MS81: WebSphere® MQ internet pass-thru Versão 1.2

S517-7421-00

Nota!
Antes de utilizar este manual e o produto a que se refere, certifique-se de ler as informações gerais em "Avisos" na página vii.

Primeira Edição, Março de 2002

Esta edição se aplica a Versão 1.2 do MS81: WebSphere MQ internet pass-thru (número de programa 5639-L92) e a todos os releases e modificações subseqüentes, até que seja indicado de outra maneira em novas edições.

Índice

Figuras

Avisos

O parágrafo a seguir não se aplica a nenhum país onde tais disposições não estejam de acordo com a legislação local.

INTERNATIONAL BUSINESS MACHINES CORPORATION FORNECE ESTA PUBLICAÇÃO "NO ESTADO EM QUE SE ENCONTRA" SEM GARANTIA DE ESPÉCIE ALGUMA, EXPLÍCITA OU IMPLÍCITA, INCLUINDO, MAS NÃO SE LIMITANDO ÀS GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO OU ADEQUAÇÃO A UM FIM ESPECÍFICO. Alguns países não permitem a exclusão de garantias expressas ou implícitas em certas transações; portanto, esta disposição pode não se aplicar ao Cliente.

Referências nesta publicação a produtos, programas ou serviços IBM não significam que a IBM pretende torná-los disponíveis em todos os países onde opera.

Qualquer referência nesta publicação a um programa licenciado da IBM ou outro produto da IBM não significa que apenas programas ou outros produtos da IBM possam ser utilizados. Qualquer programa funcionalmente equivalente, que não infrinja nenhum direito de propriedade intelectual, pode ser utilizado em substituição a este produto IBM. A avaliação e verificação da operação em conjunto com outros produtos, exceto aqueles expressamente designados pela IBM, são de inteira responsabilidade do Cliente.

A IBM pode ter patentes ou solicitações de patentes pendentes relativas a assuntos tratados nesta publicação. O fornecimento desta publicação não garante ao Cliente nenhum direito sobre tais patentes. Pedidos de licença devem ser enviados, por escrito, para Gerência de Relações Comerciais e Industriais da IBM Brasil, Av. Pasteur, 138-146, Botafogo, Rio de Janeiro, RJ, CEP 22290-240.

As informações contidas neste documento não foram submetidas a nenhum teste formal da IBM e são distribuídas NO ESTADO EM QUE SE ENCONTRAM. O uso das informações ou a implementação de qualquer uma destas técnicas é de inteira responsabilidade do Cliente, que deve avaliá-las e integrá-las ao ambiente operacional. Apesar de cada item ter sido revisado pela IBM quanto à exatidão em uma situação específica, não há garantia de que resultados iguais ou semelhantes sejam obtidos em outro lugar. A tentativa do Cliente em adaptar estas técnicas a seus próprios ambientes é por conta e risco do Cliente.

Marcas

Os termos a seguir são marcas da International Business Machines Corporation nos Estados Unidos e/ou em outros países:

AIX	FFST	First Failure Support Technology
IBM	IBMLink	MQSeries
SupportPac	WebSphere	

Microsoft, Windows, Windows NT e o logotipo do Windows são marcas da Microsoft Corporation nos Estados Unidos e/ou em outros países.

Outros nomes de empresas, produtos e serviços podem ser marcas ou marcas de serviço de terceiros.

Prefácio

O Que É internet pass-thru?

WebSphere MQ internet pass-thru era conhecimento anteriormente como MQSeries internet pass-thru. WebSphere MQ é o nome pelo qual o MQSeries será conhecido daqui em diante neste manual. Observe que nem todos os manuais MQSeries terão o nome alterado para WebSphere MQ imediatamente, ainda existirão referências a ambos, MQSeries e WebSphere MQ, durante algum tempo.

IBM® WebSphere MQ internet pass-thru:

- É uma extensão do produto base WebSphere MQ que pode ser utilizada para implementar soluções de mensagens entre sites remotos na Internet.
- Torna a passagem dos protocolos de canal do WebSphere MQ, dentro e fora de um firewall, mais simples e gerenciável, encapsulando os protocolos no HTTP ou agindo como um proxy.
- Opera como um serviço autônomo que pode receber e encaminhar fluxos de mensagens do WebSphere MQ. O sistema no qual ele é executado não precisa hospedar um gerenciador de filas do WebSphere MQ.
- Ajuda a fornecer transações business-to-business utilizando o WebSphere MQ.
- Ativa os aplicativos do WebSphere MQ existentes e inalterados para serem utilizados através de um firewall
- Fornece um ponto único de controle por meio do acesso a vários gerenciadores de filas.
- Permite a criptografia de todos os dados

Neste manual, para facilitar, WebSphere MQ internet pass-thru é freqüentemente designado como “MQIPT”.

A Quem se Destina Este Manual

Este manual destina-se a desenvolvedores de sistemas, administradores técnicos do WebSphere MQ e administradores de rede e firewall.

O Que É Preciso Saber para Entender Este Documento

Você deve ter um bom conhecimento sobre:

- Administração de gerenciadores de filas e canais de mensagens do WebSphere MQ, conforme descrito no *MQSeries System Administration* and *MQSeries Intercommunication*
- O modo como os firewalls são implementados
- Roteamento/rede do Internet Protocol
- O IBM Network Dispatcher para equilíbrio de carga e disponibilidade avançada.
- IBM WebSphere Application Server

Pré-Requisitos

Este release do internet pass-thru é executado nestas plataformas:

- Windows NT® V4.0, com Service pack 6
- Windows 2000
- Windows XP

- Sun Solaris
- AIX®
- HP-UX 11
- Linux

Nota: AIX e HP-UX estarão disponíveis quando o Java 1.4 for liberado nestas plataformas.

O JDK deve estar no nível 1.4.0 ou em um release compatível posterior.

O único protocolo de rede suportado é o TCP/IP.

A ajuda do Cliente Administrativo requer um navegador Netscape.

Informações de Acessibilidade

A GUI do Cliente Administrativo foi construída visando a acessibilidade. A execução de todas as funções disponíveis é feita diretamente, sem utilizar um mouse, utilizando os equivalentes do teclado. Você pode navegar pela tela utilizando tab, shift-tab, ctrl-tab e as teclas de cursor no modo padrão. O equivalente a pressionar botões pode ser realizado selecionando primeiro o botão e, em seguida, pressionando a tecla Enter.

As opções de menu podem ser acessadas por combinações das teclas tab e de cursor ou utilizando as teclas de aceleração, que estão disponíveis para todas as opções Por exemplo, a GUI pode ser fechada selecionando primeiro alt-f, em seguida, alt-q (Arquivo->Sair). Uma vez acessado, o item de menu pode ser ativado utilizando a tecla Enter.

Você pode navegar pela árvore utilizando as teclas de cursor. Em particular, as teclas de cursor para a direita e para a esquerda podem ser utilizadas para abrir ou fechar um nó do MQIPT, permitindo que as rotas sejam mostradas ou ocultadas.

As caixas de entrada selecionadas podem ter seus estados alterados utilizando a tecla de espaço. Os campos podem ser selecionados para edição utilizando-se a tecla Enter.

Aparência e Comportamento

O ideal é que a GUI adote a aparência e comportamento do ambiente. Como isso nem sempre é possível, você pode providenciar um arquivo de configuração para adaptar a aparência e comportamento da GUI às suas necessidades. O arquivo de configuração é chamado "custom.properties" e deve ser colocado no diretório `bin`.

Utilize este arquivo de configuração para configurar o seguinte:

- A cor do primeiro plano - a cor do texto
- A cor do plano de fundo
- A fonte do texto
- O estilo do texto - corrido, negrito, itálico ou negrito e itálico

Um arquivo de configuração de amostra "customSample.properties" foi fornecido, contendo comentários que mostram como ele pode ser alterado. Sugerimos que você copie o arquivo para `bin/custom.properties` e faça as alterações necessárias.

Bibliografia

Este manual está disponível em PDF e HTML como parte do produto instalado. Ele está instalado nos diretórios listados na Tabela 1. Antes de utilizar o Cliente Administrativo, você deve descompactar o arquivo localizado no subdiretório `<idioma>/html`.

- PDF

  `doc\<idioma>\pdf\<nomearquivo>.pdf`
- HTML (contido em um arquivo zip de auto-extração)

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

O manual foi produzido nos idiomas a seguir. Consulte a tabela abaixo para obter o idioma e o nome do arquivo correspondente:

Tabela 1. Resumo de idiomas e nomes de arquivo

Idioma	**Locale**	**Nome do arquivo PDF**	**Nome do arquivo HTML**
Chinês Simplificado	zn_CN	amqyzb00.pdf	amqyzb00.zip
Alemão	de_DE	amqygb00.pdf	amqygb00.zip
Japonês	ja_JP	amqyjb00.pdf	amqyjb00.zip
Coreano	ko_KR	amqykb00.pdf	amqykb00.zip
Português do Brasil	pt_BR	amqybb00.pdf	amqybb00.zip
Espanhol	es_ES	amqysb00.pdf	amqysb00.zip
Inglês dos Estados Unidos	en_US	amqyab00.pdf	amqyab00.zip

As seguintes publicações poderão ser úteis para você:

- *MQSeries Intercommunication*, SC33-1872
- *MQSeries System Administration*, SC33-1873
- *MQSeries Clients*, GC33-1632
- *MQSeries Queue Manager Clusters*, SC34-5349

Esses manuais fornecem informações sobre a definição dos canais do WebSphere MQ e seus atributos - em particular, a definição do CONNAME.

As publicações do WebSphere MQ estão disponíveis em:

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

Resumo das Alterações

Os aperfeiçoamentos nesta versão do WebSphere MQ internet pass-thru incluem:

- Configurações de exemplo
- Rastreio do SSL melhorado
- Java Security Manager
- Utilitário KeyMan para gerenciar certificados SSL e arquivos do conjunto de chaves
- Suporte ao Linux, incluindo Qualidade de Serviço para mensagens do WebSphere MQ
- Imagem de instalação do NLS disponível em plataformas Windows
- Os nomes de propriedades agora fazem distinção entre maiúsculas e minúsculas
- Versão de servlet
- Suporte ao cliente e servidor do Socks
- Modo proxy do SSL
- Status de luz tráfego para o Cliente Administrativo
- Suporte a clusters do WebSphere MQ

Capítulo 1. Introdução ao WebSphere MQ internet pass-thru

O WebSphere MQ internet pass-thru é uma extensão do produto WebSphere MQ base. O MQIPT é executado como um serviço autônomo que pode receber e encaminhar fluxos de mensagens do WebSphere MQ, entre dois gerenciadores de filas do WebSphere MQ ou entre um cliente do WebSphere MQ e um gerenciador de filas do WebSphere MQ. O MQIPT ativa esta conexão quando o cliente e o servidor não estão na mesma rede física.

Um ou mais MQIPTs pode ser colocados no caminho de comunicação entre dois gerenciadores de filas do WebSphere MQ, ou entre um cliente do WebSphere MQ e um gerenciador de filas do WebSphere MQ. Os MQIPTs permitem que os dois sistemas do WebSphere MQ troquem mensagens sem uma conexão TCP/IP direta entre os dois sistemas. Isso é útil se a configuração do firewall proíbe uma conexão TCP/IP direta entre os dois sistemas.

O MQIPT atende em uma ou mais portas TCP/IP a conexões de entrada, que podem transportar mensagens normais do WebSphere MQ, mensagens do WebSphere MQ encapsuladas no HTTP ou criptografadas utilizando o SSL (Secure Sockets Layer). Ele pode manipular várias conexões simultâneas.

O canal do WebSphere MQ que faz o pedido inicial de conexão TCP/IP é referido como “originador da chamada”, o canal ao qual ele está tentando se conectar como “respondedor” e o gerenciador de filas que ele está tentando contatar por último como “gerenciador de filas de destino”.

As utilizações do MQIPT previstas são:

- O MQIPT pode ser utilizado como um concentrador de canais, para que os canais de/para vários hosts separados possam aparecer para um firewall como se fossem todos de/para o host do MQIPT. Isso torna mais fácil definir e gerenciar as regras de filtragem do firewall.

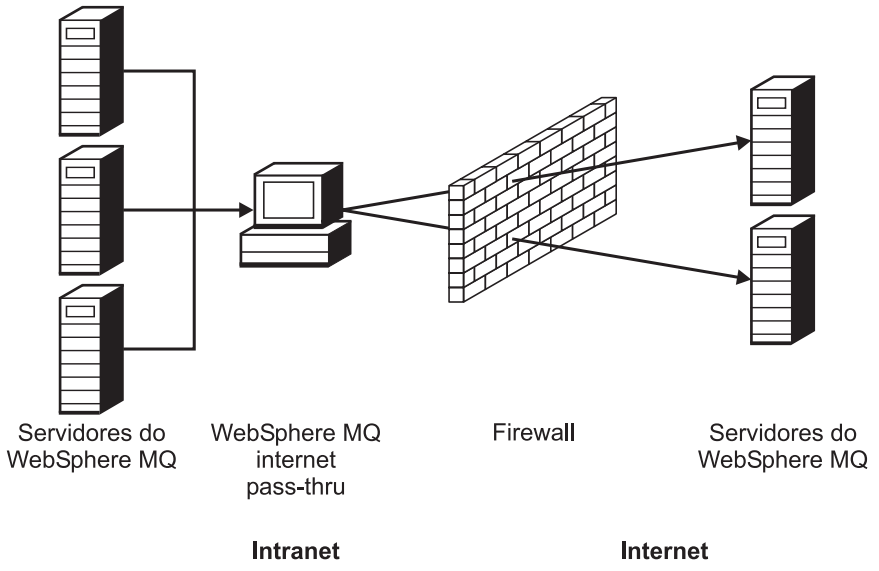

Figura 1. Exemplo do MQIPT como um concentrador de canais

- Se o MQIPT for colocado na DMZ (“zona desmilitarizada”) do firewall, em uma máquina com um endereço IP (Internet Protocol) conhecido e confiável, o MQIPT poderá ser utilizado para atender a conexões de entrada do canal do WebSphere MQ que ele pode encaminhar para a intranet confiável; o firewall interno deve permitir que esta máquina confiável faça conexões de recepção. Nesta configuração, o MQIPT impede que pedidos externos de acesso vejam os endereços IP reais das máquinas na intranet confiável. Portanto, o MQIPT fornece um único ponto de acesso.

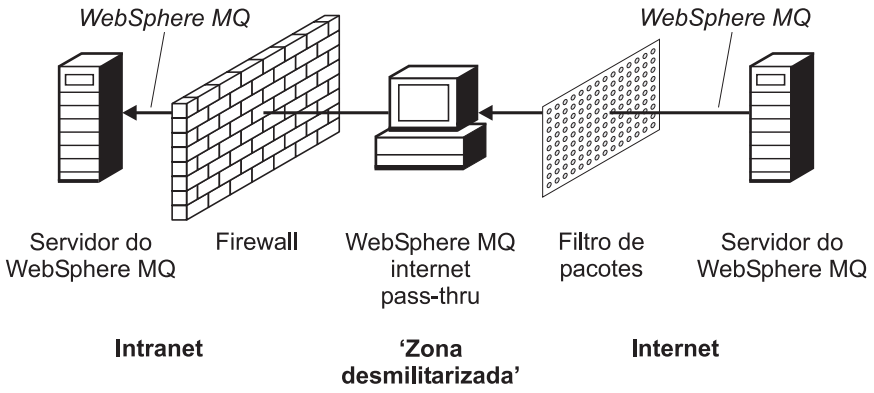

Figura 2. Exemplo do MQIPT com uma “zona desmilitarizada”

- Se dois MQIPTs forem implementados em linha, eles poderão se comunicar utilizando HTTP ou SSL. O recurso de encapsulamento HTTP permite que os pedidos sejam transmitidos através de firewalls, utilizando os proxies HTTP existentes. O primeiro MQIPT insere o protocolo do WebSphere MQ no HTTP e o segundo extrai o protocolo do WebSphere MQ de seu wrapper HTTP e o encaminha para o gerenciador de filas de destino.

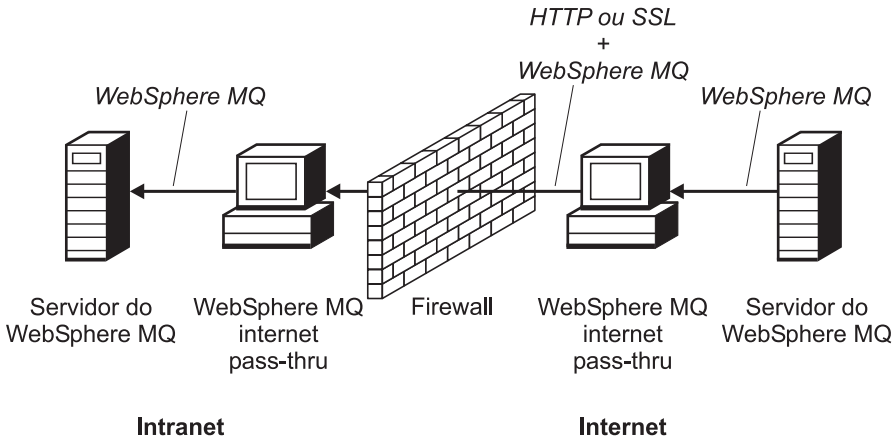

Figura 3. Exemplo de encapsulamento do MQIPT e do HTTP

- De modo semelhante, os pedidos podem ser criptografados antes da transmissão por firewalls. O primeiro MQIPT criptografa os dados e o segundo decriptografa-os utilizando o SSL, antes de enviá-los para o gerenciador de filas de destino.

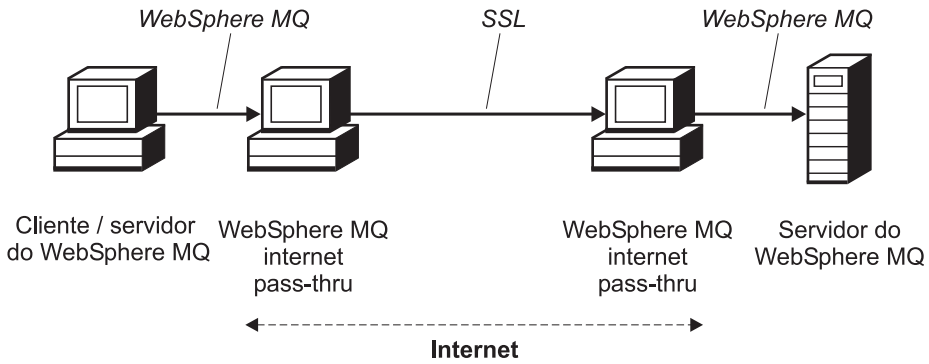

Figura 4. Exemplo do MQIPT e do SSL

O MQIPT armazena os dados na memória enquanto os encaminha da origem para o destino. Os dados não são salvos em disco (exceto para a página paginada em disco pelo sistema operacional). A única vez que o MQIPT acessa o disco explicitamente é para ler seu arquivo de configuração e para gravar registros de log e de rastreio.

O intervalo completo dos tipos de canais do WebSphere MQ pode ser determinado por um ou mais MQIPTs. A presença de MQIPTs em um caminho de comunicação não tem efeito sobre as características funcionais dos componentes do WebSphere MQ conectados, mas pode haver algum impacto sobre o desempenho da transferência de mensagens.

O MQIPT pode ser utilizado juntamente com o WebSphere MQ Publish/Subscribe ou com o intermediário de mensagens WebSphere MQ Integrator.

A Figura 5 na página 4 mostra todas as configurações possíveis para MQIPTs em uma topologia do WebSphere MQ. Na figura, observe que o proxy HTTP, o proxy SOCKS e as máquinas do MQIPT que estão do outro lado do firewall, no lado "Conexões de transmissão", representam a possibilidade do encadeamento de várias máquinas juntas na internet. Por exemplo, uma máquina do MQIPT poderia se comunicar através de uma ou máquinas de proxies SOCKS ou HTTP, ou máquinas do MQIPT adicionais, antes de chegar ao seu destino.

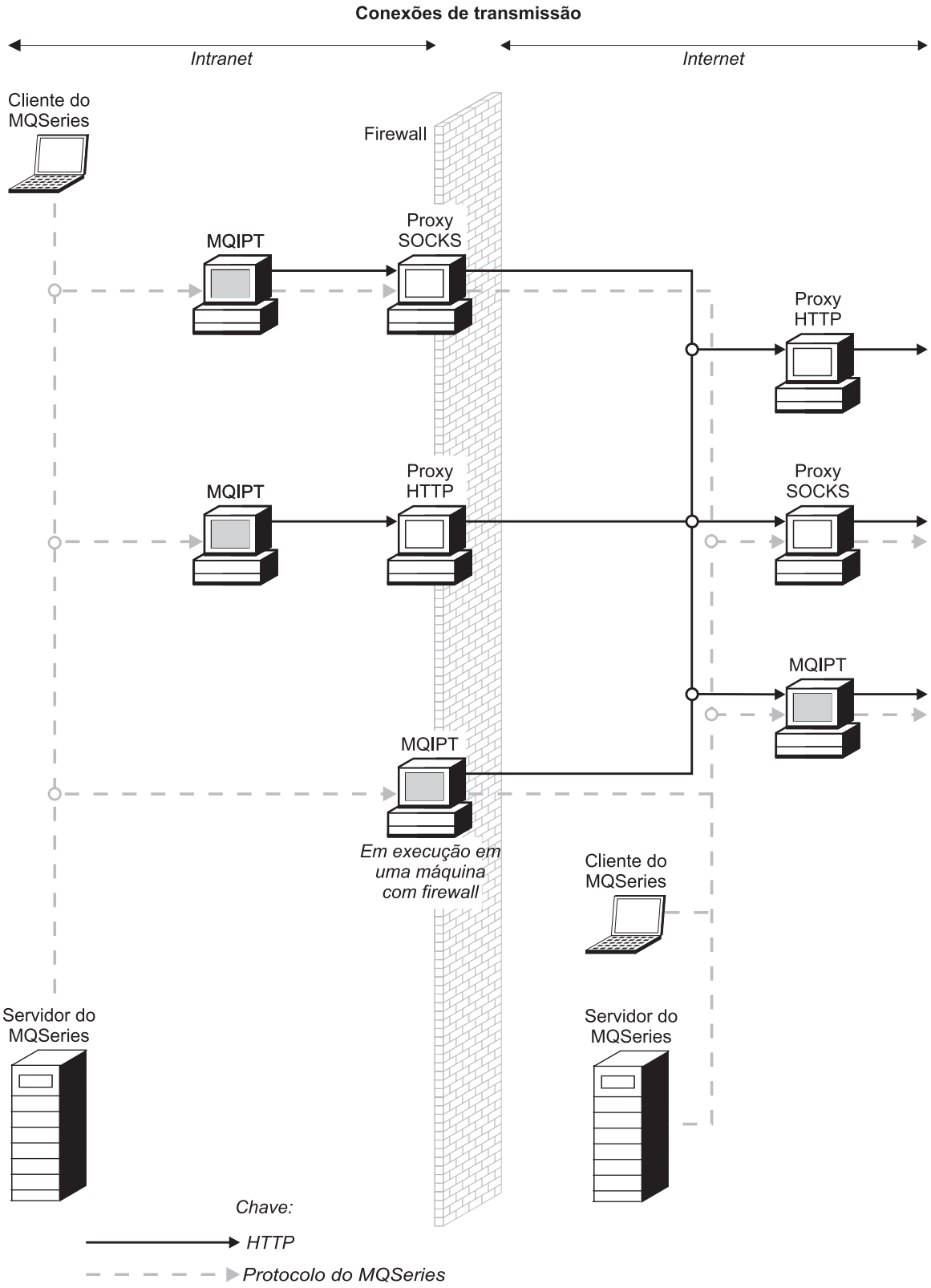

Figura 5. Topologia do WebSphere MQ mostrando as configurações do MQIPT possíveis (Parte 1 de 2)

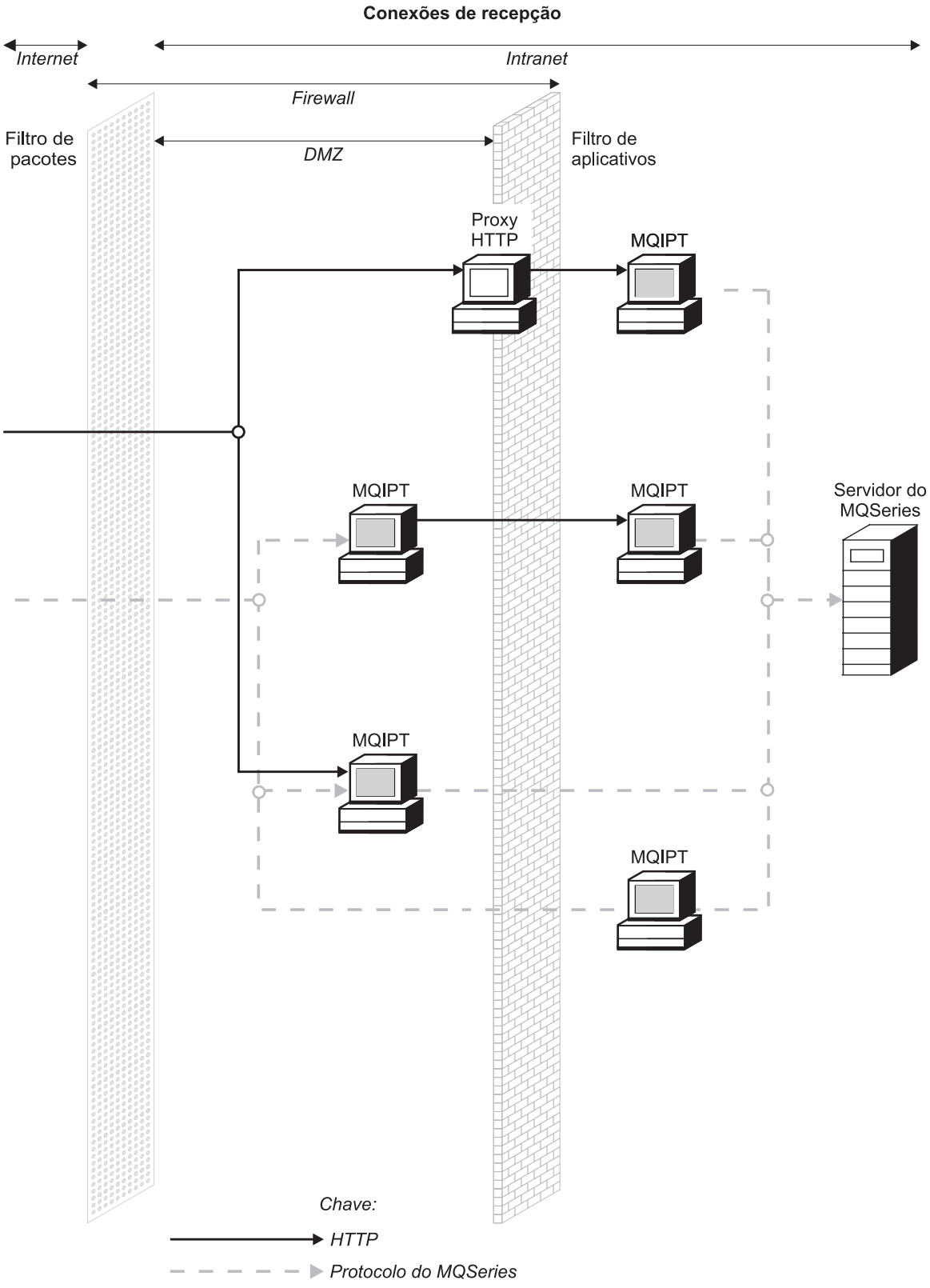

Figura 5. Topologia do WebSphere MQ mostrando as configurações do MQIPT possíveis (Parte 2 de 2)

Capítulo 2. Como Funciona o internet pass-thru

Este capítulo fornece uma visão geral de como o internet pass-thru funciona e, em seguida, descreve os seguintes itens com mais detalhes:

Visão Geral de Como Funciona do internet pass-thru

Em sua configuração mais simples, o MQIPT age como um encaminhador de protocolo do WebSphere MQ. Ele atende em uma porta TCP/IP e aceita pedidos de conexão de canais do WebSphere MQ. Se um pedido bem formado é recebido, o MQIPT estabelece uma conexão TCP/IP adicional entre si mesmo e o gerenciador de filas de destino do WebSphere MQ. Em seguida, ele transmite todos os pacotes de protocolo que recebe de sua conexão de entrada para o gerenciador de filas de destino e retorna os pacotes de protocolo do gerenciador de filas de destino para a conexão de entrada original.

Nenhuma alteração no protocolo do WebSphere MQ (cliente /servidor ou gerenciador de filas para gerenciador de filas) é envolvida - porque nenhuma extremidade está diretamente ciente da presença do intermediário - portanto, não são necessárias novas versões do código de cliente ou servidor do WebSphere MQ.

Para utilizar o MQIPT, o canal do originador da chamada deve ser configurado para utilizar o nome do host e a porta do MQIPT', não o nome do host e a porta do gerenciador de filas de destino. Isso é definido com a propriedade CONNAME do canal do WebSphere MQ. O MQIPT não examina o nome do canal; ele é simplesmente passado para o gerenciador de filas de destino. Outros campos de configuração, como ID de usuário e senha em um canal cliente /servidor, são passados de modo semelhante para o gerenciador de filas de destino.

O MQIPT pode ser utilizado para permitir o acesso a um ou mais gerenciadores de filas de destino. Para que isso funcione, deve haver um mecanismo para indicar ao MQIPT com qual gerenciador de filas será feita a conexão, portanto, o MQIPT utiliza o número da porta TCP/IP de destino para determinar isso, conforme descrito no parágrafo seguinte.

Para permitir o acesso a mais de um gerenciador de filas de destino, o MQIPT pode ser configurado para atender em várias portas TCP/IP. Cada porta de atendimento é mapeada para um gerenciador de filas de destino através de uma "rota" do MQIPT. O administrador do MQIPT pode definir até 100 dessas rotas, que associam uma porta TCP/IP de atendimento ao nome do host e porta do gerenciador de filas de destino. Isso significa que o nome do host (endereço IP) do gerenciador de filas de destino nunca fica visível para o canal de origem. Cada rota pode manipular várias conexões entre sua porta de atendimento e o destino, cada conexão agindo independentemente.

Suporte ao HTTP

Como uma opção, o MQIPT pode ser configurado para que os pacotes de dados que ele encaminha sejam codificados como pedidos HTTP. O MQIPT suporta o encapsulamento HTTP com ou sem fragmentação.

Como os canais do WebSphere MQ não aceitam atualmente pedidos HTTP, um segundo MQIPT é necessário para receber os pedidos HTTP e convertê-los de volta para os pacotes de protocolo normais do WebSphere MQ. O segundo MQIPT retira o cabeçalho HTTP para converter o pacote de entrada para um pacote de protocolo padrão do WebSphere MQ, antes de transmiti-lo para o gerenciador de filas de destino.

Ao utilizar o encapsulamento HTTP sem fragmentação, uma resposta do HTTP é enviada para o primeiro MQIPT de cada pedido HTTP. Esta resposta pode ser a do gerenciador de filas de destino ou uma confirmação fictícia. Se o sistema do WebSphere MQ tiver que enviar uma cadeia de pacotes de protocolo sucessivos do WebSphere MQ (como ocorre ao transferir uma mensagem grande), vários pares de pedido/resposta HTTP são utilizados para transferir os dados. Para conseguir isso, o MQIPT insere os fluxos de pedido ou resposta adicionais.

Ao utilizar o encapsulamento HTTP com fragmentação, apenas o primeiro pacote é agrupado em um cabeçalho HTTP. Os pacotes do meio e final possuem cabeçalhos de fragmentação. Essa disposição remove a espera de uma confirmação fictícia do segundo MQIPT e, portanto, oferece desempenho um pouco melhor que aquele fornecido pelo encapsulamento HTTP sem fragmentação.

Quando o HTTP estiver sendo utilizado entre dois MQIPTs, a conexão TCP/IP na qual os pedidos e respostas HTTP fluem é persistente e é mantida aberta pelo tempo de duração do canal de mensagem. Os MQIPTs não fecham a conexão TCP/IP entre os pares de pedido/resposta.

Se dois MQIPTs estiverem se comunicando através de HTTP, é possível que um pedido HTTP possa ficar pendente durante um longo período. Um exemplo disso é um canal solicitador/servidor, quando o lado do servidor está aguardando a chegada de novas mensagens em sua fila de transmissão. O protocolo de canal do WebSphere MQ fornece um mecanismo de "pulsação", que requer que a espera seja encerrada periodicamente para enviar mensagens de pulsação para seu parceiro (o período de pulsação padrão do canal é 5 minutos) e o MQIPT utiliza essa pulsação como a resposta HTTP. Não desative esta pulsação do canal ou defina-a para um valor excessivamente alto, para evitar problemas com tempos limite em alguns firewalls.

Alguns proxies HTTP têm suas próprias propriedades para controlar conexões persistentes, por exemplo, o número de pedidos que podem ser feitos em uma

conexão persistente. O proxy HTTP também deve suportar o protocolo HTTP 1.1. Quando o IBM WebSphere Caching Proxy é utilizado, as seguintes propriedades devem ser redefinidas:

- MaxPersistenceRequest definido para um valor alto (por exemplo, 5000)
- PersistentTimeout definido para um valor alto (por exemplo, 12 horas)
- ProxyPersistence definido para `on`

Suporte ao SOCKS

Ao fazer conexões de transmissão através de um firewall, um aplicativo pode ser ativado para SOCKS, para que todas as conexões sejam feitas através de um proxy SOCKS e, desse modo, ativando um ponto de controle de saída através do firewall.

Em releases anteriores do MQIPT, o SOCKS era suportado definindo as propriedades `SocksProxyHost` e `SocksProxyPort` do sistema Java, que afetavam todas as conexões feitas pelo MQIPT e todas as rotas eram forçadas a utilizar o mesmo proxy SOCKS. Neste release do MQIPT, o suporte ao SOCKS V5 foi implementado, mas com suporte apenas para endereços no formato IPV4 e em autenticação de usuário.

Cada rota pode ser configurada para se comunicar com um proxy SOCKS diferente, utilizando as propriedades `SocksClient`, `SocksProxy` e `SocksProxyPort`.

Cada rota também pode ser ativada para agir como um servidor SOCKS (proxy), utilizando a propriedade `SocksServer` e, desse modo, permitindo que um aplicativo do WebSphere MQ ativado para socks seja conectado através do MQIPT ao seu destino. Ao utilizar este recurso, o destino e a porta de destino são obtidos durante o protocolo de reconhecimento Socks, portanto, as propriedades `Destination` e `DestinationPort` definidas na rota são ignoradas. Este é um recurso chave para suportar o clustering do WebSphere MQ. Consulte “Clustering” na página 20 para obter mais informações sobre como utilizar o MQIPT com o clustering do WebSphere MQ.

Suporte ao SSL

O protocolo SSL fornece segurança de conexão através de canais de comunicação incertos e assegura:

Privacidade de comunicação
A conexão pode se tornar privada; por exemplo, criptografando os dados a serem trocados entre o cliente e o servidor, apenas eles têm conhecimento dos dados. Isso permite a transferência segura de informações privadas, tais como números de cartão de crédito.

Integridade de comunicação
A conexão é confiável. O transporte de mensagem inclui uma verificação de integridade de mensagem com base em uma função hash segura.

Autenticação
O cliente pode autenticar o servidor e um servidor autenticado pode autenticar o cliente. Isso garante que as informações sejam trocadas apenas entre as partes tencionadas. O mecanismo de autenticação baseia-se na troca de certificados digitais (certificados X.509v3).

O protocolo SSL pode utilizar algoritmos de assinatura digital diferentes para a autenticação das partes de comunicação. As operações criptográficas utilizadas no SSL, a criptografia para confidencialidade de dados e o hash seguro para

integridade da mensagem contam com o compartilhamento de chaves secretas entre o cliente e o servidor. O SSL fornece vários mecanismos de troca de chave que permitem o compartilhamento de chaves secretas. O SSL pode utilizar uma variedade de algoritmos para criptografia e hash. Vários algoritmos criptográficos são suportados; você os especifica utilizando conjuntos de cifras SSL. Estes conjuntos de cifras são suportados:

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

Protocolo de Reconhecimento SSL

O processo do protocolo de reconhecimento SSL ocorre durante o pedido de conexão inicial entre o cliente e servidor SSL, quando a autenticação e negociação dos conjuntos de cifras são suportadas.

