WebSphere MQ internet pass-thru Versión 1.3

SC10-3826-01

Nota:
Antes de utilizar esta información y el producto al que se refiere, lea la información general del apartado "Avisos", en la página 173.

Segunda edición (marzo de 2003)

Este manual es la traducción del original inglés *WebSphere MQ internet pass-thru version 1.3*, SC34-6100-01.

Esta edición se aplica a la Versión 1.3 de 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.

Contenido

Figuras

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 de 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.
- Registra todos los intentos de conexión.

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 *WebSphere MQ Guía de administración del sistema* y *WebSphere MQ 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
- Windows 2000
- Windows XP
- Sun Solaris
- AIX V5.1
- HP-UX 11
- Linux

J2SE V1.4.0 (JRE) es necesario para el servidor MQIPT. El SDK V1.4.0 es necesario para crear una salida de seguridad.

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. Es recomendable que copie este archivo en `bin/custom.properties` y que efectúe los cambios necesarios.

Resumen de cambios

En este apartado se describen los cambios efectuados en esta edición de WebSphere MQ internet pass-thru. Los cambios efectuados respecto a la edición anterior están marcados mediante líneas verticales a la izquierda de los cambios.

Cambios en esta edición (SC10-3826-01)

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

- Una salida de seguridad para controlar las peticiones de conexión de clientes
- Soporte de LDAP para las CRL y ARL
- Cifrado de las contraseñas de conjunto de claves
- Selección de certificado de un conjunto de claves
- Nuevas suites de cifrado de AES
- Imagen de disco UNIX genérico
- Control de la acción de reinicio de ruta
- Las plataformas AIX y HP-UX ahora dan soporte a Java 1.4

Cambios en la tercera edición (SC10-3826-00)

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

- Control de la asignación de dirección a la puerta de salida
- 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
- Sistema multitarjeta de soporte
- Estado de semáforo para el cliente de administración
- Soporte de clúster de WebSphere MQ

Cambios en la segunda edición

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

- Adición de AIX, HP-UX y Windows 2000 como plataformas para MQIPT
- Adición del soporte de proxy HTTP
- Adición del soporte de SSL (Secure Socket Layer)
- Capacidad de MQIPT para comunicarse con otro MQIPT externo o con un servidor MQSeries a través de un proxy SOCKS

- Utilización de una GUI de cliente de administración para facilitar la administración de una o varias MQIPT
- Adición del soporte para IBM Network Dispatcher
- Mejoras menores del rastreo
- Mejoras menores del mandato mqiptAdmin

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.

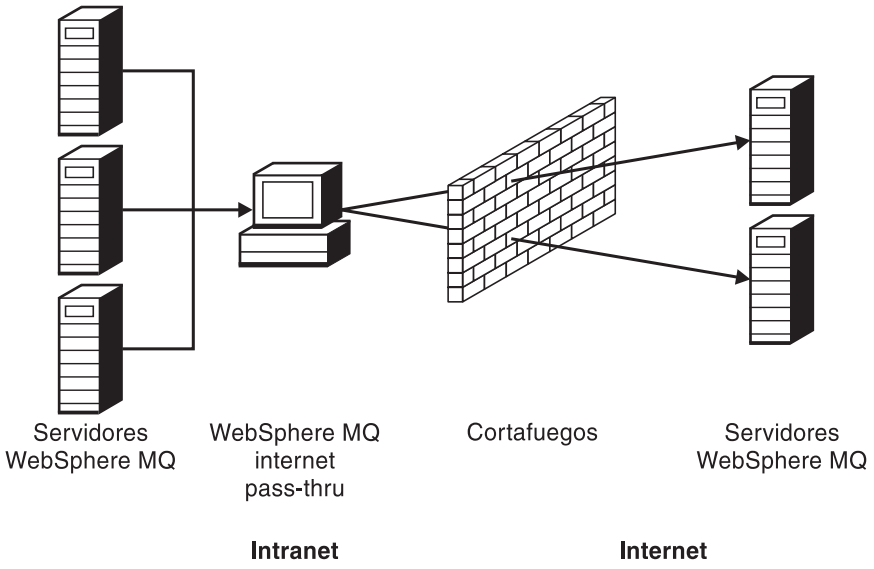

Figura 1. Ejemplo de MQIPT como un concentrador de canales

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

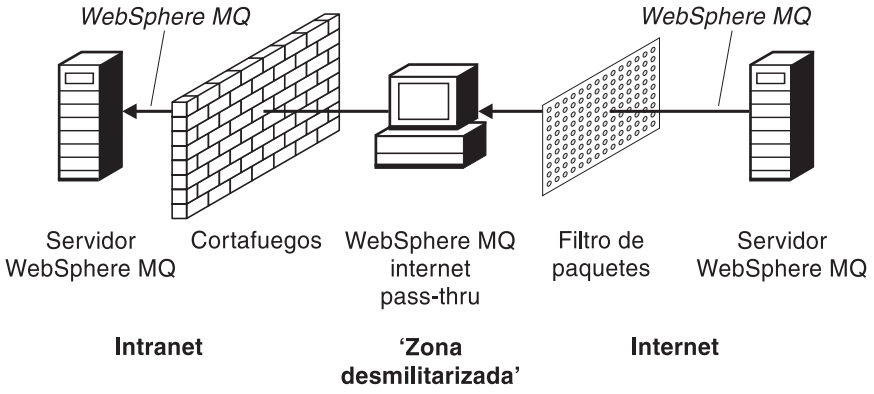

Figura 2. Ejemplo de MQIPT con una "zona desmilitarizada"

- 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.

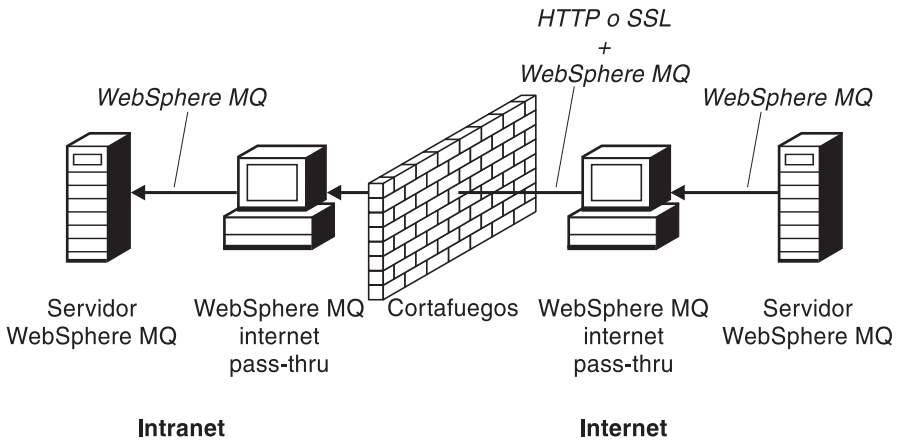

Figura 3. Ejemplo de MQIPT y la función de túnel HTTP

- 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.

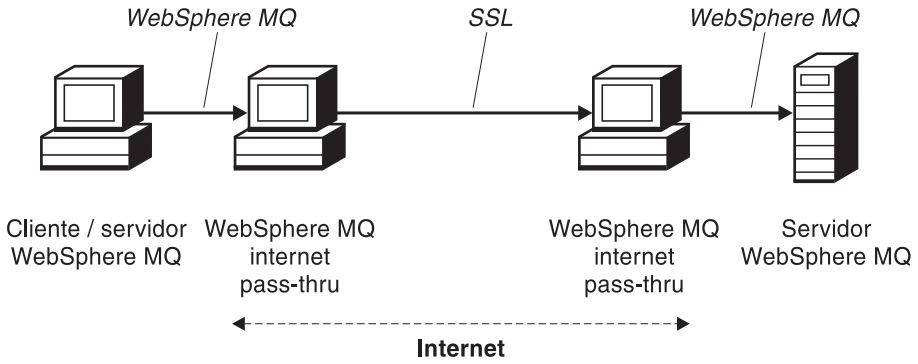

Figura 4. Ejemplo de MQIPT y SSL

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.

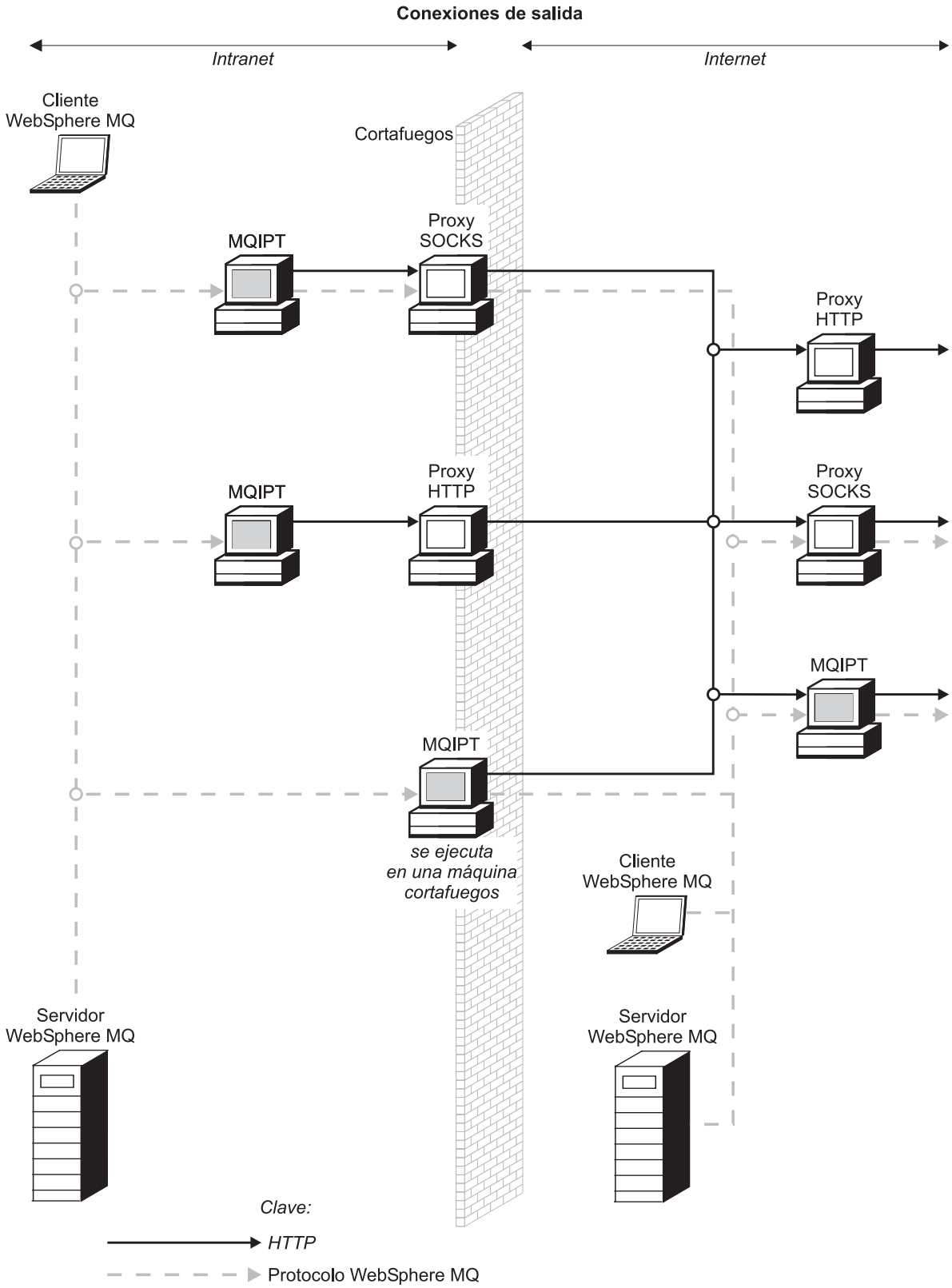

Figura 5. Topología WebSphere MQ que muestra las configuraciones posibles de MQIPT (Parte 1 de 2)

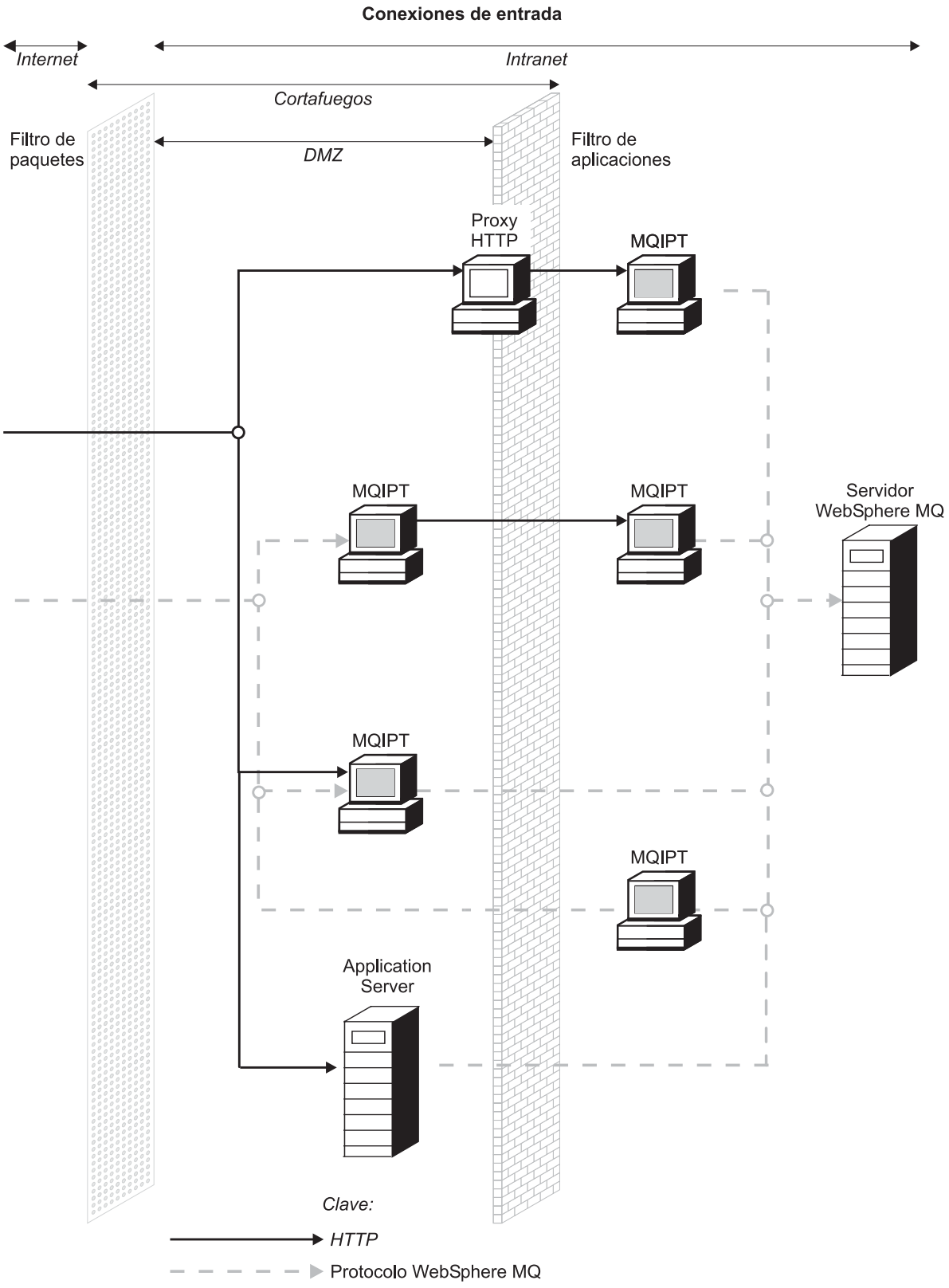

Figura 5. Topología WebSphere MQ que muestra las configuraciones posibles de MQIPT (Parte 2 de 2)

Capítulo 2. Cómo funciona internet pass-thru

En este capítulo se proporciona una visión general del funcionamiento de internet pass-thru.

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 lee los datos de entrada y simplemente los pasa a través del 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.

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.

MQIPT utiliza un archivo de configuración denominado mqipt.conf y este archivo contiene las definiciones de todas las rutas y sus propiedades asociadas. Consulte el apartado Capítulo 19, "Administración y configuración de internet pass-thru", en la página 71 para ver más información sobre este archivo.

Al lanzarse MQIPT, se inicia cada ruta del archivo de configuración. Los mensajes se escriben en la consola del sistema, mostrando el estado de cada ruta. Cuando aparece el mensaje MQCPI078 para una ruta, dicha ruta está preparada para aceptar peticiones de conexión.

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 de clúster emisor, 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.

Capítulo 3. Soporte de HTTP

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 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 intermedio 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 HTTP permanezca en estado pendiente durante un período de tiempo prolongado. Esto puede suceder, por ejemplo, en un canal de peticionario/servidor cuando la parte 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`.

Consulte el apartado “Configuración del proxy HTTP” en la página 103 para ver un ejemplo de la utilización de HTTP.

HTTPS

HTTPS se puede utilizar en una conexión HTTP habilitando las propiedades de ruta HTTPS y SSLClient en el MQIPT que emita la conexión de cliente. MQIPT debe tener acceso al certificado de CA fiable que se utilizará para autenticar el proxy/servidor HTTP de destino. La propiedad SSLClientCAKeyring se puede utilizar para definir el archivo de conjunto de claves que contiene el certificado de CA fiable.

Una configuración común de HTTPS utilizará un proxy HTTP local para salir por un túnel a través de un cortafuegos y conectarse a un servidor HTTP remoto (o a otro proxy), que, a su vez, se conectará al MQIPT remoto. Este MQIPT en la parte del servidor de la conexión no necesita ninguna configuración específica, ya que la petición de conexión se trata como cualquier conexión HTTP normal.

MQIPT utiliza las propiedades HTTPProxy y HTTPServer para distinguir los proxies local y remoto. HTTPProxy se identifica como el proxy HTTP local y HTTPServer como el servidor (o proxy) remoto.

Normalmente, las conexiones HTTPS se establecen con la dirección de la puerta de escucha 443 del proxy/servidor HTTP, pero HTTPProxyPort y HTTPServerPort se pueden utilizar para sustituir a este valor por omisión. Consulte el apartado “Configuración de HTTPS” en la página 119 para ver un ejemplo de la utilización de HTTPS.

Servlet

Ahora hay una versión de servlet de MQIPT (llamada MQIPTServlet) que puede desplegarse en un servidor de aplicaciones como aplicación no distribuida. Funciona de modo similar a MQIPT normal, pero actúa como si únicamente tuviera una ruta. Una instancia de MQIPTServlet es la encargada de manejar una petición de conexión de entrada para iniciar un canal de WebSphere MQ 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/desplegarse en el servidor de aplicaciones. Si necesita especificar un nombre de contexto cuando importe este servlet, necesitará reemplazar la propiedad UriName por omisión para que contenga el nuevo nombre de contexto. Consulte el apartado “UriName” en la página 94 para obtener más información.

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. Es recomendable que defina esta propiedad antes de iniciar MQIPTServlet.

Para controlar la cantidad de recursos que utiliza MQIPTServlet, es posible que deba cambiar algunas de las propiedades del servidor de aplicaciones. Cada servidor de aplicaciones tiene su propio modo de gestionar los datos de configuración; esto normalmente se hace utilizando una GUI, una interfaz web o bien editando el archivo de configuración. Las propiedades que probablemente se deberán cambiar son el número máximo de sesiones activas o el número de instancias del servlet en el servidor de aplicaciones. De este modo se controlará el número de conexiones de cliente y es similar a la propiedad MaxConnectionThreads utilizada en MQIPT.

Otras propiedades que puede ser necesario modificar están relacionadas con los valores de tiempo de espera, si se da soporte a las conexiones permanentes y el número de peticiones que se permiten en una conexión permanente. Como MQIPTServlet se basa en una conexión permanente al gestor de colas de destino, debe habilitarse esta propiedad. Es posible que se deban aumentar las otras propiedades, pero ello dependerá de su valor por omisión y del tipo de conexión de WebSphere MQ utilizada. Normalmente, las conexiones de cliente de WebSphere MQ son pasajeras, de modo que es bastante seguro utilizar los valores por omisión. Las conexiones de gestor de colas a gestor de colas pueden ejecutarse durante un período de tiempo indeterminado, en cuyo caso es recomendable aumentar adecuadamente algunos de los valores de tiempo de espera y el número de peticiones permitidas en una conexión permanente.

También hay una propiedad de tiempo de espera de sesión definida en el archivo web.xml con un valor por omisión de 30 minutos. Esta propiedad se puede utilizar para controlar la inactividad de un cliente y cerrará una sesión cuando no se haya detectado ninguna actividad durante el período de tiempo especificado.

También debe haber como mínimo un MQIPT en el enlace entre el cliente y MQIPTServlet. La propiedad ServletClient debe estar habilitada en el MQIPT que se conecta a MQIPTServlet y la propiedad HTTPServer puede apuntar directamente al servidor de aplicaciones o al servidor HTTP que envía información al servidor de aplicaciones.

Para comprobar si MQIPTServlet se ha iniciado correctamente, puede abrir un navegador web y escribir un nombre de URL parecido al siguiente:

```
http://localhost:80/MQIPTServlet
```

se verá una respuesta positiva en el navegador.

MQIPTServlet se ha probado con IBM WebSphere Application Server 5.0 (con y sin IBM HTTP Server), Tomcat 3.3 y Tomcat 4.0. MQIPTServlet no necesita Java 1.4 y utilizará el nivel de Java implementado por el servidor de aplicaciones.

Consulte el apartado “Configuración del servlet MQIPT” en la página 116 para ver un ejemplo de cómo utilizar el servlet.

Capítulo 4. Soporte de socks

Un proxy Socks es un servicio de red que se utiliza como un punto de salida controlado a través de un cortafuegos. Una aplicación habilitada para Socks, si se ejecuta dentro del cortafuegos, puede utilizar el proxy Socks para conectarse a una aplicación remota.

MQIPT puede actuar como un proxy Socks al habilitar la propiedad SocksServer, y de este modo se permite que una aplicación WMQ habilitada para Socks pueda conectarse a través de MQIPT a un gestor de colas WMQ remoto. Cuando se utiliza esta función, el destino del objetivo y la puerta de destino se obtienen durante el proceso de reconocimiento Socks y, por tanto, las propiedades de ruta Destination y DestinationPort se alteran temporalmente. Ésta es una función clave para dar soporte a la agrupación en clúster de WMQ. A continuación aparece más información.

MQIPT también puede actuar como un cliente Socks, en nombre de una aplicación WMQ local que no se haya habilitado para Socks. Esto resulta útil al usar un cortafuegos que sólo permite conexiones de salida a través de un proxy Socks. Se puede configurar cada ruta MQIPT de modo que se comunique con un proxy Socks diferente.

Consulte el apartado “Configuración del proxy SOCKS” en la página 111 para ver un ejemplo de cómo utilizar SOCKS.

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 *WebSphere MQ Queue Manager Clusters*, SC34-6061. El diagrama siguiente es una ampliación del definido en la tarea denominada "Adición de un gestor de colas nuevo al clúster". NEWYORK y CHICAGO están en un clúster llamado CASA y ambos contienen depósitos completos. NEWYORK, LONDON y PARIS están en otro clúster llamado INVENTARIO. 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 INVENTARIO está "oculto" detrás de un MQIPT. Dado que el gestor de colas se ha habilitado para SOCKS, cuando se inicia un canal de clúster emisor, 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 "Configuración del soporte de agrupación en clúster de MQIPT" en la página 122 para obtener un ejemplo de cómo configurar una red de clústeres.

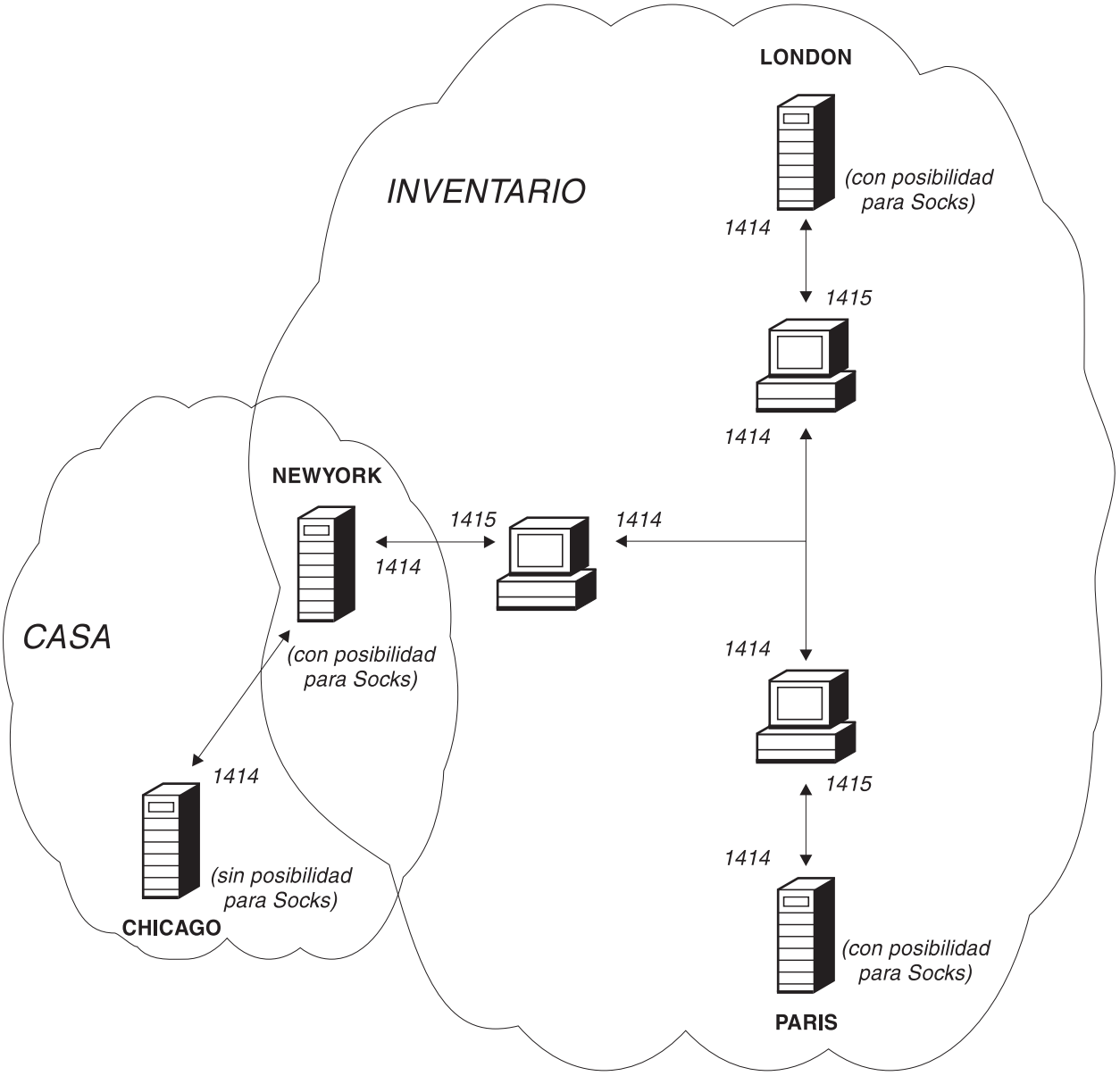

Figura 6. Soporte de la agrupación en clúster de MQIPT

Capítulo 5. Soporte y visión general 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 hash que 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_DH_anon_EXPORT_WITH_DES40_CBC_SHA
- SSL_DH_anon_WITH_3DES_EDE_CBC_SHA
- SSL_DH_anon_WITH_AES_128_CBC_SHA
- SSL_DH_anon_WITH_AES_256_CBC_SHA
- SSL_DH_anon_WITH_DES_CBC_SHA
- SSL_DH_anon_WITH_RC4_40_MD5
- SSL_DH_anon_WITH_RC4_128_MD5
- SSL_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA
- SSL_DHE_DSS_WITH_3DES__EDE_CBC_SHA
- SSL_DHE_DSS_WITH_AES_128_CBC_SHA
- SSL_DHE_DSS_WITH_AES_256_CBC_SHA
- SSL_DHE_DSS_WITH_DES_CBC_SHA
- SSL_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
- SSL_DHE_RSA_WITH_3DES__EDE_CBC_SHA
- SSL_DHE_RSA_WITH_AES_128_CBC_SHA
- SSL_DHE_RSA_WITH_AES_256_CBC_SHA
- SSL_DHE_RSA_WITH_DES_CBC_SHA
- SSL_RSA_EXPORT_WITH_DES40_CBC_SHA
- SSL_RSA_EXPORT_WITH_RC2_CBC_40_MD5#
- SSL_RSA_EXPORT_WITH_RC4_40_MD5
- SSL_RSA_WITH_3DES_EDE_CBC_SHA
- SSL_RSA_WITH_AES_128_CBC_SHA

| SSL_RSA_WITH_AES_256_CBC_SHA
| SSL_RSA_WITH_DES_CBC_SHA
| SSL_RSA_WITH_NULL_MD5
| SSL_RSA_WITH_NULL_SHA
| SSL_RSA_WITH_RC4_128_MD5
| SSL_RSA_WITH_RC4_128_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 fiable se deben mantener en la parte 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 fiable 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 fiables. 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 fiable no ofrece seguridad, podría establecer una conexión segura con un destino que no es nada seguro.

WebSphere MQ internet pass-thru 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 archivo de conjunto de claves también puede contener listas de revocación de certificados (CRL) y listas de revocación de autorizaciones (ARL). WebSphere MQ internet pass-thru utiliza el paquete IBM Secure Socket Lite (SSLite).

Un WebSphere MQ internet pass-thru 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 WebSphere MQ internet pass-thru 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 WebSphere MQ internet pass-thru 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 81 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 fiable 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 fiable.

El archivo de conjunto de claves de la parte del servidor SSL, identificado mediante la propiedad SSLServerKeyRing, debe contener su certificado personal.

El archivo de conjunto de claves de la parte del cliente SSL, identificado mediante la propiedad SSLClientCAKeyRing debe contener una lista de los certificados de CA fiables que se utilizarán para autenticar el certificado enviado desde el servidor.

Si también se requiere la autenticación del cliente, debe habilitarse la propiedad SSLServerAskClientAuth en la parte del servidor y el archivo de conjunto de claves de la parte del cliente, identificado mediante la propiedad SSLServerKeyRing, debe contener su certificado personal. El archivo de conjunto de claves de la parte del servidor, identificado mediante la propiedad SSLServerCAKeyRing, debe contener una lista de los certificados de CA fiables que se utilizarán para autenticar el cliente.

Como alternativa a utilizar los certificados firmados por una CA fiable, puede utilizar certificados autofirmados. En los archivos de conjunto de claves de ejemplo puede encontrar varios certificados autofirmados de ejemplo que se proporcionan con MQIPT en el subdirectorio ssl: sslSample.pfx y sslCAdefault.pfx.

Para abrir cualquiera de las señales PKCS#12 de estos archivos de conjunto de claves, debe utilizar una contraseña de `mqiptV1.3`.

En el subdirectorio ssl puede encontrar un programa de utilidad llamado KeyMan, con el que puede gestionar certificados SSL y archivos de conjunto de claves. Consulte el apartado "KeyMan" en la página 22 para obtener las instrucciones de instalación y demás información.

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 apartado Capítulo 20, "Iniciación a internet pass-thru", en la página 95 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 1. 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.

Tabla 1. Mensajes de error SSLRuntimeException (continuación)

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.
30	La autorización ha fallado.

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

Tabla 2. 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 reconocimiento SSL 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.
46	Se ha recibido un certificado desconocido.
47	Se ha detectado un parámetro no permitido.

LDAP y las CRL

WebSphere internet pass-thru da soporte a la utilización de un servidor LDAP (Lightweight Directory Access Protocol) para llevar a cabo la autenticación de la CRL (lista de revocación de certificados) en un certificado digital. El soporte de LDAP se ha implementado de forma parecida a la de WebSphere MQ base, ya que posiblemente puede utilizarse el mismo servidor LDAP tanto para WebSphere MQ como para MQIPT. En el capítulo 15 de la publicación ″WebSphere MQ Seguridad

Versión 5.3″ SC10-3801-01 podrá encontrar más información sobre la utilización de servidores LDAP con WebSphere MQ. A continuación se incluyen unos extractos de la publicación a efectos de consulta.

Durante el reconocimiento SSL, los socios de comunicaciones se autentican el uno ante el otro con certificados digitales. La autenticación puede incluir una comprobación de que el certificado recibido aún resulta fiable. Las autoridades de certificación (CA) revocan certificados por varios motivos, entre los cuales encontramos los siguientes:

- El propietario ha pasado a otra organización.
- La clave privada ya no es secreta.

Las CA publican los certificados personales revocados en una lista de revocación de certificados (CRL). Los certificados de CA que se hayan revocado se publican en una lista de revocación de autorizaciones (ARL). Las referencias posteriores a las CRL en este capítulo también se aplican a las ARL.

En el mercado existen varios servidores de directorio LDAP propietarios. WebSphere internet pass-thru se ha probado con IBM Directory Server: consulte la dirección de Internet `http://www.ibm.com/software/network/directory/server`. Junto con la documentación que acompaña al producto instalado encontrará instrucciones para instalar y mantener el servidor LDAP.

En la publicación ″WebSphere MQ Seguridad Versión 5.3″ SC10-3801-01 encontrará más información sobre la gestión de las CRL y ARL.

MQIPT puede dar soporte como máximo a dos servidores LDAP en cada ruta. El primer servidor LDAP se trata como el servidor principal, y el segundo se considera como un servidor de copia de seguridad, y sólo se utilizará si no se puede acceder al servidor principal. El servidor de copia de seguridad debe ser una imagen reflejada del servidor principal.

Puede proteger el acceso a la información almacenada en un servidor LDAP mediante un ID de usuario y una contraseña. Si éste es el caso, pueden utilizarse las propiedades LDAP*Userid y LDAP*Password.

