



WebSphere MQ Internet Pass-Thru Version 1.3

Hinweis

Vor Verwendung dieses Handbuchs und des darin beschriebenen Produkts sollten die allgemeinen Informationen unter „Bemerkungen“, auf Seite 177 gelesen werden.

- Die IBM Homepage finden Sie im Internet unter: **ibm.com**
- IBM und das IBM Logo sind eingetragene Marken der International Business Machines Corporation.
- Das e-business-Symbol ist eine Marke der International Business Machines Corporation.
- Infoprint ist eine eingetragene Marke der IBM.
- ActionMedia, LANDesk, MMX, Pentium und ProShare sind Marken der Intel Corporation in den USA und/oder anderen Ländern.
- C-bus ist eine Marke der Corollary, Inc. in den USA und/oder anderen Ländern.
- Java und alle auf Java basierenden Marken und Logos sind Marken der Sun Microsystems, Inc. in den USA und/oder anderen Ländern.
- Microsoft Windows, Windows NT und das Windows-Logo sind Marken der Microsoft Corporation in den USA und/oder anderen Ländern.
- PC Direct ist eine Marke der Ziff Communications Company in den USA und/oder anderen Ländern.
- SET und das SET-Logo sind Marken der SET Secure Electronic Transaction LLC.
- UNIX ist eine eingetragene Marke der Open Group in den USA und/oder anderen Ländern.
- Marken anderer Unternehmen/Hersteller werden anerkannt.

Vierte Ausgabe (März 2003)

Diese Ausgabe betrifft Version 1.3 von WebSphere MQ Internet Pass-Thru (Programmnummer 5639-L92) und alle nachfolgenden Releases und Änderungen, sofern in neuen Ausgaben nicht anders erwähnt.

Diese Veröffentlichung ist eine Übersetzung des Handbuchs

IBM WebSphere MQ Internet Pass-Thru Version 1.3,

IBM Form SC34-6100-01,

herausgegeben von International Business Machines Corporation, USA

© Copyright International Business Machines Corporation 2000, 2003

© Copyright IBM Deutschland GmbH 2003

Informationen, die nur für bestimmte Länder Gültigkeit haben und für Deutschland, Österreich und die Schweiz nicht zutreffen, wurden in dieser Veröffentlichung im Originaltext übernommen.

Möglicherweise sind nicht alle in dieser Übersetzung aufgeführten Produkte in Deutschland angekündigt und verfügbar; vor Entscheidungen empfiehlt sich der Kontakt mit der zuständigen IBM Geschäftsstelle.

Änderung des Textes bleibt vorbehalten.

Herausgegeben von:

SW TSC Germany

Kst. 2877

März 2003

Inhaltsverzeichnis

Abbildungsverzeichnis	v	Kapitel 8. Java Security Manager und Sicherheitsexits	31
Vorwort	vii	Java Security Manager	31
WebSphere MQ Internet Pass-Thru - Beschreibung	vii	Sicherheitsexit	32
Zielgruppe	vii	Klasse 'com.ibm.mq.ipt.SecurityExit'	34
Erforderliche Kenntnisse	vii	Klasse 'com.ibm.mq.ipt.SecurityExitResponse'	37
Voraussetzungen	viii	Tracefunktion.	38
Eingabehilfen	viii	Kapitel 9. Port-Adresssteuerung	39
Zusammenfassung der Änderungen	xi	Port-Adresssteuerung	39
Änderungen in dieser Ausgabe (SC12-3116-01)	xi	Multihomed-Systeme	39
Änderungen in der dritten Ausgabe (SC12-3116-00)	xi	Kapitel 10. Weitere Sicherheitsüberlegungen	41
Änderungen in der zweiten Ausgabe.	xii	Weitere Sicherheitsüberlegungen	41
Kapitel 1. WebSphere MQ Internet Pass-Thru - Einführung	1	Kapitel 11. Verschiedenes	43
Kapitel 2. Funktionsweise von WebSphere MQ Internet Pass-Thru	7	Normale Beendigung und Fehlerbedingungen.	43
Funktionsweise von WebSphere MQ Internet Pass-Thru - Übersicht	7	Nachrichtensicherheit	43
Unterstützte Kanalkonfigurationen	8	Verbindungsprotokolle.	43
Kapitel 3. HTTP-Unterstützung	9	Kapitel 12. Upgrade von der früheren Version	45
HTTPS	10	Neue Konfigurationsoptionen	45
Servlet	10	Kapitel 13. Internet Pass-Thru unter Windows installieren	47
Kapitel 4. Socks-Unterstützung	13	Dateien herunterladen und installieren	47
Clustering	13	WebSphere MQ Internet Pass-Thru einrichten	48
Kapitel 5. SSL-Übersicht und -Unterstützung	15	WebSphere MQ Internet Pass-Thru über die Befehlszeile starten	48
SSL-Handshake	16	Verwaltungsclient über die Befehlszeile starten	49
WebSphere MQ Internet Pass-Thru und SSL	17	Ein Windows-Dienststeuerungsprogramm verwenden	50
Vertrauenseinstellungen	17	Internet Pass-Thru als Windows-Dienst deinstallieren	50
SSL testen	18	WebSphere MQ Internet Pass-Thru deinstallieren	50
SSL-Fehlernachrichten	18	Kapitel 14. WebSphere MQ Internet Pass-Thru unter Sun Solaris installieren	51
LDAP und CRLs	20	Dateien herunterladen und installieren	51
Advanced Encryption Standard.	21	WebSphere MQ Internet Pass-Thru einrichten	52
Zertifikate aus einer Schlüsselringdatei auswählen	22	WebSphere MQ Internet Pass-Thru über die Befehlszeile starten	52
Schlüsselringkennwort verschlüsseln	22	WebSphere Internet Pass-Thru automatisch starten	53
KeyMan	22	Verwaltungsclient über die Befehlszeile starten	53
Unterstützte Tokens	23	WebSphere MQ Internet Pass-Thru deinstallieren	54
Unterstützte Standarddatenformate	24	Kapitel 15. Internet Pass-Thru unter AIX installieren	55
KeyMan-FAQs	25	Dateien herunterladen und installieren	55
Kapitel 6. Servicequalität (Quality of Service)	27		
Servicequalität (QoS = Quality of Service)	27		
Kapitel 7. Network Dispatcher	29		
Unterstützung für Network Dispatcher	29		

WebSphere MQ Internet Pass-Thru einrichten	56
WebSphere MQ Internet Pass-Thru über die Befehlszeile starten	56
WebSphere Internet Pass-Thru automatisch starten	57
Verwaltungsclient über die Befehlszeile starten	57
WebSphere MQ Internet Pass-Thru deinstallieren	58

Kapitel 16. WebSphere MQ Internet Pass-Thru unter HP-UX installieren 59

Dateien herunterladen und installieren	59
WebSphere MQ Internet Pass-Thru einrichten	60
WebSphere MQ Internet Pass-Thru über die Befehlszeile starten	60
WebSphere Internet Pass-Thru automatisch starten	61
Verwaltungsclient über die Befehlszeile starten	62
WebSphere MQ Internet Pass-Thru deinstallieren	62

Kapitel 17. WebSphere MQ Internet Pass-Thru unter Linux installieren 63

Dateien herunterladen und installieren	63
WebSphere MQ Internet Pass-Thru einrichten	64
WebSphere MQ Internet Pass-Thru über die Befehlszeile starten	65
WebSphere Internet Pass-Thru automatisch starten	65
Verwaltungsclient über die Befehlszeile starten	66
WebSphere MQ Internet Pass-Thru deinstallieren	66

Kapitel 18. Generische UNIX-Installation 67

Dateien herunterladen und installieren	67
WebSphere MQ Internet Pass-Thru einrichten	68
WebSphere MQ Internet Pass-Thru über die Befehlszeile starten	69
WebSphere Internet Pass-Thru automatisch starten	70
Verwaltungsclient über die Befehlszeile starten	70
WebSphere MQ Internet Pass-Thru deinstallieren	70

Kapitel 19. WebSphere MQ Internet Pass-Thru verwalten und konfigurieren. 71

Verwaltungsclient von WebSphere MQ Internet Pass-Thru verwenden	71
Verwaltungsclient starten	71
MQIPT verwalten	72
Vererbung von Eigenschaften	73
Optionen im Menü 'Datei'	73
Optionen im Menü 'MQIPT'.	73
Optionen im Menü 'Hilfe'	75
Zeilenmodusbefehle von WebSphere MQ Internet Pass-Thru verwenden	75
WebSphere MQ Internet Pass-Thru über Zeilenmodusbefehle verwalten	75
Referenzinformationen zur Konfiguration	76
Eigenschaften - Übersicht.	77

Referenzinformationen zum Abschnitt 'global'.	81
Referenzinformationen zum Abschnitt 'route'	82

Kapitel 20. WebSphere MQ Internet Pass-Thru - Erste Schritte 97

Voraussetzungen	97
Beispielkonfigurationen	98
Installationsfunktionstest	99
SSL-Serverauthentifizierung	100
SSL-Clientauthentifizierung.	102
HTTP-Proxy-Konfiguration	105
Zugriffsteuerung konfigurieren	107
Quality of Service (QoS) konfigurieren	110
SOCKS-Proxy konfigurieren	113
SOCKS-Client konfigurieren	116
SSL-Testzertifikate erstellen.	118
MQIPT-Servlet konfigurieren	119
HTTPS-Konfiguration	122
Unterstützung für MQIPT-Clustering konfigurieren	126
Eine Schlüsselringdatei erstellen	130
Port-Adressen zuordnen.	132
LDAP-Server verwenden	134
SSL-Proxy-Modus	137
Apache-Anweisung 'rewrite'	140
Sicherheitsexit	143
Sicherheitsexit weiterleiten	145
Dynamischer Exit bei nur einer Route	149

Kapitel 21. WebSphere MQ Internet Pass-Thru - Wartung und Pflege 153

Verwaltung	153
Fehlerbestimmung.	153
WebSphere MQ Internet Pass-Thru automatisch starten.	155
Durchgehende Verbindungen überprüfen	155
Tracefehler	155
Fehlermeldung	156
Durchsatzverbesserung	156
Verwaltung von Threads-Pools	156
Verbindungs-Threads.	156
Zeitlimit für Inaktivität	156

Kapitel 22. Nachrichten 157

Anhang. Bemerkungen 177

Marken	177
------------------	-----

Literaturverzeichnis 179

Index 181

Kommentare an IBM senden 185

Abbildungsverzeichnis

1. Beispiel für den Einsatz von MQIPT als Kanal-	24. SOCKS-Clientnetzplan	116
konzentrator	25. SOCKS-Clientkonfiguration	116
2. Beispiel für den Einsatz von MQIPT mit einer	26. Servlet-Netzplan	119
“Demilitarized Zone”	27. Servlet-Konfiguration	120
3. Beispiel für MQIPT und HTTP-Tunnelung	28. HTTPS-Netzplan	122
4. Beispiel für einen MQIPT mit SSL	29. HTTPS-Konfiguration	123
5. WebSphere MQ-Topologie mit möglichen	30. Clustering-Netzplan	126
MQIPT-Konfigurationen.	31. Clustering-Konfiguration.	127
6. MQIPT-Clusterunterstützung.	32. Netzplan für Port-Zuordnung	132
7. Verwendung von Network Dispatcher mit	33. Konfiguration für Port-Zuordnung	132
MQIPT	34. Netzplan für LDAP-Server	134
8. Fenster beim erstmaligen Zugriff auf einen	35. Konfiguration für LDAP-Server	135
MQIPT	36. Netzplan für SSL-Proxy-Modus	137
9. Eine Route hinzufügen.	37. Konfiguration für SSL-Proxy-Modus	138
10. IVT-Netzplan	38. Netzplan für Apache-Anweisung ‘rewrite’	140
11. IVT-Konfiguration	39. Konfiguration für Apache-Anweisung ‘rewri-	141
12. SSL-Servernetzplan	te’	141
13. SSL-Serverauthentifizierung.	40. Netzplan für Sicherheitsexit.	144
14. SSL-Clientnetzplan.	41. Konfiguration für Sicherheitsexit	144
15. SSL-Clientauthentifizierung	42. Netzplan für Sicherheitsexit-Weiterleitung	146
16. HTTP-Proxy-Netzplan	43. Konfiguration für Sicherheitsexit-Weiterlei-	147
17. HTTP-Proxy-Konfiguration	tung	147
18. Netzplan für die Zugriffssteuerung	44. Netzplan für dynamischen Exit bei nur einer	149
19. Konfiguration der Zugriffssteuerung	Route	149
20. QoS-Netzplan	45. Konfiguration für dynamischen Exit bei nur	150
21. QoS-Konfiguration	einer Route	150
22. Netzplan für SOCKS-Proxy	46. Fehlerbestimmung - Ablaufdiagramm	154
23. SOCKS-Proxy-Konfiguration		

Vorwort

WebSphere MQ Internet Pass-Thru - Beschreibung

WebSphere MQ Internet Pass-Thru war zuvor unter der Bezeichnung MQSeries Internet Pass-Thru bekannt. Im vorliegenden Buch wird MQSeries ab jetzt unter der Bezeichnung WebSphere MQ geführt. Da jedoch nicht in allen MQSeries-Handbüchern sofort eine Namensumstellung auf 'WebSphere MQ' erfolgt, wird es für einige Zeit sowohl Verweise auf MQSeries als auch auf WebSphere MQ geben.

IBM WebSphere MQ Internet Pass-Thru bietet Folgendes:

- Stellt eine Erweiterung des WebSphere MQ-Basisprodukts dar, mit deren Hilfe Messaging-Lösungen zwischen räumlich getrennten Standorten über das Internet implementiert werden können.
- Erleichtert den Durchgang der WebSphere MQ-Kanalprotokolle durch Firewalls (in beide Richtungen) und vereinfacht die Verwaltung, indem die Protokolle in HTTP getunnelt werden oder indem es als Proxy fungiert.
- Arbeitet als Standalone-Service, der WebSphere MQ-Nachrichtenflüsse empfangen und weiterleiten kann. Auf dem System, auf dem WebSphere MQ Internet Pass-Thru ausgeführt wird, muss kein WebSphere MQ-Warteschlangenmanager installiert sein.
- Unterstützt die Bereitstellung von unternehmensübergreifenden Transaktionen unter Verwendung von WebSphere MQ.
- Ermöglicht die Verwendung bereits vorhandener WebSphere MQ-Anwendungen durch eine Firewall hindurch, ohne dass Änderungen erforderlich sind.
- Stellt über den Zugriff auf mehrere WS-Manager einen zentralen Steuerungspunkt zur Verfügung.
- Erlaubt die Verschlüsselung sämtlicher Daten.
- Protokolliert alle Verbindungsversuche.

Aus praktischen Gründen wird im vorliegenden Handbuch anstelle von 'WebSphere MQ Internet Pass-Thru' häufig auch "MQIPT" verwendet.

Zielgruppe

Dieses Handbuch richtet sich an Systemdesigner, technische WebSphere MQ-Administratoren sowie Firewall- und Netzadministratoren.

Erforderliche Kenntnisse

Es werden gute Kenntnisse in folgenden Bereichen vorausgesetzt:

- Verwaltung von WebSphere MQ-Warteschlangenmanagern und Nachrichtenkanälen (siehe Beschreibung in *WebSphere MQ System Administration Guide* und *WebSphere MQ Intercommunication*)
- Implementierung von Firewalls
- Internet Protocol-Routing/-Networking
- IBM Network Dispatcher (für Lastausgleich und bessere Verfügbarkeit)
- IBM WebSphere Application Server

Voraussetzungen

Dieses Release von Internet Pass-Thru kann auf den folgenden Plattformen eingesetzt werden:

- Windows NT V4.0 mit Service Pack 6
- Windows 2000
- Windows XP
- Sun Solaris
- AIX V5.1
- HP-UX 11
- Linux

Für den MQIPT-Server ist J2SE V1.4.0 Runtime (JRE) erforderlich. Zum Erstellen eines Sicherheitsexits wird SDK V1.4.0 benötigt.

Als einziges Netzprotokoll wird TCP/IP unterstützt.

Für die Onlinehilfe des Verwaltungsclients ist der Netscape-Browser erforderlich.

Eingabehilfen

In der grafischen Benutzerschnittstelle, dem Verwaltungsclient, wurden Navigations- und Aufrufmöglichkeiten berücksichtigt. Alle verfügbaren Funktionen können direkt ohne Maus ausgeführt werden, und zwar unter Verwendung der entsprechenden Tastaturtasten. So können Sie im Bildschirm ganz normal über die Tabulator-, Umschalt-/Tabulator, Steuer-/Tabulator- und die Cursor-Tasten navigieren. Anstelle des Mausclicks drücken Sie zunächst die entsprechende Taste und anschließend die Eingabetaste.

Menüoptionen können entweder über die Kombination von Tabulator- und Cursor-Tasten ausgewählt werden oder über die Direktaufruftasten, die für alle Optionen vorhanden sind. Beispielsweise kann die grafische Benutzerschnittstelle geschlossen werden, indem Sie zunächst **Alt-f** und anschließend **Alt-q** (Datei -> Verlassen) auswählen. Nach Auswahl einer Menüoption kann diese mit Hilfe der Eingabetaste aufgerufen werden.

Die Navigation in der Baumstruktur ist mit Hilfe der Cursor-Tasten möglich. Insbesondere können MQIPT-Knoten mit den rechten und linken Cursor-Tasten geöffnet bzw. geschlossen werden, wodurch die Routen angezeigt bzw. verdeckt werden.

Der Status von Kontrollkästchen kann nach der Auswahl durch die Leertaste geändert werden. Felder können für Änderungen über die Eingabetaste ausgewählt werden.

Darstellung und Funktionsweise

Idealerweise sollte sich die grafische Benutzerschnittstelle in Darstellung und Funktionsweise ganz der Umgebung anpassen. Da dies nicht immer möglich ist, können Sie die Darstellung und Funktionsweise der GUI mit Hilfe einer Konfigurationsdatei entsprechend Ihren Bedürfnissen anpassen. Diese Konfigurationsdatei (custom.properties) sollte im Unterverzeichnis bin abgelegt werden.

Mit Hilfe dieser Konfigurationsdatei kann Folgendes angepasst werden:

- Die Vordergrundfarbe (Farbe des Textes)
- Die Hintergrundfarbe
- Die Schriftart des Textes
- Der Schriftschnitt (Standard, Fett, Kursiv, Fett Kursiv)

Eine Beispielkonfigurationsdatei (`customSample.properties`) wird zur Verfügung gestellt; sie enthält Hinweise, wie Sie diese Datei ändern können. Es wird vorgeschlagen, dass Sie diese Datei in das Verzeichnis `bin/custom.properties` kopieren und die erforderlichen Änderungen vornehmen.

Zusammenfassung der Änderungen

Dieser Abschnitt beschreibt Änderungen in dieser Ausgabe von WebSphere MQ Internet Pass-Thru. Änderungen gegenüber der vorherigen Ausgabe sind durch vertikale Linien links neben dem Text markiert.

Änderungen in dieser Ausgabe (SC12-3116-01)

Diese Version von WebSphere MQ Internet Pass-Thru beinhaltet die folgenden funktionalen Erweiterungen:

- Sicherheitsexit zur Steuerung von Clientverbindungsanforderungen
- LDAP-Unterstützung für CRLs und ARLs
- Verschlüsselung von Schlüsselringkennwörtern
- Zertifikatauswahl aus einem Schlüsselring
- Neue AES Cipher Suites
- Generisches UNIX-Plattenimage
- Steuerung der Aktion zum Routenneustart
- AIX- und HP-UX-Plattformen unterstützen jetzt Java 1.4

Änderungen in der dritten Ausgabe (SC12-3116-00)

Diese Version von WebSphere MQ Internet Pass-Thru beinhaltet die folgenden funktionalen Erweiterungen:

- Steuerung der Adresszuordnung für abgehenden Port
- Beispielkonfigurationen
- Verbesserte SSL-Tracefunktion
- Java Security Manager
- Dienstprogramm KeyMan zur Verwaltung von Zertifikaten und Schlüsselringdateien
- Linux-Unterstützung, einschließlich Servicequalität (QoS = Quality of Service) für WebSphere MQ-Nachrichten
- Bereitstellung eines NLS-Installationsimage für Windows-Plattformen
- Bei Eigenschaftennamen wird jetzt die Groß-/Kleinschreibung nicht mehr beachtet
- Servlet-Version
- SOCKS-Client- und Serverunterstützung
- SSL-Proxy-Modus
- Unterstützung für Multihomed-System
- Anzeige des Datenverkehrsstatus für den Verwaltungsclient
- WebSphere MQ-Clusterunterstützung

Änderungen in der zweiten Ausgabe

Diese Version von WebSphere MQ Internet Pass-Thru beinhaltet die folgenden funktionalen Erweiterungen:

- AIX, HP-UX und Windows 2000 als Plattformen für MQIPT
- HTTP-Proxy-Unterstützung
- Unterstützung für Secure Socket Layer (SSL)
- Möglichkeit der Kommunikation von MQIPT mit einem anderen externen MQIPT- oder MQSeries-Server über einen SOCKS-Proxy
- Verwendung einer Verwaltungsclient-GUI zur einfacheren Verwaltung eines oder mehrerer MQIPTs
- Unterstützung für IBM Network Dispatcher
- Kleine Verbesserungen der Tracefunktion
- Kleine Verbesserungen des Befehls 'mqiptAdmin'

Kapitel 1. WebSphere MQ Internet Pass-Thru - Einführung

WebSphere MQ Internet Pass-Thru stellt eine funktionale Erweiterung des WebSphere MQ-Basisprodukts dar. MQIPT arbeitet als Standalone-Service, der WebSphere MQ-Nachrichtenflüsse zwischen zwei WebSphere MQ-Warteschlangenmanagern oder zwischen einem WebSphere MQ-Client und einem WebSphere MQ-Warteschlangenmanager empfangen und weiterleiten kann. MQIPT ermöglicht diese Verbindung, wenn sich Client und Server nicht in demselben physischen Netz befinden.

In den Kommunikationspfad zwischen zwei WebSphere MQ-Warteschlangenmanagern bzw. zwischen einem WebSphere MQ-Client und einem WebSphere MQ-Warteschlangenmanager können ein oder mehrere MQIPTs eingesetzt werden. Diese ermöglichen den beiden WebSphere MQ-Systemen den Austausch von Nachrichten, ohne dass zwischen ihnen eine direkte TCP/IP-Verbindung erforderlich ist. Dies ist dann hilfreich, wenn die Firewall-Konfiguration keine direkte TCP/IP-Verbindung zwischen den beiden Systemen erlaubt.

MQIPT überwacht einen oder mehrere TCP/IP-Ports auf ankommende Verbindungen, über die entweder normale WebSphere MQ-Nachrichten, in HTTP verpackte WebSphere MQ-Nachrichten oder unter Verwendung von SSL (Secure Sockets Layer) verschlüsselte Nachrichten übertragen werden. Das Produkt kann mehrere gleichzeitige Verbindungen handhaben.

Der WebSphere MQ-Kanal, der die ursprüngliche TCP/IP-Verbindungsanforderung ausgibt, wird als "Aufrufer" bezeichnet, der Kanal, zu dem die Verbindung hergestellt werden soll, als "Responder", und der Warteschlangenmanager, der eigentlich erreicht werden soll, als "Zielwarteschlangenmanager".

Es wird davon ausgegangen, dass MQIPT wie folgt eingesetzt wird:

- MQIPT kann als Kanalkonzentrator verwendet werden; dadurch nimmt eine Firewall Kanäle zu bzw. von mehreren unterschiedlichen Hosts als einen einzigen Kanal zum bzw. vom MQIPT-Host wahr. Dies erleichtert die Definition und Verwaltung der Filterregeln für die Firewall.

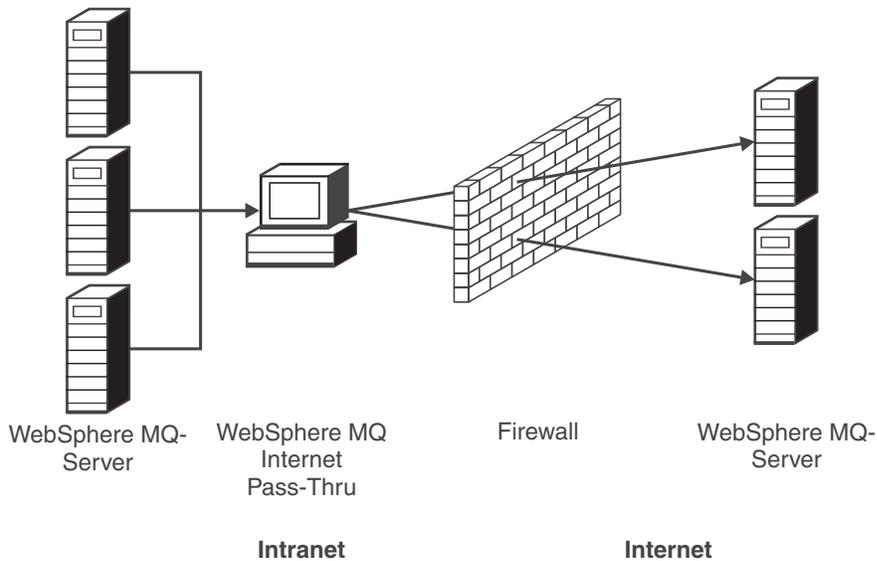


Abbildung 1. Beispiel für den Einsatz von MQIPT als Kanalkonzentrator

- Bei Einsatz auf einer Maschine mit einer bekannten und gesicherten IP-Adresse (IP = Internet-Protokoll) in der "Demilitarized Zone" (DMZ) einer Firewall kann MQIPT zur Überwachung ankommender WebSphere MQ-Kanalverbindungen verwendet werden, die es dann an das gesicherte Intranet weiterleitet; die innere Firewall muss dieser gesicherten Maschine die Herstellung eingehender Verbindungen gestatten. In dieser Konfiguration verhindert MQIPT, dass externe Zugriffsanforderungen die tatsächliche IP-Adresse der Maschinen im gesicherten Intranet erkennen. Damit stellt MQIPT einen einzigen zentralen Zugriffspunkt dar.

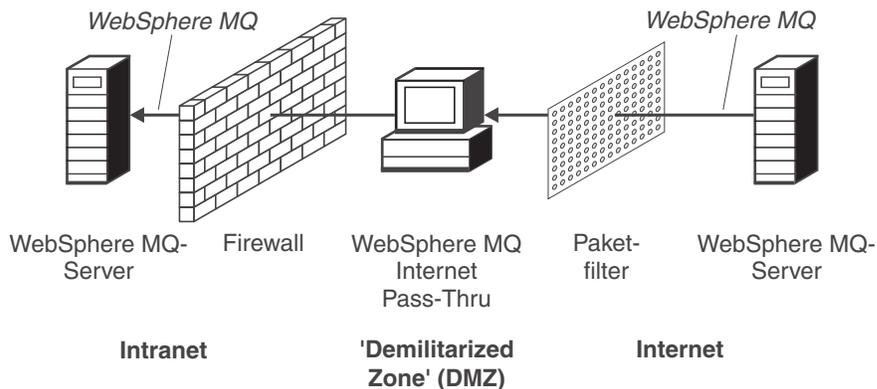


Abbildung 2. Beispiel für den Einsatz von MQIPT mit einer "Demilitarized Zone"

- Werden zwei MQIPTs nebeneinander eingesetzt, können sie über HTTP oder SSL miteinander kommunizieren. Durch die HTTP-Tunnelung können Anforderungen unter Verwendung vorhandener HTTP-Proxys durch Firewalls hindurch weitergereicht werden. Der erste MQIPT fügt das WebSphere MQ-Protokoll in das HTTP-Protokoll ein, aus dem es der zweite MQIPT wieder extrahiert und an den Zielwarteschlangenmanager weiterleitet.

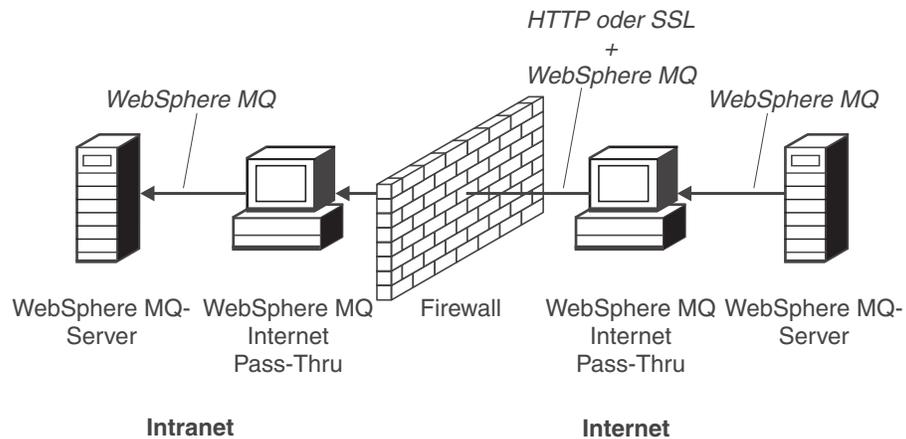


Abbildung 3. Beispiel für MQIPT und HTTP-Tunnelung

- Auf ähnliche Weise können Anforderungen verschlüsselt werden, bevor sie durch eine Firewall hindurch weitergereicht werden. Die Daten werden unter Verwendung von SSL vom ersten MQIPT ver- und vom zweiten MQIPT entschlüsselt, bevor sie an den Zielwarteschlangenmanager gesendet werden.

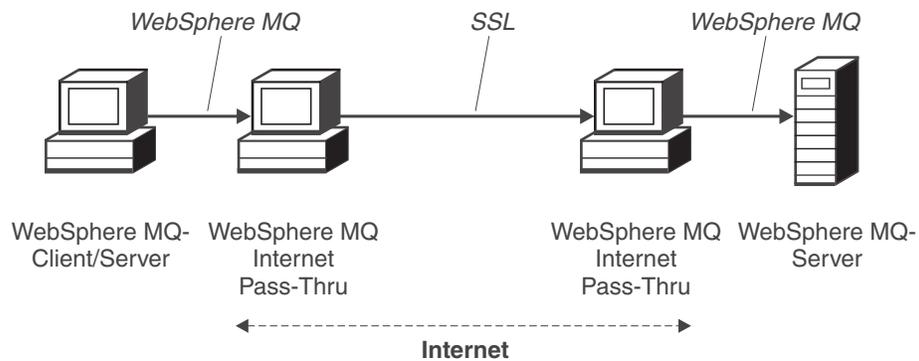


Abbildung 4. Beispiel für einen MQIPT mit SSL

MQIPT legt die Daten im Speicher ab, während sie von ihrem Ausgangspunkt an die Zieladresse weitergeleitet werden. Dabei werden keine Daten auf Platte gespeichert, mit Ausnahme des Speichers, der vom Betriebssystem auf die Festplatte umgelagert wird. MQIPT greift nur explizit auf die Festplatte zu, um die Konfigurationsdatei zu lesen und um Protokoll- und Tracesätze zu schreiben.

Sämtliche WebSphere MQ-Kanaltypen können über einen oder mehrere MQIPTs erstellt werden. Der Einsatz von MQIPTs im Kommunikationspfad hat keinerlei Auswirkungen auf die funktionalen Merkmale der verbundenen WebSphere MQ-Komponenten; allerdings können sich gewisse Auswirkungen auf die Leistung bei der Nachrichtenübertragung ergeben.

MQIPT kann zusammen mit WebSphere MQ Publish/Subscribe oder dem Nachrichtenbroker von WebSphere MQ Integrator eingesetzt werden.

In Abb. 5 auf Seite 5 sind sämtliche Konfigurationen zu sehen, die für MQIPs in einer WebSphere MQ-Topologie möglich sind. Dabei ist zu beachten, dass in der Abbildung der HTTP-Proxy, der SOCKS-Proxy und die MQIPT-Maschinen jenseits der Firewall auf der Seite der "ausgehenden Verbindungen" zeigen, wie mehrere Maschinen im Internet miteinander verbunden werden können. So kann beispielsweise eine MQIPT-Maschine Nachrichten an eine oder mehrere SOCKS- oder HTTP-Proxys oder weitere MQIPT-Maschinen weiterleiten, bevor sie ihr Ziel erreichen.

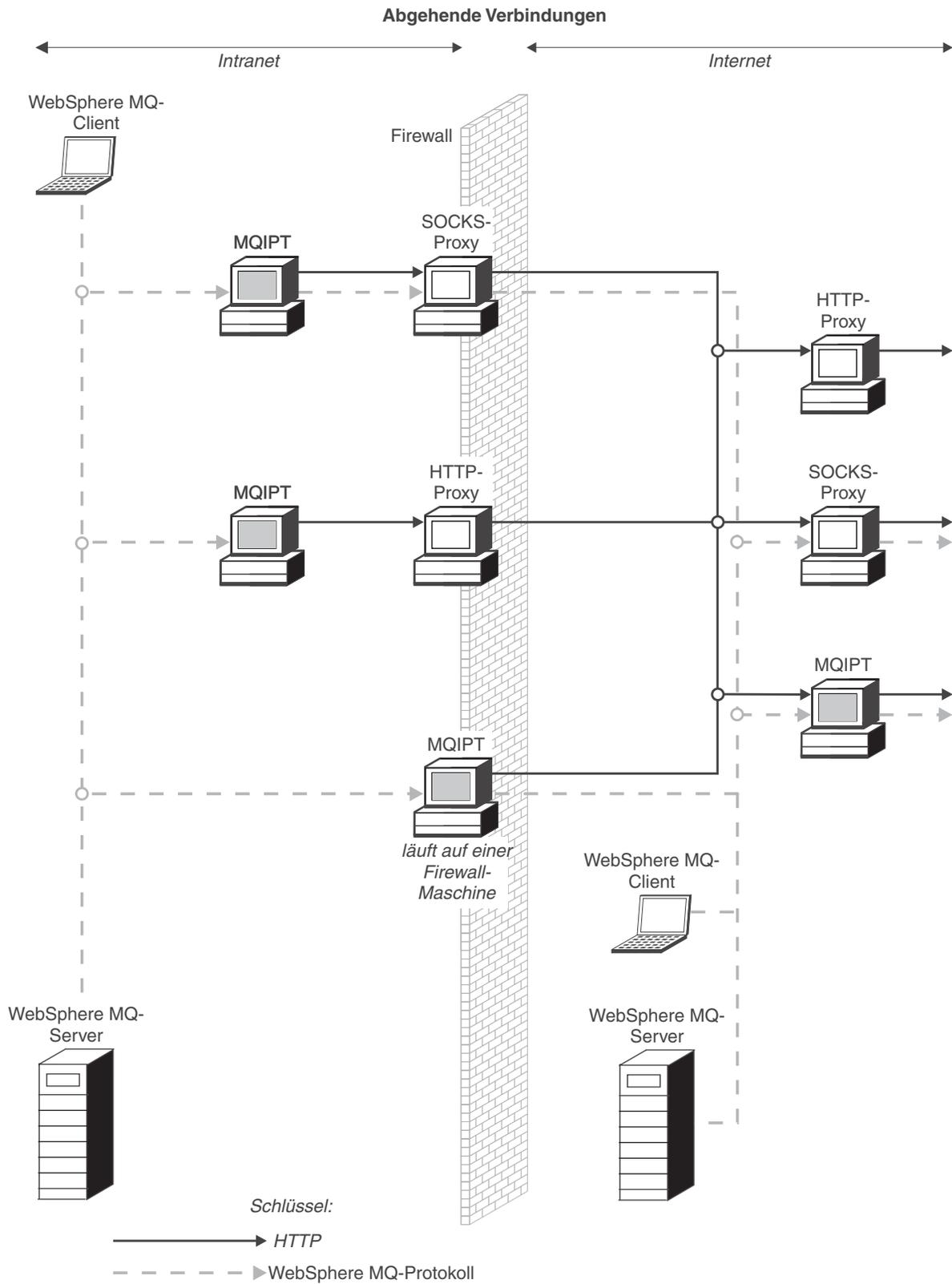


Abbildung 5. WebSphere MQ-Topologie mit möglichen MQIPT-Konfigurationen (Teil 1 von 2)

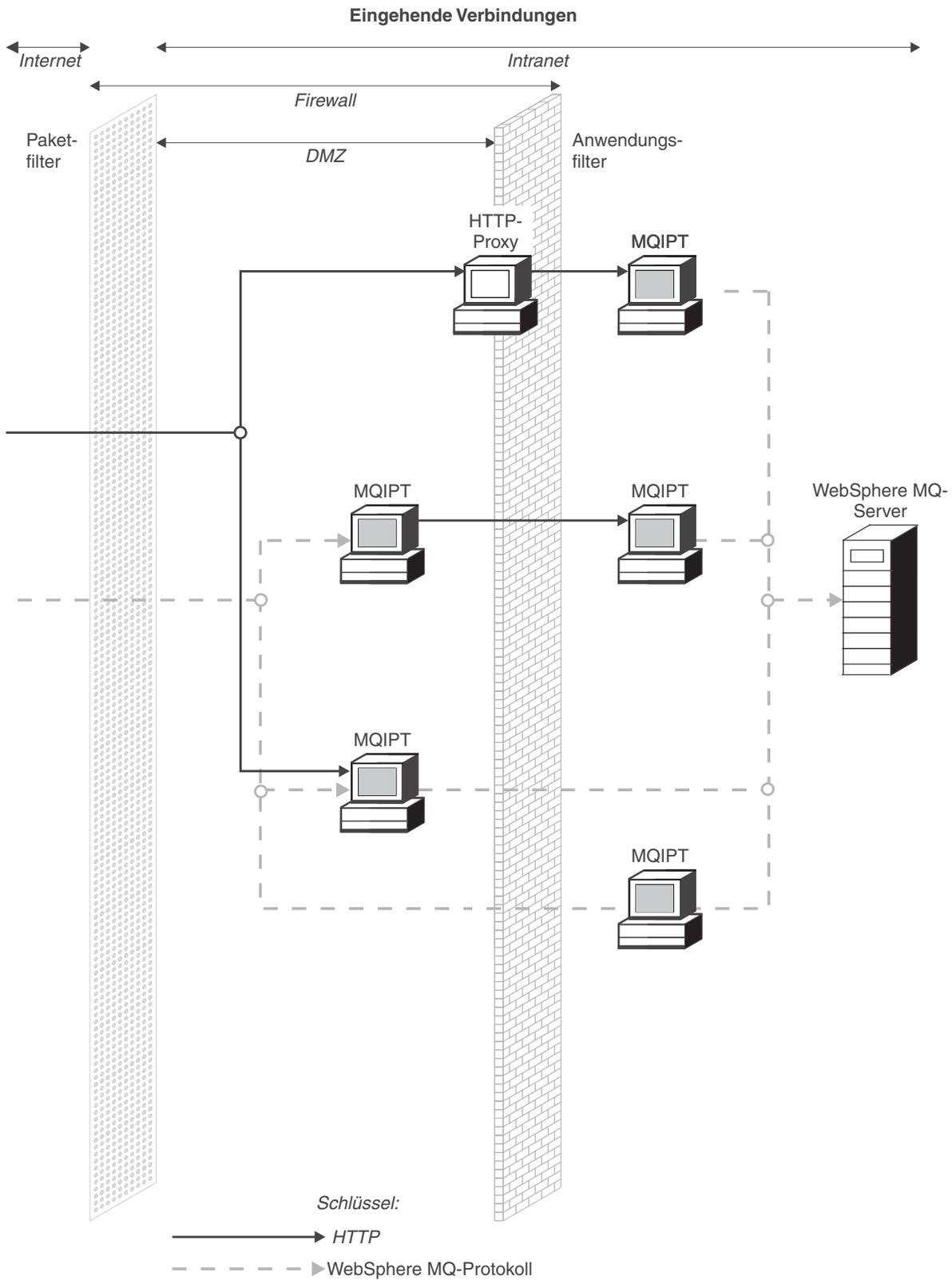


Abbildung 5. WebSphere MQ-Topologie mit möglichen MQIPT-Konfigurationen (Teil 2 von 2)

Kapitel 2. Funktionsweise von WebSphere MQ Internet Pass-Thru

Dieses Kapitel enthält eine Übersicht über die Funktionsweise von WebSphere MQ Internet Pass-Thru.

Funktionsweise von WebSphere MQ Internet Pass-Thru - Übersicht

In der einfachsten Konfiguration wird MQIPT für die Weiterleitung des WebSphere MQ-Protokolls eingesetzt. Es ist an einem TCP/IP-Port empfangsbereit und akzeptiert Verbindungsanforderungen von WebSphere MQ-Kanälen. Bei Empfang einer wohlgeformten Anforderung richtet MQIPT eine weitere TCP/IP-Verbindung zum WebSphere MQ-Zielwarteschlangenmanager ein. Anschließend übergibt es alle Protokollpakete, die es von der ankommenden Verbindung empfängt, an den Zielwarteschlangenmanager und gibt umgekehrt die Protokollpakete vom Zielwarteschlangenmanager an die ursprüngliche ankommende Verbindung zurück.

Dabei kommt es zu keinen Änderungen am WebSphere MQ-Protokoll (Client /Server oder WS-Manager/WS-Manager), da keine der beiden Seiten den zwischen- geschalteten MQIPT direkt wahrnimmt; daher sind keine neuen Versionen des WebSphere MQ-Clientcodes bzw. -Servercodes erforderlich.

Damit MQIPT genutzt werden kann, muss der aufrufende Kanal zunächst so konfiguriert werden, dass er den Hostnamen und den Port von MQIPT, und nicht den Hostnamen und den Port des Zielwarteschlangenmanagers verwendet. Dies wird über die Eigenschaft CONNAME des WebSphere MQ-Kanals definiert. MQIPT liest die ankommenden Daten und gibt sie einfach an den Zielwarteschlangenmanager weiter. Ebenso werden auch andere Konfigurationsfelder (z. B. für die Benutzer-ID und das Kennwort in einem Client-/Serverkanal) an den Zielwarteschlangenmanager übergeben.

MQIPT kann so eingesetzt werden, dass der Zugriff auf einen oder mehrere Zielwarteschlangenmanager möglich ist. Da MQIPT dazu wissen muss, zu welchem WS-Manager eine Verbindung hergestellt werden soll, legt MQIPT wie im nächsten Absatz beschrieben den betreffenden WS-Manager anhand der Nummer des ankommenden TCP/IP-Ports fest.

Soll der Zugriff auf mehrere Zielwarteschlangen möglich sein, muss MQIPT für die Überwachung mehrerer TCP/IP-Ports konfiguriert werden. Jeder dieser überwachten Ports wird über eine MQIPT-Route einem Zielwarteschlangenmanager zugeordnet. Der MQIPT-Administrator kann bis zu 100 solcher Routen festlegen, von denen jede einen überwachten TCP/IP-Port dem Hostnamen und dem Port des Zielwarteschlangenmanagers zuordnet. Dadurch ist der Hostname (die IP-Adresse) des Zielwarteschlangenmanagers für den Ursprungskanal immer unsichtbar. Jede Route kann mehrere Verbindungen zwischen dem überwachten Port und dem Ziel handhaben, wobei diese Verbindungen unabhängig voneinander laufen.

MQIPT verwendet eine Konfigurationsdatei mit dem Namen 'mqipt.conf'. Diese Datei enthält Definitionen aller Routen und der ihnen zugeordneten Eigenschaften. Weitere Informationen zu dieser Datei finden Sie in Kapitel 19, „WebSphere MQ Internet Pass-Thru verwalten und konfigurieren“, auf Seite 71.

Beim Start von MQIPT werden alle in der Konfigurationsdatei definierten Routen eingerichtet. An der Systemkonsole werden Nachrichten mit dem Status der einzelnen Routen angezeigt. Wird für eine Route die Nachricht MQCPI078 angezeigt, ist diese Route zur Annahme von Verbindungsanforderungen bereit.

Unterstützte Kanalkonfigurationen

Es werden alle WebSphere MQ-Kanaltypen unterstützt, die Konfiguration wird jedoch auf TCP/IP-Verbindungen beschränkt. Ein WebSphere MQ-Client oder -Warteschlangenmanager nimmt den MQIPT als Zielwarteschlangenmanager wahr. Sind für eine Kanalkonfiguration ein Zielhost und eine Port-Nummer erforderlich, werden der Hostname und die Nummer des Listener-Ports von MQIPT angegeben.

Client-/Serverkanäle

MQIPT übernimmt die Überwachung auf ankommende Verbindungsanforderungen von Clients, die es dann weiterleitet, entweder unter Verwendung der HTTP-Tunnelung oder des SSL-Protokolls, oder als standardmäßige WebSphere MQ-Protokollpakete. Bei Verwendung der HTTP-Tunnelung oder des SSL-Protokolls leitet MQIPT die Anforderungen an einen zweiten MQIPT weiter. Wird keine HTTP-Tunnelung verwendet, übergibt es die Anforderungen über eine Verbindung an eine Adresse, die es als Zielwarteschlangenmanager sieht (auch wenn es sich dabei um einen anderen MQIPT handeln kann). Wenn der Zielwarteschlangenmanager die Clientverbindung akzeptiert, werden die Pakete zwischen Client und Server übertragen.

Clustersender-/Clusterempfängerkanäle

Beim Empfang einer ankommenden Anforderung von einem Clustersenderkanal geht MQIPT davon aus, dass der WS-Manager SOCKSifiziert ist und die eigentliche Zieladresse beim SOCKS-Handshake übergeben wird. MQIPT leitet die Anforderung wie bei Clientverbindungskanälen an den nächsten MQIPT oder den Zielwarteschlangenmanager weiter. Dazu gehören auch automatisch definierte Clustersenderkanäle.

Sender-/Empfängerkanäle

Beim Empfang einer ankommenden Anforderung von einem Senderkanal leitet MQIPT diese Anforderung wie bei Clientverbindungskanälen an den nächsten MQIPT oder an den Zielwarteschlangenmanager weiter. Der Zielwarteschlangenmanager überprüft die ankommenden Anforderungen und startet bei Bedarf den Empfängerkanal. Die gesamte Kommunikation zwischen Sender- und Empfängerkanal (einschließlich der Sicherheitsdatenflüsse) wird übertragen.

Requester-/Serverkanäle

Diese Kombination wird wie die oben beschriebenen Kanaltypen behandelt. Die Verbindungsanforderung wird vom Serverkanal im Zielwarteschlangenmanager überprüft.

Requester-/Senderkanäle

Die 'Rückruf'konfiguration ist hilfreich, wenn zwei WS-Manager keine direkte Verbindungen zueinander aufbauen dürfen, beide jedoch eine Verbindung zu einem MQIPT herstellen und Verbindungen von diesem akzeptieren können.

Server-/Requester- und Server-/Empfängerkanäle

Diese werden von MQIPT wie Sender-/Empfängerkonfigurationen gehandhabt.

Kapitel 3. HTTP-Unterstützung

MQIPT kann so konfiguriert werden, dass die Datenpakete in Form von HTTP-Anforderungen übergeben werden. MQIPT unterstützt die HTTP-Tunnelung sowohl mit als auch ohne Chunking.

Da WebSphere MQ-Kanäle heutzutage keine HTTP-Anforderungen akzeptieren, ist ein zweiter MQIPT erforderlich, der die HTTP-Anforderungen empfängt und wieder in normale WebSphere MQ-Protokollpakete zurückverwandelt. Dazu entfernt MQIPT zunächst den HTTP-Header und wandelt dann das ankommende Paket in ein standardmäßiges WebSphere MQ-Protokollpaket um, bevor es an den Zielwarteschlangenmanager übergeben wird.

Bei Verwendung von HTTP-Tunnelung ohne Chunking wird für jede HTTP-Anforderung eine HTTP-Antwort an den ersten MQIPT zurückgesendet. Dabei kann es sich um eine Antwort vom Zielwarteschlangenmanager oder um eine Pseudobestätigung handeln. Müssen beide WebSphere MQ-Systeme eine Reihe aufeinanderfolgender WebSphere MQ-Protokollpakete senden (wie dies z. B. bei der Übertragung großer Nachrichten der Fall ist), werden mehrere HTTP-Anforderungs-/Antwortpaare für die Datenübertragung verwendet. Dazu fügt MQIPT zusätzliche Anforderungs- bzw. Antwortflüsse ein.

Bei Verwendung von HTTP-Tunnelung mit Chunking wird nur das erste Paket in einem HTTP-Header verpackt. Alle nachfolgenden Pakete, einschließlich des letzten Pakets, verfügen über Chunking-Header. Dadurch muss nicht erst auf eine Pseudobestätigung des zweiten MQIPTs gewartet werden; dies ergibt eine geringfügig bessere Systemleistung als die HTTP-Tunnelung ohne Chunking.

Bei Verwendung von HTTP zwischen zwei MQIPTs ist die TCP/IP-Verbindung, auf der die HTTP-Anforderungen und -Antworten übertragen werden, permanent und bleibt für die gesamte Lebensdauer des Nachrichtenkanals offen. Das bedeutet, dass die TCP/IP-Verbindung zwischen Anforderungs-/Antwortpaaren nicht von den MQIPTs beendet wird.

Bei der Kommunikation zweier MQIPTs über HTTP kann eine HTTP-Anforderung unter Umständen für einen längeren Zeitraum unbearbeitet bleiben. Dies ist z. B. bei einem Requester/Server-Kanal möglich, wenn die Serverseite auf das Eintreffen neuer Nachrichten in der Übertragungswarteschlange wartet. Das WebSphere MQ-Kanalprotokoll stellt ein Verfahren zur Ausgabe von **Überwachungssignalen** zur Verfügung, bei dem die wartende Seite gezwungen wird, in regelmäßigen Abständen ein Überwachungssignal an den Partner zu schicken (Standardintervall sind 5 Minuten); dieses Überwachungssignal wird von MQIPT als HTTP-Antwort verwendet. Dieses kanalspezifische Überwachungssignal darf nicht deaktiviert oder auf einen übermäßig hohen Wert gesetzt werden, da dies in einigen Firewalls zu Zeitüberschreitungsproblemen führen könnte.

Einige HTTP-Proxys verfügen über eigene Eigenschaften zur Steuerung permanenter Verbindungen, wie beispielsweise die mögliche Anzahl an Anforderungen auf einer permanenten Verbindung. Der HTTP-Proxy muss daher das HTTP-Protokoll 1.1 unterstützen.

Bei Verwendung des IBM WebSphere Caching Proxy müssen die folgenden Eigenschaften neu festgelegt werden:

- **MaxPersistenceRequest** (Max. Anzahl Anforderungen über permanente Verbindung) muss auf einen hohen Wert (z. B. 5000) gesetzt werden.
- **PersistentTimeout** (Zeitlimit für permanente Verbindung) muss auf einen hohen Wert (z. B. 12 Stunden) gesetzt werden.
- **ProxyPersistence** (Proxy-Permanenz) muss auf Ein gesetzt sein.

Unter „HTTP-Proxy-Konfiguration“ auf Seite 105 finden Sie ein Beispiel für die Verwendung von HTTP.

HTTPS

HTTPS kann auf einer HTTP-Verbindung verwendet werden, indem in MQIPT durch Ausgabe der Clientverbindung die Routeneigenschaften 'HTTPS' und 'SSLClient' aktiviert werden. MQIPT muss auf das Zertifikat der vertrauenswürdigen Zertifizierungsstelle, das zur Authentifizierung des HTTP-Zielproxys/-servers verwendet wird, zugreifen können. Mit Hilfe der Eigenschaft 'SSLClientCAKeyring' kann die Schlüsselringdatei, die das Zertifikat der vertrauenswürdigen Zertifizierungsstelle enthält, definiert werden.

Eine typische Konfiguration für HTTPS verwendet einen lokalen HTTP-Proxy zur Tunnelung einer Firewall nach außen und Herstellung einer Verbindung mit einem fernen HTTP-Server (oder einem anderen Proxy), der wiederum eine Verbindung mit dem fernen MQIPT herstellt. Für diesen MQIPT auf der Serverseite der Verbindung ist keine spezifische Konfiguration erforderlich, da die Verbindungsanforderung wie eine normale HTTP-Verbindung behandelt wird.

MQIPT verwendet die Eigenschaften 'HTTPProxy' und 'HTTPServer', um zwischen den lokalen und fernen Proxys zu unterscheiden. 'HTTPProxy' bezeichnet den lokalen HTTP-Proxy und 'HTTPServer' den fernen Server (oder Proxy).

HTTPS-Verbindungen werden in der Regel mit der Listener-Port-Adresse 443 auf dem HTTP-Proxy/-Server hergestellt, dieser Standardwert kann jedoch mit Hilfe der Eigenschaften 'HTTPProxyPort' und 'HTTPServerPort' überschrieben werden. Unter „HTTPS-Konfiguration“ auf Seite 122 finden Sie ein Beispiel für die Verwendung von HTTPS.

Servlet

Es steht jetzt eine Servlet-Version von MQIPT (MQIPTServlet) zur Verfügung, die auf einem Anwendungsserver als nicht verteilte Anwendung eingesetzt werden kann. Dieses Servlet arbeitet ähnlich wie das normale MQIPT, allerdings so, als ob es nur über eine Route verfügt. Eine ankommende Verbindungsanforderung zum Starten eines WebSphere MQ-Kanals wird von einer Instanz des MQIPTServlet bearbeitet, und jede Instanz unterhält eine permanente Verbindung zum Zielwarteschlangenmanager. Nachfolgende Datenflüsse werden über denselben Kanal geleitet, unter Verwendung der Sitzungs-ID, die bei der ersten Verbindungsanforderung erstellt wurde.

Eine Archivierungsdatei für Webanwendungen (MQIPTServlet.war) steht im Unterverzeichnis **web** zur Verfügung. Diese war-Datei muss in den Anwendungsserver importiert und dort eingesetzt werden. Wenn Sie beim Importieren des Servlets einen Kontextnamen angeben müssen, überschreiben Sie den Standardwert für die Eigenschaft 'UriName' mit dem neuen Kontextnamen. Weitere Informationen finden Sie unter „UriName“ auf Seite 96.

Die Konfiguration des MQIPTServlet erfolgt über Eigenschaften in der Datei web.xml, die sich im Unterverzeichnis **WEB-INF** des Anwendungsservers befindet. Für das MQIPTServlet steht nur ein Teil der vorhandenen MQIPT-Eigenschaften zur Verfügung. Folgende Eigenschaften können für das MQIPTServlet festgelegt werden:

- ClientAccess
- ConnectionLog
- MaxLogFileSize
- QMgrAccess
- Trace

Verbindungsprotokolle und Tracedateien werden in ein Verzeichnis geschrieben, das über die neue Eigenschaft **LogDir** (Protokollverzeichnis) definiert wird. Es wird empfohlen, diese Eigenschaft vor dem Start von MQIPTServlet zu definieren.

Um den Umfang der vom MQIPTServlet verwendeten Ressourcen zu steuern, müssen Sie möglicherweise einige der Eigenschaften des Anwendungsservers ändern. Jeder Anwendungsserver hat seine eigene Methode zur Verwaltung von Konfigurationsdaten. Die Verwaltung erfolgt normalerweise über eine GUI, eine Webschnittstelle oder das Bearbeiten der Konfigurationsdatei. Die Eigenschaften, die gegebenenfalls geändert werden sollten, betreffen die maximale Anzahl von aktiven Sitzungen bzw. die Anzahl der Servlet-Instanzen im Anwendungsserver. Dadurch wird die Anzahl von Clientverbindungen gesteuert, ähnlich wie über die in MQIPT verwendete Eigenschaft 'MaxConnectionThreads'.

Andere Eigenschaften, die möglicherweise geändert werden müssen, betreffen Zeitlimits, die mögliche Unterstützung persistenter Verbindungen und die maximal auf einer persistenten Verbindung zulässigen Anforderungen. Da das MQIPTServlet eine persistente Verbindung mit dem Zielwarteschlangenmanager voraussetzt, muss diese Eigenschaft aktiviert werden. Für die anderen Eigenschaften muss möglicherweise ein höherer Wert angegeben werden; dies ist jedoch von ihrem jeweiligen Standardwert und der Art der verwendeten WebSphere MQ-Verbindung abhängig. WebSphere MQ-Clientverbindungen bestehen normalerweise nur kurze Zeit, so dass die Verwendung von Standardwerten unproblematisch ist. Verbindungen zwischen Warteschlangenmanagern können auf unbestimmte Zeit bestehen. Für diesen Fall wird daher empfohlen, einige der Zeitlimitwerte sowie die Anzahl der auf einer persistenten Verbindung zulässigen Anforderungen entsprechend zu erhöhen.

In der Datei web.xml ist auch eine Eigenschaft für das Sitzungszeitlimit mit einem Standardwert von 30 Minuten definiert. Über diese Eigenschaft kann die Inaktivität eines Clients gesteuert und eine Sitzung geschlossen werden, wenn in der angegebenen Zeitspanne keine Aktivität festgestellt wird.

| Schließlich muss in der Verknüpfung zwischen dem Client und dem MQIPTServlet
| mindestens ein MQIPT vorhanden sein. Im MQIPT, der für die Verbindung mit
| dem MQIPTServlet zuständig ist, muss die Eigenschaft 'ServletClient' aktiviert
| werden, und die Eigenschaft 'HTTPServer' kann entweder direkt auf den Anwen-
| dungsserver oder auf den HTTP-Server, der den Anwendungsserver versorgt, zei-
| gen.

| Um zu testen, ob das MQIPTServlet erfolgreich gestartet wurde, können Sie einen
| Webbrowser starten und einen URL-Namen wie den folgenden eingeben:

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

| Im Browser wird eine positive Antwort angezeigt.

| Das MQIPTServlet wurde mit IBM WebSphere Application Server 5.0 (mit und
| ohne IBM HTTP Server), Tomcat 3.3 und Tomcat 4.0 getestet. Das Servlet benötigt
| kein Java 1.4, sondern verwendet den Java-Stand, der vom Anwendungsserver
| implementiert wird.

| Unter „MQIPT-Servlet konfigurieren“ auf Seite 119 finden Sie ein Beispiel für die
| Verwendung des Servlets.

Kapitel 4. Socks-Unterstützung

Ein Socks-Proxy ist ein Netzservice, der als Austrittsteuerungspunkt durch eine Firewall verwendet wird. Eine Socks-fähige Anwendung innerhalb der Firewall kann über den Socks-Proxy eine Verbindung mit einer fernen Anwendung herstellen.

MQIPT kann als Socks-Proxy fungieren, indem die Eigenschaft 'SocksServer' aktiviert wird, wodurch einer Socks-fähigen WMQ-Anwendung ermöglicht wird, über MQIPT eine Verbindung mit einem fernen WMQ-Warteschlangenmanager herzustellen. Bei Verwendung dieser Komponente werden Zieladresse und Ziel-Port-Adresse während des Socks-Handshakeverfahrens übergeben, so dass die Routeneigenschaften 'Destination' und 'DestinationPort' überschrieben werden. Dies ist eine Schlüsselkomponente für die Unterstützung des WMQ-Clustering. Weitere Informationen hierzu siehe unten.

MQIPT kann auch als Socks-Client im Namen einer lokalen WMQ-Anwendung, die nicht Socks-fähig ist, fungieren. Dies ist hilfreich, wenn eine Firewall verwendet wird, die nur abgehende Verbindungen über einen Socks-Proxy zulässt. Jede MQIPT-Route kann für die Kommunikation mit einem anderen Socks-Proxy konfiguriert werden.

Unter „SOCKS-Proxy konfigurieren“ auf Seite 113 finden Sie ein Beispiel für die Verwendung von SOCKS.

Clustering

WebSphere MQ-Cluster können zusammen mit MQIPT verwendet werden, indem die einzelnen WS-Manager im Cluster, der sich über das Internet erstreckt, SOCKSifiziert werden und MQIPT als Socks-Proxy konfiguriert wird. Da es sehr viele Konfigurationsmöglichkeiten für WS-Manager in einem Cluster gibt, beschränkt sich die folgende Erläuterung auf die Aufgaben, die im Handbuch *Cluster-Unterstützung in WebSphere MQ (SC12-2640)* beschrieben werden. Bei der folgenden Abbildung handelt es sich um eine Erweiterung der Abbildung unter der Aufgabe "Einen neuen WS-Manager zu einem Cluster hinzufügen". NEWYORK und CHICAGO befinden sich im Cluster HOME und enthalten beide vollständige Repositories. NEWYORK, LONDON und PARIS befinden sich in einem anderen Cluster mit dem Namen INVENTORY. CHICAGO muss nicht SOCKSifiziert werden, da er sich in einem Cluster befindet, für den kein MQIPT benötigt wird.

Jeder WS-Manager im Cluster INVENTORY wird effektiv hinter einem MQIPT "versteckt". Da der WS-Manager SOCKSifiziert wurde, wird beim Start eines Clustersenderkanals die Anforderung an die Zieladresse gesendet, wobei MQIPT als Socks-Proxy verwendet wird. In der Regel wird anhand von CONNAME in einem Clusterempfängerkanal der lokale WS-Manager ermittelt; bei der Verwendung mit MQIPT muss CONNAME jedoch den lokalen MQIPT und dessen ankommenden Listener-Port angeben. In der folgenden Abbildung haben alle ankommenden Listener-Ports die Nummer 1414, während die abgehenden Listener-Ports die Nummer 1415 haben.

Es gibt zwei Möglichkeiten für die SOCKSifizierung eines WS-Managers. Zum einen kann die gesamte Maschine, auf der der WS-Manager läuft, SOCKSifiziert werden. Zum andern können Sie auch nur allein den WS-Manager SOCKSifizieren.

Bei beiden Verfahren muss der Socks-Client so konfiguriert werden, dass er Fernverbindungen nur mit MQIPT als Socks-Proxy herstellt, und die Benutzerauthentifizierung muss deaktiviert werden. Auf dem Markt sind verschiedene Produkte erhältlich, die Socks-Unterstützung bieten. Sie benötigen ein Produkt, das das Socks-Protokoll V5 unterstützt.

Ein Beispiel für die Konfiguration eines Clusternetzes finden Sie unter „Unterstützung für MQIPT-Clustering konfigurieren“ auf Seite 126.

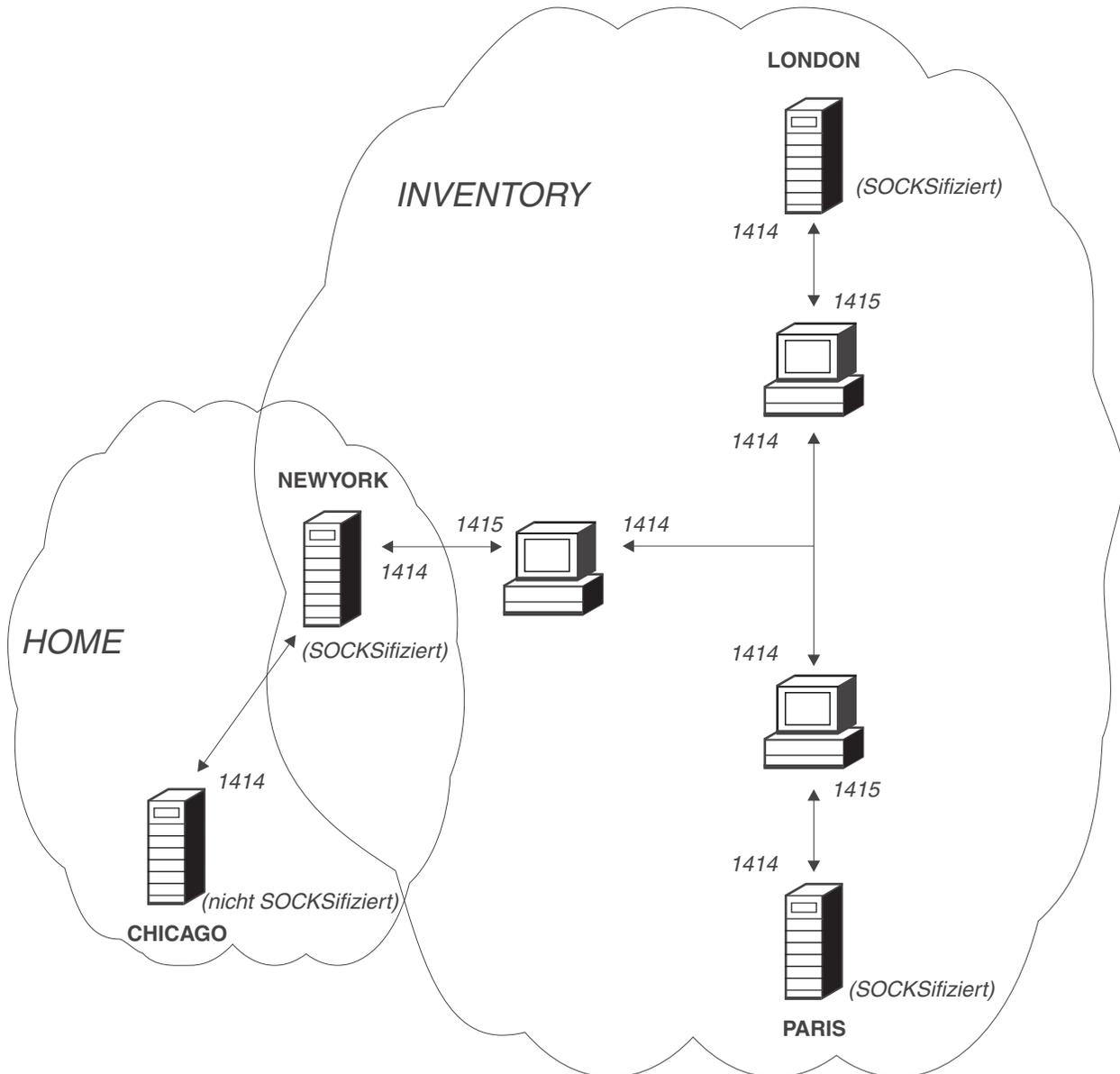


Abbildung 6. MQIPT-Clusterunterstützung

Kapitel 5. SSL-Übersicht und -Unterstützung

Das SSL-Protokoll garantiert sichere Verbindungen über unsichere Kommunikationskanäle und stellt Folgendes sicher:

Vertraulichkeit von Übertragungen

Die Verbindung kann durch Verschlüsselung der Daten, die beispielsweise zwischen Client und Server ausgetauscht werden sollen, geschützt werden; die Daten sind nur für den Client und den Server verständlich. Dadurch wird die sichere Übertragung privater Informationen, wie beispielsweise Kreditkartennummern, ermöglicht.

Integrität der Kommunikation

Die Verbindung ist zuverlässig. Zu der Nachrichtenübertragung gehört eine Integritätsprüfung der Nachricht auf Basis einer sicheren Hash-Funktion.

Authentifizierung

Der Client kann den Server authentifizieren, und ein authentifizierter Server kann wiederum einen Client authentifizieren. Dadurch wird sichergestellt, dass Daten nur zwischen den gewünschten Seiten ausgetauscht werden. Dieses Authentifizierungsverfahren basiert auf dem Austausch digitaler Zertifikate (X.509V3-Zertifikate).

Das SSL-Protokoll kann für die Authentifizierung der Kommunikationsteilnehmer verschiedene Algorithmen für digitale Signaturen verwenden. Die in SSL verwendeten kryptographischen Verfahren (Verschlüsselung zur Wahrung der Vertraulichkeit der Daten und sichere Hash-Verfahren zur Wahrung der Nachrichtenintegrität) basieren auf der gemeinsamen Nutzung geheimer Schlüssel durch Client und Server. SSL stellt verschiedene Verfahren zum Austausch von Schlüssel zur Verfügung, die die gemeinsame Benutzung geheimer Schlüssel gestatten. Für die Verschlüsselung und das Hash-Verfahren kann SSL auf eine ganze Reihe von Algorithmen zurückgreifen. Es werden verschiedene Verschlüsselungsalgorithmen unterstützt, die über SSL-Cipher Suites angegeben werden können. Die folgenden Cipher Suites werden unterstützt:

```
| 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
```

SSL-Handshake

Das SSL-Handshake-Verfahren erfolgt bei der einleitenden Verbindungsanforderung zwischen SSL-Client und -Server, und zwar während der Authentifizierung und der Festlegung der Cipher Suites.

Alle oben aufgeführten SSL-Cipher Suites (mit Ausnahme der anonymen Cipher Suites) erfordern die Serverauthentifizierung und gestatten die Clientauthentifizierung, d. h., der Server kann so konfiguriert werden, dass eine Clientauthentifizierung angefordert wird. Die Authentifizierung der Kommunikationspartner in SSL basiert auf der Verschlüsselung mit Hilfe eines öffentlichen Schlüssels und digitalen X.509V3-Zertifikaten. Eine Site, die im SSL-Protokoll authentifiziert werden soll, muss über einen privaten Schlüssel verfügen und über ein digitales Zertifikat, das den entsprechenden öffentlichen Schlüssel sowie Informationen über die Identität der Site und die Gültigkeitsdauer des Zertifikats verfügt. Die Zertifikate werden von so genannten Zertifizierungsstellen (CA = Certification Authority) signiert; die Zertifikate solcher Stellen werden als signierte Zertifikate (Signer Certificates) bezeichnet. Bei einem Zertifikat gefolgt von einem oder mehreren signierten Zertifikaten spricht man von einer Zertifikatkette. Zertifikatketten zeichnen sich dadurch aus, dass ab dem ersten Zertifikat (das Zertifikat der Site) die Signaturen der einzelnen Zertifikate in der Kette über den öffentlichen Schlüssel im nächsten signierten Zertifikat bestätigt werden kann.

Bei der Herstellung einer sicheren Verbindung, für die die Serverauthentifizierung erforderlich ist, sendet der Server an den Client eine Zertifikatkette, um seine Identität unter Beweis zu stellen. Der SSL-Client wird sich am Verbindungsaufbau zum Server nur dann beteiligen, wenn er den Server authentifizieren kann, z. B. durch Bestätigung der Signatur des Site-Zertifikats des Servers. Damit diese Signatur bestätigt werden kann, muss der SSL-Client der Serversite selbst oder zumindest einer der Zertifizierungsstellen in der vom Server gesendeten Zertifikatkette vertrauen. Die Zertifikate der vertrauenswürdigen Sites und der Zertifizierungsstellen müssen auf der Clientseite verwaltet werden, damit diese Überprüfung möglich ist.

Der SSL-Client überprüft die Zertifikatkette des Servers, wobei er mit dem Sitezertifikat beginnt. Die Signatur des Sitezertifikats wird für gültig befunden, wenn sich das Sitezertifikat im Repository für Zertifikate vertrauenswürdiger Sites oder für signierte Zertifikate befindet oder wenn ein signiertes Zertifikat in der Kette anhand des Repositories für vertrauenswürdige signierte Zertifikate bestätigt werden kann. Im letzteren Fall überprüft der SSL-Client, ob die Zertifikatkette (d. h. vom Zertifikat der vertrauenswürdigen Zertifizierungsstelle bis hin zum Zertifikat der Serversite) richtig signiert wurde. Bei jedem dieser Zertifikate wird auch das Format auf Richtigkeit und die Gültigkeitsdauer überprüft. Schlägt eine dieser Prüfungen fehl, wird die Verbindungsanforderung zum Server zurückgewiesen. Nach der Bestätigung des Serverzertifikats verwendet der Client für die weiteren Schritte des SSL-Protokolls den in diesem Zertifikat enthaltenen öffentlichen Schlüssel.

