



WebSphere MQ Internet Pass-Thru Versão 1.3

Aviso!

Antes de utilizar estas informações e o produto suportado por elas, leia as informações gerais em “Avisos”, na página 171.

Segunda Edição (Março de 2003)

Esta edição se aplica à Versão 1.3 do WebSphere MQ Internet Pass-Thru (número do programa 5639-L92) e a todos os releases e modificações subsequentes, até que seja indicado de outra forma em novas edições.

© Copyright International Business Machines Corporation 2000, 2003. Todos os direitos reservados.

Índice

Figuras	v
--------------------------	----------

Prefácio	vii
---------------------------	------------

O Que É Internet Pass-Thru?	vii
Quem Deve Ler este Manual	vii
O Que É Preciso Saber para Entender Este Documento	vii
Pré-Requisitos	vii
Informações de Acessibilidade	viii

Resumo das Alterações.	ix
---	-----------

Alterações Nesta Edição (5517-7421-01)	ix
Alterações na Terceira Edição (SC34-6100-00)	ix
Alterações na Segunda Edição	ix

Capítulo 1. Introdução ao WebSphere MQ Internet Pass-Thru	1
--	----------

Capítulo 2. Como Funciona o Internet Pass-Thru	7
---	----------

Visão Geral de Como Funciona o Internet Pass-Thru	7
Configurações de Canal Suportadas	8

Capítulo 3. Suporte ao HTTP	9
--	----------

HTTPS	10
Servlet	10

Capítulo 4. Suporte ao Socks	13
---	-----------

Clustering	13
----------------------	----

Capítulo 5. Visão Geral e Suporte a SSL	15
--	-----------

Protocolo de Reconhecimento SSL	16
WebSphere MQ internet pass-thru e SSL	17
Definições de Confiança	17
Testando o SSL	18
Mensagens de Erro do SSL	18
LDAP e CRLs	19
O Padrão Avançado de Criptografia	21
Selecionando Certificados de um Arquivo de Conjunto de Chaves	21
Criptografando uma Senha do Conjunto de Chaves KeyMan	21
Tipos de Token Suportados	22
Formatos de Dados Padrão Suportados	23
FAQs (Perguntas Mais Frequentes) do KeyMan	24

Capítulo 6. Qualidade de Serviço	27
---	-----------

QoS (Qualidade de Serviço)	27
--------------------------------------	----

Capítulo 7. Network Dispatcher	29
---	-----------

Suporte ao Network Dispatcher	29
---	----

Capítulo 8. Java Security Manager e Saídas de Segurança	31
--	-----------

Java Security Manager	31
Saída de Segurança	32
A Classe com.ibm.mq.ipt.SecurityExit	33
A Classe com.ibm.mq.ipt.SecurityExitResponse	36
Rasteio	37

Capítulo 9. Controle do Endereço de Porta	39
--	-----------

Controle do Endereço de Porta	39
Sistemas com Várias Hospedagens	39

Capítulo 10. Outras Considerações de Segurança	41
---	-----------

Outras Considerações de Segurança	41
---	----

Capítulo 11. Recursos Diversos	43
---	-----------

Terminação Normal e Condições de Falha	43
Segurança de Mensagens	43
Logs de Conexão	43

Capítulo 12. Fazendo Upgrade da Versão Anterior	45
--	-----------

Novas Opções de Configuração	45
--	----

Capítulo 13. Instalando o Internet Pass-Thru no Windows	47
--	-----------

Fazendo Download e Instalando os Arquivos	47
Configurando o Internet Pass-Thru	48
Iniciando o Internet Pass-Thru a partir da Linha de Comandos	48
Iniciando o Cliente Administrativo a partir da Linha de Comandos	49
Utilizando um Programa de Controle de Serviços do Windows	49
Desinstalando o internet pass-thru como Serviço do Windows	50
Desinstalando o Internet Pass-Thru	50

Capítulo 14. Instalando o Internet Pass-Thru no Sun Solaris	51
--	-----------

Fazendo Download e Instalando os Arquivos	51
Configurando o Internet Pass-Thru	52
Iniciando o Internet Pass-Thru a partir da Linha de Comandos	52
Iniciando o Internet Pass-Thru Automaticamente	53
Iniciando o Cliente Administrativo a partir da Linha de Comandos	53
Desinstalando o Internet Pass-Thru	54

Capítulo 15. Instalando o Internet Pass-Thru no AIX	55
Fazendo Download e Instalando os Arquivos	55
Configurando o Internet Pass-Thru	56
Iniciando o Internet Pass-Thru a partir da Linha de Comandos.	56
Iniciando o Internet Pass-Thru Automaticamente	57
Iniciando o Cliente Administrativo a partir da Linha de Comandos.	57
Desinstalando o Internet Pass-Thru	58

Capítulo 16. Instalando o Internet Pass-Thru no HP-UX.	59
Fazendo Download e Instalando os Arquivos	59
Configurando o Internet Pass-Thru	60
Iniciando o Internet Pass-Thru a partir da Linha de Comandos.	60
Iniciando o Internet Pass-Thru Automaticamente	61
Iniciando o Cliente Administrativo a partir da Linha de Comandos.	61
Desinstalando o Internet Pass-Thru	62

Capítulo 17. Instalando o Internet Pass-Thru no Linux	63
Fazendo Download e Instalando os Arquivos	63
Configurando o Internet Pass-Thru	64
Iniciando o Internet Pass-Thru a partir da Linha de Comandos.	64
Iniciando o Internet Pass-Thru Automaticamente	65
Iniciando o Cliente Administrativo a partir da Linha de Comandos.	65
Desinstalando o Internet Pass-Thru	66

Capítulo 18. Instalação Genérica do UNIX.	67
Fazendo Download e Instalando os Arquivos	67
Configurando o Internet Pass-Thru	68
Iniciando o Internet Pass-Thru a partir da Linha de Comandos.	69
Iniciando o Internet Pass-Thru Automaticamente	70
Iniciando o Cliente Administrativo a partir da Linha de Comandos.	70
Desinstalando o Internet Pass-Thru	70

Capítulo 19. Administrando e Configurando o Internet Pass-Thru	71
Utilizando o Cliente Administrativo para o Internet Pass-Thru	71
Iniciando o Cliente Administrativo	71
Administrando um MQIPT	72
A Herança de Propriedades	72
Opções do Menu Arquivo	73
Opções de Menu do MQIPT.	73
Opções do Menu Ajuda	75
Utilizando Comandos de Modo de Linha do Internet Pass-Thru	75

Administrando o Internet Pass-Thru Utilizando Comandos de Modo de Linha	75
Informações de Referência sobre Configuração	76
Resumo de Propriedades	77
Informações de Referência da Seção Global.	80
Informações de Referência da Seção Route	81

Capítulo 20. Iniciando o Internet Pass-Thru	95
Suposições.	95
Configurações de Exemplo	96
Teste de Verificação de Instalação	96
Autenticação do Servidor SSL	98
Autenticação do Cliente SSL	100
Configuração do Proxy HTTP	103
Configurando o Controle de Acesso	105
Configurando a QoS (Qualidade de Serviço)	108
Configurando o Proxy SOCKS	111
Configurando o Cliente SOCKS	113
Criando Certificados de Teste SSL	114
Configurando o Servlet do MQIPT	115
Configuração HTTPS	118
Configurando o Suporte ao Clustering do MQIPT	121
Criando um Arquivo de Conjunto de Chaves.	125
Alocando Endereços de Porta	127
Utilizando um Servidor LDAP	129
Modo de Proxy SSL	133
Regravação Apache	135
Saída de Segurança	139
Saída de Segurança de Roteamento	141
Saída Dinâmica de Uma Rota	144

Capítulo 21. Inspeccionando o Internet Pass-Thru	149
Manutenção	149
Determinação de Problemas	149
Iniciando Automaticamente o Internet Pass-Thru	151
Verificando a Conectividade de Ponta a Ponta	151
Rastreamento de Erros	151
Relatando Problemas	151
Ajuste de Desempenho	152
Gerenciamento do Conjunto de Encadeamentos	152
Encadeamentos de Conexão	152
Tempo Limite Inativo.	152

Capítulo 22. Mensagens	153
---	------------

Apêndice. Avisos.	171
Marcas	171

Bibliografia	173
-------------------------------	------------

Índice Remissivo	175
-----------------------------------	------------

Enviando Comentários à IBM	179
---	------------

Figuras

1. Exemplo do MQIPT como um concentrador de canais	1	23. Configuração do proxy SOCKS.	112
2. Exemplo do MQIPT com uma “zona desmilitarizada”	2	24. Diagrama de rede do cliente SOCKS	113
3. Exemplo de encapsulamento do MQIPT e do HTTP	2	25. Configuração do cliente SOCKS	113
4. Exemplo do MQIPT e do SSL	3	26. Diagrama de rede do servlet	115
5. Topologia do WebSphere MQ mostrando as configurações do MQIPT possíveis	4	27. Configuração do servlet	116
6. Suporte ao Clustering do MQIPT	14	28. Diagrama de rede do HTTPS	118
7. Utilizando o Network Dispatcher com o MQIPT	29	29. Configuração HTTPS	119
8. Janela para acessar pela primeira vez um MQIPT	72	30. Diagrama de rede de clustering	122
9. Incluindo uma rota	74	31. Configuração de clustering	123
10. Diagrama de rede do IVT.	96	32. Diagrama de rede de alocação de portas	127
11. Configuração do IVT	97	33. Configuração da alocação de portas	128
12. Diagrama de rede do servidor SSL.	98	34. Diagrama de rede do servidor LDAP	130
13. Autenticação do servidor SSL	99	35. configuração do servidor LDAP	131
14. Diagrama de rede do cliente SSL	101	36. Diagrama de rede do servidor LDAP	133
15. Autenticação do cliente SSL.	101	37. Configuração do modo de proxy SSL	134
16. Diagrama de rede proxy HTTP	103	38. Diagrama de rede de regravação Apache	136
17. Configuração do proxy HTTP	104	39. Configuração da regravação Apache	137
18. Diagrama de rede de controle de acesso	105	40. Diagrama de rede da saída de segurança	140
19. Configuração do controle de acesso	106	41. Configuração da saída de segurança	140
20. Diagrama de rede de QoS	108	42. Diagrama de rede de roteamento da saída de segurança	142
21. Configuração de QoS	109	43. Configuração de roteamento da saída de segurança	143
22. Diagrama de rede do proxy SOCKS	111	44. Diagrama de rede para saída dinâmica de uma rota	145
		45. Configuração de saída dinâmica de uma rota	146
		46. Fluxograma de determinação de problemas	150

Prefácio

O Que É Internet Pass-Thru?

WebSphere MQ internet pass-thru era conhecido 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, envelopando 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 por meio 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
- Registra todas as tentativas de conexão

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

Quem Deve Ler 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 *WebSphere MQ System Administration Guide* e *WebSphere MQ 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 V5.1
- HP-UX 11
- Linux

O tempo de execução J2SE V1.4.0 (JRE) é necessário para o servidor MQIPT. O SDK, V1.4.0, é necessário para criar uma saída de segurança.

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-e, 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 a tecla Enter.

Aparência e Comportamento

O ideal é que a GUI adote a aparência e o comportamento do ambiente. Como isso nem sempre é possível, você pode providenciar um arquivo de configuração para adaptar a aparência e o 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.

Resumo das Alterações

Esta seção descreve alterações nesta edição do WebSphere MQ Internet Pass-Thru. As alterações posteriores à edição anterior estão marcadas com linhas verticais à esquerda.

Alterações Nesta Edição (5517-7421-01)

As melhorias nesta versão do WebSphere MQ Internet Pass-Thru incluem:

- Uma saída de segurança para controlar pedidos de conexão do cliente
- Suporte a LDAP para CRLs e ARLs
- Criptografia de senhas do conjunto de chaves
- Seleção de certificado de um conjunto de chaves
- Novo conjunto de cifras AES
- Imagem de disco genérica do UNIX
- Controle de ação de reinício de rota
- Agora, as plataformas AIX e HP-UX oferecem suporte a Java 1.4

Alterações na Terceira Edição (SC34-6100-00)

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

- Controle de alocação do endereço de porta de saída
- Configurações de exemplo
- Rastreamento 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 o servidor do Socks
- Modo proxy do SSL
- Suporte a sistema com várias hospedagens
- Status de luz tráfego para o Cliente Administrativo
- Suporte a clusters do WebSphere MQ

Alterações na Segunda Edição

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

- Adição de AIX, HP-UX e Windows 2000 como plataformas para o MQIPT
- Adição de suporte a proxy HTTP
- Adição de suporte a SSL (Secure Socket Layer)
- Capacidade do MQIPT de comunicar-se com outro MQIPT ou servidor MQSeries externo, por meio de um proxy SOCKS

- Uso de uma GUI do Cliente Administrativo para facilitar a administração de um ou mais MQIPTs
- Adição de suporte ao IBM Network Dispatcher
- Melhorias secundárias no rastreamento
- Melhorias secundárias no comando mqiptAdmin

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 colocado 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 proibir 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.

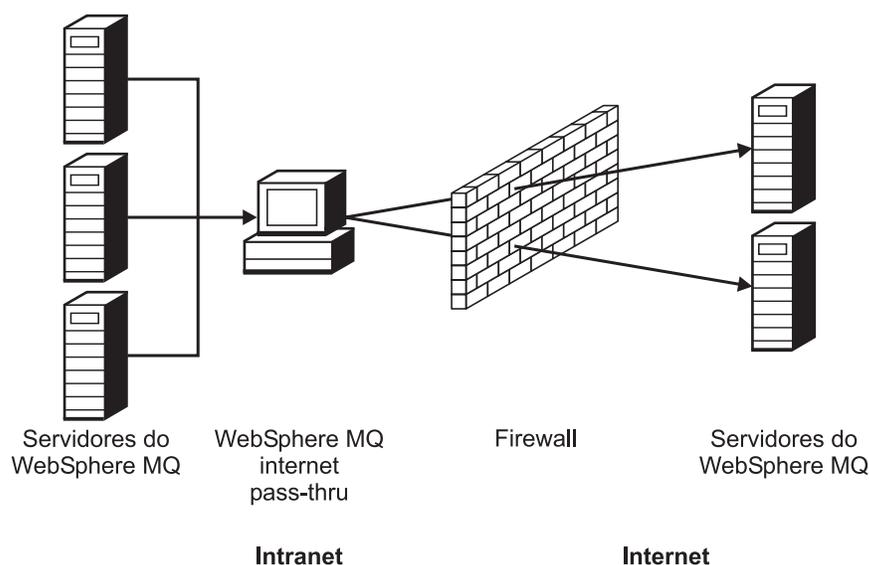


Figura 1. Exemplo do MQIPT como um concentrador de canais

- 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.

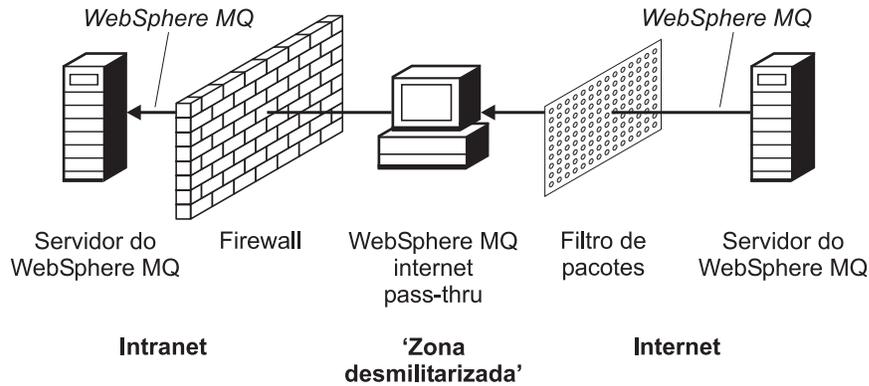


Figura 2. Exemplo do MQIPT com uma “zona desmilitarizada”

- Se dois MQIPTs forem implementados em linha, poderão comunicar-se utilizando HTTP ou SSL. O recurso de encapsulamento HTTP permite que os pedidos sejam transmitidos por meio 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.

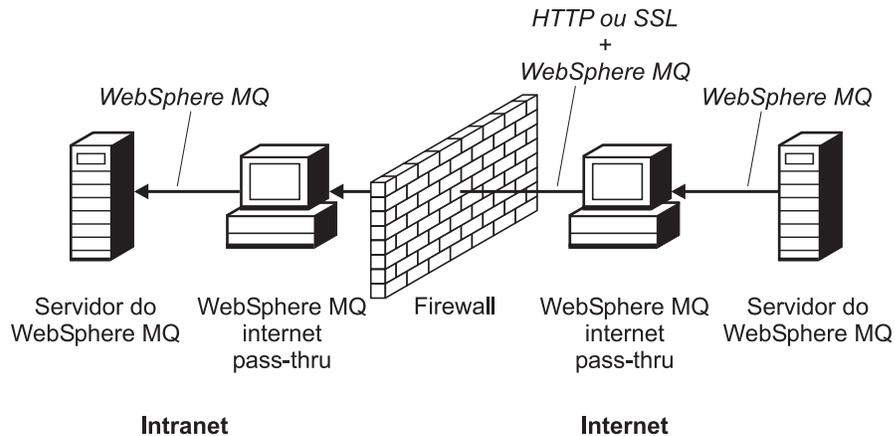


Figura 3. Exemplo de encapsulamento do MQIPT e do HTTP

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

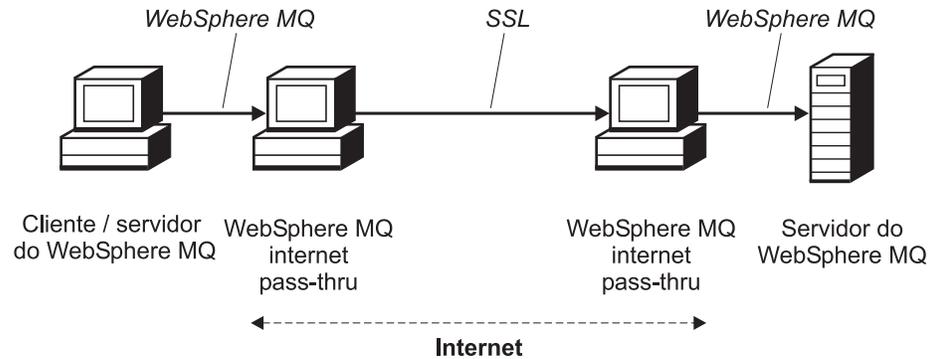


Figura 4. Exemplo do MQIPT e do SSL

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 paginação 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 rastreo.

O intervalo completo dos tipos de canais do WebSphere MQ pode ser determinado por um ou mais MQIPs. A presença de MQIPs 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 MQIPs 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 por meio de uma ou máquinas de proxies SOCKS ou HTTP ou máquinas do MQIPT adicionais, antes de chegar ao seu destino.

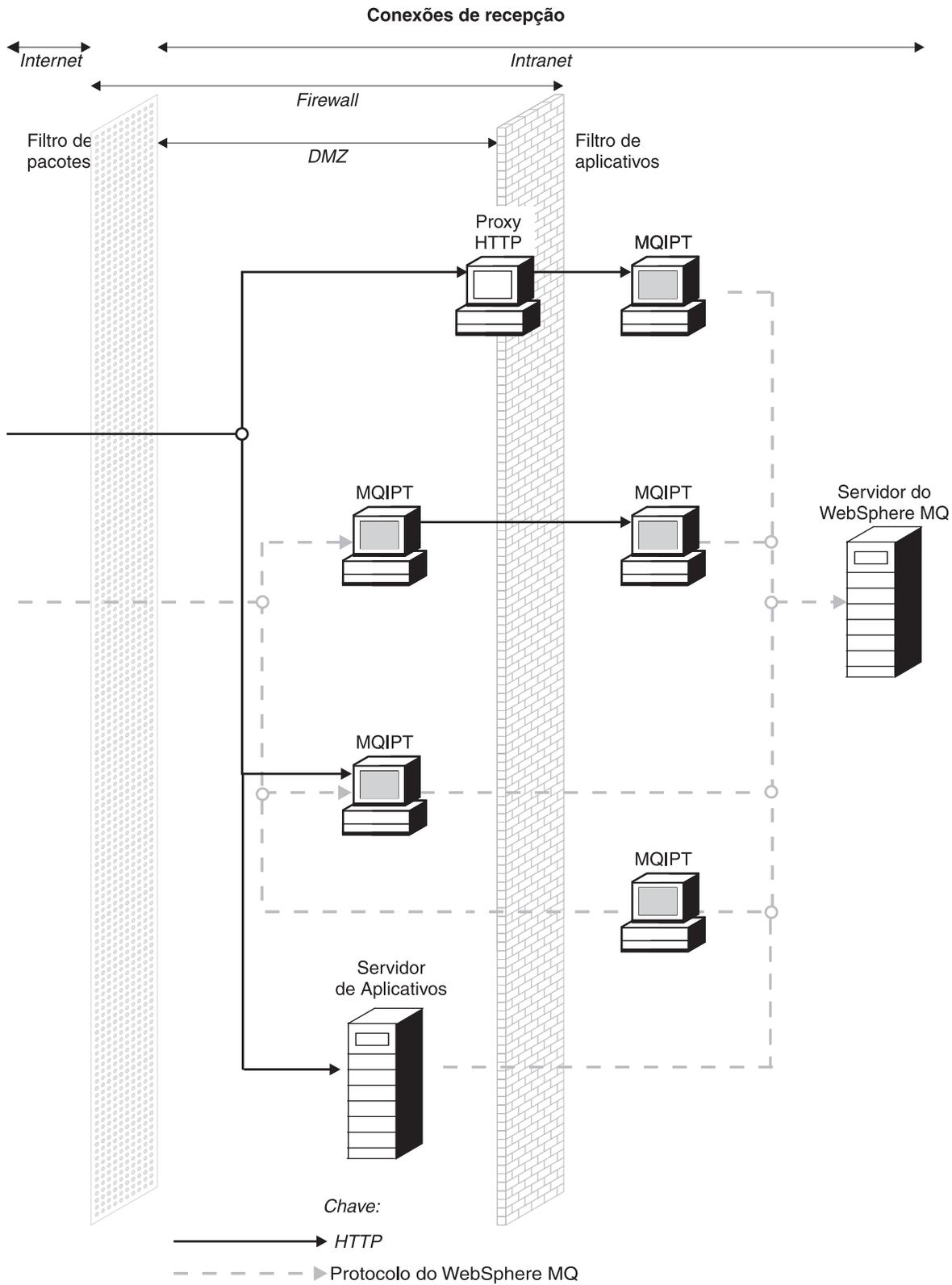


Figura 5. Topologia do WebSphere MQ mostrando as configurações do MQIPT possíveis (Parte 2 de 2)

Capítulo 2. Como Funciona o Internet Pass-Thru

Este capítulo fornece uma visão geral de como o internet pass-thru funciona.

Visão Geral de Como Funciona o 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 lê os dados recebidos e simplesmente os transmite 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 por meio 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.

O MQIPT utiliza um arquivo de configuração denominado mqipt.conf, que contém definições de todas as rotas e suas propriedades associadas. Consulte o Capítulo 19, "Administrando e Configurando o Internet Pass-Thru", na página 71 para obter mais informações sobre esse arquivo.

Ao ser ativado, o MQIPT inicia cada rota no arquivo de configuração. As mensagens são gravadas no console do sistema, mostrando o status de cada rota. Quando a mensagem MQCPI078 aparece para uma rota, significa que ela está pronta para aceitar pedidos de conexão.

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 o servidor.

Canais de emissor/receptor de cluster

Se o MQIPT recebe um pedido de entrada de um canal cluster-emissor, ele pressupõe 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 autodefinidos.

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.

Capítulo 3. Suporte ao HTTP

O MQIPT pode ser configurado para que os pacotes de dados que 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 MQIPs, 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 MQIPs não fecham a conexão TCP/IP entre os pares de pedido/resposta.

Se dois MQIPs estiverem se comunicando por meio 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

Consulte “Configuração do Proxy HTTP” na página 103 para obter um exemplo de uso de HTTP.

HTTPS

O HTTPS pode ser utilizado em uma conexão HTTP, ativando as propriedades de rota HTTPS e SSLClient no MQIPT, emitindo a conexão do cliente. O MQIPT deve ter acesso ao certificado CA confiável que será utilizado para autenticar o proxy/servidor HTTP de destino. A propriedade SSLClientCAKeyring pode ser utilizada para definir o arquivo do conjunto de chaves que contém o certificado CA confiável.

Uma configuração comum do HTTPS utilizaria um proxy HTTP local para criar um túnel por meio de um firewall e conectar-se a um servidor HTTP remoto (ou a outro proxy), que por sua vez seria conectado ao MQIPT remoto. Esse MQIPT no lado do servidor da conexão não precisa de configurações específicas, uma vez que o pedido de conexão é tratado como uma conexão HTTP normal.

O MQIPT utiliza as propriedades HTTPProxy e HTTPServer para distinguir os proxies local e remoto. O HTTPProxy é visto como o proxy HTTP local e HTTPServer como o servidor (ou proxy) remoto.

As conexões HTTPS normalmente são feitas no endereço de porta do atendente 443 no proxy/servidor HTTP, mas HTTPProxyPort e HTTPServerPort podem ser utilizados para substituir esse padrão. Consulte “Configuração HTTPS” na página 118 para obter um exemplo de uso de HTTPS.

Servlet

Há agora uma versão de servlet do MQIPT (denominada MQIPTServlet) que pode ser implementada em um Servidor de Aplicativos como aplicativo não distribuído. Ela funciona de forma semelhante ao MQIPT normal, mas 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 subsequentes 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 da web. Esse war deve ser importado/implementado no Servidor de Aplicativos. Se for necessário especificar um nome de contexto ao importar esse servlet, você precisará substituir a propriedade UriName padrão para conter o novo nome de contexto. Consulte “UriName” na página 94 para obter mais informações.

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 rastreamento são gravados em um diretório definido com uma nova propriedade denominada LogDir. Recomenda-se que você defina essa propriedade antes de iniciar o MQIPTServlet.

Para controlar a quantidade de recursos utilizados pelo MQIPTServlet, pode ser necessário alterar algumas das propriedades do Servidor de Aplicativos. Cada Servidor de Aplicativos tem sua própria forma de gerenciar dados de configuração, o que normalmente é feito utilizando uma GUI, uma interface da Web ou editando o arquivo de configuração. As propriedades que podem ser alteradas são o número máximo de sessões ativas ou o número de instâncias do servlet dentro do Servidor de Aplicativos. Essas propriedades controlam o número de conexões clientes e é semelhante à propriedade MaxConnectionThreads utilizada no MQIPT.

Outras propriedades que talvez tenham que ser alteradas estão relacionadas a valores de tempo limite, se há suporte a conexões persistentes e quantos pedidos são permitidos em uma conexão persistente. Como o MQIPTServlet confia em uma conexão persistente com o Gerenciador de Filas de destino, essa propriedade deve ser ativada. As outras propriedades talvez tenham que ser aumentadas, mas isto depende de seu valor padrão e do tipo de conexão do WebSphere MQ que está sendo utilizada. As conexões clientes do WebSphere MQ normalmente têm um tempo de vida curto, portanto, é relativamente seguro utilizar os valores padrão. As conexões de um Gerenciador de Filas para outro podem ser executadas por tempo indeterminado. Nesse caso, é recomendado que alguns dos valores de tempo limite e o número de pedidos permitidos em uma conexão persistente sejam aumentados da forma apropriada.

Existe também uma propriedade de tempo limite da sessão, definida no arquivo web.xml com um valor padrão de 30 minutos. Essa propriedade pode ser utilizada para controlar a inatividade de um cliente e fechará a sessão quando não for detectada atividade por um determinado tempo.

Deve haver no mínimo um MQIPT no link entre o cliente e o MQIPTServlet. A propriedade ServletClient deve ser ativada no MQIPT que se conecta ao MQIPTServlet e à propriedade HTTPServer pode indicar diretamente o Servidor de Aplicativos ou o servidor HTTP que alimenta o Servidor de Aplicativos.

Para testar se o MQIPTServlet foi iniciado com êxito, você pode ativar um navegador da Web e digitar um nome de URL semelhante ao seguinte:

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

uma resposta positiva será observada no navegador.

O MQIPTServlet foi testado com o IBM WebSphere Application Server 5.0 (com e sem o IBM HTTP Server), Tomcat 3.3 e Tomcat 4.0. O MQIPTServlet não exige Java 1.4 e utilizará o nível de Java implementado pelo Servidor de Aplicativos.

Consulte “Configurando o Servlet do MQIPT” na página 115 para obter um exemplo de como utilizar o servlet.

Capítulo 4. Suporte ao Socks

O proxy Socks é um serviço de rede utilizado como ponto controlado de saída por um firewall. Um aplicativo ativado para Socks, em execução dentro do firewall, pode utilizar o proxy Socks para conectar-se a um aplicativo remoto.

O MQIPT pode agir como proxy Socks, ativando a propriedade SocksServer e permitindo assim que um aplicativo WMQ ativado para Socks conecte-se por meio de MQIPT a um gerenciador de filas WMQ remoto. Ao utilizar esse recurso, o destino e o endereço de porta de destino são obtidos durante o processo de reconhecimento do Socks, portanto, as propriedades de rota Destination e DestinationPort são substituídas. Este é um recurso chave para suportar o cluster WMQ. Consulte mais informações a seguir.

O MQIPT também pode agir como cliente Socks, em nome de um aplicativo WMQ local não ativado para Socks. Isto é útil quando é utilizado um firewall que permite apenas conexões de saída por meio de um proxy Socks. Cada rota do MQIPT pode ser configurada para comunicar-se com um proxy Socks diferente.

Consulte “Configurando o Proxy SOCKS” na página 111 para obter um exemplo de como utilizar SOCKS.

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 gerenciadores de fila em um cluster, a explicação a seguir se baseia nas tarefas descritas na publicação *WebSphere MQ Queue Manager Clusters*, SC34-6061. O diagrama a seguir foi estendido a partir do definido na tarefa denominada “Adding a new queue manager to a cluster” (Incluindo um Novo Gerenciador de Filas no Cluster). NEWYORK e CHICAGO estão em um 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 emissor de cluster é iniciado, o pedido é enviado para seu destino, utilizando o MQIPT agindo como proxy SOCKS. Normalmente, o CONNAME de um canal receptor de cluster é utilizado para identificar o gerenciador de filas local, mas, quando utilizado com MQIPT, o CONNAME deve identificar o MQIPT local e sua porta de atendente de entrada. No diagrama a seguir, todos os endereços de porta do atendente de entrada são 1414 e os endereços de 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 “Configurando o Suporte ao Clustering do MQIPT” na página 121 para obter um exemplo de como configurar uma rede de clusters.