Cuando MQIPT carga una señal PKCS#12 procedente de un archivo de conjunto de claves, se comprobará la validez CRL de todos los certificados de CA. Si se ha adjuntado una CRL al certificado de CA, se comprobará si ha caducado y, si así es, se recuperará una nueva CRL del servidor LDAP. Todas las CRL recuperadas se cargarán en la señal actual y se adjuntarán a su certificado de CA. La señal actualizada puede guardarse en el archivo de conjunto de claves (consulte la propiedad LDAPSaveCRL en el apartado “Información de consulta relacionada con la sección de ruta” en la página 81).

Cuando se envía una consulta al servidor LDAP principal, si no hay ninguna entrada que coincida con la CA especificada, se supondrá que no hay ninguna CRL para la misma. El servidor de copia de seguridad no se utilizará. Si, no obstante, no se puede acceder al servidor LDAP principal o no devuelve ningún resultado dentro de un período de tiempo determinado, se utilizará el servidor de copia de seguridad. Todos los errores procedentes del servidor de copia de seguridad provocarán que la conexión del cliente finalice. Esta acción puede alterarse temporalmente estableciendo la propiedad LDAPIgnoreErrors en true.

Atención
Si habilita la propiedad LDAPIgnoreErrors, alguien podrá utilizar un certificado revocado para efectuar una conexión SSL.

El modelo de cliente LDAP se basa en la implementación ″com.sun.jndi.ldap.LdapCtxFactory″. Todas las CRL que recupere MQIPT se guardarán en una antememoria y se compartirán con todas las conexiones de dicha ruta.

Si una CRL colocada en antememoria caduca, se suprimirá de la antememoria y se recuperará una CRL nueva del servidor LDAP. Si no hay disponible ninguna CRL nueva, se seguirá rechazando la conexión.

También se comprueba si ha caducado una CRL recuperada del servidor LDAP y aparece un mensaje de la consola del sistema (MQCPW001). La CRL caducada seguirá cargada en el sistema y se rechazarán todas las peticiones de conexión que hagan referencia a dicha CRL. Deberá sustituirse la CRL caducada del servidor LDAP por una actual.

Puede utilizarse la propiedad LDAPCacheTimeout para controlar con qué frecuencia se borra la antememoria de la CRL. El valor por omisión es de 1 día. Establecer este valor en 0 significa que las entradas de la antememoria no se borrarán hasta que se reinicie la ruta.

Una CRL caducada puede almacenarse en un archivo de conjunto de claves o en un servidor LDAP. Si no se ha emitido ninguna nueva, las peticiones de conexión subsiguientes se rechazarán. Puede ignorar las CRL caducadas habilitando la propiedad IgnoreExpiredCRLs.

Atención
Si habilita la propiedad IgnoreExpiredCRLs, alguien podrá utilizar un certificado revocado para efectuar una conexión SSL.

El estándar de cifrado avanzado

El estándar de cifrado avanzado (AES) será una nueva publicación FIPS (Federal Information Processing Standard) que especificará un algoritmo criptográfico para que lo utilicen las organizaciones del Gobierno de los EE.UU. con el fin de proteger información confidencial (no clasificada). El NIST (National Institute of Standards and Technology) también anticipa que el AES lo utilizarán de forma generalizada y voluntaria las organizaciones, instituciones e individuos fuera del ámbito del Gobierno de los EE.UU., y fuera de los EE.UU., en algunos casos.

Selección de certificados de un archivo de conjunto de claves

Es posible tener más de un certificado personal almacenado en el mismo archivo de conjunto de claves, de forma que las propiedades SSLClientSite* pueden utilizarse en la parte del cliente para seleccionar el certificado que debe enviarse al servidor a efectos de autenticación y las propiedades SSLServerSite* pueden utilizarse en la parte del servidor para seleccionar el certificado que debe enviarse al cliente a efectos también de autenticación.

Mediante estas propiedades, un certificado puede seleccionarse en función de su nombre distinguido (DN). De forma alternativa, la etiqueta de certificado puede utilizarse para seleccionar un certificado mediante las propiedades SSLServerSiteLabel y SSLClientSiteLabel.

Cifrado de una contraseña de conjunto de claves

La contraseña utilizada para abrir un archivo de conjunto de claves puede cifrarse con mqiptPW. La contraseña cifrada se almacena en un archivo, que pueden utilizar cualquiera de las propiedades siguientes: SSLClientKeyRingPW, SSLClientCAKeyRingPW, SSLServerKeyRingPW y SSLServerCAKeyRingPW.

Formato del mandato:

```
mqiptPW <contraseña> <nombre_archivo> <-replace>
```

donde

contraseña
es la contraseña de texto sin cifrar necesaria para abrir el archivo de conjunto de claves

nombre_archivo
es el nombre del archivo de contraseñas que debe crearse

replace
es la opción requerida para sobrescribir el `<nombre_archivo>` si éste existe

Las contraseñas pueden incluir el carácter de espacio (" "), pero en ese caso la cadena completa de la contraseña debe especificarse entre comillas. No existe límite para la longitud ni el formato de una contraseña.

Nota: Los usuarios que hayan migrado de un nivel anterior de WebSphere internet pass-thru deberán sustituir los archivos de contraseñas actuales que contengan la contraseña de texto sin cifrar por una copia del archivo de contraseñas cifradas.

Deberá utilizar la contraseña `mqiptV1.3` para abrir los archivos de conjunto de claves de ejemplo mediante un programa de utilidad de gestión de claves (por ejemplo, KeyMan).

KeyMan

Junto con WebSphere 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 la parte 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, WebSphere internet pass-thru). 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 fiables 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 fiables (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 fiables correspondientes en un solo archivo PKCS12. Los archivos PKCS12 están protegidos mediante una frase de contraseña. Normalmente, una señal PKCS12 contiene la política fiable 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 fiable o los servidores fiables dependiendo de sus respectivos valores fiables (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 fiables para los certificados: CA e igual (″Peer″). Si acepta un certificado fiable de una CA, implícitamente considerará como fiable 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 fiables.

¿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 fiables 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 fiables 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).

Capítulo 6. Calidad de servicio

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. Adicionalmente, TQoS también permite a los administradores recopilar datos sobre el rendimiento de la política correspondiente para supervisar si ésta proporciona los objetivos del nivel de servicio (medidas importantes como rendimiento de la conexión, retardos, índice de pérdidas, etc.) para los que se han diseñado. 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.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.

El código de TQoS, junto con las instrucciones de instalación y administración, puede descargarse de la misma ubicación que MQIPT. Visite el sitio web de los SupportPacs de la familia WebSphere MQ, `http://www.ibm.com/webspheremq/supportpacs` y pulse Category 3 – Product Extensions.

MQIPT se proporciona con una biblioteca ficticia denominada `libmqiptqos.so`, que se encuentra en el subdirectorio lib de MQIPT. Con esto puede ejecutarse MQIPT en las plataformas Linux sin tener que instalar a aplicación Pagent de TQoS. Tras instalar TQoS, es posible que tenga que sustituir esta biblioteca ficticia por la que TQoS utilice. En el subdirectorio bin de MQIPT encontrará un script denominado `mqiptQoS` que puede ayudarle a llevar a cabo esta tarea. Utilice el mandato siguiente para cambiar el nombre de la biblioteca ficticia y definir un enlace dinámico a la biblioteca de tiempo de ejecución de TQoS real.

```
mqiptQoS -install
```

Para revertir las acciones anteriores, utilice `mqiptQoS -remove`.

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 81 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 108 para obtener más información sobre las definiciones de políticas.

Capítulo 7. Network Dispatcher

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 7 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.

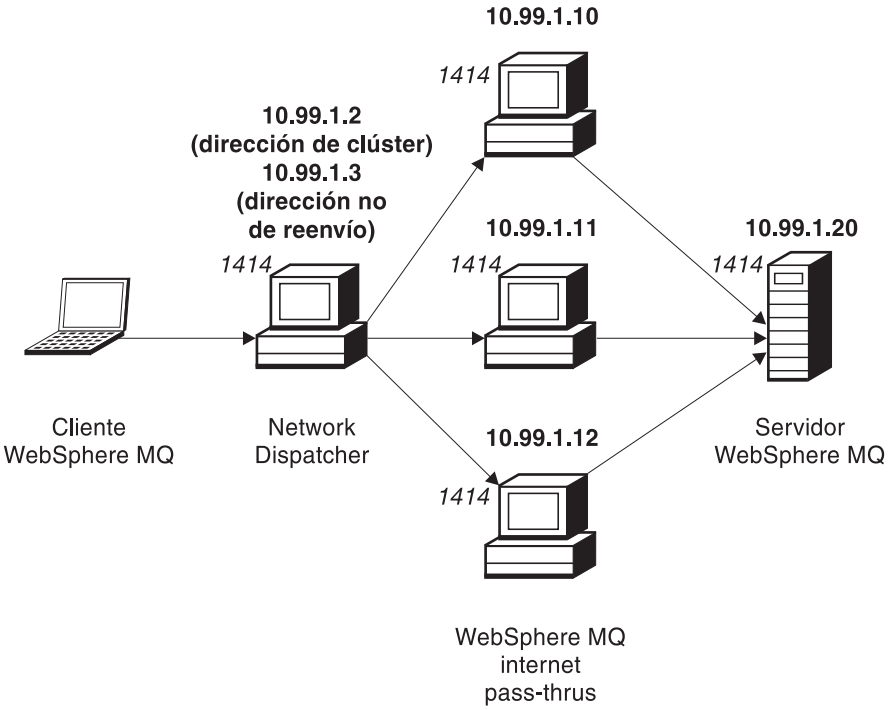

Figura 7. Utilización de Network Dispatcher con MQIPT

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.

Capítulo 8. Java Security Manager y las rutinas de salida de seguridad

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 superior 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 80 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 80 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, es recomendable 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 de 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 sólo 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 es recomendable que utilice las propiedades SecurityManager y SecurityManagerPolicy para controlar MQIPT.

Rutina de salida de seguridad

Atención

MQIPT se ejecuta en una sola JVM de forma que una rutina de salida de seguridad definida por el usuario puede poner en peligro el funcionamiento normal de MQIPT porque:

- afecta a los recursos del sistema
- genera atascos
- degrada el rendimiento

Debe comprobar exhaustivamente los efectos de la rutina de salida de seguridad antes de implementarla en un entorno de trabajo.

El objetivo de una rutina de salida de seguridad es controlar el acceso a un destino objetivo, tal como se define en la propiedad de ruta de destino objetivo. Se

invocará la rutina de salida de seguridad en el punto en que se haya recibido una petición de conexión de un cliente y antes de que MQIPT efectúe la conexión al destino objetivo. En función de las propiedades de la conexión inicial, la rutina de salida de seguridad puede decidir si se permitirá que la conexión se complete.

Al iniciarse una ruta, se invocará la rutina de salida de seguridad para que se inicialice y se autoprepare para procesar una petición de conexión. El proceso de inicialización debe utilizarse para cargar los datos de usuario y preparar los mismos para poder acceder a ellos fácil y rápidamente, con lo que se minimiza el tiempo necesario para procesar una petición de conexión.

Cada ruta puede tener su propia rutina de salida de seguridad. La propiedad SecurityExit se utiliza para habilitar/inhabilitar la rutina de salida de seguridad definida por el usuario. La propiedad SecurityExitName se utiliza para definir el nombre de clase de la rutina de salida de seguridad definida por el usuario. La propiedad SecurityExitPath se utiliza para definir el nombre del directorio que contiene el archivo class. Si no se puede establecer esta propiedad, se presupone que el archivo class estará ubicado en el subdirectorio exits. La propiedad SecurityExitPath también puede definir el nombre de un archivo jar que contiene la rutina de salida de seguridad definida por el usuario. Finalmente, MQIPT utiliza la propiedad SecurityExitTimeout para determinar cuánto tiempo debe esperar una respuesta por parte de la rutina de salida de seguridad al validar una petición de conexión.

Se ha creado una nueva clase denominada SecurityExit para permitir a MQIPT que pueda invocar una rutina de salida de seguridad definida por el usuario. La rutina de salida de seguridad definida por el usuario debe ampliar la nueva clase y la mayoría de sus métodos deben alterarse temporalmente para proporcionar la funcionalidad necesaria. Se utiliza un objeto SecurityExitResponse para devolver datos a MQIPT, que los utiliza para decidir si la petición de conexión debe aceptarse o rechazarse. SecurityExitResponse también puede contener una nueva dirección de destino y de puerta de destino, utilizada para sustituir las propiedades definidas por la ruta.

Se han facilitado tres rutinas de salida de seguridad de ejemplo para mostrar cómo se puede implementar una rutina de salida de seguridad. El primer ejemplo, denominado SampleSecurityExit, muestra cómo controlar el acceso a un gestor de colas de WebSphere MQ en función del nombre del canal de WMQ. Únicamente permitirá una conexión con un nombre de canal que empiece por la cadena "MQIPT." Consulte el apartado “Rutina de salida de seguridad” en la página 139 para obtener información más detallada.

El segundo ejemplo, denominado SampleRoutingExit, permite el direccionamiento dinámico de las peticiones de conexión de cliente a una agrupación de servidores WebSphere MQ definidos, albergando cada servidor un QM con el mismo nombre y los mismos atributos. El ejemplo incluye un archivo de configuración que contiene una lista de nombres de servidor. Consulte el apartado “Rutina de salida de seguridad de direccionamiento” en la página 141 para obtener información más detallada.

El tercer ejemplo, denominado SampleOneRouteExit, permite el direccionamiento dinámico a un QM de WMQ que está derivado del nombre de canal de WMQ utilizado en la petición de conexión. El ejemplo incluye un archivo de configuración que contiene una correlación de nombres de QM a nombres de servidor. Consulte el apartado “Rutina de salida de una ruta dinámica” en la página 144 para obtener información más detallada.

La clase com.ibm.mq.ipt.SecurityExit

La rutina de salida de seguridad definida por el usuario debe ampliar esta clase y sus métodos públicos para poder obtener acceso a algunos datos comunes y permitir que se lleve a cabo cierta inicialización de MQIPT. Antes que MQIPT invoque cada uno de los métodos, hay algunas propiedades que deben estar disponibles para que las utilicen dichos métodos. Sus valores pueden recuperarse mediante los métodos get adecuados definidos en esta clase. A continuación aparece una lista completa de los métodos soportados.

Métodos

init

```
public void init () throws IPTException
```

Hay disponibles las propiedades siguientes:

- listener port
- destination
- destination port
- version

MQIPT invocará el método init cuando se inicie una ruta. Tras generarse el resultado de retorno de este método, la rutina de salida de seguridad debe estar preparada para validar una petición de conexión. Todas las excepciones generadas en este método impedirán que la ruta se reinicie.

refresh

```
public void refresh () throws IPTException
```

Hay disponibles las propiedades siguientes:

- listener port
- destination
- destination port

MQIPT invocará el método refresh cuando el cliente de administración de MQIPT le haya solicitado que se actualice automáticamente. Normalmente se invoca esta acción cuando se cambia una propiedad del archivo de configuración. MQIPT cargará todas las propiedades del archivo de configuración y determinará cuáles se han cambiado y si debe reiniciarse una ruta inmediatamente, o si se puede esperar hasta la próxima vez que se reinicie MQIPT.

Este método debe recargar todos los datos externos que utilice (es decir, los datos cargados durante el método init). Todas las excepciones generadas en este método harán que la ruta se inhabilite.

close

```
public void close ()
```

Hay disponibles las propiedades siguientes:

- listener port
- destination
- destination port

MQIPT invocará el método close() cuando el cliente de administración de MQIPT le haya solicitado que se detenga. Esta acción debería liberar todos los recursos del sistema que haya adquirido durante su funcionamiento. MQIPT no concluirá hasta que este método haya finalizado.

También se invocará este método si se habilitó una rutina de salida de seguridad que se haya inhabilitado ahora en el archivo de configuración.

validate

```
public SecurityExitResponse validate ()
```

Hay disponibles las propiedades siguientes:

- listener port
- destination
- destination port
- timeout
- client IP address
- client port address
- channel name
- queue manager name

MQIPT invocará el método validate cuando reciba una petición de conexión para su validación. El nombre del canal y del gestor de colas no estarán disponibles si la propiedad SSLProxyMode se ha habilitado, ya que esta característica sólo se utiliza para hacer pasar los datos SSL a través de un túnel y, por tanto, no podrán leerse los datos que normalmente se obtienen del flujo de datos inicial. El nombre del gestor de colas no estará disponible para las conexiones de cliente WMQ, ya que esta información no está disponible hasta que se ha establecido la conexión con el gestor de colas de destino.

La rutina de salida de seguridad debe devolver un objeto SecurityExitResponse, que contenga la información siguiente:

- código de razón (debe establecerse)
- nueva dirección de destino (opcional)
- nueva dirección de puerta escucha de destino (opcional)
- mensaje (opcional)

El código de razón determinará si MQIPT ha aceptado o rechazado la conexión. Los campos newDestination y newDestinationPort pueden establecerse opcionalmente para definir un destino nuevo (QM). Si no establece estas propiedades, se utilizarán las propiedades Destination y DestinationPort de la ruta definidas en el archivo de configuración. Los mensajes que se emitan se adjuntarán a la entrada del archivo de anotaciones de la conexión.

Métodos soportados para obtener propiedades:

public int getListenerPort()
recupera la puerta escucha de la ruta - tal como se haya definido en la propiedad ListenerPort

public String getDestination()
recupera la dirección de destino - tal como se haya definido en la propiedad Destination

public int getDestinationPort()
recupera la dirección de puerta escucha de destino - tal como se haya definido en la propiedad DestinationPort

public String getClientIPAddress()
recupera la dirección IP del cliente que efectúa la petición de conexión

public int getClientPortAddress()
recupera la dirección de puerta utilizada por el cliente que efectúa la petición de conexión

public int getTimeout()
recupera el valor de tiempo de espera excedido. MQIPT espera a que la rutina de salida de seguridad valide una petición - tal como se haya definido en la propiedad SecurityExitTimeout

public int getConnThreadID()
recupera el ID de hebra de conexión que maneja la petición de conexión, que resulta útil a efectos de depuración

public String getChannelName()
recupera el nombre de canal WMQ utilizado en la petición de conexión

public String getQMName()
recupera el nombre del gestor de colas de WMQ utilizado en la petición de conexión

public boolean getTimedout()
la rutina de salida de seguridad puede utilizar este método para determinar si el tiempo de espera ha caducado

La clase com.ibm.mq.ipt.SecurityExitResponse

Esta clase se utilizará para devolver una respuesta a MQIPT desde una rutina de salida de seguridad definida por el usuario y se utilizará para determinar si la petición de conexión debe aceptarse o rechazarse. Los objetos de este tipo sólo se crean en el método validate (tal como se explica más arriba). Existen métodos muy cómodos de utilizar que sirven para crear dichos objetos y hay varios métodos para cada propiedad. Consulte las rutinas de salida de seguridad de ejemplo para obtener más información.

La creación de un objeto SecurityExitResponse por omisión rechazará la petición de conexión.

Métodos de creación soportados:

public SecurityExitResponse (String dest, int destPort, int rc, String msg) throws IPTException

donde:

- `dest` es el nuevo destino objetivo
- `destPort` es la nueva dirección de puerta de destino
- `rc` es el código de razón
- `msg` es un mensaje que se agregará a la entrada de las anotaciones de conexión

public SecurityExitResponse (String dest, int destPort, int rc) throws IPTException

public SecurityExitResponse (int rc, String msg) throws IPTException

public SecurityExitResponse (int rc) throws IPTException

Métodos soportados para establecer valores de propiedad:

public void setDestination(String dest)
establece una nueva dirección de destino para la petición de conexión

public void setDestinationPort(int port) throws IPTException
establece una nueva dirección de puerta de escucha de destino para la petición de conexión - genera una IPTException para una dirección de puerta no válida

public void setMessage(String msg)
agrega un mensaje al registro de anotaciones de conexión

public void setReasonCode(int rc) throws IPTException
establece el código de razón de la petición de conexión - genera una IPTException para un valor desconocido

Códigos de razón válidos:

- `SecurityExitResponse.OK = 0`
- `SecurityExitResponse.NOT_AUTHORIZED = 1`
- `SecurityExitResponse.NOT_READY = 2`

Rastreo

Para que le resulte más fácil diagnosticar problemas en una rutina de salida de seguridad definida por el usuario, puede habilitar un recurso de rastreo, parecido al que utiliza MQIPT. Si establece la propiedad Trace de la ruta en un valor de 1-5 se creará un archivo de rastreo en el subdirectorio errors. El nombre del archivo de rastreo es el mismo que el de la rutina de salida de seguridad.

Probablemente habrá más de una instancia de la rutina de salida de seguridad que se esté ejecutando al mismo tiempo de forma que las entradas individuales del archivo de rastreo puedan identificarse mediante el identificador de hebra.

MQIPT inicializa las funciones de rastreo al iniciar la rutina de salida de seguridad; todo lo que debe hacer es elegir qué información quiere rastrear. Hay muchos ejemplos de rastreo en las rutinas de salida de usuario de ejemplo.

Los requisitos mínimos para poder realizar el rastreo son una llamada de `entrada`, una llamada de `salida` y los datos que desee rastrear. Por ejemplo:

```
<a_method>
{
  SecurityExit.rastlRoute.entry(RASITraceEvent.TYPE_ENTRY_EXIT,
                                this,
                                "method_name");

  .
  .
  .
  <code>

  .
  .
  .
  SecurityExit.rastlRoute.trace(RASITraceEvent.TYPE_MISC_DATA,
                                this,
                                "data");

  .
  .
  .
  <code>
```

```
                    :
                      SecurityExit.rastlRoute.exit(RASITraceEvent.TYPE_ENTRY_EXIT,
                                                   this,
                                                   "method_name");
                    }
```

Capítulo 9. Control de dirección de puerta

Control de dirección de puerta

Cuando se utiliza MQIPT, es posible restringir el rango de direcciones de puerta local utilizadas al crear una conexión de salida estableciendo la propiedad `OutgoingPort` de la ruta. El rango de direcciones de puerta local se calcula mediante el valor `MaxConnectionThreads`. Por ejemplo, si se establece `OutgoingPort` en `1600` y se establece `MaxConnectionThreads` en `20`, el rango de direcciones de puerta local, para dicha ruta, sería `1600-1619`. El administrador de MQIPT es el responsable de asegurarse de que no haya conflictos de direcciones de puerta en las rutas. Si no se ha definido `OutgoingPort`, un valor por omisión de `0` significa que se utilizará una dirección de puerta asignada por el sistema para cada conexión.

Vea el ejemplo, "Asignación de direcciones de puerta" en la página 128, si desea obtener más información.

Sistemas multitarjeta

Cuando utilice un sistema multitarjeta, puede especificar a qué dirección IP se vinculará una conexión de salida mediante la propiedad `LocalAddress`. En esta propiedad no se da soporte a los nombres de sistema principal.

Capítulo 10. Otras consideraciones de seguridad

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 o esté utilizando una rutina de salida de seguridad.
- 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 31.
- 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 11. Características varias

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 de espera desocupado opcional. Si MQIPT detecta que un canal ha estado desocupado durante un período de tiempo que supera el valor de tiempo de espera, 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 mensaje de 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 80 para obtener información más detallada.

Cada vez que se inicia MQIPT, se crea una anotación de conexión nueva. 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.

Capítulo 12. Actualización desde la versión anterior

Para actualizar MQIPT de la Versión 1.2 a la Versión 1.3, siga estos pasos:

1. Efectúe una copia de los archivos de configuración `mqipt.conf` y `client.conf`. `mqipt.conf` está ubicado en el directorio inicial de MQIPT y `client.conf` en el subdirectorio bin.
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 V1.3, vuelva a copiar los archivos de configuración en sus ubicaciones originales.
6. Es recomendable que utilice la GUI de administración MQIPT para gestionar los cambios realizados en MQIPT. El archivo de configuración de la Versión 1.2 es compatible con la GUI.

Algunas implementaciones requieren disponer de un servicio MQIPT local que esté bajo el control de su propia organización y un servicio MQIPT remoto que podría estar bajo el control de la organización de su cliente. En esta situación, resulta muy difícil migrar ambos servicios MQIPT al mismo tiempo pero esto no es un problema para MQIPT. A menos que se indique lo contrario, las versiones anteriores de MQIPT son compatibles con la última. Esto facilita enormemente el proceso de migración de MQIPT.

También cabe la posibilidad de actualizar el núcleo de MQIPT sin desinstalarlo primero. Todas las clases necesarias para poder ejecutar MQIPT se almacenan en el archivo MQipt.jar; puede instalar la última versión de MQIPT en otra máquina y copiar el archivo MQipt.jar de dicha instalación en su sistema activo. Este método también puede aplicarse a las clases necesarias para poder ejecutar la GUI de administración. Están en el archivo guiadmin.jar.

Nuevas opciones de configuración

Las propiedades siguientes son nuevas en la Versión 1.3:

- IgnoreExpiredCRLs
- LDAP
- LDAPCacheTimeout
- LDAPIgnoreErrors
- LDAPSaveCRL
- LDAPServer1
- LDAPServer1Password
- LDAPServer1Port
- LDAPServer1Timeout
- LDAPServer1Userid
- LDAPServer2
- LDAPServer2Password

- LDAPServer2Port
- LDAPServer2Timeout
- LDAPServer2Userid
- RouteRestart
- SecurityExit
- SecurityExitName
- SecurityExitPath
- SecurityExitTimeout
- SSLClientSiteDN_C
- SSLClientSiteDN_CN
- SSLClientSiteDN_L
- SSLClientSiteDN_O
- SSLClientSiteDN_OU
- SSLClientSiteDN_ST
- SSLClientSiteLabel
- SSLServerSiteDN_C
- SSLServerSiteDN_CN
- SSLServerSiteDN_L
- SSLServerSiteDN_O
- SSLServerSiteDN_OU
- SSLServerSiteDN_ST
- SSLServerSiteLabel

Para obtener información acerca de todas las propiedades, consulte el apartado “Información de consulta relacionada con la configuración” en la página 76.

Capítulo 13. 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 (un SupportPac de categoría 3 de MS81) de la página web de WebSphere MQ SupportPac:

`http://www.ibm.com/webspheremq/supportpacs`

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.
exits\ SampleOneRouteExit.java	Rutina de salida de ejemplo.
exits\ SampleOneRouteExit.conf	Archivo de configuración de SampleOneRouteExit.

Archivo	Finalidad
exits\SampleRoutingExit.java	Rutina de salida de ejemplo.
exits\SampleRoutingExit.conf	Archivo de configuración de SampleRoutingExit.
exits\SampleSecurityExit.java	Rutina de salida de ejemplo.
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”.
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\mqiptPW.bat	Cifrado de la contraseña utilizada para abrir un archivo de conjunto de claves.
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>\html\ <nombrearchivo>.zip	Archivo maestro de la publicación *internet pass-thru* en formato HTML. Consulte el apartado “Bibliografía” en la página 175 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 apartado Capítulo 19, “Administración y configuración de internet pass-thru”, en la página 71

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 149. Los siguientes mensajes son un ejemplo de que MQIPT se ha iniciado correctamente:

```
5639-L92 (C) Copyright IBM Corp. 2000, 2003 Reservados todos los derechos
MQCPI001 Arrancando WebSphere MQ internet pass-thru Versión 1.3.0
MQCPI004 Leyendo información de configuración de c:\mqipt\mqipt.conf
MQCPI008 A la escucha de mandatos de control en la puerta 1881
MQCPI011 Se utilizará la vía de acceso c:\mqipt\logs para almacenar los archivos
         de anotaciones
MQCPI006 La ruta 1418 se ha iniciado y reenviará mensajes a:
MQCPI034 ....mqserver.company4.com(1414)
MQCPI035 ....utilizando protocolos de MQ
MQCPI078 La ruta 1418 está preparada para las solicitudes de conexión
MQCPI006 La ruta 1415 se ha iniciado y reenviará mensajes a:
MQCPI034 ....mqipt.company2.com(1415)
MQCPI035 ....utilizando protocolos de MQ
MQCPI036 ....parte del Cliente SSL habilitada con las propiedades:
MQCPI031 ......grupos de cifrado <null>
MQCPI032 ......archivo de conjunto de claves c:\mqipt\KeyMan.pfx
MQCPI038 ......nombres distinguidos CN=*Doe O=IBM OU=* L=* ST=* C=*
MQCPI078 La ruta 1415 está preparada para las solicitudes de conexión
```

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 de `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 `client` 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
```

Desinstalación 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 desinstalación desde el menú Inicio de Windows.

Capítulo 14. 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/webspheremq/supportpacs`

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.
exits/ SampleOneRouteExit.java	Rutina de salida de ejemplo.
exits/ SampleOneRouteExit.conf	Archivo de configuración de SampleOneRouteExit.
exits/SampleRoutingExit.java	Rutina de salida de ejemplo.

Archivo	Finalidad
exits/SampleRoutingExit.conf	Archivo de configuración de SampleRoutingExit.
exits/SampleSecurityExit.java	Rutina de salida de ejemplo.
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”.
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/mqiptPW	Cifrado de la contraseña utilizada para abrir un archivo de conjunto de claves.
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>/html/ <nombrearchivo>.zip	Archivo maestro de la publicación *internet pass-thru* en formato HTML. Consulte el apartado “Bibliografía” en la página 175 para obtener más información sobre cómo obtener la documentación en copia impresa.
lib/guiadmin.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 apartado Capítulo 19, “Administración y configuración de internet pass-thru”, en la página 71

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 149. Los siguientes mensajes son un ejemplo de que MQIPT se ha iniciado correctamente:

```
5639-L92 (C) Copyright IBM Corp. 2000, 2003 Reservados todos los derechos
MQCPI001 Arrancando WebSphere MQ internet pass-thru Versión 1.3.0
MQCPI004 Leyendo información de configuración de /opt/mqipt/mqipt.conf
MQCPI008 A la escucha de mandatos de control en la puerta 1881
MQCPI011 Se utilizará la vía de acceso /opt/mqipt/logs para almacenar los
         archivos de anotaciones
MQCPI006 La ruta 1418 se ha iniciado y reenviará mensajes a:
MQCPI034 ....mqserver.company4.com(1414)
MQCPI035 ....utilizando protocolos de MQ
MQCPI078 La ruta 1418 está preparada para las solicitudes de conexión
MQCPI006 La ruta 1415 se ha iniciado y reenviará mensajes a:
MQCPI034 ....mqipt.company2.com(1415)
MQCPI035 ....utilizando protocolos de MQ
MQCPI036 ....parte del Cliente SSL habilitada con las propiedades:
MQCPI031 ......grupos de cifrado <null>
MQCPI032 ......archivo de conjunto de claves /opt/mqipt/KeyMan.pfx
MQCPI038 ......nombres distinguidos CN=*Doe O=IBM OU=* L=* ST=* C=*
MQCPI078 La ruta 1415 está preparada para las solicitudes de conexión
```

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 de `Puertasocks` es 1080.

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

Desinstalación 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 53. Inicie la sesión como usuario `root` y ejecute el mandato `pkgrm`:

```
pkgrm mqipt
```

Capítulo 15. 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/webspheremq/supportpacs`

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.
exits/SampleOneRouteExit.java	Rutina de salida de ejemplo.
exits/SampleOneRouteExit.conf	Archivo de configuración de SampleOneRouteExit.
exits/SampleRoutingExit.java	Rutina de salida de ejemplo.
exits/SampleRoutingExit.conf	Archivo de configuración de SampleRoutingExit.

Archivo	Finalidad
exits/SampleSecurityExit.java	Rutina de salida de ejemplo.
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”.
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/mqiptPW	Cifrado de la contraseña utilizada para abrir un archivo de conjunto de claves.
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>/html/ <nombrearchivo>.zip	Archivo maestro de la publicación *internet pass-thru* en formato HTML. Consulte el apartado “Bibliografía” en la página 175 para obtener más información sobre cómo obtener la documentación en copia impresa.
lib/guiadmin.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 apartado Capítulo 19, “Administración y configuración de internet pass-thru”, en la página 71

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 149. Los siguientes mensajes son un ejemplo de que MQIPT se ha iniciado correctamente:

```
5639-L92 (C) Copyright IBM Corp. 2000, 2003 Reservados todos los derechos
MQCPI001 Arrancando WebSphere MQ internet pass-thru Versión 1.3.0
MQCPI004 Leyendo información de configuración de /usr/opt/mqipt/mqipt.conf
MQCPI008 A la escucha de mandatos de control en la puerta 1881
MQCPI011 Se utilizará la vía de acceso /usr/opt/mqipt/logs para almacenar
         los archivos de anotaciones
MQCPI006 La ruta 1418 se ha iniciado y reenviará mensajes a:
MQCPI034 ....mqserver.company4.com(1414)
MQCPI035 ....utilizando protocolos de MQ
MQCPI078 La ruta 1418 está preparada para las solicitudes de conexión
MQCPI006 La ruta 1415 se ha iniciado y reenviará mensajes a:
MQCPI034 ....mqipt.company2.com(1415)
MQCPI035 ....utilizando protocolos de MQ
MQCPI036 ....parte del Cliente SSL habilitada con las propiedades:
MQCPI031 ......grupos de cifrado <null>
MQCPI032 ......archivo de conjunto de claves /usr/opt/mqipt/KeyMan.pfx
MQCPI038 ......nombres distinguidos CN=*Doe O=IBM OU=* L=* ST=* C=*
MQCPI078 La ruta 1415 está preparada para las solicitudes de conexión
```

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 de `Puertasocks` es 1080.

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

Desinstalación 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 57. Inicie la sesión como usuario `root` y ejecute el mandato `installp`:

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

Capítulo 16. 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/webspheremq/supportpacs`

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.
exits/ SampleOneRouteExit.java	Rutina de salida de ejemplo.
exits/ SampleOneRouteExit.conf	Archivo de configuración de SampleOneRouteExit.
exits/SampleRoutingExit.java	Rutina de salida de ejemplo.

Archivo	Finalidad
exits/SampleRoutingExit.conf	Archivo de configuración de SampleRoutingExit.
exits/SampleSecurityExit.java	Rutina de salida de ejemplo.
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”.
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/mqiptPW	Cifrado de la contraseña utilizada para abrir un archivo de conjunto de claves.
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>/html/ <nombrearchivo>.zip	Archivo maestro de la publicación *internet pass-thru* en formato HTML. Consulte el apartado “Bibliografía” en la página 175 para obtener más información sobre cómo obtener la documentación en copia impresa.
lib/guiadmin.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 apartado Capítulo 19, “Administración y configuración de internet pass-thru”, en la página 71

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 149. Los siguientes mensajes son un ejemplo de que MQIPT se ha iniciado correctamente:

```
5639-L92 (C) Copyright IBM Corp. 2000, 2003 Reservados todos los derechos
MQCPI001 Arrancando WebSphere MQ internet pass-thru Versión 1.3.0
MQCPI004 Leyendo información de configuración de /opt/mqipt/mqipt.conf
MQCPI008 A la escucha de mandatos de control en la puerta 1881
MQCPI011 Se utilizará la vía de acceso /opt/mqipt/logs para almacenar
         los archivos de anotaciones
MQCPI006 La ruta 1418 se ha iniciado y reenviará mensajes a:
MQCPI034 ....mqserver.company4.com(1414)
MQCPI035 ....utilizando protocolos de MQ
MQCPI078 La ruta 1418 está preparada para las solicitudes de conexión
MQCPI006 La ruta 1415 se ha iniciado y reenviará mensajes a:
MQCPI034 ....mqipt.company2.com(1415)
MQCPI035 ....utilizando protocolos de MQ
MQCPI036 ....parte del Cliente SSL habilitada con las propiedades:
MQCPI031 ......grupos de cifrado <null>
MQCPI032 ......archivo de conjunto de claves /opt/mqipt/KeyMan.pfx
MQCPI038 ......nombres distinguidos CN=*Doe O=IBM OU=* L=* ST=* C=*
MQCPI078 La ruta 1415 está preparada para las solicitudes de conexión
```

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 de `Puertasocks` es 1080.

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

Desinstalación 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 61. Inicie la sesión como usuario `root` y ejecute el mandato `swremove`:

```
swremove MQIPT
```

Capítulo 17. 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/webspheremq/supportpacs
```

Siga las instrucciones para descargar los archivos.