Die SSL-Verbindung kann nur eingerichtet werden, wenn der Server auch tatsächlich über den entsprechenden privaten Schlüssel verfügt.

Die Clientauthentifizierung erfolgt nach demselben Verfahren: Wenn von einem SSL-Server eine Clientauthentifizierung angefordert wird, sendet der Client eine Zertifikatkette an den Server, um seine Identität unter Beweis zu stellen. Der Server wiederum überprüft diese Kette anhand seines Repositorys für Zertifikate vertrauenswürdiger Sites und für Zertifikate von Zertifizierungsstellen. Nach der Bestätigung des Clientzertifikats verwendet der Server für die weiteren Schritte des SSL-Protokolls den in diesem Zertifikat enthaltenen öffentlichen Schlüssel. Die SSL-Verbindung kann nur eingerichtet werden, wenn der Client auch tatsächlich über den entsprechenden privaten Schlüssel verfügt.

Das SSL-Protokoll selbst ermöglicht eine in hohem Grade sichere Kommunikation. Das Protokoll arbeitet jedoch auf Basis der Informationen, die von der Anwendung zur Verfügung gestellt werden. Nur wenn diese Daten ebenfalls sicher verwaltet werden, kann eine sichere Kommunikation auch tatsächlich gewährleistet werden. Wenn beispielsweise Ihr Repository für Zertifikate vertrauenswürdiger Sites und für signierte Zertifikate nicht länger sicher ist, stellen Sie unter Umständen eine sichere Verbindung zu einem völlig unsicheren Kommunikationspartner her.

WebSphere MQ Internet Pass-Thru und SSL

SSL V3.0 wurde implementiert; es werden PKCS#12-Tokens verwendet. Diese Tokens sind in Schlüsselringdateien (Dateityp .pp12 oder .pfx) gespeichert, die X509V3-Zertifikate enthalten. Eine Schlüsselringdatei kann auch Zertifikatwiderrufslisten (Certificate Revocation Lists, CRLs) und Berechtigungswiderrufslisten (Authority Revocation Lists, ARLs) enthalten. WebSphere MQ Internet Pass-Thru verwendet das Paket IBM Secure Socket Lite (SSLite).

WebSphere MQ Internet Pass-Thru kann als SSL-Client oder SSL-Server eingesetzt werden, je nachdem, von welcher Seite die Verbindung eingeleitet wird. Verbindungen werden vom Client gestartet, während der Server die Verbindungsanforderungen akzeptiert. Eine WebSphere MQ Internet Pass-Thru-Route kann sowohl als Client als auch als Server fungieren; allerdings wird in diesem Fall aus Leistungsgründen die Verwendung des SSL-Proxy-Modus empfohlen. Jede WebSphere MQ Internet Pass-Thru-Route kann individuell über eigene SSL-Eigenschaften konfiguriert werden. Weitere Informationen hierzu finden Sie unter „Referenzinformationen zum Abschnitt 'route'“ auf Seite 82.

Vertrauenseinstellungen

Eine Schlüsselringdatei enthält ein privates Zertifikat einschließlich des signierten Zertifikats bzw. einer Kette von signierten Zertifikaten. Damit eine Authentifizierung beim Aufbau der Verbindung möglich ist, ist für ein Zertifikat eine Vertrauenseinstellung erforderlich. Es gibt zwei Vertrauensebenen:

Vertrauen auf Peer-Ebene

Gibt an, dass nur dieses Zertifikat als vertrauenswürdig akzeptiert wird, nicht aber andere von dieser Zertifizierungsstelle signierte Zertifikate.

Vertrauen auf Ebene der Zertifizierungsstelle (CA)

Gibt an, dass alle von dieser Zertifizierungsstelle signierten Zertifikate als vertrauenswürdig angesehen werden.

Die Schlüsselringdatei auf der SSL-Serverseite, die über die Eigenschaft **SSLServerKeyRing** (SSL-Serverschlüsselring) angegeben wird, sollte das private Zertifikat enthalten.

Die Schlüsselringdatei auf der SSL-Clientseite, die durch die Eigenschaft 'SSLClientCAKeyRing' angegeben wird, sollte eine Liste von Zertifikaten vertrauenswürdiger Zertifizierungsstellen enthalten, die zur Authentifizierung des vom Server gesendeten Zertifikats verwendet wird.

Wenn auch eine Clientauthentifizierung erforderlich ist, muss auf der Serverseite die Eigenschaft 'SSLServerAskClientAuth' aktiviert werden, und die Schlüsselringdatei auf der Clientseite, die durch die Eigenschaft 'SSLClientKeyRing' angegeben wird, sollte das private Zertifikat des Clients enthalten. Die Schlüsselringdatei auf der Serverseite, die durch die Eigenschaft 'SSLServerCAKeyRing' angegeben wird, sollte eine Liste von Zertifikaten vertrauenswürdiger Zertifizierungsstellen enthalten, die zur Authentifizierung des Clients verwendet wird.

Alternativ zu Zertifikaten, die von einer vertrauenswürdigen Zertifizierungsstelle signiert wurden, können Sie selbstsignierte Zertifikate verwenden. Beispiele hierfür finden Sie in den mit MQIPT bereitgestellten Beispielschlüsselringdateien `sslSample.pfx` und `sslCAdefault.pfx` im Unterverzeichnis 'ssl'.

Zum Öffnen eines der in diesen Schlüsselringdateien gespeicherten PKCS#12-Tokens müssen Sie das Kennwort `mqiptV1.3` verwenden.

Das Unterverzeichnis 'ssl' enthält außerdem das Dienstprogramm 'KeyMan' zur Verwaltung von SSL-Zertifikaten und Schlüsselringdateien. Installationsanweisungen und weitere Informationen finden Sie unter „KeyMan“ auf Seite 22.

Sie müssen alle Schlüsselring- und Kennwortdateien mit Hilfe der Sicherheitseinstellungen des Betriebssystems schützen, um unbefugten Zugriffen vorzubeugen.

SSL testen

In Kapitel 20, „WebSphere MQ Internet Pass-Thru - Erste Schritte“, auf Seite 97 werden die einzelnen Schritte erläutert, mit deren Hilfe eine SSL-Verbindung geprüft werden kann.

Es stehen Zertifikate und Verfahren für die Zertifikatverwaltung verschiedener Hersteller zur Verfügung, z. B.:

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

SSL-Fehlernachrichten

Die folgenden `SSLRuntimeException`-Fehlercodes werden ausgegeben, wenn beispielsweise ein ungültiger Parameterwert in einem der SSL-Methodenaufrufe angegeben wird oder falsche Daten an das SSL-Protokoll übergeben werden:

Tabelle 1. SSLRuntimeException-Fehlernachrichten

ID	Beschreibung
1	Falsche Verwendung einer Methode, oder ein oder mehrere Parameterwerte liegen außerhalb des zulässigen Bereichs.

Tabelle 1. *SSLRuntimeException-Fehlernachrichten (Forts.)*

2	Die übergebenen Daten können nicht verarbeitet werden.
3	Die Signatur der übergebenen Daten kann nicht bestätigt werden.
10	Der registrierte Name der mit dem signierten Zertifikat verbundenen Person entspricht nicht dem Namen des Ausstellers des Zertifikats.
11	Der Typ eines Zertifikats wird nicht unterstützt.
12	Ein Zertifikat wird vor Beginn des Gültigkeitszeitraums verwendet.
13	Ein Zertifikat ist abgelaufen.
14	Eine Zertifikatsignatur konnte nicht bestätigt werden.
15	Ein Zertifikat kann nicht verwendet werden.
20	Keine der vom Client vorgeschlagenen Cipher Suites wird vom Server unterstützt.
21	Keines der vom Client vorgeschlagenen Komprimierungsverfahren wird vom Server unterstützt.
22	Es ist kein Zertifikat verfügbar.
23	Ein Algorithmus oder Formattyp wird nicht unterstützt.
24	Zurückweisung nicht länger gültiger Daten.
25	Ein Zertifikat wird widerrufen.
26	Eine Gruppe von CRLs ist nicht vollständig (einige Delta-CRLs fehlen).
27	Der Name, der zertifiziert werden soll, ist bereits vergeben.
28	Der öffentliche Schlüssel, der zertifiziert werden soll, ist bereits vergeben.
29	Eine Seriennummer oder ein Schlüssel (Zertifikat, CRL) ist falsch.
30	Autorisierung fehlgeschlagen

Eine *SSLException*-Fehlernachricht wird ausgegeben, wenn die Ausführung des SSL-Handshakeprotokolls abgebrochen wird.

Tabelle 2. *SSLException-Fehlernachrichten*

ID	Beschreibung
3	Das im SSL-Kontext definierte Zeitlimit für Verbindungen ist abgelaufen, ohne dass eine Antwort vom Partner empfangen wurde.
4	Die Verbindung wurde während des SSL-Handshake vom Partner ohne nähere Fehlerangaben abgebrochen.
10	Es wurde eine unerwartete Nachricht empfangen.
20	Es wurde eine Nachricht mit einem ungültigen MAC (Message Authorization Code) empfangen.
30	Fehler bei der Dekomprimierung.
40	Handshake fehlgeschlagen.
41	Vom Partner wurde kein Zertifikat gesendet.
42	Es wurde ein ungültiges Zertifikat empfangen.
43	Es wurde ein Zertifikat empfangen, das nicht unterstützt wird.
44	Es wurde ein Zertifikat empfangen, das bereits widerrufen wurde.
45	Es wurde ein abgelaufenes Zertifikat empfangen.
46	Es wurde ein unbekanntes Zertifikat empfangen.
47	Es wurde ein ungültiger Parameter festgestellt.

LDAP und CRLs

WebSphere Internet Pass-Thru unterstützt die Verwendung eines LDAP-Servers (Lightweight Directory Access Protocol) zur Ausführung einer CRL-Authentifizierung (Certificate Revocation List = Zertifikatwiderrufsliste) für ein digitales Zertifikat. Die LDAP-Unterstützung wurde auf eine ähnliche Weise wie im WebSphere MQ-Basisprodukt implementiert, da derselbe LDAP-Server sowohl für WebSphere MQ als auch für MQIPT verwendet werden kann. Weitere Informationen zur Verwendung von LDAP-Servern mit WebSphere MQ finden Sie im Handbuch "WebSphere MQ Sicherheit Version 5.3" SC12-3103-01, Kapitel 15. Der folgende Abschnitt enthält einige Auszüge aus diesem Buch.

Während des SSL-Handshakeverfahrens authentifizieren sich die miteinander kommunizierenden Partner gegenseitig durch digitale Zertifikate. Die Authentifizierung kann eine Überprüfung beinhalten, ob das empfangene Zertifikat noch vertrauenswürdig ist. Zertifizierungsstellen (Certification Authorities, CAs) können Zertifikate aus verschiedenen Gründen widerrufen:

- Der Eigner ist zu einer anderen Organisation gewechselt.
- Der private Schlüssel ist nicht mehr geheim.

CAs veröffentlichen widerrufene private Zertifikate in einer Zertifikatwiderrufsliste (Certification Revocation List, CRL). Widerrufene CA-Zertifikate werden in einer Berechtigungswiderrufsliste (Authority Revocation List, ARL) veröffentlicht. Weitere Verweise auf CRLs in diesem Kapitel gelten auch für ARLs.

Auf dem Markt werden eine Reihe von proprietären LDAP-Verzeichnisservern angeboten. WebSphere Internet Pass-Thru wurde mit dem IBM Directory Server getestet (siehe <http://www.ibm.com/software/network/directory/server>). Anweisungen zur Installation und Wartung des LDAP-Servers finden Sie in der mit dem installierten Produkt gelieferten Dokumentation.

Weitere Informationen zur Verwaltung von CRLs und ARLs finden Sie im Handbuch "WebSphere MQ Sicherheit Version 5.3" SC12-3103-01.

MQIPT kann auf jeder Route bis zu zwei LDAP-Server unterstützen. Der erste LDAP-Server wird als Hauptserver und der zweite LDAP-Server als Ausweichserver betrachtet, der nur verwendet wird, wenn der Hauptserver nicht erreichbar ist. Der Ausweichserver sollte ein Spiegelbild des Hauptservers sein.

Informationen, die auf einem LDAP-Server gespeichert sind, können durch eine Benutzer-ID und ein Kennwort vor unbefugtem Zugriff geschützt werden. In diesem Fall können die Eigenschaften 'LDAP*Userid' und 'LDAP*Password' verwendet werden.

Wenn MQIPT ein PKCS#12-Token aus einer Schlüsselringdatei lädt, werden alle CA-Zertifikate anhand der CRL auf ihre Gültigkeit überprüft. Wenn an das CA-Zertifikat eine CRL angehängt ist, wird diese überprüft, um zu sehen, ob sie abgelaufen ist. Ist dies der Fall, wird eine aktuelle CRL vom LDAP-Server abgerufen. Alle abgerufenen CRLs werden in das aktuelle Token geladen und an das jeweilige CA-Zertifikat angehängt. Das aktualisierte Token kann in der Schlüsselringdatei gespeichert werden (siehe Eigenschaft 'LDAPSaveCRL' unter „Referenzinformationen zum Abschnitt 'route'“ auf Seite 82).

Wenn beim Senden einer Abfrage an den LDAP-Hauptserver keine Einträge vorhanden sind, die mit der angegebenen CA übereinstimmen, wird davon ausgegan-

gen, dass für die betreffende CA keine CRLs vorliegen. Der Ausweichserver wird nicht verwendet. Wenn der LDAP-Hauptserver jedoch nicht erreichbar ist oder nicht innerhalb einer vorgegebenen Zeit antwortet, wird der Ausweichserver verwendet. Kommt es auf dem Ausweichserver zu einem Fehler, wird die Clientverbindung beendet. Diese Aktion kann außer Kraft gesetzt werden, indem die Eigenschaft 'LDAPIgnoreErrors' auf 'wahr' (true) gesetzt wird.

Achtung

Wenn Sie die Eigenschaft 'LDAPIgnoreErrors' aktivieren, kann ein widerrufenes Zertifikat zur Herstellung einer SSL-Verbindung verwendet werden.

Das LDAP-Clientmodell basiert auf der Implementierung von "com.sun.jndi.ldap.LdapCtxFactory". Alle CRLs, die von MQIPT empfangen werden, werden in einem Cache gespeichert und von allen Verbindungen auf der Route gemeinsam benutzt.

Wenn eine gespeicherte CRL abgelaufen ist, wird sie aus dem Cache entfernt und eine neue CRL vom LDAP-Server abgerufen. Ist keine neue CRL verfügbar, wird die Herstellung der Verbindung weiter verweigert.

Eine vom LDAP-Server abgerufene CRL wird ebenfalls auf ihre Gültigkeit überprüft und gegebenenfalls eine Warnung (MQCPW001) an der Systemkonsole angezeigt. Die abgelaufene CRL wird jedoch in das System geladen, und alle Verbindungsanforderungen, die auf diese CRL verweisen, werden zurückgewiesen. Die abgelaufene CRL auf dem LDAP-Server sollte durch eine aktuelle Liste ersetzt werden.

Über die Eigenschaft 'LDAPCacheTimeout' kann gesteuert werden, wie häufig der Inhalt des CRL-Cache gelöscht werden soll. Der Standardwert ist 1 Tag. Wird dieser Wert auf 0 gesetzt, werden die Einträge erst gelöscht, wenn die Route erneut gestartet wird.

Eine abgelaufene CRL kann in einer Schlüsselringdatei oder auf einem LDAP-Server gespeichert werden. Wenn keine neue Liste ausgegeben wurde, werden alle weiteren Verbindungsanforderungen zurückgewiesen. Sie können abgelaufene CRLs ignorieren, indem Sie die Eigenschaft 'IgnoreExpiredCRLs' aktivieren.

Achtung

Wenn Sie die Eigenschaft 'IgnoreExpiredCRLs' aktivieren, kann ein widerrufenes Zertifikat zur Herstellung einer SSL-Verbindung verwendet werden.

Advanced Encryption Standard

Der Advanced Encryption Standard (AES) ist eine neue FIPS-Veröffentlichung (Federal Information Processing Standard), in der ein Verschlüsselungsalgorithmus festgelegt ist, der von Regierungsbehörden der USA zum Schutz von sensiblen (nicht klassifizierten) Informationen verwendet wird. Das National Institute of Standards and Technology (NIST) geht davon aus, dass auch viele Organisationen, Institutionen und Einzelpersonen außerhalb der US-Regierung - und außerhalb der USA - AES auf freiwilliger Basis verwenden werden.

Zertifikate aus einer Schlüsselringdatei auswählen

In derselben Schlüsselringdatei können mehrere private Zertifikate gespeichert werden, so dass über die SSLClientSite*-Eigenschaften auf der Clientseite das Zertifikat, das zur Authentifizierung an den Server gesendet werden soll, ausgewählt werden kann und über die SSLServerSite*-Eigenschaften auf der Serverseite das Zertifikat, das zur Authentifizierung an den Client gesendet werden soll, ausgewählt werden kann.

Mit Hilfe dieser Eigenschaften kann ein Zertifikat auf Basis seines registrierten Namens (Distinguished Name, DN) ausgewählt werden. Alternativ kann über die Eigenschaften 'SSLServerSiteLabel' und 'SSLClientSiteLabel' die Zertifikatsbezeichnung zur Auswahl eines Zertifikats verwendet werden.

Schlüsselringkennwort verschlüsseln

Das Kennwort zum Öffnen einer Schlüsselringdatei kann mit dem Script 'mqipt-PW' verschlüsselt werden. Das verschlüsselte Kennwort wird in einer Datei gespeichert, die von den folgenden Eigenschaften verwendet werden kann: SSLClientKeyRingPW, SSLClientCAKeyRingPW, SSLServerKeyRingPW und SSLServerCAKeyRingPW.

Befehlsformat:

```
mqiptPW <Kennwort> <Dateiname> <-replace>
```

Dabei gilt Folgendes:

Kennwort

Das Kennwort in Klartext zum Öffnen der angegebenen Schlüsselringdatei

Dateiname

Der Name der zu erstellenden Kennwortdatei

replace

Die erforderliche Option zum Überschreiben von <Dateiname> (falls vorhanden)

Kennwörter können Leerzeichen (" ") enthalten. Damit dies akzeptiert wird, muss das gesamte Kennwort jedoch in Anführungszeichen gesetzt werden. Es gibt keine Einschränkungen für die Länge oder das Format von Kennwörtern.

Anmerkung: Benutzer, die von einer früheren Version von WebSphere Internet Pass-Thru migriert wurden, müssen die aktuellen Kennwortdateien mit dem Kennwort in Klartext durch eine Kopie der verschlüsselten Kennwortdatei ersetzen.

Zum Öffnen einer der Beispielschlüsselringdateien mit einem Dienstprogramm zur Schlüsselverwaltung (z. B. KeyMan) müssen Sie das Kennwort mqiptV1.3 verwenden.

KeyMan

WebSphere Internet Pass-Thru wird jetzt mit dem Standalone-Dienstprogramm KeyMan geliefert, das die Verwaltung der SSL-Zertifikate und Schlüsselringdateien ermöglicht. Die Zip-Datei mit KeyMan befindet sich im Unterverzeichnis `ssl`. Um dieses Dienstprogramm zu installieren, müssen Sie zunächst die Zip-Datei in einem temporären Verzeichnis entpacken und anschließend anhand der Hinweise in der

Readme-Datei vorgehen. KeyMan verfügt über eine Vielzahl an Leistungsmerkmalen, allerdings soll in diesem Abschnitt nur auf die Erstellung von Testzertifikaten und die Verwaltung von Schlüsselringdateien mit PKCS#12-Tokens eingegangen werden.

Bei KeyMan handelt es sich um ein Verwaltungs-Tool für die Clientseite der PKI-Infrastruktur (Public-Key-Infrastruktur). KeyMan verwaltet Schlüssel, Zertifikate, CRLs (Certificate Revocation Lists) und die verschiedenen Repositorys, in denen diese Komponenten gespeichert bzw. aus denen sie abgerufen werden. Es werden Zertifikate über ihre gesamte Lebensdauer sowie alle Prozesse für die Handhabung von Benutzerzertifikaten unterstützt.

KeyMan verwaltet die Repositorys, die die Schlüssel, Zertifikate und CRLs enthalten. Repositorys werden als Tokens bezeichnet. Ein Token enthält die Vertrauenseinstellungen für eine bestimmte Anwendung (z. B. WebSphere Internet Pass-Thru). In der Regel enthält ein Token private Schlüssel und die zugehörigen Zertifikatketten, über die ein Benutzer auf anderen Sites authentifiziert wird. Darüber hinaus enthält ein Token auch die Zertifikate von vertrauenswürdigen Kommunikationspartnern und von Zertifizierungsstellen (CAs).

Unterstützte Tokens

KeyMan unterstützt eine Reihe unterschiedlicher Tokens. Bei Tokens handelt es sich um Repositorys, die Schlüssel, Zertifikate, CRLs und Vertrauenseinstellungen enthalten. Einige Tokens können lediglich einen Teil dieser Komponenten enthalten.

PKCS#7-Token

Enthält eine Gruppe von Zertifikaten und optional zugehörige CRLs. In diesem Repository-Typ können keine Schlüssel gespeichert werden. Es ist keine Authentifizierung erforderlich. Zertifikate und CRLs werden durch eine Signatur geschützt. Unbefugte sind jedoch in der Lage, die Gruppe der in einem bestimmten PKCS#7-Token gespeicherten Komponenten zu ändern. Dieser Token-Standard wird verwendet, wenn die erwarteten Komponenten durch einen Kontext definiert werden.

PKCS#12-Token

Enthält private Schlüssel, Zertifikate und zugehörige CRLs. Der Inhalt wird über eine Benutzer-Passphrase geschützt. Die öffentlichen (Zertifikate, CRLs) und privaten (Schlüssel) Komponenten können durch unterschiedlich komplexe Algorithmen geschützt werden.

PKCS#11-Repositorys (CryptoKi)

Der PKCS#11-Standard definiert eine Schnittstelle für Verschlüsselungstokens. In diesen Tokens können Schlüssel und Zertifikate gespeichert werden. Die Speicherung von CRLs wird hingegen nicht unterstützt. Der Zugriff auf diese Tokens wird über eine PIN (Personal Identification Number = persönliche Identifikationsnummer) geschützt. Sie müssen die tokenspezifische PKCS#11-DLL angeben, über die KeyMan auf das Token zugreift.

KeyMan unterstützt DLLs für PKCS#11 Version 2.01 und 2.10.

Bei PKCS#7 und PKCS#12 handelt es sich um Soft-Tokens, die aus unterschiedlichen Medien (z. B. Dateien, URI oder der Zwischenablage) abgerufen werden können.

KeyMan kann PKCS#7-Tokens anhand von Daten unbekanntem Formats erstellen. Dazu durchsucht dieses Dienstprogramm die Daten nach X.509-Zertifikaten und CRLs und erstellt anschließend anhand der Zertifikate und CRLs, die ermittelt werden konnten, ein PKCS#7-Token. Wenn Sie E-Mails mit Zertifikaten oder CRLs haben, können Sie den E-Mail-Ordner in KeyMan öffnen; KeyMan wird daraufhin versuchen, die X.509-Komponenten zu extrahieren. Die Daten können natürlich nicht wieder im ursprünglichen Format gespeichert werden. Sie können in einer Datei im PKCS#7-Format gespeichert werden.

Unterstützte Standarddatenformate

KeyMan unterstützt eine Reihe von Standarddatenformaten. Im Folgenden werden diese beschrieben und ihre Verwendung erläutert:

PKCS#7

Bei diesem Datenformat handelt es sich um eine Sammlung von Zertifikaten und CRLs. Die über PKCS#7 beschriebenen Zertifikate und CRLs sind nicht geschützt. Die einzelnen Zertifikate und CRLs werden jedoch durch eine Signatur geschützt. Dieser Token-Standard wird verwendet, wenn die erwarteten Komponenten durch einen Kontext definiert werden. Auf Windows-Systemen haben PKCS#7-Dateien standardmäßig die Erweiterungen .p7r und .p7b.

PKCS#10

Der PKCS#10-Standard definiert Anforderungsnachrichten für Zertifikate. Sie enthalten den öffentlichen Schlüssel sowie Angaben zum X.500-Namen des Anforderers. Die Nachricht wird mit dem entsprechenden privaten Schlüssel signiert. PKCS#10-Nachrichten können im Binärformat und im ASCII-Armored-Format generiert werden. Diese Nachrichten müssen an eine Zertifizierungsstelle (CA) übergeben werden.

PKCS#12

Der PKCS#12-Standard wird von Browsern und Webservern für den Import und Export privater Schlüssel und zugehöriger Zertifikate verwendet. PKCS#12-Dateien können von KeyMan gelesen und geschrieben werden. Während Browser und Webserver nur ein ganz spezifisches PKCS#12-Profil erkennen, kann KeyMan auch allgemeine PKCS#12-Dateien erstellen. KeyMan speichert in einer einzigen PKCS#12-Datei ein Gruppe von privaten Schlüsseln, Zertifikaten, CRLs und den entsprechenden Vertrauenseinstellungen. PKCS#12-Dateien werden über eine Passphrase geschützt. PKCS#12-Tokens enthalten in der Regel die Vertrauensrichtlinie für eine bestimmte Anwendung. Im Fall von IBM BlueZ SSLite werden die Schlüssel und die zugehörigen Zertifikatketten für die Client/Server-Authentifizierung verwendet. Andere Zertifikate gehören wiederum je nach den jeweiligen Vertrauenseinstellungen zu vertrauenswürdigen Zertifizierungsstellen oder vertrauenswürdigen Servern. Auf Windows-Systemen haben PKCS#12-Dateien standardmäßig die Erweiterungen .p12 und .pfx.

SPKAC

SPKAC (SignedPublicKeyAndChallenge) ist ein Datenformat, das für die Anforderung von Zertifikaten von einer Zertifizierungsstelle verwendet wird. Dieses Format wird von Netscape bei Angabe des HTML-Tags <keygen> erstellt. Es enthält den öffentlichen Schlüssel und den Abruf. Dieses Datenformat kann von KeyMan im binären Format und im Base64-Format generiert werden.

X.509V3-Zertifikate

KeyMan kann X.509V3-Zertifikate im binären Format oder eingebettet im ASCII-Armored-Format lesen. Diese Dateien können in KeyMan geöffnet oder importiert werden. Darüber hinaus ist es auch möglich, Zertifikate aus einem Token in diesen beiden Formaten zu schreiben (**Certificate details -> Save Icon** (Zertifikatangaben -> Symbol speichern)). Auf Windows-Systemen haben X.509-Zertifikatdateien standardmäßig die Erweiterungen .crt, .cer und .der.

X.509V2-CRLs

KeyMan kann X.509V2-CRLs im binären Format oder eingebettet im ASCII-Armored-Format lesen. Es ist nicht möglich, eine einzelne CRL zu öffnen. KeyMan kann CRLs nur in Token importieren, die bereits das zugeordnete CA-Zertifikat enthalten. Es besteht die Möglichkeit, CRLs im binären Format oder im ASCII-Armored-Format zu schreiben (**Certificate details -> CRLs details -> Save Icon** (Zertifikatangaben -> CRL-Angaben -> Symbol speichern)). Auf Windows-Systemen haben X.509-CRL-Dateien standardmäßig die Erweiterung .crl.

KeyMan-FAQs

Antworten auf allgemeine Fragen zur Kryptografie und damit zusammenhängende Themen finden Sie unter "Frequently Asked Questions About Today's Cryptography" auf der Website von RSA Laboratories. In den folgenden FAQs geht es um Fragen in Zusammenhang mit KeyMan:

Kann KeyMan PKCS#12-Dateien lesen, die von Netscape oder dem Internet Explorer erstellt wurden?

KeyMan kann von Netscape oder IE erstellte PKCS#12-Dateien lesen, sofern Ihnen das Kennwort bekannt ist, das den Inhalt der Dateien schützt.

Kann KeyMan PKCS#12-Dateien erstellen, die von Netscape oder vom Internet Explorer gelesen werden können?

Der PKCS#12-Standard lässt sehr viel Spielraum bei der Auswahl von Algorithmen und der Anordnung der Inhalte. Die Browser können nur jeweils ein ganz spezifisches Profil lesen. KeyMan kann PKCS#12-Dateien erstellen, die von Netscape und vom IE gelesen werden können. Da KeyMan Ihnen jedoch sehr viel mehr Optionen für den PKCS#12-Standard bietet, haben Sie auch die Möglichkeit, Dateien zu erstellen, die von diesen Browsern nicht gelesen werden können. Die allgemeinen Profile, die von Browsern gelesen werden können, sehen wie folgt aus: Als öffentliche /private Verschlüsselung (siehe **Menu Options -> PKCS#12 Settings**) (Menüoptionen -> PKCS#12-Einstellungen) sollte **RC2 (40 bits)** bzw. **DES (168 bits)** angegeben werden. Das PKCS#12-Token sollte genau ein privates Zertifikat enthalten.

Was ist ein privates Zertifikat?

Wenn KeyMan einen Schlüssel und ein Zertifikat findet, die einander entsprechen, verbindet er beide zu einem privaten Zertifikat. Das bedeutet, dass Sie für jedes private Zertifikat auch über den entsprechenden privaten Schlüssel verfügen. Wenn Sie Zertifikate in ein Token importieren, prüft KeyMan, ob ein entsprechender privater Schlüssel vorhanden ist; ist dies der Fall, verbindet das Programm automatisch Schlüssel und importiertes Zertifikat zu einem privaten Zertifikat. KeyMan unterrichtet Sie hiervon in einem Dialogfenster.

Was ist ein Zertifikat auf Peer- bzw. CA-Ebene?

Zertifikate in einem Token legen die Vertrauenswürdigkeit fest. Sie geben an, wem Sie vertrauen können. Was "Vertrauenswürdigkeit" genau bedeutet sowie das genaue Auswerteverfahren für das Zertifikat hängt von der Anwendung ab, die das Token verwendet. Mit KeyMan können Sie zwei Vertrauenseinstellungen für Zertifikate festlegen: Auf CA- und auf Peer-Ebene. Wenn Sie einem Zertifikat auf CA-Ebene vertrauen, so vertrauen Sie damit sämtlichen Zertifikaten, die direkt oder indirekt von dieser CA signiert werden. Wenn Sie als Vertrauenseinstellung "Peer" angeben, so vertrauen Sie nur genau diesem Zertifikat. Das Vertrauen wird nicht auf Zertifikate ausgedehnt, die von solch einem "Peer"-Zertifikat signiert werden.

Was sind Zertifikate, die weder private Zertifikate noch CA- oder Peer-Zertifikate sind?

KeyMan versucht, für jedes private Zertifikat die gesamte Zertifikatkette bis zum Ausgangszertifikat zu speichern. Diese Zertifikate müssen nicht vertrauenswürdig sein, daher werden sie nicht unter den CA- oder Peer-Zertifikaten aufgeführt. Diese Zertifikate können durch Auswahl des Schlüsselrings **All Certificate Items** (Alle Zertifikatkomponenten) aufgerufen werden. Ungesicherte Zertifikate haben kein Symbol.

Was ist ein Token?

Bei einem Token handelt es sich um eine Sammlung von Schlüsseln, Zertifikaten und CRLs. Das Token wird in einem Medium gespeichert (z. B. einer Datei, einer URL, oder einem Hardwaredatenträger). Es gibt verschiedene Token-Typen mit unterschiedlichen Leistungsmerkmalen, wie beispielsweise Software-Tokens, Hardware-Tokens, ungeschützte Tokens oder Tokens, die durch Kennwörter oder PINs geschützt werden.

Was ist ein Schlüsselring?

Ein Token besteht aus einer Gruppe von Schlüsselringen. Jeder Schlüsselring identifiziert eine bestimmte Gruppe von Komponenten (z. B. Zertifikate derselben Vertrauensebene, Zertifikate, für die Sie über einen privaten Schlüssel verfügen oder Schlüssel ohne zugehörige Zertifikate).

Kapitel 6. Servicequalität (Quality of Service)

Servicequalität (QoS = Quality of Service)

Auf der Linux-Plattform bietet der IBM WebSphere Edge Server über das TQoS-Plug-In eine Lösung für die Zuweisung von Netzbandbreiten. TQoS (Transactional Quality of Service) bezieht sich auf den Service (im Hinblick auf Durchsatz und Verzögerungen), der Netzbenutzern zur Verfügung gestellt wird. Über die Konfiguration von Attributen kann für alle abgehenden Daten auf einer Verbindung eine bestimmte Servicequalität sichergestellt werden. Dies ermöglicht es dem Richtlinienadministrator, Richtlinien für den Datenverkehr bestimmter Server zu definieren sowie Richtlinienaktionen, über die dieser Datenverkehr explizit gesteuert werden kann. Beispielsweise kann in einer Installation eine Richtlinie definiert werden, dass Daten, die im Zuge des Serverdatenverkehrs in Zusammenhang mit dem Verkauf eines bestimmten Warenvolumens gesendet werden, eine höhere Priorität eingeräumt wird als beispielsweise dem Serverdatenverkehr in Zusammenhang mit Clientabfragen. Darüber hinaus bietet TQoS Administratoren die Möglichkeit, Leistungsdaten der entsprechenden Richtlinie zu sammeln, um zu überwachen, ob die Richtlinie die beabsichtigten Servicestufenziele liefert (wichtige Messdaten wie Verbindungsdurchsatz, Verzögerungen, Verlustverhältnis usw.). Für die Implementierung der Servicequalität (QoS) in MQIPT ist nur die Installation und die Aktivierung des Richtlinienagenten (Pagent) erforderlich.

TQoS-Richtlinien werden in einer Konfigurationsdatei für Richtlinien (`pagent.conf`) oder unter Verwendung eines LDAP-Servers definiert. Der TQoS-Pagent kann die TQoS-Richtlinieneinträge entweder aus der Konfigurationsdatei für Richtlinien und/oder vom LDAP-Server abrufen. Im Handbuch *IBM Edge Server Administration Guide* finden Sie weitere Informationen zum Richtlinienagenten. Dieses Handbuch steht unter der folgenden URL zur Verfügung:

<http://www.ibm.com/software/webservers/edgeserver/library.html>

Sie können auf dieser Website das Dokument online im HTML-Format lesen oder als PDF-Version herunterladen. In beiden Formaten ist eine Suche nach "TQoS" möglich.

Der TQoS-Code kann zusammen mit Installations- und Verwaltungsanweisungen von derselben Website wie MQIPT heruntergeladen werden. Besuchen Sie die SupportPacs-Website der WebSphere MQ-Produktfamilie unter <http://www.ibm.com/webspheremq/supportpacs>, und klicken Sie auf 'Category 3 – Product Extensions'.

MQIPT wird mit einer Pseudobibliothek (`libmqiptqos.so`) geliefert, die sich im MQIPT-Unterverzeichnis `lib` befindet. Dadurch kann MQIPT auf der Linux-Plattform ausgeführt werden, ohne dass der TQoS-Pagent installiert werden muss. Nach der Installation von TQoS müssen Sie die Pseudobibliothek gegebenenfalls durch die von TQoS verwendete Bibliothek ersetzen. Das MQIPT-Unterverzeichnis 'bin' enthält ein Script mit dem Namen `mqiptQoS` zur Unterstützung dieser Aufgabe. Benennen Sie die Pseudobibliothek mit dem folgenden Befehl um, und definieren Sie einen Softlink zur tatsächlichen TQoS-Laufzeitbibliothek:

```
mqiptQoS -install
```

Mit dem Befehl `mqiptQoS -remove` können Sie die oben genannten Aktionen rückgängig machen.

Für die Implementierung der Servicequalität (QoS) in MQIPT ist nur die Installation und die Aktivierung des Richtlinienagenten (Pagent) erforderlich. Mit MQIPT kann auf einer Route eine Anwendungspriorität für Daten in beide Richtungen definiert werden, die dann für alle Kanäle dieser Route gilt. Diese Priorität wird über die MQIPT-Eigenschaften **QosToCaller** und **QosToDest** (siehe „Referenzinformationen zum Abschnitt 'route'“ auf Seite 82) festgelegt; die hier verwendeten Werte müssen einer Richtliniendefinition für die Anwendungspriorität in der Steuerdatei `pagent.conf` entsprechen. Findet der Pagent keine entsprechende Richtlinie, wird den Daten keine Priorität zugeordnet. Alle Änderungen an einer Richtlinie werden in MQIPT erst nach einem Neustart des Pagent übernommen. Weitere Informationen zu Richtliniendefinitionen finden Sie unter „Quality of Service (QoS) konfigurieren“ auf Seite 110.

Kapitel 7. Network Dispatcher

Unterstützung für Network Dispatcher

MQIPT kann mit dem IBM Network Dispatcher verwendet werden, um über Anpassungs-Advisors (Custom Advisors) serverübergreifend eine erhöhte Verfügbarkeit und gleichmäßige Auslastung zu ermöglichen. In diesem Abschnitt wird davon ausgegangen, dass Sie mit Network Dispatcher und Anpassungs-Advisors vertraut sind.

Zusammen mit MQIPT werden zwei Anpassungs-Advisors (im Unterverzeichnis **lib**) zur Verfügung gestellt. Informationen zur Installation der Anpassungs-Advisors finden Sie im Handbuch *Network Dispatcher User's Guide* (GC31-8496). In Abb. 7 ist eine Verwendungsmöglichkeit des Network Dispatcher zur Überwachung der Port-Adresse 1414 für MQIPT dargestellt. Jede MQIPT-Instanz muss über dieselbe Konfigurationsdatei verfügen.

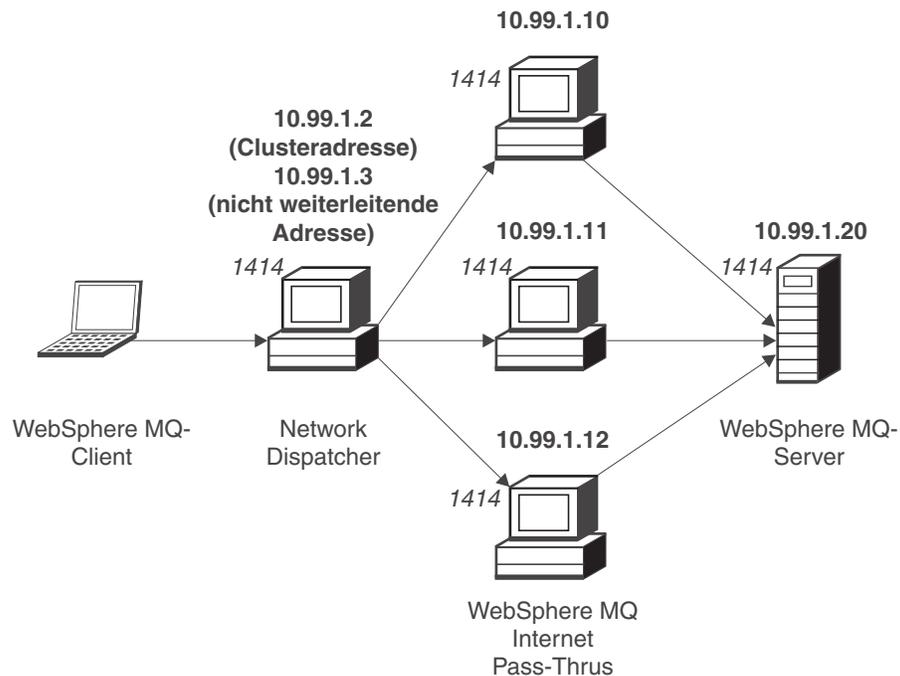


Abbildung 7. Verwendung von Network Dispatcher mit MQIPT

Konfigurationsanweisungen für die Dispatcher-Komponente zur Definition von Port 1414 und zum Festlegen der Servermaschinen für den Lastvergleich finden Sie in Kapitel 5 des Handbuchs *Network Dispatcher User's Guide*. Sie können dabei entweder die Menüoptionen des Verwaltungsclients oder den Zeilenmodusbefehl "ndcontrol" verwenden. Beispiel:

```
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
```

Die Routendefinition in der MQIPT-Konfigurationsdatei würde wie folgt aussehen:

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

Anpassungs-Advisors können nur über die Befehlszeile gestartet bzw. gestoppt werden. Beispiel:

```
ndcontrol advisor start mqipt_normal 1414
```

Mit diesem Befehl wird der MQIPT-Advisor im "normalen" Modus gestartet, in dem der Basis-Advisor eine eigene Ablaufsteuerung für die Berechnung der Gewichtungsfaktoren für die einzelnen MQIPTs vornimmt. Soll der MQIPT-Advisor im Ersetzungsmodus ("replace") verwendet werden, müssen Sie der MQIPT-Routendefinition folgende Zeile hinzufügen:

```
NDAdvisorReplaceMode=true
```

Darüber hinaus müssen Sie anstelle von **mqipt_normal** den Anpassungs-Advisor **mqipt_replace** starten. Beispiel:

```
ndcontrol advisor start mqipt_replace 1414
```

Bei Verwendung eines Advisors für die Überwachung eines SSL-Listener-Ports (d. h., in der Konfigurationsdatei **mqipt.conf** wurde **SSLServer=true** angegeben), müssen Sie in das Arbeitsverzeichnis des Network Dispatcher eine Auslösedatei einfügen. Diese Auslösedatei hat einen bestimmten Namen, der sich auf die Route, die überwacht werden soll, bezieht. Wurde beispielsweise **SSLServer=true** für Route 1414 angegeben, muss in das Verzeichnis **c:\winnt\system32** (unter Windows NT) die Datei **mqipt1414.ssl** eingefügt werden. Weitere Informationen hierzu finden Sie in der Datei **mqipt1414Sample.ssl**.

Kapitel 8. Java Security Manager und Sicherheitsexits

Java Security Manager

Die Unterstützung von Java Security Manager wurde ursprünglich für die Verwendung zusammen mit dem SSL-Proxy-Modus implementiert, und zwar für die Steuerung von Socket-Verbindungen; sie kann jedoch auch mit anderen MQIPT-Merkmalen verwendet werden, um eine weitere Sicherheitsebene bereitzustellen.

MQIPT verwendet den standardmäßigen Java Security Manager, wie er in der Klasse `java.lang.SecurityManager` definiert ist. Die Komponente Java Security Manager in MQIPT kann über die globale Eigenschaft **SecurityManager** (Sicherheitsmanager) aktiviert bzw. deaktiviert werden; weitere Informationen hierzu finden Sie unter „Referenzinformationen zum Abschnitt 'global'“ auf Seite 81.

Der Java Security Manager verwendet zwei standardmäßige Richtliniendateien. Dies ist zum einen eine globale systemspezifische Richtliniendatei (`$JREHOME/lib/security/java.policy`; dabei steht `$JREHOME` für das Verzeichnis, das die JRE (Java Runtime Environment) enthält), die von allen Instanzen einer virtuellen Maschine auf einem Host verwendet wird. Eine zweite benutzerspezifische Richtliniendatei (`.java.policy`) kann sich im Ausgangsverzeichnis des Benutzers befinden. Darüber hinaus kann auch noch eine MQIPT-Richtliniendatei verwendet werden; weitere Informationen hierzu finden Sie unter „Referenzinformationen zum Abschnitt 'global'“ auf Seite 81. Soll eine zusätzliche Richtliniendatei verwendet werden, müssen Sie sicherstellen, dass in der globalen Systemrichtliniendatei (`java.security`) die Eigenschaft **policy.allowSystemProperty** auf **true** gesetzt wurde.

Die Syntax der Richtliniendatei ist sehr komplex; sie kann zwar mit einem Texteditor geändert werden, es wird jedoch geraten, Änderungen mit Hilfe des Dienstprogramms Policytool vorzunehmen, das mit Java geliefert wird. Dieses Dienstprogramm befindet sich im Verzeichnis `$JREHOME/bin` und ist ausführlich in der Java-Dokumentation dokumentiert.

Eine Beispielrichtliniendatei (`mqiptSample.policy`) wird mit MQIPT geliefert; sie zeigt, welche Berechtigungen für den Betrieb von MQIPT gesetzt werden müssen. Damit Sie entsprechend Ihren Vorgaben festlegen können, wer eine Verbindung zu MQIPT herstellen kann und zu wem MQIPT eine Verbindung herstellen kann, müssen lediglich `java.net.SocketPermission`-Einträge hinzugefügt, geändert oder gelöscht werden. Diese Beispieldatei geht davon aus, dass MQIPT im standardmäßigen Ausgangsverzeichnis installiert wurde (z. B. `c:\Programme\IBM\Websphere MQ internet pass-thru\`). Wurde MQIPT in einem anderen Verzeichnis installiert, muss dies in den Definitionen **codeBase** und **java.io.FilePermission** angegeben werden.

Berechtigungen werden in der Regel über drei Attribute definiert; für die Steuerung von Socket-Verbindungen müssen diese Attribute die folgenden Werte haben:

Klassenberechtigung

`java.net.SocketPermission`

Name, für den die Steuerung gelten soll

Dieser Name hat das Format **Hostname:Port**; dabei kann für jede Komponente des Namens ein Platzhalterzeichen angegeben werden. Als Hostname kann ein Domänenname oder eine IP-Adresse angegeben werden. Als erstes Zeichen ganz links ist die Angabe eines Sterns möglich. So wird beispielsweise für jede der folgenden Zeichenfolgen die Zeichenfolge **harry.company1.com** zurückgegeben:

- harry
- harry.company1.com
- *.company1.com
- *
- 123.456.789 (wenn man davon ausgeht, dass dies die IP-Adresse von **harry.company1.com** ist)

Als Port kann im Namen eine einzelne Port-Adresse oder ein Port-Adressenbereich angegeben werden; Beispiel:

1414 nur Port 1414

1414- alle Port-Adressen größer oder gleich 1414

-1414 alle Port-Adressen kleiner oder gleich 1414

1-1414 alle Port-Adressen zwischen 1 und 1414 einschließlich

Zulässige Aktion

Folgende Aktionen werden von **java.net.SocketPermission** verwendet:

- **accept** (Akzeptieren): Erteilt die Berechtigung, Verbindungen vom angegebenen Ziel zu akzeptieren.
- **connect** (Verbinden): Erteilt die Berechtigung, eine Verbindung zum angegebenen Ziel herzustellen.
- **listen** (Überwachen): Erteilt die Berechtigung, den angegebenen Port bzw. die angegebenen Ports auf Verbindungsanforderungen zu überwachen.
- **resolve** (Auflösen): Erteilt die Berechtigung, den DNS-Namensservice für die Auflösung von Domännennamen in IP-Adressen zu verwenden.

Die Steuerung von Java Security Manager kann auch über die Java-Systemeigenschaften **java.security.manager** und **java.security.policy** erfolgen, es wird jedoch geraten, für die Steuerung von MQIPT die Eigenschaften **SecurityManager** (Sicherheitsmanager) und **SecurityManagerPolicy** (Richtlinie für Sicherheitsmanager) zu verwenden.

Sicherheitsexit

Achtung

MQIPT wird in einer einzelnen JVM ausgeführt, d. h., ein benutzerdefinierter Sicherheitsexit kann den normalen Betrieb von MQIPT wie folgt gefährden:

- Beeinträchtigung von Systemressourcen
- Generierung von Engpässen
- Verschlechterung der Leistung

Sie sollten die Auswirkungen eines Sicherheitsexits ausgiebig testen, bevor Sie ihn in einer Produktionsumgebung implementieren.

Der Zweck eines Sicherheitsexits besteht darin, den Zugriff auf eine Zieladresse wie durch die Routeneigenschaft 'Destination' definiert zu steuern. Der Sicherheitsexit wird aufgerufen, nachdem von einem Client eine Verbindungsanforderung empfangen wurde und bevor MQIPT die Verbindung mit der Zieladresse herstellt. Auf der Basis der anfänglichen Verbindungseigenschaften kann der Sicherheitsexit entscheiden, ob die Verbindung vollständig hergestellt werden darf.

Beim Starten einer Route wird der Sicherheitsexit aufgerufen, der dann initialisiert und auf die Verarbeitung einer Verbindungsanforderung vorbereitet wird. Der Initialisierungsprozess sollte dazu verwendet werden, Benutzerdaten zu laden und diese Daten für einen schnellen und einfachen Zugriff vorzubereiten, um so die Zeit für die Verarbeitung einer Verbindungsanforderung zu verkürzen.

Für jede Route kann es einen eigenen Sicherheitsexit geben. Über die Eigenschaft 'SecurityExit' wird der benutzerdefinierte Sicherheitsexit aktiviert bzw. inaktiviert. Über die Eigenschaft 'SecurityExitName' wird der Klassenname des benutzerdefinierten Sicherheitsexits definiert. Über die Eigenschaft 'SecurityExitPath' wird der Name des Verzeichnisses, in dem sich die Klassendatei befindet, definiert. Wenn diese Eigenschaft nicht angegeben ist, wird angenommen, dass sich die Klassendatei im Unterverzeichnis 'exits' befindet. 'SecurityExitPath' kann auch den Namen einer JAR-Datei, die den benutzerdefinierten Sicherheitsexit enthält, angeben. Schließlich legt MQIPT über die Eigenschaft 'SecurityExitTimeout' fest, wie lange bei der Überprüfung einer Verbindungsanforderung auf eine Antwort vom Sicherheitsexit gewartet werden soll.

Es wurde eine neue Klasse mit dem Namen 'SecurityExit' erstellt, mit der MQIPT einen benutzerdefinierten Sicherheitsexit aufrufen kann. Die neue Klasse muss um den benutzerdefinierten Sicherheitsexit erweitert werden, und die meisten Methoden der Klasse sollten überschrieben werden, um die gewünschte Funktionalität bereitzustellen. Mit Hilfe des Objekts 'SecurityExitResponse' werden Daten an MQIPT zurückgegeben, anhand derer MQIPT entscheidet, ob die Verbindungsanforderung akzeptiert oder zurückgewiesen wird. 'SecurityExitResponse' kann auch eine neue Zieladresse und Ziel-Port-Adresse enthalten, mit denen die routendefinierten Eigenschaften überschrieben werden.

Anhand von drei Sicherheitsexitbeispielen wird gezeigt, wie ein Sicherheitsexit implementiert werden kann. Das erste Beispiel, SampleSecurityExit, zeigt, wie der Zugriff auf einen WebSphere MQ-Warteschlangenmanager auf der Basis des WMQ-Kanalnamens gesteuert wird. Es werden nur Verbindungen mit einem Kanalnamen, der mit der Zeichenfolge 'MQIPT' beginnt, zugelassen. Weitere Informationen hierzu finden Sie unter „Sicherheitsexit“ auf Seite 143.

Das zweite Beispiel, SampleRoutingExit, ermöglicht ein dynamisches Routing von Clientverbindungsanforderungen zu einem Pool mit definierten WebSphere MQ-Servern, wobei sich auf jedem Server ein Warteschlangenmanager mit demselben Namen und denselben Attributen befindet. Das Beispiel beinhaltet eine Konfigurationsdatei mit einer Liste von Servernamen. Weitere Informationen hierzu finden Sie unter „Sicherheitsexit weiterleiten“ auf Seite 145.

Das dritte Beispiel, SampleOneRouteExit, ermöglicht ein dynamisches Routing zu einem WMQ-Warteschlangenmanager, der von dem in der Verbindungsanforderung verwendeten WMQ-Kanalnamen abgeleitet wird. Das Beispiel beinhaltet eine Konfigurationsdatei, die eine Zuordnung von WS-Managernamen zu Servernamen enthält. Weitere Informationen hierzu finden Sie unter „Dynamischer Exit bei nur einer Route“ auf Seite 149.

Klasse 'com.ibm.mq.ipt.SecurityExit'

Diese Klasse und ihre öffentlichen Methoden müssen durch den benutzerdefinierten Sicherheitsexit erweitert werden, um Zugriff auf bestimmte allgemeine Daten zu erhalten und bestimmte MQIPT-Initialisierungsprozesse durchführen zu können. Bevor die einzelnen Methoden von MQIPT aufgerufen werden, müssen einige Eigenschaften zur Verfügung gestellt werden, die von den Methoden verwendet werden. Die Werte der Eigenschaften können mit Hilfe der entsprechenden GET-Methode, die in dieser Klasse definiert sind, abgerufen werden. Es folgt eine vollständige Liste der unterstützten Methoden.

Methoden

init

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

Folgende Eigenschaften stehen zur Verfügung:

- Listener-Port
- Zieladresse
- Ziel-Port
- Version

Die Methode 'init' wird beim Starten einer Route von MQIPT aufgerufen. Bei Rückkehr dieser Methode muss der Sicherheitsexit bereit sein, eine Verbindungsanforderung auszuwerten. Wenn von der Methode eine Ausnahmebedingung ausgegeben wird, kann die Route nicht gestartet werden.

refresh

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

Folgende Eigenschaften stehen zur Verfügung:

- Listener-Port
- Zieladresse
- Ziel-Port

Die Methode 'refresh' wird von MQIPT aufgerufen, wenn es vom MQIPT-Verwaltungsclient aufgefordert wurde, sich selbst zu aktualisieren. Diese Aktion wird in der Regel aufgerufen, wenn eine Eigenschaft in der Konfigurationsdatei geändert wurde. MQIPT lädt alle Eigenschaften aus der Konfigurationsdatei, um zu ermitteln, welche geändert wurden, ob eine Route sofort erneut gestartet werden muss oder ob damit bis zum nächsten Neustart von MQIPT gewartet werden kann.

Diese Methode lädt normalerweise alle von ihr verwendeten externen Daten erneut (d. h. Daten, die von der Methode 'init' geladen wurden). Wenn von der Methode eine Ausnahmebedingung ausgegeben wird, wird die Route inaktiviert.

close

```
public void close ()
```

Folgende Eigenschaften stehen zur Verfügung:

- Listener-Port
- Zieladresse
- Ziel-Port

Die Methode 'close()' wird von MQIPT aufgerufen, wenn es vom MQIPT-Verwaltungsclient zum Stoppen aufgefordert wurde. In der Regel werden alle Systemressourcen, die während der Verarbeitung belegt wurden, freigegeben. MQIPT wartet, bis diese Methode abgeschlossen ist, bevor es sich selbst beendet.

Diese Methode wird auch aufgerufen, wenn ein Sicherheitsexit zunächst aktiviert, aber dann in der Konfigurationsdatei inaktiviert wurde.

validate

```
public SecurityExitResponse validate ()
```

Folgende Eigenschaften stehen zur Verfügung:

- Listener-Port
- Zieladresse
- Ziel-Port
- Zeitlimit
- Client-IP-Adresse
- Client-Port-Adresse
- Kanalname
- WS-Managername

Die Methode 'validate' wird von MQIPT aufgerufen, wenn es eine zu überprüfende Verbindungsanforderung empfangen hat. Der Kanalname und der WS-Managername stehen nicht zur Verfügung, wenn die Eigenschaft 'SSLProxyMode' aktiviert ist, da dieses Merkmal nur zum Tunneln von SSL-Daten verwendet wird und die Daten, die normalerweise mit dem ersten Datenfluss empfangen werden, deshalb nicht lesbar sind. Der WS-Managername steht für WMQ-Clientverbindungen nicht zur Verfügung, weil diese Information erst verfügbar ist, nachdem die Verbindung mit dem Zielwarteschlangenmanager hergestellt wurde.

Der Sicherheitsexit muss ein Objekt 'SecurityExitResponse' mit folgenden Informationen zurückgeben:

- Ursachencode (muss angegeben sein)
- neue Zieladresse (optional)
- neue Adresse für Ziel-Listener-Port (optional)
- Nachricht (optional)

Der Ursachencode entscheidet, ob die Verbindung von MQIPT akzeptiert oder zurückgewiesen wird. Die Felder 'newDestination' und 'newDestinationPort' können optional angegeben werden, um ein neues Ziel (WS-Manager) zu definieren. Wenn diese Eigenschaften nicht angegeben werden, werden die in der Konfigurationsdatei definierten Routeneigenschaften 'Destination' und 'DestinationPort' verwendet. Nachrichten werden an den Verbindungsprotokolldateieintrag angehängt.

Unterstützte Methoden zum Abrufen von Eigenschaften:

public int getListenerPort()

Ruft den Listener-Port der Route ab - wie durch die Eigenschaft 'ListenerPort' definiert.

public String getDestination()

Ruft die Zieladresse ab - wie durch die Eigenschaft 'Destination' definiert.

public int getDestinationPort()

Ruft die Adresse des Ziel-Listener-Ports ab - wie durch die Eigenschaft 'DestinationPort' definiert.

public String getClientIPAddress()

Ruft die IP-Adresse des Clients, von dem die Verbindungsanforderung kommt, ab.

public int getClientPortAddress()

Ruft die Port-Adresse ab, die vom Client, von dem die Verbindungsanforderung kommt, verwendet wird.

public int getTimeout()

Ruft das Zeitlimit ab. MQIPT wartet, bis der Sicherheitsexit eine Anforderung überprüft hat - wie durch die Eigenschaft 'SecurityExitTimeout' definiert.

public int getConnThreadID()

Ruft die Verbindungs-Thread-ID, unter der die Verbindungsanforderung bearbeitet wird, ab (für Debug-Zwecke hilfreich).

public String getChannelName()

Ruft den WMQ-Kanalnamen ab, der in der Verbindungsanforderung verwendet wird.

public String getQMName()

Ruft den WMQ-WS-Managernamen ab, der in der Verbindungsanforderung verwendet wird.

public boolean getTimedout()

Kann vom Sicherheitsexit verwendet werden, um zu ermitteln, ob das Zeitlimit abgelaufen ist.

Klasse 'com.ibm.mq.ipt.SecurityExitResponse'

Diese Klasse wird verwendet, um von einem benutzerdefinierten Sicherheitsexit eine Antwort an MQIPT zurückzugeben und um zu ermitteln, ob die Verbindungsanforderung akzeptiert oder zurückgewiesen werden soll. Objekte dieses Typs werden nur in der Methode 'validate' erstellt (siehe oben). Zum Erstellen dieser Objekte stehen benutzerfreundliche Konstruktoren und für jede Eigenschaft Festlegungsmethoden zur Verfügung. Weitere Informationen finden Sie in den Sicherheitsexitbeispielen.

Durch das Erstellen eines SecurityExitResponse-Standardobjekts wird die Verbindungsanforderung zurückgewiesen.

Unterstützte Konstruktoren:

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

Dabei gilt Folgendes:

- dest ist die neue Zieladresse.
- destPort ist die neue Ziel-Port-Adresse.
- rc ist der Ursachencode.
- msg ist eine Nachricht, die zum Verbindungsprotokolleintrag hinzugefügt wird.

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

```
public SecurityExitResponse (int rc, String msg) throws IPTException
```

```
public SecurityExitResponse (int rc) throws IPTException
```

Unterstützte Methoden zum Festlegen von Eigenschaftswerten:

```
public void setDestination(String dest)
```

Legt eine neue Zieladresse für die Verbindungsanforderung fest.

```
public void setDestinationPort(int port) throws IPTException
```

Legt eine neue Adresse für den Ziel-Listener-Port für die Verbindungsanforderung fest - Ausgabe einer IPTException-Ausnahmebedingung bei einer ungültigen Adresse.

```
public void setMessage(String msg)
```

Fügt eine Nachricht zum Verbindungsprotokollsatz hinzu.

```
public void setReasonCode(int rc) throws IPTException
```

Legt den Ursachencode für die Verbindungsanforderung fest - Ausgabe einer IPTException-Ausnahmebedingung bei einem unbekanntem Wert.

Gültige Ursachencodes:

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

Tracefunktion

Zur Unterstützung der Fehlerdiagnose in einem benutzerdefinierten Sicherheitsexit können Sie eine Tracefunktion aktivieren, die der von MQIPT ähnlich ist. Wenn Sie die Routeneigenschaft 'Trace' auf einen Wert von 1-5 setzen, wird im Unterverzeichnis 'errors' eine Tracedatei erstellt. Der Name der Tracedatei entspricht dem Namen des Sicherheitsexits.

Häufig sind mehrere Instanzen des Sicherheitsexits gleichzeitig aktiv. In solchen Fällen können Sie die einzelnen Einträge in der Tracedatei anhand der Thread-ID zuordnen.

Die Tracefunktionen werden von MQIPT initialisiert, wenn der Sicherheitsexit gestartet wird; Sie müssen lediglich die Informationen auswählen, für die ein Trace durchgeführt werden soll. Die Beispielbenutzerexits enthalten eine Vielzahl von Tracebeispielen.

Die Mindestvoraussetzungen für einen Trace sind ein entry-Aufruf, ein exit-Aufruf und die Daten, für die der Trace durchgeführt werden soll. Beispiel:

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

Kapitel 9. Port-Adresssteuerung

Port-Adresssteuerung

Bei der Nutzung von MQIPT kann der Bereich der lokalen Port-Adressen, die zum Herstellen abgehender Verbindungen verwendet werden, eingeschränkt werden, indem auf der Route die Eigenschaft `OutgoingPort` festgelegt wird. Der Bereich der lokalen Port-Adressen wird über den Wert `MaxConnectionThreads` berechnet. Wenn beispielsweise `OutgoingPort` auf 1600 und `MaxConnectionThreads` auf 20 festgelegt ist, liegt der Bereich der lokalen Port-Adressen für die betreffende Route bei 1600-1619. Der MQIPT-Administrator muss sicherstellen, dass auf Routen keine Konflikte zwischen Port-Adressen auftreten. Wenn `OutgoingPort` nicht definiert ist, wird der Standardwert 0 verwendet, d. h., für jede Verbindung wird eine vom System zugeordnete Port-Adresse verwendet.

Weitere Informationen finden Sie im Beispiel „Port-Adressen zuordnen“ auf Seite 132.

Multihomed-Systeme

Bei Verwendung eines Multihomed-Systems können Sie über die Eigenschaft `LocalAddress` angeben, an welche IP-Adresse eine abgehende Verbindung gebunden werden soll. Hostnamen werden für diese Eigenschaft nicht unterstützt.

Kapitel 10. Weitere Sicherheitsüberlegungen

Weitere Sicherheitsüberlegungen

Wenn Sie das SSL-Protokoll nicht verwenden, bietet MQIPT Sicherheitsabläufe für Kanäle; auf diese Weise können WebSphere MQ-Kanalexits verwendet werden, um die Sicherheit für den gesamten Kanal von einem Ende zum anderen zu gewährleisten.

MQIPT verfügt über mehrere zusätzliche Funktionen, die es dem Designer ermöglichen, eine sichere Lösung zu implementieren:

- Enthält ein internes Netz sehr viele Clients, die ausgehende Verbindungen anfordern, können diese alle über einen MQIPT innerhalb der Firewall geführt werden. Der Firewall-Administrator muss dann nur der MQIPT-Maschine eine externe Zugriffsberechtigung erteilen.
- MQIPT kann nur mit solchen WS-Managern eine Verbindung herstellen, die explizit in der MQIPT-Konfigurationsdatei angegeben sind, außer MQIPT wird als SOCKS-Proxy eingesetzt oder verwendet einen Sicherheitsexit.
- MQIPT überprüft, ob die von ihm empfangenen und gesendeten Nachrichten gültig sind und dem WebSphere MQ-Protokoll entsprechen. Dadurch wird verhindert, dass MQIPT für Hacker-Attacken außerhalb des WebSphere MQ-Protokolls benutzt wird. Wird MQIPT als SSL-Proxy eingesetzt und wurden alle WebSphere MQ-Daten und -Protokolle verschlüsselt, kann MQIPT nur den anfänglichen SSL-Handshake garantieren. In diesem Fall sollten Sie den Java Security Manager verwenden (siehe „Java Security Manager“ auf Seite 31).
- MQIPT lässt zu, dass Kanalexits ihre eigenen durchgehenden Sicherheitsprotokolle ausführen.
- MQIPT ermöglicht es Ihnen, die maximale Anzahl ankommender Verbindungen über die Eigenschaft **MaxConnectionThreads** (Max. Anzahl Verbindungs-Threads) festzulegen. Dadurch können ungeschützte interne WS-Manager vor Denial-of-Service-Attacken geschützt werden.

Sie müssen die MQIPT-Konfigurationsdatei (**mqipt.conf**) schützen, da diese Datei den Zugriff auf die internen Hosts steuert; darüber hinaus müssen Sie unbefugte Zugriffe auf den Befehls-Port (sofern aktiviert) verhindern, da ein solcher Zugriff es Unbefugten ermöglichen würde, MQIPT herunterzufahren.

Kapitel 11. Verschiedenes

Normale Beendigung und Fehlerbedingungen

Wenn MQIPT feststellt, dass ein WebSphere MQ-Kanal beendet wird (normal oder abnormal), so wird diese Kanalbeendigung weitergegeben. Beendet der Administrator eine Route über MQIPT, werden alle Kanäle, die diese Route verwenden, ebenfalls geschlossen.

MQIPT ermöglicht die Angabe eines optionalen Zeitlimits für Inaktivität. Wenn MQIPT feststellt, dass die Leerlaufzeit eines Kanals das festgesetzte Zeitlimit überschreitet, beendet es sofort die beiden betreffenden Verbindungen.

Die beiden WebSphere MQ-Systeme an beiden Enden des Kanals interpretieren diese abnormale Beendigung als Netzfehler oder als Beendigung durch den jeweiligen Partner. Die betreffenden Kanäle können anschließend erneut gestartet und wiederhergestellt werden (falls die Störung auftritt, während sich das Protokoll im unbestätigten Status befindet), wie dies auch der Fall wäre, wenn keine MQIPTs verwendet würden.

Nachrichtensicherheit

Bei Verwendung von schnellen, nicht permanenten WebSphere MQ-Nachrichten gehen Nachrichten unter Umständen verloren, wenn eine MQIPT-Route ausfällt oder erneut gestartet wird, während gerade eine WebSphere MQ-Nachricht übertragen wird. Bevor die Route erneut gestartet wird, sollten Sie daher sicherstellen, dass alle WebSphere MQ-Kanäle, die die MQIPT-Route verwenden, inaktiv sind.

Weitere Informationen zu WebSphere MQ-Nachrichten und -Kanälen finden Sie im Handbuch *MQSeries Intercommunication* (SC33-1872).

Verbindungsprotokolle

MQIPT bietet eine Einrichtung zur Generierung von Verbindungsprotokollen, in denen alle erfolgreichen und fehlgeschlagenen Verbindungsversuche aufgeführt werden. Diese Funktion wird über die Eigenschaften **ConnectionLog** (Verbindungsprotokoll) und **MaxLogFileSize** (Max. Protokolldateigröße) gesteuert. Weitere Informationen hierzu finden Sie unter „Referenzinformationen zum Abschnitt 'global'“ auf Seite 81.

Bei jedem Start von MQIPT wird ein neues Verbindungsprotokoll erstellt. Zur besseren Kennzeichnung enthält der Dateiname die aktuelle Zeitmarke, z. B.:

```
mqiptJJJMMTTHHmSS.log
```

Dabei gilt Folgendes:

- JJJJ steht für das Jahr
- MM steht für den Monat
- TT steht für den Tag
- HH steht für die Stunde
- mm steht für die Minuten
- SS steht für die Sekunden

Damit sie für Prüfungszwecke herangezogen werden können, werden diese Protokolldateien nie gelöscht. Für die Verwaltung dieser Dateien ist der MQIPT-Administrator zuständig; er muss sie löschen, wenn sie nicht mehr benötigt werden.

Kapitel 12. Upgrade von der früheren Version

Gehen Sie zum Upgrade von MQIPT von Version 1.2 auf Version 1.3 wie folgt vor:

1. Erstellen Sie eine Kopie der Konfigurationsdateien `mqipt.conf` und `client.conf`. `mqipt.conf` befindet sich im MQIPT-Ausgangsverzeichnis und `client.conf` im Unterverzeichnis 'bin'.
2. Stoppen Sie MQIPT, indem Sie den folgenden Befehl ausführen:
`mqiptAdmin -stop`
3. Wenn MQIPT als Service installiert wurde, müssen Sie diesen vor der Deinstallation von MQIPT zunächst entfernen:
`mqiptService -remove`
4. Führen Sie das Deinstallationsprogramm für MQIPT aus.
5. Kopieren Sie nach der Installation von MQIPT V1.3 die gespeicherten Konfigurationsdateien wieder zurück an ihre ursprünglichen Standorte.
6. Es wird empfohlen, Änderungen an MQIPT über die grafische Benutzerschnittstelle (GUI) für die MQIPT-Verwaltung vorzunehmen. Die Konfigurationsdatei von MQIPT V1.2 ist mit dieser GUI kompatibel.

Einige Implementierungen erfordern einen lokalen MQIPT-Service, der von Ihrer eigenen Organisation gesteuert wird, sowie einen fernen MQIPT-Service, der von Ihrer Clientorganisation gesteuert wird. In diesem Fall ist es sehr schwierig, beide MQIPT-Services gleichzeitig zu migrieren, dies ist jedoch für MQIPT kein Problem. Sofern nicht anders erwähnt, sind frühere Versionen von MQIPT mit der neuesten Version kompatibel. Dadurch wird der MQIPT-Migrationsprozess erheblich erleichtert.

Es besteht auch die Möglichkeit, ein Upgrade des MQIPT-Kerns durchzuführen, ohne dass MQIPT zuvor deinstalliert werden muss. Alle zur Ausführung von MQIPT benötigten Klassen sind in der Datei 'MQipt.jar' gespeichert. Sie können die neueste Version von MQIPT auf einer anderen Maschine installieren und die Datei 'MQipt.jar' von dieser Installation auf Ihr Live-System kopieren. Dasselbe gilt für die Klassen, die zur Ausführung der Verwaltungs-GUI benötigt werden. Diese befinden sich in der Datei 'guiadmin.jar'.

Neue Konfigurationsoptionen

Version 1.3 bietet die folgenden neuen Eigenschaften:

- 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

Informationen zu allen Eigenschaften finden Sie unter „Referenzinformationen zur Konfiguration“ auf Seite 76.

Kapitel 13. Internet Pass-Thru unter Windows installieren

In diesem Kapitel wird die Installation von MQIPT auf einem Windows NT-, Windows 2000- oder Windows XP-System beschrieben:

- „Dateien herunterladen und installieren“
- „WebSphere MQ Internet Pass-Thru einrichten“ auf Seite 48
- „WebSphere MQ Internet Pass-Thru über die Befehlszeile starten“ auf Seite 48
- „Verwaltungsclient über die Befehlszeile starten“ auf Seite 49
- „Ein Windows-Dienststeuerungsprogramm verwenden“ auf Seite 50
- „Internet Pass-Thru als Windows-Dienst deinstallieren“ auf Seite 50
- „WebSphere MQ Internet Pass-Thru deinstallieren“ auf Seite 50

Dateien herunterladen und installieren

MQIPT (MS81, ein SupportPac der Kategorie 3) kann von der folgenden WebSphere MQ SupportPac-Webseite heruntergeladen werden:

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

Laden Sie die Datei entsprechend den Hinweisen herunter.