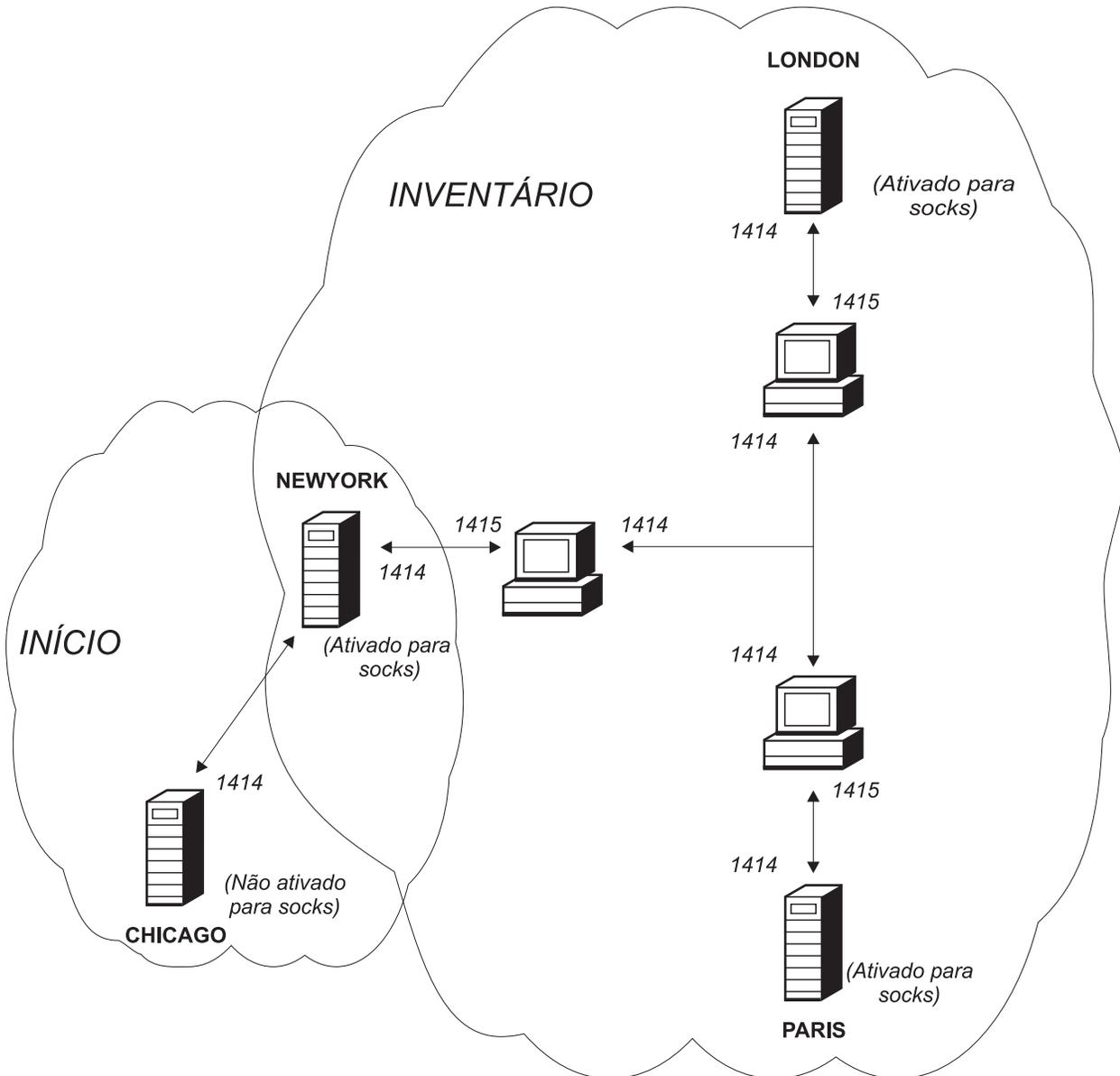


Figura 6. Suporte ao Clustering do MQIPT

Capítulo 5. Visão Geral e Suporte a SSL

O protocolo SSL fornece segurança de conexão por meio 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_DH_anon_EXPORT_WITH_DES40_CBC_SHA
SSL_DH_anon_WITH_3DES_EDE_CBC_SHA
SSL_DH_anon_WITH_AES_128_CBC_SHA
SSL_DH_anon_WITH_AES_256_CBC_SHA
SSL_DH_anon_WITH_DES_CBC_SHA
SSL_DH_anon_WITH_RC4_40_MD5
SSL_DH_anon_WITH_RC4_128_MD5
SSL_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA
SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA
SSL_DHE_DSS_WITH_AES_128_CBC_SHA
SSL_DHE_DSS_WITH_AES_256_CBC_SHA
SSL_DHE_DSS_WITH_DES_CBC_SHA
SSL_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA
SSL_DHE_RSA_WITH_AES_128_CBC_SHA
SSL_DHE_RSA_WITH_AES_256_CBC_SHA
SSL_DHE_RSA_WITH_DES_CBC_SHA
SSL_RSA_EXPORT_WITH_DES40_CBC_SHA
SSL_RSA_EXPORT_WITH_RC2_CBC_40_MD5#
SSL_RSA_EXPORT_WITH_RC4_40_MD5
SSL_RSA_WITH_3DES_EDE_CBC_SHA
SSL_RSA_WITH_AES_128_CBC_SHA
SSL_RSA_WITH_AES_256_CBC_SHA
SSL_RSA_WITH_DES_CBC_SHA
```

SSL_RSA_WITH_NULL_MD5
SSL_RSA_WITH_NULL_SHA
SSL_RSA_WITH_RC4_128_MD5
SSL_RSA_WITH_RC4_128_SHA

Protocolo de Reconhecimento SSL

O processo do protocolo de reconhecimento SSL ocorre durante o pedido de conexão inicial entre o cliente e o 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 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 certificado (certificado de site), a assinatura de cada certificado na cadeia pode ser verificada utilizando 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 à 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 do cliente, este 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.

WebSphere MQ internet pass-thru 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 arquivo do conjunto de chaves também pode conter CRLs (Listas de Revogação de Certificado) e ARLs (Listas de Revogação de Autoridade). O WebSphere MQ internet pass-thru utiliza o pacote IBM Secure Socket Lite (SSLite).

O WebSphere MQ internet pass-thru pode agir como cliente SSL ou como servidor SSL, dependendo em qual extremidade a conexão é iniciada. O cliente inicia uma conexão e o servidor aceita o pedido de conexão. É possível para uma rota do WebSphere MQ internet pass-thru agir como cliente e servidor, entretanto, neste caso, o uso do recurso Modo de Proxy SSL é recomendado, por razões de desempenho. Cada rota do WebSphere MQ internet pass-thru pode ser configurada de forma independente, com seu próprio conjunto de propriedades SSL. Consulte “Informações de Referência da Seção Route” na página 81 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.

O arquivo do conjunto de chaves no lado do cliente SSL, identificado pela propriedade SSLClientCAKeyRing, deve conter uma lista de certificados CA confiáveis, que será utilizada para autenticar o certificado enviado a partir do servidor.

Se também for necessária a autenticação do cliente, a propriedade SSLServerAskClientAuth deve ser ativada no lado do servidor e o arquivo do conjunto de chaves no lado do cliente, identificado pela propriedade SSLClientKeyRing, deve conter seu certificado pessoal. O arquivo do conjunto de chaves no lado do servidor, identificado pela propriedade SSLServerCAKeyRing, deve conter uma lista dos certificados CA confiáveis que serão utilizados para autenticar o cliente.

Como alternativa para o uso de certificados assinados por um CA confiável, você pode utilizar certificados auto-assinados. Exemplos podem ser encontrados nos arquivos de amostra do conjunto de chaves, fornecidos com o MQIPT no subdiretório ssl: sslSample.pfx e sslCAdefault.pfx.

Para abrir um dos tokens PKCS#12 armazenados nesses arquivos de conjunto de chaves, utilize a senha mqiptV1.3.

Um utilitário denominado KeyMan, com o qual você pode gerenciar certificados SSL e arquivos de conjunto de chaves, pode ser encontrado no subdiretório ssl. Consulte “KeyMan” na página 22 para obter instruções de instalação e outras informações.

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 20, “Iniciando o Internet Pass-Thru”, na página 95 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 os dados incorretos forem fornecidos para o protocolo SSL.

Tabela 1. 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
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

Tabela 1. Mensagens de erro de *SSLRuntimeException* (continuação)

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
30	Falha na autorização

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

Tabela 2. Mensagens de erro de *SSLException*

ID	Descrição
3	O tempo limite de conexão definido no <i>SSLContext</i> 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

LDAP e CRLs

O WebSphere internet pass-thru oferece suporte ao uso de um servidor LDAP (Lightweight Directory Access Protocol) para executar autenticação CRL (Certificate Revocation List) em um certificado digital. O suporte a LDAP foi implementado de forma semelhante àquela com base em WebSphere MQ, uma vez que o mesmo servidor LDAP pode ser utilizado para WebSphere MQ e MQIPT. Mais informações sobre o uso de servidores LDAP com WebSphere MQ podem ser encontradas no capítulo 15 do manual "WebSphere MQ Security Version 5.3" SC34-6079-01. Partes desse manual estão incluídas a seguir para referência.

Durante um protocolo de reconhecimento SSL, as partes que se comunicam autenticam-se com certificados digitais. A autenticação pode incluir uma verificação se o certificado recebido ainda pode ser confiável. As CAs (Autoridades de Certificação) revogam certificados por diversos motivos, inclusive:

- O proprietário foi para outra organização

- A chave privada não é mais secreta

As CAs publicam certificados pessoais revogados em uma CRL (Lista de Revogação de Certificado). Os certificados CA revogados são publicados em uma ARL (Lista de Revogação de Autoridade). As referências posteriores a CRLs neste capítulo também são válidas para ARLs.

Existem diversos servidores de diretório LDAP no mercado. O WebSphere internet pass-thru foi testado com o IBM Directory Server: consulte <http://www.ibm.com/software/network/directory/server>. As instruções de instalação e manutenção do servidor LDAP estão na documentação fornecida com o produto instalado.

Mais informações sobre o gerenciamento de CRLs e ARLs podem ser encontradas no manual "WebSphere MQ Security Version 5.3" SC34-6079-01.

O MQIPT oferece suporte a até dois servidores LDAP em cada rota. O primeiro servidor LDAP é tratado como principal e o segundo é visto como servidor de backup, utilizado somente se o servidor principal não puder ser atingido. O servidor de backup deve ser uma imagem de espelho do servidor principal.

O acesso às informações armazenadas em um servidor LDAP podem ser protegidas por um ID do usuário e senha. Se este for o caso, as propriedades LDAP*Userid e LDAP*Password podem ser utilizadas.

Quando o MQIPT carrega um token PKCS#12 a partir de um arquivo de conjunto de chaves, é verificada a validade CRL de todos os certificados CA. Se o certificado CA tiver um CRL anexo, será verificado se ele expirou e, em caso positivo, um CRL mais novo será recuperado do servidor LDAP. Os CRLs recuperados serão carregados no token atual e anexos ao seu certificado CA. O token atualizado pode ser salvo no arquivo de conjunto de chaves (consulte a propriedade LDAPSaveCRL na seção "Informações de Referência da Seção Route" na página 81).

Quando uma consulta é enviada ao servidor LDAP principal, se não houver entradas correspondentes ao CA indicado, supõe-se que não há CRLs para esse CA. O servidor de backup não será utilizado. No entanto, se o servidor LDAP não puder ser atingido ou não retornar dentro de um determinado tempo, o servidor de backup será utilizado. Erros no servidor de backup farão com que a conexão do cliente seja encerrada. Essa ação pode ser substituída, definindo a propriedade LDAPIgnoreErrors como true.

Atenção

Se você ativar a propriedade LDAPIgnoreErrors, um certificado revogado pode ser utilizado para fazer uma conexão SSL.

O modelo do cliente LDAP se baseia na implementação "com.sun.jndi.ldap.LdapCtxFactory". Os CRLs recuperados por MQIPT serão mantidos em cache e compartilhados por todas as conexões nessa rota.

Se um CRL em cache tiver expirado, será removido do cache e um novo será recuperado do servidor LDAP. Se não houver um novo CRL disponível, a conexão ainda será recusada.

Um CRL recuperado do servidor LDAP também é verificado quanto à sua expiração e uma mensagem de aviso do console do sistema é exibida (MQCPW001). O CRL expirado ainda será carregado no sistema e os pedidos de conexão que fazem referência a esse CRL serão recusados. O CRL expirado no servidor LDAP deve ser substituído por um atualizado.

A propriedade LDAPCacheTimeout pode ser utilizada para controlar com que frequência o cache do CRL é limpo. O valor padrão é 1 dia. Definir esse valor como 0 significa que as entradas no cache não serão limpas até que a rota seja iniciada novamente.

Um CRL expirado pode ser armazenado em um arquivo do conjunto de chaves ou em um servidor LDAP. Se tiver sido emitido um novo, pedidos de conexão posteriores serão recusados. Você pode ignorar CRLs expirados, ativando a propriedade IgnoreExpiredCRLs.

Atenção

Se você ativar a propriedade IgnoreExpiredCRLs, um certificado revogado pode ser utilizado para fazer uma conexão SSL.

O Padrão Avançado de Criptografia

O AES (Padrão Avançado de Criptografia) é uma nova Publicação do FIPS (Federal Information Processing Standard) que especificará um algoritmo criptográfico a ser utilizado por organizações governamentais norte-americanas para proteger informações importantes (não internas). O NIST (National Institute of Standards and Technology) também prevê que, em alguns casos, o AES será utilizado voluntariamente pelas organizações, instituições e indivíduos não governamentais, nos EUA e fora do país.

Selecionando Certificados de um Arquivo de Conjunto de Chaves

É possível ter mais de um certificado pessoal armazenado no mesmo arquivo de conjunto de chaves para que as propriedades SSLClientSite* possam ser utilizadas no lado do cliente para selecionar o certificado a ser enviado ao servidor para autenticação e para que as propriedades SSLServerSite* possam ser utilizadas no lado do servidor para selecionar o certificado a ser enviado ao cliente para autenticação.

Utilizando essas propriedades, é possível selecionar um certificado com base em seu DN (Nome Distinto). Como alternativa, o rótulo do certificado pode ser utilizado para selecionar um certificado, utilizando as propriedades SSLServerSiteLabel e SSLClientSiteLabel.

Criptografando uma Senha do Conjunto de Chaves

A senha utilizada para abrir um arquivo do conjunto de chaves pode ser criptografada com o script mqiptPW. A senha criptografada é armazenada em um arquivo, que pode ser utilizado por uma destas propriedades: SSLClientKeyRingPW, SSLClientCAKeyRingPW, SSLServerKeyRingPW e SSLServerCAKeyRingPW.

Formato do comando:

```
mqiPTPW <senha> <nome do arquivo>  
<-substituir>
```

em que

senha é a senha em texto simples, necessária para abrir o arquivo de conjunto de chaves indicado

nome do arquivo

é o nome do arquivo de senha a ser criado

substituir

é a opção necessária para sobrescrever o <nome do arquivo>, se ele existir

As senhas podem incluir o caractere de espaço (" "), mas a cadeia inteira da senha deve estar entre aspas para que isto seja aceito. Não há limite de comprimento ou formato de uma senha.

Nota: Os usuários que migraram de um nível anterior do WebSphere Internet pass-thru precisarão substituir os arquivos de senha atuais que contêm a senha em texto simples por uma cópia do arquivo de senha criptografado.

Utilize a senha mqiPTV1.3 para abrir um dos arquivos de amostra do conjunto de chaves, com um utilitário de gerenciamento de chaves (por exemplo, KeyMan).

KeyMan

Agora, um utilitário independente denominado KeyMan é enviado com o WebSphere Internet pass-thru para permitir o gerenciamento de certificados SSL e arquivos do 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 revogação de certificado) 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 inclui as definições de confiança de um determinado aplicativo (por exemplo, o WebSphere Internet pass-thru). 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 contêm 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 for definido por algum contexto. Nos sistemas Windows, os sufixos padrão de arquivos 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 certificado associadas serão utilizadas para autenticação cliente/servidor. Outros certificados representam CAs confiáveis ou servidores confiáveis, dependendo das respectivas definições de confiança. Nos sistemas Windows, os sufixos padrão de arquivos 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> for 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**). Nos sistemas Windows, os sufixos padrão dos 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**). Nos sistemas Windows, o sufixo padrão de arquivos CRL X.509 é .crl.

FAQs (Perguntas Mais Frequentes) do KeyMan

Para perguntas gerais sobre criptografia e termos relacionados, consulte a RSA Laboratories e suas "Perguntas Mais Frequentes 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).

Capítulo 6. Qualidade de Serviço

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 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. Além disso, a TQoS também permite que os administradores colem dados de desempenho da política correspondente para monitorar se ela fornece os objetivos de nível de serviço (medidas importantes como rendimento da conexão, atrasos, taxa de perda etc) para os quais são destinadas. O MQIPT requer apenas que o pagent (Policy Agent) seja instalado e executado 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.ibm.com/software/webservers/edgeserver/library.html>

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

O código de TQoS, juntamente com as instruções de instalação e administração, pode ser obtido por download do mesmo local que o MQIPT. Consulte o site SupportPacs da família WebSphere MQ no endereço <http://www.ibm.com/webspheremq/supportpacs> e clique em Category 3 – Product Extensions (Categoria 3 e Extensões do Produto).

O MQIPT é enviado com uma biblioteca fictícia denominada `libmqiptqos.so`, encontrada no subdiretório `lib` do MQIPT. Isto permite que o MQIPT seja executado na plataforma Linux sem a necessidade de instalar o pagent de TQoS. Depois de instalar a TQoS, pode ser necessário substituir essa biblioteca fictícia pela utilizada pela TQoS. Um script denominado `mqiptQoS` pode ser encontrado no subdiretório `bin` do MQIPT para ajudar com essa tarefa. Utilize o comando a seguir para renomear a biblioteca fictícia e definir um link para a biblioteca de tempo de execução de TQoS real:

```
mqiptQoS -install
```

Utilizar `mqiptQoS -remove` inverterá as ações anteriores.

O MQIPT requer apenas que o pagent seja instalado e executado 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 81 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 108 para obter mais informações sobre definições de política.

Capítulo 7. Network Dispatcher

Suporte ao Network Dispatcher

O MQIPT pode ser utilizado com o IBM Network Dispatcher para fornecer disponibilidade avançada e equilíbrio de carga entre vários servidores, utilizando orientadores personalizados. Esta seção pressupõe 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 1ib. Siga as instruções no *Network Dispatcher User's Guide* (GC31-8496) para instalar os consultores personalizados. A Figura 7 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.

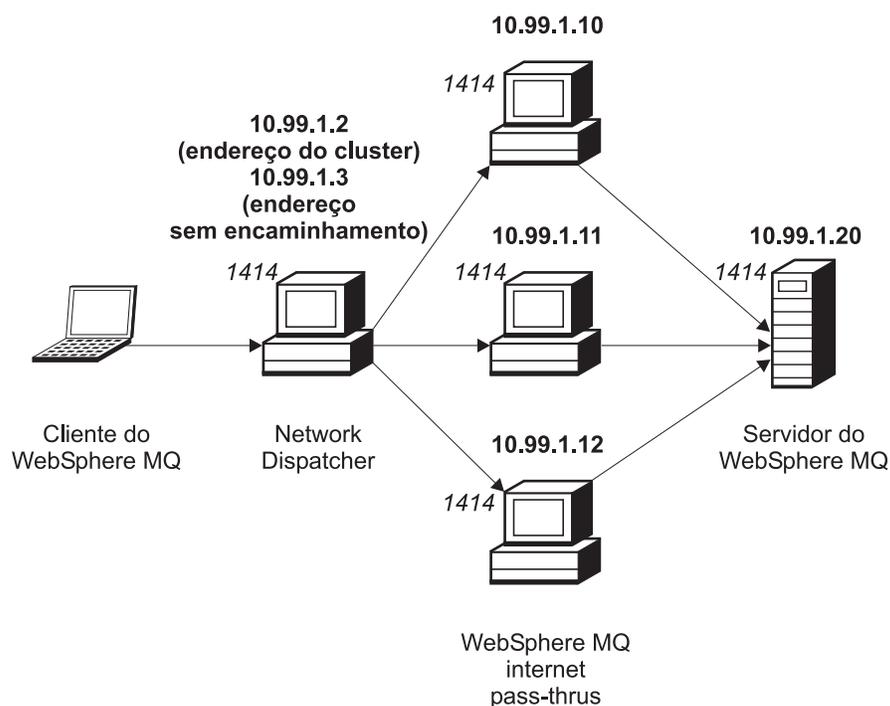


Figura 7. Utilizando o Network Dispatcher com o MQIPT

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, relacionado 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.

Capítulo 8. Java Security Manager e Saídas de Segurança

Java Security Manager

O suporte ao 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 do `SecurityManager`. Consulte “Informações de Referência da Seção Global” na página 80 para obter mais informações.

O Java Security Manager utiliza dois arquivos de critério padrão. Um arquivo de critério 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 critério específico do usuário, denominado `.java.policy`, pode existir no diretório pessoal do usuário. Um arquivo de critério adicional do MQIPT também pode ser utilizado. Consulte “Informações de Referência da Seção Global” na página 80 para obter mais informações. Para utilizar um arquivo de critério adicional, certifique-se de que a propriedade `policy.allowSystemProperty` tenha sido definida como `true` no arquivo de critério de sistema global (`java.security`).

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

Um arquivo de critério 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 pressupõe 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` corresponderia a 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 porta do nome pode ser especificado como um único endereço de porta ou um intervalo de endereços de porta, por exemplo:

1414 porta única 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 de 1 a 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 por meio das propriedades do sistema Java `java.security.manager` e `java.security.policy`, mas é recomendado que você utilize as propriedades `SecurityManager` e `SecurityManagerPolicy` para controlar o MQIPT.

Saída de Segurança

Atenção

O MQIPT é executado em uma única JVM, portanto, uma saída de segurança definida pelo usuário pode oferecer um risco para a operação normal do MQIPT das seguintes formas:

- afetando os recursos do sistema
- gerando gargalos
- prejudicando o desempenho

Faça testes abrangentes da sua saída de segurança antes de implementá-la em um ambiente de produção.

A finalidade de uma saída de segurança é controlar o acesso a um destino, conforme definido pela propriedade da rota de Destino. A saída de segurança será chamada no ponto em que um pedido de conexão for recebido de um cliente e antes de o MQIPT fazer a conexão com o destino. Com base nas propriedades iniciais da conexão, a saída de segurança pode decidir se a conexão poderá ser concluída.

Quando uma rota é iniciada, a saída de segurança é chamada para inicializar e ficar pronta para processar um pedido de conexão. O processo de inicialização deve ser utilizado para carregar dados do usuário e prepará-los para acesso rápido e fácil, minimizando o tempo para processar um pedido de conexão.

Cada rota pode ter sua própria saída de segurança. A propriedade `SecurityExit` é utilizada para ativar/desativar a saída de segurança definida pelo usuário. A propriedade `SecurityExitName` é utilizada para definir o nome da classe da saída de segurança definida pelo usuário. A propriedade `SecurityExitPath` é utilizada para definir o nome do diretório que contém o arquivo de classe. Se essa propriedade não for definida, supõe-se que o arquivo de classe esteja no subdiretório `exits`. O `SecurityExitPath` também pode definir o nome de um arquivo jar que contém a saída de segurança definida pelo usuário. Finalmente, a propriedade `SecurityExitTimeout` é utilizada pelo MQIPT para determinar por quanto tempo ele deve esperar uma resposta da saída de segurança ao validar um pedido de conexão.

Uma nova classe chamada `SecurityExit` foi criada para permitir que o MQIPT chame uma saída de segurança definida pelo usuário. Essa nova classe deve ser estendida pela saída de segurança definida pelo usuário e a maior parte dos seus métodos deve ser substituída para fornecer a funcionalidade necessária. Um objeto `SecurityExitResponse` é utilizado para retransmitir dados para o MQIPT e esses dados são utilizados pelo MQIPT para decidir se o pedido de conexão deve ser aceito ou rejeitado. A `SecurityExitResponse` também pode conter um novo destino e endereço de porta de destino, utilizados para substituir as propriedades definidas pela rota.

Três saídas de segurança de amostra foram fornecidas para mostrar como uma saída de segurança pode ser implementada. A primeira amostra, chamada `SampleSecurityExit`, mostra como controlar o acesso a um WebSphere MQ Queue Manager, com base no nome do canal WMQ. Ela apenas permite a conexão com um nome de canal que comece com a cadeia "MQIPT". Consulte "Saída de Segurança" na página 139 para obter mais informações.

A segunda amostra, chamada `SampleRoutingExit`, permite o roteamento dinâmico de pedidos de conexão do cliente para um conjunto de WebSphere MQ Servers, sendo que cada servidor é host de um QM com o mesmo nome e atributos. A amostra inclui um arquivo de configuração que contém uma lista de nomes de servidores. Consulte "Saída de Segurança de Roteamento" na página 141 para obter mais informações.

A terceira amostra, chamada `SampleOneRouteExit`, permite o roteamento dinâmico para um WMQ QM derivado do nome de canal do WMQ utilizado no pedido de conexão. A amostra inclui um arquivo de configuração que contém um mapa de nomes de QM para nomes de servidores. Consulte "Saída Dinâmica de Uma Rota" na página 144 para obter mais informações.

A Classe com `ibm.mq.ipt.SecurityExit`

Essa classe e seus métodos públicos deve ser estendida pela saída de segurança definida pelo usuário para obter acesso a alguns dados comuns e permitir que ocorra inicialização do MQIPT. Antes de cada método ser chamado pelo MQIPT, algumas propriedades serão disponibilizadas para que o método as utilize. Seus valores podem ser recuperados utilizando os métodos `get` apropriados definidos na classe. Consulte a seguir uma lista completa dos métodos suportados.

Métodos

init

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

As propriedades a seguir estão disponíveis:

- porta do atendente
- destino
- porta de destino
- versão

O método init será chamado pelo MQIPT quando uma rota for iniciada. Ao retornar desse método, a saída de segurança deve estar pronta para validar um pedido de conexão. Qualquer exceção emitida nesse método impedirá que a rota seja iniciada.

refresh

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

As propriedades a seguir estão disponíveis:

- porta do atendente
- destino
- porta de destino

O método atualizar será chamado pelo MQIPT quando o MQIPT Cliente Administrativo solicitar que ele seja atualizado. Essa ação normalmente será chamada quando uma propriedade tiver sido alterada no arquivo de configuração. O MQIPT carregará todas as propriedades do arquivo de configuração e determinará quais foram alteradas e se uma rota deve ser reiniciada imediatamente ou se pode aguardar até a próxima vez que o MQIPT for iniciado novamente.

Esse método deve executar um recarregamento dos dados externos que utiliza (isto é, dados carregados durante o método init). Qualquer exceção emitida nesse método fará com que a rota seja desativada.

close

```
public void close ()
```

As propriedades a seguir estão disponíveis:

- porta do atendente
- destino
- porta de destino

O método close() será chamado pelo MQIPT quando o MQIPT Cliente Administrativo solicitar que ele seja parado. Ele deverá liberar os recursos do sistema que tiver adquirido durante sua operação. O MQIPT aguarda a conclusão desse método antes de encerrar.

Esse método também será chamado se uma saída de segurança tiver sido ativada e que agora foi desativada no arquivo de configuração.

validate

```
public SecurityExitResponse validate ()
```

As propriedades a seguir estão disponíveis:

- porta do atendente
- destino
- porta de destino
- tempo limite
- endereço IP do cliente
- endereço de porta do cliente
- nome do canal
- nome do gerenciador de filas

O método `validate` será chamado pelo MQIPT quando ele receber um pedido de validação da conexão. O nome do canal e o nome do gerenciador de filas não estarão disponíveis se a propriedade `SSLProxyMode` tiver sido ativada, uma vez que esse recurso é utilizado somente para transmitir dados SSL pelo túnel e, portanto, os dados geralmente obtidos do fluxo de dados inicial estarão ilegíveis. O nome do gerenciador de filas não estará disponível para conexões do cliente WMQ, uma vez que essa informação não estará disponível enquanto a conexão com o Gerenciador de Filas de destino não tiver sido estabelecida.

A saída de segurança deve retornar um objeto `SecurityExitResponse`, contendo as seguintes informações:

- código de razão (deve ser definido)
- novo endereço de destino (opcional)
- novo endereço de porta do atendente de destino (opcional)
- mensagem (opcional)

O código de razão determinará se a conexão será aceita ou rejeitada pelo MQIPT. Os campos `newDestination` e `newDestinationPort` podem ser ajustados para definir um novo destino (QM). Se você não definir essas propriedades, as propriedades `route Destination` e `DestinationPort` definidas no arquivo de configuração serão utilizadas. As mensagens serão anexas à entrada do arquivo de log de conexão.

Métodos suportados para obter propriedades:

public int getListenerPort()

recupera a porta do ouvinte da rota - conforme definido pela propriedade `ListenerPort`

public String getDestination()

recupera o endereço de destino - conforme definido pela propriedade `Destination`

public int getDestinationPort()

recupera o endereço de porta do ouvinte de destino - conforme definido pela propriedade `DestinationPort`

public String getClientIPAddress()

recupera o endereço IP do cliente que faz o pedido de conexão

public int getClientPortAddress()

recupera o endereço de porta utilizado pelo cliente que faz o pedido de conexão

```

public int getTimeout()
    recupera o valor do tempo limite. O MQIPT aguardará a saída de
    segurança para validar um pedido - conforme definido pela propriedade
    SecurityExitTimeout

public int getConnThreadID()
    recupera o ID do encadeamento de conexão que trata o pedido de conexão,
    o que é útil para depuração

public String getChannelName()
    recupera o nome do canal do WMQ utilizado no pedido de conexão

public String getQMName()
    recupera o nome do Gerenciador de Filas do WMQ utilizado no pedido de
    conexão

public boolean getTimedout()
    pode ser utilizado pela saída de segurança para determinar se o tempo
    limite expirou

```

A Classe com.ibm.mq.ipt.SecurityExitResponse

Essa classe será utilizada para retransmitir uma resposta para o MQIPT a partir de uma saída de segurança definida pelo usuário e para determinar se o pedido de conexão deve ser aceito ou rejeitado. Os objetos desse tipo são criados somente no método validate (consulte anteriormente). Existem construtores de conveniência para criar esses objetos e métodos set para cada propriedade. Consulte as saídas de segurança de amostra para obter mais informações.

Criar um objeto SecurityExitResponse padrão rejeita o pedido de conexão.

Construtores suportados:

```

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

```

em que:

- dest é o novo destino
- destPort é o endereço de porta do novo destino
- rc é o código de razão
- msg é uma mensagem que será incluída na entrada do log de conexão

```

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

```

```

public SecurityExitResponse (int rc, String msg) throws IPTException

```

```

public SecurityExitResponse (int rc) throws IPTException

```

Métodos suportados para definir valores de propriedades:

```

public void setDestination(String dest)
    define um novo endereço de destino para o pedido de conexão

```

```

public void setDestinationPort(int port) throws IPTException
    define um novo endereço de porta do atendente de destino para o pedido
    de conexão - emite uma IPTException para um endereço de porta inválido

```

```

public void setMessage(String msg)
    inclui uma mensagem no registro de conexão

```

public void setReasonCode(int rc) throws IPTException

define o código de razão para o pedido de conexão - emite uma IPTException para um valor desconhecido

Códigos de razão válidos:

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

Rasteio

Para ajudar a diagnosticar problemas em uma saída de segurança definida pelo usuário, você pode ativar um recurso de rastreamento, semelhante ao utilizado pelo MQIPT. Definir a propriedade Trace da rota com um valor de 1 a 5 cria um arquivo de rastreamento no subdiretório errors. O nome do arquivo de rastreamento é igual ao da saída de segurança.

Provavelmente existirá mais de uma instância da saída de segurança em execução ao mesmo tempo, portanto, entradas individuais no arquivo de rastreamento podem ser identificadas com o identificador de encadeamento.

A inicialização das funções de rastreamento é feita pelo MQIPT quando a saída de segurança for iniciada, bastando escolher quais informações você deseja rastrear. Existem vários exemplos de rastreamento nas saídas de amostra do usuário.

Os requisitos mínimos para o rastreamento são uma chamada entry uma chamada exit e os dados que você deseja rastrear. Por exemplo:

```
<a_method>
{
    SecurityExit.rastlRoute.entry(RASITraceEvent.TYPE_ENTRY_EXIT,
                                this,
                                "method_name");
    :
    <code>
    :
    SecurityExit.rastlRoute.trace(RASITraceEvent.TYPE_MISC_DATA,
                                this,
                                "data");
    :
    <code>
    :
    SecurityExit.rastlRoute.exit(RASITraceEvent.TYPE_ENTRY_EXIT,
                                this,
                                "method_name");
}
```

Capítulo 9. Controle do Endereço de Porta

Controle do Endereço de Porta

Ao utilizar o MQIPT, é possível restringir o intervalo de endereços de porta local que ele utiliza ao fazer uma conexão de saída, definindo a propriedade `OutgoingPort` na rota. O intervalo de endereço de porta local é calculado utilizando o valor `MaxConnectionThreads`. Por exemplo, se `OutgoingPort` for definido como 1600 e `MaxConnectionThreads` como 20, o intervalo de endereços de porta local dessa rota seria 1600-1619. O administrador do MQIPT é responsável por certificar-se de que não existam conflitos de endereços de porta entre as rotas. Se `OutgoingPort` não for definido, um valor padrão 0 significa que um endereço de porta alocado pelo sistema será utilizado para cada conexão.

Consulte o exemplo “Alocando Endereços de Porta” na página 127 para obter mais informações.

Sistemas com Várias Hospedagens

Ao utilizar um sistema com várias hospedagens, você pode especificar qual endereço IP será ligado a uma conexão de saída, utilizando a propriedade `LocalAddress`. Não há suporte a nomes de host nessa propriedade.

Capítulo 10. Outras Considerações de Segurança

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 de ponta a ponta para todo o canal.

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 ou esteja utilizando uma saída de segurança.
- 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. Nesse caso, é recomendado que você utilize o Java Security Manager. Consulte “Java Security Manager” na página 31.
- 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 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 11. Recursos Diversos

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 um canal está inativo por um período de tempo superior ao tempo limite, ele encerra imediatamente as 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 uma mensagem do WebSphere MQ estiver em trânsito, esta 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 "Informações de Referência da Seção Global" na página 80 para obter mais informações.

Sempre que o MQIPT for iniciado, será criado um novo log de conexão. Para identificação, o nome do arquivo inclui a data e hora atuais, 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.

Capítulo 12. Fazendo Upgrade da Versão Anterior

Para fazer upgrade do MQIPT da Versão 1.2 para a Versão 1.3, siga estas etapas:

1. Faça uma cópia dos arquivos de configuração `mqipt.conf` e `client.conf`. O arquivo `mqipt.conf` está no diretório inicial do MQIPT e `client.conf` no subdiretório `bin`.
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 desinstalar o MQIPT:
`mqiptService -remove`
4. Execute o programa de remoção de instalação para o MQIPT.
5. Depois de instalar o MQIPT V1.3, copie os arquivos de configuração salvos de volta para seus locais originais.
6. É aconselhável utilizar a GUI de Administração do MQIPT para gerenciar as alterações no MQIPT. O arquivo de configuração da V1.2 é compatível com a GUI.

Algumas implementações exigem um serviço MQIPT local sob controle da sua organização e um serviço MQIPT remoto que pode estar sob controle da organização do cliente. Nessa situação, é muito difícil migrar os dois serviços MQIPT ao mesmo tempo, mas isto não é problema no MQIPT. A não ser que seja indicado de outra forma, versões antigas do MQIPT são compatíveis com a versão mais recente. Isto facilita muito o processo de migração do MQIPT.

Também é possível fazer o upgrade do núcleo do MQIPT sem desinstalá-lo primeiro. Todas as classes necessárias para executar o MQIPT são armazenadas no arquivo `MQipt.jar`. Você pode instalar a versão mais recente do MQIPT em outra máquina e copiar o arquivo `MQipt.jar` dessa instalação para o sistema em execução. O mesmo é válido para as classes necessárias durante a execução da GUI de Administração. Elas estão no arquivo `guiadmin.jar`.

Novas Opções de Configuração

As seguintes propriedades são novas na Versão 1.3:

- `IgnoreExpiredCRLs`
- `LDAP`
- `LDAPCacheTimeout`
- `LDAPIgnoreErrors`
- `LDAPSsaveCRL`
- `LDAPServer1`
- `LDAPServer1Password`
- `LDAPServer1Port`
- `LDAPServer1Timeout`
- `LDAPServer1Userid`
- `LDAPServer2`
- `LDAPServer2Password`
- `LDAPServer2Port`

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

Para obter informações de referência sobre todas as propriedades, consulte “Informações de Referência sobre Configuração” na página 76.

Capítulo 13. 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”
- “Configurando o Internet Pass-Thru” na página 48
- “Iniciando o Internet Pass-Thru a partir da Linha de Comandos” na página 48
- “Iniciando o Cliente Administrativo a partir da Linha de Comandos” na página 49
- “Utilizando um Programa de Controle de Serviços do Windows” na página 49
- “Desinstalando o internet pass-thru como Serviço do Windows” na página 50
- “Desinstalando o Internet Pass-Thru” na página 50

Fazendo Download e Instalando os Arquivos

É possível fazer download do MQIPT (MS81, um SupportPac da categoria 3) a partir da página da Web do WebSphere MQ SupportPac, no endereço:

<http://www.ibm.com/webspheremq/supportpacs>

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 on-line.

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
Leia-me.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
exits\SampleOneRouteExit.java	Amostra da saída de segurança
exits\SampleOneRouteExit.conf	Arquivo de configuração para SampleOneRouteExit
exits\SampleRoutingExit.java	Amostra da saída de segurança
exits\SampleRoutingExit.conf	Arquivo de configuração para SampleRoutingExit

Arquivo	Finalidade
exits\SampleSecurityExit.java	Amostra da saída de segurança
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
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\mqiptPW.bat	Criptografiação de senha utilizada para abrir os arquivos de conjunto de chaves
bin\mqiptservice.exe	Para incluir ou remover o MQIPT no Gerenciador de Controle de Serviços do Windows
bin\mqiptVersion.bat	Exibe o número de versão do MQIPT
web\MQIPServlet.war	Arquivo archive da Web para a versão do servlet.
doc\<idioma>\html\ <nomearquivo>.zip	Arquivo mestre do manual do <i>internet pass-thru</i> no formato HTML. Consulte “Bibliografia” na página 173 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 19, “Administrando e Configurando o Internet Pass-Thru”, na página 71 para obter mais informações.

Iniciando o Internet Pass-Thru a partir da Linha de Comandos

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

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

Você também pode iniciar o MQIPT no menu Iniciar -> Programas do Windows.

A execução do 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 149. As mensagens a seguir são um exemplo de um início bem-sucedido do MQIPT:

```
5639-L92 (C) Copyright IBM Corp. 2000 Todos os Direitos Reservados
MQCPI001 WebSphere MQ internet pass-thru Versão 1.3.0 iniciando
MQCPI004 Lendo informações sobre configuração de c:\mqipt\mqipt.conf
MQCPI008 Atendendo comandos de controle na porta 1881
MQCPI011 O caminho c:\mqipt\logs será usado p/ armazenar arquivos de log
MQCPI006 A rota 1418 foi iniciada e enviará mensagens para:
MQCPI034 ....mqserver.company4.com(1414)
MQCPI035 ....utilizando protocolos MQ
MQCPI078 Rota 1418 pronta para os pedidos de conexão
MQCPI006 A rota 1415 iniciou e enviará mensagens para:
MQCPI034 ....mqipt.company2.com(1415)
MQCPI035 ....utilizando protocolos MQ
MQCPI036 ....Lado do SSL ativado com as propriedades:
MQCPI031 .....conjunto de cifras <null>
MQCPI032 .....arquivo de conjunto de chaves c:\mqipt\KeyMan.pfx
MQCPI038 .....nome(s) diferente(s) CN=*Doe O=IBM OU=* L=* ST=* C=*
MQCPI078 Rota 1415 pronta para os pedidos de conexão
```

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 de “erros” no qual quaisquer registros de FFST (First Failure Support Technology (FFST) e de rastreamento são gravados

Iniciando o Cliente Administrativo a partir da Linha de Comandos

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

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

Para permitir que o Cliente Administrativo conecte-se externamente por meio 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 serviço do Windows.

O mqiptservice.exe contém os seguintes argumentos da 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 depois de instalar esse 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 `client` do JDK.

Desinstalando o internet pass-thru como Serviço do Windows

Para desinstalar o MQIPT como serviço, primeiro pare-o no painel de serviços do Windows. Em seguida, abra um prompt de comandos, vá para o subdiretório `bin` do MQIPT e digite:

```
mqiptservice -remove
```

Desinstalando o Internet Pass-Thru

Antes de desinstalar o MQIPT do sistema, remova-o como Serviço do Windows, conforme descrito anteriormente. Em seguida, execute o processo de desinstalação a partir do menu Iniciar do Windows.

Capítulo 14. 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”
- “Configurando o Internet Pass-Thru” na página 52
- “Iniciando o Internet Pass-Thru a partir da Linha de Comandos” na página 52
- “Iniciando o Internet Pass-Thru Automaticamente” na página 53
- “Iniciando o Cliente Administrativo a partir da Linha de Comandos” na página 53
- “Desinstalando o Internet Pass-Thru” na página 54

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/webspheremq/supportpacs>

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 pressupõe 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
Leia-me.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
exits/ SampleOneRouteExit.java	Amostra da saída de segurança
exits/ SampleOneRouteExit.conf	Arquivo de configuração para SampleOneRouteExit
exits/SampleRoutingExit.java	Amostra da saída de segurança

Arquivo	Finalidade
exits/SampleRoutingExit.conf	Arquivo de configuração para SampleRoutingExit
exits/SampleSecurityExit.java	Amostra da saída de segurança
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
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/mqiptPW	Criptografia de senha utilizada para abrir os arquivos de conjunto de chaves
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/MQIPServlet.war	Arquivo archive da Web para a versão do servlet.
doc/<idioma>/html/<nomearquivo>.zip	Arquivo mestre do manual do <i>internet pass-thru</i> no formato HTML. Consulte "Bibliografia" na página 173 para obter mais informações sobre a documentação em cópia eletrônica.
lib/guiadmin.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 19, "Administrando e Configurando o Internet Pass-Thru", na página 71 para obter mais informações.

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 ..
```

A execução do 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 149. As mensagens a seguir são um exemplo de um início bem-sucedido do MQIPT:

```
5639-L92 (C) Copyright IBM Corp. 2000 Todos os Direitos Reservados
MQCPI001 WebSphere MQ internet pass-thru Versão 1.3.0 iniciando
MQCPI004 Lendo informações sobre configuração de /opt/mqipt/mqipt.conf
MQCPI008 Atendendo comandos de controle na porta 1881
MQCPI011 O caminho /opt/mqipt/logs será usado p/ armazenar arquivos de log
MQCPI006 A rota 1418 foi iniciada e enviará mensagens para:
MQCPI034 ....mqserver.company4.com(1414)
MQCPI035 ....utilizando protocolos MQ
MQCPI078 Rota 1418 pronta para os pedidos de conexão
MQCPI006 A rota 1415 iniciou e enviará mensagens para:
MQCPI034 ....mqipt.company2.com(1415)
MQCPI035 ....utilizando protocolos MQ
MQCPI036 ....Lado do SSL ativado com as propriedades:
MQCPI031 .....conjunto de cifras <null>
MQCPI032 .....arquivo de conjunto de chaves /opt/mqipt/KeyMan.pfx
MQCPI038 .....nome(s) diferente(s) CN=*Doe O=IBM OU=* L=* ST=* C=*
MQCPI078 Rota 1415 pronta para os pedidos de conexão
```

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 de "erros" no qual quaisquer registros de FFST (First Failure Support Technology (FFST) e de rastreamento 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, altere o diretório para bin e execute mqiptGui. Por exemplo:

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

Para permitir que o Cliente Administrativo conecte-se externamente por meio 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.

Desinstalando o Internet Pass-Thru

Antes de desinstalar o MQIPT de seu sistema, impeça-o de iniciar automaticamente, conforme descrito em “Iniciando o Internet Pass-Thru Automaticamente” na página 53. Efetue login como root e execute o comando pkgrm:

```
pkgrm mqipt
```

Capítulo 15. Instalando o Internet Pass-Thru no AIX

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

- “Fazendo Download e Instalando os Arquivos”
- “Configurando o Internet Pass-Thru” na página 56
- “Iniciando o Internet Pass-Thru a partir da Linha de Comandos” na página 56
- “Iniciando o Internet Pass-Thru Automaticamente” na página 57
- “Iniciando o Cliente Administrativo a partir da Linha de Comandos” na página 57
- “Desinstalando o Internet Pass-Thru” na página 58

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/webspheremq/supportpacs>

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 pressupõe 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
Leia-me.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
exits/ SampleOneRouteExit.java	Amostra da saída de segurança
exits/ SampleOneRouteExit.conf	Arquivo de configuração para SampleOneRouteExit
exits/SampleRoutingExit.java	Amostra da saída de segurança
exits/SampleRoutingExit.conf	Arquivo de configuração para SampleRoutingExit

Arquivo	Finalidade
exits/SampleSecurityExit.java	Amostra da saída de segurança
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
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/mqiptPW	Criptografiação de senha utilizada para abrir os arquivos de conjunto de chaves
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>/html/<nomearquivo>.zip	Arquivo mestre do manual do <i>Internet Pass-Thru</i> no formato HTML. Consulte “Bibliografia” na página 173 para obter mais informações sobre a documentação em cópia eletrônica.
lib/guiadmin.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 19, “Administrando e Configurando o Internet Pass-Thru”, na página 71 para obter mais informações.

