

9.1

IBM MQ 보안

IBM

참고

이 정보와 이 정보가 지원하는 제품을 사용하기 전에, [591 페이지의 『주의사항』](#)에 있는 정보를 확인하십시오.

이 개정판은 새 개정판에 별도로 명시하지 않는 한, IBM® MQ의 버전 9 릴리스 1 및 모든 후속 릴리스와 수정에 적용됩니다.

IBM은 귀하가 IBM으로 보낸 정보를 귀하의 권리를 침해하지 않는 범위 내에서 적절하다고 생각하는 방식으로 사용하거나 배포할 수 있습니다.

© Copyright International Business Machines Corporation 2007년, 2024.

목차

보안 설정	5
보안 업데이트.....	5
보안 개요.....	5
보안 개념 및 메커니즘.....	5
IBM MQ 보안 메커니즘.....	19
보안 요구사항 계획.....	71
식별 및 인증 계획.....	72
권한 부여 계획.....	74
기밀성 계획.....	88
데이터 무결성 계획.....	95
감사 계획.....	95
토폴로지에 의한 보안 계획.....	96
방화벽 및 인터넷 Passthru.....	109
IBM MQ for z/OS 보안 구현 체크리스트.....	110
보안 설정.....	112
UNIX, Linux, and Windows에서 보안 설정.....	112
IBM i에서 보안 설정.....	137
z/OS에서 보안 설정.....	165
IBM MQ MQI client 보안 설정.....	240
IBM i에서 SSL 또는 TLS에 대한 통신 설정.....	242
UNIX, Linux 또는 Windows에서 SSL 또는 TLS에 대한 통신 설정.....	243
z/OS에서 SSL 또는 TLS에 대한 통신 설정.....	244
SSL/TLS에 대한 작업.....	244
사용자 식별 및 인증.....	295
권한이 있는 사용자.....	297
MQCSP 구조를 사용하여 사용자 식별 및 인증.....	299
보안 엑시트에서 식별 및 인증 구현.....	299
메시지 엑시트에서 ID 맵핑.....	300
API 엑시트와 API 교차 엑시트에서 ID 맵핑.....	300
폐기된 인증서에 대한 작업.....	301
플러그 가능한 인증 방법(PAM) 사용.....	312
오브젝트에 액세스 권한 부여.....	312
권한 부여에 사용되는 사용자 판별.....	312
UNIX, Linux, and Windows에서 OAM을 사용하여 오브젝트에 대한 액세스 제어.....	314
자원에 대한 필수 액세스 부여.....	323
UNIX, Linux, and Windows 에서 IBM MQ 를 관리하는 권한.....	361
UNIX, Linux, and Windows 에서 IBM MQ 오브젝트에 대한 작업 권한.....	363
보안 엑시트에서 액세스 제어 구현.....	367
메시지 엑시트에서 액세스 제어 구현.....	368
API 엑시트 및 API 교차 엑시트에서 액세스 제어 구현.....	369
LDAP 권한 부여.....	369
설정 권한 부여.....	370
권한 부여 표시.....	372
LDAP 권한 부여 사용 시의 기타 고려사항.....	373
OS와 LDAP 권한 부여 모델 간 전환.....	374
LDAP 관리.....	374
메시지의 기밀성.....	375
CipherSpec 사용 가능.....	376
SSL 및 TLS 비밀 키 재설정.....	400
사용자 엑시트 프로그램에서 기밀성 구현.....	401
데이터 세트 암호화를 사용한 IBM MQ for z/OS의 저장 데이터 기밀성.....	402
IBM MQ for z/OS 데이터 세트 암호화 단계의 개요.....	403

큐 관리자 활성 로그 암호화 방법 예.....	404
큐 공유 그룹에서의 z/OS 데이터 세트 암호화에 대한 고려사항.....	406
z/OS 데이터 세트 암호화 사용 시 역방향 마이그레이션 고려사항.....	407
메시지의 데이터 무결성.....	410
감사.....	410
클러스터 보안 유지.....	410
권한 없는 큐 관리자가 메시지를 전송하는 것을 중지.....	411
권한 없는 큐 관리자가 메시지를 사용자의 큐에 넣는 것을 중지.....	411
리모트 클러스터 큐에 메시지를 넣는 권한 부여.....	412
큐 관리자가 클러스터에 조인하는 것을 방지.....	412
필요하지 않은 큐 관리자는 클러스터에서 강제로 제거.....	414
큐 관리자가 메시지 수신하는 것을 방지.....	414
SSL/TLS 및 클러스터.....	415
발행/구독 보안.....	417
발행/구독 보안 설정 예.....	424
구독 보안.....	436
큐 관리자 간의 발행/구독 보안.....	438
IBM MQ Console 및 REST API 보안.....	440
사용자 및 역할 구성.....	442
REST API 및 IBM MQ Console과 함께 클라이언트 인증서 인증 사용.....	452
REST API로 HTTP 기본 인증 사용.....	456
REST API로 토큰 기반 인증 사용.....	457
IFrame에 IBM MQ Console 임베드.....	458
REST API에 대해 CORS 구성.....	459
IBM MQ Console 및 REST API에 대한 호스트 헤더 유효성 검증 구성.....	460
감사.....	461
Security considerations for the IBM MQ Console and REST API on z/OS.....	461
UNIX, Linux, and Windows에서 키 및 인증서 관리.....	466
UNIX, Linux, and Windows 의 runmqckm및 runmqakm 명령.....	467
UNIX, Linux, and Windows 의 runmqckm및 runmqakm 옵션.....	476
UNIX, Linux, and Windows 의 runmqakm 오류 코드.....	479
데이터베이스 인증의 보호 세부사항.....	486
Managed File Transfer 보호.....	487
MFT 및 IBM MQ 연결 인증.....	487
MFT 샌드박스.....	492
MFT의 SSL 또는 TLS 암호화 구성.....	498
채널 인증으로 클라이언트 모드의 큐 관리자에 연결.....	499
Connect:Direct 브릿지 에이전트와 Connect:Direct 노드 사이에서 SSL 또는 TLS 구성.....	500
AMQP 클라이언트 보안 설정.....	502
AMQP 클라이언트 인계 제한.....	504
AMQP 채널용 JAAS 구성.....	505
Advanced Message Security.....	506
Advanced Message Security의 개요.....	506
Advanced Message Security 설치 개요.....	545
z/OS에서 감사.....	545
키 저장소 및 인증서 사용.....	547
Advanced Message Security 보안 정책 관리.....	570
주의사항.....	591
프로그래밍 인터페이스 정보.....	592
상표.....	592

IBM MQ 보안 설정

보안은 IBM MQ 애플리케이션 개발자와 IBM MQ 시스템 관리자 모두에게 중요한 고려사항입니다.

보안 업데이트

보안 구역 및 운영자 워크스테이션에 있는 모든 하드웨어 및 소프트웨어에 대해 지원 라이프사이클이 만료되지 않고, 필수 소프트웨어 업데이트로 업그레이드되고, 보안 업데이트가 공개되는 즉시 적용되도록 하십시오.

다음 항목에 대한 보안 업데이트에 관한 추가 정보를 찾아볼 수 있습니다.

- 모든 플랫폼([IBM Security Bulletin](#))
- z/OS®의 보안 및 시스템 무결성 APAR([IBM Z System Integrity 포털](#))

보안 개요

이 토픽 컬렉션은 IBM MQ 보안 개념을 소개합니다.

보안 개념 및 메커니즘은 모든 컴퓨터 시스템에 적용되기 때문에 이는 처음에 표시되고 그 뒤에 해당 보안 메커니즘에 대한 설명이 오며 이는 IBM MQ에서 구현됩니다.

보안 개념 및 메커니즘

이 주제 모음에서는 IBM MQ 설치에서 고려해야 하는 보안 측면에 대해 설명합니다.

공통적으로 허용되는 보안 관점은 다음과 같습니다.

- [5 페이지의 『식별 및 인증』](#)
- [6 페이지의 『권한 부여』](#)
- [6 페이지의 『감사』](#)
- [6 페이지의 『기밀성』](#)
- [7 페이지의 『데이터 무결성』](#)

보안 메커니즘은 보안 서비스를 구현하는 데 사용되는 기술적인 도구와 기술들입니다. 메커니즘은 특정 서비스를 제공하기 위해 독자적으로 또는 다른 메커니즘으로 작동됩니다. 공통 보안 메커니즘의 예제는 다음과 같습니다.

- [7 페이지의 『암호화』](#)
- [9 페이지의 『메시지 요약 및 디지털 서명』](#)
- [9 페이지의 『디지털 인증서』](#)
- [13 페이지의 『공개 키 기반 구조\(PKI\)』](#)

IBM MQ 구현을 계획 중인 경우 사용자에게 중요한 보안 관점을 구현하기 위해 필요한 보안 메커니즘을 고려하십시오. 이러한 토픽을 읽은 후에 고려해야 할 사항에 대한 자세한 정보는 [71 페이지의 『보안 요구사항 계획』](#)의 내용을 참조하십시오.

관련 개념

[244 페이지의 『SSL/TLS에 대한 작업』](#)

이 주제에서는 IBM MQ를 사용하여 TLS 사용과 관련된 단일 태스크를 수행하기 위한 지시사항을 제공합니다.

관련 태스크

[TLS를 사용하여 두 개의 큐 관리자 연결](#)

식별 및 인증

식별은 시스템 사용자 또는 시스템에서 실행 중인 애플리케이션을 고유하게 식별하는 기능입니다. 인증은 사용자 또는 애플리케이션이 청구되는 진짜 사용자나 애플리케이션임을 증명해주는 기능입니다.

예를 들어, 사용자 ID와 비밀번호를 입력하여 시스템에 로그인하는 사용자를 고려해 보십시오. 시스템은 사용자 식별에 사용자 ID를 사용합니다. 시스템은 로그인 시에 입력한 비밀번호가 올바른지 검사하여 사용자를 인증합니다.

부인 방지

부인 방지 서비스는 식별 및 인증 서비스의 확장으로 볼 수 있습니다. 일반적으로 부인 방지는 데이터가 전자적으로 전송될 때 적용됩니다. 예를 들어, 주식을 사거나 팔기 위한 주식 중개인의 주문이나 한 계좌에서 다른 계좌로 자금을 이체하기 위한 은행의 주문 등입니다.

부인 방지 서비스는 결국 특정 메시지가 특정 개인과 연관되는지를 증명하기 위해서 사용됩니다.

부인 방지 서비스는 둘 이상의 컴포넌트를 포함할 수 있고 이들 각각의 컴포넌트는 다른 기능을 제공합니다. 메시지의 송신자가 송신했다는 것을 거부하면, 원본 증명이 있는 부인 방지 서비스가 수신자에게 그 특정 개인이 메시지를 송신했다는 거부할 수 없는 증거를 제공할 수 있습니다. 메시지의 수신자가 그것을 수신하는 것을 거부하면, 전달의 증명이 있는 부인 방지 서비스가 송신자에게 그 특정 개인이 메시지를 수신했다는 거부할 수 없는 증거를 제공할 수 있습니다.

실제로, 사실상 100% 확신을 가지는 증명, 또는 거부할 수 없는 증거는 어려운 목표입니다. 실제 상황에서는 어떤 것도 완전하게 보안되지는 않습니다. 보안 관리는 비즈니스가 받아들일 수 있는 레벨로 위험을 관리한다는 의미로 받아들여집니다. 이런 환경에서 부인 방지 서비스의 보다 현실적인 기대치는, 용인될 만한 증거를 제공하고 법원에서 사건을 지원할 수 있는 정도입니다.

부인 방지는 IBM MQ가 데이터를 전자적으로 전송하는 수단이기 때문에 IBM MQ 환경에서 적합한 보안 서비스입니다. 예를 들면, 특정 메시지가 송신되었거나 특정 개인과 연관된 애플리케이션에 의해 수신되었다는 동시 증거가 필요할 수 있습니다.

Advanced Message Security의 IBM MQ는 기본 기능의 일부로 부인 방지 서비스를 제공하지 않습니다. 그렇지만 이 제품 문서는 IBM MQ 환경 내에서 자체 엑시트 프로그램을 작성하여 자체적으로 부인 방지 서비스를 제공할 수 있는 방법에 대한 제한을 포함하고 있습니다.

관련 개념

[19 페이지의 『IBM MQ에서의 식별 및 인증』](#)

IBM MQ에서 메시지 컨텍스트 정보 및 상호 인증을 사용하여 식별 및 인증을 구현할 수 있습니다.

권한 부여

권한 부여는 권한 있는 사용자 및 해당 애플리케이션으로만 액세스를 제한하여 시스템에서 중요한 자원을 보호합니다. 자원을 권한 없이 사용하는 것이나 권한이 부여되지 않은 방식으로 사용하는 것을 막습니다.

관련 개념

[19 페이지의 『IBM MQ에서 권한 부여』](#)

특정 개인이나 애플리케이션이 IBM MQ 환경에서 수행할 수 있는 작업을 제한하기 위해 권한 부여할 수 있습니다.

감사

감사는 예상치 못한 또는 권한이 없는 활동이 발생했는지 또는 이런 활동 수행 시도가 있었는지를 감지하기 위해 이벤트를 기록 및 검사하는 프로세스입니다.

권한 설정 방법에 대한 자세한 정보는 [74 페이지의 『권한 부여 계획』](#) 및 관련 하위 주제를 참조하십시오.

관련 개념

[20 페이지의 『IBM MQ의 감사』](#)

IBM MQ는 일반적이지 않은 활동이 발생하는 레코드에 이벤트 메시지를 발행할 수 있습니다.

기밀성

기밀성 서비스는 기밀 정보가 권한 없이 노출되는 것을 막습니다.

민감한 데이터가 로컬에 저장되어 있는 경우, 데이터에 액세스할 수 없으면 읽을 수 없다는 가정 하에 액세스 제어 메커니즘으로 충분히 데이터를 보호할 수 있습니다. 상위 레벨의 보안이 필요한 경우, 데이터를 암호화할 수 있습니다.

민감한 데이터가 통신 네트워크를 통해, 특히, 인터넷과 같이 안전하지 않은 네트워크를 통해 전송될 때 이를 암호화하십시오. 네트워킹 환경에서 회선 도청 등의 데이터를 가로채려는 시도에 대해 액세스 제어 메커니즘은 효율적이지 않습니다.

데이터 무결성

데이터 무결성 서비스는 데이터가 권한 없이 수정되었는지를 감지합니다.

데이터 변경을 가져올 수 있는 두 가지 원인이 있습니다. 하드웨어 및 전송 오류이거나 의도적인 침입을 통해서입니다. 다수의 하드웨어 제품 및 전송 프로토콜에는 하드웨어 및 전송 오류를 감지하고 해결하는 메커니즘이 있습니다. 데이터 무결성 서비스의 목적은 의도적인 침입을 감지하는 것입니다.

데이터 무결성 서비스는 데이터가 수정되었는지 여부를 감지하는 것만을 목적으로 합니다. 데이터가 수정된 경우에 데이터를 원래 상태로 복원하는 것은 목적으로 하지 않습니다.

액세스 제어 메커니즘은 액세스가 거부되면 데이터를 수정할 수 없다는 점에 있어서 데이터 무결성에 기여할 수 있습니다. 그러나, 기밀성과 마찬가지로 네트워크 환경에서는 액세스 제어 메커니즘은 효율적이지 않습니다.

암호화 개념

이 주제 모음에서는 IBM MQ에 적용할 수 있는 암호화 개념에 대해 설명합니다.

용어 엔티티는 큐 관리자, IBM MQ MQI client, 개별 사용자 또는 메시지를 교환할 수 있는 기타 다른 시스템을 나타내기 위하여 사용됩니다.

관련 개념

[21 페이지의 『IBM MQ의 암호』](#)

IBM MQ에서는 TLS(Transport Security Layer) 프로토콜을 사용하여 암호화를 제공합니다.

암호화

암호화(cryptography)는 읽기 가능한 텍스트인 일반 텍스트와 읽을 수 없는 양식인 암호문 사이의 변환 프로세스입니다.

이는 다음과 같이 발생합니다.

1. 송신자가 일반 텍스트 메시지를 암호문으로 변환합니다. 이 프로세스 파트를 암호화(encryption)(때로 암호화(encipherment))라고 합니다.
2. 암호문은 수신자에게 전송됩니다.
3. 수신자는 암호문 메시지를 다시 일반 텍스트 양식으로 변환합니다. 이 프로세스 파트를 복호화(decryption)(때로 판독(decipherment))이라고 합니다.

변환은 전송하는 동안에 메시지의 모양을 변경하나 콘텐츠에 영향을 미치지 않는 일련의 산술적인 연산으로 진행됩니다. 암호화된 메시지는 이해할 수 없기 때문에 암호화 기술을 통해 기밀성이 유지되고 권한 없는 보기(도청)로부터 메시지를 보호합니다. 메시지 무결성을 보장하는 디지털 서명은 암호화 기술을 사용합니다. 자세한 정보는 [17 페이지의 『SSL/TLS의 디지털 서명』](#)의 내용을 참조하십시오.

암호화 기술은 키의 사용에 의해 특정하게 만들어진 일반적인 알고리즘과 관계가 있습니다. 알고리즘에는 두 가지로 분류됩니다.

- 두 당사자가 모두 같은 보안 키를 사용하도록 하는 알고리즘. 공유 키를 사용하는 알고리즘을 대칭 알고리즘이라고 합니다. [8 페이지의 그림 1](#)에서 대칭 키 암호화를 보여줍니다.
- 암호화에 임의의 키를 사용하고 복호화에 다른 키를 사용하는 알고리즘. 이들 중 하나는 비밀로 유지되어야 하지만 다른 하나는 공개될 수 있습니다. 공개 및 개인 키 쌍을 사용하는 알고리즘을 비대칭 알고리즘이라고 합니다. [8 페이지의 그림 2](#)에서는 공개 키 암호화라고도 하는 비대칭 키 암호화를 보여줍니다.

사용되는 암호화 및 복호화 알고리즘은 공개될 수 있지만 공유 보안 키와 개인 키는 비밀로 유지해야 합니다.

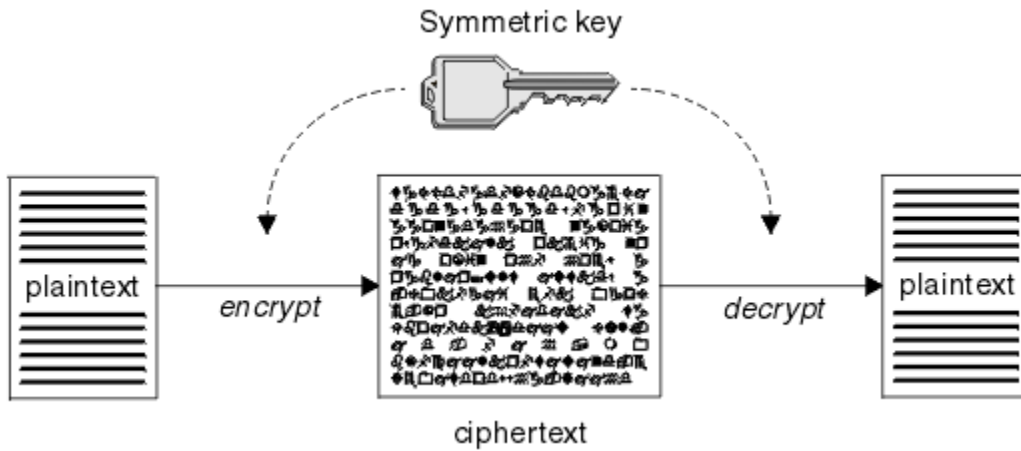


그림 1. 대칭 키 암호화

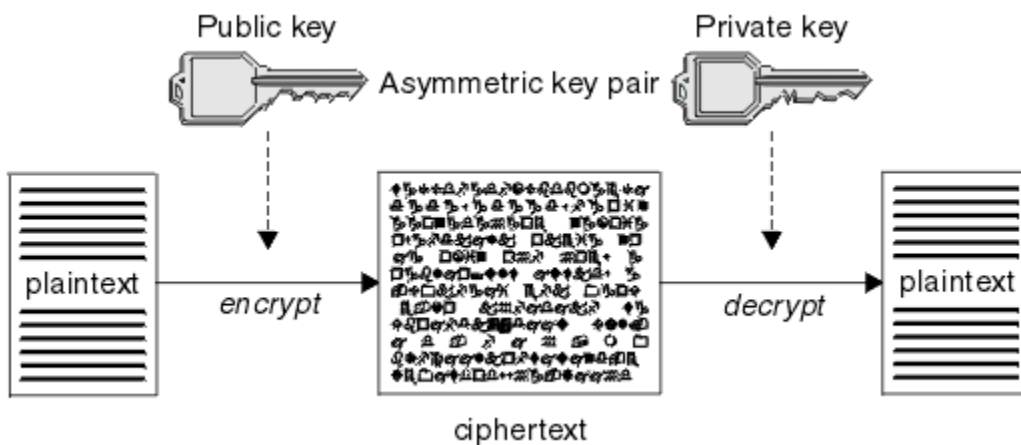


그림 2. 비대칭 키 암호화

8 페이지의 그림 2에서는 수신자의 공개 키로 암호화되고 수신자의 개인 키로 복호화되는 일반 텍스트를 보여줍니다. 의도한 수신자만 암호문 복호화를 위한 개인 키를 보유합니다. 메시지가 송신자로부터 나온다는 보장과 함께, 송신자가 개인 키로 메시지를 암호화할 수 있으며, 이렇게 하면 송신자의 공개 키를 가지고 있는 누구나 메시지를 복호화할 수 있다는 점에 주의하십시오.

비대칭 알고리즘에서 메시지는 공개 또는 개인 키로 암호화되지만 다른 키로만 복호화될 수 있습니다. 개인 키만 비밀이고, 공개 키는 누구나 알 수 있습니다. 대칭 알고리즘에서는 공유 키는 두 당사자에게만 알려져 있어야 합니다. 이를 키 분배 문제점이라고 합니다. 비대칭 알고리즘이 더 느리지만, 키 분배 문제점이 없다는 장점이 있습니다.

암호화에 연관되는 기타 용어는 다음과 같습니다.

강도

암호화 강도는 키 크기로 판별됩니다. 비대칭 알고리즘의 경우 큰 키가 필요합니다. 예를 들어,

- 1024비트 낮은 강도의 비대칭 키
- 2048비트 중간 강도의 비대칭 키
- 4096비트 높은 강도의 비대칭 키

대칭 키는 더 작습니다. 256비트 키가 강력한 암호화를 제공합니다.

블록 암호 알고리즘

이 알고리즘은 데이터를 블록으로 암호화합니다. 예를 들어, RSA Data Security Inc.의 RC2 알고리즘은 블록 8바이트 길이를 사용합니다. 블록 암호리즘은 일반적으로 스트림 암호리즘보다 느립니다.

스트림 암호 알고리즘

이 알고리즘은 각 데이터 바이트에서 조작됩니다. 스트림 암호리즘은 일반적으로 블록 암호리즘보다 빠릅니다.

메시지 요약 및 디지털 서명

메시지 요약은 메시지 콘텐츠에 대한 고정된 크기의 숫자 표시입니다. 메시지 요약은 해시 함수로 처리되어 디지털 서명을 양식화해서 암호화 가능합니다.

메시지 요약 처리에 사용되는 해시 함수는 다음 두 기준을 충족해야 합니다.

- 단방향이어야 합니다. 가능한 모든 메시지를 테스트하지 않고 특정 메시지 요약에 해당하는 메시지를 찾기 위해 함수를 되돌리는 것이 가능하면 안 됩니다.
- 같은 요약으로 해시되는 두 개의 메시지를 찾기 위한 처리는 불가능해야 합니다.

메시지 요약은 메시지 자체와 같이 송신됩니다. 수신자는 메시지에 대한 요약을 생성하고 이를 송신자의 요약과 비교할 수 있습니다. 메시지 무결성은 두 메시지 요약이 동일한 경우에 확인됩니다. 전송하는 동안에 메시지를 도용하면 거의 분명하게 다른 메시지 요약이 생깁니다.

비밀 대칭 키를 사용하여 작성되는 메시지 요약은 메시지 인증 코드(MAC)라고 하는데 이를 통해 메시지가 수정되지 않았음을 확인할 수 있기 때문입니다.

송신자도 메시지 요약을 생성하고 디지털 서명을 양식화하는 비대칭 키 쌍의 개인 키를 사용하여 요약을 암호화할 수 있습니다. 그런 다음 서명은 로컬에서 생성된 요약과 비교하기 전에 수신자에서 복호화되어야 합니다.

관련 개념

17 페이지의 『SSL/TLS의 디지털 서명』

디지털 서명은 메시지의 표현을 암호화하여 형성됩니다. 암호화는 서명인의 개인 키를 사용하고, 효율성을 위해 보통 메시지 자체가 아니라 메시지 요약에 대해 작동합니다.

디지털 인증서

디지털 인증서는 위장으로부터 보호하고 공개 키가 지정된 엔티티에 속하는지 확인합니다. 이는 인증 기관에서 발행됩니다.

디지털 인증서는 소유자가 개인, 큐 관리자 또는 다른 어떤 엔티티인지에 상관없이 공개 키를 해당 소유자로 바인딩하기 때문에 위장에 대한 보호를 제공합니다. 비대칭 키 설계를 사용할 때 공개 키의 소유권에 대해 보장해주기 때문에, 디지털 인증서를 공개 키 인증서라고도 합니다. 디지털 인증서에는 엔티티에 대한 공개 키가 있고 공개 키가 그 엔티티에 속한다는 언급이 있습니다.

- 인증서가 개별 엔티티에 대한 것인 경우, 인증서는 개인 인증서 또는 사용자 인증서라고 합니다.
- 인증서가 인증 기관에 대한 것인 경우, 인증서는 CA 인증서 또는 서명자 인증서라고 합니다.

해당 소유자가 공개 키를 다른 엔티티로 직접 송신하는 경우, 메시지가 인터셉트되고 공개 키는 다른 키로 대체될 위험이 있습니다. 이는 중간자 공격이라고 합니다. 이 문제에 대한 솔루션은 신뢰하는 써드파티를 통해 공개 키를 교환하는 것으로 이를 통해 공개 키가 실제 통신 중인 엔티티에 속하는 것임을 강력하게 보장할 수 있습니다. 공개 키를 직접 송신하는 대신, 신뢰하는 써드파티에게 이를 디지털 인증서로 통합하도록 요청합니다. 디지털 인증서를 발행하는 신뢰하는 써드파티는 [10 페이지의 『인증 기관』](#)에서 설명하는 것처럼 인증 기관(CA)이라고 합니다.

디지털 인증서의 내용

디지털 인증서에는 X.509 표준으로 판별되는 정보의 특정 부분이 포함됩니다.

IBM MQ에서 사용하는 디지털 인증서는 X.509 표준을 준수하며 이는 필요한 정보 및 송신 형식을 지정합니다. X.509는 표준의 X.500 시리즈의 인증 프레임워크 부분입니다.

디지털 인증서에는 적어도 인증되고 있는 엔티티에 대한 다음 정보가 있습니다.

- 소유자 공개 키
- 소유자 식별 이름
- 인증서를 발행한 CA의 식별 이름
- 인증서 유효 시작 날짜
- 인증서 만기 날짜

- X.509에 정의된 것과 같은 인증서 데이터 형식의 버전 번호. 현재 X.509 표준 버전은 버전 3이며 대부분의 인증서가 해당 버전을 준수합니다.
- 일련 번호. 이는 인증서를 발행한 CA에서 지정하는 고유 ID입니다. 일련 번호는 인증서를 발행한 CA 내에서 고유합니다. 동일한 CA 인증서로 서명된 두 개의 인증서가 동일한 일련 번호를 가질 수는 없습니다.

X.509 버전 2 인증서도 발행인 ID 및 해당 ID를 포함하며 X.509 버전 3 인증서는 몇 개의 확장자를 포함할 수 있습니다. 기본 제한조건 확장자와 같은 일부 인증서 확장자는 표준이지만 다른 확장자는 구현 특정적입니다. 확장자는 중요할 수 있으며 이 경우 시스템은 필드를 인식할 수 있어야 하고 필드를 인식하지 않으면 인증서를 거부해야 합니다. 확장자가 중요하지 않은 경우에는 시스템이 이를 인식하지 못하는 경우 무시할 수 있습니다.

개인 인증서의 디지털 서명은 해당 인증서를 서명한 CA의 개인 키를 사용하여 생성됩니다. 개인 인증서를 확인해야 하는 모든 사용자는 CA 공개 키를 사용하여 확인 가능합니다. CA 인증서는 해당 공개 키를 포함합니다.

디지털 인증서는 개인 키를 포함하지 않습니다. 개인 키는 안전하게 보관해야 합니다.

개인 인증서에 대한 요구사항

IBM MQ에서는 X.509 표준을 준수하는 디지털 인증서를 지원합니다. 이 경우 클라이언트 인증 옵션이 필요합니다.

IBM MQ가 피어 투 피어 시스템이기 때문에 SSL/TLS 용어에서 클라이언트 인증으로 표시됩니다. 따라서 클라이언트 인증의 키 사용을 허용하려면 SSL/TLS 인증에 사용되는 개인 인증서가 필요합니다. 모든 인증서에서 이 옵션이 사용되지 않는 경우 인증서 제공자는 보안 인증서에 대한 루트 CA에서 클라이언트 인증이 사용되도록 해야 합니다.

디지털 인증서의 데이터 형식을 지정하는 표준뿐만 아니라 인증서의 유효성을 판별하는 표준도 있습니다. 이러한 표준은 특정 유형의 보안 위반을 방지하기 위해 시간에 걸쳐 업데이트되었습니다. 예를 들어, 이전의 X.509 버전 1 및 2 인증서는 인증서가 다른 인증서 서명에 적법하게 사용될 수 있는지를 표시하지 않았습니다. 따라서, 악의적인 사용자가 합법적인 소스에서 개인 인증서를 확보하여 다른 사용자를 모방하도록 설계된 새 인증서를 생성할 수도 있었습니다.

X.509 버전 3 인증서를 사용하는 경우 BasicConstraints 및 KeyUsage 인증서 확장자가 다른 인증서를 적법하게 서명할 수 있는 인증서를 지정하는 데 사용됩니다. IETF RFC 5280 표준은 준수 애플리케이션 소프트웨어가 위장 공격을 방지하기 위해 구현해야 하는 일련의 인증서 유효성 검증 규칙을 지정합니다. 인증서 규칙 세트는 인증서 유효성 검증 정책이라고도 합니다.

IBM MQ에서의 인증서 유효성 검증 정책에 대한 자세한 정보는 39 페이지의 『IBM MQ의 인증서 유효성 검증 정책』의 내용을 참조하십시오.

인증 기관

인증 기관(CA)은 엔티티의 공개 키가 진짜로 해당 엔티티에 속하는지 확인할 수 있도록 디지털 인증서를 발행하는 신뢰 가능한 써드파티입니다.

CA의 역할은 다음과 같습니다.

- 디지털 인증서에 대한 요청을 수신하면, 개인 인증서를 빌드, 서명, 리턴하기 전에 요청자의 ID를 확인
- 해당 CA 인증서에서 CA의 자체 공개 키를 제공
- 인증서 폐기 목록(CRL)에서 더 이상 신뢰되지 않는 인증서 목록을 공개. 추가 정보는 301 페이지의 『폐기된 인증서에 대한 작업』의 내용을 참조하십시오.
- OCSP 응답자 서버를 운영하여 인증서 폐기 상태에 대한 액세스 제공

식별 이름

식별 이름(DN)은 X.509 인증서 내의 엔티티를 고유하게 식별합니다.



주의: 다음 표의 속성만 SSLPEER 필터에서 사용될 수 있습니다. 인증서 DN은 그 외의 속성을 포함할 수 있지만, 이러한 속성에 대해서는 필터링이 허용되지 않습니다.

표 1. SSLPEER 필터에서 사용할 수 있는 DN의 속성 유형	
속성 유형	설명
SERIALNUMBER	인증서 일련 번호
메일	이메일 주소

표 1. SSLPEER 필터에서 사용할 수 있는 DN의 속성 유형 (계속)	
속성 유형	설명
E	이메일 주소(MAIL보다 우선적으로는 더 이상 사용되지 않음)
UID 또는 USERID	사용자 ID
CN	공용 이름
T	제목
OU	조직 단위 이름
DC	도메인 컴포넌트
O	조직 이름
STREET	상세 주소/주소 두 번째 줄
L	지역 이름
ST(또는 SP 또는 S)	시 또는 도 이름
PC	우편번호
C	국가
UNSTRUCTUREDNAME	호스트 이름
UNSTRUCTUREDADDRESS	IP 주소
DNQ	식별 이름 규정자

X.509 표준은 보통 DN의 부분을 이루지 않는 다른 속성을 정의하나, 선택적인 확장을 디지털 인증서에게 제공할 수 있습니다.

X.509 표준은 DN이 문자열 형식으로 지정되도록 제공합니다. 예를 들면, 다음과 같습니다.

```
CN=John Smith, OU=Test, O=IBM, C=GB
```

공용 이름(CN)은 개인 사용자나, 예를 들어 웹 서버와 같은 다른 모든 엔티티를 설명할 수 있습니다.

DN에 여러 개의 OU 및 DC 속성이 포함될 수 있습니다. 기타 각 속성의 경우 하나의 인스턴스만 허용됩니다. OU 입력 항목의 순서는 중요합니다. 순서가 조직 단위(OU) 이름의 계층을 최상위 레벨 단위부터 먼저 지정합니다. DC 입력 항목의 순서도 중요합니다.

IBM MQ에서는 생성 결함이 있는 특정 DN가 허용됩니다. 자세한 정보는 [SSLPEER 값에 대한 IBM MQ 규칙을 참조](#)하십시오.

관련 개념

9 페이지의 『[디지털 인증서의 내용](#)』

디지털 인증서에는 X.509 표준으로 판별되는 정보의 특정 부분이 포함됩니다.

인증 기관에서 개인 인증서 확보

신뢰할 수 있는 외부 인증 기관(CA)에서 인증서를 확보할 수 있습니다.

디지털 인증서는 인증서 요청 양식으로 정보를 CA에 보내서 확보할 수 있습니다. X.509 표준이 이 정보에 대한 형식을 정의하지만 일부 CA는 자체적으로 고유 형식이 있습니다. 인증서 요청은 일반적으로 시스템에서 사용하는 인증서 관리 도구로 생성됩니다. 예:

- ▶ **Multi** 멀티플랫폼에서 iKeyman 도구
- ▶ **z/OS** z/OS의 RACF®.

정보에는 식별 이름 및 공개 키가 포함됩니다. 인증서 관리 도구가 인증서 요청을 생성하면 개인 키도 생성하며 이는 안전하게 보관해야 합니다. 개인 키는 분배하지 마십시오.

CA가 요청을 수신하면, 기관이 인증서를 빌드하고 이를 개인 인증서로 사용자에게 리턴하기 전에 ID를 확인합니다.

12 페이지의 그림 3는 CA로부터 디지털 인증서를 확보하는 프로세스를 보여줍니다.

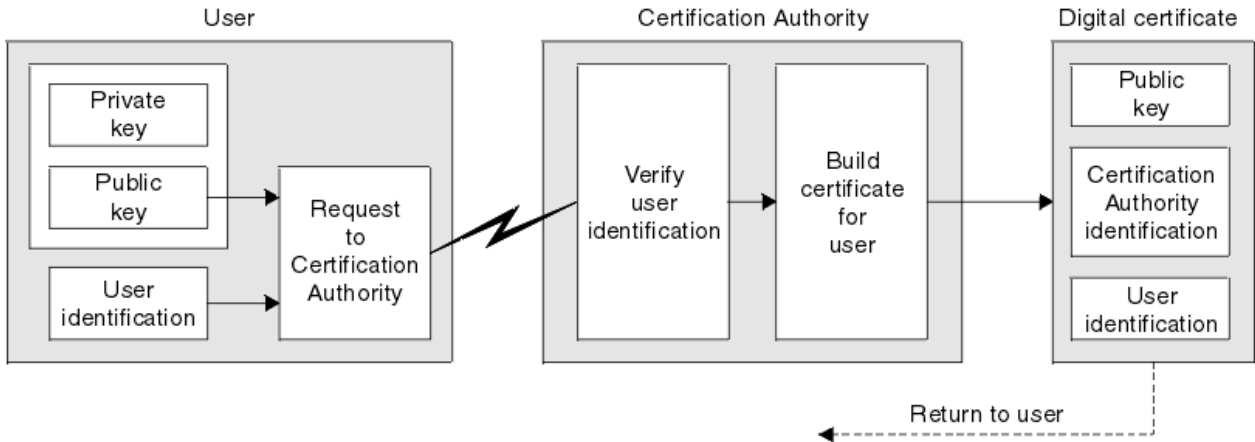


그림 3. 디지털 인증서 확보

다이어그램에서:

- 사용자 ID에는 제목 식별 이름이 포함됩니다.
- 인증 기관 ID에는 인증서를 발행하는 인증 기관의 식별 이름이 포함됩니다.

디지털 인증서에는 다이어그램에 표시되는 필드 이외에도 추가 필드가 있습니다. 디지털 인증서의 다른 필드에 대한 자세한 정보는 9 페이지의 『디지털 인증서의 내용』의 내용을 참조하십시오.

인증서 체인 작동 방법

다른 엔티티를 위해 인증서를 수신하면, 루트 CA 인증서를 얻기 위해 인증서 체인을 사용해야 할 수 있습니다.

인증 경로라고도 하는 인증서 체인은 엔티티를 인증하는 데 사용되는 인증서 목록입니다. 체인, 또는 경로는 그 엔티티의 인증서로 시작하고, 체인에 있는 각 인증서는 체인에 있는 다음 인증서에서 식별하는 엔티티에 의해 서명됩니다. 체인은 루트 CA 인증서로 종료됩니다. 루트 CA 인증서는 항상 인증 기관(CA) 자체로 서명됩니다. 체인의 모든 인증서 서명은 루트 CA 인증서에 도달할 때까지 확인해야 합니다.

13 페이지의 그림 4에서는 인증서 소유자로부터 신뢰 체인이 시작되는 루트 CA까지의 인증 경로를 보여줍니다.

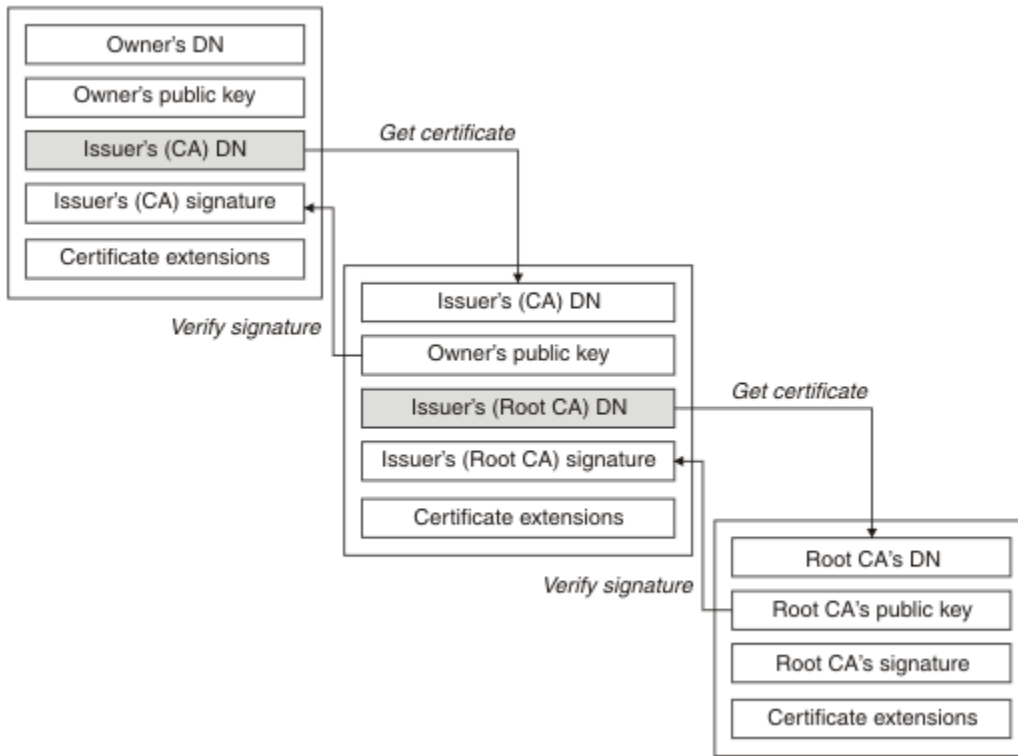


그림 4. 신뢰 체인

각 인증서는 하나 이상의 확장을 포함할 수 있습니다. CA에 속하는 인증서는 다른 인증서의 서명을 허용하도록 표시하기 위해 일반적으로 isCA 플래그가 설정되는 BasicConstraints 확장을 포함합니다.

인증서가 더 이상 유효하지 않은 경우
디지털 인증서는 만기되거나 폐기될 수 있습니다.

디지털 인증서는 고정된 기간에 대해 발행되고 그 만기 날짜 이후에는 유효하지 않습니다.

인증서는 다음을 비롯하여 다양한 이유로 폐기될 수 있습니다.

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

IBM MQ는 OCSP(Online Certificate Status Protocol) 응답자(UNIX, Linux®, and Windows전용)에 요청을 송신하여 인증서 폐기 여부를 검사할 수 있습니다. 또는, LDAP 서버의 인증서 폐기 목록(CRL)에 액세스할 수 있습니다. OCSP 폐기 및 CRL 정보는 인증 기관이 발행합니다. 자세한 정보는 301 페이지의 『폐기된 인증서에 대한 작업』의 내용을 참조하십시오.

공개 키 기반 구조(PKI)

PKI(Public Key Infrastructure)는 트랜잭션에 관련된 당사자들을 인증하기 위해 공개 키 암호화의 사용을 지원하는 기능, 정책, 서비스 시스템입니다.

PKI(Public Key Infrastructure)의 컴포넌트를 정의하는 단일 표준은 없지만 PKI는 일반적으로 인증 기관(CA) 및 등록대행 기관(RA)로 구성됩니다. CA는 다음 서비스를 제공합니다.

- 디지털 인증서 발행
- 디지털 인증서 유효성 검증
- 디지털 인증서 폐기
- 공개 키 분배

X.509 표준은 업계 표준의 PKI(Public Key Infrastructure)에 대한 기반을 제공합니다.

디지털 인증서 및 인증 기관(CA)에 대한 자세한 정보는 9 페이지의 『디지털 인증서』의 내용을 참조하십시오. RA는 디지털 인증서가 요청되면 제공된 정보를 확인합니다. RA가 해당 정보를 확인하면, CA가 디지털 인증서를 요청자에게 발행할 수 있습니다.

PKI는 디지털 인증서와 공개 키를 관리하기 위한 도구도 제공할 수 있습니다. PKI는 디지털 인증서를 관리하기 위한 신뢰 계층으로 설명되기도 하지만 대부분의 정의에는 추가 서비스가 있습니다. 일부 정의는 암호화 및 디지털 서명 서비스를 포함하지만 해당 서비스는 PKI 조작에 꼭 필요하지는 않습니다.

암호화 보안 프로토콜: TLS

암호화 프로토콜은 두 당사자가 개인정보 보호 및 데이터 무결성으로 통신하도록 하여 안전한 연결을 제공합니다. TLS(Transport Layer Security) 프로토콜은 SSL(Secure Socket Layer) 프로토콜에서 발전한 것입니다. IBM MQ는 TLS를 지원합니다.

두 프로토콜의 기본 목표는 기밀성(개인정보 보호라고도 함), 데이터 무결성, 인증, 디지털 인증서를 사용하는 인증을 제공하는 것입니다.

두 프로토콜이 유사하긴 하지만 SSL 3.0과 TLS의 다양한 버전이 상호 운용되지 않는다는 점은 상당한 차이점입니다.

관련 개념

21 페이지의 『IBM MQ의 TLS 보안 프로토콜』

IBM MQ는 메시지 채널 및 MQI 채널에 대한 링크 레벨 보안을 제공하기 위해 TLS(Transport Layer Security) 프로토콜을 지원합니다.

TLS(Transport Layer Security) 개념

TLS 프로토콜을 사용하면 두 당사자가 기밀성과 데이터 무결성이 보장된 상태로 서로 식별 및 인증하고 통신할 수 있습니다. TLS 프로토콜은 Netscape SSL 3.0 프로토콜에서 발전되었으나 TLS 및 SSL이 상호 운영되지는 않습니다.

TLS 프로토콜은 인터넷에서 통신 보안을 제공하며, 클라이언트/서버 애플리케이션이 비밀리에 안정적인 방식으로 통신할 수 있도록 허용합니다. 프로토콜에는 레코드 프로토콜과 데이터 교환 프로토콜의 두 개의 계층이 있으며 이들은 TCP/IP 등과 같은 전송 프로토콜 위에 계층을 이루고 있습니다. 이들은 비대칭 및 대칭 암호화 기술을 모두 사용합니다.

TLS 연결은 애플리케이션에 의해 시작되고 이는 TLS 클라이언트가 됩니다. 연결을 수신하는 애플리케이션은 TLS 서버가 됩니다. 모든 새 세션은 TLS 프로토콜에 의해 정의된 대로 데이터 교환으로 시작됩니다.

IBM MQ가 지원하는 모든 CipherSpec 목록은 376 페이지의 『CipherSpec 사용 가능』에 있습니다.

SSL 프로토콜에 대한 자세한 정보는 <https://www.mozilla.org/projects/security/pki/nss/ssl/draft302.txt>에서 제공되는 정보를 참조하십시오. TLS 프로토콜에 대한 자세한 정보는 IETF(Internet Engineering Task Force) 웹 사이트 (<https://www.ietf.org>)에서 TLS 작업 그룹이 제공하는 정보를 참조하십시오.

SSL/TLS 데이터 교환의 개요

SSL/TLS 데이터 교환을 사용하면 통신하는 TLS 클라이언트와 서버가 보안 키를 설정할 수 있습니다.

이 절에서는 TLS 클라이언트와 서버가 서로 통신할 수 있도록 하는 단계에 대한 요약を提供한다.

- 사용하는 프로토콜 버전 동의.
- 암호화 알고리즘 선택.
- 디지털 인증서를 교환 및 유효성 검증하여 서로 인증.
- 공유 보안 키 생성을 위한 키 분배 문제점을 막아주는 비대칭 암호화 기술 사용. 그러면 TLS는 메시지에 대해 비대칭 암호화보다 빠른 대칭 암호화의 공유 키를 사용합니다.

암호화 알고리즘 및 디지털 인증서에 대한 자세한 정보는 관련 정보를 참조하십시오.

대략적으로, TLS 데이터 교환에 연관된 단계는 다음과 같습니다.

1. TLS 클라이언트가 TLS 버전과 클라이언트가 지원하는 CipherSuite(클라이언트 환경 설정 순서대로) 등의 암호화 정보를 나열하는 "client hello" 메시지를 송신합니다. 메시지에는 나중의 처리에서 사용되는 무작위 바이트 문자열도 포함됩니다. 프로토콜은 "client hello"가 클라이언트에서 지원되는 데이터 압축 메소드도 포함하도록 허용합니다.

2. TLS 서버는 클라이언트가 제공하는 목록에서 서버가 선택한 CipherSuite, 세션 ID, 다른 무작위 바이트 문자열을 포함하는 "server hello" 메시지로 응답합니다. 서버는 해당 디지털 인증서도 송신합니다. 서버가 클라이언트 인증을 위해 디지털 인증서를 필요로 하면, 서버가 지원되는 인증서 유형 목록과 허용 가능한 인증 기관 (CA)의 식별 이름을 포함하는 "클라이언트 인증서 요청"을 송신합니다.
3. TLS 클라이언트는 서버의 디지털 인증서를 확인합니다. 추가 정보는 [15 페이지의 『TLS가 식별, 인증, 기밀성, 무결성을 제공하는 방법』](#)의 내용을 참조하십시오.
4. TLS 클라이언트는 클라이언트와 서버 모두가 후속 메시지 데이터 암호화에 사용되는 보안 키를 처리할 수 있도록 하는 무작위 바이트 문자열을 송신합니다. 무작위 바이트 문자열 자체는 서버의 공개 키로 암호화됩니다.
5. TLS 서버가 "클라이언트 인증서 요청"을 송신하면 클라이언트는 클라이언트의 개인 키와 클라이언트의 디지털 인증서 또는 "디지털 인증서 경보 없음"을 같이 암호화한 무작위 바이트 문자열을 송신합니다. 이 경보는 단지 경고일 뿐이지만 일부 구현에서 클라이언트 인증이 필수인 경우에 데이터 교환은 실패합니다.
6. TLS 서버는 클라이언트 인증서를 확인합니다. 추가 정보는 [15 페이지의 『TLS가 식별, 인증, 기밀성, 무결성을 제공하는 방법』](#)의 내용을 참조하십시오.
7. TLS 클라이언트는 데이터 교환의 클라이언트 측이 완료되었음을 표시하는 보안 키와 같이 암호화되는 "완료됨" 메시지를 서버에 송신합니다.
8. TLS 서버는 데이터 교환의 서버 측이 완료되었음을 표시하는 보안 키와 같이 암호화되는 "완료됨" 메시지를 클라이언트에 송신합니다.
9. 이제 TLS 세션 동안 서버와 클라이언트는 공유 보안 키로 대칭적으로 암호화되는 메시지를 교환할 수 있습니다.

15 페이지의 그림 5은 TLS 데이터 교환을 설명합니다.

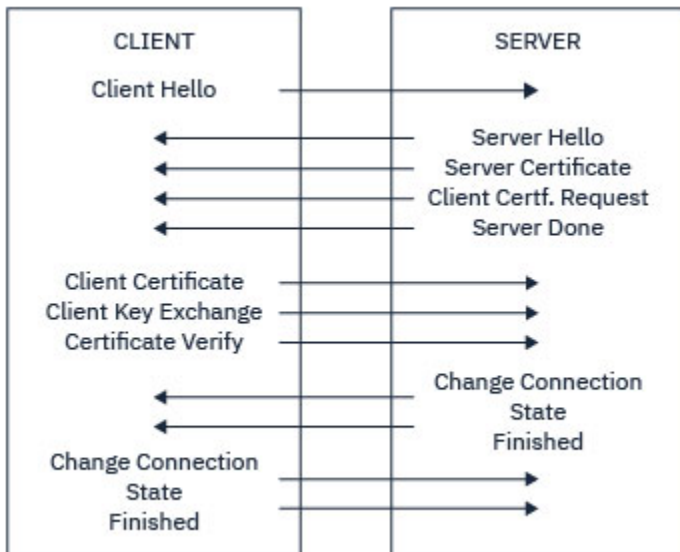


그림 5. TLS 데이터 교환의 개요

TLS가 식별, 인증, 기밀성, 무결성을 제공하는 방법

클라이언트와 서버 둘 다의 인증 동안에 비대칭 키 쌍 중 하나로 데이터가 암호화되고 해당 쌍의 다른 키로 비밀번호가 복호화되어야 하는 단계가 있습니다. 메시지 요약은 무결성을 제공하는 데 사용됩니다.

TLS 핸드셰이크에 관련된 단계에 대한 개요는 [14 페이지의 『SSL/TLS 데이터 교환의 개요』](#)의 내용을 참조하십시오.

TLS가 인증을 제공하는 방법

서버 인증에서는 클라이언트가 보안 키를 처리하는 데 사용되는 데이터를 암호화하기 위해 서버의 공개 키를 사용합니다. 서버가 정확한 개인 키로 데이터의 비밀번호를 복호화하는 경우에만 보안 키를 생성할 수 있습니다.

클라이언트 인증에서는 서버가 데이터 교환의 15 페이지의 『5』 단계 동안에 클라이언트가 송신하는 데이터의 비밀번호를 해독하기 위해 클라이언트 인증서에 있는 공개 키를 사용합니다. 보안 키로 암호화된 완료 메시지의 교환(개요에 있는 단계 15 페이지의 『7』 및 15 페이지의 『8』)으로 인증이 완료되었음을 확인합니다.

임의 인증 단계가 실패하면, 데이터 교환이 실패하고 세션이 종료됩니다.

TLS 데이터 교환 중의 디지털 인증서 교환은 인증 프로세스의 부분입니다. 인증서가 위장에 대해 보호를 제공하는 방법에 대한 자세한 정보는 관련 정보를 참조하십시오. 필수 인증서는 다음과 같습니다. 여기서 CA X는 TLS 클라이언트에게 인증서를 발행하고, CA Y는 TLS 서버에게 인증서를 발행합니다.

서버 인증의 경우에 한해 TLS 서버는 다음을 필요로 합니다.

- CA Y에 의해 서버에게 발행된 개인 인증서
- 서버 개인 키

또한 TLS 클라이언트는 다음을 필요로 합니다.

- CA Y에 대한 CA 인증서

TLS 서버에 클라이언트 인증이 필요한 경우, 서버는 클라이언트에 개인 인증서를 발행한 CA의 공개 키를 사용하여 클라이언트의 디지털 인증서를 확인하여 클라이언트의 신원을 검증합니다 (이 경우에는 CA X). 서버 및 클라이언트 인증을 위해 서버는 다음을 필요로 합니다.

- CA Y에 의해 서버에게 발행된 개인 인증서
- 서버 개인 키
- CA X에 대한 CA 인증서

또한 클라이언트는 다음을 필요로 합니다.

- CA X에 의해 클라이언트에 발행된 개인 인증서
- 클라이언트의 개인 키
- CA Y에 대한 CA 인증서

TLS 서버와 클라이언트 둘 다 루트 CA 인증서로 인증서 체인을 형성하기 위해 다른 CA 인증서를 필요로 할 수 있습니다. 인증서 체인에 대한 자세한 정보는 관련 정보를 참조하십시오.

인증서 확인 중 발생하는 사항

개요의 15 페이지의 『3』 및 15 페이지의 『6』 단계에 기술된 대로 TLS 클라이언트는 서버의 인증서를 확인하고 TLS 서버는 클라이언트의 인증서를 확인합니다. 이 확인에 대한 네 가지 관점이 있습니다.

1. 디지털 서명이 검사됩니다(17 페이지의 『SSL/TLS의 디지털 서명』 참조).
2. 인증서 체인이 검사됩니다. CA 인증서를 중개해야 합니다(12 페이지의 『인증서 체인 작동 방법』 참조).
3. 만기 및 활성화 날짜와 검증 기간을 검사합니다.
4. 인증서의 폐기 상태를 검사합니다(301 페이지의 『폐기된 인증서에 대한 작업』 참조).

보안 키 재설정

TLS 데이터 교환 중에 TLS 클라이언트와 서버 간의 데이터를 암호화하기 위해 보안 키가 생성됩니다. 보안 키는 일반 텍스트를 읽을 수 없는 암호문으로 변환하고 암호문을 일반 텍스트로 변환할 수 있도록 데이터에 적용되는 수학 공식에서 사용됩니다.

보안 키는 데이터 교환 중에 송신되는 무작위 텍스트에서 생성되면 일반 텍스트를 암호문으로 암호화하는 데 사용됩니다. 또한 보안 키는 메시지의 대체 여부를 판별하는 데 사용되는 메시지 인증 코드(MAC) 알고리즘에 사용됩니다. 자세한 정보는 9 페이지의 『메시지 요약 및 디지털 서명』의 내용을 참조하십시오.

보안 키가 발견된 경우 메시지의 일반 텍스트를 암호문에서 복호화하거나 메시지 요약을 계산하여 감지하지 않고 메시지를 대체할 수 있습니다. 복잡한 알고리즘의 경우에도 암호문에 가능한 모든 수학적 변환을 적용하여 일반 텍스트를 발견할 수 있습니다. 보안 키가 절단된 경우 복호화하거나 대체할 수 있는 데이터의 양을 최소화하기 위해 보안 키를 주기적으로 재협상할 수 있습니다. 보안 키가 재협상되면 이전에 사용하던 보안 키는 새 보안 키로 암호화된 데이터를 복호화하는 데 더 이상 사용할 수 없습니다.

TLS가 기밀성을 제공하는 방법

TLS는 메시지 개인정보 보호를 보장하기 위해 대칭과 비대칭 암호화의 결합을 사용합니다. TLS 데이터 교환 중에 TLS 클라이언트와 서버는 하나의 세션에만 사용될 암호화 알고리즘과 공유 보안 키에 동의합니다. TLS 클라이언트와 서버 사이에 전송되는 모든 메시지는 해당 알고리즘과 키를 사용하여 암호화되며, 메시지가 인터셉트 되어도 반드시 개인용으로 남아있게 됩니다. TLS가 공유 보안 키를 전송할 때는 비대칭 암호화를 사용하기 때문에, 키 분배 문제점이 없습니다. 암호화 기술에 대한 자세한 정보는 7 페이지의 『암호화』의 내용을 참조하십시오.

TLS가 무결성을 제공하는 방법

TLS는 메시지 축약을 계산하여 데이터 무결성을 제공합니다. 자세한 정보는 410 페이지의 『메시지의 데이터 무결성』의 내용을 참조하십시오.

채널 정의의 CipherSpec이 376 페이지의 『CipherSpec 사용 가능』의 표에 설명된 해시 알고리즘을 사용하는 경우 TLS를 사용하면 데이터 무결성을 확보할 수 있습니다.

특히 데이터 무결성이 중요한 경우 해시 알고리즘이 "없음"으로 표시된 CipherSpec을 선택하지 마십시오. MD5는 매우 오래되었으며 실제로도 사용 시 더 이상 안전하지 않기 때문에 사용하지 않도록 권장됩니다.

CipherSpecs 및 CipherSuites

암호화 보안 프로토콜은 안전 연결에서 사용되는 알고리즘에 동의해야 합니다. CipherSpec 및 CipherSuite는 특정 알고리즘 결합을 정의합니다.

CipherSpec은 암호화 알고리즘과 메시지 인증 코드(MAC) 알고리즘의 결합을 식별합니다. TLS 연결의 양 측이 서로 통신하려면 동일한 CipherSpec에 동의해야 합니다.

IBM MQ는 TLS 1.2 프로토콜을 지원합니다. 하지만 이를 수행해야 하는 경우 더 이상 사용되지 않는 CipherSpec을 사용으로 설정할 수 있습니다.

다음에 대한 정보는 376 페이지의 『CipherSpec 사용 가능』의 내용을 참조하십시오.

- IBM MQ에서 지원되는 CipherSpec
- 더 이상 사용되지 않는 SSL 3.0 및 TLS 1.0 CipherSpec을 사용으로 설정하는 방법

중요사항: IBM MQ 채널 처리 시 CipherSpec을 사용합니다. Java 채널, JMS 채널 또는 MQTT 채널 처리 시 CipherSuite를 지정합니다.

CipherSpec에 대한 자세한 정보는 376 페이지의 『CipherSpec 사용 가능』의 내용을 참조하십시오.

CipherSuite는 TLS 연결에 사용되는 암호화 알고리즘 스위트입니다. 스위트는 세 개의 개별 알고리즘으로 구성됩니다.

- 데이터 교환 시에 사용되는 키 교환 및 인증 알고리즘
- 데이터 암호화 시에 사용되는 암호화 알고리즘
- 메시지 요약 생성 시에 사용되는 MAC(메시지 인증 코드) 알고리즘

스위트의 각 컴포넌트에 대해서는 몇 개의 옵션이 있지만 TLS 연결에 대해 지정되는 경우 특정 결합만 유효합니다. 유효한 CipherSuite의 이름은 사용되는 알고리즘의 결합을 정의합니다. 예를 들어, CipherSuite TLS_RSA_WITH_AES_128_CBC_SHA는 다음을 지정합니다.

- RSA 키 교환과 인증 알고리즘
- 128비트 키 및 CBC(Cipher Block Chaining) 모드를 사용하는 AES 암호화 알고리즘
- SHA-1 메시지 인증 코드(MAC)

SSL/TLS의 디지털 서명

디지털 서명은 메시지의 표현을 암호화하여 형성됩니다. 암호화는 서명인의 개인 키를 사용하고, 효율성을 위해 보통 메시지 자체가 아니라 메시지 요약에 대해 작동합니다.

디지털 서명은 손으로 쓴 서명과 달리, 서명된 데이터에 따라 달라지며 이는 서명된 문서의 콘텐츠에 따라 다르지 않습니다. 두 개의 다른 메시지가 같은 엔티티에 의해 디지털로 서명되면 두 서명은 서로 다르지만 둘 다 같은 공개 키, 즉, 이 메시지에 서명한 엔티티의 공개 키를 사용하여 확인됩니다.

디지털 서명 프로세스의 단계는 다음과 같습니다.

1. 송신자가 메시지 요약(요약)을 처리한 후, 송신자의 개인 키를 사용하여 요약을 암호화하며, 이것이 디지털 서명을 구성합니다.
2. 송신자가 메시지와 같이 디지털 서명을 전송합니다.
3. 수신자가 송신자의 공개 키를 사용하여 디지털 서명을 복호화하며 이는 송신자의 메시지 요약(요약)을 다시 생성합니다.
4. 수신자가 수신된 메시지 데이터로부터 메시지 요약(요약)을 처리하고 두 개의 요약(요약)이 같은 것인지를 확인합니다.

18 페이지의 그림 6에서 이 프로세스를 설명합니다.

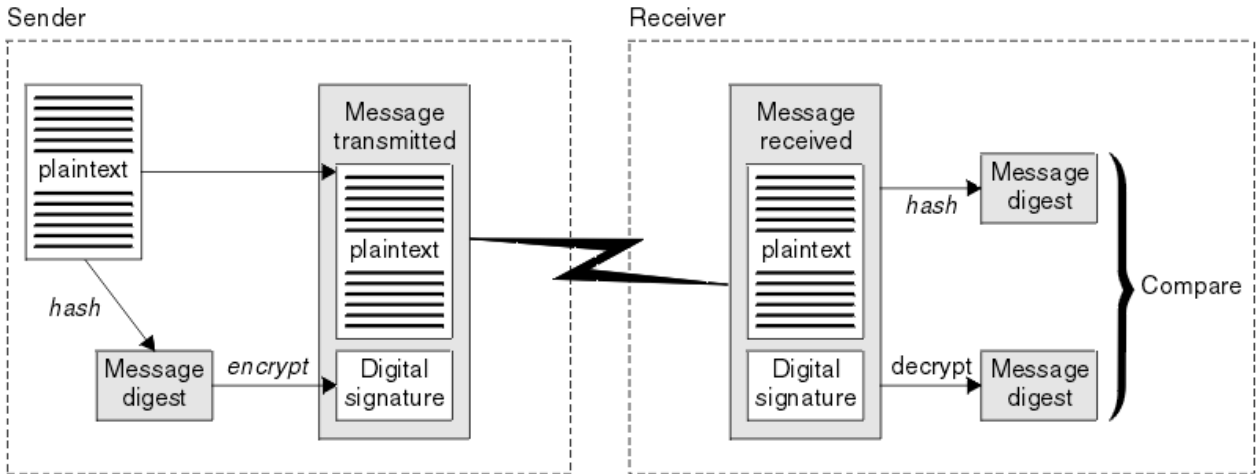


그림 6. 디지털 서명 프로세스

디지털 서명이 확인되면, 수신자가 다음을 알게 됩니다.

- 메시지가 전송 중에 수정되지 않았습니다.
- 메시지를 송신하도록 요청한 엔티티에 의해 메시지가 송신되었습니다.

디지털 서명은 무결성 및 인증 서비스의 일부입니다. 디지털 서명도 원본 증명을 제공합니다. 송신자만 개인 키를 알고 있으며 이는 송신자가 메시지의 진원지임을 증명하는 강력한 증거를 제공합니다.

참고: 메시지 자체를 암호화할 수도 있으며, 이는 메시지 안의 정보의 기밀성을 보호합니다.

FIPS(Federal Information Processing Standard)

미국 정부에서는 데이터 암호화 같은 IT 시스템과 보안에 대한 기술적 자문을 만들고 있습니다. NIST(National Institute for Standards and Technology)는 IT 시스템 및 보안과 관련된 중요한 조직입니다. NIST는 FIPS(Federal Information Processing Standard)를 포함하는 표준 및 권장사항을 생성합니다.

이들 중 중요한 표준은 FIPS 140-2이며 강력한 암호화 알고리즘을 사용해야 합니다. FIPS 140-2는 전송 중에 수정되지 못하도록 패킷을 보호하는 데 사용될 해싱 알고리즘에 대한 요구사항도 지정합니다.

IBM MQ는 이를 수행하도록 구성된 경우 FIPS 140-2 지원을 제공합니다.

시간이 경과함에 따라 분석가들이 기존 암호화 및 해싱 알고리즘에 대한 공격을 개발했습니다. 이러한 공격에 저항하기 위해 새 알고리즘이 채택되었습니다. FIPS 140-2는 이러한 변경사항을 감안하도록 주기적으로 업데이트됩니다.

관련 개념

18 페이지의 『NSA(National Security Agency) 스위트 B 암호화』

미 정부는 데이터 암호화를 포함한 IT 시스템 및 보안에 대한 기술 자문을 생성합니다. US NSA(National Security Agency)에서는 해당 스위트 B 표준에서 상호 운용 가능한 암호화 알고리즘 세트를 권장합니다.

NSA(National Security Agency) 스위트 B 암호화

미 정부는 데이터 암호화를 포함한 IT 시스템 및 보안에 대한 기술 자문을 생성합니다. US NSA(National Security Agency)에서는 해당 스위트 B 표준에서 상호 운용 가능한 암호화 알고리즘 세트를 권장합니다.

스위트 B 표준은 특정 안전 암호화 알고리즘 세트만 사용되도록 조작 모드를 지정합니다. 스위트 B 표준은 다음을 지정합니다.

- 암호화 알고리즘(AES)
- 키 교환 알고리즘(ECDH라고도 하는 Elliptic Curve Diffie-Hellman)
- 디지털 서명 알고리즘(ECDSA라고도 하는 Elliptic Curve Digital Signature Algorithm)
- 해시 알고리즘(SHA-256 또는 SHA-384)

또한, IETF RFC 6460 표준은 스위트 B 표준 준수를 위해 필요한 자세한 애플리케이션 구성 및 동작을 정의하는 스위트 B 준수 프로파일을 지정합니다. 이는 다음 두 프로파일을 정의합니다.

1. TLS 1.2에 사용할 스위트 B 준수 프로파일. 스위트 B 준수 조작을 위해 구성하는 경우 나열된 제한된 암호화 알고리즘 세트만 사용됩니다.
2. TLS 1.0 또는 TLS 1.1에 사용할 전이 프로파일. 이 프로파일을 사용하면 비스위트 B 준수 서버와의 상호 운용이 가능합니다. 스위트 B 전이 조작을 위해 구성하는 경우 추가 암호화 및 해싱 알고리즘이 사용될 수도 있습니다.

스위트 B 표준은 보증된 보안 레벨을 제공하기 위해서 사용 가능한 암호화 알고리즘 세트를 제한하기 때문에 개념상 FIPS 140-2와 비슷합니다.

Windows, UNIX and Linux 시스템에서 IBM MQ는 스위트 B 준수 TLS 1.2 프로파일을 준수하도록 구성할 수 있지만 스위트 B 전이 프로파일을 지원하지는 않습니다. 추가 정보에 대해서는 [36 페이지의 『IBM MQ에서의 NSA 스위트 B Cryptography』](#)의 내용을 참조하십시오.

관련 참조

[18 페이지의 『FIPS\(Federal Information Processing Standard\)』](#)

미국 정부에서는 데이터 암호화 같은 IT 시스템과 보안에 대한 기술적 자문을 만들고 있습니다. NIST(National Institute for Standards and Technology)는 IT 시스템 및 보안과 관련된 중요한 조직입니다. NIST는 FIPS(Federal Information Processing Standard)를 포함하는 표준 및 권장사항을 생성합니다.

IBM MQ 보안 메커니즘

이 주제 모음에서는 IBM MQ에서 다양한 보안 개념을 구현할 수 있는 방법에 대해 설명합니다.

IBM MQ에서는 [5 페이지의 『보안 개념 및 메커니즘』](#)에 도입된 모든 보안 개념을 구현하는 메커니즘을 제공합니다. 해당 내용은 다음 절에서 더 자세하게 설명됩니다.

IBM MQ에서의 식별 및 인증

IBM MQ에서 메시지 컨텍스트 정보 및 상호 인증을 사용하여 식별 및 인증을 구현할 수 있습니다.

다음은 IBM MQ 환경에서의 식별 및 인증에 대한 몇 개의 예제입니다.

- 모든 메시지는 메시지 컨텍스트 정보가 있을 수 있습니다. 이 정보는 메시지 디스크립터에 보유됩니다. 이는 애플리케이션이 메시지를 큐에 넣을 때 큐 관리자에서 생성 가능합니다. 또는, 애플리케이션에 연관된 사용자 ID가 권한이 부여되어 있으면, 애플리케이션이 정보를 제공할 수 있습니다.

메시지의 컨텍스트 정보를 사용하여 수신하는 애플리케이션이 메시지의 진원지에 대해 알 수 있습니다. 예를 들어, 메시지를 넣는 애플리케이션의 이름과 애플리케이션에 연관된 사용자 ID가 포함됩니다.

- 메시지 채널이 시작되면, 채널 각 측의 메시지 채널 에이전트(MCA)가 그 파트너를 인증하는 것이 가능합니다. 이 기술을 상호 인증이라고 합니다. MCA 전송의 경우, 메시지를 전송하는 파트너가 진짜 파트너이도록 보증합니다. 수신 MCA의 경우 이와 유사하게 진짜 파트너에서 메시지를 수신하도록 보증됩니다.

관련 개념

[5 페이지의 『식별 및 인증』](#)

식별은 시스템 사용자 또는 시스템에서 실행 중인 애플리케이션을 고유하게 식별하는 기능입니다. 인증은 사용자 또는 애플리케이션이 청구되는 진짜 사용자나 애플리케이션임을 증명해주는 기능입니다.

IBM MQ에서 권한 부여

특정 개인이나 애플리케이션이 IBM MQ 환경에서 수행할 수 있는 작업을 제한하기 위해 권한 부여할 수 있습니다.

다음은 IBM MQ 환경에서의 권한 부여 예제입니다.

- 인증된 관리자만 IBM MQ 자원 관리 명령 발행 허용.
- 애플리케이션에 연관된 사용자 ID가 수행할 권한이 있는 경우에만 애플리케이션이 큐 관리자에 연결되도록 허용.
- 애플리케이션이 자체 기능에 필요한 해당 큐만 열도록 허용.
- 애플리케이션이 자체 함수에 필요한 해당 토픽에만 구독하도록 허용.
- 애플리케이션이 자체 함수에 필요한 큐의 해당 조작만 수행하도록 허용. 예를 들어, 애플리케이션이 특정 큐에 있는 메시지를 찾아 보기만 하고, 메시지를 넣거나 가져올 수는 없을 수 있습니다.

권한 설정 방법에 대한 자세한 정보는 [74 페이지의 『권한 부여 계획』](#) 및 관련 하위 주제를 참조하십시오.

관련 개념

[6 페이지의 『권한 부여』](#)

권한 부여는 권한 있는 사용자 및 해당 애플리케이션으로만 액세스를 제한하여 시스템에서 중요한 자원을 보호합니다. 자원을 권한 없이 사용하는 것이나 권한이 부여되지 않은 방식으로 사용하는 것을 막습니다.

IBM MQ의 감사

IBM MQ는 일반적이지 않은 활동이 발생하는 레코드에 이벤트 메시지를 발행할 수 있습니다.

다음은 IBM MQ 환경에서의 감사 예제입니다.

- 애플리케이션이 열기 권한이 없는 큐 열기를 시도합니다. 도구 이벤트 메시지가 발행됩니다. 이벤트 메시지를 검사하여 이 시도가 발행하는지 검색하고 필요한 조치를 결정할 수 있습니다.
- 애플리케이션이 채널 열기를 시도하지만 SSL에서 연결을 허용하지 않기 때문에 실패합니다. 도구 이벤트 메시지가 발행됩니다. 이벤트 메시지를 검사하여 이 시도가 발행하는지 검색하고 필요한 조치를 결정할 수 있습니다.

관련 개념


[6 페이지의 『감사』](#)

감사는 예상치 못한 또는 권한이 없는 활동이 발생했는지 또는 이런 활동 수행 시도가 있었는지를 감지하기 위해 이벤트를 기록 및 검사하는 프로세스입니다.

IBM MQ의 기밀성

메시지를 암호화하여 IBM MQ에서 기밀성을 구현할 수 있습니다.

다음과 같이 IBM MQ 환경에서 기밀성이 보장됩니다.

- 송신 MCA가 전송 큐에서 메시지를 가져온 후 IBM MQ가 TLS를 사용하여 네트워크를 통해 수신 MCA로 송신하기 전에 메시지를 암호화합니다. 채널의 다른 쪽 끝에서는 수신 MCA가 그 목적지 큐에 메시지를 넣기 전에 메시지가 복호화됩니다.
- 메시지가 로컬 큐에 저장되면 IBM MQ에서 제공되는 액세스 제어 메커니즘은 권한 없는 노출에 대해 해당 콘텐츠를 보호하기에 충분한 것으로 간주될 수 있습니다. 그렇지만 최고 레벨을 보안을 위해 Advanced Message Security를 사용하여 큐에 저장된 메시지를 암호화할 수 있습니다.
-  로컬 큐에 저장된 메시지는 저장 중에 z/OS 데이터 세트 암호화를 사용하여 암호화할 수 있습니다.

[데이터 세트 암호화를 사용하는 IBM MQ for z/OS의 저장 데이터에 대한 기밀성](#) 섹션을 참조하십시오. 참조하십시오.

관련 개념

[6 페이지의 『기밀성』](#)

기밀성 서비스는 기밀 정보가 권한 없이 노출되는 것을 막습니다.

IBM MQ에서의 데이터 무결성

메시지 수정 여부를 감지하기 위해 데이터 무결성 서비스를 사용할 수 있습니다.

다음과 같이 IBM MQ 환경에서 데이터 무결성이 보장됩니다.

- TLS를 사용하여 메시지 콘텐츠가 네트워크를 통해 전송 중에 의도적으로 수정되었는지 감지할 수 있습니다. TLS에서 메시지 요약 알고리즘은 전송 중인 수정된 메시지 감지를 제공합니다.

모든 IBM MQ CipherSpec은 메시지 요약 알고리즘을 제공하며 메시지 데이터 무결성을 제공하지 않는 TLS_RSA_WITH_NULL_NULL은 예외입니다.

IBM MQ는 메시지를 수신할 때 수정된 메시지를 감지합니다. 수정된 메시지가 수신되면 IBM MQ는 AMQ9661 오류 메시지를 처리하고 채널이 중지됩니다.

- 메시지가 로컬 큐에 저장되는 동안, IBM MQ 에서 제공하는 액세스 제어 메커니즘은 메시지 콘텐츠의 의도적인 수정을 방지하기에 충분한 것으로 간주될 수 있습니다.

그러나 더 큰 보안 레벨의 경우 Advanced Message Security 를 사용하여 메시지를 큐에 넣은 시간과 큐에서 검색된 시간 사이에 메시지 콘텐츠가 의도적으로 수정되었는지 여부를 발견할 수 있습니다.

수정된 메시지를 발견하면 메시지 수신을 시도하는 응용프로그램이 2063리턴 코드를 수신하고 MQGET 호출을 사용하는 경우 메시지가 SYSTEM.PROTECTION.ERROR.QUEUE

관련 개념

7 페이지의 『데이터 무결성』

데이터 무결성 서비스는 데이터가 권한 없이 수정되었는지를 감지합니다.

IBM MQ의 암호

IBM MQ에서는 TLS(Transport Security Layer) 프로토콜을 사용하여 암호화를 제공합니다.

자세한 정보는 21 페이지의 『IBM MQ의 TLS 보안 프로토콜』의 내용을 참조하십시오.

관련 개념

7 페이지의 『암호화 개념』

이 주제 모음에서는 IBM MQ에 적용할 수 있는 암호화 개념에 대해 설명합니다.

IBM MQ의 TLS 보안 프로토콜

IBM MQ는 메시지 채널 및 MQI 채널에 대한 링크 레벨 보안을 제공하기 위해 TLS(Transport Layer Security) 프로토콜을 지원합니다.

메시지 채널 및 MQI 채널은 TLS 프로토콜을 사용하여 링크 레벨 보안을 제공합니다. 호출자 MCA는 TLS 클라이언트이며 응답자 MCA는 TLS 서버입니다. IBM MQ 은 TLS 1.0 및 TLS 1.2를 지원합니다. 채널 정의 중에 CipherSpec를 제공하여 TLS 프로토콜에서 사용되는 암호화 알고리즘을 지정할 수 있습니다.

참고: IBM MQ 8.0.0 Fix Pack 2에서는 SSLv3 및 일부 IBM MQ CipherSpec이 더 이상 사용되지 않습니다. 자세한 정보는 더 이상 사용되지 않음: SSLv3 프로토콜을 참조하십시오.

SECPROT 및 SSLCIPH 매개변수를 사용하여 채널에서 사용 중인 보안 프로토콜 및 CipherSpec을 표시할 수 있습니다.

메시지 채널의 양 끝과 MQI 채널의 서버 쪽에서, MCA는 연결되는 큐 관리자 대신 작동합니다. TLS 데이터 교환 중에 MCA는 큐 관리자의 디지털 인증서를 채널의 다른 끝에 있는 해당 파트너 MCA로 송신합니다. MQI 채널의 클라이언트 끝에 있는 IBM MQ 코드는 IBM MQ 클라이언트 애플리케이션의 사용자 대신 작동합니다. TLS 데이터 교환 중에 IBM MQ 코드는 사용자의 디지털 인증서를 MQI 채널의 서버 측에 있는 MCA로 송신합니다.

큐 관리자 및 IBM MQ 클라이언트 사용자는 SSLCAUTH(REQUIRED)가 채널의 서버 측에 지정된 경우를 제외하고는 TLS 클라이언트로 작동 중인 경우 연관된 개인용 디지털 인증서가 없어도 됩니다.

디지털 인증서는 키 저장소에 저장됩니다. 큐 관리자 속성 **SSLKeyRepository**는 큐 관리자 디지털 인증서를 보유하는 키 저장소 위치를 지정합니다. IBM MQ 클라이언트 시스템에서 MQSSLKEYR 환경 변수는 사용자의 디지털 인증서를 보유하는 키 저장소 위치를 지정합니다. 또는 IBM MQ 클라이언트 애플리케이션은 MQCONNX 호출에서 TLS 구성 옵션 구조 MQSCO의 **KeyRepository** 필드에 해당 위치를 지정할 수 있습니다. 키 저장소 및 해당 위치 지정 방법에 대한 자세한 정보는 관련 주제를 참조하십시오.

TLS에 대한 지원

IBM MQ는 사용 중인 플랫폼에 따라 TLS 1.0 및 TLS 1.2에 대한 지원을 제공합니다. TLS 프로토콜에 대한 자세한 정보는 하위 주제의 정보를 참조하십시오.

IBM i

TLS 지원은 IBM i 운영 체제에 통합되어 있습니다.

Java 및 JMS 클라이언트

이 클라이언트는 JVM을 사용하여 TLS 지원을 제공합니다.

UNIX, Linux, and Windows 시스템

TLS 지원은 IBM MQ와 같이 설치됩니다.

z/OS

TLS 지원은 z/OS 운영 체제에 통합되어 있습니다. z/OS의 TLS 지원은 시스템 SSL이라고 합니다.

IBM MQ TLS 지원에 대한 모든 필수조건 정보는 [IBM MQ의 시스템 요구사항](#)의 내용을 참조하십시오.

관련 개념

14 페이지의 『암호화 보안 프로토콜: TLS』

암호화 프로토콜은 두 당사자가 개인정보 보호 및 데이터 무결성으로 통신하도록 하여 안전한 연결을 제공합니다. TLS(Transport Layer Security) 프로토콜은 SSL(Secure Socket Layer) 프로토콜에서 발전한 것입니다. IBM MQ는 TLS를 지원합니다.

SSL/TLS 키 저장소

상호 인증된 TLS 연결에는 각 연결 측에 키 저장소가 필요합니다. 키 저장소는 디지털 인증서와 개인 키를 포함합니다.

이 정보는 일반 용어 키 저장소를 사용하여 디지털 인증서 및 해당 관련 개인 키에 대한 저장소를 설명합니다. 키 저장소는 TLS를 지원하는 다른 플랫폼 및 환경에서 다른 이름으로 참조됩니다.

- ▶ **IBM i** IBM i: 인증서 저장소
- Java 및 JMS: 키 저장소 및 신뢰 저장소
- ▶ **ULW** UNIX, Linux, and Windows: 키 데이터베이스 파일
- ▶ **z/OS** z/OS: 키 링

자세한 정보는 9 페이지의 『디지털 인증서』 및 14 페이지의 『TLS(Transport Layer Security) 개념』의 내용을 참조하십시오.

상호 인증된 TLS 연결에는 각 연결 측에 키 저장소가 필요합니다. 키 저장소는 다음 인증서와 요청을 포함할 수 있습니다.

- 큐 관리자 또는 클라이언트가 연결의 원격 끝에 있는 해당 파트너에서 수신한 인증서의 확인을 허용하는 다양한 인증 기관에서 발행된 몇 개의 CA 인증서. 개별 인증서가 인증서 체인에 있을 수 있습니다.
- 인증 기관에서 수신된 하나 이상의 개인 인증서. 별도의 개인 인증서를 각 큐 관리자 또는 IBM MQ MQI client에 연관시킵니다. 개인 인증서는 상호 인증이 필요한 경우 TLS 클라이언트에서 필수입니다. 상호 인증이 필요하지 않은 경우, 개인 인증서가 클라이언트에 필요하지 않습니다. 키 저장소는 각 개인 인증서에 해당하는 개인 키를 포함할 수도 있습니다.
- 신뢰 가능한 CA 인증서의 서명을 대기 중인 인증서 요청.

키 저장소 보호에 대한 자세한 정보는 23 페이지의 『IBM MQ 키 저장소 보호』의 내용을 참조하십시오.

키 저장소의 위치는 사용하고 있는 플랫폼에 따라 다릅니다.

▶ **IBM i** IBM i

키 저장소는 인증서 저장소입니다. 기본 시스템 인증서 저장소는 통합 파일 시스템(IFS)의 /QIBM/UserData/ICSS/Cert/Server/Default에 있습니다. IBM MQ는 인증서 저장소의 비밀번호는 비밀번호 스택 파일에 저장합니다. 예를 들어, 큐 관리자 QM1에 대한 스택 파일은 /QIBM/UserData/mqm/qmgrs/QM1/ssl/Stash.sth입니다.

또는, IBM i 시스템 인증서 저장소가 대신 사용되도록 지정할 수도 있습니다. 이를 수행하려면 큐 관리자 **SSLKEYR** 속성 값을 *SYSTEM으로 변경하십시오. 이 값은 큐 관리자가 시스템 인증서 저장소를 사용하고 큐 관리자가 디지털 인증 관리자(DCM)를 애플리케이션으로 사용하도록 등록되는 것을 나타냅니다.

인증서 저장소는 큐 관리자에 대한 개인 키도 포함합니다.

ULW UNIX, Linux, and Windows 시스템

키 저장소는 키 데이터베이스 파일입니다. 키 데이터베이스 파일 이름의 파일 확장자는 .kdb여야 합니다. 예를 들어, UNIX and Linux에서 큐 관리자 QM1의 기본 키 데이터베이스 파일은 /var/mqm/qmgrs/QM1/ssl/key.kdb입니다. IBM MQ가 기본 위치에 설치된 경우 Windows에서 해당 경로는 C:\ProgramData\IBM\MQ\Qmgrs\QM1\ssl\key.kdb입니다.

각 키 데이터베이스 파일에는 관련된 비밀번호 스테쉬 파일이 있습니다. 이 파일은 프로그램이 키 데이터베이스에 액세스하도록 허용하는 인코딩된 비밀번호를 보유합니다. 비밀번호 스테쉬 파일은 키 데이터베이스와 동일한 디렉토리에 있어야 하고 동일한 파일 시스템이 있어야 하며, .sth 접미어로 종료해야 합니다.

예: /var/mqm/qmgrs/QM1/ssl/key.sth

참고: PKCS #11 암호화 하드웨어 카드는 인증서 및 키를 포함해야 하며 그렇지 않으면 키 데이터베이스 파일에 보유됩니다. 인증서와 키가 PKCS #11 카드에 보유되는 경우, IBM MQ는 여전히 키 데이터베이스 파일 및 비밀번호 스테쉬 파일 모두에 액세스해야 합니다.

UNIX 및 Windows 시스템에서 키 데이터베이스는 큐 관리자 또는 IBM MQ MQI client에 연관된 개인 인증서에 대한 개인 키도 포함합니다.

z/OS z/OS

인증서는 z/OS의 키링에 보유됩니다.

기타 외부 보안 관리자(ESM)도 인증서 저장에 키링을 사용합니다.

개인 키는 RACF로 관리됩니다.

IBM MQ 키 저장소 보호

IBM MQ에 대한 키 저장소는 파일입니다. 의도된 사용자만 키 저장소 파일에 액세스할 수 있어야 합니다. 이렇게 하면 침입자나 다른 권한이 없는 사용자가 키 저장소 파일을 다른 시스템에 복사한 후, 그 시스템에서 동일한 사용자 ID를 설정하여 의도된 사용자로 위장하지 못하게 합니다.

파일의 권한은 사용자의 umask 및 사용하는 도구에 따라 다릅니다. Windows에서 IBM MQ 계정에는 BypassTraverseChecking 권한이 필요하며 이는 파일 경로의 폴더 권한이 아무런 영향을 주지 않음을 나타냅니다.

키 저장소 파일의 파일 권한을 확인하고 파일 및 해당 폴더에 대해 모두가 읽을 수 없도록 해야 하며 가능하면 그룹에서도 읽을 수 없어야 합니다.

사용 중인 시스템에서 키 저장소는 읽기 전용으로 하는 것이 바람직하며 관리자만 유지보수를 수행하기 위해 쓰기 조작을 사용하도록 권한 부여되는 것이 좋습니다.

실제로 모든 위치에서 비밀번호로 보호되는지 여부에 상관없이 모든 키 저장소(keystore)를 보호해야 하며 키 저장소(key repository)도 보호해야 합니다.

디지털 인증서 레이블, 요구사항 이해

디지털 인증서를 사용하기 위해 TLS를 설정할 때 사용된 플랫폼과 연결에 사용한 방법에 따라 반드시 따라야 하는 특정 레이블 요구사항이 있을 수 있습니다.

인증서 레이블의 개념

인증서 레이블은 키 저장소에 저장된 디지털 인증서를 나타내는 고유 ID이고, 키 관리 기능을 수행할 때 특정 인증서를 가리키는 데 사용되는 편리한 사람이 읽을 수 있는 이름을 제공합니다. 인증서를 키 저장소에 처음으로 추가할 때 인증서 레이블을 지정합니다.

인증서 레이블은 인증서의 **Subject Distinguished Name** 또는 **Subject Common Name** 필드와는 별개입니다. **Subject Distinguished Name** 및 **Subject Common Name**이 인증서 자체 내의 필드임을 유의하십시오. 이들은 인증서가 작성될 때 정의되고 변경될 수 없습니다. 그러나 필요한 경우 디지털 인증서와 연관된 레이블을 변경할 수 있습니다.

인증서 레이블 구문

인증서 레이블은 다음 조건과 함께 문자, 숫자 및 구두점을 포함할 수 있습니다.

- ▶ **Multi** 인증서 레이블은 최대 64자까지 포함할 수 있습니다.
- ▶ **z/OS** 인증서 레이블은 최대 32자까지 포함할 수 있습니다.
- 인증 레이블에는 공백이 포함될 수 있습니다.
- 레이블은 대소문자를 구분합니다.
- EBCDIC 가타카나를 사용하는 시스템에서는 소문자를 사용할 수 없습니다.

인증서 레이블 값의 추가 요구사항은 다음 섹션에 지정됩니다.

인증서 레이블 사용 방법

IBM MQ는 TLS 데이터 교환 동안에 전송되는 개인 인증서를 찾기 위해 인증서 레이블을 사용합니다. 이는 키 저장소에 있는 둘 이상의 개인 인증서가 있을 때 모호성을 없애줍니다.

인증서 레이블을 선택한 값으로 설정할 수 있습니다. 값을 설정하지 않으면 사용 중인 플랫폼에 따라 이름 지정 규칙을 따르는 기본 레이블이 사용됩니다. 자세한 내용은 특정 플랫폼에 대해 다음에 나오는 절을 참조하십시오.

참고사항:

- Java 또는 JMS 시스템에서 인증서 레이블을 직접 설정할 수 없습니다.
- 채널 자동 정의(CHAD) 엑시트에 의해 작성된 자동 정의된 채널은 인증서 레이블을 설정할 수 없습니다. TLS 데이터 교환은 채널이 작성되는 시간에 발생하기 때문입니다. 인바운드 채널의 경우 CHAD 엑시트에 인증서 레이블을 설정하는 것은 아무런 효과가 없습니다.

이 컨텍스트에서 TLS 클라이언트는 데이터 교환을 시작하는 연결 파트너를 가리키며 이는 IBM MQ 클라이언트 또는 또 다른 큐 관리자일 수 있습니다.

TLS 데이터 교환 중에 TLS 클라이언트는 항상 서버로부터 디지털 인증서를 확보 및 유효성을 검증합니다. IBM MQ 구현을 사용하여 TLS 서버는 항상 클라이언트로부터 인증서를 요청하고 클라이언트는 항상 서버에 인증서를 제공합니다(찾은 경우). 클라이언트가 개인 인증서를 찾을 수 없으면, 클라이언트는 서버에 no certificate 응답을 보냅니다.

TLS 서버는 항상 클라이언트 인증서가 송신되면 클라이언트 인증서의 유효성을 검증합니다. 클라이언트가 인증서를 송신하지 않은 경우에는 TLS 서버의 역할을 하고 있는 채널의 끝이 **REQUIRED**로 설정된 **SSLCAUTH** 매개변수 또는 **SSLPEER** 매개변수 값 세트에 정의된 경우 인증에 실패합니다.

인바운드 채널(수신자, 요청자, 클러스터 수신자, 자격이 없는 서버, 서버 연결 채널)은 리모트 피어의 IBM MQ 버전에서 인증서 레이블 구성을 완전하게 지원하고 채널에서 TLS CipherSpec을 사용 중인 경우에만 구성된 인증서를 송신합니다.

규정되지 않은 서버 채널은 CONNAME 필드가 설정되지 않은 채널입니다.

다른 모든 경우, 큐 관리자 **CERTLABL** 매개변수는 전송된 인증서를 판별합니다. 특히 다음은 채널 특정 레이블 설정에 관계없이 큐 관리자의 **CERTLABL** 매개변수에 의해 구성된 인증서만 수신합니다.

- IBM MQ 9.1.1 이전에는 모든 현재 Java 및 JMS 클라이언트가 있습니다.
- ▶ **V 9.1.1** From IBM MQ 9.1.1, Java and JMS clients supporting Server Name Indication (SNI), that is, certificates on a channel by channel basis.
- IBM MQ prior to IBM MQ 8.0의 버전.
- 관리 .NET 클라이언트

또한 채널이 사용하는 인증서는 채널 CipherSpec에 적합해야 합니다. 자세한 정보는 [40 페이지의 『IBM MQ에서 디지털 인증서와 CipherSpec의 호환성』](#)의 내용을 참조하십시오.

IBM MQ 8.0 이상에서는 채널 정의에서 **CERTLABL** 속성으로 지정된 채널별 인증서 레이블을 사용하여 동일한 큐 관리자에서 다중 인증서의 사용을 지원합니다. 큐 관리자의 인바운드 채널(예: 서버 연결 또는 수신자)은 큐 관리자로부터 올바른 인증서를 제공하기 위해 TLS 서버 이름 표시(SNI)를 사용하여 채널 이름 감지에 의존합니다.

채널이 IBM MQ Internet Pass-Thru (MQIPT) 를 통해 대상 큐 관리자에 연결되고 MQIPT 라우트에 **SSLServer** 및 **SSLClient** 세트가 둘 다 있는 경우, 엔드포인트 사이에 두 개의 개별 TLS 세션이 있으며 SNI 데이터는 세션 구분을 통해 흐르지 않습니다. 이렇게 하면 목적지 큐 관리자에서 MQIPT와 큐 관리자 간의 TLS 연결에 대해 채널별 인증서가 사용되지 않습니다. 목적지 큐 관리자에서 채널당 인증을 사용하려면, MQIPT를 통과하는 TLS 연결의 경우, MQIPT 라우트는 SNI 이름을 포함하여 모든 TLS 제어 플로우를 그대로 전달하는 TLS 프록시 모드를 사용해야 합니다. MQIPT의 TLS 지원에 대한 자세한 정보는 [SSL/TLS 지원을 참조하십시오](#).

MQIPT(으)로 종결되거나 시작된 TLS 연결에 사용되는 인증서는 각 라우트에 대해 개별적으로(예를 들어, **SSLServerSiteLabel** 및 **SSLClientSiteLabel** 라우트 특성을 사용하여) 구성될 수 있습니다.

단방향 인증을 사용하여 큐 관리자에 연결하는 방법 즉, TLS 클라이언트가 인증서를 송신하지 않을 경우에 대한 자세한 정보는 [단방향 인증을 사용하여 두 큐 관리자 연결을 참조하십시오](#).

멀티플랫폼 시스템



멀티플랫폼에서 TLS 서버는 인증서를 클라이언트에 보냅니다.

큐 관리자와 클라이언트는 각각 다음 소스에서 비어 있지 않은 값을 순서대로 검색합니다. 첫 번째 비어 있지 않은 값은 인증서 레이블을 판별합니다. 인증서 레이블은 키 저장소에 존재해야 합니다. 레이블의 대소문자와 형식이 정확히 일치하는 인증서가 발견되지 않으면 오류가 발생하고 TLS 데이터 교환이 실패합니다.

큐 관리자

1. 채널 인증서 레이블 속성 **CERTLABL**.
2. 큐 관리자 인증서 레이블 속성 **CERTLABL**.
3. 기본적으로 이는 큐 관리자의 이름이 추가된 **ibmwebspheremq** 형식(모두 소문자)입니다. 예를 들어, **QM1** 이름이 지정된 큐 관리자의 경우 기본 인증서 레이블은 **ibmwebspheremqmq1**입니다.

IBM MQ 클라이언트

1. CLNTCONN 채널 정의에 있는 인증서 레이블 속성 **CERTLABL**.
2. MQSCO 구조 **CertificateLabel** 속성.
3. 환경 변수 **MQCERTLABL**.
4. 클라이언트 **.ini** 파일(해당 SSL 절에서) **CertificateLabel** 속성
5. 클라이언트 애플리케이션이 실행 중인 사용자 ID가 추가된 **ibmwebspheremq** 형식의 기본값(모두 소문자)입니다. 예를 들어, **USER1**의 사용자 ID의 경우 기본 인증서 레이블은 **ibmwebspheremquser1**입니다.

z/OS 시스템



IBM MQ 클라이언트는 z/OS에서 지원되지 않습니다. 그러나 z/OS 큐 관리자는 연결을 시작할 때 TLS 클라이언트 또는 연결 요청을 승인할 때 TLS 서버의 역할을 할 수 있습니다. z/OS 큐 관리자의 인증서 레이블 요구사항은 이러한 역할 둘 모두에 적용되고 멀티플랫폼의 요구사항과는 다릅니다.

큐 관리자와 클라이언트는 각각 다음 소스에서 비어 있지 않은 값을 순서대로 검색합니다. 첫 번째 비어 있지 않은 값은 인증서 레이블을 판별합니다. 인증서 레이블은 키 저장소에 존재해야 합니다. 레이블의 대소문자와 형식이 정확히 일치하는 인증서가 발견되지 않으면 오류가 발생하고 TLS 데이터 교환이 실패합니다.

1. 채널 인증서 레이블 속성, **CERTLABL**.
2. 공유된 경우, 큐 공유 그룹 인증서 레이블 속성, **CERTQSGL**.
공유되지 않은 경우, 큐 관리자 인증서 레이블 속성, **CERTLABL**.
3. 큐 관리자 또는 큐 공유 그룹의 이름이 추가된 **ibmWebSphereMQ** 형식의 기본값입니다. 이 문자열이 대소문자를 구분하고 표시된 대로 기록되어야 함을 유의하십시오. 예를 들어, **QM1** 이름이 지정된 큐 관리자의 경우 기본 인증서 레이블은 **ibmWebSphereMQQM1**입니다.

4. 옵션 25 페이지의 『3』에 있는 형식의 인증서가 없는 경우 IBM MQ는 키 링에서 기본값으로 표시된 인증서를 사용하려고 시도합니다.

키 저장소를 표시하는 방법에 대한 정보는 286 페이지의 『z/OS에서 키 저장소에서 큐 관리자 찾기』의 내용을 참조하십시오.

IBM MQ Java 및 IBM MQ JMS 클라이언트

IBM MQ Java 및 IBM MQ JMS 클라이언트는 TLS 데이터 교환 동안에 개인 인증서를 선택하기 위해 JSSE(Java Secure Socket Extension) 제공자의 기능을 사용하므로 인증서 레이블 요구사항을 따르지 않습니다.

기본 작동은 JSSE 클라이언트가 키 저장소의 인증서를 통해 반복하여 첫 번째 발견된 승인 가능한 개인 인증서를 선택하는 것입니다. 그러나 이 작동은 단지 기본값이며 JSSE 제공자의 구현에 의존합니다.

또한 JSSE 인터페이스는 애플리케이션에 의한 런타임 시에 구성과 직접 액세스를 통해 고도로 사용자 정의 가능합니다. 특정 세부사항은 JSSE 제공자가 제공한 문서를 참조하십시오.

문제점 해결을 위해서 또는 특정 JSSE 제공자와 결합하여 IBM MQ Java 클라이언트 애플리케이션이 수행하는 데이터 교환을 보다 잘 이해하기 위해서 JVM 환경에서 `javax.net.debug=ssl`을 설정하여 디버깅을 사용 가능하게 할 수 있습니다.

구성을 통해서 또는 명령행에 `-Djavax.net.debug=ssl`을 입력하여 애플리케이션 내에 변수를 설정할 수 있습니다.

큐 관리자의 키 저장소 새로 고치기

키 저장소 콘텐츠를 변경하는 경우 큐 관리자는 즉시 새 콘텐츠를 선택하지 않습니다. 큐 관리자가 새 키 저장소 콘텐츠를 사용하도록 하려면 `REFRESH SECURITY TYPE(SSL)` 명령을 발행해야 합니다.

이 프로세스는 의도적이며 여러 개의 실행 채널이 다른 버전의 키 저장소를 사용하는 상황을 방지합니다. 보안 제어로 언제든지 큐 관리자는 한 개 버전의 키 저장소만 로드할 수 있습니다.

`REFRESH SECURITY TYPE(SSL)` 명령에 대한 자세한 정보는 `REFRESH SECURITY`를 참조하십시오.

PCF 명령 또는 IBM MQ Explorer를 사용하여 키 저장소를 새로 고칠 수 있습니다. 자세한 정보는 이 제품 문서의 IBM MQ Explorer 섹션에서 `MQCMD_REFRESH_SECURITY` 명령 및 TLS 보안 새로 고치기 주제를 참조하십시오.

관련 개념

26 페이지의 『SSL/TLS 키 저장소 콘텐츠 및 SSL/TLS 설정의 클라이언트 보기 새로 고침』

키 저장소에 대해 새로 고친 콘텐츠가 포함된 클라이언트 애플리케이션을 업데이트하려면 클라이언트 애플리케이션을 중지한 후에 다시 시작해야 합니다.

SSL/TLS 키 저장소 콘텐츠 및 SSL/TLS 설정의 클라이언트 보기 새로 고침

키 저장소에 대해 새로 고친 콘텐츠가 포함된 클라이언트 애플리케이션을 업데이트하려면 클라이언트 애플리케이션을 중지한 후에 다시 시작해야 합니다.

IBM MQ 클라이언트에서 보안을 새로 고칠 수 없습니다. 클라이언트에 대해 `REFRESH SECURITY TYPE(SSL)` 명령에 해당하는 명령이 없습니다(자세한 정보는 `REFRESH SECURITY` 참조).

키 저장소의 새로 고쳐진 콘텐츠로 클라이언트 애플리케이션을 업데이트하려면 보안 인증서를 변경할 때마다 애플리케이션을 중지한 후 재시작해야 합니다.

채널을 재시작하면 구성이 새로 고쳐지며 애플리케이션에 다시 연결 논리가 있는 경우 `STOP CHL STATUS(INACTIVE)` 명령을 발행하여 클라이언트에서 보안을 새로 고칠 수 있습니다.

관련 개념

26 페이지의 『큐 관리자의 키 저장소 새로 고치기』

키 저장소 콘텐츠를 변경하는 경우 큐 관리자는 즉시 새 콘텐츠를 선택하지 않습니다. 큐 관리자가 새 키 저장소 콘텐츠를 사용하도록 하려면 `REFRESH SECURITY TYPE(SSL)` 명령을 발행해야 합니다.

MQCSP 비밀번호 보호

IBM MQ 8.0에서 IBM MQ 기능을 사용하여 보호되거나 TLS 암호화를 사용하여 암호화된 MQCSP 구조에 포함된 비밀번호를 전송할 수 있습니다.

중요사항: MQCSP 비밀번호 보호 사용은 TLS 암호화 설정에 비해 단순하기 때문에 MQCSP 비밀번호 보호는 테스트 및 개발 용도로 유용하지만 TLS 암호화에 비해 안전하지 않습니다. 프로덕션 용도의 경우 IBM MQ 비밀번호 보호보다 우선하여 TLS 암호화를 사용해야 합니다. 특히, 클라이언트와 큐 관리자 간 네트워크가 신뢰되지 않는 경우 TLS 암호화가 더 안전하기 때문입니다.

정확히 어떤 암호화가 사용 중인지와 얼마나 많은 보호를 제공하는지 관심이 있으면 전체 TLS 암호화를 사용해야 합니다. 이 상황에서 알고리즘은 공개적으로 알려져 있고 **SSLCIPH** 채널 속성을 사용하여 엔터프라이즈에 적합한 알고리즘을 선택할 수 있습니다.

MQCSP 구조에 대한 자세한 정보는 [MQCSP 구조](#)를 참조하십시오.

비밀번호 보호는 다음 조건 모두가 충족될 때 사용됩니다.

- 연결의 양쪽 끝 모두 IBM MQ 8.0 이상을 사용 중입니다.
- 채널은 TLS 암호화를 사용 중이 아닙니다. 채널에 빈 **SSLCIPH** 속성이 있거나, **SSLCIPH** 속성이 암호화를 제공하지 않는 CipherSpec으로 설정된 경우, 채널이 TLS 암호화를 사용하지 않습니다. 예를 들어, NULL_SHA와 같은 널 암호는 암호화를 제공하지 않습니다.
- **MQCSP**를 설정합니다. **AuthenticationType** -MQCSP_AUTH_USER_ID_AND_PWD. 이 값을 설정하면 비밀번호 보호가 수행되는지 여부를 결정하기 위해 추가 검사를 평가할 수 있습니다. **MQCSP**의 기본값입니다. **AuthenticationType** 은 MQCSP_AUTH_NONE입니다. 기본 설정에서는 비밀번호 보호가 수행되지 않습니다. 자세한 정보는 **AuthenticationType**의 내용을 참조하십시오.
- 클라이언트가 IBM MQ 탐색기이고 사용자 ID 호환성 모드가 사용 불가능한 경우(이는 기본값이 아님). 이 조건은 IBM MQ 탐색기에만 적용 가능합니다.

이러한 조건이 충족되지 않은 경우에는 **PasswordProtection** 구성 설정에 의해 금지되지 않는 한 비밀번호는 일반 텍스트로 전송됩니다.

PasswordProtection 구성 설정

클라이언트 및 큐 관리자 .ini 구성 파일의 채널 섹션에 있는 **PasswordProtection** 속성은 비밀번호를 일반 텍스트로 전송하는 것을 방지할 수 있습니다. 속성은 다음 값 중 하나입니다. 기본값은 compatible입니다.

호환 가능

큐 관리자 또는 클라이언트 중 하나가 IBM MQ 8.0이전의 IBM MQ 버전을 실행 중인 경우 일반 텍스트로 비밀번호를 전송할 수 있습니다. 즉, 호환성을 위해 일반 텍스트 비밀번호가 허용됩니다.

따라서 다음과 같습니다.

- TLS 암호화가 사용되고 CipherSpec이 널이 아닌 경우 비밀번호는 TLS CipherSpec에 의해 암호화된 상태로 전송됩니다.
- 큐 관리자 또는 클라이언트 중 하나가 IBM MQ 8.0이전의 IBM MQ 버전을 실행 중이고 TLS 암호화가 사용되지 않은 경우 비밀번호가 일반 텍스트로 전송됩니다. 비밀번호는 일반 텍스트로 IBM MQ 8.0 이전 버전의 IBM MQ 가 일반 텍스트로만 비밀번호를 전송할 수 있으므로 일반 텍스트로 전송됩니다.
- 큐 관리자와 클라이언트가 둘 다 IBM MQ 8.0 이상에서 IBM MQ 버전을 실행 중이고 널 CipherSpec 이 사용되거나 TLS 암호화가 사용되지 않는 경우 비밀번호가 보호됩니다. **MQCSP.AuthenticationType** 은 MQCSP_AUTH_USER_ID_AND_PWD로 설정되어야 합니다.
- 큐 관리자와 클라이언트가 둘 다 IBM MQ 8.0 이상에서 IBM MQ 버전을 실행 중이고 **MQCSP**가 실행 중이면 비밀번호가 전송되기 전에 연결이 실패합니다. **AuthenticationType** 이 MQCSP_AUTH_USER_ID_AND_PWD로 설정되지 않았습니다.

항상

비밀번호는 널 (null) CipherSpec 또는 **MQCSP**가 아닌 CipherSpec 을 사용하여 암호화되어야 합니다. **AuthenticationType** 은 MQCSP_AUTH_USER_ID_AND_PWD로 설정되어야 합니다. 그렇지 않으면 연결이 실패합니다. 즉, 일반 텍스트 비밀번호는 허용되지 않습니다.

따라서 다음과 같습니다.

- TLS 암호화가 사용되고 CipherSpec이 널이 아닌 경우 비밀번호는 TLS CipherSpec에 의해 암호화된 상태로 전송됩니다.

- 큐 관리자와 클라이언트가 둘 다 IBM MQ 8.0 이상에서 IBM MQ 버전을 실행 중이고 TLS 암호화가 사용되지 않거나 널 (null) CipherSpec 이 사용되는 경우 비밀번호가 보호됩니다.
MQCSP.AuthenticationType 은 MQCSP_AUTH_USER_ID_AND_PWD로 설정되어야 합니다.
- 큐 관리자 또는 클라이언트가 IBM MQ IBM MQ 8.0 이전 버전을 실행 중이고, TLS 암호화를 사용하지 않는 경우 비밀번호가 송신되기 전에 연결이 실패합니다. As versions of IBM MQ earlier than IBM MQ 8.0 can send passwords only in plain text, and always requires the password to be either encrypted or protected, the connection fails.

선택사항

비밀번호는 선택적으로 보호 설정될 수 있지만 **MQCSP**인 경우 일반 텍스트로 전송됩니다. **AuthenticationType** 이 MQCSP_AUTH_USER_ID_AND_PWD로 설정되지 않았습니다. 즉, 모든 클라이언트가 일반 텍스트 비밀번호를 전송할 수 있습니다.

따라서 다음과 같습니다.

- TLS 암호화가 사용되고 CipherSpec이 널이 아닌 경우 비밀번호는 TLS CipherSpec에 의해 암호화된 상태로 전송됩니다.
- 널 (null) CipherSpec 이 사용되고 **MQCSP**인 경우 비밀번호가 일반 텍스트로 전송됩니다. **AuthenticationType** 이 MQCSP_AUTH_USER_ID_AND_PWD로 설정되지 않았습니다.
- 큐 관리자 또는 클라이언트 중 하나가 IBM MQ 8.0이전의 IBM MQ 버전을 실행 중이고 TLS 암호화가 사용되지 않은 경우 비밀번호가 일반 텍스트로 전송됩니다. 비밀번호는 일반 텍스트로 IBM MQ 8.0 이전 버전의 IBM MQ 가 일반 텍스트로만 비밀번호를 전송할 수 있으므로 일반 텍스트로 전송됩니다.
- 큐 관리자와 클라이언트가 둘 다 IBM MQ 8.0 에서 IBM MQ 버전을 실행 중인 경우, TLS 암호화가 사용되지 않거나 널 CipherSpec 이 사용되고 **MQCSP**가 사용되는 경우 비밀번호가 보호됩니다. **AuthenticationType** 은 MQCSP_AUTH_USER_ID_AND_PWD로 설정됩니다.

warn

모든 클라이언트가 일반 텍스트 비밀번호를 전송할 수 있습니다. 일반 텍스트 비밀번호가 수신되면 경고 메시지(AMQ9297)가 큐 관리자 오류 로그에 작성됩니다.

Java 및 JMS 클라이언트의 경우 **PasswordProtection** 속성의 작동은 호환 모드 또는 MQCSP 모드 사용을 선택하는지 여부에 따라 변경됩니다.

- Java 및 JMS 클라이언트가 호환 모드에서 작동 중인 경우에는 연결 처리 중에 MQCSP 구조가 플로우되지 않습니다. 따라서 **PasswordProtection** 속성의 동작은 IBM MQ 8.0이전의 IBM MQ 버전을 실행 중인 클라이언트에 대해 설명된 것과 동일한 동작입니다.
- Java 및 JMS 클라이언트가 MQCSP 모드에서 작동 중인 경우 **PasswordProtection** 속성의 작동은 설명된 것과 같은 작동입니다.

Java 및 JMS 클라이언트에 대한 연결 인증과 관련된 자세한 정보는 69 페이지의 『Java 클라이언트와의 연결 인증』의 내용을 참조하십시오.

디지털 인증 관리자(DCM, Digital Certificate Manager)

DCM을 사용하여 IBM i에서 디지털 인증서 및 개인 키를 관리합니다.

디지털 인증 관리자(DCM)를 사용하여 디지털 인증서를 관리하고 이를 IBM i 서버의 안전한 애플리케이션에서 사용할 수 있습니다. 디지털 인증 관리자를 사용하여 인증 기관(CA) 또는 다른 써드파티에서 디지털 인증서를 요청하고 처리할 수 있습니다. 또한, 로컬 인증 기관으로 작동하여 사용자를 위해 디지털 인증서를 작성하고 관리할 수도 있습니다.

DCM은 더 강력한 인증서 및 애플리케이션 유효성 검증 프로세스를 제공하기 위해 인증서 폐기 목록(CRL) 사용을 지원합니다. DCM을 사용하여 LDAP 서버에서 특정 인증 기관 CRL이 있는 위치를 정의하여 IBM MQ가 특정 인증서가 폐기되지 않았음을 확인할 수 있도록 합니다.

DCM은 다양한 형식의 인증서를 지원하며 이를 자동으로 감지할 수 있습니다. DCM이 PKCS #12 인코딩 인증서 또는 암호화된 데이터를 포함하는 PKCS #7 인증서를 감지하면, 자동으로 사용자에게 이 인증서를 암호화할 때 사용한 비밀번호 입력을 프롬프트합니다. DCM은 암호화된 데이터를 포함하지 않는 PKCS #7 인증서에 대해서는 프롬프트를 표시하지 않습니다.

DCM은 애플리케이션 및 사용자에게 대한 디지털 인증서를 관리하기 사용할 수 있는 브라우저 기반의 사용자 인터페이스를 제공합니다. 사용자 인터페이스는 탐색 프레임 및 태스크 프레임의 두 기본 프레임으로 나뉩니다.

탐색 프레임을 사용하여 인증서 또는 이를 사용하는 애플리케이션을 관리하는 태스크를 선택합니다. 일부 개별 태스크는 기본 탐색 프레임에 직접 표시되기도 하지만 탐색 프레임에서 대부분의 태스크는 범주로 구성됩니다. 예를 들어, 인증서 관리는 다양한 개별 안내 태스크(예: 인증서 보기, 인증서 갱신, 인증서 가져오기)가 포함되는 태스크 범주입니다. 탐색 프레임의 항목이 둘 이상의 태스크를 포함하는 범주인 경우에는 왼쪽에 화살표가 표시됩니다. 화살표는 범주 링크를 선택하면 펼쳐진 태스크 목록이 표시되어 수행할 태스크를 선택할 수 있음을 나타냅니다.



DCM에 대한 중요한 정보는 다음 IBM Redbooks® 발행물을 참조하십시오.


- *IBM i* 유선 네트워크 보안: OS/400 V5R1 DCM 및 암호화 향상, SG24-6168. 특히, IBM i 시스템을 로컬 CA로 설정하는 데 필요한 필수 정보는 부록을 참조하십시오.
- *AS/400 Internet Security: Developing a Digital Certificate Infrastructure*, SG24-5659. 특히, AS/400 DCM에 대해 설명하는 5장. *Digital Certificate Manager for AS/400*을 참조하십시오.


FIPS(Federal Information Processing Standard)

이 주제에서는 미국 국립 표준 기술국의 FIPS(Federal Information Processing Standard) Cryptomodule Validation Program 및 TLS 채널에서 사용할 수 있는 암호화 기술을 소개합니다.

이 정보는 다음 플랫폼에 적용됩니다.

-  UNIX, Linux, and Windows
-  z/OS

 UNIX, Linux, and Windows에서 IBM MQ TLS 연결의 FIPS 140-2준수에 대한 자세한 정보는 29 페이지의 『UNIX, Linux, and Windows용 FIPS(Federal Information Processing Standard)』의 내용을 참조하십시오.

 z/OS에서 IBM MQ TLS 연결의 FIPS 140-2준수에 대한 자세한 정보는 32 페이지의 『z/OS용 FIPS(Federal Information Processing Standard)』의 내용을 참조하십시오.

암호화 하드웨어가 있는 경우 IBM MQ에서 사용되는 암호화 모듈은 하드웨어 생산자가 제공하는 모듈로 구성 가능합니다. 모듈 구성을 완료하면 구성이 해당 암호화 모듈이 FIPS에서 인증된 경우에만 FIPS를 준수합니다.

시간이 흐름에 따라 FIPS(Federal Information Processing Standards)는 암호화 알고리즘 및 프로토콜에 대한 새 공격을 반영할 수 있도록 업데이트되었습니다. 예를 들어, 일부 CipherSpec은 FIPS 인증 CipherSpec이 되기 위해 정지될 수 있습니다. 이런 경우 IBM MQ도 최신 표준 구현으로 업데이트됩니다. 그 결과 유지보수를 적용한 후에는 동작이 변경됨을 알 수 있습니다.

관련 개념

241 페이지의 『MQI 클라이언트에서 런타임 시 FIPS 인증 CipherSpec만 사용하도록 지정』

FIPS 준수 소프트웨어를 사용하여 키 저장소를 작성한 다음 채널이 FIPS-인증 CipherSpec을 사용해야 함을 지정하십시오.

255 페이지의 『runmqckm, runmqakm 및 strmqikm을 사용하여 디지털 인증서 관리』

UNIX, Linux, and Windows 시스템에서 **strmqikm**(iKeyman) GUI를 사용하거나 **runmqckm**(iKeycmd) 또는 **runmqakm**(GSKCapiCmd)을 사용하여 키 및 디지털 인증서를 관리하십시오.

관련 태스크

IBM MQ classes for Java에서 TLS 사용

IBM MQ classes for JMS에 TLS(Transport Layer Security) 사용

관련 참조

JMS 오브젝트의 TLS 특성

18 페이지의 『FIPS(Federal Information Processing Standard)』

미국 정부에서는 데이터 암호화 같은 IT 시스템과 보안에 대한 기술적 자문을 만들고 있습니다. NIST(National Institute for Standards and Technology)는 IT 시스템 및 보안과 관련된 중요한 조직입니다. NIST는 FIPS(Federal Information Processing Standard)를 포함하는 표준 및 권장사항을 생성합니다.

 UNIX, Linux, and Windows용 FIPS(Federal Information Processing Standard)

Windows, UNIX and Linux 시스템에서 SSL/TLS 채널에 암호화가 필요한 경우, IBM MQ는 ICC(IBM Crypto for C)라고 하는 암호화 패키지를 사용합니다. Windows, UNIX and Linux 플랫폼에서 ICC 소프트웨어는 미국 국립

표준 기술원(US National Institute of Standards and Technology)의 FIPS(Federal Information Processing Standards) Cryptomodule Validation Program 레벨 140-2를 통과했습니다.

Windows, UNIX and Linux 시스템에서 IBM MQ TLS 연결의 FIPS 140-2준수는 다음과 같습니다.

- 다음과 같은 조건이 충족되면 모든 IBM MQ 메시지 채널(CLNTCONN 채널 유형 제외)에 대해 연결은 FIPS를 준수합니다.
 - 설치된 GSKit ICC 버전은 설치된 운영 체제 버전 및 하드웨어 아키텍처에서 FIPS 140-2 준수가 인증되었습니다.
 - 큐 관리자의 SSLFIPS 속성이 YES로 설정되었습니다.
 - 모든 키 저장소가 FIPS 준수 소프트웨어(예: -fips 옵션이 지정된 **runmqakm**)만을 사용하여 작성되고 조작성됩니다.
- 다음 조건이 충족되는 경우, 모든 IBM MQ MQI client 애플리케이션에 대해 연결은 GSKit을 사용하며 FIPS를 준수합니다.
 - 설치된 GSKit ICC 버전은 설치된 운영 체제 버전 및 하드웨어 아키텍처에서 FIPS 140-2 준수가 인증되었습니다.
 - MQI 클라이언트에 대한 관련 주제에 설명된 대로 FIPS 인증 암호만 사용되도록 지정했습니다.
 - 모든 키 저장소가 FIPS 준수 소프트웨어(예: -fips 옵션이 지정된 **runmqakm**)만을 사용하여 작성되고 조작성됩니다.
- 다음 조건이 충족되는 경우, 클라이언트 모드를 사용하는 IBM MQ classes for Java 애플리케이션에 대해 연결은 JRE의 TLS 구현을 사용하며 FIPS를 준수합니다.
 - 애플리케이션 실행에 사용되는 Java Runtime Environment는 설치된 운영 체제 버전 및 하드웨어 아키텍처에서 FIPS를 준수합니다.
 - Java 클라이언트에 대한 관련 주제에 설명된 대로 FIPS 인증 암호만 사용되도록 지정했습니다.
 - 모든 키 저장소가 FIPS 준수 소프트웨어(예: -fips 옵션이 지정된 **runmqakm**)만을 사용하여 작성되고 조작성됩니다.
- 다음 조건이 충족되는 경우, 클라이언트 모드를 사용하는 IBM MQ classes for JMS 애플리케이션에 대해 연결은 JRE의 TLS 구현을 사용하며 FIPS를 준수합니다.
 - 애플리케이션 실행에 사용되는 Java Runtime Environment는 설치된 운영 체제 버전 및 하드웨어 아키텍처에서 FIPS를 준수합니다.
 - JMS 클라이언트에 대한 관련 주제에 설명된 대로 FIPS 인증 암호만 사용되도록 지정했습니다.
 - 모든 키 저장소가 FIPS 준수 소프트웨어(예: -fips 옵션이 지정된 **runmqakm**)만을 사용하여 작성되고 조작성됩니다.
- 다음 조건이 충족되는 경우, 비관리 .NET 클라이언트 애플리케이션에 대해 연결은 GSKit을 사용하며 FIPS를 준수합니다.
 - 설치된 GSKit ICC 버전은 설치된 운영 체제 버전 및 하드웨어 아키텍처에서 FIPS 140-2 준수가 인증되었습니다.
 - .NET 클라이언트에 대한 관련 주제에 설명된 대로 FIPS 인증 암호만 사용되도록 지정했습니다.
 - 모든 키 저장소가 FIPS 준수 소프트웨어(예: -fips 옵션이 지정된 **runmqakm**)만을 사용하여 작성되고 조작성됩니다.
- 다음 조건이 충족되는 경우, 비관리 XMS .NET 클라이언트 애플리케이션에 대해 연결은 GSKit을 사용하며 FIPS를 준수합니다.
 - 설치된 GSKit ICC 버전은 설치된 운영 체제 버전 및 하드웨어 아키텍처에서 FIPS 140-2 준수가 인증되었습니다.
 - XMS .NET 문서에서 명시하는 것처럼 FIPS 인증 암호만 사용되도록 지정했습니다.
 - 모든 키 저장소가 FIPS 준수 소프트웨어(예: -fips 옵션이 지정된 **runmqakm**)만을 사용하여 작성되고 조작성됩니다.

각 수정팩 또는 Refresh Pack에 포함되는 Readme 파일에서 언급하는 경우를 제외하고는 모든 지원 플랫폼은 FIPS 140-2 인증되었습니다.

GSKit을 사용하는 TLS 연결에 대해 FIPS 140-2 인증된 컴포넌트 이름은 ICC입니다. 이는 지정된 모든 플랫폼에서 GSKit FIPS 준수를 판별하는 이 컴포넌트 버전입니다. 현재 설치된 ICC 버전을 판별하려면 **dspmqrver -p 64 -v** 명령어를 실행하십시오.

다음은 ICC에 관련된 **dspmqrver -p 64 -v** 출력에 대한 추출 예입니다.

```
ICC
=====
@(#)CompanyName: IBM Corporation
@(#)LegalTrademarks: IBM
@(#)FileDescription: IBM Crypto for C-language
@(#)FileVersion: 8.0.0.0
@(#)LegalCopyright: Licensed Materials - Property of IBM
@(#) ICC
@ (#) (C) Copyright IBM Corp. 2002, 2024.
@ (#) All Rights Reserved. US Government Users
@(#) Restricted Rights - Use, duplication or disclosure
@(#) restricted by GSA ADP Schedule Contract with IBM Corp.
@(#)ProductName: icc_8.0 (GoldCoast Build) 100415
@(#)ProductVersion: 8.0.0.0
@(#)ProductInfo: 10/04/15.03:32:19.10/04/15.18:41:51
@(#)CMVCInfo:
```

GSKit ICC 8 (GSKit 8에 포함됨)에 대한 NIST 인증 명령문은 [Cryptographic Module Validation Program](#)에서 찾을 수 있습니다.

암호화 하드웨어가 있는 경우 IBM MQ에서 사용되는 암호화 모듈은 하드웨어 생산자가 제공하는 모듈로 구성 가능합니다. 모듈 구성을 완료하면 구성이 해당 암호화 모듈이 FIPS에서 인증된 경우에만 FIPS를 준수합니다.

참고: Intel 시스템에서 실행 시 FIPS 140-2 준수 조작에 대해 구성된 32비트 Solaris x86 SSL 및 TLS 클라이언트가 실패합니다. FIPS 140-2 준수 GSKit-Crypto Solaris x86 32비트 라이브러리 파일은 Intel 칩 세트에 로드되지 않기 때문에 이와 같은 실패가 발생합니다. 영향받는 시스템에서 오류 AMQ9655가 클라이언트 오류 로그에 보고됩니다. 이 문제를 해결하려면 FIPS 140-2 준수를 사용 안함으로 설정하거나, 64비트 코드는 영향을 받지 않으므로 클라이언트 애플리케이션 64비트를 재컴파일하십시오.

FIPS 140-2 준수로 사용되는 경우 3중 DES(3DES) 제한이 강제로 적용됩니다.

IBM MQ가 FIPS 140-2 준수로 작동되도록 구성되면 추가 제한은 3중 DES(3DES) CipherSpec에 관련되도록 강제 적용됩니다. 이런 제한을 사용하여 US NIST SP800-67 권장사항이 준수됩니다.

1. 3중 DES 키의 모든 파트는 고유해야 합니다.
2. NIST SP800-67 정의에 따라 3중 DES 키의 어떤 파트도 Weak, Semi-Weak 또는 Possibly-Weak 키일 수 없습니다.
3. 32GB 이상의 데이터를 보안 키 재설정 수행 전에 연결로 전송할 수 없습니다. 기본적으로 IBM MQ는 비밀 세션 키를 재설정하지 않기 때문에 이 재설정은 구성해야 합니다. 3중 DES CipherSpec 및 FIPS 140-2 준수 사용 시 보안 키 재설정을 수행하지 않으면 최대 바이트 수가 초과된 후 연결은 AMQ9288 오류로 종료됩니다. 보안 키 재설정 구성 방법에 대한 정보는 400 페이지의 [『SSL 및 TLS 비밀 키 재설정』](#)의 내용을 참조하십시오.

IBM MQ는 규칙 1 및 2를 이미 준수하는 3중 DES 세션 키를 생성합니다. 그러나 세 번째 제한을 충족하려면 FIPS 140-2 구성에서 3중 DES CipherSpec을 사용할 때 보안 키 재설정을 사용으로 설정해야 합니다. 또는 3중 DES를 사용하지 않을 수 있습니다.

관련 개념

[241 페이지의 『MQI 클라이언트에서 런타임 시 FIPS 인증 CipherSpec만 사용하도록 지정』](#)

FIPS 준수 소프트웨어를 사용하여 키 저장소를 작성한 다음 채널이 FIPS-인증 CipherSpec을 사용해야 함을 지정하십시오.

[255 페이지의 『runmqckm, runmqakm 및 strmqikm을 사용하여 디지털 인증서 관리』](#)

UNIX, Linux, and Windows 시스템에서 **strmqikm**(iKeyman) GUI를 사용하거나 **runmqckm**(iKeycmd) 또는 **runmqakm**(GSKCapiCmd)을 사용하여 키 및 디지털 인증서를 관리하십시오.

관련 태스크

[IBM MQ classes for Java에서 TLS 사용](#)

[IBM MQ classes for JMS에 TLS\(Transport Layer Security\) 사용](#)

관련 참조

JMS 오브젝트의 TLS 특성

18 페이지의 『FIPS(Federal Information Processing Standard)』

미국 정부에서는 데이터 암호화 같은 IT 시스템과 보안에 대한 기술적 자문을 만들고 있습니다. NIST(National Institute for Standards and Technology)는 IT 시스템 및 보안과 관련된 중요한 조직입니다. NIST는 FIPS(Federal Information Processing Standard)를 포함하는 표준 및 권장사항을 생성합니다.

z/OS z/OS용 FIPS(Federal Information Processing Standard)

z/OS의 SSL/TLS 채널에 암호화가 필요한 경우 IBM MQ는 시스템 SSL이라는 서비스를 사용합니다. 시스템 SSL은 미국 국립 표준 기술원(US National Institute of Standards and Technology)의 FIPS(Federal Information Processing Standards) Cryptomodule Validation Program 레벨 140-2에 맞게 설계된 모드에서 안전하게 실행할 수 있도록 해줍니다.

IBM MQ TLS 연결과 FIPS 140-2 준수 연결을 구현하는 경우 몇 가지에 주의해야 합니다.

- FIPS 준수에 대해 IBM MQ 메시지 채널을 사용하려면 다음 조건이 충족되어야 합니다.
 - 시스템 SSL 보안 레벨 3 FMID가 설치 및 구성되었습니다(IBM MQ 설치 계획 참조).
 - 시스템 SSL 모듈이 유효성 검증됩니다.
 - 큐 관리자 SSLFIPS 속성이 **YES**로 설정되었습니다.

FIPS 모드에서 실행될 때 시스템 SSL은 가능한 경우, CPACF(CP Assist for Cryptographic Function)를 사용합니다. 비FIPS 모드에서 실행 중일 때 ICSF 지원 하드웨어에서 수행되는 암호화 기능은 FIPS 모드에서 실행되는 경우에도 계속 사용되며 소프트웨어에서 수행해야 하는 RSA 서명 생성의 경우는 예외입니다.

알고리즘	비FIPS		FIPS	
	키 크기	하드웨어	키 크기	하드웨어
RC2	40 및 128			
RC4	40 및 128			
DES	56	x		
TDES	168	x	168	x
AES	128 및 256	x	128 및 256	x
MD5	48			
SHA-1	160	x	160	x
SHA-2	224, 256, 384, 512	x	224, 256, 384, 512	x
RSA	512-4096	x	1024-4096	x
DSA	512-1024		1024	
DH	512-2048		2048	

FIPS 모드에서 시스템 SSL은 표 1에 표시된 알고리즘 및 키 크기를 사용하는 인증서만 사용할 수 있습니다. X.509 인증서 유효성 검증 중에 FIPS 모드와 호환되지 않는 알고리즘이 발견되는 경우 인증서를 사용할 수 없으며 올바르지 않은 것으로 처리됩니다.

WebSphere® Application Server 내에서 클라이언트 모드를 사용 중인 IBM MQ 클래스 애플리케이션의 경우 FIPS(Federal Information Processing Standards) 지원을 참조하십시오.

시스템 SSL 모듈 구성에 대한 정보는 시스템 SSL 모듈 검증 설정을 참조하십시오.

관련 참조

18 페이지의 『FIPS(Federal Information Processing Standard)』

미국 정부에서는 데이터 암호화 같은 IT 시스템과 보안에 대한 기술적 자문을 만들고 있습니다. NIST(National Institute for Standards and Technology)는 IT 시스템 및 보안과 관련된 중요한 조직입니다. NIST는 FIPS(Federal Information Processing Standard)를 포함하는 표준 및 권장사항을 생성합니다.

Multi **mqcertck**를 사용한 큐 관리자의 TLS 구성 확인

MQCERTCK 명령은 큐 관리자의 TLS 구성에서 일반적인 실수를 찾고, 문제점을 해결하기 위한 제안사항을 제공합니다.

소개

mqcertck 명령은 다음 항목을 확인합니다.

- 큐 관리자 **SSLKEYR** 속성에서 참조되는 큐 관리자의 키 저장소의 존재 및 권한.
- 큐 관리자 **CERTLABL** 속성에서 참조되는 큐 관리자 인증서에 대한 인증서의 존재 및 유효성.
- TLS 사용 채널의 **CERTLABL** 속성에서 참조되는 모든 인증서의 존재 및 유효성.
- 클라이언트 애플리케이션의 키 저장소 및 인증서(인증서가 큐 관리자에 대해 권한 부여되었는지에 대한 확인 포함)

참고: **mqcertck** 명령은 z/OS 또는 IBM i에서 사용할 수 없습니다.

사용법

mqcertck 명령을 사용하려면 명령행에서 명령 **mqcertck**를 필수 매개변수, 그리고 자신이 필요로 하는 선택적 매개변수와 함께 실행하십시오.

명령 및 명령이 취하는 매개변수에 대한 설명은 [mqcertck](#)를 참조하십시오.

예

큐 관리자의 SVRCONN 채널에 연결하는 클라이언트에서 TLS를 연결할 수 있도록 큐 관리자 QM1 설정을 완료했습니다.

다중 인증 기능을 사용 중이므로 큐 관리자 및 채널 모두의 **CERTLABL** 속성에 인증서 레이블이 지정되어 있습니다. 채널을 작성하는 동안 채널의 **CERTLABL** 속성에 오류가 발생하므로 클라이언트가 연결을 시도할 때 큐 관리자가 MQRC_SSL_INITIALIZATION_ERROR의 2393 리턴 코드를 리턴합니다.

사용자가 큐 관리자를 활성화하기 전에 **mqcertck** 명령을 사용하여 큐 관리자의 TLS 구성을 확인합니다.

mqcertck QM1 명령을 실행하고 다음 출력을 수신합니다.

```
5724-H72 (C) Copyright IBM Corp. 1994, 2024.
+-----+
| IBM MQ TLS Configuration Test tool
+-----+
| Problem identified:
| No certificate could be found for the channel
| MQCERTCK.CHANNEL
| This tool looked in the Queue Manager's key repository
| located at: 'C:\MQ Data\qmgrs\QM1\ssl\key.kdb'
| for a certificate with label 'chacert',
| which is the certificate specified in the channel's
| CERTLABL attribute, but was unable to find one.
|
| Possible resolution:
| A valid certificate with the label chacert
| needs to be added to the key repository.
|
| Alternatively, alter the channel definition to remove
| the CERTLABL value. This can be done by executing the
| following command in runmqsc:
|     ALTER CHANNEL(<Name>) CHLTYPE(<TYPE>) CERTLABL(' ')
+-----+
| mqcertck has ended. See above for any problems found.
| If there are problems then resolve these and run this
| tool again.
```

이 출력은 사용자가 서버 연결 채널 MQCERTCK.CHANNEL의 채널 정의를 확인하도록 지시합니다. 여기서, 작성한 오류가 표시되며 mqcertck 명령을 다시 실행하기 전에 오류를 정정하여 문제점을 해결했는지 확인할 수 있습니다.

클라이언트 연결 확인

mqcertck 명령에는 큐 관리자의 TLS 구성 외에 클라이언트 키 저장소를 확인하는 기능도 있습니다. 이를 수행하려면 **mqcertck**가 큐 관리자를 실행 중인 시스템에서 클라이언트의 키 저장소에 액세스할 수 있어야 합니다.

mqcertck 명령을 실행할 때, **-clientkeyr** 매개변수를 클라이언트 키 저장소의 위치(확장자는 제외)와 함께 제공하면 **mqcertck**가 이 키 저장소를 큐 관리자에 대해 확인합니다.

클라이언트가 큐 관리자에 연결하기 위해 사용할 채널을 알고 있으면 **-clientchannel** 플래그를 사용하여 지정할 수 있습니다.

클라이언트가 큐 관리자에 연결하는 데 상호 인증을 사용하고 있는 경우에는 **-clientusername** 또는 **-clientlabel** 매개변수를 사용하여 **mqcertck** 명령이 클라이언트 키 저장소에서 사용할 인증서를 지정할 수 있습니다.

기본 인증서를 사용하고 클라이언트 애플리케이션에 인증서 레이블을 제공하지 않는 경우, **-clientusername** 및 이 애플리케이션을 실행하는 **username** 매개변수를 사용할 수 있습니다.

mqcertck 명령의 조작 중에, 이 명령은 인증서 레이블 **ibmwebsphermqXXXX**를 생성하며 여기서 **XXXX**는 **-clientusername** 매개변수에서 전달된 값입니다.

클라이언트 키 저장소를 완전히 확인하기 위해, **mqcertck** 명령은 GSKit을 사용하여 더미 연결을 작성합니다. 이를 수행하려면 이 명령이 클라이언트 테스트 중에 바인드될 수 있는, 사용 가능한 포트가 있어야 합니다. 사용되는 기본 포트는 5857이지만, 이미 사용 중인 경우 클라이언트 테스트 중에 사용할 다른 포트를 지정할 수 있습니다.

참고: **mqcertck** 명령은 포트에 바인드되지만 **mqcertck**는 외부 통신을 사용하지 않으며, 모든 테스트는 로컬로 수행됩니다.

IBM MQ MQI client의 SSL/TLS

IBM MQ는 클라이언트에서 TLS를 지원합니다. 다양한 방식으로 TLS 사용을 조정할 수 있습니다.

IBM MQ provides TLS support for IBM MQ MQI clients on Windows, UNIX and Linux systems. IBM MQ classes for Java를 사용 중인 경우 IBM MQ classes for Java 사용을 참조하고 IBM MQ classes for JMS를 사용 중인 경우 IBM MQ classes for JMS 사용을 참조하십시오. 이 절의 나머지 부분은 Java 또는 JMS 환경에는 적용되지 않습니다.

IBM MQ 클라이언트 구성 파일에 MQSSLKEYR값을 사용하거나, 응용프로그램이 MQCONNX 호출을 작성할 때 IBM MQ MQI client에 대한 키 저장소를 지정할 수 있습니다. 채널이 TLS를 사용하도록 지정하기 위한 세 가지 옵션이 있습니다.

- 채널 정의 테이블 사용
- MQCONNX 호출에서 SSL 구성 옵션 구조인 MQSCO 사용
- Active Directory 사용(Windows 시스템)

MQSERVER 환경 변수를 사용해서는 채널이 TLS를 사용하도록 지정할 수 없습니다.

TLS가 채널의 다른 쪽에 지정되지 않은 경우 TLS 없이 계속 기존 IBM MQ MQI client 애플리케이션을 실행할 수 있습니다.

클라이언트 시스템에서 TLS 키 저장소의 콘텐츠, TLS 키 저장소의 위치, 인증 정보 또는 암호화 하드웨어 매개변수를 변경하면, 애플리케이션이 큐 관리자에 연결하기 위해 사용 중인 클라이언트 연결 채널에서 이러한 변경사항을 반영하기 위해 모든 TLS 연결을 종료해야 합니다. 모든 연결이 종료되면 TLS 채널을 재시작하십시오. 모든 새 TLS 설정이 사용됩니다. 이 설정은 큐 관리자 시스템에서 REFRESH SECURITY TYPE(SSL) 명령으로 새로 고쳐지는 설정과 유사합니다.

IBM MQ MQI client가 Windows, UNIX and Linux 시스템에서 암호화 하드웨어를 사용하여 실행되는 경우 MQSSLCRYP 환경 변수를 사용하여 하드웨어를 구성하십시오. 이 변수는 ALTER QMGR MQSC 명령에서의 SSLCRYP 매개변수와 동일합니다. ALTER QMGR MQSC 명령의 SSLCRYP 매개변수에 대한 설명은 ALTER QMGR을 참조하십시오. SSLCRYP 매개변수의 GSK_PCS11 버전을 사용하는 경우에는 PKCS #11 토큰 레이블은 전적으로 소문자로 지정되어야 합니다.

TLS 보안 키 재설정 및 FIPS는 IBM MQ MQI clients에서 지원됩니다. 자세한 정보는 400 페이지의 『SSL 및 TLS 비밀 키 재설정』 및 29 페이지의 『UNIX, Linux, and Windows용 FIPS(Federal Information Processing Standard)』의 내용을 참조하십시오.

IBM MQ MQI clients의 TLS 지원에 대한 자세한 정보는 240 페이지의 『IBM MQ MQI client 보안 설정』의 내용을 참조하십시오.

관련 태스크

[구성 파일을 사용하여 클라이언트 구성](#)

MQI 채널이 SSL/TLS를 사용하도록 지정

MQI 채널이 TLS를 사용하도록 클라이언트 연결 채널의 *SSLCipherSpec* 속성 값은 클라이언트 플랫폼의 IBM MQ에서 지원되는 CipherSpec 이름이어야 합니다.

다음과 같은 방법으로 이 속성 값을 가진 클라이언트 연결 채널을 정의할 수 있습니다. 이는 우선순위 감소 순으로 나열됩니다.

1. PreConnect 엑시트가 사용할 채널 정의 구조를 제공하는 경우.

PreConnect 엑시트는 채널 정의 구조 MQCD의 *SSLCipherSpec* 필드에서 CipherSpec 이름을 제공할 수 있습니다. 이 구조는 PreConnect 엑시트에서 사용하는 MQNXP 엑시트 매개변수 구조의 **ppMQCDArrayPtr** 필드에서 리턴됩니다.

2. IBM MQ MQI client 애플리케이션이 MQCONNX 호출을 발행하는 경우.

애플리케이션은 채널 정의 구조 MQCD의 *SSLCipherSpec* 필드에 CipherSpec 이름을 지정할 수 있습니다. 이 구조는 MQCONNX 호출의 매개변수인 연결 옵션 구조 MQCNO에서 참조됩니다.

3. 클라이언트 채널 정의 테이블(CCDT) 사용.

클라이언트 채널 정의 테이블에 있는 하나 이상의 입력 항목은 CipherSpec의 이름을 지정할 수 있습니다. 예를 들어, DEFINE CHANNEL MQSC 명령을 사용하여 항목을 작성한 경우 명령에 대해 SSLCIPH 매개변수를 사용하여 CipherSpec의 이름을 지정할 수 있습니다.

4. Windows에서 Active Directory 사용.

Windows 시스템에서 **setmqscp** 제어 명령을 사용하여 Active Directory에 클라이언트 연결 채널 정의를 발행할 수 있습니다. 이 정의 중 하나 이상은 CipherSpec 이름을 지정할 수 있습니다.

예를 들어, 클라이언트 애플리케이션이 MQCONNX 호출에서 MQCD 구조에 클라이언트 연결 채널 정의를 제공하는 경우, 이 정의는 IBM MQ 클라이언트가 액세스할 수 있는 클라이언트 채널 정의 테이블의 임의 항목에 대한 환경 설정에 사용됩니다.

TLS를 사용하는 MQI 채널의 클라이언트 종료 시 채널 정의를 제공하는 데 MQSERVER 환경 변수를 사용할 수 없습니다.

클라이언트 인증서가 플로우되었는지 여부를 확인하려면 피어 이름 매개변수 값의 존재에 대한 채널의 서버 측에서 채널 상태를 표시하십시오.

관련 개념

[389 페이지의 『IBM MQ MQI client를 위해 CipherSpec 지정』](#)

IBM MQ MQI client를 위해 CipherSpec을 지정하기 위한 세 가지 옵션이 있습니다.

IBM MQ의 CipherSpec 및 CipherSuite

IBM MQ는 TLS 1.2 CipherSpec 및 RSA와 Diffie-Hellman 알고리즘을 지원합니다. 하지만 이를 수행해야 하는 경우 더 이상 사용되지 않는 CipherSpec을 사용으로 설정할 수 있습니다.

다음에 대한 정보는 376 페이지의 『CipherSpec 사용 가능』의 내용을 참조하십시오.

- IBM MQ에서 지원되는 CipherSpec.

- 더 이상 사용되지 않는 SSL 3.0 및 TLS 1.0 CipherSpec을 사용으로 설정하는 방법

IBM MQ는 RAS 및 Diffie-Hellman 키 교환 및 인증 알고리즘을 지원합니다. TLS 데이터 교환 중 사용되는 키의 크기는 사용자가 사용하는 디지털 인증서에 따라 결정될 수 있지만 일부 CipherSpec은 데이터 교환 키 크기의 스펙을 포함합니다. 데이터 교환 키 크기가 클수록 보다 강력한 인증이 제공됩니다. 키 크기가 작아지면 데이터 교환이 보다 빨라집니다.

관련 개념

17 페이지의 『CipherSpecs 및 CipherSuites』

암호화 보안 프로토콜은 안전 연결에서 사용되는 알고리즘에 동의해야 합니다. CipherSpec 및 CipherSuite는 특정 알고리즘 결합을 정의합니다.

IBM MQ에서의 NSA 스위트 B Cryptography

This topic provides information about how to configure IBM MQ on Windows, Linux, and UNIX to conform to the Suite B compliant TLS 1.2 profile.

시간이 흐름에 따라 NSA Cryptography 스위트 B 표준은 암호화 알고리즘 프로토콜에 대한 새 공격을 반영할 수 있도록 업데이트되었습니다. 예를 들어, 일부 CipherSpec은 스위트 B 인증 CipherSpec이 되기 위해 정지될 수 있습니다. 이런 경우 IBM MQ도 최신 표준 구현으로 업데이트됩니다. 그 결과 유지보수를 적용한 후에는 동작이 변경됨을 알 수 있습니다. IBM MQ Readme 파일은 각 제품 유지보수 레벨에서 적용된 스위트 B의 버전을 나열합니다. IBM MQ가 스위트 B 준수를 강제 적용하도록 구성하려면 유지보수 적용 계획 시에 Readme 파일을 항상 참조하십시오. [IBM MQ, WebSphere MQ 및 MQSeries® 제품 Readme의 내용을 참조하십시오.](#)

Windows, UNIX, Linux 시스템에서 IBM MQ는 표 1에 표시되는 보안 레벨로 스위트 B 준수 TLS 1.2 프로파일을 준수하도록 구성됩니다.

표 3. 허용된 CipherSpec 및 디지털 서명 알고리즘이 사용되는 스위트 B 보안 레벨		
보안 레벨	허용되는 CipherSpec	허용되는 디지털 서명 알고리즘
128비트	ECDHE_ECDSA_AES_128_GCM_SHA256 ECDHE_ECDSA_AES_256_GCM_SHA384	SHA-256을 사용하는 ECDSA SHA-384를 사용한 ECDSA
192비트	ECDHE_ECDSA_AES_256_GCM_SHA384	SHA-384를 사용한 ECDSA
모두 ¹	ECDHE_ECDSA_AES_128_GCM_SHA256 ECDHE_ECDSA_AES_256_GCM_SHA384	SHA-256을 사용하는 ECDSA SHA-384를 사용한 ECDSA

1. 128비트 및 192비트 보안 레벨을 동시에 구성하는 것도 가능합니다. 스위트 B 구성은 최소 허용 가능 암호화 알고리즘을 판별하기 때문에 두 보안 레벨 구성은 128비트 보안 레벨 구성과 동일합니다. 192비트 보안 레벨의 암호화 알고리즘은 128비트 보안 레벨에 필요한 최소값보다 강력하기 때문에 192비트 보안 레벨이 사용 가능하지 않더라도 128비트 보안 레벨에 대해 허용됩니다.

참고: 보안 레벨에 사용되는 이름 지정 규칙은 Elliptic Curve 크기 또는 AES 암호화 알고리즘 키 크기를 표시할 필요는 없습니다.

스위트 B에 대한 CipherSpec 준수

IBM MQ의 기본 동작이 스위트 B 표준을 준수하지 않더라도 IBM MQ는 Windows, UNIX and Linux 시스템에서 이들 중 하나 또는 둘 다의 보안 레벨을 준수하도록 구성할 수 있습니다. 스위트 B를 사용하도록 IBM MQ를 올바르게 구성한 후에 스위트 B를 준수하지 않는 CipherSpec을 사용하는 아웃바운드 채널 시작 시도는 오류 AMQ9282를 초래합니다. 이 활동은 MQI 클라이언트도 이유 코드 MQRC_CIPHER_SPEC_NOT_SUITE_B를 리턴하도록 합니다. 이와 유사하게 스위트 B 구성을 준수하지 않는 CipherSpec을 사용하는 인바운드 채널 시작 시도도 오류 AMQ9616을 초래합니다.

IBM MQ CipherSpec에 대한 자세한 정보는 376 페이지의 『CipherSpec 사용 가능』의 내용을 참조하십시오.

스위트 B 및 디지털 인증서

스위트 B는 디지털 인증서 서명에 사용할 수 있는 디지털 서명 알고리즘을 제한합니다. 스위트 B는 인증서가 포함할 수 있는 공개 키 유형도 제한합니다. 따라서, IBM MQ는 디지털 서명 알고리즘 및 공개 키 유형이 원격 파트너의 구성된 스위트 B 보안 레벨에서 허용되는 인증서를 사용하도록 구성해야 합니다. 보안 레벨 요구사항을 준수하지 않는 디지털 인증서는 거부되고 연결은 AMQ9633 또는 AMQ9285 오류로 실패합니다.

128비트 스위트 B 보안 레벨에 대해 인증서 주체의 공개 키는 NIST P-256 Elliptic Curve 또는 NIST P-384 Elliptic Curve를 사용하고 NIST P-256 Elliptic Curve 또는 NIST P-384 Elliptic Curve로 서명되어야 합니다. 192비트 스위트 B 보안 레벨에서 인증서 주체의 공개 키는 NIST P-384 Elliptic Curve를 사용하고 NIST P-384 Elliptic Curve로 서명되어야 합니다.

스위트 B 준수 조작에 적합한 인증서를 확보하려면 `runmqakm` 명령을 사용하여 `-sig_alg` 매개변수를 지정하여 적합한 디지털 서명 알고리즘을 요청하십시오. `EC_ecdsa_with_SHA256` 및 `EC_ecdsa_with_SHA384` `-sig_alg` 매개변수 값은 허용되는 스위트 B 디지털 서명 알고리즘으로 서명되는 Elliptic Curve 키에 대응합니다.

`runmqakm` 명령에 대한 자세한 정보는 `runmqckm` 및 `runmqakm` 옵션을 참조하십시오.

참고: `runmqckm` 및 `strmqikm` 명령은 스위트 B 준수 조작에 대한 디지털 인증서 작성을 지원하지 않습니다.

디지털 인증서 작성 및 요청

스위트 B 테스트를 위해 자체 서명 디지털 인증서를 작성하려는 경우에는 262 페이지의 『UNIX, Linux, and Windows에서 자체 서명된 개인 인증서 작성』의 내용을 참조하십시오.

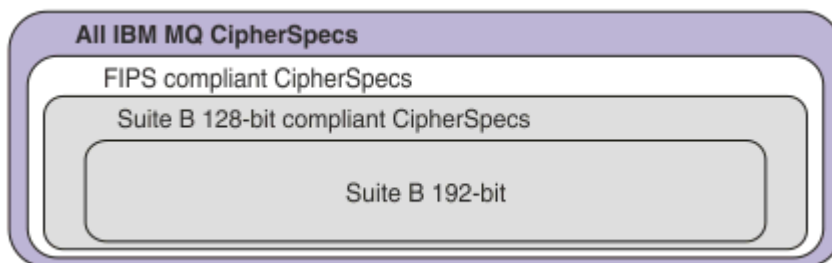
스위트 B 프로덕션 사용을 위해 CA 서명 디지털 인증서를 요청하려는 경우에는 265 페이지의 『UNIX, Linux, and Windows에서 개인 인증서 요청』의 내용을 참조하십시오.

참고: 사용 중인 인증 기관은 IETF RFC 6460에서 설명하는 요구사항을 충족시키는 디지털 인증서를 생성해야 합니다.

FIPS 140-2 및 스위트 B

스위트 B 표준은 보증된 보안 레벨을 제공하기 위해서 사용 가능한 암호화 알고리즘 세트를 제한하기 때문에 개념상 FIPS 140-2와 비슷합니다. 현재 지원되는 스위트 B CipherSpec은 IBM MQ가 FIPS 140-2 준수 조작용으로 구성된 경우에 사용할 수 있습니다. 따라서, FIPS 및 스위트 B 준수 모두에 대해 동시에 IBM MQ를 구성할 수 있으며 이 경우 두 제한사항 세트가 모두 적용됩니다.

다음 다이어그램은 이러한 서브세트 간의 관계를 보여줍니다.



스위트 B 준수 조작을 위해 IBM MQ 구성

For information about how to configure IBM MQ on Windows, UNIX and Linux for Suite B compliant operation, see 38 페이지의 『스위트 B에 대해 IBM MQ 구성』.

IBM MQ는 IBM i 및 z/OS 플랫폼에서 스위트 B 준수 조작을 지원하지 않습니다. IBM MQ Java 및 JMS 클라이언트도 스위트 B 준수 조작을 지원하지 않습니다.

관련 개념

241 페이지의 『MQI 클라이언트에서 런타임 시 FIPS 인증 CipherSpec만 사용하도록 지정』

FIPS 준수 소프트웨어를 사용하여 키 저장소를 작성한 다음 채널이 FIPS-인증 CipherSpec을 사용해야 함을 지정하십시오.

스위트 B에 대해 IBM MQ 구성

IBM MQ는 Windows, UNIX and Linux 플랫폼에서 NSA 스위트 B 표준을 준수하여 작동하도록 구성 가능합니다.

스위트 B는 보증된 보안 레벨을 제공하기 위해서 사용 가능한 암호화 알고리즘 세트를 제한합니다. IBM MQ는 보안의 확장 레벨을 제공하기 위해 스위트 B를 준수하여 작동하도록 구성 가능합니다. 스위트 B에 대한 추가 정보는 18 페이지의 『NSA(National Security Agency) 스위트 B 암호화』의 내용을 참조하십시오. 스위트 B 구성 및 TLS 채널의 효과에 대한 자세한 정보는 36 페이지의 『IBM MQ에서의 NSA 스위트 B Cryptography』의 내용을 참조하십시오.

큐 관리자

큐 관리자에 대해 **SUITEB** 매개변수를 지정한 **ALTER QMGR** 명령을 사용하여 필수 보안 레벨에 적합한 값을 설정하십시오. 추가 정보는 **ALTER QMGR**를 참조하십시오.

MQIA_SUITE_B_STRENGTH 매개변수를 지정하여 **PCF MQCMD_CHANGE_Q_MGR** 명령을 사용하여 스위트 B 준수 조작을 위한 큐 관리자를 구성할 수도 있습니다.

참고: 큐 관리자 스위트 B 설정을 대체하는 경우, MQXR 서비스를 해당 설정이 적용되도록 재시작해야 합니다.

MQI 클라이언트

기본적으로 MQI 클라이언트는 스위트 B 준수를 강제 적용하지 않습니다. 다음 옵션 중 하나를 실행하여 스위트 B 준수를 위해 MQI 클라이언트를 사용할 수 있습니다.

1. MQCONNX 호출에서 MQSCO 구조에 **EncryptionPolicySuiteB** 필드를 다음 값 중 하나 이상으로 설정.

- MQ_SUITE_B_NONE
- MQ_SUITE_B_128_BIT
- MQ_SUITE_B_192_BIT

다음 값이 포함된 MQ_SUITE_B_NONE 사용은 올바르지 않습니다.

2. MQSUITEB 환경 변수를 다음 값 중 하나 이상으로 설정:

- NONE
- 128_BIT
- 192_BIT

쉼표로 구분된 목록을 사용하여 여러 개의 값을 지정할 수 있습니다. 다른 값이 포함된 NONE 값 사용은 올바르지 않습니다.

3. 다음 값 중 하나 이상의 값으로 MQI 클라이언트 구성 파일의 SSL 스탠자에 **EncryptionPolicySuiteB** 속성 설정:

- NONE
- 128_BIT
- 192_BIT

쉼표로 구분된 목록을 사용하여 여러 개의 값을 지정할 수 있습니다. 어떠한 다른 값이 포함된 NONE 사용도 올바르지 않습니다.

참고: MQI 클라이언트 설정은 우선순위대로 나열됩니다. MQCONNX 호출의 MSCO 구조는 MQSUITEB 환경 변수의 설정을 대체하며 이는 SSL 스탠자 속성을 대체합니다.

MQSCO 구조의 전체 설명은 **MQSCO - SSL 구성 옵션**을 참조하십시오.

클라이언트 구성 파일에서 스위트 B를 사용하는 자세한 정보는 **클라이언트 구성 파일의 SSL 스탠자**를 참조하십시오.

MQSUITEB 환경 변수 사용에 대한 자세한 정보는 **환경 변수 설명**을 참조하십시오.

.NET

.NET 비관리 클라이언트에 대해 **MQC. ENCRYPTION_POLICY_SUITE_B** 특성은 필요한 스위트 B 보안 유형을 나타냅니다.

IBM MQ classes for .NET에서 스위트 B 사용에 대한 자세한 정보는 [MQEnvironment.NET](#) 클래스를 참조하십시오.

AMQP

큐 관리자에 대한 스위트 B 속성 설정은 해당 큐 관리자의 AMQP 채널에 적용됩니다. 큐 관리자 스위트 B 설정을 수정하는 경우 채널의 AMQP 서비스를 재시작하여 변경사항을 적용해야 합니다.

IBM MQ의 인증서 유효성 검증 정책

인증서 유효성 검증 정책에서는 인증서 체인 유효성 검증이 업계 보안 표준을 엄격하게 준수하는 방법을 판별합니다.

인증서 유효성 검증 정책은 다음과 같이 플랫폼 및 환경에 따라 다릅니다.

- 모든 플랫폼의 Java 및 JMS 애플리케이션의 경우, 인증서 유효성 검증 정책은 JRE(Java Runtime Environment)의 JSSE 컴포넌트에 따라 다릅니다. 인증서 유효성 검증 정책에 대한 자세한 정보는 JRE에 대한 문서를 참조하십시오.
- IBM i 시스템의 경우 인증서 유효성 검증 정책은 운영 체제에서 제공하는 보안 소켓 라이브러리에 따라 다릅니다. 인증서 유효성 검증 정책에 대한 자세한 정보는 운영 체제에 대한 문서를 참조하십시오.
- z/OS 시스템의 경우 인증서 유효성 검증 정책은 운영 체제에서 제공하는 시스템 SSL 컴포넌트에 따라 다릅니다. 인증서 유효성 검증 정책에 대한 자세한 정보는 운영 체제에 대한 문서를 참조하십시오.
- UNIX, Linux, and Windows 시스템의 경우 인증서 유효성 검증 정책은 GSKit에서 제공되며 이는 구성 가능합니다. 두 개의 서로 다른 인증서 유효성 검증 정책이 지원됩니다.
 - 현재 IETF 인증서 유효성 검증 표준을 준수하지 않는 이전 디지털 인증서와의 최대 역호환성 및 상호 운용성에 사용되는 레거시 인증서 유효성 검증 정책. 이 정책은 기본 정책이라고도 합니다.
 - RFC 5280 표준을 시행하는 엄격한 표준 준수 인증서 유효성 검증 정책. 이 정책은 표준 정책이라고도 합니다.

UNIX, Linux, and Windows에서 인증서 유효성 검증 정책 구성 방법에 대한 정보는 39 페이지의 『IBM MQ에서 인증서 유효성 검증 정책 구성』의 내용을 참조하십시오. 기본 및 표준 인증서 유효성 검증 정책 사이의 차이점에 대한 자세한 정보는 [UNIX, Linux, and Windows에서 인증서 유효성 검증 및 신뢰 정책 디자인을 참조하십시오.](#)

IBM MQ에서 인증서 유효성 검증 정책 구성

네 가지 방법으로 원격 파트너 시스템에서 수신된 디지털 인증서를 유효성 검증하는 데 사용되는 TLS 인증서 유효성 검증 정책을 지정할 수 있습니다.

큐 관리자에서 인증서 유효성 검증 정책은 다음 방법으로 설정할 수 있습니다.

- 큐 관리자 속성 **CERTVPOL**을 사용. 이 속성을 설정하는 데 대한 자세한 정보는 [ALTER QMGR](#)을 참조하십시오.
- 클라이언트에서는 인증서 유효성 검증 정책을 설정하는 데 사용할 수 있는 몇 가지 방법이 있습니다. 정책을 설정하는 데 둘 이상의 방법이 사용되는 경우 클라이언트는 다음 우선순위에 따라 설정을 사용합니다.
1. 클라이언트 MQSCO 구조의 **CertificateValPolicy** 필드 사용. 이 필드를 사용하는 데 대한 자세한 정보는 [MQSCO - SSL 구성 옵션](#)을 참조하십시오.
 2. 클라이언트 환경 변수 **MQCERTVPOL** 사용. 이 변수를 사용하는 데 대한 자세한 정보는 [MQCERTVPOL](#)을 참조하십시오.
 3. 클라이언트 SSL 스탠자 성능 조정 매개변수 설정 **CertificateValPolicy** 사용. 이 설정을 사용하는 데 대한 자세한 정보는 [클라이언트 구성 파일의 SSL 스탠자의 내용을 참조하십시오.](#)

인증서 유효성 검증 정책에 대한 자세한 정보는 39 페이지의 『IBM MQ의 인증서 유효성 검증 정책』의 내용을 참조하십시오.

IBM MQ에서 디지털 인증서와 CipherSpec의 호환성

이 토픽은 IBM MQ에서 CipherSpec과 디지털 인증서 사이의 관계를 소개하여 보안 정책에 대해 적합한 CipherSpec 및 디지털 인증서를 선택하는 방법에 대한 정보를 제공합니다.

지원되는 CipherSpec 서브세트만 디지털 인증서의 지원되는 모든 유형에 사용할 수 있습니다. 따라서, 디지털 인증서에 대해 적합한 CipherSpec을 선택해야 합니다. 이와 유사하게 조직의 보안 정책에서 특정 CipherSpec을 사용하도록 요구하면 해당 CipherSpec에 대해 적합한 디지털 인증서를 확보해야 합니다.

MD5 디지털 서명 알고리즘 및 TLS 1.2

MD5 알고리즘을 사용하여 서명된 디지털 인증서는 TLS 1.2 프로토콜이 사용되는 경우 거부됩니다. 이제는 많은 암호 분석가가 MD5 알고리즘을 취약하다고 생각하고 사용을 권장하지 않기 때문입니다. TLS 1.2 프로토콜을 기반으로 하는 최신 CipherSpec을 사용하려면 디지털 인증서가 해당 디지털 서명에 MD5 알고리즘을 사용하지 않도록 해야 합니다. TLS 1.0 프로토콜을 사용하는 이전 CipherSpec은 이 제한사항으로 제한되지 않으며 MD5 디지털 서명의 인증서를 계속 사용할 수 있습니다.

특정 인증서에 대한 디지털 서명 알고리즘을 보기 위해서 **runmqakm** 명령을 사용할 수 있습니다.

```
runmqakm -cert -details -db key.kdb -pw password -label cert_label
```

여기서, *cert_label*은 표시하려는 디지털 서명 알고리즘의 인증서 레이블입니다. 자세한 내용은 [디지털 인증서 레이블](#)을 참조하십시오.

참고: **runmqckm**(iKeycmd) 및 **strmqikm**(iKeyman) GUI를 사용하여 디지털 서명 알고리즘 선택사항을 볼 수 있지만, **runmqakm** 도구에서는 더 넓은 범위를 제공합니다.

runmqakm 명령 실행은 지정한 서명 알고리즘 사용을 표시하는 출력을 작성합니다.

```
Label : ibmmqexample
Key Size : 1024
Version : X509 V3
Serial : 4e4e93f1
Issuer : CN=Old Certificate Authority,OU=Test,O=Example,C=US
Subject : CN=Example Queue Manager,OU=Test,O=Example,C=US
Not Before : August 19, 2011 5:48:49 PM GMT+01:00
Not After : August 18, 2012 5:48:49 PM GMT+01:00
Public Key
 30 81 9F 30 0D 06 09 2A 86 48 86 F7 0D 01 01 01
 05 00 03 81 8D 00 30 81 89 02 81 81 00 98 5A 7A
 F0 18 21 EE E4 8A 6E DE C8 01 4B 3A 1E 41 90 3D
 CE 01 3F E6 32 30 6C 23 59 F0 FE 78 6D C2 80 EF
 BC 83 54 7A EB 60 80 62 6B F1 52 FE 51 9D C1 61
 80 A5 1C D4 F0 76 C7 15 6D 1F 0D 4D 31 3E DC C6
 A9 20 84 6E 14 A1 46 7D 4C F5 79 4D 37 54 0A 3B
 A9 74 ED E7 8B 0F 80 31 63 1A 0B 20 A5 99 EE 0A
 30 A6 B6 8F 03 97 F6 99 DB 6A 58 89 7F 27 34 DE
 55 08 29 D8 A9 6B 46 E6 02 17 C3 13 D3 02 03 01
 00 01
Public Key Type : RSA (1.2.840.113549.1.1.1)
Fingerprint : SHA1 :
 09 4E 4F F2 1B CB C1 F4 4F 15 C9 2A F7 32 0A 82
 DA 45 92 9F
Fingerprint : MD5 :
 44 54 81 7C 58 68 08 3A 5D 75 96 40 D5 8C 7A CB
Fingerprint : SHA256 :
 3B 47 C6 E7 7B B0 FF 85 34 E7 48 BE 11 F2 D4 35
 B7 9A 79 53 2B 07 F5 E7 65 E8 F7 84 E0 2E 82 55
Signature Algorithm : MD5WithRSASignature (1.2.840.113549.1.1.4)
Value
 3B B9 56 E6 F2 77 94 69 5B 3F 17 EA 7B 19 D0 A2
 D7 10 38 F1 88 A4 44 1B 92 35 6F 3B ED 99 9B 3A
 A5 A4 FC 72 25 5A A9 E3 B1 96 88 FC 1E 9F 9B F1
 C5 E8 8E CF C4 8F 48 7B 0E A6 BB 13 AE 2B BD D8
 63 2C 03 38 EF DC 01 E1 1F 7A 6F FB 2F 65 74 D0
 FD 99 94 BA B2 3A D5 B4 89 6C C1 2B 43 6D E2 39
 66 6A 65 CB C3 C4 E2 CC F5 49 39 A3 8B 93 5A DD
 B0 21 0B A8 B2 59 5B 24 59 50 44 89 DC 78 19 51
Trust Status : Enabled
```


Signature Algorithm 행은 MD5WithRSASignature 알고리즘이 사용되는 것을 보여줍니다. 이 알고리즘은 MD5를 기반으로 하기 때문에 이 디지털 인증서는 TLS 1.2 CipherSpec과 같이 사용할 수 없습니다.

Elliptic Curve 및 RSA CipherSpec의 상호 운용성

V 9.1.4 모든 CipherSpec을 모든 디지털 인증서와 같이 사용할 수 있는 것은 아닙니다. CipherSpecs 은 CipherSpec 이름 접두부로 표시됩니다. CipherSpec 의 각 유형은 사용할 수 있는 디지털 인증서의 유형에 대해 서로 다른 제한사항을 부과합니다. 이 제한은 모든 IBM MQ TLS 연결에 적용되지만 특히 Elliptic Curve 암호 사용자에게 연관됩니다.

다음 표는 CipherSpec과 디지털 인증서 사이의 관계를 요약합니다.

유형	CipherSpec 이름 접두부	설명	필수 공개 키 유형	디지털 서명 암호화 알고리즘	보안 키 설정 매소드
1	ECDHE_ECDSA_	Elliptic Curve 공개 키, Elliptic Curve 보안 키, Elliptic Curve 디지털 서명 알고리즘을 사용하는 CipherSpec.	Elliptic Curve	ECDSA	ECDHE
2	ECDHE_RSA_	RSA 공개 키, Elliptic Curve 보안 키 및 RSA 디지털 서명 알고리즘을 사용하는 CipherSpec.	RSA	RSA	ECDHE
V 9.1.4 3	(모든 TLS 1.3 CipherSpecs)	CipherSpecs -Elliptic Curve 또는 RSA 공개 키, Elliptic Curve 비밀 키 및 Elliptic Curve 또는 RSA 디지털 서명 알고리즘을 사용합니다.	타원 곡선 또는 RSA	ECDSA 또는 RSA	ECDHE 또는 RSA
4	(나머지 모두)	RSA 공개 키 및 RSA 디지털 서명 알고리즘을 사용하는 CipherSpec.	RSA	RSA	RSA

참고: 유형 1 및 2 CipherSpec은 IBM MQ 큐 관리자 및 IBM i 플랫폼의 MQI 클라이언트에서는 지원되지 않습니다.

필수 공개 키 유형 열은 개인 인증서가 CipherSpec 각 유형 사용 시에 가져야 하는 공개 키 유형을 보여줍니다. 개인 인증서는 해당 원격 파트너에 대해 큐 관리자 또는 클라이언트를 식별하는 일반 엔티티 인증서입니다.

Elliptic Curve(EC) 인증서가 필요한 CipherSpec 및 RSA 인증서용 또는 다른 방식의 인증서 레이블 모두를 사용하여 채널을 구성할 수 있습니다. 인증서 레벨에 이름 지정된 인증서가 채널 CipherSpec에 적합해야 합니다.

올바르게 IBM MQ를 구성한 경우 다음을 수행할 수 있습니다.

- RSA 및 EC 인증서가 혼합된 단일 큐 관리자.
- RSA 또는 EC 인증서를 사용하여 동일한 큐 관리자에서 다른 채널.

디지털 서명 암호화 알고리즘은 피어 유효성 검증에 사용되는 암호화 알고리즘을 나타냅니다. 암호화 알고리즘은 디지털 서명을 처리하기 위해 MD5, SHA-1 또는 SHA-256과 같은 해시 알고리즘을 같이 사용합니다. 사용할 수 있는 디지털 서명 알고리즘은 다양합니다(예: MD5가 포함된 RSA 또는 SHA-256이 포함된 ECDSA). 이 표에서 ECDSA는 ECDSA를 사용하는 디지털 서명 알고리즘 세트를 나타내며 RSA는 RSA를 사용하는 디지털 서명 알고리즘의 세트를 나타냅니다. 세트에서 지원되는 모든 디지털 서명 알고리즘은 언급된 암호화 알고리즘을 기반으로 하는 경우 사용 가능합니다.

유형 1 CipherSpec의 경우 개인 인증서에 Elliptic Curve 공개 키가 필요합니다. 이 CipherSpec이 사용되는 경우 Elliptic Curve Diffie Hellman Ephemeral 키 계약이 연결에 대한 보안 키 설정에 사용됩니다.

유형 2 CipherSpec의 경우 개인 인증서가 RSA 공개 키를 포함해야 합니다. 이 CipherSpec이 사용되는 경우 Elliptic Curve Diffie Hellman Ephemeral 키 계약이 연결에 대한 보안 키 설정에 사용됩니다.

유형 3 CipherSpec의 경우 개인 인증서는 RSA 공개 키를 포함해야 합니다. 이 CipherSpec이 사용되는 경우 RSA 키 교환이 연결에 대한 보안 키 설정에 사용됩니다.

이 제한 목록은 완벽하지 않으며 구성에 따라 상호 운영하는 기능에 추가 영향을 줄 수 있는 추가 제한이 있을 수도 있습니다. 예를 들어, IBM MQ가 FIPS 140-2 또는 NSA 스위트 B 표준을 준수하도록 구성되는 경우 이는 허용 가능한 구성 범위도 제한합니다. 자세한 정보는 다음 절을 참조하십시오.

동일한 큐 관리자 또는 클라이언트 애플리케이션에서 CipherSpec의 다른 유형을 사용해야 하는 경우, 적절한 인증서 레이블 및 CipherSpec 결합을 클라이언트 정의에서 구성하십시오.

세 가지 유형의 CipherSpec은 직접 상호 운용되지 않으며 이는 현재 TLS 표준의 제한사항입니다. 예를 들어, 이름이 QM1인 큐 관리자에서 이름이 TO.QM1 인 수신자 채널에 대해 ECDHE_ECDSA_AES_128_CBC_SHA256 CipherSpec 를 사용하도록 선택했다고 가정하면 수신자는 Elliptic Curve키 및 ECDSA 기반 디지털 서명이 있는 개인 인증서를 가지고 있어야 합니다. 수신자 채널이 이러한 요구사항을 충족하지 않으면 채널이 시작되지 않습니다.

큐 관리자 QM1에 연결 중인 다른 채널은 다른 CipherSpec을 사용할 수 있으며 이는 해당 채널의 CipherSpec에 대해 올바른 유형의 인증서를 각 채널이 사용하는 경우에 해당합니다. 예를 들어, QM1이 TO.QM2 송신자 채널을 사용하여 메시지를 QM2의 다른 큐 관리자로 송신한다고 가정해 보십시오. 채널의 양쪽에서 RSA 공개 키를 포함하는 인증서를 사용하는 경우 채널 TO.QM2는 유형 3 CipherSpec TLS_RSA_WITH_AES_256_CBC_SHA256을 사용할 수 있습니다. 인증서 레이블 채널 속성은 각 채널에 대해 다른 인증서를 구성하는 데 사용할 수 있습니다.

IBM MQ 네트워크를 계획할 때는 TLS가 필요한 채널을 신중하게 고려하고 각 채널에 사용되는 인증서의 유형이 해당 채널에서 CipherSpec과 함께 사용하기에 적합한지 확인하십시오.

디지털 서명에 대한 디지털 서명 알고리즘 및 공개 키 유형을 확인하기 위해 `runmqakm` 명령을 사용할 수 있습니다.

```
runmqakm -cert -details -db key.kdb -pw password -label cert_label
```

여기서, `cert_label`은 표시해야 하는 디지털 서명 알고리즘의 인증서 레이블입니다. 자세한 내용은 [디지털 인증서 레이블](#)을 참조하십시오.

`runmqakm` 명령 실행은 공개 키 유형을 표시하는 출력을 작성합니다.

```
Label : ibmmqexample
Key Size : 384
Version : X509 V3
Serial : 9ad5eeef5d756f41
Issuer : CN=Example Certificate Authority,OU=Test,O=Example,C=US
Subject : CN=Example Queue Manager,OU=Test,O=Example,C=US
Not Before : 21 August 2011 13:10:24 GMT+01:00
Not After : 21 August 2012 13:10:24 GMT+01:00
Public Key
 30 76 30 10 06 07 2A 86 48 CE 3D 02 01 06 05 2B
 81 04 00 22 03 62 00 04 3E 6F A9 06 B6 C3 A0 11
 F8 D6 22 78 FE EF 0A FE 34 52 C0 8E AB 5E 81 73
 D0 97 3B AB D6 80 08 E7 31 E9 18 3F 6B DE 06 A7
 15 D6 9D 5B 6F 56 3B 7F 72 BB 6F 1E C9 45 1C 46
 60 BE F2 DC 1B AD AC EC 64 4C 0E 06 65 6E ED 93
 B8 F5 95 E0 F9 2A 05 D6 21 02 BD FB 06 63 A1 CC
 66 C6 8A 0A 5C 3F F7 D3
Public Key Type : EC_ecPublicKey (1.2.840.10045.2.1)
Fingerprint : SHA1 :
 3C 34 58 04 5B 63 5F 5C C9 7A E7 67 08 2B 84 43
 3D 43 7A 79
Fingerprint : MD5 :
 49 13 13 E1 B2 AC 18 9A 31 41 DC 8C B4 D6 06 68
Fingerprint : SHA256 :
 6F 76 78 68 F3 70 F1 53 CE 39 31 D9 05 C5 C5 9F
 F2 B8 EE 21 49 16 1D 90 64 6D AC EB 0C A7 74 17
Signature Algorithm : EC_ecdsa_with_SHA384 (1.2.840.10045.4.3.3)
Value
 30 65 02 30 0A B0 2F 72 39 9E 24 5A 22 FE AC 95
 0D 0C 6D 6C 2F B3 E7 81 F6 C1 36 1B 9A B0 6F 07
 59 2A A1 4C 02 13 7E DD 06 D6 FE 4B E4 03 BC B1
 AC 49 54 1E 02 31 00 90 0E 46 2B 04 37 EE 2C 5F
 1B 9C 69 E5 99 60 84 84 10 71 1A DA 63 88 33 E2
 22 CC E6 1A 4E F4 61 CC 51 F9 EE A0 8E F4 DC B5
 0B B9 72 58 C3 C7 A4
Trust Status : Enabled
```

이 경우 공개 키 유형 행은 인증서에 Elliptic Curve 공개 키가 있음을 보여줍니다. 이 경우 서명 알고리즘 행은 EC_ecdsa_with_SHA384 알고리즘이 사용 중임을 보여주며 이는 ECDSA 알고리즘을 기반으로 합니다. 따라서 이 인증서는 유형 1 CipherSpec 사용에만 적합합니다.

또한 동일한 매개변수로 **runmqckm** 명령을 사용할 수도 있습니다. 또한, **strmqikm** GUI는 키 저장소를 열고 인증서 레이블을 두 번 클릭하는 경우 디지털 서명 알고리즘 확인에 사용할 수도 있습니다. 그러나 **runmqakm** 도구를 사용하여 디지털 인증서를 확인해야 합니다. 이는 광범위한 범위의 알고리즘을 지원하기 때문입니다.

TLS 1.3 CipherSpecs

V 9.1.4

TLS 1.3 CipherSpecs 는 ECDSA 및 RSA 인증서를 모두 지원합니다.

Elliptic Curve CipherSpec 및 NSA 스위트 B

IBM MQ가 스위트 B 준수 TLS 1.2 프로파일을 준수하도록 구성되면 허용되는 CipherSpec 및 디지털 서명 알고리즘은 36 페이지의 『IBM MQ에서의 NSA 스위트 B Cryptography』에서 설명하는 대로 제한됩니다. 또한, 허용 가능한 Elliptic Curve 키 범위는 구성된 보안 레벨에 따라 줄어듭니다.

128비트 스위트 B 보안 레벨에서 인증서 제목 공개 키는 NIST P-256 또는 NIST P-384 Elliptic Curve를 사용하거나 NIST P-256 Elliptic Curve 또는 NIST P-384 Elliptic Curve로 서명되어야 합니다. **runmqakm** 명령은 EC_ecdsa_with_SHA256 또는 EC_ecdsa_with_SHA384의 -sig_alg 매개변수를 사용하여 이 보안 레벨에 대한 디지털 인증서를 요청하는 데 사용할 수 있습니다.

192비트 스위트 B 보안 레벨에서 인증서 주제 공개 키는 NIST P-384 Elliptic Curve를 사용하고 NIST P-384 Elliptic Curve로 서명되어야 합니다. **runmqakm** 명령은 EC_ecdsa_with_SHA384의 -sig_alg 매개변수를 사용하여 이 보안 레벨에 대한 디지털 인증서를 요청하는 데 사용할 수 있습니다.

지원되는 NIST Elliptic Curve는 다음과 같습니다.

표 5. 지원되는 NIST Elliptic Curve		
NIST FIPS 186-3 커브 이름	RFC 4492 커브 이름	Elliptic Curve 키 크기(비트)
P-256	secp256r1	256
P-384	secp384r1	384
P-521	secp521r1	521

참고: NIST P-521 Elliptic Curve는 스위트 B 준수 조작에 사용할 수 없습니다.

관련 개념

376 페이지의 『CipherSpec 사용 가능』

DEFINE CHANNEL MQSC 명령 또는 **ALTER CHANNEL** MQSC 명령에서 **SSLCIPH** 매개변수를 사용하여 CipherSpec을 사용 가능으로 설정하십시오.

241 페이지의 『MQI 클라이언트에서 런타임 시 FIPS 인증 CipherSpec만 사용하도록 지정』

FIPS 준수 소프트웨어를 사용하여 키 저장소를 작성한 다음 채널이 FIPS-인증 CipherSpec을 사용해야 함을 지정하십시오.

36 페이지의 『IBM MQ에서의 NSA 스위트 B Cryptography』

This topic provides information about how to configure IBM MQ on Windows, Linux, and UNIX to conform to the Suite B compliant TLS 1.2 profile.

18 페이지의 『NSA(National Security Agency) 스위트 B 암호화』

미 정부는 데이터 암호화를 포함한 IT 시스템 및 보안에 대한 기술 자문을 생성합니다. US NSA(National Security Agency)에서는 해당 스위트 B 표준에서 상호 운용 가능한 암호화 알고리즘 세트를 권장합니다.

채널 인증 레코드

채널 레벨에서 연결 시스템에 부여된 액세스 권한에 대한 보다 정밀한 제어를 실행하려면 채널 인증 레코드를 사용하십시오.

클라이언트가 바람직하지 않은 조치를 수행하도록 허용하는 공백 사용자 ID 또는 상위 레벨 사용자 ID를 사용해 사용자의 큐 관리자에 연결을 시도하는 것을 발견할 수 있습니다. 채널 인증 레코드를 사용해 이 클라이언트에 대한 액세스를 차단할 수 있습니다. 아니면, 클라이언트가 클라이언트 플랫폼에서는 올바르지만 서버 플랫폼에서는 알 수 없거나 올바르지 않은 형식인 사용자 ID를 사용할 수 있습니다. 채널 인증 레코드를 사용해 사용한 사용자 ID를 올바른 사용자 ID에 매핑할 수 있습니다.

사용자의 큐 관리자에 연결해 오류를 일으키는 클라이언트 애플리케이션이 발견될 수 있습니다. 이 애플리케이션이 일으키는 문제로부터 서버를 보호하려면 방화벽 규칙이 업데이트되거나 클라이언트 애플리케이션이 수정될 때까지 클라이언트 애플리케이션이 실행되고 있는 IP 주소를 사용해 일시적으로 차단해야 합니다. 채널 인증 레코드를 사용해 클라이언트 애플리케이션이 연결하는 IP 주소를 차단할 수 있습니다.

IBM MQ Explorer와 같은 관리 도구와 해당 용도의 채널을 설정했을 경우 특정 클라이언트 컴퓨터만 사용할 수 있도록 하고 싶을 수 있습니다. 채널 인증 레코드를 사용해 특정 IP 주소에서만 채널을 사용할 수 있게 만들 수 있습니다.