Öffnen Sie ein Befehlseingabefenster, und entpacken Sie die Datei `ms81_nt.zip` in einem temporären Verzeichnis. Führen Sie anschließend die Datei `setup.exe` aus, und gehen Sie anhand der Onlineanweisungen vor.

MQIPT muss von einem Benutzer mit Administratorberechtigung installiert werden.

MQIPT enthält die in der folgenden Tabelle aufgeführten Dateien; in der nächsten Tabelle sehen Sie die Dateien für den Verwaltungsclient (die grafische Benutzerschnittstelle), der als separat installierbare Komponente geliefert wird.

Datei	Funktion
Readme.txt	Enthält die neuesten Informationen, die nicht in den Veröffentlichungen zu finden sind
mqiptSample.conf	Beispielkonfigurationsdatei
ssl\sslSample.pfx	Schlüsselringdatei zum Testen von SSL-Verbindungen
ssl\sslSample.pwd	Kennwortdatei für die Schlüsselringdatei
ssl\sslCAdefault.pfx	CA-Schlüsselringdatei (Beispieldatei)
ssl\sslCAdefault.pwd	Kennwortdatei für die CA-Schlüsselringdatei
ssl\KeyMan.zip	Dienstprogramm KeyMan
exits\ SampleOneRouteExit.java	Beispielsicherheitsexit
exits\ SampleOneRouteExit.conf	Konfigurationsdatei für SampleOneRouteExit
exits\ SampleRoutingExit.java	Beispielsicherheitsexit
exits\ SampleRoutingExit.conf	Konfigurationsdatei für SampleRoutingExit
exits\ SampleSecurityExit.java	Beispielsicherheitsexit

Datei	Funktion
lib\MQipt.jar	Enthält die Laufzeit-, Klassen- und Eigenschaftsdateien
lib\ADV_mqipt_normal.class	Network Dispatcher-Advisor für "normalen" Modus
lib\ADV_mqipt_replace.class	Network Dispatcher-Advisor für Ersetzungsmodus ("replace")
lib\mqipt1414Sample.ssl	Beispielauslösedatei für den Network Dispatcher-Advisor
bin\mqipt.bat	Direktaufruf für die Aktivierung von MQIPT über die Befehlszeile
bin\mqiptAdmin.bat	Direktaufruf zum Stoppen von MQIPT und zur Aktualisierung von Dateiinformatoren
bin\mqiptPW.bat	Verschlüsselungskennwort zum Öffnen von Schlüsselringdateien
bin\mqiptservice.exe	Ausführbare Datei zum Hinzufügen von MQIPT zum Dienststeuerungs-Manager von Windows bzw. zum Entfernen von MQIPT aus dem Dienststeuerungs-Manager
bin\mqiptVersion.bat	Zum Anzeigen der Versionsnummer von MQIPT
web\MQIPTServlet.war	Webarchivierungsdatei für die Servlet-Version
doc\<<Sprache>\html\ <Dateiname>.zip	Hauptdatei für das Handbuch <i>WebSphere MQ Internet Pass-Thru</i> im HTML-Format. Weitere Informationen zur Softcopy der Dokumentation finden Sie unter „Literaturverzeichnis“ auf Seite 179.

Zur grafischen Benutzerschnittstelle "Verwaltungsclient" gehören folgende Dateien:

Datei	Funktion
lib\guiadmin.jar	Enthält die Laufzeit-, Klassen- und Eigenschaftsdateien
bin\mqiptGui.bat	Direktaufruf für die Aktivierung des Verwaltungsclients über die Befehlszeile
bin\customSample. Eigen- schaften	Beispieldatei für die Anpassung der Darstellung des Verwaltungsclients und damit der Zugriffsmöglichkeiten auf diesen Client

Das Installationsprogramm aktualisiert die Systemumgebungsvariable CLASS-PATH, indem es den Pfad zu den Dateien **MQipt.jar** und **guiadmin.jar** hinzufügt.

WebSphere MQ Internet Pass-Thru einrichten

Bevor MQIPT zum ersten Mal gestartet wird, müssen Sie die Beispielkonfigurationsdatei **mqiptSample.conf** in die Datei **mqipt.conf** kopieren. Weitere Informationen finden Sie in Kapitel 19, „WebSphere MQ Internet Pass-Thru verwalten und konfigurieren“, auf Seite 71.

WebSphere MQ Internet Pass-Thru über die Befehlszeile starten

Öffnen Sie ein Befehlseingabefenster, wechseln Sie in das Verzeichnis **bin**, und führen Sie **mqipt** aus. Beispiel:

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

Sie können MQIPT auch über **Programme** im Startmenü von Windows starten.

Bei Ausführung des Scripts `mcipt` ohne Angabe von Optionen wird eine Standardadresse (".") für die Konfigurationsdatei `mcipt.conf` verwendet. So geben Sie ein anderes Verzeichnis an:

```
mcipt  
<Verzeichnisname>
```

An der Konsole werden Nachrichten zum Status von MQIPT angezeigt. Sollte ein Fehler auftreten, lesen Sie unter „Fehlerbestimmung“ auf Seite 153 nach. Im Folgenden ein Beispiel für die Nachrichten, die beim erfolgreichen Start von MQIPT angezeigt werden:

```
| 5639-L92 (C) Copyright IBM Corp. 2000, 2003 Alle Rechte vorbehalten.  
| MQCPI001 WebSphere MQ Internet Pass-Thru Version 1.3.0 wird gestartet.  
| MQCPI004 Die Konfigurationsdaten aus c:\mcipt\mcipt.conf werden gelesen.  
| MQCPI008 Empfangsbereit für Steuerbefehle an Port 1881.  
| MQCPI011 Die Protokolldateien werden im Pfad c:\mcipt\logs gespeichert.  
| MQCPI006 Route 1418 wurde gestartet und leitet Nachrichten weiter an :  
| MQCPI034 ....mqserver.company4.com(1414)  
| MQCPI035 ....verwendet MQ-Protokolle  
| MQCPI078 Route 1418 für Verbindungsanforderungen bereit.  
| MQCPI006 Route 1415 wurde gestartet und leitet Nachrichten weiter an :  
| MQCPI034 ....mcipt.company2.com(1415)  
| MQCPI035 ....verwendet MQ-Protokolle  
| MQCPI036 ....SSL-Clientseite mit folgenden Eigenschaften aktiviert :  
| MQCPI031 .....Cipher Suites <null>  
| MQCPI032 .....Schlüsselringdatei c:\mcipt\KeyMan.pfx  
| MQCPI038 .....registrierte Namen CN=*Doe O=IBM OU=* L=* ST=* C=*  
| MQCPI078 Route 1415 für Verbindungsanforderungen bereit.
```

Wenn MQIPT zum ersten Mal aufgerufen wird, werden automatisch die folgenden Unterverzeichnisse für das Ausgangsverzeichnis `mcipt` erstellt:

- Verzeichnis **log**, in dem das Verbindungsprotokoll gespeichert wird
- Verzeichnis **errors**, in das FFST- (First Failure Support Technology) und Trace-sätze geschrieben werden

Verwaltungsclient über die Befehlszeile starten

Öffnen Sie ein Befehlseingabefenster, wechseln Sie in das Verzeichnis `bin`, und führen Sie `mciptGui` aus. Beispiel:

```
c:  
cd \mcipt\bin  
mciptGui
```

Damit der Verwaltungsclient unter Verwendung eines SOCKS-Proxy eine Verbindung zu einem MQIPT jenseits einer Firewall herstellen kann, müssen Sie den Hostnamen oder die Adresse und die Port-Nummer angeben:

```
mciptGui <SOCKS-Hostname <SOCKS-Port>>
```

Standardeinstellung für den **SOCKS-Port** ist **1080**.

Der Status des Verwaltungsclients wird anhand von Nachrichten im Hauptfenster des Verwaltungsclients angezeigt.

Ein Windows-Dienststeuerungsprogramm verwenden

Es wird ein separates Dienststeuerungsprogramm (**mqiptservice.exe**) zur Verfügung gestellt, mit dem MQIPT als Windows-Dienst verwaltet und gestartet werden kann.

Für **mqiptservice.exe** können in der Befehlszeile die folgenden Argumente angegeben werden:

mqiptservice -install Pfad

Installiert und registriert den Dienst, so dass er im Windows-Dienstfenster als manueller Dienst angezeigt wird. Öffnen Sie das Dienstfenster, und ändern Sie die Einstellung in "automatisch"; dadurch wird MQIPT beim Systemstart automatisch gestartet. Nach der Installation dieses Dienstes müssen Sie Windows erneut starten. Die Angabe des Pfades ist erforderlich; es muss der vollständig qualifizierte Pfad zu dem Verzeichnis, das die Konfigurationsdatei **mqipt.conf** enthält, angegeben werden. Enthält der Pfadname Leerzeichen, muss er in Anführungszeichen gesetzt werden.

mqiptservice -remove

Entfernt den Dienst; er wird nicht mehr im Dienstfenster angezeigt.

mqiptservice ?

Zeigt Hilfenachrichten (in amerikanischem Englisch) mit den zulässigen Argumenten an.

Die gleichzeitige Angabe von **install** und **remove** für ein und denselben Befehl führt zu einem Fehler.

Intern ruft Windows das Programm **mqiptservice** ohne Argumente auf. Wenn Sie das Programm dagegen über die Befehlszeile ohne die Angabe von Argumenten aufrufen, reagiert das Programm mit einer Zeitlimitüberschreitung und gibt einen Fehler zurück.

Beim Start des MQIPT-Dienstes werden auch alle aktiven MQIPT-Routen gestartet. Wird dieser Dienst gestoppt, werden alle Routen ebenfalls umgehend beendet.

Anmerkung: Die Systemumgebungsvariable PATH muss den Pfad zu den JNI-Laufzeitbibliotheken enthalten. Die Datei **jvm.dll** befindet sich im JDK-Unterverzeichnis **client**.

Internet Pass-Thru als Windows-Dienst deinstallieren

Sie können MQIPT als Dienst deinstallieren, indem Sie es zunächst über das Windows-Dienstfenster stoppen. Öffnen Sie anschließend ein Befehlseingabefenster, wechseln Sie in das MQIPT-Verzeichnis **bin**, und geben Sie den folgenden Befehl ein:

```
mqiptservice -remove
```

WebSphere MQ Internet Pass-Thru deinstallieren

Bevor Sie MQIPT auf Ihrem System deinstallieren, müssen Sie es zunächst wie oben beschrieben als Windows-Dienst entfernen. Führen Sie dann über das Startmenü von Windows das Deinstallationsprogramm aus.

Kapitel 14. WebSphere MQ Internet Pass-Thru unter Sun Solaris installieren

In diesem Kapitel wird die Installation von MQIPT unter Sun Solaris beschrieben:

- „Dateien herunterladen und installieren“
- „WebSphere MQ Internet Pass-Thru einrichten“ auf Seite 52
- „WebSphere MQ Internet Pass-Thru über die Befehlszeile starten“ auf Seite 52
- „WebSphere Internet Pass-Thru automatisch starten“ auf Seite 53
- „Verwaltungsclient über die Befehlszeile starten“ auf Seite 53
- „WebSphere MQ Internet Pass-Thru deinstallieren“ auf Seite 54

Dateien herunterladen und installieren

MQIPT kann von der WebSphere MQ SupportPac-Webseite unter der folgenden Adresse heruntergeladen werden:

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

Laden Sie die Datei entsprechend den Hinweisen herunter.

Melden Sie sich als **root** an, und dekomprimieren und entpacken Sie die Datei **ms81_sol.tar.Z** in einem temporären Verzeichnis. Führen Sie den Befehl `pkgadd` wie im folgenden Beispiel gezeigt aus:

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

In diesem Beispiel wird davon ausgegangen, dass sich **ms81_sol.tar.Z** im Verzeichnis **/tmp** befindet.

MQIPT enthält die in der folgenden Tabelle aufgeführten Dateien; dazu gehören auch die Dateien des Verwaltungsclients (die grafische Benutzerschnittstelle).

Datei	Funktion
Readme.txt	Enthält die neuesten Informationen, die nicht in den Veröffentlichungen zu finden sind
mqiptSample.conf	Beispielkonfigurationsdatei
ssl/sslSample.pfx	Schlüsselringdatei zum Testen von SSL-Verbindungen
ssl/sslSample.pwd	Kennwortdatei für die Schlüsselringdatei
ssl/sslCAdefault.pfx	CA-Schlüsselringdatei (Beispieldatei)
ssl/sslCAdefault.pwd	Kennwortdatei für die CA-Schlüsselringdatei
ssl/KeyMan.zip	Dienstprogramm KeyMan
exits/ SampleOneRouteExit.java	Beispielsicherheitsexit
exits/ SampleOneRouteExit.conf	Konfigurationsdatei für SampleOneRouteExit
exits/SampleRoutingExit.java	Beispielsicherheitsexit

Datei	Funktion
exits/SampleRoutingExit.conf	Konfigurationsdatei für SampleRoutingExit
exits/SampleSecurityExit.java	Beispielsicherheitsexit
lib/MQipt.jar	Enthält die Laufzeit-, Klassen- und Eigenschaftsdateien
lib\ADV_mqipt_normal.class	Network Dispatcher-Advisor für "normalen" Modus
lib\ADV_mqipt_replace.class	Network Dispatcher-Advisor für Ersetzungsmodus ("replace")
lib/mqipt1414Sample.ssl	Beispielauslösedatei für den Network Dispatcher-Advisor
bin/mqipt	Direktaufruf für die Aktivierung von MQIPT über die Befehlszeile
bin/mqiptAdmin	Direktaufruf zum Stoppen von MQIPT und zur Aktualisierung von Dateinformationen
bin/mqiptPW	Verschlüsselungskennwort zum Öffnen von Schlüsselringdateien
bin/mqiptVersion	Zum Anzeigen der Versionsnummer von MQIPT
bin/mqiptService	Installiert MQIPT so, dass es bei jedem Systemstart automatisch ebenfalls gestartet wird
bin/mqiptEnv	Gibt den Pfad zur Datei mqipt.jar an; wird nur von den anderen Scripts verwendet
web/MQIPTServlet.war	Webarchivierungsdatei für die Servlet-Version
doc/<Sprache>/html/<Dateiname>.zip	Hauptdatei für das Handbuch <i>WebSphere MQ Internet Pass-Thru</i> im HTML-Format. Weitere Informationen zur Softcopy der Dokumentation finden Sie unter „Literaturverzeichnis“ auf Seite 179.
lib/guiadmin.jar	Enthält Laufzeit-, Klassen- und Eigenschaftsdateien für die grafische Benutzerschnittstelle "Verwaltungsclient"
bin/mqiptGui	Direktaufruf für die Ausführung des Verwaltungsclients über die Befehlszeile
bin/customSample. Eigenschaften	Beispieldatei für die Anpassung der Darstellung des Verwaltungsclients und damit der Zugriffsmöglichkeiten auf diesen Client

WebSphere MQ Internet Pass-Thru einrichten

Bevor MQIPT zum ersten Mal gestartet wird, müssen Sie die Beispielkonfigurationsdatei **mqiptSample.conf** in die Datei **mqipt.conf** kopieren. Weitere Informationen finden Sie in Kapitel 19, „WebSphere MQ Internet Pass-Thru verwalten und konfigurieren“, auf Seite 71.

WebSphere MQ Internet Pass-Thru über die Befehlszeile starten

Melden Sie sich als **root** an, und wechseln Sie in das Verzeichnis **bin**. Beispiel:

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

Bei Ausführung des Scripts **mqipt** ohne Angabe von Optionen wird eine Standardadresse (".") für die Konfigurationsdatei **mqipt.conf** verwendet. So geben Sie ein anderes Verzeichnis an:

```
mqipt
<Verzeichnisname>
```

An der Konsole werden Nachrichten zum Status von MQIPT angezeigt. Sollte ein Fehler auftreten, lesen Sie unter „Fehlerbestimmung“ auf Seite 153 nach. Im Folgenden ein Beispiel für die Nachrichten, die beim erfolgreichen Start von MQIPT angezeigt werden:

```
| 5639-L92 (C) Copyright IBM Corp. 2000, 2003 Alle Rechte vorbehalten.  
| MQCPI001 WebSphere MQ Internet Pass-Thru Version 1.3.0 wird gestartet.  
| MQCPI004 Die Konfigurationsdaten aus /opt/mqipt/mqipt.conf werden gelesen.  
| MQCPI008 Empfangsbereit für Steuerbefehle an Port 1881.  
| MQCPI011 Die Protokolldateien werden im Pfad /opt/mqipt/logs gespeichert.  
| MQCPI006 Route 1418 wurde gestartet und leitet Nachrichten weiter an :  
| MQCPI034 ....mqserver.company4.com(1414)  
| MQCPI035 ....verwendet MQ-Protokolle  
| MQCPI078 Route 1418 für Verbindungsanforderungen bereit.  
| MQCPI006 Route 1415 wurde gestartet und leitet Nachrichten weiter an :  
| MQCPI034 ....mqipt.company2.com(1415)  
| MQCPI035 ....verwendet MQ-Protokolle  
| MQCPI036 ....SSL-Clientsseite mit folgenden Eigenschaften aktiviert :  
| MQCPI031 .....Cipher Suites <null>  
| MQCPI032 .....Schlüsselringdatei /opt/mqipt/KeyMan.pfx  
| MQCPI038 .....registrierte Namen CN=*Doe O=IBM OU=* L=* ST=* C=*  
| MQCPI078 Route 1415 für Verbindungsanforderungen bereit.
```

Wenn MQIPT zum ersten Mal aufgerufen wird, werden automatisch die folgenden Unterverzeichnisse für das Ausgangsverzeichnis **mqipt** erstellt:

- Verzeichnis **log**, in dem das Verbindungsprotokoll gespeichert wird
- Verzeichnis **errors**, in das FFST- (First Failure Support Technology) und Trace-sätze geschrieben werden

WebSphere Internet Pass-Thru automatisch starten

Damit MQIPT beim Systemstart automatisch gestartet wird, müssen Sie das Script **mqiptService** ausführen. Beispiel:

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

So verhindern Sie, dass MQIPT automatisch gestartet wird:

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

Verwaltungsclient über die Befehlszeile starten

Öffnen Sie ein Befehlseingabefenster, wechseln Sie in das Verzeichnis **bin**, und führen Sie **mqiptGui** aus. Beispiel:

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

Damit der Verwaltungsclient eine Verbindung zu einem MQIPT jenseits einer Firewall herstellen kann, müssen Sie den Hostnamen oder die Adresse und die Port-Nummer angeben:

```
mqiptGui  
<SOCKS-Hostname <SOCKS-Port>>
```

Standardeinstellung für den **SOCKS-Port** ist **1080**.

Der Status des Verwaltungsclients wird anhand von Nachrichten im Hauptfenster des Verwaltungsclients angezeigt.

WebSphere MQ Internet Pass-Thru deinstallieren

Bevor Sie MQIPT auf Ihrem System deinstallieren, müssen Sie es zunächst wie unter „WebSphere Internet Pass-Thru automatisch starten“ auf Seite 53 beschrieben so konfigurieren, dass es nicht mehr automatisch gestartet wird. Melden Sie sich als **root** an, und führen Sie den Befehl `pkgrm` aus:

```
pkgrm mqipt
```

Kapitel 15. Internet Pass-Thru unter AIX installieren

In diesem Kapitel wird die Installation von MQIPT auf einem AIX-System beschrieben:

- „Dateien herunterladen und installieren“
- „WebSphere MQ Internet Pass-Thru einrichten“ auf Seite 56
- „WebSphere MQ Internet Pass-Thru über die Befehlszeile starten“ auf Seite 56
- „WebSphere Internet Pass-Thru automatisch starten“ auf Seite 57
- „Verwaltungsclient über die Befehlszeile starten“ auf Seite 57
- „WebSphere MQ Internet Pass-Thru deinstallieren“ auf Seite 58

Dateien herunterladen und installieren

MQIPT kann von der WebSphere MQ SupportPac-Webseite unter der folgenden Adresse heruntergeladen werden:

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

Laden Sie die Datei entsprechend den Hinweisen herunter.

Melden Sie sich als **root** an, und dekomprimieren und entpacken Sie die Datei **ms81_aix.tar.Z** in einem temporären Verzeichnis. Führen Sie den Befehl `installp` wie im folgenden Beispiel gezeigt aus:

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

In diesem Beispiel wird davon ausgegangen, dass sich die Datei **ms81_aix.tar.Z** im Verzeichnis **/tmp** befindet.

MQIPT enthält die in der folgenden Tabelle aufgeführten Dateien; dazu gehören auch die Dateien des Verwaltungsclients (die grafische Benutzerschnittstelle).

Datei	Funktion
Readme.txt	Enthält die neuesten Informationen, die nicht in den Veröffentlichungen zu finden sind.
mqiptSample.conf	Beispielkonfigurationsdatei
ssl/sslSample.pfx	Schlüsselringdatei zum Testen von SSL-Verbindungen
ssl/sslSample.pwd	Kennwortdatei für die Schlüsselringdatei
ssl/sslCAdefault.pfx	CA-Schlüsselringdatei (Beispieldatei)
ssl/sslCAdefault.pwd	Kennwortdatei für die CA-Schlüsselringdatei
ssl/KeyMan.zip	Dienstprogramm KeyMan
exits/ SampleOneRouteExit.java	Beispielsicherheitsexit
exits/ SampleOneRouteExit.conf	Konfigurationsdatei für SampleOneRouteExit
exits/SampleRoutingExit.java	Beispielsicherheitsexit
exits/SampleRoutingExit.conf	Konfigurationsdatei für SampleRoutingExit

Datei	Funktion
exits/SampleSecurityExit.java	Beispielsicherheitsexit
lib/MQipt.jar	Enthält die Laufzeit-, Klassen- und Eigenschaftsdateien
lib\ADV_mqipt_normal.class	Network Dispatcher-Advisor für "normalen" Modus
lib\ADV_mqipt_replace.class	Network Dispatcher-Advisor für Ersetzungsmodus ("replace")
lib/mqipt1414Sample.ssl	Beispielauslösedatei für den Network Dispatcher-Advisor
bin/mqipt	Direktaufruf für die Aktivierung von MQIPT über die Befehlszeile
bin/mqiptAdmin	Direktaufruf zum Stoppen von MQIPT und zur Aktualisierung von Dateinformationen
bin/mqiptPW	Verschlüsselungskennwort zum Öffnen von Schlüsselringdateien
bin/mqiptVersion	Zum Anzeigen der Versionsnummer von MQIPT
bin/mqiptService	Installiert MQIPT so, dass es bei jedem Systemstart automatisch ebenfalls gestartet wird
bin/mqiptEnv	Gibt den Pfad zur Datei mqipt.jar an; wird nur von den anderen Scripts verwendet
web/MQIPTServlet.war	Webarchivierungsdatei für die Servlet-Version
doc/<Sprache>/html/<Dateiname>.zip	Hauptdatei für das Handbuch <i>WebSphere MQ Internet Pass-Thru</i> im HTML-Format. Weitere Informationen zur Softcopy der Dokumentation finden Sie unter „Literaturverzeichnis“ auf Seite 179.
lib/guiadmin.jar	Enthält Laufzeit-, Klassen- und Eigenschaftsdateien für die grafische Benutzerschnittstelle "Verwaltungsclient"
bin/mqiptGui	Direktaufruf für die Aktivierung des Verwaltungsclients über die Befehlszeile
bin/customSample. Eigenschaften	Beispieldatei für die Anpassung der Darstellung des Verwaltungsclients und damit der Zugriffsmöglichkeiten auf diesen Client

WebSphere MQ Internet Pass-Thru einrichten

Bevor MQIPT zum ersten Mal gestartet wird, müssen Sie die Beispielkonfigurationsdatei **mqiptSample.conf** in die Datei **mqipt.conf** kopieren. Weitere Informationen finden Sie in Kapitel 19, „WebSphere MQ Internet Pass-Thru verwalten und konfigurieren“, auf Seite 71.

WebSphere MQ Internet Pass-Thru über die Befehlszeile starten

Melden Sie sich als **root** an, und wechseln Sie in das Verzeichnis **bin**. Beispiel:

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

Bei Ausführung des Scripts **mqipt** ohne Angabe von Optionen wird eine Standardadresse (".") für die Konfigurationsdatei **mqipt.conf** verwendet. So geben Sie ein anderes Verzeichnis an:

```
mqipt
<Verzeichnisname>
```

An der Konsole werden Nachrichten zum Status von MQIPT angezeigt. Sollte ein Fehler auftreten, lesen Sie unter „Fehlerbestimmung“ auf Seite 153 nach. Im Folgenden ein Beispiel für die Nachrichten, die beim erfolgreichen Start von MQIPT angezeigt werden:

```
| 5639-L92 (C) Copyright IBM Corp. 2000, 2003 Alle Rechte vorbehalten.  
| MQCPI001 WebSphere MQ Internet Pass-Thru Version 1.3.0 wird gestartet.  
| MQCPI004 Die Konfigurationsdaten aus /usr/opt/mqipt/mqipt.conf werden gelesen.  
| MQCPI008 Empfangsbereit für Steuerbefehle an Port 1881.  
| MQCPI011 Die Protokolldateien werden im Pfad /usr/opt/mqipt/logs gespeichert.  
| MQCPI006 Route 1418 wurde gestartet und leitet Nachrichten weiter an :  
| MQCPI034 ....mqserver.company4.com(1414)  
| MQCPI035 ....verwendet MQ-Protokolle  
| MQCPI078 Route 1418 für Verbindungsanforderungen bereit.  
| MQCPI006 Route 1415 wurde gestartet und leitet Nachrichten weiter an :  
| MQCPI034 ....mqipt.company2.com(1415)  
| MQCPI035 ....verwendet MQ-Protokolle  
| MQCPI036 ....SSL-Clientseite mit folgenden Eigenschaften aktiviert :  
| MQCPI031 .....Cipher Suites <null>  
| MQCPI032 .....Schlüsselringdatei /usr/opt/mqipt/KeyMan.pfx  
| MQCPI038 .....registrierte Namen CN=*Doe O=IBM OU=* L=* ST=* C=*  
| MQCPI078 Route 1415 für Verbindungsanforderungen bereit.
```

Wenn MQIPT zum ersten Mal aufgerufen wird, werden automatisch die folgenden Unterverzeichnisse für das Ausgangsverzeichnis **mqipt** erstellt:

- Verzeichnis **log**, in dem das Verbindungsprotokoll gespeichert wird
- Verzeichnis **errors**, in das FFST- (First Failure Support Technology) und Trace-sätze geschrieben werden

WebSphere Internet Pass-Thru automatisch starten

Damit MQIPT beim Systemstart automatisch gestartet wird, müssen Sie das Script **mqiptService** ausführen, um einen Eintrag in **inittab** hinzuzufügen. Beispiel:

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

So verhindern Sie, dass MQIPT automatisch gestartet wird, und entfernen den Eintrag für MQIPT aus **inittab**:

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

Verwaltungsclient über die Befehlszeile starten

Öffnen Sie ein Befehlseingabefenster, wechseln Sie in das Verzeichnis **bin**, und führen Sie **mqiptGui** aus. Beispiel:

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

Damit der Verwaltungsclient eine Verbindung zu einem MQIPT jenseits einer Firewall herstellen kann, müssen Sie den Hostnamen oder die Adresse und die Port-Nummer angeben:

```
mqiptGui <SOCKS-Hostname <SOCKS-Port>>
```

Standardeinstellung für den **SOCKS-Port** ist **1080**.

Der Status des Verwaltungsclients wird anhand von Nachrichten im Hauptfenster des Verwaltungsclients angezeigt.

WebSphere MQ Internet Pass-Thru deinstallieren

Bevor Sie MQIPT auf Ihrem System deinstallieren, müssen Sie es zunächst wie unter „WebSphere Internet Pass-Thru automatisch starten“ auf Seite 57 beschrieben so konfigurieren, dass es nicht mehr automatisch gestartet wird. Melden Sie sich als **root** an, und führen Sie den Befehl `installp` aus:

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

Kapitel 16. WebSphere MQ Internet Pass-Thru unter HP-UX installieren

In diesem Kapitel wird die Installation von MQIPT unter HP-UX beschrieben:

- „Dateien herunterladen und installieren“
- „WebSphere MQ Internet Pass-Thru einrichten“ auf Seite 60
- „WebSphere MQ Internet Pass-Thru über die Befehlszeile starten“ auf Seite 60
- „WebSphere Internet Pass-Thru automatisch starten“ auf Seite 61
- „Verwaltungsclient über die Befehlszeile starten“ auf Seite 62
- „WebSphere MQ Internet Pass-Thru deinstallieren“ auf Seite 62

Dateien herunterladen und installieren

MQIPT kann von der WebSphere MQ SupportPac-Webseite unter der folgenden Adresse heruntergeladen werden:

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

Laden Sie die Datei entsprechend den Hinweisen herunter.

Melden Sie sich als **root** an, und dekomprimieren und entpacken Sie die Datei **ms81_hp11.tar.Z** in einem temporären Verzeichnis. Führen Sie den Befehl **swinstall** wie im folgenden Beispiel gezeigt aus:

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

In diesem Beispiel wird davon ausgegangen, dass sich die Datei **ms81_hp11.tar.Z** im Verzeichnis **/tmp** befindet.

MQIPT enthält die in der folgenden Tabelle aufgeführten Dateien; dazu gehören auch die Dateien des Verwaltungsclients (die grafische Benutzerschnittstelle).

Datei	Funktion
Readme.txt	Enthält die neuesten Informationen, die nicht in den Veröffentlichungen zu finden sind
mqiptSample.conf	Beispielkonfigurationsdatei
ssl/sslSample.pfx	Schlüsselringdatei zum Testen von SSL-Verbindungen
ssl/sslSample.pwd	Kennwortdatei für die Schlüsselringdatei
ssl/sslCAdefault.pfx	CA-Schlüsselringdatei (Beispieldatei)
ssl/sslCAdefault.pwd	Kennwortdatei für die CA-Schlüsselringdatei
ssl/KeyMan.zip	Dienstprogramm KeyMan
exits/ SampleOneRouteExit.java	Beispielsicherheitsexit
exits/ SampleOneRouteExit.conf	Konfigurationsdatei für SampleOneRouteExit
exits/SampleRoutingExit.java	Beispielsicherheitsexit

Datei	Funktion
exits/SampleRoutingExit.conf	Konfigurationsdatei für SampleRoutingExit
exits/SampleSecurityExit.java	Beispielsicherheitsexit
lib/MQipt.jar	Enthält die Laufzeit-, Klassen- und Eigenschaftsdateien
lib\ADV_mqipt_normal.class	Network Dispatcher-Advisor für "normalen" Modus
lib\ADV_mqipt_replace.class	Network Dispatcher-Advisor für Ersetzungsmodus ("replace")
lib/mqipt1414Sample.ssl	Beispielauslösedatei für den Network Dispatcher-Advisor
bin/mqipt	Direktaufruf für die Aktivierung von MQIPT über die Befehlszeile
bin/mqiptAdmin	Direktaufruf zum Stoppen von MQIPT und zur Aktualisierung von Dateiinformatoren
bin/mqiptPW	Verschlüsselungskennwort zum Öffnen von Schlüsselringdateien
bin/mqiptVersion	Zum Anzeigen der Versionsnummer von MQIPT
bin/mqiptService	Installiert MQIPT so, dass es bei jedem Systemstart automatisch ebenfalls gestartet wird
bin/mqiptEnv	Gibt den Pfad zur Datei mqipt.jar an; wird nur von den anderen Scripts verwendet
bin/mqiptFork	Sorgt dafür, dass MQIPT beim Systemstart gestartet wird
web/MQIPTServlet.war	Webarchivierungsdatei für die Servlet-Version
doc/<Sprache>/html/<Dateiname>.zip	Hauptdatei für das Handbuch <i>WebSphere MQ Internet Pass-Thru</i> im HTML-Format. Weitere Informationen zur Softcopy der Dokumentation finden Sie unter „Literaturverzeichnis“ auf Seite 179.
lib/guiadmin.jar	Enthält Laufzeit-, Klassen- und Eigenschaftsdateien für die grafische Benutzerschnittstelle "Verwaltungsclient"
bin/mqiptGui	Direktaufruf für die Ausführung des Verwaltungsclients über die Befehlszeile
bin/customSample. Eigenschaften	Beispieldatei für die Anpassung der Darstellung des Verwaltungsclients und damit der Zugriffsmöglichkeiten auf diesen Client

WebSphere MQ Internet Pass-Thru einrichten

Bevor MQIPT zum ersten Mal gestartet wird, müssen Sie die Beispielkonfigurationsdatei **mqiptSample.conf** in die Datei **mqipt.conf** kopieren. Weitere Informationen finden Sie in Kapitel 19, „WebSphere MQ Internet Pass-Thru verwalten und konfigurieren“, auf Seite 71.

WebSphere MQ Internet Pass-Thru über die Befehlszeile starten

Melden Sie sich als **root** an, und wechseln Sie in das Verzeichnis **bin**. Beispiel:

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

Bei Ausführung des Scripts **mqipt** ohne Angabe von Optionen wird eine Standardadresse (".") für die Konfigurationsdatei **mqipt.conf** verwendet.

So geben Sie ein anderes Verzeichnis an:

```
mqipt  
<Verzeichnisname>
```

An der Konsole werden Nachrichten zum Status von MQIPT angezeigt. Sollte ein Fehler auftreten, lesen Sie unter „Fehlerbestimmung“ auf Seite 153 nach. Im Folgenden ein Beispiel für die Nachrichten, die beim erfolgreichen Start von MQIPT angezeigt werden:

```
| 5639-L92 (C) Copyright IBM Corp. 2000, 2003 Alle Rechte vorbehalten.  
| MQCPI001 WebSphere MQ Internet Pass-Thru Version 1.3.0 wird gestartet.  
| MQCPI004 Die Konfigurationsdaten aus /opt/mqipt/mqipt.conf werden gelesen.  
| MQCPI008 Empfangsbereit für Steuerbefehle an Port 1881.  
| MQCPI011 Die Protokolldateien werden im Pfad /opt/mqipt/logs gespeichert.  
| MQCPI006 Route 1418 wurde gestartet und leitet Nachrichten weiter an :  
| MQCPI034 ....mqserver.company4.com(1414)  
| MQCPI035 ....verwendet MQ-Protokolle  
| MQCPI078 Route 1418 für Verbindungsanforderungen bereit.  
| MQCPI006 Route 1415 wurde gestartet und leitet Nachrichten weiter an :  
| MQCPI034 ....mqipt.company2.com(1415)  
| MQCPI035 ....verwendet MQ-Protokolle  
| MQCPI036 ....SSL-Clientseite mit folgenden Eigenschaften aktiviert :  
| MQCPI031 .....Cipher Suites <null>  
| MQCPI032 .....Schlüsselringdatei /opt/mqipt/KeyMan.pfx  
| MQCPI038 .....registrierte Namen CN=*Doe O=IBM OU=* L=* ST=* C=*  
| MQCPI078 Route 1415 für Verbindungsanforderungen bereit.
```

Wenn MQIPT zum ersten Mal aufgerufen wird, werden automatisch die folgenden Unterverzeichnisse für das Ausgangsverzeichnis **mqipt** erstellt:

- Verzeichnis **log**, in dem das Verbindungsprotokoll gespeichert wird
- Verzeichnis **errors**, in das FFST- (First Failure Support Technology) und Trace-sätze geschrieben werden

WebSphere Internet Pass-Thru automatisch starten

Damit MQIPT beim Systemstart automatisch gestartet wird, müssen Sie das Script **mqiptService** ausführen. Beispiel:

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

Bei diesem Befehl wird davon ausgegangen, dass JDK 1.4 bereits im Verzeichnis **/opt/java1.4** installiert ist. Ist dies nicht der Fall, müssen Sie die Datei **mqipt.ske** entsprechend editieren und die Variable **PATH** so ändern, dass sie auf den Pfad zu JDK zeigt. Diese Änderungen müssen vor Ausführung des Befehls **mqiptService -install** vorgenommen werden.

Wird MQIPT als Dienst gestartet, erstellt es die Datei **console.log** im Unterverzeichnis **logs**. Dieses Unterverzeichnis wird beim erstmaligen Aufruf von MQIPT erstellt, daher muss MQIPT mindestens einmal gestartet werden, bevor es als Dienst gestartet werden kann.

So verhindern Sie, dass MQIPT automatisch gestartet wird:

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

Verwaltungsclient über die Befehlszeile starten

Öffnen Sie ein Befehlseingabefenster, wechseln Sie in das Verzeichnis **bin**, und führen Sie `mqiptGui` aus. Beispiel:

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

Damit der Verwaltungsclient eine Verbindung zu einem MQIPT jenseits einer Firewall herstellen kann, müssen Sie den Hostnamen oder die Adresse und die Portnummer angeben:

```
mqiptGui <SOCKS-Hostname <SOCKS-Port>>
```

Standardeinstellung für den **SOCKS-Port** ist **1080**.

Der Status des Verwaltungsclients wird anhand von Nachrichten im Hauptfenster des Verwaltungsclients angezeigt.

WebSphere MQ Internet Pass-Thru deinstallieren

Bevor Sie MQIPT auf Ihrem System deinstallieren, müssen Sie es zunächst wie unter „WebSphere Internet Pass-Thru automatisch starten“ auf Seite 61 beschrieben so konfigurieren, dass es nicht mehr automatisch gestartet wird. Melden Sie sich als **root** an, und führen Sie den Befehl `swremove` aus:

```
swremove MQIPT
```

Kapitel 17. WebSphere MQ Internet Pass-Thru unter Linux installieren

In diesem Kapitel wird die Installation von MQIPT unter Linux beschrieben:

- „Dateien herunterladen und installieren“
- „WebSphere MQ Internet Pass-Thru einrichten“ auf Seite 64
- „WebSphere MQ Internet Pass-Thru über die Befehlszeile starten“ auf Seite 65
- „WebSphere Internet Pass-Thru automatisch starten“ auf Seite 65
- „Verwaltungsclient über die Befehlszeile starten“ auf Seite 66
- „WebSphere MQ Internet Pass-Thru deinstallieren“ auf Seite 66

Dateien herunterladen und installieren

MQIPT kann von der WebSphere MQ SupportPac-Webseite unter der folgenden Adresse heruntergeladen werden:

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

Laden Sie die Datei entsprechend den Hinweisen herunter.

Melden Sie sich als **root** an, und dekomprimieren und entpacken Sie die Datei **ms81_linux.tar.z** in einem temporären Verzeichnis. Führen Sie den Befehl `rpm` wie im folgenden Beispiel gezeigt aus:

```
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
```

In diesem Beispiel wird davon ausgegangen, dass sich die Datei `ms81_linux.tar.z` im Verzeichnis `/tmp` befindet.

MQIPT enthält die in der folgenden Tabelle aufgeführten Dateien; dazu gehören auch die Dateien des Verwaltungsclients (die grafische Benutzerschnittstelle).

Datei	Funktion
Readme.txt	Enthält die neuesten Informationen, die nicht in den Veröffentlichungen zu finden sind
mqiptSample.conf	Beispielkonfigurationsdatei
ssl/sslSample.pfx	Schlüsselringdatei zum Testen von SSL-Verbindungen
ssl/sslSample.pwd	Kennwortdatei für die Schlüsselringdatei
ssl/sslCAdefault.pfx	CA-Schlüsselringdatei (Beispieldatei)
ssl/sslCAdefault.pwd	Kennwortdatei für die CA-Schlüsselringdatei
ssl/KeyMan.zip	Dienstprogramm KeyMan
exits/ SampleOneRouteExit.java	Beispielsicherheitsexit
exits/ SampleOneRouteExit.conf	Konfigurationsdatei für SampleOneRouteExit

Datei	Funktion
exits/SampleRoutingExit.java	Beispielsicherheitsexit
exits/SampleRoutingExit.conf	Konfigurationsdatei für SampleRoutingExit
exits/SampleSecurityExit.java	Beispielsicherheitsexit
lib/libmqiptqos.so	Pseudobibliothek für TQoS
bin/mqiptQoS	Zur Verwendung der echten TQoS-Bibliothek
lib/MQipt.jar	Enthält die Laufzeit-, Klassen- und Eigenschaftsdateien
lib\ADV_mqipt_normal.class	Network Dispatcher-Advisor für "normalen" Modus
lib\ADV_mqipt_replace.class	Network Dispatcher-Advisor für Ersetzungsmodus ("replace")
lib/mqipt1414Sample.ssl	Beispielauslösedatei für den Network Dispatcher-Advisor
lib/libiptqos.so	Laufzeitbibliothek für QoS-Unterstützung
bin/mqipt	Direktaufruf für die Aktivierung von MQIPT über die Befehlszeile
bin/mqiptAdmin	Direktaufruf zum Stoppen von MQIPT und zur Aktualisierung von Dateiinformatoren
bin/mqiptPW	Verschlüsselungskennwort zum Öffnen von Schlüsselringdateien
bin/mqiptVersion	Zum Anzeigen der Versionsnummer von MQIPT
bin/mqiptService	Installiert MQIPT so, dass es bei jedem Systemstart automatisch ebenfalls gestartet wird
bin/mqiptEnv	Gibt den Pfad zur Datei mqipt.jar an; wird nur von den anderen Scripts verwendet
web/MQIPTServlet.war	Webarchivierungsdatei für die Servlet-Version
doc/<Sprache>/html/<Dateiname>.zip	Hauptdatei für das Handbuch <i>WebSphere MQ Internet Pass-Thru</i> im HTML-Format. Weitere Informationen zur Softcopy der Dokumentation finden Sie unter „Literaturverzeichnis“ auf Seite 179.
lib/guiadmin.jar	Enthält Laufzeit-, Klassen- und Eigenschaftsdateien für die grafische Benutzerschnittstelle "Verwaltungsclient"
bin/mqiptGui	Direktaufruf für die Ausführung des Verwaltungsclients über die Befehlszeile
bin/customSample. Eigenschaften	Beispieldatei für die Anpassung der Darstellung des Verwaltungsclients und damit der Zugriffsmöglichkeiten auf diesen Client

WebSphere MQ Internet Pass-Thru einrichten

Bevor MQIPT zum ersten Mal gestartet wird, müssen Sie die Beispielkonfigurationsdatei **mqiptSample.conf** in die Datei **mqipt.conf** kopieren. Weitere Informationen finden Sie in Kapitel 19, „WebSphere MQ Internet Pass-Thru verwalten und konfigurieren“, auf Seite 71.

WebSphere MQ Internet Pass-Thru über die Befehlszeile starten

Melden Sie sich als **root** an, und wechseln Sie in das Verzeichnis **bin**. Beispiel:

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

Bei Ausführung des Scripts **mqipt** ohne Angabe von Optionen wird eine Standardadresse (".") für die Konfigurationsdatei **mqipt.conf** verwendet. So geben Sie ein anderes Verzeichnis an:

```
mqipt
<Verzeichnisname>
```

An der Konsole werden Nachrichten zum Status von MQIPT angezeigt. Sollte ein Fehler auftreten, lesen Sie unter „Fehlerbestimmung“ auf Seite 153 nach. Im Folgenden ein Beispiel für die Nachrichten, die beim erfolgreichen Start von MQIPT angezeigt werden:

```
| 5639-L92 (C) Copyright IBM Corp. 2000, 2003 Alle Rechte vorbehalten.
| MQCPI001 WebSphere MQ Internet Pass-Thru Version 1.3.0 wird gestartet.
| MQCPI004 Die Konfigurationsdaten aus /opt/mqipt/mqipt.conf werden gelesen.
| MQCPI008 Empfangsbereit für Steuerbefehle an Port 1881.
| MQCPI011 Die Protokolldateien werden im Pfad /opt/mqipt/logs gespeichert.
| MQCPI006 Route 1418 wurde gestartet und leitet Nachrichten weiter an :
| MQCPI034 ....mqserver.company4.com(1414)
| MQCPI035 ....verwendet MQ-Protokolle
| MQCPI078 Route 1418 für Verbindungsanforderungen bereit.
| MQCPI006 Route 1415 wurde gestartet und leitet Nachrichten weiter an :
| MQCPI034 ....mqipt.company2.com(1415)
| MQCPI035 ....verwendet MQ-Protokolle
| MQCPI036 ....SSL-Clientseite mit folgenden Eigenschaften aktiviert :
| MQCPI031 .....Cipher Suites <null>
| MQCPI032 .....Schlüsselringdatei /opt/mqipt/KeyMan.pfx
| MQCPI038 .....registrierte Namen CN=*Doe O=IBM OU=* L=* ST=* C=*
| MQCPI078 Route 1415 für Verbindungsanforderungen bereit.
```

Wenn MQIPT zum ersten Mal aufgerufen wird, werden automatisch die folgenden Unterverzeichnisse für das Ausgangsverzeichnis **mqipt** erstellt:

- Verzeichnis **log**, in dem das Verbindungsprotokoll gespeichert wird
- Verzeichnis **errors**, in das FFST- (First Failure Support Technology) und Trace-sätze geschrieben werden

WebSphere Internet Pass-Thru automatisch starten

Damit MQIPT beim Systemstart automatisch gestartet wird, müssen Sie das Script **mqiptService** ausführen. Beispiel:

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

Wird MQIPT als Dienst gestartet, erstellt es die Datei **console.log** im Unterverzeichnis **logs**. Dieses Unterverzeichnis wird beim erstmaligen Aufruf von MQIPT erstellt, daher muss MQIPT mindestens einmal gestartet werden, bevor es als Dienst gestartet werden kann.

So verhindern Sie, dass MQIPT automatisch gestartet wird:

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

Verwaltungsclient über die Befehlszeile starten

Öffnen Sie ein Befehlseingabefenster, wechseln Sie in das Verzeichnis **bin**, und führen Sie `mqiptGui` aus. Beispiel:

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

Damit der Verwaltungsclient eine Verbindung zu einem MQIPT jenseits einer Firewall herstellen kann, müssen Sie den Hostnamen oder die Adresse und die Portnummer angeben:

```
mqiptGui <SOCKS-Hostname <SOCKS-Port>>
```

Standardeinstellung für den **SOCKS-Port** ist **1080**.

Der Status des Verwaltungsclients wird anhand von Nachrichten im Hauptfenster des Verwaltungsclients angezeigt.

WebSphere MQ Internet Pass-Thru deinstallieren

Bevor Sie MQIPT auf Ihrem System deinstallieren, müssen Sie es zunächst wie unter „WebSphere Internet Pass-Thru automatisch starten“ auf Seite 65 beschrieben so konfigurieren, dass es nicht mehr automatisch gestartet wird. Melden Sie sich als **root** an, und führen Sie den Befehl `swremove` aus:

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

Kapitel 18. Generische UNIX-Installation

Ein Plattenimage aller allgemeinen MQIPT-Dateien wird zur allgemeinen Verwendung in einer TAR-Datei bereitgestellt. Diese Datei macht es möglich, MQIPT auch auf den UNIX-Plattformen zu installieren, die von MQIPT nicht durch eigene Installationsimages unterstützt werden. Dadurch besteht die Möglichkeit, die TAR-Datei in einem spezifischen Verzeichnis und möglicherweise mit geringen Änderungen zu entpacken sowie MQIPT auf allen Plattformen, die Java 1.4 unterstützen, zu implementieren. Gegebenenfalls muss im Script 'mqiptEnv', das sich im Unterverzeichnis 'bin' befindet, das Verzeichnis für die installierten Dateien geändert werden.

- „Dateien herunterladen und installieren“
- „WebSphere MQ Internet Pass-Thru einrichten“ auf Seite 68
- „WebSphere MQ Internet Pass-Thru über die Befehlszeile starten“ auf Seite 69
- „WebSphere Internet Pass-Thru automatisch starten“ auf Seite 70
- „Verwaltungsclient über die Befehlszeile starten“ auf Seite 70
- „WebSphere MQ Internet Pass-Thru deinstallieren“ auf Seite 70

Dateien herunterladen und installieren

MQIPT kann von der WebSphere MQ SupportPac-Webseite unter der folgenden Adresse heruntergeladen werden:

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

Laden Sie die Datei entsprechend den Hinweisen herunter.

Melden Sie sich als 'Root' an, und entpacken Sie die Datei 'ms81.tar' in das Zielverzeichnis, z. B. wie folgt:

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

In diesem Beispiel wird davon ausgegangen, dass die Datei **ms81.tar** in das Verzeichnis **/tmp** heruntergeladen wurde.

MQIPT enthält die in der folgenden Tabelle aufgeführten Dateien; dazu gehören auch die Dateien des Verwaltungsclients (die grafische Benutzerschnittstelle).

Datei	Funktion
Readme.txt	Enthält die neuesten Informationen, die nicht in den Veröffentlichungen zu finden sind
mqiptSample.conf	Beispielkonfigurationsdatei
ssl/sslSample.pfx	Schlüsselringdatei zum Testen von SSL-Verbindungen
ssl/sslSample.pwd	Kennwortdatei für die Schlüsselringdatei
ssl/sslCAdefault.pfx	CA-Schlüsselringdatei (Beispieldatei)
ssl/sslCAdefault.pwd	Kennwortdatei für die CA-Schlüsselringdatei

Datei	Funktion
ssl/KeyMan.zip	Dienstprogramm KeyMan
exits/ SampleOneRouteExit.java	Beispielsicherheitsexit
exits/ SampleOneRouteExit.conf	Konfigurationsdatei für SampleOneRouteExit
exits/SampleRoutingExit.java	Beispielsicherheitsexit
exits/SampleRoutingExit.conf	Konfigurationsdatei für SampleRoutingExit
exits/SampleSecurityExit.java	Beispielsicherheitsexit
lib/MQipt.jar	Enthält die Laufzeit-, Klassen- und Eigenschaftsdateien
lib\ADV_mqipt_normal.class	Network Dispatcher-Advisor für "normalen" Modus
lib\ADV_mqipt_replace.class	Network Dispatcher-Advisor für Ersetzungsmodus ("replace")
lib/mqipt1414Sample.ssl	Beispielauslösedatei für den Network Dispatcher-Advisor
bin/mqipt	Direktaufruf für die Aktivierung von MQIPT über die Befehlszeile
bin/mqiptAdmin	Direktaufruf zum Stoppen von MQIPT und zur Aktualisierung von Dateinformationen
bin/mqiptPW	Verschlüsselungskennwort zum Öffnen von Schlüsselringdateien
bin/mqiptVersion	Zum Anzeigen der Versionsnummer von MQIPT
bin/mqiptService	Installiert MQIPT so, dass es bei jedem Systemstart automatisch ebenfalls gestartet wird
bin/mqiptEnv	Gibt den Pfad zur Datei mqipt.jar an; wird nur von den anderen Scripts verwendet
web/MQIPTServlet.war	Webarchivierungsdatei für die Servlet-Version
doc/<Sprache>/html/ <Dateiname>.zip	Hauptdatei für das Handbuch <i>WebSphere MQ Internet Pass-Thru</i> im HTML-Format. Weitere Informationen zur Softcopy der Dokumentation finden Sie unter „Literaturverzeichnis“ auf Seite 179.
lib/guiadmin.jar	Enthält Laufzeit-, Klassen- und Eigenschaftsdateien für die grafische Benutzerschnittstelle "Verwaltungsclient"
bin/mqiptGui	Direktaufruf für die Aktivierung des Verwaltungsclients über die Befehlszeile
bin/customSample. Eigen- schaften	Beispieldatei für die Anpassung der Darstellung des Verwaltungsclients und damit der Zugriffsmöglichkeiten auf diesen Client

WebSphere MQ Internet Pass-Thru einrichten

Bevor MQIPT zum ersten Mal gestartet wird, müssen Sie die Beispielkonfigurationsdatei **mqiptSample.conf** in die Datei **mqipt.conf** kopieren. Weitere Informationen finden Sie in Kapitel 19, „WebSphere MQ Internet Pass-Thru verwalten und konfigurieren“, auf Seite 71.

In diesem Beispiel wird davon ausgegangen, dass MQIPT in ein Verzeichnis mit dem Namen 'mqipt' installiert wird. Sie müssen das Script 'mqiptEnv' aktualisieren, indem Sie das neue Verzeichnis für die Laufzeitbibliotheken angeben.

Der Standardwert für die Variable MQIPT_CP lautet:
MQIPT_CP=/opt/mqipt/lib/MQipt.jar:/opt/mqipt/lib/guiadmin.jar

In diesem Beispiel muss der Wert wie folgt geändert werden:
MQIPT_CP=/mqipt/opt/mqipt/lib/MQipt.jar:/mqipt/opt/mqipt/lib/guiadmin.jar

Außerdem müssen Sie alle Laufzeitscripts aktualisieren, bevor sie verwendet werden, und den vollständig qualifizierten Pfadnamen für das Verzeichnis des Scripts 'mqiptEnv' ändern. So müssen Sie beispielsweise das mqipt-Script bearbeiten, bevor Sie es verwenden, und die Anweisung nach dem Kommentar Get classpath wie folgt ändern:

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

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

WebSphere MQ Internet Pass-Thru über die Befehlszeile starten

Melden Sie sich als **root** an, und wechseln Sie in das Verzeichnis **bin**. Beispiel:

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

Bei Ausführung des Scripts mqipt ohne Angabe von Optionen wird eine Standardadresse (".") für die Konfigurationsdatei **mqipt.conf** verwendet. So geben Sie ein anderes Verzeichnis an:

```
mqipt  
<Verzeichnisname>
```

An der Konsole werden Nachrichten zum Status von MQIPT angezeigt. Sollte ein Fehler auftreten, lesen Sie unter „Fehlerbestimmung“ auf Seite 153 nach. Im Folgenden ein Beispiel für die Nachrichten, die beim erfolgreichen Start von MQIPT angezeigt werden:

```
5639-L92 (C) Copyright IBM Corp. 2000, 2003 Alle Rechte vorbehalten.  
MQCPI001 WebSphere MQ Internet Pass-Thru Version 1.3.0 wird gestartet.  
MQCPI004 Die Konfigurationsdaten aus /mqipt/opt/mqipt/mqipt.conf werden gelesen.  
MQCPI008 Empfangsbereit für Steuerbefehle an Port 1881.  
MQCPI011 Die Protokolldateien werden im Pfad /mqipt/opt/mqipt/logs gespeichert.  
MQCPI006 Route 1418 wurde gestartet und leitet Nachrichten weiter an :  
MQCPI034 ....mqserver.company4.com(1414)  
MQCPI035 ....verwendet MQ-Protokolle  
MQCPI078 Route 1418 für Verbindungsanforderungen bereit.  
MQCPI006 Route 1415 wurde gestartet und leitet Nachrichten weiter an :  
MQCPI034 ....mqipt.company2.com(1415)  
MQCPI035 ....verwendet MQ-Protokolle  
MQCPI036 ....SSL-Clientseite mit folgenden Eigenschaften aktiviert :  
MQCPI031 .....Cipher Suites <null>  
MQCPI032 .....Schlüsselringdatei /mqipt/opt/mqipt/KeyMan.pfx  
MQCPI038 .....registrierte Namen CN=*Doe O=IBM OU=* L=* ST=* C=*  
MQCPI078 Route 1415 für Verbindungsanforderungen bereit.
```

Wenn MQIPT zum ersten Mal aufgerufen wird, werden automatisch die folgenden Unterverzeichnisse für das Ausgangsverzeichnis **mqipt** erstellt:

- Verzeichnis **log**, in dem das Verbindungsprotokoll gespeichert wird
- Verzeichnis **errors**, in das FFST- (First Failure Support Technology) und Trace-sätze geschrieben werden

WebSphere Internet Pass-Thru automatisch starten

Das automatische Starten eines Service ist ein plattformspezifischer Vorgang. Das Script 'mqiptService' wird lediglich als ein Beispiel dafür, wie dieser Vorgang auf einem Sun Solaris-System abläuft, bereitgestellt. Abhängig von den Systemvoraussetzungen kann es einfacher sein, MQIPT mit Hilfe plattformspezifischer Dienstprogramme als Systemservice zu installieren.

Verwaltungsclient über die Befehlszeile starten

Öffnen Sie ein Befehlseingabefenster, wechseln Sie in das Verzeichnis **bin**, und führen Sie mqiptGui aus. Beispiel:

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

Damit der Verwaltungsclient eine Verbindung zu einem MQIPT jenseits einer Firewall herstellen kann, müssen Sie den Hostnamen oder die Adresse und die Portnummer angeben:

```
mqiptGui
<SOCKS-Hostname <SOCKS-Port>>
```

Standardeinstellung für den **SOCKS-Port** ist **1080**.

Der Status des Verwaltungsclients wird anhand von Nachrichten im Hauptfenster des Verwaltungsclients angezeigt.

WebSphere MQ Internet Pass-Thru deinstallieren

Da MQIPT nicht mit Hilfe eines installierbaren Systemimages installiert wurde, kann es durch Löschen der Verzeichnisstruktur, in der es installiert wurde, deinstalliert werden.

Wenn MQIPT zur Ausführung als Systemservice konfiguriert wurde, müssen Sie den Service entfernen, bevor Sie den Code deinstallieren.

Kapitel 19. WebSphere MQ Internet Pass-Thru verwalten und konfigurieren

Sie können MQIPT konfigurieren, indem Sie Änderungen an der Konfigurationsdatei `mqipt.conf` vornehmen. Es wird empfohlen, hierzu den Verwaltungsclient zu verwenden; Sie können aber auch einen Editor Ihrer Wahl verwenden. Beide Konfigurationsverfahren werden hier beschrieben; die Referenzinformationen gelten für beide Methoden.

- „Verwaltungsclient von WebSphere MQ Internet Pass-Thru verwenden“
- „Zeilenmodusbefehle von WebSphere MQ Internet Pass-Thru verwenden“ auf Seite 75
- „Referenzinformationen zur Konfiguration“ auf Seite 76

Verwaltungsclient von WebSphere MQ Internet Pass-Thru verwenden

Sie können mit Hilfe des Verwaltungsclients einen oder mehrere MQIPTs konfigurieren und aktualisieren. Er zeigt die globalen Eigenschaften eines MQIPTs und die routenspezifischen Eigenschaften an.

Für den Verwaltungsclient ist Java 1.4 keine Voraussetzung.

Bei den einzigen Daten, die lokal im Verwaltungsclient gespeichert werden, handelt es sich um die Liste der MQIPTs; diese wird in der Datei `client.conf` gespeichert. Globale Eigenschaften und Routeneigenschaften werden vom MQIPT abgerufen und dann im Verwaltungsclient angezeigt.

Verwaltungsclient starten

Starten Sie den Verwaltungsclient mit Hilfe des Scripts `mqiptGui`, das sich im MQIPT-Unterverzeichnis `bin` befindet. Hinweise zum Starten des Verwaltungsclients finden Sie in den Kapiteln zur Installation auf den verschiedenen Plattformen.

Wenn der Verwaltungsclient zum ersten Mal gestartet wird, werden Sie in einem Dialogfenster zur Eingabe von Informationen für den Aufbau einer Verbindung zu einem MQIPT aufgefordert. Folgende Angaben sind erforderlich:

MQIPT-Name

Der Name des MQIPTs. Diese Angabe ist zwar nicht zwingend notwendig, es wird jedoch empfohlen, den Namen anzugeben.

Netzadresse

Die Adresse des Systems, auf dem sich der MQIPT befindet; dabei kann es sich entweder um einen Namen (der vom Namensserver erkannt wird), um eine Adresse in Dezimalschreibweise mit Trennzeichen oder um `localhost` (wenn sich der MQIPT auf derselben Maschine wie der Client befindet) handeln.

Befehls-Port

Die Nummer des Ports, den der MQIPT auf Befehle überwacht.

Zeitlimit

Gibt an (in Sekunden), wie lange der Verwaltungsclient auf eine Verbindung zum MQIPT wartet. Dieser Wert sollte so niedrig wie möglich sein, um die Aktualisierungszeit des Fensters so gering wie möglich zu halten.

Zugriffskennwort

Das Kennwort, das bei der Kommunikation mit dem MQIPT verwendet wird. Eine Angabe muss nur erfolgen, wenn die Kennwortüberprüfung aktiv ist. (Die Kennwortüberprüfung ist aktiv, wenn die Eigenschaft **AccessPW** in der MQIPT-Konfigurationsdatei angegeben ist und ihm ein anderer Wert als eine Nullzeichenfolge zugeordnet ist.)

Kennwort speichern

Wird dieses Kontrollkästchen nicht aktiviert, wird das Kennwort nur für die Dauer der Sitzung gespeichert oder bis der MQIPT entfernt wird. Wird das Kontrollkästchen aktiviert, wird das Kennwort für künftige Sitzungen gespeichert.

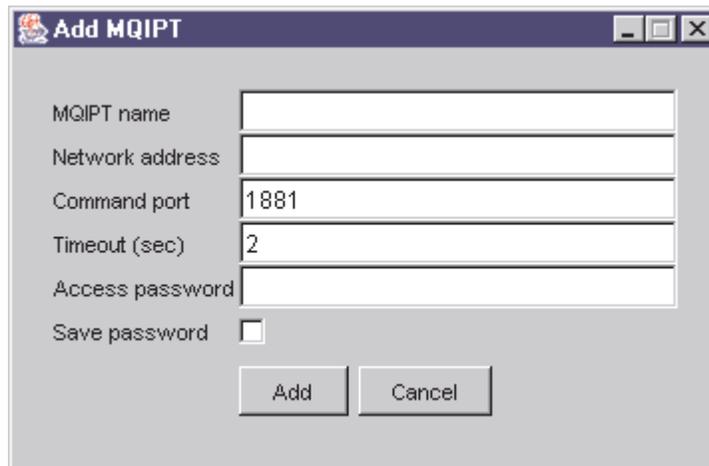


Abbildung 8. Fenster beim erstmaligen Zugriff auf einen MQIPT

MQIPT verwalten

Es kann nur jeweils ein MQIPT aktualisiert werden; wurde also in der Liste ein weiterer MQIPT ausgewählt, müssen zunächst die vorgenommenen Änderungen übernommen werden, bevor Sie fortfahren. Änderungen an Eigenschaften werden für den MQIPT erst wirksam, nachdem Sie auf die Option **Anwenden** geklickt haben.

Bei Auswahl eines MQIPTs in der Liste werden die globalen Eigenschaften und die Routeneigenschaften aus dem MQIPT abgerufen. Ist der MQIPT nicht aktiv oder wurde ein falscher Befehls-Port angegeben, wird eine Fehlermeldung ausgegeben. Änderungen am Hostnamen und am Befehls-Port müssen über die Menüoption **Verbindung** erfolgen.

Bei Doppelklicken auf einen MQIPT in der Liste werden verschiedene Routen angezeigt. Bei Auswahl einer Route werden deren Eigenschaften angezeigt. Sie können diese Eigenschaften entsprechend Ihren Anforderungen ändern.

Bei der Übernahme von Änderungen wird der Konfigurationsdatei eine Zeitmarke hinzugefügt; sie wird dann an den MQIPT zurückgesendet, und die Änderungen werden umgehend wirksam. Alle vorhandenen Kommentarzeilen gehen verloren.

Sie können über die Menüoption **Route hinzufügen** eine Route hinzufügen. Für diese neue Route werden eine Reihe von Standardeigenschaften angezeigt, die durch die globalen Eigenschaften vorgegeben sind.

Vererbung von Eigenschaften

Die Eigenschaften von MQIPs und Routen können im Verwaltungsclient nach bestimmten Kriterien festgelegt werden:

1. Für jede Eigenschaft ist ein Standardwert definiert; wird die Eigenschaft nicht in der Konfigurationsdatei gesetzt oder wurde sie im Verwaltungsclient nicht durch eine bestimmte Benutzeraktion festgelegt, so wird dieser Standardwert verwendet.
2. Die in den MQIPs gesetzten globalen Eigenschaften werden von jeder Route des betreffenden MQIPs übernommen, sofern keine anderen spezifischen Routenangaben definiert wurden. In der Konfigurationsdatei bedeutet dies, dass die in der Zeilengruppe `global` gesetzten Eigenschaften an alle Routen weitergegeben werden, es sei denn, es werden zusätzliche Eigenschaften in den `route`-Zeilengruppen gesetzt. Eigenschaften, die auf einem MQIP von einem Benutzer des Verwaltungsclient definiert wurden, werden an alle Routen weitergegeben, außer für eine Route wird eine Eigenschaft explizit gesetzt.
3. Unabhängig von Standardwerten und globalen Einstellungen werden alle für eine spezifische Route vorgenommenen Einstellungen von dieser Route übernommen.

Optionen im Menü 'Datei'

Ein Großteil der für die Verwaltung der Baumstruktur wichtigen Optionen werden bei Auswahl des Menüs **Datei** angezeigt.

MQIPT hinzufügen

Ruft dasselbe Dialogfenster auf, das auch geöffnet wird, wenn der Client zum ersten Mal verwendet wird (siehe „Verwaltungsclient starten“ auf Seite 71).

MQIPT entfernen

Entfernt den momentan hervorgehobenen MQIPT lediglich aus der Baumstruktur des Verwaltungsclient. Die Auswahl dieser Option wirkt sich nicht auf den Betrieb des MQIPs aus.

Konfiguration speichern

Speichert die MQIPT-Knoten der Baumstruktur in der Konfigurationsdatei des Verwaltungsclients, so dass sie beim nächsten Start des Clients wieder abgerufen werden können. Es werden nur die MQIPT-Knoten gespeichert. Die globalen Eigenschaften und die Routeneigenschaften werden immer aus dem MQIPT abgerufen.

Beenden

Stoppt den Verwaltungsclient. Zuvor überprüft der Verwaltungsclient jedoch, ob Änderungen an der Baumstruktur oder am aktuellen MQIPT vorgenommen wurden; ist eines oder beides der Fall, wird ein Dialogfenster angezeigt, in dem Sie gefragt werden, ob der Client gespeichert werden und/oder ob die Änderungen am MQIPT übernommen werden sollen.

Optionen im Menü 'MQIPT'

Verbindung

Ändert die Zugriffsparameter eines MQIPs. Diese Änderungen werden in der Baumstrukturansicht übernommen. Es wird ein Fenster ähnlich dem unter „Verwaltungsclient starten“ auf Seite 71 beschriebenen angezeigt.

Kennwort

Ändert die Eigenschaft **Kennwort** des fernen MQIPs. Bei Auswahl dieser Option wird ein Kennwortdialogfenster geöffnet, in dem Sie Folgendes eingeben müssen:

- **Aktuelles Kennwort:** Als Schutz gegen unbefugte Zugriffe müssen Sie hier zunächst beweisen, dass Ihnen das aktuelle Kennwort bekannt ist; erst dann können Sie es ändern. Ist momentan kein Kennwort definiert, bleibt dieses Feld leer.
- **Neues Kennwort:** Geben Sie ein neues Kennwort ein, oder lassen Sie das Feld leer, wenn für diesen MQIPT kein Kennwort mehr verwendet werden soll.
- **Neues Kennwort bestätigen:** Durch die Aufforderung, das neue Kennwort noch einmal einzugeben, werden fehlerhafte Angaben im vorherigen Feld (**Neues Kennwort**) verhindert.
- **Kennwort speichern:** Mit dieser Option können Sie festlegen, ob das neue Kennwort zusammen mit den anderen Zugriffseigenschaften des MQIPTs lokal gespeichert werden soll.

Route hinzufügen

Fügt dem ausgewählten MQIPT eine Route hinzu. Informationen hierzu finden Sie unter Abb. 9. Jeder Route muss ein eigener Listener-Port für den MQIPT zugeordnet werden.

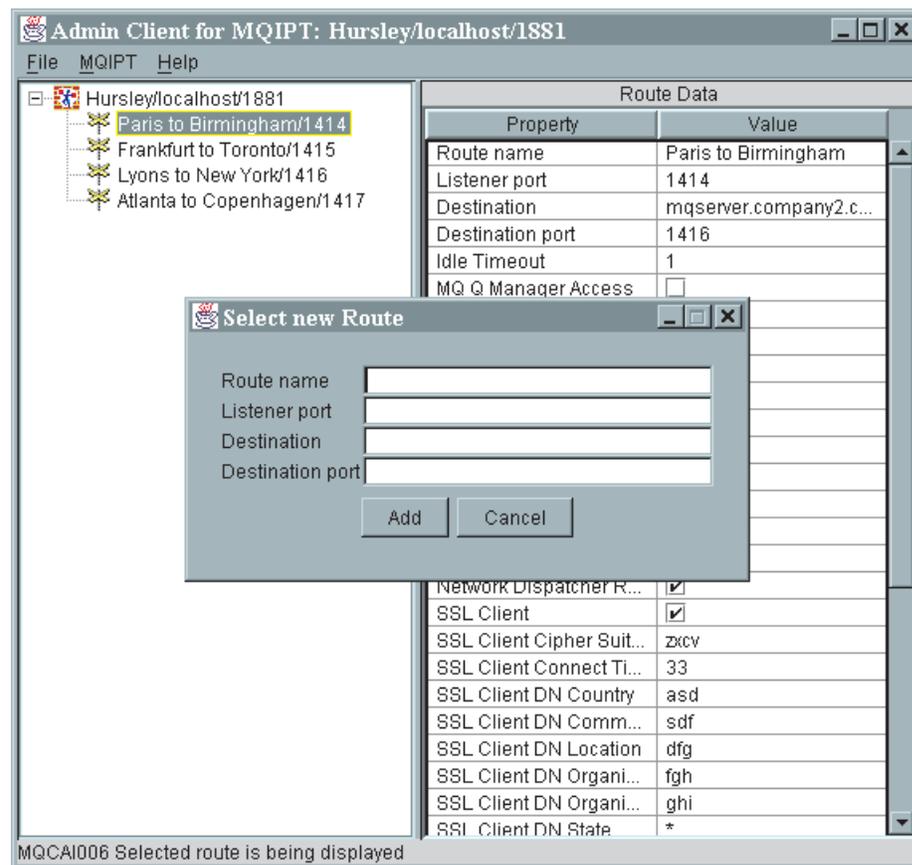


Abbildung 9. Eine Route hinzufügen

Route löschen

Löscht die ausgewählte Route aus dem MQIPT. Der Löschvorgang wird für den MQIPT erst nach Auswahl der Menüoption **Anwenden** wirksam.

Anwenden

Wenn Sie mit den Änderungen an der MQIPT-Konfiguration zufrieden sind,

wird mit dieser Option eine neue Konfigurationsdatei an den MQIPT gesendet, der diese Datei speichert. Die neuen Einstellungen werden umgehend wirksam.

Anzeige aktualisieren

Liest die Konfigurationsdatei aus dem ausgewählten MQIPT und aktualisiert die Anzeige.

Stoppen

Sendet einen Stoppbefehl an den MQIPT, der dessen Betrieb stoppt. Nach Ausführung dieses Befehls wird Ihre Verbindung zum MQIPT unterbrochen. Dieser Befehl hat nur eine Wirkung, wenn die globale Eigenschaft **RemoteShut-Down** (Fernes Beenden) gesetzt wurde.

