error para obtener más información. Si el error continúa, póngase en contacto con el servicio de soporte técnico de IBM.

MQCPE041 Unsupported level of Java - {0}

Explicación: Se ha iniciado MQIPT utilizando el nivel especificado de Java.

Respuesta del Usuario: Consulte los requisitos previos en la guía del usuario para obtener más información.

MQCPE042 There is a conflict with the following properties on route {0}:

Explicación: Hay algunas propiedades que no pueden utilizarse con otras. Este mensaje precede a la lista de propiedades que están en conflicto.

Respuesta del Usuario: Compruebe los siguientes mensajes de error y lleve a cabo la acción adecuada.

MQCPE043 ....{0} and {1}

Explicación: Las propiedades siguientes no se pueden establecer juntas a la misma hora y en la misma ruta.

Respuesta del Usuario: Edite el archivo de configuración e inhabilite una de las propiedades especificadas de la ruta especificada.

MQCPE044 {0} is only valid on the {1} operating system

Explicación: Algunas características de MQIPT solamente son válidas en determinadas plataformas.

Respuesta del Usuario: Edite el archivo de configuración e inhabilite la propiedad especificada.

MQCPE045 ....HTTP proxy name is missing

Explicación: La propiedad HTTPProxy debe establecerse si la propiedad HTTP se ha establecido en true.

Respuesta del Usuario: Edite el archivo de configuración y defina un HTTPProxy para la ruta especificada.

MQCPE046 {0} is not allowed as Pagent has failed to initialize

Explicación: Pagent es la aplicación que proporciona la calidad de servicio (QoS) para MQIPT. MQIPT no se ha podido inicializar durante el arranque y la propiedad QoS se ha establecido en true para la ruta especificada.

Respuesta del Usuario: Edite el archivo de configuración e inhabilite QoS para la ruta especificada.

MQCPE047 Pagent has failed to initialize

Explicación: Pagent es la aplicación que proporciona la calidad de servicio (QoS) para MQIPT. MQIPT no se ha podido inicializar durante el arranque.

Respuesta del Usuario: Este mensaje de error se puede ignorar si Pagent no está utilizándose, pero la propiedad QoS debe establecerse en false.

MQCPE048 Route startup failed on port {0}, exception was : {1}

Explicación: No se ha podido iniciar la ruta con el número de ListenerPort especificado.

Respuesta del Usuario: Compruebe si hay otros mensajes de error y registros de anotaciones adyacentes para obtener información adicional acerca del problema.

MQCPE049 Error starting or stopping the Java Security Manager {0}

Explicación: Se ha generado una excepción cuando se intentaba iniciar o detener el gestor de seguridad Java.

Respuesta del Usuario: El gestor de seguridad Java se había habilitado anteriormente pero los permisos de tiempo de ejecución no estaban habilitados. Añada RuntimePermission para setSecurityManager en el archivo local de políticas. MQIPT debe reiniciarse para que los cambios surtan efecto.

MQCPE050 Security exception on port {0} from the Administration Client

Explicación: Se ha generado una excepción de seguridad cuando se aceptaba una conexión del cliente de administración.

Respuesta del Usuario: El gestor de seguridad Java se había habilitado anteriormente pero no se habían otorgado los permisos para el sistema principal identificado en el mensaje de error. Para que el sistema principal pueda conectarse con MQIPT, añada un SocketPermission para aceptar o resolver conexiones en la dirección de puerta de CommandPort. El gestor de seguridad Java debe reiniciarse para que los cambios surtan efecto.

MQCPE051 Security exception accepting a connection on route {0}

Explicación: Se ha generado una excepción de seguridad al aceptar una conexión en la ruta especificada.

Respuesta del Usuario: El gestor de seguridad Java se había habilitado anteriormente pero no se habían otorgado los permisos para el sistema principal identificado en el mensaje de error. Para que el sistema principal pueda conectarse en esta ruta, añada un SocketPermission para aceptar o resolver conexiones para ListenerPort. El gestor de seguridad Java debe reiniciarse para que los cambios surtan efecto.

MQCPE052 Connection request on route {0} failed : {1}

Explicación: Este mensaje se emite en las anotaciones de conexión para registrar una excepción de seguridad para una petición de conexión.

Respuesta del Usuario: El gestor de seguridad Java se había habilitado anteriormente pero no se habían otorgado los permisos para el sistema principal identificado en el mensaje de error. Para que el sistema principal pueda conectarse en esta ruta, añada un SocketPermission para aceptar o resolver conexiones para ListenerPort. El gestor de seguridad Java debe reiniciarse para que los cambios surtan efecto.