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

```
login root
cd /tmp
uncompress -fv ms81_linux.tar.z
tar xvf ms81_linux.tar
cd i386
rpm -i WebSphereMQ-IPT-1.3.0-0.i386.rpm
```

En el ejemplo se presupone que `ms81_linux.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.
exits/ SampleOneRouteExit.java	Rutina de salida de ejemplo.
exits/ SampleOneRouteExit.conf	Archivo de configuración de SampleOneRouteExit.
exits/SampleRoutingExit.java	Rutina de salida de ejemplo.

Archivo	Finalidad
exits/SampleRoutingExit.conf	Archivo de configuración de SampleRoutingExit.
exits/SampleSecurityExit.java	Rutina de salida de ejemplo.
lib/libmqiptqos.so	Biblioteca ficticia para TQoS
bin/mqiptQoS	Para utilizar la biblioteca TQoS real
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”.
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/mqiptPW	Cifrado de la contraseña utilizada para abrir un archivo de conjunto de claves.
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>/html/ <nombrearchivo>.zip	Archivo maestro de la publicación *internet pass-thru* en formato HTML. Consulte el apartado “Bibliografía” en la página 175 para obtener más información sobre cómo obtener la documentación en copia impresa.
lib/guiadmin.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 apartado Capítulo 19, “Administración y configuración de internet pass-thru”, en la página 71

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 149. Los siguientes mensajes son un ejemplo de que MQIPT se ha iniciado correctamente:

```
5639-L92 (C) Copyright IBM Corp. 2000, 2003 Reservados todos los derechos
MQCPI001 Arrancando WebSphere MQ internet pass-thru Versión 1.3.0
MQCPI004 Leyendo información de configuración de /opt/mqipt/mqipt.conf
MQCPI008 A la escucha de mandatos de control en la puerta 1881
MQCPI011 Se utilizará la vía de acceso /opt/mqipt/logs para almacenar
         los archivos de anotaciones
MQCPI006 La ruta 1418 se ha iniciado y reenviará mensajes a:
MQCPI034 ....mqserver.company4.com(1414)
MQCPI035 ....utilizando protocolos de MQ
MQCPI078 La ruta 1418 está preparada para las solicitudes de conexión
MQCPI006 La ruta 1415 se ha iniciado y reenviará mensajes a:
MQCPI034 ....mqipt.company2.com(1415)
MQCPI035 ....utilizando protocolos de MQ
MQCPI036 ....parte del Cliente SSL habilitada con las propiedades:
MQCPI031 ......grupos de cifrado <null>
MQCPI032 ......archivo de conjunto de claves /opt/mqipt/KeyMan.pfx
MQCPI038 ......nombres distinguidos CN=*Doe O=IBM OU=* L=* ST=* C=*
MQCPI078 La ruta 1415 está preparada para las solicitudes de conexión
```

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 de `Puertasocks` es 1080.

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

Desinstalación 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 65. Inicie la sesión como usuario `root` y ejecute el mandato `swremove`:

```
rpm -e WebSphereMQ-IPT-1.3.0-0
```

Capítulo 18. Instalación en un sistema UNIX genérico

Se proporciona un archivo tar que contiene una imagen de disco de todos los archivos MQIPT comunes, para su uso general. El objetivo de este archivo es permitir que se instale MQIPT en aquellas plataformas UNIX a las que MQIPT no da soporte con sus propias imágenes de instalación. El objetivo que se pretende conseguir es desempaquetar el archivo tar en una ubicación específica y, efectuando los mínimos cambios posibles, permitir implementar MQIPT en cualquier plataforma que dé soporte a Java 1.4. Es posible que deba modificarse el script mqiptEnv, ubicado en el subdirectorio bin, para poder reflejar la ubicación de los archivos instalados.

Descarga e instalación de los archivos

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

```
http://www.ibm.com/webspheremq/supportpacs
```

Siga las instrucciones para descargar los archivos.

Inicie la sesión como root y desempaquete el archivo ms81.tar en el directorio de destino, tal como se indica en el ejemplo:

```
login root
cd /
mkdir mqipt
cd mqipt
cp /tmp/ms81.tar /mqipt/.
tar xvf ms81.tar
```

En el ejemplo se presupone que ms81.tar se ha descargado 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.

Archivo	Finalidad
ssl/KeyMan.zip	Programa de utilidad KeyMan.
exits/ SampleOneRouteExit.java	Rutina de salida de ejemplo.
exits/ SampleOneRouteExit.conf	Archivo de configuración de SampleOneRouteExit.
exits/SampleRoutingExit.java	Rutina de salida de ejemplo.
exits/SampleRoutingExit.conf	Archivo de configuración de SampleRoutingExit.
exits/SampleSecurityExit.java	Rutina de salida de ejemplo.
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”.
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/mqiptPW	Cifrado de la contraseña utilizada para abrir un archivo de conjunto de claves.
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>/html/ <nombrearchivo>.zip	Archivo maestro de la publicación *internet pass-thru* en formato HTML. Consulte el apartado “Bibliografía” en la página 175 para obtener más información sobre cómo obtener la documentación en copia impresa.
lib/guiadmin.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 apartado Capítulo 19, "Administración y configuración de internet pass-thru", en la página 71

En este ejemplo se presupone que MQIPT se desempaquetará en un directorio llamado mqipt. Debe actualizar el script mqiptEnv con la nueva ubicación de las bibliotecas de tiempo de ejecución. El valor por omisión de la variable MQIPT_CP es:

```
MQIPT_CP=/opt/mqipt/lib/MQipt.jar:/opt/mqipt/lib/guiadmin.jar
```

En este ejemplo, debe cambiarse por:

```
MQIPT_CP=/mqipt/opt/mqipt/lib/MQipt.jar:/mqipt/opt/mqipt/lib/guiadmin.jar
```

También debe actualizar todos los scripts de tiempo de ejecución antes de utilizarlos y cambiar el nombre de vía de acceso completo de la ubicación del script mqiptEnv. Por tanto, antes de utilizar el script mqipt, por ejemplo, debe editarlo y cambiar la sentencia que aparece después del comentario `Get classpath`:

```
/opt/mqipt/bin/mqiptEnv
```

a

```
/mqipt/opt/mqipt/bin/mqiptEnv
```

Inicio de internet pass-thru desde la línea de mandatos

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

```
cd /mqipt/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 149. Los siguientes mensajes son un ejemplo de que MQIPT se ha iniciado correctamente:

```
5639-L92 (C) Copyright IBM Corp. 2000, 2003 Reservados todos los derechos
MQCPI001 Arrancando WebSphere MQ internet pass-thru Versión 1.3.0
MQCPI004 Leyendo información de configuración de /mqipt/opt/mqipt/mqipt.conf
MQCPI008 A la escucha de mandatos de control en la puerta 1881
MQCPI011 Se utilizará la vía de acceso /mqipt/opt/mqipt/logs para almacenar
         los archivos de anotaciones
MQCPI006 La ruta 1418 se ha iniciado y reenviará mensajes a:
MQCPI034 ....mqserver.company4.com(1414)
MQCPI035 ....utilizando protocolos de MQ
MQCPI078 La ruta 1418 está preparada para las solicitudes de conexión
MQCPI006 La ruta 1415 se ha iniciado y reenviará mensajes a:
MQCPI034 ....mqipt.company2.com(1415)
MQCPI035 ....utilizando protocolos de MQ
MQCPI036 ....parte del Cliente SSL habilitada con las propiedades:
MQCPI031 ......grupos de cifrado <null>
MQCPI032 ......archivo de conjunto de claves /mqipt/opt/mqipt/KeyMan.pfx
MQCPI038 ......nombres distinguidos CN=*Doe O=IBM OU=* L=* ST=* C=*
MQCPI078 La ruta 1415 está preparada para las solicitudes de conexión
```

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

La capacidad de iniciar un servicio automáticamente depende de cada plataforma. El script mqiptService se proporciona únicamente como ejemplo de cómo se lleva a cabo en un sistema Sun Solaris. En función de los requisitos del sistema, es posible que resulte más fácil usar programas de utilidad específicos de la plataforma para instalar MQIPT como un servicio.

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 /mqipt/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 de `Puertasocks` es 1080.

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

Desinstalación de internet pass-thru

Como MQIPT no se instaló mediante una imagen instalable de sistema, puede desinstalarse suprimiendo la estructura de directorios en la que se instaló.

Si MQIPT se configuró para ejecutarse como un servicio del sistema, suprima el servicio antes de desinstalar el código.

Capítulo 19. 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 75
- "Información de consulta relacionada con la configuración" en la página 76

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.

Tenga en cuenta que el cliente de administración no necesita Java 1.4. como requisito previo.

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 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.

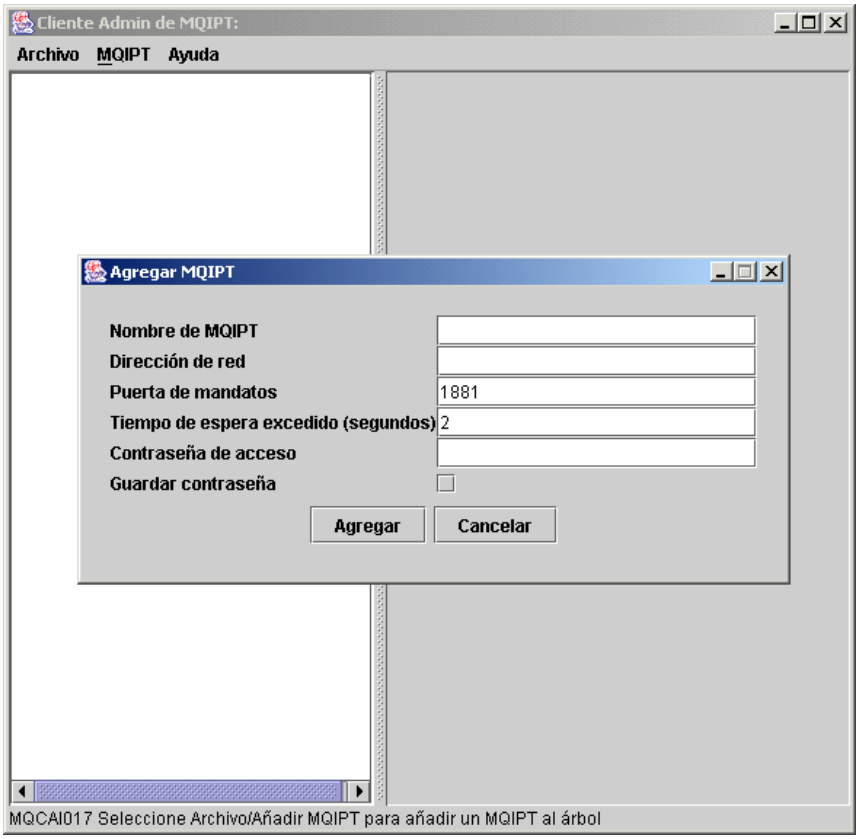

Figura 8. Ventana para acceder por primera vez a un MQIPT

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.

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 71.

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 71.

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.

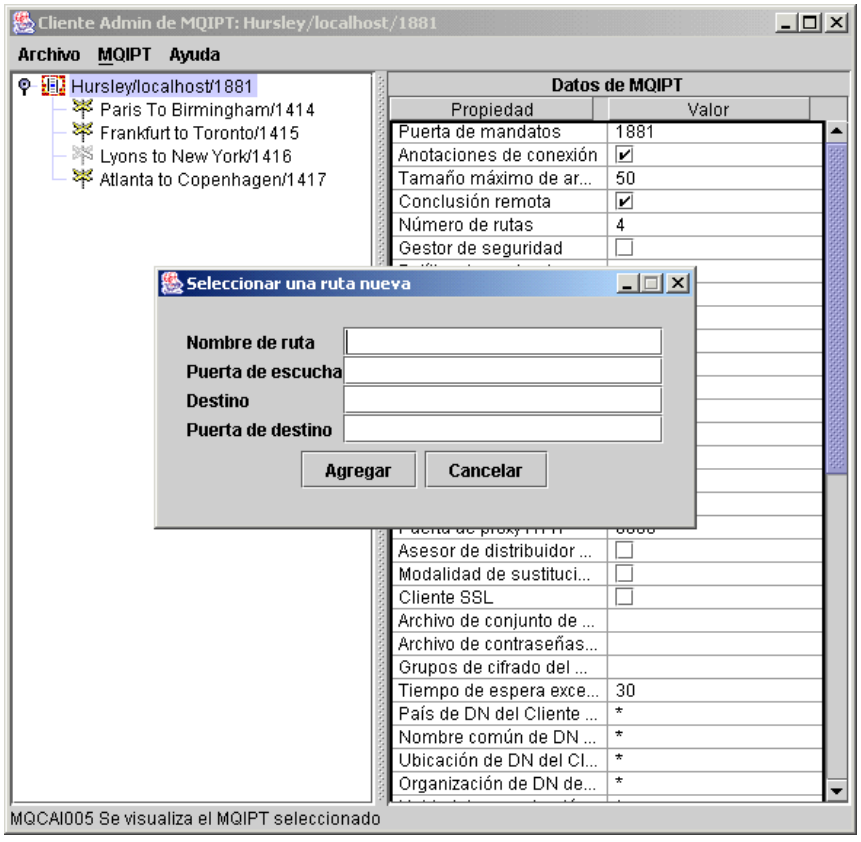

Figura 9. Adición de una ruta

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 de MQIPT, esta opción envía un archivo de configuración nuevo a 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 a MQIPT para indicarle que detenga su ejecución. Después de este mandato, perderá el contacto con 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 76 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

MQIPT utiliza un archivo de configuración denominado mqipt.conf para definir rutas y controlar las acciones del servidor MQIPT. El archivo consta de un conjunto de secciones. Hay una sección global y una sección adicional para cada ruta que se ha definido mediante MQIPT.

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.

Para cambiar las propiedades, puede hacerlo editando el archivo mqipt.conf o utilizando la GUI del cliente de administración. Para aplicar los cambios efectuados, el administrador puede emitir un mandato refresh, bien desde la GUI del cliente de administración o mediante el script mqiptAdmin.

Los cambios efectuados a ciertas propiedades sólo provocarán que una ruta se reinicie si ya hay otras propiedades que ya estén habilitadas. Por ejemplo, los cambios efectuados en las propiedades HTTP sólo entrarán vigor si la propiedad HTTP también está habilitada.

Al reiniciar una ruta, las conexiones existentes se cancelan. Para alterar temporalmente este comportamiento, establezca la propiedad RouteRestart en false. Esto evita que la ruta se reinicie, y permite que las conexiones existentes permanezcan activas hasta que se vuelve a habilitar la propiedad RouteRestart.

Si desea obtener información sobre cómo realizar algunas configuraciones sencillas, consulte el apartado Capítulo 20, “Iniciación a internet pass-thru”, en la página 95. Para consultar una configuración de ejemplo, vea el archivo `mqiptSample.conf` en el directorio inicial de MQIPT.

Resumen de las propiedades

En la Tabla 3 se muestra lo siguiente:

- Todas las propiedades.
- Si la propiedad se aplica a la sección global, a la sección de ruta o ambas secciones.
- Si falta una propiedad en la sección de ruta y en la sección global, se utilizan los valores por omisión.

Tabla 3. Resumen de las propiedades de configuración

Nombre de la propiedad	Global	Ruta	Valor por omisión
AccessPW	yes	no	<null>
Active	yes	yes	true
ClientAccess	yes	yes	false
CommandPort	yes	no	<null>
ConnectionLog	yes	no	true
Destination	no	yes	<null>
DestinationPort	no	yes	1414
HTTP[6,7]	yes	yes	false
HTTPChunking[1]	yes	yes	false
HTTPProxy[1]	yes	yes	<null>
HTTPProxyPort[1]	yes	yes	8080
HTTPS[1]	yes	yes	false
HTTPServer[1]	yes	yes	<null>

Tabla 3. Resumen de las propiedades de configuración (continuación)

Nombre de la propiedad	Global	Ruta	Valor por omisión
HTTPServerPort[1]	yes	yes	<null>
IdleTimeout	yes	yes	0
IgnoreExpiredCRLs	yes	yes	false
LDAP	yes	yes	false
LDAPIgnoreErrors[10]	yes	yes	false
LDAPCacheTimeout[10]	yes	yes	24
LDAPSaveCRL[10]	yes	yes	false
LDAPServer1[10]	yes	yes	<null>
LDAPServer1Port[10]	yes	yes	389
LDAPServer1Userid[10]	yes	yes	<null>
LDAPServer1Password[10]	yes	yes	<null>
LDAPServer1Timeout[10]	yes	yes	0
LDAPServer2[10]	yes	yes	<null>
LDAPServer2Port[10]	yes	yes	389
LDAPServer2Userid[10]	yes	yes	<null>
LDAPServer2Password[10]	yes	yes	<null>
LDAPServer2Timeout[10]	yes	yes	0
ListenerPort	no	yes	<null>
LocalAddress	yes	yes	<null>
LogDir (sólo es válido para MQIPTServlet)	no	no	<null>
MaxConnectionThreads	yes	yes	100
MaxLogFileSize	yes	no	50
MinConnectionThreads	yes	yes	5
Name	no	yes	<null>
NDAdvisor	yes	yes	false
NDAdvisorReplaceMode[4]	yes	yes	false
OutgoingPort	no	yes	0
QMgrAccess	yes	yes	true
QoS (sólo puede utilizarse en Linux)	yes	yes	false
QosToCaller[9]	yes	yes	1
QosToDest[9]	yes	yes	1
RemoteShutdown	yes	no	false
RouteRestart	yes	yes	true
SecurityExit	yes	yes	false
SecurityExitName[11]	yes	yes	<null>
SecurityExitPath[11]	yes	yes	<ipthome>\exits
SecurityExitTimeout[11]	yes	yes	5
SecurityManager	yes	no	false

Tabla 3. Resumen de las propiedades de configuración (continuación)

Nombre de la propiedad	Global	Ruta	Valor por omisión
SecurityManagerPolicy	yes	no	<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
SSLClientCAKeyRing[2]	yes	yes	<null>
SSLClientCAKeyRingPW[2]	yes	yes	<null>
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>
SSLClientSiteDN_C[2]	yes	yes	"*"[5]
SSLClientSiteDN_CN[2]	yes	yes	"*"[5]
SSLClientSiteDN_L[2]	yes	yes	"*"[5]
SSLClientSiteDN_O[2]	yes	yes	"*"[5]
SSLClientSiteDN_OU[2]	yes	yes	"*"[5]
SSLClientSiteDN_ST[2]	yes	yes	"*"[5]
SSLClientSiteLabel[2]	yes	yes	<null>
SSLProxyMode	yes	yes	false
SSLServer[6]	yes	yes	false
SSLServerAskClientAuth[3]	yes	yes	false
SSLServerCAKeyRing[3]	yes	yes	<null>
SSLServerCAKeyRingPW[3]	yes	yes	<null>
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>

Tabla 3. Resumen de las propiedades de configuración (continuación)

Nombre de la propiedad	Global	Ruta	Valor por omisión
SSLServerKeyRingPW[3]	yes	yes	<null>
SSLServerSiteDN_C[3]	yes	yes	"*"[5]
SSLServerSiteDN_CN[3]	yes	yes	"*"[5]
SSLServerSiteDN_L[3]	yes	yes	"*"[5]
SSLServerSiteDN_O[3]	yes	yes	"*"[5]
SSLServerSiteDN_OU[3]	yes	yes	"*"[5]
SSLServerSiteDN_ST[3]	yes	yes	"*"[5]
SSLServerSiteLabel[3]	yes	yes	<null>
Trace	yes	yes	0
UriName (consulte la página "UriName" en la página 94 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.
10. Establezca LDAP en true para que estas propiedades surtan efecto.
11. Establezca SecurityExit 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 81, a excepción de ListenerPort, Destination, DestinationPort, Name y OutgoingPort.

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. Cuando se aumenta el tamaño del archivo 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 31 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, 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 (y HTTP se establece en true), 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 también se ha definido HTTPServer, se emite una petición CONNECT a HTTPProxy, en lugar de una POST normal. Si cambia esta propiedad (y HTTP se establece en true), 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`, a menos que HTTPS se haya establecido en true y no haya

HTTPServer y, en ese caso, el valor por omisión es 443. Si cambia esta propiedad (y HTTP se establece en true), la ruta se detendrá y se reiniciará cuando se emita el mandato REFRESH. Todas las conexiones a esta ruta finalizarán.

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

HTTPS
Habilite esta propiedad para crear peticiones HTTPS. La propiedad HTTP también debe establecerse. Si cambia esta propiedad (y HTTP se establece en true), la ruta se detendrá y se reiniciará cuando se emita el mandato REFRESH. Todas las conexiones a esta ruta finalizarán.

HTTPServerPort
La dirección de la puerta que se ha de utilizar en el servidor HTTP. El valor por omisión es 8080, a menos que HTTPS se haya establecido en true y, en ese caso, el valor por omisión es 443. Si cambia esta propiedad (y HTTP se establece en true), 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.

IgnoreExpiredCRLs
Establezca esta propiedad en true para ignorar una CRL vencida. El valor por omisión es false.

Atención
Si habilita esta propiedad, alguien podrá utilizar un certificado revocado para efectuar una conexión SSL.

LDAP
Establezca esta propiedad en true para habilitar la utilización de un servidor LDAP cuando se utilicen conexiones SSL. MQIPT utilizará el servidor LDAP para recuperar las CRL y las ARL. También deben habilitarse las propiedades SSLClient o SSLServer para que esta propiedad entre en vigor.

LDAPIgnoreErrors
Establezca esta propiedad en true para ignorar todos los errores de tiempo de espera excedido o de conexión cuando efectúe una búsqueda LDAP. Si MQIPT no puede llevar a cabo una búsqueda satisfactoria, no permitirá que se complete la conexión con el cliente, a menos que esta propiedad se haya habilitado. Se considera que una búsqueda ha sido satisfactoria cuando se ha recuperado una CRL o no hay ninguna CRL disponible para la CA especificada. Si cambia esta propiedad (y LDAP se establece en true), la ruta se detendrá y se reiniciará cuando se emita el mandato REFRESH. Todas las conexiones a esta ruta finalizarán.

Atención

Si habilita esta propiedad, alguien podrá utilizar un certificado revocado para efectuar una conexión SSL.

LDAPCacheTimeout
Cuando se haya recuperado una CRL de un servidor LDAP, se almacenará internamente en MQIPT en una antememoria temporal. Las entradas de esta antememoria caducarán una vez transcurrido cierto tiempo de espera excedido, especificado por esta propiedad. El valor por omisión es de 24 horas. Si se especifica un valor de tiempo de espera excedido de 0 se indica que las entradas de la antememoria no caducarán hasta que se reinicie la ruta. Si cambia esta propiedad (y LDAP se establece en true), la ruta se detendrá y se reiniciará cuando se emita el mandato REFRESH. Todas las conexiones a esta ruta finalizarán.

LDAPSaveCRL
Establezca esta propiedad en true para actualizar el archivo de conjunto de claves proporcionado con cualquiera de las CRL recuperadas del servidor LDAP. Los archivos de conjunto de claves se especifican con las propiedades SSLClientKeyRing, SSLClientCAKeyRing, SSLServerKeyRing y SSLServerCAKeyRing. Esto implica que MQIPT debe tener acceso de escritura en los archivos de conjunto de claves. Si cambia esta propiedad (y LDAP se establece en true), la ruta se detendrá y se reiniciará cuando se emita el mandato REFRESH. Todas las conexiones a esta ruta finalizarán.

LDAPServer1
Establezca esta propiedad en el nombre del sistema principal o la dirección IP del servidor LDAP principal. Esta propiedad debe establecerse si se ha habilitado LDAP. Si cambia esta propiedad (y LDAP se establece en true), la ruta se detendrá y se reiniciará cuando se emita el mandato REFRESH. Todas las conexiones a esta ruta finalizarán.

LDAPServer1Port
Establezca esta propiedad en la dirección de la puerta de escucha o la dirección IP del servidor LDAP principal. Tiene un valor por omisión de 389. Si cambia esta propiedad (y LDAP se establece en true), la ruta se detendrá y se reiniciará cuando se emita el mandato REFRESH. Todas las conexiones a esta ruta finalizarán.

LDAPServer1Userid
Establezca esta propiedad en el ID de usuario necesario para acceder al servidor LDAP principal. Esta propiedad debe establecerse si se requiere autorización para poder acceder al servidor LDAP principal. Si cambia esta propiedad (y LDAP se establece en true), la ruta se detendrá y se reiniciará cuando se emita el mandato REFRESH. Todas las conexiones a esta ruta finalizarán.

LDAPServer1Password
Establezca esta propiedad en la contraseña necesaria para acceder al servidor LDAP principal. Esta propiedad debe establecerse si se ha establecido LDAPServer1Userid. Si cambia esta propiedad (y LDAP se establece en true), la ruta se detendrá y se reiniciará cuando se emita el mandato REFRESH. Todas las conexiones a esta ruta finalizarán.

LDAPServer1Timeout
Establezca esta propiedad en el número de segundos que MQIPT esperará una respuesta del servidor LDAP principal. Tiene un valor por omisión de 0, que

indica que la conexión no tendrá ningún tiempo de espera excedido. Si cambia esta propiedad (y LDAP se establece en true), la ruta se detendrá y se reiniciará cuando se emita el mandato REFRESH. Todas las conexiones a esta ruta finalizarán.

LDAPServer2
Establezca esta propiedad en el nombre del sistema principal o la dirección IP del servidor LDAP de copia de seguridad. Esta propiedad es opcional. Si cambia esta propiedad (y LDAP se establece en true), la ruta se detendrá y se reiniciará cuando se emita el mandato REFRESH. Todas las conexiones a esta ruta finalizarán.

LDAPServer2Port
Establezca esta propiedad en la dirección de la puerta de escucha o la dirección IP del servidor LDAP de copia de seguridad. Tiene un valor por omisión de 389. Si cambia esta propiedad (y LDAP se establece en true), la ruta se detendrá y se reiniciará cuando se emita el mandato REFRESH. Todas las conexiones a esta ruta finalizarán.

LDAPServer2Userid
Establezca esta propiedad en el ID de usuario necesario para acceder al servidor LDAP de copia de seguridad. Esta propiedad debe establecerse si se requiere autorización para poder acceder al servidor LDAP de copia de seguridad. Si cambia esta propiedad (y LDAP se establece en true), la ruta se detendrá y se reiniciará cuando se emita el mandato REFRESH. Todas las conexiones a esta ruta finalizarán.

LDAPServer2Password
Establezca esta propiedad en la contraseña necesaria para acceder al servidor LDAP de copia de seguridad. Esta propiedad debe establecerse si se ha habilitado LDAPServer2. Si cambia esta propiedad (y LDAP se establece en true), la ruta se detendrá y se reiniciará cuando se emita el mandato REFRESH. Todas las conexiones a esta ruta finalizarán.

LDAPServer2Timeout
Establezca esta propiedad en el número de segundos que MQIPT esperará una respuesta del servidor LDAP de copia de seguridad. Tiene un valor por omisión de 0, que indica que la conexión no tendrá ningún tiempo de espera excedido. Si cambia esta propiedad (y LDAP se establece en true), la ruta se detendrá y se reiniciará cuando se emita el mandato REFRESH. Todas las conexiones a esta ruta finalizarán.

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.

LocalAddress
La dirección IP local a la que enlazar todas las conexiones. Si cambia esta propiedad, la ruta se detendrá y se reiniciará cuando se emita el mandato REFRESH. Todas las conexiones a esta ruta finalizarán.

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). Éste 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`.

OutgoingPort
Ésta es la dirección de la puerta inicial que utilizan las conexiones de salida. El rango de direcciones de puerta coincide con el valor `MaxConnectionThread` de esta ruta. Un valor por omisión de `0` utilizará una dirección de puerta definida por el sistema. Si cambia esta propiedad, la ruta se detendrá y se reiniciará cuando se emita el mandato REFRESH. Todas las conexiones a esta ruta finalizarán.

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. Por ejemplo, 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). Por ejemplo, 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.

RouteRestart
Establezca esta propiedad en false para evitar que la ruta se reinicie cuando se cambien otras propiedades de la ruta y se haya emitido un mandato REFRESH. El valor por omisión de esta propiedad es true.

SecurityExit
Establezca esta propiedad en true para habilitar una rutina de salida de seguridad definida por el usuario. El valor por omisión de esta propiedad es false.

SecurityExitName
El nombre de clase de la rutina de salida de seguridad definida por el usuario. Esta propiedad debe establecerse si SecurityExit se ha establecido en true. Si cambia esta propiedad (y SecurityExit se establece en true), la ruta se detendrá y se reiniciará cuando se emita el mandato REFRESH. Todas las conexiones a esta ruta finalizarán.

SecurityExitPath
El nombre de vía de acceso completo que contiene la rutina de salida de seguridad definida por el usuario. Si esta propiedad no se ha establecido, tomará como valor por omisión el subdirectorio exits. La propiedad también puede definir el nombre de un archivo jar que contiene la rutina de salida de seguridad definida por el usuario. Si cambia esta propiedad (y SecurityExit se establece en true), la ruta se detendrá y se reiniciará cuando se emita el mandato REFRESH. Todas las conexiones a esta ruta finalizarán.

SecurityExitTimeout
MQIPT utiliza este valor de tiempo de espera excedido para determinar cuánto tiempo (en segundos) debe esperar una respuesta al validar una petición de conexión. El valor por omisión es de 5 segundos. Si cambia esta propiedad (y SecurityExit 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 o bien un servidor/proxy HTTP. Debe especificar el nombre del archivo de conjunto de claves con las propiedades SSLClientKeyRing o SSLClientCAKeyRing. 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

SSLClientCAKeyRing
El nombre de archivo totalmente calificado del archivo de conjunto de claves que contiene los certificados de CA, que se utiliza para autenticar certificados del servidor SSL. En las plataformas Windows, debe utilizar una barra doble

invertida (\\) como separador de archivos. Si cambia esta propiedad (y SSLClient se establece en true), la ruta se detendrá y se reiniciará cuando se emita el mandato REFRESH. Todas las conexiones a esta ruta finalizarán.

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

SSLClientCipherSuites
El nombre de la suite de cifrado SSL que se ha de utilizar en la parte 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 (y SSLClient se establece en true), 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 cambia esta propiedad (y SSLClient se establece en true), la ruta se detendrá y se reiniciará cuando se emita el mandato REFRESH. Todas las conexiones a esta ruta finalizarán.

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 país". Si cambia esta propiedad (y SSLClient se establece en true), 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 de país". Si cambia esta propiedad (y SSLClient se establece en true), 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 (y SSLClient se establece en true), 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 (y SSLClient se establece en true), 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 (y SSLClient se establece en true), 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 (y SSLClient se establece en true), 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 (y SSLClient se establece en true), 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 (y SSLClient se establece en true), la ruta se detendrá y se reiniciará cuando se emita el mandato REFRESH. Todas las conexiones a esta ruta finalizarán.

SSLClientSiteDN_C
Utilice esta propiedad para especificar un nombre de país para seleccionar un certificado que deba enviarse al servidor SSL. Si no especifica esta propiedad, se presuponen "todos los países". Si cambia esta propiedad (y SSLClient se establece en true), la ruta se detendrá y se reiniciará cuando se emita el mandato REFRESH. Todas las conexiones a esta ruta finalizarán.

SSLClientSiteDN_CN
Utilice esta propiedad para especificar un nombre común para seleccionar un certificado que deba enviarse al servidor SSL. Si no especifica esta propiedad, se presuponen "todos los nombres comunes". Si cambia esta propiedad (y SSLClient se establece en true), la ruta se detendrá y se reiniciará cuando se emita el mandato REFRESH. Todas las conexiones a esta ruta finalizarán.

SSLClientSiteDN_L
Utilice esta propiedad para especificar un nombre de ubicación para seleccionar un certificado que deba enviarse al servidor SSL. Si no especifica esta propiedad, se presuponen "todos los nombres de ubicación". Si cambia esta propiedad (y SSLClient se establece en true), la ruta se detendrá y se reiniciará cuando se emita el mandato REFRESH. Todas las conexiones a esta ruta finalizarán.

SSLClientSiteDN_O
Utilice esta propiedad para especificar un nombre de organización para seleccionar un certificado que deba enviarse al servidor SSL. Si no especifica esta propiedad, se presuponen "todos los nombres de organización". Si cambia esta propiedad (y SSLClient se establece en true), la ruta se detendrá y se reiniciará cuando se emita el mandato REFRESH. Todas las conexiones a esta ruta finalizarán.

SSLClientSiteDN_OU
Utilice esta propiedad para especificar un nombre de unidad organizativa para seleccionar un certificado que deba enviarse al servidor SSL. Si no especifica esta propiedad, se presuponen ″todos los nombres de unidades organizativas″. Si cambia esta propiedad (y SSLClient se establece en true), la ruta se detendrá y se reiniciará cuando se emita el mandato REFRESH. Todas las conexiones a esta ruta finalizarán.

SSLClientSiteDN_ST
Utilice esta propiedad para especificar un nombre de estado para seleccionar un certificado que deba enviarse al servidor SSL. Si no especifica esta propiedad, se presuponen ″todos los nombres de estado″. Si cambia esta propiedad (y SSLClient se establece en true), la ruta se detendrá y se reiniciará cuando se emita el mandato REFRESH. Todas las conexiones a esta ruta finalizarán.

SSLClientSiteLabel
Utilice esta propiedad para especificar un nombre de etiqueta para seleccionar un certificado que deba enviarse al servidor SSL. Si no especifica esta propiedad, se presuponen ″todos los nombres de etiqueta″. Si cambia esta propiedad (y SSLClient se establece en true), 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

SSLServerCAKeyRing
El nombre de archivo totalmente calificado del archivo de conjunto de claves que contiene los certificados de CA, que se utiliza para autenticar certificados del cliente SSL. En las plataformas Windows, debe utilizar una barra doble invertida (`\\`) como separador de archivos. Si cambia esta propiedad (y SSLServer se establece en true), la ruta se detendrá y se reiniciará cuando se emita el mandato REFRESH. Todas las conexiones a esta ruta finalizarán.

SSLServerCAKeyRingPW
El nombre de archivo totalmente calificado que contiene la contraseña para

abrir el conjunto de claves de CA del servidor. En las plataformas Windows, debe utilizar una barra doble invertida (\\) como separador de archivos. Si cambia esta propiedad (y SSLServer se establece en true), la ruta se detendrá y se reiniciará cuando se emita el mandato REFRESH. Todas las conexiones a esta ruta finalizarán.

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 (y SSLServer se establece en true), 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 la parte 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 (y SSLServer se establece en true), 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 (y SSLServer se establece en true), 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 (y SSLServer se establece en true), 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 (y SSLServer se establece en true), 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 (y SSLServer se establece en true), 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 (y

SSLServer se establece en true), 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 (y SSLServer se establece en true), 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 (y SSLServer se establece en true), 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 (y SSLServer se establece en true), la ruta se detendrá y se reiniciará cuando se emita el mandato REFRESH. Todas las conexiones a esta ruta finalizarán.

SSLServerSiteDN_C
Utilice esta propiedad para especificar un nombre de país para seleccionar un certificado que deba enviarse al cliente SSL. Si no especifica esta propiedad, se presuponen ″todos los países″. Si cambia esta propiedad (y SSLServer se establece en true), la ruta se detendrá y se reiniciará cuando se emita el mandato REFRESH. Todas las conexiones a esta ruta finalizarán.

SSLServerSiteDN_CN
Utilice esta propiedad para especificar un nombre común para seleccionar un certificado que deba enviarse al cliente SSL. Si no especifica esta propiedad, se presuponen ″todos los nombres comunes″. Si cambia esta propiedad (y SSLServer se establece en true), la ruta se detendrá y se reiniciará cuando se emita el mandato REFRESH. Todas las conexiones a esta ruta finalizarán.

SSLServerSiteDN_L
Utilice esta propiedad para especificar un nombre de ubicación para seleccionar un certificado que deba enviarse al cliente SSL. Si no especifica esta propiedad, se presuponen ″todas las ubicaciones″. Si cambia esta propiedad (y SSLServer se establece en true), la ruta se detendrá y se reiniciará cuando se emita el mandato REFRESH. Todas las conexiones a esta ruta finalizarán.

SSLServerSiteDN_O
Utilice esta propiedad para especificar un nombre de organización para seleccionar un certificado que deba enviarse al cliente SSL. Si no especifica esta propiedad, se presuponen ″todos los nombres de organización″. Si cambia esta propiedad (y SSLServer se establece en true), la ruta se detendrá y se reiniciará cuando se emita el mandato REFRESH. Todas las conexiones a esta ruta finalizarán.

SSLServerSiteDN_OU
Utilice esta propiedad para especificar un nombre de unidad organizativa para seleccionar un certificado que deba enviarse al cliente SSL. Si no especifica esta

propiedad, se presuponen ″todos los nombres de unidades organizativas″. Si cambia esta propiedad (y SSLServer se establece en true), la ruta se detendrá y se reiniciará cuando se emita el mandato REFRESH. Todas las conexiones a esta ruta finalizarán.

SSLServerSiteDN_ST
Utilice esta propiedad para especificar un nombre de estado para seleccionar un certificado que deba enviarse al cliente SSL. Si no especifica esta propiedad, se presuponen ″todos los nombres de estado″. Si cambia esta propiedad (y SSLServer se establece en true), la ruta se detendrá y se reiniciará cuando se emita el mandato REFRESH. Todas las conexiones a esta ruta finalizarán.

SSLServerSiteLabel
Utilice esta propiedad para especificar un nombre de etiqueta para seleccionar un certificado que deba enviarse al cliente SSL. Si no especifica esta propiedad, se presuponen ″todos los nombres de etiqueta″. Si cambia esta propiedad (y SSLServer se establece en true), 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 del proxy HTTP es:

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

El valor por omisión del 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 20. 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 siguientes.

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 95

Prueba de verificación de la instalación

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

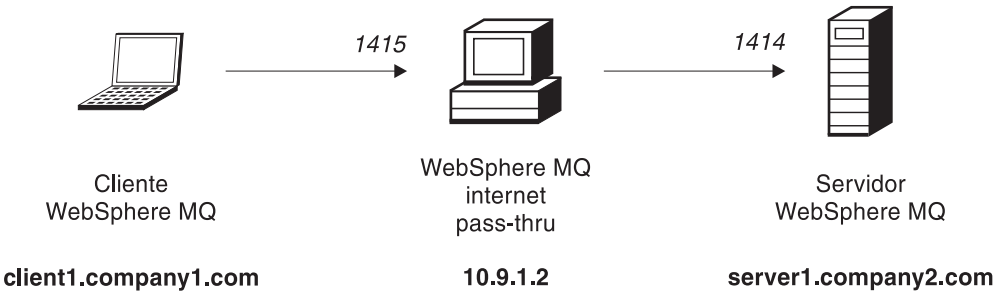

Figura 10. Diagrama de la red IVT

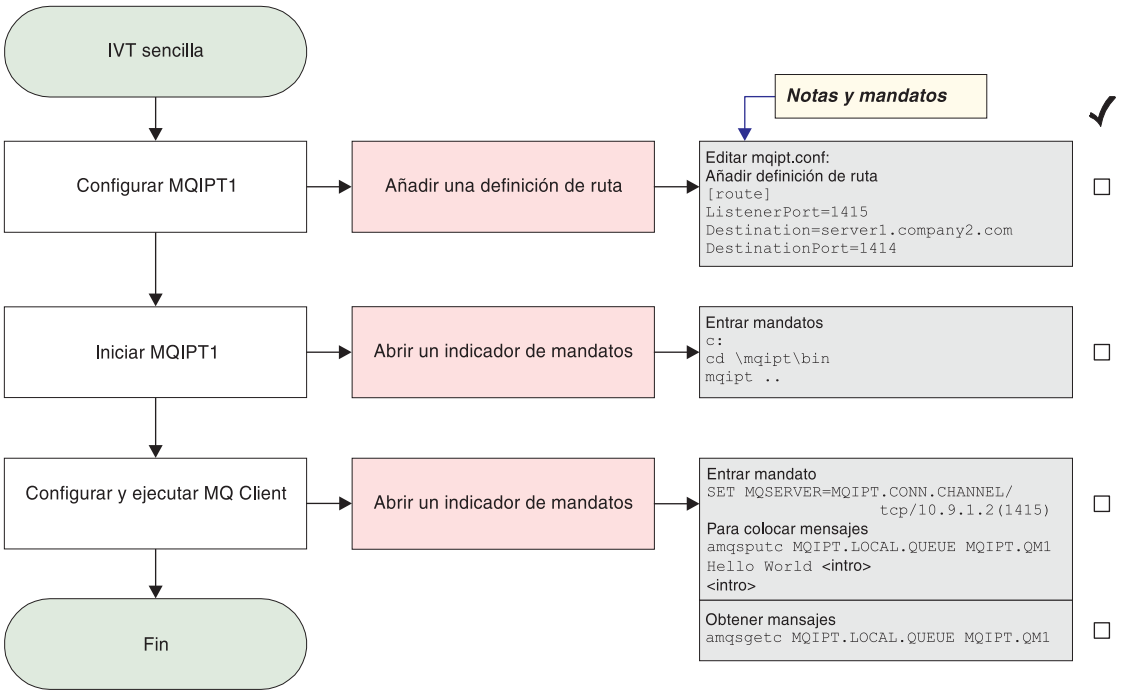

Figura 11. Configuración de IVT

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, 2003 Reservados todos los derechos
   MQCPI001 Arrancando WebSphere MQ internet pass-thru Versión 1.3.0
   MQCPI004 Leyendo información de configuración de C:\mqipt\mqipt.conf
   MQCPI011 Se utilizará la vía de acceso C:\mqipt\logs para almacenar
            los archivos de anotaciones
   MQCPI006 La ruta 1415 se ha iniciado y reenviará mensajes a:
   MQCPI034 ....server1.company2.com(1414)
   MQCPI035 ....utilizando protocolos de MQ
   MQCPI078 La ruta 1415 está preparada para las solicitudes de conexión
   ```

