WebSphere MQ internet Passthru 버전 1.3

SA30-1615-01

주!

이 정보와 이 정보가 지원하는 제품을 사용하기 전에, 반드시 189 페이지의 『주의사항』에 나와 있는 일반 정보를 읽어 보시기 바랍니다.

제 4 판(2003년 3월)

이 개정판은 WebSphere MQ internet pass-thru 버전 1.3(프로그램 번호 5639-L92) 및 새 개정판에서 별도로 언급하지 않는 한 모든 후속 릴리스 및 수정에 적용됩니다.

목차

그림

서문

internet pass-thru의 개념

WebSphere MQ internet pass-thru는 이전에는 MQSeries internet pass-thru로 알려져 있었습니다. WebSphere MQ는 지금부터 이 서적에서 MQSeries에 대해 사용하는 이름입니다. 모든 MQSeries 매뉴얼에서 그 이름을 WebSphere MQ로 변경한 것은 아니며 어떤 경우에는 MQSeries 및 WebSphere MQ에 대한 참조가 둘 다 있는 경우도 있습니다.

IBM® WebSphere MQ internet pass-thru의 특징은 다음과 같습니다.

- 인터넷에 걸쳐 있는 리모트 사이트 간의 메시징 솔루션을 구현하는 데 사용되는 WebSphere MQ 기본 제품의 확장입니다.
- HTTP 내의 프로토콜을 터널링하거나 프록시 역할을 수행하여 보다 간단하고 효과적으로 방화벽 너머 WebSphere MQ 채널 프로토콜의 메시지를 작성할 수 있습니다.
- WebSphere MQ 메시지 플로우를 수신하고 전달할 수 있는 독립형 서비스 역할을 수행할 수 있습니다. 또한 실행되는 시스템이 WebSphere MQ 큐 관리자를 호스트할 필요가 없습니다.
- WebSphere MQ를 사용하여 비즈니스 대 비즈니스 트랜잭션을 제공하는 데 도움이 됩니다.
- 방화벽을 통해 기존의 변경되지 않은 WebSphere MQ 응용프로그램을 사용 가능하게 해줍니다.
- 다중 큐 관리자에 대한 액세스를 제어하는 단일 지점을 제공합니다.
- 모든 데이터를 암호화할 수 있도록 허용합니다.
- 모든 연결 시도를 로그합니다.

이 서적에서는 WebSphere MQ internet pass-thru를 편의상 “MQIPT”라고 언급하는 경우가 종종 있습니다.

이 책의 사용자

이 서적은 시스템 설계자, WebSphere MQ 기술 관리자, 방화벽 및 네트워크 관리자를 그 대상으로 합니다.

이 책의 이해를 위한 사전 지식

다음 사항을 이해하고 있어야 합니다.

- *WebSphere MQ 시스템 관리 안내서* 및 *WebSphere MQ 상호통신*에 설명된 것과 같이 WebSphere MQ 큐 관리자 및 메시지 채널의 관리
- 방화벽이 구현되는 방법
- 인터넷 프로토콜 라우팅/네트워킹
- IBM Network Dispatcher의 로드 밸런스 및 강화 기능
- IBM WebSphere® Application Server

필수조건

internet pass-thru의 이 릴리스는 다음 플랫폼에서 실행됩니다.

- Service pack 6이 설치된 Windows NT® V4.0
- Windows® 2000
- Windows XP
- Sun Solaris
- AIX® V5.1
- HP-UX 11
- Linux

J2SE V1.4.0 런타임(JRE)은 MQIPT 서버가 필요합니다. 보안 엑시트를 작성하려면 SDK,V1.4.0이 필요합니다.

지원되는 네트워크 프로토콜은 TCP/IP뿐입니다.

관리 클라이언트 도움말에는 Netscape 브라우저가 필요합니다.

액세스 가능 표시 정보

관리 클라이언트 GUI는 액세스를 염두에 두고 빌드됩니다. 마우스를 사용하지 않고 키보드 등을 사용하여 사용 가능한 모든 기능을 수행하는 것이 목표입니다. Tab, Shift 키와 Tab, Ctrl 키와 Tab 및 커서 키를 일반적인 방법으로 사용하여 화면 주위를 탐색할 수 있습니다. 단추를 선택하고 Enter 키를 누르면 단추를 누르는 것과 동일한 결과가 나옵니다.

탭과 커서 키를 결합하거나 모든 옵션에 대해 사용 가능한 단축키를 이용하여 메뉴 옵션을 선택할 수 있습니다. 예를 들어, 먼저 Alt 키와 F를 선택한 다음, Alt 키와 Q를 사용하면 GUI를 닫을 수 있습니다(파일->종료). 일단 메뉴 항목에 이르면 Enter 키를 사용하여 활성화할 수 있습니다.

커서 키를 사용하여 트리 주위를 탐색할 수 있습니다. 특히, 오른쪽 커서 키와 왼쪽 커서 키를 사용하여 MQIPT 노드를 열거나 닫음으로써 라우트를 표시하거나 숨길 수 있습니다.

선택된 확인란에서 Space 키를 사용하여 상태를 변경할 수 있습니다. Enter 키를 사용하여 편집할 필드를 선택할 수 있습니다.

룩앤필(look and feel)

GUI로 주위의 모양과 느낌을 채택하는 것이 이상적이나 항상 가능한 것은 아니므로 GUI의 모양과 느낌을 사용자의 필요에 맞게 사용자 정의 하도록 구성 파일을 제공할 수 있습니다. 이 구성 파일은 ″custom.properties″라고 하며 `bin` 서브디렉토리에 있어야 합니다.

이 구성 파일을 사용하여 구성할 수 있는 사항은 다음과 같습니다.

- 포그라운드 색상 - 텍스트의 색상
- 백그라운드 색상
- 텍스트의 글꼴
- 텍스트의 양식 - 일반, 굵게, 기울임꼴 또는 굵게 및 기울임꼴

샘플 구성 파일인 ″customSample.properties″가 제공되며 이 파일에는 변경 방법에 대한 설명이 포함되어 있습니다. 이 파일을 `bin/custom.properties`에 복사하여 필요한 사항을 변경하십시오.

변경사항 요약

이 절에서는 현재 버전의 WebSphere MQ internet pass-thru 변경사항에 대해 설명합니다. 이전 버전 이후에 변경된 사항은 변경사항 왼쪽에 수직선으로 표시됩니다.

이 개정판의 변경사항(SA30-1615-01)

WebSphere MQ internet pass-thru의 현재 버전에서 향상된 점은 다음과 같습니다.

- 클라이언트 연결 요청을 제어하는 보안 엑시트
- CRL 및 ARL에 대한 LDAP 지원
- 키 링 암호 암호화
- 키 링에서 인증 선택
- 새 AES 암호 모음
- 일반 UNIX® 디스크 이미지
- 라우트 재시작 조치 제어
- AIX 및 HP-UX 플랫폼에서 Java™ 1.4 지원

제 3 판의 변경사항(SA30-1615)

WebSphere MQ internet pass-thru의 이번 버전에서 향상된 점은 다음과 같습니다.

- 보내는 포트 주소 할당 제어
- 예제 구성
- 개선된 SSL 추적
- Java 보안 관리자
- SSL 인증서 및 키 링 파일 관리에 필요한 KeyMan 유틸리티
- WebSphere MQ 메시지용 QoS(Quality of Service)를 포함한 Linux 지원
- Windows 플랫폼에서 사용할 수 있는 NLS 설치 이미지
- 등록 정보 이름은 대소문자를 구분하지 않음
- Servlet 버전
- Socks 클라이언트 및 서버 지원
- SSL 프록시 모드
- 멀티홈 시스템 지원
- 관리 클라이언트용 통신이 줄어든 상태
- WebSphere MQ 클러스터 지원

제 2 판의 변경사항

WebSphere MQ internet pass-thru의 이번 버전에서 향상된 점은 다음과 같습니다.

- MQIPT용 플랫폼으로서 AIX, HP-UX 및 Windows 2000 추가
- HTTP 프록시 지원 추가
- SSL(Secure Socket Layer) 지원 추가
- SOCKS 프록시를 통해 다른 외부 MQIPT 또는 MQSeries® 서버와 통신하는 MQIPT 기능
- 하나 이상의 MQIPT를 쉽게 관리할 수 있도록 관리 클라이언트 GUI 사용
- IBM Network Dispatcher에 대한 지원 추가
- 약간의 추적 개선
- 약간의 mqiptAdmin 명령 개선

제 1 장 WebSphere MQ internet pass-thru에 대한 소개

WebSphere MQ internet pass-thru는 기본 WebSphere MQ 제품에 대한 확장입니다. MQIPT는 두 WebSphere MQ 큐 관리자 또는 WebSphere MQ 클라이언트 및 WebSphere MQ 큐 관리자 간에 WebSphere MQ 메시지 플로우를 수신하고 전달할 수 있는 독립형 서비스로서 실행됩니다. MQIPT는 클라이언트와 서버가 동일한 물리적 네트워크에 있지 않은 경우에 이 연결을 사용합니다.

하나 또는 그 이상의 MQIPT는 두 개의 WebSphere MQ 큐 관리자 또는 WebSphere MQ 클라이언트와 WebSphere MQ 큐 관리자 간의 통신 경로에 배치될 수 있습니다. MQIPT는 두 개의 WebSphere MQ 시스템 간에 직접적인 TCP/IP 연결을 사용하지 않고 메시지를 교환할 수 있도록 해줍니다. 이러한 기능은 방화벽 구성이 두 시스템 간의 직접적인 TCP/IP 연결을 금지하는 경우에 유용합니다.

MQIPT는 하나 이상의 TCP/IP 포트에서 정상적인 WebSphere MQ 메시지, HTTP 내에서 터널링된 WebSphere MQ 메시지 또는 SSL(Secure Sockets Layer)을 운반하여 수신되는 연결에 대해 대기하며 다중 동시 연결을 핸들링할 수 있습니다.

초기 TCP/IP 연결 요청을 작성한 WebSphere MQ 채널을 “호출자”라고 하며 연결을 시도하는 대상이 되는 채널을 “수신자”라 하고 궁극적으로 연결을 시도하는 큐 관리자를 “목적지 큐 관리자”라고 합니다.

MQIPT의 예상 용도는 사용과 같습니다.

- MQIPT는 채널 집중기로 사용될 수 있습니다. 따라서 마치 하나의 MQIPT 호스트에서, 또는 호스트로 표시되는 것과 같은 방화벽에 대해 여러 개의 분리된 호스트에서, 또는 호스트로 채널이 표시될 수 있습니다. 이로 인해 보다 쉽게 방화벽 필터링 규칙을 정의하고 관리할 수 있습니다.

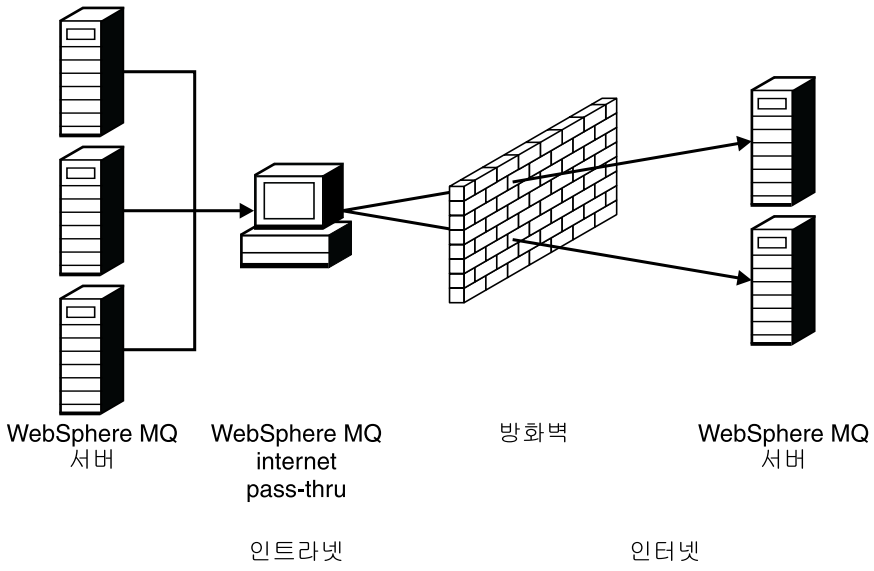

그림 1. MQIPT가 채널 집중기로 사용되는 예

- MQIPT가 방화벽의 "비무장 지대"(DMZ)에 있으면 트러스트되고 알려진 인터넷 IP(Internet Protocol)를 가진 시스템에서 MQIPT가 수신되는 WebSphere MQ 채널과의 연결에 대기하기 위해 사용될 수 있으며 이 연결은 트러스트된 인터넷으로 전달될 수 있습니다. 이 때, 내부 방화벽은 반드시 이러한 트러스트된 시스템이 내부 연결을 작성할 수 있도록 허용해야 합니다. 이 구성에서, MQIPT는 액세스에 대한 외부 요청이 트러스트된 인트라넷 내의 시스템의 진짜 IP 주소를 보는 것을 금지합니다. 따라서 MQIPT는 단일한 액세스 지점을 제공합니다.

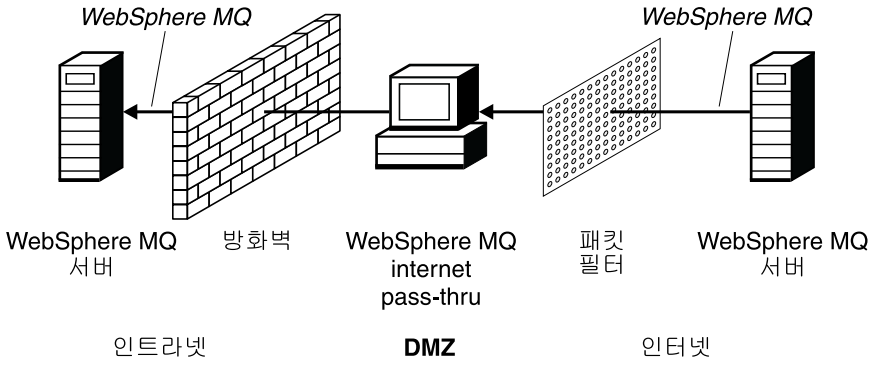

그림 2. "DMZ"가 있는 MQIPT 예

- 두 개의 MQIPT가 직렬도 전개된 경우에는 HTTP 또는 SSL을 사용하여 통신할 수 있습니다. HTTP 터널링 기능을 사용하면 기존 HTTP 프록시를 통해 방화벽을 통과하여 요청을 전송할 수 있습니다. 첫 번째 MQIPT가 WebSphere MQ 프로토콜을 HTTP에 삽입하고 두 번째 MQIPT가 HTTP 랩퍼로부터 WebSphere MQ 프로토콜을 추출하여 목적지 큐 관리자에 전달합니다.

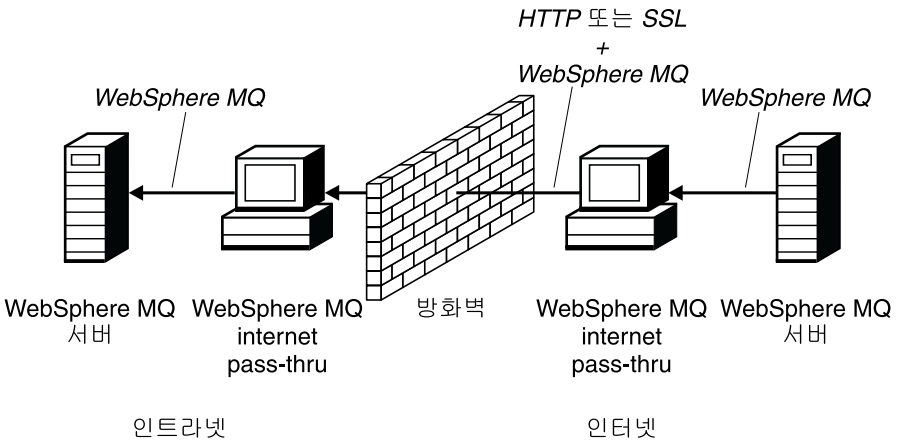

그림 3. MQIPT 및 HTTP 터널링의 예

- 이와 유사하게 방화벽을 통해 전송하기 전에 요청을 암호화할 수 있습니다. 첫 번째 MQIPT가 데이터를 암호화하고 두 번째 MQIPT가 목적지 큐 관리자로 전송하기 전에 SSL을 사용하여 암호를 해독합니다.

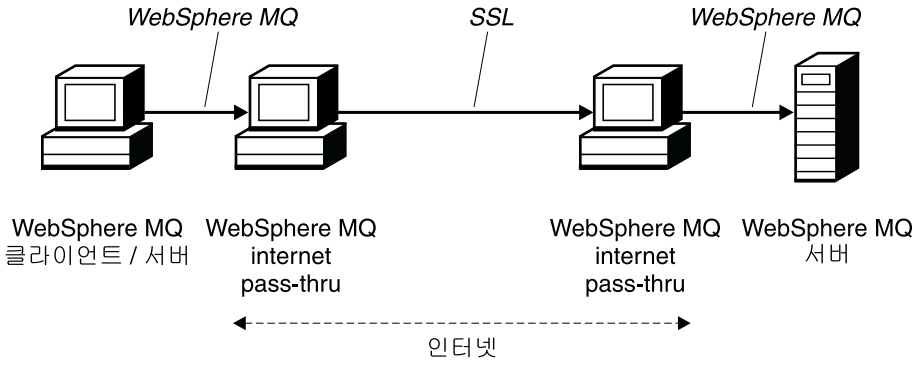

그림 4. MQIPT 및 SSL의 예

MQIPT는 데이터를 소스에서 목적지로 전달할 때 메모리에 데이터를 보유합니다. 디스크에는 데이터가 저장되지 않습니다. 운영 체제에 의해 디스크에 페이지된 메모리는 예외입니다. MQIPT가 명확히 디스크에 액세스하는 유일한 경우는 구성 파일을 읽고 로그 및 추적 레코드를 기록하는 경우입니다.

WebSphere MQ 채널 유형의 전체 범위는 하나 이상의 MQIPT를 통해 작성됩니다. 통신 경로에 있는 MQIPT의 존재는 연결된 WebSphere MQ 구성요소의 기능적인 특성에 아무런 영향을 미치지 못하나 메시지 전송의 성능에는 일정 정도 영향을 미칠 수 있습니다.

MQIPT는 WebSphere MQ Publish/Subscribe 또는 WebSphere MQ 통합자 메시지 브로커와 함께 사용할 수 있습니다.

5 페이지의 그림 5는 WebSphere MQ 토폴로지 내에서 모든 가능한 MQIPT 구성을 표시합니다. 그림에서 “외부 연결” 측의 방화벽 너머에 있는 HTTP 프록시, SOCKS 프록시 및 MQIPT 시스템은 인터넷에 함께 연결된 다중 시스템의 가능성을 나타냅니다. 예를 들어, MQIPT 시스템은 하나 이상의 SOCKS 또는 HTTP 프록시를 통하거나 추가적인 MQIPT 시스템을 통해 대상에 이르기 전에 통신할 수 있습니다.

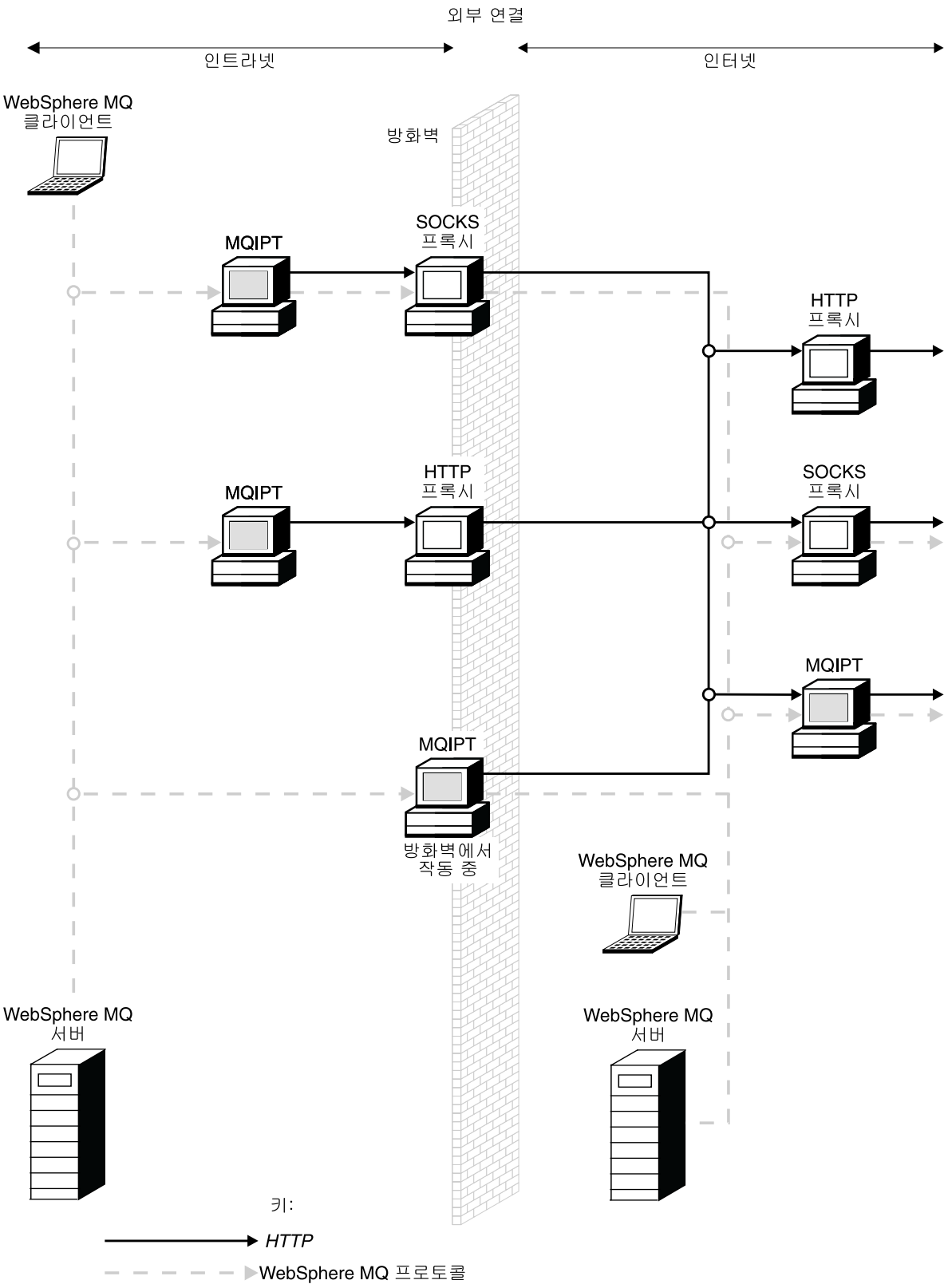

그림 5. WebSphere MQ 토폴로지는 가능한 MQIPT 구성을 표시합니다. (1/2)

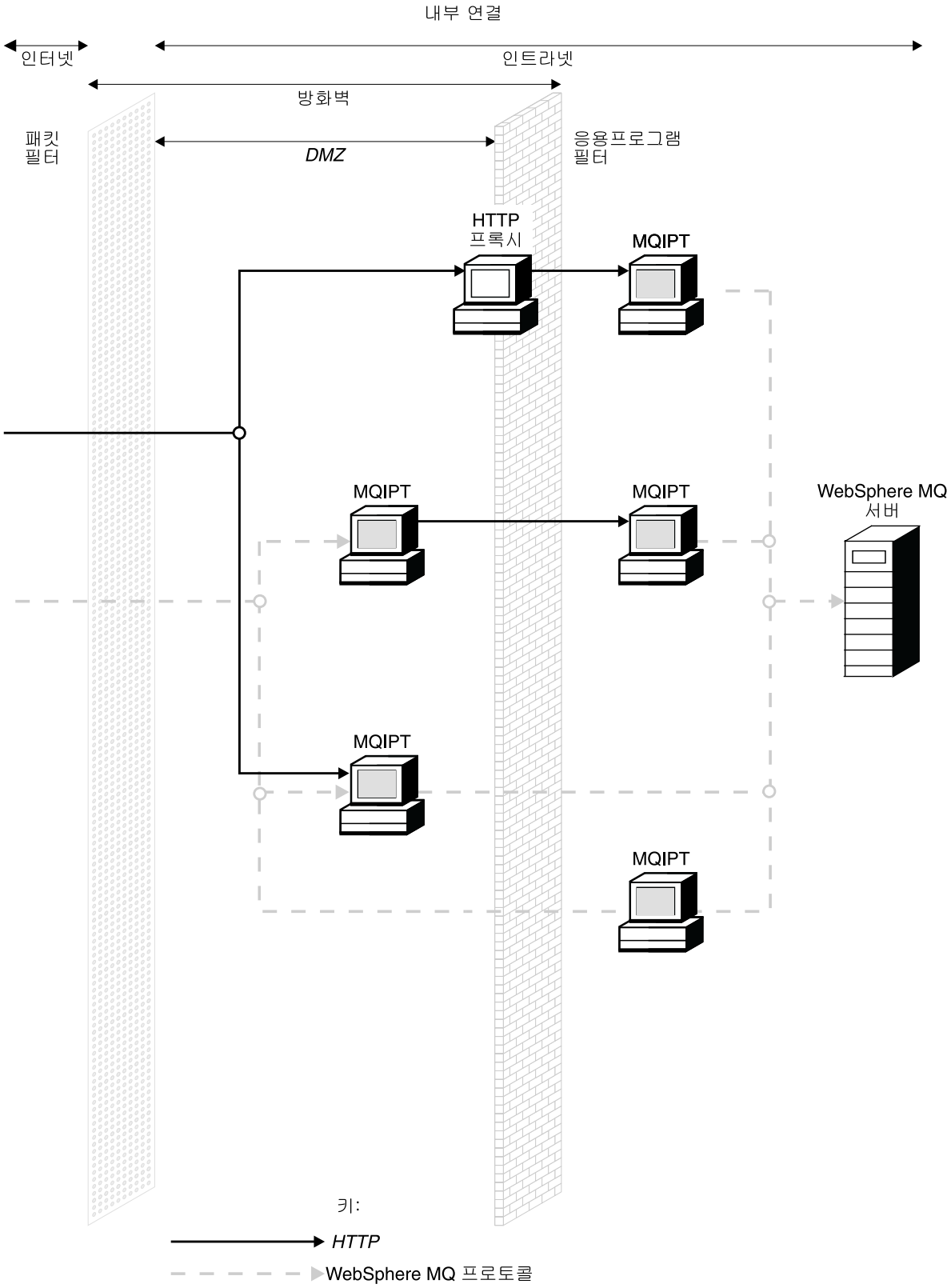

그림 5. WebSphere MQ 토폴로지는 가능한 MQIPT 구성을 표시합니다. (2/2)

제 2 장 internet pass-thru 작업 방법

이 절에서는 internet pass-thru가 작업하는 방법에 대한 개요를 제공합니다.

internet pass-thru 작업 방법 개요

MQIPT는 가장 간단한 구성일 때 WebSphere MQ 프로토콜 전달자의 역할을 합니다. MQIPT는 TCP/IP 포트에서 대기하며 WebSphere MQ 채널로부터 연결 요청을 승인합니다. 올바르게 생성된 요청이 수신되면 MQIPT가 MQIPT 자신과 목적지 WebSphere MQ 큐 관리자 간의 추가적인 TCP/IP 연결을 설정합니다. 그런 다음, 수신되는 연결에서 받은 모든 프로토콜 패킷을 목적지 큐 관리자에 전달하고 다시 목적지 큐 관리자로부터 원래의 수신되는 연결에 프로토콜 패킷을 반환합니다.

WebSphere MQ 프로토콜(클라이언트/서버 또는 큐 관리자에 대한 큐 관리자)에 대한 변경은 관련되지 않습니다. 어느 한 끝도 직접 중계의 존재를 인식하지 못하므로 WebSphere MQ 클라이언트 또는 서버 코드의 새 버전이 필요하지 않습니다.

MQIPT를 사용하려면 호출자 채널이 반드시 목적지 큐 관리자의 호스트 이름과 포트가 아니라 MQIPT의 호스트 이름과 포트를 사용하도록 구성되어야 합니다. 이 사항은 WebSphere MQ 채널의 CONNAME 등록 정보에 의해 정의됩니다. MQIPT는 수신되는 데이터를 읽고 목적지 큐 관리자로 전달합니다. 클라이언트/서버 채널의 사용자 ID와 암호 등의 다른 구성 필드도 이와 유사하게 목적지 큐 관리자로 전달됩니다.

MQIPT는 하나 이상의 목적지 큐 관리자에 액세스하도록 허용될 수 있습니다. 이런 작업을 수행하기 위해서는 반드시 MQIPT에 어떤 큐 관리자가 연결할 대상인지 알려주는 메커니즘이 있어야 하므로 MQIPT는 다음 단락에서 설명하는 것과 같이 수신되는 TCP/IP 포트 번호를 사용하여 어떤 큐 관리자가 연결할 대상인지 결정합니다.

하나 이상의 목적지 큐 관리자에 대한 액세스를 허용하면 MQIPT가 여러 TCP/IP 포트에서 대기하도록 구성될 수 있습니다. 각 대기 포트는 MQIPT "라우트"를 통해 목적지 큐 관리자에 맵핑됩니다. MQIPT 관리자는 이런 라우트를 100 개까지 정의할 수 있으며 이러한 라우트는 대기 중인 TCP/IP 포트와 목적지 큐 관리자의 호스트 이름 및 포트를 연관시킵니다. 즉, 목적지 큐 관리자의 호스트 이름(IP 주소)이 시작되는 채널에는 절대 보이지 않습니다. 각 라우트는 해당 대기 포트와 목적지 간의 각 연결을 핸들링할 수 있으며 각 연결은 독립적으로 수행됩니다.

MQIPT는 mqipt.conf라는 구성 파일을 사용하며 이 파일에는 모든 루트의 정의 및 연관된 등록 정보가 있습니다. 이 파일의 자세한 정보는 75 페이지의 제 19 장『internet pass-thru 관리 및 구성』을 참조하십시오.

MQIPT가 시작되면 구성 파일에서 각 라우트가 시작됩니다. 각 라우트의 상태를 표시한 메시지가 시스템 콘솔에 기록됩니다. 라우트에 메시지 MQCPI078이 나타나면 해당 라우트는 연결 요청을 승인할 준비가 된 것입니다.

지원되는 채널 구성

모든 WebSphere MQ 채널 유형이 지원되나 구성은 TCP/IP 연결로 제한됩니다. WebSphere MQ 클라이언트 또는 큐 관리자에 대해 MQIPT는 목적지 큐 관리자인 것처럼 표시됩니다. 채널 구성에 목적지 호스트 및 포트 번호가 필요한 경우에는 MQIPT 호스트 이름 및 리스너 포트 번호가 지정됩니다.

클라이언트/서버 채널

MQIPT는 수신되는 클라이언트 연결 요청이 있도록 대기하다가 HTTP 터널링, SSL 또는 표준 WebSphere MQ 프로토콜 패킷 중 하나를 사용하여 요청을 전달합니다. MQIPT가 HTTP 터널링 또는 SSL을 사용하는 경우에는 두 번째 MQIPT에 대한 연결에서 요청을 전달합니다. HTTP 터널링을 사용하지 않는 경우에는 다음 차례에 추가 MQIPT가 될 수 있더라도 연결 상에서 목적지 큐 관리자로 보이는 곳에 전달합니다. 일단 목적지 큐 관리자가 클라이언트 연결을 승인하면 패킷이 클라이언트와 서버 간에 교체됩니다.

클러스터 송신자/수신자 채널

MQIPT가 클러스터-송신자 채널로부터 수신되는 요청을 수신하면 큐 관리자가 socks 화되었으며 SOCKS 데이터 교환 프로세스 동안 진짜 목적지 주소가 확보되었다고 가정합니다. 또한 클라이언트 연결 채널의 경우와 정확히 일치하는 방법으로 다음 MQIPT 또는 목적지 큐 관리자에 요청을 전달합니다. 여기에는 자동 정의된 클러스터-송신자 채널이 포함됩니다.

송신자/수신자

MQIPT가 송신자 채널로부터 수신되는 요청을 수신하면 클라이언트 연결 채널의 경우와 정확히 일치하는 방법으로 다음 MQIPT 또는 목적지 큐 관리자에 요청을 전달합니다. 목적지 큐 관리자는 수신되는 요청을 유효화하고 적절한 경우에 한해 수신자 채널을 시작합니다. 보안 플로우를 포함하여 송신자와 수신자 채널 간의 모든 통신은 교체됩니다.

요청자/서버

이 결합은 앞에서 설명한 유형과 동일한 방법으로 핸들링됩니다. 연결 요청의 유효성 확인은 목적지 큐 관리자에서 서버 채널에 의해 수행됩니다.

요청자/송신자

두 개의 큐 관리자가 서로에 대해 직접 연결을 설정하지 못하지만 둘 다 MQIPT에 연결할 수 있으며 MQIPT로부터 연결을 승인할 수 있는 경우에 '콜백' 구성을 사용할 수 있습니다.

서버/요청자 및 서버/수신자

이 채널은 송신자/수신자 구성과 동일하게 MQIPT에 의해 핸들링됩니다.

제 3 장 HTTP 지원

MQIPT는 전달하는 데이터 패킷이 HTTP 요청으로 인코드되도록 구성할 수 있습니다. MQIPT는 청킹을 사용하거나 사용하지 않는 HTTP 터널링을 지원합니다.

현재 WebSphere MQ 채널이 HTTP 요청을 승인하지 않으므로 두 번째 MQIPT가 HTTP 요청을 수신하여 이를 다시 정상적인 WebSphere MQ 프로토콜 패킷으로 변환시켜야 합니다. 두 번째 MQIPT는 HTTP를 목적지 큐 관리자에 전달하기 전에 HTTP 헤더를 제거하여 수신되는 패킷을 다시 표준 WebSphere MQ 프로토콜 패킷으로 변환시킵니다.

청킹을 사용하지 않고 HTTP 터널링을 사용하는 경우에는 HTTP 응답이 다시 각 HTTP 요청에 대해 첫 번째 MQIPT로 송신됩니다. 이 응답은 목적지 큐 관리자 또는 더미 수신 확인으로부터의 응답이 될 수 있습니다. WebSphere MQ 시스템이 대규모 메시지를 전송할 때와 같이 연속적인 WebSphere MQ 프로토콜 패킷 체인을 송신해야하는 경우에는 데이터를 전송하기 위해 여러 개의 HTTP 요청/응답 쌍을 사용합니다. 이런 작업을 하기 위해 MQIPT가 추가적인 요청이나 응답 플로우를 삽입합니다.

청킹과 함께 HTTP 터널링을 사용하는 경우에는 첫 번째 패킷만이 HTTP 헤더에서 줄바꾸기됩니다. 중간 및 마지막 패킷은 청킹 헤더를 갖습니다. 이 배정은 두 번째 MQIPT으로부터 더미 수신 확인에 대한 대기를 제거하므로 청킹을 사용하지 않고 HTTP 터널링에 의해 제공되는 것보다 약간 더 나은 성능을 제공합니다.

HTTP가 두 MQIPT 사이에서 사용되는 경우에는 HTTP 요청 및 응답이 플로우되는 TCP/IP 연결이 지속적이며 메시지 채널의 존속기간 동안 열린 상태로 유지됩니다. MQIPT는 요청/응답 쌍 사이의 TCP/IP 연결을 닫지 않습니다.

두 MQIPT가 HTTP를 통해 통신하는 경우에는 HTTP 요청이 확장된 시간 동안 미해결 상태로 남아 있을 수 있습니다. 예에서는 새 메시지가 트랜스미션 큐에 도착하도록 대기하고 있을 때 요청/서버 채널에 서버 측이 있습니다. WebSphere MQ 채널 프로토콜은 대기 상태가 정기적으로 종료되어 파트너에게 휴면 메시지를 보내고(디폴트 채널 휴면 시간은 5분임) MQIPT가 이 휴면을 HTTP 응답으로 사용하는 “휴면” 메커니즘을 제공합니다. 일부 방화벽에서의 시간 종료 관련 문제점 발생을 방지하려면 이 채널 휴면를 사용 안함으로 설정하거나 과도하게 높은 값으로 설정하지 마십시오.

일부 HTTP 프록시는 지속적 연결을 제어하기 위해 자체 등록 정보를 가집니다. 예를 들어, 지속적 연결에서 작성될 수 있는 요청의 수 등입니다. 또한 HTTP 프록시는 반드시 HTTP 1.1 프로토콜을 지원해야 합니다. IBM WebSphere 캐싱 프록시를 사용하는 경우, 다음 등록 정보가 재설정되어야 합니다.

- MaxPersistenceRequest를 높은 값(예를 들어, 5000)으로 설정하십시오.

- PersistentTimeout를 높은 값(예를 들어, 12 시간)으로 설정하십시오.
- ProxyPersistence를 on으로 설정하십시오.

HTTP 사용 예를 보려면 112 페이지의 『HTTP 프록시 구성』을 참조하십시오.

HTTPS

HTTPS는 클라이언트 연결을 제공하는 MQIPT에서 HTTPS 및 SSLClient 라우트 등록 정보를 활성화하여 HTTP 연결에서 사용할 수 있습니다. MQIPT는 대상 HTTP 프록시/서버를 인증하는 데 사용할 트러스트된 CA 인증에 액세스해야 합니다. SSLClientCAKeyring 등록 정보는 트러스트된 CA 인증이 포함된 키 링 파일을 정의하는 데 사용할 수 있습니다.

HTTPS에 대한 공용 설정은 로컬 HTTP 프록시를 사용하여 방화벽으로 터널링되고 리모트 HTTP 서버(또는 다른 프록시)에 연결되어 리모트 MQIPT로 연결됩니다. 연결 요청이 정상 HTTP 연결로 처리되므로 서버측 연결에 있는 이 MQIPT에는 특정 구성이 필요하지 않습니다.

MQIPT는 HTTPProxy 및 HTTPServer 등록 정보를 사용하여 로컬 프록시와 리모트 프록시를 구별합니다. HTTPProxy는 로컬 HTTP 프록시로 간주되고 HTTPServer는 리모트 서버(또는 프록시)로 간주됩니다.

일반적으로 HTTPS 연결은 HTTP 프록시/서버의 리스너 포트 주소 443에서 이루어지지만 HTTPProxyPort와 HTTPServerPort를 사용하여 이 디폴트를 대체할 수 있습니다. HTTPS 사용 예를 보려면 129 페이지의 『HTTPS 구성』을 참조하십시오.

Servlet

비분배 응용프로그램의 응용프로그램 서버에서 전개할 수 있는 MQIPT의 servlet 버전(MQIPTServlet)이 있습니다. 작동 방법은 정상적인 MQIPT와 유사하나 라우트가 하나뿐인 것처럼 수행합니다. WebSphere MQ 채널을 시작하기 위해 수신되는 연결 요청은 MQIPTServlet의 인스턴스에 의해 핸들링되며 각 인스턴스는 대상 큐 관리자에 대해 지속적인 연결을 유지보수합니다. 후속 데이터 플로우는 첫 번째 연결 요청 동안 작성된 세션 ID를 사용하여 동일한 채널에서 유지보수됩니다.

MQIPTServlet.war라는 웹 응용프로그램 보존 파일은 웹 서브디렉토리에 있습니다. 이 war은 반드시 사용자의 응용프로그램으로 들여와야/전개해야 합니다. 이 servlet을 들여올 때 컨텍스트 이름를 지정해야 할 경우 디폴트 UriName 등록 정보를 대체하여 새 컨텍스트 이름을 포함시켜야 합니다. 자세한 정보는 102 페이지의 『UriName』을 참조하십시오

MQIPTServlet의 구성은 web.xml 파일의 등록 정보를 설정하여 수행되며 이 파일은 응용프로그램 서버의 WEB-INF 서브디렉토리에 있습니다. 기존 MQIPT 등록 정보의 서브세트만이 MQIPTServlet에 적용됩니다. 다음은 MQIPTServlet에서 사용할 수 있는 등록 정보입니다.

- ClientAccess
- ConnectionLog
- MaxLogFileSize
- QMgrAccess
- Trace

연결 로그와 추적 파일은 LogDir이라는 새 등록 정보에 의해 정의된 디렉토리에 기록됩니다. 이 등록 정보는 MQIPTServlet을 시작하기 전에 정의하는 것이 좋습니다.

MQIPTServlet에 사용될 자원의 양을 제어하려면 일부 응용프로그램 서버 등록 정보를 변경해야 합니다. 각 응용프로그램 서버에는 구성 데이터를 관리하는 고유한 방법이 있으며, 이 방법은 주로 웹 인터페이스인 GUI를 사용하거나 구성 파일을 편집하여 수행됩니다. 변경을 고려하는 등록 정보는 활성 세션의 최대 수 또는 응용프로그램 서버 내의 servlet 인스턴스 수를 설정할 수 있습니다. 이 수는 클라이언트 연결 수를 제어하며 MQIPT에 사용되는 MaxConnectionThreads 등록 정보와 유사합니다.

변경해야 하는 다른 등록 정보는 시간 종료 값, 지속적 연결의 지원 여부 및 지속적 연결에 허용되는 요청 수와 관련됩니다. MQIPTServlet이 대상 큐 관리자로의 지속적 연결을 사용하므로 이 등록 정보를 사용할 수 있어야 합니다. 다른 등록 정보는 늘어나야 하지만 디폴트 값과 사용될 WebSphere MQ 연결 유형에 따라 달라집니다. WebSphere MQ 클라이언트 연결이 대체로 일시적이기 때문에 디폴트 값을 사용하는 것이 안전합니다. 큐 관리자와 큐 관리자의 연결은 정해지지 않은 기간 동안 실행될 수 있으며 이런 경우에는 지속적 연결에 허용된 시간 종료 값과 요청 수가 적절히 늘어나는 것이 좋습니다.

또한 web.xml 파일에는 디폴트 값이 30분으로 정의된 세션-시간 종료 등록 정보가 있습니다. 이 등록 정보는 클라이언트의 비활성화를 제어하는 데 사용할 수 있으며 지정된 시간 동안 활동이 감지되지 않으면 세션을 닫습니다.

클라이언트와 MQIPTServlet 사이의 링크에는 최소한 하나의 MQIPT가 있어야 합니다. ServletClient 등록 정보는 MQIPTServlet에 연결된 MQIPT에서 사용할 수 있어야 하며 HTTPServer 등록 정보는 응용프로그램 서버 또는 응용프로그램 서버를 공급하는 HTTP 서버를 직접 가리킬 수 있습니다.

MQIPTServlet이 제대로 시작되었는지 테스트하기 위해 웹 브라우저를 시작하고 다음과 유사한 URL 이름을 입력할 수 있습니다.

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

긍정 응답이 브라우저에 표시됩니다.

MQIPTServlet은 IBM WebSphere Application Server 5.0(IBM HTTP Server와 함께거나 아님), Tomcat 3.3 및 Tomcat 4.0과 함께 테스트되었습니다. MQIPTServlet은 Java 1.4를 필요로 하지 않으며 응용프로그램 서버가 구현한 Java의 레벨을 사용합니다.

servlet 사용 예를 보려면 126 페이지의 『MQIPT Servlet 구성』을 참조하십시오.

제 4 장 Socks 지원

Socks 프록시는 방화벽을 통해 엑시트의 제어점으로 사용되는 네트워크 서비스입니다. 방화벽 내부에서 실행되는 Socks 사용 가능 응용프로그램은 Socks 프록시를 사용하여 리모트 응용프로그램에 연결할 수 있습니다.

MQIPT가 SocksServer 등록 정보를 사용하여 Socks 프록시 역할을 할 수 있으므로 Socks 사용 가능 WMQ 응용프로그램은 MQIPT를 통해 리모트 WMQ 큐 관리자에 연결할 수 있습니다. 이 기능을 사용하면 Socks 데이터 교환 프로세스 중에 대상 목적지와 목적지 포트 주소가 확보되며, 이로 인해 Destination 및 DestinationPort 라우트 등록 정보가 대체됩니다. 이 점이 WMQ 클러스터링 지원의 핵심 기능입니다. 자세한 정보는 아래를 참조하십시오.

또한 MQIPT는 Socks를 사용할 수 없는 로컬 WMQ 응용프로그램 대신 Socks 클라이언트 역할을 할 수도 있습니다. 이는 Socks 프록시를 통한 아웃바운드 연결만 허용하는 방화벽을 사용할 때 유용합니다. 각 MQIPT 라우트를 다른 Socks 프록시와 통신하도록 구성할 수 있습니다.

SOCKS 사용 방법의 예를 보려면 121 페이지의 『SOCKS 프록시 구성』을 참조하십시오.

클러스터링

WebSphere MQ 클러스터는 그 범위가 인터넷까지 해당되는 클러스터에서 각 큐 관리자를 socks화하고 MQIPT가 SOCKS 프록시를 사용할 수 있도록 함으로써 MQIPT와 함께 사용될 수 있습니다. 큐 관리자를 클러스터에 구성할 수 있는 방법은 매우 다양하며 다음 설명은 그 중에서 *WebSphere MQ Queue Manager Clusters*, SC34-6061의 1 부 3 장에서 설명한 작업을 기본으로 하는 것입니다. 다음 확장은 작업, ″클러스터에 새 큐 관리자 추가″에서 정의된 다이어그램으로부터 확장된 것입니다. NEWYORK 및 CHICAGO는 HOME이라는 클러스터에 있으며 둘 다 전체 저장소를 보유하고 있습니다. NEWYORK, LONDON 및 PARIS는 INVENTORY라는 또 다른 클러스터에 있습니다. CHICAGO는 MQIPT가 필요 없는 클러스터에 있으므로 socks화될 필요가 없습니다.

INVENTORY 클러스터의 각 큐 관리자는 MQIPT 뒤에 효과적으로 ″숨겨집니다″. 큐 관리자가 socks화되었으므로 클러스터 송신자 채널이 시작될 때, SOCKS 프록시 역할을 하는 MQIPT를 사용하여 요청이 해당 목적지로 송신됩니다. 일반적으로 클러스터 수신자 채널의 CONNAME은 로컬 큐 관리자를 식별하기 위해 사용되나 MQIPT와 함께 사용되는 경우에는 CONNAME이 반드시 로컬 MQIPT 및 수신되는 리스너 포트

를 식별해야 합니다. 아래의 다이어그램에서 수신되는 모든 리스너 포트 주소는 1414이며 보내는 리스너 포트 주소는 1415입니다.

socks화된 큐 관리자를 실행하는 방법은 두 가지입니다. 첫 번째 방법은 큐 관리자가 실행되고 있는 전체 시스템을 socks화하는 것입니다. 두 번째 방법은 큐 관리자만을 socks화하는 것입니다. 어떤 방법을 사용하더라도 MQIPT를 SOCKS 프록시로 사용하여 리모트 연결만을 작성하고 사용자 인증을 사용하지 않도록 SOCKS 클라이언트를 구성해야 합니다. 시중에는 SOCKS 지원을 받을 수 있는 수많은 제품이 있습니다. 그 중에서 반드시 SOCKS V5 프로토콜을 지원하는 제품을 선택해야 합니다.

클러스터 네트워크 구성 방법 예를 보려면 132 페이지의 『MQIPT 클러스터링 지원 구성』을 참조하십시오.

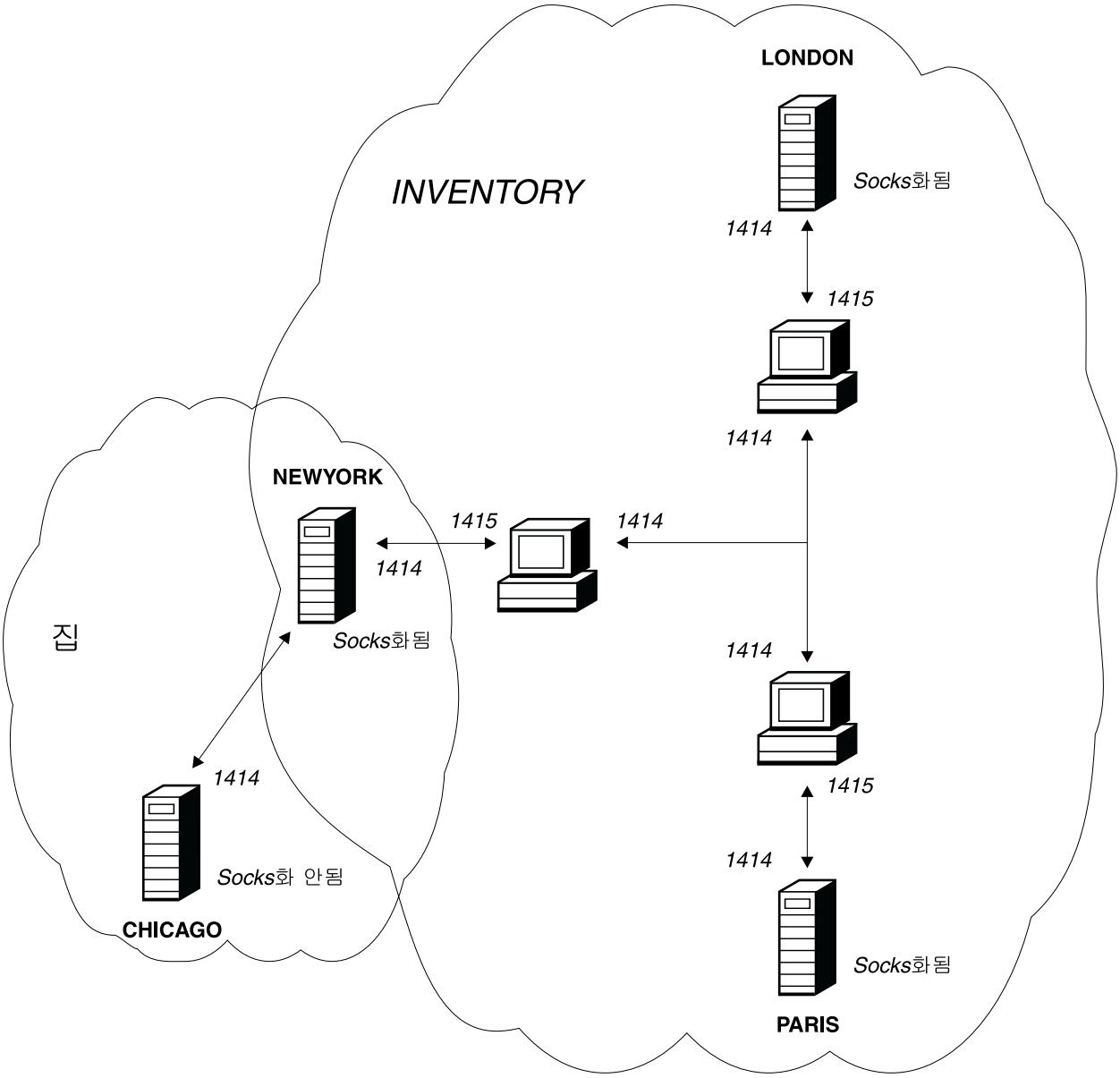

그림 6. MQIPT 클러스터링 지원

제 5 장 SSL 개요 및 지원

SSL 프로토콜은 보안되지 않는 통신 채널을 통해 연결 보안을 제공하며 다음을 보장합니다.

통신 프라이버시
클라이언트와 서버 간에 교환되는 데이터를 당사자만 의미를 알 수 있도록 암호화함으로써 연결을 개인용으로 만들 수 있습니다. 이렇게 함으로써 신용 카드 번호 등의 개인용 정보를 안전하게 전송할 수 있습니다.

통신 무결성
연결을 신뢰할 수 있습니다. 메시지 전송에는 보안 해시 기능에 기반을 둔 메시지 무결성 점검이 포함됩니다.

인증 클라이언트는 서버를 인증할 수 있으며 인증된 서버는 클라이언트를 인증할 수 있습니다. 즉, 의도된 당사자 간에만 정보가 교환되도록 보증할 수 있습니다. 인증 메커니즘의 기반은 디지털 인증서(X.509v3 인증서)의 교환입니다.

SSL 프로토콜은 통신 당사자의 인증에 대해 다른 디지털 서명 알고리즘을 사용할 수 있습니다. SSL에서 사용되는 암호화 조작, 데이터 기밀성에 필요한 암호화 및 메시지 무결성에 필요한 보안 해시는 클라이언트와 서버 간의 비밀 키 공유에 의존합니다. SSL은 비밀 키를 공유할 수 있는 다양한 키 교환 메커니즘을 제공합니다. SSL은 암호화와 해시에 필요한 다양한 알고리즘을 활용할 수 있습니다. 다양한 암호화 알고리즘이 지원되며 이는 SSL 암호 모음을 사용하여 지정할 수 있습니다. 지원되는 암호 모음은 다음과 같습니다.

- SSL_DH_anon_EXPORT_WITH_DES40_CBC_SHA
- SSL_DH_anon_WITH_3DES_EDE_CBC_SHA
- SSL_DH_anon_WITH_AES_128_CBC_SHA
- SSL_DH_anon_WITH_AES_256_CBC_SHA
- SSL_DH_anon_WITH_DES_CBC_SHA
- SSL_DH_anon_WITH_RC4_40_MD5
- SSL_DH_anon_WITH_RC4_128_MD5
- SSL_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA
- SSL_DHE_DSS_WITH_3DES__EDE_CBC_SHA
- SSL_DHE_DSS_WITH_AES_128_CBC_SHA
- SSL_DHE_DSS_WITH_AES_256_CBC_SHA
- SSL_DHE_DSS_WITH_DES_CBC_SHA
- SSL_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
- SSL_DHE_RSA_WITH_3DES__EDE_CBC_SHA
- SSL_DHE_RSA_WITH_AES_128_CBC_SHA

SSL_DHE_RSA_WITH_AES_256_CBC_SHA
SSL_DHE_RSA_WITH_DES_CBC_SHA
SSL_RSA_EXPORT_WITH_DES40_CBC_SHA
SSL_RSA_EXPORT_WITH_RC2_CBC_40_MD5#
SSL_RSA_EXPORT_WITH_RC4_40_MD5
SSL_RSA_WITH_3DES_EDE_CBC_SHA
SSL_RSA_WITH_AES_128_CBC_SHA
SSL_RSA_WITH_AES_256_CBC_SHA
SSL_RSA_WITH_DES_CBC_SHA
SSL_RSA_WITH_NULL_MD5
SSL_RSA_WITH_NULL_SHA
SSL_RSA_WITH_RC4_128_MD5
SSL_RSA_WITH_RC4_128_SHA

SSL 데이터 교환

SSL 데이터 교환 프로세스는 SSL 클라이언트와 서버 간의 초기 연결 요청 동안 암호 모음의 인증 및 교섭이 수행될 때 발생합니다.

익명 암호 모음이라는 예외가 있는 앞에서 나열된 모든 SSL 암호 모음은 서버 인증을 필요로 하며 이에는 클라이언트 인증을 허용합니다. 서버는 클라이언트 인증을 요청하도록 구성될 수 있습니다. SSL 형식의 통신 피어 인증은 공용 키 암호 및 X.509v3 디지털 인증서에 기반을 두고 있습니다. SSL 프로토콜로 인증되어야 하는 사이트는 개인용 키와 사이트의 ID, 인증 유효 기간에 관한 정보와 해당되는 공용 키를 함께 포함한 디지털 인증서가 필요합니다. 인증서는 인증 기관에 의해 서명되며 해당 기관의 인증서를 서명자 인증서라고 합니다. 인증서와 그 뒤에 오는 하나 이상의 서명자 인증서가 인증 체인을 구성합니다. 인증 체인은 첫 번째 인증서(사이트 인증서)에서 시작하며 체인 내의 각 인증서의 서명이 다음 서명자 인증서에 포함된 공용 키로 확인될 수 있다는 점이 특징입니다.

서버 인증이 필요한 보안 연결이 설정될 때 서버는 인증서 ID를 증명하기 위해 클라이언트에 인증서 체인을 송신합니다. SSL 클라이언트는 서버를 인증할 수 있는 경우에만 서버에 연결 설정을 수행합니다. 예를 들어, 서버의 사이트 인증서 서명을 확인합니다. 해당 서명을 확인하기 위해 SSL 클라이언트가 서버 사이트 자체 또는 서버에 의해 제공되는 인증서 체인에 있는 서명자 중 적어도 하나를 트러스트해야 합니다. 트러스트된 사이트 및 서명자의 인증서는 이 확인을 수행하기 위해 반드시 클라이언트 측에서 유지보수되어야 합니다.

SSL 클라이언트는 사이트 인증서부터 시작하여 서버의 인증서 체인을 검사하고 사이트 인증서가 트러스트된 사이트의 저장소 또는 사이트 인증서에 있는 경우 또는 체인 내에 있는 서명자 인증서가 트러스트된 서명자 인증서의 저장소에 기반하여 유효화될 수

있는 경우, 사이트 인증서의 서명이 유효화될 수 있는지 고려합니다. 후자의 경우, SSL 클라이언트는 인증서 체인이 트러스트된 서명자 인증으로부터 서버의 사이트 인증서에 실제로 올바르게 서명되었는지 점검합니다. 이 프로세스와 관련된 각 인증서 또한 형식과 유효 날짜가 올바른 지 검사됩니다. 이러한 점검 사항 중 올바르지 않은 항목이 하나라도 있으면 서버에 대한 연결이 거부됩니다. 서버 인증서를 확인한 후에, 클라이언트는 SSL 프로토콜의 다음 단계로 해당 인증서에 임베드된 공용 키를 사용합니다. SSL 연결은 서버가 실제로 해당되는 개인용 키를 가진 경우에만 설정될 수 있습니다.

클라이언트 인증에는 선행하는 몇 가지 프로시저가 있습니다. SSL 서버에 클라이언트 인증이 필요한 경우에는 클라이언트가 서버에 인증 체인을 송신하여 ID를 제공하고 서버가 트러스트된 사이트 및 서명자 인증서의 저장소를 기반으로 해당 체인을 확인합니다. 서버는 클라이언트 인증서를 확인한 후에, SSL 프로토콜의 다음 단계로 해당 인증서에 임베드된 공용 키를 사용합니다. SSL 연결은 클라이언트가 실제로 해당되는 개인용 키를 가진 경우에만 설정될 수 있습니다.

SSL 프로토콜 자체가 매우 높은 수준의 통신 보안을 제공합니다. 그러나 프로토콜은 응용프로그램에 의해 제공되는 정보를 기반으로 하여 조작됩니다. 해당 정보 기본이 안전하게 유지보수되는 경우에만 보안 통신의 전체 목표가 달성될 수 있습니다. 예를 들어, 트러스트된 사이트의 저장소 및 서명자 인증서가 훼손되면 매우 안전하지 못한 통신 파트너에게 보안 연결을 설정하게 될 수 있습니다.

WebSphere MQ internet pass-thru 및 SSL

SSL V3.0은 파일 유형이 .p12 또는 .pfx이며 X509.V3 인증을 포함한 키 링 파일에 저장된 PKCS(Public Key Cryptography Standards) #12 토큰을 사용하여 구현되어 왔습니다. 키 링 파일에 CRL(Certificate Revocation List)과 ARL(Authority Revocation List)이 포함될 수도 있습니다. WebSphere MQ internet pass-thru는 IBM SSLite(Secure Socket Lite) 패키지를 사용합니다.

WebSphere MQ internet pass-thru는 어떤 종료가 연결을 시작했는지에 따라 SSL 클라이언트 또는 SSL 서버의 역할을 수행할 수 있습니다. 클라이언트는 연결을 시작하고 서버는 연결 요청을 승인합니다. WebSphere MQ internet pass-thru 라우트도 클라이언트와 서버 역할을 모두 할 수 있으나 이런 경우에는 성능상의 이유로 SSL 프록시 모드 기능을 사용할 것을 권장합니다. 각 WebSphere MQ internet pass-thru 라우트는 자체 SSL 등록 정보 세트를 사용하여 독립적으로 구성될 수 있습니다. 자세한 내용은 86 페이지의 『라우트 섹션 참조 정보』를 참조하십시오.

트러스트 설정

키 링 파일은 서명자 인증서 또는 서명자 인증서 체인을 포함하여 개인 인증서를 포함합니다. 연결이 설정될 때 인증을 사용하려면 인증서에 트러스트 설정이 필요합니다. 다음과 같은 두 가지 레벨의 트러스트가 있습니다.