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 ..
```

A execução do 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 149. As mensagens a seguir são um exemplo de um início bem-sucedido do MQIPT:

```
5639-L92 (C) Copyright IBM Corp. 2000 Todos os Direitos Reservados
MQCPI001 WebSphere MQ internet pass-thru Versão 1.3.0 iniciando
MQCPI004 Lendo informações sobre configuração de /usr/opt/mqipt/mqipt.conf
MQCPI008 Atendendo comandos de controle na porta 1881
MQCPI011 Caminho /usr/opt/mqipt/logs será usado p/ armazenar arquivos de log
MQCPI006 A rota 1418 foi iniciada e enviará mensagens para:
MQCPI034 ....mqserver.company4.com(1414)
MQCPI035 ....utilizando protocolos MQ
MQCPI078 Rota 1418 pronta para os pedidos de conexão
MQCPI006 A rota 1415 iniciou e enviará mensagens para:
MQCPI034 ....mqipt.company2.com(1415)
MQCPI035 ....utilizando protocolos MQ
MQCPI036 ....Lado do SSL ativado com as propriedades:
MQCPI031 .....conjunto de cifras <null>
MQCPI032 .....arquivo de conjunto de chaves /usr/opt/mqipt/KeyMan.pfx
MQCPI038 .....nome(s) diferente(s) CN=*Doe O=IBM OU=* L=* ST=* C=*
MQCPI078 Rota 1415 pronta para os pedidos de conexão
```

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 de “erros” no qual quaisquer registros de FFST (First Failure Support Technology (FFST) e de rastreamento 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, 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 por meio 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.

Desinstalando o Internet Pass-Thru

Antes de desinstalar o MQIPT de seu sistema, impeça-o de iniciar automaticamente, conforme descrito em “Iniciando o Internet Pass-Thru Automaticamente” na página 57. Efetue login como root e execute o comando `installp`:

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

Capítulo 16. 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”
- “Configurando o Internet Pass-Thru” na página 60
- “Iniciando o Internet Pass-Thru a partir da Linha de Comandos” na página 60
- “Iniciando o Internet Pass-Thru Automaticamente” na página 61
- “Iniciando o Cliente Administrativo a partir da Linha de Comandos” na página 61
- “Desinstalando o Internet Pass-Thru” na página 62

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/webspheremq/supportpacs>

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 pressupõe 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
Leia-me.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
exits/ SampleOneRouteExit.java	Amostra da saída de segurança
exits/ SampleOneRouteExit.conf	Arquivo de configuração para SampleOneRouteExit
exits/SampleRoutingExit.java	Amostra da saída de segurança

Arquivo	Finalidade
exits/SampleRoutingExit.conf	Arquivo de configuração para SampleRoutingExit
exits/SampleSecurityExit.java	Amostra da saída de segurança
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
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/mqiptPW	Criptografia de senha utilizada para abrir os arquivos de conjunto de chaves
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>/html/<nomearquivo>.zip	Arquivo mestre do manual do <i>internet pass-thru</i> no formato HTML. Consulte “Bibliografia” na página 173 para obter mais informações sobre a documentação em cópia eletrônica.
lib/guiadmin.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 19, “Administrando e Configurando o Internet Pass-Thru”, na página 71 para obter mais informações.

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 ..
```

A execução do 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 149. As mensagens a seguir são um exemplo de um início bem-sucedido do MQIPT:

```
5639-L92 (C) Copyright IBM Corp. 2000 Todos os Direitos Reservados
MQCPI001 WebSphere MQ internet pass-thru Versão 1.3.0 iniciando
MQCPI004 Lendo informações sobre configuração de /opt/mqipt/mqipt.conf
MQCPI008 Atendendo comandos de controle na porta 1881
MQCPI011 O caminho /opt/mqipt/logs será usado p/ armazenar arquivos de log
MQCPI006 A rota 1418 foi iniciada e enviará mensagens para:
MQCPI034 ....mqserver.company4.com(1414)
MQCPI035 ....utilizando protocolos MQ
MQCPI078 Rota 1418 pronta para os pedidos de conexão
MQCPI006 A rota 1415 iniciou e enviará mensagens para:
MQCPI034 ....mqipt.company2.com(1415)
MQCPI035 ....utilizando protocolos MQ
MQCPI036 ....Lado do SSL ativado com as propriedades:
MQCPI031 .....conjunto de cifras <null>
MQCPI032 .....arquivo de conjunto de chaves /opt/mqipt/KeyMan.pfx
MQCPI038 .....nome(s) diferente(s) CN=*Doe O=IBM OU=* L=* ST=* C=*
MQCPI078 Rota 1415 pronta para os pedidos de conexão
```

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 de "erros" no qual quaisquer registros de FFST (First Failure Support Technology (FFST) e de rastreamento 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, altere o diretório para bin e execute mqiptGui. Por exemplo:

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

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

```
mqipltGui <socksHostName <socksPort>>
```

O socksPort padrão é 1080.

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

Desinstalando o Internet Pass-Thru

Antes de desinstalar o MQIPT de seu sistema, impeça-o de iniciar automaticamente, conforme descrito em “Iniciando o Internet Pass-Thru Automaticamente” na página 61. Efetue login como root e execute o comando swremove:

```
swremove MQIPT
```

Capítulo 17. Instalando o Internet Pass-Thru no Linux

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

- “Fazendo Download e Instalando os Arquivos”
- “Configurando o Internet Pass-Thru” na página 64
- “Iniciando o Internet Pass-Thru a partir da Linha de Comandos” na página 64
- “Iniciando o Internet Pass-Thru Automaticamente” na página 65
- “Iniciando o Cliente Administrativo a partir da Linha de Comandos” na página 65
- “Desinstalando o Internet Pass-Thru” na página 66

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/webspheremq/supportpacs>

Siga as instruções para fazer download.

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

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

O exemplo supõe que `ms81_linux.tar.z` esteja no diretório `/tmp`.

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

Arquivo	Finalidade
Leia-me.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
exits/ SampleOneRouteExit.java	Amostra da saída de segurança
exits/ SampleOneRouteExit.conf	Arquivo de configuração para SampleOneRouteExit
exits/SampleRoutingExit.java	Amostra da saída de segurança

Arquivo	Finalidade
exits/SampleRoutingExit.conf	Arquivo de configuração para SampleRoutingExit
exits/SampleSecurityExit.java	Amostra da saída de segurança
lib/libmqiptqos.so	Biblioteca fictícia para TQoS
bin/mqiptQoS	Para utilizar a biblioteca real de TQoS
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
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/mqiptPW	Criptografia de senha utilizada para abrir os arquivos de conjunto de chaves
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>/html/<nomearquivo>.zip	Arquivo mestre do manual do <i>internet pass-thru</i> no formato HTML. Consulte “Bibliografia” na página 173 para obter mais informações sobre a documentação em cópia eletrônica.
lib/guiadmin.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 19, “Administrando e Configurando o Internet Pass-Thru”, na página 71 para obter mais informações.

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 ..
```

A execução do 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 149. As mensagens a seguir são um exemplo de um início bem-sucedido do MQIPT:

```
5639-L92 (C) Copyright IBM Corp. 2000 Todos os Direitos Reservados
MQCPI001 WebSphere MQ internet pass-thru Versão 1.3.0 iniciando
MQCPI004 Lendo informações sobre configuração de /opt/mqipt/mqipt.conf
MQCPI008 Atendendo comandos de controle na porta 1881
MQCPI011 O caminho /opt/mqipt/logs será usado p/ armazenar arquivos de log
MQCPI006 A rota 1418 foi iniciada e enviará mensagens para:
MQCPI034 ....mqserver.company4.com(1414)
MQCPI035 ....utilizando protocolos MQ
MQCPI078 Rota 1418 pronta para os pedidos de conexão
MQCPI006 A rota 1415 iniciou e enviará mensagens para:
MQCPI034 ....mqipt.company2.com(1415)
MQCPI035 ....utilizando protocolos MQ
MQCPI036 ....Lado do SSL ativado com as propriedades:
MQCPI031 .....conjunto de cifras <null>
MQCPI032 .....arquivo de conjunto de chaves /opt/mqipt/KeyMan.pfx
MQCPI038 .....nome(s) diferente(s) CN=*Doe O=IBM OU=* L=* ST=* C=*
MQCPI078 Rota 1415 pronta para os pedidos de conexão
```

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 de “erros” no qual quaisquer registros de FFST (First Failure Support Technology (FFST) e de rastreamento 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, altere o diretório para `bin` e execute `mqiptGui`. Por exemplo:

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

Para permitir que o Cliente Administrativo conecte-se externamente por meio 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.

Desinstalando o Internet Pass-Thru

Antes de desinstalar o MQIPT de seu sistema, impeça-o de iniciar automaticamente, conforme descrito em “Iniciando o Internet Pass-Thru Automaticamente” na página 65. Efetue login como root e execute o comando swremove:

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

Capítulo 18. Instalação Genérica do UNIX

Uma imagem de disco de todos os arquivos MQIPT comuns é fornecida em um arquivo tar para uso geral. A finalidade desse arquivo é permitir que o MQIPT seja instalado nas plataformas UNIX para as quais o MQIPT não oferece suporte com suas próprias imagens de instalação. A intenção é permitir que o arquivo tar seja descompactado em uma determinada localização e, com pequenas alterações, permitir que o MQIPT seja implementado em qualquer plataforma que tenha suporte a Java 1.4. O script `mqiptEnv`, encontrado no subdiretório `bin`, pode precisar ser alterado de acordo com a localização dos arquivos instalados.

- “Fazendo Download e Instalando os Arquivos”
- “Configurando o Internet Pass-Thru” na página 68
- “Iniciando o Internet Pass-Thru a partir da Linha de Comandos” na página 69
- “Iniciando o Internet Pass-Thru Automaticamente” na página 70
- “Iniciando o Cliente Administrativo a partir da Linha de Comandos” na página 70
- “Desinstalando o Internet Pass-Thru” na página 70

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/websphermq/supportpacs>

Siga as instruções para fazer download.

Efetue login como `root` e descompacte `ms81.tar` no diretório de destino, como neste exemplo:

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

O exemplo supõe que `ms81.tar` tenha sido transferido por download para o diretório `/tmp`.

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

Arquivo	Finalidade
<code>Leia-me.txt</code>	Contém informações recentes não incluídas nas publicações
<code>mqiptSample.conf</code>	Arquivo de configuração de amostra
<code>ssl/sslSample.pfx</code>	Arquivo de conjunto de chaves de teste
<code>ssl/sslSample.pwd</code>	Arquivo de senha para o arquivo de conjunto de chaves de teste
<code>ssl/sslCAdefault.pfx</code>	Arquivo de conjunto de chaves de CA (Autoridade de Certificação) de amostra

Arquivo	Finalidade
ssl/sslCAdefault.pwd	Arquivo de senha para o arquivo de conjunto de chaves de CA
ssl/KeyMan.zip	Utilitário KeyMan
exits/ SampleOneRouteExit.java	Amostra da saída de segurança
exits/ SampleOneRouteExit.conf	Arquivo de configuração para SampleOneRouteExit
exits/SampleRoutingExit.java	Amostra da saída de segurança
exits/SampleRoutingExit.conf	Arquivo de configuração para SampleRoutingExit
exits/SampleSecurityExit.java	Amostra da saída de segurança
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
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/mqiptPW	Criptografia de senha utilizada para abrir os arquivos de conjunto de chaves
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/MQIPServlet.war	Arquivo archive da Web para a versão do servlet
doc/<idioma>/html/ <nomearquivo>.zip	Arquivo mestre do manual do <i>internet pass-thru</i> no formato HTML. Consulte “Bibliografia” na página 173 para obter mais informações sobre a documentação em cópia eletrônica.
lib/guiadmin.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. propriedades	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 19, “Administrando e Configurando o Internet Pass-Thru”, na página 71 para obter mais informações.

Este exemplo pressupõe que o MQIPT seja descompactado em um diretório chamado `mqipt`. É necessário atualizar o script `mqiptEnv` com a nova localização das bibliotecas de tempo de execução. O valor padrão da variável `MQIPT_CP` é:

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

No nosso exemplo, isto deve ser alterado para:

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

Também é necessário atualizar os scripts de tempo de execução antes de utilizá-los e alterar o nome completo do caminho para a localização do script mqiptEnv.

Assim, por exemplo, antes de utilizar o script mqipt, edite-o e altere a instrução após o comentário Obter classpath em:

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

para

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

Iniciando o Internet Pass-Thru a partir da Linha de Comandos

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

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

A execução do 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 149. As mensagens a seguir são um exemplo de um início bem-sucedido do MQIPT:

```
5639-L92 (C) Copyright IBM Corp. 2000 Todos os Direitos Reservados
MQCPI001 WebSphere MQ internet pass-thru Versão 1.3.0 iniciando
MQCPI004 Lendo informações sobre configuração de /mqipt/opt/mqipt/mqipt.conf
MQCPI008 Atendendo comandos de controle na porta 1881
MQCPI011 O caminho /mqipt/opt/mqipt/logs será usado p/ armazenar arquivos de log
MQCPI006 A rota 1418 foi iniciada e enviará mensagens para:
MQCPI034 ....mqserver.company4.com(1414)
MQCPI035 ....utilizando protocolos MQ
MQCPI078 Rota 1418 pronta para os pedidos de conexão
MQCPI006 A rota 1415 iniciou e enviará mensagens para:
MQCPI034 ....mqipt.company2.com(1415)
MQCPI035 ....utilizando protocolos MQ
MQCPI036 ....Lado do SSL ativado com as propriedades:
MQCPI031 .....conjunto de cifras <null>
MQCPI032 .....arquivo de conjunto de chaves /mqipt/opt/mqipt/KeyMan.pfx
MQCPI038 .....nome(s) diferente(s) CN=*Doe O=IBM OU=* L=* ST=* C=*
MQCPI078 Rota 1415 pronta para os pedidos de conexão
```

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 de “erros” no qual quaisquer registros de FFST (First Failure Support Technology (FFST) e de rastreamento são gravados

Iniciando o Internet Pass-Thru Automaticamente

Iniciar um serviço automaticamente é específico da plataforma. O script `mqiptService` é fornecido apenas como exemplo de como isto é feito em um sistema Sun Solaris. Dependendo dos requisitos do sistema, pode ser mais fácil usar utilitários específicos da plataforma para instalar o MQIPT como serviço do sistema.

Iniciando o Cliente Administrativo a partir da Linha de Comandos

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

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

Para permitir que o Cliente Administrativo conecte-se externamente por meio 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.

Desinstalando o Internet Pass-Thru

Como o MQIPT não foi instalado utilizando uma imagem instalável do sistema, é possível desinstalá-lo excluindo a estrutura de diretórios na qual ele foi instalado.

Se o MQIPT tiver sido configurado para executar como serviço do sistema, remova o serviço antes de desinstalar o código.

Capítulo 19. 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 o Cliente Administrativo para o Internet Pass-Thru”
- “Utilizando Comandos de Modo de Linha do Internet Pass-Thru” na página 75
- “Informações de Referência sobre Configuração” na página 76

Utilizando o Cliente Administrativo para o Internet Pass-Thru

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

Observe que o Cliente Administrativo não tem como pré-requisito o Java 1.4.

Os únicos dados armazenados localmente no Cliente Administrativo fazem parte da lista de MQIPs, em um arquivo denominado `client.conf`. As propriedades globais e de rota são sempre recuperadas do MQIPT antes de 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.

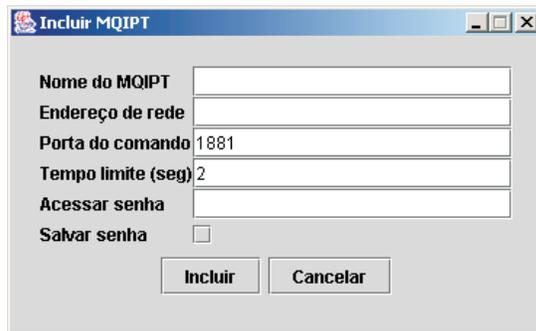
Acessar senha

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



A janela de diálogo 'Incluir MQIPT' possui os seguintes campos e controles:

- Nome do MQIPT: campo de texto vazio.
- Endereço de rede: campo de texto vazio.
- Porta do comando: campo de texto com o valor '1881'.
- Tempo limite (seg): campo de texto com o valor '2'.
- Acessar senha: campo de texto vazio.
- Salvar senha: caixa de seleção desmarcada.
- Botões: 'Incluir' e 'Cancelar'.

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 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, pressupõe-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 contrárias. 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 71.

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 71.

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 por meio 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 Figura 9 para obter detalhes. Cada rota deve ter um ListenerPort exclusivo para o MQIPT.

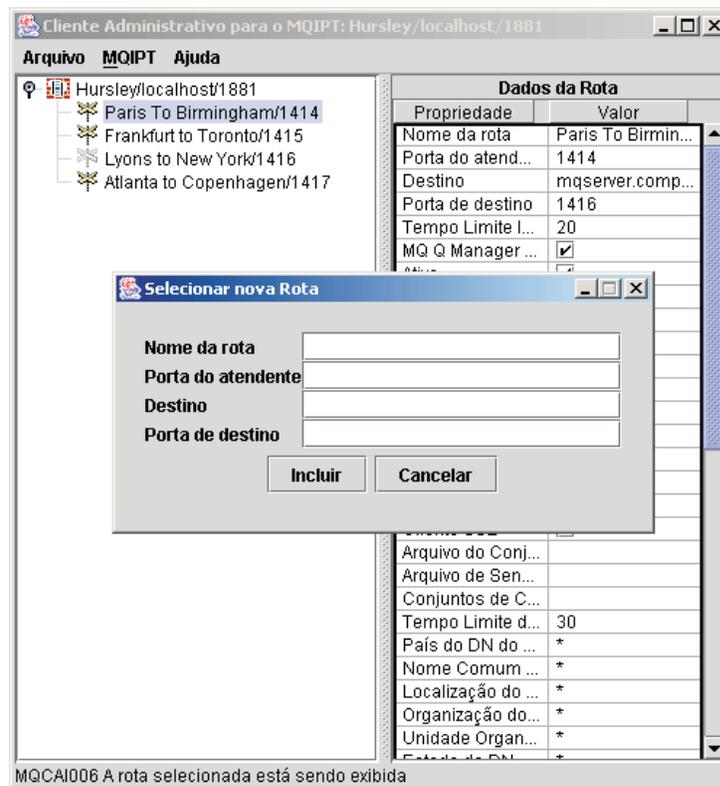


Figura 9. Incluindo uma rota

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, `mcipt.conf`, de acordo com suas necessidades. Consulte "Informações de Referência sobre Configuração" na página 76 para obter uma lista das propriedades que podem ser alteradas.

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

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

O script `mciptAdmin` 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 `mcipt.conf` especifique `RemoteShutDown=true`, este comando é ignorado.

ATUALIZAR

O MQIPT relê o `mcipt.conf`. Se o mesmo constatar:

- Que quaisquer rotas atualmente ativas estão agora marcadas como inativas (ou estão completamente ausentes), elas são encerradas e o atendimento de conexões de entrada nessas rotas é interrompido.
- Todas as rotas marcadas como ativas no arquivo de configuração e que não estejam em execução atualmente serão inicializadas.
- Que os parâmetros de configuração de uma rota atualmente em execução foram alterados, os valores alterados são aplicados a essas rotas. Nos locais possíveis (por exemplo, uma alteração na definição de rastreamento), 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

O MQIPT utiliza um arquivo de configuração denominado `mqipt.conf` para definir rotas e controlar as ações do servidor MQIPT. O arquivo 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.

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 aparecer nas seções global e route, o valor da propriedade na seção route substituirá o valor 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. Nos locais em que uma propriedade é listada com os valores `true` e `false`, é possível utilizar qualquer mistura de letras maiúsculas e minúsculas.

As alterações nas propriedades podem ser feitas editando o arquivo `mqipt.conf` ou utilizando a GUI do Cliente Administrativo. Para aplicar alterações, o administrador pode emitir um comando atualizar, a partir da GUI do Cliente Administrativo ou utilizando o script `mqiptAdmin`.

As alterações em determinadas propriedades faz com que a rota seja iniciada novamente apenas se outras propriedades já estiverem ativadas. Por exemplo, alterações em propriedades do HTTP terão efeito somente se a propriedade do HTTP também estiver ativada.

Quando uma rota é iniciada novamente, as conexões existentes são encerradas. Para cancelar esse comportamento, defina a propriedade `RouteRestart` como `false`. Isto impede que a rota seja iniciada novamente, permitindo que conexões existentes permaneçam ativas até que a propriedade `RouteRestart` seja reativada.

Para obter informações sobre como efetuar algumas configurações simples, consulte o Capítulo 20, “Iniciando o Internet Pass-Thru”, na página 95. Para uma configuração de amostra, consulte o arquivo `mqiPTSample.conf` no diretório inicial do MQIPT.

Resumo de Propriedades

A Tabela 3 mostra:

- Todas as propriedades
- Se a propriedade se aplica à seção global, à seção route ou a ambas
- Os valores padrão utilizados se uma propriedade estiver ausente nas seções route e global

Tabela 3. Resumo de propriedades de configuração

Nome da propriedade	Global	Route	Padrão
AccessPW	sim	não	<null>
Active	sim	sim	true
ClientAccess	sim	sim	false
CommandPort	sim	não	<null>
ConnectionLog	sim	não	true
Destination	não	sim	<null>
DestinationPort	não	sim	1414
HTTP ^{6,7}	sim	sim	false
HTTPChunking ¹	sim	sim	false
HTTPProxy ¹	sim	sim	<null>
HTTPProxyPort ¹	sim	sim	8080
HTTPS ¹	sim	sim	false
HTTPServer ¹	sim	sim	<null>
HTTPServerPort ¹	sim	sim	<null>
IdleTimeout	sim	sim	0
IgnoreExpiredCRLs	sim	sim	false
LDAP	sim	sim	false
LDAPIgnoreErrors ¹⁰	sim	sim	false
LDAPCacheTimeout ¹⁰	sim	sim	24
LDAPSaveCRL ¹⁰	sim	sim	false
LDAPServer1 ¹⁰	sim	sim	<null>
LDAPServer1Port ¹⁰	sim	sim	389
LDAPServer1Userid ¹⁰	sim	sim	<null>
LDAPServer1Password ¹⁰	sim	sim	<null>
LDAPServer1Timeout ¹⁰	sim	sim	0
LDAPServer2 ¹⁰	sim	sim	<null>
LDAPServer2Port ¹⁰	sim	sim	389
LDAPServer2Userid ¹⁰	sim	sim	<null>
LDAPServer2Password ¹⁰	sim	sim	<null>
LDAPServer2Timeout ¹⁰	sim	sim	0

Tabela 3. Resumo de propriedades de configuração (continuação)

Nome da propriedade	Global	Route	Padrão
ListenerPort	não	sim	<null>
LocalAddress	sim	sim	<null>
LogDir (válido apenas para MQIPTServlet)	não	não	<null>
MaxConnectionThreads	sim	sim	100
MaxLogFileSize	sim	não	50
MinConnectionThreads	sim	sim	5
Name	não	sim	<null>
NDAdvisor	sim	sim	false
NDAdvisorReplaceMode ⁴	sim	sim	false
OutgoingPort	não	sim	0
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	não	false
RouteRestart	sim	sim	true
SecurityExit	sim	sim	false
SecurityExitName ¹¹	sim	sim	<null>
SecurityExitPath ¹¹	sim	sim	<ipthome> \exits
SecurityExitTimeout ¹¹	sim	sim	5
SecurityManager	sim	não	false
SecurityManagerPolicy	sim	não	<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
SSLClientCAKeyRing ²	sim	sim	<null>
SSLClientCAKeyRingPW ²	sim	sim	<null>
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
SSLClientDN_ST ²	sim	sim	**" 5
SSLClientKeyRing ²	sim	sim	<null>

Tabela 3. Resumo de propriedades de configuração (continuação)

Nome da propriedade	Global	Route	Padrão
SSLClientKeyRingPW ²	sim	sim	<null>
SSLClientSiteDN_C ²	sim	sim	"*" 5
SSLClientSiteDN_CN ²	sim	sim	"*" 5
SSLClientSiteDN_L ²	sim	sim	"*" 5
SSLClientSiteDN_O ²	sim	sim	"*" 5
SSLClientSiteDN_OU ²	sim	sim	"*" 5
SSLClientSiteDN_ST ²	sim	sim	"*" 5
SSLClientSiteLabel ²	sim	sim	<null>
SSLProxyMode	sim	sim	false
SSLServer ⁶	sim	sim	false
SSLServerAskClientAuth ³	sim	sim	false
SSLServerCAKeyRing ³	sim	sim	<null>
SSLServerCAKeyRingPW ³	sim	sim	<null>
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>
SSLServerSiteDN_C ³	sim	sim	"*" 5
SSLServerSiteDN_CN ³	sim	sim	"*" 5
SSLServerSiteDN_L ³	sim	sim	"*" 5
SSLServerSiteDN_O ³	sim	sim	"*" 5
SSLServerSiteDN_OU ³	sim	sim	"*" 5
SSLServerSiteDN_ST ³	sim	sim	"*" 5
SSLServerSiteLabel ³	sim	sim	<null>
Trace	sim	sim	0
UriName (Consulte a página "UriName" na página 94 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 essas propriedades entrem em vigor.
9. Defina QoS como true para que essas propriedades entrem em vigor.
10. Defina LDAP como true para que essas propriedades entrem em vigor.
11. Defina SecurityExit como true para que essas propriedades entrem em vigor.

Informações de Referência da Seção Global

A seção global pode conter as propriedades a seguir e todas as propriedades de “Informações de Referência da Seção Route” na página 81, exceto ListenerPort, Destination, DestinationPort, Name e OutgoingPort.

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 desconexão 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 da conexão. Quando o tamanho do arquivo aumenta acima do máximo, é criado um backup (mqipt.back) 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 31 para obter mais informações. O valor padrão desta propriedade é false.

SecurityManagerPolicy

O nome completo de um arquivo de critério. Se esta propriedade não for definida, apenas os arquivos de critério 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 ATUALIZAR 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 MQIPs 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 ATUALIZAR 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 subsequente) 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 ATUALIZAR 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 ATUALIZAR 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, a rota será parada e iniciada novamente quando um comando ATUALIZAR 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 (e HTTP estiver definido como true), a rota será parada e iniciada novamente quando um comando ATUALIZAR 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 HTTPServer também estiver definido, um pedido CONNECT será emitido para o HTTPProxy, em vez de um POST normal. Se você alterar esta propriedade (e HTTP estiver definido como true), a rota será parada e iniciada novamente quando um comando ATUALIZAR 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, a não ser que HTTPS tenha sido definido como true e não exista HTTPServer (neste caso, o padrão é 443). Se você alterar esta propriedade (e HTTP estiver definido como true), a rota será parada e iniciada novamente quando um comando ATUALIZAR for emitido. Todas as conexões para esta rota serão encerradas.

HTTPServer

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

HTTPS

Ative esta propriedade para fazer pedidos HTTPS. A propriedade HTTP também deverá ser ativada. Se você alterar esta propriedade (e HTTP estiver definido como true), a rota será parada e iniciada novamente quando um comando ATUALIZAR for emitido. Todas as conexões para esta rota serão encerradas.

HTTPServerPort

O endereço de porta a ser utilizado no servidor HTTP. O valor padrão é 8080, a não ser que HTTPS tenha sido definido como true (nesse caso, o padrão é 443). Se você alterar esta propriedade (e HTTP estiver definido como true), a rota será parada e iniciada novamente quando um comando ATUALIZAR 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 possui a propriedade DISCONT. Se você definir o parâmetro IdleTimeout, tome

nota de DISCONT. Um valor 0 indica sem tempo limite inativo. As alterações desta propriedade entram em vigor apenas quando a rota é iniciada novamente.

IgnoreExpiredCRLs

Defina esta propriedade como true para ignorar um CRL expirado. O valor padrão é false.

Atenção

Se você ativar esta propriedade, um certificado revogado pode ser utilizado para fazer uma conexão SSL.

LDAP

Defina esta propriedade como true para permitir o uso de um servidor LDAP ao utilizar conexões SSL. O MQIPT utiliza o servidor LDAP para recuperar CRLs e ARLs. A propriedade SSLClient ou SSLServer também deve ser ativada para que esta propriedade tenha efeito.

LDAPIgnoreErrors

Defina esse propriedade como true para ignorar erros de conexão ou de tempo limite ao executar uma pesquisa LDAP. Se o MQIPT não puder executar uma pesquisa bem-sucedida, não permitirá que a conexão do cliente seja concluída, a não ser que esta propriedade tenha sido ativada. Uma pesquisa bem-sucedida significa que um CRL foi recuperado ou que não há CRLs disponíveis para o CA especificado. Se você alterar esta propriedade (e LDAP for definida como true), a rota será parada e iniciada novamente quando um comando ATUALIZAR for emitido. Todas as conexões para esta rota serão encerradas.

Atenção

Se você ativar esta propriedade, um certificado revogado pode ser utilizado para fazer uma conexão SSL.

LDAPCacheTimeout

Quando um CRL tiver sido recuperado de um servidor LDAP, ele será armazenado internamente no MQIPT em um cache temporário. As entradas nesse cache expiram depois de um determinado tempo limite, especificado por esta propriedade. O valor padrão é 24 horas. Especificar um valor de tempo limite 0 significa que as entradas no cache não expiram até que a rota seja iniciada novamente. Se você alterar esta propriedade (e LDAP for definida como true), a rota será parada e iniciada novamente quando um comando ATUALIZAR for emitido. Todas as conexões para esta rota serão encerradas.

LDAPSaveCRL

Defina esta propriedade como true para atualizar o arquivo de conjunto de chaves indicado com os CRLs recuperados do servidor LDAP. Os arquivos do conjunto de chaves são especificados com as propriedades SSLClientKeyRing, SSLClientCAKeyRing, SSLServerKeyRing e SSLServerCAKeyRing. Isso implica que o MQIPT deve ter acesso de gravação aos arquivos do conjunto de chaves. Se você alterar esta propriedade (e LDAP for definida como true), a rota será parada e iniciada novamente quando um comando ATUALIZAR for emitido. Todas as conexões para esta rota serão encerradas.

LDAPServer1

Defina esta propriedade como o nome do host ou o endereço IP do servidor

LDAP principal. Esta propriedade deve ser definida se o LDAP tiver sido ativado. Se você alterar esta propriedade (e LDAP for definida como true), a rota será parada e iniciada novamente quando um comando ATUALIZAR for emitido. Todas as conexões para esta rota serão encerradas.

LDAPServer1Port

Defina esta propriedade como o endereço de porta de atendimento do servidor LDAP principal. Seu valor padrão é 389. Se você alterar esta propriedade (e LDAP for definida como true), a rota será parada e iniciada novamente quando um comando ATUALIZAR for emitido. Todas as conexões para esta rota serão encerradas.

LDAPServer1Userid

Defina esta propriedade como o ID do usuário necessário para acessar o servidor LDAP principal. Esta propriedade deve ser definida se for necessária autorização para acessar o servidor LDAP principal. Se você alterar esta propriedade (e LDAP for definida como true), a rota será parada e iniciada novamente quando um comando ATUALIZAR for emitido. Todas as conexões para esta rota serão encerradas.

LDAPServer1Password

Defina esta propriedade como a senha necessária para acessar o servidor LDAP principal. Esta propriedade deve ser definida se LDAPServer1Userid tiver sido definido. Se você alterar esta propriedade (e LDAP for definida como true), a rota será parada e iniciada novamente quando um comando ATUALIZAR for emitido. Todas as conexões para esta rota serão encerradas.

LDAPServer1Timeout

Defina esta propriedade como o número de segundos que o MQIPT aguarda uma resposta do servidor LDAP principal. Seu valor padrão é 0, o que significa que a conexão não tem tempo limite. Se você alterar esta propriedade (e LDAP for definida como true), a rota será parada e iniciada novamente quando um comando ATUALIZAR for emitido. Todas as conexões para esta rota serão encerradas.

LDAPServer2

Defina esta propriedade como o nome do host ou o endereço IP do servidor LDAP de backup. Esta propriedade é opcional. Se você alterar esta propriedade (e LDAP for definida como true), a rota será parada e iniciada novamente quando um comando ATUALIZAR for emitido. Todas as conexões para esta rota serão encerradas.

LDAPServer2Port

Defina esta propriedade como o endereço de porta de atendimento do servidor LDAP de backup. Seu valor padrão é 389. Se você alterar esta propriedade (e LDAP for definida como true), a rota será parada e iniciada novamente quando um comando ATUALIZAR for emitido. Todas as conexões para esta rota serão encerradas.

LDAPServer2Userid

Defina esta propriedade como o ID do usuário necessário para acessar o servidor LDAP de backup. Esta propriedade deve ser definida se for necessária autorização para acessar o servidor LDAP de backup. Se você alterar esta propriedade (e LDAP for definida como true), a rota será parada e iniciada novamente quando um comando ATUALIZAR for emitido. Todas as conexões para esta rota serão encerradas.

LDAPServer2Password

Defina esta propriedade como a senha necessária para acessar o servidor LDAP de backup. Esta propriedade deve ser definida se LDAPServer2 tiver

sido ativada. Se você alterar esta propriedade (e LDAP for definida como true), a rota será parada e iniciada novamente quando um comando ATUALIZAR for emitido. Todas as conexões para esta rota serão encerradas.

LDAPServer2Timeout

Defina esta propriedade como o número de segundos que o MQIPT aguarda uma resposta do servidor LDAP de backup. Seu valor padrão é 0, o que significa que a conexão não tem tempo limite. Se você alterar esta propriedade (e LDAP for definida como true), a rota será parada e iniciada novamente quando um comando ATUALIZAR for emitido. Todas as conexões para esta rota serão encerradas.

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.

LocalAddress

O endereço IP local para ligação de todas essas conexões. Se você alterar esta propriedade, a rota será parada e iniciada novamente quando um comando ATUALIZAR for emitido. Todas as conexões para esta rota serão encerradas.

LogDir

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

MaxConnectionThreads

O número máximo de encadeamentos 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 encadeamentos estiverem em uso. Excedendo a esse número, os pedidos de conexão subsequentes 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 é utilizado quando o comando ATUALIZAR for emitido. Todas as conexões captam o novo valor imediatamente. A rota não será encerrada.

MinConnectionThreads

O número mínimo de encadeamentos de conexão (encadeamentos para manipular conexões de entrada nesta rota). Este é o número de encadeamentos alocados quando a rota é iniciada e o número total de encadeamentos 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 rastreamento. As alterações desta propriedade entram em vigor apenas quando a rota é iniciada novamente.

NDAvisor

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 ATUALIZAR for emitido. Todas as conexões para esta rota serão encerradas. Para utilizar a propriedade `NDAvvisorReplaceMode`, defina esta propriedade como `true`.

NDAvvisorReplaceMode

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 `NDAvvisor` como `true` para utilizar esta propriedade.

OutgoingPort

Este é o endereço de porta inicial utilizado por conexões de saída. O intervalo de endereços de porta corresponde ao valor `MaxConnectionThread` para essa rota. O valor padrão 0 utiliza um endereço de porta definido pelo sistema. Se você alterar esta propriedade, a rota será parada e iniciada novamente quando um comando ATUALIZAR for emitido. Todas as conexões para esta rota serão encerradas.

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 ATUALIZAR 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 ATUALIZAR 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. Por exemplo, 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 ATUALIZAR 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`). Por exemplo, 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 ATUALIZAR for emitido. Todas as conexões para esta rota serão encerradas

RouteRestart

Defina esta propriedade como `false` para impedir que a rota seja iniciada

novamente quando outras propriedades tiverem sido alteradas e um comando ATUALIZAR tiver sido emitido. O valor padrão para esta propriedade é true.

SecurityExit

Defina esta propriedade como true para ativar uma saída de segurança definida pelo usuário. O valor padrão desta propriedade é false.

SecurityExitName

O nome da classe da saída de segurança definida pelo usuário. Esta propriedade deve ser definida se SecurityExit tiver sido definida como true. Se você alterar esta propriedade (e SecurityExit estiver definida como true), a rota será parada e iniciada novamente quando um comando ATUALIZAR for emitido. Todas as conexões para esta rota serão encerradas.

SecurityExitPath

O nome completo do caminho que contém a saída de segurança definida pelo usuário. Se esta propriedade não tiver sido definida, seu padrão será o subdiretório exits. Esta propriedade também pode definir o nome de um arquivo jar que contém a saída de segurança definida pelo usuário. Se você alterar esta propriedade (e SecurityExit estiver definida como true), a rota será parada e iniciada novamente quando um comando ATUALIZAR for emitido. Todas as conexões para esta rota serão encerradas.

SecurityExitTimeout

Este valor de tempo limite é utilizado pelo MQIPT para determinar por quanto tempo ele deve esperar (em segundos) por uma resposta ao validar um pedido de conexão. O valor padrão é 5 segundos. Se você alterar esta propriedade (e SecurityExit estiver definida como true), a rota será parada e iniciada novamente quando um comando ATUALIZAR 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 ATUALIZAR 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 ATUALIZAR 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 ATUALIZAR 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 ATUALIZAR 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 ATUALIZAR 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 indica que o destino é outro MQIPT agindo como servidor SSL ou um sproxy/servidor HTTP. É necessário especificar o nome de um arquivo de conjunto de chaves, com a propriedade SSLClientKeyRing ou SSLClientCAKeyRing. Se você alterar esta propriedade, a rota será parada e iniciada novamente quando um comando ATUALIZAR for emitido. Todas as conexões para esta rota serão encerradas. Esta propriedade não pode ser utilizada com:

- HTTP
- QoS
- SSLProxyMode

SSLClientCAKeyRing

O nome completo do arquivo de conjunto de chaves que contém os certificados CA, utilizado para autenticar certificados do servidor SSL. Nas plataformas Windows, utilize duas barras invertidas (\\) como separador de arquivos. Se você alterar esta propriedade (e SSLClient for definida como true), a rota será parada e iniciada novamente quando um comando ATUALIZAR for emitido. Todas as conexões para esta rota serão encerradas.

SSLClientCAKeyRingPW

O nome completo do arquivo que contém a senha para abrir o conjunto de chaves CA do cliente. Nas plataformas Windows, utilize duas barras invertidas (\\) como separador de arquivos. Se você alterar esta propriedade (e SSLClient for definida como true), a rota será parada e iniciada novamente quando um comando ATUALIZAR for emitido. Todas as conexões para esta rota serão encerradas.

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 (e SSLClient for definida como true), a rota será parada e iniciada novamente quando um comando ATUALIZAR 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 (e SSLClient for definida como true), a rota será parada e iniciada novamente quando um comando ATUALIZAR for emitido. Todas as conexões para esta rota serão encerradas.

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 países”. Se você alterar esta propriedade (e SSLClient for definida como true), a rota será parada e iniciada novamente quando um comando ATUALIZAR 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 de países”. Se você alterar esta propriedade (e SSLClient for definida como true), a rota será parada e iniciada novamente quando um comando ATUALIZAR 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 (e SSLClient for definida como true), a rota será parada e iniciada novamente quando um comando ATUALIZAR 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 (e SSLClient for definida como true), a rota será parada e iniciada novamente quando um comando ATUALIZAR 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 organizacional 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 organizacional units”. Se você alterar esta propriedade (e SSLClient for definida como true), a rota será parada e iniciada novamente quando um comando ATUALIZAR 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 (e SSLClient for definida como true), a rota será parada e iniciada novamente quando um comando ATUALIZAR 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. Nas plataformas **Windows**, você deve utilizar uma barra dupla invertida(\\) como separador de arquivos. Você deve especificar SSLClientKeyRing se definir SSLClient como true. Se você alterar esta

propriedade (e SSLClient for definida como true), a rota será parada e iniciada novamente quando um comando ATUALIZAR 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. Nas plataformas **Windows**, você deve utilizar uma barra dupla invertida(\\) como separador de arquivos. Você deve especificar SSLClientKeyRingPW se definir SSLClient como true. Se você alterar esta propriedade (e SSLClient for definida como true), a rota será parada e iniciada novamente quando um comando ATUALIZAR for emitido. Todas as conexões para esta rota serão encerradas.

SSLClientSiteDN_C

Utilize esta propriedade para especificar um nome de País para selecionar um certificado para envio ao servidor SSL. Se você não especificar esta propriedade, subentende-se "todos os nomes de países". Se você alterar esta propriedade (e SSLClient for definida como true), a rota será parada e iniciada novamente quando um comando ATUALIZAR for emitido. Todas as conexões para esta rota serão encerradas.

SSLClientSiteDN_CN

Utilize esta propriedade para especificar um Nome Comum para selecionar um certificado para envio ao servidor SSL. Se você não especificar esta propriedade, subentende-se "todos os nomes comuns". Se você alterar esta propriedade (e SSLClient for definida como true), a rota será parada e iniciada novamente quando um comando ATUALIZAR for emitido. Todas as conexões para esta rota serão encerradas.

SSLClientSiteDN_L

Utilize esta propriedade para especificar um nome de Localização para selecionar um certificado para envio ao servidor SSL. Se você não especificar esta propriedade, subentende-se "todos os nomes de localizações". Se você alterar esta propriedade (e SSLClient for definida como true), a rota será parada e iniciada novamente quando um comando ATUALIZAR for emitido. Todas as conexões para esta rota serão encerradas.

SSLClientSiteDN_O

Utilize esta propriedade para especificar um nome de Organização para selecionar um certificado para envio ao servidor SSL. Se você não especificar esta propriedade, subentende-se "todos os nomes de organização". Se você alterar esta propriedade (e SSLClient for definida como true), a rota será parada e iniciada novamente quando um comando ATUALIZAR for emitido. Todas as conexões para esta rota serão encerradas.

SSLClientSiteDN_OU

Utilize esta propriedade para especificar um nome de Organizational Unit para selecionar um certificado para envio ao servidor SSL. Se você não especificar esta propriedade, subentende-se "todos os nomes de organizational unit". Se você alterar esta propriedade (e SSLClient for definida como true), a rota será parada e iniciada novamente quando um comando ATUALIZAR for emitido. Todas as conexões para esta rota serão encerradas.

SSLClientSiteDN_ST

Utilize esta propriedade para especificar um nome de Estado para selecionar um certificado para envio ao servidor SSL. Se você não especificar esta propriedade, subentende-se "todos os nomes de estado". Se você alterar esta

propriedade (e `SSLClient` for definida como `true`), a rota será parada e iniciada novamente quando um comando `ATUALIZAR` for emitido. Todas as conexões para esta rota serão encerradas.

SSLClientSiteLabel

Utilize esta propriedade para especificar um nome de Rótulo para selecionar um certificado para envio ao servidor SSL. Se você não especificar esta propriedade, subentende-se "todos os nomes de rótulo". Se você alterar esta propriedade (e `SSLClient` for definida como `true`), a rota será parada e iniciada novamente quando um comando `ATUALIZAR` 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 `ATUALIZAR` 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 `ATUALIZAR` for emitido. Todas as conexões para esta rota serão encerradas. Esta propriedade não pode ser utilizada com:

- QoS
- SocksServer
- SSLProxyMode

SSLServerCAKeyRing

O nome completo do arquivo de conjunto de chaves que contém os certificados CA, utilizado para autenticar certificados do cliente SSL. Nas plataformas Windows, utilize duas barras invertidas (\\) como separador de arquivos. Se você alterar esta propriedade (e `SSLServer` for definida como `true`), a rota será parada e iniciada novamente quando um comando `ATUALIZAR` for emitido. Todas as conexões para esta rota serão encerradas.

SSLServerCAKeyRingPW

O nome completo do arquivo que contém a senha para abrir o conjunto de chaves CA do servidor. Nas plataformas Windows, utilize duas barras invertidas (\\) como separador de arquivos. Se você alterar esta propriedade (e `SSLServer` for definida como `true`), a rota será parada e iniciada novamente quando um comando `ATUALIZAR` for emitido. Todas as conexões para esta rota serão encerradas.

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 (e `SSLServer` for definida como `true`), a rota será parada e

iniciada novamente quando um comando ATUALIZAR 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 (e SSLServer for definida como true), a rota será parada e iniciada novamente quando um comando ATUALIZAR 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 (e SSLServer for definida como true), a rota será parada e iniciada novamente quando um comando ATUALIZAR 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 (e SSLServer for definida como true), a rota será parada e iniciada novamente quando um comando ATUALIZAR 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 (e SSLServer for definida como true), a rota será parada e iniciada novamente quando um comando ATUALIZAR 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 (e SSLServer for definida como true), a rota será parada e iniciada novamente quando um comando ATUALIZAR 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 organizacional 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 organizacional units”. Se você alterar esta propriedade (e SSLServer for definida como true), a rota será parada e iniciada novamente quando um comando ATUALIZAR 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 (e SSLServer for definida como true), a rota será parada e iniciada novamente quando um comando ATUALIZAR 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. Nas plataformas **Windows**, você deve utilizar uma barra dupla invertida(\\) como separador de arquivos. Você deve especificar SSLServerKeyRing se definir SSLServer como true. Se você alterar esta propriedade (e SSLServer for definida como true), a rota será parada e iniciada novamente quando um comando ATUALIZAR 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. Nas plataformas **Windows**, você deve utilizar uma barra dupla invertida(\\) como separador de arquivos. Você deve especificar SSLServerKeyRingPW se definir SSLServer como true. Se você alterar esta propriedade (e SSLServer for definida como true), a rota será parada e iniciada novamente quando um comando ATUALIZAR for emitido. Todas as conexões para esta rota serão encerradas.

SSLServerSiteDN_C

Utilize esta propriedade para especificar um nome de País para selecionar um certificado para envio ao cliente SSL. Se você não especificar esta propriedade, subentende-se "todos os nomes de países". Se você alterar esta propriedade (e SSLServer for definida como true), a rota será parada e iniciada novamente quando um comando ATUALIZAR for emitido. Todas as conexões para esta rota serão encerradas.

SSLServerSiteDN_CN

Utilize esta propriedade para especificar um Nome Comum para selecionar um certificado para envio ao cliente SSL. Se você não especificar esta propriedade, subentende-se "todos os nomes comuns". Se você alterar esta propriedade (e SSLServer for definida como true), a rota será parada e iniciada novamente quando um comando ATUALIZAR for emitido. Todas as conexões para esta rota serão encerradas.

SSLServerSiteDN_L

Utilize esta propriedade para especificar um nome de Localização para selecionar um certificado para envio ao cliente SSL. Se você não especificar esta propriedade, subentende-se "todos os nomes de localizações". Se você alterar esta propriedade (e SSLServer for definida como true), a rota será parada e iniciada novamente quando um comando ATUALIZAR for emitido. Todas as conexões para esta rota serão encerradas.

SSLServerSiteDN_O

Utilize esta propriedade para especificar um nome de Organização para selecionar um certificado para envio ao cliente SSL. Se você não especificar esta propriedade, subentende-se "todos os nomes de organização". Se você alterar esta propriedade (e SSLServer for definida como true), a rota será parada e iniciada novamente quando um comando ATUALIZAR for emitido. Todas as conexões para esta rota serão encerradas.

SSLServerSiteDN_OU

Utilize esta propriedade para especificar um nome de Organizational Unit para selecionar um certificado para envio ao cliente SSL. Se você não especificar esta propriedade, subentende-se "todos os nomes de organizational unit". Se você

alterar esta propriedade (e SSLServer for definida como true), a rota será parada e iniciada novamente quando um comando ATUALIZAR for emitido. Todas as conexões para esta rota serão encerradas.

SSLServerSiteDN_ST

Utilize esta propriedade para especificar um nome de Estado para selecionar um certificado para envio ao cliente SSL. Se você não especificar esta propriedade, subentende-se "todos os nomes de estado". Se você alterar esta propriedade (e SSLServer for definida como true), a rota será parada e iniciada novamente quando um comando ATUALIZAR for emitido. Todas as conexões para esta rota serão encerradas.

SSLServerSiteLabel

Utilize esta propriedade para especificar um nome de Rótulo para selecionar um certificado para envio ao cliente SSL. Se você não especificar esta propriedade, subentende-se "todos os nomes de rótulo". Se você alterar esta propriedade (e SSLServer for definida como true), a rota será parada e iniciada novamente quando um comando ATUALIZAR for emitido. Todas as conexões para esta rota serão encerradas.

Trace

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

Se uma alteração desta propriedade afetar uma rota, o novo valor é utilizado quando o comando ATUALIZAR 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 estiverem definidos como True, a rota será parada e iniciada novamente quando um comando ATUALIZAR for emitido.

Capítulo 20. 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”
- “Configurações de Exemplo” na página 96
- “Teste de Verificação de Instalação” na página 96
- “Autenticação do Servidor SSL” na página 98
- “Autenticação do Cliente SSL” na página 100
- “Configuração do Proxy HTTP” na página 103
- “Configurando o Controle de Acesso” na página 105
- “Configurando a QoS (Qualidade de Serviço)” na página 108
- “Configurando o Proxy SOCKS” na página 111
- “Configurando o Cliente SOCKS” na página 113
- “Criando Certificados de Teste SSL” na página 114
- “Configurando o Servlet do MQIPT” na página 115
- “Configuração HTTPS” na página 118
- “Configurando o Suporte ao Clustering do MQIPT” na página 121
- “Criando um Arquivo de Conjunto de Chaves” na página 125
- “Alocando Endereços de Porta” na página 127
- “Utilizando um Servidor LDAP” na página 129
- “Modo de Proxy SSL” na página 133
- “Regravação Apache” na página 135
- “Saída de Segurança” na página 139
- “Saída de Segurança de Roteamento” na página 141
- “Saída Dinâmica de Uma Rota” na página 144

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 `amqspc`
- 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 a seguir.

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 95

Teste de Verificação de Instalação

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

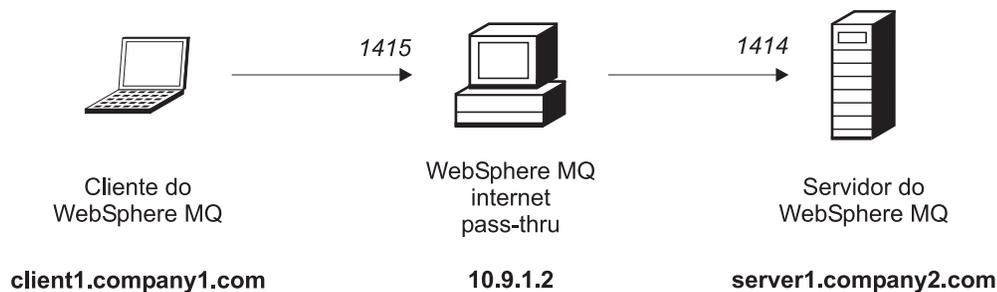


Figura 10. Diagrama de rede do IVT

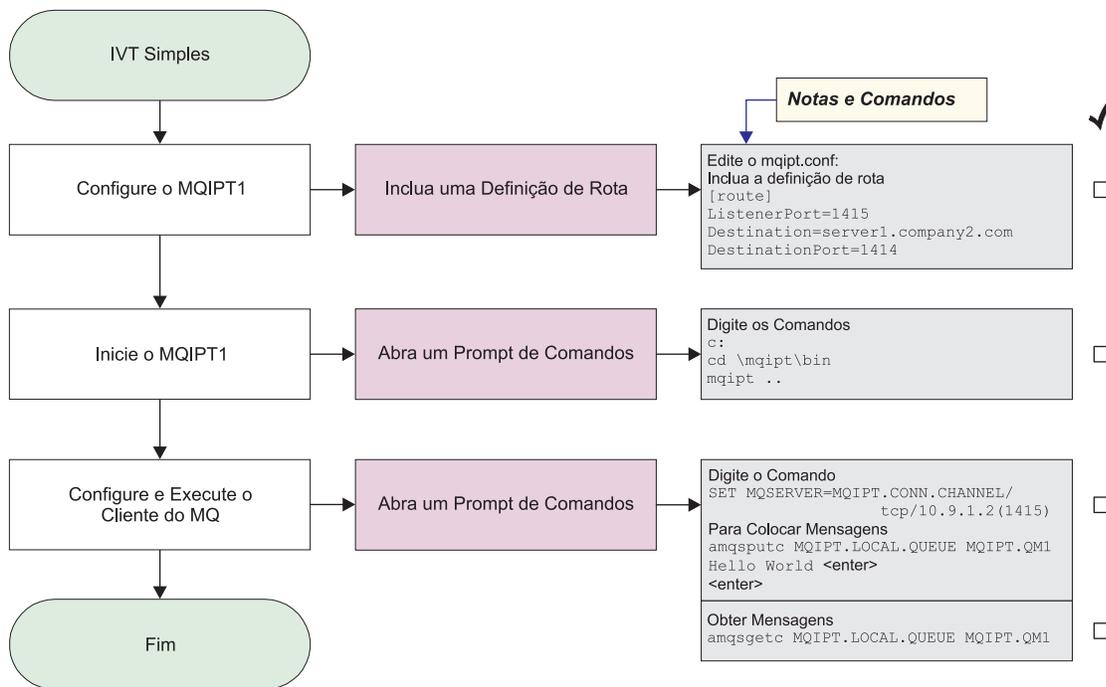


Figura 11. Configuração do IVT

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 Todos os Direitos Reservados
MQCPI001 WebSphere MQ internet pass-thru Versão 1.3.0 iniciando
MQCPI004 Lendo informações sobre configuração de C:\mqipt\mqipt.conf
MQCPI011 O caminho C:\mqipt\logs será usado p/ armazenar arquivos de log
MQCPI006 A rota 1415 iniciou e enviará mensagens para:
MQCPI034 ....server1.company2.com(1414)
MQCPI035 ....utilizando protocolos MQ
MQCPI078 Rota 1415 pronta para os pedidos de conexão
```