Todos os conjuntos de cifras do SSL listados acima, com exceção dos conjuntos de cifras anônimos, requerem a autenticação de servidor e permitem a autenticação de cliente: o servidor pode ser configurado para solicitar a autenticação de cliente. A autenticação peer da comunicação no SSL baseia-se na criptografia de chave pública e em certificados digitais X.509v3. Um site que deve ser autenticado no protocolo SSL precisa de uma chave privada e um certificado digital que contém a chave pública correspondente juntamente com as informações sobre a identidade do site e o tempo de validade do certificado. Os certificados são assinados por uma Autoridade de Certificação; os certificados dessas autoridades são denominados certificados de signatário. Um certificado seguido por um ou mais certificados de signatário constituem uma cadeia de certificados. Uma cadeia de certificados é caracterizada pelo fato de que, iniciando a partir do primeiro primeiro certificado (certificado de site), a assinatura de cada certificado na cadeia pode ser verificada utilizando-se a chave pública contida no certificado de signatário seguinte.

Quando uma conexão segura que requer autenticação do servidor está sendo estabelecida, o servidor envia para o cliente uma cadeia de certificados para provar sua identidade. O cliente SSL prosseguirá estabelecendo a conexão com o servidor apenas se puder autenticar o servidor, por exemplo, verificar a assinatura do certificado do site do servidor. Para verificar essa assinatura, o cliente SSL precisa confiar no próprio site do servidor ou pelo menos em um dos signatários da cadeia de certificados fornecida pelo servidor. Os certificados dos sites e signatários confiáveis devem ser mantidos no lado do cliente para executar esta verificação.

O cliente SSL inspeciona a cadeia de certificados do servidor, iniciando com o certificado de site e considera a assinatura do certificado de sites como válida se o certificado de site estiver no repositório de sites ou signatários confiáveis, ou se um certificado de signatário na cadeia puder ser validado com base em seu repositório de certificados de signatário confiáveis. No último caso, o cliente SSL verifica se a cadeia de certificados está corretamente assinada, do certificado de signatário confiável ao certificado de site do servidor. Cada certificado envolvido neste processo também é examinado quanto a exatidão do formato e datas de validade. Se uma das verificações falhar, a conexão com o servidor será recusada. Depois de verificar o certificado de servidor, o cliente utiliza a chave pública incorporada nesse certificado nas etapas seguintes do protocolo SSL. A conexão SSL só poderá ser estabelecida se o servidor realmente tiver a chave privada correspondente.

A autenticação de cliente segue o mesmo procedimento: se um servidor SSL precisar de autenticação de cliente, o cliente enviará uma cadeia de certificados para o servidor para provar sua identidade e o servidor verificará essa cadeia com base em seu repositório de certificados de site e signatário confiáveis. Depois de verificar o certificado do cliente, o servidor utiliza a chave pública incorporada nesse certificado nas etapas seguintes do protocolo SSL. A conexão SSL só poderá ser estabelecida se o cliente realmente tiver a chave privada correspondente.

O próprio protocolo SSL fornece segurança de comunicação bem alta. No entanto, o protocolo opera com base nas informações fornecidas pelo aplicativo. Somente se essa base de informações também for mantida seguramente, a finalidade global de comunicação segurança poderá ser completada com êxito. Por exemplo, se o repositório de certificados de site e signatário confiáveis estiver comprometido, você poderá estabelecer uma conexão segura com um parceiro de comunicação muito inseguro.

MQIPT e SSL

O SSL V3.0 foi implementado, utilizando tokens PKCS (Public Key Cryptography Standards) #12 armazenados em arquivos de conjunto de chaves (com tipos de arquivo .p12 ou .pfx), contendo certificados X509.V3.

Um MQIPT pode agir como um cliente SSL ou um servidor SSL, dependendo de qual extremidade inicia a conexão. O cliente inicia uma conexão e o servidor aceita o pedido de conexão. É possível para uma rota do MQIPT agir como um cliente e um servidor, embora, neste exemplo, o uso do recurso Modo de Proxy SSL seja recomendado por razões de desempenho. Cada rota do MQIPT pode ser configurada independentemente com seu próprio conjunto de propriedades SSL. Consulte “Informações de Referência da Seção Route” na página 57 para obter mais detalhes.

Definições de Confiança

Um arquivo de conjunto de chaves contém um certificado pessoal que inclui o certificado de signatário ou cadeia de certificados de signatário. Para ativar a autenticação quando uma conexão está sendo feita, um certificado precisa de uma definição de confiança. Há dois níveis de confiança:

Confiança como peer
Significa que apenas este certificado pode ser confiável, mas não qualquer certificado assinado por este certificado.

Confiança como CA (Autoridade de Certificação)
Significa que qualquer certificado assinado por este certificado pode ser confiável.

O arquivo de conjunto de chaves no lado do servidor SSL, identificado pela propriedade SSLServerKeyRing, deve conter seu certificado pessoal. Um segundo arquivo de conjunto de chaves, identificado pela propriedade SSLServerCAKeyRing, deve conter quaisquer certificados confiáveis (CA ou peer). O arquivo de conjunto de chaves no lado do cliente SSL, identificado pela propriedade SSLClientKeyRing, contém seu certificado pessoal. Um segundo arquivo de conjunto de chaves, identificado pela propriedade SSLClientCAKeyRing, deve conter quaisquer certificados confiáveis (CA ou peer). Um arquivo de conjunto de chaves também pode conter uma lista de CRLs (Listas de Revogações de Certificado).

Você também pode utilizar certificados auto-assinados semelhantes àqueles no arquivo de conjunto de chaves de amostra (sslSample.pfx) fornecido com o MQIPT.

Um utilitário, KeyMan, (encontrado no subdiretório ssl) pode ser utilizado para criar certificados auto-assinados, gerenciar certificados e arquivos de conjunto de chaves. Para obter mais informações, consulte “KeyMan” na página 15.

Você deve proteger quaisquer arquivos de conjunto de chaves e de senha utilizando os recursos de segurança do sistema operacional para impedir o acesso não autorizado a eles.

Testando o SSL

O Capítulo 10, “Iniciando o internet pass-thru” na página 67 descreve as tarefas que podem ser utilizadas para testar uma conexão SSL.

Os certificados e as tecnologias de gerenciamento de certificados estão disponíveis a partir de uma série de fornecedores, incluindo:

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

Mensagens de Erro do SSL

Os códigos de erro a seguir podem ser vistos em um SSLRuntimeException, se um valor de parâmetro inválido for utilizado em uma das chamadas de método do SSL ou dados incorretos forem fornecidos para o protocolo SSL.

Tabela 2. Mensagens de erro de SSLRuntimeException

ID	Descrição
1	Uso incorreto de um método ou um ou mais parâmetros de entrada estão fora dos limites
2	Os dados fornecidos não podem ser processados
3	A assinatura dos dados fornecidos não pode ser verificada
10	O nome do assunto do certificado de signatário não corresponde ao nome do emissor do certificado
11	O tipo de um certificado não é suportado
12	Um certificado é utilizado antes de seu período de validade
13	Um certificado está expirado
14	Uma assinatura de certificado não pode ser verificada
15	Um certificado não pode ser utilizado

Tabela 2. Mensagens de erro de SSLRuntimeException (continuação)

20	Nenhum dos conjuntos de cifras apresentados pelo cliente é suportado pelo servidor
21	Nenhum dos métodos de compactação apresentados pelo cliente é suportado pelo servidor
22	Não há certificado disponível
23	Um algoritmo ou tipo de formato não é suportado
24	Rejeição de informações obsoletas
25	Um certificado é revogado
26	Um conjunto de CRLs está incompleto (algumas CRLs delta estão ausentes)
27	O nome a ser certificado já existe
28	A chave pública a ser certificada já existe
29	Algum número de série ou chave (certificado, CRL) está incorreto

Uma SSLException é lançada se a exceção do protocolo de reconhecimento SSL for finalizada.

Tabela 3. Mensagens de erro de SSLException

ID	**Descrição**
3	O tempo limite de conexão definido no SSLContext está expirado e nenhuma resposta foi recebida do peer
4	A conexão foi abortada pelo peer durante o protocolo de reconhecimento SSL, sem indicação de erro adicional
10	Uma mensagem inesperada foi recebida
20	Recebida uma mensagem com um registro MAC inválido
30	Falha de descompactação
40	Falha do protocolo de reconhecimento
41	Nenhum certificado foi enviado pelo peer
42	Um certificado inválido foi recebido
43	Um certificado não suportado foi recebido
44	Um certificado revogado foi recebido
45	Um certificado expirado foi recebido
46	Um certificado desconhecido foi recebido
47	Um parâmetro inválido foi detectado

QoS (Qualidade de Serviço)

O IBM WebSphere Edge Server fornece uma solução de gerenciamento de largura de banda através do plug-in Qualidade de Serviço Transacional na plataforma Linux. O TQoS (Qualidade de Serviço Transacional) refere-se ao serviço global, em termos de elementos, como rendimento e atributo, que são fornecidos para usuários da rede. Os atributos podem ser definidos para assegurar uma qualidade de serviço associada a quaisquer dados de saída enviados juntos com uma conexão. Isso permite que o administrador de política defina regras que identificam o tráfego relacionado a servidores específicos e ações de política com controles de serviço diferenciados exclusivos para este tráfego. Por exemplo, uma instalação pode definir uma política que especifica o tratamento preferencial do tráfego de saída relacionado ao tráfego do servidor no suporte de uma venda de

uma determinada quantidade de mercadorias, e não ao tráfego do servidor no suporte de uma navegação do cliente. O MQIPT requer apenas que o pagent (Policy Agent) seja instalado e em execução para implementar uma QoS (Qualidade de Serviço).

As políticas da TQoS são definidas em um arquivo de configuração de política (`pagent.conf`) ou utilizando um servidor LDAP. O pagent da TQoS pode acessar o arquivo de configuração da política ou ir para um servidor LDAP, ou ambos, para recuperar as entradas de política da TQoS. O *IBM Edge Server Administration Guide* fornece mais informações sobre pagent; ele pode ser encontrado na seguinte URL:

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

Neste site, é possível exibir o HTML online ou fazer download da versão PDF, em qualquer um dos formatos que você possa procurar a TQoS.

Os detalhes sobre onde pode ser feito o download do WES com TQoS estão no Readme.txt do MQIPT.

O MQIPT é fornecido com uma biblioteca fictícia denominada `libmqiptqos.so`, localizada no subdiretório lib. Depois de instalar a TQoS, você deve editar o script mqipt no subdiretório bin e alterar a variável de ambiente LD_LIBRARY_PATH para apontar para o subdiretório lib do WES.

O MQIPT requer apenas que o pagent seja instalado e em execução para implementar uma QoS (Qualidade de Serviço).Utilizando o MQIPT, uma prioridade do aplicativo pode ser definida em uma rota para dados que fluem em cada direção e isso, portanto, afetará todos os canais que utilizam essa rota. A prioridade é definida utilizando as propriedades do MQIPT `QosToCaller` e `QosToDest` (consulte “Informações de Referência da Seção Route” na página 57 para obter mais informações) e os valores aqui utilizados devem corresponder a uma definição de política ApplicationPriority no arquivo de controle `pagent.conf`. Se o pagent não encontrar uma política correspondente, os dados não serão atribuídos a nenhuma prioridade. As alterações feitas em uma política não serão refletidas no MQIPT até que o pagent tenha sido iniciado novamente. Consulte “Configurando a QoS (Qualidade de Serviço)” na página 80 para obter mais informações sobre definições de política.

Servlet

Há agora uma versão de servlet do MQIPT (denominada MQIPTServlet) que pode ser implementada em um Servidor de Aplicativos. Ele funciona de um modo semelhante ao MQIPT ″normal″, porém age como se tivesse apenas uma rota. Um pedido de conexão de entrada para iniciar um canal do WebSphere MQ é manipulado por uma instância do MQIPTServlet e cada instância mantém uma conexão persistente com o gerenciador de filas de destino. Fluxos de dados subseqüentes são mantidos ao longo do mesmo canal, utilizando o ID de sessão criado durante o primeiro pedido de conexão.

Um arquivo archive do aplicativo da Web, denominado `MQIPTServlet.war`, pode ser encontrado no subdiretório web. Esse war deve ser importado para o Servidor de Aplicativos.

A configuração do MQIPTServlet é obtida definindo propriedades no arquivo web.xml, que pode ser encontrado no subdiretório WEB-INF do Servidor de

Aplicativos. Apenas um subconjunto das propriedades do MQIPT existentes é aplicável ao MQIPTServlet . As seguintes propriedades podem ser utilizadas com o MQIPTServlet:

- ClientAccess
- ConnectionLog
- MaxLogfileSize
- QMgrAccess
- Trace

Os logs de conexão e os arquivos de rastreio são gravados em um diretório definido com uma nova propriedade denominada LogDir. Recomenda-se que esta propriedade seja definida antes de iniciar o MQIPTServlet.

Para controlar a quantidade de recursos utilizados pelo MQIPTServlet, você pode definir o número máximo de sessões ativas ou o número de instâncias do servlet dentro do Servidor de Aplicativos.

O MQIPTServlet foi testado com o IBM WebSphere Application Server 4.0, Tomcat 3.3 e Tomcat 4.0.

Consulte “Configurando o Servlet do MQIPT” na página 90 para obter uma configuração de exemplo.

KeyMan

Um utilitário autônomo, denominado KeyMan, é agora fornecido com o MQIPT para permitir o gerenciamento de certificados SSL e arquivos de conjunto de chaves. Um zip contendo o KeyMan pode ser encontrado no subdiretório ssl. Para instalar o KeyMan, descompacte o arquivo em um diretório temporário e siga as instruções encontradas no arquivo README.txt. O KeyMan possui vários recursos, mas o escopo desta seção é limitado à criação de certificados de teste e ao gerenciamento de arquivos de conjunto de chaves contendo tokens PKCS#12.

KeyMan é uma ferramenta de gerenciamento para o lado do cliente da PKI (public key infrastructure). O KeyMan gerencia chaves, certificados, CRLs (listas de revogações de certificados) e os respectivos repositórios para armazenar e recuperar esses itens. O ciclo de vida completo dos certificados é suportado e os processos são envolvidos no tratamento de certificados do usuário.

O KeyMan gerencia repositórios que contêm coleções de chaves, certificados e listas de revogação. Um repositório é chamado de token. Um token é constituído de definições de confiança para um aplicativo específico (por exemplo, MQIPT). Geralmente, um token contém chaves privadas e as cadeias de certificados associadas para autenticar um usuário para outros sites. Além disso, um token contém certificados de parceiros de comunicação confiáveis e CAs (autoridades de certificação).

Tipos de Token Suportados

O KeyMan suporta uma série de tipos diferentes de tokens. Os tokens são repositórios que contém chaves, certificados, CRLs e definições de confiança. Alguns tokens só podem armazenar um subconjunto destes tipos de item.

token PKCS#7
: Contém um conjunto de certificados e, opcionalmente, CRLs associadas. As chaves não podem ser armazenadas neste tipo de repositório. Este

repositório não requer autenticação. Os certificados e CRLs são protegidos por uma assinatura. No entanto, um adversário pode alterar o conjunto de itens armazenados em um token PKCS#7 específico. Este tipo de token é utilizado quando o conjunto esperado de itens é definido por algum contexto.

token PKCS#12
Contém chaves privadas, certificados e CRLs associadas. O conteúdo é protegido por uma frase-chave. Os itens públicos (certificados, CRLs) e os itens privados (chaves) podem ser protegidos por algoritmos com restrições diferentes.

repositórios PKCS#11 (CryptoKi)
PKCS#11 define uma interface para tokens criptográficos. Esses tokens podem armazenar chaves e certificados. O armazenamento de CRLs não é suportado. O acesso a um token é protegido por um PIN (número de identificação pessoal). Você tem que especificar o DLL do PKCS#11 específico do token que é utilizado pelo KeyMan para acessar o token.

O KeyMan suporta os DLLs do PKCS#11, versão 2.01 e 2.10.

PKCS#7 e PKCS#12 são tokens temporários e podem ser recuperados de mídias diferentes (por exemplo, arquivos, URI e área de transferência).

O KeyMan tem a capacidade especial para construir tokens PKCS#7 de dados com formato desconhecido. Ele varre os dados de certificados X.509 e CRLs e constrói um token PKCS#7 a partir dos certificados e CRLs detectados. Se tiver e-mails contendo certificados ou CRLs, você poderá abrir a pasta de e-mail no KeyMan, o qual tentará extrair os itens do X.509. Os dados não poderão ser armazenados novamente no formato original. Os dados extraídos poderão ser armazenados em um arquivo utilizando o formato PKCS#7.

Formatos de Dados Padrão Suportados

O KeyMan suporta uma série de formatos de dados padrão. Seguem descrições de seu significado e contexto de uso:

PKCS#7
Este formato de dados é uma coleção de certificados e CRLs. O conjunto de certificados e CRLs, conforme descrito pelo PKCS#7, não é protegido. No entanto, cada certificado e CRL individual é protegido por uma assinatura. O PKCS#7 é utilizado sempre que o conjunto esperado de certificados e CRLs é definido por algum contexto. Em sistemas Windows, os sufixos de arquivo padrão para arquivos do PKCS#7 são .p7r e .p7b.

PKCS#10
PKCS#10 define uma mensagem de pedido de certificado. Ele contém a chave pública e informações sobre o nome X.500 do solicitador. A mensagem é assinada com a chave privada correspondente. As mensagens do PKCS#10 podem ser geradas no formato binário e no formato ASCII protegido. A mensagem deve ser submetida a uma CA (autoridade de certificação).

PKCS#12
PKCS#12 é utilizado por navegadores e servidores Web para importar e exportar chaves privadas e certificados associados. O KeyMan pode ler e gravar esses arquivos do PKCS#12. Embora esses programas reconheçam apenas um perfil muito específico do PKCS#12, o KeyMan pode gerar arquivos do PKCS#12 mais gerais. O KeyMan pode armazenar conjuntos

de chaves privadas, certificados, CRLs e definições de confiança correspondentes em um único arquivo do PKCS#12. Os arquivos do PKCS#12 são protegidos por uma frase-chave. Geralmente, um token PKCS#12 contém a política de confiança para um determinado aplicativo. No caso do IBM BlueZ SSLite, as chaves e cadeias de certificados associadas serão utilizadas para autenticação de cliente/servidor. Outros certificados representam CAs confiáveis ou servidores confiáveis, dependendo das respectivas definições de confiança. Em sistemas Windows, os sufixos de arquivo padrão para arquivos do PKCS#12 são .p12 e .pfx.

SPKAC

SPKAC (SignedPublicKeyAndChallenge) é um formato de dados para solicitar certificados de uma CA. Esse formato específico é gerado pelo Netscape sempre que a marcação HTML <keygen> é utilizada. Ele contém a chave pública assinada e o desafio. Esse formato de dados pode ser gerado pelo KeyMan no formato binário e Base64.

Certificados X.509 V3

O KeyMan pode ler certificados X.509 V3 no formato binário ou agrupados em ASCII protegido. Esses arquivos podem ser abertos ou importados no KeyMan. Também é possível gravar certificados únicos de um token nesses dois formatos (**Certificate details -> Save Icon**). Em sistemas Windows, os sufixos de arquivo padrão para os arquivos de certificado X.509 são .crt, .cer e .der.

CRLs (Listas de Revogações de Certificado) do X.509 V2

O KeyMan pode ler CRLs do X.509 V2 no formato binário ou agrupadas em ASCII protegido. Um único CRL não pode ser aberto. O KeyMan só pode importar CRLs em tokens que já contêm o certificado de CA associado. É possível gravar CRLs únicas em formato binário ou ASCII protegido (**certificate details -> CRLs details -> Save Icon**). Em sistemas Windows, o sufixo de arquivo padrão para os arquivos de CRL do X.509 é .crl.

FAQs (Perguntas Mais Freqüentes) do KeyMan

Para perguntas gerais sobre criptografia e termos relacionados, consulte a RSA Laboratories e suas ″Perguntas Mais Freqüentes sobre a Criptografia Atual″. O FAQ a seguir abrange perguntas relacionadas ao KeyMan.

O KeyMan pode ler arquivos do PKCS#12 gerados pelo Netscape ou Internet Explorer?

Os arquivos do PKCS#12 gerados pelo navegador Netscape ou pelo Internet Explorer podem ser lidos pelo KeyMan desde que você conheça a senha que protege o conteúdo.

O KeyMan pode criar arquivos do PKCS#12 que podem ser lidos pelo Netscape ou Internet Explorer?

O padrão PKCS#12 oferece bastante liberdade para escolher algoritmos e organizar o conteúdo. Os navegadores aceitam apenas um perfil muito específico de todas as opções possíveis. O KeyMan pode gerar arquivos do PKCS#12 que podem ser lidos pelo Netscape e pelo Internet Explorer. Como o KeyMan permite que sejam feitas muitas coisas com o PKCS#12, você pode criar arquivos que não sejam reconhecidos por esses navegadores. O perfil comum para navegadores é semelhante a este: a criptografia pública/privada (consulte **Menu Options -> PKCS#12 Settings**) deve ser ″RC2 (40 bits)″/″DES (168 bits)″, respectivamente. Deve haver exatamente um certificado privado no token PKCS#12.

O que é certificado privado?

Se o KeyMan detecta uma chave e certificado correspondentes, ele combina esses dois itens em um certificado privado. Isso significa que, para qualquer certificado privado, você também possui a chave privada correspondente. Se você importar certificados para um token, o KeyMan verificará se há uma chave privada correspondente e combinará automaticamente a chave e o certificado importado em um certificado privado. Se isso ocorrer, o KeyMan irá notificá-lo com um diálogo.

O que é um certificado de CA ou peer?

Os certificados contidos em um token estabelecem confiança. Eles definem em quem você deve confiar. O significado de confiança e a avaliação exata dos certificados dependem do aplicativo que está utilizando o token. Com o KeyMan, você pode configurar dois tipos de confiança para os certificados: CA e peer. Se você confiar um certificado como CA, confiará implicitamente qualquer certificado, direta ou indiretamente assinado por esta CA. Se você definir o nível de confiança como "Peer", confiará apenas esse certificado específico. A confiança não é estendida para certificados assinados por um certificado "Peer".

Quais são os certificados que não são privados, CA ou peer?

O KeyMan tenta armazenar, para cada certificado privado, a cadeia completa até o certificado raiz. Esses certificados não precisam ser confiados e, portanto, não aparecerão entre os certificados de CA ou peer. Você pode encontrar esses certificados se selecionar o conjunto de chaves "All Certificate Items". Os certificados não-confiáveis não possuem um ícone.

O que é um token?

Um token é uma coleção de chaves, certificados e CRLs. Um token é armazenado em alguma mídia (por exemplo, um arquivo, uma URL, peça de hardware). Há diferentes tipos de tokens com diferentes capacidades: tokens de software, tokens de hardware, tokens desprotegidos e tokens protegidos por senhas ou PINs.

O que é conjunto de chaves?

Um token consiste em um conjunto de chaves. Um conjunto de chaves específico identifica um conjunto específico de itens (por exemplo, certificados do mesmo nível de confiança ou certificados para os quais você possui a chave privada, ou chaves sem certificados correspondentes).

Suporte ao Network Dispatcher

O MQIPT pode ser utilizado com o IBM Network Dispatcher para fornecer disponibilidade avançada e equilíbrio de carga, através de vários servidores, pelo uso de consultores personalizados. Esta seção assume que você esteja familiarizado com o Network Dispatcher e os consultores personalizados.

Dois consultores personalizados são fornecidos com o MQIPT; eles podem ser encontrados no subdiretório `lib`. Siga as instruções no *Network Dispatcher User's Guide* (GC31-8496) para instalar os consultores personalizados. A Figura 6 na página 19 mostra um exemplo da utilização do Network Dispatcher para monitorar o endereço de porta 1414 para o MQIPT. Observe que cada MQIPT deve ter o mesmo arquivo de configuração.

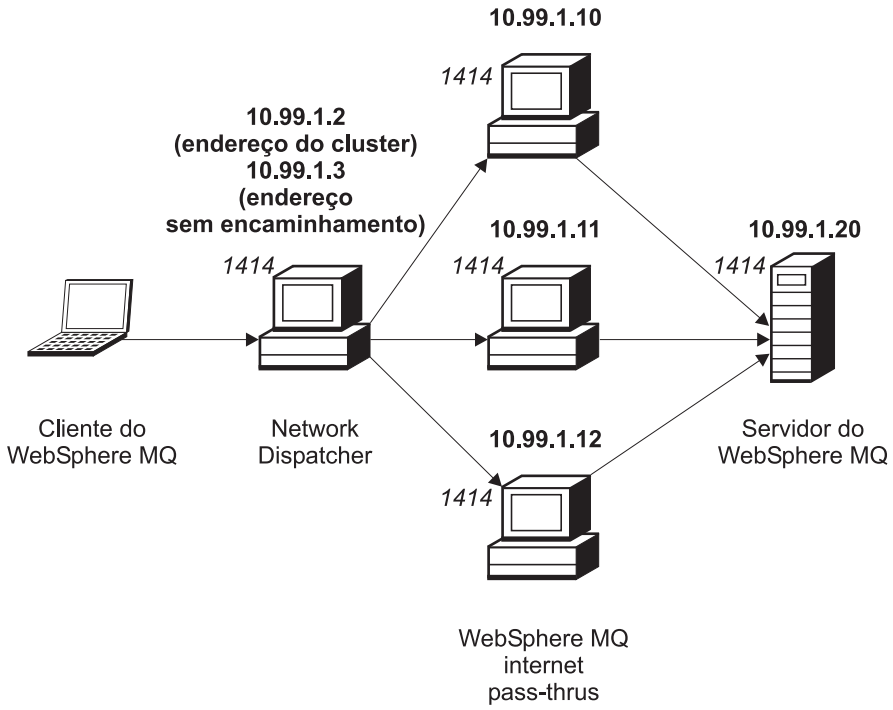

Figura 6. Utilizando o Network Dispatcher com o MQIPT

Siga as instruções no Capítulo 5 do *Network Dispatcher User's Guide* para configurar o componente do dispatcher para definir a porta 1414 e as máquinas de servidor com carga equilibrada. Você pode utilizar as opções de menu do Cliente Administrativo ou o comando de modo de linha "ndcontrol". Por exemplo:

```
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
```

A definição de rota no arquivo de configuração do MQIPT seria semelhante a este:

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

Você pode iniciar (e parar) um consultor personalizado apenas a partir da linha de comandos. Por exemplo:

```
ndcontrol advisor start mqipt_normal 1414
```

Este comando inicia o consultor do MQIPT no modo "normal", em que o consultor base executa suas próprias sincronizações para calcular os fatores ponderados de cada MQIPT. Para utilizar o consultor do MQIPT no modo "replace", inclua esta linha na definição de rota do MQIPT:

```
NDAdvisorReplaceMode=true
```

Você também deve iniciar o consultor personalizado `mqipt_replace` em vez de `mqipt_normal`. Por exemplo:

```
ndcontrol advisor start mqipt_replace 1414
```

Ao utilizar um consultor para monitorar uma porta do atendente de SSL (isto é, que possui `SSLServer=true` no arquivo de configuração `mqipt.conf`), você deve colocar um arquivo de "disparo" no diretório de trabalho do Network Dispatcher. O arquivo de "disparo" tem um nome específico, relacionando à rota que está sendo monitorada. Por exemplo, se a rota 1414 tiver `SSLServer=true`, um arquivo denominado `mqipt1414.ssl` deverá ser colocado no diretório `c:\winnt\system32` (no Windows NT). Consulte o arquivo `mqipt1414Sample.ssl` para obter mais informações.

Clustering

Os clusters do WebSphere MQ podem ser utilizados com o MQIPT, ativando para socks cada gerenciador de filas no cluster que estenda a internet e ativando o MQIPT para agir como proxy SOCKS. Como há muitas maneiras diferentes de configurar o gerenciador de filas em um cluster, a explicação a seguir baseia-se nas tarefas descritas no *MQSeries Queue Manager Clusters*, SC34-5349, Parte 1, Capítulo 3. O diagrama a seguir foi estendido daquele definido na Tarefa 2, "Incluindo um Novo Gerenciador de Filas no Cluster". NEWYORK e CHICAGO estão no cluster denominado HOME e ambos contêm repositórios completos. NEWYORK, LONDON e PARIS estão em outro cluster denominado INVENTORY. Observe que CHICAGO não precisa ser ativado para socks pois está em um cluster que não precisa de um MQIPT.

Cada gerenciador de filas no cluster INVENTORY é efetivamente "ocultado" atrás de um MQIPT. Como o gerenciador de filas foi ativado para socks, quando um canal cluster-emissor é iniciado, o pedido é enviado para seu destino, utilizando o MQIPT agindo como um proxy SOCKS. Normalmente, o CONNAME em um canal cluster-receptor é utilizado para identificar o gerenciador de filas local, mas na utilização com o MQIPT, o CONNAME deve identificar o MQIPT local e sua porta de atendente de entrada. No diagrama abaixo, todos os endereços da porta do atendente de entrada são 1414 e os endereços da porta do atendente de saída são 1415.

Há duas maneiras de executar um gerenciador de filas ativado para socks. A primeira é ativar para socks a máquina inteira na qual o gerenciador de filas está em execução. A segunda é ativar como socks apenas o gerenciador de filas. Utilizando qualquer um dos métodos, você deve configurar o cliente SOCKS, para que faça conexões remotas utilizando apenas o MQIPT como o proxy SOCKS, e desativar a autenticação do usuário. Há uma série de produtos no mercado para se conseguir o suporte ao SOCKS. Você deve escolher um que suporte o protocolo SOCKS V5. Consulte “Suporte ao SOCKS” na página 9 para obter mais informações do suporte ao Socks no MQIPT.

Consulte “Configurando o Suporte ao Clustering do MQIPT” na página 92 para um exemplo de como configurar uma rede de clusters.

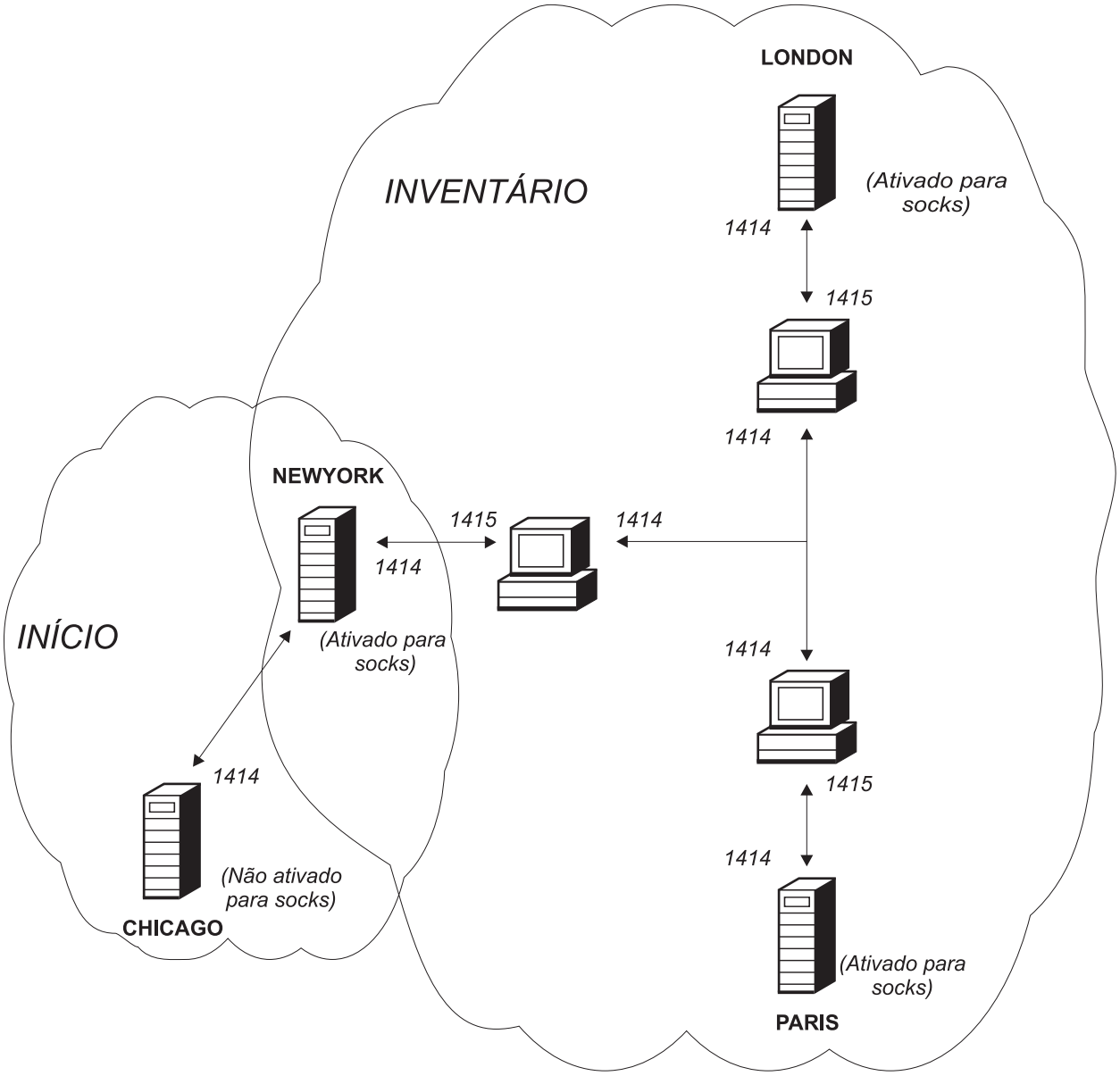

Figura 7. Suporte ao Clustering do MQIPT

Configurações de Canal Suportadas

Todos os tipos de canal do WebSphere MQ são suportados, mas a configuração é restrita a conexões TCP/IP. Para um cliente ou gerenciador de filas do WebSphere MQ, o MQIPT aparece como se fosse o gerenciador de filas de destino. Onde a configuração de canal requer um host de destino e número de porta, o nome do host do MQIPT e o número da porta do atendente são especificados.

Canais de cliente /servidor

O MQIPT atende a pedidos de conexão do cliente de entrada e, em seguida, os encaminha (utilizando o encapsulamento HTTP, o SSL ou os pacotes de protocolo padrão do WebSphere MQ). Se o MQIPT estiver utilizando o encapsulamento HTTP ou o SSL, ele os utilizará em uma conexão com um segundo MQIPT. Se não estiver utilizando o encapsulamento HTTP, ele os

encaminhará em uma conexão para o que vê como um gerenciador de filas de destino (mesmo que possa ser um MQIPT adicional). Assim que o gerenciador de filas de destino tiver aceito a conexão do cliente, os pacotes são retransmitidos entre o cliente e servidor.

Canais de emissor/receptor de cluster
Se o MQIPT recebe um pedido de entrada de um canal cluster-emissor, ele assume que o gerenciador de filas foi ativado para socks e o endereço de destino verdadeiro é obtido durante o processo de reconhecimento de protocolo SOCKS. Ele encaminha o pedido para o próximo MQIPT ou gerenciador de filas de destino exatamente da mesma maneira que para os canais de conexão do cliente. Isso também inclui os canais cluster-emissor auto-definidos.

Emissor/receptor
Se o MQIPT recebe um pedido de conexão de um canal do emissor, ele o encaminha para o próximo MQIPT ou gerenciador de filas de destino exatamente da mesma maneira que para os canais de conexão do cliente. O gerenciador de filas de destino valida o pedido de entrada e inicia o canal do receptor, se apropriado. Todas as comunicações entre o canal de emissor e receptor (incluindo fluxos de segurança) são retransmitidos.

Solicitador/servidor
Esta combinação é manipulada da mesma maneira que os tipos acima. A validação do pedido de conexão é executada pelo canal de servidor no gerenciador de filas de destino.

Solicitador/emissor
A configuração de 'callback' pode ser utilizada se os dois gerenciadores de filas não puderem estabelecer conexões diretas um com o outro, mas ambos puderem se conectar ao MQIPT e aceitar conexões dele.