Routeneigenschaften können auf dieselbe Weise wie globale MQIPT-Eigenschaften aktualisiert werden. Änderungen an den Eigenschaften einer Route werden erst wirksam, nachdem sie übernommen wurden. Wählen Sie dazu entweder im Menü **MQIPT** die Option **Anwenden** aus, oder klicken Sie auf **OK**, wenn Sie gefragt werden, ob die Konfiguration gespeichert werden soll.

Optionen im Menü 'Hilfe'

Hilfe

Zeigt im Netscape-Browser Hinweise zur Verwendung des Verwaltungsclients an; wählen Sie im linken Teilfenster den Eintrag "Administering and configuring internet pass-thru" (WebSphere MQ Internet Pass-Thru verwalten und konfigurieren) aus. Vor der Verwendung des Verwaltungsclients müssen Sie zunächst die Dateien im Unterverzeichnis **<Sprache>/html** entpacken.

Informationen zu

Öffnet ein Produktinfo-Fenster mit Angaben zur Version des Verwaltungsclients.

Zeilenmodusbefehle von WebSphere MQ Internet Pass-Thru verwenden

Wenn Sie den Verwaltungsclient nicht verwenden möchten, können Sie WebSphere MQ Internet Pass-Thru auch über Zeilenmodusbefehle verwalten und konfigurieren.

WebSphere MQ Internet Pass-Thru über Zeilenmodusbefehle verwalten

Mit einem Editor Ihrer Wahl können Sie die Konfigurationsdatei **mqipt.conf** Ihren Wünschen entsprechend ändern. Eine Liste der Eigenschaften, die geändert werden können, finden Sie unter „Referenzinformationen zur Konfiguration“ auf Seite 76.

Wird im Abschnitt **global** der Konfigurationsdatei **mqipt.conf** ein Wert für **CommandPort** angegeben, überwacht MQIPT diesen Port auf die folgenden ASCII-Verwaltungsbefehle:

```
mqiptAdmin -refresh {hostname {port} }      Sendet den Aktualisierungsbefehl
mqiptAdmin -stop {hostname {port} }        Sendet den Stoppbefehl
```

Das Script **mqiptAdmin** befindet sich im Unterverzeichnis **bin**.

Wird es nicht angegeben, wird standardmäßig **localhost** als Hostname und **1881** als Port-Adresse übernommen.

STOP

MQIPT schließt alle Verbindungen, stellt die Überwachung auf ankommende Verbindungen ein und wird beendet. Die Option **Stoppen** im Menü **MQIPT** hat dieselbe Wirkung. Dieser Befehl hat nur eine Wirkung, wenn `RemoteShutDown=true` in der Konfigurationsdatei **mqipt.conf** angegeben wurde.

REFRESH

MQIPT liest die Konfigurationsdatei `mqipt.conf` erneut. Folgendes gilt:

- Stellt MQIPT fest, dass momentan aktive Routen jetzt als 'inaktiv' markiert oder gar nicht mehr vorhanden sind, werden diese Routen geschlossen und nicht mehr auf ankommende Verbindungen überwacht.
- Stellt MQIPT fest, dass Routen, die in der Konfigurationsdatei als 'aktiv' markiert sind, momentan nicht aktiviert sind, werden diese Routen gestartet.
- Stellt MQIPT fest, dass die Konfigurationsparameter von momentan aktiven Routen geändert wurden, so werden die geänderten Einstellungen für diese Routen übernommen. Soweit möglich (z. B. bei Änderungen an den Trace-einstellungen) werden diese Änderungen übernommen, ohne die momentan aktiven Verbindungen zu beeinträchtigen. Bei einigen Parameteränderungen (z. B. bei Änderungen an einer Zieladresse) muss MQIPT vor Übernahme der Änderungen zunächst alle Verbindungen beenden und die Route(n) anschließend erneut starten.

Die Option **Anwenden** im Menü **MQIPT** hat dieselbe Wirkung, vorausgesetzt, vom Verwaltungsklient wurden keine Änderungen an den MQIPT-Einstellungen vorgenommen.

Unter Windows stehen diese Verwaltungsfunktionen auch unter **Programme** im Startmenü zur Verfügung.

Referenzinformationen zur Konfiguration

In MQIPT erfolgt die Definition von Routen und die Steuerung der Aktionen des MQIPT-Servers über eine Konfigurationsdatei mit dem Namen 'mqipt.conf'. Diese Datei besteht aus mehreren Abschnitten. Es gibt einen globalen Abschnitt (`global`) und je einen Abschnitt für jede Route, die über MQIPT definiert wird.

Jeder Abschnitt enthält Eigenschaften, die sich aus Name/Wert-Paaren zusammensetzen. Einige Eigenschaften können nur in den globalen Abschnitten verwendet werden, einige nur in den Routenabschnitten, andere wiederum können in beiden Abschnitten definiert werden. Ist eine Eigenschaft sowohl in einem Routenabschnitt als auch im globalen Abschnitt enthalten, wird dem Wert im Routenabschnitt der Vorzug vor dem Wert im globalen Abschnitt gegeben, jedoch nur für die betreffende Route. Auf diese Weise können über den globalen Abschnitt Standardeinstellungen definiert werden; diese werden für Eigenschaften übernommen, die nicht in den einzelnen Routenabschnitten gesetzt wurden.

Der globale Abschnitt beginnt mit der Zeile `[global]` und endet dort, wo der erste Routenabschnitt beginnt. Der globale Abschnitt muss immer den Routenabschnitten in der Datei vorangestellt werden. Jeder Routenabschnitt beginnt mit der Zeile `[route]`, und endet dort, wo der nächste Routenabschnitt beginnt oder wenn das Ende der Konfigurationsdatei erreicht wird.

Alle unbekanntenen Schlüsselwörter (d. h., alle Name/Wert-Paare, in denen es sich bei dem "Name"-Teil nicht um einen der in diesem Dokument definierten Namen handelt) werden ignoriert. Enthält ein Name/Wert-Paar in einem Routenabschnitt zwar einen definierten Namen, aber einen ungültigen Wert (z. B. `MinConnectionThreads=x` oder `HTTP=unsure`), so wird die betreffende Route deaktiviert, d. h., sie führt keine Überwachung auf ankommende Verbindungen mehr durch. Enthält ein Name/Wert-Paar im globalen Abschnitt einen definierten Namen, aber einen ungültigen Wert, werden alle Routen deaktiviert und MQIPT wird nicht gestartet. Bei Eigenschaften, für die Werte `true` und `false` gesetzt werden, kann eine beliebige Kombination aus Groß- und Kleinbuchstaben verwendet werden.

Die Eigenschaften können entweder durch Bearbeiten der Datei `'mqipt.conf'` oder über die GUI des Verwaltungsclients geändert werden. Zur Durchführung von Änderungen kann der Administrator entweder über die GUI des Verwaltungsclients oder unter Verwendung des Scripts `'mqiptAdmin'` einen Aktualisierungsbefehl ausgeben.

Änderungen bestimmter Eigenschaften führen nur dann dazu, dass eine Route erneut gestartet wird, wenn bereits andere Eigenschaften aktiviert sind. Beispielsweise wirken sich Änderungen der HTTP-Eigenschaften nur dann aus, wenn auch die Eigenschaft `'HTTP'` aktiviert ist.

Beim erneuten Starten einer Route werden vorhandene Verbindungen beendet. Sie können diesen Vorgang außer Kraft setzen, indem Sie die Eigenschaft `'RouteRestart'` auf `'false'` (falsch) festlegen. Dadurch wird verhindert, dass die Route erneut gestartet wird, d. h., vorhandene Verbindungen bleiben aktiv, bis die Eigenschaft `'RouteRestart'` erneut aktiviert wird.

Informationen zum Einrichten einfacher Konfigurationen finden Sie in Kapitel 20, „WebSphere MQ Internet Pass-Thru - Erste Schritte“, auf Seite 97. Eine Beispielkonfiguration finden Sie in der Datei `mqiptSample.conf` im Ausgangsverzeichnis von MQIPT.

Eigenschaften - Übersicht

Tabelle 3 enthält Folgendes:

- Alle Eigenschaften
- Die Angabe, ob eine Eigenschaft im globalen Abschnitt und/oder Routenabschnitt enthalten sein kann
- Die verwendeten Standardwerte, wenn eine Eigenschaft weder im Routenabschnitt noch im globalen Abschnitt angegeben wird

Tabelle 3. Konfigurationseigenschaften - Übersicht

Name	Global	Route	Standardwert
AccessPW	Ja	Nein	<null>
Active	Ja	Ja	true
ClientAccess	Ja	Ja	false
CommandPort	Ja	Nein	<null>
ConnectionLog	Ja	Nein	true
Destination	Nein	Ja	<null>
DestinationPort	Nein	Ja	1414

Tabelle 3. Konfigurationseigenschaften - Übersicht (Forts.)

Name	Global	Route	Standardwert
HTTP ^{6,7}	Ja	Ja	false
HTTPChunking ¹	Ja	Ja	false
HTTPProxy ¹	Ja	Ja	<null>
HTTPProxyPort ¹	Ja	Ja	8080
HTTPS ¹	Ja	Ja	false
HTTPServer ¹	Ja	Ja	<null>
HTTPServerPort ¹	Ja	Ja	<null>
IdleTimeout	Ja	Ja	0
IgnoreExpiredCRLs	Ja	Ja	false
LDAP	Ja	Ja	false
LDAPIgnoreErrors ¹⁰	Ja	Ja	false
LDAPCacheTimeout ¹⁰	Ja	Ja	24
LDAPSaveCRL ¹⁰	Ja	Ja	false
LDAPServer1 ¹⁰	Ja	Ja	<null>
LDAPServer1Port ¹⁰	Ja	Ja	389
LDAPServer1Userid ¹⁰	Ja	Ja	<null>
LDAPServer1Password ¹⁰	Ja	Ja	<null>
LDAPServer1Timeout ¹⁰	Ja	Ja	0
LDAPServer2 ¹⁰	Ja	Ja	<null>
LDAPServer2Port ¹⁰	Ja	Ja	389
LDAPServer2Userid ¹⁰	Ja	Ja	<null>
LDAPServer2Password ¹⁰	Ja	Ja	<null>
LDAPServer2Timeout ¹⁰	Ja	Ja	0
ListenerPort	Nein	Ja	<null>
LocalAddress	Ja	Ja	<null>
LogDir (gilt nur für MQIPTServlet)	Nein	Nein	<null>
MaxConnectionThreads	Ja	Ja	100
MaxLogFileSize	Ja	Nein	50
MinConnectionThreads	Ja	Ja	5
Name	Nein	Ja	<null>
NDAdvisor	Ja	Ja	false
NDAdvisorReplaceMode ⁴	Ja	Ja	false
OutgoingPort	Nein	Ja	0
QMgrAccess	Ja	Ja	true
QoS (nur unter Linux verwendbar)	Ja	Ja	false
QosToCaller ⁹	Ja	Ja	1
QosToDest ⁹	Ja	Ja	1
RemoteShutdown	Ja	Nein	false
RouteRestart	Ja	Ja	true

Tabelle 3. Konfigurationseigenschaften - Übersicht (Forts.)

Name	Global	Route	Standardwert
SecurityExit	Ja	Ja	false
SecurityExitName ¹¹	Ja	Ja	<null>
SecurityExitPath ¹¹	Ja	Ja	<ipthome> \exits
SecurityExitTimeout ¹¹	Ja	Ja	5
SecurityManager	Ja	Nein	false
SecurityManagerPolicy	Ja	Nein	<null>
ServletClient ¹	Ja	Ja	false
SOCKSClient	Ja	Ja	false
SocksProxyHost ⁸	Ja	Ja	<null>
SocksProxyPort ⁸	Ja	Ja	1080
SocksServer ⁷	Ja	Ja	false
SSLClient	Ja	Ja	false
SSLClientCAKeyRing ²	Ja	Ja	<null>
SSLClientCAKeyRingPW ²	Ja	Ja	<null>
SSLClientCipherSuites ²	Ja	Ja	<null>
SSLClientConnectTimeout ²	Ja	Ja	30
SSLClientDN_C ²	Ja	Ja	**" 5
SSLClientDN_CN ²	Ja	Ja	**" 5
SSLClientDN_L ²	Ja	Ja	**" 5
SSLClientDN_O ²	Ja	Ja	**" 5
SSLClientDN_OU ²	Ja	Ja	**" 5
SSLClientDN_ST ²	Ja	Ja	**" 5
SSLClientKeyRing ²	Ja	Ja	<null>
SSLClientKeyRingPW ²	Ja	Ja	<null>
SSLClientSiteDN_C ²	Ja	Ja	**" 5
SSLClientSiteDN_CN ²	Ja	Ja	**" 5
SSLClientSiteDN_L ²	Ja	Ja	**" 5
SSLClientSiteDN_O ²	Ja	Ja	**" 5
SSLClientSiteDN_OU ²	Ja	Ja	**" 5
SSLClientSiteDN_ST ²	Ja	Ja	**" 5
SSLClientSiteLabel ²	Ja	Ja	<null>
SSLProxyMode	Ja	Ja	false
SSLServer ⁶	Ja	Ja	false
SSLServerAskClientAuth ³	Ja	Ja	false
SSLServerCAKeyRing ³	Ja	Ja	<null>
SSLServerCAKeyRingPW ³	Ja	Ja	<null>
SSLServerCipherSuites ³	Ja	Ja	<null>
SSLServerDN_C ³	Ja	Ja	**" 5

Tabelle 3. Konfigurationseigenschaften - Übersicht (Forts.)

Name	Global	Route	Standardwert
SSLServerDN_CN ³	Ja	Ja	"*" 5
SSLServerDN_L ³	Ja	Ja	"*" 5
SSLServerDN_O ³	Ja	Ja	"*" 5
SSLServerDN_OU ³	Ja	Ja	"*" 5
SSLServerDN_ST ³	Ja	Ja	"*" 5
SSLServerKeyRing ³	Ja	Ja	<null>
SSLServerKeyRingPW ³	Ja	Ja	<null>
SSLServerSiteDN_CN ³	Ja	Ja	"*" 5
SSLServerSiteDN_CN ³	Ja	Ja	"*" 5
SSLServerSiteDN_L ³	Ja	Ja	"*" 5
SSLServerSiteDN_O ³	Ja	Ja	"*" 5
SSLServerSiteDN_OU ³	Ja	Ja	"*" 5
SSLServerSiteDN_ST ³	Ja	Ja	"*" 5
SSLServerSiteLabel ³	Ja	Ja	<null>
Trace	Ja	Ja	0
UriName (Standardeinstellungen siehe „UriName“ auf Seite 96) ¹	Ja	Ja	

Anmerkungen:

1. Setzen Sie **HTTP** auf **true**, damit diese Eigenschaften wirksam werden.
2. Setzen Sie **SSLClient** auf **true**, damit diese Eigenschaften wirksam werden.
3. Setzen Sie **SSLServer** auf **true**, damit diese Eigenschaften wirksam werden.
4. Setzen Sie **NDAdvisor** auf **true**, damit diese Eigenschaften wirksam werden.
5. Das Symbol "*" stellt ein Platzhalterzeichen dar.
6. Die Eigenschaften **HTTP** und **SSLServer** können nicht zusammen verwendet werden. Die Eigenschaft **HTTP** wird nur für die Definition der Weiterleitungsverbindung verwendet. Ankommende Daten werden am Listener-Port automatisch erkannt; wird **SSLServer** gesetzt, erfolgt die Ausgabe einer Laufzeitausnahme.
7. Die Eigenschaften **HTTP** und **SOCKSServer** können nicht zusammen verwendet werden. Die Eigenschaft **HTTP** wird nur für die Definition der Weiterleitungsverbindung verwendet. Ankommende Daten werden am Listener-Port automatisch erkannt; wird **SOCKSServer** gesetzt, erfolgt die Ausgabe einer Laufzeitausnahme.
8. Setzen Sie **SOCKSClient** auf **true**, damit diese Eigenschaften wirksam werden.
9. Setzen Sie **QoS** auf **true**, damit diese Eigenschaften wirksam werden.
10. Setzen Sie **LDAP** auf **true**, damit diese Eigenschaften wirksam werden.
11. Setzen Sie **SecurityExit** auf **true**, damit diese Eigenschaften wirksam werden.

Referenzinformationen zum Abschnitt 'global'

Der Abschnitt `global` kann die folgenden Eigenschaften sowie alle unter „Referenzinformationen zum Abschnitt 'route'“ auf Seite 82 aufgeführten Eigenschaften enthalten, mit Ausnahme von **ListenerPort Destination**, **DestinationPort**, **Name** und **OutgoingPort**.

AccessPW (Zugriffskennwort)

Das Kennwort wird verwendet, wenn der Verwaltungscontroller Befehle an den MQIPT sendet. Ist diese Eigenschaft nicht vorhanden oder ist sie auf einen Nullwert gesetzt, erfolgt keine Kennwortprüfung.

CommandPort (Befehls-Port)

Der TCP/IP-Port, auf dem der MQIPT auf Konfigurationsbefehle vom Dienstprogramm **mqiptAdmin** oder vom Verwaltungsclient wartet. Sie können den Befehls-Port über den Verwaltungsclient wie jede andere Eigenschaft ändern. Sie ändern nicht die Verbindungseigenschaften. Wenn Sie die neue Einstellung im MQIPT übernehmen, werden die Verbindungseigenschaften vom Verwaltungsclient automatisch geändert.

Wenn die Eigenschaft **CommandPort** nicht vorhanden ist, erfolgt vom MQIPT keine Überwachung auf Konfigurationsbefehle. Soll der Befehls-Port auf Konfigurationsbefehle überwacht werden, sollten Sie die Port-Adresse **1881** angeben. Der Verwaltungsclient hat keinen Standardwert für den Befehls-Port, aber **1881** ist die Standardeinstellung für die Verwendung von Zeilenmodusbefehlen.

ConnectionLog (Verbindungsprotokoll)

Zulässig sind die Werte **true** oder **false**. Bei Angabe von **true** protokolliert der MQIPT alle Verbindungsversuche (erfolgreiche und erfolglose) im Unterverzeichnis **logs** und alle Verbindungsabbauereignisse in der Datei **mqiptYYYY-MMDDHHmmSS.log**. Standardwert ist **true**. Wird diese Eigenschaft auf **false** gesetzt, schließt MQIPT das bestehende Verbindungsprotokoll und erstellt ein neues Protokoll. Dieses neue Protokoll wird verwendet, wenn die Eigenschaft erneut auf **true** gesetzt wird.

MaxLogFileSize (Maximale Protokolldateigröße)

Die maximale Größe (in KB) der Verbindungsprotokolldatei. Wenn die Größe dieser Datei den angegebenen maximalen Wert überschreitet, wird eine Sicherungskopie (**mqipt.log**) erstellt und eine neue Protokolldatei generiert. Es wird nur jeweils eine Sicherungskopie geführt; wenn die Größe der Hauptprotokolldatei erneut den maximalen Wert überschreitet, wird die vorhandene Sicherungskopie durch eine neue Sicherungskopie überschrieben. Standardwert ist 50, der zulässige Mindestwert 5.

RemoteShutDown (Fernes Beenden)

Zulässig sind die Werte **true** oder **false**. Bei Angabe von **true** (und wenn ein Befehls-Port vorhanden ist), wird der MQIPT abgeschaltet, sobald er einen Stoppbefehl am Befehls-Port empfängt. Standardwert ist **false**.

SecurityManager (Sicherheitsmanager)

Setzen Sie diese Eigenschaft auf **true**, wenn der Java Security Manager für diese MQIPT-Instanz aktiviert werden soll. Dies setzt voraus, dass die richtigen Berechtigungen erteilt werden. Weitere Informationen hierzu finden Sie unter „Java Security Manager“ auf Seite 31. Standardwert dieser Eigenschaft ist **false**.

SecurityManagerPolicy (Richtlinie für Sicherheitsmanager)

Der vollständig qualifizierte Dateiname einer Richtliniendatei. Wird diese Eigenschaft nicht gesetzt, wird nur die Datei mit den globalen Systemrichtlinien und die Datei mit den standardmäßigen Benutzerrichtlinien verwendet. Ist der Java Security Manager bereits aktiviert, werden Änderungen an dieser Eigenschaft erst wirksam, nachdem der Java Security Manager deaktiviert und anschließend erneut aktiviert wurde.

Referenzinformationen zum Abschnitt 'route'

Der Abschnitt `route` kann die folgenden Eigenschaften enthalten:

Active (Aktiv)

Die Route akzeptiert ankommende Verbindungen nur, wenn die Eigenschaft **Active** auf **true** gesetzt ist. Das bedeutet, dass Sie den Zugriff auf ein Ziel vorübergehend beenden können, indem Sie `Active=false` angeben; der Abschnitt `route` muss dazu nicht aus der Konfigurationsdatei gelöscht werden. Wenn Sie diese Eigenschaft auf **false** setzen, wird die Route bei Ausgabe eines Aktualisierungsbefehls (REFRESH) gestoppt. Alle Verbindungen zu dieser Route werden beendet.

ClientAccess (Clientzugriff)

Die Route akzeptiert ankommende Clientkanalverbindungen nur, wenn diese Eigenschaft auf **true** gesetzt ist. Sie haben die Möglichkeit, MQIPs so zu konfigurieren, dass sie entweder nur Clientanforderungen, nur WS-Manageranforderungen oder beide Arten von Anforderungen akzeptieren. Diese Eigenschaft wird in Verbund mit der Eigenschaft **QMgrAccess** verwendet. Wenn Sie diese Eigenschaft auf **false** setzen, wird die Route bei Ausgabe eines Aktualisierungsbefehls (REFRESH) gestoppt und erneut gestartet. Alle Verbindungen zu dieser Route werden beendet.

Destination (Zieladresse)

Der Hostname (oder die IP-Adresse in der Dezimalschreibweise mit Trennzeichen) des WS-Managers (oder des nächsten MQIPs), zu dem diese Route eine Verbindung herstellen soll. In jedem `route`-Abschnitt **muss** ein expliziter Wert für die Zieladresse angegeben sein. Sie können auch mehrere `route`-Abschnitte definieren, die alle auf dieselbe Zieladresse verweisen. Wirkt sich eine Änderung an dieser Eigenschaft auf eine Route aus, wird die Route bei Ausgabe eines Aktualisierungsbefehls (REFRESH) gestoppt und erneut gestartet. Alle Verbindungen zu dieser Route werden beendet.

DestinationPort (Ziel-Port)

Der Port auf dem Zielhost, zu dem die Route eine Verbindung herstellen soll. Mehrere `route`-Abschnitte können auf dieselbe Kombination aus Zieladresse und Ziel-Port verweisen. In jedem `route`-Abschnitt **muss** ein expliziter Wert für einen Ziel-Port angegeben sein. Wirkt sich eine Änderung an dieser Eigenschaft auf eine Route aus, wird die Route bei Ausgabe eines Aktualisierungsbefehls (REFRESH) gestoppt und erneut gestartet. Alle Verbindungen zu dieser Route werden beendet.

HTTP

Für Routen, die für abgehende Anforderungen unter Verwendung von HTTP-Tunnelung (d. h., für die Kommunikation mit anderen MQIPs über HTTP) zuständig sind, muss diese Eigenschaft auf **true** gesetzt werden. Für Routen zu WebSphere MQ-Warteschlangenmanagern muss dieser Wert auf **false** gesetzt werden. Wenn Sie den Wert dieser Eigenschaft ändern, wird die Route bei Ausgabe eines Aktualisierungsbefehls (REFRESH) gestoppt und erneut gestartet. Alle Verbindungen zu dieser Route werden beendet.

Soll HTTP-Chunking verwendet werden, muss diese Eigenschaft auf **true** gesetzt werden. Diese Eigenschaft kann nicht zusammen mit den folgenden Eigenschaften verwendet werden:

- QoS
- SocksClient
- SSLClient
- SSLProxyMode

HTTPChunking (HTTP-Chunking)

Für Routen, die für abgehende Anforderungen unter Verwendung von HTTP-Tunnelung mit Chunking zuständig sind, muss diese Eigenschaft auf **true** gesetzt werden. Die Eigenschaft **HTTP** muss ebenfalls auf **true** gesetzt werden. Wird kein HTTP-Chunking verwendet, muss **false** angegeben werden. Wird diese Eigenschaft geändert (und ist **HTTP** auf **true** gesetzt), wird die Route bei Ausgabe eines Aktualisierungsbefehls (REFRESH) gestoppt und erneut gestartet. Alle Verbindungen zu dieser Route werden beendet.

HTTPProxy (HTTP-Proxy)

Der Hostname (oder die IP-Adresse in der Dezimalschreibweise mit Trennzeichen) des HTTP-Proxy, den alle Verbindungen dieser Route verwenden. Wenn **HTTPServer** ebenfalls definiert ist, wird statt eines normalen POST eine Verbindungsanforderung (CONNECT) an den HTTP-Proxy ausgegeben. Wird diese Eigenschaft geändert (und ist **HTTP** auf **true** gesetzt), wird die Route bei Ausgabe eines Aktualisierungsbefehls (REFRESH) gestoppt und erneut gestartet. Alle Verbindungen zu dieser Route werden beendet.

HTTPProxyPort (HTTP-Proxy-Port)

Die Port-Adresse, die auf dem HTTP-Proxy verwendet wird. Der Standardwert lautet 8080, außer wenn **HTTPS** auf **true** gesetzt wurde und **HTTPServer** nicht angegeben ist (dann lautet der Standardwert 443). Wird diese Eigenschaft geändert (und ist **HTTP** auf **true** gesetzt), wird die Route bei Ausgabe eines Aktualisierungsbefehls (REFRESH) gestoppt und erneut gestartet. Alle Verbindungen zu dieser Route werden beendet.

HTTPServer (HTTP-Server)

Der Hostname (oder die IP-Adresse in der Schreibweise mit Trennzeichen) des HTTP-Servers, den alle Verbindungen dieser Route verwenden. Wird diese Eigenschaft geändert (und ist **HTTP** auf **true** gesetzt), wird die Route bei Ausgabe eines Aktualisierungsbefehls (REFRESH) gestoppt und erneut gestartet. Alle Verbindungen zu dieser Route werden beendet.

HTTPS

Aktivieren Sie diese Eigenschaft, um HTTPS-Anforderungen zu stellen. Die Eigenschaft **HTTP** muss ebenfalls aktiviert werden. Wird diese Eigenschaft geändert (und ist **HTTP** auf **true** gesetzt), wird die Route bei Ausgabe eines Aktualisierungsbefehls (REFRESH) gestoppt und erneut gestartet. Alle Verbindungen zu dieser Route werden beendet.

HTTPServerPort (HTTP-Server-Port)

Die Port-Adresse, die auf dem HTTP-Server verwendet wird. Der Standardwert lautet 8080, außer wenn **HTTPS** auf **true** gesetzt wurde (dann lautet der Standardwert 443). Wird diese Eigenschaft geändert (und ist **HTTP** auf **true** gesetzt), wird die Route bei Ausgabe eines Aktualisierungsbefehls (REFRESH) gestoppt und erneut gestartet. Alle Verbindungen zu dieser Route werden beendet.

IdleTimeout (Zeitlimit für Inaktivität)

Gibt (in Minuten) an, wie lange eine Verbindung inaktiv sein kann, bevor sie beendet wird. Kanäle zwischen WS-Managern verfügen zusätzlich noch über den Parameter `DISCINT`. Beim Setzen von **IdleTimeout** müssen Sie den Parameter `DISCINT` beachten. Bei Angabe von 0 gibt es kein Zeitlimit. Änderungen an dieser Eigenschaft werden erst nach einem Neustart der Route wirksam.

IgnoreExpiredCRLs (Abgelaufene CRLs ignorieren)

Setzen Sie diese Eigenschaft auf **true**, wenn eine abgelaufene CRL ignoriert werden soll. Standardwert ist **false**.

Achtung

Wenn Sie diese Eigenschaft aktivieren, kann ein widerrufenes Zertifikat zur Herstellung einer SSL-Verbindung verwendet werden.

LDAP

Setzen Sie diese Eigenschaft auf **true**, um die Verwendung eines LDAP-Servers über SSL-Verbindungen zu aktivieren. MQIPT verwendet den LDAP-Server zum Abrufen von CRLs und ARLs. Die Eigenschaft **SSLClient** bzw. **SSLServer** muss ebenfalls aktiviert werden, damit diese Eigenschaft wirksam ist.

LDAPIgnoreErrors (LDAP-Fehler ignorieren)

Setzen Sie diese Eigenschaft auf **true**, wenn bei der Ausführung einer LDAP-Suche alle Verbindungs- bzw. Zeitlimitfehler ignoriert werden sollen. Wenn MQIPT keine erfolgreiche Suche ausführen kann, lässt es die Clientverbindung nur zu, wenn diese Eigenschaft aktiviert ist. Eine erfolgreiche Suche bedeutet, dass eine CRL abgerufen wurde oder für die angegebene CA keine CRLs zur Verfügung stehen. Wird diese Eigenschaft geändert (und ist **LDAP** auf **true** gesetzt), wird die Route bei Ausgabe eines Aktualisierungsbefehls (`REFRESH`) gestoppt und erneut gestartet. Alle Verbindungen zu dieser Route werden beendet.

Achtung

Wenn Sie diese Eigenschaft aktivieren, kann ein widerrufenes Zertifikat zur Herstellung einer SSL-Verbindung verwendet werden.

LDAPCacheTimeout (LDAP-Zeitlimit für Cache)

Nachdem eine CRL von einem LDAP-Server abgerufen wurde, wird sie für MQIPT intern in einem temporären Cache gespeichert. Einträge in diesem Cache laufen nach einem bestimmten Zeitlimit, das durch diese Eigenschaft festgelegt wird, ab. Der Standardwert ist 24 (Stunden). Ein Zeitlimit von 0 bedeutet, dass Einträge erst ablaufen, wenn die Route erneut gestartet wird. Wird diese Eigenschaft geändert (und ist **LDAP** auf **true** gesetzt), wird die Route bei Ausgabe eines Aktualisierungsbefehls (`REFRESH`) gestoppt und erneut gestartet. Alle Verbindungen zu dieser Route werden beendet.

LDAPSaveCRL (LDAP-Speicherung von CRLs)

Setzen Sie diese Eigenschaft auf **true**, wenn die angegebene Schlüsselringdatei mit den vom LDAP-Server abgerufenen CRLs aktualisiert werden soll. Schlüsselringdateien werden mit den Eigenschaften **SSLClientKeyRing**, **SSLClientCAKeyRing**, **SSLServerKeyRing** und **SSLServerCAKeyRing** angegeben. Dies setzt voraus, dass MQIPT über Schreibzugriff auf die Schlüsselringdateien verfügt. Wird diese Eigenschaft geändert (und ist **LDAP** auf **true** gesetzt), wird die Route bei Ausgabe eines Aktualisierungsbefehls (`REFRESH`) gestoppt und erneut gestartet. Alle Verbindungen zu dieser Route werden beendet.

LDAPServer1 (LDAP-Server1)

Setzen Sie diese Eigenschaft auf den Hostnamen oder die IP-Adresse des LDAP-Hauptservers. Diese Eigenschaft muss gesetzt werden, wenn **LDAP** aktiviert ist. Wird diese Eigenschaft geändert (und ist **LDAP** auf **true** gesetzt), wird die Route bei Ausgabe eines Aktualisierungsbefehls (REFRESH) gestoppt und erneut gestartet. Alle Verbindungen zu dieser Route werden beendet.

LDAPServer1Port (LDAP-Server1-Port)

Setzen Sie diese Eigenschaft auf die empfangsbereite Port-Adresse des LDAP-Hauptservers. Der Standardwert ist 389. Wird diese Eigenschaft geändert (und ist **LDAP** auf **true** gesetzt), wird die Route bei Ausgabe eines Aktualisierungsbefehls (REFRESH) gestoppt und erneut gestartet. Alle Verbindungen zu dieser Route werden beendet.

LDAPServer1Userid (LDAP-Server1-Benutzer-ID)

Setzen Sie diese Eigenschaft auf die Benutzer-ID für den Zugriff auf den LDAP-Hauptserver. Diese Eigenschaft muss gesetzt werden, wenn eine Berechtigung für den Zugriff auf den LDAP-Hauptserver erforderlich ist. Wird diese Eigenschaft geändert (und ist **LDAP** auf **true** gesetzt), wird die Route bei Ausgabe eines Aktualisierungsbefehls (REFRESH) gestoppt und erneut gestartet. Alle Verbindungen zu dieser Route werden beendet.

LDAPServer1Password (LDAP-Server1-Kennwort)

Setzen Sie diese Eigenschaft auf das Kennwort für den Zugriff auf den LDAP-Hauptserver. Diese Eigenschaft muss gesetzt werden, wenn **LDAPServer1Userid** gesetzt ist. Wird diese Eigenschaft geändert (und ist **LDAP** auf **true** gesetzt), wird die Route bei Ausgabe eines Aktualisierungsbefehls (REFRESH) gestoppt und erneut gestartet. Alle Verbindungen zu dieser Route werden beendet.

LDAPServer1Timeout (LDAP-Server1-Zeitlimit)

Setzen Sie diese Eigenschaft auf die Anzahl Sekunden, die MQIPT auf eine Antwort vom LDAP-Hauptserver wartet. Der Standardwert ist 0, d. h., für die Verbindung gilt kein Zeitlimit. Wird diese Eigenschaft geändert (und ist **LDAP** auf **true** gesetzt), wird die Route bei Ausgabe eines Aktualisierungsbefehls (REFRESH) gestoppt und erneut gestartet. Alle Verbindungen zu dieser Route werden beendet.

LDAPServer2 (LDAP-Server2)

Setzen Sie diese Eigenschaft auf den Hostnamen oder die IP-Adresse des LDAP-Ausweichservers. Diese Eigenschaft ist optional. Wird diese Eigenschaft geändert (und ist **LDAP** auf **true** gesetzt), wird die Route bei Ausgabe eines Aktualisierungsbefehls (REFRESH) gestoppt und erneut gestartet. Alle Verbindungen zu dieser Route werden beendet.

LDAPServer2Port (LDAP-Server2-Port)

Setzen Sie diese Eigenschaft auf die empfangsbereite Port-Adresse des LDAP-Ausweichservers. Der Standardwert ist 389. Wird diese Eigenschaft geändert (und ist **LDAP** auf **true** gesetzt), wird die Route bei Ausgabe eines Aktualisierungsbefehls (REFRESH) gestoppt und erneut gestartet. Alle Verbindungen zu dieser Route werden beendet.

LDAPServer2Userid (LDAP-Server2-Benutzer-ID)

Setzen Sie diese Eigenschaft auf die Benutzer-ID für den Zugriff auf den LDAP-Ausweichserver. Diese Eigenschaft muss gesetzt werden, wenn eine Berechtigung für den Zugriff auf den LDAP-Ausweichserver erforderlich ist. Wird diese Eigenschaft geändert (und ist **LDAP** auf **true** gesetzt), wird die Route bei Ausgabe eines Aktualisierungsbefehls (REFRESH) gestoppt und erneut gestartet. Alle Verbindungen zu dieser Route werden beendet.

LDAPServer2Password (LDAP-Server2-Kennwort)

Setzen Sie diese Eigenschaft auf das Kennwort für den Zugriff auf den LDAP-Ausweichserver. Diese Eigenschaft muss gesetzt werden, wenn **LDAPServer2** aktiviert ist. Wird diese Eigenschaft geändert (und ist **LDAP** auf **true** gesetzt), wird die Route bei Ausgabe eines Aktualisierungsbefehls (REFRESH) gestoppt und erneut gestartet. Alle Verbindungen zu dieser Route werden beendet.

LDAPServer2Timeout (LDAP-Server2-Zeitlimit)

Setzen Sie diese Eigenschaft auf die Anzahl Sekunden, die MQIPT auf eine Antwort vom LDAP-Ausweichserver wartet. Der Standardwert ist 0, d. h., für die Verbindung gilt kein Zeitlimit. Wird diese Eigenschaft geändert (und ist **LDAP** auf **true** gesetzt), wird die Route bei Ausgabe eines Aktualisierungsbefehls (REFRESH) gestoppt und erneut gestartet. Alle Verbindungen zu dieser Route werden beendet.

ListenerPort (Listener-Port)

Die Nummer des Ports, den die Route auf ankommende Anforderungen überwachen soll. In jedem route-Abschnitt **muss** ein expliziter Wert für einen Listener-Port angegeben sein, und jeder Abschnitt muss eine eindeutige Port-Nummer enthalten. Es kann eine beliebige gültige Port-Nummer zwischen 80 und 443 angegeben werden; allerdings dürfen diese Port-Nummern nicht von anderen TCP/IP-Empfangsprogrammen verwendet werden, die auf demselben Host aktiv sind.

LocalAddress (Lokale Adresse)

Die lokale IP-Adresse, an die alle Verbindungen gebunden werden. Wenn Sie den Wert dieser Eigenschaft ändern, wird die Route bei Ausgabe eines Aktualisierungsbefehls (REFRESH) gestoppt und erneut gestartet. Alle Verbindungen zu dieser Route werden beendet.

LogDir (Protokollverzeichnis)

Über diese Eigenschaft wird das Verzeichnis für die Protokoll- und Tracedateien angegeben. Änderungen an dieser Eigenschaft werden erst wirksam, nachdem das MQIPTServlet gestoppt und erneut gestartet wurde. Standardwert ist <null>. Diese Eigenschaft gilt nur für das MQIPTServlet.

MaxConnectionThreads (Max. Anzahl Verbindungs-Threads)

Die maximale Anzahl an Verbindungs-Threads und damit die maximale Anzahl gleichzeitiger Verbindungen, die von dieser Route bearbeitet werden können. Wird dieser Schwellenwert überschritten, gibt **MaxConnectionThreads** auch die Anzahl der Verbindungen an, die in eine Warteschlange eingereiht werden, wenn alle Threads in Benutzung sind. Alle darüber hinaus gehenden Verbindungsanforderungen werden abgelehnt. Die Anzahl der mindestens zulässigen Threads ist größer 1 oder entspricht dem für **MinConnectionThreads** angegebenen Wert. Wirkt sich eine Änderung an dieser Eigenschaft auf eine Route aus, wird bei Ausgabe des Aktualisierungsbefehls (REFRESH) der neue Wert übernommen. Alle Verbindungen übernehmen den neuen Wert sofort. Die Route wird nicht beendet.

MinConnectionThreads (Mindestanzahl Verbindungs-Threads)

Die zulässige Mindestanzahl an Verbindungs-Threads (d. h. Threads für die Bearbeitung ankommender Verbindungen auf dieser Route). Dies ist die Anzahl der Threads, die der Route beim Start zugeordnet werden; solange die Route aktiv ist, sinkt die Gesamtanzahl aller zugeordneten Threads nie unter diesen Wert. Der kleinste zulässige Wert ist 0, der größte zulässige Wert muss unter dem für **MaxConnectionThreads** angegebenen Wert liegen. Änderungen an dieser Eigenschaft werden erst nach einem Neustart der Route wirksam.

Name

Ein optionaler Name zur Kennzeichnung der Route. Dieser Name wird in Konsolnachrichten und Tracedaten verwendet. Änderungen an dieser Eigenschaft werden erst nach einem Neustart der Route wirksam.

NDAvisor (Network Dispatcher Advisor)

Für die vom Network Dispatcher verwalteten Routen muss diese Eigenschaft auf **true** gesetzt werden, damit die Routen auf Anforderungen vom Anpassungs-Advisor reagieren können. Wenn Sie diese Eigenschaft auf **false** setzen, wird die Route bei Ausgabe eines Aktualisierungsbefehls (REFRESH) gestoppt. Alle Verbindungen zu dieser Route werden beendet. Soll die Eigenschaft **NDAvisorReplaceMode** verwendet werden, muss diese Eigenschaft auf **true** gesetzt werden.

NDAvisorReplaceMode (Network Dispatcher-Ersetzungsmodus)

Setzen Sie diese Eigenschaft auf **true**, wenn der Ersetzungsmodus (**replace**) des Anpassungs-Advisors der Komponente Network Dispatcher verwendet werden soll. Dazu muss zunächst der **mqipt_replace custom advisor** für den Listener-Port dieser Route gestartet werden. Setzen Sie diese Eigenschaft auf **false**, wenn der "normale" Modus verwendet werden soll. Die Eigenschaft **NDAvisor** muss auf **true** gesetzt werden, damit diese Eigenschaft verwendet werden kann.

OutgoingPort (Abgehender Port)

Dies ist die Port-Startadresse für abgehende Verbindungen. Der Bereich der Port-Adressen entspricht dem Wert **MaxConnectionThread** für diese Route. Der Standardwert 0 bedeutet, dass eine vom System definierte Port-Adresse verwendet wird. Wenn Sie den Wert dieser Eigenschaft ändern, wird die Route bei Ausgabe eines Aktualisierungsbefehls (REFRESH) gestoppt und erneut gestartet. Alle Verbindungen zu dieser Route werden beendet.

QMgrAccess (WS-Managerzugriff)

Die Route akzeptiert ankommende Kanalverbindungen (z. B. Senderkanäle) von WS-Managern nur, wenn diese Eigenschaft auf **true** gesetzt ist. Wenn Sie diese Eigenschaft auf **false** setzen, wird die Route bei Ausgabe eines Aktualisierungsbefehls (REFRESH) gestoppt. Alle Verbindungen zu dieser Route werden beendet.

QoS (Quality of Service)

Setzen Sie diese Eigenschaft auf **true**, wenn QoS (Servicequalität) für alle Verbindungen dieser Route aktiviert werden soll. Diese Eigenschaft kann nur unter Linux aktiviert werden. Wenn Sie den Wert dieser Eigenschaft ändern, wird die Route bei Ausgabe eines Aktualisierungsbefehls (REFRESH) gestoppt und erneut gestartet. Alle Verbindungen zu dieser Route werden beendet. Diese Eigenschaft kann nicht zusammen mit den folgenden Eigenschaften verwendet werden:

- HTTP
- SSLClient
- SSLProxyMode
- SSLServer

QoSToCaller (QoS an Anrufer)

Diese Eigenschaft legt die Priorität des gesamten Datenverkehrs von der MQIPT-Maschine zum Initiator der Verbindung fest. Beispielsweise legt die Angabe von **1** eine niedrige, von **2** eine mittlere und von **3** eine hohe Priorität fest (Standardwert ist **1**). Wird diese Eigenschaft geändert (und ist **QoS**) auf **true** gesetzt, wird die Route bei Ausgabe eines Aktualisierungsbefehls (REFRESH) gestoppt und erneut gestartet. Alle Verbindungen zu dieser Route werden beendet.

QoSToDest (QoS an Zieladresse)

Diese Eigenschaft legt die Priorität des gesamten Datenverkehrs von der MQIPT-Maschine zu der über die Eigenschaft **Destination** festgelegten Zieladresse der Verbindung fest. Beispielsweise legt die Angabe von **1** eine niedrige, von **2** eine mittlere und von **3** eine hohe Priorität fest (Standardwert ist **1**). Wird diese Eigenschaft geändert (und ist **QoS**) auf **true** gesetzt, wird die Route bei Ausgabe eines Aktualisierungsbefehls (REFRESH) gestoppt und erneut gestartet. Alle Verbindungen zu dieser Route werden beendet.

RouteRestart (Route-Neustart)

Setzen Sie diese Eigenschaft auf **false**, um einen Neustart der Route zu verhindern, wenn andere Routeneigenschaften geändert und ein Aktualisierungsbefehl (REFRESH) ausgegeben wurden. Der Standardwert für diese Eigenschaft ist **true**.

SecurityExit (Sicherheitsexit)

Setzen Sie diese Eigenschaft auf **true**, um einen benutzerdefinierten Sicherheitsexit zu aktivieren. Standardwert dieser Eigenschaft ist **false**.

SecurityExitName (Name des Sicherheitsexits)

Der Klassenname des benutzerdefinierten Sicherheitsexits. Diese Eigenschaft muss gesetzt werden, wenn **SecurityExit** auf **true** gesetzt ist. Wird diese Eigenschaft geändert (und ist **SecurityExit** auf **true** gesetzt), wird die Route bei Ausgabe eines Aktualisierungsbefehls (REFRESH) gestoppt und erneut gestartet. Alle Verbindungen zu dieser Route werden beendet.

SecurityExitPath (Pfad des Sicherheitsexits)

Der vollständig qualifizierte Pfadname für den benutzerdefinierten Sicherheitsexit. Wenn diese Eigenschaft nicht gesetzt wird, wird standardmäßig das Unterverzeichnis **exits** verwendet. Diese Eigenschaft kann auch den Namen einer JAR-Datei, die den benutzerdefinierten Sicherheitsexit enthält, angeben. Wird diese Eigenschaft geändert (und ist **SecurityExit** auf **true** gesetzt), wird die Route bei Ausgabe eines Aktualisierungsbefehls (REFRESH) gestoppt und erneut gestartet. Alle Verbindungen zu dieser Route werden beendet.

SecurityExitTimeout (Zeitlimit des Sicherheitsexits)

Das Zeitlimit gibt an, wie lange (in Sekunden) MQIPT bei der Überprüfung einer Verbindungsanforderung auf eine Antwort wartet. Der Standardwert ist **5** (Sekunden). Wird diese Eigenschaft geändert (und ist **SecurityExit** auf **true** gesetzt), wird die Route bei Ausgabe eines Aktualisierungsbefehls (REFRESH) gestoppt und erneut gestartet. Alle Verbindungen zu dieser Route werden beendet.

ServletClient (Servlet-Client)

Setzen Sie diese Eigenschaft auf **true**, wenn eine Verbindung zu einem MQIPT-Servlet hergestellt werden soll. Die Eigenschaft **HTTP** muss ebenfalls auf **true** gesetzt werden. Wird diese Eigenschaft geändert (und ist **HTTP** auf **true** gesetzt), wird die Route bei Ausgabe eines Aktualisierungsbefehls (REFRESH) gestoppt und erneut gestartet.

SocksClient (SOCKS-Client)

Setzen Sie diese Eigenschaft auf **true**, wenn die Route als SOCKS-Client fungieren und alle Verbindungen über den SOCKS-Proxy über die Eigenschaften **SocksProxyHost** und **SocksProxyPort** definiert werden sollen. Wenn Sie den Wert dieser Eigenschaft ändern, wird die Route bei Ausgabe eines Aktualisierungsbefehls (REFRESH) gestoppt und erneut gestartet. Alle Verbindungen zu dieser Route werden beendet. Diese Eigenschaft kann nicht zusammen mit den folgenden Eigenschaften verwendet werden:

- HTTP
- SocksServer
- SSLClient
- SSLProxyMode

SocksProxyHost (SOCKS-Proxy-Hostname)

Der Hostname (oder die IP-Adresse in der Dezimalschreibweise mit Trennzeichen) des SOCKS-Proxy, den alle Verbindungen dieser Route verwenden. Wird diese Eigenschaft geändert (und ist **SocksClient** auf **true** gesetzt), wird die Route bei Ausgabe eines Aktualisierungsbefehls (REFRESH) gestoppt und erneut gestartet. Alle Verbindungen zu dieser Route werden beendet.

SocksProxyPort (SOCKS-Proxy-Port)

Die Port-Adresse, die auf einem SOCKS-Proxy verwendet wird. Standardwert ist **1080**. Wird diese Eigenschaft geändert (und ist **SocksClient** auf **true** gesetzt), wird die Route bei Ausgabe eines Aktualisierungsbefehls (REFRESH) gestoppt und erneut gestartet. Alle Verbindungen zu dieser Route werden beendet.

SocksServer (SOCKS-Server)

Setzen Sie diese Eigenschaft auf **true**, wenn die Route als SOCKS-Proxy fungieren und SOCKS-Clientanforderungen akzeptieren soll. Wenn Sie den Wert dieser Eigenschaft ändern, wird die Route bei Ausgabe eines Aktualisierungsbefehls (REFRESH) gestoppt und erneut gestartet. Alle Verbindungen zu dieser Route werden beendet. Diese Eigenschaft kann nicht zusammen mit den folgenden Eigenschaften verwendet werden:

- SocksClient
- SSLProxyMode
- SSLServer

SSLClient (SSL-Client)

Setzen Sie diese Eigenschaft auf **true**, wenn diese Route als SSL-Client fungieren und abgehende SSL-Verbindungen herstellen soll. Die Angabe von **true** bedeutet, dass es sich bei dem Ziel entweder um einen anderen MQIPT, der als SSL-Server fungiert, oder einen HTTP-Proxy/-Server handelt. Sie müssen entweder über die Eigenschaft **SSLClientKeyRing** oder die Eigenschaft **SSLClientCAKeyRing** den Namen einer Schlüsselringdatei angeben. Wenn Sie den Wert dieser Eigenschaft ändern, wird die Route bei Ausgabe eines Aktualisierungsbefehls (REFRESH) gestoppt und erneut gestartet. Alle Verbindungen zu dieser Route werden beendet. Diese Eigenschaft kann nicht zusammen mit den folgenden Eigenschaften verwendet werden:

- HTTP
- QoS
- SSLProxyMode

SSLClientCAKeyRing (SSL-Client - CA-Schlüsselring)

Der vollständig qualifizierte Name der Schlüsselringdatei, die die CA-Zertifikate zur Authentifizierung von Zertifikaten vom SSL-Server enthält. Auf Windows-Plattformen muss als Dateitrennzeichen ein doppelter Backslash (\\) verwendet werden. Wird diese Eigenschaft geändert (und ist **SSLClient** auf **true** gesetzt), wird die Route bei Ausgabe eines Aktualisierungsbefehls (REFRESH) gestoppt und erneut gestartet. Alle Verbindungen zu dieser Route werden beendet.

SSLClientCAKeyRingPW (SSL-Client - CA-Schlüsselringkennwort)

Der vollständig qualifizierte Name der Datei, die das zum Öffnen der Client-CA-Schlüsselringdatei erforderliche Kennwort enthält. Auf Windows-Plattformen muss als Dateitrennzeichen ein doppelter Backslash (\\) verwendet werden. Wird diese Eigenschaft geändert (und ist **SSLClient** auf **true** gesetzt), wird die Route bei Ausgabe eines Aktualisierungsbefehls (REFRESH) gestoppt und erneut gestartet. Alle Verbindungen zu dieser Route werden beendet.

SSLClientCipherSuites (SSL-Client - Cipher Suites)

Der Name der SSL-Cipher Suite, die auf der SSL-Clientseite verwendet werden soll. Hier können eine oder mehr unterstützte Cipher Suites angegeben werden. Erfolgt keine Angabe für diese Eigenschaft, verwendet der SSL-Client die unterstützten Cipher Suites aus der SSL-Clientschlüsseldatei. Wird diese Eigenschaft geändert (und ist **SSLClient** auf **true** gesetzt), wird die Route bei Ausgabe eines Aktualisierungsbefehls (REFRESH) gestoppt und erneut gestartet. Alle Verbindungen zu dieser Route werden beendet.

SSLClientConnectTimeout (SSL-Client - Verbindungszeitlimit)

Setzen Sie diese Eigenschaft auf die Anzahl an Sekunden, die der SSL-Client darauf warten soll, dass eine SSL-Verbindung akzeptiert wird. Wird diese Eigenschaft geändert (und ist **SSLClient** auf **true** gesetzt), wird die Route bei Ausgabe eines Aktualisierungsbefehls (REFRESH) gestoppt und erneut gestartet. Alle Verbindungen zu dieser Route werden beendet.

SSLClientDN_C (SSL-Client - DN-Land)

Verwenden Sie diese Eigenschaft, wenn nur die vom SSL-Server gesendeten Zertifikate aus dem angegebenen Land akzeptiert werden sollen. Am Beginn bzw. Ende des Namens kann ein Stern (*) als Platzhalterzeichen verwendet werden, um einen Bereich anzugeben. Erfolgt keine Angabe, wird dies mit der Angabe "alle Ländernamen" gleichgesetzt. Wird diese Eigenschaft geändert (und ist **SSLClient** auf **true** gesetzt), wird die Route bei Ausgabe eines Aktualisierungsbefehls (REFRESH) gestoppt und erneut gestartet. Alle Verbindungen zu dieser Route werden beendet.

SSLClientDN_CN (SSL-Client - allgemeiner DN-Name)

Verwenden Sie diese Eigenschaft, wenn nur die vom SSL-Server gesendeten Zertifikate mit dem angegebenen allgemeinen Namen akzeptiert werden sollen. Am Beginn bzw. Ende des Namens kann ein Stern (*) als Platzhalterzeichen verwendet werden, um einen Bereich anzugeben. Erfolgt keine Angabe, wird dies mit der Angabe "alle Ländernamen" gleichgesetzt. Wird diese Eigenschaft geändert (und ist **SSLClient** auf **true** gesetzt), wird die Route bei Ausgabe eines Aktualisierungsbefehls (REFRESH) gestoppt und erneut gestartet. Alle Verbindungen zu dieser Route werden beendet.

SSLClientDN_L (SSL-Client - DN-Adresse)

Verwenden Sie diese Eigenschaft, wenn nur die vom SSL-Server gesendeten Zertifikate von der angegebenen Adresse akzeptiert werden sollen. Am Beginn bzw. Ende des Namens kann ein Stern (*) als Platzhalterzeichen verwendet werden, um einen Bereich anzugeben. Erfolgt keine Angabe, wird dies mit der Angabe "alle Adressen" gleichgesetzt. Wird diese Eigenschaft geändert (und ist **SSLClient** auf **true** gesetzt), wird die Route bei Ausgabe eines Aktualisierungsbefehls (REFRESH) gestoppt und erneut gestartet. Alle Verbindungen zu dieser Route werden beendet.

SSLClientDN_O (SSL-Client - DN-Organisation)

Verwenden Sie diese Eigenschaft, wenn nur die vom SSL-Server gesendeten Zertifikate von der angegebenen Organisation akzeptiert werden sollen. Am Beginn bzw. Ende des Namens kann ein Stern (*) als Platzhalterzeichen verwendet werden, um einen Bereich anzugeben. Erfolgt keine Angabe, wird dies mit der Angabe "alle Organisationen" gleichgesetzt. Wird diese Eigenschaft geändert (und ist **SSLClient** auf **true** gesetzt), wird die Route bei Ausgabe eines Aktualisierungsbefehls (REFRESH) gestoppt und erneut gestartet. Alle Verbindungen zu dieser Route werden beendet.

SSLClientDN_OU (SSL-Client - DN-Organisationseinheit)

Verwenden Sie diese Eigenschaft, wenn nur die vom SSL-Server gesendeten Zertifikate von der angegebenen Organisationseinheit akzeptiert werden sollen. Am Beginn bzw. Ende des Namens kann ein Stern (*) als Platzhalterzeichen verwendet werden, um einen Bereich anzugeben. Erfolgt keine Angabe, wird dies mit der Angabe "alle Organisationseinheiten" gleichgesetzt. Wird diese Eigenschaft geändert (und ist **SSLClient** auf **true** gesetzt), wird die Route bei Ausgabe eines Aktualisierungsbefehls (REFRESH) gestoppt und erneut gestartet. Alle Verbindungen zu dieser Route werden beendet.

SSLClientDN_ST (SSL-Client - DN-Staat)

Verwenden Sie diese Eigenschaft, wenn nur die vom SSL-Server gesendeten Zertifikate aus dem angegebenen Staat akzeptiert werden sollen. Am Beginn bzw. Ende des Namens kann ein Stern (*) als Platzhalterzeichen verwendet werden, um einen Bereich anzugeben. Erfolgt keine Angabe, wird dies mit der Angabe "alle Staaten" gleichgesetzt. Wird diese Eigenschaft geändert (und ist **SSLClient** auf **true** gesetzt), wird die Route bei Ausgabe eines Aktualisierungsbefehls (REFRESH) gestoppt und erneut gestartet. Alle Verbindungen zu dieser Route werden beendet.

SSLClientKeyRing (SSL-Client - Schlüsselring)

Der vollständig qualifizierte Name der Schlüsselringdatei, die das Clientzertifikat enthält. Auf Windows-Plattformen muss als Dateitrennzeichen ein doppelter Backslash (\\) verwendet werden. Wurde **SSLClient** auf **true** gesetzt, ist für diese Eigenschaft eine Angabe erforderlich. Wird diese Eigenschaft geändert (und ist **SSLClient** auf **true** gesetzt), wird die Route bei Ausgabe eines Aktualisierungsbefehls (REFRESH) gestoppt und erneut gestartet. Alle Verbindungen zu dieser Route werden beendet.

SSLClientKeyRingPW (SSL-Client - Schlüsselringkennwort)

Der vollständig qualifizierte Name der Datei, die das zum Öffnen der Client-Schlüsselringdatei erforderliche Kennwort enthält. Auf Windows-Plattformen muss als Dateitrennzeichen ein doppelter Backslash (\\) verwendet werden. Wurde **SSLClient** auf **true** gesetzt, ist für diese Eigenschaft eine Angabe erforderlich. Wird diese Eigenschaft geändert (und ist **SSLClient** auf **true** gesetzt), wird die Route bei Ausgabe eines Aktualisierungsbefehls (REFRESH) gestoppt und erneut gestartet. Alle Verbindungen zu dieser Route werden beendet.

SSLClientSiteDN_C (SSL-Client-Site - DN-Land)

Geben Sie über diese Eigenschaft einen Ländernamen an, um ein Zertifikat auszuwählen, das an den SSL-Server gesendet werden soll. Erfolgt keine Angabe, wird dies mit der Angabe "beliebiger Ländername" gleichgesetzt. Wird diese Eigenschaft geändert (und ist **SSLClient** auf **true** gesetzt), wird die Route bei Ausgabe eines Aktualisierungsbefehls (REFRESH) gestoppt und erneut gestartet. Alle Verbindungen zu dieser Route werden beendet.

SSLClientSiteDN_CN (SSL-Client-Site - allgemeiner DN-Name)

Geben Sie über diese Eigenschaft einen allgemeinen Namen an, um ein Zertifikat auszuwählen, das an den SSL-Server gesendet werden soll. Erfolgt keine Angabe, wird dies mit der Angabe "beliebiger allgemeiner Name" gleichgesetzt. Wird diese Eigenschaft geändert (und ist **SSLClient** auf **true** gesetzt), wird die Route bei Ausgabe eines Aktualisierungsbefehls (REFRESH) gestoppt und erneut gestartet. Alle Verbindungen zu dieser Route werden beendet.

SSLClientSiteDN_L (SSL-Client-Site - DN-Adresse)

Geben Sie über diese Eigenschaft eine Adresse an, um ein Zertifikat auszuwählen, das an den SSL-Server gesendet werden soll. Erfolgt keine Angabe, wird dies mit der Angabe "beliebige Adresse" gleichgesetzt. Wird diese Eigenschaft geändert (und ist **SSLClient** auf **true** gesetzt), wird die Route bei Ausgabe eines Aktualisierungsbefehls (REFRESH) gestoppt und erneut gestartet. Alle Verbindungen zu dieser Route werden beendet.

SSLClientSiteDN_O (SSL-Client-Site - DN-Organisation)

Geben Sie über diese Eigenschaft einen Organisationsnamen an, um ein Zertifikat auszuwählen, das an den SSL-Server gesendet werden soll. Erfolgt keine Angabe, wird dies mit der Angabe "beliebiger Organisationsname" gleichgesetzt. Wird diese Eigenschaft geändert (und ist **SSLClient** auf **true** gesetzt), wird die Route bei Ausgabe eines Aktualisierungsbefehls (REFRESH) gestoppt und erneut gestartet. Alle Verbindungen zu dieser Route werden beendet.

SSLClientSiteDN_OU (SSL-Client-Site - DN-Organisationseinheit)

Geben Sie über diese Eigenschaft den Namen einer Organisationseinheit an, um ein Zertifikat auszuwählen, das an den SSL-Server gesendet werden soll. Erfolgt keine Angabe, wird dies mit der Angabe "beliebiger Name einer Organisationseinheit" gleichgesetzt. Wird diese Eigenschaft geändert (und ist **SSLClient** auf **true** gesetzt), wird die Route bei Ausgabe eines Aktualisierungsbefehls (REFRESH) gestoppt und erneut gestartet. Alle Verbindungen zu dieser Route werden beendet.

SSLClientSiteDN_ST (SSL-Client-Site - DN-Staat)

Geben Sie über diese Eigenschaft einen Staatennamen an, um ein Zertifikat auszuwählen, das an den SSL-Server gesendet werden soll. Erfolgt keine Angabe, wird dies mit der Angabe "beliebiger Staatename" gleichgesetzt. Wird diese Eigenschaft geändert (und ist **SSLClient** auf **true** gesetzt), wird die Route bei Ausgabe eines Aktualisierungsbefehls (REFRESH) gestoppt und erneut gestartet. Alle Verbindungen zu dieser Route werden beendet.

SSLClientSiteLabel (SSL-Client-Site - Bezeichnung)

Geben Sie über diese Eigenschaft eine Bezeichnung an, um ein Zertifikat auszuwählen, das an den SSL-Server gesendet werden soll. Erfolgt keine Angabe, wird dies mit der Angabe "beliebige Bezeichnung" gleichgesetzt. Wird diese Eigenschaft geändert (und ist **SSLClient** auf **true** gesetzt), wird die Route bei Ausgabe eines Aktualisierungsbefehls (REFRESH) gestoppt und erneut gestartet. Alle Verbindungen zu dieser Route werden beendet.

SSLProxyMode (SSL-Proxy-Modus)

Setzen Sie diese Eigenschaft auf **true**, wenn die Route nur Verbindungsanforderungen von SSL-Clients akzeptieren und Anforderungen im Tunnelungsverfahren direkt an die Zieladresse übertragen soll. Wenn Sie den Wert dieser Eigenschaft ändern, wird die Route bei Ausgabe eines Aktualisierungsbefehls (REFRESH) gestoppt und erneut gestartet. Alle Verbindungen zu dieser Route werden beendet. Diese Eigenschaft kann nicht zusammen mit den folgenden Eigenschaften verwendet werden:

- HTTP
- QoS
- SocksClient
- SSLClient
- SSLServer

SSLServer (SSL-Server)

Setzen Sie diese Eigenschaft auf **true**, wenn diese Route als SSL-Server fungieren und ankommende SSL-Verbindungen akzeptieren soll. Die Angabe von **true** bedeutet, dass es sich bei dem Initiator um einen anderen MQIPT handelt, der als SSL-Client fungiert. Wenn Sie den Wert dieser Eigenschaft ändern, wird die Route bei Ausgabe eines Aktualisierungsbefehls (REFRESH) gestoppt und erneut gestartet. Alle Verbindungen zu dieser Route werden beendet. Diese Eigenschaft kann nicht zusammen mit den folgenden Eigenschaften verwendet werden:

- QoS
- SocksServer
- SSLProxyMode

SSLServerCAKeyRing (SSL-Server - CA-Schlüsselring)

| Der vollständig qualifizierte Name der Schlüsselringdatei, die die CA-Zertifikate zur Authentifizierung von Zertifikaten vom SSL-Client enthält. Auf Windows-Plattformen muss als Dateitrennzeichen ein doppelter Backslash (\\) verwendet werden. Wird diese Eigenschaft geändert (und ist **SSLServer** auf **true** gesetzt), wird die Route bei Ausgabe eines Aktualisierungsbefehls (REFRESH) gestoppt und erneut gestartet. Alle Verbindungen zu dieser Route werden beendet.

SSLServerCAKeyRingPW (SSL-Server - CA-Schlüsselringkennwort)

| Der vollständig qualifizierte Name der Datei, die das zum Öffnen der Server-CA-Schlüsselringdatei erforderliche Kennwort enthält. Auf Windows-Plattformen muss als Dateitrennzeichen ein doppelter Backslash (\\) verwendet werden. Wird diese Eigenschaft geändert (und ist **SSLServer** auf **true** gesetzt), wird die Route bei Ausgabe eines Aktualisierungsbefehls (REFRESH) gestoppt und erneut gestartet. Alle Verbindungen zu dieser Route werden beendet.

SSLServerAskClientAuth (SSL-Server - Clientauthentifizierung anfordern)

| Verwenden Sie diese Eigenschaft, wenn der SSL-Server eine SSL-Clientauthentifizierung anfordern soll. Der SSL-Client muss über ein eigenes Zertifikat verfügen, das an den SSL-Server gesendet wird. Dieses Zertifikat wird aus der Schlüsselringdatei abgerufen. Wird diese Eigenschaft geändert (und ist **SSLServer** auf **true** gesetzt), wird die Route bei Ausgabe eines Aktualisierungsbefehls (REFRESH) gestoppt und erneut gestartet. Alle Verbindungen zu dieser Route werden beendet.

SSLServerCipherSuites (SSL-Server - Cipher Suites)

Der Name der SSL-Cipher Suite, die auf der SSL-Seite verwendet werden soll. Hier können eine oder mehrere unterstützte Cipher Suites angegeben werden. Erfolgt keine Angabe für diese Eigenschaft, verwendet der SSL-Server die unterstützten Cipher Suites aus der SSL-Serverschlüsseldatei. Wird diese Eigenschaft geändert (und ist **SSLServer** auf **true** gesetzt), wird die Route bei Ausgabe eines Aktualisierungsbefehls (REFRESH) gestoppt und erneut gestartet. Alle Verbindungen zu dieser Route werden beendet.

SSLServerDN_C (SSL-Server - DN-Land)

Verwenden Sie diese Eigenschaft, wenn nur die vom SSL-Client gesendeten Zertifikate aus dem angegebenen Land akzeptiert werden sollen. Am Beginn bzw. Ende des Namens kann ein Stern (*) als Platzhalterzeichen verwendet werden, um einen Bereich anzugeben. Erfolgt keine Angabe, wird dies mit der Angabe "alle Länder" gleichgesetzt. Wird diese Eigenschaft geändert (und ist **SSLServer** auf **true** gesetzt), wird die Route bei Ausgabe eines Aktualisierungsbefehls (REFRESH) gestoppt und erneut gestartet. Alle Verbindungen zu dieser Route werden beendet.

SSLServerDN_CN (SSL-Server - allgemeiner DN-Name)

Verwenden Sie diese Eigenschaft, wenn nur die vom SSL-Client gesendeten Zertifikate mit dem angegebenen allgemeinen Namen akzeptiert werden sollen. Am Beginn bzw. Ende des Namens kann ein Stern (*) als Platzhalterzeichen verwendet werden, um einen Bereich anzugeben. Erfolgt keine Angabe, wird dies mit der Angabe "alle allgemeinen Namen" gleichgesetzt. Wird diese Eigenschaft geändert (und ist **SSLServer** auf **true** gesetzt), wird die Route bei Ausgabe eines Aktualisierungsbefehls (REFRESH) gestoppt und erneut gestartet. Alle Verbindungen zu dieser Route werden beendet.

SSLServerDN_L (SSL-Server - DN-Adresse)

Verwenden Sie diese Eigenschaft, wenn nur die vom SSL-Client gesendeten Zertifikate von der angegebenen Adresse akzeptiert werden sollen. Am Beginn bzw. Ende des Namens kann ein Stern (*) als Platzhalterzeichen verwendet werden, um einen Bereich anzugeben. Erfolgt keine Angabe, wird dies mit der Angabe "alle Adressen" gleichgesetzt. Wird diese Eigenschaft geändert (und ist **SSLServer** auf **true** gesetzt), wird die Route bei Ausgabe eines Aktualisierungsbefehls (REFRESH) gestoppt und erneut gestartet. Alle Verbindungen zu dieser Route werden beendet.

SSLServerDN_O (SSL-Server - DN-Organisation)

Verwenden Sie diese Eigenschaft, wenn nur die vom SSL-Client gesendeten Zertifikate von der angegebenen Organisation akzeptiert werden sollen. Am Beginn bzw. Ende des Namens kann ein Stern (*) als Platzhalterzeichen verwendet werden, um einen Bereich anzugeben. Erfolgt keine Angabe, wird dies mit der Angabe "alle Organisationen" gleichgesetzt. Wird diese Eigenschaft geändert (und ist **SSLServer** auf **true** gesetzt), wird die Route bei Ausgabe eines Aktualisierungsbefehls (REFRESH) gestoppt und erneut gestartet. Alle Verbindungen zu dieser Route werden beendet.

SSLServerDN_OU (SSL-Server - DN-Organisationseinheit)

Verwenden Sie diese Eigenschaft, wenn nur die vom SSL-Client gesendeten Zertifikate von der angegebenen Organisationseinheit akzeptiert werden sollen. Am Beginn bzw. Ende des Namens kann ein Stern (*) als Platzhalterzeichen verwendet werden, um einen Bereich anzugeben. Erfolgt keine Angabe, wird dies mit der Angabe "alle Organisationseinheiten" gleichgesetzt. Wird diese Eigenschaft geändert (und ist **SSLServer** auf **true** gesetzt), wird die Route bei Ausgabe eines Aktualisierungsbefehls (REFRESH) gestoppt und erneut gestartet. Alle Verbindungen zu dieser Route werden beendet.

SSLServerDN_ST (SSL-Server - DN-Staat)

Verwenden Sie diese Eigenschaft, wenn nur die vom SSL-Client gesendeten Zertifikate aus dem angegebenen Staat akzeptiert werden sollen. Am Beginn bzw. Ende des Namens kann ein Stern (*) als Platzhalterzeichen verwendet werden, um einen Bereich anzugeben. Erfolgt keine Angabe, wird dies mit der Angabe "alle Staaten" gleichgesetzt. Wird diese Eigenschaft geändert (und ist **SSLServer** auf **true** gesetzt), wird die Route bei Ausgabe eines Aktualisierungsbefehls (REFRESH) gestoppt und erneut gestartet. Alle Verbindungen zu dieser Route werden beendet.

SSLServerKeyRing (SSL-Server - Schlüsselring)

Der vollständig qualifizierte Name der Schlüsselringdatei, die das Serverzertifikat enthält. Auf Windows-Plattformen muss als Dateitrennzeichen ein doppelter Backslash (\\) verwendet werden. Wurde **SSLServer** auf **true** gesetzt, ist für diese Eigenschaft eine Angabe erforderlich. Wird diese Eigenschaft geändert (und ist **SSLServer** auf **true** gesetzt), wird die Route bei Ausgabe eines Aktualisierungsbefehls (REFRESH) gestoppt und erneut gestartet. Alle Verbindungen zu dieser Route werden beendet.

SSLServerKeyRingPW (SSL-Server - Schlüsselringkennwort)

Der vollständig qualifizierte Name der Datei, die das zum Öffnen der Server-Schlüsselringdatei erforderliche Kennwort enthält. Auf Windows-Plattformen muss als Dateitrennzeichen ein doppelter Backslash (\\) verwendet werden. Wurde **SSLServer** auf **true** gesetzt, ist für diese Eigenschaft eine Angabe erforderlich. Wird diese Eigenschaft geändert (und ist **SSLServer** auf **true** gesetzt), wird die Route bei Ausgabe eines Aktualisierungsbefehls (REFRESH) gestoppt und erneut gestartet. Alle Verbindungen zu dieser Route werden beendet.