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 96.) 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 115.

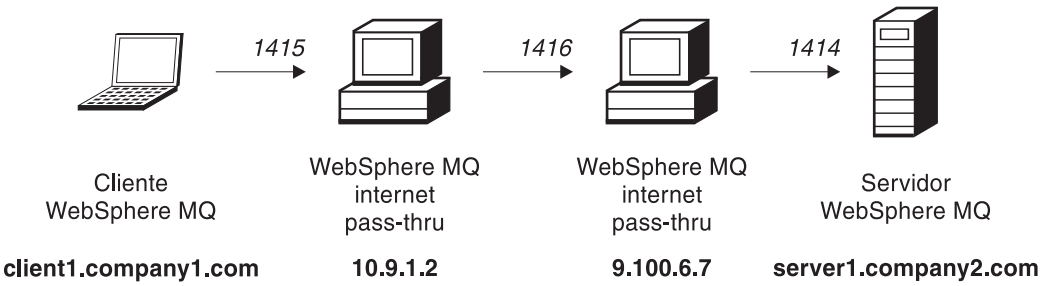

Figura 12. Diagrama de red del servidor SSL

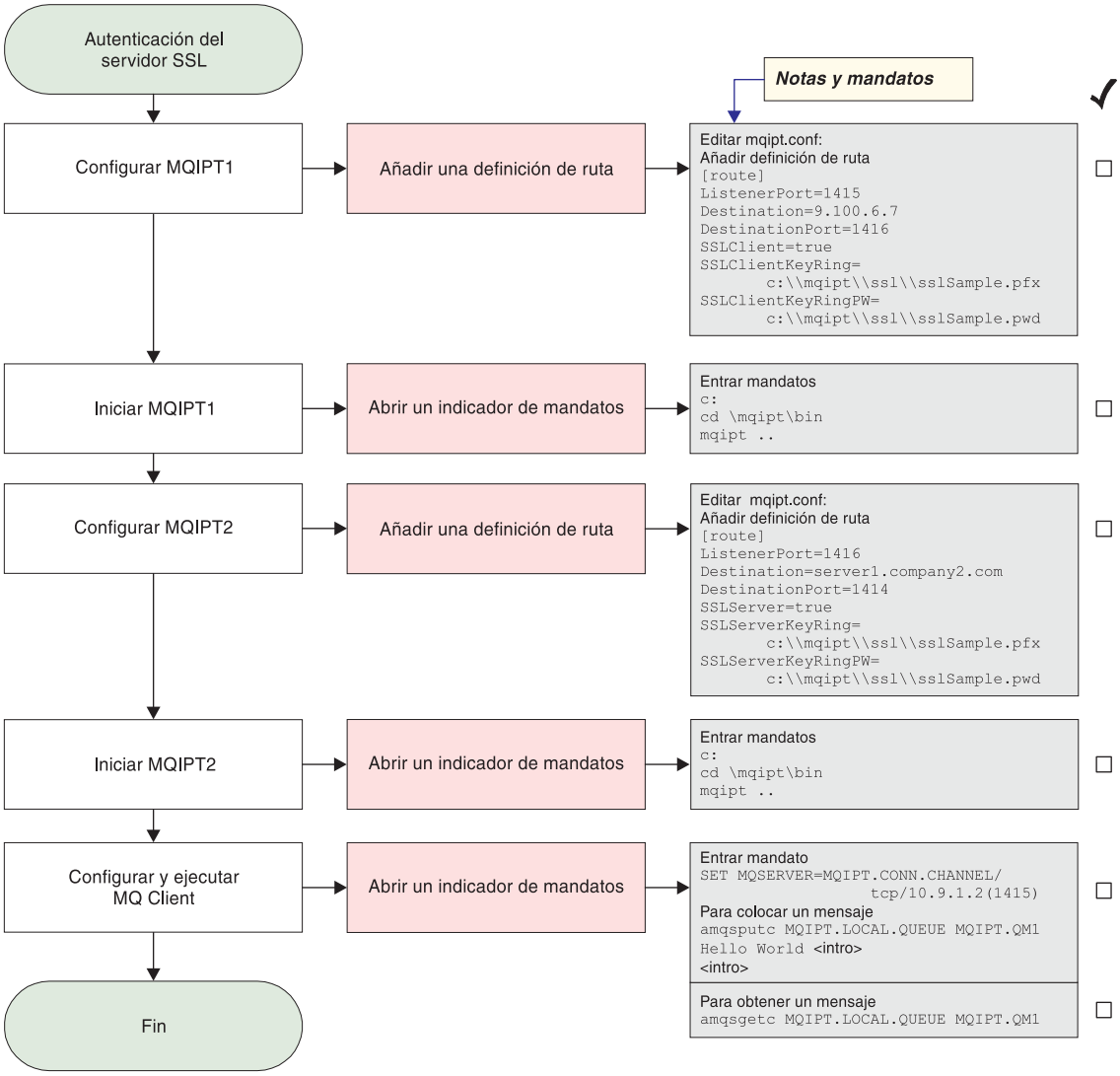

Figura 13. Autenticación del servidor SSL

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, 2003 Reservados todos los derechos
   MQCPI001 Arrancando WebSphere MQ internet pass-thru Versión 1.3.0
   MQCPI011 Se utilizará la vía de acceso c:\mqipt\logs para almacenar
            los archivos de anotaciones
   ```

```
MQCPI006 La ruta 1415 se ha iniciado y reenviará mensajes a:
MQCPI034 ....9.100.6.7(1416)
MQCPI035 ....utilizando protocolos de MQ
MQCPI036 ....parte del Cliente SSL habilitada con las propiedades:
MQCPI031 ......grupos de cifrado <null>
MQCPI032 ......archivo de conjunto de claves c:\mqipt\sslSample.pfx
MQCPI047 ......archivo de conjunto de claves de CA <null>
MQCPI038 ......nombres distinguidos CN=* O=* OU=* L=* ST=* C=*
MQCPI078 La ruta 1415 está preparada para las solicitudes de conexión
```

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, 2003 Reservados todos los derechos
   MQCPI001 Arrancando WebSphere MQ internet pass-thru Versión 1.3.0
   MQCPI011 Se utilizará la vía de acceso c:\mqipt\logs para almacenar
            los archivos de anotaciones
   MQCPI006 La ruta 1416 se ha iniciado y reenviará mensajes a:
   MQCPI034 ....server1.company2.com(1414)
   MQCPI035 ....utilizando protocolos de MQ
   MQCPI037 ....parte del Servidor SSL habilitada con las propiedades:
   MQCPI031 ......grupos de cifrado <null>
   MQCPI032 ......archivo de conjunto de claves c:\mqipt\sslSample.pfx
   MQCPI047 ......archivo de conjunto de claves de CA <null>
   MQCPI038 ......nombres distinguidos CN=* O=* OU=* L=* ST=* C=*
   MQCPI033 ......autenticación de cliente establecida en falso
   MQCPI078 La ruta 1416 está preparada para las solicitudes de conexión
   ```

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 96.)

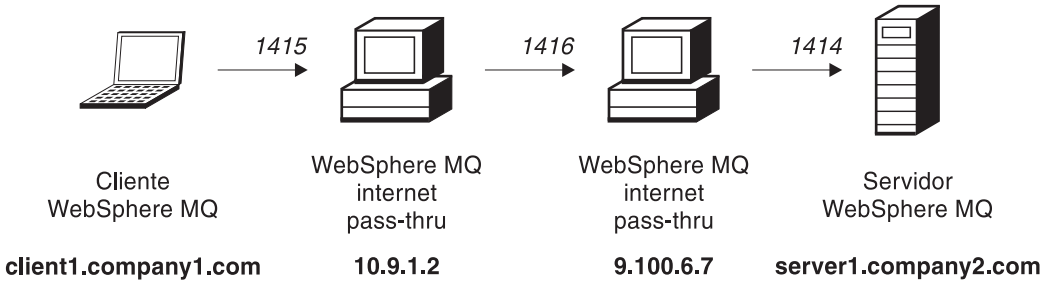

Figura 14. Diagrama de red del cliente SSL

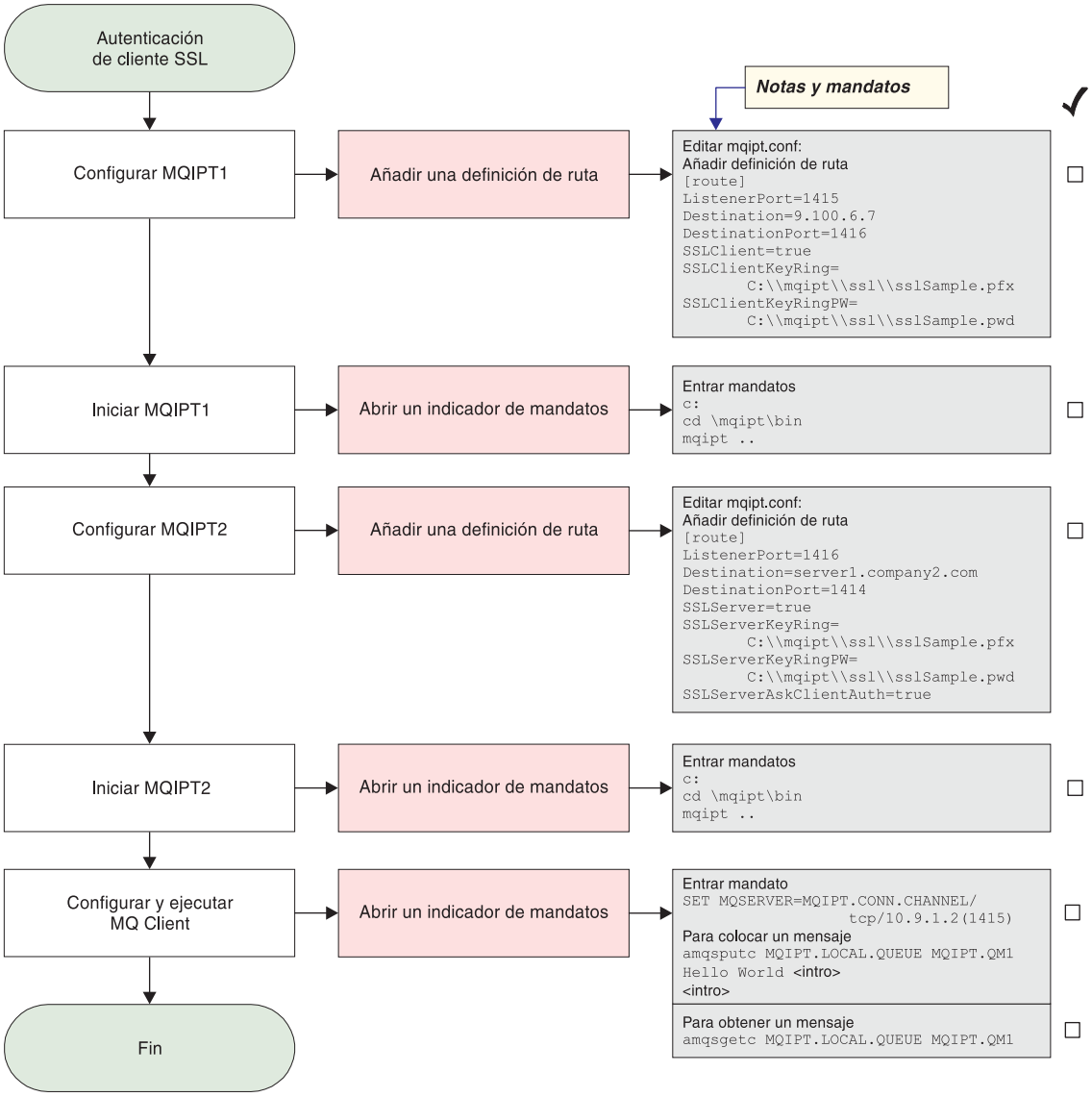

Figura 15. Autenticación del cliente SSL

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, 2003 Reservados todos los derechos
   MQCPI001 Arrancando WebSphere MQ internet pass-thru Versión 1.3.0
   MQCPI011 Se utilizará la vía de acceso c:\mqipt\logs para almacenar
            los archivos de anotaciones
   MQCPI006 La ruta 1415 se ha iniciado y reenviará mensajes a:
   MQCPI034 ....9.100.6.7(1416)
   MQCPI035 ....utilizando protocolos de MQ
   MQCPI036 ....parte del Cliente SSL habilitada con las propiedades:
   MQCPI031 ......grupos de cifrado <null>
   MQCPI032 ......archivo de conjunto de claves c:\mqipt\sslSample.pfx
   MQCPI047 ......archivo de conjunto de claves de CA <null>
   MQCPI038 ......nombres distinguidos CN=* O=* OU=* L=* ST=* C=*
   MQCPI078 La ruta 1415 está preparada para las solicitudes de conexión
   ```

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, 2003 Reservados todos los derechos
   MQCPI001 Arrancando WebSphere MQ internet pass-thru Versión 1.3.0
   MQCPI011 Se utilizará la vía de acceso c:\mqipt\logs para almacenar
            los archivos de anotaciones
   MQCPI006 La ruta 1416 se ha iniciado y reenviará mensajes a:
   MQCPI034 ....server1.company2.com(1414)
   MQCPI035 ....utilizando protocolos de MQ
   MQCPI037 ....parte del Servidor SSL habilitada con las propiedades:
   MQCPI031 ......grupos de cifrado <null>
   MQCPI032 ......archivo de conjunto de claves c:\mqipt\sslSample.pfx
   MQCPI047 ......archivo de conjunto de claves de CA <null>
   MQCPI038 ......nombres distinguidos CN=* O=* OU=* L=* ST=* C=*
   MQCPI033 ......autenticación de cliente establecida en falso
   MQCPI078 La ruta 1416 está preparada para las solicitudes de conexión
   ```

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:

- `ProxyPersistence` 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.

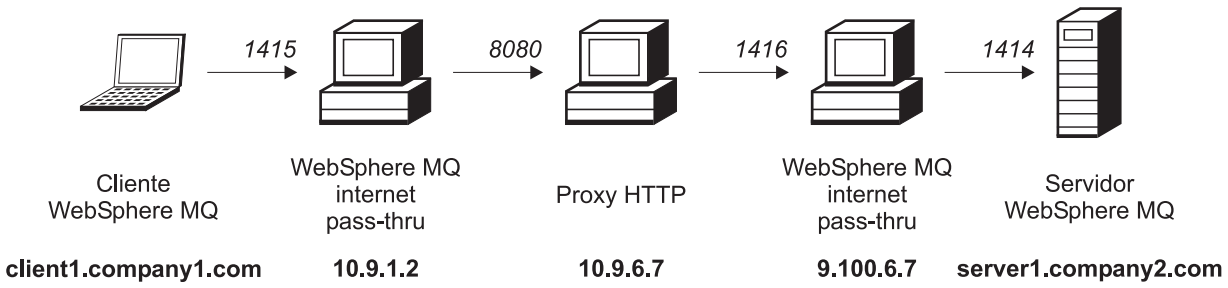

Figura 16. Diagrama de red del proxy HTTP

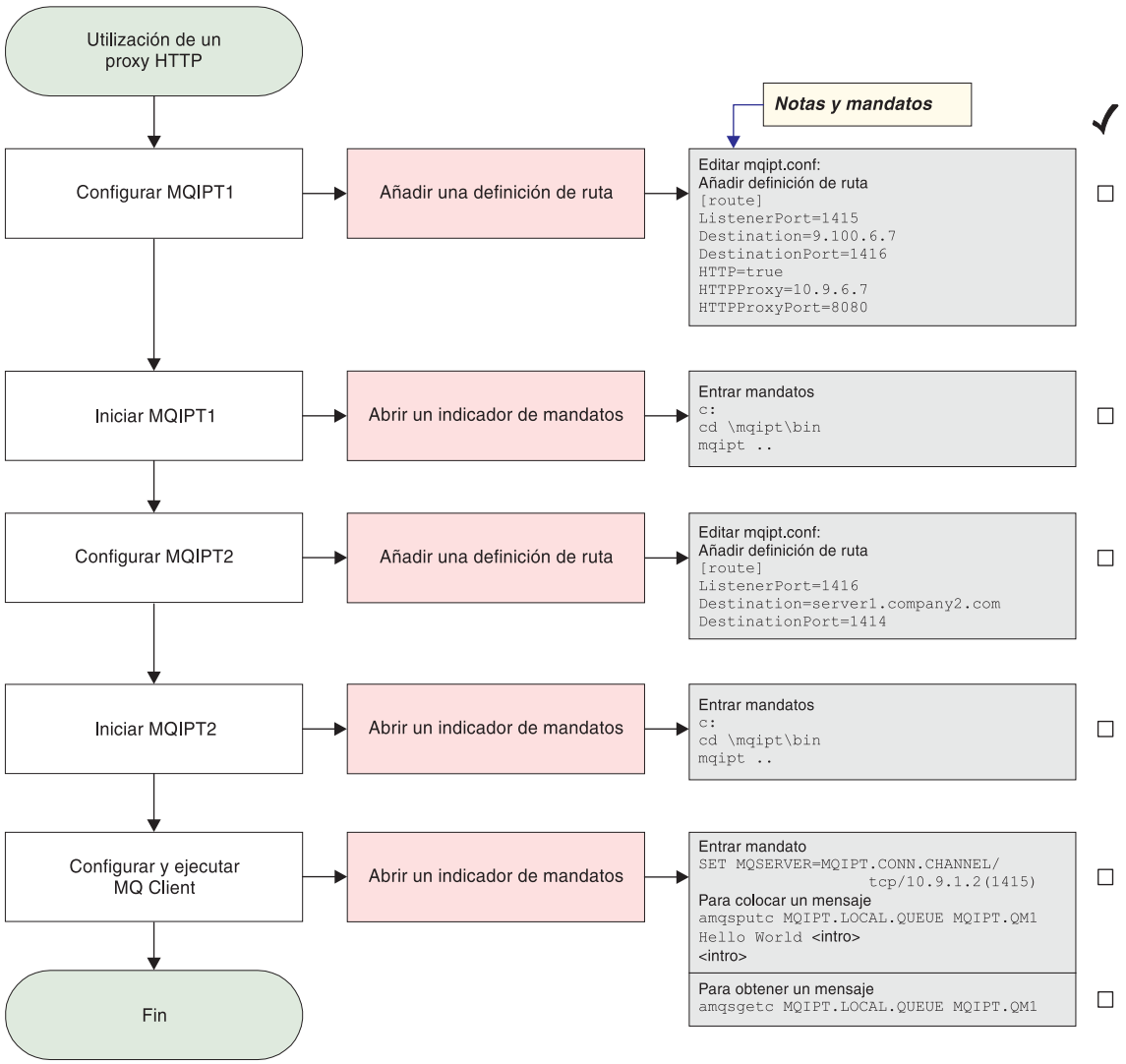

Figura 17. Configuración del proxy HTTP

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, 2003 Reservados todos los derechos
   MQCPI001 Arrancando WebSphere MQ internet pass-thru Versión 1.3.0
   MQCPI004 Leyendo información de configuración de C:\mqipt\mqipt.conf
   MQCPI011 Se utilizará la vía de acceso C:\mqipt\logs para almacenar
   ```

```
         los archivos de anotaciones
MQCPI006 La ruta 1415 se ha iniciado y reenviará mensajes a:
MQCPI034 ....9.100.6.7(1416)
MQCPI035 ....utilizando HTTP
MQCPI024 ....y el proxy HTTP en 10.9.6.7(1080)
MQCPI078 La ruta 1415 está preparada para las solicitudes de conexión
```

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, 2003 Reservados todos los derechos
   MQCPI001 Arrancando WebSphere MQ internet pass-thru Versión 1.3.0
   MQCPI004 Leyendo información de configuración de C:\mqipt\mqipt.conf
   MQCPI011 Se utilizará la vía de acceso C:\mqipt\logs para almacenar
            los archivos de anotaciones
   MQCPI006 La ruta 1416 se ha iniciado y reenviará mensajes a:
   MQCPI034 ....server1.company2.com(1414)
   MQCPI035 ....utilizando protocolos de MQ
   MQCPI078 La ruta 1416 está preparada para las solicitudes de conexión
   ```

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.

