



# MS81: WebSphere MQ Internet Pass-Thru Version 1.2

#### **Anmerkung**

Vor Verwendung dieses Handbuchs und des darin beschriebenen Produkts sollten die allgemeinen Informationen in „Bemerkungen“ auf Seite vii 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 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.

#### **Erste Ausgabe (April 2002)**

Diese Veröffentlichung ist eine Übersetzung des Handbuchs  
*IBM MS81: WebSphere MQ Internet Pass Thru, Version 1.2,*  
IBM Form SC34-6100-00,  
herausgegeben von International Business Machines Corporation, USA

© Copyright International Business Machines Corporation 2002  
© Copyright IBM Deutschland GmbH 2002

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  
April 2002

---

# Inhaltsverzeichnis

<b>Abbildungsverzeichnis</b> . . . . .	<b>v</b>
<b>Bemerkungen</b> . . . . .	<b>vii</b>
Marken . . . . .	vii
<b>Vorwort</b> . . . . .	<b>ix</b>
WebSphere MQ Internet Pass-Thru - Beschreibung . . . . .	ix
Zielgruppe . . . . .	ix
Erforderliche Kenntnisse . . . . .	ix
Voraussetzungen . . . . .	x
Eingabehilfen . . . . .	x
<b>Literaturverzeichnis</b> . . . . .	<b>xiii</b>
<b>Zusammenfassung der Änderungen</b> . . . . .	<b>xv</b>
<b>Kapitel 1. WebSphere MQ Internet Pass-Thru - Einführung</b> . . . . .	<b>1</b>
<b>Kapitel 2. Funktionsweise von WebSphere MQ Internet Pass-Thru</b> . . . . .	<b>7</b>
Funktionsweise von WebSphere MQ Internet Pass-Thru - Übersicht . . . . .	7
HTTP-Unterstützung . . . . .	8
SOCKS-Unterstützung . . . . .	9
SSL-Unterstützung . . . . .	10
SSL-Handshake . . . . .	11
MQIPT und SSL . . . . .	12
Vertrauenseinstellungen . . . . .	12
SSL testen . . . . .	13
SSL-Fehlernachrichten . . . . .	13
Dienstgüte (QoS = Quality of Service) . . . . .	15
Servlet . . . . .	16
KeyMan . . . . .	16
Unterstützte Token . . . . .	17
Unterstützte Standarddatenformate . . . . .	18
KeyMan-FAQs . . . . .	19
Unterstützung für Network Dispatcher . . . . .	20
Clustering . . . . .	22
Unterstützte Kanalkonfigurationen . . . . .	24
Java Security Manager . . . . .	25
Normale Beendigung und Fehlerbedingungen . . . . .	26
Nachrichtensicherheit . . . . .	27
Verbindungsprotokolle . . . . .	27
Weitere Sicherheitsüberlegungen . . . . .	28
<b>Kapitel 3. Upgrade von der früheren Version</b> . . . . .	<b>29</b>
Neue Konfigurationsoptionen . . . . .	29
<b>Kapitel 4. WebSphere MQ Internet Pass-Thru unter Windows installieren</b> . . . . .	<b>31</b>
Dateien herunterladen und installieren . . . . .	32

WebSphere MQ Internet Pass-Thru einrichten . . . . .	32
WebSphere MQ Internet Pass-Thru über die Befehlszeile starten . . . . .	32
Verwaltungsclient über die Befehlszeile starten . . . . .	33
Ein Windows-Dienststeuerungsprogramm verwenden . . . . .	34
WebSphere MQ Internet Pass-Thru als Windows-Dienst deinstallieren . . . . .	34
WebSphere MQ Internet Pass-Thru deinstallieren . . . . .	34

<b>Kapitel 5. WebSphere MQ Internet Pass-Thru unter Sun Solaris installieren</b> . . . . .	<b>35</b>
Dateien herunterladen und installieren . . . . .	35
WebSphere MQ Internet Pass-Thru einrichten . . . . .	36
WebSphere MQ Internet Pass-Thru über die Befehlszeile starten . . . . .	36
WebSphere Internet Pass-Thru automatisch starten . . . . .	37
Verwaltungsclient über die Befehlszeile starten . . . . .	37
WebSphere MQ Internet Pass-Thru deinstallieren . . . . .	37

<b>Kapitel 6. WebSphere MQ Internet Pass-Thru unter AIX installieren</b> . . . . .	<b>39</b>
Dateien herunterladen und installieren . . . . .	39
WebSphere MQ Internet Pass-Thru einrichten . . . . .	40
WebSphere MQ Internet Pass-Thru über die Befehlszeile starten . . . . .	40
WebSphere Internet Pass-Thru automatisch starten . . . . .	41
Verwaltungsclient über die Befehlszeile starten . . . . .	41
WebSphere MQ Internet Pass-Thru deinstallieren . . . . .	41

<b>Kapitel 7. WebSphere MQ Internet Pass-Thru unter HP-UX installieren</b> . . . . .	<b>43</b>
Dateien herunterladen und installieren . . . . .	43
WebSphere MQ Internet Pass-Thru einrichten . . . . .	44
WebSphere MQ Internet Pass-Thru über die Befehlszeile starten . . . . .	44
WebSphere Internet Pass-Thru automatisch starten . . . . .	45
Verwaltungsclient über die Befehlszeile starten . . . . .	46
WebSphere MQ Internet Pass-Thru deinstallieren . . . . .	46

<b>Kapitel 8. WebSphere MQ Internet Pass-Thru unter Linux installieren</b> . . . . .	<b>47</b>
Dateien herunterladen und installieren . . . . .	47
WebSphere MQ Internet Pass-Thru einrichten . . . . .	48
WebSphere MQ Internet Pass-Thru über die Befehlszeile starten . . . . .	48
WebSphere Internet Pass-Thru automatisch starten . . . . .	49
Verwaltungsclient über die Befehlszeile starten . . . . .	49
WebSphere MQ Internet Pass-Thru deinstallieren . . . . .	50

<b>Kapitel 9. WebSphere MQ Internet Pass-Thru verwalten und konfigurieren</b> . . . . .	<b>51</b>
---	-----------

Verwaltungsclient von WebSphere MQ Internet	
Pass-Thru verwenden . . . . .	51
Verwaltungsclient starten . . . . .	51
MQIPT verwalten . . . . .	52
Vererbung von Eigenschaften . . . . .	53
Optionen im Menü 'Datei' . . . . .	53
Optionen im Menü 'MQIPT' . . . . .	54
Optionen im Menü 'Hilfe' . . . . .	56
Zeilenmodusbefehle von WebSphere MQ Internet	
Pass-Thru verwenden . . . . .	56
WebSphere MQ Internet Pass-Thru über Zeilen-	
modusbefehle verwalten . . . . .	56
Referenzinformationen zur Konfiguration . . . . .	57
Eigenschaften - Übersicht . . . . .	58
Referenzinformationen zum Abschnitt 'global' . . . . .	60
Referenzinformationen zum Abschnitt 'route' . . . . .	61
<b>Kapitel 10. WebSphere MQ Internet</b>	
<b>Pass-Thru - Erste Schritte . . . . .</b>	<b>71</b>
Voraussetzungen . . . . .	71
Beispielkonfigurationen . . . . .	72
Installationsfunktionstest . . . . .	72
SSL-Serverauthentifizierung . . . . .	74
SSL-Clientauthentifizierung . . . . .	77
HTTP-Proxy-Konfiguration . . . . .	80
Zugriffssteuerung konfigurieren . . . . .	83
Quality of Service (QoS) konfigurieren . . . . .	85

SOCKS-Proxy konfigurieren . . . . .	88
SOCKS-Client konfigurieren . . . . .	90
SSL-Proxy konfigurieren . . . . .	91
SSL-Testzertifikate erstellen . . . . .	95
MQIPT-Servlet konfigurieren . . . . .	96
Unterstützung für MQIPT-Clustering konfigurieren . . . . .	98
Eine Schlüsselringdatei erstellen . . . . .	102

**Kapitel 11. WebSphere MQ Internet**  
**Pass-Thru - Wartung und Pflege . . . . . 105**

Verwaltung . . . . .	105
Fehlerbestimmung . . . . .	105
WebSphere MQ Internet Pass-Thru automatisch	
starten . . . . .	107
Durchgehende Verbindungen überprüfen . . . . .	107
Tracefehler . . . . .	107
Fehlermeldung . . . . .	108
Durchsatzverbesserung . . . . .	108
Verwaltung von Threads-Pools . . . . .	108
Verbindungs-Threads . . . . .	108
Zeitlimit für Inaktivität . . . . .	108

**Kapitel 12. Nachrichten . . . . . 109**

**Index . . . . . 125**

---

## Abbildungsverzeichnis

1.	Beispiel für den Einsatz von MQIPT als Kanal-	
	konzentrador . . . . .	2
2.	Beispiel für den Einsatz von MQIPT mit einer	
	“Demilitarized Zone” . . . . .	2
3.	Beispiel für MQIPT und HTTP-Tunnelung	3
4.	Beispiel für einen MQIPT mit SSL . . . . .	3
5.	WebSphere MQ-Topologie mit möglichen	
	MQIPT-Konfigurationen. . . . .	5
6.	Verwendung von Network Dispatcher mit	
	MQIPT . . . . .	21
7.	MQIPT-Clusterunterstützung. . . . .	23
8.	Fenster beim erstmaligen Zugriff auf einen	
	MQIPT . . . . .	52
9.	Eine Route hinzufügen. . . . .	55
10.	IVT-Netzplan . . . . .	72
11.	IVT-Konfiguration . . . . .	73
12.	SSL-Servernetzplan . . . . .	74
13.	SSL-Serverauthentifizierung . . . . .	75
14.	SSL-Clientnetzplan . . . . .	77
15.	SSL-Clientauthentifizierung . . . . .	78
16.	HTTP-Proxy-Netzplan . . . . .	80
17.	HTTP-Proxy-Konfiguration . . . . .	81
18.	Netzplan für die Zugriffssteuerung . . . . .	83
19.	Konfiguration der Zugriffssteuerung . . . . .	83
20.	QoS-Netzplan. . . . .	85
21.	QoS-Konfiguration . . . . .	86
22.	Netzplan für SOCKS-Proxy . . . . .	88
23.	SOCKS-Proxy-Konfiguration . . . . .	89
24.	SOCKS-Clientnetzplan . . . . .	90
25.	SOCKS-Clientkonfiguration . . . . .	90
26.	SSL-Proxy-Netzplan. . . . .	91
27.	SSL-Proxy-Konfiguration . . . . .	92
28.	Servlet-Netzplan . . . . .	96
29.	Servlet-Konfiguration . . . . .	96
30.	Clustering-Netzplan. . . . .	98
31.	Clustering-Konfiguration . . . . .	99
32.	Fehlerbestimmung - Ablaufdiagramm	106



---

## 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.

Anfragen an obige Adresse müssen auf Englisch gestellt werden.

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. Der Kunde ist für die Bewertung und Integration dieser Funktionen in die kundeneigene Betriebsumgebung verantwortlich. Obwohl die Korrektheit der einzelnen Funktionen unter Umständen von IBM in einer bestimmten Situation geprüft wurde, kann nicht Gewähr leistet 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.

Andere Namen von Unternehmen, Produkten oder Dienstleistungen können Marken anderer Unternehmen sein.





---

## 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:

- Es stellt eine Erweiterung des WebSphere MQ-Basisprodukts dar, mit deren Hilfe Messaging-Lösungen zwischen räumlich getrennten Standorten über das Internet implementiert werden können.
- Dieses Produkt erleichtert den Durchgang der WebSphere MQ-Kanalprotokolle durch Firewalls und vereinfacht die Handhabung durch die Tunnelung unter Verwendung von HTTP oder indem es als Proxy fungiert.
- Es arbeitet als Standalone-Service, der WebSphere MQ-Nachrichtenflüsse empfangen und weiterleiten kann. Auf dem System, auf dem WebSphere MQ Internet Pass-Thru läuft, muss kein WebSphere MQWarteschlangenmanager installiert sein.
- Es unterstützt die Verwendung von unternehmensübergreifenden Transaktionen unter Verwendung von WebSphere MQ.
- Es ermöglicht die Verwendung bereits vorhandener WebSphere MQ-Anwendungen durch eine Firewall hindurch, ohne dass Änderungen erforderlich sind.
- Es stellt über den Zugriff auf mehrere WS-Manager einen zentralen Steuerungspunkt zur Verfügung.
- Es erlaubt die Verschlüsselung sämtlicher Daten.

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 gründliche Kenntnisse in folgenden Bereichen vorausgesetzt:

- Verwaltung von WebSphere MQ-Warteschlangenmanagern und -Nachrichtkanälen (siehe *MQSeries System Administration* und *MQSeries Intercommunication*)
- Implementierung von Firewalls
- Internet Protocol-Routing/Networking
- IBM Network Dispatcher (für eine gleichmäßige Auslastung und eine bessere Verfügbarkeit)
- IBM WebSphere Application Server

## Voraussetzungen

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

- Windows NT<sup>®</sup> V4.0 mit Service Pack 6
- Windows 2000
- Windows XP
- Sun Solaris
- AIX<sup>®</sup>
- HP-UX 11
- Linux

**Anmerkung:** Der Einsatz unter AIX und HP-UX ist möglich, sobald Java 1.4 für diese Plattformen freigegeben wurde.

JDK 1.4.0 oder ein höheres vergleichbares Release ist erforderlich.

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 Mausklicks 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.



---

## Literaturverzeichnis

Das vorliegende Handbuch wird im PDF- und HTML-Format bei Installation des Produkts ebenfalls installiert, und zwar in den in Tabelle 1 angegebenen Verzeichnissen. Vor der Verwendung des Verwaltungsclients müssen Sie zunächst die Datei im Verzeichnis <Sprache>/html entpacken.

- PDF  
doc\<>Sprache>\pdf\<>Dateiname>.pdf
- HTML (in der selbstentpackenden Zip-Datei enthalten)  
doc\<>Sprache>\html\<>Dateiname>.zip

In der folgenden Tabelle sehen Sie, in welchen Sprachen das Handbuch vorliegt und wie die entsprechenden Dateinamen lauten:

*Tabelle 1. Sprachen und Dateinamen - Übersicht*

Sprache	Ländereinstellung	Name der PDF-Datei	Name der HTML-Datei
Vereinfachtes Chinesisch	zn_CN	amqyzb00.pdf	amqyzb00.zip
Deutsch	de_DE	amqygb00.pdf	amqygb00.zip
Japanisch	ja_JP	amqyjb00.pdf	amqyjb00.zip
Koreanisch	ko_KR	amqykb00.pdf	amqykb00.zip
Portugiesisches Brasilianisch	pt_BR	amqybb00.pdf	amqybb00.zip
Spanisch	es_ES	amqysb00.pdf	amqysb00.zip
Amerikanisches Englisch	en_US	amqyab00.pdf	amqyab00.zip

Darüber hinaus sind die folgenden Veröffentlichungen hilfreich:

- *MQSeries Intercommunication* (SC33-1872)
- *MQSeries System Administration* (SC33-1873)
- *MQSeries Clients* (GC33-1632)
- *Cluster-Unterstützung in MQSeries* (SC12-2640)

Diese Bücher enthalten Informationen zur Definition von WebSphere MQ-Kanälen und deren Attribute, insbesondere der Definition von CONNAME.

Diese WebSphere MQ-Veröffentlichungen können von der folgenden Website heruntergeladen werden:

<http://www.ibm.com/software/ts/mqseries/library/>



---

## Zusammenfassung der Änderungen

In dieser Version von WebSphere MQ Internet Pass-Thru wurden folgende funktionalen Erweiterungen vorgenommen:

- Beispielkonfigurationen
- Verbesserte SSL-Tracefunktion
- Java Security Manager
- Das Dienstprogramm KeyMan für die Verwaltung von Zertifikaten und Schlüsselringdateien
- Linux-Unterstützung, einschließlich Dienstgüte (QoS = Quality of Service) für WebSphere MQ-Nachrichten
- Für Windows-Plattformen ist ein NLS-Installationsimage verfügbar
- Bei Eigenschaftennamen wird jetzt die Groß-/Kleinschreibung nicht mehr beachtet
- Servlet-Version
- SOCKS-Client- und Serverunterstützung
- SSL-Proxy-Modus
- Anzeige des Datenverkehrsstatus für den Verkehrsclient
- WebSphere MQ-Clusterunterstützung





---

## 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.

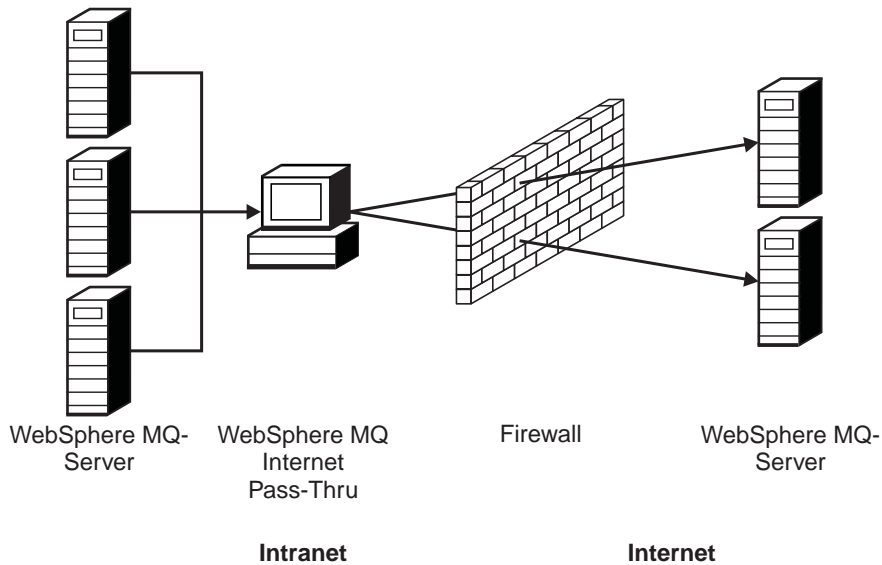


Abbildung 1. Beispiel für den Einsatz von MQIPT als Kanalkonzentrator

- Bei Einsatz auf einer Maschine mit einer bekannten und gesicherten IP-Adresse (IP = Internet-Adresse) 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.

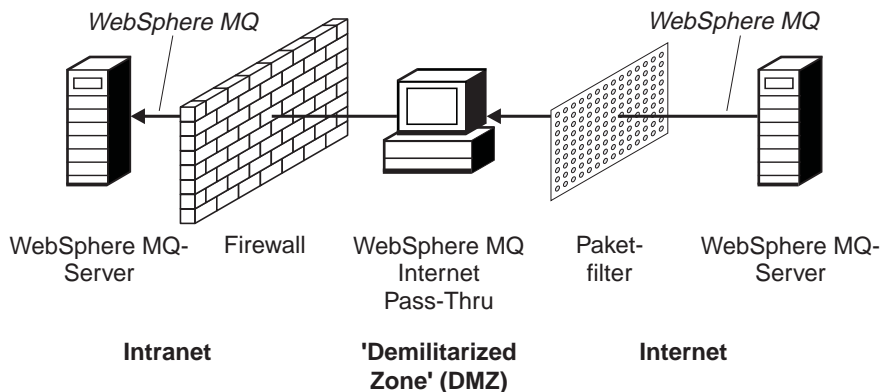


Abbildung 2. Beispiel für den Einsatz von MQIPT mit einer "Demilitarized Zone"

- 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 gereicht 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.

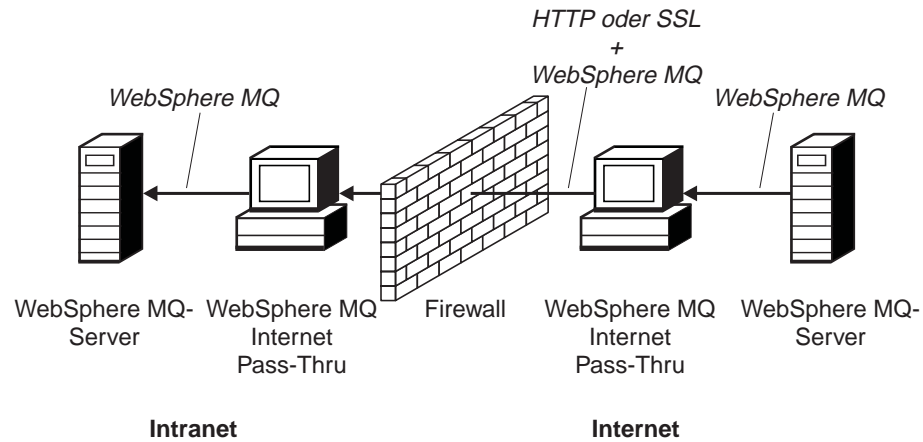


Abbildung 3. Beispiel für MQIPT und HTTP-Tunnelung

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

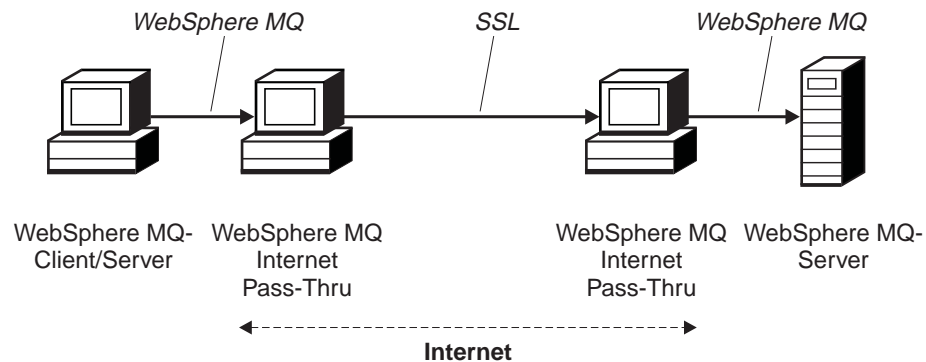


Abbildung 4. Beispiel für einen MQIPT mit SSL

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 Traceeinträge 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 MQIPTs 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.