SSLServerSiteDN_C (SSL-Server-Site - DN-Land)

Geben Sie über diese Eigenschaft einen Ländernamen an, um ein Zertifikat auszuwählen, das an den SSL-Client gesendet werden soll. Erfolgt keine Angabe, wird dies mit der Angabe "beliebiger Ländername" gleichgesetzt. Wird diese Eigenschaft geändert (und ist **SSLServer** auf **true** gesetzt), wird die Route bei Ausgabe eines Aktualisierungsbefehls (REFRESH) gestoppt und erneut gestartet. Alle Verbindungen zu dieser Route werden beendet.

SSLServerSiteDN_CN (SSL-Server-Site - allgemeiner DN-Name)

Geben Sie über diese Eigenschaft einen allgemeinen Namen an, um ein Zertifikat auszuwählen, das an den SSL-Client gesendet werden soll. Erfolgt keine Angabe, wird dies mit der Angabe "beliebiger allgemeiner Name" gleichgesetzt. Wird diese Eigenschaft geändert (und ist **SSLServer** auf **true** gesetzt), wird die Route bei Ausgabe eines Aktualisierungsbefehls (REFRESH) gestoppt und erneut gestartet. Alle Verbindungen zu dieser Route werden beendet.

SSLServerSiteDN_L (SSL-Server-Site - DN-Adresse)

Geben Sie über diese Eigenschaft eine Adresse an, um ein Zertifikat auszuwählen, das an den SSL-Client gesendet werden soll. Erfolgt keine Angabe, wird dies mit der Angabe "beliebige Adresse" gleichgesetzt. Wird diese Eigenschaft geändert (und ist **SSLServer** auf **true** gesetzt), wird die Route bei Ausgabe eines Aktualisierungsbefehls (REFRESH) gestoppt und erneut gestartet. Alle Verbindungen zu dieser Route werden beendet.

SSLServerSiteDN_O (SSL-Server-Site - DN-Organisation)

Geben Sie über diese Eigenschaft einen Organisationsnamen an, um ein Zertifikat auszuwählen, das an den SSL-Client gesendet werden soll. Erfolgt keine Angabe, wird dies mit der Angabe "beliebiger Organisationsname" gleichgesetzt. Wird diese Eigenschaft geändert (und ist **SSLServer** auf **true** gesetzt), wird die Route bei Ausgabe eines Aktualisierungsbefehls (REFRESH) gestoppt und erneut gestartet. Alle Verbindungen zu dieser Route werden beendet.

SSLServerSiteDN_OU (SSL-Server-Site - DN-Organisationseinheit)

Geben Sie über diese Eigenschaft den Namen einer Organisationseinheit an, um ein Zertifikat auszuwählen, das an den SSL-Client gesendet werden soll. Erfolgt keine Angabe, wird dies mit der Angabe "beliebiger Name einer Organisationseinheit" gleichgesetzt. Wird diese Eigenschaft geändert (und ist **SSLServer** auf **true** gesetzt), wird die Route bei Ausgabe eines Aktualisierungsbefehls (REFRESH) gestoppt und erneut gestartet. Alle Verbindungen zu dieser Route werden beendet.

SSLServerSiteDN_ST (SSL-Server-Site - DN-Staat)

Geben Sie über diese Eigenschaft einen Staatennamen an, um ein Zertifikat auszuwählen, das an den SSL-Client gesendet werden soll. Erfolgt keine Angabe, wird dies mit der Angabe "beliebiger Staatename" gleichgesetzt. Wird diese Eigenschaft geändert (und ist **SSLServer** auf **true** gesetzt), wird die Route bei Ausgabe eines Aktualisierungsbefehls (REFRESH) gestoppt und erneut gestartet. Alle Verbindungen zu dieser Route werden beendet.

SSLServerSiteLabel (SSL-Server-Site - Bezeichnung)

Geben Sie über diese Eigenschaft eine Bezeichnung an, um ein Zertifikat auszuwählen, das an den SSL-Client gesendet werden soll. Erfolgt keine Angabe, wird dies mit der Angabe "beliebige Bezeichnung" gleichgesetzt. Wird diese Eigenschaft geändert (und ist **SSLServer** auf **true** gesetzt), wird die Route bei Ausgabe eines Aktualisierungsbefehls (REFRESH) gestoppt und erneut gestartet. Alle Verbindungen zu dieser Route werden beendet.

Trace

Die gewünschte Tracestufe kann über eine ganze Zahl von 0 bis 5 angegeben werden. Bei Angabe von 0 erfolgt kein Trace, bei Angabe von 5 wird ein umfassender Trace durchgeführt.

Wirkt sich eine Änderung an dieser Eigenschaft auf eine Route aus, wird bei Ausgabe des Aktualisierungsbefehls (REFRESH) der neue Wert übernommen. Alle Verbindungen übernehmen den neuen Wert sofort. Die Route wird nicht beendet.

UriName (URI-Name)

Über diese Eigenschaft können Sie den Namen der URI (Uniform Resource Identifier) der Ressource ändern, wenn ein HTTP-Proxy oder das MQIPT-Servlet verwendet wird; für die meisten Konfigurationen sind allerdings die Standardeinstellungen ausreichend. Für den HTTP-Proxy gelten die folgenden Standardeinstellungen:

```
HTTP://<Zieladresse>:<Ziel-Port>/mqipt
```

Für das MQIPT-Servlet gelten die folgenden Standardeinstellungen:

```
HTTP://<Zieladresse>:<Ziel-Port>/MQIPTServlet
```

Wird diese Eigenschaft geändert (und ist die Eigenschaft **HTTP** oder **Servlet Client** auf **true** gesetzt), wird die Route bei Ausgabe eines Aktualisierungsbefehls (REFRESH) gestoppt und erneut gestartet.

Kapitel 20. WebSphere MQ Internet Pass-Thru - Erste Schritte

Dieses Kapitel enthält Hinweise zur Verwendung von MQIPT; es zeigt, wie Sie einige einfache Konfigurationen erstellen, anhand derer Sie feststellen können, ob das Produkt erfolgreich installiert wurde.

Dieses Kapitel enthält die folgenden Abschnitte:

- „Voraussetzungen“
- „Beispielkonfigurationen“ auf Seite 98
- „Installationsfunktionstest“ auf Seite 99
- „SSL-Serverauthentifizierung“ auf Seite 100
- „SSL-Clientauthentifizierung“ auf Seite 102
- „HTTP-Proxy-Konfiguration“ auf Seite 105
- „Zugriffssteuerung konfigurieren“ auf Seite 107
- „Quality of Service (QoS) konfigurieren“ auf Seite 110
- „SOCKS-Proxy konfigurieren“ auf Seite 113
- „SOCKS-Client konfigurieren“ auf Seite 116
- „SSL-Testzertifikate erstellen“ auf Seite 118
- „MQIPT-Servlet konfigurieren“ auf Seite 119
- „HTTPS-Konfiguration“ auf Seite 122
- „Unterstützung für MQIPT-Clustering konfigurieren“ auf Seite 126
- „Eine Schlüsselringdatei erstellen“ auf Seite 130
- „Port-Adressen zuordnen“ auf Seite 132
- „LDAP-Server verwenden“ auf Seite 134
- „SSL-Proxy-Modus“ auf Seite 137
- „Apache-Anweisung 'rewrite'“ auf Seite 140
- „Sicherheitsexit“ auf Seite 143
- „Sicherheitsexit weiterleiten“ auf Seite 145
- „Dynamischer Exit bei nur einer Route“ auf Seite 149

Voraussetzungen

Bei den Beispielen wird von Folgendem ausgegangen:

- Sie verwenden Windows NT (diese Beispielkonfigurationen sind jedoch auf allen unterstützten Plattformen möglich).
- Sie sind mit der Definition von WS-Managern, Warteschlangen und Kanälen in WebSphere MQ vertraut.
- Sie haben einen WebSphere MQ-Client und einen WebSphere MQ-Server installiert.
- MQIPT ist im Verzeichnis C:\mqipt (unter Windows) installiert.
- Der Client, der Server und die einzelnen MQIPs sind jeweils auf eigenen Maschinen installiert.
- Sie sind mit dem Einreihen von Nachrichten in Warteschlangen unter Verwendung des Befehls `amqputc` vertraut.

- Sie sind mit dem Abrufen von Nachrichten aus Warteschlangen unter Verwendung des Befehls `amqsgetc` vertraut.

Auf dem WebSphere MQ-Server wurde bereits Folgendes vorgenommen:

- Sie haben einen WS-Manager namens **MQIPT.QM1** installiert.
- Sie haben einen Serververbindungskanal namens **MQIPT.CONN.CHANNEL** definiert.
- Sie haben eine lokale Warteschlange namens **MQIPT.LOCAL.QUEUE** definiert.
- Sie haben an Port 1414 ein TCP/IP-Empfangsprogramm für **MQIPT.QM1** gestartet.

Nur jeweils eine Anwendung kann an einer gegebenen Port-Adresse auf einer Maschine empfangsbereit sein. Wenn Port 1414 bereits anderweitig zugeordnet ist, müssen Sie einen freien Port wählen und diesen in den folgenden Beispielen verwenden.

Nachdem Sie die oben beschriebenen Schritte ausgeführt haben, können Sie die Route vom WebSphere MQ-Client zum WS-Manager testen, indem Sie mit dem Befehl `amqsputc` eine Nachricht in die lokale Warteschlange des WS-Managers einreihen und mit dem Befehl `amqsgetc` wieder abrufen.

Beispielkonfigurationen

Die folgenden Beispielkonfigurationen werden anhand von Diagrammen und schrittweisen Anleitungen erläutert; in den Kästchen rechts neben den einzelnen Diagrammen können Sie die jeweils abgeschlossenen Schritte abhaken und so den Ablauf der Konfiguration verfolgen. In einigen der Beispiele müssen Sie Änderungen an der Konfigurationsdatei `mqipt.conf` vornehmen; diese Datei befindet sich im Ausgangsverzeichnis von MQIPT.

Bevor Sie beginnen, sollten Sie sicherstellen, dass Folgendes ausgeführt wurde:

- Die Datei **mqiptSample.conf** wurde in die Datei **mqipt.conf** kopiert.
- Es wurden alle `route`-Abschnitte aus der Datei **mqipt.conf** gelöscht.
- Der Wert für die Eigenschaft **ClientAccess** wurde auf **true** gesetzt.
- Der Wert für **Destination** wurde von **mqserver.company2.com** in die Adresse Ihres WS-Managers geändert.
- Für **DestinationPort** wurde die von Ihrem WS-Manager verwendete Port-Adresse angegeben.
- Sie haben den Abschnitt „Voraussetzungen“ auf Seite 97 gelesen.

Installationsfunktionstest

Dies ist eine einfache Konfiguration, mit deren Hilfe überprüft werden kann, ob MQIPT richtig installiert wurde.

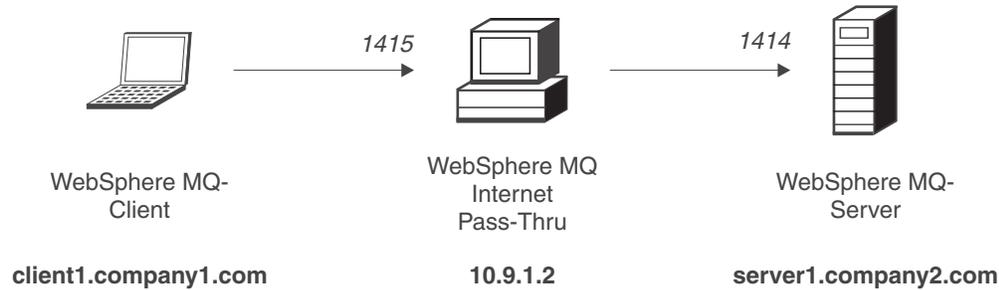


Abbildung 10. IVT-Netzplan

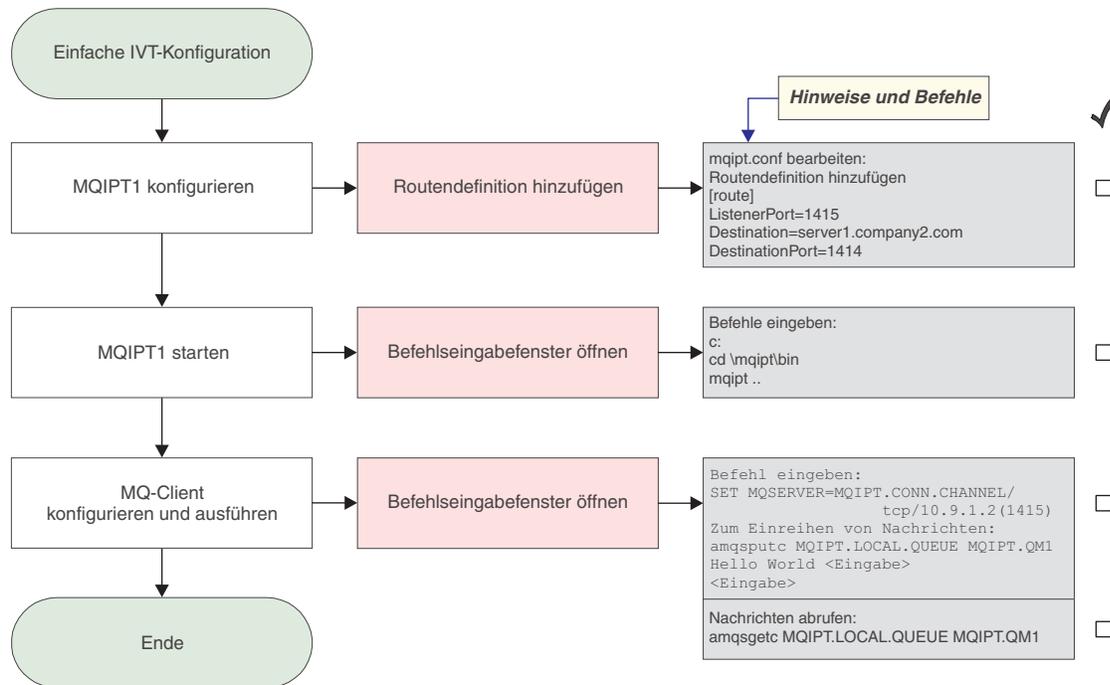


Abbildung 11. IVT-Konfiguration

1. Konfigurieren Sie MQIPT1.

Ändern Sie die Datei **mqipt.conf**, indem Sie eine Routendefinition hinzufügen:

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

2. Starten Sie MQIPT1.

Öffnen Sie ein Befehlseingabefenster, und geben Sie Folgendes ein:

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

Die folgenden Nachrichten weisen auf eine erfolgreiche Ausführung hin:

```
5639-L92 (C) Copyright IBM Corp. 2000, 2003 Alle Rechte vorbehalten.  
MQCPI001 WebSphere MQ Internet Pass-Thru Version 1.3.0 wird gestartet.  
MQCPI004 Die Konfigurationsdaten aus C:\mqipt\mqipt.conf werden gelesen.  
MQCPI011 Die Protokolldateien werden im Pfad C:\mqipt\logs gespeichert.  
MQCPI006 Route 1415 wurde gestartet und leitet Nachrichten weiter an :  
MQCPI034 ....server1.company2.com(1414)  
MQCPI035 ....verwendet MQ-Protokolle  
MQCPI078 Route 1415 für Verbindungsanforderungen bereit.
```

3. Geben Sie an einer Eingabeaufforderung auf der WebSphere MQ-Clientmaschine Folgendes ein:

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

4. Reihen Sie eine Nachricht wie folgt ein:

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

5. Rufen Sie die Nachricht wie folgt ab:

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

Es wird "Hello world" angezeigt.

SSL-Serverauthentifizierung

In diesem Beispiel wird eine SSL-Verbindung mit Hilfe eines Beispieldtestzertifikats (Schlüsselringdatei **sslsample.pfx**) getestet, indem ein WebSphere MQ-Client über zwei MQIPTs mit einem WebSphere MQ-Server verbunden wird. Während des SSL-Handshake sendet der Server sein Testzertifikat an den Client. Der Client wird den Server anhand seines eigenen Zertifikats (in dem "Vertrauen auf Peer-Ebene" gesetzt ist) authentifizieren. Es wird eine standardmäßige Cipher Suite namens **SSL_RSA_WITH_RC4_128_MD5** verwendet.

(Basiert auf der unter „Installationsfunktionstest“ auf Seite 99 erstellten Datei **mqipt.conf**). Hinweise zur Erstellung eines Testzertifikats für diese Beispieldkonfiguration finden Sie unter „SSL-Testzertifikate erstellen“ auf Seite 118.

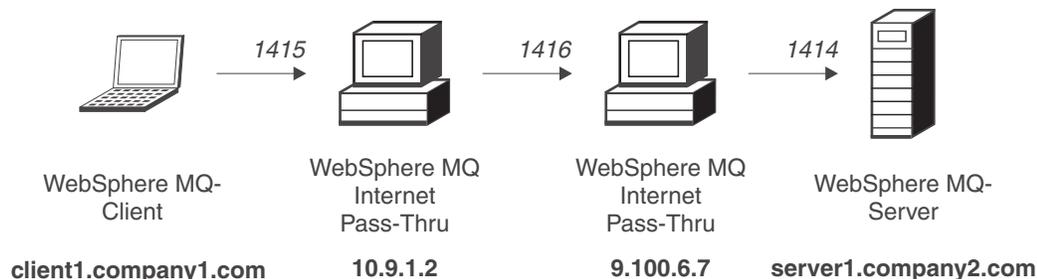


Abbildung 12. SSL-Servernetzplan

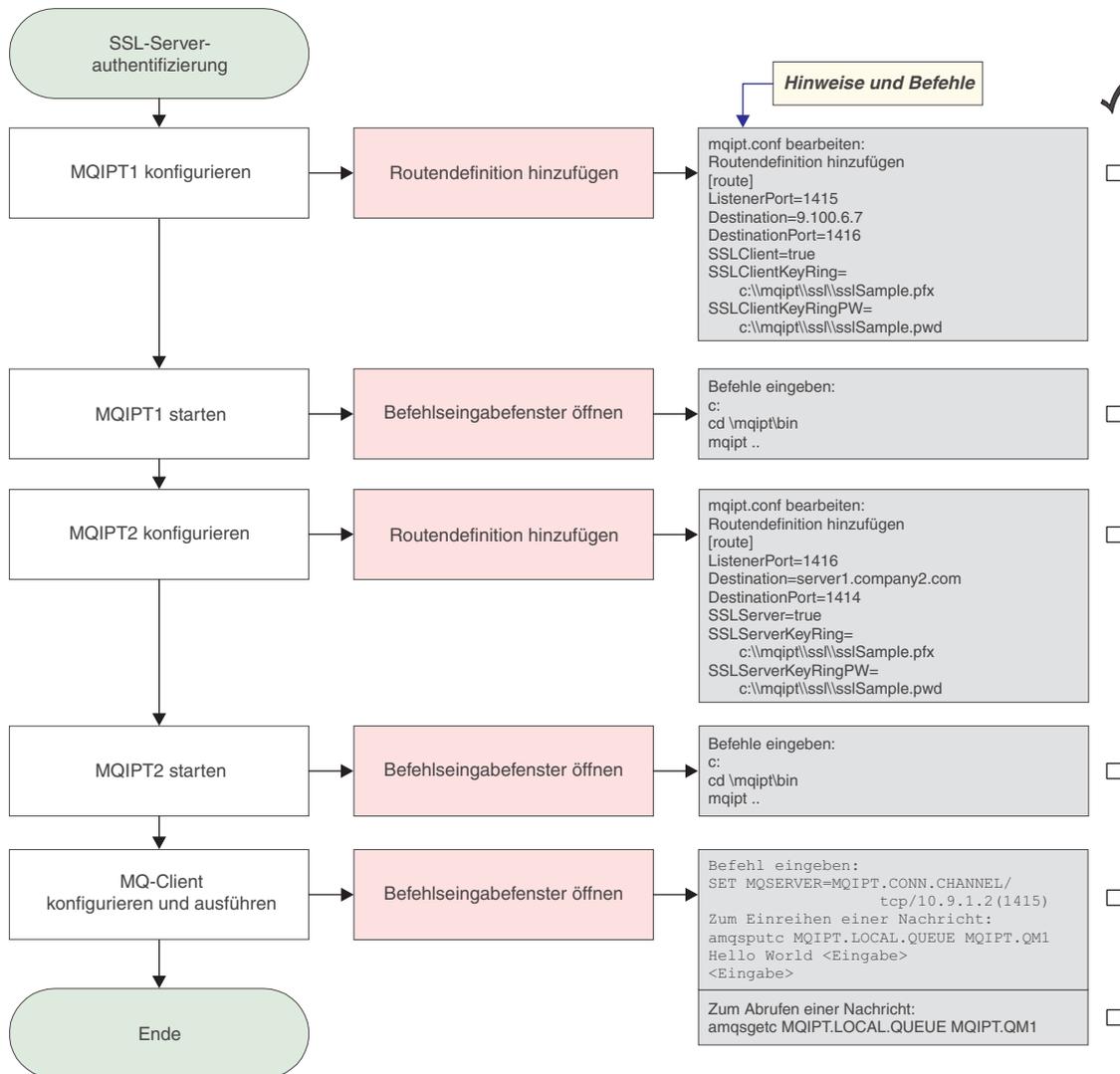


Abbildung 13. SSL-Serverauthentifizierung

1. Konfigurieren Sie MQIPT1.

Ändern Sie die Datei **mqipt.conf**, indem Sie eine Routendefinition hinzufügen:

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

2. Starten Sie MQIPT1.

Öffnen Sie ein Befehlseingabefenster, und geben Sie Folgendes ein:

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

Die folgenden Nachrichten weisen auf eine erfolgreiche Ausführung hin:

```
|
| 5639-L92 (C) Copyright IBM Corp. 2000, 2003 Alle Rechte vorbehalten.
| MQCPI001 WebSphere MQ Internet Pass-Thru Version 1.3.0 wird gestartet.
| MQCPI011 Die Protokolldateien werden im Pfad c:\mqipt\logs gespeichert.
| MQCPI006 Route 1415 wurde gestartet und leitet Nachrichten weiter an :
```

```

MQCPI034 ....9.100.6.7(1416)
MQCPI035 ....verwendet MQ-Protokolle
MQCPI036 ....SSL-Clientseite mit folgenden Eigenschaften aktiviert :
MQCPI031 .....Cipher Suites <null>
MQCPI032 .....Schlüsselringdatei c:\mqipt\sslSample.pfx
MQCPI047 .....CA-Schlüsselringdatei <null>
MQCPI038 .....registrierte Namen CN=* O=* OU=* L=* ST=* C=*
MQCPI078 Route 1415 für Verbindungsanforderungen bereit.

```

3. Konfigurieren Sie MQIPT2.

Ändern Sie die Datei **mqipt.conf**, indem Sie eine Routendefinition hinzufügen:

```

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

```

4. Starten Sie MQIPT2.

Öffnen Sie ein Befehlseingabefenster, und geben Sie Folgendes ein:

```

c:
cd \mqipt\bin
mqipt

```

Die folgenden Nachrichten weisen auf eine erfolgreiche Ausführung hin:

```

5639-L92 (C) Copyright IBM Corp. 2000, 2003 Alle Rechte vorbehalten.
MQCPI001 WebSphere MQ Internet Pass-Thru Version 1.3.0 wird gestartet.
MQCPI011 Die Protokolldateien werden im Pfad c:\mqipt\logs gespeichert.
MQCPI006 Route 1416 wurde gestartet und leitet Nachrichten weiter an :
MQCPI034 ....server1.company2.com(1414)
MQCPI035 ....verwendet MQ-Protokolle
MQCPI037 ....SSL-Serverseite mit folgenden Eigenschaften aktiviert:
MQCPI031 .....Cipher Suites <null>
MQCPI032 .....Schlüsselringdatei c:\mqipt\sslSample.pfx
MQCPI047 .....CA-Schlüsselringdatei <null>
MQCPI038 .....registrierte Namen CN=* O=* OU=* L=* ST=* C=*
MQCPI033 .....Clientauthentifizierung ist auf false gesetzt
MQCPI078 Route 1416 für Verbindungsanforderungen bereit.

```

5. Geben Sie an einer Eingabeaufforderung auf der WebSphere MQ-Clientmaschine Folgendes ein:

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

6. Reihen Sie eine Nachricht wie folgt ein:

```

amqsputc MQIPT.LOCAL.QUEUE MQIPT1.QM1
Hello world <Eingabe>
<Eingabe>

```

7. Rufen Sie die Nachricht wie folgt ab:

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

Es wird "Hello world" angezeigt.

SSL-Clientauthentifizierung

In diesem Beispiel wird eine SSL-Verbindung mit Hilfe eines Beispieletestzertifikats überprüft. Es wird eine Server- und eine Clientauthentifizierung durchgeführt. Während des SSL-Handshake sendet der Server sein Testzertifikat an den Client. Der Client wird den Server anhand seines eigenen Zertifikats, in dem "Vertrauen auf Peer-Ebene" gesetzt ist, authentifizieren. Dazu sendet der Client sein Testzertifikat an den Server. Dieser wird den Client anhand seines eigenen Zertifikats (in dem "Vertrauen auf Peer-Ebene" gesetzt ist) authentifizieren. Es wird eine standardmäßige Cipher Suite namens `SSL_RSA_WITH_RC4_128_MD5` verwendet.

(Basiert auf der unter „Installationsfunktionstest“ auf Seite 99 erstellten Datei **mqipt.conf**).

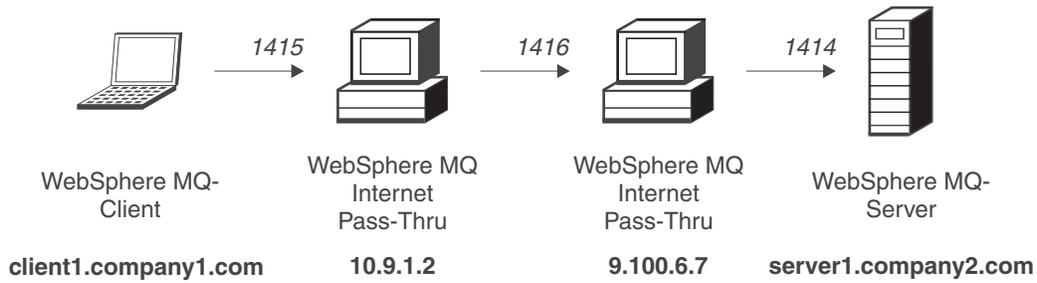


Abbildung 14. SSL-Clientnetzplan

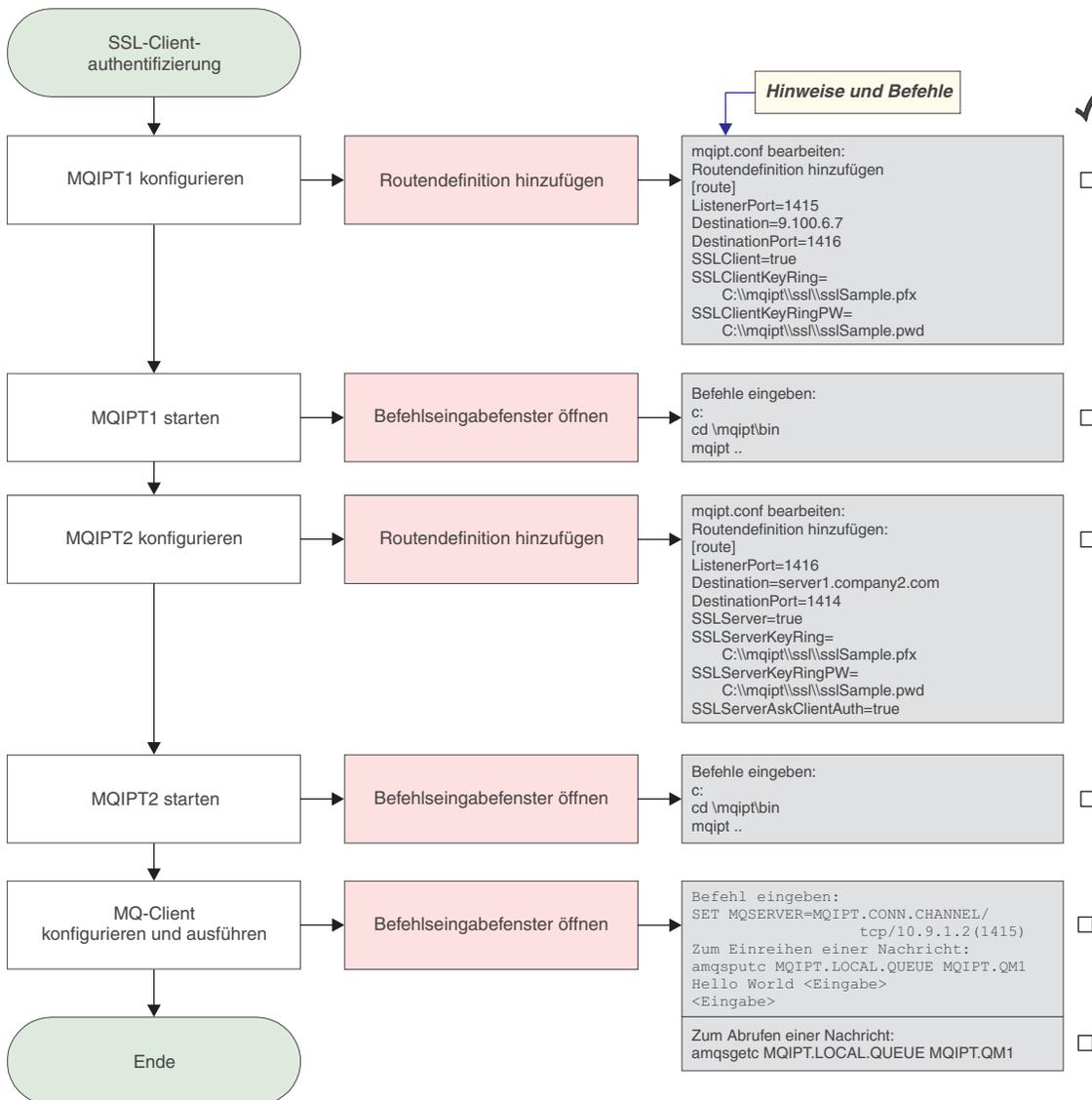


Abbildung 15. SSL-Clientauthentifizierung

1. Konfigurieren Sie MQIPT1.

Ändern Sie die Datei **mqipt.conf**, indem Sie eine Routendefinition hinzufügen:

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

2. Starten Sie MQIPT1.

Öffnen Sie ein Befehlseingabefenster, und geben Sie Folgendes ein:

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

Die folgenden Nachrichten weisen auf eine erfolgreiche Ausführung hin:

```
|
| 5639-L92 (C) Copyright IBM Corp. 2000, 2003 Alle Rechte vorbehalten.
| MQCPI001 WebSphere MQ Internet Pass-Thru Version 1.3.0 wird gestartet.
| MQCPI011 Die Protokolldateien werden im Pfad c:\mqipt\logs gespeichert.
| MQCPI006 Route 1415 wurde gestartet und leitet Nachrichten weiter an :
| MQCPI034 ....9.100.6.7(1416)
| MQCPI035 ....verwendet MQ-Protokolle
| MQCPI036 ....SSL-Clientseite mit folgenden Eigenschaften aktiviert :
| MQCPI031 .....Cipher Suites <null>
| MQCPI032 .....Schlüsselringdatei c:\mqipt\sslSample.pfx
| MQCPI047 .....CA-Schlüsselringdatei <null>
| MQCPI038 .....registrierte Namen CN=* O=* OU=* L=* ST=* C=*
| MQCPI078 Route 1415 für Verbindungsanforderungen bereit.
```

3. Konfigurieren Sie MQIPT2.

Ändern Sie die Datei **mqipt.conf**, indem Sie eine Routendefinition hinzufügen:

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

4. Starten Sie MQIPT2.

Öffnen Sie ein Befehlseingabefenster, und geben Sie Folgendes ein:

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

Die folgenden Nachrichten weisen auf eine erfolgreiche Ausführung hin:

```
|
| 5639-L92 (C) Copyright IBM Corp. 2000, 2003 Alle Rechte vorbehalten.
| MQCPI001 WebSphere MQ Internet Pass-Thru Version 1.3.0 wird gestartet.
| MQCPI011 Die Protokolldateien werden im Pfad c:\mqipt\logs gespeichert.
| MQCPI006 Route 1416 wurde gestartet und leitet Nachrichten weiter an :
| MQCPI034 ....server1.company2.com(1414)
| MQCPI035 ....verwendet MQ-Protokolle
| MQCPI037 ....SSL-Serverseite mit folgenden Eigenschaften aktiviert:
| MQCPI031 .....Cipher Suites <null>
| MQCPI032 .....Schlüsselringdatei c:\mqipt\sslSample.pfx
| MQCPI047 .....CA-Schlüsselringdatei <null>
| MQCPI038 .....registrierte Namen CN=* O=* OU=* L=* ST=* C=*
| MQCPI033 .....Clientauthentifizierung ist auf 'true' gesetzt.
| MQCPI078 Route 1416 für Verbindungsanforderungen bereit.
```

5. Geben Sie an einer Eingabeaufforderung auf der WebSphere MQ-Clientmaschine Folgendes ein:

```
SET MQSERVER=MQIPT.CONN.CHANNEL/tcp/10.9.1.2(1415)
```
6. Reihen Sie eine Nachricht wie folgt ein:

```
amqsputc MQIPT.LOCAL.QUEUE MQIPT1.QM1
Hello world <Eingabe>
<Eingabe>
```
7. Rufen Sie die Nachricht wie folgt ab:

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

Es wird "Hello world" angezeigt.

HTTP-Proxy-Konfiguration

In diesem Beispiel wird eine Verbindung mit einem HTTP-Proxy (IBM Caching Proxy) getestet. Es muss IBM Caching Proxy Version 3.6 oder höher installiert sein; außerdem sind folgende Einstellungen erforderlich:

- **ProxyPersistence** (Proxy-Permanenz) muss auf "ein" gesetzt sein; dadurch werden permanente Verbindungen ermöglicht
- **MaxPersistRequest** (Max. Anzahl Anforderungen über permanente Verbindung) muss auf "5000" gesetzt sein; dieser Wert gibt die Anzahl der maximal zulässigen Anforderungen für eine Verbindung an, bevor diese unterbrochen wird
- **PersistTimeout** (Zeitlimit für permanente Verbindung) muss auf "12 Stunden" gesetzt sein; dieser Wert gibt die Dauer einer Verbindung an

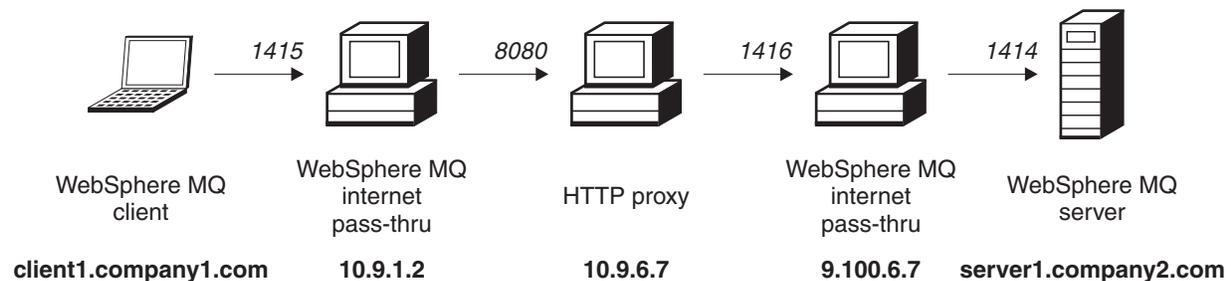


Abbildung 16. HTTP-Proxy-Netzplan

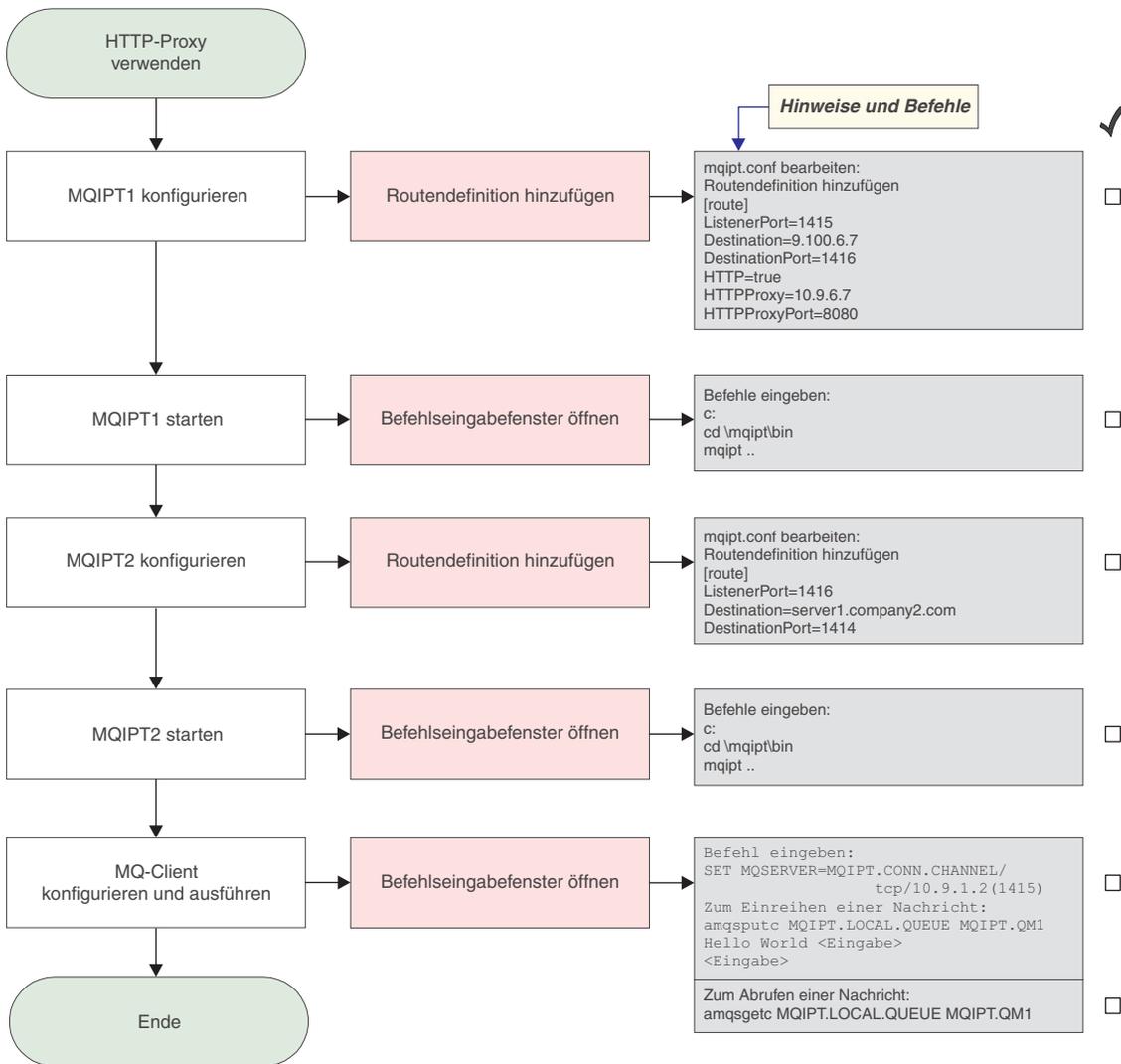


Abbildung 17. HTTP-Proxy-Konfiguration

1. Konfigurieren Sie MQIPT1.
Ändern Sie die Datei **mqipt.conf**, indem Sie eine Routendefinition hinzufügen:

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

2. Starten Sie MQIPT1.
Öffnen Sie ein Befehlseingabefenster, und geben Sie Folgendes ein:

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

Die folgenden Nachrichten weisen auf eine erfolgreiche Ausführung hin:

```
|
| 5639-L92 (C) Copyright IBM Corp. 2000, 2003 Alle Rechte vorbehalten.
| MQCPI001 WebSphere MQ Internet Pass-Thru Version 1.3.0 wird gestartet.
| MQCPI004 Die Konfigurationsdaten aus C:\mqipt\mqipt.conf werden gelesen.
| MQCPI011 Die Protokolldateien werden im Pfad C:\mqipt\logs gespeichert.
```

```

MQCPI006 Route 1415 wurde gestartet und leitet Nachrichten weiter an :
MQCPI034 ....9.100.6.7(1416)
MQCPI035 ....verwendet HTTP
MQCPI024 ....und HTTP-Proxy an 10.9.6.7(1080)
MQCPI078 Route 1415 für Verbindungsanforderungen bereit.

```

3. Konfigurieren Sie MQIPT2.

Ändern Sie die Datei **mqipt.conf**, indem Sie eine Routendefinition hinzufügen:

```

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

```

4. Starten Sie MQIPT2.

Öffnen Sie ein Befehlseingabefenster, und geben Sie Folgendes ein:

```

c:
cd \mqipt\bin
mqipt

```

Die folgenden Nachrichten weisen auf eine erfolgreiche Ausführung hin:

```

5639-L92 (C) Copyright IBM Corp. 2000, 2003 Alle Rechte vorbehalten.
MQCPI001 WebSphere MQ Internet Pass-Thru Version 1.3.0 wird gestartet.
MQCPI004 Die Konfigurationsdaten aus C:\mqipt\mqipt.conf werden gelesen.
MQCPI011 Die Protokolldateien werden im Pfad C:\mqipt\logs gespeichert.
MQCPI006 Route 1416 wurde gestartet und leitet Nachrichten weiter an :
MQCPI034 ....server1.company2.com(1414)
MQCPI035 ....verwendet MQ-Protokolle
MQCPI078 Route 1416 für Verbindungsanforderungen bereit.

```

5. Geben Sie an einer Eingabeaufforderung auf der WebSphere MQ-Clientmaschine Folgendes ein:

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

6. Reißen Sie eine Nachricht wie folgt ein:

```

amqsputc MQIPT.LOCAL.QUEUE MQIPT1.QM1
Hello world <Eingabe>
<Eingabe>

```

7. Rufen Sie die Nachricht wie folgt ab:

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

Es wird "Hello world" angezeigt.

Zugriffssteuerung konfigurieren

In diesem Beispiel wird MQIPT so konfiguriert, dass nur die Verbindungen von bestimmten Clients akzeptiert werden; dazu werden am MQIPT-Listener-Port unter Verwendung des Java Security Manager Sicherheitsprüfungen durchgeführt.

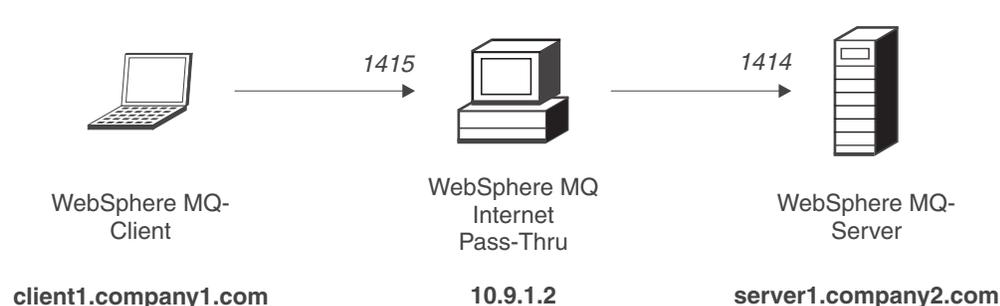


Abbildung 18. Netzplan für die Zugriffssteuerung

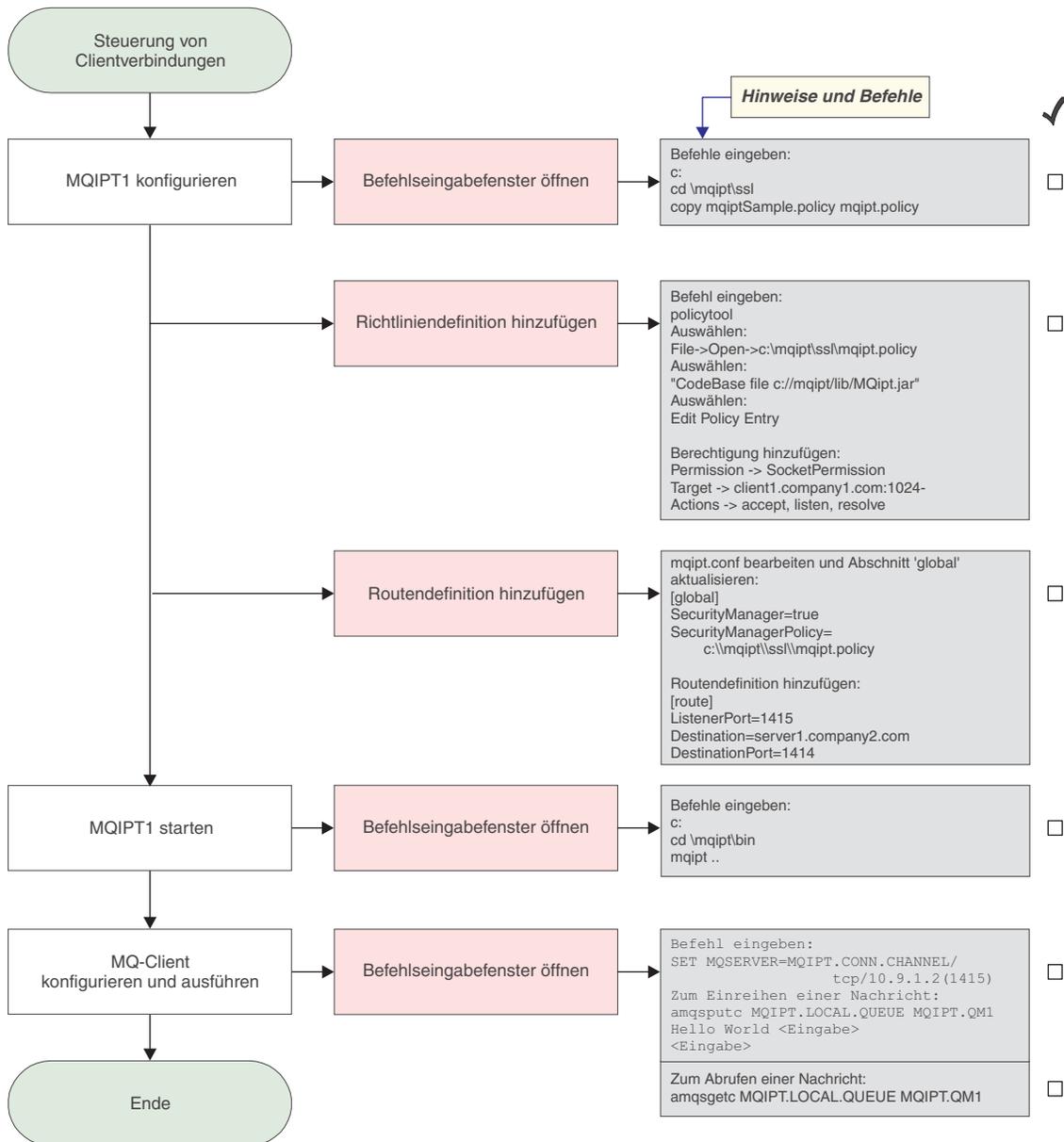


Abbildung 19. Konfiguration der Zugriffssteuerung

1. Konfigurieren Sie MQIPT1.

- a. Öffnen Sie ein Befehlseingabefenster, und geben Sie Folgendes ein:

```
c:
cd \\mqipt\\ssl
copy c:\\mqipt\\ssl\\mqiptSample.policy to mqipt.policy
```

- b. Fügen Sie mit dem folgenden Befehl eine Richtliniendefinition hinzu:

```
policytool
```

- 1) Wählen Sie **File -> Open -> c:\\mqipt\\ssl\\mqipt.policy** (Datei -> Öffnen -> c:\\mqipt\\ssl\\mqipt.policy) aus.

- 2) Wählen Sie:

```
file://C:/Program Files/IBM/WebSphere MQ internet pass-thru/lib/MQipt.jar
```

- 3) Ändern Sie die Codebasis von:
file://C:/Program Files/IBM/WebSphere MQ internet pass-thru/lib/MQipt.jar

in:
file://C:/mqipt/lib/MQipt.jar
- 4) Ändern Sie alle Berechtigungen von:
C:\Program Files\IBM\WebSphere MQ internet pass-thru

in:
C:\mqipt
- 5) Fügen Sie die Socket-Berechtigung hinzu:
Permission=SocketPermission
Target=client1.company1.com:1024-
Actions=accept, listen, resolve

c. Ändern Sie die Datei **mqipt.conf**, indem Sie Folgendes hinzufügen:

- 1) Zwei Eigenschaften im globalen Abschnitt:
[global]
SecurityManager=true
SecurityManagerPolicy=c:\mqipt\ssl\mqipt.policy
- 2) Eine Routendefinition:
[route]
ListenerPort=1415
Destination=server1.company2.com
DestinationPort=1414

2. Starten Sie MQIPT1.

Öffnen Sie ein Befehlseingabefenster, und geben Sie Folgendes ein:

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

Die folgenden Nachrichten weisen auf eine erfolgreiche Ausführung hin:

```
| 5639-L92 (C) Copyright IBM Corp. 2000, 2003 Alle Rechte vorbehalten.
| MQCPI001 WebSphere MQ Internet Pass-Thru Version 1.3.0 wird gestartet.
| MQCPI004 Die Konfigurationsdaten aus C:\mqipt\mqipt.conf werden gelesen.
| MQCPI055 Die Richtlinie für den Java Security Manager (java.security.policy)
| wird unter c:\mqipt\mqipt.policy abgestellt.
| MQCPI053 Java Security Manager wird gestartet.
| MQCPI011 Die Protokolldateien werden im Pfad C:\mqipt\logs gespeichert.
| MQCPI006 Route 1415 wurde gestartet und leitet Nachrichten weiter an :
| MQCPI034 ....server1.company2.com(1414)
| MQCPI035 ....verwendet MQ-Protokolle
| MQCPI078 Route 1415 für Verbindungsanforderungen bereit.
```

3. Geben Sie an einer Eingabeaufforderung auf der WebSphere MQ-Clientmaschine Folgendes ein:
SET MQSERVER=MQIPT.CONN.CHANNEL/tcp/10.9.1.2(1415)
4. Reihnen Sie eine Nachricht wie folgt ein:
amqsputc MQIPT.LOCAL.QUEUE MQIPT1.QM1
Hello world <Eingabe>
<Eingabe>
5. Rufen Sie die Nachricht wie folgt ab:
amqsgetc MQIPT.LOCAL.QUEUE MQIPT1.QM1

Es wird "Hello world" angezeigt.

Quality of Service (QoS) konfigurieren

In diesem Beispiel wird davon ausgegangen, dass TQoS bereits auf der derselben Maschine installiert wurde, auf der sich auch MQIPT befindet.

In diesem Beispiel wird allen Kanälen auf einer MQIPT-Route eine Servicequalität (Quality of Service, QoS) zugeordnet. Dies ist nur möglich, wenn MQIPT auf der Linux-Plattform läuft. In diesem Beispiel wird allen von MQIPT an den WebSphere MQ-Client gesendeten Daten die Prioritätsstufe 'mittel', allen an den WebSphere MQ-Server gesendeten Daten die Prioritätsstufe 'gut' zugeordnet. Mit den Beispielrichtlinien des Agent (Richtlinienagenten) können `QoSToCaller` (QoS an Anrufer) und `QoSToDest` (QoS an Zieladresse) die folgenden Prioritätsstufen zugeordnet werden:

- 1 - mittel
- 2 - gut
- 3 - sehr gut

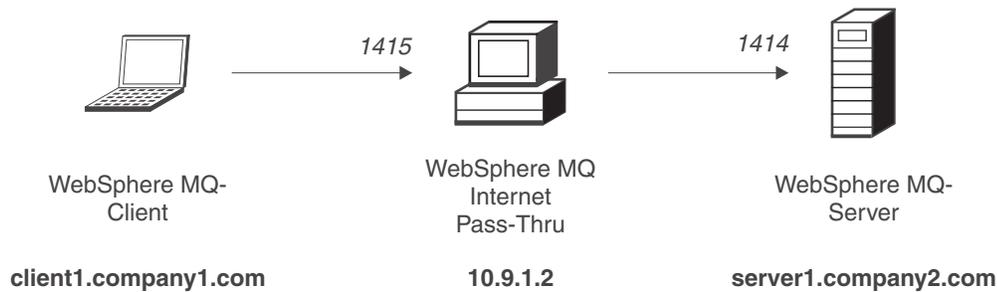


Abbildung 20. QoS-Netzplan

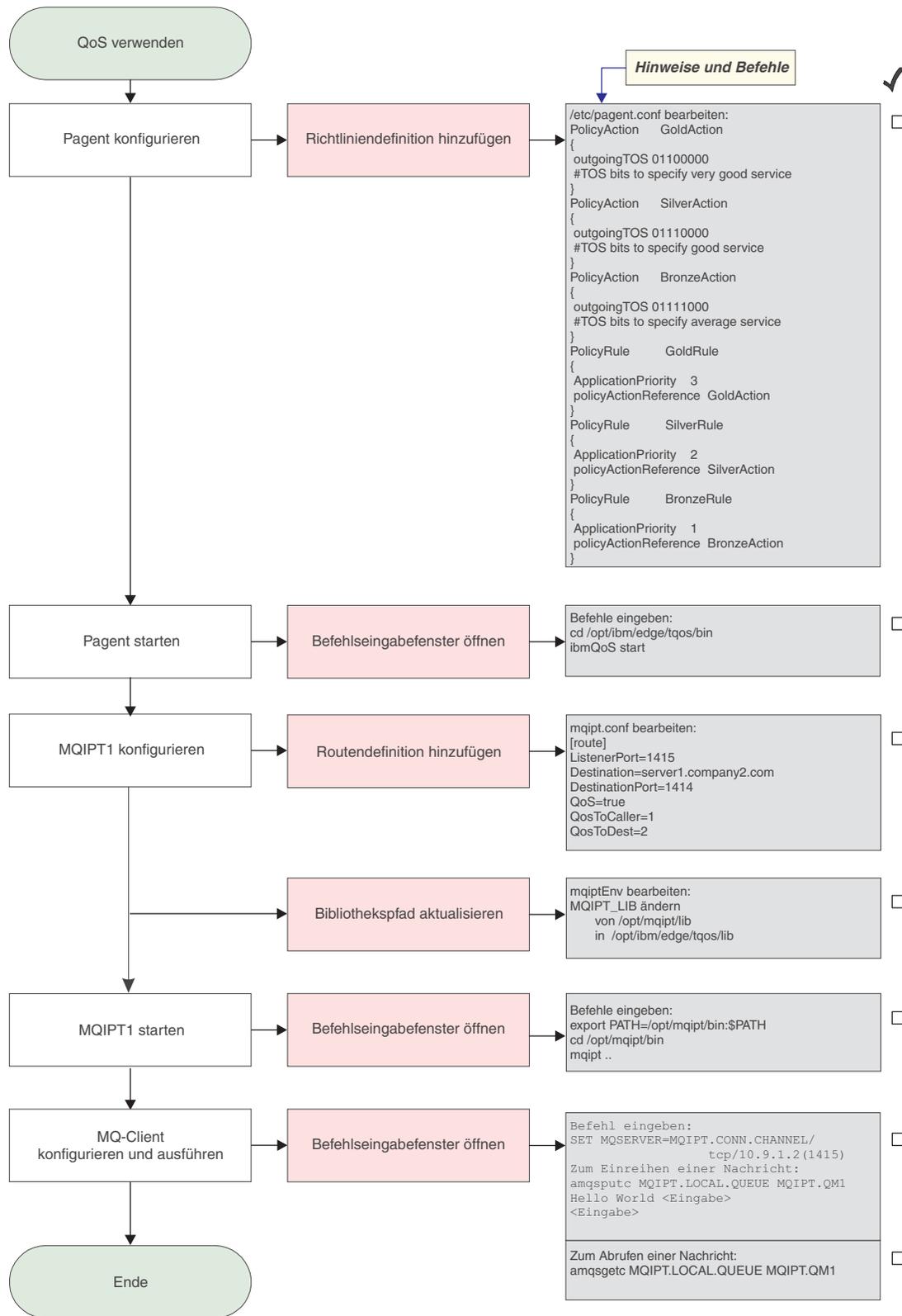


Abbildung 21. QoS-Konfiguration

1. Konfigurieren Sie den Pagent.

Ändern Sie die Datei **/etc/pagent.conf**, indem Sie Folgendes hinzufügen:

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

| Aktivieren Sie die Erfassung von Leistungsdaten für die oben definierten
| Regeln mit Hilfe der Anweisung PolicyPerformanceCollection. Eine Beschrei-
| bung dieser Anweisung und ihres Formats finden Sie in der Datei 'Pagent.conf'.

2. Starten Sie den Pagent.

Öffnen Sie ein Befehlseingabefenster, und geben Sie Folgendes ein:

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

3. Konfigurieren Sie MQIPT1.

Ändern Sie die Datei **mqipt.conf**, indem Sie eine Routendefinition hinzufügen:

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

4. Aktualisieren Sie den Bibliothekspfad.

Ändern Sie die Datei **mqiptEnv** (im Verzeichnis **/opt/mqipt/bin**), indem Sie MQIPT_LIB ändern, und zwar von:

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

in:

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

5. Starten Sie MQIPT1.

Öffnen Sie ein Befehlseingabefenster, und geben Sie Folgendes ein:

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

Die folgenden Nachrichten weisen auf eine erfolgreiche Ausführung hin:

```
5639-L92 (C) Copyright IBM Corp. 2000, 2003 Alle Rechte vorbehalten.
MQCPI001 WebSphere MQ Internet Pass-Thru Version 1.3.0 wird gestartet.
MQCPI004 Die Konfigurationsdaten aus /opt/mqipt/mqipt.conf werden gelesen.
MQCPI011 Die Protokolldateien werden im Pfad /opt/mqipt/logs gespeichert.
MQCPI006 Route 1415 wurde gestartet und leitet Nachrichten weiter an :
MQCPI034 ....server1.company2.com(1414)
MQCPI035 ....verwendet MQ-Protokolle
MQCPI049 ....QoS-Priorität für Zieladresse = 2, für Anrufer = 1
MQCPI078 Route 1415 für Verbindungsanforderungen bereit.
```

6. Geben Sie an einer Eingabeaufforderung auf der WebSphere MQ-Clientmaschine Folgendes ein:

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

7. Reihnen Sie eine Nachricht wie folgt ein:

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

8. Rufen Sie die Nachricht wie folgt ab:

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

Es wird "Hello world" angezeigt.

SOCKS-Proxy konfigurieren

In diesem Beispiel wird MQIPT als SOCKS-Proxy eingerichtet. Der WebSphere MQ-Client muss vor Ausführung dieses Beispiels SOCKSifiziert werden, damit diese Beispielkonfiguration arbeitet; außerdem muss die SOCKS-Konfiguration auf MQIPT als SOCKS-Proxy verweisen. Für die MQIPT-Eigenschaften **Destination** (Zieladresse) und **DestinationPort** (Ziel-Port) kann ein beliebiger Wert angegeben werden, da der WebSphere MQ-Client die tatsächliche Zieladresse während des SOCKS-Handshake abrufen.

Bevor Sie anfangen, muss zunächst entweder die ganze Maschine oder nur die WebSphere MQ-Clientanwendung SOCKSifiziert werden. Darüber hinaus muss der SOCKS-Client wie folgt konfiguriert werden:

- Er muss auf MQIPT als SOCKS-Proxy zeigen.
- Die Unterstützung für SOCKS V5 muss aktiviert werden.
- Die Benutzerauthentifizierung muss deaktiviert werden.
- Es dürfen nur Verbindungen zur MQIPT-Netzadresse hergestellt werden.

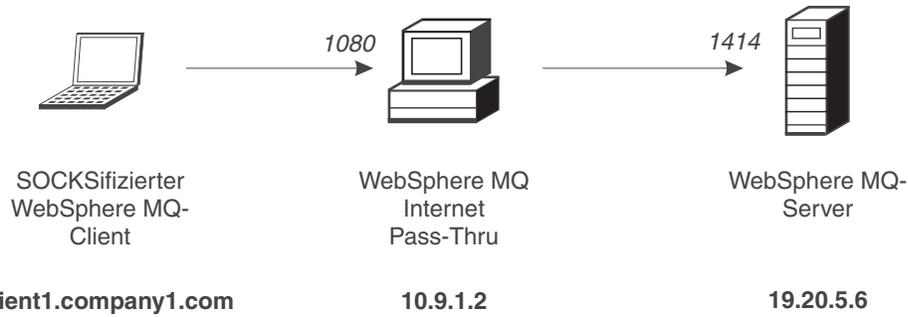


Abbildung 22. Netzplan für SOCKS-Proxy

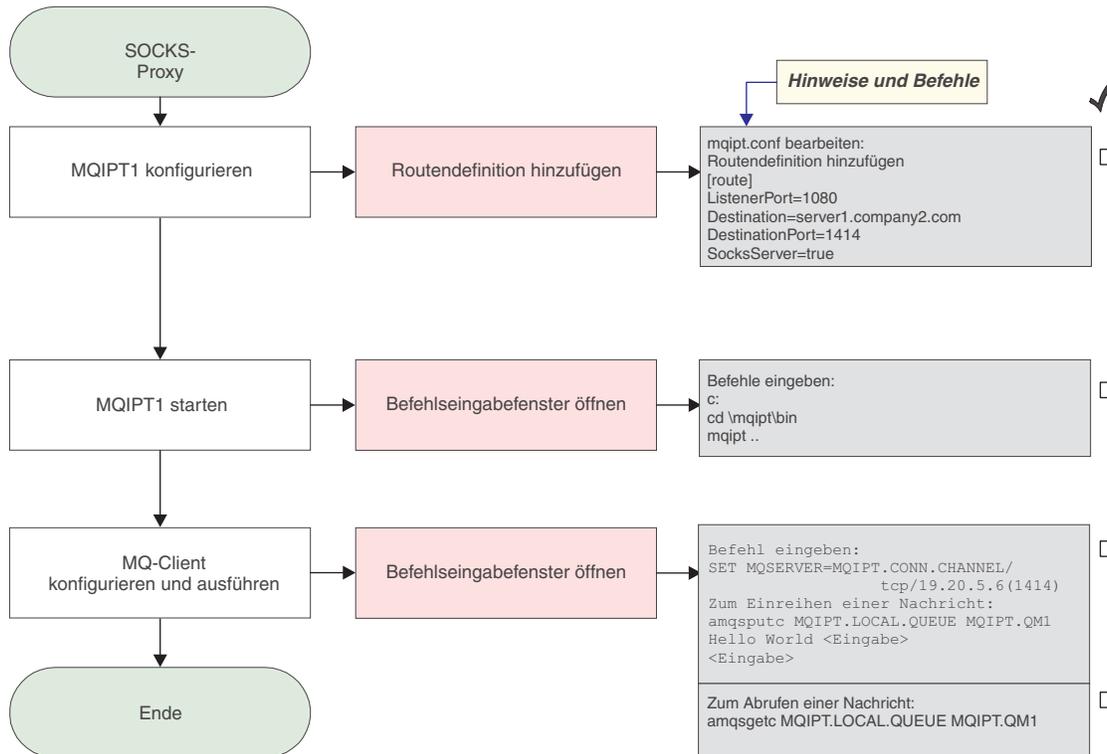


Abbildung 23. SOCKS-Proxy-Konfiguration

1. Konfigurieren Sie MQIPT1.

Ändern Sie die Datei **mqipt.conf**, indem Sie eine Routendefinition hinzufügen:

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

2. Starten Sie MQIPT1.

Öffnen Sie ein Befehlseingabefenster, und geben Sie Folgendes ein:

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

Die folgenden Nachrichten weisen auf eine erfolgreiche Ausführung hin:

```
5639-L92 (C) Copyright IBM Corp. 2000, 2003 Alle Rechte vorbehalten.
MQCPI001 WebSphere MQ Internet Pass-Thru Version 1.3.0 wird gestartet.
MQCPI004 Die Konfigurationsdaten aus C:\mqipt\mqipt.conf werden gelesen.
MQCPI011 Die Protokolldateien werden im Pfad C:\mqipt\logs gespeichert.
MQCPI006 Route 1080 wurde gestartet und leitet Nachrichten weiter an :
MQCPI034 ....server1.company2.com(1414)
MQCPI035 ....verwendet MQ-Protokolle
MQCPI052 ....Socks-Serverseite aktiviert
MQCPI078 Route 1080 für Verbindungsanforderungen bereit.
```

3. Geben Sie an einer Eingabeaufforderung auf der WebSphere MQ-Clientmaschine Folgendes ein:

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

4. Reihnen Sie eine Nachricht wie folgt ein:

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

5. Rufen Sie die Nachricht wie folgt ab:

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

Es wird "Hello world" angezeigt.

SOCKS-Client konfigurieren

In diesem Beispiel wird der MQIPT unter Verwendung eines bereits vorhandenen SOCKS-Proxy so betrieben, als ob er SOCKSifiziert ist. Dies entspricht in etwa der Konfiguration in „SOCKS-Proxy konfigurieren“ auf Seite 113, nur dass der MQIPT, und nicht der WebSphere MQ-Client eine SOCKSifizierte Verbindung herstellt.

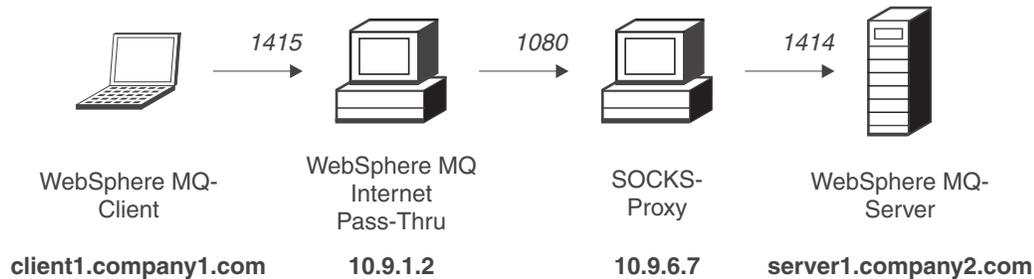


Abbildung 24. SOCKS-Clientnetzplan

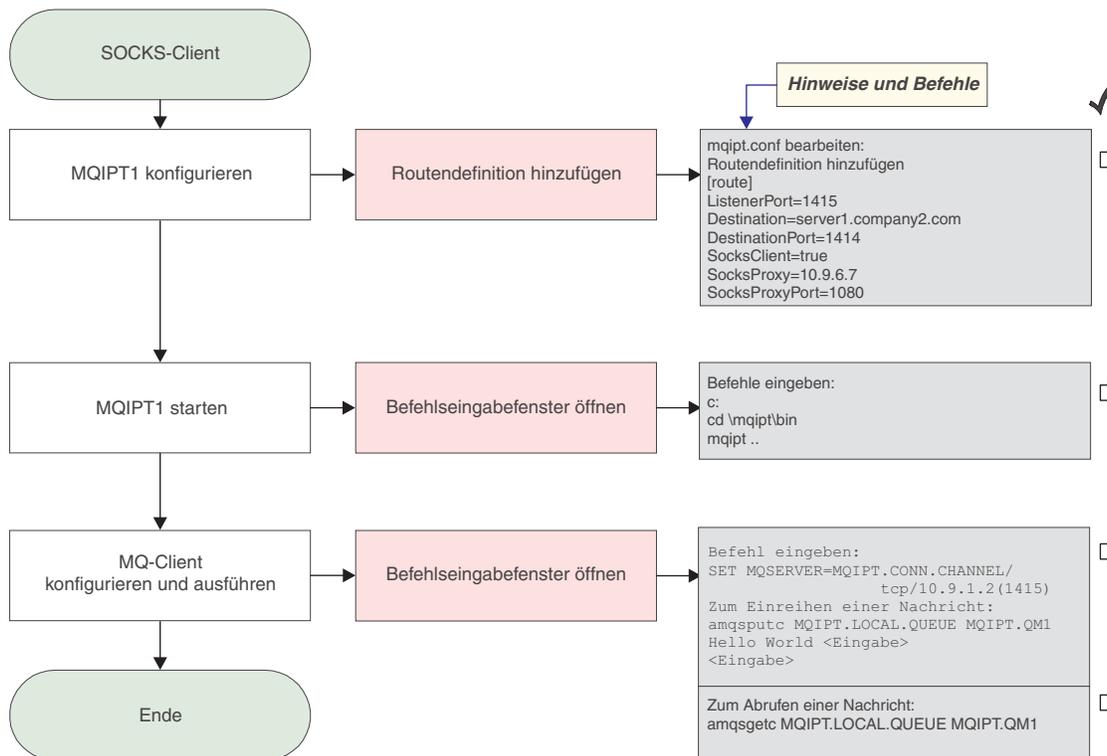


Abbildung 25. SOCKS-Clientkonfiguration

1. Konfigurieren Sie MQIPT1.

Ändern Sie die Datei **mqipt.conf**, indem Sie eine Routendefinition hinzufügen:

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

2. Starten Sie MQIPT1.

Öffnen Sie ein Befehlseingabefenster, und geben Sie Folgendes ein:

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

Die folgenden Nachrichten weisen auf eine erfolgreiche Ausführung hin:

```
| 5639-L92 (C) Copyright IBM Corp. 2000, 2003 Alle Rechte vorbehalten.
| MQCPI001 WebSphere MQ Internet Pass-Thru Version 1.3.0 wird gestartet.
| MQCPI004 Die Konfigurationsdaten aus C:\mqipt\mqipt.conf werden gelesen.
| MQCPI022 Für den Befehls-Port wurde keine Kennwortprüfung aktiviert.
| MQCPI011 Die Protokolldateien werden im Pfad C:\mqipt\logs gespeichert.
| MQCPI006 Route 1415 wurde gestartet und leitet Nachrichten weiter an :
| MQCPI034 ....server1.company2.com(1414)
| MQCPI035 ....verwendet MQ-Protokolle
| MQCPI039 ....und Socks-Proxy an 10.9.6.7(1080)
| MQCPI078 Route 1415 für Verbindungsanforderungen bereit.
```

3. Geben Sie an einer Eingabeaufforderung auf der WebSphere MQ-Clientmaschine Folgendes ein:

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

4. Reihnen Sie eine Nachricht wie folgt ein:

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

5. Rufen Sie die Nachricht wie folgt ab:

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

Es wird "Hello world" angezeigt.

SSL-Testzertifikate erstellen

Dieses Beispiel zeigt, wie Sie ein selbstsigniertes Zertifikat zum Testen von MQIPT-Routen erstellen können. In diesem Zertifikat ist "Vertrauen auf Peer-Ebene" gesetzt.