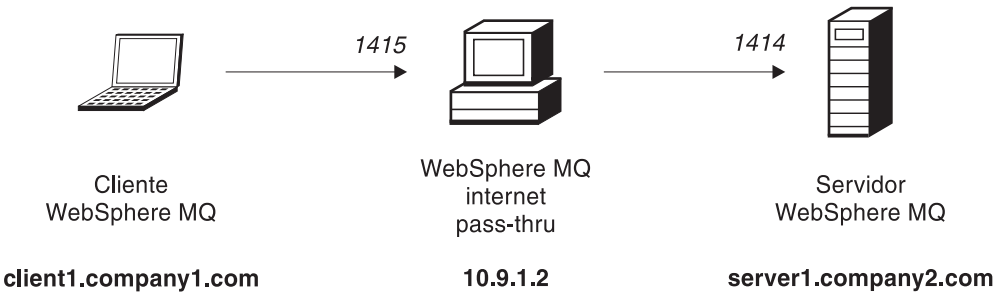

Figura 18. Diagrama de red del control de acceso

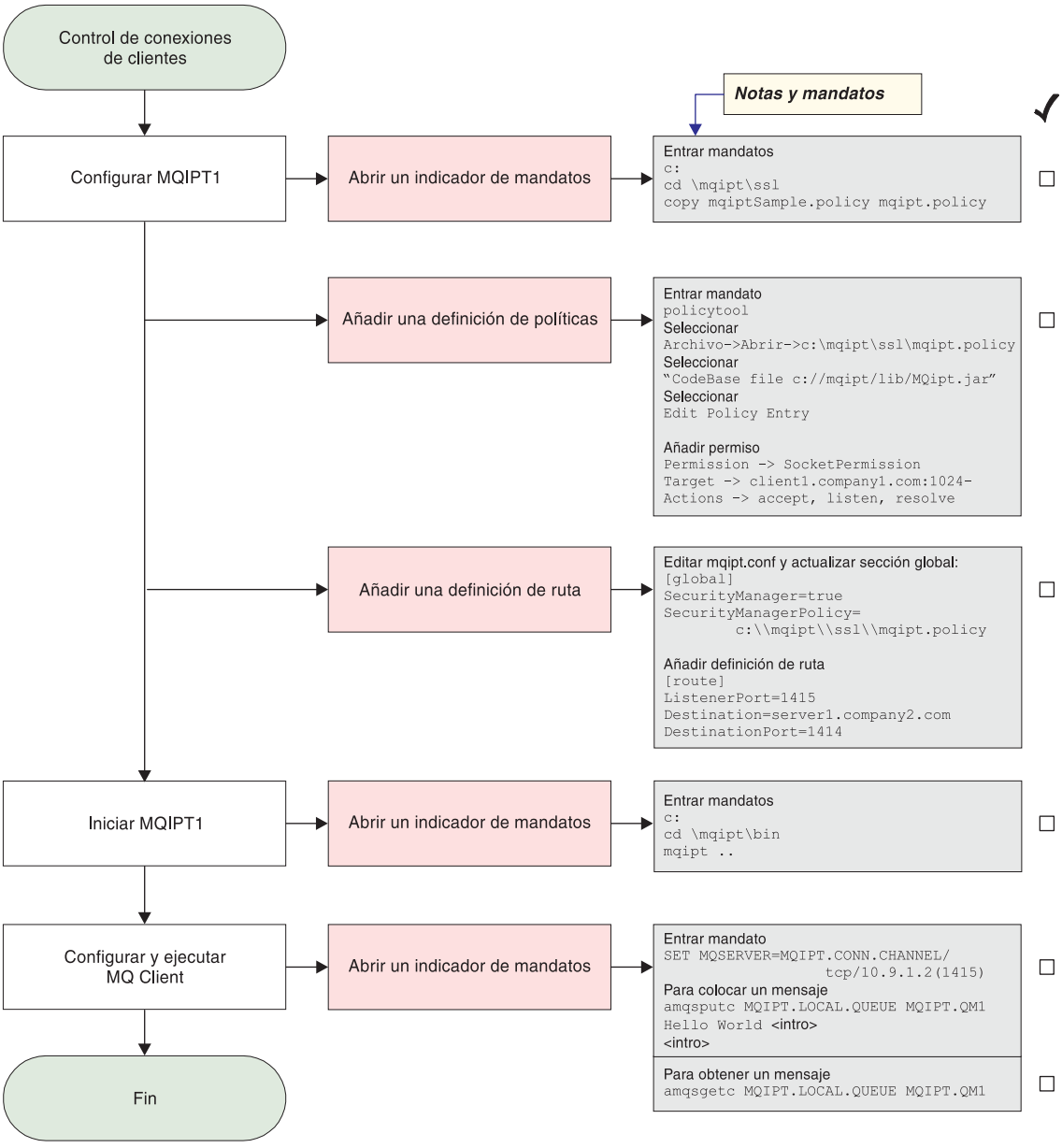

Figura 19. Configuración del control de acceso

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-
         Actions=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, 2003 Reservados todos los derechos
   MQCPI001 Arrancando WebSphere MQ internet pass-thru Versión 1.3.0
   MQCPI004 Leyendo información de configuración de C:\mqipt\mqipt.conf
   MQCPI055 Estableciendo java.security.policy en c:\mqipt\mqipt.policy
   MQCPI053 Iniciando Java Security Manager
   MQCPI011 Se utilizará la vía de acceso C:\mqipt\logs para almacenar
            los archivos de anotaciones
   MQCPI006 La ruta 1415 se ha iniciado y reenviará mensajes a:
   MQCPI034 ....server1.company2.com(1414)
   MQCPI035 ....utilizando protocolos de MQ
   MQCPI078 La ruta 1415 está preparada para las solicitudes de conexión
   ```

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)

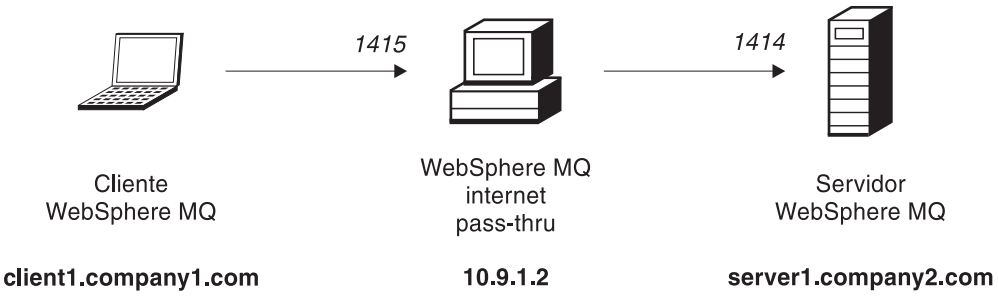

Figura 20. Diagrama de red de QoS

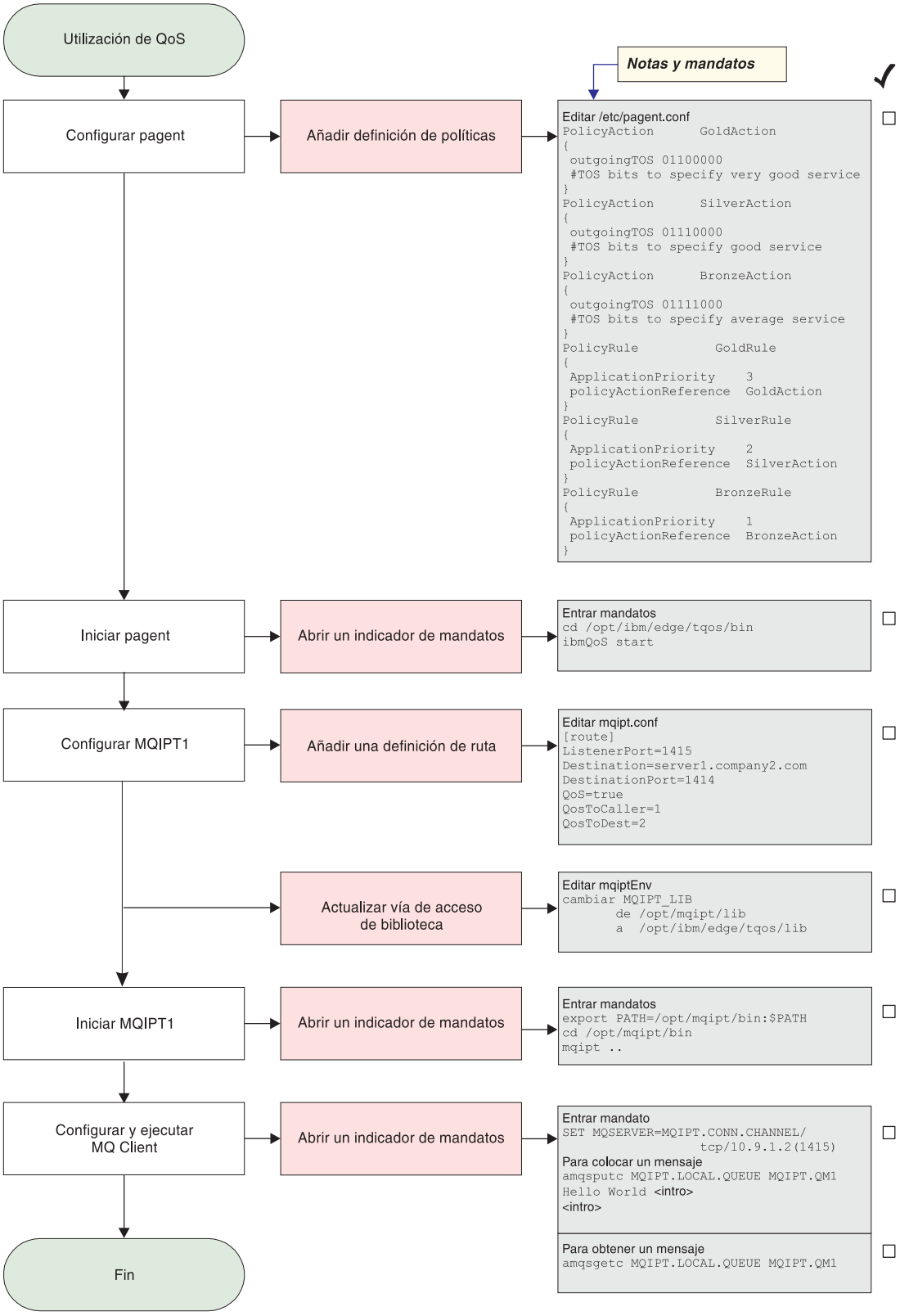

Figura 21. Configuración de QoS

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
}
```

   Para activar la recopilación de datos del rendimiento de las normas definidas más arriba, utilice la sentencia PolicyPerformanceCollection y habilítela. Consulte el archivo Pagent.conf para obtener una descripción y el formato de esta sentencia.

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, 2003 Reservados todos los derechos
MQCPI001 Arrancando WebSphere MQ internet pass-thru Versión 1.3.0
MQCPI004 Leyendo información de configuración de /opt/mqipt/mqipt.conf
MQCPI011 Se utilizará la vía de acceso /opt/mqipt/logs para almacenar
         los archivos de anotaciones
MQCPI006 La ruta 1415 se ha iniciado y reenviará mensajes a:
MQCPI034 ....server1.company2.com(1414)
MQCPI035 ....utilizando protocolos de MQ
MQCPI049 ....prioridad de QoS (Calidad de servicio) en dest = 2, en
         canal de llamada = 1
MQCPI078 La ruta 1415 está preparada para las solicitudes de conexión
```

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.

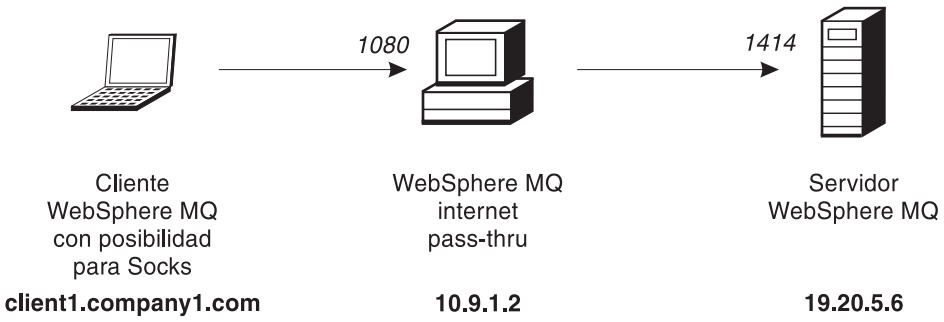

Figura 22. Diagrama de red del proxy SOCKS

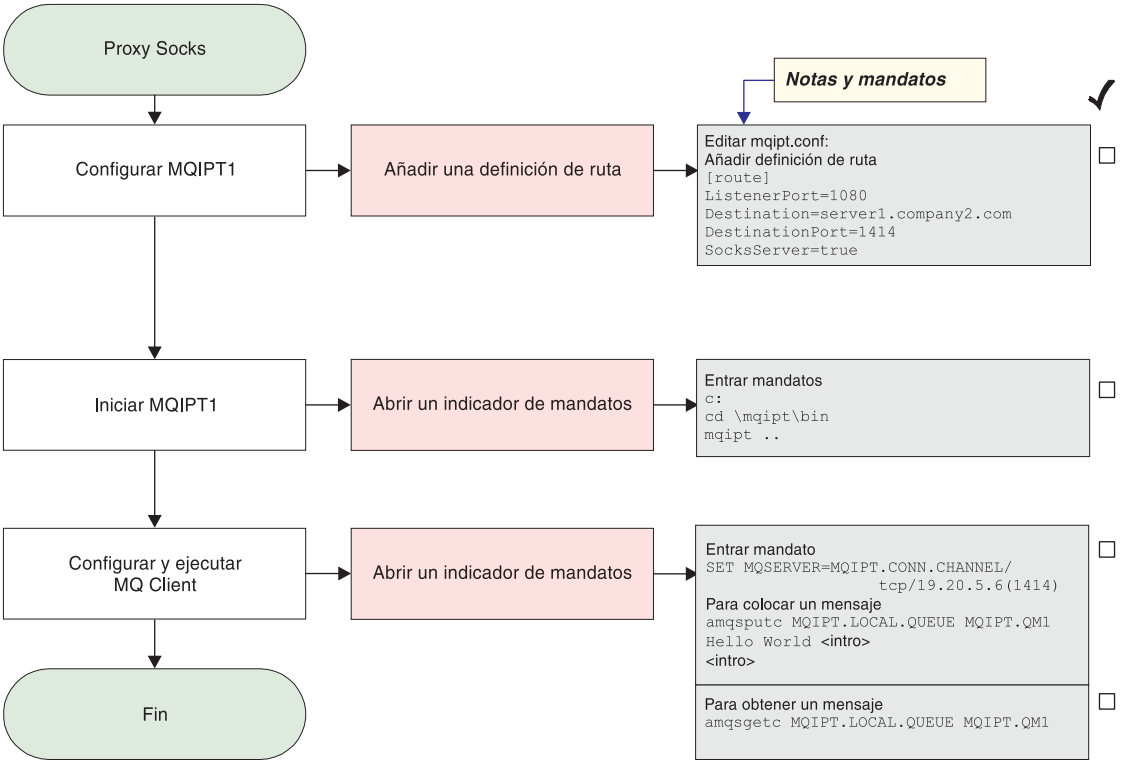

Figura 23. Configuración del proxy SOCKS

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, 2003 Reservados todos los derechos
MQCPI001 Arrancando WebSphere MQ internet pass-thru Versión 1.3.0
MQCPI004 Leyendo información de configuración de C:\mqipt\mqipt.conf
MQCPI011 Se utilizará la vía de acceso C:\mqipt\logs para almacenar
         los archivos de anotaciones
MQCPI006 La ruta 1080 se ha iniciado y reenviará mensajes a:
MQCPI034 ....server1.company2.com(1414)
MQCPI035 ....utilizando protocolos de MQ
MQCPI052 ....parte del servidor Socks habilitada
MQCPI078 La ruta 1080 está preparada para las solicitudes de conexión
```

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 111, excepto que es MQIPT el que realiza una conexión habilitada para SOCKS, en lugar del cliente de WebSphere MQ.

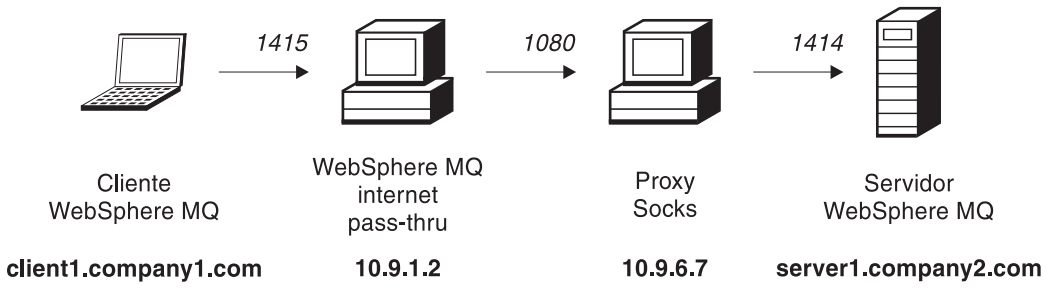

Figura 24. Diagrama de red del cliente SOCKS

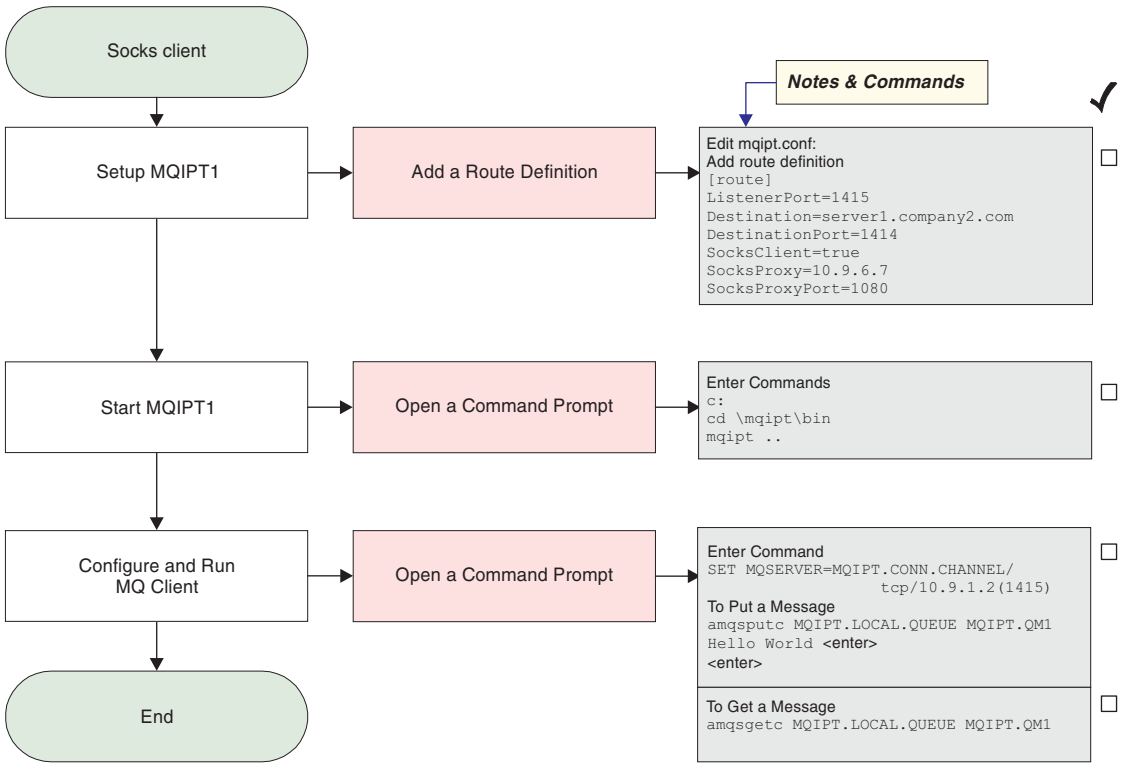

Figura 25. Configuración del cliente SOCKS

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, 2003 Reservados todos los derechos
   MQCPI001 Arrancando WebSphere MQ internet pass-thru Versión 1.3.0
   MQCPI004 Leyendo información de configuración de C:\mqipt\mqipt.conf
   MQCPI022 Se ha inhabilitado la comprobación de contraseña en la puerta de
            mandatos
   MQCPI011 Se utilizará la vía de acceso C:\mqipt\logs para almacenar los archivos
            de anotaciones
   MQCPI006 La ruta 1415 se ha iniciado y reenviará mensajes a:
   MQCPI034 ....server1.company2.com(1414)
   MQCPI035 ....utilizando protocolos de MQ
   MQCPI039 ....y el proxy Socks en 10.9.6.7(1080)
   MQCPI078 La ruta 1415 está preparada para las solicitudes de conexión
   ```

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″.

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 98.

Configuración del servlet MQIPT

Además de en el apartado “Supuestos” en la página 95, en este ejemplo también se presupone lo siguiente:

- El servidor de aplicaciones Tomcat se ha instalado en el directorio siguiente:

  `c:\jakarta-tomcat-4.0.1`

  Puede bajar Tomcat en la dirección web siguiente:

  `http://jakarta.apache.org/builds/jakarta-tomcat-4.0/release/v4.0.3/`
- IBM Web Traffic Express se ha instalado en:

  `c:\wte`

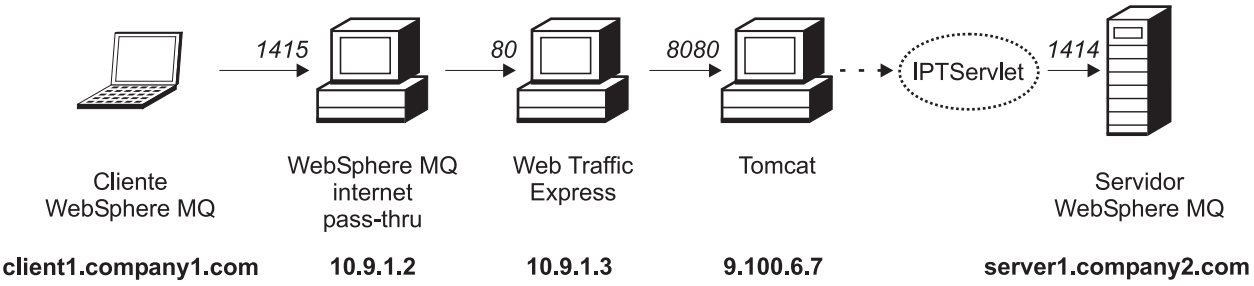

Figura 26. Diagrama de red del servlet

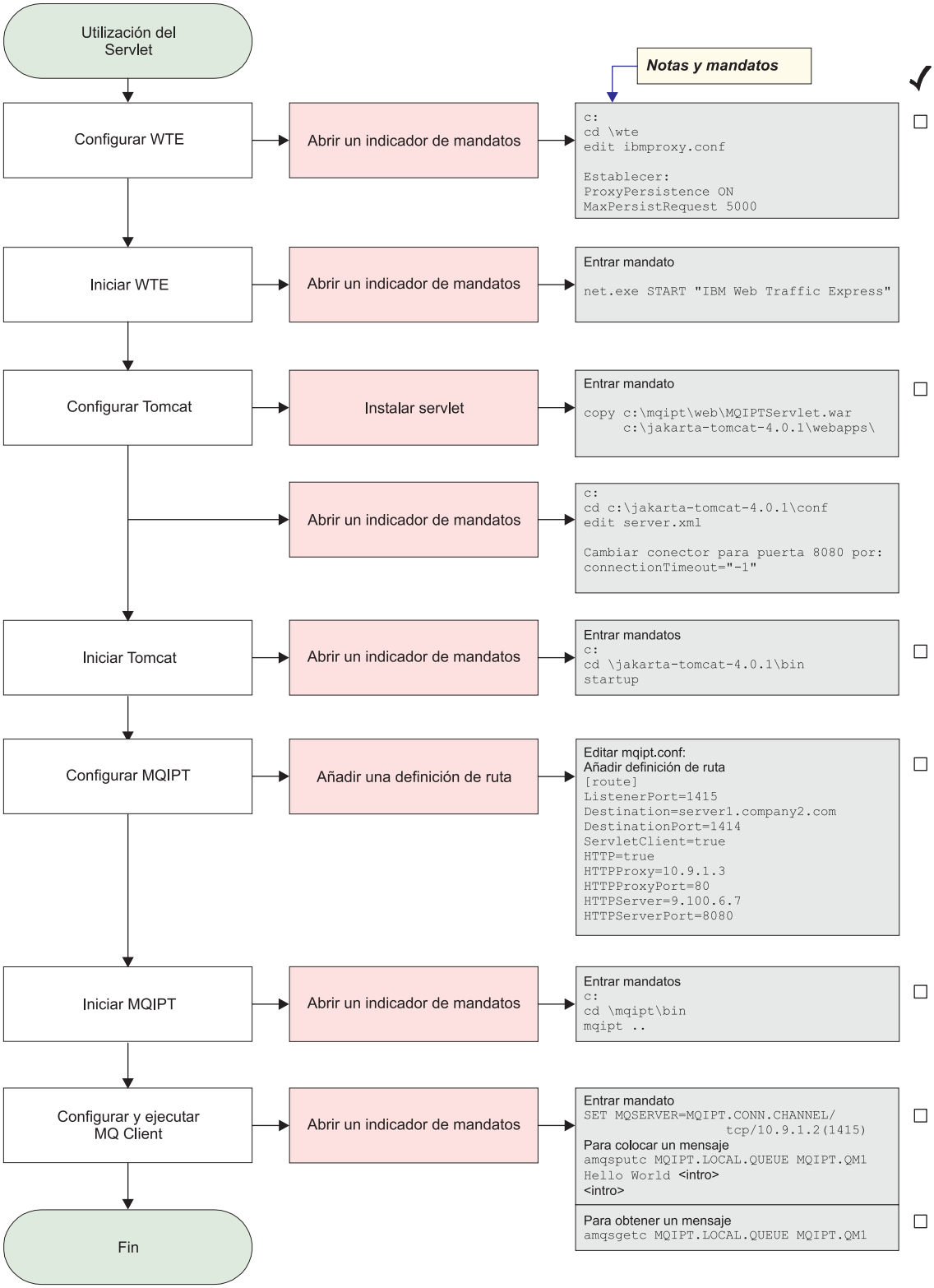

Figura 27. Configuración del servlet

1. Configure Web Traffic Express
   edite `c:\wte\ibmroxy.conf` y establezca las propiedades siguientes:

   ```
   ProxyPersistence ON
   MaxPersistRequest  5000
   ```

2. Inicie Web Traffic Express

   Abra un indicador de mandatos y escriba lo siguiente:

   ```
   net.exe Start "IBM Web Traffic Express"
   ```

3. Configure Tomcat.

   Para instalar el servlet, copie:

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

   en:

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

   Edite `c:\jakarta-tomcat-4.0.1\conf\server.xml`, habilite el conector para la puerta 8443 y establezca la propiedad `ConnectionTimeout` en `-1`.

4. Inicie Tomcat

   Abra un indicador de mandatos y escriba lo siguiente:

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

5. 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=10.9.1.3
   HTTPProxyPort=80
   HTTPServer=9.100.6.7
   HTTPServerPort=8080
   ```

6. 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, 2003 Reservados todos los derechos
   MQCPI001 Arrancando WebSphere MQ internet pass-thru Versión 1.3.0
   MQCPI004 Leyendo información de configuración de C:\mqipt\mqipt.conf
   MQCPI011 Se utilizará la vía de acceso C:\mqipt\logs para almacenar
            los archivos de anotaciones
   MQCPI006 La ruta 1415 se ha iniciado y reenviará mensajes a:
   MQCPI034 ....server1.company2.com(1414)
   MQCPI035 ....utilizando HTTP
   MQCPI024 ....y el proxy HTTP en 10.9.1.3(80)
   MQCPI066 ....y el servidor HTTP en 9.100.6.7(8080)
   MQCPI059 ....cliente del servlet habilitado
   MQCPI078 La ruta 1415 está preparada para las solicitudes de conexión
   ```

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″.

Configuración de HTTPS

Además de en el apartado “Supuestos” en la página 95, en este ejemplo también se presupone lo siguiente:

- El servidor de aplicaciones Tomcat se ha instalado en el directorio siguiente:
  `c:\jakarta-tomcat-4.0.1`

  Puede bajar Tomcat en la dirección web siguiente:
  `http://jakarta.apache.org/builds/jakarta-tomcat-4.0/release/v4.0.3/`
- IBM Web Traffic Express se ha instalado en:
  `c:\wte`

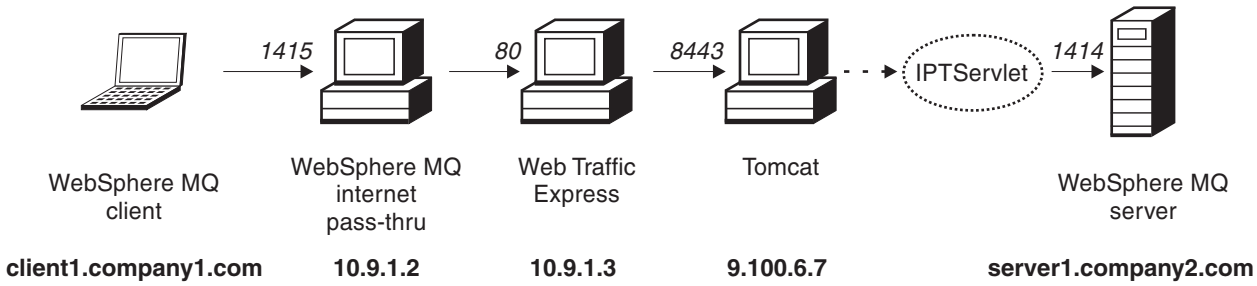

Figura 28. Diagrama de red de HTTPS

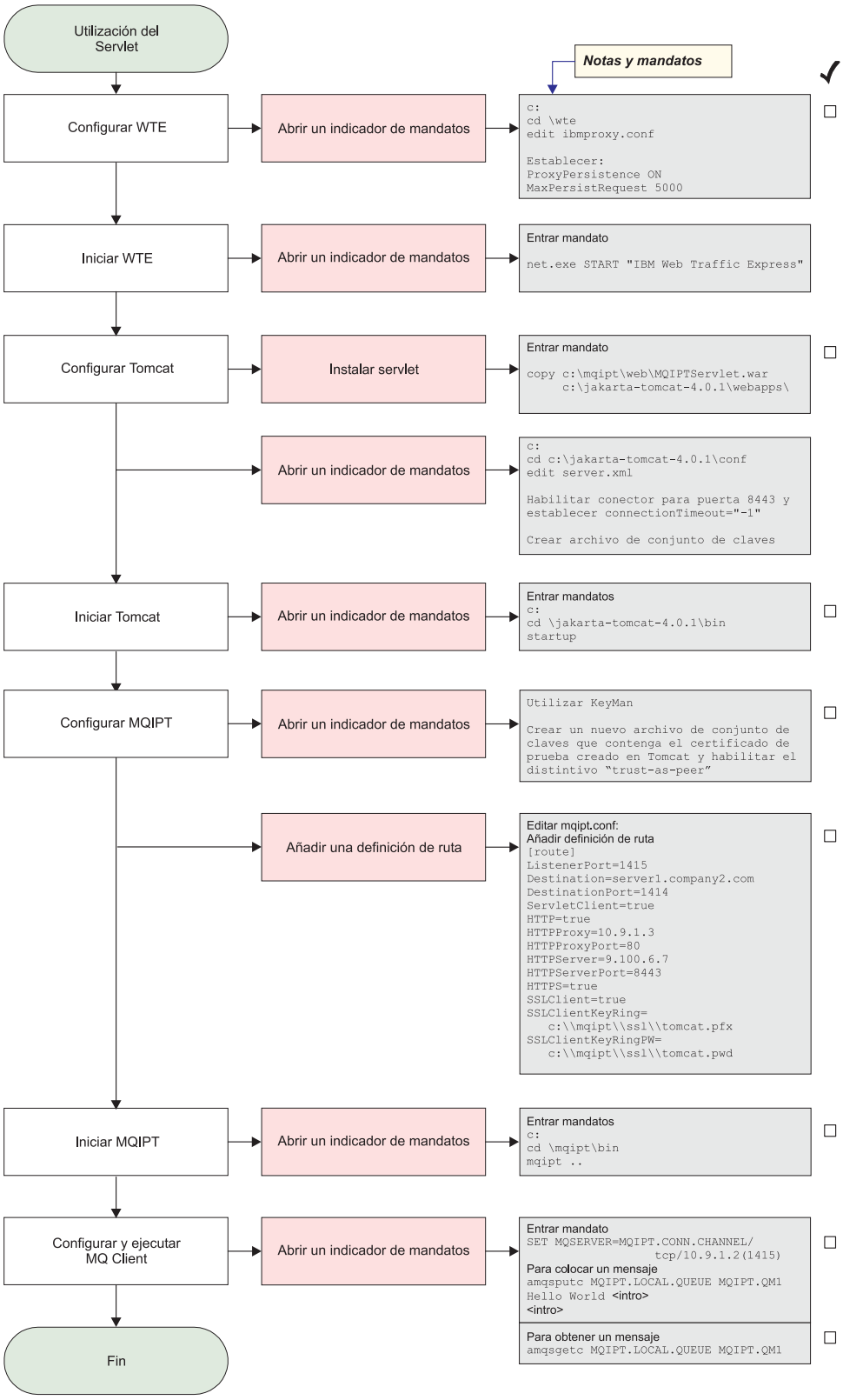

Figura 29. Configuración de HTTPS

1. Configure Web Traffic Express

   Edite `c:\wte\ibmroxy.conf` y establezca las propiedades siguientes:

   ```
   ProxyPersistence ON
   MaxPersistRequest  5000
   ```

2. Inicie Web Traffic Express

   Abra un indicador de mandatos y escriba lo siguiente:

   ```
   net.exe Start "IBM Web Traffic Express"
   ```

3. Configure Tomcat.

   Para instalar el servlet, copie:

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

   en:

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

   Edite `c:\jakarta-tomcat-4.0.1\conf\server.xml`, habilite el conector para la puerta 8443 y establezca la propiedad `ConnectionTimeout` en `-1`.

   Utilice la documentación de Tomcat, disponible en la dirección web:

   ```
   http://jakarta.apache.org/tomcat/tomcat-4.0-doc/index.html
   ```

   y siga las instrucciones de la sección ″SSL Configuration HOW-TO″ para habilitar las conexiones SSL en la puerta 8443. Cree archivo de conjunto de claves que contenga un certificado autofirmado de prueba que creará un archivo denominado `C:\winnt\profiles\<ID_usuario>\.keystore`.

4. Inicie Tomcat

   Abra un indicador de mandatos y escriba lo siguiente:

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

5. Copie el nuevo archivo de almacén de claves de la máquina Tomcat a la máquina MQIPT. Utilice KeyMan, abra el nuevo archivo de almacén de claves (la contraseña por omisión es `changeit`) y active el distintivo ″trust-as-peer″ (consulte el apartado “Creación de certificados de prueba SSL” en la página 115 para obtener más información). Guarde este archivo como `c:\mqipt\ssl\tomcat.pfx` y cree un archivo de texto denominado `c:\mqipt\ssl\tomcat.pwd` que contenga la contraseña `changeit`.

6. 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=10.9.1.3
   HTTPProxyPort=80
   HTTPServer=9.100.6.7
   HTTPServerPort=8443
   HTTPS=true
   SSLClient=true
   SSLClientKeyRing=c:\\mqipt\\ssl\\tomcat.pfx
   SSLClientKeyRingPW=c:\\mqipt\\ssl\\tomcat.pwd
   ```

7. 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, 2003 Reservados todos los derechos
MQCPI001 Arrancando WebSphere MQ internet pass-thru Versión 1.3.0
MQCPI004 Leyendo información de configuración de C:\mqipt\mqipt.conf
MQCPI011 Se utilizará la vía de acceso C:\mqipt\logs para almacenar
         los archivos de anotaciones
MQCPI006 La ruta 1415 se ha iniciado y reenviará mensajes a:
MQCPI034 ....server1.company2.com(1414)
MQCPI035 ....utilizando HTTP
MQCPI024 ....y el proxy HTTP en 10.9.1.3(80)
MQCPI066 ....y el servidor HTTP en 9.100.6.7(8080)
MQCPI059 ....cliente del servlet habilitado
MQCPI036 ....parte del Cliente SSL habilitada con las propiedades:
MQCPI031 ......grupos de cifrado <null>
MQCPI032 ......archivo de conjunto de claves c:\mqipt\ssl\tomcat.pfx
MQCPI047 ......archivo de conjunto de claves de CA <null>
MQCPI038 ......nombres distinguidos CN=* O=* OU=* L=* ST=* C=*
MQCPI078 La ruta 1415 está preparada para las solicitudes de conexión
```

8. 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)
   ```

9. Coloque un mensaje mediante el mandato siguiente:

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

10. 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 95, 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.