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 WebSphere MQ a um servidor WebSphere MQ por meio de dois MQIPTs. Durante o protocolo de reconhecimento SSL, o servidor envia seu certificado de teste para o cliente. O cliente utiliza sua cópia do certificado (com o sinalizador `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 96). Para obter detalhes sobre como criar um certificado de teste para utilizar neste exemplo, consulte "Criando Certificados de Teste SSL" na página 114.

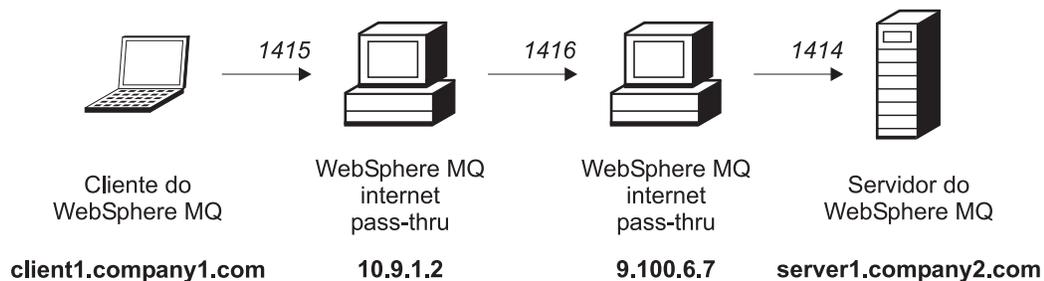


Figura 12. Diagrama de rede do servidor SSL

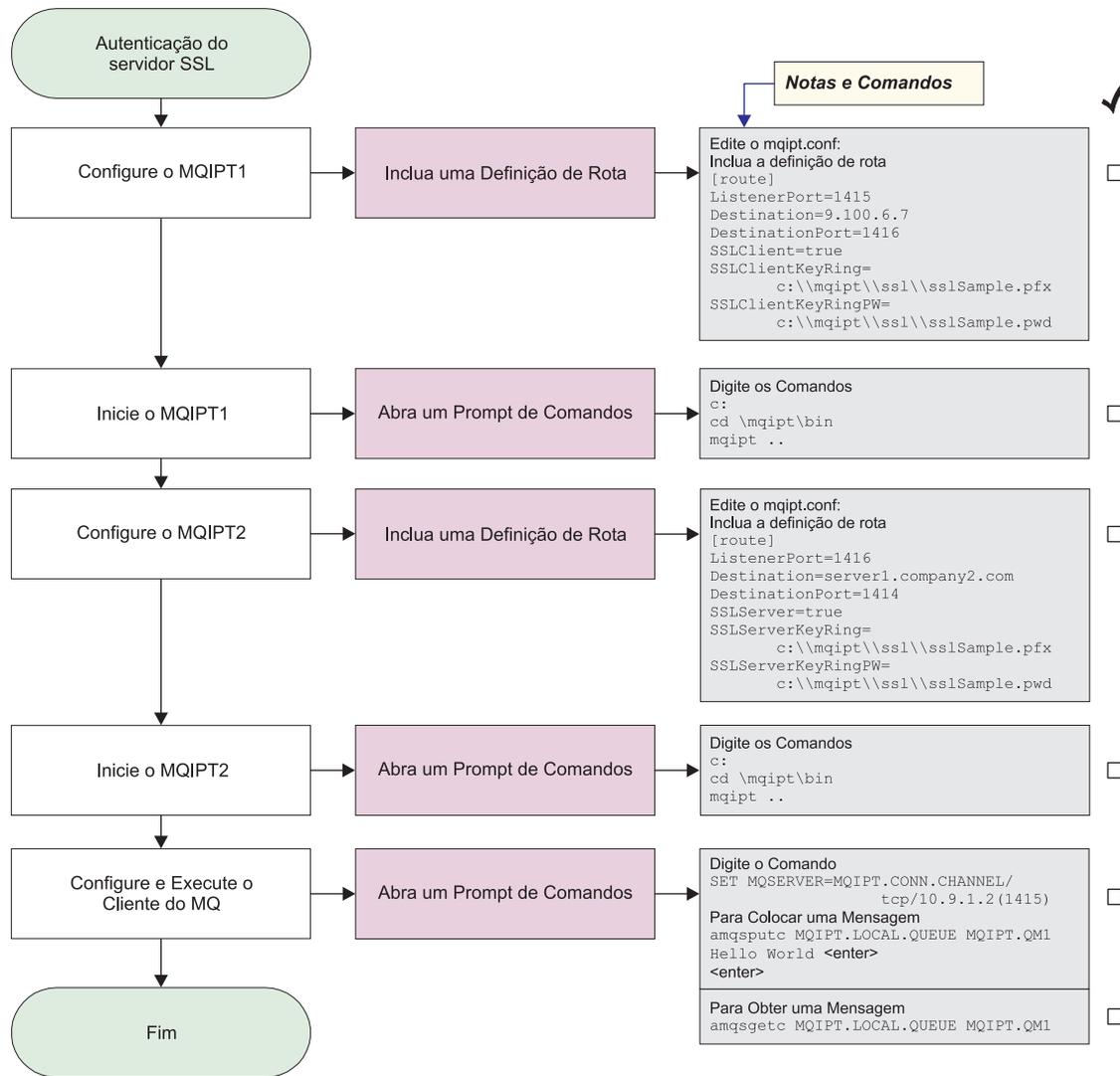


Figura 13. Autenticação do servidor SSL

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 Todos os Direitos Reservados
MQCPI001 WebSphere MQ internet pass-thru Versão 1.3.0 iniciando
MQCPI011 O caminho c:\mqipt\logs será usado p/ armazenar arquivos de log
MQCPI006 A rota 1415 iniciou e enviará mensagens para:
```

```

MQCPI034 ....9.100.6.7(1416)
MQCPI035 ....utilizando protocolos MQ
MQCPI036 ....Lado do SSL ativado com as propriedades:
MQCPI031 .....conjunto de cifras <null>
MQCPI032 .....arquivo de conjunto de chaves c:\mqipt\sslSample.pfx
MQCPI047 .....arquivo de conjunto de chaves CA <null>
MQCPI038 .....nome(s) diferente(s) CN=* O=* OU=* L=* ST=* C=*
MQCPI078 Rota 1415 pronta para os pedidos de conexão

```

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 Todos os Direitos Reservados
MQCPI001 WebSphere MQ internet pass-thru Versão 1.3.0 iniciando
MQCPI011 O caminho c:\mqipt\logs será usado p/ armazenar arquivos de log
MQCPI006 A rota 1416 foi iniciada e enviará mensagens para:
MQCPI034 ....server1.company2.com(1414)
MQCPI035 ....utilizando protocolos MQ
MQCPI037 ....Lado do SSL ativado com as propriedades:
MQCPI031 .....conjunto de cifras <null>
MQCPI032 .....arquivo de conjunto de chaves c:\mqipt\sslSample.pfx
MQCPI047 .....arquivo de conjunto de chaves CA <null>
MQCPI038 .....nome(s) diferente(s) CN=* O=* OU=* L=* ST=* C=*
MQCPI033 .....autenticação do cliente definida como false
MQCPI078 Rota 1416 pronta para os pedidos de conexão

```

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 envia seu certificado de teste para o cliente. O cliente utiliza sua cópia do certificado, com o sinalizador trust-as-peer, para autenticar o servidor. Em seguida, o cliente envia seu certificado de teste para o servidor. O servidor utiliza sua cópia do certificado, com o sinalizador 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 96).

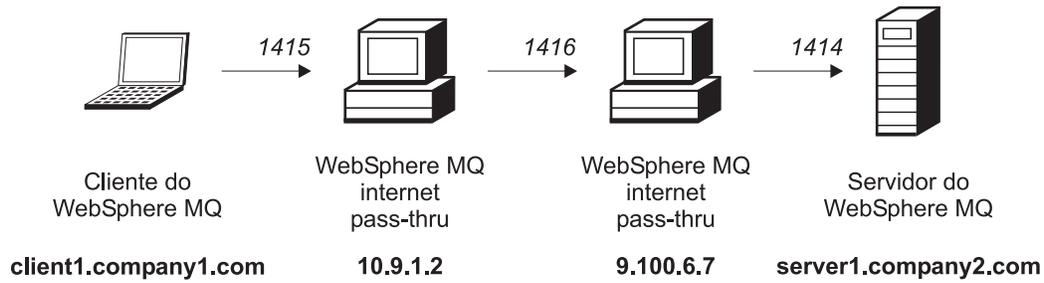


Figura 14. Diagrama de rede do cliente SSL

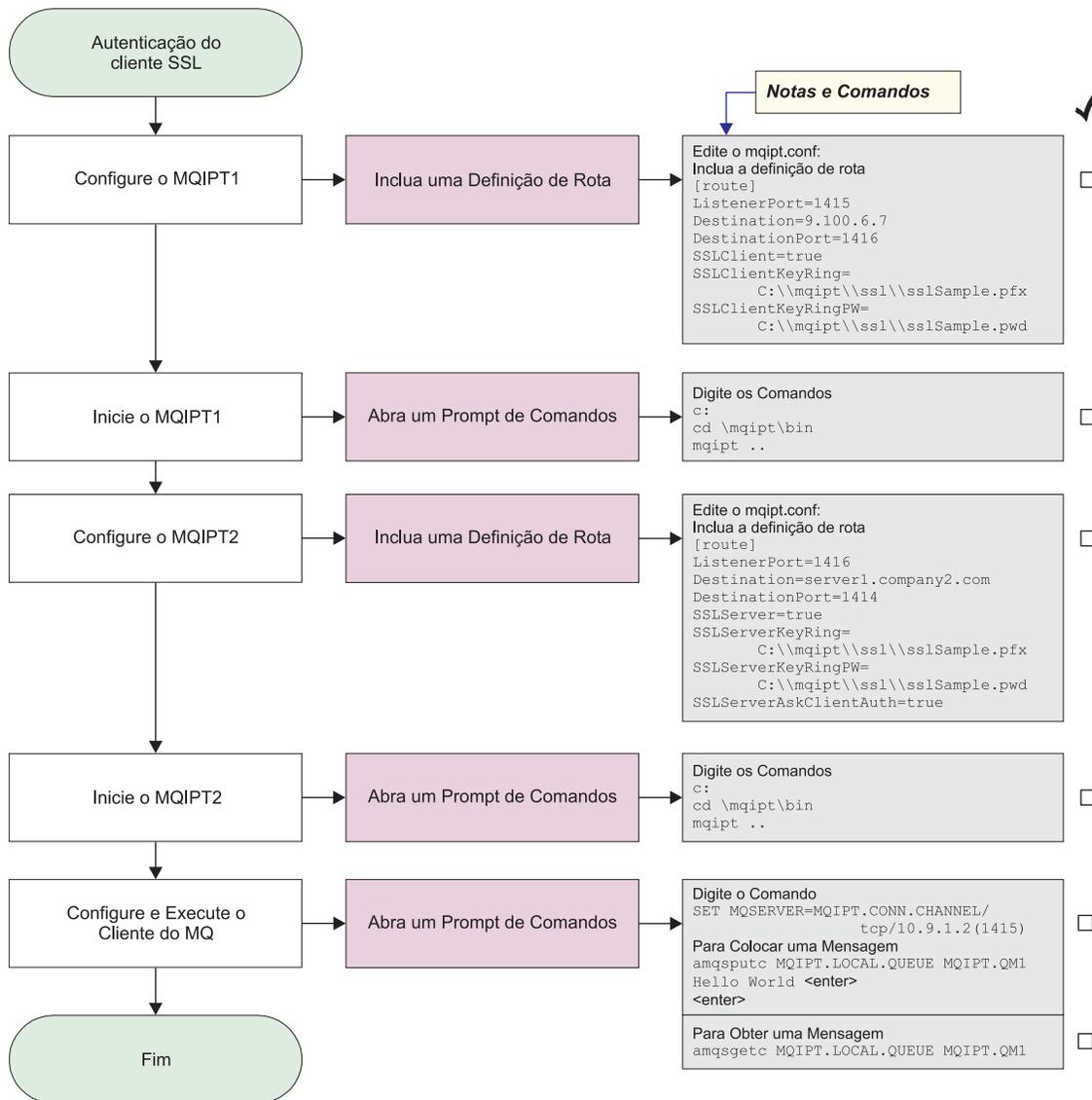


Figura 15. Autenticação do cliente SSL

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 Todos os Direitos Reservados
MQCPI001 WebSphere MQ internet pass-thru Versão 1.3.0 iniciando
MQCPI011 O caminho c:\mqipt\logs será usado p/ armazenar arquivos de log
MQCPI006 A rota 1415 iniciou e enviará mensagens para:
MQCPI034 ....9.100.6.7(1416)
MQCPI035 ....utilizando protocolos MQ
MQCPI036 ....Lado do SSL ativado com as propriedades:
MQCPI031 .....conjunto de cifras <null>
MQCPI032 .....arquivo de conjunto de chaves c:\mqipt\sslSample.pfx
MQCPI047 .....arquivo de conjunto de chaves CA <null>
MQCPI038 .....nome(s) diferente(s) CN=* O=* OU=* L=* ST=* C=*
MQCPI078 Rota 1415 pronta para os pedidos de conexão
```

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 Todos os Direitos Reservados
MQCPI001 WebSphere MQ internet pass-thru Versão 1.3.0 iniciando
MQCPI011 O caminho c:\mqipt\logs será usado p/ armazenar arquivos de log
MQCPI006 A rota 1416 foi iniciada e enviará mensagens para:
MQCPI034 ....server1.company2.com(1414)
MQCPI035 ....utilizando protocolos MQ
MQCPI037 ....Lado do SSL ativado com as propriedades:
MQCPI031 .....conjunto de cifras <null>
MQCPI032 .....arquivo de conjunto de chaves c:\mqipt\sslSample.pfx
MQCPI047 .....arquivo de conjunto de chaves CA <null>
MQCPI038 .....nome(s) diferente(s) CN=* O=* OU=* L=* ST=* C=*
MQCPI033 .....autenticação do cliente definida como true
MQCPI078 Rota 1416 pronta para os pedidos de conexão
```

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:

- ProxyPersistence deve ser on, o que 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

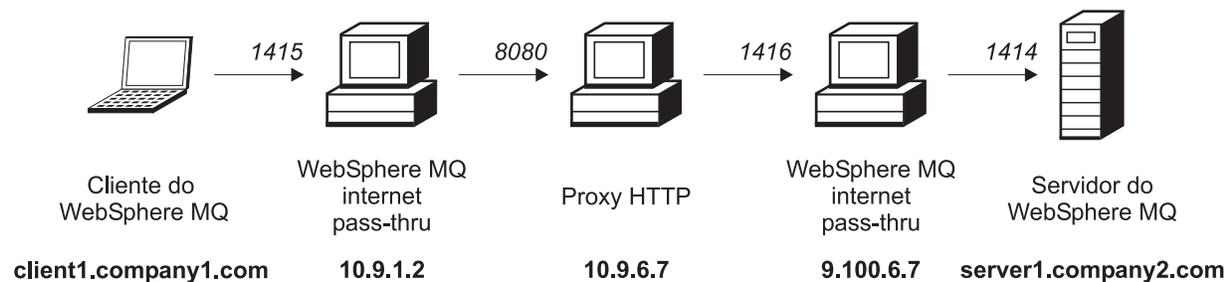


Figura 16. Diagrama de rede proxy HTTP

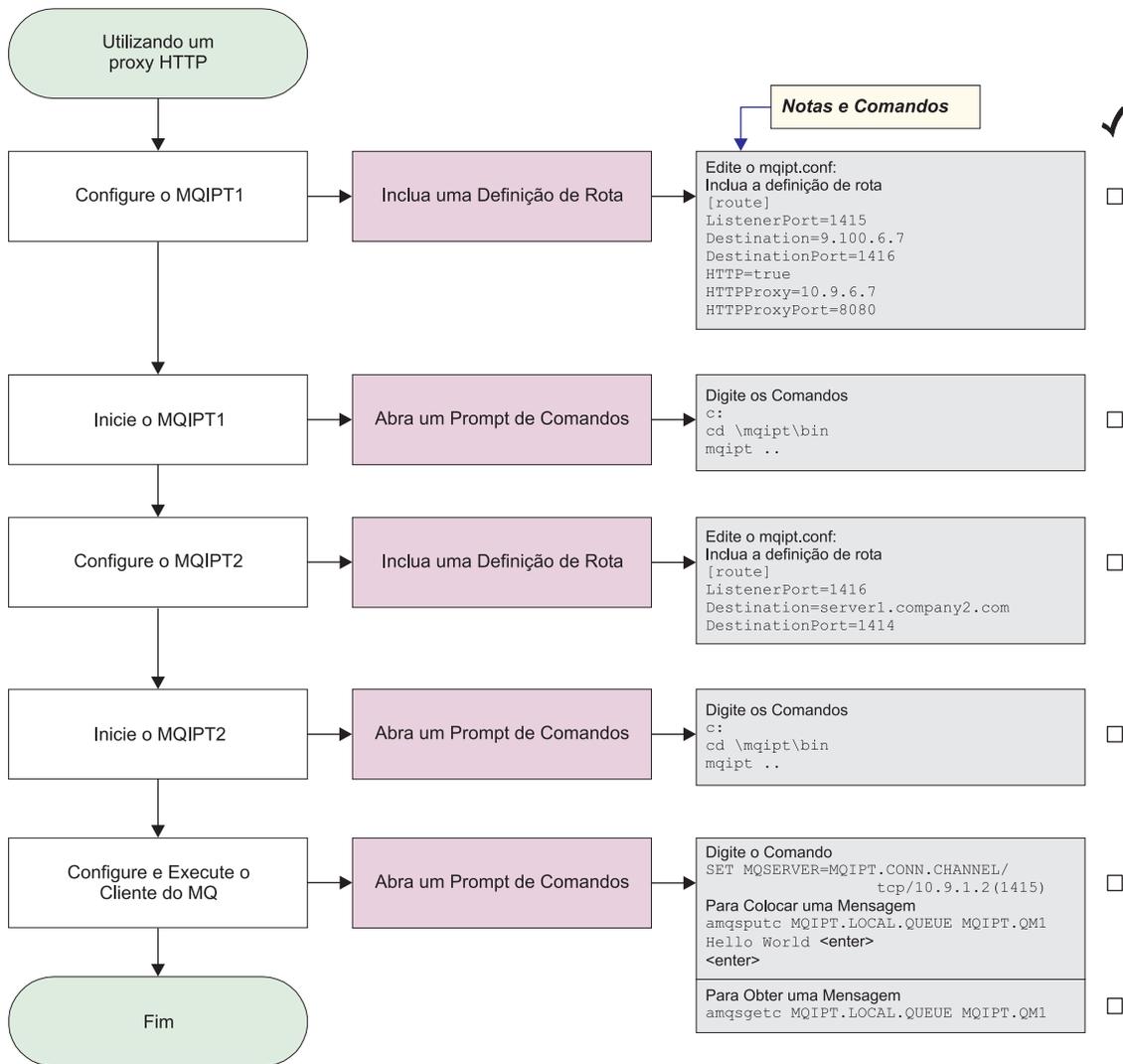


Figura 17. Configuração do proxy HTTP

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 Todos os Direitos Reservados
MQCPI001 WebSphere MQ internet pass-thru Versão 1.3.0 iniciando
MQCPI004 Lendo informações sobre configuração de C:\mqipt\mqipt.conf
MQCPI011 O caminho C:\mqipt\logs será usado p/ armazenar arquivos de log
```

```
MQCPI006 A rota 1415 iniciou e enviará mensagens para:
MQCPI034 ....9.100.6.7(1416)
MQCPI035 ....utilizando HTTP
MQCPI024 ....e proxy HTTP em 10.9.6.7(1080)
MQCPI078 Rota 1415 pronta para os pedidos de conexão
```

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 Todos os Direitos Reservados
MQCPI001 WebSphere MQ internet pass-thru Versão 1.3.0 iniciando
MQCPI004 Lendo informações sobre configuração de C:\mqipt\mqipt.conf
MQCPI011 O caminho C:\mqipt\logs será utilizado para armazenar arquivos de log
MQCPI006 A rota 1416 foi iniciada e enviará mensagens para:
MQCPI034 ....server1.company2.com(1414)
MQCPI035 ....utilizando protocolos MQ
MQCPI078 Rota 1416 pronta para os pedidos de conexão
```

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 somente conexões de clientes específicos, incluindo verificações de segurança no atendente de MQIPT, utilizando o Java Security Manager.