Servidor/solicitador e servidor/receptor
Eles são manipulados pelo MQIPT exatamente como a configuração do Emissor/Receptor.

Java Security Manager

O suporte do Java Security Manager foi implementado originalmente para ser utilizado com o recurso de modo de proxy SSL para gerenciar o controle de conexões de socket, mas também pode ser utilizado com qualquer um dos outros recursos do MQIPT para fornecer um outro nível de segurança.

O MQIPT utiliza o Java Security Manager padrão, conforme definido na classe `java.lang.SecurityManager`. O recurso Java Security Manager no MQIPT pode ser ativado ou desativado utilizando a propriedade global `SecurityManager`. Consulte "Informações de Referência da Seção Global" na página 56 para obter mais informações.

O Java Security Manager utiliza dois arquivos de política padrão. Um arquivo de política de sistema global denominado `$JREHOME/lib/security/java.policy` (em que `$JREHOME` é o diretório que contém o Java Runtime Environment) é utilizado por todas as instâncias de uma máquina virtual em um host. Um segundo arquivo de política específico do usuário, denominado `.java.policy`, pode existir no diretório pessoal do usuário. Um arquivo de política adicional do MQIPT também pode ser utilizado. Consulte "Informações de Referência da Seção Global" na página 56 para obter mais informações. Para utilizar um arquivo de política

adicional, certifique-se de que a propriedade `policy.allowSystemProperty` tenha sido definida como true no arquivo de política de sistema global (`java.security`).

A sintaxe do arquivo de política é bastante complexa e embora possa ser alterada utilizando um editor de texto, é recomendável usar o utilitário policytool fornecido com Java para fazer quaisquer alterações. O utilitário policytool pode ser encontrado no diretório `$JREHOME/bin` e está totalmente especificado na documentação do Java.

Um arquivo de política de amostra (`mqiptSample.policy`) foi fornecido com o MQIPT para mostrar quais permissões precisam ser definidas para executar o MQIPT. Apenas as entradas `java.net.SocketPermission` precisam ser incluídas/alteradas/excluídas para corresponder às suas necessidades específicas para controlar quem pode se conectar ao MQIPT e a quem o MQIPT pode se conectar. Este arquivo de amostra assume que o MQIPT foi instalado no diretório inicial padrão, por exemplo, `c:\Arquivos de Programas\IBM\Websphere MQ internet pass-thru\`. Se você tiver instalado o MQIPT em uma outra localização, precisará refletir isso nas definições `codeBase` e `java.io.FilePermission`.

As permissões são geralmente definidas com três atributos e para conexões de socket de controle. Seus valores são:

class permission
`java.net.SocketPermission`

name to control
É composto pelo formato `hostname:port`, em que cada elemento do nome pode ser especificado por um caractere curinga. O hostname pode ser um nome de domínio ou um endereço IP. A posição mais à esquerda do hostname pode ser especificado por um asterisco. Por exemplo, `harry.company1.com` seria correspondido para cada uma destas cadeias:

- `harry`
- `harry.company1.com`
- `*.company1.com`
- `*`
- `123.456.789` (assumindo que este é o endereço IP de `harry.company1.com`)

O elemento port do nome pode ser especificado como um único endereço de porta ou um intervalo de endereços de porta, por exemplo:

- 1414 (apenas porta 1414)
- 1414- (todos os endereços de porta maiores ou iguais a 1414)
- -1414 (todos os endereços de porta menores ou iguais a 1414)
- 1-1414 (todos os endereços de porta entre 1 e 1414, inclusive)

allowed action
As ações utilizadas pelo `java.net.SocketPermission` são:

- accept, possibilita a permissão para aceitar conexões do destino especificado
- connect, possibilita a permissão para conectar-se ao destino especificado
- listen, possibilita a permissão para atender na porta ou portas especificadas a pedidos de conexão
- resolve, possibilita a permissão para utilizar o serviço de nome DNS para resolver nomes de domínio em endereços IP

O controle do Java Security Manager também pode ser feito através das propriedades `java.security.manager` e `java.security.policy` do sistema Java, mas é recomendável utilizar as propriedades SecurityManager e SecurityManagerPolicy para controlar o MQIPT.

Terminação Normal e Condições de Falha

Quando o MQIPT detecta o fechamento (normal ou anormal) de um canal do WebSphere MQ, ele propaga o fechamento do canal. Se um administrador encerrar uma rota através do MQIPT, todos os canais nessa rota serão fechados.

O MQIPT fornece um recurso opcional de tempo limite inativo. Se o MQIPT detectar que uma canal ficou inativo durante um período de tempo, excedendo o tempo limite, ele executa um encerramento imediato nas duas conexões em questão.

Os dois sistemas do WebSphere MQ, em qualquer uma das extremidades do canal, observam essas condições de terminação anormal como falhas de rede ou como terminação do canal por seu parceiro. Os canais em questão podem ser iniciados novamente e recuperados (se a falha ocorrer durante um período incerto do protocolo) exatamente como seria feito se não houvesse nenhum MQIPT sendo utilizado.

Segurança de Mensagens

Ao utilizar mensagens rápidas e não-persistentes do WebSphere MQ, se a rota do MQIPT falhar ou for iniciada novamente quando um WebSphere MQ estiver em trânsito, a mensagem poderá ser perdida. Antes de iniciar novamente a rota, certifique-se de que todos os canais do WebSphere MQ que utilizam a rota do MQIPT estejam inativos.

Consulte o *MQSeries Intercommunication*, SC33-1872, para obter mais informações sobre mensagens e canais do WebSphere MQ.

Logs de Conexão

O MQIPT fornece um recurso de log de conexão que contém listas de todas as tentativas de conexão bem-sucedidas e malsucedidas. Ele é controlado utilizando as propriedades `ConnectionLog` e `MaxLogFileSize`. Consulte a seção “Informações de Referência da Seção Global” na página 56 para obter mais informações.

Toda vez que o MQIPT é iniciado, um novo log de conexão é criado; para identificação, o nome do arquivo inclui a data e hora atual. Por exemplo:

```
mqiptYYYYMMDDHHmmSS.log
```

em que

- `YYYY` é o ano
- `MM` é o mês
- `DD` é o dia
- `HH` é a hora
- `mm` é o minuto
- `SS` é o segundo

Para finalidades de auditoria, esses arquivos de log nunca são apagados. O administrador do MQIPT é responsável por gerenciar esses arquivos e excluí-los quando não forem mais necessários.

Outras Considerações de Segurança

Se você opta por não utilizar o SSL, o MQIPT permite fluxos de segurança do canal, para que as saídas de canal do WebSphere MQ possam ser utilizadas para fornecer segurança para todo o canal, de ponta a ponta.

O MQIPT tem várias funções adicionais que ajudam um designer a construir uma solução segura:

- Se houver vários clientes em uma rede interna tentando fazer conexões de saída, todos eles poderão passar por um MQIPT localizado dentro do firewall. O administrador do firewall terá que conceder acesso externo apenas à máquina do MQIPT.
- O MQIPT pode se conectar apenas aos gerenciadores de filas para os quais ele foi configurado explicitamente em seu arquivo de configuração, a menos que o MQIPT esteja agindo como um SOCKS.
- O MQIPT verifica se as mensagens que ele recebe e transmite são válidas e estão em conformidade com o protocolo do WebSphere MQ. Isso ajuda a evitar que os MQIPTs sejam utilizados para ataques de segurança fora do protocolo do WebSphere MQ. Se o MQIPT estiver agindo como um proxy SSL, quando todos os dados e protocolos do WebSphere MQ tiverem sido criptografados, o MQIPT só poderá garantir o protocolo de reconhecimento SSL inicial. Nesta situação, é recomendável utilizar o Java Security Manager, consulte "Java Security Manager" na página 22.
- Isso permite que as saídas de canal executem seus próprios protocolos de segurança de ponta a ponta.
- O MQIPT permite restringir o número total de conexões de entrada, definindo a propriedade `MaxConnectionThreads`. Isso ajuda a proteger um gerenciador de filas interno vulnerável dos ataques do tipo denial-of-service.

Você deve proteger o arquivo de configuração do MQIPT, `mqipt.conf`, porque esse arquivo controla o acesso aos hosts internos, e você deve impedir o acesso não autorizado à porta do comando (se estiver ativada), pois esse acesso permite que uma pessoa externa encerre o MQIPT.

Capítulo 3. Fazendo Upgrade da Versão Anterior

Para fazer upgrade do MQIPT da Versão 1.1 para a Versão 1.2, siga estas etapas:

1. Faça uma cópia do arquivo de configuração `mqipt.conf` e salve-a em uma localização diferente que seja diferente do diretório inicial do MQIPT.
2. Pare o MQIPT executando o comando:

   ```
   mqiptAdmin -stop
   ```
3. Se o MQIPT tiver sido instalado como um serviço, você deverá removê-lo antes de remover a instalação do MQIPT:

   ```
   mqiptService -remove
   ```
4. Execute o programa de remoção de instalação para o MQIPT.
5. Depois de instalar o MQIPT V1.2, copie o arquivo de configuração salvo novamente para o diretório inicial do MQIPT. O arquivo é compatível com a V1.2. O novo arquivo `mqiptSample.conf` mostra as novas propriedades que podem ser utilizadas.
6. É aconselhável utilizar a GUI de Administração do MQIPT para gerenciar as alterações no MQIPT. O arquivo de configuração da V1.1 é compatível com a GUI.

Novas Opções de Configuração

As seguintes propriedades são novas na Versão 1.2:

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

Para obter informações de referência sobre todas as propriedades, consulte "Informações de Referência sobre Configuração" na página 54.

Capítulo 4. Instalando o internet pass-thru no Windows

Este capítulo descreve como instalar o MQIPT em um sistema Windows NT, Windows 2000 ou Windows XP:

Fazendo Download e Instalando os Arquivos

O download do MQIPT pode ser feito na página da Web WebSphere MQ SupportPac, em:

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

Siga as instruções para fazer download.

Abra um prompt de comandos e descompacte `ms81_nt.zip` para um diretório temporário. Execute o `setup.exe` e siga as instruções online.

O MQIPT deve ser instalado por um usuário com autoridade de Administrador.

O MQIPT contém os arquivos mostrados na tabela a seguir e os arquivos para a GUI do Cliente Administrativo, fornecidos como um recurso que é instalado separadamente, mostrado na tabela a seguir.

Arquivo	**Finalidade**
Readme.txt	Contém informações recentes não incluídas nas publicações
mqiptSample.conf	Arquivo de configuração de amostra
ssl\sslSample.pfx	Arquivo de conjunto de chaves de teste
ssl\sslSample.pwd	Arquivo de senha para o arquivo de conjunto de chaves de teste
ssl\sslCAdefault.pfx	Arquivo de conjunto de chaves de CA (Autoridade de Certificação) de amostra
ssl\sslCAdefault.pwd	Arquivo de senha para o arquivo de conjunto de chaves de CA
ssl\KeyMan.zip	Utilitário KeyMan
lib\MQipt.jar	Contém arquivos de tempo de execução, classe e propriedade
lib\ADV_mqipt_normal. class	Consultor do Network Dispatcher para o modo "normal"
lib\ADV_mqipt_replace. class	Consultor do Network Dispatcher para o modo "replace"

Arquivo	Finalidade
lib\mqipt1414Sample.ssl	Arquivo de disparo de amostra para o consultor do Network Dispatcher
bin\mqipt.bat	Atalho para executar o MQIPT a partir da linha de comandos
bin\mqiptAdmin.bat	Atalho para parar o MQIPT e atualizar as informações do arquivo
bin\mqiptservice.exe	Incluir ou remover o MQIPT para/do Gerenciador de Controle de Serviços do Windows
bin\mqiptVersion.bat	Exibe o número de versão do MQIPT
web\MQIPTServlet.war	Arquivo archive da Web para a versão do servlet.
doc\<idioma>\pdf\ <nomearquivo>.pdf	O manual do *internet pass-thru* no formato PDF. Consulte "Bibliografia" na página xi para obter mais informações sobre a documentação em cópia eletrônica.
doc\<idioma>\html\ <nomearquivo>.zip	Arquivo mestre do manual do *internet pass-thru* no formato HTML. Consulte "Bibliografia" na página xi para obter mais informações sobre a documentação em cópia eletrônica.

Os arquivos associados ao recurso da GUI do Cliente Administrativo são:

Arquivo	Finalidade
lib\guiadmin.jar	Contém arquivos de tempo de execução, classe e propriedade
bin\mqiptGui.bat	Atalho para executar o Cliente Administrativo a partir da linha de comandos
bin\customSample. properties	Arquivo de amostra para personalizar a aparência e, portanto, a acessibilidade do Cliente Administrativo

O instalador atualiza a variável de ambiente CLASSPATH do sistema com a localização dos arquivos `MQipt.jar` e `guiadmin.jar`.

Configurando o internet pass-thru

Antes de iniciar o MQIPT pela primeira vez, copie o arquivo de configuração de amostra, `mqiptSample.conf`, para `mqipt.conf`. Consulte Capítulo 9, "Administrando e Configurando o internet pass-thru" na página 49 para obter informações sobre configuração e administração.

Iniciando o internet pass-thru a partir da Linha de Comandos

Abra um prompt de comandos e altere o diretório para `bin` e execute `mqipt`. Por exemplo:

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

Você também pode iniciar o MQIPT a partir do menu Iniciar -> Programas do Windows.

Executar o script mqipt sem quaisquer opções utiliza uma localização padrão de "." para o arquivo de configuração (mqipt.conf). Para especificar uma localização diferente:

```
mqipt <nome do diretório>
```

As mensagens aparecerão no console mostrando o status do MQIPT. Se ocorrer um erro, consulte "Determinação de Problemas" na página 99. As mensagens a seguir são um exemplo de um início bem-sucedido do MQIPT:

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

Os subdiretórios a seguir, do diretório inicial mqipt, são criados automaticamente quando o MQIPT é chamado pela primeira vez:

- Um diretório ″logs″ no qual o log de conexão é mantido
- Um diretório ″errors″ no qual os registros de FFST™ (First Failure Support Technology™) e de rastreio são gravados

Iniciando o Cliente Administrativo a partir da Linha de Comandos

Abra um prompt de comandos e altere o diretório para bin e execute mqiptGui. Por exemplo:

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

Para permitir que o Cliente Administrativo conecte-se externamente através de um firewall a um MQIPT utilizando um proxy SOCKS, especifique o nome do host ou endereço e número da porta:

```
mqiptGui <socksHostName <socksPort>>
```

O socksPort padrão é 1080.

O status do Cliente Administrativo é mostrado por mensagens que aparecem na janela principal do Cliente Administrativo.

Utilizando um Programa de Controle de Serviços do Windows

Um programa de controle de serviços separado, mqiptservice.exe, é fornecido para permitir que o MQIPT seja gerenciado e iniciado como um serviço do Windows.

O mqiptservice.exe contém os seguintes argumentos de linha de comandos:

mqiptservice -install ***path***
Instala e registra o serviço para que apareça no painel de serviços do Windows

como um serviço manual. Vá para o painel de serviços e altere a definição para "automático" para que o MQIPT inicie automaticamente quando o sistema for iniciado. É necessário reinicializar o Windows após a instalação deste serviço. O parâmetro path , que deve ser fornecido, é o caminho completo do diretório que contém o arquivo de configuração `mqipt.conf`. Coloque o nome do caminho entre aspas, caso tenha espaços em branco.

mqiptservice -remove
Remove o serviço, fazendo-o desaparecer do painel de serviços.

mqiptservice ?
Exibe as mensagens de ajuda, em inglês americano, que listam os argumentos válidos.

Especificar install e remove no mesmo comando ocasiona um erro.

O Windows chama internamente o programa `mqiptservice` sem argumentos. Se você chamá-lo a partir da linha de comandos sem argumentos, o tempo limite do programa será excedido e um erro será retornado.

Quando o serviço MQIPT é iniciado, todas as rotas ativas do MQIPT são inicializadas. Quando ele é parado, todas as rotas são submetidas ao encerramento imediato.

Nota: A variável de ambiente PATH do sistema deve conter a localização das bibliotecas de tempo de execução do JNI. O arquivo `jvm.dll` pode ser encontrado no subdiretório `classics` do JDK.

Removendo a Instalação do internet pass-thru como um Serviço do Windows

Remova a instalação do MQIPT como um serviço parando-o primeiramente no painel de serviços do Windows. Em seguida, abra um prompt de comandos, vá para o subdiretório `bin` do MQIPT e digite:

```
mqiptservice -remove
```

Removendo a Instalação do internet pass-thru

Antes de remover a instalação do MQIPT de seu sistema, remova-o como um Serviço do Windows, conforme descrito acima. Em seguida, execute o processo de remoção de instalação a partir do menu Iniciar do Windows.

Capítulo 5. Instalando o internet pass-thru no Sun Solaris

Este capítulo descreve como instalar o MQIPT em um sistema Sun Solaris:

Fazendo Download e Instalando os Arquivos

O download do MQIPT pode ser feito na página da Web WebSphere MQ SupportPac, em:

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

Siga as instruções para fazer download.

Efetue login como `root` e descompacte `ms81_sol.tar.Z` em um diretório temporário. Execute o comando `pkgadd`, como neste exemplo:

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

O exemplo assume que `ms81_sol.tar.Z` está no diretório `/tmp`.

O MQIPT contém os arquivos mostrados na tabela a seguir, incluindo os arquivos da GUI do Cliente Administrativo.

Arquivo	**Finalidade**
Readme.txt	Contém informações recentes não incluídas nas publicações
mqiptSample.conf	Arquivo de configuração de amostra
ssl/sslSample.pfx	Arquivo de conjunto de chaves de teste
ssl/sslSample.pwd	Arquivo de senha para o arquivo de conjunto de chaves de teste
ssl/sslCAdefault.pfx	Arquivo de conjunto de chaves de CA (Autoridade de Certificação) de amostra
ssl/sslCAdefault.pwd	Arquivo de senha para o arquivo de conjunto de chaves de CA
ssl/KeyMan.zip	Utilitário KeyMan
lib/MQipt.jar	Contém arquivos de tempo de execução, classe e propriedade
lib/ADV_mqipt_normal. class	Consultor do Network Dispatcher para o modo "normal"
lib/ADV_mqipt_replace. class	Consultor do Network Dispatcher para o modo "replace"

Arquivo	Finalidade
lib/mqipt1414Sample.ssl	Arquivo de disparo de amostra para o consultor do Network Dispatcher
bin/mqipt	Atalho para executar o MQIPT a partir da linha de comandos
bin/mqiptAdmin	Atalho para parar o MQIPT e atualizar as informações do arquivo
bin/mqiptVersion	Exibe o número de versão do MQIPT
bin/mqiptService	Instalar o MQIPT para que ele seja iniciado automaticamente na partida do sistema.
bin/mqiptEnv	Define a localização do arquivo `mqipt.jar` e é utilizado apenas pelos outros scripts.
web/MQIPTServlet.war	Arquivo archive da Web para a versão do servlet.
doc/<idioma>/pdf/ <nomearquivo>.pdf	O manual do *internet pass-thru* no formato PDF. Consulte "Bibliografia" na página xi para obter mais informações sobre a documentação em cópia eletrônica.
doc/<idioma>/html/ <nomearquivo>.zip	Arquivo mestre do manual do *internet pass-thru* no formato HTML. Consulte "Bibliografia" na página xi para obter mais informações sobre a documentação em cópia eletrônica.
lib/mqiptGui.jar	Contém arquivos de tempo de execução, classe e propriedade para a GUI do Cliente Administrativo
bin/mqiptGui	Atalho para executar o Cliente Administrativo a partir da linha de comandos
bin/customSample. properties	Arquivo de amostra para personalizar a aparência e, portanto, a acessibilidade do Cliente Administrativo

Configurando o internet pass-thru

Antes de iniciar o MQIPT pela primeira vez, copie o arquivo de configuração de amostra, `mqiptSample.conf`, para `mqipt.conf`. Consulte Capítulo 9, "Administrando e Configurando o internet pass-thru" na página 49 para obter informações sobre configuração e administração.

Iniciando o internet pass-thru a partir da Linha de Comandos

Efetue login como `root` e altere o diretório para `bin`. Por exemplo:

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

Executar o script `mqipt` sem quaisquer opções utiliza uma localização padrão de "." para o arquivo de configuração (`mqipt.conf`). Para especificar uma localização diferente:

```
mqipt <nome do diretório>
```

As mensagens aparecerão no console mostrando o status do MQIPT. Se ocorrer um erro, consulte "Determinação de Problemas" na página 99. As mensagens a seguir são um exemplo de um início bem-sucedido do MQIPT:

```
5639-L92 (C) Copyright IBM Corp. 2000-2002 All Rights Reserved
MQCPI001 WebSphere MQ internet pass-thru Version 1.2 starting
MQCPI004 Reading configuration information from /opt/mqipt/mqipt.conf
MQCPI008 Listening for control commands on port 1881
MQCPI011 The path /opt/mqipt/logs will be used to store the log files
```

```
MQCPI006 Route 1418 has started and will forward messages to :
MQCPI034 ....mqserver.company4.com(1414)
MQCPI035 ....using MQ protocols
MQCPI006 Route 1415 has started and will forward messages to :
MQCPI034 ....mqipt.company2.com(1415)
MQCPI035 ....using MQ protocols
MQCPI036 ....SSL Client side enabled with properties :
MQCPI031 ......cipher suites <null>
MQCPI032 ......keyring file /opt/mqipt/KeyMan.pfx
MQCPI038 ......distinguished name(s) CN=*Doe O=IBM OU=* L=* ST=* C=*
```

Os subdiretórios a seguir, do diretório inicial `mqipt`, são criados automaticamente quando o MQIPT é chamado pela primeira vez:

- Um diretório ″logs″ no qual o log de conexão é mantido
- Um diretório ″errors″ no qual os registros de FFST (First Failure Support Technology) e de rastreio são gravados

Iniciando o internet pass-thru Automaticamente

Para iniciar o MQIPT automaticamente quando o sistema é iniciado, execute o script `mqiptService`. Por exemplo:

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

Para impedir que o MQIPT inicie automaticamente:

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

Iniciando o Cliente Administrativo a partir da Linha de Comandos

Abra um prompt de comandos e altere o diretório para `bin` e execute `mqiptGui`. Por exemplo:

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

Para permitir que o Cliente Administrativo conecte-se externamente através de um firewall a um MQIPT, especifique o nome do host ou endereço e número da porta:

```
mqiptGui <socksHostName <socksPort>>
```

O `socksPort` padrão é 1080.

O status do Cliente Administrativo é mostrado por mensagens que aparecem na janela principal do Cliente Administrativo.

Removendo a Instalação do internet pass-thru

Antes de remover a instalação do MQIPT de seu sistema, impeça-o de iniciar automaticamente, conforme descrito em “Iniciando o internet pass-thru Automaticamente”. Efetue login como `root` e execute o comando `pkgrm`:

```
pkgrm mqipt
```

Capítulo 6. Instalando o internet pass-thru no AIX

Este capítulo descreve como instalar o MQIPT em um sistema AIX:

Fazendo Download e Instalando os Arquivos

O download do MQIPT pode ser feito na página da Web WebSphere MQ SupportPac, em:

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

Siga as instruções para fazer download.

Efetue login como `root` e descompacte `ms81_aix.tar.Z` em um diretório temporário. Execute o comando `installp`, como neste exemplo:

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

O exemplo assume que `ms81_aix.tar.Z` está no diretório `/tmp`.

O MQIPT contém os arquivos mostrados na tabela a seguir, incluindo os arquivos da GUI do Cliente Administrativo.

Arquivo	**Finalidade**
Readme.txt	Contém informações recentes não incluídas nas publicações
mqiptSample.conf	Arquivo de configuração de amostra
ssl/sslSample.pfx	Arquivo de conjunto de chaves de teste
ssl/sslSample.pwd	Arquivo de senha para o arquivo de conjunto de chaves de teste
ssl/sslCAdefault.pfx	Arquivo de conjunto de chaves de CA (Autoridade de Certificação) de amostra
ssl/sslCAdefault.pwd	Arquivo de senha para o arquivo de conjunto de chaves de CA
ssl/KeyMan.zip	Utilitário KeyMan
lib/MQipt.jar	Contém arquivos de tempo de execução, classe e propriedade
lib/ADV_mqipt_normal. class	Consultor do Network Dispatcher para o modo "normal"
lib/ADV_mqipt_replace. class	Consultor do Network Dispatcher para o modo "replace"
lib/mqipt1414Sample.ssl	Arquivo de disparo de amostra para o consultor do Network Dispatcher

Arquivo	Finalidade
bin/mqipt	Atalho para executar o MQIPT a partir da linha de comandos
bin/mqiptAdmin	Atalho para parar o MQIPT e atualizar as informações do arquivo
bin/mqiptVersion	Exibe o número de versão do MQIPT
bin/mqiptService	Instalar o MQIPT para que ele seja iniciado automaticamente na partida do sistema.
bin/mqiptEnv	Define a localização do arquivo `mqipt.jar` e é utilizado apenas pelos outros scripts.
web/MQIPTServlet.war	Arquivo archive da Web para a versão do servlet
doc/<idioma>/pdf/ <nomearquivo>.pdf	O *internet pass-thru* no formato PDF. Consulte "Bibliografia" na página xi para obter mais informações sobre a documentação em cópia eletrônica.
doc/<idioma>/html/ <nomearquivo>.zip	Arquivo mestre do manual do *internet pass-thru* no formato HTML. Consulte "Bibliografia" na página xi para obter mais informações sobre a documentação em cópia eletrônica.
lib/mqiptGui.jar	Contém arquivos de tempo de execução, classe e propriedade
bin/mqiptGui	Atalho para executar o Cliente Administrativo a partir da linha de comandos
bin/customSample. properties	Arquivo de amostra para personalizar a aparência e, portanto, a acessibilidade do Cliente Administrativo

Configurando o internet pass-thru

Antes de iniciar o MQIPT pela primeira vez, copie o arquivo de configuração de amostra, `mqiptSample.conf`, para `mqipt.conf`. Consulte Capítulo 9, "Administrando e Configurando o internet pass-thru" na página 49 para obter informações sobre configuração e administração.

Iniciando o internet pass-thru a partir da Linha de Comandos

Efetue login como `root` e altere o diretório para `bin`. Por exemplo:

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

Executar o script `mqipt` sem quaisquer opções utiliza uma localização padrão de "." para o arquivo de configuração (`mqipt.conf`). Para especificar uma localização diferente:

```
mqipt <nome do diretório>
```

As mensagens aparecerão no console mostrando o status do MQIPT. Se ocorrer um erro, consulte "Determinação de Problemas" na página 99. As mensagens a seguir são um exemplo de um início bem-sucedido do MQIPT:

```
5639-L92 (C) Copyright IBM Corp. 2000-2002 All Rights Reserved
MQCPI001 WebSphere MQ internet pass-thru Version 1.2 starting
MQCPI004 Reading configuration information from /usr/opt/mqipt/mqipt.conf
MQCPI008 Listening for control commands on port 1881
MQCPI011 The path /usr/opt/mqipt/logs will be used to store the log files
MQCPI006 Route 1418 has started and will forward messages to :
MQCPI034 ....mqserver.company4.com(1414)
MQCPI035 ....using MQ protocols
```

```
MQCPI006 Route 1415 has started and will forward messages to :
MQCPI034 ....mqipt.company2.com(1415)
MQCPI035 ....using MQ protocols
MQCPI036 ....SSL Client side enabled with properties :
MQCPI031 ......cipher suites <null>
MQCPI032 ......keyring file /usr/opt/mqipt/KeyMan.pfx
MQCPI038 ......distinguished name(s) CN=*Doe O=IBM OU=* L=* ST=* C=*
```

Os subdiretórios a seguir, do diretório inicial `mqipt`, são criados automaticamente quando o MQIPT é chamado pela primeira vez:

- Um diretório ″logs″ no qual o log de conexão é mantido
- Um diretório ″errors″ no qual os registros de FFST (First Failure Support Technology) e de rastreio são gravados

Iniciando o internet pass-thru Automaticamente

Para iniciar o MQIPT automaticamente quando o sistema é iniciado, execute o script `mqiptService` para incluir uma entrada no `inittab`. Por exemplo:

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

Para impedir que o MQIPT inicie automaticamente e remova sua entrada de `inittab`:

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

Iniciando o Cliente Administrativo a partir da Linha de Comandos

Abra um prompt de comandos e altere o diretório para `bin` e execute `mqiptGui`. Por exemplo:

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

Para permitir que o Cliente Administrativo conecte-se externamente através de um firewall a um MQIPT, especifique o nome do host ou endereço e número da porta:

```
mqiptGui <socksHostName <socksPort>>
```

O `socksPort` padrão é 1080.

O status do Cliente Administrativo é mostrado por mensagens que aparecem na janela principal do Cliente Administrativo.

Removendo a Instalação do internet pass-thru

Antes de remover a instalação do MQIPT de seu sistema, impeça-o de iniciar automaticamente, conforme descrito em “Iniciando o internet pass-thru Automaticamente”. Efetue login como `root` e execute o comando `installp`:

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

Capítulo 7. Instalando o internet pass-thru no HP-UX

Este capítulo descreve como instalar o MQIPT em um sistema HP-UX:

Fazendo Download e Instalando os Arquivos

O download do MQIPT pode ser feito na página da Web WebSphere MQ SupportPac, em:

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

Siga as instruções para fazer download.

Efetue login como `root` e descompacte `ms81_hp11.tar.Z` em um diretório temporário. Execute o comando `swinstall`, como neste exemplo:

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

O exemplo assume que `ms81_hp11.tar.Z` está no diretório `/tmp`.

O MQIPT contém os arquivos mostrados na tabela a seguir, incluindo os arquivos da GUI do Cliente Administrativo.

Arquivo	**Finalidade**
Readme.txt	Contém informações recentes não incluídas nas publicações
mqiptSample.conf	Arquivo de configuração de amostra
ssl/sslSample.pfx	Arquivo de conjunto de chaves de teste
ssl/sslSample.pwd	Arquivo de senha para o arquivo de conjunto de chaves de teste
ssl/sslCAdefault.pfx	Arquivo de conjunto de chaves de CA (Autoridade de Certificação) de amostra
ssl/sslCAdefault.pwd	Arquivo de senha para o arquivo de conjunto de chaves de CA
ssl/KeyMan.zip	Utilitário KeyMan
lib/MQipt.jar	Contém arquivos de tempo de execução, classe e propriedade
lib/ADV_mqipt_normal. class	Consultor do Network Dispatcher para o modo "normal"
lib/ADV_mqipt_replace. class	Consultor do Network Dispatcher para o modo "replace"

Arquivo	Finalidade
lib/mqipt1414Sample.ssl	Arquivo de disparo de amostra para o consultor do Network Dispatcher
bin/mqipt	Atalho para executar o MQIPT a partir da linha de comandos
bin/mqiptAdmin	Atalho para parar o MQIPT e atualizar as informações do arquivo
bin/mqiptVersion	Exibe o número de versão do MQIPT
bin/mqiptService	Instalar o MQIPT para que ele seja iniciado automaticamente na partida do sistema.
bin/mqiptEnv	Define a localização do arquivo `mqipt.jar` e é utilizado apenas pelos outros scripts.
bin/mqiptFork	Utilizando para lançar o MQIPT durante a partida do sistema
web/MQIPTServlet.war	Arquivo archive da Web para a versão do servlet
doc/<idioma>/pdf/ <nomearquivo>.pdf	O manual do *internet pass-thru* em formato PDF. Consulte "Bibliografia" na página xi para obter mais informações sobre a documentação em cópia eletrônica.
doc/<idioma>/html/ <nomearquivo>.zip	Arquivo mestre do manual do *internet pass-thru* no formato HTML. Consulte "Bibliografia" na página xi para obter mais informações sobre a documentação em cópia eletrônica.
lib/mqiptGui.jar	Contém arquivos de tempo de execução, classe e propriedade para a GUI do Cliente Administrativo
bin/mqiptGui	Atalho para executar a GUI do Cliente Administrativo a partir da linha de comandos
bin/customSample. properties	Arquivo de amostra para personalizar a aparência e, portanto, a acessibilidade do Cliente Administrativo

Configurando o internet pass-thru

Antes de iniciar o MQIPT pela primeira vez, copie o arquivo de configuração de amostra, `mqiptSample.conf`, para `mqipt.conf`. Consulte Capítulo 9, "Administrando e Configurando o internet pass-thru" na página 49 para obter informações sobre configuração e administração.

Iniciando o internet pass-thru a partir da Linha de Comandos

Efetue login como `root` e altere o diretório para `bin`. Por exemplo:

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

Executar o script `mqipt` sem quaisquer opções utiliza uma localização padrão de "." para o arquivo de configuração (`mqipt.conf`). Para especificar uma localização diferente:

```
mqipt <nome do diretório>
```

As mensagens aparecerão no console mostrando o status do MQIPT. Se ocorrer um erro, consulte "Determinação de Problemas" na página 99. As mensagens a seguir são um exemplo de um início bem-sucedido do MQIPT:

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

Os subdiretórios a seguir, do diretório inicial `mqipt`, são criados automaticamente quando o MQIPT é chamado pela primeira vez:

- Um diretório ″logs″ no qual o log de conexão é mantido
- Um diretório ″errors″ no qual os registros de FFST (First Failure Support Technology) e de rastreio são gravados

Iniciando o internet pass-thru Automaticamente

Para iniciar o MQIPT automaticamente quando o sistema é iniciado, execute o script `mqiptService`. Por exemplo:

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

Pressupõe-se que o JDK 1.4 já esteja instalado em um diretório denominado `/opt/java1.4`. Se este não for o caso, edite o arquivo `mqipt.ske` e altere a variável PATH para apontar para a localização do JDK. Você deve aplicar esta alteração antes de executar o comando `mqiptService -install`.

Quando o MQIPT é iniciado como um serviço, ele grava um arquivo `console.log` no subdiretório `logs`. Este subdiretório é criado na primeira vez em que o MQIPT é executado, portanto o MQIPT deve ser iniciado pelo menos uma vez antes de tentar iniciá-lo como um serviço.

Para impedir que o MQIPT inicie automaticamente:

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

Iniciando o Cliente Administrativo a partir da Linha de Comandos

Abra um prompt de comandos e altere o diretório para `bin` e execute `mqiptGui`. Por exemplo:

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

Para permitir que o Cliente Administrativo conecte-se externamente através de um firewall a um MQIPT, especifique o nome do host ou endereço e número da porta:

```
mqiptGui <socksHostName <socksPort>>
```

O `socksPort` padrão é 1080.

O status do Cliente Administrativo é mostrado por mensagens que aparecem na janela principal do Cliente Administrativo.

Removendo a Instalação do internet pass-thru

Antes de remover a instalação do MQIPT de seu sistema, impeça-o de iniciar automaticamente, conforme descrito em “Iniciando o internet pass-thru Automaticamente” na página 43. Efetue login como `root` e execute o comando `swremove`:

```
swremove MQIPT
```

Capítulo 8. Instalando o internet pass-thru no Linux

Este capítulo descreve como instalar o MQIPT em um sistema Linux:

Fazendo Download e Instalando os Arquivos

O download do MQIPT pode ser feito na página da Web WebSphere MQ SupportPac, em:

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

Siga as instruções para fazer download.

Efetue login como `root` e descompacte `ms81_linux.tar.gz` em um diretório temporário. Execute o comando `rpm`, como neste exemplo:

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

O exemplo assume que `ms81_linux.tar.gz` está no diretório /tmp.

O MQIPT contém os arquivos mostrados na tabela a seguir, incluindo os arquivos da GUI do Cliente Administrativo.