피어로서의 트러스트

이 인증서에 의해 서명된 임의의 인증서가 아니라 이 인증서만이 트러스트될 수 있음을 의미합니다.

인증 기관(CA)으로서의 트러스트

이 인증서에 의해 서명된 모든 인증서가 트러스트될 수 있음을 의미합니다.

SSLServerKeyRing 등록 정보에 의해 식별된 SSL 서버 측의 키 링 파일은 개인 인증서를 포함하고 있어야 합니다.

SSLClientCAKeyRing 등록 정보로 식별되는 SSL 클라이언트측 키 링 파일은 서버에서 송신한 인증을 인증하는 데 사용할 트러스트된 CA 인증 목록을 포함해야 합니다.

클라이언트 인증도 필요할 경우 SSLServerAskClientAuth 등록 정보를 서버측에서 사용해야 하며 SSLClientKeyRing 등록 정보로 식별되는 클라이언트측 키 링 파일은 개인 인증을 포함해야 합니다. SSLServerCAKeyRing 등록 정보로 식별되는 서버측 키 링 파일은 클라이언트를 인증하는 데 사용할 트러스트된 CA 인증의 목록을 포함해야 합니다.

트러스트된 CA에서 서명한 인증을 사용하는 대체 방법으로 자체 서명된 인증을 사용할 수 있습니다. 이에 대한 예는 ssl 서브디렉토리의 MQIPT에 제공된 샘플 키 링 파일(sslSample.pfx 및 sslCAdefault.pfx)에 있습니다.

이러한 키 링 파일에 저장된 PKCS#12 토큰 중 하나를 열려면 `mqiptV1.3` 암호를 사용해야 합니다.

SSL 인증과 키 링 파일을 관리할 수 있는 KeyMan라는 유틸리티는 ssl 서브디렉토리에 있습니다. 설치 지시 및 자세한 정보는 25 페이지의 『KeyMan』을 참조하십시오.

권한이 없는 액세스를 방지하기 위해 반드시 운영 체제의 보안 기능을 사용하는 모든 키 링과 암호 파일을 보호해야 합니다.

SSL 테스트

103 페이지의 제 20 장 『internet pass-thru 시작하기』는 SSL 연결을 테스트하기 위해 사용할 수 있는 작업을 설명합니다.

인증서 및 인증서 관리 기술은 다음을 포함하여 수많은 벤더로부터 사용 가능합니다.

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

SSL 오류 메시지

다음 오류 코드는 SSL 메소드 호출에서 올바르지 않은 매개변수 값이 사용되었거나 SSL 프로토콜에 올바르지 않은 데이터가 제공된 경우에 SSLRuntimeException에서 보여집니다.

표 1. SSLRuntimeException 오류 메시지

ID	설명
1	메소드 사용법이 올바르지 않거나 하나 이상의 입력 매개변수가 범위 밖입니다.
2	제공된 데이터를 프로세스할 수 없습니다.
3	제공된 데이터의 서명을 확인할 수 없습니다.
10	서명자 인증서의 주제 이름이 인증서의 발행자 이름과 일치하지 않습니다.
11	지원되지 않는 인증서 유형입니다.
12	인증서가 검증 기간 전에 사용되었습니다.
13	인증서 기간이 만기되었습니다.
14	인증서 서명을 확인할 수 없습니다.
15	인증서를 사용할 수 없습니다.
20	클라이언트에 의해 제안된 모든 암호 모음이 서버에 의해 지원되지 않습니다.
21	클라이언트에 의해 제안된 모든 압축 메소드가 서버에 의해 지원되지 않습니다.
22	사용 가능한 인증서가 없습니다.
23	지원되지 않는 알고리즘 또는 형식 유형입니다.
24	폐기된 정보 거부입니다.
25	인증서가 취소되었습니다.
26	CRL 세트가 완전하지 않습니다. 일부 델타 CRL이 누락되었습니다.
27	인증하려는 이름이 이미 존재합니다.
28	인증하려는 공용 키가 이미 존재합니다.
29	일부 일련 번호 또는 키(인증서, CRL)가 올바르지 않습니다.
30	권한을 부여하지 못했습니다.

SSL 데이터 교환 프로토콜이 종료되면 SSLException이 전달됩니다.

표 2. SSLException 오류 메시지

ID	설명
3	SSLContext에서 정의된 연결 시간 종료가 만기되었으며 피어로부터 아무런 응답이 없었습니다.
4	추가적인 오류 내용 없이 SSL 데이터 교환 동안 피어에 의해 연결이 중지되었습니다.
10	예상치 못한 메시지가 수신되었습니다.
20	잘못된 레코드 MAC와 함께 메시지가 수신되었습니다.
30	압축 풀기 실패입니다.
40	데이터 교환 실패입니다.
41	피어에 의해 인증서가 송신되지 않았습니다.
42	잘못된 인증서가 수신되었습니다.
43	지원되지 않는 인증서가 수신되었습니다.
44	취소된 인증서가 수신되었습니다.

표 2. SSLException 오류 메시지 (계속)

45	만기된 인증서가 수신되었습니다.
46	알 수 없는 인증서가 수신되었습니다.
47	잘못된 매개변수가 감지되었습니다.

LDAP 및 CRL

WebSphere internet pass-thru는 LDAP(Lightweight Directory Access Protocol) 서버 사용을 지원하여 디지털 인증에서 CRL(Certificate Revocation List) 인증을 수행합니다. WebSphere 및 MQIPT에 모두 동일한 LDAP 서버가 사용될 수 있으므로 기본 WebSphere MQ와 유사한 방식으로 LDAP 지원이 구현되었습니다. WebSphere MQ에서의 LDAP 서버 사용에 대한 자세한 정보는 서적 ″WebSphere MQ 보안 버전 5.3″ SA30-1576-01, 15 장에 있습니다. 참조를 위해 서적에서 다음을 발췌했습니다.

SSL 데이터 교환 중에 통신 파트너는 서로 디지털 인증을 사용하여 인증합니다. 인증에는 수신한 인증을 트러스트할 수 있는지에 대한 점검이 포함될 수 있습니다. 인증 기관(CA)은 다음을 포함한 여러 가지 이유에서 인증을 호출합니다.

- 소유자가 다른 조직으로 이동했습니다.
- 개인용 키가 더 이상 비밀이 아닙니다.

CA는 CRL(Certificate Revocation List)에서 호출된 개인 인증을 게시합니다. 호출된 CA 인증은 ARL(Authority Revocation List)에 게시됩니다. 이 장에서 CRL에 대한 다음 참조사항은 ARL에도 적용됩니다.

시장에는 여러 개의 독점 LDAP 디렉토리 서버가 있습니다. WebSphere internet pass-thru는 IBM 디렉토리 서버를 사용하여 테스트하였습니다. `http://www.ibm.com/software/network/directory/server`를 참조하십시오. LDAP 서버 설치 및 유지보수에 대한 지시사항은 설치된 제품과 함께 제공된 문서에 있습니다.

CRL 및 ARL 관리에 대한 추가 정보는 서적 ″WebSphere MQ 보안 버전 5.3″ SA30-1576-01에 있습니다.

MQIPT는 각 라우트마다 최대 두 대의 LDAP 서버를 지원할 수 있습니다. 첫 번째 LDAP 서버는 기본 서버로 취급되고 두 번째 LDAP 서버는 백업 서버로 간주되며 기본 서버에 연결할 수 없을 때만 사용됩니다. 백업 서버는 기본 서버의 미러 이미지이어야 합니다.

LDAP 서버에 저장된 정보에 대한 액세스는 사용자 ID와 암호로 보호되어 있을 수 있습니다. 이와 같은 경우 LDAP*Userid와 LDAP*Password 등록 정보를 사용할 수 있습니다.

MQIPT가 키 링 파일에서 PKCS#12 토큰을 로드하면 CRL 검증을 위해 CA 인증을 점검합니다. CA 인증에 첨부된 CRL이 있으면 만기 여부가 확인되며 만기된 경우 LDAP 서버에서 새 CRL이 검색됩니다. 검색된 CRL은 현재 토큰에 로드되고 CA 인증에 첨부됩니다. 갱신된 토큰은 키 링 파일에 저장할 수 있습니다(86 페이지의 『라우트 섹션 참조 정보』에서 LDAPSaveCRL 등록 정보 참조).

쿼리가 기본 LDAP 서버로 송신된 경우 지정된 CA와 일치하는 항목이 없으면 해당 CA에 대한 CRL이 없는 것으로 간주됩니다. 백업 서버는 사용되지 않습니다. 그러나 기본 LDAP 서버에 연결할 수 없거나 지정된 시간 내에 리턴되지 않으면 백업 서버가 사용됩니다. 백업 서버에서 오류가 발생하면 클라이언트 연결이 종료됩니다.
LDAPIgnoreErrors 등록 정보를 참으로 설정하면 이 조치를 대체할 수 있습니다.

주의

LDAPIgnoreErrors 등록 정보를 사용하면 SSL 연결에 호출된 인증이 사용될 수 있습니다.

LDAP 클라이언트 모델은 ″com.sun.jndi.ldap.LdapCtxFactory″ 구현을 기준으로 합니다. MQIPT에서 검색한 CRL은 캐시에 보관되고 해당 라우트의 모든 연결에서 공유합니다.

캐시된 CRL이 만기되면 캐시에서 CRL이 제거되고 LDAP 서버에서 새 CRL이 검색됩니다. 새 CRL을 사용할 수 없는 경우에도 연결이 거부됩니다.

또한 LDAP 서버에서 검색된 CRL도 만기되었는지 점검하고 경고 시스템 콘솔 메시지가 표시됩니다(MQCPW001). 만기된 CRL은 시스템에 로드되고 이 CRL을 참조하는 연결 요청은 거부됩니다. LDAP 서버에서 만기된 CRL은 현재 CRL로 바꿔야 합니다.

LDAPCacheTimeout 등록 정보를 사용하여 CRL 캐시를 지우는 빈도를 제어할 수 있습니다. 디폴트 값은 1일입니다. 이 값을 0으로 설정하면 라우트가 재시작될 때까지 캐시 항목이 지워지지 않습니다.

만기된 CRL은 키 링 파일이나 LDAP 서버에 저장될 수 있습니다. 새 CRL이 발행되지 않으면 추가 연결 요청이 거부됩니다. IgnoreExpiredCRL 등록 정보를 사용하면 만기된 CRL을 무시할 수 있습니다.

주의

IgnoreExpiredCRL 등록 정보를 사용하면 SSL 연결에 호출된 인증이 사용될 수 있습니다.

AES(Advanced Encryption Standard)

AES(Advanced Encryption Standard)는 비밀(비기밀) 정보를 보호하기 위해 미국 정부 조직에서 사용할 암호 알고리즘을 지정하는 새로운 FIPS(Federal Information Processing Standard) Publication입니다. NIST(National Institute of Standards and Technology)에서도 AES가 미국 이외 국가의 조직, 단체, 개인에 의해 자발적으로 널리 사용될 것으로 예측하고 있습니다.

키 링 파일에서 인증 선택

같은 키 링 파일에 개인 인증을 둘 이상 저장할 수 있으므로 SSLClientSite* 등록 정보를 클라이언트측에 사용하여 인증을 위해 서버로 송신할 인증을 선택할 수 있으며, SSLServerSite* 등록 정보를 서버측에 사용하여 인증을 위해 클라이언트로 송신할 인증을 선택할 수 있습니다.

이러한 등록 정보를 사용하여 식별 이름(DN)에 따라 인증을 선택할 수 있습니다. 또는 SSLServerSiteLabel과 SSLClientSiteLabel 등록 정보를 사용하여 인증을 선택하는 데 인증 레이블을 사용할 수 있습니다.

키 링 암호 암호화

키 링 파일을 여는 데 사용되는 암호는 mqiptPW 스크립트를 사용하여 암호화할 수 있습니다. 암호화된 암호는 파일에 저장되고 SSLClientKeyRingPW, SSLClientCAKeyRingPW, SSLServerKeyRingPW 및 SSLServerCAKeyRingPW 등록 정보에 사용될 수 있습니다.

명령 형식:

```
mqiptPW <password> <file name> <-replace>
```

여기서,

password
지정된 키 링 파일을 여는 데 필요한 일반 텍스트 암호입니다.

file name
작성할 암호 파일의 이름입니다.

replace
<file name>(있는 경우)을 덮어쓰는 데 필요한 옵션입니다.

암호는 공백 문자(" ")를 포함할 수 있지만 공백이 허용되려면 전체 암호 문자열을 따옴표로 묶어야 합니다. 암호 길이나 형식에 대한 제한은 없습니다.

주: 이전 레벨의 WebSphere Internet pass-thru에서 이주한 사용자는 일반 텍스트 암호가 들어 있는 현재 암호 파일을 암호화된 암호 파일의 사본으로 바꿔야 합니다.

암호 mqiptV1.3을 사용하여 키 관리 유틸리티(예: KeyMan)를 통해 샘플 키 링 파일을 열어야 합니다.

KeyMan

이제 WebSphere internet pass-thru에 KeyMan이라는 독립형 유틸리티가 동봉되어 SSL 인증서 및 키 링 파일을 관리할 수 있습니다. KeyMan을 포함한 zip은 SSL 서브디렉토리에 있습니다. KeyMan을 설치하려면 임시 디렉토리에 파일 압축을 풀고 README.txt 파일의 지시사항을 따르십시오. KeyMan에는 많은 기능이 있으나 이 절에서는 테스트 인증서 작성과 PKCS#12 토큰을 포함한 키 링 파일 관리에 대해서만 설명합니다.

KeyMan은 공용 키 인프라스트럭처(PKI)의 클라이언트 측에 대한 관리 도구입니다. KeyMan은 키, 인증서, CRL(certificate revocation list) 및 각각의 저장소를 관리하여 이러한 항목을 저장하고 검색합니다. 인증서의 전체 라이프 사이클이 지원되며 프로세스는 사용자 인증서 핸들링과 관련됩니다.

KeyMan은 키, 인증서 및 취소 목록 콜렉션을 포함한 저장소를 관리합니다. 저장소는 토큰이라 불립니다. 토큰은 WebSphere internet pass-thru 등의 특정 응용프로그램에 대한 트러스트 설정으로 구성됩니다. 일반적으로 토큰은 다른 사이트에 대해 사용자를 인증하기 위해 개인용 키 및 연관된 인증서 체인을 포함합니다. 또한 토큰은 트러스트된 통신 파트너 및 인증 기관(CA)의 인증서를 보유합니다.

지원되는 토큰 유형

KeyMan은 다양한 다른 유형의 토큰을 지원합니다. 토큰은 키, 인증서, CRL 및 트러스트 설정을 보유하는 저장소입니다. 일부 토큰은 이러한 항목 유형의 서브세트만을 저장할 수 있습니다.

PKCS#7 토큰

일련의 인증서를 포함하며 선택적으로 관련된 CRL을 포함합니다. 이 유형의 저장소에는 키를 저장할 수 없습니다. 이 저장소에는 인증이 필요하지 않습니다. 인증서 및 CRL은 서명에 의해 보호됩니다. 그러나 의도적으로 특정 PKCS#7 토큰에 저장된 항목 세트를 변경하는 사용자가 있을 수 있습니다. 이러한 유형의 토큰은 예상된 항목 세트가 어떠한 컨텍스트에 의해 정의되는 경우에 사용됩니다.

PKCS#12 토큰

개인용 키, 인증서 및 관련 CRL을 포함합니다. 컨텐츠는 사용자 암호 문구에 의해 보호됩니다. 공용 항목(인증서, CRL) 및 개인용 항목(키)은 다른 강도의 알고리즘에 의해 보호됩니다.

PKCS#11(CryptoKi) 저장소

PKCS#11은 암호 토큰에 대한 인터페이스를 정의합니다. 이러한 토큰은 키와

인증서를 저장할 수 있습니다. CRL 저장은 지원되지 않습니다. 토큰에 대한 액세스는 PIN(personal identification number)에 의해 보호됩니다. 사용자는 반드시 KeyMan이 토큰에 액세스하기 위해 사용하는 특정 토큰 PKCS#11 DLL을 지정해야 합니다.

KeyMan은 PKCS#11 버전 2.01 및 2.10 DLL을 지원합니다.

PKCS#7 및 PKCS#12는 소프트 토큰이며 파일, URI 및 클립보드 등의 다른 매체에서 검색할 수 있습니다.

KeyMan은 알 수 없는 형식의 데이터로부터 PKCS#7 토큰을 구성할 수 있는 특수한 기능이 있습니다. 즉, X.509 인증서 및 CRL에 대한 데이터를 스캔하여 감지된 인증서 및 CRL에서 PKCS#7 토큰을 구성합니다. 인증서 또는 CRL을 포함한 전자 우편이 있는 경우, KeyMan에서 전자 우편을 열면 KeyMan이 X.509 항목을 추출하려고 시도합니다. 물론 데이터는 원래 형식으로 다시 저장될 수 없습니다. 추출된 데이터는 PKCS#7 형식을 사용하여 파일에 저장될 수 있습니다.

지원되는 표준 데이터 형식

KeyMan은 다양한 표준 데이터 형식을 지원합니다. 다음은 그 의미와 사용 컨텍스트에 대한 설명입니다.

PKCS#7

이 데이터 형식은 인증서와 CRL의 콜렉션입니다. PKCS#7에서 설명된대로 인증서와 CRL 세트는 보호되지 않습니다. 그러나 각 단일한 인증서와 CRL은 서명에 의해 보호됩니다. PKCS#7은 인증서와 CRL의 예상된 세트가 어떠한 컨텍스트에 의해 정의되는 경우에 사용됩니다. Windows 시스템에서 PKCS#7에 대한 표준 파일 접미부는 .p7r 및 .p7b입니다.

PKCS#10

PKCS#10은 인증서 요청 메시지를 정의합니다. 여기에는 공용 키 및 요청자의 X.500 이름에 관한 정보가 포함됩니다. 메시지는 해당되는 개인용 키와 함께 서명됩니다. PKCS#10 메시지는 2진 형식 및 ASCII 형식으로 생성될 수 있습니다. 메시지는 반드시 인증 기관(CA)에 제출되어야 합니다.

PKCS#12

PKCS#12는 브라우저와 웹 서버에 의해 개인용 키 및 관련 인증서의 들여오기와 내보내기에 사용됩니다. KeyMan은 이러한 PKCS#12 파일을 읽고 쓸 수 있습니다. 이러한 프로그램이 PKCS#12의 아주 특정한 프로파일만 이해하는데 반해 KeyMan은 보다 일반적인 PKCS#12 파일을 생성할 수 있습니다. KeyMan은 개인용 키, 인증서, CRL 및 해당되는 트러스트 설정 세트를 단일한 PKCS#12 파일에 저장할 수 있습니다. PKCS#12 파일은 컨텐츠는 암호 문구에 의해 보호됩니다. 일반적으로 PKCS#12 토큰은 특정 응용프로그램에 대한 트러스트 정책을 포함합니다. IBM BlueZ SSLite의 경우, 키 및 연관된 인

증서 체인이 클라이언트/서버 인증에 사용됩니다. 기타 인증서는 각각의 트러스트 설정에 따라 트러스트된 CA 또는 트러스트된 서버를 나타냅니다. Windows 시스템에서 PKCS#12 파일에 대한 표준 파일 접미부는 .p12 및 .pfx입니다.

SPKAC

SignedPublicKeyAndChallenge(SPKAC)는 CA로부터 인증서를 요청하기 위한 데이터 형식입니다. 이 특정 형식은 HTML 태그인 <keygen>이 사용될 때마다 Netscape에 의해 생성됩니다. 여기에는 서명된 공용 키 및 요구가 포함됩니다. 이 데이터 형식은 KeyMan에 의해 2진 및 Base64 형식으로 생성될 수 있습니다.

X.509 V3 인증서

KeyMan은 2진 형식 또는 ASCII 형식으로 줄 바꿈된 X.509 V3 인증서를 읽을 수 있습니다. 이러한 파일은 KeyMan에서 열거나 들여올 수 있습니다. 또한 이러한 두 가지 형식으로 토큰에서 단일 인증서를 기록할 수 있습니다(**인증서 세부사항 -> 아이콘 저장**). Windows 시스템에서 X.509 인증서 파일에 대한 표준 파일 접미부는 .crt, .cer 및 .der입니다.

X.509 V2 CRL(Certificate Revocation Lists)

KeyMan은 2진 형식 또는 ASCII 형식으로 줄 바꿈된 X.509 V2 CRL을 읽을 수 있습니다. 단일 CRL은 열 수 없습니다. KeyMan은 단지 CRL을 이미 연관된 CA 인증서를 포함한 토큰으로 들여오기만 합니다. 단일 CRL을 2진 또는 ASCII 형식으로 기록할 수 있습니다(**인증서 세부사항 -> CRL 세부사항 -> 아이콘 저장**). Windows 시스템에서 X.509 CRL 파일에 대한 표준 파일 접미부는 .crl입니다.

KeyMan FAQ

암호화 및 관련 주제에 대한 일반적인 질문은 RSA Laboratories 및 ″Frequently Asked Questions About Today's Cryptography″를 참조하십시오. 다음 FAQ는 KeyMan에 관한 질문에 대한 설명입니다.

KeyMan은 Netscape 또는 Internet Explorer에 의해 생성된 PKCS#12 파일을 읽을 수 있습니까?

KeyMan은 사용자가 해당 컨텐츠를 보호하는 암호를 아는 경우에만 Netscape 브라우저 또는 Internet Explorer에 의해 생성된 PKCS#12 파일을 읽을 수 있습니다.

KeyMan은 Netscape 또는 Internet Explorer가 읽을 수 있는 PKCS#12 파일을 작성할 수 있습니까?

PKCS#12 표준은 여러 가지 알고리즘 및 컨텐츠 배열을 선택할 수 있도록 해줍니다. 브라우저는 많은 가능한 옵션 중 매우 특정한 프로파일만 승인할 수 있습니다. KeyMan은 Netscape 및 Internet Explorer가 읽을 수 있는 PKCS#12 파일을 생성할 수 있습니다. KeyMan을 사용하면 PKCS#12를 사용하여 보다

많은 작업을 할 수 있으므로 이러한 브라우저가 파악할 수 없는 파일을 작성할 수 있습니다. 브라우저에 대한 일반적인 프로파일은 다음과 같습니다. 공용/개인용 암호화(**메뉴 옵션 -> PKCS#12 설정** 참조)가 반드시 각각 ″RC2 (40 bits)″/″DES (168 bits)″여야 합니다. 또한 PKCS#12 토큰 안에 정확히 하나의 개인용 인증서가 있어야 합니다.

개인용 인증서가 무엇입니까?

KeyMan이 일치하는 키와 인증서를 감지하면 이러한 두 항목을 개인용 인증서에 결합합니다. 즉, 임의의 개인용 인증서에 대해서도 해당되는 개인용 키를 갖게되는 것입니다. 사용자가 인증서를 토큰에 들여오는 경우, KeyMan은 일치하는 개인용 키가 있는지 점검하여 자동으로 키와 들여온 인증서를 개인용 인증서에 결합합니다. 이러한 작업이 수행되면 KeyMan이 대화 상자를 사용하여 사용자에게 알립니다.

CA 또는 피어 인증서가 무엇입니까?

토큰에 포함된 인증서가 트러스트를 설정합니다. 또한 누구에게 트러스트를 설정했는지 정의합니다. 트러스트의 의미 및 인증서의 정확한 평가는 토큰을 사용하는 응용프로그램에 의해 결정됩니다. 사용자는 KeyMan을 사용하여 인증서에 대해 CA 및 피어라는 두 가지 유형의 트러스트를 설정할 수 있습니다. CA로 인증서를 트러스트하면 CA가 직접적 또는 간접적으로 서명한 모든 인증서를 암시적으로 트러스트하게 됩니다. 트러스트 레벨을 ″피어″로 설정하면 이 특정 인증서만 트러스트하게 되는 것입니다. 트러스트는 ″피어″ 인증서에 의해 서명된 인증서로 확장되지 않습니다.

개인용 인증서가 아니며 CA 또는 피어 인증서도 아닌 인증서란 무엇입니까?

KeyMan은 각 개인용 인증서를 전체 체인까지 루트 인증서에 저장하려고 시도합니다. 이러한 인증서는 트러스트될 필요가 없으므로 CA 또는 피어 인증서 사이에 표시되지 않습니다. ″전체 인증서 항목″ 키 링을 선택하면 이러한 인증서를 찾을 수 있습니다. 트러스트되지 않은 인증서에는 아이콘이 없습니다.

토큰이 무엇입니까?

토큰이란 키, 인증서 및 CRL의 콜렉션입니다. 토큰은 파일, URL 및 하드웨어 부분 등의 일부 매체에 저장됩니다. 소프트웨어 토큰, 하드웨어 토큰, 보호되지 않는 토큰 및 암호나 PIN에 의해 보호되는 토큰 등, 다른 기능을 가진 다양한 유형의 토큰이 있습니다.

키 링이 무엇입니까?

토큰은 키 링 세트로 구성됩니다. 특정 키 링은 특정 항목 세트를 식별합니다. 예를 들어, 동일한 트러스트 레벨의 인증서 또는 개인용 키를 소유한 인증서 또는 일치하는 인증서가 없는 키 등입니다.

제 6 장 QoS(Quality of Service)

QoS(Quality of Service)

IBM WebSphere Edge Server는 Linux 플랫폼에서 서비스 플러그인의 Transactional Quality를 통해 대역폭 관리 솔루션을 제공합니다. TQoS(Transactional Quality of Service)란 네트워크 사용자에게 제공되는 처리량 및 지연 등의 요소적인 측면에서 전체 서비스를 의미합니다. 속성은 연결과 함께 송신되는 보내는 데이터와 연관된 서비스의 품질을 보장하도록 설정될 수 있습니다. 이렇게 함으로써 정책 관리자가 특정 서버와 관련된 소통량 및 이 소통량에 대한 차별화된 고유한 서비스 제어가 있는 정책 조치를 식별하는 규칙을 정의할 수 있습니다. 예를 들어, 설치 시에 클라이언트 찾아보기를 지원하는 서버 소통량에 비해 특정 양의 물건 판매를 지원하기 위해 서버 소통량과 관련된 보내는 소통량을 우선하여 처리하도록 지정하는 정책을 정의할 수 있습니다. 또한 TQoS를 사용하면 관리자는 해당 정책의 성능 데이터를 수집하여 의도한 서비스 레벨 목표(연결 처리량, 지연, 손실율 등과 같은 중요한 측정)가 정책에 반영되었는지 모니터할 수 있습니다. MQIPT에서는 정책 에이전트(pagent)를 설치하고 실행하여 QoS(Quality of Service)를 구현하기만 하면 됩니다.

TQoS 정책은 정책 구성 파일(`pagent.conf`)에서 정의되거나 LDAP 서버를 사용하여 정의됩니다. TQoS pagent는 정책 구성 파일에 액세스하거나 LDAP 서버로 가거나 둘 다를 수행하여 TQoS 정책 항목을 검색할 수 있습니다. pagent에 관한 자세한 정보가 나와 있는 *IBM Edge Server Administration Guide*는 다음 URL에서 찾을 수 있습니다.

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

이 사이트에서 TQoS 검색을 수행할 수 있는 HTML 온라인을 보거나 PDF 버전으로 다운로드할 수 있습니다.

TQoS 코드는 설치 및 관리 지시사항과 함께 MQIPT와 같은 위치에서 다운로드할 수 있습니다. WebSphere MQ 제품군 SupportPacs 사이트(`http://www.ibm.com/webspheremq/supportpacs`)를 참조하고 범주 3 - 제품 확장을 누르십시오.

MQIPT에는 MQIPT lib 서브디렉토리에 있는 `libmqiptqos.so`라는 더미 라이브러리가 동봉되어 있습니다. 이를 통해 TQoS pagent를 설치하지 않아도 MQIPT를 Linux 플랫폼에서 실행할 수 있습니다. TQoS를 설치하면 이 더미 라이브러리를 TQoS에 사용된 라이브러리로 바꿔야 할 수 있습니다. 이 작업은 도와주는 `mqiptQoS`라는 스크립트는 MQIPT bin 서브디렉토리에 있습니다. 다음 명령을 사용하여 더미 라이브러리의 이름을 바꾸고 실제 TQoS 런타임 라이브러리에 대한 소프트 링크를 정의하십시오.

```
mqiptQoS -install
```

mqiptQoS -remove를 사용하면 위의 조치가 취소됩니다.

MQIPT에서는 pagent를 설치하고 실행하여 QoS(Quality of Service)를 구현하기만 하면 됩니다. 응용프로그램 우선순위는 MQIPT를 사용하여 각 방향에서 데이터 플로우에 대한 라우트에서 설정되어 해당 라우트를 사용하는 모든 채널에 영향을 미칩니다. 우선순위는 MQIPT 등록 정보인 QosToCaller 및 QosToDest를 사용하여 정의되며(자세한 정보는 86 페이지의 『라우트 섹션 참조 정보』 참조) 여기서 사용되는 값은 반드시 pagent.conf 제어 파일의 ApplicationPriority 정책 정의와 일치해야 합니다. pagent가 일치하는 정책을 찾지 못하면 데이터에 어떠한 우선순위도 지정되지 않습니다. 정책에 대한 모든 변경 사항은 pagent가 재시작될 때까지 반영되지 않습니다. 정책 정의에 대한 자세한 정보는 117 페이지의 『Qos(Quality of Service) 구성』을 참조하십시오.

제 7 장 Network dispatcher

Network Dispatcher 지원

MQIPT는 IBM Network Dispatcher와 함께 사용되어 강화된 기능을 제공하며 사용자 정의 advisor를 사용하여 여러 서버에 걸쳐 로드 밸런스를 제공합니다. 이 절에서는 사용자가 Network Dispatcher 및 사용자 정의 advisors에 익숙하다고 가정합니다.

MQIPT와 함께 두 개의 사용자 정의 advisor가 제공되며 `lib` 서브디렉토리에서 찾을 수 있습니다. 사용자 정의 advisor를 설치하려면 *Network Dispatcher User's Guide* (GC31-8496)를 참조하십시오. 그림 7은 MQIPT용 1414 포트 주소를 모니터링하기 위해 Network Dispatcher를 사용하는 예를 보여줍니다. 각 MQIPT는 반드시 동일한 구성 파일을 갖고 있어야 합니다.

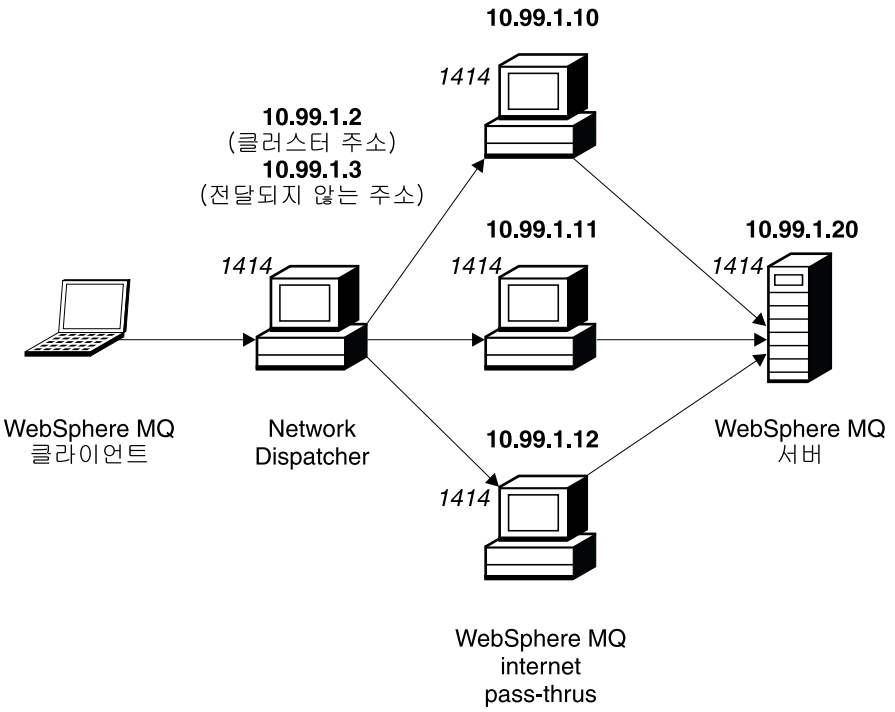

그림 7. MQIPT에서 Network Dispatcher 사용

1414 포트를 정의하고 로드 밸런스된 서버 시스템을 정의하도록 디스패처 구성요소를 구성하려면 *Network Dispatcher User's Guide* 5 장의 지시사항을 따르십시오. 관리 클라이언트의 메뉴 옵션 또는 "ndcontrol" 행 모드 명령을 사용할 수 있습니다. 예를 들어, 다음과 같습니다.

```
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
```

MQIPT 구성 파일의 라우트 정의는 다음과 같아야 합니다.

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

명령 행에서만 사용자 정의 advisor를 시작하거나 정지할 수 있습니다. 예를 들어, 다음과 같습니다.

```
ndcontrol advisor start mqipt_normal 1414
```

이 명령은 "정상" 모드에서 MQIPT advisor를 시작하며 이 모드에서는 기본 advisor가 자체 타이밍을 수행하여 각 MQIPT의 가중 요소를 계산합니다. "바꾸기" 모드에서 MQIPT를 사용하려면 다음 행을 MQIPT 라우트 정의에 추가하십시오.

```
NDAdvisorReplaceMode=true
```

사용자는 반드시 mqipt_normal 대신 mqipt_replace 사용자 정의 advisor를 시작해야 합니다. 예를 들어, 다음과 같습니다.

```
ndcontrol advisor start mqipt_replace 1414
```

SSL 리스너 포트를 모니터하기 위해 advisor를 사용하는 경우, 즉, mqipt.conf 구성 파일에서 SSLServer=true인 경우에는 반드시 Network Dispatcher의 작업 디렉토리에 ″트리거″ 파일을 두어야 합니다. 이 ″트리거″ 파일은 모니터되는 라우트에 대한 특정 이름을 갖고 있습니다. 예를 들어, Windows NT에서 라우트 1414가 SSLServer=true이면 mqipt1414.ssl이라는 파일이 반드시 c:\winnt\system32 디렉토리에 있어야 합니다. 자세한 정보는 mqipt1414Sample.ssl 파일을 참조하십시오.

제 8 장 Java 보안 관리자 및 보안 엑시트

Java 보안 관리자

Java 보안 관리자 지원은 원래 SSL 프록시 모드 기능과 함께 사용하여 소켓 연결의 제어를 관리하기 위해 구현되었으나 기타 다른 MQIPT 기능 중 하나와 함께 사용하여 보다 높은 수준의 보안을 제공할 수도 있습니다.

MQIPT는 java.lang.SecurityManager 클래스에서 정의된 대로 디폴트 Java 보안 관리자를 사용합니다. MQIPT의 Java 보안 관리자 기능은 전역 등록 정보인 SecurityManager를 사용하여 사용하거나 사용 안함으로 설정할 수 있습니다. 자세한 정보는 85 페이지의 『전역 섹션 참조 정보』를 참조하십시오.

Java 보안 관리자는 두 개의 디폴트 정책 파일을 사용합니다. 전역 시스템 정책 파일인 $JREHOME/lib/security/java.policy(여기서, $JREHOME은 사용자의 Java 런타임 환경을 포함한 디렉토리임)는 호스트에서 가상 시스템의 모든 인스턴스에 의해 사용될 수 있습니다. 두 번째 사용자 지정 정책 파일인 .java.policy는 사용자의 홈 디렉토리에 있을 수 있습니다. 추가 MQIPT 정책 파일 또한 사용될 수 있습니다. 자세한 정보는 85 페이지의 『전역 섹션 참조 정보』를 참조하십시오. 추가 정책 파일을 사용하려면 policy.allowSystemProperty 등록 정보가 전역 시스템 정책 파일(java.security)에서 참으로 설정되었는지 확인하시시오.

정책 파일의 구문은 텍스트 편집기를 사용하여 변경할 수 있으나 매우 복잡하므로 Java와 함께 제공되는 policytool 유틸리티를 사용하여 변경할 것을 권장합니다. policytool 유틸리티는 $JREHOME/bin 디렉토리에서 찾을 수 있으며 Java 문서에 전체적인 설명이 나와 있습니다.

샘플 정책 파일(mqiptSample.policy)이 MQIPT와 함께 제공되어 MQIPT 실행에 어떤 사용권한이 필요한지 보여 줍니다. 누가 MQIPT에 연결할 수 있는지, MQIPT가 누구에게 연결할 수 있는지 제어하기 위한 사용자 자신의 특정 요구사항에 맞추기 위해 추가, 변경, 삭제해야 하는 유일한 항목이 java.net.SocketPermission 항목입니다. 이 샘플 파일은 MQIPT가 c:\Program Files\IBM\Websphere MQ internet pass-thru\ 등의 디폴트 홈 디렉토리에 설치되었다고 가정합니다. 다른 위치에 MQIPT를 설치한 경우에는 codeBase 및 java.io.FilePermission 정의가 다른 위치를 반영하도록 해야 합니다.

사용권한은 일반적으로 세 개의 속성에 의해 정의되며 소켓 연결을 제어하는데 사용됩니다. 각각의 값은 다음과 같습니다.

클래스 사용권한

java.net.SocketPermission

제어할 이름

hostname:port 형식으로 구성되며 이름의 각 구성요소는 와일드카드에 의해 지정될 수 있습니다. 호스트 이름은 도메인 이름 또는 IP 주소가 될 수 있습니다. 호스트 이름의 제일 왼쪽 위치는 (*)에 의해 지정될 수 있습니다. 예를 들어, harry.company1.com은 다음 문자열 각각에 의해 일치될 수 있습니다.

- harry
- harry.company1.com
- *.company1.com
- *
- 123.456.789(harry.company1.com의 IP 주소라고 가정함)

이름의 포트 구성요소는 단일한 포트 주소 또는 포트 주소 범위를 사용하여 지정할 수 있습니다. 예를 들면, 다음과 같습니다.

1414 1414포트만

1414- 1414 이상인 모든 포트 주소

-1414 1414 이하인 모든 포트 주소

1-1414

1과 1414 사이의 모든 포트 주소, 포괄적

허용되는 조치

java.net.SocketPermission에 의해 사용되는 조치는 다음과 같습니다.

- 승인, 이 조치는 지정된 대상으로부터 연결을 승인하도록 사용 권한을 허용합니다.
- 연결, 이 조치는 지정된 대상에 연결하도록 사용 권한을 허용합니다.
- 대기, 이 조치는 지정된 포트에서 연결 요청에 대기하도록 사용 권한을 허용합니다.
- 해석, 이 조치는 도메인 이름을 IP 주소로 해석하기 위해 DNS 이름 서비스를 사용하도록 사용 권한을 허용합니다.

java.security.manager 및 java.security.policy Java 시스템 등록 정보를 사용하여 Java 보안 관리자를 제어할 수도 있으나 MQIPT 제어에서는 SecurityManager 및 SecurityManagerPolicy 등록 정보를 사용하도록 권장합니다.

보안 엑시트

주의

MQIPT가 단일 JVM에서 실행되므로 사용자 정의된 보안 엑시트는 다음과 같은 이유에서 MQIPT의 정상 조작을 방해할 수 있습니다.

- 시스템 자원에 영향을 미침
- 병목 현상 생성
- 성능 저하

프로덕션 환경에서 구현하기 전에 보안 엑시트의 영향을 광범위하게 테스트해야 합니다.

보안 엑시트의 목적은 Destination 라우트 등록 정보에 정의된 대로 대상 목적지에 대한 액세스를 제어하는 것입니다. 보안 엑시트는 클라이언트로부터 연결 요청을 수신할 때와 MQIPT가 대상 목적지에 연결하기 전에 호출됩니다. 초기 연결 등록 정보에 따라 보안 엑시트는 연결이 완료될지 결정할 수 있습니다.

라우트가 시작되면 초기화할 수 있도록 보안 엑시트가 호출되고 연결 요청을 처리하기 위한 준비가 됩니다. 사용자 데이터를 로드하고 이 데이터에 빠르고 쉽게 액세스할 수 있도록 초기화 프로세스를 사용하여 연결 요청을 처리하는 데 걸리는 시간을 최소화해야 합니다.

각 라우트에는 고유한 보안 엑시트가 있을 수 있습니다. SecurityExit 등록 정보는 사용자 정의된 보안 엑시트를 활성화/비활성화하는 데 사용됩니다. SecurityExitName 등록 정보는 사용자 정의된 보안 엑시트의 클래스 이름을 정의하는 데 사용됩니다. SecurityExitPath 등록 정보는 클래스 파일이 포함된 디렉토리 이름을 정의하는 데 사용됩니다. 이 등록 정보가 설정되지 않으면 클래스 파일은 엑시트 서브디렉토리에 있는 것으로 간주됩니다. 또한 SecurityExitPath는 사용자 정의된 보안 엑시트가 포함된 jar 파일의 이름을 정의할 수도 있습니다. 마지막으로 SecurityExitTimeout 등록 정보는 연결 요청을 유효화할 때 보안 엑시트의 응답을 기다리는 시간을 판별할 수 있도록 MQIPT에 사용됩니다.

MQIPT가 사용자 정의된 보안 엑시트를 호출할 수 있도록 SecurityExit라는 새 클래스가 작성되었습니다. 이 새 클래스는 사용자 정의된 보안 엑시트에 의해 확장되어야 하며 대부분의 메소드는 필요한 기능을 제공할 수 있도록 대체되어야 합니다. SecurityExitResponse 오브젝트는 데이터를 MQIPT로 다시 전달하는 데 사용되고 이

데이터는 MQIPT에 사용되어 연결 요청을 승인할지 또는 거부할지 결정합니다. 또한 SecurityExitResponse는 라우트 정의 등록 정보를 대체하는 데 사용되는 새 목적지와 목적지 포트 주소를 포함할 수도 있습니다.

보안 엑시트의 구현 방법을 표시하도록 세 개의 샘플 보안 엑시트가 제공되었습니다. SampleSecurityExit라는 첫 번째 샘플은 WMQ 채널의 이름에 따라 WebSphere MQ 큐 관리자에 대한 액세스 제어 방법을 표시합니다. 문자열 ″MQIPT″로 시작되는 채널 이름의 연결만 허용됩니다. 자세한 정보는 150 페이지의 『보안 엑시트』를 참조하십시오.

SampleRoutingExit라는 두 번째 샘플에서는 각각 같은 이름과 같은 속성의 QM을 호스트하는 서버인, 정의된 WebSphere MQ 서버의 풀로 클라이언트 연결 요청의 동적 라우팅이 허용됩니다. 샘플에는 서버 이름 목록이 포함된 구성 파일이 있습니다. 자세한 정보는 153 페이지의 『라우팅 보안 엑시트』를 참조하십시오.

SampleOneRouteExit라는 세 번째 샘플에서는 연결 요청에 사용된 WMQ 채널 이름에서 도출된 WMQ QM으로의 동적 라우팅이 허용됩니다. 샘플에는 서버 이름으로의 QM 이름 맵이 포함된 구성 파일이 있습니다. 자세한 정보는 156 페이지의 『동적 1 라우트 엑시트』를 참조하십시오.

com.ibm.mq.ipt.SecurityExit 클래스

이 클래스와 공용 메소드는 일부 공용 데이터에 액세스하고 일부 MQIPT 초기화가 발생할 수 있도록 사용자 정의된 보안 엑시트를 통해 확장되어야 합니다. MQIPT에서 각 메소드를 호출하기 전에 사용할 메소드에 대해 일부 등록 정보가 사용 가능하게 됩니다. 해당 값은 이 클래스에 정의된 적절한 get 메소드를 사용하여 검색할 수 있습니다. 지원되는 메소드의 모든 목록은 아래를 참조하십시오.

메소드

init

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

다음 등록 정보는 사용 가능합니다.

- 리스너 포트
- 목적지
- 목적지 포트
- 버전

init 메소드는 라우트가 시작될 때 MQIPT에 의해 호출됩니다. 보안 엑시트가 이 메소드에서 리턴되면 연결 요청을 유효화할 준비가 되어 있어야 합니다. 이 메소드에서 예외가 발생하면 라우트가 시작될 수 없습니다.

refresh

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

다음 등록 정보는 사용 가능합니다.

- 리스너 포트
- 목적지
- 목적지 포트

MQIPT 관리 클라이언트에서 새로 고치도록 요청을 받으면 MQIPT에 의해 refresh 메소드가 호출됩니다. 이 조치는 보통 구성 파일에서 등록 정보가 변경된 경우 호출됩니다. MQIPT는 구성 파일에서 모든 등록 정보를 로드하고 변경된 등록 정보를 판별하고 라우트를 즉시 재시작할지 여부 또는 다음에 MQIPT가 재시작될 때까지 대기할지 여부 등을 판별합니다.

이 메소드는 사용되는 외부 데이터(즉, init 메소드 중에 로드된 데이터)를 다시 로드해야 합니다. 이 메소드에서 예외가 발생하면 라우트가 사용 불가능하게 됩니다.

close

```
public void close ()
```

다음 등록 정보는 사용 가능합니다.

- 리스너 포트
- 목적지
- 목적지 포트

MQIPT 관리 클라이언트에서 정지하도록 요청을 받으면 MQIPT에 의해 close() 메소드가 호출됩니다. 조작 중에 확보한 시스템 자원을 해제해야 합니다. MQIPT는 이 메소드가 완료될 때까지 기다린 후 종료합니다.

이 메소드는 보안 엑시트가 사용 가능하지만 구성 파일에서는 사용할 수 없는 경우에도 호출됩니다.

validate

```
public SecurityExitResponse validate ()
```

다음 등록 정보는 사용 가능합니다.

- 리스너 포트
- 목적지
- 목적지 포트
- 시간 종료
- 클라이언트 IP 주소
- 클라이언트 포트 주소

- 채널 이름
- 큐 관리자 이름

validate 메소드는 유효화할 연결 요청을 수신할 때 MQIPT에 의해 호출됩니다. SSLProxyMode 등록 정보를 사용한 경우에는 채널 이름과 큐 관리자 이름를 사용할 수 없습니다. 이 기능은 SSL 데이터를 터널링하는 데에만 사용되므로 주로 초기 데이터 플로우에서 얻은 데이터를 읽을 수 없습니다. 큐 관리자 이름은 WMQ 클라이언트 연결에 사용할 수 없습니다. 이 정보는 대상 큐 관리자로 연결된 후에야 사용할 수 있습니다.

보안 엑시트는 다음 정보가 포함된 SecurityExitResponse 오브젝트를 리턴해야 합니다.

- 이유 코드(설정해야 함)
- 새 목적지 주소(선택적)
- 새 목적지 리스너 포트 주소(선택적)
- 메시지(선택적)

이유 코드는 MQIPT가 연결을 승인할지 또는 거부할지 판별합니다. 새 대상(QM)을 정의할 수 있도록 newDestination 및 newDestinationPort 필드를 선택적으로 설정할 수 있습니다. 이러한 등록 정보를 설정하지 않으면 구성 파일에 정의된 라우트 Destination 및 DestinationPort 등록 정보가 사용됩니다. 연결 로그 파일 항목에 메시지가 추가됩니다.

등록 정보를 확보하는 데 지원되는 메소드:

public int getListenerPort()
라우트 리스너 포트 검색 - ListenerPort 등록 정보에 정의됨

public String getDestination()
목적지 주소 검색 - Destination 등록 정보에 정의됨

public int getDestinationPort()
목적지 리스너 포트 주소 검색 - DestinationPort 등록 정보에 정의됨

public String getClientIPAddress()
연결을 요청하는 클라이언트의 IP 주소 검색

public int getClientPortAddress()
연결을 요청하는 클라이언트에 사용되는 포트 주소 검색

public int getTimeout()
시간 종료 값 검색. MQIPT는 보안 엑시트가 요청을 유효화할 때까지 대기 - SecurityExitTimeout 등록 정보에 정의됨

public int getConnThreadID()
디버깅 용도로 유용한 연결 요청을 핸들링하는 연결 스레드 ID 검색

public String getChannelName()
연결 요청에 사용된 WMQ 채널 이름 검색

public String getQMName()
연결 요청에 사용된 WMQ 큐 관리자 이름 검색

public boolean getTimedout()
시간 종료가 만기되었는지 판별하기 위해 보안 엑시트에 사용할 수 있음

com.ibm.mq.ipt.SecurityExitResponse 클래스

이 클래스는 사용자 정의된 보안 엑시트에서 다시 MQIPT로 응답을 전달하는 데 사용되며 연결 요청을 승인하거나 거부할지 판별하는 데 사용됩니다. 이 유형의 오브젝트는 validate 메소드에서만 작성됩니다(위 참조). 이러한 오브젝트를 편리하게 작성하는 구성자가 있으며 각 등록 정보에 설정된 메소드가 있습니다. 자세한 정보는 샘플 보안 엑시트를 참조하십시오.

기본 SecurityExitResponse 오브젝트를 작성하면 연결 요청이 거부됩니다.

지원되는 구성자:

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

여기서

- `dest`는 새 대상 목적지입니다.
- `destPort`는 새 목적지 포트 주소입니다.
- `rc`는 이유 코드입니다.
- `msg`는 연결 로그 입력으로 추가하는 메시지입니다.

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

public SecurityExitResponse(int rc, String msg) throws IPTException

public SecurityExitResponse(int rc) throws IPTException

등록 정보 값을 설정하는 데 지원되는 메소드:

public void setDestination(String dest)
연결 요청에 대해 새 목적지 주소를 설정합니다.

public void setDestinationPort(int port) throws IPTException
연결 요청에 대해 새 목적지 리스너 포트 주소 설정 - 올바르지 않은 포트 주소에 IPTException 발생

public void setMessage(String msg)
연결 로그 레코드로 메시지를 추가합니다.

public void setReasonCode(int rc) throws IPTException

연결 요청에 대한 이유 코드 설정 - 알 수 없는 값에 IPTException 발생

올바른 이유 코드는 다음과 같습니다.

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

추적

사용자 정의된 보안 엑시트에서 문제점을 진단하기 위해 MQIPT에 사용되는 것과 유사한 추적 기능을 사용할 수 있습니다. 라우트 Trace 등록 정보를 1-5 값으로 설정하면 오류 서브디렉토리에 추적 파일이 작성됩니다. 추적 파일의 이름은 보안 엑시트의 이름과 같습니다.

동시에 실행되는 보안 엑시트 인스턴스가 두 개 이상 있을 수 있으므로 스레드 ID를 사용하여 추적 파일의 개별 항목을 식별할 수 있습니다.

추적 기능의 초기화는 보안 엑시트가 시작될 때 MQIPT에 의해 수행됩니다. 반드시 추적할 정보를 선택해야 합니다. 샘플 사용자 종료에 다수의 추적 예가 있습니다.

추적에 대한 최소 요구사항은 entry 호출, exit 호출 및 추적할 데이터입니다. 예를 들어, 다음과 같습니다.

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

  .
  .
  .
  <code>

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

  .
  .
  .
  <code>

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

제 9 장 포트 주소 제어

포트 주소 제어

MQIPT를 사용하면 라우트에 OutgoingPort 등록 정보를 설정하여 보내는 연결을 작성할 때 사용할 로컬 포트 주소의 범위를 제한할 수 있습니다. 로컬 포트 주소의 범위는 MaxConnectionThreads 값을 사용하여 계산됩니다. 예를 들어, OutgoingPort가 1600으로 설정되고 MaxConnectionThreads가 20으로 설정되면 해당 라우트의 로컬 포트 주소 범위는 1600-1619가 됩니다. 라우트에서 포트 주소가 충돌하지 않도록 하는 것이 MQIPT 관리자의 책임입니다. OutgoingPort가 정의되지 않은 경우 디폴트 값 0은 각 연결에 시스템 할당 포트 주소가 사용됨을 의미합니다.

자세한 정보는 139 페이지의 『포트 주소 할당』에서 예를 참조하십시오.

멀티홈 시스템

멀티홈 시스템을 사용할 경우 LocalAddress 등록 정보를 사용하여 보내는 연결이 바인딩될 IP 주소를 지정할 수 있습니다. 호스트 이름은 이 등록 정보에서 지원되지 않습니다.

제 10 장 기타 보안 고려사항

기타 보안 고려사항

SSL을 사용하지 않기로 결정한 경우에는 MQIPT가 채널 보안 플로우를 허용하므로 WebSphere MQ 채널 엑시트를 사용하여 끝에서 끝까지 전체 채널에 대한 보안을 제공할 수 있습니다.

MQIPT에는 설계자가 보안 솔루션을 빌드하는 데 도움이 되는 여러 추가 기능이 있습니다.

- 내부 네트워크에 모두 보내려는 연결을 작성하려고 시도하는 클라이언트가 많이 있으면 모두 방화벽 안에 위치한 MQIPT를 통해 가능합니다. 그러면 방화벽 관리자가 MQIPT 시스템에만 외부 액세스를 부여할 수 있습니다.
- MQIPT는 SOCKS 프록시 역할 또는 보안 엑시트 사용을 수행하지 않는 한, 구성 파일에서 명확히 대상으로 구성된 큐 관리자에 대해서만 연결할 수 있습니다.
- MQIPT는 메시지에 대해 수신 및 전송이 올바른지, WebSphere MQ 프로토콜을 따르는 지 확인합니다. 이로 인해 MQIPT가 WebSphere MQ 프로토콜 외부의 보안 공격에 사용되는 것을 방지할 수 있습니다. MQIPT가 SSL 프록시 역할을 하는 경우에는 모든 WebSphere MQ 데이터와 프로토콜이 암호화되었을 때만 MQIPT가 초기 SSL 데이터 교환을 보장합니다. 이런 경우, Java 보안 관리자를 사용하도록 권장합니다. 33 페이지의 『Java 보안 관리자』를 참조하십시오.
- 채널 엑시트가 자체 엔드-투-엔드 보안 프로토콜을 실행할 수 있습니다.
- MQIPT를 사용하면 `MaxConnectionThreads` 등록 정보를 설정하여 수신되는 연결의 총 수를 제한할 수 있습니다. 이렇게 하면 서비스 거부 공격으로부터 취약한 내부 큐 관리자를 보호할 수 있습니다.

MQIPT 구성 파일인 `mqipt.conf`는 내부 호스트에 대한 액세스를 제어하므로 반드시 보호해야 하며 명령 포트(사용할 수 있는 경우만 해당됨)에 대한 무단 액세스는 외부 사용자가 MQIPT를 종료할 수 있도록 허용하므로 반드시 보호해야 합니다.

제 11 장 기타 기능

정상 종료 및 실패 조건

MQIPT가 WebSphere MQ 채널이 닫히는 것을 감지하면 정상 또는 비정상을 불문하고 채널 닫힘을 전달합니다. 관리자가 MQIPT를 통해 라우트를 닫으면 해당 라우트를 통해 나가는 모든 채널이 닫힙니다.

MQIPT는 선택적인 비활동 시간 종료 기능을 제공합니다. MQIPT가 채널이 시간 종료 시간을 초과하는 기간 동안 비활동인 것을 감지하면 해당되는 두 연결에서 즉시 종료를 수행합니다.

채널의 한 끝에 있는 두 WebSphere MQ 시스템이 이러한 비정상 종료 조건이 네트워크 실패인지 또는 파트너의 채널 종료로 인한 것인지 관찰합니다. (실패가 프로토콜 인다우트(in-doubt) 기간 동안 발생한 경우) MQIPT가 사용되지 않을 때 작동하는 것처럼 문제가 되는 채널이 재시작하고 복구할 수 있습니다.

메시지의 안전성

신속한 비지속 WebSphere MQ 메시지를 사용하는 경우, MQIPT 라우트가 실패했을 때나 WebSphere MQ 메시지가 전송 중일때 재시작되면 메시지가 손실될 수 있습니다. 라우트를 재시작하기 전에 모든 MQIPT 라우트를 사용하는 모든 WebSphere MQ 채널이 비활성인지 확인하십시오.

WebSphere MQ 메시지 및 채널에 관한 자세한 정보를 보려면
MQSeries Intercommunication, SC33-1872를 참조하십시오.

연결 로그

MQIPT는 모든 성공적이거나 비성공적인 연결 시도 목록을 포함한 연결 로그 기능을 제공합니다. 이 기능은 `ConnectionLog` 및 `MaxLogFileSize` 등록 정보에 의해 제어됩니다. 자세한 정보는 85 페이지의 『전역 섹션 참조 정보』를 참조하십시오.

MQIPT 각 시작될 때마다 새 연결 로그가 작성됩니다. 각 파일은 식별 가능하도록 파일 이름에 현재 시간 소인을 사용합니다. 예를 들면, 다음과 같습니다.

```
mqiptYYYYMMDDHHmmSS.log
```

여기서,

- `YYYY`는 연도입니다.
- `MM`은 월입니다.

- DD는 일입니다.
- HH는 시간입니다.
- mm은 분입니다.
- SS는 초입니다.

이러한 로그는 감사에 사용되므로 결코 지워지지 않습니다. 이러한 파일을 관리하고 더 이상 필요하지 않을 때 삭제하는 것은 MQIPT 관리자의 책임입니다.

제 12 장 이전 버전으로부터 업그레이드

MQIPT를 1.2 버전에서 1.3 버전으로 업그레이드하려면 다음 단계에 따르십시오.

1. 구성 파일 mqipt.conf 및 client.conf를 복사하십시오. mqipt.conf는 MQIPT 홈 디렉토리에 있고 client.conf는 용 구성 파일디렉토리에 있습니다.
2. 명령을 실행하여 MQIPT를 정지합니다.

   ```
   mqiptAdmin -stop
   ```

3. MQIPT를 서비스로 설치한 경우에는 MQIPT를 설치 제거하기 전에 반드시 제거해야 합니다.

   ```
   mqiptService -remove
   ```

4. MQIPT용 설치 제거 프로그램를 실행합니다.
5. MQIPT V1.3을 설치했으면 저장된 구성 파일을 다시 원래의 위치에 복사하십시오.
6. MQIPT 관리 GUI를 사용하여 MQIPT에 대한 변경 사항을 관리하는 것이 좋습니다. V1.2의 구성 파일은 GUI와 호환 가능합니다.

일부 구현에는 자체 조직에서 제어하는 로컬 MQIPT 서비스와 클라이언트 조직에서 제어하는 리모트 MQIPT 서비스가 필요합니다. 이런 상황에서 두 MQIPT 서비스를 동시에 이주하기 어렵지만 MQIPT에서는 그렇지 않습니다. 달리 명시하지 않는 한 MQIPT의 이전 버전은 최신 버전과 호환됩니다. 그러므로 MQIPT 이주 프로세스가 훨씬 간편합니다.

또한 먼저 설치 제거하지 않아도 MQIPT의 코어를 업그레이드할 수도 있습니다. MQIPT를 실행하는 데 필요한 모든 클래스는 MQipt.jar 파일에 저장됩니다. MQIPT의 최신 버전을 다른 시스템에 설치하고 해당 설치에서 활성 시스템으로 MQipt.jar 파일을 복사할 수 있습니다. 관리 GUI를 실행하는 데 필요한 클래스의 경우도 마찬가지입니다. 이러한 클래스는 guiadmin.jar 파일에 있습니다.

새 구성 옵션

다음 등록 정보는 1.3 버전에서 새로 나온 등록 정보입니다.

- IgnoreExpiredCRLs
- LDAP
- LDAPCacheTimeout
- LDAPIgnoreErrors
- LDAPSaveCRL
- LDAPServer1

- LDAPServer1Password
- LDAPServer1Port
- LDAPServer1Timeout
- LDAPServer1Userid
- LDAPServer2
- LDAPServer2Password
- LDAPServer2Port
- LDAPServer2Timeout
- LDAPServer2Userid
- RouteRestart
- SecurityExit
- SecurityExitName
- SecurityExitPath
- SecurityExitTimeout
- SSLClientSiteDN_C
- SSLClientSiteDN_CN
- SSLClientSiteDN_L
- SSLClientSiteDN_O
- SSLClientSiteDN_OU
- SSLClientSiteDN_ST
- SSLClientSiteLabel
- SSLServerSiteDN_C
- SSLServerSiteDN_CN
- SSLServerSiteDN_L
- SSLServerSiteDN_O
- SSLServerSiteDN_OU
- SSLServerSiteDN_ST
- SSLServerSiteLabel

모든 등록 정보에 대한 참조 정보를 보려면 81 페이지의 『구성 참조 정보』를 참조하십시오.