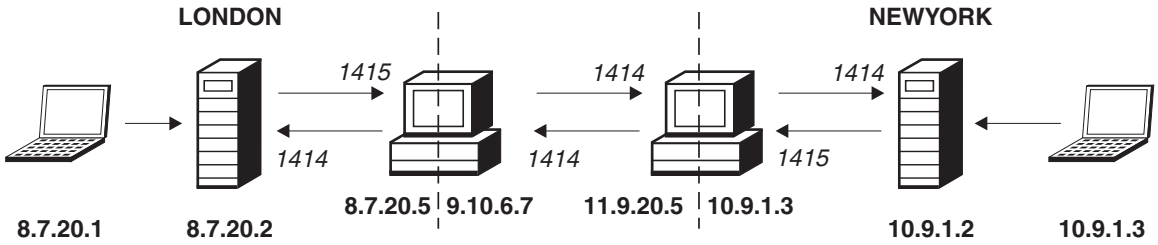

Figura 30. Diagrama de red de la agrupación en clúster

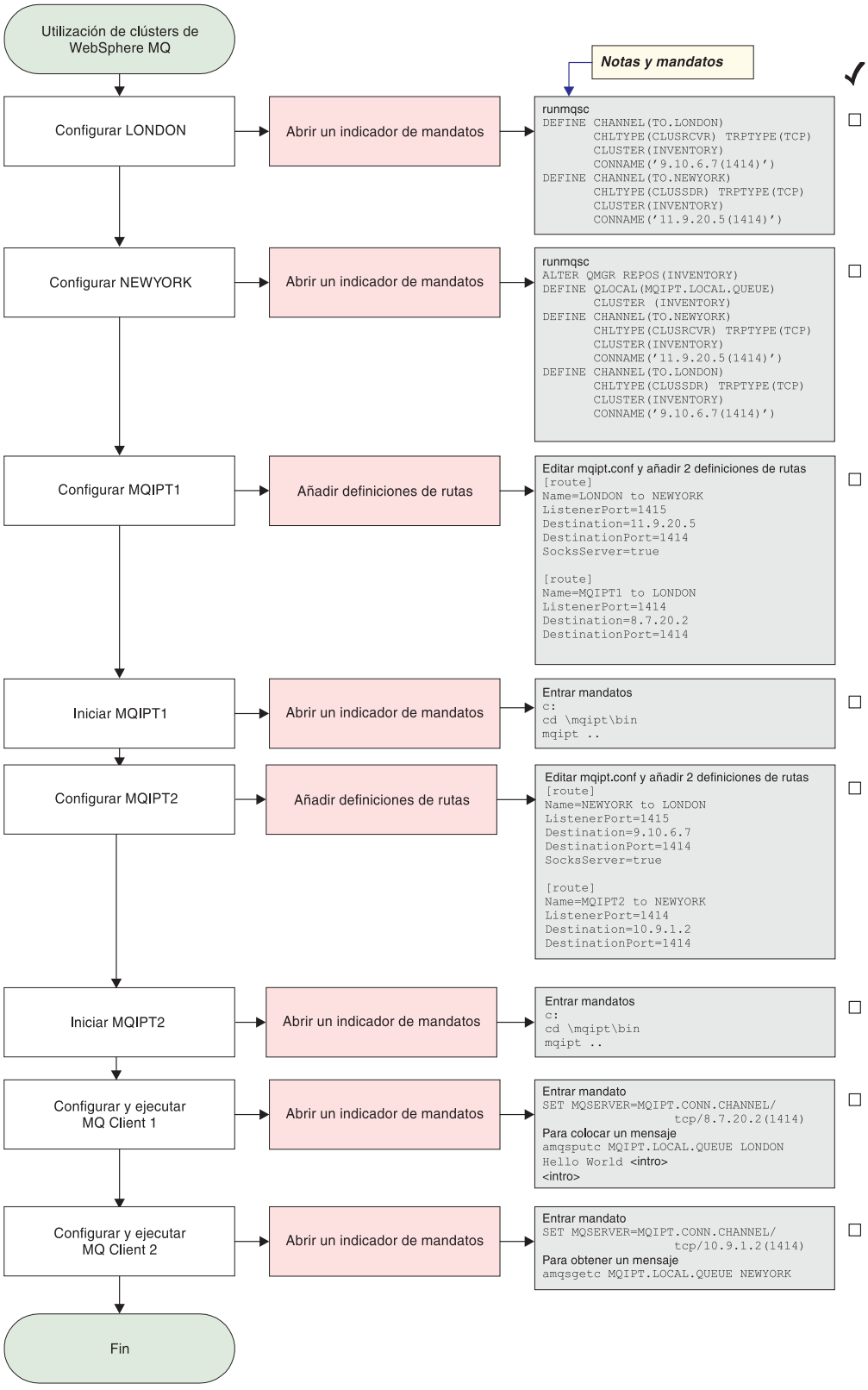

Figura 31. Configuración de la agrupación en clúster

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, 2003 Reservados todos los derechos
   MQCPI001 Arrancando WebSphere MQ internet pass-thru Versión 1.3.0
   MQCPI004 Leyendo información de configuración de C:\mqipt\mqipt.conf
   MQCPI011 Se utilizará la vía de acceso C:\mqipt\logs para almacenar
            los archivos de anotaciones
   MQCPI006 La ruta 1415 se ha iniciado y reenviará mensajes a:
   MQCPI034 ....11.9.20.5(1414)
   MQCPI035 ....utilizando protocolos de MQ
   MQCPI052 ....parte del servidor socks habilitada
   MQCPI078 La ruta 1415 está preparada para las solicitudes de conexión
   MQCPI006 La ruta 1414 se ha iniciado y reenviará mensajes a:
   MQCPI034 ....8.7.20.2(1414)
   MQCPI035 ....utilizando protocolos de MQ
   MQCPI078 La ruta 1414 está preparada para las solicitudes de conexión
   ```

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, 2003 Reservados todos los derechos
   MQCPI001 Arrancando WebSphere MQ internet pass-thru Versión 1.3.0
   MQCPI004 Leyendo información de configuración de C:\mqipt\mqipt.conf
   MQCPI011 Se utilizará la vía de acceso C:\mqipt\logs para almacenar
            los archivos de anotaciones
   MQCPI006 La ruta 1415 se ha iniciado y reenviará mensajes a:
   MQCPI034 ....9.10.6.7(1414)
   MQCPI035 ....utilizando protocolos de MQ
   MQCPI052 ....parte del servidor socks habilitada
   MQCPI078 La ruta 1415 está preparada para las solicitudes de conexión
   MQCPI006 La ruta 1414 se ha iniciado y reenviará mensajes a:
   MQCPI034 ....10.9.1.2(1414)
   MQCPI035 ....utilizando protocolos de MQ
   MQCPI078 La ruta 1414 está preparada para las solicitudes de conexión
   ```

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

En este ejemplo se presupone que ha solicitado un certificado nuevo de una CA fiable 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. Especifique 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 la parte del cliente como en la parte 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 98, 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 100 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
```

Asignación de direcciones de puerta

En este ejemplo se muestra cómo controlar las direcciones de puerta local que se utilizan al crear conexiones de salida. En este ejemplo se presupone que se ha instalado MQIPT en una máquina multitarjeta.

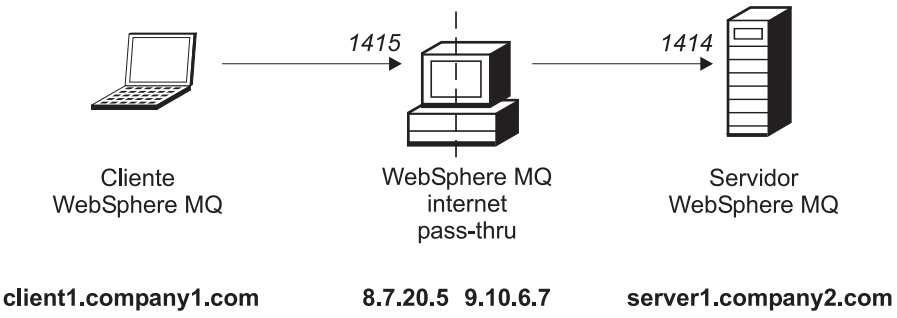

Figura 32. Diagrama de red de la asignación de puertas

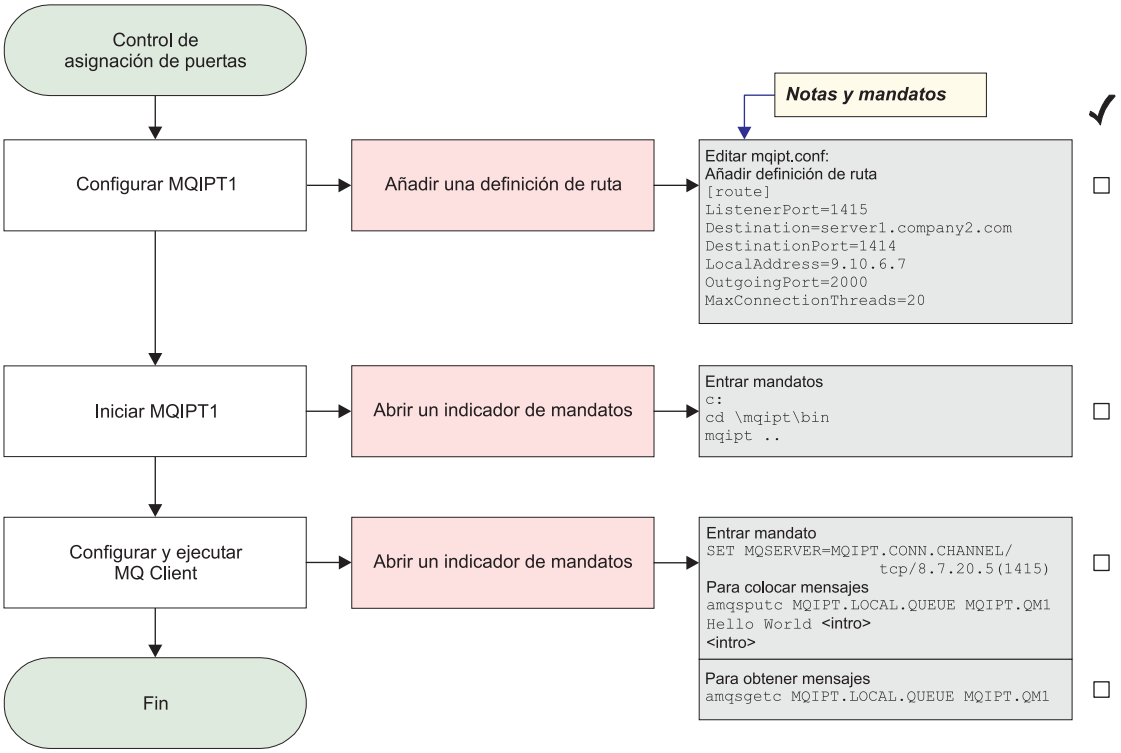

Figura 33. Configuración de asignación de puertas

1. Configure MQIPT1.

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

   ```
   [route]
   ListenerPort=1415
   Destination=server1.company2.com
   DestinationPort=1414
   LocalAddress=9.10.6.7
   OutgoingPort=2000
   MaxConnectionThreads=20
   ```

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, 2003 Reservados todos los derechos
   MQCPI001 Arrancando WebSphere MQ internet pass-thru Versión 1.3.0
   MQCPI004 Leyendo información de configuración de C:\mqipt\mqipt.conf
   MQCPI011 Se utilizará la vía de acceso C:\mqipt\logs para almacenar
            los archivos de anotaciones
   MQCPI006 La ruta 1415 se ha iniciado y reenviará mensajes a:
   MQCPI034 ....server1.company2.com(1414)
   MQCPI035 ....utilizando protocolos de MQ
   MQCPI069 ....enlazando con la dirección local 9.10.6.7
   MQCPI070 ....utilizando el rango de dirección de puerta local 2000-2019
   MQCPI078 La ruta 1415 está preparada para las solicitudes de conexión
   ```

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

   ```
   SET MQSERVER=MQIPT.CONN.CHANNEL/tcp/8.7.20.5(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″.

Utilización de un servidor LDAP

En este ejemplo se muestra cómo configurar MQIPT para que utilice un servidor LDAP para recuperar CRL. En este ejemplo no se pretende explicar cómo instalar y configurar un servidor LDAP o cómo crear un archivo de conjunto de claves que contenga certificados o personales o fiables. En él se presupone que el servidor LDAP está disponible de una autoridad de certificación (CA) conocida y fiable. No se utiliza ningún servidor LDAP de copia de seguridad, pero puede implementarse fácilmente añadiendo las propiedades de ruta adecuadas.

Para este ejemplo, se presupone lo siguiente:

- IPT2 tiene un certificado personal, emitido por la CA fiable, que se almacena en un archivo de conjunto de claves denominado myCert.pfx y la contraseña cifrada utilizada para abrir el archivo de conjunto de claves, que se almacena en el archivo myCert.pwd.
- IPT1 tiene una copia del certificado de la CA fiable que se utilizará para autenticar el certificado enviado por IPT2. Este certificado personal se almacena en un archivo de conjunto de claves denominado caCerts.pfx y la contraseña cifrada utilizada para abrir el archivo de conjunto de claves se almacena en el archivo caCerts.pwd.
- Los archivos de contraseña cifrado se ha creado mediante el script mqiptPW.

Al ejecutarse este ejemplo se permite al cliente de WMQ conectarse al gestor de colas (QM) y colocar un mensaje de WMQ en la cola de destino. Al ejecutar un rastreo de MQIPT en IPT1 se mostrará el servidor LDAP que se está utilizando pero, para demostrar cómo funcionan las CRL, la CA fiable deberá revocar el certificado personal utilizado por IPT2. A continuación, si éste es el caso, no se permitirá al cliente de WMQ conectarse al QM, ya que se rechazará la conexión de IPT1 a IPT2.

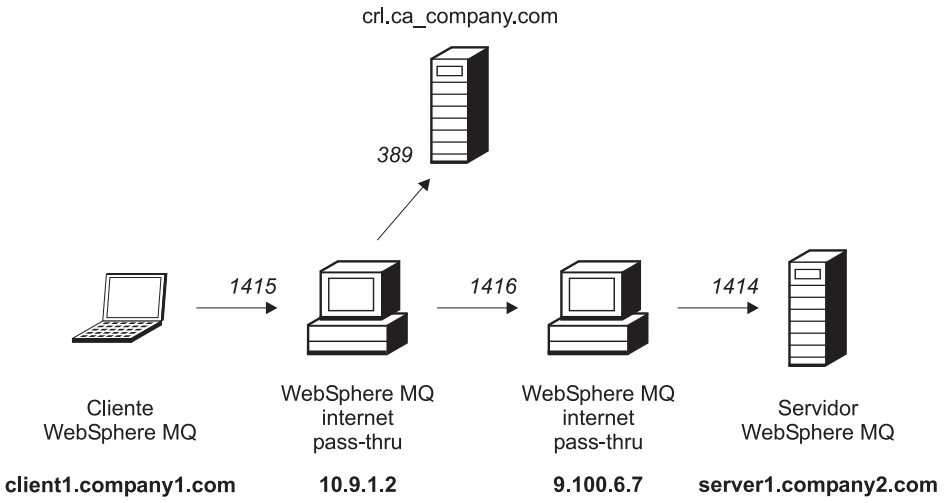

Figura 34. Diagrama de red del servidor LDAP

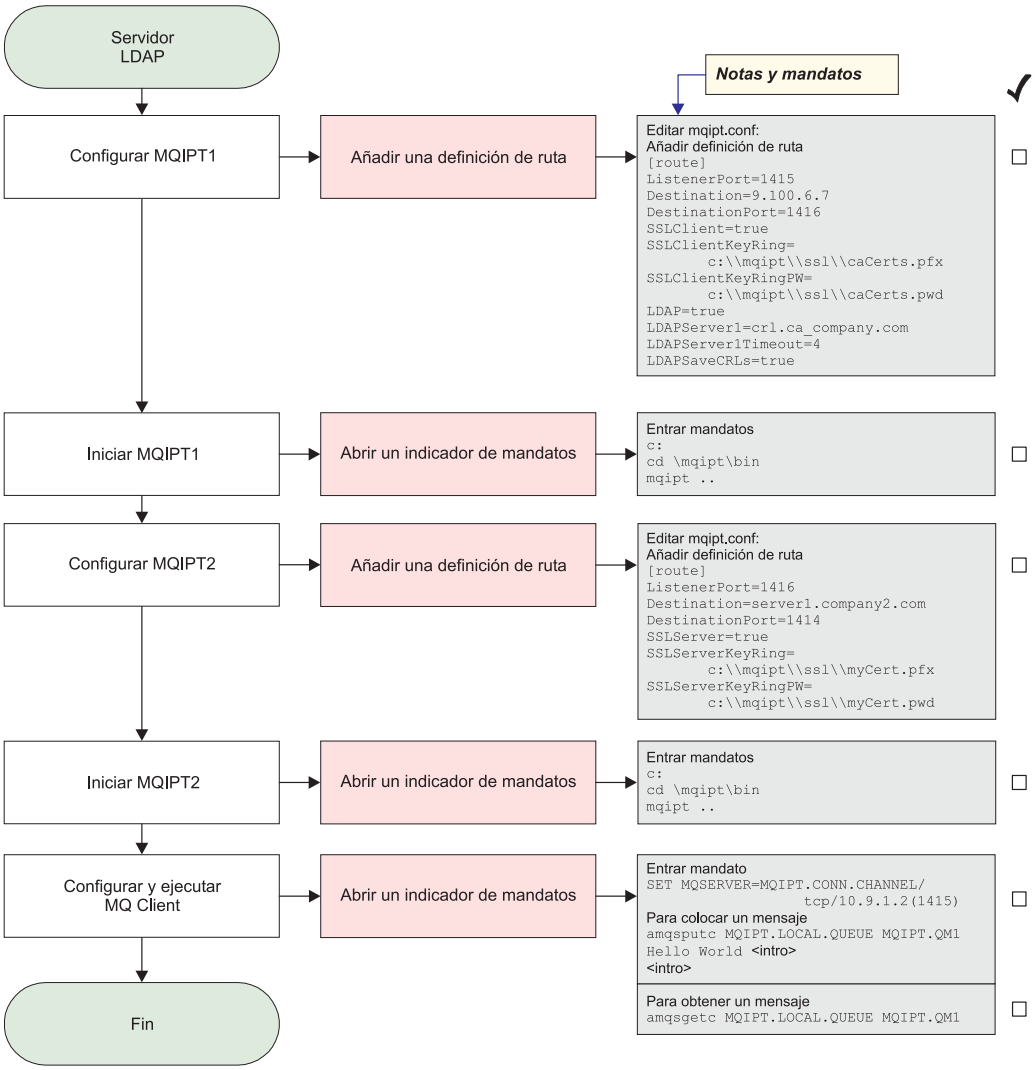

Figura 35. Configuración de LDAP

1. En IPT1

   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\\ssl\\caCerts.pfx
SSLClientKeyRingPW=c:\\mqipt\\ssl\\caCerts.pwd
LDAP=true
LDAPServer1=crl.ca_company.com
LDAPServer1Timeout=4
LDAPSaveCRLs=true
```

   Abra un indicador de mandatos:

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

   El mensaje siguiente indica que se ha realizado correctamente:

```
5639-L92 (C) Copyright IBM Corp. 2000, 2003 Reservados todos los derechos
MQCPI001 Arrancando WebSphere MQ internet pass-thru Versión 1.3.0
MQCPI004 Leyendo información de configuración de C:\mqipt\mqipt.conf
MQCPI011 Se utilizará la vía de acceso C:\mqipt\logs para almacenar los
         archivos de anotaciones
MQCPI006 La ruta 1415 se ha iniciado y reenviará mensajes a:
MQCPI034 ....9.100.6.7(1416)
MQCPI035 ....utilizando protocolos de MQ
MQCPI036 ....parte del Cliente SSL habilitada con las propiedades:
MQCPI031 ......grupos de cifrado <NULL>
MQCPI032 ......archivo de conjunto de claves <NULL>
MQCPI047 ......archivo de conjunto de claves de CA c:\mqipt\ssl\caCerts.pfx
MQCPI071 ......el certificado del sitio utiliza CN=* O=* OU=* L=* ST=* C=*
MQCPI038 ......el certificado del igual utiliza CN=* O=* OU=* L=* ST=* C=*
MQCPI075 ....servidor principal LDAP en crl.ca_company.com(389)
MQCPI086 ......tiempo de espera excedido de 4 segundos
MQCPI084 ....el tiempo de espera excedido de antememoria CRL es de 1 hora
MQCPI085 ....las CRL se guardarán en los archivos de conjunto de claves
MQCPI078 La ruta 1415 está preparada para las solicitudes de conexión
```

2. En IPT2

   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\\myCert.pfx
SSLServerKeyRingPW=c:\\mqipt\\ssl\\myCert.pwd
```

   Abra un indicador de mandatos:

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

   El mensaje siguiente indica que se ha realizado correctamente:

```
5639-L92 (C) Copyright IBM Corp. 2000, 2003 Reservados todos los derechos
MQCPI001 Arrancando IBM WebSphere MQ internet pass-thru Versión 1.3.0
MQCPI004 Leyendo información de configuración de C:\mqipt\mqipt.conf
MQCPI011 Se utilizará la vía de acceso C:\mqipt\logs para almacenar los
         archivos de anotaciones
MQCPI006 La ruta 1416 se ha iniciado y reenviará mensajes a:
MQCPI034 ....server1.company2.com(1414)
```

```
MQCPI035 ....utilizando protocolos de MQ
MQCPI037 ....parte del Servidor SSL habilitada con las propiedades:
MQCPI031 ......grupos de cifrado <NULL>
MQCPI032 ......archivo de conjunto de claves c:\mqipt\ssl\myCert.pfx
MQCPI047 ......archivo de conjunto de claves de CA <NULL>
MQCPI071 ......el certificado del sitio utiliza CN=* O=* OU=* L=* ST=* C=*
MQCPI038 ......el certificado del igual utiliza CN=* O=* OU=* L=* ST=* C=*
MQCPI033 ......autenticación de cliente establecida en falso
MQCPI078 La ruta 1416 está preparada para las solicitudes de conexión
```

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 MQIPT.QM1
   Hola amigos <Intro>
   <Intro>
   ```

5. Obtenga el mensaje mediante el mandato siguiente:

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

Verá el texto ″Hola amigos″.

Modalidad de proxy SSL

En este ejemplo se muestra cómo ejecutar 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. En él se presupone que el cliente de WMQ y el servidor son de la versión 5.3 y se han configurado para utilizar una conexión SSL.

Si desea más información sobre cómo configurar SSL para WMQ, consulte el manual ″WebSphere MQ Seguridad Versión 5.3″, número de publicación SC10-3801-01.

Para este ejemplo, se presupone lo siguiente:

- El cliente de MQ y el QM se han configurado para utilizar el canal SSL.

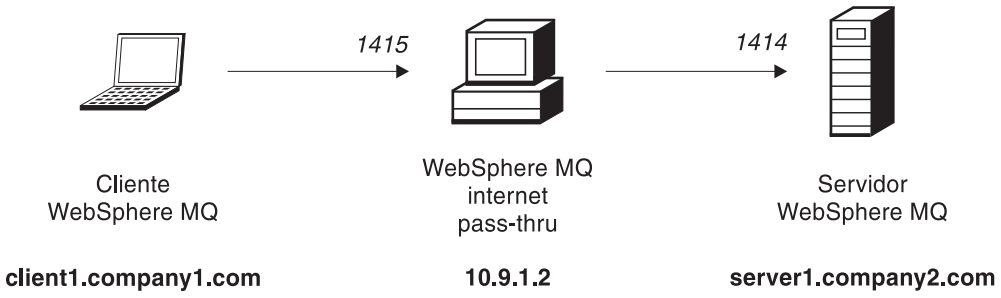

Figura 36. Diagrama de red de la modalidad de proxy SSL

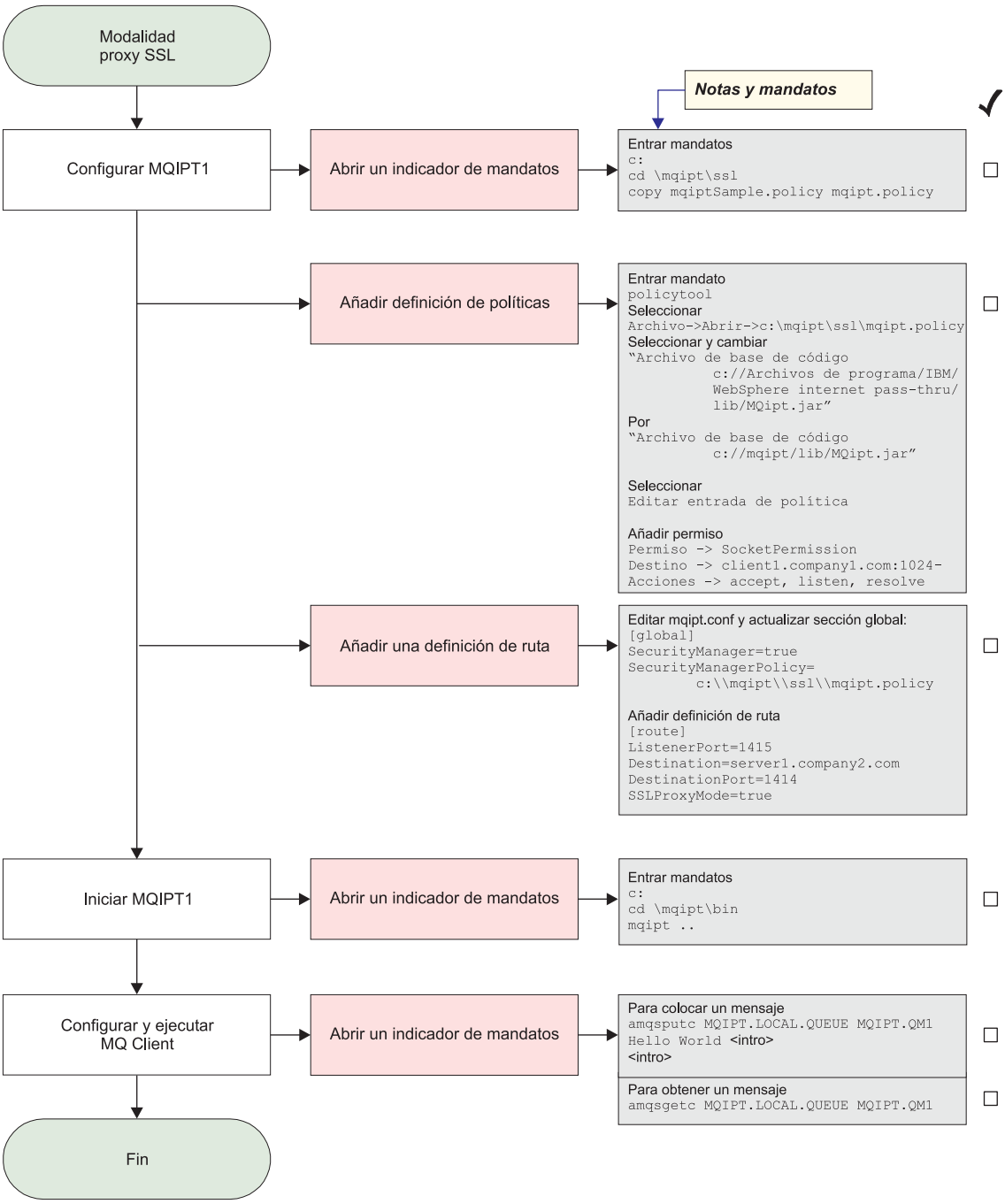

Figura 37. Configuración de la modalidad de proxy SSL

1. En IPT1
   a. Abra un indicador de mandatos y escriba lo siguiente:

      ```
      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-"
Actions = "accept, listen, resolve"
```

2. Edite el archivo `mqipt.conf` y añada las dos propiedades siguientes a la sección global y una definición de ruta:

```
[global]
SecurityManager=true
SecurityManagerPolicy=c:\\mqipt\\ssl\\mqipt.policy
[route]
ListenerPort=1415
Destination=server1.company2.com
DestinationPort=1414
SSLProxyMode=true
```

3. Abra un indicador de mandatos:

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

El mensaje siguiente indica que se ha realizado correctamente:

```
5639-L92 (C) Copyright IBM Corp. 2000, 2003 Reservados todos los derechos
MQCPI001 Arrancando WebSphere MQ internet pass-thru Versión 1.3.0
MQCPI004 Leyendo información de configuración de C:\mqipt\mqipt.conf
MQCPI011 Se utilizará la vía de acceso C:\mqipt\logs para almacenar
         los archivos de anotaciones
MQCPI006 La ruta 1415 se ha iniciado y reenviará mensajes a:
MQCPI034 ....server1.company2.com(1414)
MQCPI035 ....utilizando SSLProxyMode
MQCPI078 La ruta 1415 está preparada para las solicitudes de conexión
```

4. Coloque un mensaje mediante el mandato siguiente:

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

5. Obtenga el mensaje mediante el mandato siguiente:

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

Verá el texto ″Hola amigos″.

Reescritura de Apache

Para este ejemplo, se presupone lo siguiente:

- Se ha instalado el servidor HTTP Apache en c:\apache.
- IBM Web Traffic Express se ha instalado en c:\wte

En el ejemplo se muestra cómo utilizar la directiva de reescritura para convertir una petición HTTP en una redirección proxy de Apache interna. Deben cargarse los módulos proxy y de reescritura, pero ya que Apache no está funcionando realmente en modalidad de proxy, puede dejar comentadas todas las directivas de proxy.

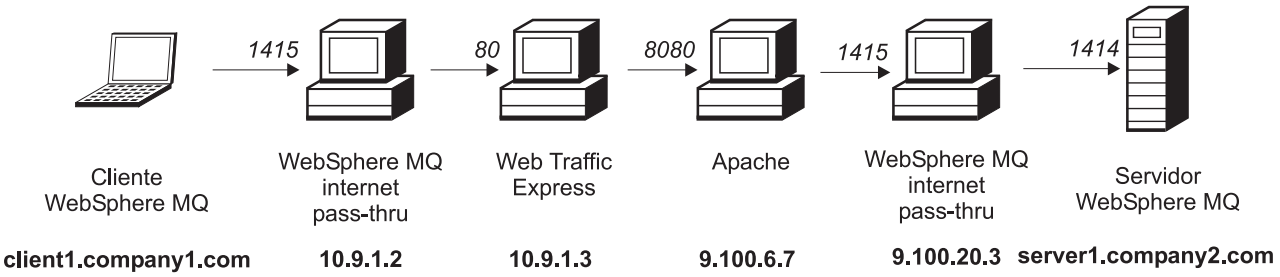

Figura 38. Diagrama de red de la reescritura de Apache

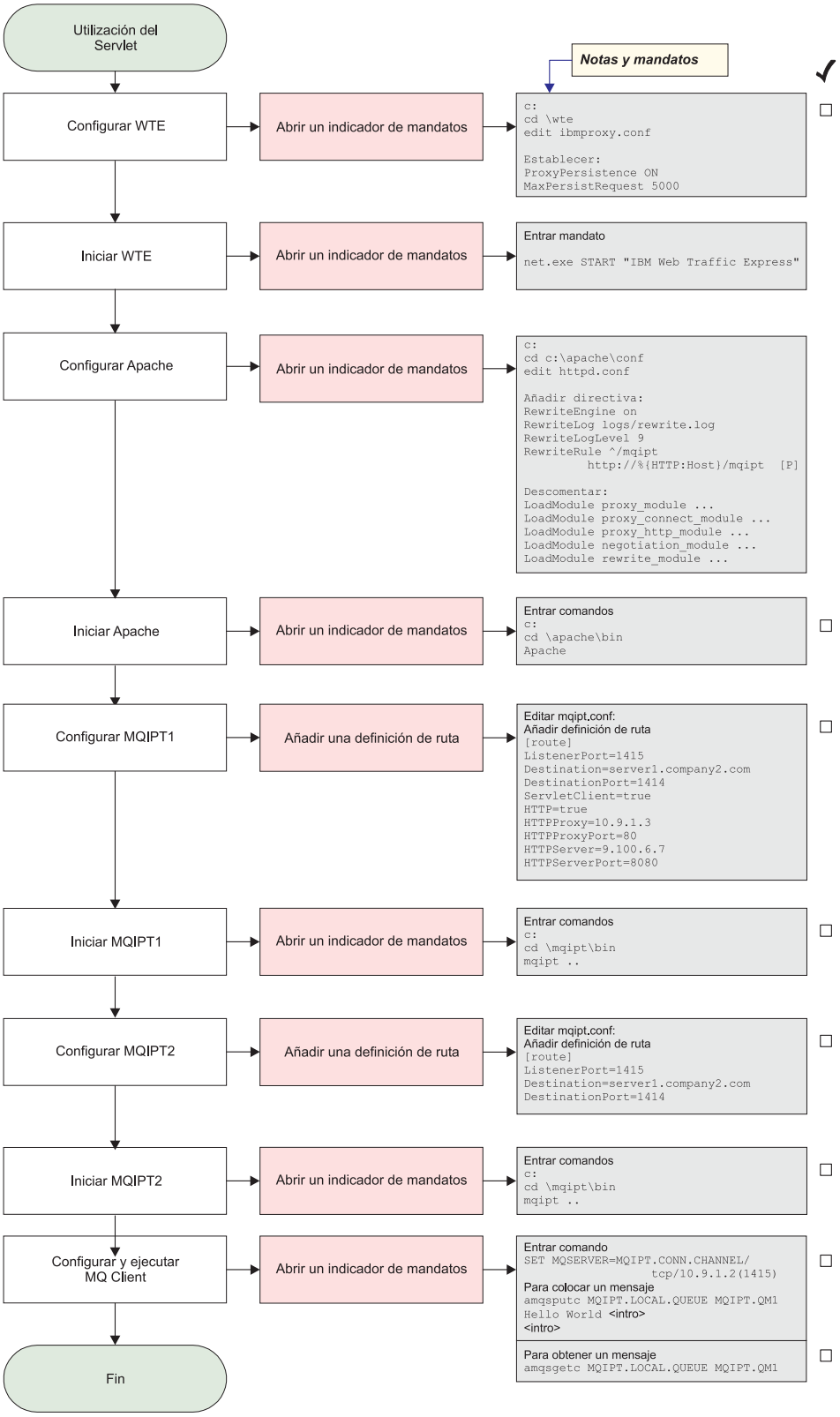

Figura 39. Configuración de la reescritura de Apache

1. En WTE

   Edite c:\wte\ibmroxy.conf

   Cambie las propiedades siguientes:

   ```
   ProxyPersistence ON
   MaxPersistRequest  5000
   ```

2. En Apache

   Edite c:\apache\conf\httpd.conf

   ```
   RewriteEngine on
   RewriteLog logs/rewrite.log
   RewriteLogLevel 9
   RewriteRule ^/mqipt  http://%{HTTP:Host}/mqipt  [P]

   LoadModule proxy_module modules/mod_proxy.so
   LoadModule proxy_connect_module modules/mod_proxy_connect.so
   LoadModule proxy_http_module modules/mod_proxy_http.so
   LoadModule negotiation_module modules/mod_negotiation.so
   LoadModule rewrite_module modules/mod_rewrite.so

   start Apache
   ```

3. En IPT1

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

   ```
   [route]
   ListenerPort=1415
   Destination=server1.company2.com
   DestinationPort=1414
   HTTP=true
   HTTPProxy=10.9.1.3
   HTTPProxyPort=80
   HTTPServer=9.100.6.7
   HTTPServerPort=8080
   ```

   Abra un indicador de mandatos:

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

   El mensaje siguiente indica que se ha realizado correctamente:

   ```
   5639-L92 (C) Copyright IBM Corp. 2000, 2003 Reservados todos los derechos
   MQCPI001 Arrancando WebSphere MQ internet pass-thru Versión 1.3.0
   MQCPI004 Leyendo información de configuración de C:\mqipt\mqipt.conf
   MQCPI011 Se utilizará la vía de acceso C:\mqipt\logs para almacenar
            los archivos de anotaciones
   MQCPI006 La ruta 1415 se ha iniciado y reenviará mensajes a:
   MQCPI034 ....server1.company2.com(1414)
   MQCPI035 ....utilizando HTTP
   MQCPI024 ....y el proxy HTTP en 10.9.1.3(80)
   MQCPI066 ....y el servidor HTTP en 9.100.6.7(8080)
   MQCPI078 La ruta 1415 está preparada para las solicitudes de conexión
   ```

4. En IPT2

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

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

   Abra un indicador de mandatos:

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

El mensaje siguiente indica que se ha realizado correctamente:

```
5639-L92 (C) Copyright IBM Corp. 2000, 2003 Reservados todos los derechos
MQCPI001 Arrancando WebSphere MQ internet pass-thru Versión 1.3.0
MQCPI004 Leyendo información de configuración de C:\mqipt\mqipt.conf
MQCPI011 Se utilizará la vía de acceso C:\mqipt\logs para almacenar
         los archivos de anotaciones
MQCPI006 La ruta 1415 se ha iniciado y reenviará mensajes a:
MQCPI034 ....server1.company2.com(1414)
MQCPI035 ....utilizando protocolos de MQ
MQCPI078 La ruta 1415 está preparada para las solicitudes de conexión
```

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 MQIPT.QM1
   Hola amigos <Intro>
   <Intro>
   ```

7. Obtenga el mensaje mediante el mandato siguiente:

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

Verá el texto ″Hola amigos″.