MQCPE053 Security exception making a connection to {0}({1})

Explicación: Se ha generado una excepción de seguridad al realizar una conexión en la ruta especificada.

Respuesta del Usuario: El gestor de seguridad Java se había habilitado anteriormente pero no se habían otorgado los permisos para el sistema principal identificado en el mensaje de error. Para que el sistema principal pueda conectarse en esta ruta, añada un SocketPermission para aceptar o resolver conexiones para ListenerPort. El gestor de seguridad Java debe reiniciarse para que los cambios surtan efecto.

MQCPE054 Connection request to {0}({1}) failed : {2}

Explicación: Este mensaje se emite en las anotaciones de conexión para registrar una excepción de seguridad para una petición de conexión con un sistema principal de destino.

Respuesta del Usuario: El gestor de seguridad Java se había habilitado anteriormente pero no se habían otorgado los permisos para el sistema principal identificado en el mensaje de error. Para que el sistema principal pueda conectarse en esta ruta, añada un SocketPermission para aceptar o resolver conexiones para ListenerPort. El gestor de seguridad Java debe reiniciarse para que los cambios surtan efecto.

MQCPE055 ....Socks proxy name is missing

Explicación: La propiedad SocksProxy debe establecerse si la propiedad SocksClient se ha establecido en true.

Respuesta del Usuario: Edite el archivo de configuración y defina un SocksProxy para la ruta especificada.

MQCPE056 Conflict with route properties

Explicación: Hay algunas propiedades que no pueden utilizarse con otras.

Respuesta del Usuario: Consulte los mensajes de la consola para obtener información detallada acerca del error y llevar a cabo la acción adecuada.

MQCPE057 Connection from {0} to host {1} closed - the SSL protocol ({2})was not recognized

Explicación: La ruta se ha establecido en modalidad de proxy SSL y no se ha reconocido el flujo de datos inicial.

Respuesta del Usuario: Asegúrese de que solamente se estén realizando conexiones SSL en esta ruta.

MQCPI001 {0} starting

Explicación: Esta instancia de MQIPT está iniciando su ejecución. Posteriormente se visualizarán mensajes de inicialización adicionales.

MQCPI002 {0} shutting down

Explicación: Se va a concluir MQIPT. Esto puede ser el resultado de un mandato STOP o puede ser una acción automática si un error de configuración impide que se lleve a cabo correctamente una acción de arranque o una acción REFRESH.

MQCPI003 {0} shutdown complete

Explicación: El proceso de conclusión ha finalizado. Todos los procesos de MQIPT han finalizado.

MQCPI004 Reading configuration information from {0}

Explicación: Se está leyendo el archivo de configuración de MQIPT, mqipt.conf, desde el directorio que se describe en este mensaje.

MQCPI005 Listener port specified as not active - {0} -> {1}({2})

Explicación: La ruta a la que se hace referencia en el mensaje se ha marcado como inactiva. En esta ruta no se aceptarán peticiones de comunicación.

MQCPI006 Route {0} has started and will forward messages to:

Explicación: Se ha iniciado una ruta en la puerta de escucha que se muestra en este mensaje. Posteriormente se visualizarán otros mensajes que listarán las propiedades asociadas a esta ruta.

MQCPI007 Route stopped on port {0}

Explicación: Se está concluyendo la ruta que estaba operando en la ListenerPort especificada. Normalmente, esta acción se lleva a cabo cuando se emite un mandato REFRESH para MQIPT y se ha modificado la configuración de la ruta.

MQCPI008 Listening for control commands on port {0}

Explicación: Esta instancia de MQIPT está escuchando los mandatos de control de la puerta especificada.

MQCPI009 Control command received: {0}

Explicación: Este mensaje indica que se ha recibido un mandato de control en la puerta de mandatos. Siempre que es aplicable, se incluyen los detalles en el mensaje.

MQCPI010 Stopping command port on {0}

Explicación: En una operación REFRESH, la puerta de mandatos ya no se está utilizando en la configuración nueva. Los mandatos ya no se aceptarán en la puerta especificada.

MQCPI011 The path {0} will be used to store the log files

Explicación: La salida de las anotaciones se dirigirá a la ubicación descrita en este mensaje, bajo la configuración actual.

Respuesta del Usuario: Esto puede ser diferente si se modifica la configuración y se solicita una operación REFRESH.