1. Starten Sie KeyMan.
2. Wählen Sie **Create new...** (Neu...) aus.
3. Wählen Sie **PKCS#12 Token** (PKCS#12-Token) aus.
4. Wählen Sie **Action -> Generate Key** (Aktion -> Schlüssel erstellen) aus.
In der Liste **RSA / 1024-bit** wird ein neues Schlüsselpaar angezeigt.
5. Wählen Sie das neue Schlüsselpaar aus.
6. Wählen Sie **Action -> Create Certificate** (Aktion -> Zertifikat erstellen) aus.
7. Wählen Sie **Self-signed Certificate** (Selbstsigniertes Zertifikat) aus.
8. Geben Sie Angaben zum Zertifikat ein.
In einem Dialogfenster werden Sie darauf hingewiesen, dass das private Zertifikat mit dem Schlüssel verknüpft wird; die Eingabe einer Kennung ist optional.
9. Wählen Sie das neue Zertifikat aus.
10. Zeigen Sie die Einzelangaben zum Zertifikat an.
11. Ändern Sie die Zertifikateigenschaften.
12. Aktivieren Sie den Parameter "Vertrauen auf Peer-Ebene".
13. Schließen Sie den Dialog, und wählen Sie **File -> Save** (Datei -> Speichern) aus.
14. Geben Sie eine Passphrase (z. B. "myPassWord") ein.
15. Geben Sie für die neue Schlüsselringdatei einen Namen ein (z. B. c:\mqipt\ssl\testRoute1414.pfx).
Als Dateiformat muss **PKCS#12 / PFX** beibehalten werden; die Option **Wrap key ring into a Java class** (Schlüsselring in Java-Klasse einbetten) darf **nicht** aktiviert werden.
16. Erstellen Sie eine Textdatei, die die oben verwendete Passphrase (myPassWord) enthält.
Beispiel: c:\mqipt\ssl\testRoute1414.pwd

Diese Schlüsselringdatei kann jetzt im Beispiel „SSL-Serverauthentifizierung“ auf Seite 100 verwendet werden.

MQIPT-Servlet konfigurieren

Zusätzlich zu den Informationen unter „Voraussetzungen“ auf Seite 97 geht dieses Beispiel von folgenden Annahmen aus:

- Der Tomcat-Anwendungsserver wurde in folgendem Verzeichnis installiert:
c:\jakarta-tomcat-4.0.1

Sie können Tomcat von folgender Website herunterladen:

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

- IBM Web Traffic Express wurde in folgendem Verzeichnis installiert:
c:\wte

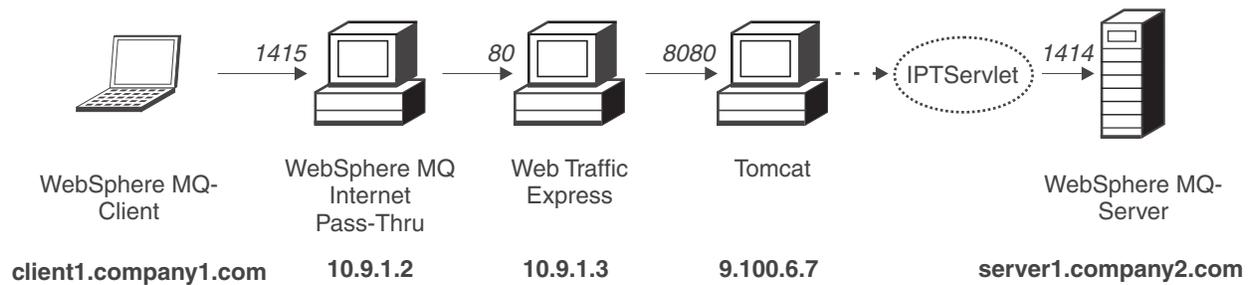


Abbildung 26. Servlet-Netzplan

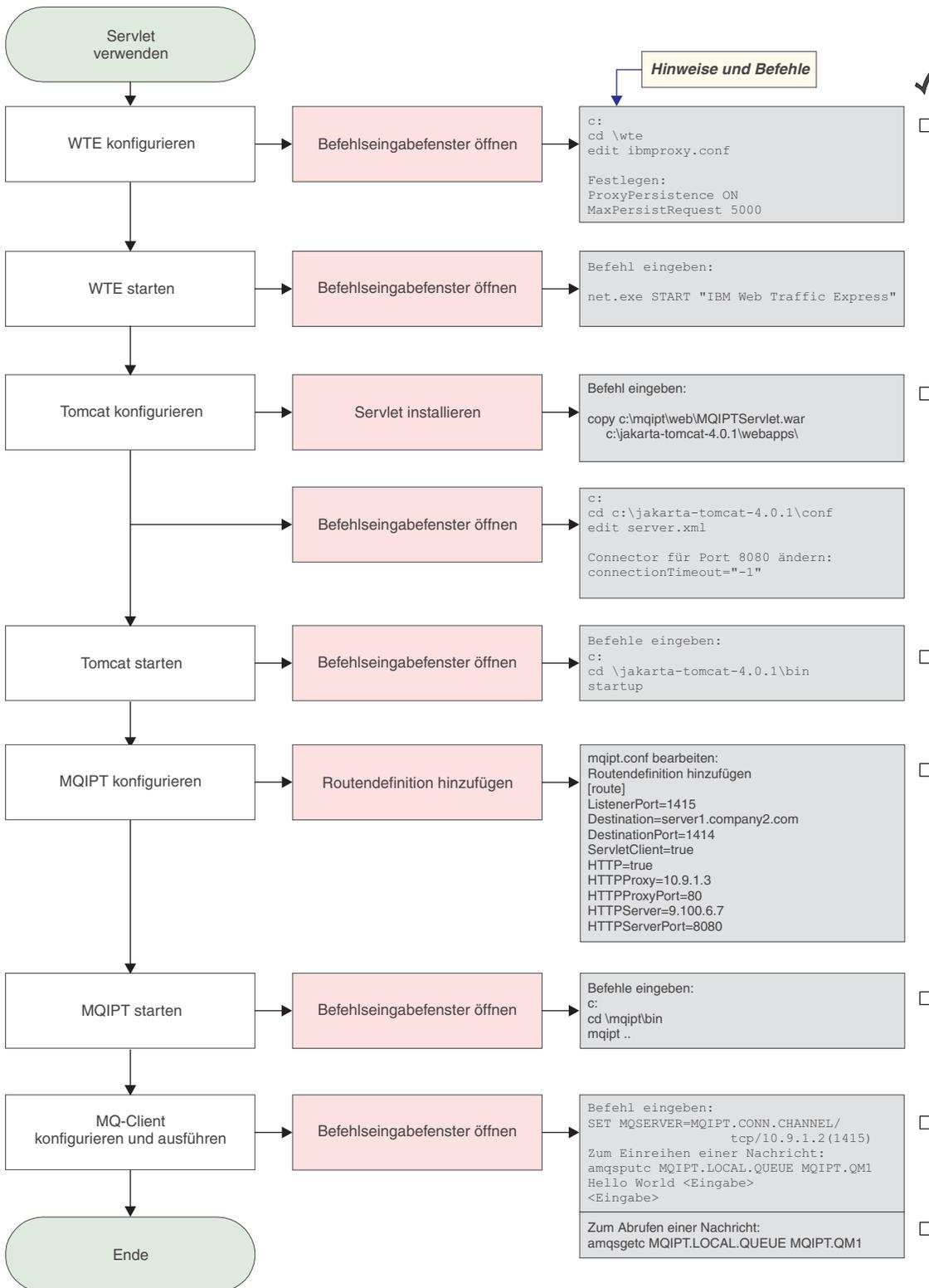


Abbildung 27. Servlet-Konfiguration

1. Konfigurieren Sie Web Traffic Express.
Legen Sie in der Datei `c:\wte\ibmproxy.conf` die folgenden Eigenschaften fest:

```
ProxyPersistence ON
MaxPersistRequest 5000
```
2. Starten Sie Web Traffic Express.
Öffnen Sie ein Befehlseingabefenster, und geben Sie Folgendes ein:

```
net.exe Start "IBM Web Traffic Express"
```
3. Konfigurieren Sie Tomcat.
Kopieren Sie zum Installieren des Servlets die Datei

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


nach:

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


Aktivieren Sie in der Datei `c:\jakarta-tomcat-4.0.1\conf\server.xml` den Connector für Port 8443, und setzen Sie die Eigenschaft `ConnectionTimeout` auf -1.
4. Starten Sie Tomcat.
Öffnen Sie ein Befehlseingabefenster, und geben Sie Folgendes ein:

```
c:
cd \jakarta-tomcat-4.0.1\bin
startup
```
5. Konfigurieren Sie MQIPT1.
Ändern Sie die Datei `mqipt.conf`, indem Sie eine Routendefinition hinzufügen:

```
[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. Starten Sie MQIPT1.
Öffnen Sie ein Befehlseingabefenster, und geben Sie Folgendes ein:

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

Die folgenden Nachrichten weisen auf eine erfolgreiche Ausführung hin:

```
|
| 5639-L92 (C) Copyright IBM Corp. 2000, 2003 Alle Rechte vorbehalten.
| MQCPI001 WebSphere MQ Internet Pass-Thru Version 1.3.0 wird gestartet.
| MQCPI004 Die Konfigurationsdaten aus C:\mqipt\mqipt.conf werden gelesen.
| MQCPI011 Die Protokolldateien werden im Pfad C:\mqipt\logs gespeichert.
| MQCPI006 Route 1415 wurde gestartet und leitet Nachrichten weiter an :
| MQCPI034 ....server1.company2.com(1414)
| MQCPI035 ....verwendet HTTP
| MQCPI024 ....und HTTP-Proxy an 10.9.1.3(80)
| MQCPI066 ....und HTTP-Server an 9.100.6.7(8080)
| MQCPI059 ....Servlet-Client aktiviert
| MQCPI078 Route 1415 für Verbindungsanforderungen bereit.
```

7. Geben Sie an einer Eingabeaufforderung auf der WebSphere MQ-Clientmaschine Folgendes ein:

```
SET MQSERVER=MQIPT.CONN.CHANNEL/tcp/10.9.1.2(1415)
```
8. Reihen Sie eine Nachricht wie folgt ein:

```
amqsputc MQIPT.LOCAL.QUEUE MQIPT1.QM1  
Hello world <Eingabe>  
<Eingabe>
```
9. Rufen Sie die Nachricht wie folgt ab:

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

Es wird "Hello world" angezeigt.

HTTPS-Konfiguration

Zusätzlich zu den Informationen unter „Voraussetzungen“ auf Seite 97 geht dieses Beispiel von folgenden Annahmen aus:

- Der Tomcat-Anwendungsserver wurde in folgendem Verzeichnis installiert:
c:\jakarta-tomcat-4.0.1

Sie können Tomcat von folgender Website herunterladen:

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

- IBM Web Traffic Express wurde in folgendem Verzeichnis installiert:
c:\wte

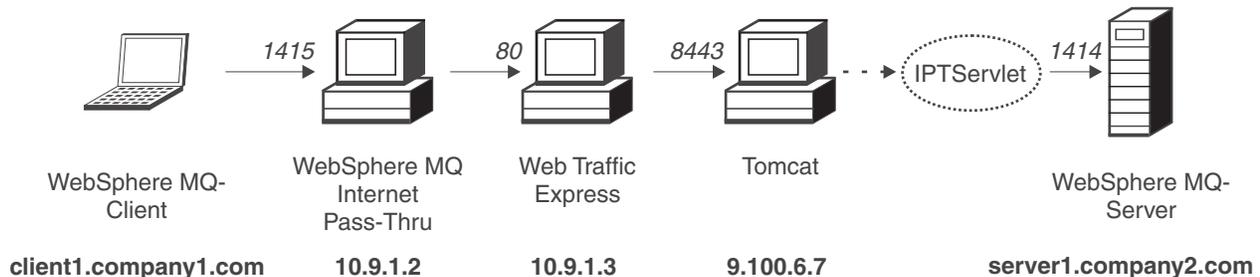


Abbildung 28. HTTPS-Netzplan

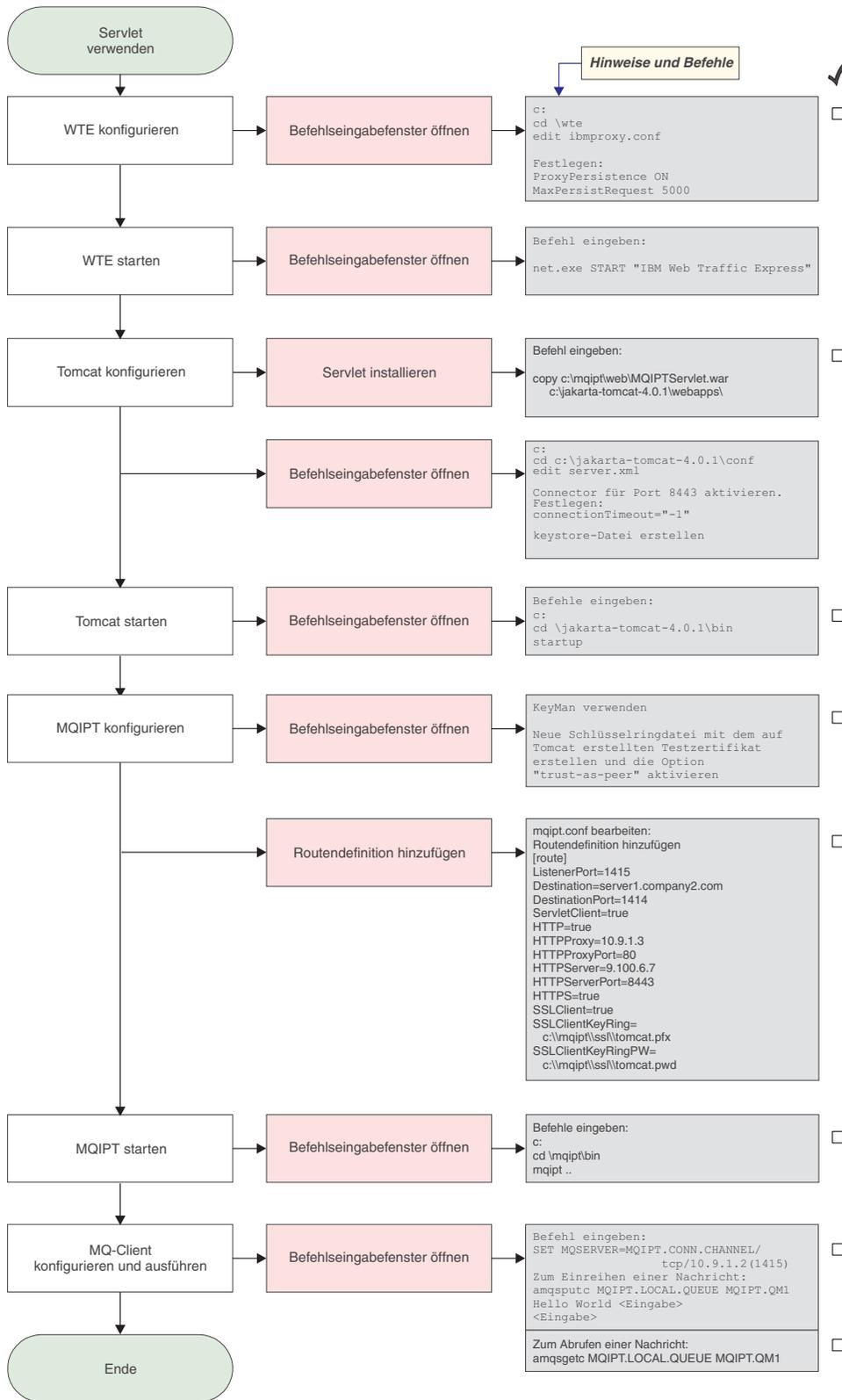


Abbildung 29. HTTPS-Konfiguration

1. Konfigurieren Sie Web Traffic Express.
Legen Sie in der Datei `c:\wte\ibmroxy.conf` die folgenden Eigenschaften fest:

```
ProxyPersistence ON
MaxPersistRequest 5000
```
2. Starten Sie Web Traffic Express.
Öffnen Sie ein Befehlseingabefenster, und geben Sie Folgendes ein:

```
net.exe Start "IBM Web Traffic Express"
```
3. Konfigurieren Sie Tomcat.
Kopieren Sie zum Installieren des Servlets die Datei

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

nach:

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

Aktivieren Sie in der Datei `c:\jakarta-tomcat-4.0.1\conf\server.xml` den Connector für Port 8443, und setzen Sie die Eigenschaft `ConnectionTimeout` auf `-1`.

Lesen Sie die Tomcat-Dokumentation, die unter
<http://jakarta.apache.org/tomcat/tomcat-4.0-doc/index.html>

zur Verfügung steht, und folgen Sie den Anweisungen unter "SSL Configuration HOW-TO", um SSL-Verbindungen für Port 8443 zu aktivieren. Erstellen Sie eine Schlüsselringdatei mit einem selbstsignierten Testzertifikat. Das Ergebnis ist eine Datei mit dem Namen

```
C:\winnt\profiles\<Benutzer-ID>\.keystore.
```
4. Starten Sie Tomcat.
Öffnen Sie ein Befehlseingabefenster, und geben Sie Folgendes ein:

```
c:
cd \jakarta-tomcat-4.0.1\bin
startup
```
5. Kopieren Sie die neue keystore-Datei vom Tomcat-System auf das MQIPT-System. Öffnen Sie mit KeyMan die neue keystore-Datei (Standardkennwort ist `changeit`), und aktivieren Sie die Option "Vertrauen auf Peer-Ebene" (weitere Informationen siehe „SSL-Testzertifikate erstellen“ auf Seite 118). Speichern Sie die Datei als `c:\mqipt\ssl\tomcat.pfx`, und erstellen Sie eine Textdatei mit dem Namen `c:\mqipt\ssl\tomcat.pwd`, die das Kennwort `changeit` enthält.
6. Konfigurieren Sie MQIPT1.
Ändern Sie die Datei **mqipt.conf**, indem Sie eine Routendefinition hinzufügen:

```
[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. Starten Sie MQIPT1.

Öffnen Sie ein Befehlseingabefenster, und geben Sie Folgendes ein:

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

Die folgenden Nachrichten weisen auf eine erfolgreiche Ausführung hin:

```
5639-L92 (C) Copyright IBM Corp. 2000, 2003 Alle Rechte vorbehalten.  
MQCPI001 WebSphere MQ Internet Pass-Thru Version 1.3.0 wird gestartet.  
MQCPI004 Die Konfigurationsdaten aus C:\mqipt\mqipt.conf werden gelesen.  
MQCPI011 Die Protokolldateien werden im Pfad C:\mqipt\logs gespeichert.  
MQCPI006 Route 1415 wurde gestartet und leitet Nachrichten weiter an :  
MQCPI034 ....server1.company2.com(1414)  
MQCPI035 ....verwendet HTTP  
MQCPI024 ....und HTTP-Proxy an 10.9.1.3(80)  
MQCPI066 ....und HTTP-Server an 9.100.6.7(8080)  
MQCPI059 ....Servlet-Client aktiviert  
MQCPI036 ....SSL-Clientseite mit folgenden Eigenschaften aktiviert :  
MQCPI031 .....Cipher Suites <null>  
MQCPI032 .....Schlüsselringdatei c:\mqipt\ssl\tomcat.pfx  
MQCPI047 .....CA-Schlüsselringdatei <null>  
MQCPI038 .....registrierte Namen CN=* O=* OU=* L=* ST=* C=*  
MQCPI078 Route 1415 für Verbindungsanforderungen bereit.
```

8. Geben Sie an einer Eingabeaufforderung auf der WebSphere MQ-Clientmaschine Folgendes ein:

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

9. Reihen Sie eine Nachricht wie folgt ein:

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

10. Rufen Sie die Nachricht wie folgt ab:

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

Es wird "Hello world" angezeigt.

Unterstützung für MQIPT-Clustering konfigurieren

Für diese Beispielkonfiguration müssen zusätzlich zu den unter „Voraussetzungen“ auf Seite 97 aufgeführten Voraussetzungen noch folgende Schritte ausgeführt worden sein:

Auf dem WebSphere MQ-Server LONDON:

- Es wurde ein WS-Manager namens LONDON definiert.
- Es wurde ein Serververbindungskanal mit der Bezeichnung MQIPT.CONN.CHANNEL definiert.
- Für LONDON wurde an Port 1414 ein TCP/IP-Empfangsprogramm gestartet.
- Der WS-Manager wurde SOCKSifiziert.

Auf dem WebSphere MQ-Server NEWYORK:

- Es wurde ein WS-Manager namens NEWYORK definiert.
- Es wurde ein Serververbindungskanal mit der Bezeichnung MQIPT.CONN.CHANNEL definiert.
- Für NEWYORK wurde an Port 1414 ein TCP/IP-Empfangsprogramm gestartet.
- Der WS-Manager wurde SOCKSifiziert.

Um den WS-Manager zu SOCKSifizieren, muss entweder die gesamte Maschine oder lediglich die WebSphere MQ-Serveranwendung SOCKSifiziert werden. Konfigurieren Sie den SOCKS-Client wie folgt:

- Er muss auf MQIPT als SOCKS-Proxy verweisen.
- Die Unterstützung für SOCKS V5 muss aktiviert werden.
- Die Benutzerauthentifizierung muss deaktiviert werden.
- Es dürfen nur ferne Verbindungen zum MQIPT hergestellt werden.

Nur jeweils eine Anwendung kann an einer gegebenen Port-Adresse auf einer Maschine empfangsbereit sein. Wenn Port 1414 bereits anderweitig zugeordnet ist, müssen Sie einen freien Port wählen und diesen in den Beispielen verwenden. Nachdem Sie die oben beschriebenen Schritte ausgeführt haben, können Sie die Routen zwischen den WS-Managern testen, indem Sie eine Nachricht in die lokale Warteschlange des WS-Managers LONDON einreihen und vom WS-Manager NEWYORK aus abrufen.

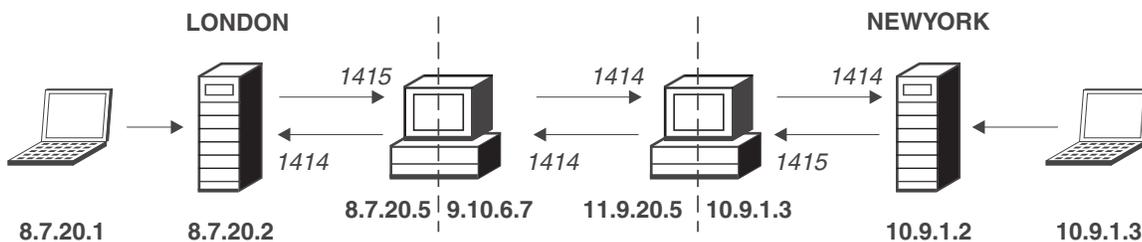


Abbildung 30. Clustering-Netzplan

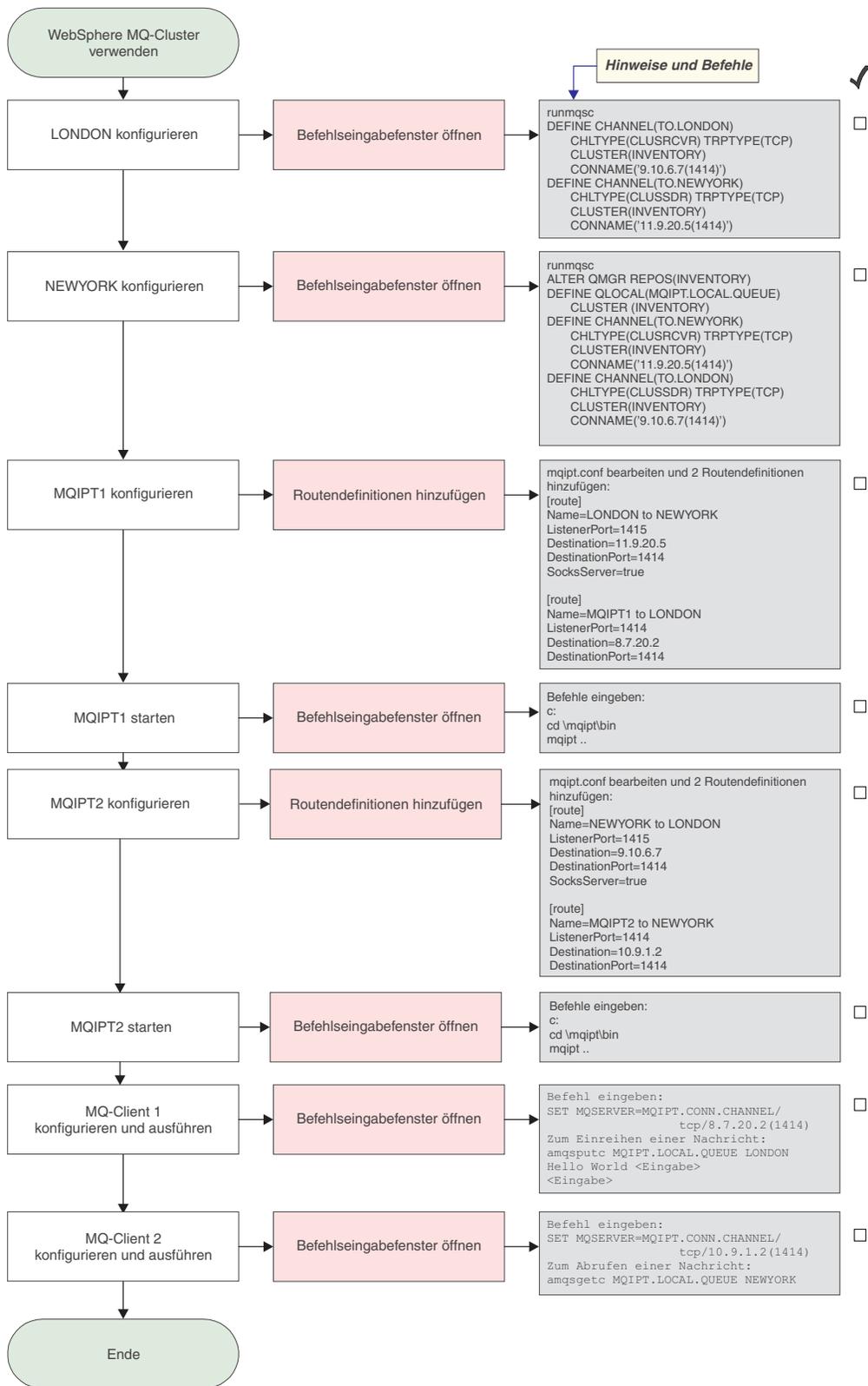


Abbildung 31. Clustering-Konfiguration

1. Konfigurieren Sie LONDON.

Öffnen Sie ein Befehlseingabefenster, und geben Sie Folgendes ein:

```
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. Konfigurieren Sie NEWYORK.

Öffnen Sie ein Befehlseingabefenster, und geben Sie Folgendes ein:

```
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. Konfigurieren Sie MQIPT1.

Ändern Sie die Datei **mqipt.conf**, indem Sie zwei Routendefinitionen hinzufügen:

```
[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. Starten Sie MQIPT1.

Öffnen Sie ein Befehlseingabefenster, und geben Sie Folgendes ein:

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

Die folgenden Nachrichten weisen auf eine erfolgreiche Ausführung hin:

```
| 5639-L92 (C) Copyright IBM Corp. 2000, 2003 Alle Rechte vorbehalten.
| MQCPI001 WebSphere MQ Internet Pass-Thru Version 1.3.0 wird gestartet.
| MQCPI004 Die Konfigurationsdaten aus C:\mqipt\mqipt.conf werden gelesen.
| MQCPI011 Die Protokolldateien werden im Pfad C:\mqipt\logs gespeichert.
| MQCPI006 Route 1415 wurde gestartet und leitet Nachrichten weiter an :
| MQCPI034 ....11.9.20.5(1414)
| MQCPI035 ....verwendet MQ-Protokolle
| MQCPI052 ....Socks-Serverseite aktiviert
| MQCPI078 Route 1415 für Verbindungsanforderungen bereit.
| MQCPI006 Route 1414 wurde gestartet und leitet Nachrichten weiter an :
| MQCPI034 ....8.7.20.2(1414)
| MQCPI035 ....verwendet MQ-Protokolle
| MQCPI078 Route 1414 für Verbindungsanforderungen bereit.
```

5. Konfigurieren Sie MQIPT2.

Ändern Sie die Datei **mqipt.conf**, indem Sie zwei Routendefinitionen hinzufügen:

```
[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. Starten Sie MQIPT2.

Öffnen Sie ein Befehlseingabefenster, und geben Sie Folgendes ein:

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

Die folgenden Nachrichten weisen auf eine erfolgreiche Ausführung hin:

```
|
| 5639-L92 (C) Copyright IBM Corp. 2000, 2003 Alle Rechte vorbehalten.
| MQCPI001 WebSphere MQ Internet Pass-Thru Version 1.3.0 wird gestartet.
| MQCPI004 Die Konfigurationsdaten aus C:\mqipt\mqipt.conf werden gelesen.
| MQCPI011 Die Protokolldateien werden im Pfad C:\mqipt\logs gespeichert.
| MQCPI006 Route 1415 wurde gestartet und leitet Nachrichten weiter an :
| MQCPI034 ....9.10.6.7(1414)
| MQCPI035 ....verwendet MQ-Protokolle
| MQCPI052 ....Socks-Serverseite aktiviert
| MQCPI078 Route 1415 für Verbindungsanforderungen bereit.
| MQCPI006 Route 1414 wurde gestartet und leitet Nachrichten weiter an :
| MQCPI034 ....10.9.1.2(1414)
| MQCPI035 ....verwendet MQ-Protokolle
| MQCPI078 Route 1414 für Verbindungsanforderungen bereit.
```

7. Geben Sie an einer Eingabeaufforderung auf der ersten WebSphere MQ-Clientmaschine (8.7.20.1) Folgendes ein:

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

8. Reihen Sie eine Nachricht wie folgt ein:

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

9. Geben Sie an einer Eingabeaufforderung auf der zweiten WebSphere MQ-Clientmaschine (10.9.1.3) Folgendes ein:

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

10. Rufen Sie an der zweiten WebSphere MQ-Clientmaschine die Nachricht wie folgt ab:

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

Es wird "Hello world" angezeigt.

Eine Schlüsselringdatei erstellen

In diesem Beispiel wird davon ausgegangen, dass Sie unter Verwendung von KeyMan ein neues Zertifikat von einer vertrauenswürdigen Zertifizierungsstelle angefordert haben, und Ihr privates Zertifikat in einer Datei (z. B. **server.cer**) an Sie zurückgegeben wurde. Dies ist ausreichend für eine Serverauthentifizierung. Wenn Sie eine Clientauthentifizierung wünschen, müssen Sie ein zweites Zertifikat (z. B. **client.cer**) anfordern und die folgenden Schritte zweimal ausführen, um zwei Schlüsselringdateien zu erstellen.

1. Starten Sie KeyMan.
2. Wählen Sie **Create new...** (Neu...) aus.
3. Wählen Sie **PKCS#12 Token** (PKCS#12-Token) aus.
4. Wählen Sie **Action -> Generate Key** (Aktion -> Schlüssel erstellen) aus.
In der Liste **RSA / 1024-bit** wird ein neues Schlüsselpaar angezeigt.
5. Wählen Sie das neue Schlüsselpaar aus.
6. Wählen Sie **Action -> Request Certificate** (Aktion -> Zertifikat anfordern) aus.
Gehen Sie anhand der Anweisungen am Bildschirm vor.
7. Wählen Sie **File -> Save** (Datei -> Speichern) aus.
8. Geben Sie das Kennwort ein.
9. Geben Sie einen Namen für die neue Schlüsselringdatei ein.
Beispiel: **c:\mqipt\ssl\myServer.pfx**.
10. Als Dateiformat wird **PKCS#12 / PFX** beibehalten; die Option **Wrap key ring into a Java class** (Schlüsselring in Java-Klasse einbetten) darf **nicht** aktiviert werden.
11. Wählen Sie **File -> Exit** (Datei -> Beenden) aus.
12. Erstellen Sie eine Textdatei, die die oben verwendete Passphrase (myPass-Word) enthält.
Beispiel: **c:\mqipt\ssl\myServer.pwd**.

Wenn Sie das Zertifikat wieder erhalten, öffnen Sie die ursprüngliche Schlüsselringdatei (myServer.pfx). Gehen Sie dann wie folgt vor:

1. Starten Sie KeyMan.
2. Wählen Sie **Open existing...** (Öffnen...) aus..
3. Wählen Sie **Local Resource** (Lokale Ressource) aus.
4. Wählen Sie **Open a file...** (Datei öffnen...) aus.
5. Geben Sie den Namen der privaten Zertifikatdatei ein.
Beispiel: **c:\mqipt\ssl\myServer.pfx**.
6. Geben Sie die Passphrase ein.
7. Wählen Sie **File -> Import** (Datei -> Importieren) aus.
8. Wählen Sie **Local Resource** (Lokale Ressource) aus.
9. Wählen Sie **Open a file...** (Datei öffnen...) aus.
10. Geben Sie **server.cer** ein.
In einem Dialogfenster werden Sie darauf hingewiesen, dass das private Zertifikat mit dem Schlüssel verknüpft wird.
11. Wählen Sie **File -> Save** (Datei -> Speichern) aus.
12. Wählen Sie **File -> Exit** (Datei -> Beenden) aus.

Wiederholen Sie diese Schritte, um ein **myClient.pfx** auf Basis der Datei **client.cer** zu erstellen. Überprüfen Sie mit Hilfe von KeyMan den Inhalt der CA-Beispiel-schlüsselringdatei (**sslCAdefault.pfx**), um festzustellen, ob Ihre privaten Zertifikate von einer der aufgeführten Zertifizierungsstellen signiert wurden. Ist dies der Fall, können Sie die mitgelieferte CA-Schlüsselringdatei verwenden. Ist dies nicht der Fall, müssen Sie eine Schlüsselringdatei erstellen, die das öffentliche CA-Zertifikat enthält, von dem Ihre privaten Zertifikate signiert wurden. Dieses CA-Zertifikat wurde unter Umständen zusammen mit Ihrem privaten Zertifikat zurückgegeben. Ist dies nicht der Fall, müssen Sie das CA-Zertifikat von derselben Zertifizierungsstelle anfordern, von der Sie Ihr privates Zertifikat erhalten haben, und dieses CA-Zertifikat in die Datei **sslCAdefault.pfx** importieren. Die CA-Schlüsselringdatei kann sowohl auf der Client- als auch auf der Serverseite verwendet werden. Hinweise zur Verwendung dieser neuen Schlüsselringdateien für die Serverauthentifizierung finden Sie unter der Beispielkonfiguration „SSL-Serverauthentifizierung“ auf Seite 100; außerdem müssen die folgenden Routeneigenschaften gesetzt werden:

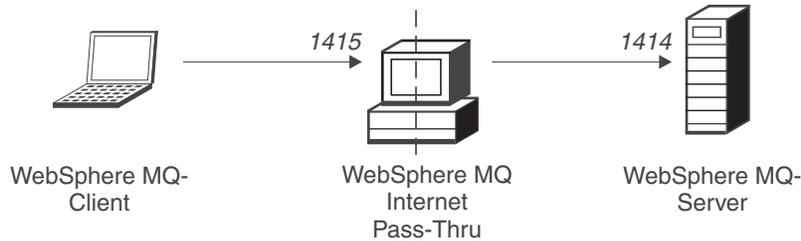
```
SSLClientCAKeyRing=c:\mqipt\ssl\sslCAdefault.pfx
SSLClientCAKeyRingPW=c:\mqipt\ssl\sslCAdefault.pwd
SSLServerKeyRing=c:\mqipt\ssl\myServer.pfx
SSLServerKeyRingPW=c:\mqipt\ssl\myServer.pwd
SSLServerCAKeyRing=c:\mqipt\ssl\sslCAdefault.pfx
SSLServerCAKeyRingPW=c:\mqipt\ssl\sslCAdefault.pwd
```

Hinweise zur Verwendung dieser neuen Schlüsselringdateien für die Client- und Serverauthentifizierung finden Sie unter der Beispielkonfiguration „SSL-Clientauthentifizierung“ auf Seite 102; außerdem müssen die folgenden Routeneigenschaften gesetzt werden:

```
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
```

Port-Adressen zuordnen

Dieses Beispiel zeigt, wie die lokalen Port-Adressen, die zum Herstellen abgehender Verbindungen verwendet werden, gesteuert werden. Das Beispiel geht davon aus, dass MQIPT auf einem Multihomed-System installiert wurde.



client1.company1.com

8.7.20.5 9.10.6.7

server1.company2.com

Abbildung 32. Netzplan für Port-Zuordnung

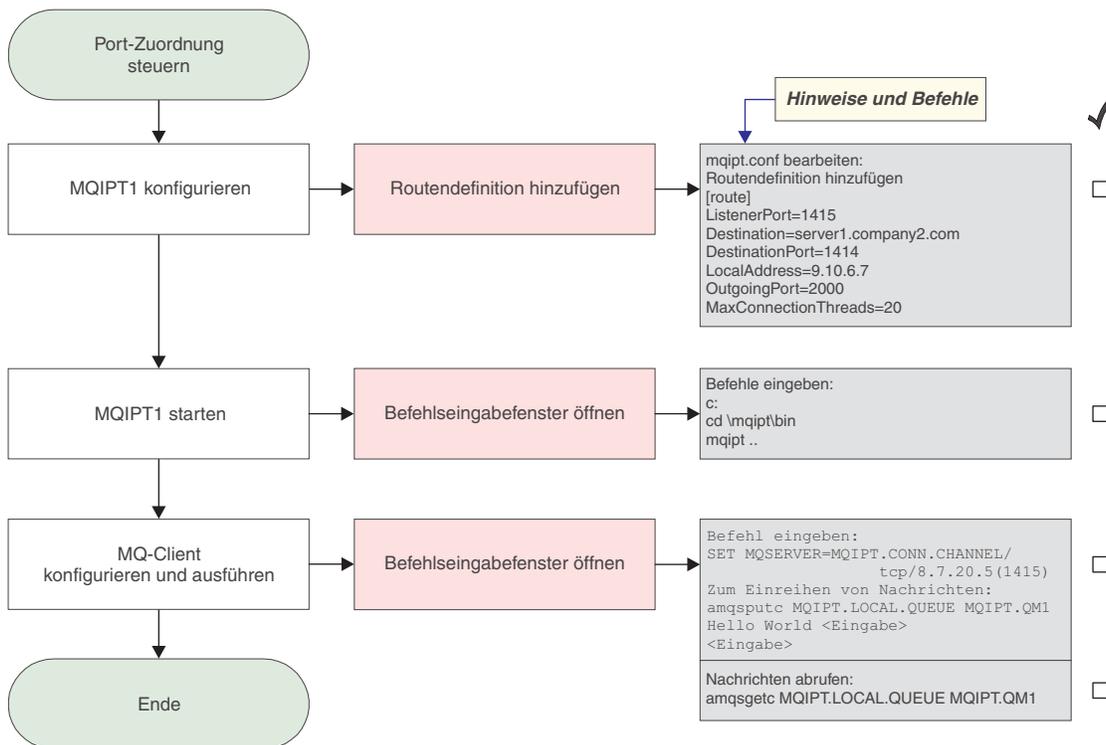


Abbildung 33. Konfiguration für Port-Zuordnung

1. Konfigurieren Sie MQIPT1.

Ändern Sie die Datei **mqipt.conf**, indem Sie eine Routendefinition hinzufügen:

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

2. Starten Sie MQIPT1.

Öffnen Sie ein Befehlseingabefenster, und geben Sie Folgendes ein:

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

Die folgenden Nachrichten weisen auf eine erfolgreiche Ausführung hin:

```
| 5639-L92 (C) Copyright IBM Corp. 2000, 2003 Alle Rechte vorbehalten.
| MQCPI001 WebSphere MQ Internet Pass-Thru Version 1.3.0 wird gestartet.
| MQCPI004 Die Konfigurationsdaten aus C:\mqipt\mqipt.conf werden gelesen.
| MQCPI011 Die Protokolldateien werden im Pfad C:\mqipt\logs gespeichert.
| MQCPI006 Route 1415 wurde gestartet und leitet Nachrichten weiter an :
| MQCPI034 ....server1.company2.com(1414)
| MQCPI035 ....verwendet MQ-Protokolle
| MQCPI069 ....Bindung an lokale Adresse 9.10.6.7
| MQCPI070 ....Verwendung des Bereichs 2000-2019 für lokale Port-Adresse
| MQCPI078 Route 1415 für Verbindungsanforderungen bereit.
```

3. Geben Sie an einer Eingabeaufforderung auf der WebSphere MQ-Clientmaschine Folgendes ein:

```
SET MQSERVER=MQIPT.CONN.CHANNEL/tcp/8.7.20.5(1415)
```

4. Reihnen Sie eine Nachricht wie folgt ein:

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

5. Rufen Sie die Nachricht wie folgt ab:

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

Es wird "Hello world" angezeigt.

LDAP-Server verwenden

Dieses Beispiel zeigt, wie MQIPT für die Verwendung eines LDAP-Servers zum Abrufen von Zertifikatwiderrufslisten (Certificate Revocation Lists, CRLs) konfiguriert wird. In diesem Beispiel wird nicht gezeigt, wie ein LDAP-Server installiert und konfiguriert oder wie eine Schlüsselringdatei mit privaten oder vertrauenswürdigen Zertifikaten erstellt wird. Das Beispiel geht davon aus, dass der LDAP-Server von einer bekannten und vertrauenswürdigen Zertifizierungsstelle (Certificate Authority, CA) zur Verfügung gestellt wird. Es wird kein LDAP-Ausweichserver verwendet, der jedoch einfach implementiert werden kann, indem die entsprechende Routeneigenschaft hinzugefügt wird.

Bei diesem Beispiel wird von Folgendem ausgegangen:

- IPT2 hat ein privates Zertifikat, das von der vertrauenswürdigen CA ausgestellt wurde, in der Schlüsselringdatei 'myCert.pfx' gespeichert, und das verschlüsselte Kennwort zum Öffnen der Schlüsselringdatei ist in der Datei 'myCert.pwd' gespeichert.
- IPT1 besitzt eine Kopie des vertrauenswürdigen CA-Zertifikats, das zur Authentifizierung des von IPT2 gesendeten Zertifikats verwendet wird. Dieses Zertifikat ist in der Schlüsselringdatei 'caCerts.pfx' und das verschlüsselte Kennwort zum Öffnen der Schlüsselringdatei in der Datei 'caCerts.pwd' gespeichert.
- Die verschlüsselten Kennwortdateien wurden mit dem Script 'mqiptPW' erstellt.

Indem der WMQ-Client dieses Beispiel ausführt, kann er eine Verbindung mit dem Warteschlangenmanager (QM) herstellen und eine WMQ-Nachricht in die Zielwarteschlange einreihen. Bei Ausführung eines MQIPT-Trace für IPT1 wird der verwendete LDAP-Server angezeigt, um zu veranschaulichen, wie CRLs funktionieren. Das von IPT3 verwendete private Zertifikat muss von der vertrauenswürdigen CA widerrufen werden. In diesem Fall kann der WMQ-Client dann keine Verbindung mit dem WS-Manager herstellen, weil die Verbindung zwischen IPT1 und IPT2 zurückgewiesen wird.

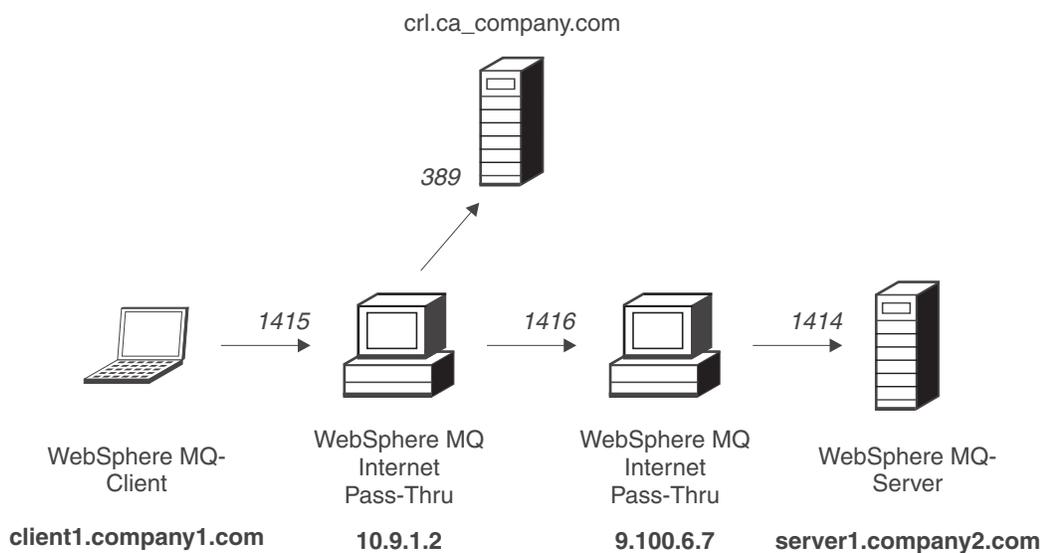


Abbildung 34. Netzplan für LDAP-Server

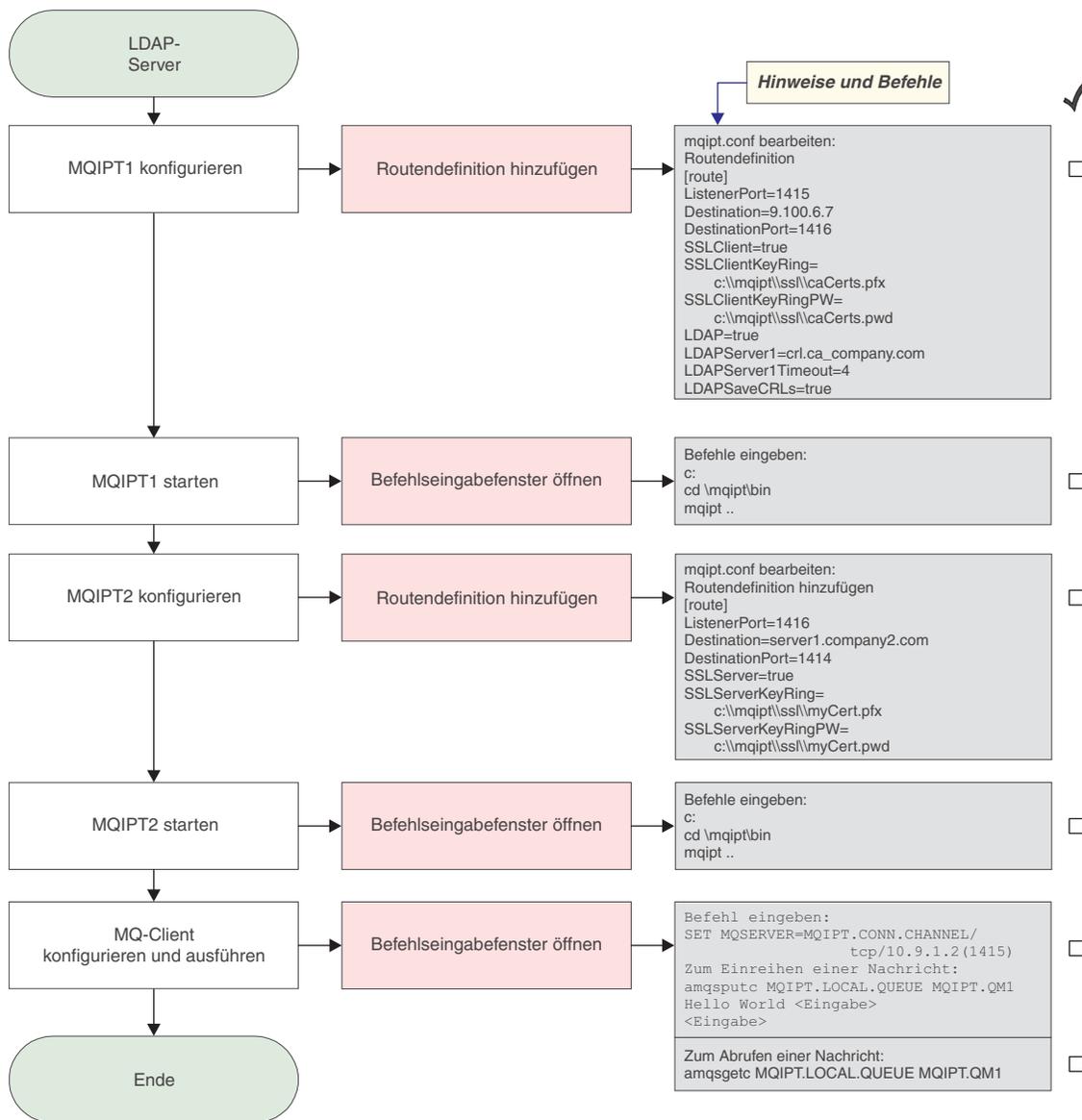


Abbildung 35. Konfiguration für LDAP-Server

1. Auf IPT1

Ändern Sie die Datei `mqipt.conf`, indem Sie eine Routendefinition hinzufügen:

```
[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
```

Öffnen Sie ein Befehlseingabefenster:

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

Die folgenden Nachrichten weisen auf eine erfolgreiche Ausführung hin:

```
5639-L92 (C) Copyright IBM Corp. 2000, 2003 Alle Rechte vorbehalten.
MQCPI001 WebSphere MQ Internet Pass-Thru Version 1.3.0 wird gestartet.
MQCPI004 Die Konfigurationsdaten aus C:\mqipt\mqipt.conf werden gelesen.
MQCPI011 Die Protokolldateien werden im Pfad C:\mqipt\logs gespeichert.
MQCPI006 Route 1415 wurde gestartet und leitet Nachrichten weiter an :
MQCPI034 ....9.100.6.7(1416)
MQCPI035 ....verwendet MQ-Protokolle
MQCPI036 ....SSL-Clientseite mit folgenden Eigenschaften aktiviert :
MQCPI031 .....Cipher Suites <NULL>
MQCPI032 .....Schlüsselringdatei <NULL>
MQCPI047 .....CA-Schlüsselringdatei c:\mqipt\ssl\caCerts.pfx
MQCPI071 .....Sitezertifikat verwendet CN=* O=* OU=* L=* ST=* C=*
MQCPI038 .....Peer-Zertifikat verwendet CN=* O=* OU=* L=* ST=* C=*
MQCPI075 ....LDAP-Hauptserver an crl.ca_company.com(389)
MQCPI086 .....Zeitlimit: 4 Sekunde(n)
MQCPI084 ....Gültigkeitsdauer für CRL im Cache beträgt 1 Stunde(n).
MQCPI085 ....CRLs werden in Schlüsselringdatei(en) gespeichert.
MQCPI078 Route 1415 für Verbindungsanforderungen bereit.
```

2. Auf IPT2

Ändern Sie die Datei **mqipt.conf**, indem Sie eine Routendefinition hinzufügen:

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

Öffnen Sie ein Befehlseingabefenster:

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

Die folgenden Nachrichten weisen auf eine erfolgreiche Ausführung hin:

```
5639-L92 (C) Copyright IBM Corp. 2000, 2003 Alle Rechte vorbehalten.
MQCPI001 IBM WebSphere MQ Internet Pass-Thru Version 1.3.0 wird gestartet.
MQCPI004 Die Konfigurationsdaten aus C:\mqipt\mqipt.conf werden gelesen.
MQCPI011 Die Protokolldateien werden im Pfad C:\mqipt\logs gespeichert.
MQCPI006 Route 1416 wird gestartet und leitet Nachrichten weiter an :
MQCPI034 ....server1.company2.com(1414)
MQCPI035 ....verwendet MQ-Protokolle
MQCPI037 ....SSL-Serverseite mit folgenden Eigenschaften aktiviert:
MQCPI031 .....Cipher Suites <NULL>
MQCPI032 .....Schlüsselringdatei c:\mqipt\ssl\myCert.pfx
MQCPI047 .....CA-Schlüsselringdatei <NULL>
MQCPI071 .....Sitezertifikat verwendet CN=* O=* OU=* L=* ST=* C=*
MQCPI038 .....Peer-Zertifikat verwendet CN=* O=* OU=* L=* ST=* C=*
MQCPI033 .....Clientauthentifizierung ist auf false gesetzt
MQCPI078 Route 1416 für Verbindungsanforderungen bereit.
```

- Geben Sie an einer Eingabeaufforderung auf der WebSphere MQ-Clientmaschine Folgendes ein:

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

- Reihen Sie eine Nachricht wie folgt ein:

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

- Rufen Sie die Nachricht wie folgt ab:

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

Es wird "Hello world" angezeigt.

SSL-Proxy-Modus

Dieses Beispiel zeigt, wie MQIPT im SSL-Proxy-Modus ausgeführt wird, so dass es SSL-Verbindungsanforderungen von einem SSL-Client akzeptiert und im Tunnelungsverfahren an einen SSL-Server weiterleitet. Das Beispiel geht davon aus, dass WMQ-Client und -Server die Version 5.3 haben und für die Verwendung einer SSL-Verbindung konfiguriert wurden.

Weitere Informationen zur Konfiguration von SSL für WMQ finden Sie im Handbuch "WebSphere MQ Sicherheit Version 5.3", SC12-3103-01.

Bei diesem Beispiel wird von Folgendem ausgegangen:

- MQ-Client und WS-Manager wurden für die Verwendung eines SSL-Kanals konfiguriert.

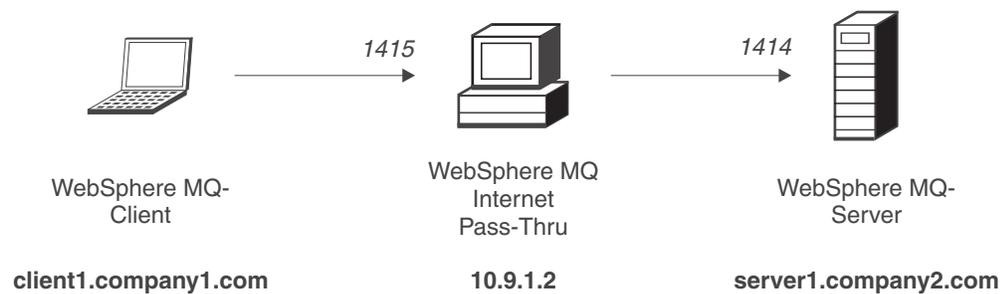


Abbildung 36. Netzplan für SSL-Proxy-Modus

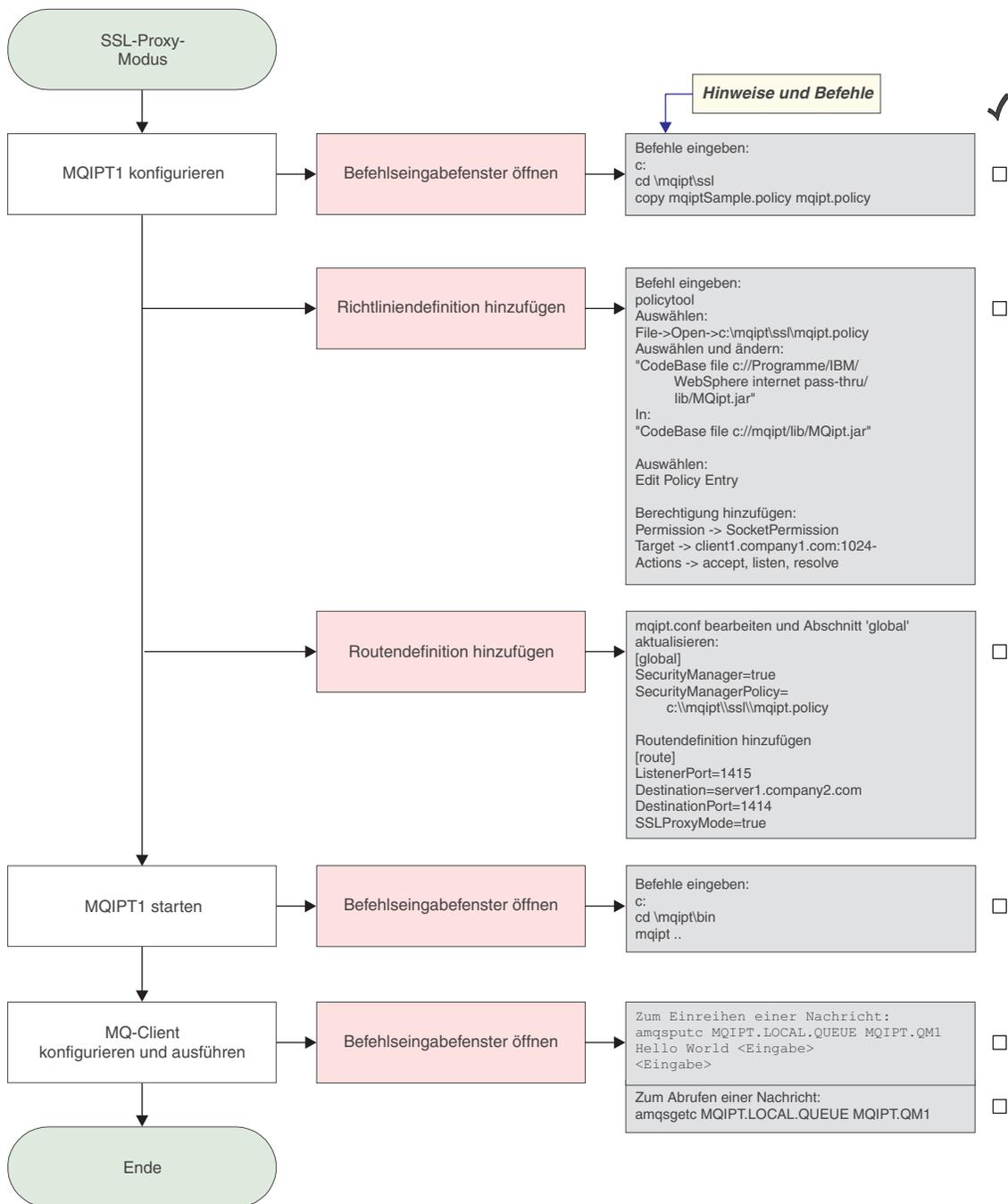


Abbildung 37. Konfiguration für SSL-Proxy-Modus

1. Auf IPT1

a. Öffnen Sie ein Befehlseingabefenster, und geben Sie Folgendes ein:

`copy c:\mqipt\ssl\mqiptSample.policy to mqipt.policy`

b. Fügen Sie mit dem folgenden Befehl eine Richtliniendefinition hinzu:

`policytool`

1) Wählen Sie **File** → **Open** → **c:\mqipt\ssl\mqipt.policy** (Datei → Öffnen -> c:\mqipt\ssl\mqipt.policy).

```

|
|           2) Wählen Sie:
|           "file:///C:/Programme/IBM/WebSphere MQ internet pass-thru/lib/MQipt.jar"
|
|           3) Ändern Sie die Codebasis von:
|           "file:///C:/Programme/IBM/WebSphere MQ internet pass-thru/lib/MQipt.jar"
|
|           in:
|           "file:///C:/mqipt/lib/MQipt.jar"
|
|           4) Ändern Sie alle Berechtigungen von:
|           "C:\\Programme\\IBM\\WebSphere MQ internet pass-thru"
|
|           in:
|           "C:\\mqipt"
|
|           5) Fügen Sie die Socket-Berechtigung hinzu:
|           Permission=SocketPermission
|           Target = "client1.company1.com:1024-"
|           Actions = "accept, listen, resolve"
|
| 2. Fügen Sie in der Datei mqipt.conf die folgenden beiden Eigenschaften zum globalen
| Abschnitt sowie eine Routendefinition hinzu:
|
| [global]
| SecurityManager=true
| SecurityManagerPolicy=c:\\mqipt\\ssl\\mqipt.policy
| [route]
| ListenerPort=1415
| Destination=server1.company2.com
| DestinationPort=1414
| SSLProxyMode=true
|
| 3. Öffnen Sie ein Befehlseingabefenster:
|
| c:
| cd \\mqipt\\bin
| mqipt ..
|
|
| Die folgenden Nachrichten weisen auf eine erfolgreiche Ausführung hin:
|
| 5639-L92 (C) Copyright IBM Corp. 2000, 2003 Alle Rechte vorbehalten.
| MQCPI001 WebSphere MQ Internet Pass-Thru Version 1.3.0 wird gestartet.
| MQCPI004 Die Konfigurationsdaten aus C:\\mqipt\\mqipt.conf werden gelesen.
| MQCPI011 Die Protokolldateien werden im Pfad C:\\mqipt\\logs gespeichert.
| MQCPI006 Route 1415 wurde gestartet und leitet Nachrichten weiter an :
| MQCPI034 ....server1.company2.com(1414)
| MQCPI035 ....verwendet SSL-Proxy-Modus
| MQCPI078 Route 1415 für Verbindungsanforderungen bereit.
|
| 4. Reihnen Sie eine Nachricht wie folgt ein:
|
| amqsputc MQIPT.LOCAL.QUEUE MQIPT.QM1
| Hello world <Eingabe>
| <Eingabe>
|
| 5. Rufen Sie die Nachricht wie folgt ab:
|
| amqsgetc MQIPT.LOCAL.QUEUE MQIPT.QM1
|
|
| Es wird "Hello world" angezeigt.

```

Apache-Anweisung 'rewrite'

Bei diesem Beispiel wird von Folgendem ausgegangen:

- Der Apache HTTP-Server wurde im Verzeichnis 'c:\apache' installiert.
- IBM Web Traffic Express wurde im Verzeichnis 'c:\wte' installiert.

Das Beispiel zeigt, wie mit der Anweisung 'rewrite' eine HTTP-Anforderung in eine Apache-Proxy-Umleitung konvertiert wird. Die Proxy- und Rewrite-Module müssen geladen werden, aber da Apache nicht wirklich im Proxy-Modus arbeitet, können alle Proxy-Anweisungen weiter auf Kommentar gesetzt sein.

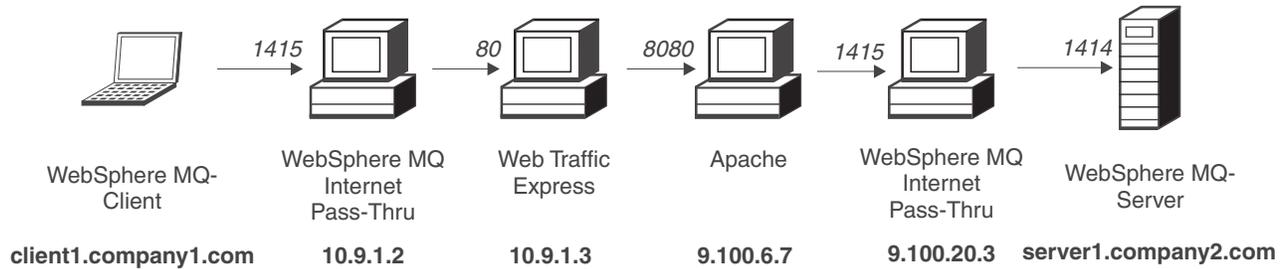


Abbildung 38. Netzplan für Apache-Anweisung 'rewrite'

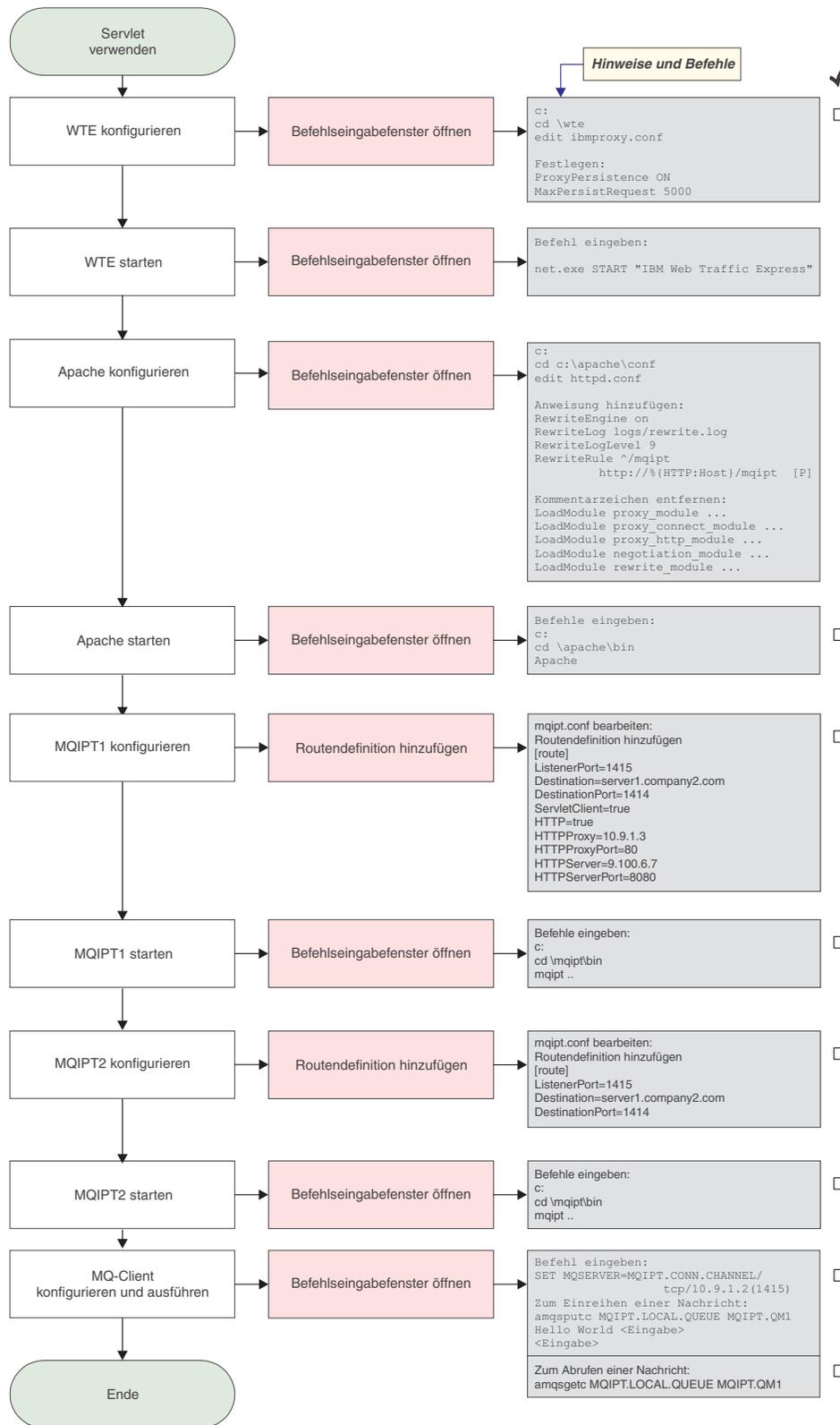


Abbildung 39. Konfiguration für Apache-Anweisung 'rewrite'

1. Auf WTE

Bearbeiten Sie die Datei c:\wte\ibmroxy.conf.

Ändern Sie folgende Eigenschaften:

```
ProxyPersistence ON
MaxPersistRequest 5000
```

2. Auf Apache

Bearbeiten Sie die Datei 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. Auf IPT1

Ändern Sie die Datei **mqipt.conf**, indem Sie eine Routendefinition hinzufügen:

```
[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
```

Öffnen Sie ein Befehlseingabefenster:

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

Die folgenden Nachrichten weisen auf eine erfolgreiche Ausführung hin:

```
5639-L92 (C) Copyright IBM Corp. 2000, 2003 Alle Rechte vorbehalten.
MQCPI001 WebSphere MQ Internet Pass-Thru Version 1.3.0 wird gestartet.
MQCPI004 Die Konfigurationsdaten aus C:\mqipt\mqipt.conf werden gelesen.
MQCPI011 Die Protokolldateien werden im Pfad C:\mqipt\logs gespeichert.
MQCPI006 Route 1415 wurde gestartet und leitet Nachrichten weiter an :
MQCPI034 ....server1.company2.com(1414)
MQCPI035 ....verwendet HTTP
MQCPI024 ....und HTTP-Proxy an 10.9.1.3(80)
MQCPI066 ....und HTTP-Server an 9.100.6.7(8080)
MQCPI078 Route 1415 für Verbindungsanforderungen bereit.
```

4. Auf IPT2

Ändern Sie die Datei **mqipt.conf**, indem Sie eine Routendefinition hinzufügen:

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

Öffnen Sie ein Befehlseingabefenster:

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

Die folgenden Nachrichten weisen auf eine erfolgreiche Ausführung hin:

```
5639-L92 (C) Copyright IBM Corp. 2000, 2003 Alle Rechte vorbehalten.  
MQCPI001 WebSphere MQ Internet Pass-Thru Version 1.3.0 wird gestartet.  
MQCPI004 Die Konfigurationsdaten aus C:\mqipt\mqipt.conf werden gelesen.  
MQCPI011 Die Protokolldateien werden im Pfad C:\mqipt\logs gespeichert.  
MQCPI006 Route 1415 wurde gestartet und leitet Nachrichten weiter an :  
MQCPI034 ....server1.company2.com(1414)  
MQCPI035 ....verwendet MQ-Protokolle  
MQCPI078 Route 1415 für Verbindungsanforderungen bereit.
```

5. Geben Sie an einer Eingabeaufforderung auf der WebSphere MQ-Clientmaschine Folgendes ein:

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

6. Reihnen Sie eine Nachricht wie folgt ein:

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

7. Rufen Sie die Nachricht wie folgt ab:

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

Es wird "Hello world" angezeigt.

Sicherheitsexit

Bei diesem Beispiel wird von Folgendem ausgegangen:

- Java 1.4 SDK ist installiert.
- Das Java-Unterverzeichnis 'bin' wurde zur Umgebungsvariablen PATH hinzugefügt.

Dieser einfache Test zeigt, wie der mitgelieferte Beispielsicherheitsexit SampleSecurityExit verwendet wird. Dieser Sicherheitsexit lässt nur Clientverbindungen über einen Kanal zu, dessen Name mit "MQIPT" beginnt.

Wenn Sie den vorgeschlagenen srvconn-Kanalnamen "MQIPT.CONN.CHANNEL" verwenden (wie in den meisten dieser Beispiele), wird die Clientverbindung erfolgreich hergestellt und eine WMQ-Nachricht in die Warteschlange eingereicht.

Sie können prüfen, ob der Sicherheitsexit wie erwartet funktioniert, indem Sie einen anderen srvconn-Kanal mit einem beliebigen Namen, der nicht mit "MQIPT" beginnt, definieren (z. B. TEST.CONN.CHANNEL) und den Befehl 'amqsputc' erneut ausgeben, nachdem Sie in der Umgebungsvariablen MQSERVER den neuen Kanalnamen angegeben haben. Dieses Mal wird die Verbindung zurückgewiesen und der Fehler 2059 ausgegeben.

Zeigen Sie, dass "TEST.CONN.CHANNEL" ohne den Sicherheitsexit funktioniert, indem Sie die Umgebungsvariable MQSERVER ändern, so dass sie direkt auf den WMQ-Listener-Port (z. B. 1414) zeigt, d. h., MQIPT wird nicht verwendet. Dieses Mal funktioniert der Befehl 'amqsputc' wie erwartet.