Arquivo	**Finalidade**
Readme.txt	Contém informações recentes não incluídas nas publicações
mqiptSample.conf	Arquivo de configuração de amostra
ssl/sslSample.pfx	Arquivo de conjunto de chaves de teste
ssl/sslSample.pwd	Arquivo de senha para o arquivo de conjunto de chaves de teste
ssl/sslCAdefault.pfx	Arquivo de conjunto de chaves de CA (Autoridade de Certificação) de amostra
ssl/sslCAdefault.pwd	Arquivo de senha para o arquivo de conjunto de chaves de CA
ssl/KeyMan.zip	Utilitário KeyMan
lib/MQipt.jar	Contém arquivos de tempo de execução, classe e propriedade
lib/ADV_mqipt_normal. class	Consultor do Network Dispatcher para o modo "normal"
lib/ADV_mqipt_replace. class	Consultor do Network Dispatcher para o modo "replace"

Arquivo	Finalidade
lib/mqipt1414Sample.ssl	Arquivo de disparo de amostra para o consultor do Network Dispatcher
lib/libiptqos.so	Biblioteca de tempo de execução para o suporte à Qualidade de Serviço
bin/mqipt	Atalho para executar o MQIPT a partir da linha de comandos
bin/mqiptAdmin	Atalho para parar o MQIPT e atualizar as informações do arquivo
bin/mqiptVersion	Exibe o número de versão do MQIPT
bin/mqiptService	Instalar o MQIPT para que ele seja iniciado automaticamente na partida do sistema.
bin/mqiptEnv	Define a localização do arquivo `mqipt.jar` e é utilizado apenas pelos outros scripts.
web/MQIPTServlet.war	Arquivo archive da Web para a versão do servlet
doc/<idioma>/pdf/ <nomearquivo>.pdf	O manual do *internet pass-thru* no formato PDF. Consulte "Bibliografia" na página xi para obter mais informações sobre a documentação em cópia eletrônica.
doc/<idioma>/html/ <nomearquivo>.zip	Arquivo mestre do manual do *internet pass-thru* no formato HTML. Consulte "Bibliografia" na página xi para obter mais informações sobre a documentação em cópia eletrônica.
lib/mqiptGui.jar	Contém arquivos de tempo de execução, classe e propriedade para a GUI do Cliente Administrativo
bin/mqiptGui	Atalho para executar a GUI do Cliente Administrativo a partir da linha de comandos
bin/customSample. properties	Arquivo de amostra para personalizar a aparência e, portanto, a acessibilidade do Cliente Administrativo

Configurando o internet pass-thru

Antes de iniciar o MQIPT pela primeira vez, copie o arquivo de configuração de amostra, `mqiptSample.conf`, para `mqipt.conf`. Consulte Capítulo 9, "Administrando e Configurando o internet pass-thru" na página 49 para obter informações sobre configuração e administração.

Iniciando o internet pass-thru a partir da Linha de Comandos

Efetue login como `root` e altere o diretório para `bin`. Por exemplo:

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

Executar o script `mqipt` sem quaisquer opções utiliza uma localização padrão de "." para o arquivo de configuração (`mqipt.conf`). Para especificar uma localização diferente:

```
mqipt <nome do diretório>
```

As mensagens aparecerão no console mostrando o status do MQIPT. Se ocorrer um erro, consulte "Determinação de Problemas" na página 99. As mensagens a seguir são um exemplo de um início bem-sucedido do MQIPT:

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

Os subdiretórios a seguir, do diretório inicial `mqipt`, são criados automaticamente quando o MQIPT é chamado pela primeira vez:

- Um diretório ″logs″ no qual o log de conexão é mantido
- Um diretório ″errors″ no qual os registros de FFST (First Failure Support Technology) e de rastreio são gravados

Iniciando o internet pass-thru Automaticamente

Para iniciar o MQIPT automaticamente quando o sistema é iniciado, execute o script `mqiptService`. Por exemplo:

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

Quando o MQIPT é iniciado como um serviço, ele grava um arquivo `console.log` no subdiretório `logs`. Este subdiretório é criado na primeira vez em que o MQIPT é executado, portanto o MQIPT deve ser iniciado pelo menos uma vez antes de tentar iniciá-lo como um serviço.

Para impedir que o MQIPT inicie automaticamente:

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

Iniciando o Cliente Administrativo a partir da Linha de Comandos

Abra um prompt de comandos e altere o diretório para `bin` e execute `mqiptGui`. Por exemplo:

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

Para permitir que o Cliente Administrativo conecte-se externamente através de um firewall a um MQIPT, especifique o nome do host ou endereço e número da porta:

```
mqiptGui <socksHostName <socksPort>>
```

O `socksPort` padrão é 1080.

O status do Cliente Administrativo é mostrado por mensagens que aparecem na janela principal do Cliente Administrativo.

Removendo a Instalação do internet pass-thru

Antes de remover a instalação do MQIPT de seu sistema, impeça-o de iniciar automaticamente, conforme descrito em “Iniciando o internet pass-thru Automaticamente” na página 47. Efetue login como `root` e execute o comando `swremove`:

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

Capítulo 9. Administrando e Configurando o internet pass-thru

Você configura o MQIPT fazendo alterações no arquivo de configuração `mqipt.conf`. Faça isso utilizando o Cliente Administrativo, que é o modo recomendado, ou utilizando um editor de sua escolha. Ambas as técnicas são aqui descritas, com informações de referência relevantes para ambas:

Utilizando Cliente Administrativo para o internet pass-thru

Você pode utilizar o Cliente Administrativo para configurar e atualizar um ou mais MQIPTs. Ele exibe propriedades globais para um MQIPT e propriedades específicas da rota.

Os únicos dados armazenados localmente no Cliente Administrativo são a lista de MQIPTs, em um arquivo denominado `client.conf`. As propriedades globais e de rota são sempre recuperadas do MQIPT antes delas serem exibidas no Cliente Administrativo.

Iniciando o Cliente Administrativo

Inicie o Cliente Administrativo utilizando o script `mqiptGui` encontrado do subdiretório `bin` do MQIPT. Consulte o capítulo de instalação para cada plataforma para obter informações sobre como iniciar o Cliente Administrativo.

Na primeira vez em que o Cliente Administrativo é iniciado, uma caixa de diálogo é exibida, solicitando informações de conexão para um MQIPT. As informações requeridas são:

Nome do MQIPT
Um nome utilizado para descrever este MQIPT. Embora esta informação não seja essencial, é recomendável fornecê-la.

Endereço de rede
O endereço do sistema no qual o MQIPT reside - um nome reconhecido pelo servidor de nomes, um endereço decimal pontilhado ou host local (se o MQIPT estiver na mesma máquina que o cliente).

Porta do comando
O número da porta na qual o MQIPT está atendendo os comandos.

Tempo limite (seg)
Este é o número de segundos que o Cliente Administrativo aguardará por uma conexão com o MQIPT. Mantenha este valor o mais baixo possível para reduzir o tempo de atualização da janela.

Acessar senha
A senha utilizada ao se comunicar com o MQIPT. Preencha este campo apenas se a verificação de senha estiver em vigor. (A verificação de senha estará em vigor se AccessPW tiver sido fornecido no arquivo de configuração do MQIPT e for diferente de uma cadeia nula.)

Salvar senha

Se esta caixa de entrada estiver desmarcada, a senha será memorizada pelo tempo de duração da sessão ou até que o MQIPT seja removido. Se esta caixa de entrada estiver selecionada, a senha será salva para sessões futuras.

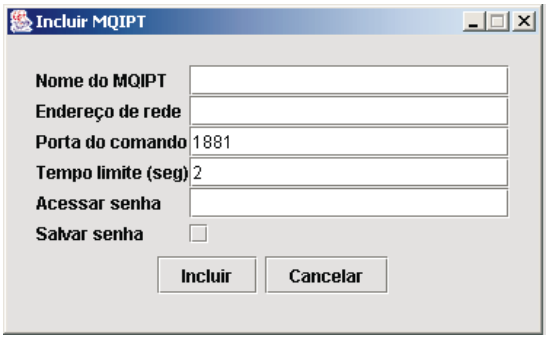

Figura 8. Janela para acessar pela primeira vez um MQIPT

Administrando um MQIPT

Apenas um MQIPT pode ser atualizado por vez, portanto, se um outro MQIPT for selecionado da lista, as alterações pendentes deverão ser aplicadas antes de continuar. As alterações feitas em qualquer uma das propriedades não afetam o MQIPT até que a opção de menu “Aplicar“ seja utilizada.

Selecionar um MQIPT na lista recupera as propriedades globais e de rota do MQIPT. Se o MQIPT não estiver em execução ou um CommandPort incorreto tiver sido especificado, uma mensagem de erro será emitida. Alterações no nome do host e no CommandPort podem ser feitas na opção de menu “Conexão”.

Dar um clique duplo em um MQIPT na lista exibe uma lista de rotas. Selecionar uma rota exibe suas propriedades. Você pode adaptar as propriedades de acordo com suas necessidades.

Quando é utilizado um arquivo de configuração (`mqipt.conf`) do MQSeries internet pass-thru Versão 1.0, não há um nome de rota. Você pode incluir um nome de rota atualizando o campo Nome.

Quando as alterações são aplicadas, a data e hora do arquivo de configuração são registradas e ele é retornado para o MQIPT, e as alterações entram em vigor imediatamente. Qualquer linha de comentário existente é perdida.

Uma rota pode ser incluída utilizando a opção de menu “Incluir Rota”. Um conjunto de propriedades padrão é exibido para esta nova rota, conforme definido pelas propriedades globais.

A Herança de Propriedades

Há uma hierarquia de formas nas quais as propriedades de MQIPTs e rotas podem ser definidas no Cliente Administrativo:

1. Cada propriedade possui um valor padrão e, se a propriedade não for mencionada no arquivo de configuração, ou não tiver sido definida especificamente pela ação do usuário no Cliente Administrativo, assume-se o valor padrão.

2. As propriedades globais definidas nos MQIPTs são assumidas em cada rota desse MQIPT, a menos que existam informações de rota específicas em contrário. No arquivo de configuração, isso significa que as propriedades definidas na sub-rotina global são propagadas para todas as rotas, a menos que propriedades adicionais sejam definidas em sub-rotinas da rota. As propriedades definidas pelo usuário do Cliente Administrativo em um MQIPT são propagadas para todas as rotas, a menos que uma propriedade seja definida especificamente em uma rota.
3. Independentemente dos valores padrão e definições globais, qualquer definição criada para uma rota é mantida para essa rota.

Opções do Menu Arquivo

A maioria das opções relevantes para gerenciar a árvore são mostradas quando o menu Arquivo é selecionado.

Incluir MQIPT
Torna visível o mesmo diálogo que aparece quando o cliente é utilizado pela primeira vez, descrito em "Iniciando o Cliente Administrativo" na página 49.

Remover MQIPT
Remove o MQIPT atualmente destacado apenas da árvore no Cliente Administrativo. Não afeta a execução do MQIPT.

Salvar configuração
Salva os nós do MQIPT da árvore no arquivo de configuração do Cliente Administrativo para que possam ser lidos novamente na próxima vez em que ele for iniciado. Apenas os nós do MQIPT são salvos. As propriedades globais e de rota são sempre recuperadas do MQIPT.

Sair
Pára a execução do Cliente Administrativo. No entanto, o Cliente Administrativo primeiro verifica se a árvore ou o MQIPT atual foi alterado; se um ou ambos tiverem sido alterados, aparecerá um ou mais diálogos perguntando se você deseja salvar o cliente, aplicar as alterações no MQIPT, ou ambos.

Opções de Menu do MQIPT

Conexão
Altera os parâmetros de acesso de um MQIPT. As alterações são refletidas na exibição em árvore. Esta opção torna visível uma janela semelhante àquela descrita em "Iniciando o Cliente Administrativo" na página 49.

Senha
Altera a propriedade da senha do MQIPT remoto. Esta ação torna visível um diálogo de senha no qual você deverá completar as seguintes entradas:

- **Senha atual**: como uma verificação contra o uso impróprio, você deve demonstrar que sabe a senha atual antes de alterá-la. Se nenhuma senha estiver atualmente em vigor, este campo ficará vazio.
- **Nova senha**: a nova senha ou espaço em branco, se você desejar descontinuar o uso de senhas neste MQIPT.
- **Confirmar nova senha**: protege contra erros de digitação no campo anterior através da repetição da mesma informação.
- **Salvar senha**: utilizado para determinar se a nova senha será salva localmente, juntamente com as outras propriedades de acesso deste MQIPT.

Incluir rota
Inclui uma rota no MQIPT selecionado. Consulte a seção Figura 9 para obter detalhes. Cada rota deve ter um ListenerPort exclusivo para o MQIPT.

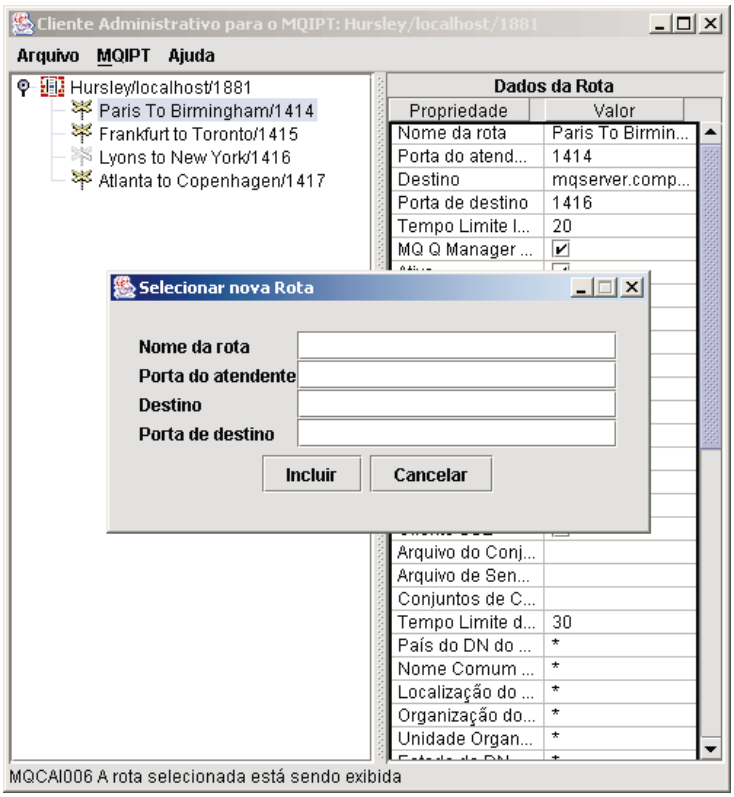

Figura 9. Incluindo uma rota

Excluir Rota
Exclui a rota selecionada do MQIPT. A exclusão não afeta o MQIPT até que a opção de menu “Aplicar” seja utilizada.

Aplicar
Quando você estiver satisfeito com as alterações feitas na configuração do MQIPT, esta opção enviará um novo arquivo de configuração para o MQIPT, que irá salvá-lo. As novas definições entram em vigor imediatamente.

Atualizar
Lê o arquivo de configuração do MQIPT selecionado e atualiza a exibição.

Parar
Envia um comando de parada para o MQIPT para indicar que ele deve parar a execução. Após este comando, perde-se o contato com o MQIPT. A menos que a propriedade global RemoteShutdown esteja ativada, este comando é ignorado.

As informações da rota podem ser atualizadas da mesma maneira que as informações globais do MQIPT. Ao alterar as propriedades de uma rota, você deve aplicar as alterações para que as mesmas entrem em vigor. Isso pode ser feito selecionando a opção de menu “MQIPT/Aplicar” ou respondendo ″Sim″ quando for perguntado se deseja salvar a configuração.

Opções do Menu Ajuda

Ajuda
Utiliza o Netscape para exibir informações sobre como utilizar o Cliente Administrativo. Selecione ″Administrando e Configurando o internet pass-thru″ no painel esquerdo. Antes de utilizar o Cliente Administrativo, você deve descompactar os arquivos encontrados no subdiretório `<idioma>/html`.

Sobre
Mostra uma janela instantânea com informações sobre a versão do Cliente Administrativo.

Utilizando Comandos de Modo de Linha do internet pass-thru

Se você optou por não utilizar o Cliente Administrativo, poderá utilizar comandos de modo de linha para administrar e configurar o internet pass-thru.

Administrando o internet pass-thru Utilizando Comandos de Modo de Linha

Utilizando um editor de sua escolha, altere o arquivo de configuração, `mqipt.conf`, de acordo com suas necessidades. Consulte “Informações de Referência sobre Configuração” na página 54 para obter uma lista das propriedades que podem ser alteradas.

Se a seção global do `mqipt.conf` especifica um valor para `CommandPort`, o MQIPT atende nesta porta para os seguintes comandos de administração ASCII:

```
mqiptAdmin -refresh {hostname {port} }      envia o comando atualizar
mqiptAdmin -stop    {hostname {port} }      envia o comando parar
```

O script `mqiptAdmin` está no subdiretório `bin`.

Se não fornecido, hostname assumirá o padrão como `localhost` e a porta como `1881`.

STOP
O MQIPT encerra todas as conexões, pára o atendimento de conexões de entrada e, em seguida, sai. Utilizar a opção de menu “MQIPT/Parar” do Cliente Administrativo tem o mesmo efeito. A menos que o arquivo `mqipt.conf` especifique `RemoteShutDown=true`, este comando é ignorado.

REFRESH
O MQIPT lê novamente o `mqipt.conf`. Se o mesmo constatar:

- Que quaisquer rotas atualmente ativas estão agora marcadas como inativas (ou estiverem completamente ausentes), elas são encerradas e o atendimento de conexões de entrada nessas rotas é interrompido.
- Quaisquer rotas marcadas como ativas no arquivo de configuração que não estejam atualmente em execução, elas são inicializadas.
- Que os parâmetros de configuração de uma rota atualmente em execução foram alterados, os valores alterados são aplicados a essas rotas. Onde possível (por exemplo, uma alteração na definição de rastreio), isso é feito sem interrupção das conexões em execução. Para algumas alterações de parâmetro (por exemplo, uma alteração em um destino), o MQIPT tem que encerrar todas as conexões antes de efetivar a alteração e iniciar novamente a rota.

Utilizar a opção de menu “MQIPT/Aplicar” do Cliente Administrativo tem o mesmo efeito, desde que o Cliente Administrativo não tenha alterado nenhuma das definições do MQIPT.

No Windows, essas funções administrativas também estão disponíveis no menu Iniciar -> Programas.

Informações de Referência sobre Configuração

Para obter informações sobre como preparar algumas configurações simples, consulte o Capítulo 10, “Iniciando o internet pass-thru” na página 67. Para uma configuração de amostra, consulte o arquivo `mqiptSample.conf` no diretório inicial do MQIPT.

O arquivo `mqipt.conf` é constituído de um conjunto de seções. Há uma seção global e uma seção adicional para cada rota que tenha sido definida através do MQIPT. Nesta configuração simples, há apenas uma rota, portanto, o arquivo contém duas seções, global e route.

Cada seção contém os pares de propriedade nome/valor. Algumas propriedades podem aparecer apenas nas seções global, outras podem aparecer apenas nas seções route e outras podem aparecer nas seções global e route. Se uma propriedade não aparecer nas seções global e route, o valor da propriedade na seção route substituirá o valor da seção global, mas apenas para a rota em questão. Desse modo, a seção global poderá ser utilizada para estabelecer os valores padrão a serem utilizados para essas propriedades não definidas nas seções route individuais.

A seção global inicia com uma linha contendo os caracteres `[global]` e encerra quando a primeira seção route é iniciada. A seção global deve preceder todas as seções route no arquivo. Cada seção route inicia com uma linha contendo os caracteres `[route]` e encerra quando a seção route seguinte é iniciada, ou quando o fim do arquivo de configuração é alcançado.

Os nomes de palavra-chave desconhecidos (isto é, pares de nome/valor em que o nome não é um daqueles definidos neste documento) são ignorados. Se um par de nome/valor que aparece em uma seção route tiver um nome reconhecido, porém um valor inválido (por exemplo `MinConnectionThreads=x` ou `HTTP=unsure`), essa rota será desativada (isto é, não atenderá quaisquer conexões de entradas). Se um par de nome/valor que aparece na seção global tiver um nome reconhecido, porém um valor inválido, todas as rotas serão desativadas e o MQIPT não será iniciado. Onde uma propriedade é listada com os valores `true` e `false`, é possível utilizar qualquer mistura de letras maiúsculas e minúsculas.

Resumo de Propriedades

A Tabela 4 na página 55 mostra:

- Todas as propriedades
- Se a propriedade se aplica à seção global, à seção route, ou a ambas
- Valores padrão

Se uma propriedade estiver ausente nas seções route e global, serão utilizados os padrões mostrados na tabela.

Tabela 4. Resumo de propriedades de configuração

Nome da propriedade	Global	Route	Padrão
AccessPW	sim		<null>
Active	sim	sim	true
ClientAccess	sim	sim	false
CommandPort	sim		<null>[1]
ConnectionLog	sim		true
Destination		sim	<null>
DestinationPort		sim	1414
HTTP[6,7]	sim	sim	false
HTTPChunking[1]	sim	sim	false
HTTPProxy[1]	sim	sim	<null>
HTTPProxyPort[1]	sim	sim	8080
IdleTimeout	sim	sim	0
ListenerPort		sim	<null>
LogDir (válido apenas para MQIPTServlet)			<null>
MaxConnectionThreads	sim	sim	100
MaxLogFileSize	sim		50
MinConnectionThreads	sim	sim	5
Name		sim	<null>
NDAdvisor	sim	sim	false
NDAdvisorReplaceMode[4]	sim	sim	false
QMgrAccess	sim	sim	true
QoS (pode ser utilizada apenas no Linux)	sim	sim	false
QosToCaller[9]	sim	sim	1
QosToDest[9]	sim	sim	1
RemoteShutdown	sim		false
SecurityManager	sim		false
SecurityManagerPolicy	sim		<null>
ServletClient[1]	sim	sim	false
SocksClient	sim	sim	false
SocksProxyHost[8]	sim	sim	<null>
SocksProxyPort[8]	sim	sim	1080
SocksServer[7]	sim	sim	false
SSLClient	sim	sim	false
SSLClientCipherSuites[2]	sim	sim	<null>
SSLClientConnectTimeout[2]	sim	sim	30
SSLClientDN_C[2]	sim	sim	*[5]
SSLClientDN_CN[2]	sim	sim	*[5]
SSLClientDN_L[2]	sim	sim	*[5]
SSLClientDN_O[2]	sim	sim	*[5]
SSLClientDN_OU[2]	sim	sim	*[5]

Tabela 4. Resumo de propriedades de configuração (continuação)

Nome da propriedade	Global	Route	Padrão
SSLClientDN_ST[2]	sim	sim	*[5]
SSLClientKeyRing[2]	sim	sim	<null>
SSLClientKeyRingPW[2]	sim	sim	<null>
SSLProxyMode	sim	sim	false
SSLServer[6]	sim	sim	false
SSLServerAskClientAuth[3]	sim	sim	false
SSLServerCipherSuites[3]	sim	sim	<null>
SSLServerDN_C[3]	sim	sim	*[5]
SSLServerDN_CN[3]	sim	sim	*[5]
SSLServerDN_L[3]	sim	sim	*[5]
SSLServerDN_O[3]	sim	sim	*[5]
SSLServerDN_OU[3]	sim	sim	*[5]
SSLServerDN_ST[3]	sim	sim	*[5]
SSLServerKeyRing[3]	sim	sim	<null>
SSLServerKeyRingPW[3]	sim	sim	<null>
Trace	sim	sim	0
UriName (Consulte a página 64 para obter detalhes sobre as definições padrão.)[1]	sim	sim	

Notas:

1. Defina HTTP como true para que estas propriedades entrem em vigor.
2. Defina SSLClient como true para que estas propriedades entrem em vigor.
3. Defina SSLServer como true para que estas propriedades entrem em vigor.
4. Defina NDAdvisor como true para que estas propriedades entrem em vigor.
5. O símbolo "*" representa um caractere curinga.
6. HTTP e SSLServer não podem ser utilizados juntos. A propriedade HTTP é utilizada apenas para definir a conexão de avanço. Os dados de entrada no ListenerPort são detectados automaticamente; definir SSLServer ocasiona uma exceção de tempo de execução.
7. HTTP e SocksServer não podem ser utilizados juntos. A propriedade HTTP é utilizada apenas para definir a conexão de avanço. Os dados de entrada no ListenerPort são detectados automaticamente; definir SocksServer ocasiona uma exceção de tempo de execução.
8. Defina SocksClient como true para que estas propriedades entrem em vigor.
9. Defina QoS como true para que estas propriedades entrem em vigor.

Informações de Referência da Seção Global

A seção global pode conter as seguintes propriedades e todas as propriedades em "Informações de Referência da Seção Route" na página 57, separadamente de ListenerPort, Destination, DestinationPort e Name.

AccessPW

A senha utilizada quando um Controlador Administrativo envia comandos para o MQIPT. Se esta propriedade não estiver presente ou estiver em branco, não ocorrerá verificação.

CommandPort
A porta TCP/IP na qual o MQIPT atende aos comandos de configuração do utilitário `mqiptAdmin` ou do Cliente Administrativo. A porta do comando pode ser alterada a partir do Cliente Administrativo da mesma maneira que qualquer outra propriedade. Observe que as propriedades de conexão não são alteradas por você. Quando você aplica a nova configuração ao MQIPT, o Cliente Administrativo altera as propriedades de conexão automaticamente.

Se a propriedade `CommandPort` não estiver presente, o MQIPT não atenderá aos comandos de configuração. Se você desejar atender na porta do comando, é aconselhável utilizar 1881. O Cliente Administrativo não possui um valor padrão para CommandPort, mas 1881 é o valor padrão quando são utilizados comandos de modo de linha.

ConnectionLog
Pode ser `true` ou `false`. Quando true, MQIPT registra todas as tentativas de conexão (bem-sucedidas, ou não) no subdiretório `logs` e os eventos de conexão no arquivo `mqiptYYYYMMDDHHmmSS.log`. O valor padrão é true. Quando esta propriedade é alterada de `true` para `false`, o MQIPT fecha o log de conexão existente e cria um outro. O novo log será utilizado quando a propriedade for redefinida como `true`.

MaxLogFileSize
O tamanho máximo (especificado em KB) do arquivo de log de conexão `mqipt.log`. Quando o tamanho do arquivo `mqipt.log` aumenta acima deste máximo, uma cópia de backup `mqipt.back` é produzida e um novo arquivo é iniciado. Apenas um arquivo backup é mantido; cada vez que um arquivo de log principal fica cheio, os backups anteriores são apagados. O valor padrão é 50; o valor mínimo permitido é 5.

RemoteShutDown
Pode ser `true` ou `false`. Quando true (e quando há uma porta do comando), o MQIPT é encerrado sempre que um comando STOP é recebido na porta do comando. O valor padrão é false.

SecurityManager
Defina esta propriedade como true para ativar o Java Security Manager para esta instância do MQIPT. Isso conta com a concessão de permissões corretas. Consulte “Java Security Manager” na página 22 para obter mais informações. O valor padrão desta propriedade é false.

SecurityManagerPolicy
O nome completo de um arquivo de política. Se esta propriedade não for definida, apenas os arquivos de política padrão do sistema e do usuário serão utilizados. Se o Java Security Manager já estiver ativado, as alterações nesta propriedade não terão efeito até que o Java Security Manager tenha sido desativado e reativado.

Informações de Referência da Seção Route

A seção route pode conter as seguintes propriedades:

Active
A rota aceita conexões de entrada apenas se o valor de Active for definido como `true`. Isso significa que você pode encerrar temporariamente o acesso ao destino, definindo `Active=false`, sem ter que excluir a seção route do arquivo de configuração. Se você alterar esta propriedade para `false`, a rota será parada quando um comando REFRESH for emitido. Todas as conexões para esta rota serão encerradas.

ClientAccess
A rota permite conexões de entrada do canal do cliente apenas se o valor de ClientAccess for definido como `true`. Observe que você pode configurar potencialmente os MQIPTs para aceitar apenas pedidos de clientes, apenas pedidos do gerenciador de filas, ou ambos os tipos de pedido. Utilize esta propriedade juntamente com a propriedade QMgrAccess. Se você alterar esta propriedade para `false`, a rota será parada e iniciada novamente quando um comando REFRESH for emitido. Todas as conexões para esta rota serão encerradas.

Destination
O nome do host (ou endereço IP decimal pontilhado) do gerenciador de filas (ou MQIPT subseqüente) ao qual esta rota será conectada. Cada seção route **deve** conter um valor explícito de Destination. Você pode ter várias seções route apontando para o mesmo Destination. Se uma alteração desta propriedade afetar uma rota, a rota será parada e iniciada novamente quando um comando REFRESH for emitido. Todas as conexões para esta rota serão encerradas.

DestinationPort
A porta no host de Destination ao qual esta rota será conectada. É válida para mais de uma rota, para apontar na mesma combinação de Destination e DestinationPort. Cada seção route **deve** conter um valor explícito de DestinationPort. Se uma alteração desta propriedade afetar uma rota, a rota será parada e iniciada novamente quando um comando REFRESH for emitido. Todas as conexões para esta rota serão encerradas.

HTTP
Defina como `true` para rotas responsáveis por fazer pedidos de encapsulamento HTTP de transmissão (isto é, se comunicar com outro MQIPT através do HTTP). Defina como `false` para rotas direcionadas em gerenciadores de filas do WebSphere MQ. Se você alterar esta propriedade para `false`, a rota será parada e iniciada novamente quando um comando REFRESH for emitido. Todas as conexões para esta rota serão encerradas. Para utilizar a fragmentação HTTP, defina esta propriedade como `true`. Esta propriedade não pode ser utilizada com:

- QoS
- SocksClient
- SSLClient
- SSLProxyMode

HTTPChunking
Defina como `true` para rotas responsáveis por fazer pedidos de transmissão utilizando o encapsulamento HTTP com fragmentação. A propriedade HTTP também deve ser definida como `true`. Defina como `false` quando você não estiver utilizando a fragmentação HTTP. Se você alterar esta propriedade para `false`, a rota será parada e iniciada novamente quando um comando REFRESH for emitido. Todas as conexões para esta rota serão encerradas.

HTTPProxy
O nome do host (ou endereço IP decimal pontilhado) do proxy HTTP utilizado por todas as conexões desta rota. Se você alterar esta propriedade, a rota será parada e iniciada novamente quando um comando REFRESH for emitido. Todas as conexões para esta rota serão encerradas.

HTTPProxyPort
O endereço da porta a ser utilizado no proxy HTTP. O valor padrão é `8080`. Se

você alterar esta propriedade, a rota será parada e iniciada novamente quando um comando REFRESH for emitido. Todas as conexões para esta rota serão encerradas.

IdleTimeout
O tempo, em minutos, após o qual uma conexão inativa é encerrada. Observe que o gerenciador de filas para os canais de gerenciador de filas também possuem a propriedade DISCINT. Se você definir o parâmetro IdleTimeout, tome nota de DISCINT. Um valor 0 indica sem tempo limite inativo. As alterações desta propriedade entram em vigor apenas quando a rota é iniciada novamente.

ListenerPort
O número da porta na qual deve atender a pedidos de entrada. Cada seção route **deve** conter um valor explícito de ListenerPort; além disso, os valores de ListenerPort definidos em cada seção devem ser distintos. Qualquer número de porta válido pode ser utilizado, incluindo portas 80 e 443, desde que as portas escolhidas já não estejam sendo utilizadas por outro atendente TCP/IP em execução no mesmo host.

LogDir
Utilize esta propriedade para definir o nome do diretório para os arquivos de log e de rastreio. As alterações nesta propriedade só entrarão em vigor depois que MQIPTServlet tiver sido parado e iniciado novamente. O valor padrão é <null>. Esta propriedade é válida apenas para MQIPTServlet

MaxConnectionThreads
O número máximo de threads de conexão e, portanto, o número máximo de conexões simultâneas que podem ser manipuladas por esta rota. Se este limite é alcançado, o valor de `MaxConnectionThreads` também indica o número de conexões que serão enfileiradas assim que todos os threads estiverem em uso. Excedendo a esse número, os pedidos de conexão subseqüentes são recusados. O valor mínimo permitido é maior que 1 ou o valor de MinConnectionThreads. Se uma alteração desta propriedade afetar uma rota, o novo valor será utilizado quando o comando REFRESH for emitido. Todas as conexões captam o novo valor imediatamente. A rota não será encerrada.

MinConnectionThreads
O número mínimo de threads de conexão (threads para manipular conexões de entrada nesta rota). Este é o número de threads alocados quando a rota é iniciada, e o número total de threads alocados não cai abaixo deste valor durante o tempo em que a rota está ativa. O valor mínimo permitido é 0 e deve ser menor que o especificado para MaxConnectionThreads. As alterações desta propriedade entram em vigor apenas quando a rota é iniciada novamente.

Name
Um nome opcional para ajudar a identificar a rota. Ele aparece nas mensagens do console e informações de rastreio. As alterações desta propriedade entram em vigor apenas quando a rota é iniciada novamente.

NDAdvisor
Defina esta propriedade como `true` para rotas gerenciadas pelo Network Dispatcher para permitir que a rota responda a pedidos do consultor personalizado. Se você alterar esta propriedade para `false`, a rota será parada quando um comando REFRESH for emitido. Todas as conexões para esta rota serão encerradas. Para utilizar a propriedade NDAdvisorReplaceMode, defina esta propriedade como `true`.

NDAdvisorReplaceMode
Defina esta propriedade como `true` para utilizar o modo "substituir" do consultor personalizado do Network Dispatcher. Você deve ter iniciado o `consultor personalizado mqipt_replace` para o endereço de ListenerPort desta rota. Defina esta propriedade para `false` para utilizar o modo "normal". Você deve definir a propriedade NDAdvisor como `true` para utilizar esta propriedade.

QMgrAccess
A rota permite conexões de entrada do canal do gerenciador de filas (por exemplo canais do emissor) apenas se o valor de QMgrAccess for definido para o valor `true`. Se você alterar esta propriedade para `false`, a rota será parada quando um comando REFRESH for emitido. Todas as conexões para esta rota serão encerradas.

QoS
Defina esta propriedade como `true` para ativar a Qualidade de Serviço para todas as conexões nesta rota. Esta propriedade só pode ser ativada no Linux. Se você alterar esta propriedade, a rota será parada e iniciada novamente quando um comando REFRESH for emitido. Todas as conexões para esta rota serão encerradas. Esta propriedade não pode ser utilizada com:

- HTTP
- SSLClient
- SSLProxyMode
- SSLServer

QosToCaller
Esta propriedade define a prioridade de todo o tráfego da máquina do MQIPT para o iniciador da conexão. Defina a propriedade como `1` para prioridade baixa, `2` para prioridade média e `3` para prioridade alta (o padrão é `1`). Se você alterar esta propriedade (e QoS for definida como `true`), a rota será parada e iniciada novamente quando um comando REFRESH for emitido. Todas as conexões para esta rota serão encerradas

QosToDest
Esta propriedade define a prioridade de todo o tráfego da máquina do MQIPT para o destino da conexão (conforme definido pela propriedade Destination). Defina a propriedade como `1` para prioridade baixa, `2` para prioridade média `3` para prioridade alta (o padrão é `1`). Se você alterar esta propriedade (e QoS for definida como `true`), a rota será parada e iniciada novamente quando um comando REFRESH for emitido. Todas as conexões para esta rota serão encerradas

ServletClient
Defina esta propriedade como `true` ao conectar-se ao servlet do MQIPT. A propriedade HTTP também deve ser definida como `true`. Se você alterar esta propriedade (e HTTP é definido como `true`) a rota será parada e iniciada novamente quando um comando REFRESH for emitido.