MQCPI012 Changing the value of MinConnectionThreads has no effect after the route is started

Explicación: El número mínimo se hebras de conexión se asigna cuando se arranca la ruta y no se puede modificar hasta que se reinicia MQIPT.

MQCPI013 Connection from {0} to host {1} closed

Explicación: Este mensaje se emite en las anotaciones de conexión para registrar la actividad de conexión.

MQCPI014 Connection from {0} to host {1} closed - the protocol was not recognized

Explicación: Este mensaje se emite en las anotaciones de conexión para registrar la actividad de conexión.

MQCPI015 Connection from a client on {0} to host {1} was rejected because client access has been disabled on this route

Explicación: Este mensaje se emite en las anotaciones de conexión para registrar la actividad de conexión.

MQCPI016 Connection from a queue manager on {0} to host {1} was rejected because queue manager access has been disabled on this route

Explicación: Este mensaje se emite en las anotaciones de conexión para registrar la actividad de conexión.

MQCPI017 A queue manager on {0} was connected to host {1}

Explicación: Este mensaje se emite en las anotaciones de conexión para registrar la actividad de conexión.

MQCPI018 A client on {0} was connected to host {1}

Explicación: Este mensaje se emite en las anotaciones de conexión para registrar la actividad de conexión.

MQCPI019 {0} routes have been created - this exceeds the maximum number of supported routes, which is {1}

Explicación: Se ha sobrepasado el número máximo de rutas soportadas.

Respuesta del Usuario: MQIPT continuará funcionando, pero se recomienda crear una segunda instancia de MQIPT y las rutas se dividirán en dos.

MQCPI020 The configuration file has been sent to the Administration Client.

Explicación: Como resultado de una petición del cliente de administración, se ha enviado el archivo de configuración.

MQCPI021 Password checking has been enabled on the command port.

Explicación: Este mensaje indica que se necesita una contraseña para acceder a la puerta de mandatos.

MQCPI022 Password checking has been disabled on the command port.

Explicación: Este mensaje indica que no se necesita una contraseña para acceder a la puerta de mandatos.

MQCPI024 ....using HTTP proxy {0}({1})

Explicación: Este mensaje indica que la conexión de salida para esta ruta se realizará utilizando el proxy HTTP.

MQCPI025 The refresh requested by Administration Client {0} has finished.

Explicación: Como resultado de la recepción de un mandato REFRESH, MQIPT ha vuelto a leer su archivo de configuración y se ha reiniciado.

MQCPI026 Administration Client {0} has requested shutdown.

Explicación: Como resultado de la recepción de un mandato STOP, MQIPT está concluyendo.

MQCPI027 {0} sent to {1} on port {2}

Explicación: Esto hace que en la consola del sistema se visualice el mandato enviado por el cliente de administración de modalidad de línea de mandatos (no de GUI) al MQIPT que se ha designado.

MQCPI031 ......cipher suites {0}

Explicación: Este mensaje lista las suites de cifrado que se utilizan para esta ruta.

MQCPI032 ......key ring file {0}

Explicación: Este mensaje proporciona el nombre de archivo de conjunto de claves para esta ruta.

MQCPI033 ......client authentication set to {0}

Explicación: Este mensaje define si un servidor SSL está solicitando la autenticación del cliente para esta ruta.

MQCPI034 ....{0}({1})

Explicación: Este mensaje muestra el destino y la dirección de la puerta de destino para esta ruta.

MQCPI035 ....using {0}

Explicación: Este mensaje muestra el protocolo que se está utilizando para el destino. El protocolo será el protocolo MQSeries o de túnel de HTTP o de fragmentación de HTTP.

MQCPI036 ....SSL Client side enabled with properties :

Explicación: Este mensaje muestra la ruta que utilizará SSL para enviar datos al sistema principal de destino.

MQCPI037 ....SSL Server side enabled with properties :

Explicación: Este mensaje muestra la ruta que utilizará SSL para recibir datos del sistema principal de destino.

;QCPI038 .....distinguished name(s) {0}

Explicación: Este mensaje lista los nombres distinguidos que se utilizan para controlar la autenticación de los certificados.

MQCPI039 ....via Socks proxy {0}({1})

Explicación: Este mensaje muestra que la conexión de salida para esta ruta se realizará mediante el proxy Socks, el cual se define cuando MQIPT se inicia desde la línea de mandatos.

MQCPI040 Command port has been accessed by Administration Client {0}

Explicación: En la consola del sistema se graban este mensaje y el archivo de anotaciones MQIPT (si las anotaciones están habilitadas). MQIPT ha recibido una conexión del cliente de administración.