클라이언트로 실행 중인 일부 샘플 애플리케이션을 시작하는 경우 채널 인증 레코드를 사용하여 큐 관리자를 안전하게 설정하는 예로 [샘플 프로그램 준비 및 실행을 참조하십시오.](#)

채널 인증 레코드를 가져와서 인바운드 채널을 제어하려면 MQSC 명령 **ALTER QMGR CHLAUTH(ENABLED)**를 사용하십시오.

CHLAUTH 규칙은 새 인바운드 연결에 대한 응답으로 작성되는 채널 MCA에 적용됩니다. 로컬에서 시작되는 채널에 대한 응답으로 작성되는 채널 MCA의 경우 **CHLAUTH** 규칙이 적용되지 않습니다.

표 6. 서로 다른 채널 쌍에 대해 CHLAUTH 규칙이 적용되는 경우	
채널 유형	CHLAUTH 규칙이 적용되는 MCA
SDR-RCVR	RCVR
RQSTR-SVR(SVR에서 시작됨)	RQSTR
RQSTR-SVR(RQSTR에서 시작됨)	SVR
RQSTR-SDR(SDR에서 시작됨)	RQSTR
RQSTR-SDR(RQSTR에서 시작됨)	초기 연결을 위한 SDR. 콜백 연결의 경우 RQSTR.

다음 기능을 수행하도록 채널 인증 레코드를 작성할 수 있습니다.

- 특정 IP 주소로부터의 연결을 차단합니다.
- 특정 사용자 ID로부터의 연결을 차단합니다.
- 특정 IP 주소로부터 연결하는 모든 채널에 대해 사용하도록 MCAUSER 값을 설정합니다.
- 특정 사용자 ID를 이용하는 모든 채널에 대해 사용하도록 MCAUSER 값을 설정합니다.
- 특정 SSL 또는 TLS 식별 이름(DN)을 갖는 모든 채널에 대해 MCAUSER 값을 사용하도록 설정합니다.
- 특정 큐 관리자로부터 연결하는 모든 채널에 대해 사용하도록 MCAUSER 값을 설정합니다.
- 특정 IP 주소로부터의 연결이 아닌 경우 특정 큐 관리자로부터의 연결을 차단합니다.
- 특정 IP 주소로부터의 연결이 아닌 경우 특정 SSL 또는 TLS 인증서를 제시하는 연결을 차단합니다.

사용에 대해서는 다음 절에서 좀 더 자세히 설명합니다.

MQSC 명령 **SET CHLAUTH** 또는 PCF 명령 **Set Channel Authentication Record**를 사용하여 채널 인증 레코드를 작성, 수정 또는 제거합니다.

참고: 채널 인증 레코드 수가 많으면 큐 관리자의 성능에 부정적인 영향을 미칠 수 있습니다.

IP 주소 차단

특정 IP 주소로부터의 액세스를 차단하는 것은 일반적으로 방화벽의 역할입니다. 하지만 IBM MQ 시스템에 대한 액세스 권한이 없는 IP 주소로부터 연결 시도가 있어 방화벽을 업데이트하기 전에 일시적으로 주소를 차단해야 할 경우가 있습니다. 이러한 연결은 IBM MQ 채널에서 시도되는 것이 아니라 IBM MQ 리스너를 대상으로 하도록 잘못 구성된 다른 소켓 애플리케이션에서 시도되는 것입니다. 유형 BLOCKADDR의 채널 인증 레코드를 설정하

여 IP 주소를 차단하십시오. 한 개 이상의 주소, 일정 범위의 주소 또는 와일드카드를 포함한 패턴을 지정할 수 있습니다.

이 방식으로 IP 주소가 차단되어 인바운드 연결이 거부될 때마다 채널 이벤트가 사용 가능하며 큐 관리자가 실행 중인 경우, 이유 규정자가 MQRQ_CHANNEL_BLOCKED_ADDRESS인 이벤트 메시지 MQRQ_CHANNEL_BLOCKED가 발행됩니다. 또한 차단된 연결 시도가 반복되어 리스너에 해당 시도가 쇄도하지 않도록 오류를 리턴하기 전에 연결을 30초간 연 상태로 유지합니다.

특정 채널에서만 IP 주소를 차단하거나 오류를 리턴하기 전에 지연되지 않도록 하려면 USERSRC(NOACCESS) 매개변수를 사용하여 ADDRESSMAP 유형의 채널 인증 레코드를 설정하십시오.

이러한 이유로 인해 인바운드 연결이 거부되면 채널 이벤트가 사용 가능하며 큐 관리자가 실행 중인 경우 이유 규정자가 MQRQ_CHANNEL_BLOCKED_NOACCESS인 이벤트 메시지 MQRQ_CHANNEL_BLOCKED가 발행됩니다.

[344 페이지의 『특정 IP 주소 차단』](#)의 예를 참조하십시오.

사용자 ID 차단

특정 사용자 ID가 클라이언트 채널을 통해 연결하지 못하게 막으려면 BLOCKUSER 유형의 채널 인증 레코드를 설정하십시오. 이런 유형의 채널 인증 레코드는 클라이언트 채널에만 적용되며 메시지 채널에는 적용되지 않습니다. 한 개 이상의 개별 사용자 ID를 지정해 차단할 수 있지만 와일드카드는 사용할 수 없습니다.

이런 이유로 인바운드 연결이 거부되면 언제나 이벤트 메시지인 MQRQ_CHANNEL_BLOCKED가 이유 규정자인 MQRQ_CHANNEL_BLOCKED_USERID와 함께 발행됩니다. 단, 채널 이벤트가 사용 가능해야 합니다.

[345 페이지의 『특정 사용자 ID 차단』](#)의 예를 참조하십시오.

USERSRC(NOACCESS) 매개변수와 함께 USERMAP 유형의 채널 인증 레코드를 설정해 특정 채널에서 지정된 사용자 ID로부터의 액세스를 차단할 수도 있습니다.

이러한 이유로 인해 인바운드 연결이 거부되면 채널 이벤트가 사용 가능하며 큐 관리자가 실행 중인 경우 이유 규정자가 MQRQ_CHANNEL_BLOCKED_NOACCESS인 이벤트 메시지 MQRQ_CHANNEL_BLOCKED가 발행됩니다.

[348 페이지의 『클라이언트 사용자 ID에 대한 액세스 차단』](#)의 예를 참조하십시오.

큐 관리자 이름 차단

지정된 큐 관리자로부터 연결되는 임의의 채널이 액세스 권한을 갖지 않도록 지정하려면 채널 인증 레코드를 USERSRC(NOACCESS) 매개변수와 함께 QMGRMAP 유형으로 설정하십시오. 와일드카드가 포함된 패턴 또는 단일 큐 관리자 이름을 지정할 수 있습니다. 큐 관리자로부터의 액세스를 차단하는 BLOCKUSER 함수에 상응하는 것은 없습니다.

이러한 이유로 인해 인바운드 연결이 거부되면 채널 이벤트가 사용 가능하며 큐 관리자가 실행 중인 경우 이유 규정자가 MQRQ_CHANNEL_BLOCKED_NOACCESS인 이벤트 메시지 MQRQ_CHANNEL_BLOCKED가 발행됩니다.

[348 페이지의 『리모트 큐 관리자로부터의 액세스 차단』](#)의 예를 참조하십시오.

SSL 또는 TLS DN 차단

지정된 DN이 포함되어 있는 SSL 또는 TLS 개인 인증서를 제시하는 사용자가 액세스 권한을 갖지 않도록 지정하려면 USERSRC(NOACCESS) 매개변수와 함께 SSLPEERMAP 유형의 채널 인증 레코드를 설정하십시오. 와일드카드가 포함된 패턴 또는 단일 식별 이름을 지정할 수 있습니다. DN용 액세스를 차단하는 BLOCKUSER 함수에 상응하는 것은 없습니다.

이러한 이유로 인해 인바운드 연결이 거부되면 채널 이벤트가 사용 가능하며 큐 관리자가 실행 중인 경우 이유 규정자가 MQRQ_CHANNEL_BLOCKED_NOACCESS인 이벤트 메시지 MQRQ_CHANNEL_BLOCKED가 발행됩니다.

[349 페이지의 『SSL 또는 TLS 식별 이름의 액세스 차단』](#)의 예를 참조하십시오.

IP 주소를 사용할 사용자 ID에 맵핑

지정된 IP 주소로부터 연결되는 임의의 채널이 특정 MCAUSER를 사용하도록 지정하려면 채널 인증 레코드를 ADDRESSMAP 유형으로 설정하십시오. 와일드카드가 포함된 패턴 또는 단일 주소, 주소 범위를 지정할 수 있습니다.

포트 포워딩 장치, DMZ 세션 브레이크 또는 큐 관리자에 제시된 IP 주소를 변경하는 다른 설정을 사용한다면 IP 주소 맵핑이 꼭 사용하기에 적합하지는 않습니다.

349 페이지의 『MCAUSER 사용자 ID에 IP 주소 맵핑』의 예를 참조하십시오.

사용할 사용자 ID에 큐 관리자 이름 맵핑

지정된 큐 관리자로부터 연결되는 임의의 채널이 특정 MCAUSER를 사용하도록 지정하려면 채널 인증 레코드를 QMGRMAP 유형으로 설정하십시오. 와일드카드가 포함된 패턴 또는 단일 큐 관리자 이름을 지정할 수 있습니다.

346 페이지의 『MCAUSER 사용자 ID에 리모트 큐 관리자 맵핑』의 예를 참조하십시오.

클라이언트가 사용한 사용자 ID를 사용할 사용자 ID에 맵핑

IBM MQ MQI 클라이언트의 연결에 특정 사용자 ID가 사용될 경우 다른 지정된 MCAUSER를 사용하도록 지정하려면 USERMAP 유형의 채널 인증 레코드를 설정하십시오. 사용자 ID 맵핑에는 와일드카드를 사용하지 않습니다.

347 페이지의 『MCAUSER 사용자 ID에 클라이언트 사용자 ID 맵핑』의 예를 참조하십시오.

사용할 사용자 ID에 SSL 또는 TLS DN 맵핑

지정된 DN이 포함된 SSL/TLS 개인 인증서를 제시하는 임의의 사용자가 특정 MCAUSER를 사용하도록 지정하려면 채널 인증 레코드를 SSLPEERMAP 유형으로 설정하십시오. 와일드카드가 포함된 패턴 또는 단일 식별 이름을 지정할 수 있습니다.

347 페이지의 『MCAUSER 사용자 ID에 SSL 또는 TLS 식별 이름 맵핑』의 예를 참조하십시오.

IP 주소에 따라 큐 관리자, 클라이언트 또는 SSL/TLS DN 맵핑

경우에 따라서는 써드파티가 큐 관리자 이름을 속일 수도 있습니다. SSL이나 TLS 인증서 또는 핵심 데이터베이스 파일이 도난되거나 재사용될 수도 있습니다. 이러한 위험으로부터 보호하기 위해 특정 큐 관리자나 클라이언트로부터 연결하거나 특정 DN을 사용할 경우 지정된 IP 주소로부터 연결하도록 지정할 수 있습니다. USERMAP, QMGRMAP 또는 SSLPEERMAP 유형의 채널 인증 레코드를 설정하고 ADDRESS 매개변수를 사용하여 허용된 IP 주소 또는 IP 주소 패턴을 지정하십시오.

346 페이지의 『MCAUSER 사용자 ID에 리모트 큐 관리자 맵핑』의 예를 참조하십시오.

채널 인증 레코드 사이의 상호 작용

연결을 시도하는 채널이 둘 이상의 채널 인증 레코드와 일치하고 이 시도가 서로 정반대의 효과를 가질 수 있습니다. 예를 들어, 한 채널이 BLOCKUSER 채널 인증 레코드에 의해 차단되어 있는 사용자 ID를 사용하는데 다른 사용자 ID를 설정하는 SSLPEERMAP 레코드와 일치하는 SSL이나 TLS 인증서를 갖고 있을 수 있습니다. 게다가, 채널 인증 레코드가 와일드카드를 사용한다면 단일 IP 주소, 큐 관리자 이름 또는 SSL이나 TLS DN이 여러 개의 패턴과 일치할 수 있습니다. 예를 들어, IP 주소 192.0.2.6은 패턴 192.0.2.0-24, 192.0.2.* 및 192.0.*.6. 수행되는 조치는 다음과 같이 결정됩니다.

- 사용된 채널 인증 레코드는 다음과 같이 선택됩니다.
 - 채널 이름과 명확히 일치하는 채널 인증 레코드가 와일드카드를 사용하여 채널 이름과 일치하는 채널 인증 레코드보다 우선합니다.
 - SSL 또는 TLS DN을 사용하는 채널 인증 레코드가 사용자 ID, 큐 관리자 이름 또는 IP 주소를 사용하는 레코드보다 높은 우선순위를 갖습니다.
 - 사용자 ID 또는 큐 관리자 이름을 사용하는 채널 인증 레코드가 IP 주소를 사용하는 레코드에 비해 높은 우선순위를 갖습니다.
- 일치하는 채널 인증 레코드가 발견되었는데 MCAUSER를 지정하는 경우 이 MCAUSER가 채널에 지정됩니다.

- 일치하는 채널 인증 레코드가 발견되었는데 이 레코드가 해당 채널이 어떤 액세스 권한도 갖지 못하도록 지정하는 경우 *NOACCESS의 MCAUSER 값이 채널에 지정됩니다. 이 값은 보안 엑시트 프로그램에 의해 나중에 변경할 수 있습니다.
 - 일치하는 채널 인증 레코드가 발견되지 않거나 일치하는 채널 인증 레코드가 발견되었는데 이 레코드가 해당 채널의 사용자 ID를 사용하도록 지정하는 경우 MCAUSER 필드가 검사됩니다.
 - MCAUSER 필드가 공백이면 클라이언트 사용자 ID가 채널에 지정됩니다.
 - MCAUSER 필드가 공백이 아니면 채널에 지정됩니다.
 - 임의의 보안 엑시트 프로그램이 실행됩니다. 이 엑시트 프로그램은 채널 사용자 ID를 설정하거나 액세스를 차단하도록 판별합니다.
 - 연결이 차단되거나 MCAUSER가 *NOACCESS로 설정되면 채널이 종료됩니다.
 - 클라이언트 채널을 제외한 어떤 채널에 대해서도 연결이 차단되지 않을 경우 이전 단계에서 판별된 채널 사용자 ID를 차단된 사용자 목록에서 확인합니다.
 - 차단된 사용자 목록에 해당 사용자 ID가 있으면 채널이 종료됩니다.
 - 차단된 사용자 목록에 해당 사용자 ID가 없으면 채널이 실행됩니다.
- 여러 개의 채널 인증 레코드가 채널 이름, IP 주소, 호스트 이름, 큐 관리자 이름 또는 SSL/TLS DN과 일치할 경우 가장 구체적으로 일치하는 것이 사용됩니다. 일치로 간주되는 경우는 다음과 같습니다.
- 가장 구체적인 일치하는 다음과 같이 와일드카드 문자가 없는 이름입니다.
 - 채널 이름 A.B.C
 - IP 주소 192.0.2.6
 - hursley.ibm.com 의 호스트 이름
 - 큐 관리자 이름 192.0.2.6
 - 가장 일반적인 일치하는 다음과 일치하는 단일 별표(*)입니다.
 - 모든 채널 이름
 - 모든 IP 주소
 - 모든 호스트 이름
 - 모든 큐 관리자 이름
 - 문자열 시작 부분에 별표가 있는 패턴이 문자열 시작 부분에 정의된 값이 있는 패턴보다 일반적입니다.
 - 채널의 경우 *.B.C가 A.*보다 일반적입니다.
 - IP 주소의 경우 *.0.2.6이 192.*보다 일반적입니다.
 - 호스트 이름의 경우, *.ibm.com은(는) hursley.*보다 일반적입니다.
 - 큐 관리자 이름의 경우 *QUEUEMANAGER가 QUEUEMANAGER*보다 일반적입니다.
 - 문자열의 특정 위치에 별표가 있는 패턴이 문자열의 같은 위치에 정의된 값이 있는 패턴보다 일반적이며, 문자열의 이후 위치에 대해서도 마찬가지입니다.
 - 채널의 경우 A.*C가 A.B.*보다 일반적입니다.
 - IP 주소의 경우 192.*.2.6이 192.0.*보다 일반적입니다.
 - 호스트 이름의 경우, hursley.*.com은(는) hursley.ibm.*보다 일반적입니다.
 - 큐 관리자 이름의 경우 Q*MANAGER가 QUEUE*보다 일반적입니다.
 - 문자열의 특정 위치에 별표가 있는 패턴이 두 개 이상 있을 경우 별표 뒤의 노드 수가 적은 패턴이 더 일반적입니다.
 - 채널의 경우, A.* 는 A.*.C보다 일반적입니다.
 - IP 주소의 경우, 192.* 는 192.*.2.*보다 일반적입니다.
 - 호스트 이름의 경우, hursley.*은(는) hursley.*.com보다 일반적입니다.
 - 큐 관리자 이름의 경우 Q*가 Q*MGR보다 일반적입니다.
 - IP 주소의 경우:

- 하이픈(-)으로 표시된 범위는 별표보다 구체적입니다. 따라서, 192.0.2.0-24는 192.0.2.*보다 구체적입니다.
 - 다음 범위의 서브세트인 범위는 더 큰 범위보다 구체적입니다. 따라서, 192.0.2.5-15는 192.0.2.0-24보다 구체적입니다.
 - 겹치는 범위는 허용되지 않습니다. 예를 들어, 192.0.2.0-15와 192.0.2.10-20 모두를 위한 채널 인증 레코드를 가질 수 없습니다.
 - 패턴이 단일 후미 문자 별표로 끝나지 않는 한 패턴의 부분 개수는 필요한 부분 개수보다 적어선 안됩니다. 예를 들어, 192.0.2는 올바르지 않지만 192.0.2.*은 유효합니다.
 - 후미 문자 별표는 적절한 부분 구분 기호(IPv4의 경우 점(.), IPv6의 경우 콜론(:))로 나머지 주소와 구분해야 합니다. 예를 들어, 192.0.*는 별표가 구분되어 있지 않으므로 올바르지 않습니다.
 - 후미 별표에 인접한 별표가 없다면 패턴에 별표를 추가할 수 있습니다. 예를 들어, 192.*.2.*는 유효하지만 192.0.*.* 유효하지 않습니다.
 - IPv6 주소 패턴에 이중 콜론 및 후미 별표가 포함되면 주소가 모호해지기 때문에 이와 같이 사용할 수 없습니다. 예를 들어, 2001::.*는 2001:0000:.*, 2001:0000:0000:.* 등으로 확장될 수 있습니다.
- SSL이나 TLS 식별 이름(DN)의 경우 하위 문자열의 우선 순위는 다음과 같습니다.

표 7. 하위 문자열의 우선 순위		
순서	DN 하위 문자열	이름
1	SERIALNUMBER=	인증서 일련 번호
2	MAIL=	이메일 주소
3	E=	이메일 주소(MAIL보다 우선적으로 는 더 이상 사용되지 않음)
4	UID=, USERID=	사용자 ID
5	CN=	공용 이름
6	T =	제목
7	OU=	조직 단위
8	DC=	도메인 컴포넌트
9	오=	조직
10	STREET=	상세 주소/주소 두 번째 줄
11	L=	구/군/시
12	ST=, SP=, S=	시/도 이름
13	PC=	우편번호
14	C=	국가
15	UNSTRUCTUREDNAME=	호스트 이름
16	UNSTRUCTUREDADDRESS=	IP 주소
17	DNQ=	식별 이름 규정자

따라서, SSL 또는 TLS 인증서가 O=IBM 및 C=UK라는 하위 문자열이 포함된 DN과 함께 제시되면, IBM MQ는 C=UK 대신 O=IBM을 위한 채널 인증 레코드를 사용합니다(두 가지 모두 존재할 경우).

DN에는 여러 개의 OU가 포함될 수 있으며 이럴 경우 보다 큰 조직 단위를 먼저 지정하는 계층 구조로 OU를 지정해야 합니다. OU 값을 제외한 다른 모든 면에서 두 가지 DN이 동일하다면 보다 구체적인 DN은 다음과 같이 판별됩니다.

1. 다른 개수의 OU 속성을 갖고 있다면 가장 많은 OU 값을 가진 DN이 더 구체적입니다. 이는 더 많은 조직 단위를 가진 DN이 DN을 보다 자세하게 설명하고 더 많은 일치하는 기준을 제공하기 때문입니다. 최상위 레벨 OU가 와일드카드(OU=*)인 경우라도 OU가 더 많은 DN이 여전히 더 구체적인 것으로 간주됩니다.
2. OU 속성 개수가 동일할 경우 다음 규칙에 따라 좌우 순서로 해당되는 OU 값 쌍을 비교해 맨 왼쪽 OU가 최상위 레벨(가장 덜 구체적)이 됩니다.
 - a. 와일드카드 값이 없는 OU는 정확히 한 개의 문자열과만 일치할 수 있기 때문에 가장 구체적입니다.
 - b. 시작 또는 끝 부분에 한 개의 와일드카드가 있는 OU(예: OU=ABC* 또는 OU=*ABC)는 그 다음으로 가장 구체적입니다.
 - c. 와일드카드가 두 개인 OU(예: OU=*ABC*)가 그 다음으로 가장 구체적입니다.
 - d. 별표만으로 구성된 OU(OU=*)는 가장 덜 구체적입니다.
3. 상세도가 동일한 두 개의 속성 값 간에 문자열을 비교할 경우에는 어떤 쪽이든 더 긴 속성 문자열이 더 구체적입니다.
4. 문자열 비교가 상세도와 길이가 동일한 속성 값 두 개와 관련되어 있다면 결과는 DN의 와일드카드를 제외한 문자열 부분을 대소문자를 구분해 비교함으로써 판별됩니다.

두 개의 DN이 해당 DC 값을 제외하고 모든 면에서 동일하면 DC 값에서 가장 왼쪽의 DC가 최하위 레벨(가장 구체적)이라는 점을 제외하면 OU와 동일한 일치 규칙이 적용되고 비교 순서도 그에 따라 달라집니다.

채널 인증 레코드 표시

채널 인증 레코드를 표시하려면 MQSC 명령인 **DISPLAY CHLAUTH** 또는 PCF 명령인 **Inquire Channel Authentication Records**를 사용하십시오. 제공된 채널 이름과 일치하는 모든 레코드를 반환하거나 명확하게 일치하는 레코드를 선택할 수 있습니다. 명확한 일치하는 채널이 특정 IP 주소, 특정 큐 관리자로부터 연결을 시도하거나 특정 사용자 ID를 사용하여 연결을 시도할 경우 사용할 채널 인증 레코드를 알려주며 선택 사항으로서 지정된 DN이 포함된 SSL/TLS 개인 인증서를 제안합니다.

관련 개념

84 페이지의 『원격 메시징의 보안』

이 절에서는 원격 메시징 보안 측면을 다룹니다.

CHLAUTH와 CONNAUTH의 상호작용

채널의 단일 대화의 경우, IBM MQ에서 채널 인증 레코드(CHLAUTH) 및 연결 인증(CONNAUTH)이 상호작용하는 방법에 대해 설명합니다.

바인딩의 다른 유형

IBM MQ는 애플리케이션이 연결하는 두 가지 방법을 지원합니다.

로컬 바인딩

애플리케이션과 큐 관리자가 동일한 운영 이미지에 있을 때 적용됩니다. CHLAUTH는 이 유형의 애플리케이션 연결과 관련이 없습니다.

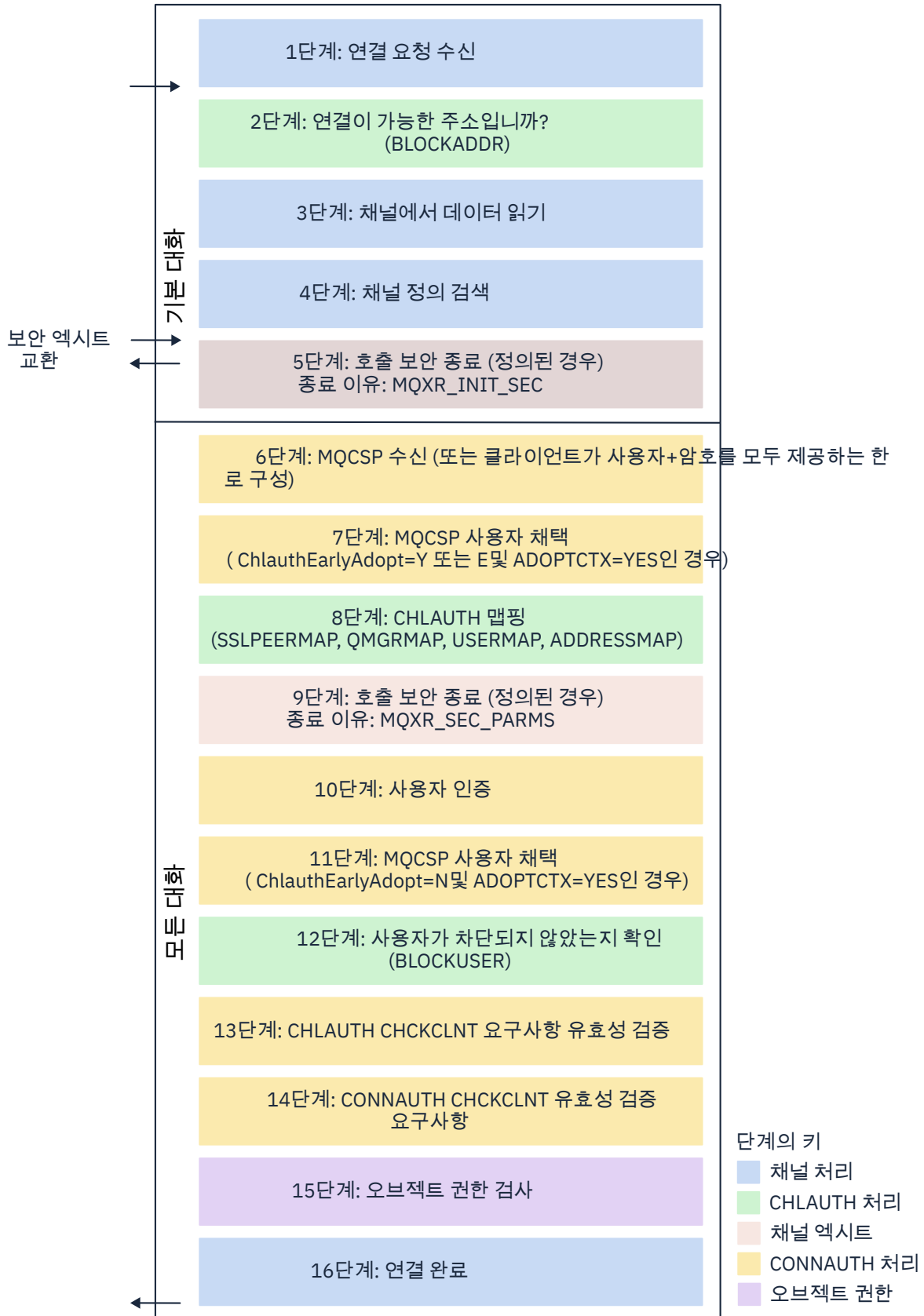
클라이언트 바인딩

애플리케이션과 큐 관리자가 통신하기 위해 네트워크를 사용할 때 적용됩니다. 애플리케이션과 큐 관리자는 동일한 시스템 또는 다른 시스템에서 실행될 수 있습니다. IBM MQ에서, 클라이언트 연결은 서버 연결(SVRCONN) 채널의 형태로 처리되며, 이 상황에서는 CONNAUTH와 CHLAUTH가 모두 적용됩니다.

채널 수신 측의 바인딩 단계

애플리케이션이 큐 관리자에 연결되면 상당한 양의 검사가 수행되어 채널의 양쪽 끝이 다른 쪽에서 지원하는 것을 이해할 수 있습니다. 채널의 수신 측은 CHLAUTH와 CONNAUTH를 포함하여 클라이언트가 연결될 수 있는지 확인하기 위해 추가 검사를 수행하며, 이 과정은 결과에 영향을 미칠 수 있으므로 보안 엑시트도 포함할 수 있습니다. 이 채널 접속 단계는 또한 결합 단계라고도 합니다.

다음 다이어그램은 서버 측(큐 관리자에서)이 시작될 때 SVRCONN 채널이 수행하는 단계를 나열합니다.



1단계: 연결 요청 수신

채널 시작기 또는 리스너는 네트워크의 임의 위치로부터 연결 요청을 수신합니다.

2단계: 연결이 가능한 주소입니까?

데이터를 읽기 전에 IBM MQ는 CHLAUTH 규칙에 대해 파트너의 IP 주소를 확인하여 주소가 *BLOCKADDR* 규칙에 있는지 검사합니다. 주소를 찾을 수 없는 경우, 차단하지 않으면 플로우는 다음 단계로 진행됩니다.

3단계: 채널에서 데이터 읽기

IBM MQ는 이제 데이터를 버퍼로 읽고, 송신 정보를 처리하기 시작합니다.

4단계: 채널 정의 검색

첫 번째 데이터 플로우에서, IBM MQ는 무엇보다도 송신 측이 시작하려고 하는 채널의 이름을 보냅니다. 수신 큐 관리자는 채널에 대해 지정된 모든 설정을 갖는 채널 정의를 검색할 수 있습니다.

5단계: 보안 엑시트 호출(정의된 경우)

채널에 보안 엑시트(SCYEXIT)가 정의되어 있으면 엑시트 이유(MQCXP.**ExitReason**)와 함께 호출됩니다. MQXR_INIT_SEC로 설정하십시오.

6단계: MQCSP 수신

필요한 경우, 클라이언트에서 사용자 ID와 비밀번호를 제공하는 한 구성합니다.

클라이언트가 호환 모드로 실행 중인 Java 또는 JMS 애플리케이션인 경우 클라이언트는 큐 관리자에 MQCSP 구조를 전달하지 않습니다. 대신, 애플리케이션이 사용자 ID 및 비밀번호를 제공한 경우에는 MQCSP 구조가 여기서 구성됩니다.

7단계: MQCSP 사용자 채택(ChlauthEarlyAdopt이(가) Y이고 ADOPTCTX=YES인 경우)

인증한 클라이언트가 확인한 사용자 ID입니다.

CONNAUTH가 확인된 식별 이름을 간략한 사용자 ID에 맵핑하는 데 LDAP을 사용하고 있는 경우에는 이 맵핑이 이 단계에서 이뤄집니다.

인증이 성공하면 이 사용자 ID가 채널에 의해 채택되며 CHLAUTH 맵핑 단계에서 사용됩니다.

참고: IBM MQ 9.0.4에서 **ChlauthEarlyAdopt= Y** 매개변수는 새 큐 관리자의 qm.ini 파일의 채널 스탠자에 자동으로 추가됩니다.

8단계: CHLAUTH 맵핑

맵핑 규칙 *SSLPEERMAP*, *USERMAP*, *QMGRMAP* 및 *ADDRESSMAP*을 찾기 위해 CHLAUTH 캐시가 다시 조사됩니다.

수신 채널과 가장 일치하는 규칙이 사용됩니다. 규칙에 **USERSRC(CHANNEL)** 또는 (*MAP*)이 있으면 채널이 바인딩을 지속합니다.

CHLAUTH 규칙이 **USERSRC(NOACCESS)**가 있는 규칙으로 평가되면 9단계에서 신임 정보가 유효한 사용자 ID 및 비밀번호로 대체되지 않는 경우 애플리케이션이 채널에 대한 연결을 차단합니다.

9단계: 보안 엑시트 호출(정의된 경우)

채널에 보안 엑시트(SCYEXIT)가 정의되어 있으면 엑시트 이유(MQCXP.**ExitReason**)와 함께 호출됩니다. MQXR_SEC_PARMS로 설정하십시오.

MQCSP에 대한 포인터는 MQCXP 구조의 **SecurityParms** 필드에 표시됩니다.

MQCSP 구조에는 사용자 ID(MQCSP.**CSPUserIdPtr**) 및 비밀번호(MQCSP.**CSPPasswordPtr**)에 대한 포인터가 있습니다.

엑시트에서 사용자 ID 및 비밀번호를 변경할 수 있습니다. 다음 예는 보안 엑시트가 감사 로그에 사용자 ID 및 비밀번호를 어떻게 기록하는지 보여줍니다.

```
if (pMQCXP -> ExitReason == MQXR_SEC_PARMS)
{
  /* It is not a good idea for security reasons to print out the user ID */
  /* and password but the following is shown for demonstration reasons */
  printf("User ID: %.*s Password: %.*s\n",
    pMQCXP -> SecurityParms -> CSPUserIdLength,
    pMQCXP -> SecurityParms -> CSPUserIdPtr,
    pMQCXP -> SecurityParms -> CSPPasswordLength,
    pMQCXP -> SecurityParms -> CSPPasswordPtr);
}
```

엑시트는 MQCXP에서 *MQXCC_CLOSE_CHANNEL*을 리턴하여 IBM MQ에 채널 닫기를 지시할 수 있습니다. **Exitresponse** 필드. 그렇지 않으면 채널 처리가 연결 인증 단계로 계속 진행됩니다.

참고: 확인된 사용자가 보안 엑시트에 의해 변경되는 경우에는 CHLAUTH 맵핑 규칙이 새 사용자에게 다시 적용되지 않습니다.

10단계: 사용자 인증

인증 단계는 큐 관리자에서 CONNAUTH가 사용으로 설정된 경우 발생합니다.

이를 확인하려면 MQSC 명령 'DISPLAY QMGR CONNAUTH'를 실행하십시오.

z/OS 다음 예제는 IBM MQ for z/OS에서 실행 중인 큐 관리자에서 **DISPLAY QMGR CONNAUTH** 명령의 출력을 보여줍니다.

```
CSQM201I !MQ25 CSQMDRTC DISPLAY QMGR DETAILS
QMNAME(MQ25)
CONNAUTH(SYSTEM.DEFAULT.AUTHINFO.IDPWOS)
  END QMGR DETAILS
CSQ9022I !MQ25 CSQMDRTC ' DISPLAY QMGR' NORMAL COMPLETION
```

Multi 다음 예제는 IBM MQ for Multiplatforms에서 실행 중인 큐 관리자에서 **'DISPLAY QMGR CONNAUTH'** 명령의 출력을 보여줍니다.

```
1 : DISPLAY QMGR CONNAUTH
AMQ8408: Display Queue Manager details.
  QMNAME(DEMO)
  CONNAUTH(SYSTEM.DEFAULT.AUTHINFO.IDPWOS)
```

CONNAUTH 값은 **AUTHINFO** IBM MQ 오브젝트의 이름입니다.

운영 체제 인증(**AUTHTYPE(IDPWOS)**)이 IBM MQ for Multiplatforms 및 IBM MQ for z/OS 모두에서 유효하므로 예제에서는 운영 체제 인증을 사용합니다.

z/OS 다음 예제는 IBM MQ for z/OS에서 실행 중인 큐 관리자에서 **AUTHTYPE(IDPWOS)**에 대해 제공된 기본 오브젝트를 보여줍니다.

```
CSQM293I !MQ25 CSQMDRTC 1 AUTHINFO FOUND MATCHING REQUEST CRITERIA
CSQM201I !MQ25 CSQMDRTC DISPLAY AUTHINFO DETAILS
AUTHINFO(SYSTEM.DEFAULT.AUTHINFO.IDPWOS)
AUTHTYPE(IDPWOS)
QSGDISP(QMGR)
ADOPTCTX(NO)
CHKCLNT(NONE)
CHKLOCL(OPTIONAL)
FAILDLAY(1)
DESCR( )
ALTDAT(2018-06-04)
ALTTIME(10.43.04)
  END AUTHINFO DETAILS
CSQ9022I !MQ25 CSQMDRTC ' DISPLAY AUTHINFO' NORMAL COMPLETION
```

Multi 다음 예제는 IBM MQ for Multiplatforms에서 실행 중인 큐 관리자에서 **AUTHTYPE(IDPWOS)**에 대해 제공된 기본 오브젝트를 보여줍니다.

```
1 : display authinfo(SYSTEM.DEFAULT.AUTHINFO.IDPWOS)
AMQ8566: Display authentication information details.
  AUTHINFO(SYSTEM.DEFAULT.AUTHINFO.IDPWOS)
  AUTHTYPE(IDPWOS)          ADOPTCTX(NO)
  DESCR( )                 CHKCLNT(REQDADM)
  CHKLOCL(OPTIONAL)       FAILDLAY(1)
  ALTDAT(2015-06-08)      ALTTIME(16.35.16)
```

AUTHINFO TYPE(IDPWOS)에는 **CHKCLNT**라는 속성이 있습니다. 값이 **REQUIRED**으로 변경되면 모든 클라이언트 애플리케이션은 유효한 사용자 ID 및 비밀번호를 제공해야 합니다.

사용자는 7단계에서 인증된 경우, MQCXP 구조의 **SecurityParms** 필드에 있는 사용자 또는 비밀번호가 9단계의 보안 엑시트에 의해 변경되지 않는 한 다시 인증 절차를 수행하지 않습니다.

11단계: MQCSP 사용자의 컨텍스트 채택(ChlauthEarlyAdopt=N 및 ADOPTCTX=YES인 경우)

채널이 MCAUSER에서 실행되는지 여부 또는 애플리케이션이 제공한 사용자 ID를 제어하는 ADOPTCTX 속성을 설정할 수 있습니다.

MQXCP 구조의 MQCSP 또는 SecurityParms 필드에서 확인된 사용자 ID가 성공적으로 인증되고 ADOPTCTX이(가) YES이면, MQXCP 구조의 SecurityParms 필드에 있는 사용자 또는 비밀번호를 9단계의 보안 엑시트를 통해 변경하지 않는 경우 7 및 8단계의 결과로 발생하는 사용자의 컨텍스트가 이 애플리케이션에 사용할 컨텍스트로 채택됩니다.

이 확인된 사용자 ID는 IBM MQ 자원을 사용하기 위한 권한 부여에 대해 확인된 사용자 ID입니다.

예를 들어, SVRCONN 채널에 MCAUSER가 설정되어 있지 않으며 클라이언트가 Linux 시스템의 'johndoe'에서 실행 중입니다. 애플리케이션이 MQCSP에서 'fred' 사용자를 지정하여 채널이 활성 MCAUSER로 'johndoe'과(와) 함께 실행을 시작합니다. CONNAUTH를 확인하고 나면 'fred' 사용자가 채택되고 채널이 활성 MCAUSER로 'fred'과(와) 함께 실행됩니다.

12단계: 사용자 차단 여부 검사(BLOCKUSER)

CONNAUTH 확인에 성공하면 CHLAUTH 캐시를 다시 검사하여 활성 MCAUSER이 BLOCKUSER 규칙에 따라 차단되었는지 확인합니다. 사용자가 차단된 경우, 채널은 종료됩니다.

Step13: CHLAUTH CHCKCLNT 요구사항 유효성 검증

8 단계에서 선택한 CHLAUTH 규칙이 추가로 REQUIRED 또는 REQDADM의 CHCKCLNT값을 지정하는 경우, 요구사항을 충족하기 위해 유효한 CONNAUTH 사용자 ID가 제공되었는지 확인하기 위해 유효성 검증이 수행됩니다.

- CHCKCLNT (REQUIRED) 가 설정된 경우 사용자는 7 또는 10단계에서 인증되어야 합니다. 그렇지 않으면 연결이 거부됩니다.
- CHCKCLNT (REQDADM) 가 설정된 경우, 이 연결이 권한이 있는 것으로 판별되면 7 또는 10 단계에서 사용자를 인증해야 합니다. 그렇지 않으면 연결이 거부됩니다.
- CHCKCLNT (ASQMGR) 가 설정되면, 이 단계는 생략된다.

참고사항:

1. CHCKCLNT (REQUIRED) 또는 CHCKCLNT (REQDADM) 가 설정되었지만 CONNAUTH를 큐 매니저에서 사용할 수 없는 경우, 구성의 충돌로 인해 MQRC_SECURITY_ERROR (2063) 리턴 코드와 함께 연결이 실패한다.
2. 사용자가 이 단계에서 다시 인증되지 않습니다.

14단계: CONNAUTH CHCKCLNT 요구조건의 유효성을 확인한다.

인증 단계는 큐 관리자에서 CONNAUTH가 사용으로 설정된 경우 발생합니다.

수신 연결에 대해 설정된 요구사항을 판별하기 위해 CONNAUTH CHCKCLNT값을 검사한다.

- CHCKCLNT (없음) 가 설정되면 이 단계를 건너뛴다.
- CHCKCLNT (OPTIONAL) 가 설정되면 이 단계는 생략된다.
- CHCKCLNT (REQUIRED) 가 설정된 경우 사용자가 7 또는 10단계에서 인증되었어야 합니다. 그렇지 않으면 연결이 거부됩니다.
- CHCKCLNT (REQDADM) 가 설정된 경우, 이 연결이 권한이 있는 것으로 판별되면 7 또는 10 단계에서 사용자를 인증해야 합니다. 그렇지 않으면 연결이 거부됩니다.

참고: 사용자가 이 단계에서 다시 인증되지 않습니다.

Multi 15단계: 오브젝트 권한 검사

활성 MCAUSER에 큐 관리자에 연결하기 위한 적절한 권한이 있는지 확인하기 위해 검사가 수행됩니다.

ULW 자세한 정보는 [오브젝트 권한 관리자의 내용을 참조하십시오.](#)

IBM i 자세한 정보는 [138 페이지의 『IBM i에서 오브젝트 권한 관리자』의 내용을 참조하십시오.](#)

16단계: 연결 완료

선행 단계를 완료하면, 연결이 완료됩니다.

관련 개념

[CONNAUTH](#)

큐 관리자는 제공된 사용자 ID와 비밀번호를 사용하여 사용자가 자원에 액세스할 권한이 있는지 확인하도록 구성될 수 있습니다.

관련 참조

[SET CHLAUTH](#)

[ALTER AUTHINFO](#)

CHLAUTH 액세스 문제 해결

채널 인증 레코드(CHLAUTH)를 사용할 때 특정 액세스 문제를 해결하는 방법에 대한 제안.

기본 CHLAUTH 규칙

CHLAUTH 처리를 위한 세 개의 기본 규칙이 있습니다.

- 모든 MQ-admin* 사용자가 모든 채널에 액세스하지 못함
- 모든 SYSTEM.*에 액세스할 수 없음.* 모든 사용자에게 의한 채널
- SYSTEM.ADMIN.SVRCONN 채널에 대한 액세스 허용(비 MQ-admin 사용자)

처음 두 개의 규칙은 모든 채널에 대한 액세스를 차단합니다. 세 번째 규칙은 더 구체적이고 채널이 SYSTEM.ADMIN.SVRCONN 채널인 경우 다른 두 채널보다 우선하여 해당 채널에 대한 액세스를 허용합니다.

공용 연결 오류

CHLAUTH 규칙은 채널을 시작할 수 있는지 여부를 결정하기 위해 사용되며, MCAUSER를 통해 다른 사용자 ID에 매핑을 허용합니다. 채널을 시작할 수 없는 경우 일반적으로 다음과 같은 오류가 발생합니다.

- RC 2035 MQRC_NOT_AUTHORIZED
- RC 2059 MQRC_Q_MGR_NOT_AVAILABLE
- AMQ4036 액세스가 허용되지 않음
- AMQ9776: 채널이 사용자 ID에 의해 차단됨
- AMQ9777: 채널이 차단됨
- MQJE001: MQException 발생함: 완료 코드 2, 이유 2035
- MQJE036: 큐 관리자가 연결 시도를 거부했음

액세스를 엄격하게 차단한 다음 CHLAUTH 규칙을 추가하여 누가 채널에 액세스하고 시작할 수 있는지 제어해야 합니다. 임시 조치로서 나열된 오류를 해결하려면 다음을 수행 할 수 있습니다.

- 54 페이지의 『CHLAUTH 규칙 사용 안함』
- 54 페이지의 『CHLAUTH 규칙 수정 또는 제거』

CHLAUTH 규칙 사용 안함

임시 조치로서 위의 오류를 해결하기 위해 CHLAUTH 규칙을 사용하지 않도록 설정할 수 있습니다. 규칙은 언제든지 다시 사용 가능하게 할 수 있으며 CHLAUTH 규칙을 사용 불가능하게 하면 연결 문제가 해결된다.

CHLAUTH 규칙을 사용 안함으로 설정하려면 다음 명령을 실행하십시오.

```
runmqsc: ALTER QMGR CHLAUTH (DISABLED)
```

또한 CHLAUTH를 WARN으로 설정하여 규칙 결과를 액세스하고 기록할 수 있다는 점에 주목하십시오.

CHLAUTH 규칙 수정 또는 제거

CHLAUTH 규칙 또는 규칙을 삭제하거나 수정하여 문제를 일으킬 수도 있습니다.

CHLAUTH 규칙을 수정하려면, ACTION(REPLACE)으로 SET CHLAUTH 명령을 사용합니다. 예를 들어, MQ-admin 사용자가 차단하지 않고 WARN으로 모든 채널에 액세스하지 못하게 하는 기본 규칙을 수정하려면 다음 명령을 실행하십시오.

```
runmqsc: SET CHLAUTH (*) TYPE (BLOCKUSER) USERLIST (*MQADMIN) WARN(YES)
ACTION (REPLACE)
```

CHLAUTH 규칙을 수정하려면, ACTION(REMOVE)으로 SET CHLAUTH 명령을 사용합니다. 예를 들어, 모든 MQ-admin 사용자가 모든 채널에 액세스하지 못하게 하는 기본 규칙을 삭제하려면 다음 명령을 실행합니다.

```
runmqsc: SET CHLAUTH (*) TYPE (BLOCKUSER) USERLIST (*MQADMIN) ACTION (REMOVE)
```

MATCH(RUNCHECK)를 사용하여 액세스 테스트

runmqsc에서 CHLAUTH 규칙의 MATCH(RUNCHECK) 옵션을 사용하여 CHLAUTH 규칙의 결과를 테스트할 수 있습니다. MATCH(RUNCHECK) 옵션은 해당 채널이 이 큐 관리자에 연결되는 경우 런타임 시에 특정 인바운드 채널이 일치하는 레코드를 리턴합니다. 다음을 제공해야 합니다.

- 채널 이름
- ADDRESS 속성
- SSLPEER 속성, 인바운드 채널이 SSL 또는 TLS를 사용하는 경우에만
- QMNAME, 인바운드 채널이 큐 관리자 채널인 경우 또는
- CLNTUSER 속성, 인바운드 채널이 클라이언트 채널인 경우

다음 예제는 기본 규칙이 있는 CHLAUTH 규칙에 따라 MQ-admin 사용자 johndoe가 CHAN1이라는 채널에 액세스하는 결과를 확인하십시오.

```
runmqsc: DISPLAY CHLAUTH (CHAN1) MATCH (RUNCHECK) CLNTUSER ('johndoe') ADDRESS
('192.168.1.138')
```

```
AMQ8878: Display channel authentication record details.
CHLAUTH(*) TYPE(BLOCKUSER)
USERLIST(*MQADMIN)
```

사용자 johndoe의 경우, *MQADMIN 사용자에게 대한 BLOCKUSER 규칙으로 인해 차단됩니다.

다음 예는 기본 규칙을 적용한 CHLAUTH 규칙이 MQ-admin 사용자가 아닌 사용자 alice가 되어 CHAN1이라는 채널에 액세스하는 지 확인합니다.

```
runmqsc: DISPLAY CHLAUTH (CHAN1) MATCH (RUNCHECK) CLNTUSER ('alice') ADDRESS
('192.168.1.138')
```

```
AMQ9783: Channel will run using MCAUSER('alice').
```

사용자 alice의 경우, 채널이 실행되고, 채널은 MCAUSER로 alice를 전달합니다. MCAUSER는 IBM MQ 오브젝트 권한을 확인하는 데 사용되는 사용자 ID입니다.

관련 참조

[SET CHLAUTH](#)

[DISPLAY CHLAUTH](#)

사용자를 위한 새 CHLAUTH 규칙 작성

사용자를 위한 일부 공용 시나리오 및 이를 이루기 위한 CHLAUTH 규칙 예제입니다.

이 주제는 다음 시나리오를 포함합니다.

- [56 페이지의 『특정 MQ-admin 사용자에게 대한 액세스 제어』](#)
- [56 페이지의 『특정 사용자 및 IBM MQ 클라이언트 애플리케이션에 대한 액세스 제어』](#)
- [57 페이지의 『해당 사용자의 인증서 DN\(식별 이름\)을 사용하여 특정 사용자에게 대한 액세스 제어』](#)

- 57 페이지의 『특정 사용자를 mqm 사용자에게 맵핑』

특정 MQ-admin 사용자에게 대한 액세스 제어

이 시나리오의 경우, 관리 관점, 즉 IBM MQ Explorer에서 연결하기 위해 전용으로 사용될 서버 연결 채널을 설정하십시오. 이 사용법을 위한 특정 채널이 있고 연결이 지정된 IP 주소 중 하나가 아닌 경우, 연결을 허용하려는 위치의 IP 주소를 정의하고 'mqm' ID에 대해 액세스를 차단합니다.

IBM MQ Explorer에 대한 SVRCONN 채널과 ADMIN.CHAN이라고 하는 MQ-admin 사용자를 작성하십시오.

```
runmqsc: DEFINE CHANNEL (ADMIN.CHAN) CHLTYPE (SVRCONN) TRPTYPE (TCP)
```

테스트의 경우, MQ-admin 그룹에 속한 사용자 정의와 그렇지 않은 사용자가 있는지 확인하십시오. 이 시나리오의 경우, mqadm은 MQ-admin 그룹에 있고 alice는 포함되어 있지 않습니다.

기본 CHLAUTH 규칙이 올바른 위치에 있습니다. 특정 사용자가 특정 IP 주소에서 MQ-admin으로 ADMIN.CHAN에 액세스할 수 있도록 허용하려면 세 개의 규칙을 추가하십시오.

- 주소에서 NOACCESS 설정
- *MQADMIN BLOCKUSER를 대체하는 사용자 nobody만 차단하도록 이 채널의 BLOCKUSER 설정
- 주소의 특정 서브넷에서 사용자 mqadm에 대한 액세스를 허용하고 mqadm 사용자 권한에 대해 맵핑

```
runmqsc:
SET CHLAUTH (ADMIN.CHAN) TYPE (ADDRESSMAP) ADDRESS ('*') USERSRC (NOACCESS)
SET CHLAUTH ('ADMIN.CHAN') TYPE (BLOCKUSER) +
DESCR ('Rule to override *MQADMIN blockuser on this channel') +
USERLIST ('nobody') ACTION (replace)
SET CHLAUTH ('ADMIN.CHAN') TYPE (USERMAP) +
CLNTUSER ('mqadm') USERSRC (MAP) MCAUSER ('mqadm') +
ADDRESS ('192.168.1.*') +
DESCR ('Allow mqadm as mqadm on local subnet') ACTION (ADD)
```

이 시점에서 사용자 mqadm은 지정된 IP 주소 범위에서, ADMIN.CHAN 채널을 액세스하고 시작할 수 있습니다.

언제든지 MATCH(RUNCHECK)를 실행하여 다음 명령의 결과를 볼 수 있습니다.

```
runmqsc:
DISPLAY CHLAUTH (ADMIN.CHAN) MATCH (RUNCHECK) CLNTUSER ('mqadm') ADDRESS
('192.168.1.138')
AMQ8878: Display channel authentication record details.
CHLAUTH(ADMIN.CHAN) TYPE (USERMAP)
ADDRESS(192.168.1.*) CLNTUSER(mqadm)
MCAUSER(mqadm)

DISPLAY CHLAUTH (ADMIN.CHAN) MATCH (RUNCHECK) CLNTUSER ('alice') ADDRESS
('192.168.1.138')
AMQ8878: Display channel authentication record details.
CHLAUTH(ADMIN.CHAN) TYPE (ADDRESSMAP)
ADDRESS(*) USERSRC (NOACCESS)
```

이 시점에서, CHLAUTH 레코드가 있는 사용자만 ADMIN.CHAN을 사용하여 액세스 할 수 있습니다.

특정 사용자 및 IBM MQ 클라이언트 애플리케이션에 대한 액세스 제어

이 시나리오의 경우, 올바른 IBM MQ 권한을 제공하기 위해 (setmqaut를 사용하여) 특정 사용자에게 대해 IBM MQ 권한을 설정해야 한다고 가정하면 기본 CHLAUTH 규칙이 적절합니다.

이 시나리오에서, 권한은 MQ-admin 사용자가 아닌 사용자 mqapp1에 대해 설정됩니다. 특정 애플리케이션과 특정 사용자가 사용할 SVRCONN 채널(APP1.CHAN)을 작성하십시오.

```
runmqsc: DEFINE CHANNEL (APP1.CHAN) CHLTYPE (SVRCONN) TRPTYPE (TCP)
```

적절한 위치의 기본 CHLAUTH 규칙으로 사용자 mqapp1은 APP1.CHAN 채널을 시작할 수 있습니다.

IBM MQ 클라이언트 애플리케이션에서 발생하는 사용자 ID는 IBM MQ 오브젝트 권한 확인에 사용됩니다. 이 경우, 'mqapp1' 사용자가 IBM MQ 클라이언트 애플리케이션을 실행하고 있다고 가정할 때 이는 IBM MQ 오브젝트 권한 확인에 사용됩니다. 그러므로, mqapp1이 애플리케이션에 필요한 IBM MQ 오브젝트에 접근할 수 있다면, 아무런 문제가 없으며, 그렇지 않을 경우 권한 오류가 발생합니다.

mqapp1 사용자 ID에 대한 특정 CHLAUTH 규칙을 생성하여 보안을 강화할 수 있지만, 기본 규칙에서 MQ-admin 그룹의 멤버는 이 채널에 액세스할 수 없습니다.

```
runmqsc:
SET CHLAUTH (APP1.CHAN) TYPE(ADDRESSMAP) ADDRESS('*') USERSRC(NOACCESS)
SET CHLAUTH('APP1.CHAN') TYPE(USERMAP) +
CLNTUSER('mqapp1') USERSRC(MAP) MCAUSER('mqapp1') +
DESCR('Allow mqapp1 as mqapp1 on local subnet') ACTION(ADD)
```

해당 사용자의 인증서 DN(식별 이름)을 사용하여 특정 사용자에게 대한 액세스 제어

이 시나리오의 경우 사용자는 큐 관리자에 플로우되는 인증서가 있어야 합니다. DN은 CHLAUTH 규칙의 [SSLPEER](#) 설정과 일치하며, SSLPEER는 와일드카드 문자를 사용할 수 있습니다.

일치하는 경우, 사용자는 IBM MQ 오브젝트 권한을 확인하기 위해 다른 MCAUSER에 매핑 될 수도 있습니다. MCAUSER 매핑은 IBM MQ 오브젝트 권한 관리자(OAM)에서 관리해야 하는 사용자 수를 최소화 할 수 있습니다.

사용중인 인증서가 있는 TLS 채널이 있으며 다음과 같은 규칙이 필요합니다.

- 특정 채널에 대한 모든 사용자 차단
- IBM MQ OAM 액세스에 대해 해당 사용자의 클라이언트를 사용하는 특정 SSLPEER이 있는 사용자만 허용하십시오.

```
.
# block all users on any IP address.
SET CHLAUTH('SSL1.SVRCONN') TYPE(ADDRESSMAP) ADDRESS('*')
USERSRC(NOACCESS) DESCR('block all') WARN(NO) ACTION(ADD)
.
# override - no MQM admin rule (allow mqm group /mqm admin users to
connect.
SET CHLAUTH('SSL1.SVRCONN') TYPE(BLOCKUSER) USERLIST('nobody')
DESCR('override no mqm admin rule') WARN(NO) ACTION(ADD)
.
# allow particular SSLPEER, use client id coming in from channel
SET CHLAUTH('SSL1.SVRCONN') TYPE(SSLPEERMAP)
SSLPEER('CN=JOHNDOE,O=IBM,C=US') USERSRC(CHANNEL) ACTION(ADD)
```

채널에 연결하는 클라이언트 사용자 ID는 IBM MQ 오브젝트의 IBM MQ OAM 권한에 사용되므로 사용자 ID는 적절한 IBM MQ 권한을 가져야 합니다.

원하는 경우 다음을 사용하여 다른 IBM MQ 사용자 ID에 매핑할 수 있습니다.

```
USERSRC(MAP) MCAUSER('mquser1')
```

instead of USERSRC (CHANNEL).

특정 사용자를 mqm 사용자에게 매핑

이는 56 페이지의 『[특정 MQ-admin 사용자에게 대한 액세스 제어](#)』에 추가 또는 수정입니다.

IBM MQ OAM에 IBM MQ 오브젝트 권한 설정이 있는 mqm 사용자 또는 MQ-admin 사용자 ID에 특정 사용자를 매핑하려면 다음 CHLAUTH 규칙을 추가하십시오.

```
runmqsc:
SET CHLAUTH('ADMIN.CHAN') TYPE(USERMAP) +
CLNTUSER('johndoe') USERSRC(MAP) MCAUSER('mqm') +
ADDRESS('192.168.1-100.*') +
DESCR('Allow johndoe as MQ-admin on local subnet') ACTION(ADD)
```

이는 특정 채널 ADMIN.CHAN을 위한 mqm 사용자에게 대해 johndoe 사용자를 허용하고 매핑합니다.

관련 개념

54 페이지의 『CHLAUTH 액세스 문제 해결』

채널 인증 레코드(CHLAUTH)를 사용할 때 특정 액세스 문제를 해결하는 방법에 대한 제안.

58 페이지의 『채널에 대한 새 CHLAUTH 규칙 작성』

사용자 고유의 CHLAUTH 규칙을 작성하는 데 도움을 주기 위해 채널에 대한 몇 가지 공통 시나리오 및 이를 이루기 위한 CHLAUTH 규칙 예제를 다음과 같이 제공합니다.

관련 참조

[SET CHLAUTH](#)

[DISPLAY CHLAUTH](#)

채널에 대한 새 CHLAUTH 규칙 작성

사용자 고유의 CHLAUTH 규칙을 작성하는 데 도움을 주기 위해 채널에 대한 몇 가지 공통 시나리오 및 이를 이루기 위한 CHLAUTH 규칙 예제를 다음과 같이 제공합니다.

이 주제는 다음 시나리오를 포함합니다.

- 58 페이지의 『특정 IP 주소 범위에서 특정 채널에 대한 액세스만 허용하십시오.』
- 58 페이지의 『특정 채널의 경우 모든 사용자를 차단하지만 특정 사용자가 연결할 수 있도록 허용하십시오.』
- 59 페이지의 『수신자 및 송신자 채널에 대해 CHLAUTH 사용』

특정 IP 주소 범위에서 특정 채널에 대한 액세스만 허용하십시오.

이 시나리오의 경우 다음과 같이 수행하십시오.

- 임의 위치에서 채널에 대한 액세스 없음 설정
- 특정 IP 주소 또는 주소 범위에서 액세스 허용

```
runmqsc:  
SET CHLAUTH('APP2.CHAN') TYPE(ADDRESSMAP) ADDRESS('*') USERSRC(NOACCESS)  
WARN(NO) ACTION(ADD)  
SET CHLAUTH('APP2.CHAN') TYPE(ADDRESSMAP) ADDRESS('9.95.100.1-5')  
USERSRC(MAP) MCAUSER('mqapp2') ACTION(ADD)
```

이것은 연결이 지정된 특정 IP 주소 범위로부터 오는 경우 APP2.CHAN 채널만 시작할 수 있도록 허용합니다.

MCAUSER로 연결하는 사용자는 mqapp2에 맵핑되며, 따라서 해당 사용자에게 대해 IBM MQ OAM 권한을 부여 받습니다.

특정 채널의 경우 모든 사용자를 차단하지만 특정 사용자가 연결할 수 있도록 허용하십시오.

이 시나리오의 경우, MY.SVRCONN 채널에 대한 액세스는 [기본 CHLAUTH 규칙](#)을 가지고 있습니다.

다음은 추가해야 합니다.

```
# block all users  
SET CHLAUTH('MY.SVRCONN') TYPE(ADDRESSMAP) ADDRESS('*') USERSRC(NOACCESS)  
DESCR('block all') WARN(NO) ACTION(ADD)  
  
# override - no MQM admin rule  
SET CHLAUTH('MY.SVRCONN') TYPE(BLOCKUSER) USERLIST('nobody') DESCR('override  
no mqm admin rule') WARN(NO) ACTION(ADD)  
  
# allow johndoe userid  
SET CHLAUTH('MY.SVRCONN') TYPE(USERMAP) CLNTUSER('johndoe')  
USERSRC(CHANNEL) DESCR('allow johndoe userid') ACTION(ADD)
```

이 코드의 첫 부분은 모든 사용자의 MY.SVRCONN에 대한 연결을 차단한 다음, 특정 사용자 ID johndoe에서 연결이 이루어질 때 MY.SVRCONN 채널만 시작할 수 있도록 허용합니다.

johndoe 채널에 연결하는 사용자는 IBM MQ 오브젝트의 IBM MQ OAM 권한에 사용됩니다. 그러므로 사용자 ID는 적절한 IBM MQ 권한이 있어야 합니다.

원하는 경우 다음을 사용하여 다른 IBM MQ 사용자 ID에 맵핑할 수 있습니다.

```
USERSRC(MAP) MCAUSER('mquser1')
```

instead of USERSRC(CHANNEL).

수신자 및 송신자 채널에 대해 CHLAUTH 사용

CHLAUTH 규칙을 사용하여 수신자 채널에 대한 액세스를 제한하려면 수신자 및 송신자 채널에 추가 보안을 추가할 수 있습니다. CHLAUTH 규칙을 추가하거나 변경하는 경우, 업데이트된 CHLAUTH 규칙은 채널을 시작할 때만 적용되므로 채널이 이미 실행중인 경우, CHLAUTH 업데이트를 적용하려면 중지하고 다시 시작해야 합니다.

CHLAUTH 규칙은 모든 채널에 사용될 수 있지만 일부 제한이 있습니다. 예를 들면, USERMAP 규칙은 SVRCONN 채널에만 적용됩니다.

이 예는 TO.MYSVR1 채널을 시작하기 위해 특정 IP 주소로에서의 연결만 허용합니다.

```
# First you could lock down the channel by disallowing all
# for channel 'TO.MYSVR1', RCVR channel
SET CHLAUTH('TO.MYSVR1') TYPE(ADDRESSMAP) ADDRESS('*') USERSRC(NOACCESS)
DESCR('Back-stop rule')

# Then you could allow this channel to be started
SET CHLAUTH('TO.MYSVR1') TYPE(ADDRESSMAP) ADDRESS('192.168.1.134') USERSRC(MAP)
MCAUSER('mqapp') ACTION(ADD)
```

이 예는 특정 큐 관리자만 연결을 허용합니다.

```
# Lock down all access:
SET CHLAUTH('TO.MYSVR1') TYPE(ADDRESSMAP) ADDRESS('*') USERSRC(NOACCESS)
DESCR('Back-stop rule')

# Then allow access from queue manager MYSVR2 and from a particular ipaddress:
SET CHLAUTH('TO.MYSVR1') TYPE(QMGRMAP) QMNAME('MYSVR2') USERSRC(MAP)
MCAUSER('mqapp') ADDRESS('192.168.1.134') ACTION(ADD)
```

관련 개념

[54 페이지의 『CHLAUTH 액세스 문제 해결』](#)

채널 인증 레코드(CHLAUTH)를 사용할 때 특정 액세스 문제를 해결하는 방법에 대한 제안.

[55 페이지의 『사용자를 위한 새 CHLAUTH 규칙 작성』](#)

사용자를 위한 일부 공용 시나리오 및 이를 이루기 위한 CHLAUTH 규칙 예제입니다.

관련 참조

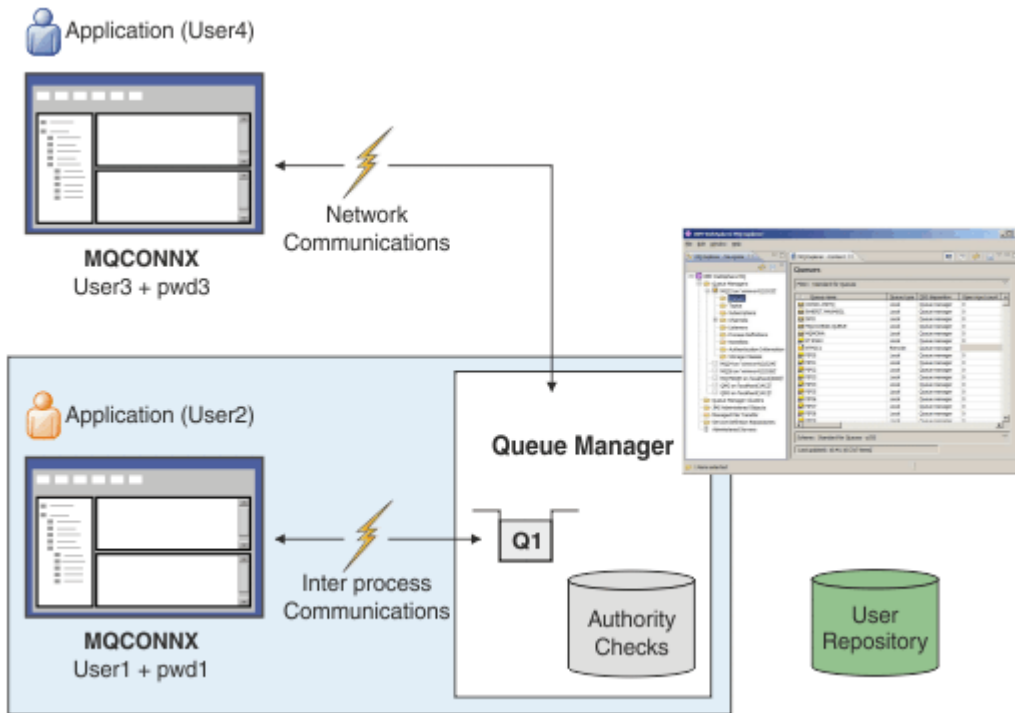
[SET CHLAUTH](#)

[DISPLAY CHLAUTH](#)

연결 인증

연결 인증은 다양한 방법으로 달성될 수 있습니다.

- 애플리케이션은 사용자 ID와 비밀번호를 제공할 수 있습니다. 애플리케이션은 각각 클라이언트이거나, 로컬 바인딩을 사용할 수 있습니다.
- 큐 관리자는 제공된 사용자 ID 및 비밀번호에 따라 작동하도록 구성될 수 있습니다.
- 저장소는 사용자 ID 및 비밀번호 결합이 유효한지 여부를 판별하기 위해 사용할 수 있습니다.



다이어그램에서 하나의 애플리케이션은 클라이언트로서, 또 하나의 애플리케이션은 로컬 바인딩을 사용하여 총 두 개의 애플리케이션이 큐 관리자와 연결합니다. 애플리케이션은 다양한 API를 사용하여 큐 관리자에 연결할 수도 있지만 모두 사용자 ID와 비밀번호를 제공할 수 있는 기능이 있습니다. 다이어그램에서 애플리케이션을 실행 중인 사용자 ID인 User2 및 User4은 IBM MQ에 제공되는 일반적인 운영 체제 사용자 ID이고, 애플리케이션이 제공하는 사용자 ID인 User1 및 User3와는 다를 수도 있습니다.

큐 관리자는 구성 명령(다이어그램에서 IBM MQ Explorer가 사용 중임)을 수신하고 자원의 열기를 관리하고 이러한 자원에 액세스하기 위한 권한을 검사합니다. IBM MQ에는 애플리케이션이 액세스할 권한을 필요로 할 수 있는 여러 가지 자원이 있습니다. 다이어그램은 출력을 위한 큐 열기를 보여주지만 동일한 원리가 또 다른 자원에도 적용됩니다.

사용자 ID 및 비밀번호 검사에 사용되는 저장소에 대한 자세한 정보는 [사용자 저장소를 참조하십시오](#).

관련 개념

60 페이지의 『연결 인증: 구성』

큐 관리자는 제공된 사용자 ID와 비밀번호를 사용하여 사용자가 자원에 액세스할 권한이 있는지 확인하도록 구성될 수 있습니다.

64 페이지의 『연결 인증: 애플리케이션 변경사항』

65 페이지의 『연결 인증: 사용자 저장소』

각 큐 관리자에 대해 사용자 ID 및 비밀번호를 인증하기 위해 서로 다른 유형의 인증 정보 오브젝트를 선택할 수 있습니다.

연결 인증: 구성

큐 관리자는 제공된 사용자 ID와 비밀번호를 사용하여 사용자가 자원에 액세스할 권한이 있는지 확인하도록 구성될 수 있습니다.

큐 관리자에서 연결 인증 켜기

큐 관리자 오브젝트에서 **CONNAUTH** 속성은 인증 정보(AUTHINFO) 오브젝트의 이름으로 설정될 수 있습니다. 이 오브젝트는 두 가지 유형 중 하나일 수 있습니다(AUTHTYPE 속성):

IDPWOS

큐 관리자가 로컬 운영 체제를 사용하여 사용자 ID와 비밀번호를 인증함을 표시합니다.

IDPWLDAP

큐 관리자가 LDAP 서버를 사용하여 사용자 ID와 비밀번호를 인증하는 것을 나타냅니다.

참고: CONNAUTH 필드에서는 다른 유형의 인증 정보 오브젝트를 사용할 수 없습니다.

IDPWOS와 IDPWLDAP는 여기에 설명된 여러 속성과 비슷합니다. 다른 속성은 나중에 고려합니다.

로컬 연결을 확인하려면 AUTHINFO 속성 **CHCKLOCL**(로컬 연결 확인)을 사용하십시오. 클라이언트 연결을 확인하려면 AUTHINFO 속성 **CHCKCLNT**(클라이언트 연결 확인)를 사용하십시오. 큐 관리자가 변경을 인식하기 전에 구성을 새로 고쳐야 합니다.

```
ALTER QMGR CONNAUTH(USE.PW)
DEFINE AUTHINFO(USE.PW) +
  AUTHTYPE(IDPWOS) +
  FAILDLAY(10) +
  CHCKLOCL(OPTIONAL) +
  CHCKCLNT(REQUIRED)
REFRESH SECURITY TYPE(CONNAUTH)
```

여기서 CONNAUTH의 USE.PW는 AUTHINFO 정의와 일치하는 문자열입니다.

CHCKLOCL과 **CHCKCLNT**에는 다양한 정확도로 검사를 수행할 수 있게 하는 동일한 세트의 값이 있습니다.

NONE

검사를 끕니다.

OPTIONAL

애플리케이션에서 사용자 ID와 비밀번호를 제공하며, 올바른 쌍인지를 확인하지만 반드시 제공할 필요는 없습니다. 이 옵션은 마이그레이션 등의 경우에 유용할 수 있습니다.


중요사항: OPTIONAL은 보다 엄중한 CHLAUTH 규칙을 사용하기 위해 설정할 수 있는 최소값입니다.

NONE 을 선택하고 클라이언트 연결이 CHCKCLNT REQUIRED (또는 z/OS이외의 플랫폼에서 REQDADM) 가 있는 CHLAUTH 레코드와 일치하는 경우, 연결이 실패합니다. z/OS 이외의 플랫폼에서 AMQ9793 메시지를 수신하고, z/OS에서 CSQX793E 메시지를 수신합니다.

REQUIRED

모든 애플리케이션에서 올바른 사용자 ID와 비밀번호를 제공해야 합니다. 다음 참고사항도 참조하십시오.

REQDADM

권한이 있는 사용자는 올바른 사용자 ID와 비밀번호를 제공해야 하지만 권한이 없는 사용자는 선택적 (OPTIONAL) 설정에서와 같이 처리됩니다. 다음 참고사항도 참조하십시오.  (이 설정은 z/OS 시스템에서는 사용할 수 없습니다.)

참고:

CHCKLOCL을 REQUIRED 또는 REQDADM으로 설정하면 사용자가 **runmqsc** 명령행에 -u UserId 매개변수를 지정하지 않는 경우 **runmqsc**(오류 AMQ8135: 인증되지 않음)를 사용하여 로컬에서 큐 관리자를 관리할 수 없습니다. 이와 같이 설정된 경우 **runmqsc**는 콘솔에서 사용자의 비밀번호를 입력하도록 프롬프트합니다.

마찬가지로 로컬 시스템에서 IBM MQ 탐색기를 실행하는 사용자가 큐 관리자에 연결하려고 하면 AMQ4036 오류가 표시됩니다. 사용자 이름 및 비밀번호를 지정하려면 로컬 큐 관리자 오브젝트를 마우스 오른쪽 단추로 클릭하고 **연결 세부사항 > 특성 ...** 을 선택하십시오. 선택하십시오. **사용자 ID** 절에서 사용할 사용자 이름과 비밀번호를 입력한 다음 **확인**을 클릭하십시오.

CHCKCLNT를 사용하는 원격 연결에도 비슷한 고려사항이 적용됩니다.

CONNAUTH는 마이그레이션된 큐 관리자에 대해서는 공백이지만 새 큐 관리자를 위해 **SYSTEM.DEFAULT.AUTHINFO.IDPWOS**로 설정됩니다. 앞의 **AUTHINFO** 정의에는 기본적으로 **REQDADM**으로 설정된 **CHCKCLNT**가 있습니다.

그러므로 연결하기 위해 권한이 있는 사용자 ID를 사용하여 기존 클라이언트에 대한 올바른 운영 체제 비밀번호를 제공해야 합니다.

경고: 일부 경우에 클라이언트 애플리케이션에 대한 MQCSP 구조의 비밀번호는 일반 텍스트로 네트워크 전체에 전송됩니다. 클라이언트 애플리케이션 비밀번호가 적절하게 보호될 수 있도록 하려면 26 페이지의 『MQCSP 비밀번호 보호』의 내용을 참조하십시오.

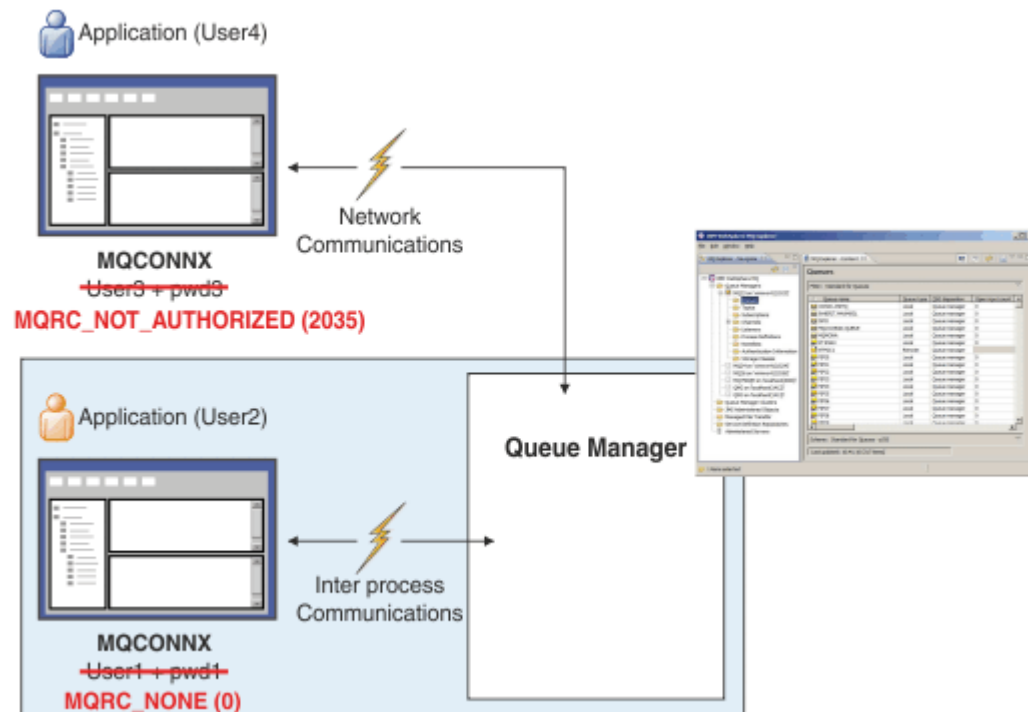
구성 세분화

사용자 ID 및 비밀번호 검사를 켜는 데 사용하는 **CHKLOCL** 및 **CHKCLNT** 외에도 **CHKCLNT**를 사용하여 더욱 구체적으로 구성할 수 있도록 CHLAUTH 규칙이 향상되었습니다.

예를 들어, 전체 **CHKCLNT** 값을 OPTIONAL로 설정한 다음 CHLAUTH 규칙에서 **CHKCLNT**를 REQUIRED 또는 REQDADM로 설정하여 이를 특정 채널을 위해 보다 엄격하게 업그레이드할 수 있습니다. 기본적으로 CHLAUTH 규칙은 CHKCLNT(ASQMGR)로 실행할 수 있지만 이 세분화는 사용하지 않아도 됩니다. 예를 들면, 다음과 같습니다.

```
DEFINE AUTHINFO(USE.PW) AUTHTYPE(XXXXXX) +
CHKCLNT(OPTIONAL)
SET CHLAUTH('*') TYPE(ADDRESSMAP) +
ADDRESS('*') USERSRC(CHANNEL) +
CHKCLNT(REQUIRED)
SET CHLAUTH('*') TYPE(SSLPEERMAP) +
SSLPEER('CN=*') USERSRC(CHANNEL)
```

오류 알림



애플리케이션에서 사용자 ID와 비밀번호를 제공하지 않거나(필수인 경우) 올바르지 않은 조합을 제공하는 경우(선택사항인 경우) 오류가 기록됩니다.

참고: **CHKLOCL** 또는 **CHKCLNT**에서 NONE 옵션을 사용하여 비밀번호 검사를 끄면 올바르지 않은 비밀번호가 감지되지 않습니다.

애플리케이션에 오류를 리턴하기 전에 **FAILDLAY** 속성에 지정된 시간(초) 동안 실패한 인증이 보류됩니다. 그러면 애플리케이션이 반복적으로 연결을 시도하지 않도록 보호합니다.

오류는 다음과 같은 여러 방식으로 기록됩니다.

애플리케이션

애플리케이션에는 표준 IBM MQ 보안 오류, RC2035 - MQRN_NOT_AUTHORIZED가 리턴됩니다.

관리자

IBM MQ 관리자는 오류 로그에 보고된 이벤트를 확인하므로 예를 들어, 연결 권한이 없기 때문이 아니라 사용자 및 비밀번호 검사에 실패했기 때문에 애플리케이션이 거부되었음을 알게 됩니다.

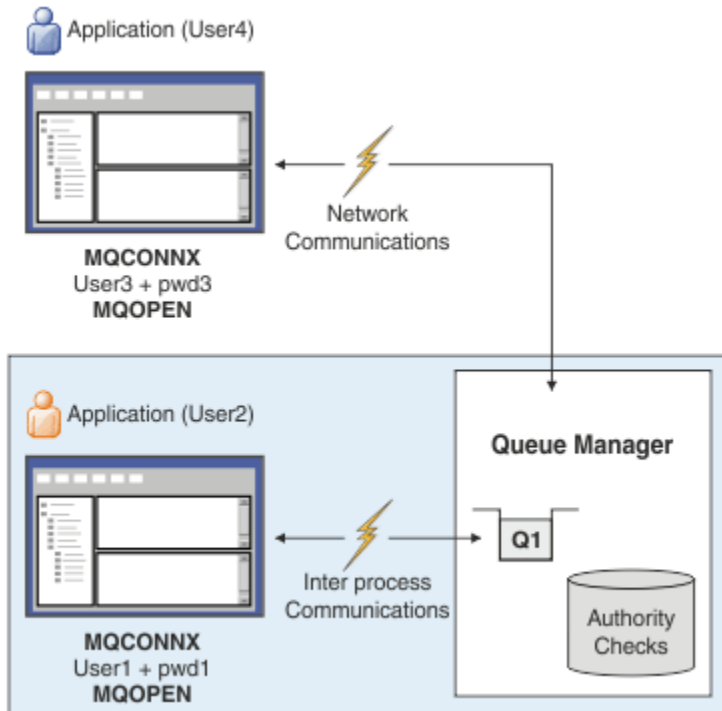
모니터링 도구

모니터링 도구는 SYSTEM.ADMIN.QMGR.EVENT 큐에 이벤트 메시지를 전송하여 권한 이벤트를 켜는 경우에도 실패를 알릴 수 있습니다.

```
ALTER QMGR AUTHOREV(ENABLED)
```

이 "권한이 부여되지 않음" 이벤트는 유형 1 연결 이벤트이며, 기타 유형 1 이벤트와 동일한 필드 외에도 제공된 MQCSP 사용자 ID의 추가 필드를 제공합니다. 이벤트 메시지에 비밀번호가 제공되지 않습니다. 즉, 이벤트 메시지에 두 개의 사용자 ID(애플리케이션을 실행 중인 ID와 사용자 ID 및 비밀번호 검사를 위해 애플리케이션에서 제공한 ID)가 있습니다.

권한 부여 관계



예를 들어, 애플리케이션이 출력을 위해 큐를 열 때 애플리케이션에서 비밀번호와 함께 제공한 사용자 ID와 애플리케이션을 실행 중인 사용자 ID가 다를 수 있으므로 특정 애플리케이션에서 사용자 ID와 비밀번호를 반드시 제공하도록 큐 관리자를 구성할 수 있습니다.

```
ALTER QMGR CONNAUTH(USE.PWD)
DEFINE AUTHINFO(USE.PWD) +
  AUTHTYPE(XXXXXX) +
  CHCKLOCL(OPTIONAL) +
  CHCKCLNT(REQUIRED) +
  ADOPTCTX(YES)
```

사용자 ID와 비밀번호를 처리하는 방식은 인증 정보 오브젝트의 **ADOPTCTX** 속성으로 제어합니다.

ADOPTCTX(YES)

나머지 연결 기간 동안 컨텍스트를 애플리케이션 컨텍스트로 채택하도록 선택하여 비밀번호로 인증된 동일한 사용자 ID를 사용하여 애플리케이션의 모든 인증을 검사합니다.



주의: ADOPTCTX(YES) 및 OS 사용자 ID를 사용할 때 채택되는 사용자 ID가 사용자 ID의 최대 길이를 초과하지 않는지 확인해야 합니다. 자세한 정보는 74 페이지의 『사용자 ID』의 내용을 참조하십시오.

ADOPTCTX(NO)

연결 시 인증하도록 애플리케이션에서 사용자 ID와 비밀번호를 제공하지만, 장래 권한 부여 검사는 애플리케이션을 실행 중인 사용자 ID를 사용하여 계속됩니다. 이 옵션은 마이그레이션할 때 또는 채널 인증 레코드와 같은 다른 메커니즘을 사용하여 메시지 채널 에이전트 사용자 ID(MCAUSER)를 지정하려는 경우에 유용할 수 있습니다.



주의:

인증 정보 오브젝트에서 **ADOPTCTX(YES)** 매개변수를 사용하는 경우 `qm.ini` 파일의 채널 스탠자에서 **ChlauthEarlyAdopt** 매개변수를 설정하는 경우가 아니면 다른 보안 컨텍스트를 채택할 수 없습니다.

예를 들어, 기본 인증 정보 오브젝트는 **ADOPTCTX(YES)**로 설정되어 있고 사용자 fred가 로그인되어 있습니다. 다음 두 가지 CHLAUTH 규칙이 구성되어 있습니다.

```
SET CHLAUTH('MY.CHLAUTH') TYPE(ADDRESSMAP) DESCR('Block all access by default') ADDRESS('*') USERSRC(NOACCESS) ACTION(REPLACE)
SET CHLAUTH('MY.CHLAUTH') TYPE(USERMAP) DESCR('Allow user bob and force CONNAUTH') CLNTUSER('bob') CHCKCLNT(REQUIRED) USERSRC(CHANNEL)
```

다음 명령을 사용자 bob의 채택된 보안 컨텍스트로 인증하려는 의도를 가지고 다음 명령이 실행됩니다.

```
runmqsc -c -u bob QMGR
```

실제로 큐 관리자는 bob이 아니라 fred의 보안 컨텍스트를 사용하고 연결이 실패합니다.

ChlauthEarlyAdopt에 대한 자세한 정보는 [속성 채널 스탠자의 속성을 참조하십시오.](#)

관련 개념

[59 페이지의 『연결 인증』](#)

[64 페이지의 『연결 인증: 애플리케이션 변경사항』](#)

[65 페이지의 『연결 인증: 사용자 저장소』](#)

각 큐 관리자에 대해 사용자 ID 및 비밀번호를 인증하기 위해 서로 다른 유형의 인증 정보 오브젝트를 선택할 수 있습니다.

연결 인증: 애플리케이션 변경사항

애플리케이션은 MQCONN가 호출될 때 연결 보안 매개변수(MQCSP) 구조 내에서 사용자 ID 및 비밀번호를 제공할 수 있습니다. 사용자 ID 및 비밀번호는 검사를 위해 큐 관리자와 함께 제공된 오브젝트 권한 관리자(OAM) 또는 z/OS 시스템에서 큐 관리자와 함께 제공된 권한 서비스 컴포넌트에 전달됩니다. 사용자 고유의 사용자 정의 인터페이스를 작성할 필요가 없습니다.

애플리케이션이 클라이언트로서 실행 중이면 사용자 ID 및 비밀번호 또한 처리를 위해 클라이언트측 및 서버측 보안 엑시트에 전달됩니다. 이들은 또한 채널 인스턴스의 메시지 채널 에이전트 사용자 ID(MCAUSER) 속성 설정에도 사용됩니다. 보안 엑시트는 이 처리를 위해 엑시트 이유 MQXR_SEC_PARMS와 함께 호출됩니다. 클라이언트측 보안 엑시트 및 사전 연결 엑시트는 큐 관리자가 전송되기 전에 MQCONN을 변경할 수 있습니다.

경고: 일부 경우에 클라이언트 애플리케이션에 대한 MQCSP 구조의 비밀번호는 일반 텍스트로 네트워크 전체에 전송됩니다. 클라이언트 애플리케이션 비밀번호가 적절하게 보호될 수 있도록 하려면 [26 페이지의 『MQCSP 비밀번호 보호』](#)의 내용을 참조하십시오.

사용자 ID 및 비밀번호를 제공하기 위해 XAOPEN 문자열을 사용하여 애플리케이션 코드의 변경을 피할 수 있습니다.

참고:

IBM WebSphere MQ 6.0부터는 보안 엑시트에서는 MQCSP를 설정할 수 있습니다. 그러므로, 이 레벨 이상에 있는 클라이언트는 업그레이드할 필요가 없습니다.

그러나 IBM MQ 8.0이전의 IBM MQ 버전에서는 MQCSP가 애플리케이션에서 제공한 사용자 ID 및 비밀번호에 대한 제한을 두지 않았습니다. 이러한 값을 IBM MQ에서 제공하는 기능과 함께 사용하는 경우 이러한 기능을 사용하는 데 적용되는 한계가 있지만 사용자 고유의 엑시트에만 전달하는 경우에는 해당 한계가 적용되지 않습니다.

관련 개념

59 페이지의 『연결 인증』

60 페이지의 『연결 인증: 구성』

큐 관리자는 제공된 사용자 ID와 비밀번호를 사용하여 사용자가 자원에 액세스할 권한이 있는지 확인하도록 구성될 수 있습니다.

65 페이지의 『연결 인증: 사용자 저장소』

각 큐 관리자에 대해 사용자 ID 및 비밀번호를 인증하기 위해 서로 다른 유형의 인증 정보 오브젝트를 선택할 수 있습니다.

연결 인증: 사용자 저장소

각 큐 관리자에 대해 사용자 ID 및 비밀번호를 인증하기 위해 서로 다른 유형의 인증 정보 오브젝트를 선택할 수 있습니다.

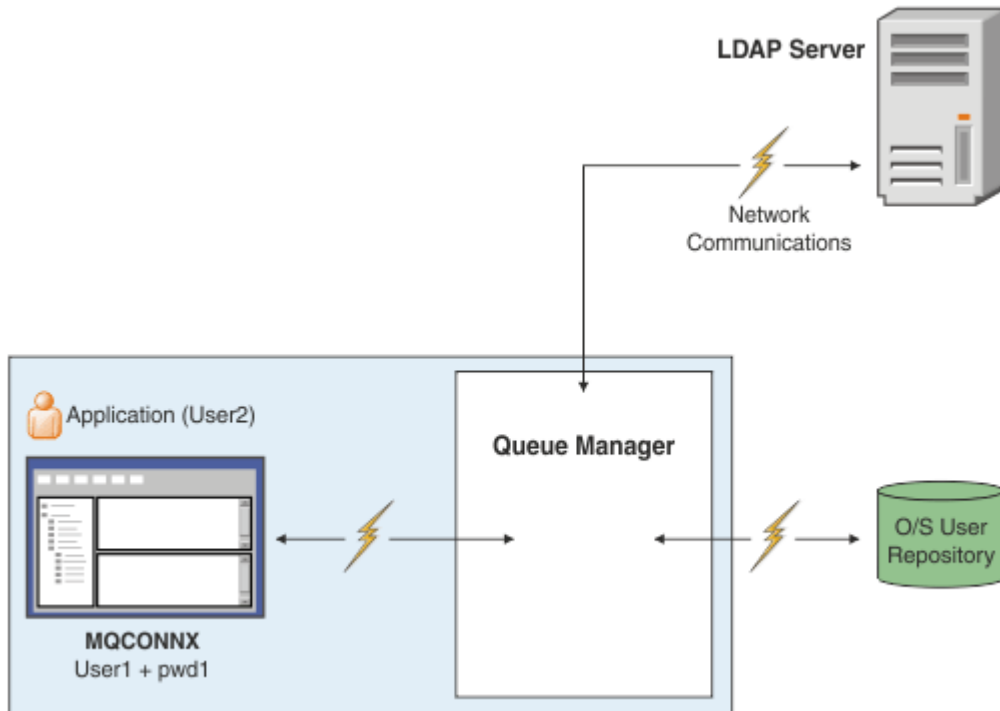


그림 7. 인증 정보 오브젝트 유형

```
DEFINE AUTHINFO(USE.OS) AUTHTYPE(IDPWOS)
DEFINE AUTHINFO(USE.LDAP) +
AUTHTYPE(IDPWLLDAP) +
CONNNAME('ldap1(389),ldap2(389)') +
LDAPUSER('CN=QMGR1') +
LDAPPWD('passw0rd') SECCOMM(YES)
```

다이어그램에 표시된 대로 두 가지 유형의 인증 정보 오브젝트가 있습니다.

- IDPWOS는 큐 관리자가 사용자 ID 및 비밀번호를 인증하기 위해 로컬 운영 체제를 사용함을 나타내는 데 사용됩니다. 로컬 운영 체제를 사용하기로 선택한 경우에는 앞의 주제에 설명된 대로 공통 속성을 설정해야 합니다.
- IDPWLLDAP는 큐 관리자가 사용자 ID 및 비밀번호를 인증하기 위해 LDAP 서버를 사용함을 나타내는 데 사용됩니다. LDAP 서버를 사용하기로 선택한 경우에는 이 주제에서 더 많은 정보가 제공됩니다.

큐 관리자의 **CONNAUTH** 속성에서 적합한 오브젝트에 이름을 지정하여 각 큐 관리자가 사용할 단 한가지 유형의 인증 정보 오브젝트만을 선택할 수 있습니다.

인증을 위해 LDAP 서버 사용

CONNAME 필드를 큐 관리자의 LDAP 서버의 주소로 설정하십시오. LDAP 서버의 추가 주소를 쉽표로 구분된 목록으로 제공할 수 있고, 이는 LDAP 서버가 이 기능 자체를 제공하지 않는 경우 중복성에 도움을 줄 수 있습니다.

큐 관리자가 LDAP 서버에 액세스하고 사용자 레코드에 대한 정보를 찾아볼 수 있도록 필수 LDAP 서버 ID 및 비밀번호를 **LDAPUSER** 및 **LDAPPWD** 필드에 설정하십시오.

LDAP 서버로의 보안 연결

채널과는 달리 LDAP 서버와 통신하기 위해 TLS의 사용을 켜기 위한 **SSLCIPH** 매개변수가 없습니다. 이 경우 IBM MQ는 LDAP 서버에서 많은 구성이 수행될 수 있도록 LDAP 서버에 클라이언트의 역할을 수행합니다. IBM MQ에서 일부 기존 매개변수는 해당 연결이 작동하는 방법을 구성하는 데 사용됩니다.

LDAP 서버에 대한 연결성이 TLS를 사용하는지 여부를 제어하려면 **SECCOMM** 필드를 설정하십시오.

이 속성에 추가로, 큐 관리자 속성 **SSLFIPS** 및 **SUITEB**는 선택된 암호 스펙의 세트를 제한합니다. LDAP 서버에 큐 관리자를 식별하는 데 사용되는 인증서 `ibmwebspheremq qmgr-name` 또는 **CERTLABL** 속성의 값입니다. 자세한 내용은 디지털 인증서 레이블을 참조하십시오.

LDAP 사용자 저장소

LDAP 사용자 저장소를 사용할 때 단지 큐 관리자에 LDAP 서버를 찾을 위치를 알려주는 것보다 더 많은 구성을 큐 관리자에서 수행해야 합니다.

LDAP 서버에 정의된 사용자 ID에는 이를 고유하게 식별하는 계층 구조가 있습니다. 그러므로 애플리케이션은 큐 관리자에 연결하고 해당 사용자 ID를 완전한 계층 구조 사용자 ID로 제공할 수 있습니다.

그러나 애플리케이션이 제공해야 하는 정보를 단순화하기 위해 계층의 첫 번째 부분은 모든 ID에 공통됨을 가정하고 애플리케이션이 제공한 단축된 ID 앞에 이를 자동으로 추가하도록 큐 관리자를 구성할 수 있습니다. 그러면 큐 관리자는 LDAP 서버에 완전한 ID를 제공할 수 있습니다.

LDAP 계층에서 LDAP이 ID를 검색하는 초기 지점으로 **BASEDNU**를 설정하십시오. **BASEDNU**를 설정하는 경우 LDAP 계층에서 ID를 검색할 때 하나의 결과만 리턴되는지 확인해야 합니다.

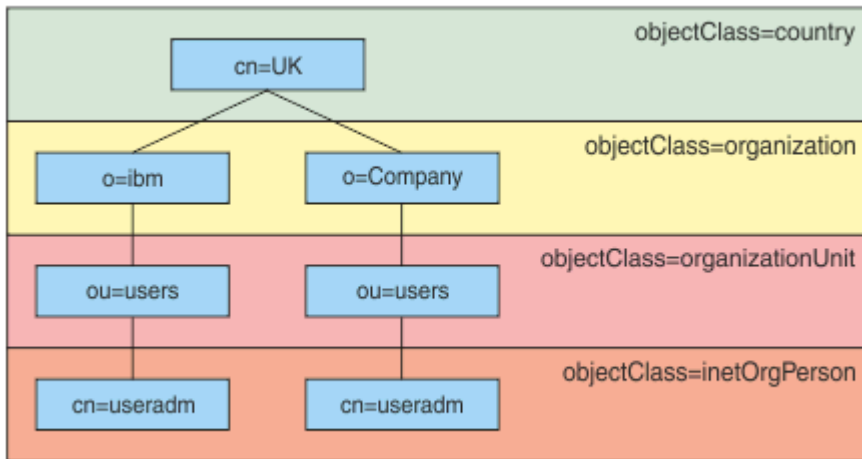


그림 8. LDAP 계층 예

예를 들어, 66 페이지의 그림 8에서 **BASEDNU**는 "ou=users,o=ibm,c=UK" 또는 "o=ibm,c=UK"로 설정할 수 있습니다. 그러나 "cn=useradm"을 포함하는 식별 이름이 "o=ibm" 분기 및 "o=Company" 분기 모두에 있으므로, **BASEDNU**는 "c=UK"로 설정할 수 없습니다. 성능 및 보안상의 이유로, LDAP 계층 중 필요한 사용자 ID 모두를 참조할 수 있는 지점에서 가장 높은 지점을 사용합니다. 이 예에서는 "ou=users,o=ibm,c=UK"가 이 지점입니다.

애플리케이션은 LDAP 속성 이름(예: CN=)을 제공하지 않고 큐 관리자에 사용자 ID를 제출할 수도 있습니다.

USRFIELD를 LDAP 속성 이름에 설정한 경우에는 이 값은 애플리케이션에서 나오는 사용자 ID에 접두부로서 추가됩니다. 이는 운영 체제 사용자 ID에서 LDAP 사용자 ID로 이동할 때 유용한 마이그레이션 보조 도구일 수 있습니다.

니다. 그러면 애플리케이션이 두 경우 모두 동일한 문자열을 제공할 수 있고 애플리케이션을 변경하는 것을 피할 수 있습니다.

그러므로 LDAP 서버에 제공된 완전한 사용자 ID는 다음과 비슷합니다.

```
USRFIELD = ID_from_application BASEDNU
```

관련 개념

[59 페이지의 『연결 인증』](#)

[60 페이지의 『연결 인증: 구성』](#)

큐 관리자는 제공된 사용자 ID와 비밀번호를 사용하여 사용자가 자원에 액세스할 권한이 있는지 확인하도록 구성될 수 있습니다.

[64 페이지의 『연결 인증: 애플리케이션 변경사항』](#)

사용자 ID 및 비밀번호(mqccred)를 삽입하기 위한 클라이언트측 보안 엑시트

If you have any client applications that are required to send a user ID or password but you are unable to change the source yet, there is a security exit shipped with IBM MQ 8.0 called **mqccred** that you can use. **mqccred**는 클라이언트 애플리케이션 대신에 .ini 파일로부터 사용자 ID 및 비밀번호를 제공합니다. 이 사용자 ID 및 비밀번호는 이들을 인증할(그렇게 구성된 경우) 큐 관리자에 전송됩니다.

개요

mqccred는 클라이언트 애플리케이션과 같은 시스템에서 실행되는 보안 엑시트입니다. 이는 사용자 ID 및 비밀번호 정보를 클라이언트 애플리케이션 대신에 제공하도록 허용합니다(해당 정보가 애플리케이션 자체에 의해 제공되는 중이 아닌 경우). 사용자 ID 및 비밀번호 정보는 [연결 보안 매개변수\(MQCSP\)](#)로서 알려진 구조로 제공되고 [연결 인증](#)이 구성된 경우 큐 관리자에 의해 인증됩니다.

사용자 ID 및 비밀번호 정보는 클라이언트 시스템에서 .ini 파일로부터 검색됩니다. 파일의 비밀번호는 클라이언트 애플리케이션을 실행 중인 사용자 ID(및 그러므로 엑시트)만이 이를 읽을 수 있도록 **runmqccred** 명령을 사용하고 또한 .ini에서 파일 권한을 확인하여 난독화를 통해 보호됩니다.

위치

mqccred가 설치됩니다:

Windows 플랫폼

`installation_directory\Tools\c\Samples\mqccred\` 디렉토리에서

UNIX 플랫폼

`installation_directory/samp/mqccred` 디렉토리에서

참고사항: 엑시트:

1. 보안 채널 엑시트로서 순수하게 작동하고, 채널에 정의된 유일한 이러한 엑시트여야 합니다.
2. 이는 일반적으로 CCDT(Client Channel Definition Table)를 통해 이름이 지정되지만 Java 클라이언트는 JNDI 오브젝트에 직접 언급된 엑시트를 가질 수 있거나, 엑시트가 [MQCD](#) 구조를 수동으로 구성하는 애플리케이션에 대해 구성되어 있을 수도 있습니다.
3. **mqccred** 및 **mqccred_r** 프로그램을 `var/mqm/exits` 디렉토리로 복사해야 합니다.

예를 들어 64비트 UNIX 플랫폼 시스템에서 다음 명령을 실행하십시오.

```
cp installation_directory/samp/mqccred/lib64/* /var/mqm/exits
```

자세한 정보는 [mqccred를 테스트하는 방법의 단계별 예](#)를 참조하십시오.

4. IBM MQ의 이전 버전에서 실행할 수 있습니다(IBM WebSphere MQ 7.0.1까지).

사용자 ID 및 비밀번호 설정

.ini 파일은 지정되지 않은 큐 관리자를 위한 글로벌 설정과 함께 각 큐 관리자의 스탠자를 포함합니다. 각 스탠자에는 큐 관리자의 이름, 사용자 ID 및 일반 텍스트 또는 난독화된 비밀번호를 포함합니다.

원하는 어떤 편집기든지 사용하여 .ini 파일을 직접 편집하고 스탠자에 일반 텍스트 비밀번호 속성을 추가해야 합니다. 제공된, **runmqccred** 프로그램을 실행하십시오. 이는 .ini 파일을 사용하고 **Password** 속성을 비밀번호의 난독화된 양식인 **OPW** 속성으로 바꿉니다.

명령 및 해당 매개변수의 설명은 **runmqccred**의 내용을 참조하십시오.

mqccred.ini 파일에는 사용자 ID 및 비밀번호 정보가 포함됩니다.

템플릿 .ini 파일이 엔터프라이즈의 시작점을 제공하기 위해 엑시트와 동일 디렉토리에 제공됩니다.

기본적으로 \$HOME/.mqc/mqccred.ini에서 이 파일을 찾습니다. 이를 다른 곳에서 찾아보고 싶으면 이를 가리키는 환경 변수 **MQCCRED**를 사용할 수 있습니다.

```
MQCCRED=C:\mydir\mqccred.ini
```

MQCCRED를 사용하는 경우에는 변수에는 .ini 파일 유형을 포함하여 구성 파일의 전체 이름을 포함해야 합니다. 이 파일에는 비밀번호(난독화되었더라도)가 포함되므로 권한 없는 사용자가 이를 읽을 수 없도록 하기 위해 운영 체제 권한을 사용하여 파일을 보호할 것으로 기대됩니다. 올바른 파일 권한이 없는 경우에는 엑시트는 성공적으로 실행되지 않습니다.

애플리케이션이 이미 **MQCSP** 구조를 제공한 경우에는 엑시트는 일반적으로 이를 예상하고 .ini 파일로부터 정보를 삽입하지 않습니다. 그러나 스탠자에서 **Force** 속성을 사용하여 이를 대체할 수 있습니다.

Force를 **TRUE** 값으로 설정하면 애플리케이션 제공 사용자 ID 및 비밀번호가 제거되고 이들이 ini 파일 버전으로 바뀝니다.

파일의 기본값을 설정하기 위해 해당 파일의 글로벌 절에서 **Force** 속성을 설정할 수도 있습니다.

Force의 기본값은 **FALSE**입니다.

모든 큐 관리자 또는 각 개별 큐 관리자에 대해 사용자 ID 및 비밀번호를 제공할 수 있습니다. 이는 mqccred.ini 파일의 예입니다.

```
# comments are permitted
AllQueueManagers:
User=abc
OPW=%^&aervrgtsr

QueueManager:
Name=QMA
User=user1
OPW=H&^dbgfh

Force=TRUE

QueueManager:
Name=QMB
User=user2
password=passw0rd
```

참고사항:

1. 개별 큐 관리자 정의는 글로벌 설정에 우선합니다.
2. 속성은 대소문자를 구분합니다.

제한조건

이 엑시트가 사용 중이면 애플리케이션을 실행하는 사용자의 로컬 사용자 ID는 클라이언트에서 서버로 플로우하지 않습니다. 사용 가능한 유일한 ID 정보는 ini 파일 콘텐츠에서 나옵니다.

그러므로 **ADOPTCTX(YES)**를 사용하도록 큐 관리자를 구성하거나 사용 가능한 메커니즘 중 하나를 사용하여 (예: 43 페이지의 『채널 인증 레코드』) 인바운드 연결 요청을 적합한 사용자 ID로 맵핑해야 합니다.

중요사항: 새 비밀번호를 추가하거나 이전 비밀번호를 업데이트하는 경우에는 **runmqccred** 명령은 일반 텍스트 비밀번호만을 처리하고 난독화된 비밀번호는 변경되지 않은 상태로 남겨둡니다.

디버그

엑시트는 사용 가능할 때 표준 IBM MQ 추적에 작성합니다.

디버깅 구성 문제를 돕기 위해 엑시트는 stdout에 직접 작성할 수도 있습니다.

채널 보안 엑시트 데이터(**SCYDATA**) 구성은 일반적으로 채널에는 필요하지 않습니다. 그러나 사용자는 다음을 지정할 수 있습니다.

오류

구성 파일을 찾을 수 없는 것과 같은 오류 조건에 대한 인쇄 정보만.

DEBUG

이러한 오류 조건 및 일부 추가적인 추적 명령문을 표시합니다.

NOCHECKS

파일 권한에 대한 제한조건 및 .ini 파일이 보호되지 않은 비밀번호를 포함하지 않아야 하는 추가 제한조건을 무시합니다.

하나 이상의 이러한 요소를 쉼표로 구분하여 임의의 순서대로 **SCYDATA** 필드에 넣을 수 있습니다. 예를 들어, SCYDATA=(NOCHECKS, DEBUG)입니다.

항목은 대소문자를 구분하여 대문자로 입력되어야 함을 유의하십시오.

mqccred 사용

파일을 설정한 후에는 SCYEXIT('mqccred(ChlExit)') 속성을 포함하도록 클라이언트 연결 채널 정의를 업데이트하여 채널 엑시트를 호출할 수 있습니다.

```
DEFINE CHANNEL(channelname) CHLTYPE(cIntconn) +  
CONNAME(remote machine) +  
QMNAME(remote qmgr) +  
SCYEXIT('mqccred(ChlExit)') +  
REPLACE
```

관련 참조

[SCYDATA](#)

[SCYEXIT](#)

[runmqccred](#)

Java 클라이언트와의 연결 인증

연결 인증은 제공된 사용자 ID 및 비밀번호를 사용하여 애플리케이션을 인증하도록 큐 관리자를 구성할 수 있는 IBM MQ의 기능입니다. 애플리케이션이 클라이언트 바인딩을 사용하는 Java 애플리케이션일 경우 호환 모드 또는 MQCSP 인증 모드에서 연결 인증을 실행할 수 있습니다.

호환 모드

IBM MQ 8.0 이전에는 Java 클라이언트가 클라이언트 연결 채널을 통해 사용자 ID와 비밀번호를 서버 연결 채널로 송신하고, 이들을 MQCD 구조의 **RemoteUserIdentifier** 및 **RemotePassword** 필드에 있는 보안 엑시트에 제공할 수 있었습니다. 호환성 모드에서 이 동작은 유지됩니다.

이 모드를 연결 인증과 결합하여 사용할 수 있고, 이전에 동일 작업을 수행하는 데 사용되었던 보안 엑시트로부터 멀리 마이그레이션할 수도 있습니다.

호환 모드에서는 클라이언트 측 사용자 ID가 큐 관리자로 송신되지 않으므로, 이 모드를 사용할 경우 ADOPTCTX(YES)를 사용하거나, TLS 인증서를 기반으로 하는 CHLAUTH 규칙과 같은 다른 방법으로 사용하여 실행 중인 MCAUSER를 설정해야 합니다.

조작의 호환 모드는 연결별 기준으로 또는 글로벌로 사용하도록 설정할 수 있습니다.

- IBM MQ classes for Java에서 **com.ibm.mq.MQQueueManager** 생성자에 전달되는 특성 해시 테이블에서 *MQConstants.USE_MQCSP_AUTHENTICATION_PROPERTY* 특성을 `false` 로 설정하십시오.
- IBM MQ classes for JMS의 경우, 연결을 작성하기 전에 적합한 연결 팩토리에서 *JmsConstants.USER_AUTHENTICATION_MQCSP* 특성을 `false`로 설정하십시오.
- 다음 예제에 표시된 대로 글로벌하게 애플리케이션을 시작할 때 명령행에서 Java 시스템 특성 `-Dcom.ibm.mq.cfg.jmqi.useMQCSPauthentication=N` 을 지정하십시오.

```
java -Dcom.ibm.mq.cfg.jmqi.useMQCSPauthentication=N application_name
```

호환 모드는 기본 설정입니다.

MQCSP 인증 모드

이 모드에서는 인증할 사용자 ID와 비밀번호뿐만 아니라 클라이언트 측 사용자 ID도 송신되므로 ADOPTCTX(NO)를 사용할 수 있습니다. 사용자 ID와 비밀번호는 MQCXP 구조에 제공되는 MQCSP 구조의 서버 연결 보안 엑시트에서 사용할 수 있습니다.

이 조작 모드는 연결별 또는 글로벌로 사용 가능할 수 있습니다:

- IBM MQ classes for Java에서 **com.ibm.mq.MQQueueManager** 생성자에 전달되는 특성 해시 테이블에서 *MQConstants.USE_MQCSP_AUTHENTICATION_PROPERTY* 특성을 `true` 로 설정하십시오.
- IBM MQ classes for JMS의 경우, 연결을 작성하기 전에 적합한 연결 팩토리에서 *JmsConstants.USER_AUTHENTICATION_MQCSP* 특성을 `true`로 설정하십시오.
- 예를 들어, `-Dcom.ibm.mq.cfg.jmqi.useMQCSPauthentication=Y`를 명령행에 추가하여 시스템 특성 `com.ibm.mq.cfg.jmqi.useMQCSPauthentication`을 `true`를 나타내는 값으로 글로벌하게 설정하십시오.

IBM MQ Explorer에서 인증 모드 선택

IBM MQ Explorer는 Java 애플리케이션이므로 호환성 모드와 MQCSP 인증 모드라는 두 개의 모드 또한 적용 가능합니다.

V 9.1.0 IBM MQ 9.1.0부터, MQCSP 인증 모드가 기본값입니다. IBM MQ 9.1 이전 버전에서는 호환 모드가 기본값입니다.

사용자 ID가 제공된 패널에는 호환 모드를 사용 또는 사용 안함으로 설정하는 선택란이 있습니다.

- **V 9.1.0** IBM MQ 9.1.0부터는 기본적으로 이 선택란이 선택되어 있지 않습니다. 호환 모드를 사용하려면 이 선택란을 선택하십시오.
- IBM MQ 9.1.0 이전 버전에서는 기본적으로 이 선택란이 사용으로 설정됩니다. MQCSP 인증을 사용하려면 이 선택란을 선택 취소하십시오.

관련 개념

[59 페이지의 『연결 인증』](#)

[64 페이지의 『연결 인증: 애플리케이션 변경사항』](#)

[65 페이지의 『연결 인증: 사용자 저장소』](#)

각 큐 관리자에 대해 사용자 ID 및 비밀번호를 인증하기 위해 서로 다른 유형의 인증 정보 오브젝트를 선택할 수 있습니다.

IBM MQ의 메시지 보안

IBM MQ 인프라에서 메시지 보안은 Advanced Message Security에 의해 제공됩니다.

Advanced Message Security(AMS)는 IBM MQ 보안 서비스를 확장하여 메시지 레벨에서 데이터 서명 및 암호화를 제공합니다. 확장된 서비스를 통해 메시지 데이터가 원래 큐에 배치된 시기와 검색된 시기 사이에서 수정되지 않도록 보장됩니다. 또한, AMS는 메시지 데이터 송신자가 서명된 메시지를 대상 큐에 배치할 권한이 있는지 확인합니다.

관련 개념

506 페이지의 『Advanced Message Security』

Advanced Message Security(AMS)는 엔드 애플리케이션에 영향을 미치지 않으면서 IBM MQ 네트워크를 통해 플로우하는 민감한 데이터에 대한 높은 레벨의 보호를 제공하는 IBM MQ의 컴포넌트입니다.

보안 요구사항 계획

이 주제 모음에서는 IBM MQ 환경에서 보안을 계획할 때 고려해야 하는 사항에 대해 설명합니다.

플랫폼 범위에서 다양한 애플리케이션에 대해 IBM MQ를 사용할 수 있습니다. 보안 요구사항은 각 애플리케이션 별로 다를 수 있습니다. 어떤 경우에는 보안이 중요한 고려사항입니다.

IBM MQ는 TLS(Transport Layer Security)에 대한 지원을 비롯하여 링크 레벨 보안 서비스 범위를 제공합니다.

IBM MQ 설치를 계획할 때 특정 보안 측면을 고려해야 합니다.

- ▶ **Multi** 멀티플랫폼에서 이런 측면을 무시하고 아무것도 수행하지 않으면 IBM MQ를 사용할 수 없습니다.
- ▶ **z/OS** z/OS에서 이런 측면을 무시하면 IBM MQ 자원이 보호되지 않습니다. 즉, 모든 사용자가 모든 IBM MQ 자원에 액세스하여 변경할 수 있습니다.

IBM MQ 관리 권한

IBM MQ 관리자는 다음을 수행할 권한이 필요합니다.

- IBM MQ 관리를 위한 명령 발행
- 사용 IBM MQ Explorer
- ▶ **IBM i** IBM i 관리 패널 및 명령 사용
- ▶ **z/OS** z/OS에서 조작 및 제어판 사용
- ▶ **z/OS** z/OS에서 IBM MQ 유틸리티 프로그램 CSQUTIL 사용
- ▶ **z/OS** z/OS에서 큐 관리자 데이터 세트 액세스

자세한 정보는 다음을 참조하십시오.

- ▶ **ULW** 361 페이지의 『UNIX, Linux, and Windows 에서 IBM MQ 를 관리하는 권한』
- ▶ **IBM i** 75 페이지의 『IBM i 에서 IBM MQ 를 관리하는 권한』
- ▶ **z/OS** 76 페이지의 『z/OS 에서 IBM MQ 를 관리하는 권한』

IBM MQ 오브젝트에 대해 작업할 권한

애플리케이션은 MQI 호출을 발행하여 다음 IBM MQ 오브젝트에 액세스할 수 있습니다.

- 큐 관리자
- 큐
- Processes
- 이름 목록
- 토픽

애플리케이션은 프로그래밍 가능 명령 형식(PCF) 명령을 사용해서도 해당 IBM MQ 오브젝트에 액세스하고 채널 및 인증 정보 오브젝트에도 액세스할 수 있습니다. 해당 오브젝트는 IBM MQ에서 보호 가능하기 때문에 애플리케이션에 연관된 사용자 ID는 이에 대한 액세스 권한이 필요합니다.

자세한 정보는 78 페이지의 『애플리케이션에서 IBM MQ를 사용하기 위한 권한 부여』의 내용을 참조하십시오.

채널 보안

메시지 채널 에이전트(MCA)에 연관된 사용자 ID는 다양한 IBM MQ 자원 액세스 권한이 필요합니다. 예를 들어, MCA는 큐 관리자에 연결할 수 있어야 합니다. 송신 MCA인 경우 채널에 대해 전송 큐를 열 수 있어야 합니다. 수신 MCA의 경우 목적지 큐를 열 수 있어야 합니다. 애플리케이션과 연관된 사용자 ID는 채널, 채널 시작기, 리스너를 관리하려면 관련 PCF 명령을 사용하기 위한 권한이 필요합니다. 그렇지만 대부분의 애플리케이션에는 이러한 액세스 권한이 필요하지 않습니다.

자세한 정보는 96 페이지의 『채널 권한 부여』의 내용을 참조하십시오.

추가적인 고려사항

특정 IBM MQ 기능이나 기본 제품 확장을 사용 중인 경우에만 다음과 같은 보안 관점도 고려해야 합니다.

- [107 페이지의 『큐 관리자 클러스터의 보안』](#)
- [108 페이지의 『IBM MQ 발행/구독에 대한 보안』](#)
- [109 페이지의 『IBM MQ Internet Pass-Thru 보안』](#)

식별 및 인증 계획

사용하려는 사용자 ID, 인증 제어에 레벨을 적용하는 방법 및 적용하는 레벨을 결정하십시오.

다른 운영 체제는 다른 길이의 사용자 ID를 지원한다는 점에 유의하여 IBM MQ 애플리케이션 사용자 식별 방법을 결정해야 합니다. 채널 인증 레코드를 사용하여 임의의 사용자 ID에서 다른 사용자 ID로 매핑하거나 일부 연결 속성을 기반으로 사용자 ID를 지정할 수 있습니다. TLS를 사용하는 IBM MQ 채널은 디지털 인증서를 식별 및 인증 메커니즘으로 사용합니다. 각 디지털 인증서는 채널 인증 레코드를 사용하여 특정 ID로 매핑 가능한 주제 식별 이름을 포함합니다. 또한, 키 저장소의 CA 인증서는 IBM MQ 인증에 사용될 수 있는 디지털 인증서를 판별합니다. 자세한 정보는 다음을 참조하십시오.

- [346 페이지의 『MCAUSER 사용자 ID에 리모트 큐 관리자 매핑』](#)
- [347 페이지의 『MCAUSER 사용자 ID에 클라이언트 사용자 ID 매핑』](#)
- [347 페이지의 『MCAUSER 사용자 ID에 SSL 또는 TLS 식별 이름 매핑』](#)
- [349 페이지의 『MCAUSER 사용자 ID에 IP 주소 매핑』](#)

클라이언트 애플리케이션에 대한 인증 계획

네 개의 레벨(통신 레벨, 보안 엑시트, 채널 인증 레코드, 보안 엑시트에 전달된 ID)에서 인증 제어를 적용할 수 있습니다.

고려해야 하는 보안 레벨에는 네 개의 레벨이 있습니다. 다이어그램은 서버에 연결된 IBM MQ MQI client를 보여줍니다. 보안은 다음 텍스트에 설명되어 있는 것처럼 네 개의 레벨에서 적용됩니다. MCA는 메시지 채널 에이전트입니다.

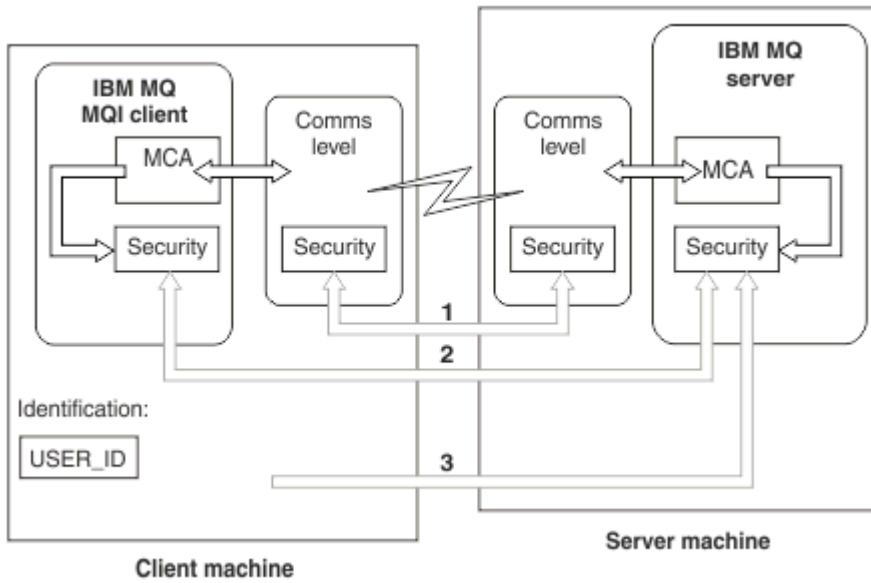


그림 9. 클라이언트/서버 연결에서의 보안

1. 통신 레벨

화살표 1을 보십시오. 통신 레벨에서 보안을 구현하려면 TLS를 사용하십시오. 자세한 정보는 [14 페이지의 『암호화 보안 프로토콜: TLS』](#)의 내용을 참조하십시오.

2. 채널 인증 레코드

화살표 2 및 3을 참조하십시오. 보안 레벨에서 IP 주소 또는 TLS 식별 이름을 사용하여 인증을 제어할 수 있습니다. 사용자 ID는 차단될 수도 있으며 확인된 사용자 ID는 올바른 사용자 ID에 매핑될 수 있습니다. 전체 설명은 [43 페이지의 『채널 인증 레코드』](#)에서 제공됩니다.

3. 연결 인증

화살표 3을 참조하십시오. 클라이언트가 ID와 비밀번호를 송신합니다. 자세한 정보는 [60 페이지의 『연결 인증: 구성』](#)의 내용을 참조하십시오.

4. 채널 보안 엑시트

화살표 2를 참조하십시오. 클라이언트 대 서버 통신의 채널 보안 엑시트는 서버 대 서버 통신과 같은 방식으로 작동할 수 있습니다. 프로토콜 독립 엑시트 쌍은 클라이언트와 서버 모두에 상호 인증을 제공하도록 작성될 수 있습니다. 전체 설명은 [채널 보안 엑시트 프로그램](#)에서 제공됩니다.

5. 채널 보안 엑시트에 전달된 ID

화살표 3을 참조하십시오. 클라이언트 대 서버 통신에서 채널 보안 엑시트는 쌍으로 작동할 필요가 없습니다. IBM MQ 클라이언트 측의 엑시트는 생략할 수 있습니다. 이 경우 사용자 ID는 채널 디스크립터(MQCD)에 저장되며 서버 측 보안 엑시트는 필요한 경우 이를 대체할 수 있습니다.

Windows 클라이언트는 또한 식별을 지원하기 위해 추가 정보를 전송합니다.

- 서버로 전달되는 사용자 ID는 클라이언트에 현재 로그인된 사용자 ID입니다.
- 현재 로그인된 사용자의 보안 ID입니다.

사용자 ID 및 가능한 경우 보안 ID 값은 IBM MQ MQI client ID를 설정하기 위해 서버 보안 엑시트에서 사용 가능합니다.

IBM MQ 8.0에서 MQCSP 구조에 포함된 비밀번호를 송신할 수 있습니다.

경고: 일부 경우에 클라이언트 애플리케이션에 대한 MQCSP 구조의 비밀번호는 일반 텍스트로 네트워크 전체에 전송됩니다. 클라이언트 애플리케이션 비밀번호가 적절하게 보호될 수 있도록 하려면 [26 페이지의 『MQCSP 비밀번호 보호』](#)의 내용을 참조하십시오.

사용자 ID

클라이언트 애플리케이션에 대한 사용자 ID를 작성할 때 이 사용자 ID는 허용되는 최대 길이보다 길어서는 안 됩니다. 예약된 사용자 ID인 UNKNOWN 및 NOBODY는 사용해서는 안 됩니다. 클라이언트가 연결되는 서버가 IBM MQ for Windows 서버인 경우에는 at 기호(@) 사용을 이스케이프해야 합니다. 허용되는 사용자 ID 길이는 서버에 사용되는 플랫폼에 따라 다릅니다.

- ▶ **z/OS** ▶ **Linux** ▶ **UNIX** z/OS 및 UNIX and Linux에서 사용자 ID의 최대 길이는 12자입니다.
- ▶ **IBM i** IBM i에서 사용자 ID의 최대 길이는 10자입니다.
- ▶ **Windows** Windows에서는 IBM MQ MQI client와 IBM MQ 서버가 모두 Windows에 있고 서버가 클라이언트 사용자 ID가 정의되는 도메인에 액세스하는 경우 사용자 ID의 최대 길이는 20자입니다. 하지만 IBM MQ 서버가 Windows 서버가 아닌 경우 사용자 ID는 12자로 잘립니다.
- MQCSP 구조를 사용하여 신임 정보를 전달하는 경우 사용자 ID의 최대 길이는 1024자입니다. MQCSP 구조 사용자 ID는 권한 부여를 위해 IBM MQ에서 사용하는 최대 사용자 ID 길이를 피하는 데 사용할 수 없습니다. MQCSP 구조에 대한 자세한 정보는 299 페이지의 『MQCSP 구조를 사용하여 사용자 식별 및 인증』의 내용을 참조하십시오.

UNIX and Linux 시스템에서 기본값은 사용자 ID가 인증에 사용되고 그룹이 권한 부여에 사용되는 것입니다. 그러나 사용자 ID에 대해 권한을 부여하도록 이러한 시스템을 구성할 수 있습니다. 자세한 정보는 314 페이지의 『UNIX and Linux의 OAM 사용자 기반 권한』의 내용을 참조하십시오. Windows 시스템은 인증 및 권한 부여를 위해 권한 및 그룹 모두에 대한 사용자 ID를 둘 다 사용할 수 있습니다.

그룹에 주의하지 않고 서비스 계정을 작성하고 모든 사용자 ID를 다르게 권한 부여하면 모든 사용자가 다른 모든 사용자의 정보에 액세스할 수 있습니다.

제한된 사용자 ID

사용자 ID UNKNOWN 및 그룹 NOBODY는 IBM MQ에서 특별한 의미를 가집니다. 운영 체제에서 UNKNOWN이라는 사용자 ID와 NOBODY라는 그룹을 작성하면 의도하지 않은 결과가 발생할 수 있습니다.

IBM MQ for Windows 서버에 연결할 때 사용자 ID

Windows

IBM MQ for Windows 서버는 클라이언트가 @ 문자를 포함하는 사용자 ID (예: abc@d) 에서 실행 중인 경우 Windows 클라이언트의 연결을 지원하지 않습니다. 클라이언트에서 MQCONN 호출에 대한 리턴 코드는 MQRC_NOT_AUTHORIZED입니다.

그렇지만 두 개의 @ 문자를 사용하는 사용자 ID(예: abc@@d)는 지정할 수 있습니다. id@domain 형식 사용은 사용자 ID가 올바른 도메인으로 일관성있게 해결(abc@@d@domain)되도록 보장하는 선호 방식입니다.

권한 부여 계획

관리 권한이 있는 사용자를 계획하고 IBM MQ MQI client에서 연결하는 것을 포함하여 IBM MQ 오브젝트를 적절히 사용하도록 애플리케이션 사용자에게 권한을 부여하는 방법을 계획하십시오.

IBM MQ를 사용하려면 개인 또는 애플리케이션에 액세스가 부여되어야 합니다. 필요한 액세스는 수행하는 역할 및 수행해야 하는 태스크에 따라 다릅니다. IBM MQ에서의 권한 부여는 다음과 같은 두 개의 기본 범주로 구분됩니다.

- 관리 조작을 수행하기 위한 권한 부여
- 애플리케이션에서 IBM MQ를 사용하기 위한 권한 부여






두 조작 클래스 모두 동일한 컴포넌트로 제어되며 개인에게는 두 조작 범주를 수행하는 권한이 부여될 수 있습니다.

다음 토픽은 고려해야 하는 특정 권한 부여 영역에 대한 자세한 정보를 제공합니다.

IBM MQ 관리 권한

IBM MQ 관리자는 다양한 기능 수행 권한이 필요합니다. 이 권한은 다른 플랫폼에서 다양한 방식으로 확보합니다.

IBM MQ 관리자는 다음을 수행할 권한이 필요합니다.

- IBM MQ 관리하는 명령 발행
-   IBM MQ Explorer을(를) 사용하십시오.
-  z/OS에서 조작 및 제어판 사용
-  z/OS에서 IBM MQ 유틸리티 프로그램 CSQUTIL을 사용하십시오.
-  z/OS에서 큐 관리자 데이터 세트 액세스

자세한 정보는 운영 체제에 해당하는 주제를 참조하십시오.

Authority to administer IBM MQ on UNIX and Windows systems

IBM MQ 관리자는 `mqm` 그룹의 구성원입니다. 이 그룹은 모든 IBM MQ 자원에 대한 액세스를 가지며 IBM MQ 제어 명령을 발행할 수 있습니다. 관리자는 다른 사용자에게 특정 권한을 부여할 수 있습니다.

UNIX 및 Windows 시스템에서 IBM MQ 관리자가 되려면 사용자가 `mqm` 그룹의 구성원이어야 합니다. 이 그룹은 IBM MQ를 설치하면 자동으로 작성됩니다. 사용자가 제어 명령을 발행하도록 허용하려면 사용자를 `mqm` 그룹에 추가해야 합니다. 여기에는 UNIX의 루트 사용자도 포함됩니다.

`mqm` 그룹의 구성원이 아닌 사용자에게 관리 권한을 부여할 수 있지만 IBM MQ 제어 명령을 발행할 수 없고 액세스가 부여된 명령만 실행할 권리가 있습니다.


또한 Windows 시스템에서 SYSTEM 및 Administrator 계정에는 IBM MQ 자원에 대한 전체 액세스 권한이 있습니다.

`mqm` 그룹의 모든 구성원은 시스템에서 실행 중인 모든 큐 관리자를 관리할 수 있는 것을 포함하여 시스템에서 모든 IBM MQ 자원에 대한 액세스를 가집니다. 이 액세스는 사용자를 `mqm` 그룹에서 제거해야만 취소할 수 있습니다. Windows 시스템에서 관리자 그룹의 구성원은 모든 IBM MQ 자원에 대한 액세스 권한도 가집니다.

관리자는 제어 명령 `runmqsc`를 사용하여 MQSC(IBM MQ Script) 명령을 발행할 수 있습니다. MQSC 명령을 리모트 큐 관리자에게 송신하는 데 간접적인 모드로 `runmqsc`가 사용되면, 각 MQSC 명령은 이스케이프 PCF 명령 안에 캡슐화됩니다. 관리자는 리모트 큐 관리자가 처리하는 MQSC 명령에 대한 필수 권한이 있어야 합니다.

IBM MQ Explorer는 PCF 명령을 발행하여 관리 태스크를 수행합니다. 관리자는 IBM MQ Explorer를 사용하여 로컬 시스템에서 큐 관리자를 관리하는 데 추가 권한이 필요하지 않습니다. IBM MQ Explorer가 또 다른 시스템에서 큐 관리자를 관리하는 데 사용되면 관리자에게는 PCF 명령이 리모트 큐 관리자에 의해 처리되기 위해서 필요한 권한이 있어야 합니다.

PCF 및 MQSC 명령이 처리될 때 수행되는 권한 검사에 대한 자세한 정보는 다음 주제를 참조하십시오.

- 큐 관리자, 큐, 채널, 프로세스, 이름 목록, 인증 정보 오브젝트에서 운영되는 명령에 대해서는 [78 페이지의 『애플리케이션에서 IBM MQ를 사용하기 위한 권한 부여』](#)의 내용을 참조하십시오.
- 채널, 채널 이니시에이터, 리스너 및 클러스터에 대해 실행되는 명령에 대해서는 [채널 보안](#)을 참조하십시오.
-  IBM MQ for z/OS에서 명령 서버로 처리되는 MQSC 명령에 대해서는 [77 페이지의 『z/OS의 명령 보안과 명령 자원 보안』](#)의 내용을 참조하십시오.

For more information about the authority you need to administer IBM MQ on UNIX and Windows systems, see the related information.

IBM i에서 IBM MQ를 관리하는 권한

IBM i의 IBM MQ 관리자가 되려면 `QMQMADM` 그룹의 구성원이어야 합니다. 이 그룹은 UNIX 및 Windows 시스템의 `mqm` 그룹 특성과 유사한 특성이 있습니다. 특히, `QMQMADM` 그룹은 IBM MQ for IBM i 설치 시에 작성되고 `QMQMADM` 그룹 구성원은 시스템의 모든 IBM MQ 자원에 대한 액세스 권한을 가집니다. *ALLOBJ 권한이 있는 사용자인 경우 모든 IBM MQ 자원에도 액세스할 수 있습니다.

관리자는 CL 명령을 사용하여 IBM MQ를 관리할 수 있습니다. 이들 명령 중 하나는 다른 사용자에게 권한을 부여하는 데 사용되는 GRTRMQMAUT입니다. 다른 명령인 STRTRMQMMQSC로 관리자가 로컬 큐 관리자에게 MQSC 명령을 발행할 수 있습니다.

IBM MQ for IBM i에서 제공되는 CL 명령의 두 그룹이 있습니다.

그룹 1

이 범주의 명령을 발행하려면 사용자가 QMQMADM 그룹의 구성원이거나 *ALLOBJ 권한이 있어야 합니다. 예를 들면 GRTRMQMAUT 및 STRTRMQMMQSC가 이 범주에 속합니다.

그룹 2

이 범주의 명령을 발행하려면 사용자가 QMQMADM 그룹의 구성원이거나 *ALLOBJ 권한이 있어야 합니다. 대신 두 레벨의 권한이 필요합니다.

- 명령을 사용하려면 사용자에게는 IBM i 권한이 필요합니다. 이 권한은 GRTOBJAUT 명령을 사용하여 부여가 가능합니다.
- 명령에 연관된 임의 IBM MQ 오브젝트에 액세스하려면 IBM MQ 권한이 필요합니다. 이 권한은 GRTRMQMAUT 명령으로 부여됩니다.

다음 예에서는 이 그룹의 명령을 보여줍니다.

- CRTMQMQ, MQM 큐 작성
- CHGMQMPRC, MQM 프로세스 변경
- DLTMQMNL, MQM 이름 목록 삭제
- DSPMQMAUTI, MQM 인증 정보 표시
- CRTMQMCHL, MQM 채널 작성

이 명령 그룹에 대한 자세한 정보는 78 페이지의 『애플리케이션에서 IBM MQ를 사용하기 위한 권한 부여』의 내용을 참조하십시오.

그룹 1과 그룹 2 명령의 전체 목록은 139 페이지의 『IBM i의 IBM MQ 오브젝트에 대한 액세스 권한』의 내용을 참조하십시오.

IBM i에서 IBM MQ를 관리하는 데 필요한 권한에 대한 자세한 정보는 [IBM i 관리](#)를 참조하십시오.

▶ z/OS z/OS에서 IBM MQ를 관리하는 권한

이 주제 모음에서는 IBM MQ for z/OS 관리에 필요한 다양한 권한의 관점에 대해 설명합니다.

▶ z/OS z/OS에서 권한 검사

IBM MQ for z/OS SAF(System Authorization Facility)를 사용하여 권한 검사에 대한 요청을 z/OS Security Server Resource Access Control Facility(RACF)와 같은 외부 보안 관리자(ESM)로 라우트합니다. IBM MQ는 자체적으로 권한 검사를 수행하지 않습니다.

ESM으로 RACF를 사용 중이라고 가정합니다. 다른 ESM을 사용 중인 경우 사용자의 ESM에 연관된 방식으로 RACF에 대해 제공되는 정보를 해석해야 할 수도 있습니다.

각 큐 관리자에 대해 개별적으로 또는 큐 공유 그룹의 모든 큐 관리자에 대해 권한 검사를 사용하는지 여부를 지정할 수 있습니다. 이 제어 레벨을 서브시스템 보안이라고 합니다. 특정 큐 관리자에 대해 서브시스템 보안을 사용하지 않도록 설정하면, 해당 큐 관리자에 대해 권한 검사를 수행하지 않습니다.

특정 큐 관리자에 대해 서브시스템 보안을 사용하도록 설정하면, 권한 검사를 다음 두 레벨로 수행할 수 있습니다.

큐 공유 그룹 레벨 보안

권한 검사는 큐 공유 그룹의 모든 큐 관리자가 공유하는 RACF 프로파일을 사용합니다. 이는 정의하고 유지보수할 프로파일이 더 적기 때문에 보안 관리가 더 쉬워지는 것을 의미합니다.

큐 관리자 레벨 보안

권한 검사는 큐 관리자에 특정되는 RACF 프로파일을 사용합니다.

큐 공유 그룹과 큐 관리자 레벨 보안의 결합을 사용할 수 있습니다. 예를 들어, 큐 관리자가 속하는 큐 공유 그룹의 프로파일을 대체하기 위해 큐 관리자에만 특정되는 프로파일을 배열할 수 있습니다.

서브시스템 보안, 큐 공유 그룹 레벨 보안, 큐 관리자 레벨 보안은 스위치 프로파일을 정의하여 이를 켜거나 끕니다. 스위치 프로파일은 IBM MQ에 특별한 의미가 있는 일반 RACF 프로파일입니다.

z/OS z/OS의 명령 보안과 명령 자원 보안

명령 보안은 명령 발행 권한에 연관됩니다. 명령 자원 권한은 자원에서 조작을 수행하는 권한에 연관됩니다. 둘 다 RACF 클래스를 사용하여 구현됩니다.

권한 검사는 IBM MQ 관리자가 MQSC 명령을 발행할 때 수행됩니다. 이것을 명령 보안이라 합니다.

명령 보안을 구현하려면 특정 RACF 프로파일을 정의하고 필요한 레벨에서 해당 프로파일에 대한 액세스를 필요한 그룹 및 사용자 ID에 부여해야 합니다. 명령 보안에 대한 프로파일의 이름은 MQSC 명령의 이름을 가집니다.

일부 MQSC 명령은 IBM MQ 자원에서 조작을 수행합니다(예: 로컬 큐를 작성하는 DEFINE QLOCAL 명령). 관리자가 MQSC 명령을 발행하면 권한 검사는 요청된 조작이 명령에 지정된 자원에서 수행한지를 판별하기 위해 수행됩니다. 이를 명령 자원 보안이라 합니다.

명령 자원 보안을 구현하려면 특정 RACF 프로파일을 정의하고 필요한 레벨에서 해당 프로파일에 대한 액세스를 필요한 그룹 및 사용자 ID에 부여해야 합니다. 명령 자원 보안의 프로파일 이름에는 IBM MQ 자원 이름 및 해당 유형(Queue, Process, Namelist, Topic, Authinfo 또는 Channel)이 포함됩니다.

명령 보안 및 명령 자원 보안은 독립적입니다. 예를 들어, 관리자가

```
DEFINE QLOCAL(MOON.EUROPA)
```

명령을 발행하면, 다음 권한 검사가 수행됩니다.

- 명령 보안이 관리자에게 DEFINE QLOCAL 명령을 발행할 수 있는 권한이 부여되었는지 검사합니다.
- 명령 자원 보안이 관리자에게 MOON.EUROPA라는 로컬 큐에서 조작을 수행할 수 있는 권한이 부여되었는지 검사합니다.

명령 보안과 명령 자원 보안은 스위치 프로파일을 정의하여 사용하거나 사용하지 않도록 설정할 수 있습니다.

z/OS z/OS에서 MQSC 명령 및 시스템 명령 입력 큐

이 주제를 사용하여 z/OS에서 명령 서버가 시스템 명령 입력 큐로 향하는 MQSC 명령을 처리하는 방법을 이해하십시오.

명령 서버가 시스템 명령 입력 큐로부터 MQSC 명령을 포함하는 메시지를 검색할 때도 명령 보안과 명령 자원 보안이 사용됩니다. 권한 검사를 위해 사용되는 사용자 ID는 메시지가 MQSC 명령을 포함하는 메시지 디스크립터의 *UserIdentifier* 필드에서 찾은 사용자 ID입니다. 이 사용자 ID는 명령이 처리되는 큐 관리자에서 필수 권한을 가져야 합니다. *UserIdentifier* 필드 및 설정 방법에 대한 자세한 정보는 [메시지 컨텍스트](#)를 참조하십시오.

MQSC 명령이 있는 메시지는 다음 상황에서 시스템 명령 입력 큐로 송신됩니다.

- 조작 및 제어판이 MQSC 명령을 대상 큐 관리자의 시스템 명령 입력 큐로 송신합니다. MQSC 명령은 패널에서 선택하는 조치에 해당합니다. 각 메시지의 *UserIdentifier* 필드는 관리자의 TSO 사용자 ID로 설정됩니다.
- IBM MQ 유틸리티 프로그램 CSQUTIL의 COMMAND 함수는 입력 데이터 세트의 MQSC 명령을 대상 큐 관리자의 시스템 명령 입력 큐로 송신합니다. COPY와 EMPTY 함수는 DISPLAY QUEUE와 DISPLAY STGCLASS 명령을 송신합니다. 각 메시지의 *UserIdentifier* 필드는 작업 사용자 ID로 설정됩니다.
- CSQINPX 데이터 세트의 MQSC 명령은 채널 시작기가 연결되어 있는 큐 관리자의 시스템 명령 입력 큐로 송신됩니다. 각 메시지의 *UserIdentifier* 필드는 채널 시작기 주소 공간 사용자 ID로 설정됩니다.

MQSC 명령이 CSQINP1과 CSQINP2 데이터 세트로부터 발행되면 권한 검사가 수행되지 않습니다. RACF 데이터 세트 보호를 사용하여 해당 데이터 세트를 업데이트할 수 있는 사용자를 제어할 수 있습니다.

- 큐 공유 그룹 내에서 채널 시작기는 START CHANNEL 명령을 연결된 큐 관리자의 시스템 명령 입력 큐로 송신할 수 있습니다. 공유 전송 큐를 사용하는 아웃바운드 채널이 트리거링으로 시작될 때 명령이 송신됩니다. 각 메시지의 *UserIdentifier* 필드는 채널 시작기 주소 공간 사용자 ID로 설정됩니다.
- 애플리케이션은 MQSC 명령을 시스템 명령 입력 큐로 송신할 수 있습니다. 기본적으로 각 메시지의 *UserIdentifier* 필드는 애플리케이션에 연관된 사용자 ID로 설정됩니다.

- UNIX, Linux, and Windows 시스템에서 **runmqsc** 제어 명령은 MQSC 명령을 z/OS에서 큐 관리자의 시스템 명령 입력 큐로 송신하는 간접 모드에서 사용 가능합니다. 각 메시지의 *UserIdentifier* 필드는 **runmqsc** 명령을 발행한 관리자의 사용자 ID로 설정됩니다.

z/OS

z/OS에서 큐 관리자 데이터 세트에 액세스

IBM MQ for z/OS 관리자에게는 큐 관리자 데이터 세트 액세스 권한이 있어야 합니다. 이 토픽을 사용하여 RACF 보호가 필요한 데이터 세트에 대해 이해하십시오.

해당 데이터 세트에는 다음이 포함됩니다.

- **V9.1.0** 큐 관리자의 시작된 태스크 프로시저에서 CSQINP1, CSQINP2 및 CSQINP로 참조되는 데이터 세트.
- 큐 관리자의 페이지 세트, 활성 로그 데이터 세트, 아카이브 로그 데이터 세트, 부트스트랩 데이터 세트(BSDS)
- 채널 시작기의 시작된 작업 프로시저에 있는 CSQXLIB 및 CSQINPX에 의해 참조되는 데이터 세트

권한이 부여되지 않은 사용자가 큐 관리자를 시작하거나 모든 큐 관리자 데이터에 대한 액세스를 얻을 수 있으면 데이터 세트를 보호해야 합니다. 그러려면 RACF 데이터 세트 보호를 사용하십시오.

애플리케이션에서 IBM MQ를 사용하기 위한 권한 부여

애플리케이션이 오브젝트에 액세스하는 경우 애플리케이션에 연관되는 사용자 ID에는 적절한 권한이 있어야 합니다.

애플리케이션은 MQI 호출을 발행하여 다음 IBM MQ 오브젝트에 액세스할 수 있습니다.

- 큐 관리자
- 큐
- Processes
- 이름 목록
- 토픽

애플리케이션은 PCF 명령을 사용하여 IBM MQ 오브젝트를 관리할 수도 있습니다. PCF 명령이 처리되면 PCF 메시지를 넣는 사용자 ID의 권한 컨텍스트를 사용합니다.

이 컨텍스트에서 애플리케이션은 사용자 및 벤더가 기록한 항목 및 IBM MQ for z/OS에서 제공되는 항목도 포함합니다. IBM MQ for z/OS에서 제공하는 애플리케이션에는 다음이 포함됩니다.

- 조작 및 제어판
- IBM MQ 유틸리티 프로그램, CSQUTIL
- 데드-레터 큐 핸들러 유틸리티인 CSQUDLQH

IBM MQ classes for Java, IBM MQ classes for JMS, IBM MQ classes for .NET 또는 C/C++ 및 .NET용 메시지 서비스 클라이언트를 사용하는 애플리케이션은 MQI를 간접적으로 사용합니다.

MCA는 MQI 호출을 발행하고 MCA에 연관된 사용자 ID는 해당 IBM MQ 오브젝트에 액세스하는 권한이 있어야 합니다. 이 사용자 ID와 필요한 권한에 대한 자세한 정보는 [96 페이지의 『채널 권한 부여』](#)의 내용을 참조하십시오.

z/OS에서 애플리케이션은 MQSC 명령을 사용하여 해당 IBM MQ 오브젝트에 액세스할 수는 있지만 명령 보안 및 명령 자원 보안은 이런 상황에서 권한 검사를 제공합니다. **z/OS** 자세한 정보는 [77 페이지의 『z/OS의 명령 보안과 명령 자원 보안』](#) 및 [77 페이지의 『z/OS에서 MQSC 명령 및 시스템 명령 입력 큐』](#)의 내용을 참조하십시오.

IBM i에서 그룹 2에서 CL 명령을 발행하는 사용자의 경우 명령에 연관된 IBM MQ 오브젝트 액세스 권한이 필요할 수도 있습니다. 자세한 정보는 [78 페이지의 『권한 검사가 수행되는 시기』](#)의 내용을 참조하십시오.

권한 검사가 수행되는 시기

권한 검사는 애플리케이션이 큐 관리자, 큐, 프로세스 또는 이름 목록에 액세스를 시도할 때 수행됩니다.

IBM i에서 권한 검사는 이 IBM MQ 오브젝트 중 임의의 오브젝트에 액세스하는 그룹 2에서 CL 명령을 발행할 때 수행될 수도 있습니다. 다음과 같은 상황에서 검사가 수행됩니다.

애플리케이션이 MQCONN 또는 MQCONNX 호출을 사용하여 큐 관리자에 연결하는 경우

큐 관리자가 애플리케이션에 연관된 사용자 ID를 운영 체제에 요청하는 경우. 그러면 큐 관리자는 사용자 ID에 연결 권한이 있는지 및 이후 검사를 위한 사용자 ID를 보유하고 있는지를 검사합니다.

사용자는 IBM MQ에 사인온할 필요는 없습니다. IBM MQ에서는 사용자가 근본적인 운영 체제에 사인온하고 이미 인증되었다고 간주합니다.

애플리케이션이 MQOPEN 또는 MQPUT1 호출을 사용하여 IBM MQ 오브젝트를 열 때

모든 권한 검사는 나중에 액세스할 때가 아니라 오브젝트를 열 때 수행됩니다. 예를 들어, 권한 검사는 애플리케이션이 큐를 열 때 수행됩니다. 애플리케이션이 큐에 메시지를 넣거나 큐에서 메시지를 가져올 때는 수행되지 않습니다.

애플리케이션이 오브젝트를 열 때, 오브젝트에서 수행해야 하는 조作的 유형을 지정합니다. 예를 들어, 애플리케이션이 큐를 열어 큐 안의 메시지를 찾아보거나 메시지를 가져오기만 하고, 메시지를 넣지는 않을 수 있습니다. 조作的 유형별로 큐 관리자는 애플리케이션에 연관된 사용자 ID에 해당 조작을 수행할 권한이 있는지 검사합니다.

애플리케이션이 큐를 열 때 권한 검사가 오브젝트 디스크립터의 ObjectName 필드에 이름 지정된 오브젝트에 대해 수행됩니다. ObjectName 필드는 MQOPEN 또는 MQPUT1 호출에서 사용됩니다. 오브젝트가 알리어스 큐 또는 리모트 큐 정의인 경우, 권한 검사는 오브젝트 자체에 대해 수행됩니다. 알리어스 큐나 리모트 큐 정의가 해결되는 큐에서 수행되지 않습니다. 이는 사용자가 여기에 액세스할 권한이 필요하지 않음을 의미합니다. 큐 작성 권한을 권한이 있는 사용자로 제한하십시오. 그렇게 하지 않으면 사용자가 알리어스를 작성하는 것만으로 일반 액세스 제어를 무시할 수도 있습니다.

애플리케이션은 리모트 큐를 명확하게 참조할 수 있습니다. 이는 오브젝트 디스크립터의 ObjectName 및 ObjectQMgrName 필드를 리모트 큐 및 리모트 큐 관리자 이름으로 설정합니다. 권한 검사는 리모트 큐 관리자와 동일한 이름의 전송 큐에 대해 수행됩니다. z/OS에서는 리모트 큐 관리자 이름과 일치하는 RACF 큐 프로파일에 검사 수행합니다. 멀티플랫폼에서는 클러스터링이 사용되는 경우 리모트 큐 관리자 이름과 일치하는 RQMNAME 프로파일에 대해 검사를 수행합니다. 오브젝트 디스크립터에서 ObjectName 필드를 클러스터 큐의 이름으로 설정하여 애플리케이션이 클러스터 큐를 명시적으로 참조할 수 있습니다. 권한 검사는 클러스터 전송 큐 SYSTEM.CLUSTER.TRANSMIT.QUEUE에 대해 수행됩니다.

동적 큐의 권한은 도출된 모델 큐를 기반으로 하지만 동일할 필요는 없습니다. 참고 1을 참조하십시오.

큐 관리자가 권한 검사에 사용하는 사용자 ID는 운영 체제에서 확보합니다. 사용자 ID는 애플리케이션이 큐 관리자에 연결될 때 확보합니다. 적절히 권한이 부여된 애플리케이션은 대체 사용자 ID를 지정하는 MQOPEN 호출을 발행할 수 있습니다. 그런 다음 대체 사용자 ID에 대해 액세스 제어 검사를 수행합니다. 대체 사용자 ID의 사용은 애플리케이션과 연관된 사용자 ID를 변경하지 않으며 액세스 제어 검사에 사용된 사용자 ID만 변경됩니다.

애플리케이션에서 MQSUB 호출을 사용하여 토픽을 구독할 때

애플리케이션이 토픽을 구독할 때 이는 수행해야 할 조作的 유형을 지정합니다. 이는 구독을 작성, 기존 구독 수정 또는 기존 구독을 변경하지 않고 재개합니다. 조作的 유형마다 큐 관리자는 애플리케이션에 연관된 사용자 ID에 해당 조작을 수행할 권한이 있는지 검사합니다.

애플리케이션이 토픽을 구독할 때 권한 검사는 토픽 트리에 있는 토픽 오브젝트에 대해 수행됩니다. 토픽 오브젝트는 애플리케이션이 구독하는 토픽 트리 지점 이상에 있습니다. 권한 검사에는 둘 이상의 토픽 오브젝트에 대한 검사가 포함될 수 있습니다. 큐 관리자가 권한 검사에 사용하는 사용자 ID는 운영 체제에서 확보합니다. 사용자 ID는 애플리케이션이 큐 관리자에 연결될 때 확보합니다.

큐 관리자는 관리 큐가 아니라 구독자 큐에서 권한 검사를 수행합니다.

애플리케이션이 MQCLOSE 호출을 사용하여 영구적 동적 큐를 삭제하는 경우

MQCLOSE 호출에 지정되는 오브젝트 핸들은 영구적 동적 큐를 작성한 MQOPEN 호출에서 리턴되는 것과 동일할 필요는 없습니다. 다른 경우, 큐 관리자는 MQCLOSE 호출을 발행한 애플리케이션에 연관된 사용자 ID를 검사합니다. 사용자 ID가 큐를 삭제할 권한이 있는지 검사합니다.

제거를 위해 구독을 담은 애플리케이션이 이를 작성하지 않으면 제거에 필요한 적절한 권한이 필요합니다.

IBM MQ 오브젝트에서 운영되는 PCF 명령이 명령 서버로 처리되는 경우

이 규칙에는 PCF 명령이 인증 정보 오브젝트에서 운영되는 경우를 포함합니다.

권한 검사에 사용되는 사용자 ID는 PCF 명령의 메시지 디스크립터에서 `UserIdentifier` 필드에 있는 사용자 ID입니다. 이 사용자 ID는 명령이 처리되는 큐 관리자에서 필수 권한을 가져야 합니다. 이스케이프 PCF 명령 안에 캡슐화되어 있는 동등한 MQSC 명령은 같은 방식으로 처리됩니다. `UserIdentifier` 필드에 대한 자세한 정보 및 설정 방법에 대한 정보는 80 페이지의 『메시지 컨텍스트』의 내용을 참조하십시오.

IBM i IBM i에서 사용자가 IBM MQ 오브젝트를 조작하는 그룹 2의 CL 명령을 발행하는 경우

이 규칙에는 그룹 2의 CL 명령이 인증 정보 오브젝트에서 운영되는 경우가 포함됩니다.

검사는 사용자가 명령에 연관된 IBM MQ 오브젝트에서 조작할 권한이 있는지 판별하기 위해 수행됩니다. 사용자가 `QMADM` 그룹의 구성원이거나 `*ALLOBJ` 권한이 있는 경우를 제외하고는 검사가 수행됩니다. 필요한 권한은 오브젝트에 대해 명령이 수행하는 조작 유형에 따라 다릅니다. 예를 들어, `CHGMQM`(MQM 큐 변경) 명령은 명령이 지정하는 큐의 속성을 변경할 수 있는 권한을 필요로 합니다. 반대로, `DSPMQM`(MQM 큐 표시) 명령은 명령이 지정하는 큐의 속성을 표시할 수 있는 권한을 필요로 합니다.

여러 명령이 둘 이상의 오브젝트에 대해 작용합니다. 예를 들어, `DLTMQM`(MQM 큐 삭제) 명령을 발행하려면 다음 권한이 필요합니다.

- 명령에 의해 지정된 큐 관리자에 연결할 수 있는 권한
- 명령에 의해 지정된 큐를 삭제할 수 있는 권한

일부 명령은 오브젝트에 전혀 작용하지 않습니다. 이 경우 사용자에게는 이러한 명령 중 하나를 실행할 수 있는 IBM i 권한만 필요합니다. `STRMQLSR`, MQM 리스너를 시작한다.

대체 사용자 권한

애플리케이션이 오브젝트를 열거나 토픽을 구독하는 경우, 애플리케이션은 `MQOPEN`, `MQPUT1` 또는 `MQSUB` 호출에 사용자 ID를 제공할 수 있습니다. 큐 관리자가 이 사용자 ID를 애플리케이션에 연관된 사용자 ID 대신 권한 검사에 사용하도록 요청할 수 있습니다.

다음 두 조건이 모두 충족된 경우에만 애플리케이션이 오브젝트를 열 수 있습니다.

- 애플리케이션에 연관된 사용자 ID가 권한 검사를 위해 다른 사용자 ID를 제공할 수 있는 권한을 가집니다. 애플리케이션은 대체 사용자 권한이 있는 것으로 언급됩니다.
- 애플리케이션에서 제공한 사용자 ID에는 요청된 조작의 유형에 맞게 오브젝트를 열거나 토픽을 구독할 권한이 있습니다.

메시지 컨텍스트

메시지 컨텍스트 정보를 사용하여 메시지를 검색하는 애플리케이션이 메시지의 진원지를 알 수 있습니다. 정보는 메시지 디스크립터의 필드에 보유하고 필드는 세 개의 논리 파트로 분할됩니다.

해당 파트는 다음과 같습니다.

ID 컨텍스트(identity context)

이 필드는 메시지를 큐에 넣는 애플리케이션의 사용자 정보를 포함합니다.

원본 컨텍스트

이 필드는 애플리케이션 자체에 대한 정보 및 메시지가 큐에 추가되는 시기에 대한 정보를 포함합니다.

사용자 컨텍스트

이러한 필드에는 애플리케이션에서 큐 관리자가 전달해야 하는 메시지를 선택하는 데 사용할 수 있는 메시지 특성이 포함됩니다.

애플리케이션이 메시지를 큐에 넣을 때, 애플리케이션은 큐 관리자에게 메시지에 컨텍스트 정보를 생성하도록 요청할 수 있습니다. 이것이 기본 조치입니다. 또는, 컨텍스트 필드가 정보를 포함하지 않도록 지정할 수 있습니다. 애플리케이션과 연관된 사용자 ID는 이를 수행하기 위한 특별한 권한을 필요로 하지 않습니다.

애플리케이션이 ID 컨텍스트 필드를 메시지에 설정할 수 있으면, 큐 관리자가 원본 컨텍스트를 생성할 수 있거나, 모든 컨텍스트 필드를 설정할 수 있습니다. 애플리케이션이 검색한 메시지로부터 큐에 넣고 있는 메시지로 ID 컨텍스트 필드를 전달하거나, 모든 컨텍스트 필드를 전달할 수 있습니다. 그렇지만 애플리케이션에 연관된 사용자 ID는 컨텍스트 정보를 설정하거나 전달하는 데 권한을 필요로 하지 않습니다. 애플리케이션이 메시지를 넣기 직전의 큐를 열 때 컨텍스트 정보를 설정하거나 전달하려고 하는지를 지정하고, 그에 대한 권한이 이 때에 검사됩니다.

다음은 컨텍스트 필드 각각에 대한 간단한 설명입니다.

ID 컨텍스트

UserIdentifier

메시지를 넣는 애플리케이션에 연관된 사용자 ID. 큐 관리자가 이 필드를 설정하면, 애플리케이션이 큐 관리자에 연결될 때 운영 체제에서 확보한 사용자 ID로 설정됩니다.

AccountingToken

메시지의 결과로 완료된 작업에 청구하는 데 사용할 수 있는 정보.

ApplIdentityData

애플리케이션에 연관된 사용자 ID가 ID 컨텍스트 필드를 설정하거나 모든 컨텍스트 필드를 설정할 수 있는 권한을 가지면, 애플리케이션이 이 필드를 ID에 관련된 임의 값으로 설정할 수 있습니다. 큐 관리자가 이 필드를 설정하면, 공백으로 설정됩니다.

원본 컨텍스트

PutApplType

메시지를 넣는 애플리케이션 유형(예: CICS® 트랜잭션).

PutApplName

메시지를 넣는 애플리케이션 이름.

PutDate

메시지를 넣은 날짜.

PutTime

메시지를 넣은 시간.

ApplOriginData

애플리케이션에 연관된 사용자 ID가 모든 컨텍스트 필드를 설정할 수 있는 권한을 가지면, 애플리케이션이 이 필드를 원본에 관련된 임의 값으로 설정할 수 있습니다. 큐 관리자가 이 필드를 설정하면, 공백으로 설정됩니다.

사용자 컨텍스트

다음 값은 MQINQMP 또는 MQSETMP에 대해 지원됩니다.

MQPD_USER_CONTEXT

특성은 사용자 컨텍스트와 연관됩니다.

MQSETMP 호출을 사용하여 사용자 컨텍스트와 연관된 특성을 설정할 수 있는 특수 권한은 필요하지 않습니다.

V7.0 또는 후속 큐 관리자에서 사용자 컨텍스트에 연관된 특성은 MQOO_SAVE_ALL_CONTEXT에 대해 설명된 대로 저장됩니다. MQOO_PASS_ALL_CONTEXT가 지정된 MQPUT를 통해 특성이 저장된 컨텍스트에서 새 메시지로 복사됩니다.

MQPD_NO_CONTEXT

특성은 메시지 컨텍스트와 연관되지 않습니다.

인식할 수 없는 값은 MQRC_PD_ERROR로 거부됩니다. 이 필드의 초기값은 MQPD_NO_CONTEXT입니다.

각 컨텍스트 필드에 대한 자세한 정보는 [MQMD - 메시지 디스크립터](#)를 참조하십시오. 메시지 컨텍스트 사용 방법에 대한 자세한 정보는 [메시지 컨텍스트](#)를 참조하십시오.

IBM i, UNIX, Linux, and Windows 시스템에서 IBM

MQ 오브젝트에 대한 작업 권한

IBM MQ에서 제공되는 권한 서비스 컴포넌트는 오브젝트 권한 관리자(OAM)라고 합니다. 이는 인증 및 권한 검사를 통해 액세스 제어를 제공합니다.

인증.

IBM MQ에서 제공되는 OAM이 수행하는 인증 검사는 기본이며 특정 상황에서만 수행됩니다. 매우 안전한 환경에서 예상되는 엄격한 요구사항을 충족시키기 위한 것은 아닙니다.

OAM은 애플리케이션이 큐 관리자에 연결되고 다음 조건에 해당될 때 인증 검사를 수행합니다.

- MQCSP 구조가 연결 애플리케이션에 연결 애플리케이션에서 제공되었습니다. 그리고

- MQCSP 구조의 *AuthenticationType* 속성에 MQCSP_AUTH_USER_ID_AND_PWD 값이 지정되었습니다. 그리고
- 구성된 AUTHINFO 오브젝트의 CHCKLOCL 또는 CHKCCLNT 값이 'NONE' 이 아닙니다.

OAM의 인증 단계에서는 운영 체제 서비스를 사용하여 비밀번호의 유효성을 검증합니다. 운영 체제 서비스는 사용자 이름에서 올바르지 않은 비밀번호 테스트를 너무 많이 시도하지 않았는지 확인하는 등의 추가 검사를 수행하도록 구성되었을 수 있습니다.

새 인증 서비스 컴포넌트를 작성하거나 공급업체로부터 확보하는 경우 대체 인증 메커니즘을 사용할 수 있습니다.

권한 부여.

권한 검사는 포괄적이며 대부분의 일반 요구사항을 충족시키기 위해 수행됩니다.

권한 검사는 애플리케이션이 큐 관리자, 큐, 프로세스, 토픽 또는 이름 목록 액세스를 위해 MQI 호출을 발하는 경우에 수행됩니다. 이는 명령 서버로 명령이 수행 중인 경우처럼 다른 상황에서도 수행됩니다.

IBM i IBM i, UNIX, Linux, and Windows 시스템에서, 권한 서비스는 애플리케이션이 큐 관리자, 큐, 프로세스, 토픽 또는 이름 목록인 IBM MQ 오브젝트에 액세스하는 MQI 호출을 발생할 때 액세스 제어를 제공합니다. 여기에는 대체 사용자 권한 및 컨텍스트 정보 설정 또는 전달 권한에 대한 검사가 포함됩니다.

Windows Windows에서 OAM은 관리 그룹 구성원에서 모든 IBM MQ 오브젝트 액세스 권한을 부여하며 UAC가 사용되는 경우도 포함됩니다. 또한 Windows 시스템에서 SYSTEM 계정에는 IBM MQ 자원에 대한 전체 액세스 권한이 있습니다.

권한 서비스는 PCF 명령이 다음 IBM MQ 오브젝트 중 하나 또는 인증 정보 오브젝트에서 수행되는 경우에도 권한 검사를 제공합니다. 이스케이프 PCF 명령 안에 캡슐화되어 있는 동등한 MQSC 명령은 같은 방식으로 처리됩니다.

IBM i IBM i에서 사용자가 QMQADM 그룹의 구성원이거나 *ALLOBJ 권한을 가진 경우를 제외하고는 권한 서비스는 IBM MQ 오브젝트 또는 인증 정보 오브젝트에서 조작되는 그룹 2에서 CL 명령을 사용자가 발행하는 경우에도 권한 검사를 제공합니다.

권한 서비스는 설치 가능 서비스이며, 이는 하나 이상의 설치 가능 서비스 구성요소에 의해 구현된다는 것을 의미합니다. 각 컴포넌트는 문서화된 인터페이스를 사용하여 호출됩니다. 이를 사용하면 사용자 및 벤더가 IBM MQ 제품에서 제공되는 컴포넌트를 기능 보강하거나 대체하기 위해 컴포넌트를 제공할 수 있습니다.

IBM MQ에서 제공되는 권한 서비스 컴포넌트는 오브젝트 권한 관리자(OAM)라고 합니다. OAM은 작성하는 각 큐 관리자에 자동으로 사용 가능하게 되어 있습니다.

OAM은 액세스를 제어 중인 각 IBM MQ 오브젝트에 대해 액세스 제어 목록(ACL)을 유지보수합니다. UNIX and Linux 시스템에서 그룹 ID만 ACL에 표시 가능합니다. 이는 그룹의 모든 구성원에 같은 권한이 있다는 것을 의미합니다.

IBM i IBM i 및 Windows 시스템에서는 사용자 ID와 그룹 ID 모두 ACL에 표시 가능합니다. 이는 권한이 개별 사용자 및 그룹에 부여될 수 있음을 의미합니다.

12자 제한은 그룹 및 사용자 ID 모두에 적용됩니다. 일반적으로, UNIX 플랫폼은 사용자 ID의 길이를 12자로 제한합니다. AIX® 및 Linux에서는 이러한 제한이 약화되었지만, IBM MQ는 계속해서 모든 UNIX 플랫폼에 대해 12자 제한을 적용합니다. 12자보다 많은 사용자 ID를 사용하면 IBM MQ는 이를 "UNKNOWN" 값으로 바꿉니다. 사용자 ID를 "UNKNOWN" 값으로 정의하지 마십시오.

OAM은 사용자를 인증하고 적절한 ID 컨텍스트 필드를 변경할 수 있습니다. MQCONNX 호출에서 연결 보안 매개 변수 구조(MQCSP)를 지정하여 이를 사용 가능하게 할 수 있습니다. 이 구조는 적절한 ID 컨텍스트 필드를 설정하는 OAM 인증 사용자 함수(MQZ_AUTHENTICATE_USER)에 전달됩니다. MQCONNX 연결이 IBM MQ 클라이언트에서의 연결인 경우, MQCSP의 정보가 클라이언트 연결 및 서버 연결 채널을 통해 클라이언트가 연결되는 큐 관리자로 플로우됩니다. 보안 엑시트가 해당 채널에 정의되면 MQCSP가 각 보안 엑시트로 전달되고 엑시트에 의해 변경될 수 있습니다. 보안 엑시트가 MQCSP를 작성할 수도 있습니다. 이 컨텍스트에서 보안 엑시트 사용에 대한 자세한 정보는 채널 보안 엑시트 프로그램을 참조하십시오.

경고: 일부 경우에 클라이언트 애플리케이션에 대한 MQCSP 구조의 비밀번호는 일반 텍스트로 네트워크 전체에 전송됩니다. 클라이언트 애플리케이션 비밀번호가 적절하게 보호될 수 있도록 하려면 IBM MQCSP 비밀번호 보호를 참조하십시오.

UNIX, Linux, Windows 시스템에서 제어 명령 **setmqaut**는 권한 부여 및 취소하고 ACL 유지보수에 사용됩니다. 예를 들어,

```
setmqaut -m JUPITER -t queue -n MOON.EUROPA -g VOYAGER +browse +get
```

명령은 그룹 VOYAGER의 구성원이 큐 관리자 JUPITER가 소유하는 큐 MOON.EUROPA에 있는 메시지를 볼 수 있게 합니다. 구성원들이 큐에서 메시지를 가져오게도 합니다. 이 권한을 나중에 취소하려면 다음 명령을 입력하십시오.

```
setmqaut -m JUPITER -t queue -n MOON.EUROPA -g VOYAGER -browse -get
```

:NONE.

```
setmqaut -m JUPITER -t queue -n MOON.* -g VOYAGER +put
```

이는 그룹 VOYAGER의 구성원이 MOON. 문자로 시작되는 이름의 임의 큐에 메시지를 넣도록 허용합니다. MOON.* 은 일반 프로파일의 이름이다. 일반 프로파일을 사용하면 단일 **setmqaut** 명령을 사용하여 오브젝트 세트에 대한 권한을 부여할 수 있습니다.

제어 명령 **dspmqaut**는 사용자 또는 그룹이 지정된 오브젝트에 대해 갖는 현재 권한을 표시할 수 있습니다. 제어 명령 **dmpmqaut**도 일반 프로파일에 연관된 현재 권한을 표시하는 데 사용 가능합니다.

IBM i IBM i에서 관리자는 CL 명령 GRTMQMAUT를 사용하여 권한을 부여하고 CL 명령 RVKMQMAUT를 사용하여 권한을 취소합니다. 일반 프로파일도 마찬가지로 사용될 수 있습니다. 예를 들어, CL 명령:

```
GRTMQMAUT MQMNAME(JUPITER) OBJTYPE(*Q) OBJ('MOON.*') USER(VOYAGER) AUT(*PUT)
```

setmqaut 명령의 이전 예제와 동일한 기능을 제공합니다. 그룹 VOYAGER의 구성원이 MOON. 문자로 시작하는 이름을 사용하여 큐에 메시지를 넣을 수 있습니다.

IBM i CL 명령 DSPMQMAUT는 사용자 또는 그룹이 지정된 오브젝트에 대해 갖는 현재 권한을 표시합니다. CL 명령 WRKMQMAUT와 WRKMQMAUTD는 오브젝트 및 일반 프로파일과 연관된 현재 권한에 대해서도 작업할 수 있습니다.

권한 검사를 하지 않는 경우(예를 들어, 테스트 환경), OAM을 사용하지 않을 수 있습니다.

Multi PCF를 사용하여 OAM 명령에 액세스
IBM i, UNIX, Linux, and Windows 시스템에서는 PCF 명령을 사용하여 OAM 관리 명령에 액세스할 수 있습니다. PCF 명령과 대응되는 OAM 명령은 다음과 같습니다.

표 8. PCF 명령 및 대응되는 OAM 명령	
PCF 명령	OAM 명령
권한 레코드 조회	dmpmqaut
엔티티 권한 조회	dspmqaut
권한 레코드 설정	setmqaut
권한 레코드 삭제	-remove 옵션이 포함된 setmqaut

setmqaut 및 **dmpmqaut** 명령은 mqm 그룹의 구성원으로 제한됩니다. 대응되는 PCF 명령은 큐 관리자에 대해 dsp 및 chg 권한이 부여된 그룹의 사용자만 실행할 수 있습니다.

해당 명령 사용에 대한 자세한 정보는 [프로그래밍 가능 명령 형식\(PCF\) 소개](#)를 참조하십시오.

z/OS z/OS에서 IBM MQ 오브젝트에 대한 작업 권한

z/OS에서 MQI 호출에 연관되는 권한 검사에는 7개의 범주가 있습니다. 특정 RACF 프로파일을 정의하고 해당 프로파일에 적절한 액세스를 부여해야 합니다. RESLEVEL 프로파일을 사용하여 몇 명의 사용자 ID가 검사되는지를 제어할 수 있습니다.

MQI 호출과 연관된 7개의 권한 검사 범주:

연결 보안

애플리케이션을 큐 관리자에 연결할 때 수행되는 권한 검사

큐 보안

애플리케이션이 큐를 열거나 영구적 동적 큐를 삭제할 때 수행되는 권한 검사

프로세스 보안

애플리케이션이 프로세스 오브젝트를 열 때 수행되는 권한 검사

이름 목록 보안

애플리케이션이 이름 목록 오브젝트를 열 때 수행되는 권한 검사

대체 사용자 보안

오브젝트를 열 때 애플리케이션이 대체 사용자 권한을 요청하는 경우 수행되는 권한 검사

컨텍스트 보안

애플리케이션이 큐를 열고 큐에 넣는 메시지에 컨텍스트 정보를 설정하거나 전달하도록 지정할 때 수행되는 권한 검사

토픽 보안

애플리케이션이 토픽을 열 때 수행되는 권한 검사

각 권한 검사 범주는 명령 보안 및 명령 자원 보안이 구현되는 것과 같은 방식으로 구현됩니다. 특정 RACF 프로파일을 정의하고 필요한 레벨에서 해당 프로파일에 대한 액세스를 필요한 그룹 및 사용자 ID에 부여해야 합니다. 큐 보안의 경우, 액세스의 레벨로 애플리케이션이 큐에서 수행할 수 있는 조作的 유형을 판별합니다. 컨텍스트 보안의 경우 액세스 레벨은 애플리케이션이 수행할 수 있는지 여부를 판별합니다.

- 모든 컨텍스트 필드 전달
- 모든 컨텍스트 필드 전달 및 ID 컨텍스트 필드 설정
- 모든 컨텍스트 필드 전달 및 설정

권한 검사의 각 범주는 스위치 프로파일을 정의하여 켜거나 끌 수 있습니다.

연결 보안을 제외한 모든 범주는 통칭하여 API-자원 보안이라고 합니다.

기본적으로 애플리케이션에서 배치 연결을 사용하여 MQI 호출의 결과로서 API-자원 보안 확인을 수행하면 단 하나의 사용자 ID만이 검사됩니다. 검사는 CICS 또는 IMS 애플리케이션 또는 채널 시작기의 MQI 호출 결과로 수행되는 경우 두 개의 사용자 ID가 검사됩니다.

그러나, RESLEVEL 프로파일을 정의하여 0 - 2개의 사용자 ID가 검사될지를 제어할 수 있습니다. 검사한 사용자 ID 개수는 애플리케이션이 큐 관리자에 연결할 때 연결 유형과 연관된 사용자 ID 및 해당 사용자 ID가 RESLEVEL 프로파일에 대해 가지고 있는 액세스 레벨에 의해 판별됩니다. 각 연결 유형과 연관된 사용자 ID는 다음과 같습니다.

- 배치 연결에 대한 연결 작업의 사용자 ID
- CICS 연결을 위한 CICS 주소 공간 사용자 ID
- IMS 연결을 위한 IMS 지역 주소 공간 사용자 ID
- 채널 시작기 연결을 위한 채널 시작기 주소 공간 사용자 ID

z/OS에서 IBM MQ 오브젝트에 대해 작업할 수 있는 권한에 대한 자세한 정보는 76 페이지의 『z/OS에서 IBM MQ를 관리하는 권한』의 내용을 참조하십시오.

원격 메시징의 보안

이 절에서는 원격 메시징 보안 측면을 다룹니다.

IBM MQ 기능을 사용할 권한을 가진 사용자를 제공해야 합니다. 이 사용자는 오브젝트와 정의에 대해 취해질 조치에 따라 구성됩니다. 예를 들면, 다음과 같습니다.

- 큐 관리자는 권한이 부여된 사용자가 시작하고 중지할 수 있습니다.
- 애플리케이션은 큐 관리자에 연결해야 하며 큐를 사용할 권한이 있어야 합니다.
- 권한 부여된 사용자가 메시지 채널을 작성하고 제어해야 합니다.
- 오브젝트가 라이브러리에 유지되며 이 라이브러리에 대한 액세스가 제한될 수 있습니다.

원격 사이트의 메시지 채널 에이전트는 이 원격 사이트에서 이를 수행하도록 권한을 가진 사용자로부터 생성되어 전달 중인 메시지를 확인합니다. 또한, MCA를 원격으로 시작할 수 있으므로, MCA를 시작하려고 시도하는 원격 프로세스가 이를 수행하도록 권한 부여되었는지 확인해야 할 수 있습니다. 다음 네 가지 방법으로 이를 처리할 수 있습니다.

1. RCVR, RQSTR 또는 CLUSRCVR 채널 정의의 PutAuthority 속성을 적절히 사용하여, 큐에 수신 메시지를 넣을 때 권한 검사를 위해 사용되는 사용자를 제어하십시오. MQSC 명령 참조에서 DEFINE CHANNEL 명령 설명을 참조하십시오.
2. 원하지 않는 연결 시도를 거부하거나 원격 IP 주소, 원격 사용자 ID, 제공된 TLS 주제 식별 이름(DN) 또는 리모트 큐 관리자 이름을 기반으로 하는 MCAUSER 값을 설정하도록 채널 인증 레코드를 구현하십시오.
3. 해당 메시지 채널에 권한이 있는지 확인하는 사용자 엑시트 보안 검사를 구현하십시오. 해당 채널을 호스트하는 설치 보안이 모든 사용자가 적절하게 권한 부여되어 개별 메시지를 검사하지 않아도 되는지 확인하십시오.
4. 사용자 엑시트 메시지 프로세싱을 구현하여 개별 메시지에 대한 권한을 면밀히 조사했는지 확인하십시오.

IBM i IBM MQ for IBM i 오브젝트 보안

이 절에서는 원격 메시지 보안 측면을 다룹니다.

IBM MQ for IBM i 기능을 사용할 권한을 사용자에게 제공해야 합니다. 이 권한은 오브젝트 및 정의에 관련되어 수행되는 조치에 따라 구성됩니다. 예를 들면, 다음과 같습니다.

- 큐 관리자는 권한이 부여된 사용자가 시작하고 중지할 수 있습니다.
- 애플리케이션은 큐 관리자에 연결해야 하며, 큐를 사용할 권한이 있어야 합니다.
- 메시지 채널은 권한이 있는 사용자가 작성하고 제어해야 합니다.

원격 사이트의 메시지 채널 에이전트는 전달 중인 메시지가 이 원격 사이트에서 메시지를 발행하는 권한이 있는 사용자에게 도출되었는지 확인해야 합니다. 또한, MCA를 원격으로 시작할 수 있으므로, MCA를 시작하려고 시도하는 원격 프로세스가 이를 수행하도록 권한 부여되었는지 확인해야 할 수 있습니다. 다음 네 가지 방법으로 이를 처리할 수 있습니다.

- 메시지가 허용 가능한 컨텍스트 권한을 포함해야 함을 채널 정의에서 지정하십시오. 그렇지 않으면 제거됩니다..
- 원하지 않는 연결 시도를 거부하거나 원격 IP 주소, 원격 사용자 ID, 제공된 TLS 식별 이름(DN) 또는 리모트 큐 관리자 이름 중 하나를 기반으로 하는 MCAUSER 값을 설정하도록 채널 인증 레코드를 구현하십시오.
- 해당 메시지 채널에 권한이 있는지 확인하는 사용자 엑시트 보안 검사 구현하십시오. 해당 채널을 호스트하는 설치 보안이 모든 사용자가 적절하게 권한 부여되어 개별 메시지를 검사하지 않아도 되는지 확인하십시오.
- 사용자 엑시트 메시지 처리를 구현하여 개별 메시지에 대한 권한을 면밀히 조사했는지 확인하십시오.

다음은 IBM MQ for IBM i에서 보안을 운영하는 방법에 대한 몇 가지 사실입니다.

- 사용자는 IBM i에서 식별되고 인증됩니다.
- 애플리케이션이 호출하는 큐 관리자 서비스는 큐 관리자 사용자 프로파일의 권한으로 실행되지만 사용자의 프로세스에 있습니다.
- 사용자 명령에서 호출하는 큐 관리자 서비스는 큐 관리자 사용자 프로파일의 권한으로 실행됩니다.

Linux UNIX UNIX and Linux에서 오브젝트의 보안

이 ID가 IBM MQ 관리 명령을 사용하는 경우, 관리 사용자는 시스템에서 mqm 그룹의 파트너야 합니다(루트 포함).

항상 "mqm" 사용자 ID로 amqcrsta를 실행해야 합니다.

UNIX and Linux에서 사용자 ID

큐 관리자는 모든 대문자 또는 대소문자 혼합 사용자 ID를 소문자로 변환합니다. 그런 다음 큐 관리자는 사용자 ID를 메시지의 컨텍스트 부분에 삽입하거나 해당 권한을 검사합니다. 따라서 권한은 소문자 ID만을 기반으로 합니다.

Windows Windows 시스템에서 오브젝트 보안

이 ID가 IBM MQ 관리 명령을 사용하는 경우 관리 사용자는 Windows 시스템의 관리자 그룹 및 mqm 그룹의 일 부여야 합니다.

Windows 시스템의 사용자 ID

Windows 시스템에서 메시지 액시트가 설치되지 않은 경우 큐 관리자는 모든 대문자 또는 대소문자 혼합 사용자 ID를 소문자로 변환합니다. 그런 다음 큐 관리자는 사용자 ID를 메시지의 컨텍스트 부분에 삽입하거나 해당 권한을 검사합니다. 따라서 권한은 소문자 ID만을 기반으로 합니다.

시스템 전체에 걸친 사용자 ID

Windows, UNIX and Linux 시스템 이외의 플랫폼은 메시지에서 사용자 ID에 대해 대문자를 사용합니다.

Windows, UNIX and Linux 시스템이 메시지에서 소문자의 사용자 ID를 사용할 수 있도록 하려면 메시지 채널 에이전트(MCA)가 영문자의 적절한 변환을 수행해야 합니다.

Windows, UNIX and Linux 시스템이 메시지에서 소문자의 사용자 ID를 사용할 수 있도록 하기 위해 다음 변환이 해당 플랫폼의 메시지 채널 에이전트(MCA)에서 수행됩니다.

송신 측에서

메시지 액시트가 설치되지 않은 경우, 모든 사용자 ID의 영문자는 대문자로 변환됩니다.

수신 측에서

메시지 액시트가 설치되지 않은 경우, 모든 사용자 ID의 영문자는 소문자로 변환됩니다.

다른 어떤 이유로 UNIX, Linux, and Windows에서 메시지 액시트를 제공하는 경우, 자동 변환이 수행되지 않습니다.