Rutina de salida de seguridad

Para este ejemplo, se presupone lo siguiente:

- Se ha instalado Java 1.4 SDK.
- Se ha añadido el subdirectorio bin de Java a la variable de entorno PATH.

Ésta es una prueba simple para mostrar cómo utilizar la rutina de salida de seguridad de ejemplo proporcionada, denominada SampleSecurityExit. Esta rutina de salida de seguridad se ha escrito sólo para que puedan utilizarse conexiones de cliente cuyo nombre empiece por los caracteres ″MQIPT″.

Utilizando el nombre de canal srvconn sugerido ″MQIPT.CONN.CHANNEL″ (tal como se usa en la mayoría de estos ejemplos), se podrá completar la conexión del cliente y podrá colocarse un mensaje de WMQ en la cola.

Para comprobar que la rutina de salida de seguridad funciona tal como se esperaba, defina otro canal srvconn con cualquier nombre que no empiece con los caracteres ″MQIPT″; por ejemplo, ″TEST.CONN.CHANNEL″ y repita el mandato amqsputc, pero cambie antes la variable de entorno MQSERVER para que utilice el nuevo nombre de canal. Esta vez se rechazará la conexión y aparecerá un error 2059.

Para comprobar que ″TEST.CONN.CHANNEL″ funciona correctamente sin utilizar la rutina de salida de seguridad, establezca la variable de entorno MQSERVER de forma que señale directamente a la puerta del escucha de WMQ (por ejemplo, 1414), para que no se utilice MQIPT. Esta vez, el mandato amqsputc funcionará como se esperaba.

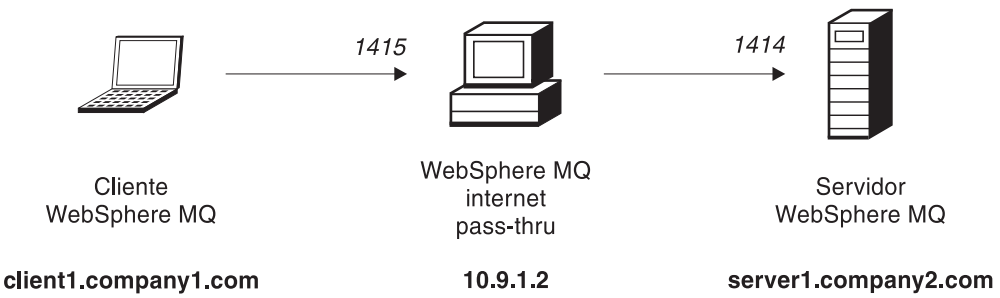

Figura 40. Diagrama de red de la rutina de salida de seguridad

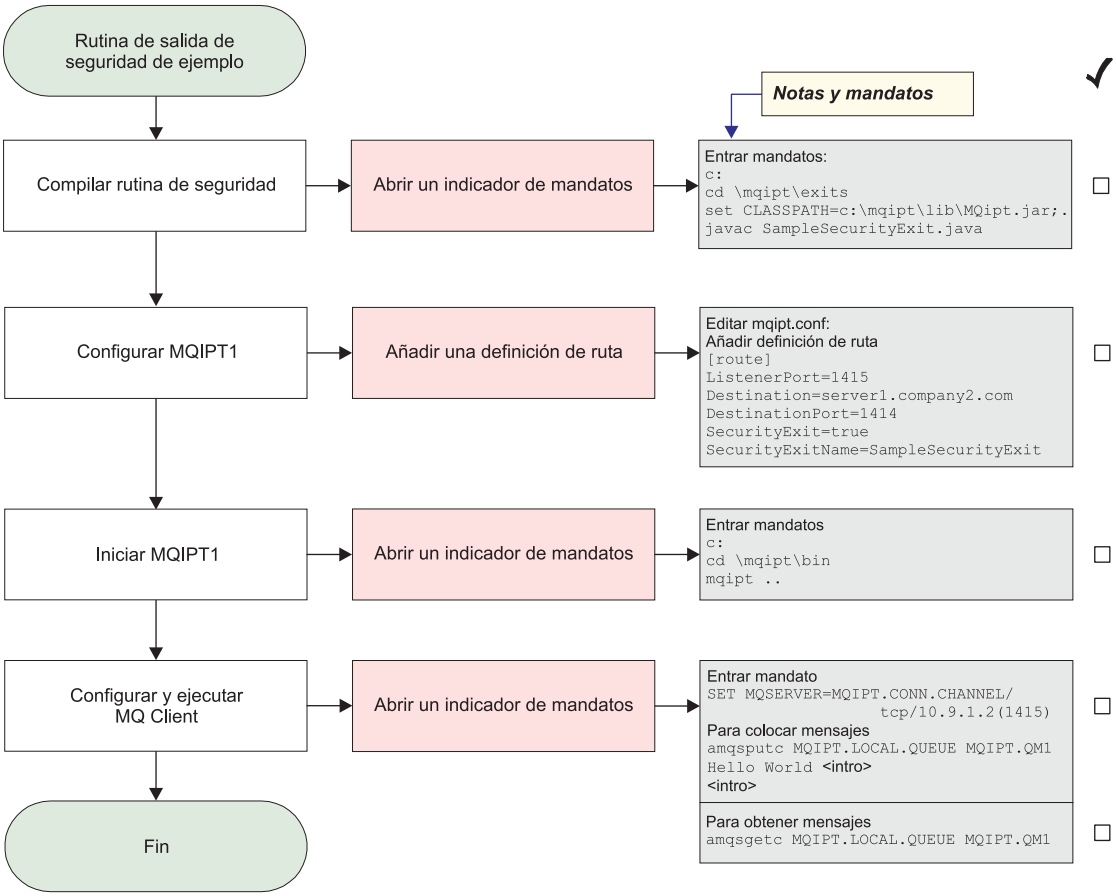

Figura 41. Configuración de la rutina de salida de seguridad

1. En IPT1

   Abra un indicador de mandatos:

   ```
   c:
   cd \mqipt\exits
   set CLASSPATH=c:\mqipt\lib\MQipt.jar;.
   javac SampleSecurityExit.java
   ```

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

   ```
   [route]
   ListenerPort=1415
   Destination=server1.company2.com
   DestinationPort=1414
   SecurityExit=true
   SecurityExitName=SampleSecurityExit
   ```

   Abra un indicador de mandatos:

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

   El mensaje siguiente indica que se ha realizado correctamente:

   ```
   5639-L92 (C) Copyright IBM Corp. 2000, 2003 Reservados todos los derechos
   MQCPI001 Arrancando WebSphere MQ internet pass-thru Versión 1.3.0
   MQCPI004 Leyendo información de configuración de c:\mqipt\mqipt.conf
   MQCPI011 Se utilizará la vía de acceso c:\mqipt\logs para almacenar los
            archivos de anotaciones
   MQCPI006 La ruta 1415 se ha iniciado y reenviará mensajes a:
   MQCPI034 ....server1.company2.com(1414)
   MQCPI035 ....utilizando protocolos de MQ
   MQCPI079 ....utilizando la rutina de salida de seguridad c:\mqipt\
            exits\SampleSecurityExit
   MQCPI080 ......y un tiempo de espera excedido de 5 segundos
   MQCPI078 La ruta 1415 está preparada para las solicitudes de conexión
   ```

2. 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)
   ```

3. Coloque un mensaje mediante el mandato siguiente:

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

4. Obtenga el mensaje mediante el mandato siguiente:

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

Verá el texto ″Hola amigos″.

Rutina de salida de seguridad de direccionamiento

Para este ejemplo, se presupone lo siguiente:

- Se ha instalado Java 1.4 SDK.
- Se ha añadido el subdirectorio bin de Java a la variable de entorno PATH.
- Se han creado tres gestores de colas idénticos en tres servidores distintos.

El ejemplo siguiente es un ejemplo funcional en el que se dirigirán peticiones de conexión de clientes dinámicamente, y de forma circular, a un grupo de servidores de gestores de colas de WMQ. El gestor de colas de cada servidor del grupo debe ser una imagen reflejada de cada uno de los otros.

La lista de nombres de servidor se leerá de un archivo de configuración. El nombre y la ubicación del archivo de configuración se definen mediante las propiedades SecurityExitName y SecurityExitPath. El archivo de configuración de ejemplo, denominado SampleRoutingExit.conf, contiene las entradas siguientes:

```
server1.company.com:1414
server2.company.com:1415
server3.company.com:1416
```

Debe cambiar estos nombres de servidor para que se ajusten a su entorno.

La primera vez que se emita el mandato amqsputc, el mensaje de WMQ se colocará en la cola MQIPT.LOCAL.QUEUE del QM de server1. La segunda vez que se emita, el mensaje aparecerá en el QM de server2, etc. Mediante esta configuración, el mandato amqsgetc no puede recuperar el mensaje que se acaba de colocar en la cola, ya que la petición de conexión del cliente que utiliza el mandato amqsgetc se pasará al siguiente QM de la lista. Pero al emitir tres mandatos amqsputc, seguidos de tres mandatos amqsgetc, se garantizará que cada mensaje se recupere en el mismo orden. Por tanto, al utilizar otro cliente de WMQ, si se conecta directamente a un QM (es decir, sin utilizar el MQIPT de este ejemplo), podrá recuperar de forma selectiva los mensajes de cualquiera de los gestores de colas.

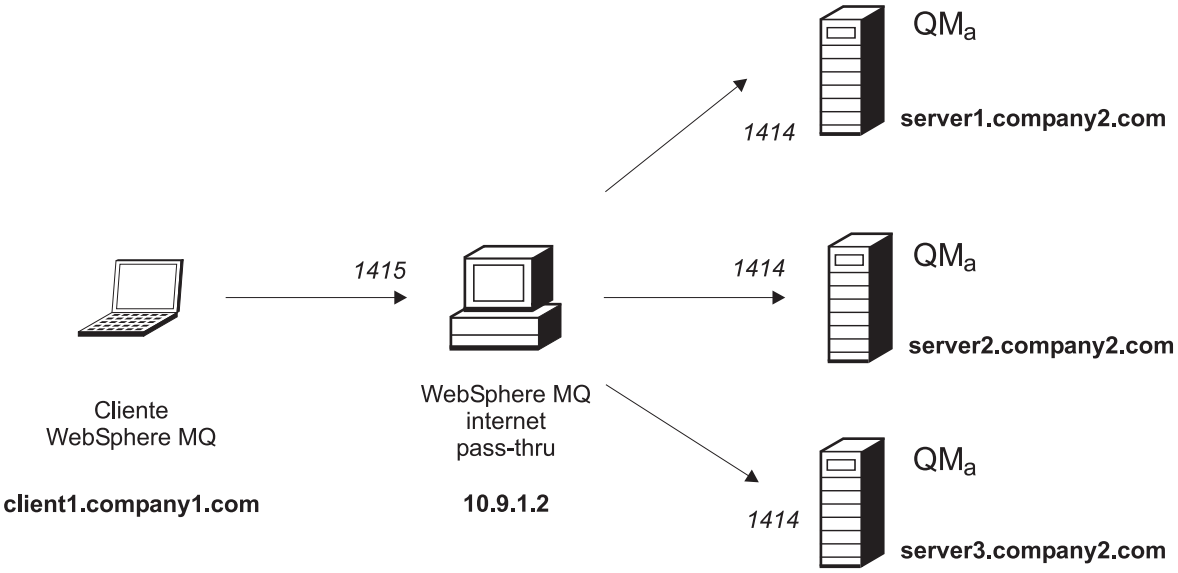

Figura 42. Diagrama de red de la rutina de salida de seguridad de direccionamiento

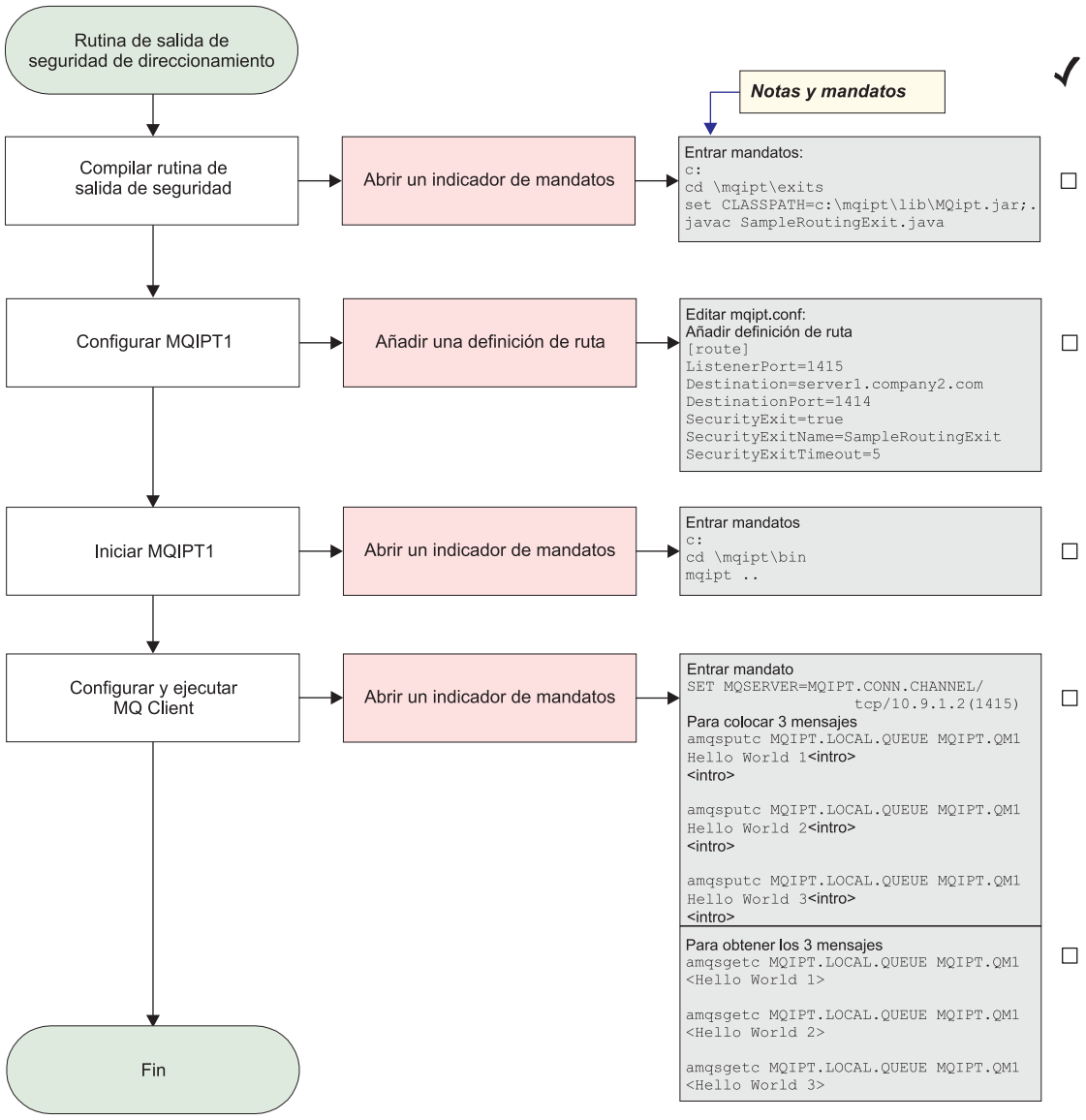

Figura 43. Configuración rutina de salida de seguridad de direccionamiento

1. En IPT1

   Abra un indicador de mandatos:

   ```
   c:
   cd \mqipt\exits
   set CLASSPATH=c:\mqipt\lib\MQipt.jar;.
   javac SampleRoutingExit.java
   ```

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

   ```
   [route]
   ListenerPort=1415
   Destination=server1.company2.com
   DestinationPort=1414
   SecurityExit=true
   SecurityExitName=SampleRoutingExit
   ```

   Abra un indicador de mandatos:

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

El mensaje siguiente indica que se ha realizado correctamente:

```
5639-L92 (C) Copyright IBM Corp. 2000, 2003 Reservados todos los derechos
MQCPI001 Arrancando WebSphere MQ internet pass-thru Versión 1.3.0
MQCPI004 Leyendo información de configuración de c:\mqipt\mqipt.conf
MQCPI011 Se utilizará la vía de acceso c:\mqipt\logs para almacenar
         los archivos de anotaciones
MQCPI006 La ruta 1415 se ha iniciado y reenviará mensajes a:
MQCPI034 ....server1.company2.com(1414)
MQCPI035 ....utilizando protocolos de MQ
MQCPI079 ....utilizando la rutina de salida de seguridad c:\mqipt\
         exits\SampleRoutingExit
MQCPI080 ......y un tiempo de espera excedido de 5 segundos
MQCPI078 La ruta 1415 está preparada para las solicitudes de conexión
```

2. 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)
```

3. Coloque tres mensajes mediante el mandato siguiente:

```
amqsputc MQIPT.LOCAL.QUEUE MQIPT.QM1
Hola amigos 1 <Intro>
<Intro>amqsputc MQIPT.LOCAL.QUEUE MQIPT.QM1
Hola amigos 2 <Intro>
<Intro>amqsputc MQIPT.LOCAL.QUEUE MQIPT.QM1
Hola amigos 3 <Intro>
<Intro>
```

4. Obtenga el mensaje mediante el mandato siguiente:

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

Verá el texto ″Hola amigos 1″, ″Hola amigos 2″ y ″Hola amigos 3″.

Rutina de salida de una ruta dinámica

Para este ejemplo, se presupone lo siguiente:

- Se ha instalado Java 1.4 SDK.
- Se ha añadido el subdirectorio bin de Java a la variable de entorno PATH.
- Se han creado tres gestores de colas diferentes en tres servidores distintos.

El ejemplo siguiente es un ejemplo funcional en el que se muestra cómo dirigir peticiones de conexión de clientes dinámicamente a un servidor de destino, en función del nombre del canal que se utiliza. La primera parte del nombre del canal es el nombre del gestor de colas, de ahí que, en el ejemplo, para poder conectarse al QM1, el nombre de un canal svrconn deba ser QM1.MQIPT.CONN.CHANNEL. Mediante este convenio de denominación de canales, MQIPT sólo necesita una ruta para poder proporcionar los servicios necesarios a todas las peticiones de conexión.

La lista de nombres de servidor y de gestores de colas de servidor se leerá de un archivo de configuración. El nombre y la ubicación del archivo de configuración se definen mediante las propiedades SecurityExitName y SecurityExitPath. El archivo de configuración de ejemplo, denominado SampleOneRouteExit.conf, contiene las entradas siguientes:

```
QM1   server1.company.com:1414
QM2   server2.company.com:1415
QM3   server3.company.com:1416
```

Debe cambiar estos nombres de servidor para que se ajusten a su entorno.

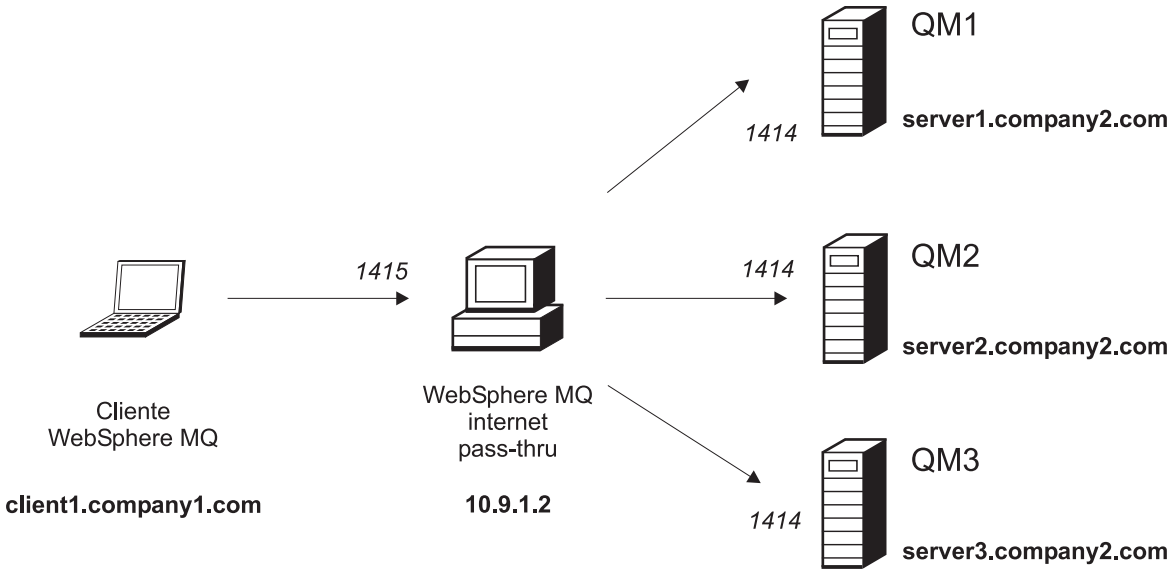

Figura 44. Diagrama de red de la rutina de salida de una ruta dinámica

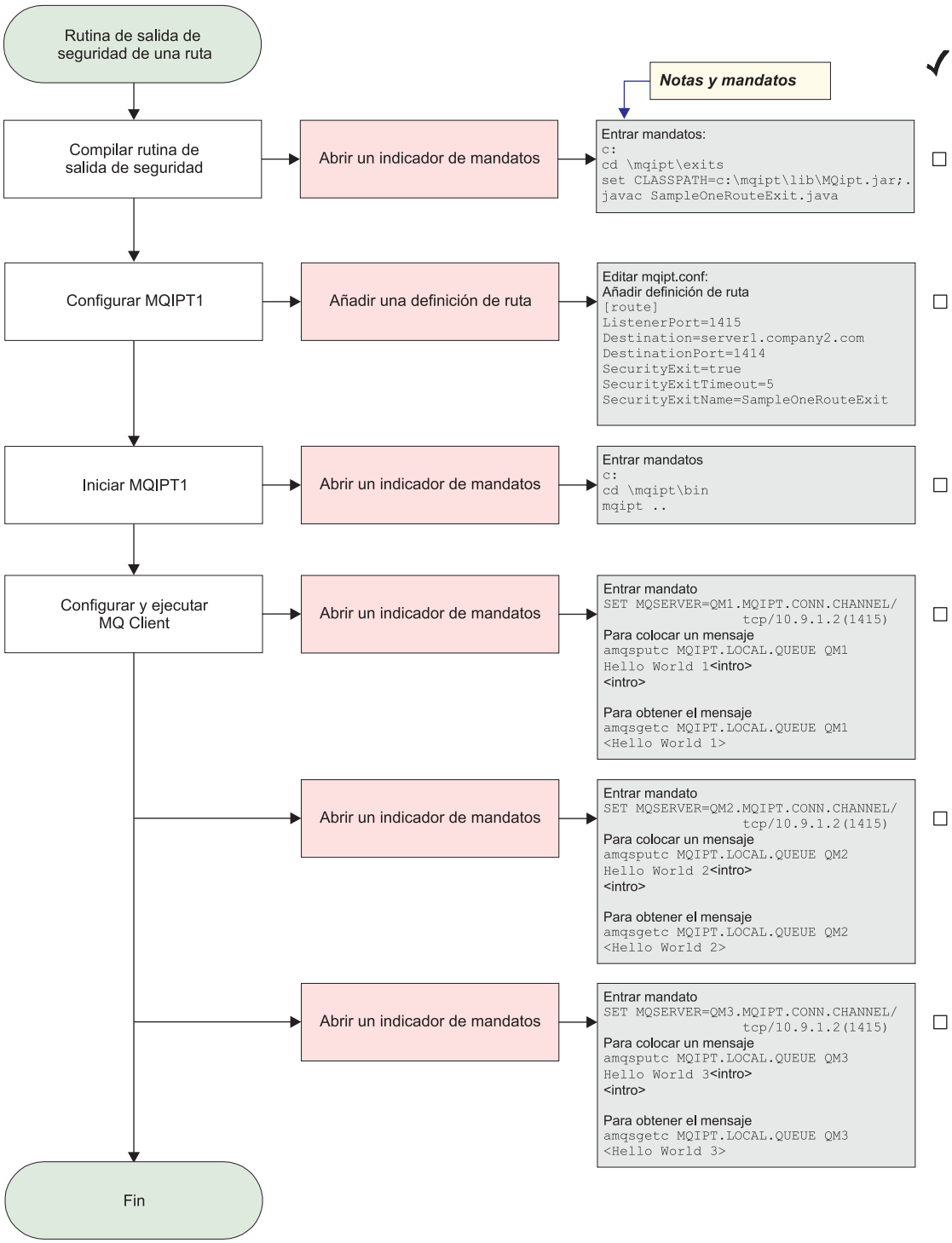

Figura 45. Configuración de la rutina de salida de una ruta dinámica

1. En IPT1

   Abra un indicador de mandatos:

   ```
   c:
   cd \mqipt\exits
   set CLASSPATH=c:\mqipt\lib\MQipt.jar;.
   javac SampleOneRouteExit.java
   ```

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

   ```
   [route]
   ListenerPort=1415
   Destination=server1.company2.com
   DestinationPort=1414
   SecurityExit=true
   SecurityExitName=SampleOneRouteExit
   ```

   Abra un indicador de mandatos:

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

   El mensaje siguiente indica que se ha realizado correctamente:

   ```
   5639-L92 (C) Copyright IBM Corp. 2000, 2003 Reservados todos los derechos
   MQCPI001 Arrancando WebSphere MQ internet pass-thru Versión 1.3.0
   MQCPI004 Leyendo información de configuración de c:\mqipt\mqipt.conf
   MQCPI011 Se utilizará la vía de acceso c:\mqipt\logs para almacenar
            los archivos de anotaciones
   MQCPI006 La ruta 1415 se ha iniciado y reenviará mensajes a:
   MQCPI034 ....server1.company2.com(1414)
   MQCPI035 ....utilizando protocolos de MQ
   MQCPI079 ....utilizando la rutina de salida de seguridad c:\mqipt\
            exits\SampleOneRouteExit
   MQCPI080 ......y un tiempo de espera excedido de 5 segundos
   MQCPI078 La ruta 1415 está preparada para las solicitudes de conexión
   ```

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

   ```
   SET MQSERVER=QM1.MQIPT.CONN.CHANNEL/TCP/10.9.1.2(1415)
   ```

3. Coloque un mensaje mediante el mandato siguiente:

   ```
   amqsputc MQIPT.LOCAL.QUEUE QM1
   Hola amigos 1 <Intro>
   <Intro>
   ```

4. Obtenga el mensaje mediante el mandato siguiente:

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

   Verá el texto ″Hola amigos 1″.

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

   ```
   SET MQSERVER=QM2.MQIPT.CONN.CHANNEL/TCP/10.9.1.2(1415)
   ```

6. Coloque un mensaje mediante el mandato siguiente:

   ```
   amqsputc MQIPT.LOCAL.QUEUE QM2
   Hola amigos 2 <Intro>
   <Intro>
   ```

7. Obtenga el mensaje mediante el mandato siguiente:

   ```
   amqsgetc MQIPT.LOCAL.QUEUE QM2
   ```

   Verá el texto ″Hola amigos 2″.

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

   ```
   SET MQSERVER=QM3.MQIPT.CONN.CHANNEL/TCP/10.9.1.2(1415)
   ```

9. Coloque un mensaje mediante el mandato siguiente:

   ```
   amqsputc MQIPT.LOCAL.QUEUE QM3
   Hola amigos 3 <Intro>
   <Intro>
   ```

10. Obtenga el mensaje mediante el mandato siguiente:

    ```
    amqsgetc MQIPT.LOCAL.QUEUE QM3
    ```

    Verá el texto ″Hola amigos 3″.

Capítulo 21. Mantenimiento de internet pass-thru

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

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 las 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 46 en la página 150. Los números hacen referencia a las notas siguientes.

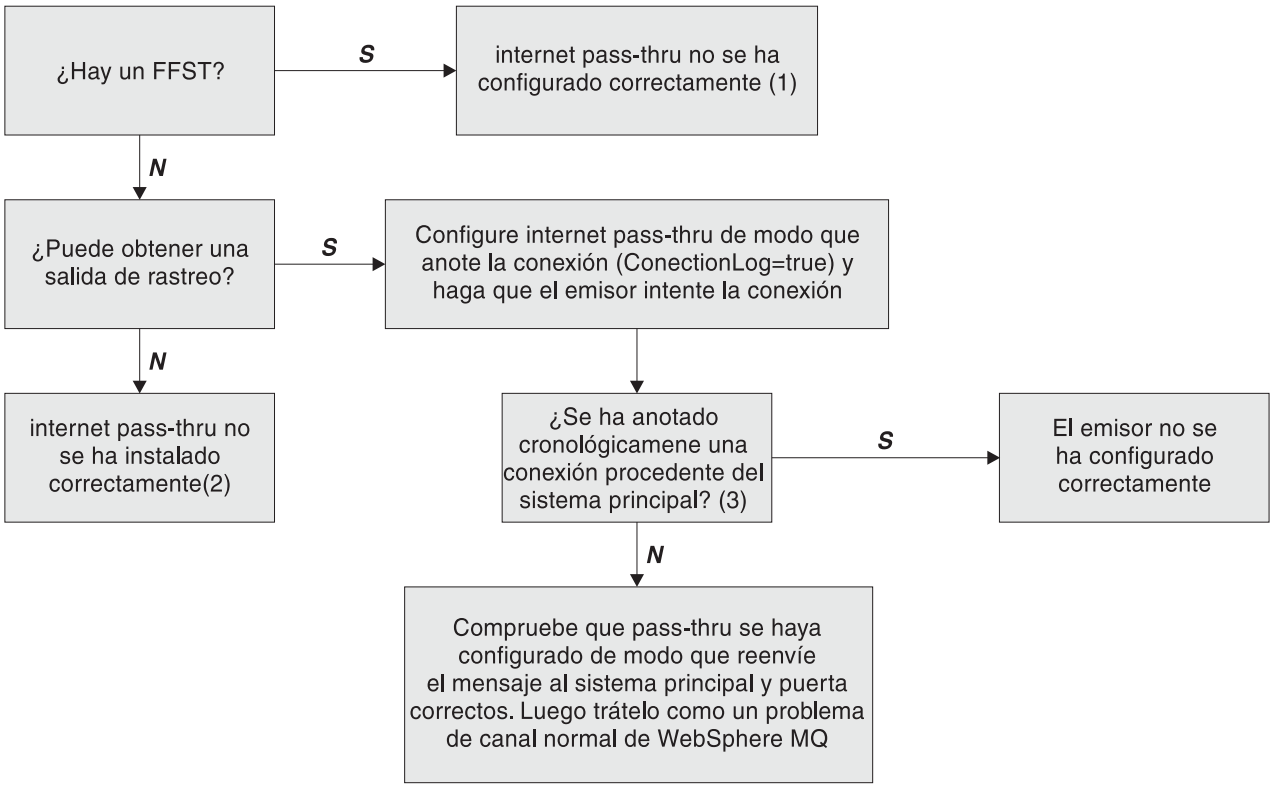

Figura 46. Diagrama de flujo de determinación de problemas

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 50 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. Ésta 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 22. Mensajes

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

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 MQCxWxxx son mensajes de aviso.
- Los mensajes MQCxExxx son mensajes de error.

MQCAE001 Sistema principal desconocido: {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 El sistema ha reportado el siguiente error: {0}

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

MQCAE005 No se ha definido ninguna dirección válida de destino.

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 se ha definido ninguna puerta válida de destino.

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 se ha definido ninguna puerta de escucha válida.

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 se ha definido ninguna dirección válida de red.

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 se ha definido ninguna puerta válida de mandatos.

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 No se ha podido mostrar la ayuda en línea.

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

Respuesta del Usuario: Asegúrese de que tenga instalado un navegador de la web y que esté disponible en la variable de entorno PATH.

MQCAE011 No se ha podido analizar el parámetro.

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 No se ha podido encontrar el archivo de ayuda en línea {0}

Explicación: No se ha podido encontrar el archivo ″passtfrm.htm″.

Respuesta del Usuario: Asegúrese de que este archivo

esté accesible en el subdirectorio doc idioma.

MQCAE013 Se ha producido una interrupción al intentar mostrar la ayuda en línea.

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 No se reconoce la contraseña que acaba de entrar.

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 Discrepancia de nodos.

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 No se ha podido crear texto NLS para el mensaje {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 ″guiadmin.jar″ esté en la variable CLASSPATH del sistema.
- Que el archivo ″guiadmin.properties″ esté en el archivo ″guiadmin.jar″.
- Que el número de mensaje esté en el archivo ″guiadmin.properties″.