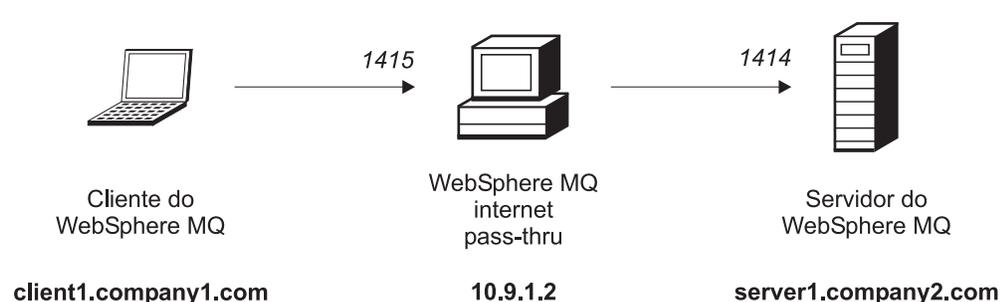


Figura 18. Diagrama de rede de controle de acesso

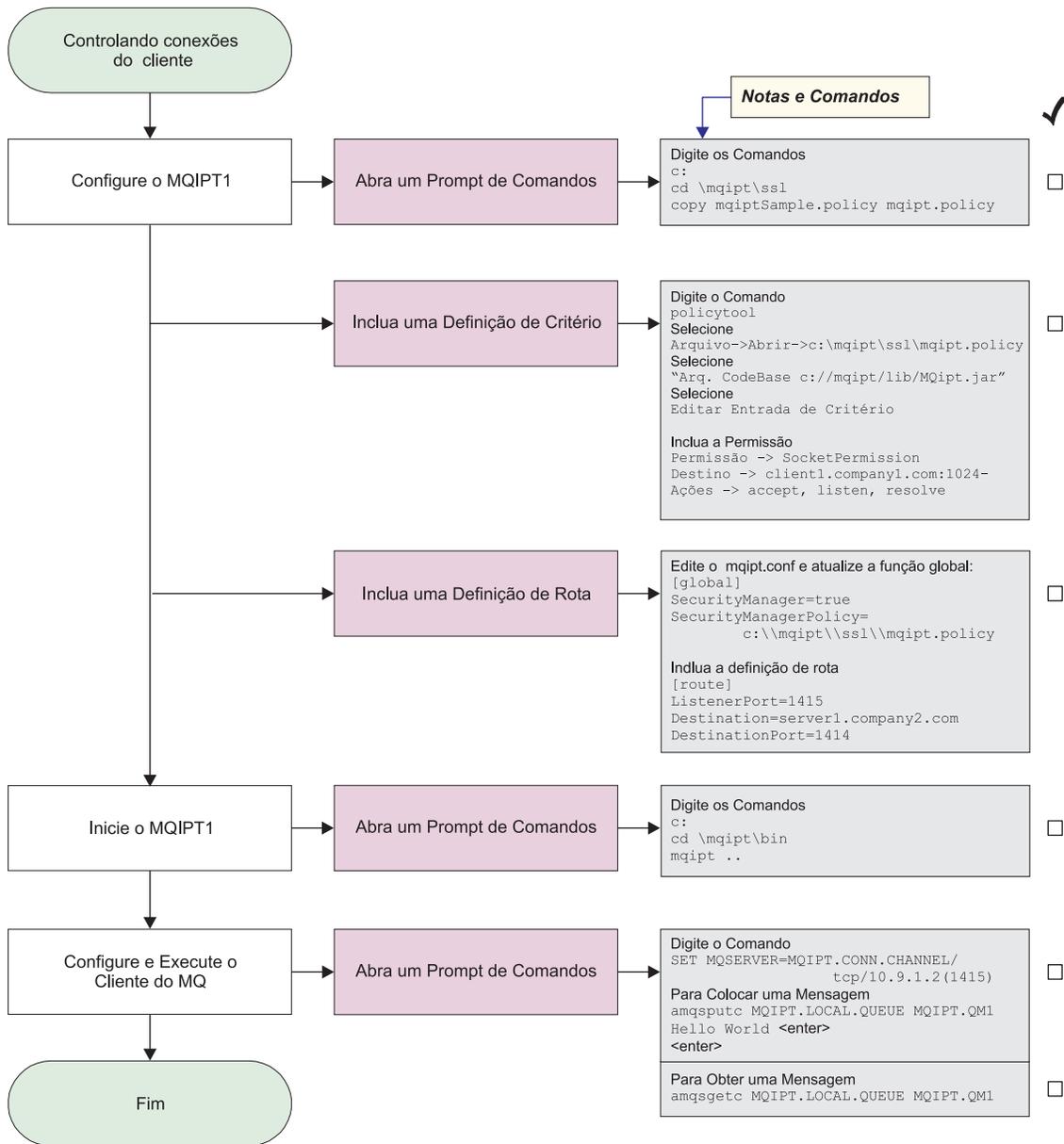


Figura 19. Configuração do controle de acesso

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) Selezione Arquivo -> Abrir -> c:\mqipt\ssl\mqipt.policy

2) Selezione:

```
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-
Actions=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 Todos os Direitos Reservados
MQCPI001 WebSphere MQ internet pass-thru Versão 1.3.0 iniciando
MQCPI004 Lendo informações sobre configuração de C:\\mqipt\\mqipt.conf
MQCPI055 Configurando o java.security.policy em c:\\mqipt\\mqipt.policy
MQCPI053 Iniciando o Java Security Manager
MQCPI011 O caminho C:\\mqipt\\logs será utilizado para armazenar arquivos de log
MQCPI006 A rota 1415 iniciou e enviará mensagens para:
MQCPI034 ....server1.company2.com(1414)
MQCPI035 ....utilizando protocolos MQ
MQCPI078 Rota 1415 pronta para os pedidos de conexão
```

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, pressupõe-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 "médio" para todos os dados enviados do MQIPT para o cliente do WebSphere MQ e uma prioridade "bom" 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

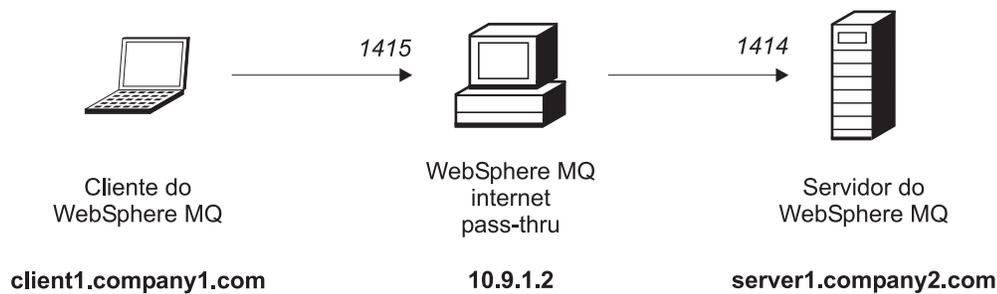


Figura 20. Diagrama de rede de QoS

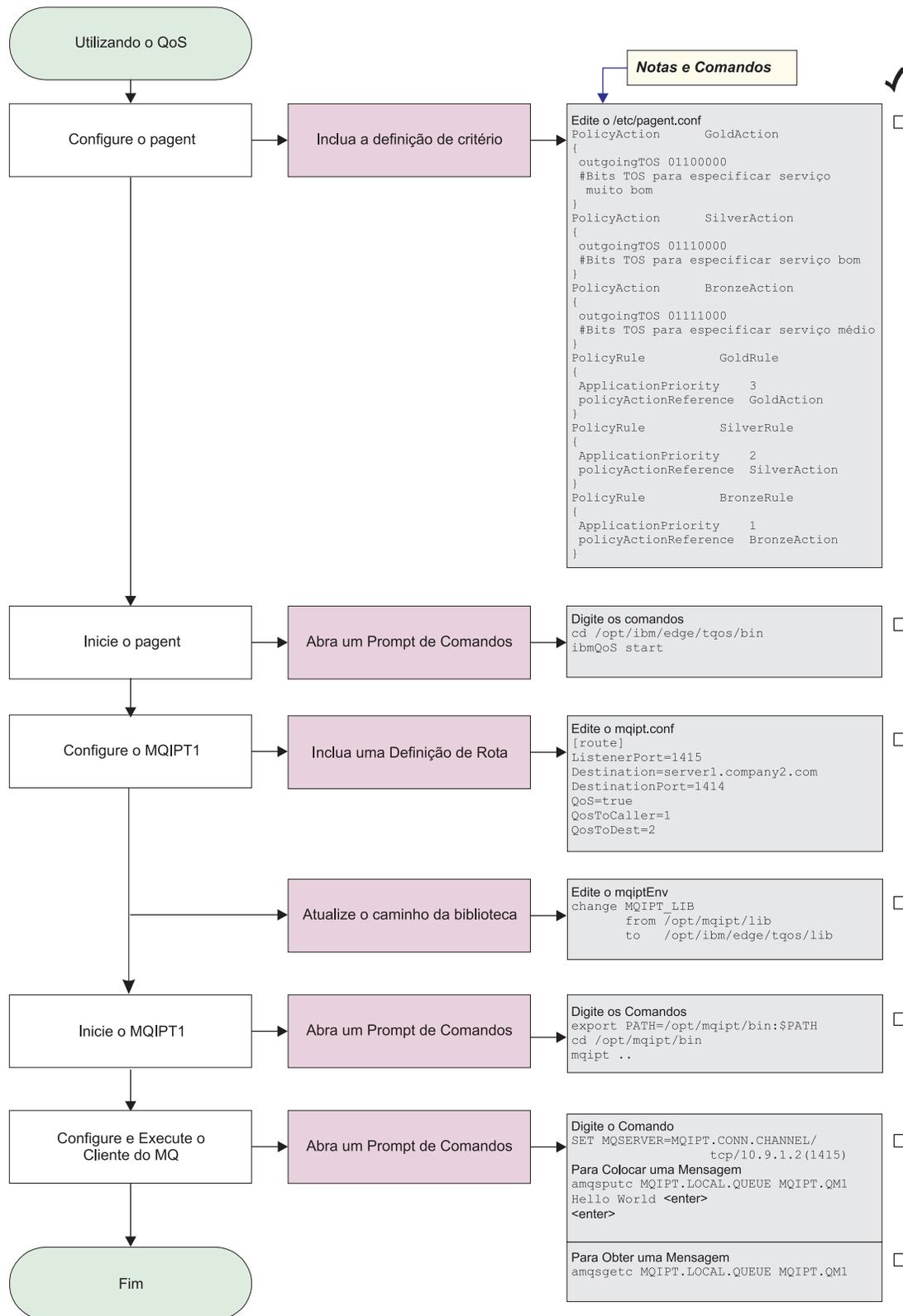


Figura 21. Configuração de QoS

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
}

```

Para ativar a coleta de dados de desempenho para as regras definidas anteriormente, utilize a instrução `PolicyPerformanceCollection` e ative-a. Consulte `Pagent.conf` para obter uma descrição e o formato dessa instrução.

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 Todos os Direitos Reservados
MQCPI001 Websphere MQ internet pass-thru Version 1.3.0 starting
MQCPI004 Lendo informações sobre configuração de /opt/mqipt/mqipt.conf
MQCPI011 O caminho /opt/mqipt/logs será usado p/ armazenar arquivos de log
MQCPI006 A rota 1415 iniciou e enviará mensagens para:
MQCPI034 ....server1.company2.com(1414)
MQCPI035 ....utilizando protocolos MQ
MQCPI049 ....QoS prioridade p/ destino = 2, p/ o responsável pela chamada = 1
MQCPI078 Rota 1415 pronta para os pedidos de conexão

```

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

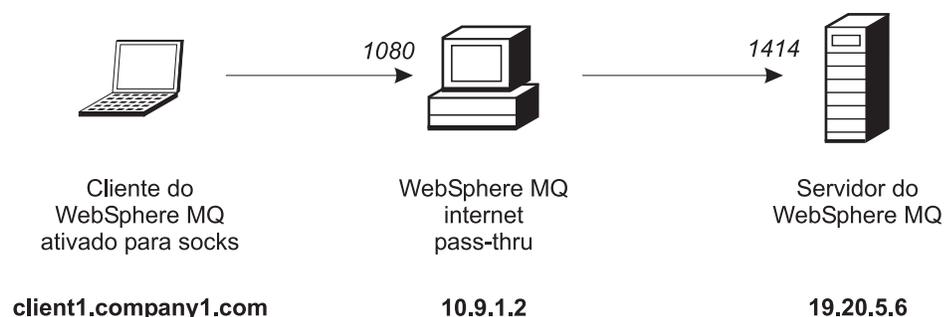


Figura 22. Diagrama de rede do proxy SOCKS

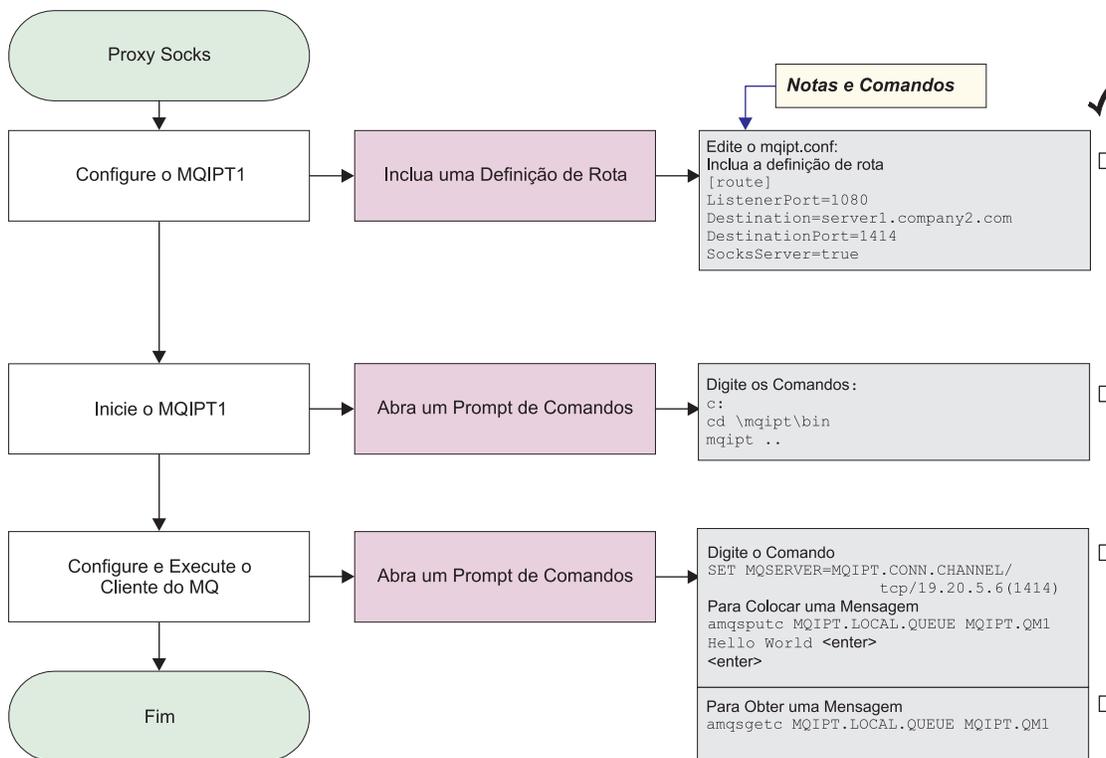


Figura 23. Configuração do proxy SOCKS

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 Todos os Direitos Reservados
MQCPI001 WebSphere MQ internet pass-thru Versão 1.3.0 iniciando
MQCPI004 Lendo informações sobre configuração de C:\mqipt\mqipt.conf
MQCPI011 O caminho C:\mqipt\logs será utilizado para armazenar arquivos de log
MQCPI006 A rota 1080 foi iniciada e enviará mensagens para:
MQCPI034 ....server1.company2.com(1414)
MQCPI035 ...utilizando protocolos MQ
MQCPI052 ....Lado do Servidor Socks ativado
MQCPI078 Rota 1080 pronta para os pedidos de conexão
```

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>
```

- 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 111, exceto que o MQIPT faz uma conexão com socks ativado, em vez do cliente do WebSphere MQ.

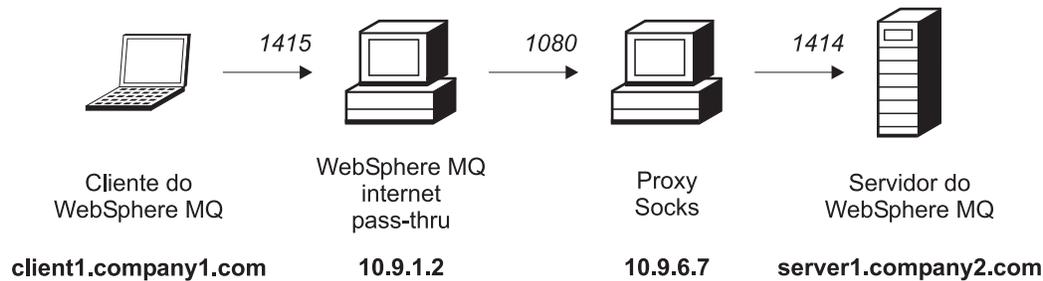


Figura 24. Diagrama de rede do cliente SOCKS

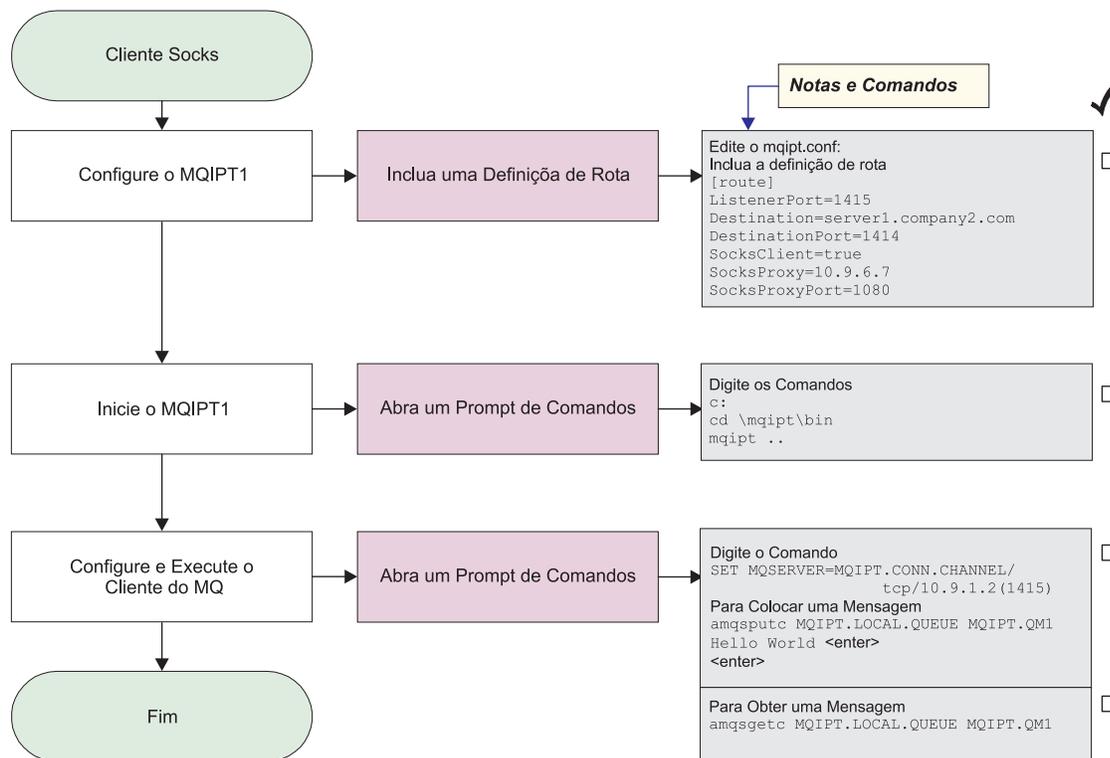


Figura 25. Configuração do cliente SOCKS

- 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 Todos os Direitos Reservados
MQCPI001 WebSphere MQ internet pass-thru Versão 1.3.0 iniciando
MQCPI004 Lendo informações sobre configuração de C:\mqipt\mqipt.conf
MQCPI022 A verificação de senha foi desativada na porta do comando
MQCPI011 O caminho C:\mqipt\logs será usado p/ armazenar arquivos de log
MQCPI006 A rota 1415 iniciou e enviará mensagens para:
MQCPI034 ....server1.company2.com(1414)
MQCPI035 ....utilizando protocolos MQ
MQCPI039 ....e o proxy Socks em 10.9.6.7(1080)
MQCPI078 Rota 1415 pronta para os pedidos de conexão
```

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".

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 sinalizador trust-as-peer ativado.

1. Inicie o KeyMan
2. Selecione "Criar novo..."
3. Selecione "Token PKCS#12"
4. Selecione "Ação -> Gerar Chave"
um novo par de chaves aparecerá na lista "RSA / 1024-bit"
5. Selecione o novo par de chaves
6. Selecione "Ação -> Criar Certificado"
7. Selecione "Certificado Auto-Assinado"
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 sinalizador trust-as-peer

13. Feche o diálogo. Selecione "Arquivo -> Salvar"
 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 "Formato de arquivo como PKCS#12 / PFX" - **não selecione** "Agrupar conjunto de chaves em uma classe Java"
 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 98.

Configurando o Servlet do MQIPT

Além da seção "Suposições" na página 95, este exemplo também faz as seguintes suposições:

- O Tomcat Application Server foi instalado no seguinte diretório:
 c:\jakarta-tomcat-4.0.1

Faça download do Tomcat do endereço:

<http://jakarta.apache.org/builds/jakarta-tomcat-4.0/release/v4.0.3/>

- O IBM Web Traffic Express foi instalado em:
 c:\wte

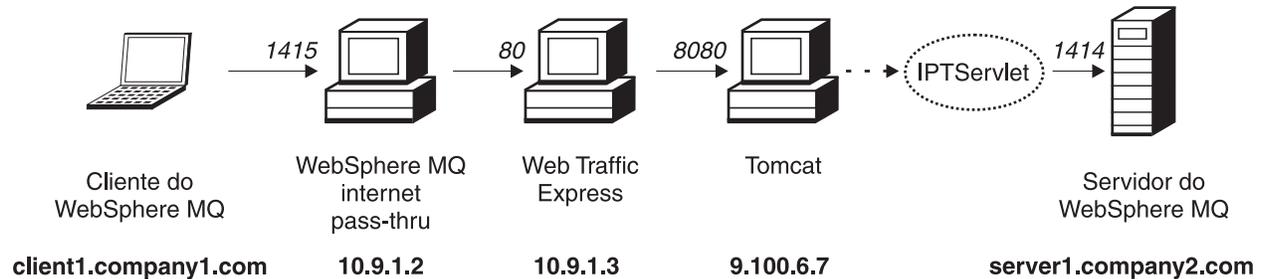


Figura 26. Diagrama de rede do servlet

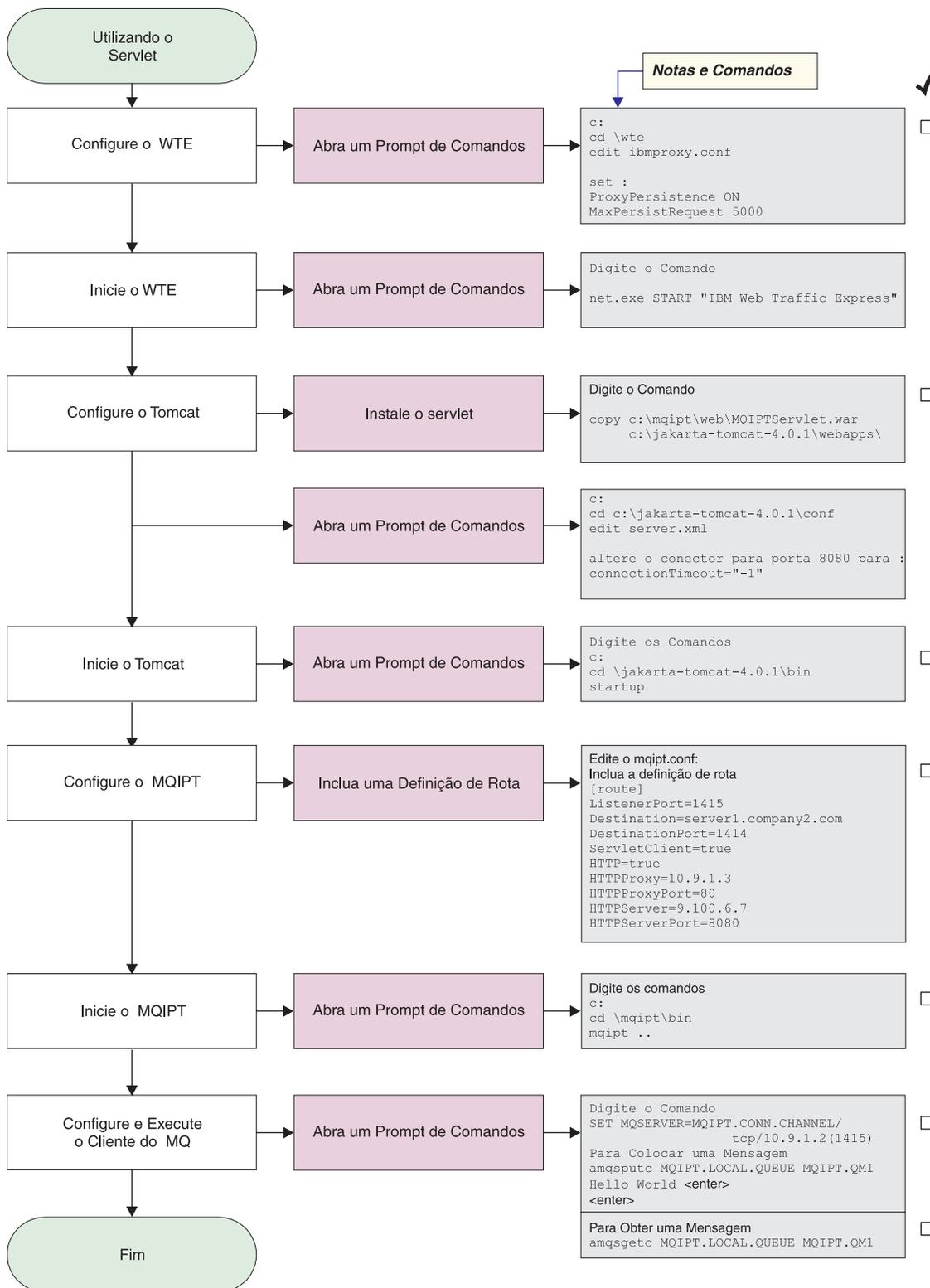


Figura 27. Configuração do servlet

1. Configure o Web Traffic Express
edite `c:\wte\ibmroxy.conf` e defina as seguintes propriedades:
ProxyPersistence ON
MaxPersistRequest 5000

2. Inicie o Web Traffic Express

Abra um prompt de comandos e digite o seguinte:

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

3. Configure o Tomcat

Para instalar o Servlet, copie:

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

para:

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

Edite c:\jakarta-tomcat-4.0.1\conf\server.xml, ative o conector da porta 8443 e defina a propriedade ConnectionTimeout como -1.

4. Inicie o Tomcat

Abra um prompt de comandos e digite o seguinte:

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

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

6. 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 Todos os Direitos Reservados  
MQCPI001 Websphere MQ internet pass-thru Version 1.3.0 starting  
MQCPI004 Lendo informações sobre configuração de C:\mqipt\mqipt.conf  
MQCPI011 O caminho C:\mqipt\logs será utilizado para armazenar arquivos de log  
MQCPI006 A rota 1415 iniciou e enviará mensagens para:  
MQCPI034 ....server1.company2.com(1414)  
MQCPI035 ....utilizando HTTP  
MQCPI024 ....e o proxy HTTP em 10.9.1.3(80)  
MQCPI066 ....e o servidor HTTP em 9.100.6.7(8080)  
MQCPI059 ....cliente servlet ativado  
MQCPI078 Rota 1415 pronta para os pedidos de conexão
```

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".

Configuração HTTPS

Além da seção "Suposições" na página 95, este exemplo também faz as seguintes suposições:

- O Tomcat Application Server foi instalado no seguinte diretório:
c:\jakarta-tomcat-4.0.1

Faça download do Tomcat do endereço:

<http://jakarta.apache.org/builds/jakarta-tomcat-4.0/release/v4.0.3/>

- O IBM Web Traffic Express foi instalado em:
c:\wte

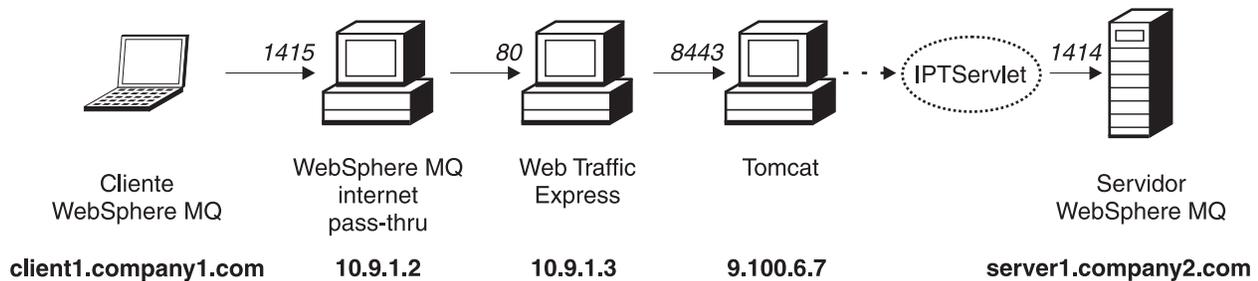


Figura 28. Diagrama de rede do HTTPS

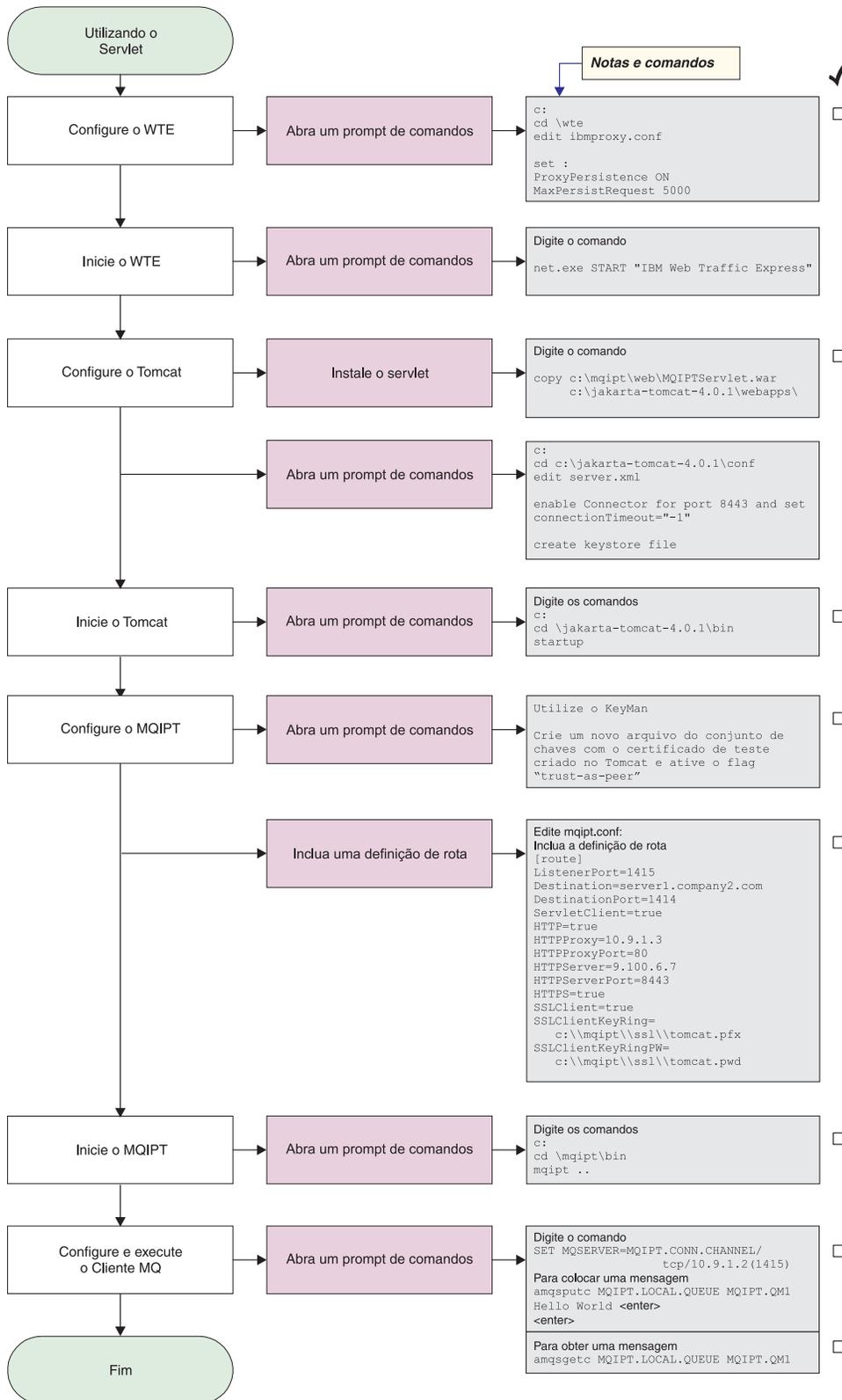


Figura 29. Configuração HTTPS

1. Configure o Web Traffic Express

Edite `c:\wte\ibmproxy.conf` e defina as seguintes propriedades:

```
ProxyPersistence ON
MaxPersistRequest 5000
```

2. Inicie o Web Traffic Express

Abra um prompt de comandos e digite o seguinte:

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

3. Configure o Tomcat

Para instalar o Servlet, copie:

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

para:

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

Edite `c:\jakarta-tomcat-4.0.1\conf\server.xml`, ative o conector da porta 8443 e defina a propriedade `ConnectionTimeout` como -1.

Utilize a documentação do Tomcat, disponível em:

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

e siga as instruções em "SSL Configuration HOW-TO" para ativar conexões SSL na porta 8443. Crie um arquivo do conjunto de chaves com um certificado de teste auto-assinado. Essa ação cria um arquivo denominado `C:\winnt\profiles\<userid>\.keystore`.

4. Inicie o Tomcat

Abra um prompt de comandos e digite o seguinte:

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

5. Copie o novo arquivo keystore da máquina do Tomcat para a máquina do MQIPT. Utilize KeyMan, abra o novo arquivo keystore (a senha padrão é `changeit`) e ative o sinalizador "trust-as-peer" (consulte a seção "Criando Certificados de Teste SSL" na página 114 para obter mais informações). Salve esse arquivo como `c:\mqipt\ssl\tomcat.pfx` e crie um arquivo de texto denominado `c:\mqipt\ssl\tomcat.pwd`, contendo a senha `changeit`.

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

7. Inicie 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 Todos os Direitos Reservados
MQCPI001 Websphere MQ internet pass-thru Version 1.3.0 starting
MQCPI004 Lendo informações sobre configuração de C:\mqipt\mqipt.conf
MQCPI011 O caminho C:\mqipt\logs será utilizado para armazenar arquivos de log
MQCPI006 A rota 1415 iniciou e enviará mensagens para:
MQCPI034 ....server1.company2.com(1414)
MQCPI035 ....utilizando HTTP
MQCPI024 ....e o proxy HTTP em 10.9.1.3(80)
MQCPI066 ....e o servidor HTTP em 9.100.6.7(8080)
MQCPI059 ....cliente servlet ativado
MQCPI036 ....Lado do SSL ativado com as propriedades:
MQCPI031 .....conjunto de cifras <null>
MQCPI032 .....arquivo de conjunto de chaves c:\mqipt\ssl\tomcat.pfx
MQCPI047 .....arquivo de conjunto de chaves CA <null>
MQCPI038 .....nome(s) diferente(s) CN=* O=* OU=* L=* ST=* C=*
MQCPI078 Rota 1415 pronta para os pedidos de conexão
```

8. 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)
```

9. Coloque uma mensagem utilizando:

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

10. 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 95, 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.

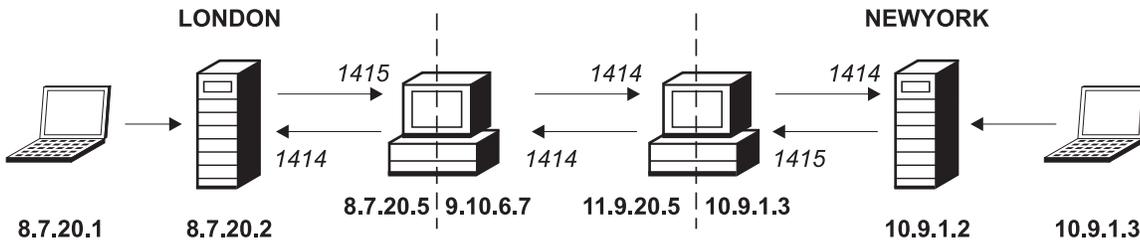


Figura 30. Diagrama de rede de clustering

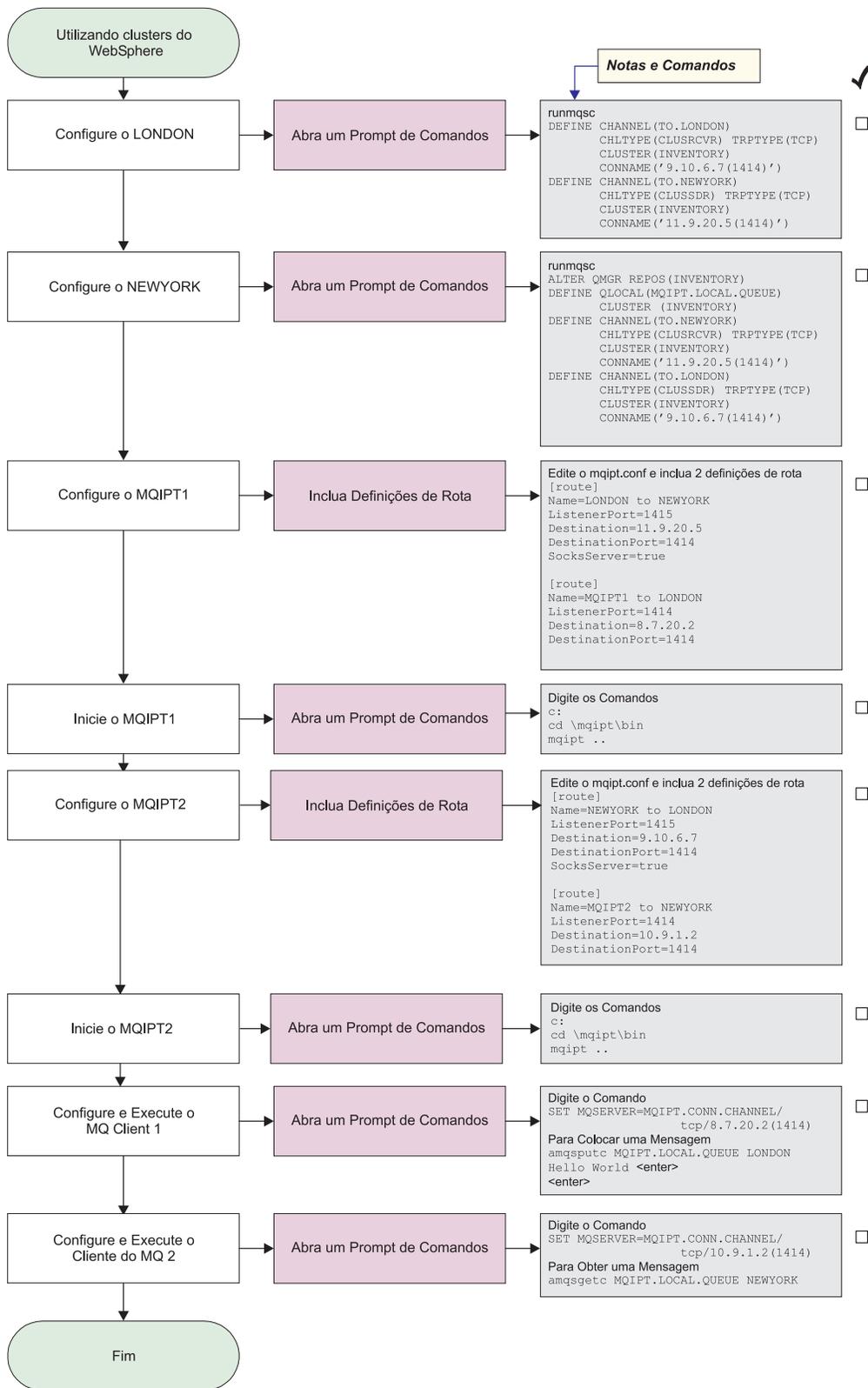


Figura 31. Configuração de clustering

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 Todos os Direitos Reservados
MQCPI001 WebSphere MQ internet pass-thru Versão 1.3.0 iniciando
MQCPI004 Lendo informações sobre configuração de C:\mqipt\mqipt.conf
MQCPI011 O caminho C:\mqipt\logs será usado p/ armazenar arquivos de log
MQCPI006 A rota 1415 iniciou e enviará mensagens para:
MQCPI034 ....11.9.20.5(1414)
MQCPI035 ...utilizando protocolos MQ
MQCPI052 ....Lado do Servidor Socks ativado
MQCPI078 Rota 1415 pronta para os pedidos de conexão
MQCPI006 A rota 1414 foi iniciada e enviará mensagens para:
MQCPI034 ....8.7.20.2(1414)
MQCPI035 ...utilizando protocolos MQ
MQCPI078 Rota 1414 pronta para os pedidos de conexão

```

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 Todos os Direitos Reservados
MQCPI001 WebSphere MQ internet pass-thru Versão 1.3.0 iniciando
MQCPI004 Lendo informações sobre configuração de C:\mqipt\mqipt.conf
MQCPI011 O caminho C:\mqipt\logs será utilizado para armazenar arquivos de log
MQCPI006 A rota 1415 iniciou e enviará mensagens para:
MQCPI034 ....9.10.6.7(1414)
MQCPI035 ....utilizando protocolos MQ
MQCPI052 ....Lado do Servidor Socks ativado
MQCPI078 Rota 1415 pronta para os pedidos de conexão
MQCPI006 A rota 1414 foi iniciada e enviará mensagens para:
MQCPI034 ....10.9.1.2(1414)
MQCPI035 ....utilizando protocolos MQ
MQCPI078 Rota 1414 pronta para os pedidos de conexão
```

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 pressupõe 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 "Criar novo..."