사용자 정의 권한 서비스 사용

IBM MQ에서는 설치 가능한 권한 서비스를 제공합니다. 대체 서비스 설치를 선택할 수 있습니다.

IBM MQ에서 제공되는 권한 서비스 컴포넌트는 오브젝트 권한 관리자(OAM)라고 합니다. OAM이 필요한 권한 기능을 제공하지 않으면 자체적으로 권한 서비스 컴포넌트를 작성할 수 있습니다. 권한 서비스 컴포넌트로 구현해야 하는 설치 가능한 서비스 함수에 대해서는 [설치 가능 서비스 인터페이스 참조 정보](#)에서 설명됩니다.

클라이언트의 액세스 제어

액세스 제어는 사용자 ID를 기반으로 합니다. 관리할 사용자 ID가 많고 사용자 ID는 다른 형식일 수 있습니다. 서버 연결 채널 특성 MCAUSER를 클라이언트에서 사용되는 특수 사용자 ID 값으로 설정할 수 있습니다.

IBM MQ의 액세스 제어는 사용자 ID를 기반으로 합니다. MQI 호출을 수행하는 프로세스의 사용자 ID가 일반적으로 사용됩니다. MQ MQI 클라이언트의 경우, 서버 연결 MCA는 MQ MQI 클라이언트를 대신하여 MQI 호출을 작성합니다. 서버 연결 MCA가 MQI 호출 작성에 사용할 대체 사용자 ID를 선택할 수 있습니다. 대체 사용자 ID는 클라이언트 워크스테이션이나 클라이언트의 액세스를 구성 및 제어하는 데 선택하는 모든 것과 연관될 수 있습니다. 사용자 ID에는 MQI 호출을 발행하기 위해 필요한 권한이 서버에서 할당되어야 합니다. 클라이언트가 서버 연결 MCA의 권한으로 MQI 호출을 작성할 수 있게 하려면 대체 사용자 ID를 선택하는 것이 좋습니다.

표 9. 서버 연결 채널에서 사용되는 사용자 ID	
사용자 ID	사용되는 경우
보안 액시트로 설정되는 사용자 ID	CHLAUTH TYPE (BLOCKUSER) 규칙으로 차단되는 경우를 제외하고 사용됨. 자세한 정보는 87 페이지의 『보안 액시트에서 사용자 ID 설정』 절을 참조하십시오.

표 9. 서버 연결 채널에서 사용되는 사용자 ID (계속)	
사용자 ID	사용되는 경우
CHLAUTH 규칙으로 설정되는 사용자 ID	보안 엑시트로 겹쳐쓰지는 경우를 제외하고는 사용됨. 자세한 정보는 채널 인증 레코드를 참조하십시오 .
SVRCONN 인증 정의의 MCAUSER 속성에 정의되는 사용자 ID	보안 엑시트 또는 CHLAUTH 규칙으로 겹쳐쓰지는 경우를 제외하고는 사용됨.
클라이언트 시스템에서 플로우되는 사용자 ID	다른 방법으로 설정된 사용자 ID가 없는 경우 사용됨.
서버 연결 채널을 시작한 사용자 ID	다른 방법으로 설정된 사용자 ID가 없고 클라이언트 사용자 ID가 플로우되지 않는 경우 사용됨. 자세한 정보는 88 페이지의 『 채널 프로그램을 실행하는 사용자 ID 』 절을 참조하십시오.

서버 연결 MCA가 원격 사용자를 대신하여 MQI 호출을 작성하기 때문에 원격 클라이언트 대신 MQI 호출을 발행하는 서버 연결 MCA의 보안 포함 및 잠재적으로 많은 수의 사용자 액세스를 관리하는 방법을 고려하는 것이 중요합니다.

- 한 가지 방법은 서버 연결 MCA가 자체 권한으로 MQI 호출을 발행하는 것입니다. 하지만 일반적으로 서버 연결 MCA가 자체의 강력한 액세스 성능으로 클라이언트 사용자 대신 MQI 호출을 발행하는 것은 바람직하지 않음에 유념하십시오.
- 다른 방법은 클라이언트에서 플로우되는 사용자 ID를 사용하는 방법입니다. 서버 연결 MCA가 클라이언트 사용자 ID의 액세스 성능을 사용하여 MQI 호출을 발행할 수 있습니다. 이 방식은 고려해야 하는 몇 가지 질문을 작성합니다.
 1. 각 플랫폼의 사용자 ID 형식이 서로 다릅니다. 클라이언트의 사용자 ID 형식이 서버에서 허용 가능한 형식과 다른 경우 이는 문제가 될 수 있습니다.
 2. 서로 다르며 사용자 ID가 변경되는 잠재적으로 많은 클라이언트가 있을 수 있습니다. 서버에서 ID를 정의하거나 관리해야 합니다.
 3. 사용자 ID는 신뢰됩니까? 모든 사용자 ID(로그온한 사용자의 ID가 아니어도 됨)를 클라이언트에서 사용될 수 있습니다. 예를 들어, 클라이언트는 보안을 이유로 서버에서만 의도적으로 정의된 전체 mqm 권한이 있는 ID를 플로우할 수 있습니다.
- 바람직한 방법은 서버에서 클라이언트 식별 토큰을 정의하여 클라이언트 연결된 애플리케이션의 성능을 제한하는 것입니다. 이는 일반적으로 서버 연결 채널 특성 MCAUSER를 클라이언트에서 사용되는 특수 사용자 ID 값으로 설정하고 서버의 권한 레벨과 다른 레벨로 클라이언트에서 사용되는 몇 개의 ID를 정의하여 수행합니다.

보안 엑시트에서 사용자 ID 설정

IBM MQ MQI clients에 대해 MQI 호출을 발행하는 프로세스는 서버 연결 MCA입니다. 서버 연결 MCA에서 사용하는 사용자 ID는 MQCD의 MCAUserIdentifier 또는 LongMCAUserIdentifier 필드에 포함된 것입니다. 이러한 필드의 콘텐츠는 다음으로 설정됩니다.

- 보안 엑시트에 의해 설정된 값
- 클라이언트의 사용자 ID
- MCAUSER(서버 연결 채널 정의에서)

보안 엑시트는 호출될 때 인식되는 값을 대체할 수 있습니다.

- 서버 연결 채널 MCAUSER 속성이 공백으로 설정되지 않으면 MCAUSER 값이 사용됩니다.
- 서버 연결 채널 MCAUSER 속성이 공백이면 클라이언트에서 수신된 사용자 ID가 사용됩니다.
- 서버 연결 채널 MCAUSER 속성이 공백이면 클라이언트에서 사용자 ID가 수신되지 않고 서버 연결 채널을 시작한 사용자 ID가 사용됩니다.

클라이언트측 보안 엑시트가 사용 중일 때 IBM MQ 클라이언트는 확인된 사용자 ID를 서버에 보내지 않습니다.

채널 프로그램을 실행하는 사용자 ID

서버 연결 채널을 시작한 사용자 ID에서 사용자 ID 필드가 도출되면 다음 값이 사용됩니다.

- ▶ **z/OS** z/OS의 경우 z/OS 시작 프로시저 테이블에서 채널 시작기 시작 태스크에 지정된 사용자 ID.
- TCP/IP(비z/OS)에 대해 `inetd.conf` 항목의 사용자 ID 또는 리스너를 시작하는 사용자 ID.
- SNA(비z/OS)의 경우, SNA 서버 항목 또는(없는 경우) 수신 첨부 요청 또는 리스너를 시작한 사용자 ID의 사용자 ID.
- NetBIOS 또는 SPX의 경우 리스너를 시작한 사용자 ID.

MCAUSER 속성을 공백으로 설정한 서버 연결 채널 정의가 있으면 클라이언트에서 이 채널 정의를 사용하여 큐 관리자에 연결할 수 있습니다. 이때 클라이언트에서 사용하는 액세스 권한은 클라이언트에서 제공한 사용자 ID로 결정됩니다. 큐 관리자가 실행되고 있는 시스템에서 권한 없는 네트워크 연결을 허용할 경우 보안이 노출될 수 있습니다. IBM MQ 기본 서버 연결 채널(SYSTEM.DEF.SVRCONN)에는 MCAUSER 속성이 공백으로 설정되어 있습니다. 무단 액세스를 방지하려면 기본 정의의 MCAUSER 속성을 IBM MQ MQ 오브젝트에 대한 액세스 권한이 없는 사용자 ID로 업데이트하십시오.

사용자 ID의 대소문자

runmqsc를 사용하여 채널을 정의할 때 사용자 ID가 작은따옴표 내에 포함되지 않으면 MCAUSER 속성이 대문자로 변경됩니다.

▶ **ULW** UNIX, Linux, and Windows의 서버의 경우, 클라이언트에서 수신한 MCAUserIdentifier 필드의 콘텐츠는 소문자로 변경됩니다.

▶ **IBM i** IBM i의 서버의 경우, 클라이언트에서 수신한 LongMCAUserIdentifier 필드 콘텐츠는 대문자로 변경됩니다.

▶ **Linux** ▶ **UNIX** UNIX and Linux 시스템의 서버의 경우, 클라이언트에서 수신한 LongMCAUserIdentifier 필드의 콘텐츠는 소문자로 변경됩니다.

기본적으로 IBM MQ JMS 바인딩 애플리케이션이 사용될 때 전달되는 사용자 ID는 애플리케이션이 실행 중인 JVM의 사용자 ID입니다.

createQueueConnection 메소드를 통해 사용자 ID를 전달할 수도 있습니다.

기밀성 계획

데이터 기밀 보관 방법을 계획합니다.

애플리케이션 레벨 또는 링크 레벨에서 기밀성을 구현할 수 있습니다. TLS를 사용하도록 선택할 수 있습니다. 이 경우 디지털 서명을 사용하도록 계획해야 합니다. 또한, 표준 기능이 요구사항에 맞지 않는 경우에는 채널 엑시트 프로그램을 사용할 수도 있습니다.

관련 개념

88 페이지의 [『링크 레벨 보안과 애플리케이션 레벨 보안 비교』](#)

이 토픽에는 다양한 측면의 링크 레벨 보안 및 애플리케이션 레벨 보안에 대한 정보가 들어 있고 두 보안 레벨을 비교합니다.

93 페이지의 [『채널 엑시트 프로그램』](#)

채널 엑시트 프로그램은 MCA의 처리 순서에서 정의된 위치에서 호출되는 프로그램입니다. 사용자와 벤더는 자체적으로 채널 엑시트 프로그램을 작성할 수 있습니다. 일부는 IBM에서 제공됩니다.

99 페이지의 [『SSL/TLS을 사용하는 채널 보호』](#)

IBM MQ에서의 TLS 지원은 큐 관리자 인증 정보 오브젝트 및 다양한 MQSC 명령을 사용합니다. 또한, 디지털 인증서 사용도 고려해야 합니다.

링크 레벨 보안과 애플리케이션 레벨 보안 비교

이 토픽에는 다양한 측면의 링크 레벨 보안 및 애플리케이션 레벨 보안에 대한 정보가 들어 있고 두 보안 레벨을 비교합니다.

링크 레벨 및 애플리케이션 레벨 보안은 89 페이지의 그림 10에서 설명됩니다.

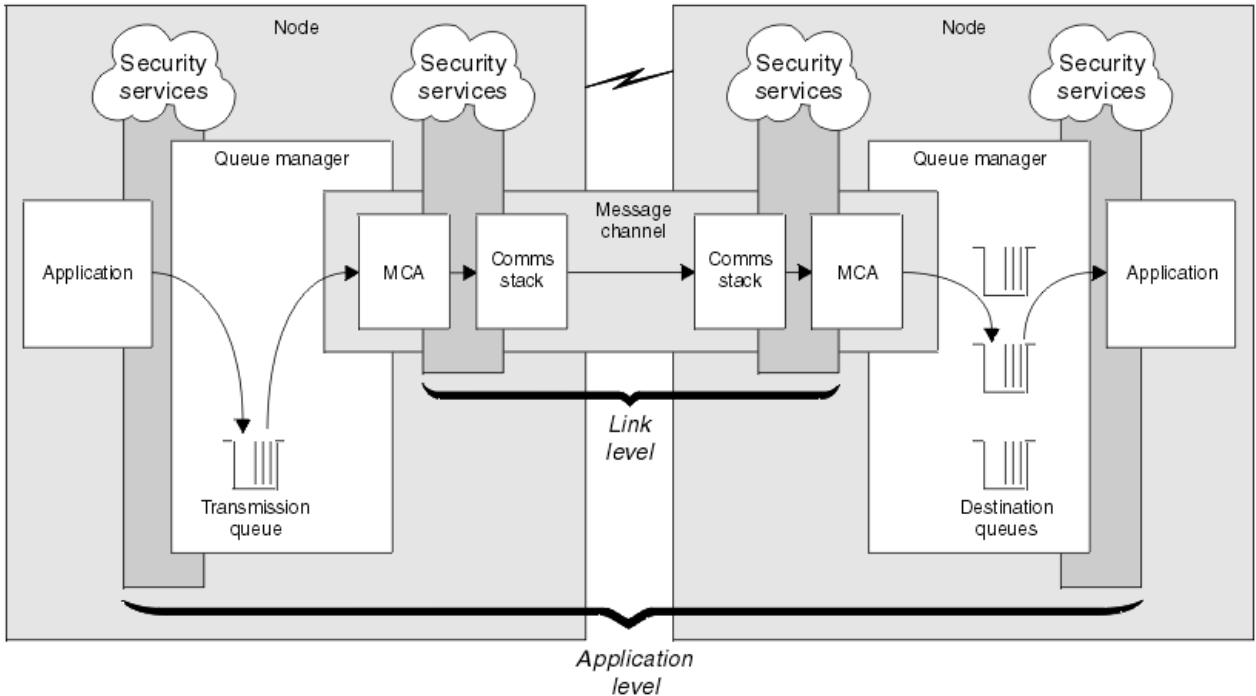


그림 10. 링크 레벨 보안 및 애플리케이션 레벨 보안

큐의 보호 메시지

링크 레벨 보안은 메시지가 하나의 큐 관리자에서 다른 큐 관리자로 전송되는 동안 이를 보호할 수 있습니다. 비 보안 네트워크에서 메시지가 전송될 때 특히 중요합니다. 그러나 이는 메시지가 소스 큐 관리자, 목적지 큐 관리자 또는 중간 큐 관리자에서 큐에 저장되어 있는 동안에는 메시지를 보호할 수 없습니다.

z/OS V 9.1.4 z/OS 데이터 세트 암호화는 큐에 저장된 메시지에 어느 정도의 보호를 제공할 수 있지만, 이는 로컬 큐 관리자의 저장 데이터로 한정됩니다. 데이터 세트 암호화를 사용하는 IBM MQ for z/OS의 저장 데이터에 대한 기밀성 섹션을 참조하십시오. 참조하십시오.

애플리케이션 레벨 보안은 메시지가 큐에 저장되어 있는 동안 이를 보호할 수 있으며 분산 큐잉이 사용되지 않는 경우에도 적용됩니다. 이는 링크 레벨 보안과 애플리케이션 레벨 보안의 주요 차이점이며 89 페이지의 그림 10에 설명되어 있습니다.

큐 관리자가 제어되고 신뢰되는 환경에서 실행 중이 아님

큐 관리자가 제어되고 신뢰되는 환경에서 실행 중인 경우 IBM MQ에서 제공되는 액세스 제어 메커니즘은 해당 큐에 저장된 메시지 보호에 충분한 것으로 간주됩니다. 이는 특히 로컬 큐잉만이 관련되고 메시지가 큐 관리자를 떠나지 않는 경우에 해당합니다. 이 경우 애플리케이션 레벨 보안은 불필요한 것으로 간주될 수도 있습니다.

애플리케이션 레벨 보안은 또한 메시지가 제어되고 신뢰되는 환경에서 실행 중인 또 다른 큐 관리자로 전송되거나 이러한 큐 관리자로부터 받는 경우에 불필요한 것으로 간주될 수도 있습니다. 메시지가 제어되고 신뢰되는 환경에서 실행 중인 큐 관리자로 전송되거나 이러한 큐 관리자로부터 받은 경우에 애플리케이션 레벨 보안의 필요성은 더욱 커집니다.

비용의 차이점

애플리케이션 레벨 보안은 관리 및 성능의 관점에서 링크 레벨 보안보다 비용이 더 많이 들어갈 수도 있습니다.

구성 및 유지보수하는 데 잠재적인 제한조건이 더 많기 때문에 관리 비용이 더 클 수 있습니다. 예를 들면, 특정 사용자가 특정 유형의 메시지만을 송신하고 메시지를 특정 목적지에만 송신하는지를 확인해야 할 수도 있습니다. 반대로, 특정 사용자가 특정 유형의 메시지만을 받고 특정 소스로부터의 메시지만 받도록 해야 할 수도 있습니다. 하나의 메시지 채널에서 링크 레벨 보안 서비스를 관리하는 대신에, 그 채널에서 메시지를 교환하는 모든 쌍의 사용자에게 대해 규칙을 구성하고 유지보수해야 할 수 있습니다.

애플리케이션이 메시지를 넣거나 가져올 때마다 보안 서비스가 호출되는 경우 성능에 영향을 미칠 수도 있습니다.

조직은 링크 레벨 보안이 구현하기가 더 쉬우므로 이를 먼저 고려하는 경향이 있습니다. 조직은 링크 레벨 보안이 모든 요구사항을 만족하지 못하는 경우 애플리케이션 레벨 보안을 고려합니다.

컴포넌트 가용성

일반적으로 분산 환경에서는 보안 서비스에는 둘 이상의 시스템에 있는 컴포넌트가 필요합니다. 예를 들어, 메시지가 한 시스템에서 암호화되고 또 다른 시스템에서 복호화될 수도 있습니다. 이는 링크 레벨 보안 및 애플리케이션 레벨 보안 둘 모두에 적용됩니다.

사용 중인 다른 플랫폼들에 대해 각각이 다른 레벨의 보안 기능을 가지는 이기종 환경에서, 보안 서비스의 필수 구성요소들이 그들이 필요로 하는 모든 플랫폼에서, 사용하기 쉬운 형식으로 사용할 수 없을 수도 있습니다. 이는 링크 레벨 보안에서보다 애플리케이션 레벨 보안에서 더 큰 문제입니다. 특히 다양한 소스로부터 컴포넌트를 구매하여 사용자 고유의 애플리케이션 레벨 보안을 제공하려는 경우에 더욱 그렇습니다.

데드-레터 큐의 메시지

메시지가 애플리케이션 레벨 보안에 의해 보호되는 경우 어떤 이유에서든지 메시지가 해당 목적지에 도달하지 못하고 데드-레터 큐에 놓이는 경우 문제가 발생할 수 있습니다. 메시지 디스크립터 및 데드 레터 헤더의 정보에서 메시지를 처리하는 방법을 알아낼 수 없는 경우에는 애플리케이션 데이터의 콘텐츠를 검사해야 할 수도 있습니다. 애플리케이션 데이터가 암호화되고 의도한 수신인만이 이를 암호 해독할 수 있는 경우 이를 수행할 수 없습니다.

애플리케이션 레벨 보안이 할 수 없는 일

애플리케이션 레벨 보안은 완벽한 솔루션은 아닙니다. 애플리케이션 레벨 보안을 구현하더라도 여전히 몇몇 링크 레벨 보안 서비스가 필요할 수도 있습니다. 예를 들면, 다음과 같습니다.

- 채널이 시작될 때, 두 MCA가 여전히 상호 인증해야 할 수 있습니다. 이는 링크 레벨 보안 서비스만이 수행할 수 있습니다.
- 애플리케이션 레벨 보안은 임베디드 메시지 디스크립터를 포함하는 전송 큐 헤더, MQXQH를 보호할 수 없습니다. 메시지 데이터가 아닌 IBM MQ 채널 프로토콜 플로우의 데이터를 보호할 수도 없습니다. 링크 레벨 보안만이 이 보호를 제공할 수 있습니다.
- 애플리케이션 레벨 보안 서비스가 MQI 채널의 서버 측에서 호출된 경우 서비스는 채널을 통해 전송된 MQI 호출의 매개변수를 보호할 수 없습니다. 특히 MQPUT, MQPUT1 또는 MQGET 호출의 애플리케이션 데이터는 보호되지 않습니다. 이 경우, 링크 레벨 보안만 보호를 제공할 수 있습니다.

링크 레벨 보안

링크 레벨 보안은 MCA, 통신 서브시스템 또는 함께 작동하는 두 개의 결합에 의해 직접 또는 간접적으로 호출되는 보안 서비스를 의미합니다.

링크 레벨 보안은 [89 페이지의 그림 10](#)에서 설명됩니다.

다음은 링크 레벨 보안 서비스의 몇 개 예입니다.

- 메시지 채널의 양 측에 있는 MCA는 해당 파트너를 인증할 수 있습니다. 이는 채널이 시작되고 통신 연결이 설정되면 메시지가 플로우를 시작하기 전에 수행됩니다. 어느 쪽에서든지 인증이 실패하면, 채널이 닫히고 메시지가 전송되지 않습니다. 이는 식별과 인증 서비스의 예입니다.
- 메시지는 채널의 송신 측에서 암호화되고 수신 측에서 복호화됩니다. 이는 기밀성 서비스의 예입니다.
- 네트워크에서 메시지가 전송되는 동안 콘텐츠가 의도적으로 수정되었는지를 판별하기 위해 채널의 수신 측에서 메시지가 검사될 수 있습니다. 이는 데이터 무결성 서비스의 예입니다.

IBM MQ에서 제공되는 링크 레벨 보안

IBM MQ에서의 기밀성 및 데이터 무결성의 프로비저닝을 위한 기본 방법은 TLS를 사용하는 것입니다. IBM MQ에서 TLS를 사용하는 것에 관한 자세한 정보는 [21 페이지의 『IBM MQ의 TLS 보안 프로토콜』](#)의 내용을 참조하십시오. 인증을 위해 IBM MQ는 채널 인증 레코드 사용 기능을 제공합니다. 채널 인증 레코드는 개별 채널이나 채

널 그룹의 레벨에서 연결 시스템에 부여되는 액세스에 대해 세밀한 제어를 제공합니다. 자세한 정보는 [43 페이지의 『채널 인증 레코드』](#)의 내용을 참조하십시오.

사용자 고유의 링크 레벨 보안 제공

사용자 고유의 링크 레벨 보안 서비스를 제공할 수 있습니다. 사용자 고유의 채널 엑시트 프로그램을 작성하는 것이 사용자 고유의 링크 레벨 보안 서비스를 제공하는 기본적인 방법입니다.

채널 엑시트 프로그램은 [93 페이지의 『채널 엑시트 프로그램』](#)에 소개되어 있습니다. 동일한 주제에서는 IBM MQ for Windows와 함께 제공되는 채널 엑시트 프로그램(SSPI 채널 엑시트 프로그램)에 대해서도 설명합니다. 이 채널 엑시트 프로그램은 소스 코드를 수정하여 요구사항을 충족시킬 수 있도록 소스 형식으로 제공됩니다. 이 채널 엑시트 프로그램 또는 다른 벤더에서 제공되는 채널 엑시트 프로그램이 요구사항에 맞지 않는 경우, 사용자 고유로 설계하고 작성할 수 있습니다. 이 주제에서는 채널 엑시트 프로그램이 보안 서비스를 제공할 수 있는 방법을 제안합니다. 채널 엑시트 프로그램 작성 방법에 대한 정보는 [채널 엑시트 프로그램 작성](#)을 참조하십시오.

보안 엑시트를 사용하는 링크 레벨 보안

보안 엑시트는 보통 쌍으로 작동합니다. 채널의 각 끝에서 하나씩 작동합니다. 이들은 채널이 시동될 때 초기 데이터 조정이 끝난 직후 호출됩니다.

보안 엑시트는 식별 및 인증, 액세스 제어, 기밀성을 제공하기 위해 사용할 수 있습니다.

메시지 엑시트를 사용하는 링크 레벨 보안

메시지 엑시트는 MQI 채널이 아니라 메시지 채널에서만 사용할 수 있습니다. 메시지 엑시트는 임베드된 메시지 디스크립터를 포함하는 전송 큐 헤더인 MQXQH와 메시지 안의 애플리케이션 데이터에 모두 액세스할 수 있습니다. 메시지 엑시트는 메시지의 콘텐츠를 수정하고 그 길이를 변경할 수 있습니다.

메시지 엑시트는 메시지의 일부가 아니라 전체에 액세스해야 하는 경우에도 사용될 수 있습니다.

메시지 엑시트는 식별 및 인증, 액세스 제어, 기밀성, 데이터 무결성, 비거절, 보안 이외의 다른 이유로 제공하는 데 사용할 수 있습니다.

송신 및 수신 엑시트를 사용하는 링크 레벨 보안

송신 및 수신 엑시트는 메시지 및 MQI 채널 모두에서 사용 가능합니다. 이는 채널에서 플로우되는 모든 유형의 데이터에 대해 호출되고, 양방향 모두의 플로우에 대해 호출됩니다.

송신 및 수신 엑시트가 각 전송 세그먼트에 액세스할 수 있습니다. 해당 콘텐츠를 수정하고 그 길이를 변경할 수 있습니다.

메시지 채널에서 MCA가 메시지를 분할하여 둘 이상의 전송 세그먼트로 송신해야 하면, 메시지의 일부가 있는 각 전송 세그먼트에 대해 송신 엑시트가 호출되고, 수신하는 쪽에서는 각 전송 세그먼트에 대해 수신 엑시트가 호출됩니다. MQI 채널에서 MQI 호출의 입력이나 출력 매개변수가 너무 커서 하나의 전송 세그먼트로 송신될 수 없는 경우에도 같은 일이 발생합니다.

MQI 채널에서는 전송 세그먼트의 바이트 10이 MQI 호출을 식별하고, 전송 세그먼트에 호출의 입력이나 출력 매개변수가 있는지 여부를 표시합니다. 송신 및 수신 엑시트가 MQI 호출에 보호되어야 할 수 있는 애플리케이션 데이터가 있는지 여부를 판별하기 위해 이 바이트를 조사할 수 있습니다.

송신 엑시트가 처음으로 호출되면, 필요한 모든 자원을 확보하고 초기화하기 위해 MCA에게 전송 세그먼트를 보유하는 버퍼 내 지정된 양의 공간을 예약하게 할 수 있습니다. 전송 세그먼트를 처리하기 위해 나중에 호출되는 경우, 이 공간을 사용하여 암호화된 키나 디지털 서명 등을 추가할 수 있습니다. 채널의 다른 쪽에 있는 해당하는 수신 엑시트는 송신 엑시트로 추가된 데이터를 제거하고, 전송 세그먼트를 처리하는 데 사용할 수 있습니다.

송신 및 수신 엑시트는 처리 중인 데이터 구조를 알 필요가 없기 때문에 각 전송 세그먼트를 2진 오브젝트로 처리할 수 있다는 점에서 최적입니다.

송신 및 수신 엑시트는 기밀성 및 데이터 무결성을 제공하는 데 사용할 수 있으며 보안 이외의 용도로 사용하기 위해서도 제공 가능합니다.

관련 태스크

[송신 또는 수신 엑시트 프로그램에서 API 호출 식별](#)

애플리케이션 레벨의 보안

애플리케이션 레벨 보안은 애플리케이션과 애플리케이션이 연결된 큐 관리자 사이의 인터페이스에서 호출되는 해당 보안 서비스를 나타냅니다.

해당 서비스는 애플리케이션이 큐 관리자에 MQI 호출을 발행할 때 호출됩니다. 서비스는 애플리케이션, 큐 관리자, IBM MQ를 지원하는 다른 제품 또는 같이 작동하는 이들의 결합으로 간접 또는 직접 호출될 수 있습니다. 애플리케이션 레벨 보안은 89 페이지의 그림 10에서 설명됩니다.

애플리케이션 레벨 보안은 엔드-투-엔드 보안 또는 메시지 레벨의 보안이라고도 합니다.

다음은 애플리케이션 레벨 보안 서비스의 몇 가지 예입니다.

- 애플리케이션이 메시지를 큐에 넣으면 메시지 디스크립터는 애플리케이션에 연관된 사용자 ID를 포함합니다. 그렇지만 사용자 ID 인증에 사용할 수 있는 암호화된 비밀번호와 같은 데이터는 없습니다. 보안 서비스는 이 데이터를 추가할 수 있습니다. 메시지가 결국 수신 애플리케이션에서 검색되는 경우, 서비스의 다른 컴포넌트는 메시지와 같이 전달되는 데이터를 사용하여 사용자 ID를 인증할 수 있습니다. 이는 식별과 인증 서비스의 예입니다.
- 메시지는 애플리케이션이 큐에 이를 넣을 때 암호화되고 수신 애플리케이션이 이를 검색할 때 복호화됩니다. 이는 기밀성 서비스의 예입니다.
- 메시지는 수신 애플리케이션이 이를 검색할 때 검사 가능합니다. 이 검사는 애플리케이션 전송에 의해 메시지를 큐에 처음 넣은 후에 콘텐츠가 의도적으로 수정되었는지 여부를 판별합니다. 이는 데이터 무결성 서비스의 예입니다.

Advanced Message Security 계획

Advanced Message Security(AMS)는 엔드 애플리케이션에 영향을 미치지 않으면서 IBM MQ 네트워크를 통해 흐르는 민감한 데이터에 대한 높은 레벨의 보호를 제공하는 IBM MQ의 컴포넌트입니다.

특히 기밀 또는 지불 관련 정보(예: 환자 보고서 또는 신용카드 정보)와 같은 아주 민감하거나 높은 가치의 정보를 이동하는 경우, 정보 보안에 특히 주의해야 합니다. 회사 내에서 이동하는 정보의 해당 무결성을 유지하고 권한 없는 액세스로부터 보호하는 것은 매우 위험하고 책임이 따르는 일입니다. 이 때 보안 규제를 준수해야 하며 그렇지 못할 경우에는 커다란 불이익이 있을 수 있습니다.

IBM MQ에 대해 자체적으로 보안 확장을 개발할 수도 있습니다. 그렇지만 이런 솔루션의 경우 전문가의 기술이 필요하며 유지보수가 복잡하고 비용이 많이 들 수 있습니다. Advanced Message Security는 기업 내에서 정보를 이동할 때 거의 모든 상용 IT 시스템 유형 사이에서 발생하는 이런 문제 해결에 사용할 수 있습니다.

Advanced Message Security는 다음과 같은 방식으로 IBM MQ의 보안 기능을 확장합니다.

- 메시지 암호화 또는 디지털 서명을 사용하여 애플리케이션 레벨, 지점간 메시징 인프라에 대한 엔드-투-엔드 보호를 제공합니다.
- 복잡한 보호 코드를 작성하거나 기존 애플리케이션을 수정하거나 다시 컴파일하지 않고도 포괄적인 보호를 제공합니다.
- PKI(Public Key Infrastructure) 기술을 사용하여 메시지에 대해 인증, 권한 부여, 기밀성, 데이터 무결성 서비스를 제공합니다.
- 메인프레임 및 분산 서버에 대한 보안 정책 관리를 제공합니다.
- IBM MQ 서버 및 클라이언트 모두를 지원합니다.
- 엔드-투-엔드 안전 메시징 솔루션을 제공하기 위해 Managed File Transfer와 통합됩니다.

자세한 정보는 506 페이지의 『Advanced Message Security』의 내용을 참조하십시오.

사용자 고유의 애플리케이션 레벨 보안 제공

사용자 고유의 애플리케이션 레벨 보안 서비스를 제공할 수 있습니다. 애플리케이션 레벨 보안을 구현할 수 있도록 IBM MQ는 두 개의 엑시트인 API 엑시트와 API 교차 엑시트를 제공합니다.

API 엑시트와 API 교차 엑시트는 ID 및 인증, 액세스 제어, 기밀성, 데이터 무결성 및 부인 방지 서비스 및 보안과 무관한 기타 기능을 제공할 수 있습니다.

API 엑시트나 API 교차 엑시트가 시스템 환경에서 지원되지 않으면, 사용자 고유의 애플리케이션 레벨 보안을 제공하는 다른 방법을 고려하는 것을 원할 수 있습니다. 한 가지 방법은 MQI를 캡슐화하는 상위 레벨 API를 개발하는 것입니다. 그러면 프로그래머가 이 API를 MQI 대신 사용하여 IBM MQ 애플리케이션을 작성합니다.

상위 레벨 API를 사용하는 가장 보편적인 이유는 다음과 같습니다.

- MQI의 향상된 기능들을 프로그래머에게 숨기기 위해.
- MQI를 사용할 때 표준을 강화하기 위해.
- MQI에 함수를 추가하기 위해. 이 추가된 함수들이 보안 서비스일 수 있습니다.

일부 벤더 제품은 이 기술을 사용하여 IBM MQ에 대한 애플리케이션 레벨 보안을 제공합니다.

보안 서비스를 이 방법으로 제공하려고 계획하고 있으면, 데이터 변환에 대한 다음 사항들을 알아두십시오.

- 디지털 서명 등의 보안 토큰이 메시지의 애플리케이션 데이터에 추가되었으면, 데이터 변환을 수행하고 있는 어떠한 코드이든지 이 토큰이 있다는 것을 알아야 합니다.
- 보안 토큰이 애플리케이션 데이터의 2진 이미지로부터 도출되었을 수 있습니다. 따라서, 데이터를 변환하기 전에 모든 토큰 검사가 완료되어야 합니다.
- 메시지의 애플리케이션 데이터가 암호화되었으면, 데이터 변환 전에 복호화되어야 합니다.

채널 엑시트 프로그램

채널 엑시트 프로그램은 MCA의 처리 순서에서 정의된 위치에서 호출되는 프로그램입니다. 사용자와 벤더는 자체적으로 채널 엑시트 프로그램을 작성할 수 있습니다. 일부는 IBM에서 제공됩니다.

여러 유형의 채널 엑시트 프로그램이 있으나, 네 개만이 링크 레벨 보안을 제공하는 역할을 합니다.

- 보안 엑시트
- 메시지 엑시트
- 송신 엑시트
- 수신 엑시트

이러한 네 가지 유형의 채널 엑시트 프로그램은 [93 페이지의 그림 11](#)에 설명되어 있으며 다음 주제에서도 설명됩니다.

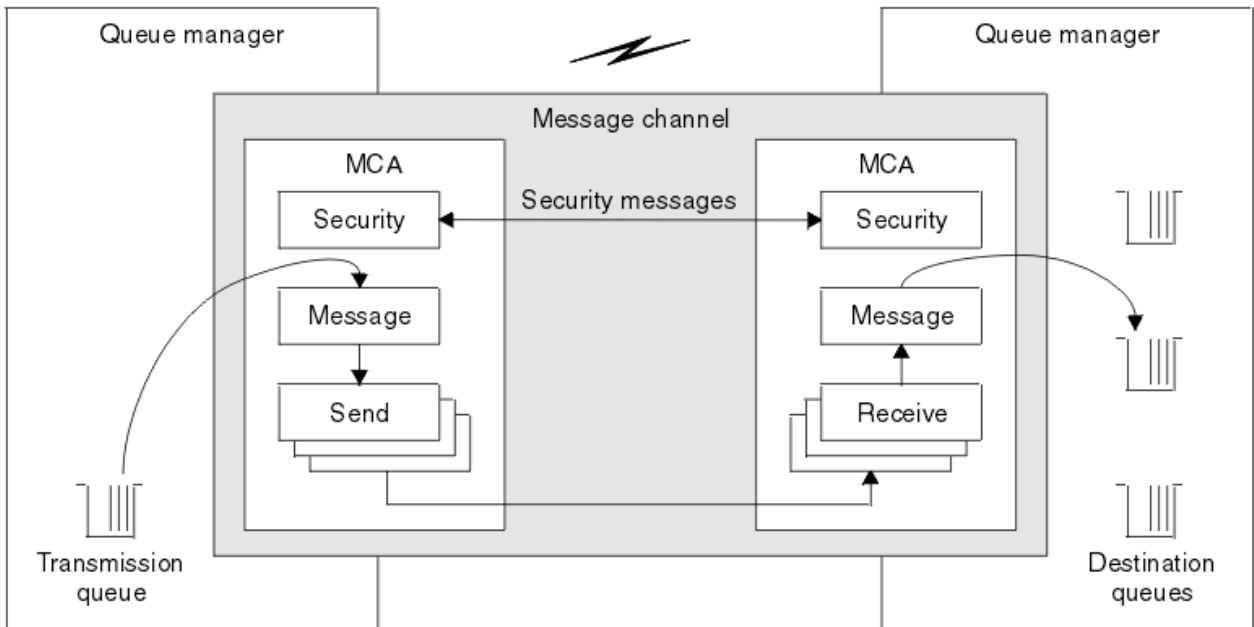


그림 11. 메시지 채널의 보안, 메시지, 송신, 수신

관련 개념

메시지 채널에 대한 채널 엑시트 프로그램

보안 엑시트 개요

보안 엑시트는 일반적으로 쌍으로 작동합니다. 이는 메시지가 플로우되기 전에 호출되고 MCA가 해당 파트너를 인증할 수 있도록 하기 위해 사용됩니다.

일반적으로 보안 엑시트가 채널의 양쪽 끝에서 하나씩 쌍으로 작동합니다. 이를 초기 데이터 협상이 채널 시작 시에 완료된 후 메시지가 플로우를 시작하기 전에 즉시 호출됩니다. 보안 엑시트는 기본적으로 채널 양쪽 끝의 MCA가 해당 파트너를 인증하도록 하기 위해 사용됩니다. 보안과는 전혀 상관없는 기능이더라도 보안 엑시트가 다른 기능을 수행하는 것을 막는 것은 아무것도 없습니다.

보안 엑시트는 보안 메시지를 송신하여 서로 통신할 수 있습니다. 보안 메시지의 형식은 정의되어 있지 않고 사용자가 결정합니다. 보안 메시지 교환의 가능한 한 가지 결과는 보안 엑시트 중 하나가 더 이상 수행되지 않도록 결정될 수도 있다는 점입니다. 이런 경우 채널은 닫히고 메시지가 플로우되지 않습니다. 채널의 한쪽 끝에만 보안 엑시트가 있는 경우에도 여전히 엑시트가 호출되고 채널을 계속할지 또는 닫을지 여부를 선택할 수 있습니다.

보안 엑시트는 메시지와 MQI 채널 둘 다에서 호출될 수 있습니다. 보안 엑시트의 이름은 채널 양쪽의 채널 정의에서 매개변수로 지정됩니다.

보안 엑시트에 대한 자세한 정보는 91 페이지의 『보안 엑시트를 사용하는 링크 레벨 보안』의 내용을 참조하십시오.

메시지 엑시트

메시지 엑시트는 메시지 채널에서만 작동되며 보통 쌍으로 작동합니다. 메시지 엑시트는 전체 메시지에 대해 작동될 수 있으며 다양하게 변경할 수 있습니다.

채널의 송신 및 수신 측에 있는 메시지 엑시트는 보통 쌍으로 작동합니다. 채널의 송신 측에 있는 메시지 엑시트는 MCA가 전송 큐에서 메시지를 받은 후에 호출됩니다. 채널의 수신 측에 있는 메시지 엑시트는 MCA가 그 목적지 큐에 메시지를 넣기 전에 호출됩니다.

메시지 엑시트는 임베드된 메시지 디스크립터를 포함하는 전송 큐 헤더인 MQXQH와 메시지 안의 애플리케이션 데이터에 모두 액세스할 수 있습니다. 메시지 엑시트는 메시지의 콘텐츠를 수정하고 그 길이를 변경할 수 있습니다. 메시지를 압축, 압축 풀기, 암호화 또는 복호화로 인해 길이가 변경될 수 있습니다. 또는 메시지에 데이터를 추가하거나, 데이터를 제거한 결과일 수도 있습니다.

메시지 엑시트는 반드시 보안을 위해서 뿐만 아니라, 메시지의 일부가 아닌 전체 메시지에 액세스해야 하는 어떠한 목적을 위해서든지 사용될 수 있습니다.

메시지 엑시트는 현재 처리하고 있는 메시지가 해당 목적지로 더 이상 진행하면 안된다는 것을 판별할 수 있습니다. 그런 후, MCA가 데드-레터 큐에 메시지를 넣습니다. 메시지 엑시트는 채널을 닫을 수도 있습니다.

메시지 엑시트는 MQI 채널이 아니라 메시지 채널에서만 호출될 수 있습니다. 이는 MQI 호출의 입력 및 출력 매개변수가 IBM MQ MQI client 애플리케이션과 큐 관리자 사이에서 플로우될 수 있도록 하기 위해 MQI 채널이 사용되기 때문입니다.

메시지 엑시트의 이름은 양측 채널에 있는 채널 정의에서 매개변수로 지정됩니다. 연속적으로 실행되도록 메시지 엑시트 목록을 지정할 수도 있습니다.

메시지 엑시트에 대한 자세한 정보는 91 페이지의 『메시지 엑시트를 사용하는 링크 레벨 보안』의 내용을 참조하십시오.

송신 및 수신 엑시트

송신 및 수신 엑시트는 일반적으로 쌍으로 작동합니다. 이는 전송 세그먼트에서 운영되며 처리 중인 데이터 구조가 적절하지 않은 경우에 사용하기에 적합합니다.

채널의 한 쪽에 있는 송신 엑시트와 다른 쪽에 있는 수신 엑시트는 보통 쌍으로 작동합니다. 송신 엑시트는 MCA가 통신 연결에서 데이터를 송신하기 위해 통신 송신을 발행하기 직전에 호출됩니다. 수신 엑시트는 MCA가 통신 수신 후에 제어를 다시 확보하고 통신 연결에서 데이터를 수신한 직후에 호출됩니다. MQI 채널을 통해 공유 대화가 사용 중인 경우, 송신 및 수신 엑시트의 다른 인스턴스가 각 대화에 대해 호출됩니다.

IBM MQ 채널 프로토콜은 제어 정보와 메시지 데이터 모두를 포함하는 메시지 채널의 두 MCA 사이를 플로우합니다. 유사하게 MQI 채널에서 플로우하는 제어 정보와 MQI 호출 매개변수 모두를 포함합니다. 송신 및 수신 엑시트는 모든 데이터 유형에 대해 호출됩니다.

메시지 데이터는 메시지 채널에서 한 방향으로만 플로우되지만 MQI 채널에서 MQI 호출의 입력 매개변수는 한 방향으로 플로우되고 출력 매개변수는 다른 방향으로 플로우됩니다. 메시지와 MQI 채널 모두에서 제어 정보는 두 방향으로 모두 플로우합니다. 그 결과 송신 및 수신 엑시트는 채널의 양 측에서 모두 호출 가능합니다.

두 MCA 사이에서 하나의 플로우로 전송되는 데이터 단위를 전송 세그먼트라 합니다. 송신 및 수신 엑시트가 각 전송 세그먼트에 액세스할 수 있습니다. 해당 콘텐츠를 수정하고 그 길이를 변경할 수 있습니다. 그렇지만 송신 엑시트는 전송 세그먼트의 처음 8바이트를 변경하면 안됩니다. 이 8바이트는 IBM MQ 채널 프로토콜 헤더 파트를 양식화합니다. 송신 엑시트가 전송 세그먼트의 길이를 늘릴 수 있는 양에도 제한이 있습니다. 특히, 송신 엑시트는 채널이 시동될 때 두 개의 MCA 사이에서 협상된 최대 길이 이상으로 그 길이를 늘릴 수 없습니다.

메시지 채널에서, 메시지가 너무 커서 하나의 전송 세그먼트로 송신할 수 없으면, 송신 MCA가 메시지를 분할하고 둘 이상의 전송 세그먼트로 이를 송신합니다. 결과적으로, 메시지의 일부를 포함하는 각 전송 세그먼트에 대해 송신 엑시트가 호출되고, 수신 측에서는 각 전송 세그먼트에 대해 수신 엑시트가 호출됩니다. 수신 MCA는 수신 엑시트가 전송 세그먼트를 처리한 후에 해당 세그먼트에서 메시지를 다시 구성합니다.

이와 유사하게 MQI 채널에서는 MQI 호출의 입력이나 출력 매개변수가 너무 큰 경우 둘 이상의 전송 세그먼트로 송신됩니다. 예를 들어, 애플리케이션 데이터가 충분히 클 경우, MQPUT, MQPUT1, 또는 MQGET 호출에서 둘 이상의 세그먼트로 분할될 수 있습니다.

이런 점들을 고려해볼 때, 송신 및 수신 엑시트는 처리 중인 데이터 구조를 알 필요가 없기 때문에 각 전송 세그먼트를 2진 오브젝트로 처리하는 것이 적절합니다.

송신 또는 수신 엑시트는 채널을 종료할 수 있습니다.

송신 엑시트와 수신 엑시트 이름은 채널 양 측의 채널 정의에서 매개변수로 지정됩니다. 연속적으로 실행되도록 송신 엑시트를 지정할 수도 있습니다. 이와 유사한 방법으로 수신 엑시트 목록을 지정할 수 있습니다.

송신 및 수신 엑시트에 대한 자세한 정보는 [91 페이지의 『송신 및 수신 엑시트를 사용하는 링크 레벨 보안』](#)의 내용을 참조하십시오.

데이터 무결성 계획

데이터 무결성 보존 방법을 계획합니다.

애플리케이션 레벨 또는 링크 레벨에서 데이터 무결성을 구현할 수 있습니다.

애플리케이션 레벨에서 표준 기능이 요구사항에 맞지 않는 경우 API 엑시트 프로그램을 사용할 수 있습니다. 권한 없는 수정으로부터 보호하기 위해 Advanced Message Security(AMS)를 사용하여 메시지에 디지털로 서명하도록 선택할 수 있습니다.

링크 레벨에서 TLS를 사용하도록 선택할 수 있으며 이 경우 디지털 인증서 사용을 계획해야 합니다. 또한, 표준 기능이 요구사항에 맞지 않는 경우에는 채널 엑시트 프로그램을 사용할 수도 있습니다.

관련 개념

[99 페이지의 『SSL/TLS을 사용하는 채널 보호』](#)

IBM MQ에서의 TLS 지원은 큐 관리자 인증 정보 오브젝트 및 다양한 MQSC 명령을 사용합니다. 또한, 디지털 인증서 사용도 고려해야 합니다.

[20 페이지의 『IBM MQ에서의 데이터 무결성』](#)

메시지 수정 여부를 감지하기 위해 데이터 무결성 서비스를 사용할 수 있습니다.

[92 페이지의 『Advanced Message Security 계획』](#)

Advanced Message Security(AMS)는 엔드 애플리케이션에 영향을 미치지 않으면서 IBM MQ 네트워크를 통해 플로우하는 민감한 데이터에 대한 높은 레벨의 보호를 제공하는 IBM MQ의 컴포넌트입니다.

채널 엑시트 호출 및 데이터 구조

관련 참조

[API 엑시트 참조](#)

감사 계획

감사해야 하는 데이터 및 감사 정보 캡처 및 처리 방법을 결정합니다. 시스템이 올바르게 구성되었는지 검사하는 방법을 고려하십시오.

활동 모니터링에는 몇 개의 측면이 있습니다. 고려해야 하는 측면은 감사자 요구사항으로 정의되는 경우가 있으며 해당 요구사항은 HIPAA(Health Insurance Portability and Accountability Act) 또는 SOX(Sarbanes-Oxley)와 같은 규제 표준으로 구동되는 경우가 있습니다. IBM MQ에서는 이런 표준 준수를 위한 기능을 제공합니다.

예외에만 관심이 있는지 또는 모든 시스템 작동에 대해서 관심이 있는지를 고려하십시오.

일부 감사 측면은 가동 모니터링으로 고려할 수도 있습니다. 감사에 대한 한 가지 탁월함은 실시간 경보만 보는 것이 아니라 히스토리 데이터로 볼 수 있다는 점입니다. 모니터링은 모니터링 및 성능 절에서 설명됩니다.

감사하려는 데이터

다음 절에서 설명하는 것처럼 감사해야 하는 데이터 또는 활동 유형을 고려하십시오.

IBM MQ 인터페이스를 사용하여 IBM MQ에 수행되는 변경

도구 이벤트, 특히 명령 이벤트 및 구성 이벤트를 발행하도록 IBM MQ를 구성하십시오.

해당 제어를 벗어난 IBM MQ에 대한 변경

일부 변경은 IBM MQ 작동 방식에 영향을 줄 수 있지만 IBM MQ에서 직접 모니터링할 수는 없습니다. 이런 변경의 예에는 구성 파일 `mqs.ini`, `qm.ini` 및 `mqclient.ini` 변경, 큐 관리자 작성 및 삭제, 사용자 엑시트 프로그램과 같은 2진 파일 설치, 파일 권한 변경이 포함됩니다. 이런 활동을 모니터링하려면 운영 체제 레벨에서 실행 중인 도구를 사용해야 합니다. 다른 도구를 사용할 수 있으며 이는 다른 운영 체제에 적합합니다. `sudo`와 같이 관련된 도구로 작성되는 로그가 있을 수도 있습니다.

IBM MQ의 조작 제어

큐 관리자 시작 및 중지와 같은 활동을 감사하기 위해 운영 체제를 사용해야 할 수도 있습니다. IBM MQ가 도구 이벤트를 발행하도록 구성 가능한 경우도 있습니다.

IBM MQ 내에서 애플리케이션 활동

큐 열기 및 메시지 넣기 및 가져오기와 같은 애플리케이션 조치를 감사하려면 적절한 이벤트를 발행하도록 IBM MQ를 구성하십시오.

불법 침입 경보

시도된 보안 결함을 감사하려면 권한 이벤트를 발행하도록 시스템을 구성하십시오. 채널 이벤트는 활동을 표시하는 데 유용할 수도 있으며 특히 채널이 예상치 못하게 종료되는 경우입니다.

감사 데이터 캡처, 표시, 아카이브 계획

필요한 다수의 요소가 IBM MQ 이벤트 메시지로 보고됩니다. 해당 메시지를 읽고 형식화할 수 있는 도구를 선택해야 합니다. 장기 기억장치 및 분석에 관심이 있는 경우, 이를 데이터베이스와 같은 보조 기억장치 메커니즘으로 이동해야 합니다. 이런 메시지를 처리하지 않으면 계속 이벤트 큐에 남아 있어서 큐를 채울 수도 있습니다. 일부 이벤트(예: 보안 실패가 발생하는 경우 경보 발행)를 기반으로 조치를 자동으로 수행하는 도구를 구현하도록 결정할 수도 있습니다.

시스템이 올바르게 구성되었는지 확인

테스트 세트가 IBM MQ Explorer에서 제공됩니다. 이를 사용하여 오브젝트 정의에서 문제점을 검사하십시오.

또한, 시스템 구성이 예상과 맞는지 주기적으로 검사하십시오. 명령 및 구성 이벤트가 임의의 변경이 수행될 때 보고될 수는 있지만 구성을 덤프하고 이를 알려진 좋은 사본과 비교하는 것도 유용합니다.

토폴로지에 의한 보안 계획

이 절에서는 특정 상황, 즉 채널, 큐 관리자 클러스터, 발행/구독, 멀티캐스트 애플리케이션에서의 보안 및 방화벽을 사용하는 경우의 보안에 대해 설명합니다.

자세한 정보는 다음 하위 주제를 참조하십시오.

채널 권한 부여

채널을 통해 메시지를 송수신하는 경우, 다양한 IBM MQ 자원에 대해 액세스를 제공해야 합니다. 메시지 채널 에이전트(MCA)는 큐 관리자 사이에서 메시지를 이동하는 필수 IBM MQ 애플리케이션이기 때문에 제대로 작동하기 위해 다양한 IBM MQ 자원에 대한 액세스가 필요합니다.

MCA에 대해 PUT 시에 메시지를 수신하기 위해 MCA에 연관된 사용자 ID 또는 메시지에 연관된 사용자 ID를 사용할 수 있습니다.

CONNECT 시에 **CHLAUTH** 채널 인증 레코드를 사용하여 어설션된 사용자 ID를 대체 사용자에게 맵핑할 수 있습니다.

IBM MQ에서 채널은 TLS 지원으로 보호 가능합니다.

MCAUSER 속성이 사용되지 않는 송신자 채널을 제외한 송신 및 수신 채널에 연관된 사용자 ID의 경우 다음 자원에 대한 액세스가 필요합니다.

- 송신 채널에 연관된 사용자 ID에는 큐 관리자, 전송 큐, 데드-레터 큐에 대한 액세스가 필요하며 채널 엑시트에 필요한 다른 모든 자원에 대한 액세스도 필요합니다.
- 수신자 채널의 MCAUSER 사용자 ID에는 **+setall** 권한이 필요합니다. 이유는 수신자 채널이 원격 송신자 채널에 수신된 데이터를 사용하여 전체 컨텍스트 필드가 포함된 전체 MQMD를 작성해야 하기 때문입니다. 따라서, 큐 관리자의 경우 이 활동을 수행하는 사용자에게 **+setall** 권한이 있도록 요구합니다. 이 **+setall** 권한은 다음을 위해 사용자에게 부여되어야 합니다.

- 수신자 채널이 유효하게 메시지를 넣는 모든 큐.
- 큐 관리자 오브젝트. 자세한 정보는 컨텍스트에 대한 권한 부여를 참조하십시오.

- 발신자가 COA 보고 메시지를 요청한 수신자 채널의 MCAUSER 사용자 ID에는 보고 메시지를 리턴하는 전송 큐에 대한 **+setall** 권한이 필요합니다. 이 권한이 없으면 AMQ8077 오류 메시지가 로깅됩니다.
- 수신 채널에 연관된 사용자 ID로 대상 큐를 열어 메시지를 큐에 넣을 수 있습니다. 이 때 메시지 큐잉 인터페이스(MQI)가 사용되기 때문에 IBM MQ Object Authority Manager(OAM)를 사용 중이지 않은 경우 추가 액세스 제어 검사가 필요할 수 있습니다. MCA에 연관된 사용자 ID(이 주제에 설명된 대로) 또는 메시지에 연관된 사용자 ID(MQMD `UserIdentifier` 필드에서)에 대해 권한 검사가 수행되는지 여부를 지정할 수 있습니다.

적용되는 채널 유형에 대해 채널 정의의 **PUTAUT** 매개변수는 해당 검사에 사용되는 사용자 ID를 지정합니다.

- 채널은 기본적으로 큐 관리자의 서비스 계정을 사용하는데 이 계정은 전체 관리 권한을 가지고 있어서 특별한 권한이 필요하지 않습니다.
- 서버 연결 채널의 경우, 관리 연결은 CHLAUTH 규칙에 의해 기본적으로 차단되며 명시적인 프로비저닝이 필요합니다.
- 수신자, 요청자, 클러스터 수신자 유형의 채널을 사용하면 인접 큐 관리자의 로컬 관리가 허용되며 관리에서 이 액세스를 제한하기 위해 단계를 수행하는 경우는 제외됩니다.
- 수신자 채널의 MCAUSER 사용자 ID에 대해 **dsp** 및 **ctrlx** 권한을 부여할 필요가 없습니다.
- IBM MQ 8.0.0 Fix Pack 4 이전에는 IBM MQ 관리 권한이 없는 사용자 ID를 사용할 경우, 채널에 대한 **dsp** 및 **ctrlx** 권한을 작업하려는 채널의 사용자 ID에 부여해야 합니다.

IBM MQ 8.0.0 Fix Pack 4부터, 채널이 스스로 다시 동기화하고 순서를 정정 할 때 권한 검사가 없습니다.

그러나 수동으로 RESET CHANNEL 명령을 실행하는 것은 여전히 모든 릴리스에서 **+dsp** 및 **+ctrlx** 권한이 필요합니다.



주의: 메시지 배치(batch) 확인에 채널 재설정이 필요한 경우 IBM MQ에서 채널을 조회하며 이를 위해서는 **+dsp** 권한이 필요합니다.

- MCAUSER 속성은 SDR 채널 유형에는 사용되지 않습니다.
- 메시지에 연관된 사용자 ID를 사용하는 경우 사용자 ID는 원격 시스템의 사용자 ID일 수 있습니다. 원격 시스템 사용자 ID는 대상 시스템에서 인식되어야 합니다. 다음 명령은 원격 시스템에서 사용자 ID에 권한을 부여할 때 발행할 수 있는 명령 유형의 예입니다.

```
setmqaut -m QMgrName -t qmgr -g GroupName +connect +inq +setall
```

```
setmqaut -m QMgrName -t chl -n Profile -g GroupName +dsp +ctrlx
```

여기서 *Profile*은 채널입니다.

```
setmqaut -m QMgrName -t q -n Profile -g GroupName +put +setall
```


여기서 *Profile*은 데드-레터 큐입니다(설정된 경우).

```
setmqaut -m QMgrName -t q -n Profile -g GroupName +put +setall
```

여기서 *Profile*은 권한 부여된 큐의 목록입니다.



주의: 명령 큐 및 다른 민감한 시스템 큐에 메시지를 넣기 위해 사용자 ID에 권한을 부여하는 경우에는 주의해야 합니다.

MCA에 연관된 사용자 ID는 MCA 유형에 따라 다릅니다. 두 가지 유형의 MCA가 있습니다.

호출자 MCA

채널을 시작하는 MCA. 호출자 MCA는 개별 프로세스, 채널 시작기 스레드 또는 프로세스 풀 스레드로 시작 가능합니다. 사용되는 사용자 ID는 상위 프로세스(채널 시작기)에 연관된 사용자 ID 또는 MCA를 시작하는 프로세스에 연관된 사용자 ID입니다.

응답자 MCA

응답자 MCA는 호출자 MCA 요청 결과로 시작되는 MCA입니다. 응답자 MCA는 개별 프로세스, 리스너 스레드 또는 프로세스 풀 스레드로 시작 가능합니다. 사용자 ID는 다음 유형 중 하나일 수 있습니다(환경 설정의 순서대로).

1. APPC에서 호출자 MCA는 응답자 MCA에 사용되는 사용자 ID를 표시할 수 있습니다. 이는 네트워크 사용자 ID라고 하며 개별 프로세스로 시작되는 채널에만 적용됩니다. 채널 정의의 **USERID** 매개변수를 사용하여 네트워크 사용자 ID를 설정하십시오.
2. **USERID** 매개변수가 사용되지 않는 경우 응답자 MCA의 채널 정의는 MCA가 사용해야 하는 사용자 ID를 지정할 수 있습니다. 채널 정의의 **MCAUSER** 매개변수를 사용하여 사용자 ID를 설정하십시오.
3. 사용자 ID가 이전 두 메소드 중 하나로 설정되지 않은 경우, MCA로 시작되는 프로세스의 사용자 ID 또는 상위 프로세스(리스너)의 사용자 ID가 사용됩니다.

관련 개념

[43 페이지의 『채널 인증 레코드』](#)

채널 레벨에서 연결 시스템에 부여된 액세스 권한에 대한 보다 정밀한 제어를 실행하려면 채널 인증 레코드를 사용하십시오.

[채널 인증 레코드 특성](#)

채널 시작기 정의 보호

mqm 그룹의 구성원만 채널 시작기를 조작할 수 있습니다.

IBM MQ 채널 시작기는 IBM MQ 오브젝트가 아닙니다. 이에 대한 액세스는 OAM으로 제어되지 않습니다. IBM MQ는 해당 사용자 ID가 mqm 그룹의 구성원인 경우를 제외하고는 사용자나 애플리케이션이 해당 오브젝트를 조작하는 것을 허용하지 않습니다. PCF 명령 **StartChannelInitiator**를 발행하는 애플리케이션이 있는 경우, PCF 메시지의 메시지 디스크립터에 지정된 사용자 ID는 대상 큐 관리자의 mqm 그룹 구성원이어야 합니다.

또한, 사용자 ID는 이스케이프 PCF 명령을 통하거나 간접 모드에서 **runmqsc**를 사용하여 대응하는 MQSC 명령을 발행하도록 대상 시스템에서 MQM 그룹의 구성원이어야 합니다.

전송 큐

큐 관리자는 자동으로 원격 메시지를 전송 큐에 넣으며 이를 위해 특수 권한이 필요하지는 않습니다.

그렇지만 메시지를 전송 큐에 직접 넣어야 하는 경우, 특수 권한이 필요합니다. [114 페이지의 표 12](#)의 내용을 참조하십시오.

채널 엑시트

채널 인증 레코드가 적합하지 않는 경우, 추가된 보안에 대해 채널 엑시트를 사용할 수 있습니다. 보안 엑시트는 두 보안 엑시트 프로그램 사이에서 안전한 연결을 양식화합니다. 하나의 프로그램은 메시지 채널 에이전트(MCA)를 송신하기 위해 사용되며 다른 하나는 MCA 수신에 사용됩니다.

채널 엑시트에 대한 자세한 정보는 [93 페이지의 『채널 엑시트 프로그램』](#)의 내용을 참조하십시오.

SSL/TLS을 사용하는 채널 보호

IBM MQ에서의 TLS 지원은 큐 관리자 인증 정보 오브젝트 및 다양한 MQSC 명령을 사용합니다. 또한, 디지털 인증서 사용도 고려해야 합니다.

디지털 인증서 및 키 저장소

큐 관리자 인증서 레이블 속성(CERTLABL)을 주요 채널에 사용되는 개인 인증서 이름으로 설정하고 다른 인증서가 필요한 해당 채널에서 인증서 레이블을 설정하여 이를 예외에 대해 대체하는 것은 바람직합니다.

큐 관리자의 기본 인증서 설정과 다른 인증서가 포함된 다수의 채널이 필요한 경우, 여러 개의 큐 관리자에서 채널을 분리하거나 큐 관리자 앞에 QMIPT 프록시를 사용하여 다른 인증서를 표시하도록 해야 합니다.

모든 채널에 대한 다른 인증서를 사용할 수는 있지만 키 저장소에 너무 많은 인증서를 저장하는 경우 TLS 채널 시작 시에 성능이 저하될 수 있습니다. 키 저장소에서 인증서 수를 50개 미만으로 유지하고 최대 100개까지만 고려하여 GSKit 성능이 너무 큰 키 저장소로 인해 저하되는 것을 방지하십시오.

동일한 큐 관리자에 여러 개의 인증서를 허용하면 여러 개의 CA 인증서가 동일한 큐 관리자에서 사용될 가능성이 높아집니다. 그러면 별도의 인증 기관에서 발행되는 인증서에 대해 인증서의 해당 식별 이름 네임스페이스 충돌 가능성이 높아집니다.

전문 인증 기관이 더 주의하는 것과는 달리 회사 내 인증 기관에서는 이름 지정 규칙에서 명확성이 떨어지는 경우가 많아서 임의의 CA 사이에서 의도치 않은 일치가 발생하는 경우가 있습니다.

해당 식별 이름뿐만 아니라 인증서 발행인 식별 이름도 검사해야 합니다. 이를 수행하기 위해 채널 인증 SSLPEERMAP 레코드를 사용하고 **SSLPEER** 및 **SSLCERTI** 필드 모두를 해당 DN 및 발행인 DN에 각각 일치하도록 설정하십시오.

자체 서명 및 CA 서명 인증서

애플리케이션을 개발 및 테스트하는 경우와 프로덕션에서 이를 사용하는 경우 모두에서 디지털 인증서 사용을 계획하는 것이 중요합니다. CA 서명 인증서 또는 자체 서명 인증서를 큐 관리자 및 클라이언트 애플리케이션 사용법에 따라 사용할 수 있습니다.

CAN 서명 인증서

프로덕션 시스템의 경우 인증서를 신뢰 가능한 인증 기관(CA)에서 확보하십시오. 외부 CA에서 인증서를 확보하는 경우 서비스 비용을 지불합니다.

자체 서명 인증서

애플리케이션을 자체적으로 개발 중인 경우 자체 서명 인증서 또는 로컬 CA 발행 인증서를 플랫폼별로 사용할 수 있습니다.

ULW Windows, UNIX, Linux 시스템에서 자체 서명 인증서를 사용할 수 있습니다. 지시사항은 [262 페이지의 『UNIX, Linux, and Windows에서 자체 서명된 개인 인증서 작성』](#)의 내용을 참조하십시오.

IBM i IBM i 시스템에서 로컬 CA에서 서명된 인증서를 사용할 수 있습니다. 지시사항은 [248 페이지의 『IBM i에서 서버 인증서 요청』](#)의 내용을 참조하십시오.

z/OS z/OS에서 자체 서명 또는 로컬 CA 서명 인증서를 사용할 수 있습니다. 지시사항은 [287 페이지의 『z/OS에서 자체 서명된 개인 인증서 작성』](#) 또는 [288 페이지의 『z/OS에서 개인 인증서 요청』](#)의 내용을 참조하십시오.

자체 서명 인증서는 다음과 같은 이유로 프로덕션에서 사용하기에 적합하지 않습니다.

- 자체 서명 인증서는 폐기할 수 없습니다. 폐기하는 경우 개인 키가 손상된 후에 공격자가 ID를 모방할 수 있습니다. CA는 손상된 인증서를 폐기할 수 있으며 폐기된 후에는 더 이상 사용할 수 없습니다. 따라서 CA 서명 인증서는 프로덕션 환경에서 사용하기에 더 안전하며 자체 서명 인증서는 테스트 시스템에서 더 편리합니다.
- 자체 서명 인증서는 만기되지 않습니다. 이는 테스트 환경에서 안전하고 더 편리하지만 프로덕션 환경인 경우 계속 열려 있기 때문에 결국 보안 위반을 초래하게 됩니다. 자체 서명 인증서는 폐기할 수 없다는 점이 이런 위험을 초래합니다.
- 자체 서명 인증서는 개인 인증서 및 루트(또는 신뢰 앵커) CA 인증서 모두로 사용할 수 있습니다. 자체 서명 개인 인증서를 사용하는 사용자는 다른 개인 인증서 서명에 이를 사용할 수도 있습니다. 일반적으로 CA에서 발행되는 개인 인증서에서는 가능하지 않으며 이는 중요한 노출이 됩니다.

CipherSpec 및 디지털 인증서

지원되는 CipherSpec 서브세트만 디지털 인증서의 지원되는 모든 유형에 사용할 수 있습니다. 따라서, 디지털 인증서에 대해 적합한 CipherSpec을 선택해야 합니다. 이와 유사하게 조직의 보안 정책에서 특정 CipherSpec을 사용하도록 요구하면 적합한 디지털 인증서를 확보해야 합니다.

CipherSpec과 디지털 인증서 사이의 관계에 대한 자세한 정보는 40 페이지의 『IBM MQ에서 디지털 인증서와 CipherSpec의 호환성』의 내용을 참조하십시오.

인증서 유효성 검증 정책

IETF RFC 5280 표준은 준수 애플리케이션 소프트웨어가 위장 공격을 방지하기 위해 구현해야 하는 일련의 인증서 유효성 검증 규칙을 지정합니다. 인증서 유효성 검증 규칙 세트는 인증서 유효성 검증 정책이라고도 합니다. IBM MQ에서의 인증서 유효성 검증 정책에 대한 자세한 정보는 39 페이지의 『IBM MQ의 인증서 유효성 검증 정책』의 내용을 참조하십시오.

인증서 폐기 검사 계획

다른 인증 권한의 여러 인증서를 허용하면 불필요한 추가 인증서 폐기 검사가 수행됩니다.

특히, 특정 CA의 폐기 서버 사용을 명시적으로 구성하는 경우(예를 들어, AUTHINFO 오브젝트 또는 인증 정보 레코드(MQAIR) 구조 사용) 다른 CA의 인증서로 표시되면 폐기 검사가 실패합니다.

명시적인 인증서 폐기 서버 구성을 하면 안됩니다. 대신, 각 인증서가 자체 폐기 서버 위치를 인증서 확장자(예: CRL 분배 위치 또는 OCSP AuthorityInfoAccess)에 포함하는 암시적 검사를 사용해야 합니다.

자세한 정보는 [OCSPCheckExtensions](#) 및 [CDPCheckExtensions](#)를 참조하십시오.

TLS 지원에 대한 명령 및 속성

TLS(Transport Layer Security) 프로토콜은 도청, 도용, 위장에 대한 보호를 사용하여 채널 보안을 제공합니다. TLS에 대한 IBM MQ 지원을 사용하면 채널 정의에서 특정 채널이 TLS 보안을 사용하도록 지정할 수 있습니다. 또한, 사용하려는 암호화 알고리즘과 같은 필요한 보안 유형의 세부사항을 지정할 수도 있습니다.

- 다음 MQSC 명령이 TLS를 지원합니다.

ALTER AUTHINFO

인증 정보 오브젝트 속성을 수정합니다.

DEFINE AUTHINFO

인증 정보 오브젝트를 작성합니다.

DELETE AUTHINFO

인증 정보 오브젝트를 삭제합니다.

DISPLAY AUTHINFO

특정 인증 정보 오브젝트 속성을 표시합니다.

- 다음 큐 관리자 매개변수가 TLS를 지원합니다.

CERTLABL

사용하려는 개인 인증서 레이블을 정의합니다.

SSLCRLNL

SSLCRLNL 속성은 향상된 TLS 인증서 검사를 허용하기 위해 인증서 폐기 위치를 제공하는 데 사용되는 인증 정보 오브젝트 이름 목록을 지정합니다.

SSLCRYP

Windows, UNIX and Linux 시스템에서 **SSLCryptoHardware** 큐 관리자 속성을 설정합니다. 이 속성은 시스템에 있는 암호화 하드웨어를 구성하는 데 사용할 수 있는 매개변수 문자열의 이름입니다.

SSLEV

TLS를 사용하는 채널이 TLS 연결 설정에 실패할 경우 TLS 이벤트 메시지를 보고할 것인지를 판별합니다.

SSLFIPS

암호화가 암호화 하드웨어가 아니라 IBM MQ에서 수행되는 경우에 FIPS 준수 알고리즘만 사용되는지 여부를 지정합니다. 암호화 하드웨어가 구성된 경우, 하드웨어 제품에서 제공되는 암호화 모듈이 사용되고 이는 특정 레벨에 대한 FIPS를 준수할 수 있습니다. 이는 사용 중인 하드웨어 제품에 따라 다릅니다.

SSLKEYR

UNIX, Linux, and Windows 시스템의 경우 키 저장소를 큐 관리자와 연관시키십시오. 키 데이터베이스는 GSKit 키 데이터베이스에 보유됩니다. GSKit(IBM Global Security Kit)을 사용하면 Windows, UNIX and Linux 시스템에서 TLS 보안을 사용할 수 있습니다.

SSLRKEYC

보안 키가 재협상되기 전에 TLS 대화 내에서 송수신되는 바이트 수. 바이트 수에는 MCA에서 전송된 제어 정보가 포함됩니다.

- 다음 채널 매개변수가 TLS를 지원합니다.

CERTLABL

사용하려는 개인 인증서 레이블을 정의합니다.

SSLCAUTH

IBM MQ에서 TLS 클라이언트의 인증서 필요 여부 및 유효성 검증 여부를 정의합니다.

SSLCIPH

암호화 강도 및 기능(CipherSpec)(예: TLS_RSA_WITH_AES_128_CBC_SHA)을 지정합니다. CipherSpec은 채널의 양 측과 일치해야 합니다.

SSLPEER

허용된 파트너의 식별 이름(고유 ID)을 지정합니다.

이 절에서는 인증 정보 오브젝트를 지원하는 **setmqaut**, **dspmqaut**, **dmpmqaut**, **rcrmqobj**, **rcdmqimg**, **dspmqfls** 명령을 설명합니다. 또한 UNIX and Linux 시스템에서 인증서를 관리하기 위한 **runmqckm** (iKeycmd) 명령과 UNIX, Linux, and Windows에서 인증서를 관리하기 위한 **runmqakm** 도구에 대해 설명합니다. 다음 절을 참조하십시오.

- [setmqaut](#)
- [dspmqaut](#)
- [dmpmqaut](#)
- [rcrmqobj](#)
- [rcdmqimg](#)
- [dspmqfls](#)
- [키 및 인증서 관리](#)

TLS를 사용하는 채널 보안 개요는 다음을 참조하십시오.

- [21 페이지의 『IBM MQ의 TLS 보안 프로토콜』](#)

TLS에 연관된 MQSC 명령에 대한 자세한 내용은 다음을 참조하십시오.

- [ALTER AUTHINFO](#)
- [DEFINE AUTHINFO](#)
- [DELETE AUTHINFO](#)
- [DISPLAY AUTHINFO](#)

TLS와 연관된 PCF 명령에 대한 자세한 내용은 다음을 참조하십시오.

- [인증 정보 오브젝트 변경, 복사 및 작성](#)
- [인증 정보 오브젝트 삭제](#)
- [인증 정보 오브젝트 조회](#)

IBM MQ for z/OS 서버 연결 채널

IBM MQ for z/OS SVRCONN 채널은 채널 인증을 구현하거나 TLS를 사용하여 보안을 추가하지 않고는 안전하지 않습니다. SVRCONN 채널에는 기본적으로 보안 엑시트가 정의되어 있지 않습니다.

보안 문제

SVRCONN 채널은 처음에 정의된 대로는 안전하지 않습니다. 예를 들어, SYSTEM.DEF.SVRCONN.SVRCONN 채널을 보안 설정하려면 `SET CHLAUTH` 명령을 사용하여 채널 인증을 설정하거나 보안 엑시트를 설치하고 TLS를 구현해야 합니다.

공개적으로 사용 가능한 샘플 보안 엑시트를 사용하거나, 보안 엑시트 자체를 작성하거나 보안 엑시트를 구매해야 합니다.

사용자 자체의 SVRCONN 채널 보안 엑시트를 작성하기 위한 좋은 시작점으로 사용할 수 있는 몇몇 샘플이 있습니다.

IBM MQ for z/OS에서 hlq.SCSQC37S 라이브러리의 구성원 CSQ4BCX3은 C 언어로 작성된 보안 엑시트 샘플입니다. 샘플 CSQ4BCX3 또한 hlq.SCSQAUTH 라이브러리에서 사전에 컴파일된 상태로 제공됩니다.

컴파일된 구성원 hlq.SCSQAUTH(CSQ4BCX3)를 CHIN Proc에서 CSQXLIB DD에 할당된 로드 라이브러리에 복사하여 CSQ4BCX3 샘플 엑시트를 구현할 수 있습니다. CHIN은 로드 라이브러리를 "프로그램 제어"로 설정해야 함을 유의하십시오.

CSQ4BCX3을 보안 엑시트로 설정하기 위해 SVRCONN 채널을 변경하십시오.

V 9.1.4 클라이언트가 이 SVRCONN 채널을 사용하여 연결하는 경우 CSQ4BCX3은 MQCD의 **RemoteUserIdentifier** 및 **RemotePassword** 쌍을 사용하여 인증하며, IBM MQ 9.1.4부터는 MQCSP의 **CSPUserIdPtr** 및 **CSPPasswordPtr** 쌍을 사용하여 인증합니다. 인증에 성공하면 **RemoteUserIdentifier**를 **MCAUserIdentifier**로 복사하며 스레드의 ID 컨텍스트를 변경합니다.

For Long Term Support and Continuous Delivery before IBM MQ 9.1.4, when a client connects using that SVRCONN channel, CSQ4BCX3 will authenticate using the **RemoteUserIdentifier** and **RemotePassword** pair from MQCD. 인증에 성공하면 **RemoteUserIdentifier**를 **MCAUserIdentifier**로 복사하며 스레드의 ID 컨텍스트를 변경합니다.

IBM MQ Java 클라이언트에 작성 중인 경우 팝업을 사용하여 사용자를 조회하고 MQEnvironment.userID 및 MQEnvironment.password를 설정할 수 있습니다. 이러한 값은 연결이 설정될 때 전달됩니다.

이제 기능 보안 종료기 있으므로 연결할 때 사용자 ID 및 비밀번호가 후속 IBM MQ 메시지의 콘텐츠에서와 같이 네트워크에서 일반 텍스트로 전송되는 추가 문제가 있습니다. TLS를 사용하여 이 초기 연결 정보와 IBM MQ 메시지의 콘텐츠를 암호화할 수 있습니다.

예

IBM MQ Explorer SVRCONN 채널 SYSTEM.ADMIN.SVRCONN 은 다음 단계를 완료합니다.

1. hlq.SCSQAUTH(CSQ4BCX3)를 CHINIT Proc에서 CSQXLIB DD에 할당된 로드 라이브러리에 복사하십시오.
2. 로드 라이브러리가 프로그램 제어임을 확인하십시오.
3. SYSTEM ADMIN.SVRCONN을 보안 엑시트 CSQ4BCX3을 사용하도록 변경하십시오.
4. IBM MQ Explorer에서 z/OS 큐 관리자 이름을 마우스 오른쪽 단추로 클릭하고 **연결 세부사항 > 특성 > 사용자 ID**를 선택하고 z/OS 사용자 ID를 입력하십시오.
5. 비밀번호를 입력하여 z/OS 큐 관리자에 연결하십시오.

추가 정보

CSQ4BCX3 엑시트를 프로그램 제어 환경에서 실행하려면 CHIN 주소 공간에 로드된 모든 것은 프로그램 제어 라이브러리에서 로드되어야 합니다. 예를 들어, STEPLIB의 모든 라이브러리 및 CSQXLIB DD에서 이름 지정된 모든 라이브러리입니다. 로드 라이브러리를 프로그램 제어로 설정하려면 RACF 명령을 실행하십시오. 다음 예에서 로드 라이브러리 이름은 MY.TEST.LOADLIB입니다.

```
RALTER PROGRAM * ADDMEM('MY.TEST.LOADLIB'//NOPADCHK)
SETROPTS WHEN(PROGRAM)REFRESH
```

CSQ4BCX3을 구현하도록 SVRCONN 채널을 변경하려면 다음 IBM MQ 명령을 실행하십시오.

```
ALTER CHANNEL(SYSTEM ADMIN.SVRCONN) CHLTYPE(SVRCONN) SCYEXIT(CSQ4BCX3)
```

위의 예에서 사용 중인 SVRCONN 채널은 SYSTEM ADMIN.SVRCONN입니다.

채널 엑시트에 대한 자세한 정보는 93 페이지의 『채널 엑시트 프로그램』의 내용을 참조하십시오.

관련 태스크

[z/OS에서 채널 엑시트 프로그램 작성](#)

SNA LU 6.2 보안 서비스

SNA LU 6.2는 세션 레벨 암호화, 세션 레벨 인증, 대화 레벨 인증을 제공합니다.

참고: 이 주제 모음에서는 SNA(Systems Network Architecture)에 대해 기본적으로 이해하고 있는 것으로 간주합니다. 이 절에서 언급하는 다른 문서에는 관련 개념 및 용어에 대한 간략한 소개가 포함됩니다. SNA에 대한 더 광범위한 기술적인 소개가 필요하다면, *Systems Network Architecture Technical Overview*, GC30-3073을 참조하십시오.

SNA LU 6.2는 세 개의 보안 서비스를 제공합니다.

- 세션 레벨 암호화
- 세션 레벨 인증
- 대화 레벨 인증

세션 레벨 암호화와 세션 레벨 인증에서는 SNA가 데이터 암호화 표준(DES) 알고리즘을 사용합니다. DES 알고리즘은 데이터를 암호화하고 복호화하기 위해 대칭 키를 사용하는 블록 암호 알고리즘입니다. 블록 및 키 모두 길이는 8바이트입니다.

세션 레벨 암호화

세션 레벨 암호화는 DES 알고리즘을 사용하여 세션 데이터를 암호화하고 복호화합니다. 따라서, SNA LU 6.2 채널에서 링크 레벨 기밀성 서비스를 제공하는 데 사용될 수 있습니다.

논리 장치(LU)는 필수(또는 필요한) 데이터 암호화, 선택 데이터 암호화 또는 데이터 암호화 없음을 제공합니다.

필수 암호화 세션에서 LU는 모든 아웃바운드 데이터 요청 장치를 암호화하고 모든 인바운드 데이터 요청 장치를 복호화합니다.

선택 암호화 세션에서 LU는 송신 트랜잭션 프로그램(TP)로 지정된 데이터 요청 장치만 암호화합니다. 송신 LU는 요청 헤더에 표시기를 설정하여 데이터가 암호화되었다는 것을 신호합니다. 이 표시기를 검사하여 수신 LU는 요청 장치를 수신 TP로 전달하기 전에 복호화해야 하는 요청 장치를 알려줄 수 있습니다.

SNA 네트워크에서 IBM MQ MCA는 트랜잭션 프로그램입니다. MCA는 송신하는 어떠한 데이터에 대한 암호화도 요청하지 않습니다. 선택 데이터 암호화가 옵션이 아니므로, 필수 데이터 암호화나 데이터 암호화 없음만이 세션에서 가능합니다.

필수 데이터 암호화 구현 방법에 대한 정보는 SNA 서브시스템 문서를 참조하십시오. 플랫폼에서 사용 가능할 수도 있는 더 강력한 암호화 양식(예: z/OS에서 3중 DES 24바이트 암호화)에 대한 정보는 동일한 문서를 참조하십시오.

세션 레벨 암호화에 대한 일반적인 정보는 *Systems Network Architecture LU 6.2 Reference: Peer Protocols*, SC31-6808을 참조하십시오.

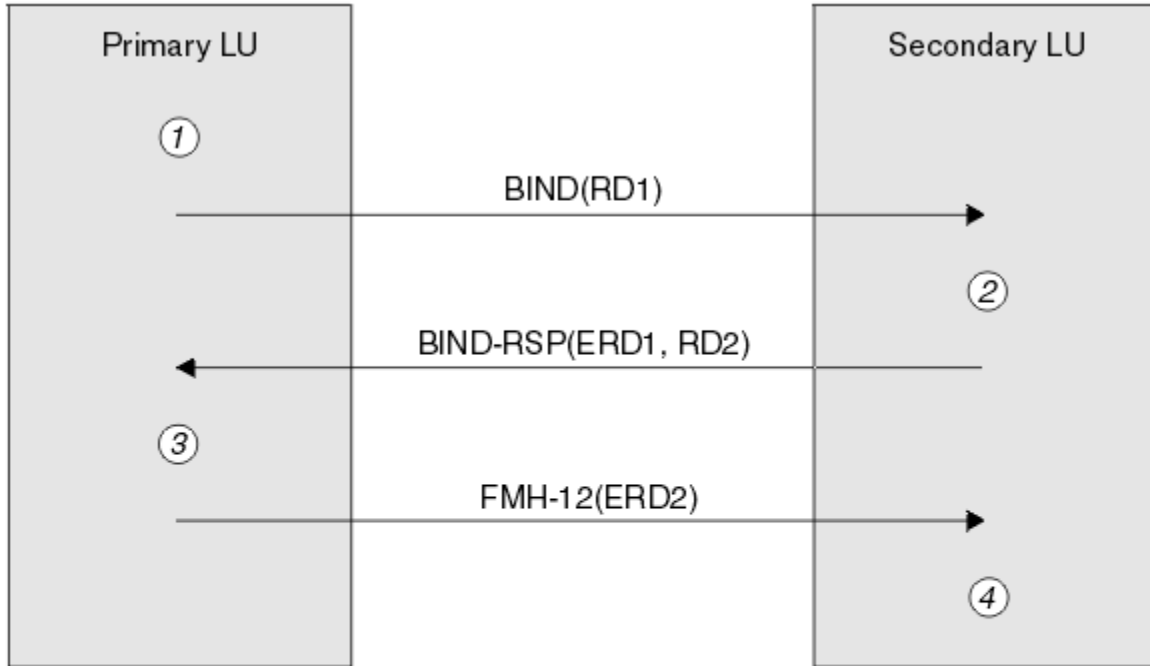
세션 레벨 인증

세션 레벨 인증은 두 개의 LU가 세션을 활성화하고 있는 동안에 서로 인증하게 하는 세션 레벨 보안 프로토콜입니다. LU-LU 확인이라고도 합니다.

LU는 네트워크에서 시스템으로의 효율적인 "게이트웨이"이기 때문에, 어떤 상황에서는 이런 레벨의 인증이 충분하다고 고려할 수도 있습니다. 예를 들면, 큐 관리자가, 제어되고 신뢰되는 환경에서 실행 중인 리모트 큐 관리자와 메시지를 교환해야 하면, LU가 인증된 후에는 원격 시스템의 나머지 구성요소의 ID를 신뢰할 준비가 되어 있을 수 있습니다.

각 LU가 그 파트너의 비밀번호를 확인하여 세션 레벨 인증이 수행됩니다. 하나의 비밀번호가 LU의 각 쌍 사이에서 설정되기 때문에 비밀번호를 LU-LU 비밀번호라고 합니다. LU-LU 비밀번호가 설정되는 방식은 구현에 따라 다르고 SNA의 범위 밖에 있습니다.

104 페이지의 그림 12는 세션 레벨 인증에 대한 플로우를 나타냅니다.



Legend:

BIND = BIND request unit
 BIND-RSP = BIND response unit
 ERD = Encrypted random data
 FMH-12 = Function Management Header 12
 RD = Random data

그림 12. 세션 레벨 인증 플로우

세션 레벨 인증의 프로토콜은 다음과 같습니다. 프로시저에 있는 번호는 104 페이지의 그림 12의 번호에 해당합니다.

1. 1차 LU가 무작위 데이터 값(RD1)을 생성하고 BIND 요청으로 2차 LU에게 송신합니다.
2. 2차 LU가 무작위 데이터가 있는 BIND 요청을 수신하면, DES 알고리즘을 사용하여 데이터를 암호화하고 LU-LU 비밀번호의 사본을 키로서 가집니다. 그러면 2차 LU가 2차 무작위 데이터 값(RD2)를 생성하고 이를 암호화된 데이터(ERD1)와 함께 BIND 응답의 1차 LU로 송신합니다.
3. 1차 LU가 BIND 응답을 수신하면, 원래 생성했던 무작위 데이터에서 암호화된 데이터의 자체 버전을 처리합니다. DES 알고리즘을 사용하여 이렇게 하고 LU-LU 비밀번호의 사본을 키로서 가집니다. 그런 후, BIND 응답에서 수신한 암호화된 데이터와 함께 그 버전을 비교합니다. 두 값이 같으면, 1차 LU는 2차 LU가 같은 비밀번호를 가지고 있다는 것을 알게 되고 2차 LU가 인증됩니다. 두 값이 일치하지 않으면, 1차 LU가 세션을 종료합니다.

 그런 다음, 1차 LU는 BIND 응답에서 수신한 무작위 데이터를 암호화하고 암호화된 데이터(ERD2)를 FMH-12(함수 관리 헤더 12)로 2차 LU에게 송신합니다.
4. 2차 LU가 FMH-12를 수신하면, 원래 생성했던 무작위 데이터에서 암호화된 데이터의 자체 버전을 처리합니다. 그런 후, FMH-12로 수신한 암호화된 데이터와 함께 해당 버전을 비교합니다. 두 값이 같으면, 1차 LU가 인증됩니다. 두 값이 일치하지 않으면, 2차 LU가 세션을 종료합니다.

중간자 공격에 대해 더 나은 보호를 제공하는 프로토콜의 개선된 버전에서, 2차 LU는 LU-LU 비밀번호의 사본을 키로서 사용하여 RD1, RD2와 2차 LU의 전체 이름으로부터 DES 메시지 인증 코드(MAC)를 처리합니다. 2차 LU가 ERD1 대신에 BIND 응답으로 MAC을 1차 LU에게 송신합니다.

1차 LU는 BIND 응답에서 수신한 MAC과 비교하는 자신의 MAC 버전을 처리하여 2차 LU를 인증합니다. 그런 후, 1차 LU는 RD1과 RD2의 두 번째 MAC을 처리하고, MAC을 ERD2 대신에 FMH-12로 2차 LU에게 송신합니다.

2차 LU는 FMH-12에서 수신한 MAC과 비교하는 자신의 2차 MAC 버전을 처리하여 1차 LU를 인증합니다.

세션 레벨 인증 구성 방법에 대한 정보는 SNA 서브시스템 문서를 참조하십시오. 세션 레벨 인증에 대해 더 일반적인 정보는 *Systems Network Architecture LU 6.2 Reference: Peer Protocols*, SC31-6808을 참조하십시오.

대화 레벨 인증

로컬 TP가 파트너 TP로 대화를 할당하려고 할 때, 로컬 LU가 파트너 LU로 첨부 요청을 송신하며, 파트너 LU가 파트너 TP를 첨부하도록 요청합니다. 어떤 상황에서는 첨부 요청이 보안 정보를 포함할 수 있으며, 파트너 LU가 로컬 TP를 인증하는 데 이를 사용할 수 있습니다. 이는 대화 레벨 인증 또는 일반 사용자 확인이라고 합니다.

다음 주제에서는 IBM MQ가 대화 레벨 인증에 대한 지원을 제공하는 방법에 대해 설명합니다.

대화 레벨 인증에 대한 자세한 정보는 *Systems Network Architecture LU 6.2 Reference: Peer Protocols*, SC31-6808을 참조하십시오. z/OS에 특정되는 정보는 *z/OS MVS Planning: APPC/MVS Management*, SA22-7599를 참조하십시오.

CPI-C에 대한 자세한 정보는 *Common Programming Interface Communications CPI-C Specification*, SC31-6180을 참조하십시오. APPC/MVS TP Conversation Callable Services에 대한 자세한 정보는 *z/OS MVS Programming: Writing Transaction Programs for APPC/MVS*, SA22-7621을 참조하십시오.



IBM i, UNIX 및 Windows에서 대화 레벨 인증 지원

이 주제를 사용하여 IBM i, UNIX 및 Windows에서 대화 레벨 인증이 작동하는 방법에 대한 개요를 확인하십시오.

IBM i, UNIX 및 Windows에서 대화 레벨 인증 지원은 [106 페이지의 그림 13](#)에서 설명됩니다. 다이어그램에 있는 번호는 그 뒤에 오는 설명에 있는 번호에 해당합니다.

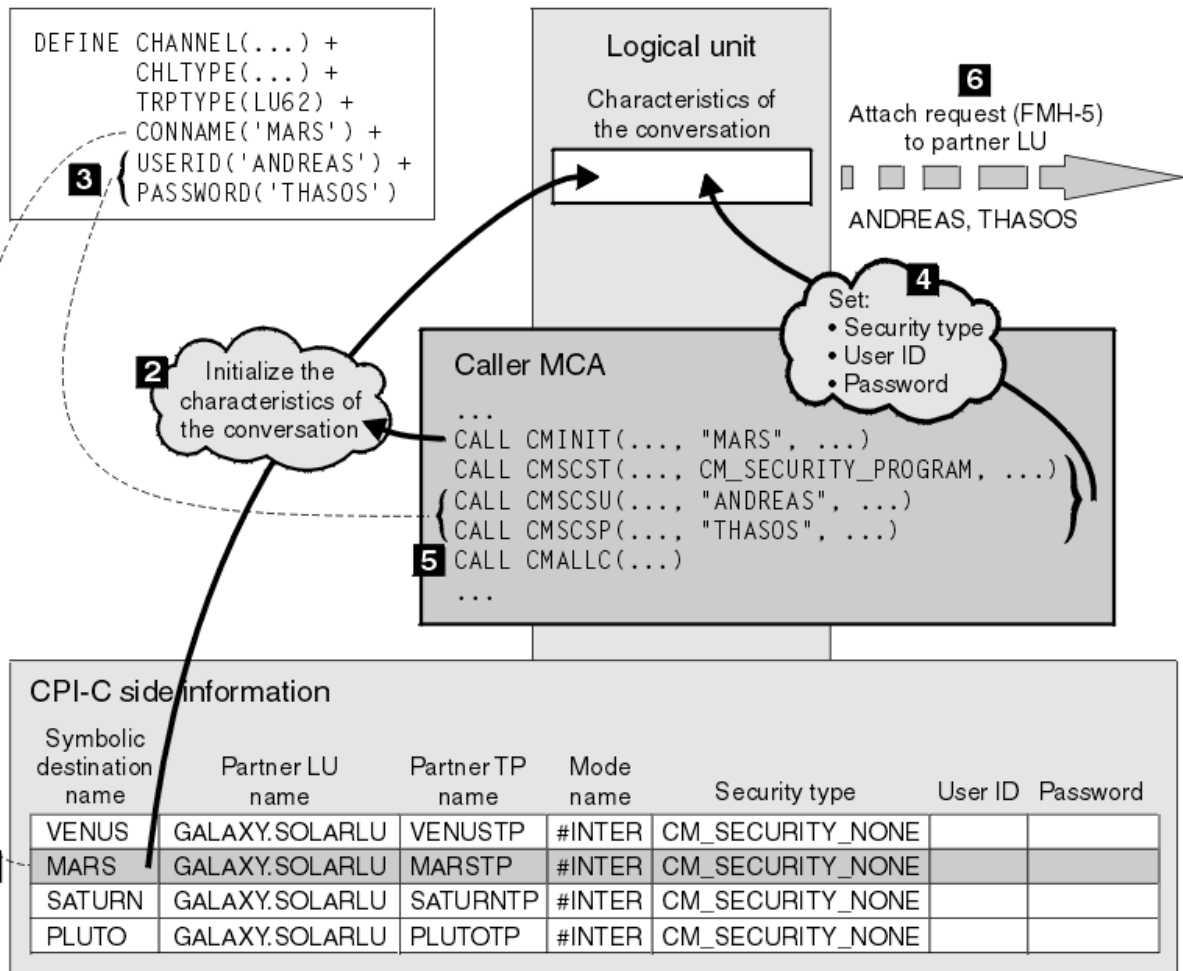


그림 13. 대화 레벨 인증에 대한 IBM MQ 지원

IBM i, UNIX, Windows에서 MCA는 CPI-C(Common Programming Interface Communications) 호출을 사용하여 SNA 네트워크에서 파트너 MCA와 통신합니다. 채널의 호출자 측에 있는 채널 정의에서, CONNAME 매개변수의 값은 목적지 기호 이름이며, 이는 CPI-C 부가 정보 항목(1)을 식별합니다. 이 항목은 다음을 지정합니다.

- 파트너 LU의 이름
- 응답 MCA인 파트너 TP의 이름
- 대화에 사용할 모드의 이름

부가 정보 항목은 다음 보안 정보도 지정할 수 있습니다.

- 보안 유형

흔히 구현되는 보안 유형은 CM_SECURITY_NONE, CM_SECURITY_PROGRAM, CM_SECURITY_SAME이지만, 다른 것이 CPI-C 스펙에 정의되어 있습니다.

- 사용자 ID
- 비밀번호

호출자 MCA가 호출에서 매개변수 중 하나로서 CONNAME의 값을 사용하여 CPI-C 호출 CMINIT를 발행함으로써 응답자 MCA에 대화를 할당하기 위해 준비합니다. CMINIT 호출이 로컬 LU의 특성으로, MCA가 대화에 사용하려고 하는 부가 정보 항목을 식별합니다. 로컬 LU는 대화의 특성을 초기화하기 위해 이 항목에 있는 값을 사용합니다(2).

그런 다음 호출자 MCA가 채널 정의에서 USERID와 PASSWORD 매개변수의 값을 검사합니다(3). USERID가 설정되면, 호출자 MCA가 다음 CPI-C 호출을 발행합니다(4).

- CMSCST - 대화의 보안 유형을 CM_SECURITY_PROGRAM으로 설정.

- CMSCSU - 대화의 사용자 ID를 USERID의 값으로 설정.
- CMSCSP - 대화의 비밀번호를 PASSWORD의 값으로 설정. PASSWORD가 설정되지 않으면, CMSCSP는 호출되지 않습니다.

이 호출이 설정하는 보안 유형, 사용자 ID와 비밀번호는 이전에 부가 정보 항목에서 얻은 모든 값을 대체합니다. 그런 후, 호출자 MCA가 CPI-C 호출 CMALLC를 발행하여 대화를 할당합니다(5). 이 호출에 응답하여, 로컬 LU가 첨부 요청(함수 관리 헤더 5, 즉 FMH-5)을 파트너 LU로 송신합니다(6).

파트너 LU가 사용자 ID와 비밀번호를 승인하면, USERID와 PASSWORD의 값이 첨부 요청에 포함됩니다. 파트너 LU가 사용자 ID와 비밀번호를 승인하지 않으면, 값이 첨부 요청에 포함되지 않습니다. LU들이 세션을 양식화하기 위해 바인딩할 때 로컬 LU는 파트너 LU가 사용자 ID와 비밀번호를 정보 교환의 일부로서 승인할 것인지를 알아냅니다.

첨부 요청의 이후 버전에서는 비밀번호 대체가 명확한 비밀번호 대신에 LU 사이에서 플로우될 수 있습니다. 비밀번호 대체는 비밀번호에서 양식화된 DES 메시지 인증 코드(MAC) 또는 SHA-1 메시지 요약입니다. 비밀번호 대체는 두 LU가 모두 그것을 지원하는 경우에만 사용될 수 있습니다.

파트너 LU가 사용자 ID와 비밀번호가 있는 첨부 요청을 수신하면, 식별과 인증을 목적으로 사용자 ID와 비밀번호를 사용할 수 있습니다. 액세스 제어 목록을 참조하여, 파트너 LU는 사용자 ID가 대화를 할당하고 응답 MCA를 첨부할 수 있는 권한을 가지는지도 판별할 수 있습니다.

또한, 응답 MCA는 첨부 요청에 포함된 사용자 ID에서 실행될 수 있습니다. 이런 경우에, 사용자 ID는 응답 MCA에 대한 디폴트 사용자 ID가 되고 MCA가 큐 관리자에 연결하려고 할 때 권한 검사에 사용됩니다. 이는 MCA가 큐 관리자의 자원에 액세스하려고 할 때 계속해서 권한 검사를 위해 사용될 수도 있습니다.

첨부 요청의 사용자 ID와 비밀번호가 식별, 인증, 액세스 제어를 위해 사용될 수 있는 방법은 구현에 따라 다릅니다. 사용자의 SNA 서브시스템에만 적용되는 정보는 해당 문서를 참조하십시오.

USERID가 설정되지 않으면, 호출자 MCA가 CMSCST, CMSCSU, CMSCSP를 호출하지 않습니다. 이런 경우에, 첨부 요청에서 플로우되는 보안 정보는 부가 정보 항목에 지정된 것과 파트너 LU가 승인하는 것에 의해서만 판별됩니다.

대화 레벨 인증 및 *IBM MQ for z/OS*

이 토픽을 사용하여 z/OS에서 대화 레벨 인증이 작동하는 방법에 대한 개요를 확인하십시오.

IBM MQ for z/OS에서 MCA는 CPI-C를 사용하지 않습니다. 대신에, 일부 CPI-C 특성을 가지는 APPC(Advanced Program-to-Program Communication)의 구현인 APPC/MVS TP Conversation Callable Services를 사용합니다. 호출자 MCA가 대화를 할당하면, SAME이라는 보안 유형이 호출에서 지정됩니다. 그러므로, APPC/MVS LU가 아웃바운드 대화가 아니라 인바운드 대화에 대해서만 지속 확인을 지원하기 때문에, 두 가지 가능성이 있습니다.

- 파트너 LU가 APPC/MVS LU를 트러스트하고 이미 확인된 사용자 ID를 승인하면, APPC/MVS LU가 다음을 포함하는 첨부 요청을 송신합니다.
 - 채널 시작기 주소 공간 사용자 ID
 - RACF가 사용되는 채널 시작기 주소 공간 사용자 ID의 현재 연결 그룹 이름인 보안 프로파일 이름
 - 이미 확인된 표시기
- 파트너 LU가 APPC/MVS LU를 트러스트하지 않고 이미 확인된 사용자 ID를 승인하지 않으면, APPC/MVS LU가 보안 정보를 포함하지 않는 첨부 요청을 송신합니다.

IBM MQ for z/OS에서 DEFINE CHANNEL 명령의 USERID 및 PASSWORD 매개변수는 메시지 채널에 사용될 수 없으며 MQI 채널의 클라이언트 연결 끝에서만 유효합니다. 그러므로, APPC/MVS LU의 첨부 요청은 이 매개변수에 의해 지정되는 값은 절대로 포함하지 않습니다.

큐 관리자 클러스터의 보안

큐 관리자 클러스터가 사용하기는 편리하지만 보안에는 주의해야 합니다.

큐 관리자 클러스터는 일부 방식에서 논리적으로 연관된 큐 관리자의 네트워크입니다. 클러스터의 멤버인 큐 관리자를 클러스터 큐 관리자라 합니다.

클러스터 큐 관리자에 속하는 큐를 같은 클러스터의 다른 큐 관리자가 알도록 할 수 있습니다. 이런 큐를 클러스터 큐라고 합니다. 클러스터의 모든 큐 관리자는 다음 중에서 아무것도 알지 못해도 클러스터 큐에 메시지를 송신할 수 있습니다.

- 각 클러스터 큐에 대한 명시적인 리모트 큐 정의
- 각 리모트 큐 관리자로 송신 및 수신을 위해 명백히 정의된 채널
- 각 아웃바운드 채널에 대한 별도의 전송 큐

두 개 이상의 큐 관리자가 복제되는 클러스터를 작성할 수 있습니다. 즉, 큐 관리자가 클러스터 큐로 선언된 모든 로컬 큐를 비롯하여 동일한 로컬 큐의 인스턴스를 포함하고 동일한 서버 애플리케이션의 인스턴스를 지원할 수 있습니다.

클러스터 큐 관리자에 연결된 애플리케이션이 메시지를 복제된 큐 관리자 각각에서 인스턴스를 포함하는 클러스터 큐로 송신하면 IBM MQ는 이를 송신할 큐 관리자를 결정합니다. 다수의 애플리케이션이 메시지를 클러스터 큐에 송신하는 경우, IBM MQ는 큐의 인스턴스를 포함하는 각 큐 관리자에서 워크로드 밸런스를 유지합니다. 복제된 큐 관리자를 호스트하는 시스템 중 하나가 실패하면 IBM MQ는 실패한 시스템에 재시작될 때까지 나머지 큐 관리자에서 워크로드 밸런스를 계속 유지합니다.

큐 관리자 클러스터를 사용하는 경우 다음의 보안 문제점을 고려해야 합니다.


- 선택된 큐 관리자만 큐 관리자로 메시지를 송신하도록 허용
- 리모트 큐 관리자의 선택된 사용자만 큐 관리자의 큐로 메시지를 송신하도록 허용
- 큐 관리자에 연결된 애플리케이션이 선택된 리모트 큐로만 메시지를 송신하도록 허용

클러스터를 사용하고 있지 않아도 이 사항들은 관련이 있으며, 클러스터를 사용하고 있으면 더욱 중요합니다.

애플리케이션이 한 클러스터 큐로 메시지를 송신하면, 추가 리모트 큐 정의나 전송 큐 또는 채널 없이도 다른 모든 클러스터 큐로 메시지를 송신할 수 있습니다. 따라서, 큐 관리자의 클러스터 큐에 대한 액세스를 제한하고 애플리케이션이 메시지를 송신할 수 있는 클러스터 큐를 제한해야 하는지를 고려하는 것이 더욱 중요할 수 있습니다.

다음은 큐 관리자 클러스터를 사용하고 있는 경우에만 관련이 있는 일부 추가 보안 고려사항입니다.

- 선택된 큐 관리자만 클러스터를 조인하도록 허용
- 필요하지 않은 큐 관리자는 클러스터에서 강제로 제거

이 모든 고려사항에 대한 자세한 정보는 클러스터 안전 유지를 참조하십시오.  IBM MQ for z/OS 고유의 고려사항은 235 페이지의 『z/OS의 큐 관리자 클러스터에서 보안』의 내용을 참조하십시오.

관련 태스크

414 페이지의 『큐 관리자가 메시지 수신하는 것을 방지』

엑시트 프로그램을 사용하여 클러스터 큐 관리자가 수신할 권한이 없는 메시지를 수신하는 것을 막을 수 있습니다.

IBM MQ 발행/구독에 대한 보안

IBM MQ 발행/구독을 사용 중인 경우에는 추가 보안 고려사항이 있습니다.

발행/구독 시스템에는 발행자와 구독자의 두 애플리케이션 유형이 있습니다. 발행자는 IBM MQ 메시지의 양식으로 정보를 제공합니다. 발행자가 메시지를 발행하면, 메시지에 있는 정보의 주제를 식별하는 토픽을 지정합니다.

구독자는 발행되는 정보의 사용자입니다. 구독자는 토픽을 구독하여 관심 토픽을 지정합니다.

큐 관리자는 IBM MQ 발행/구독에서 제공되는 애플리케이션입니다. 이는 발행자에서 발행된 메시지를 수신하고 구독자에서 구독 요청을 수신하여 발행된 메시지를 구독자에게 라우트합니다. 구독자는 구독된 해당 토픽의 메시지만 수신합니다.

자세한 정보는 [발행/구독 보안](#)을 참조하십시오.

멀티캐스트 보안

이 정보를 사용하여 보안 프로세스가 IBM MQ 멀티캐스트에 필요한 이유를 이해하십시오.

IBM MQ Multicast는 기본 제공 보안이 필요하지 않습니다. 보안 검사는 MQOPEN 시에 큐 관리자에서 처리되고 MQMD 필드 설정은 클라이언트에서 처리됩니다. 네트워크에 있는 일부 애플리케이션은 IBM MQ 애플리케이션이 아닐 수 있습니다(예: LLM 애플리케이션. 자세한 정보는 [IBM MQ LLM\(Low Latency Messaging\)과의 멀티캐스트 상호 운용성 참조](#)). 따라서 수신 애플리케이션이 컨텍스트 필드의 유효성을 확인할 수 없으므로 자체 보안 프로시저를 구현해야 할 수도 있습니다.

고려해야 하는 보안 프로세스는 세 가지입니다.

액세스 제어

IBM MQ의 액세스 제어는 사용자 ID를 기반으로 합니다. 이 주제에 대한 자세한 정보는 [86 페이지의 『클라이언트의 액세스 제어』](#)의 내용을 참조하십시오.

네트워크 보안

격리된 네트워크는 허위 메시지를 방지하는 가능한 보안 옵션일 수 있습니다. 멀티캐스트 그룹 주소의 애플리케이션이 고유 통신 기능을 사용하여 악의적인 메시지(동일한 멀티캐스트 그룹 주소의 애플리케이션에서 오기 때문에 MQ 메시지가 구분할 수 없음)를 발행할 수 있습니다.

멀티캐스트 그룹 주소의 클라이언트가 동일한 멀티캐스트 그룹 주소의 다른 클라이언트에 대한 메시지를 수신할 수도 있습니다.

멀티캐스트 네트워크를 격리하면 올바른 클라이언트 및 애플리케이션만 액세스를 가지도록 할 수 있습니다. 이 보안 예방책을 사용하여 악의적인 메시지가 수신되는 것과 기밀 정보가 송신되는 것을 방지할 수 있습니다.

멀티캐스트 그룹 네트워크 주소에 대한 정보는 [멀티캐스트 트래픽에 적절한 네트워크 설정을 참조하십시오](#).

디지털 서명

디지털 서명은 메시지의 표현을 암호화하여 형성됩니다. 암호화는 서명인의 개인 키를 사용하고, 효율성을 위해 보통 메시지 자체가 아니라 메시지 요약에 대해 작동합니다. MQPUT 이전에는 메시지 디지털 서명이 좋은 보안 해결책이었지만 이 프로세스는 메시지의 볼륨이 큰 경우 성능에 좋지 않은 영향을 줄 수도 있습니다.

디지털 서명은 서명 중인 데이터에 따라 다릅니다. 두 개의 다른 메시지가 같은 엔티티에 의해 디지털로 서명되면 두 서명은 서로 다르지만 둘 다 같은 공개 키, 즉, 이 메시지에 서명한 엔티티의 공개 키를 사용하여 확인됩니다.

이 절의 앞에서 언급한 것처럼 멀티캐스트 그룹 주소의 애플리케이션이 고유 통신 기능을 사용하여 악의적인 메시지를 발행할 수 있으며, 이는 MQ 메시지에서 구별할 수 없습니다. 디지털 서명은 원본 증명을 제공하며 송신자만 개인 키를 알기 때문에 송신자가 메시지의 진원지인 강력한 증거를 제시합니다.

이 주제에 대한 자세한 정보는 [7 페이지의 『암호화 개념』](#)의 내용을 참조하십시오.

방화벽 및 인터넷 Passthru

일반적으로 방화벽을 사용하여 적대적인 IP 주소(예: 서비스 거부 공격)에서 액세스를 방지합니다. 그렇지만 보안 관리자가 방화벽 규칙을 업데이트하기를 대기하는 동안처럼 IBM MQ 내에서 임시로 IP 주소를 차단해야 할 수도 있습니다.

하나 이상의 IP 주소를 차단하려면 유형 BLOCKADDR 또는 ADDRESSMAP의 채널 인증 레코드를 작성하십시오. 자세한 정보는 [344 페이지의 『특정 IP 주소 차단』](#)의 내용을 참조하십시오.

IBM MQ Internet Pass-Thru 보안

IBM MQ Internet Pass-Thru는 방화벽을 통한 통신을 간소화할 수 있지만, 이는 보안에 영향을 줍니다.

IBM MQ Internet Pass-Thru(MQIPT)는 인터넷을 통한 원격 사이트 간 메시징 솔루션을 구현하는 데 사용할 수 있는, IBM MQ의 선택적 컴포넌트입니다.

MQIPT는 직접 TCP/IP 연결 없이도 인터넷을 통해 두 큐 관리자가 메시지를 교환할 수 있도록 하거나, IBM MQ 클라이언트 애플리케이션이 큐 관리자에 연결할 수 있도록 합니다. 방화벽이 두 시스템 사이에 직접적인 TCP/IP 연결을 막는 경우에 이 기능이 유용합니다. HTTP 내의 플로우를 터널링하거나 프록시로 작동하여 방화벽을 통과하는 IBM MQ 채널 프로토콜 플로우 통로가 더 단순해지고 관리하기도 쉬워집니다. TLS(Transport Layer Security)를 사용하여 인터넷에서 송신되는 메시지를 암호화하고 비밀번호를 해독하는 데 사용할 수도 있습니다.

IBM MQ 시스템이 MQIPT와 통신하는 경우, MQIPT에서 SSL 프록시 모드를 사용하는 경우를 제외하면 IBM MQ가 사용하는 CipherSpec이 MQIPT가 사용하는 CipherSuite와 일치하도록 하십시오.

- MQIPT가 TLS 서버 역할을 수행하며 IBM MQ가 TLS 클라이언트로서 연결하는 경우, IBM MQ가 사용하는 CipherSpec은 관련 MQIPT 키 링에서 사용으로 설정된 CipherSuite에 대응해야 합니다.
- MQIPT가 TLS 클라이언트 역할을 수행하며 IBM MQ TLS 서버에 연결하는 경우, MQIPT CipherSuite는 수신 IBM MQ 채널에 정의된 CipherSpec과 일치해야 합니다.

MQIPT에서 통합된 IBM MQ TLS 지원으로 마이그레이션하는 경우, `mqiptKeyman` 또는 `mqiptKeycmd`를 사용하여 MQIPT 키 링에서 디지털 인증서를 전송하십시오.

자세한 정보는 [IBM MQ Internet Pass-Thru](#)의 내용을 참조하십시오.

z/OS IBM MQ for z/OS 보안 구현 체크리스트

이 토픽은 각 IBM MQ 큐 관리자에 대한 보안 구현에 대해 작업하고 정의하기 위해 사용할 수 있는 단계별 프로시저를 제공합니다.

RACF는 제공되는 해당 정적 CDT(Class Descriptor Table)에서 IBM MQ 보안 클래스에 대한 정의를 제공합니다. 체크리스트를 통해 작업하는 동안 설정이 필요한 해당 클래스를 판별할 수 있습니다. [165 페이지의 『RACF 보안 클래스』](#)에서 설명하는 대로 이를 활성화해야 합니다.

자세한 내용은 다른 절(특히, [175 페이지의 『IBM MQ 자원에 대한 액세스 제어에 사용되는 프로파일』](#))을 참조하십시오.

보안 검사가 필요한 경우 이 체크리스트에 따라 구현하십시오.

1. RACF MQADMIN(대문자 프로파일) 또는 MXADMIN(대소문자 혼합 프로파일) 클래스를 활성화하십시오.
 - 큐 공유 그룹 레벨, 큐 관리자 레벨 또는 둘의 결합에서 보안이 필요합니까?
[170 페이지의 『큐 공유 그룹 또는 큐 관리자 레벨 보안을 제어할 프로파일』](#)의 내용을 참조하십시오.
2. 연결 보안이 필요합니까?
 - 예: MQCONN 클래스를 활성화하십시오. 큐 관리자 레벨이나 큐 공유 그룹 레벨의 적절한 연결 프로파일을 MQCONN 클래스에 정의하십시오. 그런 다음 해당 프로파일에 적절한 사용자나 그룹 액세스를 허용하십시오.
참고: MQCONN API 요청의 사용자 또는 CICS 또는 IMS 주소 공간 사용자 ID만 해당 연결 프로파일에 대한 액세스가 필요합니다.
 - 아니오: 큐 관리자 레벨 또는 큐 공유 그룹 레벨의 hlq.NO.CONNECT.CHECKS 프로파일을 MQADMIN 또는 MXADMIN 클래스에 정의하십시오.
3. 명령에서 보안 검사가 필요합니까?
 - 예: MQCMDS 클래스를 활성화하십시오. 큐 관리자 레벨이나 큐 공유 그룹 레벨에서 적절한 명령 프로파일을 MQCMDS 클래스에 정의하십시오. 그런 다음 해당 프로파일에 적절한 사용자나 그룹 액세스를 허용하십시오.
큐 공유 그룹을 사용 중인 경우 큐 관리자 자체 및 채널 시작기에서 사용되는 사용자 ID를 포함해야 할 수도 있습니다. [227 페이지의 『IBM MQ for z/OS 자원 보안 설정』](#)의 내용을 참조하십시오.
 - 아니오: 필수 큐 관리자 또는 큐 공유 그룹의 hlq.NO.CMD.CHECKS 프로파일을 MQADMIN 또는 MXADMIN 클래스에 정의하십시오.
4. 명령에서 사용되는 자원에 보안이 필요합니까?
 - 예: MQADMIN 또는 MXADMIN 클래스가 활성화되어 있어야 합니다. 큐 관리자 레벨이나 큐 공유 그룹 레벨의 명령의 자원 보호를 위한 적절한 프로파일을 MQADMIN 또는 MXADMIN 클래스에 정의하십시오. 그런 다음 해당 프로파일에 적절한 사용자나 그룹 액세스를 허용하십시오. CSQ6SYSP에서 CMDUSER 매개 변수를 명령 보안 검사에 사용되는 기본 사용자 ID로 설정하십시오.
큐 공유 그룹을 사용 중인 경우 큐 관리자 자체 및 채널 시작기에서 사용되는 사용자 ID를 포함해야 할 수도 있습니다. [227 페이지의 『IBM MQ for z/OS 자원 보안 설정』](#)의 내용을 참조하십시오.
 - 아니오: 필수 큐 관리자 또는 큐 공유 그룹의 hlq.NO.CMD.RESC.CHECKS 프로파일을 MQADMIN 또는 MXADMIN 클래스에 정의하십시오.

5. 큐 보안이 필요합니까?

- **예:** MQQUEUE 또는 MXQUEUE 클래스를 활성화하십시오. 필수 큐 관리자 또는 큐 공유 그룹에 필요한 적절한 큐 프로파일을 MQQUEUE 또는 MXQUEUE 클래스에 정의하십시오. 그런 다음 해당 프로파일에 적절한 사용자나 그룹 액세스를 허용하십시오.
- **아니오:** 필수 큐 관리자 또는 큐 공유 그룹의 hlq.NO.QUEUE.CHECKS 프로파일을 MQADMIN 또는 MXADMIN 클래스에 정의하십시오.

6. 프로세스 보안이 필요합니까?

- **예:** MQPROC 또는 MXPROC 클래스를 활성화하십시오. 큐 관리자나 큐 공유 그룹 레벨에서 적절한 프로세스 프로파일을 정의하고 적절한 사용자 또는 그룹 액세스를 해당 프로파일에 허용하십시오.
- **아니오:** 적절한 큐 관리자 또는 큐 공유 그룹의 hlq.NO.PROCESS.CHECKS 프로파일을 MQADMIN 또는 MXADMIN 클래스에 정의하십시오.

7. 이름 목록 보안이 필요합니까?

- **예:** MQNLIST 또는 MXNLIST 클래스를 활성화하십시오. 큐 관리자 레벨이나 큐 공유 그룹 레벨의 적절한 이름 목록 프로파일을 MQNLIST 또는 MXNLIST 클래스에 정의하십시오. 그런 다음 해당 프로파일에 적절한 사용자나 그룹 액세스를 허용하십시오.
- **아니오:** 필수 큐 관리자 또는 큐 공유 그룹의 hlq.NO.NLIST.CHECKS 프로파일을 MQADMIN 또는 MXADMIN 클래스에 정의하십시오.

8. 토픽 보안이 필요합니까?

- **예:** MXTOPIC 클래스를 활성화하십시오. 큐 관리자 레벨이나 큐 공유 그룹 레벨에서 적절한 토픽 프로파일을 MXTOPIC 클래스에 정의하십시오. 그런 다음 해당 프로파일에 적절한 사용자나 그룹 액세스를 허용하십시오.
- **아니오:** 필수 큐 관리자 또는 큐 공유 그룹의 hlq.NO.TOPIC.CHECKS 프로파일을 MQADMIN 또는 MXADMIN 클래스에 정의하십시오.

9. 컨텍스트 사용에 관련되어 MQOPEN 또는 MQPUT1 옵션 사용을 보호해야 하는 사용자가 있습니까?

- **예:** MQADMIN 또는 MXADMIN 클래스가 활성화되어 있어야 합니다. 큐, 큐 관리자 또는 큐 공유 그룹 레벨의 명령의 hlq.CONTEXT.queueName 프로파일을 MQADMIN 또는 MXADMIN 클래스에 정의하십시오. 그런 다음 해당 프로파일에 적절한 사용자나 그룹 액세스를 허용하십시오.
- **아니오:** 필수 큐 관리자 또는 큐 공유 그룹의 hlq.NO.CONTEXT.CHECKS 프로파일을 MQADMIN 또는 MXADMIN 클래스에 정의하십시오.

10. 대체 사용자 ID 사용을 보호해야 합니까?

- **예:** MQADMIN 또는 MXADMIN 클래스가 활성화되어 있어야 합니다. 필수 큐 관리자 또는 큐 공유 그룹에 대해 적절한 hlq.ALTERNATE.USER.alternateuserid 프로파일을 정의하고 필수 사용자 또는 그룹 액세스를 해당 프로파일에 허용하십시오.
- **아니오:** 필수 큐 관리자 또는 큐 공유 그룹의 hlq.NO.ALTERNATE.USER.CHECKS 프로파일을 MQADMIN 또는 MXADMIN 클래스에 정의하십시오.

11. RESLEVEL을 통해 자원 보안 검사에 사용되는 사용자 ID를 조정해야 합니까?

- **예:** MQADMIN 또는 MXADMIN 클래스가 활성화되어 있어야 합니다. 큐 관리자 레벨 또는 큐 공유 그룹 레벨의 hlq.RESLEVEL 프로파일을 MQADMIN 또는 MXADMIN 클래스에 정의하십시오. 그런 다음 프로파일에 필수 사용자나 그룹 액세스를 허용하십시오.
- **아니오:** hlq.RESLEVEL 적용 가능한 일반 프로파일이 MQADMIN 또는 MXADMIN 클래스에 없도록 하십시오. 필수 큐 관리자 또는 큐 공유 그룹에 대한 hlq.RESLEVEL 프로파일을 정의하고 사용자나 그룹이 이에 액세스하지 않도록 하십시오.

12. IBM MQ에서 사용되는 많은 사용자 ID를 '제한시간 초과'해야 합니까?

- **예:** 사용하려는 제한시간 값을 결정하고 MQSC ALTER SECURITY 명령을 발행하여 TIMEOUT 및 INTERVAL 매개변수를 변경하십시오.
- **아니오:** MQSC ALTER SECURITY 명령을 발행하여 INTERVAL 값을 0으로 설정하십시오.

참고: MQSC ALTER SECURITY 명령이 큐 관리자 시작 시에 자동으로 발행되도록 서브시스템에서 사용되는 CSQINP1 초기화 입력 데이터 세트를 업데이트하십시오.

13. 분산 큐잉을 사용합니까?

- 예: 채널 인증 레코드를 사용하십시오. 자세한 정보는 [43 페이지의 『채널 인증 레코드』](#)의 내용을 참조하십시오.
- 각 채널에 대해 적절한 MCAUSER 속성 값을 판별하거나 적합한 채널 보안 엑시트를 제공할 수 있습니다.

14. TLS(Transport Layer Security)를 사용하시겠습니까?

- 예: 지정된 DN을 포함하는 TLS 개인 인증서를 제출하는 사용자가 특정 MCAUSER를 사용하도록 지정하려면 SSLPEERMAP 유형의 채널 인증 레코드를 설정하십시오. 와일드카드가 포함된 패턴 또는 단일 식별 이름을 지정할 수 있습니다.
- TLS 인프라를 계획하십시오. z/OS의 시스템 SSL 기능을 설치하십시오. RACF에서 CNF(Certificate Name Filter) 및 디지털 인증서를 사용 중인 경우 이를 설정하십시오. SSL 키링을 설정하십시오. SSLKEYR 큐 관리자 속성이 공백이 아니고 SSL 키링을 지시하도록 하십시오. 또한, SSLTASKS 값이 2이상하도록 하십시오.
- 아니요: SSLKEYR이 공백이고 SSLTASKS는 0이도록 하십시오.

TLS에 대한 자세한 내용은 [21 페이지의 『IBM MQ의 TLS 보안 프로토콜』](#)의 내용을 참조하십시오.

15. 클라이언트를 사용합니까?

- 예: 채널 인증 레코드를 사용하십시오.
- 각 서버 연결 채널에 대해 적절한 MCAUSER 속성을 판별하거나 필요한 경우 적합한 채널 보안 엑시트를 제공할 수 있습니다.

16. 스위치 설정을 검사하십시오.

IBM MQ는 큐 관리자가 시작될 때 보안 설정을 표시하는 메시지를 발행합니다. 이 메시지를 사용하여 스위치가 제대로 설정되었는지 판별하십시오.

17. 클라이언트 애플리케이션에서 비밀번호를 송신합니까?

- 예: z/OS 기능이 설치되어 ICSF(Integrated Cryptographic Service Facility)가 최적의 보호를 위해 시작되도록 하십시오.
- 아니요: ICSF가 시작되지 않았음을 보고하는 오류 메시지를 무시할 수 있습니다.

ICSF에 대한 자세한 정보는 [235 페이지의 『ICSF\(Integrated Cryptographic Service Facility\) 사용』](#)의 내용을 참조하십시오.

보안 설정

이 토픽 컬렉션에는 다른 운영 체제 및 클라이언트 사용에 특정되는 정보가 포함됩니다.

ULW UNIX, Linux, and Windows에서 보안 설정

UNIX, Linux, and Windows 시스템 특정 보안 고려사항입니다.

IBM MQ 큐 관리자는 잠재적으로 중요한 정보를 전송하기 때문에 권한 시스템을 사용하여 권한 없는 사용자가 큐 관리자에 액세스하지 못하도록 해야 합니다. 다음과 같은 보안 제어 유형을 고려하십시오.

IBM MQ 관리 사용자

IBM MQ 관리를 위해 명령을 발행할 수 있는 사용자 세트를 정의할 수 있습니다.

IBM MQ 오브젝트 사용자

MQI 호출 및 PCF 명령을 사용하여 다음을 수행할 수 있는 사용자(주로 애플리케이션)를 정의할 수 있습니다.

- 큐 관리자 연결 사용자
- 오브젝트(큐, 프로세스 정의, 이름 목록, 채널, 클라이언트 연결 채널, 리스너, 서비스 및 인증 정보 오브젝트)에 액세스할 수 있는 사용자 및 해당 오브젝트에 대해 필요한 액세스 유형.
- IBM MQ 메시지에 액세스하는 사용자.
- 메시지와 연관된 컨텍스트 정보에 액세스할 수 있는 사용자.

채널 보안

메시지를 원격 시스템에 송신하는 데 사용되는 채널이 필수 자원에 액세스할 수 있도록 해야 합니다.

표준 조작 기능을 사용하여 프로그램 라이브러리, MQI 링크 라이브러리 및 명령에 대한 액세스를 부여할 수 있습니다. 그렇지만 큐 및 기타 큐 관리자 데이터가 포함된 디렉토리는 IBM MQ에 대해 개인용입니다. MQI 자원에 권한을 부여하거나 취소하는 경우에는 표준 운영 체제 명령을 사용하지 마십시오.

ULW UNIX, Linux, and Windows에서의 권한 작동 방법

이 절의 주제에 있는 권한 스펙 표는 권한이 작동하는 방법 및 적용되는 제한사항을 정확하게 정의합니다.

표는 다음과 같은 상황에 적용됩니다.

- MQI 호출을 발행한 애플리케이션
- 이스케이프 PCF로 MQSC 명령을 발행하는 관리 프로그램
- PCF 명령을 발행하는 관리 프로그램

이 절에서 정보는 다음을 지정하는 표의 세트로 표시됩니다.

수행할 조치

MQI 옵션, MQSC 명령 또는 PCF 명령

액세스 제어 오브젝트

큐, 프로세스, 큐 관리자, 이름 목록, 인증 정보, 채널, 클라이언트 연결 채널, 리스너 또는 서비스.

필수 권한

MQZAO_ 상수로 표현됩니다.

표에서 접두부가 MQZAO_인 상수는 특정 엔티티를 위한 setmqaut 명령에 대한 권한 목록의 키워드에 대응합니다. 예를 들어, MQZAO_BROWSE는 키워드 +browse에 대응하고 MQZAO_SET_ALL_CONTEXT는 키워드 +setall 등에 대응합니다. 이런 상수는 제품에서 제공하는 헤더 파일 cmqzc.h에 정의됩니다.

ULW MQI 호출에 대한 권한 부여

MQCONN, MQOPEN, MQPUT1, MQCLOSE에서 권한 검사가 필요할 수도 있습니다. 이 주제의 표에는 각 호출에 필요한 권한이 요약되어 있습니다.

실행 중인(또는 권한으로 간주 가능한) 사용자 ID에 관련 권한이 부여된 경우에만 애플리케이션은 특정 MQI 호출 및 옵션을 발행하도록 허용됩니다.

MQI 호출에 권한 검사가 필요할 수 있습니다. **MQCONN, MQOPEN, MQPUT1, MQCLOSE.**

MQOPEN 및 MQPUT1의 경우, 권한 검사는 이름이 해결된 후의 이름에서가 아니라 열려 있는 오브젝트 이름에 대해 수행됩니다. 예를 들면, 애플리케이션에는 알리어스가 해석되는 기본 큐를 열 수 있는 권한은 부여되지 않고 알리어스 큐를 열 수 있는 권한이 부여될 수 있습니다. 큐 관리자 알리어스 정의가 직접 열리는 경우(즉, 해당 이름이 오브젝트 디스크립터의 *ObjectName* 필드에 표시)를 제외하고 큐 관리자 알리어스가 아닌 이름을 해결하는 프로세스 중에 발생하는 첫 번째 정의에서 검사가 수행되는 것이 규칙입니다. 열려 있는 오브젝트에 대한 권한은 항상 필요합니다. 큐 관리자 오브젝트의 권한 부여를 통해 확보되는 추가 큐 독립 권한이 필요한 경우도 있습니다.

114 페이지의 표 10, 114 페이지의 표 11, 114 페이지의 표 12, 115 페이지의 표 13에는 각 호출에 필요한 권한이 요약되어 있습니다. 표에서 적용할 수 없음은 권한 검사가 이 조작과 관련이 없음을 의미하며, 검사 안함은 권한 검사를 수행하지 않음을 의미합니다.

참고: 이 표에서는 이름 목록, 채널, 클라이언트 연결 채널, 리스너, 서비스 또는 인증 정보 오브젝트에 대해 언급하지 않습니다. 이는 동일한 권한이 다른 오브젝트에도 적용되는 MQOO_INQUIRE를 제외하고 이러한 오브젝트에 적용되는 권한이 없기 때문입니다.

특수 권한 MQZAO_ALL_MQI에는 관리 권한으로 분류되는 MQZAO_DELETE 및 MQZAO_DISPLAY를 제외하고 오브젝트 유형과 관련된 표의 모든 권한이 포함됩니다.

임의 메시지 컨텍스트 옵션을 수정하려면 호출을 발행할 수 있는 해당 권한이 있어야 합니다. 예를 들어, MQOO_SET_IDENTITY_CONTEXT 또는 MQPMO_SET_IDENTITY_CONTEXT를 사용하려면 +setid 권한이 있어야 합니다.

표 10. MQCONN 호출에 필요한 보안 권한			
다음에 대한 권한 필요	큐 오브젝트(115 페이지의 『1』)	프로세스 오브젝트	큐 관리자 오브젝트
MQCONN	적용할 수 없음	적용할 수 없음	MQZAO_CONNECT

표 11. MQOPEN 호출에 대해 필요한 보안 권한			
다음에 대한 권한 필요	큐 오브젝트(115 페이지의 『1』)	프로세스 오브젝트	큐 관리자 오브젝트
MQOO_INQUIRE	MQZAO_INQUIRE	MQZAO_INQUIRE	MQZAO_INQUIRE
MQOO_BROWSE	MQZAO_BROWSE	적용할 수 없음	검사 안함
MQOO_INPUT_*	MQZAO_INPUT	적용할 수 없음	검사 안함
MQOO_SAVE_ALL_CONTEXT (115 페이지의 『2』)	MQZAO_INPUT	적용할 수 없음	적용할 수 없음
MQOO_OUTPUT(정상 큐) (115 페이지의 『3』)	MQZAO_OUTPUT	적용할 수 없음	적용할 수 없음
MQOO_PASS_IDENTITY_CONTEXT (115 페이지의 『4』)	MQZAO_PASS_IDENTITY_CONTEXT	적용할 수 없음	검사 안함
MQOO_PASS_ALL_CONTEXT (115 페이지의 『4』, 115 페이지의 『5』)	MQZAO_PASS_ALL_CONTEXT	적용할 수 없음	검사 안함
MQOO_SET_IDENTITY_CONTEXT (115 페이지의 『4』, 115 페이지의 『5』)	MQZAO_SET_IDENTITY_CONTEXT	적용할 수 없음	MQZAO_SET_IDENTITY_CONTEXT (115 페이지의 『6』)
MQOO_SET_ALL_CONTEXT (115 페이지의 『4』, 115 페이지의 『7』)	MQZAO_SET_ALL_CONTEXT	적용할 수 없음	MQZAO_SET_ALL_CONTEXT (115 페이지의 『6』)
MQOO_OUTPUT(전송 큐) (115 페이지의 『8』)	MQZAO_SET_ALL_CONTEXT	적용할 수 없음	MQZAO_SET_ALL_CONTEXT (115 페이지의 『6』)
MQOO_SET	MQZAO_SET	적용할 수 없음	검사 안함
MQOO_ALTERNATE_USER_AUTHORITY	(115 페이지의 『9』)	(115 페이지의 『9』)	MQZAO_ALTERNATE_USER_AUTHORITY (115 페이지의 『9』, 116 페이지의 『10』)

표 12. MQPUT1 호출에 필요한 보안 권한			
다음에 대한 권한 필요	큐 오브젝트(115 페이지의 『1』)	프로세스 오브젝트	큐 관리자 오브젝트
MQPMO_PASS_IDENTITY_CONTEXT	MQZAO_PASS_IDENTITY_CONTEXT (116 페이지의 『11』)	적용할 수 없음	검사 안함

표 12. MQPUT1 호출에 필요한 보안 권한 (계속)			
다음에 대한 권한 필요	큐 오브젝트(115 페이지의 『1』)	프로세스 오브젝트	큐 관리자 오브젝트
MQPMO_PASS_ALL_CONTEXT	MQZAO_PASS_ALL_CONTEXT (116 페이지의 『11』)	적용할 수 없음	검사 안함
MQPMO_SET_IDENTITY_CONTEXT	MQZAO_SET_IDENTITY_CONTEXT (116 페이지의 『11』)	적용할 수 없음	MQZAO_SET_IDENTITY_CONTEXT (115 페이지의 『6』)
MQPMO_SET_ALL_CONTEXT	MQZAO_SET_ALL_CONTEXT (116 페이지의 『11』)	적용할 수 없음	MQZAO_SET_ALL_CONTEXT (115 페이지의 『6』)
(전송 큐) (115 페이지의 『8』)	MQZAO_SET_ALL_CONTEXT	적용할 수 없음	MQZAO_SET_ALL_CONTEXT (115 페이지의 『6』)
MQPMO_ALTERNATE_USER_AUTHORITY	(116 페이지의 『12』)	적용할 수 없음	MQZAO_ALTERNATE_USER_AUTHORITY (116 페이지의 『10』)

표 13. MQCLOSE 호출에 대해 필요한 보안 권한			
다음에 대한 권한 필요	큐 오브젝트(115 페이지의 『1』)	프로세스 오브젝트	큐 관리자 오브젝트
MQCO_DELETE	MQZAO_DELETE (116 페이지의 『13』)	적용할 수 없음	적용할 수 없음
MQCO_DELETE_PURGE	MQZAO_DELETE (116 페이지의 『13』)	적용할 수 없음	적용할 수 없음

표에 대한 참고:

- 모델 큐를 여는 경우:
 - 열기 액세스 유형의 경우 모델 큐를 열 수 있는 권한 외에 MQZAO_DISPLAY 권한이 모델 큐에 필요합니다.
 - 동적 큐 작성에 MQZAO_CREATE 권한은 필요하지 않습니다.
 - 모델 큐를 여는 데 사용되는 사용자 ID는 모든 큐 특정 권한을 작성된 동적 큐에 대해 자동 부여합니다 (MQZAO_ALL에 해당).
- MQOO_INPUT_*도 지정해야 합니다. 이것은 로컬, 모델 또는 알리어스 큐에도 유효합니다.
- 이 검사는 전송 큐를 제외한 모든 출력의 경우에 대해서도 수행됩니다(115 페이지의 『8』 참고 참조).
- MQOO_OUTPUT도 지정해야 합니다.
- 이 옵션으로 MQOO_PASS_IDENTITY_CONTEXT도 포함해야 합니다.
- 이 권한은 큐 관리자 오브젝트와 특정 큐 모두에 필요합니다.
- 이 옵션으로 MQOO_PASS_IDENTITY_CONTEXT, MQOO_PASS_ALL_CONTEXT, MQOO_SET_IDENTITY_CONTEXT도 포함해야 합니다.
- 이 검사는 MQUS_TRANSMISSION의 Usage 큐 속성을 갖고 있고 출력을 위해 직접 열려 있는 로컬 또는 모델 큐에 대해 수행됩니다. 리모트 큐가 열려 있는 경우(리모트 큐 관리자 이름과 리모트 큐 이름을 지정하거나 리모트 큐의 로컬 정의 이름을 지정하여) 적용되지 않습니다.
- MQOO_INQUIRE(모든 오브젝트 유형에 대해) 또는 MQOO_BROWSE, MQOO_INPUT_*, MQOO_OUTPUT 또는 MQOO_SET(큐에 대해) 중 하나 이상도 지정해야 합니다. 검사는 특정 이름의 오브젝트 권한에 대해 제공되는 대체 사용자 ID 및 MQZAO_ALTERNATE_USER_IDENTIFIER 검사에 대한 현재 애플리케이션 권한을 사용하여 지정된 다른 옵션에 대해 수행됩니다.

10. 이 권한은 모든 *AlternateUserId* 지정을 허용합니다.
11. 큐에 MQUS_TRANSMISSION의 *Usage* 큐 속성이 없는 경우, MQZAO_OUTPUT 검사가 수행됩니다.
12. 검사는 특정 이름의 큐 권한에 대해 제공되는 대체 사용자 ID 및 MQZAO_ALTERNATE_USER_IDENTIFIER 검사에 대한 현재 애플리케이션 권한을 사용하여 지정된 다른 옵션에 대해 수행됩니다.
13. 검사는 다음 두 가지 사항에 모두 해당하는 경우에만 수행됩니다.
 - 영구적 동적 큐가 닫히고 삭제 중인 경우.
 - 사용되고 있는 오브젝트 핸들을 리턴한 MQOPEN 호출에 의해 큐가 작성되지 않은 경우.
 그렇지 않으며 검사가 수행되지 않습니다.

ULW 이스케이프 PCF에서 MQSC 명령의 권한 부여

이 정보는 Escape PCF에 포함된 각 MQSC 명령에 필요한 권한을 요약합니다.

적용할 수 없음은 이 조작이 이 오브젝트 유형에 연관되지 않았음을 나타냅니다.

명령을 제출하는 프로그램이 실행 중인 사용자 ID는 다음 권한도 있어야 합니다.

- 큐 관리자에 대한 MQZAO_CONNECT 권한
- PCF 명령을 수행하기 위한 큐 관리자의 MQZAO_DISPLAY 권한
- 이스케이프 PCF 명령 텍스트 내에서 MQSC 명령을 발행하는 권한

ALTER object

오브젝트	필수 권한
큐	MQZAO_CHANGE
주제	MQZAO_CHANGE
프로세스	MQZAO_CHANGE
큐 관리자	MQZAO_CHANGE
이름 목록	MQZAO_CHANGE
인증 정보	MQZAO_CHANGE
채널	MQZAO_CHANGE
클라이언트 연결 채널	MQZAO_CHANGE
리스너	MQZAO_CHANGE
서비스	MQZAO_CHANGE
통신 정보	MQZAO_CHANGE

CLEAR object

오브젝트	필수 권한
큐	MQZAO_CLEAR
주제	MQZAO_CLEAR
프로세스	적용할 수 없음
큐 관리자	적용할 수 없음
이름 목록	적용할 수 없음
인증 정보	적용할 수 없음
채널	적용할 수 없음

오브젝트	필수 권한
클라이언트 연결 채널	적용할 수 없음
리스너	적용할 수 없음
서비스	적용할 수 없음
통신 정보	적용할 수 없음

DEFINE object NOREPLACE (120 페이지의 『1』)

오브젝트	필수 권한
큐	MQZAO_CREATE (120 페이지의 『2』)
주제	MQZAO_CREATE (120 페이지의 『2』)
프로세스	MQZAO_CREATE (120 페이지의 『2』)
큐 관리자	적용할 수 없음
이름 목록	MQZAO_CREATE (120 페이지의 『2』)
인증 정보	MQZAO_CREATE (120 페이지의 『2』)
채널	MQZAO_CREATE (120 페이지의 『2』)
클라이언트 연결 채널	MQZAO_CREATE (120 페이지의 『2』)
리스너	MQZAO_CREATE (120 페이지의 『2』)
서비스	MQZAO_CREATE (120 페이지의 『2』)
통신 정보	MQZAO_CREATE (120 페이지의 『2』)

DEFINE object REPLACE (120 페이지의 『1』, 120 페이지의 『3』)

오브젝트	필수 권한
큐	MQZAO_CHANGE
주제	MQZAO_CHANGE
프로세스	MQZAO_CHANGE
큐 관리자	적용할 수 없음
이름 목록	MQZAO_CHANGE
인증 정보	MQZAO_CHANGE
채널	MQZAO_CHANGE
클라이언트 연결 채널	MQZAO_CHANGE
리스너	MQZAO_CHANGE
서비스	MQZAO_CHANGE
통신 정보	MQZAO_CHANGE

DELETE object

오브젝트	필수 권한
큐	MQZAO_DELETE
주제	MQZAO_DELETE

오브젝트	필수 권한
프로세스	MQZAO_DELETE
큐 관리자	적용할 수 없음
이름 목록	MQZAO_DELETE
인증 정보	MQZAO_DELETE
채널	MQZAO_DELETE
클라이언트 연결 채널	MQZAO_DELETE
리스너	MQZAO_DELETE
서비스	MQZAO_DELETE
통신 정보	MQZAO_DELETE

DISPLAY object

오브젝트	필수 권한
큐	MQZAO_DISPLAY
주제	MQZAO_DISPLAY
프로세스	MQZAO_DISPLAY
큐 관리자	MQZAO_DISPLAY
이름 목록	MQZAO_DISPLAY
인증 정보	MQZAO_DISPLAY
채널	MQZAO_DISPLAY
클라이언트 연결 채널	MQZAO_DISPLAY
리스너	MQZAO_DISPLAY
서비스	MQZAO_DISPLAY
통신 정보	MQZAO_DISPLAY

START object

오브젝트	필수 권한
큐	적용할 수 없음
주제	적용할 수 없음
프로세스	적용할 수 없음
큐 관리자	적용할 수 없음
이름 목록	적용할 수 없음
인증 정보	적용할 수 없음
채널	MQZAO_CONTROL
클라이언트 연결 채널	적용할 수 없음
리스너	MQZAO_CONTROL
서비스	MQZAO_CONTROL

오브젝트	필수 권한
통신 정보	적용할 수 없음

STOP object

오브젝트	필수 권한
큐	적용할 수 없음
주제	적용할 수 없음
프로세스	적용할 수 없음
큐 관리자	적용할 수 없음
이름 목록	적용할 수 없음
인증 정보	적용할 수 없음
채널	MQZAO_CONTROL
클라이언트 연결 채널	적용할 수 없음
리스너	MQZAO_CONTROL
서비스	MQZAO_CONTROL
통신 정보	적용할 수 없음

채널 명령

명령	오브젝트	필수 권한
PING CHANNEL	채널	MQZAO_CONTROL
RESET CHANNEL	채널	MQZAO_CONTROL_EXTENDED
RESOLVE CHANNEL	채널	MQZAO_CONTROL_EXTENDED

구독 명령

명령	오브젝트	필수 권한
ALTER SUB	주제	MQZAO_CONTROL
DEFINE SUB	주제	MQZAO_CONTROL
DELETE SUB	주제	MQZAO_CONTROL
DISPLAY SUB	주제	MQZAO_DISPLAY

보안 명령

명령	오브젝트	필수 권한
SET AUTHREC	큐 관리자	MQZAO_CHANGE
DELETE AUTHREC	큐 관리자	MQZAO_CHANGE
DISPLAY AUTHREC	큐 관리자	MQZAO_DISPLAY
DISPLAY AUTHSERV	큐 관리자	MQZAO_DISPLAY
DISPLAY ENTAUTH	큐 관리자	MQZAO_DISPLAY
SET CHLAUTH	큐 관리자	MQZAO_CHANGE

명령	오브젝트	필수 권한
DISPLAY CHLAUTH	큐 관리자	MQZAO_DISPLAY
REFRESH SECURITY	큐 관리자	MQZAO_CHANGE

상태 표시

명령	오브젝트	필수 권한
DISPLAY CHSTATUS	큐 관리자	MQZAO_DISPLAY 채널 유형이 CLUSSDR이면 전송 큐에 +inq 권한(또는 MQZAO_INQUIRE)이 필요합니다.
DISPLAY LSSTATUS	큐 관리자	MQZAO_DISPLAY
DISPLAY PUBSUB	큐 관리자	MQZAO_DISPLAY
DISPLAY SBSTATUS	큐 관리자	MQZAO_DISPLAY
DISPLAY SVSTATUS	큐 관리자	MQZAO_DISPLAY
DISPLAY TPSTATUS	큐 관리자	MQZAO_DISPLAY

클러스터 명령

명령	오브젝트	필수 권한
DISPLAY CLUSQMGR	큐 관리자	MQZAO_DISPLAY
REFRESH CLUSTER	'mqm' 그룹 멤버십 필수	
RESET CLUSTER	'mqm' 그룹 멤버십 필수	
SUSPEND QMGR	'mqm' 그룹 멤버십 필수	
RESUME QMGR	'mqm' 그룹 멤버십 필수	

기타 관리 명령

명령	오브젝트	필수 권한
PING QMGR	큐 관리자	MQZAO_DISPLAY
REFRESH QMGR	큐 관리자	MQZAO_CHANGE
RESET QMGR	큐 관리자	MQZAO_CHANGE
DISPLAY CONN	큐 관리자	MQZAO_DISPLAY
STOP CONN	큐 관리자	MQZAO_CHANGE

참고:

1. DEFINE 명령의 경우, LIKE 오브젝트(지정된 경우)에 대한 MQZAO_DISPLAY 권한도 필요하며, LIKE가 생략된 경우 적절한 SYSTEM.DEFAULT.xxx 오브젝트에 대한 권한이 필요합니다.
2. MQZAO_CREATE 권한은 특정 오브젝트나 오브젝트 유형에 특정되지 않습니다. 작성 권한은 setmqaut 명령에 오브젝트 유형 QMGR을 지정하여 지정된 큐 관리자에 대한 모든 오브젝트에 부여됩니다.
3. 이는 바꿀 오브젝트가 이미 있는 경우에도 적용됩니다. 존재하지 않는 경우, 검사는 DEFINE object NOREPLACE로 수행됩니다.

관련 정보

클러스터링: REFRESH CLUSTER 사용 우수 사례

ULW PCF 명령의 권한 부여

이 절에서는 각 PCF 명령에 필요한 권한을 요약합니다.

검사 안함은 권한 검사가 수행되지 않는 것을 나타내며 적용할 수 없음은 이 조작이 이 오브젝트 유형에 연관되지 않았음을 나타냅니다.

명령을 제출하는 프로그램이 실행 중인 사용자 ID는 다음 권한도 있어야 합니다.

- 큐 관리자에 대한 MQZAO_CONNECT 권한
- PCF 명령을 수행하기 위한 큐 관리자의 MQZAO_DISPLAY 권한

특수 권한 MQZAO_ALL_ADMIN에는 특정 오브젝트 또는 오브젝트 유형에 특정하지 않는 MQZAO_CREATE를 제외한 오브젝트 유형에 관련되는 다음 목록의 모든 권한을 포함합니다.

object 변경

오브젝트	필수 권한
큐	MQZAO_CHANGE
토픽	MQZAO_CHANGE
프로세스	MQZAO_CHANGE
큐 관리자	MQZAO_CHANGE
이름 목록	MQZAO_CHANGE
인증 정보	MQZAO_CHANGE
채널	MQZAO_CHANGE
클라이언트 연결 채널	MQZAO_CHANGE
리스너	MQZAO_CHANGE
서비스	MQZAO_CHANGE
통신 정보	MQZAO_CHANGE

object 지우기

오브젝트	필수 권한
큐	MQZAO_CLEAR
토픽	MQZAO_CLEAR
프로세스	적용할 수 없음
큐 관리자	적용할 수 없음
이름 목록	적용할 수 없음
인증 정보	적용할 수 없음
채널	적용할 수 없음
클라이언트 연결 채널	적용할 수 없음
리스너	적용할 수 없음
서비스	적용할 수 없음
통신 정보	적용할 수 없음

object 복사(대체 제외)(1)

오브젝트	필수 권한
큐	MQZAO_CREATE (2)
토픽	MQZAO_CREATE (2)
프로세스	MQZAO_CREATE (2)
큐 관리자	적용할 수 없음
이름 목록	MQZAO_CREATE (2)
인증 정보	MQZAO_CREATE (2)
채널	MQZAO_CREATE (2)
클라이언트 연결 채널	MQZAO_CREATE (2)
리스너	MQZAO_CREATE (2)
서비스	MQZAO_CREATE (2)
통신 정보	MQZAO_CREATE (126 페이지의 『2』)

Copy object(바꾸기 포함)(1, 4)

오브젝트	필수 권한
큐	MQZAO_CHANGE
토픽	MQZAO_CHANGE
프로세스	MQZAO_CHANGE
큐 관리자	적용할 수 없음
이름 목록	MQZAO_CHANGE
인증 정보	MQZAO_CHANGE
채널	MQZAO_CHANGE
클라이언트 연결 채널	MQZAO_CHANGE
리스너	MQZAO_CHANGE
서비스	MQZAO_CHANGE
통신 정보	MQZAO_CHANGE

object 작성(대체 제외)(3)

오브젝트	필수 권한
큐	MQZAO_CREATE (2)
토픽	MQZAO_CREATE (2)
프로세스	MQZAO_CREATE (2)
큐 관리자	적용할 수 없음
이름 목록	MQZAO_CREATE (2)
인증 정보	MQZAO_CREATE (2)
채널	MQZAO_CREATE (2)

오브젝트	필수 권한
클라이언트 연결 채널	MQZAO_CREATE (2)
리스너	MQZAO_CREATE (2)
서비스	MQZAO_CREATE (2)
통신 정보	MQZAO_CREATE (2)

Create object(바꾸기 포함)(3, 4)

오브젝트	필수 권한
큐	MQZAO_CHANGE
토픽	MQZAO_CHANGE
프로세스	MQZAO_CHANGE
큐 관리자	적용할 수 없음
이름 목록	MQZAO_CHANGE
인증 정보	MQZAO_CHANGE
채널	MQZAO_CHANGE
클라이언트 연결 채널	MQZAO_CHANGE
리스너	MQZAO_CHANGE
서비스	MQZAO_CHANGE
통신 정보	MQZAO_CHANGE

object 삭제

오브젝트	필수 권한
큐	MQZAO_DELETE
토픽	MQZAO_DELETE
프로세스	MQZAO_DELETE
큐 관리자	적용할 수 없음
이름 목록	MQZAO_DELETE
인증 정보	MQZAO_DELETE
채널	MQZAO_DELETE
클라이언트 연결 채널	MQZAO_DELETE
리스너	MQZAO_DELETE
서비스	MQZAO_DELETE
통신 정보	MQZAO_DELETE

object 조회

오브젝트	필수 권한
큐	MQZAO_DISPLAY
토픽	MQZAO_DISPLAY

오브젝트	필수 권한
<u>프로세스</u>	MQZAO_DISPLAY
<u>큐 관리자</u>	MQZAO_DISPLAY
<u>이름 목록</u>	MQZAO_DISPLAY
<u>인증 정보</u>	MQZAO_DISPLAY
<u>채널</u>	MQZAO_DISPLAY
<u>클라이언트 연결 채널</u>	MQZAO_DISPLAY
<u>리스너</u>	MQZAO_DISPLAY
<u>서비스</u>	MQZAO_DISPLAY
<u>통신 정보</u>	MQZAO_DISPLAY

object 이름 조회

오브젝트	필수 권한
큐	검사 안함
주제	검사 안함
프로세스	검사 안함
큐 관리자	검사 안함
이름 목록	검사 안함
인증 정보	검사 안함
채널	검사 안함
클라이언트 연결 채널	검사 안함
리스너	검사 안함
서비스	검사 안함
통신 정보	검사 안함

object 시작

오브젝트	필수 권한
큐	적용할 수 없음
주제	적용할 수 없음
프로세스	적용할 수 없음
큐 관리자	적용할 수 없음
이름 목록	적용할 수 없음
인증 정보	적용할 수 없음
<u>채널</u>	MQZAO_CONTROL
클라이언트 연결 채널	적용할 수 없음
<u>리스너</u>	MQZAO_CONTROL
<u>서비스</u>	MQZAO_CONTROL

오브젝트	필수 권한
통신 정보	적용할 수 없음

object 중지

오브젝트	필수 권한
큐	적용할 수 없음
주제	적용할 수 없음
프로세스	적용할 수 없음
큐 관리자	적용할 수 없음
이름 목록	적용할 수 없음
인증 정보	적용할 수 없음
채널	MQZAO_CONTROL
클라이언트 연결 채널	적용할 수 없음
리스너	MQZAO_CONTROL
서비스	MQZAO_CONTROL
통신 정보	적용할 수 없음

채널 명령

명령	오브젝트	필수 권한
채널 ping	채널	MQZAO_CONTROL
채널 재설정	채널	MQZAO_CONTROL_EXTENDED
채널 분석	채널	MQZAO_CONTROL_EXTENDED

구독 명령

명령	오브젝트	필수 권한
구독 변경	주제	MQZAO_CONTROL
구독 작성	주제	MQZAO_CONTROL
구독 삭제	주제	MQZAO_CONTROL
구독 조회	주제	MQZAO_DISPLAY

보안 명령

명령	오브젝트	필수 권한
권한 레코드 설정	큐 관리자	MQZAO_CHANGE
권한 레코드 삭제	큐 관리자	MQZAO_CHANGE
권한 레코드 조회	큐 관리자	MQZAO_DISPLAY
권한 서비스 조회	큐 관리자	MQZAO_DISPLAY
엔티티 권한 조회	큐 관리자	MQZAO_DISPLAY
채널 인증 레코드 설정	큐 관리자	MQZAO_CHANGE

명령	오브젝트	필수 권한
<u>채널 인증 레코드 조회</u>	큐 관리자	MQZAO_DISPLAY
<u>보안 새로 고치기</u>	큐 관리자	MQZAO_CHANGE

상태 표시

명령	오브젝트	필수 권한
<u>채널 상태 조회</u>	큐 관리자	MQZAO_DISPLAY 채널 유형이 CLUSSDR이면 전송 큐에 +inq 권한(또는 MQZAO_INQUIRE)이 필요합니다.
<u>채널 리스너 상태 조회</u>	큐 관리자	MQZAO_DISPLAY
<u>발행/구독 상태 조회</u>	큐 관리자	MQZAO_DISPLAY
<u>구독 상태 조회</u>	큐 관리자	MQZAO_DISPLAY
<u>서비스 상태 조회</u>	큐 관리자	MQZAO_DISPLAY
<u>토픽 상태 조회</u>	큐 관리자	MQZAO_DISPLAY

클러스터 명령

명령	오브젝트	필수 권한
<u>클러스터 큐 관리자 조회</u>	큐 관리자	MQZAO_DISPLAY
<u>클러스터 새로 고치기</u>	'mqm' 그룹 멤버십 필수	'mqm' 그룹 멤버십 필수
<u>클러스터 재설정</u>	'mqm' 그룹 멤버십 필수	'mqm' 그룹 멤버십 필수
<u>큐 관리자 클러스터 일시중단</u>	'mqm' 그룹 멤버십 필수	'mqm' 그룹 멤버십 필수
<u>큐 관리자 클러스터 재개</u>	'mqm' 그룹 멤버십 필수	'mqm' 그룹 멤버십 필수

기타 관리 명령

명령	오브젝트	필수 권한
<u>큐 관리자 ping</u>	큐 관리자	MQZAO_DISPLAY
<u>큐 관리자 새로 고치기</u>	큐 관리자	MQZAO_CHANGE
<u>큐 관리자 재설정</u>	큐 관리자	MQZAO_CHANGE
<u>큐 통계 재설정</u>	큐	MQZAO_DISPLAY and MQZAO_CHANGE
<u>연결 조회</u>	큐 관리자	MQZAO_DISPLAY
<u>연결 중지</u>	큐 관리자	MQZAO_CHANGE

참고:

- 복사 명령의 경우, From 오브젝트에 대한 MQZAO_DISPLAY 권한도 필요합니다.
- MQZAO_CREATE 권한은 특정 오브젝트나 오브젝트 유형에 특정되지 않습니다. 작성 권한은 setmqaut 명령에 오브젝트 유형 QMGR을 지정하여 지정된 큐 관리자에 대한 모든 오브젝트에 부여됩니다.
- 작성 명령의 경우, 해당 SYSTEM.DEFAULT.* 객체 (object)

4. 이는 바꿀 오브젝트가 이미 있는 경우에도 적용됩니다. 없는 경우, 검사는 복사 또는 작성(바꾸기 없음)에 대해 수행됩니다.

AIX AIX에서 그룹 작성 및 관리

AIX에서 NIS 또는 NIS+를 사용하지 않는 경우 SMITTY를 사용하여 그룹에 대해 작업하십시오.

이 태스크 정보

AIX에서 SMITTY를 사용하여 그룹 작성, 그룹에 사용자 추가, 그룹에 있는 사용자 목록 표시, 그룹에서 사용자 제거를 수행할 수 있습니다.

프로시저

1. SMITTY에서 보안 및 사용자를 선택하고 Enter를 누르십시오.
2. 그룹을 선택하고 Enter를 누르십시오.
3. 그룹을 작성하려면 다음 단계를 완료하십시오.
 - a) 그룹 추가를 선택하고 Enter를 누르십시오.
 - b) 그룹 이름 및 그룹에 추가하려는 모든 사용자 이름을 쉼표로 구분하여 입력하십시오.
 - c) Enter를 눌러 그룹을 작성하십시오.
4. 그룹에 사용자를 추가하려면 다음 단계를 완료하십시오.
 - a) 그룹 특성 변경 / 표시를 선택하고 Enter를 누르십시오.
 - b) 그룹 구성원 목록을 표시하려는 그룹 이름을 입력하십시오.
 - c) 그룹에 추가하려는 사용자 이름을 쉼표로 구분하여 추가하십시오.
 - d) 이름을 그룹에 추가하려면 Enter를 누르십시오.
5. 그룹에 있는 사용자를 표시하려면 다음 단계를 완료하십시오.
 - a) 그룹 특성 변경 / 표시를 선택하고 Enter를 누르십시오.
 - b) 그룹 구성원 목록을 표시하려는 그룹 이름을 입력하십시오.
6. 그룹에서 사용자를 제거하려면 다음 단계를 완료하십시오.
 - a) 그룹 특성 변경 / 표시를 선택하고 Enter를 누르십시오.
 - b) 그룹 구성원 목록을 표시하려는 그룹 이름을 입력하십시오.
 - c) 그룹에서 제거하려는 사용자의 이름을 삭제하십시오.
 - d) 그룹에서 이름을 제거하려면 Enter를 누르십시오.

Linux Linux에서 그룹 작성 및 관리

Linux에서 NIS 또는 NIS+를 사용하지 않는 경우 /etc/group 파일을 사용하여 그룹에 대해 작업하십시오.

이 태스크 정보

Linux에서 그룹 정보는 /etc/group 파일에 보유됩니다. 명령을 사용하여 그룹 작성, 그룹에 사용자 추가, 그룹에 있는 사용자 목록 표시, 그룹에서 사용자 제거를 수행할 수 있습니다.

프로시저

1. 새 그룹을 작성하려면 **groupadd** 명령을 사용하십시오.
다음 명령을 입력하십시오.

```
groupadd -g group-ID group-name
```

여기서 *group-ID*는 그룹의 숫자 ID이고 *group-name*은 그룹의 이름입니다.

- 보충 그룹에 멤버를 추가하려면, **usermod** 명령을 사용하여 사용자가 현재 멤버인 보충 그룹과 사용자가 멤버가 되는 보충 그룹을 나열하십시오.
예를 들어, 사용자가 이미 `groupa` 그룹의 멤버이고 `groupb`의 멤버가 되는 경우 다음 명령을 사용하십시오.

```
usermod -G groupa,groupb user-name
```

여기서 `user-name`은 사용자 이름입니다.

- 그룹의 멤버를 표시하려면 **getent** 명령을 사용하십시오.
다음 명령을 입력하십시오.

```
getent group group-name
```

여기서, `group-name`은 그룹 이름입니다.

- 보충 그룹에서 멤버를 제거하려면 **usermod** 명령을 사용하여 사용자를 멤버로 남겨두려는 보충 그룹을 나열하십시오.
예를 들어, 사용자의 기본 그룹이 `users`이고 사용자가 `mqm`, `groupa` 및 `groupb`의 멤버이기도 한 경우 `mqm` 그룹에서 사용자를 제거하려면 다음 명령을 사용하십시오.

```
usermod -G groupa,groupb user-name
```

여기서 `user-name`은 사용자 이름입니다.

Solaris Solaris에서 그룹 작성 및 관리

Solaris에서 NIS 또는 NIS+를 사용하지 않는 경우 `/etc/group` 파일을 사용하여 그룹에 대해 작업하십시오.

이 태스크 정보

Solaris에서 그룹 정보는 `/etc/group` 파일에 보유됩니다. 명령을 사용하여 그룹 작성, 그룹에 사용자 추가, 그룹에 있는 사용자 목록 표시, 그룹에서 사용자 제거를 수행할 수 있습니다.

프로시저

- 새 그룹을 작성하려면 **groupadd** 명령을 사용하십시오.
다음 명령을 입력하십시오.

```
groupadd -g group-ID group-name
```

여기서 `group-ID`는 그룹의 숫자 ID이고 `group-name`은 그룹의 이름입니다.

- 보충 그룹에 멤버를 추가하려면, **usermod** 명령을 사용하여 사용자가 현재 멤버인 보충 그룹과 사용자가 멤버가 되는 보충 그룹을 나열하십시오.
예를 들어, 사용자가 이미 `groupa` 그룹의 멤버이고 `groupb`의 멤버가 되는 경우 다음 명령을 사용하십시오.

```
usermod -G groupa,groupb user-name
```

여기서 `user-name`은 사용자 이름입니다.

- 그룹의 멤버를 찾으려면 `/etc/group` 파일에서 해당 그룹의 항목을 검사하십시오.
- 보충 그룹에서 멤버를 제거하려면 **usermod** 명령을 사용하여 사용자를 멤버로 남겨두려는 보충 그룹을 나열하십시오.
예를 들어, 사용자의 기본 그룹이 `users`이고 사용자가 `mqm`, `groupa` 및 `groupb`의 멤버이기도 한 경우 `mqm` 그룹에서 사용자를 제거하려면 다음 명령을 사용하십시오.

```
usermod -G groupa,groupb user-name
```

여기서 `user-name`은 사용자 이름입니다.

Windows Windows에서 그룹 작성 및 관리

Windows에서 컴퓨터 관리 기능을 사용하여 워크스테이션 또는 멤버 서버 시스템에서 그룹을 관리합니다.

이 태스크 정보

도메인 제어기에 대해 사용자 및 그룹은 Active Directory를 통해 관리됩니다. Active Directory 사용에 대한 자세한 정보는 해당하는 운영 체제 지시사항을 참조하십시오.

프린시펄의 그룹 멤버십에 대한 변경은 큐 관리자가 재시작되거나 MQSC 명령 **REFRESH SECURITY**(또는 PCF와 동일)를 실행해야 인식됩니다.

Windows 컴퓨터 관리 패널을 사용하여 사용자 및 그룹에 대해 작업하십시오. 현재 로그인한 사용자에 대한 모든 변경사항은 사용자가 다시 로그인할 때까지 적용되지 않을 수 있습니다.

Windows Windows에서 그룹 작성

제어판을 사용하여 그룹을 작성합니다.

프로시저

1. 제어판을 여십시오.
2. **관리 도구**를 두 번 클릭하십시오.
관리 도구 패널이 열립니다.
3. **컴퓨터 관리**를 두 번 클릭하십시오.
컴퓨터 관리 패널이 열립니다.
4. **로컬 사용자 및 그룹**을 펼치십시오.
5. **그룹**을 마우스의 오른쪽 단추 클릭하고 **새 그룹...**을 선택하십시오.
새 그룹 패널이 표시됩니다.
6. 그룹 이름 필드에 적절한 이름을 입력하고 **작성**을 클릭하십시오.
7. **닫기**를 클릭하십시오.

Windows Windows에서 그룹에 사용자 추가

제어판을 사용하여 그룹에 사용자를 추가합니다.

프로시저

1. 제어판을 여십시오.
2. **관리 도구**를 두 번 클릭하십시오.
관리 도구 패널이 열립니다.
3. **컴퓨터 관리**를 두 번 클릭하십시오.
컴퓨터 관리 패널이 열립니다.
4. 컴퓨터 관리 패널에서 **로컬 사용자 및 그룹**을 펼치십시오.
5. **사용자**를 선택하십시오.
6. 그룹에 추가하려는 사용자를 두 번 클릭하십시오.
사용자 특성 패널이 표시됩니다.
7. **멤버** 탭을 선택하십시오.
8. 사용자를 추가할 그룹을 선택하십시오. 필요한 그룹이 표시되지 않는 경우에는 다음을 수행하십시오.
 - a) **추가...**를 클릭하십시오.
그룹 선택 패널이 표시됩니다.
 - b) **위치...**를 클릭하십시오.
위치 패널이 표시됩니다.
 - c) 목록에서 사용자를 추가하려는 그룹 위치를 선택하고 **확인**을 클릭하십시오.

- d) 제공된 필드에 그룹 이름을 입력하십시오.
또는 **고급 ...** 을 클릭하십시오. 그런 다음 현재 선택한 위치에서 사용 가능한 그룹을 나열하려면 **지금 찾기** 를 선택하십시오. 여기에서 사용자를 추가하려는 그룹을 선택하고 **확인** 을 클릭하십시오.
 - e) **확인** 을 클릭하십시오.
추가한 그룹을 표시하는 사용자 특성 패널이 표시됩니다.
 - f) 그룹을 선택하십시오.
9. **확인** 을 클릭하십시오.
컴퓨터 관리 패널이 표시됩니다.

Windows의 그룹에 있는 구성원 표시

제어판을 사용하여 그룹의 구성원을 표시합니다.

프로시저

1. 제어판을 여십시오.
2. **관리 도구** 를 두 번 클릭하십시오.
관리 도구 패널이 열립니다.
3. **컴퓨터 관리** 를 두 번 클릭하십시오.
컴퓨터 관리 패널이 열립니다.
4. 컴퓨터 관리 패널에서 **로컬 사용자 및 그룹** 을 펼치십시오.
5. **그룹** 을 선택하십시오.
6. 그룹을 두 번 클릭하십시오. 그룹 특성 패널이 표시됩니다.
그룹 특성 패널이 표시됩니다.

결과

그룹 구성원이 표시됩니다.

Windows의 그룹에서 사용자 제거

제어판을 사용하여 그룹에서 사용자를 제거합니다.

프로시저

1. 제어판을 여십시오.
2. **관리 도구** 를 두 번 클릭하십시오.
관리 도구 패널이 열립니다.
3. **컴퓨터 관리** 를 두 번 클릭하십시오.
컴퓨터 관리 패널이 열립니다.
4. 컴퓨터 관리 패널에서 **로컬 사용자 및 그룹** 을 펼치십시오.
5. **사용자** 를 선택하십시오.
6. 그룹에 추가하려는 사용자를 두 번 클릭하십시오.
사용자 특성 패널이 표시됩니다.
7. **멤버 탭** 을 선택하십시오.
8. 사용자를 제거하려는 그룹을 선택하고 **제거** 를 클릭하십시오.
9. **확인** 을 클릭하십시오.
컴퓨터 관리 패널이 표시됩니다.

결과

이제 그룹에서 사용자를 제거했습니다.

Windows Windows의 보안에 대한 특별한 고려사항

일부 보안 기능은 Windows의 다른 버전에 대해 다르게 작동합니다.

IBM MQ 보안은 사용자 권한 및 그룹 멤버십에 대한 정보의 운영 체제 API에 대한 호출에 의존합니다. 일부 기능은 Windows 시스템에서 동일하게 작동하지 않습니다. 이 주제 콜렉션에는 Windows 환경에서 IBM MQ를 실행할 때 이러한 차이점이 IBM MQ 보안에 미치는 영향에 대한 설명이 포함되어 있습니다.

Windows IBM MQ Windows 서비스용 로컬 및 도메인 사용자 계정

IBM MQ가 실행 중인 경우 권한 부여된 사용자만 큐 관리자 또는 큐에 액세스할 수 있도록 해야 합니다. 따라서 이러한 액세스를 시도하는 사용자에 대한 정보를 IBM MQ에서 조회하는 데 사용할 수 있는 특수 사용자 계정이 필요합니다.

- 131 페이지의 『Prepare IBM MQ Wizard를 사용하여 특수 사용자 계정 구성』
- 131 페이지의 『IBM MQ에서 Active Directory 사용』
- 132 페이지의 『IBM MQ Windows 서비스에 필요한 사용자 권한』

Prepare IBM MQ Wizard를 사용하여 특수 사용자 계정 구성

Prepare IBM MQ Wizard는 Windows 서비스가 이를 사용해야 하는 프로세스에 의해 공유될 수 있도록 특수 사용자 계정을 작성합니다(IBM MQ 준비 마법사로 IBM MQ 구성 참조).

Windows 서비스는 IBM MQ 설치를 위한 클라이언트 프로세스 사이에 공유됩니다. 한 가지 서비스가 각 설치를 위해 작성됩니다. 각 서비스의 이름은 `MQ_InstallationName` 이고, 표시 이름은 `IBM MQ(InstallationName)`입니다.

각 서비스가 비대화식 및 대화식 로그온 세션 사이에 공유되어야 하기 때문에, 특수 사용자 계정에서 각각을 실행해야 합니다. 모든 서비스에 대해 하나의 특수 사용자 계정을 사용하거나 다른 특수 사용자 계정을 작성할 수 있습니다. 각 특수 사용자 계정에는 서비스로서 로그온에 대한 사용자 권한이 있어야 합니다. 자세한 정보는 132 페이지의 표 14의 내용을 참조하십시오. 사용자 ID에 서비스를 실행할 권한이 없으면 서비스가 시작되지 않고 Windows 시스템 이벤트 로그에서 오류가 리턴됩니다. 일반적으로 Prepare IBM MQ Wizard를 실행하고 사용자 ID를 올바르게 설정합니다. 그러나 사용자 ID를 수동으로 구성한 경우 해결해야 할 문제가 있을 수 있습니다.

IBM MQ를 설치하고 Prepare IBM MQ Wizard를 처음 실행할 때, 서비스로 로그온을 포함하여 필수 설정 및 권한으로 `MUSR_MQADMIN`이라는 서비스에 대한 로컬 사용자 계정을 작성합니다.

후속 설치의 경우, Prepare IBM MQ Wizard는 `MUSR_MQADMINx`라는 사용자 계정을 작성합니다. 여기서 `x`는 존재하지 않는 사용자 ID를 표시하는 다음에 사용 가능한 숫자입니다. `MUSR_MQADMINx`에 대한 비밀번호는 계정이 작성될 때 무작위로 생성되고 서비스에 대한 로그온 환경을 구성하기 위해 사용됩니다. 생성된 비밀번호는 만기되지 않습니다.

이 IBM MQ 계정은 특정 기간 이후에 계정 비밀번호가 변경되도록 요청하기 위해 시스템에 설정되는 계정 정책에 의해 영향을 받지 않습니다.

비밀번호는 이 일회성 처리 외부에는 알려지지 않고 레지스트리의 보안 파트에 Windows 운영 체제에 의해 저장됩니다.

IBM MQ에서 Active Directory 사용

사용자 계정이 Active Directory 디렉토리 서비스를 사용 중인 도메인 제어기에서 정의되는 일부 네트워크 구성에서, IBM MQ가 실행 중인 로컬 사용자 계정에는 기타 도메인 사용자 계정의 그룹 멤버십을 조회하기 위해 필요한 권한이 없을 수 있습니다. IBM MQ를 설치할 때 Prepare IBM MQ Wizard는 네트워크 구성에 대한 질문을 하고 테스트를 실행하는 경우인지 여부를 식별합니다.

IBM MQ가 실행 중인 로컬 사용자 계정에 필수 권한이 없는 경우, Prepare IBM MQ Wizard는 특별 사용자 권한을 가지는 도메인 사용자 계정의 계정 세부사항에 대한 사용자를 프롬프트합니다. Windows 도메인 계정을 작성하고 설정하는 자세한 방법은 [IBM MQ용 Windows 도메인 계정 작성 및 설정](#)을 참조하십시오. 도메인 사용자 계정이 요구하는 사용자 권한에 대해서는 132 페이지의 표 14의 내용을 참조하십시오.

도메인 사용자 계정에 대한 올바른 계정 세부사항을 Prepare IBM MQ Wizard에 입력하면, 마법사가 새 계정에서 실행하기 위한 IBM MQ Windows 서비스를 구성합니다. 계정 세부사항이 레지스트리의 보안 부분에 보유하고 사용자는 읽을 수 없습니다.

서비스가 실행 중일 때, IBM MQ Windows 서비스가 실행되고 서비스가 실행 중인 한 실행으로 남습니다. Windows 서비스가 실행된 후 서버에 로그인하는 IBM MQ 관리자는 IBM MQ Explorer 를 사용하여 서버에서 큐 관리자를 관리할 수 있습니다. 이는 IBM MQ Explorer를 기존Windows 서비스 프로세스에 연결합니다. 이러한 두 개의 조치가 작동하려면 다른 레벨의 권한이 필요합니다.

- 시작 프로세스에는 실행 권한이 필요합니다.
- IBM MQ 관리자에는 액세스 권한이 필요합니다.

IBM MQ Windows 서비스에 필요한 사용자 권한

다음 표에는 IBM MQ 설치에 대한 Windows 서비스가 실행되는 로컬 및 도메인 사용자 계정에 필요한 사용자 권한이 나열되어 있습니다.

표 14. IBM MQ Windows 서비스에 필요한 사용자 권한	
권한	설명
배치 작업으로 로그인	이 사용자 계정에서 실행하기 위한 IBM MQ Windows 서비스를 사용합니다.
서비스로 로그인	사용자가 구성된 계정을 사용하여 로그인하기 위해 IBM MQ Windows 서비스를 설정할 수 있게 합니다.
시스템 종료	IBM MQ Windows 서비스가 서비스의 복구가 실패할 때 수행하도록 하기 구성되면 서버를 다시 시작할 수 있게 허용합니다.
쿼터 늘리기	운영 체제 CreateProcessAsUser 호출에 필요합니다.
운영 체제의 일부로 수행	운영 체제 LogonUser 호출에 필요합니다.
통과 검사 우회	운영 체제 LogonUser 호출에 필요합니다.
프로세스 레벨 토큰 교체	운영 체제 LogonUser 호출에 필요합니다.

참고: ASP 및 IIS 애플리케이션을 실행하는 환경에서는 디버그 프로그램 관리가 필요할 수 있습니다.

사용자의 도메인 사용자 계정은 이러한 Windows 사용자 권한을 로컬 보안 정책 애플리케이션에 나열된 대로 유효한 사용자 권한으로 설정되게 해야 합니다. 그렇지 않으면, 서버에서 로컬 보안 정책 애플리케이션을 로컬로 사용하거나 도메인 보안 애플리케이션 도메인을 사용하여 이를 설정하십시오.

Windows Windows 서버 보안 권한

IBM MQ 설치하는 로컬 사용자 또는 도메인 사용자가 설치를 수행하는지 여부에 따라 Windows 서버에서 다르게 작동합니다.

로컬 사용자가 IBM MQ를 설치하는 경우, Prepare IBM MQ Wizard가 IBM MQ Windows 서비스에 대해 작성된 로컬 사용자가 설치 사용자의 그룹 멤버십 정보를 검색할 수 있음을 감지합니다. Prepare IBM MQ Wizard는 Windows 2000 이상에서 실행 중인 도메인 제어기에 정의된 다른 사용자 계정이 있는지를 판별하기 위해 네트워크 구성에 대한 질문을 합니다. 그런 경우, IBM MQ Windows 서비스는 특정 설정 및 권한의 도메인 사용자 계정으로 실행되어야 합니다. Prepare IBM MQ Wizard 는 준비 IBM MQ 마법사를 사용하여 IBM MQ 구성에 설명된 대로 이 사용자의 계정 세부사항에 대해 사용자에게 프롬프트합니다.

도메인 사용자가 IBM MQ를 설치하는 경우, Prepare IBM MQ Wizard가 IBM MQ Windows 서비스에 대해 작성된 로컬 사용자가 설치 사용자의 그룹 멤버십 정보를 검색할 수 없음을 감지합니다. 이런 경우, Prepare IBM MQ Wizard는 항상 사용하려는 IBM MQ Windows 서비스에 대한 도메인 사용자 계정의 계정 세부사항을 사용자에게 프롬프트합니다.

IBM MQ Windows 서비스가 도메인 사용자 계정을 사용해야 하는 경우, IBM MQ는 Prepare IBM MQ Wizard를 사용하여 구성될 때까지 제대로 작동할 수 없습니다. Prepare IBM MQ Wizard 준비 마법사는 Windows 서비스가 적합한 계정으로 구성될 때까지 사용자가 다른 태스크로 계속하는 것을 허용하지 않습니다.

자세한 정보는 IBM MQ의 도메인 계정 작성 및 설정을 참조하십시오.

Windows IBM MQ 서비스와 연관된 사용자 이름 변경

새 계정을 작성하고 Prepare IBM MQ Wizard를 사용하여 세부사항을 입력하여 IBM MQ 서비스와 연관된 사용자 이름을 변경할 수 있습니다.

이 태스크 정보

IBM MQ를 설치하고 Prepare IBM MQ Wizard를 처음 실행할 때, MUSR_MQADMIN이라는 서비스에 대한 로컬 사용자 계정을 작성합니다. 후속 설치의 경우, Prepare IBM MQ Wizard는 MUSR_MQADMINx라는 사용자 계정을 작성합니다. 여기서 x는 존재하지 않는 사용자 ID를 표시하는 다음에 사용 가능한 숫자입니다.

IBM MQ 서비스와 연관된 사용자 이름을 MUSR_MQADMIN 또는 MUSR_MQADMINx에서 다른 것으로 변경해야 할 수도 있습니다. 예를 들어, 큐 관리자가 Db2®와 연관된 경우 이를 수행해야 할 수도 있습니다. DB2는 8자를 초과하는 사용자 이름을 승인하지 않습니다.

프로시저

1. 새 사용자 계정을 작성하십시오(예: **NEW_NAME**)
2. Prepare IBM MQ Wizard를 사용하여 새 사용자 계정의 세부사항을 입력하십시오.

관련 태스크

[IBM MQ 준비 마법사로 IBM MQ 구성](#)

Windows IBM MQ Windows 서비스 로컬 사용자 계정의 비밀번호 변경

컴퓨터 관리 패널을 사용하여 IBM MQ Windows 서비스 로컬 사용자 계정의 비밀번호를 변경할 수 있습니다.

이 태스크 정보

IBM MQ Windows 서비스 로컬 사용자 계정의 비밀번호를 변경하려면 다음 단계를 수행하십시오.

프로시저

1. 서비스가 실행 중인 사용자를 식별하십시오.
2. 컴퓨터 관리 패널에서 IBM MQ 서비스를 중지하십시오.
3. 개인의 비밀번호를 변경하는 동일한 방법으로 필수 비밀번호를 변경하십시오.
4. 컴퓨터 관리 패널에서 IBM MQ 서비스에 대한 특성으로 이동하십시오.
5. **로그온** 페이지를 선택하십시오.
6. 지정된 계정 이름이 비밀번호가 수정된 사용자와 일치하는지 확인하십시오.
7. 비밀번호를 **비밀번호** 및 **비밀번호 확인** 필드에 입력하고 **확인**을 클릭하십시오.

Windows 도메인 사용자 계정에서 실행 중인 설치를 위한 IBM MQ Windows 서비스의 비밀번호 변경

Prepare IBM MQ Wizard 를 사용하여 도메인 사용자 계정의 계정 세부사항을 입력하는 대신, 컴퓨터 관리 패널을 사용하여 설치 특정 IBM MQ 서비스에 대한 **로그온** 세부사항을 변경할 수 있습니다.

이 태스크 정보

설치를 위한 IBM MQ Windows 서비스가 도메인 사용자 계정에서 실행 중인 경우, 다음과 같이 계정에 대한 비밀번호를 변경할 수 있습니다.

프로시저

1. 도메인 제어기에서 도메인 계정에 대한 비밀번호를 변경하십시오. 도메인 관리자가 이를 수행하도록 요청해야 할 수도 있습니다.
2. 다음 단계를 완료하여 IBM MQ 서비스에 대한 **로그온** 페이지를 수정하십시오.
 - a) 서비스가 실행 중인 사용자를 식별하십시오.
 - b) 컴퓨터 관리 패널에서 IBM MQ 서비스를 중지하십시오.

- c) 개인의 비밀번호를 변경하는 동일한 방법으로 필수 비밀번호를 변경하십시오.
- d) 컴퓨터 관리 패널에서 IBM MQ 서비스에 대한 특성으로 이동하십시오.
- e) 로그인 페이지를 선택하십시오.
- f) 지정된 계정 이름이 비밀번호가 수정된 사용자와 일치하는지 확인하십시오.
- g) 비밀번호를 비밀번호 및 비밀번호 확인 필드에 입력하고 확인을 클릭하십시오.