SocksClient
Defina esta propriedade como `true` para fazer a rota agir como um cliente Socks e definir todas as conexões através do proxy Socks com as propriedades SocksProxyHost e SocksProxyPort. Se você alterar esta propriedade, a rota será parada e iniciada novamente quando um comando REFRESH for emitido. Todas as conexões para esta rota serão encerradas. Esta propriedade não pode ser utilizada com:

- HTTP

- SocksServer
- SSLClient
- SSLProxyMode

SocksProxyHost
O nome do host (ou endereço IP decimal pontilhado) do proxy Socks utilizado por todas as conexões desta rota. Se você alterar esta propriedade (e SocksClient é definido como `true`), a rota será parada e iniciada novamente quando um comando REFRESH for emitido. Todas as conexões para esta rota serão encerradas

SocksProxyPort
O endereço da porta a ser utilizado em um proxy Socks. O valor padrão é 1080. Se você alterar esta propriedade (e SocksClient é definido como `true`), a rota será parada e iniciada novamente quando um comando REFRESH for emitido. Todas as conexões para esta rota serão encerradas

SocksServer
Defina esta propriedade como `true` para fazer a rota agir como um proxy Socks e aceitar conexões do cliente de Socks. Se você alterar esta propriedade, a rota será parada e iniciada novamente quando um comando REFRESH for emitido. Todas as conexões para esta rota serão encerradas. Esta propriedade não pode ser utilizada com:

- SocksClient
- SSLProxyMode
- SSLServer

SSLClient
Defina esta propriedade como `true` para fazer a rota agir como um cliente SSL e fazer conexões SSL de saída. Definir `true` subentende-se que o destino é um outro MQIPT agindo como um servidor SSL. Se você alterar esta propriedade, a rota será parada e iniciada novamente quando um comando REFRESH for emitido. Todas as conexões para esta rota serão encerradas. Esta propriedade não pode ser utilizada com:

- HTTP
- QoS
- SSLProxyMode

SSLClientCipherSuites
O nome do conjunto de cifras do SSL a ser utilizado no lado do cliente SSL. Este pode ser um ou mais dos conjuntos de cifras suportados. Se você deixar em branco, o cliente SSL utilizará os conjuntos de cifras do SSLClientKeyRing suportados. Se você alterar esta propriedade, a rota será parada e iniciada novamente quando um comando REFRESH for emitido. Todas as conexões para esta rota serão encerradas.

SSLClientConnectTimeout
Defina esta propriedade para o número de segundos que um cliente SSL aguardará até que uma conexão SSL seja aceita. Se você alterar esta propriedade, a rota será parada e iniciada novamente quando um comando REFRESH for emitido. A rota não será encerrada.

SSLClientDN_C
Utilize esta propriedade para aceitar os certificados recebidos do servidor SSL com este nome de país. O nome pode conter um asterisco (*) como prefixo ou sufixo para estender seu escopo. Se você não especificar esta propriedade, subentende-se “todos os nomes de companhia”. Se você alterar esta

propriedade, a rota será parada e iniciada novamente quando um comando REFRESH for emitido. Todas as conexões para esta rota serão encerradas.

SSLClientDN_CN
Utilize esta propriedade para aceitar os certificados recebidos do servidor SSL com este nome comum. O nome pode conter um asterisco (*) como prefixo ou sufixo para estender seu escopo. Se você não especificar esta propriedade, subentende-se “todos os nomes comuns”. Se você alterar esta propriedade, a rota será parada e iniciada novamente quando um comando REFRESH for emitido. Todas as conexões para esta rota serão encerradas.

SSLClientDN_L
Utilize esta propriedade para aceitar os certificados recebidos do servidor SSL com esta localização. O nome pode conter um asterisco (*) como prefixo ou sufixo para estender seu escopo. Se você não especificar esta propriedade, subentende-se “todas as localizações”. Se você alterar esta propriedade, a rota será parada e iniciada novamente quando um comando REFRESH for emitido. Todas as conexões para esta rota serão encerradas.

SSLClientDN_O
Utilize esta propriedade para aceitar os certificados recebidos do servidor SSL com esta organização. O nome pode conter um asterisco (*) como prefixo ou sufixo para estender seu escopo. Se você não especificar esta propriedade, subentende-se “todas as organizações”. Se você alterar esta propriedade, a rota será parada e iniciada novamente quando um comando REFRESH for emitido. Todas as conexões para esta rota serão encerradas.

SSLClientDN_OU
Utilize esta propriedade para aceitar os certificados recebidos do servidor SSL com esta organizational unit. O nome pode conter um asterisco (*) como prefixo ou sufixo para estender seu escopo. Se você não especificar esta propriedade, subentende-se “todas as organizational units”. Se você alterar esta propriedade, a rota será parada e iniciada novamente quando um comando REFRESH for emitido. Todas as conexões para esta rota serão encerradas.

SSLClientDN_ST
Utilize esta propriedade para aceitar os certificados recebidos do servidor SSL com este estado. O nome pode conter um asterisco (*) como prefixo ou sufixo para estender seu escopo. Se você não especificar esta propriedade, subentende-se “todos os estados”. Se você alterar esta propriedade, a rota será parada e iniciada novamente quando um comando REFRESH for emitido. Todas as conexões para esta rota serão encerradas.

SSLClientKeyRing
O nome completo do arquivo de conjunto de chaves que contém o certificado de cliente. Em **plataformas Windows**, utilize uma barra dupla invertida (\\) como o separador de arquivo. Você deve especificar SSLClientKeyRing se definir SSLClient como `true`. Se você alterar esta propriedade, a rota será parada e iniciada novamente quando um comando REFRESH for emitido. Todas as conexões para esta rota serão encerradas.

SSLClientKeyRingPW
O nome completo do arquivo que contém a senha para abrir o conjunto de chaves do cliente. Em **plataformas Windows**, utilize uma barra dupla invertida (\\) como o separador de arquivo. Você deve especificar SSLClientKeyRingPW se definir SSLClient como `true`. Se você alterar esta propriedade, a rota será parada e iniciada novamente quando um comando REFRESH for emitido. Todas as conexões para esta rota serão encerradas.

SSLProxyMode
Defina esta propriedade como `true` para ativar a rota para aceitar apenas pedidos de conexão do cliente SSL e encapsular o pedido diretamente no destino. Se você alterar esta propriedade, a rota será parada e iniciada novamente quando um comando REFRESH for emitido. Todas as conexões para esta rota serão encerradas. Esta propriedade não pode ser utilizada com:

- HTTP
- QoS
- SocksClient
- SSLClient
- SSLServer

SSLServer
Defina esta propriedade como `true` para fazer a rota agir como um servidor SSL e aceitar conexões SSL de entrada. Definir `true` subentende-se que o originador da chamada é um outro MQIPT agindo como um cliente SSL. Se você alterar esta propriedade, a rota será parada e iniciada novamente quando um comando REFRESH for emitido. Todas as conexões para esta rota serão encerradas. Esta propriedade não pode ser utilizada com:

- QoS
- SocksServer
- SSLProxyMode

SSLServerAskClientAuth
Utilize esta propriedade para solicitar autenticação do cliente SSL pelo servidor SSL. O cliente SSL deve ter seu próprio certificado para enviar ao servidor SSL. O certificado é recuperado do arquivo de conjunto de chaves. Se você alterar esta propriedade, a rota será parada e iniciada novamente quando um comando REFRESH for emitido. Todas as conexões para esta rota serão encerradas.

SSLServerCipherSuites
O nome do conjunto de cifras do SSL a ser utilizado no lado do servidor SSL. Este pode ser um ou mais dos conjuntos de cifras suportados. Se você deixa em branco, o servidor SSL utiliza os conjuntos de cifras do SSLServerKeyRing suportados. Se você alterar esta propriedade, a rota será parada e iniciada novamente quando um comando REFRESH for emitido. Todas as conexões para esta rota serão encerradas.

SSLServerDN_C
Utilize esta propriedade para aceitar os certificados recebidos do cliente SSL com este nome de país. O nome pode conter um asterisco (*) como prefixo ou sufixo para estender seu escopo. Se você não especifica esta propriedade, subentende-se “todos os nomes de companhia”. Se você alterar esta propriedade, a rota será parada e iniciada novamente quando um comando REFRESH for emitido. Todas as conexões para esta rota serão encerradas.

SSLServerDN_CN
Utilize esta propriedade para aceitar os certificados recebidos do cliente SSL com este nome comum. O nome pode conter um asterisco (*) como prefixo ou sufixo para estender seu escopo. Se você não especificar esta propriedade, subentende-se “todos os nomes comuns”. Se você alterar esta propriedade, a rota será parada e iniciada novamente quando um comando REFRESH for emitido. Todas as conexões para esta rota serão encerradas.

SSLServerDN_L
Utilize esta propriedade para aceitar os certificados recebidos do cliente SSL

com esta localização. O nome pode conter um asterisco (*) como prefixo ou sufixo para estender seu escopo. Se você não especificar esta propriedade, subentende-se “todas as localizações”. Se você alterar esta propriedade, a rota será parada e iniciada novamente quando um comando REFRESH for emitido. Todas as conexões para esta rota serão encerradas.

SSLServerDN_O
Utilize esta propriedade para aceitar os certificados recebidos do cliente SSL com esta organização. O nome pode conter um asterisco (*) como prefixo ou sufixo para estender seu escopo. Se você não especificar esta propriedade, subentende-se “todas as organizações”. Se você alterar esta propriedade, a rota será parada e iniciada novamente quando um comando REFRESH for emitido. Todas as conexões para esta rota serão encerradas.

SSLServerDN_OU
Utilize esta propriedade para aceitar os certificados recebidos do cliente SSL com esta organizational unit. O nome pode conter um asterisco (*) como prefixo ou sufixo para estender seu escopo. Se você não especificar esta propriedade, subentende-se “todas as organizational units”. Se você alterar esta propriedade, a rota será parada e iniciada novamente quando um comando REFRESH for emitido. Todas as conexões para esta rota serão encerradas.

SSLServerDN_ST
Utilize esta propriedade para aceitar os certificados recebidos do cliente SSL neste estado. O nome pode conter um asterisco (*) como prefixo ou sufixo para estender seu escopo. Se você não especificar esta propriedade, subentende-se “todos os estados”. Se você alterar esta propriedade, a rota será parada e iniciada novamente quando um comando REFRESH for emitido. Todas as conexões para esta rota serão encerradas.

SSLServerKeyRing
O nome completo do arquivo de conjunto de chaves que contém o certificado de servidor. Em **plataformas Windows**, utilize uma barra dupla invertida (\\) como o separador de arquivo. Você deve especificar SSLServerKeyRing se definir SSLServer como `true`. Se você alterar esta propriedade, a rota será parada e iniciada novamente quando um comando REFRESH for emitido. Todas as conexões para esta rota serão encerradas.

SSLServerKeyRingPW
O nome completo do arquivo que contém a senha para abrir o conjunto de chaves do servidor. Em **plataformas Windows**, utilize uma barra dupla invertida (\\) como o separador de arquivo. Você deve especificar SSLServerKeyRingPW se definir SSLServer como `true`. Se você alterar esta propriedade, a rota será parada e iniciada novamente quando um comando REFRESH for emitido. Todas as conexões para esta rota serão encerradas.

Trace
O nível de rastreio requerido pode ser especificado por um inteiro no intervalo 0-5. Um valor 0 significa que não há rastreio; 5 solicita um rastreio completo.

Se uma alteração desta propriedade afetar uma rota, o novo valor é utilizado quando o comando REFRESH for emitido. Todas as conexões captam o novo valor imediatamente. A rota não será encerrada.

UriName
Esta propriedade pode ser utilizada para alterar o nome do Uniform Resource Identifier do recurso ao utilizar um proxy HTTP ou o servlet do MQIPT, embora os valores padrão sejam adequados para a maioria das configurações. O padrão para o proxy HTTP é:

```
HTTP://<destination>:<destination_port>/mqipt
```

O padrão para o servlet do MQIPT é:

```
HTTP://<destination>:<destination_port>/MQIPTServlet
```

Se você alterar esta propriedade (e HTTP ou ServletClient são definidos como `True`, a rota será parada e iniciada novamente quando um comando REFRESH for emitido.

Capítulo 10. Iniciando o internet pass-thru

Este capítulo ajudará você a iniciar o MQIPT: ele o conduz pela instalação de algumas configurações simples para confirmar que o produto foi instalado com êxito.

Este capítulo contém as seguintes seções:

Suposições

Para cada exemplo, fazemos as seguintes suposições:

- Você está utilizando o Windows NT, (embora estes exemplos sejam executados em qualquer uma das plataformas suportadas)
- Você está familiarizado com a definição de gerenciadores de filas, filas e canais no WebSphere MQ
- Você já instalou um cliente e um servidor do WebSphere MQ
- O MQIPT está instalado em um diretório denominado `C:\mqipt` (no Windows)
- O cliente, o servidor e cada MQIPT são instalados em máquinas separadas
- Você está familiarizado com a colocação de mensagens em uma fila utilizando o comando `amqsputc`
- Você está familiarizado com a obtenção de mensagens de uma fila utilizando o comando `amqsgetc`

No servidor do WebSphere MQ, você fez o seguinte:

- Definiu um gerenciador de filas denominado `MQIPT.QM1`
- Definiu um canal de conexão do servidor denominado `MQIPT.CONN.CHANNEL`
- Definiu uma fila local denominada `MQIPT.LOCAL.QUEUE`
- Iniciou um atendente TCP/IP para o `MQIPT.QM1` na porta 1414

Apenas um aplicativo pode atender em um determinado endereço de porta na mesma máquina. Se a porta 1414 já estiver sendo utilizada, escolha um endereço de porta livre e substitua-o nos exemplos.

Depois de feito isso, você pode testar a rota do Cliente do WebSphere MQ para o gerenciador de filas, colocando uma mensagem na fila local do gerenciador de filas com o comando `amqsputc` e recuperando-a com o comando `amqsgetc`.

Configurações de Exemplo

Os exemplos a seguir são representados como diagramas e instruções passo a passo, você pode utilizar as caixas de visto à direita de cada diagrama para acompanhar o progresso do exemplo. Em alguns exemplos, é necessário editar o arquivo `mqipt.conf`, que está localizado no diretório inicial do MQIPT.

Antes de iniciar, assegure-se de fazer o seguinte:

- Copie `mqiptSample.conf` para `mqipt.conf`
- Edite o `mqipt.conf` e exclua todas as rotas
- Altere a entrada de `ClientAccess` para `True`
- Altere o Destination de `mqserver.company2.com` para aquele do gerenciador de filas
- Altere o endereço de DestinationPort para aquele utilizado pelo gerenciador de filas
- Leia "Suposições" na página 67

Teste de Verificação de Instalação

Esta é uma configuração simples para assegurar que o MQIPT tenha sido instalado corretamente.

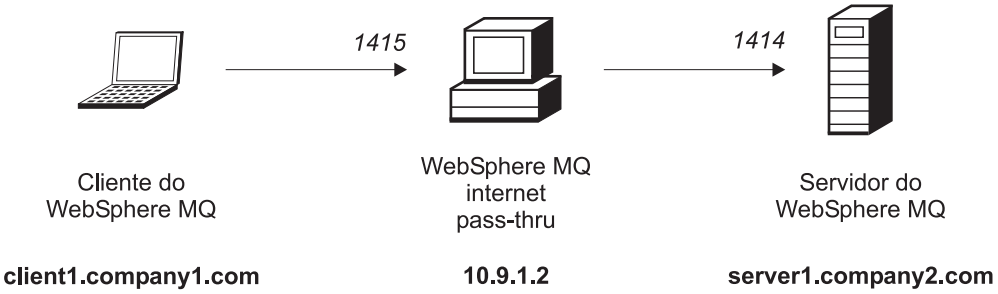

Figura 10. Diagrama de rede do IVT

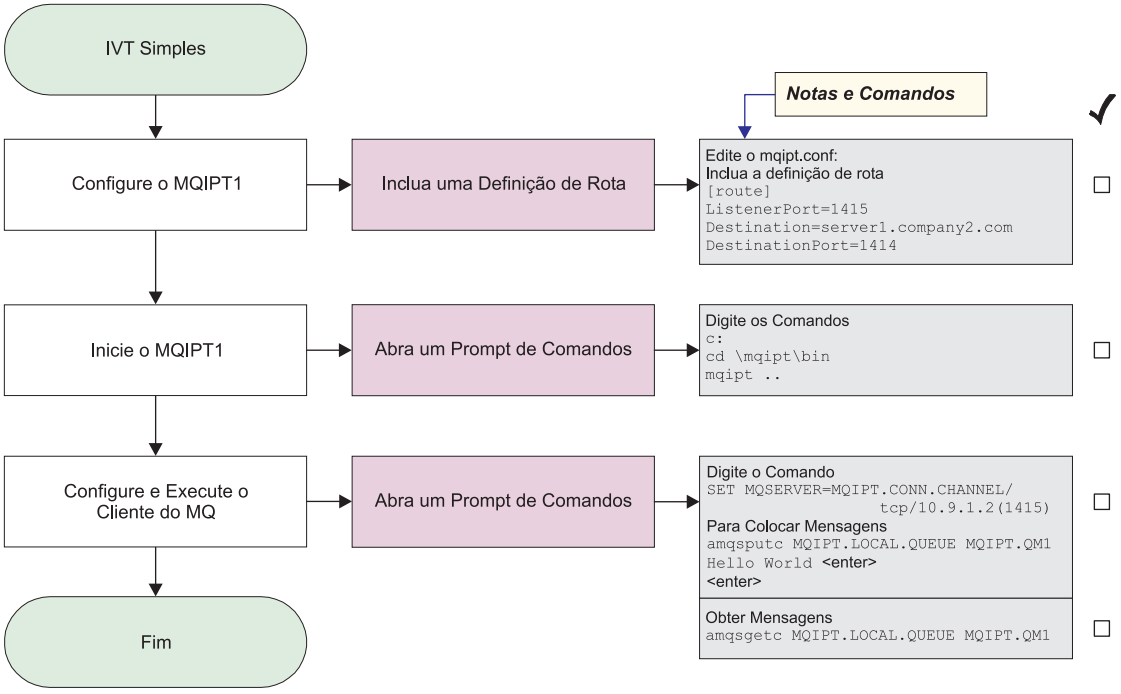

Figura 11. Configuração do IVT

Antes de iniciar:

1. Configure o MQIPT1

   Edite o `mqipt.conf` e inclua uma definição de rota:

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

2. Inicie o MQIPT1

   Abra um prompt de comandos e digite o seguinte:

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

   A seguinte mensagem indica uma conclusão bem-sucedida:

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

3. Em um prompt de comandos na máquina do cliente do WebSphere MQ, digite o seguinte:

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

4. Coloque uma mensagem utilizando:

   ```
   amqsputc MQIPT.LOCAL.QUEUE MQIPT1.QM1
   Hello world <enter>
    <enter>
   ```

5. Obtenha a mensagem utilizando:

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

Você verá ″Hello world″.

Autenticação do Servidor SSL

Neste exemplo, você testará uma conexão SSL utilizando o certificado de teste de amostra (arquivo de conjunto de chaves `sslsample.pfx`) conectando um cliente do WebSphere MQ a um servidor do WebSphere MQ através de dois MQIPTs. Durante o protocolo de reconhecimento SSL, o servidor enviará seu certificado de teste para o cliente. O cliente utilizará sua cópia do certificado (com o flag trust-as-peer) para autenticar o servidor. Um conjunto de cifras padrão, SSL_RSA_WITH_RC4_128_MD5, será utilizado. (Baseia-se no `mqipt.conf` criado em "Teste de Verificação de Instalação" na página 68). Para obter detalhes sobre como criar um certificado de teste para utilizar neste exemplo, consulte "Criando Certificados de Teste SSL" na página 89.

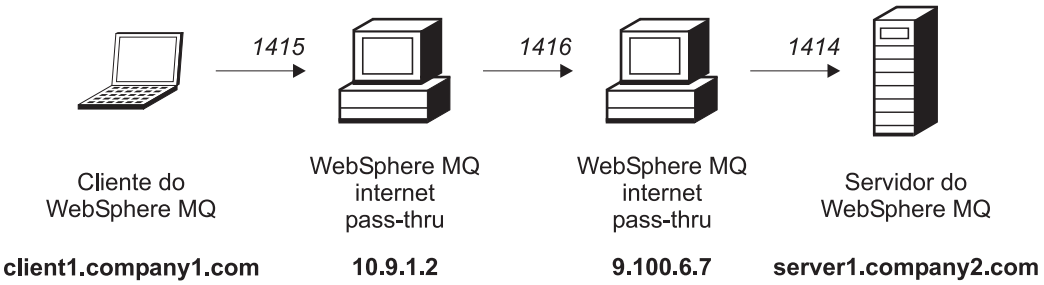

Figura 12. Diagrama de rede do servidor SSL

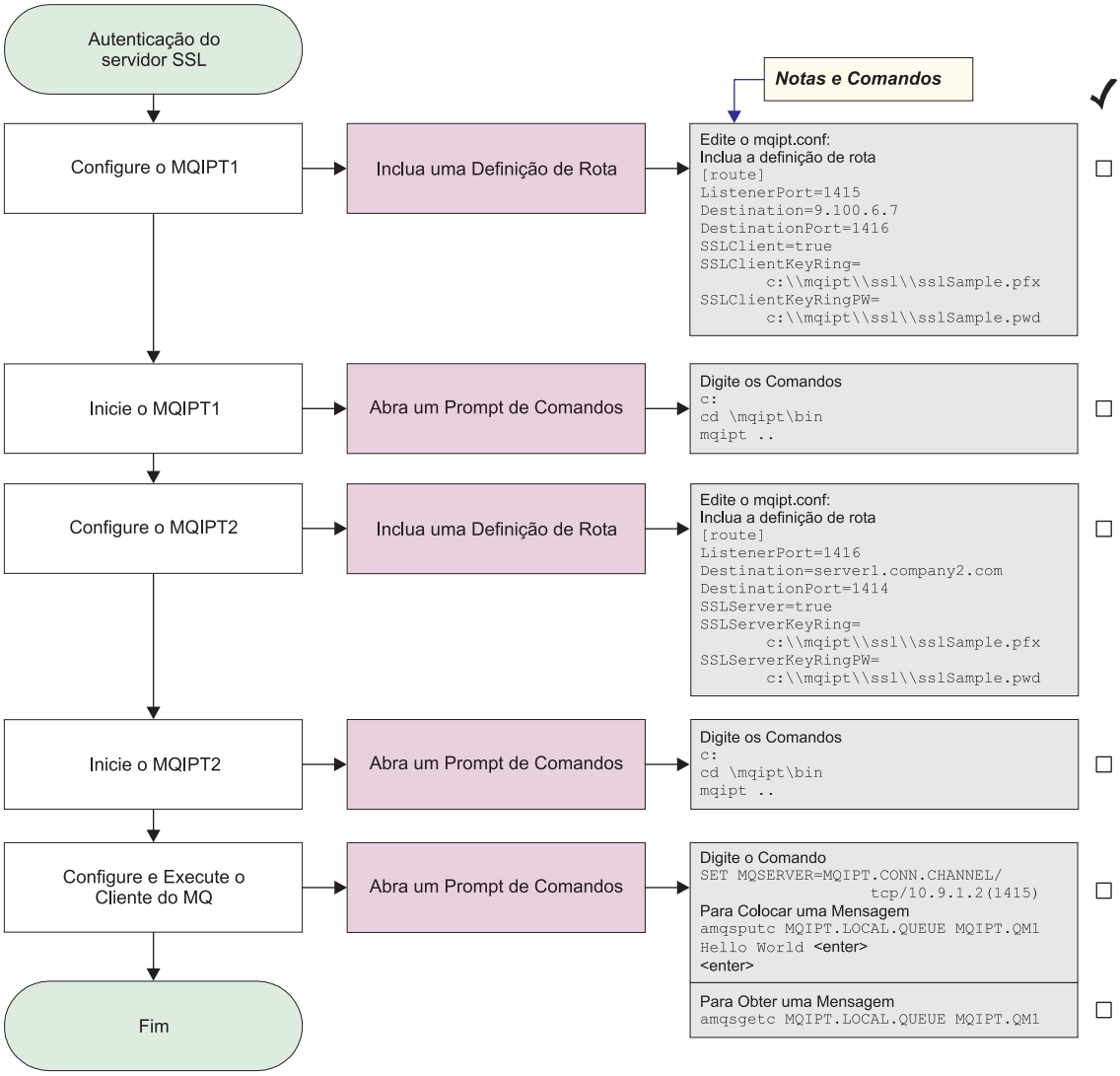

Figura 13. Autenticação do servidor SSL

1. Configure o MQIPT1

   Edite o `mqipt.conf` e inclua uma definição de rota:

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

2. Inicie o MQIPT1

   Abra um prompt de comandos e digite o seguinte:

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

   A seguinte mensagem indica uma conclusão bem-sucedida:

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

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

3. Configure o MQIPT2

   Edite o `mqipt.conf` e inclua uma definição de rota:

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

4. Inicie o MQIPT2

   Abra um prompt de comandos e digite o seguinte:

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

   A seguinte mensagem indica uma conclusão bem-sucedida:

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

5. Em um prompt de comandos na máquina do cliente do WebSphere MQ, digite o seguinte:

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

6. Coloque uma mensagem utilizando:

   ```
   amqsputc MQIPT.LOCAL.QUEUE MQIPT1.QM1
   Hello world <enter>
    <enter>
   ```

7. Obtenha a mensagem utilizando:

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

Você verá ″Hello world″.

Autenticação do Cliente SSL

Neste exemplo, você testará uma conexão SSL com o certificado de teste de amostra. Isso executará a autenticação do servidor e do cliente. Durante o protocolo de reconhecimento SSL, o servidor enviará seu certificado de teste para o cliente. O cliente utilizará sua cópia do certificado, com o flag trust-as-peer, para autenticar o servidor. O cliente envia seu certificado de teste para o servidor. O servidor utilizará sua cópia do certificado, com o flag trust-as-peer, para autenticar o cliente. Um conjunto de cifras padrão, SSL_RSA_WITH_RC4_128_MD5, será

utilizado. (Baseia-se no `mqipt.conf` criado em "Teste de Verificação de Instalação" na página 68).

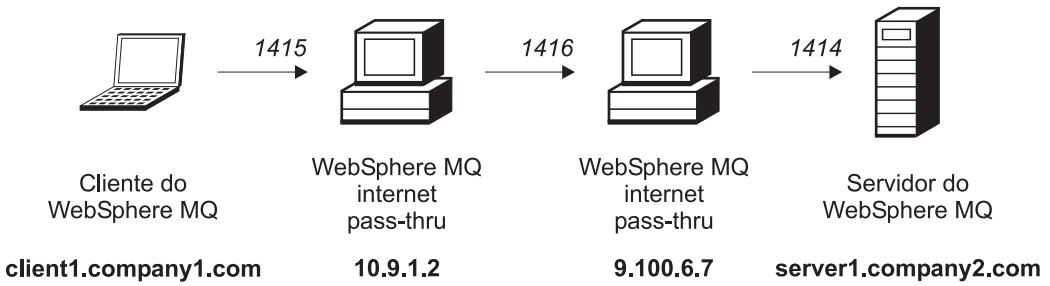

Figura 14. Diagrama de rede do cliente SSL

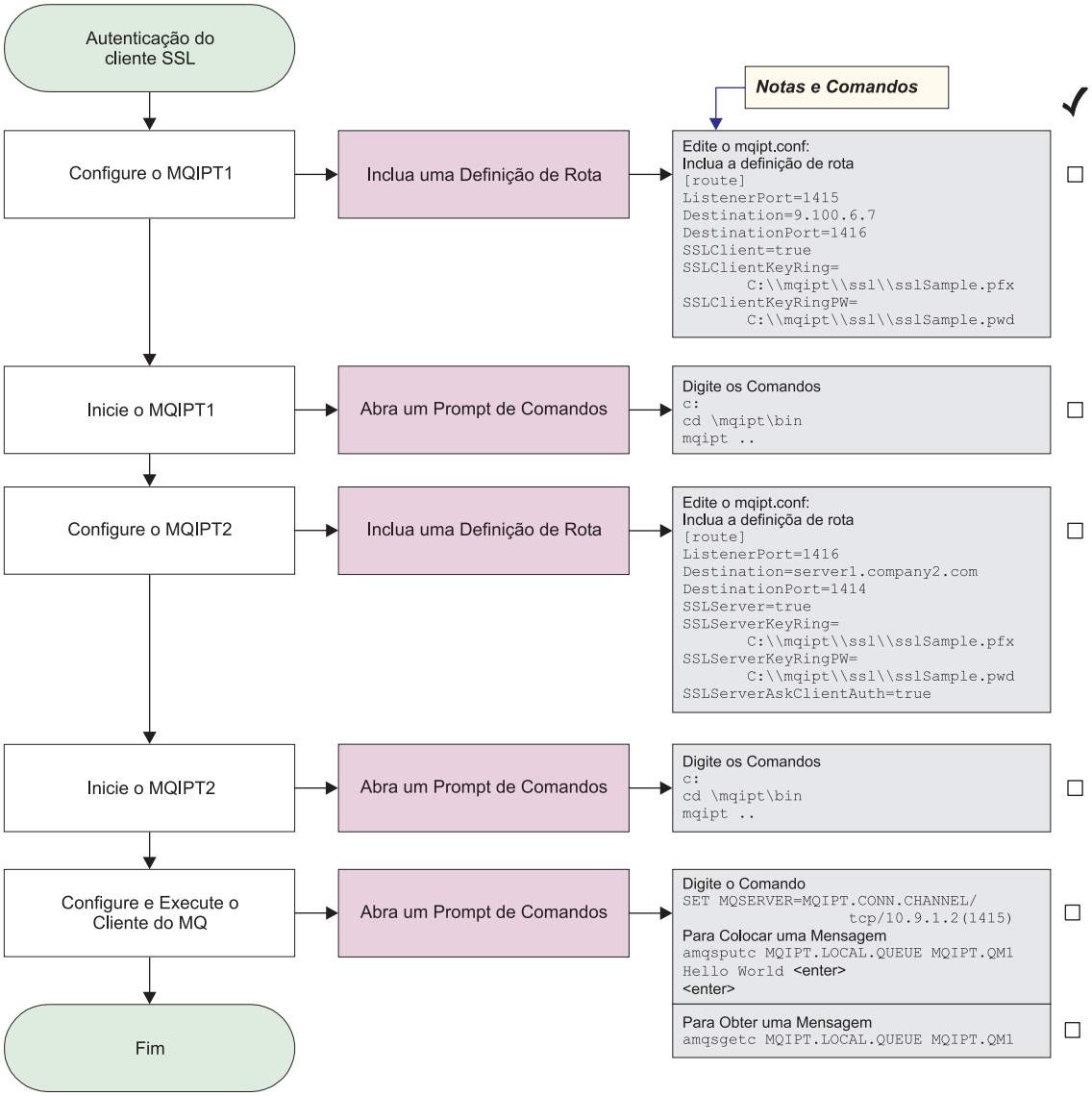

Figura 15. autenticação do cliente SSL

1. Configure o MQIPT1

   Edite o `mqipt.conf` e inclua uma definição de rota:

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

2. Inicie o MQIPT1

   Abra um prompt de comandos e digite o seguinte:

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

   A seguinte mensagem indica uma conclusão bem-sucedida:

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

3. Configure o MQIPT2

   Edite o `mqipt.conf` e inclua uma definição de rota:

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

4. Inicie o MQIPT2

   Abra um prompt de comandos e digite o seguinte:

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

   A seguinte mensagem indica uma conclusão bem-sucedida:

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

5. Em um prompt de comandos na máquina do cliente do WebSphere MQ, digite o seguinte:

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

6. Coloque uma mensagem utilizando:

```
amqsputc MQIPT.LOCAL.QUEUE MQIPT1.QM1
Hello world <enter>
 <enter>
```

7. Obtenha a mensagem utilizando:

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

Você verá ″Hello world″.

Configuração do Proxy HTTP

Neste exemplo, você testará a conexão utilizando um proxy HTTP (IBM Caching Proxy). O CP deve estar no nível 3.6 ou superior, e você também deve verificar o seguinte:

- `ProxyPersistance` deve ser `on`. Isso permite conexões persistentes
- `MaxPersistRequest` 5000. Este é o número de pedidos permitidos em uma única conexão antes da conexão ser interrompida
- `PersistTimeout` 12hrs. Este é o tempo permitido para a existência da conexão

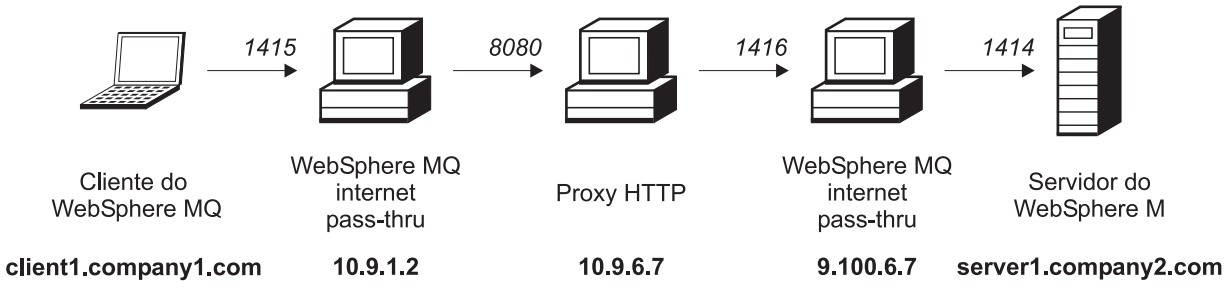

Figura 16. Diagrama de rede proxy HTTP

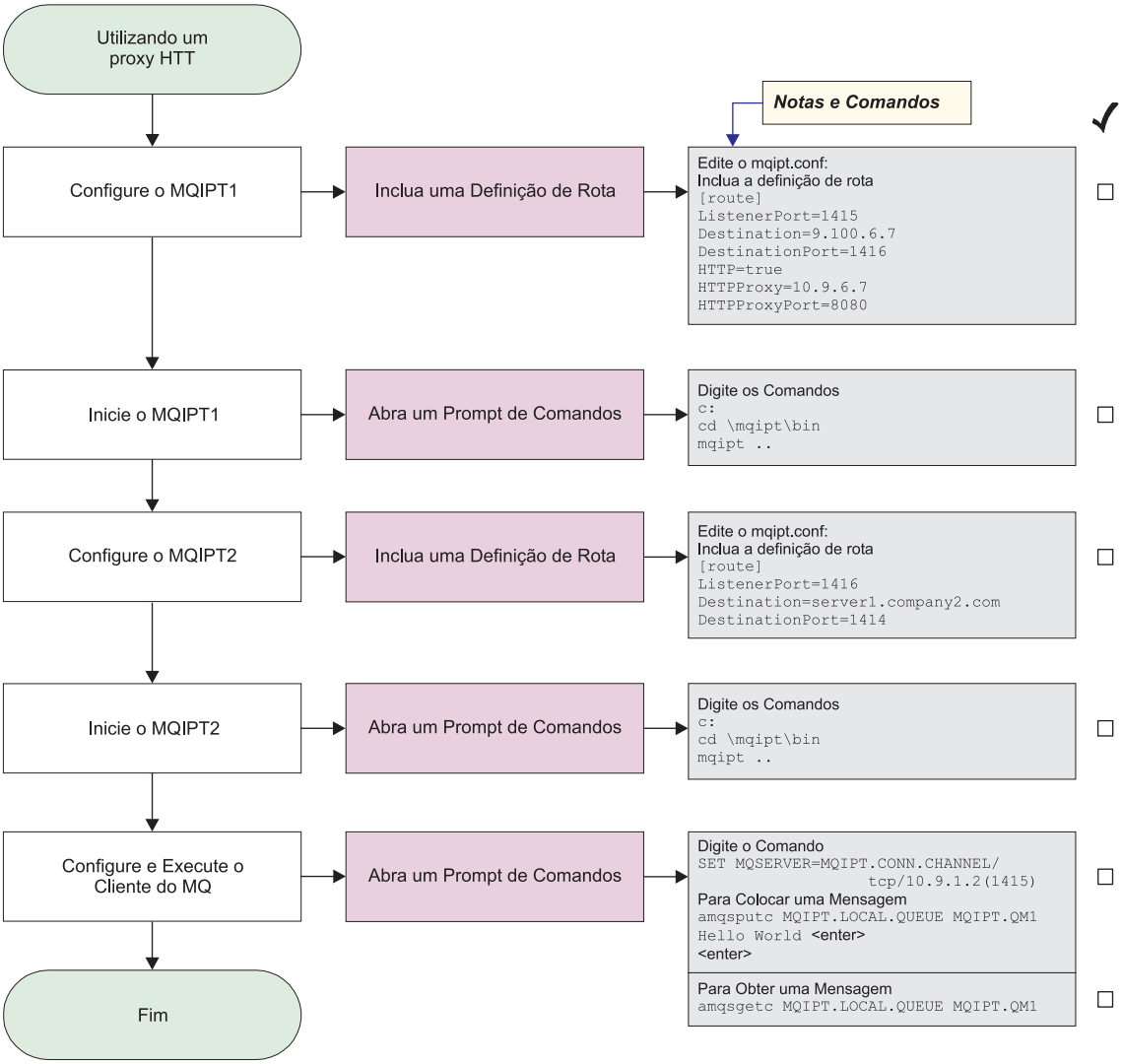

Figura 17. Configuração do proxy HTTP

1. Configure o MQIPT1

   Edite o `mqipt.conf` e inclua uma definição de rota:

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

2. Inicie o MQIPT1

   Abra um prompt de comandos e digite o seguinte:

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

   A seguinte mensagem indica uma conclusão bem-sucedida:

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

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

3. Configure o MQIPT2

   Edite o `mqipt.conf` e inclua uma definição de rota:

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

4. Inicie o MQIPT2

   Abra um prompt de comandos e digite o seguinte:

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

   A seguinte mensagem indica uma conclusão bem-sucedida:

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

5. Em um prompt de comandos na máquina do cliente do WebSphere MQ, digite o seguinte:

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

6. Coloque uma mensagem utilizando:

   ```
   amqsputc MQIPT.LOCAL.QUEUE MQIPT1.QM1
   Hello world <enter>
    <enter>
   ```

7. Obtenha a mensagem utilizando:

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

Você verá "Hello world".