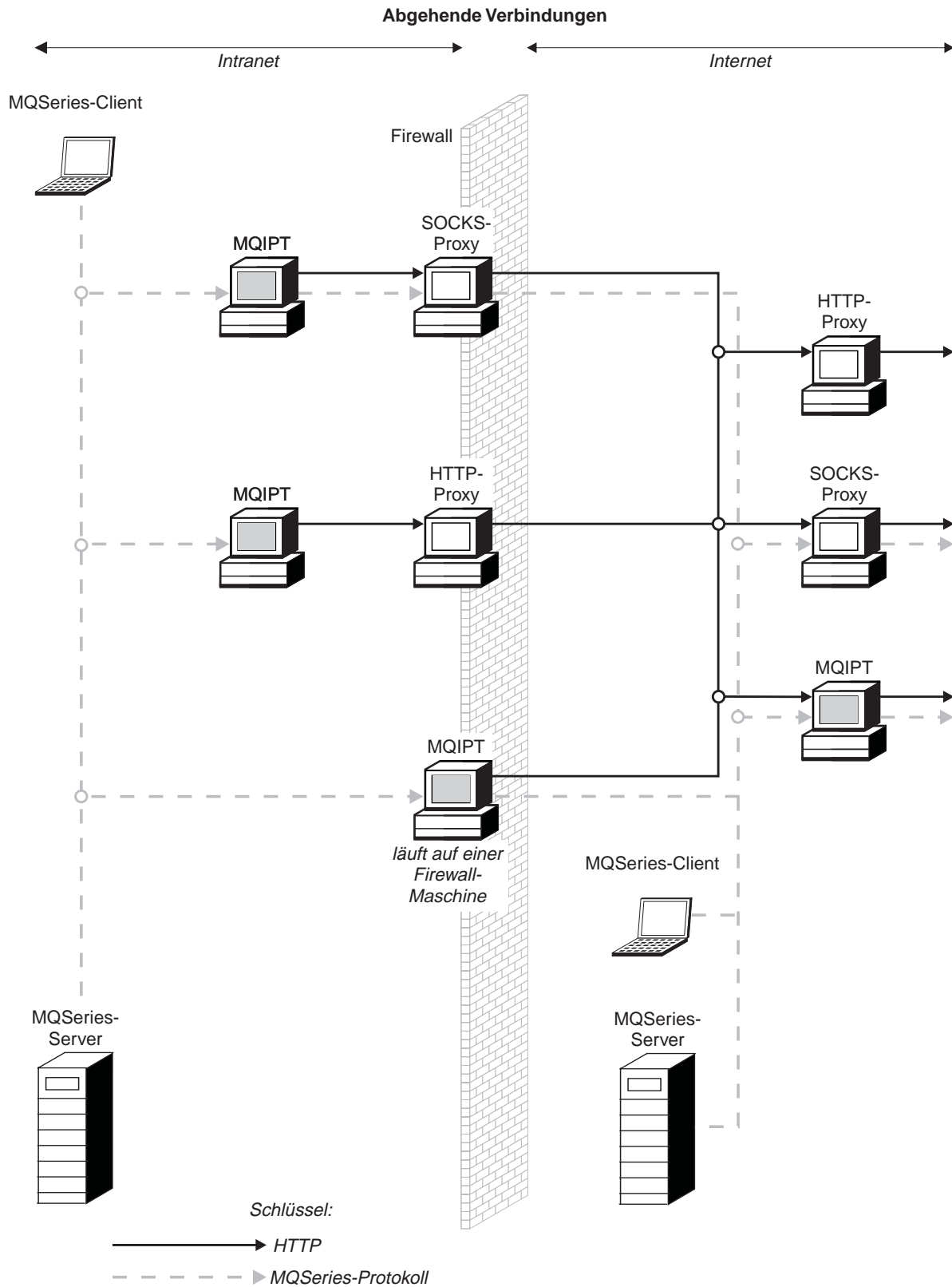


Abbildung 5. WebSphere MQ-Topologie mit möglichen MQIPT-Konfigurationen (Teil 1 von 2)

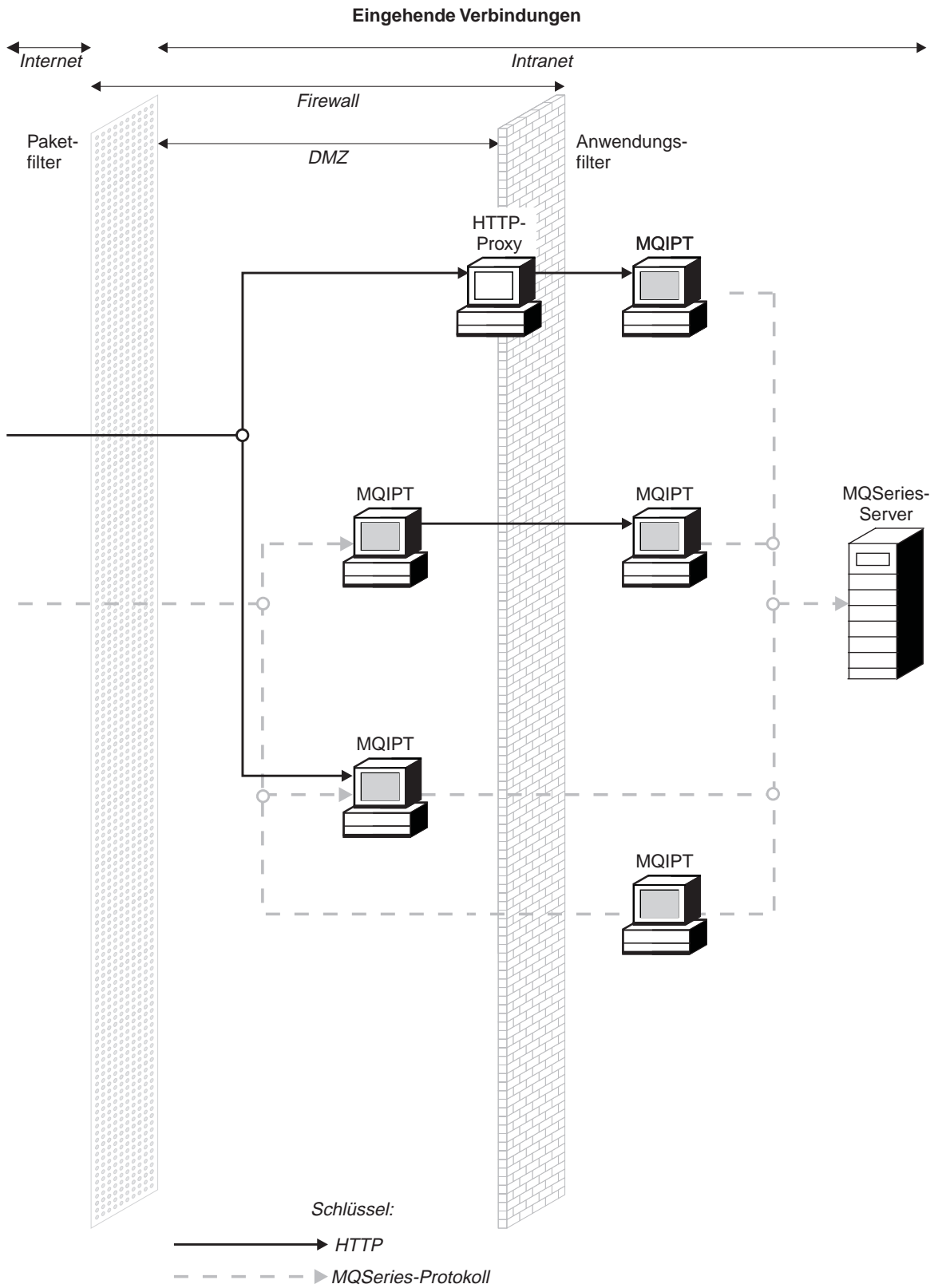


Abbildung 5. WebSphere MQ-Topologie mit möglichen MQIPT-Konfigurationen (Teil 2 von 2)

---

## Kapitel 2. Funktionsweise von WebSphere MQ Internet Pass-Thru

Dieses Kapitel enthält eine Übersicht über die Funktionsweise von WebSphere MQ Internet Pass-Thru; darüber hinaus werden hier die folgenden Komponenten erläutert:

- „HTTP-Unterstützung“ auf Seite 8
- „SOCKS-Unterstützung“ auf Seite 9
- „SSL-Unterstützung“ auf Seite 10
- „Dienstgüte (QoS = Quality of Service)“ auf Seite 15
- „KeyMan“ auf Seite 16
- „Unterstützung für Network Dispatcher“ auf Seite 20
- „Clustering“ auf Seite 22
- „Unterstützte Kanalkonfigurationen“ auf Seite 24
- „Java Security Manager“ auf Seite 25
- „Normale Beendigung und Fehlerbedingungen“ auf Seite 26
- „Nachrichtensicherheit“ auf Seite 27
- „Verbindungsprotokolle“ auf Seite 27
- „Weitere Sicherheitsüberlegungen“ auf Seite 28

---

### 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. Der Kanalname wird von MQIPT nicht überprüft, sondern einfach an den Zielwarteschlangenmanager übergeben. 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.

---

## HTTP-Unterstützung

Es besteht die Möglichkeit, MQIPT so zu konfigurieren, 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 bleibt. 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 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 gesetzt 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.

---

## SOCKS-Unterstützung

Bei der Herstellung abgehender Verbindungen durch eine Firewall kann eine Anwendung SOCKS-fähig sein; in diesem Fall werden alle Verbindungen über einen SOCKS-Proxy eingerichtet, wodurch ein Austrittsteuerungspunkt durch die Firewall ermöglicht wird.

In älteren Releases von MQIPT wurde SOCKS unterstützt, indem die Java-Systemeigenschaften **SocksProxyHost** (SOCKS-Proxy-Hostname) und **SocksProxyPort** (SOCKS-Proxy-Port) gesetzt wurden; diese galten für alle von MQIPT hergestellten Verbindungen, wodurch alle Routen denselben SOCKS-Proxy verwenden mussten. Dieses MQIPT-Release bietet Unterstützung für SOCKS V5, jedoch nur mit Unterstützung für Adressen im IPV4-Format und ohne Benutzerauthentifizierung.

Jede Route kann unter Verwendung der Eigenschaften **SocksClient** (SOCKS-Client), **SocksProxy** (SOCKS-Proxy) und **SocksProxyPort** (SOCKS-Proxy-Port) für die Kommunikation mit einem anderen SOCKS-Proxy konfiguriert werden.

Jede Route kann außerdem über die Eigenschaft **SocksServer** (SOCKS-Server) so konfiguriert werden, dass sie als SOCKS-Server (Proxy) fungiert; dadurch kann eine SOCKS-fähige WebSphere MQ-Anwendung über MQIPT eine Verbindung zum Ziel herstellen. Bei Verwendung dieser Einrichtung werden Ziel und Ziel-Port während des SOCKS-Handshake übergeben, daher werden die für die Route definierten Eigenschaften **Zieladresse** und **Ziel-Port** ignoriert. Dies ist ein wichtiges Leistungsmerkmal für die Unterstützung des WebSphere MQ-Clustering. Weitere Informationen zur Verwendung von MQIPT mit WebSphere MQ-Clustering finden Sie unter „Clustering“ auf Seite 22.

---

## SSL-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_RSA_EXPORT_WITH_RC4_40_MD5
SSL_RSA_EXPORT_WITH_DES40_CBC_SHA
SSL_RSA_EXPORT_WITH_RC2_CBC_40_MD5#
SSL_RSA_WITH_3DES_EDE_CBC_SHA
SSL_RSA_WITH_NULL_MD5
SSL_RSA_WITH_NULL_SHA
SSL_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
SSL_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA
SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA
SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA
SSL_DH_anon_WITH_RC4_40_MD5
SSL_DH_anon_EXPORT_WITH_DES40_CBC_SHA
SSL_RSA_WITH_RC4_128_MD5
SSL_RSA_WITH_RC4_128_SHA
SSL_RSA_WITH_DES_CBC_SHA
SSL_DHE_RSA_WITH_DES_CBC_SHA
SSL_DHE_DSS_WITH_DES_CBC_SHA
SSL_DH_anon_WITH_3DES_EDE_CBC_SHA
SSL_DH_anon_WITH_RC4_128_MD5
SSL_DH_anon_WITH_DES_CBC_SHA
```

## 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; dabei beginnt er zunächst mit dem Sitezertifikat; die Signatur des Sitezertifikats wird dann 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 Repositorys 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 Client-Authentifizierung erfolgt analog; wird von einem SSL-Server eine Clientauthentifizierung angefordert, 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.

## MQIPT und SSL

SSL V3.0 wurde implementiert; es werden PKCS#12-Token verwendet. Diese Token sind in Schlüsselringdateien (Dateityp .pp12 oder .pfx) gespeichert, die X509V3-Zertifikate enthalten.

Ein MQIPT kann als SSL-Client oder als 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 MQIPT-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 MQIPT-Route kann über eigene SSL-Eigenschaften konfiguriert werden. Weitere Informationen hierzu finden Sie unter „Referenzinformationen zum Abschnitt 'route'“ auf Seite 61.

## 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. Eine zweite Schlüsselringdatei, die über die Eigenschaft **SSLServerCAKeyRing** (SSL-Server - CA-Schlüsselringdatei) angegeben wird, sollte alle als vertrauenswürdig angesehenen Zertifikate (auf CA- oder auf Peer-Ebene) enthalten.

Die Schlüsselringdatei auf der SSL-Clientseite, die über die Eigenschaft **SSLClientKeyRing** (SSL-Clientschlüsselring) angegeben wird, enthält das private Zertifikat. Eine zweite Schlüsselringdatei, die über die Eigenschaft **SSLClientCAKeyRing** (SSL-Client - CA-Schlüsselringdatei) angegeben wird, sollte alle als vertrauenswürdigen angesehenen Zertifikate (auf CA- oder auf Peer-Ebene) enthalten. Eine Schlüsselringdatei kann darüber hinaus auch eine Liste mit CRLs (Certification Revocation Lists) enthalten.

Sie können außerdem auch selbstsignierte Zertifikate verwenden, ähnlich denen, die sich in dem mit MQIPT gelieferten Beispielschlüsselring (sslSample.pfx) befinden.

Mit Hilfe des Dienstprogramms KeyMan (im Unterverzeichnis **ssl**) können Zertifikate und Schlüsselringdateien verwaltet werden. Weitere Informationen hierzu finden Sie unter „KeyMan“ auf Seite 16.

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

## SSL testen

In Kapitel 10, „WebSphere MQ Internet Pass-Thru - Erste Schritte“ auf Seite 71 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](http://www.rsasecurity.com))
- Entrust Technologies ([www.entrust.com](http://www.entrust.com))
- Verisign ([www.verisign.com](http://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 2. SSLRuntimeException-Fehlernachrichten*

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

Tabelle 2. *SSLRuntimeException-Fehlernachrichten (Forts.)*

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 (Certificate Revocation List = Sperreintragsliste) 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.

Die *SSLException*-Fehlernachrichten werden ausgegeben, wenn die Ausführung des SSL-Handshake-Protokolls abgebrochen wird.

Tabelle 3. *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.

---

## Dienstgüte (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 Dienstgüte 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 Client-Abfragen. Für die Implementierung der Dienstgüte (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-3.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.

Hinweise, wie der IBM WebSphere Edge Server mit der TQoS-Komponente heruntergeladen werden kann, finden Sie in der Readme-Datei (`Readme.txt`) für MQIPT.

MQIPT wird mit einer Pseudobibliothek (`libmqiptqos.so`) geliefert, die sich im Unterverzeichnis **lib** befindet. Nach der Installation des TQoS-Plug-In müssen Sie im Script **mqipt** im Unterverzeichnis **bin** die Umgebungsvariable `LD_LIBRARY_PATH` ändern, so dass sie auf das WES-Unterverzeichnis **lib** zeigt.

Für die Implementierung der Dienstgüte (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 **QoS an Anrufer** und **QoS an Zieladresse** (siehe „Referenzinformationen zum Abschnitt 'route'“ auf Seite 61) 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 85.

---

## Servlet

Es steht jetzt eine Servlet-Version von MQIPT (MQIPTServlet) zur Verfügung, die auf einem Anwendungsserver eingesetzt werden kann. Dieses Servlet arbeitet ähnlich wie das "normale" MQIPT, jedoch so, als ob es nur über eine Route verfügt. Eine eingehende 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 Datei muss in den Anwendungsserver importiert werden.

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 gesetzt werden:

- **Client-Zugriff**
- **Verbindungsprotokoll**
- **Maximale Protokolldateigröße**
- **WS-Managerzugriff**
- **Trace**

Verbindungsprotokolle und Tracedateien werden in ein Verzeichnis geschrieben, das über die neue Eigenschaft **LogDir** (Protokollverzeichnis) definiert wird. Diese Eigenschaft sollte vor dem Start des MQIPTServlet definiert werden.

Sie können den Umfang der vom MQIPTServlet verwendeten Ressourcen steuern, indem Sie die maximale Anzahl an aktiven Sitzungen bzw. die Anzahl der Servlet-Instanzen im Anwendungsserver festlegen.

Das MQIPTServlet wurde mit dem IBM WebSphere Application Server 4.0, Tomcat 3.3 und Tomcat 4.0 getestet.

Eine Beispielkonfiguration finden Sie unter „MQIPT-Servlet konfigurieren“ auf Seite 96.

---

## KeyMan

MQIPT 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-Token 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 Repositories, 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 Token bezeichnet. Ein Token enthält die Vertrauenseinstellungen für eine bestimmte Anwendung (z. B. MQIPT). 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 vertrauenswürdiger Kommunikationspartner und von Zertifizierungsstellen (CAs).

## Unterstützte Token

KeyMan unterstützt eine Reihe unterschiedlicher Token. Bei Token handelt es sich um Repositorys, die Schlüssel, Zertifikate, CRLs und Vertrauenseinstellungen enthalten. Einige Token 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 Verschlüsselungstoken. In diesen Token können Schlüssel und Zertifikate gespeichert werden. Die Speicherung von CRLs wird hingegen nicht unterstützt. Der Zugriff auf diese Token wird über eine PIN (Personal Identification Number = persönliche Identifikationsnummer) geschützt. Sie müssen die token-spezifische 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-Token, die aus unterschiedlichen Medien (z. B. Dateien, URI oder der Zwischenablage) abgerufen werden können.

KeyMan kann PKCS#7-Token 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-Token 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 ist 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

Bei allgemeinen Fragen zur Kryptografie und damit zusammenhängenden Themen finden Sie unter "Frequently Asked Questions About Today's Cryptography" auf der Website von RSA Laboratories. In der folgenden FAQ 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-Token, Hardware-Token, ungeschützte Token oder Token, 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).

---

## **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. 6 auf Seite 21 ist eine Verwendungsmöglichkeit des Network Dispatcher zur Überwachung der Port-Adresse 1414 für MQIPT dargestellt. Jede MQIPT-Instanz muss über dieselbe Konfigurationsdatei verfügen.

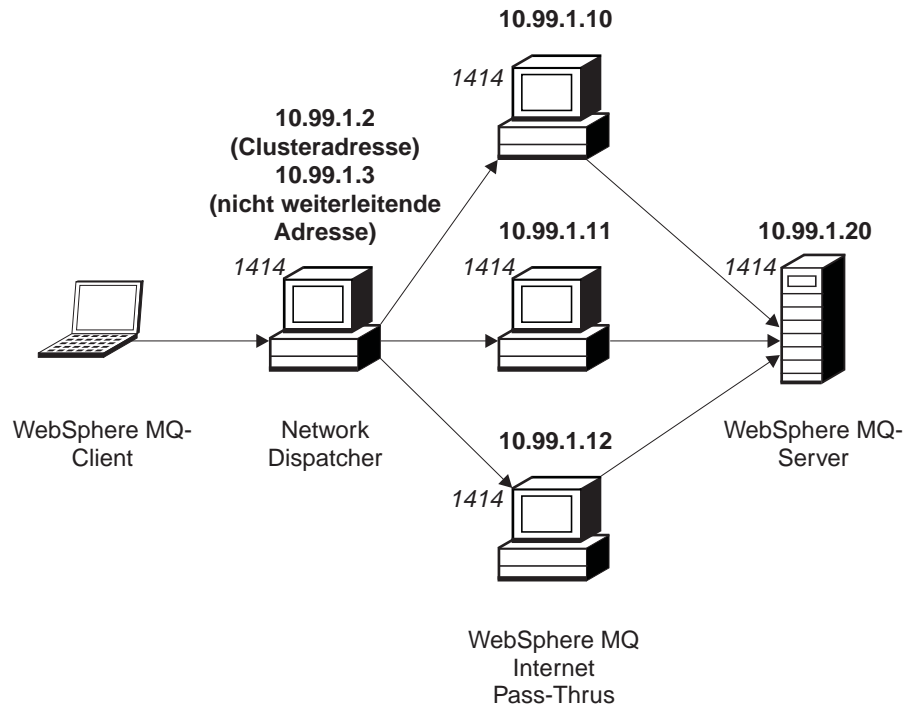


Abbildung 6. Verwendung von Network Dispatcher mit MQIPT

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 Verwaltungsclient 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**.

---

## 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 so viele Konfigurationsmöglichkeiten für WS-Manager in einem Cluster gibt, beschränkt sich die folgende Erläuterung auf die Aufgaben, die in Teil, 1, Kapitel 3 des Handbuchs *Cluster-Unterstützung in MQSeries* (SC12-2640) beschrieben werden. Bei der folgenden Abbildung handelt es sich um eine Erweiterung der Abbildung aus dem Abschnitt "Aufgabe 2: 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 namens 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. Weitere Informationen zur SOCKS-Unterstützung in MQIPT finden Sie unter „SOCKS-Unterstützung“ auf Seite 9.

Ein Beispiel für die Konfiguration eines Clusternetzes finden Sie unter „Unterstützung für MQIPT-Clustering konfigurieren“ auf Seite 98.

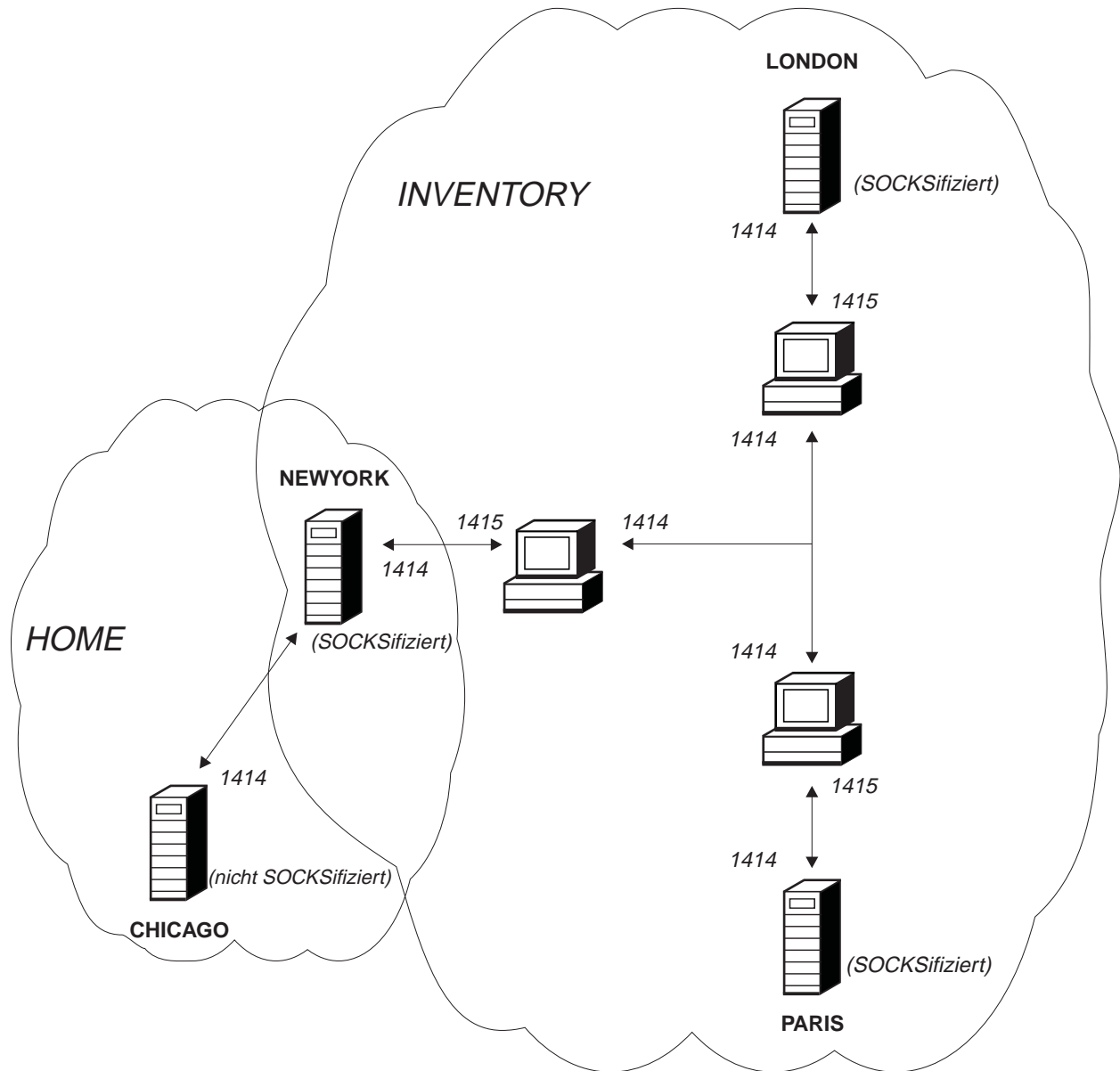


Abbildung 7. MQIPT-Clusterunterstützung

---

## 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.



---

## 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 zu erhalten.

MQIPT verwendet den standardmäßigen Java Security Manager, wie er in der Klasse `java.lang.SecurityManager` definiert ist. Das Java Security Manager-Merkmal in MQIPT kann über die globale Eigenschaft **Sicherheitsmanager** aktiviert bzw. deaktiviert werden; weitere Informationen hierzu finden Sie unter „Referenzinformationen zum Abschnitt 'global'“ auf Seite 60.

Der Java Security Manager verwendet zwei standardmäßige Richtliniendateien. Dies ist einmal 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 60. 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:\Program Files\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-gleich 1414)
- -1414 (alle Port-Adressen kleiner-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 **Sicherheitsmanager** und **Richtlinie für Sicherheitsmanager** zu verwenden.

---

## 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 WebSphere MQ-Nachrichten übertragen werden. 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 **Verbindungsprotokoll** und **Maximale Protokolldateigröße** gesteuert. Weitere Informationen hierzu finden Sie unter „Referenzinformationen zum Abschnitt 'global'“ auf Seite 60.

Bei jedem Start von MQIPT wird ein neues Verbindungsprotokoll erstellt; zur besseren Kennzeichnung enthält der Dateiname die aktuelle Zeitmarke. Beispiel:

```
mqiptJJJMMTTHHmSS.1log
```

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.

---

## Weitere Sicherheitsüberlegungen

Wenn Sie das SSL-Protokoll nicht verwenden, bietet MQIPT Sicherheitsabläufe für Kanäle; auf diese Weise können WebSphere MQ-Kanal-Exits 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 zu solchen WS-Managern eine Verbindung herstellen, die explizit in der MQIPT-Konfigurationsdatei angegeben sind, außer MQIPT wird als SOCKS-Proxy eingesetzt.
- 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 25).
- MQIPT lässt zu, dass Kanal-Exits ihre eigenen durchgehenden Sicherheitsprotokolle ausführen.
- MQIPT ermöglicht es Ihnen, die maximale Anzahl ankommender Verbindungen über die Eigenschaft **Maximale Anzahl von Verbindungs-Threads** festzulegen. Dadurch können ungeschützte interne WS-Manager vor Denial-of-Service-Attacken bewahrt 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 3. Upgrade von der früheren Version

Für den MQIPT-Upgrade von Version 1.1 auf Version 1.2 müssen folgende Schritte ausgeführt werden:

1. Erstellen Sie eine Kopie der Konfigurationsdatei **mqipt.conf**, und speichern Sie diese Kopie in einem anderen Verzeichnis als dem MQIPT-Ausgangsverzeichnis.
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 die gespeicherte Konfigurationsdatei wieder in das MQIPT-Ausgangsverzeichnis. Diese Datei ist mit V1.2 kompatibel. Die neue Datei **mqiptSample.conf** enthält die neuen Eigenschaften, die Sie unter Umständen verwenden möchten.
6. Es wird empfohlen, Änderungen an MQIPT über die grafische Benutzeroberfläche (GUI) für die MQIPT-Verwaltung vorzunehmen. Die Konfigurationsdatei von MQIPT V1.1 ist mit dieser GUI kompatibel.

---

### Neue Konfigurationsoptionen

Die folgenden Eigenschaften in Version 1.2 sind neu:

- LogDir** (Protokollverzeichnis)
- Quality of Service (QoS)**
- QoS an Zieladresse**
- QoS an Anrufer**
- Sicherheitsmanager**
- Richtlinie für Sicherheitsmanager**
- Servlet-Client**
- SOCKS-Client**
- SOCKS-Server**
- SOCKS-Proxy-Hostname**
- SOCKS-Proxy-Port**
- SSL-Proxy-Modus**
- URI-Name**

Informationen zu allen Eigenschaften finden Sie unter „Referenzinformationen zur Konfiguration“ auf Seite 57.



---

## Kapitel 4. WebSphere MQ Internet Pass-Thru unter Windows installieren

In diesem Kapitel wird die Installation von MQIPT unter Windows NT, Windows 2000 und Windows XP beschrieben:

- „Dateien herunterladen und installieren“
- „WebSphere MQ Internet Pass-Thru einrichten“ auf Seite 32
- „WebSphere MQ Internet Pass-Thru über die Befehlszeile starten“ auf Seite 32
- „Verwaltungsclient über die Befehlszeile starten“ auf Seite 33
- „Ein Windows-Dienststeuerungsprogramm verwenden“ auf Seite 34
- „WebSphere MQ Internet Pass-Thru als Windows-Dienst deinstallieren“ auf Seite 34
- „WebSphere MQ Internet Pass-Thru deinstallieren“ auf Seite 34

---

### Dateien herunterladen und installieren

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

<http://www.ibm.com/software/ts/mqseries/downloads>

Laden Sie die Datei entsprechend den Hinweisen herunter.

Öffnen Sie ein Befehlseingabefenster, und entpacken Sie die Datei `ms81_nt.zip` in einem temporäres 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
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

Datei	Funktion
bin\mqipt.bat	Direktaufruf für die Aktivierung von MQIPT über die Befehlszeile
bin\mqiptAdmin.bat	Direktaufruf zum Stoppen von MQIPT und zur Aktualisierung von Dateinformationen
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>\pdf\ <Dateiname>.pdf	Das Handbuch <i>WebSphere MQ Internet Pass-Thru</i> im PDF-Format. Weitere Informationen zur Softcopy der Dokumentation finden Sie unter „Literaturverzeichnis“ auf Seite xiii.
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 xiii.

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.properties	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** auf die Datei **mqipt.conf** kopieren. Informationen zur Konfiguration und Verwaltung finden Sie unter Kapitel 9, „WebSphere MQ Internet Pass-Thru verwalten und konfigurieren“ auf Seite 51.

---

## 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 `mqi`pt ohne Angabe von Optionen wird eine Standardadresse (".") für die Konfigurationsdatei `mqi`pt.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 105 nach. Im Folgenden ein Beispiel für die Nachrichten, die beim erfolgreichen Start von MQIPT angezeigt werden:

```
5639-L92 (C) Copyright IBM Corp. 2000-2002 Alle Rechte vorbehalten.  
MQCPI001 WebSphere MQ Internet Pass-Thru Version 1.2 wird gestartet.  
MQCPI004 Die Konfigurationsdaten aus c:\mqipt\mqipt.conf werden gelesen.  
MQCPI008 Empfangsbereit für Steuerbefehle an Port 1881.  
MQCPI011 Die Protokolldateien werden im Pfad c:\mqipt\logs gespeichert.  
MQCPI006 Route 1418 wurde gestartet und leitet Nachrichten weiter an :  
MQCPI034 ....mqserver.company4.com(1414)  
MQCPI035 ....verwendet MQ-Protokolle  
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 c:\mqipt\KeyMan.pfx  
MQCPI038 .....registrierte Namen CN=*Doe O=IBM OU=* L=* ST=* C=*
```

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

- Verzeichnis `log`, in dem das Verbindungsprotokoll gespeichert wird
- Verzeichnis `errors`, in das FFST™ - (First Failure Support Technology™) und Traceinträge geschrieben werden

---

## Verwaltungsclient über die Befehlszeile starten

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

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

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:

```
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.

---

## 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**.

---

## WebSphere MQ 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 5. 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 36
- „WebSphere MQ Internet Pass-Thru über die Befehlszeile starten“ auf Seite 36
- „WebSphere Internet Pass-Thru automatisch starten“ auf Seite 37
- „Verwaltungsclient über die Befehlszeile starten“ auf Seite 37
- „WebSphere MQ Internet Pass-Thru deinstallieren“ auf Seite 37

---

### Dateien herunterladen und installieren

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

<http://www.ibm.com/software/ts/mqseries/downloads>

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
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

Datei	Funktion
bin/mqipt	Direktaufufruf für die Aktivierung von MQIPT über die Befehlszeile
bin/mqiptAdmin	Direktaufufruf zum Stoppen von MQIPT und zur Aktualisierung von Dateinformationen
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 <b>mqipt.jar</b> an; wird nur von den anderen Scripts verwendet
web/MQIPTServlet.war	Webarchivierungsdatei für die Servlet-Version
doc/<Sprache>/pdf/<Dateiname>.pdf	Das Handbuch <i>WebSphere MQ Internet Pass-Thru</i> im PDF-Format. Weitere Informationen zur Softcopy der Dokumentation finden Sie unter „Literaturverzeichnis“ auf Seite xiii.
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 xiii.
lib/mqiptGui.jar	Enthält Laufzeit-, Klassen- und Eigenschaftsdateien für die grafische Benutzerschnittstelle "Verwaltungsclient"
bin/mqiptGui	Direktaufufruf für die Ausführung des Verwaltungsclients über die Befehlszeile
bin/customSample.properties	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** auf die Datei **mqipt.conf** kopieren. Informationen zur Konfiguration und Verwaltung finden Sie unter Kapitel 9, „WebSphere MQ Internet Pass-Thru verwalten und konfigurieren“ auf Seite 51.

---

## 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 105 nach. Im Folgenden ein Beispiel für die Nachrichten, die beim erfolgreichen Start von MQIPT angezeigt werden:

```
5639-L92 (C) Copyright IBM Corp. 2000-2002 Alle Rechte vorbehalten.
MQCPI001 WebSphere MQ Internet Pass-Thru Version 1.2 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
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=*

```

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 Traceeinträge 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“ 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 6. WebSphere MQ Internet Pass-Thru unter AIX installieren

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

- „Dateien herunterladen und installieren“
- „WebSphere MQ Internet Pass-Thru einrichten“ auf Seite 40
- „WebSphere MQ Internet Pass-Thru über die Befehlszeile starten“ auf Seite 40
- „WebSphere Internet Pass-Thru automatisch starten“ auf Seite 41
- „Verwaltungsclient über die Befehlszeile starten“ auf Seite 41
- „WebSphere MQ Internet Pass-Thru deinstallieren“ auf Seite 41

---

### Dateien herunterladen und installieren

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

<http://www.ibm.com/software/ts/mqseries/downloads>

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
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

Datei	Funktion
bin/mqipt	Direktaufruf für die Aktivierung von MQIPT über die Befehlszeile
bin/mqiptAdmin	Direktaufruf zum Stoppen von MQIPT und zur Aktualisierung von Dateinformationen
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 <b>mqipt.jar</b> an; wird nur von den anderen Scripts verwendet
web/MQIPTServlet.war	Webarchivierungsdatei für die Servlet-Version
doc/<Sprache>/pdf/<Dateiname>.pdf	Das Handbuch <i>WebSphere MQ Internet Pass-Thru</i> im PDF-Format. Weitere Informationen zur Softcopy der Dokumentation finden Sie unter „Literaturverzeichnis“ auf Seite xiii.
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 xiii.
lib/mqiptGui.jar	Enthält die Laufzeit-, Klassen- und Eigenschaftsdateien
bin/mqiptGui	Direktaufruf für die Aktivierung des Verwaltungsclients über die Befehlszeile
bin/customSample.properties	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** auf die Datei **mqipt.conf** kopieren. Informationen zur Konfiguration und Verwaltung finden Sie unter Kapitel 9, „WebSphere MQ Internet Pass-Thru verwalten und konfigurieren“ auf Seite 51.

---

## 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 105 nach. Im Folgenden ein Beispiel für die Nachrichten, die beim erfolgreichen Start von MQIPT angezeigt werden:

```
5639-L92 (C) Copyright IBM Corp. 2000-2002 Alle Rechte vorbehalten.
MQCPI001 WebSphere MQ Internet Pass-Thru Version 1.2 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
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=*

```

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 Traceeinträge 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“ 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 7. 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 44
- „WebSphere MQ Internet Pass-Thru über die Befehlszeile starten“ auf Seite 44
- „WebSphere Internet Pass-Thru automatisch starten“ auf Seite 45
- „Verwaltungsclient über die Befehlszeile starten“ auf Seite 46
- „WebSphere MQ Internet Pass-Thru deinstallieren“ auf Seite 46

---

### Dateien herunterladen und installieren

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

<http://www.ibm.com/software/ts/mqseries/downloads>

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
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

Datei	Funktion
bin/mqipt	Direktaufruf für die Aktivierung von MQIPT über die Befehlszeile
bin/mqiptAdmin	Direktaufruf zum Stoppen von MQIPT und zur Aktualisierung von Dateinformationen
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 <b>mqipt.jar</b> 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>/pdf/<Dateiname>.pdf	Das Handbuch <i>WebSphere MQ Internet Pass-Thru</i> im PDF-Format. Weitere Informationen zur Softcopy der Dokumentation finden Sie unter „Literaturverzeichnis“ auf Seite xiii.
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 xiii.
lib/mqiptGui.jar	Enthält Laufzeit-, Klassen- und Eigenschaftsdateien für die grafische Benutzerschnittstelle "Verwaltungsclient"
bin/mqiptGui	Direktaufruf für die Ausführung des Verwaltungsclients über die Befehlszeile
bin/customSample.properties	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** auf die Datei **mqipt.conf** kopieren. Informationen zur Konfiguration und Verwaltung finden Sie unter Kapitel 9, „WebSphere MQ Internet Pass-Thru verwalten und konfigurieren“ auf Seite 51.

---

## 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 105 nach. Im Folgenden ein Beispiel für die Nachrichten, die beim erfolgreichen Start von MQIPT angezeigt werden:

```
5639-L92 (C) Copyright IBM Corp. 2000-2002 Alle Rechte vorbehalten.
MQCPI001 WebSphere MQ Internet Pass-Thru Version 1.2 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
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=*
```

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 Traceinträge 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 45 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 8. 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 48
- „WebSphere MQ Internet Pass-Thru über die Befehlszeile starten“ auf Seite 48
- „WebSphere Internet Pass-Thru automatisch starten“ auf Seite 49
- „Verwaltungsclient über die Befehlszeile starten“ auf Seite 49
- „WebSphere MQ Internet Pass-Thru deinstallieren“ auf Seite 50

---

### Dateien herunterladen und installieren

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

<http://www.ibm.com/software/ts/mqseries/downloads>

Laden Sie die Datei entsprechend den Hinweisen herunter.

Melden Sie sich als **root** an, und dekomprimieren und entpacken Sie die Datei **ms81\_linux.tar.gz** in einem temporären Verzeichnis. Führen Sie den Befehl **rpm** wie im folgenden Beispiel gezeigt aus:

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

In diesem Beispiel wird davon ausgegangen, dass sich die Datei **ms81\_linux.tar.gz** 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
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")

Datei	Funktion
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 Dateinformationen
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 <b>mqipt.jar</b> an; wird nur von den anderen Scripts verwendet
web/MQIPTServlet.war	Webarchivierungsdatei für die Servlet-Version
doc/<Sprache>/pdf/<Dateiname>.pdf	Das Handbuch <i>WebSphere MQ Internet Pass-Thru</i> im PDF-Format. Weitere Informationen zur Softcopy der Dokumentation finden Sie unter „Literaturverzeichnis“ auf Seite xiii.
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 xiii.
lib/mqiptGui.jar	Enthält Laufzeit-, Klassen- und Eigenschaftsdateien für die grafische Benutzerschnittstelle "Verwaltungsclient"
bin/mqiptGui	Direktaufruf für die Ausführung des Verwaltungsclients über die Befehlszeile
bin/customSample.properties	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** auf die Datei **mqipt.conf** kopieren. Informationen zur Konfiguration und Verwaltung finden Sie unter Kapitel 9, „WebSphere MQ Internet Pass-Thru verwalten und konfigurieren“ auf Seite 51.