IBM MQ Windows 서비스가 실행되는 사용자 계정은 사용자 인터페이스 애플리케이션에서 실행되거나 시스템 시동, 시스템 종료 또는 서비스 복구에서 자동으로 수행되는 MQSC 명령을 실행합니다. 따라서 이 사용자 계정에는 IBM MQ 관리 권한이 있어야 합니다. 기본적으로 서버의 로컬 mqm 그룹에 추가됩니다. 이 멤버십이 제거되면 IBM MQ Windows 서비스는 작동하지 않습니다. 사용자 권한에 대한 자세한 정보는 [132 페이지](#)의 『IBM MQ Windows 서비스에 필요한 사용자 권한』의 내용을 참조하십시오.

보안 문제점이 IBM MQ Windows 서비스가 실행되는 사용자 계정과 함께 발생하면 오류 메시지 및 설명이 시스템 이벤트 로그에 나타납니다.

관련 태스크

[IBM MQ 준비 마법사로 IBM MQ 구성](#)

Windows Windows 서버를 도메인 제어기로 승격시킬 때 고려사항

Windows 서버를 도메인 제어기로 승격시키는 경우, 사용자 및 그룹 권한과 관련된 보안 설정이 적절한지 여부를 고려해야 합니다. 서버와 도메인 제어기 사이에서 Windows 시스템의 상태가 변경되면, IBM MQ에서는 로컬로 정의된 mqm 그룹을 사용하므로 이것이 IBM MQ의 조작에 영향을 줄 수 있음을 고려해야 합니다.

도메인 사용자 및 그룹 권한과 관련된 보안 설정

IBM MQ가 보안 정책 구현을 위해 그룹 멤버십 정보에 의존하므로 IBM MQ 운영을 수행하는 사용자 ID가 다른 사용자의 그룹 멤버십을 판별할 수 있는지 여부가 중요합니다.

Windows 서버를 도메인 제어기로 승격하면, 사용자 및 그룹 권한과 관련된 보안 설정 옵션이 표시됩니다. 이 옵션은 임의 사용자가 Active Directory에서 그룹 멤버십을 검색할 수 있도록 하는지 여부를 제어합니다. 로컬 계정에 도메인 사용자 계정이 그룹 멤버십을 조회할 권한을 부여하도록 도메인 제어기가 설정된 경우, 설치 프로세스 중에 IBM MQ에서 작성되는 기본 사용자 ID는 필요에 따라 다른 사용자에게 그룹 멤버십을 확보할 수 있습니다. 그러나 로컬 계정이 도메인 사용자 계정의 그룹 멤버십을 조회할 권한을 갖지 않도록 도메인 제어기가 설정된 경우, 도메인에 정의된 사용자에게 큐 관리자 또는 큐에 액세스할 권한이 부여되었는지 확인하는 검사가 IBM MQ에서 완료되지 않아 액세스가 실패합니다. 이 방법으로 설정된 도메인 제어기에서 Windows를 사용하는 경우 필수 권한이 있는 특수 도메인 계정이 사용되어야 합니다.

이런 경우 다음을 알아야 합니다.

- Windows 버전의 보안 권한이 작동하는 방식
- 도메인 mqm 그룹 멤버가 그룹 멤버십을 읽는 방법
- 도메인 사용자에서 실행되도록 IBM MQ Windows 서비스를 구성하는 방법

자세한 정보는 [IBM MQ의 사용자 계정 구성](#)을 참조하십시오.

mqm 그룹에 대한 IBM MQ 액세스

Windows 서버가 도메인 제어기로 승격되거나 도메인 제어기에서 강등되는 경우, IBM MQ는 로컬 qm 그룹에 대한 액세스 권한이 상실됩니다.

서버가 도메인 제어기로 승격되는 경우 범위는 로컬에서 도메인 로컬로 변경됩니다. 시스템이 서버로 강등되면 모든 도메인 로컬 그룹이 제거됩니다. 즉, 서버에서 도메인 제어기로 시스템을 변경 및 서버로 다시 변경하는 경우, 로컬 mqm 그룹에 대한 액세스가 유실됨을 의미합니다. 증상은 로컬 mqm 그룹 부족을 표시하는 오류로 예를 들어 다음과 같습니다.

```
>crtmqm qm0
AMQ8066:Local mqm group not found.
```

이 문제를 해결하려면 표준 Windows 관리 도구를 사용하여 로컬 mqm 그룹을 다시 작성하십시오. 모든 그룹 멤버십 정보가 유실되기 때문에 새로 작성한 로컬 mqm 그룹에서 특권이 있는 IBM MQ 사용자를 다시 복원시켜야

합니다. 시스템이 도메인 멤버인 경우, 특권이 있는 도메인 IBM MQ 사용자 ID에 필요한 권한 레벨을 부여하기 위해 도메인 mqm 그룹을 로컬 mqm 그룹에도 추가해야 합니다.

Windows Windows에서 중첩 그룹에 대한 제한사항

중첩 그룹 사용에는 제한이 있습니다. 이는 도메인 기능 레벨에서 부분적으로 초래되고 일부는 IBM MQ 제한에서 초래됩니다.

Active Directory는 도메인 기능 레벨에 따라 도메인 컨텍스트 내에서 다른 그룹 유형을 지원할 수 있습니다. 기본적으로 Windows 2003 도메인은 "Windows 2000 혼합" 기능 레벨에 있습니다. (Windows Server 2008 및 Windows Server 2012는 Windows 2003 도메인 모델을 따릅니다.) 도메인 기능 레벨은 지원되는 도메인 환경에서 사용자 ID를 구성할 때 허용되는 지원 그룹 유형 및 중첩 레벨을 판별합니다. 그룹 범위 및 포함 기준에 대한 자세한 내용은 Active Directory 문서를 참조하십시오.

Active Directory 요구사항뿐만 아니라 추가 제한이 IBM MQ에서 사용되는 ID에도 있습니다. IBM MQ에서 사용되는 네트워크 API는 도메인 기능 레벨에서 지원하는 모든 구성을 지원하지는 않습니다. 이로 인해 IBM MQ는 도메인 로컬 그룹에 있으며 로컬 그룹에 중첩되는 모든 도메인 ID의 그룹 멤버십을 조회할 수 없습니다. 더구나 글로벌 및 유니버설 그룹의 다중 중첩은 지원되지 않습니다. 그렇지만 바로 중첩된 글로벌 또는 유니버설 그룹은 지원됩니다.

Windows 사용자에게 IBM MQ의 원격 사용 권한 부여

IBM MQ에 원격으로 연결될 때 큐 관리자를 작성 및 시작해야 하는 경우, 글로벌 오브젝트 작성 사용자 액세스 권한이 있어야 합니다.

이 태스크 정보

참고: 관리자에게는 기본적으로 글로벌 오브젝트 작성 사용자 액세스 권한이 있습니다. 따라서 관리자인 경우에는 사용자 권한을 변경하지 않고 원격으로 연결될 때 큐 관리자를 작성하고 시작할 수 있습니다.

터미널 서비스는 원격 데스크탑 연결을 사용하여 Windows 시스템에 연결하고 큐 관리자 작성, 시작 또는 삭제에 문제가 발생하는 경우, 이는 글로벌 오브젝트 작성에 대한 사용자 액세스 권한이 없기 때문일 수 있습니다.

글로벌 오브젝트 작성 사용자 액세스는 글로벌 네임스페이스에서 오브젝트를 작성하도록 권한이 부여된 사용자로 제한됩니다. 애플리케이션에서 글로벌 오브젝트를 작성하기 위해서는 글로벌 네임스페이스에서 실행되거나 애플리케이션을 실행하는 사용자에게 글로벌 오브젝트 작성 사용자 액세스 권한이 적용되어야 합니다.

터미널 서비스 또는 원격 데스크탑 연결을 사용하여 원격으로 Windows 시스템에 연결하는 경우, 애플리케이션은 자체 보유한 로컬 네임스페이스에서 실행됩니다. IBM MQ Explorer를 사용하거나 **crtmqm** 또는 **dltmqm** 명령을 사용하여 큐 관리자를 작성하거나 삭제하는 경우 또는 **strmqm** 명령을 사용하여 큐 관리자를 시작하려고 하면 권한 부여에 실패합니다. 그러면 프로브 ID가 XY132002인 IBM MQ FDC가 작성됩니다.

IBM MQ Explorer를 사용하거나 **amqmdain qmgr start** 명령을 사용하면 큐 관리자가 제대로 시작되는데, 이는 이 명령으로 큐 관리자가 직접 시작되는 것이 아니기 때문입니다. 대신, 이 명령은 큐 관리자 시작 요청을 글로벌 네임스페이스에서 실행되는 별도의 프로세스로 송신합니다.

IBM MQ에 대한 다양한 관리 방법이 터미널 서비스 사용 시에 작동하지 않으면 글로벌 오브젝트 작성 사용자 권한을 설정하십시오.

프로시저

1. 관리 도구 패널을 여십시오.

Windows Server 2008 및 Windows Server 2012

제어판 > 시스템 및 유지보수 > 관리 도구를 사용하여 이 패널에 액세스하십시오.

Windows 8.1

관리 도구 > 컴퓨터 관리를 사용하여 이 패널에 액세스하십시오.

2. 로컬 보안 정책을 두 번 클릭하십시오.
3. 로컬 정책을 펼치십시오.
4. 사용자 권한 지정을 클릭하십시오.
5. 새 사용자 또는 그룹을 글로벌 오브젝트 작성 정책에 추가하십시오.

Windows Windows에서 SSPI 채널 엑시트 프로그램

IBM MQ for Windows는 보안 엑시트 프로그램을 제공하며 이는 메시지 및 MQI 채널 모두에서 사용 가능합니다. 엑시트는 소스 및 오브젝트 코드로 제공되며 단방향 및 양방향 인증을 제공합니다.

보안 엑시트는 SSPI(Security Support Provider Interface)를 사용하며 이는 Windows 플랫폼의 통합 보안 기능을 제공합니다.

보안 엑시트는 다음의 식별 및 인증 서비스를 제공합니다.

단방향 인증

이는 Windows NT LAN Manager(NTLM) 인증 지원을 사용합니다. NTLM을 사용하여 서버가 해당 클라이언트를 인증합니다. 클라이언트가 서버를 인증하는 것이나, 임의의 서버가 다른 서버를 인증하는 것은 허용하지 않습니다. NTLM은 서버가 조작되지 않았다고 가정되는 네트워크 환경을 위해 설계되었습니다. NTLM은 IBM WebSphere MQ 7.0에서 지원하는 모든 Windows 플랫폼에서 지원됩니다.

이 서비스는 일반적으로 MQI 채널에서 사용되어 서버 큐 관리자가 IBM MQ MQI client 애플리케이션을 인증하도록 합니다. 클라이언트 애플리케이션은 실행 중인 프로세스에 연관된 사용자 ID로 식별됩니다.

인증을 수행하려면, 채널의 클라이언트 쪽에 있는 보안 엑시트가 NTLM에서 인증 토큰을 얻고 토큰을 보안 메시지로 채널의 다른 쪽에 있는 해당 파트너에게 송신합니다. 파트너 보안 엑시트는 토큰을 NTLM에게 전달하며, NTLM은 해당 토큰이 인증된 것인지 검사합니다. 파트너 보안 엑시트가 토큰 인증을 만족시키지 않으면 MCA가 채널을 닫도록 지시합니다.

양방향 또는 상호 인증

이는 Kerberos 인증 서비스를 사용합니다. Kerberos 프로토콜은 네트워크 환경에 있는 서버가 진짜라고 가정하지 않습니다. 서버가 클라이언트와 다른 서버를 인증할 수 있고, 클라이언트가 서버를 인증할 수 있습니다. Kerberos는 IBM WebSphere MQ 7.0에서 지원하는 모든 Windows 플랫폼에서 지원됩니다.

이 서비스는 메시지와 MQI 채널 둘 다에서 사용될 수 있습니다. 메시지 채널에서는 두 개의 큐 관리자의 상호 인증을 제공합니다. MQI 채널에서 서버 큐 관리자 및 IBM MQ MQI client 애플리케이션이 서로를 인증하도록 합니다. 큐 관리자는 `ibmqSeries/` 문자열이 접두부로 붙은 이름에 의해 식별됩니다. 클라이언트 애플리케이션은 실행 중인 프로세스에 연관된 사용자 ID로 식별됩니다.

상호 인증을 수행하기 위해, 시작 측 보안 엑시트가 Kerberos 보안 서버에서 인증 토큰을 취득하여 토큰을 보안 메시지로 파트너에게 송신합니다. 파트너 보안 엑시트는 토큰을 Kerberos 서버에 전달하며 Kerberos 서버는 토큰이 인증된 것인지 검사합니다. Kerberos 보안 서버는 파트너가 시작 측 보안 엑시트에 보안 메시지로 송신하는 두 번째 토큰을 생성합니다. 그런 다음, 시작 측 보안 엑시트가 Kerberos 서버에게 두 번째 토큰이 인증되었는지 검사하도록 요청합니다. 이 교환 동안에, 보안 엑시트 중 어느 것이든 상대방이 송신한 토큰의 인증에 만족하지 않으면 MCA에게 채널을 닫으라고 지시합니다.

보안 엑시트는 소스와 오브젝트 형식 둘 다로 제공됩니다. 자체 채널 엑시트 프로그램을 쓰기 위한 시작점으로서 소스 코드를 사용하거나, 오브젝트 모듈을 제공된 대로 사용할 수 있습니다. 오브젝트 모듈에는 두 개의 시작점이 있는데, 하나는 NTLM 인증 지원을 사용하는 단방향 인증용이고 다른 하나는 Kerberos 인증 서비스를 사용하는 양방향 인증용입니다.

SSPI 채널 엑시트 프로그램이 작동하는 방법에 대한 자세한 정보 및 구현 방법에 대한 지시사항은 [Windows 시스템에서 SSPI 보안 엑시트 사용을 참조하십시오.](#)

Windows Windows에서 보안 템플릿 파일 적용

템플릿을 적용하면 IBM MQ 파일 및 디렉토리에 적용되는 보안 설정에 영향을 줄 수 있습니다. 매우 안전한 템플릿을 사용하는 경우 IBM MQ 설치 전에 이를 적용하십시오.

Windows는 보안 구성 및 분석 MMC 스냅인으로 하나 이상의 컴퓨터에 균등한 보안 설정을 적용할 수 있도록 하는 텍스트 기반의 보안 템플릿 파일을 지원합니다. 특히, Windows는 특정 보안 레벨을 제공하기 위한 보안 설정 범위를 포함하는 몇 개의 템플릿을 제공합니다. 이런 템플릿에는 Compatible, Secure, Highly Secure가 포함됩니다.

이 템플릿 중 하나를 적용하면 IBM MQ 파일 및 디렉토리에 적용되는 보안 설정에 영향을 줄 수 있습니다. Highly Secure 템플릿을 사용하려는 경우, IBM MQ 설치 전에 시스템을 구성하십시오.

Highly Secure 템플릿을 IBM MQ가 이미 설치된 시스템에 적용하는 경우, IBM MQ 파일 및 디렉토리에 이미 설정한 모든 권한이 제거됩니다. 이 권한이 제거되기 때문에 오류 디렉토리에서 관리자, `mqm`, 적용되는 경우 모든 사용자 그룹 액세스가 유실됩니다.

Windows IBM MQ 에 연결하는 Windows 애플리케이션에 대한 추가 권한 구성

IBM MQ 프로세스가 실행되는 계정은 애플리케이션 프로세스에 대해 SYNCHRONIZE 액세스가 부여되기 전에 추가 인증이 필요할 수도 있습니다.

이 태스크 정보

Windows 애플리케이션이 있는 경우에 문제가 발생할 수 있습니다. 예를 들어, ASP 페이지로 정상적인 보안 레벨 이상으로 실행되도록 구성되는 IBM MQ 연결됩니다.

IBM MQ의 경우 특정 조치를 통합하려면 애플리케이션 프로세스에 대해 SYNCHRONIZE 액세스가 필요합니다. 서버 애플리케이션이 처음으로 큐 관리자 연결을 시도하는 경우, IBM MQ는 IBM MQ 관리자에 대해 SYNCHRONIZE 권한을 부여하기 위해 프로세스를 수정합니다. 그러나 IBM MQ 프로세스가 실행되는 계정은 요청된 액세스가 부여되기 전에 추가 권한이 필요할 수 있습니다.

IBM MQ 프로세스가 실행되는 사용자 ID에 대해 추가 권한을 구성하려면 다음 단계를 완료하십시오.

프로시저

1. 로컬 보안 정책 도구를 시작하고 **보안 설정->로컬 정책->사용자 권한 지정**을 클릭한 후 **디버그 프로그램을** 클릭하십시오.
2. **디버그 프로그램**을 두 번 클릭하고 IBM MQ 사용자 ID를 목록에 추가하십시오.

시스템이 Windows 도메인에 있고 유효한 정책 설정이 여전히 설정되지 않았다면 로컬 정책 설정이 설정되더라도 사용자 ID는 도메인 보안 정책 도구를 사용하여 도메인 레벨에서 동일한 방식으로 권한 부여되어야 합니다.

IBM i IBM i에서 보안 설정

IBM i에서 보안은 IBM MQ 오브젝트 권한 관리자(OAM) 및 IBM i 오브젝트 레벨 보안을 사용하여 구현됩니다.

IBM MQ 오브젝트에 대한 액세스 권한을 판별할 때 수행해야 하는 보안 고려사항.

엔터프라이즈의 사용자에 대한 권한을 설정할 때 다음 사항을 고려해야 합니다.

1. IBM i GRTOBJAUT 및 RVKOBJAUT 명령을 사용하여 IBM MQ for IBM i 명령에 대한 권한을 부여하고 취소합니다.

QMOM 라이브러리에서 특정 비명령(*cmd) 오브젝트가 *USE에 대한 *PUBLIC 권한을 갖도록 설정됩니다. 권한을 제공하기 위해 권한 목록을 사용하거나 이 오브젝트의 권한을 변경하지 마십시오. 잘못된 모든 권한으로 인해 IBM MQ 기능이 손상될 수 있습니다.

2. IBM MQ for IBM i 설치 중에 다음 특수 사용자 프로파일이 작성됩니다.

QMOM

내부 제품 전용 기능으로 주로 사용됩니다. 그렇지만 MQCNO_FASTPATH_BINDINGS를 사용하여 신뢰 애플리케이션 실행에 사용할 수 있습니다. MQCONNX 호출을 사용하여 큐 관리자에 연결을 참조하십시오.

QMOMADM

IBM MQ 관리자의 그룹 프로파일로 사용됩니다. 그룹 프로파일은 CL 명령 및 IBM MQ 자원에 대한 액세스를 제공합니다.

IBM MQ 명령을 호출하는 프로그램을 제출하기 위해 SBMJOB을 사용하는 경우, USER는 QMOMADM에 명시적으로 설정되면 안됩니다. 대신, USER를 QMOM 또는 그룹으로 QMOMADM을 지정한 다른 사용자 프로파일에 설정합니다.

3. 채널 명령을 리모트 큐 관리자에게 보내려는 경우 사용자 프로파일이 대상 시스템의 QMOMADM 그룹 멤버인지 확인하십시오. PCF 및 MQSC 채널 명령 목록에 대해서는 IBM MQ for IBM i CL 명령을 참조하십시오.
4. 그룹 권한 부여가 OAM에서 처리될 때 사용자와 연관된 그룹 세트가 캐시됩니다.

큐 관리자를 다시 시작하거나 RFRMQMAUT를 실행하여 보안을 새로 고칠 때까지, 그룹 세트가 캐시된 후 사용자의 그룹 멤버십에 작성된 변경사항이 인식되지 않습니다.

5. 특히 예민한 명령과 작업할 권한이 있는 사용자의 수를 제한합니다. 이 명령에는 다음이 포함됩니다.

- 메시지 큐 관리자 작성(CRTMQM)
 - 메시지 큐 관리자 삭제(DLTMQM)
 - 메시지 큐 관리자 시작(STRMQM)
 - 메시지 큐 관리자 종료(ENDMQM)
 - 명령 서버 시작(STRMQMCSVR)
 - 명령 서버 종료(ENDMQMCSVR)
6. 채널 정의는 보안 엑시트 프로그램 스펙을 포함합니다. 채널 작성 및 수정에는 특별한 고려사항이 필요합니다. 보안 엑시트의 세부사항은 94 페이지의 『보안 엑시트 개요』에서 제공됩니다.
7. 채널 엑시트 및 트리거 모니터 프로그램은 대체 가능합니다. 이러한 대체에 대한 보안은 프로그래머의 책임입니다.

IBM i IBM i에서 오브젝트 권한 관리자

오브젝트 권한 관리자(OAM)는 큐 및 프로세스 정의를 포함하여 IBM MQ 오브젝트를 조작하기 위해 사용자의 권한을 관리합니다. 또한, 특정 사용자 그룹에 대해 오브젝트에 대한 액세스 권한을 부여하거나 취소하는 명령 인터페이스도 제공합니다. 자원 액세스 허용 여부는 OAM이 결정하며 큐 관리자는 해당 결정을 따릅니다. OAM이 결정하지 못하는 경우 큐 관리자가 해당 자원 액세스를 차단합니다.

OAM을 통해 다음을 제어할 수 있습니다.

- MQI를 통해 IBM MQ 오브젝트 액세스. 애플리케이션 프로그램이 오브젝트에 대해 액세스를 시도하면 OAM은 요청을 수행하는 사용자 프로파일에 요청된 조작에 대한 권한이 있는지를 검사합니다.
특히, 권한 없는 액세스로부터 큐의 메시지와 큐를 보호할 수 있습니다.
- PCF 및 MQSC 명령 사용 권한.

다른 사용자 그룹은 동일한 오브젝트에 대해 다른 액세스 권한을 가집니다. 예를 들어, 특정 큐에 대해 한 그룹은 넣기 및 가져오기 조작을 모두 수행할 수 있지만 다른 그룹은 큐를 찾아보는 것만 허용될 수도 있습니다(browse 옵션이 포함된 MQGET). 이와 유사하게 일부 그룹은 큐에 대해 가져오기 및 넣기 권한이 있지만 큐를 대체하거나 삭제할 수는 없습니다.

IBM MQ for IBM i 오브젝트에 대한 IBM MQ for IBM i 명령 및 수행 조작

IBM i IBM i의 IBM MQ 권한

IBM MQ 오브젝트에 액세스하려면 명령을 발행하고 참조되는 오브젝트에 액세스할 권한이 필요합니다. 관리자도 모든 IBM MQ 자원에 액세스 권한이 있습니다.

IBM MQ 오브젝트 액세스는 다음에 대한 권한으로 제어됩니다.

1. IBM MQ 명령 발행
2. 명령에서 참조되는 IBM MQ 오브젝트 액세스

모든 IBM MQ for IBM i CL 명령은 QMQM 소유자와 같이 제공되고 관리 프로파일(QMQMQADM)에는 *PUBLIC 액세스가 *EXCLUDE로 설정된 *USE 권한이 있습니다.

참고: QSRDUPER 프로그램은 IBM i의 IBM MQ 라이선스가 있는 프로그램 설치 프로그램에서 QSYS의 명령(*CMD) 오브젝트를 복제하는 데 사용됩니다. IBM i V5R4 이상에서 QSRDUPER 프로그램은 기본 동작이 원래 명령 중복이 아니라 프록시 명령 작성이 되도록 변경되었습니다. 프록시 명령은 명령 실행은 다른 명령으로 경로 지정하고 PRX 속성을 포함합니다. 복사 중인 명령과 동일한 이름의 프록시 명령이 라이브러리 QSYS에 있는 경우, 프록시 명령에 대한 개인용 권한은 제품 라이브러리의 명령에 부여되지 않습니다. QSYS의 프록시 명령 프롬프트 또는 실행 시도는 제품 라이브러리에서 대상 명령 권한을 검사합니다. 따라서 권한에서 *CMD로의 모든 변경은 제품 라이브러리(QMQM)에서 수행해야 하며 QSYS의 권한은 수정할 필요가 없습니다. 예를 들면, 다음과 같습니다.

```
GRTOBJAUT OBJ(QMQM/DSPMQM) OBJTYPE(*CMD) USER(MQUSER) AUT(*USE)
```

제품 CL 명령 일부의 권한 구조 변경을 수행하는 IBM MQ 오브젝트에 대한 필수 OAM 권한이 있는 경우 이 변경을 통해 해당 명령을 공개적으로 사용할 수 있게 됩니다.

IBM i의 IBM MQ 관리자가 되려면 QMQMADM 그룹의 구성원이어야 합니다. 이 그룹에는 UNIX, Linux, Windows 시스템의 mqm 그룹 특성과 유사한 특성이 있습니다. 특히, QMQMADM 그룹은 IBM MQ for IBM i 설치 시에 작성되고 QMQMADM 그룹 구성원은 시스템의 모든 IBM MQ 자원에 대한 액세스 권한을 가집니다. *ALLOBJ 권한이 있는 사용자인 경우 모든 IBM MQ 자원에도 액세스할 수 있습니다.

관리자는 CL 명령을 사용하여 IBM MQ를 관리할 수 있습니다. 이들 명령 중 하나는 다른 사용자에게 권한을 부여하는 데 사용되는 GRTMQMAUT입니다. 다른 명령인 STRMQMMQSC로 관리자가 로컬 큐 관리자에게 MQSC 명령을 발행할 수 있습니다.

관련 개념

75 페이지의 『IBM i에서 IBM MQ를 관리하는 권한』

IBM i IBM i의 IBM MQ 오브젝트에 대한 액세스 권한

IBM MQ CL 명령 실행에 필요한 액세스 권한입니다.

IBM MQ for IBM i는 제품의 CL 명령을 두 그룹으로 범주화합니다.

그룹 1

해당 명령을 처리하려면 사용자는 QMQMADM 사용자 그룹에 있거나 *ALLOBJ 권한이 있어야 합니다. 이 권한 중 하나가 있는 사용자는 추가 권한 없이도 모든 범주의 모든 명령을 처리할 수 있습니다.

참고: 이 권한은 모든 OAM 권한을 대체합니다.

이 명령은 다음과 같이 그룹화할 수 있습니다.

- 명령 서버 명령
 - ENDMQMCSVR, IBM MQ 명령 서버 종료
 - STRMQMCSVR, IBM MQ 명령 서버 시작
- 데드-레터 큐 핸들러 명령
 - STRMQMDLQ, IBM MQ 데드-레터 큐 핸들러 시작
- 리스너 명령
 - ENDMQMLSR, IBM MQ 리스너 종료
 - STRMQMLSR, 비오브젝트 리스너 시작
- 매체 복원 명령
 - RCDMQMIMG, 레코드 IBM MQ 오브젝트 이미지
 - RCRMQMOBJ, IBM MQ 오브젝트 재작성
 - WRKMQMTRN, IBM MQ Q 트랜잭션에 대한 작업
- 큐 관리자 명령
 - CRTMQM, 메시지 큐 관리자 작성
 - DLTMQM, 메시지 큐 관리자 삭제
 - ENDMQM, 메시지 큐 관리자 종료
 - STRMQM, 메시지 큐 관리자 시작
- 보안 명령
 - GRTMQMAUT, IBM MQ 오브젝트 권한 부여
 - RVKMQMAUT, IBM MQ 오브젝트 권한 취소
- 추적 명령
 - TRCMQM, IBM MQ 작업 추적
- 트랜잭션 명령
 - RSVMQMTRN, IBM MQ 트랜잭션 해결

- 트리거 모니터 명령
 - STRMQMTRM, 트리거 모니터 시작
- IBM MQSC 명령
 - RUNMQSC, IBM MQSC 명령 실행
 - STRMQMMQSC, IBM MQSC 명령 시작

그룹 2

2 레벨의 권한이 필요한 나머지 명령:

1. 명령 실행을 위한 IBM i 권한. IBM MQ 관리자는 **GRTOBJAUT** 명령으로 사용자 또는 사용자 그룹에 대한 *PUBLIC(*EXCLUDE) 제한을 대체하여 이를 설정합니다.

예를 들면, 다음과 같습니다.

```
GRTOBJAUT OBJ(QMQM/DSPMQMQ) OBJTYPE(*CMD) USER(MQUSER) AUT(*USE)
```

2. IBM MQ authority to manipulate the IBM MQ objects associated with the command, or commands, given the correct IBM i authority in Step 1.

이 권한은 **GRMQMAUT** 명령을 사용하여 IBM MQ 관리자가 설정한 필수 조치에 대해 적절한 OAM 권한이 있는 사용자에게 의해 제어됩니다.

예를 들면, 다음과 같습니다.

```
GRMQMAUT *connect authority to the queue manager + *admchg authority to the queue
```

명령은 다음과 같이 그룹화할 수 있습니다.

- 채널 명령
 - CHGMQMCHL, IBM MQ 채널 변경
 - 큐 관리자에 대해서는 *connect 권한이 필요하고 채널에 대해서는 *admchg 권한이 필요합니다.
 - CPYMQMCHL, IBM MQ 채널 복사
 - 큐 관리자에 대해서는 *connect 및 *admcrtr 권한이 필요하고 복사되는 기본 채널 유형에 대해서는 *admdsp 권한이 필요하며 채널 오브젝트 클래스에 대해서는 *admcrtr 권한이 필요합니다.
 - 예를 들어, 송신자 채널을 복사하려면 SYSTEM.DEF.SENDER 채널에 대해 *admdsp 권한이 필요합니다.
 - CRTMQMCHL, IBM MQ 채널 작성
 - 큐 관리자에 대해서는 *connect 및 *admcrtr 권한이 필요하고 작성되는 기본 채널 유형에 대해서는 *admdsp 권한이 필요하고 채널 오브젝트 클래스에 대해서는 *admcrtr 권한이 필요합니다.
 - 예를 들어, 송신자 채널을 작성하려면 SYSTEM.DEF.SENDER 채널에 대해 *admdsp 권한이 필요합니다.
 - DLTMQMCHL, IBM MQ 채널 삭제
 - 큐 관리자에 대해서는 *connect 권한이 필요하고 채널에 대해서는 *admdltr 권한이 필요합니다.
 - RSVMQMCHL, IBM MQ 채널 분석
 - 큐 관리자에 대해서는 *connect 권한이 필요하고 채널에 대해서는 *ctrlx 권한이 필요합니다.
- 명령 표시
 - DSP 명령을 처리하려면 사용자에게 나열된 모든 특정 옵션과 같이 큐 관리자를 위한 *connect 및 *admdsp 권한을 부여해야 합니다.
 - DSPMQM, 메시지 큐 관리자 표시
 - DSPMQMAUT, IBM MQ 오브젝트 권한 표시

- DSPMQMAUTI, IBM MQ 인증 정보 표시 - 인증 정보 오브젝트에 대해 *admdsp
- DSPMQMCHL, IBM MQ 채널 표시 - 채널에 대해 *admdsp
- DSPMQMCSVR, IBM MQ 명령 서버 표시
- DSPMQMNL, IBM MQ 이름 목록 표시 - 이름 목록에 대해 *admdsp
- DSPMQMOBJN, IBM MQ 오브젝트 이름 표시
- DSPMQMPRC, IBM MQ 프로세스 표시 - 프로세스에 대해 *admdsp
- DSPMQMQ, IBM MQ 큐 표시 - 큐에 대해 *admdsp
- DSPMQMTOP, IBM MQ 토픽 표시 - 토픽에 대해 *admdsp
- 명령에 대해 작업
 - WRK 명령을 처리하고 옵션 패널을 표시하려면 사용자에게 나열된 모든 특정 옵션과 같이 큐 관리자를 위한 *connect 및 *admdsp 권한을 부여해야 합니다.
 - WRKMQM, 메시지 큐 관리자에 대해 작업
 - WRKMQMAUT, IBM MQ 오브젝트 권한에 대해 작업
 - WRKMQMAUTD, IBM MQ 오브젝트 권한 데이터에 대해 작업
 - WRKMQMAUTI, IBM MQ 인증 정보에 대해 작업
 - IBM MQ 인증 정보 변경 명령의 경우 *admchg
 - *admcrf for the Create and Copy IBM MQ Authentication Information Object command.
 - *admdl for the Delete IBM MQ Authentication Information Object command.
 - IBM MQ 인증 정보 오브젝트 표시 명령의 경우 *admdsp
 - WRKMQMCHL, IBM MQ 채널에 대해 작업

여기에는 다음 권한이 필요합니다.

 - IBM MQ 채널 변경 명령의 경우 *admchg 입니다.
 - IBM MQ 채널 지우기 명령의 경우 *admclr
 - *admcrf for the Create and Copy IBM MQ Channel command.
 - *admdl for the Delete IBM MQ Channel command.
 - *admdsp for the Display IBM MQ Channel command.
 - 시작 IBM MQ 채널 명령의 경우 *ctrlr 입니다.
 - IBM MQ 채널 종료 명령의 경우 *ctrl
 - ping IBM MQ 채널 명령의 경우 *ctrlr 입니다.
 - IBM MQ 채널 재설정 명령의 경우 *ctrlx
 - *ctrlx for the Resolve IBM MQ Channel command.
 - WRKMQMCHST, IBM MQ 채널 상태에 대해 작업

이 명령에는 채널에 대해 *admdsp 권한이 필요합니다.
 - WRKMQMCL, IBM MQ 클러스터에 대해 작업
 - WRKMQMCLQ, IBM MQ 클러스터 큐에 대해 작업
 - WRKMQMCLQM, IBM MQ 클러스터 큐 관리자에 대해 작업
 - WRKMQMLSR, IBM MQ 리스너에 대해 작업
 - WRKMQMMSG, IBM MQ 메시지에 대해 작업

이 명령에는 큐에 대해 *browse 권한이 필요합니다.
 - WRKMQMNL, IBM MQ 이름 목록에 대해 작업

여기에는 다음 권한이 필요합니다.

- IBM MQ Namelist 변경 명령의 경우 *admchg 입니다.
- *admcrt for the Create and Copy IBM MQ Namelist command.
- IBM MQ 이름 목록 삭제 명령의 경우 *admdlt 입니다.
- IBM MQ 이름 목록 표시 명령의 경우 *admdsp
- WRKMQMPRC, IBM MQ 프로세스에 대해 작업
여기에는 다음 권한이 필요합니다.
 - IBM MQ Process Change에 대한 *admchg .
 - *admcrt for the Create and Copy IBM MQ Process command.
 - IBM MQ Process 삭제 명령의 경우 *admdlt 입니다.
 - IBM MQ Process 명령에 대한 *admdsp .
- WRKMQMQ, IBM MQ 큐에 대해 작업
여기에는 다음 권한이 필요합니다.
 - IBM MQ 큐 변경 명령의 경우 *admchg 입니다.
 - *admcrlr for the Clear IBM MQ Queue command.
 - *admcrt for the Create and Copy IBM MQ Queue command.
 - IBM MQ 큐 삭제 명령의 경우 *admdlt 입니다.
 - IBM MQ 큐 표시 명령의 경우 *admdsp
- WRKMQMQSTS, IBM MQ 큐 상태에 대해 작업
- WRKMQMTOP, IBM MQ 토픽에 대해 작업
여기에는 다음 권한이 필요합니다.
 - IBM MQ 주제 변경 명령의 경우 *admchg
 - *admcrt for the Create and Copy IBM MQ Topic command.
 - *admdlt for the Delete IBM MQ Topic command.
 - IBM MQ 주제 표시 명령의 경우 *admdsp
- WRKMQMSUB, IBM MQ 구독에 대해 작업
- 기타 채널 명령
채널 명령을 처리하려면 사용자에게 나열된 특정 권한을 부여해야 합니다.
 - ENDMQMCHL, IBM MQ 채널 종료
여기에는 큐 관리자에 대해 *connect 권한 및 채널에 연관된 전송 큐에 대해 *allmqi 권한이 필요합니다.
 - ENDMQMLSR, IBM MQ 리스너 종료
여기에는 큐 관리자에 대해 *connect 권한 및 이름 지정된 리스너 오브젝트에 대해 *ctrl 권한이 필요합니다.
 - PNGMQMCHL, IBM MQ 채널 ping
여기에는 큐 관리자에 대해 *connect 및 *inq 권한 및 채널 오브젝트에 대해 *ctrl 권한이 필요합니다.
 - RSTMQMCHL, IBM MQ 채널 재설정
여기에는 큐 관리자에 대한 *connect 권한이 필요합니다.
 - STRMQMCHL, IBM MQ 채널 시작
여기에는 큐 관리자에 대해 *connect 권한 및 채널 오브젝트에 대해 *ctrl 권한이 필요합니다.
 - STRMQMCHLI, IBM MQ 채널 시작기 시작

여기에는 큐 관리자에 대해 *connect 및 *inq 권한 및 채널의 전송 큐에 연관된 이니시에이션 큐에 대해 *allmqi 권한이 필요합니다.

- STRMQLSR, IBM MQ 리스너 시작

여기에는 큐 관리자에 대해 *connect 권한 및 이름 지정된 리스너 오브젝트에 대해 *ctrl 권한이 필요합니다.

• 기타 명령:

다음 명령을 처리하려면 사용자에게 나열된 특정 권한을 부여해야 합니다.

- CCTMQM, 메시지 큐 관리자에 연결

여기에는 IBM MQ 오브젝트 권한이 필요하지 않습니다.

- CHGMQM, 메시지 큐 관리자 변경

여기에는 큐 관리자에 대한 *connect 및 *admchg 권한이 필요합니다.

- CHGMQMAUTI, IBM MQ 인증 정보 변경

여기에는 큐 관리자에 대해 *connect 권한 및 인증 정보 오브젝트에 대해 *admchg 및 *admdsp 권한이 필요합니다.

- CHGMQMNL, IBM MQ 이름 목록 변경

여기에는 큐 관리자에 대해 *connect 권한 및 이름 목록에 대해 *admchg 권한이 필요합니다.

- CHGMQMPCR, IBM MQ 프로세스 변경

여기에는 큐 관리자에 대해 *connect 권한 및 프로세스에 대해 *admchg 권한이 필요합니다.

- CHGMQMQ, IBM MQ 큐 변경

여기에는 큐 관리자에 대해 *connect 권한 및 큐에 대해 *admchg 권한이 필요합니다.

- CLRMQMQ, IBM MQ 큐 지우기

여기에는 큐 관리자에 대해 *connect 권한 및 큐에 대해 *admclr 권한이 필요합니다.

- CPYMQMAUTI, IBM MQ 인증 정보 복사

여기에는 큐 관리자에 대해 *connect 권한, 인증 정보 오브젝트에 대해 *admdsp 권한, 인증 정보 오브젝트 클래스에 대한 *admcrtr 권한이 필요합니다.

- CPYMQMNL, IBM MQ 이름 목록 복사

여기에는 큐 관리자에 대한 *connect 및 *admcrtr 권한이 필요합니다.

- CPYMQMPRC, IBM MQ 프로세스 복사

여기에는 큐 관리자에 대한 *connect 및 *admcrtr 권한이 필요합니다.

- CPYMQMQ, IBM MQ 큐 복사

여기에는 큐 관리자에 대한 *connect 및 *admcrtr 권한이 필요합니다.

- CRTMQMAUTI, IBM MQ 인증 정보 작성

여기에는 큐 관리자에 대해 *connect 권한, 인증 정보 오브젝트에 대해 *admdsp 권한, 인증 정보 오브젝트 클래스에 대한 *admcrtr 권한이 필요합니다.

- CRTMQMNL, IBM MQ 이름 목록 작성

여기에는 큐 관리자에 대해 *connect 및 *admcrtr 권한 및 기본 이름 목록에 대해 *admdsp 권한이 필요합니다.

- CRTMQMPRC, IBM MQ 프로세스 작성

여기에는 큐 관리자에 대해 *connect 및 *admcrtr 권한 및 기본 프로세스에 대해 *admdsp 권한이 필요합니다.

- CRTMQMQ, IBM MQ 큐 작성

- 여기에는 큐 관리자에 대해 *connect 및 *admcrt 권한 및 기본 큐에 대해 *admdsp 권한이 필요합니다.
- CVTMQMDTA, IBM MQ 데이터 유형 변환 명령
여기에는 IBM MQ 오브젝트 권한이 필요하지 않습니다.
 - DLTMQMAUTI, IBM MQ 인증 정보 삭제
여기에는 큐 관리자에 대해 *connect 권한 및 인증 정보 오브젝트에 대해 *ctrlx 권한이 필요합니다.
 - DLTMQMNL, IBM MQ 이름 목록 삭제
여기에는 큐 관리자에 대해 *connect 권한 및 이름 목록에 대해 *admdl 권한이 필요합니다.
 - DLTMQMPRC, IBM MQ 프로세스 삭제
여기에는 큐 관리자에 대해 *connect 권한 및 프로세스에 대해 *admdl 권한이 필요합니다.
 - DLTMQMQ, IBM MQ 큐 삭제
여기에는 큐 관리자에 대해 *connect 권한 및 큐에 대해 *admdl 권한이 필요합니다.
 - DSCMQM, 메시지 큐 관리자에서 연결 끊기
여기에는 IBM MQ 오브젝트 권한이 필요하지 않습니다.
 - RFRMQMAUT, 보안 새로 고치기
여기에는 큐 관리자에 대한 *connect 권한이 필요합니다.
 - RFRMQMCL, 클러스터 새로 고치기
여기에는 큐 관리자에 대한 *connect 권한이 필요합니다.
 - RSMMQMCLQM, 클러스터 큐 관리자 재개
여기에는 큐 관리자에 대한 *connect 권한이 필요합니다.
 - RSTMQMCL, 클러스터 재설정
여기에는 큐 관리자에 대한 *connect 권한이 필요합니다.
 - SPDMQMCLQM, 클러스터 큐 관리자 일시중단
여기에는 큐 관리자에 대한 *connect 권한이 필요합니다.

IBM i IBM i에서의 액세스 권한 부여

이 정보를 사용하여 액세스 권한 부여 명령에 대해 이해하십시오.

GRTMQMAUT 및 RVKMQMAUT 명령에서 AUT 키워드로 정의되는 권한은 다음과 같이 분류할 수 있습니다.

- MQI 호출에 연관된 권한
- 권한 부여 관련 관리 명령
- 컨텍스트 권한
- MQI 호출, 명령 또는 둘 다를 위한 일반 권한

다음 표는 MQI 호출, 컨텍스트 호출, MQSC 및 PCF 명령, 일반 조작에 대해 AUT 매개변수를 사용하여 다른 권한을 나열합니다.

표 15. MQI 호출에 대한 권한 부여	
AUT	설명
*ALTUSR	다른 사용자의 권한이 MQOPEN 및 MQPUT1 호출에 사용되도록 허용합니다.
*BROWSE	BROWSE 옵션과 함께 MQGET을 호출하여 큐에서 메시지를 검색합니다.
*CONNECT	MQCONN을 호출하여 지정된 큐 관리자에 애플리케이션을 연결합니다.
*GET	MQGET을 호출하여 큐에서 메시지를 검색합니다.

표 15. MQI 호출에 대한 권한 부여 (계속)	
AUT	설명
*INQ	MQINQ를 호출하여 특정 큐에 대한 조회를 작성합니다.
*PUB	MQPUT 호출을 사용하여 메시지를 발행하기 위해 토픽을 엽니다.
*PUT	MQPUT을 호출하여 특정 큐에 메시지를 넣습니다.
*RESUME	MQSUB 호출을 사용하여 구독을 재개합니다.
*SET	MQSET을 호출하여 MQI의 큐에서 속성을 설정합니다. 다중 옵션에 대해 큐를 여는 경우, 각 큐에 대해 권한이 있어야 합니다.
*SUB	MQSUB 호출을 사용하여 토픽에 대한 구독을 작성, 대체 또는 재개합니다.

표 16. 컨텍스트 호출에 대한 권한 부여	
AUT	설명
*PASSALL	지정한 큐의 모든 컨텍스트를 전달합니다. 모든 컨텍스트 필드가 원래 요청으로부터 복사됩니다.
*PASSID	지정된 큐의 ID 컨텍스트를 전달합니다. ID 컨텍스트는 요청의 컨텍스트와 동일합니다.
*SETALL	지정된 큐에 모든 컨텍스트를 설정합니다. 이것은 특수 시스템 유틸리티에서 사용됩니다.
*SETID	지정된 큐에 ID 컨텍스트를 설정합니다. 이것은 특수 시스템 유틸리티에서 사용됩니다.

표 17. MQSC 및 PCF 호출에 대한 권한 부여	
AUT	설명
*ADMCHG	지정된 오브젝트의 속성을 변경합니다.
*ADMCLR	지정된 오브젝트(PCF Clear 오브젝트 명령에만 해당)를 지웁니다.
*ADMCRT	지정된 유형의 오브젝트를 작성합니다.
*ADMDLT	지정된 오브젝트를 삭제합니다.
*ADMDSP	지정된 오브젝트의 속성을 표시합니다.

표 18. 일반 조작에 대한 권한	
AUT	설명
*ALL	오브젝트에 적용할 수 있는 모든 조작을 사용합니다. all 권한은 오브젝트 유형에 적합한 권한 alladm, allmqi 및 system의 결합과 동등합니다.
*ALLADM	오브젝트에 대해 적용할 수 있는 모든 관리 조작을 수행합니다.
*ALLMQI	오브젝트에 적용할 수 있는 모든 MQI 호출을 사용합니다.
*CTRL	채널, 리스너, 서비스의 시동 및 종료를 제어합니다.
*CTRLX	순서 번호를 재설정하고 인다우트 채널을 해석합니다.

IBM i IBM i에서 액세스 권한 부여 명령 사용

이 정보를 사용하여 액세스 권한 부여 명령에 대해 학습하고 명령 예제를 사용하십시오.

GRTMQMAUT 명령 사용

권한이 필요한 경우, GRTMQMAUT 명령을 사용하여 특정 오브젝트에 액세스하는 사용자 프로파일 또는 사용자 그룹에 권한을 부여할 수 있습니다. 다음 예제는 GRTMQMAUT 명령이 사용되는 방법을 설명합니다.

1.

```
GRTMQMAUT OBJ(RED.LOCAL.QUEUE) OBJTYPE(*LCLQ) USER(GROUPA) +
AUT(*BROWSE *PUT) MQMNAME('saturn.queue.manager')
```

이 예제에서

- RED.LOCAL.QUEUE는 오브젝트 이름입니다.
 - *LCLQ(로컬 큐)는 오브젝트 유형입니다.
 - GROUPA는 권한이 변경되는 시스템의 사용자 프로파일 이름입니다. 이 프로파일은 다른 사용자의 그룹 프로파일로 사용 가능합니다.
 - *BROWSE 및 *PUT는 지정한 큐에 부여 중인 권한입니다.
*BROWSE는 큐에서 메시지를 찾기 위한 권한을 추가합니다(browse 옵션을 포함하여 MQGET 발행).
*PUT은 큐에 메시지를 넣는(MQPUT) 권한을 추가합니다.
 - saturn.queue.manager는 큐 관리자 이름입니다.
2. 다음 명령은 사용자 JACK 및 JILL에게 기본 큐 관리자에 대해 모든 프로세스 정의에 적용 가능한 모든 권한을 부여합니다.

```
GRTMQMAUT OBJ(*ALL) OBJTYPE(*PRC) USER(JACK JILL) AUT(*ALL)
```

3. 다음 명령은 사용자 GEORGE에게 큐 관리자 TRENT에서 큐 ORDERS에 메시지를 넣는 권한을 부여합니다.

```
GRTMQMAUT OBJ(TRENT) OBJTYPE(*MQM) USER(GEORGE) AUT(*CONNECT) MQMNAME (TRENT)
GRTMQMAUT OBJ(ORDERS) OBJTYPE(*Q) USER(GEORGE) AUT(*PUT) MQMNAME (TRENT)
```

RVKMQMAUT 명령 사용

권한이 필요한 경우 RVKMQMAUT 명령을 사용하여 특정 오브젝트에 액세스하는 사용자 프로파일 또는 사용자 그룹에 대해 이전에 부여된 권한을 제거할 수 있습니다. 다음 예제는 RVKMQMAUT 명령이 사용되는 방법을 설명합니다.

1.

```
RVKMQMAUT OBJ(RED.LOCAL.QUEUE) OBJTYPE(*LCLQ) USER(GROUPA) +
AUT(*PUT) MQMNAME('saturn.queue.manager')
```

이전 예제에서 부여된 지정한 큐에 메시지를 넣는 권한이 GROUPA에 대해 제거됩니다.

2.

```
RVKMQMAUT OBJ(PAY*) OBJTYPE(*Q) USER(*PUBLIC) AUT(*GET) +
MQMNAME(PAYROLLQM)
```

큐 관리자 PAYROLLQM이 소유하고 문자 PAY로 시작되는 이름의 모든 큐에서 메시지를 가져오는 권한이 시스템의 모든 사용자에서 제거되지만 해당 사용자 또는 해당 사용자가 속하는 그룹이 별도로 권한 부여된 경우는 제외됩니다.

DSPMQMAUT 명령 사용

MQM 권한 표시(DSPMQMAUT) 명령은 지정한 오브젝트 및 사용자에게 사용자 오브젝트에 대해 가지는 권한 목록을 표시합니다. 다음 예제는 명령이 사용되는 방법에 대해 설명합니다.

```
DSPMQMAUT OBJ(ADMINNL) OBJTYPE(*NMLIST) USER(JOE) OUTPUT(*PRINT) +
MQMNAME(ADMINQM)
```

RFRMQMAUT 명령 사용

MQM 보안 새로 고치기(RFRMQMAUT) 명령을 사용하면 큐 관리자를 중지하고 재시작하지 않고도 운영 체제 레벨에서 수행된 변경사항을 반영하여 OAM 권한 그룹 정보를 즉시 업데이트할 수 있습니다. 다음 예제는 명령이 사용되는 방법에 대해 설명합니다.

```
RFRMQMAUT MQMNAME (ADMINQM)
```

IBM i IBM i에서의 권한 스펙 표

이 정보를 사용하여 특정 API 호출, 해당 호출의 특정 옵션을 큐 오브젝트, 프로세스 오브젝트, 큐 관리자 오브젝트에서 사용하기 위해 필요한 권한을 판별합니다.

148 페이지의 표 19에서 시작되는 권한 스펙 표는 권한이 작동하는 방법 및 적용되는 제한사항을 정확하게 정의합니다. 표는 다음과 같은 상황에 적용됩니다.

- MQI 호출을 발행한 애플리케이션
- 이스케이프 PCF로 MQSC 명령을 발행하는 관리 프로그램
- PCF 명령을 발행하는 관리 프로그램

이 절에서 정보는 다음 데이터를 지정하는 표의 세트로 표시됩니다.

수행할 조치

MQI 옵션, MQSC 명령 또는 PCF 명령

액세스 제어 오브젝트

큐, 프로세스 정의, 큐 관리자, 이름 목록, 채널, 클라이언트 연결 채널, 리스너, 서비스 또는 인증 정보 오브젝트

필수 권한

MQZAO_ 상수로 표현됩니다.

표에서 접두부가 MQZAO_인 상수는 특정 엔티티를 위한 **GRTMQMAUT** 및 **RVKMQMAUT** 명령에 대한 권한 목록의 키워드에 대응합니다. 예를 들어, MQZAO_BROWSE는 키워드 *BROWSE에 대응하고 유사하게 키워드 MQZAO_SET_ALL_CONTEXT는 키워드 *SETALL 등에 대응합니다. 이 상수는 제품에서 제공하는 헤더 파일 cmqzc.h에 정의됩니다.

MQI 권한

실행 중인(또는 권한으로 간주 가능한) 사용자 ID에 관련 권한이 부여된 경우에만 애플리케이션은 특정 MQI 호출 및 옵션을 발행하도록 허용됩니다.

MQCONN, MQOPEN, MQPUT1, MQCLOSE의 네 MQI 호출에 권한 검사가 필요합니다.

MQOPEN 및 MQPUT1의 경우, 권한 검사가 여는 중인 오브젝트의 이름에 대해 수행되며, 이름이 해석된 후에 발생하는 이름에 대해서는 수행되지 않습니다. 예를 들어, 애플리케이션에는 알리어스가 해석되는 기본 큐를 열 수 있는 권한은 부여되지 않고 알리어스 큐를 열 수 있는 권한이 부여됩니다. 큐 관리자 알리어스 정의가 직접 열리는 경우(즉, 해당 이름이 오브젝트 디스크립터의 *ObjectName* 필드에 표시)를 제외하고 큐 관리자 알리어스가 아닌 이름을 해석하는 프로세스 중에 발생하는 첫 번째 정의에서 검사가 수행되는 것이 규칙입니다. 권한은 열리는 특정 오브젝트에 대해 항상 필요하며, 큐 관리자 오브젝트에 대한 권한 부여를 통해 확보되는 추가 큐 독립 권한이 필요한 경우도 있습니다.

148 페이지의 표 19, 148 페이지의 표 20, 149 페이지의 표 21, 149 페이지의 표 22에는 각 호출에 필요한 권한이 요약되어 있습니다.

참고: 이 표는 이름 목록, 채널, 클라이언트 연결 채널, 리스너, 서비스 또는 인증 정보 오브젝트는 언급하지 않습니다. 이는 동일한 권한이 다른 오브젝트에도 적용되는 MQOO_INQUIRE를 제외하고 이러한 오브젝트에 적용되는 권한이 없기 때문입니다.

표 19. MQCONN 호출에 필요한 보안 권한			
다음에 대한 권한 필요	큐 오브젝트(149 페이지의 『1』)	프로세스 오브젝트	큐 관리자 오브젝트
MQCONN 옵션	적용할 수 없음	적용할 수 없음	MQZAO_CONNECT

표 20. MQOPEN 호출에 대해 필요한 보안 권한			
다음에 대한 권한 필요	큐 오브젝트(149 페이지의 『1』)	프로세스 오브젝트	큐 관리자 오브젝트
MQOO_INQUIRE	MQZAO_INQUIRE (149 페이지의 『2』)	MQZAO_INQUIRE (149 페이지의 『2』)	MQZAO_INQUIRE (149 페이지의 『2』)
MQOO_BROWSE	MQZAO_BROWSE	적용할 수 없음	검사 안함
MQOO_INPUT_*	MQZAO_INPUT	적용할 수 없음	검사 안함
MQOO_SAVE_ALL_CONTEXT (149 페이지의 『3』)	MQZAO_INPUT	적용할 수 없음	적용할 수 없음
MQOO_OUTPUT(정상 큐) (149 페이지의 『4』)	MQZAO_OUTPUT	적용할 수 없음	적용할 수 없음
MQOO_PASS_IDENTITY_CONTEXT (149 페이지의 『5』)	MQZAO_PASS_IDENTITY_CONTEXT	적용할 수 없음	검사 안함
MQOO_PASS_ALL_CONTEXT (149 페이지의 『5』, 149 페이지의 『6』)	MQZAO_PASS_ALL_CONTEXT	적용할 수 없음	검사 안함
MQOO_SET_IDENTITY_CONTEXT (149 페이지의 『5』, 149 페이지의 『6』)	MQZAO_SET_IDENTITY_CONTEXT	적용할 수 없음	MQZAO_SET_IDENTITY_CONTEXT (149 페이지의 『7』)
MQOO_SET_ALL_CONTEXT (149 페이지의 『5』, 149 페이지의 『8』)	MQZAO_SET_ALL_CONTEXT	적용할 수 없음	MQZAO_SET_ALL_CONTEXT (149 페이지의 『7』)
MQOO_OUTPUT(전송 큐) (149 페이지의 『9』)	MQZAO_SET_ALL_CONTEXT	적용할 수 없음	MQZAO_SET_ALL_CONTEXT (149 페이지의 『7』)
MQOO_SET	MQZAO_SET	적용할 수 없음	검사 안함
MQOO_ALTERNATE_USER_AUTHORITY	(150 페이지의 『10』)	(150 페이지의 『10』)	MQZAO_ALTERNATE_USER_AUTHORITY (150 페이지의 『10』, 150 페이지의 『11』)

표 21. MQPUT1 호출에 필요한 보안 권한			
다음에 대한 권한 필요	큐 오브젝트(149 페이지의 『1』)	프로세스 오브젝트	큐 관리자 오브젝트
MQPMO_PASS_IDENTITY_CONTEXT	MQZAO_PASS_IDENTITY_CONTEXT (150 페이지의 『12』)	적용할 수 없음	검사 안함
MQPMO_PASS_ALL_CONTEXT	MQZAO_PASS_ALL_CONTEXT (150 페이지의 『12』)	적용할 수 없음	검사 안함
MQPMO_SET_IDENTITY_CONTEXT	MQZAO_SET_IDENTITY_CONTEXT (150 페이지의 『12』)	적용할 수 없음	MQZAO_SET_IDENTITY_CONTEXT (149 페이지의 『7』)
MQPMO_SET_ALL_CONTEXT	MQZAO_SET_ALL_CONTEXT (150 페이지의 『12』)	적용할 수 없음	MQZAO_SET_ALL_CONTEXT (149 페이지의 『7』)
(전송 큐) (149 페이지의 『9』)	MQZAO_SET_ALL_CONTEXT	적용할 수 없음	MQZAO_SET_ALL_CONTEXT (149 페이지의 『7』)
MQPMO_ALTERNATE_USER_AUTHORITY	(150 페이지의 『13』)	적용할 수 없음	MQZAO_ALTERNATE_USER_AUTHORITY (150 페이지의 『11』)

표 22. MQCLOSE 호출에 대해 필요한 보안 권한			
다음에 대한 권한 필요	큐 오브젝트(149 페이지의 『1』)	프로세스 오브젝트	큐 관리자 오브젝트
MQCO_DELETE	MQZAO_DELETE (150 페이지의 『14』)	적용할 수 없음	적용할 수 없음
MQCO_DELETE_PURGE	MQZAO_DELETE (150 페이지의 『14』)	적용할 수 없음	적용할 수 없음

표에 대한 참고:

- 모델 큐를 열고 있는 경우:
 - 열기 액세스 유형의 경우 모델 큐를 열 수 있는 권한 외에 MQZAO_DISPLAY 권한이 모델 큐에 필요합니다.
 - 동적 큐 작성에 MQZAO_CREATE 권한은 필요하지 않습니다.
 - 모델 큐를 여는 데 사용되는 사용자 ID는 모든 큐 특정 권한을 작성된 동적 큐에 대해 자동 부여합니다 (MQZAO_ALL에 해당).
- 큐, 프로세스, 이름 목록 또는 큐 관리자 오브젝트가 열고 있는 오브젝트 유형에 따라 검사됩니다.
- MQOO_INPUT_*도 지정해야 합니다. 이 옵션은 로컬, 모델 또는 알리어스 큐에 대해 유효합니다.
- 이 검사는 149 페이지의 『9』 참고에서 지정하는 경우를 제외하고는 모든 출력의 경우에 대해 수행됩니다.
- MQOO_OUTPUT도 지정해야 합니다.
- 이 옵션으로 MQOO_PASS_IDENTITY_CONTEXT도 포함해야 합니다.
- 이 권한은 큐 관리자 오브젝트와 특정 큐 모두에 필요합니다.
- 이 옵션으로 MQOO_PASS_IDENTITY_CONTEXT, MQOO_PASS_ALL_CONTEXT, MQOO_SET_IDENTITY_CONTEXT도 포함해야 합니다.
- 이 검사는 MQUS_TRANSMISSION의 Usage 큐 속성을 갖고 있고 출력을 위해 직접 열려 있는 로컬 또는 모델 큐에 대해 수행됩니다. 리모트 큐가 열려 있는 경우(리모트 큐 관리자 이름과 리모트 큐 이름을 지정하거나 리모트 큐의 로컬 정의 이름을 지정하여) 적용되지 않습니다.

10. MQOO_INQUIRE(모든 오브젝트 유형에 대해) 또는 (큐에 대해) MQOO_BROWSE, MQOO_INPUT_*, MQOO_OUTPUT 또는 MQOO_SET 중 하나 이상을 지정해야 합니다. 검사는 특정 이름의 오브젝트 권한에 대해 제공되는 대체 사용자 ID 및 MQZAO_ALTERNATE_USER_IDENTIFIER 검사에 대한 현재 애플리케이션 권한을 사용하여 지정된 다른 옵션에 대해 수행됩니다.
11. 이 권한은 모든 *AlternateUserId* 지정을 허용합니다.
12. 큐에 MQUS_TRANSMISSION의 *Usage* 큐 속성이 없는 경우, MQZAO_OUTPUT 검사가 수행됩니다.
13. 검사는 이름 지정된 큐 권한에 대해 제공되는 대체 사용자 ID 및 MQZAO_ALTERNATE_USER_IDENTIFIER 검사에 대한 현재 애플리케이션 권한을 사용하여 지정된 다른 옵션에 대해 수행됩니다.
14. 검사는 다음 두 가지 사항에 모두 해당하는 경우에만 수행됩니다.
 - 영구적 동적 큐가 닫히고 삭제 중인 경우.
 - 사용되고 있는 오브젝트 핸들을 리턴한 MQOPEN에 의해 큐가 작성되지 않은 경우.
 그렇지 않으며 검사가 수행되지 않습니다.

일반 참고:

1. 특수 권한 MQZAO_ALL_MQI에는 오브젝트 유형에 연관되는 다음 모든 권한이 포함됩니다.
 - MQZAO_CONNECT
 - MQZAO_INQUIRE
 - MQZAO_SET
 - MQZAO_BROWSE
 - MQZAO_INPUT
 - MQZAO_OUTPUT
 - MQZAO_PASS_IDENTITY_CONTEXT
 - MQZAO_PASS_ALL_CONTEXT
 - MQZAO_SET_IDENTITY_CONTEXT
 - MQZAO_SET_ALL_CONTEXT
 - MQZAO_ALTERNATE_USER_AUTHORITY
2. MQZAO_DELETE(150 페이지의 『14』 참조 참조) 및 MQZAO_DISPLAY는 관리 권한으로 분류됩니다. 따라서 이는 MQZAO_ALL_MQI에 포함되지 않습니다.
3. 검사 안함은 권한 검사가 수행되지 않는 것을 나타냅니다.
4. 적용할 수 없음은 이 조작에 권한 검사가 연관되지 않음을 나타냅니다. 예를 들어, MQPUT 호출을 발행하여 오브젝트를 처리할 수 없습니다.

IBM i IBM i에서 이스케이프 PCF의 MQSC 명령에 대한 권한

이 권한을 사용하여 관리 명령을 이스케이프 PCF 메시지로 발행할 수 있습니다. 이 메소드는 해당 사용자를 대신하여 실행하기 위해 프로그램이 관리 명령을 큐 관리자에 메시지로 송신하도록 허용합니다.

이 절은 이스케이프 PCF에 포함된 각 MQSC 명령에 필요한 권한을 요약합니다.

적용할 수 없음은 이 조작에 권한 검사가 연관되지 않음을 나타냅니다.

명령을 제출하는 프로그램이 실행 중인 사용자 ID는 다음 권한도 있어야 합니다.

- 큐 관리자에 대한 MQZAO_CONNECT 권한
- PCF 명령을 수행하기 위한 큐 관리자의 DISPLAY 권한
- 이스케이프 PCF 명령 텍스트 내에서 MQSC 명령을 발행하는 권한

ALTER object

오브젝트	필수 권한
큐	MQZAO_CHANGE

오브젝트	필수 권한
주제	MQZAO_CHANGE
프로세스	MQZAO_CHANGE
큐 관리자	MQZAO_CHANGE
이름 목록	MQZAO_CHANGE
인증 정보	MQZAO_CHANGE
채널	MQZAO_CHANGE
클라이언트 연결 채널	MQZAO_CHANGE
리스너	MQZAO_CHANGE
서비스	MQZAO_CHANGE

CLEAR object

오브젝트	필수 권한
큐	MQZAO_CLEAR
주제	MQZAO_CLEAR
프로세스	적용할 수 없음
큐 관리자	적용할 수 없음
이름 목록	적용할 수 없음
인증 정보	적용할 수 없음
채널	적용할 수 없음
클라이언트 연결 채널	적용할 수 없음
리스너	적용할 수 없음
서비스	적용할 수 없음

DEFINE object NOREPLACE (154 페이지의 『1』)

오브젝트	필수 권한
큐	MQZAO_CREATE (154 페이지의 『2』)
주제	MQZAO_CREATE (154 페이지의 『2』)
프로세스	MQZAO_CREATE (154 페이지의 『2』)
큐 관리자	적용할 수 없음
이름 목록	MQZAO_CREATE (154 페이지의 『2』)
인증 정보	MQZAO_CREATE (154 페이지의 『2』)
채널	MQZAO_CREATE (154 페이지의 『2』)
클라이언트 연결 채널	MQZAO_CREATE (154 페이지의 『2』)
리스너	MQZAO_CREATE (154 페이지의 『2』)
서비스	MQZAO_CREATE (154 페이지의 『2』)

DEFINE object REPLACE (154 페이지의 『1』, 154 페이지의 『3』)

오브젝트	필수 권한
큐	MQZAO_CHANGE
주제	MQZAO_CHANGE
프로세스	MQZAO_CHANGE
큐 관리자	적용할 수 없음
이름 목록	MQZAO_CHANGE
인증 정보	MQZAO_CHANGE
채널	MQZAO_CHANGE
클라이언트 연결 채널	MQZAO_CHANGE
리스너	MQZAO_CHANGE
서비스	MQZAO_CHANGE

DELETE object

오브젝트	필수 권한
큐	MQZAO_DELETE
주제	MQZAO_DELETE
프로세스	MQZAO_DELETE
큐 관리자	적용할 수 없음
이름 목록	MQZAO_DELETE
인증 정보	MQZAO_DELETE
채널	MQZAO_DELETE
클라이언트 연결 채널	MQZAO_DELETE
리스너	MQZAO_DELETE
서비스	MQZAO_DELETE

DISPLAY object

오브젝트	필수 권한
큐	MQZAO_DISPLAY
주제	MQZAO_DISPLAY
프로세스	MQZAO_DISPLAY
큐 관리자	MQZAO_DISPLAY
이름 목록	MQZAO_DISPLAY
인증 정보	MQZAO_DISPLAY
채널	MQZAO_DISPLAY
클라이언트 연결 채널	MQZAO_DISPLAY
리스너	

오브젝트	필수 권한
서비스	

PING CHANNEL

오브젝트	필수 권한
큐	적용할 수 없음
주제	적용할 수 없음
프로세스	적용할 수 없음
큐 관리자	적용할 수 없음
이름 목록	적용할 수 없음
인증 정보	적용할 수 없음
채널	MQZAO_CONTROL
클라이언트 연결 채널	적용할 수 없음
리스너	적용할 수 없음
서비스	적용할 수 없음

RESET CHANNEL

오브젝트	필수 권한
큐	적용할 수 없음
주제	적용할 수 없음
프로세스	적용할 수 없음
큐 관리자	적용할 수 없음
이름 목록	적용할 수 없음
인증 정보	적용할 수 없음
채널	MQZAO_CONTROL_EXTENDED
클라이언트 연결 채널	적용할 수 없음
리스너	적용할 수 없음
서비스	적용할 수 없음

RESOLVE CHANNEL

오브젝트	필수 권한
큐	적용할 수 없음
주제	적용할 수 없음
프로세스	적용할 수 없음
큐 관리자	적용할 수 없음
이름 목록	적용할 수 없음
인증 정보	적용할 수 없음
채널	MQZAO_CONTROL_EXTENDED

오브젝트	필수 권한
클라이언트 연결 채널	적용할 수 없음
리스너	적용할 수 없음
서비스	적용할 수 없음

START object

오브젝트	필수 권한
큐	적용할 수 없음
주제	적용할 수 없음
프로세스	적용할 수 없음
큐 관리자	적용할 수 없음
이름 목록	적용할 수 없음
인증 정보	적용할 수 없음
채널	MQZAO_CONTROL
클라이언트 연결 채널	적용할 수 없음
리스너	MQZAO_CONTROL
서비스	MQZAO_CONTROL

STOP object

오브젝트	필수 권한
큐	적용할 수 없음
주제	적용할 수 없음
프로세스	적용할 수 없음
큐 관리자	적용할 수 없음
이름 목록	적용할 수 없음
인증 정보	적용할 수 없음
채널	MQZAO_CONTROL
클라이언트 연결 채널	적용할 수 없음
리스너	MQZAO_CONTROL
서비스	MQZAO_CONTROL

참고:

1. DEFINE 명령의 경우, LIKE 오브젝트(지정된 경우)에 대한 MQZAO_DISPLAY 권한도 필요하며, LIKE가 생략된 경우 적절한 SYSTEM.DEFAULT.xxx 오브젝트에 대한 권한이 필요합니다.
2. MQZAO_CREATE 권한은 특정 오브젝트나 오브젝트 유형에 특정되지 않습니다. 작성 권한은 GRTRMQMAUT 명령에 오브젝트 유형 QMGR을 지정하여 지정된 큐 관리자의 모든 오브젝트에 대해 부여됩니다.
3. 이 옵션은 바꿀 오브젝트가 이미 있는 경우에만 적용됩니다. 존재하지 않는 경우, 검사는 DEFINE object NOREPLACE로 수행됩니다.

IBM i IBM i에서 PCF 명령의 권한 부여

이 권한 부여를 통해 사용자는 관리 명령을 PCF 명령으로 발행할 수 있습니다. 이 메소드는 해당 사용자를 대신하여 실행하기 위해 프로그램이 관리 명령을 큐 관리자에 메시지로 송신하도록 허용합니다.

이 절에서는 각 PCF 명령에 필요한 권한을 요약합니다.

검사 안함은 권한 검사가 수행되지 않는 것을 나타내며 적용할 수 없음은 권한 검사가 이 조작에 연관되지 않음을 나타냅니다.

명령을 제출하는 프로그램이 실행 중인 사용자 ID는 다음 권한도 있어야 합니다.

- 큐 관리자에 대한 MQZAO_CONNECT 권한
- PCF 명령을 수행하기 위한 큐 관리자의 DISPLAY 권한

특수 권한 MQZAO_ALL_ADMIN에는 다음 권한이 포함됩니다.

- MQZAO_CHANGE
- MQZAO_CLEAR
- MQZAO_DELETE
- MQZAO_DISPLAY
- MQZAO_CONTROL
- MQZAO_CONTROL_EXTENDED

MQZAO_CREATE는 특정 오브젝트 또는 오브젝트 유형에 특정되지 않기 때문에 포함되지 않습니다.

object 변경

오브젝트	필수 권한
큐	MQZAO_CHANGE
주제	MQZAO_CHANGE
프로세스	MQZAO_CHANGE
큐 관리자	MQZAO_CHANGE
이름 목록	MQZAO_CHANGE
인증 정보	MQZAO_CHANGE
채널	MQZAO_CHANGE
클라이언트 연결 채널	MQZAO_CHANGE
리스너	MQZAO_CHANGE
서비스	MQZAO_CHANGE

object 지우기

오브젝트	필수 권한
큐	MQZAO_CLEAR
주제	MQZAO_CLEAR
프로세스	적용할 수 없음
큐 관리자	적용할 수 없음
이름 목록	적용할 수 없음
인증 정보	적용할 수 없음
채널	적용할 수 없음

오브젝트	필수 권한
클라이언트 연결 채널	적용할 수 없음
리스너	적용할 수 없음
서비스	적용할 수 없음

오브젝트 복사(대체 제외) (160 페이지의 『1』)

오브젝트	필수 권한
큐	MQZAO_CREATE (160 페이지의 『2』)
주제	MQZAO_CREATE (160 페이지의 『2』)
프로세스	MQZAO_CREATE (160 페이지의 『2』)
큐 관리자	적용할 수 없음
NamelistMQZAO_CREATE	MQZAO_CREATE (160 페이지의 『2』)
인증 정보	MQZAO_CREATE (160 페이지의 『2』)
채널	MQZAO_CREATE (160 페이지의 『2』)
클라이언트 연결 채널	MQZAO_CREATE (160 페이지의 『2』)
리스너	MQZAO_CREATE (160 페이지의 『2』)
서비스	MQZAO_CREATE (160 페이지의 『2』)

Copy object(바꾸기 포함)(160 페이지의 『1』 , 160 페이지의 『4』)

오브젝트	필수 권한
큐	MQZAO_CHANGE
주제	MQZAO_CHANGE
프로세스	MQZAO_CHANGE
큐 관리자	적용할 수 없음
이름 목록	MQZAO_CHANGE
인증 정보	MQZAO_CHANGE
채널	MQZAO_CHANGE
클라이언트 연결 채널	MQZAO_CHANGE
리스너	MQZAO_CHANGE
서비스	MQZAO_CHANGE

오브젝트 작성(대체 제외) (160 페이지의 『3』)

오브젝트	필수 권한
큐	MQZAO_CREATE (160 페이지의 『2』)
주제	MQZAO_CREATE (160 페이지의 『2』)
프로세스	MQZAO_CREATE (160 페이지의 『2』)
큐 관리자	적용할 수 없음
이름 목록	MQZAO_CREATE (160 페이지의 『2』)

오브젝트	필수 권한
인증 정보	MQZAO_CREATE (160 페이지의 『2』)
채널	MQZAO_CREATE (160 페이지의 『2』)
클라이언트 연결 채널	MQZAO_CREATE (160 페이지의 『2』)
리스너	MQZAO_CHANGE
서비스	MQZAO_CHANGE

Create object(바꾸기 포함)(160 페이지의 『3』 , 160 페이지의 『4』)

오브젝트	필수 권한
큐	MQZAO_CHANGE
주제	MQZAO_CHANGE
프로세스	MQZAO_CHANGE
큐 관리자	적용할 수 없음
이름 목록	MQZAO_CHANGE
인증 정보	MQZAO_CHANGE
채널	MQZAO_CHANGE
클라이언트 연결 채널	MQZAO_CHANGE
리스너	MQZAO_CHANGE
서비스	MQZAO_CHANGE

object 삭제

오브젝트	필수 권한
큐	MQZAO_DELETE
주제	MQZAO_DELETE
프로세스	MQZAO_DELETE
큐 관리자	MQZAO_DELETE
이름 목록	MQZAO_DELETE
인증 정보	MQZAO_DELETE
채널	MQZAO_DELETE
클라이언트 연결 채널	MQZAO_DELETE
리스너	MQZAO_DELETE
서비스	MQZAO_DELETE

object 조회

오브젝트	필수 권한
큐	MQZAO_DISPLAY
주제	MQZAO_DISPLAY
프로세스	MQZAO_DISPLAY

오브젝트	필수 권한
큐 관리자	MQZAO_DISPLAY
이름 목록	MQZAO_DISPLAY
인증 정보	MQZAO_DISPLAY
채널	MQZAO_DISPLAY
클라이언트 연결 채널	MQZAO_DISPLAY
리스너	MQZAO_DISPLAY
서비스	MQZAO_DISPLAY

object 이름 조회

오브젝트	필수 권한
큐	검사 안함
주제	검사 안함
프로세스	검사 안함
큐 관리자	검사 안함
이름 목록	검사 안함
인증 정보	검사 안함
채널	검사 안함
클라이언트 연결 채널	검사 안함
리스너	검사 안함
서비스	검사 안함

채널 ping

오브젝트	필수 권한
큐	적용할 수 없음
주제	적용할 수 없음
프로세스	적용할 수 없음
큐 관리자	적용할 수 없음
이름 목록	적용할 수 없음
인증 정보	적용할 수 없음
채널	MQZAO_CONTROL
클라이언트 연결 채널	적용할 수 없음
리스너	적용할 수 없음
서비스	적용할 수 없음

채널 재설정

오브젝트	필수 권한
큐	적용할 수 없음

오브젝트	필수 권한
주제	적용할 수 없음
프로세스	적용할 수 없음
큐 관리자	적용할 수 없음
이름 목록	적용할 수 없음
인증 정보	적용할 수 없음
채널	MQZAO_CONTROL_EXTENDED
클라이언트 연결 채널	적용할 수 없음
리스너	적용할 수 없음
서비스	적용할 수 없음

큐 통계 재설정

오브젝트	필수 권한
큐	MQZAO_DISPLAY and MQZAO_CHANGE
주제	적용할 수 없음
프로세스	적용할 수 없음
큐 관리자	적용할 수 없음
이름 목록	적용할 수 없음
인증 정보	적용할 수 없음
채널	적용할 수 없음
클라이언트 연결 채널	적용할 수 없음
리스너	
서비스	

채널 분석

오브젝트	필수 권한
큐	적용할 수 없음
주제	적용할 수 없음
프로세스	적용할 수 없음
큐 관리자	적용할 수 없음
이름 목록	적용할 수 없음
인증 정보	적용할 수 없음
채널	MQZAO_CONTROL_EXTENDED
클라이언트 연결 채널	적용할 수 없음
리스너	적용할 수 없음
서비스	적용할 수 없음

채널 시작

오브젝트	필수 권한
큐	적용할 수 없음
주제	적용할 수 없음
프로세스	적용할 수 없음
큐 관리자	적용할 수 없음
이름 목록	적용할 수 없음
인증 정보	적용할 수 없음
채널	MQZAO_CONTROL
클라이언트 연결 채널	적용할 수 없음
리스너	적용할 수 없음
서비스	적용할 수 없음

채널 중지

오브젝트	필수 권한
큐	적용할 수 없음
주제	적용할 수 없음
프로세스	적용할 수 없음
큐 관리자	적용할 수 없음
이름 목록	적용할 수 없음
인증 정보	적용할 수 없음
채널	MQZAO_CONTROL
클라이언트 연결 채널	적용할 수 없음
리스너	적용할 수 없음
서비스	적용할 수 없음

참고:

1. 복사 명령의 경우, From 오브젝트에 대한 MQZAO_DISPLAY 권한도 필요합니다.
2. MQZAO_CREATE 권한은 특정 오브젝트나 오브젝트 유형에 특정되지 않습니다. 작성 권한은 GRTRMQMAUT 명령에 오브젝트 유형 QMGR을 지정하여 지정된 큐 관리자의 모든 오브젝트에 대해 부여됩니다.
3. 작성 명령의 경우, 해당 SYSTEM.DEFAULT.* 객체 (object)
4. 이 옵션은 바꿀 오브젝트가 이미 있는 경우에만 적용됩니다. 없는 경우, 검사는 복사 또는 작성(바꾸기 없음)에 대해 수행됩니다.

IBM i의 일반 OAM 프로파일

오브젝트 권한 관리자(OAM) 일반 프로파일을 사용하면 각 오브젝트가 작성될 때마다 개별적으로 별도의 GRTRMQMAUT 명령을 발행하지 않고 사용자가 여러 오브젝트에 가지는 권한을 한 번에 설정할 수 있습니다. GRTRMQMAUT 명령에서 일반 프로파일을 사용하면 해당 프로파일에 맞게 나중에 작성되는 모든 오브젝트에 대해 일반 권한을 설정할 수 있습니다.

이 절의 나머지에서는 일반 프로파일 사용에 대해 좀 더 자세하게 설명합니다.

- 161 페이지의 『와일드카드 문자 사용』

와일드카드 문자 사용

프로파일을 일반적으로 작성하는 방법은 프로파일 이름에 특수 문자(와일드카드 문자)를 사용하는 것입니다. 예를 들어 물음표(?) 와일드카드 문자는 이름에서 단일 문자를 일치시킵니다. 따라서, ABC.?EF를 지정하면 해당 프로파일에 부여한 권한이 ABC.DEF, ABC.CEF, ABC.BEF 이름 등으로 작성되는 모든 오브젝트에 적용됩니다.

사용 가능한 와일드카드 문자는 다음과 같습니다.

?

단일 문자 대신 물음표(?) 사용. 예를 들어, AB.?D는 오브젝트 AB.CD, AB.ED, AB.FD에 적용됩니다.

*

별표(*)를 다음과 같이 사용하십시오.

- 오브젝트 이름에 있는 규정자와 일치하는 프로파일 이름의 규정자. 규정자는 마침표로 구분되는 오브젝트 이름의 한 부분입니다. 예를 들어, ABC.DEF.GHI에서 규정자는 ABC, DEF 및 GHI입니다.

예를 들어, ABC.*.JKL은 오브젝트 ABC.DEF.JKL 및 ABC.GHI.JKL에 적용됩니다. (이는 ABC.JKL에 적용되지 **않습니다**. 이 컨텍스트에 사용되는 *는 항상 하나의 규정자를 표시합니다.)

- 오브젝트 이름에 있는 규정자 내에서 0개 또는 그 이상의 문자와 일치하는 프로파일 이름의 규정자 문자. 예를 들어, ABC.DE*.JKL은 오브젝트 ABC.DE.JKL, ABC.DEF.JKL, ABC.DEGH.JKL에 적용됩니다.

**

다음과 같이 프로파일 이름에서는 이중 별표(**)를 **한 번만** 사용하십시오.

- 모든 오브젝트 이름과 일치하는 전체 프로파일 이름. 예를 들어 OBJTYPE (*PRC) 키워드를 사용하여 프로세스를 식별하는 경우, 프로파일 이름으로 **를 사용하면 모든 프로세스의 권한을 변경할 수 있습니다.
- 오브젝트 이름에 있는 0개 또는 그 이상의 규정자와 일치하는 프로파일 이름의 시작, 중간 또는 종료 규정자로서 사용됩니다. 예를 들어, **.ABC는 모든 오브젝트를 최종 규정자 ABC로 식별합니다.

프로파일 우선순위

일반 프로파일을 사용할 경우 이해해야 하는 중요한 점은 작성 중인 오브젝트에 적용할 권한을 결정할 때 프로파일에 지정되는 우선순위입니다. 예를 들어, 다음 명령을 발행한 것으로 가정해 보십시오.

```
GRTRMOMAUT OBJ(AB.*) OBJTYPE(*Q) USER(FRED) AUT(*PUT) MQMNAME(MYQMGR)
GRTRMOMAUT OBJ(AB.C*) OBJTYPE(*Q) USER(FRED) AUT(*GET) MQMNAME(MYQMGR)
```

첫 번째는 프로파일 AB.*와 일치하는 이름을 가진 프린시펄 FRED에 대한 모든 큐에 대한 권한을 부여합니다. 두 번째는 프로파일 AB.C*.

이제 AB.CD 큐를 작성한다고 가정합니다. 와일드카드 적용에 대한 규칙에 따라 GRTRMOMAUT 중 하나가 해당 큐에 적용됩니다. 따라서, 넣기 또는 가져오기 권한이 있습니까?

응답을 찾기 위해 여러 프로파일을 오브젝트에 적용할 수 있을 때마다 **가장 특정되게 적용되는** 규칙만 적용합니다. 이 규칙을 적용하는 방법은 프로파일 이름을 왼쪽에서 오른쪽으로 비교하는 것입니다. 다른 경우, 일반 문자가 아닌 문자가 일반 문자보다 더 특정되는 문자입니다. 따라서, 이전 예에서 큐 AB.CD는 **가져오기** 권한을 가집니다(AB.C*는 AB.*보다 더 특정됩니다).

일반 문자를 비교할 때 특이성의 순서는 다음과 같습니다.

1. ?
2. *
3. **

IBM i에 설치된 권한 서비스 지정

사용하려는 권한 서비스 컴포넌트를 지정할 수 있습니다.

The parameter **Service Component name** on **GRTMQMAUT** and **RVKMQMAUT** allows you to specify the name of the installed authorization service component.

초기 패널에서 **F24**를 선택하고 명령 중 하나의 다음 패널에서 **F9=모든 매개변수**를 선택하면 설치된 권한 부여 컴포넌트(*DFT) 또는 큐 관리자 qm.ini 파일의 서비스 스탠자에 지정된 필수 권한 서비스 컴포넌트 이름을 지정할 수 있습니다.

DSPMQMAUT도 이 추가 매개변수를 포함합니다. 이 매개변수를 사용하면 설치된 모든 권한 부여 컴포넌트(*DFT) 또는 지정된 권한 서비스 컴포넌트 이름을 지정한 오브젝트 이름, 오브젝트 유형, 사용자에게 대해 검색할 수 있습니다.

IBM i IBM i에서 권한 프로파일을 사용하거나 사용하지 않고 작업

이 정보를 사용하여 권한 프로파일에 대해 작업하는 방법 및 권한 프로파일 없이 작업하는 방법에 대해 학습합니다.

162 페이지의 『[권한 프로파일에 대해 작업](#)』에서 설명하는 대로 권한 프로파일을 사용하여 작업하거나 여기에서 설명하는 대로 권한 프로파일을 사용하지 않고 작업할 수 있습니다.

권한 프로파일을 사용하지 않고 작업하려면 *NONE을 **GRTMQMAUT**에서 Authority 매개변수로 사용하여 권한없이 프로파일을 작성하십시오. 기존의 프로파일은 모두 변경되지 않고 유지됩니다.

RVKMQMAUT에서 Authority 매개변수로 *REMOVE를 사용하여 기존 권한 프로파일을 제거하십시오.

권한 프로파일에 대해 작업

권한 프로파일에는 두 개의 연관된 명령이 있습니다.

- **WRKMQMAUT**
- **WRKMQMAUTD**

해당 명령에는 명령행에서 직접 또는 **WRKMQM** 패널에서 다음 방법으로 액세스 가능합니다.

1. 큐 관리자 이름에 입력하고 Enter 키를 눌러서 **WRKMQM** 결과 패널에 액세스하십시오.
2. 이 패널에서 F23=More options 선택하십시오.

옵션 24는 **WRKMQMAUT** 명령에 대한 결과 패널을 선택하고 옵션 25는 SSL 바인딩 계층과 함께 사용되는 **WRKMQMAUTI** 명령을 선택합니다.

WRKMQMAUT

이 명령을 사용하여 권한 큐에 보유된 권한 데이터에 대해 작업할 수 있습니다.

참고: 이 명령을 실행하려면 큐 관리자에 대해 *connect 및 *admdsp 권한이 있어야 합니다. 그렇지만 프로파일을 작성하거나 삭제하려면 QMQMADM 권한이 필요합니다.

정보를 화면으로 출력하는 경우 권한 프로파일 이름 목록이 해당 유형과 같이 표시됩니다. 출력을 인쇄하는 경우 모든 권한 데이터, 등록된 사용자, 해당 권한에 대한 자세한 목록을 수신합니다.

이 패널에서 오브젝트 또는 프로파일 이름을 입력하고 ENTER를 누르면 **WRKMQMAUT**에 대한 결과 패널이 표시됩니다.

4=Delete를 선택하면 지정하는 일반 권한 프로파일 이름에 등록되는 모든 사용자 이름 삭제를 확인할 수 있는 새 패널로 이동합니다. 이 옵션은 모든 사용자에게 대해 *REMOVE 옵션과 같이 **RVKMQMAUT**를 실행하고 일반 프로파일 이름에만 적용됩니다.

12=Work with profile을 선택하면 163 페이지의 『[WRKMQMAUTD](#)』에서 설명하는 대로 **WRKMQMAUTD** 명령 결과 패널로 이동합니다.

WRKMQMAUTD

이 명령을 사용하면 특정 권한 프로파일 이름 및 오브젝트 유형에 등록되는 모든 사용자를 표시할 수 있습니다. 이 명령을 실행하려면 큐 관리자에 대해 *connect 및 *admdsp 권한이 있어야 합니다. 그렇지만 프로파일에 권한 부여, 실행, 작성 또는 삭제하려면 QMQADM 권한이 필요합니다.

초기 입력 패널에서 F24=More keys 를 선택한 후 F9=All Parameters 옵션을 선택하면 **GRTMQMAUT** 및 **RVKMQMAUT**에 대한 서비스 컴포넌트 이름이 표시됩니다.

참고: F11=Display Object Authorizations 키는 다음 유형의 권한을 전환합니다.

- 오브젝트 권한
- 컨텍스트 권한
- MQI 권한

화면의 옵션은 다음과 같습니다.

2=Grant

현재 권한을 추가하는 **GRTMQMAUT** 패널로 이동합니다.

3=Revoke

일부 현재 정의를 제거하는 **RVKMQMAUT** 패널로 이동합니다.

4=Delete

지정한 사용자에 대한 권한 데이터를 삭제할 수 있는 패널로 이동합니다. 이는 *REMOVE 옵션과 같이 **RVKMQMAUT**를 실행합니다.

5=Display

기존 **DSPMQMAUT** 명령으로 이동합니다.

F6=Create

프로파일 권한 레코드를 작성할 수 있는 **GRTMQMAUT** 패널로 이동합니다.

IBM i에서 오브젝트 권한 관리자 지침

오브젝트 권한 관리자(OAM) 사용에 대한 추가 힌트 및 팁

민감한 조작에 대한 액세스 제한

일부 조작은 민감하며 권한이 있는 사용자로 제한됩니다. 예:

- 전송 큐와 같은 일부 특수 큐 또는 명령 큐 SYSTEM.ADMIN.COMMAND.QUEUE에 액세스
- 전체 MQI 컨텍스트 옵션을 사용하는 프로그램 실행
- 애플리케이션 큐 작성 및 복사

큐 관리자 디렉토리

큐 및 기타 큐 관리자 데이터를 포함하는 디렉토리 및 라이브러리는 제품에 대해 개인용입니다. MQI 자원에 대한 권한을 부여하거나 취소할 때 표준 운영 체제 명령을 사용하지 마십시오.

큐

동적 큐의 권한은 도출된 모델 큐를 기반으로 하지만 동일할 필요는 없습니다.

알리어스 큐 또는 리모트 큐의 경우, 권한은 알리어스 큐나 리모트 큐가 해결되는 큐가 아니라 오브젝트 자체에 대한 권한입니다. 사용자 프로파일에 액세스 권한이 없는 로컬 큐로 해결되는 알리어스 큐에 액세스하도록 사용자 프로파일에 권한을 부여할 수 있습니다.

큐 작성 권한을 권한이 있는 사용자로 제한하십시오. 그렇게 하지 않으면 사용자가 알리어스를 작성하여 일반 액세스 제어를 무시할 수 있습니다.

대체 사용자 권한

대체 사용자 권한은 한 개의 사용자 프로파일이 IBM MQ 오브젝트 액세스 시에 다른 사용자 프로파일의 권한을 사용할 수 있는지 여부를 제어합니다. 이 기술은 서버가 프로그램의 요청을 수신하고 서버가 프로그램에 요청에 필요한 권한이 있는지 확인하려는 경우에 필수입니다. 서버에는 필수 권한이 있을 수 있지만 프로그램이 요청한 조치에 대한 권한이 있는지 여부를 알아야 합니다.

예를 들면, 다음과 같습니다.

- 사용자 프로파일 PAYSERV에서 실행 중인 서버 프로그램은 사용자 프로파일 USER1으로 큐에 넣은 요청 메시지를 큐에서 검색합니다.
- 서버 프로그램이 요청 메시지를 가져오면 요청을 처리하고 요청 메시지에 지정된 응답 대상 큐로 응답을 다시 넣습니다.
- 응답 대상 큐 열기 권한을 부여하기 위해 자체 사용자 프로파일(PAYSERV)을 사용하는 대신 서버는 다른 사용자 프로파일(이 경우에는 USER1)을 지정할 수 있습니다. 이 예에서 대체 사용자 권한을 사용하여 응답 대상 큐를 열 때 PAYSERV가 대체 사용자 프로파일로 USER1을 지정할 수 있는지 여부를 제어할 수 있습니다.

대체 사용자 프로파일은 오브젝트 디스크립터의 *AlternateUserId* 필드에 지정됩니다.

참고: 모든 IBM MQ 오브젝트에서 대체 사용자 프로파일을 사용할 수 있습니다. 대체 사용자 프로파일 사용은 다른 자원 관리자에서 사용되는 사용자 프로파일에는 영향을 주지 않습니다.

컨텍스트 권한

컨텍스트는 특정 메시지에 적용되는 정보이며, 메시지의 일부인 메시지 설명자 MQMD에 포함되어 있습니다.

컨텍스트에 연관된 메시지 디스크립터 필드의 설명에 대해서는 [MQMD 개요](#)를 참조하십시오.

컨텍스트 옵션에 대한 정보는 [메시지 컨텍스트](#)를 참조하십시오.

원격 보안 고려사항

원격 보안에 대해서는 다음을 고려하십시오.

넣기 권한

큐 관리자에서 보안을 위해 채널이 다른 큐 관리자에서 송신된 메시지를 수신할 때 사용되는 넣기 권한을 지정할 수 있습니다.

이 매개변수는 RQSTR, RQSTR 또는 CLUSRCVR 채널 유형에 대해서만 유효합니다. 다음과 같은 채널 속성 PUTAUT를 지정하십시오.

DEF

기본 사용자 프로파일. 이는 메시지 채널 에이전트가 실행 중인 QMQM 사용자 프로파일입니다.

CTX

메시지 컨텍스트의 사용자 프로파일.

전송 큐

큐 관리자는 자동으로 원격 메시지를 전송 큐에 넣으며 이를 위해 특수 권한이 필요하지는 않습니다. 그렇지만 메시지를 전송 큐에 직접 넣으려면 특수한 권한이 필요합니다.

채널 엑시트

채널 엑시트는 추가된 보안에 사용할 수 있습니다.

채널 인증 레코드

채널 레벨에서 연결 시스템에 부여된 액세스 권한에 대한 보다 정밀한 제어를 실행하기 위해 사용합니다.

원격 보안에 대한 자세한 정보는 96 페이지의 『[채널 권한 부여](#)』의 내용을 참조하십시오.

SSL/TLS을 사용하는 채널 보호

TLS(Transport Layer Security) 프로토콜은 도청, 도용, 위장에 대한 보호를 사용하여 채널 보안을 제공합니다. TLS에 대한 IBM MQ 지원을 사용하면 채널 정의에서 특정 채널이 TLS 보안을 사용하도록 지정할 수 있습니다. 또한, 사용하려는 암호화 알고리즘과 같은 필요한 보안 세부사항을 지정할 수도 있습니다.

IBM MQ에서의 TLS 지원은 큐 관리자 인증 정보 오브젝트와 다양한 CL 및 MQSC 명령, 필요한 TLS 지원 세부사항을 자세하게 정의하는 큐 관리자 및 채널 매개변수를 사용합니다.

다음 CL 명령이 TLS를 지원합니다.

WRKMQMAUTI

인증 정보 오브젝트 속성에 대해 작업합니다.

CHGMQMAUTI

인증 정보 오브젝트 속성을 수정합니다.

CRTMQMAUTI

인증 정보 오브젝트를 작성합니다.

CPYMQMAUTI

기존 인증 정보 오브젝트를 복사하여 이를 작성합니다.

DLTMQMAUTI

인증 정보 오브젝트를 삭제합니다.

DSPMQMAUTI

특정 인증 정보 오브젝트 속성을 표시합니다.

TLS를 사용하는 채널 보안 개요는 다음을 참조하십시오.

- [TLS로 채널 보호](#)

TLS와 연관된 PCF 명령에 대한 자세한 내용은 다음을 참조하십시오.

- [인증 정보 오브젝트 변경, 복사 및 작성](#)
- [인증 정보 오브젝트 삭제](#)
- [인증 정보 오브젝트 조회](#)

z/OS

z/OS에서 보안 설정

z/OS에 특정되는 보안 고려사항입니다.

IBM MQ for z/OS의 보안은 RACF 또는 이에 대응하는 외부 보안 관리자(ESM)으로 제어됩니다.

다음 지시사항에서는 RACF를 사용하는 것으로 간주합니다.

관련 참조

[보안 시나리오: z/OS의 두 개의 큐 관리자](#)

[보안 시나리오: z/OS의 큐 공유 그룹](#)

z/OS

RACF 보안 클래스

RACF 클래스는 IBM MQ 보안 검사에 필요한 프로파일 보유에 사용됩니다. 멤버 클래스 중 다수는 동등한 그룹 클래스를 가집니다. 클래스를 활성화하고 일반 프로파일을 승인하도록 이를 사용해야 합니다.

각 RACF 클래스는 [166 페이지의 표 23](#)에서 보여주는 대로 검사 순서의 일정 시점에 사용되는 하나 이상의 프로파일을 보유합니다.

표 23. IBM MQ 에 의해 사용되는 RACF 클래스

멤버 클래스	그룹 클래스	컨텐츠
MQADMIN	GMQADMIN	<p>프로파일:</p> <p>관리 유형 기능에 대한 프로파일 보유에 주로 사용됩니다. 예를 들면, 다음과 같습니다.</p> <ul style="list-style-type: none"> • IBM MQ 보안 스위치의 프로파일 • RESLEVEL 보안 프로파일 • 대체 사용자 보안을 위한 프로파일 • 컨텍스트 보안 프로파일 • 명령 자원 보안을 위한 프로파일
MXADMIN	GMXADMIN	<p>프로파일:</p> <p>관리 유형 기능에 대한 프로파일 보유에 주로 사용됩니다. 예를 들면, 다음과 같습니다.</p> <ul style="list-style-type: none"> • IBM MQ 보안 스위치의 프로파일 • RESLEVEL 보안 프로파일 • 대체 사용자 보안을 위한 프로파일 • 컨텍스트 보안 프로파일 • 명령 자원 보안을 위한 프로파일 <p>이 클래스는 대문자 및 대소문자 혼합 RACF 프로파일 모두를 보유할 수 있습니다.</p>
MQCONN		연결 보안에 사용되는 프로파일
MQCMDSD		명령 보안에 사용되는 프로파일
MQQUEUE	GMQQUEUE	큐 자원 보안에서 사용되는 프로파일
MXQUEUE	GMXQUEUE	큐 자원 보안에서 사용되는 대소문자 혼합 및 대문자 프로파일
MQPROC	GMQPROC	프로세스 자원 보안에서 사용되는 프로파일
MXPROC	GMXPROC	프로세스 자원 보안에서 사용되는 대소문자 혼합 및 대문자 프로파일
MQNLIST	GMQNLIST	이름 목록 자원 보안에서 사용되는 프로파일
MXNLIST	GMXNLIST	이름 목록 자원 보안에서 사용되는 대소문자 혼합 및 대문자 프로파일
MXTOPIC	GMXTOPIC	토픽 보안에서 사용되는 대소문자 혼합 및 대문자 프로파일

일부 클래스는 유사한 액세스 요구사항이 있는 자원 그룹을 같이 넣을 수 있도록 하는 관련된 그룹 클래스를 가집니다. 구성원 및 그룹 클래스 간의 차이점과 구성원 또는 그룹 클래스를 사용하는 시기에 대한 세부사항은 [z/OS Security Server RACF 보안 관리자 안내서](#)를 참조하십시오.

클래스는 보안 검사 수행 전에 활성화해야 합니다. 모든 IBM MQ 클래스를 활성화하기 위해 다음 RACF 명령을 사용할 수 있습니다.

```
SETROPTS CLASSACT(MQADMIN, MXADMIN, MQQUEUE, MXQUEUE, MQPROC, MXPROC,
MQNLIST, MXNLIST, MXTOPIC, MQCONN, MQCMDSD)
```

클래스가 일반 프로파일을 승인할 수 있도록 클래스도 설정해야 합니다. RACF 명령 SETROPTS로도 이를 수행합니다. 예:

```
SETROPTS GENERIC (MQADMIN, MXADMIN, MQQUEUE, MXQUEUE, MQPROC, MXPROC,
                  MQNLIST, MXNLIST, MXTOPIC, MQCONN, MQCMDS)
```

z/OS RACF 프로파일

IBM MQ 에 사용되는 모든 RACF 프로파일에는 큐 관리자 이름 또는 큐 공유 그룹 이름인 접두부가 포함되어 있습니다. 와일드카드 퍼센트 부호를 사용하는 경우에는 주의해야 합니다.

IBM MQ 에 사용되는 모든 RACF 프로파일에는 접두부가 포함되어 있습니다. 큐 공유 그룹 레벨 보안의 경우에는 큐 공유 그룹 이름입니다. 큐 관리자 레벨 보안의 경우 접두부는 큐 관리자 이름입니다. 큐 관리자와 큐 공유 그룹 레벨 보안을 혼합하여 사용 중인 경우에는 두 유형의 접두부 모두가 포함된 프로파일을 사용합니다. (큐 공유 그룹 및 큐 관리자 레벨 보안은 [IBM MQ for z/OS 개념: 보안](#)에서 설명됩니다.)

큐 공유 그룹 레벨의 큐 공유 그룹 OSG1의 QUEUE_FOR_SUBSCRIBER_LIST 큐를 보호하려는 경우 적절한 프로파일이 다음과 같이 RACF에 정의됩니다.

```
RDEFINE MQQUEUE QSG1.QUEUE_FOR_SUBSCRIBER_LIST
```

큐 관리자 레벨에서 큐 관리자 STCD에 속하는 QUEUE_FOR_LOST_CARD_LIST 큐를 보호하려는 경우, 다음과 같이 적절한 프로파일에 RACF에 정의됩니다.

```
RDEFINE MQQUEUE STCD.QUEUE_FOR_LOST_CARD_LIST
```

이는 다른 큐 관리자와 큐 공유 그룹이 동일한 RACF 데이터베이스를 공유할 수 있지만 다른 보안 옵션을 사용하는 것을 나타냅니다.

예기치 못한 사용자 액세스를 방지하기 위해 프로파일에는 일반적인 큐 관리자 이름은 사용하지 마십시오.

IBM MQ는 오브젝트 이름에서 퍼센트 부호(%) 사용을 허용합니다. 그렇지만 RACF는 % 문자를 단일 문자의 와일드카드로 사용합니다. 즉, 이름에 % 문자를 사용하여 오브젝트 이름을 정의하는 경우 해당 프로파일을 정의할 때 이를 고려해야 합니다.

예를 들어, 큐 관리자 CRDP의 큐 REDIT_CARD_%_RATE_INQUIRY에 대해 프로파일은 다음과 같이 RACF에 정의됩니다.

```
RDEFINE MQQUEUE CRDP.CREDIT_CARD_%_RATE_INQUIRY
```

이 큐는 CRDP.**와 같은 일반 프로파일로는 보호할 수 없습니다.

IBM MQ는 오브젝트 이름에서 대소문자가 혼합된 문자 사용을 허용합니다. 다음을 정의하여 이런 오브젝트를 보호할 수 있습니다.

1. 적절하게 대소문자가 혼합된 RACF 클래스의 대소문자 혼합 프로파일 또는
2. 적합한 대문자의 RACF 클래스의 일반 프로파일.

대소문자가 혼합된 프로파일 및 대소문자가 혼합된 RACF 클래스를 사용하려면 239 페이지의 『z/OS 대소문자 혼용 보안으로 큐 관리자 마이그레이션』에서 설명하는 단계를 사용해야 합니다.

값이 IBM MQ에서만 제공되기 때문에 대문자로 유지되는 일부 프로파일 또는 프로파일 부분이 있습니다. 즉, 다음과 같습니다.

- 스위치 프로파일.
- 서브시스템 및 큐 공유 그룹 ID를 포함하는 모든 상위 레벨 규정자(HLQ)
- SYSTEM 오브젝트에 대한 프로파일

- 기본 오브젝트에 대한 프로파일.
- 모든 명령 프로파일이 대문자 전용이 될 수 있도록 **MQCMDS** 클래스.
- 모든 연결 프로파일이 대문자 전용이 될 수 있도록 **MQCONN** 클래스.
- **RESLEVEL** 프로파일
- 명령 자원 프로파일의 'object' 규정, 예: h1q.QUEUE.queueName. 자원 이름은 대소문자 혼합 전용입니다.
- 동적 큐 프로파일 h1q.CSQOREXX.*, h1q.CSQUTIL.*, CSQXCMD.*.
- 'CONTEXT' h1q.CONTEXT.resourcename의 일부입니다.
- h1q.ALTERNATE.USER.userid의 'ALTERNATE.USER' 부분.

예를 들어, 큐 관리자 QM01에 PAYROLL.Dept1 큐가 있고 다음을 사용 중인 경우:

- 대소문자 혼합 프로파일: IBM MQ RACF 클래스 MXQUEUE에 프로파일을 정의할 수 있습니다.

```
RDEFINE MXQUEUE MQ01.PAYROLL.Dept1
```

- 대문자 프로파일: 프로파일을 IBM MQ RACF 클래스 MQQUEUE에 정의할 수 있습니다.

```
RDEFINE MQQUEUE MQ01.PAYROLL.*
```

대소문자 혼합 프로파일을 사용하는 첫 번째 예는 자원 액세스에 대한 권한 부여에 더 세밀한 제어를 제공합니다.

z/OS 스위치 프로파일

IBM MQ에서 수행되는 보안 검사를 제어하려면 스위치 프로파일을 사용합니다. 스위치 프로파일은 IBM MQ에 특별한 의미가 있는 일반 RACF 프로파일입니다. 스위치 프로파일의 액세스 목록은 IBM MQ에서 사용되지 않습니다.

IBM MQ는 서브시스템 레벨 보안의 스위치 프로파일, 큐 공유 그룹 또는 큐 관리자 레벨 보안에 대한 스위치 프로파일 및 자원 검사 스위치 프로파일 표에 표시된 각 스위치 유형에 대한 내부 스위치를 유지보수합니다. 스위치 프로파일은 큐 공유 그룹 레벨 또는 큐 관리자 레벨 또는 둘의 조합으로 유지보수할 수 있습니다. 큐 공유 그룹 보안 스위치 프로파일의 단일 세트를 사용하여 큐 공유 그룹 내의 모든 큐 관리자에 대해 보안을 제어할 수 있습니다.

보안 스위치를 켜면 스위치에 연관된 보안 검사가 수행됩니다. 보안 스위치가 꺼지면 스위치에 연관된 보안 검사는 생략됩니다. 모든 보안 스위치는 켜지는 것이 기본값입니다.

z/OS 스위치 및 클래스

큐 관리자를 시작하거나 보안을 새로 고칠 때 IBM MQ는 다양한 RACF 클래스 상태에 따라 스위치를 설정합니다.

큐 관리자가 시작되면(또는 MQADMIN 또는 MXADMIN 클래스가 IBM MQ REFRESH SECURITY 명령에서 새로 고치는 경우) IBM MQ는 우선 RACF 상태 및 해당 클래스 상태를 검사합니다.

- 대문자 프로파일을 사용 중인 경우 MQADMIN 클래스
- 대소문자 혼합 프로파일을 사용 중인 경우 MXADMIN 클래스.

다음 조건 중 하나라도 적용되는 경우에는 서브시스템 보안 스위치를 끕니다.

- RACF는 비활성 또는 설치되지 않았습니다.
- MQADMIN 또는 MXADMIN 클래스가 정의되지 않습니다(해당 클래스는 클래스 디스크립터 테이블(CDT)에 포함되기 때문에 RACF에 대해 정의).
- MQADMIN 또는 MXADMIN 클래스가 활성화되지 않았습니다.

RACF 및 MQADMIN 또는 MXADMIN 클래스 모두 활성화된 경우 IBM MQ는 정의된 스위치 프로파일이 있는지 확인하기 위해 MQADMIN 또는 MXADMIN 클래스를 검사합니다. 우선 169 페이지의 『서브시스템 보안을 제어할 프로파일』에서 설명하는 프로파일을 검사합니다. 서브시스템 보안이 필요하지 않은 경우 IBM MQ는 내부 서브시스템 보안 스위치를 끄고 추가 검사를 수행하지 않습니다.

프로파일은 해당 IBM MQ 스위치가 켜거나 끄는지 여부를 판별합니다.

- 스위치를 끄는 경우, 해당 보안 유형은 활성화 해제됩니다.
- IBM MQ 스위치가 설정된 경우 IBM MQ 는 IBM MQ 스위치에 해당하는 보안 유형과 연관된 RACF 클래스의 상태를 확인합니다. 클래스가 설치되지 않았거나 활성화되지 않은 경우, IBM MQ 스위치가 꺼집니다. 예를 들어, 프로세스 보안 검사는 MQPROC 또는 MXPROC 클래스가 활성화되지 않은 경우 수행되지 않습니다. 활성화되지 않은 클래스는 이 RACF 데이터베이스를 사용하는 모든 큐 관리자 및 큐 공유 그룹에 대해 NO.PROCESS.CHECKS 프로파일을 정의하는 것과 동일합니다.

z/OS 스위치 작동 방법

보안 스위치를 설정하려면 NO.*를 정의하십시오. 를 사용하여 프로파일을 작성한다. 당신은 NO.*를 대체할 수 있다. YES.*를 정의하여 큐 공유 그룹 레벨의 프로파일 세트 큐 매니저에 대한 프로파일을 정의한다.

보안 스위치를 설정하려면 NO.*를 정의해야 한다. 를 사용하여 프로파일을 작성한다. NO.*의 존재 프로파일은 특정 큐 관리자에서 큐 공유 그룹 레벨 설정을 대체하도록 선택하지 않는 한, 해당 자원 유형에 대해 보안 검사가 수행되지 않음을 의미합니다. 이 프로그램은 169 페이지의 『[큐 공유 그룹 레벨 설정 대체](#)』에서 설명합니다.

큐 관리자가 큐 공유 그룹의 멤버가 아닌 경우 큐 공유 그룹 레벨을 정의하거나 프로파일을 대체할 필요가 없습니다. 그렇지만 큐 관리자가 나중에 큐 공유 그룹을 조인하는 경우 해당 프로파일을 정의해야 합니다.

각각의 NO.* IBM MQ 가 발견한 스위치 프로파일은 해당 자원 유형에 대한 검사를 해제합니다. 스위치 프로파일은 큐 관리자 시동 중에 활성화됩니다. 영향을 받는 큐 관리자가 실행 중에 스위치 프로파일을 변경하는 경우 IBM MQ REFRESH SECURITY 명령을 발행하여 IBM MQ가 변경을 인식하도록 할 수 있습니다.

스위치 프로파일은 항상 MQADMIN 또는 클래스 클래스에 정의되어야 합니다. 이를 GMQADMIN 또는 GMXADMIN 클래스에 정의하지 마십시오. 표 [서브시스템 레벨 보안에 대한 스위치 프로파일 및 자원 검사용 스위치 프로파일](#)에서는 유효한 스위치 프로파일 및 제어하는 보안 유형을 보여줍니다.

큐 공유 그룹 레벨 설정 대체

해당 그룹의 멤버인 특정 큐 관리자에 대한 큐 공유 그룹 레벨 보안 설정을 대체할 수 있습니다. 그룹의 다른 큐 관리자에서 수행되지 않는 개별 큐 관리자에서 큐 관리자 검사를 수행하려면 (qmgr-name.YES. *) 를 사용하십시오. 스위치 프로파일.

반대로, 큐 공유 그룹 내의 특정 큐 관리자에 대해 특정 검사를 수행하지 않으려면 (qmgr-name.NO. *) 를 정의하십시오. 큐 관리자의 특정 자원 유형에 대한 프로파일이며, 큐 공유 그룹에 대한 프로파일을 정의하지 않습니다. (IBM MQ 는 큐 관리자 레벨 프로파일을 찾을 수 없는 경우에만 큐 공유 그룹 레벨 프로파일을 확인합니다.)

z/OS 서브시스템 보안을 제어할 프로파일

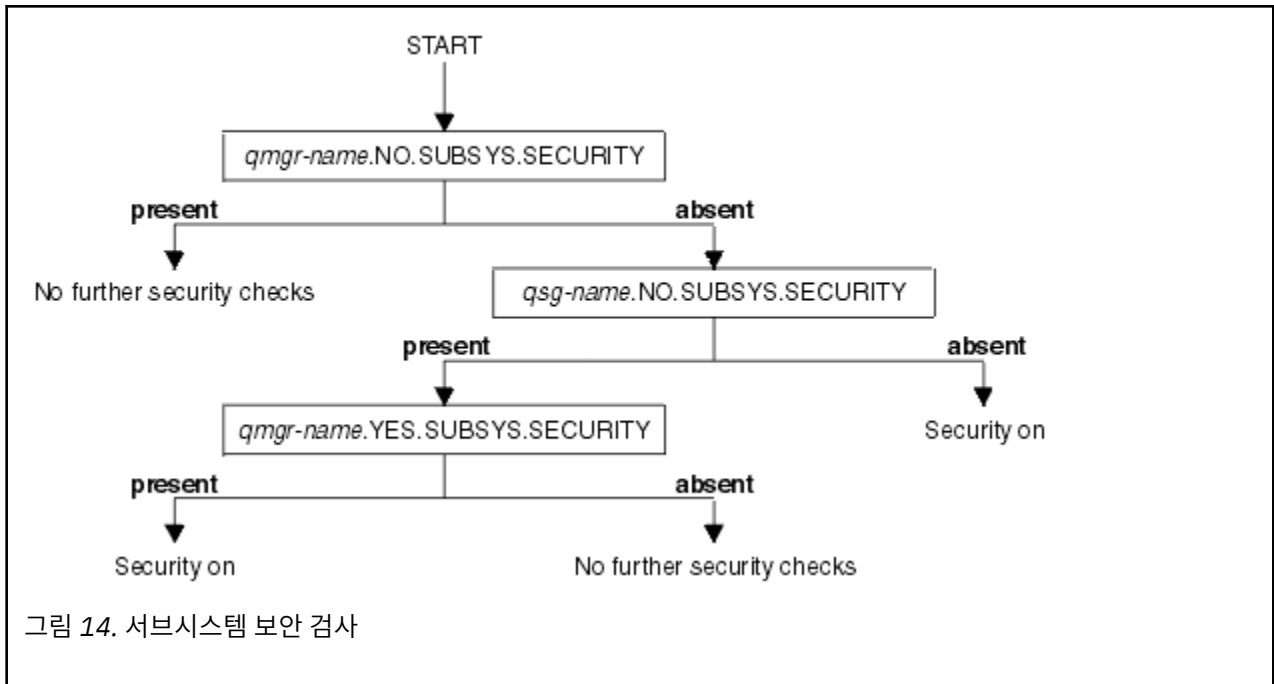
IBM MQ는 서브시스템 보안 검사가 서브시스템, 큐 관리자, 큐 공유 그룹에 대해 필요한지를 검사합니다.

IBM MQ에서 수행되는 첫 번째 보안 검사는 전체 IBM MQ 서브시스템에 대해 보안 검사가 필요한지를 판별하는데 사용됩니다. 서브시스템 보안이 필요하지 않음으로 지정하는 경우 추가 검사는 수행되지 않습니다.

다음 스위치 프로파일은 서브시스템 보안이 필요한지 여부를 판별하기 위해 검사됩니다. 170 페이지의 그림 14에서는 검사되는 순서를 보여줍니다.

스위치 프로파일 이름	제어되는 검사 또는 자원의 유형
qmgr-name.NO.SUBSYS.SECURITY	이 큐 관리자에 대한 서브시스템 보안
qsg-name.NO.SUBSYS.SECURITY	큐 공유 그룹에 대한 서브시스템 보안
qmgr-name.YES.SUBSYS.SECURITY	이 큐 관리자에 대한 서브시스템 보안 대체

큐 관리자가 큐 공유 그룹의 멤버가 아닌 경우, IBM MQ는 qmgr-name.NO.SUBSYS.SECURITY 스위치 프로파일만 검사합니다.



z/OS 큐 공유 그룹 또는 큐 관리자 레벨 보안을 제어할 프로파일

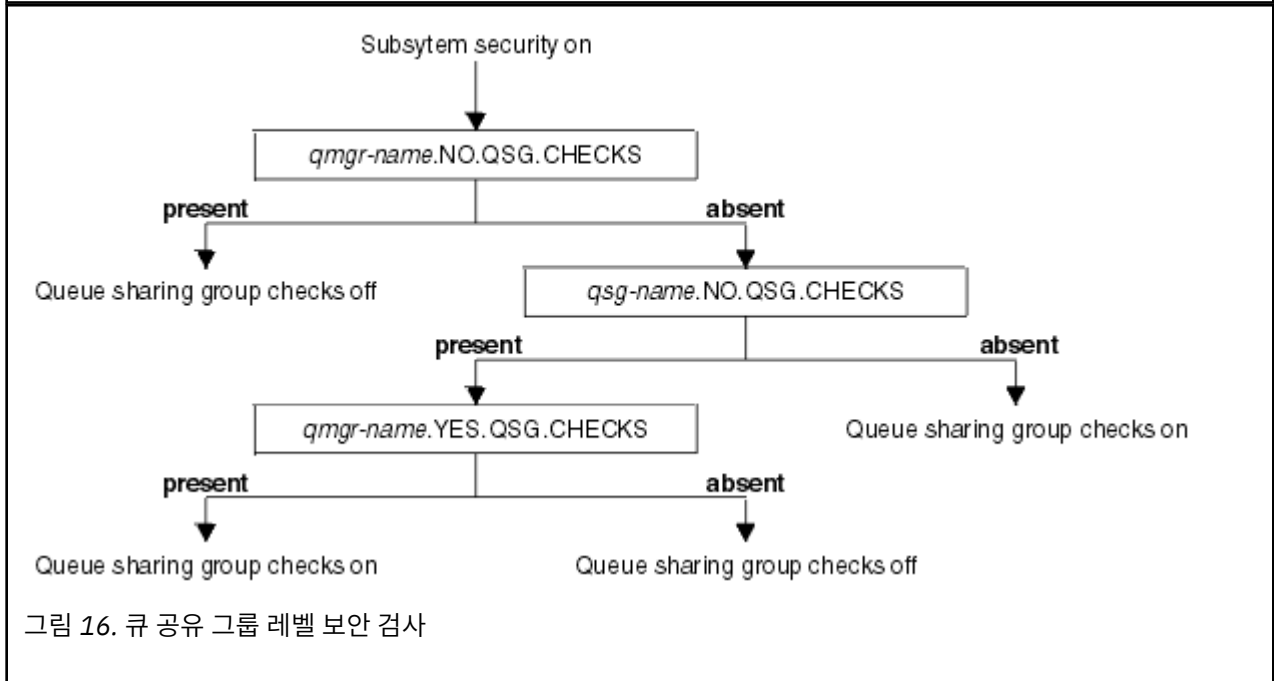
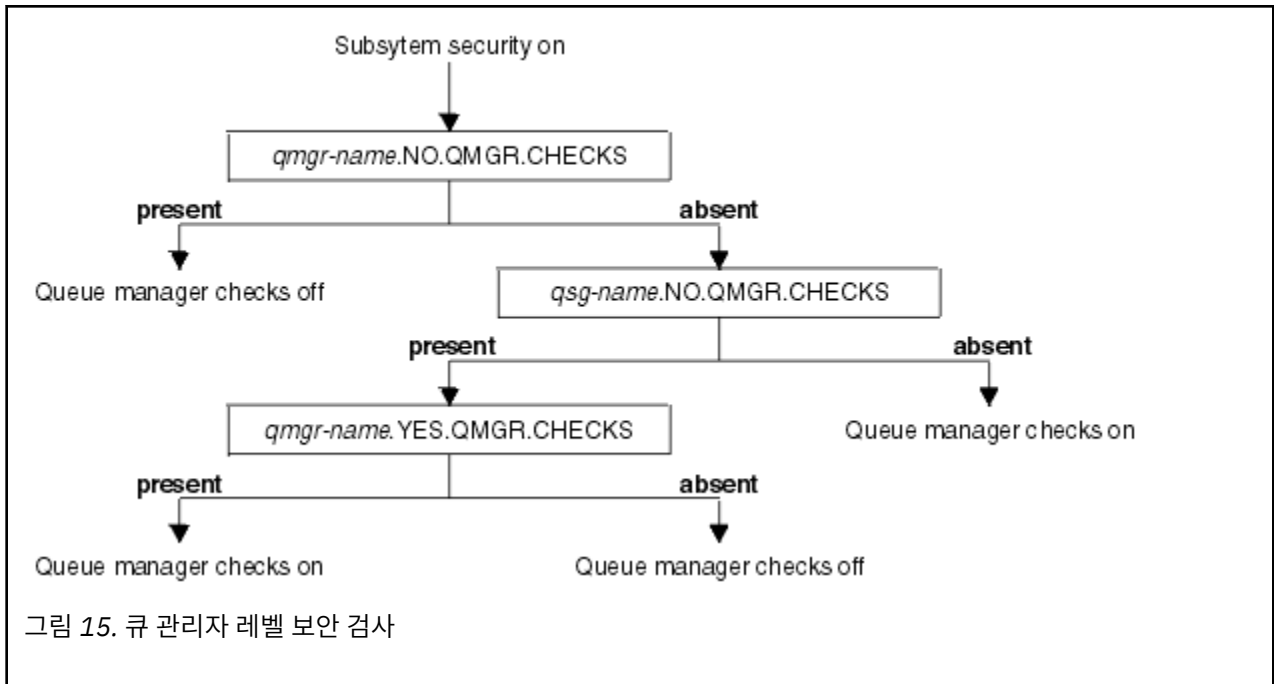
서브시스템 보안 검사가 필요한 경우, IBM MQ는 큐 공유 그룹 또는 큐 관리자 레벨에서 보안 검사가 필요한지를 검사합니다.

IBM MQ에서 보안 검사가 필요한 것으로 판별하면 검사가 큐 공유 그룹 또는 큐 관리자 레벨, 또는 둘 모두에서 필요한지를 판별합니다. 큐 관리자가 큐 공유 그룹의 구성원이 아닌 경우 이 검사는 수행되지 않습니다.

필요한 레벨을 판별하기 위해 다음 스위치 프로파일이 검사됩니다. 171 페이지의 그림 15 및 171 페이지의 그림 16에서는 검사 순서를 보여줍니다.

스위치 프로파일 이름	제어되는 검사 또는 자원의 유형
qmgr-name.NO.QMGR.CHECKS	이 큐 관리자에 대한 큐 관리자 레벨 검사 없음
qsg-name.NO.QMGR.CHECKS	이 큐 공유 그룹에 대한 큐 관리자 레벨 검사 없음
qmgr-name.YES.QMGR.CHECKS	이 큐 관리자에 대한 큐 관리자 레벨 검사 대체
qmgr-name.NO.QSG.CHECKS	이 큐 관리자에 대한 큐 공유 그룹 레벨 검사 없음
qsg-name.NO.QSG.CHECKS	이 큐 공유 그룹에 대한 큐 공유 그룹 레벨 검사 없음
qmgr-name.YES.QSG.CHECKS	이 큐 관리자에 대한 큐 공유 그룹 레벨 검사 대체

서브시스템 보안이 활성화된 경우 큐 공유 그룹 및 큐 관리자 레벨 보안 모두 끌 수는 없습니다. 끄는 경우, IBM MQ가 두 레벨 모두에서 보안 검사를 설정합니다.



z/OS 보안 스위치에 대한 올바른 결합
 특정 조합의 스위치만 유효합니다. 올바르지 않은 스위치 설정 결합을 사용하는 경우, 메시지 CSQH026I가 발행되고 보안 검사가 큐 공유 그룹 및 큐 관리자 레벨 모두에서 설정됩니다.

171 페이지의 표 26, 172 페이지의 표 27, 172 페이지의 표 28, 172 페이지의 표 29에서는 각 보안 레벨 유형에 유효한 스위치 설정 결합 세트를 보여줍니다.

표 26. 큐 관리자 레벨 보안에 대한 올바른 보안 스위치 결합
결합
qmgr-name.NO.QSG.CHECKS
qsg-name.NO.QSG.CHECKS

표 26. 큐 관리자 레벨 보안에 대한 올바른 보안 스위치 결합 (계속)

결합

qmgr-name.NO.QSG.CHECKS
 qsg-name.NO.QMGR.CHECKS
 qmgr-name.YES.QMGR.CHECKS

qsg-name.NO.QSG.CHECKS
 qsg-name.NO.QMGR.CHECKS
 qmgr-name.YES.QMGR.CHECKS

표 27. 큐 공유 그룹 레벨 보안에 대한 올바른 보안 스위치 결합

결합

qmgr-name.NO.QMGR.CHECKS

qsg-name.NO.QMGR.CHECKS

qmgr-name.NO.QMGR.CHECKS
 qsg-name.NO.QSG.CHECKS
 qmgr-name.YES.QSG.CHECKS

qsg-name.NO.QMGR.CHECKS
 qsg-name.NO.QSG.CHECKS
 qmgr-name.YES.QSG.CHECKS

표 28. 큐 관리자 및 큐 공유 그룹 레벨 보안에 대한 올바른 보안 스위치 결합

결합

qsg-name.NO.QMGR.CHECKS
 qmgr-name.YES.QMGR.CHECKS
 No QSG.* profiles defined

No QMGR.* profiles defined
 qsg-name.NO.QSG.CHECKS
 qmgr-name.YES.QSG.CHECKS

qsg-name.NO.QMGR.CHECKS
 qmgr-name.YES.QMGR.CHECKS
 qsg-name.NO.QSG.CHECKS
 qmgr-name.YES.QSG.CHECKS

어떤 스위치에 대해서도 프로파일이 정의되지 않음

표 29. 두 레벨의 검사를 전환하는 기타 올바른 보안 스위치 결합 **on.**

결합

qmgr-name.NO.QMGR.CHECKS
 qmgr-name.NO.QSG.CHECKS

표 29. 두 레벨의 검사를 전환하는 기타 올바른 보안 스위치 결합 on . (계속)
결합
qsg-name.NO.QMGR.CHECKS qsg-name.NO.QSG.CHECKS
qmgr-name.NO.QMGR.CHECKS qsg-name.NO.QSG.CHECKS
qsg-name.NO.QMGR.CHECKS qmgr-name.NO.QSG.CHECKS

z/OS 자원 레벨 검사

자원 액세스 제어에 사용되는 많은 스위치 프로파일입니다. 큐 관리자 또는 큐 공유 그룹에서 수행 중인 일부 중지 검사입니다. 이는 특정 큐 관리자 검사를 사용하는 프로파일로 대체 가능합니다.

173 페이지의 표 30에서는 IBM MQ 자원 액세스 제어에 사용되는 스위치 프로파일을 보여줍니다.

큐 관리자가 큐 공유 그룹의 일부이고 큐 관리자 및 큐 공유 그룹 보안이 활성화 상태인 경우, YES.*를 사용할 수 있습니다. 특정 큐 관리자에 대해 특별히 보안을 설정하여 큐 공유 그룹 레벨 프로파일을 대체하도록 프로파일을 전환합니다.

일부 프로파일은 큐 관리자 및 큐 공유 그룹 모두에 적용됩니다. 이는 *hlq* 문자열로 접두부가 추가되고 큐 공유 그룹 또는 큐 관리자의 이름을 대체해야 합니다(적용되는 경우). *qmgr-name*이 접두부로 표시되는 프로파일 이름은 큐 관리자 대체 프로파일입니다. 큐 관리자 이름을 대체해야 합니다.

표 30. 자원 검사 스위치 프로파일		
제어되는 자원 검사 유형	스위치 프로파일 이름	특정 큐 관리자에 대한 대체 프로파일
연결 보안	hlq.NO.CONNECT.CHECKS	qmgr-name.YES.CONNECT.CHECKS
큐 보안	hlq.NO.QUEUE.CHECKS	qmgr-name.YES.QUEUE.CHECKS
프로세스 보안	hlq.NO.PROCESS.CHECKS	qmgr-name.YES.PROCESS.CHECKS
이름 목록 보안	hlq.NO.NLIST.CHECKS	qmgr-name.YES.NLIST.CHECKS
컨텍스트 보안	hlq.NO.CONTEXT.CHECKS	qmgr-name.YES.CONTEXT.CHECKS
대체 사용자 보안	hlq.NO.ALTERNATE.USER.CHECKS	qmgr-name.YES.ALTERNATE.USER.CHECKS
명령 보안	hlq.NO.CMD.CHECKS	qmgr-name.YES.CMD.CHECKS
명령 자원 보안	hlq.NO.CMD.RESC.CHECKS	qmgr-name.YES.CMD.RESC.CHECKS
토픽 보안	hlq.NO.TOPIC.CHECKS	qmgr-name.YES.TOPIC.CHECKS
참고: 일반 스위치 프로파일 (예: hlq.NO) * * IBM MQ 에서 무시됩니다.		

예를 들어, 큐 공유 그룹 QSG3의 멤버이지만 그룹의 다른 큐 관리자에 대해서는 프로세스 보안 검사를 수행하지 않으려는 큐 관리자 QM01에서 프로세스 보안 검사를 수행하려는 경우, 다음 스위치 프로파일을 정의하십시오.

```
QSG3.NO.PROCESS.CHECKS
QM01.YES.PROCESS.CHECKS
```

큐 공유 그룹에서 QM02를 제외한 모든 큐 관리자에서 큐 보안 검사를 수행하려는 경우, 다음 스위치 프로파일을 정의하십시오.

(검사는 정의된 프로파일이 없는 경우 자동으로 사용되기 때문에 큐 공유 그룹에 대해 프로파일을 정의할 필요가 없습니다.)

z/OS 스위치 정의 예

다른 IBM MQ 서브시스템에는 다른 보안 요구사항이 있으며 이는 다른 스위치 프로파일을 사용하여 구현 가능합니다.

4개의 IBM MQ 서브시스템이 정의되었습니다.

- MQP1(프로덕션 시스템)
- MQP2(프로덕션 시스템)
- MQD1(개발 시스템)
- MQT1(테스트 시스템)

4개 큐 관리자 모두 큐 공유 그룹 GS01의 멤버입니다. 모든 IBM MQ RACF 클래스가 정의되어 활성화되었습니다.

이 서브시스템에는 다른 보안 요구사항이 있습니다.

- 프로덕션 시스템의 경우, 전체 IBM MQ 보안 검사가 두 시스템 모두의 큐 공유 그룹 레벨에서 활성화되어야 합니다.

이는 다음 프로파일을 지정하여 수행합니다.

```
RDEFINE MQADMIN QS01.NO.QMGR.CHECKS
```

이는 큐 공유 그룹의 모든 큐 관리자에 대해 큐 공유 그룹 레벨 검사를 설정합니다. 이 시스템에서 대해서는 모두를 검사하려고 하기 때문에 프로덕션 큐 관리자에 대해 다른 어떤 스위치 프로파일도 정의할 필요가 없습니다.

- 테스트 큐 관리자 MQT1에도 전체 보안 검사가 필요합니다. 하지만 이를 나중에 변경할 수 있기 때문에 보안은 큐 관리자 레벨에 정의되어 다른 큐 공유 그룹 멤버에 영향을 주지 않고도 이 큐 관리자에 대한 보안 설정을 변경할 수 있습니다.

이는 MQT1에 대해 다음과 같이 NO.QSG.CHECKS 프로파일을 정의하여 수행합니다.

```
RDEFINE MQADMIN MQT1.NO.QSG.CHECKS
```

- 개발 큐 관리자 MQD1은 나머지 큐 공유 그룹과는 다른 보안 요구사항이 있습니다. 연결 및 큐 보안만 활성화되어야 합니다.

이는 이 큐 관리자에 대해 MQD1.YES.QMGR.CHECKS 프로파일을 정의하고 다음 프로파일을 정의하고 검사할 필요가 없는 자원에 대한 보안 검사를 꺼서 수행합니다.

```
RDEFINE MQADMIN MQD1.NO.CMD.CHECKS
RDEFINE MQADMIN MQD1.NO.CMD.RESC.CHECKS
RDEFINE MQADMIN MQD1.NO.PROCESS.CHECKS
RDEFINE MQADMIN MQD1.NO.NLIST.CHECKS
RDEFINE MQADMIN MQD1.NO.CONTEXT.CHECKS
RDEFINE MQADMIN MQD1.NO.ALTERNATE.USER.CHECKS
```

큐 관리자가 활성화되면 DISPLAY SECURITY MQSC 명령을 발행하여 현재 보안 설정을 표시할 수 있습니다.

큐 관리자가 실행 중인 경우 적절한 스위치 프로파일을 MQADMIN 클래스에 정의하거나 삭제하여 스위치 설정을 변경할 수도 있습니다. 스위치 설정에 대한 변경을 활성화하려면 MQADMIN 클래스에 대해 REFRESH SECURITY 명령을 발행해야 합니다.

DISPLAY SECURITY 및 REFRESH SECURITY 명령 사용에 대한 자세한 내용은 [223 페이지의 『z/OS에서 큐 관리자 보안 새로 고치기』](#)의 내용을 참조하십시오.

z/OS IBM MQ 자원에 대한 액세스 제어에 사용되는 프로파일

You must define RACF profiles to control access to IBM MQ resources, in addition to the switch profiles that might have been defined. 이 주제 콜렉션에는 다른 유형의 IBM MQ 자원에 대한 RACF 프로파일에 대한 정보가 있습니다.

특정 보안 검사에 대해 정의된 자원 프로파일이 없고 사용자가 해당 검사 수행에 사용되는 요청을 발행하는 경우, IBM MQ는 액세스를 거부합니다. 비활성화된 임의 보안 스위치에 연관된 보안 유형에 대해 프로파일을 정의할 필요가 없습니다.

z/OS 연결 보안을 위한 프로파일

연결 보안이 활성화된 경우 MQCONN 클래스에 프로파일을 정의하고 필요한 그룹이나 사용자 ID에 해당 프로파일에 대한 액세스를 허용하여 IBM MQ에 연결할 수 있도록 해야 합니다.

연결하려면 사용자에게 해당 프로파일에 대한 RACF READ 액세스를 부여해야 합니다. (큐 관리자 레벨 프로파일 이 없고 큐 관리자가 큐 공유 그룹의 멤버인 경우, 검사는 큐 공유 그룹 레벨 프로파일에 대해 수행되도록 보안이 설정된 경우 그렇게 수행됩니다.)

큐 관리자 이름으로 규정된 연결 프로파일은 특정 큐 관리자에 대한 액세스를 제어하고 이 프로파일에 대한 액세스가 부여된 사용자는 해당 큐 관리자에 연결할 수 있습니다. 큐 공유 그룹 이름으로 규정된 연결 프로파일은 해당 연결 유형에 대한 큐 공유 그룹 내의 모든 큐 관리자에 대한 액세스를 제어합니다. 예를 들어, QS01.BATCH에 액세스하는 사용자는 큐 관리자 레벨 프로파일 이 정의되지 않은 큐 공유 그룹 GQ01의 모든 큐 관리자에 배치 연결을 사용할 수 있습니다.

참고:

1. 다른 보안 요청에 대해 검사되는 사용자 ID 정보는 213 페이지의 『z/OS의 보안 검사를 위한 사용자 ID』의 내용을 참조하십시오.
2. 자원 레벨 보안(RESLEVEL) 검사는 연결 시에도 수행됩니다. 자세한 내용은 207 페이지의 『RESLEVEL 보안 프로파일』의 내용을 참조하십시오.

IBM MQ 보안은 다음과 같은 다른 유형의 연결을 인식합니다.

- 배치(및 배치 유형) 연결에는 다음이 포함됩니다.
 - z/OS 배치 작업
 - TSO 애플리케이션
 - USS 사인온
 - Db2 스토어드 프로시저
- CICS 연결
- 제어 및 애플리케이션 처리 영역에서의 IMS 연결
- IBM MQ 채널 시작기

z/OS 배치 연결에 대한 연결 보안 프로파일

배치 유형 연결 검사 프로파일은 큐 관리자 또는 큐 공유 그룹 이름과 그 뒤에 BATCH 단어로 구성됩니다. 연결 주소 공간에 연관된 사용자 ID에 연결 프로파일에 대한 READ 액세스를 부여하십시오.

배치 및 배치 유형 연결 검사 프로파일은 다음 양식을 사용합니다.

```
h1q.BATCH
```

여기서 h1q는 qmgr-name(큐 관리자 이름) 또는 qsg-name(큐 공유 그룹 이름)입니다. 큐 관리자와 큐 공유 그룹 레벨 보안을 모두 사용하는 경우 IBM MQ는 큐 관리자 이름이 접두부로 추가된 프로파일을 검사합니다. 찾을 수 없는 경우 큐 공유 그룹 이름의 접두부가 추가된 프로파일을 검색합니다. 두 프로파일 모두 찾기에 실패하는 연결 요청이 실패합니다.

배치 또는 배치 유형 연결 요청에 대해 연결 주소 공간에 연관된 사용자 ID가 연결 프로파일에 액세스하도록 허용해야 합니다. 예를 들어, 다음 RACF 명령을 사용하면 CONNTQM1 그룹의 사용자가 큐 관리자 TQM1에 연결할 수 있습니다. 해당 사용자 ID는 모든 배치 또는 배치 유형 연결 사용이 허용됩니다.

```
RDEFINE MQCONN TQM1.BATCH UACC(NONE)
PERMIT TQM1.BATCH CLASS(MQCONN) ID(CONNTQM1) ACCESS(READ)
```

z/OS 로컬에서 바인딩된 애플리케이션 **CHKKLOCL** 사용

CHKKLOCL은 BATCH 연결을 통해서 작성된 연결에만 적용되고 CICS 또는 IMS에서 작성된 연결에는 적용되지 않습니다. 채널 시작기를 통해 작성된 연결은 **CHKKCLNT**에 의해 제어됩니다.

개요

z/OS 큐 관리자를 로컬로 바인딩된 애플리케이션의 전체가 아닌 일부에 대해 사용자 ID 및 비밀번호 검사를 지시하도록 구성하고 싶은 경우에는 다음 몇몇 추가 구성을 수행해야 합니다.

이에 대한 이유는 **CHKKLOCL(REQUIRED)**이 구성된 후에는 MQCONN API 호출을 사용하는 레거시 배치 애플리케이션은 더 이상 큐 관리자에 연결할 수 없습니다.

z/OS의 경우에만, 주소 공간의 연결 보안을 기반으로 하는 보다 세분화된 메커니즘을 특별히 정의된 사용자 ID에 대해 글로벌 **CHKKLOCL(REQUIRED)** 구성을 **CHKKLOCL(OPTIONAL)**에 다운로드하는 데 사용할 수 있습니다. 사용된 메커니즘은 다음 텍스트에 예와 함께 설명되어 있습니다.

CHKKLOCL(REQUIRED)에서 EVERYONE보다 더 많은 세부성을 허용하기 위해 주소 공간을 MQCONN 클래스의 h1q.batch 연결 프로파일에 연결하는 것과 연관된 사용자 ID의 액세스 레벨을 수정하는 것과 같은 방법으로 **CHKKLOCL**을 수정하십시오.

주소 공간 사용자 ID에 연결하기 위해 필요한 최소한인 READ 액세스만 있는 경우에는, **CHKKLOCL** 구성이 작성된 대로 적용됩니다.

주소 공간 사용자 ID에 UPDATE 액세스(또는 이상)가 있으면 **CHKKLOCL** 구성은 **OPTIONAL** 모드에서 작동합니다. 즉, 사용자 ID 및 비밀번호를 제공할 필요는 없지만 제공하는 경우에는 사용자 ID와 비밀번호가 올바른 쌍이어야 합니다.

z/OS 큐 관리자에 이미 구성된 연결 보안

z/OS 큐 관리자에 이미 연결 보안이 구성되어 있고 **CHKKLOCL(REQUIRED)**이 다른 애플리케이션이 아닌 WAS 로컬 바인딩 애플리케이션에만 적용되기를 원하는 경우에는 다음 단계를 수행하십시오.

1. **CHKKLOCL(OPTIONAL)**을 구성으로서 시작하십시오. 즉 제공된 모든 사용자 ID 및 비밀번호가 검증을 위해 검사되지만 명령하지는 않음을 의미합니다.
2. 다음 명령을 실행하여 연결 보안 프로파일에 대한 액세스가 있는 모든 사용자를 나열하십시오.

```
RLIST MQCONN MQ23.BATCH AUTHUSER
```

예를 들어, 이 명령은 다음을 표시합니다.

CLASS	NAME		
MQCONN	MQ23.BATCH		
USER	ACCESS	ACCESS	COUNT
JOHNDOE	READ	000009	
JDOE1	READ	000003	
WASUSER	READ	000000	

3. READ 액세스가 있는 것으로 나열되는 각 사용자 ID의 경우 액세스를 변경하십시오.

```
UPDATE:- PERMIT MQ23.BATCH CLASS(MQCONN) ID(JOHNDOE) ACCESS(UPDATE)
```

4. IBM MQ 구성을 **CHKLOCL**(*REQUIRED*)로 변경하십시오.

MQ23.BATCH에 대한 UPDATE 액세스와 현재 설정의 결합은 **CHKLOCL**(*OPTIONAL*)을 사용 중임을 의미합니다.

5. 이제 해당 영역에서 나오는 모든 연결이 사용자 ID 및 비밀번호를 제공할 수 있도록 **CHKLOCL**(*REQUIRED*) 동작을 하나의 특정 사용자 ID(예: WASUSER)에 적용하십시오.

다음 명령을 실행하여 이전에 작성한 변경사항을 전환하여 이를 수행하십시오.

```
PERMIT MQ23.BATCH CLASS(MQCONN) ID(WASUSER) ACCESS(READ)
```

z/OS 큐 관리자에 구성되지 않은 연결 보안

이 상황에서, 다음을 수행해야 합니다.

1. 다음 명령을 실행하여 MQCONN 클래스에서 h1q.BATCH에 대한 연결 프로파일을 작성하십시오.

```
RDEFINE MQCONN MQ23.BATCH UACC(NONE)
```

2. 이 프로파일에 대한 UPDATE 액세스를 가질 수 있도록 배치 연결을 작성한 모든 사용자 ID에 큐 관리자에 대한 권한을 부여하십시오. 이를 수행하면 연결 시에 사용자 ID와 비밀번호의 **CHKLOCL**(*REQUIRED*) 요구사항이 무시됩니다.

다음 명령을 실행하여 이를 수행하십시오.

```
PERMIT MQ23.BATCH CLASS(MQCONN) ID(JOHNDOE) ACCESS(UPDATE)
```

여기에는 사용자 ID가 포함됩니다.

a. CSQUTIL, ISPF 패널 및 기타 로컬로 바인드된 도구에 사용됩니다.

b. 큐 관리자에 연결과 같은 배치와 연관됩니다. 예를 들어, Advanced Message Security, IBM Integration Bus, Db2 스토어드 프로시저, USS 및 TSO 사용자 및 Java 애플리케이션을 고려하십시오.

3. 다음 명령을 실행하여 큐 관리자의 스위치 프로파일을 삭제하십시오.

```
h1q.NO.CONNECT.CHECKS
```

4. 이제 해당 영역에서 나오는 모든 연결이 사용자 ID 및 비밀번호를 제공할 수 있도록 **CHKLOCL**(*REQUIRED*) 동작을 하나의 특정 사용자 ID(예: WASUSER)에 적용하십시오.

다음 명령을 실행하여 이전에 작성한 변경사항을 전환하여 이를 수행하십시오.

```
PERMIT MQ23.BATCH CLASS(MQCONN) ID(WASUSER) ACCESS(READ)
```

z/OS CICS 연결에 대한 연결 보안 프로파일

CICS 연결 검사를 위한 프로파일은 뒤에 CICS 단어가 오는 큐 관리자 또는 큐 공유 그룹 이름으로 구성됩니다. CICS 주소 공간에 연관된 사용자 ID에 연결 프로파일에 대한 READ 액세스를 부여하십시오.

CICS 연결 검사 프로파일은 다음 양식을 사용합니다.

```
h1q.CICS
```

여기서 h1q는 qmgr-name(큐 관리자 이름) 또는 qsg-name(큐 공유 그룹 이름)입니다. 큐 관리자와 큐 공유 그룹 레벨 보안을 모두 사용하는 경우 IBM MQ는 큐 관리자 이름이 접두부로 추가된 프로파일을 검사합니다. 찾을 수 없는 경우 큐 공유 그룹 이름의 접두부가 추가된 프로파일을 검색합니다. 두 프로파일 모두 찾기에 실패하는 경우, 연결 요청이 실패합니다.

CICS의 연결 요청에 대해 CICS 주소 공간 사용자 ID만 연결 프로파일에 액세스하도록 허용해야 합니다.

예를 들면, 다음 RACF 명령은 CICS 주소 공간 사용자 ID KCBCICS가 큐 관리자 TQM1에 연결될 수 있게 허용합니다.

```
RDEFINE MQCONN TQM1.CICS UACC(NONE)
PERMIT TQM1.CICS CLASS(MQCONN) ID(KCBCICS) ACCESS(READ)
```

Z/OS IMS 연결에 대한 연결 보안 프로파일

IMS 연결 검사를 위한 프로파일은 뒤에 *IMS* 단어가 오는 큐 관리자 또는 큐 공유 그룹 이름으로 구성됩니다. IMS 제어 및 종속 영역 사용자 ID에 연결 프로파일에 대한 READ 액세스를 부여하십시오.

IMS 연결 검사 프로파일은 다음 양식을 사용합니다.

```
hlq.IMS
```

여기서 *hlq*는 *qmgr-name*(큐 관리자 이름) 또는 *qsg-name*(큐 공유 그룹 이름)입니다. 큐 관리자와 큐 공유 그룹 레벨 보안을 모두 사용하는 경우 IBM MQ는 큐 관리자 이름이 접두부로 추가된 프로파일을 검사합니다. 찾을 수 없는 경우 큐 공유 그룹 이름의 접두부가 추가된 프로파일을 검색합니다. 두 프로파일 모두 찾기에 실패하는 경우, 연결 요청이 실패합니다.

IMS의 연결 요청에 대해 IMS 제어 및 종속 영역 사용자 ID에 연결 프로파일 액세스 권한을 부여하십시오.

예를 들어, 다음 RACF 명령은 다음을 허용합니다.

- 큐 관리자 TQM1에 연결하기 위한 IMS 영역 사용자 ID, IMSREG.
- BMPGRP 그룹의 사용자는 BMP 작업을 제출할 수 있습니다.

```
RDEFINE MQCONN TQM1.IMS UACC(NONE)
PERMIT TQM1.IMS CLASS(MQCONN) ID(IMSREG,BMPGRP) ACCESS(READ)
```

Z/OS 채널 시작기에 대한 연결 보안 프로파일

채널 시작기에서의 연결 검사를 위한 프로파일은 큐 관리자 또는 큐 공유 그룹 이름과 그 뒤에 오는 *CHIN*으로 구성됩니다. 채널 시작기로 시작된 태스크 주소 공간에서 사용되는 사용자 ID에 연결 프로파일에 대한 READ 액세스를 부여하십시오.

채널 시작기에서 연결을 검사하는 프로파일은 다음 양식을 사용합니다.

```
hlq.CHIN
```

여기서 *hlq*는 *qmgr-name*(큐 관리자 이름) 또는 *qsg-name*(큐 공유 그룹 이름)입니다. 큐 관리자와 큐 공유 그룹 레벨 보안을 모두 사용하는 경우 IBM MQ는 큐 관리자 이름이 접두부로 추가된 프로파일을 검사합니다. 찾을 수 없는 경우 큐 공유 그룹 이름의 접두부가 추가된 프로파일을 검색합니다. 두 프로파일 모두 찾기에 실패하는 경우, 연결 요청이 실패합니다.

채널 시작기의 연결 요청에 대해, 채널 시작기로 시작된 태스크 주소 공간에서 사용되는 사용자 ID에 대해 연결 프로파일 액세스를 정의하십시오.

예를 들어, 다음 RACF 명령을 사용하면 사용자 ID DQCTRL로 실행 중인 채널 시작기 주소 공간이 큐 관리자 TQM1에 연결 가능합니다.

```
RDEFINE MQCONN TQM1.CHIN UACC(NONE)
PERMIT TQM1.CHIN CLASS(MQCONN) ID(DQCTRL) ACCESS(READ)
```

z/OS 큐 보안을 위한 프로파일

큐 보안이 활성화된 경우 해당 클래스에 프로파일을 정의하고 필요한 그룹이나 사용자 ID에 해당 프로파일에 대한 액세스를 허용해야 합니다. 큐 보안 프로파일은 큐 관리자 또는 큐 공유 그룹 및 열리는 큐에 따라 지정됩니다.

큐 보안이 활성화된 경우 다음을 수행해야 합니다.

- 대문자로 된 프로파일을 사용하는 경우 **MQQUEUE** 또는 **GMQUEUE** 클래스에 프로파일을 정의하십시오.
- 대소문자 혼용 프로파일을 사용하는 경우 **MXQUEUE** 또는 **GMXQUEUE** 클래스에 프로파일을 정의하십시오.
- 필요한 그룹이나 사용자 ID에 해당 프로파일에 대한 액세스를 허용하여 큐를 사용하는 IBM MQ API 요청을 발행할 수 있도록 해야 합니다.

큐 보안을 위한 프로파일은 다음 양식을 사용합니다.

```
hlq.queueName
```

여기서 hlq는 qmgr-name(큐 관리자 이름) 또는 qsg-name(큐 공유 그룹 이름) 중 하나일 수 있고 queueName은 MQOPEN 또는 MQPUT1 호출에서 오브젝트 디스크립터에 지정된 대로 열고 있는 큐 이름입니다.

큐 관리자 이름이 접두부로 추가된 프로파일은 해당 큐 관리자에서 단일 큐에 대한 액세스를 제어합니다. 큐 공유 그룹 이름의 접두부가 추가된 프로파일은 큐 공유 그룹 내의 모든 큐 관리자에서 해당 이름의 하나 이상의 큐에 대한 액세스 또는 그룹 내의 임의의 큐 관리자의 공유 큐에 대한 액세스를 제어합니다. 이 액세스는 해당 큐 관리자에서 이 큐에 대해 큐 관리자 레벨 프로파일을 정의하여 개별 큐 관리자에서 대체 가능합니다.

큐 관리자가 큐 공유 그룹의 멤버이고 큐 관리자와 큐 공유 그룹 레벨 보안을 모두 사용하는 경우 IBM MQ는 큐 관리자 이름이 접두부로 추가된 프로파일을 먼저 검사합니다. 찾을 수 없는 경우 큐 공유 그룹 이름의 접두부가 추가된 프로파일을 검색합니다.

공유 큐를 사용 중인 경우 큐 공유 그룹 레벨 보안을 사용하도록 권장됩니다.

큐 이름이 알리어스 또는 모델 큐 **z/OS**의 이름인 경우 큐 보안이 작동하는 방법에 대한 자세한 내용은 181 페이지의 『알리어스 큐에 대한 고려사항』 및 182 페이지의 『모델 큐에 대한 고려사항』의 내용을 참조하십시오.

큐를 여는 데 필요한 RACF 액세스는 지정된 MQOPEN 또는 MQPUT1 옵션에 따라 다릅니다. 둘 이상의 MQOO_* 및 MQPMO_* 옵션이 코드화되면 큐 보안 검사가 필요한 가장 높은 RACF 권한에 대해 수행됩니다.

표 31. MQOPEN 또는 MQPUT1 호출을 사용하는 큐 보안에 대한 액세스 레벨	
MQOPEN 또는 MQPUT1 옵션	hlq.queueName에 필요한 RACF 액세스 레벨
MQOO_BROWSE	READ
MQOO_INQUIRE	READ
MQOO_BIND_*	UPDATE
MQOO_INPUT_*	UPDATE
MQOO_OUTPUT 또는 MQPUT1	UPDATE
MQOO_PASS_ALL_CONTEXT MQPMO_PASS_ALL_CONTEXT	UPDATE
MQOO_PASS_IDENTITY_CONTEXT MQPMO_PASS_IDENTITY_CONTEXT	UPDATE
MQOO_SAVE_ALL_CONTEXT	UPDATE

표 31. MQOPEN 또는 MQPUT1 호출을 사용하는 큐 보안에 대한 액세스 레벨 (계속)	
MQOPEN 또는 MQPUT1 옵션	hlq.queueName에 필요한 RACF 액세스 레벨
MQOO_SET_IDENTITY_CONTEXT MQPMO_SET_IDENTITY_CONTEXT	UPDATE
MQOO_SET_ALL_CONTEXT MQPMO_SET_ALL_CONTEXT	UPDATE
MQOO_SET	ALTER

예를 들어, IBM MQ 큐 관리자 QM77에서 RACF 그룹 PAYGRP의 모든 사용자 ID는 'PAY'로 시작되는 이름의 모든 큐에서 메시지를 가져오거나 여기에 메시지를 넣기 위해 액세스가 부여됩니다. 다음 RACF 명령으로 이를 수행할 수 있습니다.

```
RDEFINE MQQUEUE QM77.PAY.** UACC(NONE)
PERMIT QM77.PAY.** CLASS(MQQUEUE) ID(PAYGRP) ACCESS(UPDATE)
```

또한, PAYGRP 그룹의 모든 사용자 ID는 PAY 이름 지정 규칙을 사용하지 않는 큐에 메시지를 넣을 권한이 있어야 합니다. 예를 들면, 다음과 같습니다.

```
REQUEST_QUEUE_FOR_PAYROLL
SALARY.INCREASE.SERVER
REPLIES.FROM.SALARY.MODEL
```


GMQQUEUE 클래스에서 해당 큐에 대한 프로파일을 정의하고 다음과 같이 해당 클래스에 액세스를 부여하여 이를 수행할 수 있습니다.

```
RDEFINE GMQQUEUE PAYROLL.EXTRAS UACC(NONE)
ADDMEM(QM77.REQUEST_QUEUE_FOR_PAYROLL,
        QM77.SALARY.INCREASE.SERVER,
        QM77.REPLIES.FROM.SALARY.MODEL)
PERMIT PAYROLL.EXTRAS CLASS(GMQQUEUE) ID(PAYGRP) ACCESS(UPDATE)
```

참고:

1. 애플리케이션이 큐 보안 프로파일에 대해 가지는 RACF 액세스 레벨이 변경되면, 변경사항은 해당 큐에 대해 확보된(즉, 새 MQOPEN) 모든 새 오브젝트 핸들에 대해서만 적용됩니다. 해당 핸들은 변경이 큐에 대해 기존 액세스를 유지하는 시점에 이미 있습니다. 애플리케이션이 기존 액세스 레벨이 아니라 큐에 대해 변경된 액세스 레벨을 사용해야 하는 경우, 변경이 필요한 각 오브젝트 핸들에 대해 큐를 닫은 후 다시 열어야 합니다.
2. 예에서 큐 관리자 이름 QM77은 큐 공유 그룹의 이름일 수도 있습니다.

지정된 열기 옵션 및 활성화된 보안 유형에 따라 다른 보안 검사 유형은 큐를 열 때 발생할 수도 있습니다.

 194 페이지의 『컨텍스트 보안을 위한 프로파일』 및 192 페이지의 『대체 사용자 보안을 위한 프로파일』의 내용도 참조하십시오. 큐, 컨텍스트 및 대체 사용자 보안이 모두 활성화된 경우 필요한 열기 옵션 및 보안 권한을 보여주는 요약 테이블은 186 페이지의 표 36의 내용을 참조하십시오.

발행/구독을 사용 중인 경우에는 다음을 고려해야 합니다. MQSUB 요청이 처리될 때 보안 검사는 요청을 작성 중인 사용자 ID에 대상 IBM MQ 큐에 메시지를 넣기 위해 필요한 액세스 권한이 있는지 및 IBM MQ 토픽 구독에 필요한 액세스 권한이 있는지도 확인하기 위해 수행됩니다.

표 32. MQSUB 호출을 사용하는 큐 보안의 액세스 레벨	
MQSUB 옵션	hlq.queueename에 필요한 RACF 액세스 레벨
MQSO_ALTER, MQSO_CREATE, MQSO_RESUME	UPDATE

참고:

1. hlq.queueename은 발행물의 목적지 큐입니다. 이 큐가 관리 큐인 경우 관리 큐 및 작성되는 동적 큐에 사용되는 적합한 모델 큐에 대한 액세스가 필요합니다.
2. 구독을 작성 중인 사용자와 목적지 큐에서 발행물을 검색하는 사용자를 구분하려는 경우, 이와 같은 기술을 MQSUB API 호출에서 제공하는 목적지 큐에 사용할 수 있습니다.

z/OS 알리어스 큐에 대한 고려사항

알리어스 큐에 대해 MQOPEN 또는 MQPUT1 호출을 발행하는 경우 IBM MQ는 호출에서 오브젝트 디스크립터 (MQOD)에 지정되는 큐 이름에 대해 자원 검사를 수행합니다. 대상 큐 이름에 대해 사용자의 액세스가 허용되는지는 검사하지 않습니다.

예를 들어, PAYROLL.REQUEST 이름의 알리어스 큐는 PAY.REQUEST의 대상 큐로 해석됩니다. 큐 보안이 활성화 되면 큐 PAYROLL.REQUEST에만 액세스하도록 권한 부여되어야 합니다. 큐 PAY.REQUEST에 액세스하도록 권한 부여되었는지 확인하는 검사는 수행되지 않습니다.

z/OS 알리어스 큐를 사용하여 MQGET 및 MQPUT 요청 구분

하나의 액세스 레벨에서 사용할 수 있는 MQI 호출 범위는 MQPUT 호출 또는 MQGET 호출만 허용되도록 큐에 대한 액세스를 제한하려는 경우 문제가 될 수 있습니다. 큐는 해당 큐로 해결되는 다음 두 개의 알리어스를 정의하여 보호할 수 있습니다. 하나는 애플리케이션이 큐에서 메시지를 가져오도록 허용하는 알리어스이고 다른 하나는 애플리케이션이 큐에 메시지를 넣도록 하는 알리어스입니다.

다음 텍스트는 IBM MQ에 대해 큐를 정의하는 방법에 대한 예를 보여줍니다.

```
DEFINE QLOCAL(MUST_USE_ALIAS_TO_ACCESS) GET(ENABLED)
PUT(ENABLED)

DEFINE QALIAS(USE_THIS_ONE_FOR_GETS) GET(ENABLED)
PUT(DISABLED) TARGET(MUST_USE_ALIAS_TO_ACCESS)

DEFINE QALIAS(USE_THIS_ONE_FOR_PUTS) GET(DISABLED)
PUT(ENABLED) TARGET(MUST_USE_ALIAS_TO_ACCESS)
```

다음 RACF 정의도 작성해야 합니다.

```
RDEFINE MQQUEUE hlq.MUST_USE_ALIAS_TO_ACCESS UACC(NONE)
RDEFINE MQQUEUE hlq.USE_THIS_ONE_FOR_GETS UACC(NONE)
RDEFINE MQQUEUE hlq.USE_THIS_ONE_FOR_PUTS UACC(NONE)
```

그런 다음 큐 hlq.MUST_USE_ALIAS_TO_ACCESS에 대해 액세스 권한이 있는 사용자가 없도록 하고 적절한 사용자나 그룹 액세스를 알리어스에 부여하십시오. 다음 RACF 명령으로 이를 수행할 수 있습니다.

```
PERMIT hlq.USE_THIS_ONE_FOR_GETS CLASS(MQQUEUE)
ID(GETUSER,GETGRP) ACCESS(UPDATE)
PERMIT hlq.USE_THIS_ONE_FOR_PUTS CLASS(MQQUEUE)
ID(PUTUSER,PUTGRP) ACCESS(UPDATE)
```

즉, 사용자 ID GETUSER 및 GETGRP 그룹의 사용자 ID만 알리어스 큐 USE_THIS_ONE_FOR_GETS를 통해 MUST_USE_ALIAS_TO_ACCESS에서 메시지를 가져오도록 허용됩니다. 사용자 ID PUTUSER 및 PUTGRP 그룹의 사용자 ID만 알리어스 큐 USE_THIS_ONE_FOR_PUTS를 통해 메시지를 넣도록 허용됩니다.

참고:

1. 이런 기술을 사용하려면 애플리케이션 개발자에게 통보하여 개발자가 해당 프로그램을 적절하게 설계하도록 해야 합니다.

- 구독을 작성하는 사용자와 목적지 큐에서 발행물을 '가져오는' 사용자를 구별하려는 경우 MQSUB API 요청에 제공하는 목적지 큐에 대해 이와 같은 기술을 사용할 수 있습니다.

z/OS 모델 큐에 대한 고려사항

모델 큐를 열려면 모델 큐 자체와 해결하려는 동적 큐 모두를 열 수 있어야 합니다. IBM MQ 유틸리티에서 사용하는 동적 큐를 포함하여 동적 큐에 대한 일반 RACF 프로파일을 정의하십시오.

모델 큐를 열 때 IBM MQ 보안은 두 개의 큐 보안 검사를 작성합니다.

- 모델 큐에 액세스할 권한이 있습니까?
- 모델 큐가 해결되는 동적 큐에 액세스할 권한이 있습니까?

동적 큐 이름에 후미 별표(*) 문자가 있는 경우, 이 *는 IBM MQ에서 생성되는 문자열로 바뀌어서 고유한 이름의 동적 큐가 작성됩니다. 그렇지만 이 생성된 문자열을 포함하는 전체 이름이 권한 검사에 사용되기 때문에 해당 큐에 대한 일반 프로파일을 정의해야 합니다.

예를 들어, MQOPEN 호출은 CREDIT.CHECK.REPLY.MODEL 및 동적 대기열 이름인 CREDIT.REPLY.* 큐 관리자(또는 큐 공유 그룹)에서 MQSP.

이를 수행하려면 다음 RACF 명령을 발행하여 필요한 큐 프로파일을 정의해야 합니다.

```
RDEFINE MQQUEUE MQSP.CREDIT.CHECK.REPLY.MODEL
RDEFINE MQQUEUE MQSP.CREDIT.REPLY.**
```

해당 RACF PERMIT 명령도 발행하여 해당 프로파일에 대한 사용자 액세스도 허용해야 합니다.

MQOPEN으로 작성되는 일반적인 동적 큐 이름은 CREDIT.REPLY.A346EF00367849A0과 유사합니다. 마지막 규정자의 정밀도 값은 예상할 수 없기 때문에 이런 큐 이름에 일반 프로파일을 사용해야 합니다.

많은 IBM MQ 유틸리티가 메시지를 동적 큐에 넣습니다. 다음 동적 큐 이름에 대해 프로파일을 정의하고 관련 사용자 ID에 RACF UPDATE 액세스 권한을 부여해야 합니다(올바른 사용자 ID에 대해서는 213 페이지의 『z/OS의 보안 검사를 위한 사용자 ID』 참조).

```
SYSTEM.CSQUTIL.* (used by CSQUTIL)
SYSTEM.CSQOREXX.* (used by the operations and control panels)
SYSTEM.CSQXCMD.* (used by the channel initiator when processing CSQINPX)
CSQ4SAMP.* (used by the IBM MQ supplied samples)
```

애플리케이션 프로그래밍 사본 멤버에서 기본적으로 사용되는 동적 큐 이름 사용을 제어하기 위해 프로파일 정의도 고려할 수 있습니다. IBM MQ 제공 사본에는 CSQ.*인 기본 *DynamicQueueName*이 포함됩니다. 이를 사용하여 적절한 RACF 프로파일이 설정됩니다.

참고: 동적 큐 이름에 대해 애플리케이션 프로그래머가 한 개의 *를 지정하지 못하도록 하십시오. 그렇게 하는 경우, hlq. **를 정의해야 합니다. MQQUEUE 클래스에 있는 프로파일을 사용할 수 있으며, 광범위한 액세스 권한을 부여해야 한다. 즉, 이 프로파일은 더 특정된 RACF 프로파일을 포함하지 않는 다른 비동적 큐에 대해서도 사용될 수 있습니다. 따라서 사용자가 액세스하면 안되는 큐에도 액세스할 수 있게 됩니다.

z/OS 영구적 동적 큐에서 닫기 옵션

애플리케이션이 다른 애플리케이션으로 작성된 영구적 동적 큐를 열고 MQCLOSE 옵션으로 해당 큐 삭제를 시도하는 경우, 일부 추가 보안 검사가 시도 수행 시에 적용됩니다.

MQCLOSE 옵션	hlq.queueName에 필요한 RACF 액세스 레벨
MQCO_DELETE	ALTER
MQCO_DELETE_PURGE	ALTER

z/OS

보안 및 리모트 큐

메시지를 리모트 큐에 넣을 때 로컬 큐 관리자가 구현하는 큐 보안은 리모트 큐를 열 때 지정되는 방법에 따라 다릅니다.

다음 규칙이 적용됩니다.

1. 리모트 큐가 IBM MQ DEFINE QREMOTE 명령을 통해 로컬 큐 관리자에 정의된 경우, 선택된 큐는 리모트 큐의 이름입니다. 예를 들어, 리모트 큐가 큐 관리자 MQS1에 다음과 같이 정의되는 경우:

```
DEFINE QREMOTE (BANK7.CREDIT.REFERENCE)
RNAME(CREDIT.SCORING.REQUEST)
RQMNAME (BNK7)
XMITQ(BANK1.TO.BANK7)
```

이 경우 BANK7.CREDIT.REFERENCE의 프로파일은 MQQUEUE 클래스에 정의되어야 합니다.

2. 요청에 대한 *ObjectQMgrName*이 로컬 큐 관리자로 해결되지 않는 경우, 보안 검사가 해결된(리모트) 큐 관리자 이름에 대해 수행되며 검사가 클러스터 큐 이름에 대해 수행되는 클러스터 큐의 경우는 제외됩니다.

예를 들어, 전송 큐 BANK1.TO.BANK7이 큐 관리자 MQS1에 정의됩니다. MQPUT1 요청은 *ObjectName*을 BANK1.TO.BANK7의 *ObjectQMgrName* 및 BANK1.INTERBANK.TRANSFERS으로 지정하여 MQS1에서 발행됩니다. 이 경우, 요청을 수행하는 사용자는 BANK1.TO.BANK7에 대한 액세스 권한이 있어야 합니다.

3. 큐에 대해 MQPUT 요청을 수행하고 *ObjectQMgrName*을 로컬 큐 관리자의 알리어스 이름으로 지정하는 경우, 큐 이름은 큐 관리자가 아니라 보안에 대해 검사됩니다.

리모트 큐 관리자로 메시지를 가져오는 경우, 추가 보안 처리가 수행될 수도 있습니다. 자세한 정보는 [84 페이지의 『원격 메시징의 보안』](#)의 내용을 참조하십시오.

z/OS

데드-레터 큐 보안

다수의 사용자가 데드-레터 큐에 메시지를 넣을 수는 있지만 메시지 검색을 위한 액세스는 엄격하게 제한되기 때문에 데드-레터 큐에는 특수한 고려사항이 적용됩니다. 이는 다른 RACF 권한을 데드-레터 큐 및 알리어스 큐에 적용하여 수행할 수 있습니다.

미전달 메시지는 데드-레터 큐라고 하는 특수 큐에 넣을 수 있습니다. 이 큐에서 종료될 수도 있는 민감한 데이터가 있는 경우 권한 없는 사용자가 이 데이터를 검색하지 못하도록 하기 위해 이런 보안 내포사항을 고려해야 합니다.

메시지를 데드-레터 큐에 넣으려면 다음 각각이 허용되어야 합니다.

- 애플리케이션 프로그램.
- 채널 시작기 주소 공간 및 임의 MCA 사용자 ID. (RESLEVEL 프로파일이 없거나 정의되어 채널 사용자 ID가 검사되는 경우, 채널 사용자 ID도 데드-레터 큐에 메시지를 넣으려면 권한이 필요합니다.)
- CKTI, CICS 제공 CICS 채널 시작기.
- CSQQTRMN, IBM MQ 제공 IMS 트리거 모니터.

데드-레터 큐에서 메시지를 검색할 수 있는 유일한 애플리케이션은 이런 메시지를 처리하는 '특수한' 애플리케이션이어야 합니다. However, a problem arises if you give applications RACF UPDATE authority to the dead-letter queue for MQPUT s because they can then automatically retrieve messages from the queue using MQGET calls. 가져오기 조작에 대해서는 데드-레터 큐를 사용 불가능하게 설정할 수 없으며 그렇게 설정하면 '특수한' 애플리케이션 조작도 메시지를 검색할 수 없습니다.

이 문제점에 대한 한 가지 해결책은 데드-레터 큐에 대해 두 레벨의 액세스를 설정하는 것입니다. CKTI, 메시지 채널 에이전트 트랜잭션 또는 채널 시작기 주소 공간 및 '특수한' 애플리케이션에는 직접 액세스가 있습니다. 다른 애플리케이션은 알리어스 큐를 통해서만 데드-레터 큐에 액세스할 수 있습니다. 이 알리어스는 애플리케이션이 메시지를 데드-레터 큐에서 가져오기 위해서가 아니라 넣을 수 있도록 허용하기 위해 정의되는 것입니다.

이는 원래 예상된 동작입니다.

1. 샘플 thlqual.SCSQPROC(CSQ4INYG)에 표시되는 것처럼 속성 PUT(ENABLED) 및 GET(ENABLED)을 사용하여 실제 데드-레터 큐를 정의하십시오.
2. 다음 사용자 ID에 대해 RACF UPDATE 권한을 데드-레터 큐에 부여하십시오.

- CKTI 및 MCA 또는 채널 시작기 주소 공간이 실행되는 사용자 ID.
 - '특수한' 데드-레터 큐 처리 애플리케이션에 연관되는 사용자 ID.
3. 실제 데드-레터 큐로 해결되는 알리어스 큐를 정의하지만 알리어스 큐에는 PUT(ENABLED) 및 GET(DISABLED) 속성을 지정하십시오. 알리어스 큐 이름은 데드-레터 큐 이름과 동일한 방식으로 지정하고 여기에 ".PUT" 문자를 추가하십시오. 예를 들어, 데드-레터 큐 이름이 hlq.DEAD.QUEUE인 경우 알리어스 큐 이름은 hlq.DEAD.QUEUE.PUT입니다.
 4. 데드-레터 큐에 메시지를 넣기 위해 애플리케이션은 알리어스 큐를 사용합니다. 다음은 애플리케이션이 수행해야 합니다.
 - 실제 데드-레터 큐 이름을 검색합니다. 수행하기 위해 MQOPEN을 사용하여 큐 관리자 오브젝트를 열고 MQINQ를 발행하여 데드-레터 큐 이름을 가져옵니다.
 - 이 이름에 '.PUT'를 추가하여 알리어스 큐 이름을 빌드합니다(이 경우 hlq.DEAD.QUEUE.PUT).
 - 알리어스 큐 hlq.DEAD.QUEUE.PUT를 여십시오.
 - MQPUT을 알리어스 큐에 대해 발행하여 실제 데드-레터 큐에 메시지를 넣으십시오.
 5. 애플리케이션에 연관된 사용자 ID에 알리어스에 대한 RACF UPDATE 권한을 부여하지만 실제 데드-레터 큐에 대한 액세스는 부여하지 마십시오(권한 NONE). 이는 다음을 의미합니다.
 - 애플리케이션은 알리어스 큐를 사용하여 데드-레터 큐에 메시지를 넣을 수 있습니다.
 - 애플리케이션은 알리어스 큐가 가져오기 조작에 사용할 수 없기 때문에 알리어스 큐를 사용하여 데드-레터 큐에서 메시지를 가져올 수 없습니다.

애플리케이션은 올바른 RACF 권한이 있어서 실제 데드-레터 큐에서 어떤 메시지도 가져올 수 없습니다.

184 페이지의 표 34에서는 이 솔루션의 다양한 참가자에 필요한 RACF 권한을 요약합니다.

표 34. 데드-레터 큐 및 해당 알리어스에 대한 RACF 권한		
연관된 사용자 ID	실제 데드-레터 큐 (hlq.DEAD.QUEUE)	알리어스 데드-레터 큐 (hlq.DEAD.QUEUE.PUT)
MCA 또는 채널 시작기 주소 공간 및 CKTI	UPDATE	NONE
'특수한' 애플리케이션(데드-레터 큐 처리용)	UPDATE	NONE
사용자 작성 애플리케이션 사용자 ID	NONE	UPDATE


이 메소드를 사용하면 애플리케이션은 데드-레터 큐의 최대 메시지 길이(MAXMSGL)를 판별할 수 없습니다. 이는 MAXMSGL 속성이 알리어스 큐에서 검색 불가능하기 때문입니다. 따라서, 애플리케이션은 최대 메시지 길이가 IBM MQ for z/OS에서 지원하는 최대 크기인 100MB라고 간주해야 합니다. 실제 데드-레터 큐의 MAXMSGL 속성도 100MB로 정의되어야 합니다.

참고: 사용자 작성 애플리케이션 프로그램은 일반적으로 대체 사용자 권한을 사용하여 메시지를 데드-레터 큐에 넣지 않습니다. 이를 통해 데드-레터 큐에 액세스하는 사용자 ID 수가 줄어듭니다.

시스템 큐 보안

특정 시스템 큐에 대한 특정 사용자 ID 액세스를 허용하기 위해 RACF 액세스를 설정해야 합니다.

다수의 시스템 큐는 IBM MQ의 보조 파트에서 액세스합니다.

- CSQUTIL 유틸리티
- 메시지 보안 정책 유틸리티(CSQOUTIL)
- 조작 및 제어판
- 채널 시작기 주소 공간(큐된 발행/구독 디먼 포함)
-  MQ Console 및 REST API에서 사용하는 mqweb 서버.

185 페이지의 표 35에 표시된 대로 이러한 실행에 있는 사용자 ID에 이러한 큐에 대한 RACF 액세스 권한이 부여되어야 합니다.

표 35. IBM MQ 에 의해 시스템 큐에 필요한 액세스					
SYSTEM 큐	CSQUTIL	CSQOUTIL	mqweb 서버	조작 및 제어 판	분산 큐잉을 위한 채널 시작기
SYSTEM.ADMIN.CHANNEL.EVENT	-	-	-	-	UPDATE
SYSTEM.ADMIN.COMMAND.QUEUE	-	-	UPDATE	-	-
SYSTEM.BROKER.ADMIN.STREAM	-	-	-	-	ALTER
SYSTEM.BROKER.CONTROL.QUEUE	-	-	-	-	ALTER
SYSTEM.BROKER.DEFAULT.STREAM	-	-	-	-	ALTER
SYSTEM.BROKER.INTER.BROKER.COMMUNICATIONS	-	-	-	-	UPDATE
SYSTEM.CHANNEL.INITQ	-	-	-	-	UPDATE
SYSTEM.CHANNEL.SYNCQ	-	-	-	-	UPDATE
SYSTEM.CLUSTER.COMMAND.QUEUE	-	-	-	-	ALTER
SYSTEM.CLUSTER.REPOSITORY.QUEUE	-	-	-	-	UPDATE
SYSTEM.CLUSTER.TRANSMIT.QUEUE	-	-	-	-	ALTER
SYSTEM.COMMAND.INPUT	UPDATE	-	-	UPDATE	UPDATE
SYSTEM.COMMAND.REPLY.*	-	-	-	-	UPDATE
SYSTEM.COMMAND.REPLY.MODEL	UPDATE	-	-	UPDATE	UPDATE
SYSTEM.CSQOREXX.*	-	-	-	UPDATE	-
SYSTEM.CSQUTIL.*	UPDATE	-	-	-	-
SYSTEM.CSQXCMD.*	-	-	-	-	UPDATE
SYSTEM.HIERARCHY.STATE	-	-	-	-	UPDATE
SYSTEM.INTER.QMGR.CONTROL	-	-	-	-	UPDATE
SYSTEM.INTER.QMGR.PUBS	-	-	-	-	UPDATE
SYSTEM.INTER.QMGR.FANREQ	-	-	-	-	UPDATE
SYSTEM.PROTECTION.ERROR.QUEUE	-	-	-	-	UPDATE
SYSTEM.PROTECTION.POLICY.QUEUE	-	UPDATE 185 페이지의 『1』	-	-	READ
SYSTEM.QSG.CHANNEL.SYNCQ	-	-	-	-	UPDATE
SYSTEM.QSG.TRANSMIT.QUEUE	-	-	-	-	UPDATE
SYSTEM.REST.REPLY.QUEUE	-	-	UPDATE	-	-
SYSTEM.BLUEMIX.REGISTRATION.QUEUE	-	-	-	-	UPDATE

참고사항:

1. Advanced Message Security 주소 공간 사용자는 이 큐에 대한 READ 액세스 권한도 필요합니다.

표 36. MQOPEN, MQPUT1, MQSUB, MQCLOSE 옵션 및 필수 보안 권한. (1)과 같이 표시되는 콜아웃은 이 테이블의 참조를 나타냅니다.

		필요한 최소 RACF 액세스 레벨		
RACF 클래스:	MXTOPIC	MQQUEUE 또는 MXQUEUE (1)	MQADMIN 또는 MXADMIN	MQADMIN 또는 MXADMIN
RACF 프로파일:	(15 또는 16)	(2)	(3)	(4)
MQOPEN 옵션				
MQOO_INQUIRE		READ (5)	검사 안함	검사 안함
MQOO_BROWSE		READ	검사 안함	검사 안함
MQOO_INPUT_*		UPDATE	검사 안함	검사 안함
MQOO_SAVE_ALL_CONTEXT (6)		UPDATE	검사 안함	검사 안함
MQOO_OUTPUT (USAGE=NORMAL) (7)		UPDATE	검사 안함	검사 안함
MQOO_PASS_IDENTITY_CONTEXT (8)		UPDATE	READ	검사 안함
MQOO_PASS_ALL_CONTEXT (8) (9)		UPDATE	READ	검사 안함
MQOO_SET_IDENTITY_CONTEXT (8) (9)		UPDATE	UPDATE	검사 안함
MQOO_SET_ALL_CONTEXT (8) (10)		UPDATE	CONTROL	검사 안함
MQOO_OUTPUT (USAGE (XMITQ)) (11)		UPDATE	CONTROL	검사 안함
MQOO_OUTPUT(토픽 오브젝트)	UPDATE (16)			
MQOO_OUTPUT(토픽 오브젝트에 대한 알리어스 큐)	UPDATE (16)	UPDATE		
MQOO_SET		ALTER	검사 안함	검사 안함
MQOO_ALTERNATE_USER_AUTHORITY		(12)	(12)	UPDATE
MQPUT1 옵션				
정상 큐에 넣기(7)		UPDATE	검사 안함	검사 안함
MQPMO_PASS_IDENTITY_CONTEXT		UPDATE	READ	검사 안함
MQPMO_PASS_ALL_CONTEXT		UPDATE	READ	검사 안함
MQPMO_SET_IDENTITY_CONTEXT		UPDATE	UPDATE	검사 안함
MQPMO_SET_ALL_CONTEXT		UPDATE	CONTROL	검사 안함
MQOO_OUTPUT 전송 큐에 넣기(11)		UPDATE	CONTROL	검사 안함
MQOO_OUTPUT(토픽 오브젝트)	UPDATE (16)			
MQOO_OUTPUT(토픽 오브젝트에 대한 알리어스 큐)	UPDATE (16)	UPDATE		
MQPMO_ALTERNATE_USER_AUTHORITY		(13)	(13)	UPDATE
MQCLOSE 옵션				

표 36. MQOPEN, MQPUT1, MQSUB, MQCLOSE 옵션 및 필수 보안 권한. (1)과 같이 표시되는 콜아웃은 이 테이블의 참고를 나타냅니다. (계속)

		필요한 최소 RACF 액세스 레벨		
RACF 클래스:	MXTOPIC	MQQUEUE 또는 MXQUEUE (1)	MQADMIN 또는 MXADMIN	MQADMIN 또는 MXADMIN
RACF 프로파일:	(15 또는 16)	(2)	(3)	(4)
MQCO_DELETE (14)		ALTER	검사 안함	검사 안함
MQCO_DELETE_PURGE (14)		ALTER	검사 안함	검사 안함
MQCO_REMOVE_SUB	ALTER (15)			
MQSUB 옵션				
MQSO_CREATE	ALTER (15)	(17)	(18)	
MQSO_ALTER	ALTER (15)	(17)	(18)	
MQSO_RESUME	READ (15)	(17)	검사 안함	
MQSO_ALTERNATE_USER_AUTHORITY				UPDATE
MQSO_SET_IDENTITY_CONTEXT			(18)	

참고:

- 이 옵션은 큐로 제한되지 않습니다. 이름 목록에 대한 MQNLIST 또는 MXNLIST 클래스 및 프로세스에 대한 MQPROC 또는 MXPROC 클래스.
- RACF 프로파일: hlq.resourcename을 사용하십시오.
- RACF 프로파일: hlq.CONTEXT.queueName을 사용하십시오.
- RACF 프로파일: hlq.ALTERNATE.USER.alternateuserid를 사용하십시오.
alternateuserid는 오브젝트 디스크립터의 AlternateUserId 필드에 지정되는 사용자 ID입니다. 최대 12자의 AlternateUserId 필드가 이 검사에 사용되며 이는 다른 검사에서 사용자 ID의 처음 8자만 사용되는 것과 다릅니다.
- 조회를 위해 큐 관리자를 여는 경우에는 검사가 수행되지 않습니다.
- MQOO_INPUT_*도 지정해야 합니다. 이는 로컬, 모델 또는 알리어스 큐에 대해 유효합니다.
- 이 검사는 **Usage** 큐 속성이 MQUS_NORMAL인 로컬이나 모델 큐에 대해 수행되며 알리어스 또는 리모트 큐(연결된 큐 관리자에 정의)에 대해서도 수행됩니다. 큐가 ObjectQMGrName(연결된 큐 관리자 이름이 아님)을 명시적으로 지정하여 열리는 리모트 큐인 경우, ObjectQMGrName과 동일한 이름의 큐(**Usage** 큐 속성이 MQUS_TRANSMISSION인 로컬 큐여야 함)에 대해 검사가 수행됩니다.
- MQOO_OUTPUT도 지정해야 합니다.
- MQOO_PASS_IDENTITY_CONTEXT도 이 옵션으로 표시됩니다.
- MQOO_PASS_IDENTITY_CONTEXT, MQOO_PASS_ALL_CONTEXT, MQOO_SET_IDENTITY_CONTEXT도 이 옵션으로 표시됩니다.
- Usage** 큐 속성이 MQUS_TRANSMISSION인 로컬 또는 모델 큐에서 이 검사가 수행되며 출력을 위해 직접 열립니다. 리모트 큐를 여는 중에는 적용되지 않습니다.
- MQOO_INQUIRE, MQOO_BROWSE, MQOO_INPUT_*, MQOO_OUTPUT 또는 MQOO_SET 중에서 하나 이상도 지정해야 합니다. 수행되는 검사는 지정되는 다른 옵션의 검사와 동일합니다.
- 수행되는 검사는 지정되는 다른 옵션의 검사와 동일합니다.
- 이는 모델 큐를 통해 열린 것이 아니라 직접 열린 영구적 동적 큐에 대해서만 적용됩니다. 임시 동적 큐 삭제 시에는 보안이 필요하지 않습니다.
- RACF 프로파일 hlq.SUBSCRIBE.topicName을 사용하십시오.