3. Selecione "Token PKCS#12"
4. Selecione "Ação -> Gerar Chave"
Um novo par de chaves aparecerá na lista "RSA / 1024-bit"
5. Selecione o novo par de chaves
6. Selecione "Ação -> Solicitar Certificado"
Siga as instruções on-line
7. Selecione "Arquivo -> Salvar"
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 "Formato de arquivo como PKCS#12 / PFX" - **não selecione**
"Agrupar conjunto de chaves em uma classe Java"
11. Selecione "Arquivo -> Sair"
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 "Abrir existente...".
3. Selecione "Recurso Local"
4. Selecione "Abrir um arquivo..."
5. Digite o nome do arquivo de certificado pessoal
Por exemplo, c:\mqipt\ssl\myServer.pfx
6. Digite a frase-chave
7. Selecione "Arquivo -> Importar"
8. Selecione "Recurso Local"
9. Selecione "Abrir um arquivo..."
10. Digite server.cer
Aparecerá um diálogo explicando que o certificado privado será unido à
chave privada
11. Selecione "Arquivo -> Salvar"
12. Selecione "Arquivo -> Sair"

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 98 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 o servidor, consulte o exemplo em “Autenticação do Cliente SSL” na página 100 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

```

Alocando Endereços de Porta

Este exemplo mostra como controlar os endereços de porta local utilizando-os ao fazer conexões de saída. Neste exemplo, supomos que você tenha instalado o MQIPT em uma máquina com várias hospedagens.

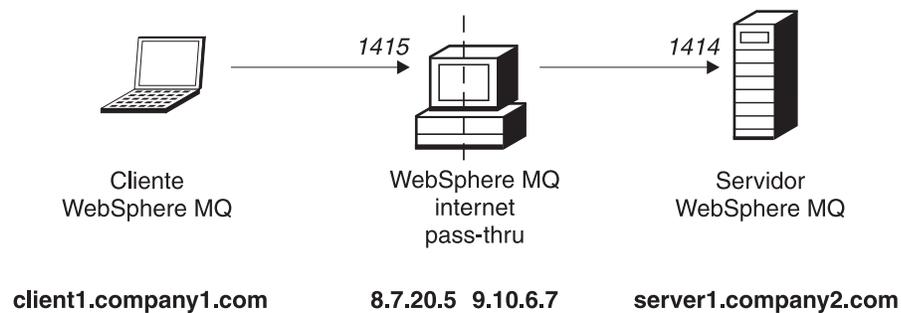


Figura 32. Diagrama de rede de alocação de portas

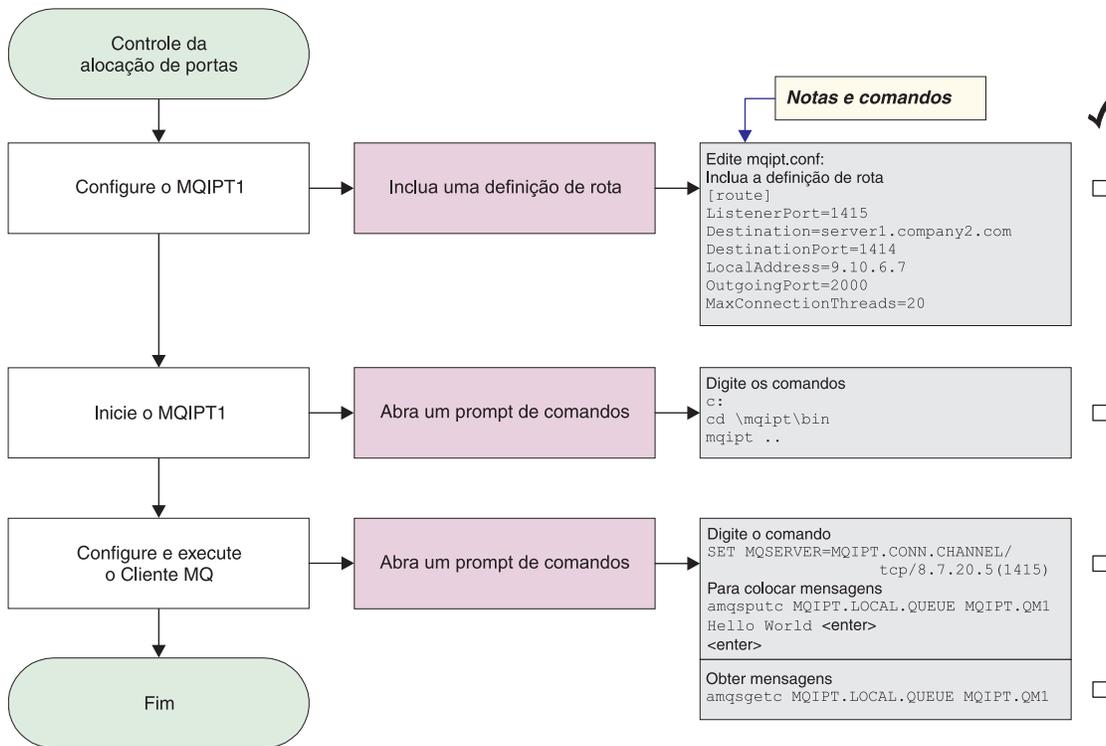


Figura 33. Configuração da alocação de portas

1. Configure o MQIPT1

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

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

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 Todos os Direitos Reservados
MQCPI001 WebSphere MQ internet pass-thru Versão 1.3.0 iniciando
MQCPI004 Lendo informações sobre configuração de C:\mqipt\mqipt.conf
MQCPI011 O caminho C:\mqipt\logs será utilizado para armazenar arquivos de log
MQCPI006 A rota 1415 iniciou e enviará mensagens para:
MQCPI034 ...server1.company2.com(1414)
MQCPI035 ...utilizando protocolos MQ
MQCPI069 ...ligação para o endereço local 9.10.6.7
MQCPI070 ...utilizando a faixa de endereços da porta local 2000-2019
MQCPI078 Rota 1415 pronta para os pedidos de conexão
```

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

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

Utilizando um Servidor LDAP

Este exemplo mostra como configurar o MQIPT para utilizar um servidor LDAP para recuperar CRLs. Não é intenção deste exemplo explicar como instalar e configurar um servidor LDAP ou como criar um arquivo do conjunto de chaves contendo certificados pessoais ou confiáveis. Ele supõe que o servidor LDAP esteja disponível a partir de uma Autoridade de Certificação (CA) conhecida e confiável. Um servidor LDAP de backup não está sendo utilizado, mas poderia facilmente ser implementado, incluindo as propriedades de Rota apropriadas.

Para este exemplo, fazemos as seguintes suposições:

- O IPT2 tem um certificado pessoal, emitido pela CA confiável, armazenado em um arquivo do conjunto de chaves denominado myCert.pfx e a senha criptografada utilizada para abrir o arquivo do conjunto de chaves está armazenada no arquivo myCert.pwd.
- O IPT1 tem uma cópia do certificado da CA confiável, que será utilizada para autenticar o certificado enviado pelo IPT2. Esse certificado está armazenado em um arquivo do conjunto de chaves denominado caCerts.pfx e a senha criptografada utilizada para abrir o arquivo do conjunto de chaves está armazenada no arquivo caCerts.pwd.
- Os arquivos de senha criptografada foram criados utilizando o script mqiptPW.

A execução desta amostra permite que o cliente WMQ conecte-se ao Gerenciador de Filas (QM) e coloque uma mensagem do WMQ na fila de destino. A execução de um rastreamento do MQIPT em IPT1 mostra que o servidor LDAP está sendo utilizado, mas para demonstrar como CRLs funcionam, o certificado pessoal utilizado pelo IPT2 deve ser revogado pela CA confiável. Em seguida, neste caso, o cliente WMQ não poderá conectar-se ao QM, uma vez que a conexão entre IPT1 e IPT2 será rejeitada.

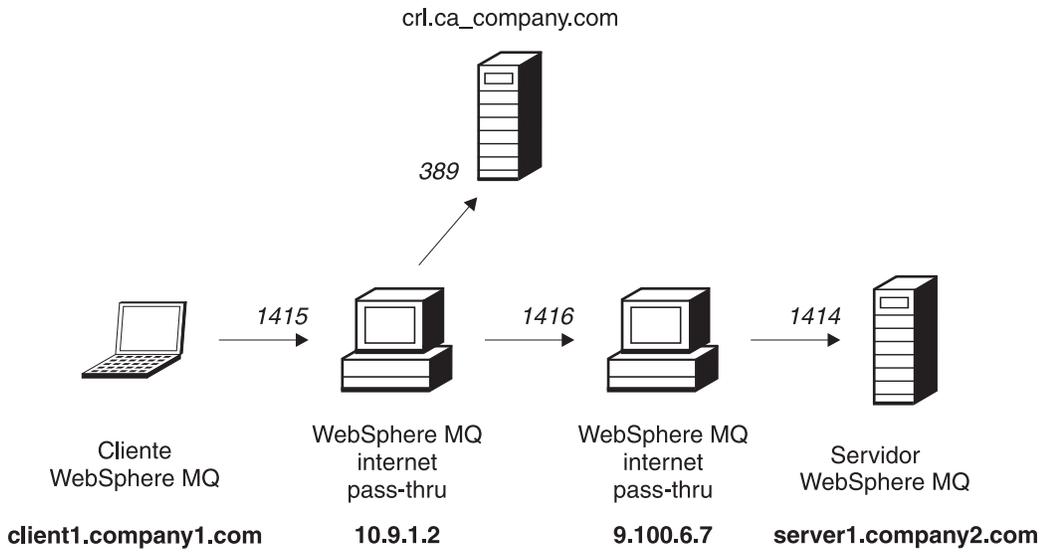


Figura 34. Diagrama de rede do servidor LDAP

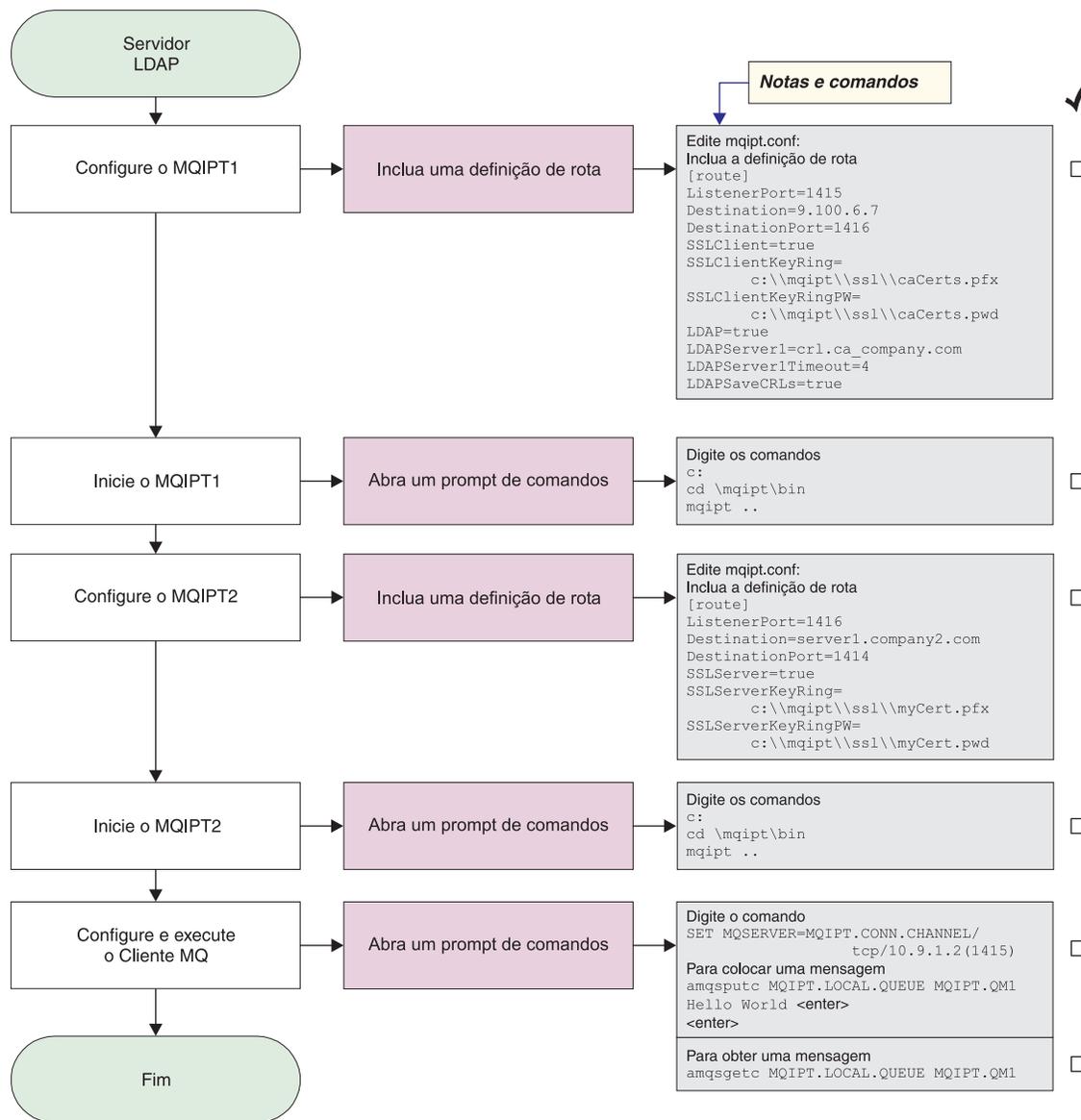


Figura 35. configuração do servidor LDAP

1. No IPT1

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\ssl\caCerts.pfx
SSLClientKeyRingPW=c:\mqipt\ssl\caCerts.pwd
LDAP=true
LDAPServer1=cr1.ca_company.com
LDAPServer1Timeout=4
LDAPSaveCRLs=true
  
```

Abra um prompt de comandos:

```

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

A seguinte mensagem indica uma conclusão bem-sucedida:

```
5639-L92 (C) Copyright IBM Corp. 2000 Todos os Direitos Reservados
MQCPI001 Websphere MQ internet pass-thru Version 1.3.0 starting
MQCPI004 Lendo informações sobre configuração de C:\mqipt\mqipt.conf
MQCPI011 O caminho C:\mqipt\logs será utilizado para armazenar arquivos de log
MQCPI006 A rota 1415 iniciou e enviará mensagens para:
MQCPI034 ....9.100.6.7(1416)
MQCPI035 ...utilizando protocolos MQ
MQCPI036 ....Lado do SSL ativado com as propriedades:
MQCPI031 .....conjunto de cifras <NULL>
MQCPI032 .....arquivo de conjunto de chaves <NULL>
MQCPI047 .....arquivo de conjunto de chaves CA c:\mqipt\ssl\caCerts.pfx
MQCPI071 .....certificado do site utiliza CN=* O=* OU=* L=* ST=* C=*
MQCPI038 .....certificado do peer utiliza CN=* O=* OU=* L=* ST=* C=*
MQCPI075 ....principal servidor LDAP em crl.ca_company.com(389)
MQCPI086 .....tempo limite de 4 segundo(s)
MQCPI084 ....o tempo limite de expiração do cache CRL é de 1 hora
MQCPI085 ....os CRLs serão salvos no(s) arquivo(s) de conjunto de chaves
MQCPI078 Rota 1415 pronta para os pedidos de conexão
```

2. No IPT2

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

Abra um prompt de comandos:

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

A seguinte mensagem indica uma conclusão bem-sucedida:

```
5639-L92 (C) Copyright IBM Corp. 2000 Todos os Direitos Reservados
MQCPI001 IBM WebSphere MQ internet pass-thru Version 1.3.0 starting
MQCPI004 Lendo informações sobre configuração de C:\mqipt\mqipt.conf
MQCPI011 O caminho C:\mqipt\logs será utilizado para armazenar arquivos de log
MQCPI006 A rota 1416 está iniciando e enviará mensagens para:
MQCPI034 ....server1.company2.com(1414)
MQCPI035 ...utilizando protocolos MQ
MQCPI037 ....Lado do SSL ativado com as propriedades:
MQCPI031 .....conjunto de cifras <NULL>
MQCPI032 .....arquivo de conjunto de chaves c:\mqipt\ssl\myCert.pfx
MQCPI047 .....arquivo de conjunto de chaves CA <NULL>
MQCPI071 .....certificado do site utiliza CN=* O=* OU=* L=* ST=* C=*
MQCPI038 .....certificado do peer utiliza CN=* O=* OU=* L=* ST=* C=*
MQCPI033 .....autenticação do cliente definida como false
MQCPI078 Rota 1416 pronta para os pedidos de conexão
```

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 MQIPT.QM1
Hello world <enter>
<enter>
```

5. Obtenha a mensagem utilizando:

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

Você verá "Hello world".

Modo de Proxy SSL

Este exemplo mostra como executar o MQIPT no modo proxy do SSL para que ele aceite um pedido de conexão SSL de um cliente SSL e crie um túnel dessa conexão para um servidor SSL. Supõe-se que o cliente e o servidor WMQ sejam da V5.3 e tenham sido configurados para utilizar uma conexão SSL.

Para obter mais informações sobre como configurar SSL para o WMQ, consulte "WebSphere MQ Security Version 5.3" SC34-6079-01.

Neste exemplo, fazemos a seguinte suposição:

- O MQClient e o QM foram configurados para utilizar o canal SSL.

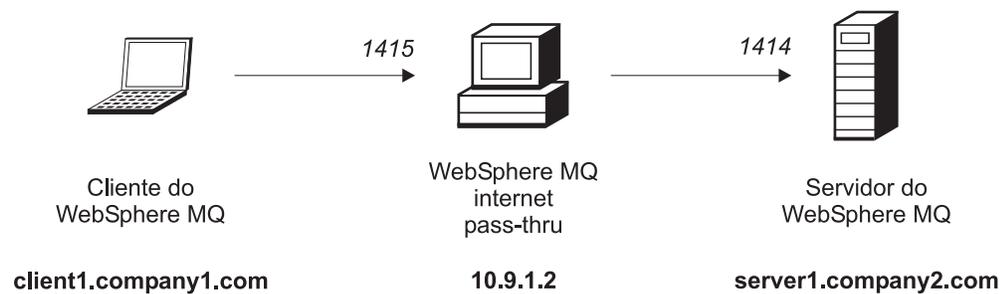


Figura 36. Diagrama de rede do servidor LDAP

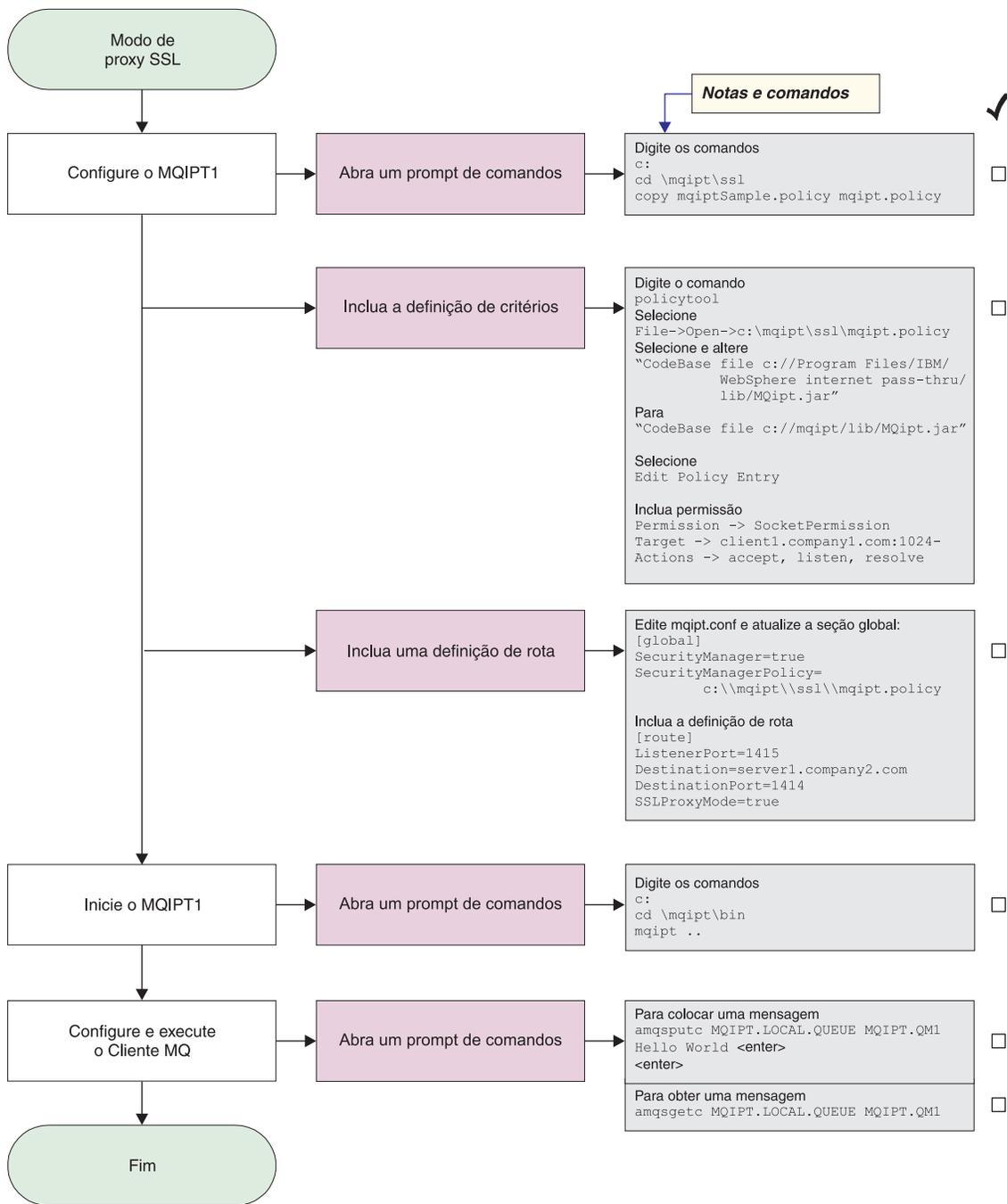


Figura 37. Configuração do modo de proxy SSL

1. No IPT1
 - a. Abra um prompt de comandos e digite o seguinte:
 - 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-"
Actions = "accept, listen, resolve"
```
2. Edite mqipt.conf e inclua as duas propriedades a seguir na seção global e uma definição de rota:


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


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

A seguinte mensagem indica uma conclusão bem-sucedida:

```
5639-L92 (C) Copyright IBM Corp. 2000 Todos os Direitos Reservados
MQCPI001 Websphere MQ internet pass-thru Version 1.3.0 starting
MQCPI004 Lendo informações sobre configuração de C:\\mqipt\\mqipt.conf
MQCPI011 O caminho C:\\mqipt\\logs será utilizado para armazenar arquivos de log
MQCPI006 A rota 1415 iniciou e enviará mensagens para:
MQCPI034 ....server1.company2.com(1414)
MQCPI035 ....utilizando SSLProxyMode
MQCPI078 Rota 1415 pronta para os pedidos de conexão
```

4. Coloque uma mensagem utilizando:


```
amqsputc MQIPT.LOCAL.QUEUE MQIPT.QM1
Hello world <enter>
<enter>
```
5. Obtenha a mensagem utilizando:


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

Você verá "Hello world".

Regravação Apache

Para este exemplo, fazemos as seguintes suposições:

- O servidor HTTP Apache foi instalado em c:\apache
- O IBM Web Traffic Express foi instalado em c:\wte

O exemplo mostra como utilizar a diretriz de regravação para converter um pedido HTTP em um redirecionamento de proxy Apache interno. Os módulos de proxy e de regravação devem ser carregados, mas, na verdade, o Apache não está funcionando no modo de proxy. Todas as diretrizes de proxy podem permanecer comentadas.

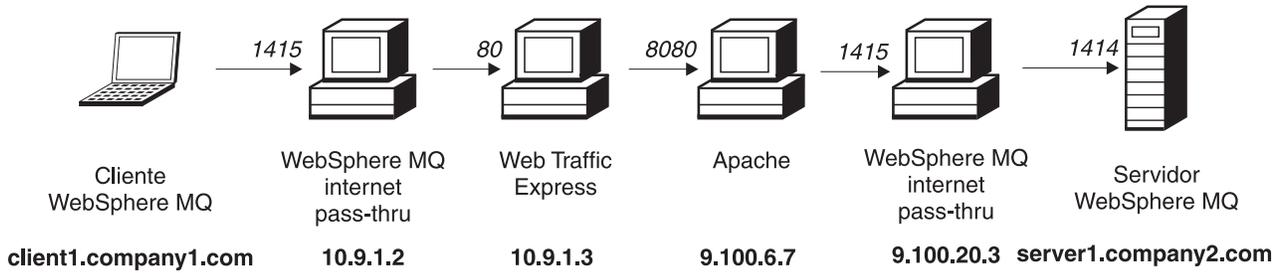


Figura 38. Diagrama de rede de regravação Apache

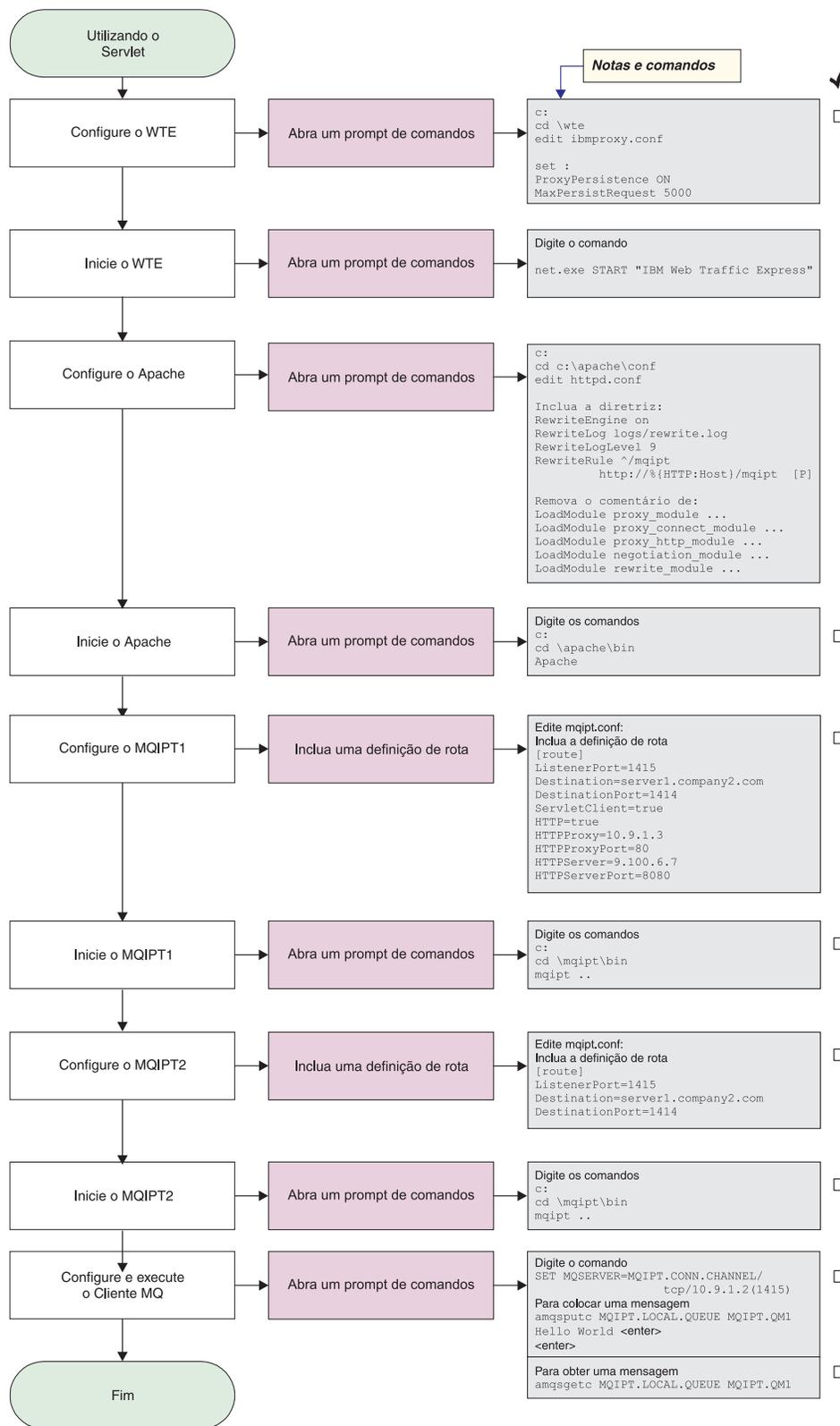


Figura 39. Configuração da gravação Apache

- No WTE
edite `c:\wte\ibmroxy.conf`

Altere as seguintes propriedades:

```
ProxyPersistence ON  
MaxPersistRequest 5000
```

2. No Apache

edite c:\apache\conf\httpd.conf

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

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

start Apache

3. No IPT1

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

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

Abra um prompt de comandos:

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

A seguinte mensagem indica uma conclusão bem-sucedida:

```
5639-L92 (C) Copyright IBM Corp. 2000 Todos os Direitos Reservados  
MQCPI001 Websphere MQ internet pass-thru Version 1.3.0 starting  
MQCPI004 Lendo informações sobre configuração de C:\mqipt\mqipt.conf  
MQCPI011 O caminho C:\mqipt\logs será utilizado para armazenar arquivos de log  
MQCPI006 A rota 1415 iniciou e enviará mensagens para:  
MQCPI034 ....server1.company2.com(1414)  
MQCPI035 ....utilizando HTTP  
MQCPI024 ....e o proxy HTTP em 10.9.1.3(80)  
MQCPI066 ....e o servidor HTTP em 9.100.6.7(8080)  
MQCPI078 Rota 1415 pronta para os pedidos de conexão
```

4. No IPT2

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

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

Abra um prompt de comandos:

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

A seguinte mensagem indica uma conclusão bem-sucedida:

```
5639-L92 (C) Copyright IBM Corp. 2000 Todos os Direitos Reservados
MQCPI001 Websphere MQ internet pass-thru Version 1.3.0 starting
MQCPI004 Lendo informações sobre configuração de C:\mqipt\mqipt.conf
MQCPI011 O caminho C:\mqipt\logs será utilizado para armazenar arquivos de log
MQCPI006 A rota 1415 iniciou e enviará mensagens para:
MQCPI034 ....server1.company2.com(1414)
MQCPI035 ....utilizando protocolos MQ
MQCPI078 Rota 1415 pronta para os pedidos de conexão
```

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 MQIPT.QM1
Hello world <enter>
<enter>
```

7. Obtenha a mensagem utilizando:

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

Você verá "Hello world".

Saída de Segurança

Para este exemplo, fazemos as seguintes suposições:

- Java 1.4 SDK instalado
- O subdiretório Java foi adicionado à variável de ambiente PATH

Este é um teste simples para mostrar como utilizar a saída de segurança de amostra fornecida, denominada SampleSecurityExit. Esta saída de segurança foi escrita para permitir apenas as conexões de cliente cujo nome de canal comece com os caracteres "MQIPT."

Utilizando o nome de canal sugerido "MQIPT.CONN.CHANNEL" (como utilizado na maioria destas amostras), a conexão do cliente poderá ser concluída e uma mensagem WMQ poderá ser colocada na fila.

Para provar que a saída de segurança está funcionando conforme esperado, defina outro canal srvconn com um nome que não comece com os caracteres "MQIPT.", por exemplo, "TEST.CONN.CHANNEL" e tente o comando amqsputc novamente, mas alterando a variável de ambiente MQSERVER para utilizar o novo nome de canal. Desta vez, a conexão será recusada e será fornecido um erro 2059.

Para mostrar que "TEST.CONN.CHANNEL" está funcionando sem utilizar a saída de segurança, defina a variável de ambiente MQSERVER para que indique diretamente a porta do atendente do WMQ (por exemplo, 1414) para que MQIPT não seja utilizado. Desta vez, o comando amqsputc funcionará conforme esperado.

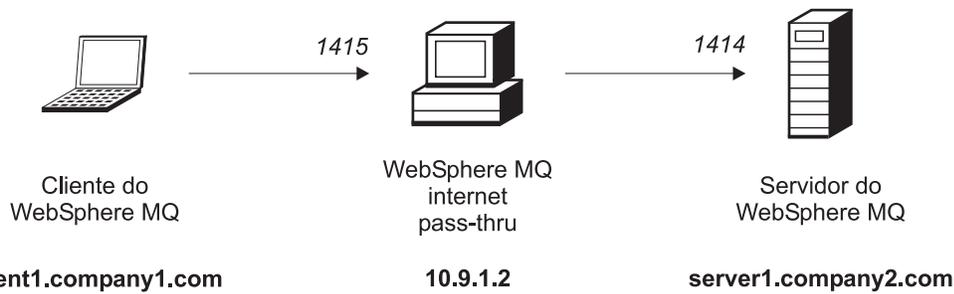


Figura 40. Diagrama de rede da saída de segurança

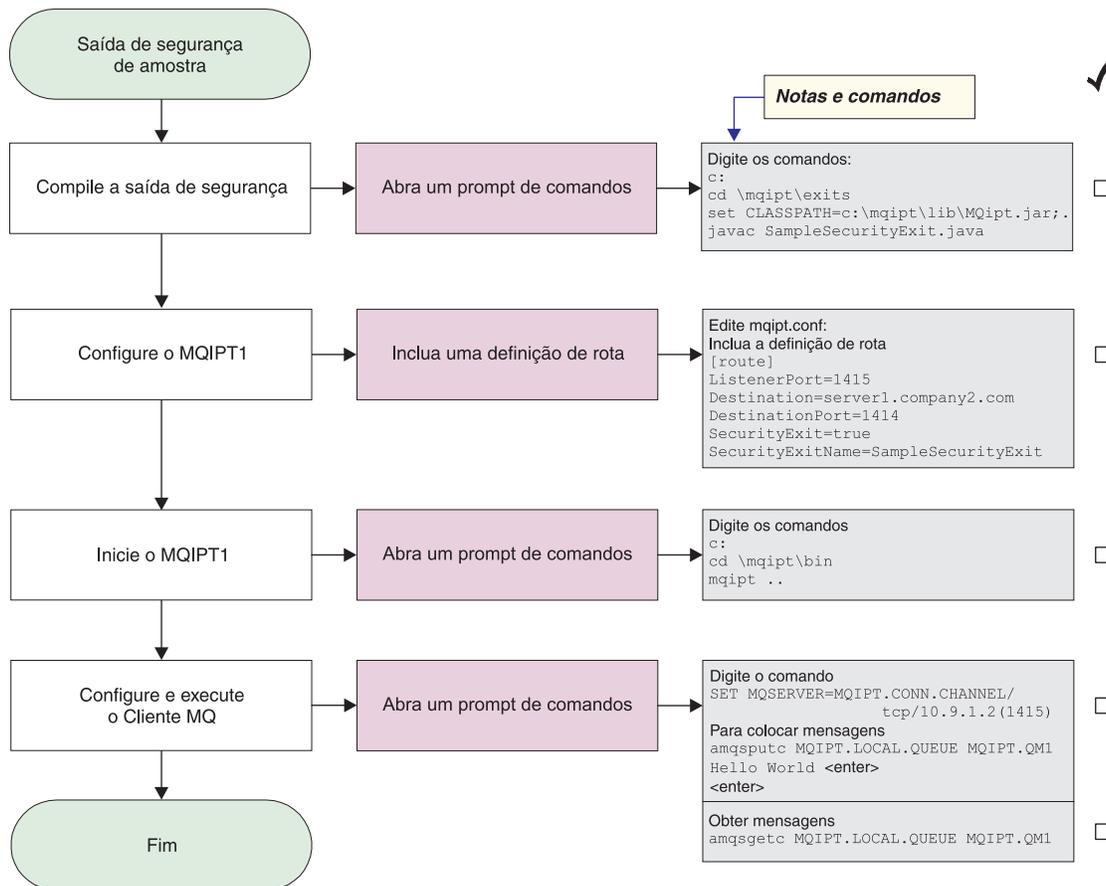


Figura 41. Configuração da saída de segurança

1. No IPT1

Abra um prompt de comandos:

```

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

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

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

Abra um prompt de comandos:

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

A seguinte mensagem indica uma conclusão bem-sucedida:

```
5639-L92 (C) Copyright IBM Corp. 2000 Todos os Direitos Reservados
MQCPI001 Websphere MQ internet pass-thru Version 1.3.0 starting
MQCPI004 Lendo informações sobre configuração de c:\mqipt\mqipt.conf
MQCPI011 O caminho c:\mqipt\logs será usado p/ armazenar arquivos de log
MQCPI006 A rota 1415 iniciou e enviará mensagens para:
MQCPI034 ....server1.company2.com(1414)
MQCPI035 ....utilizando protocolos MQ
MQCPI079 ....utilizando saída de segurança c:\mqipt\exits\SampleSecurityExit
MQCPI080 .....e tempo limite de 5 segundos
MQCPI078 Rota 1415 pronta para os pedidos de conexão
```

2. 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)
```

3. Coloque uma mensagem utilizando:

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

4. Obtenha a mensagem utilizando:

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

Você verá "Hello world".

Saída de Segurança de Roteamento

Para este exemplo, fazemos as seguintes suposições:

- Java 1.4 SDK instalado
- O subdiretório Java foi adicionado à variável de ambiente PATH
- Três gerenciadores de fila idênticos foram criados em três servidores separados

Este é um exemplo que roteia dinamicamente os pedidos de conexão do cliente, na forma de programador de rodízio para um grupo de servidores do Gerenciador de Filas do WMQ. O Gerenciador de Filas em cada servidor do grupo deve ser uma imagem espelhada de cada um dos outros.

A lista de nomes de servidores será lida a partir de um arquivo de configuração. O nome e a localização do arquivo de configuração são definidos com as propriedades SecurityExitName e SecurityExitPath. O arquivo de configuração de amostra, denominado SampleRoutingExit.conf, contém as entradas:

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

É necessário alterar esses nomes de servidores de acordo com seu ambiente.

Na primeira vez que o comando `amqsputc` for emitido, a mensagem do WMQ será colocada em `MQIPT.LOCAL.QUEUE` no QM no `server1`. Na segunda vez, a mensagem aparecerá no QM no `server2` e assim por diante. Utilizando essa configuração, o comando `amqsgetc` não poderá recuperar a mensagem que acaba de ser colocada na fila, uma vez que o pedido de conexão do cliente utilizado pelo comando `amqsgetc` será transmitido para o próximo QM na lista. Emitir os três comandos `amqsputc`, seguidos de três comandos `amqsgetc` garante que cada mensagem seja recuperada na mesma ordem. É claro que se você utilizar outro cliente WMQ e conectar-se diretamente a um QM (isto é, sem utilizar o MQIPT deste exemplo), poderá recuperar mensagens seletivamente de quaisquer dos gerenciadores de fila.

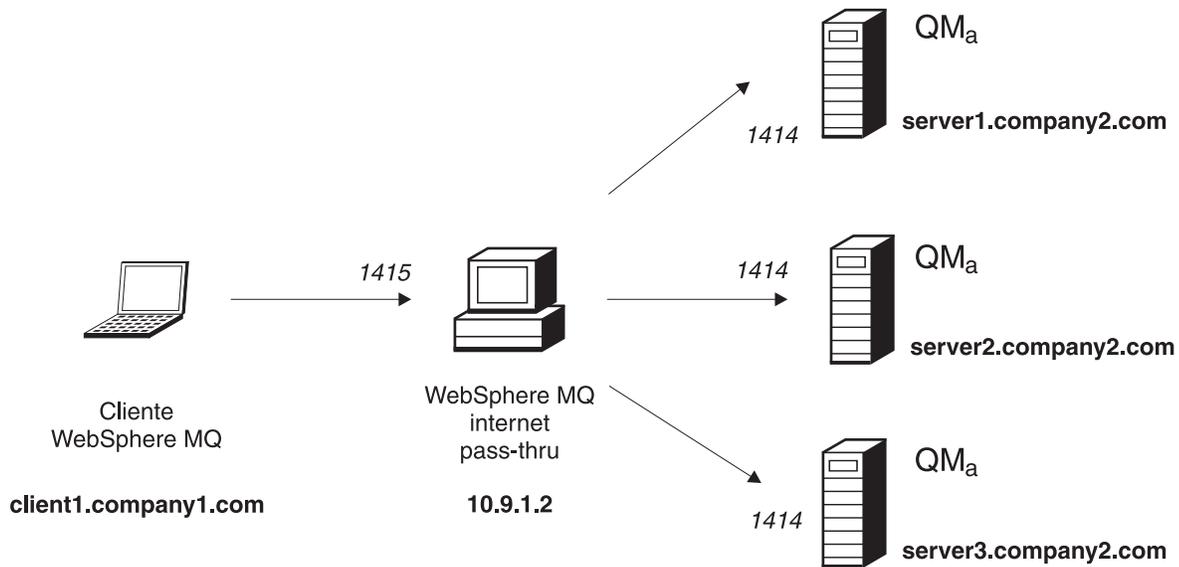


Figura 42. Diagrama de rede de roteamento da saída de segurança

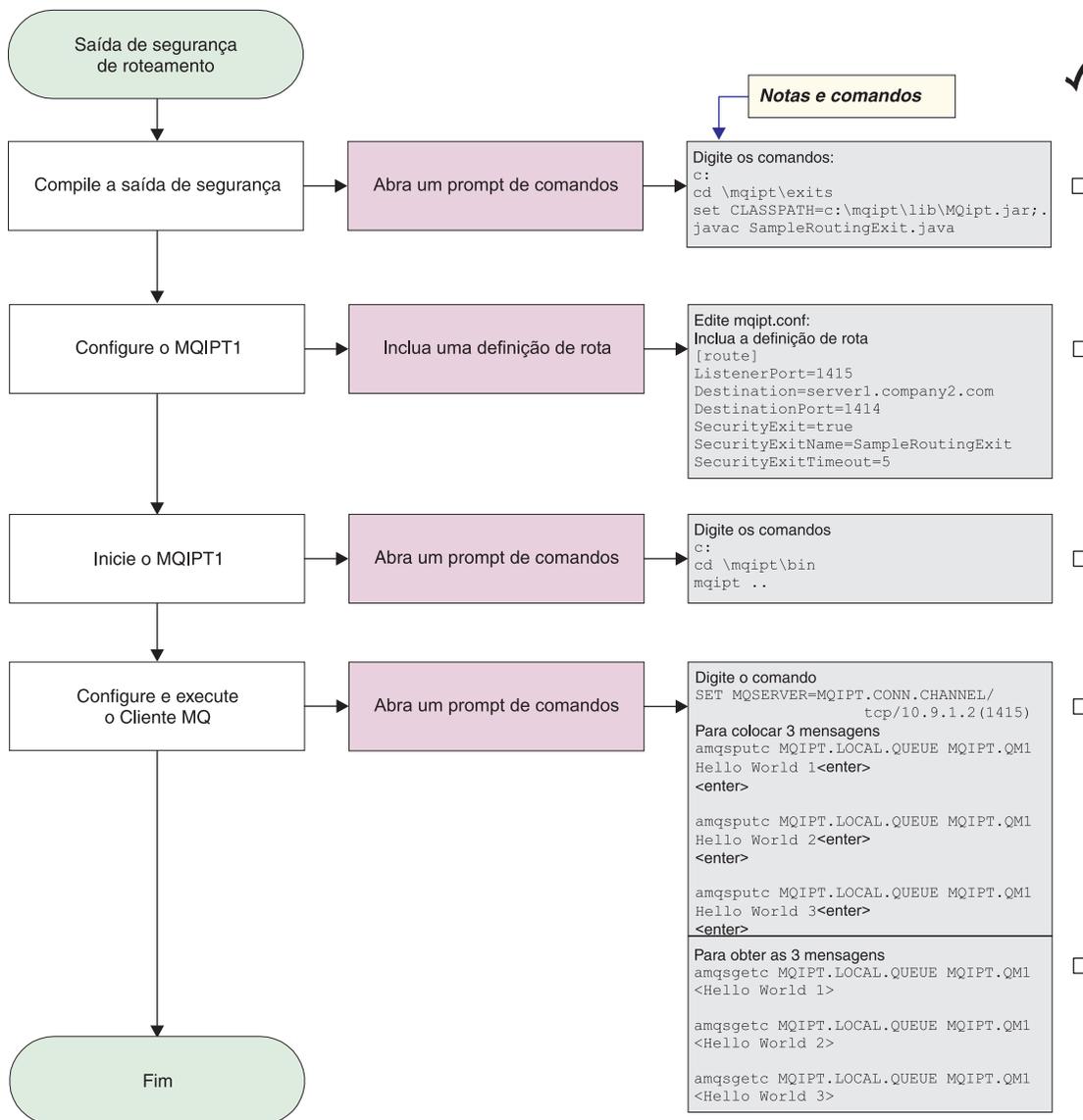


Figura 43. Configuração de roteamento da saída de segurança

1. No IPT1

Abra um prompt de comandos:

```

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

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

```

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

Abra um prompt de comandos:

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

A seguinte mensagem indica uma conclusão bem-sucedida:

```
5639-L92 (C) Copyright IBM Corp. 2000 Todos os Direitos Reservados
MQCPI001 Websphere MQ internet pass-thru Version 1.3.0 starting
MQCPI004 Lendo informações sobre configuração de c:\mqipt\mqipt.conf
MQCPI011 O caminho c:\mqipt\logs será usado p/ armazenar arquivos de log
MQCPI006 A rota 1415 iniciou e enviará mensagens para:
MQCPI034 ....server1.company2.com(1414)
MQCPI035 ....utilizando protocolos MQ
MQCPI079 ....utilizando saída de segurança c:\mqipt\exits\SampleRoutingExit
MQCPI080 .....e tempo limite de 5 segundos
MQCPI078 Rota 1415 pronta para os pedidos de conexão
```

2. 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)
```

3. Coloque três mensagens, utilizando:

```
amqsputc MQIPT.LOCAL.QUEUE MQIPT.QM1
Hello world 1 <enter>
<enter>
amqsputc MQIPT.LOCAL.QUEUE MQIPT.QM1
Hello world 2 <enter>
<enter>
amqsputc MQIPT.LOCAL.QUEUE MQIPT.QM1
Hello world 3 <enter>
<enter>
```

4. Obtenha as mensagens, utilizando:

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

Você verá "Hello world 1", "Hello world 2" e "Hello world 3".

Saída Dinâmica de Uma Rota

Para este exemplo, fazemos as seguintes suposições:

- Java 1.4 SDK instalado
- O subdiretório Java foi adicionado à variável de ambiente PATH
- Três gerenciadores de fila diferentes foram criados em três servidores separados

Este é um exemplo que mostra como rotear dinamicamente pedidos de conexão do cliente para um servidor de destino, com base no nome do canal que está sendo utilizado. A primeira parte do nome do canal é o nome do Gerenciador de Filas. Por exemplo, para conectar-se ao QM1, o nome de um canal svrconn seria QM1.MQIPT.CONN.CHANNEL. Utilizando essa convenção de nomenclatura de canal, o MQIPT precisa utilizar apenas uma rota para atender todos os pedidos de conexão.

A lista de nomes de Gerenciadores de Fila e servidores será lida a partir de um arquivo de configuração. O nome e a localização do arquivo de configuração são definidos com as propriedades SecurityExitName e SecurityExitPath. O arquivo de configuração de amostra, denominado SampleOneRouteExit.conf, contém as entradas:

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

É necessário alterar esses nomes de servidores de acordo com seu ambiente.

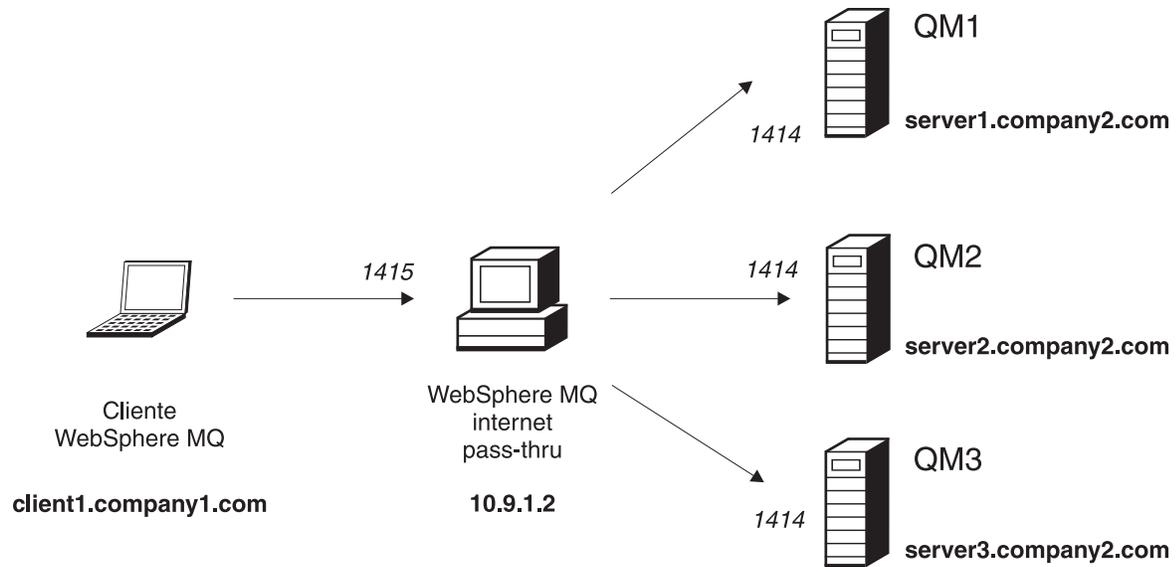


Figura 44. Diagrama de rede para saída dinâmica de uma rota

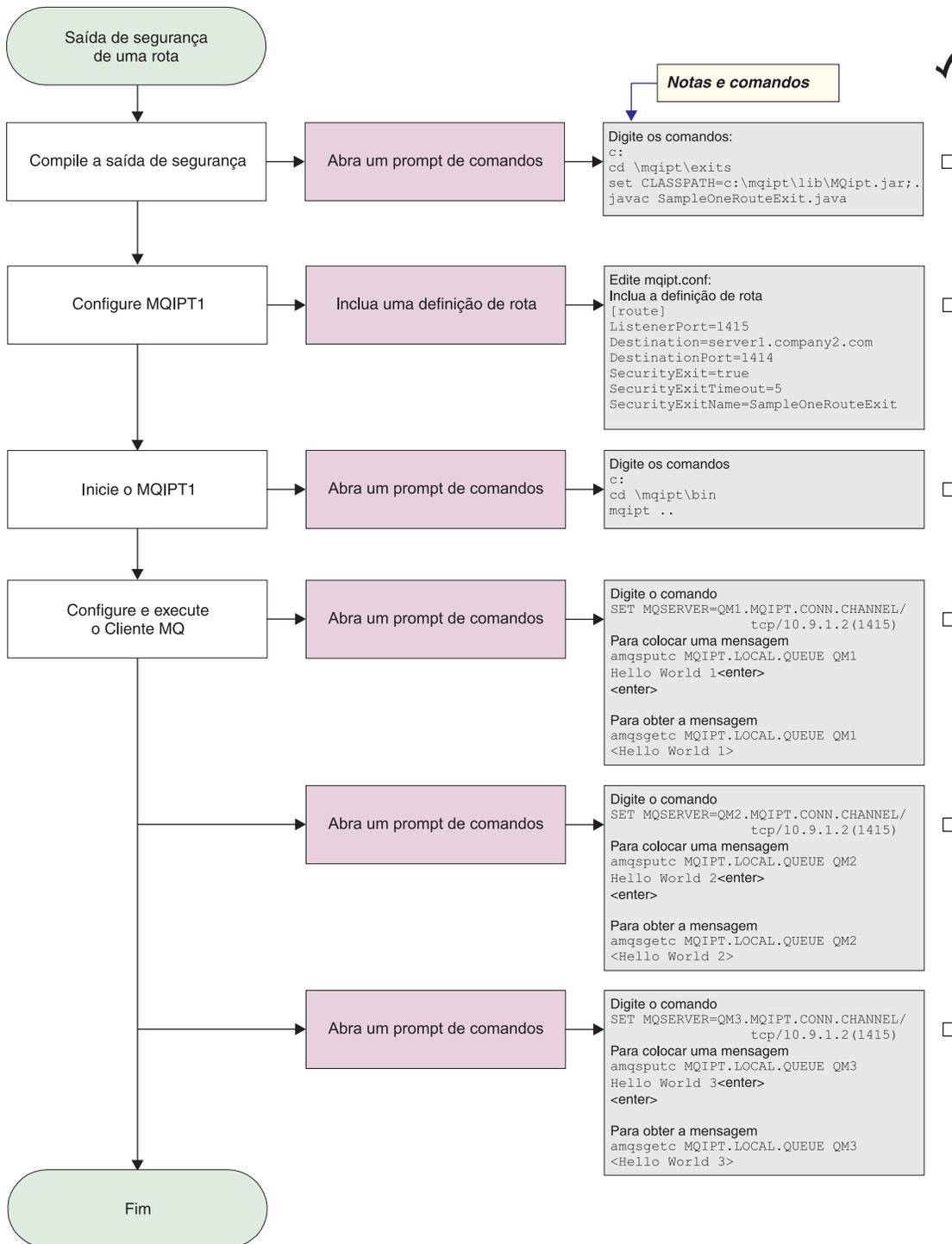


Figura 45. Configuração de saída dinâmica de uma rota

1. No IPT1

Abra um prompt de comandos:

```

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

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

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

Abra um prompt de comandos:

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

A seguinte mensagem indica uma conclusão bem-sucedida:

```
5639-L92 (C) Copyright IBM Corp. 2000 Todos os Direitos Reservados
MQCPI001 Websphere MQ internet pass-thru Version 1.3.0 starting
MQCPI004 Lendo informações sobre configuração de c:\mqipt\mqipt.conf
MQCPI011 O caminho c:\mqipt\logs será usado p/ armazenar arquivos de log
MQCPI006 A rota 1415 iniciou e enviará mensagens para:
MQCPI034 ....server1.company2.com(1414)
MQCPI035 ....utilizando protocolos MQ
MQCPI079 ....utilizando saída de segurança c:\mqipt\exits\SampleOneRouteExit
MQCPI080 .....e tempo limite de 5 segundos
MQCPI078 Rota 1415 pronta para os pedidos de conexão
```

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

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

3. Coloque uma mensagem utilizando:

```
amqsputc MQIPT.LOCAL.QUEUE QM1
Hello world 1 <enter>
<enter>
```

4. Obtenha a mensagem utilizando:

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

Você verá "Hello world 1".

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

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

6. Coloque uma mensagem utilizando:

```
amqsputc MQIPT.LOCAL.QUEUE QM2
Hello world 2 <enter>
<enter>
```

7. Obtenha a mensagem utilizando:

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

Você verá "Hello world 2".

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

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

9. Coloque uma mensagem utilizando:

```
amqsputc MQIPT.LOCAL.QUEUE QM3
Hello world 3 <enter>
<enter>
```

10. Obtenha a mensagem utilizando:

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

Você verá "Hello world 3".

Capítulo 21. Inspeccionando 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 152

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 MQIPs 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 46 na página 150. Os números referem-se às notas, mostradas em seguida.

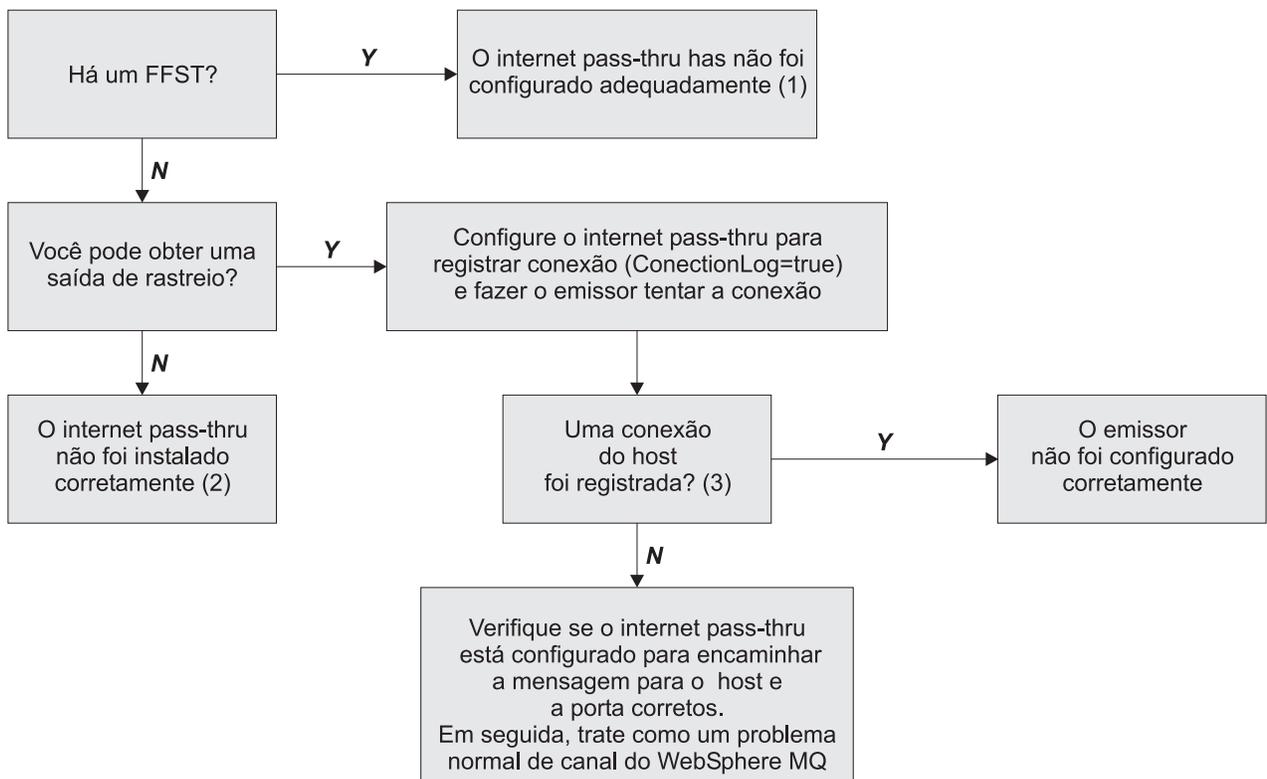


Figura 46. Fluxograma de determinação de problemas

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 inicialização. Corrija o problema que provocou 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 Serviço do Windows NT e tiver alterado sua inicialização para automática, ele será iniciado quando o sistema for ativado. Antes de tentar instalar o MQIPT como Serviço Windows NT, sempre inicie o MQIPT manualmente uma vez para confirmar a instalação correta. Consulte “Utilizando um Programa de Controle de Serviços do Windows” na página 49 para obter mais detalhes.

Se for recebida a mensagem de erro “Não é possível localizar o DLL...”, você está utilizando o programa `mciptService` 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, `mcipt.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.

Rastreamento de Erros

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

```
iptrountnnnn.trc
```

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

Erros fatais inesperados são gravados como registros `FFST` em um arquivo de log de erro, mantido no diretório `xxx\errors` (em que `xxx` is é o diretório que contém `mcipt.conf`). Os arquivos do `FFST` têm o seguinte formato:

```
iptxxx.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 `mcipt0.FFST`. Se o arquivo `mcipt0.FFST` for criado, você deverá parar e iniciar novamente o MQIPT na primeira oportunidade e excluir os arquivos antigos.

Relatando Problemas

Se for necessário relatar um problema para o Centro de Serviços da IBM, a resolução será mais rápida se você puder 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 rastreo em cada MQIPT
- Apague os arquivos de rastreo antigos
- Execute o cliente para produzir o problema - desse modo, os arquivos de rastreo 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 Encadeamentos

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

Encadeamentos de Conexão

Cada rota do MQIPT é atribuída a um conjunto de trabalho de encadeamentos simultaneamente em execução que manipulam pedidos de comunicação de entrada. Na partida, um conjunto de encadeamentos 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 encadeamentos 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 encadeamentos 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 encadeamentos 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 encadeamentos 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 encadeamentos são reciclados para uso colocando-os de volta no conjunto de trabalho.

Capítulo 22. Mensagens

Quando executado a partir da linha de comandos, o MQIPT exibe um pequeno número de mensagens informativas, de aviso e de erro no console.

Observe que:

- Mensagens MQCAxxxx são mensagens do Cliente Administrativo.
- Mensagens MQCPxxxx são mensagens do MQIPT.
- Mensagens MQCxIxxx são mensagens informativas.
- Mensagens MQCxWxxx são de aviso.
- Mensagens MQCxExxx são mensagens de erro.

MQCAE001 Host desconhecido: {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 A mensagem de erro a seguir foi relatada pelo sistema: {0}

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

MQCAE005 Não foi definido endereço de destino válido

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 Não foi definida porta de destino válida

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 Não foi definida porta do atendente válida

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 Não foi definido endereço de rede válido

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 Não foi definida porta de comando válida

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 Não foi possível mostrar a ajuda on-line

Explicação: O arquivo para ajuda on-line estava disponível mas não pôde ser exibido.

Resposta do Usuário: Certifique-se de que exista um navegador da Web instalado e disponível na variável de ambiente PATH do sistema.

MQCAE011 Não foi possível analisar o parâmetro

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 Não foi possível localizar o arquivo de ajuda on-line {0}

Explicação: O arquivo "passtfrm.htm" não foi encontrado.

Resposta do Usuário: Certifique-se de que esse arquivo esteja acessível no subdiretório language.

MQCAE013 Interrompido quando tentava mostrar a ajuda on-line

Explicação: Ocorreu um erro do sistema durante a exibição da ajuda on-line.

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

MQCAE015 A senha informada não foi reconhecida

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 Incompatibilidade de nó

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

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

MQCAE017 Não foi possível criar texto NLS para a mensagem {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 Leia-me para verificar se há uma nova mensagem
 - o arquivo "guiadmin.jar" está no CLASSPATH do sistema
 - o arquivo "guiadmin.properties" está no arquivo "guiadmin.jar"
 - o número da mensagem está no arquivo "guiadmin.properties"
-

MQCAE018 Não foi possível criar texto NLS para a mensagem MQCAE017

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

Resposta do Usuário: O arquivo "guiadmin.properties" pode estar danificado. Verifique o seguinte:

- o arquivo "guiadmin.jar" está no CLASSPATH do sistema
 - o arquivo "guiadmin.properties" está no arquivo "guiadmin.jar"
-

- o número da mensagem está no arquivo "guiadmin.properties"
-

MQCAE019 Falha ao repetir a nova senha proposta

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 Falha ao alterar os parâmetros de acesso MQIPT

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

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

MQCAE021 Falha interna ao identificar MQIPT

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

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

MQCAE022 Falha interna ao salvar a configuração MQIPT

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

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

MQCAE023 O MQIPT {0} não reconheceu a senha.

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 O MQIPT {0} não reconheceu o comando.

Explicação: O Cliente Administrativo enviou um comando para o MQIPT que não foi reconhecido.

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

MQCAE025 Falha do MQIPT {0} ao enviar o arquivo de configuração.

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

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

MQCAE026 O encerramento remoto foi desativado em 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 A aparência e o comportamento {0} não são suportados.

Explicação: A Aparência e o Comportamento recomendado 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 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 O número mínimo de encadeamentos de conexão não deve ser negativo nem maior que o o número máximo de encadeamentos de conexão

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

Resposta do Usuário: Altere o valor apropriadamente.

MQCAE030 O número máximo de encadeamentos de conexão deve ser maior que zero e pelo menos tão grande quando o número mínimo de encadeamentos de conexão

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

Resposta do Usuário: Altere o valor apropriadamente.

MQCAE031 Os números da porta devem estar entre 0 e 65535

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

Resposta do Usuário: Altere o valor apropriadamente.

MQCAE032 O rastreo deve estar entre 0 e 5

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

Resposta do Usuário: Altere o valor apropriadamente.

MQCAE033 O tamanho máximo do arquivo de log deve estar entre 5 e 50

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

Resposta do Usuário: Altere o valor apropriadamente.

MQCAE049 Não há rota selecionada em qualquer 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 Não foi possível conectar ao MQIPT {0}

Explicação: O Cliente Administrativo 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 Cliente Administrativo está utilizando o CommandPort do MQIPT.
 - O tempo limite do pedido expirou.
-

MQCAE051 Não foi possível ler a resposta do 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 Cliente Administrativo seja igual à do MQIPT.

MQCAE052 A configuração não foi salva

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 O MQIPT não confirmou se salvou a configuração

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 Cliente Administrativo está utilizando o CommandPort do MQIPT.
- O tempo limite do pedido expirou.

MQCAE054 Os dados do MQIPT não foram atualizados

Explicação: Foi feito contato com o MQIPT mas o Cliente Administrativo 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 Não houve seleção de MQIPT ou de rota em um MQIPT

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 A porta duplicada do atendente foi rejeitada

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 O MQIPT não está sendo exibido

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

MQCAI003 Uma nova rota é exibida

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

MQCAI004 A rota não está sendo exibida

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

MQCAI005 O MQIPT selecionado está sendo exibido

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

MQCAI006 A rota selecionada está sendo exibida

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

MQCAI007 A configuração do cliente foi salva

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

MQCAI008 A exibição da ajuda on-line foi bem-sucedida

Explicação: A ajuda on-line foi exibida conforme solicitado.

MQCAI009 A tabela foi atualizada

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

MQCAI010 Não houve seleção de MQIPT ou de rota

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

MQCAI011 A Ação do Usuário foi cancelada

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

MQCAI014 A configuração foi salva no 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 A ajuda on-line foi finalizada

Explicação: A ajuda on-line foi exibida conforme solicitado e, subsequentemente, finalizada.

MQCAI017 Selecione Arquivo/Incluir MQIPT para incluir um MQIPT à árvore

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

MQCAI018 Novo MQIPT incluído para exibição

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

MQCAI019 Os parâmetros de acesso do MQIPT foram alterados

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

MQCAI021 Selecione um MQIPT ou rota na árvore para exibir seu conteúdo

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

MQCAI022 A porta do comando foi alterada

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

MQCAI023 A senha foi alterada

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

MQCAI025 O MQIPT {0} foi atualizado.

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

MQCAI026 O MQIPT {0} recebeu um pedido de encerramento.

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

MQCAI027 A configuração do cliente foi atualizada

Explicação: As informações exibidas no Cliente Administrativo foram atualizadas a partir do arquivo "client.conf" local.

MQCAI028 O MQIPT {0} está ativo

Explicação: O MQIPT respondeu com êxito a um pedido de ping.

MQCAI029 O MQIPT {0} não está ativo

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 A rota {0} está ativa

Explicação: O MQIPT respondeu com êxito a um pedido de ping.

MQCAI031 A rota {0} não está ativa

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 Este script é utilizado para iniciar o Cliente Administrativo para {0}. Especificar um proxy SOCKS permite que o Cliente Administrativo converse com um MQIPT por meio de um firewall.

Explicação: Informações de ajuda on-line para o script mqiptGui.

MQCAI101 O formato do comando é:

Explicação: Informações de ajuda on-line para o script mqiptGui.

MQCAI102 mqiptGui {socks_host{socks_port}}

Explicação: Informações de ajuda on-line para o script mqiptGui.

MQCAI103 socks_host-host nome do proxy SOCKS (opcional)

Explicação: Informações de ajuda on-line para o script mqiptGui.

MQCAI104 socks_porta-SOCKS proxy porta endereço (opcional-default 1080)

Explicação: Informações de ajuda on-line para o script mqiptGui.

MQCPE000 Não foi possível localizar os dados da mensagem quando estava tratando a mensagem {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 O diretório não existe ou não é um diretório

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 Falha da inicialização da rota na porta {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 O arquivo de configuração {0} não pôde ser localizado

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 O número de rotas excedeu {0}. O MQIPT será iniciado, mas essa configuração não será suportada.

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 A rota não foi iniciada novamente na porta do atendente {0}

Explicação: Em uma operação ATUALIZAR, 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 Rota duplicada definida para porta do atendente {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 O diretório de log {0} não é válido.

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 O número da porta do comando ou do atendente {0} não é válido

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 O nível de rastreamento {0} está fora da faixa válida 0 - 5

Explicação: A opção de rastreamento especificada foi solicitada, mas não está no intervalo válido 0-5.

Resposta do Usuário: Especifique um valor de rastreamento de 0-5.

MQCPE012 O valor {0} não é válido para o atributo {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 A propriedade ListenerPort não foi localizada na rota {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 O valor da propriedade ListenerPort {0} não é válido

Explicação: Um endereço de porta inválido foi especificado para a propriedade ListenerPort de uma rota.

Resposta do Usuário: O endereço de porta deve estar no intervalo 0 – 65535. Verifique cada ListenerPort no arquivo de configuração.

MQCPE015 Não foi localizado o texto do número da mensagem {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 Leia-me 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 O número máximo de encadeamentos de conexão é {0} porém esse valor é inferior ao número mínimo de encadeamentos de conexão que é {1}

Explicação: Sua configuração especificou o número mínimo de encadeamentos de conexão com um valor que excede o número máximo de encadeamentos 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 A exceção {0} foi descartada, fazendo com que o MQIPT encerrasse

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 A propriedade ListenerPort está em branco - a rota não será iniciada

Explicação: O número de ListenerPort foi omitido em uma rota.

Resposta do Usuário: Edite o arquivo de configuração e inclua um ListenerPort válido.

MQCPE019 A sub-rotina {0} não foi localizada antes do seguinte: {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 O novo valor para MaxConnectionThreads é {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 O destino da propriedade não foi fornecido para a rota {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 O valor CommandPort {0} está fora da faixa válida 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 A solicitação de encerramento do Cliente Administrativo {0} foi ignorada porque está desativada.

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 O comando recebido pelo controlador MQIPT não foi reconhecido.

Explicação: O MQIPT recebeu um comando não reconhecido por meio de sua porta de comando.

Resposta do Usuário: Verifique o arquivo "mqipt.log" para obter a identidade do comando.

MQCPE025 Falha ao conectar ao servidor no host {0}, porta {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 Nenhuma resposta recebida do servidor no host {0}, porta {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 Resposta do MQIPT não reconhecida.

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 Sub-rotina inválida detectada: {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 Não foi possível esvaziar a saída do log.

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 não tornou-se cheio e se o MQIPT ainda tem acesso ao subdiretório logs.

MQCPE030 {0} não localizado em 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} classe não localizada.

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 Falha ao enviar o arquivo de configuração para o Cliente Administrativo em {0}

Explicação: Ocorreu um erro ao enviar o arquivo de configuração para o Cliente Administrativo.

Resposta do Usuário: Verifique se o arquivo de configuração está no diretório inicial do MQIPT e não está sendo compartilhado por outro processo.

MQCPE034 O Cliente Administrativo em {0} não forneceu a senha correta.

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 Falha ao iniciar o atendente do comando na porta {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 não iniciou como esperado

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 Ocorreu um erro de E/S durante a execução do script mqipt

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 Ocorreu interrupção durante a execução do script mqipt

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 Nível não suportado de Java - {0}

Explicação: O MQIPT foi iniciado utilizando o nível especificado de Java.

Resposta do Usuário: Verifique os pré-requisitos no Guia do Usuário para obter mais informações.

MQCPE042 Há um conflito com as propriedades a seguir na rota {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} e {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} é válido apenas no sistema operacional {1}

Explicação: Alguns recursos do MQIPT são válidos apenas em determinadas plataformas.

Resposta do Usuário: Edite o arquivo de configuração e desative a propriedade especificada.

MQCPE045O nome do proxy HTTP está ausente

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} que não foi permitida como Pagent falhou durante a inicialização

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 Falha do Pagent durante a inicialização

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 Falha de inicialização da rota na porta {0}, a exceção era : {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 Erro ao iniciar ou parar o Java Security Manager {0}

Explicação: Foi emitida uma exceção ao tentar 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 critério local. O MQIPT deve ser iniciado novamente para que as alterações entrem em vigor.

MQCPE050 Exceção de segurança na porta {0} do Cliente Administrativo

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 Exceção de segurança aceitando uma conexão na rota {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 Falha do pedido de conexão na rota {0}: {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 Exceção de segurança fazendo uma conexão para {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 Falha do pedido de conexão para {0}({1}): {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 ...O nome do proxy Socks está ausente

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 Conflito com as propriedades da rota

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 O protocolo SSL ({0}) não foi reconhecido

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.

MQCPE058 Falha do pedido CONNECT {2}({3}) por meio do {0}({1})

Explicação: Um pedido HTTP CONNECT foi enviado para o proxy HTTP para criar um túnel SSL para o servidor HTTP. O proxy HTTP não retornou uma resposta "200 OK" para esse pedido.

Resposta do Usuário: Isto pode ser provocado por diversos problemas. Ative o rastreamento na rota e tente conectar-se novamente. O arquivo de rastreamento mostrará o erro real.

MQCPE059 Não há arquivos de conjunto de chaves definidos

Explicação: Um cliente ou servidor SSL foi definido sem especificar no mínimo um arquivo do conjunto de chaves.

Resposta do Usuário: Utilize as propriedades

SSLClientKeyRing e SSLClientCAKeyRing no lado do cliente ou SSLServerKeyRing e SSLServerCAKeyRing no lado do servidor para definir um arquivo do conjunto de chaves e, em seguida, inicie a rota novamente.

MQCPE060 Erro de tempo de execução ao definir o tempo limite de conexão ao cliente SSL para {0} segundos

Explicação: Um erro de tempo de execução SSL ocorreu no lado do cliente ao definir o valor do tempo limite.

Resposta do Usuário: Verifique se o valor especificado na propriedade SSLClientConnectTimeout é válido. A execução de um rastreamento na rota indicada mostrará mais informações sobre o erro.

MQCPE061 Não há conjuntos de cifras ativados

Explicação: Uma conexão cliente ou servidor SSL foi iniciada, mas o MQIPT não pôde determinar um conjunto de cifras válido.

Resposta do Usuário: Verifique se há certificados válidos nos arquivos de conjunto de chaves definidos. As chaves públicas e privadas utilizadas para gerar os certificados e os algoritmos de criptografia utilizados devem estar em conformidade com a lista de conjuntos de cifras suportados, encontrada no manual do MQIPT.

MQCPE062 Erro de tempo de execução ao definir o conjunto de cifras SSL {0}

Explicação: Um conjunto de cifras SSL não suportado foi definido no lado do cliente ou do servidor.

Resposta do Usuário: Verifique se o valor especificado em SSLClientCipherSuites ou em SSLServerCipherSuites é válido e se tem suporte nesta conexão. A execução de um rastreamento na rota indicada mostrará a lista de conjuntos de cifras ativados. O manual do MQIPT contém uma lista de conjuntos de cifras suportados.