제 13 장 Windows에 internet pass-thru 설치

이 장에서는 Windows NT, Windows 2000 또는 Windows XP 시스템에 MQIPT를 설치하는 방법을 설명합니다.

파일 다운로드 및 설치

MQIPT(MS81, 범주 3 SupportPac™)는 다음 주소의 WebSphere MQ SupportPac 웹 페이지에서 다운로드됩니다.

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

다운로드하려면 다음 지시사항을 따르십시오.

일단 명령 프롬프트를 열고 `ms81_nt.zip`을 임시 디렉토리로 팩을 푸십시오. `setup.exe`를 실행하고 온라인 지시사항에 따르십시오.

MQIPT는 반드시 관리자 권한이 있는 사용자에 의해 설치되어야 합니다.

MQIPT에는 다음 표에 표시된 파일, 관리 클라이언트 GUI용 파일 및 다음 표에 표시된 것과 같이 별도로 설치할 수 있는 피처 등이 들어 있습니다.

파일	용도
Readme.txt	책에 포함되지 않은 최신 정보
mqiptSample.conf	샘플 구성 파일
ssl\sslSample.pfx	테스트 키 링 파일
ssl\sslSample.pwd	테스트 키 링 파일용 암호
ssl\sslCAdefault.pfx	샘플 인증 권한(CA) 키 링 파일
ssl\sslCAdefault.pwd	샘플 CA 키 링 파일용 암호 파일
ssl\KeyMan.zip	KeyMan 유틸리티
exits\SampleOneRouteExit.java	샘플 보안 엑시트
exits\SampleOneRouteExit.conf	SampleOneRouteExit용 구성 파일
exits\SampleRoutingExit.java	샘플 보안 엑시트

파일	용도
exits\SampleRoutingExit.conf	SampleRoutingExit용 구성 파일
exits\SampleSecurityExit.java	샘플 보안 엑시트
lib\MQipt.jar	런타임, 클래스 및 등록 정보 파일 포함
lib\ADV_mqipt_normal. class	"정상" 모드에 대한 Network Dispatcher advisor
lib\ADV_mqipt_replace. class	"바꾸기" 모드에 대한 Network Dispatcher advisor
lib\mqipt1414Sample.ssl	Network Dispatcher advisor에 대한 샘플 트리거 파일
bin\mqipt.bat	명령 행에서 MQIPT 실행에 대한 바로 가기
bin\mqiptAdmin.bat	MQIPT 정지 및 파일 정보 새로 고침에 대한 바로 가기
bin\mqiptPW.bat	키 링 파일을 여는 데 사용되는 암호 암호화
bin\mqiptservice.exe	Windows 서비스 제어 관리자에 MQIPT를 추가하거나 Windows 서비스 제어 관리자로부터 MQIPT를 제거하는데 사용됨
bin\mqiptVersion.bat	MQIPT의 버전 번호 표시
web\MQIPTServlet.war	servlet 버전용 웹 보존 파일
doc\<lang>\html\ <filename>.zip	HTML 형식의 *internet pass-thru* 매뉴얼에 대한 마스터 파일. 소프트카피 문서에 대한 자세한 정보는 191 페이지의 『참고 문헌』을 참조하십시오.

관리 클라이언트 GUI 피처와 연관된 파일을 다음과 같습니다.

파일	용도
lib\guiadmin.jar	런타임, 클래스 및 등록 정보 파일 포함
bin\mqiptGui.bat	명령 행에서 관리 클라이언트 실행에 대한 바로 가기
bin\customSample. properties	관리 클라이언트의 화면 및 액세스 가능성을 사용자 정의하는 샘플 파일

설치 프로그램은 `MQipt.jar` 및 `guiadmin.jar` 파일의 위치와 함께 시스템 CLASSPATH 환경 변수를 갱신합니다.

internet pass-thru 설정

처음으로 MQIPT를 시작하기 전에 샘플 구성 파일인 `mqiptSample.conf`를 `mqipt.conf`로 복사하십시오. 자세한 정보는 75 페이지의 제 19 장 『internet pass-thru 관리 및 구성』을 참조하십시오.

명령 행에서 internet pass-thru 시작

명령 프롬프트를 열어 디렉토리를 `bin` 디렉토리로 변경하고 `mqipt`를 실행합니다. 예를 들어, 다음과 같습니다.

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

또한 Windows 시작 -> 프로그램 메뉴에서 MQIPT를 시작할 수 있습니다.

옵션 없이 mqipt 스크립트를 실행하면 구성 파일(mqipt.conf)에 대해 "."의 디폴트 위치를 사용합니다. 다른 위치를 지정하려면 다음과 같이 하십시오.

```
mqipt <directory name>
```

MQIPT의 상태를 나타내는 메시지가 콘솔에 표시됩니다. 오류가 발생한 경우에는 161 페이지의 『문제점 판별』을 참조하십시오. MQIPT가 성공적으로 시작되면, 예를 들어 다음과 같은 메시지가 표시됩니다.

```
5639-L92 (C) Copyright IBM Corp. 2000, 2003 All Rights Reserved
MQCPI001 WebSphere MQ internet pass-thru Version 1.3.0 starting
MQCPI004 Reading configuration information from c:\mqipt\mqipt.conf
MQCPI008 Listening for control commands on port 1881
MQCPI011 The path c:\mqipt\logs will be used to store the log files
MQCPI006 Route 1418 has started and will forward messages to :
MQCPI034 ....mqserver.company4.com(1414)
MQCPI035 ....using MQ protocols
MQCPI078 Route 1418 ready for connection requests
MQCPI006 Route 1415 has started and will forward messages to :
MQCPI034 ....mqipt.company2.com(1415)
MQCPI035 ....using MQ protocols
MQCPI036 ....SSL Client side enabled with properties :
MQCPI031 ......cipher suites <null>
MQCPI032 ......keyring file c:\mqipt\KeyMan.pfx
MQCPI038 ......distinguished name(s) CN=*Doe O=IBM OU=* L=* ST=* C=*
MQCPI078 Route 1415 ready for connection requests
```

mqipt 홈 디렉토리의 다음 서브디렉토리는 MQIPT가 처음으로 호출될 때 자동으로 작성됩니다.

- "logs" 디렉토리는 연결 로그가 보존되는 디렉토리입니다.
- "오류" 디렉토리는 FFST™(First Failure Support Technology™) 및 추적 레코드가 기록되는 디렉토리입니다.

명령 행에서 관리 클라이언트 시작

명령 프롬프트를 열어 디렉토리를 bin 디렉토리로 변경하고 mqiptGui를 실행합니다. 예를 들어, 다음과 같습니다.

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

관리 클라이언트가 방화벽을 넘어 MQIPT로 연결될 수 있도록 하려면 SOCKS 프록시를 사용하여 호스트 이름이나 주소 및 포트 번호를 지정하십시오.

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

디폴트 socksPort는 1080입니다.

관리 클라이언트의 상태는 관리 클라이언트의 기본 창에 나타나는 메시지에 의해 표시됩니다.

Windows 서비스 제어 프로그램 사용

MQIPT를 Windows 서비스로 관리하고 시작할 수 있도록 허용하기 위해 별도의 서비스 제어 프로그램인 mqiptservice.exe가 제공됩니다.

mqiptservice.exe는 다음과 같은 명령 행 인수를 사용합니다.

mqiptservice -install *path*
서비스를 설치하고 등록하여 매뉴얼 서비스로 Windows 서비스 패널에 표시합니다. 서비스 패널로 가서 설정을 "자동"으로 변경하여 시스템이 시작될 때 MQIPT가 자동으로 시작되도록 하십시오. 이 서비스를 설치한 후에는 Windows를 다시 시동해야 합니다. 경로 매개변수는 반드시 제공해야 하며 mqipt.conf 구성 파일을 포함한 디렉토리에 대한 완전한 경로입니다. 이름에 공백이 있으면 이름 주위에 인용 부호를 넣으십시오.

mqiptservice -remove
서비스를 제거하여 서비스 패널에 표시되지 않도록 합니다.

mqiptservice ?
올바른 인수를 나열하는 영어(미국) 도움말 메시지를 표시합니다.

동일한 명령에 설치와 제거를 모두 지정하면 오류가 발생합니다.

Windows는 내부적으로 인수 없이 mqiptservice 프로그램을 호출합니다. 인수 없이 명령 행에서 프로그램을 호출하면 프로그램이 시간 종료되고 오류를 반환합니다.

MQIPT 서비스가 시작될 때 모든 활성 MQIPT 라우트가 시동됩니다. 또한 정지되면 모든 라우트가 즉시 종료됩니다.

주: 시스템 PATH 환경 변수는 반드시 JNI 런타임 라이브러리의 위치를 포함해야 합니다. jvm.dll 파일은 JDK의 클라이언트 서브디렉토리에서 찾을 수 있습니다.

internet pass-thru를 Windows 서비스로 설치 제거

먼저 Windows 서비스 패널에서 MQIPT를 정지함으로써 MQIPT를 서비스로 설치 제거할 수 있습니다. 그런 다음, 명령 프롬프트를 열고 MQIPT의 bin 서브디렉토리로 가서 다음을 입력합니다.

```
mqiptservice -remove
```

internet pass-thru 설치 제거

시스템에서 MQIPT를 설치 제거하기 전에 앞에서 설명한 대로 Windows 서비스로 제거하십시오. 그런 다음, Windows 시작 메뉴에서 설치 제거 프로세스를 실행하십시오.

제 14 장 Sun Solaris에 internet pass-thru 설치

이 장에서는 Sun Solaris 시스템에 MQIPT를 설치하는 방법을 설명합니다.

파일 다운로드 및 설치

MQIPT는 다음 주소의 WebSphere MQ SupportPac 웹 페이지에서 다운로드됩니다.

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

다운로드하려면 다음 지시사항을 따르십시오.

root로 로그인하여 ms81_sol.tar.Z를 임시 디렉토리로 압축 해제하십시오. 다음 예에서와 같이 pkgadd 명령을 실행하십시오.

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

예에서는 ms81_sol.tar.Z가 /tmp 디렉토리에 있다고 가정합니다.

MQIPT에는 관리 클라이언트 GUI용 파일을 포함하여 다음 표에 표시된 파일이 들어 있습니다.

파일	용도
Readme.txt	책에 포함되지 않은 최신 정보
mqiptSample.conf	샘플 구성 파일
ssl/sslSample.pfx	테스트 키 링 파일
ssl/sslSample.pwd	테스트 키 링 파일용 암호
ssl/sslCAdefault.pfx	샘플 인증 권한(CA) 키 링 파일
ssl/sslCAdefault.pwd	샘플 CA 키 링 파일용 암호 파일
ssl/KeyMan.zip	KeyMan 유틸리티
exits/ SampleOneRouteExit.java	샘플 보안 엑시트
exits/ SampleOneRouteExit.conf	SampleOneRouteExit용 구성 파일

파일	용도
exits/SampleRoutingExit.java	샘플 보안 엑시트
exits/SampleRoutingExit.conf	SampleRoutingExit용 구성 파일
exits/SampleSecurityExit.java	샘플 보안 엑시트
lib/MQipt.jar	런타임, 클래스 및 등록 정보 파일 포함
lib/ADV_mqipt_normal. class	"정상" 모드에 대한 Network Dispatcher advisor
lib/ADV_mqipt_replace. class	"바꾸기" 모드에 대한 Network Dispatcher advisor
lib/mqipt1414Sample.ssl	Network Dispatcher advisor에 대한 샘플 트리거 파일
bin/mqipt	명령 행에서 MQIPT 실행에 대한 바로 가기
bin/mqiptAdmin	MQIPT 정지 및 파일 정보 새로 고침에 대한 바로 가기
bin/mqiptPW	키 링 파일을 여는 데 사용되는 암호 암호화
bin/mqiptVersion	MQIPT의 버전 번호 표시
bin/mqiptService	MQIPT를 설치하여 시스템 시동 시에 자동으로 시작되도록 함
bin/mqiptEnv	mqipt.jar 파일의 위치 정의 및 다른 스크립트에 의해서만 사용되는지 여부 결정
web/MQIPTServlet.war	servlet 버전용 웹 보존 파일
doc/<lang>/html/ <filename>.zip	HTML 형식의 *internet pass-thru* 매뉴얼에 대한 마스터 파일. 소프트카피 문서에 대한 자세한 정보는 191 페이지의 『참고 문헌』을 참조하십시오.
lib/guiadmin.jar	관리 클라이언트 GUI에 대한 런타임, 클래스 및 등록 정보 파일 포함
bin/mqiptGui	명령 행에서 관리 클라이언트 GUI 실행에 대한 바로 가기
bin/customSample. properties	관리 클라이언트의 화면 및 액세스 가능성을 사용자 정의하는 샘플 파일

internet pass-thru 설정

처음으로 MQIPT를 시작하기 전에 샘플 구성 파일인 mqiptSample.conf를 mqipt.conf로 복사하십시오. 자세한 정보는 75 페이지의 제 19 장 『internet pass-thru 관리 및 구성』을 참조하십시오.

명령 행에서 internet pass-thru 시작

root로 로그인하고 디렉토리를 bin 디렉토리로 변경합니다. 예를 들어, 다음과 같습니다.

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

옵션 없이 mqipt 스크립트를 실행하면 구성 파일(mqipt.conf)에 대해 "."의 디폴트 위치를 사용합니다. 다른 위치를 지정하려면 다음과 같이 하십시오.

```
mqipt <directory name>
```

MQIPT의 상태를 나타내는 메시지가 콘솔에 표시됩니다. 오류가 발생한 경우에는 161 페이지의 『문제점 판별』을 참조하십시오. MQIPT가 성공적으로 시작되면, 예를 들어 다음과 같은 메시지가 표시됩니다.

```
5639-L92 (C) Copyright IBM Corp. 2000, 2003 All Rights Reserved
MQCPI001 WebSphere MQ internet pass-thru Version 1.3.0 starting
MQCPI004 Reading configuration information from /opt/mqipt/mqipt.conf
MQCPI008 Listening for control commands on port 1881
MQCPI011 The path /opt/mqipt/logs will be used to store the log files
MQCPI006 Route 1418 has started and will forward messages to :
MQCPI034 ....mqserver.company4.com(1414)
MQCPI035 ....using MQ protocols
MQCPI078 Route 1418 ready for connection requests
MQCPI006 Route 1415 has started and will forward messages to :
MQCPI034 ....mqipt.company2.com(1415)
MQCPI035 ....using MQ protocols
MQCPI036 ....SSL Client side enabled with properties :
MQCPI031 ......cipher suites <null>
MQCPI032 ......keyring file /opt/mqipt/KeyMan.pfx
MQCPI038 ......distinguished name(s) CN=*Doe O=IBM OU=* L=* ST=* C=*
MQCPI078 Route 1415 ready for connection requests
```

mqipt 홈 디렉토리의 다음 서브디렉토리는 MQIPT가 처음으로 호출될 때 자동으로 작성됩니다.

- "logs" 디렉토리는 연결 로그가 보존되는 디렉토리입니다.
- "오류" 디렉토리는 FFST(First Failure Support Technology) 및 추적 레코드가 기록되는 디렉토리입니다.

자동으로 internet pass-thru 시작

시스템에 시작될 때 자동으로 MQIPT가 시작되도록 하려면 mqiptService 스크립트를 실행하십시오. 예를 들어, 다음과 같습니다.

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

MQIPT가 자동으로 시작되는 것을 금지하려면 다음과 같이 하십시오.

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

명령 행에서 관리 클라이언트 시작

명령 프롬프트를 열어 디렉토리를 bin 디렉토리로 변경하고 mqiptGui를 실행합니다. 예를 들어, 다음과 같습니다.

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

관리 클라이언트가 방화벽을 넘어 MQIPT로 연결될 수 있도록 하려면 호스트 이름이나 주소 및 포트 번호를 지정하십시오.

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

디폴트 socksPort는 1080입니다.

관리 클라이언트의 상태는 관리 클라이언트의 기본 창에 나타나는 메시지에 의해 표시됩니다.

internet pass-thru 설치 제거

시스템에서 MQIPT를 설치 해제하기 전에 57 페이지의 『자동으로 internet pass-thru 시작』에서 설명한 대로 자동으로 시작되는 것을 방지하십시오. root로 로그인하고 pkgrm 명령을 실행하십시오.

```
pkgrm mqipt
```

제 15 장 AIX에 internet pass-thru 설치

이 장에서는 AIX 시스템에 MQIPT를 설치하는 방법을 설명합니다.

파일 다운로드 및 설치

MQIPT는 다음 주소의 WebSphere MQ SupportPac 웹 페이지에서 다운로드됩니다.

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

다운로드하려면 다음 지시사항을 따르십시오.

root로 로그인하여 ms81_aix.tar.Z의 압축을 풀고 임시 디렉토리로 압축 해제하십시오. 다음 예에서와 같이 installp 명령을 실행하십시오.

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

예에서는 ms81_aix.tar.Z가 /tmp 디렉토리에 있다고 가정합니다.

MQIPT에는 관리 클라이언트 GUI용 파일을 포함하여 다음 표에 표시된 파일이 들어 있습니다.

파일	용도
Readme.txt	책에 포함되지 않은 최신 정보
mqiptSample.conf	샘플 구성 파일
ssl/sslSample.pfx	테스트 키 링 파일
ssl/sslSample.pwd	테스트 키 링 파일용 암호
ssl/sslCAdefault.pfx	샘플 인증 권한(CA) 키 링 파일
ssl/sslCAdefault.pwd	샘플 CA 키 링 파일용 암호 파일
ssl/KeyMan.zip	KeyMan 유틸리티
exits/ SampleOneRouteExit.java	샘플 보안 엑시트
exits/ SampleOneRouteExit.conf	SampleOneRouteExit용 구성 파일
exits/SampleRoutingExit.java	샘플 보안 엑시트

파일	용도
exits/SampleRoutingExit.conf	SampleRoutingExit용 구성 파일
exits/SampleSecurityExit.java	샘플 보안 엑시트
lib/MQipt.jar	런타임, 클래스 및 등록 정보 파일 포함
lib/ADV_mqipt_normal. class	"정상" 모드에 대한 Network Dispatcher advisor
lib/ADV_mqipt_replace. class	"바꾸기" 모드에 대한 Network Dispatcher advisor
lib/mqipt1414Sample.ssl	Network Dispatcher advisor에 대한 샘플 트리거 파일
bin/mqipt	명령 행에서 MQIPT 실행에 대한 바로 가기
bin/mqiptAdmin	MQIPT 정지 및 파일 정보 새로 고침에 대한 바로 가기
bin/mqiptPW	키 링 파일을 여는 데 사용되는 암호 암호화
bin/mqiptVersion	MQIPT의 버전 번호 표시
bin/mqiptService	MQIPT를 설치하여 시스템 시동 시에 자동으로 시작되도록 함
bin/mqiptEnv	mqipt.jar 파일의 위치 정의 및 다른 스크립트에 의해서만 사용되는지 여부 결정
web/MQIPTServlet.war	servlet 버전용 웹 보존 파일
doc/<lang>/html/ <filename>.zip	HTML 형식의 *internet pass-thru* 매뉴얼에 대한 마스터 파일. 소프트카피 문서에 대한 자세한 정보는 191 페이지의 『참고 문헌』을 참조하십시오.
lib/guiadmin.jar	관리 클라이언트 GUI에 대한 런타임, 클래스 및 등록 정보 파일 포함
bin/mqiptGui	명령 행에서 관리 클라이언트 실행에 대한 바로 가기
bin/customSample. properties	관리 클라이언트의 화면 및 액세스 가능성을 사용자 정의하는 샘플 파일

internet pass-thru 설정

처음으로 MQIPT를 시작하기 전에 샘플 구성 파일인 mqiptSample.conf를 mqipt.conf로 복사하십시오. 자세한 정보는 75 페이지의 제 19 장 『internet pass-thru 관리 및 구성』을 참조하십시오.

명령 행에서 internet pass-thru 시작

root로 로그인하고 디렉토리를 bin 디렉토리로 변경합니다. 예를 들어, 다음과 같습니다.

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

옵션 없이 mqipt 스크립트를 실행하면 구성 파일(mqipt.conf)에 대해 "."의 디폴트 위치를 사용합니다. 다른 위치를 지정하려면 다음과 같이 하십시오.

```
mqipt <directory name>
```

MQIPT의 상태를 나타내는 메시지가 콘솔에 표시됩니다. 오류가 발생한 경우에는 161 페이지의 『문제점 판별』을 참조하십시오. MQIPT가 성공적으로 시작되면, 예를 들어 다음과 같은 메시지가 표시됩니다.

```
5639-L92 (C) Copyright IBM Corp. 2000, 2003 All Rights Reserved
MQCPI001 WebSphere MQ internet pass-thru Version 1.3.0 starting
MQCPI004 Reading configuration information from /usr/opt/mqipt/mqipt.conf
MQCPI008 Listening for control commands on port 1881
MQCPI011 The path /usr/opt/mqipt/logs will be used to store the log files
MQCPI006 Route 1418 has started and will forward messages to :
MQCPI034 ....mqserver.company4.com(1414)
MQCPI035 ....using MQ protocols
MQCPI078 Route 1418 ready for connection requests
MQCPI006 Route 1415 has started and will forward messages to :
MQCPI034 ....mqipt.company2.com(1415)
MQCPI035 ....using MQ protocols
MQCPI036 ....SSL Client side enabled with properties :
MQCPI031 ......cipher suites <null>
MQCPI032 ......keyring file /usr/opt/mqipt/KeyMan.pfx
MQCPI038 ......distinguished name(s) CN=*Doe O=IBM OU=* L=* ST=* C=*
MQCPI078 Route 1415 ready for connection requests
```

mqipt 홈 디렉토리의 다음 서브디렉토리는 MQIPT가 처음으로 호출될 때 자동으로 작성됩니다.

- "logs" 디렉토리는 연결 로그가 보존되는 디렉토리입니다.
- "오류" 디렉토리는 FFST(First Failure Support Technology) 및 추적 레코드가 기록되는 디렉토리입니다.

자동으로 internet pass-thru 시작

시스템에 시작될 때 자동으로 MQIPT가 시작되도록 하려면 mqiptService 스크립트를 실행하여 inittab에 항목을 추가하십시오. 예를 들어, 다음과 같습니다.

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

MQIPT가 자동으로 시작되는 것을 금지하려면 inittab에서 해당 항목을 제거하십시오.

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

명령 행에서 관리 클라이언트 시작

명령 프롬프트를 열어 디렉토리를 bin 디렉토리로 변경하고 mqiptGui를 실행합니다. 예를 들어, 다음과 같습니다.

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

관리 클라이언트가 방화벽을 넘어 MQIPT로 연결될 수 있도록 하려면 호스트 이름이나 주소 및 포트 번호를 지정하십시오.

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

디폴트 socksPort는 1080입니다.

관리 클라이언트의 상태는 관리 클라이언트의 기본 창에 나타나는 메시지에 의해 표시됩니다.

internet pass-thru 설치 제거

시스템에서 MQIPT를 설치 제거하기 전에 61 페이지의 『자동으로 internet pass-thru 시작』에서 설명한 대로 자동으로 시작되는 것을 방지하십시오. root로 로그인하고 installp 명령을 실행하십시오.

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

제 16 장 HP-UX에 internet pass-thru 설치

이 장에서는 HP-UX 시스템에 MQIPT를 설치하는 방법을 설명합니다.

파일 다운로드 및 설치

MQIPT는 다음 주소의 WebSphere MQ SupportPac 웹 페이지에서 다운로드됩니다.

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

다운로드하려면 다음 지시사항을 따르십시오.

root로 로그인하여 ms81_hp11.tar.Z 임시 디렉토리로 압축 해제하십시오. 다음 예에서와 같이 swinstall 명령을 실행하십시오.

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

예에서는 ms81_hp11.tar.Z가 /tmp 디렉토리에 있다고 가정합니다.

MQIPT에는 관리 클라이언트 GUI용 파일을 포함하여 다음 표에 표시된 파일이 들어 있습니다.

파일	용도
Readme.txt	책에 포함되지 않은 최신 정보
mqiptSample.conf	샘플 구성 파일
ssl/sslSample.pfx	테스트 키 링 파일
ssl/sslSample.pwd	테스트 키 링 파일용 암호
ssl/sslCAdefault.pfx	샘플 인증 권한(CA) 키 링 파일
ssl/sslCAdefault.pwd	샘플 CA 키 링 파일용 암호 파일
ssl/KeyMan.zip	KeyMan 유틸리티
exits/ SampleOneRouteExit.java	샘플 보안 엑시트
exits/ SampleOneRouteExit.conf	SampleOneRouteExit용 구성 파일

파일	용도
exits/SampleRoutingExit.java	샘플 보안 엑시트
exits/SampleRoutingExit.conf	SampleRoutingExit용 구성 파일
exits/SampleSecurityExit.java	샘플 보안 엑시트
lib/MQipt.jar	런타임, 클래스 및 등록 정보 파일 포함
lib/ADV_mqipt_normal. class	"정상" 모드에 대한 Network Dispatcher advisor
lib/ADV_mqipt_replace. class	"바꾸기" 모드에 대한 Network Dispatcher advisor
lib/mqipt1414Sample.ssl	Network Dispatcher advisor에 대한 샘플 트리거 파일
bin/mqipt	명령 행에서 MQIPT 실행으로 바로 가기
bin/mqiptAdmin	MQIPT 정지 및 파일 정보 새로 고침으로 바로 가기
bin/mqiptPW	키 링 파일을 여는 데 사용되는 암호 암호화
bin/mqiptVersion	MQIPT의 버전 번호 표시
bin/mqiptService	MQIPT를 설치하여 시스템 시동 시에 자동으로 시작되도록 함
bin/mqiptEnv	mqipt.jar 파일의 위치 정의 및 다른 스크립트에 의해서만 사용되는지 여부 결정
bin/mqiptFork	시스템을 시동하는 도중에 MQIPT를 시작하는 데 사용됨
web/MQIPTServlet.war	servlet 버전용 웹 보존 파일
doc/<lang>/html/ <filename>.zip	HTML 형식의 *internet pass-thru* 매뉴얼에 대한 마스터 파일. 소프트카피 문서에 대한 자세한 정보는 191 페이지의 『참고 문헌』을 참조하십시오.
lib/guiadmin.jar	관리 클라이언트 GUI에 대한 런타임, 클래스 및 등록 정보 파일 포함
bin/mqiptGui	명령 행에서 관리 클라이언트 GUI 실행에 대한 바로 가기
bin/customSample. properties	관리 클라이언트의 화면 및 액세스 가능성을 사용자 정의하는 샘플 파일

internet pass-thru 설정

처음으로 MQIPT를 시작하기 전에 샘플 구성 파일인 mqiptSample.conf를 mqipt.conf로 복사하십시오. 자세한 정보는 75 페이지의 제 19 장 『internet pass-thru 관리 및 구성』을 참조하십시오.

명령 행에서 internet pass-thru 시작

root로 로그인하고 디렉토리를 bin 디렉토리로 변경합니다. 예를 들어, 다음과 같습니다.

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

옵션 없이 mqipt 스크립트를 실행하면 구성 파일(mqipt.conf)에 대해 "."의 디폴트 위치를 사용합니다. 다른 위치를 지정하려면 다음과 같이 하십시오.

```
mqipt <directory name>
```

MQIPT의 상태를 나타내는 메시지가 콘솔에 표시됩니다. 오류가 발생한 경우에는 161 페이지의 『문제점 판별』을 참조하십시오. MQIPT가 성공적으로 시작되면, 예를 들어 다음과 같은 메시지가 표시됩니다.

```
5639-L92 (C) Copyright IBM Corp. 2000, 2003 All Rights Reserved
MQCPI001 WebSphere MQ internet pass-thru Version 1.3.0 starting
MQCPI004 Reading configuration information from /opt/mqipt/mqipt.conf
MQCPI008 Listening for control commands on port 1881
MQCPI011 The path /opt/mqipt/logs will be used to store the log files
MQCPI006 Route 1418 has started and will forward messages to :
MQCPI034 ....mqserver.company4.com(1414)
MQCPI035 ....using MQ protocols
MQCPI078 Route 1418 ready for connection requests
MQCPI006 Route 1415 has started and will forward messages to :
MQCPI034 ....mqipt.company2.com(1415)
MQCPI035 ....using MQ protocols
MQCPI036 ....SSL Client side enabled with properties :
MQCPI031 ......cipher suites <null>
MQCPI032 ......keyring file /opt/mqipt/KeyMan.pfx
MQCPI038 ......distinguished name(s) CN=*Doe O=IBM OU=* L=* ST=* C=*
MQCPI078 Route 1415 ready for connection requests
```

mqipt 홈 디렉토리의 다음 서브디렉토리는 MQIPT가 처음으로 호출될 때 자동으로 작성됩니다.

- "logs" 디렉토리는 연결 로그가 보존되는 디렉토리입니다.
- "오류" 디렉토리는 FFST(First Failure Support Technology) 및 추적 레코드가 기록되는 디렉토리입니다.

자동으로 internet pass-thru 시작

시스템에 시작될 때 자동으로 MQIPT가 시작되도록 하려면 mqiptService 스크립트를 실행하십시오. 예를 들어, 다음과 같습니다.

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

여기서는 JDK 1.4가 이미 /opt/java1.4라는 디렉토리에 설치되어 있다고 가정합니다. 설치되어 있지 않은 경우라면 mqipt.ske 파일을 편집하여 PATH 변수가 JDK의 위치를 가리키도록 변경하십시오. mqiptService -install 명령을 실행하기 전에 반드시 변경 사항을 적용해야 합니다.

MQIPT가 서비스로 시작될 때 console.log 파일을 logs 서브디렉토리로 기록합니다. 이 서브디렉토리는 MQIPT가 처음으로 실행될 때 작성되므로 MQIPT를 서비스로 시작하려고 시도하기 전에 최소한 한 번은 MQIPT를 시작해야 합니다.

MQIPT가 자동으로 시작되는 것을 금지하려면 다음과 같이 하십시오.

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

명령 행에서 관리 클라이언트 시작

명령 프롬프트를 열어 디렉토리를 bin 디렉토리로 변경하고 mqiptGui를 실행합니다. 예를 들어, 다음과 같습니다.

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

관리 클라이언트가 방화벽을 넘어 MQIPT로 연결될 수 있도록 하려면 호스트 이름이나 주소 및 포트 번호를 지정하십시오.

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

디폴트 socksPort는 1080입니다.

관리 클라이언트의 상태는 관리 클라이언트의 기본 창에 나타나는 메시지에 의해 표시됩니다.

internet pass-thru 설치 제거

시스템에서 MQIPT를 설치 제거하기 전에 65 페이지의 『자동으로 internet pass-thru 시작』에서 설명한 대로 자동으로 시작되는 것을 방지하십시오. root로 로그인하고 swremove 명령을 실행하십시오.

```
swremove MQIPT
```

제 17 장 Linux에 internet pass-thru 설치

이 장에서는 Linux 시스템에 MQIPT를 설치하는 방법을 설명합니다.

파일 다운로드 및 설치

MQIPT는 다음 주소의 WebSphere MQ SupportPac 웹 페이지에서 다운로드됩니다.

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

다운로드하려면 다음 지시사항을 따르십시오.

root로 로그인하여 ms81_linux.tar.z를 임시 디렉토리로 압축 해제하십시오. 다음 예에서와 같이 rpm 명령을 실행하십시오.

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

예에서는 ms81_linux.tar.z가 /tmp 디렉토리에 있다고 가정합니다.

MQIPT에는 관리 클라이언트 GUI용 파일을 포함하여 다음 표에 표시된 파일이 들어 있습니다.

파일	용도
Readme.txt	책에 포함되지 않은 최신 정보
mqiptSample.conf	샘플 구성 파일
ssl/sslSample.pfx	테스트 키 링 파일
ssl/sslSample.pwd	테스트 키 링 파일용 암호
ssl/sslCAdefault.pfx	샘플 인증 권한(CA) 키 링 파일
ssl/sslCAdefault.pwd	샘플 CA 키 링 파일용 암호 파일
ssl/KeyMan.zip	KeyMan 유틸리티
exits/ SampleOneRouteExit.java	샘플 보안 엑시트
exits/ SampleOneRouteExit.conf	SampleOneRouteExit용 구성 파일

파일	용도
exits/SampleRoutingExit.java	샘플 보안 엑시트
exits/SampleRoutingExit.conf	SampleRoutingExit용 구성 파일
exits/SampleSecurityExit.java	샘플 보안 엑시트
lib/libmqiptqos.so	TQoS용 더미 라이브러리
bin/mqiptQoS	실제 TQoS 라이브러리 사용
lib/MQipt.jar	런타임, 클래스 및 등록 정보 파일 포함
lib/ADV_mqipt_normal. class	"정상" 모드에 대한 Network Dispatcher advisor
lib/ADV_mqipt_replace. class	"바꾸기" 모드에 대한 Network Dispatcher advisor
lib/mqipt1414Sample.ssl	Network Dispatcher advisor에 대한 샘플 트리거 파일
lib/libiptqos.so	Quality of Service 지원에 필요한 런타임 라이브러리
bin/mqipt	명령 행에서 MQIPT 실행으로 바로 가기
bin/mqiptAdmin	MQIPT 정지 및 파일 정보 새로 고침으로 바로 가기
bin/mqiptPW	키 링 파일을 여는 데 사용되는 암호 암호화
bin/mqiptVersion	MQIPT의 버전 번호 표시
bin/mqiptService	MQIPT를 설치하여 시스템 시동 시에 자동으로 시작되도록 함
bin/mqiptEnv	`mqipt.jar` 파일의 위치 정의 및 다른 스크립트에 의해서만 사용되는지 여부 결정
web/MQIPTServlet.war	servlet 버전용 웹 보존 파일
doc/<lang>/html/ <filename>.zip	HTML 형식의 *internet pass-thru* 매뉴얼에 대한 마스터 파일. 소프트카피 문서에 대한 자세한 정보는 191 페이지의 『참고 문헌』을 참조하십시오.
lib/guiadmin.jar	관리 클라이언트 GUI에 대한 런타임, 클래스 및 등록 정보 파일 포함
bin/mqiptGui	명령 행에서 관리 클라이언트 GUI 실행에 대한 바로 가기
bin/customSample. properties	관리 클라이언트의 화면 및 액세스 가능성을 사용자 정의하는 샘플 파일

internet pass-thru 설정

처음으로 MQIPT를 시작하기 전에 샘플 구성 파일인 `mqiptSample.conf`를 `mqipt.conf`로 복사하십시오. 자세한 정보는 75 페이지의 제 19 장 『internet pass-thru 관리 및 구성』을 참조하십시오.

명령 행에서 internet pass-thru 시작

`root`로 로그인하고 디렉토리를 `bin` 디렉토리로 변경합니다. 예를 들어, 다음과 같습니다.

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

옵션 없이 `mqipt` 스크립트를 실행하면 구성 파일(`mqipt.conf`)에 대해 "."의 디폴트 위치를 사용합니다. 다른 위치를 지정하려면 다음과 같이 하십시오.

```
mqipt <directory name>
```

MQIPT의 상태를 나타내는 메시지가 콘솔에 표시됩니다. 오류가 발생한 경우에는 161 페이지의 『문제점 판별』을 참조하십시오. MQIPT가 성공적으로 시작되면, 예를 들어 다음과 같은 메시지가 표시됩니다.

```
5639-L92 (C) Copyright IBM Corp. 2000, 2003 All Rights Reserved
MQCPI001 WebSphere MQ internet pass-thru Version 1.3.0 starting
MQCPI004 Reading configuration information from /opt/mqipt/mqipt.conf
MQCPI008 Listening for control commands on port 1881
MQCPI011 The path /opt/mqipt/logs will be used to store the log files
MQCPI006 Route 1418 has started and will forward messages to :
MQCPI034 ....mqserver.company4.com(1414)
MQCPI035 ....using MQ protocols
MQCPI078 Route 1418 ready for connection requests
MQCPI006 Route 1415 has started and will forward messages to :
MQCPI034 ....mqipt.company2.com(1415)
MQCPI035 ....using MQ protocols
MQCPI036 ....SSL Client side enabled with properties :
MQCPI031 ......cipher suites <null>
MQCPI032 ......keyring file /opt/mqipt/KeyMan.pfx
MQCPI038 ......distinguished name(s) CN=*Doe O=IBM OU=* L=* ST=* C=*
MQCPI078 Route 1415 ready for connection requests
```

mqipt 홈 디렉토리의 다음 서브디렉토리는 MQIPT가 처음으로 호출될 때 자동으로 작성됩니다.

- "logs" 디렉토리는 연결 로그가 보존되는 디렉토리입니다.
- "오류" 디렉토리는 FFST(First Failure Support Technology) 및 추적 레코드가 기록되는 디렉토리입니다.

자동으로 internet pass-thru 시작

시스템에 시작될 때 자동으로 MQIPT가 시작되도록 하려면 mqiptService 스크립트를 실행하십시오. 예를 들어, 다음과 같습니다.

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

MQIPT가 서비스로 시작될 때 console.log 파일을 logs 서브디렉토리로 기록합니다. 이 서브디렉토리는 MQIPT가 처음으로 실행될 때 작성되므로 MQIPT를 서비스로 시작하려고 시도하기 전에 최소한 한 번은 MQIPT를 시작해야 합니다.

MQIPT가 자동으로 시작되는 것을 금지하려면 다음과 같이 하십시오.

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

명령 행에서 관리 클라이언트 시작

명령 프롬프트를 열어 디렉토리를 bin 디렉토리로 변경하고 mqiptGui를 실행합니다. 예를 들어, 다음과 같습니다.

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

관리 클라이언트가 방화벽을 넘어 MQIPT로 연결될 수 있도록 하려면 호스트 이름이나 주소 및 포트 번호를 지정하십시오.

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

디폴트 socksPort는 1080입니다.

관리 클라이언트의 상태는 관리 클라이언트의 기본 창에 나타나는 메시지에 의해 표시됩니다.

internet pass-thru 설치 제거

시스템에서 MQIPT를 설치 제거하기 전에 69 페이지의 『자동으로 internet pass-thru 시작』에서 설명한 대로 자동으로 시작되는 것을 방지하십시오. root로 로그인하고 swremove 명령을 실행하십시오.

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

제 18 장 일반 UNIX 설치

모든 공용 MQIPT 파일의 디스크 이미지는 일반적으로 사용할 수 있도록 tar 파일로 제공됩니다. 이 파일의 목적은 고유한 설치 이미지를 사용하는 MQIPT에서 지원하지 않는 UNIX 플랫폼에 MQIPT가 설치되도록 허용하는 것입니다. 또한 지정된 위치에 tar 파일을 압축 해제하고 약간의 변경에 따라 Java 1.4를 지원하는 플랫폼에 MQIPT를 구현할 수 있게 하는 것입니다. 설치된 파일의 위치를 나타내기 위해 bin 서브디렉토리에 있는 mqiptEnv 스크립트를 변경해야 할 수 있습니다.

- 『파일 다운로드 및 설치』
- 72 페이지의 『internet pass-thru 설정』
- 73 페이지의 『명령 행에서 internet pass-thru 시작』
- 74 페이지의 『자동으로 internet pass-thru 시작』
- 74 페이지의 『명령 행에서 관리 클라이언트 시작』
- 74 페이지의 『internet pass-thru 설치 제거』

파일 다운로드 및 설치

MQIPT는 다음 주소의 WebSphere MQ SupportPac 웹 페이지에서 다운로드됩니다.

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

다운로드하려면 다음 지시사항을 따르십시오.

다음 예와 같이 루트로 로그인하고 대상 디렉토리에 ms81.tar를 압축 해제하십시오.

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

예에서는 ms81.tar가 /tmp 디렉토리로 다운로드되었다고 가정합니다.

MQIPT에는 관리 클라이언트 GUI용 파일을 포함하여 다음 표에 표시된 파일이 들어 있습니다.

파일	용도
Readme.txt	책에 포함되지 않은 최신 정보
mqiptSample.conf	샘플 구성 파일
ssl/sslSample.pfx	테스트 키 링 파일
ssl/sslSample.pwd	테스트 키 링 파일용 암호

파일	용도
ssl/sslCAdefault.pfx	샘플 인증 권한(CA) 키 링 파일
ssl/sslCAdefault.pwd	샘플 CA 키 링 파일용 암호 파일
ssl/KeyMan.zip	KeyMan 유틸리티
exits/ SampleOneRouteExit.java	샘플 보안 엑시트
exits/ SampleOneRouteExit.conf	SampleOneRouteExit용 구성 파일
exits/SampleRoutingExit.java	샘플 보안 엑시트
exits/SampleRoutingExit.conf	SampleRoutingExit용 구성 파일
exits/SampleSecurityExit.java	샘플 보안 엑시트
lib/MQipt.jar	런타임, 클래스 및 등록 정보 파일 포함
lib/ADV_mqipt_normal. class	"정상" 모드에 대한 Network Dispatcher advisor
lib/ADV_mqipt_replace. class	"바꾸기" 모드에 대한 Network Dispatcher advisor
lib/mqipt1414Sample.ssl	Network Dispatcher advisor에 대한 샘플 트리거 파일
bin/mqipt	명령 행에서 MQIPT 실행으로 바로 가기
bin/mqiptAdmin	MQIPT 정지 및 파일 정보 새로 고침으로 바로 가기
bin/mqiptPW	키 링 파일을 여는 데 사용되는 암호 암호화
bin/mqiptVersion	MQIPT의 버전 번호 표시
bin/mqiptService	MQIPT를 설치하여 시스템 시동 시에 자동으로 시작되도록 함
bin/mqiptEnv	`mqipt.jar` 파일의 위치 정의 및 다른 스크립트에 의해서만 사용되는지 여부 결정
web/MQIPTServlet.war	servlet 버전용 웹 보존 파일
doc/<lang>/html/ <filename>.zip	HTML 형식의 *internet pass-thru* 매뉴얼에 대한 마스터 파일. 소프트카피 문서에 대한 자세한 정보는 191 페이지의 『참고 문헌』을 참조하십시오.
lib/guiadmin.jar	관리 클라이언트 GUI에 대한 런타임, 클래스 및 등록 정보 파일 포함
bin/mqiptGui	명령 행에서 관리 클라이언트 실행에 대한 바로 가기
bin/customSample. 등록 정보	관리 클라이언트의 화면 및 액세스 가능성을 사용자 정의하는 샘플 파일

internet pass-thru 설정

처음으로 MQIPT를 시작하기 전에 샘플 구성 파일인 `mqiptSample.conf`를 `mqipt.conf`로 복사하십시오. 자세한 정보는 75 페이지의 제 19 장 『internet pass-thru 관리 및 구성』을 참조하십시오.

이 예에서는 MQIPT가 mqipt라는 디렉토리에 압축 해제되는 것으로 간주합니다. mqiptEnv 스크립트를 런타임 라이브러리의 새 위치로 갱신해야 합니다. MQIPT_CP 변수의 디폴트 값은 다음과 같습니다.

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

이 예에서는 다음으로 변경해야 합니다.

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

또한 런타임 스크립트를 사용하기 전에 갱신하고 mqiptEnv 스크립트의 위치에 대한 완전한 경로 이름을 변경해야 합니다. 예를 들어 mqipt 스크립트를 사용하기 전에 먼저 편집하고 Get classpath 뒤의 명령문을 다음에서

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

다음과 같이 변경합니다.

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

명령 행에서 internet pass-thru 시작

root로 로그인하고 디렉토리를 bin 디렉토리로 변경합니다. 예를 들어, 다음과 같습니다.

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

옵션 없이 mqipt 스크립트를 실행하면 구성 파일(mqipt.conf)에 대해 "."의 디폴트 위치를 사용합니다. 다른 위치를 지정하려면 다음과 같이 하십시오.

```
mqipt <directory name>
```

MQIPT의 상태를 나타내는 메시지가 콘솔에 표시됩니다. 오류가 발생한 경우에는 161 페이지의 『문제점 판별』을 참조하십시오. MQIPT가 성공적으로 시작되면, 예를 들어 다음과 같은 메시지가 표시됩니다.

```
5639-L92 (C) Copyright IBM Corp. 2000, 2003 All Rights Reserved
MQCPI001 WebSphere MQ internet pass-thru Version 1.3.0 starting
MQCPI004 Reading configuration information from /mqipt/opt/mqipt/mqipt.conf
MQCPI008 Listening for control commands on port 1881
MQCPI011 The path /mqipt/opt/mqipt/logs will be used to store the log files
MQCPI006 Route 1418 has started and will forward messages to :
MQCPI034 ....mqserver.company4.com(1414)
MQCPI035 ....using MQ protocols
MQCPI078 Route 1418 ready for connection requests
MQCPI006 Route 1415 has started and will forward messages to :
MQCPI034 ....mqipt.company2.com(1415)
MQCPI035 ....using MQ protocols
MQCPI036 ....SSL Client side enabled with properties :
MQCPI031 ......cipher suites <null>
MQCPI032 ......keyring file /mqipt/opt/mqipt/KeyMan.pfx
MQCPI038 ......distinguished name(s) CN=*Doe O=IBM OU=* L=* ST=* C=*
MQCPI078 Route 1415 ready for connection requests
```

mqipt 홈 디렉토리의 다음 서브디렉토리는 MQIPT가 처음으로 호출될 때 자동으로 작성됩니다.

- "logs" 디렉토리는 연결 로그가 보존되는 디렉토리입니다.
- "오류" 디렉토리는 FFST(First Failure Support Technology) 및 추적 레코드가 기록되는 디렉토리입니다.

자동으로 internet pass-thru 시작

서비스 자동 시작은 플랫폼별로 고유합니다. mqiptService 스크립트는 Sun Solaris 시스템에서 수행되는 방법의 한 예로만 제공됩니다. 시스템 요구사항에 따라 플랫폼별 유틸리티를 사용하여 MQIPT를 시스템 서비스로 설치하는 것이 편리할 수 있습니다.

명령 행에서 관리 클라이언트 시작

명령 프롬프트를 열어 디렉토리를 bin 디렉토리로 변경하고 mqiptGui를 실행합니다. 예를 들어, 다음과 같습니다.

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

관리 클라이언트가 방화벽을 넘어 MQIPT로 연결될 수 있도록 하려면 호스트 이름이나 주소 및 포트 번호를 지정하십시오.

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

디폴트 socksPort는 1080입니다.

관리 클라이언트의 상태는 관리 클라이언트의 기본 창에 나타나는 메시지에 의해 표시됩니다.

internet pass-thru 설치 제거

시스템 설치 이미지를 사용해서 MQIPT를 설치하지 않았으므로 설치되어 있는 디렉토리 구조를 삭제하여 MQIPT를 제거할 수 있습니다.

시스템 서비스로 실행되도록 MQIPT를 구성한 경우 먼저 서비스를 제거한 후 코드를 제거하십시오.

제 19 장 internet pass-thru 관리 및 구성

구성 파일인 mqipt.conf를 변경하여 MQIPT를 구성할 수 있습니다. 관리 클라이언트를 사용하여 이러한 작업을 하도록 권장하나 편집기나 기타 사용자의 선택에 따라 다른 방법을 사용할 수도 있습니다. 여기서는 두 가지 기술을 모두 설명하며 관련된 참조 정보를 제공합니다.

- 『internet pass-thru 관리 클라이언트 사용』
- 80 페이지의 『internet pass-thru 행 모드 명령』
- 81 페이지의 『구성 참조 정보』

internet pass-thru 관리 클라이언트 사용

관리 클라이언트를 사용하여 하나 이상의 MQIPT를 구성하고 갱신할 수 있습니다. MQIPT에 대한 전역 등록 정보 및 라우트별 등록 정보를 표시합니다.

Java 1.4는 관리 클라이언트의 필수조건이 아닙니다.

관리 클라이언트에 로컬로 저장된 유일한 데이터는 MQIPT의 목록이며 client.conf라는 파일에 저장됩니다. 전역 및 라우트 등록 정보는 관리 클라이언트에 표시되기 전에 항상 MQIPT에서 검색됩니다.

관리 클라이언트 시작

MQIPT의 서브디렉토리인 bin에 있는 mqiptGui 스크립트를 사용하여 관리 클라이언트를 시작하십시오. 각 플랫폼에서 관리 클라이언트를 설치하는 방법을 보려면 설치에 관한 장을 참조하십시오.

관리 클라이언트가 처음 시작될 때는 대화 상자가 표시되며 MQIPT에 연결 정보를 입력하라는 메시지가 표시됩니다. 필요한 정보는 다음과 같습니다.

MQIPT 이름

이 MQIPT를 설명하는 데 사용되는 이름입니다. 필수적인 정보는 않으나 입력하는 것이 좋습니다.

네트워크 주소

MQIPT가 상주하는 시스템의 주소로서 이름 서버, 점분리 십진수 또는 로컬 호스트(MQIPT가 클라이언트와 동일한 시스템에 있는 경우)로 인식되는 이름입니다.

명령 포트

MQIPT가 명령에 대해 대기하고 있는 포트의 번호입니다.

시간 종료

관리 클라이언트가 MQIPT에 연결하기까지 대기하는 초 수를 나타냅니다. 창의 새로 고침 시간을 줄이기 위해 가능한 한 이 값을 낮게 유지하십시오.

액세스 암호

MQIPT와 통신할 때 사용하는 암호입니다. 암호 확인이 강제 실행인 경우에만 이 필드를 채우십시오(MQIPT 구성 파일에서 AccessPW가 제고되며 널(null) 문자열이 아니면 암호 확인이 강제 실행됩니다).

암호 저장

이 선택란의 왼쪽이 공백이면 세션 지속 기간 또는 MQIPT가 제거될 때까지 암호가 기억됩니다. 선택란이 선택되어 있으면 이후의 세션에 대해 암호가 저장됩니다.

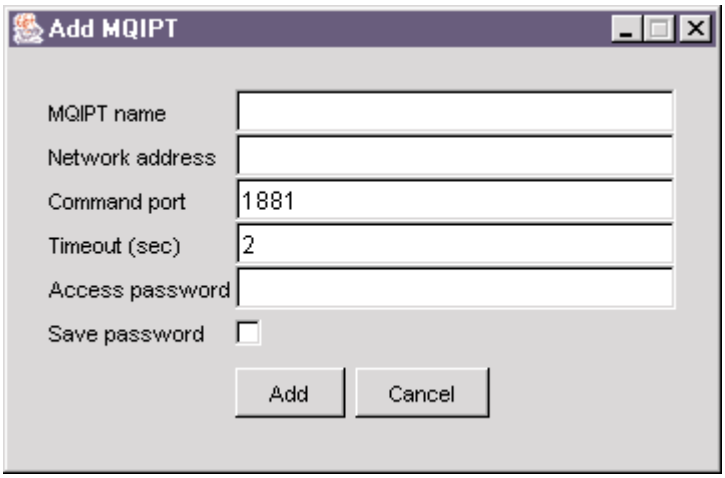

그림 8. MQIPT에 처음 액세스하기 위한 창

MQIPT 관리

한 번에 하나의 MQIPT만을 갱신할 수 있으므로 목록에서 다른 MQIPT를 선택한 경우에는 계속하기 전에 반드시 미해결 변경을 완료해야 합니다. 등록 정보에 대한 변경은 “적용“ 메뉴 옵션을 사용할 때까지 MQIPT에 적용되지 않습니다.

목록에서 MQIPT를 선택하면 MQIPT에서 전역 등록 정보 및 라우트 등록 정보가 검색됩니다. MQIPT가 실행 중이 아니거나 잘못된 CommandPort를 선택한 지정한 경우에는 오류 메시지가 발생됩니다. 호스트 이름과 CommandPort는 “연결” 메뉴 옵션에서 변경할 수 있습니다.

목록에서 MQIPT를 두 번 클릭하면 라우트 목록이 표시됩니다. 라우트를 선택하면 등록 정보가 표시됩니다. 요구사항에 따라 등록 정보를 조정할 수 있습니다.

변경이 적용될 때, 구성 파일에 시간 소인이 생기고 다시 MQIPT로 송신되어 변경이 즉시 적용됩니다. 기존의 모든 주석 행은 손실됩니다.

라우트는 "라우트 추가" 메뉴 옵션을 사용하여 추가할 수 있습니다. 새 라우트에 전역 등록 정보에 의해 정의된 디폴트 등록 정보 설정이 표시됩니다.

등록 정보 상속

관리 클라이언트에서 MQIPT 및 라우트의 등록 정보가 설정되는 계층이 있습니다.

1. 모든 등록 정보에는 디폴트 값이 있으며 구성 파일에서 등록 정보에 대해 언급하지 않거나 사용자가 관리 클라이언트에서 특별히 따로 설정하지 않으면 이 디폴트 값이 적용됩니다.
2. MQIPT에 대해 설정된 전역 등록 정보는 달리 특정한 라우트 정보가 없으면 해당 MQIPT에 대한 모든 라우트에 대해 적용됩니다. 즉, 구성 파일의 추가 등록 정보가 라우트 스탠자에서 설정되지 않은 한 전역 스탠자에서 설정된 등록 정보가 모든 라우트로 전달됩니다. MQIPT에 대해 관리 클라이언트 사용자에 의해 설정된 등록 정보는 라우트에 대해 등록 정보가 특별히 설정되지 않은 한 모든 라우트로 전달됩니다.
3. 디폴트 값과 전역 설정에 상관없이 라우트에 대한 설정은 해당 라우트에서 계속 유지됩니다.

파일 메뉴 옵션

트리 관리에 관련된 대부분의 옵션은 파일 메뉴를 선택할 때 표시됩니다.

MQIPT 추가

75 페이지의 『관리 클라이언트 시작』에서 설명된 것처럼, 클라이언트를 처음 사용할 때 표시되는 것과 동일한 대화 상자를 불러옵니다.

MQIPT 제거

관리 클라이언트 상의 트리에서 현재 강조 표시되어 있는 MQIPT만을 제거합니다. MQIPT의 실행에는 영향을 미치지 않습니다.

구성 저장

트리의 MQIPT 노드를 관리 클라이언트의 구성 파일에 저장하여 다음에 시작될 때 다시 읽을 수 있습니다. MQIPT 노드만 저장됩니다. 전역 및 라우트 등록 정보는 항상 MQIPT에서 검색됩니다.

종료

관리 클라이언트 실행을 정지시킵니다. 그러나 먼저 관리 클라이언트가 트리나 현재 MQIPT가 변경되었는 지 점검하며 하나 또는 둘 다 변경된 경우에는 클라이언트를 저장할 것인지 묻는 메시지를 표시하여 MQIPT 또는 둘 다에 변경 사항을 적용합니다.

MQIPT 메뉴 옵션

연결

MQIPT의 액세스 매개변수를 변경합니다. 변경 사항은 트리 뷰에서 반영됩니다. 75 페이지의 『관리 클라이언트 시작』에서 설명한 것과 유사한 창을 불러옵니다.

암호

리모트 MQIPT의 암호 등록 정보를 변경합니다. 이 조치로 인해 다음 입력을 작성해야 하는 암호 대화 상자가 표시됩니다.

- **현재 암호**: 적절한 사용자인지 점검하기 위해 반드시 암호를 변경하기 전에 현재 암호를 알고 있다는 사실을 증명해야 합니다. 암호 없음이 강제 실행 중이면 이 필드가 공백으로 남습니다.
- **새 암호**: 새 암호를 입력합니다. 이 MQIPT에서 암호 사용을 중단하려면 공백으로 둡니다.
- **새 암호 반복**: 같은 정보를 반복하도록 요청하여 이전 필드에서 잘못 입력하는 것을 방지합니다.
- **암호 저장**: 이 MQIPT의 다른 액세스 등록 정보와 같이 새 암호도 로컬로 저장할 것인지 결정하는 데 사용됩니다.

라우트 추가

선택된 MQIPT에 라우트를 추가합니다. 자세한 내용은 79 페이지의 그림 9를 참조하십시오. 각 라우트에는 반드시 MQIPT에 대한 고유한 ListenerPort가 있어야 합니다.

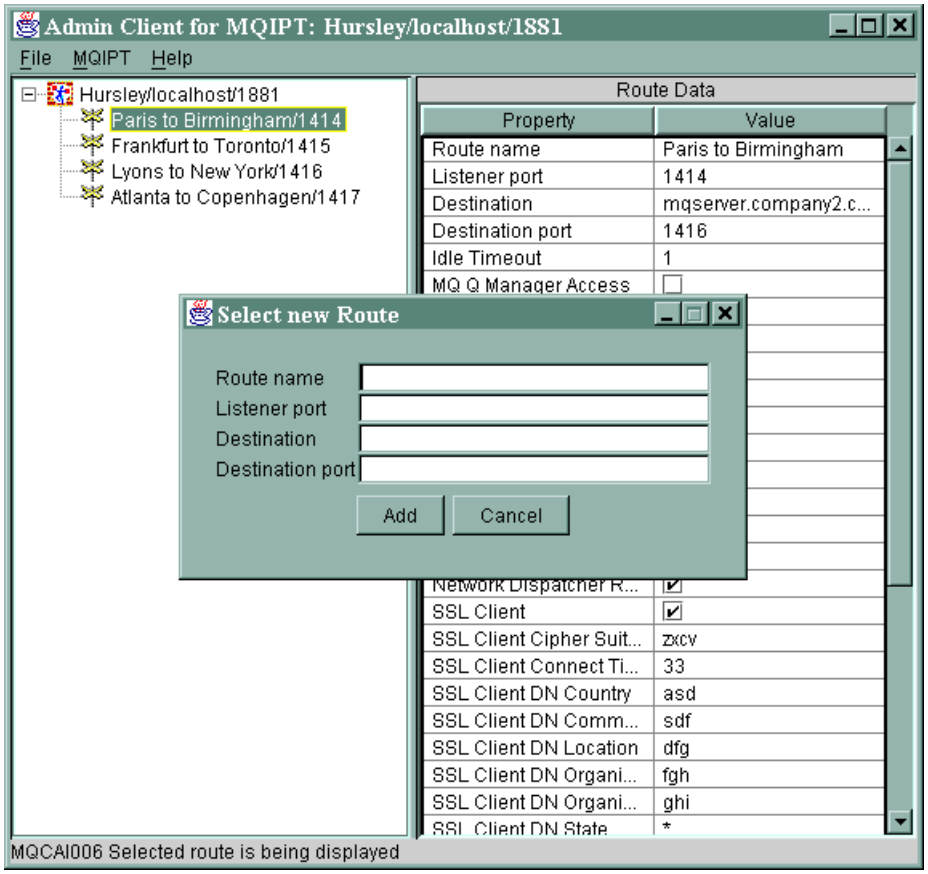

그림 9. 라우트 추가

라우트 삭제

MQIPT에서 선택된 라우트를 삭제합니다. 삭제는 “적용” 메뉴 옵션을 사용할 때까지 MQIPT에 적용되지 않습니다.

적용

MQIPT 구성을 원하는 대로 변경하였으면 이 옵션을 사용하여 새 구성 파일을 MQIPT에 송신하여 저장하도록 합니다. 그러면 즉시 새 설정이 적용됩니다.

새로 고침

선택된 MQIPT에서 구성 파일을 읽고 표시를 새로 고칩니다.

정지

MQIPT에 정지 명령을 송신하여 실행을 정지시키도록 명령합니다. 이 명령을 발행한 후에는 MQIPT와 접속할 수 없습니다. 전역 등록 정보인 RemoteShutdown이 켜져 있지 않으면 이 명령이 무시됩니다.

라우트 정보는 MQIPT 전역 정보와 동일한 방법으로 갱신할 수 있습니다. 라우트의 임의의 등록 정보를 변경하면 변경 사항이 적용되기 전에 이를 먼저 적용해야 합니다. “MQIPT/적용” 메뉴 옵션을 선택하거나 구성을 저장할 것인지 묻는 등록 정보에 ″예″라고 대답하여 적용시킬 수 있습니다.

도움말 메뉴 옵션

도움말

Netscape에 관리 클라이언트를 사용하는 방법에 관한 정보를 표시하는 데 사용됩니다. 왼쪽 분할창에서 ″internet pass-thru 관리 및 구성″을 선택하십시오. 관리 클라이언트를 사용하기 전에 반드시 <lang>/html 서브디렉토리에 있는 파일의 압축을 풀어야 합니다.

정보

관리 클라이언트의 버전 정보가 있는 스플래시 창을 표시합니다.

---

internet pass-thru 행 모드 명령

관리 클라이언트를 사용하지 않기로 선택한 경우에는 행 모드 명령을 사용하여 internet pass-thru를 관리하고 구성할 수 있습니다.