---

## 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 105 nach. Im Folgenden ein Beispiel für die Nachrichten, die beim erfolgreichen Start von MQIPT angezeigt werden:



```

5639-L92 (C) Copyright IBM Corp. 2000-2002 Alle Rechte vorbehalten.
MQCPI001 WebSphere MQ Internet Pass-Thru Version 1.2 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
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=*

```

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 Traceeinträge 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 49 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-1.2.0-0
```

---

## Kapitel 9. 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 56
- „Referenzinformationen zur Konfiguration“ auf Seite 57

---

### 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.

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 das **Zugriffskennwort** in der MQIPT-Konfigurationsdatei enthalten 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.

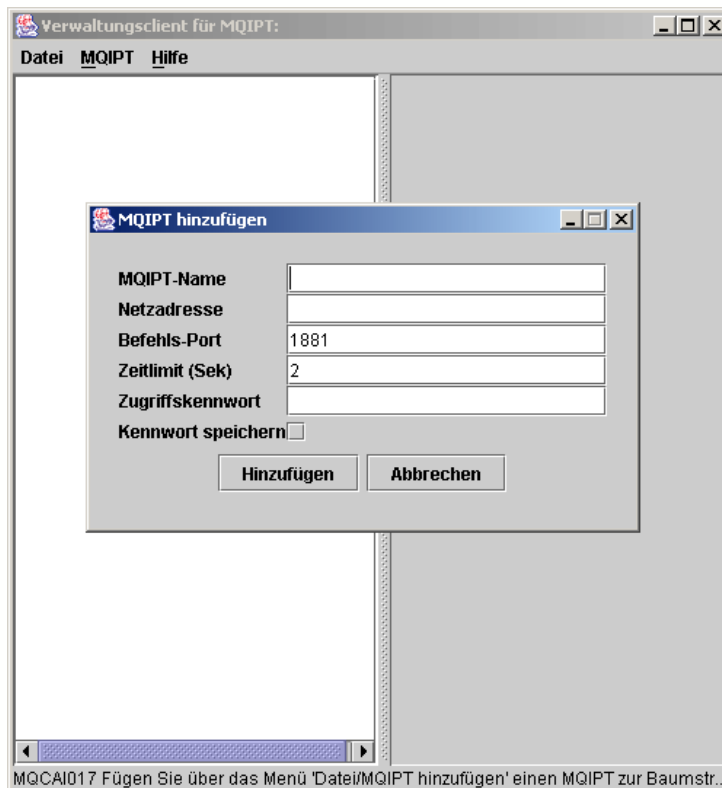


Abbildung 8. Fenster beim erstmaligen Zugriff auf einen MQIPT

## 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 Fehlernachricht 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.

Wenn Sie eine Konfigurationsdatei (**mqipt.conf**) von MQSeries internet pass-thru Version 1.0 verwenden, werden keine Routennamen angezeigt. Sie können einen Routennamen über das Feld **Name** hinzufügen.

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 MQIPTs 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 MQIPTs gesetzten globalen Eigenschaften werden von jeder Route des betreffenden MQIPTs 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 MQIPT 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 51).

### **MQIPT entfernen**

Entfernt den momentan hervorgehobenen MQIPT lediglich aus der Baumstruktur des Verwaltungsclient. Die Auswahl dieser Option wirkt sich nicht auf den Betrieb des MQIPTs 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 MQIPTs. Diese Änderungen werden in der Baumstrukturansicht übernommen. Es wird ein Fenster ähnlich dem unter „Verwaltungsclient starten“ auf Seite 51 beschriebenen angezeigt.

### Kennwort

Ändert die Eigenschaft **Kennwort** des fernen MQIPTs. 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 auf Seite 55. Jeder Route muss ein eigener Listener-Port für den MQIPT zugeordnet werden.

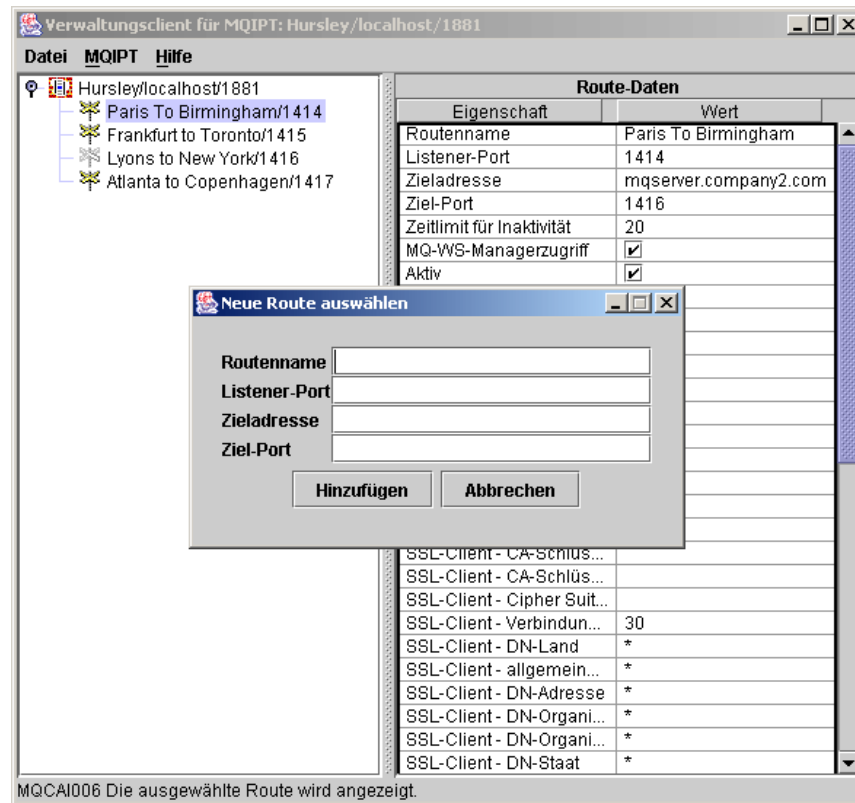


Abbildung 9. Eine Route hinzufügen

### 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 **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 57.

Wird im Abschnitt **global** der Konfigurationsdatei **mqipt.conf** ein Wert für **CommandPort** (Befehls-Port) 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, so 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 Verwaltungsclient wurden keine Änderungen an den MQIPT-Einstellungen vorgenommen.

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

---

## Referenzinformationen zur Konfiguration

Hinweise zum Einrichten einiger einfachen Konfigurationen finden Sie unter Kapitel 10, „WebSphere MQ Internet Pass-Thru - Erste Schritte“ auf Seite 71. Eine Beispielformatierung finden Sie in der Datei **mqiptSample.conf** im Ausgangsverzeichnis von MQIPT.

Die Datei **mqipt.conf** besteht aus einer Reihe von Abschnitten. Es gibt einen globalen Abschnitt (`global`) und je einen Abschnitt für jede Route, die über MQIPT definiert wird. In dieser einfachen Konfiguration gibt es nur eine Route, daher besteht die Datei lediglich aus zwei Abschnitten, nämlich `global` und einem `route`-Abschnitt.

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 unbekannt 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.

## Eigenschaften - Übersicht

Tabelle 4 enthält Folgendes:

- Alle Eigenschaften
- Die Angabe, ob eine Eigenschaft im globalen Abschnitt und/oder Routenabschnitt enthalten sein kann
- Standardwerte

Für Eigenschaften, die weder im globalen Abschnitt noch in den Routenabschnitten gesetzt werden, werden die in der Tabelle aufgeführten Standardwerte übernommen.

Tabelle 4. Konfigurationseigenschaften - Übersicht

Name	Global	Route	Standardwert
AccessPW (Zugriffskennwort)	Ja		<Null>
Active (Aktiv)	Ja	Ja	true
ClientAccess (Clientzugriff)	Ja	Ja	false
CommandPort (Befehls-Port)	Ja		<Null> <sup>1</sup>
ConnectionLog (Verbindungsprotokoll)	Ja		true
Destination (Zieladresse)		Ja	<Null>
DestinationPort (Ziel-Port)		Ja	1414
HTTP <sup>6,7</sup>	Ja	Ja	false
HTTPChunking <sup>1</sup> (HTTP-Chunking)	Ja	Ja	false
HTTPProxy <sup>1</sup> (HTTP-Proxy)	Ja	Ja	<Null>
HTTPProxyPort <sup>1</sup> (HTTP-Proxy-Port)	Ja	Ja	8080
IdleTimeout (Zeitlimit für Inaktivität)	Ja	Ja	0
ListenerPort (Listener-Port)		Ja	<Null>
LogDir (Protokollverzeichnis, gilt nur für MQIPTServlet)			<Null>
MaxConnectionThreads (Max. Anzahl von Verbindungs-Threads)	Ja	Ja	100
MaxLogFileSize (Max. Protokolldateigröße)	Ja		50
MinConnectionThreads (Mindestanzahl von Verbindungs-Threads)	Ja	Ja	5
Name		Ja	<Null>
NDAdvisor (Network Dispatcher Advisor)	Ja	Ja	false
NDAdvisorReplaceMode <sup>4</sup> (Network Dispatcher-Ersetzungsmodus)	Ja	Ja	false
QMgrAccess (WS-Managerzugriff)	Ja	Ja	true
QoS (Quality of Service (QoS); nur unter Linux verwendbar)	Ja	Ja	false
QosToCaller <sup>9</sup> (QoS an Anrufer)	Ja	Ja	1
QosToDest <sup>9</sup> (QoS an Zieladresse)	Ja	Ja	1
RemoteShutdown (Fernes Beenden)	Ja		false
SecurityManager (Sicherheitsmanager)	Ja		false

Tabelle 4. Konfigurationseigenschaften - Übersicht (Forts.)

Name	Global	Route	Standardwert
SecurityManagerPolicy (Richtlinie für Sicherheitsmanager)	Ja		<Null>
ServletClient <sup>1</sup> (Servlet-Client)	Ja	Ja	false
SocksClient (SOCKS-Client)	Ja	Ja	false
SocksProxyHost <sup>8</sup> (SOCKS-Proxy-Hostname)	Ja	Ja	<Null>
SocksProxyPort <sup>8</sup> (SOCKS-Proxy-Port)	Ja	Ja	1080
SocksServer <sup>7</sup> (SOCKS-Server)	Ja	Ja	false
SSLClient (SSL-Client)	Ja	Ja	false
SSLClientCipherSuites <sup>2</sup> (SSL-Client - Cipher Suites)	Ja	Ja	<Null>
SSLClientConnectTimeout <sup>2</sup> (SSL-Client - Verbindungszeitlimit)	Ja	Ja	30
SSLClientDN_C <sup>2</sup> (SSL-Client - DN-Land)	Ja	Ja	*5
SSLClientDN_CN <sup>2</sup> (SSL-Client - allgemeiner DN-Name)	Ja	Ja	*5
SSLClientDN_L <sup>2</sup> (SSL-Client - DN-Adresse)	Ja	Ja	*5
SSLClientDN_O <sup>2</sup> (SSL-Client - DN-Organisation)	Ja	Ja	*5
SSLClientDN_OU <sup>2</sup> (SSL-Client - DN-Organisationseinheit)	Ja	Ja	*5
SSLClientDN_ST <sup>2</sup> (SSL-Client - DN-Staat)	Ja	Ja	*5
SSLClientKeyRing <sup>2</sup> (SSL-Client - Schlüsselringdatei)	Ja	Ja	<Null>
SSLClientKeyRingPW <sup>2</sup> (SSL-Client - Schlüsselringkennwortdatei)	Ja	Ja	<Null>
SSLProxyMode (SSL-Proxy-Modus)	Ja	Ja	false
SSLServer <sup>6</sup> (SSL-Server)	Ja	Ja	false
SSLServerAskClientAuth <sup>3</sup> (SSL-Server - Clientauthentifizierung anfordern)	Ja	Ja	false
SSLServerCipherSuites <sup>3</sup> (SSL-Server - Cipher Suites)	Ja	Ja	<Null>
SSLServerDN_C <sup>3</sup> (SSL-Server - DN-Land)	Ja	Ja	*5
SSLServerDN_CN <sup>3</sup> (SSL-Server - allgemeiner DN-Name)	Ja	Ja	*5
SSLServerDN_L <sup>3</sup> (SSL-Server - DN-Adresse)	Ja	Ja	*5
SSLServerDN_O <sup>3</sup> (SSL-Server - DN-Organisation)	Ja	Ja	*5
SSLServerDN_OU <sup>3</sup> (SSL-Server - DN-Organisationseinheit)	Ja	Ja	*5
SSLServerDN_ST <sup>3</sup> (SSL-Server - DN-Staat)	Ja	Ja	*5
SSLServerKeyRing <sup>3</sup> (SSL-Server - Schlüsselringdatei)	Ja	Ja	<Null>
SSLServerKeyRingPW <sup>3</sup> (SSL-Server - Schlüsselringkennwortdatei)	Ja	Ja	<Null>
Trace	Ja	Ja	0
UriName (URI-Name; Angaben zu Standard-einstellungen finden Sie auf S. 70) <sup>1</sup>	Ja	Ja	

### Anmerkungen:

1. Setzen Sie **HTTP** auf **true**, damit diese Eigenschaften wirksam werden.
2. Setzen Sie **SSL-Client** auf **true**, damit diese Eigenschaften wirksam werden.
3. Setzen Sie **SSL-Server** auf **true**, damit diese Eigenschaften wirksam werden.
4. Setzen Sie **Network Dispatcher Advisor** auf **true**, damit diese Eigenschaften wirksam werden.
5. Das Symbol "\*" stellt ein Platzhalterzeichen dar.
6. Die Eigenschaften **HTTP** und **SSL-Server** 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 **SSL-Server** gesetzt, erfolgt die Ausgabe einer Laufzeitausnahme.
7. Die Eigenschaften **HTTP** und **SOCKS-Server** 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 **SOCKS-Server** gesetzt, erfolgt die Ausgabe einer Laufzeitausnahme.
8. Setzen Sie **SOCKS-Client** auf **true**, damit diese Eigenschaften wirksam werden.
9. Setzen Sie **Quality of Service (QoS)** auf **true**, damit diese Eigenschaften wirksam werden.

## Referenzinformationen zum Abschnitt 'global'

Der Abschnitt `global` kann die folgenden Eigenschaften sowie alle der in „Referenzinformationen zum Abschnitt 'route'“ auf Seite 61 aufgeführten Eigenschaften enthalten, mit Ausnahme von **Listener-Port Zieladresse**, **Ziel-Port** und **Name**.

### 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.

### 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 **Befehls-Port** 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.

### 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 **mqiptYYYYMMDDHHmmSS.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.

### Maximale Protokolldateigröße

Die maximale Größe (in KB) der Verbindungsprotokolldatei **mqipt.log**. 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.

### 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**.

### 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 25. Standardwert dieser Eigenschaft ist **false**.

### 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:

### Aktiv

Die Route akzeptiert ankommende Verbindungen nur, wenn die Eigenschaft **Aktiv** 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 ebenfalls beendet.

### Clientzugriff

Die Route akzeptiert ankommende Clientkanalverbindungen nur, wenn diese Eigenschaft auf **true** gesetzt ist. Sie haben die Möglichkeit, MQIPTs 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 **WS-Managerzugriff** 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.

### 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.

### 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 diese Eigenschaft auf **false** setzen, 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:

- Quality of Service (QoS)
- SOCKS-Client
- SSL-Client
- SSL-Proxy-Modus

### 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 HTTP-Chunking nicht verwendet, muss **false** angegeben werden. 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.

### HTTP-Proxy

Der Hostname (oder die IP-Adresse in der Dezimalschreibweise mit Trennzeichen) des HTTP-Proxy, den alle Verbindungen dieser Route verwenden. 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.

### HTTP-Proxy-Port

Die Port-Adresse, die auf dem HTTP-Proxy verwendet wird. Standardwert ist **8080**. 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.

### **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 DISCONT. Beim Setzen von **Zeitlimit für Inaktivität** müssen Sie den Parameter DISCONT beachten. Bei Angabe von 0 gibt es kein Zeitlimit. Änderungen an dieser Eigenschaft werden erst nach einem Neustart der Route wirksam.

### **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.

### **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.

### **Maximale Anzahl von 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 **Maximale Anzahl an Verbindungs-Threads** 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 **Mindestanzahl von Verbindungs-Threads** 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.

### **Mindestanzahl von 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 **Maximal Anzahl von Verbindungs-Threads** 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.

### 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 **Network Dispatcher-Ersetzungsmodus** verwendet werden, muss diese Eigenschaft auf **true** gesetzt werden.

### 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 **Network Dispatcher Advisor** muss auf **true** gesetzt werden, damit diese Eigenschaft verwendet werden kann.

### 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.

### Quality of Service (QoS)

Setzen Sie diese Eigenschaft auf **true**, wenn QoS (Dienstgüte) 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
- SSL-Client
- SSL-Proxy-Modus
- SSL-Server

### 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 **Quality of Service (QoS)** auf **true** gesetzt), wird die Route bei Ausgabe eines Aktualisierungsbefehls (REFRESH) gestoppt und erneut gestartet. Alle Verbindungen zu dieser Route werden beendet.

### QoS an Zieladresse

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



### **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.

### **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 **SOCKS-Proxy-Hostname** und **SOCKS-Proxy-Port** 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
- SOCKS-Server
- SSL-Client
- SSL-Proxy-Modus

### **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 **SOCKS-Client** auf **true** gesetzt), wird die Route bei Ausgabe eines Aktualisierungsbefehls (REFRESH) gestoppt und erneut gestartet. Alle Verbindungen zu dieser Route werden beendet.

### **SOCKS-Proxy-Port**

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

### **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:

- SOCKS-Client
- SSL-Proxy-Modus
- SSL-Server

### **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 um einen anderen MQIPT handelt, der als SSL-Server 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:

- HTTP
- Quality of Service (QoS)
- SSL-Proxy-Modus

**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. 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.

**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. Wirkt sich eine Änderung an dieser Eigenschaft auf eine Route aus, wird bei Ausgabe des Aktualisierungsbefehls (REFRESH) der neue Wert übernommen. Die Route wird nicht beendet.

**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 Länder" gleichgesetzt. 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.

**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 allgemeinen Namen" gleichgesetzt. 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.

**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. 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.

**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. 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.

### **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. 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.

### **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. 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.

### **SSL-Client - Schlüsselringdatei**

Der vollständig qualifizierte Name der Schlüsselringdatei, die das Clientzertifikat enthält. Unter **Windows** muss als Dateitrennzeichen ein doppelter Backslash (\\) verwendet werden. Wurde **SSL-Client** auf **true** gesetzt, ist für diese Eigenschaft eine Angabe erforderlich. 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.

### **SSL-Client - Schlüsselringkennwortdatei**

Der vollständig qualifizierte Name der Datei, die das zum Öffnen der Client-Schlüsselringdatei erforderliche Kennwort enthält. Unter **Windows** muss als Dateitrennzeichen ein doppelter Backslash (\\) verwendet werden. Wurde **SSL-Client** auf **true** gesetzt, ist für diese Eigenschaft eine Angabe erforderlich. 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.

### **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
- Quality of Service (QoS)
- SOCKS-Client
- SSL-Client
- SSL-Server

### **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:

- Quality of Service (QoS)
- SOCKS-Server
- SSL-Proxy-Modus

### **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. 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.

### **SSL-Server - Cipher Suites**

Der Name der SSL-Cipher Suite, die auf der SSL-Serverseite verwendet werden soll. Hier können eine oder mehr unterstützte Cipher Suites angegeben werden. Erfolgt keine Angabe für diese Eigenschaft, verwendet der SSL-Server die unterstützten Cipher Suites aus der SSL-Serverschlüsseldatei. 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.

### **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. 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.

### **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. 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.

### **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. 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.

### **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. 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.

### **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. 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.

### **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. 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.

### **SSL-Server - Schlüsselringdatei**

Der vollständig qualifizierte Name der Schlüsselringdatei, die das Serverzertifikat enthält. Unter **Windows** muss als Dateitrennzeichen ein doppelter Backslash (\\) verwendet werden. Wurde **SSL-Server** auf **true** gesetzt, ist für diese Eigenschaft eine Angabe erforderlich. 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.

### SSL-Server - Schlüsselringkennwortdatei

Der vollständig qualifizierte Name der Datei, die das zum Öffnen der Server-Schlüsselringdatei erforderliche Kennwort enthält. Unter **Windows** muss als Dateitrennzeichen ein doppelter Backslash (\\) verwendet werden. Wurde **SSL-Server** auf **true** gesetzt, ist für diese Eigenschaft eine Angabe erforderlich. 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.

### 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.

### 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 10. WebSphere MQ Internet Pass-Thru - Erste Schritte

Dieses Kapitel enthält Hinweise zur Verwendung von MQIPT; es enthält schrittweise Anleitungen zum Einrichten einiger einfacher Konfigurationen, anhand derer Sie feststellen können, ob das Produkt erfolgreich installiert wurde.

Dieses Kapitel enthält die folgenden Abschnitte:

- „Voraussetzungen“
- „Beispielkonfigurationen“ auf Seite 72
- „Installationsfunktionstest“ auf Seite 72
- „SSL-Serverauthentifizierung“ auf Seite 74
- „SSL-Clientauthentifizierung“ auf Seite 77
- „HTTP-Proxy-Konfiguration“ auf Seite 80
- „Zugriffssteuerung konfigurieren“ auf Seite 83
- „Quality of Service (QoS) konfigurieren“ auf Seite 85
- „SOCKS-Proxy konfigurieren“ auf Seite 88
- „SOCKS-Client konfigurieren“ auf Seite 90
- „SSL-Proxy konfigurieren“ auf Seite 91
- „SSL-Testzertifikate erstellen“ auf Seite 95
- „MQIPT-Servlet konfigurieren“ auf Seite 96
- „Unterstützung für MQIPT-Clustering konfigurieren“ auf Seite 98
- „Eine Schlüsselringdatei erstellen“ auf Seite 102

---

### 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 MQIPTs sind jeweils auf eigenen Maschinen installiert.
- Sie sind mit dem Einreihen von Nachrichten in Warteschlangen unter Verwendung des Befehls `amqsputc` vertraut.
- Sie sind mit dem Abruf 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 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 auf die Datei **mqipt.conf** kopiert.
- Es wurden alle **route**-Abschnitte aus der Datei **mqipt.conf** gelöscht.
- Der Wert für die Eigenschaft **ClientAccess** (Clientzugriff) wurde auf **true** gesetzt.
- Der Wert für **Destination** (Zieladresse) wurde von **mqserver.company2.com** in die Adresse Ihres WS-Managers geändert.
- Für **DestinationPort** (Ziel-Port) wurde die von Ihrem WS-Manager verwendete Port-Adresse angegeben.
- Sie haben den Abschnitt „Voraussetzungen“ auf Seite 71 gelesen

---

## Installationsfunktionstest

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

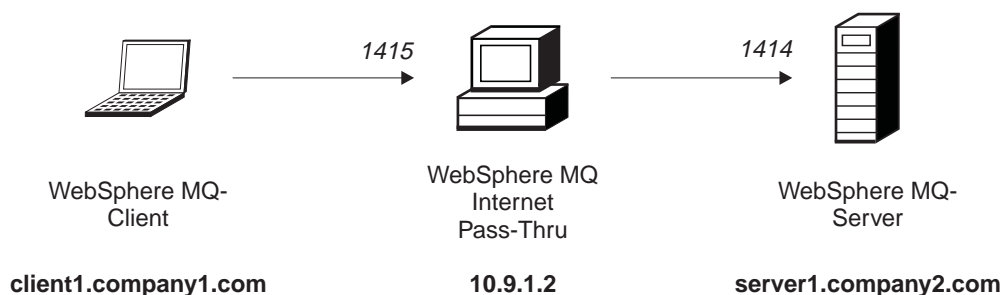


Abbildung 10. IVT-Netzplan



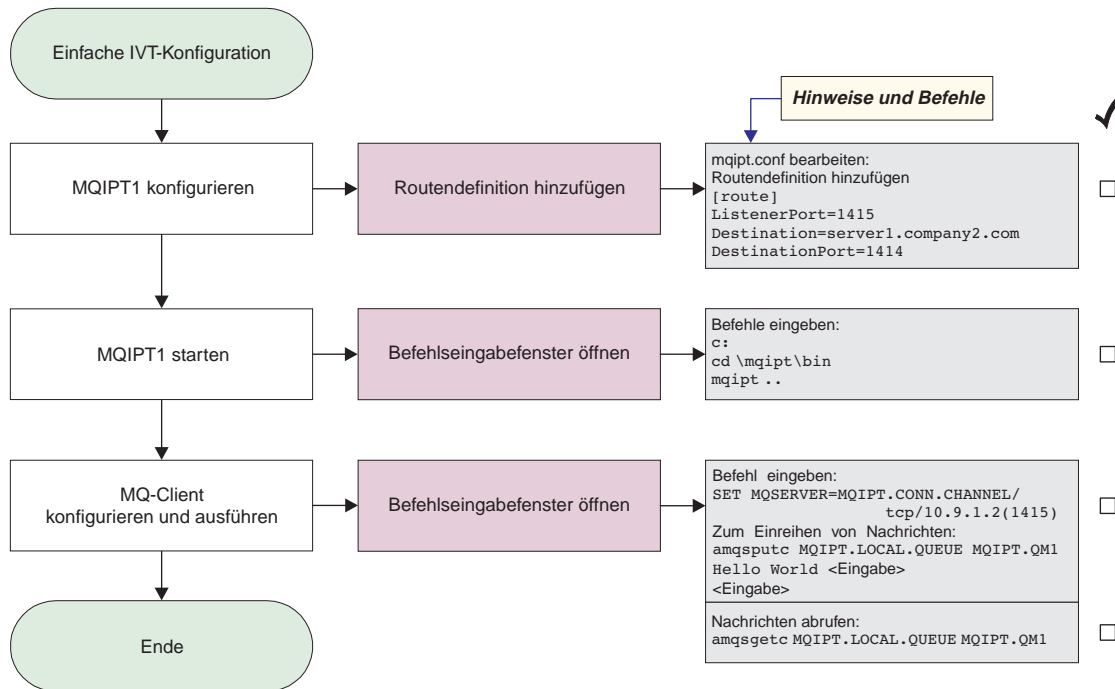


Abbildung 11. IVT-Konfiguration

Vor dem Beginn müssen folgende Schritte ausgeführt werden:

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. 2000-2002 Alle Rechte vorbehalten.
MQCPI001 WebSphere MQ Internet Pass-Thru Version 1.2 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
```

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 Beispielttestzertifikats (Schlüsselringdatei **sslsample.pfx**) getestet, indem ein WebSphere MQ-Client über zwei MQIPTs mit einem WebSphere MQ-Server verbunden wird. Im Verlauf 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 72 erstellten Datei **mqipt.conf**).