16. RACF 프로파일 hlq.PUBLISH.topicname을 사용하십시오.
17. MQSUB 요청에서 발행물을 송신하려는 발행 목적지 큐를 지정하는 경우 보안 검사가 해당 큐에 대한 쓰기 권한이 있는지 확인하기 위해 큐에 대해 수행됩니다.
18. MQSUB 요청에서 MQSO_CREATE 또는 MQSO_ALTER 옵션을 지정하여 MQSD 구조에 임의 ID 컨텍스트 필드를 설정하려면 MQSO_SET_IDENTITY_CONTEXT 옵션도 지정해야 하며 목적지 큐에 대한 컨텍스트 프로파일에 대해 적절한 권한도 필요합니다.

z/OS 토픽 보안을 위한 프로파일

토픽 보안이 활성화된 경우 해당 클래스에 프로파일을 정의하고 필요한 그룹이나 사용자 ID에 해당 프로파일에 대한 액세스를 허용해야 합니다.

토픽 트리 내에서 토픽 보안 개념은 보안 발행/구독에서 설명됩니다.

토픽 보안이 활성화된 경우 다음 조치를 수행해야 합니다.

- **MXTOPIC** 또는 **GMXTOPIC** 클래스에 프로파일을 정의하십시오.
- 필요한 그룹이나 사용자 ID에 해당 프로파일에 대한 액세스를 허용하여 토픽을 사용하는 IBM MQ API 요청을 발행할 수 있도록 해야 합니다.

토픽 보안을 위한 프로파일은 다음 양식을 사용합니다.

```
hlq.SUBSCRIBE.topicname
hlq.PUBLISH.topicname
```

여기서,

- hlq는 qmgr-name(큐 관리자 이름) 또는 qsg-name(큐 공유 그룹 이름)입니다.
- topicname은 MQSUB 호출을 통해 구독 중이거나 MQOPEN 호출을 통해 발행 중인 토픽에 연관된 토픽 트리의 토픽 관리 노드 이름입니다.

큐 관리자 이름이 접두부로 추가된 프로파일은 해당 큐 관리자에서 단일 토픽에 대한 액세스를 제어합니다. 큐 공유 그룹 이름의 접두부가 추가된 프로파일은 큐 공유 그룹 내의 모든 큐 관리자에서 해당 큐 이름의 하나 이상의 토픽에 대한 액세스를 제어합니다. 이 액세스는 해당 큐 관리자에서 이 토픽에 대해 큐 관리자 레벨 프로파일을 정의하여 개별 큐 관리자에서 대체 가능합니다.

큐 관리자가 큐 공유 그룹의 멤버이고 큐 관리자와 큐 공유 그룹 레벨 보안을 모두 사용하는 경우 IBM MQ는 큐 관리자 이름이 접두부로 추가된 프로파일을 먼저 검사합니다. 찾을 수 없는 경우 큐 공유 그룹 이름의 접두부가 추가된 프로파일을 검색합니다.

구독

토픽을 구독하려면 구독하려는 토픽과 발행물의 목적지 큐 둘 다에 대한 액세스가 필요합니다.

MQSUB 요청을 발행하는 경우 다음 보안 검사가 수행됩니다.

- 해당 토픽을 구독할 수 있는 적절한 레벨의 액세스 권한이 있는지 여부와 목적지 큐 (지정된 경우) 가 출력을 위해 열려 있는지 여부
- 해당 대상 큐에 대한 적절한 레벨의 액세스 권한이 있는지 여부.

표 37. 구독하려는 토픽 보안에 필요한 액세스 레벨	
MQSUB 옵션	MXTOPIC 클래스의 hlq.SUBSCRIBE.topicname 프로파일에 필요한 RACF 액세스
MQSO_CREATE 및 MQSO_ALTER	ALTER
MQSO_RESUME	READ

표 38. 비관리 대상 큐를 사용하여 구독하는 데 필요한 추가 권한	
MQSUB 옵션	MQADMIN 또는 MXADMIN 클래스의 hlq.CONTEXT.queueName 프로파일에 필요한 RACF 액세스
MQSO_CREATE, MQSO_ALTER, MQSO_RESUME	UPDATE
	RACF MQQUEUE 또는 MXQUEUE 클래스에서 hlq.queueName 프로파일에 필요한 액세스
MQSO_CREATE 및 MQSO_ALTER	UPDATE
	RACF MQADMIN 또는 MXADMIN 클래스의 hlq.ALTERNATE.USER.alternateuserid 프로파일에 필요한 액세스
MQSO_ALTERNATE_USER_AUTHORITY	UPDATE

구독하려는 관리 큐에 대한 고려사항

보안 검사는 토픽을 구독할 수 있는지를 확인하기 위해 수행됩니다. 그렇지만 관리 큐가 작성되는 경우 또는 이 목적지 큐에 대해 메시지를 넣을 액세스가 있는지를 판별하기 위해서는 보안 검사가 수행되지 않습니다.

관리 큐는 닫거나 삭제할 수 없습니다.

사용되는 모델 큐는 **SYSTEM.DURABLE.MODEL.QUEUE** 및 **SYSTEM.NDURABLE.MODEL.QUEUE**입니다.

이 모델 큐에서 작성되는 관리 큐는 마지막 규정자를 예상할 수 없는 **SYSTEM.MANAGED.DURABLE.A346EF00367849A0** 및 **SYSTEM.MANAGED.NDURABLE.A346EF0036785EA0** 양식을 사용합니다.

해당 큐에 대해 어떤 사용자에게도 액세스를 부여하지 마십시오. 큐는 권한이 부여되지 않은 양식 **SYSTEM.MANAGED.DURABLE.*** 및 **SYSTEM.MANAGED.NDURABLE.***의 일반 프로파일을 사용하여 보호가 가능합니다.

메시지는 MQSUB 요청에서 리턴되는 핸들을 사용하여 해당 큐에서 검색 가능합니다.

MQCO_REMOVE_SUB 옵션을 지정하여 구독에 대해 MQCLOSE 호출을 명시적으로 발행하고 이 핸들로 닫기 중인 구독을 작성하지 않은 경우, 조작을 수행할 올바른 권한이 있는지 확인하기 위해 닫을 때 보안 검사가 수행됩니다.

표 39. 구독 닫기 조작에 대한 토픽 보안을 위한 프로파일에 필요한 액세스 레벨	
MQCLOSE 옵션	MXTOPIC 클래스의 hlq.SUBSCRIBE.topicName 프로파일에 필요한 RACF 액세스
MQCO_REMOVE_SUB	ALTER

발행

토픽에서 발행하려면 토픽 및 알리어스 큐를 사용 중인 경우에는 알리어스 큐에도 액세스가 필요합니다.

표 40. 공개할 토픽 보안에 필요한 액세스 레벨	
MQOPEN 또는 MQPUT1 옵션	MXTOPIC 클래스의 hlq.PUBLISH.topicName 프로파일에 필요한 RACF 액세스
MQOO_OUTPUT 또는 MQPUT1	UPDATE

표 41. 토픽으로 해석되는 알리어스 큐를 여는 데 필요한 액세스 레벨	
MQOPEN 또는 MQPUT1 옵션	알리어스 큐에 대한 MQQUEUE 또는 MXQUEUE 클래스의 hlq.queueName 프로파일에 필요한 RACF 액세스
MQOO_OUTPUT 또는 MQPUT1	UPDATE

토픽 이름으로 해결되는 알리어스 큐가 발행을 위해 열리는 경우 토픽 보안이 조작되는 방법에 대한 자세한 내용은 190 페이지의 『발행 조작을 위해 토픽에 대해 해결되는 알리어스 큐에 대한 고려사항』의 내용을 참조하십시오.

알리어스 큐가 PUT 또는 GET 제한에 대해 목적지 큐에 사용되도록 고려하는 경우에는 181 페이지의 『알리어스 큐에 대한 고려사항』의 내용을 참조하십시오.

애플리케이션이 토픽 보안 프로파일에 대해 가지는 RACF 액세스 레벨이 변경되는 경우 변경사항은 해당 토픽에 대해 획득하는 모든 새 오브젝트 핸들(즉, 새 MQSUB 또는 MQOPEN)에 대해서만 적용됩니다. 해당 핸들은 변경이 토픽에 대한 기존 액세스를 유지하는 시점에서 이미 있습니다. 또한, 기존 구독자는 이미 수행한 모든 구독에 대한 액세스도 보유하고 있습니다.

발행 조작을 위해 토픽에 대해 해결되는 알리어스 큐에 대한 고려사항

토픽에 대해 해결되는 알리어스 큐에 대해 MQOPEN 또는 MQPUT1 호출을 발행하는 경우, IBM MQ는 두 개의 자원 검사를 수행합니다.

- 첫 번째 검사는 MQOPEN 또는 MQPUT1 호출에서 오브젝트 디스크립터(MQOD)에 지정하는 알리어스 큐 이름에 대한 검사입니다.
- 두 번째는 알리어스 큐가 해결되는 토픽에 대한 검사입니다.

이 동작은 알리어스 큐가 다른 큐에 대해 해결되는 경우의 동작과는 다릅니다. 발행 조치를 계속하려면 두 프로파일 모두에 대해 올바른 액세스 권한이 필요합니다.

시스템 토픽 보안

다음 시스템 주제는 채널 시작기 주소 공간에서 액세스합니다.

190 페이지의 표 42에 표시된 대로 이 실행을 실행하는 사용자 ID에 이러한 큐에 대한 RACF 액세스 권한이 부여되어야 합니다.

표 42. SYSTEM 토픽에 필요한 액세스		
SYSTEM 토픽	프로파일	분산 큐잉을 위한 채널 시작기
SYSTEM.BROKER.ADMIN.STREAM	hlq.PUBLISH.topicname	UPDATE
SYSTEM.BROKER.ADMIN.STREAM	hlq.SUBSCRIBE.topicname	ALTER

z/OS 프로세스를 위한 프로파일

프로세스 보안이 활성화된 경우 해당 클래스에 프로파일을 정의하고 필요한 그룹이나 사용자 ID에 해당 프로파일에 대한 액세스를 허용해야 합니다.

프로세스 보안이 활성화된 경우 다음을 수행해야 합니다.

- 대문자 프로파일을 사용 중인 경우 **MQPROC** 또는 **GMQPROC** 클래스에 프로파일을 정의하십시오.
- 대소문자 혼합 프로파일을 사용 중인 경우 **MXPROC** 또는 **GMXPROC** 클래스에 프로파일을 정의하십시오.
- 필요한 그룹이나 사용자 ID에 해당 프로파일에 대한 액세스를 허용하여 프로세스를 사용하는 IBM MQ API 요청을 발행할 수 있도록 해야 합니다.

프로세스를 위한 프로파일은 다음 양식을 사용합니다.

```
hlq.processname
```

여기서 hlq는 qmgr-name(큐 관리자 이름) 또는 qsg-name(큐 공유 그룹 이름)이며 processname는 열려 있는 프로세스 이름입니다.

큐 관리자 이름이 접두부로 추가된 프로파일은 해당 큐 관리자에서 단일 프로세스 정의에 대한 액세스를 제어합니다. 큐 공유 그룹 이름의 접두부가 추가된 프로파일은 큐 공유 그룹 내의 모든 큐 관리자에서 해당 이름의 하나 이상의 프로세스 정의에 대한 액세스를 제어합니다. 이 액세스는 해당 큐 관리자에서 이 프로세스 정의에 대해 큐 관리자 레벨 프로파일을 정의하여 개별 큐 관리자에서 대체 가능합니다.

큐 관리자가 큐 공유 그룹의 멤버이고 큐 관리자와 큐 공유 그룹 레벨 보안을 모두 사용하는 경우 IBM MQ는 큐 관리자 이름이 접두부로 추가된 프로파일을 먼저 검사합니다. 찾을 수 없는 경우 큐 공유 그룹 이름의 접두부가 추가된 프로파일을 검색합니다.

다음 표는 프로세스 열기에 필요한 액세스를 보여줍니다.

표 43. 프로세스 보안에 대한 액세스 레벨	
MQOPEN 옵션	hlq.processname에 필요한 RACF 액세스 레벨
MQOO_INQUIRE	READ

예를 들어, 큐 관리자 MQS9에서 RACF 그룹 INQVPRC는 V 문자로 시작되는 모든 프로세스에서 조회(MQINQ)할 수 있어야 합니다. 이에 대한 RACF 정의는 다음과 같습니다.

```
RDEFINE MQPROC MQS9.V* UACC(NONE)
PERMIT MQS9.V* CLASS(MQPROC) ID(INQVPRC) ACCESS(READ)
```

프로세스 정의 오브젝트가 열릴 때 지정되는 열기 옵션에 따라 대체 사용자 보안이 활성화될 수도 있습니다.

z/OS 이름 목록에 대한 프로파일

이름 목록 보안이 활성화되는 경우 적절한 클래스로 프로파일을 정의하고 필요한 그룹 또는 사용자 ID에 해당 프로파일에 대한 액세스를 제공합니다.

이름 목록 보안이 활성화된 경우 다음을 수행해야 합니다.

- 대문자 프로파일을 사용 중인 경우 **MQNLIST** 또는 **GMQNLIST** 클래스에 프로파일을 정의하십시오.
- 대소문자 혼합 프로파일을 사용 중인 경우 **MXNLIST** 또는 **GMXNLIST** 클래스에 프로파일을 정의하십시오.
- 해당 프로파일에 대한 액세스를 필수 그룹이나 사용자 ID에 허용하십시오.

이름 목록 프로파일은 다음 양식을 사용합니다.

```
hlq.namelistname
```

여기서 hlq는 qmgr-name(큐 관리자 이름) 또는 qsg-name(큐 공유 그룹 이름)이고 namelistname은 열려 있는 이름 목록입니다.

큐 관리자 이름이 접두부로 추가된 프로파일은 해당 큐 관리자에서 단일 이름 목록에 대한 액세스를 제어합니다. 큐 공유 그룹 이름의 접두부가 추가된 프로파일은 큐 공유 그룹 내의 모든 큐 관리자에서 해당 이름의 하나 이상의 이름 목록에 대한 액세스를 제어합니다. 이 액세스는 해당 큐 관리자에서 이 이름 목록에 대해 큐 관리자 레벨 프로파일을 정의하여 개별 큐 관리자에서 대체 가능합니다.

큐 관리자가 큐 공유 그룹의 멤버이고 큐 관리자와 큐 공유 그룹 레벨 보안을 모두 사용하는 경우 IBM MQ는 큐 관리자 이름이 접두부로 추가된 프로파일을 먼저 검사합니다. 찾을 수 없는 경우 큐 공유 그룹 이름의 접두부가 추가된 프로파일을 검색합니다.

다음 표는 이름 목록 열기에 필요한 액세스를 보여줍니다.

표 44. 이름 목록 보안에 대한 액세스 레벨	
MQOPEN 옵션	hlq.namelistname 에 필요한 RACF 액세스 레벨
MQOO_INQUIRE	READ

예를 들어, 큐 관리자(또는 큐 공유 그룹) PQM3에서 RACF 그룹 DEPT571은 해당 이름 목록에서 조회(MQINQ)할 수 있어야 합니다.

- "DEPT571"로 시작하는 모든 이름 목록.
- PRINTER/DESTINATIONS/DEPT571
- AGENCY/REQUEST/QUEUES
- WAREHOUSE.BROADCAST

이를 수행하는 RACF 정의는 다음과 같습니다.

```
RDEFINE MQNLIST PQM3.DEPT571.** UACC(NONE)
PERMIT PQM3.DEPT571.** CLASS(MQNLIST) ID(DEPT571) ACCESS(READ)

RDEFINE GMQNLIST NLISTS.FOR.DEPT571 UACC(NONE)
ADDMEM(PQM3.PRINTER/DESTINATIONS/DEPT571,
        PQM3.AGENCY/REQUEST/QUEUES,
        PQM3.WAREHOUSE.BROADCAST)
PERMIT NLISTS.FOR.DEPT571 CLASS(GMQNLIST) ID(DEPT571) ACCESS(READ)
```

이름 목록 오브젝트가 열릴 때 지정되는 열기 옵션에 따라 대체 사용자 보안이 활성화될 수 있습니다.

시스템 이름 목록 보안

다수의 시스템 이름 목록은 IBM MQ의 보조 파트에서 액세스합니다.

- CSQUTIL 유틸리티
- 조작 및 제어판
- 채널 시작기 주소 공간(큐된 발행/구독 디먼 포함)

192 페이지의 표 45에 표시된 대로 이러한 실행 중인 사용자 ID에 이러한 이름 목록에 대한 RACF 액세스 권한이 부여되어야 합니다.

표 45. IBM MQ 이 시스템 이름 목록에 액세스해야 합니다.			
SYSTEM 이름 목록	CSQUTIL	조작 및 제어판	분산 큐잉을 위한 채널 시작기
SYSTEM.QPUBSUB.QUEUE.NAMELIST	-	-	READ
SYSTEM.QPUBSUB.SUBPOINT.NAMELIST	-	-	READ

대체 사용자 보안을 위한 프로파일

대체 사용자 보안이 활성화되는 경우 적절한 클래스로 프로파일을 정의하고 필요한 그룹 또는 사용자 ID에 해당 프로파일에 대한 액세스를 제공합니다.

*AlternateUserId*에 대한 자세한 정보는 [AlternateUserID \(MQCHAR12\)](#)를 참조하십시오.

대체 사용자 보안이 활성화된 경우 다음을 수행해야 합니다.

- 대문자 프로파일을 사용하는 중인 경우 MQADMIN 또는 GMQADMIN 클래스에 프로파일을 정의하십시오.
- 대소문자 혼합 프로파일을 사용하는 중인 경우 MXADMIN 또는 GMXADMIN 클래스에 프로파일을 정의하십시오.

필요한 그룹이나 사용자 ID에 해당 프로파일에 대한 액세스를 허용하여 오브젝트를 열 때 ALTERNATE_USER_AUTHORITY 옵션을 사용할 수 있도록 해야 합니다.

대체 사용자 보안을 위한 프로파일은 서브시스템 레벨 또는 큐 공유 그룹 레벨에 지정할 수 있으며 다음 양식을 사용합니다.

```
hlq.ALTERNATE.USER.alternateuserid
```

여기서 hlq는 qmgr-name(큐 관리자 이름) 또는 qsg-name(큐 공유 그룹 이름)이며 alternateuserid는 오브젝트 디스크립터의 *AlternateUserId* 필드 값입니다.

큐 관리자 이름이 접두부로 추가된 프로파일은 해당 큐 관리자의 대체 사용자 ID 사용을 제어합니다. 큐 공유 그룹 이름의 접두부가 추가된 프로파일은 큐 공유 그룹 내에서 모든 큐 관리자의 대체 사용자 ID 사용을 제어합니다. 이 대체 사용자 ID는 올바른 액세스 권한이 있는 사용자가 큐 공유 그룹 내의 모든 큐 관리자에서 사용할 수 있습니다. 이 액세스는 해당 큐 관리자에서 이 대체 사용자 ID에 대해 큐 관리자 레벨 프로파일을 정의하여 개별 큐 관리자에서 대체 가능합니다.

큐 관리자가 큐 공유 그룹의 멤버이고 큐 관리자와 큐 공유 그룹 레벨 보안을 모두 사용하는 경우 IBM MQ는 큐 관리자 이름이 접두부로 추가된 프로파일을 먼저 검사합니다. 찾을 수 없는 경우 큐 공유 그룹 이름의 접두부가 추가된 프로파일을 검색합니다.

다음 표는 대체 사용자 옵션을 지정하는 경우 액세스를 보여줍니다.

표 46. 대체 사용자 보안의 액세스 레벨	
MQOPEN, MQSUB 또는 MQPUT1 옵션	필요한 RACF 액세스 레벨
MQOO_ALTERNATE_USER_AUTHORITY MQSO_ALTERNATE_USER_AUTHORITY MQPMO_ALTERNATE_USER_AUTHORITY	UPDATE

대체 사용자 보안 검사 이외에도 큐, 프로세스, 이름 목록, 컨텍스트 보안에 대한 다른 보안 검사를 수행할 수 있습니다. 대체 사용자 ID가 제공되는 경우 이는 큐, 프로세스 정의 또는 이름 목록 자원에서의 보안 검사에만 사용됩니다. 대체 사용자 및 컨텍스트 보안의 경우 해당 검사를 요청하는 사용자 ID가 사용됩니다. 사용자 ID가 처리되는 방법에 대한 자세한 내용은 213 페이지의 『z/OS의 보안 검사를 위한 사용자 ID』의 내용을 참조하십시오. 큐, 컨텍스트, 대체 사용자 보안이 모두 활성화되는 경우 필요한 열기 옵션 및 보안 검사를 보여주는 요약 테이블에 대해서는 186 페이지의 표 36의 내용을 참조하십시오.

대체 사용자 프로파일은 대체 사용자 ID에 지정된 사용자 ID에 연관된 자원에 대해 요청 사용자 ID 액세스를 부여합니다. 예를 들어, 큐 관리자 QMPY의 사용자 ID PAYSERV에서 실행 중인 PAYROLL 서버는 PS로 시작하는 모든 개인용 사용자 ID의 요청을 처리합니다. 요청 사용자의 사용자 ID로 수행되는 PAYROLL 서버에서 작업이 수행되도록 하기 위해 대체 사용자 권한이 사용됩니다. PAYROLL 서버는 요청 프로그램이 MQPMO_DEFAULT_CONTEXT 메시지 넣기 옵션을 사용하여 메시지를 생성하기 때문에 대체 사용자 ID로 지정해야 하는 사용자 ID를 알고 있습니다. 대체 사용자 ID 확보 위치에 대한 세부사항은 213 페이지의 『z/OS의 보안 검사를 위한 사용자 ID』의 내용을 참조하십시오.

다음 예제 RACF 정의를 사용하여 서버 프로그램은 문자 PS로 시작하는 대체 사용자 ID를 지정할 수 있습니다.

```
RDEFINE MQADMIN QMPY.ALTERNATE.USER.PS* UACC(NONE)
PERMIT QMPY.ALTERNATE.USER.PS* CLASS(MQADMIN) ID(PAYSERV) ACCESS(UPDATE)
```

참고:

1. 오브젝트 디스크립터 및 구독 디스크립터의 *AlternateUserId* 필드 길이는 12바이트입니다. 12바이트 모두 프로파일 검사에 사용되지만 처음 8바이트만 IBM MQ의 사용자 ID로 사용됩니다. 이 사용자 ID 자르기는 바람직하지 않으며 요청을 작성하는 애플리케이션 프로그램이 8바이트 이상의 모든 대체 사용자 ID를 적절하게 변환해야 합니다.
2. MQOO_ALTERNATE_USER_AUTHORITY, MQSO_ALTERNATE_USER_AUTHORITY 또는 MQPMO_ALTERNATE_USER_AUTHORITY를 지정하고 *AlternateUserId* 필드를 오브젝트 디스크립터에 지정하지 않으면 공백 사용자 ID가 사용됩니다. 대체 사용자 보안 검사를 위해 *AlternateUserId* 규정자에 사용되는 사용자 ID는 -BLANK-입니다(예: RDEF MQADMIN hlq.ALTERNATE.USER.-BLANK-).

사용자가 이 프로파일에 액세스할 수 있는 경우 모든 추가 검사는 공백의 사용자 ID로 수행됩니다. 공백 사용자 ID에 대한 세부사항은 220 페이지의 『공백 사용자 ID 및 UACC 레벨』의 내용을 참조하십시오.

대체 사용자 ID 관리는 일반 대체 사용자 프로파일을 사용할 수 있는 사용자 ID에 대한 이름 지정 규칙이 있는 경우 더 쉽습니다. 없는 경우에는 RACF RACVARS 기능을 사용할 수 있습니다. RACVARS에 대한 자세한 내용은 *z/OS SecureWay Security Server RACF Security Administrator's Guide*를 참조하십시오.

메시지를 대체 사용자 권한으로 열린 큐에 넣고 메시지 컨텍스트가 큐 관리자로 생성된 경우, MQMD_USER_IDENTIFIER 필드는 대체 사용자 ID로 설정됩니다.

z/OS 컨텍스트 보안을 위한 프로파일

IBM MQ는 특정 메시지에만 해당하는 컨텍스트 정보 액세스 제어를 위해 프로파일을 사용합니다. 컨텍스트는 메시지 디스크립터(MQMD)에 포함됩니다.

컨텍스트 보안에 대해 프로파일 사용

컨텍스트 보안이 활성화된 경우 다음을 수행해야 합니다.

- 대문자 프로파일을 사용 중인 경우 **MQADMIN** 클래스에 프로파일을 정의하십시오.
- 대소문자 혼합 프로파일을 사용 중인 경우 **MXADMIN** 클래스에 프로파일을 정의하십시오.

프로파일의 이름은 hlq.CONTEXT.queueName 또는 hlq.CONTEXT.topicName입니다. 여기서,

hlq

qmgr-name(큐 관리자 이름) 또는 qsg-name(큐 공유 그룹 이름)입니다.

queueName

컨텍스트 프로파일을 정의하려는 큐의 전체 이름 또는 일반 프로파일입니다.

topicName

컨텍스트 프로파일을 정의하려는 토픽의 전체 이름 또는 일반 프로파일일 수 있습니다.

큐 관리자 이름으로 접두부가 지정되고 **가 큐 또는 토픽 이름으로 지정된 프로파일에서는 해당 큐 관리자에 속하는 모든 큐 및 토픽에서 컨텍스트 보안을 제어할 수 있습니다. 이는 해당 큐 또는 주제의 컨텍스트에 대한 특정 프로파일을 정의하여 개별 큐 또는 토픽에서 대체될 수 있습니다.

큐 공유 그룹 이름으로 접두부가 지정되고 **가 큐 또는 주제 이름으로 지정된 프로파일은 큐 공유 그룹 내의 큐 관리자에 속하는 모든 큐 및 토픽에서 컨텍스트에 대한 제어를 허용합니다. 이는 큐 관리자 이름을 접두부로 사용하는 프로파일을 지정하여 해당 큐 관리자에서 컨텍스트에 대해 큐 관리자 레벨 프로파일을 정의해서 개별 큐 관리자에서 대체 가능합니다. 또한 큐 또는 토픽 이름으로 접미부가 붙은 프로파일을 지정하여 개별 큐 또는 토픽에서 대체할 수도 있습니다.

큐 관리자가 큐 공유 그룹의 멤버이고 큐 관리자와 큐 공유 그룹 레벨 보안을 모두 사용하는 경우 IBM MQ는 큐 관리자 이름이 접두부로 추가된 프로파일을 먼저 검사합니다. 찾을 수 없는 경우 큐 공유 그룹 이름의 접두부가 추가된 프로파일을 검색합니다.

이 프로파일에 대한 액세스를 필수 그룹이나 사용자 ID에 부여해야 합니다. 다음 표는 큐가 열릴 때 컨텍스트 옵션의 스펙에 따라 필요한 액세스 레벨을 보여줍니다.

표 47. 컨텍스트 보안에 대한 액세스 레벨	
MQOPEN 또는 MQPUT1 옵션	hlq.CONTEXT.queueName 또는 hlq.CONTEXT.topicName에 대한 RACF 액세스 레벨
MQPMO_NO_CONTEXT	컨텍스트 보안 검사 없음
MQPMO_DEFAULT_CONTEXT	컨텍스트 보안 검사 없음
MQOO_SAVE_ALL_CONTEXT	컨텍스트 보안 검사 없음
MQOO_PASS_IDENTITY_CONTEXT MQPMO_PASS_IDENTITY_CONTEXT	READ

표 47. 컨텍스트 보안에 대한 액세스 레벨 (계속)	
MQOPEN 또는 MQPUT1 옵션	hlq.CONTEXT.queueName 또는 hlq.CONTEXT.topicName 에 대한 RACF 액세스 레벨
MQOO_PASS_ALL_CONTEXT MQPMO_PASS_ALL_CONTEXT	READ
MQOO_SET_IDENTITY_CONTEXT MQPMO_SET_IDENTITY_CONTEXT	UPDATE
MQOO_SET_ALL_CONTEXT MQPMO_SET_ALL_CONTEXT	CONTROL
MQOO_OUTPUT 또는 MQPUT1(USAGE(XMITQ))	CONTROL
MQSUB 옵션	
MQSO_SET_IDENTITY_CONTEXT (참고 2)	UPDATE

참고:

1. 분산 큐잉에 사용되는 사용자 ID는 목적지 큐에 메시지를 넣으려면 hlq.CONTEXT.queueName에 대한 CONTROL 액세스가 필요합니다. 사용되는 사용자 ID에 대한 자세한 정보는 216 페이지의 『채널 시작기에 서 사용되는 사용자 ID』의 내용을 참조하십시오.
2. MQSUB 요청에서 MQSO_CREATE 또는 MQSO ALTER 옵션을 지정하여 MQSD 구조에 임의 ID 컨텍스트 필드를 설정하려면 MMQSO_SET_IDENTITY_CONTEXT 옵션도 지정해야 합니다. 또한, 목적지 큐에 대한 컨텍스트 프로파일에 적절한 권한도 필요합니다.

시스템 명령 입력 큐에 명령을 넣는 경우, 기본 컨텍스트 메시지 넣기 옵션을 사용하여 올바른 사용자 ID와 명령을 연관시키십시오.

예를 들어, IBM MQ 제공 유틸리티 프로그램 CSQUTIL은 큐에 메시지를 오프로드하고 다시 로드하는 데 사용할 수 있습니다. 메시지 오프로드가 큐로 복원되면 CSQUTIL 유틸리티는 MQOO_SET_ALL_CONTEXT 옵션을 사용하여 메시지를 해당 원래 상태로 되돌립니다. 이 열기 옵션에 필요한 큐 보안뿐만 아니라 컨텍스트 권한도 필요합니다. 예를 들어, 이 권한이 큐 관리자 MQS1의 그룹 BACKGRP에 필요한 경우 다음으로 정의됩니다.

```
RDEFINE MQADMIN MQS1.CONTEXT.** UACC(NONE)
PERMIT MQS1.CONTEXT.** CLASS(MQADMIN) ID(BACKGRP) ACCESS(CONTROL)
```

지정되는 옵션 및 수행되는 보안 유형에 따라 다른 유형의 보안 검사가 큐가 열릴 때 발생할 수도 있습니다. 여기에는 큐 보안(179 페이지의 『큐 보안을 위한 프로파일』 참조) 및 대체 사용자 보안(192 페이지의 『대체 사용자 보안을 위한 프로파일』 참조)이 포함됩니다. 큐, 컨텍스트, 대체 사용자 보안이 모두 활성화되는 경우 필요한 열기 옵션 및 보안 검사를 보여주는 요약 테이블에 대해서는 186 페이지의 표 36의 내용을 참조하십시오.

시스템 큐 컨텍스트 보안

많은 시스템 큐는 IBM MQ의 보조 부분에서 액세스할 수 있습니다(예: 채널 시작기 주소 공간 **V9.1.0** 및 IBM MQ Console과 REST API에서 사용하는 mqweb 서버).

아래에서 실행되는 사용자 ID에는 195 페이지의 표 48에 표시된 대로 이러한 큐에 대한 RACF 액세스 권한이 부여되어야 합니다.

표 48. 컨텍스트 조작에 대해 SYSTEM 큐에 필요한 액세스		
SYSTEM 큐	분산 큐잉을 위한 채널 시작기	mqweb 서버
SYSTEM.ADMIN.COMMAND.QUEUE	-	CONTROL
SYSTEM.BROKER.CONTROL.QUEUE	CONTROL	-

표 48. 컨텍스트 조작에 대해 SYSTEM 큐에 필요한 액세스 (계속)		
SYSTEM 큐	분산 큐잉을 위한 채널 시작기	mqweb 서버
SYSTEM.BROKER.INTER.BROKER.COMMUNICATIONS	CONTROL	-
SYSTEM.CHANNEL.SYNCQ	CONTROL	-
SYSTEM.CLUSTER.COMMAND.QUEUE	CONTROL	-
SYSTEM.CLUSTER.TRANSMIT.QUEUE	CONTROL	-

z/OS 명령 보안을 위한 프로파일

명령에 대한 보안 검사를 사용하려면 프로파일을 MQCMD5 클래스에 추가하십시오. 프로파일 이름은 MQSC 명령을 기반으로 하지만 MQSC와 PCF 명령 모두를 제어합니다. 프로파일은 큐 관리자 또는 큐 공유 그룹에 적용 가능합니다.

명령에 대해 보안 검사를 수행하려면(명령 보안 스위치 프로파일 hlq.NO.CMD.CHECKS을 정의하지 않음) 프로파일을 MQCMD5 클래스에 추가해야 합니다.

동일한 보안 프로파일이 MQSC와 PCF 명령 모두를 제어합니다. 명령 보안 검사에 대한 RACF 프로파일 이름은 MQSC 명령어 자체를 기반으로 합니다. 해당 프로파일은 다음 양식을 사용합니다.

```
hlq.verb.pkw
```

여기서, hlq는 qmgr-name(큐 관리자 이름) 또는 qsg-name(큐 공유 그룹 이름)이며 verb는 명령 이름의 VERB 파트이고(예: ALTER) pkw는 오브젝트 유형(예: 로컬 큐에 대한 QLOCAL)입니다.

따라서 서브시스템 CSQ1에서 ALTER QLOCAL 명령의 프로파일 이름은 다음과 같습니다.

```
CSQ1.ALTER.QLOCAL
```

일반 프로파일을 사용하여 명령 세트를 보호해서 유지보수하는 프로파일 수도 더 적어지고 액세스 목록 수도 더 적게 할 수 있습니다. 더 특정되는 프로파일로 보호되지 않는 모든 명령에 적용되는 일반 프로파일 작성을 고려하십시오. 이 프로파일을 UACC(NONE)으로 정의하고 관리자가 포함된 RACF 그룹에만 ALTER 액세스를 부여하십시오. 그러면 모든 DISPLAY 명령에 적용 가능한 일반 프로파일을 작성하고 이에 대해 광범위한 액세스를 부여할 수 있습니다. 이 극단적인 차이에서 특정 명령 세트에 액세스해야 하는 사용자 그룹을 식별할 수 있으며 해당 세트에 대해 프로파일을 작성하고 해당 사용자 클래스를 나타내는 RACF 그룹에 대해 액세스를 부여할 수도 있습니다. 사용자에게 필요하지 않은 명령에 대한 액세스를 부여하지 마십시오. 최소 권한 원칙만 적용하여 사용자가 해당 작업에 필요한 명령에만 액세스하도록 하십시오.

큐 관리자 이름이 접두부로 추가된 프로파일은 해당 큐 관리자에서 명령 사용을 제어합니다. 큐 공유 그룹 이름의 접두부가 추가된 프로파일은 큐 공유 그룹 내의 모든 큐 관리자에서 명령 사용을 제어합니다. 이 액세스는 해당 큐 관리자에서 이 명령에 대해 큐 관리자 레벨 프로파일을 정의하여 개별 큐 관리자에서 대체 가능합니다.

큐 관리자가 큐 공유 그룹의 멤버이고 큐 관리자와 큐 공유 그룹 레벨 보안을 모두 사용하는 경우 IBM MQ는 큐 관리자 이름이 접두부로 추가된 프로파일을 검사합니다. 찾을 수 없는 경우 큐 공유 그룹 이름의 접두부가 추가된 프로파일을 검색합니다.

큐 관리자 레벨로 명령 프로파일을 설정하여 사용자는 특정 큐 관리자에서 명령이 발행되는 것을 제한할 수 있습니다. 또는 각 명령 verb에 대해 큐 공유 그룹을 위한 한 개의 프로파일을 정의하고 모든 보안 검사는 개별 큐 관리자가 아니라 해당 프로파일에 대해 수행되도록 할 수 있습니다.

서브시스템 보안 및 큐 공유 그룹 보안 모두 활성화되고 로컬 프로파일은 없는 경우, 명령 보안 검사는 사용자가 큐 공유 그룹 프로파일에 대한 액세스 권한이 있는지를 확인하기 위해 수행됩니다.

CMDSCOPE 속성을 사용하여 명령을 큐 공유 그룹의 다른 큐 관리자에게 라우트하는 경우 보안은 명령이 실행되는 각 큐 관리자에서 검사되지만 명령이 입력되는 큐 관리자일 필요는 없습니다.

197 페이지의 표 49에서는 각 IBM MQ 명령에 대해 수행되는 명령 보안 검사에 필요한 프로파일 및 MQCMD5 클래스의 각 프로파일에 해당하는 액세스 레벨을 보여줍니다.

201 페이지의 표 50에서는 각 IBM MQ PCF 명령에 대해 수행되는 명령 보안 검사에 필요한 프로파일 및 MQCMD5 클래스의 각 프로파일에 해당하는 액세스 레벨을 보여줍니다.

표 49. MQSC 명령, 프로파일, 해당 액세스 레벨				
명령	MQCMD5에 대한 명령 프로파일	MQCMD5에 대한 액세스 레벨	MQADMIN 또는 MXADMIN에 대한 명령 자원 프로파일	MQADMIN 또는 MXADMIN에 대한 액세스 레벨
ALTER AUTHINFO	hlq.ALTER.AUTHINFO	ALTER	hlq.AUTHINFO.resourcenam e	ALTER
ALTER BUFFPOOL	hlq.ALTER.BUFFPOOL	ALTER	검사 안함	-
ALTER CFSTRUCT	hlq.ALTER.CFSTRUCT	ALTER	검사 안함	-
ALTER CHANNEL	hlq.ALTER.CHANNEL	ALTER	hlq.CHANNEL.channel	ALTER
ALTER NAMELIST	hlq.ALTER.NAMELIST	ALTER	hlq.NAMELIST.namelist	ALTER
ALTER PROCESS	hlq.ALTER.PROCESS	ALTER	hlq.PROCESS.process	ALTER
ALTER PSID	hlq.ALTER.PSID	ALTER	검사 안함	-
ALTER QALIAS	hlq.ALTER.QALIAS	ALTER	hlq.QUEUE.queue	ALTER
ALTER QLOCAL	hlq.ALTER.QLOCAL	ALTER	hlq.QUEUE.queue	ALTER
ALTER QMGR	hlq.ALTER.QMGR	ALTER	검사 안함	-
ALTER QMODEL	hlq.ALTER.QMODEL	ALTER	hlq.QUEUE.queue	ALTER
ALTER QREMOTE	hlq.ALTER.QREMOTE	ALTER	hlq.QUEUE.queue	ALTER
ALTER SECURITY	hlq.ALTER.SECURITY	ALTER	검사 안함	-
ALTER SMDS	hlq.ALTER.SMDS	ALTER	검사 안함	-
ALTER STGCLASS	hlq.ALTER.STGCLASS	ALTER	검사 안함	-
ALTER SUB	hlq.ALTER.SUB	ALTER	검사 안함	-
ALTER TOPIC	hlq.ALTER.TOPIC	ALTER	hlq.TOPIC.topic	ALTER
ALTER TRACE	hlq.ALTER.TRACE	ALTER	검사 안함	-
ARCHIVE LOG	hlq.ARCHIVE.LOG	CONTROL	검사 안함	-
BACKUP CFSTRUCT	hlq.BACKUP.CFSTRUCT	CONTROL	검사 안함	-
CLEAR QLOCAL	hlq.CLEAR.QLOCAL	ALTER	hlq.QUEUE.queue	ALTER
CLEAR TOPICSTR 201 페이지의 『3』	hlq.CLEAR.TOPICSTR	ALTER	hlq.TOPIC.topic	ALTER
DEFINE AUTHINFO	hlq.DEFINE.AUTHINFO	ALTER	hlq.AUTHINFO.resourcenam e	ALTER
DEFINE BUFFPOOL	hlq.DEFINE.BUFFPOOL	ALTER	검사 안함	-
DEFINE CFSTRUCT	hlq.DEFINE.CFSTRUCT	ALTER	검사 안함	-
DEFINE CHANNEL	hlq.DEFINE.CHANNEL	ALTER	hlq.CHANNEL.channel	ALTER
DEFINE LOG	hlq.DEFINE.LOG	ALTER	검사 안함	-
DEFINE MAXSMGS	hlq.DEFINE.MAXSMGS	ALTER	검사 안함	-

표 49. MQSC 명령, 프로파일, 해당 액세스 레벨 (계속)				
명령	MQCMDs에 대한 명령 프로파일	MQCMDs에 대한 액세스 레벨	MQADMIN 또는 MXADMIN에 대한 명령 자원 프로파일	MQADMIN 또는 MXADMIN에 대한 액세스 레벨
DEFINE NAMELIST	hlq.DEFINE.NAMELIST	ALTER	hlq.NAMELIST.namelist	ALTER
DEFINE PROCESS	hlq.DEFINE.PROCESS	ALTER	hlq.PROCESS.process	ALTER
DEFINE PSID	hlq.DEFINE.PSID	ALTER	검사 안함	-
DEFINE QALIAS	hlq.DEFINE.QALIAS	ALTER	hlq.QUEUE.queue	ALTER
DEFINE QLOCAL	hlq.DEFINE.QLOCAL	ALTER	hlq.QUEUE.queue	ALTER
DEFINE QMODEL	hlq.DEFINE.QMODEL	ALTER	hlq.QUEUE.queue	ALTER
DEFINE QREMOTE	hlq.DEFINE.QREMOTE	ALTER	hlq.QUEUE.queue	ALTER
DEFINE STGCLASS	hlq.DEFINE.STGCLASS	ALTER	검사 안함	-
DEFINE SUB	hlq.DEFINE.SUB	ALTER	검사 안함	-
DEFINE TOPIC	hlq.DEFINE.TOPIC	ALTER	hlq.TOPIC.topic	ALTER
DELETE AUTHINFO	hlq.DELETE.AUTHINFO	ALTER	hlq.AUTHINFO.resourcenam e	ALTER
DELETE BUFFPOOL	hlq.DELETE.BUFFPOOL	ALTER	검사 안함	-
DELETE CFSTRUCT	hlq.DELETE.CFSTRUCT	ALTER	검사 안함	-
DELETE CHANNEL	hlq.DELETE.CHANNEL	ALTER	hlq.CHANNEL.channel	ALTER
DELETE NAMELIST	hlq.DELETE.NAMELIST	ALTER	hlq.NAMELIST.namelist	ALTER
DELETE PROCESS	hlq.DELETE.PROCESS	ALTER	hlq.PROCESS.process	ALTER
DELETE PSID	hlq.DELETE.PSID	ALTER	검사 안함	-
DELETE QALIAS	hlq.DELETE.QALIAS	ALTER	hlq.QUEUE.queue	ALTER
DELETE QLOCAL	hlq.DELETE.QLOCAL	ALTER	hlq.QUEUE.queue	ALTER
DELETE QMODEL	hlq.DELETE.QMODEL	ALTER	hlq.QUEUE.queue	ALTER
DELETE QREMOTE	hlq.DELETE.QREMOTE	ALTER	hlq.QUEUE.queue	ALTER
DELETE STGCLASS	hlq.DELETE.STGCLASS	ALTER	검사 안함	-
DELETE SUB	hlq.DELETE.SUB	ALTER	검사 안함	-
DELETE TOPIC	hlq.DELETE.TOPIC	ALTER	hlq.TOPIC.topic	ALTER
DISPLAY ARCHIVE 201 페이지의 『1』	hlq.DISPLAY.ARCHIVE	READ	검사 안함	-
DISPLAY AUTHINFO	hlq.DISPLAY.AUTHINFO	READ	검사 안함	-
DISPLAY CFSTATUS	hlq.DISPLAY.CFSTATUS	READ	검사 안함	-
DISPLAY CFSTRUCT	hlq.DISPLAY.CFSTRUCT	READ	검사 안함	-
DISPLAY CHANNEL	hlq.DISPLAY.CHANNEL	READ	검사 안함	-
DISPLAY CHINIT	hlq.DISPLAY.CHINIT	READ	검사 안함	-

표 49. MQSC 명령, 프로파일, 해당 액세스 레벨 (계속)				
명령	MQCMDS에 대한 명령 프로파일	MQCMDS에 대한 액세스 레벨	MQADMIN 또는 MXADMIN에 대한 명령 자원 프로파일	MQADMIN 또는 MXADMIN에 대한 액세스 레벨
DISPLAY CHLAUTH	hlq.DISPLAY.CHLAUTH	READ	검사 안함	-
DISPLAY CHSTATUS	hlq.DISPLAY.CHSTATUS	READ	검사 안함	-
DISPLAY CLUSQMGR	hlq.DISPLAY.CLUSQMGR	READ	검사 안함	-
DISPLAY CMDSERV	hlq.DISPLAY.CMDSERV	READ	검사 안함	-
DISPLAY CONN 201 페이지의 『1』	hlq.DISPLAY.CONN	READ	검사 안함	-
DISPLAY GROUP	hlq.DISPLAY.GROUP	READ	검사 안함	-
DISPLAY LOG 201 페이지의 『1』	hlq.DISPLAY.LOG	READ	검사 안함	-
DISPLAY MAXSMSGS	hlq.DISPLAY.MAXSMSGS	READ	검사 안함	-
DISPLAY NAMELIST	hlq.DISPLAY.NAMELIST	READ	검사 안함	-
DISPLAY PROCESS	hlq.DISPLAY.PROCESS	READ	검사 안함	-
DISPLAY PUBSUB	hlq.DISPLAY.PUBSUB	READ	검사 안함	-
DISPLAY QALIAS	hlq.DISPLAY.QALIAS	READ	검사 안함	-
DISPLAY QCLUSTER	hlq.DISPLAY.QCLUSTER	READ	검사 안함	-
DISPLAY QLOCAL	hlq.DISPLAY.QLOCAL	READ	검사 안함	-
DISPLAY QMGR	hlq.DISPLAY.QMGR	READ	검사 안함	-
DISPLAY QMODEL	hlq.DISPLAY.QMODEL	READ	검사 안함	-
DISPLAY QREMOTE	hlq.DISPLAY.QREMOTE	READ	검사 안함	-
DISPLAY QSTATUS	hlq.DISPLAY.QSTATUS	READ	검사 안함	-
DISPLAY QUEUE	hlq.DISPLAY.QUEUE	READ	검사 안함	-
DISPLAY SBSTATUS	hlq.DISPLAY.SBSTATUS	READ	검사 안함	-
DISPLAY SMDS	hlq.DISPLAY.SMDS	READ	검사 안함	-
DISPLAY SMDSCONN	hlq.DISPLAY.SMDSCONN	READ	검사 안함	-
DISPLAY SUB	hlq.DISPLAY.SUB	READ	검사 안함	-
DISPLAY SECURITY	hlq.DISPLAY.SECURITY	READ	검사 안함	-
DISPLAY STGCLASS	hlq.DISPLAY.STGCLASS	READ	검사 안함	-
DISPLAY SYSTEM 201 페이지의 『1』	hlq.DISPLAY.SYSTEM	READ	검사 안함	-
DISPLAY THREAD	hlq.DISPLAY.THREAD	READ	검사 안함	-
DISPLAY TPSTATUS	hlq.DISPLAY.TPSTATUS	READ	검사 안함	-
DISPLAY TOPIC	hlq.DISPLAY.TOPIC	READ	검사 안함	-
DISPLAY TPSTATUS	hlq.DISPLAY.TPSTATUS	READ	검사 안함	-

표 49. MQSC 명령, 프로파일, 해당 액세스 레벨 (계속)				
명령	MQCMDS에 대한 명령 프로파일	MQCMDS에 대한 액세스 레벨	MQADMIN 또는 MXADMIN에 대한 명령 자원 프로파일	MQADMIN 또는 MXADMIN에 대한 액세스 레벨
DISPLAY TRACE	hlq.DISPLAY.TRACE	READ	검사 안함	-
DISPLAY USAGE 201 페이지의 『1』	hlq.DISPLAY.USAGE	READ	검사 안함	-
MOVE QLOCAL	hlq.MOVE.QLOCAL	ALTER	hlq.QUEUE.from-queue hlq.QUEUE.to-queue	ALTER
PING CHANNEL	hlq.PING.CHANNEL	CONTROL	hlq.CHANNEL.channel	CONTROL
RECOVER BSDS	hlq.RECOVER.BSDS	CONTROL	검사 안함	-
RECOVER CFSTRUCT	hlq.RECOVER.CFSTRUCT	CONTROL	검사 안함	-
REFRESH CLUSTER	hlq.REFRESH.CLUSTER	ALTER	검사 안함	-
REFRESH QMGR	hlq.REFRESH.QMGR	ALTER	검사 안함	-
REFRESH SECURITY	hlq.REFRESH.SECURITY	ALTER	검사 안함	-
RESET CFSTRUCT	hlq.RESET.CFSTRUCT	CONTROL	검사 안함	-
RESET CHANNEL	hlq.RESET.CHANNEL	CONTROL	hlq.CHANNEL.channel	CONTROL
RESET CLUSTER	hlq.RESET.CLUSTER	CONTROL	검사 안함	-
RESET QMGR	hlq.RESET.QMGR	CONTROL	검사 안함	-
RESET QSTATS	hlq.RESET.QSTATS	CONTROL	hlq.QUEUE.queue	CONTROL
RESET SMDS	hlq.RESET.SMDS	CONTROL	검사 안함	-
RESET TPIPE	hlq.RESET.TPIPE	CONTROL	검사 안함	-
RESOLVE CHANNEL	hlq.RESOLVE.CHANNEL	CONTROL	hlq.CHANNEL.channel	CONTROL
RESOLVE INDOUBT	hlq.RESOLVE.INDOUBT	CONTROL	검사 안함	-
RESUME QMGR	hlq.RESUME.QMGR	CONTROL	검사 안함	-
RVERIFY SECURITY	hlq.RVERIFY.SECURITY	ALTER	검사 안함	-
SET ARCHIVE	hlq.SET.ARCHIVE	CONTROL	검사 안함	-
SET CHLAUTH	hlq.SET.CHLAUTH	CONTROL	검사 안함	-
SET LOG	hlq.SET.LOG	CONTROL	검사 안함	-
SET SYSTEM	hlq.SET.SYSTEM	CONTROL	검사 안함	-
START CHANNEL	hlq.START.CHANNEL	CONTROL	hlq.CHANNEL.channel	CONTROL
START CHINIT 201 페이지의 『4』	hlq.START.CHINIT	CONTROL	검사 안함	-
START CMDSERV	hlq.START.CMDSERV	CONTROL	검사 안함	-
START LISTENER	hlq.START.LISTENER	CONTROL	검사 안함	-
START QMGR	없음 201 페이지의 『2』	-	-	-
START SMDSCONN	hlq.START.SMDSCONN	CONTROL	검사 안함	-

명령	MQCMDS에 대한 명령 프로파일	MQCMDS에 대한 액세스 레벨	MQADMIN 또는 MXADMIN에 대한 명령 자원 프로파일	MQADMIN 또는 MXADMIN에 대한 액세스 레벨
START TRACE	hlq.START.TRACE	CONTROL	검사 안함	-
STOP CHANNEL	hlq.STOP.CHANNEL	CONTROL	hlq.CHANNEL.channel	CONTROL
STOP CHINIT	hlq.STOP.CHINIT	CONTROL	검사 안함	-
STOP CMDSERV	hlq.STOP.CMDSERV	CONTROL	검사 안함	-
STOP LISTENER	hlq.STOP.LISTENER	CONTROL	검사 안함	-
STOP QMGR	hlq.STOP.QMGR	CONTROL	검사 안함	-
STOP SMDSCONN	hlq.STOP.SMDSCONN	CONTROL	검사 안함	-
STOP TRACE	hlq.STOP.TRACE	CONTROL	검사 안함	-
SUSPEND QMGR	hlq.SUSPEND.QMGR	CONTROL	검사 안함	-

참고사항:

- 해당 명령은 큐 관리자에서 내부적으로 발행될 수 있으며 이런 경우 권한이 검사되지 않습니다.
- IBM MQ는 START QMGR 명령을 발행하는 사용자의 권한을 검사하지 않습니다. 그렇지만 RACF 또는 대체 보안 기능을 사용하여 START QMGR 명령 결과로 발행되는 START xxxxMSTR 명령 액세스를 제어할 수 있습니다. 이는 RACF 연산자 명령(OPERCMDS) 클래스에서 MVS.START.STC.xxxxMSTR 프로파일 액세스를 제어하여 수행합니다. 이 프로시저에 대한 자세한 내용은 *z/OS SecureWay Security Server RACF Security Administrator's Guide*를 참조하십시오. 이 기술을 사용하고 권한 없는 사용자가 큐 관리자 시작을 시도하면 이유 코드 00F30216으로 종료됩니다.
- hlq.TOPIC.topic** 자원은 TOPICSTR에서 도출된 토픽 오브젝트를 참조합니다. 자세한 정보는 417 페이지의 『[발행/구독 보안](#)』의 내용을 참조하십시오.
- IBM MQ for z/OS V6 이전의 릴리스에서 MVS.START.STC.CSQ1CHIN에 대한 보안 검사. IBM MQ for z/OS V6 이상에서 자원 이름에는 추가 JOBNAME 규정이 추가되었습니다. 이로 인해 채널 시작기 시작 시에 문제가 발행할 수 있습니다.

문제를 해결하려면 MVS.START.STC를 바꾸십시오. *ssid* CHIN - MVS.START.STC라는 자원의 프로파일 포함. *ssid* CHIN.* 또는 MVS.START.STC를 선택하십시오. *ssid* CHIN. *ssid* CHIN. 여기서 *ssid*는 큐 관리자의 하위 시스템 ID입니다. 이 경우, RACF UPDATE 권한이 필요합니다. 자세한 내용은 [조작 계획, MVS 명령, RACF 액세스 권한 및 자원 이름에 대한 z/OS 제품 문서](#)를 참조하십시오.

ssid MSTR에 대한 START는 JOBNAME= 매개변수를 포함하지 않습니다. 일관성을 위해 MVS.START.STC.*ssid*MSTR에 대한 프로파일을 MVS.START.STC.*ssid*MSTR.*로 업데이트할 수도 있습니다.

명령	MQCMDS에 대한 명령 프로파일	MQCMDS에 대한 액세스 레벨	MQADMIN 또는 MXADMIN에 대한 명령 자원 프로파일	MQADMIN 또는 MXADMIN에 대한 액세스 레벨
백업 CF 구조	hlq.BACKUP.CFSTRUCT	CONTROL	검사 안함	-
인증 정보 오브젝트 변경	hlq.ALTER.AUTHINFO	ALTER	hlq.AUTHINFO.resourcename	ALTER
CF 구조 변경	hlq.ALTER.CFSTRUCT	ALTER	검사 안함	-
채널 변경	hlq.ALTER.CHANNEL	ALTER	hlq.CHANNEL.channel	ALTER

표 50. PCF 명령, 프로파일, 해당 액세스 레벨 (계속)

명령	MQCMDs에 대한 명령 프로파일	MQCMDs에 대한 액세스 레벨	MQADMIN 또는 MXADMIN에 대한 명령 자원 프로파일	MQADMIN 또는 MXADMIN에 대한 액세스 레벨
이름 목록 변경	hlq.ALTER.NAMELIST	ALTER	hlq.NAMELIST.namelist	ALTER
프로세스 변경	hlq.ALTER.PROCESS	ALTER	hlq.PROCESS.process	ALTER
큐 변경	hlq.ALTER.QUEUE	ALTER	hlq.QUEUE.queue	ALTER
큐 관리자 변경	hlq.ALTER.QMGR	ALTER	검사 안함	-
보안 변경	hlq.ALTER.SECURITY	ALTER	검사 안함	-
SMDS 변경	hlq.ALTER.SMDS	ALTER	검사 안함	-
스토리지 클래스 변경	hlq.ALTER.STGCLASS	ALTER	검사 안함	-
구독 변경	hlq.ALTER.SUB	ALTER	검사 안함	-
토픽 변경	hlq.ALTER.TOPIC	ALTER	hlq.TOPIC.topic	ALTER
큐 지우기	hlq.CLEAR.QLOCAL	ALTER	hlq.QUEUE.queue	ALTER
토픽 문자열 지우기 205 페이지의 『1』	hlq.CLEAR.TOPICSTR	ALTER	hlq.TOPIC.topic	ALTER
인증 정보 오브젝트 복사	hlq.DEFINE.AUTHINFO	ALTER	hlq.AUTHINFO.resourcename	ALTER
CF 구조 복사	hlq.DEFINE.CFSTRUCT	ALTER	검사 안함	-
채널 복사	hlq.DEFINE.CHANNEL	ALTER	hlq.CHANNEL.channel	ALTER
이름 목록 복사	hlq.DEFINE.NAMELIST	ALTER	hlq.NAMELIST.namelist	ALTER
프로세스 복사	hlq.DEFINE.PROCESS	ALTER	hlq.PROCESS.process	ALTER
큐 복사	hlq.DEFINE.QUEUE	ALTER	hlq.QUEUE.queue	ALTER
구독 복사	hlq.DEFINE.SUB	ALTER	검사 안함	-
스토리지 클래스 복사	hlq.DEFINE.STGCLASS	ALTER	검사 안함	-
토픽 복사	hlq.DEFINE.TOPIC	ALTER	hlq.TOPIC.topic	ALTER
인증 정보 오브젝트 작성	hlq.DEFINE.AUTHINFO	ALTER	hlq.AUTHINFO.resourcename	ALTER
CF 구조 작성	hlq.DEFINE.CFSTRUCT	ALTER	검사 안함	-
채널 작성	hlq.DEFINE.CHANNEL	ALTER	hlq.CHANNEL.channel	ALTER
이름 목록 작성	hlq.DEFINE.NAMELIST	ALTER	hlq.NAMELIST.namelist	ALTER
프로세스 작성	hlq.DEFINE.PROCESS	ALTER	hlq.PROCESS.process	ALTER
큐 작성	hlq.DEFINE.QUEUE	ALTER	hlq.QUEUE.queue	ALTER
스토리지 클래스 작성	hlq.DEFINE.STGCLASS	ALTER	검사 안함	-
구독 작성	hlq.DEFINE.SUB	ALTER	검사 안함	-
토픽 작성	hlq.DEFINE.TOPIC	ALTER	hlq.TOPIC.topic	ALTER
인증 정보 오브젝트 삭제	hlq.DELETE.AUTHINFO	ALTER	hlq.AUTHINFO.resourcename	ALTER
CF 구조 삭제	hlq.DELETE.CFSTRUCT	ALTER	검사 안함	-
채널 삭제	hlq.DELETE.CHANNEL	ALTER	hlq.CHANNEL.channel	ALTER
이름 목록 삭제	hlq.DELETE.NAMELIST	ALTER	hlq.NAMELIST.namelist	ALTER
프로세스 삭제	hlq.DELETE.PROCESS	ALTER	hlq.PROCESS.process	ALTER

표 50. PCF 명령, 프로파일, 해당 액세스 레벨 (계속)

명령	MQCMLS에 대한 명령 프로파일	MQCMLS에 대한 액세스 레벨	MQADMIN 또는 MXADMIN에 대한 명령 자원 프로파일	MQADMIN 또는 MXADMIN에 대한 액세스 레벨
큐 삭제	hlq.DELETE.QUEUE	ALTER	hlq.QUEUE.queue	ALTER
스토리지 클래스 삭제	hlq.DELETE.STGCLASS	ALTER	검사 안함	-
구독 삭제	hlq.DELETE.SUB	ALTER	검사 안함	-
토픽 삭제	hlq.DELETE.TOPIC	ALTER	hlq.TOPIC.topic	ALTER
아카이브 조회	hlq.DISPLAY.ARCHIVE	READ	검사 안함	-
인증 정보 오브젝트 조회	hlq.DISPLAY.AUTHINFO	READ	검사 안함	-
인증 정보 오브젝트 이름 조회	hlq.DISPLAY.AUTHINFO	READ	검사 안함	-
CF 구조 조회	hlq.DISPLAY.CFSTRUCT	READ	검사 안함	-
CF 구조 이름 조회	hlq.DISPLAY.CFSTRUCT	READ	검사 안함	-
CF 구조 상태 조회	hlq.DISPLAY.CFSTATUS	READ	검사 안함	-
채널 조회	hlq.DISPLAY.CHANNEL	READ	검사 안함	-
채널 인증 레코드 조회	hlq.DISPLAY.CHLAUTH	READ	검사 안함	-
채널 시작기 조회	hlq.DISPLAY.CHINIT	READ	검사 안함	-
채널 이름 조회	hlq.DISPLAY.CHANNEL	READ	검사 안함	-
채널 상태 조회	hlq.DISPLAY.CHSTATUS	READ	검사 안함	-
클러스터 큐 관리자 조회	hlq.DISPLAY.CLUSQMGR	READ	검사 안함	-
연결 조회	hlq.DISPLAY.CONNPCF	READ	검사 안함	-
그룹 조회	hlq.DISPLAY.GROUP	READ	검사 안함	-
로그 조회	hlq.DISPLAY.LOG	READ	검사 안함	-
이름 목록 조회	hlq.DISPLAY.NAMELIST	READ	검사 안함	-
이름 목록 이름 조회	hlq.DISPLAY.NAMELIST	READ	검사 안함	-
프로세스 조회	hlq.DISPLAY.PROCESS	READ	검사 안함	-
프로세스 이름 조회	hlq.DISPLAY.PROCESS	READ	검사 안함	-
발행/구독 상태 조회	hlq.DISPLAY.PUBSUB	READ	검사 안함	-
큐 조회	hlq.DISPLAY.QUEUE	READ	검사 안함	-
큐 관리자 조회	hlq.DISPLAY.QMGR	READ	검사 안함	-
큐 이름 조회	hlq.DISPLAY.QUEUE	READ	검사 안함	-
큐 상태 조회	hlq.DISPLAY.QSTATUS	READ	검사 안함	-
보안 조회	hlq.DISPLAY.SECURITY	READ	검사 안함	-
SMDS 조회	hlq.DISPLAY.SMDS	READ	검사 안함	-
SMDSCONN 조회	hlq.DISPLAY.SMDSCONN	READ	검사 안함	-
스토리지 클래스 조회	hlq.DISPLAY.STGCLASS	READ	검사 안함	-
스토리지 클래스 이름 조회	hlq.DISPLAY.STGCLASS	READ	검사 안함	-

표 50. PCF 명령, 프로파일, 해당 액세스 레벨 (계속)

명령	MQCMLS에 대한 명령 프로파일	MQCMLS에 대한 액세스 레벨	MQADMIN 또는 MXADMIN에 대한 명령 자원 프로파일	MQADMIN 또는 MXADMIN에 대한 액세스 레벨
구독 조회	hlq.INQUIRE.SUB	READ	검사 안함	-
구독 상태 조회	hlq.INQUIRE.SBSTATUS	READ	검사 안함	-
시스템 조회	hlq.DISPLAY.SYSTEM	READ	검사 안함	-
토픽 조회	hlq.DISPLAY.TOPIC	READ	검사 안함	-
토픽 이름 조회	hlq.DISPLAY.TOPIC	READ	검사 안함	-
토픽 상태 조회	hlq.DISPLAY.TPSTATUS	READ	검사 안함	-
사용 조회	hlq.DISPLAY.USAGE	READ	검사 안함	-
큐 이동	hlq.MOVE.QLOCAL	ALTER	hlq.QUEUE.from-queue hlq.QUEUE.to-queue	ALTER
채널 ping	hlq.PING.CHANNEL	CONTROL	hlq.CHANNEL.channel	CONTROL
CF 구조 복구	hlq.RECOVER.CFSTRUCT	CONTROL	검사 안함	-
클러스터 새로 고치기	hlq.REFRESH.CLUSTER	ALTER	검사 안함	-
큐 관리자 새로 고치기	hlq.REFRESH.QMGR	ALTER	검사 안함	-
보안 새로 고치기	hlq.REFRESH.SECURITY	ALTER	검사 안함	-
CF 구조 재설정	hlq.RESET.CFSTRUCT	CONTROL	검사 안함	-
채널 재설정	hlq.RESET.CHANNEL	CONTROL	hlq.CHANNEL.channel	CONTROL
클러스터 재설정	hlq.RESET.CLUSTER	CONTROL	검사 안함	-
큐 관리자 재설정	hlq.RESET.QMGR	CONTROL	검사 안함	-
큐 통계 재설정	hlq.RESET.QSTATS	CONTROL	hlq.QUEUE.queue	CONTROL
SMDS 재설정	hlq.RESET.SMDS	CONTROL	검사 안함	-
채널 분석	hlq.RESOLVE.CHANNEL	CONTROL	hlq.CHANNEL.channel	CONTROL
큐 관리자 재개	hlq.RESUME.QMGR	CONTROL	검사 안함	-
큐 관리자 클러스터 재개	hlq.RESUME.QMGR	CONTROL	검사 안함	-
보안 재확인	hlq.RVERIFY.SECURITY	ALTER	검사 안함	-
아카이브 설정	hlq.SET.ARCHIVE	CONTROL	검사 안함	-
채널 인증 레코드 설정	hlq.SET.CHLAUTH	CONTROL	검사 안함	-
로그 설정	hlq.SET.LOG	CONTROL	검사 안함	-
시스템 설정	hlq.SET.SYSTEM	CONTROL	검사 안함	-
채널 시작	hlq.START.CHANNEL	CONTROL	hlq.CHANNEL.channel	CONTROL
채널 시작기 시작	hlq.START.CHINIT	CONTROL	검사 안함	-
채널 리스너 시작	hlq.START.LISTENER	CONTROL	검사 안함	-
SMDS 연결 시작	hlq.START.SMDSCONN	CONTROL	검사 안함	-
채널 중지	hlq.STOP.CHANNEL	CONTROL	hlq.CHANNEL.channel	CONTROL
채널 시작기 중지	hlq.STOP.CHINIT	CONTROL	검사 안함	-
채널 리스너 중지	hlq.STOP.LISTENER	CONTROL	검사 안함	-

표 50. PCF 명령, 프로파일, 해당 액세스 레벨 (계속)

명령	MQCMDMS에 대한 명령 프로파일	MQCMDMS에 대한 액세스 레벨	MQADMIN 또는 MXADMIN에 대한 명령 자원 프로파일	MQADMIN 또는 MXADMIN에 대한 액세스 레벨
SMDS 연결 중지	hlq.STOP.SMDSCONN	CONTROL	검사 안함	-
큐 관리자 일시중단	hlq.SUSPEND.QMGR	CONTROL	검사 안함	-
큐 관리자 클러스터 일시 중단	hlq.SUSPEND.QMGR	CONTROL	검사 안함	-

참고사항:

1. **hlq.TOPIC.topic** 자원은 TOPICSTR에서 도출된 토픽 오브젝트를 참조합니다. 자세한 정보는 417 페이지의 『발행/구독 보안』의 내용을 참조하십시오.

V 9.1.0 IBM MQ Console를 사용할 때 필요한 IBM MQ PCF 프로파일에 대한 자세한 내용은 205 페이지의 『IBM MQ Console - 필수 명령 보안 프로파일』를 참조하십시오.

z/OS V 9.1.0 IBM MQ Console - 필수 명령 보안 프로파일

MQWebAdmin 또는 MQWebAdminRO의 사용자가 IBM MQ Console에서 수행하는 조작은 mqweb 서버 시작 태스크 사용자 ID의 보안 컨텍스트에서 수행됩니다. IBM MQ Console을 사용하려면 mqweb 서버의 시작된 태스크 사용자 ID에 특정 PCF 명령을 실행하는 권한이 필요합니다.

205 페이지의 표 51에서는 각 IBM MQ PCF 명령에 대해 필요한 명령 보안 프로파일 및 IBM MQ Console에 필요한 MQCMDMS 클래스의 각 프로파일에 해당하는 액세스 레벨을 표시합니다.

표 51. IBM MQ Console PCF 명령, 프로파일 및 해당 액세스 레벨

명령	MQCMDMS에 대한 명령 프로파일	MQCMDMS에 대한 액세스 레벨	MQADMIN 또는 MXADMIN에 대한 명령 자원 프로파일	MQADMIN 또는 MXADMIN에 대한 액세스 레벨
인증 정보 오브젝트 변경	hlq.ALTER.AUTHINFO	ALTER	hlq.AUTHINFO.resourcename	ALTER
채널 변경	hlq.ALTER.CHANNEL	ALTER	hlq.CHANNEL.channel	ALTER
큐 변경	hlq.ALTER.QUEUE	ALTER	hlq.QUEUE.queue	ALTER
큐 관리자 변경	hlq.ALTER.QMGR	ALTER	검사 안함	-
토픽 변경	hlq.ALTER.TOPIC	ALTER	hlq.TOPIC.topic	ALTER
큐 지우기	hlq.CLEAR.QLOCAL	ALTER	hlq.QUEUE.queue	ALTER
인증 정보 오브젝트 작성	hlq.DEFINE.AUTHINFO	ALTER	hlq.AUTHINFO.resourcename	ALTER
채널 작성	hlq.DEFINE.CHANNEL	ALTER	hlq.CHANNEL.channel	ALTER
큐 작성	hlq.DEFINE.QUEUE	ALTER	hlq.QUEUE.queue	ALTER
구독 작성	hlq.DEFINE.SUB	ALTER	검사 안함	-
토픽 작성	hlq.DEFINE.TOPIC	ALTER	hlq.TOPIC.topic	ALTER
인증 정보 오브젝트 삭제	hlq.DELETE.AUTHINFO	ALTER	hlq.AUTHINFO.resourcename	ALTER
채널 삭제	hlq.DELETE.CHANNEL	ALTER	hlq.CHANNEL.channel	ALTER
큐 삭제	hlq.DELETE.QUEUE	ALTER	hlq.QUEUE.queue	ALTER
구독 삭제	hlq.DELETE.SUB	ALTER	검사 안함	-
토픽 삭제	hlq.DELETE.TOPIC	ALTER	hlq.TOPIC.topic	ALTER

표 51. IBM MQ Console PCF 명령, 프로파일 및 해당 액세스 레벨 (계속)

명령	MQCMDS에 대한 명령 프로파일	MQCMDS에 대한 액세스 레벨	MQADMIN 또는 MXADMIN에 대한 명령 자원 프로파일	MQADMIN 또는 MXADMIN에 대한 액세스 레벨
인증 정보 오브젝트 조회	hlq.DISPLAY.AUTHINFO	READ	검사 안함	-
인증 정보 오브젝트 이름 조회	hlq.DISPLAY.AUTHINFO	READ	검사 안함	-
채널 조회	hlq.DISPLAY.CHANNEL	READ	검사 안함	-
채널 인증 레코드 조회	hlq.DISPLAY.CHLAUTH	READ	검사 안함	-
채널 시작기 조회	hlq.DISPLAY.CHINIT	READ	검사 안함	-
채널 이름 조회	hlq.DISPLAY.CHANNEL	READ	검사 안함	-
채널 상태 조회	hlq.DISPLAY.CHSTATUS	READ	검사 안함	-
큐 조회	hlq.DISPLAY.QUEUE	READ	검사 안함	-
큐 관리자 조회	hlq.DISPLAY.QMGR	READ	검사 안함	-
큐 이름 조회	hlq.DISPLAY.QUEUE	READ	검사 안함	-
큐 상태 조회	hlq.DISPLAY.QSTATUS	READ	검사 안함	-
구독 조회	hlq.INQUIRE.SUB	READ	검사 안함	-
구독 상태 조회	hlq.INQUIRE.SBSTATUS	READ	검사 안함	-
토픽 조회	hlq.DISPLAY.TOPIC	READ	검사 안함	-
토픽 이름 조회	hlq.DISPLAY.TOPIC	READ	검사 안함	-
토픽 상태 조회	hlq.DISPLAY.TPSTATUS	READ	검사 안함	-
채널 ping	hlq.PING.CHANNEL	CONTROL	hlq.CHANNEL.channel	CONTROL
클러스터 새로 고치기	hlq.REFRESH.CLUSTER	ALTER	검사 안함	-
보안 새로 고치기	hlq.REFRESH.SECURITY	ALTER	검사 안함	-
채널 재설정	hlq.RESET.CHANNEL	CONTROL	hlq.CHANNEL.channel	CONTROL
채널 분석	hlq.RESOLVE.CHANNEL	CONTROL	hlq.CHANNEL.channel	CONTROL
채널 인증 레코드 설정	hlq.SET.CHLAUTH	CONTROL	검사 안함	-
채널 시작	hlq.START.CHANNEL	CONTROL	hlq.CHANNEL.channel	CONTROL
채널 중지	hlq.STOP.CHANNEL	CONTROL	hlq.CHANNEL.channel	CONTROL

z/OS 명령 자원 보안을 위한 프로파일

명령에 연관된 자원에 대해 보안 검사를 수행하기 때문에 명령 자원 보안 스위치 프로파일을 정의하지 않은 경우, 각 자원에 대한 자원 프로파일을 해당 클래스에 추가해야 합니다. 동일한 보안 프로파일이 MQSC와 PCF 명령 모두를 제어합니다.

명령에 연관된 자원에 대해 보안 검사를 수행하기 때문에 명령 자원 보안 스위치 프로파일 hlq.NO.CMD.RESC.CHECKS를 정의하지 않은 경우, 다음을 수행해야 합니다.

- 대문자 프로파일을 사용 중인 경우 각 자원에 대해 **MQADMIN** 클래스에 자원 프로파일을 추가하십시오.
- 대소문자 혼합 프로파일을 사용 중인 경우 각 자원에 대해 **MXADMIN** 클래스에 자원 프로파일을 추가하십시오.

동일한 보안 프로파일이 MQSC와 PCF 명령 모두를 제어합니다.

명령 자원 보안 검사에 대한 프로파일은 다음 양식을 사용합니다.

hlq.type.resourcename

여기서 hlq는 qmgr-name(큐 관리자 이름) 또는 qsg-name(큐 공유 그룹 이름)입니다.

큐 관리자 이름이 접두부로 추가된 프로파일은 해당 큐 관리자에서 명령에 연관된 자원에 대한 액세스를 제어합니다. 큐 공유 그룹 이름의 접두부가 추가된 프로파일은 큐 공유 그룹 내의 모든 큐 관리자에서 명령에 연관된 자원 액세스를 제어합니다. 이 액세스는 해당 큐 관리자에서 이 명령 자원에 대해 큐 관리자 레벨 프로파일을 정의하여 개별 큐 관리자에서 대체 가능합니다.

큐 관리자가 큐 공유 그룹의 멤버이고 큐 관리자와 큐 공유 그룹 레벨 보안을 모두 사용하는 경우 IBM MQ는 큐 관리자 이름이 접두부로 추가된 프로파일을 먼저 검사합니다. 찾을 수 없는 경우 큐 공유 그룹 이름의 접두부가 추가된 프로파일을 검색합니다.

예를 들어, 서브시스템 CSQ1에서 모델 큐 CREDIT.WORTHY에 대한 명령 자원 보안 검사용 RACF 프로파일 이름은 다음과 같습니다.

CSQ1.QUEUE.CREDIT.WORTHY

모든 유형의 명령 자원의 프로파일이 MQADMIN 클래스에서 보유되기 때문에 프로파일 이름의 "유형" 파트가 동일한 이름의 다른 유형 자원 사이를 구분하기 위해 프로파일에서 필요합니다. 프로파일 이름의 "유형" 파트는 CHANNEL, QUEUE, TOPIC, PROCESS 또는 NAMELIST입니다. 예를 들어, 사용자가 hlq.QUEUE.PAYROLL.ONE을 정의할 권한은 있지만 hlq.PROCESS.PAYROLL.ONE을 정의할 권한은 없습니다.

자원 유형이 큐이고 프로파일은 큐 공유 그룹 레벨 프로파일인 경우, 큐 공유 그룹 내에서 하나 이상의 로컬 큐에 대한 액세스를 제어하거나 큐 공유 그룹에서 임의 큐 관리자의 단일 공유 큐에 대한 액세스를 제어합니다.

z/OS MQSC 명령, 프로파일, 해당 액세스 레벨은 각 IBM MQ MQSC 명령에 대해 수행되는 명령 보안 검사에 필요한 프로파일 및 MQCMDS 클래스의 각 프로파일에 대한 해당 액세스 레벨을 보여줍니다.

z/OS PCF 명령, 프로파일, 해당 액세스 레벨은 각 IBM MQ PCF 명령에 대해 수행되는 명령 보안 검사에 필요한 프로파일 및 MQCMDS 클래스의 각 프로파일에 대한 해당 액세스 레벨을 보여줍니다.

z/OS 알리어스 큐 및 리모트 큐를 검사하는 명령 자원 보안
알리어스 큐 및 리모트 큐는 둘 다 다른 큐에 대한 간접화를 제공합니다. 해당 큐에 대해 보안 검사를 고려할 때 추가 지점이 적용됩니다.

알리어스 큐

알리어스 큐를 정의할 때 명령 자원 보안 검사는 알리어스가 해결되는 대상 큐 이름이 아니라 알리어스 큐 이름에 대해서만 수행됩니다.

알리어스 큐는 로컬 및 리모트 큐 모두에 대해 해결 가능합니다. 특정 로컬이나 리모트 큐에 대해 사용자 액세스를 허용하지 않으려면 다음 둘 다를 수행해야 합니다.

1. 해당 로컬 및 리모트 큐에 대해 사용자 액세스를 허용하지 마십시오.
2. 사용자가 해당 큐에 대해 알리어스를 정의하지 못하도록 제한하십시오. 즉, DEFINE QALIAS 및 ALTER QALIAS 명령을 발행하는 것을 금지하십시오.

리모트 큐

리모트 큐를 정의할 때 명령 자원 보안 검사는 리모트 큐 이름에 대해서만 수행됩니다. 리모트 큐 오브젝트 정의의 RNAME 또는 XMITQ 속성에 지정된 큐 이름에 대해서는 검사가 수행되지 않습니다.

z/OS RESLEVEL 보안 프로파일

API 자원 보안에 대해 검사되는 사용자 ID 수를 제어하기 위해 MQADMIN 또는 MXADMIN 클래스에 특수 프로파일을 정의할 수 있습니다. 이 프로파일을 RESLEVEL 프로파일이라고 합니다. 이 프로파일이 API 자원 보안에 영향을 주는 방법은 IBM MQ에 대한 액세스 방법에 따라 다릅니다.

애플리케이션이 IBM MQ 연결을 시도하면 IBM MQ는 연결에 연관된 사용자 ID가 호출된 MQADMIN 또는 MXADMIN 클래스에 프로파일에 대해 가지는 액세스를 검사합니다.

hlq.RESLEVEL

여기서 hlq는 ssid(서브시스템 ID) 또는 qsg(큐 공유 그룹 ID)입니다.

각 연결 유형에 연관된 사용자 ID는 다음과 같습니다.

- 배치 연결에 대한 연결 작업의 사용자 ID
- CICS 연결을 위한 CICS 주소 공간 사용자 ID
- IMS 연결을 위한 IMS 지역 주소 공간 사용자 ID
- 채널 시작기 연결을 위한 채널 시작기 주소 공간 사용자 ID



주의: RESLEVEL은 매우 강력한 옵션입니다. 이로 인해 특정 연결에 대한 모든 자원 보안 검사가 생략될 수 있습니다.

정의된 RESLEVEL 프로파일이 없는 경우 MQADMIN 클래스의 다른 프로파일이 hlq.RESLEVEL에 일치하지 않도록 주의해야 합니다. 예를 들어, hq. ** 라고 하는 MQADMIN에 프로파일이 있다. hlq.RESLEVEL 프로파일이 없는 경우, hlq. ** 의 결과를 알 수 있습니다. ** 이 프로파일은 RESLEVEL 체크에 사용되기 때문에 프로파일을 작성할 수 있다.

RESLEVEL 프로파일이 전혀 없는 것보다는 hlq.RESLEVEL 프로파일을 정의하고 UACC를 NONE으로 설정하십시오. 가능하면 액세스 목록에 있는 사용자나 그룹 수를 작게 하십시오. RESLEVEL 액세스 감사 방법에 대한 자세한 내용은 230 페이지의 『z/OS에서 감사 고려사항』의 내용을 참조하십시오.

큐 관리자 레벨 보안만 사용 중인 경우 IBM MQ는 qmgr-name.RESLEVEL 프로파일에 대해 RESLEVEL 검사를 수행합니다. 큐 공유 그룹 레벨 보안만 사용 중인 경우, IBM MQ는 qsg-name.RESLEVEL 프로파일에 대해 RESLEVEL 검사를 수행합니다. 큐 관리자와 큐 공유 그룹 레벨 보안 결함을 사용 중인 경우, IBM MQ는 우선 큐 관리자 레벨에서 RESLEVEL 프로파일의 존재 여부를 검사합니다. 찾을 수 없는 경우에는 큐 공유 그룹 레벨에서 RESLEVEL 프로파일을 검사합니다.

RESLEVEL 프로파일을 찾을 수 없는 경우, IBM MQ는 CICS 또는 IMS 연결에 대해 작업 및 태스크(또는 대체 사용자) ID 모두에 대한 검사를 사용합니다. 배치 연결의 경우, IBM MQ는 작업(또는 대체) 사용자 ID 검사를 사용합니다. 채널 시작기의 경우, IBM MQ는 채널 사용자 ID 및 MCA(또는 대체) 사용자 ID에 대해 검사를 사용합니다.

RESLEVEL 프로파일이 있는 경우 검사 레벨은 환경 및 프로파일의 액세스 레벨에 따라 다릅니다.

큐 관리자가 큐 공유 그룹의 멤버이고 이 프로파일을 큐 관리자 레벨에 정의하지 않은 경우 검사 레벨에 영향을 주는 프로파일이 큐 공유 그룹 레벨에 정의될 수도 있습니다. 두 사용자 ID 검사를 활성화하려면 RESLEVEL 프로파일(큐 관리자 이름 또는 큐 공유 그룹 이름으로 접두부가 추가)을 UACC(NONE)으로 정의하여 관련 사용자에게 이 프로파일에 대한 액세스가 부여되지 않도록 합니다.

채널 시작기 사용자 ID가 RESLEVEL에 가지는 액세스를 고려할 때 채널 시작기로 설정된 연결은 채널에서도 사용되는 연결임에 주의하십시오. 채널 시작기 사용자 ID에 대한 모든 자원 보안 검사 생략을 초래하는 설정은 효율적으로 모든 채널에 대한 보안 검사도 생략합니다. RESLEVEL에 대한 채널 시작기 사용자 ID 액세스가 NONE이 아닌 경우, 하나의 사용자 ID(READ 또는 UPDATE의 액세스 레벨에 대해)만 액세스에 대해 검사되거나 사용자 ID(CONTROL 또는 ALTER 액세스 레벨에 대해)가 액세스에 대해 검사되지 않습니다. RESLEVEL에 대해 NONE 이외의 액세스 레벨을 채널 시작기 사용자 ID에 부여하는 경우, 채널에 대해 수행되는 보안 검사에서 이 설정의 영향에 대해 이해하고 있어야 합니다.

RESLEVEL 프로파일 사용은 정상 보안 감사 레코드가 사용되지 않는 것을 의미합니다. 예를 들어, 사용자에 UAUDIT를 넣는 경우, MQADMIN에서 hlq.RESLEVEL 프로파일에 대한 액세스는 감사되지 않습니다.

RACF WARNING 옵션을 hlq.RESLEVEL 프로파일에서 사용하는 경우 RESLEVEL 클래스의 프로파일에 대해 RACF 경고 메시지가 생성되지 않습니다.

COD와 같은 보고서 메시지에 대한 보안 검사는 원래 애플리케이션에 연관된 RESLEVEL 프로파일로 제어됩니다. 예를 들어, 배치 작업 사용자 ID가 RESLEVEL 프로파일에 대해 CONTROL 또는 ALTER 권한을 가지는 경우, 배치 작업으로 수행되는 모든 자원 검사가 생략되며 여기에는 보고서 메시지 보안 검사도 포함됩니다.

RESLEVEL 프로파일을 변경하는 경우, 변경이 적용되기 전에 사용자는 연결을 끊은 후 다시 연결해야 합니다. (여기에는 분산 큐잉 주소 공간 사용자 ID가 RESLEVEL 프로파일에 대해 가지는 액세스가 변경되는 경우 채널 시작기 중지 및 재시작도 포함됩니다.)

RESLEVEL 감사를 끄려면 RESAUDIT 시스템 매개변수를 사용하십시오.

z/OS RESLEVEL 및 배치 연결

기본적으로 IBM MQ 자원이 배치 및 배치 유형 연결을 통해 액세스 중인 경우 사용자는 특정 조작에 대한 자원 액세스가 부여되어야 합니다. 적절한 RESLEVEL 정의를 설정하여 보안 검사를 생략할 수 있습니다.

사용자 검사 여부는 연결 시에 사용되는 사용자 ID를 기반으로 하며 연결 검사에 사용되는 사용자 ID와 동일합니다.

예를 들어, 신뢰하는 사용자가 배치 연결을 통해 특정 자원에 액세스하는 경우 어떠한 API 자원 보안 검사가 수행되지 않지만, 신뢰하지 않는 사용자가 동일한 자원에 액세스를 시도하면 보안 검사가 정상적으로 수행되도록 RESLEVEL을 설정할 수 있습니다. 사용자를 충분히 신뢰하고 해당 사용자가 프로그램을 실행하는 경우에만 API 자원 보안 검사를 생략하도록 RESLEVEL 검사를 설정해야 합니다.

다음 표는 배치 연결에 대해 수행되는 검사를 보여줍니다.

표 52. 배치 연결에 대해 다른 RACF 액세스 레벨에서 수행되는 검사	
RACF 액세스 레벨	검사 레벨
NONE	수행되는 자원 검사
READ	수행되는 자원 검사
UPDATE	수행되는 자원 검사
CONTROL	검사하지 않습니다.
ALTER	검사하지 않습니다.

z/OS RESLEVEL 및 시스템 기능

조작 및 제어판 및 CSQUTIL에 대한 RESLEVEL 애플리케이션

조작 및 제어판 및 CSQUTIL 유틸리티는 배치 유형의 애플리케이션으로 큐 관리자의 명령 서버에 대한 요청을 수행하기 때문에 209 페이지의 『RESLEVEL 및 배치 연결』에서 설명하는 고려사항의 대상입니다. RESLEVEL을 사용하여 사용되는 SYSTEM.COMMAND.INPUT 및 SYSTEM.COMMAND.REPLY.MODEL 큐에 대한 보안 검사를 생략하지만 동적 큐 SYSTEM.CSQCXCMD.*, SYSTEM.CSQOREXX.* 및 SYSTEM.CSQUTIL.*에 대한 보안 검사를 생략하지 않을 수 있습니다.

명령 서버는 큐 관리자의 필수 파트로 연관된 연결이나 RESLEVEL 검사가 없습니다. 보안을 유지보수하여 명령 서버가 요청 애플리케이션의 사용자 ID가 응답에 사용 중인 큐 열기에 대한 권한을 가지도록 해야 합니다. 이는 조작 및 제어판에 대해서는 SYSTEM.CSQOREXX.*입니다. CSQUTIL의 경우에는 SYSTEM.CSQUTIL.*입니다. 184 페이지의 『시스템 큐 보안』에서 설명하는 대로 부여된 모든 RESLEVEL 권한 이외에도 사용자에게는 해당 큐 사용 권한도 있어야 합니다.

명령 서버를 사용하는 다른 애플리케이션의 경우 응답 대상 큐로 이름 지정한 큐입니다. 이런 다른 애플리케이션은 자체 사용자 ID보다 더 신뢰할 수 있는 사용자 ID를 명령 서버로 전달(메시지 컨텍스트로)하여 권한이 없는 큐에 메시지를 배치하도록 명령 서버를 속일 수도 있습니다. 이를 방지하기 위해 CONTEXT 프로파일을 사용하여 SYSTEM.COMMAND.INPUT에 배치된 메시지의 ID 컨텍스트를 보호하십시오.

z/OS RESLEVEL 및 CICS 연결

기본적으로 API 자원 보안 검사가 CICS 연결에 수행되는 경우 두 개의 사용자 ID가 검사됩니다. RESLEVEL 프로파일을 설정하여 검사되는 사용자 ID를 변경할 수 있습니다.

검사되는 첫 번째 사용자 ID는 CICS 주소 공간의 사용자 ID입니다. This is the user ID on the job card of the CICS job, or the user ID assigned to the CICS started task by the z/OS STARTED class or the started procedures table. (CICS DFLTUSER는 아닙니다.)

검사되는 두 번째 사용자 ID는 CICS 트랜잭션에 연관되는 사용자 ID입니다.

이 사용자 ID 중 하나에 자원에 대한 액세스 권한이 없는 경우, 요청은 완료 코드 MQRC_NOT_AUTHORIZED로 실패합니다. CICS 주소 공간 사용자 ID 및 CICS 트랜잭션을 실행 중인 사용자의 사용자 ID 모두는 올바른 레벨의 자원에 대한 액세스가 있어야 합니다.

RESLEVEL이 수행되는 검사에 주는 영향

RESLEVEL 프로파일 설정 방법에 따라 자원에 대한 액세스가 요청될 때 검사되는 사용자 ID를 변경할 수 있습니다. 자세한 정보는 210 페이지의 표 53의 내용을 참조하십시오.

검사되는 사용자 ID는 연결 시에 사용되는 사용자 ID에 따릅니다. 즉, CICS 주소 공간 사용자 ID에 따라 다릅니다. 이 제어를 사용하면 하나의 시스템 (예: 테스트 시스템, TESTCICS) 에서 들어오는 IBM MQ 요청에 대한 API 자원 보안 검사를 생략할 수 있지만 다른 시스템 (예: 프로덕션 시스템, PRODCICS) 에 대해 이를 구현할 수 있습니다.

참고: STARTED 클래스 또는 RACF 시작 프로시저 테이블 ICHRIN03의 "신뢰할 수 있는" 속성을 사용하여 CICS 주소 공간 사용자 ID를 설정하면, 이는 큐 관리자의 RESLEVEL 프로파일이 설정한 CICS 주소 공간에 대한 모든 사용자 ID 검사를 대체합니다. 즉, 큐 관리자가 CICS 주소 공간에 대한 보안 검사를 수행하지 않습니다. 자세한 정보는 *CICS Transaction Server for z/OS V3.2 RACF Security Guide*를 참조하십시오.

다음 표는 CICS 연결에 대해 수행되는 검사를 보여줍니다.

표 53. CICS 연결에 대해 서로 다른 RACF 액세스 레벨에서 확인이 수행됩니다.	
RACF 액세스 레벨	검사 레벨
NONE	IBM MQ에서 CICS 주소 공간 사용자 ID와 트랜잭션 사용자 ID를 검사합니다.
READ	IBM MQ에서 CICS 주소 공간 사용자 ID만 검사합니다.
UPDATE	트랜잭션이 CICS에 대해 RESSEC(YES)로 정의된 경우, IBM MQ에서는 CICS 주소 공간 사용자 ID와 트랜잭션 사용자 ID를 검사합니다.
UPDATE	트랜잭션이 CICS에 대해 RESSEC(NO)로 정의된 경우, IBM MQ에서는 CICS 주소 공간 사용자 ID만 검사합니다.
CONTROL 또는 ALTER	IBM MQ에서 사용자 ID를 검사하지 않습니다.

z/OS RESLEVEL 및 IMS 연결

기본적으로 API 자원 보안 검사가 IMS 연결에 수행되는 경우 두 개의 사용자 ID가 검사됩니다. RESLEVEL 프로파일을 설정하여 검사되는 사용자 ID를 변경할 수 있습니다.

기본적으로 API 자원 보안 검사가 IMS 연결에 대해 수행되는 경우, 두 사용자 ID가 검사되어 자원 액세스 허용 여부를 확인합니다.

검사되는 첫 번째 사용자 ID는 IMS 영역의 주소 공간 사용자 ID입니다. 이는 작업 카드의 USER 필드 또는 z/OS STARTED 클래스 또는 시작된 프로시저 테이블(SPT)의 지역에 지정된 사용자 ID에서 사용됩니다.

검사되는 두 번째 사용자 ID는 종속 영역에서 수행 중인 작업에 연관됩니다. 이는 두 번째 사용자 ID가 IMS(tm) 연결에 대해 판별되는 방법에 표시되는 대로 종속 영역 유형에 따라 판별됩니다.

첫 번째 또는 두 번째 IMS 사용자 ID 중 하나에 자원에 대한 액세스 권한이 없는 경우, 요청은 완료 코드 MQRC_NOT_AUTHORIZED로 실패합니다.

IBM MQ RESLEVEL 프로파일 설정은 IMS 트랜잭션이 IBM-supplied MQ-IMS 트리거 모니터 프로그램 CSQQTRMN에서 스케줄되는 사용자 ID를 대체할 수 없습니다. 이 사용자 ID는 해당 트리거 모니터의 PSBNAME으로 기본적으로 CSQQTRMN입니다.

RESLEVEL이 수행되는 검사에 주는 영향

RESLEVEL 프로파일 설정 방법에 따라 자원에 대한 액세스가 요청될 때 검사되는 사용자 ID를 변경할 수 있습니다. 가능한 검사는 다음과 같습니다.

- IMS 지역 주소 공간 사용자 ID 및 두 번째 사용자 ID 또는 대체 사용자 ID를 검사합니다.

- IMS 지역 주소 공간 사용자 ID만 검사합니다.
- 어떤 사용자 ID도 검사하지 않습니다.

다음 표는 IMS 연결에 대해 수행되는 검사를 보여줍니다.

표 54. IMS 연결에 대해 서로 다른 RACF 액세스 레벨에서 확인이 수행됩니다.	
RACF 액세스 레벨	검사 레벨
NONE	IMS 주소 공간 사용자 ID 및 IMS 두 번째 사용자 ID 또는 대체 사용자 ID를 검사합니다.
READ	IMS 주소 공간 사용자 ID를 검사합니다.
UPDATE	IMS 주소 공간 사용자 ID를 검사합니다.
CONTROL	검사하지 않습니다.
ALTER	검사하지 않습니다.

z/OS RESLEVEL 및 채널 시작기 연결

기본적으로 API 자원 보안 검사는 채널 시작기로 수행되고 두 사용자 ID가 검사됩니다. RESLEVEL 프로파일을 설정하여 검사되는 사용자 ID를 변경할 수 있습니다.

기본적으로 API 자원 보안 검사는 채널 시작기로 수행되고 두 사용자 ID가 검사되어 자원 액세스 허용 여부를 확인합니다.

검사된 사용자 ID는 MCAUSER 채널 속성으로 지정된 사용자 ID, 네트워크에서 수신된 사용자 ID 채널 시작기 주소 공간의 사용자 ID 또는 메시지 디스크립터의 대체 사용자 ID일 수 있습니다. 검사되는 사용자 ID는 사용 중인 통신 프로토콜 및 PUTAUT 채널 속성의 설정에 따라 다릅니다. 자세한 정보는 216 페이지의 『채널 시작기에서 사용되는 사용자 ID』의 내용을 참조하십시오.

이 사용자 ID 중 하나에 자원에 대한 액세스 권한이 없는 경우, 요청은 완료 코드 MQRC_NOT_AUTHORIZED로 실패합니다.

RESLEVEL이 수행되는 검사에 주는 영향

RESLEVEL 프로파일 설정 방법에 따라 자원에 대한 액세스가 요청될 때 검사되는 사용자 ID 및 검사 횟수를 변경할 수 있습니다.

다음 표에서는 채널 시작기 연결 및 이 연결을 사용한 이후의 모든 채널에 대해 수행되는 검사를 보여줍니다.

표 55. 채널 시작기 연결에 대해 다른 RACF 액세스 레벨로 수행된 검사	
RACF 액세스 레벨	검사 레벨
NONE	두 사용자 ID를 검사합니다.
READ	하나의 사용자 ID를 검사합니다.
UPDATE	하나의 사용자 ID를 검사합니다.
CONTROL	검사하지 않습니다.
ALTER	검사하지 않습니다.

참고: 검사되는 사용자 ID 정의에 대해서는 216 페이지의 『채널 시작기에서 사용되는 사용자 ID』의 내용을 참조하십시오.

z/OS RESLEVEL 및 내부 그룹 큐잉

기본적으로 API 자원 보안 검사는 그룹 내 큐잉 에이전트로 수행되고 두 사용자 ID가 검사되어 자원 액세스 허용 여부를 확인합니다. RESLEVEL 프로파일을 설정하여 검사되는 사용자 ID를 변경할 수 있습니다.

검사하는 사용자 ID는 수신 큐 관리자의 IGQUSER 속성에 의해 판별되는 사용자 ID, 메시지를 SYSTEM.QSG.TRANSMIT.QUEUE에 넣는 큐 공유 그룹 내의 큐 관리자 사용자 ID 또는 메시지의 메시지 디스크립터에서 *UserIdentifier* 필드에 지정되는 대체 사용자 ID일 수 있습니다. 자세한 정보는 [219 페이지의 『내부 그룹 큐잉 에이전트가 사용하는 사용자 ID』](#)의 내용을 참조하십시오.

그룹 내 큐잉 에이전트는 내부 큐 관리자 태스크이기 때문에 명시적인 연결 요청을 발행하지 않고 큐 관리자의 사용자 ID로 실행됩니다. 그룹 내 큐잉 에이전트는 큐 관리자 초기화 시에 시작됩니다. 그룹 내 큐잉 에이전트 초기화 중에 IBM MQ는 큐 관리자에 연관된 사용자 ID가 호출된 MQADMIN 클래스의 프로파일에 대해 가지는 액세스를 검사합니다.

```
hlq.RESLEVEL
```

이 검사는 hlq.NO.SUBSYS.SECURITY 스위치가 설정된 경우를 제외하고는 항상 수행됩니다.

RESLEVEL 프로파일이 없는 경우, IBM MQ는 두 사용자 ID에 대해 검사를 사용합니다. RESLEVEL 프로파일이 있는 경우, 검사 레벨은 프로파일에 대해 큐 관리자의 사용자 ID에게 부여된 액세스 레벨에 따라 다릅니다. 그룹 내 큐잉 에이전트에 대해 다른 RACF(r) 액세스 레벨에서 수행되는 검사는 그룹 내 큐잉 에이전트에 대해 수행되는 검사를 보여줍니다.

표 56. 그룹 내 큐잉 에이전트에 대해 다른 RACF 액세스 레벨에서 수행되는 검사	
RACF 액세스 레벨	검사 레벨
NONE	두 사용자 ID를 검사합니다.
READ	하나의 사용자 ID를 검사합니다.
UPDATE	하나의 사용자 ID를 검사합니다.
CONTROL	검사하지 않습니다.
ALTER	검사하지 않습니다.

참고: 검사되는 사용자 ID 정의에 대해서는 [219 페이지의 『내부 그룹 큐잉 에이전트가 사용하는 사용자 ID』](#)의 내용을 참조하십시오.

큐 관리자 사용자 ID에 대한 RESLEVEL 프로파일에 부여된 권한이 변경되면 그룹 내 큐잉 에이전트는 새 권한을 선택하기 위해 중지된 후 재시작해야 합니다. 그룹 내 큐잉 에이전트를 독립적으로 중지하고 재시작할 수 있는 방법이 없기 때문에 이를 위해 큐 관리자를 중지한 후 재시작해야 합니다.

z/OS 검사한 RESLEVEL 및 사용자 ID

RESLEVEL 프로파일 설정 및 해당 액세스 부여 예제

배치 연결의 프로파일 이름에 대해 검사되는 사용자 ID - LU 6.2 및 TCP/IP 서버 연결 채널의 프로파일 이름에 대해 검사되는 사용자 ID는 RESLEVEL이 다른 MQI 요청에 대해 검사되는 사용자 ID에 영향을 주는 방법을 보여줍니다.

예를 들어, 다음과 같은 요구사항의 큐 관리자 QM66 있습니다.

- 사용자 WS21B는 자원 보안에서 제외됩니다.
- 주소 공간 사용자 ID CICSWXN에서 실행 중인 CICS가 시작하는 태스크 WXNCICS는 RESSEC(YES)로 정의된 트랜잭션에 대해서만 전체 자원 검사를 수행합니다.

적절한 RESLEVEL 프로파일을 정의하려면 다음 RACF 명령을 발행하십시오.

```
RDEFINE MQADMIN QM66.RESLEVEL UACC(NONE)
```

그런 다음 다음 명령으로 이 프로파일에 대해 사용자 액세스를 부여하십시오.

```
PERMIT QM66.RESLEVEL CLASS(MQADMIN) ID(WS21B) ACCESS(CONTROL)
PERMIT QM66.RESLEVEL CLASS(MQADMIN) ID(CICSWXN) ACCESS(UPDATE)
```


사용자 ID가 큐 관리자 QM66에 연결된 동안 이런 변경을 수행하려면 변경사항이 적용되기 전에 사용자는 연결을 끊은 후에 다시 연결해야 합니다.

사용자 연결 시에 서브시스템 보안이 활성화되지 않지만 이 사용자가 여전히 연결되어 있다면 서브시스템 보안은 활성화되고 전체 자원 보안 검사가 사용자에게 적용됩니다. 사용자는 올바른 RESLEVEL 처리를 위해 다시 연결해야 합니다.

z/OS z/OS의 보안 검사를 위한 사용자 ID

IBM MQ는 사용자, 터미널, 애플리케이션, 기타 자원에 연관된 사용자 ID를 기반으로 보안 검사를 시작합니다. 이 토픽 컬렉션은 각 보안 검사 유형에 사용되는 사용자 ID를 나열합니다.

z/OS 연결 보안을 위한 사용자 ID

연결 보안에 사용된 사용자 ID는 연결 유형에 따라 다릅니다.

연결 유형	사용자 ID 콘텐츠
배치 연결	연결 태스크의 사용자 ID. 예를 들면, 다음과 같습니다. <ul style="list-style-type: none"> TSO 사용자 ID USER JCL 매개변수로 배치 작업에 지정되는 사용자 ID STARTED 클래스 또는 시작된 프로시저 테이블로 시작되는 태스크에 지정되는 사용자 ID
CICS 연결	CICS 주소 공간 사용자 ID.
IMS 연결	IMS 지역 주소 공간 사용자 ID.
채널 시작기 연결	채널 시작기 주소 공간 사용자 ID.

z/OS 명령 및 명령 자원 보안을 위한 사용자 ID

명령 보안 및 명령 자원 보안에 사용되는 사용자 ID는 명령 발행 위치에 따라 다릅니다.

발행 위치...	사용자 ID 콘텐츠
CSQINP1, CSQINP2 또는 CSQINPT	검사가 수행되지 않습니다.
시스템 명령 입력 큐	명령을 포함하는 메시지의 메시지 디스크립터의 <i>UserIdentifier</i> 에서 사용자 ID를 찾았습니다. 메시지가 <i>UserIdentifier</i> 를 포함하지 않는 경우, 공백의 사용자 ID가 보안 관리자에게 전달됩니다.
콘솔	사용자 ID가 콘솔에 사인온했습니다. 콘솔이 사인온되지 않은 경우, 기본 사용자 ID는 CSQ6SYSP의 CMDUSER 시스템 매개변수로 설정됩니다. 콘솔에서 명령을 발행하려면 콘솔에 z/OS SYS AUTHORITY 속성이 있어야 합니다.
SDSF/TSO 콘솔	TSO 또는 작업 사용자 ID.
조작 및 제어판	TSO 사용자 ID. 조작 및 제어판을 사용하려는 경우, 선택하는 조치에 해당하는 명령 발행에 필요한 권한이 있어야 합니다. 또한 모든 hlq.DISPLAY에 대한 READ 액세스 권한이 있어야 합니다. 패널이 다양한 DISPLAY 명령을 사용하여 존재하는 정보를 수집하므로 MQCMDMS 클래스의 <i>object</i> 프로파일.
MGCRE	MGCRE와 UTOKEN을 같이 사용하는 경우, UTOKEN의 사용자 ID. MGCRE가 UTOKEN 없이 발행되는 경우, TSO 또는 작업 사용자 ID가 사용됩니다.
CSQOUTIL	작업 사용자 ID.

발행 위치...	사용자 ID 콘텐츠
CSQUTIL	작업 사용자 ID.
CSQINPX	채널 시작기 주소 공간의 사용자 ID.

z/OS 자원 보안을 위한 사용자 ID(MQOPEN, MQSUB, MQPUT1)

이 정보는 각 유형의 연결에 대해 정상 및 대체 사용자 ID의 사용자 ID 콘텐츠를 보여줍니다. 검사 수는 RESLEVEL 프로파일로 정의됩니다. 검사되는 사용자 ID는 MQOPEN, MQSUB 또는 MQPUT1 호출에 사용되는 사용자 ID입니다.

참고: 모든 사용자 ID 필드는 수신될 때 정확하게 검사됩니다. 변환은 수행되지 않으며 예를 들어, "Bob", "BOB", "bob"를 포함하는 세 사용자 ID 필드는 동일하지 않습니다.

z/OS 배치 연결에 대해 검사되는 사용자 ID

배치 연결에 대해 검사되는 사용자 ID는 태스크 실행 방법 및 대체 사용자 ID 지정 여부에 따라 다릅니다.

표 57. 배치 연결을 위한 프로파일 이름에 대한 사용자 ID 검사

열기 시에 대체 사용자 ID 지정 여부	hlq.ALTERNATE.USER.userid 프로파일	hlq.CONTEXT.queueName 프로파일	hlq.resourcename 프로파일
아니오	-	JOB	JOB
예	JOB	JOB	대체

키:

대체

대체 사용자 ID.

JOB

- TSO 또는 USS 사인온의 사용자 ID.
- 배치 작업에 지정되는 사용자 ID.
- STARTED 클래스로 시작된 태스크 또는 시작된 프로시저 테이블에 지정되는 사용자 ID.
- 실행 중인 Db2 스토어드 프로시저에 연관되는 사용자 ID

배치 작업은 RESLEVEL이 READ로 설정되고 대체 사용자 ID 검사는 꺼진 상태로 호출된 Q1 큐에 대해 MQPUT1을 수행합니다.

배치 연결에 대해 다른 RACF(r) 액세스 레벨에서 수행되는 검사 및 배치 연결에 대해 프로파일 이름에 대한 사용자 ID 검사에서 작업 사용자 ID가 프로파일 hlq.Q1에 대해 검사되는 것을 보여줍니다.

z/OS CICS 연결에 대해 검사되는 사용자 ID

CICS 연결에 대해 검사되는 사용자 ID는 하나 또는 두 개의 검사가 수행되는지 및 대체 사용자 ID 지정 여부에 따라 다릅니다.

표 58. CICS 유형 사용자 ID의 프로파일 이름에 대한 사용자 ID 검사

열기 시에 대체 사용자 ID 지정 여부	hlq.ALTERNATE.USER.userid 프로파일	hlq.CONTEXT.queueName 프로파일	hlq.resourcename 프로파일
아니오, 1 검사	-	ADS	ADS
아니오, 2 검사	-	ADS+TXN	ADS+TXN
예, 1 검사	ADS	ADS	ADS
예, 2 검사	ADS+TXN	ADS+TXN	ADS+ALT

키:

대체

대체 사용자 ID

ADS

CICS 배치 작업에 연관된 사용자 ID 또는 CICS가 시작된 태스크로 실행 중인 경우 STARTED 클래스 또는 시작된 프로시저 테이블에 연관되는 사용자 ID.

TXN

CICS 트랜잭션에 연관되는 사용자 ID. 이는 일반적으로 트랜잭션을 시작한 터미널 사용자의 사용자 ID입니다. 이는 CICS DFLTUSER 또는 PRESET 보안 터미널 또는 수동으로 사인온한 사용자일 수 있습니다.

다음 조건에 대해 검사되는 사용자 ID 판별:

- CICS 주소 공간 사용자 ID의 RESLEVEL 프로파일에 대한 RACF 액세스 레벨은 NONE으로 설정됩니다.
- MQOPEN 호출은 MQOO_OUTPUT 및 MQOO_PASS_IDENTITY_CONTEXT로 큐에 대해 수행됩니다.

우선, RESLEVEL 프로파일에 대한 CICS 주소 공간 사용자 ID를 기반으로 검사되는 CICS 사용자 ID 수를 확인하십시오. 209 페이지의 『RESLEVEL 및 CICS 연결』 토픽의 210 페이지의 표 53에서 RESLEVEL 프로파일이 NONE으로 설정되는 경우 두 개의 사용자 ID가 검사됩니다. 그런 다음 214 페이지의 표 58에서 해당 검사가 수행됩니다.

- hlq.ALTERNATE.USER.userid 프로파일은 검사되지 않습니다.
- hlq.CONTEXT.queueName 프로파일은 CICS 주소 공간 사용자 ID 및 CICS 트랜잭션 사용자 ID 모두로 검사됩니다.
- hlq.resourcename 프로파일은 CICS 주소 공간 사용자 ID 및 CICS 트랜잭션 사용자 ID 모두로 검사됩니다.

즉, 이 MQOPEN 호출에 대해 4개의 보안 검사가 수행됩니다.

IMS 연결에 대해 검사되는 사용자 ID

IMS 연결에 대해 검사되는 사용자 ID는 하나 또는 두 개의 검사가 수행되는지 및 대체 사용자 ID 지정 여부에 따라 다릅니다. 두 번째 사용자 ID가 검사되는 경우, 종속 영역 유형 및 사용 가능한 사용자 ID에 따라 다릅니다.

표 59. IMS 유형 사용자 ID의 프로파일 이름에 대한 사용자 ID 검사			
열기 시에 대체 사용자 ID 지정 여부	hlq.ALTERNATE.USER.userid 프로파일	hlq.CONTEXT.queueName 프로파일	hlq.resourcename 프로파일
아니오, 1 검사	-	REG	REG
아니오, 2 검사	-	REG+SEC	REG+SEC
예, 1 검사	REG	REG	REG
예, 2 검사	REG+SEC	REG+SEC	REG+ALT

키:

대체

대체 사용자 ID.

REG

사용자 ID는 일반적으로 STARTED 클래스 또는 시작된 프로시저 테이블을 통해 설정되거나 IMS가 실행 중인 경우 제출된 작업에서 USER JCL 매개변수로 설정됩니다.

SEC

두 번째 사용자 ID는 종속 영역에서 수행 중인 작업에 연관됩니다. 이는 216 페이지의 표 60에 따라 판별됩니다.

표 60. 두 번째 사용자 ID가 IMS 연결에 대해 판별되는 방법	
종속 영역 유형	두 번째 사용자 ID 판별 계층
<ul style="list-style-type: none"> • BMP 메시지 구동 및 성공적인 GET UNIQUE 발행. • IFP 및 GET UNIQUE 발행. • MPP. 	사용자가 사인온한 경우 IMS 트랜잭션에 연관되는 사용자 ID. LTERM 이름이 사용 가능한 경우 해당 이름. PSBNAME.
<ul style="list-style-type: none"> • BMP 메시지 구동 및 성공적인 GET UNIQUE가 발행되지 않음. • BMP가 메시지 구동되지 않음 • IFP 및 GET UNIQUE가 발행되지 않음. 	모두 공백 또는 모두 0이 아닌 경우 IMS 종속 영역 주소 공간에 연관된 사용자 ID. PSBNAME.

z/OS 채널 시작기에서 사용되는 사용자 ID
 이 주제 모음에서는 수신 채널 및 서버 연결 채널을 통해 발행되는 클라이언트 MQI 요청에 대해 검사 및 사용되는 사용자 ID에 대해 설명합니다. TCP/IP 및 LU 6.2에 대한 정보가 제공됩니다.

수신 채널 정의의 PUTAUT 매개변수를 사용하여 사용되는 보안 검사 유형을 판별할 수 있습니다. IBM MQ 네트워크에서 일관성 있는 보안 검사가 수행되도록 하기 위해 ONLYMCA 및 ALTMCA 옵션을 사용할 수 있습니다.

DISPLAY CHSTATUS 명령을 사용하여 MCA에서 사용되는 사용자 ID를 판별할 수 있습니다.

z/OS TCP/IP를 사용하여 채널 수신
 검사하는 사용자 ID는 채널의 PUTAUT 옵션 및 하나 또는 두 개의 검사가 수행되는지 여부에 따라 다릅니다.

표 61. TCP/IP 채널의 프로파일 이름에 대해 검사되는 사용자 ID			
수신자 또는 요청자 채널에 지정되는 PUTAUT 옵션	hlq.ALTERNATE.USER.userid 프로파일	hlq.CONTEXT.queueename 프로파일	hlq.resourcename 프로파일
DEF, 1 검사	-	CHL	CHL
DEF, 2 검사	-	CHL + MCA	CHL + MCA
CTX, 1 검사	CHL	CHL	CHL
CTX, 2 검사	CHL + MCA	CHL + MCA	CHL + ALT
ONLYMCA, 1 검사	-	MCA	MCA
ONLYMCA, 2 검사	-	MCA	MCA
ALTMCA, 1 검사	MCA	MCA	MCA
ALTMCA, 2 검사	MCA	MCA	MCA + ALT

키:

MCA(MCA 사용자 ID)

수신자에서 MCAUSER 채널 속성에 대해 지정되는 사용자 ID. 공백인 경우, 수신자 또는 요청자 측의 채널 시작기 주소 공간 사용자 ID가 사용됩니다.

CHL(채널 사용자 ID)

TCP/IP에서 보안은 채널에 대해 통신 시스템에서 지원되지 않습니다. TLS(Transport Layer Security)가 사용 중이고 디지털 인증서가 파트너에서 플로우된 경우, 이 인증서에 연관된 사용자 ID(설치된 경우) 또는 RACF Certificate Name Filtering(CNF)을 사용하여 발견된 일치하는 필터에 연관된 사용자 ID가 사용됩니다. 연관된 사용자 ID가 없거나 TLS를 사용 중이지 않은 경우 PUTAUT 매개변수를 DEF 또는 CTX로 설정하여 정의된 채널에서 수신자 또는 요청자측의 채널 시작기 주소 공간을 채널 사용자 ID로 사용합니다.

참고: RACF Certificate Name Filtering(CNF)을 사용하면 동일한 RACF 사용자 ID를 여러 원격 사용자(예를 들어, 동일한 조직 단위의 모든 사용자)로 기본적으로 모두 동일한 보안 권한을 가짐)에 지정할 수 있습니다. 즉, 전 세계에 있는 가능한 모든 원격 사용자의 인증서 사본이 서버에 없어도 되므로 인증서 관리와 배포가 매우 간편해집니다.

PUTAUT 매개변수를 채널에 대해 ONLYMCA 또는 ALTMCA로 설정하는 경우, 채널 사용자 ID는 무시되고 수신자 또는 요청자의 MCA 사용자 ID가 사용됩니다. TLS를 사용하는 TCP/IP 채널에도 적용됩니다.

ALT(대체 사용자 ID)

메시지의 메시지 디스크립터 내에서 컨텍스트 정보의 사용자 ID(즉, *UserIdentifier* 필드). 이 사용자 ID는 **MQOPEN** 또는 **MQPUT1** 호출이 대상 목적지 큐에 대해 발행되기 전에 오브젝트 디스크립터의 *AlternateUserID* 필드로 이동합니다.



LU 6.2를 사용하여 채널 수신

검사하는 사용자 ID는 채널의 PUTAUT 옵션 및 하나 또는 두 개의 검사가 수행되는지 여부에 따라 다릅니다.

표 62. LU 6.2 채널의 프로파일 이름에 대해 검사되는 사용자 ID			
수신자 또는 요청자 채널에 지정되는 PUTAUT 옵션	hlq.ALTERNATE.USER.userid 프로파일	hlq.CONTEXT.queuename 프로파일	hlq.resourcename 프로파일
DEF, 1 검사	-	CHL	CHL
DEF, 2 검사	-	CHL + MCA	CHL + MCA
CTX, 1 검사	CHL	CHL	CHL
CTX, 2 검사	CHL + MCA	CHL + MCA	CHL + ALT
ONLYMCA, 1 검사	-	MCA	MCA
ONLYMCA, 2 검사	-	MCA	MCA
ALTMCA, 1 검사	MCA	MCA	MCA
ALTMCA, 2 검사	MCA	MCA	MCA + ALT

키:

MCA(MCA 사용자 ID)

수신자에서 MCAUSER 채널 속성에 대해 지정되는 사용자 ID. 공백인 경우, 수신자 또는 요청자 측의 채널 시작기 주소 공간 사용자 ID가 사용됩니다.

CHL(채널 사용자 ID)

요청자-서버 채널

채널이 요청자에서 시작되면 네트워크 사용자 ID(채널 사용자 ID)를 수신할 기회가 없습니다.

PUTAUT 매개변수가 요청자 채널에서 DEF 또는 CTX로 설정하는 경우, 네트워크에서 사용자 ID가 수신되지 않기 때문에 채널 사용자 ID는 요청자의 채널 시작기 주소 공간의 사용자 ID입니다.

PUTAUT 매개변수를 ONLYMCA 또는 ALTMCA로 설정하는 경우, 채널 사용자 ID는 무시되고 요청자의 MCA 사용자 ID가 사용됩니다.

기타 채널 유형

수신자 또는 요청자 채널에서 PUTAUT 매개변수가 DEF 또는 CTX로 설정되는 경우, 채널 사용자 ID는 채널이 시작될 때 통신 서버에서 수신된 사용자 ID입니다.

- 송신 채널이 z/OS에 있는 경우 수신되는 채널 사용자 ID는 송신자의 채널 시작기 주소 공간 사용자 ID입니다.
- 송신 채널이 다른 플랫폼(예: AIX)에 있는 경우 수신되는 채널 사용자 ID는 일반적으로 채널 정의의 USERID로 제공됩니다.

수신되는 사용자 ID가 공백이거나 사용자 ID가 수신되지 않으면 공백의 채널 사용자 ID가 사용됩니다.

ALT(대체 사용자 ID)

메시지의 메시지 디스크립터 내에서 컨텍스트 정보의 사용자 ID(즉, *UserIdentifier* 필드). 이 사용자 ID는 MQOPEN 또는 MQPUT1 호출이 대상 목적지 큐에 대해 발행되기 전에 오브젝트 디스크립터의 *AlternateUserID* 필드로 이동합니다.

z/OS 클라이언트 MQI 요청

설정된 사용자 ID 및 환경 변수에 따라 다양한 사용자 ID를 사용할 수 있습니다. 이 사용자 ID는 사용되는 PUTAUT 옵션 및 대체 사용자 ID 지정 여부에 따라 다양한 프로파일에 대해 검사됩니다.

이 절에서는 TCP/IP 및 LU 6.2에 대한 서버 연결 채널을 통해 발행되는 클라이언트 MQI 요청에 대해 검사되는 사용자 ID에 대해 설명합니다. MCA 사용자 ID 및 채널 사용자 ID는 이전 절에서 설명하는 TCP/IP 및 LU 6.2 채널용입니다.

서버 연결 채널의 경우, MCAUSER 속성이 공백인 경우 클라이언트에 수신되는 사용자 ID가 사용됩니다.

자세한 정보는 86 페이지의 『클라이언트의 액세스 제어』의 내용을 참조하십시오.

클라이언트 MQOPEN, MQSUB, MQPUT1 요청의 경우, 다음 규칙을 사용하여 검사되는 프로파일을 판별하십시오.

- 요청에서 대체 사용자 권한을 지정하는 경우 *hlq.ALTERNATE.USER.userid* 프로파일입니다.
- 요청에서 컨텍스트 권한을 지정하는 경우 *hlq.context* 프로파일입니다.
- 모든 MQOPEN, MQSUB, MQPUT1 요청의 경우, 검사는 *hlq.resourcename* 프로파일에 대해 수행됩니다.

검사되는 프로파일을 판별하는 경우, 다음 표를 사용하여 해당 프로파일에 대해 검사되는 사용자 ID를 판별하십시오.

서버 연결 채널에 지정되는 PUTAUT 옵션	열기 시에 대체 사용자 ID 지정 여부	hlq.ALTERNATE.USER.userid 프로파일	hlq.CONTEXT.queueename 프로파일	hlq.resourcename 프로파일
DEF, 1 검사	아니오	-	CHL	CHL
DEF, 1 검사	예	CHL	CHL	CHL
DEF, 2 검사	아니오	-	CHL + MCA	CHL + MCA
DEF, 2 검사	예	CHL + MCA	CHL + MCA	CHL + ALT
ONLYMCA, 1 검사	아니오	-	MCA	MCA
ONLYMCA, 1 검사	예	MCA	MCA	MCA
ONLYMCA, 2 검사	아니오	-	MCA	MCA
ONLYMCA, 2 검사	예	MCA	MCA	MCA + ALT

키:

MCA(MCA 사용자 ID)

서버 연결에서 MCAUSER 채널 속성에 대해 지정되는 사용자 ID. 공백인 경우, 채널 시작기 주소 공간 사용자 ID가 사용됩니다.

CHL(채널 사용자 ID)

TCP/IP에서 보안은 채널에 대해 통신 시스템에서 지원되지 않습니다. TLS(Transport Layer Security)가 사용 중이고 디지털 인증서가 파트너에서 플로우된 경우, 이 인증서에 연관된 사용자 ID(설치된 경우) 또는 RACF Certificate Name Filtering(CNF)을 사용하여 발견된 일치하는 필터에 연관된 사용자 ID가 사용됩니

다. 연관된 사용자 ID가 없는 경우 또는 TLS를 사용하지 않는 경우, 채널 시작기 주소 공간의 사용자 ID가 PUTAUT 매개변수를 DEF 또는 CTX로 설정하여 정의된 채널에서 채널 사용자 ID로 사용됩니다.

참고: RACF Certificate Name Filtering(CNF)을 사용하면 동일한 RACF 사용자 ID를 여러 원격 사용자(예를 들어, 동일한 조직 단위의 모든 사용자로 기본적으로 모두 동일한 보안 권한을 가짐)에 지정할 수 있습니다. 즉, 전 세계에 있는 가능한 모든 원격 사용자의 인증서 사본이 서버에 없어도 되므로 인증서 관리와 배포가 매우 간편해집니다.

PUTAUT 매개변수를 채널에 대해 ONLYMCA 또는 ALTMCA로 설정하는 경우, 채널 사용자 ID는 무시되고 서버 연결 채널의 MCA 사용자 ID가 사용됩니다. TLS를 사용하는 TCP/IP 채널에도 적용됩니다.

ALT(대체 사용자 ID)

메시지의 메시지 디스크립터 내에서 컨텍스트 정보의 사용자 ID(즉, *UserIdentifier* 필드). 이 사용자 ID는 MQOPEN, MQSUB 또는 MQPUT1 호출이 클라이언트 애플리케이션 대신 발행되기 전에 오브젝트 또는 구독 디스크립터의 *AlternateUserID* 필드로 이동합니다.

z/OS 채널 시작기 예

RACF 프로파일에 대해 사용자 ID가 검사되는 방법에 대한 예입니다.

사용자는 큐 관리자 QM02에서 호출된 QB 큐로 해결되는 큐 관리자 QM01의 큐에 대해 MQPUT1 조사를 수행합니다. 메시지는 QM01.TO.QM02의 TCP/IP 채널로 송신됩니다. RESLEVEL은 NONE으로 설정되고 대체 사용자 ID 및 컨텍스트 검사를 사용하여 열기가 수행됩니다. 수신자 채널 정의에는 PUTAUT(CTX)가 있고 MCA 사용자 ID가 설정됩니다. 큐 QB에 메시지를 넣기 위해 수신 채널에서 사용되는 사용자 ID는?

답변: 211 페이지의 표 55에서는 RESLEVEL이 NONE으로 설정되었으므로 두 개의 사용자 ID가 검사되는 것을 보여줍니다.

216 페이지의 표 61에서는 PUTAUT는 CTX로 설정된 2개의 검사를 사용하여 다음 사용자 ID가 검사되는 것을 보여줍니다.

- 채널 시작기 사용자 ID 및 MCAUSER 사용자 ID는 hlq.ALTERNATE.USER.userid 프로파일에 대해 검사됩니다.
- 채널 시작기 사용자 ID 및 MCAUSER 사용자 ID는 hlq.CONTEXT.queueName 프로파일에 대해 검사됩니다.
- 채널 시작기 사용자 ID 및 메시지 디스크립터(MQMD)에 지정된 대체 사용자 ID는 hlq.Q2 프로파일에 대해 검사됩니다.

z/OS 내부 그룹 큐잉 에이전트가 사용하는 사용자 ID

그룹 내 큐잉 에이전트가 목적지 큐를 열 때 검사되는 사용자 ID는 IGQAUT 및 IGQUSER 큐 관리자 속성 값으로 판별됩니다.

가능한 사용자 ID는 다음과 같습니다.

그룹 내 큐잉 사용자 ID(IGQ)

수신 큐 관리자의 IGQUSER 속성으로 판별되는 사용자 ID. 공백으로 설정되는 경우 수신 큐 관리자의 사용자 ID가 사용됩니다. 그렇지만 수신 큐 관리자는 정의된 모든 큐에 액세스할 권한이 있기 때문에 보안 검사가 수신 큐 관리자의 사용자 ID에 대해 수행되지 않습니다. 이 경우 다음과 같은 상황이 발생합니다.

- 하나의 사용자 ID만 검사되고 사용자 ID는 수신 큐 관리자의 사용자 ID인 경우 보안 검사가 수행되지 않습니다. 이는 IGQAUT가 ONLYIGQ 또는 ALTIGQ로 설정될 때 발생할 수 있다.
- 두 사용자 ID가 검사되고 사용자 ID 중 하나가 수신 큐 관리자의 사용자 ID인 경우 보안 검사는 다른 사용자 ID에 대해서만 수행됩니다. 이것은 IGQAUT가 DEF, CTX, 또는 ALTIGQ로 설정될 때 발생할 수 있다.
- 두 사용자 ID가 검사되고 두 사용자 ID 모두 수신 큐 관리자의 사용자 ID인 경우 보안 검사가 수행되지 않습니다. 이는 IGQAUT가 ONLYIGQ로 설정될 때 발생할 수 있다.

송신 큐 관리자 사용자 ID(SND)

메시지를 SYSTEM.QSG.TRANSMIT.QUEUE에 넣는 큐 공유 그룹 내에서 큐 관리자의 사용자 ID.

대체 사용자 ID(ALT)

메시지의 메시지 디스크립터에서 *UserIdentifier* 필드에 지정된 사용자 ID.

표 64. 그룹 내 큐잉의 프로파일 이름에 대해 검사되는 사용자 ID.			
수신 큐 관리자에 지정된 IGQAUT 옵션	hlq.ALTERNATE.USER.userid 프로파일	hlq.CONTEXT.queuename 프로파일	hlq.resourcename 프로파일
DEF, 1 검사	-	SND	SND
DEF, 2 검사	-	SND +IGQ	SND +IGQ
CTX, 1 검사	SND	SND	SND
CTX, 2 검사	SND + IGQ	SND +IGQ	SND + ALT
ONLYIGQ, 1 검사	-	IGQ	IGQ
ONLYIGQ, 2 검사	-	IGQ	IGQ
ALTIGQ, 1 검사	-	IGQ	IGQ
ALTIGQ, 2 검사	IGQ	IGQ	IGQ + ALT

키:

대체

대체 사용자 ID.

IGQ

IGQ 사용자 ID.

SND

송신 큐 관리자 사용자 ID.

z/OS 공백 사용자 ID 및 UACC 레벨

공백 사용자 ID가 발생하면 RACF에서 정의되지 않은 사용자가 사인온합니다. 정의되지 않은 사용자에게 광범위한 범위의 액세스를 부여하지 마십시오.

공백 사용자 ID는 사용자가 컨텍스트 또는 대체 사용자 보안을 사용하여 메시지를 조작하거나 IBM MQ가 공백 사용자 ID를 전달하는 경우에 존재할 수 있습니다. 예를 들어, 메시지가 컨텍스트 없이 시스템 명령 입력 큐로 작성될 때 사용됩니다.

참고: "*"의 사용자 ID(즉, 별표 문자 및 뒤에 오는 7개의 공백)는 정의되지 않은 사용자 ID로 처리됩니다.

IBM MQ는 RACF에 공백 사용자 ID를 전달하고 RACF 정의되지 않은 사용자가 사인온합니다. 그러면 모든 보안 검사는 유니버설 액세스(UACC)를 관련 프로파일에 대해 사용합니다. 액세스 레벨 설정 방법에 따라 UACC는 정의되지 않은 사용자에게 광범위한 액세스를 부여할 수도 있습니다.

예를 들어, 다음 RACF 명령을 TSO에서 발행하는 경우:

```
RDEFINE MQQUEUE Q.AVAILABLE.TO.EVERYONE UACC(UPDATE)
```

z/OS 정의 사용자 ID(액세스 목록에 넣지 않음) 및 해당 큐에 메시지를 넣고 여기에서 메시지를 가져오려는 RACF 정의되지 않은 사용자 ID 모두를 사용하는 프로파일을 정의합니다.

공백 사용자 ID에 대해 보호하려면 액세스 레벨을 주의깊게 계획하고 컨텍스트 및 대체 사용자 보안을 사용할 수 있는 사용자 수를 제한해야 합니다. RACF 정의되지 않은 사용자 ID를 사용하여 액세스하면 안되는 자원에 대해 액세스하는 것을 막아야 합니다. 그렇지만 동시에 정의된 사용자 ID의 사용자 액세스는 허용해야 합니다. 그러기 위해 RACF 명령 PERMIT에서 별표(*)의 사용자 ID를 지정하여 모든 정의된 사용자 ID에 대해 자원 액세스를 부여할 수 있습니다. 따라서, 정의되지 않은 모든 사용자 ID(예: "*")의 경우 액세스가 거부됩니다. 예를 들어, 해당 RACF 명령은 RACF 정의되지 않은 사용자 ID가 메시지를 넣거나 가져오기 위해 큐에 대한 액세스를 부여받는 것을 방지합니다.

```
RDEFINE MQQUEUE Q.AVAILABLE.TO.RACF.DEFINED.USERS.ONLY UACC(NONE)
PERMIT Q.AVAILABLE.TO.RACF.DEFINED.USERS.ONLY CLASS(MQQUEUE) ACCESS(UPDATE) ID(*)
```

IBM Multi-Factor Authentication for z/OS를 사용하는 z/OS 보안 관리자는 식별된 사용자가 다중 인증 요소(예: 비밀번호와 암호화 토큰 둘 다)를 사용하여 z/OS 시스템에 사인온하도록 요구함으로써 SAF 인증을 강화할 수 있습니다. IBM MFA는 또한 시간 기반의 일회성 비밀번호 생성 기술(예: RSA SecureId)에 대한 지원도 제공합니다.

대부분의 경우 IBM MQ 은 사용자가 IBM MQ 작업을 구동하는 CICS 또는 일괄처리 시스템에 "로그온" 한 방법을 인식하지 못하고 사인온한 사용자 ID 신임 정보는 z/OS 태스크 또는 주소 공간과 연관되며 IBM MQ 는 이를 사용하여 자원에 대한 권한을 확인합니다. MFA를 지원하는 사용자 ID는 IBM MQ 자원에 대한 권한 부여 및 CICS 및 IMS 브릿지에서 사용되는 패스 티켓을 통한 인증에 사용할 수 있습니다.

중요사항: 그러나 `MQCSP_AUTH_USER_ID_AND_PWD` 옵션을 사용하여 `MQCONN` API 호출에서 사용자 ID 및 비밀번호 신임 정보를 전달하는 IBM MQ Explorer와 같은 애플리케이션을 사용하는 경우에는 특수 고려사항이 적용됩니다. IBM MQ에는 추가 신임 정보를 이 API 요청에 전달하는 기능이 없습니다.

제한사항과 잠재적인 임시 해결책은 다음 텍스트에 설명되어 있습니다.

IBM MQ Explorer

IBM MQ Explorer 에서 z/OS로 2차 인증 요인을 전달하는 기능이 없으므로 IBM MQ Explorer 를 사용하여 MFA 가 사용으로 설정된 사용자 ID로 z/OS 시스템에 로그인할 수 없습니다.

또한 IBM MQ Explorer에서 사용자 ID와 비밀번호 신임 정보를 재사용하는 데 두 가지 다른 메커니즘을 사용할 수 있는데, 이 메커니즘을 사용할 경우 일회용 비밀번호를 사용할 때 특별한 주의가 필요합니다.

1. IBM MQ Explorer는 나중에 로그인할 수 있도록 비밀번호를 난독화된 형식으로 로컬 시스템에 저장하는 기능을 제공합니다. z/OS 큐 관리자에 연결될 때마다 비밀번호를 묻는 프롬프트가 탐색기에 표시되도록 하여 이 기능을 사용 안함으로 설정해야 합니다.

이를 수행하려면 다음 프로시저를 따르십시오.

- a. **큐 관리자**를 선택하십시오.
- b. 표시되는 목록에서 필요한 큐 관리자를 선택하고 해당 큐 관리자를 마우스 오른쪽 단추로 클릭하십시오.
- c. 표시되는 메뉴 목록에서 **연결 세부사항**을 선택하십시오.
- d. 다음 메뉴 목록에서 **특성**을 선택하고 **사용자 ID** 탭을 선택하십시오.

비밀번호 묻기 단일 선택 단추를 선택해야 합니다.

2. IBM MQ Explorer의 다양한 조작(예: 큐에서 메시지 찾아보기, 구독 테스트 등)은 로그인할 때 처음 사용된 신임 정보를 사용하여 IBM MQ를 인증하는 새 세트를 시작합니다. 비밀번호 신임 정보는 다시 사용할 수 없으므로 이러한 조작을 사용할 수 없습니다.

이러한 문제에 대해 MFA 구성 레벨에서 사용 가능한 두 가지 임시 해결책이 있습니다.

- MFA의 애플리케이션 ID 제외를 사용하여 IBM MQ 태스크를 MFA 처리에서 모두 함께 제외시키십시오.

이를 수행하려면 다음 명령을 실행하십시오.

1. `RDEFINE MFADEF MFABYPASS.USERID.chinuser`

여기서 `chinuser`는 채널 시작기 주소 공간 레벨 사용자 ID(STC 클래스를 거치는 채널 시작기와 연관됨)입니다.

2. `PERMIT MFABYPASS.USERID.chinuser CLASS MFADEF ACCESS(READ) ID(explorer user)`

이 접근 방식에 대한 자세한 정보는 [애플리케이션에 대해 IBM MFA 우회](#)를 참조하십시오.

- IBM MFA 1.2에서 도입된 MFA에 대한 아웃오브밴드 지원을 사용하십시오. 이 접근 방식을 사용할 경우, IBM MFA 웹 서버를 사전 인증하고 사용자 ID와 비밀번호 이외에도 정책을 통해 결정된 추가 인증을 지정할 수 있습니다. IBM MFA 서버는 캐시 토큰 신임 정보를 생성합니다. 그러면 사용자는 이 신임 정보를 IBM MQ Explorer 인증 대화 상자에 지정할 수 있습니다. 보안 관리자는 IBM MQ Explorer를 정상적으로 사용할 수 있도록 이 신임 정보를 적당한 기간 동안 재실행할 수 있습니다.

이 접근 방식에 대한 자세한 정보는 [IBM MFA 소개](#)를 참조하십시오.

z/OS IBM MQ for z/OS 보안 관리

IBM MQ는 스토리지 내 테이블을 사용하여 각 사용자 및 각 사용자의 액세스 요청에 연관된 정보를 보유하고 있습니다. 이 테이블을 효율적으로 관리하고 IBM MQ에서 외부 보안 관리자(ESM)으로의 요청 수를 줄이기 위해 여러 제어를 사용할 수 있습니다.

이 제어는 조작 및 제어판 및 IBM MQ 명령 모두를 통해 사용할 수 있습니다.

z/OS 사용자 ID 재확인

예를 들어, 사용자를 새 그룹에 연결하여 IBM MQ 자원을 사용하는 사용자의 RACF 정의가 변경된 경우, 다음에 IBM MQ 자원에 액세스하려고 시도할 때 큐 관리자에게 이 사용자에게 다시 로그인하도록 지시할 수 있습니다. 이는 IBM MQ 명령 RVERIFY SECURITY를 사용하여 수행할 수 있습니다.

- 사용자 HX0804가 큐 관리자 PRD1의 PAYROLL 큐에 메시지를 넣고 가져옵니다. 그렇지만 HX0804는 동일한 큐 관리자(PRD1)의 PENSION 큐 중 일부에 대한 액세스를 필요로 합니다.
- 데이터 보안 관리자는 사용자 HX0804를 PENSION 큐에 액세스가 허용되는 RACF 그룹에 연결합니다.
- 따라서 해당 HX0804는 큐 관리자 PRD1을 종료하지 않고 또는 HX0804가 제한시간을 초과하기를 대기하지 않고 즉시 PENSION 큐에 액세스할 수 있으며 IBM MQ 명령을 사용해야 합니다.

```
RVERIFY SECURITY(HX0804)
```

참고: 큐 관리자가 실행되는 동안 장시간(며칠에서 한 주까지) 사용자 ID 제한시간을 끄는 경우, 해당 시점에서 권한 취소 또는 삭제된 모든 사용자에 대해 RVERIFY SECURITY 명령을 실행해야 합니다.

z/OS 사용자 ID 제한시간

비활성화 기간 후에 IBM MQ가 사용자를 큐 관리자에서 사인오프하도록 할 수 있습니다.

사용자가 IBM MQ 자원에 액세스하면 큐 관리자는 이 사용자를 큐 관리자에 사인온을 시도합니다(서브시스템 보안이 활성화된 경우). 이는 사용자가 ESM에 인증되는 것을 나타냅니다. 이 사용자는 큐 관리자가 종료되거나 사용자 ID가 제한시간(인증이 경과함) 또는 재검증(재인증됨) 될 때까지 IBM MQ에 사인온한 상태로 남아 있습니다.

사용자가 제한시간을 초과하면 사용자 ID는 큐 관리자 내에서 사인오프되고 이 사용자에 대해 유지되던 모든 보안 관련 정보가 제거됩니다. 큐 관리자에서 사용자 사인온 및 사인오프는 애플리케이션 프로그램 또는 사용자에 대해 명확하지 않습니다.

사용자가 미리 판별된 기간 동안 어떤 IBM MQ 자원도 사용하지 않으면 제한시간 초과될 수 있습니다. 이 기간은 MQSC ALTER SECURITY 명령으로 설정됩니다.

두 개의 값이 ALTER SECURITY 명령에 지정 가능합니다.

TIMEOUT

사용되지 않은 사용자 ID 및 해당 관련 자원이 IBM MQ 큐 관리자에서 유지 가능한 기간(분).

INTERVAL

TIMEOUT이 만기되었는지 판별하기 위해 사용자 ID 및 해당 관련 자원에 대한 검사 사이의 기간(분).

예를 들어, TIMEOUT 값이 30이고 INTERVAL 값이 10이며 10분마다 IBM MQ는 사용자 ID와 해당하는 관련 자원을 검사하여 지난 30분 동안 사용되지 않은 것이 있는지를 판별합니다. 시간 종료된 사용자 ID가 발견되면 해당 사용자 ID가 큐 관리자 내에서 로그오프됩니다. 제한시간 초과되지 않은 사용자 ID에 연관된 모든 제한시간 초과된 자원 정보가 있는 경우 해당 자원 정보는 제거됩니다. 사용자 ID의 제한시간이 초과되지 않도록 하려면 INTERVAL 값을 0으로 설정하십시오. 그렇지만 INTERVAL 값이 0이면 사용자 ID 및 해당 관련 자원이 차지하는 스토리지는 REFRESH SECURITY 또는 RVERIFY SECURITY 명령을 발행할 때까지 다시 사용할 수 없습니다.

1회용 사용자가 많은 경우 이 값을 성능 조정하는 것이 중요합니다. 간격 및 제한시간 값을 작게 설정하면 더 이상 필요하지 않은 자원이 다시 사용 가능해 집니다.

참고: 기본값이 아닌 INTERVAL 또는 TIMEOUT 값을 사용하는 경우 큐 관리자가 시동될 때마다 명령을 다시 입력해야 합니다. ALTER SECURITY 명령을 해당 큐 관리자에 대한 CSQINP1 데이터 세트에 추가하여 자동으로 이를 수행할 수 있습니다.

z/OS z/OS에서 큐 관리자 보안 새로 고치기

IBM MQ for z/OS는 성능 향상을 위해 RACF 데이터를 캐시합니다. 특정 보안 클래스를 변경하는 경우, 이 캐시된 정보를 새로 고쳐야 합니다. 성능 향상을 위해 보안은 자주 새로 고치지 마십시오. TLS 보안 정보만 새로 고치도록 선택할 수도 있습니다.

큐를 처음으로 여는 경우(또는 보안 새로 고치기 이후 처음으로) IBM MQ는 RACF 검사를 수행하여 사용자의 액세스 권한을 가져와서 이 정보를 캐시에 배치합니다. 캐시된 데이터에는 보안 검사가 수행된 사용자 ID 및 자원이 포함됩니다. 동일한 사용자가 큐를 다시 여는 경우 캐시된 데이터의 존재는 IBM MQ가 RACF 검사를 발행할 필요가 없으며 이로 인해 성능이 향상될 수 있음을 나타냅니다. 보안 새로 고치기 조치는 캐시된 모든 보안 정보를 제거하고 IBM MQ가 RACF에 대해 새 검사를 수행하도록 강제 실행합니다. MQADMIN, MXADMIN, MQPROC, MXPROC, MQQUEUE, MXQUEUE, MQNLIST, MXNLIST 또는 MXTOPIC 클래스에 보유되는 RACF 자원 프로파일을 추가, 변경 또는 삭제할 때마다 이 클래스를 사용하여 보유한 보안 정보를 새로 고치도록 큐 관리자에 요청해야 합니다. 이를 수행하려면 다음 명령을 실행하십시오.

- RACF 레벨에서 새로 고치려면 RACF SETROPTS RACLIST(classname) REFRESH 명령.
- 큐 관리자가 보유한 보안 정보를 새로 고치려면 IBM MQ REFRESH SECURITY 명령. 이 명령은 변경된 프로파일일 때 액세스하는 각 큐 관리자가 발행해야 합니다. 큐 공유 그룹이 있는 경우 명령 범위 속성을 사용하여 명령이 그룹의 모든 큐 관리자로 전달되도록 할 수 있습니다.

참고: 기존 그룹에 새 사용자를 연결한 경우에는 IBM MQ RVERIFY SECURITY(userid) 명령을 실행해야 합니다. REFRESH SECURITY(*) 명령은 이 사용자가 다음에 IBM MQ 자원에 액세스하려 하는 경우 큐 관리자가 이 사용자를 다시 사인온하지 않도록 합니다.

임의 IBM MQ 클래스에서 일반 프로파일을 사용 중인 경우 임의의 일반 프로파일을 변경, 추가 또는 삭제하는 경우에도 정상 RACF 새로 고치 명령을 발행해야 합니다. 예를 들어, SETROPTS GENERIC(classname) REFRESH.

그러나 RACF RACF 자원 프로파일이 추가, 변경 또는 삭제되고 적용되는 자원이 아직 액세스되지 않은 경우(따라서 정보가 캐시되지 않음) IBM MQ는 REFRESH SECURITY 명령을 실행하지 않고 새 RACF 정보를 사용합니다.

RACF 감사가 켜진 경우(예를 들어, RACF RALTER AUDIT(access-attempt (audit_access_level)) 명령 사용) 캐시가 수행되지 않기 때문에 IBM MQ는 모든 검사에 대해 직접 RACF 데이터 공간을 참조합니다. 따라서 변경은 즉시 선택되고 REFRESH SECURITY는 변경에 액세스할 필요가 없습니다. RACF RLIST 명령을 사용하여 RACF 감사가 켜져있는지 여부를 확인할 수 있습니다. 예를 들어, 다음 명령을 발행할 수 있습니다.

```
RLIST MQQUEUE (qmgr.SYSTEM.COMMAND.INPUT) GEN
```

및 다음 결과 수신

```
CLASS      NAME
-----
MQQUEUE    QP*.SYSTEM.COMMAND.*.** (G)
           AUDITING
           -----
           FAILURES(READ)
```

이는 감사가 켜져 있음을 표시합니다. 자세한 정보는 *z/OS Security Server RACF Auditor's Guide* 및 *z/OS Security Server RACF Command Language Reference*를 참조하십시오.

224 페이지의 [그림 17](#)은 보안 정보가 캐시되고 캐시된 정보가 사용되는 상황을 요약합니다.

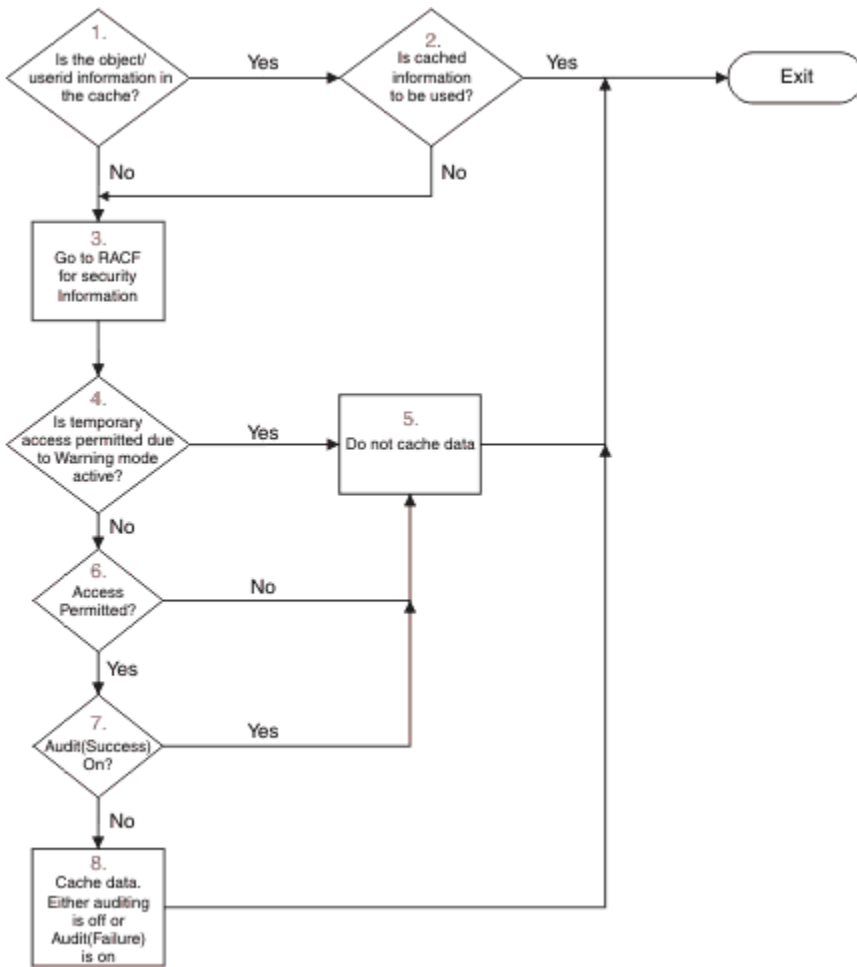


그림 17. IBM MQ 보안 캐싱에 대한 논리 플로우

MQADMIN 또는 MXADMIN 클래스에서 스위치 프로파일을 추가하거나 삭제하여 보안 설정을 변경하는 경우, 다음 명령 중 하나를 사용하여 해당 변경을 동적으로 선택하십시오.

```

REFRESH SECURITY(*)
REFRESH SECURITY(MQADMIN)
REFRESH SECURITY(MXADMIN)
  
```

즉, 새 보안 유형을 활성화하거나 큐 관리자를 다시 시작하지 않고 이를 비활성화할 수 있습니다.

성능 상의 이유로 REFRESH SECURITY 명령에 의해 영향받은 받는 클래스만 있습니다. MQCONN 또는 MQCMDSD 클래스의 프로파일을 변경하는 경우에는 REFRESH SECURITY를 사용하지 않아도 됩니다.

참고: MQADMIN 또는 MXADMIN 클래스 새로 고치기는 RESLEVEL 보안 프로파일을 변경하는 경우 필요하지 않습니다.

성능 상의 이유로 REFRESH SECURITY를 가능한 자주 사용하지 마십시오. 피크타임이 아닌 경우에만 사용하는 것이 좋습니다. 액세스 목록에 개별 사용자를 배치하지 않고 IBM MQ 프로파일의 액세스 목록에 이미 있는 RACF 그룹에 사용자를 연결하여 보안 새로 고치기의 수를 최소화할 수 있습니다. 이런 방식으로 자원 프로파일이 아니라 사용자를 변경합니다. 보안을 새로 고치는 대신 해당하는 사용자를 RVERIFY SECURITY할 수도 있습니다.

REFRESH SECURITY의 예로 큐 관리자 PRMQ에서 INSURANCE.LIFE로 시작되는 큐에 대한 액세스를 보호하기 위해 새 프로파일을 정의한다고 가정해 보십시오. 다음 RACF 명령을 사용합니다.

```

RDEFINE MQQUEUE PRMQ.INSURANCE.LIFE.** UACC(NONE)
PERMIT PRMQ.INSURANCE.LIFE.** ID(LIFEGRP) ACCESS(UPDATE)
  
```


다음 명령을 발행하여 RACF에게 보유 중인 보안 정보를 새로 고치도록 지시하십시오. 예:

```
SETROPTS RACLIST(MQQUEUE) REFRESH
```

해당 프로파일은 일반적이기 때문에 RACF가 MQQUEUE에 대한 일반 프로파일을 새로 고치도록 지시해야 합니다. 예를 들면, 다음과 같습니다.

```
SETROPTS GENERIC(MQQUEUE) REFRESH
```

그리고 다음 명령을 사용하여 큐 프로파일이 변경된 큐 관리자 PRMQ에 지시해야 합니다.

```
REFRESH SECURITY(MQQUEUE)
```

SSL/TLS 보안 새로 고치기

TLS 키 저장소의 캐시된 보기를 새로 고치려면 옵션 TYPE(SSL)이 지정된 REFRESH SECURITY 명령을 실행하십시오. 그러면 채널 시작기를 재시작하지 않고도 TLS 설정 일부를 업데이트할 수 있습니다.

보안 상태 표시

보안 스위치 상태 및 기타 보안 제어를 표시하려면 MQSC DISPLAY SECURITY 명령을 발행하십시오.

다음 그림은 DISPLAY SECURITY ALL 명령의 일반적인 출력을 표시합니다.

```
CSQH015I +CSQ1 Security timeout = 54 MINUTES
CSQH016I +CSQ1 Security interval = 12 MINUTES
CSQH030I +CSQ1 Security switches ...
CSQH034I +CSQ1 SUBSYSTEM: ON, 'SQ05.NO.SUBSYS.SECURITY' not found
CSQH032I +CSQ1 QMGR: ON, 'CSQ1.YES.QMGR.CHECKS' found
CSQH031I +CSQ1 QSG: OFF, 'SQ05.NO.QSG.CHECKS' found
CSQH031I +CSQ1 CONNECTION: OFF, 'CSQ1.NO.CONNECT.CHECKS' found
CSQH034I +CSQ1 COMMAND: ON, 'CSQ1.NO.COMMAND.CHECKS' not found
CSQH031I +CSQ1 CONTEXT: OFF, 'CSQ1.NO.CONTEXT.CHECKS' found
CSQH034I +CSQ1 ALTERNATE USER: ON, 'CSQ1.NO.ALTERNATE.USER.CHECKS' not found
CSQH034I +CSQ1 PROCESS: ON, 'CSQ1.NO.PROCESS.CHECKS' not found
CSQH034I +CSQ1 NAMELIST: ON, 'CSQ1.NO.NLIST.CHECKS' not found
CSQH034I +CSQ1 QUEUE: ON, 'CSQ1.NO.QUEUE.CHECKS' not found
CSQH034I +CSQ1 TOPIC: ON, 'CSQ1.NO.TOPIC.CHECKS' not found
CSQH031I +CSQ1 COMMAND RESOURCES: OFF, 'CSQ1.NO.CMD.RESC.CHECKS' found
CSQ9022I +CSQ1 CSQHPDTC ' DISPLAY SECURITY' NORMAL COMPLETION
```

그림 18. DISPLAY SECURITY 명령의 일반 출력

예는 명령에 회신하는 큐 관리자의 서브시스템, 명령, 대체 사용자, 프로세스, 이름 목록, 큐 보안이 큐 관리자 레벨에서 활성화되어 있지만 큐 공유 그룹 레벨에서는 그렇지 않습니다. 연결, 명령 자원, 컨텍스트 보안이 활성화되지 않습니다. 이는 사용자 ID 제한시간이 활성화되어 있고 12분마다 큐 관리자가 54분 동안 이 큐 관리자에서 사용되지 않은 사용자 ID를 검사하여 이를 제거하는 것도 보여줍니다.

참고: 이 명령은 현재 보안 상태를 보여줍니다. RACF에 정의된 스위치 프로파일의 현재 상태 또는 RACF 클래스 상태를 반영할 필요는 없습니다. 예를 들어, 스위치 프로파일은 이 큐 관리자의 마지막 재시작 또는 REFRESH SECURITY 명령 이후에 변경되었을 수 있습니다.

z/OS에 대한 보안 설치태스크

IBM MQ를 설치하고 사용자 정의한 후에 RACF에 대해 시작된 태스크 프로시저에 권한을 부여하고, 다양한 자원에 대한 액세스 권한을 부여하며 RACF 정의를 설정하십시오. 선택적으로 TLS에 대해 시스템을 구성하십시오.

IBM MQ가 처음으로 설치되고 사용자 정의되면 다음 보안 관련 태스크를 수행해야 합니다.

1. 다음을 수행하여 IBM MQ 데이터 세트 및 시스템 보안을 설정하십시오.

- 큐 관리자 시작 태스크 프로시저 xxxxMSTR 및 분산 큐인 시작 태스크 프로시저 xxxxCHIN이 RACF에서 실행되도록 권한 부여.

- 큐 관리자 데이터 세트에 대한 액세스 권한 부여.
 - 큐 관리자와 유틸리티 프로그램을 사용하는 해당 사용자 ID에 대해 자원 액세스 권한 부여.
 - 커풀링 기능 목록 구조를 사용하여 해당 큐 관리자에 대한 액세스 권한 부여.
 - Db2를 사용하는 해당 큐 관리자의 액세스 권한 부여.
2. IBM MQ 보안에 대한 RACF 정의를 설정하십시오.
 3. TLS(Transport Layer Security)를 사용하려면 시스템이 인증서 및 키를 사용하도록 준비하십시오.

z/OS IBM MQ for z/OS 데이터 세트 보안 설정

다양한 유형의 IBM MQ 사용자가 있습니다. RACF를 사용하여 시스템 데이터 세트에 대한 액세스를 제어하십시오.

IBM MQ 데이터 세트의 가능한 사용자에는 다음 엔티티가 포함됩니다.

- 큐 관리자 자체
- 채널 시작기
- IBM MQ 데이터 세트를 작성하고 유틸리티 프로그램을 실행하여 유사 태스크도 실행해야 하는 IBM MQ 관리자.
- IBM MQ 제공 사본, 포함 데이터 세트, 매크로, 유사 자원을 사용해야 하는 애플리케이션 프로그래머.
- 다음 중 하나 이상에 사용되는 애플리케이션:
 - 배치 작업
 - TSO 사용자
 - CICS 지역
 - IMS 지역
- 데이터 세트 CSQOUTX 및 CSQSNAP
- 동적 큐 SYSTEM.CSQXCMD.*

For all these potential users, protect the IBM MQ data sets with RACF.

'CSQINP' 데이터 세트에 대한 액세스도 제어해야 합니다.

z/OS 시작된 태스크 프로시저에 대한 RACF 권한

일부 IBM MQ 데이터 세트는 큐 관리자 독점 사용을 위한 것입니다. RACF를 사용하여 IBM MQ 데이터 세트를 보호하는 경우, RACF를 사용하여 큐 관리자 시작 태스크 프로시저 xxxxMSTR 및 분산 큐잉 시작 태스크 프로시저 xxxxCHIN도 권한 부여해야 합니다. 이를 수행하려면 STARTED 클래스를 사용하십시오. 또는, 표준 프로시저 테이블(ICHIN03)을 사용할 수 있지만, 이후 변경이 적용되기 전에 z/OS 시스템의 IPL을 수행해야 합니다.

자세한 정보는 *z/OS Security Server RACF System Programmer's Guide*를 참조하십시오.

식별되는 RACF 사용자 ID는 시작된 태스크 프로시저의 데이터 세트에 대해 필요한 액세스 권한이 있어야 합니다. 예를 들어, CSQ1MSTR의 큐 관리자가 시작한 태스크 프로시저를 RACF 사용자 ID QMGRCSQ1과 연관시키는 경우, 사용자 ID QMGRCSQ1은 CSQ1 큐 관리자가 액세스하는 z/OS 자원에 대해 액세스 권한이 있어야 합니다.

또한, 큐 관리자의 사용자 ID에서 GROUP 필드 콘텐츠는 해당 큐 관리자에 대한 STARTED 프로파일의 GROUP 필드 콘텐츠와 동일해야 합니다. 각 GROUP 필드의 콘텐츠가 일치하지 않으면 해당 사용자 ID는 시스템에 입력하지 못합니다. 이런 상황으로 인해 IBM MQ는 정의되지 않은 사용자 ID로 실행되고 결국 보안 위반으로 인해 종료됩니다.

큐 관리자 및 채널 시작기로 시작된 태스크 프로시저에 연관된 RACF 사용자 ID는 TRUSTED 속성이 설정되면 안 됩니다.

z/OS 데이터 세트에 대한 액세스 권한 부여

IBM MQ 데이터 세트는 권한 없는 사용자가 큐 관리자 인스턴스를 실행하거나 큐 관리자 데이터에 대한 액세스를 부여받지 못하도록 보호되어야 합니다. 그러려면 정상 z/OS RACF 데이터 세트 보호를 사용하십시오.

227 페이지의 표 65에서는 다른 데이터 세트에 대해 큐 관리자가 시작한 태스크 프로시저가 가져야 하는 RACF 액세스를 요약합니다.

표 65. 큐 관리자에 연관된 데이터 세트에 대한 RACF 액세스	
RACF 액세스	데이터 세트는
READ	<ul style="list-style-type: none"> • thlqual.SCSQAUTH 및 thlqual.SCSQANLx (여기서 x는 자국어에 대한 언어 문자입니다). • 큐 관리자로 시작된 태스크 프로시저에서 CSQINP1, CSQINP2, CSQXLIB로 참조되는 데이터 세트. • 그룹에 있는 다른 큐 관리자가 소유하는 SMDS 데이터 세트 • 그룹에 있는 다른 큐 관리자에 대한 로그, BSDS 및 아카이브 로그 데이터 세트
UPDATE	<ul style="list-style-type: none"> • 모든 페이지 세트 및 BSDS 데이터 세트. • 큐 관리자가 소유한 SMDS 데이터 세트
ALTER	<ul style="list-style-type: none"> • 모든 아카이브 로그 데이터 세트.

227 페이지의 표 66는 분산 큐잉에 대해 시작된 태스크 프로시저가 다른 데이터 세트에 대해 가져야 하는 RACF 액세스를 요약합니다.


표 66. 분산 큐잉에 연관된 데이터 세트에 대한 RACF 액세스	
RACF 액세스	데이터 세트는
READ	<ul style="list-style-type: none"> • thlqual.SCSQAUTH, thlqual.SCSQANLx(여기서 x는 자국어에 대한 언어 문자), thlqual.SCSQMVR1. • LE 라이브러리 데이터 세트. • 채널 시작기 시작 태스크 프로시저에서 CSQXLIB 및 CSQINPX에 의해 참조되는 데이터 세트.
UPDATE	<ul style="list-style-type: none"> • 데이터 세트 CSQOUTX 및 CSQSNAP

자세한 정보는 [z/OS Security Server RACF Security Administrator's Guide](#)를 참조하십시오.

데이터 세트 암호화

The IBM MQ data sets can be encrypted with z/OS data set encryption, so that the data is protected, or for regulatory reasons.

z/OS 데이터 세트를 사용하여 모든 페이지 세트, 활성 로그 및 부트스트랩(BSDS) 데이터 세트를 보호할 수 있습니다.

 **주의:** IBM MQ for z/OS 9.1.3 또는 그 이전에 z/OS 데이터 세트 암호화를 사용하여 공유 메시지 데이터 세트 (SMDS) 를 보호할 수 없습니다.

데이터 세트 암호화를 사용하는 IBM MQ for z/OS의 저장 데이터에 대한 기밀성 섹션을 참조하십시오. 참조하십시오.

IBM MQ for z/OS 자원 보안 설정

다양한 유형의 IBM MQ 사용자가 있습니다. RACF를 사용하여 IBM MQ 자원에 대한 액세스를 제어하십시오.

큐 및 채널과 같은 IBM MQ 자원에 대해 가능한 사용자에는 다음 엔티티가 포함됩니다.

- 큐 관리자 자체
- 채널 시작기

- IBM MQ 데이터 세트를 작성하고 유틸리티 프로그램을 실행하여 유사 태스크도 실행해야 하는 IBM MQ 관리자.
- IBM MQ 제공 사본, 포함 데이터 세트, 매크로, 유사 자원을 사용해야 하는 애플리케이션 프로그래머.
- 다음 중 하나 이상에 사용되는 애플리케이션:
 - 배치 작업
 - TSO 사용자
 - CICS 지역
 - IMS 지역
- 데이터 세트 CSQOUTX 및 CSQSNAP
- 동적 큐 SYSTEM.CSQXCMD.*

이러한 모든 잠재적 사용자에게 대해 IBM MQ 자원을 RACF로 보호하십시오. 특히, 채널 시작기는 233 페이지의 『z/OS에서 채널 시작기에 대한 보안 고려사항』에서 설명하는 대로 다양한 자원에 대해 액세스해야 하기 때문에 실행되는 사용자 ID는 해당 자원에 대한 액세스 권한이 부여되어야 합니다.

큐 공유 그룹을 사용 중인 경우 큐 관리자는 다양한 명령을 내부적으로 발행해야 할 수 있기 때문에 사용하는 사용자 ID는 이런 명령을 발행할 권한이 부여되어야 합니다. 해당 명령에는 다음이 포함됩니다.

- QSGDISP(GROUP)이 포함된 모든 오브젝트에 대한 DEFINE, ALTER, DELETE
- CHLDISP(SHARED)에서 사용되는 모든 채널에 대한 START 및 STOP CHANNEL

▶ z/OS TLS를 사용하도록 z/OS 시스템 구성

RACF 명령을 사용하여 TLS (Transport Layer Security) 로 IBM MQ for z/OS 를 구성하는 방법의 예제로 이 주제를 사용하십시오.

채널 보안에 TLS를 사용하려는 경우 시스템에서 몇 개의 태스크를 수행해야 합니다. (인증서 및 키 저장소(키링)에서의 RACF 명령 사용에 대한 자세한 내용은 z/OS에서 TLS에 대한 작업을 참조하십시오.)

1. RACF RACDCERT 명령을 사용하여 RACF에서 키링을 작성하여 시스템에 대한 모든 키와 인증서를 보유하십시오. 예를 들면, 다음과 같습니다.

```
RACDCERT ID(CHINUSER) ADDRING(QM1RING)
```

ID는 채널 시작기 주소 공간 사용자 ID 또는 공유 키링인 경우 키링을 소유하는 사용자 ID여야 합니다.

2. RACF RACDCERT 명령을 사용하여 각 큐 관리자에 대해 디지털 인증서를 작성하십시오.

인증서 레이블은 IBM MQ **CERTLABL** 속성 값(설정된 경우) 또는 큐 관리자 또는 큐 공유 그룹의 이름이 추가된 기본 **ibmWebSphereMQ**여야 합니다. 자세한 내용은 디지털 인증서 레이블을 참조하십시오. 이 예에서는 **ibmWebSphereMQM1**입니다.

예를 들면, 다음과 같습니다.

```
RACDCERT ID(USERID) GENCERT
SUBJECTSDN(CN('username') O('IBM') OU('departmentname') C('England'))
WITHLABEL('ibmWebSphereMQM1')
```

3. RACF RACDCERT 명령을 사용하여 RACF의 인증서를 키링에 연결하십시오. 예를 들면, 다음과 같습니다.

```
RACDCERT CONNECT(ID(USERID) LABEL('ibmWebSphereMQM1') RING(QM1RING))
CONNECT ID(CHINUSER)
```

키링에 관련된 모든 서명자 인증서(인증 기관의)에도 연결해야 합니다. 즉, 이 큐 관리자의 TLS 인증서에 대한 모든 인증 기관 및 이 큐 관리자가 통신하는 모든 TLS 인증서의 모든 인증 기관입니다. 예를 들면, 다음과 같습니다.

```
RACDCERT ID(CHINUSER)
CONNECT(CERTAUTH LABEL('My CA') RING(QM1RING) USAGE(CERTAUTH))
```

4. 각 큐 관리자에서 IBM MQ ALTER QMGR 명령을 사용하여 큐 관리자가 지시해야 하는 키 저장소를 지정하십시오. 예를 들어, 키링이 채널 시작기 주소 공간에서 소유되는 경우에는 다음과 같습니다.

```
ALTER QMGR SSLKEYR(QM1RING)
```

또는, 공유 키링을 사용 중인 경우는 다음과 같습니다.

```
ALTER QMGR SSLKEYR(userid/QM1RING)
```

여기서, *userid*는 공유 키링을 소유하는 사용자 ID입니다.

5. 인증서 폐기 목록(CRL)을 사용하면 인증 기관이 더 이상 신뢰할 수 없는 인증서를 폐기할 수 있습니다. CRL은 LDAP 서버에 저장됩니다. LDAP 서버에서 이 목록에 액세스하려면 우선 IBM MQ DEFINE AUTHINFO 명령을 사용하여 AUTHTYPE CRLLDAP의 AUTHINFO 오브젝트를 작성해야 합니다. 예를 들면, 다음과 같습니다.

```
DEFINE AUTHINFO(LDAP1)
AUTHTYPE(CRLLDAP)
CONNAME(ldap.server(389))
LDAPUSER('')
LDAPPWD('')
```

이 예에서는 인증서 폐기 목록이 LDAP 서버의 공개 영역에 저장되기 때문에 LDAPUSER 및 LDAPPWD 필드는 필요하지 않습니다.

그런 다음 IBM MQ DEFINE NAMELIST 명령을 사용해 AUTHINFO 오브젝트를 이름 목록에 넣으십시오. 예를 들면, 다음과 같습니다.

```
DEFINE NAMELIST(LDAPNL) NAMES(LDAP1)
```

마지막으로 IBM MQ ALTER QMGR 명령을 사용해 이름 목록을 각 큐 관리자와 연관시키십시오. 예를 들면, 다음과 같습니다.

```
ALTER QMGR SSLCRLNL(LDAPNL)
```

6. IBM MQ ALTER QMGR 명령을 사용하여 TLS 호출이 실행되도록 큐 관리자를 설정하십시오. 이는 SSL 호출만 처리하는 서버의 하위 태스크를 정의하며 이 경우 정상 디스패처는 어떠한 SSL 호출의 영향도 받지 않고 정상적으로 처리를 계속합니다. 이 하위 태스크 중 둘 이상이 있어야 합니다. 예를 들면, 다음과 같습니다.

```
ALTER QMGR SSLTASKS(8)
```

이런 변경은 채널 시작기가 재시작되는 경우에만 적용됩니다.

7. IBM MQ DEFINE CHANNEL 또는 ALTER CHANNEL 명령을 사용하여 각 채널에 사용되는 암호 스펙을 지정하십시오. 예를 들면, 다음과 같습니다.

```
ALTER CHANNEL(LDAPCHL)
CHLTYPE(SDR)
SSLCIPH(TLS_RSA_WITH_AES_128_CBC_SHA256)
```

채널 양 측 모두 동일한 암호 스펙을 지정해야 합니다.

z/OS 큐 공유 그룹에서 채널 인증 레코드 관리

채널 인증 레코드는 작성되는 큐 관리자에 적용되며 큐 공유 그룹(QSG) 내에서 공유되지 않습니다. 따라서, 큐 공유 그룹의 모든 큐 관리자가 동일한 규칙을 가져야 하는 경우 모든 규칙의 일관성을 유지하기 위해 일부 관리를 수행해야 합니다.

1. 항상 CMDSCOPE(*) 옵션은 모든 SET CHLAUTH 명령에 추가하십시오. 이는 큐 공유 그룹에서 실행 중인 모든 큐 관리자에 명령을 송신합니다.
2. DISPLAY CHLAUTH 명령과 CMDSCOPE(*) 옵션을 같이 사용하고 응답을 분석하여 레코드가 모든 큐 관리자에서 동일한지 확인하십시오. 불일치가 있는 경우 CMDSCOPE(*) 또는 CMDSCOPE(qmgr-name)이 있는 동일 규칙이 포함된 SET CHLAUTH 명령을 발행할 수 있습니다.
3. 전체 규칙 세트를 포함하는 큐 관리자의 CSQINP2 연속에 멤버를 추가하십시오(자세한 내용은 초기화 명령 참조). 이는 큐 관리자의 초기화 프로세스 중에 임합니다. SET CHLAUTH 명령이 ACTION(ADD)를 사용하면 규칙은 존재했던 적이 없는 경우에만 추가됩니다. ACTION(REPLACE) 사용은 기존 규칙이 이미 있는 경우 이를 대체하고 없는 경우에는 이를 추가합니다. 그러면 동일 멤버가 큐 공유 그룹의 모든 큐 관리자의 CSQINP2 연속에 배치될 수 있습니다.
4. CSQUTIL 유틸리티(자세한 내용은 IBM MQ에 명령 발행(COMMAND) 참조)를 사용하면 MAKEDEF 또는 MAKEREP 옵션을 사용하여 하나의 큐 관리자에서 규칙을 추출할 수 있습니다. 그런 다음 CSQUTIL을 사용하여 출력을 대상 큐 관리자로 응답하십시오.

관련 개념

채널 인증 레코드

채널 레벨에서 연결 시스템에 부여된 액세스 권한에 대한 보다 정밀한 제어를 실행하려면 채널 인증 레코드를 사용하십시오.

z/OS z/OS에서 감사 고려사항

정상 RACF 감사 제어는 큐 관리자 보안 감사 수행에 사용할 수 있습니다. IBM MQ는 자체적으로 어떤 보안 통계도 수집하지 않습니다. 감사로 작성 가능한 통계가 유일합니다.

RACF 감사는 다음을 기반으로 할 수 있습니다.

- 사용자 ID
- 자원 클래스
- 프로파일

자세한 내용은 *z/OS Security Server RACF Auditor's Guide*를 참조하십시오.

참고: 감사로 성능 저하: 구현하는 감사가 많아지면 성능이 더 저하됩니다. 이는 RACF WARNING 옵션 사용을 위한 고려사항이기도 합니다.

z/OS RESLEVEL 감사

RESAUDIT 시스템 매개변수를 사용하여 RESLEVEL 감사 레코드 프로덕션을 제어합니다. RACF GENERAL 감사 레코드가 생성됩니다.

RESAUDIT 시스템 매개변수를 YES로 설정하여 RESLEVEL 감사 레코드를 생성합니다. RESAUDIT 매개변수가 NO로 설정되면 감사 레코드가 생성되지 않습니다. 이 매개변수 설정에 대한 자세한 정보는 *CSQ6SYSP* 사용을 참조하십시오.

RESAUDIT가 YES로 설정되는 경우, hlq.RESLEVEL 프로파일에 대해 주소 공간 사용자 ID가 가지는 액세스를 확인하기 위해 RESLEVEL 검사를 수행할 때 정상 RACF 감사 레코드가 사용되지 않습니다. 대신, IBM MQ는 RACF가 GENERAL 감사 레코드(이벤트 번호 27)를 작성하도록 요청합니다. 이 검사는 연결 시에만 수행되기 때문에 성능 비용은 최소입니다.

IBM MQ 일반 감사 레코드는 RACF 보고서 기록기(RACFRW)를 사용하여 보고할 수 있습니다. 다음 RACFRW 명령을 사용하여 RESLEVEL 액세스를 보고할 수 있습니다.

```
RACFRW
SELECT PROCESS
EVENT GENERAL
LIST
END
```

Date, Time 및 SYSID 필드를 제외한 RACFRW의 샘플 보고서가 231 페이지의 그림 19에 표시됩니다.

RACF REPORT - LISTING OF PROCESS RECORDS PAGE 4

*JOB/USER	*STEP/	--TERMINAL--	--	E	V	Q	E	U	N	A
NAME	GROUP	ID	LVL	T	L	T	L	T	L	L
WS21B	MQMGRP	IGJZM000	0	27	0	JOBID=(WS21B 05.111 09:44:57),USERDATA=(
TRUSTED	USER					AUTH=(NONE),REASON=(NONE)				
						SESSION=TSOLOGON,TERMINAL=IGJZM000,				
						LOGSTR='CSQH RESLEVEL CHECK PERFORMED AGAINST				
						PROFILE(QM66.RESLEVEL),				
						CLASS(MQADMIN), ACCESS EQUATES TO				
						(CONTROL)',RESULT=SUCCESS,MQADMIN				

그림 19. RESLEVEL 일반 감사 레코드를 보여주는 RACFRW의 샘플 출력

이 샘플 출력의 LOGSTR 데이터 검사에서 TSO 사용자 WS21B가 QM66.RESLEVEL에 대해 CONTROL 액세스를 가지고 있는 것을 볼 수 있습니다. 이는 모든 자원 보안 검사가 WS21B 사용자가 QM66 자원에 액세스할 때 생략되는 것을 의미합니다.

RACFRW 사용에 대한 자세한 정보는 z/OS 보안 서버 RACF 작성자 안내서를 참조하십시오.

z/OS 보안 사용자 정의

IBM MQ 보안이 작동하는 방식을 변경하려면 이는 SAF 엑시트(ICHRFR00) 또는 외부 보안 관리자의 엑시트를 사용하여 수행해야 합니다.

RACF 엑시트에 대한 자세한 정보는 z/OS Security Server RACROUTE Macro Reference 매뉴얼을 참조하십시오.

참고: IBM MQ는 ESM에 대한 호출을 최적화하기 때문에 RACROUTE 요청은 예를 들어, 특정 사용자의 특정 큐에 대한 모든 열기에 대해 수행되지 않을 수도 있습니다.

z/OS에서 보안 위반 메시지

보안 위반은 애플리케이션 프로그램에서 리턴 코드 MQRC_NOT_AUTHORIZED 또는 작업 로그의 메시지로 표시됩니다.

MQRC_NOT_AUTHORIZED 리턴 코드는 다음과 같은 이유로 애플리케이션 프로그램에 리턴 가능합니다.

- 사용자의 큐 관리자 연결이 허용되지 않습니다. 이런 경우, 배치/TSO, CICS 또는 IMS 작업 로그에 KCH4081 메시지가 표시됩니다.
- 큐 관리자에 사용자의 사인온은 예를 들어, 작업 사용자 ID가 유효하지 않거나 적절하지 않음 또는 태스크 사용자 ID나 대체 사용자 ID가 유효하지 않아서 실패했습니다. 이런 사용자 ID 중 하나 이상이 취소 또는 삭제되어 유효하지 않을 수 있습니다. 이런 경우, 사인온 실패 이유를 표시하기 위해 큐 관리자 작업 로그에 ICHxxxx 메시지 및 가능한 경우 IRRxxxx 메시지도 표시됩니다. 예를 들면, 다음과 같습니다.


```

ICH408I USER(NOTDFND ) GROUP(          ) NAME(???)
LOGON/JOB INITIATION - USER AT TERMINAL          NOT RACF-DEFINED
IRR012I VERIFICATION FAILED. USER PROFILE NOT FOUND

```

- 대체 사용자가 요청되었지만 작업 또는 태스크 사용자 ID는 대체 사용자 ID에 액세스 권한이 없습니다. 이런 실패의 경우 관련 큐 관리자의 작업 로그에 위반 메시지가 표시됩니다.
- 컨텍스트 옵션이 사용되었거나 출력에 대한 전송 큐를 열어서 그럴 가능성이 있지만 작업 사용자 ID 또는 적용 가능한 경우 태스크 또는 대체 사용자 ID가 컨텍스트 옵션에 액세스 권한이 없습니다. 이런 경우, 위반 메시지가 관련 큐 관리자의 작업 로그에 추가됩니다.
- 권한 없는 사용자가 안전한 큐 관리자 오브젝트(예: 큐) 액세스를 시도했습니다. 이런 경우, 위반에 대한 ICH408I 메시지가 관련 큐 관리자의 작업 로그에 추가됩니다. 이 위반은 작업 때문일 수 있으며 적용 가능한 경우 태스크 또는 대체 사용자 ID로 인해 발생할 수 있습니다.

명령 보안 및 명령 자원 보안에 대한 위반 메시지는 큐 관리자의 작업 로그에서도 찾을 수 있습니다.

ICH408I 위반 메시지는 사용자 ID가 아니라 큐 관리자 jobname을 표시하면, 이는 일반적으로 지정 중인 공백 대체 사용자 ID의 결과입니다. 예를 들면, 다음과 같습니다.

```

ICH408I JOB(MQS1MSTR) STEP(MQS1MSTR)
MQS1.PAYROLL.REQUEST CL(MQQUEUE)
INSUFFICIENT ACCESS AUTHORITY
ACCESS INTENT(UPDATE ) ACCESS ALLOWED(NONE )

```

MQADMIN 프로파일 hlq.ALTERNATE.USER.-BLANK-의 액세스 목록을 검사하여 공백 대체 사용자 ID를 사용할 수 있는 사용자를 찾을 수 있습니다.