Configurando o Controle de Acesso

Neste exemplo, você configurará o MQIPT para aceitar apenas conexões de clientes específicos, incluindo verificações de segurança na porta do atendente do MQIPT, utilizando o Java Security Manager.

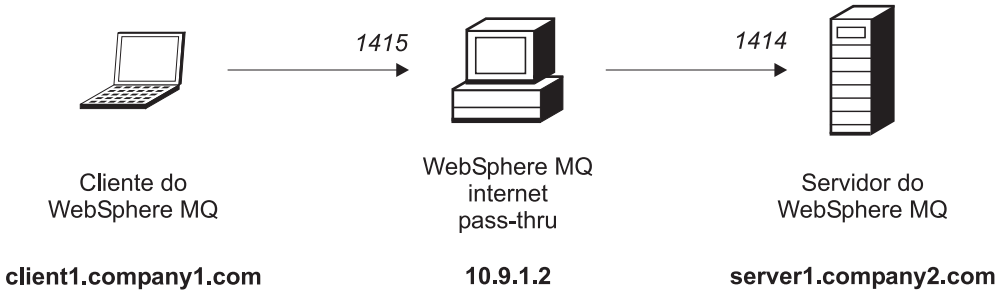

Figura 18. Diagrama de rede de controle de acesso

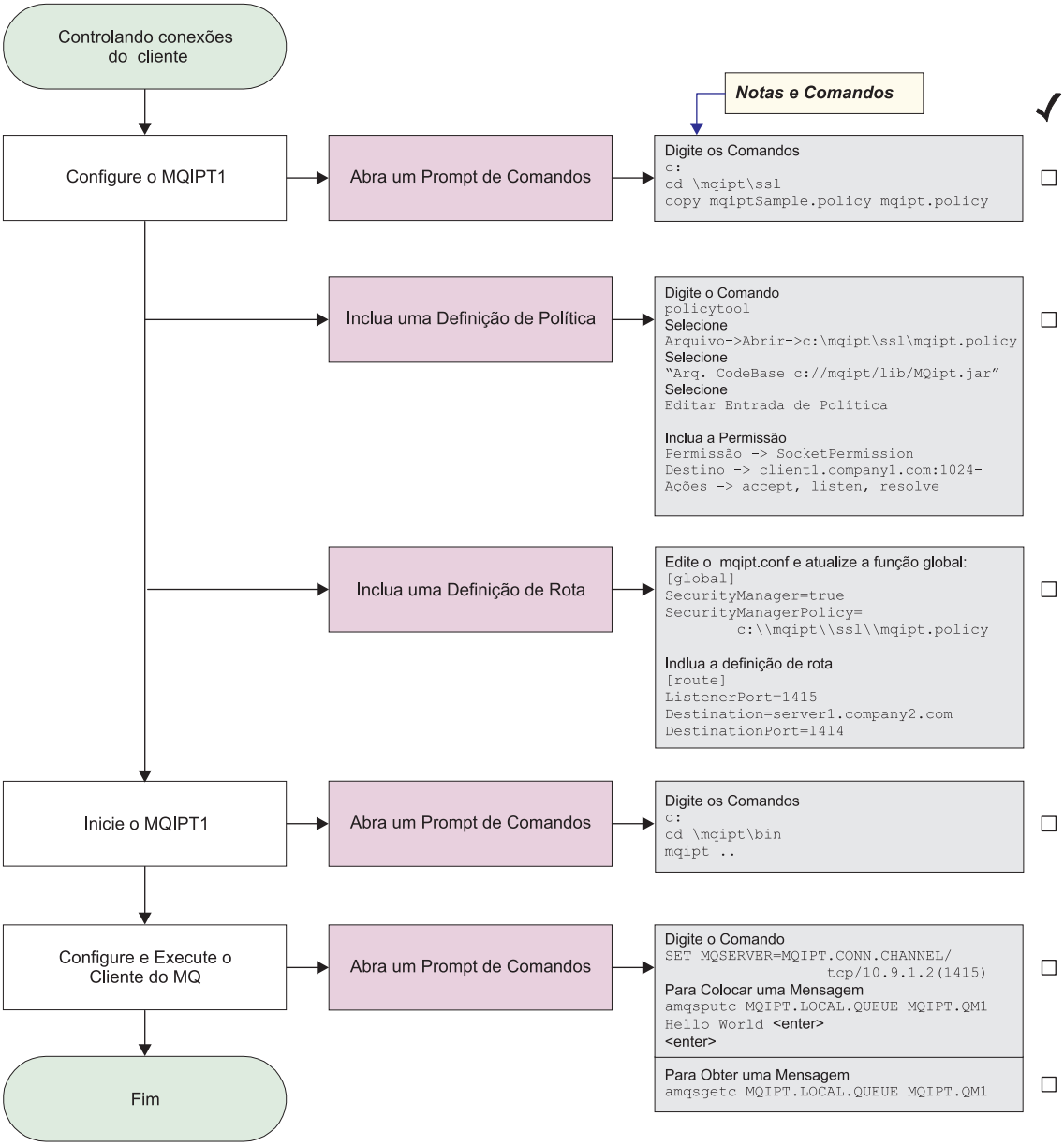

Figura 19. Configuração do controle de acesso

1. Configure o MQIPT1
   a. Abra um prompt de comandos e digite o seguinte:

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

   b. Inclua uma definição de política utilizando o seguinte comando:

      ```
      policytool
      ```

      1) Selecione Arquivo -> Abrir -> `c:\mqipt\ssl\mqipt.policy`
      2) Selecione:

         ```
         arquivo://C:/Arquivos de Programas/IBM/WebSphere MQ internet
         pass-thru/lib/MQipt.jar
         ```

      3) Altere o CodeBase de:

```
arquivo://C:/Arquivos de Programas/IBM/WebSphere MQ internet
pass-thru/lib/MQipt.jar
```

para:

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

4) Altere todas as permissões de:

```
C:\\Arquivos de Programas\\IBM\\WebSphere MQ internet
pass-thru
```

para:

```
C:\\mqipt
```

5) Inclua SocketPermission:

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

c. Edite o `mqipt.conf` e inclua:

1) Duas propriedades na seção global:

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

2) Uma definição de rota:

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

2. Inicie o MQIPT1

Abra um prompt de comandos e digite o seguinte:

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

A seguinte mensagem indica uma conclusão bem-sucedida:

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

3. Em um prompt de comandos na máquina do cliente do WebSphere MQ, digite o seguinte:

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

4. Coloque uma mensagem utilizando:

```
amqsputc MQIPT.LOCAL.QUEUE MQIPT1.QM1
Hello world <enter>
 <enter>
```

5. Obtenha a mensagem utilizando:

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

Você verá ″Hello world″.

Configurando a QoS (Qualidade de Serviço)

Neste exemplo, assume-se que a TQoS já tenha sido instalada na mesma máquina que o MQIPT.

Neste exemplo, você aplicará uma QoS (Qualidade de Serviço) a todos os canais de uma rota do MQIPT. Isso só pode ser implementado quando o MQIPT é executado na plataforma Linux. Esta amostra define uma propriedade ″average″ para todos os dados enviados do MQIPT para o cliente do WebSphere MQ e uma prioridade ″good″ para todos os dados enviados para o servidor do WebSphere MQ. Utilizando as políticas de pagent de amostra listadas abaixo, as seguintes prioridades podem ser aplicadas ao `QosToCaller` e `QosToDest`:

- 1 - médio
- 2 - bom
- 3 - muito bom

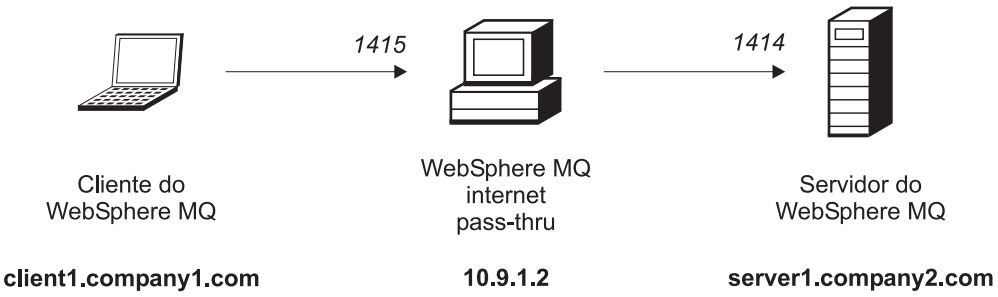

Figura 20. Diagrama de rede de QoS

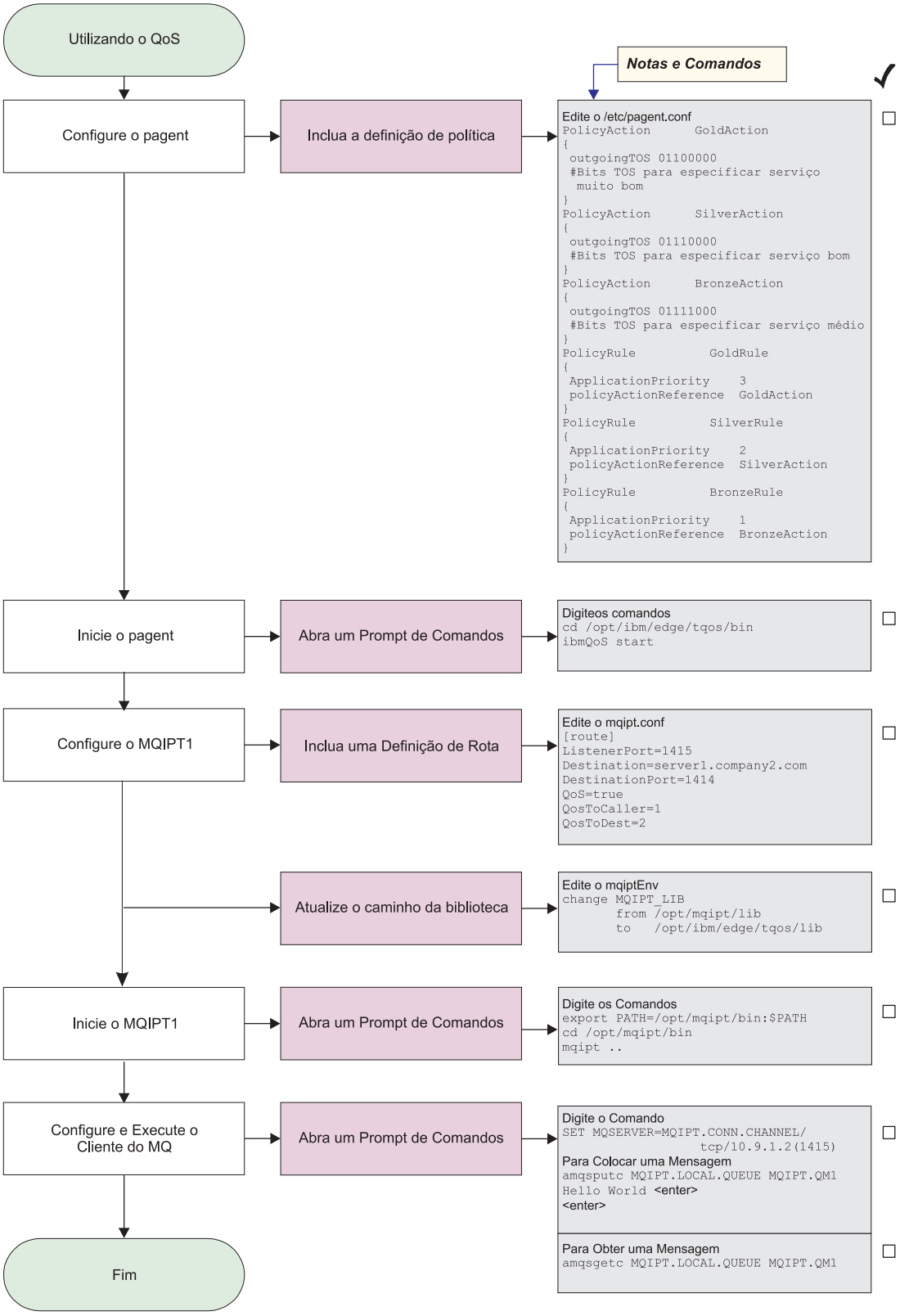

Figura 21. configuração de QoS

1. Configure o pagent
   Edite o `/etc/pagent.conf` e inclua o seguinte:

```
PolicyAction      GoldAction
{
 outgoingTOS 01100000
 #Bits TOS para especificar serviço muito bom
}
PolicyAction      SilverAction
{
 outgoingTOS 01110000
 #Bits TOS para especificar serviço bom
}
PolicyAction      BronzeAction
{
 outgoingTOS 01111000
 #Bits TOS para especificar serviço médio
}
PolicyRule          GoldRule
{
 ApplicationPriority    3
 policyActionReference  GoldAction
}
PolicyRule          SilverRule
{
 ApplicationPriority    2
 policyActionReference  SilverAction
}
PolicyRule          BronzeRule
{
 ApplicationPriority    1
 policyActionReference  BronzeAction
}
```

2. Inicie o pagent

   Abra um prompt de comandos e digite o seguinte:

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

3. Configure o MQIPT1

   Edite o `mqipt.conf` e inclua uma definição de rota:

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

4. Atualize o caminho da biblioteca

   Edite o `mqiptEnv` (localizado no `/opt/mqipt/bin`) e altere o MQIPT_LIB de:

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

   para:

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

5. Inicie o MQIPT1

   Abra um prompt de comandos e digite o seguinte:

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

   A seguinte mensagem indica uma conclusão bem-sucedida:

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

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

6. Em um prompt de comandos na máquina do cliente do WebSphere MQ, digite o seguinte:

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

7. Coloque uma mensagem utilizando:

```
amqsputc MQIPT.LOCAL.QUEUE MQIPT1.QM1
Hello world <enter>
 <enter>
```

8. Obtenha a mensagem utilizando:

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

Você verá "Hello world".

Configurando o Proxy SOCKS

Neste exemplo, você fazer o MQIPT agir como um proxy SOCKS. O cliente do WebSphere MQ deve ser ativado para socks antes de executar esta amostra e a configuração do SOCKS deve apontar para o MQIPT como o proxy SOCKS. As definições das propriedades Destination e DestinationPort do MQIPT podem ser qualquer uma, pois o destino verdadeiro é obtido do cliente do WebSphere MQ durante o processo do protocolo de reconhecimento socks.

Antes de iniciar, você deve ativar o socks para a máquina inteira ou apenas para o aplicativo cliente do WebSphere MQ (amqsputc/amqsgetc). Você deve configurar o cliente SOCKS para:

- Apontar para o MQIPT como um proxy Socks
- Ativar o suporte ao Socks V5
- Desativar a autenticação do usuário
- Fazer conexões apenas com o endereço de rede do MQIPT

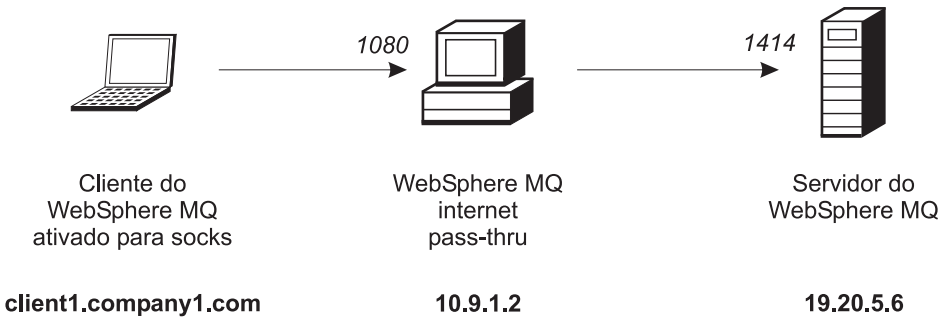

Figura 22. Diagrama de rede do proxy SOCKS

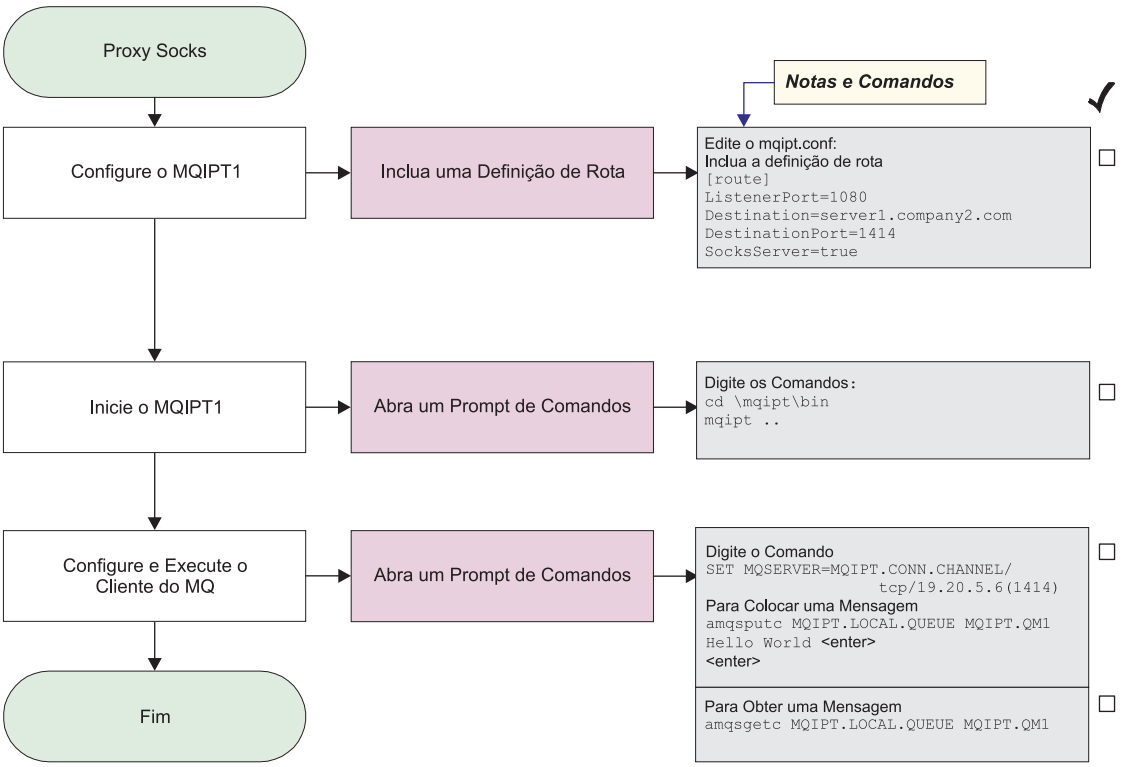

Figura 23. Configuração do proxy SOCKS

1. Configure o MQIPT1

   Edite o `mqipt.conf` e inclua uma definição de rota:

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

2. Inicie o MQIPT1

   Abra um prompt de comandos e digite o seguinte:

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

   A seguinte mensagem indica uma conclusão bem-sucedida:

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

3. Em um prompt de comandos na máquina do cliente do WebSphere MQ, digite o seguinte:

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

4. Coloque uma mensagem utilizando:

   ```
   amqsputc MQIPT.LOCAL.QUEUE MQIPT1.QM1
   Hello world <enter>
    <enter>
   ```

5. Obtenha a mensagem utilizando:

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

   Você verá ″Hello world″.

Configurando o Cliente SOCKS

Neste exemplo, você executará o MQIPT como se ele tivesse sido ativado para socks, utilizando um proxy SOCKS existente. Isso é semelhante a “Configurando o Proxy SOCKS” na página 83, exceto que o MQIPT faz uma conexão com socks ativado, em vez do cliente do WebSphere MQ.

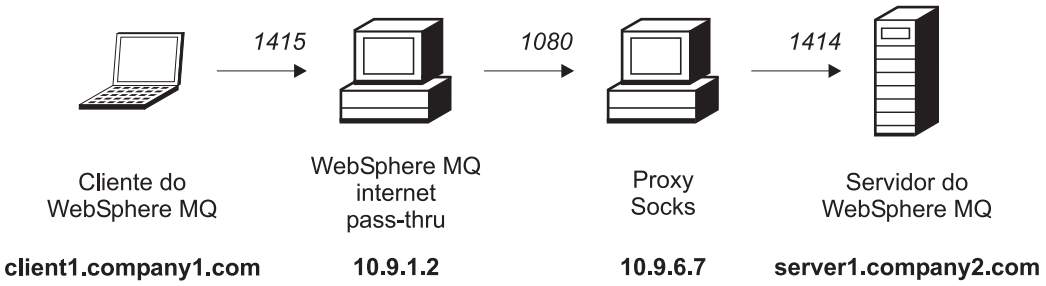

Figura 24. Diagrama de rede do cliente SOCKS

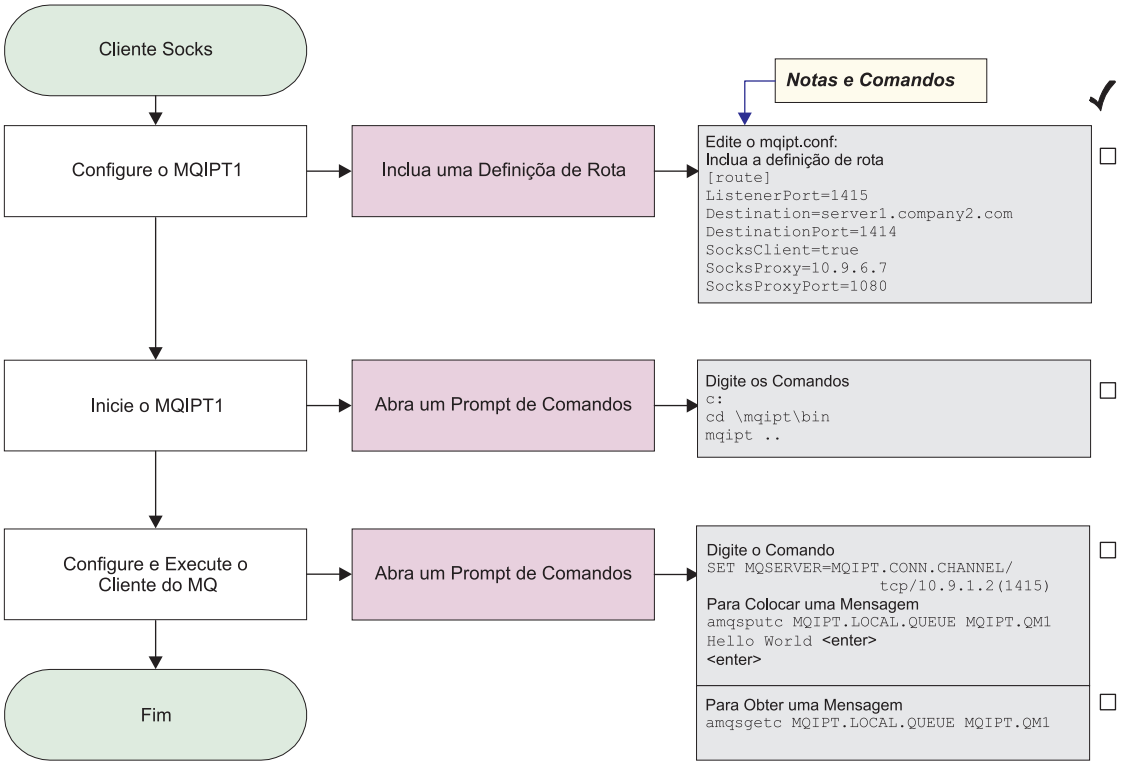

Figura 25. configuração do cliente SOCKS

1. Configure o MQIPT1

   Edite o `mqipt.conf` e inclua uma definição de rota:

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

```
DestinationPort=1414
SocksClient=true
SocksProxy=10.9.6.7
SocksProxyPort=1080
```

2. Inicie o MQIPT1

   Abra um prompt de comandos e digite o seguinte:

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

   A seguinte mensagem indica uma conclusão bem-sucedida:

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

3. Em um prompt de comandos na máquina do cliente do WebSphere MQ, digite o seguinte:

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

4. Coloque uma mensagem utilizando:

   ```
   amqsputc MQIPT.LOCAL.QUEUE MQIPT1.QM1
   Hello world <enter>
    <enter>
   ```

5. Obtenha a mensagem utilizando:

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

Você verá ″Hello world″.

Configurando o Proxy SSL

Neste exemplo, você executará o MQIPT no modo de proxy SSL, portanto, ele aceitará um pedido de conexão SSL de um cliente SSL e o encapsulará em um servidor SSL.

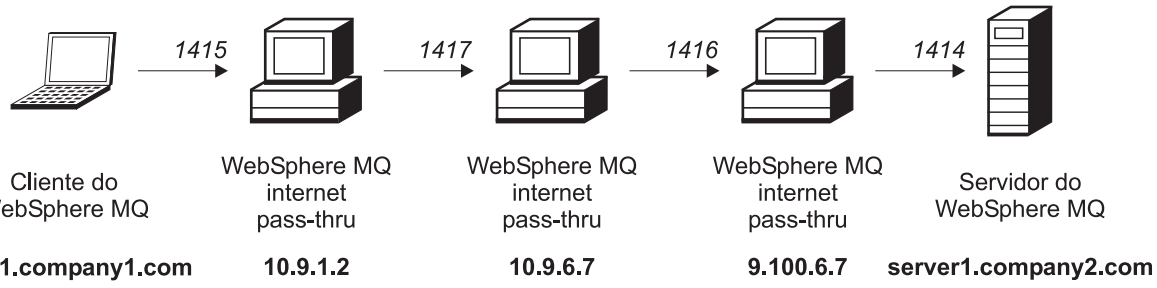

Figura 26. Diagrama de rede do proxy SSL

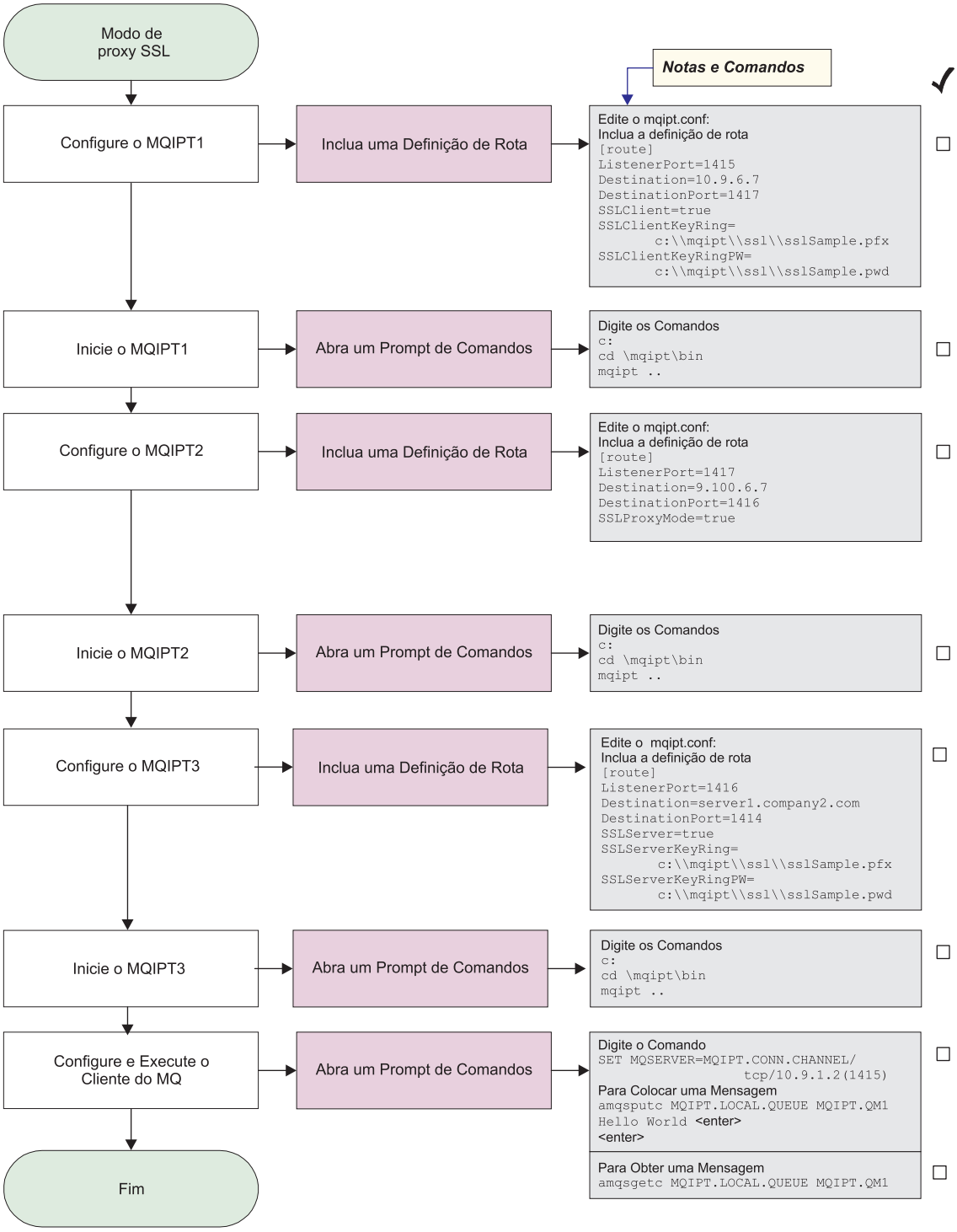

Figura 27. Configuração do proxy SSL

1. Configure o MQIPT1

   Edite o `mqipt.conf` e inclua uma definição de rota:

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

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

2. Inicie o MQIPT1

   Abra um prompt de comandos e digite o seguinte:

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

   A seguinte mensagem indica uma conclusão bem-sucedida:

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

3. Configure o MQIPT2

   Edite o `mqipt.conf` e inclua uma definição de rota:

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

4. Inicie o MQIPT2

   Abra um prompt de comandos e digite o seguinte:

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

   A seguinte mensagem indica uma conclusão bem-sucedida:

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

5. Configure o MQIPT3

   Edite o `mqipt.conf` e inclua uma definição de rota:

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

6. Inicie o MQIPT3

   Abra um prompt de comandos e digite o seguinte:

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

A seguinte mensagem indica uma conclusão bem-sucedida:

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

7. Em um prompt de comandos na máquina do cliente do WebSphere MQ, digite o seguinte:

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

8. Coloque uma mensagem utilizando:

   ```
   amqsputc MQIPT.LOCAL.QUEUE MQIPT1.QM1
   Hello world <enter>
    <enter>
   ```

9. Obtenha a mensagem utilizando:

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

Você verá ″Hello world″.

Criando Certificados de Teste SSL

Neste exemplo, nós mostraremos como criar um certificado auto-assinado que pode ser utilizado para testar as rotas do MQIPT. O certificado terá o flag trust-as-peer ativado.

1. Inicie o KeyMan
2. Selecione ″Create new...″
3. Selecione ″PKCS#12 Token″
4. Selecione ″Action -> Generate Key″

   um novo par de chaves aparecerá na lista ″RSA / 1024-bit″
5. Selecione o novo par de chaves
6. Selecione ″Action -> Create Certificate″
7. Selecione ″Self-signed Certificate″
8. Digite os detalhes do certificado.

   Aparecerá um diálogo explicando que o certificado privado será unido com a chave. A digitação de um rótulo é opcional
9. Selecione o novo certificado
10. Exiba os detalhes do certificado
11. Altere as propriedades do certificado
12. Ative o flag trust-as-peer
13. Feche o diálogo. Selecione ″File -> Save″
14. Digite uma frase-chave (por exemplo, minhaFraseChave)
15. Digite um nome para o novo arquivo de conjunto de chaves (por exemplo, c:\mqipt\ssl\testRoute1414.pfx)

    Você deve manter ″File format as PKCS#12 / PFX″ - **não selecione** ″Wrap key ring into a Java class″

16. Crie um arquivo de texto contendo a frase-chave (minhaFraseChave) utilizada acima.

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

Este arquivo de conjunto de chaves agora pode ser utilizado no exemplo em "Autenticação do Servidor SSL" na página 70.

Configurando o Servlet do MQIPT

Esta amostra utiliza o servidor de aplicativos Tomcat e supõe que ele tenha sido instalado anteriormente em um diretório denominado `c:\jakarta-tomcat-4.0.1`.

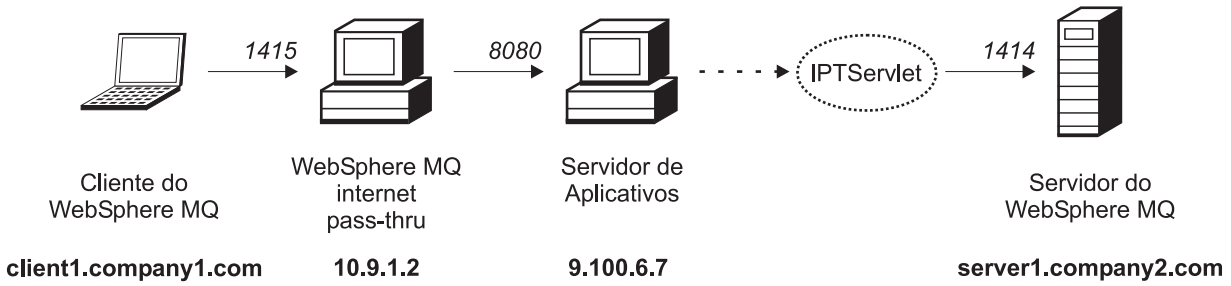

Figura 28. Diagrama de rede do servlet

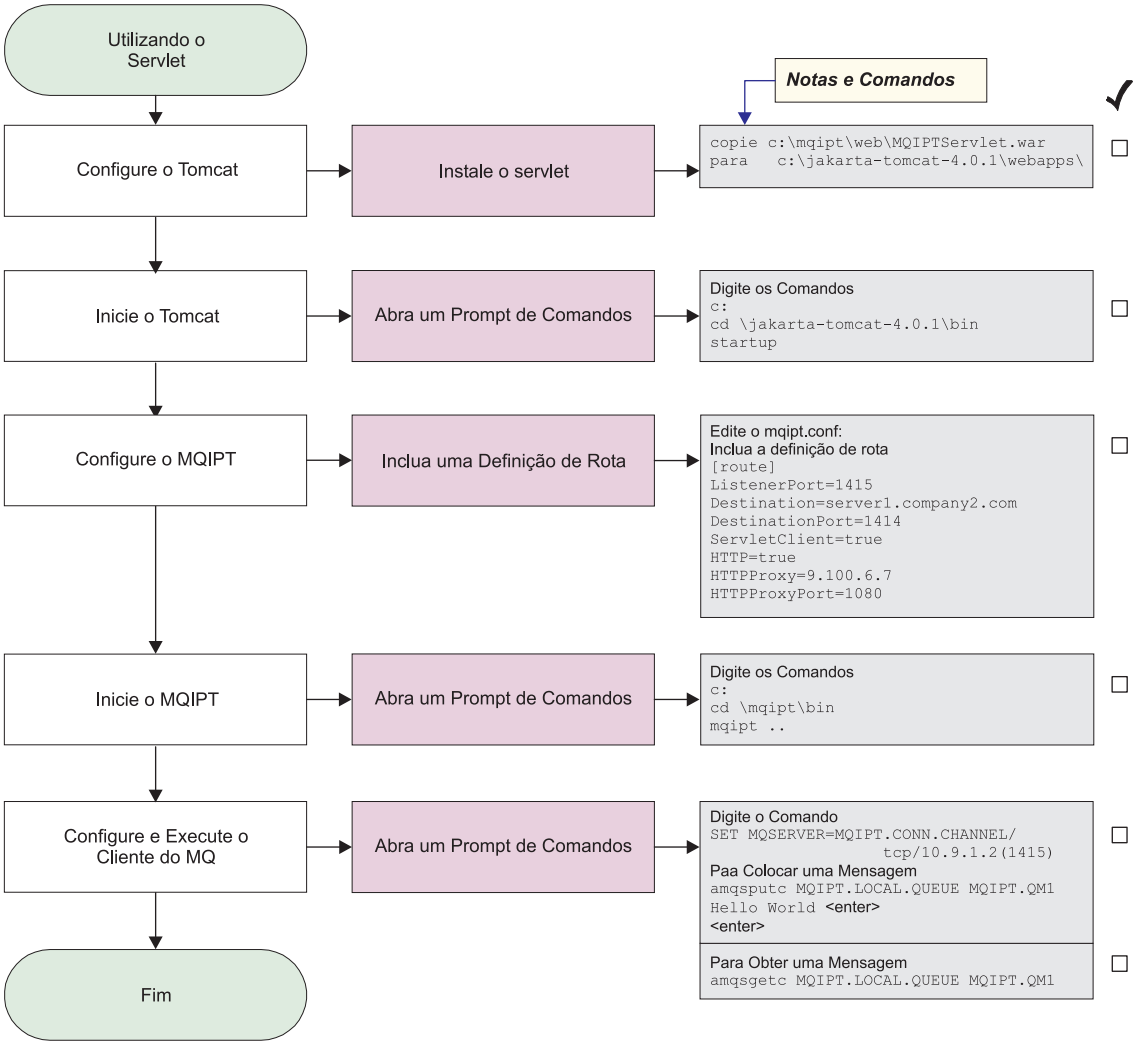

Figura 29. Configuração do servlet

1. Configure o Tomcat

   copie:

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

   para:

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

2. Inicie o Tomcat

   Abra um prompt de comandos e digite o seguinte:

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

3. Configure o MQIPT1

   Edite o `mqipt.conf` e inclua uma definição de rota:

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

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

4. Inicie o MQIPT1

   Abra um prompt de comandos e digite o seguinte:

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

   A seguinte mensagem indica uma conclusão bem-sucedida:

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

5. Em um prompt de comandos na máquina do cliente do WebSphere MQ, digite o seguinte:

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

6. Coloque uma mensagem utilizando:

   ```
   amqsputc MQIPT.LOCAL.QUEUE MQIPT1.QM1
   Hello world <enter>
    <enter>
   ```

7. Obtenha a mensagem utilizando:

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

Você verá ″Hello world″.