Hinweise zur Erstellung eines Testzertifikats für diese Beispielkonfiguration finden Sie unter „SSL-Testzertifikate erstellen“ auf Seite 95.

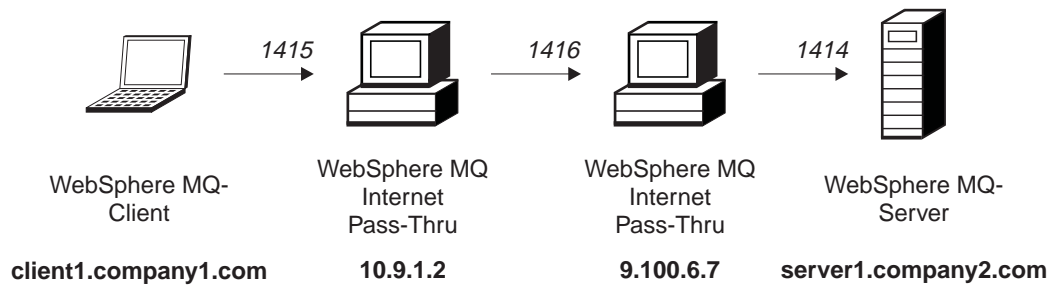


Abbildung 12. SSL-Servernetzplan

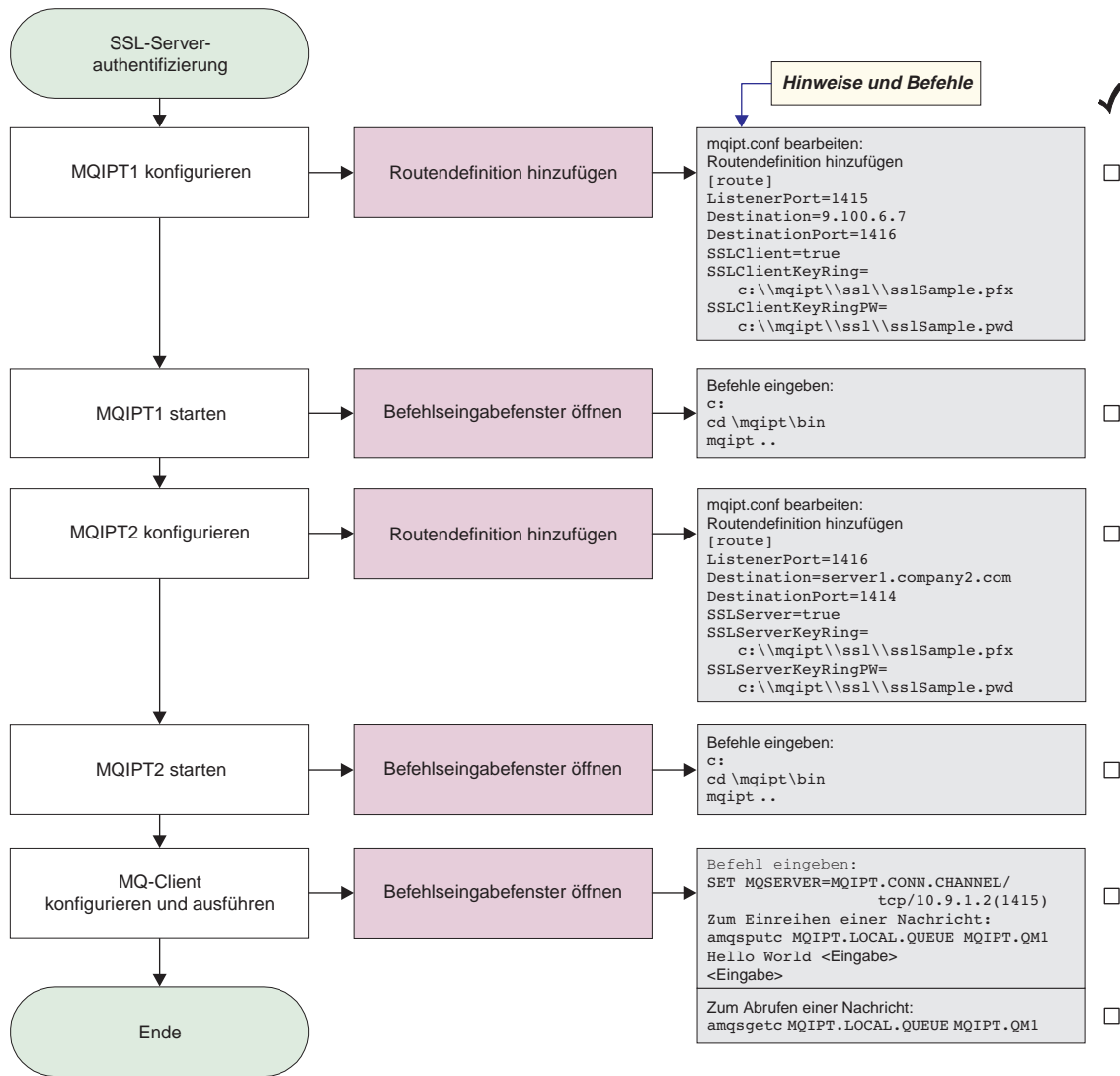


Abbildung 13. SSL-Serverauthentifizierung

### 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\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. 2000-2002 Alle Rechte vorbehalten.  
MQCPI001 WebSphere MQ Internet Pass-Thru Version 1.2 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=*
```

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. 2000-2002 Alle Rechte vorbehalten.  
MQCPI001 WebSphere MQ Internet Pass-Thru Version 1.2 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
```

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 Beispieldtestzertifikats überprüft. Es wird eine Server- und eine Clientauthentifizierung durchgeführt. Im Verlauf 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 72 erstellten Datei **mqipt.conf**).

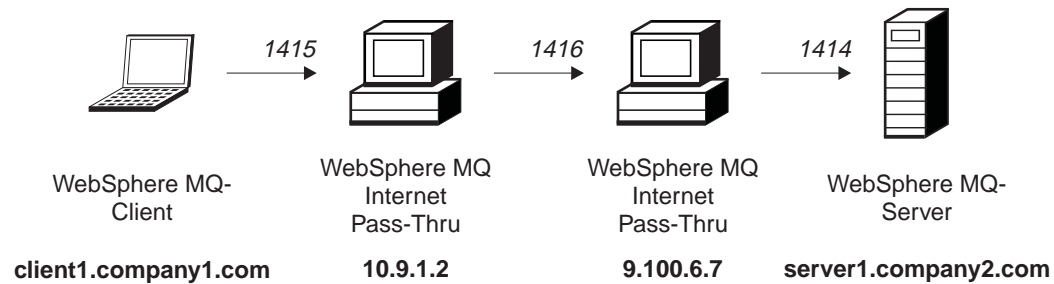


Abbildung 14. SSL-Clientnetzplan

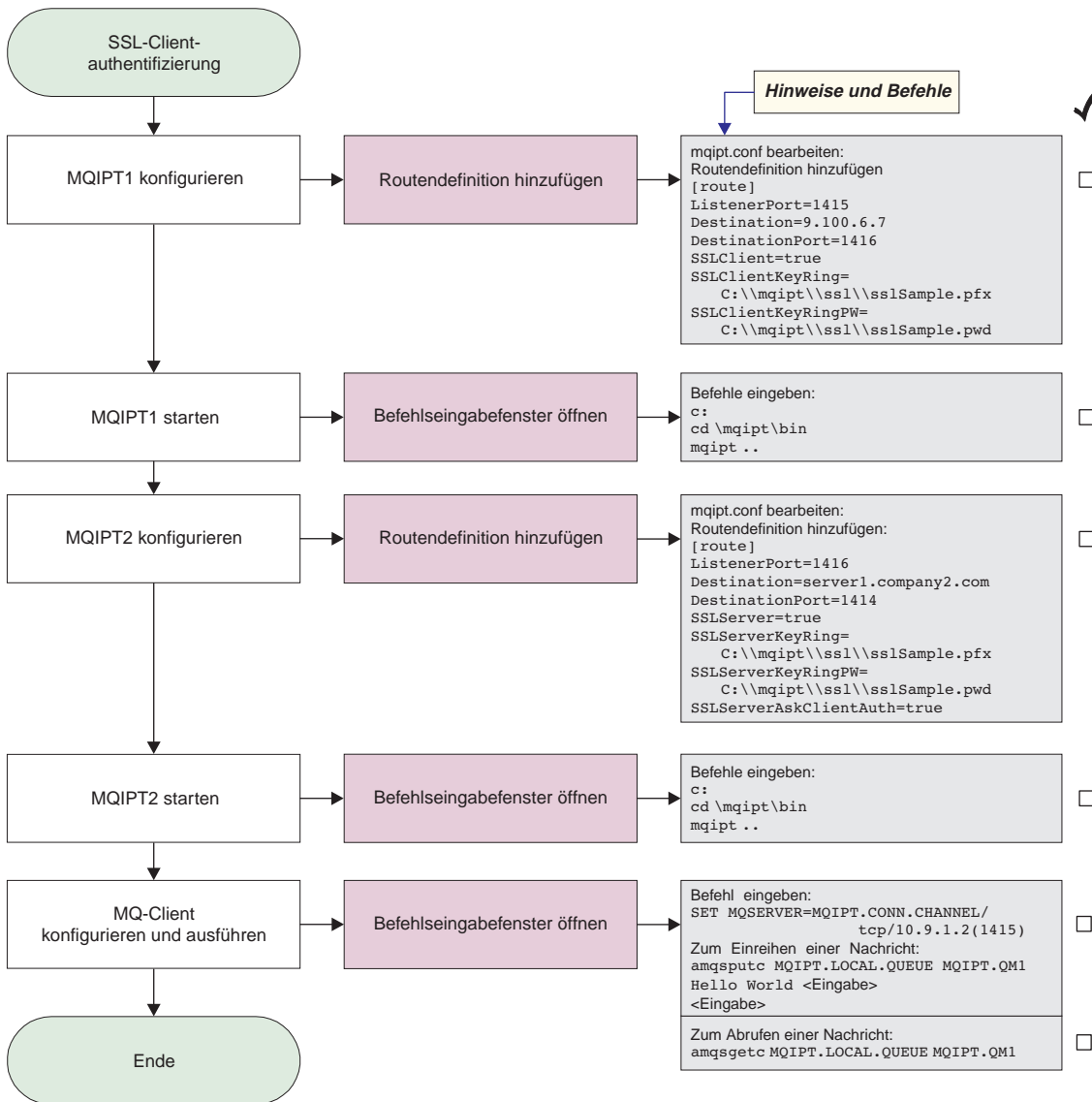


Abbildung 15. SSL-Clientauthentifizierung

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. 2000-2002 Alle Rechte vorbehalten.  
MQCPI001 WebSphere MQ Internet Pass-Thru Version 1.2 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=*
```

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. 2000-2002 Alle Rechte vorbehalten.  
MQCPI001 WebSphere MQ Internet Pass-Thru Version 1.2 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
```

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. Reichen 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 abgebaut wird
- **PersistTimeout** (Zeitlimit für permanente Verbindung) muss auf "12 Stunden" gesetzt sein; dieser Wert gibt die Lebensdauer einer Verbindung an

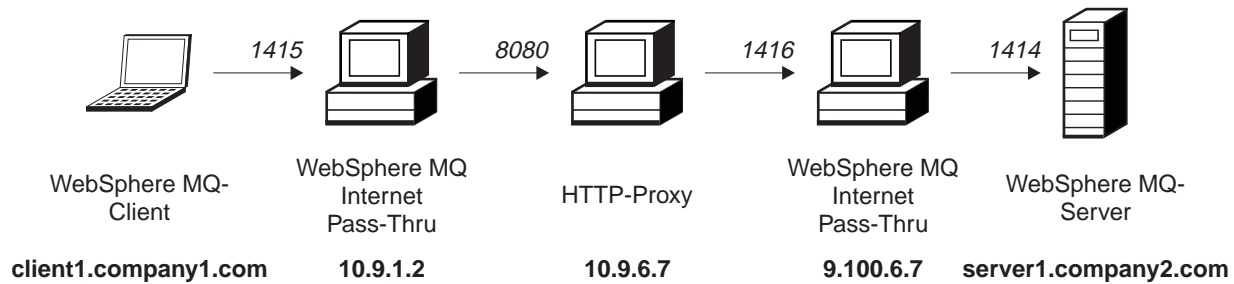


Abbildung 16. HTTP-Proxy-Netzplan



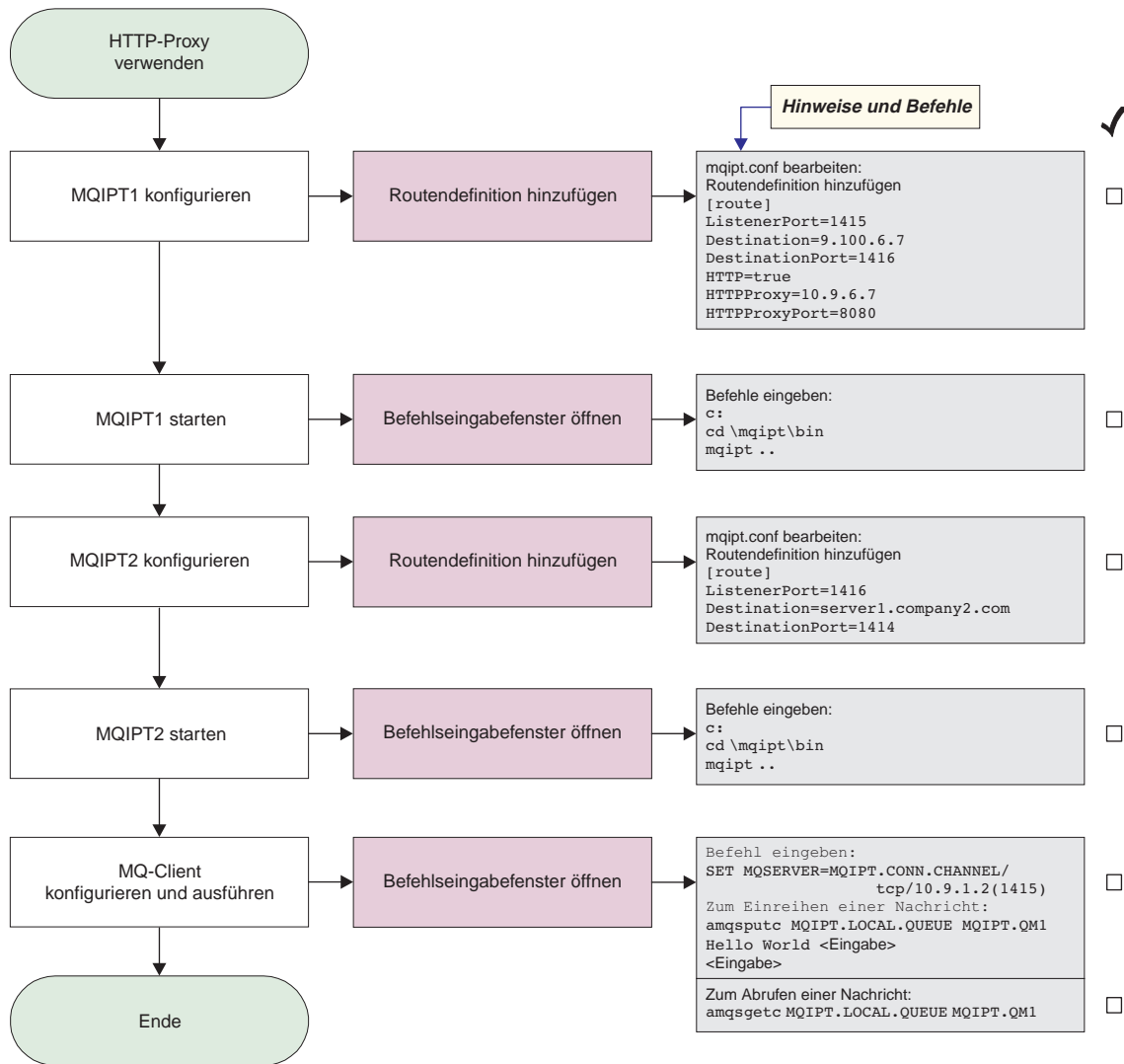


Abbildung 17. HTTP-Proxy-Konfiguration

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. 2000-2002 Alle Rechte vorbehalten.  
MQCPI001 WebSphere MQ Internet Pass-Thru Version 1.2 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)
```

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. 2000-2002 Alle Rechte vorbehalten.  
MQCPI001 WebSphere MQ Internet Pass-Thru Version 1.2 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
```

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. Reichen 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.