ICH408I 위반 메시지는 다음으로도 생성 가능합니다.

- 컨텍스트 없이 시스템 명령 입력 큐로 전송 중인 명령. 시스템 명령 입력 큐에 작성되는 사용자 작성 프로그램은 항상 컨텍스트 옵션을 사용해야 합니다. 자세한 정보는 194 페이지의 『컨텍스트 보안을 위한 프로파일』의 내용을 참조하십시오.
- IBM MQ 자원에 액세스하는 작업은 연관된 사용자 ID가 없는 경우 또는 IBM MQ 어댑터가 어댑터 환경에서 사용자 ID를 추출할 수 없는 경우.

위반 메시지는 큐 공유 그룹과 큐 관리자 레벨 보안 모두를 사용 중인 경우에도 발생할 수 있습니다. 큐 관리자 레벨에 프로파일이 없음을 나타내는 메시지가 표시될 수는 있지만 큐 공유 그룹 레벨 프로파일로 인해 여전히 액세스가 부여됩니다.

```

ICH408I JOB(MQS1MSTR) STEP(MQS1MSTR)
MQS1.PAYROLL.REQUEST CL(MQQUEUE)
PROFILE NOT FOUND - REQUIRED FOR AUTHORITY CHECKING
ACCESS INTENT(UPDATE ) ACCESS ALLOWED(NONE )

```

z/OS 액세스가 잘못 허용 또는 허용되지 않는 경우 수행할 작업

z/OS Security Server RACF Security Administrator's Guide에서 설명하는 단계뿐만 아니라 자원에 대한 액세스가 잘못 제어되는 것으로 보이는 경우 다음 체크리스트도 사용하십시오.

- 스위치 프로파일이 제대로 설정되었습니까?
 - RACF가 활성화되었습니까?
 - IBM MQ RACF 클래스가 설치되어 활성화되었습니까?
 - RACF 명령, SETROPTS LIST를 사용하여 이를 검사하십시오.
 - IBM MQ DISPLAY SECURITY 명령을 사용하여 큐 관리자에서 현재 스위치 상태를 표시하십시오.
 - MQADMIN 클래스에서 스위치 프로파일을 검사하십시오.

- 이에 대해 RACF 명령, SEARCH 및 RLIST를 사용하십시오.
- IBM MQ REFRESH SECURITY (MQADMIN) 명령을 실행하여 RACF 스위치 프로파일을 다시 확인하십시오.
- RACF 자원 프로파일이 변경되었습니까? 예를 들어, 프로파일의 유니버설 액세스가 변경되었거나 프로파일의 액세스 목록이 변경되었습니까?
 - 프로파일이 일반입니까?
 - 맞는 경우, RACF 명령, SETROPTS GENERIC(classname) REFRESH를 발행하십시오.
 - 이 큐 관리자에서 보안을 새로 고쳤습니까?
 - 필요한 경우, RACF 명령. SETROPTS RACLIST(classname) REFRESH를 발행하십시오.
 - 필요한 경우, IBM MQ REFRESH SECURITY(*) 명령을 실행하십시오.
- 사용자의 RACF 정의가 변경되었습니까? 예를 들어, 사용자가 새 그룹에 연결되었거나 사용자 액세스 권한이 취소되었습니까?
 - IBM MQ RVERIFY SECURITY(userid) 명령을 발행하여 사용자를 재확인했습니까?
- RESLEVEL로 인해 보안 검사를 생략 중입니까?
 - RESLEVEL 프로파일에 대한 연결 사용자 ID 액세스를 검사하십시오. RACF 감사 레코드를 사용하여 RESLEVEL이 설정된 사항을 판별하십시오.
 - 채널에 대해, 채널 시작기의 사용자 ID가 RESLEVEL이어야 하는 액세스 레벨이 모든 채널에서 상속되기 때문에 모든 검사를 생략해야 하는 ALTER와 같은 액세스 레벨로 인해 보안 검사가 모든 채널에 대해 생략됩니다.
 - CICS에서 실행 중인 경우 트랜잭션의 RESSEC 설정을 검사하십시오.
 - RESLEVEL이 사용자 연결 중에 변경되는 경우, 새 RESLEVEL 설정이 적용되기 전에 연결을 끊고 다시 연결해야 합니다.
- 큐 공유 그룹을 사용 중입니까?
 - 큐 공유 그룹 및 큐 관리자 레벨 보안을 모두 사용 중인 경우, 모든 올바른 프로파일을 정의했는지 확인하십시오. 큐 관리자 프로파일이 정의되지 않은 경우 프로파일을 찾을 수 없음을 나타내는 메시지가 로그에 송신됩니다.
 - 전체 보안 검사 설정을 초래하는 올바르지 않은 스위치 설정 결합을 사용했습니까?
 - 큐 관리자에 대해 큐 공유 그룹 설정 일부를 대체하도록 보안 스위치를 정의할 필요가 있습니까?
 - 큐 관리자 레벨 프로파일이 큐 공유 그룹 레벨 프로파일보다 우선적으로 사용됩니까?

z/OS에서 채널 시작기에 대한 보안 고려사항

분산 큐잉 환경에서 자원 보안을 사용 중인 경우 채널 시작기 주소 공간에는 다양한 IBM MQ 자원에 대해 해당 액세스 권한이 필요합니다. ICSF(Integrated Cryptographic Support Facility)를 사용하여 비밀번호 보호 알고리즘을 시드할 수 있습니다.

자원 보안 사용

자원 보안을 사용 중인 경우 분산 큐잉을 사용하고 있다면 다음과 같은 점도 고려하십시오.

시스템 큐

The channel initiator address space needs RACF UPDATE access to the system queues listed at [184 페이지의 『시스템 큐 보안』](#), and to all the user destination queues and the dead-letter queue (but see [183 페이지의 『데드-레터 큐 보안』](#)).

전송 큐

채널 시작기 주소 공간은 모든 사용자 전송 큐에 대해 ALTER 액세스가 필요합니다.

컨텍스트 보안

채널 사용자 ID(및 MCA 사용자 ID가 지정된 경우 MCA 사용자 ID)는 MQADMIN 클래스의 hlq.CONTEXT.queueName 프로파일에 대해 RACF CONTROL 액세스가 필요합니다. RESLEVEL 프로파일에 따라 채널 사용자 ID는 해당 프로파일에 대해 CONTROL 액세스도 필요할 수 있습니다.

모든 채널은 MQADMIN hlq.CONTEXT에 대한 CONTROL 액세스 권한이 필요합니다. 데드-레터 큐 프로파일. 모든 채널(시작 또는 응답에 따라)은 보고서를 생성할 수 있으며 결과적으로 hlq.CONTEXT.reply-q 프로파일에 대해 CONTROL 액세스가 필요합니다.

SENDER, CLUSSDR, SERVER 채널은 채널을 시작해서 정상적으로 종료하기 위해 전송 큐에 메시지를 넣을 수 있으려면 hlq.CONTEXT.xmit-queue-name 프로파일에 대해 CONTROL 액세스가 필요합니다.

참고: 채널 사용자 ID 또는 채널 사용자 ID가 연결된 RACF 그룹이 hlq.RESLEVEL에 대해 CONTROL 또는 ALTER 액세스를 가지는 경우 채널 시작기 또는 다른 해당 채널에 대해 자원 검사가 없습니다.

자세한 정보는 194 페이지의 『컨텍스트 보안을 위한 프로파일』 211 페이지의 『RESLEVEL 및 채널 시작기 연결』 및 213 페이지의 『z/OS의 보안 검사를 위한 사용자 ID』의 내용을 참조하십시오.

CSQINPX

CSQINPX 입력 데이터 세트를 사용 중인 경우 채널 시작기는 CSQINPX에 대해 READ 액세스가 필요하고 데이터 세트 CSQOUTX 및 동적 큐 SYSTEM.CSQXCMD.*에 대해 UPDATE 액세스도 필요합니다.

연결 보안

채널 시작기 주소 공간 연결 요청의 경우 적절한 액세스 보안이 설정되어야 하는 CHIN 연결 유형을 사용해야 합니다. 178 페이지의 『채널 시작기에 대한 연결 보안 프로파일』의 내용을 참조하십시오.

데이터 세트는

채널 시작기 주소 공간에는 큐 관리자 데이터 세트에 대해 적절한 액세스가 필요합니다. 226 페이지의 『데이터 세트에 대한 액세스 권한 부여』의 내용을 참조하십시오.

명령

분산 큐잉 명령(예: DEFINE CHANNEL, START CHINIT, START LISTENER, 기타 채널 명령)에는 해당 명령 보안 세트가 있어야 합니다. 197 페이지의 표 49의 내용을 참조하십시오.

큐 공유 그룹을 사용 중인 경우 채널 시작기는 다양한 명령을 내부적으로 발행해야 할 수 있기 때문에 사용하는 사용자 ID는 이런 명령을 발행할 권한이 부여되어야 합니다. 이 명령은 CHLDISP(SHARED)에서 사용되는 모든 채널에 대한 START 및 STOP CHANNEL입니다.

큐 관리자의 PSMODE가 DISABLED가 아닌 경우, 채널 시작기는 DISPLAY PUBSUB 명령에 대해 READ 액세스가 있어야 합니다.

채널 보안

채널, 특히 수신자 및 서버 연결의 경우 적절한 보안을 설정해야 합니다. 자세한 정보는 213 페이지의 『z/OS의 보안 검사를 위한 사용자 ID』의 내용을 참조하십시오.

TLS(Transport Layer Security) 프로토콜을 사용하여 채널에 보안도 제공할 수 있습니다. IBM MQ에서 TLS 사용에 대한 자세한 정보는 21 페이지의 『IBM MQ의 TLS 보안 프로토콜』를 참조하십시오.

서버 연결 보안에 대한 정보에 대해서는 86 페이지의 『클라이언트의 액세스 제어』도 참조하십시오.

사용자 ID

216 페이지의 『채널 시작기에서 사용되는 사용자 ID』 및 219 페이지의 『내부 그룹 큐잉 에이전트가 사용하는 사용자 ID』에서 설명하는 사용자 ID는 다음 액세스가 필요합니다.

- 해당 목적지 큐 및 데드-레터 큐에 대해 RACF UPDATE 액세스
- 수신자에서 컨텍스트 점검이 수행되는 경우 hlq.CONTEXT.queueName 프로파일에 대한 RACF CONTROL 액세스
- 사용해야 할 수도 있는 hlq.ALTERNATE.USER.userid 프로파일에 해당하는 액세스
- 클라이언트의 경우 사용되는 자원에 대한 적절한 RACF 액세스

APPC 보안

LU 6.2 전송 프로토콜을 사용 중인 경우 적절한 APPC 보안을 설정하십시오. (예를 들어, APPCLU RACF 클래스를 사용하십시오.) APPC에 대한 보안 설정 정보는 다음 매뉴얼을 참조하십시오.

- z/OS V1R2.0 MVS 계획: APPC 관리
- Multiplatform APPC 구성 안내서, IBM Redbooks 서적

아웃바운드 전송은 "SECURITY(SAME)" APPC 옵션을 사용합니다. 따라서, 채널 시작기 주소 공간의 사용자 ID 및 해당 기본 프로파일(RACF GROUP)은 사용자 ID가 이미 확인한(ALREADYV) 표시기를 사용하여 네트워크를 통해 수신자로 플로우됩니다.

수신 측도 z/OS인 경우, 사용자 ID와 프로파일은 APPC로 확인되고 사용자 ID는 수신자 채널에 표시되어 채널 사용자 ID로 사용됩니다.

큐 관리자가 APPC를 사용하여 동일한 또는 다른 z/OS 시스템의 다른 큐 관리자와 통신하는 환경에서는 다음도 확인해야 합니다.

- LU와 통신하는 VTAM 정의는 SETACPT(ALREADYV) 지정
- SETACPT(ALREADYV)를 지정하는 LU 사이의 연결에 대해 RACF APPCLU 프로파일이 있음

보안 설정 변경

채널 사용자 ID 또는 MCA 사용자 ID가 목적지 큐에 대해 가지는 RACF 액세스 레벨이 변경되는 경우 이 변경은 목적지 큐에 대한 새 오브젝트 핸들(즉, 새 MQOPEN)에 대해서만 적용됩니다. MCA가 큐를 열고 닫는 시간은 가변적입니다. 채널이 이런 액세스 변경이 수행될 때 이미 실행 중인 경우, MCA는 업데이트된 보안 액세스가 아니라 사용자 ID의 기존 보안 액세스를 사용하여 목적지 큐에 메시지를 계속 넣을 수 있습니다. 채널을 중지하고 다시 시작하면 업데이트된 액세스 레벨이 이 시나리오를 더 이상 사용할 수 없습니다.

자동 재시작

z/OS 자동 재시작 관리자(ARM)를 사용하여 채널 시작기를 재시작하는 경우 XCFAS 주소 공간에 연관된 사용자 ID IBM MQ START CHINIT 명령을 발행한 권한이 있어야 합니다.

ICSF(Integrated Cryptographic Service Facility) 사용

채널 시작기는 TLS가 사용 중이 아닌 경우 클라이언트 채널을 통해 흐르는 비밀번호를 난독화하기 위해 비밀번호 보호 알고리즘 시드(seed)를 수행할 때 ICSF를 사용하여 난수를 생성할 수 있습니다. 난수 생성 프로세스를 엔트로피라고 합니다.

z/OS 기능이 설치되어 있지만 ICSF는 시작하지 않은 경우 CSQX213E 메시지가 표시되고 채널 시작기는 엔트로피에 대해 STCK를 사용합니다.

메시지 CSQX213E는 메시지 비밀번호 보호 알고리즘이 그다지 안전하지 않음을 경고합니다. 그렇지만 프로세스는 계속 수행할 수 있으며 런타임에는 아무런 영향도 주지 않습니다.

z/OS 기능이 설치되어 있지 않은 경우 채널 시작기는 자동으로 STCK를 사용합니다.

참고사항:

1. 엔트로피에 대해 ICSF를 사용하면 STCK 사용 시보다 더 많은 임의 순서가 생성됩니다.
2. ICSF를 시작하는 경우, 채널 시작기를 다시 시작해야 합니다.
3. ICSF는 특정 CipherSpec에 필요합니다. 이 CipherSpec 중 하나를 사용하도록 하지만 ICSF가 설치되지 않은 경우 CSQX629E 메시지가 수신됩니다.

z/OS의 큐 관리자 클러스터에서 보안

클러스터에 대한 보안 고려사항은 클러스터되지 않은 큐 관리자 및 채널에 대해 동일합니다. 채널 시작기는 일부 추가 시스템 큐에 대한 액세스가 필요하며 일부 추가 명령은 적절한 보안 세트가 필요합니다.

MCA 사용자 ID, 채널 인증 레코드, TLS, 보안 엑시트를 사용하여 클러스터 채널을 인증할 수 있습니다(일반적인 채널로). 클러스터 수신자 채널에 연관된 채널 인증 레코드 또는 보안 엑시트는 리모트 큐 관리자가 서버 큐 관리자의 클러스터 큐에 대한 액세스가 허용되는지를 검사해야 합니다. 기존 큐 액세스 보안을 변경하지 않고 IBM MQ 클러스터 지원을 사용하여 시작할 수 있습니다. 그렇지만 클러스터의 다른 큐 관리자가 클러스터를 조인하는 경우, SYSTEM.CLUSTER.COMMAND.QUEUE에 쓰는 것을 허용해야 합니다.

IBM MQ 클러스터 지원은 클라이언트 역할에만 대한 클러스터 멤버를 제한하는 메커니즘을 제공하지 않습니다. 그렇기 때문에 클러스터에 허용하는 모든 큐 관리자를 신뢰할 수 있어야 합니다. 클러스터의 임의 큐 관리자가 특정 이름의 큐를 작성하는 경우, 이는 메시지를 해당 큐에 넣는 애플리케이션의 의도에 상관없이 해당 큐에 대한 메시지를 수신할 수 있습니다.

클러스터 멤버십을 제한하려면 큐 관리자가 수신자 채널에 연결되는 것을 방지할 때 수행한 조치와 동일한 조치를 수행하십시오. 채널 인증 레코드를 사용하거나 수신자 채널에 보안 엑시트 프로그램을 작성하여 클러스터 멤버십을 제한할 수 있습니다. 권한 없는 큐 관리자가 SYSTEM.CLUSTER.COMMAND.QUEUE에 쓰는 것을 방지하는 엑시트 프로그램을 작성할 수도 있습니다.

참고: 애플리케이션이 SYSTEM.CLUSTER.TRANSMIT.QUEUE를 직접 열도록 허용하는 것은 바람직하지 않습니다. 또한, 애플리케이션이 다른 임의 전송 큐를 직접 열도록 허용하는 것도 바람직하지 않습니다.

자원 보안을 사용 중인 경우 233 페이지의 『z/OS에서 채널 시작기에 대한 보안 고려사항』에 포함되는 고려사항뿐만 아니라 다음과 같은 점도 고려하십시오.

시스템 큐

채널 시작기는 다음 시스템 큐에 대해 RACF ALTER 액세스가 필요합니다.

- SYSTEM.CLUSTER.COMMAND QUEUE
- SYSTEM.CLUSTER.TRANSMIT.QUEUE.

및 SYSTEM.CLUSTER.REPOSITORY.QUEUE에 대한 UPDATE 액세스

클러스터링에 사용되는 모든 이름 목록에 대한 READ 액세스도 필요합니다.

명령

클러스터 지원 명령(REFRESH and RESET CLUSTER, SUSPEND, RESUME QMGR)에 대해 197 페이지의 표 49에서 설명하는 대로 적합한 명령 보안을 설정하십시오.

z/OS CICS 에서 IBM MQ 사용에 대한 보안 고려사항

IBM MQ 9.0.0에서 지원하는 모든 CICS 버전과 나중에 어댑터 및 브릿지의 CICS 제공 버전을 사용하십시오.

보안 고려사항에 대한 자세한 정보는 다음을 참조하십시오.

- [CICS-IBM MQ 어댑터에 대한 보안.](#)
- [CICS-IBM MQ 브릿지에 대한 보안.](#)

z/OS IMS 에서 IBM MQ 사용에 대한 보안 고려사항

IBM MQ를 IMS와 함께 사용할 때 보안 요구사항을 계획하려면 이 주제를 사용하십시오.

OPERCMDS 클래스 사용

OPERCMDS 클래스에서 자원을 보호하기 위해 RACF를 사용 중인 경우에는 IBM MQ 큐 관리자 주소 공간과 연관된 사용자 ID에 이 사용자 ID가 연결할 수 있는 IMS 시스템에 MODIFY 명령을 실행할 권한이 있는지 확인하십시오.

IMS 브릿지에 대한 보안 고려사항

IMS 브릿지의 보안 요구사항을 결정할 때 고려해야 할 네 가지 측면은 다음과 같습니다.

- IBM MQ를 IMS에 연결할 때 필요한 보안 권한
- IMS에 액세스하기 위해 브릿지를 사용하여 애플리케이션에서 수행하는 보안 검사의 양
- 이러한 애플리케이션이 사용할 수 있는 IMS 자원
- 브릿지가 놓고 가져오는 메시지에 사용될 권한

IMS 브릿지에 대한 보안 요구사항을 정의할 때 다음을 고려해야 합니다.

- 브릿지를 걸쳐 지나가는 메시지가 강력한 보안 기능을 제공하지 않는 플랫폼 상의 애플리케이션에서 발생했을 수도 있습니다.
- 브릿지를 걸쳐 지나가는 메시지가 동일 엔터프라이즈 또는 조직이 제어하지 않는 애플리케이션에서 발생했을 수도 있습니다.

z/OS IMS에 연결하기 위한 보안 고려사항

IBM MQ 큐 관리자 주소 공간 액세스의 사용자 ID를 OTMA 그룹에 부여하십시오.

IMS 브릿지는 OTMA 클라이언트입니다. IMS로의 연결은 IBM MQ 큐 관리자 주소 공간의 사용자 ID 하에서 작동합니다. 이는 일반적으로 시작된 태스크 그룹의 구성원으로 정의됩니다. 이 사용자 ID에는 OTMA 그룹에 대한 액세스가 부여되어야 합니다(/SECURE OTMA 설정이 NONE이 아닌 한).

이를 수행하려면 FACILITY 클래스에서 다음 프로파일을 정의하십시오.

```
IMSXCF.xcfigname.mqxcfmname
```

여기서 xcfigname은 XCF 그룹 이름이고 mqxcfmname은 IBM MQ의 XCF 구성원 이름입니다.

이 프로파일에 사용자의 IBM MQ 큐 관리자 사용자 ID 읽기 액세스를 제공해야 합니다.

참고:

1. FACILITY 클래스에서 권한을 변경하는 경우 변경사항을 활성화하려면 RACF 명령 SETROPTS RACLIST(FACILITY) REFRESH을 실행해야 합니다.
2. 프로파일 hlq.NO.SUBSYS.SECURITY가 MQADMIN 클래스에 있는 경우, /SECURE OTMA 설정이 NONE이 아닌 한 IMS에 사용자 ID가 전달되지 않고 연결이 실패합니다.

IMS 브릿지에 대한 애플리케이션 액세스 제어

각 IMS 시스템에 대한 FACILITY 클래스에 RACF 프로파일을 정의하십시오. IBM MQ 큐 관리자 사용자 ID에 적합한 액세스 레벨을 부여하십시오.

IMS 연결하는 각 IMS 시스템에 대해 FACILITY 클래스에 다음 RACF 프로파일을 정의하여 IMS 시스템에 전달된 각 메시지에 대해 수행되는 보안 검사의 양을 판별할 수 있습니다.

```
IMSXCF.xcfigname.imsxcfmname
```

여기서 xcfigname은 XCF 그룹 이름이고 imsxcfmname은 IMS의 XCF 구성원 이름입니다. (각 IMS 시스템에 별도의 프로파일을 정의해야 합니다.)

이 프로파일의 IBM MQ 큐 관리자 사용자 ID에 대해 허용하는 액세스 레벨은 IMS IMS에 연결될 때 IBM MQ 로 리턴되며 후속 트랜잭션에 필요한 보안 레벨을 표시합니다. 후속 트랜잭션의 경우 IBM MQ는 RACF에게 적합한 서비스를 요청하고 여기서 사용자 ID가 권한 부여되고, 메시지를 IMS에 전달합니다.

OTMA는 IMS /SIGN 명령을 지원하지 않습니다. 그러나 IBM MQ는 필요한 제어 레벨을 구현하기 위해 각 메시지의 액세스 검사를 설정할 수 있도록 허용합니다.

다음 액세스 레벨 정보가 리턴될 수 있습니다.

NONE 또는 NO PROFILE FOUND

이러한 값은 최대 보안이 필요함을 나타냅니다. 즉, 모든 트랜잭션에 대해 인증이 필요합니다. MQMD 구조의 *UserIdentifier* 필드에 지정된 사용자 ID 및 MQIIB 구조의 *Authenticator* 필드에 지정된 비밀번호 또는 PassTicket이 RACF에 알려져 있는지와 올바른 결합인지를 확인하는 검사가 수행됩니다. UTOKEN은 비밀번호 또는 PassTicket과 함께 작성되고 IMS에 전달됩니다. UTOKEN은 캐싱되지 않습니다.

참고: 프로파일 hlq.NO.SUBSYS.SECURITY가 MQADMIN 클래스에 있으면, 이 보안 레벨은 프로파일에 정의된 내용을 대체합니다.

READ

이 값은 다음 상황 하에서는 NONE에 관해서는 동일한 인증이 수행됨을 나타냅니다.

- 특정 사용자 ID를 처음 마주칠 때
- 사용자 ID는 이전에 마주쳤지만 캐싱된 UTOKEN이 비밀번호 또는 PassTicket을 사용하여 작성되지 않은 경우

IBM MQ는 필요한 경우 UTOKEN을 요청하고 이를 IMS에 전달합니다.

참고: 보안을 재검증하기 위한 요청이 작용하면 모든 캐싱된 정보는 유실되고 나중에 각 사용자 ID를 처음 마주칠 때 UTOKEN이 요청됩니다.

UPDATE

MQMD 구조의 *UserIdentifier* 필드에 있는 사용자 ID가 RACF에 알려져 있는지 확인하기 위한 검사가 수행됩니다.

UTOKEN이 빌드되고 IMS에 전달됩니다. UTOKEN이 캐싱됩니다.

CONTROL/ALTER

이러한 값은 이 IMS 시스템에 대해 보안 UTOKEN을 제공할 필요가 없음을 나타냅니다. (개발과 테스트 시스템을 위해서만 이 옵션을 사용하게 될 것입니다.)



주의: MQMD 구조의 *UserIdentifier* 필드에 포함된 사용자 ID는 여전히 **CONTROL/ALTER**에 대해 전달됨을 유의하십시오.

참고:

1. 이 액세스는 IBM MQ이 IMS에 연결할 때 정의되고, 연결 지속 기간 동안 지속됩니다. 보안 레벨을 변경하려면 보안 프로파일에 대한 액세스를 변경한 다음에 브릿지가 중지 및 재시작되어야 합니다(예를 들어, OTMA를 중지한 후 재시작하여).
2. FACILITY 클래스에서 권한을 변경하는 경우 변경사항을 활성화하려면 RACF 명령 SETROPTS RACLIST(FACILITY) REFRESH을 실행해야 합니다.
3. 비밀번호나 PassTicket을 사용할 수 있지만 IMS 브릿지가 데이터를 암호화하지 않는다는 점을 기억해야 합니다. PassTicket 사용에 대한 자세한 정보는 239 페이지의 『IMS 헤더에서 RACF PassTickets 사용』의 내용을 참조하십시오.
4. 이러한 결과의 일부는 /SECURE OTMA 명령을 사용하여 IMS의 보안 설정에 의해 영향을 받을 수도 있습니다.
5. 캐싱된 UTOKEN 정보는 IBM MQ ALTER SECURITY 명령의 INTERVAL 및 TIMEOUT 매개변수에 의해 정의된 지속 기간 동안 보유됩니다.
6. RACF WARNING 옵션은 IMSXCF.xcfgname.imsxcfname 프로파일에 영향을 미치지 않습니다. 이를 사용해도 부여된 액세스 레벨에 영향을 미치지 않고 RACF WARNING 메시지가 생성되지 않습니다.

z/OS IMS에 대한 보안 검사

브릿지를 걸쳐 지나가는 메시지에는 보안 정보가 들어 있습니다. 보안 검사는 IMS 명령 /SECURE OTMA의 설정에 따라 수행됩니다.

브릿지를 걸쳐 지나가는 각 IBM MQ 메시지에는 다음 보안 정보가 들어 있습니다.

- MQMD 구조의 *UserIdentifier* 필드에 포함되는 사용자 ID
- MQIIH 구조의 *SecurityScope* 필드에 포함되는 보안 범위(MQIIH 구조가 있는 경우)
- UTOKEN(IBM MQ 서브시스템에 관련 IMSXCF.xcfgname.imsxcfname 프로파일에 대한 CONTROL 또는 ALTER 액세스가 있지 않는 한)

보안 검사는 다음과 같이 IMS 명령 /SECURE OTMA의 설정에 따라 수행됩니다.

/SECURE OTMA NONE

트랜잭션을 위한 어떤 보안 검사도 수행하지 않습니다.

/SECURE OTMA CHECK

MQMD 구조의 *UserIdentifier* 필드가 트랜잭션 또는 명령 권한 검사를 위해 IMS에 전달됩니다.

ACEE(Accessor Environment Element)가 IMS 제어 영역에 빌드됩니다.

/SECURE OTMA FULL

MQMD 구조의 *UserIdentifier* 필드가 트랜잭션 또는 명령 권한 검사를 위해 IMS에 전달됩니다.

ACEE는 IMS 의존 영역뿐만 아니라 IMS 제어 영역에 빌드됩니다.

/SECURE OTMA PROFILE

MQMD 구조의 *UserIdentifier* 필드가 트랜잭션 또는 명령 권한 검사를 위해 IMS에 전달됩니다.

MQIIH 구조의 *SecurityScope* 필드는 IMS 의존 영역뿐만 아니라 제어 영역에 ACEE를 빌드할지 여부를 판별하는 데 사용됩니다.

참고:

1. TIMS 또는 CIMS 클래스 또는 연관된 그룹 클래스 GIMS 또는 DIMS에서 권한을 변경하는 경우에는 변경사항을 활성화하려면 다음 IMS 명령을 실행해야 합니다.
 - /MODIFY PREPARE RACF

- /MODIFY COMMIT

2. /SECURE OTMA PROFILE을 사용하지 않는 경우에는 MQIIB 구조의 *SecurityScope* 필드에 지정된 값이 무시됩니다.

▶ z/OS IMS 브릿지에 의해 수행되는 보안 검사

수행 중인 조치에 따라 다른 권한이 사용됩니다.

브릿지가 메시지를 넣거나 가져올 때 다음 권한이 사용됩니다.

브릿지 큐로부터 메시지 가져오기
보안 검사가 수행되지 않습니다.

예외 또는 COA 보고서 메시지 넣기
MQMD 구조의 *UserIdentifier* 필드에서 사용자 ID의 권한을 사용합니다.

응답 메시지 넣기
원본 메시지의 MQMD 구조의 *UserIdentifier* 필드에서 사용자 ID의 권한을 사용합니다.

데드-레터 큐에 메시지 넣기
보안 검사가 수행되지 않습니다.

참고:

1. IBM MQ 클래스 프로파일을 변경하는 경우에는 변경사항을 활성화하려면 IBM MQ REFRESH SECURITY(*) 명령을 실행해야 합니다.
2. 사용자의 권한을 변경하는 경우 변경사항을 활성화하려면 MQSC RVERIFY SECURITY 명령을 실행해야 합니다.

▶ z/OS IMS 헤더에서 RACF PassTickets 사용

IMS 헤더에서 비밀번호의 위치에 PassTicket을 사용할 수 있습니다.

IMS 헤더(MQIIB)에서 비밀번호 대신에 PassTicket을 사용하고 싶으면 메시지가 라우트될 IMS 브릿지 큐의 STGCLASS 정의의 PASSTKTA 속성에서 PassTicket이 유효성 검증되는 대상 애플리케이션 이름을 지정하십시오.

PASSTKTA 값이 공백으로 남겨지면 PassTicket이 생성되도록 배열해야 합니다. 이 경우 애플리케이션 이름은 MVSxxxx 양식이어야 합니다. 여기서 xxxx는 대상 큐 관리자가 실행되는 z/OS 시스템의 SMFID입니다.

PassTicket은 사용자 ID, 대상 애플리케이션 이름 및 보안 키로부터 빌드됩니다. 이는 대문자 알파벳 및 숫자 문자를 포함하는 8바이트 값입니다. 이는 한 번만 사용될 수 있고 20분 동안 유효합니다. PassTicket이 로컬 RACF 시스템에 의해 생성되면, RACF는 프로파일이 존재하는지만 검사하고 사용자에게 프로파일에 대한 권한이 있는지는 검사하지 않습니다. PassTicket이 원격 시스템에서 생성된 경우에는 RACF는 프로파일에 대한 사용자 ID의 액세스를 유효성 검증합니다. PassTicket에 대한 자세한 정보는 *z/OS SecureWay Security Server RACF Security Administrator's Guide*를 참조하십시오.

IMS 헤더의 PassTickets 은 IMS가 아니라 IBM MQ에 의해 RACF 에 제공됩니다.

▶ z/OS z/OS 대소문자 혼용 보안으로 큐 관리자 마이그레이션

다음 단계에 따라 대소문자 혼용 보안으로 큐 관리자를 마이그레이션합니다. 사용하는 보안 제품 레벨을 검토하고 새 IBM MQ 외부 보안 모니터 클래스를 활성화합니다. **REFRESH SECURITY** 명령을 실행하여 대소문자 혼용 프로파일을 활성화합니다.

시작하기 전에

1. 모든 IBM MQ 외부 보안 모니터 클래스가 활성화되었는지 확인하십시오.
2. 큐 관리자가 시작되었는지 확인하십시오.

이 태스크 정보

다음 단계에 따라 대소문자 혼용 보안으로 큐 관리자를 변환하십시오.

프로시저

1. 기존 모든 프로파일 및 액세스 레벨을 대문자 클래스에서 이에 해당하는 대소문자 혼용 외부 보안 모니터 클래스로 복사하십시오.
 - a) MQADMIN에서 MXADMIN으로.
 - b) MQPROC에서 MXPROC으로.
 - c) MQNLIST에서 MXNLIST으로.
 - d) MQQUEUE에서 MXQUEUE으로.
2. SCYCASE 속성의 값을 MIXED로 변경하십시오.

```
ALTER QMGR SCYCASE(MIXED)
```

3. 기존 보안 프로파일을 활성화하십시오.

```
REFRESH SECURITY(*) TYPE(CLASSES)
```

4. 보안 프로파일이 올바르게 작동 중인지 테스트하십시오.

다음에 수행할 작업

오브젝트 정의를 검토하고 새 대소문자 혼용 프로파일을 적절하게 작성하며, 필요에 따라 **REFRESH SECURITY** 를 사용하여 프로파일을 활성화하십시오.

IBM MQ MQI client 보안 설정

클라이언트 애플리케이션이 서버에서 자원에 대한 무제한 액세스를 갖지 않도록 IBM MQ MQI client 보안을 고려해야 합니다.

클라이언트 애플리케이션을 실행할 때 필요한 것보다 많은 액세스 권한을 가지고 있는 사용자 ID를 사용하여 애플리케이션을 실행하지 마십시오. 예를 들어, mqm 그룹의 사용자 또는 mqm 사용자 자체입니다.

너무 많은 액세스 권한을 가진 사용자로서 애플리케이션을 실행하면 애플리케이션이 실수로 또는 악의적으로 큐 관리자의 일부에 액세스하고 변경하는 위험이 있을 수 있습니다.

클라이언트 애플리케이션과 해당 큐 관리자 서버 간에는 인증 및 액세스 제어라는 두 가지 측면의 보안이 있습니다.

- 인증은 특정 사용자로서 실행 중인 클라이언트 애플리케이션이 본인이 주장하는 사용자가 맞는지를 확인하는 데 사용할 수 있습니다. 인증을 사용하면 공격자가 애플리케이션 중 하나를 위장하여 사용자의 큐 관리자에 대한 액세스를 얻는 것을 방지할 수 있습니다.

IBM MQ 8.0부터는 인증은 다음 두 옵션 중 하나에 의해 제공됩니다.

- 연결 인증 기능.

연결 인증에 대한 자세한 정보는 59 페이지의 『연결 인증』의 내용을 참조하십시오.

- TLS 내에서 상호 인증 사용.

TLS에 대한 자세한 정보는 244 페이지의 『SSL/TLS에 대한 작업』의 내용을 참조하십시오.

- 특정 사용자 또는 사용자 그룹의 액세스 권한을 제공하거나 제거하기 위해 액세스 제어를 사용할 수 있습니다. 특별히 작성된 사용자(또는 특정 그룹에 있는 사용자)로 클라이언트 애플리케이션을 실행하면 애플리케이션이 액세스할 수 없어야 하는 큐 관리자의 일부에 액세스할 수 없도록 하기 위해 액세스 제어를 사용할 수 있습니다.

액세스 제어를 설정할 때에는 채널 인증 규칙 및 채널의 MCAUSER 필드를 고려해야 합니다. 이러한 두 기능에는 모두 액세스 제어 권한을 확인하는 데 사용되는 사용자 ID를 변경하는 기능이 있습니다.

액세스 제어에 대한 자세한 정보는 312 페이지의 『오브젝트에 액세스 권한 부여』의 내용을 참조하십시오.

제한된 ID로 특정 채널에 액세스하기 위해 클라이언트 애플리케이션을 설정했지만 채널에는 해당 MCAUSER 필드에 설정된 관리자 ID가 있는 경우에는, 클라이언트 애플리케이션이 성공적으로 연결하는 경우 관리자 ID는 액

세스 제어 검사에 사용됩니다. 그러므로 클라이언트 애플리케이션은 큐 관리자에 대한 전체 액세스 권한을 가지고 있습니다.

MCAUSER 속성에 대한 자세한 정보는 [347 페이지의 『MCAUSER 사용자 ID에 클라이언트 사용자 ID 맵핑』](#)의 내용을 참조하십시오.

채널 인증 규칙은 승인될 연결을 위해 특정 규칙 및 기준을 설정하여 큐 관리자에 대한 액세스 제어를 위한 메소드로서 사용될 수도 있습니다.

채널 인증 규칙에 대한 자세한 정보는 [43 페이지의 『채널 인증 레코드』](#)의 내용을 참조하십시오.

MQI 클라이언트에서 런타임 시 FIPS 인증 CipherSpec만 사용하도록 지정

FIPS 준수 소프트웨어를 사용하여 키 저장소를 작성한 다음 채널이 FIPS-인증 CipherSpec을 사용해야 함을 지정하십시오.

런타임 시에 FIPS 준수를 위해서는 -fips 옵션과 함께 runmqakm 등과 같은 FIPS 준수 소프트웨어만을 사용하여 작성 및 관리되어야 합니다.

TLS 채널은 우선순위 순서로 나열된 세 가지 방법으로 FIPS-인증 CipherSpec만을 사용해야 함을 지정할 수 있습니다.

1. MQSCO 구조의 FipsRequired 필드를 MQSSL_FIPS_YES로 설정하십시오.
2. 환경 변수 MQSSLFIPS를 YES로 설정하십시오.
3. 클라이언트 구성 파일의 SSLFipsRequired 속성을 YES로 설정하십시오.

기본적으로 FIPS-인증 CipherSpec은 필요하지 않습니다.

이러한 값은 ALTER QMGR SSLFIPS(ALTER QMGR 참조)에서 동등한 매개변수 값과 동일한 의미가 있습니다. 현재 클라이언트 프로세스에 활성화된 TLS 연결이 없고, FipsRequired 값이 SSL MQCONN에 올바르게 지정된 경우에는 이 프로세스와 연관된 모든 후속 TLS 연결은 이 값과 연관된 CipherSpec만을 사용해야 합니다. 이는 이 연결 및 다른 모든 TLS 연결이 중지될 때까지 적용되며, 이 단계에서 후속 MQCONN가 FipsRequired에 새 값을 제공할 수 있습니다.

암호화 하드웨어가 존재하면 IBM MQ에 의해 사용되는 암호화 모듈은 하드웨어 제품이 제공하는 모듈로 구성될 수 있고, 이들은 특정 레벨로 FIPS-인증될 수도 있습니다. 구성 가능한 모듈 및 이들이 FIPS-인증인지 여부는 사용 중인 하드웨어 제품에 따라 다릅니다.

가능한 경우 FIPS-전용 CipherSpec이 구성되면 MQI 클라이언트는 MQRC_SSL_INITIALIZATION_ERROR와 함께 비FIPS CipherSpec을 지정하는 연결을 거부합니다. IBM MQ는 이러한 모든 연결을 거부한다고 보장하지 않으며 IBM MQ 구성이 FIPS 준수인지 판별하는 것은 사용자의 책임입니다.

관련 개념

[29 페이지의 『UNIX, Linux, and Windows용 FIPS\(Federal Information Processing Standard\)』](#)

Windows, UNIX and Linux 시스템에서 SSL/TLS 채널에 암호화가 필요한 경우, IBM MQ는 ICC(IBM Crypto for C)라고 하는 암호화 패키지를 사용합니다. Windows, UNIX and Linux 플랫폼에서 ICC 소프트웨어는 미국 국립 표준 기술원(US National Institute of Standards and Technology)의 FIPS(Federal Information Processing Standards) Cryptomodule Validation Program 레벨 140-2를 통과했습니다.

[클라이언트 구성 파일의 SSL 스탠자](#)

관련 참조

[FipsRequired\(MQLONG\)](#)

[MQSSLFIPS](#)

AIX

AIX에서 GSKit V8.0의 다중 설치에서 TLS 클라이언트 애플리케이션 실행

AIX의 TLS 클라이언트 애플리케이션이 다중 GSKit V8.0 설치가 있는 AIX 시스템에서 실행 중이면 MQRC_CHANNEL_CONFIG_ERROR 및 AMQ6175 오류가 발생할 수 있습니다.

다중 GSKit V8.0 설치가 있는 AIX 시스템에서 클라이언트 애플리케이션을 실행할 때 TLS를 사용하는 경우 클라이언트 연결 호출이 MQRC_CHANNEL_CONFIG_ERROR을(를) 리턴할 수 있습니다. /var/mqm/errors에서는 실패하는 클라이언트 애플리케이션의 AMQ6175 및 AMQ9220 레코드 오류를 로깅합니다. 예를 들어 다음과 같습니다.

```

09/08/11 11:16:13 - Process(24412.1) User(user) Program(example)
Host(machine.example.ibm.com) Installation(Installation1)
VRMF(7.1.0.0)
AMQ6175: The system could not dynamically load the shared library
'/usr/mqm/gskit8/lib64/libgsk8ssl_64.so'. The system returned
error number '8' and error message 'Symbol resolution failed
for /usr/mqm/gskit8/lib64/libgsk8ssl_64.so because:
Symbol VALUE_EC_NamedCurve_secp256r1__9GSKASN0ID (number 16) is not
exported from dependent module /db2data/db2inst1/sqllib/lib64/libgsk8cms_64.so.
Symbol VALUE_EC_NamedCurve_secp384r1__9GSKASN0ID (number 17) is not exported from
dependent module /db2data/db2inst1/sqllib/lib64/libgsk8cms_64.so.
Symbol VALUE_EC_NamedCurve_secp521r1__9GSKASN0ID (number 18) is not exported from
dependent module /db2data/db2inst1/sqllib/lib64/libgsk8cms_64.so.
Symbol VALUE_EC_ecPublicKey__9GSKASN0ID (number 19) is not exported from dependent
module /db2data/db2inst1/sqllib/lib64/libgsk8cms_64.so.
Symbol VALUE_EC_ecdsa_with_SHA1__9GSKASN0ID (number 20) is not exported from
dependent module /db2data/db2inst1/sqllib/lib64/libgsk8cms_64.so.
Symbol VALUE_EC_ecdsa__9GSKASN0ID (number 21) is not exported from dependent
module /db2data/db2inst1/sqllib/lib64/libgsk8cms_64.so.'

```

EXPLANATION:

This message applies to AIX systems. The shared library
 '/usr/mqm/gskit8/lib64/libgsk8ssl_64.so' failed
 to load correctly due to a problem with the library.

ACTION:

Check the file access permissions and that the file has not been corrupted.

```
----- amqxufnx.c : 1284 -----
```

```

09/08/11 11:16:13 - Process(24412.1) User(user) Program(example)
Host(machine.example.ibm.com) Installation(Installation1)
VRMF(7.1.0.0)
AMQ9220: The GSKit communications program could not be loaded.

```

EXPLANATION:

The attempt to load the GSKit library or procedure
 '/usr/mqm/gskit8/lib64/libgsk8ssl_64.so' failed with error code
 536895861.

ACTION:

Either the library must be installed on the system or the environment changed
 to allow the program to locate it.

```
----- amqcgkska.c : 836 -----
```

이 오류의 일반적인 원인은 LIBPATH 또는 LD_LIBRARY_PATH 환경 변수의 설정 때문에 IBM MQ 클라이언트가 다른 두 GSKit V8.0 설치에서 혼합된 라이브러리 세트를 로드하기 때문입니다. Db2 환경에서 IBM MQ 클라이언트 애플리케이션을 실행하면 이 오류가 발생할 수 있습니다.

이 오류를 피하려면 IBM MQ 라이브러리가 우선할 수 있도록 라이브러리 경로 앞에 IBM MQ 라이브러리 디렉토리를 포함하십시오. 이는 **setmqenv** 명령을 **-k** 매개변수와 함께 사용하여 달성할 수 있습니다. 예를 들어 다음과 같습니다.

```
. /usr/mqm/bin/setmqenv -s -k
```

setmqenv 명령의 사용에 대한 자세한 정보는 [setmqenv\(IBM MQ 환경 설정\)](#)를 참조하십시오.

IBM i IBM i에서 SSL 또는 TLS에 대한 통신 설정

SSL 또는 TLS 암호화 보안 프로토콜을 사용하는 보안 통신은 통신 채널 설정 및 인증하는 데 사용할 디지털 인증서 관리를 수반합니다.

SSL 또는 TLS 설치를 설정하려면 SSL 또는 TLS를 사용하도록 채널을 정의해야 합니다. 디지털 인증서도 작성하고 관리해야 합니다. 일부 운영 체제에서는 자체 서명 인증서로 테스트를 수행할 수 있습니다. 하지만 IBM i에서는 로컬 CA가 서명한 개인 인증서를 사용해야 합니다.

인증서 작성 및 관리에 대한 전체 정보는 244 페이지의 『IBM i에서 SSL/TLS에 대한 작업』의 내용을 참조하십시오.

이 주제 모음에서는 SSL 또는 TLS 통신 설정과 관련된 태스크 중 일부를 소개하고 이러한 태스크를 완료하는 것과 관련된 단계별 지침을 제공합니다.

SSL 및 TLS 프로토콜의 선택적 부분인 SSL 또는 TLS 클라이언트 인증도 테스트하려고 할 수 있습니다. SSL 또는 TLS 데이터 교환 동안에 SSL 또는 TLS 클라이언트는 항상 서버로부터 디지털 인증서를 확보하고 유효성 검증합니다. IBM MQ 구현을 사용하는 경우 SSL 또는 TLS 서버는 항상 클라이언트로부터 인증서를 요청합니다.

IBM i의 경우 SSL 또는 TLS 클라이언트는 올바른 IBM MQ 형식으로 레이블 지정된 인증서가 있는 경우에만 인증서를 전송합니다.

- 큐 관리자의 경우는 소문자로 변경된 큐 관리자 이름이 뒤따라오는 `ibmwebspheremq`입니다. 예를 들어, QM1의 경우 `ibmwebspheremqqm1`입니다.
- IBM i에 대한 IBM MQ C 클라이언트의 경우, 로그인 사용자 ID가 소문자로 변경되었습니다(`ibmwebspheremq` 예: `ibmwebspheremqmyuserid`).

IBM MQ는 레이블에 `ibmwebspheremq` 접두부를 사용하여 다른 제품에 대한 인증서와의 혼동을 피합니다. 전체 인증서 레이블을 소문자로 지정해야 합니다.

SSL 또는 TLS 서버는 항상 클라이언트 인증서를 유효성 검증합니다(전송된 경우). SSL 또는 TLS 클라이언트가 인증서를 전송하지 않으면 SSL 또는 TLS 서버 역할을 수행하는 채널의 끝이 SSLCAUTH 매개변수가 REQUIRED로 설정되거나 SSLPEER 매개변수 값이 설정된 상태로 정의된 경우에만 인증이 실패합니다. 자세한 정보는 [SSL 또는 TLS를 사용하여 두 개의 큐 관리자 연결을 참조하십시오](#).

ULW UNIX, Linux 또는 Windows에서 SSL 또는 TLS에 대한 통신 설정

SSL 또는 TLS 암호화 보안 프로토콜을 사용하는 보안 통신은 통신 채널 설정 및 인증하는 데 사용할 디지털 인증서 관리를 수반합니다.

SSL 또는 TLS 설치를 설정하려면 SSL 또는 TLS를 사용하도록 채널을 정의해야 합니다. 디지털 인증서도 작성하고 관리해야 합니다. UNIX, Linux 및 Windows 시스템의 경우 자체 서명 인증서로 테스트를 수행할 수 있습니다.



주의: TLS 지원 채널을 사용하여 함께 조인할 큐 관리자에서 Elliptic Curve 서명 인증서와 RSA 서명 인증서를 혼합해서 사용하는 것은 불가능합니다.

TLS 지원 채널을 사용하는 큐 관리자는 모두 RSA 서명 인증서를 사용하거나 모두 EC 서명 인증서를 사용해야 합니다. 이 둘을 혼합해서 사용할 수는 없습니다.

자세한 정보는 40 페이지의 『IBM MQ에서 디지털 인증서와 CipherSpec의 호환성』의 내용을 참조하십시오.

자체 서명 인증서는 폐기할 수 없으므로 개인 키가 손상된 후 공격자가 ID를 모방할 수 있습니다. CA는 손상된 인증서를 폐기할 수 있으며 폐기된 후에는 더 이상 사용할 수 없습니다. 따라서 CA 서명 인증서는 프로덕션 환경에서 사용하기에 더 안전하며 자체 서명 인증서는 테스트 시스템에서 더 편리합니다.

인증서 작성 및 관리에 대한 전체 정보는 255 페이지의 『UNIX, Linux, and Windows에서 SSL/TLS에 대한 작업』의 내용을 참조하십시오.

이 주제 모음에서는 SSL 통신 설정과 관련된 태스크 중 일부를 소개하고 이러한 태스크를 완료하는 것과 관련된 단계별 지침을 제공합니다.

프로토콜의 선택적 부분인 SSL 또는 TLS 클라이언트 인증도 테스트하려고 할 수 있습니다. SSL 또는 TLS 데이터 교환 동안에 SSL 또는 TLS 클라이언트는 항상 서버로부터 디지털 인증서를 확보하고 유효성 검증합니다. IBM MQ 구현을 사용하는 경우 SSL 또는 TLS 서버는 항상 클라이언트로부터 인증서를 요청합니다.

UNIX, Linux, and Windows의 경우 SSL 또는 TLS 클라이언트는 올바른 IBM MQ 형식으로 레이블 지정된 인증서가 있는 경우에만 인증서를 전송합니다.

- 큐 관리자의 경우 형식은 소문자로 변경된 큐 관리자 이름이 뒤따라오는 `ibmwebspheremq`입니다. 예를 들어, QM1의 경우 `ibmwebspheremqqm1`입니다.
- IBM MQ 클라이언트의 경우 소문자로 변경된 로그인 사용자 ID가 뒤따라오는 `ibmwebspheremq`입니다(예: `ibmwebspheremqmyuserid`).

IBM MQ는 레이블에 `ibmwebspheremq` 접두부를 사용하여 다른 제품에 대한 인증서와의 혼동을 피합니다. 전체 인증서 레이블을 소문자로 지정해야 합니다.

SSL 또는 TLS 서버는 항상 클라이언트 인증서를 유효성 검증합니다(전송된 경우). 클라이언트가 인증서를 전송하지 않으면 SSL 또는 TLS 서버 역할을 수행하는 채널의 끝이 SSLCAUTH 매개변수가 REQUIRED로 설정되거나

SSLPEER 매개변수 값이 설정된 상태로 정의된 경우에만 인증이 실패합니다. 자세한 정보는 [SSL 또는 TLS를 사용하여 두 개의 큐 관리자 연결을 참조하십시오](#).

z/OS z/OS에서 SSL 또는 TLS에 대한 통신 설정

SSL 또는 TLS 암호화 보안 프로토콜을 사용하는 보안 통신은 통신 채널 설정 및 인증하는 데 사용할 디지털 인증서 관리를 수반합니다.

SSL 또는 TLS 설치를 설정하려면 SSL 또는 TLS를 사용하도록 채널을 정의해야 합니다. 디지털 인증서도 작성하고 관리해야 합니다. z/OS의 경우 자체 서명 인증서를 사용하거나 로컬 인증 기관(CA)이 서명한 개인 인증서를 사용하여 테스트를 수행할 수 있습니다.

자체 서명 인증서는 폐기할 수 없으므로 개인 키가 손상된 후 공격자가 ID를 모방할 수 있습니다. CA는 손상된 인증서를 폐기할 수 있으며 폐기된 후에는 더 이상 사용할 수 없습니다. 따라서 CA 서명 인증서는 프로덕션 환경에서 사용하기에 더 안전하며 자체 서명 인증서는 테스트 시스템에서 더 편리합니다.

인증서 작성 및 관리에 대한 전체 정보는 [284 페이지의 『z/OS에서 SSL/TLS에 대한 작업』](#)의 내용을 참조하십시오.

이 주제 모음에서는 SSL 또는 TLS 통신 설정과 관련된 태스크 중 일부를 소개하고 이러한 태스크를 완료하는 것과 관련된 단계별 지침을 제공합니다.

프로토콜의 선택적 부분인 SSL 또는 TLS 클라이언트 인증도 테스트하려고 할 수 있습니다. SSL 또는 TLS 데이터 교환 동안에 SSL 또는 TLS 클라이언트는 항상 서버로부터 디지털 인증서를 확보하고 유효성 검증합니다. IBM MQ 구현을 사용하는 경우 SSL 또는 TLS 서버는 항상 클라이언트로부터 인증서를 요청합니다.

z/OS의 경우 SSL 또는 TLS 클라이언트는 다음 인증서 중 하나가 있는 경우에만 인증서를 전송합니다.

- 큐 공유 그룹 이름이 뒤따라오는 `ibmWebSphereMQ` 형식의 레이블을 가진 인증서(공유 채널 전용)(예: `ibmWebSphereMQQSG1`)
- 큐 관리자 이름이 뒤따라오는 `ibmWebSphereMQ` 형식의 레이블을 가진 인증서(예: `ibmWebSphereMQQM1`)
- 기본 인증서(`ibmWebSphereMQ` 인증서일 수 있음)

채널이 공유되는 경우 채널은 먼저 큐 공유 그룹에 대한 인증서를 찾으려고 시도합니다. 큐 공유 그룹에 대한 인증서를 찾지 못하는 경우에는 큐 관리자에 대한 인증서를 찾으려고 시도합니다.

z/OS의 경우 IBM MQ는 레이블에 `ibmWebSphereMQ` 접두부를 사용하여 다른 제품에 대한 인증서와의 혼동을 피합니다.

SSL 또는 TLS 서버는 항상 클라이언트 인증서를 유효성 검증합니다(전송된 경우). SSL 또는 TLS 클라이언트가 인증서를 전송하지 않으면 SSL 또는 TLS 서버 역할을 수행하는 채널의 끝이 `SSLCAUTH` 매개변수가 `REQUIRED`로 설정되거나 `SSLPEER` 매개변수 값이 설정된 상태로 정의된 경우에만 인증이 실패합니다. 자세한 정보는 [SSL 또는 TLS를 사용하여 두 개의 큐 관리자 연결을 참조하십시오](#).

SSL/TLS에 대한 작업

이 주제에서는 IBM MQ를 사용하여 TLS 사용과 관련된 단일 태스크를 수행하기 위한 지시사항을 제공합니다.

이들 대부분은 다음 절에 설명된 고급 수준 태스크에서 단계로서 사용됩니다.

- [295 페이지의 『사용자 식별 및 인증』](#)
- [312 페이지의 『오브젝트에 액세스 권한 부여』](#)
- [375 페이지의 『메시지의 기밀성』](#)
- [410 페이지의 『메시지의 데이터 무결성』](#)
- [410 페이지의 『클러스터 보안 유지』](#)

IBM i IBM i에서 SSL/TLS에 대한 작업

이 주제 콜렉션에서는 IBM MQ for IBM i에서 TLS(Transport Layer Security) 관련 작업을 수행하는 개별 태스크에 대한 지시사항을 제공합니다.

IBM i의 경우, TLS 지원은 운영 체제에 통합되어 있습니다. IBM i의 하드웨어 및 소프트웨어 요구사항에 나열된 필수조건을 설치했는지 확인하십시오.

IBM i에서 디지털 인증 관리자(DCM) 도구를 사용하여 키 및 디지털 인증을 관리합니다.

DCM 액세스

DCM 인터페이스에 액세스하려면 다음 지시사항을 따르십시오.

이 태스크 정보

프레임을 지원하는 웹 브라우저에서 다음 단계를 수행하십시오.

프로시저

1. `http:// machine.domain:2001` 또는 `https:// machine.domain:2010`으로 이동하십시오. 여기서 `machine`은 컴퓨터의 이름입니다.
2. 요청되면 올바른 사용자 프로파일 및 비밀번호를 입력하십시오.
사용자 프로파일에 새 인증서 저장소를 작성할 수 있는 *ALLOBJ 및 *SECADM 특수 권한이 있는지 확인하십시오. 특수 권한이 없는 경우에는 개인 인증서를 관리하거나 권한이 있는 오브젝트의 오브젝트 서명을 보기만 할 수 있습니다. 오브젝트 서명 애플리케이션을 사용할 권한이 있으면 DCM으로부터 오브젝트에 서명할 수도 있습니다.
3. 인터넷 구성 페이지에서 **디지털 인증 관리자**를 클릭하십시오.
디지털 인증 관리자 페이지가 표시됩니다.

IBM i에서 큐 관리자에 인증서 지정

큐 관리자에 인증서를 지정하려면 DCM을 사용하십시오.

인증서를 큐 관리자에 지정하려면 기존 IBM i 디지털 인증서 관리를 사용하십시오. 즉 큐 관리자가 시스템 인증서 저장소를 사용하고, 큐 관리자가 디지털 인증 관리자와 함께 애플리케이션으로서 사용하도록 등록되도록 지정할 수 있음을 의미합니다. 이를 수행하려면 큐 관리자 **SSLKEYR** 속성의 값을 *SYSTEM으로 변경하십시오.

SSLKEYR 매개변수가 *SYSTEM으로 변경되면 IBM MQ 는 큐 관리자를 QIBM_WEBSPPHERE_MQ_QMGRNAME의 고유한 응용프로그램 레이블과 Qmgrname (WMQ) 설명이 있는 레이블을 사용하여 서버 응용프로그램으로 등록합니다. *SYSTEM 인증서 저장소를 사용하는 경우에는 채널 **CERTLABL** 속성이 사용되지 않음을 유의하십시오. 그러면, 큐 관리자가 디지털 서명 관리자(DCM)의 서버 애플리케이션으로 표시되고 시스템 저장소에 있는 임의의 서버 또는 클라이언트 인증서를 이 애플리케이션에 지정할 수 있습니다.

큐 관리자는 애플리케이션으로 등록되므로 CA 신뢰 목록 정의 등과 같은 DCM의 고급 기능을 실행할 수 있습니다.

SSLKEYR 매개변수가 *SYSTEM이외의 값으로 변경되면 IBM MQ 는 큐 관리자를 디지털 Certificate Manager가 있는 어플리케이션으로 등록 해제합니다. 큐 관리자가 삭제되면 이는 또한 DCM에서 등록 취소됩니다. 충분한 *SECADM 권한이 있는 사용자는 또한 DCM에서 애플리케이션을 수동으로 추가하거나 제거할 수도 있습니다.

IBM i에서 키 저장소 설정

키 저장소는 연결의 양쪽 끝에 설정되어야 합니다. 기본 인증서 저장소를 사용하거나 새로 고유의 것을 새로 만들 수 있습니다.

TLS 연결의 경우 연결의 각 끝에 키 저장소가 있어야 합니다. 각 큐 관리자 및 IBM MQ MQI client에는 키 저장소에 대한 액세스가 있어야 합니다. 파일 이름 및 비밀번호를 사용하여(즉, *SYSTEM 옵션을 사용하지 않고) 키 저장소에 액세스하려면 QMQM 사용자 프로파일에 다음 권한이 있는지 확인하십시오.

- 키 저장소를 포함하는 디렉토리의 권한을 실행하십시오.
- 키 저장소를 포함하는 파일의 권한을 읽으십시오.

자세한 정보는 22 페이지의 『SSL/TLS 키 저장소』의 내용을 참조하십시오. *SYSTEM 인증서 저장소를 사용하는 경우에는 채널 **CERTLABL** 속성이 사용되지 않습니다.

IBM i에서, 디지털 인증서는 DCM으로 관리되는 인증서 저장소에 저장됩니다. 이러한 디지털 인증서에는 레이블이 있고, 이는 인증서를 큐 관리자 또는 IBM MQ MQI client와 연관시킵니다. TLS가 인증 목적으로 인증서를 사용합니다.

레이블은 설정된 경우, **CERTLABL** 속성의 값이거나, 큐 관리자의 이름이 있는 기본 **ibmwebspheremq** 또는 사용자 로그온 ID가 추가된 **IBM MQ MQI client**(모두 소문자)입니다. 자세한 내용은 [디지털 인증서 레이블을 참조](#) 하십시오.

큐 관리자 또는 **IBM MQ MQI client**인증서 저장소 이름은 경로 및 스템 이름으로 구성됩니다. 기본 경로는 **/QIBM/UserData/ICSS/Cert/Server/**이고 기본 스템 이름은 **Default**입니다. **IBM i**에서 기본 인증서 저장소 (**/QIBM/UserData/ICSS/Cert/Server/Default.kdb**)는 ***SYSTEM**라고도 합니다. 또는 사용자 고유의 경로와 스템 이름을 정의할 수도 있습니다.

사용자 고유의 경로나 파일 이름을 정의하는 경우에는 이에 대한 액세스를 엄격하게 제어하기 위해 파일에 권한을 설정하십시오.

[247 페이지의 『IBM i에서 큐 관리자의 키 저장소 위치 변경』](#)에서는 인증서 저장소 이름 지정에 대해서 알려줍니다. 인증서 저장소를 작성하기 전이나 후에 인증서 저장소 이름을 지정할 수 있습니다.

참고: DCM으로 수행할 수 있는 조작용 사용자 프로파일의 권한에 의해 제한될 수도 있습니다. 예를 들어, CA 인증서를 작성하려면 ***ALLOBJ** 및 ***SECADM** 권한이 필요합니다.

IBM i에서 인증서 저장소 작성

기본 인증서 저장소를 사용하지 않으려면 이 프로시저를 따라 사용자 고유의 것을 작성하십시오.

이 태스크 정보

IBM i 기본 인증서 저장소를 사용하지 않으려는 경우에만 새 인증서 저장소를 작성하십시오.

IBM i 시스템 인증서 저장소를 사용하도록 지정하려면 큐 관리자의 **SSLKEYR** 속성 값을 ***SYSTEM**으로 변경하십시오. 이 값은 큐 관리자가 시스템 인증서 저장소를 사용하고 큐 관리자가 디지털 인증 관리자(DCM)을 사용하여 애플리케이션으로서 사용하도록 등록되어 있음을 나타냅니다.

프로시저

1. [245 페이지의 『DCM 액세스』](#)에 설명된 대로 DCM 인터페이스에 액세스하십시오.
2. 탐색 패널에서 **새 인증서 저장소 작성**을 클릭하십시오.
새 인증서 저장소 작성 페이지가 태스크 프레임에 표시됩니다.
3. 태스크 프레임에서 **다른 시스템 인증서 저장소**를 선택하고 **계속**을 클릭하십시오.
새 인증서 저장소 페이지에 인증서 작성이 태스크 프레임에 표시됩니다.
4. **아니오 - 인증서 저장소에 인증서를 작성하지 않음**을 선택하고 **계속**을 클릭하십시오.
인증서 저장소 이름 및 비밀번호 페이지가 태스크 프레임에 표시됩니다.
5. **인증서 저장소 경로 및 파일 이름** 필드에 IFS 경로 및 파일 이름을 입력하십시오(예: **/QIBM/UserData/mqm/qmgrs/qm1/key.kdb**)
6. **비밀번호** 필드에 비밀번호를 입력하고 **비밀번호 확인** 필드에 다시 입력하십시오. **계속**을 클릭하십시오.
저장소 키를 감출 때 필요하므로 비밀번호(대소문자 구분)를 기록해 두십시오.
7. DCM을 종료하려면 브라우저 창을 닫으십시오.

다음에 수행할 작업

DCM을 사용하여 인증서 저장소를 작성한 경우에는 [246 페이지의 『IBM i 시스템에 인증서 저장소 비밀번호 숨기기』](#)에 설명된 대로 비밀번호를 숨기십시오.

관련 태스크

[251 페이지의 『IBM i에서 인증서를 키 저장소로 가져오기』](#)

인증서를 가져오려면 이 프로시저를 따르십시오.

IBM i 시스템에 인증서 저장소 비밀번호 숨기기

CL 명령을 사용하여 인증서 저장소 비밀번호를 숨기십시오.

다음 지시사항은 큐 관리자를 위해 **IBM i**에 인증서 저장소 비밀번호를 숨기는 데 적용됩니다. 또는 **IBM MQ MQI client**의 경우, ***SYSTEM** 인증 저장소 (즉, **MQSSLKEYR** 환경이 ***SYSTEM** 이외의 값으로 설정됨) 를 사용하지 않

는 경우, 253 페이지의 『IBM i용 IBM MQ SSL 클라이언트 유틸리티(amqrsslc)』의 254 페이지의 『인증서 저장소 비밀번호를 숨기십시오.』 섹션에 설명된 프로시저를 따르십시오.

*SYSTEM 인증서 저장소가 사용됨을 지정한 경우에는(큐 관리자의 SSLKEYR 속성을 *SYSTEM으로 변경하여) 다음 단계를 따르지 않아야 합니다.

DCM을 사용하여 인증서 저장소를 작성한 경우에는 다음 명령을 사용하여 비밀번호를 숨기십시오.

```
STRMQM MQMNAME('queue_manager_name')
CHGMQM MQMNAME('queue_manager_name') SSLKEYRPWD('password')
```

비밀번호는 대소문자를 구분합니다. 246 페이지의 『IBM i에서 인증서 저장소 작성』의 6단계에서 입력한 대로 정확하게 비밀번호를 작은따옴표 안에 입력해야 합니다.

참고: 기본 시스템 인증서 저장소를 사용 중이 아니고 비밀번호를 숨기지 않은 경우에는 인증서 저장소에 액세스하는 데 필요한 비밀번호를 확보할 수 없으므로 TLS 채널 시작에 실패합니다.

IBM i에서 키 저장소에서 큐 관리자 찾기

이 프로시저를 사용하여 큐 관리자의 인증서 저장소의 위치를 확보하십시오.

프로시저

1. 다음 명령을 사용하여 큐 관리자의 속성을 표시하십시오.

```
DSPMQM MQMNAME('queue manager name')
```

2. 인증서 저장소의 경로 및 스템 이름의 명령 출력을 검사하십시오.

예: /QIBM/UserData/ICSS/Cert/Server/Default. 여기서 /QIBM/UserData/ICSS/Cert/Server는 경로이고 Default는 스템 이름입니다.

IBM i에서 큐 관리자의 키 저장소 위치 변경

CHGMQM 또는 ALTER QMGR을 사용하여 큐 관리자의 인증서 저장소의 위치를 변경하십시오.

프로시저

CHGMQM 명령 또는 ALTER QMGR MQSC 명령을 사용하여 큐 관리자의 키 저장소 속성을 설정하십시오.

- a) CHGMQM 사용: CHGMQM MQMNAME('qm1') SSLKEYR('/QIBM/UserData/ICSS/Cert/Server/MyKey')
- b) ALTER QMGR 사용: ALTER QMGR SSLKEYR('/QIBM/UserData/ICSS/Cert/Server/MyKey')

두 경우 모두 인증서 저장소에는 완전한 파일 이름(/QIBM/UserData/ICSS/Cert/Server/MyKey.kdb)이 있습니다.

다음에 수행할 작업

큐 관리자의 인증서 저장소의 위치를 변경할 때 인증서는 이전 위치에서 전송되지 않습니다. 인증서 저장소를 작성할 때 사전 설치된 CA 인증서가 충분하지 않으면 251 페이지의 『IBM i에서 인증서를 키 저장소로 가져오기』에 설명된 대로 새 인증서 저장소에 인증서를 채워야 합니다. 또한 246 페이지의 『IBM i 시스템에 인증서 저장소 비밀번호 숨기기』에 설명된 대로 새 위치의 비밀번호를 숨겨야 합니다.

IBM i 테스트를 위한 인증 기관 및 인증서 작성

이 프로시저를 사용하여 인증서 요청을 서명하기 위해 로컬 CA 인증서를 작성하고 CA 인증서를 작성 및 설치하십시오.

시작하기 전에

이 주제의 지시사항은 로컬 인증 기관(CA)이 존재하지 않는다고 가정합니다. 로컬 CA가 존재하는 경우에는 248 페이지의 『IBM i에서 서버 인증서 요청』으로 이동하십시오.

이 태스크 정보

TLS를 설치할 때 제공된 CA 인증서는 CA를 발행하여 서명됩니다. IBM i에서는 시스템에서 TLS 통신을 테스트하기 위해 서버 인증서에 서명할 수 있는 로컬 인증 기관을 생성할 수 있습니다. 로컬 CA 인증서를 작성하려면 웹 브라우저에서 다음 단계를 따르십시오.

프로시저

1. 245 페이지의 『DCM 액세스』에 설명된 대로 DCM 인터페이스에 액세스하십시오.
2. 탐색 패널에서 **인증 기관 작성**을 클릭하십시오.
인증 기관 작성 페이지가 태스크 프레임에 표시됩니다.
3. **인증서 저장소 비밀번호** 필드에 비밀번호를 입력하고 **비밀번호 확인** 필드에 다시 입력하십시오.
4. **인증 기관(CA) 이름** 필드에 이름을 입력하십시오(예: TLS Test Certificate Authority).
5. **공통 이름 및 조직** 필드에 적합한 값을 입력하고 국가를 선택하십시오. 나머지 선택 필드에는 필요한 값을 입력하십시오.
6. **검증 기간** 필드에 로컬 CA의 검증 기간을 입력하십시오.
기본값은 1095일입니다.
7. **계속**을 클릭하십시오.
CA가 작성되고 DCM은 로컬 CA를 위해 인증서 저장소 및 CA 인증서를 작성합니다.
8. **인증서 설치**를 클릭하십시오.
다운로드 관리자 대화 상자가 표시됩니다.
9. CA 인증서를 저장하려는 임시 파일의 전체 경로 이름을 입력하고 **저장**을 클릭하십시오.
10. 다운로드가 완료되면 **열기**를 클릭하십시오.
인증서 창이 표시됩니다.
11. **인증서 설치**를 클릭하십시오.
인증서 가져오기 마법사가 표시됩니다.
12. **다음**을 클릭하십시오.
13. **인증서 유형을 기반으로 인증서 저장소 자동 선택**을 선택하고 **다음**을 클릭하십시오.
14. **마침**을 클릭하십시오.
확인 창이 표시됩니다.
15. **확인**을 클릭하십시오.
16. 인증서 창에서 **확인**을 클릭하십시오.
17. **계속**을 클릭하십시오.
인증 기관 정책 페이지가 태스크 프레임에 표시됩니다.
18. **사용자 인증서 작성 허용** 필드에서 **예**를 선택하십시오.
19. **검증 기간** 필드에 로컬 CA가 발행한 인증서의 검증 기간을 입력하십시오.
기본값은 365일입니다.
20. **계속**을 클릭하십시오.
새 인증서 저장소 페이지에 인증서 작성이 태스크 프레임에 표시됩니다.
21. 애플리케이션의 아무 것도 선택되지 않았는지 확인하십시오.
22. 로컬 CA 설정을 완료하려면 **계속**을 클릭하십시오.

IBM i에서 서버 인증서 요청

디지털 인증서는 위장으로부터 보호하고 공개 키가 지정된 엔티티에 속하는지 확인합니다. 새 서버 인증서는 디지털 인증 관리자(DCM)를 사용하여 인증 기관으로부터 요청될 수 있습니다.

이 태스크 정보

웹 브라우저에서 다음 단계를 수행하십시오.

프로시저

1. 245 페이지의 『DCM 액세스』에 설명된 대로 DCM 인터페이스에 액세스하십시오.
2. 탐색 패널에서 **인증서 저장소 선택**을 클릭하십시오.
인증서 저장소 선택 페이지가 태스크 프레임에 표시됩니다.
3. 사용하려는 인증서 저장소를 선택하고 **계속**을 클릭하십시오.
4. 옵션: 3단계에서 ***SYSTEM**을 선택한 경우에는 시스템 저장소 비밀번호를 입력하고 **계속**을 클릭하십시오.
5. 옵션: 3단계에서 **다른 시스템 인증서 저장소**를 선택한 경우에는 **인증서 저장소 경로 및 파일 이름** 필드에 인증서 저장소를 작성할 때 설정한 IFS 경로 및 파일 이름을 입력하십시오. 또한 **인증서 저장소 비밀번호** 필드에 비밀번호를 입력하십시오. 그런 다음 **계속**을 클릭하십시오.
6. 탐색 패널에서 **인증서 작성**을 클릭하십시오.
7. 태스크 프레임에서 **서버 또는 클라이언트 인증서** 단일 선택 단추를 선택하고 **계속**을 클릭하십시오.
인증 기관(CA) 선택 페이지가 태스크 프레임에 표시됩니다.
8. 워크스테이션에 로컬 CA가 있는 경우 로컬 CA 또는 상업 CA를 선택하여 인증서에 서명하십시오. 원하는 CA의 단일 선택 단추를 선택하고 **계속**을 클릭하십시오.
인증서 작성 페이지가 태스크 프레임에 표시됩니다.
9. 옵션: 큐 관리자의 경우 **인증서 레이블** 필드에 인증서 레이블을 입력하십시오.
레이블은 설정된 경우 **CERTLABL** 속성의 값이거나 큐 관리자의 이름이 추가된 **ibmwebspheremq**(모두 소문자)입니다. 자세한 내용은 [디지털 인증서 레이블](#)을 참조하십시오.
예를 들어, 큐 관리자 QM1의 경우 기본값을 사용하려면 **ibmwebspheremqmqm1**을 입력하십시오.
10. 옵션: IBM MQ MQI client의 경우 **인증서 레이블** 필드에 소문자로 접힌 로그인 사용자 ID가 뒤따르는 **ibmwebspheremq**를 입력하십시오.
예를 들어 **ibmwebspheremqmyuserid**를 입력하십시오.
11. **공통 이름** 및 **조직** 필드에 적합한 값을 입력하고 국가를 선택하십시오. 나머지 선택 필드에는 필요한 값을 입력하십시오.

결과

인증서에 서명하기 위해 상업용 CA를 선택한 경우에는 DCM은 인증서 요청을 PEM(Privacy-Enhanced Mail) 형식으로 작성합니다. 요청을 선택한 CA로 전달하십시오.

인증서에 서명하기 위해 로컬 CA를 선택한 경우에는 DCM은 인증서가 인증서 저장소에 작성되었고 사용할 수 있음을 사용자에게 알립니다.

IBM i에서 IBM 키 관리자에 대한 서버 인증서 요청

로컬 인증 기관(CA)이 서명한 인증서를 작성하거나 IBM 키 관리자(iKeyman) 유틸리티로 가져오기 위해 상업용 CA가 서명한 서버 인증서를 신청하려면 이 프로시저를 따르십시오.

이 태스크 정보

사용자 인증서는 디지털 인증 관리자(DCM)가 다중 플랫폼에서 IBM MQ을 위한 인증서 관리자의 역할을 할 때 사용되어야 합니다. 다른 플랫폼으로 분배된 개인 인증서 또는 iKeyman 유틸리티로의 가져오기를 위해 웹 브라우저에서 다음 단계를 수행하십시오.

프로시저

1. 245 페이지의 『DCM 액세스』에 설명된 대로 DCM 인터페이스에 액세스하십시오.
2. 탐색 분할창에서 **인증서 작성**을 클릭하십시오.
인증서 작성 페이지가 태스크 프레임에 표시됩니다.
3. **인증서 작성** 패널에서 **사용자 인증서** 단일 선택 단추를 선택하고 **계속**을 클릭하십시오.
사용자 인증서 작성 페이지가 표시됩니다.
4. **사용자 인증서 작성** 패널에서 **조직 이름**, **시/도** 또는 **구/군/시**, **국가** 또는 **지역**의 인증서 정보 아래에서 필수 필드를 완료하십시오. 또는 **조직 단위** 및 **로컬성** 또는 **구/군/시** 필드에 값을 입력하십시오. **계속**을 클릭하십시오.

- 공통 이름은 iSeries 시스템에 로그인할 때 사용하는 사용자 ID로 자동으로 설정됩니다.
5. 다음 사용자 인증서 작성 패널에서 인증서 설치를 클릭하고 계속을 클릭하십시오.
개인 인증서가 설치되었습니다. 이 인증서의 백업 사본을 보관해야 합니다.
 6. 확인을 클릭하십시오.
 7. DCM에 액세스하는 데 사용한 인터넷 브라우저에 따라서 다음 단계를 수행하십시오.
 - a) Microsoft Edge의 경우 도구> 인터넷 옵션> 콘텐츠 탭> 인증서 단추> 개인 탭을 선택하십시오. 인증서를 선택하고 내보내기를 클릭하십시오.
 - b) Mozilla Firefox의 경우 도구> 옵션> 고급> 암호화 탭> 인증서 보기 단추> 사용자 인증서 탭을 선택하십시오. 인증서를 선택하고 백업을 클릭하십시오. 경로 및 파일 이름을 선택하고 확인을 클릭하십시오.
 8. FTP를 사용하여 내보낸 인증서를 2진 형식으로 원격 시스템으로 전송하십시오.
 9. 7단계에서 내보낸 인증서를 키 데이터베이스에서 iKeyman 유틸리티에 추가하십시오.
 - a) 인증서가 Microsoft Edge를 사용하여 저장된 경우에는 Microsoft .pfx에서 가져오기 파일에 설명된 지시사항을 사용하십시오.
 - b) 인증서가 Mozilla Firefox를 사용하여 저장된 경우에는 개인 인증서를 키 저장소로 가져오기에 설명된 지시사항을 사용하십시오.

가져오기 동안에 개인 인증서 및 서명자 인증서의 레이블 이름이 IBM MQ이 예상하는 것으로 변경되었는지 확인하십시오. 레이블은 설정된 경우 IBM MQ CERTLABL 속성의 값이거나 큐 관리자의 이름이 추가된 ibmwebspheremq(모두 소문자)여야 합니다. 자세한 내용은 디지털 인증서 레이블을 참조하십시오.

IBM i에서 키 저장소에 서버 인증서 추가

요청된 인증서를 키 저장소에 추가하려면 이 프로시저를 따르십시오.

이 태스크 정보

CA가 새 서버 인증서를 송신한 후에는 이를 사용자가 요청을 생성한 인증서 저장소에 추가할 수 있습니다. CA가 이메일 메시지의 일부로서 인증서를 송신하면 인증서를 별도의 파일로 복사하십시오.

참고:

- 서버 인증서가 로컬 CA에 의해 서명된 경우에는 이 프로시저를 수행할 필요가 없습니다.
- 서버 인증서를 PKCS #12 형식으로 DCM에 가져오기 전에 먼저 해당하는 CA 인증서를 가져와야 합니다.

서버 인증서를 큐 관리자 인증서 저장소에서 수신하려면 다음 프로시저를 사용하십시오.

프로시저

1. 245 페이지의 『DCM 액세스』에 설명된 대로 DCM 인터페이스에 액세스하십시오.
2. 탐색 패널의 인증서 관리 태스크 범주에서 인증서 가져오기를 클릭하십시오.
인증서 가져오기 페이지가 태스크 프레임에 표시됩니다.
3. 인증서 유형에 맞는 단일 선택 단추를 선택하고 계속을 클릭하십시오.
서버 또는 클라이언트 인증서 가져오기 페이지 또는 인증 기관(CA) 인증서 가져오기 페이지가 태스크 프레임에 표시됩니다.
4. 파일 가져오기 필드에 가져오려는 인증서의 파일 이름을 입력하고 계속을 클릭하십시오.
DCM은 자동으로 파일의 형식을 판별합니다.
5. 인증서가 서버 또는 클라이언트 인증서이면 태스크 프레임에 비밀번호를 입력하고 계속을 클릭하십시오.
DCM은 인증서가 가져오기되었음을 알려줍니다.

IBM i에서 키 저장소로부터 인증서 내보내기

인증서를 내보내면 공개 키와 개인 키가 모두 내보내집니다. 개인 키가 누출되면 보안이 심각하게 위협받으므로 이 조치는 각별히 주의하여 실행해야 합니다.

시작하기 전에

사용자의 인증서를 다른 사용자와 공유할 때 공개 키를 교환합니다. 이 프로세스는 **태스크 5. UNIX의 AMS에 대한 빠른 시작 안내서의 인증서 공유하기**. 여기에 설명된 것과 같이 인증서를 내보내면 개인 키와 공개 키가 모두 내보내집니다. 개인 키가 누출되면 보안이 심각하게 위협받으므로 이 조치는 각별히 주의하여 실행해야 합니다.

이 태스크 정보

인증서를 내보내려는 컴퓨터에서 다음 단계를 수행하십시오.

프로시저

1. 245 페이지의 『DCM 액세스』에 설명된 대로 DCM 인터페이스에 액세스하십시오.
2. 탐색 패널에서 **인증서 저장소 선택**을 클릭하십시오.
인증서 저장소 선택 페이지가 태스크 프레임에 표시됩니다.
3. 사용하려는 인증서 저장소를 선택하고 **계속**을 클릭하십시오.
4. 옵션: 3단계에서 ***SYSTEM**을 선택한 경우에는 시스템 저장소 비밀번호를 입력하고 **계속**을 클릭하십시오.
5. 옵션: 3단계에서 **다른 시스템 인증서 저장소**를 선택한 경우에는 **인증서 저장소 경로 및 파일 이름** 필드에 인증서 저장소를 작성할 때 설정한 IFS 경로 및 파일 이름을 입력하고 **인증서 저장소 비밀번호** 필드에 비밀번호를 입력하십시오. 그런 다음 **계속**을 클릭하십시오.
6. 탐색 패널의 **인증서 관리** 태스크 범주에서 **인증서 내보내기**를 클릭하십시오.
인증서 내보내기 페이지가 태스크 프레임에 표시됩니다.
7. 인증서 유형에 맞는 단일 선택 단추를 선택하고 **계속**을 클릭하십시오.
서버 또는 클라이언트 인증서 내보내기 페이지 또는 인증 기관(CA) 인증서 내보내기 페이지가 태스크 프레임에 표시됩니다.
8. 내보내려는 인증서를 선택하십시오.
9. 인증서를 파일에 또는 다른 인증서 저장소에 직접 내보내려는지 여부를 지정하려면 단일 선택 단추를 선택하십시오.
10. 서버나 클라이언트 인증서를 파일에 내보내기로 선택한 경우에는 다음 정보를 제공하십시오.
 - 내보낸 인증서를 저장하려는 위치의 경로 및 파일 이름.
 - 개인 인증서의 경우 내보낸 인증서 및 대상 릴리스를 암호화하는 데 사용되는 비밀번호. CA 인증서의 경우 비밀번호를 지정할 필요가 없습니다.
11. 인증서를 다른 인증서 저장소로 직접 내보내기로 선택한 경우에는 대상 인증서 저장소 및 해당 비밀번호를 지정하십시오.
12. **계속**을 클릭하십시오.

IBM i에서 인증서를 키 저장소로 가져오기

인증서를 가져오려면 이 프로시저를 따르십시오.

시작하기 전에

PKCS #12 형식으로 개인 인증서를 DCM으로 가져오기 전에 먼저 해당하는 CA 인증서를 가져와야 합니다.

이 태스크 정보

인증서를 가져오려는 시스템에서 다음 단계를 수행하십시오.

프로시저

1. 245 페이지의 『DCM 액세스』에 설명된 대로 DCM 인터페이스에 액세스하십시오.
2. 탐색 패널에서 **인증서 저장소 선택**을 클릭하십시오.
인증서 저장소 선택 페이지가 태스크 프레임에 표시됩니다.
3. 사용하려는 인증서 저장소를 선택하고 **계속**을 클릭하십시오.

4. 옵션: 3단계에서 ***SYSTEM**을 선택한 경우에는 시스템 저장소 비밀번호를 입력하고 **계속**을 클릭하십시오.
5. 옵션: 3단계에서 **다른 시스템 인증서 저장소**를 선택한 경우에는 **인증서 저장소 경로 및 파일 이름** 필드에 인증서 저장소를 작성할 때 설정한 IFS 경로 및 파일 이름을 입력하고 **인증서 저장소 비밀번호** 필드에 비밀번호를 입력하십시오. 그런 다음 **계속**을 클릭하십시오.
6. 탐색 패널의 **인증서 관리** 태스크 범주에서 **인증서 가져오기**를 클릭하십시오.
인증서 가져오기 페이지가 태스크 프레임에 표시됩니다.
7. 인증서 유형에 맞는 단일 선택 단추를 선택하고 **계속**을 클릭하십시오.
서버 또는 클라이언트 인증서 가져오기 페이지 또는 인증 기관(CA) 인증서 가져오기 페이지가 태스크 프레임에 표시됩니다.
8. **파일 가져오기** 필드에 가져오려는 인증서의 파일 이름을 입력하고 **계속**을 클릭하십시오.
DCM은 자동으로 파일의 형식을 판별합니다.
9. 인증서가 **서버 또는 클라이언트** 인증서이면 태스크 프레임에 비밀번호를 입력하고 **계속**을 클릭하십시오.
DCM은 인증서가 가져오기되었음을 알려줍니다.

IBM i에서 인증서 제거

개인 인증서를 제거하려면 이 프로시저를 사용하십시오.

프로시저

1. 245 페이지의 『DCM 액세스』에 설명된 대로 DCM 인터페이스에 액세스하십시오.
2. 탐색 패널에서 **인증서 저장소 선택**을 클릭하십시오.
인증서 저장소 선택 페이지가 태스크 프레임에 표시됩니다.
3. **다른 시스템 인증서 저장소** 선택란을 선택한 후 **계속**을 클릭하십시오.
인증서 저장소 및 비밀번호 페이지가 표시됩니다.
4. **인증서 저장소 경로 및 파일 이름** 필드에 인증서 저장소를 작성할 때 설정한 IFS 경로 및 파일 이름을 입력하십시오.
5. **인증서 저장소 비밀번호** 필드에 비밀번호를 입력하십시오. **계속**을 클릭하십시오.
현재 인증서 저장소 페이지가 태스크 프레임에 표시됩니다.
6. 탐색 패널의 **인증서 관리** 태스크 범주에서 **인증서 삭제**를 클릭하십시오.
인증서 삭제 확인 페이지가 태스크 프레임에 표시됩니다.
7. 삭제하려는 인증서를 선택하십시오. **삭제**를 클릭하십시오.
8. 인증서를 삭제하고 싶음을 확인하려면 **예**를 클릭하십시오. 그렇지 않으면 **아니오**를 클릭하십시오.
DCM은 인증서가 삭제되었음을 알립니다.

IBM i에서 단방향 인증을 위해 *SYSTEM 인증 저장소 사용

단방향 인증을 설정하려면 이러한 지시사항을 따르십시오.

시작하기 전에

- 큐 관리자, 채널 및 전송 큐를 작성하십시오.
- 서버 큐 관리자에서 서버 또는 클라이언트 인증서를 작성하십시오.
- CA 인증서를 클라이언트 큐 관리자로 전송하고 키 저장소로 가져오기했습니다.
- 서버 및 클라이언트 큐 관리자에서 리스너를 시작하십시오.

이 태스크 정보

TLS 서버로 IBM i를 실행 중인 컴퓨터를 사용하여 단방향 인증을 사용하려면 SSL키 저장소 (SSLKEYR) 매개변수를 *SYSTEM으로 설정하십시오. 이 설정은 IBM MQ 큐 관리자를 애플리케이션으로서 등록합니다. 그런 다음 단방향 인증을 사용으로 설정하기 위해 큐 관리자에 인증서를 지정할 수 있습니다.

개인 키 저장소를 사용하여 키 저장소에 클라이언트 큐 관리자를 위한 더미 인증서를 작성하여 단방향 인증을 구현할 수도 있습니다.

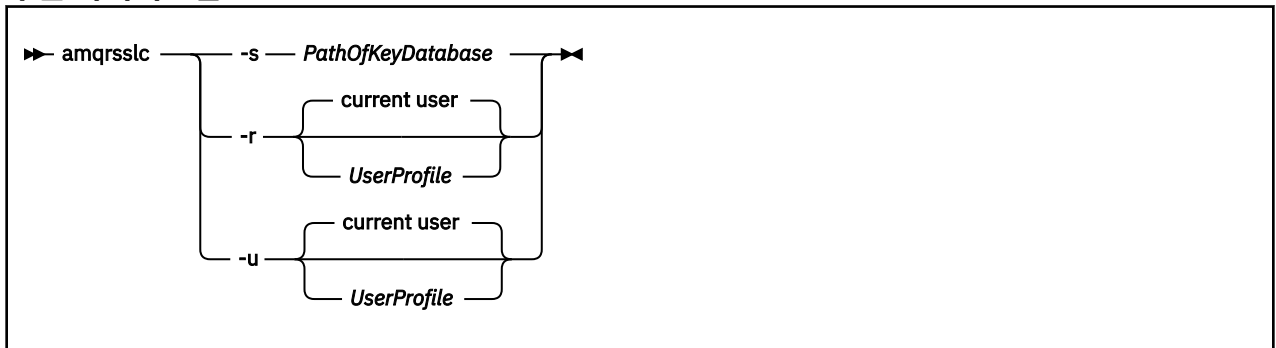
프로시저

1. 서버 및 클라이언트 큐 관리자에서 다음 단계를 수행하십시오.
 - a) CHGMQM MQMNAME(SSL) SSLKEYR(*SYSTEM) 명령을 실행하여 SSLKEYR 매개변수를 설정하려면 큐 관리자를 변경하십시오.
 - b) CHGMQM MQMNAME(SSL) SSLKEYRPWD('xxxxxxx') 명령을 실행하여 기본 키 저장소의 비밀번호를 숨기십시오.
비밀번호는 작은따옴표에 있어야 합니다.
 - c) SSLCIPHER 매개변수에서 올바른 CipherSpec을 가지도록 채널을 변경하십시오.
 - d) RFRMQMAUT QMNAME(QMGRNAME) TYPE(*SSL) 명령을 실행하여 TLS 보안을 새로 고치십시오.
2. 다음과 같이 DCM을 사용하여 서버 큐 관리자에 인증서를 지정하십시오.
 - a) 245 페이지의 『DCM 액세스』에 설명된 대로 DCM 인터페이스에 액세스하십시오.
 - b) 탐색 패널에서 **인증서 저장소 선택**을 클릭하십시오.
인증서 저장소 선택 페이지가 태스크 프레임에 표시됩니다.
 - c) *SYSTEM 인증서 저장소를 선택하고 **계속**을 클릭하십시오.
 - d) 왼쪽 패널에서 **애플리케이션 관리**를 펼치십시오.
 - e) 큐 관리자가 애플리케이션으로 등록되었는지 확인하려면 **애플리케이션 보기** 정의를 선택하십시오.
SSL(WMQ)이 테이블에 나열됩니다.
 - f) **인증서 지정 업데이트**를 선택하십시오.
 - g) **서버**를 선택하고 **계속**을 클릭하십시오.
 - h) QMGRNAME(WMQ)을 선택하고 **인증서 지정 업데이트**를 클릭하십시오.
 - i) 인증서를 선택하고 **새 인증서 지정**을 클릭하십시오. 인증서가 애플리케이션에 지정되었음을 알리는 창이 열립니다.

IBM i용 IBM MQ SSL 클라이언트 유틸리티(amqrsslc)

IBM i의 IBM MQ SSL 클라이언트 유틸리티 (amqrsslc)는 IBM i 시스템의 IBM MQ MQI client에서 클라이언트 사용자 프로파일을 등록 또는 등록 취소하거나 인증서 저장소 비밀번호를 숨기는 데 사용됩니다. 유틸리티는 *ALLOBJ 특수 권한이 있는 프로파일이 있는 사용자 또는 디지털 인증 관리자(DCM)에서 애플리케이션 등록을 작성하거나 삭제할 옵션이 있는 QMQMADM의 구성원에 의해서만 실행될 수 있습니다.

구문 다이어그램



클라이언트 사용자 프로파일 등록

IBM MQ MQI client가 *SYSTEM 인증 저장소를 사용하는 경우, 디지털 Certificate Manager (DCM)를 사용하여 애플리케이션으로 사용할 클라이언트 사용자 프로파일 (로그온 사용자)을 등록해야 합니다.

클라이언트 사용자 프로파일을 등록하려면 *UserProfile*을 사용하여 -r 옵션과 함께 **amqrsslc** 프로그램을 실행하십시오. **amqrsslc**를 호출할 때 사용되는 사용자 프로파일에는 *USE 권한이 있어야 합니다. -r 옵션을 사용하여 *UserProfile*을 제공하면 *UserProfile*을 QIBM_WEBSPPHERE_MQ_UserProfile의 고유 애플리케이션 레이블과 *UserProfile* (WMQ)에 대한 설명이 있는 레이블이 있는 서버 애플리케이션으로 등록합니다. 그런 다음 이

서버 애플리케이션은 DCM에 표시되고 시스템 저장소에 있는 모든 서버나 클라이언트 인증서를 이 애플리케이션에 지정할 수 있습니다.

참고: 사용자 프로파일이 `-r` 옵션으로 지정되지 않은 경우에는 **amqrrssl** 도구를 실행 중인 사용자의 사용자 프로파일이 등록됩니다.

다음 코드는 **amqrrssl**를 사용하여 사용자 프로파일을 등록합니다. 첫 번째 예에서 지정된 사용자 프로파일이 등록됩니다. 두 번째에서는 이는 로그인한 사용자의 프로파일입니다.

```
CALL PGM(QMQM/AMQRSSLC) PARM('-r' UserProfile)
CALL PGM(QMQM/AMQRSSLC) PARM('-r')
```

클라이언트 사용자 프로파일 등록 취소

클라이언트 프로파일을 등록 취소하려면 *UserProfile* 프로파일을 `-u` 옵션과 함께 사용하여 **amqrrssl** 프로그램을 실행하십시오. **amqrrssl**를 호출할 때 사용되는 사용자 프로파일에는 *USE 권한이 있어야 합니다.

Providing the *UserProfile* with the `-u` option unregisters *UserProfile* with label QIBM_WEBSPPHERE_MQ_*UserProfile* from the DCM.

참고: 사용자 프로파일이 `-u` 옵션으로 지정되지 않은 경우에는 **amqrrssl** 도구를 실행 중인 사용자의 사용자 프로파일이 등록됩니다.

다음 코드는 **amqrrssl**를 사용하여 사용자 프로파일을 등록 취소합니다. 첫 번째 예에서 지정된 사용자 프로파일이 등록 취소됩니다. 두 번째에서는 이는 로그인한 사용자의 프로파일입니다.

```
CALL PGM(QMQM/AMQRSSLC) PARM('-u' UserProfile)
CALL PGM(QMQM/AMQRSSLC) PARM('-u')
```

인증서 저장소 비밀번호를 숨기십시오.

IBM MQ MQI client 가 *SYSTEM 인증 저장소를 사용하지 않고 다른 인증서 저장소 (즉, MQSSLKEYR은 *SYSTEM 이외의 값으로 설정됨) 를 사용하지 않는 경우, 키 데이터베이스의 비밀번호가 숨겨져야 합니다. 키 데이터베이스의 비밀번호를 숨기기 위해 `-s` 옵션을 사용하십시오.

다음 코드에서 인증서 저장소의 완전한 파일 이름은 `/Path/Of/KeyDatabase/MyKey.kdb`입니다.

```
CALL PGM(QMQM/AMQRSSLC) PARM('-s' '/Path/Of/KeyDatabase/MyKey')
```

이 코드를 실행하면 이 키 데이터베이스의 비밀번호가 요청됩니다. 이 비밀번호는 `.sth` 확장자를 사용하여 키 데이터베이스와 같은 이름의 파일에 숨겨집니다. 이 파일은 키 데이터베이스와 같은 경로에 저장됩니다. 이 코드 예에서는 스테쉬 파일 `/Path/Of/KeyDatabase/MyKey.sth`를 생성합니다. QMQM은 사용자 소유자이고 QMQMADM은 이 파일의 그룹 소유자입니다. QMQM 및 QMQMADM에는 읽기, 쓰기 권한이 있고 다른 프로파일에는 읽기 권한만 있습니다.

인증서 또는 인증서 저장소의 변경사항이 IBM i에서 적용되는 시기

인증서 저장소에서 인증서 또는 인증서 저장소의 위치를 변경할 때 변경사항은 채널 유형 및 채널이 실행 중인 방법에 따라 적용됩니다.

인증서 저장소의 인증서 및 키 저장소 속성의 변경사항은 다음 상황에서 적용됩니다.

- 새 아웃바운드 단일 프로세스가 처음으로 TLS 채널을 실행할 때.
- 새 인바운드 TCP/IP 단일 채널 프로세스가 처음으로 TLS 채널을 시작하라는 요청을 수신할 때.
- MQSC 명령 REFRESH SECURITY TYPE(SSL)이 IBM MQ TLS 환경을 새로 고치기 위해 실행될 때.
- 클라이언트 애플리케이션 프로세스의 경우, 프로세스에서 마지막 TLS 연결이 닫힐 때. 다음 TLS 연결에는 인증서 변경사항이 적용됩니다.
- 프로세스 풀링 프로세스(amqrmppa)의 스레드로서 실행되는 채널의 경우 프로세스 풀링 프로세스가 시작되거나 재시작되고 TLS 채널을 처음 시작할 때. 프로세스 풀링 프로세스가 이미 TLS 채널을 실행했고 변경사항을 즉시 적용하고 싶은 경우, MQSC 명령 REFRESH SECURITY TYPE(SSL)을 실행하십시오.

- 채널 시작기의 스레드로서 실행되는 채널의 경우 채널 시작기가 시작되거나 재시작되고 TLS 채널을 처음 실행할 때, 채널 시작기 프로세스가 이미 TLS 채널을 실행했고 변경사항을 즉시 적용하고 싶은 경우에는 MQSC 명령 REFRESH SECURITY TYPE(SSL)을 실행하십시오.
- TCP/IP 리스너의 스레드로서 실행되는 채널의 경우 리스너가 시작되거나 재시작되고 TLS 채널을 시작하라는 요청을 처음으로 수신할 때, 리스너가 이미 TLS 채널을 실행했고 변경사항을 즉시 적용하고 싶으면 MQSC 명령 REFRESH SECURITY TYPE(SSL)을 실행하십시오.

IBM i에서 암호화 하드웨어 구성

이 프로시저를 사용하여 IBM i에서 암호화 코프로세서를 구성하십시오.

시작하기 전에

사용자 프로파일에 코프로세서 하드웨어를 구성할 수 있게 해주는 *ALLOBJ 및 *SECADM 특수 권한이 있는지 확인하십시오.

프로시저

1. `http://machine.domain:2001` 또는 `https://machine.domain:2010`로 이동하십시오. 여기서 *machine* 은 컴퓨터의 이름입니다.
사용자 이름 및 비밀번호를 요청하는 대화 상자가 표시됩니다.
2. 올바른 IBM i 사용자 프로파일 및 비밀번호를 입력하십시오.
3. 자세한 정보를 보려면 [암호화](#)로 이동하여 해당 링크를 클릭하십시오.

다음에 수행할 작업

4767 암호화 코프로세서 구성에 대한 자세한 정보는 [4767 암호화 코프로세서를 참조](#)하십시오.

UNIX, Linux, and Windows에서 SSL/TLS에 대한 작업


UNIX, Linux, and Windows 시스템에서 TLS(Transport Layer Security) 지원이 IBM MQ와 함께 설치됩니다.

인증서 유효성 검증 정책에 대한 보다 자세한 정보는 [인증서 유효성 검증 및 신뢰 정책 설계의 내용](#)을 참조하십시오.

`runmqckm`, `runmqakm` 및 `strmqikm`을 사용하여 디지털 인증서 관리

UNIX, Linux, and Windows 시스템에서 `strmqikm`(iKeyman) GUI를 사용하거나 `runmqckm`(iKeycmd) 또는 `runmqakm`(GSKCapiCmd)을 사용하여 키 및 디지털 인증서를 관리하십시오.

V 9.1.0

 **주의:** `runmqckm` 명령과 `strmqikm` 명령은 모두 IBM MQ JRE(Java Runtime Environment)에 의존합니다. IBM MQ 9.1부터는, JRE가 설치되지 않은 경우 AMQ9183 메시지가 수신됩니다.

• UNIX and Linux 시스템의 경우:

- `strmqikm`(iKeyman) 명령을 사용하여 iKeyman GUI를 시작하십시오.
- `runmqckm`(iKeycmd) 명령을 사용하여 iKeycmd 명령행 인터페이스로 태스크를 수행하십시오.
- `runmqakm`(GSKCapiCmd) 명령을 사용하여 `runmqakm` 명령행 인터페이스로 태스크를 수행하십시오.
`runmqakm`의 명령 구문은 `runmqckm`의 구문과 같습니다.

FIPS를 준수하는 방법으로 TLS 인증서를 관리해야 하는 경우, `runmqckm` 또는 `strmqikm` 명령 대신에 `runmqakm` 명령을 사용하십시오.

`runmqckm` 및 `runmqakm` 명령에 대한 명령행 인터페이스의 전체 설명은 [키 및 인터페이스 관리](#)를 참조하십시오.

PKCS #11 암호화 하드웨어에 저장된 인증서 또는 키를 사용 중인 경우 iKeycmd 및 iKeyman은 64비트 프로그램입니다. PKCS #11 지원에 필요한 외부 모듈이 64비트 프로세스에 로드되므로 암호화 하드웨어 관리를 위

해서는 64비트 PKCS #11 라이브러리를 설치해야 합니다. iKeyman 및 iKeycmd 프로그램이 이러한 플랫폼에서 32비트이므로 Windows 및 Linux x86 32비트 플랫폼은 유일한 예외입니다.

자세한 정보는 [GSKit: PKCS#11 및 IBM MQ JRE 주소 지정 모드를 참조하십시오](#).

strmqikm 명령을 실행하여 iKeyman GUI를 시작하기 전에 X Window 시스템을 실행할 수 있는 시스템에서 작업 중인지와 다음을 수행하는지를 확인하십시오.

- DISPLAY 환경 변수를 다음과 같이 설정하십시오.

```
export DISPLAY=mypc:0
```

- PATH 환경 변수에 **/usr/bin** 및 **/bin**이 포함되어 있는지 확인하십시오. 이는 또한 **runmqckm** 및 **runmqakm** 명령에도 필요합니다. 예를 들면, 다음과 같습니다.

```
export PATH=$PATH:/usr/bin:/bin
```

• Windows 시스템의 경우:

- **strmqikm** 명령을 사용하여 iKeyman GUI를 시작하십시오.
- **runmqckm** 명령을 사용하여 iKeycmd 명령행 인터페이스를 사용하여 태스크를 수행하십시오.
FIPS를 준수하는 방법으로 TLS 인증서를 관리해야 하는 경우, **runmqckm** 또는 **strmqikm** 명령 대신에 **runmqakm** 명령을 사용하십시오.
- **runmqakm -keydb** 명령을 **stashpw** 또는 **stash** 옵션과 함께 사용하십시오.

예를 들어 다음과 같은 방식으로 **runmqakm -keydb** 명령을 실행하는 경우:

```
runmqakm -keydb -create -db key.kdb -pw secretpwd -stash
```

결과 .sth 파일에는 mqm 그룹에 대한 읽기 권한이 없습니다.

작성자만이 파일을 읽을 수 있습니다. **runmqakm** 명령을 사용하여 스테시 파일을 작성한 후 파일 권한을 검사하고 큐 관리자를 실행하는 서비스 계정에 또는 로컬 mqm과 같은 그룹에 권한을 부여하십시오.

UNIX, Linux 또는 Windows 시스템에서 TLS 추적을 요청하려면 [strmqtrc](#)를 참조하십시오.

관련 참조

[runmqckm 및 runmqakm 명령](#)

이 절에서는 명령의 오브젝트에 따른 runmqckm 및 runmqakm 명령에 대해 설명합니다.

UNIX, Linux, and Windows에서 키 저장소 설정

strmqikm(iKeyman) GUI를 사용하거나 **runmqckm**(iKeycmd) 또는 **runmqakm**(GSKCapiCmd) 명령을 사용하여 명령행에서 키 저장소를 설정할 수 있습니다.

이 태스크 정보

TLS 연결의 경우 연결의 각 끝에 키 저장소가 있어야 합니다. 각 IBM MQ 큐 관리자 및 IBM MQ MQI client에는 키 저장소에 대한 액세스가 있어야 합니다. 자세한 정보는 [22 페이지의 『SSL/TLS 키 저장소』](#)의 내용을 참조하십시오.

UNIX, Linux, and Windows 시스템에서 디지털 인증서는 **strmqikm** 사용자 인터페이스를 사용하거나 **runmqckm** 또는 **runmqakm** 명령을 사용하여 관리되는 키 데이터베이스 파일에 저장됩니다. 이러한 디지털 인증서에는 레이블이 있습니다. 특정 레이블은 개인 인증서를 큐 관리자 또는 IBM MQ MQI client와 연관시킵니다. TLS가 인증 목적으로 해당 인증서를 사용합니다. UNIX, Linux, and Windows 시스템에서 IBM MQ는 **CERTLABL** 속성 값 (설정된 경우) 또는 큐 관리자의 이름이 있는 기본 **ibmwebspheremq** 또는 추가된 IBM MQ MQI client 사용자 로그인 ID (모두 소문자) 를 사용합니다. 자세한 내용은 [디지털 인증서 레이블을 참조하십시오](#).

키 데이터베이스 파일 이름은 경로와 스템 이름으로 구성됩니다.

- UNIX and Linux 시스템에서 큐 관리자의 기본 경로(큐 관리자를 작성할 때 설정됨)는 `/var/mqm/qmgrs/queue_manager_name/ssl`입니다.

Windows 시스템에서 기본 경로는 `MQ_INSTALLATION_PATH\Qmgrs\queue_manager_name\ssl`입니다. 여기서 `MQ_INSTALLATION_PATH`는 IBM MQ가 설치된 디렉토리입니다. 예를 들어, `C:\Program Files\IBM\MQ\Qmgrs\QM1\ssl`입니다.

기본 스템 이름은 `key`입니다. 선택적으로 사용자 고유의 경로 및 스템 이름을 선택할 수 있지만 확장자는 `.kdb`여야 합니다.

사용자 고유의 경로나 파일 이름을 선택하는 경우에는 이에 대한 액세스를 엄격하게 제어하기 위해 파일에 권한을 설정하십시오.

- IBM MQ 클라이언트의 경우 기본 경로나 스템 이름이 없습니다. 이 파일에 대한 액세스를 엄격하게 제어하십시오. 확장자는 `.kdb`여야 합니다.

파일 레벨 잠금을 지원하지 않는 파일 시스템에서 키 저장소를 작성하지 마십시오(예: Linux 시스템에서 NFS 버전 2).

키 데이터베이스 파일 이름 검사 및 지정에 대한 자세한 정보는 260 페이지의 『UNIX, Linux, and Windows에서 큐 관리자의 키 저장소 위치 변경』의 내용을 참조하십시오. 키 데이터베이스 파일을 작성하기 전후에 키 데이터베이스 파일 이름을 지정할 수 있습니다.

strmqikm 또는 **runmqckm** 명령을 실행하는 사용자 ID에는 키 데이터베이스 파일을 작성하거나 업데이트한 디렉토리에 대한 쓰기 권한이 있어야 합니다. 기본 `ssl` 디렉토리를 사용하는 큐 관리자의 경우 **strmqikm** 또는 **runmqckm**를 실행하는 사용자 ID는 `mqm` 그룹의 구성원이어야 합니다. IBM MQ MQI client의 경우, 클라이언트를 실행 중인 사용자 ID와 다른 사용자 ID로부터 **strmqikm** 또는 **runmqckm**을 실행하는 경우에는 IBM MQ MQI client가 런타임 시에 키 데이터베이스 파일에 액세스할 수 있도록 파일 권한을 변경해야 합니다. 자세한 정보는 259 페이지의 『Windows에서 키 데이터베이스 파일 액세스 및 보안』 또는 259 페이지의 『UNIX and Linux 시스템에서 키 데이터베이스 파일 액세스 및 보안』의 내용을 참조하십시오.

In **strmqikm** or **runmqckm** for IBM WebSphere MQ 7.0, new key databases are automatically populated with a set of pre-defined certificate authority (CA) certificates. In **strmqikm** or **runmqckm** for IBM MQ 8.0, key databases are not automatically populated, making the initial setup more secure because you include only the CA certificates that you want, in your key database file.

참고: CA 인증서가 저장소에 더 이상 자동으로 추가되지 않는 GSKit 8.0의 동작이 이러한 변경으로 인해 선호하는 CA 인증서를 수동으로 추가해야 합니다. 이 동작의 변화는 사용된 CA 인증서에 대한 보다 세부 단위의 제어를 제공합니다. 259 페이지의 『GSKit 8.0를 사용하여 UNIX, Linux, and Windows의 빈 키 저장소에 기본 CA 인증서 추가』을 참조하십시오.

명령행을 사용하거나 **strmqikm** (iKeyman) 사용자 인터페이스를 사용하여 키 데이터베이스를 작성합니다.

참고: FIPS를 준수하는 방법으로 TLS 인증서를 관리해야 하는 경우, **runmqakm** 명령을 사용하십시오. **strmqikm** 사용자 인터페이스는 FIPS 준수 옵션을 제공하지 않습니다.

프로시저

명령행을 사용하여 키 데이터베이스를 작성한다.

1. 다음 명령 중 하나를 실행하십시오.

- **runmqckm** 사용:

```
runmqckm -keydb -create -db filename -pw password -type cms -stash
```

- **runmqakm** 사용:

```
runmqakm -keydb -create -db filename -pw password -type cms -stash -fips -strong
```

설명:

-db filename

CMS 키 데이터베이스의 완전한 파일 이름을 지정하고 .kdb의 파일 확장자가 있어야 합니다.

-pw password

CMS 키 데이터베이스의 비밀번호를 지정합니다.

-type cms

데이터베이스의 유형을 지정합니다. (IBM MQ의 경우 cms여야 합니다.)

-stash

키 데이터베이스 비밀번호를 파일에 저장합니다.

-fips

명령이 FIPS 모드에서 실행되도록 지정합니다. FIPS 모드에서는 ICC 컴포넌트는 FIPS 140-2 유효성 검증된 알고리즘을 사용합니다. ICC 컴포넌트가 FIPS 모드에서 초기화되지 않는 경우에는 **runmqakm** 명령이 실패합니다.

-strong

입력한 비밀번호가 비밀번호 강도에 대한 최소 요구사항을 충족하는지 검사합니다. 비밀번호의 최소 요구사항은 다음과 같습니다.

- 비밀번호는 최소 14자여야 합니다.
- 비밀번호에는 최소 하나의 소문자, 하나의 대문자 및 하나의 숫자 또는 특수 문자를 포함해야 합니다. 특수 문자에는 별표(*), 달러 부호(\$), 숫자 부호(#) 및 퍼센트 부호(%)가 포함됩니다. 공백은 특수 문자로 분류됩니다.
- 각 문자는 비밀번호에서 최대 3회 사용될 수 있습니다.
- 비밀번호에서 최대 두 개의 연속하는 문자가 동일할 수 있습니다.
- 모든 문자는 0x20 - 0x7E 범위 내의 표준 ASCII 인쇄 가능한 문자 세트에 있습니다.

또는 **strmqikm** (iKeyman) 사용자 인터페이스를 사용하여 키 데이터베이스를 작성하십시오.

2. UNIX and Linux 시스템에서 루트 사용자로서 로그인하십시오. Windows 시스템에서 관리자 또는 MQM 그룹의 구성원으로서 로그인하십시오.
3. **strmqikm** 명령을 실행하여 사용자 인터페이스를 시작하십시오.
4. 키 데이터베이스 파일 메뉴에서 새로 작성을 클릭하십시오.
새 창이 열립니다.
5. 키 데이터베이스 유형을 클릭하고 **CMS**(인증서 관리 시스템)를 선택하십시오.
6. 파일 이름 필드에 파일 이름을 입력하십시오.
이 필드에는 이미 key.kdb 텍스트가 포함되어 있습니다. 스템 이름이 key인 경우 이 필드를 변경하지 말고 그대로 두십시오. 다른 스템 이름을 지정한 경우에는 key를 사용자의 스템 이름으로 바꾸십시오. 그러나 .kdb 확장자는 변경하지 않아야 합니다.
7. 위치 필드에 경로를 입력하십시오.
예를 들면, 다음과 같습니다.
 - 큐 관리자의 경우: /var/mqm/qmgrs/QM1/ssl(UNIX and Linux 시스템에서) 또는 C:\ProgramData\IBM\MQ\qmgrs\QM1\ssl(Windows 시스템에서).
경로 이름은 큐 관리자의 **SSLKeyRepository** 속성의 값과 일치해야 합니다.
 - IBM MQ 클라이언트의 경우: /var/mqm/ssl(UNIX and Linux 시스템에서) 또는 C:\mqm\ssl(Windows 시스템에서).
8. 확인을 클릭하십시오.
비밀번호 프롬프트 창이 열립니다.
9. 비밀번호 필드에 비밀번호를 입력하고 비밀번호 확인 필드에 다시 입력하십시오.
10. 파일에 비밀번호 숨김 선택란을 선택하십시오.
참고: 비밀번호를 숨기지 않은 경우에는 키 데이터베이스 파일에 액세스하는 데 필요한 비밀번호를 구할 수 없으므로 TLS 채널을 시작하려는 시도가 실패합니다.
11. 확인을 클릭하십시오.

개인 인증서 창이 열립니다.

12. 259 페이지의 『Windows에서 키 데이터베이스 파일 액세스 및 보안』 또는 259 페이지의 『UNIX and Linux 시스템에서 키 데이터베이스 파일 액세스 및 보안』에 설명된 대로 액세스 권한을 설정하십시오.

Windows Windows에서 키 데이터베이스 파일 액세스 및 보안

키 데이터베이스 파일에는 적합한 액세스 권한이 없을 수도 있습니다. 이러한 파일에 대한 적합한 액세스를 설정해야 합니다.

key.kdb, *key.sth*, *key.crl* 및 *key.rdb* 파일에 대한 액세스 제어를 설정하십시오. 여기서, *key*는 제한된 사용자 세트에 권한을 부여하기 위한 키 데이터베이스의 스템 이름입니다.

다음과 같은 액세스 부여를 고려하십시오.

전체 권한

BUILTIN\Administrators, NT AUTHORITY\SYSTEM 및 데이터베이스 파일을 작성한 사용자입니다.

읽기 권한

큐 관리자의 경우 로컬 mqm 그룹만 해당됩니다. 이는 MCA가 mqm 그룹에 있는 사용자 ID 하에서 실행 중이라고 가정합니다.

클라이언트의 경우 클라이언트 프로세스를 실행하고 있는 사용자 ID입니다.

Linux UNIX UNIX and Linux 시스템에서 키 데이터베이스 파일 액세스 및 보안

키 데이터베이스 파일에는 적합한 액세스 권한이 없을 수도 있습니다. 이러한 파일에 대한 적합한 액세스를 설정해야 합니다.

큐 관리자의 경우 큐 관리자 및 채널 프로세스가 필요할 때 읽을 수 있고 다른 사용자는 읽을 수 없도록 키 데이터베이스 파일에 대한 권한을 설정하십시오. 일반적으로 mqm 사용자는 읽기 권한이 필요합니다. mqm 사용자로서 로그인하여 키 데이터베이스 파일을 작성한 경우에는 권한이 충분할 것입니다. mqm 사용자가 아니지만 mqm 그룹의 다른 사용자인 경우에는 mqm 그룹의 다른 사용자에게 읽기 권한을 부여해야 할 수도 있습니다.

마찬가지로 클라이언트의 경우 클라이언트 애플리케이션 프로세스가 필요할 때 읽을 수 있지만 다른 사용자는 읽거나 수정할 수 없도록 키 데이터베이스 파일에 대한 권한을 설정하십시오. 일반적으로 클라이언트 프로세스를 실행하는 사용자는 읽기 권한이 필요합니다. 해당 사용자로서 로그인하여 키 데이터베이스 파일을 작성한 경우에는 권한이 충분할 것입니다. 클라이언트 프로세스 사용자가 아니라 해당 그룹의 다른 사용자라면 그룹의 다른 사용자에게 읽기 권한을 부여해야 할 수도 있습니다.

key.kdb, *key.sth*, *key.crl* 및 *key.rdb* 파일(여기서 *key*는 키 데이터베이스의 스템 이름)에 대한 권한을 파일 소유자의 경우 읽기 및 쓰기, mqm 또는 클라이언트 사용자 그룹의 경우 읽기로 설정하십시오(-rw-r-----).

ULW GSKit 8.0 를 사용하여 UNIX, Linux, and Windows 의 빈 키 저장소에 기본 CA 인증서 추가

GSKit 버전 8이 있는 빈 키 저장소에 기본 CA 인증서를 하나 이상 추가하려면 이 프로시저를 따르십시오.

GSKit 7.0에서 새 키 저장소를 작성할 때의 작동은 일반적으로 사용되는 인증 기관의 기본 CA 인증서 세트를 자동으로 추가하는 것이었습니다. GSKit 버전 8의 경우, 이 동작은 CA 인증서가 더 이상 자동으로 저장소에 추가되지 않도록 변경되었습니다. 사용자는 이제 키 저장소에 CA 인증서를 수동으로 추가해야 합니다.

strmqikm 사용

CA 인증서를 추가하고 싶은 시스템에서 다음 단계를 수행하십시오.

1. **strmqikm** 명령을 사용하여 GUI를 시작하십시오(UNIX, Linux, and Windows에서).
2. 키 데이터베이스 파일 메뉴에서 열기를 클릭하십시오. 열기 창이 열립니다.
3. 키 데이터베이스 유형을 클릭하고 **CMS**(인증서 관리 시스템)를 선택하십시오.
4. 키 데이터베이스 파일이 있는 디렉토리로 이동하려면 **찾아보기**를 클릭하십시오.
5. 인증서를 추가할 키 데이터베이스 파일을 선택하십시오(예: *key.kdb*).
6. 열기를 클릭하십시오. 비밀번호 프롬프트 창이 열립니다.
7. 키 데이터베이스를 작성할 때 설정한 비밀번호를 입력하고 **확인**을 클릭하십시오. 키 데이터베이스 파일의 이름이 **파일 이름** 필드에 표시됩니다.

8. 키 데이터베이스 콘텐츠 필드에서 서명자 인증서를 선택하십시오.
9. 채우기를 클릭하십시오. CA의 인증서 추가 창이 열립니다.
10. 저장소에 추가할 수 있는 CA 인증서가 계층 구조 트리 구조에 표시됩니다. 올바른 CA 인증서의 전체 목록을 보려면 신뢰하려는 CA 인증서가 포함된 조직의 맨 위 레벨 항목을 선택하십시오.
11. 목록에서 신뢰하려는 CA 인증서를 선택하고 **확인**을 클릭하십시오. 인증서가 키 저장소에 추가됩니다.

명령행 사용

다음 명령을 사용하여 나열한 다음 **runmqckm**을 사용하여 CA 인증서를 추가하십시오.

- 다음 명령을 실행하여 기본 CA 인증서를 이를 발행한 조직과 함께 나열하십시오.

```
runmqckm -cert -listsigners
```

- 레이블 필드에 지정된 조직의 모든 CA 인증서를 추가하려면 다음 명령을 실행하십시오.

```
runmqckm -cert -populate -db filename -pw password -label label
```

설명:

- db *filename* 키 데이터베이스의 완전한 경로 이름입니다.
- pw *password* 키 데이터베이스의 비밀번호입니다.
- label *label* 인증서에 첨부된 레이블입니다.

참고: CA 인증서를 키 저장소에 추가하면 IBM MQ이 해당 CA 인증서로 서명된 모든 개인 인증서를 신뢰하는 결과 나옵니다. 어떤 인증 기관을 신뢰할지 신중히 검토하고 클라이언트와 관리자를 인증하는 데 필요한 CA 인증서 세트만 추가하십시오. 보안 정책의 결정적인 요구사항이 아닌 한 기본 CA 인증서의 전체 세트를 추가하는 것은 바람직하지 않습니다.

UNIX, Linux, and Windows에서 키 저장소에서 큐 관리자 찾기

큐 관리자의 키 데이터베이스 파일 위치를 확보하려면 이 프로시저를 사용하십시오.

프로시저

1. 다음 MQSC 명령을 사용하여 큐 관리자의 속성을 표시하십시오.

```
DISPLAY QMGR ALL
DISPLAY QMGR SSLKEYR
```

IBM MQ Explorer 또는 PCF 명령을 사용하여 큐 관리자의 속성을 표시할 수도 있습니다.

2. 키 데이터베이스 파일의 경로 및 스템 이름의 명령 출력을 검사하십시오. 예를 들면 다음과 같습니다.
 - a. UNIX and Linux의 경우: `/var/mqm/qmgrs/QM1/ssl/key`. 여기서 `/var/mqm/qmgrs/QM1/ssl`은 경로이고 `key`는 스템 이름입니다.
 - b. Windows: `MQ_INSTALLATION_PATH\qmgrs\QM1\ssl\key`, 여기서 `MQ_INSTALLATION_PATH\qmgrs\QM1\ssl`는 경로이고 `key`은 스템 이름입니다. `MQ_INSTALLATION_PATH`는 IBM MQ가 설치되어 있는 상위 레벨 디렉토리를 나타냅니다.

UNIX, Linux, and Windows에서 큐 관리자의 키 저장소 위치 변경

MQSC 명령 ALTER QMGR을 포함한 다양한 수단을 사용하여 큐 관리자의 키 데이터베이스 파일의 위치를 변경할 수 있습니다.

큐 관리자의 키 저장소 속성을 설정하려면 MQSC 명령 ALTER QMGR을 사용하여 큐 관리자의 키 데이터베이스 파일 위치를 변경할 수 있습니다. 예를 들어 UNIX and Linux에서는 다음과 같습니다.

```
ALTER QMGR SSLKEYR('/var/mqm/qmgrs/QM1/ssl/MyKey')
```

키 데이터베이스 파일에는 완전한 파일 이름(/var/mqm/qmgrs/QM1/ssl/MyKey.kdb)이 있습니다.

Windows의 경우:

```
ALTER QMGR SSLKEYR('C:\Program Files\IBM\MQ\Qmgrs\QM1\ssl\Mykey')
```

키 데이터베이스 파일에는 완전한 파일 이름(C:\Program Files\IBM\MQ\Qmgrs\QM1\ssl\Mykey.kdb)이 있습니다.



주의: SSLKEYR 키워드에서 파일 이름에 .kdb 확장자를 포함하지 않도록 하십시오. 큐 관리자가 이 확장자를 자동으로 추가하기 때문입니다.

IBM MQ 탐색기 또는 PCF 명령을 사용하여 큐 관리자의 속성을 변경할 수도 있습니다.

큐 관리자의 키 데이터베이스 파일의 위치를 변경할 때 인증서는 이전 위치에서 전송되지 않습니다. 현재 액세스 중인 키 데이터베이스 파일이 새 키 데이터베이스 파일인 경우 274 페이지의 『UNIX, Linux, and Windows에서 개인 인증서를 키 저장소로 가져오기』에 설명된 대로 필요한 CA 및 개인용 인증서로 채워야 합니다.

UNIX, Linux, and Windows 에서 IBM MQ MQI client 에 대한 키 저장소 찾기

키 저장소의 위치는 MQSSLKEYR 변수에 의해 제공되거나 MQCONNX 호출에 지정됩니다.

IBM MQ MQI client의 키 데이터베이스 파일의 위치를 찾으려면 MQSSLKEYR 환경 변수를 검사하십시오. 예를 들면, 다음과 같습니다.

```
echo $MQSSLKEYR
```

키 데이터베이스 파일 이름은 261 페이지의 『UNIX, Linux, and Windows 에서 IBM MQ MQI client 에 대한 키 저장소 위치 지정』에 설명된 대로 MQCONNX 호출에 설정될 수도 있으므로 애플리케이션도 검사하십시오. MQCONNX 호출에 설정한 값은 MQSSLKEYR의 값을 대체합니다.

UNIX, Linux, and Windows 에서 IBM MQ MQI client 에 대한 키 저장소 위치 지정

IBM MQ MQI client의 기본 키 저장소가 없습니다. 위치를 다음 두 방법 중 하나로 지정할 수 있습니다. 키 데이터베이스 파일이 다른 시스템으로 무단 복사되는 것을 막기 위해 의도한 사용자 또는 관리자만이 액세스할 수 있는지 확인하십시오.

IBM MQ MQI client의 키 데이터베이스 파일의 위치를 두 가지 방법으로 지정할 수 있습니다.

- MQSSLKEYR 환경 변수 설정. 예를 들어 UNIX and Linux에서는 다음과 같습니다.

```
export MQSSLKEYR=/var/mqm/ssl/key
```

키 데이터베이스 파일에는 완전한 파일 이름이 있습니다.

```
/var/mqm/ssl/key.kdb
```

Windows의 경우:

```
set MQSSLKEYR=C:\Program Files\IBM\MQ\ssl\key
```

키 데이터베이스 파일에는 완전한 파일 이름이 있습니다.

```
C:\Program Files\IBM\MQ\ssl\key.kdb
```


참고: .kdb 확장자는 파일 이름의 필수 부분이지만 환경 변수의 값의 일부로는 포함되지 않습니다.

- 애플리케이션이 MQCONNX 호출을 할 때 MQSCO 구조의 *KeyRepository* 필드에 키 데이터베이스 파일의 경로 및 스템 이름 제공. MQCONNX에서 MQSCO 구조의 사용에 대한 자세한 정보는 [MQSCO 개요](#)의 내용을 참조하십시오.

ULW 인증서 또는 인증서 저장소의 변경사항이 UNIX, Linux, and Windows에서 적용되는 시기

인증서 저장소에서 인증서 또는 인증서 저장소의 위치를 변경할 때 변경사항은 채널 유형 및 채널이 실행 중인 방법에 따라 적용됩니다.

키 데이터베이스 파일의 인증서 및 키 저장소 속성의 변경사항은 다음 경우에 적용됩니다.

- 새 아웃바운드 단일 프로세스가 처음으로 TLS 채널을 실행할 때.
- 새 인바운드 TCP/IP 단일 채널 프로세스가 처음으로 TLS 채널을 시작하라는 요청을 수신할 때.
- MQSC 명령 REFRESH SECURITY TYPE(SSL)이 TLS 환경을 새로 고치기 위해 실행될 때.
- 클라이언트 애플리케이션 프로세스의 경우, 프로세스에서 마지막 TLS 연결이 닫힐 때. 다음 TLS 연결에는 인증서 변경사항이 적용됩니다.
- 프로세스 풀링 프로세스(amqrmppa)의 스레드로서 실행되는 채널의 경우 프로세스 풀링 프로세스가 시작되거나 재시작되고 TLS 채널을 처음 시작할 때. 프로세스 풀링 프로세스가 이미 TLS 채널을 실행했고 변경사항을 즉시 적용하고 싶은 경우, MQSC 명령 REFRESH SECURITY TYPE(SSL)을 실행하십시오.
- 채널 시작기의 스레드로서 실행되는 채널의 경우 채널 시작기가 시작되거나 재시작되고 TLS 채널을 처음 실행할 때. 채널 시작기 프로세스가 이미 TLS 채널을 실행했고 변경사항을 즉시 적용하고 싶은 경우에는 MQSC 명령 REFRESH SECURITY TYPE(SSL)을 실행하십시오.
- TCP/IP 리스너의 스레드로서 실행되는 채널의 경우 리스너가 시작되거나 재시작되고 TLS 채널을 시작하라는 요청을 처음으로 수신할 때. 리스너가 이미 TLS 채널을 실행했고 변경사항을 즉시 적용하고 싶으면 MQSC 명령 REFRESH SECURITY TYPE(SSL)을 실행하십시오.

또한 IBM MQ 탐색기 또는 PCF 명령을 사용하여 IBM MQ TLS 환경을 새로 고칠 수도 있습니다.

ULW UNIX, Linux, and Windows에서 자체 서명된 개인 인증서 작성

strmqikm(iKeyman) GUI를 사용하거나 **runmqckm**(iKeycmd) 또는 **runmqakm**(GSKCapiCmd)을 사용하여 명령행에서 자체 서명한 인증서를 작성할 수 있습니다.

참고: IBM MQ는 SHA-3 또는 SHA-5 알고리즘을 지원하지 않습니다. 디지털 서명 알고리즘 이름 SHA384WithRSA 및 SHA512WithRSA를 사용할 수 있습니다. 두 알고리즘 모두 SHA-2 제품군의 구성원이기 때문입니다.

디지털 서명 알고리즘 이름 SHA3WithRSA 및 SHA5WithRSA는 각각 SHA384WithRSA 및 SHA512WithRSA의 축약된 양식이므로 더 이상 사용되지 않습니다.

자체 서명 인증서를 사용하고 싶은 이유에 대한 자세한 정보는 두 큐 관리자의 상호 인증을 위해 자체 서명 인증 사용을 참조하십시오.

모든 디지털 인증서를 모든 CipherSpec과 함께 사용할 수 있는 것은 아닙니다. 사용해야 하는 CipherSpec과 호환되는 인증서를 작성하는지 확인하십시오. IBM MQ는 세 가지 유형의 CipherSpec을 지원합니다. 자세한 내용은 40 페이지의 『IBM MQ에서 디지털 인증서와 CipherSpec의 호환성』 주제에서 41 페이지의 『Elliptic Curve 및 RSA CipherSpec의 상호 운용성』의 내용을 참조하십시오.

유형 1 CipherSpecs (ECDHE_ECDSA_로 시작하는 이름) 를 사용하려면 **runmqakm** 명령을 사용하여 인증서를 작성해야 하며, 생략 곡선 ECDSA 서명 알고리즘 매개변수 (예: **-sig_alg EC_ecdsa_with_SHA384**) 를 지정해야 합니다.

-sig_alg 해싱 알고리즘에서 사용 가능한 옵션 목록은 476 페이지의 『UNIX, Linux, and Windows의 runmqckm 및 runmqakm 옵션』 를 참조하십시오.

사용 도구가 다음과 같은 경우

- GUI인 경우 263 페이지의 『strmqikm 사용자 인터페이스 사용:』 참조
- 명령행인 경우 263 페이지의 『명령행 사용』 참조

strmqikm 사용자 인터페이스 사용:

strmqikm(iKeyman) GUI를 사용하여 개인 인증서를 작성할 수 있습니다.

이 태스크 정보

strmqikm에서는 FIPS 준수 옵션을 제공하지 않습니다. FIPS를 준수하는 방법으로 TLS 인증서를 관리해야 하는 경우, **runmqakm** 명령을 사용하십시오.

프로시저

다음 단계를 완료하여 그래픽 사용자 인터페이스를 통해 큐 관리자 또는 IBM MQ MQI client에 대한 개인 인증서를 작성하십시오.

1. **strmqikm** 명령을 사용하여 GUI를 시작하십시오.
2. 키 데이터베이스 파일 메뉴에서 **열기**를 클릭하십시오.
열기 창이 표시됩니다.
3. 키 데이터베이스 유형을 클릭하고 **CMS**(인증서 관리 시스템)를 선택하십시오.
4. 키 데이터베이스 파일이 있는 디렉토리로 이동하려면 **찾아보기**를 클릭하십시오.
5. 요청을 생성하려는 키 데이터베이스 파일을 선택하십시오(예: key.kdb).
6. **확인**을 클릭하십시오.
비밀번호 프롬프트 창이 열립니다.
7. 키 데이터베이스를 작성할 때 설정한 비밀번호를 입력하고 **확인**을 클릭하십시오.
키 데이터베이스 파일의 이름이 **파일 이름** 필드에 표시됩니다.
8. **작성** 메뉴에서 **새 자체 서명 인증서**를 클릭하십시오. 새 자체 서명 인증서 작성 창이 표시됩니다.
9. **키 레이블** 필드에 인증서 레이블을 입력하십시오.
레이블은 **CERTLABL** 속성의 값 (설정된 경우) 또는 큐 관리자의 이름이 있는 기본 **ibmwebspheremq** 또는 IBM MQ MQI client 로그온 사용자 ID (모두 소문자)입니다. 자세한 내용은 [디지털 인증서 레이블을 참조하십시오](#).
10. **식별 이름** 필드 또는 **제목 대체 이름** 필드에서 임의의 필드의 값을 입력하거나 선택하십시오.
11. 나머지 필드의 경우 기본값을 승인하거나 새 값을 입력하거나 선택하십시오.
식별 이름에 대한 자세한 정보는 [10 페이지의 『식별 이름』의 내용을 참조하십시오](#).
12. **확인**을 클릭하십시오.
개인 인증서 목록은 사용자가 작성한 자체 서명 개인 인증서의 레이블을 보여줍니다.

다음에 수행할 작업

인증서 요청을 CA에 제출하십시오. 자세한 정보는 [269 페이지의 『UNIX, Linux, and Windows에서 키 저장소에 개인 인증서 수신』의 내용을 참조하십시오](#).

명령행 사용

runmqckm(iKeycmd) 또는 **runmqakm**(GSKCapiCmd) 명령을 사용하여 명령행에서 개인 인증서를 작성할 수 있습니다. FIPS를 준수하는 방법으로 SSL 또는 TLS 인증서를 관리해야 하는 경우, **runmqakm** 명령을 사용하십시오.

프로시저

runmqckm 또는 **runmqakm**(GSKCapiCmd) 명령을 사용하여 자체 서명된 개인 인증서를 작성하십시오.

- UNIX, Linux, and Windows에서 **runmqckm** 사용:

```
runmqckm -cert -create -db filename -pw  
password -label label  
-dn distinguished_name -size key_size
```

```
-x509version version -expire days
-sig_alg algorithm
```

-dn *distinguished_name* 대신 -san_dnsname *DNS_names*, -san_emailaddr *email_addresses* 또는 -san_ipaddr *IP_addresses*을(를) 사용할 수 있습니다.

• **runmqakm** 사용:

```
runmqakm -cert -create -db filename -pw
password -label label
        -dn distinguished_name -size key_size
        -x509version version -expire days

        -fips -sig_alg algorithm
```

설명:

-db filename

CMS 키 데이터베이스의 완전한 파일 이름을 지정합니다.

-pw password

CMS 키 데이터베이스의 비밀번호를 지정합니다.

-label label

인증서에 첨부된 키 레이블을 지정합니다. 레이블은 **CERTLABL** 속성의 값(설정된 경우)이거나 큐 관리자의 이름 또는 IBM MQ MQI client 로그인 사용자 ID가 추가된 기본 **ibmwebspheremq**(모두 소문자)입니다. 자세한 내용은 23 페이지의 『디지털 인증서 레이블, 요구사항 이해』의 내용을 참조하십시오.

-dn distinguished_name

큰따옴표로 묶인 X.500 식별 이름을 지정합니다. 하나 이상의 속성이 필요합니다. 여러 OU 및 DC 속성을 제공할 수 있습니다.

참고: **runmqckm** 및 **runmqakm** 도구는 우편번호 속성을 PC가 아니라 POSTALCODE로 참조합니다. 이러한 인증서 관리 명령을 사용하여 우편 번호가 있는 인증서를 요청하는 경우 항상 **-dn** 매개변수에 POSTALCODE를 지정하십시오.

-size key_size

키 크기를 지정합니다. **runmqckm**을 사용 중인 경우 값은 512 또는 1024일 수 있습니다. **runmqakm**을 사용 중인 경우 값은 512, 1024 또는 2048일 수 있습니다.

x509version version

작성할 X.509 인증서의 버전입니다. 값은 1, 2 또는 3일 수 있습니다. 기본은 3입니다.

-file filename

인증서 요청의 파일 이름을 지정합니다.

-expire days

인증서의 만기 시간(일)입니다. 기본값은 인증서의 경우 365일입니다.

-fips

명령이 FIPS 모드에서 실행되도록 지정합니다. FIPS ICC 컴포넌트만이 사용되고 이 컴포넌트는 FIPS 모드에서 성공적으로 초기화되어야 합니다. FIPS 모드에서 ICC 컴포넌트는 FIPS 140-2 유효성 검증된 알고리즘을 사용합니다. ICC 컴포넌트가 FIPS 모드에서 초기화되지 않는 경우에는 **runmqakm** 명령이 실패합니다.

-sig_alg

runmqckm의 경우, 항목의 키 쌍 작성에 사용된 비대칭 서명 알고리즘을 지정합니다. 값은 다음과 같을 수 있습니다. MD2_WITH_RSA, MD2WithRSA, MD5_WITH_RSA, MD5WithRSA, SHA1WithDSA, SHA1WithECDSA, SHA1WithRSA, SHA2/ECDSA, SHA224WithECDSA, SHA256_WITH_RSA, SHA256WithECDSA, SHA256WithRSA, SHA2WithECDSA, SHA3/ECDSA, SHA384_WITH_RSA, SHA384WithECDSA, SHA384WithRSA, SHA3WithECDSA, SHA5/ECDSA, SHA512_WITH_RSA, SHA512WithECDSA, SHA512WithRSA, SHA5WithECDSA, SHA_WITH_DSA, SHA_WITH_RSA, SHAWithDSA, SHAWithRSA. 기본값은 SHA1WithRSA입니다.

-sig_alg

runmqakm의 경우 인증서 요청의 작성 동안에 사용된 해싱 알고리즘을 지정합니다. 이 해싱 알고리즘은 새로 작성된 인증서 요청과 연관된 서명을 작성하는 데 사용됩니다. 값은 md5, MD5_WITH_RSA,

MD5WithRSA, SHA_WITH_DSA, SHA_WITH_RSA, sha1, SHA1WithDSA, SHA1WithECDSA, SHA1WithRSA, sha224, SHA224_WITH_RSA, SHA224WithDSA, SHA224WithECDSA, SHA224WithRSA, sha256, SHA256_WITH_RSA, SHA256WithDSA, SHA256WithECDSA, SHA256WithRSA, SHA2WithRSA, sha384, SHA384_WITH_RSA, SHA384WithECDSA, SHA384WithRSA, sha512, SHA512_WITH_RSA, SHA512WithECDSA, SHA512WithRSA, SHAWithDSA, SHAWithRSA, EC_ecdsa_with_SHA1, EC_ecdsa_with_SHA224, EC_ecdsa_with_SHA256, EC_ecdsa_with_SHA384 또는 EC_ecdsa_with_SHA512일 수 있습니다. 기본값은 SHA1WithRSA입니다.

-san_dnsname *DNS_names*

작성 중인 항목의 쉼표로 구분되거나 공백으로 구분된 DNS 이름 목록을 지정합니다.

-san_emailaddr *email_addresses*

작성 중인 항목의 쉼표로 구분되거나 공백으로 구분된 이메일 주소 목록을 지정합니다.

-san_ipaddr *IP_addresses*

작성 중인 항목의 쉼표로 구분되거나 공백으로 구분된 IP 주소 목록을 지정합니다.

다음에 수행할 작업

인증서 요청을 CA에 제출하십시오. 자세한 정보는 [269 페이지의 『UNIX, Linux, and Windows에서 키 저장소에 개인 인증서 수신』](#)의 내용을 참조하십시오.

UNIX, Linux, and Windows에서 개인 인증서 요청

strmqikm(iKeyman) GUI를 사용하거나 **runmqckm**(iKeycmd) 또는 **runmqakm**(GSKCapiCmd) 명령을 사용하여 명령행에서 개인 인증서를 요청할 수 있습니다. FIPS를 준수하는 방법으로 SSL 또는 TLS 인증서를 관리해야 하는 경우, **runmqakm** 명령을 사용하십시오.

이 태스크 정보

strmqikm GUI를 사용하거나 명령행에서 개인 인증서를 요청할 수 있으며 다음 고려사항이 적용됩니다.

- IBM MQ는 SHA-3 또는 SHA-5 알고리즘을 지원하지 않습니다. 디지털 서명 알고리즘 이름 SHA384WithRSA 및 SHA512WithRSA를 사용할 수 있습니다. 두 알고리즘 모두 SHA-2 제품군의 구성원이기 때문입니다.
- 디지털 서명 알고리즘 이름 SHA3WithRSA 및 SHA5WithRSA는 각각 SHA384WithRSA 및 SHA512WithRSA의 축약된 양식이므로 더 이상 사용되지 않습니다.
- 모든 디지털 인증서를 모든 CipherSpec과 함께 사용할 수 있는 것은 아닙니다. 사용해야 하는 CipherSpec과 호환 가능한 인증서를 요청하는지 확인하십시오. IBM MQ는 세 가지 유형의 CipherSpec을 지원합니다. 자세한 내용은 [40 페이지의 『IBM MQ에서 디지털 인증서와 CipherSpec의 호환성』](#) 주제에서 [41 페이지의 『Elliptic Curve 및 RSA CipherSpec의 상호 운용성』](#)의 내용을 참조하십시오.
- 유형 1 CipherSpecs (ECDHE_ECDSA_로 시작하는 이름 포함) 를 사용하려면 **runmqakm** 명령을 사용하여 인증서를 요청하고, Elliptic Curve ECDSA 서명 알고리즘 매개변수 (예: **-sig_alg EC_ecdsa_with_SHA384**) 를 지정해야 합니다.

-sig_alg 해싱 알고리즘에서 사용 가능한 옵션 목록은 [476 페이지의 『UNIX, Linux, and Windows의 runmqckm 및 runmqakm 옵션』](#) 를 참조하십시오.

- **runmqakm** 명령만 FIPS 준수 옵션을 제공합니다.
- 암호화 하드웨어를 사용 중인 경우에는 [282 페이지의 『PKCS #11 하드웨어의 개인 인증서 요청』](#)의 내용을 참조하십시오.

사용 도구가 다음과 같은 경우

- GUI인 경우 [266 페이지의 『strmqikm 사용자 인터페이스 사용:』](#) 참조
- 명령행인 경우 [266 페이지의 『명령행 사용』](#) 참조

strmqikm(iKeyman) GUI를 사용하거나 **runmqckm**(iKeycmd) 또는 **runmqakm**(GSKCapiCmd) 명령을 사용하여 명령행에서 개인 인증서를 요청할 수 있습니다. FIPS를 준수하는 방법으로 SSL 또는 TLS 인증서를 관리해야 하는 경우, **runmqakm** 명령을 사용하십시오.

이 태스크 정보

strmqikm에서는 FIPS 준수 옵션을 제공하지 않습니다. FIPS를 준수하는 방법으로 TLS 인증서를 관리해야 하는 경우, **runmqakm** 명령을 사용하십시오.

프로시저

iKeyman 사용자 인터페이스를 사용하여 개인 인증서를 신청하려면 다음 단계를 완료하십시오.

1. **strmqikm** 명령을 사용하여 사용자 인터페이스를 시작하십시오.
2. 키 데이터베이스 파일 메뉴에서 열기를 클릭하십시오.
열기 창이 열립니다.
3. 키 데이터베이스 유형을 클릭하고 **CMS**(인증서 관리 시스템)를 선택하십시오.
4. 키 데이터베이스 파일이 있는 디렉토리로 이동하려면 **찾아보기**를 클릭하십시오.
5. 요청을 생성하려는 키 데이터베이스 파일을 선택하십시오(예: key.kdb).
6. 열기를 클릭하십시오.
비밀번호 프롬프트 창이 열립니다.
7. 키 데이터베이스를 작성할 때 설정한 비밀번호를 입력하고 **확인**을 클릭하십시오.
키 데이터베이스 파일의 이름이 **파일 이름** 필드에 표시됩니다.
8. 작성 메뉴에서 **새 인증서 요청**을 클릭하십시오. **새 키 및 인증서 요청 작성** 창이 열립니다.
9. 키 레이블 필드에 인증서 레이블을 입력하십시오.
레이블은 **CERTLABL** 속성의 값 (설정된 경우) 또는 큐 관리자의 이름이 있는 기본 **ibmwebspheremq** 또는 IBM MQ MQI client 로그온 사용자 ID (모두 소문자)입니다. 자세한 내용은 [디지털 인증서 레이블을 참조하십시오](#).
10. 식별 이름 필드 또는 제목 대체 이름 필드에서 임의의 필드의 값을 입력하거나 선택하십시오. 나머지 필드의 경우 기본값을 승인하거나 새 값을 입력하거나 선택하십시오.
식별 이름에 대한 자세한 정보는 [10 페이지의 『식별 이름』](#)의 내용을 참조하십시오.
11. 인증서 요청을 저장할 파일의 이름 입력 필드에서 기본 **certreq.arm**을 승인하거나 전체 경로가 포함된 새 값을 입력하십시오.
12. **확인**을 클릭하십시오.
확인 창이 표시됩니다.
13. **확인**을 클릭하십시오.
개인 인증서 요청 목록이 사용자가 작성한 새 개인 인증서 요청의 레이블을 보여줍니다. 인증서 요청이 [266 페이지의 『11』](#) 단계에서 선택한 파일에 저장됩니다.
14. 파일을 인증 기관(CA)으로 보내거나 파일을 CA의 웹 사이트에서 요청 양식으로 복사하여 새 개인 인증서를 요청하십시오.

runmqckm(iKeycmd) 또는 **runmqakm**(GSKCapiCmd) 명령을 사용하여 명령행에서 개인 인증서를 요청할 수 있습니다. FIPS를 준수하는 방법으로 SSL 또는 TLS 인증서를 관리해야 하는 경우, **runmqakm** 명령을 사용하십시오.

프로시저

runmqckm 또는 **runmqakm**(GSKCapiCmd) 명령을 사용하여 개인 인증서를 요청하십시오.

- **runmqckm** 사용:

```
runmqckm -certreq -create -db filename -pw  
password -label label  
-dn distinguished_name -size key_size  
-file filename -sig_alg algorithm
```

-dn *distinguished_name* 대신 -san_dsname *DNS_names*, -san_emailaddr *email_addresses* 또는 -san_ipaddr *IP_addresses*을(를) 사용할 수 있습니다.

- **runmqakm** 사용:

```
runmqakm -certreq -create -db filename -pw  
password -label label  
-dn distinguished_name -size key_size  
-file filename -fips -sig_alg algorithm
```

설명:

-db filename

CMS 키 데이터베이스의 완전한 파일 이름을 지정합니다.

-pw password

CMS 키 데이터베이스의 비밀번호를 지정합니다.

-label label

인증서에 첨부된 키 레이블을 지정합니다. 레이블은 **CERTLABL** 속성의 값(설정된 경우)이거나 큐 관리자의 이름 또는 IBM MQ MQI client 로그온 사용자 ID가 추가된 기본 *ibmwebspheremq*(모두 소문자)입니다. 자세한 내용은 23 페이지의 『디지털 인증서 레이블, 요구사항 이해』의 내용을 참조하십시오.

-dn distinguished_name

큰따옴표로 묶인 X.500 식별 이름을 지정합니다. 하나 이상의 속성이 필요합니다. 여러 OU 및 DC 속성을 제공할 수 있습니다.

참고: **runmqckm** 및 **runmqakm** 도구는 우편번호 속성을 PC가 아니라 POSTALCODE로 참조합니다. 이러한 인증서 관리 명령을 사용하여 우편 번호가 있는 인증서를 요청하는 경우 항상 **-dn** 매개변수에 POSTALCODE를 지정하십시오.

-size key_size

키 크기를 지정합니다. **runmqckm**을 사용 중인 경우 값은 512 또는 1024일 수 있습니다. **runmqakm**을 사용 중인 경우 값은 512, 1024 또는 2048일 수 있습니다.

-file filename

인증서 요청의 파일 이름을 지정합니다.

-fips

명령이 FIPS 모드에서 실행되도록 지정합니다. FIPS 모드에서는 ICC 컴포넌트는 FIPS 140-2 유효성 검증된 알고리즘을 사용합니다. ICC 컴포넌트가 FIPS 모드에서 초기화되지 않는 경우에는 **runmqakm** 명령이 실패합니다.

-sig_alg

runmqckm의 경우, 항목의 키 쌍 작성에 사용된 비대칭 서명 알고리즘을 지정합니다. 값은 다음과 같을 수 있습니다. MD2_WITH_RSA, MD2WithRSA, MD5_WITH_RSA, MD5WithRSA, SHA1WithDSA, SHA1WithECDSA, SHA1WithRSA, SHA2/ECDSA, SHA224WithECDSA, SHA256_WITH_RSA, SHA256WithECDSA, SHA256WithRSA, SHA2WithECDSA, SHA3/ECDSA, SHA384_WITH_RSA, SHA384WithECDSA, SHA384WithRSA, SHA3WithECDSA, SHA5/ECDSA, SHA512_WITH_RSA, SHA512WithECDSA, SHA512WithRSA, SHA5WithECDSA, SHA_WITH_DSA, SHA_WITH_RSA, SHAWithDSA, SHAWithRSA. 기본값은 SHA1WithRSA입니다.

-sig_alg

runmqakm의 경우 인증서 요청의 작성 동안에 사용된 해싱 알고리즘을 지정합니다. 이 해싱 알고리즘은 새로 작성된 인증서 요청과 연관된 서명을 작성하는 데 사용됩니다. 값은 md5, MD5_WITH_RSA, MD5WithRSA, SHA_WITH_DSA, SHA_WITH_RSA, sha1, SHA1WithDSA, SHA1WithECDSA, SHA1WithRSA, sha224, SHA224_WITH_RSA, SHA224WithDSA, SHA224WithECDSA,

SHA224WithRSA, sha256, SHA256_WITH_RSA, SHA256WithDSA, SHA256WithECDSA, SHA256WithRSA, SHA2WithRSA, sha384, SHA384_WITH_RSA, SHA384WithECDSA, SHA384WithRSA, sha512, SHA512_WITH_RSA, SHA512WithECDSA, SHA512WithRSA, SHAWithDSA, SHAWithRSA, EC_ecdsa_with_SHA1, EC_ecdsa_with_SHA224, EC_ecdsa_with_SHA256, EC_ecdsa_with_SHA384 또는 EC_ecdsa_with_SHA512일 수 있습니다. 기본값은 SHA1WithRSA입니다.

-san_dnsname DNS_names

작성 중인 항목의 쉼표로 구분되거나 공백으로 구분된 DNS 이름 목록을 지정합니다.

-san_emailaddr email_addresses

작성 중인 항목의 쉼표로 구분되거나 공백으로 구분된 이메일 주소 목록을 지정합니다.

-san_ipaddr IP_addresses

작성 중인 항목의 쉼표로 구분되거나 공백으로 구분된 IP 주소 목록을 지정합니다.

다음에 수행할 작업

인증서 요청을 CA에 제출하십시오. 자세한 정보는 [269 페이지의 『UNIX, Linux, and Windows에서 키 저장소에 개인 인증서 수신』](#)의 내용을 참조하십시오.

UNIX, Linux, and Windows에서 기존 개인 인증서 갱신

strmqikm(iKeyman) GUI를 사용하거나 **runmqckm**(iKeycmd) 또는 **runmqakm**(GSKCapiCmd) 명령을 사용하여 명령행으로부터 개인 인증서를 갱신할 수 있습니다.

이 태스크 정보

개인 인증서에 더 큰 키 크기를 사용해야 하는 요구사항이 있는 경우 기존 인증서를 갱신할 수 없습니다. 필요한 키 크기를 사용하는 새 인증서 요청을 작성하려면 [265 페이지의 『UNIX, Linux, and Windows에서 개인 인증서 요청』](#)에 설명된 단계를 따라서 기존 키를 대체해야 합니다.

개인 인증서에는 만기 날짜가 있고, 그 후에는 인증서를 더 이상 사용할 수 없습니다. 이 태스크는 인증서가 만기 되기 전에 기존 개인 인증서를 갱신하는 방법을 설명합니다.

strmqikm 사용자 인터페이스 사용:

이 태스크 정보

strmqikm에서는 FIPS 준수 옵션을 제공하지 않습니다. FIPS를 준수하는 방법으로 TLS 인증서를 관리해야 하는 경우, **runmqakm** 명령을 사용하십시오.

프로시저

strmqikm 사용자 인터페이스를 사용하여 개인 인증서를 신청하려면 다음 단계를 완료하십시오.

1. UNIX, Linux, and Windows에서 **strmqikm** 명령을 사용하여 사용자 인터페이스를 시작하십시오.
2. 키 데이터베이스 파일 메뉴에서 열기를 클릭하십시오.
열기 창이 열립니다.
3. 키 데이터베이스 유형을 클릭하고 **CMS**(인증서 관리 시스템)를 선택하십시오.
4. 키 데이터베이스 파일이 있는 디렉토리로 이동하려면 **찾아보기**를 클릭하십시오.
5. 요청을 생성하려는 키 데이터베이스 파일을 선택하십시오(예: key.kdb).
6. 열기를 클릭하십시오.
비밀번호 프롬프트 창이 열립니다.
7. 키 데이터베이스를 작성할 때 설정한 비밀번호를 입력하고 **확인**을 클릭하십시오.
키 데이터베이스 파일의 이름이 **파일 이름** 필드에 표시됩니다.
8. 드롭 다운 선택 메뉴에서 **개인 인증서**를 선택하고 갱신하려는 목록에서 인증서를 선택하십시오.
9. **요청 재작성 ...** 을 클릭하십시오. 표시됩니다.

파일 이름과 파일 위치 정보를 입력하기 위한 창이 열립니다.

10. **파일 이름** 필드에서 기본 `certreq.arm`을 승인하거나, 전체 파일 경로를 포함하여 새 값을 입력하십시오.
11. **확인**을 클릭하십시오. 인증서 요청이 [268 페이지의 『9』 단계](#)에서 선택한 파일에 저장됩니다.
12. 파일을 인증 기관(CA)으로 보내거나 파일을 CA의 웹 사이트에서 요청 양식으로 복사하여 새 개인 인증서를 요청하십시오.

명령행 사용

프로시저

`runmqckm` 또는 `runmqakm` 명령을 사용하여 개인 인증서를 요청하려면 다음 명령을 사용하십시오.

- UNIX, Linux, and Windows 시스템에서 `runmqckm` 사용:

```
runmqckm -certreq -recreate -db filename -pw
password -label label
-target filename
```

- `runmqakm` 사용:

```
runmqakm -certreq -recreate -db filename -pw
password -label label
-target filename
```

설명:

-db filename

CMS 키 데이터베이스의 완전한 파일 이름을 지정합니다.

-pw password

CMS 키 데이터베이스의 비밀번호를 지정합니다.

-target filename

인증서 요청의 파일 이름을 지정합니다.

다음에 수행할 작업

인증 기관으로부터 서명된 개인 인증서를 받은 후에는 이를 [269 페이지의 『UNIX, Linux, and Windows에서 키 저장소에 개인 인증서 수신』](#)에 설명된 단계를 사용하여 키 데이터베이스에 추가할 수 있습니다.

UNIX, Linux, and Windows에서 키 저장소에 개인 인증서 수신

개인 인증서를 키 데이터베이스 파일에 수신하려면 이 프로시저를 사용하십시오. 키 저장소는 인증서 요청을 작성한 곳과 같은 저장소여야 합니다.

CA가 새 개인 인증서를 송신한 후에 새 인증서 요청을 생성한 위치인 키 데이터베이스 파일에 이를 추가합니다. CA가 이메일 메시지의 일부로서 인증서를 송신하면 인증서를 별도의 파일로 복사하십시오.

strmqikm 사용

FIPS를 준수하는 방법으로 TLS 인증서를 관리해야 하는 경우, `runmqakm` 명령을 사용하십시오. `strmqikm`에서는 FIPS 준수 옵션을 제공하지 않습니다.

가져올 인증서 파일에 현재 사용자에게 쓰기 권한이 있는지 확인한 다음 큐 관리자 또는 IBM MQ MQI client를 위해 다음 프로시저를 사용하여 개인 인증서를 키 데이터베이스 파일에 수신하십시오.

1. `strmqikm` 명령을 사용하여 GUI를 시작하십시오(Windows UNIX and Linux에서).
2. 키 데이터베이스 파일 메뉴에서 열기를 클릭하십시오. 열기 창이 열립니다.
3. 키 데이터베이스 유형을 클릭하고 **CMS**(인증서 관리 시스템)를 선택하십시오.
4. 키 데이터베이스 파일이 있는 디렉토리로 이동하려면 **찾아보기**를 클릭하십시오.
5. 인증서를 추가할 키 데이터베이스 파일을 선택하십시오(예: `key.kdb`).

6. 열기를 클릭한 다음 **확인**을 클릭하십시오. 비밀번호 프롬프트 창이 열립니다.
7. 키 데이터베이스를 작성할 때 설정한 비밀번호를 입력하고 **확인**을 클릭하십시오. 키 데이터베이스 파일의 이름이 **파일 이름** 필드에 표시됩니다. **개인 인증서** 보기를 선택하십시오.
8. 수신을 클릭하십시오. 파일에서 인증서 수신 창이 열립니다.
9. 새 개인 인증서의 인증서 파일 이름 및 위치를 입력하거나 **찾아보기**를 클릭하여 이름 및 위치를 선택하십시오.
10. **확인**을 클릭하십시오. 키 데이터베이스에 이미 개인 인증서가 있는 경우, 추가 중인 키를 데이터베이스에서 기본 키로 설정할지를 묻는 창이 열립니다.
11. **예** 또는 **아니오**를 클릭하십시오. 레이블 입력 창이 열립니다.
12. **확인**을 클릭하십시오. **개인 인증서** 필드가 사용자가 추가한 새 개인 인증서의 레이블을 보여줍니다.

명령행 사용

개인 인증서를 키 데이터베이스 파일에 추가하려면 다음 명령 중 하나를 사용하십시오.

- **runmqckm** 사용:

```
runmqckm -cert -receive -file filename -db filename -pw password
          -format ascii
```

- **runmqakm** 사용:

```
runmqakm -cert -receive -file filename -db filename -pw password -fips
```

설명:

-file filename

개인 인증서의 완전한 파일 이름을 지정합니다.

-db filename

CMS 키 데이터베이스의 완전한 파일 이름을 지정합니다.

-pw password

CMS 키 데이터베이스의 비밀번호를 지정합니다.

-format ascii

인증서의 형식을 지정합니다. 값은 Base64-encoded ASCII의 경우 `ascii` 또는 2진 DER 데이터의 경우 `binary`일 수 있습니다. 기본값은 `ascii`입니다.

-fips

명령이 FIPS 모드에서 실행되도록 지정합니다. FIPS 모드에서 ICC 컴포넌트는 FIPS 140-2 유효성 검증된 알고리즘을 사용합니다. ICC 컴포넌트가 FIPS 모드에서 초기화되지 않는 경우에는 **runmqakm** 명령이 실패합니다.

암호화 하드웨어를 사용 중인 경우에는 283 페이지의 『PKCS #11 하드웨어로 개인 인증서 수신』의 내용을 참조하십시오.

UNIX, Linux, and Windows에서 키 저장소로부터 인증서 추출

CA 인증서를 추출하려면 이 프로시저를 따르십시오.

strmqikm 사용

FIPS를 준수하는 방법으로 TLS 인증서를 관리해야 하는 경우, **runmqakm** 명령을 사용하십시오. **strmqikm**(iKeyman)에서는 FIPS 준수 옵션을 제공하지 않습니다.

CA 인증서를 추출하려는 시스템에서 다음 단계를 수행하십시오.

1. **strmqikm** 명령을 사용하여 GUI를 시작하십시오.
2. 키 데이터베이스 파일 메뉴에서 열기를 클릭하십시오. 열기 창이 열립니다.
3. 키 데이터베이스 유형을 클릭하고 **CMS**(인증서 관리 시스템)를 선택하십시오.

4. 키 데이터베이스 파일이 있는 디렉토리로 이동하려면 **찾아보기**를 클릭하십시오.
5. 추출하려는 키 데이터베이스 파일을 선택하십시오(예: key.kdb).
6. **열기**를 클릭하십시오. 비밀번호 프롬프트 창이 열립니다.
7. 키 데이터베이스를 작성할 때 설정한 비밀번호를 입력하고 **확인**을 클릭하십시오. 키 데이터베이스 파일의 이름이 **파일 이름** 필드에 표시됩니다.
8. 키 데이터베이스 콘텐츠 필드에서 **서명자 인증서**를 선택하고 추출하려는 인증서를 선택하십시오.
9. **추출**을 클릭하십시오. 파일에 인증서 추출 창이 열립니다.
10. 인증서의 **데이터 유형**을 선택하십시오. 예를 들어, .arm 확장자가 있는 파일의 경우 **Base64 인코딩된 ASCII 데이터**입니다.
11. 인증서를 저장하려는 인증서 파일 이름 및 위치를 입력하거나 **찾아보기**를 클릭하여 이름과 위치를 선택하십시오.
12. **확인**을 클릭하십시오. 인증서가 사용자가 지정한 파일에 쓰여집니다.

명령행 사용

다음 명령을 사용하여 **runmqckm**를 사용하여 CA 인증서를 추출하십시오.

- UNIX, Linux, and Windows의 경우:

```
runmqckm -cert -extract -db filename -pw password -label label -target filename
          -format ascii
```

설명:

-db <i>filename</i>	CMS 키 데이터베이스의 완전한 경로 이름입니다.
-pw <i>password</i>	CMS 키 데이터베이스의 비밀번호입니다.
-label <i>label</i>	인증서에 첨부된 레이블입니다.
-target <i>filename</i>	대상 파일의 이름입니다.
-format <i>ascii</i>	인증서의 형식입니다. 값은 Base64-encoded ASCII의 경우 <i>ascii</i> 또는 2진 DER 데이터의 경우 <i>binary</i> 일 수 있습니다. 기본값은 <i>ascii</i> 입니다.
-fips	명령이 FIPS 모드에서 실행되도록 지정합니다. FIPS 모드에서 ICC 컴포넌트는 FIPS 140-2 유효성 검증된 알고리즘을 사용합니다. ICC 컴포넌트가 FIPS 모드에서 초기화되지 않는 경우에는 runmqakm 명령이 실패합니다.

UNIX, Linux, and Windows에서 키 저장소로부터 자체 서명 인증서의 공용 부분 추출

자체 서명 인증서의 공용 부분을 추출하려면 이 프로시저를 따르십시오.

strmqikm 사용

FIPS를 준수하는 방법으로 TLS 인증서를 관리해야 하는 경우, **runmqakm** 명령을 사용하십시오. **strmqikm**(iKeyman)에서는 FIPS 준수 옵션을 제공하지 않습니다.

자체 서명 인증서의 공용 부분을 추출하려는 시스템에서 다음 단계를 수행하십시오.

1. **strmqikm** 명령을 사용하여 GUI를 시작하십시오(UNIX, Linux, and Windows에서).
2. 키 데이터베이스 파일 메뉴에서 **열기**를 클릭하십시오. 열기 창이 열립니다.
3. 키 데이터베이스 유형을 클릭하고 **CMS**(인증서 관리 시스템)를 선택하십시오.
4. 키 데이터베이스 파일이 있는 디렉토리로 이동하려면 **찾아보기**를 클릭하십시오.
5. 예를 들어, key.kdb와 같이 인증서를 추출하려는 키 데이터베이스 파일을 선택하십시오.
6. **확인**을 클릭하십시오. 비밀번호 프롬프트 창이 열립니다.

7. 키 데이터베이스를 작성할 때 설정한 비밀번호를 입력하고 **확인**을 클릭하십시오. 키 데이터베이스 파일의 이름이 **파일 이름** 필드에 표시됩니다.
8. 키 데이터베이스 **컨텐츠** 필드에서 **개인 인증서**를 선택한 후 인증서를 선택하십시오.
9. **인증서 추출**을 클릭하십시오. 파일에 인증서 추출 창이 열립니다.
10. 인증서의 **데이터 유형**을 선택하십시오. 예를 들어, .arm 확장자가 있는 파일의 경우 **Base64 인코딩된 ASCII 데이터**입니다.
11. 인증서를 저장하려는 인증서 파일 이름 및 위치를 입력하거나 **찾아보기**를 클릭하여 이름과 위치를 선택하십시오.
12. **확인**을 클릭하십시오. 인증서가 사용자가 지정한 파일에 쓰여집니다. 인증서를 추출(내보내기가 아니라)할 때는 인증서의 공용 부분만 포함되므로 비밀번호가 필요하지 않습니다.

명령행 사용

다음 명령에서 **runmqckm** 또는 **runmqakm**을 사용하여 자체 서명 인증서의 공용 부분을 추출하려면 다음 명령을 사용하십시오.

- UNIX, Linux, and Windows의 경우:

```
runmqckm -cert -extract -db filename -pw password -label label -target filename
        -format ascii
```

- runmqakm 사용:

```
runmqakm -cert -extract -db filename -pw password -label label
        -target filename -format ascii -fips
```

설명:

-db <i>filename</i>	CMS 키 데이터베이스의 완전한 경로 이름입니다.
-pw <i>password</i>	CMS 키 데이터베이스의 비밀번호입니다.
-label <i>label</i>	인증서에 첨부된 레이블입니다.
-target <i>filename</i>	대상 파일의 이름입니다.
-format <i>ascii</i>	인증서의 형식입니다. 값은 Base64-encoded ASCII의 경우 <i>ascii</i> 또는 2진 DER 데이터의 경우 <i>binary</i> 일 수 있습니다. 기본값은 <i>ascii</i> 입니다.
-fips	명령이 FIPS 모드에서 실행되도록 지정합니다. FIPS 모드에서 ICC 컴포넌트는 FIPS 140-2 유효성 검증된 알고리즘을 사용합니다. ICC 컴포넌트가 FIPS 모드에서 초기화되지 않는 경우에는 runmqakm 명령이 실패합니다.

UNIX, Linux, and Windows에서 CA 인증서 또는 자체 서명 인증서의 공용 부분을 키 저장소에 추가

CA 인증서 또는 자체 서명 인증서의 공용 부분을 키 저장소에 추가하려면 이 프로시저를 따르십시오.

추가하려는 인증서가 인증서 체인에 있는 경우 체인에서 위에 있는 모든 인증서 또한 추가해야 합니다. 인증서를 루트에서 시작하여 체인에서 바로 아래에 있는 CA 인증서가 뒤따르는 방식으로 내림차순으로 엄격하게 추가해야 합니다.

여기서 다음 지시사항은 CA 인증서를 가리키고, 이들은 또한 자체 서명 인증서의 공용 부분에도 적용됩니다.

참고: 인증서가 ASCII(UTF-8) 또는 2진(DER) 인코딩인지 확인해야 합니다. IBM Global Secure Toolkit(GSKit)는 다른 유형의 인코딩이 있는 인증서를 지원하지 않기 때문입니다.

strmqikm 사용

FIPS를 준수하는 방법으로 TLS 인증서를 관리해야 하는 경우, **runmqakm** 명령을 사용하십시오. **strmqikm**에서는 FIPS 준수 옵션을 제공하지 않습니다.

CA 인증서를 추가하고 싶은 시스템에서 다음 단계를 수행하십시오.

1. **strmqikm** 명령(UNIX, Linux 및 Windows 시스템에서)을 사용하여 GUI를 시작하십시오.
2. 키 데이터베이스 파일 메뉴에서 열기를 클릭하십시오. 열기 창이 열립니다.
3. 키 데이터베이스 유형을 클릭하고 **CMS**(인증서 관리 시스템)를 선택하십시오.
4. 키 데이터베이스 파일이 있는 디렉토리로 이동하려면 **찾아보기**를 클릭하십시오.
5. 인증서를 추가할 키 데이터베이스 파일을 선택하십시오(예: key.kdb).
6. **확인**을 클릭하십시오. 비밀번호 프롬프트 창이 열립니다.
7. 키 데이터베이스를 작성할 때 설정한 비밀번호를 입력하고 **확인**을 클릭하십시오. 키 데이터베이스 파일의 이름이 **파일 이름** 필드에 표시됩니다.
8. 키 데이터베이스 콘텐츠 필드에서 **서명자 인증서**를 선택하십시오.
9. **추가**를 클릭하십시오. 파일에서 CA 인증 추가 창이 열립니다.
10. 인증서가 저장된 인증서 파일 이름 및 위치를 입력하거나 **찾아보기**를 클릭하여 이름 및 위치를 선택하십시오.
11. **확인**을 클릭하십시오. 레이블 입력 창이 열립니다.
12. 레이블 입력 창에서 인증서 이름을 입력하십시오.
13. **확인**을 클릭하십시오. 인증서가 키 데이터베이스에 추가됩니다.

명령행 사용

CA 인증서를 키 데이터베이스에 추가하려면 다음 명령 중 하나를 사용하십시오.

- **runmqckm** 사용:

```
runmqckm -cert -add -db filename -pw password -label label  
-file filename -format ascii
```

- **runmqakm** 사용:

```
runmqakm -cert -add -db filename -pw password -label label  
-file filename -format ascii -fips
```

설명:

-db filename

CMS 키 데이터베이스의 완전한 파일 이름을 지정합니다.

-pw password

CMS 키 데이터베이스의 비밀번호를 지정합니다.

-label label

인증서에 첨부되는 레이블을 지정합니다.

-file filename

인증서를 포함하는 파일의 이름을 지정합니다.

-format ascii

인증서의 형식을 지정합니다. 값은 Base64-encoded ASCII의 경우 **ascii** 또는 2진 DER 데이터의 경우 **binary**일 수 있습니다. 기본값은 **ascii**입니다.

-fips

명령이 FIPS 모드에서 실행되도록 지정합니다. FIPS 모드에서 ICC 컴포넌트는 FIPS 140-2 유효성 검증된 알고리즘을 사용합니다. ICC 컴포넌트가 FIPS 모드에서 초기화되지 않는 경우에는 **runmqakm** 명령이 실패합니다.

UNIX, Linux, and Windows에서 키 저장소로부터 개인 인증서 내보내기

개인 인증서를 내보내려면 이 프로시저를 따르십시오.

strmqikm 사용

FIPS를 준수하는 방법으로 TLS 인증서를 관리해야 하는 경우, **runmqakm** 명령을 사용하십시오. **strmqikm**(iKeyman)에서는 FIPS 준수 옵션을 제공하지 않습니다.

개인 인증서를 내보내려는 시스템에서 다음 단계를 수행하십시오.

1. **strmqikm** 명령을 사용하여 GUI를 시작하십시오(Windows UNIX and Linux에서).
2. 키 데이터베이스 파일 메뉴에서 열기를 클릭하십시오. 열기 창이 열립니다.
3. 키 데이터베이스 유형을 클릭하고 **CMS**(인증서 관리 시스템)를 선택하십시오.
4. 키 데이터베이스 파일이 있는 디렉토리로 이동하려면 **찾아보기**를 클릭하십시오.
5. 인증서를 내보내려는 키 데이터베이스 파일을 선택하십시오(예: key.kdb).
6. 열기를 클릭하십시오. 비밀번호 프롬프트 창이 열립니다.
7. 키 데이터베이스를 작성할 때 설정한 비밀번호를 입력하고 **확인**을 클릭하십시오. 키 데이터베이스 파일의 이름이 **파일 이름** 필드에 표시됩니다.
8. 키 데이터베이스 콘텐츠 필드에서 **개인 인증서**를 선택하고 내보내려는 인증서를 선택하십시오.
9. **내보내기/가져오기**를 클릭하십시오. 키 내보내기/가져오기 창이 열립니다.
10. 키 내보내기를 선택하십시오.
11. 내보내려는 인증서의 **키 파일 유형**을 선택하십시오(예: **PKCS12**).
12. 인증서를 내보내려는 파일 이름 및 위치를 입력하거나 **찾아보기**를 클릭하여 이름과 위치를 선택하십시오.
13. **확인**을 클릭하십시오. 비밀번호 프롬프트 창이 열립니다. 인증서를 내보낼 때(추출이 아니라) 인증서의 공용 및 개인용 부분 모두가 포함된다는 점을 유의하십시오. 내보낸 파일이 비밀번호로 보호되기 때문입니다. 인증서를 추출할 때 인증서의 공용 부분만이 포함되므로 비밀번호는 필요하지 않습니다.
14. **비밀번호** 필드에 비밀번호를 입력하고 **비밀번호 확인** 필드에 다시 입력하십시오.
15. **확인**을 클릭하십시오. 인증서는 지정한 파일로 내보내기됩니다.

명령행 사용


다음 명령을 사용하여 **runmqckm**를 사용하여 개인 인증서를 내보내십시오.

- UNIX, Linux, and Windows의 경우:

```
runmqckm -cert -export -db filename -pw password -label label -type cms  
-target filename -target_pw password -target_type pkcs12
```

설명:

-db <i>filename</i>	CMS 키 데이터베이스의 완전한 경로 이름입니다.
-fips	명령이 FIPS 모드에서 실행되도록 지정합니다. FIPS 모드에서 ICC 컴포넌트는 FIPS 140-2 유효성 검증된 알고리즘을 사용합니다. ICC 컴포넌트가 FIPS 모드에서 초기화되지 않는 경우에는 runmqakm 명령이 실패합니다.
-pw <i>password</i>	CMS 키 데이터베이스의 비밀번호입니다.
-label <i>label</i>	인증서에 첨부된 레이블입니다.
-type <i>cms</i>	데이터베이스의 유형입니다.
-target <i>filename</i>	대상 파일의 완전한 경로 이름입니다.
-target_pw <i>password</i>	인증서를 암호화하기 위한 비밀번호입니다.
-target_type <i>pkcs12</i>	인증서의 유형입니다.

 **UNIX, Linux, and Windows**에서 개인 인증서를 키 저장소로 가져오기
개인 인증서를 가져오려면 이 프로시저를 따르십시오.

PKCS #12 형식으로 된 개인 인증서를 키 데이터베이스 파일로 가져오기 전에 CA 인증서 발행의 전체 유효 체인을 키 데이터베이스 파일에 추가해야 합니다(272 페이지의 『UNIX, Linux, and Windows에서 CA 인증서 또는 자체 서명 인증서의 공용 부분을 키 저장소에 추가』 내용 참조).

PKCS #12 파일은 임시로 간주되어야 하고 사용 후에 삭제되어야 합니다.

strmqikm 사용

FIPS를 준수하는 방법으로 TLS 인증서를 관리해야 하는 경우, `runmqakm` 명령을 사용하십시오. `strmqikm`에서는 FIPS 준수 옵션을 제공하지 않습니다.

개인 인증서를 가져오려는 시스템에서 다음 단계를 수행하십시오.

1. `strmqikm` 명령을 사용하여 GUI를 시작하십시오.
2. 키 데이터베이스 파일 메뉴에서 열기를 클릭하십시오. 열기 창이 표시됩니다.
3. 키 데이터베이스 유형을 클릭하고 **CMS**(인증서 관리 시스템)를 선택하십시오.
4. 키 데이터베이스 파일이 있는 디렉토리로 이동하려면 **찾아보기**를 클릭하십시오.
5. 인증서를 추가할 키 데이터베이스 파일을 선택하십시오(예: `key.kdb`).
6. 열기를 클릭하십시오. 비밀번호 프롬프트 창이 표시됩니다.
7. 키 데이터베이스를 작성할 때 설정한 비밀번호를 입력하고 **확인**을 클릭하십시오. 키 데이터베이스 파일의 이름이 **파일 이름** 필드에 표시됩니다.
8. 키 데이터베이스 콘텐츠 필드에서 **개인 인증서**를 선택하십시오.
9. 개인 인증서 보기에 인증서가 있는 경우 다음 단계를 따르십시오.
 - a. **내보내기/가져오기**를 클릭하십시오. 키 내보내기/가져오기 창이 표시됩니다.
 - b. **키 가져오기**를 선택하십시오.
10. 개인 인증서 보기에 인증서가 없는 경우 **가져오기**를 클릭하십시오.
11. 가져오려는 인증서의 **키 파일 유형**을 선택하십시오(예: PKCS12).
12. 인증서가 저장된 인증서 파일 이름 및 위치를 입력하거나 **찾아보기**를 클릭하여 이름 및 위치를 선택하십시오.
13. **확인**을 클릭하십시오. 비밀번호 프롬프트 창이 표시됩니다.
14. **비밀번호** 필드에 인증서가 내보내기되었을 때 사용된 비밀번호를 입력하십시오.
15. **확인**을 클릭하십시오. 레이블 변경 창이 표시됩니다. 예를 들어 같은 레이블이 있는 인증서가 대상 키 데이터베이스에 존재하는 경우 가져오기 중인 인증서의 레이블을 변경할 수 있습니다. 인증서 레이블 변경은 인증서 체인 유효성 검증에 영향을 미치지 않습니다. 인증서를 특정 큐 관리자 또는 IBM MQ MQI client와 연관시키려면 IBM MQ는 **CERTLABL** 속성의 값(설정된 경우) 또는 큐 관리자의 이름을 사용하는 기본 `ibmwebspheremq` 또는 추가된 IBM MQ MQI client 사용자 로그인 ID(모두 소문자)를 사용합니다. 자세한 내용은 [디지털 인증서 레이블](#)을 참조하십시오.
16. 레이블을 변경하려면 **변경할 레이블 선택** 목록에서 필수 레이블을 선택하십시오. 레이블이 **새 레이블 입력** 입력 항목 필드로 복사됩니다. 레이블 텍스트를 새 레이블의 레이블 텍스트로 바꾸고 **적용**을 클릭하십시오.
17. **새 레이블 입력** 입력 항목 필드의 텍스트가 다시 **변경할 레이블 선택** 필드로 복사되어 원래 선택된 레이블을 대체하고 해당하는 인증서를 다시 레이블 지정합니다.
18. 변경해야 하는 모든 레이블을 변경한 후에는 **확인**을 클릭하십시오. 레이블 변경 창이 닫히고, 원래 IBM 키 관리 창이 **개인 인증서 및 서명자 인증서** 필드가 올바르게 레이블된 인증서로 업데이트된 상태로 다시 나타납니다.
19. 인증서가 대상 키 데이터베이스로 가져오기됩니다.

명령행 사용

`runmqckm`을 사용하여 개인 인증서를 가져오려면 다음 명령을 사용하십시오.

- UNIX, Linux, and Windows의 경우:

```
runmqckm -cert -import -file filename -pw password -type pkcs12 -target filename
-target_pw password -target_type cms -label label
```

설명:

- file *filename* PKCS #12 인증서를 포함하는 파일의 완전한 파일 이름입니다.
- pw *password* PKCS #12 인증서의 비밀번호입니다.
- type *pkcs12* 파일의 유형입니다.
- target *filename* 대상 CMS 키 데이터베이스의 이름입니다.
- target_pw *password* CMS 키 데이터베이스의 비밀번호입니다.
- target_type *cms* -target에 의해 지정된 데이터베이스의 유형입니다.
- label *label* 소스 키 데이터베이스로부터 가져오려는 인증서의 레이블입니다.
- new_label *label* 대상 데이터베이스에서 인증서에 지정될 레이블입니다. -new_label 옵션을 생략하면 기본값은 -label 옵션과 같은 옵션을 사용합니다.
- fips 명령이 FIPS 모드에서 실행되도록 지정합니다. FIPS 모드에서 ICC 컴포넌트는 FIPS 140-2 유효성 검증된 알고리즘을 사용합니다. ICC 컴포넌트가 FIPS 모드에서 초기화되지 않는 경우에는 **runmqakm** 명령이 실패합니다.

runmqckm에서는 인증서 레이블을 직접 변경하는 명령을 제공하지 않습니다. 인증서 레이블을 변경하려면 다음 단계를 사용하십시오.

1. **-cert -export** 명령을 사용하여 인증서를 PKCS #12 파일에 내보내십시오. -label 옵션의 기존 인증서 레이블을 지정하십시오.
2. **-cert -delete** 명령을 사용하여 원래 키 데이터베이스에서 인증서의 기존 사본을 제거하십시오.
3. **-cert -import** 명령을 사용하여 PKCS #12 파일에서 인증서를 가져오십시오. -label 옵션의 이전 레이블을 지정하고 -new_label 옵션에 필수 새 레이블을 지정하십시오. 인증서가 필수 레이블과 함께 키 데이터베이스로 다시 가져오기됩니다.

Microsoft.pfx 파일에서 개인 인증서 가져오기

UNIX, Linux, and Windows의 Microsoft.pfx 파일에서 가져오려면 이 프로시저를 따르십시오.