MQCPI041 ....will reply to Network Dispatcher advisor requests in {0} mode

Explicación: Este mensaje se graba en la consola del sistema cuando se inicia una ruta. Se utiliza para mostrar la modalidad que utilizará MQIPT para responder al asesor de Network Dispatcher. Las opciones válidas son ″Normal″ y ″Replace″ (Sustituir).

MQCPI042 Maximum connections reached on route {0} - further requests will be blocked

Explicación: Este mensaje se graba en la consola del sistema cuando se alcanza el número máximo de conexiones para la ruta especificada. Las peticiones posteriores se bloquearán hasta que la conexión quede libre o hasta que se aumente el valor de MaxConnectionThreads.

MQCPI043 Connections on route {0} now unblocked

Explicación: Este mensaje se graba en la consola del sistema cuando se desbloquea la ruta y puede aceptar peticiones de conexión.

MQCPI044 MQIPT has been launched from system startup

Explicación: Se ha iniciado MQIPT como un servicio del sistema.

MQCPI045 Launching MQIPT from system startup

Explicación: MQIPT se va a iniciar como un servicio del sistema.

MQCPI046 Sleeping for {0} seconds while MQIPT is launched from system startup

Explicación: El proceso fork permanecerá inactivo durante este período mientras comprueba si MQIPT se ha iniciado correctamente con un servicio del sistema.

MQCPI047 .....CA keyring file {0}

Explicación: Este mensaje proporciona el nombre de archivo de conjunto de claves CA para esta ruta.

MQCPI048 The ping by Administration Client {0} has finished

Explicación: Mensaje de respuesta de IPTController al cliente de administración.

MQCPI049 ....QoS priority to dest = {0}, to caller = {1}

Explicación: Se muestra la prioridad del tráfico en las dos direcciones de esta ruta.

MQCPI050 Adding entry to inittab to automatically start MQIPT at system startup

Explicación: El usuario ha ejecutado el script mqiptService para iniciar MQIPT como un servicio del sistema.

MQCPI051 Removing entry from inittab that automatically starts MQIPT at system startup

Explicación: El usuario ha ejecutado el script mqiptService para que MQIPT no se inicie como un servicio del sistema.

MQCPI052 ....Socks server side enabled

Explicación: Esta ruta actuará como un servidor SOCKS (proxy) y aceptará las conexiones de una aplicación con posibilidad para Socks.

MQCPI053 Starting the Java Security Manager

Explicación: El gestor de seguridad Java se iniciará ya que la propiedad SecurityManager se ha establecido en true.

MQCPI054 Stopping the Java Security Manager

Explicación: El gestor de seguridad Java se detendrá ya que la propiedad SecurityManager se ha establecido en false.

MQCPI055 Setting the java.security.policy to {0}

Explicación: El gestor de seguridad Java está a punto de iniciarse y utilizará el archivo de políticas proporcionado.

MQCPI056 The Java Security Manager must be restarted to use a new policy file

Explicación: La propiedad SecurityManagerPolicy se ha modificado, pero no entrará en vigor hasta que se reinicie el gestor de seguridad Java.

Respuesta del Usuario: Cambie la propiedad SecurityManager a false, emita un mandato refresh para detener el gestor de seguridad Java. A continuación, vuelva a cambiar la propiedad SecurityManager a true y emita otro mandato refresh para iniciar el gestor de seguridad Java con el nuevo archivo de políticas.

MQCPI057 ....trace level {0} enabled

Explicación: Este mensaje se graba en la consola del sistema cuando se inicia una ruta. Se utiliza para mostrar el nivel de rastreo que está habilitado en esta ruta.

MQCPI058 ....and a URI name of {0}

Explicación: Este mensaje se graba en la consola del sistema cuando se inicia una ruta. Se utiliza para mostrar el nombre del identificador de recursos uniforme (Uniforme Resource Identifier) de esta ruta.

MQCPI059 ....servlet client enabled

Explicación: Este mensaje se graba en la consola del sistema cuando se inicia una ruta. Esta ruta se conectará con el servlet MQIPT.

MQCPI060 Installing files to automatically start MQIPT at system startup

Explicación: El usuario ha ejecutado el script mqiptService para iniciar MQIPT como un servicio del sistema.

MQCPI061 Removing files that automatically starts MQIPT at system startup

Explicación: El usuario ha ejecutado el script mqiptService para que MQIPT no se inicie como un servicio del sistema.