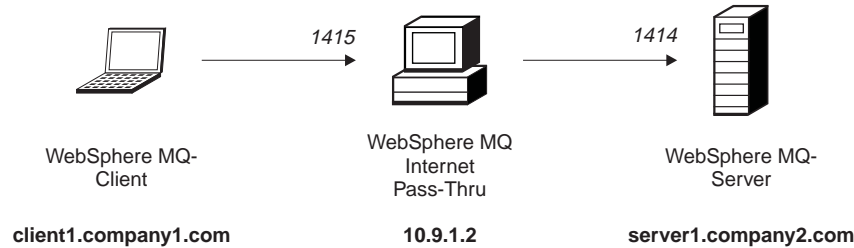


Abbildung 18. Netzplan für die Zugriffssteuerung

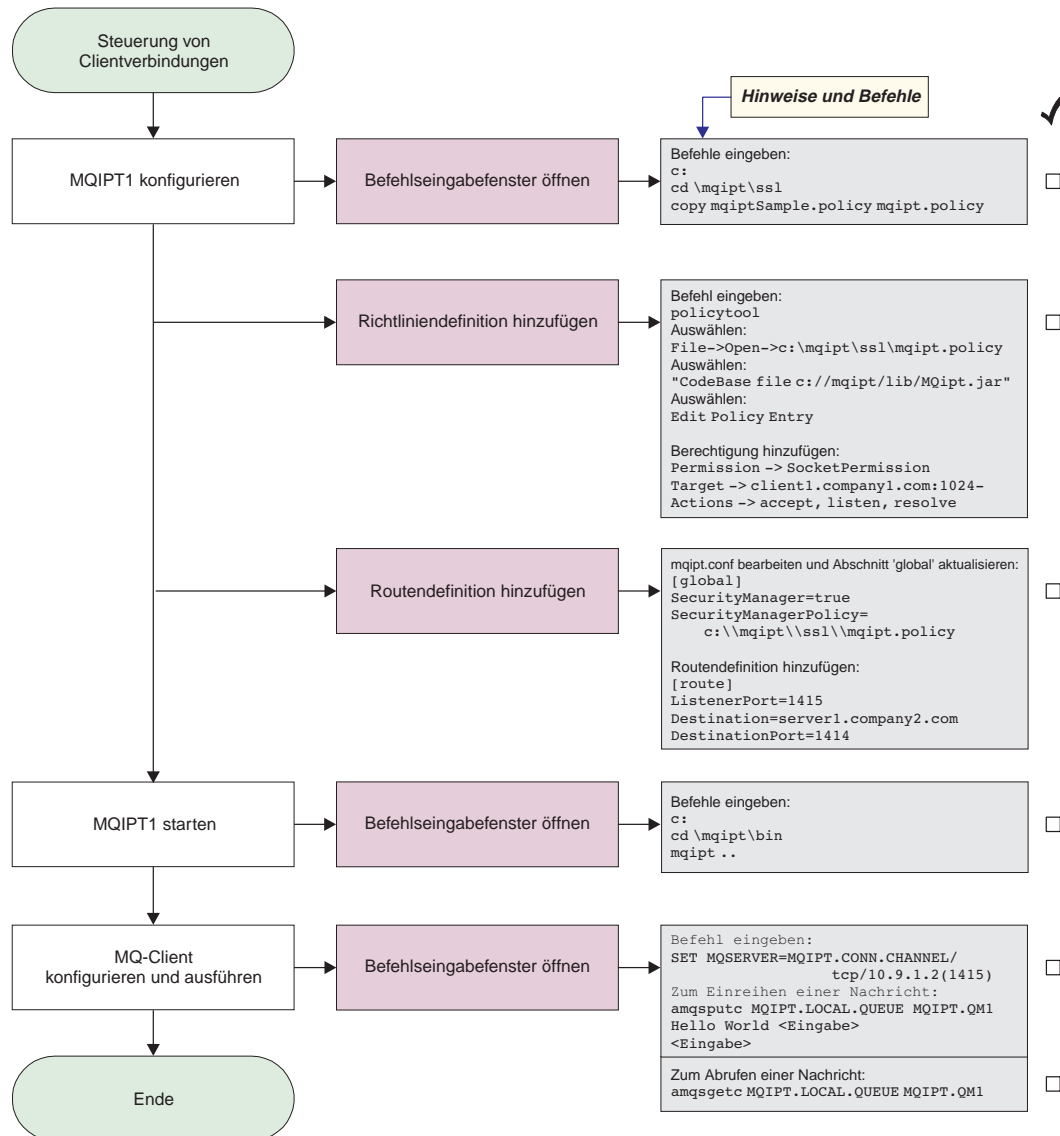


Abbildung 19. Konfiguration der Zugriffssteuerung

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. 2000-2002 Alle Rechte vorbehalten.  
MQCPI001 WebSphere MQ Internet Pass-Thru Version 1.2 wird gestartet.  
MQCPI004 Die Konfigurationsdaten aus C:\mqipt\mqipt.conf werden gelesen.  
MQCPI055 Die Richtlinie für den Java Security Manager (java.security.policy)  
wird auf c:\mqipt\mqipt.policy  
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
```

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. Reichen 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 Dienstgüte (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 Pagent (Richtlinienagenten) können QoSToCaller (QoS an Anrufer) und QoSToDest (QoS an Zieladresse) die folgenden Prioritätsstufen zugeordnet werden:

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

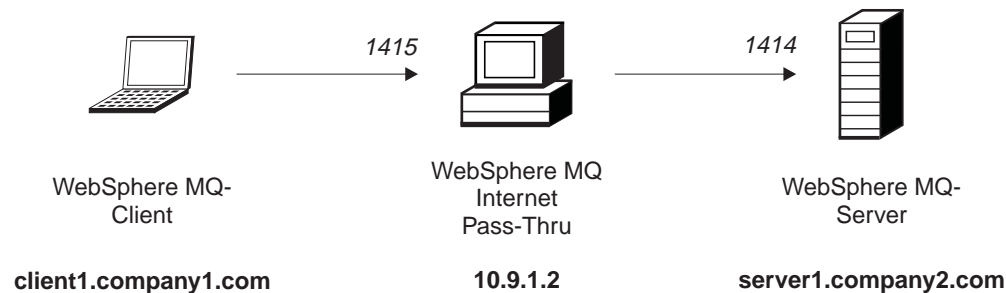


Abbildung 20. QoS-Netzplan

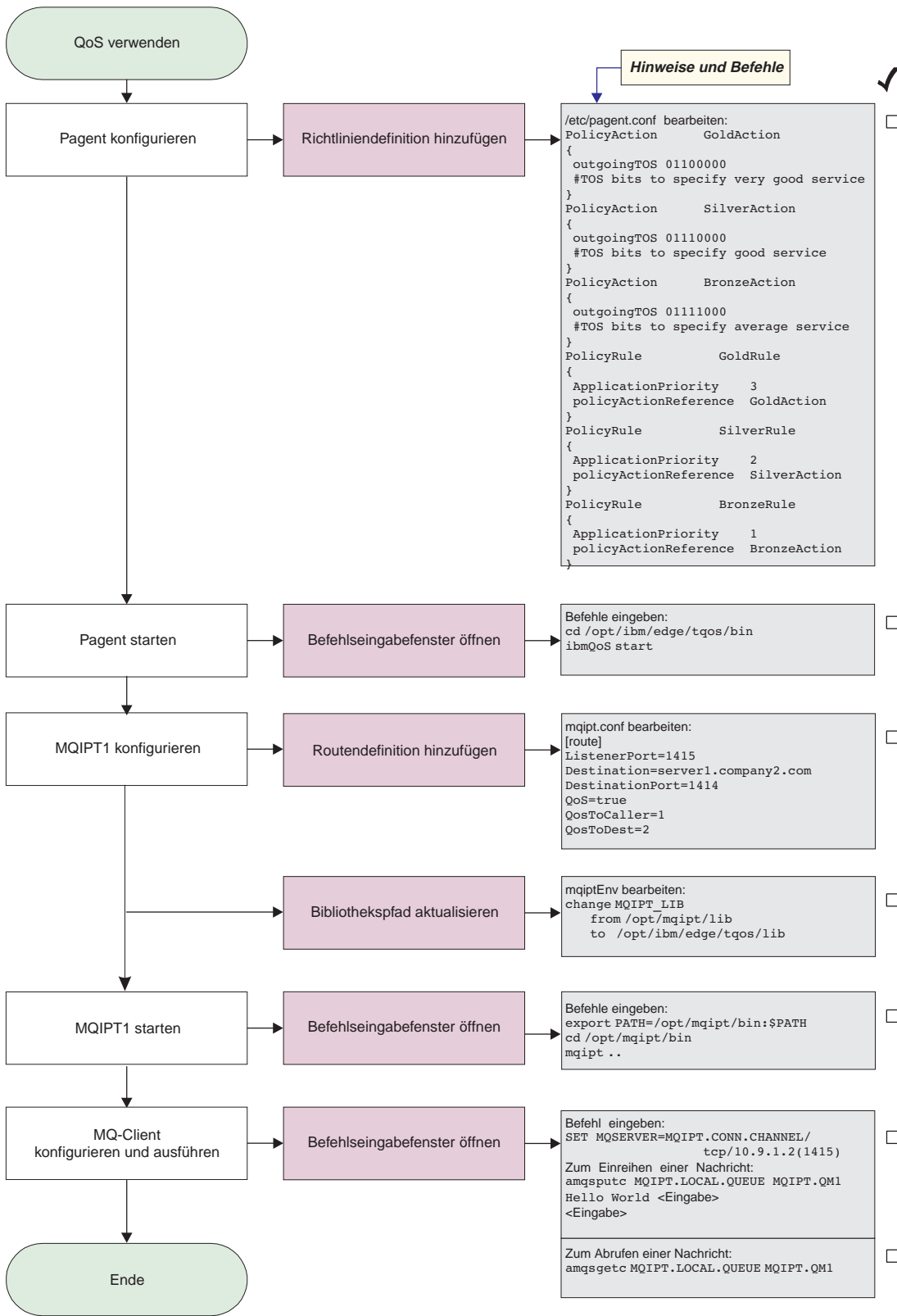


Abbildung 21. QoS-Konfiguration

1. Konfigurieren Sie den Richtlinienagenten (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
}
```

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. 2000-2002 Alle Rechte vorbehalten.  
MQCPI001 WebSphere MQ Internet Pass-Thru Version 1.2 wird gestartet.  
MQCPI004 Die Konfigurationsdaten aus /opt/mqiplt/mqiplt.conf werden gelesen.  
MQCPI011 Die Protokolldateien werden im Pfad /opt/mqiplt/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
```

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. Reihen 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 **Zieladresse** und **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 verweisen.
- Die Unterstützung für SOCKS V5 muss aktiviert werden.
- Die Benutzerauthentifizierung muss deaktiviert werden.
- Es dürfen nur Verbindungen zur MQIPT-Netzadresse hergestellt werden.

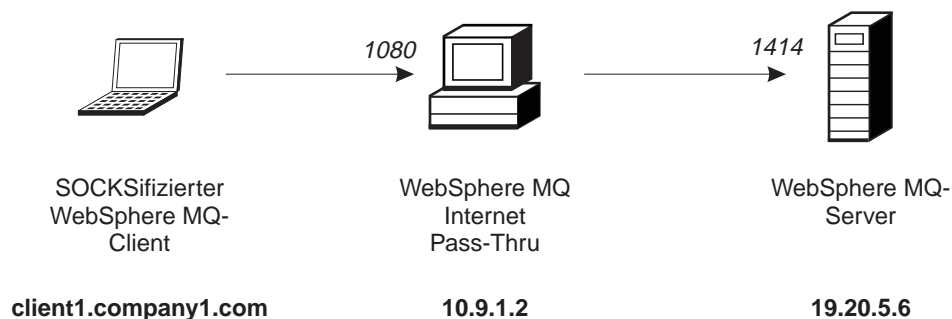


Abbildung 22. Netzplan für SOCKS-Proxy



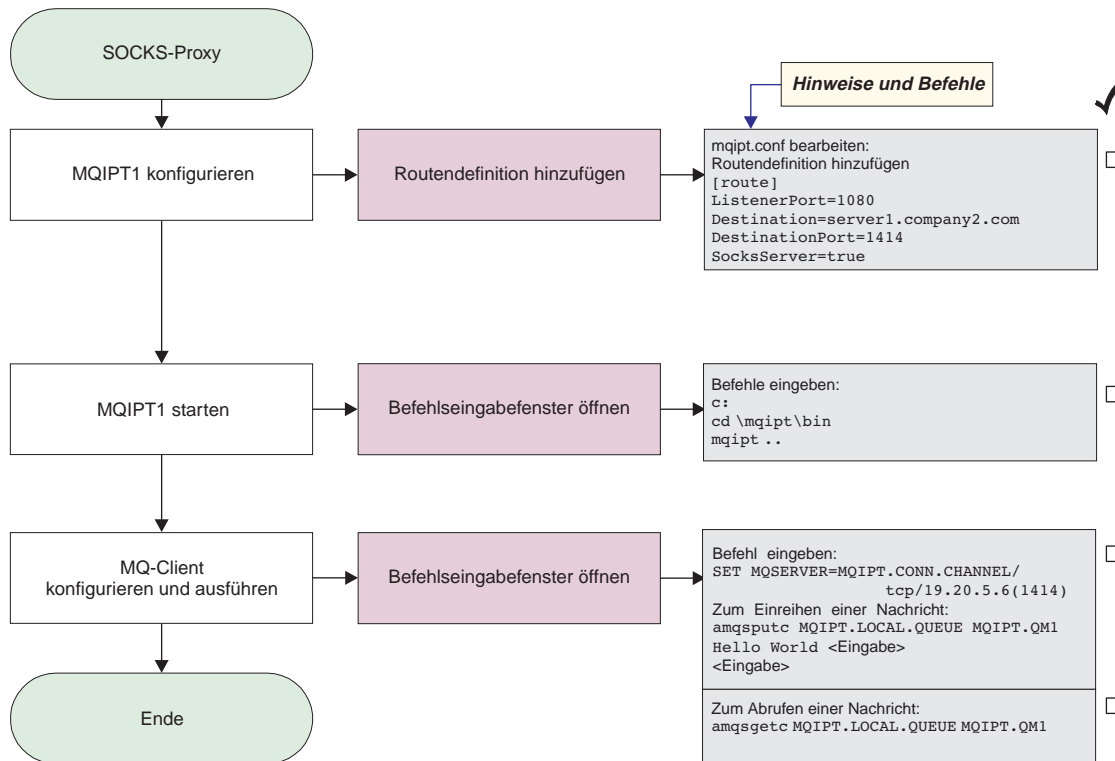


Abbildung 23. SOCKS-Proxy-Konfiguration

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. 2000-2002 Alle Rechte vorbehalten.
MQCPI001 WebSphere MQ Internet Pass-Thru Version 1.2 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
```
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. Reihsen 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 88, nur dass der MQIPT, und nicht der WebSphere MQ-Client eine SOCKSifizierte Verbindung herstellt.

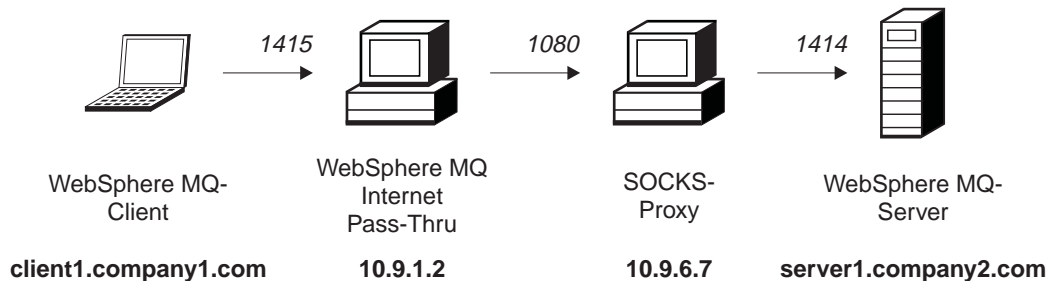


Abbildung 24. SOCKS-Clientnetzplan

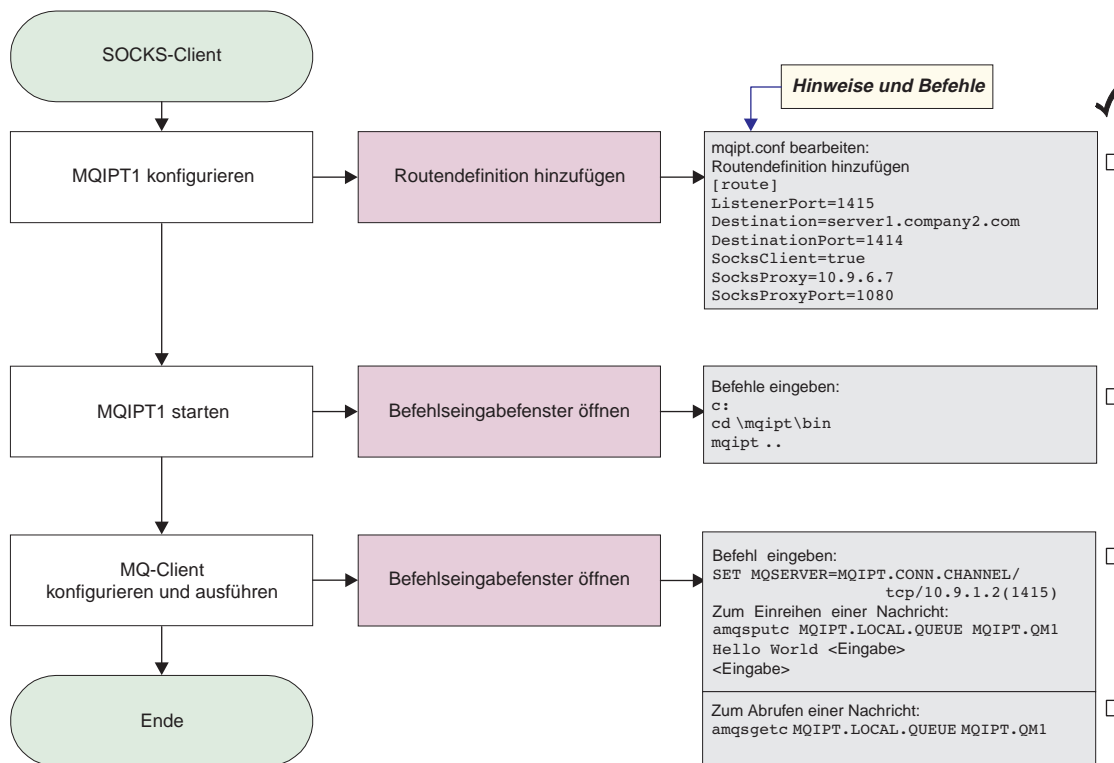


Abbildung 25. SOCKS-Clientkonfiguration

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. 2000-2002 Alle Rechte vorbehalten.
MQCPI001 WebSphere MQ Internet Pass-Thru Version 1.2 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)
```

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-Proxy konfigurieren

In diesem Beispiel wird MQIPT im SSL-Proxy-Modus betrieben, so dass der MQIPT SSL-Verbindungsanforderungen von einem SSL-Client akzeptiert und im Tunnelungsverfahren an einen SSL-Server weiterleitet.

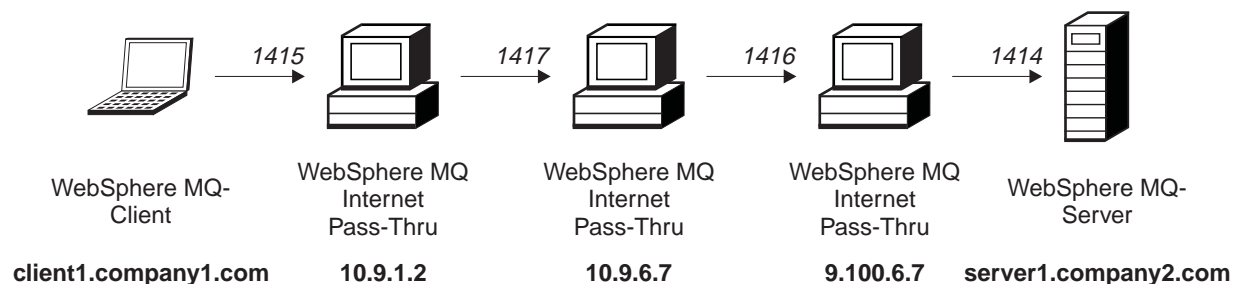


Abbildung 26. SSL-Proxy-Netzplan

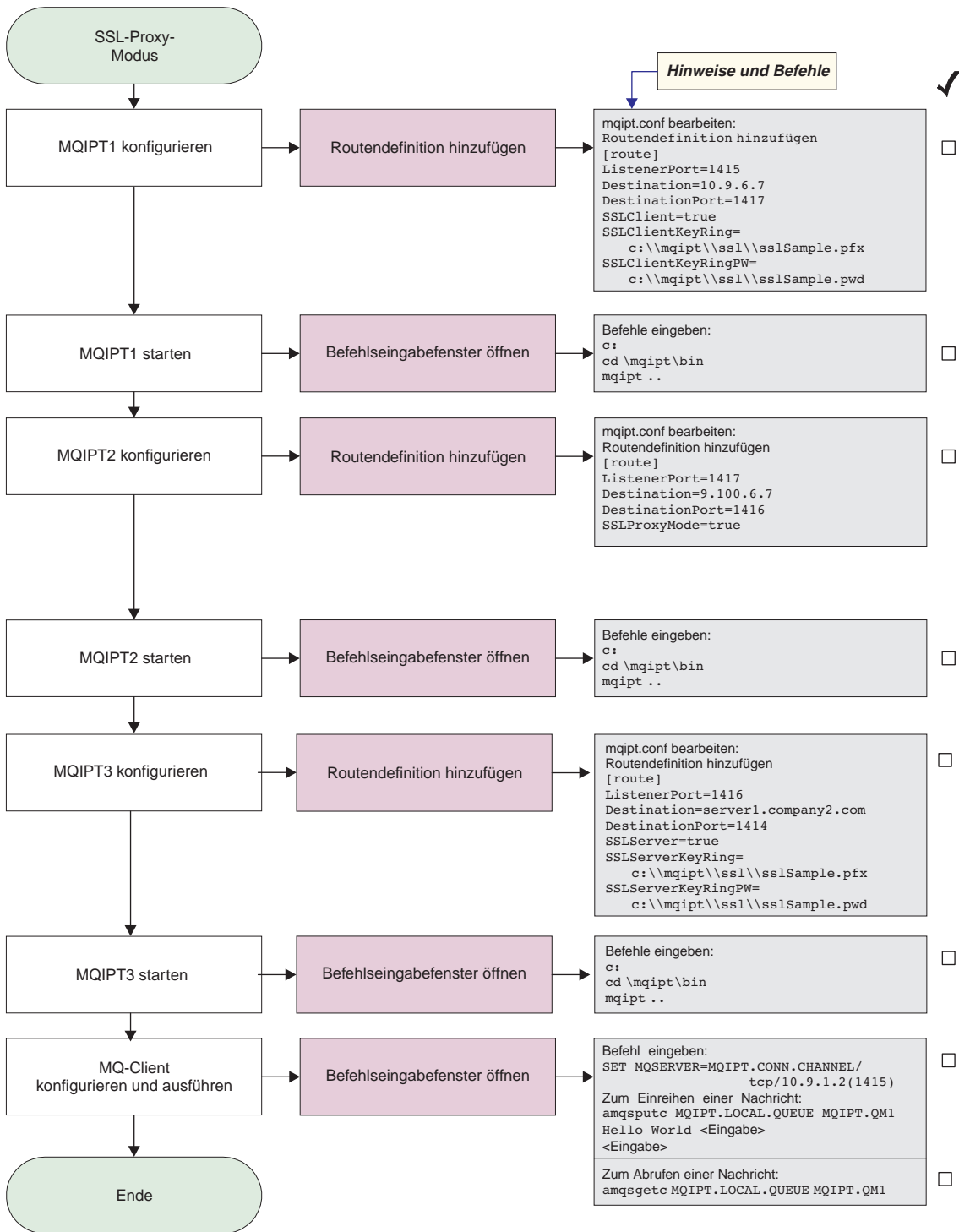


Abbildung 27. SSL-Proxy-Konfiguration

1. Konfigurieren Sie MQIPT1.

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

```
[route]
ListenerPort=1415
Destination=10.9.6.7
DestinationPort=1417
SSLClient=true
SSLClientKeyRing=c:\mqipt\ssl\sslSample.pfx
SSLClientKeyRingPW=c:\mqipt\ssl\sslSample.pwd
```

2. 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. 2000-2002 Alle Rechte vorbehalten.
MQCPI001 WebSphere MQ Internet Pass-Thru Version 1.2 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 ....10.9.6.7(1417)
MQCPI035 ....verwendet MQ-Protokolle
MQCPI036 ....SSL-Clientseite mit folgenden Eigenschaften aktiviert:
MQCPI031 .....Cipher Suites <Null>
MQCPI032 .....Schlüsselringdatei c:\mqipt\ssl\sslSample.pfx
MQCPI047 .....CA-Schlüsselringdatei <Null>
MQCPI038 .....registrierte Namen CN=* O=* OU=* L=* ST=* C=*
```

3. Konfigurieren Sie MQIPT2.

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

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

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. 2000-2002 Alle Rechte vorbehalten.
MQCPI001 WebSphere MQ Internet Pass-Thru Version 1.2 wird gestartet.
MQCPI004 Die Konfigurationsdaten aus C:\mqipt\mqipt.conf werden gelesen.
MQCPI011 Die Protokolldateien werden im Pfad C:\mqipt\logs gespeichert.
MQCPI006 Route 1417 wurde gestartet und leitet Nachrichten weiter an:
MQCPI034 ....9.100.6.7(1416)
MQCPI035 ....verwendet SSL-Proxy-Modus
```

5. Konfigurieren Sie MQIPT3.

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

6. Starten Sie MQIPT3.

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. 2000-2002 Alle Rechte vorbehalten.
MQCPI001 WebSphere MQ Internet Pass-Thru Version 1.2 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
MQCPI037 ....SSL-Serverseite mit folgenden Eigenschaften aktiviert:
MQCPI031 .....Cipher Suites <Null>
MQCPI032 .....Schlüsselringdatei c:\mqipt\ssl\sslSample.pfx
MQCPI047 .....CA-Schlüsselringdatei <Null>
MQCPI038 .....registrierte Namen CN=* O=* OU=* L=* ST=* C=*
MQCPI033 .....Clientauthentifizierung ist auf false gesetzt
```

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.