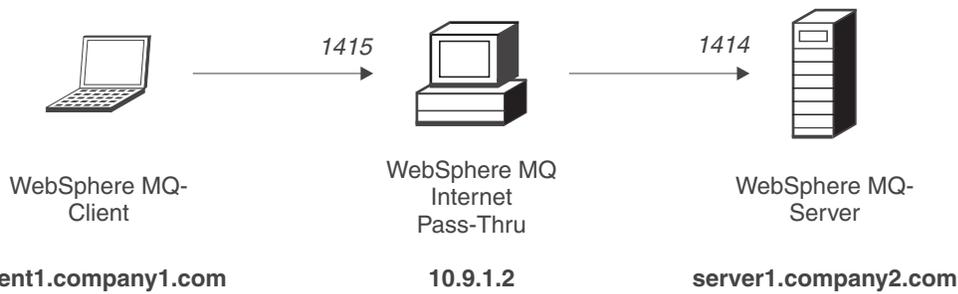


Abbildung 40. Netzplan für Sicherheitsexit

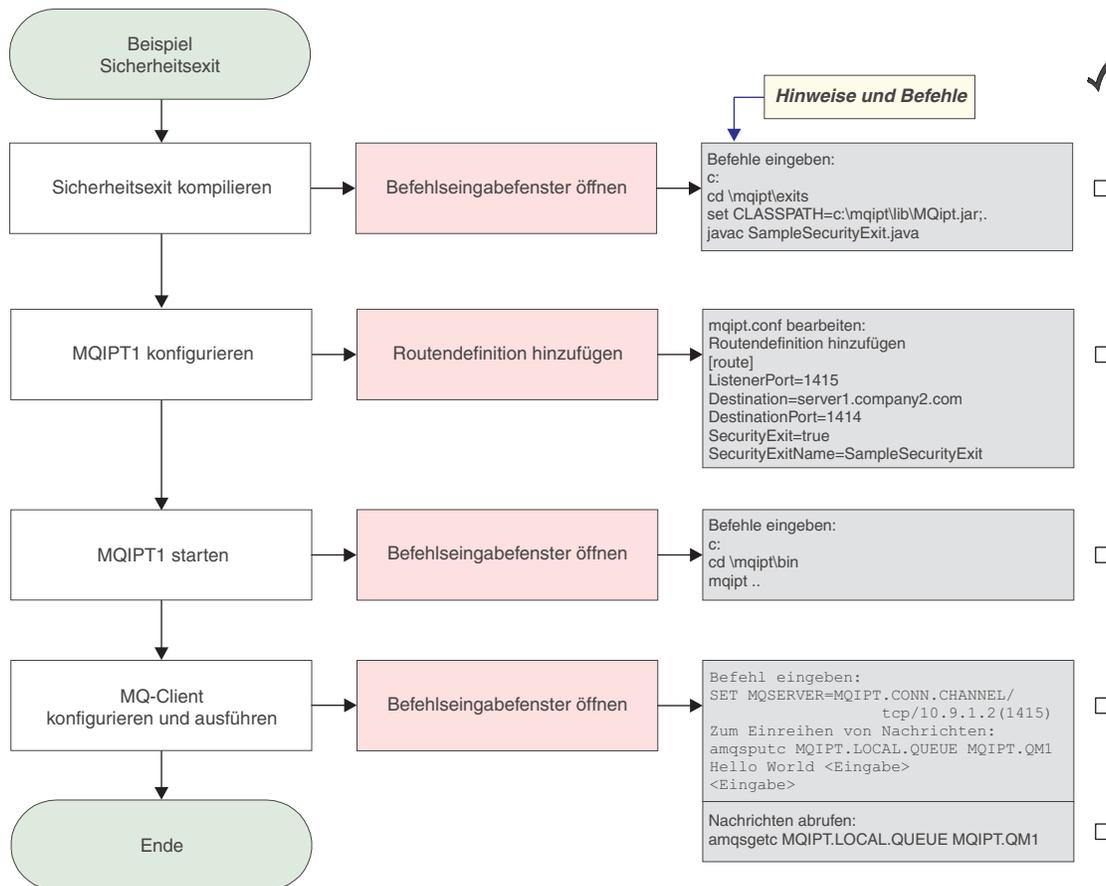


Abbildung 41. Konfiguration für Sicherheitsexit

1. Auf IPT1

Öffnen Sie ein Befehlseingabefenster:

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

Ändern Sie die Datei **mqipt.conf**, indem Sie eine Routendefinition hinzufügen:

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

Öffnen Sie ein Befehlseingabefenster:

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

Die folgenden Nachrichten weisen auf eine erfolgreiche Ausführung hin:

```
5639-L92 (C) Copyright IBM Corp. 2000, 2003 Alle Rechte vorbehalten.
MQCPI001 WebSphere MQ Internet Pass-Thru Version 1.3.0 wird gestartet.
MQCPI004 Die Konfigurationsdaten aus c:\mqipt\mqipt.conf werden gelesen.
MQCPI011 Die Protokolldateien werden im Pfad c:\mqipt\logs gespeichert.
MQCPI006 Route 1415 wurde gestartet und leitet Nachrichten weiter an :
MQCPI034 ....server1.company2.com(1414)
MQCPI035 ....verwendet MQ-Protokolle
MQCPI079 ....verwendet Sicherheitsexit c:\mqipt\exits\SampleSecurityExit
MQCPI080 .....und ein Zeitlimit von 5 Sekunden
MQCPI078 Route 1415 für Verbindungsanforderungen bereit.
```

2. Geben Sie an einer Eingabeaufforderung auf der WebSphere MQ-Clientmaschine Folgendes ein:

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

3. Reihnen Sie eine Nachricht wie folgt ein:

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

4. Rufen Sie die Nachricht wie folgt ab:

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

Es wird "Hello world" angezeigt.

Sicherheitsexit weiterleiten

Bei diesem Beispiel wird von Folgendem ausgegangen:

- Java 1.4 SDK ist installiert.
- Das Java-Unterverzeichnis 'bin' wurde zur Umgebungsvariablen PATH hinzugefügt.
- Auf drei separaten Servern wurden drei identische WS-Manager erstellt.

Dies ist ein ausführbares Beispiel, mit dem Clientverbindungsanforderungen in einem Round-Robin-Verfahren dynamisch an eine Servergruppe mit WMQ-Warteschlangenmanagern weitergeleitet werden. Bei den WS-Managern auf den einzelnen Servern der Gruppe handelt es sich um Spiegelbilder.

Die Liste der Servernamen wird aus einer Konfigurationsdatei gelesen. Name und Verzeichnis der Konfigurationsdatei werden in den Eigenschaften SecurityExit-Name und SecurityExitPath definiert.

Die Beispielkonfigurationsdatei 'SampleRoutingExit.conf' enthält folgende Einträge:

```

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

```

Sie müssen diese Servernamen an Ihre Umgebung anpassen.

Bei der ersten Ausgabe des Befehls 'amqspc' wird die WMQ-Nachricht in die Warteschlange MQIPT.LOCAL.QUEUE auf dem WS-Manager (QM) auf Server1 eingereicht. Beim zweiten Mal wird die Nachricht an den WS-Manager auf Server2 übergeben, usw. Bei Verwendung dieser Konfiguration ist es nicht möglich, die gerade eingereichte Nachricht mit dem Befehl 'amqsget' abzurufen, weil die vom Befehl verwendete Clientverbindungsanforderung an den nächsten WS-Manager in der Liste übergeben wird. Indem dreimal der Befehl 'amqspc' und anschließend dreimal der Befehl 'amqsget' ausgegeben wird, kann jedoch sichergestellt werden, dass die Nachrichten in derselben Reihenfolge abgerufen werden. Natürlich können Sie Nachrichten gezielt von einem der WS-Manager abrufen, indem Sie einen anderen WMQ-Client verwenden, der direkt mit einem WS-Manager verbunden ist (d. h., in diesem Beispiel wird nicht MQIPT verwendet).

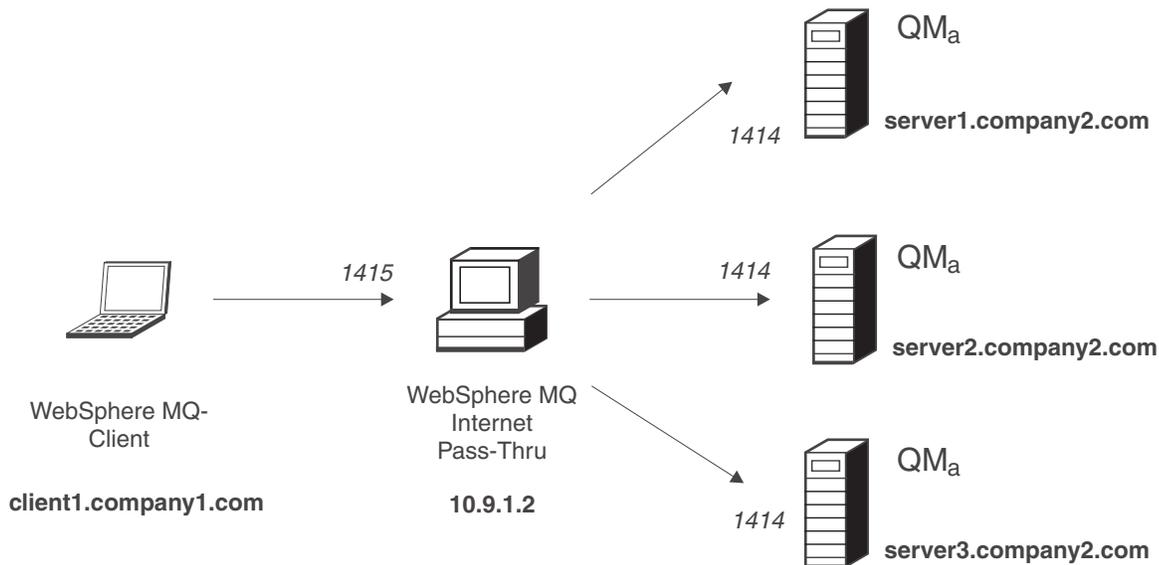


Abbildung 42. Netzplan für Sicherheitsexit-Weiterleitung

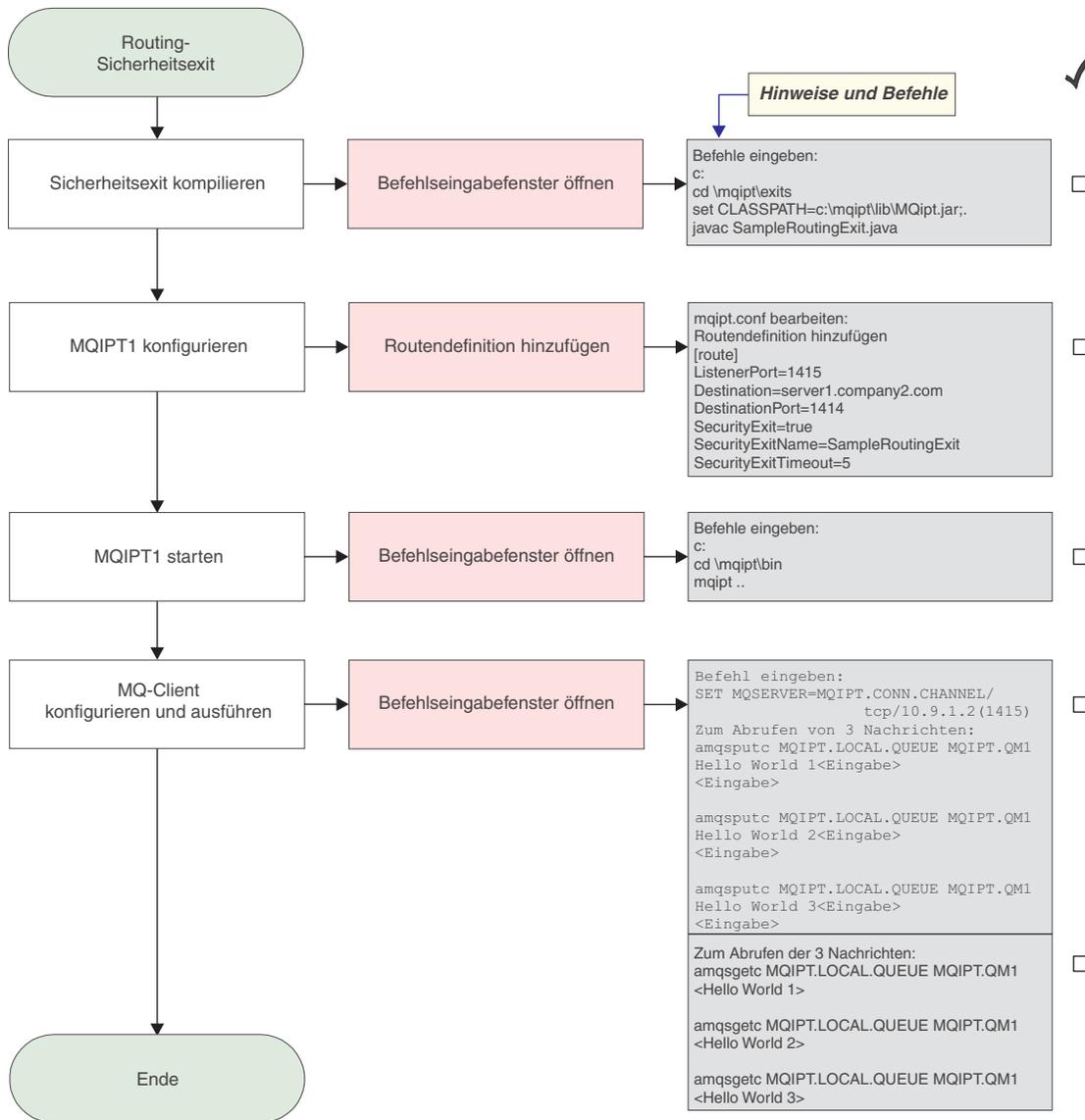


Abbildung 43. Konfiguration für Sicherheitsexit-Weiterleitung

|
| 1. Auf IPT1

| Öffnen Sie ein Befehlseingabefenster:

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

| Ändern Sie die Datei **mqipt.conf**, indem Sie eine Routendefinition hinzufügen:

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

| Öffnen Sie ein Befehlseingabefenster:

| c:
| cd \mqipt\bin
| mqipt ..

| Die folgenden Nachrichten weisen auf eine erfolgreiche Ausführung hin:

| 5639-L92 (C) Copyright IBM Corp. 2000, 2003 Alle Rechte vorbehalten.
| MQCPI001 WebSphere MQ Internet Pass-Thru Version 1.3.0 wird gestartet.
| MQCPI004 Die Konfigurationsdaten aus c:\mqipt\mqipt.conf werden gelesen.
| MQCPI011 Die Protokolldateien werden im Pfad c:\mqipt\logs gespeichert.
| MQCPI006 Route 1415 wurde gestartet und leitet Nachrichten weiter an :
| MQCPI034server1.company2.com(1414)
| MQCPI035verwendet MQ-Protokolle
| MQCPI079verwendet Sicherheitsexit c:\mqipt\exits\SampleRoutingExit
| MQCPI080und ein Zeitlimit von 5 Sekunden
| MQCPI078 Route 1415 für Verbindungsanforderungen bereit.

| 2. Geben Sie an einer Eingabeaufforderung auf der WebSphere MQ-Clientma-
| schine Folgendes ein:

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

| 3. Reihnen Sie drei Nachrichten wie folgt ein:

| amqsputc MQIPT.LOCAL.QUEUE MQIPT.QM1
| Hello world 1 <Eingabe>
| <Eingabe>
| amqsputc MQIPT.LOCAL.QUEUE MQIPT.QM1
| Hello world 2 <Eingabe>
| <Eingabe>
| amqsputc MQIPT.LOCAL.QUEUE MQIPT.QM1
| Hello world 3 <Eingabe>
| <Eingabe>

| 4. Rufen Sie die Nachrichten wie folgt ab:

| amqsgetc MQIPT.LOCAL.QUEUE MQIPT.QM1
| amqsgetc MQIPT.LOCAL.QUEUE MQIPT.QM1
| amqsgetc MQIPT.LOCAL.QUEUE MQIPT.QM1

| Es wird "Hello world 1", "Hello world 2" und "Hello world 3" angezeigt.

Dynamischer Exit bei nur einer Route

Bei diesem Beispiel wird von Folgendem ausgegangen:

- Java 1.4 SDK ist installiert.
- Das Java-Unterverzeichnis 'bin' wurde zur Umgebungsvariablen PATH hinzugefügt.
- Auf drei separaten Servern wurden drei unterschiedliche WS-Manager erstellt.

Dies ist ein ausführbares Beispiel, das zeigt, wie Clientverbindungsanforderungen dynamisch an einen Zielserver weitergeleitet werden, wobei der Name des verwendeten Kanals als Basis dient. Der erste Teil des Kanalnamens ist der Name des WS-Managers, z. B. QM1. Der Name eines svrconn-Kanals würde QM1.MQIPT.CONN.CHANNEL lauten. Bei Verwendung dieser Namenskonvention benötigt MQIPT nur eine einzige Route, um alle Verbindungsanforderungen zu bedienen.

Die Liste der WS-Manager- und Servernamen wird aus einer Konfigurationsdatei gelesen. Name und Verzeichnis der Konfigurationsdatei werden in den Eigenschaften SecurityExitName und SecurityExitPath definiert. Die Beispielkonfigurationsdatei 'SampleOneRouteExit.conf' enthält folgende Einträge:

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

Sie müssen diese Servernamen an Ihre Umgebung anpassen.

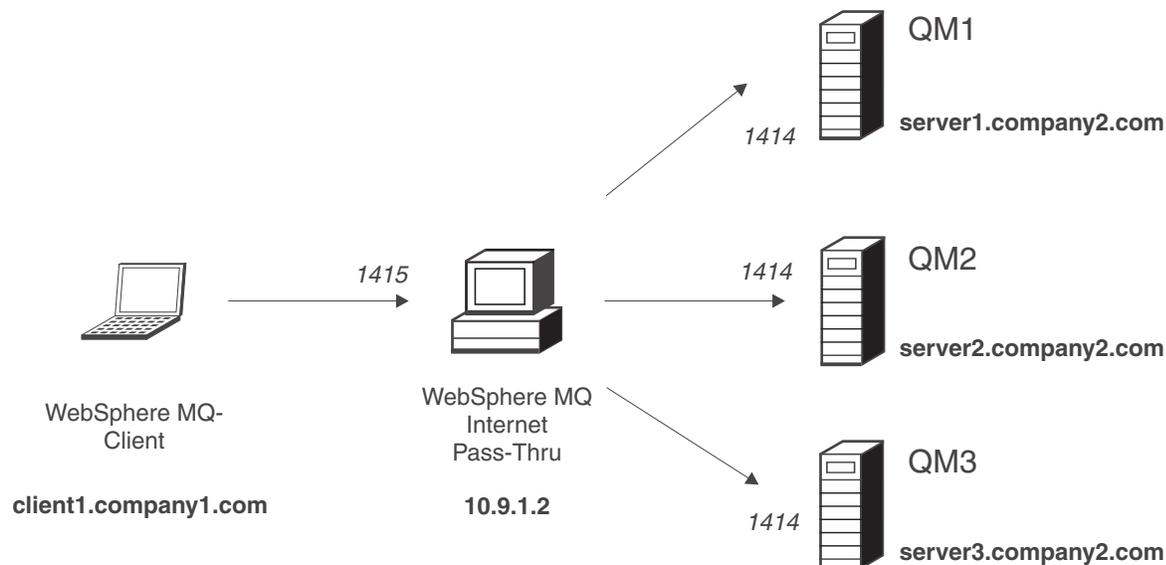


Abbildung 44. Netzplan für dynamischen Exit bei nur einer Route

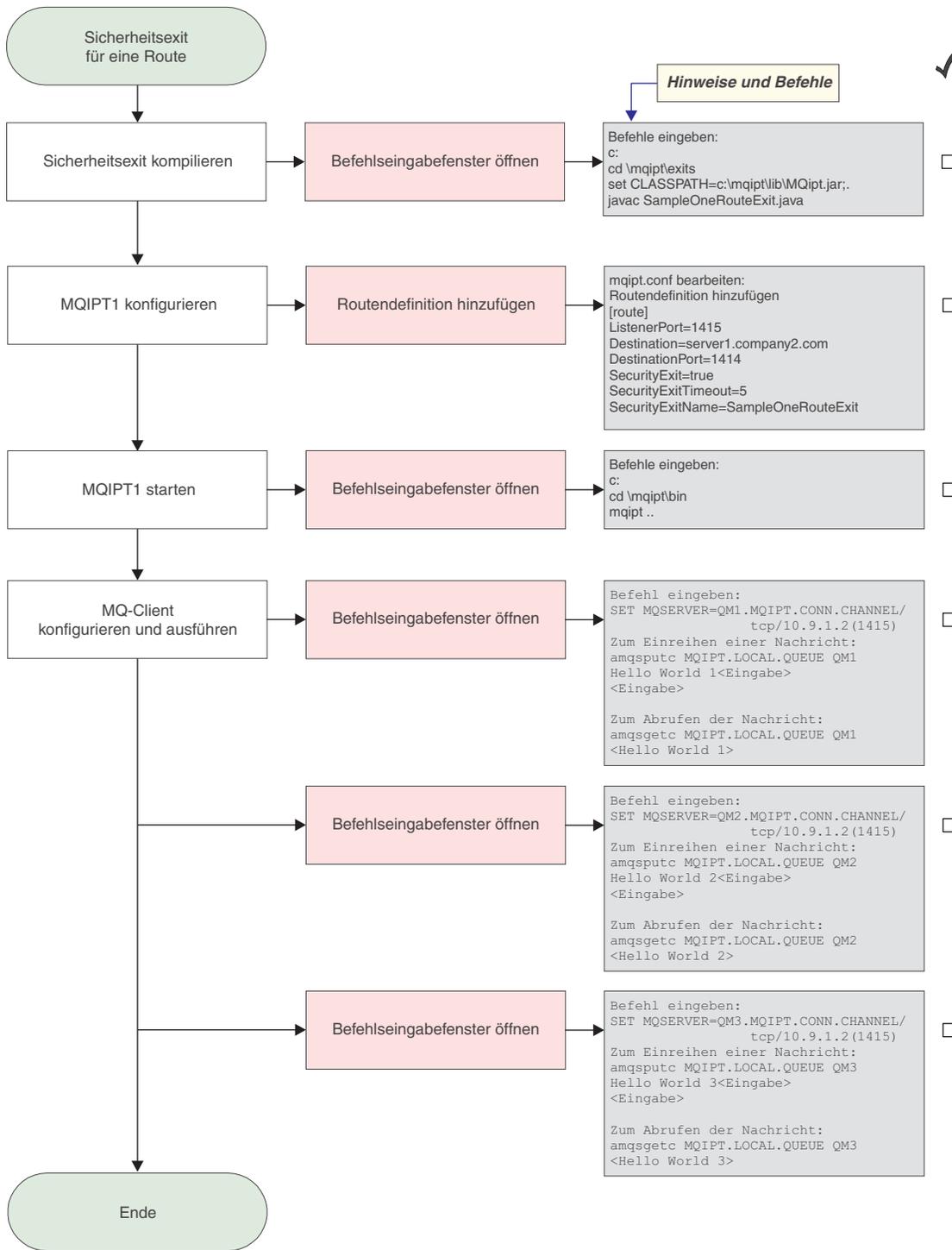


Abbildung 45. Konfiguration für dynamischen Exit bei nur einer Route

1. Auf IPT1

Öffnen Sie ein Befehlseingabefenster:

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

Ändern Sie die Datei **mqipt.conf**, indem Sie eine Routendefinition hinzufügen:

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

Öffnen Sie ein Befehlseingabefenster:

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

Die folgenden Nachrichten weisen auf eine erfolgreiche Ausführung hin:

```
5639-L92 (C) Copyright IBM Corp. 2000, 2003 Alle Rechte vorbehalten.  
MQCPI001 WebSphere MQ Internet Pass-Thru Version 1.3.0 wird gestartet.  
MQCPI004 Die Konfigurationsdaten aus c:\mqipt\mqipt.conf werden gelesen.  
MQCPI011 Die Protokolldateien werden im Pfad c:\mqipt\logs gespeichert.  
MQCPI006 Route 1415 wurde gestartet und leitet Nachrichten weiter an :  
MQCPI034 ....server1.company2.com(1414)  
MQCPI035 ....verwendet MQ-Protokolle  
MQCPI079 ...verwendet Sicherheitsexit c:\mqipt\exits\SampleOneRouteExit  
MQCPI080 .....und ein Zeitlimit von 5 Sekunden  
MQCPI078 Route 1415 für Verbindungsanforderungen bereit.
```

2. Geben Sie an einer Eingabeaufforderung auf der WebSphere MQ-Clientmaschine Folgendes ein:

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

3. Reihen Sie eine Nachricht wie folgt ein:

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

4. Rufen Sie die Nachricht wie folgt ab:

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

Es wird "Hello world 1" angezeigt.

5. Geben Sie an einer Eingabeaufforderung auf der WebSphere MQ-Clientmaschine Folgendes ein:

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

6. Reihen Sie eine Nachricht wie folgt ein:

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

7. Rufen Sie die Nachricht wie folgt ab:

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

Es wird "Hello world 2" angezeigt.

- |
- | 8. Geben Sie an einer Eingabeaufforderung auf der WebSphere MQ-Clientma-
- | schine Folgendes ein:
- | SET MQSERVER=QM3.MQIPT.CONN.CHANNEL/TCP/10.9.1.2(1415)
- |
- | 9. Reihen Sie eine Nachricht wie folgt ein:
- | amqsputc MQIPT.LOCAL.QUEUE QM3
- | Hello world 3 <Eingabe>
- | <Eingabe>
- |
- | 10. Rufen Sie die Nachricht wie folgt ab:
- | amqsgetc MQIPT.LOCAL.QUEUE QM3
- |
- | Es wird "Hello world 3" angezeigt.

Kapitel 21. WebSphere MQ Internet Pass-Thru - Wartung und Pflege

In diesem Kapitel wird erläutert, wie Sie den problemlosen Betrieb von WebSphere MQ Internet Pass-Thru sicherstellen können; es enthält die folgenden Abschnitte:

- „Verwaltung“
- „Fehlerbestimmung“
- „Durchsatzverbesserung“ auf Seite 156

Verwaltung

Folgende Dateien sollten im Zuge Ihrer normalen Backup-Verfahren in regelmäßigen Abständen gesichert werden:

- Die Konfigurationsdatei **mqipt.conf**
- Die SSL-Schlüsselringdateien in **mqipt.conf**, die über die folgenden Eigenschaften definiert sind:
 - SSLClientKeyRing
 - SSLClientCAKeyRing
 - SSLServerKeyRing
 - SSLServerCAKeyRing
- Die SSL-Schlüsselringkennwortdateien, die in **mqipt.conf** über die folgenden Eigenschaften definiert sind:
 - SSLClientKeyRingPW
 - SSLClientCAKeyRingPW
 - SSLServerKeyRingPW
 - SSLServerCAKeyRingPW
- Die Konfigurationsdatei des Verwaltungsagenten (**client.conf**), die Verbindungsdaten zu allen im Verwaltungsclient aufgeführten MQIPTs enthält

Fehlerbestimmung

Beim Auftreten von Problemen sollten Sie zuerst die folgenden häufigen Fehlerursachen überprüfen:

- Das MQIPT-System wurde gerade erst installiert und ist noch nicht neu gestartet worden.
- **HTTP** wurde für eine Route auf true gesetzt, die direkt mit einem WS-Manager verbunden ist.
- **SSL-Client** wurde für eine Route auf true gesetzt, die direkt mit einem WS-Manager verbunden ist.
- Die Variable CLASSPATH wurde nicht richtig gesetzt.
- Die Variable PATH wurde nicht richtig gesetzt.
- Bei den Kennwörtern für die Schlüsselringdateien muss die Groß-/Kleinschreibung beachtet werden.

Als Nächstes sollten Sie das Ablaufdiagramm in Abb. 46 auf Seite 154 durchgehen. Die Zahlen beziehen sich auf die Anmerkungen am Ende des Diagramms.

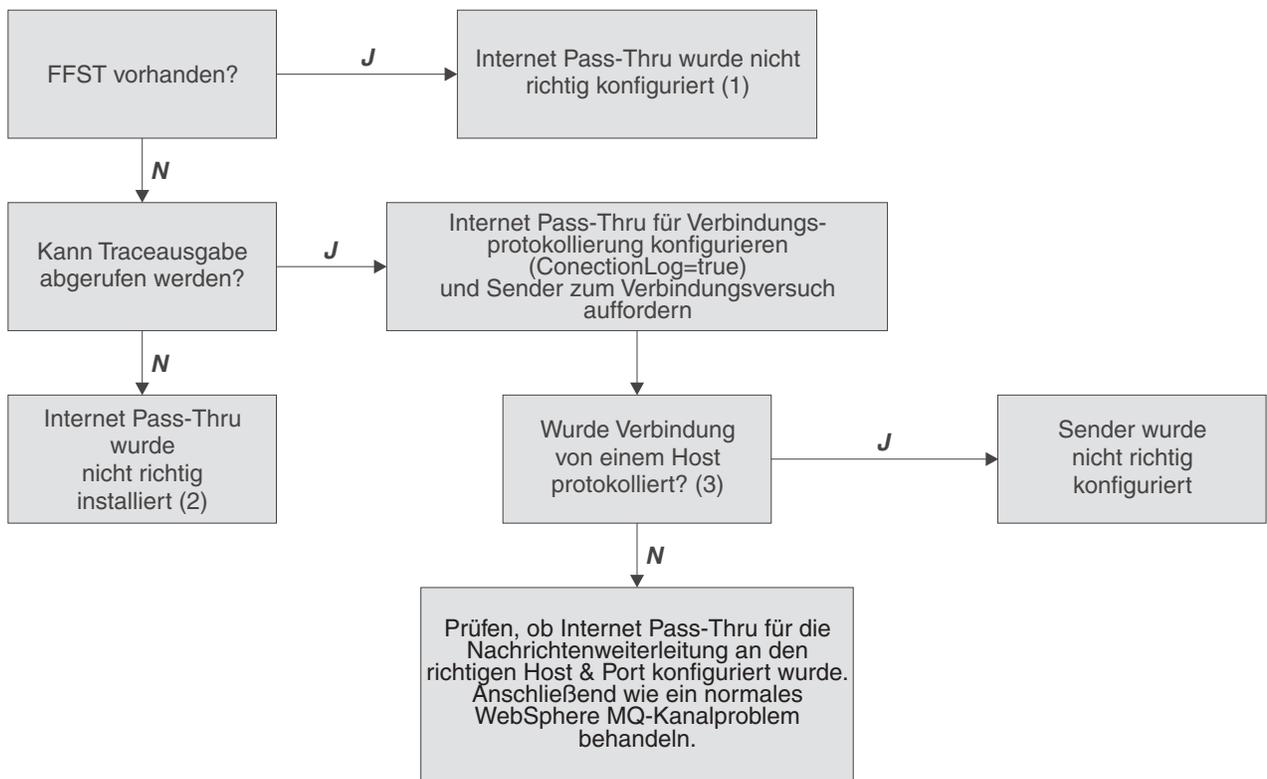


Abbildung 46. Fehlerbestimmung - Ablaufdiagramm

Anmerkungen:

1. Falls FFST-Berichte vorliegen (im Unterverzeichnis **errors**), wissen Sie, dass MQIPT richtig installiert wurde. Unter Umständen liegt ein Konfigurationsfehler vor.

Jeder FFST meldet einen Fehler, durch den der Start von MQIPT oder einer Route abgebrochen wird. Beheben Sie die in den FFST-Berichten angegebenen Fehler. Löschen Sie anschließend die alten FFST-Berichte, und starten Sie MQIPT erneut bzw. aktualisieren Sie MQIPT.

2. Wurde MQIPT nicht korrekt installiert, überprüfen Sie, ob alle Dateien im richtigen Verzeichnis stehen und die Variable CLASSPATH aktualisiert wurde. Versuchen Sie dazu, MQIPT manuell zu starten.

3. So starten Sie MQIPT manuell:

Öffnen Sie ein Befehlseingabefenster. Wechseln Sie in das Unterverzeichnis **bin**, und geben Sie Folgendes ein:

```
mqipt xxx
```

Dabei steht *xxx* für das Ausgangsverzeichnis von MQIPT, in diesem Fall `..`.

MQIPT wird daraufhin gestartet, und es wird nach der Konfigurationsdatei im Ausgangsverzeichnis gesucht. Überprüfen Sie das Unterverzeichnis **errors** auf Fehlermeldungen und FFSTs.

Überprüfen Sie die Textausgabe von MQIPT auf Fehlermeldungen, und korrigieren Sie die Fehler. Überprüfen Sie, ob FFSTs vorhanden sind; wenn ja, korrigieren Sie die gemeldeten Fehler. Falls ein Fehler im Abschnitt `global` der Konfigurationsdatei vorliegt, kann MQIPT nicht gestartet werden. Ebenso wird eine Route, die im `route`-Abschnitt falsch definiert wurde, nicht gestartet.

WebSphere MQ Internet Pass-Thru automatisch starten

Wenn Sie MQIPT als Windows NT-Dienst installieren und für den Start 'automatisch' angeben, wird MQIPT beim Hochfahren des Systems gestartet. Sie sollten MQIPT zunächst einmal automatisch starten, bevor Sie es als Windows NT-Dienst installieren; so können Sie feststellen, ob MQIPT richtig installiert wurde. Weitere Informationen hierzu finden Sie unter „Ein Windows-Dienststeuerungsprogramm verwenden“ auf Seite 50.

Wenn Sie die Fehlermeldung "Unable to locate DLL..." (DLL konnte nicht gefunden werden) erhalten, so verwenden Sie entweder das falsche **mqiptService**-Programm, oder die Systemumgebungsvariable PATH wurde nicht richtig konfiguriert. Diese Umgebungsvariable muss den Pfad zu den JNI-Laufzeitbibliotheken enthalten. Die Datei **jvm.dll** befindet sich im JDK-Unterverzeichnis **client**.

Durchgehende Verbindungen überprüfen

Wurde MQIPT richtig installiert, müssen Sie in einem nächsten Schritt überprüfen, ob die Routen richtig konfiguriert wurden.

Setzen Sie in der Konfigurationsdatei **mqipt.conf** die Eigenschaft **ConnectionLog** (Verbindungsprotokoll) auf **true**. Starten bzw. aktualisieren Sie MQIPT, und versuchen Sie, eine Verbindung herzustellen. Das Verbindungsprotokoll wird im Verzeichnis **logs** direkt unter dem Ausgangsverzeichnis erstellt. Wurde es nicht erstellt, weist dies darauf hin, dass MQIPT nicht richtig installiert wurde. Wurden keine Verbindungsversuche aufgezeichnet, so ist der Sender nicht richtig konfiguriert worden. Wenn Verbindungsversuche aufgezeichnet wurden, überprüfen Sie, ob MQIPT die Nachrichten an die richtige Adresse weiterleitet.

Tracefehler

MQIPT stellt eine umfassende Ausführungstracefunktion zur Verfügung, die über das Attribut **Trace** gesteuert wird. Für jede Route kann ein eigener Trace durchgeführt werden. Die Tracedateien werden in das Verzeichnis **xxx\errors** geschrieben (dabei steht **xxx** für das Verzeichnis, in dem sich die Konfigurationsdatei **mqipt.conf** befindet). Jeder Tracedatei wird ein Name des folgenden Formats zugewiesen:

`iptroutennnnn.trc`

Dabei steht **nnnn** für die Nummer des Ports, an dem die Route empfangsbereit ist. Traceausgaben von Threads, die keiner bestimmten Route zugeordnet sind (z. B. Threads, die für die Bearbeitung von Befehlseingaben zuständig sind), werden in eine eigene Datei namens `iptmain.trc` geschrieben.

Unerwartete schwer wiegende Fehler werden in Form von FFST-Berichten in einer Fehlerprotokolldatei aufgezeichnet, die sich im Verzeichnis **xxx\errors** befindet (dabei steht **xxx** für das Verzeichnis, das die Konfigurationsdatei **mqipt.conf** enthält). Die Namen der FFST-Dateien haben das folgende Format:

`iptxxx.FFST`

Dabei steht **xxx** für die Reihenfolge, in der der FFST-Bericht erstellt wurde (d. h., die älteste FFST-Datei hat die Nummer '1'. In Systemen mit langen Betriebszeiten wird unter Umständen die für das System maximal zulässige Anzahl an FFST-Berichten erreicht. In diesem Fall werden die FFST-Berichte, die erstellt wurden, in die Datei `mqipt0.FFST` geschrieben. Wenn diese Datei (`mqipt0.FFST`) erstellt wird, sollten Sie MQIPT bei der ersten Gelegenheit stoppen und erneut starten, und die alten FFST-Dateien löschen.

Fehlermeldung

Muss ein Problem an das IBM Service Center gemeldet werden, können Sie die Problemlösung beschleunigen, wenn Sie die folgenden Informationen bereit halten:

- Erstellen Sie einen einfachen Netzplan, der die Maschinen enthält, die verwendet werden; geben Sie außerdem die IP-Adressen an.
- Wird mehr als ein MQIPT verwendet, synchronisieren Sie die Systemtaktgeber auf den einzelnen MQIPT-Maschinen; dadurch können Traceinträge in den einzelnen MQIPs besser miteinander verglichen werden.
- Löschen Sie alte Tracedateien.
- Führen Sie den Client aus, um den Fehler zu reproduzieren; die Tracedateien enthalten auf diese Weise den Fehler nur einmal.
- Senden Sie eine Kopie aller MQIPT-Dateien mit den Erweiterungen **.trc** und **.log**.

Durchsatzverbesserung

Hier einige Hinweise, wie Sie Ihr System optimieren können.

Verwaltung von Threads-Pools

Die relative Leistung der einzelnen Routen kann durch eine Kombination aus Thread-Pool und Angabe eines Zeitlimits für Inaktivität optimiert werden.

Verbindungs-Threads

Jeder MQIPT-Route wird ein Arbeits-Pool mit gleichzeitig aktiven Threads zugeordnet, die eingehende Kommunikationsanforderungen bearbeiten. Bei der Initialisierung wird ein Thread-Pool erstellt, dessen Größe von der Definition des Attributs **MinConnectionThreads** (Mindestanzahl Verbindungs-Threads) im Abschnitt `route` der Konfigurationsdatei abhängt; außerdem wird ein Thread festgelegt, der für die Bearbeitung der ersten eingehenden Anforderung zuständig ist. Wenn diese Anforderung eintrifft, beginnt der Thread sofort mit ihrer Verarbeitung, und der nächste Thread wird für die Bearbeitung der nächsten eingehenden Anforderung bestimmt. Wenn alle Threads zugeordnet sind, wird ein neuer Thread erstellt, dem Arbeits-Pool hinzugefügt und zur Bearbeitung einer Anforderung zugeordnet. Auf diese Weise vergrößert sich der Pool, bis der über das Attribut **MaxConnectionThreads** (Maximale Anzahl Verbindungs-Threads) angegebene Wert erreicht wird. Wenn dieser Fall eintritt, wartet die nächste eingehende Anforderung, bis ein Thread für den Arbeits-Pool wieder freigegeben wird. Dies ist die maximale Arbeitskapazität der Route; wird diese überschritten, können keine weiteren Anforderungen akzeptiert werden. Die Threads werden für den Pool wieder freigegeben, nachdem eine Kommunikation beendet wird oder das angegebene Zeitlimit für Inaktivität überschritten wurde.

Zeitlimit für Inaktivität

Standardmäßig werden Threads bei Inaktivität nicht beendet. Wenn ein Thread einer Kommunikation zugeordnet wird, bleibt diese Zuordnung bestehen, bis die Kommunikation normal beendet, die Route deaktiviert oder MQIPT heruntergefahren wird. Optional können Sie aber ein Zeitlimit für Inaktivität angeben; dadurch wird ein Thread, der über eine bestimmte Zeit (in Minuten) inaktiv war, beendet. Ein Monitor-Thread überwacht die Zeitlimits für Inaktivität der einzelnen Threads und beendet diejenigen, deren Schwellenwert überschritten wird. Threads sind wiederverwendbar, d. h., sie werden nach der Freigabe wieder im Arbeits-Pool zur Verfügung gestellt.

Kapitel 22. Nachrichten

Bei Ausführung von MQIPT über die Befehlszeile werden verschiedene Informations-, Warn- und Fehlermeldungen an der Konsole angezeigt.

Dabei werden folgende Nachrichtenarten unterschieden:

- MQCAxxxx-Nachrichten sind Nachrichten des Verwaltungsclients.
- MQCPxxxx-Nachrichten sind MQIPT-Nachrichten.
- MQCxIxxx-Nachrichten sind Informationsnachrichten.
- MQCxWxxx-Nachrichten sind Warnungen.
- MQCxExxx-Nachrichten sind Fehlermeldungen.

MQCAE001 Unbekannter Host: {0}

Erläuterung: Der MQIPT-Host kann nicht gefunden werden.

Benutzeraktion: Überprüfen Sie, ob Sie den Namen des Hosts, auf dem MQIPT installiert ist, richtig angegeben haben.

MQCAE002 Das System hat folgenden Fehler gemeldet: {0}

Erläuterung: Es ist ein Fehler aufgetreten. Bei der Ausführung eines Systembefehls wurde ein Fehler gemeldet.

MQCAE005 Es wurde keine gültige Zieladresse definiert.

Erläuterung: Beim Hinzufügen einer Route wurde kein Wert im Feld für die Zieladresse angegeben.

Benutzeraktion: Geben Sie eine gültige Zieladresse ein.

MQCAE006 Es wurde kein gültiger Ziel-Port definiert.

Erläuterung: Beim Hinzufügen einer Route wurde kein Wert im Feld für den Ziel-Port angegeben.

Benutzeraktion: Geben Sie einen gültigen Ziel-Port ein.

MQCAE007 Es wurde kein gültiger Listener-Port definiert.

Erläuterung: Beim Hinzufügen einer Route wurde kein Wert im Feld für den Listener-Port angegeben.

Benutzeraktion: Geben Sie die gültige Adresse eines Listener-Ports ein (zwischen 1 und 65535).

MQCAE008 Es wurde keine gültige Netzadresse definiert.

Erläuterung: Beim Hinzufügen eines MQIPs wurde keine Netzadresse im gleichnamigen Feld angegeben.

Benutzeraktion: Geben Sie eine gültige Netzadresse ein.

MQCAE009 Es wurde kein gültiger Befehls-Port definiert.

Erläuterung: Beim Hinzufügen eines MQIPT wurde eine ungültige Befehls-Port-Adresse angegeben.

Benutzeraktion: Geben Sie die gültige Adresse eines Befehls-Ports ein (zwischen 1 und 65535).

MQCAE010 Die Onlinehilfe konnte nicht angezeigt werden.

Erläuterung: Die Datei mit der Onlinehilfe ist verfügbar, konnte aber nicht angezeigt werden.

Benutzeraktion: Stellen Sie sicher, dass ein Webbrowser installiert und in der Systemumgebungsvariablen PATH angegeben ist.

MQCAE011 Ein Parameter konnte nicht syntaktisch analysiert werden.

Erläuterung: Es ist ein interner Fehler aufgetreten, durch den versucht wurde, einen nicht vorhandenen Parameter in der Tabelle zu aktualisieren.

Benutzeraktion: Wenn der Fehler bestehen bleibt, wenden Sie sich an die Technische Unterstützung von IBM.

MQCAE012 Die Onlinehilfedatei {0} wurde nicht gefunden.

Erläuterung: Die Datei `passtfrm.htm` konnte nicht gefunden werden.

Benutzeraktion: Stellen Sie sicher, dass die Datei im Unterverzeichnis **doc** für Ihre Sprache vorhanden ist.

MQCAE013 Fehler beim Anzeigen der Onlinehilfe.

Erläuterung: Bei der Anzeige der Onlinehilfe ist ein Systemfehler aufgetreten.

Benutzeraktion: Wiederholen Sie den Vorgang. Wenn der Fehler bestehen bleibt, wenden Sie sich an die Technische Unterstützung von IBM.

MQCAE015 Das gerade eingegebene Kennwort wurde nicht erkannt.

Erläuterung: Der MQIPT erwartet ein gültiges Kennwort; im letzten Befehl wurde ein falsches Kennwort angegeben. Das Kennwort muss dem in der Konfigurationsdatei definierten Kennwort entsprechen.

Benutzeraktion: Ändern Sie das Kennwort über MQIPT -> **Verbindung**, und geben Sie den letzten Befehl erneut ein.

MQCAE016 Knoteninformationen stimmen nicht überein.

Erläuterung: Es besteht eine interne Inkonsistenz zwischen dem in der Baumstruktur ausgewählten Knoten und den Daten im Speicher.

Benutzeraktion: Schließen Sie den Verwaltungsclient, und geben Sie den Befehl erneut ein. Wenn der Fehler bestehen bleibt, wenden Sie sich an die Technische Unterstützung von IBM.

MQCAE017 Die Nachricht {0} konnte nicht in der Landessprache erstellt werden.

Erläuterung: Für die definierte Nachrichtennummer wurde keine Entsprechung in der Landessprache gefunden.

Benutzeraktion: Unter Umständen ist die Datei **guiadmin.properties** fehlerhaft, und die angegebene Nachrichtennummer konnte nicht gefunden werden. Gehen Sie wie folgt vor:

- Überprüfen Sie die Readme-Datei auf mögliche neue Nachrichten.
- Überprüfen Sie, ob die Datei **guiadmin.jar** in der Systemvariablen CLASSPATH angegeben ist.
- Überprüfen Sie, ob die Datei **guiadmin.properties** in der Datei **guiadmin.jar** enthalten ist.
- Überprüfen Sie, ob die Nachrichtennummer in der Datei **guiadmin.properties** enthalten ist.

MQCAE018 Could not create NLS text for message MQCAE017 (Die Nachricht MQCAE017 konnte nicht in der Landessprache erstellt werden)

Erläuterung: Die Nachricht {0} konnte nicht in der Liste mit den Systemeigenschaften gefunden werden.

Benutzeraktion: Die Datei **guiadmin.properties** ist möglicherweise beschädigt; gehen Sie wie folgt vor:

- Überprüfen Sie, ob die Datei **guiadmin.jar** in der Systemvariablen CLASSPATH angegeben ist.
- Überprüfen Sie, ob die Datei **guiadmin.properties** in der Datei **guiadmin.jar** enthalten ist.
- Überprüfen Sie, ob die Nachrichtennummer in der Datei **guiadmin.properties** enthalten ist.

MQCAE019 Das neue Kennwort wurde nicht durch eine zweite Eingabe bestätigt.

Erläuterung: Beim Ändern des Kennworts haben Sie das neue Kennwort nicht zweimal zum Bestätigen eingegeben.

Benutzeraktion: Geben Sie das neue Kennwort ein zweites Mal im entsprechenden Feld (**Neues Kennwort bestätigen**) ein.

MQCAE020 Fehler bei der Änderung der MQIPT-Zugriffsparemeter.

Erläuterung: Bei dem Versuch, MQIPT-Zugriffsparemeter zu ändern, ist ein interner Fehler festgestellt worden.

Benutzeraktion: Schließen Sie den Verwaltungsclient, und geben Sie den Befehl erneut ein. Wenn der Fehler bestehen bleibt, wenden Sie sich an die Technische Unterstützung von IBM.

MQCAE021 Interner Fehler bei der Identifizierung des MQIPT.

Erläuterung: Bei dem Versuch, eine Konfigurationsdatei in einem MQIPT zu speichern, ist ein interner Fehler festgestellt worden.

Benutzeraktion: Schließen Sie den Verwaltungsclient, und geben Sie den Befehl erneut ein. Wenn der Fehler bestehen bleibt, wenden Sie sich an die Technische Unterstützung von IBM.

MQCAE022 Interner Fehler beim Speichern der MQIPT-Konfiguration.

Erläuterung: Bei dem Versuch, eine Konfigurationsdatei in einem MQIPT zu speichern, ist ein interner Fehler festgestellt worden.

Benutzeraktion: Schließen Sie den Verwaltungsclient, und geben Sie den Befehl erneut ein. Wenn der Fehler

bestehen bleibt, wenden Sie sich an die Technische Unterstützung von IBM.

MQCAE023 MQIPT {0} hat das angegebene Kennwort nicht erkannt.

Erläuterung: Der MQIPT erwartet ein gültiges Kennwort; im letzten Befehl wurde ein falsches Kennwort angegeben. Das Kennwort muss dem in der Konfigurationsdatei definierten Kennwort entsprechen.

Benutzeraktion: Ändern Sie das Kennwort über das Menü **MQIPT -> Verbindung**, und geben Sie den letzten Befehl erneut ein.

MQCAE024 MQIPT {0} hat den Befehl nicht erkannt.

Erläuterung: Der Verwaltungsclient hat einen Befehl an den MQIPT gesendet, den dieser nicht erkannt hat.

Benutzeraktion: Stellen Sie sicher, dass der Verwaltungsclient dieselbe Clientcodeversion wie der MQIPT verwendet.

MQCAE025 MQIPT {0} konnte die Konfigurationsdatei nicht senden.

Erläuterung: Der Versuch des MQIPTs, die Konfigurationsdatei zu senden, ist fehlgeschlagen.

Benutzeraktion: Schließen Sie den Verwaltungsclient, und geben Sie den Befehl erneut ein. Bleibt der Fehler bestehen, stoppen Sie den MQIPT, und starten Sie ihn anschließend erneut.

MQCAE026 Fernes Beenden ist für MQIPT {0} nicht aktiviert.

Erläuterung: Der Versuch, den MQIPT fern abzuschalten, ist fehlgeschlagen, da die Eigenschaft **RemoteShutDown** in der Konfigurationsdatei nicht aktiviert wurde.

Benutzeraktion: Damit der MQIPT fern abgeschaltet werden kann, müssen Sie die Eigenschaft **RemoteShutDown** (Fernes Beenden) in der Konfigurationsdatei auf **true** setzen.

MQCAE027 Darstellung und Funktionsweise {0} wird nicht unterstützt.

Erläuterung: Die für die von Ihnen verwendete Plattform empfohlene Darstellung und Funktionsweise ist nicht verfügbar.

Benutzeraktion: Die Verarbeitung wird mit der vom System vorgegebenen Darstellung und Funktionsweise fortgesetzt.

MQCAE028 Klasse {0} für Darstellung und Funktionsweise wurde nicht gefunden.

Erläuterung: Die für die von Ihnen verwendete Plattform empfohlene Darstellung und Funktionsweise ist nicht verfügbar.

Benutzeraktion: Die Verarbeitung wird mit der vom System vorgegebenen Darstellung und Funktionsweise fortgesetzt.

MQCAE029 Die Mindestanzahl von Verbindungs-Threads darf nicht negativ und nicht größer als die maximale Anzahl von Verbindungs-Threads sein.

Erläuterung: Für die Mindestanzahl von Verbindungs-Threads muss ein Wert kleiner-gleich dem Wert für die maximale Anzahl von Verbindungs-Threads sein.

Benutzeraktion: Ändern Sie den Wert entsprechend.

MQCAE030 Der Wert muss größer als null und mindestens so groß wie die Mindestanzahl von Verbindungs-Threads sein.

Erläuterung: Für die maximale Anzahl von Verbindungs-Threads muss ein Wert größer-gleich dem Wert für die Mindestanzahl von Verbindungs-Threads angegeben werden.

Benutzeraktion: Ändern Sie den Wert entsprechend.

MQCAE031 Port-Nummern müssen im Bereich von 0 bis 65535 liegen.

Erläuterung: Sie versuchen, einen Wert anzugeben, der nicht den Vorgaben entspricht.

Benutzeraktion: Ändern Sie den Wert entsprechend.

MQCAE032 Trace muss im Bereich von 0 bis 5 liegen.

Erläuterung: Sie versuchen, einen Wert anzugeben, der nicht den Vorgaben entspricht.

Benutzeraktion: Ändern Sie den Wert entsprechend.

MQCAE033 Die maximale Protokollgröße muss im Bereich von 5 bis 50 liegen.

Erläuterung: Sie versuchen, einen Wert anzugeben, der nicht den Vorgaben entspricht.

Benutzeraktion: Ändern Sie den Wert entsprechend.

MQCAE049 Es wurde keine Route für einen MQIPT ausgewählt.

Erläuterung: Es wurde versucht, eine Route zu löschen, ohne sie vorher auszuwählen.

Benutzeraktion: Wählen Sie eine Route aus, und

geben Sie den Befehl erneut ein.

MQCAE050 Die Verbindung mit MQIPT {0} konnte nicht hergestellt werden.

Erläuterung: Der Verwaltungsclient konnte keine Verbindung zu dem angegebenen MQIPT herstellen.

Benutzeraktion: Dies kann eine der folgende Ursachen haben:

- MQIPT ist nicht aktiv.
- MQIPT ist am eigenen Befehls-Port nicht empfangsbereit.
- Der Befehls-Port von MQIPT wird nur von einem einzigen Verwaltungsclient verwendet.
- Das zulässige Zeitlimit für die Anforderung wurde überschritten.

MQCAE051 Die Antwort vom MQIPT {0} konnte nicht gelesen werden.

Erläuterung: Vom MQIPT wurde eine Antwort empfangen, die nicht dem erwarteten Protokoll entsprach.

Benutzeraktion: Stellen Sie sicher, dass der Verwaltungsclient dieselbe Clientcodeversion wie der MQIPT verwendet.

MQCAE052 Die Konfiguration wurde nicht gespeichert.

Erläuterung: Vom MQIPT wurde eine gültige Antwort empfangen, er konnte die Konfigurationsdatei jedoch nicht speichern.

Benutzeraktion: Überprüfen Sie, ob der MQIPT Schreibzugriff auf die Konfigurationsdatei hat.

MQCAE053 Der MQIPT hat das Speichern der Konfiguration nicht bestätigt.

Erläuterung: Die Konfigurationsdatei wurde an den MQIPT gesendet, der Empfang wurde jedoch nicht vom MQIPT bestätigt.

Benutzeraktion: Dies kann eine der folgende Ursachen haben:

- MQIPT ist nicht aktiv.
- MQIPT ist am eigenen Befehls-Port nicht empfangsbereit.
- Der Befehls-Port von MQIPT wird nur von einem einzigen Verwaltungsclient verwendet.
- Das zulässige Zeitlimit für die Anforderung wurde überschritten.

MQCAE054 Die Anzeige der MQIPT-Daten wurde nicht aktualisiert.

Erläuterung: Es wurde eine Verbindung zum MQIPT hergestellt, der Verwaltungsclient konnte jedoch die Konfigurationsdatei nicht lesen.

Benutzeraktion: Dies kann eine der folgende Ursachen haben:

1. Der MQIPT ist ausgefallen.
2. Das zulässige Zeitlimit für die Anforderung wurde überschritten.

MQCAE055 Es wurde kein MQIPT bzw. keine Route für einen MQIPT ausgewählt.

Erläuterung: Die von Ihnen ausgewählte Menüoption konnte nicht ausgeführt werden, da kein MQIPT bzw. keine Route ausgewählt wurde.

Benutzeraktion: Wählen Sie den entsprechenden MQIPT bzw. die entsprechende Route aus, und wiederholen Sie den Vorgang.

MQCAE056 Doppelter Listener-Port wurde zurückgewiesen.

Erläuterung: Der angegebene Listener-Port wurde zurückgewiesen, da er bereits von einer anderen Route verwendet wird.

Benutzeraktion: Wählen Sie einen anderen Listener-Port aus, und wiederholen Sie den Vorgang.

MQCAI002 Der MQIPT wurde aus der Anzeige entfernt.

Erläuterung: Der MQIPT, dessen Knoten Sie in der Baumstruktur ausgewählt haben, wurde aus dem Speicher des Clients entfernt.

MQCAI003 Neue Route wurde zur Anzeige hinzugefügt.

Erläuterung: Die gerade von Ihnen angegebene Route wurde dem aktuellen MQIPT hinzugefügt.

MQCAI004 Route wurde aus der Anzeige entfernt.

Erläuterung: Die von Ihnen in der Baumstruktur ausgewählte Route wurde aus dem Speicher des Clients entfernt.

MQCAI005 Der ausgewählte MQIPT wird angezeigt.

Erläuterung: Die globalen Parameter des von Ihnen in der Baumstruktur ausgewählten MQIPTs werden in der Tabelle angezeigt.

MQCAI006 Die ausgewählte Route wird angezeigt.

Erläuterung: Die Parameter der von Ihnen in der Baumstruktur ausgewählten Route werden in der Tabelle angezeigt.

MQCAI007 Die Clientkonfiguration wurde gespeichert.

Erläuterung: Die Zugriffsparameter für alle MQIPTS in der Baumstruktur wurden gespeichert.

MQCAI008 Die Onlinehilfe wurde erfolgreich angezeigt.

Erläuterung: Die Onlinehilfe wurde wie gefordert angezeigt.

MQCAI009 Die Tabelle wurde aktualisiert.

Erläuterung: Der Wert, den Sie gerade in die Tabelle eingegeben haben, wurde im Modell im Speicher übernommen.

MQCAI010 Es wurde kein MQIPT bzw. keine Route ausgewählt.

Erläuterung: Es wurde keine Aktion ausgeführt, da nicht genügend Informationen verfügbar waren.

MQCAI011 Die Benutzeraktion wurde abgebrochen.

Erläuterung: Sie haben eine zuvor von Ihnen eingeleitete Aktion (in die ein Dialogfenster involviert war) abgebrochen.

MQCAI014 Die Konfiguration für MQIPT wurde gespeichert.

Erläuterung: In dem momentan in der Baumstruktur ausgewählten MQIPT wurde eine neue Konfigurationsdatei gespeichert; der MQIPT wurde mit diesen Konfigurationsinformationen erneut gestartet.

MQCAI015 Die Onlinehilfefunktion wurde beendet.

Erläuterung: Die Onlinehilfe wurde wie gefordert angezeigt und anschließend geschlossen.

MQCAI017 Fügen Sie über das Menü 'Datei/MQIPT hinzufügen' einen MQIPT zur Baumstruktur hinzu.

Erläuterung: Diese Nachricht wird angezeigt, wenn die Baumstruktur keine MQIPTS enthält; die Nachricht gibt Hinweise, wie Sie der Baumstruktur einen MQIPT hinzufügen.

MQCAI018 Der neue MQIPT wurde zur Anzeige hinzugefügt.

Erläuterung: Der Baumstruktur wurde wie angewiesen ein neuer MQIPT hinzugefügt.

MQCAI019 Die MQIPT-Zugriffsparameter wurden geändert.

Erläuterung: Die Zugriffsparameter für den momentan in der Baumstruktur ausgewählten MQIPT wurden geändert.

MQCAI021 Wählen Sie einen MQIPT oder eine Route in der Baumstruktur aus, um den Inhalt anzuzeigen.

Erläuterung: Diese Nachricht wird angezeigt, wenn die Tabelle keine Informationen enthält; die Nachricht gibt Hinweise, wie Informationen angezeigt werden können.

MQCAI022 Der Befehls-Port wurde geändert.

Erläuterung: Der Befehls-Port des MQIPTS wurde wie angewiesen geändert.

MQCAI023 Das Kennwort wurde geändert.

Erläuterung: Die Kommunikation mit dem MQIPT, an dem gerade Änderungen vorgenommen wurden, wird künftig unter Verwendung des neuen Kennworts erfolgen.

MQCAI025 Die Anzeige für MQIPT {0} wurde aktualisiert.

Erläuterung: Die Informationen im MQIPT wurden mit Hilfe seiner Konfigurationsdatei aktualisiert.

MQCAI026 MQIPT {0} hat eine Anforderung zum Beenden empfangen.

Erläuterung: Der MQIPT hat den Empfang einer Anforderung zum Abschalten bestätigt und wird heruntergefahren.

MQCAI027 Die Anzeige der Clientkonfiguration wurde aktualisiert.

Erläuterung: Die im Verwaltungsclient angezeigten Informationen wurden anhand der lokalen Datei `client.conf` aktualisiert.

MQCAI028 MQIPT {0} ist aktiv.

Erläuterung: Der MQIPT hat auf eine PING-Anforderung erfolgreich geantwortet.

MQCAI029 MQIPT {0} ist nicht aktiv.

Erläuterung: Der MQIPT hat auf eine PING-Anforderung nicht innerhalb der angegebenen Zeit geantwortet.

Benutzeraktion: Dies kann eine der folgende Ursachen haben:

- MQIPT ist nicht aktiv.
- MQIPT ist am eigenen Befehls-Port nicht empfangsbereit.
- Das zulässige Zeitlimit für die Anforderung wurde überschritten. Das Zeitlimit kann erhöht werden, indem die Eigenschaft **Zeitlimit (Sek)** in den Verbindungsinformationen des MQIPTs geändert wird.

MQCAI030 Route {0} ist aktiv.

Erläuterung: Der MQIPT hat auf eine PING-Anforderung erfolgreich geantwortet.

MQCAI031 Route {0} ist nicht aktiv.

Erläuterung: Die MQIPT-Route hat auf eine PING-Anforderung nicht innerhalb der angegebenen Zeit geantwortet.

Benutzeraktion: Dies kann eine der folgende Ursachen haben:

- MQIPT ist nicht aktiv.
- MQIPT ist am eigenen Befehls-Port nicht empfangsbereit.
- Das zulässige Zeitlimit für die Anforderung wurde überschritten. Das Zeitlimit kann erhöht werden, indem die Eigenschaft **Zeitlimit (Sek)** in den Verbindungsinformationen des MQIPTs geändert wird.

MQCAI100 Dieses Script startet den Verwaltungsclient für {0}. Bei Angabe eines SOCKS-Proxy kann der Verwaltungsclient durch eine Firewall mit einem MQIPT kommunizieren.

Erläuterung: Onlinehilfeinformationen zum Script `mciptGui`.

MQCAI101 Das Befehlsformat lautet:

Erläuterung: Onlinehilfeinformationen zum Script `mciptGui`.

MQCAI102 `mciptGui {Socks_Host{Socks_Port}}`

Erläuterung: Onlinehilfeinformationen zum Script `mciptGui`.

MQCAI103 Socks_Host - Hostname des SOCKS-Proxy (optional)

Erläuterung: Onlinehilfeinformationen zum Script `mciptGui`.

MQCAI104 Socks_Port - Port-Adresse des SOCKS-Proxy (optional - Standardwert 1080)

Erläuterung: Onlinehilfeinformationen zum Script `mciptGui`.

MQCPE000 Bei der Bearbeitung der Nachricht {0} konnten keine Nachrichtendaten gefunden werden

Erläuterung: Die Nachricht {0} konnte nicht in der Liste mit den Systemeigenschaften gefunden werden.

Benutzeraktion: Die Datei `mcipt.properties` ist fehlerhaft, die angegebene Nachrichtennummer konnte nicht gefunden werden. Gehen Sie wie folgt vor:

- Prüfen Sie, ob die Datei `MQipt.jar` in der Systemvariablen CLASSPATH definiert ist.
- Prüfen Sie, ob die Datei `mcipt.properties` in der Datei `MQipt.jar` angegeben ist.
- Prüfen Sie, ob die Nachrichtennummer in der Datei `mcipt.properties` definiert ist.

MQCPE001 Das Verzeichnis ist nicht vorhanden, oder der Verzeichnisname ist falsch.

Erläuterung: Bei der Initialisierung konnte ein erforderliches Verzeichnis nicht gefunden werden. Diese Nachricht bezieht sich auf ein Verzeichnis, das in der MQIPT-Konfigurationsdatei `mcipt.conf` oder in der Befehlszeile als Standardverzeichnis in den MQIPT-Startoptionen angegeben wurde.

Benutzeraktion: Geben Sie das richtige Verzeichnis an, und geben Sie den Befehl erneut ein.

MQCPE004 Fehler beim Starten der Route an Port {0}.

Erläuterung: Die Route konnte nicht mit der angegebenen Listener-Port-Nummer gestartet werden.

Benutzeraktion: Beim Start der Route ist ein E/A-Fehler aufgetreten. Überprüfen Sie, ob noch andere zugehörige Nachrichten und Protokolleinträge vorliegen, die weitere Informationen zu diesem Fehler enthalten.

MQCPE005 Die Konfigurationsdatei {0} wurde nicht gefunden.

Erläuterung: Die MQIPT-Konfigurationsdatei `mcipt.conf` konnte nicht in dem angegebenen Verzeichnis gefunden werden.

Benutzeraktion: Geben Sie das richtige Verzeichnis an, und geben Sie den Befehl erneut ein.

MQCPE006 Die maximale Anzahl von {0} Routen wurde überschritten. MQIPT wird zwar gestartet, diese Konfiguration jedoch nicht unterstützt.

Erläuterung: In Ihrer Konfiguration wurde die Anzahl der Routen überschritten, die maximal für eine MQIPT-Instanz unterstützt werden. Der Betrieb wird nicht gestoppt, das System wird jedoch unter Umständen instabil oder überlastet. Konfigurationen, die die angegebene Anzahl der maximal möglichen Routen überschreiten, werden nicht unterstützt.

Benutzeraktion: Starten Sie eventuell weitere MQIPT-Instanzen mit jeweils weniger Routen.

MQCPE007 Die Route an Listener-Port {0} wurde nicht erneut gestartet.

Erläuterung: Bei einer REFRESH-Operation wurde die Route am angegebenen Listener-Port in der neuen Konfiguration nicht erneut gestartet.

Benutzeraktion: Überprüfen Sie, ob noch andere zugehörige Nachrichten vorliegen, die weitere Informationen zu diesem Fehler enthalten.

MQCPE008 Für Listener-Port {0} wurde eine Route doppelt definiert.

Erläuterung: Es wurde mehr als eine Route mit demselben Listener-Port definiert.

Benutzeraktion: Entfernen Sie die doppelt vorhandene Routendefinition aus der Konfigurationsdatei, und geben Sie den Befehl erneut ein.

MQCPE009 Protokollverzeichnis {0} ist nicht gültig.

Erläuterung: Der im Text angezeigte Protokollpfad ist entweder nicht vorhanden oder momentan nicht verfügbar.

Benutzeraktion: Überprüfen Sie, ob das Verzeichnis vorhanden ist und der MQIPT Zugriff darauf hat.

MQCPE010 Nummer {0} für den Listener- bzw. Befehls-Port ist ungültig.

Erläuterung: Die für den Parameter `CommandPort` oder `ListenerPort` angegebene Port-Nummer ist ungültig.

Benutzeraktion: Geben Sie eine gültige Port-Nummer an, die noch nicht vergeben ist. Holen Sie sich von Ihrem Netzadministrator Hinweise zur Verwendung von Port-Nummern in Ihrem Netz.

MQCPE011 Tracestufe {0} liegt nicht im gültigen Bereich von 0 bis 5.

Erläuterung: Die angegebene Traceoption wurde angefordert, liegt jedoch außerhalb des zulässigen Bereich von 0 bis 5.

Benutzeraktion: Geben Sie für den Trace einen Wert zwischen 0 und 5 an.

MQCPE012 Der Wert {0} ist für die Eigenschaft {1} ungültig.

Erläuterung: Für eine Eigenschaft wurde ein ungültiger Wert angegeben.

Benutzeraktion: Die zulässigen Werte für die einzelnen Steuerparameter können Sie dem vorliegenden Handbuch entnehmen.

MQCPE013 Für Route {0} ist keine Eigenschaft ListenerPort angegeben.

Erläuterung: MQIPT hat festgestellt, dass in einem route-Abschnitt in der Konfigurationsdatei die Eigenschaft `ListenerPort` fehlt. Diese Eigenschaft ist die primäre und eindeutige Kennzeichnung für die einzelnen Routen, daher ist diese Angabe unbedingt erforderlich.

Benutzeraktion: Geben Sie für die angegebene Route einen gültigen Listener-Port-Nummer an.

MQCPE014 Der Wert {0} für die Eigenschaft ListenerPort ist ungültig.

Erläuterung: Für die Eigenschaft `ListenerPort` einer Route wurde eine ungültige Port-Adresse angegeben.

Benutzeraktion: Die Port-Adresse muss im Bereich von 0 bis 65535 liegen. Überprüfen Sie die einzelnen Listener-Port-Adressen in der Konfigurationsdatei.

MQCPE015 Für Nachrichtennummer {0} wurde kein Text gefunden.

Erläuterung: Es ist ein interner Fehler aufgetreten, für den keine Beschreibung vorliegt.

Benutzeraktion: Die Datei `mqipt.properties` ist fehlerhaft, die angegebene Nachrichtennummer konnte nicht gefunden werden. Gehen Sie wie folgt vor:

- Überprüfen Sie die Readme-Datei auf mögliche neue Nachrichten.
 - Prüfen Sie, ob die Datei `MQipt.jar` in der Systemvariablen `CLASSPATH` definiert ist.
 - Prüfen Sie, ob die Datei `mqipt.properties` in der Datei `MQipt.jar` angegeben ist.
 - Prüfen Sie, ob die Nachrichtennummer in der Datei `mqipt.properties` definiert ist.
-

MQCPE016 Die maximale Anzahl von Verbindungs-Threads ist {0} und damit kleiner als die Mindestanzahl von {1}.

Erläuterung: In Ihrer Konfiguration für die Mindestanzahl von Verbindungs-Threads ist ein Wert angegeben, der über der maximalen Anzahl von Verbindungs-Threads liegt.

Benutzeraktion: Hier kann es sich um einen Fehler in einer einzelnen Route oder um einen Konflikt zwischen einer globalen Eigenschaft und einer Routeneigenschaft handeln, oder eine Routeneigenschaft setzt einen systemspezifischen Standardwert außer Kraft. Hinweise auf die zulässigen Werte und Standardwerte finden Sie in den vorderen Kapiteln des vorliegenden Handbuchs.

MQCPE017 Die Ausnahme {0} hat die Beendigung von MQIPT verursacht.

Erläuterung: MQIPT wurde abnormal beendet und heruntergefahren. Die Ursache dafür liegt möglicherweise in Bedingungen oder Vorgaben der Systemumgebung (z. B. Speicherüberlauf).

Benutzeraktion: Wenn der Fehler bestehen bleibt, wenden Sie sich an die Technische Unterstützung von IBM.

MQCPE018 Die Eigenschaft ListenerPort ist nicht angegeben. Die Route wird nicht gestartet.

Erläuterung: Für eine Route wurde keine Nummer für den Listener-Port angegeben.

Benutzeraktion: Fügen Sie in der Konfigurationsdatei dem entsprechenden route-Abschnitt eine gültigen Listener-Port hinzu.

MQCPE019 Die Zeilengruppe {0} fehlt vor folgendem Eintrag: {1}

Erläuterung: In der Konfigurationsdatei liegt unter Umständen ein Fehler in der Reihenfolge vor.

Benutzeraktion: Stellen Sie sicher, dass in der Konfigurationsdatei alle [route]-Einträge nach den [global]-Einträgen stehen.

MQCPE020 Der neue Wert für MaxConnectionThreads ist {0}. Er muss größer als der aktuelle Wert {1} sein.

Erläuterung: Nach dem Start der Route kann die Eigenschaft **MaxConnectionThread** (Maximale Anzahl Verbindungs-Threads) nur erhöht werden.