Configurando o Suporte ao Clustering do MQIPT

Para este exemplo, além de “Suposições” na página 67, você também deve ter feito o seguinte:

No servidor LONDON do WebSphere MQ:

- Definido um gerenciador de filas denominado LONDON
- Definido um canal de conexão do servidor denominado MQIPT.CONN.CHANNEL
- Iniciado um atendente TCP/IP para o LONDON na porta 1414
- Ativado o socks para o gerenciador de filas

No servidor NEWYORK do WebSphere MQ:

- Definido um gerenciador de filas denominado NEWYORK
- Definido um canal de conexão do servidor denominado MQIPT.CONN.CHANNEL
- Iniciado um atendente TCP/IP para o NEWYORK na porta 1414
- Ativado o socks para o gerenciador de filas

Para ativar o socks para o gerenciador de filas, ative-o para a máquina inteira ou apenas para o aplicativo servidor do WebSphere MQ. Configure o cliente SOCKS para

- Apontar para o MQIPT como o proxy SOCKS

- Ativar o suporte ao SOCKS V5
- Desativar a autenticação do usuário
- Fazer conexões remotas apenas com o MQIPT

Apenas um aplicativo pode atender em um determinado endereço de porta na mesma máquina, se a porta 1414 já estiver em uso, escolha um endereço de porta livre e substitua-o nos exemplos. Depois de feito isso, você pode testar as rotas entre os gerenciadores de filas, colocando uma mensagem na fila local do LONDON e recuperando-a de NEWYORK.

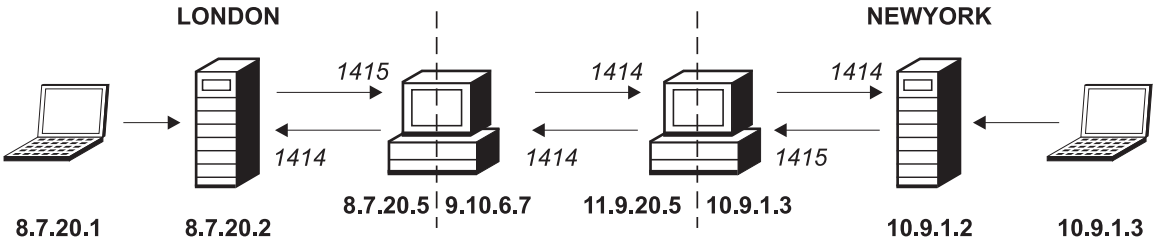

Figura 30. Diagrama de rede de clustering

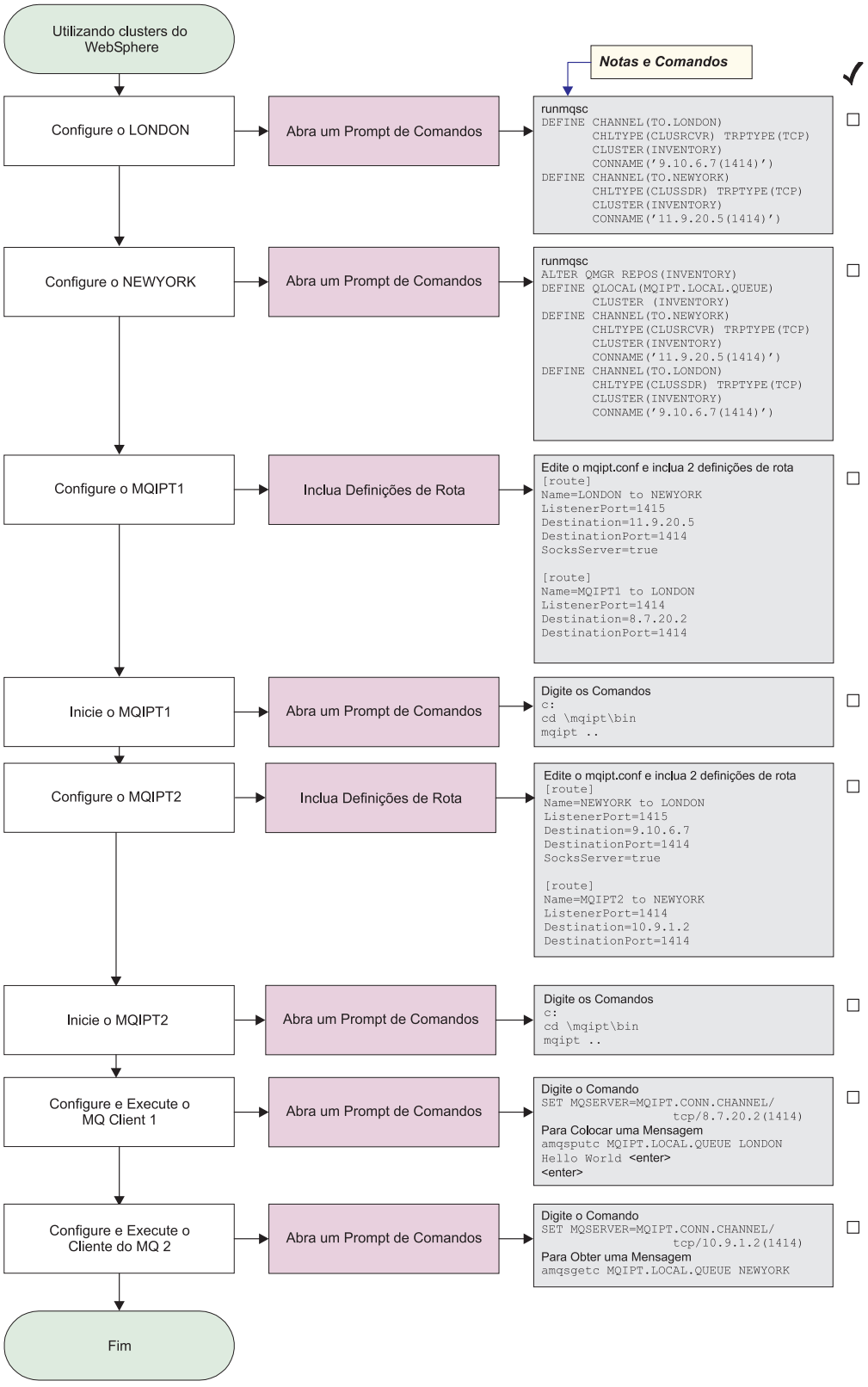

Figura 31. Configuração de clustering

1. Configure o LONDON

   Abra um prompt de comandos e digite o seguinte:

```
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 o NEWYORK

   Abra um prompt de comandos e digite o seguinte:

```
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 o MQIPT1

   Edite o `mqipt.conf` e inclua duas definições de rota:

```
[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 o MQIPT1

   Abra um prompt de comandos e digite o seguinte:

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

   A seguinte mensagem indica uma conclusão bem-sucedida:

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

5. Configure o MQIPT2

   Edite o `mqipt.conf` e inclua duas definições de rota:

```
[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 o MQIPT2

   Abra um prompt de comandos e digite o seguinte:

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

   A seguinte mensagem indica uma conclusão bem-sucedida:

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

7. Em um prompt de comandos na primeira máquina do cliente do WebSphere MQ (8.7.20.1), digite o seguinte:

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

8. Coloque uma mensagem utilizando:

   ```
   amqsputc MQIPT.LOCAL.QUEUE LONDON
   Hello world <enter>
    <enter>
   ```

9. Em um prompt de comandos na segunda máquina do cliente do WebSphere MQ (10.9.1.3), digite o seguinte:

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

10. Na segunda máquina do cliente do WebSphere MQ, obtenha a mensagem utilizando:

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

Você verá ″Hello world″.

Criando um Arquivo de Conjunto de Chaves

Esta amostra assume que você tenha solicitado um novo certificado de uma CA confiável utilizando o Keyman e o seu certificado pessoal foi retornado em um arquivo (por exemplo, `server.cer`). Isso será suficiente para executar a autenticação do servidor. Se a autenticação de cliente for necessária, você precisará solicitar um segundo certificado (por exemplo, `client.cer`) e executar duas vezes as etapas a seguir, para criar dois arquivos de conjunto de chaves.

1. Inicie o KeyMan
2. Selecione ″Create new...″
3. Selecione ″PKCS#12 Token″
4. Selecione ″Action -> Generate Key″

Um novo par de chaves aparecerá na lista ″RSA / 1024-bit″

5. Selecione o novo par de chaves
6. Selecione ″Action -> Request Certificate″

   Siga as instruções online
7. Selecione ″File -> Save″
8. Digite a senha
9. Digite o nome do arquivo do novo arquivo de conjunto de chaves

   Por exemplo, `c:\mqipt\ssl\myServer.pfx`
10. Mantenha ″File format as PKCS#12 / PFX″ - **não selecione** `″Wrap key ring into a Java class″`
11. Selecione ″File -> Exit″
12. Crie um arquivo de texto contendo a frase-chave (minhaFraseChave) utilizada acima.

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

Quando você receber de volta o certificado, abra o arquivo de conjunto de chaves original (`myServer.pfx`). Em seguida:

1. Inicie o KeyMan
2. Selecione ″Open existing...″.
3. Selecione ″Local resource″
4. Selecione ″Open a file...″
5. Digite o nome do arquivo de certificado pessoal

   Por exemplo, `c:\mqipt\ssl\myServer.pfx`
6. Digite a frase-chave
7. Selecione ″File -> Import″
8. Selecione ″Local resource″
9. Selecione ″Open a file...″
10. Digite server.cer

    Aparecerá um diálogo explicando que o certificado privado será unido à chave privada
11. Selecione ″File -> Save″
12. Selecione ″File -> Exit″