행 모드 명령을 사용하여 internet pass-thru 관리

사용자의 선택에 따라 편집기를 사용하여 구성 파일인 mqipt.conf를 변경함으로써 요구사항에 맞출 수 있습니다. 사용자가 변경할 수 있는 등록 정보 목록을 보려면 81 페이지의 『구성 참조 정보』의 내용을 참조하십시오.

mqipt.conf의 전역 섹션이 CommandPort에 대한 값을 지정하는 경우에는 MQIPT가 이 포트에서 다음 ASCII 관리 명령이 올 때까지 대기합니다.

```
mqiptAdmin -refresh {hostname {port} }      새로 고침 명령 송신
mqiptAdmin -stop    {hostname {port} }      중지 명령
송신
```

mqiptAdmin 스크립트는 bin 서브디렉토리에 있습니다.

호스트 이름과 포트를 제공하지 않으면 localhost에 대한 디폴트 값과 1881 포트가 사용됩니다.

STOP

MQIPT가 모든 연결을 닫고 수신되는 연결에 대한 대기를 정지하고 종료됩니다. 관리 클라이언트의 “MQIPT/정지” 메뉴 옵션을 사용하여도 같은 결과가 나옵니다. mqipt.conf 파일이 RemoteShutDown=true를 지정하지 않으면 이 명령이 무시됩니다.

REFRESH

MQIPT가 mqipt.conf를 다시 읽습니다. 다음 경우에 적용됩니다.

- 현재 활성 중인 라우트 중 비활성으로 표시되거나 알고리즘을 상실한 것으로 표시된 것이 있으면 라우트를 닫고 이러한 라우트에 대해서 수신되는 연결 대기 상태를 중지합니다.

- 현재 실행 중이지 않은 구성 파일에 활성으로 표시된 라우트가 있으면 이를 시작합니다.
- 현재 실행 중인 라우트의 구성 매개변수가 변경되었으면 해당 라우트에 변경된 값을 적용합니다. 추적 설정에 대한 변경 등, 가능한 경우에는 실행 중인 연결을 방해하지 않고 이 작업을 수행합니다. 목적지에 대한 변경 등 일부 매개변수 변경에 대해서는 변경 사항을 적용하고 라우트를 재시작하기 전에 MQIPT가 모든 연결을 닫아야 합니다.

관리 클라이언트가 MQIPT의 설정을 변경하지 않은 한, 관리 클라이언트의 "MQIPT/적용" 메뉴 옵션을 사용하여도 같은 결과가 나옵니다.

Windows에서 시작 -> 프로그램 메뉴를 사용하여 이러한 관리 기능을 수행할 수 있습니다.

구성 참조 정보

MQIPT는 mqipt.conf라는 구성 파일을 사용하여 MQIPT 서버 조치의 라우트 및 제어를 정의합니다. 파일은 일련의 섹션으로 구성됩니다. 즉, 하나의 전역 섹션인 MQIPT를 통해 정의된 각 라우트에 대한 추가 섹션으로 구성됩니다.

각 섹션에는 이름/값 등록 정보 쌍이 포함됩니다. 일부 등록 정보는 전역 섹션에만 표시될 수 있으며 일부는 라우트 섹션에만 표시될 수 있으며 일부는 라우트와 전역 섹션 둘 다에 표시될 수 있습니다. 등록 정보가 라우트와 전역 섹션 둘 다에 표시되는 경우에는 라우트 섹션의 등록 정보 값이 전역 값을 대체하나 논의 중의 라우트만 해당됩니다. 이런 방법으로 개별 라우트 섹션에서 설정되지 않은 등록 정보에 대해 사용할 디폴트 값을 설정하기 위해 전역 섹션을 사용할 수 있습니다.

전역 섹션은 `[global]` 문자를 포함하는 행으로 시작하여 첫 번째 라우트 섹션이 시작할 때 종료됩니다. 전역 섹션은 반드시 파일 내의 모든 라우트 섹션보다 앞서야 합니다. 각 라우트 섹션은 `[route]` 문자를 포함하는 행으로 시작하여 다음 라우트 섹션이 시작하거나 구성 파일의 맨 끝에 도달하면 종료됩니다.

인식할 수 없는 모든 키워드 이름, 즉 이름/값 쌍에서 이름이 이 문서에서 정의된 이름 중 하나가 아닌 경우에는 무시됩니다. 라우트 섹션에 표시되는 이름/값 쌍에 인식할 수는 있으나 `MinConnectionThreads=x` 또는 `HTTP=unsure` 등과 같이 올바르지 않은 값이 있으면 라우트를 사용하지 않습니다. 즉, 수신되는 모든 연결에 대해 대기하지 않습니다. 전역 섹션에서 표시되는 이름/값 쌍이 인식되는 이름이나 올바르지 않은 값을 가지고 있으면 모든 라우트가 사용 불가능하게 되며 MQIPT가 시작되지 않습니다. 여기서 등록 정보는 값이 `true` 및 `false`를 사용하는 대로 나열되며 대문자와 소문자를 혼용할 수 있습니다.

mqipt.conf 파일을 편집하거나 관리 클라이언트 GUI를 사용하여 등록 정보를 변경할 수 있습니다. 변경사항을 적용하기 위해 관리자는 관리 클라이언트 GUI에서 또는 mqiptAdmin 스크립트를 사용하여 refresh 명령을 발행할 수 있습니다.

이미 다른 등록 정보가 사용된 경우 특정 등록 정보를 변경하면 라우트만 재시작됩니다. 예를 들어 HTTP 등록 정보의 변경은 HTTP 등록 정보도 사용할 수 있어야 적용됩니다.

라우트가 재시작되면 기존 연결이 종료됩니다. 이 작동을 대체하려면 RouteRestart 등록 정보를 거짓으로 설정하십시오. 이렇게 하면 라우트가 재시작되지 않으므로 RouteRestart 등록 정보를 다시 사용할 수 있을 때까지 기존 연결이 활성 상태로 유지될 수 있습니다.

일부 간단한 구성을 설정하는 방법에 대한 정보를 보려면 103 페이지의 제 20 장 『internet pass-thru 시작하기』를 참조하십시오. 샘플 구성을 보려면 MQIPT의 홈 디렉토리에서 `mqiptSample.conf` 파일을 참조하십시오.

등록 정보 요약

표 3에는 다음과 같은 내용이 표시됩니다.

- 모든 등록 정보
- 등록 정보가 전역 섹션과 라우트 섹션 중 어디에 적용되는지, 또는 둘 다에 적용되는지 여부
- 디폴트 값은 등록 정보가 라우트 섹션과 전역 섹션 둘 다에서 누락된 경우에 사용됩니다.

표 3. 구성 등록 정보 요약

등록 정보 이름	전역	라우트	디폴트
AccessPW	예	아니오	<널(null)>
Active	예	예	참
ClientAccess	예	예	거짓
CommandPort	예	아니오	<널(null)>
ConnectionLog	예	아니오	참
Destination	아니오	예	<널(null)>
DestinationPort	아니오	예	1414
HTTP[6,7]	예	예	거짓
HTTPChunking[1]	예	예	거짓
HTTPProxy[1]	예	예	<널(null)>
HTTPProxyPort[1]	예	예	8080
HTTPS[1]	예	예	거짓
HTTPServer[1]	예	예	<널(null)>
HTTPServerPort[1]	예	예	<널(null)>
IdleTimeout	예	예	0

표 3. 구성 등록 정보 요약 (계속)

등록 정보 이름	전역	라우트	디폴트
IgnoreExpiredCRLs	예	예	거짓
LDAP	예	예	거짓
LDAPIgnoreErrors[10]	예	예	거짓
LDAPCacheTimeout[10]	예	예	24
LDAPSaveCRL[10]	예	예	거짓
LDAPServer1[10]	예	예	<널(null)>
LDAPServer1Port[10]	예	예	389
LDAPServer1Userid[10]	예	예	<널(null)>
LDAPServer1Password[10]	예	예	<널(null)>
LDAPServer1Timeout[10]	예	예	0
LDAPServer2[10]	예	예	<널(null)>
LDAPServer2Port[10]	예	예	389
LDAPServer2Userid[10]	예	예	<널(null)>
LDAPServer2Password[10]	예	예	<널(null)>
LDAPServer2Timeout[10]	예	예	0
ListenerPort	아니오	예	<널(null)>
LocalAddress	예	예	<널(null)>
LogDir(MQIPTServlet에만 해당됨)	아니오	아니오	<널(null)>
MaxConnectionThreads	예	예	100
MaxLogFileSize	예	아니오	50
MinConnectionThreads	예	예	5
Name	아니오	예	<널(null)>
NDAdvisor	예	예	거짓
NDAdvisorReplaceMode[4]	예	예	거짓
OutgoingPort	아니오	예	0
QMgrAccess	예	예	참
QoS(Linux에서만 사용할 수 있음)	예	예	거짓
QosToCaller[9]	예	예	1
QosToDest[9]	예	예	1
RemoteShutdown	예	아니오	거짓
RouteRestart	예	예	참
SecurityExit	예	예	거짓
SecurityExitName[11]	예	예	<널(null)>
SecurityExitPath[11]	예	예	<ipthome>\exits
SecurityExitTimeout[11]	예	예	5
SecurityManager	예	아니오	거짓
SecurityManagerPolicy	예	아니오	<널(null)>
ServletClient[1]	예	예	거짓
SocksClient	예	예	거짓

표 3. 구성 등록 정보 요약 (계속)

등록 정보 이름	전역	라우트	디폴트
SocksProxyHost[8]	예	예	<널(null)>
SocksProxyPort[8]	예	예	1080
SocksServer[7]	예	예	거짓
SSLClient	예	예	거짓
SSLClientCAKeyRing[2]	예	예	<널(null)>
SSLClientCAKeyRingPW[2]	예	예	<널(null)>
SSLClientCipherSuites[2]	예	예	<널(null)>
SSLClientConnectTimeout[2]	예	예	30
SSLClientDN_C[2]	예	예	"*"[5]
SSLClientDN_CN[2]	예	예	"*"[5]
SSLClientDN_L[2]	예	예	"*"[5]
SSLClientDN_O[2]	예	예	"*"[5]
SSLClientDN_OU[2]	예	예	"*"[5]
SSLClientDN_ST[2]	예	예	"*"[5]
SSLClientKeyRing[2]	예	예	<널(null)>
SSLClientKeyRingPW[2]	예	예	<널(null)>
SSLClientSiteDN_C[2]	예	예	"*"[5]
SSLClientSiteDN_CN[2]	예	예	"*"[5]
SSLClientSiteDN_L[2]	예	예	"*"[5]
SSLClientSiteDN_O[2]	예	예	"*"[5]
SSLClientSiteDN_OU[2]	예	예	"*"[5]
SSLClientSiteDN_ST[2]	예	예	"*"[5]
SSLClientSiteLabel[2]	예	예	<널(null)>
SSLProxyMode	예	예	거짓
SSLServer[6]	예	예	거짓
SSLServerAskClientAuth[3]	예	예	거짓
SSLServerCAKeyRing[3]	예	예	<널(null)>
SSLServerCAKeyRingPW[3]	예	예	<널(null)>
SSLServerCipherSuites[3]	예	예	<널(null)>
SSLServerDN_C[3]	예	예	"*"[5]
SSLServerDN_CN[3]	예	예	"*"[5]
SSLServerDN_L[3]	예	예	"*"[5]
SSLServerDN_O[3]	예	예	"*"[5]
SSLServerDN_OU[3]	예	예	"*"[5]
SSLServerDN_ST[3]	예	예	"*"[5]
SSLServerKeyRing[3]	예	예	<널(null)>
SSLServerKeyRingPW[3]	예	예	<널(null)>
SSLServerSiteDN_C[3]	예	예	"*"[5]
SSLServerSiteDN_CN[3]	예	예	"*"[5]
SSLServerSiteDN_L[3]	예	예	"*"[5]

표 3. 구성 등록 정보 요약 (계속)

등록 정보 이름	전역	라우트	디폴트
SSLServerSiteDN_O[3]	예	예	"*"[5]
SSLServerSiteDN_OU[3]	예	예	"*"[5]
SSLServerSiteDN_ST[3]	예	예	"*"[5]
SSLServerSiteLabel[3]	예	예	<널(null)>
Trace	예	예	0
UriName(디폴트 설정에 대한 자세한 내용은 102 페이지의 『UriName』 페이지 참조) [1]	예	예	

주:

1. HTTP 등록 정보가 적용되도록 하려면 HTTP를 참으로 설정하십시오.
2. SSLClient 등록 정보가 적용되도록 하려면 SSLClient를 참으로 설정하십시오.
3. SSLServer 등록 정보가 적용되도록 하려면 SSLServer를 참으로 설정하십시오.
4. NDAdvisor 등록 정보가 적용되도록 하려면 NDAdvisor를 참으로 설정하십시오.
5. "*" 기호는 와일드카드를 나타냅니다.
6. HTTP 및 SSLServer는 함께 사용할 수 없습니다. HTTP 등록 정보는 전달 연결을 정의하는 데만 사용됩니다. ListenerPort에 수신되는 데이터는 자동으로 감지되며 SSLServer를 설정하면 런타임 예외가 발생합니다.
7. HTTP 및 SocksServer는 함께 사용할 수 없습니다. HTTP 등록 정보는 전달 연결을 정의하는 데만 사용됩니다. ListenerPort에 수신되는 데이터는 자동으로 감지되며 SocksServer를 설정하면 런타임 예외가 발생합니다.
8. SocksClient 등록 정보가 적용되도록 하려면 SocksClient를 참으로 설정하십시오.
9. QoS 등록 정보가 적용되도록 하려면 QoS를 참으로 설정하십시오.
10. LDAP 등록 정보가 적용되도록 하려면 SocksClient를 참으로 설정하십시오.
11. SecurityExit 등록 정보가 적용되도록 하려면 QoS를 참으로 설정하십시오.

전역 섹션 참조 정보

전역 섹션은 ListenerPort, Destination, DestinationPort, Name 및 OutgoingPort는 별도로 하고 다음 등록 정보와 86 페이지의 『라우트 섹션 참조 정보』에 나오는 모든 등록 정보를 포함할 수 있습니다.

AccessPW

관리 제어기가 MQIPT에 명령을 송신할 때 사용하는 암호입니다. 이 등록 정보가 없거나 공백으로 설정되어 있으면 점검이 수행되지 않습니다.

CommandPort

MQIPT가 `mqiptAdmin` 유틸리티 또는 관리 클라이언트로부터 구성 명령에 대기하는 TCP/IP 포트입니다. 다른 등록 정보와 동일한 방법으로 관리 클라이언트에서 명

령 포트를 변경할 수 있습니다. 연결 등록 정보는 변경하지 않도록 주의하십시오. 새 설정을 MQIPT에 적용하는 경우에는 관리 클라이언트가 연결 등록 정보를 변경합니다.

CommandPort 등록 정보가 없으면 MQIPT가 구성 명령에 대해 대기하지 않습니다. 명령 포트에서 대기하려면 1881을 사용하도록 권장합니다. 관리 클라이언트는 CommandPort에 대해 디폴트 값이 없지만 행 모드 명령을 사용하는 경우에는 1881이 디폴트 값입니다.

ConnectionLog

참 또는 거짓입니다. 참이면 MQIPT가 logs 서브디렉토리에 성공 여부에 상관없이 모든 연결 시도를 기록하고 mqiptYYYYMMDDHHmmSS.log 파일에 연결 끊기 이벤트를 기록합니다. 디폴트 값은 참입니다. 이 등록 정보가 참에서 거짓으로 변경되면 MQIPT가 기존 연결 로그를 닫고 새 로그를 작성합니다. 새 로그는 등록 정보가 참으로 재설정될 때 사용됩니다.

MaxLogFileSize

연결 로그 파일의 최대 *크기*이며 KB 단위로 지정됩니다. 파일 *크기*가 이 최대 값 이상으로 증가하면 백업 사본인 mqipt.back이 만들어지고 새 파일이 시작됩니다. 하나의 백업 파일만이 보존되며 기본 로그 파일이 채워질 때마다 이전 백업이 지워집니다. 디폴트 값은 50이며 허용되는 최소 값은 5입니다.

RemoteShutDown

참 또는 거짓입니다. 참이며 명령 포트가 있는 경우에는 명령 포트에서 STOP 명령을 수신할 때마다 MQIPT가 종료됩니다. 디폴트 값은 거짓입니다.

SecurityManager

MQIPT의 해당 인스턴스에 대해 Java 보안 관리자를 사용하려면 이 등록 정보를 참으로 설정하십시오. 이 설정은 올바른 권한이 부여되었는지에 의해 결정됩니다. 자세한 정보는 33 페이지의 『Java 보안 관리자』를 참조하십시오. 이 등록 정보에 대한 디폴트 값은 거짓입니다.

SecurityManagerPolicy

정책 파일의 완전한 파일 이름입니다. 이 등록 정보가 설정되지 않으면 디폴트 시스템 및 사용자 정책 파일이 사용됩니다. Java 보안 관리자를 이미 사용할 수 있는 경우에는 Java 보안 관리자를 사용할 수 없게 되었다가 다시 사용할 수 있게 될 때까지 이 등록 정보가 적용되지 않도록 변경합니다.

라우트 섹션 참조 정보

라우트 섹션은 다음과 같은 등록 정보를 포함할 수 있습니다.

Active

라우트는 Active의 값이 참으로 설정된 경우에만 수신되는 연결을 승인합니다. 즉, 구성 파일에서 라우트 섹션을 삭제하지 않고도 Active=false를 설정하여 목적지

에 대한 액세스를 임시로 종료할 수 있음을 의미합니다. 이 등록 정보를 거짓으로 변경하면 REFRESH 명령이 발행될 때 라우트가 정지됩니다. 이 라우트에 대한 모든 연결이 종료됩니다.

ClientAccess

라우트는 ClientAccess의 값이 참으로 설정된 경우에만 수신되는 클라이언트 채널 연결을 승인합니다. 이후에 MQIPT가 클라이언트 요청만, 큐 관리자 요청만 또는 두 유형의 요청을 모두 승인하도록 구성할 가능성이 있다는 점에 주의하십시오. 이 등록 정보는 QMgrAccess 등록 정보와 함께 사용하십시오. 이 등록 정보를 거짓으로 변경하면 REFRESH 명령이 발행될 때 라우트가 정지되었다가 재시작됩니다. 이 라우트에 대한 모든 연결이 종료됩니다.

Destination

해당 라우트에 대해 연결할 큐 관리자 또는 후속 MQIPT의 호스트 이름 또는 점 분리 십진수 IP 주소입니다. 각 라우트 섹션은 **반드시** 명확한 Destination 값을 포함해야 합니다. 여러 라우트 섹션이 동일한 목적지를 지정하도록 할 수 있습니다. 이 등록 정보에 대한 변경이 라우트에 적용되면 REFRESH 명령이 발행될 때 라우트가 정지되었다가 재시작됩니다. 이 라우트에 대한 모든 연결이 종료됩니다.

DestinationPort

이 라우트가 연결된 Destination 호스트 상의 포트입니다. Destination 및 DestinationPort의 동일한 결합에 둘 이상의 라우트가 지정되는 것도 가능합니다. 각 라우트 섹션은 **반드시** 명확한 DestinationPort 값을 포함해야 합니다. 이 등록 정보에 대한 변경이 라우트에 적용되면 REFRESH 명령이 발행될 때 라우트가 정지되었다가 재시작됩니다. 이 라우트에 대한 모든 연결이 종료됩니다.

HTTP

이 등록 정보를 참으로 설정하면 라우트가 외부 HTTP 터널링 요청 작성에 책임을 지게 됩니다. 즉, HTTP를 통해 다른 MQIPT와 통신하게 됩니다. 거짓으로 설정하면 라우트가 WebSphere MQ 큐 관리자에 전달됩니다. 이 등록 정보가 변경되면 REFRESH 명령이 발행될 때 라우트가 정지되었다가 재시작됩니다. 이 라우트에 대한 모든 연결이 종료됩니다. HTTP 청킹을 사용하려면 이 등록 정보를 참으로 설정하십시오. 이 등록 정보는 다음 등록 정보와 함께 사용할 수 없습니다.

- QoS
- SocksClient
- SSLClient
- SSLProxyMode

HTTPChunking

이 등록 정보를 참으로 설정하면 라우트가 청킹과 함께 HTTP 터널링을 사용하여 외부 요청을 작성하는 것에 대해 책임을 지게 됩니다. HTTP 등록 정보는 또한 반드시 참으로 설정되어야 합니다. HTTP 청킹을 사용하지 않는 경우에는 거짓으로

설정하십시오. 이 등록 정보가 변경되고 HTTP가 참으로 설정되어 있으면 REFRESH 명령이 발행될 때 라우트가 정지되었다가 재시작됩니다. 이 라우트에 대한 모든 연결이 종료됩니다.

HTTPProxy

해당 라우트에 대한 모든 연결이 사용할 HTTP 프록시의 호스트 이름 또는 점분리 십진수 IP 주소입니다. HTTPServer도 정의되면 정상 POST 대신 HTTPProxy에 CONNECT 요청이 발행됩니다. 이 등록 정보가 변경되고 HTTP가 참으로 설정되어 있으면 REFRESH 명령이 발행될 때 라우트가 정지되었다가 재시작됩니다. 이 라우트에 대한 모든 연결이 종료됩니다.

HTTPProxyPort

HTTP 프록시에서 사용할 포트 주소입니다. HTTPS가 참으로 설정되고 HTTPServer가 없는 경우를 제외하면 디폴트 값은 8080이고, HTTPS가 참으로 설정되고 HTTPServer가 없는 경우 디폴트 값은 443입니다. 이 등록 정보가 변경되고 HTTP가 참으로 설정되어 있으면 REFRESH 명령이 발행될 때 라우트가 정지되었다가 재시작됩니다. 이 라우트에 대한 모든 연결이 종료됩니다.

HTTPServer

해당 라우트에 대한 모든 연결이 사용할 HTTP 서버의 호스트 이름 또는 점분리 십진수 IP 주소입니다. 이 등록 정보가 변경되고 HTTP가 참으로 설정되어 있으면 REFRESH 명령이 발행될 때 라우트가 정지되었다가 재시작됩니다. 이 라우트에 대한 모든 연결이 종료됩니다.

HTTPS

이 등록 정보를 사용하여 HTTPS 요청을 수행합니다. HTTP 등록 정보는 또한 사용 가능해야 합니다. 이 등록 정보가 변경되고 HTTP가 참으로 설정되어 있으면 REFRESH 명령이 발행될 때 라우트가 정지되었다가 재시작됩니다. 이 라우트에 대한 모든 연결이 종료됩니다.

HTTPServerPort

HTTP 서버에서 사용할 포트 주소입니다. HTTPS가 참으로 설정되지 않은 경우 디폴트 값은 8080이고 HTTPS가 참으로 설정된 경우 디폴트 값은 443입니다. 이 등록 정보가 변경되고 HTTP가 참으로 설정되어 있으면 REFRESH 명령이 발행될 때 라우트가 정지되었다가 재시작됩니다. 이 라우트에 대한 모든 연결이 종료됩니다.

IdleTimeout

비활동 연결이 닫히기 전에 경과하는 분 단위 시간입니다. 큐 관리자 또한 큐 관리자 채널에 대해 DISCINT 등록 정보를 갖습니다. IdleTimeout 매개변수를 설정하면 DISCINT를 기록해 두십시오. 값이 0이면 비활동 시간이 없음을 표시합니다. 라우트가 재시작되는 경우에만 이 등록 정보의 변경 사항이 적용됩니다.

IgnoreExpiredCRLs

만기된 CRL을 무시하려면 이 등록 정보를 참으로 설정하십시오. 디폴트 값은 거짓입니다.

주의

이 등록 정보를 사용하면 SSL 연결에 호출된 인증이 사용될 수 있습니다.

LDAP

SSL 연결을 사용할 때 LDAP 서버 사용을 사용 가능하게 하려면 등록 정보를 참으로 설정하십시오. MQIPT는 LDAP 서버를 CRL 및 ARL을 검색하는데 사용합니다. 이 등록 정보를 적용하려면 SSLClient 또는 SSLServer 등록 정보도 사용해야 합니다.

LDAPIgnoreErrors

이 등록 정보를 참으로 설정하여 LDAP 검색 시 연결이나 시간 종료 오류를 무시하십시오. MQIPT가 성공적인 검색을 수행할 수 없는 경우 이 등록 정보가 사용되지 않으면 클라이언트 연결을 완료할 수 없습니다. 성공적인 검색이란 CRL을 검색했거나 지정된 CA에 사용 가능한 CRL이 없음을 의미합니다. 이 등록 정보가 변경되고(LDAP가 참으로 설정되어 있으면) REFRESH 명령이 발행될 때 라우트가 정지되었다가 재시작됩니다. 이 라우트에 대한 모든 연결이 종료됩니다.

주의

이 등록 정보를 사용하면 SSL 연결에 호출된 인증이 사용될 수 있습니다.

LDAPCacheTimeout

CRL이 LDAP 서버에서 검색되면 CRL은 내부적으로 임시 캐시의 MQIPT에 저장됩니다. 이러한 캐시의 항목은 이 등록 정보에 지정된 특정 시간 종료 후에 만기됩니다. 디폴트 값은 24 시간입니다. 시간 종료 값 0을 지정하면 캐시의 항목은 라우트가 재시작되어야 만기됩니다. 이 등록 정보가 변경되고 (LDAP가 참으로 설정되어 있으면) REFRESH 명령이 발행될 때 라우트가 정지되었다가 재시작됩니다. 이 라우트에 대한 모든 연결이 종료됩니다.

LDAPSaveCRL

이 등록 정보를 참으로 설정하여 지정된 키 링 파일을 LDAP 서버에서 검색한 CRL로 갱신하십시오. 키 링 파일은 SSLClientKeyRing, SSLClientCAKeyRing, SSLServerKeyRing 및 SSLServerCAKeyRing 등록 정보와 함께 지정됩니다. 그러므로 MQIPT에는 키 링 파일에 대한 쓰기 액세스 권한이 있어야 합니다. 이 등록 정보가 변경되고(LDAP가 참으로 설정되어 있으면) REFRESH 명령이 발행될 때 라우트가 정지되었다가 재시작됩니다. 이 라우트에 대한 모든 연결이 종료됩니다.

LDAPServer1

이 등록 정보는 호스트 이름 또는 기본 LDAP 서버 IP 주소를 설정합니다. 이 등록 정보는 LDAP가 사용 가능한 경우 설정해야 합니다. 이 등록 정보가 변경되고 (LDAP가 참으로 설정되어 있으면) REFRESH 명령이 발행될 때 라우트가 정지되었다가 재시작됩니다. 이 라우트에 대한 모든 연결이 종료됩니다.

LDAPServer1Port

이 등록 정보는 기본 LDAP 서버의 대기 포트 주소를 설정합니다. 디폴트 값은 389입니다. 이 등록 정보가 변경되고 (LDAP가 참으로 설정되어 있으면) REFRESH 명령이 발행될 때 라우트가 정지되었다가 재시작됩니다. 이 라우트에 대한 모든 연결이 종료됩니다.

LDAPServer1Userid

이 등록 정보는 기본 LDAP 서버를 액세스하는 데 필요한 사용자 ID를 설정합니다. 이 등록 정보는 기본 LDAP 서버에 액세스 권한 부여가 필요할 경우에 설정해야 합니다. 이 등록 정보가 변경되고 (LDAP가 참으로 설정되어 있으면) REFRESH 명령이 발행될 때 라우트가 정지되었다가 재시작됩니다. 이 라우트에 대한 모든 연결이 종료됩니다.

LDAPServer1Password

이 등록 정보는 기본 LDAP 서버를 액세스하는 데 필요한 암호를 설정합니다. 이 등록 정보는 LDAPServer1Userid가 설정한 경우 설정해야 합니다. 이 등록 정보가 변경되고 (LDAP가 참으로 설정되어 있으면) REFRESH 명령이 발행될 때 라우트가 정지되었다가 재시작됩니다. 이 라우트에 대한 모든 연결이 종료됩니다.

LDAPServer1Timeout

이 등록 정보는 기본 LDAP 서버에서 MQIPT가 응답하는 초 수로 설정하십시오. 디폴트 값은 연결이 시간 종료되지 않음을 나타내는 0입니다. 이 등록 정보가 변경되고(LDAP가 참으로 설정되어 있으면) REFRESH 명령이 발행될 때 라우트가 정지되었다가 재시작됩니다. 이 라우트에 대한 모든 연결이 종료됩니다.

LDAPServer2

이 등록 정보는 호스트 이름 또는 백업 LDAP 서버 IP 주소를 설정합니다. 이 등록 정보는 선택적입니다. 이 등록 정보가 변경되고 (LDAP가 참으로 설정되어 있으면) REFRESH 명령이 발행될 때 라우트가 정지되었다가 재시작됩니다. 이 라우트에 대한 모든 연결이 종료됩니다.

LDAPServer2Port

이 등록 정보는 백업 LDAP 서버의 대기 포트 주소를 설정합니다. 디폴트 값은 389입니다. 이 등록 정보가 변경되고 (LDAP가 참으로 설정되어 있으면) REFRESH 명령이 발행될 때 라우트가 정지되었다가 재시작됩니다. 이 라우트에 대한 모든 연결이 종료됩니다.

LDAPServer2Userid

이 등록 정보는 백업 LDAP 서버를 액세스하는 데 필요한 사용자 ID를 설정합니

다. 이 등록 정보는 백업 LDAP 서버에 액세스 권한 부여가 필요할 경우에 설정해야 합니다. 이 등록 정보가 변경되고 (LDAP가 참으로 설정되어 있으면) REFRESH 명령이 발행될 때 라우트가 정지되었다가 재시작됩니다. 이 라우트에 대한 모든 연결이 종료됩니다.

LDAPServer2Password

이 등록 정보는 백업 LDAP 서버를 액세스하는 데 필요한 암호를 설정합니다. 이 등록 정보는 LDAPServer2가 사용 가능한 경우 설정해야 합니다. 이 등록 정보가 변경되고 (LDAP가 참으로 설정되어 있으면) REFRESH 명령이 발행될 때 라우트가 정지되었다가 재시작됩니다. 이 라우트에 대한 모든 연결이 종료됩니다.

LDAPServer2Timeout

이 등록 정보는 백업 LDAP 서버에서 MQIPT가 응답하는 초 수로 설정하십시오. 디폴트 값은 연결이 시간 종료되지 않음을 나타내는 0입니다. 이 등록 정보가 변경되고 (LDAP가 참으로 설정되어 있으면) REFRESH 명령이 발행될 때 라우트가 정지되었다가 재시작됩니다. 이 라우트에 대한 모든 연결이 종료됩니다.

ListenerPort

라우트가 수신되는 요청에 대해 대기하는 포트 번호입니다. 각 라우트 섹션은 **반드시** 명확한 ListenerPort 값을 포함해야 하며 각 섹션에서 지정된 ListenerPort 값이 구별되어야 합니다. 80 및 443 포트를 포함하여 임의의 올바른 포트 번호를 사용할 수 있습니다. 단, 동일한 호스트에서 실행 중인 다른 리스너에 의해 이미 선택된 포트는 사용할 수 없습니다.

LocalAddress

로컬 IP 주소는 모든 연결로 바인딩합니다. 이 등록 정보가 변경되면 REFRESH 명령이 발행될 때 라우트가 정지되었다가 재시작됩니다. 이 라우트에 대한 모든 연결이 종료됩니다.

LogDir

이 등록 정보는 로그 및 추적 파일에 사용하는 디렉토리 이름을 정의합니다. 이 등록 정보에 대한 변경은 MQIPTServlet이 정지되고 재시작되어야 적용됩니다. 디폴트 값은 <널(null)>입니다. 이 등록 정보는 MQIPTServlet에 대해서만 해당됩니다.

MaxConnectionThreads

연결 스레드의 최대 수이며, 따라서 해당 라우트에 의해 핸들링될 수 있는 동시 연결의 최대 수가 됩니다. 이 한계에 이르면 `MaxConnectionThreads` 값 즉 모든 스레드에 한번에 대기되는 연결 수가 모두 사용 중임을 표시합니다. 이 수를 초과하면 후속 연결이 거부됩니다. 최소 허용 값은 1 또는 MinConnectionThreads 보다 커야 합니다. 이 등록 정보에 대한 변경이 라우트에 적용되면 REFRESH 명령이 발행될 때 새 값이 사용됩니다. 모든 연결은 즉시 새 값을 선택합니다. 라우트가 종료되지 않습니다.

MinConnectionThreads

연결 스레드, 즉 해당 라우트에서 수신되는 연결을 처리하는 스레드의 최소 수입니

다. 라우트가 시작될 때 하당되는 스레드의 수이며 할당된 스레드의 총 수는 라우트가 활성 상태인 동안 이 값 아래로 내려가지 않습니다. 허용되는 최소 값은 0이며 값은 반드시 MaxConnectionThreads에 대해 지정된 값 미만이어야 합니다. 라우트가 재시작되는 경우에만 이 등록 정보의 변경 사항이 적용됩니다.

Name

라우트를 식별하는 데 도움이 되는 선택적 이름입니다. 콘솔 메시지 및 추적 정보에 표시됩니다. 라우트가 재시작되는 경우에만 이 등록 정보의 변경 사항이 적용됩니다.

NDAdvisor

Network Dispatcher에 의해 관리되는 라우트에 대해 이 등록 정보를 참으로 설정하면 라우트가 사용자 정의 advisor로부터의 요청에 응답할 수 있습니다. 이 등록 정보를 거짓으로 변경하면 REFRESH 명령이 발행될 때 라우트가 정지됩니다. 이 라우트에 대한 모든 연결이 종료됩니다. NDAdvisorReplaceMode 등록 정보를 사용하려면 이 등록 정보를 참으로 설정하십시오.

NDAdvisorReplaceMode

Network Dispatcher 사용자 정의 advisor의 "바꾸기" 모드를 사용하려면 이 등록 정보를 참으로 설정하십시오. 해당 라우트의 ListenerPort 주소에 대해 `mqipt_replace custom advisor`를 시작한 상태여야 합니다. "정상" 모드를 사용하려면 이 등록 정보를 거짓으로 설정하십시오. 이 등록 정보를 사용하려면 반드시 NDAdvisor 등록 정보를 참으로 설정해야 합니다.

OutgoingPort

보내는 연결에 사용되는 시작 포트 주소입니다. 포트 주소의 범위는 이 라우트의 `MaxConnectionThread` 값과 일치합니다. 디폴트 값 `0`은 시스템 정의된 포트 주소를 사용합니다. 이 등록 정보가 변경되면 REFRESH 명령이 발행될 때 라우트가 정지되었다가 재시작됩니다. 이 라우트에 대한 모든 연결이 종료됩니다.

QMgrAccess

라우트는 QMgrAccess의 값이 참으로 설정된 경우에만 수신 큐 관리자 채널 연결(송신자 채널)이 허용됩니다. 이 등록 정보를 거짓으로 변경하면 REFRESH 명령이 발행될 때 라우트가 정지됩니다. 이 라우트에 대한 모든 연결이 종료됩니다.

QoS

이 라우트 상의 모든 연결에 대해 Quality of Service를 사용하려면 이 등록 정보를 참으로 설정하십시오. 이 등록 정보는 Linux에서만 사용할 수 있습니다. 이 등록 정보가 변경되면 REFRESH 명령이 발행될 때 라우트가 정지되었다가 재시작됩니다. 이 라우트에 대한 모든 연결이 종료됩니다. 이 등록 정보는 다음 등록 정보와 함께 사용할 수 없습니다.

- HTTP
- SSLClient

- SSLProxyMode
- SSLServer

QosToCaller

이 등록 정보는 MQIPT 시스템으로부터 연결의 시작기에 대한 모든 소통의 우선순위를 설정합니다. 예를 들어, 낮은 우선순위에 대해서는 이 등록 정보를 1로 설정하고 중간 우선순위에 대해서는 2로 설정하며 높은 우선순위에 대해서는 이 등록 정보를 3으로 설정합니다. 디폴트 값은 1입니다. 이 등록 정보가 변경되고 QoS가 참으로 설정되어 있으면 REFRESH 명령이 발행될 때 라우트가 정지되었다가 재시작됩니다. 이 라우트에 대한 모든 연결이 종료됩니다.

QosToDest

이 등록 정보는 Destination 등록 정보에 의해 정의된 대로 MQIPT 시스템으로부터 연결의 목적지에 대한 모든 소통의 우선순위를 설정합니다. 예를 들어, 낮은 우선순위에 대해서는 이 등록 정보를 1로 설정하고 중간 우선순위에 대해서는 2로 설정하며 높은 우선순위에 대해서는 이 등록 정보를 3으로 설정합니다. 디폴트 값은 1입니다. 이 등록 정보가 변경되고 QoS가 참으로 설정되어 있으면 REFRESH 명령이 발행될 때 라우트가 정지되었다가 재시작됩니다. 이 라우트에 대한 모든 연결이 종료됩니다.

RouteRestart

이 등록 정보를 거짓으로 설정하여 다른 라우트 등록 정보를 변경하고 REFRESH 명령이 발행될 때 라우트가 재시작되지 않게 하십시오. 이 등록 정보에 대한 디폴트 값은 참입니다.

SecurityExit

사용자 정의된 보안 엑시트를 사용 가능하게 하려면 이 등록 정보를 참으로 설정하십시오. 이 등록 정보에 대한 디폴트 값은 거짓입니다.

SecurityExitName

사용자 정의된 보안 엑시트의 클래스 이름입니다. 이 등록 정보는 SecurityExit가 참으로 설정한 경우 설정해야 합니다. 이 등록 정보가 변경되고(SecurityExit가 참으로 설정되어 있으면) REFRESH 명령이 발행될 때 라우트가 정지되었다가 재시작됩니다. 이 라우트에 대한 모든 연결이 종료됩니다.

SecurityExitPath

완전한 경로 이름은 사용자 정의된 보안 엑시트를 포함합니다. 이 등록 정보가 설정되지 않으면 엑시트 서브디렉토리로 기본 설정됩니다. 이 등록 정보는 또한 사용자 정의된 보안 엑시트를 포함하는 jar 파일 이름을 정의할 수 있습니다. 이 등록 정보가 변경되고 (SecurityExit가 참으로 설정되어 있으면) REFRESH 명령이 발행될 때 라우트가 정지되었다가 재시작됩니다. 이 라우트에 대한 모든 연결이 종료됩니다.

SecurityExitTimeout

이 시간 종료 값은 연결 요청을 유효화할 때 응답을 기다리는 시간(초)을 판별할 수 있도록 MQIPT에 사용됩니다. 디폴트 값은 5 초입니다. 이 등록 정보가 변경되고 (SecurityExit가 참으로 설정되어 있으면) REFRESH 명령이 발행될 때 라우트가 정지되었다가 재시작됩니다. 이 라우트에 대한 모든 연결이 종료됩니다.

ServletClient

MQIPT servlet에 연결할 때 이 등록 정보를 참으로 설정하십시오. HTTP 등록 정보는 또한 반드시 참으로 설정되어야 합니다. 이 등록 정보가 변경되고 HTTP가 참으로 설정되어 있으면 REFRESH 명령이 발행될 때 라우트가 정지되었다가 재시작됩니다.

SocksClient

라우트가 Socks 클라이언트 역할을 하도록 하고 SocksProxyHost 및 SocksProxyPort 등록 정보를 사용하여 Socks 프록시를 통해 모든 연결을 정의하려면 이 등록 정보를 참으로 설정하십시오. 이 등록 정보가 변경되면 REFRESH 명령이 발행될 때 라우트가 정지되었다가 재시작됩니다. 이 라우트에 대한 모든 연결이 종료됩니다. 이 등록 정보는 다음 등록 정보와 함께 사용할 수 없습니다.

- HTTP
- SocksServer
- SSLClient
- SSLProxyMode

SocksProxyHost

해당 라우트에 대한 모든 연결이 사용할 Socks 프록시의 호스트 이름 또는 점 분리 십진수 IP 주소입니다. 이 등록 정보가 변경되고 SocksClient가 참으로 설정되어 있으면 REFRESH 명령이 발행될 때 라우트가 정지되었다가 재시작됩니다. 이 라우트에 대한 모든 연결이 종료됩니다.

SocksProxyPort

Socks 프록시에서 사용할 포트 주소입니다. 디폴트 값은 1080입니다. 이 등록 정보가 변경되고 SocksClient가 참으로 설정되어 있으면 REFRESH 명령이 발행될 때 라우트가 정지되었다가 재시작됩니다. 이 라우트에 대한 모든 연결이 종료됩니다.

SocksServer

라우트가 Socks 프록시 역할을 하도록 하고 Socks 클라이언트 연결을 승인하려면 이 등록 정보를 참으로 설정하십시오. 이 등록 정보가 변경되면 REFRESH 명령이 발행될 때 라우트가 정지되었다가 재시작됩니다. 이 라우트에 대한 모든 연결이 종료됩니다. 이 등록 정보는 다음 등록 정보와 함께 사용할 수 없습니다.

- SocksClient
- SSLProxyMode

- SSLServer

SSLClient

라우트가 SSL 클라이언트 역할을 하고 송신하는 SSL 연결을 작성하려면 이 등록 정보를 참으로 설정하십시오. 참으로 설정한다는 것은 목적지가 SSL 서버 또는 HTTP 프록시/서버 역할을 하는 또 다른 MQIPT라는 것을 의미합니다. SSLClientKeyRing 또는 SSLClientCAKeyRing 등록 정보로 키 링 파일의 이름을 지정해야 합니다. 이 등록 정보가 변경되면 REFRESH 명령이 발행될 때 라우트가 정지되었다가 재시작됩니다. 이 라우트에 대한 모든 연결이 종료됩니다. 이 등록 정보는 다음 등록 정보와 함께 사용할 수 없습니다.

- HTTP
- QoS
- SSLProxyMode

SSLClientCAKeyRing

CA 인증이 있는 키 링 파일의 완전한 파일 이름으로, SSL 서버에서 인증을 인증하는 데 사용됩니다. Windows 플랫폼에서는 파일 분리 문자로 반드시 두 개의 백 슬래시(\\)를 사용해야 합니다. 이 등록 정보가 변경되고(SSLClient가 참으로 설정되어 있으면) REFRESH 명령이 발행될 때 라우트가 정지되었다가 재시작됩니다. 이 라우트에 대한 모든 연결이 종료됩니다.

SSLClientCAKeyRingPW

클라이언트 CA 키 링을 열기 위해 사용하는 암호를 포함한 완전한 파일 이름입니다. Windows 플랫폼에서는 파일 분리 문자로 반드시 두 개의 백 슬래시(\\)를 사용해야 합니다. 이 등록 정보가 변경되고(SSLClient가 참으로 설정되어 있으면) REFRESH 명령이 발행될 때 라우트가 정지되었다가 재시작됩니다. 이 라우트에 대한 모든 연결이 종료됩니다.

SSLClientCipherSuites

SSL 클라이언트 측에서 사용하는 SSL 암호 모음의 이름입니다. 하나 이상의 지원되는 암호 모음이 될 수 있습니다. 이 등록 정보를 공백으로 두면 SSL 클라이언트가 SSLClientKeyRing으로부터 지원되는 암호 모음을 사용합니다. 이 등록 정보가 변경되고(SSLClient가 참으로 설정되어 있으면) REFRESH 명령이 발행될 때 라우트가 정지되었다가 재시작됩니다. 이 라우트에 대한 모든 연결이 종료됩니다.

SSLClientConnectTimeout

SSL 연결이 승인되도록 SSL 클라이언트가 대기하는 초 수로 이 등록 정보를 설정하십시오. 이 등록 정보가 변경되고(SSLClient가 참으로 설정되어 있으면) REFRESH 명령이 발행될 때 라우트가 정지되었다가 재시작됩니다. 이 라우트에 대한 모든 연결이 종료됩니다.

SSLClientDN_C

해당 국가 이름의 SSL 서버로부터 수신되는 인증을 승인하려면 이 등록 정보를 사

용하십시오. 범위를 확장하기 위해 이름의 접두부나 접미부에 별표(*)를 사용할 수 있습니다. 이 등록 정보를 지정하지 않으면 "국가 이름"을 의미하게 됩니다. 이 등록 정보가 변경되고(SSLClient가 참으로 설정되어 있으면) REFRESH 명령이 발행될 때 라우트가 정지되었다가 재시작됩니다. 이 라우트에 대한 모든 연결이 종료됩니다.

SSLClientDN_CN

해당 공용 이름의 SSL 서버로부터 수신되는 인증을 승인하려면 이 등록 정보를 사용하십시오. 범위를 확장하기 위해 이름의 접두부나 접미부에 별표(*)를 사용할 수 있습니다. 이 등록 정보를 지정하지 않으면 "국가 이름"을 의미하게 됩니다. 이 등록 정보가 변경되고 (SSLClient가 참으로 설정되어 있으면) REFRESH 명령이 발행될 때 라우트가 정지되었다가 재시작됩니다. 이 라우트에 대한 모든 연결이 종료됩니다.

SSLClientDN_L

해당 위치의 SSL 서버로부터 수신되는 인증을 승인하려면 이 등록 정보를 사용하십시오. 범위를 확장하기 위해 이름의 접두부나 접미부에 별표(*)를 사용할 수 있습니다. 이 등록 정보를 지정하지 않으면 "전체 위치"를 의미하게 됩니다. 이 등록 정보가 변경되고 (SSLClient가 참으로 설정되어 있으면) REFRESH 명령이 발행될 때 라우트가 정지되었다가 재시작됩니다. 이 라우트에 대한 모든 연결이 종료됩니다.

SSLClientDN_O

해당 조직의 SSL 서버로부터 수신되는 인증을 승인하려면 이 등록 정보를 사용하십시오. 범위를 확장하기 위해 이름의 접두부나 접미부에 별표(*)를 사용할 수 있습니다. 이 등록 정보를 지정하지 않으면 "전체 조직"을 의미하게 됩니다. 이 등록 정보가 변경되고 (SSLClient가 참으로 설정되어 있으면) REFRESH 명령이 발행될 때 라우트가 정지되었다가 재시작됩니다. 이 라우트에 대한 모든 연결이 종료됩니다.

SSLClientDN_OU

해당 조직 단위의 SSL 서버로부터 수신되는 인증을 승인하려면 이 등록 정보를 사용하십시오. 범위를 확장하기 위해 이름의 접두부나 접미부에 별표(*)를 사용할 수 있습니다. 이 등록 정보를 지정하지 않으면 "전체 조직 단위"를 의미하게 됩니다. 이 등록 정보가 변경되고 (SSLClient가 참으로 설정되어 있으면) REFRESH 명령이 발행될 때 라우트가 정지되었다가 재시작됩니다. 이 라우트에 대한 모든 연결이 종료됩니다.

SSLClientDN_ST

해당 상태의 SSL 서버로부터 수신되는 인증을 승인하려면 이 등록 정보를 사용하십시오. 범위를 확장하기 위해 이름의 접두부나 접미부에 별표(*)를 사용할 수 있습니다. 이 등록 정보를 지정하지 않으면 "전체 상태"를 의미하게 됩니다. 이 등록

정보가 변경되고 (SSLClient가 참으로 설정되어 있으면) REFRESH 명령이 발행될 때 라우트가 정지되었다가 재시작됩니다. 이 라우트에 대한 모든 연결이 종료됩니다.

SSLClientKeyRing

클라이언트 인증을 포함한 키 링의 파일의 완전한 파일 이름입니다. **Windows 플랫폼에서는** 파일 분리 문자로 반드시 두 개의 백 슬래시(\\)를 사용해야 합니다. SSLClient를 참으로 설정한 경우에는 반드시 SSLClientKeyRing을 지정해야 합니다. 이 등록 정보가 변경되고(SSLClient가 참으로 설정되어 있으면) REFRESH 명령이 발행될 때 라우트가 정지되었다가 재시작됩니다. 이 라우트에 대한 모든 연결이 종료됩니다.

SSLClientKeyRingPW

클라이언트 키 링을 열기 위해 사용하는 암호를 포함한 완전한 파일 이름입니다. **Windows 플랫폼에서는** 파일 분리 문자로 반드시 두 개의 백 슬래시(\\)를 사용해야 합니다. SSLClient를 참으로 설정한 경우에는 반드시 SSLClientKeyRingPW를 지정해야 합니다. 이 등록 정보가 변경되고(SSLClient가 참으로 설정되어 있으면) REFRESH 명령이 발행될 때 라우트가 정지되었다가 재시작됩니다. 이 라우트에 대한 모든 연결이 종료됩니다.

SSLClientSiteDN_C

이 등록 정보는 국가 이름을 지정하여 SSL 서버로 송신할 인증을 선택하는 데 사용합니다. 이 등록 정보를 지정하지 않으면 ″국가 이름″을 의미하게 됩니다. 이 등록 정보가 변경되고(SSLClient가 참으로 설정되어 있으면) REFRESH 명령이 발행될 때 라우트가 정지되었다가 재시작됩니다. 이 라우트에 대한 모든 연결이 종료됩니다.

SSLClientSiteDN_CN

이 등록 정보는 공용 이름을 지정하여 SSL 서버로 송신할 인증을 선택하는 데 사용합니다. 이 등록 정보를 지정하지 않으면 ″공용 이름″을 의미하게 됩니다. 이 등록 정보가 변경되고(SSLClient가 참으로 설정되어 있으면) REFRESH 명령이 발행될 때 라우트가 정지되었다가 재시작됩니다. 이 라우트에 대한 모든 연결이 종료됩니다.

SSLClientSiteDN_L

이 등록 정보는 위치 이름을 지정하여 SSL 서버로 송신할 인증을 선택하는 데 사용합니다. 이 등록 정보를 지정하지 않으면 ″위치 이름″을 의미하게 됩니다. 이 등록 정보가 변경되고(SSLClient가 참으로 설정되어 있으면) REFRESH 명령이 발행될 때 라우트가 정지되었다가 재시작됩니다. 이 라우트에 대한 모든 연결이 종료됩니다.

SSLClientSiteDN_O

이 등록 정보는 조직 이름을 지정하여 SSL 서버로 송신할 인증을 선택하는 데 사용합니다. 이 등록 정보를 지정하지 않으면 ″조직 이름″을 의미하게 됩니다. 이 등

록 정보가 변경되고 (SSLClient가 참으로 설정되어 있으면) REFRESH 명령이 발행될 때 라우트가 정지되었다가 재시작됩니다. 이 라우트에 대한 모든 연결이 종료됩니다.

SSLClientSiteDN_OU

이 등록 정보는 조직 단위 이름을 지정하여 SSL 서버로 송신할 인증을 선택하는 데 사용합니다. 이 등록 정보를 지정하지 않으면 ″조직 단위 이름″을 의미하게 됩니다. 이 등록 정보가 변경되고(SSLClient가 참으로 설정되어 있으면) REFRESH 명령이 발행될 때 라우트가 정지되었다가 재시작됩니다. 이 라우트에 대한 모든 연결이 종료됩니다.

SSLClientSiteDN_ST

이 등록 정보는 상태 이름을 지정하여 SSL 서버로 송신할 인증을 선택하는 데 사용합니다. 이 등록 정보를 지정하지 않으면 ″상태 이름″을 의미하게 됩니다. 이 등록 정보가 변경되고(SSLClient가 참으로 설정되어 있으면) REFRESH 명령이 발행될 때 라우트가 정지되었다가 재시작됩니다. 이 라우트에 대한 모든 연결이 종료됩니다.

SSLClientSiteLabel

이 등록 정보는 레이블 이름을 지정하여 SSL 서버로 송신할 인증을 선택하는 데 사용합니다. 이 등록 정보를 지정하지 않으면 ″레이블 이름″을 의미하게 됩니다. 이 등록 정보가 변경되고(SSLClient가 참으로 설정되어 있으면) REFRESH 명령이 발행될 때 라우트가 정지되었다가 재시작됩니다. 이 라우트에 대한 모든 연결이 종료됩니다.

SSLProxyMode

라우트가 SSL 클라이언트 연결 요청만을 승인하고 목적지에 대해 직접 요청을 터널링하도록 하려면 이 등록 정보를 참으로 설정하십시오. 이 등록 정보가 변경되면 REFRESH 명령이 발행될 때 라우트가 정지되었다가 재시작됩니다. 이 라우트에 대한 모든 연결이 종료됩니다. 이 등록 정보는 다음 등록 정보와 함께 사용할 수 없습니다.

- HTTP
- QoS
- SocksClient
- SSLClient
- SSLServer

SSLServer

라우트가 SSL 서버 역할을 하도록 하고 수신되는 SSL 연결을 승인하도록 하려면 이 등록 정보를 참으로 설정하십시오. 참으로 설정한다는 것은 호출자가 SSL 클라이언트 역할을 하는 또 다른 MQIPT라는 것을 의미합니다. 이 등록 정보가 변경

되면 REFRESH 명령이 발행될 때 라우트가 정지되었다가 재시작됩니다. 이 라우트에 대한 모든 연결이 종료됩니다. 이 등록 정보는 다음 등록 정보와 함께 사용할 수 없습니다.

- QoS
- SocksServer
- SSLProxyMode

SSLServerCAKeyRing

CA 인증이 있는 키 링 파일의 완전한 파일 이름으로, SSL 클라이언트에서 인증을 인증하는 데 사용됩니다. Windows 플랫폼에서는 파일 분리 문자로 반드시 두 개의 백 슬래시(\\)를 사용해야 합니다. 이 등록 정보가 변경되고(SSLServer가 참으로 설정되어 있으면) REFRESH 명령이 발행될 때 라우트가 정지되었다가 재시작됩니다. 이 라우트에 대한 모든 연결이 종료됩니다.

SSLServerCAKeyRingPW

서버 CA 키 링을 열기 위해 사용하는 암호를 포함한 완전한 파일 이름입니다. Windows 플랫폼에서는 파일 분리 문자로 반드시 두 개의 백 슬래시(\\)를 사용해야 합니다. 이 등록 정보가 변경되고(SSLServer가 참으로 설정되어 있으면) REFRESH 명령이 발행될 때 라우트가 정지되었다가 재시작됩니다. 이 라우트에 대한 모든 연결이 종료됩니다.

SSLServerAskClientAuth

SSL 서버에 의한 SSL 클라이언트 인증을 요청하려면 이 등록 정보를 사용하십시오. SSL 클라이언트는 반드시 SSL 서버에 송신하기 위해 자체 인증이 있어야 합니다. 인증은 키 링 파일로부터 검색됩니다. 이 등록 정보가 변경되고(SSLServer가 참으로 설정되어 있으면) REFRESH 명령이 발행될 때 라우트가 정지되었다가 재시작됩니다. 이 라우트에 대한 모든 연결이 종료됩니다.

SSLServerCipherSuites

SSL 서버 측에서 사용하는 SSL 암호 모음의 이름입니다. 하나 이상의 지원되는 암호 모음이 될 수 있습니다. 이 등록 정보를 공백으로 두면 SSL 서버가 SSLServerKeyRing으로부터 지원되는 암호 모음을 사용합니다. 이 등록 정보가 변경되고(SSLServer가 참으로 설정되어 있으면) REFRESH 명령이 발행될 때 라우트가 정지되었다가 재시작됩니다. 이 라우트에 대한 모든 연결이 종료됩니다.

SSLServerDN_C

해당 국가 이름의 SSL 클라이언트로부터 수신되는 인증을 승인하려면 이 등록 정보를 사용하십시오. 범위를 확장하기 위해 이름의 접두부나 접미부에 별표(*)를 사용할 수 있습니다. 이 등록 정보를 지정하지 않으면 “전체 회사 이름”을 의미하게 됩니다. 이 등록 정보가 변경되고 (SSLServer가 참으로 설정되어 있으면) REFRESH 명령이 발행될 때 라우트가 정지되었다가 재시작됩니다. 이 라우트에 대한 모든 연결이 종료됩니다.

SSLServerDN_CN

해당 공용 이름의 SSL 클라이언트로부터 수신되는 인증을 승인하려면 이 등록 정보를 사용하십시오. 범위를 확장하기 위해 이름의 접두부나 접미부에 별표(*)를 사용할 수 있습니다. 이 등록 정보를 지정하지 않으면 "전체 공용 이름"을 의미하게 됩니다. 이 등록 정보가 변경되고 (SSLServer가 참으로 설정되어 있으면) REFRESH 명령이 발행될 때 라우트가 정지되었다가 재시작됩니다. 이 라우트에 대한 모든 연결이 종료됩니다.

SSLServerDN_L

해당 위치의 SSL 클라이언트로부터 수신되는 인증을 승인하려면 이 등록 정보를 사용하십시오. 범위를 확장하기 위해 이름의 접두부나 접미부에 별표(*)를 사용할 수 있습니다. 이 등록 정보를 지정하지 않으면 "전체 위치"를 의미하게 됩니다. 이 등록 정보가 변경되고 (SSLServer가 참으로 설정되어 있으면) REFRESH 명령이 발행될 때 라우트가 정지되었다가 재시작됩니다. 이 라우트에 대한 모든 연결이 종료됩니다.

SSLServerDN_O

해당 조직의 SSL 클라이언트로부터 수신되는 인증을 승인하려면 이 등록 정보를 사용하십시오. 범위를 확장하기 위해 이름의 접두부나 접미부에 별표(*)를 사용할 수 있습니다. 이 등록 정보를 지정하지 않으면 "전체 조직"을 의미하게 됩니다. 이 등록 정보가 변경되고 (SSLServer가 참으로 설정되어 있으면) REFRESH 명령이 발행될 때 라우트가 정지되었다가 재시작됩니다. 이 라우트에 대한 모든 연결이 종료됩니다.

SSLServerDN_OU

해당 조직 단위의 SSL 클라이언트로부터 수신되는 인증을 승인하려면 이 등록 정보를 사용하십시오. 범위를 확장하기 위해 이름의 접두부나 접미부에 별표(*)를 사용할 수 있습니다. 이 등록 정보를 지정하지 않으면 "전체 조직 단위"를 의미하게 됩니다. 이 등록 정보가 변경되고 (SSLServer가 참으로 설정되어 있으면) REFRESH 명령이 발행될 때 라우트가 정지되었다가 재시작됩니다. 이 라우트에 대한 모든 연결이 종료됩니다.

SSLServerDN_ST

해당 상태의 SSL 클라이언트로부터 수신되는 인증을 승인하려면 이 등록 정보를 사용하십시오. 범위를 확장하기 위해 이름의 접두부나 접미부에 별표(*)를 사용할 수 있습니다. 이 등록 정보를 지정하지 않으면 "전체 상태"를 의미하게 됩니다. 이 등록 정보가 변경되고 (SSLServer가 참으로 설정되어 있으면) REFRESH 명령이 발행될 때 라우트가 정지되었다가 재시작됩니다. 이 라우트에 대한 모든 연결이 종료됩니다.

SSLServerKeyRing

서버 인증을 포함한 키 링의 파일의 완전한 파일 이름입니다. **Windows 플랫폼에서는** 파일 분리 문자로 반드시 두 개의 백 슬래시(\\)를 사용해야 합니다.

SSLServer를 참으로 설정한 경우에는 반드시 SSLServerKeyRing을 지정해야 합니다. 이 등록 정보가 변경되고(SSLServer가 참으로 설정되어 있으면) REFRESH 명령이 발행될 때 라우트가 정지되었다가 재시작됩니다. 이 라우트에 대한 모든 연결이 종료됩니다.

SSLServerKeyRingPW

서버 키 링을 열기 위해 사용하는 암호를 포함한 완전한 파일 이름입니다. **Windows 플랫폼에서는** 파일 분리 문자로 반드시 두 개의 백 슬래시(\\)를 사용해야 합니다. SSLServer를 참으로 설정한 경우에는 반드시 SSLServerKeyRingPW를 지정해야 합니다. 이 등록 정보가 변경되고(SSLServer가 참으로 설정되어 있으면) REFRESH 명령이 발행될 때 라우트가 정지되었다가 재시작됩니다. 이 라우트에 대한 모든 연결이 종료됩니다.

SSLServerSiteDN_C

이 등록 정보는 국가 이름을 지정하여 SSL 클라이언트로 송신할 인증을 선택하는 데 사용합니다. 이 등록 정보를 지정하지 않으면 ″국가 이름″을 의미하게 됩니다. 이 등록 정보가 변경되고(SSLServer가 참으로 설정되어 있으면) REFRESH 명령이 발행될 때 라우트가 정지되었다가 재시작됩니다. 이 라우트에 대한 모든 연결이 종료됩니다.