Benutzeraktion: Ändern Sie in der Konfigurationsdatei den Wert der Eigenschaft **MaxConnectionThread** entsprechend.

MQCPE021 Für Route {0} wurde nicht die Eigenschaft 'Destination' angegeben.

Erläuterung: Die Eigenschaft **Destination** (Zieladresse) muss in einem route-Abschnitt vorhanden sein, fehlt aber für die angegebene Route.

Benutzeraktion: Fügen Sie in der Konfigurationsdatei dem entsprechenden route-Abschnitt die Eigenschaft **Destination** hinzu.

MQCPE022 Der Wert {0} für den Befehls-Port (CommandPort) liegt nicht im gültigen Bereich von 1 bis 65535.

Erläuterung: Der Wert für den Befehls-Port lag außerhalb des Bereichs von 1 und 65535.

Benutzeraktion: Geben Sie in der Konfigurationsdatei eine gültige Adresse für die Eigenschaft **CommandPort** an.

MQCPE023 Die Beendigungsanforderung vom Verwaltungsclient {0} wird ignoriert, weil diese Funktion inaktiviert ist.

Erläuterung: Der Versuch, den MQIPT fern abzuschalten, ist fehlgeschlagen, da die Eigenschaft **RemoteShutDown** in der Konfigurationsdatei nicht aktiviert wurde.

Benutzeraktion: Damit der MQIPT fern abgeschaltet werden kann, müssen Sie die Eigenschaft **RemoteShutDown** (Fernes Beenden) in der Konfigurationsdatei auf **true** setzen.

MQCPE024 Der vom MQIPT-Controller empfangene Befehl wurde nicht erkannt.

Erläuterung: MQIPT hat am Befehls-Port einen unbekanntem Befehl empfangen.

Benutzeraktion: Überprüfen Sie die Identität des Befehls anhand der Datei **mqipt.log**.

MQCPE025 Fehler beim Herstellen einer Verbindung mit dem Server auf Host {0}, Port {1}.

Erläuterung: Die Zeilenmodusversion (nicht GUI) des Verwaltungsclients kann nicht mit dem MQIPT kommunizieren.

Benutzeraktion: Stellen Sie sicher, dass in der Konfigurationsdatei für die Eigenschaft **CommandPort** der Wert {1} angegeben ist und der MQIPT an {0} läuft.

MQCPE026 Es wurde keine Antwort vom Server auf Host {0}, Port {1} empfangen.

Erläuterung: Die Zeilenmodusversion (nicht GUI) des Verwaltungsclients hat eine Verbindung zum MQIPT hergestellt, hat aber keine Antwort erhalten.

Benutzeraktion: Dies deutet darauf hin, dass das zulässige Zeitlimit für die Anforderung überschritten wurde oder ein Problem mit dem MQIPT vorliegt.

MQCPE027 Die Antwort vom MQIPT wurde nicht erkannt.

Erläuterung: Die Zeilenmodusversion (nicht GUI) des Verwaltungsclients hat eine Antwort vom MQIPT erhalten, die der Verwaltungsclient nicht erkennt.

Benutzeraktion: Überprüfen, ob das Script `mqiptAdmin` und der MQIPT dieselbe Version der Datei `MQipt.jar` verwenden.

MQCPE028 Ungültige Zeilengruppe gefunden: {0}

Erläuterung: Die angegebene unbekannte Zeilengruppe wurde in der Konfigurationsdatei gefunden.

Benutzeraktion: In der Konfigurationsdatei sind nur die Zeilengruppen `[global]` und `[route]` zulässig.

MQCPE029 Die Protokollausgabe konnte nicht aktualisiert werden.

Erläuterung: Unter Umständen wurden einige Nachrichten nicht in das Protokoll geschrieben, da der Kommunikationspuffer nicht geleert werden konnte.

Benutzeraktion: Überprüfen Sie, ob im Ausgangsverzeichnis von MQIPT noch Platz ist und ob MQIPT noch Zugriff auf das Unterverzeichnis `logs` hat.

MQCPE030 {0} ist nicht im CLASSPATH enthalten.

Erläuterung: Die angegebene `.jar`-Datei wurde nicht in der Systemumgebungsvariablen `CLASSPATH` gefunden.

Benutzeraktion: Fügen Sie der Systemumgebungsvariablen `CLASSPATH` die angegebene Datei hinzu.

MQCPE031 Die Klasse {0} wurde nicht gefunden.

Erläuterung: Diese Nachricht wird bei Anzeige der Versionsnummer von MQIPT erstellt. Die angegebene Klasse konnte nicht in der `.jar`-Datei von MQIPT gefunden werden oder die Systemumgebungsvariable `CLASSPATH` ist fehlerhaft.

Benutzeraktion: Überprüfen Sie, ob die angegebene Klassendatei in der Datei `MQipt.jar` und die Datei `MQipt.jar` in der Systemumgebungsvariablen `CLASSPATH` enthalten ist.

MQCPE033 Fehler beim Senden der Konfigurationsdatei an den Verwaltungsclient an {0}.

Erläuterung: Beim Senden der Konfigurationsdatei an den Verwaltungsclient ist ein Fehler aufgetreten.

Benutzeraktion: Überprüfen Sie, ob sich die

Konfigurationsdatei im MQIPT-Ausgangsverzeichnis befindet und nicht von einem anderen Prozess benutzt wird.

MQCPE034 Der Verwaltungsclient an {0} hat nicht das richtige Kennwort angegeben.

Erläuterung: Das in der Konfigurationsdatei angegebene Zugriffskennwort (`AccessPW`) entspricht nicht dem vom Verwaltungsclient übergebenen Kennwort.

Benutzeraktion: Sie müssen entweder das in der Konfigurationsdatei angegebene Zugriffskennwort (Eigenschaft `AccessPW`) oder das im Verwaltungsclient gespeicherte Kennwort ändern.

MQCPE035 Fehler beim Starten des Befehlsempfangsprogramms an Port {0}.

Erläuterung: Beim Starten des Befehlsempfangsprogramms an der angegebenen Port-Adresse ist ein E/A-Fehler aufgetreten.

Benutzeraktion: Überprüfen Sie die Port-Adresse, die in der Konfigurationsdatei für die Eigenschaft `CommandPort` angegeben ist.

MQCPE038 MQIPT wurde nicht wie erwartet gestartet.

Erläuterung: Diese Nachricht wird vom `mqiptFork`-Prozess erstellt, der MQIPT als Systemservice startet.

Benutzeraktion: Überprüfen Sie die Fehlerprotokolle auf weitere Informationen. Versuchen Sie, das Ruheintervall zu erhöhen, nach dessen Ablauf `IPTFork` prüft, ob MQIPT aktiv ist. Ändern Sie dazu im Script `mqiptFork` den Parameter, der an `IPTFork` übergeben wird.

MQCPE039 E/A-Fehler bei Ausführung des Scripts mqipt.

Erläuterung: Beim Starten von MQIPT über den Aufspaltungsprozess (Fork-Prozess) ist ein Fehler aufgetreten.

Benutzeraktion: Überprüfen Sie, ob die Systemumgebungsvariable `PATH` den Pfad zu `JDK` enthält und das Script `mqipt` über die Ausführungsberechtigung verfügt.

MQCPE040 Fehler bei Ausführung des Scripts mqipt.

Erläuterung: Nach dem Start von MQIPT über den Aufspaltungsprozess (Fork-Prozess) ist ein Fehler aufgetreten.

Benutzeraktion: Überprüfen Sie die Fehlerprotokolle auf weitere Informationen. Wenn der Fehler bestehen bleibt, wenden Sie sich an die Technische Unterstützung von IBM.

MQCPE041 Java-Stufe wird nicht unterstützt - {0}

Erläuterung: MQIPT wurde mit der angegebenen Java-Stufe gestartet.

Benutzeraktion: Überprüfen Sie die im vorliegenden Benutzerhandbuch aufgeführten Voraussetzungen auf weitere Informationen.

MQCPE042 Es gibt einen Konflikt zwischen folgenden Eigenschaften für Route {0}:

Erläuterung: Einige der Eigenschaften können nicht mit anderen Eigenschaften zusammen verwendet werden. Im Anschluss an diese Nachrichten folgt eine Liste der Eigenschaften, zwischen denen eine Konflikt besteht.

Benutzeraktion: Überprüfen Sie die nachfolgenden Fehlernachrichten, und führen Sie die entsprechenden Maßnahmen aus.

MQCPE043{0} und {1}

Erläuterung: Die folgenden Eigenschaften können nicht gleichzeitig für ein und dieselbe Route gesetzt werden.

Benutzeraktion: Deaktivieren Sie in der Konfigurationsdatei eine der angegebenen Eigenschaften für die betreffende Route.

MQCPE044 {0} ist nur unter Betriebssystem {1} gültig.

Erläuterung: Einige Leistungsmerkmale von MQIPT sind nur auf bestimmten Plattformen gültig.

Benutzeraktion: Deaktivieren Sie in der Konfigurationsdatei die angegebene Eigenschaft.

MQCPE045Name für HTTP-Proxy fehlt.

Erläuterung: Wenn die Eigenschaft HTTP auf true gesetzt wurde, muss für die Eigenschaft HTTPProxy ein Wert angegeben werden.

Benutzeraktion: Definieren Sie in der Konfigurationsdatei einen HTTP-Proxy für die betreffende Route.

MQCPE046 {0} ist nicht zulässig, da Pagent nicht initialisiert werden konnte.

Erläuterung: Der Richtlinienagent (Pagent) ist eine Anwendung, die QoS für MQIPT zur Verfügung stellt. MQIPT konnte den Pagent beim Start nicht initialisieren, und die Eigenschaft QoS (Quality of Service) ist für die betreffende Route auf true gesetzt.

Benutzeraktion: Deaktivieren Sie in der Konfigurationsdatei QoS für die betreffende Route.

MQCPE047 Pagent konnte nicht initialisiert werden.

Erläuterung: Der Richtlinienagent (Pagent) ist eine Anwendung, die QoS für MQIPT zur Verfügung stellt. MQIPT konnte beim Start nicht initialisiert werden.

Benutzeraktion: Wird der Pagent nicht verwendet, können Sie diese Fehlernachricht ignorieren; in diesem Fall muss allerdings die Eigenschaft QoS auf false gesetzt werden.

MQCPE048 Fehler beim Starten der Route an Port {0}; Ausnahme : {1}

Erläuterung: Die Route konnte nicht mit der angegebenen Listener-Port-Nummer gestartet werden.

Benutzeraktion: Überprüfen Sie, ob noch andere zugehörige Nachrichten und Protokolleinträge vorliegen, die weitere Informationen zu diesem Fehler enthalten.

MQCPE049 Fehler beim Starten bzw. Stoppen von Java Security Manager {0}

Erläuterung: Bei dem Versuch, den Java Security Manager zu starten oder zu stoppen, wurde eine Ausnahmebedingung ausgegeben.

Benutzeraktion: Der Java Security Manager wurde zuvor aktiviert, es wurden jedoch keine Laufzeitberechtigungen aktiviert. Fügen Sie in der lokalen Richtliniendatei RuntimePermission (Laufzeitberechtigung) für setSecurityManager hinzu. Die Änderungen werden erst nach einem Neustart von MQIPT wirksam.

MQCPE050 Sicherheitsausnahme an Port {0} vom Verwaltungsclient

Erläuterung: Beim Akzeptieren einer Verbindung vom Verwaltungsclient wurde eine Sicherheitsausnahme ausgegeben.

Benutzeraktion: Der Java Security Manager wurde zuvor aktiviert, es wurden jedoch dem in der Fehlermeldung angegebenen Host keine Berechtigungen erteilt. Damit der Host eine Verbindung zum MQIPT herstellen kann, müssen Sie eine Socket-Berechtigung hinzufügen, damit Verbindungen an der Adresse des Befehls-Ports akzeptiert bzw. aufgelöst werden können. Die Änderungen werden erst nach einem Neustart des Java Security Manager wirksam.

MQCPE051 Sicherheitsausnahme bei Annahme einer Verbindung auf Route {0}

Erläuterung: Beim Akzeptieren einer Verbindung von der angegebenen Route wurde eine Sicherheitsausnahme ausgegeben.

Benutzeraktion: Der Java Security Manager wurde zuvor aktiviert, es wurden jedoch dem in der Fehlermeldung angegebenen Host keine Berechtigungen

erteilt. Damit der Host eine Verbindung zu dieser Route herstellen kann, müssen Sie eine Socket-Berechtigung hinzufügen, damit Verbindungen für den Listener-Port akzeptiert bzw. aufgelöst werden können. Die Änderungen werden erst nach einem Neustart des Java Security Manager wirksam.

MQCPE052 Fehler bei Verbindungsanforderung auf Route {0} : {1}

Erläuterung: Diese Nachricht wird in das Verbindungsprotokoll geschrieben, um eine Sicherheitsausnahme für eine Verbindungsanforderung aufzuzeichnen.

Benutzeraktion: Der Java Security Manager wurde zuvor aktiviert, es wurden jedoch dem in der Fehlermeldung angegebenen Host keine Berechtigungen erteilt. Damit der Host eine Verbindung zu dieser Route herstellen kann, müssen Sie eine Socket-Berechtigung hinzufügen, damit Verbindungen für den Listener-Port akzeptiert bzw. aufgelöst werden können. Die Änderungen werden erst nach einem Neustart des Java Security Manager wirksam.

MQCPE053 Sicherheitsausnahme beim Herstellen einer Verbindung mit {0}({1})

Erläuterung: Beim Herstellen einer Verbindung auf der angegebenen Route wurde eine Sicherheitsausnahme ausgegeben.

Benutzeraktion: Der Java Security Manager wurde zuvor aktiviert, es wurden jedoch dem in der Fehlermeldung angegebenen Host keine Berechtigungen erteilt. Damit der Host eine Verbindung zu dieser Route herstellen kann, müssen Sie eine Socket-Berechtigung hinzufügen, damit Verbindungen für den Listener-Port akzeptiert bzw. aufgelöst werden können. Die Änderungen werden erst nach einem Neustart des Java Security Manager wirksam.

MQCPE054 Fehler bei Verbindungsanforderung an {0}({1}) : {2}

Erläuterung: Diese Nachricht wird in das Verbindungsprotokoll geschrieben, um eine Sicherheitsausnahme für eine Verbindungsanforderung an einen Zielhost aufzuzeichnen.

Benutzeraktion: Der Java Security Manager wurde zuvor aktiviert, es wurden jedoch dem in der Fehlermeldung angegebenen Host keine Berechtigungen erteilt. Damit der Host eine Verbindung zu dieser Route herstellen kann, müssen Sie eine Socket-Berechtigung hinzufügen, damit Verbindungen für den Listener-Port akzeptiert bzw. aufgelöst werden können. Die Änderungen werden erst nach einem Neustart des Java Security Manager wirksam.

MQCPE055Name für Socks-Proxy fehlt.

Erläuterung: Wenn die Eigenschaft `SocksClient` auf `true` gesetzt wurde, muss für die Eigenschaft `SocksProxy` ein Wert angegeben werden.

Benutzeraktion: Definieren Sie in der Konfigurationsdatei einen SOCKS-Proxy für die betreffende Route.

MQCPE056 Konflikt zwischen Routeneigenschaften

Erläuterung: Einige der Eigenschaften können nicht mit anderen Eigenschaften zusammen verwendet werden.

Benutzeraktion: Überprüfen Sie die Konsolnachrichten auf nähere Angaben zu dem Fehler, und nehmen Sie die entsprechenden Maßnahmen vor.

MQCPE057 SSL-Protokoll ({0}) ist unbekannt.

Erläuterung: Für die Route wurde der SSL-Proxy-Modus definiert, der Eingangsdatenfluss wurde jedoch nicht erkannt.

Benutzeraktion: Stellen Sie sicher, dass zu dieser Route nur SSL-Verbindungen hergestellt werden.

MQCPE058 CONNECT-Anforderung an {2}({3}) über {0}({1}) ist fehlgeschlagen.

Erläuterung: An den HTTP-Proxy wurde eine HTTP-CONNECT-Anforderung gesendet, um einen SSL-Tunnel zum HTTP-Server zu erstellen. Der HTTP-Proxy hat auf diese Anforderung nicht mit **200 OK** geantwortet.

Benutzeraktion: Dies kann verschiedene Ursachen haben. Aktivieren Sie die Tracefunktion für die Route, und wiederholen Sie die Verbindungsanforderung. In der Tracedatei wird der tatsächliche Fehler angegeben.

| **MQCPE059 Es sind keine Schlüsselringdateien definiert.**

| **Erläuterung:** Es wurde ein SSL-Client oder -Server definiert, ohne dass mindestens eine Schlüsselringdatei angegeben wurde.

| **Benutzeraktion:** Definieren Sie über die Eigenschaften `SSLClientKeyRing` und `SSLClientCAKeyRing` auf der Clientseite oder `SSLServerKeyRing` und `SSLServerCAKeyRing` auf der Serverseite eine Schlüsselringdatei, und starten Sie die Route erneut.

| **MQCPE060 Laufzeitfehler beim Festlegen des Zeitlimits für die SSL-Clientverbindung auf {0} Sekunden.**

| **Erläuterung:** Beim Festlegen des Zeitlimits ist auf der Clientseite ein SSL-Laufzeitfehler aufgetreten.

| **Benutzeraktion:** Überprüfen Sie, ob der für die Eigenschaft `SSLClientConnectTimeout` angegebene Wert gültig

tig ist. Führen Sie einen Trace für die angegebene Route durch, um weitere Fehlerinformationen zu erhalten.

MQCPE061 Es sind keine Cipher Suites aktiviert.

Erläuterung: Eine SSL-Client- oder -Serververbindung wurde gestartet, MQIPT kann jedoch keine gültige Cipher Suite finden.

Benutzeraktion: Überprüfen Sie, ob die definierten Schlüsselringdateien gültige Zertifikate enthalten. Die privaten und öffentlichen Schlüssel zur Generierung der Zertifikate und der verwendete Verschlüsselungsalgorithmus müssen der Liste der unterstützten Cipher Suites, die im MQIPT-Buch aufgeführt ist, entsprechen.

MQCPE062 Laufzeitfehler beim Festlegen der SSL-Cipher Suite {0}.

Erläuterung: Auf der Client- oder Serverseite wurde eine SSL-Cipher Suite definiert, die nicht unterstützt wird.

Benutzeraktion: Überprüfen Sie, ob der Wert für SSLClientCipherSuites bzw. SSLServerCipherSuites gültig ist und für diese Verbindung unterstützt wird. Führen Sie einen Trace für die angegebene Route durch, um eine Liste mit den aktivierten Cipher Suites zu erhalten. Das MQIPT-Buch enthält eine Liste der unterstützten Cipher Suites.

MQCPE063 Die Datei {0} ist bereits vorhanden. Verwenden Sie die Ersetzungsoption.

Erläuterung: Der für das Script mqiptPW angegebene Dateinamenparameter ist bereits vorhanden.

Benutzeraktion: Wählen Sie einen anderen Dateinamen, oder verwenden Sie die Ersetzungsoption.

MQCPE064 Laufzeitfehler beim Generieren von Entschlüsselungsschlüsseln:\n {0}

Erläuterung: Beim Generieren von Chiffrierschlüsseln zum Entschlüsseln des Kennworts zum Öffnen einer Schlüsselringdatei ist ein Fehler aufgetreten.

Benutzeraktion: Beheben Sie den in der Nachricht angegebenen Laufzeitfehler, und führen Sie den Befehl erneut aus.

MQCPE065 Name des LDAP-Servers fehlt.

Erläuterung: Die Eigenschaft LDAPServer1 oder LDAPServer2 muss festgelegt werden, wenn die Eigenschaft LDAP auf **true** gesetzt wurde.

Benutzeraktion: Definieren Sie in der Konfigurationsdatei einen LDAP-Server (LDAPServer*) für die betreffende Route.

MQCPE066 LDAP-Kennwort für die Eigenschaft LDAPServer{0}Password fehlt.

Erläuterung: Es wurde eine LDAP-Benutzer-ID ohne ein Kennwort angegeben.

Benutzeraktion: Definieren Sie in der Konfigurationsdatei ein LDAP-Server-Kennwort (LDAPServer*Password) für die betreffende Route.

MQCPE067 Kein SSL-Client oder SSL-Server für LDAP-Server angegeben.

Erläuterung: Die Eigenschaft SSLClient oder SSLServer muss festgelegt werden, wenn die Eigenschaft LDAP auf **true** gesetzt ist.

Benutzeraktion: Definieren Sie in der Konfigurationsdatei einen SSL-Client oder SSL-Server für die betreffende Route.

MQCPE068 Name des Sicherheitsexits fehlt.

Erläuterung: Die Eigenschaft SecurityExitName (Name des Sicherheitsexits) muss festgelegt werden, wenn die Eigenschaft SecurityExit (Sicherheitsexit) auf **true** gesetzt ist.

Benutzeraktion: Definieren Sie in der Konfigurationsdatei einen Sicherheitsexitnamen für die betreffende Route.

MQCPE069 Ungültige Port-Adresse {0} in Sicherheitsexitantwort.

Erläuterung: Die für die Eigenschaft SecurityExitResponse (Antwort des Sicherheitsexits) angegebene Port-Adresse ist ungültig.

Benutzeraktion: Die Port-Adresse muss im Bereich von 1024 bis 65535 liegen.

MQCPE070 Unbekannter Ursachencode {0} in Sicherheitsexitantwort.

Erläuterung: Der für die Eigenschaft SecurityExitResponse (Antwort des Sicherheitsexits) angegebene Ursachencode wird nicht unterstützt.

Benutzeraktion: Im MQIPT-Buch finden Sie eine Liste der unterstützten Ursachencodes.

MQCPE071 Fehler beim Schreiben in {0}.

Erläuterung: Beim Erstellen oder Aktualisieren der angegebenen Datei ist ein Fehler aufgetreten. Die Fehlnachricht enthält auch die ausgegebene Ausnahmebedingung.

Benutzeraktion: Beheben Sie den in der Ausnahmebedingung angegebenen Fehler, und führen Sie den Befehl erneut aus.

MQCPE072 **Unbekannter Fehler in Sicherheitsexit {0}.**

Erläuterung: Bei der Prüfung einer Verbindungsanforderung ist in einem benutzerdefinierten Sicherheitsexit ein Fehler aufgetreten.

Benutzeraktion: Aktivieren Sie die Tracefunktion für den Sicherheitsexit, und wiederholen Sie die Verbindungsanforderung. Der Fehler wird in die Trace-Datei für den Sicherheitsexit eingetragen.

MQCPI001 **{0} wird gestartet.**

Erläuterung: Diese MQIPT-Instanz beginnt mit der Ausführung. Es werden weitere Initialisierungsnachrichten ausgegeben.

MQCPI002 **{0} wird beendet.**

Erläuterung: MQIPT wird beendet. Die Beendigung erfolgt entweder auf Grund eines Stoppbefehls (STOP) oder automatisch, wenn ein Konfigurationsfehler einen erfolgreichen Start bzw. eine erfolgreiche Aktualisierung (REFRESH) verhindert.

MQCPI003 **{0} wurde beendet.**

Erläuterung: Der Systemabschluss ist abgeschlossen. Alle MQIPT-Prozesse wurden beendet.

MQCPI004 **Die Konfigurationsdaten aus {0} werden gelesen.**

Erläuterung: Die MQIPT-Konfigurationsdatei `mqipt.conf` wird aus dem in dieser Nachricht angegebenen Verzeichnis gelesen.

MQCPI005 **Der Listener-Port ist als inaktiv markiert - {0} -> {1}({2})**

Erläuterung: Die in dieser Nachricht angegebene Route wurde als 'inaktiv' gekennzeichnet. Es werden keine Kommunikationsanforderungen von dieser Route akzeptiert.

MQCPI006 **Route {0} wird gestartet und leitet Nachrichten weiter an:**

Erläuterung: Eine Route wurde an dem in der Nachricht angegebenen Listener-Port gestartet. Auf diese Nachricht folgen weitere Nachrichten mit allen Eigenschaften, die für diese Route definiert sind. Nachricht MQCPI078 wird ausgegeben, wenn die Route zur Entgegennahme von Verbindungen bereit ist.

MQCPI007 **Route {0} wurde gestoppt.**

Erläuterung: Die an dem angegebenen Listener-Port aktive Route wurde gestoppt. Dieser Fall tritt ein, wenn ein Aktualisierungsbefehl (REFRESH) an MQIPT ausgegeben und die Routenkonfiguration geändert wurde.

MQCPI008 **Empfangsbereit für Steuerbefehle an Port {0}.**

Erläuterung: Diese MQIPT-Instanz ist an dem angegebenen Port empfangsbereit für Steuerbefehle.

MQCPI009 **Steuerbefehl empfangen: {0}**

Erläuterung: Diese Nachricht meldet, dass an dem angegebenen Befehls-Port ein Steuerbefehl empfangen wurde. Gegebenenfalls enthält die Nachricht weitere Angaben.

MQCPI010 **Befehls-Port für {0} wird gestoppt.**

Erläuterung: Nach einer Aktualisierung (REFRESH) wird der Befehls-Port in der neuen Konfiguration nicht mehr verwendet. Es werden keine Befehle mehr an dem angegebenen Port angenommen.

MQCPI011 **Die Protokolldateien werden im Pfad {0} gespeichert.**

Erläuterung: In der aktuellen Konfiguration werden Protokollausgaben an den in der Nachricht angegebenen Pfad übertragen.

Benutzeraktion: Dieser Pfad kann sich ändern, wenn die Konfiguration geändert und anschließend eine Aktualisierung (REFRESH) angefordert wird.

MQCPI012 **Eine Änderung des Wertes für die Mindestanzahl von Verbindungsthreads (MinConnectionThreads) wird erst nach dem erneuten Starten der Route wirksam.**

Erläuterung: Die Mindestanzahl von Verbindungsthreads werden einer Route bei deren Start zugeordnet. Dieser Wert kann erst wieder bei einem Neustart von MQIPT geändert werden.

MQCPI013 **Die Verbindung zwischen {0} und Host {1} wurde geschlossen.**

Erläuterung: Diese Nachricht wird in das Verbindungsprotokoll geschrieben, um einen Verbindungsvorgang aufzuzeichnen.

MQCPI014 Signalmarkierungsprotokoll ({0}) ist unbekannt.

Erläuterung: Diese Nachricht wird in das Verbindungsprotokoll geschrieben, um einen Verbindungsvorgang aufzuzeichnen.

MQCPI015 Clientzugriff wurde auf dieser Route inaktiviert.

Erläuterung: Diese Nachricht wird in das Verbindungsprotokoll geschrieben, um einen Verbindungsvorgang aufzuzeichnen.

MQCPI016 WS-Manager-Zugriff wurde auf dieser Route inaktiviert.

Erläuterung: Diese Nachricht wird in das Verbindungsprotokoll geschrieben, um einen Verbindungsvorgang aufzuzeichnen.

MQCPI017 Ein WS-Manager auf {0} wurde mit Host {1} verbunden.

Erläuterung: Diese Nachricht wird in das Verbindungsprotokoll geschrieben, um einen Verbindungsvorgang aufzuzeichnen.

MQCPI018 Ein Client auf {0} wurde mit Host {1} verbunden.

Erläuterung: Diese Nachricht wird in das Verbindungsprotokoll geschrieben, um einen Verbindungsvorgang aufzuzeichnen.

MQCPI019 {0} Routen wurden erstellt. Dies überschreitet die maximal unterstützte Anzahl von {1} Routen.

Erläuterung: Die Anzahl der maximal unterstützten Routen wurde überschritten.

Benutzeraktion: Der MQIPT-Betrieb wird fortgesetzt; es wird jedoch empfohlen, eine zweite MQIPT-Instanz zu erstellen und die Routen zwischen beiden aufzuteilen.

MQCPI020 Die Konfigurationsdatei wurde an den Verwaltungsclient gesendet.

Erläuterung: Die Konfigurationsdatei wurde auf Anforderung des Verwaltungsclients gesendet.

MQCPI021 Für den Befehls-Port wurde eine Kennwortprüfung aktiviert.

Erläuterung: Diese Nachricht weist darauf hin, dass für den Zugriff auf den Befehls-Port ein Kennwort erforderlich ist.

MQCPI022 Für den Befehls-Port wurde keine Kennwortprüfung aktiviert.

Erläuterung: Diese Nachricht weist darauf hin, dass für den Zugriff auf den Befehls-Port kein Kennwort erforderlich ist.

MQCPI024verwendet HTTP-Proxy {0}({1})

Erläuterung: Diese Nachricht gibt an, dass die abgehende Verbindung für diese Route über den angegebenen HTTP-Proxy erfolgt.

MQCPI025 Die vom Verwaltungsclient {0} angeforderte Aktualisierung ist beendet.

Erläuterung: Auf Grund eines Aktualisierungsbefehls (REFRESH) hat der MQIPT seine Konfigurationsdatei erneut gelesen und wurde anschließend erneut gestartet.

MQCPI026 Der Verwaltungsclient {0} hat die Beendigung des MQIPT angefordert.

Erläuterung: Auf Grund eines Stoppbefehls (STOP) wird der MQIPT beendet.

MQCPI027 {0} wurde gesendet an {1} über Port {2}.

Erläuterung: Diese Nachricht zeigt an, der Systemkonsole den Befehl an, der über die Zeilenmodusversion (nicht die GUI) des Verwaltungsclients an den angegebenen MQIPT gesendet wurde.

MQCPI031Cipher Suites {0}

Erläuterung: Diese Nachricht gibt die Cipher Suites an, die für diese Route verwendet werden.

MQCPI032Schlüsselringdatei {0}

Erläuterung: Diese Nachricht gibt den Namen der Schlüsselringdatei für diese Route an.

MQCPI033Clientauthentifizierung ist auf {0} gesetzt.

Erläuterung: Diese Nachricht gibt an, ob ein SSL-Server die Clientauthentifizierung für diese Route fordert.

MQCPI034 ...{0}({1})

Erläuterung: Diese Nachricht gibt die Zieladresse und den Ziel-Port dieser Route an.

MQCPI035verwendet {0}

Erläuterung: Diese Nachricht gibt das Protokoll an, das für diese Zieladresse verwendet wird. Hierbei kann es sich entweder um das MQSeries-Protokoll, HTTP-Tunnelung oder HTTP-Chunking handeln.

MQCPI036SSL-Clientseite mit folgenden Eigenschaften aktiviert:

Erläuterung: Diese Nachricht gibt an, dass die Route die Daten über SSL an den Zielhost sendet.

MQCPI037SSL-Serverseite mit folgenden Eigenschaften aktiviert:

Erläuterung: Diese Nachricht gibt an, dass die Route die Daten über SSL vom sendenden Host empfängt.

MQCPI038Peer-Zertifikat verwendet {0}.

Erläuterung: Diese Nachricht listet die registrierten Namen auf, die zur Steuerung der Authentifizierung von Peer-Zertifikaten verwendet werden.

MQCPI039über SOCKS-Proxy {0}({1})

Erläuterung: Diese Nachricht gibt an, dass die abgehende Verbindung für diese Route über den angegebenen SOCKS-Proxy erfolgt, der beim Start von MQIPT über die Befehlszeile definiert wird.

MQCPI040 Der Verwaltungsclient {0} hat auf den Befehls-Port zugegriffen.

Erläuterung: Diese Nachricht wird an die Systemkonsole und an die MQIPT-Protokolldatei ausgegeben, sofern die Protokollfunktion aktiviert wurde. Der MQIPT hat eine Verbindung vom Verwaltungsclient empfangen.

MQCPI041antwortet auf Anforderungen des Network Dispatcher Advisor im {0}-Modus.

Erläuterung: Diese Nachricht wird beim Start einer Route an die Systemkonsole ausgegeben. Sie gibt den Modus an, den MQIPT für Antworten an den Advisor des Network Dispatcher verwendet. Zulässig sind die Optionen 'Normal' und 'Replace'.

MQCPI042 Die maximale Anzahl Verbindungen auf Route {0} wurde erreicht. Weitere Anforderungen werden blockiert.

Erläuterung: Diese Nachricht wird an die Systemkonsole ausgegeben, wenn die maximal zulässige Anzahl an Verbindungen für eine gegebene Route erreicht wurde. Weitere Anforderungen werden blockiert, bis eine Verbindung freigegeben wird oder der Wert von MaxConnectionThreads (Maximale Anzahl Ver-

bindungs-Threads) erhöht wird.

MQCPI043 Die Blockierung von Verbindungen auf Route {0} wurde aufgehoben.

Erläuterung: Diese Nachricht wird an die Systemkonsole ausgegeben, wenn die angegebene Route wieder Verbindungsanforderungen akzeptiert.

MQCPI044 MQIPT wurde beim Systemstart gestartet.

Erläuterung: MQIPT wurde als Systemservice gestartet.

MQCPI045 MQIPT wird beim Systemstart gestartet.

Erläuterung: MQIPT wird als Systemservice gestartet.

MQCPI046 Inaktivierung für {0} Sekunden, während MQIPT beim Systemstart gestartet wird.

Erläuterung: Dieser Fork-Prozess (Aufspaltungsprozess) wird für die angegebene Dauer inaktiviert, wenn MQIPT erfolgreich als Systemservice gestartet wurde.

MQCPI047CA-Schlüsselringdatei {0}

Erläuterung: Diese Nachricht gibt den Namen der CA-Schlüsselringdatei für diese Route an.

MQCPI048 Ping durch Verwaltungsclient {0} ist beendet.

Erläuterung: Antwortnachricht vom IPTController an den Verwaltungsclient.

MQCPI049QoS-Priorität für Zieladresse = {0}, für Anrufer = {1}

Erläuterung: Diese Nachricht gibt die Priorität des Datenverkehrs in beide Richtungen auf dieser Route an.

MQCPI050 Eintrag zum automatischen Starten von MQIPT beim Systemstart wird zur init-tab hinzugefügt.

Erläuterung: Der Benutzer hat das Script `mqiptService` ausgeführt, um MQIPT als Systemservice zu starten.

MQCPI051 Eintrag zum automatischen Starten von MQIPT beim Systemstart wird aus init-tab entfernt.

Erläuterung: Der Benutzer hat das Script `mqiptService` ausgeführt, damit MQIPT nicht mehr als Systemservice gestartet wird.

MQCPI052Socks-Serverseite aktiviert

Erläuterung: Diese Route wird als SOCKS-Server (Proxy) fungieren und Verbindungen von einer SOCKS-fizierten Anwendung annehmen.

MQCPI053 Java Security Manager wird gestartet.

Erläuterung: Der standardmäßige Java Security Manager wird gestartet, da die Eigenschaft `SecurityManager` (Sicherheitsmanager) auf `true` gesetzt ist.

MQCPI054 Java Security Manager wird gestoppt.

Erläuterung: Der standardmäßige Java Security Manager wird gestoppt, da die Eigenschaft `SecurityManager` (Sicherheitsmanager) auf `false` gesetzt wurde.

MQCPI055 Die Richtlinie für den Java Security Manager (`java.security.policy`) wird auf {0} gesetzt.

Erläuterung: Der standardmäßige Java Security Manager soll gestartet werden und wird die übergebene Richtliniendatei verwenden.

MQCPI056 Der Java Security Manager muss erneut gestartet werden, damit er die neue Richtliniendatei verwendet.

Erläuterung: Die Eigenschaft `SecurityManagerPolicy` (Richtlinie für Sicherheitsmanager) wurde geändert; die Änderung wird jedoch erst bei einem Neustart des Java Security Manager wirksam.

Benutzeraktion: Setzen Sie die Eigenschaft **SecurityManager** (Sicherheitsmanager) auf `false`, geben Sie einen Aktualisierungsbefehl (REFRESH) ein, und stoppen Sie den Java Security Manager. Setzen Sie anschließend **SecurityManager** wieder auf `true`, geben Sie einen weiteren Aktualisierungsbefehl (REFRESH) ein, und starten Sie den Java Security Manager mit der neuen Richtliniendatei.

MQCPI057Tracestufe {0} aktiviert

Erläuterung: Diese Nachricht wird beim Start einer Route an die Systemkonsole ausgegeben. Sie gibt die Tracestufe an, die für diese Route aktiviert wurde.

MQCPI058und URI-Name {0}

Erläuterung: Diese Nachricht wird beim Start einer Route an die Systemkonsole ausgegeben. Sie gibt den URI-Namen für diese Route an.

MQCPI059Servlet-Client aktiviert

Erläuterung: Diese Nachricht wird beim Start einer Route an die Systemkonsole ausgegeben. Diese Route wird eine Verbindung zum MQIPT-Servlet herstellen.

MQCPI060 Die Dateien zum automatischen Starten von MQIPT beim Systemstart werden installiert.

Erläuterung: Der Benutzer hat das Script `mqiptService` ausgeführt, um MQIPT als Systemservice zu starten.

MQCPI061 Die Dateien zum automatischen Starten von MQIPT beim Systemstart werden entfernt.

Erläuterung: Der Benutzer hat das Script `mqiptService` ausgeführt, damit MQIPT nicht mehr als Systemservice gestartet wird.

MQCPI064keine SSL-Authentifizierung für diese Route

Erläuterung: Diese Nachricht wird beim Start einer Route an die Systemkonsole ausgegeben; sie gibt an, dass für diese Route keine SSL-Authentifizierung verwendet wird, da eine anonyme Cipher Suite angegeben wurde.

MQCPI065im SSL-Proxy-Modus

Erläuterung: Diese Nachricht wird beim Start einer Route an die Systemkonsole ausgegeben und gibt an, dass diese Route im SSL-Proxy-Modus arbeitet.

MQCPI066und HTTP-Server an {0}{1}

Erläuterung: Diese Nachricht gibt an, dass die abgehende Verbindung für diese Route über den angegebenen HTTP-Server erfolgt.

MQCPI067 Verknüpfungen zu den TQoS-Laufzeitbibliotheken werden eingerichtet.

Erläuterung: Der Benutzer hat das Script `mqiptQoS` ausgeführt, um Verknüpfungen zu den echten TQoS-Laufzeitbibliotheken herzustellen.

MQCPI068 Verknüpfungen zu den TQoS-Laufzeitbibliotheken werden entfernt.

Erläuterung: Der Benutzer hat das Script `mqiptQoS` ausgeführt, um Verknüpfungen zu den echten TQoS-Laufzeitbibliotheken zu entfernen.

<p>MQCPI069Bindung zur lokalen Adresse {0}</p> <p>Erläuterung: Diese Nachricht zeigt die lokale IP-Adresse an, an die jede einzelne Verbindung gebunden ist. Sie sollten nur auf einem Multihomed-System verwendet werden.</p>	<p>MQCPI079Verwendung von Sicherheitsexit {0}</p> <p>Erläuterung: Diese Nachricht wird beim Start einer Route an der Systemkonsole ausgegeben. Dabei wird der vollständig qualifizierte Name des Sicherheitsexits angezeigt.</p>
<p>MQCPI070Verwendung des Bereichs {0}-{10} für lokale Port-Adresse</p> <p>Erläuterung: Diese Nachricht zeigt die lokalen Port-Adressen an, die für eine Verbindung verwendet werden. Dies gibt Firewall-Administratoren die Möglichkeit, Verbindungen von MQIPT einzuschränken.</p>	<p>MQCPI080und Zeitlimit von {0} Sekunden</p> <p>Erläuterung: Diese Nachricht wird beim Start einer Route an der Systemkonsole ausgegeben. Dabei wird das Zeitlimit des Sicherheitsexits angezeigt.</p>
<p>MQCPI071 Sitezertifikat verwendet {0}.</p> <p>Erläuterung: Diese Nachricht listet die registrierten Namen auf, die zur Steuerung der Auswahl eines Sitezertifikats verwendet werden.</p>	<p>MQCPI081 Startnachricht für WebSphere MQ Internet Pass-Thru</p> <p>Erläuterung: Startnachricht für WebSphere MQ Internet Pass-Thru als Dienst</p>
<p>MQCPI072und Zertifikatsbezeichnung {0}</p> <p>Erläuterung: Diese Nachricht listet die Bezeichnungen auf, die zur Steuerung der Auswahl eines Sitezertifikats verwendet werden.</p>	<p>MQCPI082 Stoppnachricht für WebSphere MQ Internet Pass-Thru</p> <p>Erläuterung: Stoppnachricht für WebSphere MQ Internet Pass-Thru als Dienst</p>
<p>MQCPI073 Datei {0} wurde aktualisiert.</p> <p>Erläuterung: Der für das Script mqiptPW angegebene Dateiname wurde aktualisiert.</p>	<p>MQCPI083Aktualisierungsbefehle starten die Route nicht erneut.</p> <p>Erläuterung: Diese Nachricht gibt an, dass die Route nach der Ausgabe eines Aktualisierungsbefehls (REFRESH) nicht erneut gestartet wird.</p>
<p>MQCPI074 Datei {0} wurde erstellt.</p> <p>Erläuterung: Der für das Script mqiptPW angegebene Dateiname wurde erstellt.</p>	<p>MQCPI084Gültigkeitsdauer für CRL im Cache beträgt {0} Stunden.</p> <p>Erläuterung: Diese Konsolnachricht zeigt die Gültigkeitsdauer einer CRL (bzw. ARL) im MQIPT-Cache an.</p>
<p>MQCPI075LDAP-Hauptserver an {0}({1})</p> <p>Erläuterung: Diese Nachricht gibt den Namen des LDAP-Hauptservers für die CRL-Unterstützung an.</p>	<p>MQCPI085CRLs werden in Schlüsselringdatei(en) gespeichert.</p> <p>Erläuterung: Diese Konsolnachricht bedeutet, dass alle von einem LDAP-Server empfangenen CRLs (bzw. ARLs) in der Schlüsselringdatei, die an das zugeordnete CA-Zertifikat angehängt ist, gespeichert wird.</p>
<p>MQCPI076LDAP-Ausweichserver an {0}({1})</p> <p>Erläuterung: Diese Nachricht gibt den Namen des LDAP-Ausweichservers für die CRL-Unterstützung an.</p>	<p>MQCPI086Zeitlimit: {0} Sekunden</p> <p>Erläuterung: Diese Nachricht wird beim Start einer Route an der Systemkonsole ausgegeben. Dabei wird das Zeitlimit für die Herstellung einer Verbindung mit dem LDAP-Server angezeigt.</p>
<p>MQCPI077LDAP-Fehler werden ignoriert.</p> <p>Erläuterung: Diese Nachricht bedeutet, dass alle von LDAP empfangenen Fehler ignoriert werden.</p>	<p>MQCPI087Benutzer-ID: {0}</p> <p>Erläuterung: Diese Nachricht wird beim Start einer Route an der Systemkonsole ausgegeben. Dabei wird die Benutzer-ID für die Herstellung einer Verbindung mit dem LDAP-Server angezeigt.</p>
<p>MQCPI078 Route {0} für Verbindungsanforderungen bereit.</p> <p>Erläuterung: Diese Nachricht wird angezeigt, wenn eine Route zur Entgegennahme von Verbindungsanforderungen bereit ist.</p>	

MQCPI100	Dieses Script startet {0}.	MQCPI112	Dabei entspricht Nachrichten_ID einem Schlüssel in der Datei mqipt.properties.
Erläuterung:	Onlinehilfenachricht von Script mqipt.	Erläuterung:	Onlinehilfenachricht von der Klasse IPT- Messages.
MQCPI101	Das Befehlsformat lautet:	MQCPI113	Dieses Script dient zur Verwaltung von MQIPT als Systemservice.
Erläuterung:	Onlinehilfenachricht von Script mqipt.	Erläuterung:	Onlinehilfenachricht von Script mqipt- Service.
MQCPI102	mqipt {Verzeichnisname}	MQCPI114	mqiptService (-install -remove)
Erläuterung:	Onlinehilfenachricht von Script mqipt.	Erläuterung:	Onlinehilfenachricht von Script mqipt- Service.
MQCPI103	Verzeichnisname - Verzeichnis, in dem sich mqipt.conf befindet	MQCPI115	-install: Installiert die Dateien zum automatischen Starten von MQIPT beim Systemstart
Erläuterung:	Onlinehilfenachricht von Script mqipt.	Erläuterung:	Onlinehilfenachricht von Script mqipt- Service.
MQCPI106	Dieses Script dient zur Anzeige der aktuellen Versionsnummer.	MQCPI116	-remove: Entfernt die Dateien zum automatischen Starten von MQIPT beim Systemstart
Erläuterung:	Onlinehilfenachricht von Script mqipt- Version.	Erläuterung:	Onlinehilfenachricht von Script mqipt- Service.
MQCPI107	mqiptVersion {-v}	MQCPI117	Dieses Script wird zur Verwaltung von Verknüpfungen zu TQoS-Laufzeitbibliotheken verwendet.
Erläuterung:	Onlinehilfenachricht von Script mqipt- Version.	Erläuterung:	Onlinehilfenachricht von Script mqipt- Service.
MQCPI108	Bei Angabe von -v wird auch das Build-Datum angezeigt.	MQCPI118	mqiptQoS (-install -remove)
Erläuterung:	Onlinehilfenachricht von Script mqipt- Version.	Erläuterung:	Onlinehilfenachricht von Script mqipt- Service.
MQCPI109	Dieses Script startet {0} beim Systemstart in einer anderen JVM und wird nur in mqipt.ske verwendet. Verwenden Sie das Script 'mqipt', um MQIPT über die Befehlszeile zu starten.	MQCPI119	-install: Richtet Verknüpfungen zu den echten TQoS-Laufzeitbibliotheken ein.
Erläuterung:	Onlinehilfenachricht von Script mqipt- Fork.	Erläuterung:	Onlinehilfenachricht von Script mqipt- Service.
MQCPI110	Diese Klasse zeigt eine einfache Nachricht in der Landessprache an der Konsole an.	MQCPI120	-remove: Entfernt Verknüpfungen zu den echten TQoS-Laufzeitbibliotheken.
Erläuterung:	Onlinehilfenachricht von der Klasse IPT- Messages.	Erläuterung:	Onlinehilfenachricht von Script mqipt- Service.
MQCPI111	java com.ibm.mq.ippt.IPTMessages (Nachrichten_ID1) {Nachrichten_ID2} {Nachrichten_ID...}		
Erläuterung:	Onlinehilfenachricht von der Klasse IPT- Messages.		

| MQCPI121 Verwenden Sie dieses Script, um ein
| Kennwort zu verschlüsseln und in einer
| Datei zu speichern.

| **Erläuterung:** Onlinehilfenachricht von Script
| mqiPTPW.

| MQCPI122 mqiPTPW Kennwort Dateiname { -re-
| place }

| **Erläuterung:** Onlinehilfenachricht von Script
| mqiPTPW.

| MQCPI123 Kennwort - Kennwort zum Öffnen einer
| Schlüsselringdatei.

| **Erläuterung:** Onlinehilfenachricht von Script
| mqiPTPW.

| MQCPI124 Dateiname - Verschlüsseltes Kennwort
| wird in dieser Datei gespeichert.

| **Erläuterung:** Onlinehilfenachricht von Script
| mqiPTPW.

| MQCPI125 Zur Aktualisierung einer vorhandenen
| Datei muss die Ersetzungsoption (-re-
| place) verwendet werden.

| **Erläuterung:** Onlinehilfenachricht von Script
| mqiPTPW.

| MQCPI126 mqiPT (-start | -stop)

| **Erläuterung:** Onlinehilfenachricht von Script mqiPT-
| QoS.

| MQCPW001 CRL für {0} abgelaufen.

| **Erläuterung:** Diese Nachricht wird angezeigt, wenn
| eine CRL (bzw. ARL) von einem LDAP-Server oder
| einer Schlüsselringdatei empfangen wird.

| **Benutzeraktion:** Aktualisieren Sie die angegebene
| CRL auf dem LDAP-Server oder in der Schlüsselring-
| datei.

| MQCPW002 Fehler beim Aktualisieren einer CRL in
| Schlüsselringdatei {0}.

| **Erläuterung:** Diese Nachricht wird angezeigt, wenn
| die Eigenschaft LDAPSaveCRLs aktiviert ist, aber die
| angegebene Schlüsselringdatei nicht aktualisiert werden
| kann.

| **Benutzeraktion:** Die angegebene Datei ist möglicher-
| weise beschädigt. Gehen Sie wie folgt vor:

- | 1. Prüfen Sie, ob Schreibzugriff für MQIPT aktiviert
| ist.
- | 2. Prüfen Sie, ob eine andere Anwendung die Datei
| geöffnet hat.

| MQCPW003Abgelaufene CRLs werden ignoriert.

| **Erläuterung:** Diese Konsolnachricht bedeutet, dass alle
| abgelaufenen CRLs (bzw. ARLs) ignoriert und die
| Verbindungsanforderung möglicherweise zugelassen
| wird.

Anhang. Bemerkungen

Hinweise auf IBM Produkte, Programme und Dienstleistungen in dieser Veröffentlichung bedeuten nicht, dass IBM diese in allen Ländern, in denen IBM vertreten ist, anbietet.

Hinweise auf IBM Lizenzprogramme oder andere IBM Produkte bedeuten nicht, dass nur Programme, Produkte oder Dienstleistungen von IBM verwendet werden können. Anstelle der IBM Produkte können auch andere ihnen äquivalente Programme verwendet werden, solange diese keine gewerblichen Schutzrechte verletzen. Die Verantwortung für den Betrieb der Produkte in Verbindung mit Fremdprodukten liegt beim Kunden, soweit solche Verbindungen nicht ausdrücklich von IBM bestätigt sind.

Für in diesem Handbuch beschriebene Erzeugnisse und Verfahren kann es IBM Patente oder Patentanmeldungen geben. Mit der Auslieferung dieses Handbuchs ist keine Lizenzierung dieser Patente verbunden. Lizenzanfragen sind schriftlich an IBM Europe, Director of Licensing, 92066 Paris La Defense Cedex, France, zu richten.

Die Informationen in diesem Dokument wurden noch keinem formalen Test durch IBM unterzogen. IBM gibt daher keine Garantie für die Richtigkeit der in diesem Handbuch enthaltenen Daten. Die Verantwortlichkeit für die Verwendung dieser Informationen oder der Implementierung einer der Funktionen liegt beim Kunden. Obwohl die Korrektheit der einzelnen Funktionen unter Umständen von IBM in einer bestimmten Situation geprüft wurde, kann nicht gewährleistet werden, dass dieselben oder ähnliche Ergebnisse in einer anderen Umgebung erzielt werden. Das Anpassen dieser Funktionen an die kundeneigenen Umgebungen erfolgt auf Risiko des Kunden.

Marken

Folgende Namen sind in gewissen Ländern Marken der IBM Corporation:

AIX	FFST	First Failure Support Technology
IBM SupportPac	IBMLink WebSphere	MQSeries

Microsoft, Windows, Windows NT und das Windows Logo sind in gewissen Ländern Marken der Microsoft Corporation.

Java und alle Java-basierten Marken sind in gewissen Ländern Marken der Sun Microsystems.

UNIX ist in gewissen Ländern eine registrierte Marke von The Open Group.

Andere Namen von Unternehmen, Produkten oder Dienstleistungen können Marken oder Dienstleistungsmarken anderer Unternehmen sein.

Literaturverzeichnis

Das vorliegende Handbuch wird bei Installation des Produkts im HTML-Format zur Verfügung gestellt. Die HTML-Datei befindet sich in einer selbstextrahierenden Zip-Datei im Verzeichnis `doc\<Ländereinstellung>\html\<Dateiname>.zip`. Vor der Verwendung des Verwaltungsclients müssen Sie die Datei im Unterverzeichnis `<Ländereinstellung>/html` entpacken. Die folgende Tabelle gibt einen Überblick über die Sprachen, in denen das Handbuch vorliegt, und die entsprechenden Dateinamen:

Tabelle 4. Sprachen und Dateinamen - Übersicht

Sprache	Länder-einstellung	Name der HTML-Datei
Vereinfachtes Chinesisch	zn_CN	amqyzb01.zip
Deutsch	de_DE	amqygb01.zip
Japanisch	ja_JP	amqyjb01.zip
Koreanisch	ko_KR	amqykb01.zip
Brasilianisches Portugiesisch	pt_BR	amqybb01.zip
Spanisch	es_ES	amqysb01.zip
Amerikanisches Englisch	en_US	amqyab01.zip

Übersetzte PDF-Dateien können von folgender Website heruntergeladen werden:
<http://www.ibm.com/webspheremq/downloads>

Folgende Sprachen stehen zur Verfügung:

Tabelle 5. PDF-Sprachen und -Dateinamen

Sprache	Länder-einstellung	Name der PDF-Datei
Vereinfachtes Chinesisch	zn_CN	amqyzb01.pdf
Deutsch	de_DE	amqygb01.pdf
Japanisch	ja_JP	amqyjb01.pdf
Koreanisch	ko_KR	amqykb01.pdf
Brasilianisches Portugiesisch	pt_BR	amqybb01.pdf
Spanisch	es_ES	amqysb01.pdf
Amerikanisches Englisch	en_US	amqyab01.pdf

Darüber hinaus sind die folgenden Veröffentlichungen hilfreich:

- *WebSphere MQ Intercommunication*, SC34-6059
- *WebSphere MQ System Administration Guide*, SC34-6068
- *WebSphere MQ Clients*, GC34-6058
- *Cluster-Unterstützung in WebSphere MQ*, SC12-2640

Diese Bücher enthalten Informationen zur Definition von WebSphere MQ-Kanälen und von deren Attributen, insbesondere zur Definition von CON-NAME.

Diese WebSphere MQ-Veröffentlichungen können von der folgenden Website heruntergeladen werden:
<http://www.ibm.com/webspheremq/library>

Index

A

AccessPW, Eigenschaft 81
Active, Konfigurationseigenschaft 82
Adresssteuerung, Ports 39
Advanced Encryption Standard 21
AES 21
AIX
MQIPT automatisch starten 57
MQIPT-Dateien herunterladen 55
MQIPT-Dateien installieren 55
MQIPT deinstallieren 58
MQIPT einrichten 56
MQIPT installieren 55
MQIPT über die Befehlszeile starten 56
Verwaltungsclient über die Befehlszeile starten 57
Allgemeine Probleme 153
Ausführungstracefunktion 155
Automatisch starten, MQIPT
Fehler 155

B

Beendigung 43
Beispielkonfigurationen 1, 98
Apache, rewrite 140
dynamischer Exit bei nur einer Route 149
HTTP-Proxy-Konfiguration 105
HTTPS-Konfiguration 122
Installationsfunktionstest (IVT) 99
LDAP-Server verwenden 134
MQIPT-Servlet konfigurieren 119
Port-Adressen zuordnen 132
Quality of Service (QoS) konfigurieren 110
Schlüsselringdatei erstellen 130
Sicherheitsexit 143
Sicherheitsexit weiterleiten 145
SOCKS-Client konfigurieren 116
SOCKS-Proxy konfigurieren 113
SSL-Clientauthentifizierung 102
SSL-Proxy-Modus 137
SSL-Serverauthentifizierung 100
SSL-Testzertifikate erstellen 118
Unterstützung für MQIPT-Clustering konfigurieren 126
Zugriffssteuerung konfigurieren 107

C

Chunking, HTTP 9
Cipher Suites 15
Client-/Serverkanäle 8
ClientAccess, Konfigurationseigenschaft 82
Clustering 13
Clustersender-
/Clusterempfängerkanäle 8

CommandPort, Konfigurationseigenschaft 81
ConnectionLog, Konfigurationseigenschaft 81

D

Demilitarized Zone, MQIPT mit 2
Denial-of-Service-Attacken 41
Destination, Konfigurationseigenschaft 82
DestinationPort, Konfigurationseigenschaft 82
Dienststeuerungsprogramm, Windows 50
Durchgehende Verbindungen
Fehler 155
Durchsatzverbesserung 156

E

Eigenschaften
Abschnitt 'global' 81
Abschnitt 'route' 82
neue 45
Übersicht 77
Einführung 1
Einsatzmöglichkeiten für MQIPT 1
Erste Schritte mit MQIPT 97

F

Fehlerbedingungen 43
Fehlerbestimmung 153
Fehlerisolierung 153
Fehlermeldung 156
FFST-Berichte 154

G

Generisch
MQIPT automatisch starten 70
MQIPT-Dateien herunterladen 67
MQIPT-Dateien installieren 67
MQIPT deinstallieren 70
MQIPT einrichten 68
MQIPT installieren 67
MQIPT über die Befehlszeile starten 69
Verwaltungsclient über die Befehlszeile starten 70

H

Handshake 16
Herunterladen, MQIPT-Dateien
unter AIX 55
unter HP-UX 59
unter Linux 63

Herunterladen, MQIPT-Dateien (*Forts.*)
unter Sun Solaris 51
unter Windows 47

HP-UX

MQIPT automatisch starten 61
MQIPT-Dateien herunterladen 59
MQIPT-Dateien installieren 59
MQIPT deinstallieren 62
MQIPT einrichten 60
MQIPT installieren 59
MQIPT über die Befehlszeile starten 60
Verwaltungsclient über die Befehlszeile starten 62

HTTP, Konfigurationseigenschaft 82
HTTP-Tunnelung, MQIPT mit 2
HTTP-Unterstützung 9
HTTPChunking, Konfigurationseigenschaft 83
HTTPProxy, Konfigurationseigenschaft 83
HTTPProxyPort, Konfigurationseigenschaft 83
HTTPS 10
HTTPS, Konfigurationseigenschaft 83
HTTPServer, Konfigurationseigenschaft 83
HTTPServerPort, Konfigurationseigenschaft 83

I

IdleTimeout, Konfigurationseigenschaft 84
IgnoreExpiredCRLs, Konfigurationseigenschaft 84
Installationsfunktionstest (IVT) 99
Installieren, MQIPT-Dateien
unter AIX 55
unter HP-UX 59
unter Linux 63
unter Sun Solaris 51
unter Windows 47

J

Java Security Manager 31

K

Kanalkonzentrator, MQIPT als 1
KeyMan 22
FAQ (Häufig gestellte Fragen) 25
unterstützte Standarddatenformate 24
unterstützte Tokens 23
Konfiguration
Datei, Zugriffsschutz 41
Eigenschaften, Übersicht 77
Referenzinformationen 76

Konfiguration (*Forts.*)
Referenzinformationen zu Eigenschaften 81
Standardkonfigurationsdatei 77
Verwaltungsclient verwenden 71
Zeilenmodusbefehle verwenden 75

L

LDAP, Konfigurationseigenschaft 84
LDAP und CRLs 20
LDAPCacheTimeout, Konfigurationseigenschaft 84
LDAPIgnoreErrors, Konfigurationsfehler 84
LDAPSaveCRL, Konfigurationseigenschaft 84
LDAPServer1, Konfigurationseigenschaft 85
LDAPServer1Password, Konfigurationseigenschaft 85
LDAPServer1Port, Konfigurationseigenschaft 85
LDAPServer1Timeout, Konfigurationseigenschaft 85
LDAPServer1Userid, Konfigurationseigenschaft 85
LDAPServer2, Konfigurationseigenschaft 85
LDAPServer2Password, Konfigurationseigenschaft 86
LDAPServer2Port, Konfigurationseigenschaft 85
LDAPServer2Timeout, Konfigurationseigenschaft 86
LDAPServer2Userid, Konfigurationseigenschaft 85
Linux
MQIPT automatisch starten 65
MQIPT-Dateien herunterladen 63
MQIPT-Dateien installieren 63
MQIPT deinstallieren 66
MQIPT einrichten 64
MQIPT installieren 63
MQIPT über die Befehlszeile starten 65
Verwaltungsclient über die Befehlszeile starten 66
ListenerPort, Konfigurationseigenschaft 86
Literaturverzeichnis 179
LocalAddress, Konfigurationseigenschaft 86
LogDir, Konfigurationseigenschaft 86

M

MaxConnectionThreads, Konfigurationseigenschaft 86
MaxLogFileSize, Konfigurationseigenschaft 81
MinConnectionThreads, Konfigurationseigenschaft 86
MQIPT automatisch starten
unter AIX 57
unter generischem UNIX 70

MQIPT automatisch starten (*Forts.*)
unter HP-UX 61
unter Linux 65
MQIPT-Dateien herunterladen
unter generischem UNIX 67
MQIPT-Dateien installieren
unter generischem UNIX 67
MQIPT deinstallieren
unter AIX 58
unter generischem UNIX 70
unter HP-UX 62
unter Linux 66
unter Sun Solaris 54
unter Windows 50
MQIPT einrichten
generisch 68
unter AIX 56
unter HP-UX 60
unter Linux 64
unter Sun Solaris 52
unter Windows 48
MQIPT über die Befehlszeile starten
unter generischem UNIX 69
Multihomed-Systeme 39

N

Nachrichten 157
Nachrichtensicherheit 43
Name, Konfigurationseigenschaft 87
Navigations- und Aufrufmöglichkeiten-viii
NDAdvisor, Eigenschaft 87
NDAdvisorReplaceMode, Eigenschaft 87
Network Dispatcher 29
Normale Beendigung 43

O

OutgoingPort, Konfigurationseigenschaft 87

P

PKCS#10 24
PKCS#11-Repositorys (CryptoKi) 23
PKCS#12 24
PKCS#12-Token 23
PKCS#7 24
PKCS#7-Token 23
Port 39
Port-Adresssteuerung 39
Protokollweiterleitung durch MQIPT 7

Q

QMgrAccess, Konfigurationseigenschaft 87
QoS, Konfigurationseigenschaft 87
QoS (Servicequalität) 27
QoSToCaller, Konfigurationseigenschaft 88
QoSToDest, Konfigurationseigenschaft 88

R

REFRESH, Zeilenmodusbefehl 76
RemoteShutDown, Konfigurationseigenschaft 81
Requester-/Senderkanäle 8
Requester-/Serverkanäle 8
RouteRestart, Konfigurationseigenschaft 88

S

Schlüsselringdatei
Kennwort verschlüsseln 22
Zertifikate auswählen 22
SecurityExit, Konfigurationseigenschaft 88
SecurityExitName, Konfigurationseigenschaft 88
SecurityExitPath, Konfigurationseigenschaft 88
SecurityExitTimeout, Konfigurationseigenschaft 88
SecurityManager, Konfigurationseigenschaft 81
SecurityManagerPolicy, Konfigurationseigenschaft 82
Sender-/Empfängerkanäle 8
Server-/Empfängerkanäle 8
Server-/Requester-Kanäle 8
Servlet 10
ServletClient, Konfigurationseigenschaft 88
Sicherheit von Nachrichten 43
Sicherheitsexit
com.ibm.mq.ipt.SecurityExit, Klasse 34
com.ibm.mq.ipt.SecurityExitResponse, Klasse 37
Tracefunktion 38
Übersicht 32
Sicherheitsüberlegungen, weitere 41
Sicherung von Dateien 153
Socks-Unterstützung 13
SocksClient, Konfigurationseigenschaft 89
SocksProxyHost, Konfigurationseigenschaft 89
SocksProxyPort, Konfigurationseigenschaft 89
SocksServer, Konfigurationseigenschaft 89
SPKAC 24
SSL-Übersicht 15
SSL-Unterstützung 15
Advanced Encryption Standard 21
AES 21
Beispiel 3
Fehlernachrichten 18
Handshake 16
LDAP und CRLs 20
testen 18
Vertrauenseinstellungen 17
WebSphere MQ Internet Pass-Thru und SSL 17
SSLClient, Konfigurationseigenschaft 89

- SSLClientCAKeyRing, Konfigurationseigenschaft 90
- SSLClientCAKeyRingPW, Konfigurationseigenschaft 90
- SSLClientCipherSuites, Konfigurationseigenschaft 90
- SSLClientConnectTimeout, Eigenschaft 90
- SSLClientDN_C, Konfigurationseigenschaft 90
- SSLClientDN_CN, Konfigurationseigenschaft 90
- SSLClientDN_L, Konfigurationseigenschaft 91
- SSLClientDN_O, Konfigurationseigenschaft 91
- SSLClientDN_OU, Konfigurationseigenschaft 91
- SSLClientDN_ST, Konfigurationseigenschaft 91
- SSLClientKeyRing, Konfigurationseigenschaft 91
- SSLClientKeyRingPW, Konfigurationseigenschaft 91
- SSLClientSiteDN_C, Konfigurationseigenschaft 92
- SSLClientSiteDN_CN, Konfigurationseigenschaft 92
- SSLClientSiteDN_L, Konfigurationseigenschaft 92
- SSLClientSiteDN_O, Konfigurationseigenschaft 92
- SSLClientSiteDN_OU, Konfigurationseigenschaft 92
- SSLClientSiteDN_ST, Konfigurationseigenschaft 92
- SSLClientSiteLabel, Konfigurationseigenschaft 92
- SSLProxyMode, Konfigurationseigenschaft 93
- SSLServer, Konfigurationseigenschaft 93
- SSLServerAskClientAuth, Konfigurationseigenschaft 93
- SSLServerCAKeyRing, Konfigurationseigenschaft 93
- SSLServerCAKeyRingPW, Konfigurationseigenschaft 93
- SSLServerCipherSuites, Konfigurationseigenschaft 94
- SSLServerDN_C, Konfigurationseigenschaft 94
- SSLServerDN_CN, Konfigurationseigenschaft 94
- SSLServerDN_L, Konfigurationseigenschaft 94
- SSLServerDN_O, Konfigurationseigenschaft 94
- SSLServerDN_OU, Konfigurationseigenschaft 94
- SSLServerDN_ST, Konfigurationseigenschaft 95
- SSLServerKeyRing, Konfigurationseigenschaft 95
- SSLServerKeyRingPW, Konfigurationseigenschaft 95
- SSLServerSiteDN_C, Konfigurationseigenschaft 95

- SSLServerSiteDN_CN, Konfigurationseigenschaft 95
- SSLServerSiteDN_L, Konfigurationseigenschaft 95
- SSLServerSiteDN_O, Konfigurationseigenschaft 95
- SSLServerSiteDN_OU, Konfigurationseigenschaft 96
- SSLServerSiteDN_ST, Konfigurationseigenschaft 96
- SSLServerSiteLabel, Konfigurationseigenschaft 96
- Starten, MQIPT automatisch
 - unter Sun Solaris 53
- Starten, MQIPT über die Befehlszeile
 - unter AIX 56
 - unter HP-UX 60
 - unter Linux 65
 - unter Sun Solaris 52
 - unter Windows 48
- STOP, Zeilenmodusbefehl 76
- Sun Solaris
 - MQIPT automatisch starten 53
 - MQIPT-Dateien herunterladen 51
 - MQIPT-Dateien installieren 51
 - MQIPT deinstallieren 54
 - MQIPT einrichten 52
 - MQIPT installieren 51
 - starten, MQIPT über die Befehlszeile 52
 - Verwaltungsclient über die Befehlszeile starten 53
- SupportPac, Adresse der Webseite 47

T

- TCP/IP und MQIPT 7
- Topologie, MQIPs 4
- Trace, Konfigurationseigenschaft 96
- Tracefehler 155
- Tunnelung, HTTP 9

U

- Übersicht über MQIPT 7
- Überwachungssignal, Verfahren 9
- Upgrade von einer früheren MQIPT-Version 45
- UriName, Konfigurationseigenschaft 96

V

- Verbindungs-Threads
 - Durchsatzverbesserung 156
- Verbindungsprotokolle 43
- Vererbung von Eigenschaften 73
- Verschlüsselung 3
- Verschlüsselungsalgorithmen 15
- Vertrauenseinstellungen 17
- Verwalten, MQIPT 71
- Verwalten, MQIPT über Zeilenmodusbefehle 75
- Verwaltung 153
- Verwaltung von Thread-Pools 156
- Verwaltungsclient 71
 - einen MQIPT verwalten 72

- Verwaltungsclient (*Forts.*)
 - Hilfeinformationen 75
 - Optionen im Menü 'Datei' 73
 - Optionen im Menü 'MQIPT' 73
 - starten 71
 - unter AIX starten 57
 - unter generischem UNIX starten 70
 - unter HP-UX starten 62
 - unter Linux starten 66
 - unter Sun Solaris starten 53
 - unter Windows starten 49
 - Verbindungsinformationen 71
 - Vererbung von Eigenschaften 73
 - Voraussetzungen viii, 97

W

- Wartung und Pflege von MQIPT 153
- WebSphere MQ Internet Pass-Thru und SSL 17
- Weitere Sicherheitsüberlegungen 41
- Windows
 - Dienststeuerungsprogramm 50
 - MQIPT als Dienst deinstallieren 50
 - MQIPT-Dateien herunterladen 47
 - MQIPT-Dateien installieren 47
 - MQIPT deinstallieren 50
 - MQIPT einrichten 48
 - MQIPT installieren 47
 - starten, MQIPT über die Befehlszeile 48
 - Verwaltungsclient über die Befehlszeile starten 49

X

- X.509V2-CRLs 25
- X.509V3-Zertifikate 25

Z

- Zeilenmodusbefehle 75
- Zeitlimit für Inaktivität
 - Durchsatzverbesserung 156
- Zertifikatspezifische Technologien 18
- Zielwarteschlangenmanager, Zugriff auf 7
- Zusammenfassung der Änderungen xi

Kommentare an IBM senden

Sie können uns Anmerkungen zu dem vorliegenden Handbuch über die nachfolgend aufgeführten Wege zukommen lassen.

Bitte lassen Sie es uns wissen, wenn Informationen Ihrer Meinung nach fehlerhaft sind oder ganz fehlen, oder wenn Sie Anmerkungen zur Richtigkeit, zum Aufbau, Inhalt oder zur Vollständigkeit des Handbuchs haben.

Bitte senden Sie uns Kommentare nur im Zusammenhang mit dem vorliegenden Handbuch und nur über die hier aufgeführten Übermittlungskanäle zu.

Wenn Sie Anmerkungen zu Funktionen von IBM Produkten bzw. IBM Systemen haben, wenden Sie sich bitte an Ihren IBM Ansprechpartner bzw. den zuständigen IBM Vertriebspartner.

Bei IBM eingehende Kommentare können von IBM beliebig verwendet werden, ohne dass hieraus eine Verpflichtung gegenüber dem Absender entsteht.

Ihre Kommentare können Sie IBM auf folgenden Wegen zukommen lassen:

- Per Post an folgende Adresse:

User Technologies Department (MP095)
IBM United Kingdom Laboratories
Hursley Park
WINCHESTER,
Hampshire
SO21 2JN Großbritannien

- Per Fax:

- Benutzer außerhalb von Großbritannien müssen im Anschluss an die jeweilige internationale Durchwahl (in Deutschland z. B. 00) folgende Nummer wählen: 44-1962-816151

- Benutzer in Großbritannien müssen folgende Nummer wählen: 01962-816151

- Per E-Mail, unter Angabe der entsprechenden Netz-ID:

- IBM Mail Exchange: GBIBM2Q9 at IBMMAIL

- IBMLink: HURSLEY(IDRCF)

- Internet: idrcf@hursley.ibm.com

Unabhängig von der Übertragungsart sind auf jeden Fall folgende Angaben erforderlich:

- Die Bestellnummer sowie der Titel der Veröffentlichung.
- Der Abschnitt, auf den Sie sich beziehen.
- Ihre Adresse: Name, Adresse, Telefonnummer, Faxnummer, Netz-ID.