MQCAE018 No se ha podido crear texto NLS para el mensaje 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 ″guiadmin.properties″ esté dañado. Compruebe lo siguiente:

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

MQCAE019 La reintroducción de la nueva contraseña propuesta no ha sido satisfactoria.

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 No se ha podido cambiar los parámetros de acceso de MQIPT.

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 Se ha producido una anomalía interna al identificar 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 Se ha producido una anomalía interna al guardar la configuración de 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.

MQCAE023 MQIPT {0} no ha reconocido la contraseña.

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} no ha reconocido el mandato.

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} no ha podido enviar el archivo de configuración.

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 La conclusión remota está inhabilitada en 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 El aspecto {0} no está soportado.

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 La clase de aspecto {0} no se puede encontrar.

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 Los números de puerta deben encontrarse en el rango que oscila de 0 a 65535.

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

Respuesta del Usuario: Cambie el valor como corresponda.

MQCAE032 El rastreo debe encontrarse en el rango que oscila de 0 a 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 se ha seleccionado ninguna ruta en ningún 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 No se puede conectar a 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 No se puede leer la respuesta de 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 No se ha guardado la configuración.

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 no ha confirmado el guardado de la configuración.

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 Los datos de MQIPT no se han renovado.

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 se ha seleccionado ni MQIPT ni ninguna ruta en un MQIPT.

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 Se ha rechazado la puerta de escucha duplicada.

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 MQIPT se ha eliminado de la vista.

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

MQCAI003 Se ha añadido una ruta nueva para su visualización.

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

MQCAI004 La ruta se ha eliminado de la vista.

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

MQCAI005 Se visualiza el MQIPT seleccionado.

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

MQCAI006 Se visualiza la ruta seleccionada.

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

MQCAI007 Se ha guardado la configuración del cliente.

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

MQCAI008 La visualización de la ayuda en línea es satisfactoria.

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

MQCAI009 La tabla ha sido actualizada.

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

MQCAI010 No se ha seleccionado MQIPT ni ninguna ruta.

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

MQCAI011 La acción del usuario ha sido cancelada.

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

MQCAI014 Se ha guardado la configuración en 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 La ayuda en línea ha finalizado.

Explicación: Se ha visualizado la ayuda en línea tal y como se había solicitado y, a continuación, se ha cerrado.

MQCAI017 Seleccione Archivo/Añadir MQIPT para añadir un MQIPT al árbol.

Explicación: Este mensaje aparece cuando no hay ningún MQIPT en el árbol. Indica que debe añadir uno.

MQCAI018 Se ha añadido un nuevo MQIPT para su visualización.

Explicación: Se ha añadido un MQIPT nuevo tal y como se había indicado.

MQCAI019 Los parámetros de acceso de MQIPT han sido modificados.

Explicación: Se han modificado los parámetros de acceso del MQIPT que actualmente está seleccionado en el árbol.

MQCAI021 Seleccione un MQIPT o una ruta del árbol para visualizar su contenido.

Explicación: Este mensaje aparece cuando no se muestra información en la tabla y le indica cómo puede visualizarla.

MQCAI022 La puerta de mandatos ha cambiado.

Explicación: Se ha solicitado que se modificara la puerta de mandatos de un MQIPT y la acción se ha llevado a cabo.

MQCAI023 La contraseña ha cambiado.

Explicación: Para las comunicaciones futuras con el MQIPT que acaba de modificar debe utilizar la nueva contraseña.

MQCAI025 MQIPT {0} ha sido renovado.

Explicación: La información que contiene el MQIPT se ha actualizado mediante la lectura de su archivo de configuración.

MQCAI026 MQIPT {0} ha recibido una petición de conclusión.

Explicación: El MQIPT ha reconocido que ha recibido una petición de conclusión y ahora concluirá.

MQCAI027 Se ha renovado la configuración de cliente.

Explicación: La información que aparece en el cliente de administración se ha renovado a partir del archivo ″client.conf″ local.

MQCAI028 MQIPT {0} está activo.

Explicación: El MQIPT ha respondido satisfactoriamente a una solicitud ping.

MQCAI029 MQIPT {0} no está activo

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 La ruta {0} no está activa.

Explicación: El MQIPT ha respondido satisfactoriamente a una solicitud ping.

MQCAI031 La ruta {0} no está activa.

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 Este script se utiliza para iniciar el Cliente de Administración para {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 El formato del mandato es:

Explicación: Información de ayuda en línea para el script mqiptGui.

MQCAI102 mqiptGui {sistpral_socks{puerta_socks}}

Explicación: Información de ayuda en línea para el script mqiptGui.

MQCAI103 sistemapral_socks - nombre de sistema principal del proxy SOCKS (opcional)

Explicación: Información de ayuda en línea para el script mqiptGui.

MQCAI104 puerta_socks - dirección de puerta del proxy SOCKS (opcional - por omisión 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 El directorio no existe o no es un directorio.

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 Se ha producido un error en el inicio de la ruta en la puerta {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 No se ha podido encontrar el archivo de configuración {0}.

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 El número de rutas ha excedido {0}. MQIPT se iniciará pero esta configuración no está soportada.

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 La ruta no se ha reiniciado en la puerta de escucha {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 Ruta duplicada definida para la puerta de escucha {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 El directorio de archivo de anotaciones {0} no es válido.

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 El número de puerta de mandatos o de escucha {0} no es válido.

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 El nivel de rastreo {0} está fuera del rango válido que va de 0 a 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 No se ha encontrado la propiedad ListenerPort en la ruta {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 El valor de la propiedad ListenerPort {0} no es válido.

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 0–65535. Compruebe cada ListenerPort en el archivo de configuración.

MQCPE015 No se ha encontrado ningún texto para el número de mensaje {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 El número máximo de hebras de conexión es {0} pero este número es menor que el número mínimo de hebras de conexión, que es {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 Se ha lanzando la excepción {0} que ha provocado que MQIPT se concluya.

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 La propiedad ListenerPort está en blanco - la ruta no se iniciará.

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 No se ha encontrado la sección {0} antes de lo siguiente: {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 El nuevo valor de MaxConnectionThreads es {0}. Este número debe ser mayor que el valor actual {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 El valor CommandPort {0} está fuera del rango válido que va de 1 a 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 La petición de conclusión recibida del Cliente de Administración {0} se ha ignorado porque está inhabilitado.

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 El mandato recibido por el controlador de MQIPT no ha sido reconocido.

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 No se ha podido conectar el servidor en el sistema principal {0}, puerta {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 se ha recibido ninguna respuesta del servidor en el sistema principal {0}, puerta {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 No se ha reconocido la respuesta de MQIPT.

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 Se ha detectado una sección no válida: {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 No se ha podido desechar la salida de las anotaciones.

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 No se ha encontrado {0} en 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 No se ha encontrado la clase {0}.

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 No se ha podido enviar el archivo de configuración al Cliente de Administración en {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 El Cliente de Administración en {0} no ha proporcionado la contraseña correcta.

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 No se ha podido iniciar la escucha de mandatos en la puerta {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 no se ha iniciado como se esperaba.

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 Se ha producido un error de E/S al ejecutar el script mqipt.

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 Se ha producido una interrupción al ejecutar el script mqipt.

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 Nivel no soportado de 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 Existe un conflicto con las propiedades siguientes en la ruta {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} y {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} sólo es válido en el sistema operativo {1}.

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 ...falta el nombre de proxy de HTTP

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} no está permitido ya que la aplicación Pagent no ha podido inicializarse.

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 La aplicación Pagent no ha podido inicializarse.

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 El inicio de la ruta no se ha podido realizar en la puerta {0}, la excepción ha sido: {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 al iniciar o detener Java Security Manager {0}

Explicación: Se ha generado una excepción cuando se intentaba iniciar o detener Java Security Manager.

Respuesta del Usuario: Java Security Manager 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 Excepción de seguridad en la puerta {0} desde el Cliente de Administración.

Explicación: Se ha generado una excepción de seguridad cuando se aceptaba una conexión del cliente de administración.

Respuesta del Usuario: Java Security Manager 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. Java Security Manager debe reiniciarse para que los cambios surtan efecto.

MQCPE051 Excepción de seguridad que acepta una conexión en la ruta {0}.

Explicación: Se ha generado una excepción de seguridad al aceptar una conexión en la ruta especificada.

Respuesta del Usuario: Java Security Manager 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. Java Security Manager debe reiniciarse para que los cambios surtan efecto.

MQCPE052 La petición de conexión en la ruta {0} no se ha podido realizar: {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: Java Security Manager 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. Java Security Manager debe reiniciarse para que los cambios surtan efecto.

MQCPE053 Excepción de seguridad que realiza una conexión a {0}({1}).

Explicación: Se ha generado una excepción de seguridad al realizar una conexión en la ruta especificada.

Respuesta del Usuario: Java Security Manager 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. Java Security Manager debe reiniciarse para que los cambios surtan efecto.

MQCPE054 La petición de conexión en {0}({1}) no se ha podido realizar: {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: Java Security Manager 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. Java Security Manager debe reiniciarse para que los cambios surtan efecto.

MQCPE055 ....falta el nombre de proxy Socks

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 una propiedad SocksProxy para la ruta especificada.

MQCPE056 Existe un conflicto con las propiedades de ruta.

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 El protocolo SSL ({0}) no se ha reconocido.

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.

MQCPE058 La petición CONNECT a {2}({3}) a través de {0}({1}) ha fallado.

Explicación: Se ha enviado una petición CONNECT HTTP al proxy HTTP para crear un túnel SSL al servidor HTTP. El proxy HTTP no ha devuelto una respuesta ″200 OK″ a esta petición.

Respuesta del Usuario: Esto puede ser debido a varios problemas. Habilite el rastreo de la ruta y reintente la conexión. En el archivo de rastreo se mostrará el error real.

MQCPE059 No se ha definido ningún archivo de conjunto de claves.

Explicación: Se ha definido un cliente o un servidor SSL sin especificar al menos un archivo de conjunto de claves.

Respuesta del Usuario: Utilice las propiedades SSLClientKeyRing y SSLClientCAKeyRing de la parte del cliente o SSLServerKeyRing y SSLServerCAKeyRing de la parte del servidor para definir un archivo de conjunto de claves y reinicie la ruta.

MQCPE060 Error en tiempo de ejecución al establecer el tiempo de espera excedido de cliente SSL en {0} segundos.

Explicación: Se ha producido un error en tiempo de ejecución SSL en la parte del cliente al establecer el valor del tiempo de espera excedido.

Respuesta del Usuario: Compruebe que el valor especificado en la propiedad SLClientConnectTimeout sea válido. Si ejecuta un rastreo en la ruta especificada aparecerá más información de error.

MQCPE061 No se ha habilitado ningún grupo de cifrado.

Explicación: Se ha iniciado una conexión de cliente o servidor SSL pero MQIPT no puede determinar una suite de cifrado válida.

Respuesta del Usuario: Compruebe que haya certificados válidos en los archivos de conjunto de claves definidos. Las claves privada y pública utilizadas para generar los certificados y los algoritmos de cifrado utilizados deben cumplir las condiciones indicadas en la lista de suites de cifrado soportadas, que pueden encontrarse en el manual de MQIPT.

MQCPE062 Error en tiempo de ejecución al establecer el grupo de cifrado SSL {0}.

Explicación: Se ha definido una suite de cifrado SSL no soportada en la parte del cliente o del servidor.

Respuesta del Usuario: Compruebe que el valor especificado en las propiedades SSLClientCipherSuites o SSLServerCipherSuites sea válido y que esta conexión le dé soporte. Si ejecuta un rastreo en la ruta especificada aparecerá la lista de suites de cifrado soportadas. El manual de MQIPT contiene una lista de las suites de cifrado soportadas.

MQCPE063 El archivo {0} ya existe: utilice la opción de sustitución.

Explicación: El parámetro de nombre de archivo especificado para el script mqiptPW ya existe.

Respuesta del Usuario: Seleccione otro nombre de archivo o utilice la opción de sustitución.

MQCPE064 Error en tiempo de ejecución al generar las claves de descifrado:\n {0}

Explicación: Se ha producido un error al generar claves de cifrado para descifrar la contraseña utilizada para abrir un archivo de conjunto de claves.

Respuesta del Usuario: El error en tiempo de ejecución que aparece en el mensaje debe solucionarse y el mandato debe volverse a ejecutar.

MQCPE065 Falta el nombre del servidor LDAP.

Explicación: Debe establecerse la propiedad LDAPServer1 o LDAPServer2 si la propiedad LDAP se ha establecido en true.

Respuesta del Usuario: Edite el archivo de configuración y defina una propiedad LDAPServer* para la ruta especificada.

MQCPE066 Falta la contraseña LDAP de la propiedad LDAPServer{0}Password.

Explicación: Se ha especificado un ID de usuario LDAP sin contraseña.

Respuesta del Usuario: Edite el archivo de configuración y defina una propiedad LDAPServer*Password para la ruta especificada.

MQCPE067 Falta el Cliente SSL o el Servidor SSL para el servidor LDAP.

Explicación: Debe establecerse la propiedad SSLClient o SSLServer si la propiedad LDAP se ha establecido en true.

Respuesta del Usuario: Edite el archivo de configuración y defina una propiedad SSLClient o SSLServer para la ruta especificada.

MQCPE068 Falta el nombre de la rutina de salida de seguridad.

Explicación: La propiedad SecurityExitName debe establecerse si la propiedad SecurityExit se ha establecido en true.

Respuesta del Usuario: Edite el archivo de configuración y defina una propiedad SecurityExitName para la ruta especificada.

MQCPE069 Dirección de puerta no válida {0} en la respuesta de rutina de salida de seguridad.

Explicación: La dirección de puerta especificada en SecurityExitResponse no es válida.

Respuesta del Usuario: La dirección de puerta debe estar dentro del rango de 1024-65535.

MQCPE070 Código de razón desconocido en la respuesta de rutina de salida de seguridad {0}.

Explicación: No se da soporte al código de razón especificado en SecurityExitResponse.

Respuesta del Usuario: Consulte el manual de MQIPT para obtener una lista de los códigos de razón soportados.

MQCPE071 Error al escribir en {0}.

Explicación: Se ha producido un error al crear o actualizar el archivo especificado. El mensaje de error también contiene la excepción generada.

Respuesta del Usuario: Debe rectificarse el error indicado en la excepción y debe ejecutarse de nuevo el mandato.

MQCPE072 Se ha producido un error desconocido en la rutina de salida de seguridad {0}.

Explicación: Se ha producido un error en una rutina de salida de seguridad definida por el usuario al validar una petición de conexión.

Respuesta del Usuario: Habilita el rastreo en la rutina de salida de seguridad y reintente la petición de la conexión. El error se grabará en el archivo de rutina de salida de seguridad de rastreo.

MQCPI001 {0} starting

Explicación: Esta instancia de MQIPT está iniciando su ejecución. Posteriormente se visualizarán mensajes de inicialización adicionales.

MQCPI002 Concluyendo {0}.

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 Conclusión de {0} completa.

Explicación: El proceso de conclusión ha finalizado. Todos los procesos de MQIPT han finalizado.

MQCPI004 Leyendo información de configuración desde {0}.

Explicación: Se está leyendo el archivo de configuración de MQIPT, mqipt.conf, desde el directorio que se describe en este mensaje.

MQCPI005 Puerta de escucha especificada como no activa - {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 La ruta {0} se está iniciando y reenviará mensajes a:

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. Cuando la ruta esté preparada para aceptar conexiones, aparecerá el mensaje MQCPI078.

MQCPI007 La ruta {0} se ha detenido.

Explicación: Se está concluyendo la ruta que estaba operando en la propiedad 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 A la escucha de mandatos de control en la puerta {0}.

Explicación: Esta instancia de MQIPT está escuchando los mandatos de control en la puerta especificada.

MQCPI009 Mandato de control recibido: {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 Deteniendo puerta de mandatos en {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 Se utilizará la vía de acceso {0} para almacenar los archivos de anotaciones.

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 El cambio de valor de MinConnectionThreads no ha tenido ninguna repercusión una vez que se ha iniciado la ruta.

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 Se ha cerrado la conexión de {0} al sistema principal {1}.

Explicación: Este mensaje se emite en las anotaciones de conexión para registrar la actividad de conexión.

MQCPI014 No se ha reconocido el protocolo de captador de atención ({0}).

Explicación: Este mensaje se emite en las anotaciones de conexión para registrar la actividad de conexión.

MQCPI015 El acceso al cliente se ha inhabilitado en esta ruta.

Explicación: Este mensaje se emite en las anotaciones de conexión para registrar la actividad de conexión.

MQCPI016 El acceso al gestor de colas se ha inhabilitado en esta ruta.

Explicación: Este mensaje se emite en las anotaciones de conexión para registrar la actividad de conexión.

MQCPI017 Se ha conectado un gestor de colas en {0} al sistema principal {1}.

Explicación: Este mensaje se emite en las anotaciones de conexión para registrar la actividad de conexión.

MQCPI018 Se ha conectado un cliente en {0} al sistema principal {1}.

Explicación: Este mensaje se emite en las anotaciones de conexión para registrar la actividad de conexión.

MQCPI019 Se han creado {0} rutas - esta cifra supera el número máximo de rutas soportadas, que es {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 Se ha enviado el archivo de configuración al Cliente de Administración.

Explicación: Como resultado de una petición del cliente de administración, se ha enviado el archivo de configuración.

MQCPI021 Se ha habilitado la comprobación de contraseña en la puerta de mandatos.

Explicación: Este mensaje indica que se necesita una contraseña para acceder a la puerta de mandatos.

MQCPI022 Se ha inhabilitado la comprobación de contraseña en la puerta de mandatos.

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 La renovación solicitada por el Cliente de Administración {0} ha finalizado.

Explicación: Como resultado de la recepción de un mandato REFRESH, MQIPT ha vuelto a leer su archivo de configuración y se ha reiniciado.

MQCPI026 El Cliente de Administración {0} ha solicitado la conclusión.

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 ....parte del Cliente SSL habilitada con las propiedades:

Explicación: Este mensaje muestra la ruta que utilizará SSL para enviar datos al sistema principal de destino.

MQCPI037 ....parte del servidor SSL habilitada con las propiedades:

Explicación: Este mensaje muestra la ruta que utilizará SSL para recibir datos del sistema principal de destino.

MQCPI038 ......el certificado del igual utiliza {0}

Explicación: Este mensaje lista los nombres distinguidos que se utilizan para controlar la autenticación de los certificados de igual.

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 El Cliente de Administración {0} ha accedido a la puerta de mandatos.

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 ....responderá a las peticiones del asesor de distribuidor de la red en la modalidad{0}.

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 Se ha alcanzado el número máximo de conexiones en la ruta {0} - se bloquearán las próximas peticiones.

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 Ahora las conexiones en la ruta {0} están desbloqueadas.

Explicación: Este mensaje se graba en la consola del sistema cuando se desbloquea la ruta y puede aceptar peticiones de conexión.

MQCPI044 MQIPT se ha lanzado desde el inicio del sistema.

Explicación: Se ha iniciado MQIPT como un servicio del sistema.

MQCPI045 Lanzando MQIPT desde el inicio del sistema.

Explicación: MQIPT se va a iniciar como un servicio del sistema.

MQCPI046 Esté inactivo durante {0} segundos mientras se lanza MQIPT desde el inicio del sistema.

Explicación: El proceso fork permanecerá inactivo durante este período mientras comprueba si MQIPT se ha iniciado correctamente con un servicio del sistema.

MQCPI047 .....archivo de conjunto de claves de CA {0}.

Explicación: Este mensaje proporciona el nombre de archivo de conjunto de claves CA para esta ruta.

MQCPI048 El sondeo realizado por el Cliente de Administración {0} ha finalizado.

Explicación: Mensaje de respuesta de IPTController al cliente de administración.

MQCPI049 ....prioridad de QoS (Calidad de servicio) en dest = {0}, en canal de llamada = {1}

Explicación: Se muestra la prioridad del tráfico en las dos direcciones de esta ruta.

MQCPI050 Agregando entrada en inittab para iniciar automáticamente MQIPT al iniciar el sistema.

Explicación: El usuario ha ejecutado el script mqiptService para iniciar MQIPT como un servicio del sistema.

MQCPI051 Quitando entrada de inittab que inicia automáticamente MQIPT al iniciar el sistema.

Explicación: El usuario ha ejecutado el script mqiptService para que MQIPT no se inicie como un servicio del sistema.

MQCPI052 ....Parte del servidor socks habilitado.

Explicación: Esta ruta actuará como un servidor SOCKS (proxy) y aceptará las conexiones de una aplicación con posibilidad para Socks.

MQCPI053 Iniciando Java Security Manager

Explicación: El producto Java Security Manager por omisión se iniciará ya que la propiedad SecurityManager se ha establecido en true.

MQCPI054 Deteniendo Java Security Manager

Explicación: Java se detendrá ya que la propiedad SecurityManager se ha establecido en false.

MQCPI055 Estableciendo java.security.policy en {0}

Explicación: Java está a punto de iniciarse y utilizará el archivo de políticas proporcionado.

MQCPI056 Java Security Manager debe reiniciarse para utilizar el archivo de una nueva política.

Explicación: La propiedad SecurityManagerPolicy se ha modificado, pero no entrará en vigor hasta que se reinicie Java Security Manager.

Respuesta del Usuario: Cambie la propiedad SecurityManager a false, emita un mandato refresh para detener Java. A continuación, vuelva a cambiar la propiedad SecurityManager a true y emita otro mandato refresh para iniciar Java Security Manager con el nuevo archivo de políticas.

MQCPI057 ....nivel de rastreo {0} habilitado.

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 ....y un nombre de URI de {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 ....cliente del servlet habilitado

Explicación: Este mensaje se graba en la consola del sistema cuando se inicia una ruta. Esta ruta se conectará con el servlet MQIPT.

MQCPI060 Instalando los archivos para iniciar automáticamente MQIPT al iniciar el sistema.

Explicación: El usuario ha ejecutado el script mqiptService para iniciar MQIPT como un servicio del sistema.

MQCPI061 Quitando los archivos que inician automáticamente MQIPT al iniciar el sistema.

Explicación: El usuario ha ejecutado el script mqiptService para que MQIPT no se inicie como un servicio del sistema.

MQCPI064 ....no hay autenticación de SSL en esta ruta.

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 ....en modalidad de proxy de SSL.

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.

MQCPI066 ....servidor HTTP en {0}{1}.

Explicación: Este mensaje indica que la conexión de salida para esta ruta se realizará utilizando el servidor HTTP.

MQCPI067 Configurando los enlaces a bibliotecas en tiempo de ejecución TQoS.

Explicación: El usuario ha ejecutado el script mqiptQoS para enlazar con las bibliotecas de tiempo de ejecución de TQoS reales.

MQCPI068 Eliminando los enlaces a bibliotecas en tiempo de ejecución TQoS.

Explicación: El usuario ha ejecutado el script mqiptQoS para eliminar los enlaces con las bibliotecas de tiempo de ejecución de TQoS reales.

MQCPI069 ....enlazando con la dirección local {0}.

Explicación: Este mensaje muestra la dirección IP local a la que se enlaza cada conexión. Esto sólo debe utilizarse en un sistema multitarjeta.

MQCPI070 ....utilizando el rango de dirección de puerta local {0}-{10}.

Explicación: Este mensaje muestra las direcciones de puerta locales que se utilizarán para una conexión. Esto permitirá a los administradores del cortafuegos restringir las conexiones procedentes de MQIPT.

MQCPI071 El certificado del sitio utiliza {0}.

Explicación: Este mensaje lista los nombres distinguidos que se utilizan para controlar la selección del certificados de un sitio.

MQCPI072 .....y la etiqueta del certificado {0}.

Explicación: Este mensaje lista el nombre de etiqueta que se utiliza para controlar la selección del certificados de un sitio.

MQCPI073 Se ha actualizado el archivo {0}.

Explicación: Se ha actualizado el nombre de archivo especificado para el script mqiptPW.

MQCPI074 Se ha creado el archivo {0}.

Explicación: Se ha creado el nombre de archivo especificado para el script mqiptPW.

MQCPI075 ....servidor principal LDAP en {0}({1}).

Explicación: Este mensaje indica el nombre del servidor LDAP principal utilizado para el soporte de CRL.

MQCPI076 ....servidor de copia de seguridad LDAP en {0}({1}).

Explicación: Este mensaje indica el nombre del servidor LDAP de copia de seguridad utilizado para el soporte de CRL.

MQCPI077 ....los errores LDAP se ignorarán.

Explicación: Este mensaje indica que se ignorarán todos los errores recibidos de LDAP.

MQCPI078 La ruta {0} está preparada para las solicitudes de conexión.

Explicación: Este mensaje aparece cuando una ruta está preparada para aceptar peticiones de conexión.

MQCPI079 ....utilizando la rutina de salida de seguridad {0}.

Explicación: Este mensaje se graba en la consola del sistema cuando se inicia una ruta. Se utiliza para mostrar el nombre totalmente calificado de la rutina de salida de seguridad.

MQCPI080 .....y un tiempo de espera excedido de {0} segundos.

Explicación: Este mensaje se graba en la consola del sistema cuando se inicia una ruta. Se utiliza para mostrar el valor de tiempo de espera excedido de la

rutina de salida de seguridad.

MQCPI081 Mensaje de inicio de WebSphere MQ internet pass-thru

Explicación: Mensaje de inicio de WebSphere MQ internet pass-thru como servicio.

MQCPI082 Mensaje de detención de WebSphere MQ internet pass-thru

Explicación: Mensaje de detención de WebSphere MQ internet pass-thru como servicio.

MQCPI083 ....los mandatos de renovación no reiniciarán la ruta.

Explicación: Este mensaje indica que cuando se emita un mandato refresh, la ruta no se reiniciará.

MQCPI084 ....el tiempo de espera excedido de antememoria CRL es de {0} hora(s)

Explicación: Este mensaje de consola muestra cuánto tiempo permanecerá una CRL (o ARL) en la antememoria de MQIPT.

MQCPI085 ....las CRL se guardarán en los archivos de conjunto de claves

Explicación: Este mensaje de consola significa que todas las CRL (o ARL) que se recuperen de un servidor LDAP se guardarán en el archivo de conjunto de claves, adjuntadas al certificado de CA asociado.

MQCPI086 ......tiempo de espera excedido de {0} segundos.

Explicación: Este mensaje se graba en la consola del sistema cuando se inicia una ruta. Se utiliza para mostrar el valor de tiempo de espera excedido para poder realizar la conexión al servidor LDAP.

MQCPI087 ......el ID de usuario es {0}.

Explicación: Este mensaje se graba en la consola del sistema cuando se inicia una ruta. Se utiliza para mostrar el nombre de ID de usuario para poder realizar la conexión al servidor LDAP.

MQCPI100 Este script se utiliza para iniciar {0}.

Explicación: Mensaje de ayuda en línea para el script mqipt.

MQCPI101 El formato del mandato es:

Explicación: Mensaje de ayuda en línea para el script mqipt.

MQCPI102 mqipt {nombre_dir}

Explicación: Mensaje de ayuda en línea para el script mqipt.

MQCPI103 nombre_dir - directorio que contiene mqipt.conf

Explicación: Mensaje de ayuda en línea para el script mqipt.

MQCPI106 Este script se utiliza para ver el número de la versión actual.

Explicación: Mensaje de ayuda en línea para el script mqiptVersion.

MQCPI107 mqiptVersion {-v}

Explicación: Mensaje de ayuda en línea para el script mqiptVersion.

MQCPI108 donde -v también mostrará la indicación de la hora del build.

Explicación: Mensaje de ayuda en línea para el script mqiptVersion.

MQCPI109 Este script se utiliza para iniciar {0}, desde el inicio del sistema, en otra JVM y sólo se utiliza en mqipt.ske. Utilice el script mqipt para iniciar MQIPT desde la línea de mandatos.

Explicación: Mensaje de ayuda en línea del script mqiptFork.

MQCPI110 Esta clase se utiliza para ver un mensaje NLS sencillo en la consola.

Explicación: Mensaje de ayuda en línea de la clase IPTMessages.

MQCPI111 java com.ibm.mq.ipt.IPTMessages (id1_mensaje) {id2_mensaje} {id_mensaje...}

Explicación: Mensaje de ayuda en línea de la clase IPTMessages.

MQCPI112 donde id1_mensaje equivale a una clave del archivo mqipt.properties.

Explicación: Mensaje de ayuda en línea de la clase IPTMessages.

MQCPI113 Este script se utiliza para gestionar MQIPT como un servicio del sistema.

Explicación: Mensaje de ayuda en línea del script mqiptVersion.

MQCPI114 mqiptService (-install | -remove)

Explicación: Mensaje de ayuda en línea del script mqiptVersion.

MQCPI115 -install instalará los archivos para iniciar MQIPT automáticamente al iniciar el sistema.

Explicación: Mensaje de ayuda en línea del script mqiptVersion.

MQCPI116 -remove eliminará los archivos que inician MQIPT automáticamente al iniciar el sistema.

Explicación: Mensaje de ayuda en línea del script mqiptVersion.

MQCPI117 Este script se utiliza para gestionar los enlaces a las bibliotecas de tiempo de ejecución de TQoS.

Explicación: Mensaje de ayuda en línea del script mqiptVersion.

MQCPI118 mqiptQoS (-install | -remove)

Explicación: Mensaje de ayuda en línea del script mqiptVersion.

MQCPI119 -install configurará los enlaces a las bibliotecas en tiempo de ejecución TQoS.

Explicación: Mensaje de ayuda en línea del script mqiptVersion.

MQCPI120 -remove eliminará los enlaces a las bibliotecas en tiempo de ejecución TQoS reales.

Explicación: Mensaje de ayuda en línea del script mqiptVersion.

MQCPI121 Utilice este script para cifrar una contraseña y almacenarla en un archivo.

Explicación: Mensaje de ayuda en línea del script mqiptPW.

MQCPI122 mqiptPW contraseña nombre_archivo { -replace }

Explicación: Mensaje de ayuda en línea del script mqiptPW.

MQCPI123 contraseña - contraseña utilizada para abrir un archivo de conjunto de claves.

Explicación: Mensaje de ayuda en línea del script mqiptPW.

MQCPI124 nombre_archivo - la contraseña cifrada se almacenará en este archivo.

Explicación: Mensaje de ayuda en línea del script mqiptPW.

MQCPI125 Para actualizar un archivo existente debe utilizarse la opción de sustitución.

Explicación: Mensaje de ayuda en línea del script mqiptPW.

MQCPI126 mqipt (-start | -stop)

Explicación: Mensaje de ayuda en línea del script mqiptQoS.

MQCPW001 La CRL ha vencido para {0}.

Explicación: Este mensaje aparece cuando se recupera una CRL (o ARL) de un archivo de conjunto de claves o un servidor LDAP.

Respuesta del Usuario: Actualice la CRL especificada en el servidor LDAP o el archivo de conjunto de claves.

MQCPW002 Error al actualizar el archivo de conjunto de claves {0} con la CRL.

Explicación: Este mensaje aparece cuando se ha habilitado la propiedad LDAPSaveCRLs y no puede actualizarse el archivo de conjunto de claves especificado.

Respuesta del Usuario: Es posible que el archivo especificado esté dañado. Compruebe lo siguiente:

1. Que el acceso de escritura esté habilitado para MQIPT.
2. Que el archivo no se haya abierto con ninguna otra aplicación.

MQCPW003 ....las CRL vencidas se ignorarán.

Explicación: Este mensaje de la consola significa que todas las CRL (o ARL) que hayan caducado se ignorarán y que la petición de conexión puede asignarse.

Apéndice. 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 bajo licencia de IBM o a otros productos IBM en esta publicación no pretende afirmar ni implicar que sólo se puedan utilizar los programas u otros productos de IBM. En lugar del producto 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 este documento. La entrega de este documento no le otorga ninguna licencia sobre dichas patentes. Puede enviar consultas sobre 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/o en otros países:

AIX	FFST	First Failure Support Technology
IBM	IBMLink	MQSeries
SupportPac	WebSphere	

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

Java y todas las marcas basadas en Java son marcas registradas de Sun Microsystems, Inc. en Estados Unidos o en otros países.

UNIX es una marca registrada de The Open Group en Estados Unidos o en otros países.

Otros nombres de empresas, productos y servicios pueden ser marcas registradas o nombres comerciales de terceros.

Bibliografía

Esta publicación está disponible en formato HTML como parte del producto instalado. El HTML se encuentra en un archivo comprimido autoextraíble en el directorio `doc\<entorno_local>\html\<nombre_archivo>.zip`. Antes de utilizar el cliente de administración, debe descomprimir el archivo que se encuentra en el subdirectorio `<entorno_local>\html`. La publicación se proporciona en varios idiomas. La tabla siguiente muestra el idioma y el nombre de archivo correspondiente:

Tabla 4. Resumen de idiomas y nombres de archivos

Idioma	Entorno local	Nombre del archivo HTML
Chino simplificado	zn_CN	amqyzb01.zip
Alemán	de_DE	amqygb01.zip
Japonés	ja_JP	amqyjb01.zip
Coreano	ko_KR	amqykb01.zip
Portugués de Brasil	pt_BR	amqybb01.zip
Español	es_ES	amqysb01.zip
Inglés americano	en_US	amqyab01.zip

Los PDF traducidos se pueden bajar desde el siguiente URL:

`http://www.ibm.com/webspheremq/downloads`

Está disponible en los siguientes idiomas:

Tabla 5. Idiomas y nombres de los archivos PDF

Idioma	Entorno local	Nombre del archivo PDF
Chino simplificado	zn_CN	amqyzb01.pdf
Alemán	de_DE	amqygb01.pdf
Japonés	ja_JP	amqyjb01.pdf
Coreano	ko_KR	amqykb01.pdf
Portugués de Brasil	pt_BR	amqybb01.pdf
Español	es_ES	amqysb01.pdf
Inglés americano	en_US	amqyab01.pdf

También le resultarán útiles las publicaciones siguientes:

- *WebSphere MQ Intercommunication*, SC34-6059
- *Guía de administración del sistema*, SC10-3802
- *WebSphere MQ Clientes*, GC10-3795
- *WebSphere MQ Queue Manager Clusters*, SC34-6061

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/webspheremq/library`

Índice

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.