SSLServerSiteDN_CN

이 등록 정보는 공용 이름을 지정하여 SSL 클라이언트로 송신할 인증을 선택하는 데 사용합니다. 이 등록 정보를 지정하지 않으면 ″공용 이름″을 의미하게 됩니다. 이 등록 정보가 변경되고 (SSLServer가 참으로 설정되어 있으면) REFRESH 명령이 발행될 때 라우트가 정지되었다가 재시작됩니다. 이 라우트에 대한 모든 연결이 종료됩니다.

SSLServerSiteDN_L

이 등록 정보는 위치 이름을 지정하여 SSL 클라이언트로 송신할 인증을 선택하는 데 사용합니다. 이 등록 정보를 지정하지 않으면 ″위치 이름″을 의미하게 됩니다. 이 등록 정보가 변경되고 (SSLServer가 참으로 설정되어 있으면) REFRESH 명령이 발행될 때 라우트가 정지되었다가 재시작됩니다. 이 라우트에 대한 모든 연결이 종료됩니다.

SSLServerSiteDN_O

이 등록 정보는 조직 이름을 지정하여 SSL 클라이언트로 송신할 인증을 선택하는 데 사용합니다. 이 등록 정보를 지정하지 않으면 ″조직 이름″을 의미하게 됩니다. 이 등록 정보가 변경되고(SSLServer가 참으로 설정되어 있으면) REFRESH 명령이 발행될 때 라우트가 정지되었다가 재시작됩니다. 이 라우트에 대한 모든 연결이 종료됩니다.

SSLServerSiteDN_OU

이 등록 정보는 조직 단위 이름을 지정하여 SSL 클라이언트로 송신할 인증을 선택하는 데 사용합니다. 이 등록 정보를 지정하지 않으면 ″조직 단위 이름″을 의미하

게 됩니다. 이 등록 정보가 변경되고(SSLServer가 참으로 설정되어 있으면) REFRESH 명령이 발행될 때 라우트가 정지되었다가 재시작됩니다. 이 라우트에 대한 모든 연결이 종료됩니다.

SSLServerSiteDN_ST

이 등록 정보는 상태 이름을 지정하여 SSL 클라이언트로 송신할 인증을 선택하는 데 사용합니다. 이 등록 정보를 지정하지 않으면 ″상태 이름″을 의미하게 됩니다. 이 등록 정보가 변경되고(SSLServer가 참으로 설정되어 있으면) REFRESH 명령이 발행될 때 라우트가 정지되었다가 재시작됩니다. 이 라우트에 대한 모든 연결이 종료됩니다.

SSLServerSiteLabel

이 등록 정보는 레이블 이름을 지정하여 SSL 클라이언트로 송신할 인증을 선택하는 데 사용합니다. 이 등록 정보를 지정하지 않으면 ″레이블 이름″을 의미하게 됩니다. 이 등록 정보가 변경되고(SSLServer가 참으로 설정되어 있으면) REFRESH 명령이 발행될 때 라우트가 정지되었다가 재시작됩니다. 이 라우트에 대한 모든 연결이 종료됩니다.

Trace

필요한 추적 레벨은 0-5 범위에서 정수 단위로 지정될 수 있습니다. 0 값은 추적이 없음을 의미합니다. 5는 전체 추적을 요청합니다.

이 등록 정보에 대한 변경이 라우트에 적용되면 REFRESH 명령이 발행될 때 새 값이 사용됩니다. 모든 연결은 즉시 새 값을 선택합니다. 라우트가 종료되지 않습니다.

UriName

이 등록 정보는 디폴트 값으로 최적의 구성이 되었음에도 불구하고 HTTP 프록시 또는 MQIPT servlet을 사용할 때 자원의 URI(Uniform Resource Identifier) 이름을 변경하는 데 사용됩니다. HTTP 프록시에 대한 디폴트 값은 다음과 같습니다.

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

MQIPT servlet에 대한 디폴트 값은 다음과 같습니다.

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

이 등록 정보를 변경하고 HTTP 또는 ServletClient가 참으로 설정되어 있으면 REFRESH 명령이 발행될 때 라우트가 정지되었다가 재시작됩니다.

제 20 장 internet pass-thru 시작하기

이 장에서는 MQIPT 시작하기에 대한 도움말을 제공합니다. 즉, 일부 간단한 구성을 설정하여 제품이 성공적으로 설치될 수 있도록 해줍니다.

이 장은 다음과 같은 절로 구성됩니다.

가정

각 예에서 다음과 같은 가정을 합니다.

- 해당 예가 지원되는 다른 플랫폼에서 실행되고 있더라도 사용자가 Windows NT를 사용하고 있다고 가정합니다.
- WebSphere MQ에서의 큐 관리자, 큐 및 채널 정의에 익숙하다고 가정합니다.
- 이미 WebSphere MQ 클라이언트와 서버를 설치하였다고 가정합니다.
- MQIPT가 Windows에서 C:\mqipt라는 디렉토리에 설치되었다고 가정합니다.
- 클라이언트, 서버 및 각 MQIPT가 별도의 시스템에 설치되어 있다고 가정합니다.
- amqsputc 명령을 사용하여 큐에 메시지를 넣어두는 데 익숙하다고 가정합니다.
- amqsgetc 명령을 사용하여 큐에서 메시지를 가져오는 데 익숙하다고 가정합니다.

WebSphere MQ 서버에서 다음을 수행하였다고 가정합니다.

- MQIPT.QM1이라는 큐 관리자 정의
- MQIPT.CONN.CHANNEL이라는 서버 연결 채널 정의
- MQIPT.LOCAL.QUEUE라는 로컬 큐 정의
- 1414 포트에서 MQIPT.QM1에 대한 TCP/IP 리스너 시작

동일한 시스템의 지정된 포트 주소에서는 하나의 응용프로그램만이 대기할 수 있습니다. 1414 포트가 이미 사용 중인 경우에는 사용할 수 있는 포트 주소를 선택하여 다음 예에서 대신 사용하십시오.

일단 이 작업을 수행하였으면 amqsputc 명령을 사용하여 큐 관리자의 로컬 큐에 메시지를 넣고 amqsgetc 명령을 사용하여 검색함으로서 WebSphere MQ 클라이언트로부터 큐 관리자에 대한 라우트를 테스트할 수 있습니다.

구성 예

다음 예는 다이어그램 및 단계별 지시사항으로 표현되며 각 다이어그램의 오른쪽에 있는 체크 표시 상자를 사용하여 예에서의 진행 상황을 살펴볼 수 있습니다. 일부 예에서는 MQIPT 홈 디렉토리에 있는 mqipt.conf 파일을 편집해야 합니다.

시작하기 전에 다음을 수행하였는지 확인하십시오.

- mqipt.conf에 mqiptSample.conf 복사
- mqipt.conf 편집 및 라우트 모두 삭제
- ClientAccess의 입력을 참으로 변경
- Destination을 mqserver.company2.com에서 사용자의 큐 관리자의 Destination으로 변경
- DestinationPort 주소를 사용자의 큐 관리자가 사용하는 것으로 변경
- 103 페이지의 『가정』 읽기

설치 확인 테스트

다음은 MQIPT가 올바르게 설치되었는지 확인할 수 있는 간단한 구성입니다.

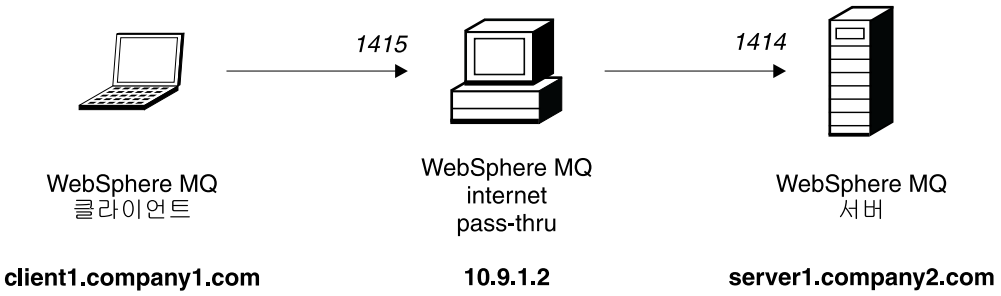

그림 10. IVT 네트워크 다이어그램

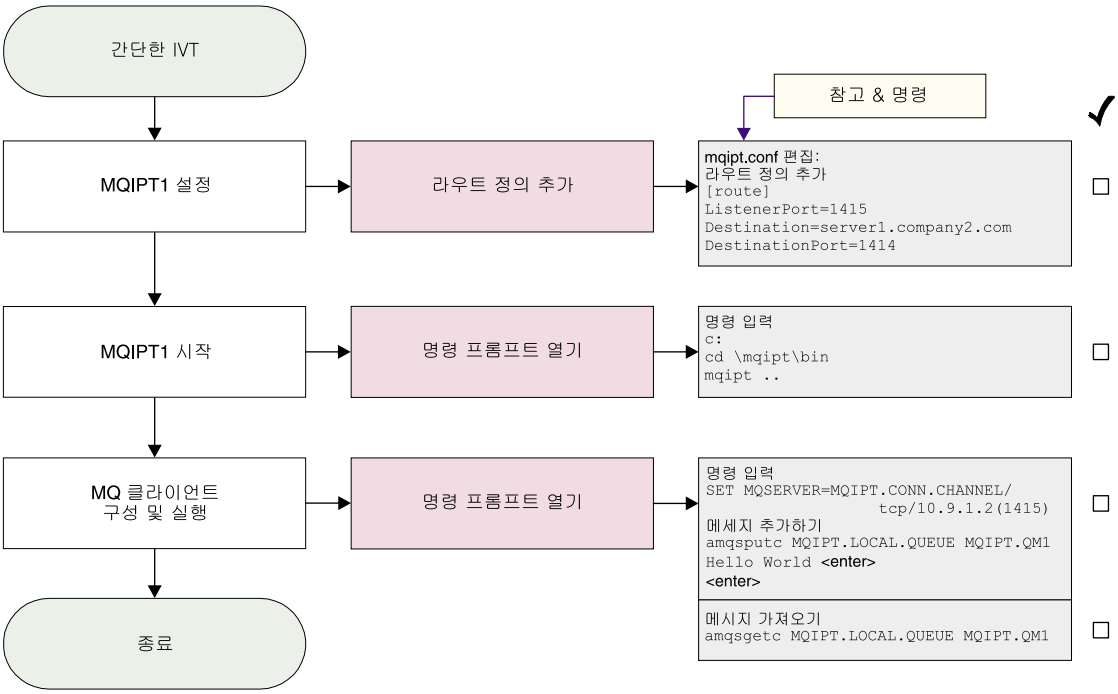

그림 11. IVT 구성

1. MQIPT1을 설정합니다.

   mqipt.conf를 편집하고 라우트 정의를 추가합니다.

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

2. MQIPT1을 시작합니다.

   명령 프롬프트를 열고 다음을 입력합니다.

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

다음 메시지가 표시되면 성공적으로 완료되었다는 것을 알 수 있습니다.

```
5639-L92 (C) Copyright IBM Corp. 2000, 2003 All Rights Reserved
MQCPI001 WebSphere MQ internet pass-thru Version 1.3.0 starting
MQCPI004 Reading configuration information from C:\mqipt\mqipt.conf
MQCPI011 The path C:\mqipt\logs will be used to store the log files
MQCPI006 Route 1415 has started and will forward messages to :
MQCPI034 ....server1.company2.com(1414)
MQCPI035 ....using MQ protocols
MQCPI078 Route 1415 ready for connection requests
```

3. WebSphere MQ 클라이언트 시스템의 명령 프롬프트에 다음을 입력합니다.

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

4. 다음을 사용하여 메시지를 넣습니다.

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

5. 다음을 사용하여 메시지를 가져옵니다.

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

그러면 "Hello world"를 볼 수 있습니다.

SSL 서버 인증

이 예에서는 두 개의 MQIPT를 통해 WebSphere MQ 클라이언트를 WebSphere MQ 서버에 연결함으로써 샘플 테스트 인증(sslsample.pfx 키 링 파일)을 사용하여 SSL 연결을 테스트합니다. SSL 데이터 교환 동안 서버가 테스트 인증을 클라이언트에 송신합니다. 클라이언트는 trust-as-peer 플래그와 함께 인증의 사본을 사용하여 서버를 인증합니다. 이 때 디폴트 암호 모음인 SSL_RSA_WITH_RC4_128_MD5가 사용됩니다 (105 페이지의 『설치 확인 테스트』에서 작성된 mqipt.conf를 기본으로 함). 테스트 인증을 작성하여 예에서 사용하는 방법에 대한 자세한 내용은 125 페이지의 『SSL 테스트 인증 작성』을 참조하십시오.

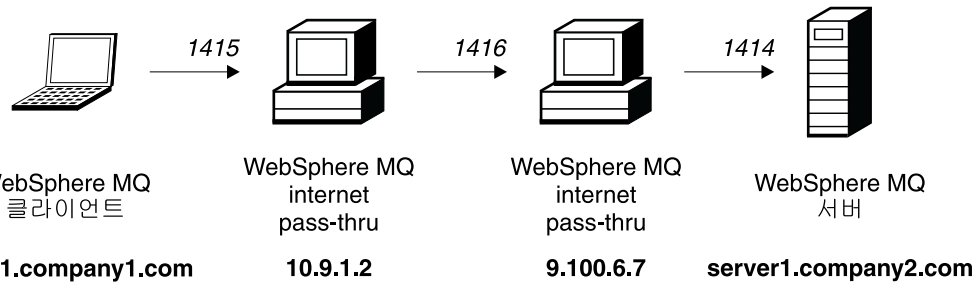

그림 12. SSL 서버 네트워크 다이어그램

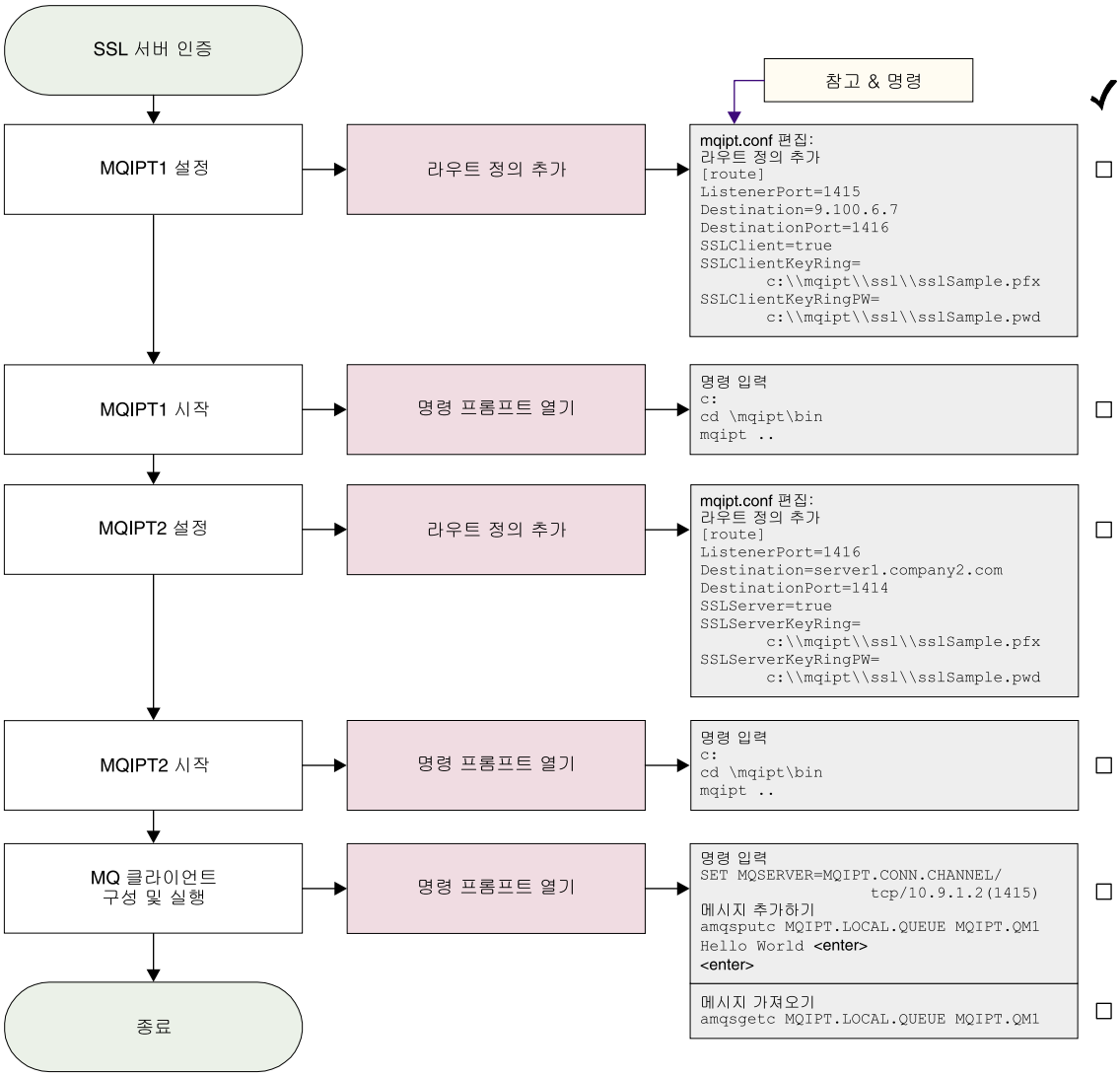

그림 13. SSL 서버 인증

1. MQIPT1을 설정합니다.

   mqipt.conf를 편집하고 라우트 정의를 추가합니다.

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

2. MQIPT1을 시작합니다.

   명령 프롬프트를 열고 다음을 입력합니다.

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

다음 메시지가 표시되면 성공적으로 완료되었다는 것을 알 수 있습니다.

```
5639-L92 (C) Copyright IBM Corp. 2000, 2003 All Rights Reserved
MQCPI001 WebSphere MQ internet pass-thru Version 1.3.0 starting
MQCPI011 The path c:\mqipt\logs will be used to store the log files
MQCPI006 Route 1415 has started and will forward messages to :
MQCPI034 ....9.100.6.7(1416)
MQCPI035 ....using MQ protocols
MQCPI036 ....SSL Client side enabled with properties :
MQCPI031 ......cipher suites <null>
MQCPI032 ......keyring file c:\mqipt\sslSample.pfx
MQCPI047 ......CA keyring file <null>
MQCPI038 ......distinguished name(s) CN=* O=* OU=* L=* ST=* C=*
MQCPI078 Route 1415 ready for connection requests
```

3. MQIPT2를 설정합니다.

   mqipt.conf를 편집하고 라우트 정의를 추가합니다.

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

4. MQIPT2를 시작합니다.

   명령 프롬프트를 열고 다음을 입력합니다.

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

   다음 메시지가 표시되면 성공적으로 완료되었다는 것을 알 수 있습니다.

   ```
   5639-L92 (C) Copyright IBM Corp. 2000, 2003 All Rights Reserved
   MQCPI001 WebSphere MQ internet pass-thru Version 1.3.0 starting
   MQCPI011 The path c:\mqipt\logs will be used to store the log files
   MQCPI006 Route 1416 has started and will forward messages to :
   MQCPI034 ....server1.company2.com(1414)
   MQCPI035 ....using MQ protocols
   MQCPI037 ....SSL Server side enabled with properties :
   MQCPI031 ......cipher suites <null>
   MQCPI032 ......keyring file c:\mqipt\sslSample.pfx
   MQCPI047 ......CA keyring file <null>
   MQCPI038 ......distinguished name(s) CN=* O=* OU=* L=* ST=* C=*
   MQCPI033 ......client authentication set to false
   MQCPI078 Route 1416 ready for connection requests
   ```

5. WebSphere MQ 클라이언트 시스템의 명령 프롬프트에 다음을 입력합니다.

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

6. 다음을 사용하여 메시지를 넣습니다.

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

7. 다음을 사용하여 메시지를 가져옵니다.

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

그러면 ″Hello world″를 볼 수 있습니다.

SSL 클라이언트 인증

이 예에서는 샘플 테스트 인증을 사용하여 SSL 연결을 테스트합니다. 이 작업으로 서버 및 클라이언트 인증이 수행됩니다. SSL 데이터 교환 동안 서버가 테스트 인증을 클라이언트에 송신합니다. 클라이언트는 trust-as-peer 플래그와 함께 인증의 사본을 사용하여 서버를 인증합니다. 그런 다음, 클라이언트가 테스트 인증을 서버에 송신합니다. 서버는 trust-as-peer 플래그와 함께 인증의 사본을 사용하여 클라이언트를 인증합니다. 이때 디폴트 암호 모음인 SSL_RSA_WITH_RC4_128_MD5가 사용됩니다(105 페이지의 『설치 확인 테스트』에서 작성된 `mqipt.conf`를 기본으로 함).

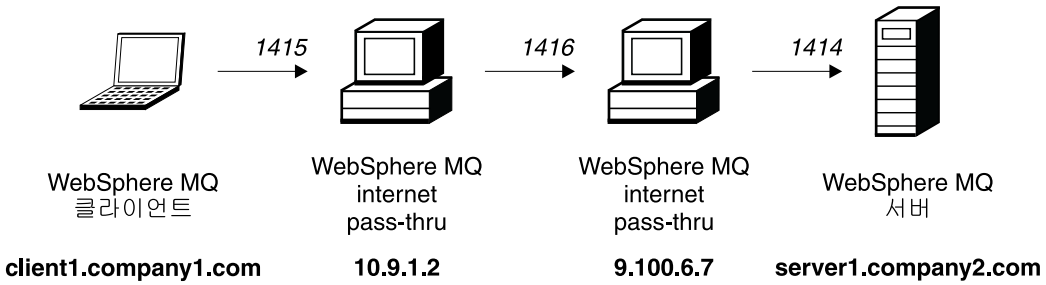

그림 14. SSL 클라이언트 네트워크 다이어그램

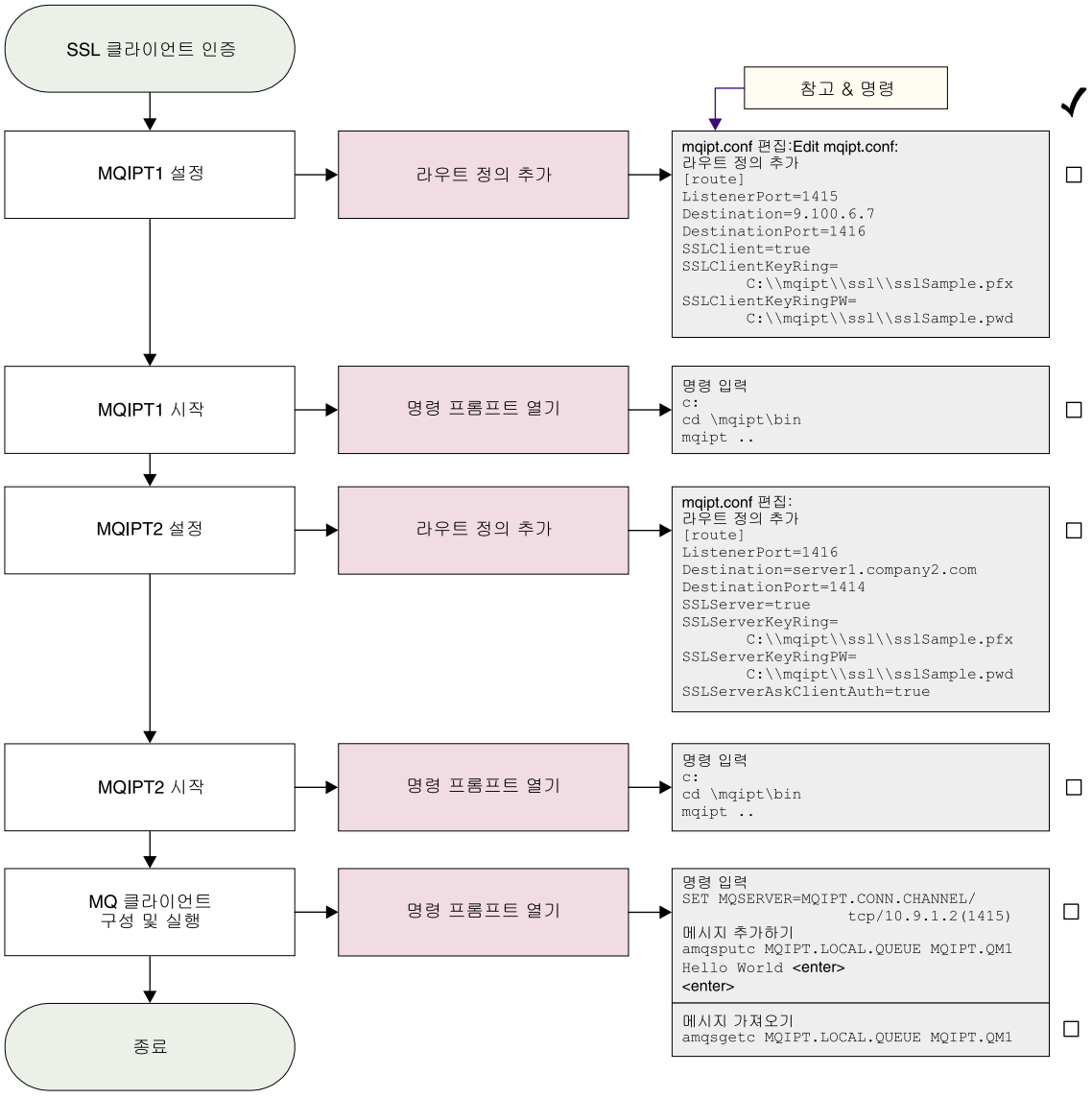

그림 15. SSL 클라이언트 인증

1. MQIPT1을 설정합니다.

   mqipt.conf를 편집하고 라우트 정의를 추가합니다.

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

2. MQIPT1을 시작합니다.

   명령 프롬프트를 열고 다음을 입력합니다.

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

다음 메시지가 표시되면 성공적으로 완료되었다는 것을 알 수 있습니다.

```
5639-L92 (C) Copyright IBM Corp. 2000, 2003 All Rights Reserved
MQCPI001 WebSphere MQ internet pass-thru Version 1.3.0 starting
MQCPI011 The path c:\mqipt\logs will be used to store the log files
MQCPI006 Route 1415 has started and will forward messages to :
MQCPI034 ....9.100.6.7(1416)
MQCPI035 ....using MQ protocols
MQCPI036 ....SSL Client side enabled with properties :
MQCPI031 ......cipher suites <null>
MQCPI032 ......keyring file c:\mqipt\sslSample.pfx
MQCPI047 ......CA keyring file <null>
MQCPI038 ......distinguished name(s) CN=* O=* OU=* L=* ST=* C=*
MQCPI078 Route 1415 ready for connection requests
```

3. MQIPT2를 설정합니다.

   mqipt.conf를 편집하고 라우트 정의를 추가합니다.

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

4. MQIPT2를 시작합니다.

   명령 프롬프트를 열고 다음을 입력합니다.

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

   다음 메시지가 표시되면 성공적으로 완료되었다는 것을 알 수 있습니다.

   ```
   5639-L92 (C) Copyright IBM Corp. 2000, 2003 All Rights Reserved
   MQCPI001 WebSphere MQ internet pass-thru Version 1.3.0 starting
   MQCPI011 The path c:\mqipt\logs will be used to store the log files
   MQCPI006 Route 1416 has started and will forward messages to :
   MQCPI034 ....server1.company2.com(1414)
   MQCPI035 ....using MQ protocols
   MQCPI037 ....SSL Server side enabled with properties :
   MQCPI031 ......cipher suites <null>
   MQCPI032 ......keyring file c:\mqipt\sslSample.pfx
   MQCPI047 ......CA keyring file <null>
   MQCPI038 ......distinguished name(s) CN=* O=* OU=* L=* ST=* C=*
   MQCPI033 ......client authentication set to true
   MQCPI078 Route 1416 ready for connection requests
   ```

5. WebSphere MQ 클라이언트 시스템의 명령 프롬프트에 다음을 입력합니다.

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

6. 다음을 사용하여 메시지를 넣습니다.

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

7. 다음을 사용하여 메시지를 가져옵니다.

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

그러면 ″Hello world″를 볼 수 있습니다.

HTTP 프록시 구성

이 예에서는 HTTP 프록시(IBM 캐싱 프록시)를 사용하여 연결을 테스트합니다. CP 레벨이 3.6 이상이어야 하며 다음을 점검해야 합니다.

- `ProxyPersistence`는 반드시 지속적 연결을 허용하는 `on`이어야 합니다.
- `MaxPersistRequest 5000`은 연결이 중단되기 전에 단일 연결에 허용하도록 하는 요청 수입니다.
- `PersistTimeout 12`는 연결 종료를 허용하는 시간입니다.

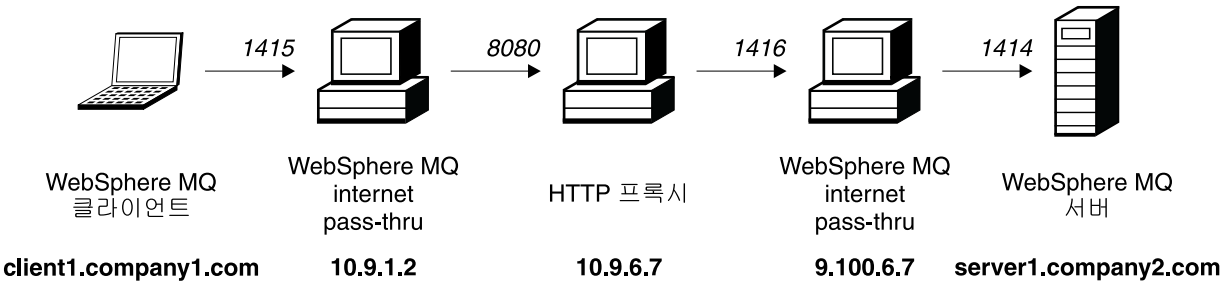

그림 16. HTTP 프록시 네트워크 다이어그램

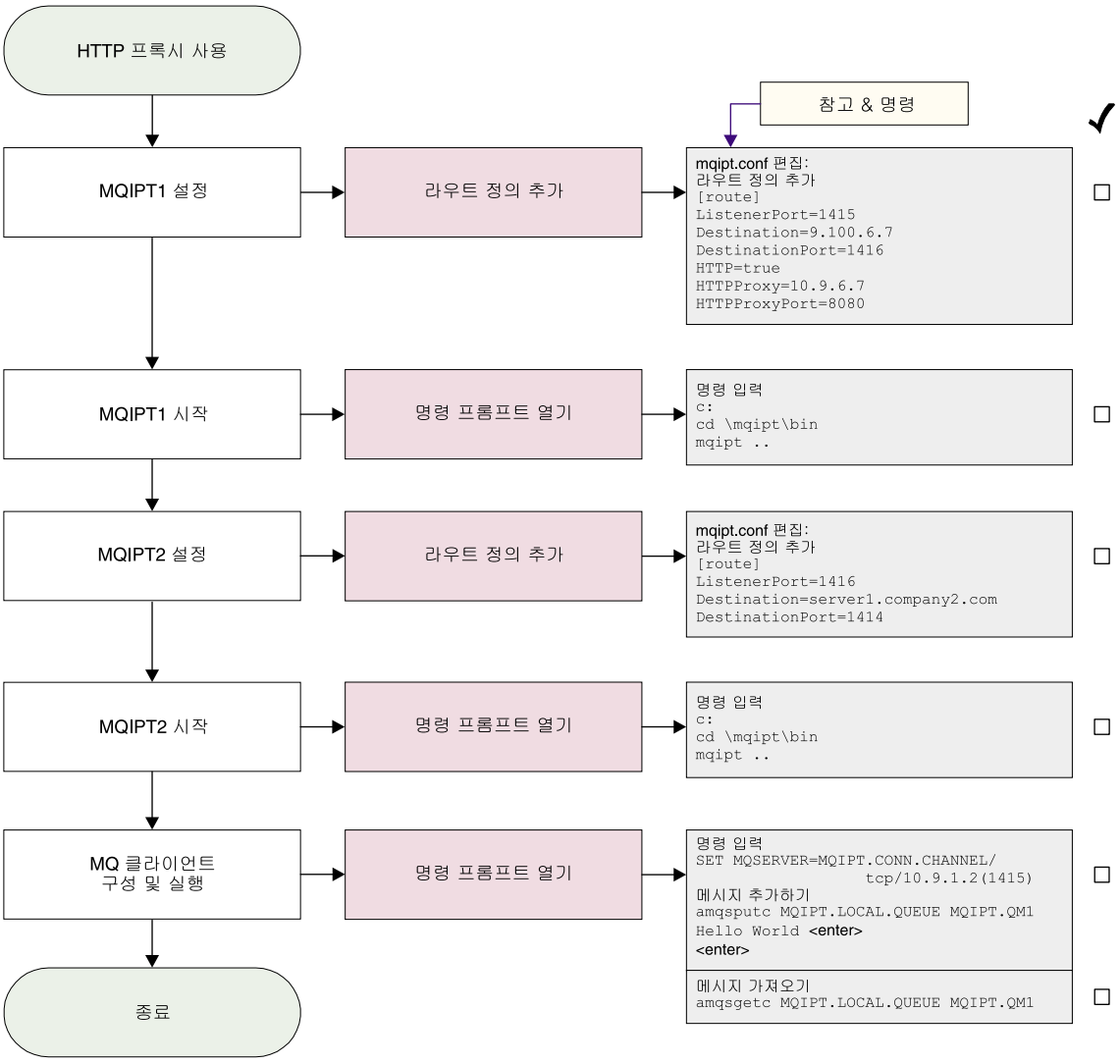

그림 17. HTTP 프록시 구성

1. MQIPT1을 설정합니다.

   mqipt.conf를 편집하고 라우트 정의를 추가합니다.

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

2. MQIPT1을 시작합니다.

   명령 프롬프트를 열고 다음을 입력합니다.

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

   다음 메시지가 표시되면 성공적으로 완료되었다는 것을 알 수 있습니다.

```
5639-L92 (C) Copyright IBM Corp. 2000, 2003 All Rights Reserved
MQCPI001 WebSphere MQ internet pass-thru Version 1.3.0 starting
MQCPI004 Reading configuration information from C:\mqipt\mqipt.conf
MQCPI011 The path C:\mqipt\logs will be used to store the log files
MQCPI006 Route 1415 has started and will forward messages to :
MQCPI034 ....9.100.6.7(1416)
MQCPI035 ....using HTTP
MQCPI024 ....and HTTP proxy at 10.9.6.7(1080)
MQCPI078 Route 1415 ready for connection requests
```

3. MQIPT2를 설정합니다.

   mqipt.conf를 편집하고 라우트 정의를 추가합니다.

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

4. MQIPT2를 시작합니다.

   명령 프롬프트를 열고 다음을 입력합니다.

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

   다음 메시지가 표시되면 성공적으로 완료되었다는 것을 알 수 있습니다.

   ```
   5639-L92 (C) Copyright IBM Corp. 2000, 2003 All Rights Reserved
   MQCPI001 WebSphere MQ internet pass-thru Version 1.3.0 starting
   MQCPI004 Reading configuration information from C:\mqipt\mqipt.conf
   MQCPI011 The path C:\mqipt\logs will be used to store the log files
   MQCPI006 Route 1416 has started and will forward messages to :
   MQCPI034 ....server1.company2.com(1414)
   MQCPI035 ....using MQ protocols
   MQCPI078 Route 1416 ready for connection requests
   ```

5. WebSphere MQ 클라이언트 시스템의 명령 프롬프트에 다음을 입력합니다.

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

6. 다음을 사용하여 메시지를 넣습니다.

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

7. 다음을 사용하여 메시지를 가져옵니다.

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

그러면 "Hello world"를 볼 수 있습니다.

액세스 제어 구성

이 예에서는 Java 보안 관리자를 사용하여 MQIPT 리스너 포트에 보안 점검을 추가하여 특정한 클라이언트로부터의 연결만을 승인하도록 MQIPT를 설정합니다.

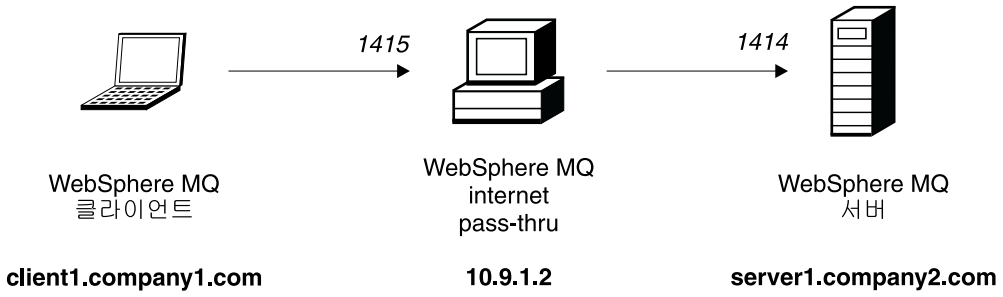

그림 18. 액세스 제어 네트워크 다이어그램

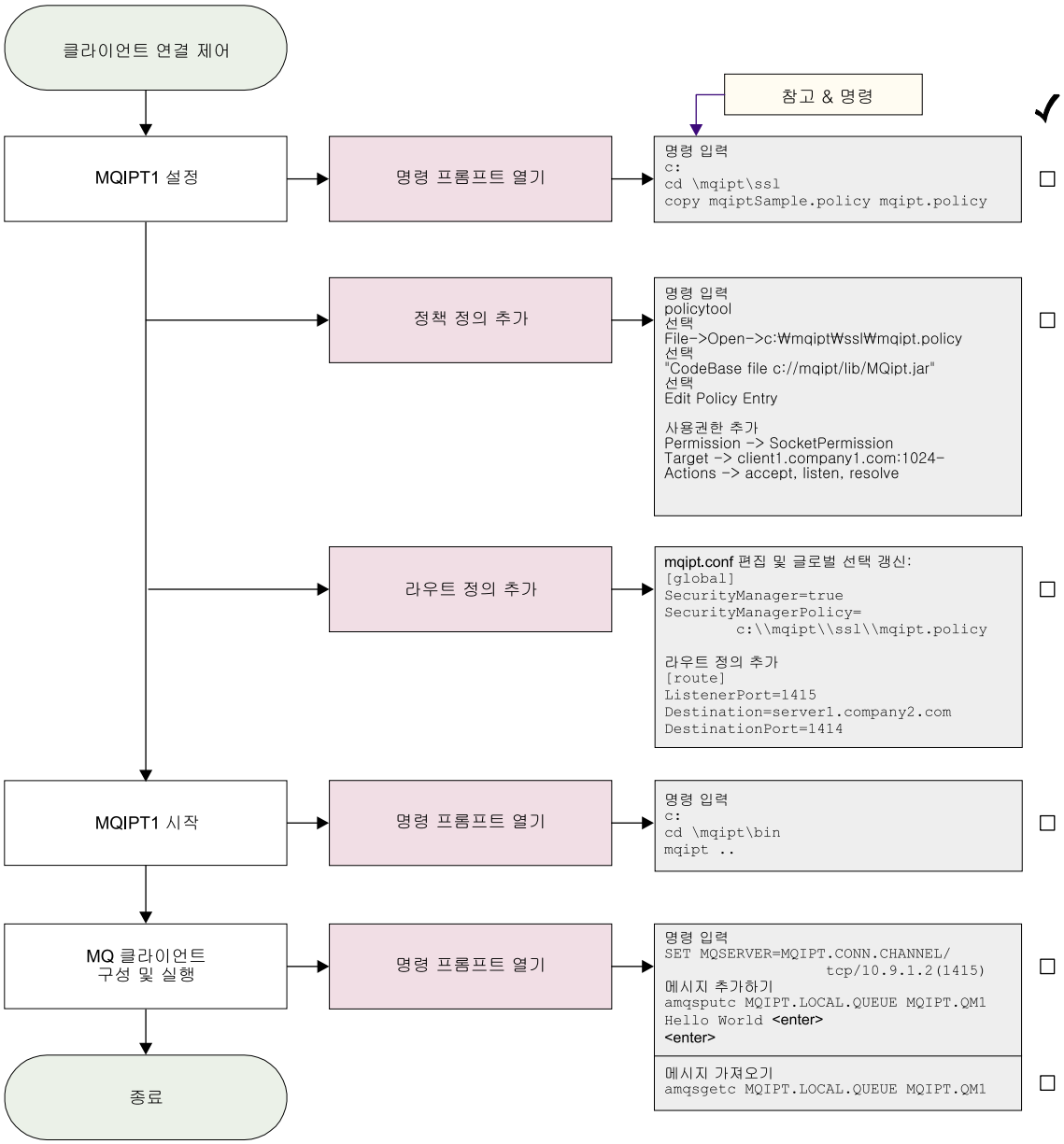

그림 19. 액세스 제어 구성

1. MQIPT1을 설정합니다.
   a. 명령 프롬프트를 열고 다음을 입력합니다.

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

   b. 다음 명령을 사용하여 정책 정의를 추가합니다.

      ```
      policytool
      ```

      1) 파일 -> 열기 -> c:\mqipt\ssl\mqipt.policy를 선택합니다.
      2) 다음을 선택합니다.

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

      3) 다음에서 CodeBase를 변경합니다.

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

         다음과 같이 변경합니다.

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

      4) 다음에서 모든 권한을 변경합니다.

         ```
         C:\\Program Files\\IBM\\WebSphere MQ internet pass-thru
         ```

         다음과 같이 변경합니다.

         ```
         C:\\mqipt
         ```

      5) SocketPermission을 추가합니다.

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

   c. mqipt.conf를 편집하고 다음을 추가합니다.
      1) 전역 섹션에 대한 두 개의 등록 정보

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

      2) 라우트 정의

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

2. MQIPT1을 시작합니다.

   명령 프롬프트를 열고 다음을 입력합니다.

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

   다음 메시지가 표시되면 성공적으로 완료되었다는 것을 알 수 있습니다.

```
5639-L92 (C) Copyright IBM Corp. 2000, 2003 All Rights Reserved
MQCPI001 WebSphere MQ internet pass-thru Version 1.3.0 starting
MQCPI004 Reading configuration information from C:\mqipt\mqipt.conf
MQCPI055 Setting the java.security.policy to c:\mqipt\mqipt.policy
MQCPI053 Starting the Java Security Manager
MQCPI011 The path C:\mqipt\logs will be used to store the log files
MQCPI006 Route 1415 has started and will forward messages to :
MQCPI034 ....server1.company2.com(1414)
MQCPI035 ....using MQ protocols
MQCPI078 Route 1415 ready for connection requests
```

3. WebSphere MQ 클라이언트 시스템의 명령 프롬프트에 다음을 입력합니다.

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

4. 다음을 사용하여 메시지를 넣습니다.

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

5. 다음을 사용하여 메시지를 가져옵니다.

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

그러면 "Hello world"를 볼 수 있습니다.

Qos(Quality of Service) 구성

이 예에서는 TQoS가 이미 MQIPT와 동일한 기계에 설치되었다고 가정합니다.

이 예에서는 MQIPT 라우트 상의 모든 채널에 QoS(Quality of Service)를 적용합니다. 이는 MQIPT가 Linux 플랫폼에서 실행 중인 경우에만 구현될 수 있습니다. 이 샘플은 MQIPT로부터 WebSphere MQ 클라이언트에 송신되는 모든 데이터에 대한 우선순위를 "평균"으로 설정하고 WebSphere MQ 서버에 송신되는 모든 데이터에 대해 우선순위를 "높음"으로 설정합니다. 아래에 나열된 샘플 pagent 정책을 사용하여 다음 우선순위를 QosToCaller 및 QosToDest에 적용할 수 있습니다.

- 1 - 평균
- 2 - 높음
- 3 - 아주 높음

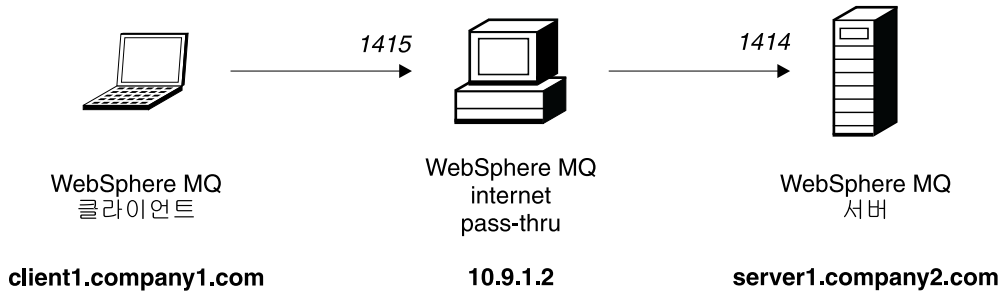

그림 20. QoS 네트워크 다이어그램

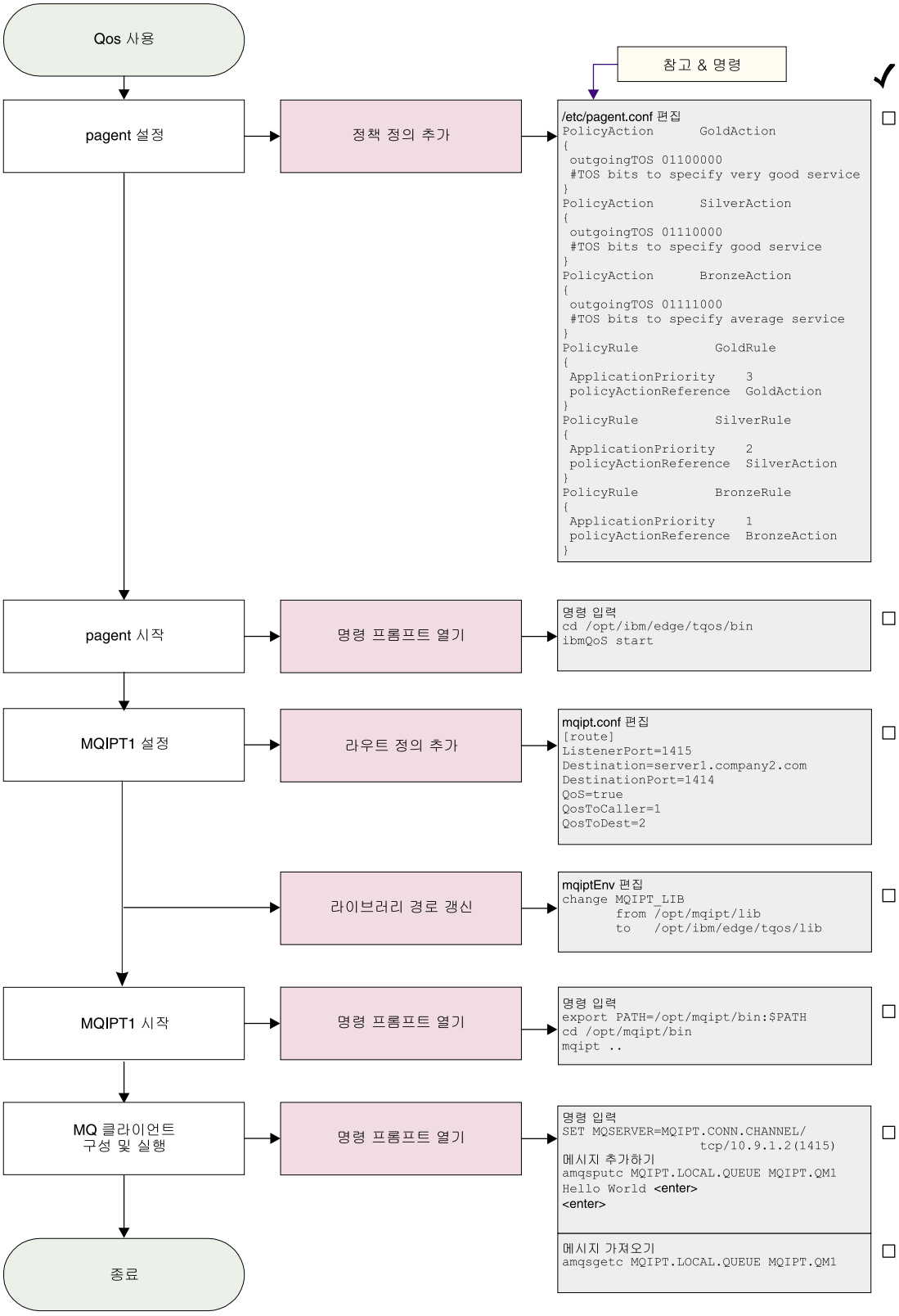

그림 21. QoS 구성

1. pagent를 설정합니다.

/etc/pagent.conf를 편집하고 다음을 추가합니다.

```
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
}
```

위에서 정의한 규칙에 대해 성능 데이터 콜렉션을 켜려면 명령문 PolicyPerformanceCollection을 사용하여 활성화하십시오. 이 명령문에 대한 설명과 형식은 Pagent.conf를 참조하십시오.

2. pagent를 시작합니다.

   명령 프롬프트를 열고 다음을 입력합니다.

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

3. MQIPT1을 설정합니다.

   mqipt.conf를 편집하고 라우트 정의를 추가합니다.

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

4. 라이브러리 경로를 갱신합니다.

   /opt/mqipt/bin에 있는 mqiptEnv를 편집하고 MQIPT_LIB를 변경합니다.

/opt/mqipt/lib에서

다음과 같이 변경합니다.

/opt/ibm/edge/tqos/lib

5. MQIPT1을 시작합니다.

명령 프롬프트를 열고 다음을 입력합니다.

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

다음 메시지가 표시되면 성공적으로 완료되었다는 것을 알 수 있습니다.

```
5639-L92 (C) Copyright IBM Corp. 2000, 2003 All Rights Reserved
MQCPI001 Websphere MQ internet pass-thru Version 1.3.0 starting
MQCPI004 Reading configuration information from /opt/mqipt/mqipt.conf
MQCPI011 The path /opt/mqipt/logs will be used to store the log files
MQCPI006 Route 1415 has started and will forward messages to :
MQCPI034 ....server1.company2.com(1414)
MQCPI035 ....using MQ protocols
MQCPI049 ....QoS priority to dest = 2, to caller = 1
MQCPI078 Route 1415 ready for connection requests
```

6. WebSphere MQ 클라이언트 시스템의 명령 프롬프트에 다음을 입력합니다.

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

7. 다음을 사용하여 메시지를 넣습니다.

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

8. 다음을 사용하여 메시지를 가져옵니다.

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

그러면 ″Hello world″를 볼 수 있습니다.

SOCKS 프록시 구성

다음 예에서는 MQIPT가 SOCKS 프록시 역할을 수행하도록 할 수 있습니다. WebSphere MQ 클라이언트는 이 샘플을 실행하기 전에 반드시 SOCKS화되어야 하며 SOCKS 구성은 반드시 SOCKS 프록시로 MQIPT를 지정해야 합니다.
MQIPTDestination 및 DestinationPort 등록 정보의 정의는 임의의 것이 될 수 있습니다. SOCKS 데이터 교환 프로세스 동안 WebSphere MQ 클라이언트로부터 진짜 목적지를 확보할 수 있습니다.

시작하기 전에 반드시 전체 시스템을 socks화하거나 WebSphere MQ 클라이언트 응용프로그램(amqsputc/amqsgetc)만을 socks화해야 합니다. 또한 반드시 SOCKS 클라이언트를 다음과 같이 구성해야 합니다.

- MQIPT가 SOCKS 프록시를 지정하도록 함

- Socks V5 지원 사용
- 사용자 인증 사용 안함
- MQIPT 네트워크 주소로만 연결되도록 함

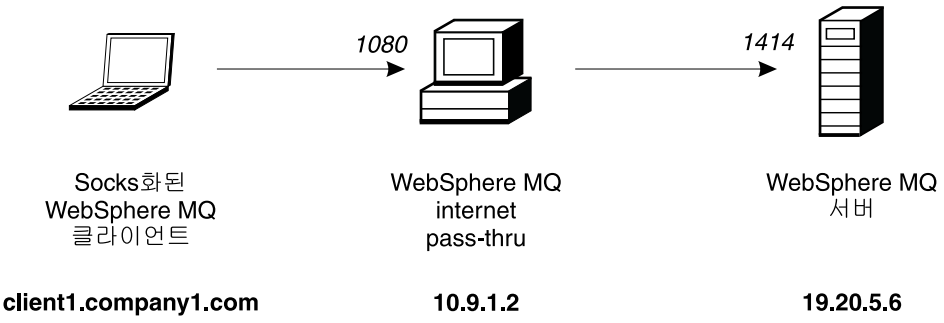

그림 22. SOCKS 프록시 네트워크 다이어그램

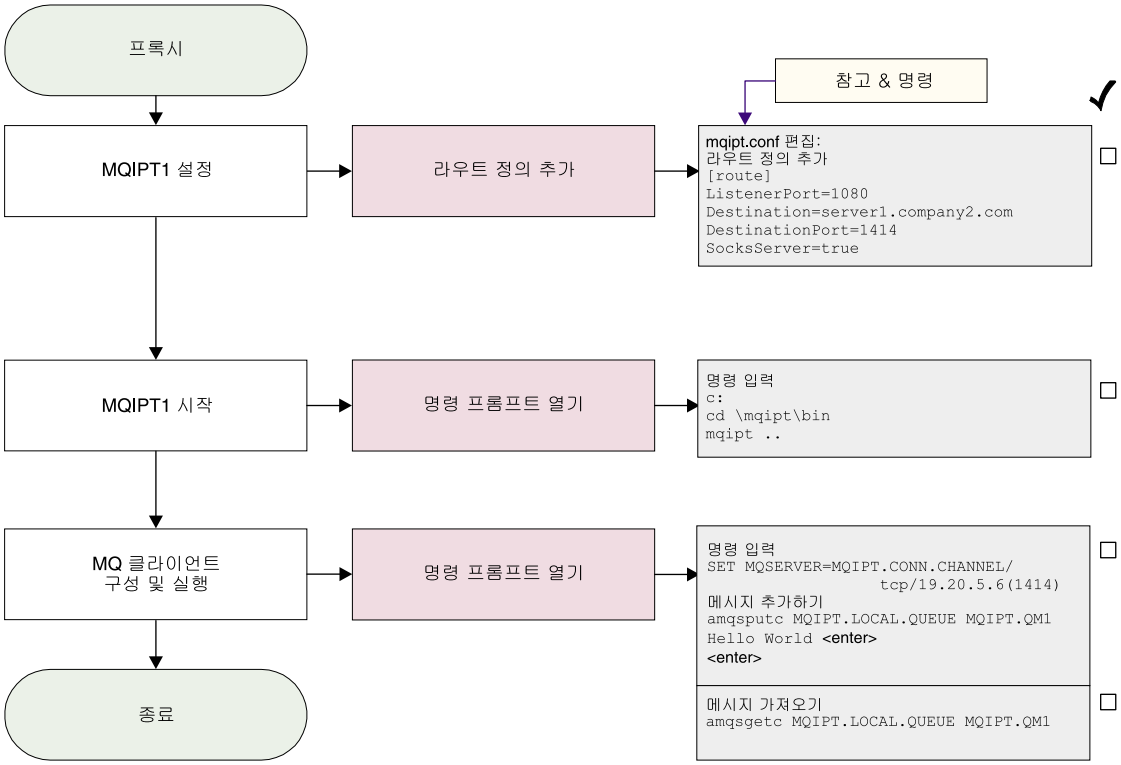

그림 23. SOCKS 프록시 구성

1. MQIPT1을 설정합니다.

   `mqipt.conf`를 편집하고 라우트 정의를 추가합니다.

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

2. MQIPT1을 시작합니다.

   명령 프롬프트를 열고 다음을 입력합니다.

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

   다음 메시지가 표시되면 성공적으로 완료되었다는 것을 알 수 있습니다.

```
5639-L92 (C) Copyright IBM Corp. 2000, 2003 All Rights Reserved
MQCPI001 WebSphere MQ internet pass-thru Version 1.3.0 starting
MQCPI004 Reading configuration information from C:\mqipt\mqipt.conf
MQCPI011 The path C:\mqipt\logs will be used to store the log files
MQCPI006 Route 1080 has started and will forward messages to :
MQCPI034 ....server1.company2.com(1414)
MQCPI035 ....using MQ protocols
MQCPI052 ....Socks server side enabled
MQCPI078 Route 1080 ready for connection requests
```

3. WebSphere MQ 클라이언트 시스템의 명령 프롬프트에 다음을 입력합니다.

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

4. 다음을 사용하여 메시지를 넣습니다.

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

5. 다음을 사용하여 메시지를 가져옵니다.

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

그러면 ″Hello world″를 볼 수 있습니다.

SOCKS 클라이언트 구성

이 예에서는 기존 SOCKS 프록시를 사용하여 MQIPT가 SOCKS화된 것처럼 실행합니다. 이 작업은 MQIPT가 WebSphere MQ 클라이언트 대신 SOCKS화된 연결을 만든다는 것을 제외하면 121 페이지의 『SOCKS 프록시 구성』과 유사합니다.

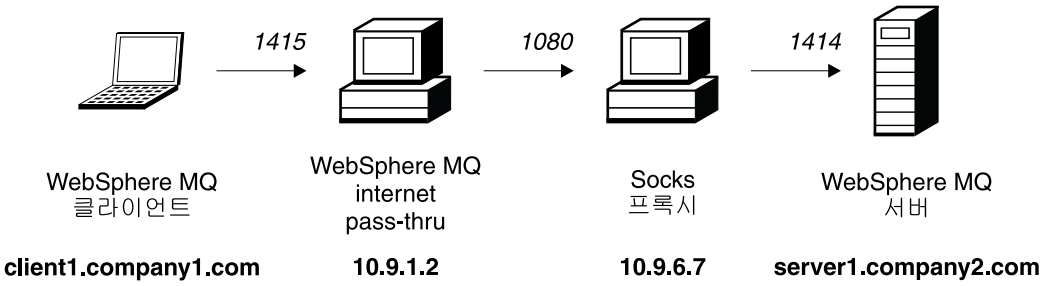

그림 24. SOCKS 클라이언트 네트워크 다이어그램

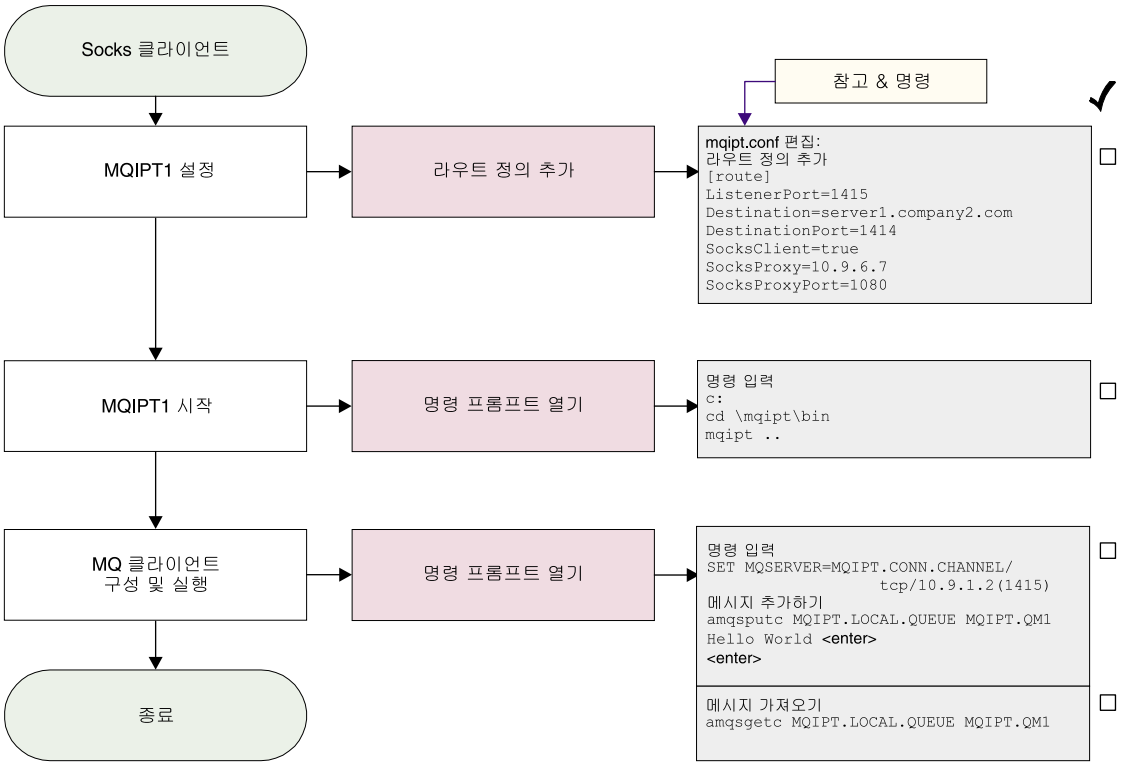

그림 25. SOCKS 클라이언트 구성

1. MQIPT1을 설정합니다.

   `mqipt.conf`를 편집하고 라우트 정의를 추가합니다.