---

## 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 Angaben 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 74 verwendet werden.

# MQIPT-Servlet konfigurieren

In diesem Beispiel wird ein Tomcat Anwendungsserver verwendet; es wird davon ausgegangen, dass dieser Server im Verzeichnis `c:\jakarta-tomcat-4.0.1` installiert wurde.

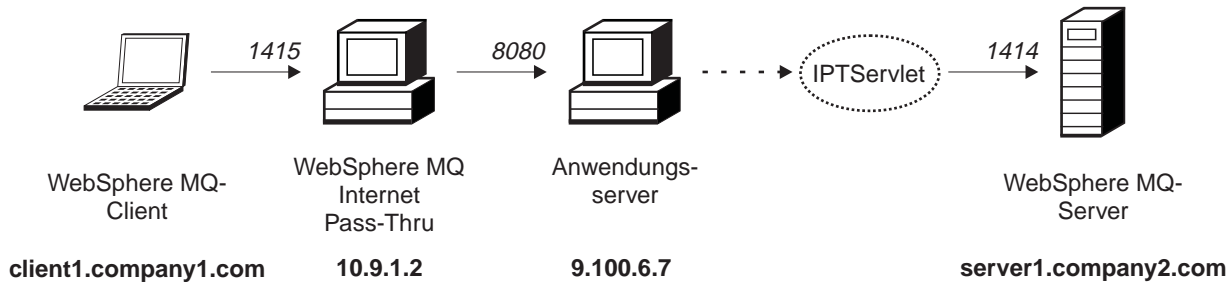


Abbildung 28. Servlet-Netzplan

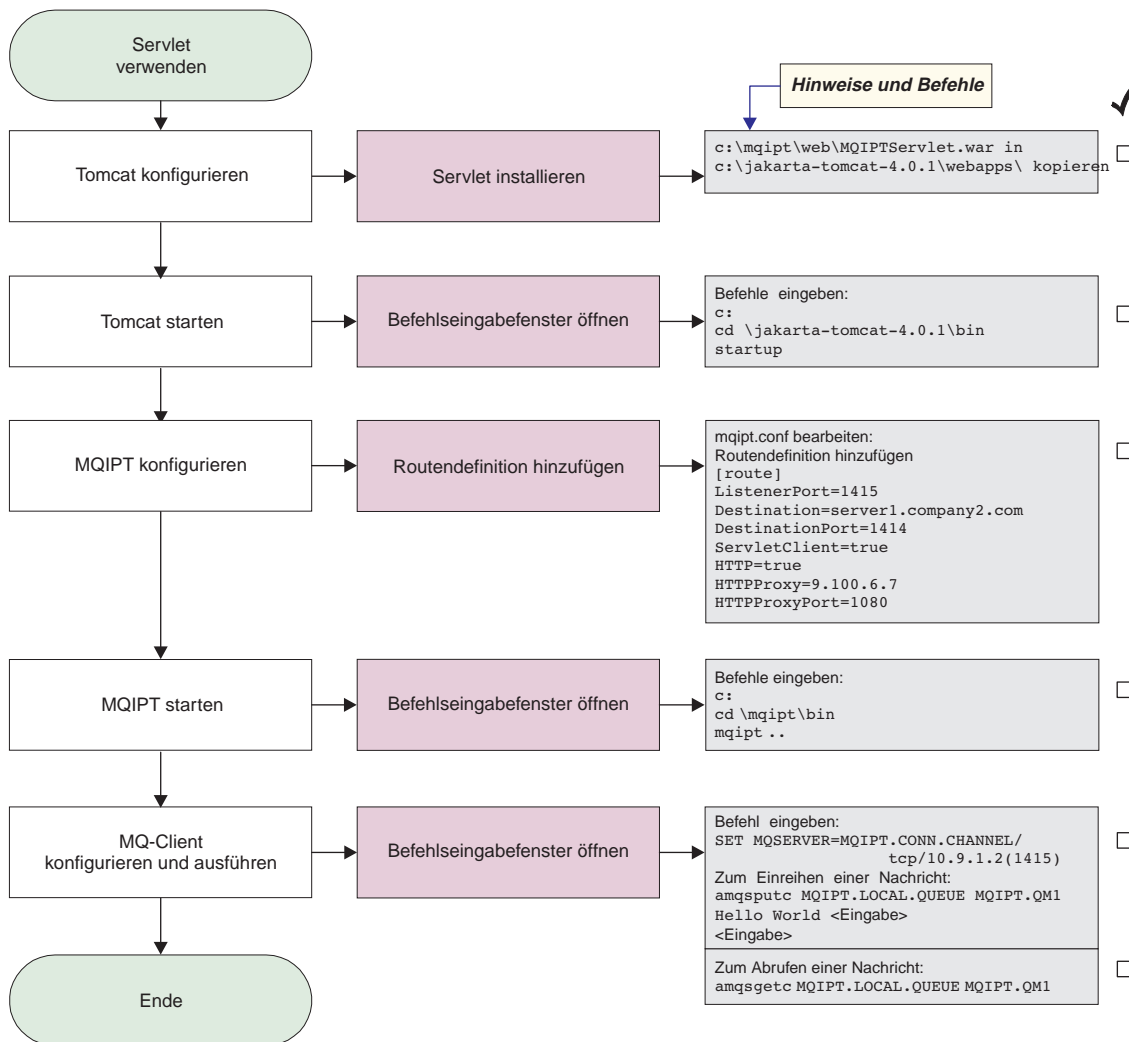


Abbildung 29. Servlet-Konfiguration



1. Konfigurieren Sie Tomcat.  
Kopieren Sie:  
c:\mqipt\web\MQIPTServlet.war  
  
in:  
c:\jakarta-tomcat-4.0.1\webapps
2. Starten Sie Tomcat.  
Öffnen Sie ein Befehlseingabefenster, und geben Sie Folgendes ein:  
c:  
cd \jakarta-tomcat-4.0.1\bin  
startup
3. 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=9.100.6.7  
HTTPProxyPort=8080
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. 2000-2002 Alle Rechte vorbehalten.
MQCPI001 WebSphere MQ Internet Pass-Thru Version 1.2 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 9.100.6.7(8080)
MQCPI059 ....Servlet-Client aktiviert
```

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. Reihem 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.

## Unterstützung für MQIPT-Clustering konfigurieren

Für diese Beispielkonfiguration müssen zusätzlich zu den unter „Voraussetzungen“ auf Seite 71 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.

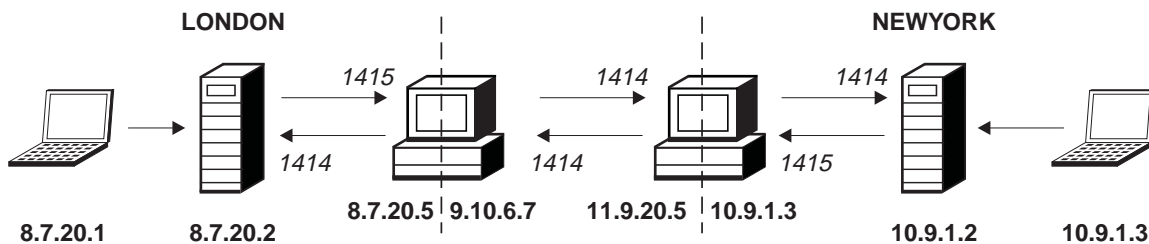


Abbildung 30. Clustering-Netzplan

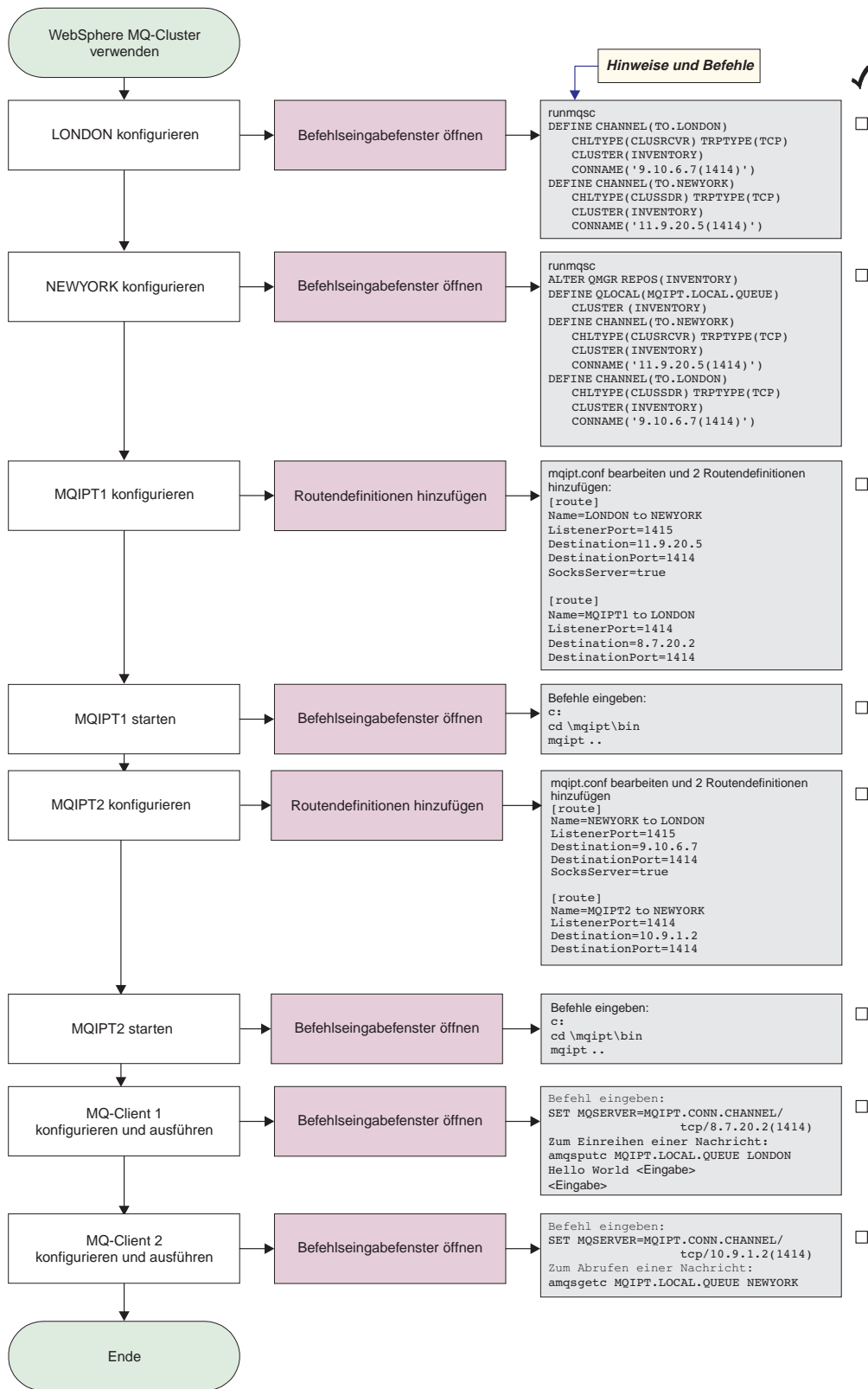


Abbildung 31. Clustering-Konfiguration

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. 2000-2002 Alle Rechte vorbehalten.
MQCPI001 WebSphere MQ Internet Pass-Thru Version 1.2 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
MQCPI006 Route 1414 wurde gestartet und leitet Nachrichten weiter an:
MQCPI034 ....8.7.20.2(1414)
MQCPI035 ....verwendet MQ-Protokolle
```

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. 2000-2002 Alle Rechte vorbehalten.
MQCPI001 WebSphere MQ Internet Pass-Thru Version 1.2 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
MQCPI006 Route 1414 wurde gestartet und leitet Nachrichten weiter an:
MQCPI034 ....10.9.1.2(1414)
MQCPI035 ....verwendet MQ-Protokolle
```

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 74; 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 77; 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
```





---

## Kapitel 11. 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 108

---

### 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** (SSL-Client - Schlüsselringdatei)
  - **SSLClientCAKeyRing** (SSL-Client - CA-Schlüsselringdatei)
  - **SSLServerKeyRing** (SSL-Server - Schlüsselringdatei)
  - **SSLServerCAKeyRing** (SSL-Server - CA-Schlüsselringdatei)
- Die SSL-Schlüsselringkennwortdateien, die in **mqipt.conf** über die folgenden Eigenschaften definiert sind:
  - **SSLClientKeyRingPW** (SSL-Client - Schlüsselringkennwortdatei)
  - **SSLClientCAKeyRingPW** (SSL-Client - CA-Schlüsselringkennwortdatei)
  - **SSLServerKeyRingPW** (SSL-Server - Schlüsselringkennwortdatei)
  - **SSLServerCAKeyRingPW** (SSL-Server - CA-Schlüsselringkennwortdatei)
- 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. 32 auf Seite 106 durchgehen. Die Zahlen beziehen sich auf die Anmerkungen am Ende des Diagramms.

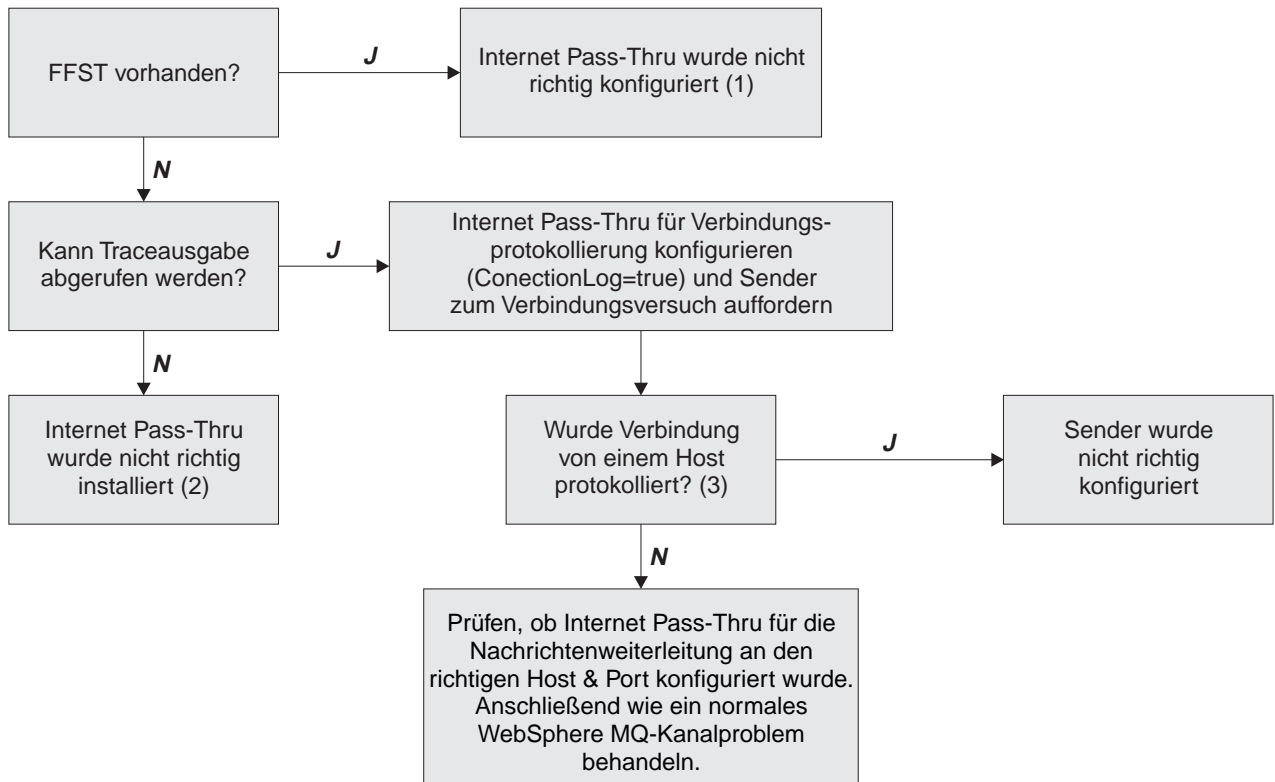


Abbildung 32. Fehlerbestimmung - Ablaufdiagramm

#### Anmerkungen:

1. Falls FFST-Berichte vorliegen (im Unterverzeichnis **errors**), so 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 eine 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, diesem Fall " ..".

MQIPT wird daraufhin gestartet, und es wird nach der Konfigurationsdatei im Ausgangsverzeichnis gesucht. Überprüfen Sie das Unterverzeichnis **errors** auf Fehlernachrichten und FFSTs.

Überprüfen Sie die Textausgabe von MQIPT auf Fehlernachrichten, 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 34.

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 MQIPTs 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 von 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 von 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 12. Nachrichten

Bei Ausführung von MQIPT über die Befehlszeile werden einige Informations- und Fehlernachrichten an der Konsole angezeigt.

Es gilt Folgendes:

- Bei MQCAxxxx-Nachrichten handelt es sich um Nachrichten des Verwaltungsclients.
- Bei MQCPxxxx-Nachrichten handelt es sich um MQIPT-Nachrichten.
- Bei MQCXIxxx-Nachrichten handelt es sich um Informationsnachrichten.
- Bei MQCXExxx-Nachrichten handelt es sich um Fehlernachrichten.

---

### 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 keine Zieladresse im gleichnamigen Feld angegeben.

**Benutzeraktion:** Geben Sie eine gültige Zieladresse ein.

---

### MQCAE006 Es wurde kein gültiger Ziel-Port definiert.

**Erläuterung:** Beim Hinzufügen einer Route wurde kein Ziel-Port im gleichnamigen Feld angegeben.

**Benutzeraktion:** Geben Sie einen gültigen Ziel-Port ein.

---

### MQCAE007 Es wurde kein gültiger Listener-Port definiert.

**Erläuterung:** Beim Hinzufügen einer Route wurde kein Listener-Port im gleichnamigen Feld 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 Acrobat Reader in der Systemvariable PATH verfügbar 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 Eine Datei für die Onlinehilfe wurde nicht gefunden.

**Erläuterung:** Die Datei `guiadmin.pdf` konnte nicht gefunden werden.

**Benutzeraktion:** Stellen Sie sicher, dass die Datei im Unterverzeichnis **doc** 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 wiederholen Sie den Befehl. 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 **guideadmin.properties** fehlerhaft, und 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 **guideadmin.jar** in der Systemvariable CLASSPATH definiert ist.
- Prüfen Sie, ob die Datei **guideadmin.properties** in der Datei **guideadmin.jar** angegeben ist.
- Prüfen Sie, ob die Nachrichtennummer in der Datei **guideadmin.properties** definiert 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:** Unter Umständen ist die Datei **guideadmin.properties** fehlerhaft; gehen Sie wie folgt vor:

- Prüfen Sie, ob die Datei **guideadmin.jar** in der Systemvariable CLASSPATH definiert ist.
- Prüfen Sie, ob die Datei **guideadmin.properties** in der Datei **guideadmin.jar** angegeben ist.
- Prüfen Sie, ob die Nachrichtennummer in der Datei **guideadmin.properties** definiert 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-Zugriffparameter.

**Erläuterung:** Bei dem Versuch, MQIPT-Zugriffparameter 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 wiederholen Sie den Befehl. 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 wiederholen Sie den Befehl. 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 **Fernes Beenden** nicht in der Konfigurationsdatei aktiviert wurde.

**Benutzeraktion:** Damit der MQIPT fern abgeschaltet werden kann, müssen Sie die Eigenschaft `RemoteShutDowns` (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:

- Der MQIPT ist nicht aktiv.
- Der MQIPT ist am eigenen Befehls-Port nicht empfangsbereit.
- Der Befehls-Port des MQIPTs wird nur von einem 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:

- Der MQIPT ist nicht aktiv.
- Der MQIPT ist am eigenen Befehls-Port nicht empfangsbereit.
- Der Befehls-Port des MQIPTs wird nur von einem 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:

- Der MQIPT ist nicht aktiv.
- Der 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:** Die MQIPT-Route 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:

- Der MQIPT ist nicht aktiv.
- Der 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 Systemvariable 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** Der Protokollpfadparameter {0} ist ungültig.

**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 **Befehls-Port** oder **Listener-Port** 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** (Listener-Port) 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 gültige Listener-Port-Nummer an.

---

**MQCPE014** Der Wert {0} für die Eigenschaft ListenerPort ist ungültig.

**Erläuterung:** Für die Eigenschaft **Listener-Port** einer Route wurde eine ungültige Port-Adresse angegeben.

**Benutzeraktion:** Als Port-Adresse muss eine Nummer zwischen 1 und 65535 angegeben werden. 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 Systemvariable 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 (Maximale Anzahl Verbindungs-Threads) ist {0}. Er muss größer als der aktuelle Wert {1} sein.

**Erläuterung:** Nach dem Start der Route kann die Eigenschaft Maximale Anzahl von 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 (Zieladresse) angegeben.