MQCPI064 ....no SSL authentication on this route

Explicación: Este mensaje se graba en la consola del sistema cuando se inicia una ruta y muestra que en esta ruta no se está utilizando la autenticación SSL, ya que se ha especificado una suite de cifrado anónima.

MQCPI065 ....in SSL proxy mode

Explicación: Este mensaje se graba en la consola del sistema cuando se inicia una ruta y muestra que ésta está funcionando en modalidad de proxy SSL.

MQCPI100 This script is used to start {0}

Explicación: Mensaje de ayuda en línea para el script mqipt.

MQCPI101 Format of command is :

Explicación: Mensaje de ayuda en línea para el script mqipt.

MQCPI102 mqipt {dir_name}

Explicación: Mensaje de ayuda en línea para el script mqipt.

MQCPI103 dir_name - directory containing mqipt.conf

Explicación: Mensaje de ayuda en línea para el script mqipt.

MQCPI106 This script is used to display the current version number of {0}

Explicación: Mensaje de ayuda en línea para el script mqiptVersion.

MQCPI107 mqiptVersion {-v}

Explicación: Mensaje de ayuda en línea para el script mqiptVersion.

MQCPI108 where -v will also display the build timestamp

Explicación: Mensaje de ayuda en línea para el script mqiptVersion.

MQCPI109 This script is used to start {0}, from system startup, in another JVM and is only used in mqipt.ske. Use the mqipt script to start MQIPT from the command line.

Explicación: Mensaje de ayuda en línea del script mqiptFork.

MQCPI110 This class is used to display a simple NLS message on the console

Explicación: Mensaje de ayuda en línea de la clase IPTMessages.

MQCPI111 java com.ibm.mq.ipt.IPTMessages (message_id1) {message_id2} {message_id...}

Explicación: Mensaje de ayuda en línea de la clase IPTMessages.

MQCPI112 where message_id matches a key in the file mqipt.properties

Explicación: Mensaje de ayuda en línea de la clase IPTMessages.

MQCPI113 This script is used to manage MQIPT as a system service

Explicación: Mensaje de ayuda en línea del script mqiptVersion.

MQCPI114 mqiptService (-install | -remove)

Explicación: Mensaje de ayuda en línea del script mqiptVersion.

MQCPI115 -install will install files to start MQIPT automatically at system startup

Explicación: Mensaje de ayuda en línea del script mqiptVersion.

MQCPI116 -remove will remove files that start MQIPT automatically at system startup

Explicación: Mensaje de ayuda en línea del script mqiptVersion.

Índice

© Copyright IBM Corp. 2000-2002

J

K

L

M

N

P

Q

R

S

T

U

V

W

Z

Envío de comentarios a IBM

Si algo le ha agradado o desagradado excesivamente en esta publicación, puede utilizar uno de los métodos que se indican a continuación para enviar sus comentarios a IBM.

Envíe sus comentarios sobre lo que considera errores específicos u omisiones, y también los aspectos relacionados con la precisión, organización, los temas tratados y si éstos se han descrito de forma detallada.

Limite sus comentarios a la información contenida en esta publicación y al modo en que se presenta esta información.

Si desea realizar algún comentario acerca de las funciones de los productos o sistemas IBM, póngase en contacto con el representante de IBM o con el distribuidor autorizado de IBM.

Cuando se envían comentarios a IBM, se otorga a IBM un derecho no exclusivo para utilizar o distribuir la información del modo que considere adecuado, sin incurrir por ello en ninguna obligación para con el remitente.

Puede enviar sus comentarios a IBM utilizando cualquiera de los métodos siguientes:

- Por correo, a la dirección siguiente:

  User Technologies Department (MP095)
  IBM United Kingdom Laboratories
  Hursley Park
  WINCHESTER,
  Hampshire
  SO21 2JN
  Reino Unido
- Por fax:
  - Si llama desde fuera del Reino Unido, después del código de acceso internacional marque 44–1962–816151
  - Desde el Reino Unido, marque 01962–816151
- Por correo electrónico, utilice el ID de red correcto:
  - IBM Mail Exchange: GBIBM2Q9 at IBMMAIL
  - IBMLink: HURSLEY(IDRCF)
  - Por Internet: idrcf@hursley.ibm.com

Sea cual sea el método que utilice, no olvide incluir:

- El título de la publicación y el número de pedido
- El tema al que se aplican los comentarios
- El nombre, la dirección y el número de teléfono/fax/ID de red.

© Copyright IBM Corp. 2000-2002