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

2. MQIPT1을 시작합니다.

   명령 프롬프트를 열고 다음을 입력합니다.

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

다음 메시지가 표시되면 성공적으로 완료되었다는 것을 알 수 있습니다.

```
5639-L92 (C) Copyright IBM Corp. 2000, 2003 All Rights Reserved
MQCPI001 WebSphere MQ internet pass-thru Version 1.3.0 starting
MQCPI004 Reading configuration information from C:\mqipt\mqipt.conf
MQCPI022 Password checking has been disabled on the command port
MQCPI011 The path C:\mqipt\logs will be used to store the log files
MQCPI006 Route 1415 has started and will forward messages to :
MQCPI034 ....server1.company2.com(1414)
MQCPI035 ....using MQ protocols
MQCPI039 ....and Socks proxy at 10.9.6.7(1080)
MQCPI078 Route 1415 ready for connection requests
```

3. WebSphere MQ 클라이언트 시스템의 명령 프롬프트에 다음을 입력합니다.

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

4. 다음을 사용하여 메시지를 넣습니다.

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

5. 다음을 사용하여 메시지를 가져옵니다.

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

그러면 ″Hello world″를 볼 수 있습니다.

SSL 테스트 인증 작성

이 예에서는 MQIPT 라우트 테스트에 사용할 수 있는 자체 서명된 인증을 작성하는 방법을 보여줍니다. 인증은 trust-as-peer 플래그를 켭니다.

1. KeyMan을 시작합니다.
2. ″Create new...″를 선택합니다.
3. ″PKCS#12 Token″을 선택합니다.
4. ″Action -> Generate Key″를 선택합니다.

   목록에 다음과 같은 새 키 쌍이 표시됩니다. ″RSA / 1024-bit″
5. 새 키 쌍을 선택합니다.
6. ″Action -> Create Certificate″를 선택합니다.
7. ″Self-signed Certificate″를 선택합니다.
8. 인증 세부사항을 입력합니다.

   개인용 인증이 키와 함께 결합될 것이며 선택적으로 레이블을 입력하라는 대화 상자가 표시됩니다.
9. 새 인증을 선택합니다.

10. 인증 세부사항을 표시합니다.
11. 인증 등록 정보를 변경합니다.
12. trust-as-peer 플래그를 켭니다.
13. 대화 상자를 닫고 ″File -> Save″를 선택합니다.
14. 암호(myPassWord 등)를 입력합니다.
15. 새 키 링 파일의 파일 이름을 입력합니다. 예를 들어, c:\mqipt\ssl\testRoute1414.pfx 입니다.

    이 때, 반드시 ″파일 형식을 PKCS#12 / PFX″로 유지해야 합니다. - ″Wrap key ring into a Java class″를 선택하면 **안됩니다**.
16. 앞에서 사용한 암호 문구(myPassWord)를 포함한 텍스트 파일을 작성합니다.

    예를 들어, c:\mqipt\ssl\testRoute1414.pwd등입니다.

이제 106 페이지의 『SSL 서버 인증』의 예에서 이 키 링 파일을 사용할 수 있습니다.

MQIPT Servlet 구성

103 페이지의 『가정』 뿐만 아니라 이 예에서는 다음과 같이 가정합니다.

- Tomcat 응용프로그램 서버가 다음 디렉토리에 설치되었습니다.

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

  다음에서 Tomcat을 다운로드할 수 있습니다.

  ```
  http://jakarta.apache.org/builds/jakarta-tomcat-4.0/release/v4.0.3/
  ```
- IBM Web Traffic Express가 다음에 설치되었습니다.

  ```
  c:\wte
  ```

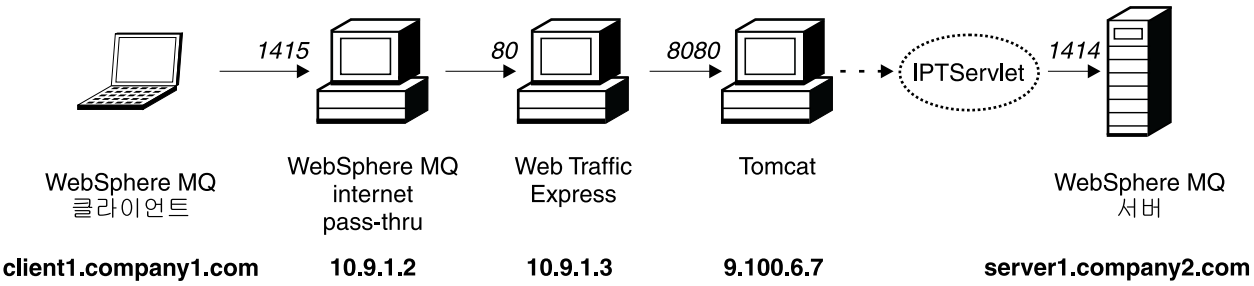

그림 26. Servlet 네트워크 다이어그램

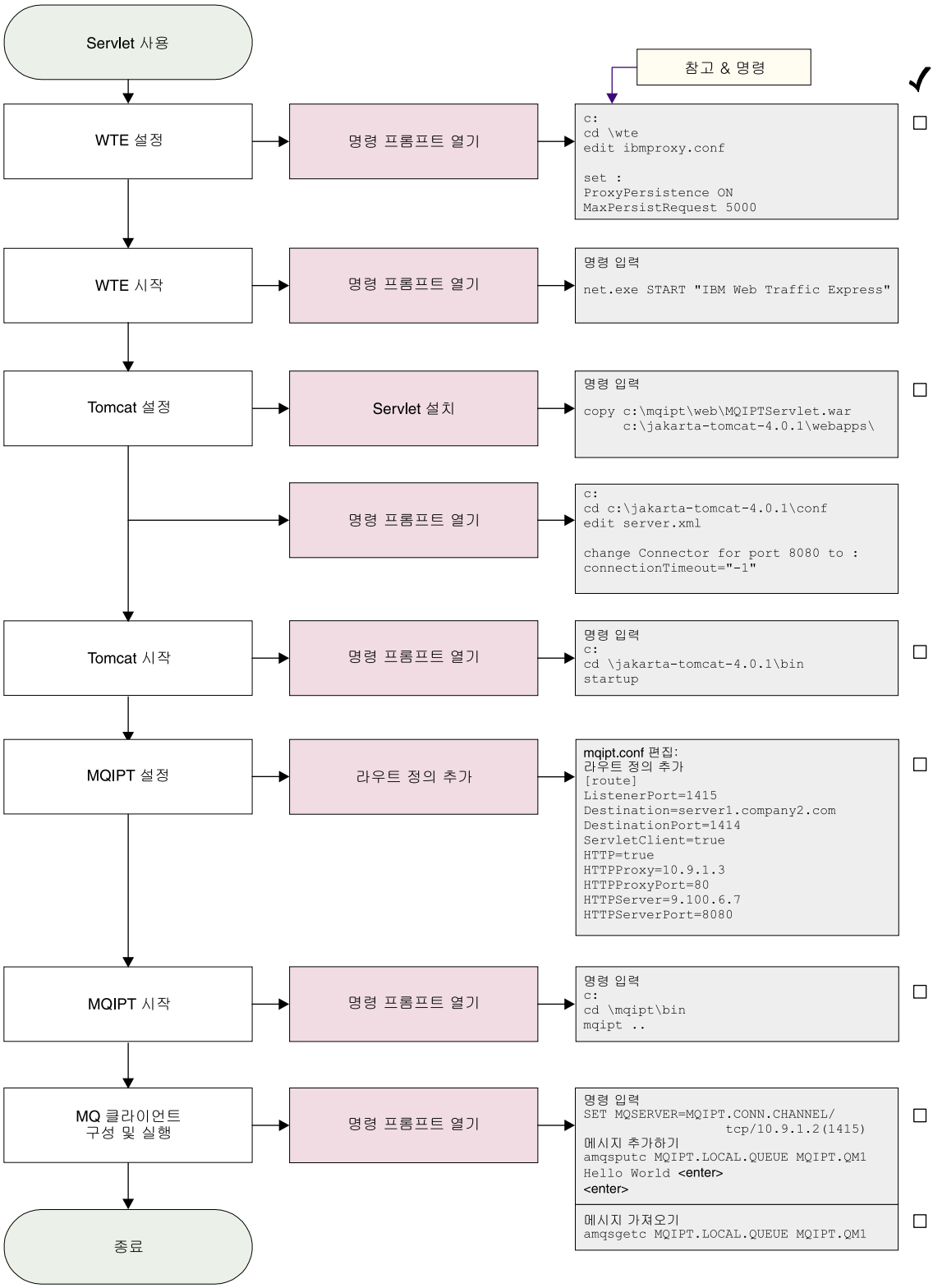

그림 27. Servlet 구성

1. Web Traffic Express를 설정합니다.

   `c:\wte\ibmroxy.conf`를 편집하고 다음 등록 정보를 설정합니다.

```
ProxyPersistence ON
MaxPersistRequest  5000
```

2. Web Traffic Express를 시작합니다.

   명령 프롬프트를 열고 다음을 입력합니다.

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

3. Tomcat을 설정합니다.

   Servlet을 설치하려면 다음을 복사하십시오.

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

   다음과 같이 변경합니다.

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

   c:\jakarta-tomcat-4.0.1\conf\server.xml을 편집하고 포트 8443용 커넥터를 사용 가능하게 하고 ConnectionTimeout 등록 정보를 -1로 설정하십시오.

4. Tomcat을 시작합니다.

   명령 프롬프트를 열고 다음을 입력합니다.

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

5. MQIPT1을 설정합니다.

   mqipt.conf를 편집하고 라우트 정의를 추가합니다.

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

6. MQIPT1을 시작합니다.

   명령 프롬프트를 열고 다음을 입력합니다.

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

   다음 메시지가 표시되면 성공적으로 완료되었다는 것을 알 수 있습니다.

```
5639-L92 (C) Copyright IBM Corp. 2000, 2003 All Rights Reserved
MQCPI001 Websphere MQ internet pass-thru Version 1.3.0 starting
MQCPI004 Reading configuration information from C:\mqipt\mqipt.conf
MQCPI011 The path C:\mqipt\logs will be used to store the log files
MQCPI006 Route 1415 has started and will forward messages to :
MQCPI034 ....server1.company2.com(1414)
MQCPI035 ....using HTTP
```

```
MQCPI024 ....and HTTP proxy at 10.9.1.3(80)
MQCPI066 ....and HTTP server at 9.100.6.7(8080)
MQCPI059 ....servlet client enabled
MQCPI078 Route 1415 ready for connection requests
```

7. WebSphere MQ 클라이언트 시스템의 명령 프롬프트에 다음을 입력합니다.

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

8. 다음을 사용하여 메시지를 넣습니다.

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

9. 다음을 사용하여 메시지를 가져옵니다.

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

그러면 "Hello world"를 볼 수 있습니다.

HTTPS 구성

103 페이지의 『가정』 뿐만 아니라 이 예에서는 다음과 같이 가정합니다.

- Tomcat 응용프로그램 서버가 다음 디렉토리에 설치되었습니다.

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

  다음에서 Tomcat을 다운로드할 수 있습니다.

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

- IBM Web Traffic Express가 다음에 설치되었습니다.

  ```
  c:\wte
  ```

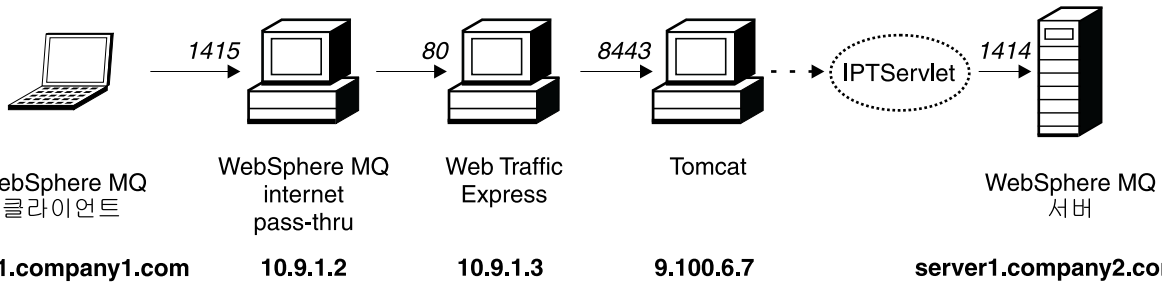

그림 28. HTTPS 네트워크 다이어그램

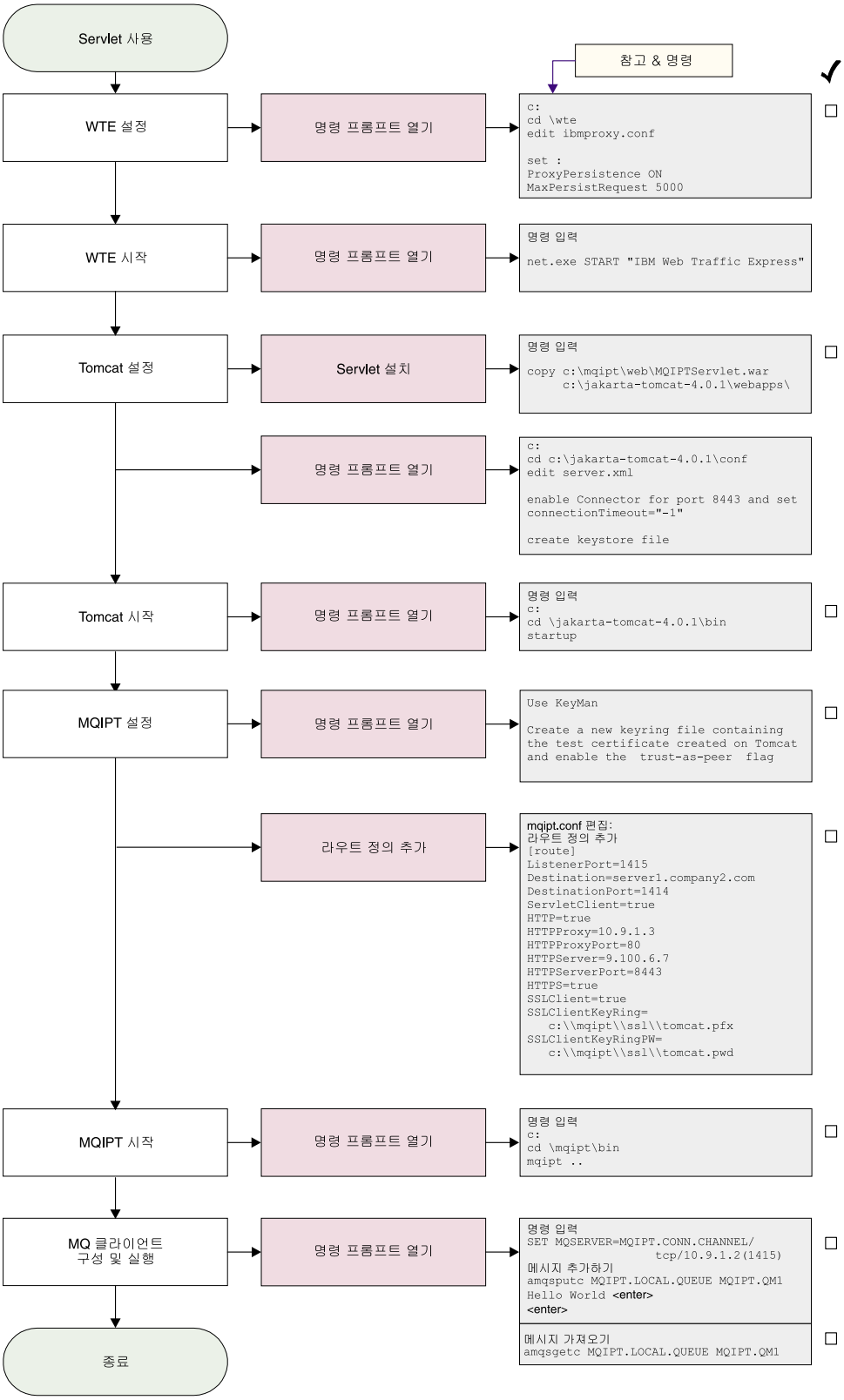

그림 29. HTTPS 구성

1. Web Traffic Express를 설정합니다.

c:\wte\ibmroxy.conf를 편집하고 다음 등록 정보를 설정합니다.

```
ProxyPersistence ON
MaxPersistRequest  5000
```

2. Web Traffic Express를 시작합니다.

   명령 프롬프트를 열고 다음을 입력합니다.

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

3. Tomcat을 설정합니다.

   Servlet을 설치하려면 다음을 복사하십시오.

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

   다음과 같이 변경합니다.

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

   c:\jakarta-tomcat-4.0.1\conf\server.xml을 편집하고 포트 8443용 커넥터를 사용 가능하게 하고 ConnectionTimeout 등록 정보를 -1로 설정하십시오.

   다음에 있는 Tomcat 문서를 사용하고

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

   "SSL Configuration HOW-TO"에 있는 지시사항을 따라 포트 8443에서 SSL 연결을 사용하십시오. 테스트 자체 서명된 인증이 있는 키 링 파일을 작성하십시오. 그렇게 하면 C:\winnt\profiles\<userid>\.keystore라는 파일이 작성됩니다.

4. Tomcat을 시작합니다.

   명령 프롬프트를 열고 다음을 입력합니다.

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

5. Tomcat 시스템에서 MQIPT 시스템으로 새 키스토어 파일을 복사하십시오. KeyMan을 사용하여 새 키스토어 파일(디폴트 암호는 changeit임)을 열고 "trust-as-peer" 플래그를 켜십시오(자세한 정보는 125 페이지의 『SSL 테스트 인증 작성』 참조). 이 파일을 c:\mqipt\ssl\tomcat.pfx로 저장하고 암호 changeit이 있는 c:\mqipt\ssl\tomcat.pwd라는 텍스트 파일을 작성하십시오.

6. MQIPT1을 설정합니다.

   mqipt.conf를 편집하고 라우트 정의를 추가합니다.

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

```
HTTPServerPort=8443
HTTPS=true
SSLClient=true
SSLClientKeyRing=c:\\mqipt\\ssl\\tomcat.pfx
SSLClientKeyRingPW=c:\\mqipt\\ssl\\tomcat.pwd
```

7. MQIPT1을 시작합니다.

   명령 프롬프트를 열고 다음을 입력합니다.

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

   다음 메시지가 표시되면 성공적으로 완료되었다는 것을 알 수 있습니다.

   ```
   5639-L92 (C) Copyright IBM Corp. 2000, 2003 All Rights Reserved
   MQCPI001 Websphere MQ internet pass-thru Version 1.3.0 starting
   MQCPI004 Reading configuration information from C:\mqipt\mqipt.conf
   MQCPI011 The path C:\mqipt\logs will be used to store the log files
   MQCPI006 Route 1415 has started and will forward messages to :
   MQCPI034 ....server1.company2.com(1414)
   MQCPI035 ....using HTTP
   MQCPI024 ....and HTTP proxy at 10.9.1.3(80)
   MQCPI066 ....and HTTP server at 9.100.6.7(8080)
   MQCPI059 ....servlet client enabled
   MQCPI036 ....SSL Client side enabled with properties :
   MQCPI031 ......cipher suites <null>
   MQCPI032 ......keyring file c:\mqipt\ssl\tomcat.pfx
   MQCPI047 ......CA keyring file <null>
   MQCPI038 ......distinguished name(s) CN=* O=* OU=* L=* ST=* C=*
   MQCPI078 Route 1415 ready for connection requests
   ```

8. WebSphere MQ 클라이언트 시스템의 명령 프롬프트에 다음을 입력합니다.

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

9. 다음을 사용하여 메시지를 넣습니다.

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

10. 다음을 사용하여 메시지를 가져옵니다.

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

그러면 "Hello world"를 볼 수 있습니다.

MQIPT 클러스터링 지원 구성

이 예의 경우에는 103 페이지의 『가정』 뿐만 아니라 다음을 수행하였다고 가정합니다.

WebSphere MQ 서버 LONDON에서,

- LONDON이라는 큐 관리자 정의
- MQIPT.CONN.CHANNEL이라는 서버 연결 채널 정의
- 1414 포트에서 LONDON에 대한 TCP/IP 리스너 시작

- 큐 관리자 Socks화

WebSphere MQ 서버 NEWYORK에서,

- NEWYORK이라는 큐 관리자 정의
- MQIPT.CONN.CHANNEL이라는 서버 연결 채널 정의
- 1414 포트에서 NEWYORK에 대한 TCP/IP 리스너 시작
- 큐 관리자 Socks화

큐 관리자를 socks화하기 위해 전체 시스템을 socks화하거나 WebSphere MQ 서버 응용프로그램만을 socks화하십시오. SOCKS 클라이언트를 다음과 같이 구성하십시오.

- MQIPT가 SOCKS 프록시를 지정하도록 함
- SOCKS V5 지원 사용
- 사용자 인증 사용 안함
- MQIPT에 리모트 연결만 작성함

동일한 시스템에서 지정된 포트 주소에 하나의 응용프로그램만이 대기할 수 있으며 1414 포트가 이미 사용 중인 경우에는 사용할 수 있는 포트 주소를 선택하여 예에서 대신 사용하십시오. 일단 이 작업을 수행하였으면 LONDON의 로컬 큐에 메시지를 넣고 NEWYORK에서 이를 검색하여 큐 관리자 간의 라우트를 테스트할 수 있습니다.

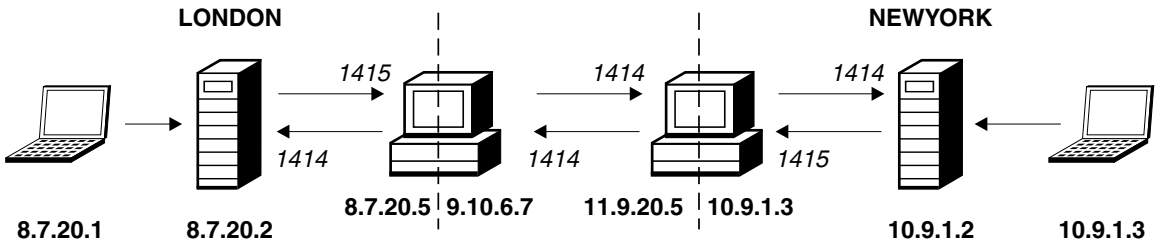

그림 30. 클러스터링 네트워크 다이어그램

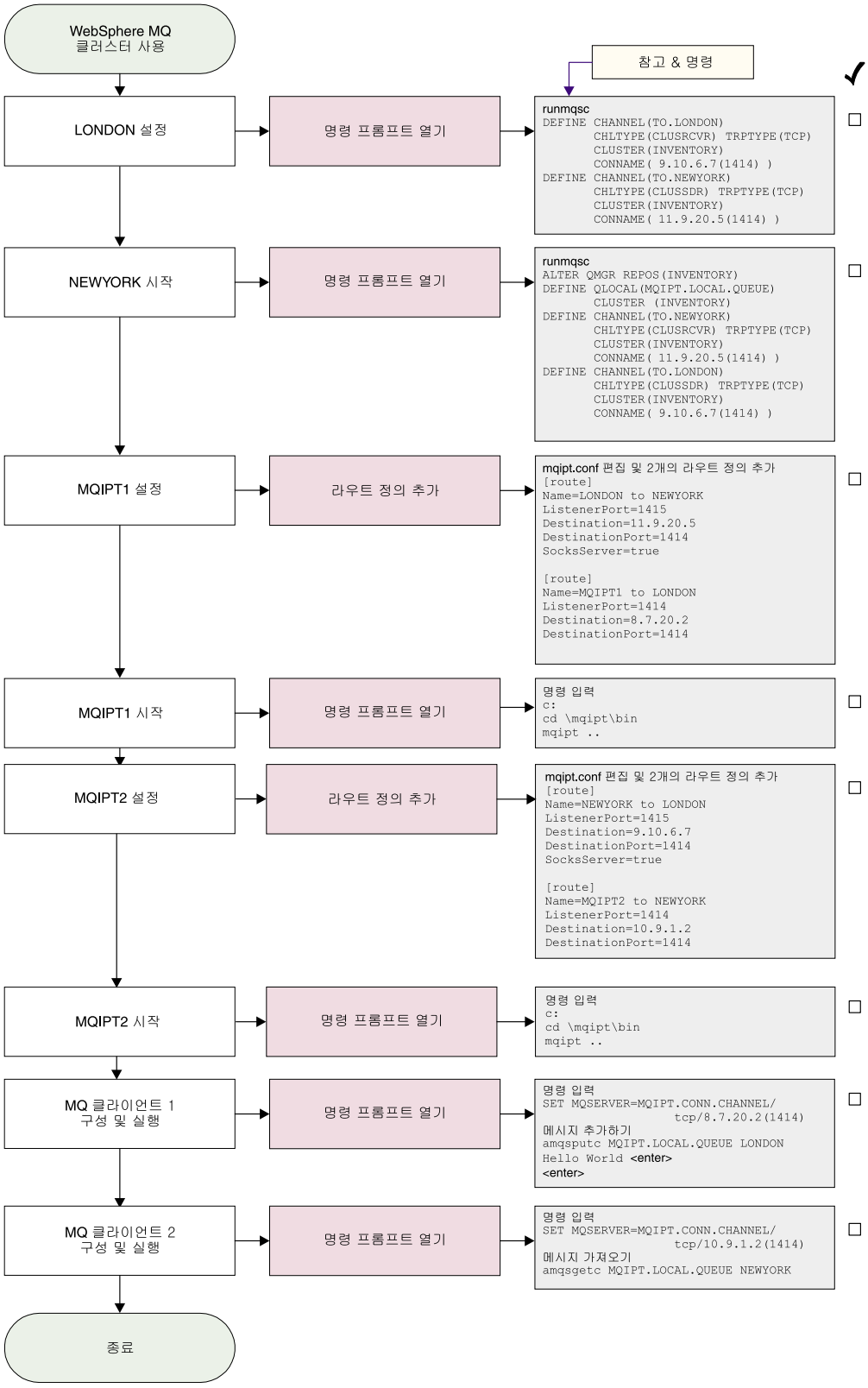

그림 31. 클러스터링 구성

1. LONDON을 설정합니다.

명령 프롬프트를 열고 다음을 입력합니다.

```
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. NEWYORK을 설정합니다.

   명령 프롬프트를 열고 다음을 입력합니다.

```
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. MQIPT1을 설정합니다.

   mqipt.conf를 편집하고 두 개의 라우트 정의를 추가합니다.

```
[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. MQIPT1을 시작합니다.

   명령 프롬프트를 열고 다음을 입력합니다.

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

   다음 메시지가 표시되면 성공적으로 완료되었다는 것을 알 수 있습니다.

```
5639-L92 (C) Copyright IBM Corp. 2000, 2003 All Rights Reserved
MQCPI001 WebSphere MQ internet pass-thru Version 1.3.0 starting
MQCPI004 Reading configuration information from C:\mqipt\mqipt.conf
MQCPI011 The path C:\mqipt\logs will be used to store the log files
MQCPI006 Route 1415 has started and will forward messages to :
MQCPI034 ....11.9.20.5(1414)
```

```
MQCPI035 ....using MQ protocols
MQCPI052 ....Socks server side enabled
MQCPI078 Route 1415 ready for connection requests
MQCPI006 Route 1414 has started and will forward messages to :
MQCPI034 ....8.7.20.2(1414)
MQCPI035 ....using MQ protocols
MQCPI078 Route 1414 ready for connection requests
```

5. MQIPT2를 설정합니다.

   mqipt.conf를 편집하고 두 개의 라우트 정의를 추가합니다.

   ```
   [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. MQIPT2를 시작합니다.

   명령 프롬프트를 열고 다음을 입력합니다.

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

   다음 메시지가 표시되면 성공적으로 완료되었다는 것을 알 수 있습니다.

```
5639-L92 (C) Copyright IBM Corp. 2000, 2003 All Rights Reserved
MQCPI001 WebSphere MQ internet pass-thru Version 1.3.0 starting
MQCPI004 Reading configuration information from C:\mqipt\mqipt.conf
MQCPI011 The path C:\mqipt\logs will be used to store the log files
MQCPI006 Route 1415 has started and will forward messages to :
MQCPI034 ....9.10.6.7(1414)
MQCPI035 ....using MQ protocols
MQCPI052 ....Socks server side enabled
MQCPI078 Route 1415 ready for connection requests
MQCPI006 Route 1414 has started and will forward messages to :
MQCPI034 ....10.9.1.2(1414)
MQCPI035 ....using MQ protocols
MQCPI078 Route 1414 ready for connection requests
```

7. 첫 번째 WebSphere MQ 클라이언트 시스템(8.7.20.1)의 명령 프롬프트에 다음을 입력합니다.

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

8. 다음을 사용하여 메시지를 넣습니다.

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

9. 두 번째 WebSphere MQ 클라이언트 시스템(10.9.1.3)의 명령 프롬프트에 다음을 입력합니다.

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

10. 두 번째 WebSphere MQ 클라이언트 시스템에 다음을 사용하여 메시지를 가져옵니다.

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

그러면 ″Hello world″를 볼 수 있습니다.

키 링 파일 작성

이 샘플에서는 사용자가 Keyman을 사용하여, 트러스트된 CA로부터 새 인증을 요청하였으며 사용자의 개인용 인증이 server.cer 등의 파일 형식으로 사용자에게 리턴되었다고 가정합니다. 이 가정으로 충분히 서버 인증을 수행할 수 있습니다. 클라이언트 인증이 필요한 경우에는 두 번째 인증(client.cer 등)을 요청해야 하며 다음 단계를 두 번 수행하여 두 개의 키 링 파일을 작성해야 합니다.

1. KeyMan을 시작합니다.
2. ″Create new...″를 선택합니다.
3. ″PKCS#12 Token″을 선택합니다.
4. ″Action -> Generate Key″를 선택합니다.

   목록에 다음과 같은 새 키 쌍이 표시됩니다. ″RSA / 1024-bit″
5. 새 키 쌍을 선택합니다.
6. ″Action -> Request Certificate″를 선택합니다.

   다음 온라인 지시사항에 따릅니다.
7. ″File -> Save″를 선택합니다.
8. 암호를 입력합니다.
9. 새 키 링 파일의 파일 이름을 입력합니다.

   예를 들어, c:\mqipt\ssl\myServer.pfx입니다.
10. 이 때, 반드시 ″파일 형식을 PKCS#12 / PFX″로 유지해야 합니다. - ″Wrap key ring into a Java class 맵핑″을 선택하면 **안됩니다**.
11. ″File -> Exit″를 선택합니다.
12. 앞에서 사용한 암호 문구(myPassWord)를 포함한 텍스트 파일을 작성합니다.

    예를 들어, c:\mqipt\ssl\myServer.pwd 등입니다.

다시 인증을 가져왔으면 원래 키 링 파일(myServer.pfx)을 엽니다. 그런 다음, 다음을 수행합니다.

1. KeyMan을 시작합니다.
2. ″Open existing...″을 선택합니다.
3. ″Local resource″를 선택합니다.
4. ″Open a file...″을 선택합니다.

5. 개인용 cert 파일의 파일 이름을 입력합니다.

   예를 들어, c:\mqipt\ssl\myServer.pfx입니다.
6. 암호 구문을 입력합니다.
7. ″File -> Import″를 선택합니다.
8. ″Local resource″를 선택합니다.
9. ″Open a file...″을 선택합니다.
10. server.cer 파일을 입력합니다.

    개인용 인증이 개인용 키와 함께 결합될 것임을 설명하는 대화 상자가 표시됩니다.
11. ″File -> Save″를 선택합니다.
12. ″File -> Exit″를 선택합니다.

이러한 단계를 반복하여 client.cer 파일에서 myClient.pfx 파일을 작성합니다. KeyMan을 사용하여 샘플 CA 키 링 파일인 sslCAdefault.pfx의 컨텐트를 점검하여 개인용 인증이 나열된 CA 중 하나에 의해 서명되었는 지 확인하십시오. 서명되었으면 샘플 CA 키 링 파일을 사용할 수 있습니다. 그렇지 않으면 사용자의 개인용 인증을 서명한 공용 CA 인증을 포함한 키 링 파일을 작성해야 합니다. 이 파일은 사용자의 개인용 인증과 함께 리턴되었을 수 있습니다. 그렇지 않으면 개인용 인증을 공급한 동일한 CA로부터 CA 인증을 요청하고 이를 sslCAdefault.pfx에 들여와야 합니다. CA 키 링 파일은 클라이언트 및 서버 측 모두에서 사용할 수 있습니다. 이러한 새 키 링 파일을 서버 인증에 사용하려면 예제 106 페이지의 『SSL 서버 인증』을 참조하고 다음 라우트 등록 정보를 설정하십시오.

```
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
```

이러한 새 키 링 파일을 클라이언트 및 서버 인증에 사용하려면 예제 109 페이지의 『SSL 클라이언트 인증』을 참조하고 다음 라우트 등록 정보를 설정하십시오.

```
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
```

포트 주소 할당

이 예는 보내는 연결을 설정할 때 사용되는 로컬 포트 주소의 제어 방법을 보여줍니다. 이 예에서는 MQIPT가 멀티홈 시스템에 설치된 것으로 가정합니다.

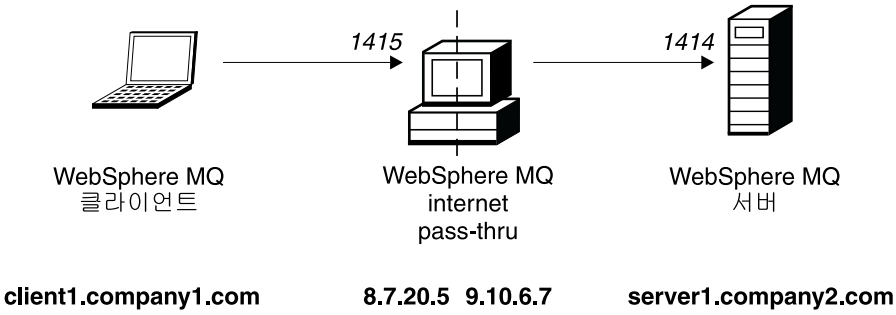

그림 32. 포트 할당 네트워크 다이어그램

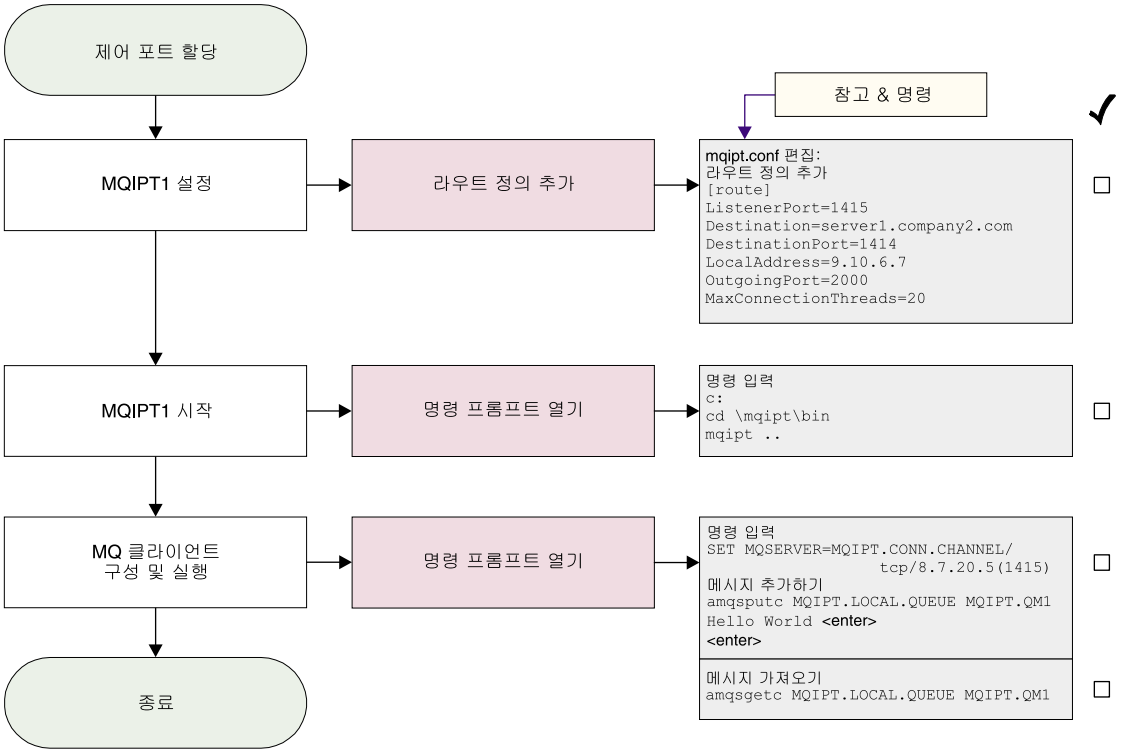

그림 33. 포트 할당 구성

1. MQIPT1을 설정합니다.

   mqipt.conf를 편집하고 라우트 정의를 추가합니다.

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

```
DestinationPort=1414
LocalAddress=9.10.6.7
OutgoingPort=2000
MaxConnectionThreads=20
```

2. MQIPT1을 시작합니다.

   명령 프롬프트를 열고 다음을 입력합니다.

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

   다음 메시지가 표시되면 성공적으로 완료되었다는 것을 알 수 있습니다.

   ```
   5639-L92 (C) Copyright IBM Corp. 2000, 2003 All Rights Reserved
   MQCPI001 WebSphere MQ internet pass-thru Version 1.3.0 starting
   MQCPI004 Reading configuration information from C:\mqipt\mqipt.conf
   MQCPI011 The path C:\mqipt\logs will be used to store the log files
   MQCPI006 Route 1415 has started and will forward messages to :
   MQCPI034 ....server1.company2.com(1414)
   MQCPI035 ....using MQ protocols
   MQCPI069 ....binding to local address 9.10.6.7
   MQCPI070 ....using local port address range 2000-2019
   MQCPI078 Route 1415 ready for connection requests
   ```

3. WebSphere MQ 클라이언트 시스템의 명령 프롬프트에 다음을 입력합니다.

   ```
   SET MQSERVER=MQIPT.CONN.CHANNEL/tcp/8.7.20.5(1415)
   ```

4. 다음을 사용하여 메시지를 넣습니다.

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

5. 다음을 사용하여 메시지를 가져옵니다.

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

그러면 ″Hello world″를 볼 수 있습니다.

LDAP 서버 사용

이 샘플은 LDAP 서버를 사용하여 CRL을 검색하도록 MQIPT를 구성하는 방법을 보여줍니다. LDAP 서버 설치 및 설정 방법, 개인 인증이나 트러스트된 인증이 있는 키 링 파일 작성 방법을 설명하는 것이 이 샘플의 목적은 아닙니다. 이 샘플에서는 트러스트된 알려진 인증 권한(CA)에서 LDAP 서버를 사용할 수 있는 것으로 가정합니다. 백업 LDAP 서버는 사용되지 않지만 해당 라우트 등록 정보를 추가하면 백업 LDAP 서버를 쉽게 구현할 수 있습니다.

이 예에서 다음과 같은 가정을 합니다.

- 트러스트된 CA에서 발행하고 myCert.pfx라는 키 링 파일에 저장된 개인 인증이 IPT2에 있으며 키 링 파일을 여는 데 사용된 암호화된 암호는 myCert.pwd에 저장됩니다.

- IPT2에서 송신한 인증을 인증하는 데 사용하는 트러스트된 CA 사본 하나가 IPT1에 있습니다. 이 인증은 caCerts.pfx라는 키 링 파일에 저장되고 키 링 파일을 여는 데 사용된 암호화된 암호는 caCerts.pwd 파일에 저장됩니다.
- mqiptPW 스크립트를 사용하여 암호화된 암호 파일을 작성했습니다.

이 샘플을 실행하면 WMQ 클라이언트를 큐 관리자(QM)에 연결할 수 있고 WMQ 메시지를 대상 큐에 넣을 수 있습니다. IPT1에서 MQIPT 추적을 실행하면 사용되는 LDAP 서버가 표시되지만 CRL의 작동 방법을 표시하려면 트러스트된 CA에서 IPT2에 사용된 개인 인증을 호출해야 합니다. 따라서 IPT1에서 IPT2로의 연결이 거부되므로 이 경우에는 WMQ 클라이언트가 QM에 연결될 수 없습니다.

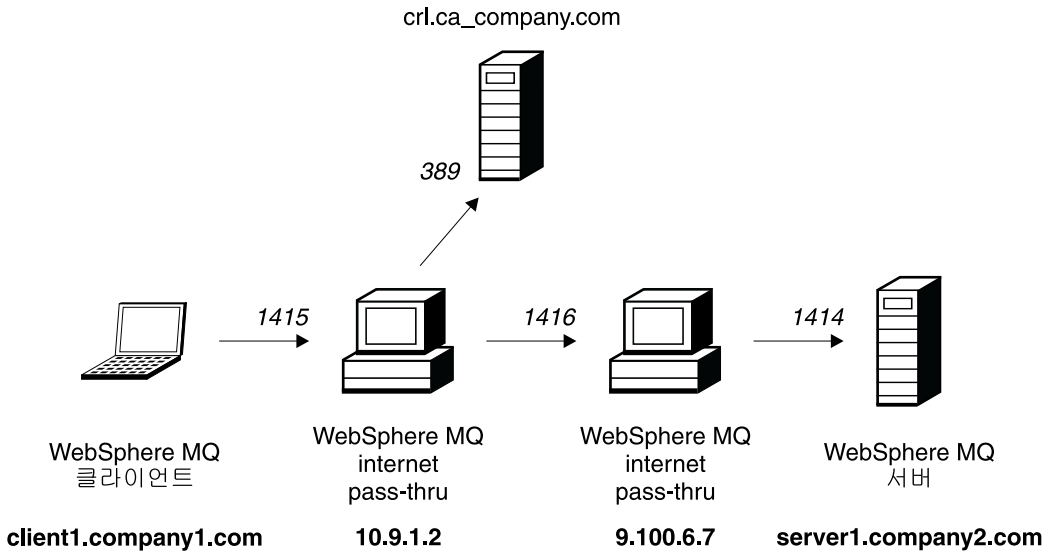

그림 34. LDAP 서버 네트워크 다이어그램

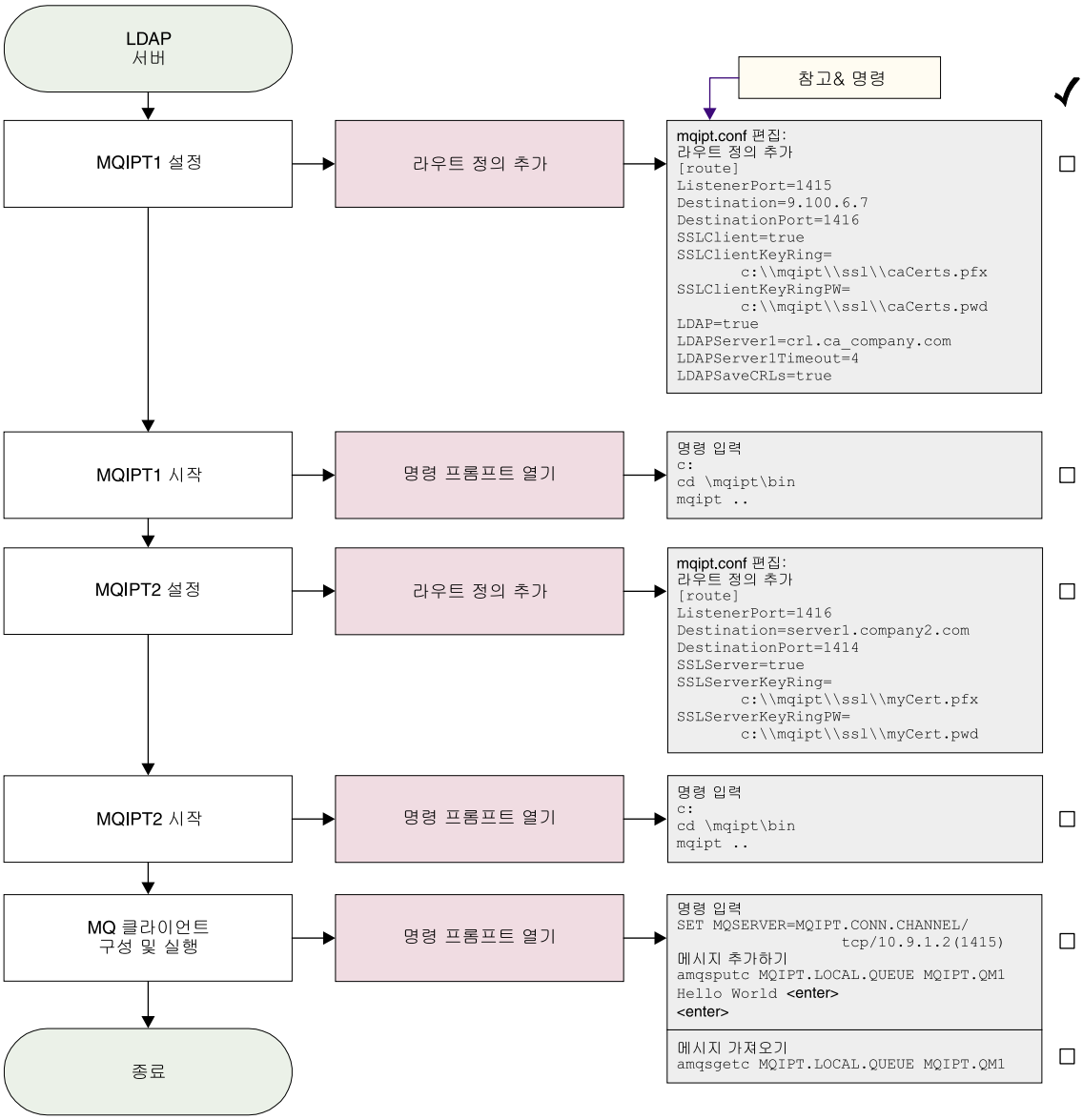

그림 35. LDAP 서버 구성

1. IPT1에서

   mqipt.conf를 편집하고 라우트 정의를 추가합니다.

```
[route]
ListenerPort=1415
Destination=9.100.6.7
DestinationPort=1416
SSLClient=true
SSLClientKeyRing=c:\\mqipt\\ssl\\caCerts.pfx
SSLClientKeyRingPW=c:\\mqipt\\ssl\\caCerts.pwd
LDAP=true
LDAPServer1=crl.ca_company.com
LDAPServer1Timeout=4
LDAPSaveCRLs=true
```

명령 프롬프트를 여십시오.

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

다음 메시지가 표시되면 성공적으로 완료되었다는 것을 알 수 있습니다.

```
5639-L92 (C) Copyright IBM Corp. 2000, 2003 All Rights Reserved
MQCPI001 Websphere MQ internet pass-thru Version 1.3.0 starting
MQCPI004 Reading configuration information from C:\mqipt\mqipt.conf
MQCPI011 The path C:\mqipt\logs will be used to store the log files
MQCPI006 Route 1415 has started and will forward messages to :
MQCPI034 ....9.100.6.7(1416)
MQCPI035 ....using MQ protocols
MQCPI036 ....SSL Client side enabled with properties :
MQCPI031 ......cipher suites <NULL>
MQCPI032 ......keyring file <NULL>
MQCPI047 ......CA keyring file c:\mqipt\ssl\caCerts.pfx
MQCPI071 ......site certificate uses CN=* O=* OU=* L=* ST=* C=*
MQCPI038 ......peer certificate uses CN=* O=* OU=* L=* ST=* C=*
MQCPI075 ....LDAP main server at crl.ca_company.com(389)
MQCPI086 ......timeout of 4 second(s)
MQCPI084 ....CRL cache expiry timeout is 1 hour(s)
MQCPI085 ....CRLs will be saved in the key ring file(s)
MQCPI078 Route 1415 ready for connection requests
```

2. IPT2에서

mqipt.conf를 편집하고 라우트 정의를 추가합니다.

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

명령 프롬프트를 여십시오.

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

다음 메시지가 표시되면 성공적으로 완료되었다는 것을 알 수 있습니다.

```
5639-L92 (C) Copyright IBM Corp. 2000, 2003 All Rights Reserved
MQCPI001 IBM WebSphere MQ internet pass-thru Version 1.3.0 starting
MQCPI004 Reading configuration information from C:\mqipt\mqipt.conf
MQCPI011 The path C:\mqipt\logs will be used to store the log files
MQCPI006 Route 1416 is starting and will forward messages to :
MQCPI034 ....server1.company2.com(1414)
MQCPI035 ....using MQ protocols
MQCPI037 ....SSL Server side enabled with properties :
MQCPI031 ......cipher suites <NULL>
MQCPI032 ......keyring file c:\mqipt\ssl\myCert.pfx
MQCPI047 ......CA keyring file <NULL>
MQCPI071 ......site certificate uses CN=* O=* OU=* L=* ST=* C=*
```

```
MQCPI038 ......peer certificate uses CN=* O=* OU=* L=* ST=* C=*
MQCPI033 ......client authentication set to false
MQCPI078 Route 1416 ready for connection requests
```

3. WebSphere MQ 클라이언트 시스템의 명령 프롬프트에 다음을 입력합니다.

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

4. 다음을 사용하여 메시지를 넣습니다.

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

5. 다음을 사용하여 메시지를 가져옵니다.

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

그러면 "Hello world"를 볼 수 있습니다.

SSL 프록시 모드

이 샘플에서는 SSL 프록시 모드에서 MQIPT를 실행하는 방법을 보여주고, SSL 클라이언트로부터 SSL 연결 요청을 승인하고 이를 SSL 서버로 터널링하도록 합니다. WMQ 클라이언트와 서버가 모두 V5.3이며 SSL 연결을 사용하도록 구성된 것으로 가정합니다.

WMQ용 SSL 설정에 대한 자세한 정보는 "WebSphere MQ 보안 버전 5.3" SA30-1576-01을 참조하십시오.

이 예에서 다음과 같은 가정을 합니다.

- MQClient 및 QM은 SSL 채널을 사용하도록 설정했습니다.

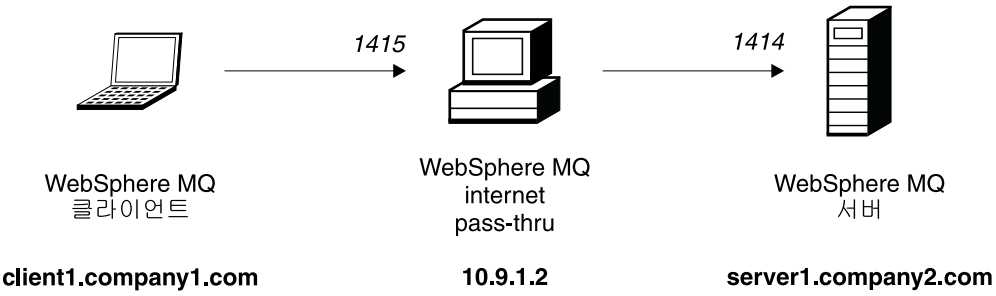

그림 36. SSL 프록시 모드 네트워크 다이어그램

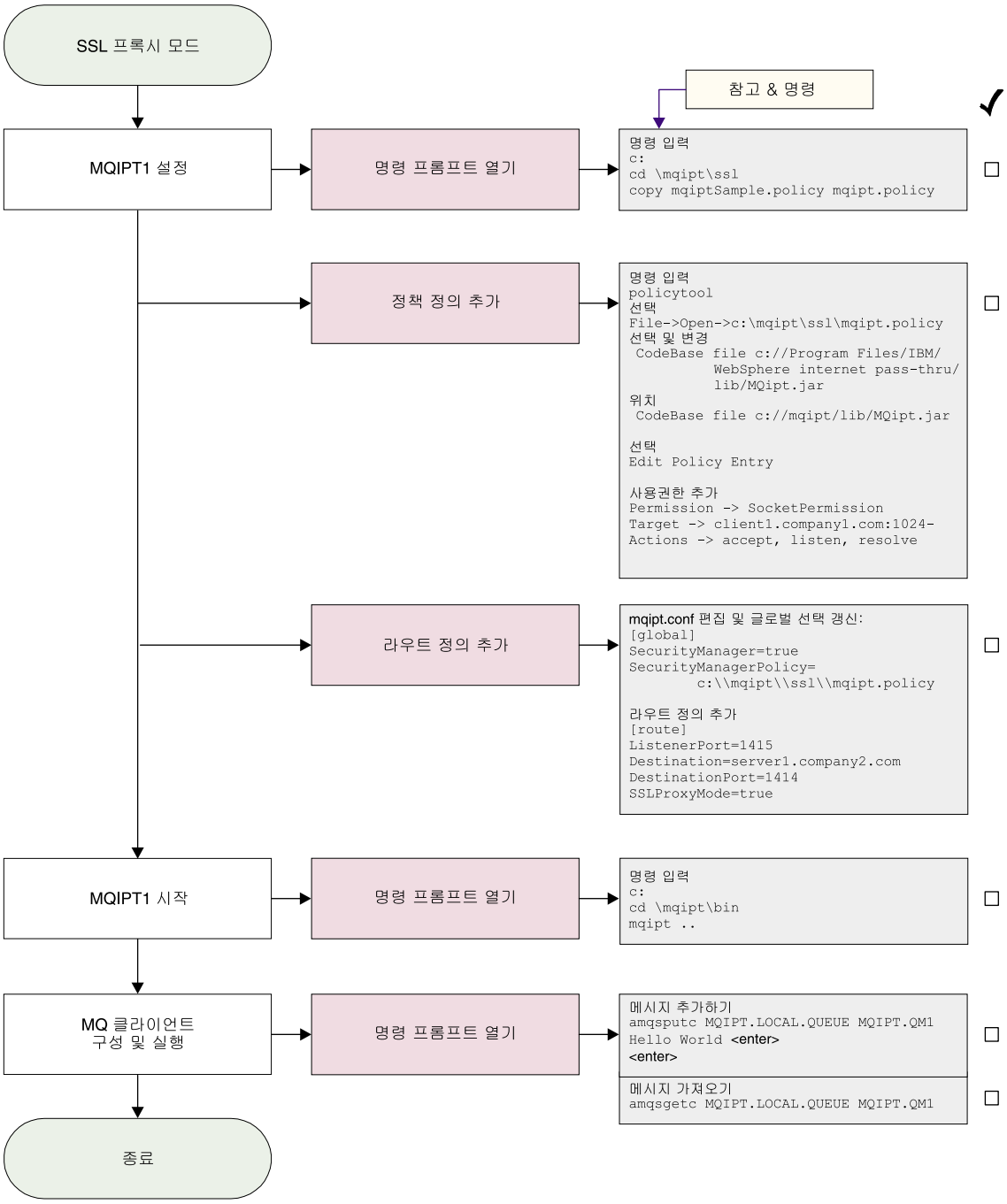

그림 37. SSL 프록시 모드 구성

1. IPT1에서
   a. 명령 프롬프트를 열고 다음을 입력합니다.

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

   b. 다음 명령을 사용하여 정책 정의를 추가합니다.

      ```
      policytool
      ```

      1) 다음을 선택하십시오. **파일 --> 열기 --> c:\mqipt\ssl\mqipt.policy**

2) 다음을 선택합니다.

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

3) 다음에서 CodeBase를 변경합니다.

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

다음과 같이 변경합니다.

```
"file://C:/mqipt/lib/MQipt.jar"
```

4) 다음에서 모든 권한을 변경합니다.

```
"C:\\Program Files\\IBM\\WebSphere MQ internet pass-thru"
```

다음과 같이 변경합니다.

```
"C:\\mqipt"
```

5) SocketPermission을 추가합니다.

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

2. mqipt.conf를 편집하고 다음 두 등록 정보를 전역 절과 라우트 정의로 추가하십시오.

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

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

3. 명령 프롬프트를 여십시오.

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

다음 메시지가 표시되면 성공적으로 완료되었다는 것을 알 수 있습니다.

```
5639-L92 (C) Copyright IBM Corp. 2000, 2003 All Rights Reserved
MQCPI001 Websphere MQ internet pass-thru Version 1.3.0 starting
MQCPI004 Reading configuration information from C:\mqipt\mqipt.conf
MQCPI011 The path C:\mqipt\logs will be used to store the log files
MQCPI006 Route 1415 has started and will forward messages to :
MQCPI034 ....server1.company2.com(1414)
MQCPI035 ....using SSLProxyMode
MQCPI078 Route 1415 ready for connection requests
```

4. 다음을 사용하여 메시지를 넣습니다.

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

5. 다음을 사용하여 메시지를 가져옵니다.

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

그러면 ″Hello world″를 볼 수 있습니다.

Apache 다시 쓰기

이 예에서 다음과 같은 가정을 합니다.

- Apache HTTP 서버가 c:\apache에 설치되었습니다.
- IBM Web Traffic Express는 c:\wte에 설치되었습니다.

이 샘플은 HTTP 요청을 내부 Apache 프록시 리디렉션(redirect)으로 변환하기 위해 다시 쓰기 지시문을 사용하는 방법을 보여줍니다. 프록시와 다시 쓰기 모듈을 로드해야 하지만 Apache가 실제로 프록시 모드에서 작동하지 않으므로 모든 프록시 지시문에 주석을 달아 둘 수 있습니다.

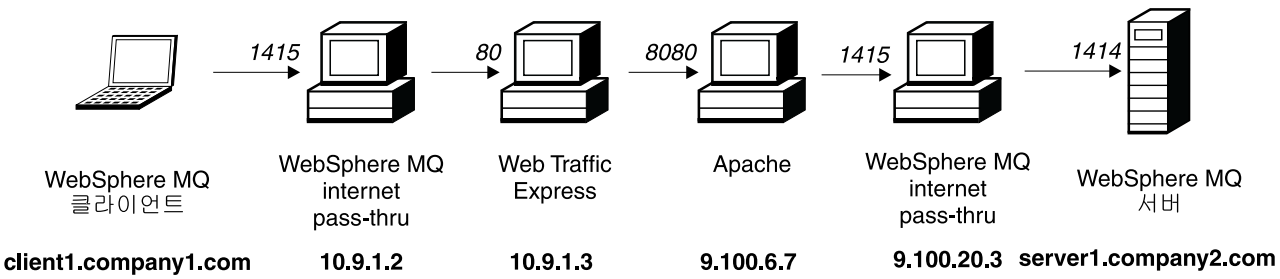

그림 38. Apache 다시 쓰기 네트워크 다이어그램

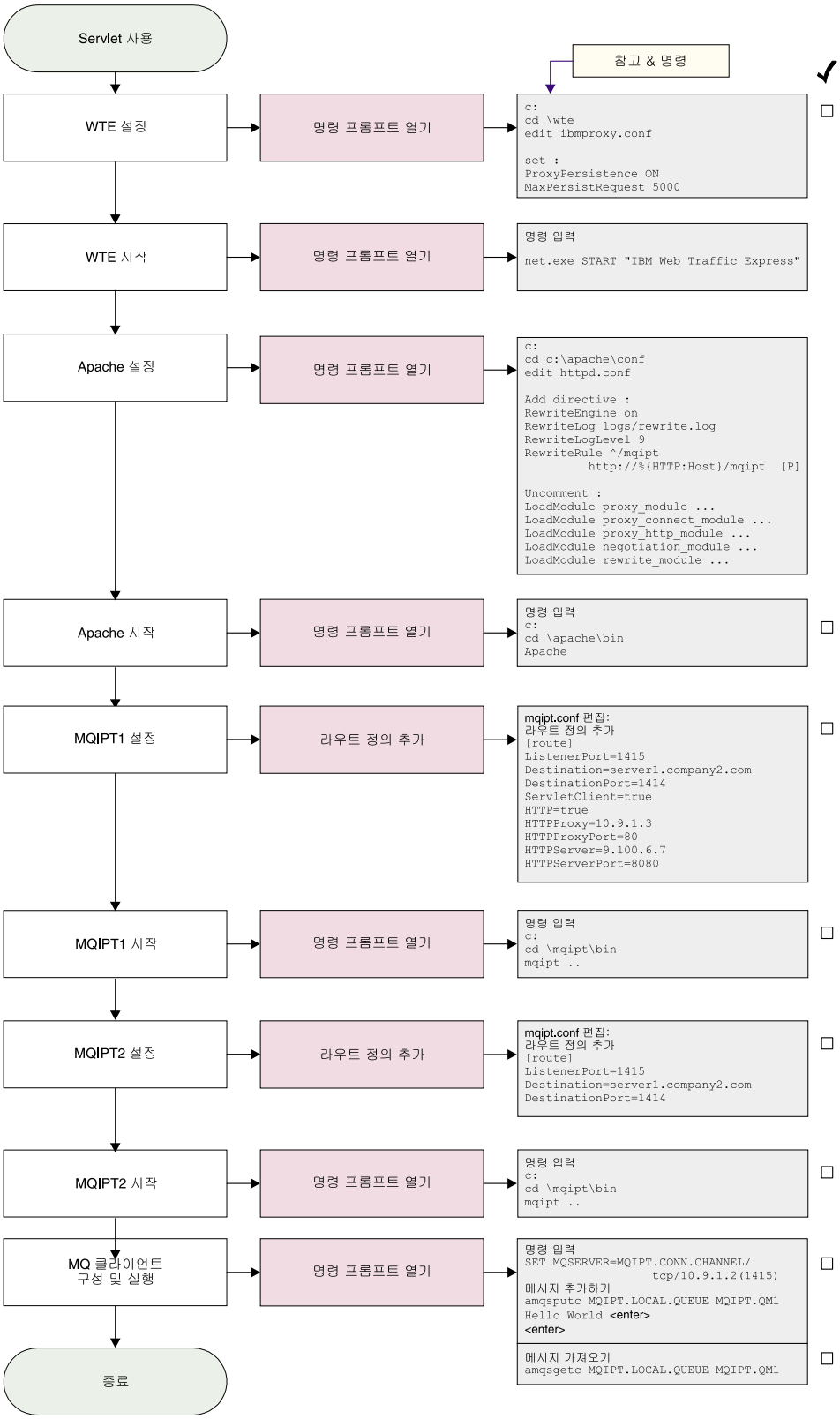

그림 39. Apache 다시 쓰기 구성

1. WTE에서

   edit c:\wte\ibmroxy.conf

   다음 등록 정보를 변경하십시오.