.pfx 파일은 동일 키와 관련된 두 개의 인증서를 포함할 수 있습니다. 하나는 개인 또는 사이트 인증서(공용 및 개인용 키 모두 포함)입니다. 다른 하나는 CA(서명자) 인증서(공용 키만을 포함)입니다. 이러한 인증서는 동일한 CMS 키 데이터베이스 파일에 공존할 수 없으므로 이들 중 하나만을 가져올 수 있습니다. 또한 "친근한 이름" 또는 레이블은 서명자 인증서에만 첨부됩니다.

개인 인증서는 시스템 생성 UID(Unique User Identifier)에 의해서 식별됩니다. 이 섹션은 이전에 CA(서명자) 인증서에 지정한 친근한 이름으로 레이블을 지정하는 동안 pfx 파일에서 개인 인증서를 가져오기를 보여줍니다. 발행 CA(서명자) 인증서는 이미 대상 키 데이터베이스에 추가되어야 합니다. PKCS#12 파일은 임시적인 것으로 간주되고 사용 후 삭제되어야 합니다.

소스 pfx 키 데이터베이스에서 개인 인증서를 가져오려면 다음 단계를 수행하십시오.

1. **strmqikm** 명령을 사용하여 GUI를 시작하십시오. IBM 키 관리 창이 표시됩니다.
2. 키 데이터베이스 파일 메뉴에서 열기를 클릭하십시오. 열기 창이 표시됩니다.
3. 키 데이터베이스 유형 **PKCS12**를 선택하십시오.
4. 이 단계를 수행하기 전에 pfx 데이터베이스를 백업하는 것이 좋습니다. 가져오려는 pfx 키 데이터베이스를 선택하십시오. 열기를 클릭하십시오. 비밀번호 프롬프트 창이 표시됩니다.
5. 키 데이터베이스 비밀번호를 입력하고 확인을 클릭하십시오. IBM 키 관리 창이 표시됩니다. 제목 표시줄은 선택된 pfx 키 데이터베이스 파일의 이름을 보여주고 파일이 열려 있고 준비되어 있음을 나타냅니다.

6. 목록에서 **서명자 인증서**를 선택하십시오. 필수 인증서의 "최근한 이름"이 서명자 인증서 패널에 레이블로서 표시됩니다.
7. 레이블 항목을 선택하고 **삭제**를 클릭하여 서명자 인증서를 제거하십시오. 확인 창이 표시됩니다.
8. **예**를 클릭하십시오. 선택한 레이블이 더 이상 서명자 인증서 패널에 표시되지 않습니다.
9. 모든 서명자 인증서에 대해 6, 7 및 8 단계를 반복하십시오.
10. **키 데이터베이스 파일** 메뉴에서 **열기**를 클릭하십시오. 열기 창이 표시됩니다.
11. pfx 파일이 가져오기되고 있는 대상 키 CMS 데이터베이스를 선택하십시오. **열기**를 클릭하십시오. 비밀번호 프롬프트 창이 표시됩니다.
12. 키 데이터베이스 비밀번호를 입력하고 **확인**을 클릭하십시오. IBM 키 관리 창이 표시됩니다. 제목 표시줄은 선택한 키 데이터베이스 파일의 이름을 표시하여 파일이 열려 있고 준비가 되었음을 나타냅니다.
13. 목록에서 **개인 인증서**를 선택하십시오.
14. 개인 인증서 보기에 인증서가 있는 경우 다음 단계를 따르십시오.
 - a. **키 가져오기/내보내기**를 클릭하십시오. 키 내보내기/가져오기 창이 표시됩니다.
 - b. 조치 유형 선택에서 **가져오기**를 선택하십시오.
15. 개인 인증서 보기에 인증서가 없는 경우 **가져오기**를 클릭하십시오.
16. PKCS12 파일을 선택하십시오.
17. 4단계에서 사용된 pfx 파일의 이름을 입력하십시오. **확인**을 클릭하십시오. 비밀번호 프롬프트 창이 표시됩니다.
18. 서명자 인증서를 삭제할 때 지정한 것과 같은 비밀번호를 지정하십시오. **확인**을 클릭하십시오.
19. 레이블 변경 창이 표시됩니다(가져오기에는 단 하나의 인증서만이 사용 가능해야 하므로). 인증서의 레이블은 xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx 형식인 UUID여야 합니다.
20. 레이블을 변경하려면 **변경할 레이블 선택** 패널에서 UUID를 선택하십시오. 레이블이 **새 레이블 입력**: 필드로 복제됩니다. 레이블 텍스트를 7단계에서 삭제된 친숙한 이름의 레이블 텍스트로 바꾸고 **적용**을 클릭하십시오. 친숙한 이름은 IBM MQ **CERTLABL** 속성의 값 (설정된 경우) 또는 큐 관리자의 이름이 있는 기본 **ibmwebspheremq** 또는 추가된 IBM MQ MQI client 사용자 로그인 ID (모두 소문자) 여야 합니다. 자세한 내용은 [디지털 인증서 레이블](#)을 참조하십시오.
21. **확인**을 클릭하십시오. 레이블 변경 창이 제거되고 원래 IBM 키 관리 창이 올바르게 레이블된 개인 인증서로 업데이트된 상태로 개인 인증서 및 서명자 인증서 패널과 함께 다시 나타납니다.
22. pfx 개인 인증서가 이제 (대상)데이터베이스로 가져오기됩니다.

runmqckm 또는 **runmqakm**을 사용하여 인증서 레이블을 변경할 수 없습니다.

명령행 사용

UNIX, Linux, and Windows에서 **runmqckm** 를 사용하여 개인 인증서를 가져오려면 다음 명령을 사용하십시오.

```
runmqckm -cert -import -file filename -pw password -type pkcs12 -target filename
-target_pw password -target_type cms -label label -pfx
```

runmqakm을 사용하여 개인 인증서를 가져오려면 다음 명령을 사용하십시오.

```
runmqakm -cert -import -file filename -pw password -type pkcs12 -target filename
-target_pw password -target_type cms -label label -fips -pfx
```

설명:

- | | |
|-------------------------|--------------------------------------|
| -file <i>filename</i> | PKCS #12 인증서를 포함하는 파일의 완전한 파일 이름입니다. |
| -pw <i>password</i> | PKCS #12 인증서의 비밀번호입니다. |
| -type <i>pkcs12</i> | 파일의 유형입니다. |
| -target <i>filename</i> | 대상 CMS 키 데이터베이스의 이름입니다. |

-target_pw password	CMS 키 데이터베이스의 비밀번호입니다.
-target_type cms	-target에 의해 지정된 데이터베이스의 유형입니다.
-label label	소스 키 데이터베이스로부터 가져오려는 인증서의 레이블입니다.
-new_label label	대상 데이터베이스에서 인증서에 지정될 레이블입니다. -new_label 옵션을 생략하면 기본값은 -label 옵션과 같은 옵션을 사용합니다.
-fips	명령이 FIPS 모드에서 실행되도록 지정합니다. FIPS 모드에서 ICC 컴포넌트는 FIPS 140-2 유효성 검증된 알고리즘을 사용합니다. ICC 컴포넌트가 FIPS 모드에서 초기화되지 않는 경우에는 runmqakm 명령이 실패합니다.
-pfx	PFX 파일 형식을 나타냅니다.

runmqckm에서는 인증서 레이블을 직접 변경하는 명령을 제공하지 않습니다. 인증서 레이블을 변경하려면 다음 단계를 사용하십시오.

1. **-cert -export** 명령을 사용하여 인증서를 PKCS #12 파일에 내보내십시오. -label 옵션의 기존 인증서 레이블을 지정하십시오.
2. **-cert -delete** 명령을 사용하여 원래 키 데이터베이스에서 인증서의 기존 사본을 제거하십시오.
3. **-cert -import** 명령을 사용하여 PKCS #12 파일에서 인증서를 가져오십시오. -label 옵션의 이전 레이블을 지정하고 -new_label 옵션에 필수 새 레이블을 지정하십시오. 인증서가 필수 레이블과 함께 키 데이터베이스로 다시 가져오기됩니다.

PKCS #7 파일로부터 개인 인증서 가져오기

strmqikm(iKeyman) 및 **runmqckm**(iKeycmd) 도구에서는 PKCS #7(.p7b) 파일을 지원하지 않습니다. **runmqckm** 도구를 사용하여 UNIX, Linux, and Windows의 PKCS #7에서 인증서를 가져오십시오.

CA 인증서를 PKCS #7 파일로부터 추가하려면 다음 명령을 사용하십시오.

```
runmqckm -cert -add -db filename -pw password -type cms -file filename
-label label
```

-db filename	CMS 키 데이터베이스의 완전한 파일 이름입니다.
-pw password	키 데이터베이스의 비밀번호입니다.
-type cms	키 데이터베이스의 유형입니다.
-file filename	PKCS #7 파일의 이름입니다.
-label label	대상 데이터베이스에서 인증서에 지정된 레이블입니다. 첫 번째 인증서는 제공된 레이블을 받습니다. 있는 경우, 다른 모든 인증서에는 제목 이름이 레이블 지정됩니다.

개인 인증서를 PKCS #7 파일에서 가져오려면 다음 명령을 사용하십시오.

```
runmqckm -cert -import -db filename -pw password -type pkcs7 -target filename
-target_pw password -target_type cms -label label -new_label label
```

-db filename	PKCS #7 인증서를 포함하는 파일의 완전한 파일 이름입니다.
-pw password	PKCS #7 인증서의 비밀번호입니다.
-type pkcs7	파일의 유형입니다.
-target filename	목적지 키 데이터베이스의 이름입니다.
-target_pw password	목적지 키 데이터베이스의 비밀번호입니다.
-target_type cms	-target에 의해 지정된 데이터베이스의 유형입니다.
-label label	가져오려는 인증서의 레이블입니다.

-new_label *label*

대상 데이터베이스에서 인증서에 지정될 레이블입니다. -new_label 옵션을 생략하면 사용할 기본값은 -label 옵션과 같습니다.

ULW UNIX, Linux, and Windows에서 키 저장소로부터 인증서 삭제

개인 또는 CA 인증서를 제거하려면 이 프로시저를 사용하십시오.

strmqikm 사용

FIPS를 준수하는 방법으로 TLS 인증서를 관리해야 하는 경우, **runmqakm** 명령을 사용하십시오. **strmqikm**(iKeyman)에서는 FIPS 준수 옵션을 제공하지 않습니다.

1. **strmqikm** 명령을 사용하여 GUI를 시작하십시오(UNIX, Linux, and Windows에서).
2. 키 데이터베이스 파일 메뉴에서 열기를 클릭하십시오. 열기 창이 열립니다.
3. 키 데이터베이스 유형을 클릭하고 **CMS**(인증서 관리 시스템)를 선택하십시오.
4. 키 데이터베이스 파일이 있는 디렉토리로 이동하려면 **찾아보기**를 클릭하십시오.
5. 예를 들어, key.kdb와 같이 인증서를 삭제하려는 키 데이터베이스 파일을 선택하십시오.
6. 열기를 클릭하십시오. 비밀번호 프롬프트 창이 열립니다.
7. 키 데이터베이스를 작성할 때 설정한 비밀번호를 입력하고 **확인**을 클릭하십시오. 키 데이터베이스 파일의 이름이 **파일 이름** 필드에 표시됩니다.
8. 드롭 다운 목록에서 **개인 인증서** 또는 **서명자 인증서**를 선택하십시오.
9. 삭제하려는 인증서를 선택하십시오.
10. 인증서의 사본을 이미 가지고 있지 않고 이를 저장하고 싶으면 **내보내기/가져오기**를 클릭하고 이를 내보내십시오(273 페이지의 『UNIX, Linux, and Windows에서 키 저장소로부터 개인 인증서 내보내기』 참조).
11. 인증서를 선택한 상태에서 **삭제**를 클릭하십시오. 확인 창이 열립니다.
12. 예를 클릭하십시오. **개인 인증서** 필드가 더 이상 사용자가 삭제한 인증서의 레이블을 보여주지 않습니다.

명령행 사용

runmqckm를 사용하여 인증서를 삭제하려면 다음 명령을 사용하십시오.

- UNIX, Linux, and Windows의 경우:

```
runmqckm -cert -delete -db filename -pw password -label label
```

설명:

-db <i>filename</i>	CMS 키 데이터베이스의 완전한 파일 이름입니다.
-pw <i>password</i>	CMS 키 데이터베이스의 비밀번호입니다.
-label <i>label</i>	개인 인증서에 첨부된 레이블입니다.
-fips	명령이 FIPS 모드에서 실행되도록 지정합니다. FIPS 모드에서 ICC 컴포넌트는 FIPS 140-2 유효성 검증된 알고리즘을 사용합니다. ICC 컴포넌트가 FIPS 모드에서 초기화되지 않는 경우에는 runmqakm 명령이 실패합니다.

ULW UNIX, Linux, and Windows에서 키 저장소 보호를 위한 강력한 비밀번호 생성

runmqakm(GSKCapiCmd) 명령을 사용하여 키 저장소 보호를 위해 강력한 비밀번호를 생성할 수 있습니다.

강력한 비밀번호를 생성하기 위해 다음 매개변수와 함께 **runmqakm** 명령을 사용할 수 있습니다.

```
runmqakm -random -create -length 14 -strong -fips
```


후속 인증서 관리 명령의 **-pw** 매개변수에서 생성된 비밀번호를 사용할 때 항상 비밀번호 주변에 큰따옴표를 두십시오. UNIX and Linux 시스템에서 다음 문자가 비밀번호 문자열에 나타나는 경우 백슬래시 문자를 사용하여 이스케이프 처리해야 합니다.

! \ " ' ,

runmqckm, **runmqakm** 또는 **strmqikm** GUI로부터의 프롬프트에 대한 응답에 비밀번호를 입력할 때는 비밀번호를 따옴표로 묶거나 이스케이프 처리할 필요가 없습니다. 운영 체제 셸이 이러한 경우 데이터 입력 항목에 영향을 주지 않기 때문에 이는 필요하지 않습니다.

ULW UNIX, Linux, and Windows에서 암호화 하드웨어 구성

큐 관리자 또는 클라이언트의 암호화 하드웨어를 여러 방법으로 구성할 수 있습니다.

다음 방법 중 하나를 사용하여 UNIX, Linux, and Windows에서 큐 관리자에 대한 암호화 하드웨어를 구성할 수 있습니다.

- [ALTER QMGR](#)에 설명된 대로 **SSLCRYP** 매개변수와 함께 **ALTER QMGR MQSC** 명령을 사용하십시오.
- IBM MQ 탐색기를 사용하여 UNIX, Linux 또는 Windows 시스템에서 암호화 하드웨어를 구성하십시오. 자세한 정보는 온라인 도움말을 참조하십시오.

다음 방법 중 하나를 사용하여 UNIX, Linux, and Windows 에서 IBM MQ 클라이언트에 대한 암호화 하드웨어를 구성할 수 있습니다.

- **MQSSLCRYP** 환경 변수를 설정하십시오. **MQSSLCRYP**에 허용되는 값은 [ALTER QMGR](#)에 설명된 대로 **SSLCRYP** 매개변수에서와 같습니다.

SSLCRYP 매개변수의 **GSK_PKCS11** 버전을 사용하는 경우 **PKCS #11** 토큰 레이블은 하드웨어를 구성한 레이블과 일치해야 합니다.

- **MQCONN** 호출에서 **SSL** 구성 옵션 구조의 **CryptoHardware** 필드, **MQSCO**를 설정하십시오. 자세한 정보는 **MQSCO**의 개요를 참조하십시오.

이러한 방법을 사용하여 **PKCS #11** 인터페이스를 사용하는 암호화 하드웨어를 구성한 경우에는 사용자가 구성한 암호화 토큰의 키 데이터베이스 파일에 채널에 사용할 개인 인증서를 저장해야 합니다. 이 프로그램은 [280 페이지](#)의 『**PKCS #11 하드웨어에서 인증서 관리**』에서 설명합니다.

ULW PKCS #11 하드웨어에서 인증서 관리

PKCS #11 인터페이스를 지원하는 암호화 하드웨어에서 디지털 인증서를 관리할 수 있습니다.

이 태스크 정보

인증 기관(CA) 인증서를 저장할 의도가 없더라도 IBM MQ 환경을 준비하기 위해 키 데이터베이스를 작성해야 하고 모든 인증서를 암호화 하드웨어에 저장합니다. 키 데이터베이스는 **SSLKEYR** 필드에서 참조하기 위해 큐 관리자에 필요하거나 클라이언트 애플리케이션이 **MQSSLKEYR** 환경 변수에서 참조하기 위해 필요합니다. 이 키 데이터베이스는 또한 인증서 요청을 작성 중인 경우에 필수입니다.

명령행을 사용하거나 **strmqikm** (iKeyman) 사용자 인터페이스를 사용하여 키 데이터베이스를 작성합니다.

프로시저

명령행을 사용하여 키 데이터베이스를 작성한다.

1. 다음 명령 중 하나를 실행하십시오.

- **runmqckm** 사용:

```
runmqckm -keydb -create -db filename -pw password -type cms -stash
```

• **runmqakm** 사용:

```
runmqakm -keydb -create -db filename -pw password -type cms  
-stash -fips -strong
```

설명:

-db filename

CMS 키 데이터베이스의 완전한 파일 이름을 지정하고 .kdb의 파일 확장자가 있어야 합니다.

-pw password

CMS 키 데이터베이스의 비밀번호를 지정합니다.

-type cms

데이터베이스의 유형을 지정합니다. (IBM MQ의 경우 cms여야 합니다.)

-stash

키 데이터베이스 비밀번호를 파일에 저장합니다.

-fips

명령이 FIPS 모드에서 실행되도록 지정합니다. FIPS 모드에서는 ICC 컴포넌트는 FIPS 140-2 유효성 검증된 알고리즘을 사용합니다. ICC 컴포넌트가 FIPS 모드에서 초기화되지 않는 경우에는 **runmqakm** 명령이 실패합니다.

-strong

입력한 비밀번호가 비밀번호 강도에 대한 최소 요구사항을 충족하는지 검사합니다. 비밀번호의 최소 요구사항은 다음과 같습니다.

- 비밀번호는 최소 14자여야 합니다.
- 비밀번호에는 최소 하나의 소문자, 하나의 대문자 및 하나의 숫자 또는 특수 문자를 포함해야 합니다. 특수 문자에는 별표(*), 달러 부호(\$), 숫자 부호(#) 및 퍼센트 부호(%)가 포함됩니다. 공백은 특수 문자로 분류됩니다.
- 각 문자는 비밀번호에서 최대 3회 사용될 수 있습니다.
- 비밀번호에서 최대 두 개의 연속하는 문자가 동일할 수 있습니다.
- 모든 문자는 0x20 - 0x7E 범위 내의 표준 ASCII 인쇄 가능한 문자 세트에 있습니다.

또는 **strmqikm** (iKeyman) 사용자 인터페이스를 사용하여 키 데이터베이스를 작성하십시오.

2. UNIX and Linux 시스템에서 루트 사용자로서 로그인하십시오. Windows 시스템에서 관리자 또는 MQM 그룹의 구성원으로서 로그인하십시오.

3. Java 보안 특성 파일 `java.security`를 여십시오.

- UNIX and Linux 시스템에서는 Java 보안 특성 파일이 IBM MQ 설치 디렉토리의 `java/jre64/jre/lib/security` 서브디렉토리에 있습니다.
- Windows 시스템에서는 Java 보안 특성 파일이 IBM MQ 설치 디렉토리의 `java\jre\lib\security` 서브디렉토리에 있습니다.

이 파일에 `IBMPKCS11Impl` 보안 제공자가 아직 없는 경우에는 이를 추가하십시오. 예를 들면 다음과 같은 행을 추가할 수 있습니다.

```
security.provider.12=com.ibm.crypto.pkcs11impl.provider.IBMPKCS11Impl
```

4. **strmqikm** 명령을 실행하여 사용자 인터페이스를 시작하십시오.

5. 키 데이터베이스 파일 > 열기를 클릭하십시오.

6. 키 데이터베이스 유형을 클릭하고 **PKCS11Direct**를 선택하십시오.

7. 파일 이름 필드에 암호화 하드웨어를 관리하기 위한 모듈 이름을 입력하십시오(예: `PKCS11_API.so`).

PKCS #11 암호화 하드웨어에 저장된 인증서 또는 키를 사용 중인 경우 **runmqckm** 및 **strmqikm**은 64비트 프로그램입니다. PKCS #11 지원에 필요한 외부 모듈이 64비트 프로세스에 로드되므로 암호화 하드웨어 관리를 위해서는 64비트 PKCS #11 라이브러리를 설치해야 합니다. **strmqikm** 및 **runmqckm** 프로그램은 Windows 및 Linux x86 32비트 플랫폼에서 32비트이므로 이 플랫폼에서는 이 사항이 적용되지 않습니다.

8. 위치 필드에 경로를 입력하십시오.

- UNIX and Linux 시스템에서 이는 예를 들어, /usr/lib/pkcs11일 수 있습니다.
- Windows 시스템에서 라이브러리 이름을 입력할 수 있습니다(예: cryptoki).

확인을 클릭하십시오. 암호화 토큰 열기 창이 열립니다.

9. 인증서를 저장하는 데 사용할 암호화 디바이스 토큰 레이블을 선택하십시오.
10. **암호화 토큰 비밀번호** 필드에 암호화 하드웨어를 구성할 때 설정한 비밀번호를 입력하십시오.
11. 암호화 하드웨어에 개인 인증서를 받거나 가져오는 데 필요한 서명자 인증서를 보유하기 위한 용량이 있는 경우에는 보조 키 데이터베이스 확인란을 둘 모두 지우고 [282 페이지의 『15』](#) 단계부터 계속하십시오.
서명자 인증서를 보유하기 위해 보조 CMS 키 데이터베이스가 필요한 경우에는 **기존 보조 키 데이터베이스 파일 열기** 또는 **새 보조 키 데이터베이스 파일 작성**을 선택하십시오.
12. **파일 이름** 필드에 파일 이름을 입력하십시오. 이 필드에는 이미 key.kdb 텍스트가 있습니다. 스템 이름이 key이면 이 필드를 변경하지 말고 두십시오. 다른 스템 이름을 지정한 경우에는 key를 사용자의 스템 이름으로 바꾸십시오. .kdb 접미부를 변경하지 않아야 합니다.
13. **위치** 필드에 경로를 입력하십시오. 예:
 - 큐 관리자의 경우: /var/mqm/qmgrs/QM1/ss1
 - IBM MQ MQI client의 경우: /var/mqm/ss1

확인을 클릭하십시오. 비밀번호 프롬프트 창이 열립니다.

14. 비밀번호를 입력하십시오.
[282 페이지의 『11』](#) 단계에서 **기존 보조 키 데이터베이스 파일 열기**를 선택한 경우에는 **비밀번호** 필드에 비밀번호를 입력하십시오.
[282 페이지의 『11』](#) 단계에서 **새 보조 키 데이터베이스 파일 작성**을 선택한 경우 다음 하위 단계를 완료하십시오.
 - a) **비밀번호** 필드에 비밀번호를 입력하고 **비밀번호 확인** 필드에 다시 입력하십시오.
 - b) **파일에 비밀번호 숨김**을 선택하십시오. 비밀번호를 숨기지 않은 경우에는 키 데이터베이스 파일에 액세스하는 데 필요한 비밀번호를 구할 수 없으므로 TLS 채널 시작 시도에 실패합니다.
 - c) **확인**을 클릭하십시오. 비밀번호가 key.sth 파일에 있음을 확인하는 창이 열립니다(다른 스템 이름을 지정하지 않은 경우).
15. **확인**을 클릭하십시오. 키 데이터베이스 콘텐츠 프레임이 표시됩니다.

PKCS #11 하드웨어의 개인 인증서 요청

큐 관리자 또는 IBM MQ MQI client가 사용자의 암호화 하드웨어의 개인 인증서를 요청하려면 이 프로시저를 사용하십시오.

이 태스크 정보

이 태스크에서는 **stirmqikm** 사용자 인터페이스를 사용하여 개인 인증서를 요청하는 방법을 설명합니다. 명령행 인터페이스를 사용하는 경우, [266 페이지의 『명령행 사용』](#)의 내용을 참조하십시오.

참고: IBM MQ는 SHA-3 또는 SHA-5 알고리즘을 지원하지 않습니다. 디지털 서명 알고리즘 이름 SHA384WithRSA 및 SHA512WithRSA를 사용할 수 있습니다. 두 알고리즘 모두 SHA-2 제품군의 구성원이기 때 문입니다.

디지털 서명 알고리즘 이름 SHA3WithRSA 및 SHA5WithRSA는 각각 SHA384WithRSA 및 SHA512WithRSA의 축약된 양식이므로 더 이상 사용되지 않습니다.

프로시저

stirmqikm(iKeyman) 사용자 인터페이스에서 개인 인증서를 요청하려면 다음 단계를 완료하십시오.

1. 암호화 하드웨어에 대해 작업하기 위한 단계를 완료하십시오. [280 페이지의 『PKCS #11 하드웨어에서 인증서 관리』](#)의 내용을 참조하십시오.
2. **작성** 메뉴에서 **새 인증서 요청**을 클릭하십시오.
새 키 및 인증서 요청 작성 창이 열립니다.

3. 키 레이블 필드에 인증서 레이블을 입력하십시오.
레이블은 **CERTLABL** 속성의 값 (설정된 경우) 또는 큐 관리자의 이름이 있는 기본 `ibmwebsphermq` 또는 `IBM MQ MQI client` 로그인 사용자 ID (모두 소문자) 입니다. 자세한 내용은 [디지털 인증서 레이블을 참조하십시오](#).
4. 필요한 키 크기 및 서명 알고리즘을 선택하십시오.
5. 공통 이름 및 조직의 값을 입력하고 국가를 선택하십시오. 나머지 선택적 필드에는 기본값을 승인하거나 새 값을 입력하거나 선택하십시오.
조직 단위 필드에 단 하나의 이름만을 제공할 수 있음을 유의하십시오. 이러한 필드에 대한 자세한 정보는 [10 페이지의 『식별 이름』](#)의 내용을 참조하십시오.
6. 인증서 요청을 저장할 파일의 이름 입력 필드에서 기본 `certreq.arm`을 승인하거나 전체 경로가 포함된 새 값을 입력하십시오.
7. 확인을 클릭하십시오.
확인 창이 열립니다.
8. 확인을 클릭하십시오.
개인 인증서 요청 목록이 사용자가 작성한 새 개인 인증서 요청의 레이블을 보여줍니다. 인증서 요청이 [283 페이지의 『6』](#) 단계에서 선택한 파일에 저장됩니다.
9. 파일을 인증 기관(CA)으로 보내거나 파일을 CA의 웹 사이트에서 요청 양식으로 복사하여 새 개인 인증서를 요청하십시오.

ULW PKCS #11 하드웨어로 개인 인증서 수신
큐 관리자 또는 IBM MQ MQI client가 사용자의 암호화 하드웨어로 개인 인증서를 수신하도록 하려면 이 프로시저를 사용하십시오.

시작하기 전에

개인 인증서에 서명한 CA의 CA 인증서를 추가하십시오. 이를 암호화 하드웨어 또는 보조 CMS 키 데이터베이스에 추가하십시오. 암호화 하드웨어에 서명된 인증서를 수신하기 전에 이를 수행하십시오. 키 링에 CA 인증서를 추가하려면 [272 페이지의 『UNIX, Linux, and Windows에서 CA 인증서 또는 자체 서명 인증서의 공용 부분을 키 저장소에 추가』](#)의 프로시저를 따르십시오.

프로시저

- **strmqikm**(iKeyman) 사용자 인터페이스를 사용하여 개인 인증서를 수신하려면 다음 단계를 완료하십시오.
 - a) 암호화 하드웨어에 대해 작업하기 위한 단계를 완료하십시오. [280 페이지의 『PKCS #11 하드웨어에서 인증서 관리』](#)의 내용을 참조하십시오.
 - b) 수신을 클릭하십시오. 파일에서 인증서 수신 창이 열립니다.
 - c) 새 개인 인증서의 인증서 파일 이름 및 위치를 입력하거나 **찾아보기**를 클릭하여 이름 및 위치를 선택하십시오.
 - d) **확인**을 클릭하십시오. 키 데이터베이스에 개인 인증서가 이미 있는 경우, 사용자가 추가 중인 키를 데이터베이스에서 기본 키로 설정할지 여부를 묻는 창이 열립니다.
 - e) **예** 또는 **아니오**를 클릭하십시오. 레이블 입력 창이 열립니다.
 - f) **확인**을 클릭하십시오. **개인 인증서** 목록이 추가한 새 개인 인증서의 레이블을 표시합니다. 이 레이블은 제 공한 레이블 앞에 암호화 토큰 레이블을 추가하여 구성합니다.
- **runmqakm**(GSKCapiCmd) 명령을 사용하여 개인 인증서를 수신하려면 다음 단계를 완료하십시오.
 - a) 사용자 환경에 대해 구성된 명령 창을 여십시오.
 - b) **runmqakm**(GSKCapiCmd) 명령을 사용하여 개인 인증서를 수신하십시오.

```
runmqakm -cert -receive -file filename -crypto module_name
          -tokenlabel hardware_token -pw hardware_password
          -format cert_format -fips
          -secondaryDB filename -secondaryDBpw password
```

설명:

-file filename

개인 인증서를 포함하고 있는 파일의 완전한 파일 이름을 지정합니다.

-crypto module_name

암호화 하드웨어와 함께 제공된 PKCS #11 라이브러리의 완전한 이름을 지정합니다.

-tokenlabel hardware_token

PKCS #11 암호화 디바이스 토큰 레이블을 지정합니다.

-pw hardware_password

암호화 하드웨어의 액세스 비밀번호를 지정합니다.

-format cert_format

인증서의 형식을 지정합니다. 값은 Base64 인코딩된 ASCII의 경우 `ascii`이거나 2진 DER 데이터의 경우 `binary`입니다. 기본값은 ASCII입니다.

-fips

명령이 FIPS 모드에서 실행되도록 지정합니다. FIPS 모드에서는 ICC 컴포넌트는 FIPS 140-2 유효성 검증된 알고리즘을 사용합니다. ICC 컴포넌트가 FIPS 모드에서 초기화되지 않는 경우에는 `runmqakm` 명령이 실패합니다.

-secondaryDB filename

CMS 키 데이터베이스의 완전한 파일 이름을 지정합니다.

-secondaryDBpw password

CMS 키 데이터베이스의 비밀번호를 지정합니다.

MQ Appliance IBM MQ Appliance에서 SSL/TLS에 대한 작업

IBM MQ Appliance에는 TLS(Transport Layer Security) 지원이 있습니다.

IBM MQ Appliance에는 인증서를 관리하기 위한 특징적 명령을 가지고 있습니다. 인증서 관리에 대한 자세한 정보는 IBM MQ Appliance 문서, [TLS 인증서 관리](#)를 참조하십시오.

z/OS z/OS에서 SSL/TLS에 대한 작업

이 정보는 z/OS에서 TLS(Transport Layer Security)를 설정하고 작업하는 방법을 설명합니다.

각 주제에는 RACF를 사용하여 각 태스크를 수행하는 예가 포함되어 있습니다. 다른 외부 보안 관리자를 사용하여 유사한 태스크를 수행할 수 있습니다.

z/OS에서 285 페이지의 『z/OS에서 SSLTASKS 매개변수 설정』에 설명된 대로 각 큐 관리자가 TLS 호출 처리에 사용하는 서버 서브태스크의 수를 설정할 수도 있습니다.

z/OS TLS 지원은 운영 체제에 통합되어 있고 시스템 SSL로 알려져 있습니다. 시스템 SSL은 z/OS의 암호화 서비스 기본 요소의 일부입니다. 암호화 서비스 기본 구성원은 `pdsname`에 설치됩니다. SIEALNKE 파티션된 데이터 세트(PDS). 시스템 SSL을 설치할 때, 필요로 하는 CipherSpec을 제공하는 적당한 옵션을 선택했는지 확인하십시오.

z/OS z/OS에서 TLS에 대한 추가 사용자 ID 요구사항

이 정보에서는 z/OS에서 TLS를 설정하고 작업하기 위해 사용자 ID에 필요한 추가 요구사항을 설명합니다.

시스템에 적합한 HIPER(High Impact or Pervasive) 업데이트가 모두 있는지 확인하십시오.

다음 필수조건을 설정했는지 확인하십시오.

- `ssidCHIN` 사용자 ID는 RACF에 올바르게 정의되고, `ssidCHIN` 사용자 ID에는 다음 프로파일에 대한 READ 액세스가 있습니다.

- IRR.DIGTCERT.LIST
- IRR.DIGTCERT.LISTRING

이러한 변수는 RACF FACILITY 클래스에 정의되어 있습니다.

- `ssidCHIN` 사용자 ID는 키 링의 소유자입니다.

- 큐 관리자의 개인 인증서는 RACDCERT 명령에 의해 작성된 경우 `ssidCHIN` 사용자 ID와도 같은 인증서 유형 사용자 ID로 작성됩니다.
- 키 링에 작성한 변경사항을 선택하기 위해 채널 시작기가 재이용되거나 **REFRESH SECURITY TYPE(SSL)** 명령이 실행됩니다.
- IBM MQ 채널 시작기 프로시저에는 링크 목록, LPA 또는 STEPLIB DD문을 통해 시스템 SSL 런타임 라이브러리 `pdsname.SIEALNKE`에 대한 액세스가 있습니다. 이 라이브러리는 APF 권한이 있어야 합니다.
- 채널 시작기가 실행 중인 권한이 있는 사용자 ID는 z/OS UNIX 시스템 서비스 계획 문서에 설명된 대로 UNIX USS (System Services) 를 사용하도록 구성됩니다.

채널 시작기는 특수 권한을 필요로 하지 않고 UNIX 내에서 `superuser`로 실행하지 않으므로, 채널 시작기가 게스트/기본 UID 및 OMVS 세그먼트를 사용하여 UNIX System Services를 호출하게 하지 않으려는 사용자는 기본 세그먼트에 기초하여 새 OMVS 세그먼트를 모델링하기만 하면 됩니다.

▶ z/OS z/OS에서 SSLTASKS 매개변수 설정

ALTER QMGR 명령을 사용하여 TLS 호출을 처리하기 위한 서버 서브태스크의 수를 설정합니다.

TLS 채널을 사용하려면, ALTER QMGR 명령을 사용할 때 SSLTASKS 매개변수를 설정하여 적어도 두 개의 서버 서브태스크가 있는지 확인하십시오. 예를 들면, 다음과 같습니다.

```
ALTER QMGR SSLTASKS(5)
```

스토리지 할당 문제를 피하려면 SSLTASKS 속성을 인증서 폐기 목록(CRL) 검사가 없는 환경에서는 8보다 큰 값으로 설정하지 마십시오.

CRL 검사가 사용되는 경우에는 SSLTASK는 해당 검사의 지속 기간 동안 관련된 채널에 의해 보유됩니다. 이는 관련된 LDAP 서버에 연결하는 동안 상당한 시간 동안일 수 있습니다. 각 SSLTASK는 z/OS TCB(Task Control Block)이기 때문입니다.

SSLTASKS 속성의 값을 변경하는 경우에는 채널 시작기를 다시 시작해야 합니다.

▶ z/OS z/OS에서 키 저장소 설정

연결의 양쪽 끝에 키 저장소를 설정합니다. 각 키 저장소를 해당 큐 관리자와 연관시키십시오.

TLS 연결의 경우 연결의 각 끝에 키 저장소가 있어야 합니다. 각각의 큐 관리자는 키 저장소에 액세스할 수 있어야 합니다. ALTER QMGR 명령에 SSLKEYR 매개변수를 사용하여 키 저장소를 큐 관리자에 연관시키십시오. 자세한 정보는 22 페이지의 『SSL/TLS 키 저장소』의 내용을 참조하십시오.

z/OS에서 디지털 인증서는 외부 보안 관리자(ESM)가 관리하는 키 링에 저장됩니다. 이러한 디지털 인증서에는 인증서를 큐 관리자와 연관시키는 레이블이 있습니다. TLS가 인증 목적으로 해당 인증서를 사용합니다. 뒤에 나오는 모든 예에서는 RACF 명령을 사용합니다. 기타 ESM 프로그램에도 이와 동일한 기능의 명령이 있습니다.

z/OS에서 IBM MQ는 설정된 경우 **CERTLABL** 속성의 값 또는 큐 관리자의 이름이 추가된 기본 `ibmWebSphereMQ`를 사용합니다. 자세한 내용은 [디지털 인증서 레이블](#)을 참조하십시오.

큐 관리자의 키 저장소 이름은 RACF 데이터베이스에서 키 링의 이름입니다. 키 링을 작성하기 전과 후에 키 링 이름을 지정할 수 있습니다.

큐 관리자에 새 키 링을 작성하려면 다음 프로시저를 사용하십시오.

1. RACDCERT 명령을 실행하기 위한 적합한 권한이 있는지 확인하십시오(자세한 정보는 *SecureWay Security Server RACF* 명령 언어 참조를 참조하십시오).
2. 다음 명령을 실행하십시오.

```
RACDCERT ID( userid1 ) ADDRING( ring-name )
```

설명:

- `userid1`는 채널 시작기 주소 공간의 사용자 ID 또는 키 링을 소유할 사용자 ID입니다(키 링이 공유되는 경우).

- *ring-name*은 키 링에 부여할 이름입니다. 이 이름의 최대 길이는 237자입니다. 이 이름은 대소문자를 구분합니다. 문제를 피하려면 *ring-name*을 대문자로 지정하십시오.

z/OS z/OS에서 CA 인증서를 큐 관리자에게 사용 가능하게 하기
키 링을 작성한 후에 임의의 관련 CA 인증서를 여기에 연결하십시오.

데이터 세트에 CA 인증서가 있는 경우 먼저 다음 명령을 사용하여 RACF 데이터베이스에 인증서를 추가해야 합니다.

```
RACDCERT ID( userid1 ) ADD( input-data-set-name ) WITHLABEL( 'My CA' )
```

그런 다음 My CA의 CA 인증서를 사용자의 키 링에 연결하려면 다음 명령을 사용하십시오.

```
RACDCERT ID(userid1)  
CONNECT(CERTAUTH LABEL('My CA') RING(ring-name) USAGE(CERTAUTH))
```

여기서 *userid1*은 채널 시작기 사용자 ID 또는 공유된 키 링의 소유자입니다.

CA 인증서에 대한 자세한 정보는 9 페이지의 『디지털 인증서』의 내용을 참조하십시오.

z/OS z/OS에서 키 저장소에서 큐 관리자 찾기

큐 관리자의 키 링의 위치를 확보하려면 이 프로시저를 사용하십시오.

1. 다음 MQSC 명령을 사용하여 큐 관리자의 속성을 표시하십시오.

```
DISPLAY QMGR ALL  
DISPLAY QMGR SSLKEYR
```

2. 키 링의 위치를 위해서는 명령 출력을 조사하십시오.

z/OS z/OS에서 큐 관리자의 키 저장소 위치 지정

큐 관리자의 키 링의 위치를 지정하려면 ALTER QMGR MQSC 명령을 사용하여 큐 관리자의 키 저장소 속성을 설정하십시오.

예를 들면, 다음과 같습니다.

```
ALTER QMGR SSLKEYR(CSQ1RING)
```

채널 시작기 주소 공간에서 키 링을 소유하는 경우.

```
ALTER QMGR SSLKEYR(userid1/CSQ1RING)
```

공유 키 링인 경우, 여기서 *userid1*은 키 링을 소유하는 사용자 ID입니다.

z/OS z/OS에서 채널 시작기에 올바른 액세스 권한 부여

채널 시작기(CHINIT)는 키 저장소 및 특정 보안 프로파일에 대한 액세스가 필요합니다.

키 저장소를 읽기 위한 CHINIT 액세스 부여

키 저장소를 CHINIT 사용자 ID가 소유하는 경우 이 사용자 ID는 FACILITY 클래스에서 IRR.DIGTCERT.LISTRING 프로파일에 대한 읽기 액세스가 필요하고, 그렇지 않은 경우 업데이트 액세스가 필요합니다. PERMIT 명령을 ACCESS(UPDATE) 또는 ACCESS(READ)와 함께 적절하게 사용하여 액세스를 부여하십시오.

```
PERMIT IRR.DIGTCERT.LISTRING CLASS(FACILITY) ID( userid ) ACCESS(UPDATE)
```

여기서 *userid*는 채널 시작기 주소 공간의 사용자 ID입니다.

적합한 CSF* 프로파일에 CHINIT 읽기 액세스 부여

사용할 ICSF(Integrated Cryptographic Service Facility)를 통해 제공되는 하드웨어 지원을 위해 CHINIT 사용자 ID에 다음 명령을 사용하여 CSFSERV 클래스에서 CSF* 프로파일에 대한 읽기 액세스가 있는지 확인하십시오.

```
PERMIT csf-resource CLASS(CSFSERV) ID( userid ) ACCESS(READ)
```

여기서 *csf-resource*는 CSF* 프로파일의 이름이며 *userid*는 채널 시작기 주소 공간의 사용자 ID입니다.

다음의 각 CSF* 프로파일에 대해 이 명령을 반복하십시오.

- CSFDSG
- CSFDSV
- CSFPKD
- CSFPKE
- CSFPKI

CHINIT 사용자 ID에는 다른 CSF* 프로파일에 대한 읽기 액세스 권한도 필요할 수 있습니다. 예를 들어, ECDHE_RSA_AES_256_GCM_SHA384 Cipher Spec을 사용하는 경우 CHINIT 사용자 ID는 다음 CSF* 프로파일에 대한 읽기 액세스 권한도 필요합니다.

- CSF1DVK
- CSF1GAV
- CSF1GKP
- CSF1SKE
- CSF1TRC
- CSF1TRD

자세한 정보는 [RACF CSFSERV 자원 요구사항](#)을 참조하십시오.

ICSF가 설치에 저장되어 있고 설치가 ICSF에 저장된 키에 대한 액세스 제어를 설정한 경우에는 다음 명령을 사용하여 CHINIT 사용자 ID에 CSFKEYS 클래스에서 프로파일에 대한 읽기 액세스가 있는지 확인하십시오.

```
PERMIT IRR.DIGTCERT. userid.* CLASS(CSFKEYS) ID( userid ) ACCESS(READ)
```

여기서 *userid*는 채널 시작기 주소 공간의 사용자 ID입니다.

ICSF(Integrated Cryptographic Service Facility) 사용

채널 시작기는 TLS가 사용 중이 아닌 경우 클라이언트 채널을 통해 흐르는 비밀번호를 난독화하기 위해 비밀번호 보호 알고리즘 시드(seed)를 수행할 때 ICSF를 사용하여 난수를 생성할 수 있습니다.

추가 정보는 235 페이지의 『[ICSF\(Integrated Cryptographic Service Facility\) 사용](#)』의 내용을 참조하십시오.

z/OS z/OS에서 인증서 또는 키 저장소의 변경사항이 적용되는 시기
변경사항은 채널 시작기가 시작되거나 저장소가 새로 고쳐질 때 적용됩니다.

특히, 키 링의 인증서의 변경사항 및 키 저장소 속성의 변경사항은 다음 경우에 적용됩니다.

- 채널 시작기가 시작되거나 재시작될 때.
- 키 저장소의 콘텐츠를 새로 고치기 위해 REFRESH SECURITY TYPE(SSL) 명령이 발행될 때.

z/OS z/OS에서 자체 서명된 개인 인증서 작성

자체 서명된 개인 인증서를 작성하려면 이 프로시저를 사용하십시오.

1. 다음 명령을 사용하여 인증서와 공개 키 및 개인 키 쌍을 생성하십시오.

```
RACDCERT ID(userid2) GENCERT
SUBJECTSDN(CN('common-name')
            T('title')
            OU('organizational-unit')
            O('organization')
            L('locality')
            SP('state-or-province')
            C('country'))
WITHLABEL('label-name')
```

2. 다음 명령을 사용하여 키 링에 인증서를 연결하십시오.

```
RACDCERT ID(userid1)
CONNECT(ID(userid2) LABEL('label-name') RING(ring-name) USAGE(PERSONAL))
```

설명:

- *userid1*은 채널 시작기 주소 공간의 사용자 ID 또는 공유 키 링의 소유자입니다.
- *userid2*는 인증서와 연관된 사용자 ID이고 채널 시작기 주소 공간의 사용자 ID여야 합니다. *userid1* 및 *userid2*는 동일 ID일 수 있습니다.
- *ring-name*은 285 페이지의 『z/OS에서 키 저장소 설정』에서 키 링에 부여한 이름입니다.
- *label-name*은 IBM MQ **CERTLABL** 속성(설정된 경우)의 값이거나 큐 관리자의 이름이 추가된 기본 *ibmWebSphereMQ*입니다. 자세한 내용은 [디지털 인증서 레이블을 참조하십시오](#).

▶ z/OS z/OS에서 개인 인증서 요청

RACF를 사용하여 개인 인증서를 신청하십시오.

개인 인증서를 신청하려면 다음과 같이 RACF를 사용하십시오.

1. 287 페이지의 『z/OS에서 자체 서명된 개인 인증서 작성』에서처럼 자체 서명된 개인 인증서를 작성하십시오. 이 인증서는 요청에 식별 이름의 속성 값을 제공합니다.
2. 다음 명령을 사용하여 데이터 세트에 기록되는 PKCS #10 Base64 인코드 인증서 요청을 작성하십시오.

```
RACDCERT ID(userid2) GENREQ(LABEL(' label_name ')) DSN(' output_data_set_name ')
```

여기서,

- *userid2*는 인증서와 연관된 사용자 ID이고 채널 시작기 주소 공간의 사용자 ID여야 합니다.
- *label_name*은 자체 서명 인증서를 작성할 때 사용한 레이블입니다.

세부사항은 23 페이지의 『디지털 인증서 레이블, 요구사항 이해』을(를) 참조하십시오.

3. 새 개인 인증서를 요청하기 위해 데이터 세트를 인증 기관(CA)에 전송하십시오.
4. 인증 기관이 서명된 인증서를 사용자에게 리턴하는 경우, 289 페이지의 『z/OS에서 키 저장소에 개인 인증서 추가』에 설명된 대로 원래 레이블을 사용하여 인증서를 다시 RACF 데이터베이스에 추가하십시오.

▶ z/OS RACF 서명된 개인 인증서 작성

RACF는 인증 기관의 역할을 수행하고 자체 CA 인증서를 발행할 수 있습니다.

이 절에서는 서명자 인증서 라는 용어를 사용하여 RACF가 발행한 CA 인증서를 표시합니다.

다음 프로시저를 수행하기 전에 서명자 인증서의 개인 키는 RACF 데이터베이스에 있어야 합니다.

1. 다음 명령을 사용하여 RACF 데이터베이스에 포함된 서명자 인증서를 사용하여 RACF에 의해 서명된 개인 인증서를 생성하십시오.

```
RACDCERT ID(userid2) GENCERT
SUBJECTSDN(CN('common-name')
            T('title')
            OU('organizational-unit')
            O('organization'))
```

```
L('locality')
SP('state-or-province')
C('country')
WITHLABEL('label-name')
SIGNWITH(CERTAUTH LABEL('signer-label'))
```

2. 다음 명령을 사용하여 키 링에 인증서를 연결하십시오.

```
RACDCERT ID(userid1)
CONNECT(ID(userid2) LABEL('label-name') RING(ring-name) USAGE(PERSONAL))
```

설명:

- *userid1*은 채널 시작기 주소 공간의 사용자 ID 또는 공유 키 링의 소유자입니다.
- *userid2*는 인증서와 연관된 사용자 ID이고 채널 시작기 주소 공간의 사용자 ID여야 합니다.
userid1 및 *userid2*는 동일 ID일 수 있습니다.
- *ring-name*은 285 페이지의 『z/OS에서 키 저장소 설정』에서 키 링에 부여한 이름입니다.
- *label-name*은 설정된 경우 IBM MQ **CERTLABL** 속성의 값이거나 큐 관리자 또는 큐 공유 그룹의 이름이 추가된 기본 *ibmWebSphereMQ*여야 합니다. 자세한 내용은 [디지털 인증서 레이블](#)을 참조하십시오.
- *signer-label*은 사용자의 서명자 인증서 레이블입니다.

z/OS에서 키 저장소에 개인 인증서 추가

이 프로시저를 사용하여 개인 인증서를 키 링에 추가하거나 가져오십시오.

인증 기관이 새 개인 인증서를 송신한 후에 다음 프로시저를 사용하여 이를 키 링에 추가하십시오.

1. 다음 명령을 사용하여 인증서를 RACF 데이터베이스에 추가하십시오.

```
RACDCERT ID( userid2 ) ADD( input-data-set-name ) WITHLABEL(' label-name ')
```

2. 다음 명령을 사용하여 키 링에 인증서를 연결하십시오.

```
RACDCERT ID( userid1 )
CONNECT(ID( userid2 ) LABEL(' label-name ' ) RING( ring-name ) USAGE(PERSONAL))
```

설명:

- *userid1*은 채널 시작기 주소 공간의 사용자 ID 또는 공유 키 링의 소유자입니다.
- *userid2*는 인증서와 연관된 사용자 ID이고 채널 시작기 주소 공간의 사용자 ID여야 합니다.
- *ring-name*은 285 페이지의 『z/OS에서 키 저장소 설정』에서 키 링에 부여한 이름입니다.
- *input-data-set-name*은 CA 서명 인증서를 포함하는 데이터 세트의 이름입니다. 이 데이터 세트는 카탈로그화되어야 하며 PDS 또는 PDS의 구성원이 아니어야 합니다. RACDCERT에 의해 내보낸 레코드 형식(RECFM)은 VB입니다. RACDCERT는 데이터 세트를 동적으로 할당하고 열며, 이것의 인증서를 2진 데이터로 읽습니다.
- *label-name*은 원래 요청을 작성할 때 사용된 레이블 이름입니다. 설정된 경우 IBM MQ **CERTLABL** 속성의 값이거나 큐 관리자 또는 큐 공유 그룹의 이름이 추가된 기본 *ibmWebSphereMQ*여야 합니다. 자세한 내용은 [디지털 인증서 레이블](#)을 참조하십시오.

z/OS에서 키 저장소로부터 개인 인증서 내보내기

RACDCERT 명령을 사용하여 인증서를 내보내십시오.

인증서를 내보내려는 시스템에서 다음 명령을 사용하십시오.

```
RACDCERT ID(userid2) EXPORT(LABEL('label-name'))
DSN(output-data-set-name) FORMAT(CERTB64)
```

설명:

- `userid2`는 인증서를 키 링에 추가할 때 사용한 사용자 ID입니다.
- `label-name`은 추출하려는 인증서의 레이블입니다.
- `output-data-set-name`은 인증서가 있는 데이터 세트입니다.
- CERTB64는 Base64 형식에서 DER 인코딩된 X.509 인증서입니다. 다음 예와 같은 대체 형식을 선택할 수 있습니다.

CERTDER

2진 형식으로 된 DER 인코딩된 X.509 인증서

PKCS12B64

Base64 형식으로 된 PKCS #12 인증서

PKCS12DER

2진 형식으로 된 PKCS #12 인증서

z/OS z/OS에서 키 저장소로부터 개인 인증서 삭제

RACDCERT 명령을 사용하여 개인 인증서를 삭제하십시오.

개인 인증서를 삭제하기 전에, 그 사본을 저장하려고 할 수 있습니다. 개인 인증서를 삭제하기 전에 데이터 세트로 복사하려면, 289 페이지의 『z/OS에서 키 저장소로부터 개인 인증서 내보내기』의 프로시저를 따르십시오. 그런 후, 개인 인증서를 삭제하기 위해 다음 명령을 사용하십시오.

```
RACDCERT ID( userid2 ) DELETE(LABEL(' label-name '))
```

설명:

- `userid2`는 인증서를 키 링에 추가할 때 사용한 사용자 ID입니다.
- `label-name`은 삭제하려는 인증서의 레이블입니다.

z/OS z/OS에서 키 저장소로부터 개인 인증서 이름 바꾸기

RACDCERT 명령을 사용하여 개인 인증서의 이름을 바꾸십시오.

특정 레이블이 있는 인증서가 보이는 것을 원하지 않으나 삭제하는 것도 원하지 않으면, 다음 명령을 사용하여 임시로 이름을 바꿀 수 있습니다.

```
RACDCERT ID( userid2 ) LABEL(' label-name ') NEWLABEL(' new-label-name ')
```

설명:

- `userid2`는 인증서를 키 링에 추가할 때 사용한 사용자 ID입니다.
- `label-name`은 이름을 바꾸려는 인증서의 이름입니다.
- `new-label-name`은 인증서의 새 이름입니다.

TLS 클라이언트 인증서를 테스트할 때 유용할 수 있습니다.

z/OS z/OS에서 사용자 ID를 디지털 인증서와 연관시키기

IBM MQ는 RACF 인증서와 연관된 사용자 ID를 채널 사용자 ID로서 사용할 수 있습니다. 인증서를 사용자 ID 하에 설치하거나 Certificate Name Filter를 사용하여 사용자 ID를 인증서와 연관시키십시오.

이 주제에 설명된 방법은 사용자 ID를 디지털 인증서와 연관시키기 위한 플랫폼 독립 방법에 대한 대안이며 이는 채널 인증 레코드를 사용합니다. 채널 인증 레코드에 대한 자세한 정보는 43 페이지의 『채널 인증 레코드』의 내용을 참조하십시오.

TLS 채널의 한쪽 끝에서 엔티티가 원격 연결로부터 인증서를 수신하면 엔티티는 해당 인증서와 연관된 사용자 ID가 있는지 RACF에 묻습니다. 엔티티는 그 사용자 ID를 채널 사용자 ID로 사용합니다. 인증서에 연관된 사용자 ID가 없으면, 엔티티가 채널 시작기가 실행 중인 사용자 ID를 사용합니다.

다음 방법 중에서 사용하여 사용자 ID를 인증서와 연관시키십시오.

- 289 페이지의 『z/OS에서 키 저장소에 개인 인증서 추가』에 설명된 대로 해당 인증서를 연관시킬 사용자 ID로 RACF 데이터베이스에 설치하십시오.

- 주제의 식별 이름이나 인증서의 발행인을 사용자 ID로 매핑하려면 291 페이지의 『z/OS에서 인증서 이름 필터 설정』에 있는 대로 CNF(Certificate Name Filter)를 사용하십시오.

z/OS z/OS에서 인증서 이름 필터 설정
 RACDCERT 명령을 사용하여 식별 이름을 사용자 ID에 매핑하는 인증서 이름 필터(CNF)를 정의하십시오.
 CNF를 설정하려면 다음 단계를 수행하십시오.

1. 다음 명령을 사용하여 CNF 기능을 사용으로 설정하십시오. 이를 수행하려면 클래스 DIGTNMAP에서 업데이트 권한이 필요합니다.

```
SETROPTS CLASSACT(DIGTNMAP) RACLIST(DIGTNMAP)
```

2. CNF를 정의하십시오. 예를 들면, 다음과 같습니다.

```
RACDCERT ID(USER1) MAP WITHLABEL('filter1') TRUST  

SDNFILTER('O=IBM.C=UK') IDNFILTER('O=ExampleCA.L=Internet')
```

여기서 USER1 는 다음 경우에 사용할 사용자 ID입니다.

- 제목의 DN에는 IBM이라는 조직과 UK라는 국가가 있습니다.
- 발행인의 DN에 ExampleCA라는 조직과 Internet이라는 장소가 있습니다.

3. 다음과 같이 CNF 매핑을 새로 고치십시오.

```
SETROPTS RACLIST(DIGTNMAP) REFRESH
```

참고:

1. 실제 인증서가 RACF 데이터베이스에 저장되는 경우 설치 시 사용된 사용자 ID가 CNF와 연관된 사용자 ID에 우선하여 사용됩니다. 인증서가 RACF 데이터베이스에 저장되지 않은 경우 대부분의 특정 일치하는 CNF와 연관된 사용자 ID가 사용됩니다. 제목 DN의 일치가 발행인 DN의 일치보다 더 특정한 것으로 간주됩니다.
2. CNF 매핑을 새로 고칠 때까지 CNF에 대한 변경사항이 적용되지 않습니다.
3. DN 필터가 DN의 가장 영향을 미치지 않는 부분과 동일하면 DN이 CNF에 있는 DN 필터에 일치됩니다. DN에서 가장 영향을 미치지 않는 부분은 보통 DN의 오른쪽 끝에 나열되지만 인증서의 맨 앞에 표시되는 속성을 구성합니다.

예를 들어, SDNFILTER 'O=IBM.C=UK' 를 고려하십시오. 'CN=QM1.O=IBM.C=UK' 의 제목 DN은 해당 필터와 일치하지만 'CN=QM1.O=IBM.L=Hursley.C=UK' 의 제목 DN은 해당 필터와 일치하지 않습니다.

일부 인증서의 최소 부분만이 DN 필터와 일치하지 않는 필드를 포함할 수 있습니다. DEFINE CHANNEL 명령의 SSLPEER 패턴에서 DN 패턴을 지정하여 이 인증서를 제외하는 것을 고려하십시오.

4. 가장 특징적인 CNF가 RACF에 NOTRUST로서 정의되어 있는 경우 엔티티는 채널 시작기를 실행할 때 사용한 사용자 ID를 사용합니다.
5. RACF 는 ' .' 문자를 구분 기호로 사용합니다. IBM MQ는 쉼표 또는 세미콜론을 사용합니다.

엔티티는 채널 시작기가 그 아래에서 실행 중인 사용자 ID로서의 채널 사용자 ID를 기본값으로 설정하지 않는다는 것을 확인하기 위해 CNF를 정의할 수 있습니다. 엔티티와 연관된 키 링에 있는 각 CA 인증서에 대해 해당 CA 인증서의 주제 DN과 정확히 일치하는 IDNFILTER를 사용하여 CNF를 정의하십시오. 이렇게 하면 엔티티가 사용할 수 있는 모든 인증서가 이 CNF 중 적어도 하나와 일치합니다. 이는 이러한 모든 인증서가 엔티티와 연관된 키 링으로 연결되거나 인증서가 엔티티와 연관된 키 링에 연결된 CA에 의해 발행되어야 하기 때문입니다.

CNF를 조직하기 위해 사용하는 명령에 대한 자세한 정보는 *SecureWay Security Server RACF Security Administrator's Guide*를 참조하십시오.

z/OS z/OS의 QMA에서 송신자 채널 및 전송 큐 정의
 DEFINE CHANNEL 및 DEFINE QLOCAL 명령을 사용하여 필수 오브젝트를 설정하십시오.

프로시저

QMA에서 다음 예와 같은 명령을 실행하십시오.

```
DEFINE CHANNEL(TO.QMB) CHLTYPE(SDR) TRPTYPE(TCP) CONNAME(QMB.MACH.COM) XMITQ(QMB)
SSLCIPH(TLS_RSA_WITH_AES_128_CBC_SHA256) DESCR('Sender channel using TLS from QMA to QMB')

DEFINE QLOCAL(QMB) USAGE(XMITQ)
```

결과

송신자 채널, TO.QMB 및 전송 큐, QMB가 작성됩니다.

z/OS의 QMB에서 수신자 채널 정의

DEFINE CHANNEL 명령을 사용하여 필수 오브젝트를 설정하십시오.

프로시저

QMB에서 다음 예와 같은 명령을 실행하십시오.

```
DEFINE CHANNEL(TO.QMB) CHLTYPE(RCVR) TRPTYPE(TCP) SSLCIPH(TLS_RSA_WITH_AES_128_CBC_SHA256)
SSLCAUTH(REQUIRED) DESCR('Receiver channel using TLS to QMB')
```

결과

수신자 채널, TO.QMB가 작성됩니다.

z/OS의 QMA에서 송신자 채널 시작

필요한 경우 리스너 프로그램을 시작하고 보안을 새로 고치십시오. 그런 다음 **START CHANNEL** 명령을 사용하여 채널을 시작하십시오.

프로시저

1. 옵션: 아직 하지 않은 경우 QMB에서 리스너 프로그램을 시작하십시오.
리스너 프로그램은 수신 네트워크 요청을 청취하고 필요할 때 수신자 채널을 시작합니다. 리스너를 시작하는 방법에 대한 자세한 정보는 [채널 리스너 시작](#)을 참조하십시오.
2. 옵션: SSL/TLS 채널이 이전에 실행된 경우 **REFRESH SECURITY TYPE(SSL)** 명령을 실행하십시오.
이 명령은 키 저장소에 작성된 모든 변경사항을 사용 가능하도록 합니다.
3. **START CHANNEL(TO.QMB)** 명령을 사용하여 QMA에서 채널을 시작하십시오.

결과

송신자 채널이 시작됩니다.

z/OS에서 자체 서명된 인증서 사용

이전에 추출한 인증서를 교환하십시오. FTP를 사용하는 경우에는 올바른 형식을 사용하십시오.

프로시저

QM1 인증서의 CA 부분을 예를 들어, FTP를 사용하여 QM2 시스템에 전송하고 그 반대로 수행하십시오.

FTP를 사용하여 인증서를 전송하는 경우에는 이를 올바른 형식으로 수행해야 합니다.

다음 인증서 유형은 2진 형식으로 전송하십시오.

- DER 인코딩된 2진 X.509
- PKCS #7(CA 인증서)
- PKCS #12(개인 인증서)

다음 인증서 유형을 ASCII 형식으로 전송하십시오.

- PEM(비공개 확장 메일)
- Base64 인코드 X.509

z/OS z/OS의 QM1에서 송신자 채널 및 전송 큐 정의

DEFINE CHANNEL 및 **DEFINE QLOCAL** 명령을 사용하여 필수 오브젝트를 설정하십시오.

프로시저

QM1에서 다음 예와 같은 명령을 실행하십시오.

```
DEFINE CHANNEL(QM1.TO.QM2) CHLTYPE(SDR) TRPTYPE(TCP) CONNAME(QM1.MACH.COM) XMITQ(QM2)
SSLCIPH(TLS_RSA_WITH_AES_128_CBC_SHA) DESCR('Sender channel using TLS from QM1 to QM2')

DEFINE QLOCAL(QM2) USAGE(XMITQ)
```

채널의 각 끝에 있는 CipherSpec은 동일해야 합니다.

채널에서 TLS를 사용하고자 하는 경우에 SSLCIPH 매개변수만 필수입니다. SSLCIPH 매개변수에 허용된 값에 대한 자세한 정보는 35 페이지의 『IBM MQ의 CipherSpec 및 CipherSuite』의 내용을 참조하십시오.

결과

송신자 채널, QM1.TO.QM2 및 전송 큐, QM2가 작성됩니다.

z/OS z/OS의 QM2에서 수신자 채널 정의

DEFINE CHANNEL 명령을 사용하여 필수 오브젝트를 설정하십시오.

프로시저

QM2에서 다음 예와 같은 명령을 실행하십시오.

```
DEFINE CHANNEL(QM1.TO.QM2) CHLTYPE(RCVR) TRPTYPE(TCP) SSLCIPH(TLS_RSA_WITH_AES_128_CBC_SHA256)
SSLCAUTH(REQUIRED) DESCR('Receiver channel using TLS from QM1 to QM2')
```

채널은 293 페이지의 『z/OS의 QM1에서 송신자 채널 및 전송 큐 정의』에 정의된 송신자 채널과 이름이 같아야 하고 동일한 CipherSpec을 사용해야 합니다.

z/OS z/OS의 QM1에서 송신자 채널 시작

필요한 경우 리스너 프로그램을 시작하고 보안을 새로 고치십시오. 그런 다음 **START CHANNEL** 명령을 사용하여 채널을 시작하십시오.

프로시저

1. 옵션: 아직 하지 않은 경우 QM2에서 리스너 프로그램을 시작하십시오.
리스너 프로그램은 수신 네트워크 요청을 청취하고 필요할 때 수신자 채널을 시작합니다. 리스너 시작 방법에 대한 정보는 [채널 리스너 시작](#)을 참조하십시오.
2. 옵션: SSL/TLS 채널이 이미 실행된 경우에는 REFRESH SECURITY TYPE(SSL) 명령을 실행하십시오.
이 명령은 키 저장소에 작성된 모든 변경사항을 사용 가능하도록 합니다.
3. QM1에서 **START CHANNEL(QM1.TO.QM2)** 명령을 사용하여 채널을 시작하십시오.

결과

송신자 채널이 시작됩니다.

z/OS z/OS에서 SSL 또는 TLS 환경 새로 고치기

REFRESH SECURITY 명령을 사용하여 큐 관리자 QMA에서 TLS 환경을 새로 고치십시오.

프로시저

QMA에서 다음 명령을 입력하십시오.

```
REFRESH SECURITY TYPE(SSL)
```

이 명령은 키 저장소에 작성된 모든 변경사항을 사용 가능하도록 합니다.

z/OS에서 수신자 채널에 익명 연결 허용

SSL 또는 TLS 클라이언트 인증을 선택사항으로 만들려면 **ALTER CHANNEL** 명령을 사용하십시오.

프로시저

QMB에서 다음 명령을 입력하십시오.

```
ALTER CHANNEL(TO.QMB) CHLTYPE(RCVR) SSLCAUTH(OPTIONAL)
```

z/OS의 QM1에서 송신자 채널 시작

필요한 경우 채널 시작기를 시작하고, 리스너 프로그램을 시작하고 보안을 새로 고치십시오. 그런 다음 **START CHANNEL** 명령을 사용하여 채널을 시작하십시오.

프로시저

1. 옵션: 아직 하지 않은 경우 채널 시작기를 시작하십시오.
2. 옵션: 아직 하지 않은 경우 QM2에서 리스너 프로그램을 시작하십시오.
리스너 프로그램은 수신 네트워크 요청을 청취하고 필요할 때 수신자 채널을 시작합니다. 리스너 시작 방법에 대한 정보는 [채널 리스너 시작](#)을 참조하십시오.
3. 옵션: 채널 시작기가 이미 실행 중이거나 SSL/TLS 채널이 이미 실행된 경우에는 REFRESH SECURITY TYPE(SSL) 명령을 실행하십시오.
이 명령은 키 저장소에 작성된 모든 변경사항을 사용 가능하도록 합니다.
4. QM1에서 START CHANNEL(QM1.TO.QM2) 명령을 사용하여 채널을 시작하십시오.

결과

송신자 채널이 시작됩니다.

z/OS의 QMA에서 송신자 채널 시작

필요한 경우 채널 시작기를 시작하고, 리스너 프로그램을 시작하고 보안을 새로 고치십시오. 그런 다음 **START CHANNEL** 명령을 사용하여 채널을 시작하십시오.

프로시저

1. 옵션: 아직 하지 않은 경우 채널 시작기를 시작하십시오.
2. 옵션: 아직 하지 않은 경우 QMB에서 리스너 프로그램을 시작하십시오.
리스너 프로그램은 수신 네트워크 요청을 청취하고 필요할 때 수신자 채널을 시작합니다. 리스너를 시작하는 방법에 대한 자세한 정보는 [채널 리스너 시작](#)을 참조하십시오.
3. 옵션: 채널 시작기가 이미 실행 중이거나 SSL/TLS 채널이 이미 실행된 경우에는 REFRESH SECURITY TYPE(SSL) 명령을 실행하십시오.
이 명령은 키 저장소에 작성된 모든 변경사항을 사용 가능하도록 합니다.
4. START CHANNEL(TO.QMB) 명령을 사용하여 QMA에서 채널을 시작하십시오.

결과

송신자 채널이 시작됩니다.

z/OS의 타원 곡선 키 길이 수정

GSK_CLIENT_ECURVE_LIST 환경 변수를 수정하여 클라이언트가 지정한 타원 곡선 또는 지원되는 그룹 목록을 사용 환경 설정 순서에 따라 4자로 된 하나 이상의 값으로 구성된 문자열로 설정하는 방법.

중요사항: TLS 1.0, TLS 1.1 및/또는 TLS 1.2 협상 연결을 사용할 때 운영 체제에서 특정 타원 곡선이 적용되도록 하려면 z/OS APAR [OA61783](#) 에 수정사항을 적용해야 합니다.

CEEOPTS DD문을 사용하여 채널 시작기 시작 JCL에 이 TLS 환경 변수를 설정할 수 있습니다.

```
CEEOPTS DD DSN=<dataset-name>,DISP=SHR
```

위에서 참조된 데이터 세트에서 사용할 목록을 지정하십시오. 예를 들어 다음과 같습니다.

```
ENVAR("GSK_CLIENT_ECURVE_LIST=002300240025")
```

중요사항: In-Stream 데이터와 함께 이 CEEOPTS문을 사용하지 마십시오. 그러면 해당 명령문을 사용하는 모든 TLS 작업에 환경 변수가 설정되지 않습니다.

1보다 큰 SSLTASKS 값을 사용할 때 작동하도록 시퀀스 데이터 세트 또는 파티션된 데이터 세트 멤버를 참조하십시오.

GSK_SERVER_ALLOWED_KEX_ECURVES인 GSK_CLIENT_ECURVE_LIST 서버 아날로그와 같은 서버를 사용할 수도 있다. 자세한 정보는 [키 교환 생략 곡선 제한](#) 을 참조하십시오.

또한 유효한 4자의 타원 곡선 및 지원되는 그룹 스펙 목록은 [암호 스위트 정의](#) 의 표 5를 참조하십시오.

기본 사양은 00210023002400250019입니다. TLS V1.3이 사용된 경우 0029 (x25519)가 기본 목록의 끝에 추가됩니다.

사용자 식별 및 인증

MQCSP 구조를 사용하거나 여러 유형의 사용자 엑시트 프로그램을 사용하여 사용자를 식별하고 인증할 수 있습니다.

X.509 인증서 사용

CHLAUTH 명령 및 **SSLPEER** 매개변수와 함께 x.509 인증서를 사용하여 사용자를 식별하고 인증할 수 있습니다. **SSLPEER** 매개변수는 채널의 다른 쪽 끝에 있는 피어 큐 관리자 또는 클라이언트의 인증서의 주제 식별 이름과 비교하는 데 사용할 필터를 지정합니다.

CHLAUTH 명령 및 **SSLPEER** 매개변수 사용에 대한 자세한 정보는 [SET CHLAUTH](#)를 참조하십시오.

MQCSP 구조 사용

MQCONNX 호출에서 MQCSP 연결 보안 매개변수 구조를 지정할 수 있습니다. 이 구조에는 사용자 ID 및 비밀번호가 포함됩니다. 필요한 경우 보안 엑시트에서 MQCSP를 변경할 수 있습니다.

참고: 오브젝트 권한 관리자(OAM)는 비밀번호를 사용하지 않습니다. 그러나 OAM은 사용자 ID를 사용하여 인증의 사소한 양식으로 간주될 수 있는 몇몇 제한된 작업을 수행합니다. 이러한 검사는 사용자가 애플리케이션에서 이러한 매개변수를 사용하는 경우 사용자가 또 다른 사용자 ID를 채택하는 것을 중지합니다.

경고: 일부 경우에 클라이언트 애플리케이션에 대한 MQCSP 구조의 비밀번호는 일반 텍스트로 네트워크 전체에 전송됩니다. 클라이언트 애플리케이션 비밀번호가 적절하게 보호될 수 있도록 하려면 [26 페이지의 『MQCSP 비밀번호 보호』](#)의 내용을 참조하십시오.

보안 엑시트에서 식별 및 인증 구현

보안 엑시트의 1차 목적은 해당 파트너를 인증하기 위해 채널의 각 끝에서 MCA를 사용 가능으로 하는 것입니다. 메시지 채널의 각 끝과 MQI 채널의 서버 측에서 MCA는 일반적으로 연결된 큐 관리자 대신에 작동합니다. MQI 채널의 클라이언트 끝에서 MCA는 일반적으로 IBM MQ 클라이언트 애플리케이션의 사용자 대신에 작동합니다. 이 경우 상호 인증은 실제로 두 큐 관리자 사이 또는 큐 관리자와 IBM MQ MQI client 애플리케이션의 사용자 사이에 발생합니다.

제공된 보안 엑시트(SSPI 채널 엑시트)는 생성된 인증 토큰을 교환한 다음 Kerberos 등과 같은 신뢰되는 인증 서버에 의해 검사되는 방법으로 상호 인증이 구현되는 방법을 보여줍니다. 자세한 정보는 [136 페이지의 『Windows에서 SSPI 채널 엑시트 프로그램』](#)의 내용을 참조하십시오.

상호 인증은 PKI(Public Key Infrastructure) 기술을 사용하여 구현할 수도 있습니다. 각 보안 엑시트가 어떤 무작위 데이터를 생성하고, 그것이 나타내고 있는 큐 관리자나 사용자의 개인 키를 사용하여 서명하고, 서명된 데이터를 보안 메시지로 그 파트너에게 송신합니다. 파트너 보안 엑시트가 큐 관리자나 사용자의 공개 키를 사용하여 디지털 서명을 검사하여 인증을 수행합니다. 디지털 서명을 교환하기 전에, 둘 이상의 알고리즘이 사용 가능한 경우, 보안 엑시트가 메시지 요약을 생성하기 위해 알고리즘에 동의해야 할 수 있습니다.

보안 엑시트가 서명된 데이터를 그 파트너에게 송신하면, 파트너도 그것이 나타내고 있는 큐 관리자나 사용자를 식별하는 어떤 수단을 송신해야 할 수 있습니다. 이것은 식별 이름이거나, 디지털 인증서일 수도 있습니다. 디지털 인증서가 송신되면, 파트너 보안 엑시트가 루트 CA 인증서로 가는 인증서 체인을 통해 작업하여 인증서의 유효성을 검증할 수 있습니다. 이렇게 하면 디지털 서명을 검사하는 데 사용되는 공개 키의 소유권의 보장을 제공합니다.

파트너 보안 엑시트가 인증서 체인의 나머지 인증서를 포함하는 키 저장소에 액세스할 수 있는 경우에만 디지털 인증서의 유효성을 검증할 수 있습니다. 큐 관리자나 사용자를 위한 디지털 인증서가 송신되지 않으면, 파트너 보안 엑시트가 액세스할 수 있는 키 저장소에서 사용 가능해야 합니다. 파트너 보안 엑시트가 서명자의 공개 키를 찾을 수 없으면 디지털 서명을 검사할 수 없습니다.

TLS(Transport Layer Security)는 방금 설명한 것과 같은 PKI 기술을 사용합니다. TLS가 인증을 수행하는 방법에 대한 자세한 정보는 [14 페이지의 『TLS\(Transport Layer Security\) 개념』](#)의 내용을 참조하십시오.

신뢰받는 인증 서버 또는 PKI 지원을 사용할 수 없으면 다른 기술을 사용할 수 있습니다. 보안 엑시트에 구현될 수 있는 공통적인 기술은 대칭 키 알고리즘을 사용합니다.

보안 엑시트 중 하나인 엑시트 A가 난수를 생성하여 파트너 보안 엑시트인 엑시트 B에 보안 메시지로 송신합니다. 엑시트 B가 두 개의 보안 엑시트에만 알려져 있는 키의 사본을 사용하여 숫자를 암호화합니다. 엑시트 B가 암호화된 숫자를 생성한 또 다른 난수와 함께 보안 메시지로 엑시트 A에게 송신합니다. 엑시트 A는 첫 번째 난수가 정확하게 암호화되었는지를 확인하고, 키의 사본을 사용하여 두 번째 난수를 암호화하며, 암호화된 숫자를 엑시트 B에게 보안 메시지로 송신합니다. 그런 후, 엑시트 B가 두 번째 난수가 제대로 암호화되었는지를 확인합니다. 이 교환 동안에, 보안 엑시트 중 어느 것이든지 다른 쪽의 인증에 만족하지 않으면, MCA에게 채널을 닫으라고 지시할 수 있습니다.

이 기술의 장점은 키나 암호가 교환 중에 통신 연결에서 송신되지 않는다는 것입니다. 단점은 공유 키를 보안된 방식으로 분배하는 방법에 대한 문제점의 해결책을 제공하지 못한다는 것입니다. 이 문제점에 대한 한 가지 해결책이 [401 페이지의 『사용자 엑시트 프로그램에서 기밀성 구현』](#)에 설명되어 있습니다. 비슷한 기술이 SNA에서 두 개의 LU가 세션을 형성하기 위해 바인딩될 때 상호 인증을 위해 사용됩니다. 이 기술은 [103 페이지의 『세션 레벨 인증』](#)에 설명되어 있습니다.

상호 인증을 위한 모든 앞선 기술은 단방향 인증을 제공하기 위해 채택될 수 있습니다.

메시지 엑시트에서 식별 및 인증 구현

애플리케이션이 메시지를 큐에 넣을 때, 메시지 설명자의 *UserIdentifier* 필드에 애플리케이션과 연관된 사용자 ID가 있습니다. 그러나, 사용자 ID를 인증하는 데 사용될 수 있는 데이터가 없습니다. 이 데이터는 채널의 송신 측에 있는 메시지 엑시트에 의해 추가되고 채널의 수신 측에 있는 메시지 엑시트에 의해 검사됩니다. 예를 들면, 데이터를 인증하는 것은 암호화된 암호이거나 디지털 서명일 수 있습니다.

이 서비스가 애플리케이션 레벨에서 구현되면 더 효율적일 수 있습니다. 기본적인 요구사항은 메시지를 수신하는 애플리케이션 사용자가 메시지를 송신한 애플리케이션의 사용자를 식별하고 인증할 수 있어야 한다는 것입니다. 그러므로, 이 서비스를 애플리케이션 레벨에서 구현하는 것을 고려하는 것이 당연합니다. 자세한 정보는 [300 페이지의 『API 엑시트와 API 교차 엑시트에서 ID 매핑』](#)의 내용을 참조하십시오.

API 엑시트 및 API 교차 엑시트에서 식별 및 인증 구현

개별 메시지의 레벨에서, 식별과 인증은 메시지의 송신자와 수신자의 두 사용자와 관계가 있는 서비스입니다. 기본적인 요구사항은 메시지를 수신하는 애플리케이션 사용자가 메시지를 송신한 애플리케이션의 사용자를 식별하고 인증할 수 있어야 한다는 것입니다. 요구사항은 양방향이나 단방향 인증이라는 것을 알아두십시오.

구현된 방법에 따라, 사용자와 애플리케이션은 서비스와 인터페이스되어 있거나, 대화해야 할 수도 있습니다. 또한, 서비스가 사용되는 때와 방법은 사용자와 애플리케이션이 있는 위치와 애플리케이션 자체의 성격에 따라 다

를 수 있습니다. 그러므로, 서비스를 링크 레벨이 아니라 애플리케이션 레벨에서 구현하는 것을 고려하는 것이 당연합니다.

이 서비스를 링크 레벨에서 구현하는 것을 고려하는 경우, 다음과 같은 문제를 해결해야 할 수 있습니다.

- 메시지 채널에서 어떻게 서비스를 필요로 하는 메시지에만 서비스를 적용할 것인가?
- 필요한 경우, 사용자와 애플리케이션을 어떻게 서비스와 인터페이스하거나 상호작용할 수 있게 할 것인가?
- 멀티 호핑(multi-hop) 상황에서, 목적지로 가는 둘 이상의 메시지 채널에서 메시지가 어디로 송신될 것인가? 서비스의 구성요소를 어디에서 호출할 것인가?

다음은 식별 및 인증 서비스를 애플리케이션 레벨에서 구현하는 방법의 몇몇 예입니다. 용어 *API 엑시트*는 API 엑시트 또는 API 교차 엑시트를 의미합니다.

- 애플리케이션이 큐에 메시지를 넣으면 API 엑시트가 Kerberos와 같은 트러스트 인증 서버에서 인증 토큰을 확보할 수 있습니다. API 엑시트가 이 토큰을 메시지 안의 애플리케이션 데이터에 추가할 수 있습니다. 메시지가 수신하고 있는 애플리케이션에 의해 검색될 때, 또 다른 API 엑시트가 인증 서버에게 토큰을 검사하여 송신자를 인증하라고 요청할 수 있습니다.
- 애플리케이션이 메시지를 큐에 넣을 때, API 엑시트가 다음 항목을 메시지의 애플리케이션 데이터에 추가할 수 있습니다.
 - 송신자의 디지털 인증서
 - 송신자의 디지털 서명

메시지 요약을 위한 다른 알고리즘이 사용 가능하면, API 엑시트가 사용했던 알고리즘의 이름을 포함할 수 있습니다.

메시지가 수신하고 있는 애플리케이션에 의해 검색될 때, 또 다른 API 엑시트가 다음 검사를 수행할 수 있습니다.

- API 엑시트가 루트 CA 인증서로 가는 인증서 체인을 통해 작업하여 디지털 인증서의 유효성을 검증할 수 있습니다. 이를 수행하려면 API 엑시트가 인증서 체인의 나머지 인증서를 포함하는 키 저장소에 액세스할 수 있어야 합니다. 이 검사는 식별 이름에 의해 식별되는 송신자가 인증서에 있는 공개키의 조작 및 변경되지 않은 순수한 소유자라는 것을 보장합니다.
- API 엑시트가 인증서에 있는 공개키를 사용하여 디지털 서명을 검사할 수 있습니다. 이 검사는 송신자를 인증합니다.

송신자의 식별 이름이 전체 디지털 인증서 대신에 송신될 수 있습니다. 이런 경우에, 키 저장소에 송신자의 인증서가 있어야 두 번째 API 엑시트가 송신자의 공개 키를 찾을 수 있습니다. 다른 가능성은 인증서 체인에 있는 모든 인증서를 송신하는 것입니다.

- 애플리케이션이 메시지를 큐에 넣을 때, 메시지 설명자의 *UserIdentifier* 필드에 애플리케이션과 연관된 사용자 ID가 있습니다. 사용자 ID는 송신자를 식별하는 데 사용될 수 있습니다. 인증을 가능하게 하려면, API 엑시트가 암호화된 암호와 같은 데이터를 메시지의 애플리케이션 데이터에 추가할 수 있습니다. 메시지가 수신하고 있는 애플리케이션에 의해 검색될 때, 또 다른 API 엑시트가 메시지와 함께 돌아다니는 데이터를 사용하여 사용자 ID를 인증할 수 있습니다.

이 기술은 제어되고 트러스트되는 환경 및 트러스트되는 인증 서버나 PKI 지원이 사용 불가능한 환경에서 작성된 메시지에 대해서 충분하다고 간주될 수 있습니다.

플러그 가능한 인증 방법(PAM)



PAM은 이제 UNIX and Linux 플랫폼 전체에 걸쳐 공통이고 서비스로부터 사용자 인증의 세부사항을 숨기는 일반 메커니즘을 제공합니다.

서비스 자체에 변경이 필요 없이 규칙을 구성하여 다양한 인증 규칙을 여러 서비스에 사용할 수 있습니다.

자세한 정보는 312 페이지의 『플러그 가능한 인증 방법(PAM) 사용』의 내용을 참조하십시오.

권한이 있는 사용자

권한 부여된 사용자는 IBM MQ에 대한 전체 관리 권한이 있는 사용자입니다.

다음 표에 나열된 사용자 이외에도, 큐 관리자의 무결성과 보안을 보장하기 위해 액세스 권한을 부여할 때 특별한 주의를 기울여야 하는 특정 오브젝트와 권한이 있습니다. 다음 권한 중 하나를 부여할 때 추가로 검토해야 합니다.

- SYSTEM 오브젝트에 대한 모든 권한
- 오브젝트를 작성하고 대체하고 삭제하는 관리 권한.

▶ **z/OS** z/OS의 경우, 이는 DEFINE, ALTER 및 DELETE 명령을 실행하는 명령 보안 및 명령 자원 보안 권한입니다.

▶ **Multi** 다른 모든 플랫폼에서는 이러한 권한이 +crt, +chg 및 +dlt 등의 관리 권한입니다.

- 큐를 지우는 관리 권한.

▶ **z/OS** z/OS의 경우, 이는 CLEAR 명령을 실행하는 명령 보안 및 명령 자원 보안 권한입니다.

▶ **Multi** 다른 모든 플랫폼에서, 이 권한은 +clr입니다.

- 채널을 중지하거나 메시지를 백아웃하거나 커미트하는 관리 권한.

▶ **z/OS** z/OS의 경우, 이는 RESET CHANNEL, START CHANNEL 및 STOP CHANNEL과 같은 명령을 실행하는 명령 보안 및 명령 자원 보안 권한입니다.

▶ **Multi** 다른 모든 플랫폼에서, 이러한 권한은 +ctrl 및 +ctrlx입니다.

- 애플리케이션이 권한 검사를 위해 권한을 에스컬레이션할 수 있게 하는 대체 사용자 MQI 권한.

▶ **z/OS** z/OS의 경우, 이는 대체 사용자 보안 프로파일에 부여된 임의 권한입니다.

▶ **Multi** 다른 모든 플랫폼에서, 이 권한은 +altusr입니다.

- 애플리케이션이 메시지의 보안 컨텍스트를 변경할 수 있게 하는 컨텍스트 권한.

▶ **z/OS** z/OS의 경우, 이는 컨텍스트 보안 프로파일에 부여된 임의 권한입니다.

▶ **Multi** 다른 모든 플랫폼에서, 이러한 권한은 +setall 및 +setid입니다.

메시징 애플리케이션에는 필요한 큐 또는 토픽에 대한 기본 MQI 권한만 부여하는 것이 일반적인 원칙입니다. 권한을 부여받지 못한 MCAUSER 하에서 실행되는 MCA 채널 및 특정한 다른 특수 유형의 애플리케이션(예: 데드-레터 큐)이 올바르게 작용하려면 애플리케이션에 정상적으로 부여되지 않은 추가 권한이 필요할 수 있습니다.

플랫폼	권한이 있는 사용자
Windows 시스템	<ul style="list-style-type: none"> • SYSTEM • mqm 그룹의 구성원 • 관리자 그룹의 구성원
UNIX and Linux 시스템	<ul style="list-style-type: none"> • mqm 그룹의 구성원
▶ IBM i ▶ IBM i IBM i 시스템	<ul style="list-style-type: none"> • 프로파일 qmqm 및 qmqmadm • qmqmadm 그룹의 모든 구성원 • *ALLOBJ 설정으로 정의된 모든 사용자
z/OS	채널 시작기, 큐 관리자 및 고급 메시지 보안 주소 공간을 실행 중인 사용자 ID. 이러한 사용자 ID가 IBM MQ에 대한 전체 관리 권한을 자동으로 갖지는 않지만 이러한 사용자 ID에 일반적으로 부여되는 액세스 권한 레벨로 인해 권한이 있는 것으로 간주됩니다.

MQCSP 구조를 사용하여 사용자 식별 및 인증

MQCONNX 호출에서 MQCSP 연결 보안 매개변수 구조를 지정할 수 있습니다.

MQCSP 연결 보안 매개변수 구조에는 권한 서비스가 사용자를 식별하고 인증하는 데 사용할 수 있는 사용자 ID 및 비밀번호가 포함되어 있습니다.

보안 엑시트에서 MQCSP를 변경할 수 있습니다.

경고: 일부 경우에 클라이언트 애플리케이션에 대한 MQCSP 구조의 비밀번호는 일반 텍스트로 네트워크 전체에 전송됩니다. 클라이언트 애플리케이션 비밀번호가 적절하게 보호될 수 있도록 하려면 [26 페이지의 『MQCSP 비밀번호 보호』](#)의 내용을 참조하십시오.

MQCSP와 AdoptCTX 설정 간의 관계

IBM MQ는 연결 인증 기능이 사용으로 설정되지 않은 경우를 제외하고 항상 MQCSP 구조를 통해 전달된 신임 정보를 인증합니다. 신임 정보가 성공적으로 인증되면 IBM MQ는 ADOPTCTX가 사용으로 설정되지 않은 경우를 제외하고 향후 권한 검사를 위해 사용자 ID를 채택하려고 시도합니다.

IBM MQ에는 권한 검사에 사용할 수 있는 사용자 ID 길이에 대한 한계가 있습니다. 이러한 한계는 [74 페이지의 『사용자 ID』](#)에 자세히 설명되어 있습니다. MQCSP 구조를 통해 전달된 사용자 ID를 채택할 때 IBM MQ는 기타 구성 옵션에 따라 다르게 작동합니다.

- LDAP 연결 인증을 사용할 때 IBM MQ는 해당 사용자의 사용자 LDAP 레코드에서 SHORTUSR에 설정된 필드의 값을 검색하고 해당 사용자 ID를 채택합니다.

예를 들어, SHORTUSR이 'CN'로 설정되고 LDAP 레코드가 사용자를 'CN=Test,SN=MQ,O=IBM,C=UK'로 나열하는 경우 사용자 ID Test가 사용됩니다.

- OS 연결 인증 또는 PAM 인증을 사용할 때 ADOPTCTX가 YES인 경우, MQCSP 구조를 통해 전달되는 사용자 ID는 연결 컨텍스트로 채택될 때 IBM MQ의 12자사용자 ID 한계를 충족시키기 위해 잘립니다.

Ch1AuthEarlyAdopt가 사용으로 설정되면 사용자 신임 정보가 인증된 후에 잘립니다.

Ch1AuthEarlyAdopt가 사용으로 설정되지 않은 경우 채택 전에 잘림이 발생합니다. Windows에서 사용자가 user@domain형식으로 제공되는 경우 이는 사용자가 12자미만인 경우 도메인 스페이스가 올바르지 않을 수 있음을 의미합니다.

예를 들어, 사용자 'ibmmq@windowsdomain'가 MQCSP를 통해 제공되는 경우 이 시나리오에서는 'ibmmq@window'로 잘립니다. 이는 다음과 같은 오류를 초래합니다.

```
AMQ8074W: SID 'SID' 가 엔티티 'ibmmq@window' 와 일치하지 않으므로 권한 부여에 실패했습니다.
```

이를 기반으로 12자보다 긴 사용자 ID (예: user@domain양식의 Windows 도메인 사용자 ID)를 MQCSP를 통해 전달하는 경우 qm.ini 파일에서 **Ch1AuthEarlyAdopt=Y**를 구성하여 이 오류를 방지해야 합니다.

또는 CONNAUTH AUTHINFO 구성에서 ADOPTCTX (NO)를 사용하고 CHLAUTH USERMAP 규칙, 보안 엑시트 또는 채널 오브젝트 MCAUSER 설정과 같은 대체 접근 방식을 사용하여 채널의 사용자 ID를 설정하십시오.

보안 엑시트에서 식별 및 인증 구현

단방향 또는 상호 인증을 구현하기 위해 보안 엑시트를 사용할 수 있습니다.

보안 엑시트의 1차 목적은 해당 파트너를 인증하기 위해 채널의 각 끝에서 MCA를 사용 가능으로 하는 것입니다. 메시지 채널의 각 끝과 MQI 채널의 서버 측에서 MCA는 일반적으로 연결된 큐 관리자 대신에 작동합니다. MQI 채널의 클라이언트 끝에서 MCA는 일반적으로 IBM MQ MQI client 애플리케이션의 사용자 대신에 작동합니다. 이 경우 상호 인증은 실제로 두 큐 관리자 사이 또는 큐 관리자와 IBM MQ MQI client 애플리케이션의 사용자 사이에 발생합니다.

제공된 보안 엑시트(SSPI 채널 엑시트)는 생성된 인증 토큰을 교환한 다음 Kerberos 등과 같은 신뢰되는 인증 서버에 의해 검사되는 방법으로 상호 인증이 구현되는 방법을 보여줍니다. 자세한 정보는 [136 페이지의 『Windows에서 SSPI 채널 엑시트 프로그램』](#)의 내용을 참조하십시오.

상호 인증은 PKI(Public Key Infrastructure) 기술을 사용하여 구현할 수도 있습니다. 각 보안 엑시트가 어떤 무작위 데이터를 생성하고, 그것이 나타내고 있는 큐 관리자나 사용자의 개인 키를 사용하여 서명하고, 서명된 데이터를 보안 메시지로 그 파트너에게 송신합니다. 파트너 보안 엑시트가 큐 관리자나 사용자의 공개 키를 사용하여

디지털 서명을 검사하여 인증을 수행합니다. 디지털 서명을 교환하기 전에, 둘 이상의 알고리즘이 사용 가능한 경우, 보안 엑시트가 메시지 요약을 생성하기 위해 알고리즘에 동의해야 할 수 있습니다.

보안 엑시트가 서명된 데이터를 그 파트너에게 송신하면, 파트너도 그것이 나타내고 있는 큐 관리자나 사용자를 식별하는 어떤 수단을 송신해야 할 수 있습니다. 이것은 식별 이름이거나, 디지털 인증서일 수도 있습니다. 디지털 인증서가 송신되면, 파트너 보안 엑시트가 루트 CA 인증서로 가는 인증서 체인을 통해 작업하여 인증서의 유효성을 검증할 수 있습니다. 이렇게 하면 디지털 서명을 검사하는 데 사용되는 공개 키의 소유권의 보장을 제공합니다.

파트너 보안 엑시트가 인증서 체인의 나머지 인증서를 포함하는 키 저장소에 액세스할 수 있는 경우에만 디지털 인증서의 유효성을 검증할 수 있습니다. 큐 관리자나 사용자를 위한 디지털 인증서가 송신되지 않으면, 파트너 보안 엑시트가 액세스할 수 있는 키 저장소에서 사용 가능해야 합니다. 파트너 보안 엑시트가 서명자의 공개 키를 찾을 수 없으면 디지털 서명을 검사할 수 없습니다.

TLS(Transport Layer Security)는 방금 설명한 것과 같은 PKI 기술을 사용합니다. SSL(Secure Sockets Layer)의 인증 수행에 대한 자세한 정보는 [14 페이지의 『TLS\(Transport Layer Security\) 개념』](#)의 내용을 참조하십시오.

신뢰받는 인증 서버 또는 PKI 지원을 사용할 수 없으면 다른 기술을 사용할 수 있습니다. 보안 엑시트에 구현될 수 있는 공통적인 기술은 대칭 키 알고리즘을 사용합니다.

보안 엑시트 중 하나인 엑시트 A가 난수를 생성하여 파트너 보안 엑시트인 엑시트 B에 보안 메시지로 송신합니다. 엑시트 B가 두 개의 보안 엑시트에만 알려져 있는 키의 사본을 사용하여 숫자를 암호화합니다. 엑시트 B가 암호화된 숫자를 생성한 또 다른 난수와 함께 보안 메시지로 엑시트 A에게 송신합니다. 엑시트 A는 첫 번째 난수가 정확하게 암호화되었는지를 확인하고, 키의 사본을 사용하여 두 번째 난수를 암호화하며, 암호화된 숫자를 엑시트 B에게 보안 메시지로 송신합니다. 그런 후, 엑시트 B가 두 번째 난수가 제대로 암호화되었는지를 확인합니다. 이 교환 동안에, 보안 엑시트 중 어느 것이든 다른 쪽의 인증에 만족하지 않으면, MCA에게 채널을 닫으라고 지시할 수 있습니다.

이 기술의 장점은 키나 암호가 교환 중에 통신 연결에서 송신되지 않는다는 것입니다. 단점은 공유 키를 보안된 방식으로 분배하는 방법에 대한 문제점의 해결책을 제공하지 못한다는 것입니다. 이 문제점에 대한 한 가지 해결책이 [401 페이지의 『사용자 엑시트 프로그램에서 기밀성 구현』](#)에 설명되어 있습니다. 비슷한 기술이 SNA에서 두 개의 LU가 세션을 형성하기 위해 바인딩될 때 상호 인증을 위해 사용됩니다. 이 기술은 [103 페이지의 『세션 레벨 인증』](#)에 설명되어 있습니다.

상호 인증을 위한 모든 앞선 기술은 단방향 인증을 제공하기 위해 채택될 수 있습니다.

메시지 엑시트에서 ID 맵핑

인증은 애플리케이션 레벨에서 구현하는 것이 더 나을 수도 있지만 메시지 엑시트를 사용하여 사용자 ID를 인증하기 위해 정보를 처리할 수 있습니다.

애플리케이션이 메시지를 큐에 넣을 때, 메시지 설명자의 *UserIdentifier* 필드에 애플리케이션과 연관된 사용자 ID가 있습니다. 그러나, 사용자 ID를 인증하는 데 사용될 수 있는 데이터가 없습니다. 이 데이터는 채널의 송신 측에 있는 메시지 엑시트에 의해 추가되고 채널의 수신 측에 있는 메시지 엑시트에 의해 검사됩니다. 예를 들면, 데이터를 인증하는 것은 암호화된 암호이거나 디지털 서명일 수 있습니다.

이 서비스가 애플리케이션 레벨에서 구현되면 더 효율적일 수 있습니다. 기본적인 요구사항은 메시지를 수신하는 애플리케이션 사용자가 메시지를 송신한 애플리케이션의 사용자를 식별하고 인증할 수 있어야 한다는 것입니다. 그러므로, 이 서비스를 애플리케이션 레벨에서 구현하는 것을 고려하는 것이 당연합니다. 추가 정보는 [300 페이지의 『API 엑시트와 API 교차 엑시트에서 ID 맵핑』](#)의 내용을 참조하십시오.

API 엑시트와 API 교차 엑시트에서 ID 맵핑

메시지를 받는 애플리케이션은 메시지를 전송한 애플리케이션의 사용자를 식별하고 인증할 수 있어야 합니다. 이 서비스는 일반적으로 애플리케이션 레벨에서 가장 잘 구현됩니다. API 엑시트는 다양한 방법으로 서비스를 구현할 수 있습니다.

개별 메시지의 레벨에서, 식별과 인증은 메시지의 송신자와 수신자의 두 사용자와 관계가 있는 서비스입니다. 기본적인 요구사항은 메시지를 수신하는 애플리케이션 사용자가 메시지를 송신한 애플리케이션의 사용자를 식별하고 인증할 수 있어야 한다는 것입니다. 요구사항은 양방향인 것이 아닌 단방향 인증이라는 것을 알아두십시오.

구현된 방법에 따라, 사용자와 애플리케이션은 서비스와 인터페이스되어 있거나, 대화해야 할 수도 있습니다. 또한, 서비스가 사용되는 때와 방법은 사용자와 애플리케이션이 있는 위치와 애플리케이션 자체의 성격에 따라 다

를 수 있습니다. 그러므로, 서비스를 링크 레벨이 아니라 애플리케이션 레벨에서 구현하는 것을 고려하는 것이 당연합니다.

이 서비스를 링크 레벨에서 구현하는 것을 고려하는 경우, 다음과 같은 문제를 해결해야 할 수 있습니다.

- 메시지 채널에서 어떻게 서비스를 필요로 하는 메시지에만 서비스를 적용할 것인가?
- 필요한 경우, 사용자와 애플리케이션을 어떻게 서비스와 인터페이스하거나 상호작용할 수 있게 할 것인가?
- 멀티 호핑(multi-hop) 상황에서, 목적지로 가는 둘 이상의 메시지 채널에서 메시지가 어디로 송신될 것인가? 서비스의 구성요소를 어디에서 호출할 것인가?

다음은 식별 및 인증 서비스를 애플리케이션 레벨에서 구현하는 방법의 몇몇 예입니다. 용어 *API 엑시트*는 API 엑시트 또는 API 교차 엑시트를 의미합니다.

- 애플리케이션이 큐에 메시지를 넣으면 API 엑시트가 Kerberos와 같은 트러스트 인증 서버에서 인증 토큰을 확보할 수 있습니다. API 엑시트가 이 토큰을 메시지 안의 애플리케이션 데이터에 추가할 수 있습니다. 메시지가 수신하고 있는 애플리케이션에 의해 검색될 때, 또 다른 API 엑시트가 인증 서버에게 토큰을 검사하여 송신자를 인증하라고 요청할 수 있습니다.
- 애플리케이션이 메시지를 큐에 넣을 때, API 엑시트가 다음 항목을 메시지의 애플리케이션 데이터에 추가할 수 있습니다.
 - 송신자의 디지털 인증서
 - 송신자의 디지털 서명

메시지 요약을 위한 다른 알고리즘이 사용 가능하면, API 엑시트가 사용했던 알고리즘의 이름을 포함할 수 있습니다.

메시지가 수신하고 있는 애플리케이션에 의해 검색될 때, 또 다른 API 엑시트가 다음 검사를 수행할 수 있습니다.

- API 엑시트가 루트 CA 인증서로 가는 인증서 체인을 통해 작업하여 디지털 인증서의 유효성을 검증할 수 있습니다. 이를 수행하려면 API 엑시트가 인증서 체인의 나머지 인증서를 포함하는 키 저장소에 액세스할 수 있어야 합니다. 이 검사는 식별 이름에 의해 식별되는 송신자가 인증서에 있는 공개키의 조작 및 변경되지 않은 순수한 소유자라는 것을 보장합니다.
- API 엑시트가 인증서에 있는 공개키를 사용하여 디지털 서명을 검사할 수 있습니다. 이 검사는 송신자를 인증합니다.

송신자의 식별 이름이 전체 디지털 인증서 대신에 송신될 수 있습니다. 이런 경우에, 키 저장소에 송신자의 인증서가 있어야 두 번째 API 엑시트가 송신자의 공개 키를 찾을 수 있습니다. 다른 가능성은 인증서 체인에 있는 모든 인증서를 송신하는 것입니다.

- 애플리케이션이 메시지를 큐에 넣을 때, 메시지 설명자의 *UserIdentifier* 필드에 애플리케이션과 연관된 사용자 ID가 있습니다. 사용자 ID는 송신자를 식별하는 데 사용될 수 있습니다. 인증을 가능하게 하려면, API 엑시트가 암호화된 암호와 같은 데이터를 메시지의 애플리케이션 데이터에 추가할 수 있습니다. 메시지가 수신하고 있는 애플리케이션에 의해 검색될 때, 또 다른 API 엑시트가 메시지와 함께 돌아다니는 데이터를 사용하여 사용자 ID를 인증할 수 있습니다.

이 기술은 제어되고 트러스트되는 환경 및 트러스트되는 인증 서버나 PKI 지원이 사용 불가능한 환경에서 작성된 메시지에 대해서 충분하다고 간주될 수 있습니다.

폐기된 인증서에 대한 작업

디지털 인증서는 인증 기관에 의해 폐기될 수 있습니다. 플랫폼에 따라 LDAP 서버의 CRL 또는 OCSP를 사용하여 인증서의 폐기 상태를 검사할 수 있습니다.

TLS 데이터 교환 중 통신하고 있는 파트너는 디지털 인증서를 사용하여 서로를 인증합니다. 인증은 수신된 인증서가 아직도 신뢰될 수 있는지를 검사하는 것을 포함할 수 있습니다. 인증 기관(CA)은 다음을 포함한 여러 가지 이유로 인증서를 폐기합니다.

- 소유자가 다른 조직으로 이동
- 개인 키가 더 이상 기밀이 아님

CA가 인증서 폐기 목록(CRL)에 폐기된 개인 인증서를 공개합니다. 폐기된 CA 인증서가 권한 취소 목록(ARL)에 공개됩니다.

다음 플랫폼에서 IBM MQ SSL 지원은 OCSP(Online Certificate Status Protocol)를 사용하거나 CRL 및 ARL을 사용하여 LDAP(Lightweight Directory Access Protocol) 서버에서 철회된 인증서를 검사합니다. OCSP가 기본 메소드입니다.

-  Linux
-  UNIX
-  Windows

IBM MQ classes for Java 및 IBM MQ classes for JMS에서는 클라이언트 채널 정의 테이블 파일에서 OCSP 정보를 사용할 수 없습니다. 그러나 [온라인 인증서 프로토콜 사용](#)에서 설명한 대로 OCSP를 구성할 수 있습니다.

다음 플랫폼에서 IBM MQ SSL 지원은 LDAP 서버에 한해 CRL 및 ARL을 사용하여 철회된 인증서를 검사합니다.

-  IBM i
-  z/OS

인증 기관에 대한 자세한 정보는 9 페이지의 『디지털 인증서』의 내용을 참조하십시오.

OCSP/CRL 검사

OCSP(Online Certificate Status Protocol)/CRL(Certificate Revocation List) 검사는 원격 수신 인증서에 대해 수행됩니다. 이 프로세스는 관련된 체인 전체를 원격 시스템의 개인 인증서부터 해당 루트 인증서까지 전부 검사합니다.

openSSL을 사용하여 OCSP 유효성 검증 확인

회사에서 OpenSSL을 사용하여 OCSP의 유효성을 검증하고 GSKit TLS 연결을 사용하려고 하면 UNKNOWN 상태 경고가 표시됩니다.

GSKit에서 루트를 제외하고 체인에 있는 모든 인증서의 취소 상태를 확인하기 때문입니다. GSKit 조작은 RFC 5280에 따르면 GSKit 신뢰 정책에 설명되어 있습니다. GSKit 알고리즘은 RFC 5280과 GSKit 신뢰 정책에 설명된 대로 사용 가능한 모든 정보에서 취소 정보를 확인합니다.

OCSP/CRL 검사가 IBM MQ에서 작동하는 방식

IBM MQ는 인증서 확장에 지정되어 있거나 AUTHINFO 오브젝트에 정의된, 이름 지정된 OCSP 또는 CRL 엔드포인트에 대해 인증서를 검사할 때의 제어 작동에 대해 두 가지 메커니즘을 지원합니다.

- [qm.ini 파일의 SSL 스탠자의 OCSPCheckExtensions, CDPCheckExtensions 및 OCSPAuthentication 속성](#)
- 큐 관리자의 SSLCRLNL 매개변수와 AUTHINFO OCSP 및 CRLLDAP 구성을 사용하여. 자세한 정보는 [ALTER AUTHINFO](#) 및 [ALTER QMGR](#)를 참조하십시오.



주의:

AUTHTYPE(OCSP)을 포함하는 ALTER AUTHINFO 명령은 IBM i 또는 z/OS 큐 관리자에 대한 사용에는 적용되지 않습니다. 그러나 클라이언트가 사용하도록 클라이언트 채널 테이블(CCDT)에 복사할 플랫폼에는 지정할 수 있습니다.

OCSPCheckExtensions 및 **CDPCheckExtensions** SSL 스탠자 속성은 IBM MQ가 인증서의 AIA 확장에 지정되어 있는 OCSP 또는 CRL 서버에 대해 인증서를 확인하는지 제어합니다.

사용으로 설정되지 않은 경우에는 인증서 확장에 있는 OCSP 또는 CRL 서버에 접속하지 않습니다.

AUTHINFO 오브젝트를 통해 OCSP 또는 CRL 서버가 설정되었으며 SSLCRLNL **QMGR** 속성을 사용하여 참조된 경우에는 인증서 폐기 처리 중에 IBM MQ가 이러한 서버에 접속하려 시도합니다.

중요사항: SSLCRLNL 이름 목록에는 하나의 OCSP AUTHINFO 오브젝트만 정의할 수 있습니다.

경우:

OCSPCheckExtensions=NO 및 **CDPCheckExtensions=NO**가 설정되었으며,
AUTHINFO 오브젝트에 OCSP 또는 CRL 서버가 정의되지 않은 경우

인증서 폐기 검사가 수행되지 않습니다.

확인이 사용으로 설정된 경우 IBM MQ는 인증서의 폐기 상태를 확인할 때 이름 지정된 OCSP 또는 CRL 서버에 다음 순서대로 접속합니다.

1. **AUTHTYPE(OCSP)** 오브젝트에 설정되었으며 **SSLCRLNL QMGR** 속성에서 참조하는 OCSP 서버
2. 인증서의 AIA 확장에 설정된 OCSP 서버(**OCSPCheckExtensions=YES**인 경우)
3. 인증서의 **CRLDistributionPoints** 확장에 설정된 CRL 서버(**CDPCheckExtensions=YES**인 경우)
4. **AUTHINFO(CRLLDAP)** 오브젝트에 설정되었으며 **SLCRLNL QMGR** 속성에서 참조하는 CRL 서버

인증서를 확인하는 중에, 특정 단계에서 OCSP 또는 CRL 서버가 인증서에 대해 결정적인 REVOKED 또는 VALID 응답을 리턴하는 경우에는 추가적인 검사가 수행되지 않으며 표시된 대로의 인증서 상태가 인증서의 신뢰 여부를 결정하는 데 사용됩니다.

OCSP 또는 CRL 서버가 UNKNOWN 결과를 리턴하는 경우에는 OCSP 또는 CRL 서버가 결정적인 결과를 리턴하거나 모든 옵션이 소진될 때까지 처리가 계속됩니다.

인증서를 폐기된 것으로 간주하거나, 상태를 판별할 수 없는 것으로 간주하는 작동은 OCSP 서버와 CRL 서버 간에 다릅니다.

- CRL 서버의 경우에는 CRL을 확보할 수 없는 경우 해당 인증서를 NOT_REVOKED로 간주합니다.
- OCSP 서버의 경우, 이름 지정된 OCSP 서버로부터 폐기 상태를 확보할 수 없으면 작동이 **qm.ini** 파일의 SSL 스탠자에 있는 **OCSPAuthentication** 속성을 통해 제어됩니다.

이 속성은 연결을 차단하거나, 연결을 허용하거나, 경고 메시지를 표시하며 연결을 허용하도록 구성할 수 있습니다.

필요한 경우에는 **qm.ini** 및 **mqclient.ini** 파일의 SSL 스탠자에 있는 **SSLHTTPProxyName=string** 속성을 OCSP 검사에 사용할 수 있습니다. 이 문자열은 GSKit이 OCSP 검사에 사용하는 HTTP 프록시 서버의 호스트 이름 또는 네트워크 주소입니다.

IBM MQ 9.1.5 에서 취소 확인을 수행할 때 OCSP 응답자가 대기하는 시간(초)을 설정하는 **qm.ini** 또는 **mqclient.ini** 파일의 SSL 스탠자에 **OCSPTimeout** 값을 설정할 수 있습니다.

폐기된 인증서 및 OCSP

IBM MQ는 사용할 OCSP(Online Certificate Status Protocol) 응답자를 판별하고, 수신한 응답을 핸들링합니다. OCSP 응답자에 액세스할 수 있도록 하는 단계를 수행해야 할 수도 있습니다.

참고: 이 정보는 UNIX, Linux, and Windows 시스템의 IBM MQ에만 적용됩니다.

OCSP를 사용하여 디지털 인증서의 폐기 상태를 검사하기 위해 IBM MQ는 두 개의 방법을 사용하여 어떤 OCSP 응답자에게 연락할지를 판별할 수 있습니다.

- 검사할 인증서에서 AIA(AuthorityInfoAccess) 인증서 확장자를 사용
- 인증 정보 오브젝트에 지정되거나 클라이언트 애플리케이션에 의해 지정된 URL 사용

인증 정보 오브젝트 또는 클라이언트 애플리케이션에서 지정한 URL은 AIA 인증서 확장자에 있는 URL보다 우선합니다.

OCSP 응답자의 URL이 방화벽 뒤에 놓인 경우 OCSP 응답자에 액세스할 수 있도록 방화벽을 재구성하거나 OCSP 프록시 서버를 설정하십시오. SSL 스탠자에 있는 **SSLHTTPProxyName** 변수를 사용하여 프록시 서버의 이름을 지정하십시오. 클라이언트 시스템에서는 환경 변수 **MQSSLPROXY**를 사용하여 프록시 서버의 이름을 지정할 수도 있습니다. 자세한 내용은 관련 정보를 참조하십시오.

아마도 테스트 환경에서 실행 중이므로 TLS 인증서의 폐기 여부가 중요하지 않으면, SSL 스탠자에서 **OCSPCheckExtensions**를 **아니오**로 설정할 수 있습니다. 이 변수를 설정하면 모든 AIA 인증서 확장자가 무시됩니다. 이 솔루션은 프로덕션 환경에서는 사용할 수 없습니다. 여기에서는 폐기된 인증서를 제시하는 사용자에게 액세스를 허용하지 않습니다.

OCSP 응답자 액세스 호출은 다음 세 가지 결과 중 하나를 초래할 수 있습니다.

보통

인증서가 올바릅니다.

해지됨




인증서가 폐기되었습니다.

알 수 없음

이 결과는 세 가지 중 하나의 이유로 발생할 수 있습니다.

- IBM MQ가 OCSP 응답자에 액세스할 수 없습니다.
- OCSP 응답자가 응답을 송신했으나 IBM MQ가 응답의 디지털 서명을 확인할 수 없습니다.
- OCSP 응답자가 인증서에 대한 폐기 데이터를 가지고 있지 않음을 표시하는 응답을 송신했습니다.

IBM MQ에서 알 수 없음의 OCSP 결과를 수신하는 경우 이에 따른 작동은 OCSPAuthentication 속성의 설정에 따라 다릅니다. 큐 관리자의 경우 이 속성은 다음 위치 중 하나에 보관됩니다.

-   UNIX and Linux의 경우 qm.ini 파일의 SSL 스탠자.
-  Windows 레지스트리.

이 속성은 IBM MQ Explorer를 사용하여 설정할 수 있습니다. 클라이언트의 경우 클라이언트 구성 파일의 SSL 스탠자에 속성이 저장됩니다.

알 수 없음 결과를 수신하고 OCSPAuthentication이 REQUIRED(기본값)로 설정되면, IBM MQ는 연결을 거부하고 AMQ9716 유형의 오류 메시지를 발행합니다. 큐 관리자 SSL 이벤트 메시지가 사용 가능한 경우, ReasonQualifier가 MQRQ_SSL_HANDSHAKE_ERROR로 설정된 MQR_CHANNEL_SSL_ERROR 유형의 SSL 이벤트 메시지가 생성됩니다.

알 수 없음 결과를 수신하고 OCSPAuthentication이 OPTIONAL로 설정되면, IBM MQ에서는 SSL 채널이 시작되고 경고 또는 SSL 이벤트 메시지는 생성되지 않습니다.

알 수 없음 결과를 수신하고 OCSPAuthentication이 WARN으로 설정된 경우, SSL 채널은 시작되지만 IBM MQ는 오류 로그에 AMQ9717 유형의 경고 메시지를 발행합니다. 큐 관리자 SSL 이벤트 메시지가 사용되는 경우에는 ReasonQualifier가 MQRQ_SSL_UNKNOWN_REVOCATION으로 설정된 MQR_CHANNEL_SSL_WARNING 유형의 SSL 이벤트 메시지가 생성됩니다.

OCSP 응답의 디지털 서명

OCSP 응답자는 세 가지 방법 중 하나를 사용하여 응답에 서명할 수 있습니다. 응답자는 사용되는 방법에 대해 사용자에게 알려줍니다.

- 검사 중인 인증서를 발행한 동일한 CA 인증서를 사용하여 OCSP 응답에 디지털로 서명할 수 있습니다. 이 경우 추가 인증서를 설정할 필요가 없습니다. TLS 연결을 설정하기 위해 이미 수행한 단계가 OCSP 응답을 확인하기에 충분합니다.
- OCSP 응답은 검사 중인 인증서를 발행한 것과 동일한 인증 기관(CA)이 서명한 또 다른 인증서를 사용하여 디지털로 서명할 수 있습니다. 이 경우 서명 인증서는 OCSP 응답과 함께 전송됩니다. OCSP 응답자로부터 전송된 인증서에는 이 용도로 신뢰할 수 있도록 id-kp-OCSPSigning으로 설정된 확장 키 사용 확장(Extended Key Usage Extension)이 있어야 합니다. OCSP 응답이 서명한 인증서와 함께 전송되므로(인증서는 이미 TLS 연결을 위해 신뢰된 CA가 서명함) 다른 추가 인증서 설정이 필요하지 않습니다.
- 검사 중인 인증서와 직접 관련이 없는 다른 인증서를 사용하여 OCSP 응답에 디지털로 서명할 수 있습니다. 이 경우 OCSP 응답은 OCSP 응답자 자체가 발행한 인증서에 의해 서명됩니다. OCSP 점검을 수행하는 큐 관리자나 클라이언트의 키 데이터베이스에 OCSP 응답자 인증서 사본을 추가해야 합니다. 272 페이지의 『UNIX, Linux, and Windows에서 CA 인증서 또는 자체 서명 인증서의 공용 부분을 키 저장소에 추가』의 설명을 참조하십시오. CA 인증서가 추가되면, 기본적으로 신뢰 루트로서 추가되며 이는 이 컨텍스트에서 필수 설정입니다. 이 인증서를 추가할 수 없으면, IBM MQ는 OCSP 응답에서 디지털 서명을 확인할 수 없고 OCSPAuthentication 값에 따라 OCSP 검사에서는 알 수 없음 결과를 발생시켜 IBM MQ에서 채널을 종료시킬 수 있습니다.

Java 및 JMS 클라이언트 애플리케이션에서 온라인 인증서 상태 프로토콜(OCSP)

Java API의 제한으로 인해, IBM MQ는 OCSP가 전체 Java 가상 머신(JVM) 프로세스에 대해 사용 가능한 경우에만 TLS 보안 소켓에 대해 온라인 인증서 상태 프로토콜(OCSP) 인증서 폐기 검사를 사용할 수 있습니다. JVM의 모든 보안 소켓에 대해 OCSP를 사용 가능으로 설정하는 방법은 두 가지가 있습니다.

- 테이블 1에 표시되는 OCSP 구성 설정을 포함하도록 JRE java.security 파일을 편집하고 애플리케이션을 재시작하십시오.
- 적용되는 모든 Java Security Manager 정책에 따라 java.security.Security.setProperty() API를 사용하십시오.

최소한 ocspl.enable 및 ocspl.responderURL 값 중 하나를 지정해야 합니다.

특성 이름	설명
ocsp.enable	이 특성 값은 true 또는 false입니다. true인 경우 인증서 폐기 검사를 수행할 때 OCSP 검사를 사용할 수 있고, false 또는 설정되지 않은 경우 OCSP 검사를 사용할 수 없습니다.
ocsp.responderURL	이 특성 값은 OCSP 응답자의 위치를 식별하는 URL입니다. 다음은 예입니다. ocspl.responderURL=http://ocsp.example.net:80. 기본적으로 OCSP 응답자의 위치는 유효성을 검증하는 인증서로부터 암시적으로 판별됩니다. 특성은 (RFC 3280에서 정의된) 권한 정보 액세스 확장 기능이 인증서에 없거나 대체해야 하는 경우 사용됩니다.
ocsp.responderCertSubjectName	이 특성 값은 OCSP 응답자의 인증서 제목 이름입니다. 다음은 예입니다. ocspl.responderCertSubjectName="CN=OCSP Responder, O=XYZ Corp". 기본적으로 OCSP 응답자의 인증서는 유효성을 검증하는 발행인의 인증서입니다. 이 특성은 기본이 적용되지 않을 경우 OCSP 응답자의 인증서를 식별합니다. 값은 인증서 경로 유효성 검증 도중 제공되는 인증서 세트에서 인증서를 식별하는 문자열 식별 이름(RFC 2253에서 정의됨)입니다. 제목 이름만으로는 인증서를 고유하게 식별하기에 부족한 경우, ocspl.responderCertIssuerName 및 ocspl.responderCertSerialNumber 특성 모두를 대신 사용해야 합니다. 이 특성이 설정되면 특성 ocspl.responderCertIssuerName 및 ocspl.responderCertSerialNumber는 무시됩니다.
ocsp.responderCertIssuerName	이 특성 값은 OCSP 응답자 인증서의 발행인 이름입니다. 다음은 예입니다. ocspl.responderCertIssuerName="CN=Enterprise CA, O=XYZ Corp". 기본적으로 OCSP 응답자의 인증서는 유효성을 검증하는 발행인의 인증서입니다. 이 특성은 기본이 적용되지 않을 경우 OCSP 응답자의 인증서를 식별합니다. 값은 인증서 경로 유효성 검증 도중 제공되는 인증서 세트에서 인증서를 식별하는 문자열 식별 이름(RFC 2253에서 정의됨)입니다. 이 특성이 설정되면 ocspl.responderCertSerialNumber 특성도 설정해야 합니다. ocspl.responderCertSubjectName 특성이 설정되면 이 특성은 무시합니다.
ocsp.responderCertSerialNumber	이 특성 값은 OCSP 응답자 인증서의 일련 번호입니다. 다음은 예입니다. ocspl.responderCertSerialNumber=2A:FF:00. 기본적으로 OCSP 응답자의 인증서는 유효성을 검증하는 발행인의 인증서입니다. 이 특성은 기본이 적용되지 않을 경우 OCSP 응답자의 인증서를 식별합니다. 값은 인증서 경로 유효성 검증 도중 제공되는 인증서 세트에서 인증서를 식별하는 16진 문자열(콜론이나 공백 분리문자가 있을 수 있음)입니다. 이 특성이 설정되면 ocspl.responderCertIssuerName 특성도 설정되어야 합니다. ocspl.responderCertSubjectName 특성이 설정되면 이 특성은 무시합니다.

이러한 방식으로 OCSP를 사용으로 설정하기 전에는 여러 가지를 고려해야 합니다.

- OCSP 구성의 설정값은 JVM 프로세스에 있는 모든 보안 소켓에 영향을 줍니다. 어떤 경우에는 JVM이 TLS 보안 소켓을 사용하는 다른 애플리케이션 코드와 공유될 때 이 구성에는 원하지 않는 역효과가 있을 수 있습니다. 선택된 OCSP 구성이 동일한 JVM에서 실행하는 모든 애플리케이션에 적합한지 확인하십시오.
- JRE에 유지보수를 적용하면 java.security 파일이 덮어쓰기됩니다. java.security 파일의 덮어쓰기를 피하려면 Java 임시 수정사항 및 제품 유지보수를 적용할 때 주의하십시오. 유지보수를 적용한 후 java.security 변경사항을 다시 적용해야 하는 경우도 있습니다. 이러한 이유로 java.security.Security.setProperty() API를 대신 사용한 OCSP 구성 설정을 고려할 수 있습니다.
- OCSP 검사 사용 설정은 폐기 검사도 사용으로 설정된 경우에만 효과가 있습니다. 폐기 검사는 PKIXParameters.setRevocationEnabled() 메소드에 의해 사용으로 설정됩니다.
- 원시 인터셉터에서 OCSP 확인 사용에 설명된 AMS Java 인터셉터를 사용하는 경우, 키 저장소 구성 파일에서 AMS OCSP 구성과 충돌하는 java.security OCSP 구성을 사용하지 않도록 주의하십시오.

인증서 폐기 목록(CRL) 및 권한 취소 목록(ARL) 관련 작업

CRL 및 ARL에 대한 IBM MQ 지원은 플랫폼마다 다릅니다.

각 플랫폼의 CRL 및 ARL 지원은 다음과 같습니다.

- z/OS에서, 시스템 SSL은 Tivoli Public Key Infrastructure(PKI) 제품에 의해 LDAP 서버에 저장된 CRL 및 ARL을 지원합니다.
- 다른 플랫폼에서 CRL 및 ARL 지원은 PKIX X.509 V2 CRL 프로파일 권장사항을 준수합니다.

IBM MQ는 앞서 12시간 동안 액세스된 CRL 및 ARL의 캐시를 유지합니다.

큐 관리자 또는 IBM MQ MQI client가 인증서를 수신하면 이는 인증서가 여전히 유효한지 확인하기 위해 CRL을 검사합니다. IBM MQ는 먼저 캐시가 있는 경우 캐시를 검사합니다. CRL이 캐시에 없으면 IBM MQ에서 사용 가능한 CRL을 찾을 때까지 SSLCRLNL 속성을 통해 지정한 인증 정보 오브젝트의 이름 목록에 표시되는 순서대로 IBM MQ에서 LDAP CRL 서버 위치를 조사합니다. 이름 목록이 지정되어 있지 않거나, 빈 값으로 지정되어 있으면, CRL이 검사되지 않습니다.

LDAP 서버 설정

CA의 식별 이름의 계층을 반영하여 LDAP 디렉토리 정보 트리 구조를 구성하십시오. LDAP 데이터 교환 형식 파일을 사용하여 이를 수행하십시오.

LDAP 디렉토리 정보 트리(DIT) 구조를 구성하여 인증서와 CRL을 발행하는 CA의 식별 이름(DN)에 해당하는 계층을 사용하십시오. LDAP 데이터 교환 형식(LDIF)을 사용하는 파일로 DIT 구조를 설정할 수 있습니다. 디렉토리를 업데이트하는 데 LDIF 파일을 사용할 수도 있습니다.

LDIF 파일은 LDAP 디렉토리 안에서 오브젝트를 정의하는 데 필요한 정보를 가지는 ASCII 텍스트 파일입니다. LDIF 파일에는 하나 이상의 항목이 있으며, 이들 각각은 식별 이름(DN), 적어도 하나의 오브젝트 클래스 정의와, 선택적으로 여러 속성 정의를 이룹니다.

certificateRevocationList;binary 속성에는 폐기된 사용자 인증서의 목록의 2진 형식이 있습니다. authorityRevocationList;binary 속성에는 취소된 CA 인증서의 2진 목록이 포함되어 있습니다. IBM MQ TLS와 함께 사용하기 위해 이러한 속성의 2진 데이터는 DER(Definite Encoding Rules) 형식을 준수해야 합니다. LDIF 파일에 대한 자세한 정보는 LDAP 서버와 함께 제공된 문서를 참조하십시오.

307 페이지의 그림 20 shows a sample LDIF file that you might create as input to your LDAP server to load the CRLs and ARLs issued by CA1, which is an imaginary Certificate Authority with the Distinguished Name "CN=CA1, OU=Test, O=IBM, C=GB", set up by the Test organization within IBM.

```

dn: o=IBM, c=GB
o: IBM
objectclass: top
objectclass: organization

dn: ou=Test, o=IBM, c=GB
ou: Test
objectclass: organizationalUnit

dn: cn=CA1, ou=Test, o=IBM, c=GB
cn: CA1
objectclass: cRLDistributionPoint
objectclass: certificateAuthority
authorityRevocationList;binary:: (DER format data)
certificateRevocationList;binary:: (DER format data)
caCertificate;binary:: (DER format data)

```

그림 20. 인증 기관의 샘플 LDIF 파일 이는 구현에 따라 달라질 수 있습니다.

307 페이지의 그림 21 shows the DIT structure that your LDAP server creates when you load the sample LDIF file shown in 307 페이지의 그림 20 together with a similar file for CA2, an imaginary Certificate Authority set up by the PKI organization, also within IBM.

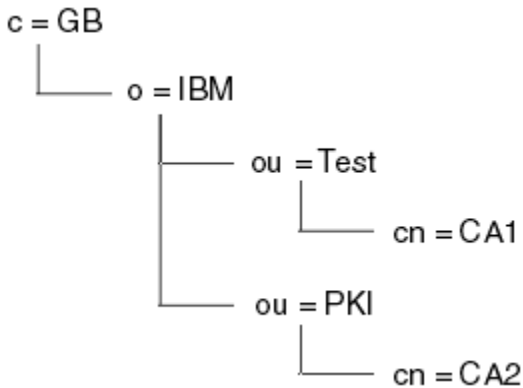


그림 21. LDAP 디렉토리 정보 트리(DIT) 구조의 예

WebSphere MQ는 CRL 및 ARL 둘 모두를 검사합니다.

참고: LDAP 서버의 액세스 제어 목록을 사용하여 권한이 부여된 사용자가 CRL과 ARL을 보유하는 항목을 읽고 검색하고 비교할 수 있는지 확인하십시오. WebSphere MQ는 AUTHINFO 오브젝트의 LDAPUSER 및 LDAPPWD 특성을 사용하여 LDAP 서버에 액세스합니다.

LDAP 서버 구성 및 업데이트

이 프로시저를 사용하여 LDAP 서버를 구성하거나 업데이트하십시오.

1. 인증 기관에서 DER 형식의 CRL 및 ARL을 확보하십시오.
2. 텍스트 편집기나 LDAP 서버에 제공되는 도구를 사용하여 CA의 식별 이름과 필요한 오브젝트 클래스 정의를 포함하는 하나 이상의 LDIF 파일을 작성하십시오. DER 형식 데이터를 CRL의 `certificateRevocationList;binary` 속성, ARL의 `authorityRevocationList;binary` 속성 값 또는 둘 모두로서 LDIF 파일에 복사하십시오.
3. LDAP 서버를 시작하십시오.
4. 307 페이지의 『2』 단계에서 작성한 LDIF 파일에서 항목을 추가하십시오.

LDAP CRL 서버를 구성한 후에 올바르게 설정되었는지 검사하십시오. 먼저, 채널에서 폐기되지 않은 인증서를 사용해 보고 채널이 올바르게 시작되는지 검사하십시오. 그런 다음, 폐기된 인증서를 사용한 후 채널 시작에 실패하는지 검사하십시오.

인증 기관으로부터 업데이트된 CRL을 자주 얻으십시오. LDAP 서버에서 12시간마다 확보하도록 하십시오.

큐 관리자로 CRL 및 ARL에 액세스

큐 관리자는 LDAP CRL 서버의 주소를 보유하는 하나 이상의 인증 정보 오브젝트와 연관되어 있습니다.

IBM i IBM i의 IBM MQ은 다른 플랫폼과 다르게 작동합니다.

이 절에 있는 인증서 폐기 목록(CRL)에 대한 정보는 권한 취소 목록(ARL)에도 적용됩니다.

큐 관리자에게 각각 LDAP CRL 서버의 주소를 보유하는 인증 정보 오브젝트를 제공하여 큐 관리자에게 CRL에 액세스하는 방법을 알려주십시오. 인증 정보 오브젝트는 `SSLCRLNL` 큐 관리자 속성에 지정된 이름 목록에 보유됩니다.

다음 예에서는 매개변수를 지정하는 데 MQSC가 사용됩니다.

1. AUTHTYPE 매개변수를 CRLLDAP으로 설정한 DEFINE AUTHINFO MQSC 명령을 사용하여 인증 정보 오브젝트를 정의하십시오. **IBM i** IBM i에서는 CRTMQMAUTI CL 명령도 사용할 수 있습니다.

AUTHTYPE 매개변수의 CRLLDAP 값은 LDAP 서버에서 CRL에 액세스됨을 나타냅니다. 사용자가 작성한 CRLLDAP 유형을 가진 각 인증 정보 오브젝트는 LDAP 서버의 주소를 보유합니다. 둘 이상의 인증 정보 오브젝트를 가지고 있는 경우, 이러한 오브젝트가 가리키는 LDAP 서버에 동일한 정보가 있어야 합니다. 이렇게 하면 하나 이상의 LDAP 서버가 실패하는 경우에 서비스의 지속성을 제공합니다.

z/OS 또한 z/OS에서만, 모든 LDAP 서버는 동일 사용자 ID 및 비밀번호를 사용하여 액세스되어야 합니다. 사용되는 사용자 ID와 암호는 이름 목록의 첫 번째 AUTHINFO 오브젝트에 지정된 것입니다.

모든 플랫폼에서 사용자 ID와 비밀번호는 암호화되지 않은 LDAP 서버에 전송됩니다.

2. DEFINE NAMLIST MQSC 명령을 사용하여, 인증 정보 오브젝트의 이름에 이름 목록을 정의하십시오.

z/OS z/OS에서는 NLTYPE 이름 목록 속성이 AUTHINFO로 설정되는지 확인하십시오.

3. ALTER QMGR MQSC 명령을 사용하여 큐 관리자에 이름 목록을 제공하십시오. 예를 들면, 다음과 같습니다.

```
ALTER QMGR SSLCRLNL(sslcrlnlname)
```

여기서, `sslcrlnlname`은 인증 정보 오브젝트의 이름 목록입니다.

이 명령은 `SSLCRLNL`이라는 큐 관리자 속성을 설정합니다. 이 속성에 대한 큐 관리자의 초기값은 공백입니다.

IBM i IBM i에서 인증 정보 오브젝트를 지정할 수 있지만 큐 관리자는 인증 정보 오브젝트 또는 인증 정보 오브젝트의 이름 목록을 사용할 수 없습니다. IBM i 큐 관리자가 생성한 클라이언트 연결 테이블을 사용하는 IBM MQ 클라이언트만 해당 IBM i 큐 관리자에 지정된 인증 정보를 사용합니다. IBM i의 `SSLCRLNL` 큐 관리자 속성은 클라이언트가 사용하는 인증 정보를 판별합니다. IBM i 큐 관리자에게 CRL에 액세스하는 방법에 대한 정보는 [308 페이지의 『IBM i에서 CRL 및 ARL에 액세스』](#)를 참조하십시오.

최대 10개의 대체 LDAP 서버에 대한 연결을 이름 목록에 추가하여 하나 이상의 LDAP 서버가 실패하는 경우에 서비스의 지속성을 보장할 수 있습니다. LDAP 서버에는 동일한 정보가 있어야 합니다.

IBM i IBM i에서 CRL 및 ARL에 액세스

IBM i에서 CRL 또는 ARL에 액세스하려면 이 프로시저를 사용하십시오.

이 절에 있는 인증서 폐기 목록(CRL)에 대한 정보는 권한 취소 목록(ARL)에도 적용됩니다.

IBM i에서 특정 인증서에 대해 CRL 위치를 설정하려면 다음 단계를 수행하십시오.

1. [245 페이지의 『DCM 액세스』](#)에 설명된 대로 DCM 인터페이스에 액세스하십시오.
2. 검색 패널의 **CRL 위치 관리** 작업 범주에서 **CRL 위치 추가**를 누르십시오. CRL 위치 관리 페이지가 작업 프레임에 표시됩니다.
3. **CRL 위치 이름** 필드에 CRL 위치 이름을 입력하십시오 (예: LDAP Server #1).
4. **LDAP 서버** 필드에 LDAP 서버 이름을 입력하십시오.
5. **SSL(Secure Sockets Layer)** 필드에서, TLS를 사용하여 LDAP 서버에 연결하려면 **예**를 선택하십시오. 그렇지 않으면 **아니오**를 선택합니다.
6. **포트 번호** 필드에 LDAP 서버의 포트 번호를 입력하십시오(예: 389).

7. LDAP 서버가 익명 사용자의 디렉토리 조회를 허용하지 않는 경우, **로그인 식별 이름** 필드에 이 서버의 로그인 식별 이름을 입력하십시오.
8. **확인**을 클릭하십시오. DCM이 CRL 위치를 작성했음을 알려줍니다.
9. 탐색 패널에서 **인증서 저장소 선택**을 클릭하십시오. 인증서 저장소 선택 페이지가 태스크 프레임에 표시됩니다.
10. **다른 시스템 인증서 저장소** 선택란을 선택한 후 **계속**을 클릭하십시오. 인증서 저장소 및 비밀번호 페이지가 표시됩니다.
11. **인증서 저장소 경로 및 파일 이름** 필드에 246 페이지의 『IBM i에서 인증서 저장소 작성』에서 설정한 IFS 경로 및 파일 이름을 입력하십시오.
12. **인증서 저장소 비밀번호** 필드에 비밀번호를 입력하십시오. **계속**을 클릭하십시오. 현재 인증서 저장소 페이지가 태스크 프레임에 표시됩니다.
13. 검색 패널의 **인증서 관리** 작업 범주에서 **CRL 위치 지정 업데이트**를 클릭하십시오. CRL 위치 지정 페이지가 작업 프레임에 표시됩니다.
14. CRL 위치를 지정하려는 CA 인증서의 단일 선택 단추를 선택하십시오. **CRL 위치 지정 업데이트**를 클릭하십시오. CRL 위치 지정 업데이트 페이지가 작업 프레임에 표시됩니다.
15. 인증서에 지정하려는 CRL 위치의 단일 선택 단추를 선택하십시오. **인증 업데이트**를 클릭하십시오. DCM이 지정을 업데이트했음을 알려줍니다.

DCM은 사용자가 인증 기관별로 다른 LDAP 서버를 지정하도록 허용함을 유의하십시오.

*IBM MQ Explorer*를 사용하여 CRL 및 ARL에 액세스

IBM MQ Explorer를 사용하여 큐 관리자에게 CRL에 액세스하는 방법을 알려줄 수 있습니다.

이 절에 있는 인증서 폐기 목록(CRL)에 대한 정보는 권한 취소 목록(ARL)에도 적용됩니다.

CRL에 LDAP 연결을 설정하려면 다음 프로시저를 사용하십시오.

1. 큐 관리자를 시작했는지 확인하십시오.
2. **인증 정보** 폴더를 마우스 오른쪽 단추로 클릭하고 **새로 작성 -> 인증 정보**를 클릭하십시오. 열리는 등록 정보 시트에서 다음과 같이 하십시오.
 - a. 첫 페이지인 **인증 정보 작성**에서 CRL(LDAP) 오브젝트에 이름을 입력하십시오.
 - b. **특성 변경의 일반** 페이지에서 연결 유형을 선택하십시오. 선택적으로 설명을 입력할 수 있습니다.
 - c. **특성 변경의 CRL(LDAP)** 페이지를 선택하십시오.
 - d. 네트워크 이름이나 IP 주소로 LDAP 서버 이름을 입력하십시오.
 - e. 서버가 로그인 세부사항을 필요할 경우, 사용자 ID와 암호(필요 시)를 제공하십시오.
 - f. **확인**을 클릭하십시오.
3. 이름 목록 폴더를 마우스 오른쪽 단추로 클릭하고 **새로 작성 -> 이름 목록**을 클릭하십시오. 열리는 등록 정보 시트에서 다음과 같이 하십시오.
 - a. 이름 목록에 이름을 입력하십시오.
 - b. CRL(LDAP) 오브젝트의 이름을(309 페이지의 『2.a』 단계로부터) 목록에 추가하십시오.
 - c. **확인**을 클릭하십시오.
4. 큐 관리자를 마우스 오른쪽 단추로 클릭하고 **특성**을 선택하고, **SSL** 페이지를 선택하십시오.
 - a. 인증서 폐기 목록(CRL)에 대해 이 큐 관리자가 수신한 인증서 검사 선택란을 선택하십시오.
 - b. **CRL 이름 목록** 필드에 이름 목록의 이름(309 페이지의 『3.a』 단계로부터)을 입력하십시오.

IBM MQ MQI client를 사용하여 CRL 및 ARL에 액세스

IBM MQ MQI client에 의해 검사를 위해 CRL을 보유하는 LDAP 서버를 지정하는 세 가지 옵션이 있습니다.

이 절에 있는 인증서 폐기 목록(CRL)에 대한 정보는 권한 취소 목록(ARL)에도 적용됩니다.

LDAP 서버를 지정하는 3가지 방법은 다음과 같습니다.

- 채널 정의 테이블 사용

- MQCONNX 호출에서 SSL 구성 옵션 구조인 MQSCO 사용
 - Active Directory를 지원하는 Windows 시스템에서 Active Directory 사용
- 자세한 내용은 관련 정보를 참조하십시오.


10개까지의 연결을 대체 LDAP 서버에 포함시켜 하나 이상의 LDAP 서버가 실패할 경우 서비스의 지속성을 보장할 수 있습니다. LDAP 서버에는 동일한 정보가 있어야 합니다.

Linux (zSeries 실행 중인 IBM MQ MQI client 채널에서 LDAP CRL에 액세스할 수 없습니다.

OCSP 응답자 및 CRL을 보유하는 LDAP 서버의 위치

IBM MQ MQI client 시스템에서 OCSP 응답자의 위치 및 인증서 폐기 목록(CRL)을 보유하는 LDAP(Lightweight Directory Access Protocol) 서버의 위치를 지정할 수 있습니다.

여기에 나와 있는 세 가지 방식으로(아래로 갈수록 우선순위가 낮아짐) 이 위치를 지정할 수 있습니다.

 IBM i의 경우 IBM i에서 CRL 및 ARL 액세스를 참조하십시오.

IBM MQ MQI client 애플리케이션이 MQCONNX 호출을 실행할 때



MQCONNX 호출에 OCSP 응답자 또는 CRL을 보유하는 LDAP 서버를 지정할 수 있습니다.

MQCONNX 호출에서 연결 옵션 구조, MQCNO은 SSL 구성 옵션 구조, MQSCO를 참조할 수 있습니다. 대신 MQSCO 구조는 하나 이상의 인증 정보 레코드 구조, MQAIR을 참조할 수 있습니다. 각 MQAIR 구조에는 IBM MQ MQI client가 OCSP 응답자 또는 CRL을 보유하는 LDAP 서버에 액세스하기 위해 필요한 모든 정보가 포함되어 있습니다. 예를 들어, MQAIR 구조의 필드 중 하나는 응답자가 접속할 수 있는 URL입니다. MQAIR 구조에 대한 자세한 정보는 [MQAIR - 인증 정보 레코드](#)를 참조하십시오.

OCSP 응답자 또는 LDAP 서버에 액세스하기 위해 클라이언트 채널 정의 테이블(ccdt) 사용

IBM MQ MQI client가 OCSP 응답자 또는 CRL을 보유하는 LDAP 서버에 액세스할 수 있도록 클라이언트 채널 정의 테이블에 하나 이상의 인증 정보 오브젝트의 속성을 포함하십시오.

서버 큐 관리자에서 하나 이상의 인증 정보 오브젝트를 정의할 수 있습니다. 인증 오브젝트의 속성은 OCSP 응답자(OCSP가 지원되는 플랫폼에서) 또는 CRL을 보유하는 LDAP 서버에 액세스하기 위해 필요한 모든 정보를 포함합니다. 속성 중 하나는 OCSP 응답자 URL을 지정하고, 또 다른 하나는 LDAP 서버가 실행될 수 있는 시스템의 호스트 주소 또는 IP 주소를 지정합니다.

  AUTHTYPE(OCSP)이 있는 인증 정보 오브젝트는 IBM i 또는 z/OS 큐 관리자에서 사용하도록 적용되지 않지만 해당 플랫폼에서 클라이언트용으로 클라이언트 채널 정의 테이블(CCDT)에 복사되도록 지정될 수 있습니다.

OCSP 응답자 또는 CRL을 보유하는 LDAP 서버에 액세스하기 위해 IBM MQ MQI client를 사용 가능으로 설정하려면 하나 이상의 인증 정보 오브젝트의 속성이 클라이언트 채널 정의 테이블에 포함될 수 있습니다. 다음 방법 중 하나로 이러한 속성을 포함할 수 있습니다.

 Multi

서버 플랫폼 AIX, Linux, IBM i, Solaris 및 Windows에서

하나 이상의 인증 정보 오브젝트의 이름을 포함하는 이름 목록을 정의할 수 있습니다. 그런 다음 큐 관리자 속성, **SSLCRLNL**을 이 이름 목록의 이름으로 설정할 수 있습니다.

CRL을 사용 중인 경우 둘 이상의 LDAP 서버가 보다 높은 사용 가능성을 제공하도록 구성할 수 있습니다. 이는 각 LDAP 서버가 동일한 CRL을 보유하도록 하기 위한 것입니다. 한 LDAP 서버가 필요할 때 사용할 수 없는 경우, IBM MQ MQI client는 다른 서버에 액세스하려고 시도할 수 있습니다.

이름 목록으로 식별되는 인증 정보 오브젝트의 속성이 여기에서는 집합적으로 인증서 폐기 위치로 참조됩니다. 큐 관리자 속성, **SSLCRLNL**을 이름 목록의 이름으로 설정하면 인증서 폐기 위치가 큐 관리자와 연관된 클라이언트 채널 정의 표에 복사됩니다. CCDT를 공유 파일로서 클라이언트 시스템으로부터 액세스할 수 있거나 CCDT가 클라이언트 시스템에 복사되는 경우, 해당 시스템의 IBM MQ MQI client는 CCDT에서 인증서 폐기 위치를 사용하여 OCSP 응답자 또는 CRL을 보유하는 LDAP 서버에 액세스할 수 있습니다.

큐 관리자의 인증서 폐기 위치가 나중에 변경되면 변경사항이 큐 관리자와 연관된 CCDT에 반영됩니다. 큐 관리자 속성 **SSLCRLNL**이 공백으로 설정되면 CCDT에서 인증서 폐기 위치가 제거됩니다. 이들 변경사항은 클라이언트 시스템의 테이블 사본에 반영되지 않습니다.

MQI 채널에서 클라이언트 및 서버 끝의 인증서 폐기 위치가 달라야 하고 서버 큐 관리자가 인증서 폐기 위치를 작성하는 데 사용되는 경우 다음을 수행할 수 있습니다.

1. 서버 큐 관리자에서 클라이언트 시스템에 사용할 인증서 폐기 위치를 작성하십시오.
2. 인증서 폐기 위치가 포함된 CCDT를 클라이언트 시스템에 복사하십시오.
3. 서버 큐 관리자에서 MQI 채널의 서버 측에 필요한 정보로 인증서 폐기 위치를 변경하십시오.
4. 클라이언트 시스템에서 **runmqsc** 명령을 **-n** 매개변수와 함께 사용할 수 있습니다.

Multi

클라이언트 플랫폼 AIX, Linux, IBM i, Solaris 및 Windows에서

runmqsc 명령을 CCDT 파일에 있는 **-n** 매개변수 및 **DEFINE AUTHINFO** 오브젝트와 함께 사용하여 클라이언트 시스템에 CCDT를 빌드할 수 있습니다. 오브젝트가 정의되는 순서는 이들이 파일에서 사용되는 순서입니다. **DEFINE AUTHINFO** 오브젝트에서 사용할 수 있는 모든 이름은 파일에 보관되지 않습니다. 유일한 자릿수는 **AUTHINFO** 오브젝트를 CCDT 파일에 **DISPLAY**할 때 사용됩니다.

참고: **-n** 매개변수를 지정하는 경우 다른 매개변수를 지정하지 않아야 합니다.

Windows에서 Active Directory 사용

Windows

Windows 시스템에서 **setmqcrl** 제어 명령을 사용하여 Active Directory에서 현재 CRL 정보를 공개할 수 있습니다.

setmqcrl 명령은 OCSP 정보를 공개하지 않습니다.

이 명령 및 해당 구문에 대한 자세한 정보는 [setmqcrl](#)의 내용을 참조하십시오.

IBM MQ classes for Java 및 **IBM MQ classes for JMS**를 사용하여 **CRL** 및 **ARL**에 액세스

IBM MQ classes for Java 및 IBM MQ classes for JMS는 다른 플랫폼에서와 다르게 CRL에 액세스합니다.

IBM MQ classes for Java에서 CRL 및 ARL에 대한 작업의 정보는 [인증서 폐기 목록 사용](#)을 참조하십시오.

IBM MQ classes for JMS에서 CRL 및 ARL에 대한 작업 정보는 [SSLCERTSTORES 오브젝트 특성](#)을 참조하십시오.

인증 정보 오브젝트 조작

MQSC 또는 PCF 명령 또는 IBM MQ Explorer를 사용하여 인증 정보 오브젝트를 조작할 수 있습니다.

다음 MQSC 명령이 인증 정보 오브젝트에 대해 수행합니다.

- DEFINE AUTHINFO
- ALTER AUTHINFO
- DELETE AUTHINFO
- DISPLAY AUTHINFO

이러한 명령에 대한 완전한 설명은 [MQSC 명령](#)을 참조하십시오.

다음 프로그래밍 가능 명령 형식(PCF) 명령이 인증 정보 오브젝트에 대해 수행합니다.

- 인증 정보 작성
- 인증 정보 복사
- 인증 정보 변경
- 인증 정보 삭제
- 인증 정보 조회

- 인증 정보 이름 조회

이러한 명령의 전체 설명은 [프로그램 가능한 명령 형식의 정의를](#) 참조하십시오.

사용 가능한 플랫폼에서 IBM MQ Explorer를 사용할 수도 있습니다.

Linux UNIX 플러그 가능한 인증 방법(PAM) 사용

UNIX and Linux 플랫폼에서만 PAM을 사용할 수 있습니다. 일반적 UNIX 시스템에는 일반 인증 메커니즘을 구현하는 PAM 모듈이 있지만 더 있을 수도 있습니다. 비밀번호 유효성 검증의 기본 태스크뿐만 아니라 PAM 모듈은 또한 추가 규칙을 수행하기 위해 호출될 수도 있습니다.

구성 파일은 각 애플리케이션에 어떤 인증 방법이 사용될지를 정의합니다. 예 애플리케이션에는 표준 터미널 로그인, ftp 및 텔넷이 포함됩니다.

PAM의 장점은 애플리케이션이 사용자 ID가 실제로 인증되는 방법에 대해서 알 필요가 없고 관심을 갖지 않는다는 것입니다. 애플리케이션이 올바른 인증 데이터 양식을 PAM에 제공할 수 있는 한 그 뒤에 있는 메커니즘은 투명합니다.

인증 데이터의 양식은 사용 중인 시스템에 달려 있습니다. 예를 들어, IBM MQ 는 매개변수를 통해 암호를 얻습니다(예: MQCONN API 호출에서 사용되는 [MQCSP](#) 구조).

중요사항: IBM MQ 8.0.0 Fix Pack 3를 설치할 때까지 **AUTHENMD** 속성을 설정한 다음 **802 (strmqm 명령에서)의 -e CMDLEVEL=레벨** 을 사용하여 큐 관리자를 재시작하여 필요한 명령 레벨을 설정할 수 없습니다.

PAM을 사용하도록 시스템 구성

PAM을 호출할 때 IBM MQ가 사용하는 서비스 이름은 *ibmmq*입니다.

IBM MQ 설치하는 다른 운영 체제의 알려진 기본값을 기반으로 운영 체제 사용자로부터의 연결을 사용하는 기본 PAM 구성을 유지보수하려고 시도함을 유의하십시오.

그러나 시스템 관리자가 `/etc/pam.conf` 또는 `/etc/pam.d/ibmmq` 파일에 정의된 규칙이 여전히 적절인지 확인해야 합니다.

오브젝트에 액세스 권한 부여

이 절에는 오브젝트에 대한 액세스를 제어하기 위해 오브젝트 권한 관리자 및 채널 엑시트 프로그램 사용에 대한 정보가 포함되어 있습니다.

ULW UNIX, Linux, and Windows 시스템에서. 오브젝트 권한 관리자(OAM)를 사용하여 오브젝트에 대한 액세스를 제어합니다. 이 토픽 콜렉션에는 OAM에 대한 명령 인터페이스 사용에 대한 정보가 포함됩니다.

이 절에는 모든 플랫폼에서 사용자 시스템에 보안을 적용하기 위해 수행할 태스크를 결정하기 위한 체크리스트와, IBM MQ를 관리하고 IBM MQ 오브젝트에 대해 작업할 수 있는 권한을 부여할 때의 고려사항도 포함되어 있습니다.

제공된 보안 메커니즘이 사용자의 필요를 충족시키지 않은 경우 사용자 고유의 채널 엑시트 프로그램을 개발할 수 있습니다.

권한 부여에 사용되는 사용자 판별

자원에 액세스할 수 있는 권한은 사용자가 구성원인 그룹에 부여되거나 특정 모드에서 연결과 연관된 사용자에게 직접 부여됩니다. 연결 프로세스 중, 특히 리모트(클라이언트) 연결의 경우, 이 ID는 큐 관리자의 구성에 의해 변경될 수 있습니다. 이 페이지에는 연결 애플리케이션의 ID 및 이러한 기능이 적용되는 우선순위에 영향을 줄 수 있는 IBM MQ의 다양한 기능 및 해당 구성 옵션이 나열되어 있습니다.

채택된 사용자를 수정할 수 있는 기능

권한을 부여해야 하는 사용자를 설정할 수 있는 다른 기능은 다음과 같습니다.

애플리케이션 확인 사용자

IBM MQ에서 원격 연결을 시작하면 프로세스가 실행 중인 운영 체제 사용자가 수신 큐 관리자로 송신됩니다. 이 사용자는 사용자를 수정하는 추가 구성이 없는 경우 권한 검사에 사용할 수 있는 사용자가 있는지 확인하기 위해 전송됩니다.

서버 측 유효성 검증 없이 연결이 해당 ID를 어설션할 수 있으므로 이 사용자를 권한 부여의 기초로 사용하는 것은 권장되지 않습니다. 여기에는 관리 사용자('mqm')도 포함될 수 있습니다.

채널 MCAUSER 설정

네트워크 바인딩을 통해 연결하는 애플리케이션은 IBM MQ 채널 정의를 사용하여 이를 수행합니다. 채널 정의는 **MCAUSER** 속성을 지원합니다. 이 속성을 사용하여 연결 애플리케이션에서 어설션한 사용자 대신 권한 부여에 사용할 다른 사용자를 지정할 수 있습니다.

연결 인증 ADOPTCTX

애플리케이션은 인증을 위해 큐 관리자에 송신할 사용자 및 비밀번호를 지정할 수 있습니다. 이러한 신임 정보는 연결 인증 기능에 지정된 구성을 사용하여 인증됩니다. 연결 인증을 위한 **ADOPTCTX** 옵션은 사용자가 성공적으로 유효성 검증된 후 권한 부여에 사용되어야 하는지 여부를 제어합니다. YES로 설정하면 인증을 위해 제공되는 사용자가 권한 검사를 위해 채택됩니다.

채널 인증 레코드 MCAUSER

연결 처리 중에 큐 관리자가 연결과 일치하는 채널 인증 레코드를 찾으려고 시도합니다. 채널 인증 레코드가 일치하고 해당 **USERSRC** 속성 값이 MAP으로 설정된 경우, IBM MQ는 권한 부여에 사용되는 사용자를 **MCAUSER** 속성의 값으로 변경합니다.

보안 엑시트

보안 엑시트는 IBM MQ 보안 처리 중에 작성하고 호출할 수 있는 사용자 정의 함수입니다. 함수가 호출되면 권한 검사에 사용될 연결 사용자와 관련된 여러 필드를 포함하는 MQCD 구조의 사본과 함께 제공됩니다. 보안 엑시트는 이러한 필드를 수정하여 권한을 부여할 사용자를 변경할 수 있습니다.

우선 순서

다음 표는 IBM MQ가 권한을 부여할 사용자를 선택할 때 312 페이지의 『채택된 사용자를 수정할 수 있는 기능』에 설명된 각 보안 기능의 우선순위를 표시합니다. 순서는 가장 낮은 행부터 가장 높은 행까지입니다. 즉, 첫 번째 행에서 사용자를 설정하는 보안 기능은 다른 행으로 대체됩니다.

표 68. 보안 기능의 우선순위	
순서	기능
1 (최저값)	애플리케이션 확인 ID
2	채널 정의 MCAUSER 속성
3	ADOPTCTX(YES) 를 사용한 연결 인증
4	USERSRC(MAP) 의 채널 인증 레코드
5 (최고)	보안 엑시트

초기 채택의 영향

연결 인증 및 채널 인증 레코드는 연결 인증 사용자 채택이 수행되는 시기를 제어하는 구성 옵션을 제공합니다. 이 설정을 초기 채택이라고 합니다. 초기 채택이 사용으로 설정된 경우 채널 인증 레코드가 처리되기 전에 연결 인증 ID 채택이 발생합니다 (즉, 채널 인증 레코드가 **CONNAUTH** 채택을 대체함).

사용 안함으로 설정하면 순서가 반대로 됩니다. 즉, **CONNAUTH** 채택 전에 채널 인증 레코드가 처리됩니다. 이 상황에서 연결 인증 채택은 채널 인증이 기록하는 것보다 더 높은 유효 우선순위를 가집니다.

초기 채택의 기본 설정은 사용입니다.

UNIX, Linux, and Windows에서 OAM을 사용하여 오브젝트에 대한 액세스 제어

오브젝트 권한 관리자(OAM)는 IBM MQ 오브젝트에 권한을 부여하고 권한 취소하기 위한 명령 인터페이스를 제공합니다.

361 페이지의 『UNIX, Linux, and Windows에서 IBM MQ를 관리하는 권한』에서 설명한 바와 같이 이러한 명령을 사용할 적합한 권한을 가지고 있어야 합니다. IBM MQ를 관리할 권한이 있는 사용자 ID에는 큐 관리자에 대한 슈퍼유저 권한을 가지고 있습니다. 이는 이들에게 MQI 요청이나 명령을 실행하기 위해 추가 권한을 부여할 필요가 없다는 의미입니다.

Linux

UNIX

UNIX and Linux의 OAM 사용자 기반 권한

IBM MQ 8.0부터는 UNIX and Linux 시스템에서 오브젝트 권한 관리자(OAM)가 사용자 기반 권한과 그룹 기반 권한을 모두 사용할 수 있습니다.

IBM MQ 8.0 이전에, UNIX and Linux의 액세스 제어 목록(ACL)은 그룹 전용 기반이었습니다. IBM MQ 8.0에서 ACL은 사용자 ID 및 그룹을 기반으로 하며 설치 가능 서비스 구성 및 UNIX 및 Linux에서 권한 부여 서비스 스탠자 구성에 설명된 대로 **SecurityPolicy** 속성을 적절한 값으로 설정하여 권한 부여를 위해 사용자 기반 모델 또는 그룹 기반 모델을 사용할 수 있습니다.

IBM MQ 8.0 이상에서 작동의 변경사항

IBM MQ 8.0부터, 사용자 기반 정책으로 실행할 때 일부 명령은 이전 버전의 제품과 다른 정보를 리턴합니다.

- **dmpmqaut** 및 **dmpmqcfg** 명령은 PCF와 동등한 조작과 마찬가지로 사용자 기반 레코드를 표시합니다.
- IBM MQ Explorer의 OAM 플러그인이 사용자 기반 레코드를 표시하고 사용자 기반 수정을 허용합니다.
- OAM **Inquire** 기능은 사용자가 수행할 수 있는 작업을 표시하는 결과를 리턴합니다.

setmqaut 명령에서 **-p** 속성을 사용하면 **qm.ini** 서비스 스탠자에 설명된 대로 **qm.ini** 파일에서 사용자 기반 권한 부여가 사용 가능한 경우 동일한 기본 그룹의 모든 사용자에게 액세스 권한을 부여하지 않습니다.

사용자 기반 권한을 적용하기 시작하고 다수의 사용자가 있는 경우, 그룹 기반 모델을 사용하는 것보다 AUTH 큐에 저장된 더 많은 레코드가 있을 수 있으며 권한 부여 프로세스에는 확인할 레코드가 더 많기 때문에 이전에 비해 더 오랜 시간이 걸릴 수 있습니다. 이 시간 증가는 그다지 크지 않아야 합니다. 필요할 경우 사용자와 그룹 권한의 혼합을 사용할 수 있습니다.

마이그레이션 고려사항

그룹에서 기존 큐 관리자에 대한 사용자로 모델을 변경할 경우, 즉각적인 효과는 없습니다. 이미 작성된 권한이 계속해서 적용됩니다. 큐 관리자에 연결된 사용자는 이전과 동일한 권한을 받습니다(해당 ID가 속한 모든 그룹의 결합). 새 **setmqaut** 명령이 사용자 ID에 발행되면 이는 즉시 적용됩니다.

사용자 정책을 사용하여 새 큐 관리자를 작성하는 경우, 이 큐 관리자는 해당 큐 관리자를 작성하는 사용자(일반적으로 반드시 **mqm** 사용자 ID일 필요는 없음)에 대한 권한만 가질 수 있습니다. 자동으로 **mqm** 그룹에 부여되는 권한도 있습니다. 그러나 기본 그룹으로서 **mqm**을 가지고 있지 않으면 **mqm** 그룹은 초기 권한부여 세트에 포함되지 않습니다.

사용자에서 그룹 정책으로 이동할 경우, 사용자 기반 권한이 자동으로 삭제되지 않습니다. 그러나 권한 검사 동안에는 더 이상 사용되지 않습니다. 정책을 되돌리기 전에 현재 구성을 저장하고 정책을 변경하고 큐 관리자를 다시 시작한 후 스크립트를 재생하십시오. 이제 이는 그룹 기반 큐 관리자이므로 해당 사용자 ID 규칙이 기본 그룹을 기반으로 저장되는 효과가 나타납니다.

관련 개념

OAM(Object Authority Manager)

UNIX, Linux 및 Windows의 프린시פל 및 그룹

qm.ini 파일의 Service 스탠자

관련 참조

crtmqm(큐 관리자 작성) 명령

setmqaut 제어 명령, **SET AUTHREC** MQSC 명령 또는 **MQCMD_SET_AUTH_REC** PCF 명령을 사용하여 사용자 및 사용자 그룹에게 IBM MQ 오브젝트에 대한 액세스를 제공하십시오. IBM MQ Appliance 에서는 **SET AUTHREC** 명령만 사용할 수 있습니다.

setmqaut 제어 명령 및 해당 구문의 전체 정의에 대해서는 [setmqaut](#)의 내용을 참조하십시오.

SET AUTHREC MQSC 명령 및 해당 구문의 전체 정의에 대해서는 [SET AUTHREC](#)의 내용을 참조하십시오.

MQCMD_SET_AUTH_REC PCF 명령 및 해당 구문의 전체 정의에 대해서는 [권한 레코드 설정](#)을 참조하십시오.

이 명령을 실행하려면 큐 관리자가 실행 중이어야 합니다. 프린시펄에 대한 액세스를 변경한 경우에는 변경사항은 OAM에 의해 즉시 반영됩니다.

사용자에게 오브젝트에 대한 액세스를 제공하려면 다음을 지정해야 합니다.

- 작업 중인 오브젝트를 소유하는 큐 관리자의 이름입니다. 큐 관리자의 이름을 지정하지 않는 경우에는 기본 큐 관리자가 가정됩니다.
- 오브젝트의 이름 및 유형(오브젝트를 고유하게 식별하기 위함). 이름을 프로파일로서 지정할 수 있습니다. 이는 오브젝트의 명시적인 이름이거나 와일드카드 문자를 포함하는 일반적인 이름입니다. 일반 프로파일에 대한 자세한 설명과 일반 프로파일에서 와일드카드 문자 사용에 대해서는 [316 페이지의 『UNIX, Linux, and Windows에서 OAM 일반 프로파일 사용』](#)의 내용을 참조하십시오.
- 권한이 적용되는 하나 이상의 프린시펄 및 그룹 이름입니다.

사용자 ID에 공백이 포함되는 경우에는 이 명령을 사용할 때 이를 따옴표에 넣으십시오. Windows 시스템에서 사용자 ID를 도메인 이름으로 규정할 수 있습니다. 실제 사용자 ID에 at 기호(@) 기호가 포함되는 경우 이를 @@로 바꿔서 이것이 사용자 ID와 도메인 이름 간의 구분 기호가 아니라 사용자 ID의 일부분임을 표시하십시오.

- 권한 부여 목록입니다. 목록의 각 항목은 해당 오브젝트에 권한 부여되거나 권한 취소되는 액세스 유형을 지정합니다. 목록의 각 권한 부여는 더하기 부호(+) 또는 빼기 부호(-)가 접두부로 추가되는 키워드로 지정됩니다. 더하기 부호를 사용하여 지정된 권한 부여를 추가하고, 빼기 부호를 사용하여 권한 부여를 제거하십시오. + 또는 - 부호와 키워드 사이에는 공백이 없어야 합니다.

단일 명령에 여러 권한 부여를 지정할 수 있습니다. 예를 들어, 사용자 또는 그룹이 큐에 메시지를 넣고 이들을 찾아볼 수 있지만 메시지 가져오기에 대한 액세스를 취소하려면 권한 부여 목록은 다음과 같습니다.

```
+browse -get +put
```

setmqaut 명령 사용 예

다음 예는 오브젝트를 사용하기 위한 권한을 부여하고 취소하기 위해 **setmqaut** 명령을 사용하는 방법을 보여줍니다.

```
setmqaut -m saturn.queue.manager -t queue -n RED.LOCAL.QUEUE
-g groupa +browse -get +put
```

이 예제에서

- saturn.queue.manager는 큐 관리자 이름입니다.
- queue는 오브젝트 유형입니다.
- RED.LOCAL.QUEUE는 오브젝트 이름입니다.
- groupa는 변경할 권한 부여가 있는 그룹의 ID입니다.
- +browse -get +put는 지정된 큐의 권한 부여 목록입니다.
 - +browse는 큐에서 메시지를 찾아보기 위한 권한 부여를 추가합니다(찾아보기 옵션과 함께 **MQGET**를 실행하기 위해)
 - -get은 큐에서 메시지를 가져오기(**MQGET**) 위한 권한 부여를 제거합니다.

- +put은 메시지를 큐에 넣기(MQPUT) 위한 권한 부여를 추가합니다.

다음 명령은 프린시펄 fvuser 및 그룹 groupa 및 groupb로부터 큐 MyQueue에 넣기 권한을 취소합니다. UNIX and Linux 시스템에서 이 명령은 또한 fvuser와 같은 기본 그룹에서 모든 프린시펄의 넣기 권한을 취소합니다.

```
setmqaut -m saturn.queue.manager -t queue -n MyQueue -p fvuser
-g groupa -g groupb -put
```

setmqaut 명령을 여러 권한 서비스와 함께 사용

OAM 대신 본인의 권한 서비스를 사용 중인 경우, **setmqaut** 명령에서 이 서비스 이름을 지정하여 이 서비스로 명령을 전달할 수 있습니다. 동시에 실행 중인 여러 설치 가능한 컴포넌트가 있는 경우에는 이 매개변수를 지정해야 합니다. 그렇지 않으면 권한 서비스의 가장 먼저 설치 가능한 컴포넌트에 업데이트가 작성됩니다. 기본적으로 이는 제공된 OAM입니다.

SET AUTHREC의 사용 참고사항

추가할 권한 목록과 제거할 권한 목록이 겹치면 안됩니다. 예를 들어 같은 명령을 사용하여 표시 권한을 추가하고 표시 권한을 제거할 수는 없습니다. 다른 옵션을 사용하여 권한을 표시한 경우에도 이 규칙이 적용됩니다. 예를 들어 다음 명령은 DSP 권한이 ALLADM 권한과 겹치기 때문에 실패합니다.

```
SET AUTHREC PROFILE(*) OBJTYPE(Queue) PRINCIPAL(PRINC01) AUTHADD(DSP) AUTHRMV(ALLADM)
```

이 겹치기 동작이 적용되지 않는 경우는 ALL 권한입니다. 다음 명령은 먼저 ALL 권한을 추가한 다음 SETID 권한을 제거합니다.

```
SET AUTHREC PROFILE(*) OBJTYPE(Queue) PRINCIPAL(PRINC01) AUTHADD(ALL) AUTHRMV(SETID)
```

다음 명령은 먼저 ALL 권한을 제거한 다음 DSP 권한을 추가합니다.

```
SET AUTHREC PROFILE(*) OBJTYPE(Queue) PRINCIPAL(PRINC01) AUTHADD(DSP) AUTHRMV(ALL)
```

명령에 제공되는 순서에 관계없이 ALL은 가장 먼저 처리됩니다.

ULW UNIX, Linux, and Windows에서 OAM 일반 프로파일 사용

작성 시 각 개별 오브젝트에 대해 별도의 **setmqaut** 명령 또는 **SET AUTHREC** 명령을 실행하지 않고 단일 조각으로 여러 오브젝트에 대한 사용자의 권한을 설정하려면 OAM 일반 프로파일을 사용하십시오. IBM MQ Appliance에서는 **SET AUTHREC** 명령만 사용할 수 있습니다.

setmqaut 또는 **SET AUTHREC** 명령에서 일반 프로파일을 사용하면 해당 프로파일에 맞는 모든 오브젝트에 일반 권한을 설정할 수 있습니다.

이 주제 모음에서는 일반 프로파일의 사용을 보다 자세히 설명합니다.

OAM 프로파일에서 와일드카드 문자 사용

프로파일을 일반적으로 작성하는 방법은 프로파일 이름에 특수 문자(와일드카드 문자)를 사용하는 것입니다. 예를 들어 물음표(?) 와일드카드 문자는 이름에서 단일 문자를 일치시킵니다. 따라서 ABC.?EF를 지정하는 경우 해당 프로파일에 제공하는 권한 부여는 이름 ABC.DEF, ABC.CEF, ABC.BEF 등등이 있는 오브젝트에 적용됩니다.

사용 가능한 와일드카드 문자는 다음과 같습니다.

?

단일 문자 대신 물음표(?) 사용. 예를 들어, AB.?D는 오브젝트 AB.CD, AB.ED 및 AB.FD에 적용됩니다.

*

별표(*)를 다음과 같이 사용하십시오.

- 오브젝트 이름에 있는 규정자와 일치하는 프로파일 이름의 규정자. 규정자는 마침표로 구분되는 오브젝트 이름의 한 부분입니다. 예를 들어, ABC.DEF.GHI에서 규정자는 ABC, DEF 및 GHI입니다.

예를 들어, ABC.*.JKL은 오브젝트 ABC.DEF.JKL 및 ABC.GHI.JKL에 적용됩니다. (이것은 ABC.JKL에 적용되지 **않습니다**. 이 컨텍스트에 사용되는 *는 항상 하나의 규정자를 표시합니다.)

- 오브젝트 이름에 있는 규정자 내에서 0개 또는 그 이상의 문자와 일치하는 프로파일 이름의 규정자 문자. 예를 들어, ABC.DE*.JKL은 오브젝트 ABC.DE.JKL, ABC.DEF.JKL 및 ABC.DEGH.JKL에 적용됩니다.

**

다음과 같이 프로파일 이름에서는 이중 별표(**)를 **한 번만** 사용하십시오.

- 모든 오브젝트 이름과 일치하는 전체 프로파일 이름. 예를 들어, -t prcs 를 사용하여 프로세스를 식별한 후 프로파일 이름으로 ** 를 사용하는 경우 모든 프로세스에 대한 권한을 변경합니다.
- 오브젝트 이름에 있는 0개 또는 그 이상의 규정자와 일치하는 프로파일 이름의 시작, 중간 또는 종료 규정자로서 사용됩니다. 예를 들어, **.ABC는 모든 오브젝트를 최종 규정자 ABC로 식별합니다.

완전한 규정자로 이중 별표 ** 만 사용할 수 있습니다.

```
** .DEF
ABC.**
A*.**
```

그러나 다음과 같이

```
A**
```

그렇지 않으면 AMQ7226E: 프로파일 이름이 올바르지 않습니다. 라는 메시지를 수신합니다.

참고: UNIX 및 Linux 시스템에서 와일드카드 문자를 사용할 때 프로파일 이름을 작은따옴표에 묶어야 합니다.

프로파일 우선순위

일반 프로파일을 사용할 경우 이해해야 하는 중요한 점은 작성 중인 오브젝트에 적용할 권한을 결정할 때 프로파일에 지정되는 우선순위입니다. 예를 들어, 다음 명령을 발행한 것으로 가정해 보십시오.

```
setmqaut -n AB.* -t q +put -p fred
setmqaut -n AB.C* -t q +get -p fred
```

첫 번째는 프로파일 AB.*; 와 일치하는 이름을 가진 프린시펄 fred에 대한 모든 큐에 넣기 권한을 부여합니다. 두 번째는 AB.C*

이제 AB.CD 큐를 작성한다고 가정합니다. 와일드카드 일치 규칙에 따라 각각 setmqaut가 해당 큐에 적용될 수 있습니다. 따라서, 넣기 또는 가져오기 권한이 있습니까?

응답을 찾기 위해 여러 프로파일을 오브젝트에 적용할 수 있을 때마다 **가장 특정되게 적용되는** 규칙만 적용합니다. 이 규칙을 적용하는 방법은 프로파일 이름을 왼쪽에서 오른쪽으로 비교하는 것입니다. 다른 경우, 일반 문자가 아닌 문자가 일반 문자보다 더 고유한 문자입니다. 따라서, 이 예에서 큐 AB.CD에는 **가져오기** 권한(AB.C*가 AB.*보다 더 특정적임)이 있습니다.

일반 문자를 비교할 때 특이성의 순서는 다음과 같습니다.

1. ?
2. *
3. **

프로파일 설정 버리기

dmpmqaut 제어 명령 및 해당 구문의 전체 정의에 대해서는 [dmpmqaut](#)의 내용을 참조하십시오.

DISPLAY AUTHREC MQSC 명령 및 해당 구문의 전체 정의에 대해서는 [DISPLAY AUTHREC](#)의 내용을 참조하십시오.

MQCMD_INQUIRE_AUTH_RECS PCF 명령 및 해당 구문의 전체 정의에 대해서는 [권한 레코드 설정을 참조하십시오](#).

다음 예는 일반 프로파일의 권한 레코드를 버리기 위해 **dmpmqaut** 제어 명령을 사용하는 방법을 보여줍니다.

1. 이 예는 프린시펄 user1에 대해 큐 a.b.c와 일치하는 프로파일이 있는 모든 권한 레코드를 버립니다.

```
dmpmqaut -m qm1 -n a.b.c -t q -p user1
```

버리기 결과는 다음과 같습니다.

```
profile:      a.b.*
object type: queue
entity:       user1
type:         principal
authority:    get, browse, put, inq
```

참고: UNIX 및 Linux의 사용자는 **dmpmqaut** 명령에 -p 옵션을 사용할 수 있지만 권한을 정의할 때 대신 -g groupname 를 사용해야 합니다.

2. 이 예는 큐 a.b.c와 일치하는 프로파일이 있는 모든 권한 레코드를 버립니다.

```
dmpmqaut -m qmgr1 -n a.b.c -t q
```

버리기 결과는 다음과 같습니다.

```
profile:      a.b.c
object type: queue
entity:       Administrator
type:         principal
authority:    all
-----
profile:      a.b.*
object type: queue
entity:       user1
type:         principal
authority:    get, browse, put, inq
-----
profile:      a.**
object type: queue
entity:       group1
type:         group
authority:    get
```

3. 이 예제는 a.b.* 프로파일에 대한 모든 권한 레코드를 덤프합니다. 표시합니다.

```
dmpmqaut -m qmgr1 -n a.b.* -t q
```

버리기 결과는 다음과 같습니다.

```
profile:      a.b.*
object type: queue
entity:       user1
type:         principal
authority:    get, browse, put, inq
```

4. 이 예는 큐 관리자 qmX의 모든 권한 레코드를 버립니다.

```
dmpmqaut -m qmX
```

버리기 결과는 다음과 같습니다.

```
profile:      q1
object type: queue
entity:       Administrator
```

```

type:      principal
authority: all
-----
profile:   q*
object type: queue
entity:    user1
type:      principal
authority: get, browse
-----
profile:   name.*
object type: namelist
entity:    user2
type:      principal
authority: get
-----
profile:   pr1
object type: process
entity:    group1
type:      group
authority: group

```

5. 이 예는 큐 관리자 qmX의 모든 프로파일 이름 및 오브젝트 유형을 버립니다.

```
dmpmqaut -m qmX -l
```

버리기 결과는 다음과 같습니다.

```

profile: q1, type: queue
profile: q*, type: queue
profile: name.*, type: namelist
profile: pr1, type: process

```

참고: IBM MQ for Windows의 경우에만 표시된 모든 프린시펄에는 도메인 정보가 포함됩니다. 예:

```

profile:      a.b.*
object type: queue
entity:       user1@domain1
type:         principal
authority:    get, browse, put, inq

```

ULW UNIX, Linux, and Windows에서 OAM 프로파일에 와일드카드 문자 사용

오브젝트 권한 관리자(OAM) 프로파일 이름에서 와일드카드 문자를 사용하여 해당 프로파일을 둘 이상의 오브젝트에 적용할 수 있게 만드십시오.

프로파일을 일반적으로 작성하는 방법은 프로파일 이름에 특수 문자(와일드카드 문자)를 사용하는 것입니다. 예를 들어 물음표(?) 와일드카드 문자는 이름에서 단일 문자를 일치시킵니다. 따라서 ABC.?EF를 지정하는 경우 해당 프로파일에 제공하는 권한 부여는 이름 ABC.DEF, ABC.CEF, ABC.BEF 등등이 있는 오브젝트에 적용됩니다.

사용 가능한 와일드카드 문자는 다음과 같습니다.

?

단일 문자 대신 물음표(?) 사용. 예를 들어, AB.?D는 오브젝트 AB.CD, AB.ED 및 AB.FD에 적용됩니다.

별표(*)를 다음과 같이 사용하십시오.

- 오브젝트 이름에 있는 규정자와 일치하는 프로파일 이름의 규정자. 규정자는 마침표로 구분되는 오브젝트 이름의 한 부분입니다. 예를 들어, ABC.DEF.GHI에서 규정자는 ABC, DEF 및 GHI입니다.

예를 들어, ABC.*.JKL은 오브젝트 ABC.DEF.JKL 및 ABC.GHI.JKL에 적용됩니다. (이것은 ABC.JKL에 적용되지 **않습니다**. 이 컨텍스트에 사용되는 *는 항상 하나의 규정자를 표시합니다.)

- 오브젝트 이름에 있는 규정자 내에서 0개 또는 그 이상의 문자와 일치하는 프로파일 이름의 규정자 문자. 예를 들어, ABC.DE*.JKL은 오브젝트 ABC.DE.JKL, ABC.DEF.JKL 및 ABC.DEGH.JKL에 적용됩니다.

다음과 같이 프로파일 이름에서는 이중 별표(**)를 **한 번만** 사용하십시오.

- 모든 오브젝트 이름과 일치하는 전체 프로파일 이름. 예를 들어, `-t prcs` 를 사용하여 프로세스를 식별한 후에 `**` 를 프로파일 이름으로 사용하면 모든 프로세스에 대한 권한을 변경합니다.
- 오브젝트 이름에 있는 0개 또는 그 이상의 규정자와 일치하는 프로파일 이름의 시작, 중간 또는 종료 규정자로서 사용됩니다. 예를 들어, `** .ABC`는 모든 오브젝트를 최종 규정자 `ABC`로 식별합니다.

참고: UNIX and Linux 시스템에서 와일드카드 문자를 사용할 때 프로파일 이름을 작은따옴표에 묶어야 합니다.

ULW UNIX, Linux, and Windows에서 프로파일 우선순위

둘 이상의 일반 프로파일을 단일 오브젝트에 적용할 수 있습니다. 이 경우이면 가장 특정 규칙이 적용됩니다.

일반 프로파일을 사용할 경우 이해해야 하는 중요한 점은 작성 중인 오브젝트에 적용할 권한을 결정할 때 프로파일에 지정되는 우선순위입니다. 예를 들어, 다음 명령을 발행한 것으로 가정해 보십시오.

```
setmqaut -n AB.* -t q +put -p fred
setmqaut -n AB.C* -t q +get -p fred
```

첫 번째는 프로파일과 일치하는 이름을 가진 프린시פל `fred`에 대한 모든 큐에 대한 권한을 부여한다. 두 번째는 프로파일 `AB.C*`.

이제 `AB.CD` 큐를 작성한다고 가정합니다. 와일드카드 일치 규칙에 따라 각각 `setmqaut`가 해당 큐에 적용될 수 있습니다. 따라서, 넣기 또는 가져오기 권한이 있습니까?

응답을 찾기 위해 여러 프로파일을 오브젝트에 적용할 수 있을 때마다 **가장 특정되게 적용되는** 규칙만 적용합니다. 이 규칙을 적용하는 방법은 프로파일 이름을 왼쪽에서 오른쪽으로 비교하는 것입니다. 다른 경우, 일반 문자가 아닌 문자가 일반 문자보다 더 고유한 문자입니다. 따라서, 이 예에서 큐 `AB.CD`에는 **가져오기** 권한(`AB.C*`가 `AB.*`보다 더 특정적임)이 있습니다.

일반 문자를 비교할 때 특이성의 순서는 다음과 같습니다.

1. ?
2. *
3. **

이 MQSC 명령을 사용할 때 동등한 정보에 대해서는 [SET AUTHREC](#)의 내용을 참조하십시오.

ULW UNIX, Linux, and Windows에서 프로파일 설정 덤프

지정된 프로파일과 연관된 현재 권한을 덤프하려면 `dmpmqaut` 제어 명령, `DISPLAY AUTHREC` MQSC 명령 또는 `MQCMD_INQUIRE_AUTH_RECS` PCF 명령을 사용하십시오. IBM MQ Appliance에서는 `DISPLAY AUTHREC` 명령만 사용할 수 있습니다.

`dmpmqaut` 제어 명령 및 해당 구문의 전체 정의에 대해서는 `dmpmqaut`의 내용을 참조하십시오.

`DISPLAY AUTHREC` MQSC 명령 및 해당 구문의 전체 정의에 대해서는 [DISPLAY AUTHREC](#)의 내용을 참조하십시오.

`MQCMD_INQUIRE_AUTH_RECS` PCF 명령 및 해당 구문의 전체 정의에 대해서는 [권한 레코드 설정](#)을 참조하십시오.