MQCPE063 O arquivo {0} já existe - utilizar a opção substituir

Explicação: O parâmetro de nome de arquivo especificado para o script mqiptPW já existe.

Resposta do Usuário: Selecione outro nome de arquivo ou utilize a opção substituir.

MQCPE064 Erro de tempo de execução ao gerar as chaves de criptografia : \n {0}

Explicação: Ocorreu um erro ao gerar chaves de cifras para criptografar a senha utilizada para abrir um arquivo do conjunto de chaves.

Resposta do Usuário: O erro de tempo de execução

listado na mensagem deve ser corrigido e o comando deve ser executado novamente.

MQCPE065 O nome do servidor LDAP está ausente

Explicação: A propriedade LDAPServer1 ou LDAPServer2 deve ser definida se a propriedade LDAP tiver sido definida como true.

Resposta do Usuário: Edite o arquivo de configuração e defina um LDAPServer* para a rota indicada.

MQCPE066 A senha LDAP está ausente para a propriedade LDAPServer{0>Password

Explicação: Um ID de usuário LDAP foi especificado sem senha.

Resposta do Usuário: Edite o arquivo de configuração e defina uma LDAPServer*Password para a rota indicada.

MQCPE067 SSLClient ou SSLServer ausente para o servidor LDAP

Explicação: A propriedade SSLClient ou SSLServer deve ser definida se a propriedade LDAP tiver sido definida como true.

Resposta do Usuário: Edite o arquivo de configuração e defina um SSLClient ou SSLServer para a rota indicada.

MQCPE068 O nome de saída de segurança está ausente

Explicação: A propriedade SecurityExitName deverá ser definida se a propriedade SecurityExit tiver sido definida como true.

Resposta do Usuário: Edite o arquivo de configuração e defina um SecurityExitName para a rota indicada.

MQCPE069 Endereço de porta inválido {0} na security exit response

Explicação: O endereço de porta especificado na SecurityExitResponse não é válido.

Resposta do Usuário: O endereço de porta deve estar no intervalo 1024 - 65535.

MQCPE070 Código de razão desconhecido {0} na security exit response

Explicação: Não há suporte ao código de razão especificado na SecurityExitResponse.

Resposta do Usuário: Consulte o manual do MQIPT para obter uma lista de códigos de razão para os quais existe suporte.

MQCPE071 Erro ao gravar em {0}

Explicação: Ocorreu um erro ao criar ou atualizar o arquivo especificado. A mensagem de erro também contém a exceção emitida.

Resposta do Usuário: O erro descrito na exceção deve ser retificado e o comando deve ser executado novamente.

MQCPE072 Ocorreu um erro desconhecido na saída de segurança {0}

Explicação: Ocorreu um erro em uma saída de segurança definida pelo usuário ao validar um pedido de conexão.

Resposta do Usuário: Ative o rastreo na saída de segurança e tente o pedido de conexão novamente. O erro será registrado no arquivo de rastreo da saída de segurança.

MQCPI001 {0} iniciando

Explicação: Esta instância do MQIPT está iniciando a execução. Seguem mensagens de inicialização adicionais.

MQCPI002 {0} encerrando

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 ATUALIZAR.

MQCPI003 {0} encerramento concluído

Explicação: O processo de encerramento foi concluído. Todos os processos do MQIPT agora estão encerrados.

MQCPI004 Lendo as informações sobre configuração de {0}

Explicação: O arquivo de configuração mqipt.conf do MQIPT está sendo lido no diretório descrito nesta mensagem.

MQCPI005 Porta do atendente especificada como não ativa - {0} -> {1}{2}

Explicação: A rota referida na mensagem foi marcada como inativa. Nenhum pedido de comunicação será aceito nesta rota.

MQCPI006 A rota {0} está iniciando e enviará as mensagens para:

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. A mensagem

MQCPI078 será emitida quando a rota estiver pronta para aceitar conexões.

MQCPI007 A rota {0} foi parada

Explicação: A rota que estava operando no ListenerPort especificado está sendo encerrada. Esta ação normalmente ocorre quando um comando ATUALIZAR é emitido para o MQIPT e a configuração da rota foi alterada.

MQCPI008 Atendendo os comandos de controle na porta {0}

Explicação: Esta instância do MQIPT está atendendo a comandos de controle na porta especificada.

MQCPI009 Comando de controle recebido: {0}

Explicação: Esta mensagem indica que um comando de controle foi recebido na porta do comando. Detalhes são incluídos na mensagem, onde aplicáveis.

MQCPI010 Parando a porta do comando em {0}

Explicação: Em uma operação ATUALIZAR, a porta do comando não está mais em uso na nova configuração. Os comandos não serão mais aceitos na porta especificada.

MQCPI011 O caminho {0} será usado p/ armazenar os arquivos de log

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 ATUALIZAR for solicitada.

MQCPI012 A alteração do valor de MinConnectionThreads não tem efeito depois que a rota tiver sido iniciada

Explicação: O número mínimo de encadeamentos de conexão é atribuído durante a partida da rota e não pode ser alterado até que o MQIPT seja iniciado novamente.

MQCPI013 Conexão de {0} para host {1} fechada

Explicação: Esta mensagem é emitida no log de conexão para registrar a atividade da conexão.

MQCPI014 Protocolo Eyecatcher ({0}) não reconhecido

Explicação: Esta mensagem é emitida no log de conexão para registrar a atividade da conexão.

MQCPI015 O acesso ao cliente foi desativado nesta rota

Explicação: Esta mensagem é emitida no log de conexão para registrar a atividade da conexão.

MQCPI016 O acesso ao Gerenciador de Filas foi desativado nesta rota

Explicação: Esta mensagem é emitida no log de conexão para registrar a atividade da conexão.

MQCPI017 Um gerenciador de filas no {0} foi conectada ao host {1}

Explicação: Esta mensagem é emitida no log de conexão para registrar a atividade da conexão.

MQCPI018 Um cliente em {0} foi conectado ao host {1}

Explicação: Esta mensagem é emitida no log de conexão para registrar a atividade da conexão.

MQCPI019 As rotas {0} foram criadas - isso excede o número máximo de rotas suportadas que é {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 O arquivo de configuração foi enviado ao Cliente Administrativo.

Explicação: Como resultado de um pedido do Cliente Administrativo, o arquivo de configuração foi enviado.

MQCPI021 A verificação de senha foi ativada na porta do comando.

Explicação: Esta mensagem mostra que uma senha é requerida para acessar a porta do comando.

MQCPI022 A verificação da senha foi desativada na porta do comando.

Explicação: Esta mensagem mostra que uma senha não é requerida para acessar a porta do comando.

MQCPI024utilizando o proxy HTTP {0}({1})

Explicação: Esta mensagem indica que a conexão de saída para a rota será feita utilizando este proxy HTTP.

MQCPI025 A atualização solicitada pelo Cliente Administrativo {0} foi concluída.

Explicação: Como resultado do recebimento de um comando ATUALIZAR, o MQIPT leu novamente seu arquivo de configuração e foi iniciado novamente.

MQCPI026 O Cliente Administrativo {0} solicitou o encerramento.

Explicação: Como resultado do recebimento de um comando STOP, o MQIPT está sendo encerrado.

MQCPI027 {0} enviado para {1} na porta {2}

Explicação: Isso exibe, no console do sistema, o comando enviado pelo Cliente Administrativo de modo de linha (não-GUI) para o MQIPT designado.

MQCPI031conjuntos de cifras {0}

Explicação: Esta mensagem lista os conjuntos de cifras em uso para esta rota.

MQCPI032arquivo de conjunto de chaves {0}

Explicação: Esta mensagem fornece o nome do arquivo do conjunto de chaves para esta rota.

MQCPI033autenticação do cliente definida como {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.

MQCPI035utilizando {0}

Explicação: Esta mensagem mostra o protocolo que está sendo utilizado para o destino. Este pode ser o protocolo MQSeries, túnel HTTP ou fragmentação HTTP.

MQCPI036Lado do Cliente SSL ativado com as propriedades :

Explicação: Esta mensagem mostra que a rota utilizará o SSL para enviar dados para o host de destino.

MQCPI037Lado do Servidor SSL ativado com as propriedades:

Explicação: Esta mensagem mostra que a rota utilizará o SSL para receber dados do host de envio.

MQCPI038o certificado peer utiliza {0}

Explicação: Esta mensagem indica os nomes distintos utilizados para controlar a autenticação de certificados peer.

MQCPI039por meio do proxy Socks {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 A porta do comando foi acessada pelo Cliente Administrativo {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.

MQCPI041responderá às solicitações do orientador do Network Dispatcher no modo {0}

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 Conexões máximas alcançadas na rota {0} - os pedidos posteriores serão bloqueados

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 No momento, as conexões na rota {0} estão desbloqueadas

Explicação: Esta mensagem é gravada no console do sistema quando a rota especificada está desbloqueada para os pedidos de conexão.

MQCPI044 O MQIPT foi ativado a partir da inicialização do sistema

Explicação: O MQIPT foi iniciado como um serviço do sistema.

MQCPI045 Ativando o MQIPT a partir da inicialização do sistema

Explicação: O MQIPT será iniciado como um serviço do sistema.

MQCPI046 Suspendendo por {0} segundos enquanto o MQIPT estiver sendo ativado a partir da inicialização do sistema

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.

MQCPI047arquivo de conjunto de chaves CA {0}

Explicação: Esta mensagem fornece o nome do arquivo do conjunto de chaves CA para esta rota.

MQCPI048 O ping do Cliente Administrativo {0} foi concluído

Explicação: Mensagem de resposta do IPTController para o Cliente Administrativo.

MQCPI049prioridade QoS para destino = {0}, para responsável pela chamada = {1}

Explicação: Isso mostra a prioridade de tráfego em ambas as direções nesta rota.

MQCPI050 Adicionando entrada ao inittab para iniciar o MQIPT automaticamente na inicialização do sistema

Explicação: O usuário executou o script mqiptService para iniciar o MQIPT como um serviço do sistema.

MQCPI051 Removendo entrada do inittab para iniciar o MQIPT automaticamente na inicialização do sistema

Explicação: O usuário executou o script mqiptService para impedir que o MQIPT inicie como um serviço do sistema.

MQCPI052lado do servidor Socks ativado

Explicação: Esta rota agirá como um servidor SOCKS (proxy) e aceitará conexões de um aplicativo ativado para socks.

MQCPI053 Iniciando o Java Security Manager

Explicação: O Java Security Manager padrão será iniciado, pois a propriedade SecurityManager foi definida como true.

MQCPI054 Parando o Java Security Manager

Explicação: O Java Security Manager padrão será parado, pois a propriedade SecurityManager foi definida como false.

MQCPI055 Definindo o `java.security.policy` para {0}

Explicação: O Java Security Manager está prestes a ser iniciado e utilizará o arquivo de critério fornecido.

MQCPI056 O Java Security Manager deve ser iniciado novamente para utilizar um novo arquivo de critério.

Explicação: A propriedade `SecurityManagerPolicy` foi alterada, mas entrará em vigor somente quando o Java Security Manager for iniciado novamente.

Resposta do Usuário: Altere a propriedade `SecurityManager` para `false` e emita um comando atualizar a fim de parar o Java Security Manager. Em seguida, retorne o `SecurityManager` para `true` e emita outro comando atualizar para iniciar o Java Security Manager com o novo arquivo de critério.

MQCPI057nível de rastreo {0} ativado

Explicação: Esta mensagem é gravada no console do sistema quando uma rota é iniciada. Utilizada para mostrar o nível de rastreo ativado nesta rota.

MQCPI058e um nome URI de {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.

MQCPI059cliente servlet ativado

Explicação: Esta mensagem é gravada no console do sistema quando uma rota é iniciada. Esta rota será conectada ao servlet do MQIPT.

MQCPI060 Instalando os arquivos para iniciar o MQIPT automaticamente na inicialização do sistema

Explicação: O usuário executou o script `mqiptService` para iniciar o MQIPT como um serviço do sistema.

MQCPI061 Removendo arquivos para iniciar o MQIPT automaticamente na inicialização do sistema

Explicação: O usuário executou o script `mqiptService` para impedir que o MQIPT inicie como um serviço do sistema.

MQCPI064nenhuma autenticação SSL nesta rota

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.

MQCPI065no modo proxy SSL

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.

MQCPI066e o servidor HTTP em {0}{1}

Explicação: Esta mensagem indica que a conexão de saída desta rota será feita utilizando este servidor HTTP.

MQCPI067 Definindo links para as bibliotecas do tempo de execução TQoS

Explicação: O usuário executou o script `mqiptQoS` para criar um link com as bibliotecas de tempo de execução TQoS reais.

MQCPI068 Removendo links das bibliotecas do tempo de execução TQoS

Explicação: O usuário executou o script `mqiptQoS` para remover o link com as bibliotecas de tempo de execução TQoS reais.

MQCPI069ligando ao endereço local {0}

Explicação: Esta mensagem mostra o endereço IP local ao qual cada conexão está ligada. Deve ser utilizada somente em um sistema com várias hospedagens.

MQCPI070utilizando a faixa de endereço de porta local {0}-{10}

Explicação: Esta mensagem mostra os endereços de porta local que serão utilizados para uma conexão. Isto permite que administradores de firewall restrinjam conexões a partir do MQIPT.

MQCPI071 o certificado de site utiliza {0}

Explicação: Esta mensagem relaciona os nomes distintos utilizados para controlar a seleção de um certificado de site.

MQCPI072e certificado de rótulo {0}

Explicação: Esta mensagem relaciona os nomes de rótulos utilizados para controlar a seleção de um certificado de site.

MQCPI073 Arquivo atualizado {0}

Explicação: O nome do arquivo especificado para o script `mqiptPW` foi atualizado.

MQCPI074 Arquivo criado {0}
Explicação: O nome do arquivo especificado para o script mqiptPW foi criado.

MQCPI075servidor LDAP principal em {0}({1})
Explicação: Esta mensagem indica o nome do servidor LDAP principal utilizado para suporte ao CRL.

MQCPI076Servidor LDAP de backup em {0}({1})
Explicação: Esta mensagem indica o nome do servidor LDAP de backup utilizado para suporte ao CRL.

MQCPI077os erros LDAP serão ignorados
Explicação: Esta mensagem significa que os erros recebidos do LDAP serão ignorados.

MQCPI078 Rota {0} pronta para pedidos de conexão
Explicação: Esta mensagem é exibida quando uma rota está pronta para acessar pedidos de conexão.

MQCPI079utilizando a saída de segurança {0}
Explicação: Esta mensagem é gravada no console do sistema quando uma rota é iniciada. É utilizada para mostrar o nome completo da saída de segurança.

MQCPI080e o tempo limite de {0} segundos
Explicação: Esta mensagem é gravada no console do sistema quando uma rota é iniciada. É utilizada para mostrar o valor do tempo limite da saída de segurança.

MQCPI081 Iniciar mensagem do WebSphere MQ internet pass-thru
Explicação: Mensagem inicial do WebSphere MQ internet pass-thru como serviço

MQCPI082 Parar mensagem do WebSphere MQ internet pass-thru
Explicação: Mensagem de parada do WebSphere MQ internet pass-thru como serviço

MQCPI083os comandos de atualização não serão iniciados novamente na rota
Explicação: Esta mensagem indica que quando um comando atualizar é emitido, a rota não é iniciada novamente.

MQCPI084o tempo limite de expiração do cache CRL é {0} hora(s)
Explicação: Esta mensagem do console mostra por quanto tempo uma CRL (ou ARL) permanecerá no cache do MQIPT.

MQCPI085os CRLs serão salvos no(s) arquivo(s) de conjunto de chaves
Explicação: Esta mensagem do console significa que as CRLs (ou ARLs) recuperadas de um servidor LDAP serão salvas no arquivo do conjunto de chaves, conectadas ao certificado CA associado.

MQCPI086tempo limite de {0} segundo(s)
Explicação: Esta mensagem é gravada no console do sistema quando uma rota é iniciada. É utilizada para mostrar o valor do tempo limite para conexão com o servidor LDAP.

MQCPI087o ID do usuário é {0}
Explicação: Esta mensagem é gravada no console do sistema quando uma rota é iniciada. É utilizada para mostrar o nome do ID do usuário para conexão com o servidor LDAP.

MQCPI100 Este script é utilizado para iniciar {0}
Explicação: Mensagem de ajuda on-line do script mqipt.

MQCPI101 O formato do comando é:
Explicação: Mensagem de ajuda on-line do script mqipt.

MQCPI102 mqipt {dir_nome}
Explicação: Mensagem de ajuda on-line do script mqipt.

MQCPI103 dir_nome - diretório contendo mqipt.conf
Explicação: Mensagem de ajuda on-line do script mqipt.

MQCPI106 Este script é utilizado para exibir o número da versão atual
Explicação: Mensagem de ajuda on-line do script mqiptVersion.

MQCPI107 `mqiptVersion {-v}`

Explicação: Mensagem de ajuda on-line do script `mqiptVersion`.

MQCPI108 `em que -v também exibirá data e hora da compilação`

Explicação: Mensagem de ajuda on-line do script `mqiptVersion`.

MQCPI109 `Este script é utilizado para iniciar o {0}, a partir da inicialização do sistema, em outro JVM e é utilizado apenas no mqipt.ske. Utilize o script mqipt para iniciar o MQIPT a partir da linha de comandos.`

Explicação: Mensagem de ajuda on-line do script `mqiptFork`.

MQCPI110 `Esta classe é utilizada para exibir uma mensagem NLS simples no console`

Explicação: Mensagem de ajuda on-line da classe `IPMessages`.

MQCPI111 `java com.ibm.mq.ip.IPTMessages (mensagem_id1) {mensagem_id2} {mensagem_id...}`

Explicação: Mensagem de ajuda on-line da classe `IPMessages`.

MQCPI112 `em que mensagem_id corresponde à chave no arquivo mqipt.properties`

Explicação: Mensagem de ajuda on-line da classe `IPMessages`.

MQCPI113 `Este script é utilizado para gerenciar o MQIPT como um serviço do sistema`

Explicação: Mensagem de ajuda on-line do script `mqiptService`.

MQCPI114 `mqiptService (-install | -remove)`

Explicação: Mensagem de ajuda on-line do script `mqiptService`.

MQCPI115 `-install instalará os arquivos para iniciar o MQIPT automaticamente na inicialização do sistema`

Explicação: Mensagem de ajuda on-line do script `mqiptService`.

MQCPI116 `-remove removerá os arquivos que iniciam o MQIPT automaticamente na inicialização do sistema`

Explicação: Mensagem de ajuda on-line do script `mqiptService`.

MQCPI117 `Este script é utilizado para gerenciar links para as bibliotecas de tempo de execução TQoS`

Explicação: Mensagem de ajuda on-line do script `mqiptService`.

MQCPI118 `mqiptQoS (-install | -remove)`

Explicação: Mensagem de ajuda on-line do script `mqiptService`.

MQCPI119 `-install configurará os links às bibliotecas de tempo de execução TQoS real`

Explicação: Mensagem de ajuda on-line do script `mqiptService`.

MQCPI120 `-remove removerá os links das bibliotecas de tempo de execução TQoS real`

Explicação: Mensagem de ajuda on-line do script `mqiptService`.

MQCPI121 `Utilize este script para criptografar uma senha e armazená-la em um arquivo`

Explicação: Mensagem de ajuda on-line do script `mqiptPW`.

MQCPI122 `mqiptPW senha arquivo_nome { -substituir }`

Explicação: Mensagem de ajuda on-line do script `mqiptPW`.

MQCPI123 `senha - senha utilizada para abrir um arquivo de conjunto de chaves`

Explicação: Mensagem de ajuda on-line do script `mqiptPW`.

MQCPI124 `arquivo_nome - a senha criptografada será armazenada neste arquivo`

Explicação: Mensagem de ajuda on-line do script `mqiptPW`.

| **MQCPI125** A opção substituir deve ser utilizada
| para atualizar um arquivo existente

| **Explicação:** Mensagem de ajuda on-line do script
| mqiptPW.

| **MQCPI126** mqipt (-start | -stop)

| **Explicação:** Mensagem de ajuda on-line do script
| mqiptQoS.

| **MQCPW001** CRL expirado para {0}

| **Explicação:** Esta mensagem é exibida quando uma
| CRL (ou ARL) é recuperada de um servidor LDAP ou
| arquivo do conjunto de chaves.

| **Resposta do Usuário:** Atualize a CRL especificada no
| servidor LDAP ou no arquivo do conjunto de chaves.

| **MQCPW002** Erro de atualização do arquivo de
| conjunto de chaves {0} com CRL

| **Explicação:** Esta mensagem é exibida quando a
| propriedade LDAPSaveCRLs tiver sido ativada e o
| arquivo do conjunto de chaves especificado não puder
| ser atualizado.

| **Resposta do Usuário:** O arquivo especificado pode
| estar danificado. Verifique o seguinte:

- | 1. o acesso de gravação do MQIPT deve estar ativado
- | 2. o arquivo não está aberto por outro aplicativo

| **MQCPW003**As CRLs expiradas serão ignoradas

| **Explicação:** Esta mensagem do console significa que as
| CRLs (ou ARLs) expiradas serão ignoradas e o pedido
| de conexão pode ser permitido.

Apêndice. 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 nos quais opera.

Qualquer referências nesta publicação a um programa licenciado da IBM ou a 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 esse produto IBM. A avaliação e verificação da operação em conjunto com outros produtos, exceto aqueles expressamente designados pela IBM, são de inteira responsabilidade do usuário.

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 a 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 SupportPac	IBMLink WebSphere	MQSeries

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

Java e todas as marcas baseadas em Java são marcas da Sun Microsystems, Inc. nos Estados Unidos e/ou em outros países.

UNIX é uma marca registrada do The Open Group nos Estados Unidos e em outros países.

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

Bibliografia

Este manual está disponível em HTML como parte do produto instalado. O HTML está contido em um arquivo zip de descompactação automática, no diretório `doc\<locale>\html\<nome_do_arquivo>.zip`. Antes de utilizar o Cliente Administrativo, é necessário descompactar o arquivo que está no subdiretório `<locale>\html`. O manual foi produzido nos idiomas a seguir. Consulte a tabela abaixo para obter o idioma e o nome do arquivo correspondente:

Tabela 4. Resumo de idiomas e nomes de arquivo

Idioma	Locale	Nome do arquivo HTML
Chinês simplificado	zn_CN	amqyzb01.zip
Alemão	de_DE	amqygb01.zip
Japonês	ja_JP	amqyjb01.zip
Coreano	ko_KR	amqykb01.zip
Português do Brasil	pt_BR	amqybb01.zip
Espanhol	es_ES	amqysb01.zip
Inglês dos Estados Unidos	en_US	amqyab01.zip

Os PDFs traduzidos podem ser transferidos por download a partir do seguinte URL:

<http://www.ibm.com/webspheremq/downloads>

Eles estão disponíveis nos seguintes idiomas:

Tabela 5. Idiomas e nomes de arquivos PDF

Idioma	Locale	Nome do arquivo PDF
Chinês simplificado	zn_CN	amqyzb01.pdf
Alemão	de_DE	amqygb01.pdf
Japonês	ja_JP	amqyjb01.pdf
Coreano	ko_KR	amqykb01.pdf
Português do Brasil	pt_BR	amqybb01.pdf
Espanhol	es_ES	amqysb01.pdf
Inglês dos Estados Unidos	en_US	amqyab01.pdf

As seguintes publicações poderão ser úteis para você:

- *WebSphere MQ Intercommunication*, SC34-6059
- *WebSphere MQ System Administration Guide*, SC34-6068
- *WebSphere MQ Clients*, GC34-6058
- *WebSphere MQ Queue Manager Clusters*, SC34-6061

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/webspheremq/library>

Índice Remissivo

A

- administrando o MQIPT 71
- administrando o MQIPT utilizando comandos de modo de linha 75
- AES 21
- AIX
 - configurando o MQIPT 56
 - fazendo download de arquivos do MQIPT 55
 - iniciando o Cliente Administrativo a partir da linha de comandos 57
 - iniciando o MQIPT a partir da linha de comandos 56
 - iniciando o MQIPT automaticamente 57
 - instalando arquivos do MQIPT 55
 - instalando o MQIPT 55
 - removendo a instalação do MQIPT 58
- ajuste de desempenho 152
- algoritmos criptográficos 15
- arquivo de conjunto de chaves criptografando uma senha 21
- selecionando certificados 21

B

- bibliografia 173

C

- canais de cliente /servidor 8
- canais de emissor/receptor 8
- canais de emissor/receptor de cluster 8
- canais de servidor/receptor 8
- canais de servidor/solicitador 8
- canais de solicitador/ emissor 8
- canais de solicitador/servidor 8
- Certificados X.509 V3 24
- Cliente Administrativo 71
 - administrando um MQIPT 72
 - herança de propriedades 72
 - informações de ajuda 75
 - informações de conexão 71
 - iniciando 71
 - iniciando no AIX 57
 - iniciando no HP-UX 61
 - iniciando no Linux 65
 - iniciando no Sun Solaris 53
 - iniciando no UNIX genérico 70
 - iniciando no Windows 49
 - opções de menu do MQIPT 73
 - opções do menu arquivo 73
- cluster 13
- comando de modo de linha ATUALIZAR 75
- comando de modo de linha STOP 75
- comandos de modo de linha 75
- concentrador de canais, MQIPT como um 1

- condições de falha 43
- conectividade de ponta a ponta problemas 151
- configuração
 - arquivo de configuração padrão 77
 - informações de referência 76
 - informações de referência de propriedades 80
 - proteção do arquivo 41
 - resumo de propriedades 77
 - utilizando comandos de modo de linha 75
 - utilizando o Cliente Administrativo 71
- configurações de exemplo 1, 96
 - alocando endereços de porta 127
 - autenticação do cliente SSL 100
 - autenticação do servidor SSL 98
 - configuração do proxy HTTP 103
 - configuração HTTPS 118
 - configurando a QoS (Qualidade de Serviço) 108
 - configurando o cliente SOCKS 113
 - configurando o controle de acesso 105
 - configurando o proxy SOCKS 111
 - configurando o servlet do MQIPT 115
 - configurando o suporte ao clustering do MQIPT 121
 - criando certificados de teste SSL 114
 - criando um arquivo de conjunto de chaves 125
 - Modo proxy do SSL 133
 - regravação Apache 135
 - saída de segurança 139
 - saída de segurança de roteamento 141
 - saída dinâmica de uma rota 144
 - teste de verificação de instalação 96
 - utilizando um servidor LDAP 129
- configurando o MQIPT
 - em genérico 68
 - no AIX 56
 - no HP-UX 60
 - no Linux 64
 - no Sun Solaris 52
 - no Windows 48
- conjuntos de cifras 15
- controle do endereço de porta 39
- criptografia 2
- CRLs (Listas de Revogações de Certificado) do X.509 V2 24

D

- definições de confiança 17
- denial of service, ataques 41
- determinação de problemas 149

E

- encadeamentos de conexão
 - ajuste de desempenho 152
- encaminhador de protocolo, MQIPT como 7
- encapsulamento, HTTP 9
- encapsulamento HTTP, HTTP com 2
- endereço da página da Web do SupportPac 47
- endereço de porta, controle 39

F

- fazendo backup de arquivos de chaves 149
- fazendo download de arquivos do MQIPT
 - no AIX 55
 - no HP-UX 59
 - no Linux 63
 - no Sun Solaris 51
 - no UNIX genérico 67
 - no Windows 47
- fazendo upgrade um MQIPT anterior 45
- fragmentação, HTTP 9

G

- genérico
 - configurando o MQIPT 68
 - fazendo download de arquivos do MQIPT 67
 - iniciando o Cliente Administrativo a partir da linha de comandos 70
 - iniciando o MQIPT a partir da linha de comandos 69
 - iniciando o MQIPT automaticamente 70
 - instalando arquivos do MQIPT 67
 - instalando o MQIPT 67
 - removendo a instalação do MQIPT 70
- gerenciadores de fila de destino, acesso a 7
- gerenciamento do conjunto de encadeamentos 152

H

- herança de propriedades 72
- HP-UX
 - configurando o MQIPT 60
 - fazendo download de arquivos do MQIPT 59
 - iniciando o Cliente Administrativo a partir da linha de comandos 61
 - iniciando o MQIPT a partir da linha de comandos 60

HP-UX (*continuação*)
 iniciando o MQIPT
 automaticamente 61
 instalando arquivos do MQIPT 59
 instalando o MQIPT 59
 removendo a instalação do
 MQIPT 62
HTTPS 10

I

informações de acessibilidade viii
iniciando automaticamente o MQIPT
 problemas 151
iniciando o MQIPT 95
iniciando o MQIPT a partir da linha de
 comandos
 no AIX 56
 no HP-UX 60
 no Linux 64
 no Sun Solaris 52
 no UNIX genérico 69
 no Windows 48
iniciando o MQIPT automaticamente
 no AIX 57
 no HP-UX 61
 no Linux 65
 no Sun Solaris 53
 no UNIX genérico 70
inspecionando o MQIPT 149
instalando arquivos do MQIPT
 no AIX 55
 no HP-UX 59
 no Linux 63
 no Sun Solaris 51
 no UNIX genérico 67
 no Windows 47
introdução 1

J

Java Security Manager 31

K

KeyMan 22
 formatos de dados padrão
 suportados 23
 perguntas mais freqüentes 24
 tipos de token suportados 22

L

LDAP e CRLs 19
Linux
 configurando o MQIPT 64
 fazendo download de arquivos do
 MQIPT 63
 iniciando o Cliente Administrativo a
 partir da linha de comandos 65
 iniciando o MQIPT a partir da linha
 de comandos 64
 iniciando o MQIPT
 automaticamente 65
 instalando arquivos do MQIPT 63

Linux (*continuação*)
 instalando o MQIPT 63
 removendo a instalação do
 MQIPT 66
logs de conexão 43

M

manutenção 149
mecanismo de pulsação 9
mensagens 153
mensagens, segurança de 43

N

Network Dispatcher 29

O

outras considerações sobre segurança 41

P

padrão avançado de criptografia 21
PKCS#10 23
PKCS#12 23
PKCS#7 23
porta 39
pré-requisitos vii
problemas comuns 149
procura de falhas 149
programa de controle de serviços,
 Windows 49
propriedade AccessPW 80
propriedade de configuração Active 81
propriedade de configuração
 ClientAccess 81
propriedade de configuração
 CommandPort 80
propriedade de configuração
 ConnectionLog 80
propriedade de configuração
 Destination 81
propriedade de configuração
 DestinationPort 81
propriedade de configuração HTTP 81
propriedade de configuração
 HTTPChunking 82
propriedade de configuração
 HTTPProxy 82
propriedade de configuração
 HTTPProxyPort 82
propriedade de configuração HTTPS 82
propriedade de configuração
 HTTPServer 82
propriedade de configuração
 HTTPServerPort 82
propriedade de configuração
 IdleTimeout 82
propriedade de configuração
 IgnoreExpiredCRLs 83
propriedade de configuração LDAP 83
propriedade de configuração
 LDAPCacheTimeout 83

propriedade de configuração
 LDAPIgnoreErrors 83
propriedade de configuração
 LDAPSaveCRL 83
propriedade de configuração
 LDAPServer1 83
propriedade de configuração
 LDAPServer1Password 84
propriedade de configuração
 LDAPServer1Port 84
propriedade de configuração
 LDAPServer1Timeout 84
propriedade de configuração
 LDAPServer1Userid 84
propriedade de configuração
 LDAPServer2 84
propriedade de configuração
 LDAPServer2Password 84
propriedade de configuração
 LDAPServer2Port 84
propriedade de configuração
 LDAPServer2Timeout 85
propriedade de configuração
 LDAPServer2Userid 84
propriedade de configuração
 ListenerPort 85
propriedade de configuração
 LocalAddress 85
propriedade de configuração LogDir 85
propriedade de configuração
 MaxConnectionThreads 85
propriedade de configuração
 MaxLogFileSize 80
propriedade de configuração
 MinConnectionThreads 85
propriedade de configuração Name 85
propriedade de configuração
 OutgoingPort 86
propriedade de configuração
 QMGrAccess 86
propriedade de configuração QoS 86
propriedade de configuração
 QosToCaller 86
propriedade de configuração
 QosToDest 86
propriedade de configuração
 RemoteShutDown 80
propriedade de configuração
 RouteRestart 86
propriedade de configuração
 SecurityExit 87
propriedade de configuração
 SecurityExitName 87
propriedade de configuração
 SecurityExitPath 87
propriedade de configuração
 SecurityExitTimeout 87
propriedade de configuração
 SecurityManager 81
propriedade de configuração
 SecurityManagerPolicy 81
propriedade de configuração
 ServletClient 87
propriedade de configuração
 SocksClient 87
propriedade de configuração
 SocksProxyHost 87

- propriedade de configuração
 - SocksProxyPort 87
- propriedade de configuração
 - SocksServer 88
- propriedade de configuração
 - SSLClient 88
- propriedade de configuração
 - SSLClientCAKeyRing 88
- propriedade de configuração
 - SSLClientCAKeyRingPW 88
- propriedade de configuração
 - SSLClientCipherSuites 88
- propriedade de configuração
 - SSLClientDN_C 89
- propriedade de configuração
 - SSLClientDN_CN 89
- propriedade de configuração
 - SSLClientDN_L 89
- propriedade de configuração
 - SSLClientDN_O 89
- propriedade de configuração
 - SSLClientDN_OU 89
- propriedade de configuração
 - SSLClientDN_ST 89
- propriedade de configuração
 - SSLClientKeyRing 89
- propriedade de configuração
 - SSLClientKeyRingPW 90
- propriedade de configuração
 - SSLClientSiteDN_C 90
- propriedade de configuração
 - SSLClientSiteDN_CN 90
- propriedade de configuração
 - SSLClientSiteDN_L 90
- propriedade de configuração
 - SSLClientSiteDN_O 90
- propriedade de configuração
 - SSLClientSiteDN_OU 90
- propriedade de configuração
 - SSLClientSiteDN_ST 90
- propriedade de configuração
 - SSLClientSiteLabel 91
- propriedade de configuração
 - SSLProxyMode 91
- propriedade de configuração
 - SSLServer 91
- propriedade de configuração
 - SSLServerAskClientAuth 91
- propriedade de configuração
 - SSLServerCAKeyRing 91
- propriedade de configuração
 - SSLServerCAKeyRingPW 91
- propriedade de configuração
 - SSLServerCipherSuites 92
- propriedade de configuração
 - SSLServerDN_C 92
- propriedade de configuração
 - SSLServerDN_CN 92
- propriedade de configuração
 - SSLServerDN_L 92
- propriedade de configuração
 - SSLServerDN_O 92
- propriedade de configuração
 - SSLServerDN_OU 92
- propriedade de configuração
 - SSLServerDN_ST 92

- propriedade de configuração
 - SSLServerKeyRing 93
- propriedade de configuração
 - SSLServerKeyRingPW 93
- propriedade de configuração
 - SSLServerSiteDN_C 93
- propriedade de configuração
 - SSLServerSiteDN_CN 93
- propriedade de configuração
 - SSLServerSiteDN_L 93
- propriedade de configuração
 - SSLServerSiteDN_O 93
- propriedade de configuração
 - SSLServerSiteDN_OU 93
- propriedade de configuração
 - SSLServerSiteDN_ST 94
- propriedade de configuração
 - SSLServerSiteLabel 94
- propriedade de configuração Trace 94
- propriedade de configuração
 - UriName 94
- propriedade NDAdvisor 85
- propriedade
 - NDAdvisorReplaceMode 86
- propriedade
 - SSLClientConnectTimeout 88
- propriedades
 - novas 45
 - resumo 77
 - seção global 80
 - seção route 81
- protocolo de reconhecimento 16

Q

- QoS 27

R

- rastreando erros 151
- recurso de rastreamento detalhado, 151
- relatando problemas 151
- relatórios FFST 150
- removendo a instalação do MQIPT
 - no AIX 58
 - no HP-UX 62
 - no Linux 66
 - no Sun Solaris 54
 - no UNIX genérico 70
 - no Windows 50
- repositórios PKCS#11 (CryptoKi) 23
- resumo das alterações ix

S

- saída de segurança
 - com.ibm.mq.ippt.SecurityExit, classe 33
 - com.ibm.mq.ippt.SecurityExitResponse, classe 36
 - rastreamento 37
 - visão geral 32
- segurança, outras considerações sobre 41
- segurança de mensagens 43
- servlet 10

- sistemas com várias hospedagens 39
- SPKAC 24
- SSL, visão geral 15
- Sun Solaris
 - configurando o MQIPT 52
 - fazendo download de arquivos do MQIPT 51
 - iniciando o Cliente Administrativo a partir da linha de comandos 53
 - iniciando o MQIPT a partir da linha de comandos 52
 - iniciando o MQIPT automaticamente 53
 - instalando arquivos do MQIPT 51
 - instalando o MQIPT 51
 - removendo a instalação do MQIPT 54
- suporte ao HTTP 9
- suporte ao SOCKS 13
- suporte ao SSL 15
 - AES 21
 - definições de confiança 17
 - exemplo 2
 - LDAP e CRLs 19
 - mensagens de erro 18
 - padrão avançado de criptografia 21
 - protocolo de reconhecimento 16
 - testando 18
 - WebSphere MQ internet pass-thru e SSL 17
- suposições 95

T

- TCP/IP e MQIPT 7
- tecnologias relacionadas a
 - certificados 18
- tempo limite inativo
 - ajuste de desempenho 152
- terminação 43
- terminação normal 43
- teste de verificação de instalação 96
- token PKCS#12 23
- token PKCS#7 22
- topologia de MQIPs 3

U

- utilizações do MQIPT 1

V

- visão geral do MQIPT 7

W

- WebSphere MQ internet pass-thru e SSL 17
- Windows
 - configurando o MQIPT 48
 - desinstalando o MQIPT como um serviço 50
 - fazendo download de arquivos do MQIPT 47

Windows (*continuação*)

- iniciando o Cliente Administrativo a partir da linha de comandos 49
- iniciando o MQIPT a partir da linha de comandos 48
- instalando arquivos do MQIPT 47
- instalando o MQIPT 47
- programa de controle de serviços 49
- removendo a instalação do MQIPT 50

Z

- zona desmilitarizada, MQIPT com 2

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

- By fax:
 - From outside the U.K., after your international access code use 44-1962-816151
 - From within the U.K., use 01962-816151
- 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.