   ```
   ProxyPersistence ON
   MaxPersistRequest  5000
   ```

2. Apache에서

   edit c:\apache\conf\httpd.conf

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

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

   start Apache
   ```

3. IPT1에서

   mqipt.conf를 편집하고 라우트 정의를 추가합니다.

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

   명령 프롬프트를 여십시오.

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

   다음 메시지가 표시되면 성공적으로 완료되었다는 것을 알 수 있습니다.

   ```
   5639-L92 (C) Copyright IBM Corp. 2000, 2003 All Rights Reserved
   MQCPI001 Websphere MQ internet pass-thru Version 1.3.0 starting
   MQCPI004 Reading configuration information from C:\mqipt\mqipt.conf
   MQCPI011 The path C:\mqipt\logs will be used to store the log files
   MQCPI006 Route 1415 has started and will forward messages to :
   MQCPI034 ....server1.company2.com(1414)
   MQCPI035 ....using HTTP
   MQCPI024 ....and HTTP proxy at 10.9.1.3(80)
   MQCPI066 ....and HTTP server at 9.100.6.7(8080)
   MQCPI078 Route 1415 ready for connection requests
   ```

4. IPT2에서

   mqipt.conf를 편집하고 라우트 정의를 추가합니다.

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

   명령 프롬프트를 여십시오.

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

   다음 메시지가 표시되면 성공적으로 완료되었다는 것을 알 수 있습니다.

   ```
   5639-L92 (C) Copyright IBM Corp. 2000, 2003 All Rights Reserved
   MQCPI001 Websphere MQ internet pass-thru Version 1.3.0 starting
   MQCPI004 Reading configuration information from C:\mqipt\mqipt.conf
   MQCPI011 The path C:\mqipt\logs will be used to store the log files
   MQCPI006 Route 1415 has started and will forward messages to :
   MQCPI034 ....server1.company2.com(1414)
   MQCPI035 ....using MQ protocols
   MQCPI078 Route 1415 ready for connection requests
   ```

5. WebSphere MQ 클라이언트 시스템의 명령 프롬프트에 다음을 입력합니다.

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

6. 다음을 사용하여 메시지를 넣습니다.

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

7. 다음을 사용하여 메시지를 가져옵니다.

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

그러면 ″Hello world″를 볼 수 있습니다.

보안 엑시트

이 예에서 다음과 같은 가정을 합니다.

- Java 1.4 SDK가 설치되었습니다.
- Java bin 서브디렉토리가 PATH 환경 변수에 추가되었습니다.

SampleSecurityExit라는 제공된 샘플 보안 엑시트의 사용 방법을 보여주는 간단한 테스트입니다. 이 보안 엑시트는 ″MQIPT″ 문자로 시작되는 채널 이름을 사용하여 클라이언트 연결만 가능하도록 작성되었습니다.

제안된 ″MQIPT.CONN.CHANNEL″의 srvconn 채널 이름(이 예의 대부분에 사용)을 사용하면 클라이언트 연결을 완료할 수 있고 WMQ 메시지를 큐에 넣을 수 있습니다.

보안 엑시트가 제대로 작동하는지 알아보려면 ″MQIPT’ 문자로 시작되지 않는 이름(예: ″TEST.CONN.CHANNEL″)으로 다른 srvconn 채널을 정의하고 새 채널 이름을 사용할 MQSERVER 환경 변수를 변경하여 amqsputc 명령을 다시 시도하십시오. 그러면 연결이 거부되고 2059 오류가 발생합니다.

보안 엑시트를 사용하지 않고 ″TEST.CONN.CHANNEL″이 작동하는지 표시하려면 MQSERVER 환경 변수가 직접 WMQ 리스너 포트(예: 1414)를 가리키도록 설정하십시오. 그러면 MQIPT가 사용되지 않습니다. amqsputc 명령이 제대로 작동하게 됩니다.

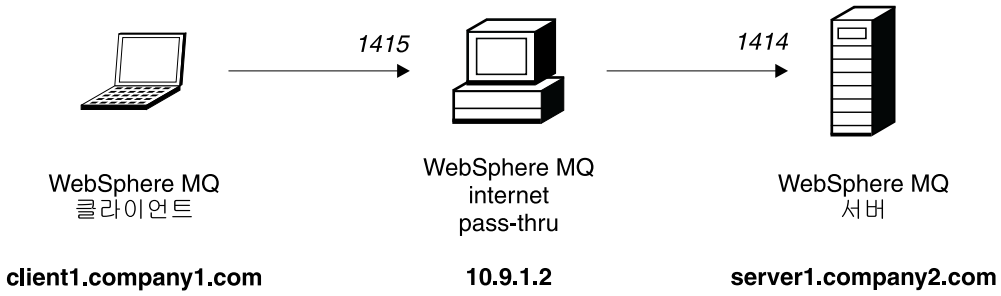

그림 40. 보안 엑시트 네트워크 다이어그램

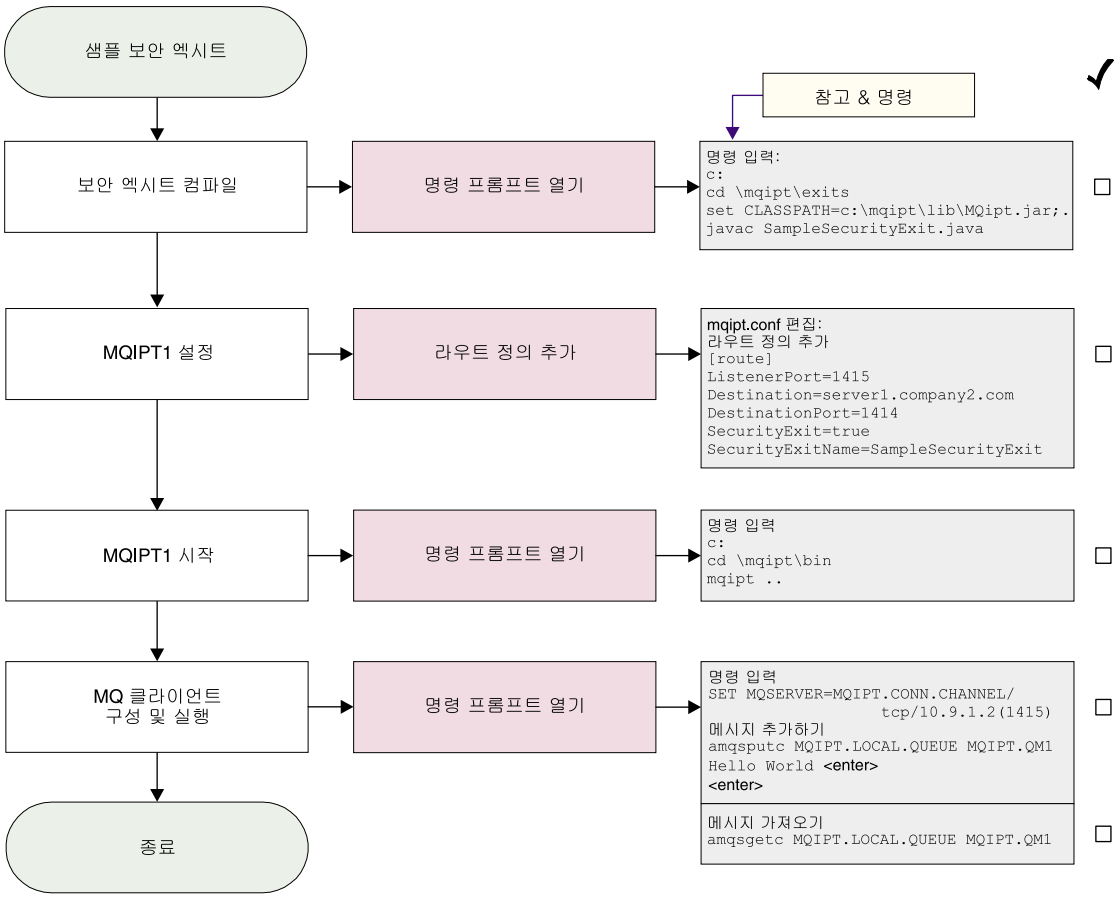

그림 41. 보안 엑시트 구성

1. IPT1에서

   명령 프롬프트를 여십시오.

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

   mqipt.conf를 편집하고 라우트 정의를 추가합니다.

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

   명령 프롬프트를 여십시오.

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

   다음 메시지가 표시되면 성공적으로 완료되었다는 것을 알 수 있습니다.

```
5639-L92 (C) Copyright IBM Corp. 2000, 2003 All Rights Reserved
MQCPI001 Websphere MQ internet pass-thru Version 1.3.0 starting
MQCPI004 Reading configuration information from c:\mqipt\mqipt.conf
MQCPI011 The path c:\mqipt\logs will be used to store the log files
MQCPI006 Route 1415 has started and will forward messages to :
MQCPI034 ....server1.company2.com(1414)
MQCPI035 ....using MQ protocols
MQCPI079 ....using security exit c:\mqipt\exits\SampleSecurityExit
MQCPI080 ......and timeout of 5 seconds
MQCPI078 Route 1415 ready for connection requests
```

2. WebSphere MQ 클라이언트 시스템의 명령 프롬프트에 다음을 입력합니다.

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

3. 다음을 사용하여 메시지를 넣습니다.

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

4. 다음을 사용하여 메시지를 가져옵니다.

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

그러면 "Hello world"를 볼 수 있습니다.

라우팅 보안 엑시트

이 예에서 다음과 같은 가정을 합니다.

- Java 1.4 SDK가 설치되었습니다.
- Java bin 서브디렉토리가 PATH 환경 변수에 추가되었습니다.
- 각각의 세 서버에서 세 개의 동일한 큐 관리자가 작성되었습니다.

이 예는 클라이언트 연결 요청을 라운드 로빈 형태로 WMQ 큐 관리자 서버 그룹에 동적으로 라우트하는 방법을 설명합니다. 그룹에 있는 각 서버의 큐 관리자는 각각의 미러 이미지이어야 합니다.

서버 이름의 목록은 구성 파일에서 읽습니다. 구성 파일의 이름과 위치는 SecurityExitName 및 SecurityExitPath 등록 정보로 정의됩니다. SampleRoutingExit.conf 라는 샘플 구성 파일에는 다음과 같은 항목이 있습니다.

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

이러한 서버 이름을 사용자 환경에 맞게 변경해야 합니다.

amqsputc 명령이 처음 발행되면 WMQ 메시지는 server1에서 QM의 MQIPT.LOCAL.QUEUE에 놓입니다. 두 번째로 발행될 때 이 메시지는 server2의 QM에 나타납니다. 이 설정을 사용하면 amqsgetc 명령에 사용된 클라이언트 연결 요청이 목록의 다음 QM으로 전달되므로 amqsgetc 명령이 큐에 놓인 메시지를 검색할 수 없

습니다. 그러나 세 개의 amqsputc 명령 다음에 세 개의 amqsgetc 명령을 발행하면 각각의 메시지가 같은 순서로 검색됩니다. 물론, 다른 WMQ 클라이언트를 사용하여 QM에 직접 연결하면(이 샘플에서는 MQIPT를 사용하지 않음) 큐 관리자에서 메시지를 선택적으로 검색할 수 있습니다.

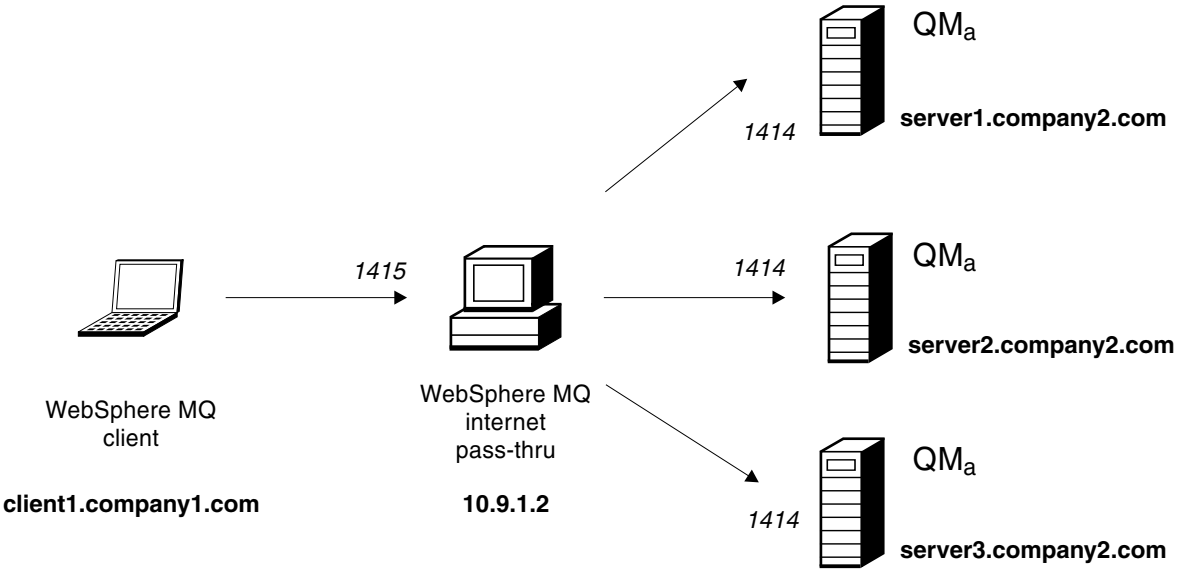

그림 42. 라우팅 보안 엑시트 네트워크 다이어그램

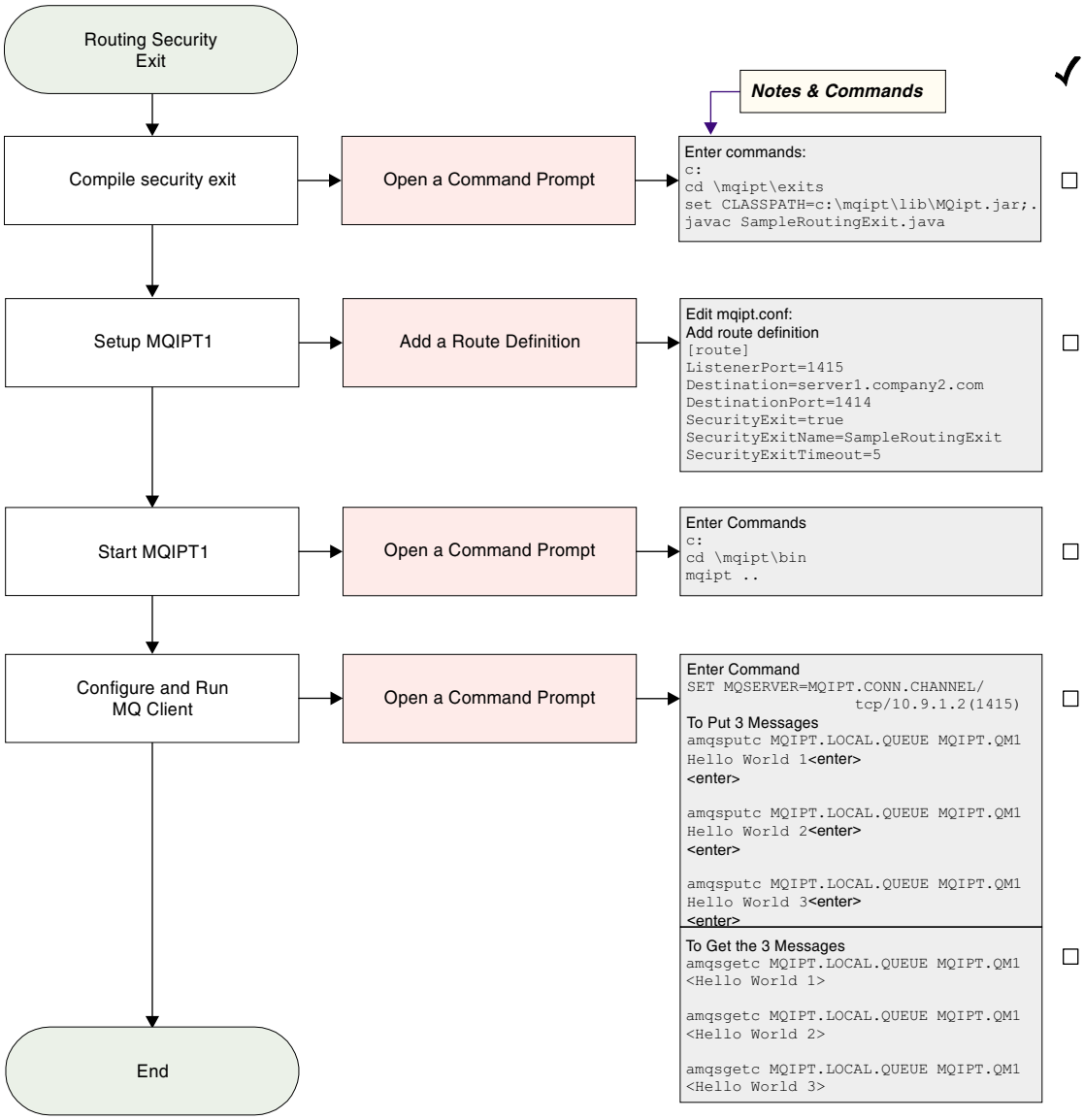

그림 43. 라우팅 보안 엑시트 구성

1. IPT1에서

   명령 프롬프트를 여십시오.

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

   mqipt.conf를 편집하고 라우트 정의를 추가합니다.

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

명령 프롬프트를 여십시오.

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

다음 메시지가 표시되면 성공적으로 완료되었다는 것을 알 수 있습니다.

```
5639-L92 (C) Copyright IBM Corp. 2000, 2003 All Rights Reserved
MQCPI001 Websphere MQ internet pass-thru Version 1.3.0 starting
MQCPI004 Reading configuration information from c:\mqipt\mqipt.conf
MQCPI011 The path c:\mqipt\logs will be used to store the log files
MQCPI006 Route 1415 has started and will forward messages to :
MQCPI034 ....server1.company2.com(1414)
MQCPI035 ....using MQ protocols
MQCPI079 ....using security exit c:\mqipt\exits\SampleRoutingExit
MQCPI080 ......and timeout of 5 seconds
MQCPI078 Route 1415 ready for connection requests
```

2. WebSphere MQ 클라이언트 시스템의 명령 프롬프트에 다음을 입력합니다.

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

3. 다음을 사용하여 메시지를 넣습니다.

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

4. 다음을 사용하여 메시지를 가져옵니다.

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

그러면 ″Hello world 1″, ″Hello world 2″ 및 ″Hello world 3″을 볼 수 있습니다.

동적 1 라우트 엑시트

이 예에서 다음과 같은 가정을 합니다.

- Java 1.4 SDK가 설치되었습니다.
- Java bin 서브디렉토리가 PATH 환경 변수에 추가되었습니다.
- 각각의 세 서버에 세 개의 다른 큐 관리자가 작성되었습니다.

이 예는 사용된 채널 이름에 따라 클라이언트 연결 요청을 대상 서버에 동적으로 라우트하는 방법을 설명합니다. 채널 이름의 첫 부분은 큐 관리자의 이름입니다. 예를 들어

QM1에 연결할 경우 svrconn 채널의 이름은 QM1.MQIPT.CONN.CHANNEL이 됩니다. 이 채널 이름 지정 규칙을 사용하여 MQIPT는 모든 연결 요청에 하나의 라우트만 사용해야 합니다.

큐 관리자와 서버 이름의 목록은 구성 파일에서 읽습니다. 구성 파일의 이름과 위치는 SecurityExitName 및 SecurityExitPath 등록 정보로 정의됩니다.
SampleOneRouteExit.conf라는 샘플 구성 파일에는 다음과 같은 항목이 있습니다.

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

이러한 서버 이름을 사용자 환경에 맞게 변경해야 합니다.

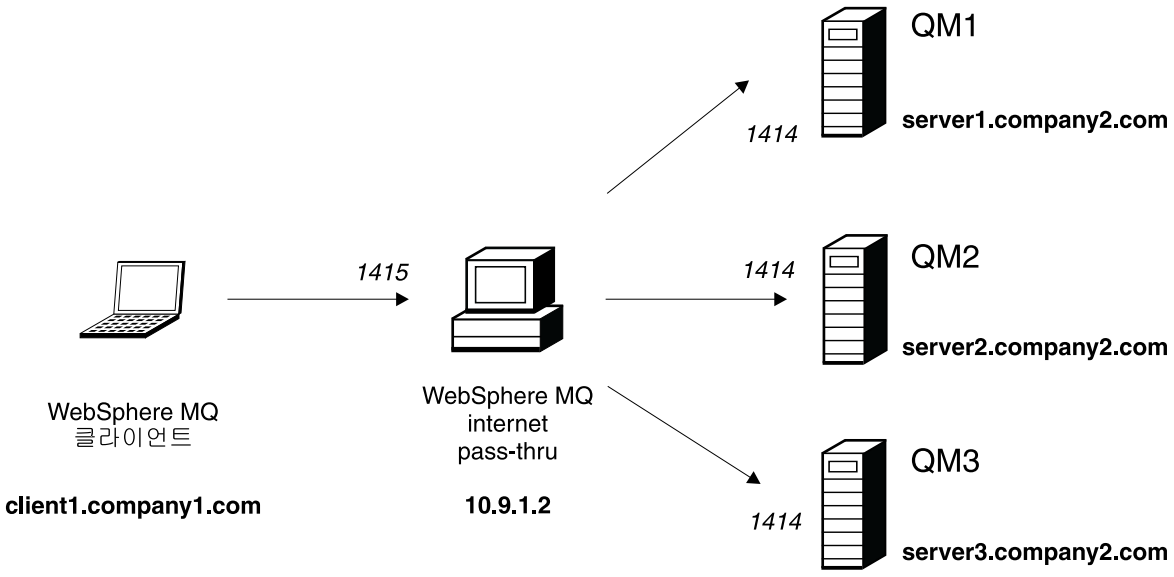

그림 44. 동적 1 라우트 엑시트 네트워크 다이어그램

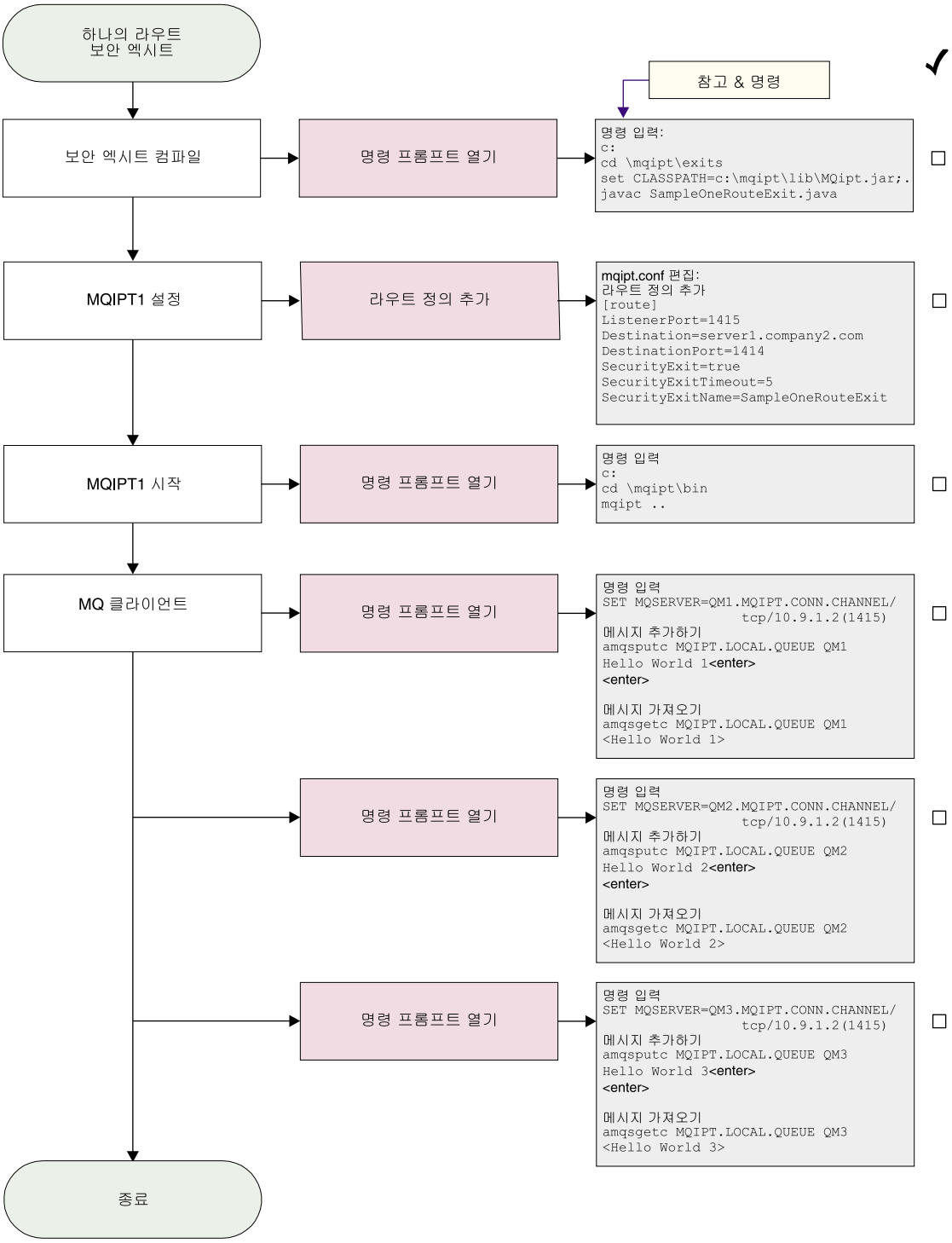

그림 45. 동적 1 라우트 엑시트 구성

1. IPT1에서

   명령 프롬프트를 여십시오.

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

mqipt.conf를 편집하고 라우트 정의를 추가합니다.

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

명령 프롬프트를 여십시오.

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

다음 메시지가 표시되면 성공적으로 완료되었다는 것을 알 수 있습니다.