**Erläuterung:** Die Eigenschaft Destination (Ziel-Adresse) 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 CommandPort (Befehls-Port) 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 den Befehls-Port an.

---

**MQCPE023** Die Beendigungsanforderung vom Verwaltungsclient {0} wird ignoriert, weil diese Funktion inaktiviert ist.

**Erläuterung:** Der Versuch, den MQIPT fern abzuschalten, ist fehlgeschlagen, da Fernes Beenden nicht in der Konfigurationsdatei aktiviert wurde.

**Benutzeraktion:** Damit der MQIPT fern abgeschaltet werden kann, müssen Sie die Eigenschaft RemoteShutDowns (Fernes Beenden) in der Konfigurationsdatei auf true setzen.

---

**MQCPE024** Der vom MQIPT-Controller empfangene Befehl wurde nicht erkannt.

**Erläuterung:** Der MQIPT hat am Befehls-Port einen Befehl empfangen, den er nicht erkennt.

**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 den Befehls-Port {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 das Ausgangsverzeichnis von MQIPT voll 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 Systemumgebungsvariable `CLASSPATH` gefunden.

**Benutzeraktion:** Fügen Sie der Systemumgebungsvariable `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 Systemumgebungsvariable `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` (Befehls-Port) 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.

---

**MQCPE045 ....Name für HTTP-Proxy fehlt.**

**Erläuterung:** Wenn die Eigenschaft HTTP auf true gesetzt wurde, muss für die Eigenschaft HTTPProxy (HTTP-Proxy) 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 des Java Security Manager {0}**

**Erläuterung:** Bei dem Versuch, den Java Security Manager zu starten bzw. stoppen wurde eine Ausnahme 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.

---

**MQCPE055 ....Name für Socks-Proxy fehlt.**

**Erläuterung:** Wenn die Eigenschaft `SocksClient` (SOCKS-Client) auf `true` gesetzt wurde, muss für die Eigenschaft `SocksProxy` (SOCKS-Proxy) 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 Verbindung zwischen {0} und Host {1} wurde geschlossen. Das SSL-Protokoll ({2}) wurde nicht erkannt.**

**Erläuterung:** Für die Route wurde der SSL-Proxy-Modus definiert, und der Eingangsdatenfluss wurde nicht erkannt.

**Benutzeraktion:** Stellen Sie sicher, dass zu dieser Route nur SSL-Verbindungen hergestellt werden.

---

**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} wurde 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.

---

**MQCPI007** Die Route an Port {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 empfängsbereit 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 Verbindungs-Threads (MinConnectionThreads) wird erst nach dem erneuten Starten der Route wirksam.

**Erläuterung:** Die Mindestanzahl von Verbindungs-Threads 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** Verbindung zwischen {0} und Host {1} wurde geschlossen. Das Protokoll wurde nicht erkannt.

**Erläuterung:** Diese Nachricht wird in das Verbindungsprotokoll geschrieben, um einen Verbindungsvorgang aufzuzeichnen.

---

**MQCPI015** Die Verbindung zwischen einem Client auf {0} und Host {1} wurde zurückgewiesen, weil der Clientzugriff für diese Route inaktiviert ist.

**Erläuterung:** Diese Nachricht wird in das Verbindungsprotokoll geschrieben, um einen Verbindungsvorgang aufzuzeichnen.

---

**MQCPI016** Die Verbindung zwischen einem WS-Manager auf {0} und Host {1} wurde zurückgewiesen, weil der WS-Managerzugriff für diese Route inaktiviert ist.

**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.

---

**MQCPI024** ....verwendet 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.

---

**MQCPI031** .....Cipher Suites {0}

**Erläuterung:** Diese Nachricht gibt die Cipher Suites an, die für diese Route verwendet werden.

---

**MQCPI032** .....Schlüsselringdatei {0}

**Erläuterung:** Diese Nachricht gibt den Namen der Schlüsselringdatei für diese Route an.

---

**MQCPI033** .....Clientauthentifizierung 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.

---

**MQCPI035** ....verwendet {0}

**Erläuterung:** Diese Nachricht gibt das Protokoll an, das für diese Zieladresse verwendet wird. Hierbei kann es sich entweder um das MQSeries-Protokoll, um HTTP-Tunnelung oder um HTTP-Chunking handeln.

---

**MQCPI036** ....SSL-Clientseite mit folgenden Eigenschaften aktiviert:

**Erläuterung:** Diese Nachricht gibt an, dass die Route die Daten über SSL an den Zielhost sendet.

---

**MQCPI037** ....SSL-Serverseite mit folgenden Eigenschaften aktiviert:

**Erläuterung:** Diese Nachricht gibt an, dass die Route die Daten über SSL vom sendenden Host empfängt.

---

**MQCPI038** .....registrierte Namen {0}

**Erläuterung:** Diese Nachricht gibt die registrierten Namen an, die zur Steuerung der Zertifikatauthentifizierung verwendet werden.

---

**MQCPI039** ....über 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.

---

**MQCPI041** ....antwortet 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 von Verbindungs-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.

---

**MQCPI047** .....CA-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.

---

**MQCPI049** ....QoS-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.

---

**MQCPI052** ....Socks-Serverseite aktiviert

**Erläuterung:** Diese Route wird als SOCKS-Server (Proxy) fungieren und Verbindungen von einer SOCKSifizierten 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 des Sicherheitsmanagers) wurde geändert;

die Änderung wird jedoch erst bei einem Neustart des Java Security Manager wirksam.

**Benutzeraktion:** Setzen Sie die Eigenschaft **Sicherheitsmanager** auf **false**, geben Sie einen Aktualisierungsbefehl (REFRESH) ein, und stoppen Sie den Java Security Manager. Setzen Sie anschließend **Sicherheitsmanager** wieder auf **true**, geben Sie einen weiteren Aktualisierungsbefehl (REFRESH) ein, und starten Sie den Java Security Manager mit der neuen Richtliniendatei.

---

**MQCPI057** ....Tracestufe {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.

---

**MQCPI058** ....und URI-Name {0}

**Erläuterung:** Diese Nachricht wird beim Start einer Route an die Systemkonsole ausgegeben. Sie gibt den URI-Namen für diese Route an.

---

**MQCPI059** ....Servlet-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 System-service gestartet wird.

---

**MQCPI064** ....keine 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.

---

**MQCPI065** ....im 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.

---

**MQCPI100** Dieses Script startet {0}.

**Erläuterung:** Onlinehilfenachricht von Script **mqipt**.

---

**MQCPI101** Das Befehlsformat lautet:

**Erläuterung:** Onlinehilfenachricht von Script **mqipt**.

---

**MQCPI102** **mqipt** {Verzeichnisname}

**Erläuterung:** Onlinehilfenachricht von Script **mqipt**.

---

**MQCPI103** Verzeichnisname - Verzeichnis, in dem sich **mqipt.conf** befindet

**Erläuterung:** Onlinehilfenachricht von Script **mqipt**.

---

**MQCPI106** Dieses Script zeigt die aktuelle Versionsnummer von {0} an.

**Erläuterung:** Onlinehilfenachricht von Script **mqipt-Version**.

---

**MQCPI107** **mqiptVersion** {-v}

**Erläuterung:** Onlinehilfenachricht von Script **mqipt-Version**.

---

**MQCPI108** Bei Angabe von -v wird auch das Build-Datum angezeigt.

**Erläuterung:** Onlinehilfenachricht von Script **mqipt-Version**.

---

**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.

**Erläuterung:** Onlinehilfenachricht von Script **mqipt-Fork**.

---

**MQCPI110** Diese Klasse zeigt eine einfache Nachricht in der Landessprache an der Konsole an.

**Erläuterung:** Onlinehilfenachricht von der Klasse **IPTMessages**.

---

**MQCPI111** **java com.ibm.mq.ipt.IPTMessages** (Nachrichten\_ID1) {Nachrichten\_ID2} {Nachrichten\_ID...}

**Erläuterung:** Onlinehilfenachricht von der Klasse **IPTMessages**.

---

**MQCPI112** Dabei entspricht `Nachrichten_ID` einem Schlüssel in der Datei `mcipt.properties`.

**Erläuterung:** Onlinehilfenachricht von der Klasse `IPT-Messages`.

---

**MQCPI113** Dieses Script dient zur Verwaltung von MQIPT als Systemservice.

**Erläuterung:** Onlinehilfenachricht von Script `mcipt-Service`.

---

**MQCPI114** `mciptService (-install | -remove )`

**Erläuterung:** Onlinehilfenachricht von Script `mcipt-Service`.

---

**MQCPI115** `-install`: Installiert die Dateien zum automatischen Starten von MQIPT beim Systemstart

**Erläuterung:** Onlinehilfenachricht von Script `mcipt-Service`.

---

**MQCPI116** `-remove`: Entfernt die Dateien zum automatischen Starten von MQIPT beim Systemstart

**Erläuterung:** Onlinehilfenachricht von Script `mcipt-Service`.

---

# Index

## A

- AIX
  - MQIPT automatisch starten 41
  - MQIPT-Dateien herunterladen 39
  - MQIPT-Dateien installieren 39
  - MQIPT deinstallieren 41
  - MQIPT einrichten 40
  - MQIPT installieren 39
  - MQIPT über die Befehlszeile starten 40
  - Verwaltungsclient über die Befehlszeile starten 41
- Aktiv, Konfigurationseigenschaft 61
- Allgemeine Probleme 105
- Ausführungstracefunktion 107
- Automatisch starten, MQIPT
  - Fehler 107

## B

- Beendigung 26
- Befehls-Port, Konfigurationseigenschaft 60
- Beispielkonfigurationen 1, 72
  - HTTP-Proxy-Konfiguration 80
  - Installationsfunktionstest (IVT) 72
  - MQIPT-Servlet konfigurieren 96
  - Quality of Service (QoS) konfigurieren 85
  - Schlüsselringdatei erstellen 102
  - SOCKS-Client konfigurieren 90
  - SOCKS-Proxy konfigurieren 88
  - SSL-Clientauthentifizierung 77
  - SSL-Proxy konfigurieren 91
  - SSL-Serverauthentifizierung 74
  - SSL-Testzertifikate erstellen 95
  - Unterstützung für MQIPT-Clustering konfigurieren 98
  - Zugriffssteuerung konfigurieren 83

## C

- Chunking, HTTP 8
- Cipher Suites 10
- Client-/Serverkanäle 24
- Clientzugriff, Konfigurationseigenschaft 61
- Clustersender-/Clusterempfängerkanäle 24

## D

- Deinstallieren, MQIPT
  - unter AIX 41
  - unter HP-UX 46
  - unter Linux 50
  - unter Sun Solaris 37
  - unter Windows 34
- Demilitarized Zone, MQIPT mit 2

- Denial-of-Service-Attacken 28
- Dienststeuerungsprogramm, Windows 34
- Durchgehende Verbindungen
  - Fehler 107
- Durchsatzverbesserung 108

## E

- Eigenschaften
  - neue 29
  - Übersicht 58
- Einführung 1
- Einrichten, MQIPT
  - unter AIX 40
  - unter HP-UX 44
  - unter Linux 48
  - unter Sun Solaris 36
  - unter Windows 32
- Einsatzmöglichkeiten für MQIPT 1
- Erste Schritte mit MQIPT 71

## F

- Fehlerbedingungen 26
- Fehlerbestimmung 105
- Fehlerisolierung 105
- Fehlermeldung 108
- Fernes Beenden, Konfigurationseigenschaft 61
- FFST-Berichte 106

## H

- Handshake 11
- Herunterladen, MQIPT-Dateien
  - unter AIX 39
  - unter HP-UX 43
  - unter Linux 47
  - unter Sun Solaris 35
  - unter Windows 31
- HP-UX
  - MQIPT automatisch starten 45
  - MQIPT-Dateien herunterladen 43
  - MQIPT-Dateien installieren 43
  - MQIPT deinstallieren 46
  - MQIPT einrichten 44
  - MQIPT installieren 43
  - MQIPT über die Befehlszeile starten 44
  - Verwaltungsclient über die Befehlszeile starten 46
- HTTP, Konfigurationseigenschaft 62
- HTTP-Chunking, Konfigurationseigenschaft 62
- HTTP-Proxy, Konfigurationseigenschaft 62
- HTTP-Proxy-Port, Konfigurationseigenschaft 62
- HTTP-Tunnelung, MQIPT mit 3

- HTTP-Unterstützung 8

## I

- Installieren, MQIPT-Dateien
  - unter AIX 39
  - unter HP-UX 43
  - unter Linux 47
  - unter Sun Solaris 35
  - unter Windows 31

## J

- Java Security Manager 25

## K

- Kanalkonfigurationen 24
- Kanalkonzentrator, MQIPT als 1
- KeyMan 16
  - FAQ (Häufig gestellte Fragen) 19
  - unterstützte Standarddatenformate 18
  - unterstützte Token 17
- Konfiguration
  - Datei, Zugriffsschutz 28
  - Eigenschaften, Übersicht 58
  - Referenzinformationen 57
  - Referenzinformationen zu Eigenschaften 60
  - Standardkonfigurationsdatei 57
  - Verwaltungsclient verwenden 51
  - Zeilenmodusbefehle verwenden 56

## L

- Linux
  - MQIPT automatisch starten 49
  - MQIPT-Dateien herunterladen 47
  - MQIPT-Dateien installieren 47
  - MQIPT deinstallieren 50
  - MQIPT einrichten 48
  - MQIPT installieren 47
  - MQIPT über die Befehlszeile starten 48
  - Verwaltungsclient über die Befehlszeile starten 49
- Listener-Port, Konfigurationseigenschaft 63
- Literaturverzeichnis xiii
- LogDir (Protokollverzeichnis), Konfigurationseigenschaft 63

## M

- Maximale Anzahl von Verbindungsthreads, Konfigurationseigenschaft 63
- Maximale Protokolldateigröße, Konfigurationseigenschaft 61

Mindestanzahl von Verbindungs-Threads,  
Konfigurationseigenschaft 63  
MQIPT und SSL 12

## N

Nachrichten 109  
Name, Konfigurationseigenschaft 63  
Navigations- und Aufrufmöglichkeiten x  
Network Dispatcher 20  
Network Dispatcher Advisor, Eigenschaft 64  
Network Dispatcher-Ersetzungsmodus, Eigenschaft 64  
Normale Beendigung 26

## P

PKCS#10 18  
PKCS#11-Repositorys (CryptoKi) 17  
PKCS#12 18  
PKCS#12-Token 17  
PKCS#7 18  
PKCS#7-Token 17  
Protokollweiterleitung durch MQIPT 7

## Q

QoS (Dienstgüte) 15  
QoS an Anrufer, Konfigurationseigenschaft 64  
QoS an Zieladresse, Konfigurationseigenschaft 64  
Quality of Service (QoS), Konfigurationseigenschaft 64

## R

REFRESH, Zeilenmodusbefehl 56  
Requester-/Senderkanäle 24  
Requester-/Serverkanäle 24  
Richtlinie für Sicherheitsmanager, Konfigurationseigenschaft 61

## S

Sender-/Empfängerkanäle 24  
Server-/Empfängerkanäle 24  
Server-/Requester-Kanäle 24  
Servlet 16  
Servlet-Client, Konfigurationseigenschaft 65  
Sicherheitsmanager, Konfigurationseigenschaft 61  
Sicherung von Dateien 105  
SOCKS-Client, Konfigurationseigenschaft 65  
SOCKS-Proxy-Hostname, Konfigurationseigenschaft 65  
SOCKS-Proxy-Port, Konfigurationseigenschaft 65  
SOCKS-Server, Konfigurationseigenschaft 65  
SOCKS-Unterstützung 9

SPKAC 18  
SSL-Client - allgemeiner DN-Name, Konfigurationseigenschaft 66  
SSL-Client - DN-Adresse, Konfigurationseigenschaft 66  
SSL-Client - DN-Land, Konfigurationseigenschaft 66  
SSL-Client - DN-Organisation, Konfigurationseigenschaft 66  
SSL-Client - DN-Organisationseinheit, Konfigurationseigenschaft 67  
SSL-Client - DN-Staat, Konfigurationseigenschaft 67  
SSL-Client - Schlüsselringdatei, Konfigurationseigenschaft 67  
SSL-Client - Schlüsselringkennwortdatei, Konfigurationseigenschaft 67  
SSL-Client - Verbindungszeitlimit, Eigenschaft 66  
SSL-Client, Konfigurationseigenschaft 65  
SSL-Client Cipher Suites, Konfigurationseigenschaft 66  
SSL-Proxy-Modus, Konfigurationseigenschaft 67  
SSL-Server - allgemeiner DN-Name 68  
SSL-Server - Cipher Suites, Konfigurationseigenschaft 68  
SSL-Server - Clientauthentifizierung anfordern 68  
SSL-Server - DN-Adresse, Konfigurationseigenschaft 69  
SSL-Server - DN-Land, Konfigurationseigenschaft 68  
SSL-Server - DN-Organisation, Konfigurationseigenschaft 69  
SSL-Server - DN-Organisationseinheit, Konfigurationseigenschaft 69  
SSL-Server - DN-Staat, Konfigurationseigenschaft 69  
SSL-Server - Schlüsselringdatei, Konfigurationseigenschaft 69  
SSL-Server - Schlüsselringkennwortdatei, Konfigurationseigenschaft 70  
SSL-Server, Konfigurationseigenschaft 68  
SSL-Unterstützung 10  
  Beispiel 3  
  Fehlernachrichten 13  
  Handshake 11  
  MQIPT und SSL 12  
  testen 13  
  Vertrauenseinstellungen 12  
Starten, MQIPT automatisch  
  unter AIX 41  
  unter HP-UX 45  
  unter Linux 49  
  unter Sun Solaris 37  
Starten, MQIPT über die Befehlszeile  
  unter AIX 40  
  unter HP-UX 44  
  unter Linux 48  
  unter Sun Solaris 36  
  unter Windows 32  
STOP, Zeilenmodusbefehl 56  
Sun Solaris  
  MQIPT automatisch starten 37  
  MQIPT-Dateien herunterladen 35

Sun Solaris (*Forts.*)  
  MQIPT-Dateien installieren 35  
  MQIPT deinstallieren 37  
  MQIPT einrichten 36  
  MQIPT installieren 35  
  MQIPT über die Befehlszeile starten 36  
  Verwaltungsclient über die Befehlszeile starten 37  
SupportPac, Adresse der Webseite 31

## T

TCP/IP und MQIPT 7  
Topologie, MQIPs 4  
Trace, Konfigurationseigenschaft 70  
Tracefehler 107  
Tunnelung, HTTP 8

## U

Übersicht über MQIPT 7  
Überwachungssignal, Verfahren 9  
Upgrade von einer früheren MQIPT-Version 29  
URI-Name, Konfigurationseigenschaft 70

## V

Verbindungs-Threads  
  Durchsatzverbesserung 108  
Verbindungsprotokoll, Konfigurationseigenschaft 60  
Verbindungsprotokolle 27  
Vererbung von Eigenschaften 53  
Verschlüsselung 3  
Verschlüsselungsalgorithmen 10  
Vertrauenseinstellungen 12  
Verwalten, MQIPT 51  
Verwalten, MQIPT über Zeilenmodusbefehle 56  
Verwaltung 105  
Verwaltung von Thread-Pools 108  
Verwaltungsclient 51  
  einen MQIPT verwalten 52  
  Hilfeinformationen 56  
  Optionen im Menü 'Datei' 53  
  Optionen im Menü 'MQIPT' 54  
  starten 51  
  unter AIX starten 41  
  unter HP-UX starten 46  
  unter Linux starten 49  
  unter Sun Solaris starten 37  
  unter Windows starten 33  
  Verbindungsinformationen 51  
  Vererbung von Eigenschaften 53  
Voraussetzungen x, 71

## W

Windows  
  Dienststeuerungsprogramm 34  
  MQIPT als Dienst deinstallieren 34  
  MQIPT-Dateien herunterladen 31

## Windows (Forts.)

- MQIPT-Dateien installieren 31
- MQIPT deinstallieren 34
- MQIPT einrichten 32
- MQIPT installieren 31
- MQIPT über die Befehlszeile starten 32
- Verwaltungsclient über die Befehlszeile starten 33
- WS-Managerzugriff, Konfigurationseigenschaft 64

## X

- X.509V2-CRLs 19
- X.509V3-Zertifikate 18

## Z

- Zeilenmodusbefehle 56
- Zeitlimit für Inaktivität
  - Durchsatzverbesserung 108
- Zeitlimit für Inaktivität, Konfigurationseigenschaft 63
- Zertifikatspezifische Technologien 13
- Ziel-Port, Konfigurationseigenschaft 62
- Zieladresse, Konfigurationseigenschaft 62
- Zielwarteschlangenmanager, Zugriff auf 7
- Zugriffskennwort, Eigenschaft 60
- Zusammenfassung der Änderungen xv





---

# Antwort

MS81: WebSphere MQ  
Internet Pass-Thru  
Version 1.2

IBM Form SC12-3116-00

Anregungen zur Verbesserung und Ergänzung dieser Veröffentlichung nehmen wir gerne entgegen. Bitte informieren Sie uns über Fehler, ungenaue Darstellungen oder andere Mängel.

Zur Klärung technischer Fragen sowie zu Liefermöglichkeiten und Preisen wenden Sie sich bitte entweder an Ihre IBM Geschäftsstelle, Ihren IBM Geschäftspartner oder Ihren Händler.

**Unsere Telefonauskunft "HALLO IBM" (Telefonnr.: 01803/31 32 33) steht Ihnen ebenfalls zur Klärung allgemeiner Fragen zur Verfügung.**

Kommentare:

Danke für Ihre Bemühungen.

Sie können ihre Kommentare betr. dieser Veröffentlichung wie folgt senden:

- Als Brief an die Postanschrift auf der Rückseite dieses Formulars
- Als E-Mail an die folgende Adresse: [ibmterm@de.ibm.com](mailto:ibmterm@de.ibm.com)

---

Name

---

Adresse

---

Firma oder Organisation

---

Rufnummer

---

E-Mail-Adresse

IBM Deutschland GmbH  
SW TSC Germany

70548 Stuttgart