Repita estas etapas para criar um `myClient.pfx` no arquivo `client.cer`. Verifique o conteúdo do arquivo de conjunto de chaves de CA de amostra, `sslCAdefault.pfx`, utilizando o KeyMan, para ver se os certificados pessoais foram assinados por uma das CAs listadas. Se isso for verdadeiro, você poderá utilizar o arquivo de conjunto de chaves de CA de amostra. Se não, você precisará criar um arquivo de conjunto de chaves contendo o certificado de CA público que assinou os certificados pessoais. Isso pode ter sido retornado com o certificado pessoal. Se não, você precisará solicitar o certificado de CA da mesma CA que forneceu os certificados pessoais e importá-lo para `sslCAdefault.pfx`. O arquivo de conjunto de chaves de CA pode ser utilizado no lado do cliente e do servidor. Para utilizar estes novos arquivos de conjunto de chaves para autenticação do servidor, consulte o exemplo em “Autenticação do Servidor SSL” na página 70 e defina as seguintes propriedades de rota:

```
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 estes novos arquivos de conjunto de chaves para a autenticação de cliente e servidor, consulte o exemplo em "Autenticação do Cliente SSL" na página 72 e defina as seguintes propriedades de rota:

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

Capítulo 11. Inspecionando o internet pass-thru

Este capítulo descreve como manter o internet pass-thru em execução, sob estes títulos:

- "Manutenção"
- "Determinação de Problemas"
- "Ajuste de Desempenho" na página 102

Manutenção

Você deve fazer backup regularmente dos seguintes arquivos como parte de seus procedimentos normais de backup:

- O arquivo de configuração `mqipt.conf`
- Os arquivos de conjunto de chaves SSL no `mqipt.conf`, quando definidos com as seguintes propriedades:
  - `SSLClientKeyRing`
  - `SSLClientCAKeyRing`
  - `SSLServerKeyRing`
  - `SSLServerCAKeyRing`
- Os arquivos de senha do conjunto de chaves SSL no `mqipt.conf`, quando definidos com as seguintes propriedades:
  - `SSLClientKeyRingPW`
  - `SSLClientCAKeyRingPW`
  - `SSLServerKeyRingPW`
  - `SSLServerCAKeyRingPW`
- O arquivo de configuração do Cliente Administrativo, `client.conf`, que contém informações de conexão sobre todos os MQIPTs conhecidos pelo Cliente Administrativo.

Determinação de Problemas

Há algumas verificações comuns a serem feitas primeiro se você encontrar um problema:

- O sistema MQIPT acabou de ser instalado e não foi reinicializado.
- O HTTP foi definido como `true` em uma rota conectada diretamente a um gerenciador de filas.
- O SSLClient foi definido como `true` em uma rota diretamente conectada a um gerenciador de filas.
- O CLASSPATH não foi configurado corretamente.
- O PATH não foi configurado corretamente.
- As senhas armazenadas para os arquivos de conjunto de chaves fazem distinção entre maiúsculas e minúsculas.

A próxima etapa é seguir o fluxograma mostrado na Figura 32 na página 100. Os números referem-se às notas, mostradas em seguida.

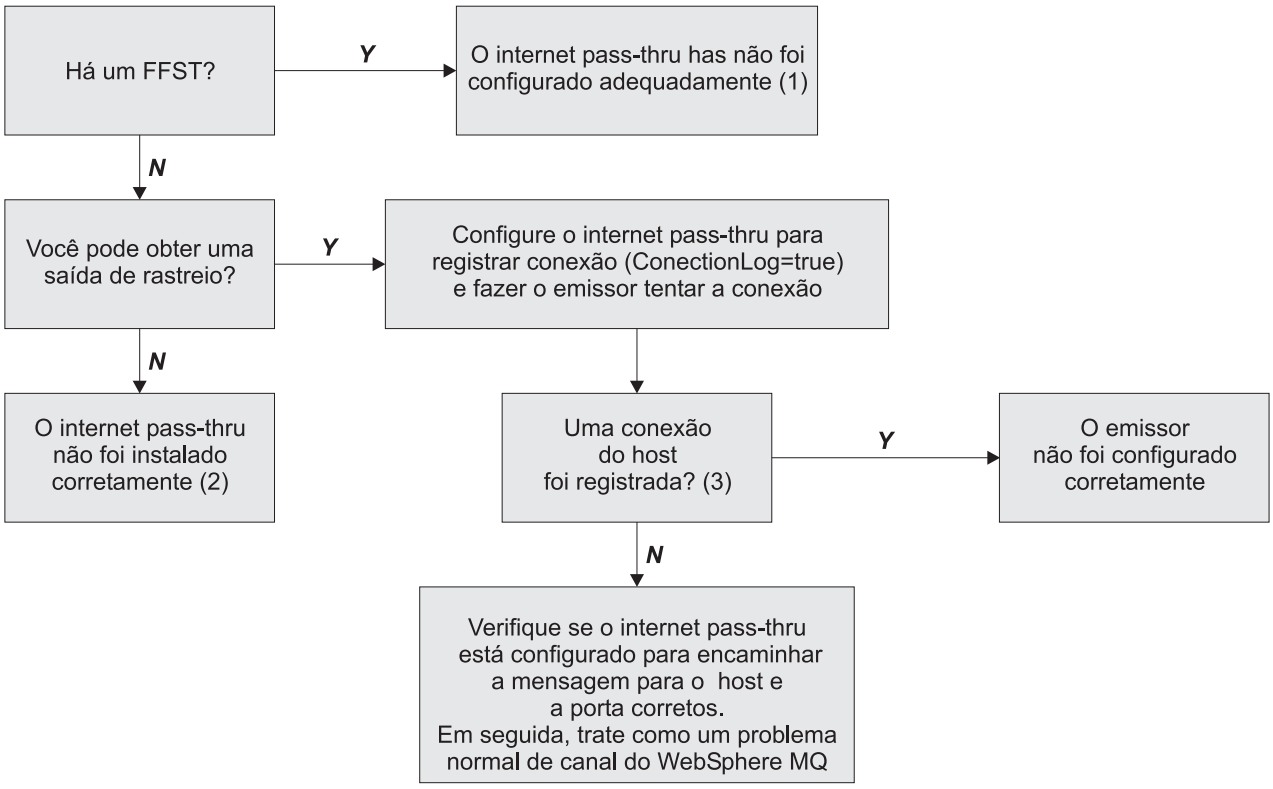

Figura 32. Fluxograma de determinação de problemas

Notas:

1. Se você encontrar relatórios FFST (no subdiretório errors), saberá que o MQIPT foi instalado corretamente. Pode ter ocorrido um problema com a configuração.

   Cada FFST relata um problema que faz com que o MQIPT, ou uma rota, termine seu processo de partida. Corrija o problema que causou cada FFST. Em seguida, exclua os FFSTs antigos e inicie novamente ou atualize o MQIPT.
2. Se o MQIPT não tiver sido instalado corretamente, verifique se todos os arquivos foram colocados no local correto e o CLASSPATH foi atualizado. Para verificar se isso está correto, tente iniciar o MQIPT manualmente.
3. Iniciar manualmente o MQIPT.

   Abra um prompt de comandos. Vá para o subdiretório `bin` e digite:

   ```
   mqipt xxx
   ```

   em que *xxx* é o diretório inicial do MQIPT; neste caso, é "`..`".

   Isso inicia o MQIPT e procura a configuração no diretório inicial. Procure por quaisquer mensagens de erro e FFSTs no subdiretório `errors`.

   Examine a saída de texto do MQIPT quanto a mensagens de erro e corrija o(s) erro(s). Verifique os FFSTs e corrija quaisquer erros. O MQIPT não será iniciado se houver um problema na seção global do arquivo de configuração. Uma rota não será iniciada se houver um problema na seção route do arquivo de configuração.

Iniciando Automaticamente o internet pass-thru

Se você instalar o MQIPT como um serviço do Windows NT e tiver alterado sua partida para automática, ele será iniciado junto com o sistema. Inicie sempre uma vez o MQIPT manualmente, antes de tentar instalar o MQIPT como um Serviço do Windows NT para confirmar se a instalação está correta. Consulte "Utilizando um Programa de Controle de Serviços do Windows" na página 31 para obter mais detalhes.

Se for recebida a mensagem de erro "Não é possível localizar o DLL...", você está utilizando o programa `mqiptService` incorreto ou não configurou a variável de ambiente PATH corretamente. O PATH deve conter a localização das bibliotecas de tempo de execução do JNI. Este arquivo (`jvm.dll`) pode ser encontrado no subdiretório do cliente do JDK.

Verificando a Conectividade de Ponta a Ponta

Se o MQIPT estiver instalado corretamente, a próxima etapa é verificar se as rotas estão configuradas corretamente.

No arquivo de configuração, `mqipt.conf`, defina a propriedade `ConnectionLog` como true. Inicie ou atualize o MQIPT e tente uma conexão. O log de conexão é criado no diretório logs abaixo do diretório inicial. Se ele não for criado, você saberá que o MQIPT não foi instalado corretamente. Se não forem registradas tentativas de conexão, o emissor não foi configurado corretamente. Se forem registradas tentativas de conexão, verifique se o MQIPT está encaminhando as mensagens para o endereço correto.

Rastreando Erros

O MQIPT fornece um recurso de rastreio de execução detalhado, que é controlado pelo atributo trace. Cada rota pode ser rastreada independentemente. Os arquivos de rastreio são gravados no diretório *xxx*`\errors` (em que *xxx* é o diretório que contém o `mqipt.conf`. Cada arquivo de rastreio produzido tem um nome com o seguinte formato:

`iptroute`*nnnnn*`.trc`

em que *nnnnn* é o número da porta na qual a rota está atendendo. A saída de rastreio de threads não associados diretamente a nenhuma rota específica (por exemplo, a entrada do comando de tratamento de threads) é gravada em um arquivo separado denominado `iptmain.trc`.

Erros fatais inesperados são gravados como registros FFST em um arquivo de log de erros, contido no diretório *xxx*`\errors` (em que *xxx* é o diretório que contém o `mqipt.conf`). Os arquivos do FFST possuem o seguinte formato:

`ipt`*xxx*`.FFST`

em que *xxx* é a seqüência em que o FFST foi gerado (1 é o mais antigo). Em um sistema de execução longa, você pode alcançar o número máximo que o sistema pode gerar. Neste caso, os FFSTs gerados são gravados no arquivo `mqipt0.FFST`. Se o arquivo `mqipt0.FFST` for criado, você deverá parar e iniciar novamente o MQIPT na primeira oportunidade e excluir os arquivos antigos.

Relatando Problemas

Se você tiver que relatar um problema para o Centro de Serviços da IBM, o problema poderá ser resolvido mais rapidamente se você fornecer as seguintes informações:

- Forneça um diagrama de rede simples das máquinas que estão sendo utilizadas, incluindo endereços IP
- Se houver mais de um MQIPT sendo utilizado, sincronize o clock do sistema em cada máquina do MQIPT - isso ajudará a corresponder as entradas de rastreio em cada MQIPT
- Apague os arquivos de rastreio antigos
- Execute o cliente para produzir o problema - desse modo, os arquivos de rastreio contêm apenas uma instância do problema
- Envie uma cópia de todos os arquivos .trc e .log do MQIPT

Ajuste de Desempenho

Seguem algumas sugestões para ajuste do sistema.

Gerenciamento do Conjunto de Threads

O desempenho relativo de cada rota pode ser ajustado utilizando uma combinação de um conjunto de threads e uma especificação de tempo limite inativo.

Threads de Conexão

Cada rota do MQIPT é atribuída a um conjunto de trabalho de threads simultaneamente em execução que manipulam pedidos de comunicação de entrada. Na partida, um conjunto de threads é criado (do tamanho especificado no atributo `MinConnectionThreads` da rota) e um thread é designado para manipular o primeiro pedido de entrada. Quando este pedido chega, o thread começa a trabalhar neste pedido imediatamente e o thread seguinte é atribuído como pronto para o próximo pedido de entrada. Quando todos os threads estão atribuídos ao trabalho, um novo thread é criado, incluído no conjunto de trabalho e atribuído ao trabalho. Desse modo, o conjunto aumenta até que `MaxConnectionThreads` seja alcançado. Quando o número de threads de trabalho está em `MaxConnectionThreads`, o pedido de entrada seguinte aguarda até que um thread seja liberado para o conjunto de trabalho. Esta é a capacidade máxima de trabalho da rota, após a qual nenhum pedido adicional pode ser aceito. Os threads são liberados novamente para o conjunto quando uma conversão é encerrada ou o período de tempo limite inativo tiver decorrido.

Tempo Limite Inativo

Por padrão, os threads de trabalho não são finalizados em razão da inatividade. Quando um thread tiver sido atribuído a uma conversação, ele permanecerá atribuído a essa conversação até que seja fechado normalmente, a rota seja desativada ou o MQIPT seja encerrado. Opcionalmente, um intervalo de tempo limite inativo pode ser especificado, para que qualquer thread que tenha ficado inativo pelo período de tempo especificado (em minutos) seja finalizado. Um thread de monitor faz uma verificação regular sobre tempos de inatividade do thread e finaliza aqueles que excederam o limite. Os threads são reciclados para uso colocando-os de volta no conjunto de trabalho.

Capítulo 12. Mensagens

Quando executado a partir da linha de comandos, o MQIPT exibe um pequeno número de mensagens informativas e de erro no console, apenas no idioma Inglês dos Estados Unidos.

Observe que:

- Mensagens MQCAxxxx são mensagens do Administration Client.
- Mensagens MQCPxxxx são mensagens do MQIPT.
- Mensagens MQCxIxxx são mensagens informativas.
- Mensagens MQCxExxx são mensagens de erro.

MQCAE001 Unknown host: {0}

Explicação: Não foi possível encontrar o host do MQIPT.

Resposta do Usuário: Verifique se você especificou corretamente o nome do host no qual o MQIPT está localizado.

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

Explicação: Ocorreu um erro. Ao longo de um comando do sistema, um erro foi relatado.

MQCAE005 No valid destination address has been defined

Explicação: Durante a inclusão de uma rota, o campo de destino foi deixado em branco.

Resposta do Usuário: Digite um endereço de destino válido.

MQCAE006 No valid destination port has been defined

Explicação: Durante a inclusão de uma rota, o campo de endereço da porta de destino foi deixado em branco.

Resposta do Usuário: Digite um endereço válido para a porta de destino.

MQCAE007 No valid listener port has been defined

Explicação: Durante a inclusão de uma rota, o campo de endereço da porta do atendente foi deixado em branco.

Resposta do Usuário: Digite um endereço válido para a porta do atendente, entre 1 e 65535.

MQCAE008 No valid network address has been defined

Explicação: Durante a inclusão de um MQIPT, o campo de endereço de rede foi deixado em branco.

Resposta do Usuário: Digite um endereço de rede válido.

MQCAE009 No valid command port has been defined

Explicação: Durante a inclusão de um MQIPT, um endereço de porta de comando inválido foi utilizado.

Resposta do Usuário: Digite um endereço válido para a porta do comando, entre 1 e 65535.

MQCAE010 Could not show online help

Explicação: O arquivo para ajuda online estava disponível mas não pôde ser exibido.

Resposta do Usuário: Certifique-se de que o Acrobat Reader esteja disponível no PATH do sistema.

MQCAE011 Could not parse parameter

Explicação: Ocorreu um erro interno que causou a tentativa de atualizar um parâmetro não-existente na tabela.

Resposta do Usuário: Se a condição persistir, entre em contato com o Suporte Técnico da IBM.

MQCAE012 Could not find file for online help

Explicação: O arquivo "guiadmin.pdf" não pôde ser encontrado.

Resposta do Usuário: Certifique-se de que este arquivo esteja acessível no subdiretório doc.

MQCAE013 Interrupted while trying to show online help

Explicação: Ocorreu um erro do sistema durante a exibição da ajuda online.

Resposta do Usuário: Tente novamente. Se a condição persistir, entre em contato com o Suporte Técnico da IBM.

MQCAE015 The password you have just entered has not been recognized

Explicação: O MQIPT espera uma senha válida; a que foi utilizada no último comando estava incorreta. A senha deve corresponder àquela que foi definida no arquivo de configuração.

Resposta do Usuário: Altere a senha utilizando o painel **MQIPT->Conexão** e repita o último comando.

MQCAE016 Node mismatch

Explicação: Há uma inconsistência interna entre o nó selecionado na árvore e os dados contidos na memória.

Resposta do Usuário: Feche o Administration Client e repita o comando. Se a condição persistir, entre em contato com o Suporte Técnico da IBM.

MQCAE017 Could not create NLS text for message {0}

Explicação: Nenhum texto NLS foi encontrado para o número de mensagem definido.

Resposta do Usuário: O arquivo ″guiadmin.properties″ pode ter sido danificado e o número de mensagem especificado não pôde ser encontrado. Verifique o seguinte:

- consulte o arquivo Readme para verificar se há uma nova mensagem
- o arquivo ″guideadmin.jar″ está no CLASSPATH do sistema
- o arquivo ″guideadmin.properties″ está no arquivo ″guideadmin.jar″
- o número de mensagem está no arquivo ″guideadmin.properties″

MQCAE018 Could not create NLS text for message MQCAE017

Explicação: O número de mensagem {0} não foi encontrado na lista de propriedades do sistema.

Resposta do Usuário: O arquivo ″guideadmin.properties″ pode ter sido danificado. Verifique o seguinte:

- o arquivo ″guideadmin.jar″ está no CLASSPATH do sistema
- o arquivo ″guideadmin.properties″ está no arquivo ″guideadmin.jar″
- o número de mensagem está no arquivo ″guideadmin.properties″

MQCAE019 You have failed to repeat your proposed new password

Explicação: Durante a alteração da senha, ela não foi digitada duas vezes para verificação.

Resposta do Usuário: Digite a nova senha mais uma vez no campo apropriado.

MQCAE020 Failed to change MQIPT access parameters

Explicação: Um erro interno foi detectado durante a tentativa de alterar os parâmetros de acesso do MQIPT.

Resposta do Usuário: Feche o Administration Client e repita o comando. Se a condição persistir, entre em contato com o Suporte Técnico da IBM.

MQCAE021 Internal failure to identify MQIPT

Explicação: Um erro interno foi detectado durante a tentativa de salvar um arquivo de configuração em um MQIPT.

Resposta do Usuário: Feche o Administration Client e repita o comando. Se a condição persistir, entre em contato com o Suporte Técnico da IBM.

MQCAE022 Internal failure to save MQIPT configuration

Explicação: Um erro interno foi detectado durante a tentativa de salvar um arquivo de configuração em um MQIPT.

Resposta do Usuário: Feche o Administration Client e repita o comando. Se a condição persistir, entre em contato com o Suporte Técnico da IBM.

MQCAE023 MQIPT {0} did not recognize your password.

Explicação: O MQIPT espera uma senha válida; a que foi utilizada no último comando estava incorreta. A senha deve corresponder àquela que foi definida no arquivo de configuração

Resposta do Usuário: Altere a senha utilizando o painel do menu **MQIPT->Conexão** e repita o comando.

MQCAE024 MQIPT {0} has not recognized the command.

Explicação: O Administration Client enviou um comando para o MQIPT que não foi reconhecido.

Resposta do Usuário: Certifique-se de que a versão do

código utilizada pelo Administration Client seja igual à do MQIPT.

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

Explicação: O MQIPT tentou enviar o arquivo de configuração, mas falhou.

Resposta do Usuário: Feche o Administration Client e repita o comando. Se isso não funcionar, pare e inicie novamente o MQIPT.

MQCAE026 Remote shutdown is disabled on MQIPT {0}.

Explicação: Uma tentativa de encerrar o MQIPT remotamente falhou porque o encerramento remoto não estava ativado no arquivo de configuração.

Resposta do Usuário: Para ativar o encerramento remoto do MQIPT, edite o arquivo de configuração e defina a propriedade RemoteShutDown para true.

MQCAE027 Look and feel {0} is not supported.

Explicação: A Aparência e o Comportamento da plataforma que você está utilizando não está disponível.

Resposta do Usuário: O processamento continua com a Aparência e o Comportamento padrão do sistema.

MQCAE028 Look and feel class {0} cannot be found. A classe de aparência e comportamento {0} não foi encontrada.

Explicação: A Aparência e o Comportamento da plataforma que você está utilizando não está disponível.

Resposta do Usuário: O processamento continua com a Aparência e o Comportamento padrão do sistema.

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

Explicação: O número mínimo de threads de conexão deve ser menor ou igual ao valor de número máximo de threads de conexão.

Resposta do Usuário: Altere o valor apropriadamente.

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

Explicação: O número máximo de threads de conexão deve ser maior que o valor de número mínimo de threads de conexão.

Resposta do Usuário: Altere o valor apropriadamente.

MQCAE031 Port numbers must be in the range 0 to 65535

Explicação: Você está tentando definir um valor que não corresponde à especificação.

Resposta do Usuário: Altere o valor apropriadamente.

MQCAE032 Trace must be in the range 0 to 5

Explicação: Você está tentando definir um valor que não corresponde à especificação.

Resposta do Usuário: Altere o valor apropriadamente.

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

Explicação: Você está tentando definir um valor que não corresponde à especificação.

Resposta do Usuário: Altere o valor apropriadamente.

MQCAE049 No route has been selected on any MQIPT

Explicação: Foi feita uma tentativa de excluir uma rota sem primeiro selecioná-la.

Resposta do Usuário: Selecione uma rota e repita o comando.

MQCAE050 Could not connect to MQIPT {0}

Explicação: O Administration Client não pôde conectar-se ao MQIPT especificado.

Resposta do Usuário: Isso pode ser causado pelas seguintes razões:

- O MQIPT não está em execução.
- O MQIPT não está atendendo em sua porta de comando.
- Apenas um Administration Client está utilizando o CommandPort do MQIPT.
- O tempo limite do pedido expirou.

MQCAE051 Could not read reply from MQIPT {0}

Explicação: Foi recebida uma resposta do MQIPT que não estava em conformidade com o protocolo esperado.

Resposta do Usuário: Certifique-se de que a versão do código utilizada pelo Administration Client seja igual à do MQIPT.

MQCAE052 Configuration has not been saved

Explicação: Uma resposta válida foi recebida do MQIPT, mas, subseqüentemente, ele falhou ao salvar o arquivo de configuração.

Resposta do Usuário: Verifique se o MQIPT tem acesso de gravação para o arquivo de configuração.

MQCAE053 MQIPT has not confirmed saving of configuration

Explicação: O arquivo de configuração foi enviado para o MQIPT, mas o MQIPT falhou ao confirmá-lo.

Resposta do Usuário: Isso pode ser causado pelas seguintes razões:

- O MQIPT não está em execução.
- O MQIPT não está atendendo em sua porta de comando.
- Apenas um Administration Client está utilizando o CommandPort do MQIPT.
- O tempo limite do pedido expirou.

MQCAE054 MQIPT data has not been refreshed

Explicação: Foi feito contato com o MQIPT mas o Administration Client não pôde ler o arquivo de configuração.

Resposta do Usuário: Isso pode ser causado pelas seguintes razões:

1. O MQIPT falhou
2. O tempo limite do pedido expirou.

MQCAE055 No MQIPT or route on an MQIPT has been selected

Explicação: Sua opção de menu escolhida não pode ser executada porque nenhum MQIPT ou rota foi selecionado.

Resposta do Usuário: Selecione um MQIPT ou rota apropriado e tente novamente.

MQCAE056 Duplicate listener port has been rejected

Explicação: A porta do atendente especificada foi rejeitada porque já está sendo utilizada por outra rota.

Resposta do Usuário: Escolha uma porta de atendente diferente e tente novamente.

MQCAI002 The MQIPT has been removed from display

Explicação: O MQIPT cujo nó você selecionou na árvore foi removido da memória do cliente.

MQCAI003 New route added to the display

Explicação: A nova rota recentemente especificada foi incluída no MQIPT atual.

MQCAI004 Route has been removed from the display

Explicação: A rota que você selecionou na árvore foi removida da memória do cliente.

MQCAI005 Selected MQIPT is being displayed

Explicação: Os parâmetros globais do MQIPT que você selecionou na árvore estão sendo mostrados na tabela.

MQCAI006 Selected route is being displayed

Explicação: Os parâmetros da rota que você selecionou na árvore estão sendo mostrados na tabela.

MQCAI007 Client configuration has been saved

Explicação: Os parâmetros de acesso de todos os MQIPTs na árvore foram salvos.

MQCAI008 Display of online help succeeded

Explicação: A ajuda online foi exibida conforme solicitado.

MQCAI009 Table has been updated

Explicação: O valor recém-digitado na tabela foi utilizado para atualizar o modelo na memória.

MQCAI010 No MQIPT or route has been selected.

Explicação: Nenhuma ação foi executada porque não há informações suficientes para isso.

MQCAI011 User Action has been cancelled

Explicação: Você cancelou uma ação, envolvendo uma janela popup, que havia sido iniciada anteriormente.

MQCAI014 Configuration has been saved on MQIPT

Explicação: Um novo arquivo de configuração foi salvo no MQIPT que está atualmente selecionado na árvore e foi utilizado para iniciar novamente o MQIPT.

MQCAI015 Online help has terminated

Explicação: A ajuda online foi exibida conforme solicitado e, subseqüentemente, finalizada.

MQCAI017 Select File/Add MQIPT to add an MQIPT to the tree

Explicação: Esta mensagem aparece quando não há MQIPTs na árvore; ela indica como incluir um.

MQCAI018 New MQIPT added to display

Explicação: Um novo MQIPT foi incluído na árvore, conforme instruído.

MQCAI019 MQIPT access parameters have been changed

Explicação: Os parâmetros de acesso do MQIPT que estão atualmente selecionados na árvore foram alterados.

MQCAI021 Select an MQIPT or route on the tree to display its contents

Explicação: Esta mensagem aparece quando não há informações sendo mostradas na tabela; ela indica como exibir alguma.

MQCAI022 The command port has changed

Explicação: O MQIPT, cuja porta do comando foi instruída para ser alterada, agora foi alterado.

MQCAI023 The password has changed

Explicação: Qualquer comunicação futura com o MQIPT que você acabou de alterar utilizará a nova senha.

MQCAI025 MQIPT {0} has been refreshed.

Explicação: As informações contidas no MQIPT foram atualizadas pela leitura de seu arquivo de configuração.

MQCAI026 MQIPT {0} has received shutdown request.

Explicação: O MQIPT confirmou o recebimento de um pedido de encerramento e agora será encerrado.

MQCAI027 Client configuration has been refreshed

Explicação: As informações exibidas no Administration Client foram atualizadas no arquivo ″client.conf″ local.

MQCAI028 MQIPT {0} is active

Explicação: O MQIPT respondeu com êxito a um pedido de ping.

MQCAI029 MQIPT {0} is not active

Explicação: O MQIPT não respondeu a um pedido de ping dentro de um tempo específico.

Resposta do Usuário: Isso pode ser causado pelas seguintes razões:

- O MQIPT não está em execução.
- O MQIPT não está atendendo em sua porta de comando.
- O tempo limite do pedido expirou. O tempo limite pode ser aumentado alterando a propriedade de tempo limite nas informações de conexão do MQIPT.

MQCAI030 Route {0} is active

Explicação: O MQIPT respondeu com êxito a um pedido de ping.

MQCAI031 Route {0} is not active

Explicação: A rota do MQIPT não respondeu a um pedido de ping dentro de um tempo específico.

Resposta do Usuário: Isso pode ser causado pelas seguintes razões:

- O MQIPT não está em execução.
- O MQIPT não está atendendo em sua porta de comando.
- O tempo limite do pedido expirou. O tempo limite pode ser aumentado alterando a propriedade de tempo limite nas informações de conexão do MQIPT.

MQCAI100 This script is used to start the Administration Client for {0}. Especificar um proxy SOCKS permite que o Cliente Administrativo converse com um MQIPT através de um firewall.

Explicação: Informações de ajuda online para o script mqiptGui.

MQCAI101 Format of command is:

Explicação: Informações de ajuda online para o script mqiptGui.

MQCAI102 mqiptGui {socks_host{socks_port}}

Explicação: Informações de ajuda online para o script mqiptGui.

MQCAI103 socks_host-host name of SOCKS proxy (optional)

Explicação: Informações de ajuda online para o script mqiptGui.

MQCAI104 socks_port-SOCKS proxy port address (optional-default 1080)

Explicação: Informações de ajuda online para o script mqiptGui.

MQCPE000 Could not locate message data when handling message {0}

Explicação: O número de mensagem {0} não foi encontrado na lista de propriedades do sistema.

Resposta do Usuário: O arquivo ″mqipt.properties″ pode ter sido danificado e o número de mensagem especificado não pôde ser encontrado. Verifique o seguinte:

- o arquivo ″MQipt.jar″ está no CLASSPATH do sistema
- o arquivo ″mqipt.properties″ está no arquivo ″MQipt.jar″
- o número de mensagem está no arquivo ″mqipt.properties″

MQCPE001 Directory does not exist or is not a directory

Explicação: Durante a inicialização, um diretório requerido não pôde ser encontrado. Esta mensagem refere-se a um diretório especificado no arquivo de configuração mqipt.conf do MQIPT ou nas opções de partida da linha de comandos do MQIPT no diretório padrão.

Resposta do Usuário: Especifique o diretório correto e repita o comando.

MQCPE004 Route startup failed on port {0}

Explicação: Não foi possível iniciar a rota com o número de ListenerPort especificado.

Resposta do Usuário: Ocorreu um erro de E/S durante a partida da rota. Verifique outras mensagens de erro e logs de erros adjacentes para obter uma explicação adicional do problema.

MQCPE005 The configuration file {0} could not be found

Explicação: O arquivo de configuração ″mqipt.conf″ do MQIPT não pôde ser encontrado no diretório especificado

Resposta do Usuário: Especifique o diretório correto e repita o comando.

MQCPE006 The number of routes has exceeded {0}. MQIPT will start but this configuration is unsupported.

Explicação: Sua configuração excedeu o número máximo suportado de rotas para uma instância do MQIPT. A operação não será descontinuada mas, como resultado, o sistema poderá ficar instável ou sobrecarregado como resultado. As configurações que excedem o número máximo de rotas declarado não serão suportadas.

Resposta do Usuário: Considere iniciar as instâncias adicionais do MQIPT com menos rotas por instância.

MQCPE007 Route not restarted on listener port {0}

Explicação: Em uma operação REFRESH, a rota que estava operando no ListenerPort especificado não foi iniciada novamente na nova configuração.

Resposta do Usuário: Verifique outras mensagens de erro adjacentes para uma explicação adicional do problema.

MQCPE008 Duplicate route defined for listener port {0}

Explicação: Mais de uma rota foi definida com o mesmo valor de ListenerPort.

Resposta do Usuário: Remova rota duplicada do arquivo de configuração e repita o comando.

MQCPE009 LogPath parameter {0} is not valid.

Explicação: O caminho do log mostrado no texto não existe ou não pode ser acessado no momento.

Resposta do Usuário: Verifique se o diretório existe e é acessível pelo MQIPT.

MQCPE010 Listener or command port number {0} is not valid

Explicação: O número da porta fornecido para o parâmetro de porta do comando ou porta do atendente é inválido.

Resposta do Usuário: Especifique um número de porta que esteja disponível para ser utilizado. Para orientação sobre a utilização de números de porta na rede, consulte o administrador da rede.

MQCPE011 The trace level {0} is outside the valid range 0 - 5

Explicação: A opção de rastreio especificada foi solicitada, mas não está no intervalo válido 0-5.

Resposta do Usuário: Especifique um valor de rastreio de 0–5.

MQCPE012 The value {0} is not valid for the attribute {1}

Explicação: Um valor de propriedade inválido foi especificado.

Resposta do Usuário: Consulte este Guia do Usuário para obter detalhes completos dos valores válidos de cada parâmetro de controle.

MQCPE013 ListenerPort property was not found in route {0}

Explicação: O MQIPT detectou uma rota no arquivo de configuração que não contém uma propriedade ListenerPort. A propriedade ListenerPort é o identificador principal e exclusivo de cada rota e, portanto, é obrigatória.

Resposta do Usuário: Especifique um ListenerPort válido para a rota especificada.

MQCPE014 ListenerPort property value {0} is not valid

Explicação: Um endereço de porta inválido foi especificado para a propriedade ListenerPort de uma rota.

Resposta do Usuário: Um endereço de porta deve estar no intervalo 1024–65535. Verifique cada ListenerPort no arquivo de configuração.

MQCPE015 No text was found for message number {0}

Explicação: Foi encontrado um erro interno para o qual não há descrição disponível.

Resposta do Usuário: O arquivo ″mqipt.properties″ pode ter sido danificado e o número de mensagem especificado não pôde ser encontrado. Verifique o seguinte:

- consulte o arquivo Readme para verificar se há uma nova mensagem
- o arquivo ″MQipt.jar″ está no CLASSPATH do sistema
- o arquivo ″mqipt.properties″ está no arquivo ″MQipt.jar″
- o número de mensagem está no arquivo ″mqipt.properties″

MQCPE016 The maximum number of connection threads is {0} but this is less than the minimum number of connection threads, which is {1}

Explicação: Sua configuração especificou o número mínimo de threads de conexão com um valor que excede o número máximo de threads de conexão.

Resposta do Usuário: Isso pode ser um erro de uma única rota, um conflito entre uma propriedade global e uma propriedade de rota, ou uma propriedade de rota substituindo os valores padrão do sistema. Consulte os capítulos anteriores deste Guia do Usuário para obter detalhes completos dos valores válidos e padrões aplicáveis.

MQCPE017 The exception {0} was thrown, causing MQIPT to shut down

Explicação: O MQIPT terminou anormalmente e foi encerrado. Isso pode ter ocorrido por causa de condições e limitações ambientais do sistema, como estouro de memória.

Resposta do Usuário: Se a condição persistir, entre em contato com o Suporte Técnico da IBM.

MQCPE018 The ListenerPort property is blank - the route will not start

Explicação: O número de ListenerPort foi omitido em uma rota.

Resposta do Usuário: Edite o arquivo de configuração e inclua um ListenerPort válido.

MQCPE019 The stanza {0} was not found before the following: {1}

Explicação: Ocorreu um erro de seqüência no arquivo de configuração.

Resposta do Usuário: Edite o arquivo de configuração e certifique-se de que todas as entradas [route] estejam após as entradas [global].

MQCPE020 The new value for MaxConnectionThreads is {0}. Este valor deve ser maior que o valor atual {1}

Explicação: Depois que a rota é iniciada, a propriedade MaxConnectionThread só pode ser aumentada.

Resposta do Usuário: Edite o arquivo de configuração e altere a propriedade MaxConnectionThread.

MQCPE021 The property Destination was not supplied for route {0}

Explicação: A propriedade Destination é obrigatória dentro de uma rota, mas foi omitida na rota especificada.

Resposta do Usuário: Edite o arquivo de configuração e inclua uma propriedade Destination para a rota especificada.

MQCPE022 The CommandPort value {0} is outside the valid range 1 - 65535.

Explicação: A propriedade CommandPort estava fora do intervalo 1-65535.

Resposta do Usuário: Edite o arquivo de configuração e altere a propriedade CommandPort para um endereço de porta válido.

MQCPE023 Request for shutdown from Administration Client {0} is ignored because it is disabled.

Explicação: Uma tentativa de encerrar o MQIPT remotamente falhou porque o encerramento remoto não estava ativado no arquivo de configuração.

Resposta do Usuário: Para ativar o encerramento remoto do MQIPT, edite o arquivo de configuração e defina a propriedade RemoteShutDown para true.

MQCPE024 The command received by the MQIPT controller has not been recognized.

Explicação: O MQIPT recebeu um comando desconhecido através de sua porta de comando.

Resposta do Usuário: Verifique o arquivo ″mqipt.log″ para obter a identidade do comando.

MQCPE025 Failed to connect to server on host {0}, port {1}.

Explicação: O Cliente Administrativo (não-GUI) de modo de linha falhou ao se comunicar com o MQIPT.

Resposta do Usuário: Certifique-se de que a propriedade CommandPort tenha sido especificada como {1} no arquivo de configuração e o MQIPT esteja sendo executado em {0}.

MQCPE026 No reply received from server on host {0}, port {1}.

Explicação: O Cliente Administrativo (não-GUI) de modo de linha conectou-se ao MQIPT mas não recebeu uma resposta.

Resposta do Usuário: Isso indica que o tempo limite do pedido foi excedido ou há um problema com o MQIPT.

MQCPE027 Reply from MQIPT not recognized.

Explicação: O Cliente Administrativo (não-GUI) de modo de linha não reconhece uma resposta recebida do MQIPT.

Resposta do Usuário: Verifique se o script mqiptAdmin está utilizando a mesma versão do arquivo ″MQipt.jar″ que o MQIPT.

MQCPE028 Invalid stanza detected: {0}

Explicação: A sub-rotina declarada como desconhecida foi encontrada no arquivo de configuração.

Resposta do Usuário: Apenas as sub-rotinas [global] e [route] são válidas no arquivo de configuração.

MQCPE029 Was not able to flush log output.

Explicação: Algumas mensagens podem não ter sido gravadas no log porque o buffer de comunicação não pôde ser esvaziado.

Resposta do Usuário: Verifique se o disco do diretório inicial do MQIPT está cheio e se o MQIPT ainda tem acesso ao subdiretório logs.

MQCPE030 {0} not found in CLASSPATH.

Explicação: O arquivo jar especificado não foi encontrado na variável de ambiente CLASSPATH do sistema.

Resposta do Usuário: Inclua o arquivo especificado no CLASSPATH do sistema.

MQCPE031 {0} class not found.

Explicação: Esta mensagem é gerada durante a exibição do número de versão do MQIPT. A classe especificada não pôde ser encontrada no arquivo jar do MQIPT ou a variável de ambiente CLASSPATH do sistema foi danificada.

Resposta do Usuário: Verifique se o arquivo de classe especificado está no arquivo ″MQipt.jar″ e este, por sua vez, está no CLASSPATH do sistema.

MQCPE033 Failed to send configuration file to Administration Client at {0}

Explicação: Ocorreu um erro ao enviar o arquivo de configuração para o Administration Client.

Resposta do Usuário: Verifique se o arquivo de configuração está no diretório inicial do MQIPT e não está sendo compartilhado por outro processo.

MQCPE034 Administration Client at {0} did not supply the correct password.

Explicação: A propriedade AccessPW no arquivo de configuração não correspondeu àquela fornecida pelo Cliente Administrativo.

Resposta do Usuário: Altere a propriedade AccessPW no arquivo de configuração ou a senha salva no Cliente Administrativo.

MQCPE035 Failed to start command listener on port {0}

Explicação: Ocorreu um erro de E/S ao iniciar o atendente do comando no endereço de porta especificado.

Resposta do Usuário: Verifique o endereço de porta utilizado para a propriedade CommandPort no arquivo de configuração.

MQCPE038 MQIPT has not started as expected

Explicação: Esta mensagem é gerada pelo processo de bifurcação do mqipt, que inicia o MQIPT como um serviço do sistema.

Resposta do Usuário: Verifique os logs de erros para obter mais informações. Você pode tentar aumentar o tempo de inatividade utilizado pelo IPTFork antes dele verificar se o MQIPT está em execução. Edite o script

mqiptFork e aumente o parâmetro passado para o IPTFork.

MQCPE039 I/O error occurred running mqipt script

Explicação: Ocorreu um erro ao lançar o MQIPT a partir do processo de bifurcação

Resposta do Usuário: Verifique se a variável de ambiente PATH do sistema contém a localização do JDK e se o script mqipt tem autoridade para execução.

MQCPE040 Interruption occurred running mqipt script

Explicação: Ocorreu um erro depois de lançar o MQIPT a partir do processo de bifurcação.

Resposta do Usuário: Verifique os logs de erros para obter mais informações. Se a condição persistir, entre em contato com o Suporte Técnico da IBM.

MQCPE041 Unsupported level of Java - {0}

Explicação: O MQIPT foi iniciado utilizando o nível especificado do Java.

Resposta do Usuário: Verifique os pré-requisitos no Guia do Usuário para obter mais informações.

MQCPE042 There is a conflict with the following properties on route {0}:

Explicação: Algumas propriedades não podem ser utilizadas com outras. Esta mensagem precede a lista de propriedades em conflito.

Resposta do Usuário: Verifique as mensagens de erro seguintes e execute a ação apropriada.

MQCPE043 ....{0} and {1}

Explicação: As seguintes propriedades não podem ser definidas ao mesmo tempo na mesma rota.

Resposta do Usuário: Edite o arquivo de configuração e desative uma das propriedades especificadas na rota especificada.

MQCPE044 {0} is only valid on the {1} operating system

Explicação: Alguns recursos do MQIPT são válidos apenas em determinadas plataformas.

Resposta do Usuário: Edite o arquivo de configuração e desative a propriedade especificada.

MQCPE045 ....HTTP proxy name is missing

Explicação: A propriedade HTTPProxy deverá ser definida se a propriedade HTTP tiver sido definida como true.

Resposta do Usuário: Edite o arquivo de configuração e defina um HTTPProxy para a rota especificada.

MQCPE046 {0} is not allowed as Pagent has failed to initialize

Explicação: Pagent é o aplicativo que fornece a Qualidade de Serviço para o MQIPT. O MQIPT falhou ao inicializá-lo durante a partida e a propriedade QoS foi definida como true para a rota especificada.

Resposta do Usuário: Edite o arquivo de configuração e desativa a QoS para a rota especificada.

MQCPE047 Pagent has failed to initialize

Explicação: Pagent é o aplicativo que fornece a Qualidade de Serviço para o MQIPT. O MQIPT falhou ao inicializá-lo durante a partida.

Resposta do Usuário: Esta mensagem de erro poderá ser ignorada se o Pagent não estiver sendo utilizado, mas você deverá definir a propriedade QoS como false.

MQCPE048 Route startup failed on port {0}, exception was : {1}

Explicação: Não foi possível iniciar a rota com o número de ListenerPort especificado.

Resposta do Usuário: Verifique outras mensagens de erro e logs de erros adjacentes para obter uma explicação adicional do problema.

MQCPE049 Error starting or stopping the Java Security Manager {0}

Explicação: Uma exceção foi lançada durante a tentativa de iniciar ou parar o Java Security Manager.

Resposta do Usuário: O Java Security Manager foi ativado anteriormente, mas as permissões de tempo de execução não foram ativadas. Inclua um RuntimePermission para setSecurityManager em seu arquivo de política local. O MQIPT deve ser iniciado novamente para que as alterações entrem em vigor.

MQCPE050 Security exception on port {0} from the Administration Client

Explicação: Uma exceção de segurança foi lançada durante a aceitação de uma conexão do Cliente Administrativo.

Resposta do Usuário: O Java Security Manager foi ativado anteriormente, mas as permissões não foram concedidas para o host identificado na mensagem de

erro. Para permitir a conexão do host com o MQIPT, inclua um SocketPermission para aceitar/resolver conexões no endereço de porta do CommandPort. O Java Security Manager deve ser iniciado novamente para que as alterações entrem em vigor.

MQCPE051 Security exception accepting a connection on route {0}

Explicação: Uma exceção de segurança foi lançada durante a aceitação de uma conexão na rota especificada.

Resposta do Usuário: O Java Security Manager foi ativado anteriormente, mas as permissões não foram concedidas para o host identificado na mensagem de erro. Para permitir a conexão do host nesta rota, inclua um SocketPermission para aceitar/resolver conexões de ListenerPort. O Java Security Manager deve ser iniciado novamente para que as alterações entrem em vigor.

MQCPE052 Connection request on route {0} failed : {1}

Explicação: Esta mensagem é emitida no log de conexão para registrar uma exceção de segurança de um pedido de conexão.

Resposta do Usuário: O Java Security Manager foi ativado anteriormente, mas as permissões não foram concedidas para o host identificado na mensagem de erro. Para permitir a conexão do host nesta rota, inclua um SocketPermission para aceitar/resolver conexões de ListenerPort. O Java Security Manager deve ser iniciado novamente para que as alterações entrem em vigor.

MQCPE053 Security exception making a connection to {0}({1})

Explicação: Uma exceção de segurança foi lançada ao fazer uma conexão na rota especificada.

Resposta do Usuário: O Java Security Manager foi ativado anteriormente, mas as permissões não foram concedidas para o host identificado na mensagem de erro. Para permitir a conexão do host nesta rota, inclua um SocketPermission para aceitar/resolver conexões de ListenerPort. O Java Security Manager deve ser iniciado novamente para que as alterações entrem em vigor.

MQCPE054 Connection request to {0}({1}) failed : {2}

Explicação: Esta mensagem é emitida no log de conexão para registrar uma exceção de segurança de um pedido de conexão com um host de destino.

Resposta do Usuário: O Java Security Manager foi ativado anteriormente, mas as permissões não foram concedidas para o host identificado na mensagem de erro. Para permitir a conexão do host nesta rota, inclua um SocketPermission para aceitar/resolver conexões de ListenerPort. O Java Security Manager deve ser iniciado novamente para que as alterações entrem em vigor.

MQCPE055 ....Socks proxy name is missing

Explicação: A propriedade SocksProxy deverá ser definida se a propriedade SocksClient tiver sido definida como true.

Resposta do Usuário: Edite arquivo de configuração e defina um SocksProxy para a rota especificada.

MQCPE056 Conflict with route properties

Explicação: Algumas propriedades não pode ser utilizadas com outras.

Resposta do Usuário: Verifique as mensagens do console para obter detalhes do erro e execute a ação apropriada.

MQCPE057 Connection from {0} to host {1} closed - the SSL protocol ({2})was not recognized

Explicação: A rota foi colocada no modo de proxy SSL e o fluxo de dados inicial não é reconhecido.

Resposta do Usuário: Certifique-se de que apenas conexões SSL estejam sendo feitas nesta rota.

MQCPI001 {0} starting

Explicação: Esta instância do MQIPT está iniciando a execução. Seguem mensagens de inicialização adicionais.

MQCPI002 {0} shutting down

Explicação: O MQIPT está sendo encerrado. Isso pode resultar de um comando STOP, ou automaticamente se um erro de configuração impedir uma partida bem-sucedida da ação REFRESH.

MQCPI003 {0} shutdown complete

Explicação: O processo de encerramento foi concluído. Todos os processos do MQIPT agora estão encerrados.

MQCPI004 Reading configuration information from {0}

Explicação: O arquivo de configuração mqipt.conf do MQIPT está sendo lido no diretório descrito nesta mensagem.

MQCPI005 Listener port specified as not active - {0} -> {1}({2})

Explicação: A rota referida na mensagem foi marcada como inativa. Nenhum pedido de comunicação será aceito nesta rota.

MQCPI006 Route {0} has started and will forward messages to:

Explicação: Uma rota foi iniciada na porta do atendente mostrada nesta mensagem. Esta mensagem é seguida por outras mensagens que listam quaisquer propriedades associadas a esta rota.

MQCPI007 Route stopped on port {0}

Explicação: A rota que estava operando no ListenerPort especificado está sendo encerrada. Esta ação normalmente ocorre quando um comando REFRESH é emitido para o MQIPT e a configuração da rota foi alterada.

MQCPI008 Listening for control commands on port {0}

Explicação: Esta instância do MQIPT está atendendo a comandos de controle na porta especificada.

MQCPI009 Control command received: {0}

Explicação: Esta mensagem indica que um comando de controle foi recebido na porta do comando. Detalhes são incluídos na mensagem, onde aplicáveis.

MQCPI010 Stopping command port on {0}

Explicação: Em uma operação REFRESH, a porta do comando não está mais em uso na nova configuração. Os comandos não serão mais aceitos na porta especificada.

MQCPI011 The path {0} will be used to store the log files

Explicação: A saída de registro será direcionada para a localização descrita nesta mensagem, sob a configuração atual.

Resposta do Usuário: Isso poderá ser alterado se a configuração for corrigida e uma operação REFRESH for solicitada.

MQCPI012 Changing the value of MinConnectionThreads has no effect after the route is started

Explicação: O número mínimo de threads de conexão é atribuído durante a partida da rota e não pode ser alterado até que o MQIPT seja iniciado novamente.

MQCPI013 Connection from {0} to host {1} closed

Explicação: Esta mensagem é emitida no log de conexão para registrar a atividade da conexão.

MQCPI014 Connection from {0} to host {1} closed - the protocol was not recognized

Explicação: Esta mensagem é emitida no log de conexão para registrar a atividade da conexão.

MQCPI015 Connection from a client on {0} to host {1} was rejected because client access has been disabled on this route

Explicação: Esta mensagem é emitida no log de conexão para registrar a atividade da conexão.

MQCPI016 Connection from a queue manager on {0} to host {1} was rejected because queue manager access has been disabled on this route

Explicação: Esta mensagem é emitida no log de conexão para registrar a atividade da conexão.

MQCPI017 A queue manager on {0} was connected to host {1}

Explicação: Esta mensagem é emitida no log de conexão para registrar a atividade da conexão.

MQCPI018 A client on {0} was connected to host {1}

Explicação: Esta mensagem é emitida no log de conexão para registrar a atividade da conexão.

MQCPI019 {0} routes have been created - this exceeds the maximum number of supported routes, which is {1}

Explicação: O número máximo de rotas suportadas foi excedido.

Resposta do Usuário: O MQIPT continuará operando, mas é recomendável que uma segunda instância do MQIPT seja criada e as rotas divididas entre as duas.

MQCPI020 The configuration file has been sent to the Administration Client.

Explicação: Como resultado de um pedido do Cliente Administrativo, o arquivo de configuração foi enviado.

MQCPI021 Password checking has been enabled on the command port.

Explicação: Esta mensagem mostra que uma senha é requerida para acessar a porta do comando.

MQCPI022 Password checking has been disabled on the command port.

Explicação: Esta mensagem mostra que uma senha não é requerida para acessar a porta do comando.

MQCPI024 ....using HTTP proxy {0}({1})

Explicação: Esta mensagem indica que a conexão de saída para a rota será feita utilizando este proxy HTTP.

MQCPI025 The refresh requested by Administration Client {0} has finished.

Explicação: Como resultado do recebimento de um comando REFRESH, o MQIPT leu novamente seu arquivo de configuração e foi iniciado novamente.

MQCPI026 Administration Client {0} has requested shutdown.

Explicação: Como resultado do recebimento de um comando STOP, o MQIPT está sendo encerrado.

MQCPI027 {0} sent to {1} on port {2}

Explicação: Isso exibe, no console do sistema, o comando enviado pelo Cliente Administrativo de modo de linha (não-GUI) para o MQIPT designado.

MQCPI031 ......cipher suites {0}

Explicação: Esta mensagem lista os conjuntos de cifras em uso para esta rota.

MQCPI032 ......key ring file {0}

Explicação: Esta mensagem fornece o nome do arquivo do conjunto de chaves para esta rota.

MQCPI033 ......client authentication set to {0}

Explicação: Esta mensagem define se um servidor SSL está solicitando autenticação de cliente para esta rota.

MQCPI034 ....{0}({1})

Explicação: Esta mensagem mostra o endereço do destino e da porta de destino para esta rota.

MQCPI035 ....using {0}

Explicação: Esta mensagem mostra o protocolo que está sendo utilizado para o destino. Poderá ser o protocolo MQSeries, o encapsulamento HTTP ou a fragmentação HTTP.

MQCPI036 ....SSL Client side enabled with properties :

Explicação: Esta mensagem mostra que a rota utilizará o SSL para enviar dados para o host de destino.

MQCPI037 ....SSL Server side enabled with properties :

Explicação: Esta mensagem mostra que a rota utilizará o SSL para receber dados do host de envio.

MQCPI038 ......distinguished name(s) {0}

Explicação: Esta mensagem lista os nomes distintos utilizados para controlar a autenticação de certificados.

MQCPI039 ....via Socks proxy {0}({1})

Explicação: Esta mensagem mostra que a conexão de saída para esta rota será feita utilizando este proxy Socks, que é definido quando o MQIPT é iniciado a partir da linha de comandos.

MQCPI040 Command port has been accessed by Administration Client {0}

Explicação: Esta mensagem é gravada no console do sistema e no arquivo de log do MQIPT (se o registro estiver ativado). O MQIPT recebeu uma conexão do Cliente Administrativo.

MQCPI041 ....will reply to Network Dispatcher advisor requests in {0} mode

Explicação: Esta mensagem é gravada no console do sistema quando uma rota é iniciada. Utilizado para mostrar qual modo o MQIPT utilizará para responder ao consultor do Network Dispatcher. As opções válidas são o modo ″Normal″ e ″Replace″.

MQCPI042 Maximum connections reached on route {0} - further requests will be blocked

Explicação: Esta mensagem é gravada no console do sistema quando o número máximo de conexões tiver sido alcançado para a rota especificada. Pedidos adicionais serão bloqueados até que uma conexão seja liberada ou o valor de MaxConnectionThreads seja aumentado.

MQCPI043 Connections on route {0} now unblocked

Explicação: Esta mensagem é gravada no console do sistema quando a rota especificada está desbloqueada para os pedidos de conexão.

MQCPI044 MQIPT has been launched from system startup

Explicação: O MQIPT foi iniciado como um serviço do sistema.

MQCPI045 Launching MQIPT from system startup

Explicação: O MQIPT será iniciado como um serviço do sistema.

MQCPI046 Sleeping for {0} seconds while MQIPT is launched from system startup

Explicação: O processo de bifurcação ficará inativo durante este período de tempo antes de verificar se o MQIPT foi iniciado com êxito como um serviço do sistema.

MQCPI047 .....CA keyring file {0}

Explicação: Esta mensagem fornece o nome do arquivo do conjunto de chaves CA para esta rota.

MQCPI048 The ping by Administration Client {0} has finished

Explicação: Mensagem de resposta do IPTController para o Cliente Administrativo.

MQCPI049 ....QoS priority to dest = {0}, to caller = {1}

Explicação: Isso mostra a prioridade de tráfego em ambas as direções nesta rota.

MQCPI050 Adding entry to inittab to automatically start MQIPT at system startup

Explicação: O usuário executou o script mqiptService para iniciar o MQIPT como um serviço do sistema.

MQCPI051 Removing entry from inittab that automatically starts MQIPT at system startup

Explicação: O usuário executou o script mqiptService para impedir que o MQIPT inicie como um serviço do sistema.

MQCPI052 ....Socks server side enabled

Explicação: Esta rota agirá como um servidor SOCKS (proxy) e aceitará conexões de um aplicativo ativado para socks.

MQCPI053 Starting the Java Security Manager

Explicação: O Java Security Manager padrão será iniciado porque a propriedade SecurityManager foi definida como true

MQCPI054 Stopping the Java Security Manager

Explicação: O Java Security Manager padrão será parado porque a propriedade SecurityManager foi definida como false

MQCPI055 Setting the java.security.policy to {0}

Explicação: O Java Security Manager padrão está prestes a ser iniciado e utilizará o arquivo de política fornecido.

MQCPI056 The Java Security Manager must be restarted to use a new policy file

Explicação: A propriedade SecurityManagerPolicy foi alterada, mas só entrará em vigor depois que o Java Security Manager for iniciado novamente.

Resposta do Usuário: Altere a propriedade SecurityManager como false e emita um comando refresh com a finalidade de parar o Java Security Manager. Em seguida, altere o SecurityManager novamente para true e emita um outro comando refresh para iniciar o Java Security Manager com o novo arquivo de política.

MQCPI057 ....trace level {0} enabled

Explicação: Esta mensagem é gravada no console do sistema quando uma rota é iniciada. Utilizada para mostrar o nível de rastreio ativado nesta rota.

MQCPI058 ....and a URI name of {0}

Explicação: Esta mensagem é gravada no console do sistema quando uma rota é iniciada. Utilizada para mostrar o nome de Uniform Resource Identifier nesta rota.

MQCPI059 ....servlet client enabled

Explicação: Esta mensagem é gravada no console do sistema quando uma rota é iniciada. Esta rota será conectada ao servlet do MQIPT.

MQCPI060 Installing files to automatically start MQIPT at system startup

Explicação: O usuário executou o script mqiptService para iniciar o MQIPT como um serviço do sistema.

MQCPI061 Removing files that automatically starts MQIPT at system startup

Explicação: O usuário executou o script mqiptService para impedir que o MQIPT inicie como um serviço do sistema.

MQCPI064 ....no SSL authentication on this route

Explicação: Esta mensagem é gravada no console do sistema quando uma rota é iniciada e mostra que não há autenticação SSL em uso para esta rota, pois um conjunto de cifras anônimo foi especificado.

MQCPI065 ....in SSL proxy mode

Explicação: Esta mensagem é gravada no console do sistema quando uma rota é iniciada e mostra que a rota está trabalhando no modo de proxy SSL.

MQCPI100 This script is used to start {0}

Explicação: Mensagem de ajuda online do script mqipt.

MQCPI101 Format of command is :

Explicação: Mensagem de ajuda online do script mqipt.

MQCPI102 mqipt {dir_name}

Explicação: Mensagem de ajuda online do script mqipt.

MQCPI103 dir_name - directory containing mqipt.conf

Explicação: Mensagem de ajuda online do script mqipt.

MQCPI106 This script is used to display the current version number of {0}

Explicação: Mensagem de ajuda online do script mqiptVersion.

MQCPI107 mqiptVersion {-v}

Explicação: Mensagem de ajuda online do script mqiptVersion.

MQCPI108 where -v will also display the build timestamp

Explicação: Mensagem de ajuda online do script mqiptVersion.

MQCPI109 This script is used to start {0}, from system startup, in another JVM and is only used in mqipt.ske. Use the mqipt script to start MQIPT from the command line.

Explicação: Mensagem de ajuda online do script mqiptFork.

MQCPI110 This class is used to display a simple NLS message on the console

Explicação: Mensagem de ajuda online da classe IPTMessages.

MQCPI111 java com.ibm.mq.ipt.IPTMessages (message_id1) {message_id2} {message_id...}

Explicação: Mensagem de ajuda online da classe IPTMessages.

MQCPI112 where message_id matches a key in the file mqipt.properties

Explicação: Mensagem de ajuda online da classe IPTMessages.

MQCPI113 This script is used to manage MQIPT as a system service

Explicação: Mensagem de ajuda online do script mqiptService.

MQCPI114 mqiptService (-install | -remove)

Explicação: Mensagem de ajuda online do script mqiptService.

MQCPI115 -install will install files to start MQIPT automatically at system startup

Explicação: Mensagem de ajuda online do script mqiptService.

MQCPI116 -remove will remove files that start MQIPT automatically at system startup

Explicação: Mensagem de ajuda online do script mqiptService.

Índice Remissivo

J

K

L

M

N

P

Q

R

S

T

U

V

W

Z

Enviando Comentários à IBM

Se você desejar expressar seus comentários sobre este manual, utilize um dos métodos listados abaixo para enviá-los para a IBM.

Sinta-se à vontade para comentar sobre erros ou omissões específicas e sobre a exatidão, organização, assunto ou integralidade deste manual.

Solicitamos, por gentileza, que os comentários limitem-se às informações deste manual e ao modo de apresentação das informações.

Para fazer comentários sobre as funções de produtos ou sistemas da IBM, fale com o seu representante da IBM ou com o seu revendedor autorizado da IBM.

Quando o Cliente envia seus comentários para IBM, concede direitos, não exclusivos, à IBM para usá-los ou distribuí-los da maneira que achar conveniente, sem que isso implique em qualquer obrigação para com o cliente.

Os comentários podem ser enviados à IBM de uma das seguintes maneiras:

- Por correio, para este endereço:

  Centro Industrial
  IBM Brasil
  Centro de Traduções MM21
  Caixa Postal 71
  13001-970
  Campinas, SP,
  Brasil

- Eletronicamente, utilize o ID de rede apropriado:
  - Intercâmbio de Correio da IBM: GBIBM2Q9 at IBMMAIL
  - IBMLink: HURSLEY(IDRCF)
  - Internet: idrcf@hursley.ibm.com

Qualquer que seja o método utilizado, certifique-se de incluir:

- O título e o número de pedido da publicação
- O tópico a que se refere seu comentário
- Seu nome e endereço/número de telefone/número de fax/ID de rede.

Impresso em Brazil

S517-7421-00