```
5639-L92 (C) Copyright IBM Corp. 2000, 2003 All Rights Reserved
MQCPI001 Websphere MQ internet pass-thru Version 1.3.0 starting
MQCPI004 Reading configuration information from c:\mqipt\mqipt.conf
MQCPI011 The path c:\mqipt\logs will be used to store the log files
MQCPI006 Route 1415 has started and will forward messages to :
MQCPI034 ....server1.company2.com(1414)
MQCPI035 ....using MQ protocols
MQCPI079 ....using security exit c:\mqipt\exits\SampleOneRouteExit
MQCPI080 ......and timeout of 5 seconds
MQCPI078 Route 1415 ready for connection requests
```

2. WebSphere MQ 클라이언트 시스템의 명령 프롬프트에 다음을 입력합니다.

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

3. 다음을 사용하여 메시지를 넣습니다.

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

4. 다음을 사용하여 메시지를 가져옵니다.

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

그러면 ″Hello world1″을 볼 수 있습니다.

5. WebSphere MQ 클라이언트 시스템의 명령 프롬프트에 다음을 입력합니다.

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

6. 다음을 사용하여 메시지를 넣습니다.

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

7. 다음을 사용하여 메시지를 가져옵니다.

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

그러면 ″Hello world2″를 볼 수 있습니다.

8. WebSphere MQ 클라이언트 시스템의 명령 프롬프트에 다음을 입력합니다.

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

9. 다음을 사용하여 메시지를 넣습니다.

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

10. 다음을 사용하여 메시지를 가져옵니다.

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

그러면 ″Hello world3″을 볼 수 있습니다.

제 21 장 internet pass-thru 감독

이 장에서는 다음과 같은 표제 하에, internet pass-thru 실행을 유지하는 방법에 대해 설명합니다.

- 『유지보수』
- 『문제점 판별』
- 164 페이지의 『성능 조정』

유지보수

다음과 같은 파일은 정상적인 백업 프로시저의 일부로 정기적으로 백업해야 합니다.

- 구성 파일, `mqipt.conf`
- 다음 등록 정보에서 정의된 대로 `mqipt.conf`에 있는 SSL 키 링 파일
  - `SSLClientKeyRing`
  - `SSLClientCAKeyRing`
  - `SSLServerKeyRing`
  - `SSLServerCAKeyRing`
- 다음 등록 정보에서 정의된 대로 `mqipt.conf`에 있는 SSL 키 링 암호 파일
  - `SSLClientKeyRingPW`
  - `SSLClientCAKeyRingPW`
  - `SSLServerKeyRingPW`
  - `SSLServerCAKeyRingPW`
- 관리 클라이언트 구성 파일, `client.conf`. 이 파일은 관리 클라이언트에 알려진 모든 MQIPT에 대한 연결 정보를 포함하고 있습니다.

문제점 판별

문제가 발생했을 때 다음과 같은 경우일 가능성이 크므로 이를 먼저 점검해야 합니다.

- MQIPT 시스템이 방금 설치되었으며 재시동되지 않았습니다.
- HTTP가 큐 관리자에 직접 연결된 라우트에서 참으로 설정되었습니다.
- SSLClient가 큐 관리자에 직접 연결된 라우트에서 참으로 설정되었습니다.
- CLASSPATH가 올바르게 설정되지 않았습니다.
- PATH가 올바르게 설정되지 않았습니다.
- 키 링 파일에 저장된 암호가 대소문자를 구분합니다.

다음 단계는 그림 46에 표시된 순서도를 따릅니다. 번호는 다음 참고를 의미합니다.

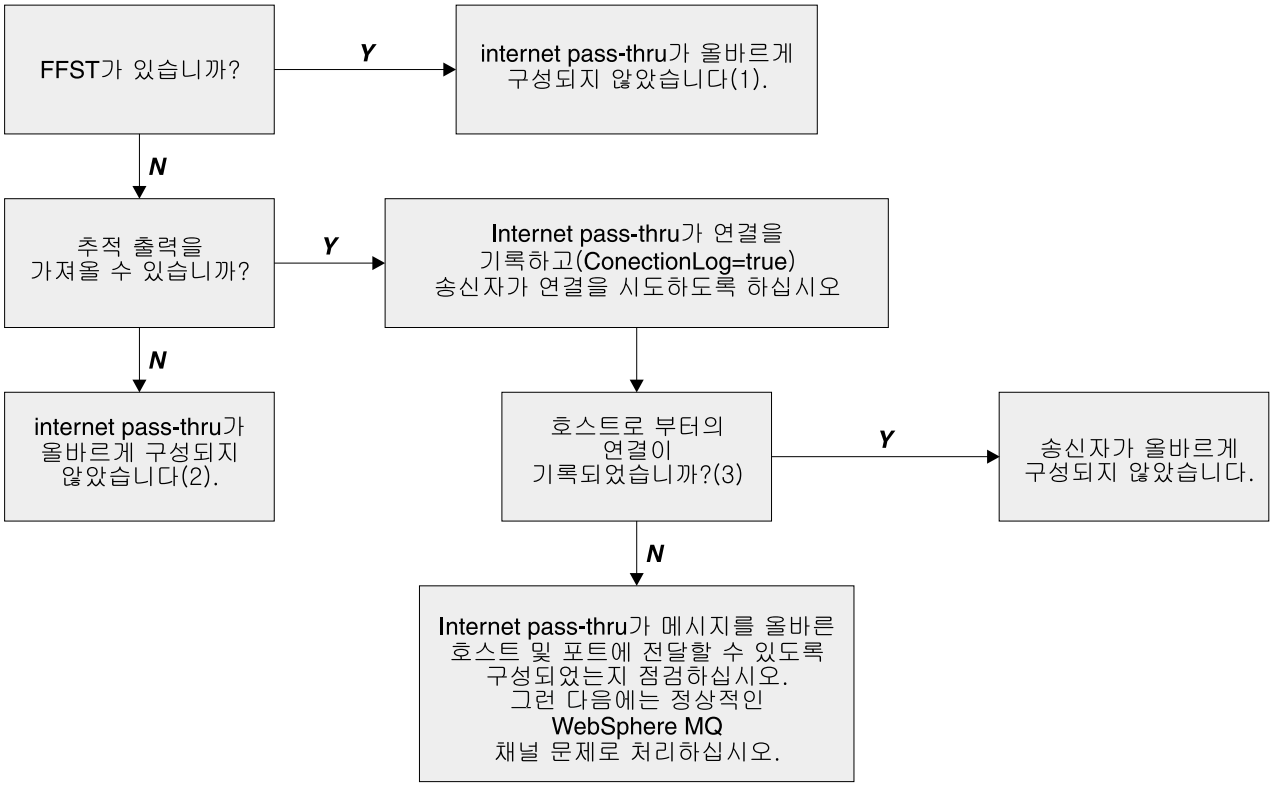

그림 46. 문제점 파악 순서도

주:

1. 오류 서브디렉토리에서 FFST 보고서를 찾으면 MQIPT가 제대로 설치되었는지 알 수 있습니다. 구성에 문제가 있을 수 있습니다.

   각 FFST는 MQIPT 또는 라우트가 시동 프로세스를 종료하도록 하는 원인이 되는 문제점을 보고합니다. 각 FFST의 원인이 되는 문제점을 수정하십시오. 그런 다음 오래된 FFST를 삭제하고 MQIPT를 재시작하거나 새로 고치십시오.
2. MQIPT가 제대로 설치되지 않은 경우에는 모든 파일이 올바른 위치에 배치되었는지, CLASSPATH가 갱신되었는지 점검하십시오. 이 점이 제대로 되었는지 점검하려면 MQIPT를 수동으로 시작하려고 시도해 보십시오.
3. 수동으로 MQIPT 시작.

   명령 프롬프트를 여십시오. `bin` 서브디렉토리로 가서 다음을 입력합니다.

   ```
   mqipt xxx
   ```

   여기서, *xxx*는 MQIPT 홈 디렉토리이며 이 경우에는 " `..`"가 됩니다.

   이렇게 함으로써 MQIPT가 시작되고 홈 디렉토리에서 구성을 찾습니다. `errors` 서브디렉토리에서 오류 메시지와 FFST를 찾으십시오.

MQIPT의 텍스트 출력에서 오류 메시지가 있는지 점검하고 오류를 수정하십시오. FFST를 점검하고 오류를 수정하십시오. 구성 파일의 전역 섹션에 문제점이 있으면 MQIPT가 시작되지 않습니다. 구성 파일의 라우트 섹션에 문제점이 있으면 라우트가 시작되지 않습니다.

internet pass-thru 자동 시작

MQIPT를 Windows NT 서비스로 설치하여 자동으로 시동되도록 변경하면 시스템이 시작될 때 MQIPT가 시작됩니다. MQIPT를 Windows NT 서비스로 설치하려고 시도하기 전에 설치가 제대로 되었는지 확인하기 위해 항상 MQIPT를 수동으로 한 번 시작하십시오. 자세한 내용은 52 페이지의 『Windows 서비스 제어 프로그램 사용』을 참조하십시오

"Unable to locate DLL..."이라는 오류 메시지를 수신하는 이유는 올바르지 않은 `mqiptService` 프로그램을 사용하고 있거나 시스템 PATH 환경 변수를 올바르게 구성하지 않았기 때문입니다. PATH는 반드시 JNI 런타임 라이브러리의 위치를 포함해야 합니다. 이 파일(`jvm.dll`)은 JDK의 클라이언트 서브디렉토리에서 찾을 수 있습니다.

엔드-투-엔드 연결성 점검

MQIPT가 올바르게 설치되었으면 다음 단계는 라우트가 올바르게 설정되었는지 점검하는 일입니다.

구성 파일인 `mqipt.conf`에서 `ConnectionLog` 등록 정보를 참으로 설정하십시오. MQIPT를 시작하거나 새로 고치고 연결을 시도하십시오. 연결 로그는 홈 디렉토리 밑의 로그 디렉토리에 작성됩니다. 연결 로그가 작성되지 않으면 MQIPT가 올바르게 설치되지 않았다는 것을 알 수 있습니다. 연결 시도가 기록되지 않으면 송신자가 올바르게 설치되지 않았다는 의미입니다. 시도가 기록되었으면 MQIPT가 메시지를 올바른 주소로 전달하고 있는지 확인하십시오.

오류 추적

MQIPT는 추적 속성에 의해 제어되는 세밀한 추적 실행 기능을 제공합니다. 각 라우트는 독립적으로 추적될 수 있습니다. 추적 파일은 *xxx*`\errors` 디렉토리에 작성되며 여기서, *xxx*는 `mqipt.conf`를 포함한 디렉토리입니다. 생산된 각 추적 파일은 다음과 같은 형식의 이름을 갖습니다.

`iptroute`*nnnnn*`.trc`

여기서, *nnnnn*은 라우트가 대기하고 있는 포트의 번호입니다. 스레드 핸들링 명령 입력과 같이 특정 라우트와 직접적으로 연관되지 않은 스레드의 `iptmain.trc`라는 별도의 파일에 기록됩니다.

예상치 못한 심각한 오류는 FFST 레코드로서 *xxx*\errors 디렉토리에 있는 오류 로그 파일에 기록되며 여기서, *xxx*는 mqipt.conf를 포함한 디렉토리입니다. FFST 파일의 형식은 다음과 같습니다.

ipt*xxx*.FFST

여기서, *xxx*는 FFST가 생성된 순차입니다. 1이 가장 오래된 것입니다. 오래 실행되는 시스템에서는 시스템이 생성할 수 있는 최대 번호에 이를 수 있습니다. 이런 경우에는 생성된 모든 FFST가 mqipt0.FFST 파일에 기록됩니다. mqipt0.FFST 파일이 작성되면 적절한 시기에 MQIPT를 정지하고 재시작하여 오래된 파일을 삭제해야 합니다.

문제점 보고

IBM 서비스 센터에 문제점을 보고해야 하는 경우에는 다음 정보를 제공하면 문제를 보다 신속하게 해결하는 데 도움이 됩니다.

- IP 주소를 포함하여, 사용 중인 시스템의 간단한 네트워크 다이어그램을 제공해 주십시오.
- 둘 이상의 MQIPT를 사용하고 있는 경우에는 각 MQIPT 시스템의 시스템 시계를 동기화하면 각 MQIPT의 추적 항목을 일치시키는데 도움이 됩니다.
- 오래된 추적 파일을 지웁니다.
- 클라이언트를 실행하여 문제점을 생성해서 추적 파일이 하나의 문제점 인스턴스만 포함하도록 하십시오.
- MQIPT .trc 및 .log 파일의 모든 사본을 보내주십시오.

성능 조정

여기서는 시스템의 성능을 조정하는 몇 가지 포인터를 제공합니다.

스레드 풀 관리

각 라우트의 상대 성능은 스레드 풀과 비활동 시간 종료 스펙을 결합하여 조정할 수 있습니다.

연결 스레드

각 MQIPT 라우트는 수신되는 통신 요청을 핸들링하는 동시에 실행 중인 스레드의 작업 풀에 지정됩니다. 스레드 풀은 라우트의 MinConnectionThreads 속성에서 지정된 크기대로 초기화될 때 작성되며 스레드는 첫 번째로 수신되는 요청을 핸들링하도록 지정됩니다. 이 스레드가 수신되면 스레드가 해당 요청을 즉시 작업하도록 설정되며 다음 스레드가 다음으로 수신되는 요청에 대해 준비되도록 지정됩니다. 모든 스레드가 작업에 지정되면 새 스레드가 작성되어 작업 풀에 추가되며 작업에 대해 지정됩니다. 이런 방식으로 MaxConnectionThreads에 이를 때까지 풀이 증가합니다. 작업 스레드의 수가 MaxConnectionThreads에서 지정된 수가 되면 스레드가 다시 작업 풀로 릴리스될

때까지 다음으로 수신되는 요청이 대기해야 합니다. 이는 라우트의 최대 작업 용량이며 이 이후에는 추가 요청을 승인할 수 없습니다. 대화가 종료되거나 지정된 비활동 시간 종료 기간이 경과하면 스레드가 다시 풀로 릴리스됩니다.

비활동 시간 종료

디폴트로 작업 스레드는 비활동으로 인해 종료되지 않습니다. 스레드가 대화에 지정되었으면 정상적으로 닫히거나 라우트가 비활성화되거나 MQIPT가 종료될 때까지 해당 대화에 지정된 상태로 남습니다. 선택적으로 비활동 시간 종료 간격을 지정하여 분 단위로 지정된 시간 동안 비활동 상태인 스레드를 종료할 수 있습니다. 모니터 스레드는 스레드 비활동 시간을 정기적으로 점검하며 임계값을 초과한 스레드를 종료시킵니다. 스레드를 다시 작업 풀에 배치하여 재사용할 수 있습니다.

제 22 장 메시지

MQIPT는 명령 행에서 실행될 때 콘솔에 정보, 경고 및 오류 메시지의 일부만 표시합니다.

다음을 참고하십시오.

- MQCAxxxx 메시지는 관리 클라이언트 메시지입니다.
- MQCPxxxx 메시지는 MQIPT 메시지입니다.
- MQCxIxxx 메시지는 정보 메시지입니다.
- MQCxWxxx 메시지는 경고 메시지입니다.
- MQCxExxx 메시지는 오류 메시지입니다.

MQCAE001 알 수 없는 호스트: {0}

설명: MQIPT 호스트를 찾을 수 없습니다.

사용자 응답: MQIPT가 있는 호스트 이름을 제대로 지정했는지 점검하십시오.

MQCAE002 시스템이 다음 오류를 보고했습니다: {0}

설명: 오류가 발생했습니다. 다음 시스템 명령 뒤에 오류가 보고되었습니다.

MQCAE005 No valid destination address has been defined

설명: 라우트를 추가할 때 목적지 필드가 공백으로 남아 있습니다.

사용자 응답: 올바른 목적지 주소를 입력하십시오.

MQCAE006 No valid destination port has been defined

설명: 라우트를 추가할 때 목적지 포트 주소 필드가 공백으로 남아 있습니다.

사용자 응답: 올바른 목적지 포트 주소를 입력하십시오.

MQCAE007 No valid listener port has been defined

설명: 라우트를 추가할 때 리스너 포트 주소 필드가 공백으로 남아 있습니다.

사용자 응답: 0에서 65535 사이의 올바른 리스너 포트 주소를 입력하십시오.

MQCAE008 No valid network address has been defined

설명: MQIPT를 추가할 때, 네트워크 주소 필드가 공백으로 남아 있습니다.

사용자 응답: 올바른 네트워크 주소를 입력하십시오.

MQCAE009 No valid command port has been defined

설명: MQIPT를 추가할 때 올바르지 않음 명령 포트 주소가 사용되었습니다.

사용자 응답: 1에서 65535 사이의 올바른 명령 포트 주소를 입력하십시오.

MQCAE010 Could not show online help

설명: 온라인 도움말에 대한 파일이 사용 가능하나 표시할 수 없습니다.

사용자 응답: 웹 브라우저가 설치되었으며 시스템 PATH 환경 변수에서 사용할 수 있는지 확인하십시오.

MQCAE011 Could not parse parameter

설명: 내부 오류가 있어서 테이블 내의 존재하지 않는 매개변수를 갱신하려면 시도가 발생하였습니다.

사용자 응답: 이러한 상태가 지속되면 IBM 기술 지원 담당자에 문의하십시오.

MQCAE012 Could not find online help file {0}

설명: ″passtfrm.htm″ 파일을 찾을 수 없습니다.

사용자 응답: 이 파일을 doc 언어 서브디렉토리에서 액세스할 수 있는지 확인하십시오.

MQCAE013 Interrupted while trying to show online help

설명: 온라인 도움말을 표시하는 중에 시스템 오류가 발생하였습니다.

사용자 응답: 다시 시도하십시오. 이러한 상태가 지속되면 IBM 기술 지원 담당자에게 문의하십시오.

MQCAE015 The password you have just entered has not been recognized

설명: MQIPT가 올바른 암호를 예상하였으나 마지막 명령에 사용된 암호가 올바르지 않았습니다. 구성 파일에서 정의된 것 중 하나와 반드시 일치해야 합니다.

사용자 응답: **MQIPT -> 연결** 패널을 사용하여 암호를 변경하고 마지막 명령을 다시 시도하십시오.

MQCAE016 Node mismatch

설명: 트리에서 선택된 노드와 메모리에 보유된 데이터 간에 내부 불일치가 있습니다.

사용자 응답: 관리 클라이언트를 닫고 명령을 재시도하십시오. 이러한 상태가 지속되면 IBM 기술 지원 담당자에게 문의하십시오.

MQCAE017 Could not create NLS text for message {0}

설명: 정의된 메시지 번호에 대한 NLS 텍스트를 찾을 수 없습니다.

사용자 응답: ″guiadmin.properties″ 파일이 손상되었을 가능성이 있으며 지정된 메시지 번호를 찾을 수 없습니다. 다음 사항을 점검하십시오.

- Readme 파일에 해당되는 새 메시지가 있는지 확인하십시오.
- ″guiadmin.jar″ 파일이 시스템 CLASSPATH에 있는지 확인하십시오.
- ″guiadmin.properties″ 파일이 ″guiadmin.jar″ 파일에 있는지 확인하십시오.
- 메시지 번호가 ″guiadmin.properties″ 파일에 있는지 확인하십시오.

MQCAE018 Could not create NLS text for message MQCAE017

설명: 메시지 번호 {0}을 시스템 등록 정보 목록에서 찾을 수 없습니다.

사용자 응답: ″guiadmin.properties″ 파일이 손상되었을 가능성이 있습니다. 다음 사항을 점검하십시오.

- ″guiadmin.jar″ 파일이 시스템 CLASSPATH에 있는지 확인하십시오.
- ″guiadmin.properties″ 파일이 ″guiadmin.jar″ 파일에 있는지 확인하십시오.
- 메시지 번호가 ″guiadmin.properties″ 파일에 있는지 확인하십시오.

MQCAE019 You have failed to repeat your proposed new password

설명: 암호를 변경할 때 확인할 수 있도록 두 번 입력되지 않았습니다.

사용자 응답: 적절한 필드에 새 암호를 다시 입력하십시오.

MQCAE020 Failed to change MQIPT access parameters

설명: MQIPT 액세스 매개변수를 변경하려고 시도하는 중에 내부 오류가 감지되었습니다.

사용자 응답: 관리 클라이언트를 닫고 명령을 재시도하십시오. 이러한 상태가 지속되면 IBM 기술 지원 담당자에 문의하십시오.

MQCAE021 Internal failure to identify MQIPT

설명: MQIPT에 구성 파일을 저장하려고 시도하는 중에 내부 오류가 감지되었습니다.

사용자 응답: 관리 클라이언트를 닫고 명령을 재시도하십시오. 이러한 상태가 지속되면 IBM 기술 지원 담당자에 문의하십시오.

MQCAE022 Internal failure to save MQIPT configuration

설명: MQIPT에 구성 파일을 저장하려고 시도하는 중에 내부 오류가 감지되었습니다.

사용자 응답: 관리 클라이언트를 닫고 명령을 재시도하십시오. 이러한 상태가 지속되면 IBM 기술 지원 담당자에 문의하십시오.

MQCAE023 MQIPT {0} did not recognize your password.

설명: MQIPT가 올바른 암호를 예상하였으나 마지막 명령에 사용된 암호가 올바르지 않았습니다. 구성 파일에서 정의된 것 중 하나와 반드시 일치해야 합니다.

사용자 응답: **MQIPT -> 연결** 패널을 사용하여 암호를 변경하고 명령을 다시 시도하십시오.

MQCAE024 MQIPT {0}이(가) 명령을 인식하지 않았습니다.

설명: 관리 클라이언트가 인식되지 않은 MQIPT에 명령을 송신하였습니다.

사용자 응답: 관리 클라이언트가 사용한 코드 버전이 MQIPT와 동일한지 확인하십시오.

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

설명: MQIPT가 구성 파일을 송신하려고 시도하였으나 실패하였습니다.

사용자 응답: 관리 클라이언트를 닫고 명령을 재시도하십시오. 명령이 실행되지 않으면 MQIPT를 정지하고 재시작하십시오.

MQCAE026 MQIPT {0}에서 리모트 종료가 사용 안 함으로 설정되어 있습니다.

설명: 구성 파일에서 리모트 종료를 사용할 수 없으므로 MQIPT를 리모트 방식으로 종료하려는 시도가 실패하였습니다.

사용자 응답: MQIPT 리모트 종료를 사용하려면 구성 파일을 편집하여 RemoteShutDown 등록 정보를 참으로 설정하십시오.

MQCAE027 Look and feel {0} is not supported.

설명: 현재 사용하고 있는 플랫폼에 대해 권장되는 룩앤필(look and feel)을 사용할 수 없습니다.

사용자 응답: 시스템 디폴트 룩앤필(look and feel)을 사용하여 계속 처리하십시오.

MQCAE028 Look and feel class {0} cannot be found.

설명: 현재 사용하고 있는 플랫폼에 대해 권장되는 룩앤필(look and feel)을 사용할 수 없습니다.

사용자 응답: 시스템 디폴트 룩앤필(look and feel)을 사용하여 계속 처리하십시오.

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

설명: 최소 연결 스레드 값은 반드시 최대 연결 스레드 값 이하여야 합니다.

사용자 응답: 값을 적절히 변경하십시오.

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

설명: 최대 연결 스레드 값은 반드시 최소 연결 스레드 값보다 커야 합니다.

사용자 응답: 값을 적절히 변경하십시오.

MQCAE031 Port numbers must be in the range 0 to 65535

설명: 조건에 맞지 않는 값을 설정하려고 시도하였습니다.

사용자 응답: 값을 적절히 변경하십시오.

MQCAE032 Trace must be in the range 0 to 5

설명: 조건에 맞지 않는 값을 설정하려고 시도하였습니다.

사용자 응답: 값을 적절히 변경하십시오.

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

설명: 조건에 맞지 않는 값을 설정하려고 시도하였습니다.

사용자 응답: 값을 적절히 변경하십시오.

MQCAE049 No route has been selected on any MQIPT

설명: 먼저 삭제할 라우트를 선택하지 않고 라우트를 삭제하려는 시도를 하였습니다.

사용자 응답: 라우트를 선택하고 명령을 재시도하십시오.

MQCAE050 Could not connect to MQIPT {0}

설명: 관리 클라이언트가 지정된 MQIPT에 연결할 수 없습니다.

사용자 응답: 그 이유는 다음 중 하나일 수 있습니다.

- MQIPT가 실행 중이 아닙니다.
- MQIPT가 해당 명령 포트에서 대기 중이 아닙니다.
- 하나의 관리 클라이언트만이 MQIPT CommandPort를 사용하고 있습니다.
- 요청이 시간 종료되었습니다.

MQCAE051 Could not read reply from MQIPT {0}

설명: 예상된 프로토콜을 준수하지 않는 MQIPT로부터 응답을 수신하였습니다.

사용자 응답: 관리 클라이언트가 사용한 코드 버전이 MQIPT와 동일한지 확인하십시오.

MQCAE052 Configuration has not been saved

설명: MQIPT로부터 올바른 응답을 수신하였으나 그 결과로서 구성 파일 저장이 실패하였습니다.

사용자 응답: MQIPT가 구성 파일에 대한 쓰기 액세스를 갖고 있는 지 점검하십시오.

MQCAE053 MQIPT has not confirmed saving of configuration

설명: 구성 파일이 MQIPT에 송신되었으나 MQIPT가 이를 수신확인하지 못했습니다.

사용자 응답: 그 이유는 다음 중 하나일 수 있습니다.

- MQIPT가 실행 중이 아닙니다.
- MQIPT가 해당 명령 포트에서 대기 중이 아닙니다.
- 하나의 관리 클라이언트만이 MQIPT CommandPort를 사용하고 있습니다.
- 요청이 시간 종료되었습니다.

MQCAE054 MQIPT data has not been refreshed

설명: MQIPT와 접속되었으나 관리 클라이언트가 구성 파일을 읽을 수 없습니다.

사용자 응답: 그 이유는 다음 중 하나일 수 있습니다.

1. MQIPT가 실패했습니다.
2. 요청이 시간 종료되었습니다.

MQCAE055 No MQIPT or route on an MQIPT has been selected

설명: MQIPT 또는 라우트가 선택되지 않아 사용자가 선택한 메뉴 옵션을 수행할 수 없습니다.

사용자 응답: 적절한 MQIPT 또는 라우트를 선택하고 다시 시도하십시오.

MQCAE056 Duplicate listener port has been rejected

설명: 지정된 리스너 포트가 이미 다른 라우트에 의해 사용 중이므로 거부되었습니다.

사용자 응답: 다른 리스너 포트를 선택하고 다시 시도하십시오.

MQCAI002 The MQIPT has been removed from display

설명: 사용자가 트리에서 노드를 선택한 MQIPT가 클라이언트의 메모리에서 제거되었습니다.

MQCAI003 New route added to the display

설명: 방금 지정한 새 라우트가 현재 MQIPT에 추가되었습니다.

MQCAI004 Route has been removed from the display

설명: 사용자가 트리에서 선택한 라우트가 클라이언트의 메모리에서 제거되었습니다.

MQCAI005 Selected MQIPT is being displayed

설명: 사용자가 트리에서 선택한 MQIPT의 전역 매개변수가 테이블에 표시됩니다.

MQCAI006 Selected route is being displayed

설명: 사용자가 트리에서 선택한 라우트의 매개변수가 테이블에 표시됩니다.

MQCAI007 Client configuration has been saved

설명: 트리에 있는 모든 MQIPT에 대한 액세스 매개변수가 저장되었습니다.

MQCAI008 Display of online help succeeded

설명: 요청한 대로 온라인 도움말이 표시되었습니다.

MQCAI009 Table has been updated

설명: 테이블에 방금 입력한 값이 메모리의 모델을 갱신하는 데 사용되었습니다.

MQCAI010 No MQIPT or route has been selected.

설명: 조치에 대한 정보가 충분하지 않아 아무런 조치도 취해지지 않았습니다.

MQCAI011 User Action has been cancelled

설명: 앞에서 시작한 팝업 창 관련 조치를 취소하였습니다.

MQCAI014 Configuration has been saved on MQIPT

설명: 트리에서 현재 선택되어 있는 MQIPT에 관해 새 구성 파일이 저장되었으며 MQIPT를 재시작하는 데 사용할 수 있습니다.

MQCAI015 Online help has terminated

설명: 요청한 대로 온라인 도움말이 표시되었으며 그 결과로서 종료되었습니다.

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

설명: 이 메시지는 트리에 MQIPT가 없을 때 표시되며 MQIPT 추가 방법에 대해 설명합니다.

MQCAI018 New MQIPT added to display

설명: 설명한 대로 새 MQIPT가 트리에 추가되었습니다.

MQCAI019 MQIPT access parameters have been changed

설명: 트리에서 현재 선택되어 있는 MQIPT의 액세스 매개변수가 변경되었습니다.

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

설명: 이 메시지는 테이블에 정보가 표시되지 않을 때 표시되며 정보를 보는 방법에 대해 설명합니다.

MQCAI022 The command port has changed

설명: 명령 포트의 변경을 지시한 MQIPT가 변경되었습니다.

MQCAI023 The password has changed

설명: 방금 변경한 MQIPT와의 추가 통신에서는 새 암호를 사용합니다.

MQCAI025 MQIPT {0}이(가) 새로 고쳐졌습니다.

설명: MQIPT에 보유한 정보가 구성 파일을 읽고 갱신되었습니다.

MQCAI026 MQIPT {0}이(가) 종료 요청을 수신했습니다.

설명: MQIPT가 종료 요청을 수신 확인하였으며 이제 종료하려고 합니다.

MQCAI027 Client configuration has been refreshed

설명: 관리 클라이언트에 표시되는 정보가 로컬 ″client.conf″ 파일에서 새로 고쳐졌습니다.

MQCAI028 MQIPT {0} is active

설명: MQIPT가 ping 요청에 성공적으로 응답하였습니다.

MQCAI029 MQIPT {0} is not active

설명: MQIPT가 지정된 시간 내에 ping 요청에 응답하지 않았습니다.

사용자 응답: 그 이유는 다음 중 하나일 수 있습니다.

- MQIPT가 실행 중이 아닙니다.
- MQIPT가 해당 명령 포트에서 대기 중이 아닙니다.
- 요청이 시간 종료되었습니다. MQIPT용 연결 정보에서 시간 종료 등록 정보를 변경하여 시간 종료 값을 증가시킬 수 있습니다.

MQCAI030 Route {0} is active

설명: MQIPT가 ping 요청에 성공적으로 응답하였습니다.

MQCAI031 Route {0} is not active

설명: MQIPT 라우트가 지정된 시간 내에 ping 요청에 응답하지 않았습니다.

사용자 응답: 그 이유는 다음 중 하나일 수 있습니다.

- MQIPT가 실행 중이 아닙니다.
- MQIPT가 해당 명령 포트에서 대기 중이 아닙니다.
- 요청이 시간 종료되었습니다. MQIPT용 연결 정보에서 시간 종료 등록 정보를 변경하여 시간 종료 값을 증가시킬 수 있습니다.

MQCAI100 This script is used to start the Administration Client for {0}. Specifying a SOCKS proxy will allow the Administrator Client to talk to an MQIPT through a firewall.

설명: mqiptGui 스크립트에 대한 온라인 도움말 정보입니다.

MQCAI101 Format of command is:

설명: mqiptGui 스크립트에 대한 온라인 도움말 정보입니다.

MQCAI102 mqiptGui {socks_host{socks_port}}

설명: mqiptGui 스크립트에 대한 온라인 도움말 정보입니다.

MQCAI103 socks_host-host name of SOCKS proxy (optional)

설명: mqiptGui 스크립트에 대한 온라인 도움말 정보입니다.

MQCAI104 socks_port-SOCKS proxy port address (optional-default 1080)

설명: mqiptGui 스크립트에 대한 온라인 도움말 정보입니다.

MQCPE000 Could not locate message data when handling message {0}

설명: 메시지 번호 {0}을 시스템 등록 정보 목록에서 찾을 수 없습니다.

사용자 응답: ″mqipt.properties″ 파일이 손상되었을 가능성이 있으며 지정된 메시지 번호를 찾을 수 없습니다. 다음 사항을 점검하십시오.

- ″mqipt.jar″ 파일이 시스템 CLASSPATH에 있는지 확인하십시오.
- ″mqipt.properties″ 파일이 ″MQipt.jar″ 파일에 있는지 확인하십시오.
- 메시지 번호가 ″mqipt.properties″ 파일에 있는지 확인하십시오.

MQCPE001 디렉토리가 없거나 디렉토리가 아닙니다.

설명: 초기화할 때 필요한 디렉토리를 찾을 수 없습니다. 이 메시지는 MQIPT 구성 파일인 mqipt.conf 또는 디폴트 디렉토리의 MQIPT 명령 행 시동 옵션에서 지정된 디렉토리를 참조합니다.

사용자 응답: 올바른 디렉토리를 지정하고 명령을 재시도하십시오.

MQCPE004 {0} 포트에서 라우트를 시작하는데 실패했습니다.

설명: 지정된 ListenerPort 번호를 사용하여 라우트를 시작할 수 없습니다.

사용자 응답: 라우트 시동 중에 I/O 오류가 발생하였습니다. 다른 인접 오류 메시지와 로그 레코드에서 문제에 대한 추가 설명을 제공합니다.

MQCPE005 {0} 구성 파일을 찾을 수 없습니다.

설명: 지정된 디렉토리에서 MQIPT 구성 파일인 ″mqipt.conf″를 찾을 수 없습니다.

사용자 응답: 올바른 디렉토리를 지정하고 명령을 재시도하십시오.

MQCPE006 라우트 수가 {0}을(를) 초과했습니다. MQIPT가 시작되나 이 구성이 지원되지 않습니다.

설명: 구성이 MQIPT의 한 인스턴스당 지원되는 최대 라우트 수를 초과하였습니다. 조작은 정지되지 않으나 결과적으로 시스템이 불안정해지거나 과부하가 될 수 있습니다. 명시된 최대 라우트 수를 초과하는 구성은 지원되지 않습니다.

사용자 응답: 인스턴스당 라우트 수를 줄이고 MQIPT의 추가 인스턴스를 시작하는 것을 고려해 보십시오.

MQCPE007 {0} 리스너 포트에서 라우트가 재시작되지 않았습니다.

설명: 새로 고침 조작에서 지정된 ListenerPort에서 조작 중이던 라우트를 새 구성에서 재시작할 수 없습니다.

사용자 응답: 다른 인접 오류 메시지에서 문제에 대한 추가 설명을 점검하십시오.

MQCPE008 {0} 리스너 포트에 대해 중복 라우트가 정의되었습니다.

설명: 동일한 ListenerPort 값을 사용하여 둘 이상의 라우트가 정의되었습니다.

사용자 응답: 구성 파일에서 중복되는 라우트를 제거하고 명령을 재시도하십시오.

MQCPE009 로그 디렉토리 {0}이(가) 올바르지 않습니다.

설명: 텍스트에 표시된 로그 경로가 존재하지 않거나 현재 액세스할 수 없습니다.

사용자 응답: 디렉토리가 존재하는지, MQIPT가 액세스할 수 있는지 점검하십시오.

MQCPE010 리스너 또는 명령 포트 번호 {0}이(가) 올바르지 않습니다.

설명: 명령 포트 또는 리스너 포트 매개변수에 대해 지정된 포트 번호가 올바르지 않습니다.

사용자 응답: 자유롭게 사용할 수 있는 올바른 포트 번호를 지정하십시오. 네트워크에서 포트 번호를 사용하는 것

에 대한 자세한 내용은 네트워크 관리자에게 문의하십시오.

MQCPE011 추적 레벨 {0}이(가) 올바른 범위 0 - 5에 속하지 않습니다.

설명: 지정된 추적 옵션이 요청되었으나 올바른 범위안에 있지 않습니다.

사용자 응답: 0-5 사이의 추적 값을 지정하십시오.

MQCPE012 {0} 값은 {1} 등록 정보에 올바르지 않습니다.

설명: 올바르지 않은 등록 정보 값이 지정되었습니다.

사용자 응답: 각 제어 매개변수의 올바른 값에 관한 자세한 내용을 보려면 이 사용자 안내서를 참조하십시오.

MQCPE013 {0} 라우트에서 ListenerPort 등록 정보를 찾을 수 없습니다.

설명: MQIPT가 ListenerPort 등록 정보를 포함하지 않는 구성 파일에서 라우트를 감지하였습니다. ListenerPort 등록 정보는 각 라우트에 대한 고유한 1차 ID이며 필수 사항입니다.

사용자 응답: 지정된 라우트에 대해 올바른 ListenerPort를 지정하십시오.

MQCPE014 ListenerPort 등록 정보 값 {0}이(가) 올바르지 않습니다.

설명: 라우트의 ListenerPort 등록 정보에 대해 올바르지 않은 포트 주소가 지정되었습니다.

사용자 응답: 포트 주소는 반드시 0-65535 사이의 범위에 있어야 합니다. 구성 파일에서 각 ListenerPort를 점검하십시오.

MQCPE015 메시지 번호 {0}에 대한 텍스트를 찾을 수 없습니다.

설명: 설명할 수 없는 내부 오류가 발견되었습니다.

사용자 응답: ″mqipt.properties″ 파일이 손상되었을 가능성이 있으며 지정된 메시지 번호를 찾을 수 없습니다. 다음 사항을 점검하십시오.

- Readme 파일에 해당되는 새 메시지가 있는지 확인하십시오.
- ″mqipt.jar″ 파일이 시스템 CLASSPATH에 있는지 확인하십시오.
- ″mqipt.properties″ 파일이 ″MQipt.jar″ 파일에 있는지 확인하십시오.
- 메시지 번호가 ″mqipt.properties″ 파일에 있는지 확인하십시오.

MQCPE016 최대 연결 스레드 수는 {0}이나 이 값이 최소 연결 스레드 수 {1}보다 작습니다.

설명: 구성에서 연결 스레드의 최대 수를 초과하는 값을 사용하여 연결 스레드의 최소 수를 지정하였습니다.

사용자 응답: 이렇게 되면 단일 라우트에서 오류가 발생할 수 있으며 전역 등록 정보와 라우트 등록 정보 간에 충돌이 발생하거나 라우트 등록 정보가 시스템 디폴트 값을 대체할 수 있습니다. 올바른 값과 적용 가능한 디폴트 값에 관한 자세한 내용을 보려면 이 사용자 안내서의 이전 장을 참조하십시오.

MQCPE017 {0} 예외가 전달되어 MQIPT가 종료되었습니다.

설명: MQIPT가 비정상적으로 종료되었습니다. 메모리 오버플로우 등의 시스템의 환경적 조건이나 제한조건으로 인해 발생하였을 가능성이 있습니다.

사용자 응답: 이러한 상태가 지속되면 IBM 기술 지원 담당자에 문의하십시오.

MQCPE018 ListenerPort 등록 정보가 공백입니다 - 라우트가 시작되지 않습니다.

설명: 라우트에서 ListenerPort 번호가 생략되었습니다.

사용자 응답: 구성 파일을 편집하고 올바른 ListenerPort를 추가하십시오.

MQCPE019 {0} 스탠자를 {1} 앞에서 찾을 수 없습니다.

설명: 구성 파일에서 순차 오류가 발생하였습니다.

사용자 응답: 구성 파일을 편집하고 모든 [라우트] 항목

이 [전역] 항목 뒤에 있는지 확인하십시오.

MQCPE020 MaxConnectionThreads의 새 값이 {0} 입니다. 이 값은 현재 값 {1}보다 커야 합니다.

설명: 라우트가 시작된 후에는 MaxConnectionThread 등록 정보가 증가되는 것만 가능합니다.

사용자 응답: 구성 파일을 편집하고 MaxConnectionThread 등록 정보를 변경하십시오.

MQCPE021 {0} 라우트의 목적지 등록 정보를 입력하지 않았습니다.

설명: 등록 정보 대상은 라우트 내에서 필수인데, 지정된 라우트에서는 생략되었습니다.

사용자 응답: 구성 파일을 편집하고 지정된 라우트에 대해 목적지 등록 정보를 추가하십시오.

MQCPE022 CommandPort 값 {0}이(가) 올바른 범위 1 - 65535에 속하지 않습니다.

설명: CommandPort 등록 정보가 1-65535 범위를 벗어났습니다.

사용자 응답: 구성 파일을 편집하고 올바른 포트 주소로 CommandPort 등록 정보를 변경하십시오.

MQCPE023 리모트 종료가 사용 안함으로 설정되어 있으므로 {0} 관리 클라이언트로부터의 종료 요청이 무시됩니다.

설명: 구성 파일에서 리모트 종료를 사용할 수 없으므로 MQIPT를 리모트 방식으로 종료하려는 시도가 실패하였습니다.

사용자 응답: MQIPT 리모트 종료를 사용하려면 구성 파일을 편집하여 RemoteShutDown 등록 정보를 참으로 설정하십시오.

MQCPE024 MQIPT 제어기에서 수신한 명령이 인식되지 않았습니다.

설명: MQIPT가 인식할 수 없는 명령 포트를 통해 명령을 수신하였습니다.

사용자 응답: ″mqipt.log″ 파일에서 명령 ID를 점검하십시오.

MQCPE025 호스트 {0}, 포트 {1}에 있는 서버에 연결하는데 실패했습니다.

설명: GUI가 아닌 행 모드 관리 클라이언트가 MQIPT와 통신하는 데 실패했습니다.

사용자 응답: CommandPort 등록 정보가 구성 파일에서 {1}로 지정되어 있는지, MQIPT가 {0}에서 실행 중인지 확인하십시오.

MQCPE026 호스트 {0}, 포트 {1}에 있는 서버로부터 응답이 수신되지 않았습니다.

설명: GUI가 아닌 행 모드 관리 클라이언트가 MQIPT에 연결되었으나 응답을 수신하지 않았습니다.

사용자 응답: 요청이 시간 종료되었거나 MQIPT에 문제가 있음을 표시합니다.

MQCPE027 MQIPT로부터의 응답이 인식되지 않았습니다.

설명: GUI가 아닌 행 모드 관리 클라이언트가 MQIPT에서 인식할 수 없는 응답을 수신하였습니다.

사용자 응답: mqiptAdmin 스크립트가 MQIPT와 동일한 버전의 ″MQipt.jar″ 파일을 사용하는 지 점검하십시오.

MQCPE028 올바르지 않은 스탠자가 감지되었습니다: {0}

설명: 구성 파일에 메시지에서 명시한 인식할 수 없는 스탠자가 발견되었습니다.

사용자 응답: 구성 파일에는 [전역] 및 [라우트] 스탠자만이 유효합니다.

MQCPE029 로그 출력을 비울 수 없습니다.

설명: 통신 버퍼를 비울 수 없어서 일부 메시지를 로그에 기록할 수 없었습니다.

사용자 응답: MQIPT 홈 디렉토리 디스크가 가득 차지 않았는지, MQIPT가 여전히 로그 서브디렉토리에 대한 액세스를 갖고 있는지 확인하십시오.

MQCPE030 CLASSPATH에서 {0}을(를) 찾을 수 없습니다.

설명: 시스템 환경 CLASSPATH 변수에서 지정된 jar 파일을 찾을 수 없습니다.

사용자 응답: 시스템 CLASSPATH에 지정된 파일을 추가하십시오.

MQCPE031 {0} 클래스를 찾을 수 없습니다.

설명: 이 메시지는 MQIPT의 버전 번호를 표시할 때 생성됩니다. 지정된 클래스를 MQIPT jar 파일에서 찾을 수 없거나 시스템 환경 CLASSPATH 변수가 손상되었습니다.

사용자 응답: 지정된 클래스 파일이 ″MQipt.jar″ 파일에 있는지, ″MQipt.jar″ 파일이 시스템 CLASSPATH에 있는지 점검하십시오.

MQCPE033 {0}에 있는 관리 클라이언트에 구성 파일을 송신하는데 실패했습니다.

설명: 관리 클라이언트에 구성 파일을 송신하는 중에 오류가 발생하였습니다.

사용자 응답: 구성 파일이 MQIPT 홈 디렉토리에 있는지, 다른 프로세스에 의해 공유되고 있지 않은 지 점검하십시오.

MQCPE034 {0}에 있는 관리 클라이언트가 올바른 암호를 제공하지 않았습니다.

설명: 구성 파일의 AccessPW 등록 정보가 관리 클라이언트에 의해 제공되는 것과 일치하지 않습니다.

사용자 응답: 구성 파일의 AccessPW 등록 정보를 변경하거나 관리 클라이언트에 저장된 암호를 변경하십시오.

MQCPE035 {0} 포트에 있는 명령 리스너를 시작하는데 실패했습니다.

설명: 지정된 포트 주소에서 명령 리스너를 시작하는 중에 I/O 오류가 발생하였습니다.

사용자 응답: 구성 파일에서 CommandPort 등록 정보에 사용되는 포트 주소를 점검하십시오.

MQCPE038 MQIPT가 예상과 달리 시작되지 않았습니다.

설명: 이 메시지는 MQIPT를 시스템 서비스로 시작하는 mqipt 포크(fork) 프로세스에 의해 생성됩니다.

사용자 응답: 오류 로그를 점검하면 자세한 정보를 볼 수 있습니다. MQIPT가 실행 중인지 점검하기 전에 IPTFork가 사용하는 유휴 시간을 증가시키려고 시도하였습니다. mqiptFork 스크립트를 편집하여 IPTFork에 전달되는 매개변수를 증가시키십시오.

MQCPE039 mqipt 스크립트 실행 중 I/O 오류가 발생했습니다.

설명: 포크(fork) 프로세스에서 MQIPT를 시작하는 중에 오류가 발생하였습니다.

사용자 응답: 시스템 PATH 환경 변수가 JDK의 위치를 포함하고 있는지, mqipt 스크립트가 실행 권한을 갖고 있는지 점검하십시오.

MQCPE040 mqipt 스크립트 실행 중 인터럽트가 발생했습니다.

설명: 포크(fork) 프로세스에서 MQIPT를 시작한 후에 오류가 발생하였습니다.

사용자 응답: 오류 로그를 점검하면 자세한 정보를 볼 수 있습니다. 이러한 상태가 지속되면 IBM 기술 지원 담당자에 문의하십시오.

MQCPE041 지정되지 않는 Java 레벨 - {0}

설명: MQIPT가 지정된 레벨의 Java를 사용하여 시작되었습니다.

사용자 응답: 자세한 정보를 보려면 사용자 안내서에서 필수조건을 점검하십시오.

MQCPE042 {0} 라우트에서 다음 등록 정보 간에 충돌이 있습니다.

설명: 일부 등록 정보는 다른 등록 정보와 함께 사용할 수 없습니다. 이 메시지 다음에는 충돌 관계에 있는 등록 정보 목록이 표시됩니다.

사용자 응답: 다음 오류 메시지를 점검하고 적절한 조치를 취하십시오.

MQCPE043 ....{0}와(과) {1}

설명: 다음 등록 정보는 동일한 라우트에서 동시에 둘 다 설정할 수 없습니다.

사용자 응답: 구성 파일을 편집하고 지정된 등록 정보 중 하나를 지정된 라우트에 대해 사용 안함으로 설정하십시오.

MQCPE044 {0}은(는) {1} 운영 체제에서만 올바릅니다.

설명: MQIPT의 일부 기능은 특정 플랫폼에서만 유효합니다.

사용자 응답: 구성 파일을 편집하고 지정된 등록 정보를 사용 안함으로 설정하십시오.

MQCPE045 ....HTTP 프록시 또는 서버 이름이 누락되었습니다.

설명: HTTP 등록 정보가 참으로 설정되어 있으면 반드시 HTTPProxy 등록 정보를 설정해야 합니다.

사용자 응답: 구성 파일을 편집하고 지정된 라우트에 대해 HTTPProxy를 정의하십시오.

MQCPE046 Pagent가 초기화에 실패했으므로 {0}이(가) 허용되지 않습니다.

설명: Pagent는 MQIPT에 대해 Quality of Service를 제공하는 응용프로그램입니다. MQIPT가 시동 중에 초기화하는 데 실패하였으며 QoS 등록 정보가 지정된 라우트에 대해 참으로 설정되었습니다.

사용자 응답: 구성 파일을 편집하고 지정된 라우트에 대해 QoS를 사용 안함으로 설정하십시오.

MQCPE047 Pagent가 초기화에 실패했습니다.

설명: Pagent는 MQIPT에 대해 Quality of Service를 제공하는 응용프로그램입니다. MQIPT가 시동 중에 초기화하는 데 실패하였습니다.

사용자 응답: Pagent가 사용되고 있지 않으면 이 오류 메시지를 무시해도 됩니다. 단, 반드시 QoS 등록 정보를 거짓으로 설정해야 합니다.

MQCPE048 {0}에서 라우트를 시작하는데 실패했습니다. 예외는 다음과 같습니다: {1}

설명: 지정된 ListenerPort 번호를 사용하여 라우트를 시작할 수 없습니다.

사용자 응답: 다른 인접 오류 메시지와 로그 레코드에서 문제에 대한 추가 설명을 제공합니다.

MQCPE049 {0} Java 보안 관리자를 시작 또는 정지하는 중 오류가 발생했습니다.

설명: Java 보안 관리자를 시작 또는 정지하려고 시도하는 중에 예외가 전달되었습니다.

사용자 응답: Java 보안 관리자를 이전에 사용할 수 있었으나 런타임 권한을 사용할 수 없습니다. 로컬 정책 파일에 setSecurityManager에 대한 RuntimePermission을 추가하십시오. 변경 사항을 적용하려면 반드시 MQIPT를 재시작해야 합니다.

MQCPE050 관리 클라이언트로부터의 연결을 승인하는 중 {0} 포트에서 보안 예외가 발생했습니다.

설명: 관리 클라이언트로부터 연결을 승인하는 중에 보안 예외가 전달되었습니다.

사용자 응답: Java 보안 관리자를 이전에 사용할 수 있었으나 오류 메시지에서 식별된 호스트에 대한 권한이 부여되지 않았습니다. 호스트가 MQIPT에 연결될 수 있도록 허용하려면 CommandPort의 포트 주소의 연결 승인/결정에 SocketPermission을 추가하십시오. 변경 사항을 적용하려면 반드시 Java 보안 관리자를 재시작해야 합니다.

MQCPE051 {0} 라우트에서 연결을 승인하는 중 보안 예외가 발생했습니다.

설명: 관리 라우트 상의 연결을 승인하는 중에 보안 예외가 전달되었습니다.

사용자 응답: Java 보안 관리자를 이전에 사용할 수 있었으나 오류 메시지에서 식별된 호스트에 대한 권한이 부여되지 않았습니다. 호스트가 이 라우트에 연결될 수 있도

록 허용하려면 ListenerPort에 대한 연결 승인/결정에 SocketPermission을 추가하십시오. 변경 사항을 적용하려면 반드시 Java 보안 관리자를 재시작해야 합니다.

MQCPE052 {0} 라우트에서의 연결 요청이 실패했습니다: {1}

설명: 이 메시지는 연결 요청에 대한 보안 예외를 기록하기 위해 연결 로그에서 발행됩니다.

사용자 응답: Java 보안 관리자를 이전에 사용할 수 있었으나 오류 메시지에서 식별된 호스트에 대한 권한이 부여되지 않았습니다. 호스트가 이 라우트에 연결될 수 있도록 허용하려면 ListenerPort에 대한 연결 승인/결정에 SocketPermission을 추가하십시오. 변경 사항을 적용하려면 반드시 Java 보안 관리자를 재시작해야 합니다.

MQCPE053 {0}({1})에 연결하는 중 보안 예외가 발생했습니다.

설명: 관리 라우트 상의 연결을 설정하는 중에 보안 예외가 전달되었습니다.

사용자 응답: Java 보안 관리자를 이전에 사용할 수 있었으나 오류 메시지에서 식별된 호스트에 대한 권한이 부여되지 않았습니다. 호스트가 이 라우트에 연결될 수 있도록 허용하려면 ListenerPort에 대한 연결 승인/결정에 SocketPermission을 추가하십시오. 변경 사항을 적용하려면 반드시 Java 보안 관리자를 재시작해야 합니다.

MQCPE054 {0}({1})(으)로의 연결 요청이 실패했습니다: {2}

설명: 이 메시지는 대상 호스트에 대한 연결 요청에 관한 보안 예외를 기록하기 위해 연결 로그에서 발행됩니다.

사용자 응답: Java 보안 관리자를 이전에 사용할 수 있었으나 오류 메시지에서 식별된 호스트에 대한 권한이 부여되지 않았습니다. 호스트가 이 라우트에 연결될 수 있도록 허용하려면 ListenerPort에 대한 연결 승인/결정에 SocketPermission을 추가하십시오. 변경 사항을 적용하려면 반드시 Java 보안 관리자를 재시작해야 합니다.

MQCPE055 ....Socks 프록시 이름이 누락되었습니다.

설명: SocksClient 등록 정보가 참으로 설정되어 있으면 반드시 SocksProxy 등록 정보를 설정해야 합니다.

사용자 응답: 구성 파일을 편집하고 지정된 라우트에 대해 SocksProxy를 정의하십시오.

MQCPE056 라우트 등록 정보와의 충돌.

설명: 일부 등록 정보는 다른 등록 정보와 함께 사용할 수 없습니다.

사용자 응답: 콘솔 메시지에서 오류의 자세한 내용에 대해 점검하고 적절한 조치를 취하십시오.

MQCPE057 SSL 프로토콜({0})이 인식되지 않았습니다.

설명: 라우트가 SSL 프록시 모드에 배치되었으며 초가 데이터 플로우가 인식되지 않습니다.

사용자 응답: 이 라우트에 대해 SSL 연결만 작성되었는지 확인하십시오.

MQCPE058 {2}({3}) - {0}({1})에 대한 CONNECT 요청에 실패했습니다

설명: HTTP 서버로의 SSL 터널을 작성하기 위한 HHTTP CONNECT 요청이 HTTP 프록시로 송신되었습니다. HTTP 프록시가 이 요청에 ″200 OK″ 응답을 다시 송신하지 않았습니다.

사용자 응답: 여러 가지 문제점이 원인이 될 수 있습니다. 라우트에서 추적을 사용하고 연결을 재시도하십시오. 추적 파일에 실제 오류가 표시됩니다.

MQCPE059 정의된 키 링 파일이 없습니다.

설명: 최소한 하나의 키 링 파일을 지정하지 않고 SSL 클라이언트나 서버를 정의했습니다.

사용자 응답: SSLClientKeyRing 및 SSLClientCAKeyRing 등록 정보를 클라이언트측에 사용하거나 SSLServerKeyRing 및 SSLServerCAKeyRing을 서버측에 사용하여 키 링 파일을 정의한 다음 라우트를 재시작하십시오.

MQCPE060 SSL 클라이언트 연결 시간 종료를 {0} 초로 설정하는 중 런타임 오류가 발생했습니다.

설명: 시간 종료 값을 설정하는 클라이언트측에서 SSL 런타임 오류가 발생했습니다.

사용자 응답: SSLClientConnectTimeout 등록 정보에 지정한 값이 올바른지 점검하십시오. 지정된 라우트에서 추적을 실행하면 추가 오류 정보가 표시됩니다.

MQCPE061 사용된 암호 세트가 없습니다.

설명: SSL 클라이언트 또는 서버 연결이 시작되었으나 MQIPT가 올바른 암호 모음을 판별할 수 없습니다.

사용자 응답: 정의된 키 링 파일에 올바른 인증이 있는지 점검하십시오. 사용된 인증 및 암호화 알고리즘의 생성에 사용된 개인용 키와 공용 키는 MQIPT 서적에 있는 지원되는 암호 모음 목록을 준수해야 합니다.

MQCPE062 SSL 암호 세트 {0}을(를) 설정하는 중 런타임 오류가 발생했습니다.

설명: 클라이언트측 또는 서버측에서 지원되지 않는 SSL 암호 모음을 정의했습니다.

사용자 응답: SSLClientCipherSuites 또는 SSLServerCipherSuites에 지정한 값이 올바르고 이 연결에 지원되는지 확인하십시오. 지정된 라우트에서 추적을 실행하면 사용 가능한 암호 모음 목록이 표시됩니다. MQIPT 서적에 지원되는 암호 모음 목록이 있습니다.

MQCPE063 {0} 파일이 이미 존재합니다 - 바꾸기 옵션 사용

설명: mqiptPW 스크립트에 지정한 파일 이름 매개변수가 이미 있습니다.

사용자 응답: 다른 파일 이름을 선택하거나 바꾸기 옵션을 사용할 수 있습니다.

MQCPE064 암호 해독 키 생성 중 런타임 오류가 발생했습니다: \n {0}

설명: 키 링 파일을 여는 데 사용된 암호를 해독하기 위해 암호 키를 생성하는 중에 오류가 발생했습니다.

사용자 응답: 메시지에 나열된 런타임 오류를 수정하고 명령을 다시 실행해야 합니다.

MQCPE065 ....LDAP 서버 이름이 누락되었습니다.

설명: LDAP가 등록 정보가 참으로 설정되어 있으면 반드시 LDAPServer1 또는 LDAPServer2 등록 정보를 설정해야 합니다.

사용자 응답: 구성 파일을 편집하고 지정된 라우트에 대해 LDAPServer*를 정의하십시오.

MQCPE066 ....LDAPServer{0}Password 등록 정보의 LDAP 암호가 누락되었습니다.

설명: LDAP 사용자 ID는 암호없이 지정되었습니다.

사용자 응답: 구성 파일을 편집하고 지정된 라우트에 대해 LDAPServer*Password를 정의하십시오.

MQCPE067 ....LDAP 서버의 SSLClient 또는 SSLServer가 누락되었습니다.

설명: LDAP가 등록 정보가 참으로 설정되어 있으면 반드시 SSLClient 또는 SSLServer 등록 정보를 설정해야 합니다.

사용자 응답: 구성 파일을 편집하고 지정된 라우트에 대해 SSLClient 또는 SSLServer를 정의하십시오.

MQCPE068 ....보안 엑시트 이름이 누락되었습니다.

설명: SecurityExit 등록 정보가 참으로 설정되어 있으면 반드시 SecurityExitName 등록 정보를 설정해야 합니다.

사용자 응답: 구성 파일을 편집하고 지정된 라우트에 대해 SecurityExitName을 정의하십시오.

MQCPE069 보안 엑시트 응답에 올바르지 않은 포트 주소 {0}이(가) 있습니다.

설명: SecurityExitResponse에 지정한 포트 주소가 올바르지 않습니다.

사용자 응답: 포트 주소는 반드시 1024-65535 사이의 범위에 있어야 합니다.

MQCPE070 보안 엑시트 응답에 알 수 없는 이유 코드 {0}이(가) 있습니다.

설명: SecurityExitResponse에 지정한 이유 코드가 지원되지 않습니다.

사용자 응답: 지원되는 이유 코드의 목록은 MQIPT 서적을 참조하십시오.

MQCPE071 {0}에 작성 중 오류가 발생했습니다.

설명: 지정된 파일을 작성 또는 갱신하는 중에 오류가 발생했습니다. 오류 메시지에는 발생된 예외도 포함되어 있습니다.

사용자 응답: 예외에 나열된 오류를 수정하고 명령을 다시 실행해야 합니다.

MQCPE072 보안 엑시트 {0}에서 알 수 없는 오류가 발생했습니다.

설명: 연결 요청을 유효화하는 중에 사용자 정의된 보안 엑시트에서 오류가 발생했습니다.

사용자 응답: 보안 엑시트에서 추적을 사용하고 연결 요청을 다시 시도하십시오. 보안 엑시트 추적 파일에 오류가 기록됩니다.

MQCPI001 {0} 시작 중

설명: 이 MQIPT 인스턴스가 실행을 시작합니다. 추가적인 초기화 메시지가 표시될 것입니다.

MQCPI002 {0} 종료 중

설명: MQIPT가 종료되려고 합니다. STOP 명령을 사용하여 종료되거나 구성 오류로 인해 성공적인 시동 또는 REFRESH 조치를 취할 수 없는 경우에는 자동으로 종료됩니다.

MQCPI003 {0}이(가) 종료되었습니다

설명: 종료 프로세스가 완료되었습니다. 모든 MQIPT 프로세스가 종료되었습니다.

MQCPI004 {0}에서 구성 정보를 읽는 중

설명: MQIPT 구성 파일인 mqipt.conf가 이 메시지에서 지정한 디렉토리로부터 읽힙니다.

MQCPI005 리스너 포트가 비활성으로 지정되어 있습니다 - {0} -> {1}({2})

설명: 이 메시지에서 언급된 라우트가 비활성으로 표시되었습니다. 이 라우트에서는 통신 요청이 승인되지 않습니다.

MQCPI006 {0} 라우트가 시작 중이며 다음으로 메시지를 전달합니다.

설명: 이 메시지에 표시된 리스너 포트에서 라우트가 시작되었습니다. 이 메시지 다음에는 이 라우트와 연관된 모든 등록 정보를 나열한 다른 메시지가 표시됩니다. 메시지 MQCPI078은 라우트가 연결을 승인할 수 있을 때 발행됩니다.

MQCPI007 {0} 라우트가 정지되었습니다.

설명: 지정된 ListenerPort에서 작업 중이던 라우트가 종료됩니다. 이 조치는 일반적으로 MQIPT에 대해 REFRESH 명령이 발행되고 라우트 구성이 변경되었을 때 발생합니다.

MQCPI008 {0} 포트에서 제어 명령 대기 중

설명: 이 THIS 인스턴스가 지정된 포트에서 제어 명령이 발행되도록 대기하고 있습니다.

MQCPI009 제어 명령이 수신되었습니다: {0}

설명: 이 메시지는 명령 포트에서 제어 명령이 수신되었음을 표시합니다. 해당되는 경우에 한해 메시지에 자세한 내용이 포함됩니다.

MQCPI010 {0}에서 명령 포트 정지 중

설명: REFRESH 조작에서 명령 포트가 더 이상 새 구성에서 사용되지 않습니다. 명령이 지정된 포트에서 더 이상 승인되지 않습니다.

MQCPI011 {0} 경로가 로그 파일을 저장하는데 사용됩니다.

설명: 출력 로그 기록이 현재 구성 하의 메시지에서 지정된 위치로 전달됩니다.

사용자 응답: 구성이 수정되고 REFRESH 조작이 요청되면 변경될 수 있습니다.

MQCPI012 라우트가 시작된 후에는 MinConnectionThreads의 값 변경이 효력을 가지지 않습니다.

설명: 최소 수의 연결 스레드가 라우트 시동에 지정되었으며 MQIPT가 재시작될 때까지 변경될 수 없습니다.

MQCPI013 {0}에서 {1} 호스트로의 연결이 닫혔습니다.

설명: 이 메시지는 연결 활동을 기록하기 위해 연결 로그에서 발행됩니다.

MQCPI014 Eyecatcher 프로토콜({0})이 인식되지 않습니다.

설명: 이 메시지는 연결 활동을 기록하기 위해 연결 로그에서 발행됩니다.

MQCPI015 이 라우트에서 클라이언트 액세스를 사용하지 않았습니다.

설명: 이 메시지는 연결 활동을 기록하기 위해 연결 로그에서 발행됩니다.

MQCPI016 이 라우트에서 큐 관리자 액세스를 사용하지 않았습니다.

설명: 이 메시지는 연결 활동을 기록하기 위해 연결 로그에서 발행됩니다.

MQCPI017 {0}에 있는 큐 관리자가 {1} 호스트에 연결되었습니다.

설명: 이 메시지는 연결 활동을 기록하기 위해 연결 로그에서 발행됩니다.

MQCPI018 {0}에 있는 클라이언트가 {1} 호스트에 연결되었습니다.

설명: 이 메시지는 연결 활동을 기록하기 위해 연결 로그에서 발행됩니다.

MQCPI019 {0}개의 라우트를 작성했습니다 - 이 값은 지원되는 최대 라우트 수인 {1}을(를) 초과합니다.

설명: 지원되는 라우트 최대 수를 초과하였습니다.

사용자 응답: MQIPT는 계속하여 조작하려고 하지만 두 번째 인스턴스를 작성하여 이 두 인스턴스가 라우트를 나누도록 권장합니다.

MQCPI020 구성 파일이 {0} 관리 클라이언트로 송신되었습니다.

설명: 관리 클라이언트로부터의 요청 결과로 구성 파일이 송신되었습니다.

MQCPI021 명령 포트에서 암호 점검이 사용으로 설정되었습니다.

설명: 이 메시지는 명령 포트에 액세스하기 위해 암호가 필요하다는 것을 표시합니다.

MQCPI022 명령 포트에서 암호 점검이 사용 안함으로 설정되었습니다.

설명: 이 메시지는 명령 포트에 액세스하기 위해 암호가 필요하지 않다는 것을 표시합니다.

MQCPI024 ....및 {0}({1})에 있는 HTTP 프록시

설명: 이 메시지는 해당 라우트에 대해 보내는 연결이 이 HTTP 프록시를 사용하여 작성될 것임을 나타냅니다.

MQCPI025 {0} 관리 클라이언트가 요청한 새로 고침이 완료되었습니다.

설명: REFRESH 명령을 수신한 결과, MQIPT가 구성 파일을 다시 읽고 재시작되었습니다.

MQCPI026 {0} 관리 클라이언트가 종료를 요청했습니다.

설명: STOP 명령을 수신한 결과, MQIPT가 종료됩니다.

MQCPI027 {0}이(가) {2} 포트에 있는 {1}(으)로 송신되었습니다.

설명: GUI가 아닌 행 모드 관리 클라이언트에 의해 지정된 MQIPT에 송신된 시스템 콘솔 명령을 표시합니다.

MQCPI031 .....암호 스위트 {0}

설명: 이 메시지는 이 라우트를 사용하는 암호 모음을 나열합니다.

MQCPI032 .....키 링 파일 {0}

설명: 이 메시지는 해당 라우트에 대한 키 링의 파일 이름을 표시합니다.

MQCPI033 .....클라이언트 인증이 {0}(으)로 설정되어 있습니다

설명: 이 메시지는 SSL 서버가 해당 라우트에 대해 클라이언트 인증을 요청하는지 여부를 정의합니다.

MQCPI034 ....{0}({1})

설명: 이 메시지는 해당 라우트에 대한 목적지 및 목적지 포트 주소를 표시합니다.

MQCPI035 ....{0} 사용 중

설명: 이 메시지는 목적지에서 사용하는 프로토콜을 표시합니다. MQSeries 프로토콜, HTTP 터널링 또는 HTTP 청킹 중 하나입니다.

MQCPI036 ....등록 정보에 SSL 클라이언트측이 사용으로 설정되어 있습니다.

설명: 이 메시지는 라우트가 SSL을 사용하여 데이터를 목적지 호스트에 송신할 것임을 나타냅니다.

MQCPI037 ....등록 정보에 SSL 서버측이 사용으로 설정되어 있습니다.

설명: 이 메시지는 라우트가 SSL을 사용하여 송신 호스트로부터 데이터를 수신할 것임을 나타냅니다.

MQCPI038 .....피어 인증이 {0}을(를) 사용합니다.

설명: 이 메시지는 피어 인증 제어에 사용되는 식별 이름을 나열합니다.

MQCPI039 ....및 {0}({1})에 있는 Socks 프록시

설명: 이 메시지는 해당 라우트에 대해 보내는 연결이 MQIPT가 명령 행으로부터 시작될 때 정의된 이 Socks 프록시를 사용하여 작성될 것임을 나타냅니다.

MQCPI040 {0} 관리 클라이언트가 명령 포트에 액세스했습니다.

설명: 이 메시지는 시스템 콘솔 및 MQIPT 로그 파일(로그 기록이 가능한 경우에 한함)에 작성됩니다. MQIPT가 관리 클라이언트로부터 연결을 수신하였습니다.

MQCPI041 ....{0} 모드로 Network Dispatcher advisor 요청에 응답합니다.

설명: 이 메시지는 라우트가 시작될 때 시스템 콘솔에 작성됩니다. Network Dispatcher advisor에 응답할 때 어떤 모드의 MQIPT를 사용할 것인지 표시합니다. 올바른 옵션은 "정상" 및 "바꾸기" 모드입니다.

MQCPI042 {0} 라우트에서 최대 연결 수에 이르렀습니다 - 추가적인 요청이 블로킹됩니다.

설명: 이 메시지는 지정된 라우트에 대해 최대 수의 연결에 도달했을 때 시스템 콘솔에 기록됩니다. 연결이 사용 가능해지거나 MaxConnectionThreads 값이 증가될 때까지 추가적인 요청이 차단됩니다.

MQCPI043 {0} 라우트의 연결이 블로킹 해제되었습니다.

설명: 이 메시지는 지정된 라우트가 연결 요청에 대한 차단이 해제될 때 시스템 콘솔에 기록됩니다.

MQCPI044 MQIPT가 시스템 시동으로 시작되었습니다.

설명: MQIPT가 시스템 서비스로 시작되었습니다.

MQCPI045 시스템 시동으로 MQIPT 시작 중

설명: MQIPT가 시스템 서비스로 시작되려고 합니다.

MQCPI046 MQIPT가 시스템 시동으로 시작되는 동안 {0}초간 휴면 중

설명: MQIPT가 시스템 서비스로서 성공적으로 시작되었는지 검사하기 전에 포크(fork) 프로세스가 유휴 상태로 있을 시간을 지정합니다.

MQCPI047 .....CA 키 링 파일 {0}

설명: 이 메시지는 해당 라우트에 대한 CA 키 링의 파일 이름을 표시합니다.

MQCPI048 {0} 관리 클라이언트에 의한 ping이 완료되었습니다.

설명: 관리 클라이언트에 대한 IPTController로부터의 응답 메시지입니다.

MQCPI049 ....목적지에 대한 QoS 우선순위 = {0}, 호출자에 대한 QoS 우선순위 = {1}

설명: 라우트를 따라 진행되는 양 방향에서 소통될 우선순위를 표시합니다.

MQCPI050 inittab에 시스템 시동 시 MQIPT를 자동으로 시작하는 항목 추가 중

설명: 사용자가 MQIPT를 시스템 서비스로 시작하기 위해 mqiptService 스크립트를 실행하였습니다.

MQCPI051 inittab에서 시스템 시동 시 MQIPT를 자동으로 시작하는 항목 제거 중

설명: 사용자가 시스템 서비스로 시작하는데서 MQIPT를 제거하기 위해 mqiptService 스크립트를 실행하였습니다.

MQCPI052 ....Socks 서버측이 사용으로 설정되어 있습니다.

설명: 이 라우트는 SOCKS 서버(프록시) 역할을 할 것이며 socksified 응용프로그램으로부터 연결을 승인할 것입니다.

MQCPI053 Java 보안 관리자 시작 중

설명: SecurityManager 등록 정보가 참으로 설정되면서 디폴트 Java 보안 관리자가 시작될 것입니다.

MQCPI054 Java 보안 관리자 정지 중

설명: SecurityManager 등록 정보가 거짓으로 설정되면서 디폴트 Java 보안 관리자가 정지될 것입니다.

MQCPI055 java.security.policy를 {0}에 설정 중

설명: 디폴트 Java 보안 관리자가 시작되려고 하며 제공되는 정책 파일을 사용할 것입니다.

MQCPI056 새 정책 파일을 사용하려면 Java 보안 관리자를 재시작해야 합니다.

설명: SecurityManagerPolicy 등록 정보가 변경되었으나 Java 보안 관리자가 재시작될 때까지 적용되지 않습니다.

사용자 응답: SecurityManager 등록 정보를 거짓으로 변경하고 새로 고침 명령을 발행하여 Java 보안 관리자를 정지하십시오. 그런 다음, SecurityManager를 다시 참으로 설정하고 한 번 더 새로 고침 명령을 발행하여 새 정책 파일을 가진 Java 보안 관리자를 시작하십시오.

MQCPI057 ....추적 레벨 {0}이(가) 사용으로 설정되어 있습니다.

설명: 이 메시지는 라우트가 시작될 때 시스템 콘솔에 작성됩니다. 해당 라우트에 대해 사용할 수 있는 추적 레벨을 표시하는 데 사용됩니다.

MQCPI058 ....및 URI 이름 {0}

설명: 이 메시지는 라우트가 시작될 때 시스템 콘솔에 작성됩니다. 해당 라우트에 관한 Uniform Resource Identifier 이름을 표시하는 데 사용됩니다.

MQCPI059 ....servlet 클라이언트가 사용으로 설정되어 있습니다.

설명: 이 메시지는 라우트가 시작될 때 시스템 콘솔에 작성됩니다. 이 라우트는 MQIPT servlet에 연결됩니다.

MQCPI060 시스템 시동 시 MQIPT를 자동으로 시작하는 파일 설치 중

설명: 사용자가 MQIPT를 시스템 서비스로 시작하기 위해 mqiptService 스크립트를 실행하였습니다.

MQCPI061 시스템 시동 시 MQIPT를 자동으로 시작하는 파일 제거 중

설명: 사용자가 시스템 서비스로 시작하는데서 MQIPT를 제거하기 위해 mqiptService 스크립트를 실행하였습니다.

MQCPI064 ....이 라우트에 SSL 인증이 없습니다.

설명: 이 메시지는 라우트가 시작될 때 시스템 콘솔에 작성되며, 익명 암호 모음이 지정되었으므로 이 라우트에 대해 사용되는 SSL 인증이 없음을 표시합니다.

MQCPI065 ....SSL 프록시 모드로

설명: 이 메시지는 라우트가 시작될 때 시스템 콘솔에 작성되어 이 라우트가 SSL 프록시 모드에서 작업 중임을 표시합니다.

MQCPI066 ....및 {0}{1}에 있는 HTTP 서버

설명: 이 메시지는 해당 라우트에 대해 보내는 연결이 이 HTTP 서버를 사용하여 작성될 것임을 나타냅니다.

MQCPI067 TQoS 런타임 라이브러리에 링크 설정

설명: mqiptQoS 스크립트를 실행하여 실제 TQoS 런타임 라이브러리에 링크시켰습니다.

MQCPI068 TQoS 런타임 라이브러리에 대한 링크 제거

설명: mqiptQoS 스크립트를 실행하여 실제 TQoS 런타임 라이브러리로의 링크를 제거했습니다.

MQCPI069 ....로컬 주소 {0}에 바인딩

설명: 이 메시지는 각 연결이 바인딩된 로컬 IP 주소를 표시합니다. 멀티홈 시스템에서만 사용해야 합니다.

MQCPI070 ....로컬 포트 주소 범위 {0}-{10} 사용

설명: 이 메시지는 연결에 사용할 로컬 포트 주소를 표시합니다. 이를 통해 방화벽 관리자는 MQIPT로부터의 연결을 제한할 수 있습니다.

MQCPI071 사이트 인증이 {0}을(를) 사용합니다.

설명: 이 메시지는 사이트 인증의 선택 제어에 사용되는 식별 이름을 나열합니다.

MQCPI072 .....및 인증 레이블 {0}

설명: 이 메시지는 사이트 인증의 선택 제어에 사용되는 레이블 이름을 나열합니다.

MQCPI073 갱신된 파일 {0}

설명: mqiptPW 스크립트에 지정한 파일 이름이 갱신되었습니다.

MQCPI074 작성된 파일 {0}

설명: mqiptPW 스크립트에 지정한 파일 이름이 작성되었습니다.

MQCPI075 ....{0}({1})에 있는 LDAP 기본 서버

설명: 이 메시지는 CRL 지원에 사용된 기본 LDAP 서버의 이름을 나열합니다.

MQCPI076 ....{0}({1})에 있는 LDAP 백업 서버

설명: 이 메시지는 CRL 지원에 사용된 백업 LDAP 서버의 이름을 나열합니다.

MQCPI077 ....LDAP 오류가 무시됩니다.

설명: 이 메시지는 LDAP에서 수신한 오류가 무시됨을 나타냅니다.

MQCPI078 연결 요청을 위해 {0} 라우트 준비.

설명: 이 메시지는 라우트가 연결 요청을 승인할 수 있을 때 표시됩니다.

MQCPI079 ....보안 엑시트 {0} 사용

설명: 이 메시지는 라우트가 시작될 때 시스템 콘솔에 작성됩니다. 보안 엑시트의 완전한 이름을 표시하는 데 사용됩니다.

MQCPI080 .....및 {0} 초의 시간 종료

설명: 이 메시지는 라우트가 시작될 때 시스템 콘솔에 작성됩니다. 보안 엑시트의 시간 종료 값을 표시하는 데 사용됩니다.

MQCPI081 WebSphere MQ internet pass-thru의 시작 메시지

설명: WebSphere MQ internet pass-thru의 메시지를 서비스로 시작합니다.

MQCPI082 WebSphere MQ internet pass-thru의 정지 메시지

설명: WebSphere MQ internet pass-thru의 메시지를 서비스로 정지합니다.

MQCPI083 ....새로 고침 명령은 라우트를 재시작하지 않습니다.

설명: 이 메시지는 refresh 명령을 발행했을 때 라우트가 재시작되지 않았음을 나타냅니다.

MQCPI084 ....CRL 캐시 시간 종료는 {0} 시간입니다.

설명: 이 콘솔 메시지는 CRL(또는 ARL)이 MQIPT 캐시에 남아있는 시간을 표시합니다.

MQCPI085 ....CRL은 키 링 파일에 저장됩니다.

설명: 이 콘솔 메시지는 LDAP 서버에서 검색한 CRL(또는 ARL)이 연관된 CA 인증에 첨부된 키 링 파일에 저장됨을 의미합니다.

MQCPI086 .....{0} 의 시간 종료(초)

설명: 이 메시지는 라우트가 시작될 때 시스템 콘솔에 작성됩니다. LDAP 서버 연결에 대한 시간 종료 값을 표시하는 데 사용됩니다.

MQCPI087 .....사용자 ID는 {0}입니다.

설명: 이 메시지는 라우트가 시작될 때 시스템 콘솔에 작성됩니다. LDAP 서버에 연결할 사용자 ID 이름을 표시하는 데 사용됩니다.

MQCPI100 이 스크립트는 {0}을(를) 시작하는 데 사용됩니다.

설명: mqipt 스크립트의 온라인 도움말 메시지입니다.

MQCPI101 명령 형식은 다음과 같습니다.

설명: mqipt 스크립트의 온라인 도움말 메시지입니다.

MQCPI102 mqipt {dir_name}

설명: mqipt 스크립트의 온라인 도움말 메시지입니다.

MQCPI103 dir_name - mqipt.conf가 있는 디렉토리

설명: mqipt 스크립트의 온라인 도움말 메시지입니다.

MQCPI106 이 스크립트는 현재 버전 번호를 표시하는 데 사용됩니다.

설명: mqiptVersion 스크립트의 온라인 도움말 메시지입니다.

MQCPI107 mqiptVersion {-v}

설명: mqiptVersion 스크립트의 온라인 도움말 메시지입니다.

MQCPI108 여기서 -v는 빌드 시간 소인도 표시합니다.

설명: mqiptVersion 스크립트의 온라인 도움말 메시지입니다.

MQCPI109 이 스크립트는 시스템 시동 시 다른 JVM에서 {0}을(를) 시작하는데 사용되며 mqipt.ske에서만 사용됩니다. 명령행에서 MQIPT를 시작하려면 mqipt 스크립트를 사용하십시오.

설명: mqiptFork 스크립트의 온라인 도움말 메시지입니다.

MQCPI110 이 클래스는 콘솔에 간단한 NLS 메시지를 표시하는데 사용됩니다.

설명: IPTMessages 클래스의 온라인 도움말 메시지입니다.

MQCPI111 java com.ibm.mq.ipt.IPTMessages (message_id1) {message_id2} {message_id...}

설명: IPTMessages 클래스의 온라인 도움말 메시지입니다.

MQCPI112 여기서 message_id는 mqipt.properties 파일에 있는 하나의 키와 일치합니다.

설명: IPTMessages 클래스의 온라인 도움말 메시지입니다.

MQCPI113 이 스크립트는 MQIPT를 시스템 서비스로서 관리하는데 사용됩니다.

설명: mqiptService 스크립트의 온라인 도움말 메시지입니다.

MQCPI114 mqiptService (-install | -remove)

설명: mqiptService 스크립트의 온라인 도움말 메시지입니다.

MQCPI115 -install 시동 시 MQIPT를 자동으로 시작하는 파일을 설치합니다.

설명: mqiptService 스크립트의 온라인 도움말 메시지입니다.

MQCPI116 -remove 시동 시 MQIPT를 자동으로 시작하는 파일을 제거합니다.

설명: mqiptService 스크립트의 온라인 도움말 메시지입니다.

MQCPI117 이 스크립트는 TQoS 런타임 라이브러리로의 링크를 관리하는 데 사용됩니다.

설명: mqiptService 스크립트의 온라인 도움말 메시지입니다.

MQCPI118 mqiptQoS (-install | -remove)

설명: mqiptService 스크립트의 온라인 도움말 메시지입니다.

MQCPI119 -install 실제 TQoS 런타임 라이브러리에 링크를 설정합니다.

설명: mqiptService 스크립트의 온라인 도움말 메시지입니다.

MQCPI120 -remove 실제 TQoS 런타임 라이브러리에 대한 링크를 제거합니다.

설명: mqiptService 스크립트의 온라인 도움말 메시지입니다.

MQCPI121 암호를 암호화하고 파일에 저장하려면 이 스크립트를 사용하십시오.

설명: mqiptPW 스크립트의 온라인 도움말 메시지입니다.

MQCPI122 mqiptPW password file_name { -replace }

설명: mqiptPW 스크립트의 온라인 도움말 메시지입니다.

MQCPI123 password - 키 링 파일을 열기 위해 사용되는 암호

설명: mqiptPW 스크립트의 온라인 도움말 메시지입니다.

MQCPI124 file_name - 암호화된 암호는 이 파일에 저장됩니다.

설명: mqiptPW 스크립트의 온라인 도움말 메시지입니다.

MQCPI125 바꾸기 옵션은 기존 파일을 갱신하기 위해 사용되어야 합니다.

설명: mqiptPW 스크립트의 온라인 도움말 메시지입니다.

MQCPI126 mqipt (-start | -stop)

설명: mqiptQoS 스크립트의 온라인 도움말 메시지입니다.

MQCPW001 {0}의 CRL이 만기되었습니다.

설명: 이 메시지는 CRL(또는 ARL)이 LDAP 서버나 키 링 파일에서 검색될 때 표시됩니다.

사용자 응답: LDAP 서버나 키 링 파일에 지정한 CRL을 갱신하십시오.

MQCPW002 CRL로 키 링 파일 {0}을(를) 갱신하는 중 오류가 발생했습니다.

설명: 이 메시지는 LDAPSaveCRL 등록 정보를 사용했으나 지정된 키 링 파일을 갱신할 수 없을 때 표시됩니다.

사용자 응답: 지정된 파일이 손상되었을 수 있습니다. 다음 사항을 점검하십시오.

1. MQIPT에 대한 쓰기 액세스 권한이 사용 가능해야 함
2. 다른 응용프로그램에서 파일을 열지 않음

MQCPW003 ....만기된 CRL이 무시됩니다.

설명: 이 콘솔 메시지는 만기된 CRL(또는 ARL)이 무시되고 연결 요청이 허용될 수 있음을 나타냅니다.

부록. 주의사항

다음 단락은 현지법과 상충하는 국가에서는 적용되지 않습니다.

IBM은 타인의 권리 비침해, 상품성 및 특정 목적에의 적합성에 대한 묵시적 보증을 포함하여(단, 이에 한하지 않음) 묵시적이든 명시적이든 어떠한 종류의 보증없이 이 책을 현상태대로 제공합니다. 일부 국가에서는 특정 거래에서 명시적 또는 묵시적 보증의 면책사항을 허용하지 않으므로, 이 사항이 적용되지 않을 수도 있습니다.

이 책에서 IBM 제품 또는 서비스를 언급하는 것이 IBM이 영업하는 모든 국가에서 이들 제품 또는 서비스를 사용할 수 있다는 것을 의미하지는 않습니다.

이 책에서 IBM 라이센스 프로그램에 대해 언급하는 것이 IBM의 라이센스 프로그램 또는 기타 제품만을 사용할 수 있다는 의미는 아닙니다. 지적 재산권을 침해하지 않는 범위내에서 기능적으로 동등한 모든 프로그램을 IBM 제품 대신 사용할 수 있습니다. IBM이 명시적으로 지정한 제품을 제외한 다른 제품과 관련된 조작을 평가하고 검증하는 것은 사용자의 책임입니다.

IBM은 이 책에서 다루고 있는 특정 내용에 대해 특허를 보유하고 있거나 현재 특허 출원 중일 수 있습니다. 이 책을 제공한다고 해서 특허에 대한 라이센스까지 부여하는 것은 아닙니다. 라이센스에 대한 의문사항은 다음으로 문의하십시오.

135-270
서울특별시 강남구 도곡동 467-12, 군인공제회관빌딩
한국 아이.비.엠 주식회사
고객만족센터
전화번호: 080-023-8080

본 문서에 포함된 정보는 어떠한 공식적인 IBM 테스트에도 제출되지 않았으며 현상태대로 분배됩니다. 정보의 사용 및 해당 기술의 구현은 고객의 책임이며 고객의 평가 능력 및 운영 환경에의 통합 능력에 따라 결정됩니다. IBM은 각 항목에 대해 정확도를 높이기 위해 특정 환경에서 검토하였으며 다른 환경에서도 동일하거나 유사한 결과가 산출된다는 보장을 하지 않습니다. 이러한 기술을 자체 환경에 적용하려고 시도하는 고객은 스스로 위험을 감수해야 합니다.

상표

다음 용어는 미국 또는 기타 국가에서 사용되는 IBM Corporation의 상표입니다.

AIX	FFST	First Failure Support Technology
IBM	IBMLink	MQSeries
SupportPac	WebSphere	

Microsoft, Windows, Windows NT 및 Windows 로고는 미국 또는 기타 국가에서 사용되는 Microsoft Corporation의 상표입니다.

Java 및 모든 Java 기반 상표는 미국이나 기타 국가에서 사용되는 Microsoft Corporation의 상표 또는 등록상표입니다.

UNIX는 미국 또는 기타 국가에서 Open Group의 등록상표입니다.

기타 회사, 제품 및 서비스 이름은 타사의 상표 및 서비스표입니다.

참고 문헌

이 서적은 설치된 제품의 일부로서 HTML 형식으로 사용할 수 있습니다. HTML은 doc\<locale>\html\& lt;filename>.zip 디렉토리에 자동 압축 해제 파일로 들어 있습니다. 관리 클라이언트를 사용하기 전에 반드시 <locale>\html 서브디렉토리에 있는 파일의 압축을 풀어야 합니다. 이 서적은 다음과 같은 언어 버전이 있습니다. 언어 및 해당되는 파일 이름을 보려면 아래 표를 참조하십시오.

표 4. 언어 및 파일 이름 요약

언어	로케일	**HTML** 파일 이름
중국어	zn_CN	amqyzb01.zip
독일어	de_DE	amqygb01.zip
일본어	ja_JP	amqyjb01.zip
한국어	ko_KR	amqykb01.zip
브라질 포르투갈어	pt_BR	amqybb01.zip
스페인어	es_ES	amqysb01.zip
영어(미국)	en_US	amqyab01.zip

번역된 PDF는 다음 URL에서 다운로드받을 수 있습니다.

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

다음은 사용 가능한 언어입니다.

표 5. PDF 언어 및 파일 이름

언어	로케일	**PDF** 파일 이름
중국어	zn_CN	amqyzb01.pdf
독일어	de_DE	amqygb01.pdf
일본어	ja_JP	amqyjb01.pdf
한국어	ko_KR	amqykb01.pdf
브라질 포르투갈어	pt_BR	amqybb01.pdf
스페인어	es_ES	amqysb01.pdf
영어(미국)	en_US	amqyab01.pdf

또한 다음 서적을 참조할 수도 있습니다.

- *WebSphere MQ 상호통신*, SA30-1575
- *WebSphere MQ 시스템 관리 안내서*, SA30-1583
- *WebSphere MQ 클라이언트*, GA30-1574
- *WebSphere MQ Queue Manager Clusters*, SC34-6061

이러한 서적은 WebSphere MQ 채널 및 그 속성의 정의, 특히 CONNAME의 정의에 관한 정보를 제공합니다.

WebSphere MQ 간행물을 보려면 다음을 참조하십시오.

http://www.ibm.com/webspheremq/library

색인

[가]

[다]

[마]

[바]

[사]

[아]

M

N

O

P

Q

R

S

T

U

W

X

IBM에 의견 보내기

이서적에 관해 특별히 좋게 생각하는 점이나 나쁘게 생각하는 점이 있으면 다음 방법 중 하나를 선택하여 IBM에 귀하의 의견을 보내 주십시오.

이서적의 정확도, 구성, 주제 또는 완성도 등에 관한 특정한 오류 또는 누락 등 어떠한 점에 관해서든 의견을 보내주시기 바랍니다.

단, 이서적의 내용이나 전달 방식에 대한 의견만 해당됩니다.

IBM 제품 또는 시스템의 기능에 대한 의견은 IBM 담당자나 IBM이 권한을 부여한 재판매인에게 말씀해 주시기 바랍니다.

귀하가 IBM에 의견을 보내는 경우에는 적절하다고 판단되는 방법을 사용하여 귀하의 의견을 사용하거나 배포할 수 있는 비독점적인 권리를 IBM에 부여한 것으로 간주합니다. 단 귀하에게는 어떠한 의무도 부과되지 않습니다.

다음과 같은 방법으로 IBM에 의견을 보낼 수 있습니다.

- 우편:

  135-270
  서울특별시 강남구 도곡동 467-12, 군인공제회관빌딩
  한국 아이.비.엠 주식회사
  고객만족센터

- 팩스:
  - 영국 외: 국제 전화 코드 다음에 44-1962-816151을 사용하십시오.
  - 3781-5200

- 전자우편 보내기:
  - IBM 메일 교환: IBMMAIL의 GBIBM2Q9
  - IBMLink™: HURSLEY(IDRCF)
  - ibmkspoe@kr.ibm.com

사용하는 방법을 불문하고 다음 정보를 제공해 주십시오.

- 간행물 제목 및 주문 번호
- 의견을 제시하는 주제
- 귀하의 이름, 주소, 전화 번호, 팩스 번호 및 네트워크 ID

IBM 한글 지원에 관한 설문

FAX : (02) 3787-0123

보내 주시는 의견은 더 나은 고객 지원 체제를 위한 귀중한 자료가 됩니다.
독자 여러분의 좋은 의견을 기다립니다.

책 제목: WebSphere MQ internet Passthru 버전 1.3

책 번호: SA30-1615-01

성 명		직위/담당업무	
회 사 명		부 서 명	
주 소			
전화번호		팩스번호	
전자우편 주소			
사용중인 시스템	o 중대형 서버 o UNIX 서버 o PC 및 PC 서버		

1. IBM에서 제공하는 한글 책자와 영문 책자 중 어느 것을 더 좋아하십니까? 그 이유는 무엇입니까?
   ☐ 한글 책자 ☐ 영문 책자
   (이유:)

2. 본 책자와 해당 소프트웨어에서 사용된 한글 용어에 대한 귀하의 평가 점수는?
   ☐ 수 ☐ 우 ☐ 미 ☐ 양 ☐ 가

3. 본 책자와 해당 소프트웨어에서 번역 품질에 대한 귀하의 평가 점수는?
   ☐ 수 ☐ 우 ☐ 미 ☐ 양 ☐ 가

4. 본 책자의 인쇄 상태에 대한 귀하의 평가 점수는?
   ☐ 수 ☐ 우 ☐ 미 ☐ 양 ☐ 가

5. 한글 소프트웨어 및 책자가 지원되는 분야에 대해 귀하는 어떻게 생각하십니까?
   ☐ 한글 책자를 늘려야 함 ☐ 현재 수준으로 만족
   ☐ 그다지 필요성을 느끼지 않음

6. IBM은 인쇄물 형식(hardcopy)과 화면 형식(softcopy)의 두 종류로 책자를 제공합니다. 어느 형식을 더 좋아하십니까?
   ☐ 인쇄물 형식(hardcopy) ☐ 화면 형식(softcopy) ☐ 둘 다

IBM 한글 지원 서비스에 대해 기타 제안사항이 있으시면 적어주십시오.

☺ 설문에 답해 주셔서 감사합니다.
귀하의 의견은 저희에게 매우 소중한 것이며, 고객 여러분들께 보다 좋은 제품을 제공해 드리기 위해 최선을 다하겠습니다.

Printed in Australia

SA30-1615-01