다음 예는 일반 프로파일의 권한 레코드를 버리기 위해 `dmpmqaut` 제어 명령을 사용하는 방법을 보여줍니다.

1. 이 예는 프린시פל `user1`에 대해 큐 `a.b.c`와 일치하는 프로파일이 있는 모든 권한 레코드를 버립니다.

```
dmpmqaut -m qm1 -n a.b.c -t q -p user1
```

버리기 결과는 다음과 같습니다.

```
profile:      a.b.*
object type: queue
entity:      user1
type:        principal
authority:    get, browse, put, inq
```

참고: UNIX and Linux 사용자는 -p 옵션을 사용할 수 없습니다. 이들은 대신 -g groupname을 사용해야 합니다.

2. 이 예는 큐 a.b.c와 일치하는 프로파일이 있는 모든 권한 레코드를 버립니다.

```
dmpmqaut -m qmgr1 -n a.b.c -t q
```

버리기 결과는 다음과 같습니다.

```
profile:      a.b.c
object type:  queue
entity:       Administrator
type:         principal
authority:    all
-----
profile:      a.b.*
object type:  queue
entity:       user1
type:         principal
authority:    get, browse, put, inq
-----
profile:      a.**
object type:  queue
entity:       group1
type:         group
authority:    get
```

3. 이 예제는 프로파일 a.b에 대한 모든 권한 레코드를 덤프합니다. *, 큐에 넣을 수 있다.

```
dmpmqaut -m qmgr1 -n a.b.* -t q
```

버리기 결과는 다음과 같습니다.

```
profile:      a.b.*
object type:  queue
entity:       user1
type:         principal
authority:    get, browse, put, inq
```

4. 이 예는 큐 관리자 qmX의 모든 권한 레코드를 버립니다.

```
dmpmqaut -m qmX
```

버리기 결과는 다음과 같습니다.

```
profile:      q1
object type:  queue
entity:       Administrator
type:         principal
authority:    all
-----
profile:      q*
object type:  queue
entity:       user1
type:         principal
authority:    get, browse
-----
profile:      name.*
object type:  namelist
entity:       user2
type:         principal
authority:    get
-----
profile:      pr1
object type:  process
entity:       group1
type:         group
authority:    get
```


5. 이 예는 큐 관리자 qmX의 모든 프로파일 이름 및 오브젝트 유형을 버립니다.

```
dmpmqaut -m qmX -l
```

버리기 결과는 다음과 같습니다.

```
profile: q1, type: queue
profile: q*, type: queue
profile: name.*, type: namelist
profile: pr1, type: process
```

참고: IBM MQ for Windows의 경우에만 표시된 모든 프린시펄에는 도메인 정보가 포함됩니다. 예:

```
profile: a.b.*
object type: queue
entity: user1@domain1
type: principal
authority: get, browse, put, inq
```

ULW UNIX, Linux, and Windows에서 액세스 설정 표시

특정 프린시펄 또는 그룹이 특정 오브젝트에 대해 갖는 권한을 보려면 **dspmqa**ut 제어 명령, **DISPLAY AUTHREC** MQSC 명령 또는 **MQCMD_INQUIRE_ENTITY_AUTH** PCF 명령을 사용하십시오. IBM MQ 어플라이언스에서는 **DISPLAY AUTHREC** 명령만을 사용할 수 있음을 유의하십시오.

이 명령을 실행하려면 큐 관리자가 실행 중이어야 합니다. 프린시펄에 대한 액세스를 변경하면 변경사항은 OAM에 의해 즉시 반영됩니다. 권한 부여는 한 번에 하나의 그룹이나 프린시펄에만 표시될 수 있습니다.

dmpmqaut 제어 명령 및 해당 구문의 전체 정의에 대해서는 **dmpmqaut**의 내용을 참조하십시오.

DISPLAY AUTHREC MQSC 명령 및 해당 구문의 전체 정의에 대해서는 **DISPLAY AUTHREC**의 내용을 참조하십시오.

MQCMD_INQUIRE_AUTH_RECS PCF 명령 및 해당 구문의 전체 정의에 대해서는 [권한 레코드 설정을 참조하십시오](#).

다음 예는 **dspmqa**ut 제어 명령을 사용하여 GpAdmin 그룹이 QueueMan1 큐 관리자에 있는 이름이 Annuities인 프로세스 정의에 가지고 있는 권한 부여를 표시하는 방법을 보여줍니다.

```
dspmqa -m QueueMan1 -t process -n Annuities -g GpAdmin
```

ULW UNIX, Linux, and Windows에서 IBM MQ 오브젝트에 대한 액세스 변경 및 취소

사용자 또는 그룹이 오브젝트에 대해 가지고 있는 액세스 레벨을 변경하려면 **setmqaut** 제어 명령, **DELETE AUTHREC** MQSC 명령 또는 **MQCMD_DELETE_AUTH_REC** PCF 명령을 사용하십시오. [MQ Appliance](#) IBM MQ 어플라이언스에서는 **DELETE AUTHREC** 명령만 사용할 수 있습니다.

사용자를 그룹에서 제거하는 프로세스는 다음에서 설명됩니다.

- ▶ **Windows** 129 페이지의 『Windows에서 그룹 작성 및 관리』
- ▶ **AIX** 127 페이지의 『AIX에서 그룹 작성 및 관리』
- ▶ **Solaris** 128 페이지의 『Solaris에서 그룹 작성 및 관리』
- ▶ **Linux** 127 페이지의 『Linux에서 그룹 작성 및 관리』

IBM MQ 오브젝트를 작성하는 사용자 ID에는 해당 오브젝트에 대한 전체 제어 권한이 부여됩니다. 로컬 mqm 그룹(또는 Windows 시스템의 관리자)에서 이 사용자 ID를 제거하는 경우 이러한 권한은 취소되지 않습니다.

setmqaut 제어 명령 또는 **MQCMD_DELETE_AUTH_REC** PCF 명령을 사용하여 오브젝트를 mqm 또는 관리자 그룹에서 제거한 후에 이를 작성한 사용자 ID의 오브젝트에 대한 액세스를 취소하십시오.

setmqaut 제어 명령 및 해당 구문의 전체 정의에 대해서는 [setmqaut](#)의 내용을 참조하십시오.

DELETE AUTHREC MQSC 명령 및 해당 구문의 전체 정의에 대해서는 [DELETE AUTHREC](#)의 내용을 참조하십시오.

MQCMD_DELETE_AUTH_REC PCF 명령 및 해당 구문의 전체 정의에 대해서는 권한 레코드 설정을 참조하십시오.

Windows On Windows, from IBM MQ 8.0, you can delete the OAM entries corresponding to a particular Windows user account at any time using the **-u** 시드 parameter of [setmqaut](#).

IBM MQ 8.0 이전에는 사용자 프로파일을 삭제하기 전에 특정 Windows 사용자 계정에 해당하는 OAM 항목을 삭제했어야 했습니다. 사용자 계정을 제거한 후 OAM 항목을 제거하는 것이 불가능했습니다.

ULW UNIX, Linux, and Windows 시스템에서 보안 액세스 검사 방지

모든 보안 검사를 끄려면 오브젝트 권한 관리자(OAM)를 사용 안함으로 설정하면 됩니다. 이는 테스트 환경에 적합할 수 있습니다. OAM을 사용 안함으로 설정하거나 제거하면 OAM을 기존 큐 관리자에 추가할 수 없습니다.

보안 검사를 수행하지 않기로 결정한 경우(예를 들어, 테스트 환경에서) 다음 두 방법 중 하나를 사용하여 OAM을 사용 안함으로 설정할 수 있습니다.

- 큐 관리자를 작성하기 전에 운영 체제 환경 변수 MQSNOAUT를 설정하십시오.

MQSNOAUT 변수 설정의 영향 및 Windows 및 UNIX에서 MQSNOAUT를 설정하는 방법에 대한 정보는 [환경 변수 설명](#)을 참조하십시오.

- 서비스를 제거하려면 큐 관리자 구성 파일을 편집하십시오.

OAM이 사용 불가능한 상태에서 [setmqaut](#) 또는 [dspmqaut](#) 명령을 사용하는 경우 다음 사항에 유의하십시오.

- OAM은 지정된 프린시פל 또는 그룹을 유효성 검증하지 않습니다. 즉, 명령이 올바르지 않은 값을 승인할 수 있음을 의미합니다.
- OAM은 보안 검사를 수행하지 않고 모든 프린시פל 및 그룹이 모든 적용 가능한 오브젝트 조작을 수행할 권한이 있음을 나타냅니다.



경고: OAM이 제거되면 이를 기존 큐 관리자에 다시 넣을 수 없습니다. 이는 OAM은 오브젝트 작성 시에 배치되어야 하기 때문입니다. IBM MQ OAM을 제거한 후 다시 사용하려면 큐 관리자를 다시 빌드해야 합니다.

관련 개념

[UNIX, Linux 및 Windows용 설치 가능 서비스 및 컴포넌트](#)

관련 태스크

[설치 가능 서비스 구성](#)

관련 참조

[설치 가능 서비스 참조 정보](#)

자원에 대한 필수 액세스 부여

이 주제를 사용하여 UNIX, Linux, Windows, IBM i 및 z/OS에서 IBM MQ 시스템에 보안을 적용하기 위해 수행할 태스크를 판별하십시오.

이 태스크 정보

이 태스크 동안에 적합한 보안 레벨을 IBM MQ 설치의 요소에 적용하기 위해 어떤 조치가 필요한지를 결정하십시오. 언급된 각 개별 태스크는 모든 플랫폼에 대한 단계별 지시사항을 제공합니다.

프로시저

1. 큐 관리자에 대한 액세스를 특정 사용자로 제한해야 합니까?
 - a) 아니오: 추가 조치를 취하지 마십시오.
 - b) 예: 다음 질문으로 이동하십시오.
2. 이러한 사용자가 큐 관리자 자원의 서브세트에서 부분 관리 액세스를 필요로 합니까?
 - a) 아니오: 다음 질문으로 이동하십시오.
 - b) 예: 324 페이지의 『[큐 관리자 자원의 서브세트에서 부분 관리 액세스 부여](#)』의 내용을 참조하십시오.
3. 이러한 사용자가 큐 관리자 자원의 서브세트에서 전체 관리 액세스를 필요로 합니까?
 - a) 아니오: 다음 질문으로 이동하십시오.
 - b) 예: 333 페이지의 『[큐 관리자 자원의 서브세트에서 전체 관리 액세스 부여](#)』의 내용을 참조하십시오.
4. 이러한 사용자가 모든 큐 관리자 자원에 대한 읽기 전용 액세스를 필요로 합니까?
 - a) 아니오: 다음 질문으로 이동하십시오.
 - b) 예: 339 페이지의 『[큐 관리자에서 모든 자원에 읽기 전용 액세스 부여](#)』의 내용을 참조하십시오.
5. 이러한 사용자가 모든 큐 관리자 자원에서 전체 관리 액세스를 필요로 합니까?
 - a) 아니오: 다음 질문으로 이동하십시오.
 - b) 예: 341 페이지의 『[큐 관리자에서 모든 자원에 전체 관리 액세스 부여](#)』의 내용을 참조하십시오.
6. 사용자 애플리케이션을 큐 관리자에 연결해야 합니까?
 - a) 아니오: 342 페이지의 『[큐 관리자에 대한 연결성 제거](#)』에 설명한 대로 연결성을 사용 안함으로 설정하십시오.
 - b) 예: 343 페이지의 『[사용자 애플리케이션이 큐 관리자에 연결할 수 있도록 허용](#)』의 내용을 참조하십시오.

Multi z/OS 큐 관리자 자원의 서브세트에서 부분 관리 액세스 부여

특정 사용자에게 큐 관리자 자원의 전체가 아닌 일부에 대한 부분 관리 액세스를 제공해야 합니다. 수행해야 하는 조치를 판별하려면 이 테이블을 사용하십시오.

표 69. 큐 관리자 자원의 서브세트에 부분 관리 액세스 부여	
사용자가 관리해야 하는 오브젝트 유형	수행 조치
큐	325 페이지의 『 일부 큐에 제한된 관리 액세스 부여 』에 설명된 대로 필수 큐에 부분 관리 액세스를 부여하십시오.
토픽	326 페이지의 『 일부 토픽에 제한된 관리 액세스 부여 』에 설명된 대로 필수 토픽에 부분 관리 액세스를 부여하십시오.
채널	327 페이지의 『 일부 채널에 제한된 관리 액세스 부여 』에 설명된 대로 필수 채널에 부분 관리 액세스를 부여하십시오.
큐 관리자	328 페이지의 『 큐 관리자에 제한된 관리 액세스 부여 』에 설명된 대로 큐 관리자에 부분 관리 액세스를 부여하십시오.
프로세스	329 페이지의 『 일부 프로세스에 제한된 관리 액세스 부여 』에 설명된 대로 필수 프로세스에 부분 관리 액세스를 부여하십시오.
이름 목록	331 페이지의 『 일부 이름 목록에 제한된 관리 액세스 부여 』에 설명된 대로 필수 이름 목록에 부분 관리 액세스를 부여하십시오.

표 69. 큐 관리자 자원의 서브세트에 부분 관리 액세스 부여 (계속)	
사용자가 관리해야 하는 오브젝트 유형	수행 조치
서비스	332 페이지의 『일부 서비스에 제한된 관리 액세스 부여』에 설명된 대로 필수 서비스에 부분 관리 액세스를 부여하십시오.

일부 큐에 제한된 관리 액세스 부여

비즈니스 요구사항이 있는 각 사용자 그룹에 큐 관리자에서 일부 큐에 부분 관리 액세스를 부여하십시오.

이 태스크 정보

일부 조치를 위해 일부 큐에 제한된 관리 액세스를 부여하려면 운영 체제에 적합한 명령을 사용하십시오.

다음 플랫폼에서는 SET AUTHREC 명령도 사용할 수 있습니다.

- ▶ **IBM i** IBM i
- ▶ **Linux** Linux
- ▶ **UNIX** UNIX
- ▶ **IBM i** Windows

참고: **MQ Appliance** IBM MQ Appliance에서는 **SET AUTHREC** 명령만 사용할 수 있습니다.

프로시저

- ▶ **ULW**
UNIX, Linux, and Windows 시스템의 경우 다음 명령을 실행하십시오.

```
setmqaut -m QMgrName -n ObjectProfile -t queue -g GroupName ReqdAction
```

- ▶ **IBM i**
IBM i의 경우 다음 명령을 실행하십시오.

```
GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*Q) USER(GroupName) AUT(ReqdAction) MQMNAME(' QMgrName ')
```

- ▶ **z/OS** z/OS의 경우 ID 컨텍스트 또는 모든 컨텍스트를 전달하려면 다음 명령을 실행하십시오.

```
RDEFINE MQADMIN QMgrName.QUEUE. ObjectProfile UACC(NONE)  
PERMIT QMgrName.QUEUE. ObjectProfile CLASS(MQADMIN) ID(GroupName) ACCESS(ALTER)
```

큐에 대해 사용자가 수행할 수 있는 MQSC 명령을 판별하려면 각 MQSC 명령에 대해 다음 명령을 실행하십시오.

```
RDEFINE MQCMD5 QMgrName. ReqdAction. QType UACC(NONE)  
PERMIT QMgrName. ReqdAction. QType CLASS(MQCMD5) ID(GroupName) ACCESS(ALTER)
```

사용자가 DISPLAY QUEUE 명령을 사용하도록 허용하려면 다음 명령을 실행하십시오.

```
RDEFINE MQCMD5 QMgrName.DISPLAY. QType UACC(NONE)  
PERMIT QMgrName.DISPLAY. QType CLASS(MQCMD5) ID(GroupName) ACCESS(READ)
```

변수 이름에는 다음과 같은 의미가 있습니다.

QMgrName

큐 관리자 이름.

z/OS z/OS에서 이 값은 또한 큐 공유 그룹의 이름일 수도 있습니다.

ObjectProfile

권한을 변경한 오브젝트 또는 일반 프로파일의 이름입니다.

GroupName

액세스가 부여될 그룹의 이름입니다.

ReqdAction

그룹이 수행할 수 있는 조치:

- **ULW** UNIX, Linux, and Windows 시스템에서 다음 권한의 결합입니다. +chg, +clr, +dlt, +dsp. 권한 +alladm은 +chg +clr +dlt +dsp와 동등합니다.
- **IBM i** IBM i에서 다음 권한의 결합입니다. *ADMCHG, *ADMCLR, *ADMDLT, *ADMDSP. 권한 *ALLADM은 이러한 개별 권한 모두와 동등합니다.
- **z/OS** z/OS에서 값 ALTER, CLEAR, DELETE 또는 MOVE 중 하나입니다.

참고: 큐에 +crt를 간접적으로 부여하면 사용자 또는 그룹을 관리자로 만듭니다. 일부 큐에 제한된 관리 액세스를 부여하기 위해 +crt 권한을 사용하지 마십시오.

QType

DISPLAY 명령의 경우 값 QUEUE, QLOCAL, QALIAS, QMODEL, QREMOTE 또는 QCLUSTER의 중 하나입니다.

ReqdAction의 다른 값의 경우 값 QLOCAL, QALIAS, QMODEL 또는 QREMOTE 중 하나입니다.

일부 토픽에 제한된 관리 액세스 부여

비즈니스 요구사항이 있는 각 사용자 그룹에 큐 관리자에서 일부 토픽에 부분 관리 액세스를 부여하십시오.

이 태스크 정보

일부 조치를 위해 일부 토픽에 제한된 관리 액세스를 부여하려면 운영 체제에 적합한 명령을 사용하십시오.

다음 플랫폼에서는 SET AUTHREC 명령도 사용할 수 있습니다.

- **IBM i** IBM i
- **Linux** Linux
- **UNIX** UNIX
- **IBM i** Windows

참고: **MQ Appliance** IBM MQ Appliance에서는 SET AUTHREC 명령만 사용할 수 있습니다.

프로시저

- **ULW** UNIX, Linux, and Windows 시스템의 경우 다음 명령을 실행하십시오.

```
setmqaut -m QMgrName -n ObjectProfile -t topic -g GroupName ReqdAction
```

- **IBM i** IBM i의 경우 다음 명령을 실행하십시오.

```
GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*TOPIC) USER(GroupName) AUT(ReqdAction) MQMNAME(' QMgrName ')
```

- **z/OS** z/OS의 경우 다음 명령을 실행하십시오.

```
RDEFINE MQADMIN QMgrName.TOPIC. ObjectProfile UACC(NONE)
PERMIT QMgrName.TOPIC. ObjectProfile CLASS(MQADMIN) ID(GroupName) ACCESS(ALTER)
```

이러한 명령은 지정된 토픽에 액세스를 부여합니다. 사용자가 토픽에서 어떤 MQSC 명령을 수행할 수 있는지를 판별하려면 각 MQSC 명령에 대해 다음 명령을 실행하십시오.

```
RDEFINE MQCMDS QMgrName. ReqdAction.TOPIC UACC(NONE)
PERMIT QMgrName. ReqdAction.TOPIC CLASS(MQCMDS) ID(GroupName) ACCESS(ALTER)
```


사용자가 DISPLAY TOPIC 명령을 사용하도록 허용하려면 다음 명령을 실행하십시오.

```
RDEFINE MQCMDS QMgrName.DISPLAY.TOPIC UACC(NONE)
PERMIT QMgrName.DISPLAY.TOPIC CLASS(MQCMDS) ID(GroupName) ACCESS(READ)
```

변수 이름에는 다음과 같은 의미가 있습니다.

QMgrName

큐 관리자 이름.

 z/OS에서 이 값은 또한 큐 공유 그룹의 이름일 수도 있습니다.

ObjectProfile




권한을 변경한 오브젝트 또는 일반 프로파일의 이름입니다.

GroupName

액세스가 부여될 그룹의 이름입니다.

ReqdAction

그룹이 수행할 수 있는 조치:

-  UNIX, Linux, and Windows 시스템에서 다음 권한의 결합입니다. +chg, +clr, +crt, +dlt, +dsp, +ctrl. 권한 +alladm은 +chg +clr +dlt +dsp와 동등합니다.
-  IBM i에서 다음 권한의 결합입니다. *ADMCHG, *ADMCLR, *ADMCR, *ADMCLT, *ADMDS, *CTRL. 권한 *ALLADM은 이러한 개별 권한 모두와 동등합니다.
-  z/OS에서 값 ALTER, CLEAR, DEFINE, DELETE 또는 MOVE 중 하나입니다.





일부 채널에 제한된 관리 액세스 부여


비즈니스 요구사항이 있는 각 사용자 그룹에 큐 관리자에서 일부 채널에 부분 관리 액세스를 부여하십시오.

이 태스크 정보

일부 조치를 위해 일부 채널에 제한된 관리 액세스를 부여하려면 운영 체제에 적합한 명령을 사용하십시오.

다음 플랫폼에서는 SET AUTHREC 명령도 사용할 수 있습니다.

-  IBM i
-  Linux
-  UNIX
-  Windows

참고:  IBM MQ Appliance에서는 **SET AUTHREC** 명령만 사용할 수 있습니다.

프로시저

-  UNIX, Linux, and Windows의 경우:


```
setmqaut -m QMgrName -n ObjectProfile -t channel -g GroupName ReqdAction
```

IBM i

IBM i의 경우:

```
GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*CHL) USER(GroupName) AUT(ReqdAction) MQMNAME(' QMgrName ')
```

z/OS

z/OS의 경우:

```
RDEFINE MQADMIN QMgrName.CHANNEL. ObjectProfile UACC(NONE)  
PERMIT QMgrName.CHANNEL. ObjectProfile CLASS(MQADMIN) ID(GroupName) ACCESS(ALTER)
```

이러한 명령은 지정된 채널에 액세스를 부여합니다. 사용자가 채널에서 어떤 MQSC 명령을 수행할 수 있는지를 판별하려면 각 MQSC 명령에 대해 다음 명령을 실행하십시오.

```
RDEFINE MQCMD5 QMgrName. ReqdAction.CHANNEL UACC(NONE)  
PERMIT QMgrName. ReqdAction.CHANNEL CLASS(MQCMD5) ID(GroupName) ACCESS(ALTER)
```

사용자가 DISPLAY CHANNEL 명령을 사용하도록 허용하려면 다음 명령을 실행하십시오.

```
RDEFINE MQCMD5 QMgrName.DISPLAY.CHANNEL UACC(NONE)  
PERMIT QMgrName.DISPLAY.CHANNEL CLASS(MQCMD5) ID(GroupName) ACCESS(READ)
```

변수 이름에는 다음과 같은 의미가 있습니다.

QMgrName

큐 관리자 이름.

z/OS

z/OS에서 이 값은 또한 큐 공유 그룹의 이름일 수도 있습니다.

ObjectProfile

권한을 변경한 오브젝트 또는 일반 프로파일의 이름입니다.

GroupName

액세스가 부여될 그룹의 이름입니다.

ReqdAction

그룹이 수행할 수 있는 조치:

- **ULW** UNIX, Linux, and Windows에서 다음 권한의 조합입니다. +chg, +clr, +crt, +dlt, +dsp, +ctrl, +ctrlx. 권한 +alladm은 +chg +clr +dlt +dsp와 동등합니다.
- **IBM i** IBM i에서 다음 권한의 조합입니다. *ADMCHG, *ADMCLR, *ADMCRRT, *ADMDLT, *ADMDSPP, *CTRL, *CTRLX. 권한 *ALLADM은 이러한 개별 권한 모두와 동등합니다.
- **z/OS** z/OS에서 값 ALTER, CLEAR, DEFINE, DELETE 또는 MOVE 중 하나입니다.

큐 관리자에 제한된 관리 액세스 부여

비즈니스 요구사항이 있는 각 사용자 그룹에 큐 관리자에 대한 부분 관리 액세스를 부여하십시오.

이 태스크 정보

일부 조치를 위해 큐 관리자에 제한된 관리 액세스를 부여하려면 운영 체제에 적합한 명령을 사용하십시오.

다음 플랫폼에서는 SET AUTHREC 명령도 사용할 수 있습니다.

- ▶ **IBM i** IBM i
- ▶ **Linux** Linux
- ▶ **UNIX** UNIX

- ▶ **IBM i** Windows

참고: ▶ **MQ Appliance** IBM MQ Appliance에서는 **SET AUTHREC** 명령만 사용할 수 있습니다.

프로시저

- ▶ **ULW**

UNIX, Linux, and Windows의 경우:

```
setmqaut -m QMgrName -n ObjectProfile -t qmgr -g GroupName ReqdAction
```

- ▶ **IBM i**

IBM i의 경우:

```
GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*MQM) USER(GroupName) AUT(ReqdAction) MQMNAME(' QMgrName ')
```

- ▶ **z/OS**

z/OS의 경우:

사용자가 큐 관리자에서 어떤 MQSC 명령을 수행할 수 있는지를 판별하려면 각 MQSC 명령에 대해 다음 명령을 실행하십시오.

```
RDEFINE MQCMDS QMgrName. ReqdAction.QMGR UACC(NONE)
PERMIT QMgrName. ReqdAction.QMGR CLASS(MQCMDS) ID(GroupName) ACCESS(ALTER)
```

사용자가 DISPLAY QMGR 명령을 사용하도록 허용하려면 다음 명령을 실행하십시오.

```
RDEFINE MQCMDS QMgrName.DISPLAY.QMGR UACC(NONE)
PERMIT QMgrName.DISPLAY.QMGR CLASS(MQCMDS) ID(GroupName) ACCESS(READ)
```

변수 이름에는 다음과 같은 의미가 있습니다.

QMGrName

큐 관리자 이름.

ObjectProfile

권한을 변경한 오브젝트 또는 일반 프로파일의 이름입니다.

GroupName

액세스가 부여될 그룹의 이름입니다.

ReqdAction

그룹이 수행할 수 있는 조치:

- ▶ **ULW** UNIX, Linux, and Windows에서 다음 권한의 결합입니다. +chg, +clr, +crt, +dlt, +dsp. 권한 +alladm은 +chg +clr +dlt +dsp와 동등합니다.

+set가 MQI 권한이고 일반적으로 관리적인 것으로 간주되지 않더라도 큐 관리자에 +set를 부여하면 간접적으로 전체 관리 권한으로 이어질 수 있습니다. 일반 사용자 및 애플리케이션에 +set를 부여하지 마십시오.

- ▶ **IBM i** IBM i에서 다음 권한의 결합입니다. *ADMCHG, *ADMCLR, *ADMCRRT, *ADMDLT, *ADM DSP. 권한 *ALLADM은 이러한 개별 권한 모두와 동등합니다.

일부 프로세스에 제한된 관리 액세스 부여

비즈니스 요구사항이 있는 각 사용자 그룹에 큐 관리자에서 일부 프로세스에 부분 관리 액세스를 부여하십시오.

이 태스크 정보

일부 조치를 위해 일부 프로세스에 제한된 관리 액세스를 부여하려면 운영 체제에 적합한 명령을 사용하십시오.

다음 플랫폼에서는 `SET AUTHREC` 명령도 사용할 수 있습니다.

- ▶ **IBM i** IBM i
- ▶ **Linux** Linux
- ▶ **UNIX** UNIX
- ▶ **IBM i** Windows

참고: **MQ Appliance** IBM MQ Appliance에서는 `SET AUTHREC` 명령만 사용할 수 있습니다.

프로시저

- ▶ **ULW**
UNIX, Linux, and Windows의 경우:

```
setmqaut -m QMgrName -n ObjectProfile -t process -g GroupName ReqdAction
```

- ▶ **IBM i**
IBM i의 경우:

```
GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*PRC) USER(GroupName) AUT(ReqdAction) MQMNAME(' QMgrName ')
```

- ▶ **z/OS** z/OS의 경우:

```
RDEFINE MQADMIN QMgrName.PROCESS. ObjectProfile UACC(NONE)  
PERMIT QMgrName.PROCESS. ObjectProfile CLASS(MQADMIN) ID(GroupName) ACCESS(ALTER)
```

이러한 명령은 지정된 채널에 액세스를 부여합니다. 사용자가 채널에서 어떤 MQSC 명령을 수행할 수 있는지를 판별하려면 각 MQSC 명령에 대해 다음 명령을 실행하십시오.

```
RDEFINE MQCMD5 QMgrName. ReqdAction.PROCESS UACC(NONE)  
PERMIT QMgrName. ReqdAction.PROCESS CLASS(MQCMD5) ID(GroupName) ACCESS(ALTER)
```

사용자가 `DISPLAY PROCESS` 명령을 사용하도록 허용하려면 다음 명령을 실행하십시오.

```
RDEFINE MQCMD5 QMgrName.DISPLAY.PROCESS UACC(NONE)  
PERMIT QMgrName.DISPLAY.PROCESS CLASS(MQCMD5) ID(GroupName) ACCESS(READ)
```

변수 이름에는 다음과 같은 의미가 있습니다.

QMGrName

큐 관리자 이름.

▶ **z/OS** z/OS에서 이 값은 또한 큐 공유 그룹의 이름일 수도 있습니다.

ObjectProfile

권한을 변경한 오브젝트 또는 일반 프로파일의 이름입니다.

GroupName

액세스가 부여될 그룹의 이름입니다.

ReqdAction

그룹이 수행할 수 있는 조치:

- ▶ **ULW** UNIX, Linux, and Windows에서 다음 권한의 결합입니다. +chg, +clr, +crt, +dlt, +dsp.
권한 +alladm은 +chg +clr +dlt +dsp와 동등합니다.

- **IBM i** IBM i에서 다음 권한의 결합입니다. *ADMCHG, *ADMCLR, *ADMCRRT, *ADMDLT, *ADMDSP. 권한 *ALLADM은 이러한 개별 권한 모두와 동등합니다.
- **z/OS** z/OS에서 값 ALTER, CLEAR, DEFINE, DELETE 또는 MOVE 중 하나입니다.

일부 이름 목록에 제한된 관리 액세스 부여

비즈니스 요구사항이 있는 각 사용자 그룹에 큐 관리자에서 일부 이름 목록에 부분 관리 액세스를 부여하십시오.

이 태스크 정보

일부 조치를 위해 일부 이름 목록에 제한된 관리 액세스를 부여하려면 운영 체제에 적합한 명령을 사용하십시오.

다음 플랫폼에서는 SET AUTHREC 명령도 사용할 수 있습니다.

- **IBM i** IBM i
- **Linux** Linux
- **UNIX** UNIX
- **IBM i** Windows

참고: **MQ Appliance** IBM MQ Appliance에서는 **SET AUTHREC** 명령만 사용할 수 있습니다.

프로시저

- **ULW** UNIX, Linux, and Windows의 경우:

```
setmqaut -m QMgrName -n ObjectProfile -t namelist -g GroupName ReqdAction
```

- **IBM i** IBM i의 경우:

```
GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*NMLIST) USER(GroupName) AUT(ReqdAction) MQMNAME(' QMgrName ')
```

- **z/OS** z/OS의 경우:

```
RDEFINE MQADMIN QMgrName.NAMELIST. ObjectProfile UACC(NONE)
PERMIT QMgrName.NAMELIST. ObjectProfile CLASS(MQADMIN) ID(GroupName) ACCESS(ALTER)
```

이들 명령은 지정된 이름 목록에 대한 액세스 권한을 부여합니다. 사용자가 이름 목록에서 수행할 수 있는 MQSC 명령을 판별하려면 각 MQSC 명령에 대해 다음 명령을 발행하십시오.

```
RDEFINE MQCMD S QMgrName. ReqdAction.NAMELIST UACC(NONE)
PERMIT QMgrName. ReqdAction.NAMELIST CLASS(MQCMD S) ID(GroupName) ACCESS(ALTER)
```

사용자가 DISPLAY NAMELIST 명령을 사용할 수 있게 하려면 다음 명령을 발행하십시오.

```
RDEFINE MQCMD S QMgrName.DISPLAY.NAMELIST UACC(NONE)
PERMIT QMgrName.DISPLAY.NAMELIST CLASS(MQCMD S) ID(GroupName) ACCESS(READ)
```

변수 이름에는 다음과 같은 의미가 있습니다.

QMgrName

큐 관리자 이름.

z/OS z/OS에서 이 값은 또한 큐 공유 그룹의 이름일 수도 있습니다.

ObjectProfile

권한을 변경한 오브젝트 또는 일반 프로파일의 이름입니다.

GroupName

액세스가 부여될 그룹의 이름입니다.

ReqdAction

그룹이 수행할 수 있는 조치:

- **ULW** UNIX, Linux, and Windows에서 다음 권한의 결합입니다. +chg, +clr, +crt, +dlt, +ctrl, +ctrlx, +dsp. 권한 +alladm은 +chg +clr +dlt +dsp와 동등합니다.
- **IBM i** IBM i에서 다음 권한의 결합입니다. *ADMCHG, *ADMCLR, *ADMCRRT, *ADMCLT, *ADMDSPL, *CTRL, *CTRLX. 권한 *ALLADM은 이러한 개별 권한 모두와 동등합니다.
- **z/OS** z/OS에서 값 ALTER, CLEAR, DEFINE, DELETE 또는 MOVE 중 하나입니다.

일부 서비스에 제한된 관리 액세스 부여

비즈니스 요구사항이 있는 각 사용자 그룹에 큐 관리자에서 일부 서비스에 부분 관리 액세스를 부여하십시오.

이 태스크 정보

일부 조치를 위해 일부 서비스에 제한된 관리 액세스를 부여하려면 운영 체제에 적합한 명령을 사용하십시오.

z/OS z/OS에는 서비스 오브젝트가 존재하지 않습니다.

다음 플랫폼에서는 SET AUTHREC 명령도 사용할 수 있습니다.

- **IBM i** IBM i
- **Linux** Linux
- **UNIX** UNIX
- **IBM i** Windows

참고: **MQ Appliance** IBM MQ Appliance에서는 SET AUTHREC 명령만 사용할 수 있습니다.

프로시저

- **ULW** UNIX, Linux, and Windows의 경우:

```
setmqaut -m QMgrName -n ObjectProfile -t service -g GroupName ReqdAction
```

- IBM i의 경우:

```
GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*SVC) USER(GroupName) AUT(ReqdAction) MQMNAME(' QMgrName ')
```

- **z/OS** z/OS의 경우:

이러한 명령은 지정된 서비스에 액세스를 부여합니다. 사용자가 서비스에서 어떤 MQSC 명령을 수행할 수 있는지를 판별하려면 각 MQSC 명령에 대해 다음 명령을 실행하십시오.

```
RDEFINE MQCMD5 QMgrName. ReqdAction.SERVICE UACC(NONE)  
PERMIT QMgrName. ReqdAction.SERVICE CLASS(MQCMD5) ID(GroupName) ACCESS(ALTER)
```

사용자가 DISPLAY SERVICE 명령을 사용하도록 허용하려면 다음 명령을 실행하십시오.

```
RDEFINE MQCMD5 QMgrName.DISPLAY.SERVICE UACC(NONE)  
PERMIT QMgrName.DISPLAY.SERVICE CLASS(MQCMD5) ID(GroupName) ACCESS(READ)
```

변수 이름에는 다음과 같은 의미가 있습니다.

QMgrName

큐 관리자 이름.

ObjectProfile

권한을 변경한 오브젝트 또는 일반 프로파일의 이름입니다.

GroupName

액세스가 부여될 그룹의 이름입니다.

ReqdAction

그룹이 수행할 수 있는 조치:

- **ULW** UNIX, Linux, and Windows 시스템에서 다음 권한의 결합입니다. +chg, +clr, +crt, +dlt, +ctrl, +ctrlx, +dsp. 권한 +alladm은 +chg +clr +dlt +dsp와 동등합니다.
- **IBM i** IBM i에서 다음 권한의 결합입니다. *ADMCHG, *ADMCLR, *ADMCRRT, *ADMCLT, *ADMDSPP, *CTRL, *CTRLX. 권한 *ALLADM은 이러한 개별 권한 모두와 동등합니다.

큐 관리자 자원의 서브세트에서 전체 관리 액세스 부여

특정 사용자에게 큐 관리자 자원의 전체가 아닌 일부에 대한 전체 관리 액세스를 제공해야 합니다. 수행해야 하는 조치를 판별하려면 이 테이블을 사용하십시오.

표 70. 큐 관리자 자원의 서브세트에 전체 관리 액세스 부여	
사용자가 관리해야 하는 오브젝트 유형	수행 조치
큐	333 페이지의 『일부 큐에 전체 관리 액세스 부여』에 설명된 대로 필수 큐에 전체 관리 액세스를 부여하십시오.
토픽	334 페이지의 『일부 토픽에 전체 관리 액세스 부여』에 설명된 대로 필수 토픽에 전체 관리 액세스를 부여하십시오.
채널	335 페이지의 『일부 채널에 전체 관리 액세스 부여』에 설명된 대로 필수 채널에 전체 관리 액세스를 부여하십시오.
큐 관리자	336 페이지의 『큐 관리자에 전체 관리 액세스 부여』에 설명된 대로 큐 관리자에 전체 관리 액세스를 부여하십시오.
프로세스	337 페이지의 『일부 프로세스에 전체 관리 액세스 부여』에 설명된 대로 필수 프로세스에 전체 관리 액세스를 부여하십시오.
이름 목록	338 페이지의 『일부 이름 목록에 전체 관리 액세스 부여』에 설명된 대로 필수 이름 목록에 전체 관리 액세스를 부여하십시오.
서비스	338 페이지의 『일부 서비스에 전체 관리 액세스 부여』에 설명된 대로 필수 서비스에 전체 관리 액세스를 부여하십시오.

일부 큐에 전체 관리 액세스 부여

비즈니스 요구사항이 있는 각 사용자 그룹에 큐 관리자에서 일부 큐에 전체 관리 액세스를 부여하십시오.

이 태스크 정보

일부 큐에 전체 관리 액세스를 부여하려면 운영 체제에 적합한 명령을 사용하십시오.

다음 플랫폼에서는 SET AUTHREC 명령도 사용할 수 있습니다.

- ▶ **IBM i** IBM i
- ▶ **Linux** Linux
- ▶ **UNIX** UNIX
- ▶ **IBM i** Windows

참고: **MQ Appliance** IBM MQ Appliance에서는 **SET AUTHREC** 명령만 사용할 수 있습니다.

프로시저

- ▶ **ULW**
UNIX, Linux, and Windows의 경우:

```
setmqaut -m QMgrName -n ObjectProfile -t queue -g GroupName +alladm
```

- ▶ **IBM i**
IBM i의 경우:

```
GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*Q) USER(GroupName) AUT(*ALLADM) MQMNAME(' QMgrName')
```

- ▶ **z/OS**
z/OS의 경우:

```
RDEFINE MQADMIN QMgrName.QUEUE. ObjectProfile UACC(NONE)  
PERMIT QMgrName.QUEUE. ObjectProfile CLASS(MQADMIN) ID(GroupName) ACCESS(ALTER)
```

변수 이름에는 다음과 같은 의미가 있습니다.

QMGrName

큐 관리자 이름.

▶ **z/OS** z/OS에서 이 값은 또한 큐 공유 그룹의 이름일 수도 있습니다.

ObjectProfile

권한을 변경한 오브젝트 또는 일반 프로파일의 이름입니다.

GroupName

액세스가 부여될 그룹의 이름입니다.

일부 토픽에 전체 관리 액세스 부여

비즈니스 요구사항이 있는 각 사용자 그룹에 큐 관리자에서 일부 토픽에 전체 관리 액세스를 부여하십시오.

이 태스크 정보

일부 조치를 위해 일부 토픽에 전체 관리 액세스를 부여하려면 운영 체제에 적합한 명령을 사용하십시오.

다음 플랫폼에서는 **SET AUTHREC** 명령도 사용할 수 있습니다.

- ▶ **IBM i** IBM i
- ▶ **Linux** Linux
- ▶ **UNIX** UNIX
- ▶ **IBM i** Windows

참고: **MQ Appliance** IBM MQ Appliance에서는 **SET AUTHREC** 명령만 사용할 수 있습니다.

프로시저

ULW

UNIX, Linux, and Windows의 경우:

```
setmqaut -m QMgrName -n ObjectProfile -t topic -g GroupName +alladm
```

IBM i

IBM i의 경우:

```
GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*TOPIC) USER(GroupName) AUT(ALLADM) MQMNAME(' QMgrName ')
```

z/OS

z/OS의 경우:

```
RDEFINE MQADMIN QMgrName.TOPIC. ObjectProfile UACC(NONE)  
PERMIT QMgrName.TOPIC. ObjectProfile CLASS(MQADMIN) ID(GroupName) ACCESS(ALTER)
```

변수 이름에는 다음과 같은 의미가 있습니다.

QMGrName

큐 관리자 이름.

z/OS

z/OS에서 이 값은 또한 큐 공유 그룹의 이름일 수도 있습니다.

ObjectProfile

권한을 변경한 오브젝트 또는 일반 프로파일의 이름입니다.

GroupName

액세스가 부여될 그룹의 이름입니다.

일부 채널에 전체 관리 액세스 부여

비즈니스 요구사항이 있는 각 사용자 그룹에 큐 관리자에서 일부 채널에 전체 관리 액세스를 부여하십시오.

이 태스크 정보

일부 채널에 전체 관리 액세스를 부여하려면 운영 체제에 적합한 명령을 사용하십시오.

다음 플랫폼에서는 [SET AUTHREC](#) 명령도 사용할 수 있습니다.

IBM i

IBM i

Linux

Linux

UNIX

UNIX

IBM i

Windows

참고: [MQ Appliance](#) IBM MQ Appliance에서는 **SET AUTHREC** 명령만 사용할 수 있습니다.

프로시저

ULW

UNIX, Linux, and Windows의 경우:

```
setmqaut -m QMgrName -n ObjectProfile -t channel -g GroupName +alladm
```

IBM i

IBM i의 경우:

```
GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*CHL) USER(GroupName) AUT(ALLADM) MQMNAME(' QMgrName ')
```

- ▶ **z/OS**

z/OS의 경우:

```
RDEFINE MQADMIN QMgrName.CHANNEL. ObjectProfile UACC(NONE)  
PERMIT QMgrName.CHANNEL. ObjectProfile CLASS(MQADMIN) ID(GroupName) ACCESS(ALTER)
```

변수 이름에는 다음과 같은 의미가 있습니다.

QMGrName

큐 관리자 이름.

- ▶ **z/OS**

z/OS에서 이 값은 또한 큐 공유 그룹의 이름일 수도 있습니다.

ObjectProfile

권한을 변경한 오브젝트 또는 일반 프로파일의 이름입니다.

GroupName

액세스가 부여될 그룹의 이름입니다.

큐 관리자에 전체 관리 액세스 부여

비즈니스 요구사항이 있는 각 사용자 그룹에 큐 관리자에 대한 전체 관리 액세스를 부여하십시오.

이 태스크 정보

일부 큐 관리자에 전체 관리 액세스를 부여하려면 운영 체제에 적합한 명령을 사용하십시오.

다음 플랫폼에서는 [SET AUTHREC](#) 명령도 사용할 수 있습니다.

- ▶ **IBM i** IBM i
- ▶ **Linux** Linux
- ▶ **UNIX** UNIX
- ▶ **IBM i** Windows

참고: [MQ Appliance](#) IBM MQ Appliance에서는 **SET AUTHREC** 명령만 사용할 수 있습니다.

프로시저

- ▶ **ULW**

UNIX, Linux, and Windows의 경우:

```
setmqaut -m QMgrName -t qmgr -g GroupName +alladm
```

- ▶ **IBM i**

IBM i의 경우:

```
GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*MQM) USER(GroupName) AUT(*ALLADM) MQMNAME(' QMgrName ')
```

- ▶ **z/OS**


z/OS의 경우:

```
RDEFINE MQADMIN QMgrName.QMGR UACC(NONE)  
PERMIT QMgrName.QMGR CLASS(MQADMIN) ID(GroupName) ACCESS(ALTER)
```

변수 이름에는 다음과 같은 의미가 있습니다.

QMgrName

큐 관리자 이름.

 z/OS에서 이 값은 또한 큐 공유 그룹의 이름일 수도 있습니다.

ObjectProfile

권한을 변경한 오브젝트 또는 일반 프로파일의 이름입니다.

GroupName

액세스가 부여될 그룹의 이름입니다.





일부 프로세스에 전체 관리 액세스 부여


비즈니스 요구사항이 있는 각 사용자 그룹에 큐 관리자에서 일부 프로세스에 전체 관리 액세스를 부여하십시오.

이 태스크 정보


일부 프로세스에 전체 관리 액세스를 부여하려면 운영 체제에 적합한 명령을 사용하십시오.

다음 플랫폼에서는 `SET AUTHREC` 명령도 사용할 수 있습니다.


-  IBM i
-  Linux
-  UNIX
-  Windows

참고:  IBM MQ Appliance에서는 `SET AUTHREC` 명령만 사용할 수 있습니다.


프로시저

-  UNIX, Linux, and Windows의 경우:

```
setmqaut -m QMgrName -n ObjectProfile -t process -g GroupName +alladm
```

-  IBM i의 경우:

```
GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*PRC) USER(GroupName) AUT(*ALLADM) MQMNAME(' QMgrName ')
```


-  z/OS의 경우:

```
RDEFINE MQADMIN QMgrName.CHANNEL. ObjectProfile UACC(NONE)  
PERMIT QMgrName.PROCESS. ObjectProfile CLASS(MQADMIN) ID(GroupName) ACCESS(ALTER)
```

변수 이름에는 다음과 같은 의미가 있습니다.

QMgrName

큐 관리자 이름.

 z/OS에서 이 값은 또한 큐 공유 그룹의 이름일 수도 있습니다.

ObjectProfile

권한을 변경한 오브젝트 또는 일반 프로파일의 이름입니다.

GroupName

액세스가 부여될 그룹의 이름입니다.

일부 이름 목록에 전체 관리 액세스 부여

비즈니스 요구사항이 있는 각 사용자 그룹에 큐 관리자에서 일부 이름 목록에 전체 관리 액세스를 부여하십시오.

이 태스크 정보

일부 이름 목록에 전체 관리 액세스를 부여하려면 운영 체제에 적합한 명령을 사용하십시오.

다음 플랫폼에서는 [SET AUTHREC](#) 명령도 사용할 수 있습니다.

- ▶ **IBM i** IBM i
- ▶ **Linux** Linux
- ▶ **UNIX** UNIX
- ▶ **IBM i** Windows

참고: [MQ Appliance](#) IBM MQ Appliance에서는 **SET AUTHREC** 명령만 사용할 수 있습니다.

프로시저

- ▶ **ULW**
UNIX, Linux, and Windows의 경우:

```
setmqaut -m QMgrName -n ObjectProfile -t namelist -g GroupName +alladm
```

- ▶ **IBM i**
IBM i의 경우:

```
GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*NMLIST) USER(GroupName) AUT(*ALLADM) MQMNAME(' QMgrName ')
```

- ▶ **z/OS**
z/OS의 경우:

```
RDEFINE MQADMIN QMgrName.NAMELIST. ObjectProfile UACC(NONE)  
PERMIT QMgrName.NAMELIST. ObjectProfile CLASS(MQADMIN) ID(GroupName) ACCESS(ALTER)
```

변수 이름에는 다음과 같은 의미가 있습니다.

QMgrName

큐 관리자 이름.

▶ **z/OS** z/OS에서 이 값은 또한 큐 공유 그룹의 이름일 수도 있습니다.

ObjectProfile

권한을 변경한 오브젝트 또는 일반 프로파일의 이름입니다.

GroupName

액세스가 부여될 그룹의 이름입니다.

일부 서비스에 전체 관리 액세스 부여




비즈니스 요구사항이 있는 각 사용자 그룹에 큐 관리자에서 일부 서비스에 전체 관리 액세스를 부여하십시오.


이 태스크 정보

일부 서비스 전체 관리 액세스를 부여하려면 운영 체제에 적합한 명령을 사용하십시오.


다음 플랫폼에서는 [SET AUTHREC](#) 명령도 사용할 수 있습니다.

- ▶ **IBM i** IBM i


-  Linux
-  UNIX
-  Windows

참고:  IBM MQ Appliance에서는 **SET AUTHREC** 명령만 사용할 수 있습니다.


프로시저

-  UNIX, Linux, and Windows의 경우:

```
setmqaut -m QMgrName -n ObjectProfile -t service -g GroupName +alladm
```

-  IBM i의 경우:

```
GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*SVC) USER(GroupName) AUT(*ALLADM) MQMNAME(' QMgrName ')
```


-  z/OS의 경우:

```
RDEFINE MQADMIN QMgrName.SERVICE. ObjectProfile UACC(NONE)
PERMIT QMgrName.SERVICE. ObjectProfile CLASS(MQADMIN) ID(GroupName) ACCESS(ALTER)
```

변수 이름에는 다음과 같은 의미가 있습니다.

QMGrName

큐 관리자 이름.

 z/OS에서 이 값은 또한 큐 공유 그룹의 이름일 수도 있습니다.

ObjectProfile

권한을 변경한 오브젝트 또는 일반 프로파일의 이름입니다.

GroupName

액세스가 부여될 그룹의 이름입니다.

큐 관리자에서 모든 자원에 읽기 전용 액세스 부여


비즈니스 요구사항이 있는 각 사용자 그룹에 큐 관리자에서 모든 자원에 읽기 전용 액세스를 부여하십시오.

이 태스크 정보

역할 기반 권한 추가 마법사 또는 운영 체제에 적합한 명령을 사용하십시오.

다음 플랫폼에서는 **SET AUTHREC** 명령도 사용할 수 있습니다.

-  IBM i
-  Linux
-  UNIX
-  Windows

참고:  IBM MQ Appliance에서는 **SET AUTHREC** 명령만 사용할 수 있습니다.

권한 세부사항을 변경한 후 **REFRESH SECURITY** 명령을 사용하여 보안 새로 고치기를 수행하십시오.

프로시저

- 마법사 사용:

a) IBM MQ Explorer 네비게이터 분할창에서 큐 관리자를 마우스의 오른쪽 단추로 클릭하고 **오브젝트 권한 > 역할 기반 권한 추가**를 클릭하십시오.
역할 기반 권한 추가 마법사가 열립니다.

- 

UNIX 및 Windows 시스템의 경우 다음 명령을 실행하십시오.

```
setmqaut -m QMgrName -n ** -t queue -g GroupName +browse +dsp
setmqaut -m QMgrName -n SYSTEM.ADMIN.COMMAND.QUEUE -t queue -g GroupName +dsp +inq +put
setmqaut -m QMgrName -n SYSTEM.MQEXPLORER.REPLY.MODEL -t queue -g GroupName +dsp +inq +get
+put
setmqaut -m QMgrName -n ** -t topic -g GroupName +dsp
setmqaut -m QMgrName -n ** -t channel -g GroupName +dsp +inq
setmqaut -m QMgrName -n ** -t clntconn -g GroupName +dsp
setmqaut -m QMgrName -n ** -t authinfo -g GroupName +dsp
setmqaut -m QMgrName -n ** -t listener -g GroupName +dsp
setmqaut -m QMgrName -n ** -t namelist -g GroupName +dsp
setmqaut -m QMgrName -n ** -t process -g GroupName +dsp
setmqaut -m QMgrName -n ** -t service -g GroupName +dsp
setmqaut -m QMgrName -t qmgr -g GroupName +dsp +inq +connect
```

SYSTEM.ADMIN.COMMAND.QUEUE 및 SYSTEM.MQEXPLORER.REPLY.MODEL 은 IBM MQ Explorer를 사용하여려는 경우에만 필요합니다.

- 

IBM i의 경우 다음 명령을 실행하십시오.

```
GRTMQMAUT OBJ(*ALL) OBJTYPE(*Q) USER('GroupName') AUT(*ADM DSP *BROWSE) MQMNAME('QMgrName')
GRTMQMAUT OBJ(*ALL) OBJTYPE(*TOPIC) USER('GroupName') AUT(*ADM DSP) MQMNAME('QMgrName')
GRTMQMAUT OBJ(*ALL) OBJTYPE(*CHL) USER('GroupName') AUT(*ADM DSP *INQ) MQMNAME('QMgrName')
GRTMQMAUT OBJ(*ALL) OBJTYPE(*CLTCN) USER('GroupName') AUT(*ADM DSP) MQMNAME('QMgrName')
GRTMQMAUT OBJ(*ALL) OBJTYPE(*AUTHINFO) USER('GroupName') AUT(*ADM DSP) MQMNAME('QMgrName')
GRTMQMAUT OBJ(*ALL) OBJTYPE(*LSR) USER('GroupName') AUT(*ADM DSP) MQMNAME('QMgrName')
GRTMQMAUT OBJ(*ALL) OBJTYPE(*NMLIST) USER('GroupName') AUT(*ADM DSP) MQMNAME('QMgrName')
GRTMQMAUT OBJ(*ALL) OBJTYPE(*PRC) USER('GroupName') AUT(*ADM DSP) MQMNAME('QMgrName')
GRTMQMAUT OBJ(*ALL) OBJTYPE(*SVC) USER('GroupName') AUT(*ADM DSP) MQMNAME('QMgrName')
GRTMQMAUT OBJ('object-name') OBJTYPE(*MQM) USER('GroupName') AUT(*ADM DSP *CONNECT *INQ)
MQMNAME('QMgrName')
```

- 


z/OS의 경우 다음 명령을 실행하십시오.

```
RDEFINE MQQUEUE QMgrName.** UACC(NONE)
PERMIT QMgrName.** CLASS(MQQUEUE) ID(GroupName) ACCESS(READ)
RDEFINE MXTOPIC QMgrName.** UACC(NONE)
PERMIT QMgrName.** CLASS(MXTOPIC) ID(GroupName) ACCESS(READ)
RDEFINE MQPROC QMgrName.** UACC(NONE)
PERMIT QMgrName.** CLASS(MQPROC) ID(GroupName) ACCESS(READ)
RDEFINE MQNLIST QMgrName.** UACC(NONE)
PERMIT QMgrName.** CLASS(MQNLIST) ID(GroupName) ACCESS(READ)
RDEFINE MQCONN QMgrName.BATCH UACC(NONE)
PERMIT QMgrName.BATCH CLASS(MQCONN) ID(GroupName) ACCESS(READ)
RDEFINE MQCONN QMgrName.CICS UACC(NONE)
PERMIT QMgrName.CICS CLASS(MQCONN) ID(GroupName) ACCESS(READ)
RDEFINE MQCONN QMgrName.IMS UACC(NONE)
PERMIT QMgrName.IMS CLASS(MQCONN) ID(GroupName) ACCESS(READ)
RDEFINE MQCONN QMgrName.CHIN UACC(NONE)
PERMIT QMgrName.CHIN CLASS(MQCONN) ID(GroupName) ACCESS(READ)
```

변수 이름에는 다음과 같은 의미가 있습니다.

QMgrName

큐 관리자 이름.

 z/OS에서 이 값은 또한 큐 공유 그룹의 이름일 수도 있습니다.

GroupName

액세스가 부여될 그룹의 이름입니다.

큐 관리자에서 모든 자원에 전체 관리 액세스 부여

비즈니스 요구사항이 있는 각 사용자 그룹에 큐 관리자에서 모든 자원에 전체 관리 액세스를 부여하십시오.

이 태스크 정보

역할 기반 권한 추가 마법사 또는 운영 체제에 적합한 명령을 사용할 수 있습니다.

다음 플랫폼에서는 `SET AUTHREC` 명령도 사용할 수 있습니다.

- ▶ IBM i IBM i
- ▶ Linux Linux
- ▶ UNIX UNIX
- ▶ IBM i Windows

참고: ▶ MQ Appliance IBM MQ Appliance에서는 `SET AUTHREC` 명령만 사용할 수 있습니다.

참고사항: ▶ ULW

1. `runmqsc` 를 사용하여 IBM MQ Explorer 대신 큐 관리자를 관리하는 경우, `SYSTEM.MQSC.REPLY.QUEUE`, `SYSTEM.MQEXPLORER.REPLY.MODEL` 큐.
2. 큐 관리자의 모든 자원에 대한 사용자 액세스 권한을 부여하는 경우, 해당 사용자에게 `qm.ini` 파일에 대한 읽기 액세스 권한이 없으면 사용자가 실행할 수 없는 몇 가지 명령이 있습니다. `qm.ini` 파일을 읽을 수 있는 `mqm` 사용자가 아닌 사용자에 대한 제한사항 때문입니다.

사용자가 `qm.ini` 파일에 대한 읽기 액세스 권한을 부여한 경우가 아니면 다음 명령을 실행할 수 없습니다.

- TLS를 사용하도록 구성된 채널 정의
- `qm.ini`에 정의된 자동 구성 삽입 변수를 사용하여 채널 정의

프로시저

- 마법사를 사용하는 경우 IBM MQ Explorer 네비게이터 분할창에서 큐 관리자를 마우스 오른쪽 단추로 클릭하고 **오브젝트 권한 > 역할 기반 권한 추가**를 클릭하십시오.

역할 기반 권한 추가 마법사가 열립니다.

- ▶ Linux ▶ UNIX

UNIX and Linux 시스템의 경우 다음 명령을 실행하십시오.

```
setmqaut -m QMgrName -n '**' -t queue -g GroupName +alladm +browse
setmqaut -m QMgrName -n @class -t queue -g GroupName +crt
setmqaut -m QMgrName -n SYSTEM.ADMIN.COMMAND.QUEUE -t queue -g GroupName +dsp +inq +put
setmqaut -m QMgrName -n SYSTEM.MQEXPLORER.REPLY.MODEL -t queue -g GroupName +dsp +inq +get +put
setmqaut -m QMgrName -n '**' -t topic -g GroupName +alladm
setmqaut -m QMgrName -n @class -t topic -g GroupName +crt
setmqaut -m QMgrName -n '**' -t channel -g GroupName +alladm
setmqaut -m QMgrName -n @class -t channel -g GroupName +crt
setmqaut -m QMgrName -n '**' -t clntconn -g GroupName +alladm
setmqaut -m QMgrName -n @class -t clntconn -g GroupName +crt
setmqaut -m QMgrName -n '**' -t authinfo -g GroupName +alladm
setmqaut -m QMgrName -n @class -t authinfo -g GroupName +crt
setmqaut -m QMgrName -n '**' -t listener -g GroupName +alladm
setmqaut -m QMgrName -n @class -t listener -g GroupName +crt
setmqaut -m QMgrName -n '**' -t namelist -g GroupName +alladm
setmqaut -m QMgrName -n @class -t namelist -g GroupName +crt
setmqaut -m QMgrName -n '**' -t process -g GroupName +alladm
setmqaut -m QMgrName -n @class -t process -g GroupName +crt
setmqaut -m QMgrName -n '**' -t service -g GroupName +alladm
setmqaut -m QMgrName -n @class -t service -g GroupName +crt
setmqaut -m QMgrName -t qmgr -g GroupName +alladm +connect
```

@class 에 대한 자세한 정보는 `setmqaut` 을 참조하십시오.

• **Windows**

Windows 시스템의 경우 UNIX and Linux 시스템에서와 같은 명령을 발행하지만 @class 대신에 프로파일 이름 @CLASS를 사용하십시오.

• **IBM i**

IBM i의 경우 다음 명령을 실행하십시오.

```
GRTMQMAUT OBJ(*ALL) OBJTYPE(*ALL) USER(' GroupName ') AUT(*ALLADM) MQMNAME(' QMgrName ')
```

• **z/OS**

z/OS의 경우 다음 명령을 실행하십시오.

```
RDEFINE MQADMIN QMgrName.*.** UACC(NONE)
PERMIT QMgrName.*.** CLASS(MQADMIN) ID(GroupName) ACCESS(ALTER)
```

변수 이름에는 다음과 같은 의미가 있습니다.

QMgrName

큐 관리자 이름.

z/OS

z/OS에서 이 값은 또한 큐 공유 그룹의 이름일 수도 있습니다.

GroupName

액세스가 부여될 그룹의 이름입니다.

큐 관리자에 대한 연결성 제거

사용자 애플리케이션이 큐 관리자에 연결하기를 원치 않는 경우에는 이에 대한 연결 권한을 제거하십시오.

이 태스크 정보

사용자의 운영 체제에 적합한 명령을 사용하여 큐 관리자에 연결하기 위한 모든 사용자의 권한을 취소하십시오.

UNIX, Linux, Windows 시스템 및 IBM i에서 [DELETE AUTHREC](#) 명령을 사용할 수도 있습니다.

참고: IBM MQ 어플라이언스에서는 **DELETE AUTHREC** 명령만을 사용할 수 있습니다.

프로시저

• **ULW**

UNIX, Linux, and Windows 시스템의 경우 다음 명령을 실행하십시오.

```
setmqaut -m QMgrName -t qmgr -g GroupName -connect
```

• **IBM i**

IBM i의 경우 다음 명령을 실행하십시오.

```
RVKMQMAUT OBJ (' QMgrName') OBJTYPE(*MQM) USER(*ALL) AUT(*CONNECT)
```

• **z/OS**

z/OS의 경우 다음 명령을 실행하십시오.


```
RDEFINE MQCONN QMgrName.BATCH UACC(NONE)
RDEFINE MQCONN QMgrName.CHIN UACC(NONE)
RDEFINE MQCONN QMgrName.CICS UACC(NONE)
RDEFINE MQCONN QMgrName.IMS UACC(NONE)
```

PERMIT 명령을 발행하지 마십시오.

변수 이름에는 다음과 같은 의미가 있습니다.

QMgrName

큐 관리자 이름.

 z/OS에서 이 값은 또한 큐 공유 그룹의 이름일 수도 있습니다.

GroupName

액세스를 거부할 그룹의 이름

사용자 애플리케이션이 큐 관리자에 연결할 수 있도록 허용

사용자 애플리케이션이 큐 관리자에 연결할 수 있도록 허용하고 싶습니다. 취해야 할 조치를 판별하려면 이 토픽의 테이블을 사용하십시오.

먼저 클라이언트 애플리케이션이 큐 관리자에 연결하는지 여부를 판별하십시오.

큐 관리자에 연결할 애플리케이션이 모두 클라이언트 애플리케이션이 아니면 350 페이지의 『큐 관리자에 대한 원격 액세스 사용 안함으로 설정』에 설명된 대로 원격 액세스를 사용 안함으로 설정하십시오.

큐 관리자에 연결할 애플리케이션의 하나 이상의 클라이언트 애플리케이션이면 343 페이지의 『큐 관리자에 대한 원격 연결성 보안』에 설명된 대로 원격 연결성을 보안 설정하십시오.

두 경우 모두 350 페이지의 『연결 보안 설정』에 설명된 대로 연결 보안을 설정하십시오.

큐 관리자에 연결 중인 각 사용자의 자원에 대한 액세스를 제어하려면 다음 테이블을 참조하십시오. 첫 번째 열의 명령문이 참이면 두 번째 열에 나열된 조치를 취하십시오.

설명	수행 조치
큐를 사용하는 애플리케이션이 있습니다.	351 페이지의 『큐에 대한 사용자 액세스 제어』 참조
토픽을 사용하는 애플리케이션이 있습니다.	357 페이지의 『토픽에 대한 사용자 액세스 제어』 참조
큐 관리자 오브젝트에서 조회한 애플리케이션이 있습니다.	359 페이지의 『큐 관리자에서 조사하기 위한 권한 부여』 참조
프로젝트 오브젝트를 사용하는 애플리케이션이 있습니다.	359 페이지의 『프로세스에 액세스하기 위한 권한 부여』 참조
이름 목록을 사용하는 애플리케이션이 있습니다.	360 페이지의 『이름 목록에 액세스하기 위한 권한 부여』 참조

큐 관리자에 대한 원격 연결성 보안

TLS, 보안 엑시트, 채널 인증 레코드 또는 이러한 메소드의 결합을 사용하여 큐 관리자에 대한 원격 연결성을 보안 설정할 수 있습니다.

이 태스크 정보

클라이언트 워크스테이션에서 클라이언트 연결 채널을 사용하거나 서버에서 서버 연결 채널을 사용하여 큐 관리자에 클라이언트를 연결합니다. 다음 방법 중 하나로 이러한 연결을 보안 설정하십시오.

프로시저

1. 채널 인증 레코드와 함께 TLS 사용:

- 모든 식별 이름(DN)을 USERSRC(NOACCESS)에 맵핑하려면 SSLPEERMAP 채널 인증 레코드를 사용하여 DN이 채널을 열지 못하도록 하십시오.
- 특정 DN 또는 DN 세트를 USERSRC(CHANNEL)에 맵핑하려면 SSLPEERMAP 채널 인증 레코드를 사용하여 채널을 열도록 허용하십시오.

2. 보안 엑시트와 함께 TLS 사용:

- 서버 연결 채널의 MCAUSER를 권한이 없는 사용자 ID로 설정하십시오.
- MQCD 구조에서 엑시트로 전달된 SSLPeerNamePtr 및 SSLPeerNameLength 필드에서 수신하는 TLS DN의 값에 따라 MCAUSER 값을 지정하도록 보안 엑시트를 작성하십시오.

3. 고정된 채널 정의 값과 함께 TLS 사용:
 - a) 서버 연결 채널의 SSLPEER를 특정 값으로 설정하거나 값 범위를 줄이십시오.
 - b) 서버 연결 채널의 MCAUSER를 채널을 실행해야 하는 사용자 ID로 설정하십시오.
4. TLS를 사용하지 않는 채널에서 채널 인증 레코드 사용:
 - a) 주소 맵핑 채널 인증 레코드를 ADDRESS(*) 및 USERSRC(NOACCESS)와 함께 사용하여 IP 주소가 채널을 열지 못하도록 하십시오.
 - b) 이러한 주소에 대한 주소 맵핑 채널 인증 레코드를 USERSRC(CHANNEL)와 함께 사용하여 특정 IP 주소가 채널을 열도록 허용하십시오.
5. 보안 엑시트 사용:
 - a) 사용자가 선택하는 특성을 기반으로(예: 발신 IP 주소) 연결을 인증하려면 보안 엑시트를 작성하십시오.
6. 특정 상황에 필요한 경우 보안 엑시트와 함께 채널 인증 레코드를 사용하거나 세 메소드를 모두 사용할 수 있습니다.

특정 IP 주소 차단

채널 인증 레코드를 사용하여 특정 채널이 IP 주소의 인바운드 연결을 승인하지 않도록 하거나 전체 큐 관리자가 IP 주소의 액세스를 허용하지 않도록 할 수 있습니다.

시작하기 전에

다음 명령을 실행하여 채널 인증 레코드를 사용하십시오.

```
ALTER QMGR CHLAUTH(ENABLED)
```

이 태스크 정보

특정 채널에서 인바운드 연결을 승인하지 않고 올바른 채널 이름을 사용하는 경우에만 연결을 승인하도록 하려는 경우 IP 주소를 차단하도록 한 가지 규칙 유형을 사용할 수 있습니다. 전체 큐 관리자에 대한 IP 주소 액세스를 허용하지 않으려면 일반적으로 방화벽을 사용하여 이를 영구적으로 차단합니다. 그러나 다른 규칙 유형을 사용하여 예를 들어 방화벽 업데이트를 기다리는 동안 임시로 몇 개의 주소를 차단할 수 있습니다.

프로시저

- 특정 채널을 사용하지 않도록 IP 주소를 차단하려면 MQSC 명령 **SET CHLAUTH**, 또는 PCF 명령 **Set Channel Authentication Record**를 사용하여 채널 인증 레코드를 설정하십시오.

```
SET CHLAUTH(generic-channel-name) TYPE(ADDRESSMAP) ADDRESS(generic-ip-address)
USERSRC(NOACCESS)
```

명령에 3개 부분이 있습니다.

SET CHLAUTH (*generic-channel-name*)

전체 큐 관리자, 단일 채널 또는 채널 범위의 연결을 차단하고 싶은지 여부를 제어하려면 이 명령 부분을 사용합니다. 여기에 넣는 것이 어떤 영역이 포함되는지를 판별합니다.

예를 들면, 다음과 같습니다.

- SET CHLAUTH('*') - 큐 관리자에서 모든 채널을 차단합니다. 즉, 전체 큐 관리자입니다.
- SET CHLAUTH('SYSTEM.*') - SYSTEM으로 시작하는 모든 채널을 차단합니다.
- SET CHLAUTH('SYSTEM.DEF.SVRCONN') - SYSTEM.DEF.SVRCONN 채널을 차단합니다.

CHLAUTH 규칙 유형

명령의 이 부분을 사용하여 명령의 유형을 지정하고, 단일 주소 또는 주소 목록을 제공할지 여부를 판별합니다.

예를 들면, 다음과 같습니다.

- TYPE(ADDRESSMAP) - 단일 주소 또는 와일드카드 주소를 제공하려면 ADDRESSMAP을 사용합니다. 예를 들어, ADDRESS('192.168.*')은 192.168로 시작하여 IP 주소에서 나오는 모든 연결을 차단합니다.

패턴이 있는 IP 주소 필터링에 대한 자세한 정보는 [일반 IP 주소](#)를 참조하십시오.

- TYPE (BLOCKADDR) - 차단할 주소 목록을 제공하고 싶은 경우 BLOCKADDR를 사용합니다.

추가 매개변수

이러한 매개변수는 명령의 두 번째 부분에서 사용한 규칙의 유형에 의존합니다.

- TYPE (ADDRESSMAP)의 경우 ADDRESS를 사용합니다.
- TYPE (BLOCKADDR)의 경우 ADDRLIST를 사용합니다.

관련 참조

[SET CHLAUTH](#)

큐 관리자가 실행 중이 아닌 경우 특정 IP 주소를 일시적으로 차단

큐 관리자가 실행 중이 아니므로 MQSC 명령을 실행할 수 없을 때 특정 IP 주소 또는 주소 범위를 차단하고 싶은 수도 있습니다. `blockaddr.ini` 파일을 수정하여 예외적으로 IP 주소를 일시적으로 차단할 수 있습니다.

이 태스크 정보

`blockaddr.ini` 파일에는 큐 관리자가 사용하는 BLOCKADDR 정의의 사본이 포함됩니다. 이 파일은 리스너가 큐 관리자보다 먼저 시작된 경우 리스너가 판독합니다. 이러한 상황에서 리스너는 `blockaddr.ini` 파일에 수동으로 추가한 값을 사용합니다.

그러나 큐 관리자가 시작될 때 BLOCKADDR 정의의 세트를 `blockaddr.ini` 파일에 기록하여 사용자가 수행했을 수 있는 모든 수동 편집을 겹쳐씹니다. 마찬가지로, **SET CHLAUTH** 명령을 사용하여 BLOCKADDR 정의를 추가하거나 삭제할 때마다 `blockaddr.ini` 파일이 업데이트됩니다. 그러므로 큐 관리자가 실행 중일 때 **SET CHLAUTH** 명령을 사용하는 방법으로만 BLOCKADDR 정의를 영구적으로 변경할 수 있습니다.

프로시저

1. 텍스트 편집기에서 `blockaddr.ini` 파일을 여십시오.
파일은 큐 관리자의 데이터 디렉토리에 있습니다.
2. IP 주소를 단순 키워드-값 쌍으로서 추가하십시오. 여기서 키워드는 `Addr`입니다.
패턴이 있는 IP 주소 필터링에 대한 자세한 정보는 [일반 IP 주소](#)를 참조하십시오.
예를 들면, 다음과 같습니다.

```
Addr = 192.0.2.0  
Addr = 192.0.*  
Addr = 192.0.2.1-8
```

관련 태스크

[344 페이지의 『특정 IP 주소 차단』](#)

채널 인증 레코드를 사용하여 특정 채널이 IP 주소의 인바운드 연결을 승인하지 않도록 하거나 전체 큐 관리자가 IP 주소의 액세스를 허용하지 않도록 할 수 있습니다.

관련 참조

[SET CHLAUTH](#)

특정 사용자 ID 차단

채널이 종료되도록 하는 사용자 ID가 확인된 경우 해당 사용자 ID를 지정하여 특정 사용자가 채널을 사용하지 못하게 할 수 있습니다. 채널 인증 레코드를 설정하여 이를 수행합니다.

시작하기 전에

다음과 같이 채널 인증 레코드를 사용할 수 있는지 확인하십시오.

```
ALTER QMGR CHLAUTH(ENABLED)
```


프로시저

MQSC 명령 **SET CHLAUTH** 또는 PCF 명령 **Set Channel Authentication Record**를 사용하여 채널 인증 레코드를 설정하십시오. 예를 들어, 다음 MQSC 명령을 실행할 수 있습니다.

```
SET CHLAUTH(' generic-channel-name ') TYPE(BLOCKUSER) USERLIST(userID1, userID2)
```

*generic-channel-name*은 액세스를 제어하려는 채널의 이름이거나 채널 이름과 일치하는 와일드카드로서 별표(*) 기호를 포함하는 패턴입니다.

TYPE(BLOCKUSER)에서 제공되는 사용자 목록만 SVRCONN 채널에 적용되고 큐 관리자 채널에 대해서는 큐 관리자가 적용되지 않습니다.

userID1 및 *userID2*는 채널을 사용하지 못하도록 할 각 사용자의 ID입니다. 특수 값 *MQADMIN을 지정하여 권한이 부여된 관리 사용자를 참조할 수도 있습니다. 권한이 있는 사용자에 대한 자세한 정보는 [297 페이지의 『권한이 있는 사용자』](#)의 내용을 참조하십시오. *MQADMIN에 대한 자세한 정보는 [SET CHLAUTH](#)를 참조하십시오.

관련 참조

SET CHLAUTH

MCAUSER 사용자 ID에 리모트 큐 관리자 맵핑 채널이 연결 중인 원래 큐 관리자에 따라 채널 인증 레코드를 사용하여 채널의 *MCAUSER* 속성을 설정할 수 있습니다.

시작하기 전에

다음과 같이 채널 인증 레코드를 사용할 수 있는지 확인하십시오.

```
ALTER QMGR CHLAUTH(ENABLED)
```

이 태스크 정보

선택적으로 규칙이 적용되는 IP 주소를 제한할 수 있습니다.

이 기술은 서버 연결 채널에는 적용되지 않습니다. 다음 명령에서 서버-연결 채널의 이름을 지정하는 경우 이는 아무런 효과가 없습니다.

프로시저

- MQSC 명령 **SET CHLAUTH** 또는 PCF 명령 **Set Channel Authentication Record**를 사용하여 채널 인증 레코드를 설정하십시오. 예를 들어, 다음 MQSC 명령을 실행할 수 있습니다.

```
SET CHLAUTH(' generic-channel-name ') TYPE (QMGRMAP) QMNAME(generic-partner-qmgr-name ) USERSRC(MAP) MCAUSER(user)
```

*generic-channel-name*은 액세스를 제어하려는 채널의 이름이거나 채널 이름과 일치하는 와일드카드로서 별표(*) 기호를 포함하는 패턴입니다.

*generic-partner-qmgr-name*은 큐 관리자의 이름이거나, 큐 관리자 이름과 일치하는 와일드카드로서 별표(*) 기호를 포함하는 패턴입니다.

*user*는 지정된 큐 관리자에서 모든 연결에 사용할 사용자 ID입니다.

- 특정 IP 주소로 이 명령을 제한하려면 다음과 같이 **ADDRESS** 매개변수를 포함시키십시오.

```
SET CHLAUTH(' generic-channel-name ') TYPE (QMGRMAP) QMNAME(generic-partner-qmgr-name ) USERSRC(MAP) MCAUSER(user) ADDRESS( generic-ip-address)
```

*generic-channel-name*은 액세스를 제어하려는 채널의 이름이거나 채널 이름과 일치하는 와일드카드로서 별표(*) 기호를 포함하는 패턴입니다.

*generic-ip-address*는 단일 주소이거나, 와일드카드로서 별표(*)를 또는 주소와 일치하는 범위를 나타내는 하이픈(-)을 포함하는 패턴입니다. 일반 IP 주소에 대한 자세한 정보는 [일반 IP 주소를 참조하십시오](#).

관련 참조

[SET CHLAUTH](#)

MCAUSER 사용자 ID에 클라이언트 사용자 ID 매핑

클라이언트에서 수신한 사용자 ID에 따라 채널 인증 레코드를 사용하여 서버 연결 채널의 *MCAUSER* 속성을 변경할 수 있습니다.

시작하기 전에

다음과 같이 채널 인증 레코드를 사용할 수 있는지 확인하십시오.

```
ALTER QMGR CHLAUTH(ENABLED)
```

이 태스크 정보

이 기술은 서버 연결 채널에만 적용됩니다. 다른 채널 유형에는 영향을 주지 않습니다.

프로시저

MQSC 명령 **SET CHLAUTH** 또는 PCF 명령 **Set Channel Authentication Record**를 사용하여 채널 인증 레코드를 설정하십시오. 예를 들어, 다음 MQSC 명령을 실행할 수 있습니다.

```
SET CHLAUTH(' generic-channel-name ') TYPE (USERMAP) CLNTUSER(client-user-name) USERSRC(MAP)
MCAUSER(
user)
```

*generic-channel-name*은 액세스를 제어하려는 채널의 이름이거나 채널 이름과 일치하는 와일드카드로서 별표(*) 기호를 포함하는 패턴입니다.

*client-user-name*은 클라이언트 애플리케이션과 연관된 사용자 ID입니다. 값은 클라이언트 애플리케이션에서 확인하거나, 조기 채택을 사용하는 연결 인증에서 변경하거나, 채널 엑시트를 통해 설정할 수 있습니다.

*user*는 클라이언트 사용자 이름 대신 사용될 사용자 ID입니다.

관련 참조

[SET CHLAUTH](#)

[Channels 스탠자의 속성\(ChlauthEarlyAdopt\)](#)

MCAUSER 사용자 ID에 SSL 또는 TLS 식별 이름 매핑

수신한 식별 이름(DN)에 따라 채널 인증 레코드를 사용하여 채널의 *MCAUSER* 속성을 설정할 수 있습니다.

시작하기 전에

다음과 같이 채널 인증 레코드를 사용할 수 있는지 확인하십시오.

```
ALTER QMGR CHLAUTH(ENABLED)
```

프로시저

MQSC 명령 **SET CHLAUTH** 또는 PCF 명령 **Set Channel Authentication Record**를 사용하여 채널 인증 레코드를 설정하십시오. 예를 들어, 다음 MQSC 명령을 실행할 수 있습니다.

```
SET CHLAUTH('generic-channel-name') TYPE (SSLPEERMAP)
SSLPEER(generic-ssl-peer-name) SSLCERTI(generic-issuer-name)
USERSRC(MAP) MCAUSER(user)
```

*generic-channel-name*은 액세스를 제어하려는 채널의 이름이거나 채널 이름과 일치하는 와일드카드로서 별표(*) 기호를 포함하는 패턴입니다.

*generic-ssl-peer-name*은 SSLPEER 값의 표준 IBM MQ 규칙을 따르는 문자열입니다. SSLPEER 값의 IBM MQ 규칙을 참조하십시오.

*user*는 지정된 DN을 사용하는 모든 연결에 사용할 사용자 ID입니다.

*generic-issuer-name*은 일치시킬 인증서의 발행인 DN을 가리킵니다. 이 매개변수는 선택적이지만 여러 인증 기관이 사용 중인 경우 잘못된 인증서와 가짜로 일치하는 것을 피하기 위해서 이를 사용해야 합니다.

관련 참조

SET CHLAUTH

리모트 큐 관리자로부터의 액세스 차단

채널 인증 레코드를 사용하여 리모트 큐 관리자가 채널을 시작하지 못하도록 할 수 있습니다.

시작하기 전에

다음과 같이 채널 인증 레코드를 사용할 수 있는지 확인하십시오.

```
ALTER QMGR CHLAUTH(ENABLED)
```

이 태스크 정보

이 기술은 서버 연결 채널에는 적용되지 않습니다. 다음 명령에서 서버-연결 채널의 이름을 지정하는 경우 이는 아무런 효과가 없습니다.

프로시저

MQSC 명령 **SET CHLAUTH** 또는 PCF 명령 **Set Channel Authentication Record**를 사용하여 채널 인증 레코드를 설정하십시오. 예를 들어, 다음 MQSC 명령을 실행할 수 있습니다.

```
SET CHLAUTH(' generic-channel-name ') TYPE(QMGRMAP) QMNAME(' generic-partner-qmgr-name ')  
USERSRC (NOACCESS)
```

*generic-channel-name*은 액세스를 제어하려는 채널의 이름이거나 채널 이름과 일치하는 와일드카드로서 별표(*) 기호를 포함하는 패턴입니다.

*generic-partner-qmgr-name*은 큐 관리자의 이름이거나, 큐 관리자 이름과 일치하는 와일드카드로서 별표(*) 기호를 포함하는 패턴입니다.

관련 참조

SET CHLAUTH

클라이언트 사용자 ID에 대한 액세스 차단

채널 인증 레코드를 사용하여 클라이언트 사용자 ID가 채널에 연결하지 못하도록 설정할 수 있습니다.

시작하기 전에

다음과 같이 채널 인증 레코드를 사용할 수 있는지 확인하십시오.

```
ALTER QMGR CHLAUTH(ENABLED)
```

이 태스크 정보

이 기술은 서버 연결 채널에만 적용됩니다. 다른 채널 유형에는 영향을 주지 않습니다.

프로시저

MQSC 명령 **SET CHLAUTH** 또는 PCF 명령 **Set Channel Authentication Record**를 사용하여 채널 인증 레코드를 설정하십시오. 예를 들어, 다음 MQSC 명령을 실행할 수 있습니다.

```
SET CHLAUTH(' generic-channel-name ') TYPE(USERMAP) CLNTUSER(' client-user-name ')
USERSRC(NOACCESS)
```

*generic-channel-name*은 액세스를 제어하려는 채널의 이름이거나 채널 이름과 일치하는 와일드카드로서 별표(*) 기호를 포함하는 패턴입니다.

*client-user-name*은 클라이언트 애플리케이션과 연관된 사용자 ID입니다. 값은 클라이언트 애플리케이션에서 확인하거나, 초기 채택을 사용하는 연결 인증에서 변경하거나, 채널 엑시트를 통해 설정할 수 있습니다.

관련 참조

[SET CHLAUTH](#)

SSL 또는 TLS 식별 이름의 액세스 차단

TLS 식별 이름(DN)이 채널을 시작하는 것을 막기 위해 채널 인증 레코드를 사용할 수 있습니다.

시작하기 전에

다음과 같이 채널 인증 레코드를 사용할 수 있는지 확인하십시오.

```
ALTER QMGR CHLAUTH(ENABLED)
```

프로시저

MQSC 명령 **SET CHLAUTH** 또는 PCF 명령 **Set Channel Authentication Record**를 사용하여 채널 인증 레코드를 설정하십시오. 예를 들어, 다음 MQSC 명령을 실행할 수 있습니다.

```
SET CHLAUTH(' generic-channel-name ') TYPE(SSLPEERMAP)
SSLPEER(' generic-ssl-peer-name ') SSLCERTI(' generic-issuer-name ')
USERSRC(NOACCESS)
```

*generic-channel-name*은 액세스를 제어하려는 채널의 이름이거나 채널 이름과 일치하는 와일드카드로서 별표(*) 기호를 포함하는 패턴입니다.

*generic-ssl-peer-name*은 SSLPEER 값의 표준 IBM MQ 규칙을 따르는 문자열입니다. [SSLPEER 값의 IBM MQ 규칙](#)을 참조하십시오.

*generic-issuer-name*은 일치시킬 인증서의 발행인 DN을 가리킵니다. 이 매개변수는 선택적이지만 여러 인증 기관이 사용 중인 경우 잘못된 인증서와 가짜로 일치하는 것을 피하기 위해서 이를 사용해야 합니다.

관련 참조

[SET CHLAUTH](#)

MCAUSER 사용자 ID에 IP 주소 매핑

연결을 수신한 IP 주소에 따라 채널 인증 레코드를 사용하여 채널의 MCAUSER 속성을 설정할 수 있습니다.

시작하기 전에

다음과 같이 채널 인증 레코드를 사용할 수 있는지 확인하십시오.

```
ALTER QMGR CHLAUTH(ENABLED)
```

프로시저

MQSC 명령 **SET CHLAUTH** 또는 PCF 명령 **Set Channel Authentication Record**를 사용하여 채널 인증 레코드를 설정하십시오. 예를 들어, 다음 MQSC 명령을 실행할 수 있습니다.

```
SET CHLAUTH(' generic-channel-name ') TYPE(ADDRESSMAP) ADDRESS(' generic-ip-address ')
USERSRC(MAP) MCAUSER(' user')
```

*generic-channel-name*은 액세스를 제어하려는 채널의 이름이거나 채널 이름과 일치하는 와일드카드로서 별표(*) 기호를 포함하는 패턴입니다.

*user*는 지정된 DN을 사용하는 모든 연결에 사용할 사용자 ID입니다.

*generic-ip-address*는 연결되는 주소이거나, 와일드카드로서 별표(*)를 또는 주소와 일치하는 범위를 나타내는 하이픈(-)을 포함하는 패턴입니다.

관련 참조

SET CHLAUTH

큐 관리자에 대한 원격 액세스 사용 안함으로 설정

클라이언트 애플리케이션이 큐 관리자에 연결하는 것을 원치 않으면 이에 대한 원격 액세스를 사용 안함으로 설정하십시오.

이 태스크 정보

다음 방법 중 하나를 사용하여 클라이언트 애플리케이션이 큐 관리자에 연결하는 것을 막으십시오.

프로시저

- MQSC 명령 **DELETE CHANNEL**을 사용하여 모든 서버 연결 채널을 삭제하십시오.
- MQSC 명령 **ALTER CHANNEL**을 사용하여 채널의 메시지 채널 에이전트 사용자 ID(MCAUSER)를 액세스 권한이 없는 사용자 ID로 설정하십시오.

연결 보안 설정


비즈니스 요구사항이 있는 각 사용자 또는 사용자 그룹에 큐 관리자에 연결하는 권한을 부여하십시오.

이 태스크 정보

연결 보안을 설정하려면 운영 체제에 적합한 명령을 사용하십시오.

다음 플랫폼에서는 **SET AUTHREC** 명령도 사용할 수 있습니다.


-  IBM i
-  Linux
-  UNIX
-  Windows

참고:  IBM MQ Appliance에서는 **SET AUTHREC** 명령만 사용할 수 있습니다.


프로시저

-  UNIX, Linux, and Windows의 경우:

```
setmqaut -m QMgrName -t qmgr -g GroupName +connect
```

-  IBM i의 경우:

```
GRTMQMAUT OBJ('QMgrName') OBJTYPE(*MQM) USER('GroupName') AUT(*CONNECT)
```

-  z/OS의 경우:

```
RDEFINE MQCONN QMgrName.BATCH UACC(NONE)  
PERMIT QMgrName.BATCH CLASS(MQCONN) ID(GroupName) ACCESS(READ)
```

```
RDEFINE MQCONN QMgrName.CICS UACC(NONE)
PERMIT QMgrName.CICS CLASS(MQCONN) ID(GroupName) ACCESS(READ)
RDEFINE MQCONN QMgrName.IMS UACC(NONE)
PERMIT QMgrName.IMS CLASS(MQCONN) ID(GroupName) ACCESS(READ)
RDEFINE MQCONN QMgrName.CHIN UACC(NONE)
PERMIT QMgrName.CHIN CLASS(MQCONN) ID(GroupName) ACCESS(READ)
```

이러한 명령은 배치, CICS, IMS 및 채널 시작기(CHIN)에 연결하기 위한 권한을 제공합니다. 특정 연결 유형을 사용하지 않으면 관련 명령을 생략하십시오.

변수 이름에는 다음과 같은 의미가 있습니다.

QMGrName

큐 관리자 이름. z/OS에서 이 값은 또한 큐 공유 그룹의 이름일 수도 있습니다.

ObjectProfile

권한을 변경한 오브젝트 또는 일반 프로파일의 이름입니다.

GroupName

액세스가 부여될 그룹의 이름입니다.

관련 개념

178 페이지의 『채널 시작기에 대한 연결 보안 프로파일』

채널 시작기에서의 연결 검사를 위한 프로파일은 큐 관리자 또는 큐 공유 그룹 이름과 그 뒤에 오는 CHIN으로 구성됩니다. 채널 시작기로 시작된 태스크 주소 공간에서 사용되는 사용자 ID에 연결 프로파일에 대한 READ 액세스를 부여하십시오.

큐에 대한 사용자 액세스 제어

큐에 대한 애플리케이션 액세스를 제어하고 싶습니다. 취할 조치를 판별하려면 이 토픽을 사용하십시오.

첫 번째 열의 각 실패 명령문에 대해 두 번째 열에 표시된 조치를 취하십시오.

설명	Action
애플리케이션은 큐로부터 메시지를 받습니다.	351 페이지의 『큐로부터 메시지를 가져오는 권한 부여』 참조
애플리케이션이 컨텍스트를 설정합니다.	352 페이지의 『컨텍스트를 설정하기 위한 권한 부여』 참조
애플리케이션이 컨텍스트를 전달합니다.	353 페이지의 『컨텍스트를 전달하기 위한 권한 부여』 참조
애플리케이션이 메시지를 클러스터된 큐에 넣습니다.	412 페이지의 『리모트 클러스터 큐에 메시지를 넣는 권한 부여』 참조
애플리케이션이 메시지를 로컬 큐에 넣습니다.	354 페이지의 『메시지를 로컬 큐에 넣기 위한 권한 부여』 참조
애플리케이션이 메시지를 모델 큐에 넣습니다.	355 페이지의 『메시지를 모델 큐에 넣기 위한 권한 부여』 참조
애플리케이션이 메시지를 리모트 큐에 넣습니다.	356 페이지의 『메시지를 리모트 클러스터 큐에 넣기 위한 권한 부여』 참조



큐로부터 메시지를 가져오는 권한 부여

비즈니스 요구사항이 있는 각 사용자 그룹에 큐 또는 큐 세트로부터 메시지를 가져오는 권한을 부여하십시오.

이 태스크 정보

일부 큐로부터 메시지를 가져오는 권한을 부여하려면 운영 체제에 적합한 명령을 사용하십시오.

다음 플랫폼에서는 [SET AUTHREC](#) 명령도 사용할 수 있습니다.

-  IBM i
-  Linux

- ▶ **UNIX** UNIX
- ▶ **IBM i** Windows

참고: **MQ Appliance** IBM MQ Appliance에서는 **SET AUTHREC** 명령만 사용할 수 있습니다.

프로시저

- UNIX, Linux, and Windows 시스템의 경우 다음 명령을 실행하십시오.

```
setmqaut -m QMgrName -n ObjectProfile -t queue -g GroupName +get
```

- IBM i의 경우 다음 명령을 실행하십시오.

```
GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*Q) USER(GroupName) AUT(*GET) MQMNAME(' QMgrName ')
```

- z/OS의 경우 다음 명령을 실행하십시오.

```
RDEFINE MQQUEUE QMgrName.ObjectProfile UACC(NONE)
PERMIT QMgrName.ObjectProfile CLASS(MQADMIN) ID(GroupName) ACCESS(UPDATE)
```

변수 이름에는 다음과 같은 의미가 있습니다.

QMgrName

큐 관리자 이름. z/OS에서 이 값은 또한 큐 공유 그룹의 이름일 수도 있습니다.

ObjectProfile

권한을 변경한 오브젝트 또는 일반 프로파일의 이름입니다.

GroupName

액세스가 부여될 그룹의 이름입니다.

컨텍스트를 설정하기 위한 권한 부여

비즈니스 요구사항이 있는 각 사용자 그룹에 넣고 있는 메시지에 컨텍스트를 설정하기 위한 권한을 부여하십시오.

이 태스크 정보

일부 큐에 컨텍스트를 설정하기 위한 권한을 부여하려면 운영 체제에 적합한 명령을 사용하십시오.

다음 플랫폼에서는 **SET AUTHREC** 명령도 사용할 수 있습니다.

- ▶ **IBM i** IBM i
- ▶ **Linux** Linux
- ▶ **UNIX** UNIX
- ▶ **IBM i** Windows

참고: **MQ Appliance** IBM MQ Appliance에서는 **SET AUTHREC** 명령만 사용할 수 있습니다.

프로시저

- UNIX, Linux, and Windows 시스템의 경우 다음 명령 중 하나를 실행하십시오.

- ID 컨텍스트만을 설정하려면:

```
setmqaut -m QMgrName -n ObjectProfile -t queue -g GroupName +setid
```

- 모든 컨텍스트를 설정하려면:

```
setmqaut -m QMgrName -n ObjectProfile -t queue -g GroupName +setall
```

참고: `setid` 또는 `setall` 권한을 사용하려면 적절한 큐 오브젝트와 큐 관리자 오브젝트 모두에 권한을 부여해야 합니다.

- IBM i의 경우 다음 명령 중 하나를 실행하십시오.

- ID 컨텍스트만을 설정하려면:

```
GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*Q) USER(GroupName) AUT(*SETID) MQMNAME(' QMgrName ')
```

- 모든 컨텍스트를 설정하려면:

```
GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*Q) USER(GroupName) AUT(*SETALL) MQMNAME(' QMgrName ')
```

- z/OS의 경우 다음 명령 세트 중 하나를 실행하려면:

- ID 컨텍스트만을 설정하려면:

```
RDEFINE MQQUEUE QMgrName.ObjectProfile UACC(NONE)  
PERMIT QMgrName.ObjectProfile CLASS(MQQUEUE) ID(GroupName) ACCESS(UPDATE)
```

- 모든 컨텍스트를 설정하려면:

```
RDEFINE MQQUEUE QMgrName.ObjectProfile UACC(NONE)  
PERMIT QMgrName.ObjectProfile CLASS(MQQUEUE) ID(GroupName) ACCESS(CONTROL)
```

변수 이름에는 다음과 같은 의미가 있습니다.

QMgrName

큐 관리자 이름. z/OS에서 이 값은 또한 큐 공유 그룹의 이름일 수도 있습니다.

ObjectProfile

권한을 변경한 오브젝트 또는 일반 프로파일의 이름입니다.

GroupName

액세스가 부여될 그룹의 이름입니다.


컨텍스트를 전달하기 위한 권한 부여


컨텍스트를 검색된 메시지에서 비즈니스 요구사항이 있는 각 사용자 그룹에 넣는 중인 메시지로 전달하기 위한 권한을 부여하십시오.

이 태스크 정보

일부 큐에 컨텍스트를 전달하기 위한 권한을 부여하려면 운영 체제에 적합한 명령을 사용하십시오.

다음 플랫폼에서는 `SET AUTHREC` 명령도 사용할 수 있습니다.

-  IBM i
-  Linux
-  UNIX
-  Windows

참고:  IBM MQ Appliance에서는 `SET AUTHREC` 명령만 사용할 수 있습니다.

프로시저

▶ ULW

UNIX, Linux, and Windows 시스템의 경우 다음 명령 중 하나를 실행하십시오.

- ID 컨텍스트만을 전달하려면:

```
setmqaut -m QMgrName -n ObjectProfile -t queue -g GroupName +passid
```

- 모든 컨텍스트를 전달하려면:

```
setmqaut -m QMgrName -n ObjectProfile -t queue -g GroupName +passall
```

▶ IBM i

IBM i의 경우 다음 명령 중 하나를 실행하십시오.

- ID 컨텍스트만을 전달하려면:

```
GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*Q) USER(GroupName) AUT(*PASSID) MQMNAME(' QMgrName ')
```

- 모든 컨텍스트를 전달하려면:

```
GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*Q) USER(GroupName) AUT(*PASSALL) MQMNAME(' QMgrName ')
```

▶ z/OS

z/OS의 경우 ID 컨텍스트 또는 모든 컨텍스트를 전달하려면 다음 명령을 실행하십시오.

```
RDEFINE MQQUEUE QMgrName.ObjectProfile UACC(NONE)  
PERMIT QMgrName.ObjectProfile CLASS(MQQUEUE) ID(GroupName) ACCESS(UPDATE)
```

변수 이름에는 다음과 같은 의미가 있습니다.

QMgrName

큐 관리자 이름. z/OS에서 이 값은 또한 큐 공유 그룹의 이름일 수도 있습니다.

ObjectProfile

권한을 변경한 오브젝트 또는 일반 프로파일의 이름입니다.

GroupName

액세스가 부여될 그룹의 이름입니다.

메시지를 로컬 큐에 넣기 위한 권한 부여

비즈니스 요구사항이 있는 각 사용자 그룹에 로컬 큐 또는 큐 세트에 메시지를 넣기 위한 권한을 부여하십시오.

이 태스크 정보

일부 로컬 큐에 메시지를 넣기 위한 권한을 부여하려면 운영 체제에 적합한 명령을 사용하십시오.

다음 플랫폼에서는 [SET AUTHREC](#) 명령도 사용할 수 있습니다.

- ▶ IBM i IBM i
- ▶ Linux Linux
- ▶ UNIX UNIX
- ▶ IBM i Windows

참고: [MQ Appliance](#) IBM MQ Appliance에서는 **SET AUTHREC** 명령만 사용할 수 있습니다.

프로시저

- UNIX, Linux, and Windows 시스템의 경우 다음 명령을 실행하십시오.

```
setmqaut -m QMgrName -n ObjectProfile -t queue -g GroupName +put
```

- IBM i의 경우 다음 명령을 실행하십시오.

```
GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*Q) USER(GroupName) AUT(*PUT) MQMNAME(' QMgrName ')
```

- z/OS의 경우 다음 명령을 실행하십시오.

```
RDEFINE MQQUEUE QMgrName.ObjectProfile UACC(NONE)  
PERMIT QMgrName.ObjectProfile CLASS(MQQUEUE) ID(GroupName) ACCESS(UPDATE)
```

변수 이름에는 다음과 같은 의미가 있습니다.

QMgrName

큐 관리자 이름. z/OS에서 이 값은 또한 큐 공유 그룹의 이름일 수도 있습니다.

ObjectProfile

권한을 변경한 오브젝트 또는 일반 프로파일의 이름입니다.

GroupName

액세스가 부여될 그룹의 이름입니다.

메시지를 모델 큐에 넣기 위한 권한 부여


비즈니스 요구사항이 있는 각 사용자 그룹에 모델 큐 또는 모델 큐 세트에 메시지를 넣기 위한 권한을 부여하십시오.

이 태스크 정보

모델 큐는 동적 큐를 작성하는 데 사용됩니다. 그러므로 모델 및 동적 큐 둘 모두에 권한을 부여해야 합니다. 이러한 권한을 부여하려면 운영 체제에 적합한 명령을 사용하십시오.

다음 플랫폼에서는 [SET AUTHREC](#) 명령도 사용할 수 있습니다.

-  IBM i
-  Linux
-  UNIX
-  Windows

참고:  IBM MQ Appliance에서는 **SET AUTHREC** 명령만 사용할 수 있습니다.

프로시저

- UNIX, Linux, and Windows 시스템의 경우 다음 명령을 실행하십시오.

```
setmqaut -m QMgrName -n ModelQueueName -t queue -g GroupName +put  
setmqaut -m QMgrName -n ObjectProfile -t queue -g GroupName +put
```

- IBM i의 경우 다음 명령을 실행하십시오.

```
GRTMQMAUT OBJ(' ModelQueueName ') OBJTYPE(*Q) USER(GroupName) AUT(*PUT) MQMNAME(' QMgrName ')  
GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*Q) USER(GroupName) AUT(*PUT) MQMNAME(' QMgrName ')
```

- z/OS의 경우 다음 명령을 실행하십시오.

```
RDEFINE MQQUEUE QMgrName.ModelQueueName UACC(NONE)
```

```
PERMIT QMgrName.ModelQueueName CLASS(MQQUEUE) ID(GroupName) ACCESS(UPDATE)
RDEFINE MQQUEUE QMgrName.ObjectProfile UACC(NONE)
PERMIT QMgrName.ObjectProfile CLASS(MQQUEUE) ID(GroupName) ACCESS(UPDATE)
```

변수 이름에는 다음과 같은 의미가 있습니다.

QMgrName

큐 관리자 이름. z/OS에서 이 값은 또한 큐 공유 그룹의 이름일 수도 있습니다.

ModelQueueName

동적 큐가 기반으로 하는 모델의 이름입니다.

ObjectProfile

권한 부여를 변경할 동적 큐 또는 일반 프로파일의 이름입니다.

GroupName

액세스가 부여될 그룹의 이름입니다.

메시지를 리모트 클러스터 큐에 넣기 위한 권한 부여

비즈니스 요구사항이 있는 각 사용자 그룹에 리모트 클러스터 큐 또는 큐 세트에 메시지를 넣기 위한 권한을 부여하십시오.

이 태스크 정보

리모트 클러스터 큐에 메시지를 넣기 위해 리모트 큐의 로컬 정의에 넣거나 완전한 리모트 큐에 넣을 수 있습니다. 리모트 큐의 로컬 정의를 사용 중인 경우에는 로컬 오브젝트에 넣기 위한 권한이 필요합니다. 354 페이지의 『메시지를 로컬 큐에 넣기 위한 권한 부여』의 내용을 참조하십시오. 완전한 리모트 큐를 사용 중인 경우에는 리모트 큐에 넣기 위한 권한이 필요합니다. 운영 체제에 적합한 명령을 사용하여 이 권한을 부여하십시오.

기본 동작은 SYSTEM.CLUSTER.TRANSMIT.QUEUE에 대한 액세스 제어를 수행하는 것입니다. 이 작동은 여러 전송 큐를 사용 중인 경우에도 적용된다는 점을 유의하십시오.

이 주제에 설명된 특정 동작은 보안 스탠자 주제에 설명된 대로 `qm.ini` 파일에서

ClusterQueueAccessControl 속성을 `RQMName`으로 구성하고 큐 관리자를 재시작한 경우에만 적용됩니다.

다음 플랫폼에서는 `SET AUTHREC` 명령도 사용할 수 있습니다.

- ▶ IBM i IBM i
- ▶ Linux Linux
- ▶ UNIX UNIX
- ▶ IBM i Windows

참고: ▶ MQ Appliance IBM MQ Appliance에서는 **SET AUTHREC** 명령만 사용할 수 있습니다.

프로시저

- UNIX, Linux, and Windows 시스템의 경우 다음 명령을 실행하십시오.

```
setmqaut -m QMgrName -t rqmname -n
ObjectProfile -g GroupName +put
```

리모트 클러스터 큐에 대해서만 `rqmname` 오브젝트를 사용할 수 있음을 유의하십시오.

- IBM i의 경우 다음 명령을 실행하십시오.

```
GRTMQMAUT OBJTYPE(*RMTMQMNAME) OBJ('
ObjectProfile') USER(GroupName) AUT(*PUT) MQMNAME('
QMgrName')
```

리모트 클러스터 큐에 대해서만 `RMTMQMNAME` 오브젝트를 사용할 수 있음을 유의하십시오.

- z/OS의 경우 다음 명령을 실행하십시오.

```
RDEFINE MQQUEUE QMgrName.ObjectProfile UACC(NONE)
PERMIT QMgrName.QUEUE.ObjectProfile CLASS(MQQUEUE)
ID(GroupName) ACCESS(UPDATE)
```

리모트 클러스터 큐에 대해서만 리모트 큐 관리자(또는 큐 공유 그룹)의 이름을 사용할 수 있음을 유의하십시오.

변수 이름에는 다음과 같은 의미가 있습니다.

QMgrName

큐 관리자 이름. z/OS에서 이 값은 또한 큐 공유 그룹의 이름일 수도 있습니다.

ObjectProfile

권한 부여를 변경하려는 리모트 큐 관리자 또는 일반 프로파일의 이름입니다.

GroupName

액세스가 부여될 그룹의 이름입니다.

토픽에 대한 사용자 액세스 제어

토픽에 대한 애플리케이션의 액세스를 제어해야 합니다. 취할 조치를 판별하려면 이 토픽을 사용하십시오.

첫 번째 열의 각 신뢰 명령문에 대해 두 번째 열에 표시된 조치를 취하십시오.

표 71. 토픽에 대한 사용자 액세스 제어	
설명	Action
애플리케이션이 토픽에 메시지를 발행합니다.	357 페이지의 『토픽에 메시지를 발행하기 위한 권한 부여』 참조
애플리케이션이 토픽을 구독합니다.	358 페이지의 『토픽을 구독하기 위한 권한 부여』 참조




토픽에 메시지를 발행하기 위한 권한 부여


비즈니스 요구사항이 있는 각 사용자 그룹에 메시지를 토픽 또는 토픽 세트에 발행하기 위한 권한을 부여하십시오.

이 태스크 정보

메시지를 일부 토픽에 발행하기 위한 권한을 부여하려면 운영 체제에 적합한 명령을 사용하십시오.

다음 플랫폼에서는 [SET AUTHREC](#) 명령도 사용할 수 있습니다.

-  IBM i
-  Linux
-  UNIX
-  Windows

참고:  IBM MQ Appliance에서는 **SET AUTHREC** 명령만 사용할 수 있습니다.

프로시저

- UNIX, Linux, and Windows 시스템의 경우 다음 명령을 실행하십시오.

```
setmqaut -m QMgrName -n ObjectProfile -t topic -g GroupName +pub
```

- IBM i의 경우 다음 명령을 실행하십시오.


```
GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*TOPIC) USER(GroupName) AUT(*PUB) MQMNAME(' QMgrName ')
```

- z/OS의 경우 다음 명령을 실행하십시오.

```
RDEFINE MQTOPIC QMgrName.ObjectProfile UACC(NONE)  
PERMIT QMgrName.ObjectProfile CLASS(MQTOPIC) ID(GroupName) ACCESS(UPDATE)
```

변수 이름에는 다음과 같은 의미가 있습니다.

QMgrName

큐 관리자 이름. z/OS에서 이 값은 또한 큐 공유 그룹의 이름일 수도 있습니다.

ObjectProfile

권한을 변경한 오브젝트 또는 일반 프로파일의 이름입니다.

GroupName

액세스가 부여될 그룹의 이름입니다.

토픽을 구독하기 위한 권한 부여


비즈니스 요구사항이 있는 각 사용자 그룹에 토픽 또는 토픽 세트를 구독하기 위한 권한을 부여하십시오.

이 태스크 정보

일부 토픽을 구독하기 위한 권한을 부여하려면 운영 체제에 적합한 명령을 사용하십시오.

다음 플랫폼에서는 SET AUTHREC 명령도 사용할 수 있습니다.

-  IBM i
-  Linux
-  UNIX
-  Windows

참고:  IBM MQ Appliance에서는 **SET AUTHREC** 명령만 사용할 수 있습니다.

프로시저

- UNIX, Linux, and Windows 시스템의 경우 다음 명령을 실행하십시오.

```
setmqaut -m QMgrName -n ObjectProfile -t topic -g GroupName +sub
```

- IBM i의 경우 다음 명령을 실행하십시오.

```
GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*TOPIC) USER(GroupName) AUT(*SUB) MQMNAME(' QMgrName ')
```

- z/OS의 경우 다음 명령을 실행하십시오.

```
RDEFINE MQTOPIC QMgrName.SUBSCRIBE.ObjectProfile UACC(NONE)  
PERMIT QMgrName.SUBSCRIBE.ObjectProfile CLASS(MQTOPIC) ID(GroupName) ACCESS(UPDATE)
```

변수 이름에는 다음과 같은 의미가 있습니다.

QMgrName

큐 관리자 이름. z/OS에서 이 값은 또한 큐 공유 그룹의 이름일 수도 있습니다.

ObjectProfile

권한을 변경한 오브젝트 또는 일반 프로파일의 이름입니다.

GroupName

액세스가 부여될 그룹의 이름입니다.

큐 관리자에서 조사하기 위한 권한 부여

비즈니스 요구사항이 있는 각 사용자 그룹에 큐 관리자에서 조사하기 위한 권한을 부여하십시오.

이 태스크 정보

큐 관리자에서 조사하기 위한 권한을 부여하려면 운영 체제에 적합한 명령을 사용하십시오.

다음 플랫폼에서는 [SET AUTHREC](#) 명령도 사용할 수 있습니다.

- ▶ IBM i IBM i
- ▶ Linux Linux
- ▶ UNIX UNIX
- ▶ IBM i Windows

참고: [MQ Appliance](#) IBM MQ Appliance에서는 **SET AUTHREC** 명령만 사용할 수 있습니다.

프로시저

- UNIX, Linux, and Windows 시스템의 경우 다음 명령을 실행하십시오.

```
setmqaut -m QMgrName -n ObjectProfile -t qmgr -g GroupName +inq
```

- IBM i의 경우 다음 명령을 실행하십시오.

```
GRTRMQAUT OBJ(' ObjectProfile ') OBJTYPE(*MQM) USER(GroupName) AUT(*INQ) MQMNAME(' QMgrName')
```

- z/OS의 경우 다음 명령을 실행하십시오.

```
RDEFINE MQCMLS QMgrName.ObjectProfile UACC(NONE)  
PERMIT QMgrName.ObjectProfile CLASS(MQCMLS) ID(GroupName) ACCESS(READ)
```

이러한 명령은 지정된 큐 관리자에 액세스를 부여합니다. 사용자가 MQINQ 명령을 사용하도록 허용하려면 다음 명령을 실행하십시오.

```
RDEFINE MQCMLS QMgrName.MQINQ.QMGR UACC(NONE)  
PERMIT QMgrName.MQINQ.QMGR CLASS(MQCMLS) ID(GroupName) ACCESS(READ)
```

변수 이름에는 다음과 같은 의미가 있습니다.

QMgrName

큐 관리자 이름. z/OS에서 이 값은 또한 큐 공유 그룹의 이름일 수도 있습니다.

ObjectProfile

권한을 변경한 오브젝트 또는 일반 프로파일의 이름입니다.

GroupName

액세스가 부여될 그룹의 이름입니다.

프로세스에 액세스하기 위한 권한 부여

비즈니스 요구사항이 있는 각 사용자 그룹에 프로세스 또는 프로세스 세트에 액세스하기 위한 권한을 부여하십시오.

이 태스크 정보

일부 프로세스에 액세스하기 위한 권한을 부여하려면 운영 체제에 적합한 명령을 사용하십시오.

다음 플랫폼에서는 `SET AUTHREC` 명령도 사용할 수 있습니다.

- ▶ **IBM i** IBM i
- ▶ **Linux** Linux
- ▶ **UNIX** UNIX
- ▶ **IBM i** Windows

참고: **MQ Appliance** IBM MQ Appliance에서는 `SET AUTHREC` 명령만 사용할 수 있습니다.

프로시저

- UNIX, Linux, and Windows 시스템의 경우 다음 명령을 실행하십시오.

```
setmqaut -m QMgrName -n ObjectProfile -t process -g GroupName +all
```

- IBM i의 경우 다음 명령을 실행하십시오.

```
GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*PRC) USER(GroupName) AUT(*ALL) MQMNAME(' QMgrName')
```

- z/OS의 경우 다음 명령을 실행하십시오.

```
RDEFINE MQPROC QMgrName.ObjectProfile UACC(NONE)  
PERMIT QMgrName.ObjectProfile CLASS(MQPROC) ID(GroupName) ACCESS(READ)
```

변수 이름에는 다음과 같은 의미가 있습니다.

QMgrName

큐 관리자 이름. z/OS에서 이 값은 또한 큐 공유 그룹의 이름일 수도 있습니다.

ObjectProfile

권한을 변경한 오브젝트 또는 일반 프로파일의 이름입니다.

GroupName

액세스가 부여될 그룹의 이름입니다.

이름 목록에 액세스하기 위한 권한 부여

비즈니스 요구사항이 있는 각 사용자 그룹에 이름 목록 또는 이름 목록 세트에 액세스하기 위한 권한을 부여하십시오.

이 태스크 정보

일부 이름 목록에 액세스하기 위한 권한을 부여하려면 운영 체제에 적합한 명령을 사용하십시오.

다음 플랫폼에서는 `SET AUTHREC` 명령도 사용할 수 있습니다.

- ▶ **IBM i** IBM i
- ▶ **Linux** Linux
- ▶ **UNIX** UNIX
- ▶ **IBM i** Windows

참고: **MQ Appliance** IBM MQ Appliance에서는 `SET AUTHREC` 명령만 사용할 수 있습니다.

프로시저

- UNIX, Linux, and Windows 시스템의 경우 다음 명령을 실행하십시오.

```
setmqaut -m QMgrName -n  
ObjectProfile -t namelist -g GroupName  
+all
```

- IBM i의 경우 다음 명령을 실행하십시오.

```
GRTMQMAUT OBJ('ObjectProfile  
) OBJTYPE(*NMLIST) USER(GroupName) AUT(*ALL) MQMNAME('QMgrName')
```

- z/OS의 경우 다음 명령을 실행하십시오.

```
RDEFINE MQNLIST  
QMgrName.ObjectProfile UACC(NONE)  
PERMIT QMgrName.ObjectProfile  
CLASS(MQNLIST) ID(GroupName) ACCESS(READ)
```

변수 이름에는 다음과 같은 의미가 있습니다.

QMgrName

큐 관리자 이름. z/OS에서 이 값은 또한 큐 공유 그룹의 이름일 수도 있습니다.

ObjectProfile

권한을 변경한 오브젝트 또는 일반 프로파일의 이름입니다.

GroupName

액세스가 부여될 그룹의 이름입니다.

ULW

UNIX, Linux, and Windows 에서 IBM MQ 를 관리하는 권한

IBM MQ 관리자는 모든 IBM MQ 명령을 사용하고 다른 사용자에게 권한을 부여할 수 있습니다. 관리자가 리모트 큐 관리자에게 명령을 발행할 때 관리자는 리모트 큐 관리자에 대해 필요한 권한이 있어야 합니다. 추가 고려사항은 Windows 시스템에 적용됩니다.

IBM MQ 관리자에게는 모든 IBM MQ 명령(다른 사용자에게 대한 IBM MQ 권한을 부여하기 위한 명령 포함)을 사용할 권한이 있습니다.

IBM MQ 관리자가 되려면 **mqm** 그룹이라는 특수 그룹의 구성원이어야 합니다.

Windows 또는 Windows 에서만 로컬 계정이 Windows 시스템에서 관리자 그룹의 구성원인 경우 IBM MQ 를 관리할 수 있습니다.



주의: 관리자 명령을 사용하여 **mqm** 그룹에 Azure AD 사용자를 추가할 수 있습니다. 예를 들어, `net localgroup mqm AzureAD\<your userID> /add` 명령을 사용하십시오. 그런 다음, IBM MQ 관리 명령을 실행하거나 IBM MQ Explorer를 사용하십시오.

mqm 그룹은 IBM MQ가 설치될 때 자동으로 작성됩니다. 추가 사용자가 관리를 수행할 수 있도록 이들을 그룹에 추가할 수 있습니다. 이 그룹의 모든 구성원은 모든 자원에 대한 액세스 권한을 가집니다. **mqm** 그룹에서 사용자를 제거하고 **REFRESH SECURITY** 명령을 실행하여 이 액세스 권한을 취소할 수 있습니다.

관리자는 IBM MQ를 관리하기 위한 제어 명령을 사용할 수 있습니다. 이러한 제어 명령 중 하나는 **setmqaut**이고, 이는 다른 사용자들이 IBM MQ 자원에 액세스하거나 제어할 수 있도록 권한을 부여하는 데 사용됩니다. 권한 레코드 관리를 위한 PCF 명령은 큐 관리자에 대해 **dsp** 및 **chg** 권한을 부여받은 비관리자가 사용할 수 있습니다. PCF 명령을 사용한 권한 관리에 대한 자세한 정보는 [PCF\(Programmable Command Format\)](#)를 참조하십시오.


관리자는 리모트 큐 관리자가 처리하는 MQSC 명령에 대한 필수 권한이 있어야 합니다. IBM MQ Explorer는 PCF 명령을 발행하여 관리 태스크를 수행합니다. 관리자는 IBM MQ Explorer를 사용하여 로컬 시스템에서 큐 관리자를 관리하는 데 추가 권한이 필요하지 않습니다. IBM MQ Explorer가 또 다른 시스템에서 큐 관리자를 관리하는 데 사용되면 관리자에게는 PCF 명령이 리모트 큐 관리자에 의해 처리되기 위해서 필요한 권한이 있어야 합니다.



주의: IBM MQ 8.0에서 IBM MQ 스크립트 (MQSC) 명령을 실행하는 제어 명령 **runmqsc**를 사용하는 관리자가 되지 않아도 됩니다.

MQSC 명령을 리모트 큐 관리자에게 송신하는 데 간접적인 모드로 **runmqsc**가 사용되면, 각 MQSC 명령은 이스케이프 PCF 명령 안에 캡슐화됩니다.

PCF 및 MQSC 명령이 처리될 때의 권한 확인에 대한 자세한 정보는 다음 주제를 참조하십시오.

- 큐 관리자, 큐, 프로세스, 이름 목록 및 인증 정보 오브젝트에 대해 작동하는 PCF 명령의 경우 [IBM MQ 오브젝트에 대해 작업하는 권한](#)을 참조하십시오. PCF 나가기 명령 내에서 캡슐화된 동등한 MQSC 명령에 대해서 이 절을 참조하십시오.
- 채널, 채널 이니시에이터, 리스너 및 클러스터에 대해 실행되는 PCF 명령은 [채널 보안](#)을 참조하십시오.
- 권한 레코드에 대해 작동하는 PCF 명령의 경우 [PCF 명령에 대한 권한 검사](#)를 참조하십시오.
-  [IBM MQ for z/OS에서 명령 서버가 처리하는 MQSC 명령의 경우 z/OS에서 명령 보안 및 명령 자원 보안](#)을 참조하십시오.

또한 Windows 시스템에서 SYSTEM 계정에는 IBM MQ 자원에 대한 전체 액세스 권한이 있습니다.

UNIX and Linux 플랫폼에서는 제품에서만 사용할 **mqm**의 특수 사용자 ID도 작성됩니다. 권한을 부여받지 못한 사용자에게 사용 가능해서는 안 됩니다. 모든 IBM MQ 오브젝트는 사용자 ID **mqm**이 소유하고 있습니다.

Windows 시스템에서 관리자 그룹의 구성원은 시스템 계정을 사용하여 큐 관리자를 관리할 수도 있습니다. 도메인 내에서 활성 상태인 모든 권한 있는 사용자 ID가 포함된 도메인 제어기에 도메인 **mqm** 그룹을 작성하고 이 그룹을 로컬 **mqm** 그룹에 추가할 수도 있습니다. **crtmqm**과 같은 일부 명령은 IBM MQ 오브젝트에서 권한을 조작하므로 이러한 오브젝트에 대해 작업하기 위한 권한이 필요합니다(다음 절에 설명된 대로). **mqm** 그룹의 구성원은 모든 오브젝트에 대해 작업할 수 있는 권한이 있지만, Windows 시스템에서 같은 이름의 로컬 사용자와 도메인 인증 사용자가 있는 경우 권한이 거부되는 경우가 있을 수 있습니다. 이 프로그램은 365 페이지의 『UNIX, Linux, and Windows에서 프린시플 및 그룹』에서 설명합니다.

사용자 계정 제어(UAC) 기능이 포함된 Windows 버전은 사용자가 관리자 그룹의 구성원일 경우에도 특정 운영 체제 기능에 대해 수행할 수 있는 조치를 제한합니다. 사용자 ID가 관리자 그룹에 있지만 **mqm** 그룹이 아닌 경우, 승격된 명령 프롬프트를 사용하여 **crtmqm**와 같은 IBM MQ 관리 명령을 실행해야 합니다. 그렇지 않으면 **AMQ7077**: 요청된 조작을 수행할 권한이 없습니다 라는 오류가 생성됩니다. 상승된 명령 프롬프트를 열려면 시작 메뉴 항목 또는 명령 프롬프트의 경우 아이콘을 마우스 오른쪽 단추로 클릭하고 **관리자로서 실행**을 선택하십시오.

다음 조치를 취하기 위해 **mqm** 그룹의 구성원일 필요는 없습니다.

- PCF 나가기 명령 내에 PCF 명령 또는 MQSC 명령을 발행하는 애플리케이션 프로그램에서 명령을 발행하십시오(채널 이니시에이터를 조작하지 않는 경우). (이러한 명령은 98 페이지의 『채널 시작기 정의 보호』에 설명되어 있습니다.)
- 애플리케이션 프로그램에서 MQI 호출을 발행하십시오(MQCONN 호출에 빠른 경로 바인딩을 사용하지 않는 경우).
- **crtmqcvx** 명령을 사용하여 데이터 유형 구조에 대한 데이터 변환을 수행하는 코드의 단편을 작성하십시오.
- **dspmq** 명령을 사용하여 큐 관리자를 표시하십시오.
- **dspmqtrc** 명령을 사용하여 IBM MQ 형식화된 추적 출력을 표시하십시오.



그룹과 사용자 ID 둘 모두에 12자 제한이 적용됩니다.

일반적으로, UNIX and Linux 플랫폼은 사용자 ID의 길이를 12자로 제한합니다. AIX 5.3에서는 이 한계를 높였지만 IBM MQ에서는 모든 UNIX and Linux 플랫폼에서 12자 제한을 유지합니다. 12자보다 많은 사용자 ID를 사용하면 IBM MQ는 이를 UNKNOWN 값으로 바꿉니다. 사용자 ID를 UNKNOWN 값으로 정의하지 마십시오.

UNIX, Linux, and Windows에서 **mqm** 그룹 관리

mqm 그룹의 사용자에게는 IBM MQ에 대한 전체 관리 권한이 부여됩니다. 이러한 이유로 애플리케이션과 일반 사용자를 **mqm** 그룹에 등록해서는 안 됩니다. **mqm** 그룹에는 IBM MQ 관리자의 계정만을 포함해야 합니다.

이러한 태스크가 다음에 설명되어 있습니다.

-  [Windows에서 그룹 작성 및 관리](#)
-  [AIX에서 그룹 작성 및 관리](#)

• **Solaris** Solaris에서 그룹 작성 및 관리

• **Linux** Linux에서 그룹 작성 및 관리

Windows 도메인 제어가 Windows 2000 또는 Windows 2003 이상에서 실행되는 경우 도메인 관리자는 IBM MQ가 사용할 특수 계정을 설정했을 수도 있습니다. 자세한 정보는 [Prepare IBM MQ Wizard](#)을 사용하여 IBM MQ 구성 및 IBM MQ에 대한 Windows 도메인 계정 작성 및 설정을 참조하십시오.

ULW UNIX, Linux, and Windows 에서 IBM MQ 오브젝트에 대한 작업 권한

모든 오브젝트는 IBM MQ에 의해 보호되고, 프린시פל에는 이에 액세스하기 위한 적합한 권한이 제공되어야 합니다. 서로 다른 프린시פל은 다른 오브젝트마다 다른 액세스 권한이 필요합니다.

큐 관리자, 큐, 프로세스 정의, 이름 목록, 채널, 클라이언트 연결 채널, 리스너, 서비스 및 인증 정보 오브젝트는 모두 MQI 호출 또는 PCF 명령을 사용하는 애플리케이션에서 액세스됩니다. 이러한 자원은 모두 IBM MQ에 의해 보호되고, 애플리케이션에는 이에 액세스하기 위한 권한이 제공되어야 합니다. 요청을 하는 엔티티는 사용자, MQI 호출을 실행하는 애플리케이션 프로그램 또는 PCF 명령을 실행하는 관리 프로그램일 수 있습니다. 요청자의 ID를 프린시פל이라고 합니다.

서로 다른 프린시פל 그룹에 동일한 오브젝트에 대한 서로 다른 유형의 액세스 권한을 부여할 수 있습니다. 예를 들어, 특정 큐의 경우 한 그룹이 넣기 및 가져오기 조작 둘 모두를 수행하도록 허용될 수도 있고 다른 그룹은 큐를 찾아보기만이 허용될 수도 있습니다(찾아보기 옵션이 있는 MQGET). 마찬가지로, 일부 그룹에 큐에 대한 가져오기(get) 및 넣기(put) 권한을 주는 동시에 큐 속성 변경 또는 큐 삭제를 할 수 없도록 할 수 있습니다.

일부 조작은 특히 민감하여 권한이 있는 사용자로 제한해야 합니다. 예를 들면, 다음과 같습니다.

- 특정 큐(예: 트랜스미션 큐)나 커맨드 큐 SYSTEM.ADMIN.COMMAND.QUEUE에 액세스
- 전체 MQI 컨텍스트 옵션을 사용하는 프로그램 실행
- 애플리케이션 큐 작성 및 삭제

오브젝트에 대한 전체 액세스 권한은 오브젝트를 작성한 사용자 ID에 및 mqm 그룹의 모든 구성원(및 Windows 시스템에서 로컬 관리자 그룹의 구성원)에게 자동으로 제공됩니다.

관련 개념

361 페이지의 『UNIX, Linux, and Windows 에서 IBM MQ 를 관리하는 권한』

IBM MQ 관리자는 모든 IBM MQ 명령을 사용하고 다른 사용자에 대한 권한을 부여할 수 있습니다. 관리자가 리모트 큐 관리자에게 명령을 발행할 때 관리자는 리모트 큐 관리자에 대해 필요한 권한이 있어야 합니다. 추가 고려사항은 Windows 시스템에 적용됩니다.

ULW UNIX, Linux, and Windows에서 보안 검사가 수행되는 시기

보안 검사는 일반적으로 큐 관리자에 연결할 때, 오브젝트를 열거나 닫을 때 및 메시지를 넣거나 가져올 때 수행됩니다.

일반 애플리케이션에 대한 보안 검사는 다음과 같습니다.

큐 관리자에 연결(MQCONN 또는 MQCONNX 호출)

이 때 애플리케이션이 특정 큐 관리자와 처음으로 연관됩니다. 큐 관리자는 운영 환경을 조사하여 애플리케이션과 연관된 사용자 ID를 검색합니다. IBM MQ는 그러면 사용자 ID가 큐 관리자에 연결되는지 확인하고 나중에 검사하기 위해 사용자 ID를 보존합니다.

사용자는 IBM MQ에 사인온할 필요가 없습니다. IBM MQ는 사용자가 기본 운영 체제에 사인온했고 이에 의해 인증되었음을 가정합니다.

오브젝트 열기(MQOPEN 또는 MQPUT1 호출)

IBM MQ 오브젝트는 오브젝트를 열고 이에 대해 명령을 실행하여 액세스합니다. 모든 자원 검사는 오브젝트에 실제로 액세스할 때가 아니라 오브젝트를 열 때 수행됩니다. 이는 **MQOPEN** 요청이 필요한 액세스 유형을 지정해야 함을 의미합니다. 예를 들어, 사용자가 오브젝트를 찾아보기만을 원하는지 또는 메시지를 큐에 넣기 등과 같은 업데이트를 수행하고 싶어하는지 여부입니다.

IBM MQ는 **MQOPEN** 요청에 이름이 지정된 자원을 검사합니다. 알리어스 큐 또는 리모트 큐 오브젝트의 경우, 권한은 알리어스 큐나 리모트 큐가 해석하는 큐가 아니라 오브젝트 자체에 대해 사용한 권한입니다. 이는 사

용자가 여기에 액세스할 권한이 필요하지 않음을 의미합니다. 큐 작성 권한을 권한이 있는 사용자로 제한하십시오. 그렇게 하지 않으면 사용자가 알리어스를 작성하는 것만으로 일반 액세스 제어를 무시할 수도 있습니다. 리모트 큐에서 큐와 큐 관리자 이름을 명시적으로 참조하는 경우, 리모트 큐 관리자와 연관된 트랜스미션 큐를 검사합니다.

동적 큐에 대한 권한은 구동된 모델 큐 권한을 기본으로 하므로 반드시 동일할 필요는 없습니다. 이에 대해서는 참고 115 페이지의 『1』에서 설명됩니다.

액세스 검사를 위해 큐 관리자가 사용하는 사용자 ID는 큐 관리자에 연결된 응용프로그램의 운영 환경에서 확보한 사용자 ID입니다. 적절히 권한이 부여된 애플리케이션은 대체 사용자 ID를 지정하는 **MQOPEN** 호출을 발행할 수 있습니다. 그런 다음 대체 사용자 ID에 대해 액세스 제어 검사를 수행합니다. 이러한 조치로 애플리케이션과 연관된 사용자 ID가 변경되지 않으며 액세스 제어 검사에 사용된 사용자 ID가 변경됩니다.

메시지 넣기 및 가져오기(MQPUT 또는 MQGET 호출)

액세스 제어 검사가 수행되지 않습니다.

오브젝트 닫기(MQCLOSE)

MQCLOSE가 동적 큐를 삭제하는 결과를 낳지 않는 한 액세스 제어 검사가 수행되지 않습니다. 이 경우 사용자 ID가 큐를 삭제할 권한이 있는지 검사합니다.

토픽 구독하기(MQSUB)

애플리케이션이 토픽을 구독할 때 이는 수행해야 할 조작의 유형을 지정합니다. 새 구독을 작성하거나, 기존 구독을 변경하거나, 이를 변경하지 않고 기존 구독을 재개하는 것입니다. 조작의 유형마다 큐 관리자는 애플리케이션에 연관된 사용자 ID에 해당 조작을 수행할 권한이 있는지 검사합니다.

애플리케이션이 토픽을 구독할 때 구독한 애플리케이션이 있는 토픽 트리 이상의 위치에서 발견된 토픽 오브젝트에 대해 권한 검사가 수행됩니다. 권한 검사에는 두 개 이상의 토픽 오브젝트에 대한 검사가 포함될 수 있습니다.

큐 관리자가 권한 검사를 위해 사용하는 사용자 ID는 애플리케이션이 큐 관리자에 연결할 때 운영 체제로부터 얻은 사용자 ID입니다.

큐 관리자는 관리 큐가 아니라 구독자 큐에서 권한 검사를 수행합니다.

ULW UNIX, Linux, and Windows 에서 IBM MQ 로 액세스 제어를 구현하는 방법

IBM MQ는 오브젝트 권한 관리자를 사용하여 기본 운영 체제가 제공하는 보안 서비스를 사용합니다. IBM MQ는 액세스 제어 목록을 작성하고 유지보수하기 위한 명령을 제공합니다.

권한 서비스 인터페이스라는 액세스 제어 인터페이스는 IBM MQ의 일부입니다. IBM MQ는 액세스 제어 관리자의 구현을 제공합니다(오브젝트 권한 관리자(OAM)로 알려진 권한 서비스 인터페이스 준수). 이는 사용자가 별도로 지정하지 않는 한 자동으로 설치되고 사용자가 작성하는 각 큐 관리자에서 사용 가능으로 설정됩니다(323 페이지의 『UNIX, Linux, and Windows 시스템에서 보안 액세스 검사 방지』에 설명된 대로). OAM은 권한 서비스 인터페이스를 준수하는 사용자 또는 벤더가 작성한 컴포넌트로 대체될 수 있습니다.

OAM은 운영 체제 사용자 및 그룹 ID를 사용하여 기본 운영 체제의 보안 기능을 사용합니다. 사용자는 연결 권한이 있는 경우에만 IBM MQ 오브젝트에 액세스할 수 있습니다. 314 페이지의 『UNIX, Linux, and Windows에서 OAM을 사용하여 오브젝트에 대한 액세스 제어』에서는 이 권한을 부여하고 취소하는 방법을 설명합니다.

OAM은 제어하는 각 자원에 대해 액세스 제어 목록(ACL)을 유지보수합니다. 권한 부여 데이터는 SYSTEM.AUTH.DATA.QUEUE라는 로컬 큐에 저장됩니다. 이 큐에 대한 액세스는 mqm 그룹의 사용자로 제한되며 Windows에서 관리자 그룹의 사용자 및 시스템 ID로 로그인한 사용자로 제한됩니다. 큐에 대한 사용자 액세스는 변경될 수 없습니다.

IBM MQ는 액세스 제어 목록을 작성하고 유지보수하기 위한 명령을 제공합니다. 이러한 명령에 대한 자세한 정보는 314 페이지의 『UNIX, Linux, and Windows에서 OAM을 사용하여 오브젝트에 대한 액세스 제어』의 내용을 참조하십시오.

IBM MQ는 OAM에 프린시플, 자원 이름 및 액세스 유형을 포함하는 요청을 전달합니다. OAM은 유지보수하는 ACL을 기본으로 액세스 권한을 부여하거나 거부합니다. IBM MQ는 OAM의 결정을 따릅니다. OAM이 결정을 내릴 수 없는 경우 IBM MQ는 액세스를 허용하지 않습니다.

오브젝트 권한 관리자는 자원에 대한 액세스를 요청하고 있는 프린시펄을 식별합니다. 프린시펄로서 사용되는 사용자 ID는 컨텍스트에 따라 다릅니다.

오브젝트 권한 관리자(OAM)는 특정 자원에 대한 액세스를 요청 중인 사용자를 식별할 수 있어야 합니다. IBM MQ는 이 ID를 가리키기 위해 프린시펄이라는 용어를 사용합니다. 프린시펄은 애플리케이션이 처음 큐 관리자에 연결할 때 설정됩니다. 이는 연결 애플리케이션과 연관된 사용자 ID로부터 큐 관리자에 의해 판별됩니다. (애플리케이션이 큐 관리자에 연결하지 않고 XA 호출을 실행하면 xa_open 호출을 실행한 애플리케이션과 연관된 사용자 ID가 큐 관리자에 의해 권한 검사에 사용됩니다.)

UNIX and Linux 시스템에서 권한 루틴은 실제(로그인한) 사용자 ID 또는 애플리케이션과 연관된 유효 사용자 ID를 검사합니다. 검사된 사용자 ID는 바인드 유형에 의존할 수 있습니다. 자세한 내용은 [설치 가능 서비스를 참조](#) 하십시오.

IBM MQ는 시스템으로부터 받은 사용자 ID를 각 메시지의 메시지 헤더(MQMD 구조)에 사용자의 ID로서 전파합니다. 이 ID는 메시지 컨텍스트 정보의 일부이고 367 페이지의 『UNIX, Linux, and Windows에서 컨텍스트 권한』에서 설명됩니다. 애플리케이션은 컨텍스트 정보를 변경할 권한이 부여되지 않는 한 이 정보를 변경할 수 없습니다.

프린시펄은 그룹에 속할 수 있습니다. 개인이 아닌 그룹에 자원 액세스를 부여하면 필요한 관리의 양을 줄일 수 있습니다. 액세스 제어 목록(ACL)은 그룹 및 사용자 ID 둘 모두를 기반으로 합니다.

예를 들어, 특정 애플리케이션을 실행하고 싶어하는 사용자로 구성된 그룹을 정의할 수도 있습니다. 기타 사용자는 해당 사용자 ID를 적절한 그룹에 추가하여 필요한 모든 자원에 대한 액세스를 제공받을 수 있습니다.

그룹을 정의하고 관리하는 이 프로세스는 특정 플랫폼별로 설명됩니다.

- **Windows** [Windows에서 그룹 작성 및 관리](#)
- **AIX** [AIX에서 그룹 작성 및 관리](#)
- **Solaris** [Solaris에서 그룹 작성 및 관리](#)
- **Linux** [Linux에서 그룹 작성 및 관리](#)

프린시펄은 둘 이상의 그룹(해당 그룹 세트)에 속할 수 있습니다. 이는 해당 그룹 세트에서 각 그룹에 부여된 모든 권한의 집합을 가지고 있습니다. 이러한 권한은 캐시되므로 프린시펄의 그룹 멤버십에 작성한 변경사항은 사용자가 MQSC 명령 **REFRESH SECURITY**(또는 해당 PCF에 해당하는 명령)을 실행하지 않는 한 큐 관리자가 재시작될 때까지는 인식되지 않습니다.

IBM MQ 8.0에서 액세스 제어 목록(ACL)은 사용자 ID 및 그룹을 기반으로 하며 [설치 가능 서비스 구성 및 UNIX 및 Linux에서 권한 부여 서비스 스탠다드 구성에 설명된 대로 SecurityPolicy 속성을 적절한 값으로 설정하여 권한 부여에 사용할 수 있습니다.](#)

IBM MQ 8.0부터, 권한 부여를 위해 사용자 기반 모델을 사용할 수 있으며, 이를 통해 사용자와 그룹을 모두 사용할 수 있습니다. 그러나 `setmqaut` 명령에 사용자를 지정할 때 새 권한은 사용자에게만 적용되고 해당 사용자가 속한 그룹에는 적용되지 않습니다. 자세한 정보는 [UNIX 및 Linux 시스템의 OAM 사용자 기반 권한을 참조](#) 하십시오.

권한 부여를 위해 그룹 기반 모델을 사용하는 경우, 사용자 ID가 속하는 기본 그룹이 ACL에 포함됩니다. 개별 사용자 ID는 포함되지 않고 권한은 해당 그룹의 모든 구성원에게 부여됩니다. 이로 인해 동일 그룹에서 또 다른 프린시펄의 권한을 변경하여 프린시펄의 권한을 부주의하게 변경할 수 있음을 유의하십시오.

모든 사용자가 명목상으로 nobody 기본 사용자 그룹에 지정되고, 기본적으로 이 그룹에는 권한 부여가 제공되지 않습니다. nobody 그룹의 권한을 변경하여 특정 권한 없이 사용자에게 IBM MQ 자원에 대한 액세스를 부여할 수 있습니다.

UNKNOWN 값으로 사용자 ID를 정의하지 마십시오. UNKNOWN 값은 사용자 ID가 너무 길 때 사용되므로 임의의 사용자 ID는 UNKNOWN의 액세스 권한을 사용합니다.

사용자는 최대 12자를 포함할 수 있고 그룹 이름은 12자를 포함할 수 있습니다.

Windows Windows 시스템

ACL은 사용자 ID 및 그룹 둘 모두를 기반으로 합니다. UNIX에서도 검사는 동일합니다. 동일한 사용자 ID가 있는 다른 도메인에서는 다른 사용자를 가질 수 있습니다. IBM MQ는 이러한 사용자에게 다른 액세스 레벨이 부여될 수 있도록 사용자 ID가 도메인 이름에 의해 규정되도록 허용합니다.

그룹 이름에는 선택적으로 다음 형식으로 지정된 도메인 이름을 포함할 수 있습니다.

```
GroupName@domain domain_name\group_name
```

글로벌 그룹은 두 가지 경우에만 OAM에 의해 검사됩니다.

1. 큐 관리자 보안 스탠자에는 GroupModel=GlobalGroups 설정이 포함됩니다. [보안을 참조하십시오](#).
2. 큐 관리자는 대체 보안 액세스 그룹을 사용 중입니다. [crtmqm](#) 을 참조하십시오.

사용자 ID는 최대 20자까지 포함하고 도메인 이름은 최대 15자, 그룹 이름은 최대 64자까지 포함할 수 있습니다.

OAM은 먼저 로컬 보안 데이터베이스를 검사한 다음 1차 도메인의 데이터베이스를 검사하고 마지막으로 신뢰하는 도메인의 데이터베이스를 검사합니다. 발견된 첫 번째 사용자 ID가 검사를 위해 OAM에 의해 사용됩니다. 이러한 각 사용자 ID에는 특정 컴퓨터에 여러 그룹 멤버십이 있을 수 있습니다.

일부 제어 명령(예: [crtmqm](#))은 오브젝트 권한 관리자(OAM)를 사용하여 IBM MQ 오브젝트에서 권한을 변경합니다. OAM은 특정 사용자 ID의 권한을 판별하기 위해 앞의 단락에 지정된 순서로 보안 데이터베이스를 검색합니다. 그 결과 OAM에 의해 판별된 권한은 사용자 ID가 로컬 mqm 그룹의 구성원이라는 사실을 대체할 수도 있습니다. 예를 들어, 글로벌 그룹을 통해 로컬 mqm 그룹의 멤버십을 가지고 있는 도메인 제어기에 의해 인증된 사용자 ID로부터 [crtmqm](#) 명령을 실행하는 경우 시스템에 로컬 mqm 그룹에 없고 이름이 같은 로컬 사용자가 있는 경우 명령이 실패합니다.

Windows에서 [SecurityPolicy](#) 속성을 설정하는 방법에 대한 자세한 정보는 [설치 가능 서비스 및 Windows에서 권한 부여 서비스 스탠자 구성을 참조하십시오](#).

Windows Windows 보안 ID(SID)

Windows의 IBM MQ는 사용 가능한 SID를 사용합니다. Windows SID가 권한 부여 요청과 함께 제공되지 않은 경우에는 IBM MQ는 사용자 이름만을 기반으로 사용자를 식별하지만 잘못된 권한이 부여되는 결과가 나올 수도 있습니다.

Windows 시스템에서 사용자 ID를 보충하기 위해 보안 ID(SID)가 사용됩니다. SID에는 사용자가 정의된 Windows 보안 계정 관리자(SAM) 데이터베이스에서 전체 사용자 계정 세부사항을 식별합니다. IBM MQ for Windows에서 메시지가 작성되면 IBM MQ는 SID를 메시지 디스크립터에 저장합니다. Windows에서 IBM MQ이 권한 검사를 수행하는 경우, SID는 SID를 사용하여 SAM 데이터베이스에서 전체 정보를 조회합니다. (이 조회가 성공하려면 사용자가 정의된 SAM 데이터베이스에 액세스할 수 있어야 합니다.)

기본적으로, Windows SID에 권한 부여 요청이 제공되지 않은 경우에는, IBM MQ는 사용자 이름만을 기반으로 사용자를 식별합니다. 이는 보안 데이터베이스를 다음 순서로 검색하여 수행됩니다.

1. 로컬 보안 데이터베이스
2. 1차 도메인의 보안 데이터베이스
3. 신뢰되는 도메인의 보안 데이터베이스

사용자 이름이 고유하지 않은 경우 잘못된 IBM MQ 권한이 부여될 수도 있습니다. 이 문제를 방지하려면 각 권한 요청에 SID를 포함하십시오. SID는 IBM MQ가 사용자 신임 정보를 설정하기 위해 사용합니다.

모든 권한 요청에 SID가 포함되도록 지정하려면 [regedit](#)를 사용하십시오. SecurityPolicy를 NTSIDsRequired로 설정하십시오.

ULW UNIX, Linux, and Windows에서 대체 사용자 권한

사용자 ID가 IBM MQ 오브젝트에 액세스할 때 또 다른 사용자의 권한을 사용할 수 있는 사용자 ID를 지정할 수 있습니다. 이는 대체 사용자 권한이라 불리고 이를 임의의 IBM MQ 오브젝트에서 사용할 수 있습니다.

대체 사용자 권한은 서버가 프로그램으로부터 요청을 수신하고 프로그램에 요청의 필수 권한이 있는지 확인하고 싶은 경우에 필수입니다. 서버에는 필수 권한이 있을 수 있지만 프로그램이 요청한 조치에 대한 권한이 있는지 여부를 알아야 합니다.

예를 들어, 사용자 ID PAYSERV 하에서 실행 중인 서버 프로그램이 큐에서 사용자 ID USER1에 의해 큐에 놓여진 요청 메시지를 검색한다고 가정해 보십시오. 서버 프로그램이 요청 메시지를 가져오면 요청을 처리하고 요청 메시지에 지정된 응답 대상 큐로 응답을 다시 넣습니다. 자체 사용자 ID(PAYSERV)를 사용하여 응답 대상 큐를 여는 권한을 부여하는 대신에 서버는 다른 사용자 ID를 지정할 수 있습니다. 이 경우에는 USER1입니다. 이 예에서는 대체 사용자 권한을 사용하여 PAYSERV가 응답 대상 큐를 열 때 대체 사용자 ID로서 USER1을 지정하도록 허용되는지 여부를 제어할 수 있습니다.

대체 사용자 ID는 오브젝트 디스크립터의 **AlternateUserId** 필드에 지정됩니다.

ULW UNIX, Linux, and Windows에서 컨텍스트 권한

컨텍스트는 특정 메시지에 적용되는 정보이며, 메시지의 일부인 메시지 설명자 MQMD에 포함되어 있습니다. 애플리케이션은 MQOPEN 또는 MQPUT 호출이 만들어질 때 컨텍스트 데이터를 지정할 수 있습니다.

컨텍스트 정보는 다음과 같은 두 개의 섹션으로 구성됩니다.

ID 섹션

메시지 송신자. 이는 UserIdentifier, AccountingToken 및 ApplIdentityData 필드로 구성됩니다.

원본 섹션

메시지 송신자 및 큐에 넣는 시기. 이는 PutApplType, PutApplName, PutDate, PutTime 및 ApplOriginData 필드로 구성됩니다.

애플리케이션은 MQOPEN 또는 MQPUT 호출이 만들어질 때 컨텍스트 데이터를 지정할 수 있습니다. 이 데이터는 애플리케이션에서 생성할 수 있으며, 다른 메시지에서 전달되거나 기본적으로 큐 관리자가 생성할 수 있습니다. 예를 들어, 서버 프로그램이 요청자의 ID를 검사하기 위해 컨텍스트 데이터를 사용하여 메시지가 권한 있는 사용자 ID 하에서 실행 중인 애플리케이션에서 나왔는지 여부를 테스트할 수 있습니다.

서버 프로그램은 UserIdentifier를 사용하여 대체 사용자의 사용자 ID를 판별할 수 있습니다. 컨텍스트 권한을 사용하여 사용자가 MQOPEN 또는 MQPUT1 호출에서 컨텍스트 옵션을 지정할 수 있는지 여부를 제어할 수 있습니다.

컨텍스트 옵션에 대한 정보는 [컨텍스트 정보 제어](#)를 참조하고 컨텍스트와 관련된 메시지 디스크립터 필드의 설명은 MQMD에 대한 개요를 참조하십시오.

보안 엑시트에서 액세스 제어 구현

MCAUserIdentifier 또는 오브젝트 권한 관리자를 사용하여 보안 엑시트에서 액세스 제어를 구현할 수 있습니다.

MCAUserIdentifier

현재 상태인 채널의 모든 인스턴스는 관련된 채널 정의 구조, 즉 MQCD를 가지고 있습니다. MQCD의 필드의 초기 값은 IBM MQ 관리자가 작성하는 채널 정의에 의해 판별됩니다. 특히, 필드 중 하나인 *MCAUserIdentifier*의 초기 값은 DEFINE CHANNEL 명령에서 MCAUSER 매개변수의 값에 의해 판별되거나, 채널 정의가 다른 방법으로 작성되는 경우에는 MCAUSER에 해당하는 값에 의해 판별됩니다.

MQCD 구조가 MCA에 의해 호출될 때 채널 엑시트 프로그램으로 전달됩니다. 보안 엑시트가 MCA에 의해 호출될 때, 보안 엑시트가 *MCAUserIdentifier*의 값을 변경할 수 있으며, 채널 정의에 지정된 모든 값을 바꿉니다.

Multi 멀티플랫폼에서 *MCAUserIdentifier*의 값이 공백이 아닌 한, 큐 관리자는 MCA가 큐 관리자에 연결한 후에 큐 관리자의 자원에 액세스하려고 시도할 때 *MCAUserIdentifier*의 값을 권한 검사를 위한 사용자 ID로서 사용합니다. *MCAUserIdentifier*의 값이 공백인 경우, 큐 관리자는 MCA의 기본 사용자 ID를 대신 사용합니다. 이는 RCVR, RQSTR, CLUSRCVR 및 SVRCONN 채널에 적용됩니다. MCA를 전송하기 위해 *MCAUserIdentifier*의 값이 공백이 아닐지라도 기본 사용자 ID가 항상 권한 검사에 사용됩니다.

z/OS

z/OS에서 큐 관리자는 공백이 아닌 경우 권한 검사를 위해 *MCAUserIdentifier*의 값을 사용할 수도 있습니다. 수신 MCA와 서버 연결 MCA의 경우, 큐 관리자가 권한 검사를 위해 *MCAUserIdentifier*의 값을 사용할 지 여부는 다음에 따라 결정됩니다.

- 채널 정의에 있는 PUTAUT 매개변수의 값
- 검사에 사용된 RACF 프로파일
- 채널 시작기 주소 공간 사용자 ID의 RESLEVEL 프로파일로의 액세스 레벨

송신 MCA의 경우에는, 다음에 따라 달라집니다.

- 송신 MCA가 호출자인지 응답자인지 여부
- 채널 시작기 주소 공간 사용자 ID의 RESLEVEL 프로파일로의 액세스 레벨

보안 엑시트가 *MCAUserIdentifier*에 저장하는 사용자 ID는 다양한 방법으로 얻을 수 있습니다. 다음은 일부 예입니다.

- MQI 채널의 클라이언트 끝에 보안 엑시트가 없는 경우, IBM MQ 클라이언트 애플리케이션과 연관된 사용자 ID는 클라이언트 애플리케이션이 MQCONN 호출을 실행할 때 클라이언트 연결 MCA에서 서버 연결 MCA로 흐릅니다. 서버 연결 MCA는 이 사용자 ID를 채널 정의 구조인 MQCD에서 *RemoteUserIdentifier* 필드에 저장합니다. *MCAUserIdentifier*의 값이 이 때에 비어 있으면, MCA가 *MCAUserIdentifier*에 같은 사용자 ID를 저장합니다. MCA가 사용자 ID를 *MCAUserIdentifier*에 저장하지 않는 경우 보안 엑시트는 *MCAUserIdentifier*를 *RemoteUserIdentifier*의 값으로 설정하여 이를 나중에 수행할 수 있습니다.

클라이언트 시스템에서 흐르는 사용자 ID가 새 보안 도메인을 입력하고 있고 서버 시스템에서 유효하지 않는 경우에는 보안 엑시트는 유효한 도메인을 위해 사용자 ID를 대체하고 대체된 사용된 ID를 *MCAUserIdentifier*에 저장합니다.

- 사용자 ID가 보안 메시지에서 파트너 보안 엑시트에 의해 송신될 수 있습니다.

메시지 채널에서 송신 MCA에 의해 호출되는 보안 엑시트의 경우 송신 MCA가 실행 중인 사용자 ID를 송신할 수 있습니다. 그런 후, 수신 MCA에 의해 호출되는 보안 엑시트가 사용자 ID를 *MCAUserIdentifier*에 저장할 수 있습니다. 마찬가지로 MQI 채널에서 채널의 클라이언트 끝에 있는 보안 엑시트는 IBM MQ MQI client 애플리케이션과 연관된 사용자 ID를 전송할 수 있습니다. 그런 후, 채널의 서버 측에 있는 보안 엑시트가 사용자 ID를 *MCAUserIdentifier*에 저장할 수 있습니다. 이전 예에 있는 것처럼, 사용자 ID가 대상 시스템에서 유효하지 않으면, 보안 엑시트가 유효한 사용자 ID로 그것을 대체하고 *MCAUserIdentifier*에 대체된 사용자 ID를 저장할 수 있습니다.

디지털 인증서가 식별과 인증 서비스의 일부로 수신되면, 보안 엑시트가 인증서의 식별 이름을 대상 시스템에서 유효한 사용자 ID로 맵핑할 수 있습니다. 그런 후, 사용자 ID를 *MCAUserIdentifier*에 저장할 수 있습니다.

- 채널에서 TLS가 사용되면 파트너의 식별 이름(DN)이 MQCD의 SSLPeerNamePtr 필드에 있는 엑시트로 전달되고 해당 인증서 발행인의 DN이 MQCXP의 SSLRemCertIssNamePtr 필드에 있는 엑시트로 전달됩니다.

MCAUserIdentifier 필드, 채널 정의 구조, MQCD 및 채널 엑시트 매개변수 구조, MQCXP에 대한 자세한 정보는 [채널 엑시트 호출 및 데이터 구조를 참조하십시오](#). MQI 채널에서 클라이언트 시스템에서 흐르는 사용자 ID에 대한 정보는 [액세스 제어](#)를 참조하십시오.

참고: IBM WebSphere MQ 7.1 릴리스 이전에 구성된 보안 엑시트 애플리케이션은 업데이트가 필요할 수 있습니다. 자세한 정보는 [채널 보안 엑시트 프로그램](#)을 참조하십시오.

IBM MQ 오브젝트 권한 관리자 사용자 인증

IBM MQ MQI client 연결에서 보안 엑시트는 오브젝트 권한 관리자(OAM) 사용자 인증에 사용된 MQCSP 구조를 수정하거나 작성하는 데 사용될 수 있습니다. 이에 대해서는 [메시지 채널의 채널 엑시트 프로그램](#)에 설명되어 있습니다.

메시지 엑시트에서 액세스 제어 구현

한 사용자 ID를 다른 사용자 ID로 대체하기 위해 메시지 엑시트를 사용해야 할 수도 있습니다.

메시지를 서버 애플리케이션에 전송하는 클라이언트 애플리케이션을 고려하십시오. 서버 애플리케이션은 메시지 디스크립터에서 *UserIdentifier* 필드로부터 사용자 ID를 추출하고, 대체 사용자 권한이 있는 경우 클라이언트 대신에 IBM MQ 자원에 액세스할 때 큐 관리자에게 이 사용자 ID를 사용하도록 요청합니다.

PUTAUT 매개변수가 채널 정의에서 CTX(또는 z/OS에서 ALTMCA)로 설정되면 각 수신 메시지의 *UserIdentifier* 필드의 사용자 ID는 MCA가 목적지 큐를 열 때 권한 검사에 사용됩니다.

어떤 상황에서는 보고 메시지가 생성되면, 보고가 필요한 메시지의 *UserIdentifier* 필드에 있는 사용자 ID의 권한이 필요하게 됩니다. 특히, COD(confirm-on-delivery) 보고서와 만기 보고서는 항상 이 권한이 필요합니다.

이런 상황 때문에, 메시지가 새 보안 도메인에 들어갈 때 *UserIdentifier* 필드에서 하나의 사용자 ID를 다른 것 대신에 사용할 필요가 있을 수 있습니다. 이는 채널의 수신 측에 있는 메시지 엑시트에 의해 수행될 수 있습니다. 또는, 수신되는 메시지의 *UserIdentifier* 필드에 있는 사용자 ID가 새 보안 도메인에 정의되어 있는지를 확인할 수 있습니다.

수신되는 메시지에 메시지를 송신한 애플리케이션의 사용자에 대한 디지털 인증서가 있으면, 메시지 엑시트가 인증서의 유효성을 검증하고 인증서의 식별 이름을 수신하고 있는 시스템에서 유효한 사용자 ID로 맵핑할 수 있습니다. 그런 후, 메시지 설명자에 있는 *UserIdentifier* 필드를 이 사용자 ID로 설정할 수 있습니다.

메시지 엑시트가 수신되는 메시지에 있는 *UserIdentifier* 필드의 값을 변경하는 것이 필요하다면, 메시지 엑시트가 메시지의 송신자를 동시에 인증하는 것이 적당할 수 있습니다. 자세한 정보는 [300 페이지의 『메시지 엑시트에서 ID 맵핑』](#)의 내용을 참조하십시오.

API 엑시트 및 API 교차 엑시트에서 액세스 제어 구현

API 또는 API 교차 엑시트는 IBM MQ가 제공한 액세스 제어를 보충하기 위해 액세스 제어를 제공할 수 있습니다. 특히 엑시트는 메시지 레벨에서 액세스 제어를 제공할 수 있습니다. 엑시트는 애플리케이션이 특정 기준을 충족하는 메시지만을 큐에 넣고, 큐에서 가져오도록 확실히 할 수 있습니다.

다음 예를 고려하십시오.



- 메시지에 임의의 주문에 대한 정보가 있습니다. 애플리케이션이 메시지를 큐에 넣을 때, API 또는 API 교차 엑시트는 주문의 총 값이 몇몇 미리 정해진 한계 미만인지 확인할 수 있습니다.
- 메시지가 리모트 큐 관리자로부터 목적지 큐에 도착합니다. 애플리케이션이 큐로부터 메시지를 가져오려고 시도할 때 API 또는 API 교차 엑시트는 메시지의 송신자가 메시지를 큐에 전송할 권한이 있는지 확인할 수 있습니다.

LDAP 권한 부여

LDAP 권한 부여를 사용하여 로컬 사용자 ID에 대한 필요를 제거할 수 있습니다.

지원 플랫폼에서 LDAP 권한 부여의 가용성

LDAP 권한 부여는 다음 플랫폼에서 사용 가능합니다.

-  UNIX
-  IBM i
-  Windows



주의:

IBM MQ 9.0 GA(General Availability)부터 이 기능은 이전 릴리스에서 마이그레이션되었던 새 항목이든 상관없이 모든 큐 관리자에서 사용 가능합니다.

LDAP 권한 부여의 개요

LDAP 권한을 사용하여 **setmqaut** 및 **DISPLAY AUTHREC**와 같은 권한 부여 구성을 처리하는 명령이 식별 이름을 처리할 수 있습니다. 이전에는 사용자는 신임 정보를 로컬 운영 체제에서 사용자 및 그룹에 대해 존재하는 최대 사용 가능한 문자와 비교하여 인증되었습니다.



주의: **DEFINE AUTHINFO** 명령을 실행한 경우 큐 관리자를 재시작해야 합니다. 큐 관리자를 다시 시작하지 않으면 **setmqaut** 명령이 올바른 결과를 리턴하지 않습니다.

사용자가 식별 이름이 아니라 사용자 ID를 제공하는 경우에는 사용자 ID가 처리됩니다. 예를 들어, 채널에 PUTAUT(CTX)와 함께 수신 메시지가 있으면 사용자 ID의 문자는 LDAP 식별 이름으로 매핑되고 적합한 권한 검사가 수행됩니다.

DISPLAY CONN 등과 같은 다른 명령은 해당 사용자 ID가 실제 로컬 OS에 존재하지 않을 수도 있지만 계속해서 작업하고 사용자 ID의 실제 값을 보여줍니다.

UNIX LDAP 권한이 부여된 경우, 큐 관리자는 `qm.ini` 파일의 **SecurityPolicy** 속성에 관계없이 항상 UNIX 플랫폼에서 보안의 사용자 모델을 사용합니다. 따라서 개별 사용자에게 권한을 설정하면 해당 사용자에게만 영향을 미치고 해당 사용자의 그룹에 속하는 다른 사용자에게는 영향을 미치지 않습니다.

OS 모델에서처럼 사용자는 여전히 개별 및 사용자가 속하는 모든 그룹(있는 경우) 둘 모두에 지정된 결합된 권한을 가지고 있습니다.

예를 들어, 다음 레코드가 LDAP 저장소에 정의되었다고 가정하십시오.

- **inetOrgPerson** 클래스에서:

```
dn="cn=JohnDoe, ou=users, o=yourcompany, c=yourcountry"
  email=JohnDoe1@yourcompany.com [longer than 12 characters]
  shortu=jodoe
  Phone=1234567
```

- **groupOfNames** 클래스에서:

```
dn="cn=Application Group A, ou=groups, o=yourcompany, c=yourcountry"
  longname=ApplicationGroupA [longer than 12 characters]
  members="cn=JaneDoe, ou=users, o=yourcompany, c=yourcountry",
          "cn=JohnDoe, ou=users, o=yourcompany, c=yourcountry"
```

인증 용도를 위해 이 LDAP 서버를 사용하는 큐 관리자는 해당 **CONNAUTH** 값이 IDPWLDAP 유형의 **AUTHINFO** 오브젝트를 가리키고 관련 이름-해석 속성이 다음과 같이 적절하게 설정되도록 정의되어 있어야 합니다.

```
USRFIELD(email) SHORTUSR(shortu)
BASEDNU(ou=users,o=yourcompany,c=yourcountry) CLASSUSR(inetOrgPerson)
```

인증을 위해 이 구성이 제공되면 애플리케이션은 MQCNO 호출 내에서 사용된 **CSPUserID** 필드를 다음 값 세트 하나로 채울 수 있습니다.

```
" cn=JohnDoe ", " JohnDoe1@yourcompany.com ", " email=JohnDoe1@yourcompany.com "
```

또는

```
" cn=JohnDoe, ou=users, o=ibm, c=uk ", " shortu=jodoe "
```

어느 경우든 시스템은 제공된 값을 사용하여 "jodoe"의 OS 컨텍스트를 인증할 수 있습니다.

설정 권한 부여

권한 부여를 사용하기 위해 약칭이나 **USRFIELD**를 사용하는 방법입니다.

369 페이지의 『LDAP 권한 부여』에 설명된 여러 형식에 대해 작업하는 방법은 권한 부여 명령으로 계속되고 추가적으로 확장하여 `shortname` 또는 **USRFIELD**를 꾸밈없는 방식으로 사용할 수 있습니다.

문자열은 권한 부여를 위한 사용자(프린시펄)의 이름을 지정할 때 LDAP 레코드에 특정 속성을 지정합니다.

중요사항: 이 문자는 운영 체제 사용자 ID에 사용할 수 없으므로 문자열은 = 문자를 포함해서는 안 됩니다.

잠재적으로 `shortname`인 권한 부여를 위해 프린시펄 이름을 OAM에 전달하는 경우에는 문자열은 12자에 맞아야 합니다. 매핑 알고리즘은 먼저 LDAP 조회에서 **SHORTUSR** 속성을 사용하여 이를 DN으로 해석하려고 시도합니다.

이것이 UNKNOWN_ENTITY 오류로 실패하거나 제공된 문자열이 shortname일 수 없으면 USRFIELD 속성을 사용하여 LDAP 조회를 구성하려는 추가 시도가 작성됩니다.



주의: DEFINE AUTHINFO 명령을 실행한 경우 큐 관리자를 재시작해야 합니다. 큐 관리자를 다시 시작하지 않으면 `setmqaut` 명령이 올바른 결과를 리턴하지 않습니다.

사용자 권한 부여 처리를 위해 다음 `setmqaut` 명령 설정은 모두 동등합니다.

표 72. 사용자 권한 부여 설정	
명령	참고
<code>setmqaut -m QM -t qmgr -p jodoe +connect</code>	이는 SHORTUSR을 통해 해석되는 평평한 완전하지 않은 이름입니다.
<code>setmqaut -m QM -t qmgr -pJohnDoe1@yourcompany.com +connect</code>	또한 USRFIELD를 통해 동일 엔티티로 해석되는 평평한 완전하지 않은 이름입니다.
<code>setmqaut -m QM -t qmgr -p email=JohnDoe1@yourcompany.com +connect</code>	이름 지정된 속성 사용.
<code>setmqaut -m QM -t qmgr -p "phone=1234567" +connect</code>	AUTHINFO 오브젝트에 구성된 속성일 필요가 없는 또 다른 이름 지정된 속성을 사용.

SET AUTHREC MQSC 명령을 `setmqaut` 명령의 대안으로 사용할 수 있습니다.

```
SET AUTHREC OBJTYPE(QMGR) PRINCIPAL('JohnDoe1@yourcompany.com') AUTHADD(connect)
```

또는 Set Authority Record (MQCMD SET AUTH_REC) PCF 명령을 다음 문자열을 포함하는 MQCACF_PRINCIPAL_ENTITY_NAMES 요소와 함께 사용하십시오.

```
"cn=JohnDoe,ou=users,o=yourcompany,c=yourcountry"
```

그룹을 처리할 때 그룹 이름의 양식을 12자에 맞춰야 한다는 요구사항이 없기 때문에 shortname 처리에 대한 모호성이 없습니다. 그러므로 그룹의 SHORTUSR 속성에 상응하는 속성이 없습니다.

즉, 371 페이지의 표 73에 설명된 구문 예는 올바른 의미를 의미하고 AUTHINFO 오브젝트를 확장된 속성과 함께 구성했고 다음으로 설정한 것으로 가정합니다.

```
GRPFIELD(longname)
BASEDNG(ou=groups,o=yourcompany,c=yourcountry ) CLASSGRP(groupOfNames)
```

표 73. 그룹 권한 부여 설정	
명령	참고
<code>setmqaut -m QM -t qmgr -g ApplicationGroupA +connect</code>	해석하기 위해 GRPFIELD 사용
<code>setmqaut -m QM -t qmgr -g longname=ApplicationGroupA +connect</code>	단일 속성 이름 지정
<code>setmqaut -m QM -t qmgr -g "cn=Application Group A,ou=groups,o=yourcompany,c=yourcountry" +connect</code>	전체 DN 사용

SET AUTHREC MQSC 명령을 앞의 **setmqaut** 명령에 대한 대안으로 사용할 수 있습니다.

```
SET AUTHREC OBJTYPE(QMGR) GROUP('ApplicationGroupA')
AUTHADD(connect)
```

또는 권한 레코드 설정(MQCMD SET AUTH_REC) PCF 명령을 다음 문자열을 포함하는 MQCACF_GROUP_ENTITY_NAMES 요소와 함께 사용하십시오.

```
"ApplicationGroupA"
```

중요사항:

사용자나 그룹이건 이름을 참조하기 위해 사용하는 형식은 고유한 DN을 파생하는 것이 가능해야 합니다.

따라서 예를 들어, 둘 모두 "shortu=jodoe"를 가지고 있는 두 개의 개별 레코드가 있으면 안됩니다.

단일 고유 DN을 판별할 수 없으면 OAM은 MQRC_UNKNOWN_ENTITY를 리턴합니다.

권한 부여 표시

사용자 또는 그룹의 권한 부여를 표시하는 다양한 방법

dspmqaout 명령

사용자 또는 그룹에 사용 가능한 권한 부여를 표시하기 위한 가장 단순한 방법은 **dspmqaout** 명령을 사용하는 것입니다.

사용자 또는 그룹을 식별하기 위해 구문 변화에 대한 조회를 사용할 수 있습니다. 명령 출력은 명령행에 제공된 형식으로 ID를 반복하는 점을 유의하십시오. 출력은 전체 해석된 DN에 대해서는 보고하지 않습니다.

예를 들면, 다음과 같습니다.

```
dspmqaout -m QM -t qmgr -p johndoe
Entity johndoe has the following authorizations for object QM:
connect
```

또는

```
dspmqaout -m QM -t qmgr -p email=JohnDoe1@yourcompany.com
Entity email=JohnDoe1@yourcompany.com has the following authorizations for object QM:
connect
```

dmpmqaut 및 dmpmqcfg 명령

dmpmqaut 명령 및 해당 MQSC 또는 PCF에 상응하는 명령은 지원되는 어떤 형식으로든 프린시플 또는 그룹을 지정할 수 있습니다(예: 370 페이지의 『설정 권한 부여』에 설명된 **setmqaut**처럼). 그러나 **dspmqaout**와 달리, **dmpmqaut** 명령은 항상 전체 DN을 보고합니다.

```
dmpmqaut -m QM -t qmgr -p jodoe
-----
profile: self
object type:qmgr
entity:cn=JohnDoe, ou=users, o=yourcompany, c=yourcountry
entity type: principal
authority: connect
```

마찬가지로, 선택된 레코드에서 필터링이 없는 **dmpmqcfg** 명령은 항상 나중에 재실행할 수 있는 형식으로 전체 DN을 표시합니다.

```
dmpmqcfg -m QM -x authrec
-----
SET AUTHREC PROFILE(SELF) +
```

```
PRINCIPAL('cn=JohnDoe, ou=users, o=yourcompany, c=yourcountry') +
OBJTYPE(QMGR)
AUTHADD(CONNECT)
```

LDAP 권한 부여 사용 시의 기타 고려사항

IBM MQ 9.0.0에서 LDAP 권한 부여를 사용할 때 알아야 하는 메시지 큐 인터페이스(MQI)와 기타 MQSC 및 PCF 명령의 변경사항에 대한 간략한 설명입니다.

ADOPTCTX

애플리케이션이 인증 정보를 제공하거나 ADOPTCTX 속성을 YES로 설정할 요구사항이 없습니다.

애플리케이션이 명백하게 인증하지 않거나 **ADOPTCTX**가 활성 CONNAUTH 오브젝트에 대해 NO로 설정된 경우에는 운영 체제 사용자 ID로부터 애플리케이션과 연관된 ID 컨텍스트를 구합니다.

권한 부여를 적용해야 하는 할 때, 해당 컨텍스트는 `setmqaut` 명령에서와 같은 규칙을 사용하여 LDAP ID에 맵핑됩니다.

MQI 호출에 대한 입력 매개변수

`MQOPEN`, `MQPUT1` 및 `MQSUB`에는 대체 사용자 ID를 지정할 수 있는 구조가 있습니다.

이러한 필드가 사용되면 12자 사용자 ID는 `setmqaut`, `dmpmqaut` 및 `dspmqaut` 명령에서와 같은 명령을 사용하여 DN에 맵핑됩니다.

`MQPUT` 및 `MQPUT1`은 또한 적합하게 권한이 부여된 프로그램이 `MQMD UserIdentifier` 필드를 설정하도록 허용합니다. 이 필드의 값은 PUT 프로세스 동안에 치안이 유지되지 않고 값으로 설정될 수도 있습니다.

그러나 평소처럼 **UserIdentifier** 값이 메시지 처리의 마지막 단계에서 권한 부여에 사용될 수 있습니다. 예를 들어, `PUTAUT(CTX)`가 수신 채널에 정의될 때입니다.

이 때 ID는 LDAP 또는 OS 기반일 수 있는 해당 수신 큐 관리자의 구성을 사용하여 권한 부여가 검사됩니다.

MQI 호출에 대한 출력 매개변수

MQI 구조에서 프로그램에 사용자 ID가 제공될 때마다 이는 연결과 연관된 12자의 약칭 버전입니다.

예를 들어, API 엑시트의 `MQAXC.UserId` 값은 LDAP 맵핑으로부터 돌아온 약칭입니다.

기타 관리 MQSC 및 PCF 명령

`DISPLAY CONN USERID` 등과 같이 오브젝트 상태에서 사용자 정보를 보여주는 명령은 컨텍스트와 연관된 12자 약칭 이름을 리턴합니다. 전체 DN은 표시되지 않습니다.

`CHLAUTH` 맵핑 규칙 또는 채널의 `MCAUSER` 값과 같이 ID의 어설션을 허용하는 명령은 이러한 속성에 정의된 최대 길이까지의 값을 취합니다(현재 64자).

구문에는 변경이 없습니다. 해당 ID에 대해 권한 부여가 필요할 때 이는 `setmqaut`, `dmpmqaut` 및 `dspmqaut` 명령에서와 같은 규칙을 사용하여 DN에 내부적으로 맵핑됩니다.

즉 채널 정의에서 `MCAUSER` 값은 `DISPLAY CHSTATUS`와 같은 문자열을 표시하지 않지만 이들이 동일한 ID를 참조한다는 의미입니다.

예를 들면, 다음과 같습니다.

```
DEFINE CHL(SV1) CHLTYPE(SVRCONN) MCAUSER('cn=JohnDoe')
DEFINE CHL(SV2) CHLTYPE(SVRCONN) MCAUSER('jodoe')
DEFINE CHL(SV3) CHLTYPE(SVRCONN) MCAUSER('JohnDoe1@yourcompany.com')
```

그런 다음 `DISPLAY CHSTATUS(*) ALL`은 모든 연결에 대해 `SHORTUSR` 값, `MCAUSER(jodoe)`를 표시합니다.

OS와 LDAP 권한 부여 모델 간 전환

서로 다른 플랫폼에서 서로 다른 권한 부여 메소드 간에 전환하는 방법입니다.

큐 관리자의 CONNAUTH 속성은 AUTHINFO 오브젝트를 가리킵니다. d오브젝트가 IDPWLDAP 유형이고 LDAP 저장소가 인증에 사용될 때.

이제 OS 기반 권한 부여를 계속할 수 있게 해주거나 LDAP 권한 부여에 대해 작업할 수 있게 해주는 동일 오브젝트에 권한 부여 메소드를 적용할 수 있습니다.

UNIX 플랫폼 및 IBM i



큐 관리자는 언제든지 OS와 LDAP 모델 사이에서 스위치할 수 있습니다. 구성을 변경하고 REFRESH SECURITY TYPE (CONNAUTH) 명령을 사용하여 해당 구성을 활성으로 만들 수 있습니다.

예를 들어, 이 오브젝트가 이미 인증을 위한 연결 정보로 구성된 경우:

```
ALTER AUTHINFO(MYLDAP) AUTHTYPE(IDPWLDAP) +
    AUTHORMD(SEARCHGRP) +
    BASEDNG('ou=groups,o=ibm,c=uk') +
    'other attributes'
ALTER QMGR CONNAUTH(MYLDAP)
REFRESH SECURITY
```

Windows



권한 구성 변경에 OS 및 LDAP 모델 간 전환이 포함된 경우 변경사항을 적용하려면 큐 관리자를 다시 시작해야 합니다. 그렇지 않으면 REFRESH SECURITY TYPE (CONNAUTH) 명령을 사용하여 변경사항을 활성화해야 합니다.

처리 규칙

OS에서 LDAP 권한 부여로 전환하면 설정된 기존 OS 권한이 비활성이 되고 표시되지 않게 됩니다.

dmpmqaut 등과 같은 명령은 이러한 OS 규칙을 표시하지 않습니다. 마찬가지로 LDAP에서 OS로 전환할 때 정의된 LDAP 권한 부여는 비활성이 되고 보이지 않게 되고 원본 OS 규칙을 복원합니다.

어떤 이유로든 **dmpmqcfcg** 명령을 사용하여 큐 관리자의 정의를 백업하고 싶은 경우에는 해당 백업에는 백업 시에 적용되는 권한 부여 메소드에 대해 정의된 규칙만을 포함할 것입니다.

LDAP 관리

각 플랫폼이 LDAP를 관리하는 방법의 개요.

LDAP 권한 부여를 사용할 때 운영 체제에서 mqm 그룹(또는 이에 상당하는 그룹)의 멤버십은 그다지 중요하지 않습니다. 해당 그룹의 구성원은 특정 명령행 명령을 처리할 수 있는지 여부만을 제어합니다.

특히, **strmqm** 및 **endmqm** 명령을 실행하려면 해당 그룹에 있어야 합니다.

일단 큐 관리자가 실행 중이면 이제는 완전한 권한이 있는 계정에는 한계가 있습니다. **strmqm** 명령을 실행한 사용자의 사용자 ID와는 별개로, OS mqm(또는 이에 상당하는) 그룹에 속하는 다른 사용자는 특수 권한을 받지 않습니다.

다른 사용자의 권한 부여는 이들이 속하는 LDAP 그룹에 따라 다릅니다. **setmqaut** 등과 같은 명령에서 mqm 그룹 이름을 자격 없이 사용하면 LDAP 그룹에 맵핑하도록 허용되지 않습니다.

UNIX 플랫폼



일단 큐 관리자가 실행 중이면 자동으로 완전한 권한이 있는 계정만이 큐 관리자를 시작한 실제 사용자입니다.

mqm ID가 여전히 존재하고 파일 등과 같은 OS 자원의 소유자로서 사용됩니다. mqm은 큐 관리자를 실행 중인 유효 ID이기 때문입니다. 그러나 mqm 사용자는 OAM에 의해 제어되는 관리 태스크를 자동으로 수행할 수 없을 것입니다.

IBM i

IBM i

IBM i에서 자동으로 권한이 있는 계정은 큐 관리자 및 QMQM ID를 시작한 계정입니다.

큐 관리자를 시작한 사용자 ID는 시스템을 시작하기 위해서만 필요하므로 두 ID 모두 필요합니다. 일단 실행 중이면 큐 관리자 프로세스에는 QMQM 권한만이 있습니다.

Windows 플랫폼

Windows

Windows에서 자동으로 전체 권한이 제공되는 계정은 큐 관리자를 시작한 OS 사용자와 코어 큐 관리자 프로세스를 실행하는 사용자입니다. 예를 들어, 큐 관리자가 Windows 서비스로 시작된 경우의 MUSR_MQADMIN입니다.

LDAP 권한 부여 모드에서 실행할 때 Windows는 UNIX 플랫폼과 매우 유사하게 작동합니다. 이는 12자 축약 이름 및 전체 DN을 다룹니다.

샘플 스크립트

큐 관리자에서 전체 관리를 수행할 수 있는 그룹이 있는 것이 유용하므로 샘플 스크립트는 UNIX 플랫폼에 다음과 같이 탑재되어 있습니다.

```
MQ_INSTALLATION_PATH/samp/bin/amqauthg.sh
```

이 샘플은 두 개의 매개변수를 사용합니다.

- 큐 관리자 이름
- LDAP 그룹 이름

샘플은 `setmqaut` 명령을 처리하여 모든 오브젝트에 전체 권한을 부여합니다. 이는 관리 역할을 위해 IBM MQ Explorer OAM 마법사가 생성한 것과 동일한 스크립트입니다. 예를 들어, 코드는 다음과 같이 시작됩니다.

```
setmqaut -t q -m qmgr -n "*" +alladm +allmqi -g  
groupname
```

메시지의 기밀성

기밀성을 유지하려면 메시지를 암호화하십시오. 사용자의 필요에 따라 IBM MQ에서 메시지를 암호화하는 다양한 방법이 있습니다.

사용자가 선택한 CipherSpec은 사용자가 가지는 기밀성 레벨을 판별합니다.

포인트-투-포인트 메시징 인프라에 대해 애플리케이션 레벨의 엔드-투-엔드 데이터 보호가 필요한 경우 Advanced Message Security를 사용하여 메시지를 암호화하거나 자체 API 엑시트 또는 API 교차 엑시트를 작성할 수 있습니다.

큐 관리자에 적합한 보안이 있기 때문에 채널을 통해 전송되는 동안에만 메시지를 암호화해야 하는 경우에는 TLS를 사용하거나 사용자 고유의 보안 엑시트, 메시지 엑시트 또는 송신 및 수신 엑시트 프로그램을 작성할 수 있습니다.

z/OS V 9.1.4 큐 관리자에서 저장 메시지를 암호화해야 하는 경우에는 해당 큐 관리자에서 z/OS 데이터 세트 암호화를 사용할 수 있습니다.

Advanced Message Security에 대한 자세한 정보는 92 페이지의 『Advanced Message Security 계획』의 내용을 참조하십시오. IBM MQ에서 TLS를 사용하는 방법은 21 페이지의 『IBM MQ의 TLS 보안 프로토콜』에 설

명되어 있습니다. 메시지 암호화에서 엑시트 프로그램의 사용은 401 페이지의 『사용자 엑시트 프로그램에서 기밀성 구현』에 설명됩니다.

데이터 세트 암호화를 사용하는 IBM MQ for z/OS의 저장 데이터에 대한 기밀성 섹션을 참조하십시오. z/OS 데이터 세트 암호화에 대한 자세한 정보를 제공합니다.

관련 태스크

[TLS를 사용하여 두 개의 큐 관리자 연결](#)
[클라이언트를 큐 관리자에 안전하게 연결](#)

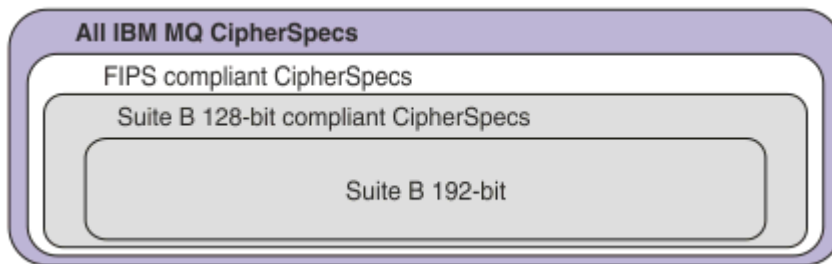
CipherSpec 사용 가능

DEFINE CHANNEL MQSC 명령 또는 **ALTER CHANNEL** MQSC 명령에서 **SSLCIPH** 매개변수를 사용하여 CipherSpec을 사용 가능으로 설정하십시오.

IBM MQ에 사용할 수 있는 CipherSpec 중 일부는 FIPS를 준수합니다. FIPS 준수 CipherSpec 중 일부는 스위트 B도 준수하지만 TLS_RSA_WITH_3DES_EDE_CBC_SHA와 같은 일부는 이를 준수하지 않습니다.

모든 스위트 B 준수 CipherSpec은 FIPS도 준수합니다. 모든 스위트 B 준수 CipherSpec은 두 개의 그룹에 해당합니다. 128비트(예: ECDHE_ECDSA_AES_128_GCM_SHA256) 및 192비트(예: ECDHE_ECDSA_AES_256_GCM_SHA384)입니다.

다음 다이어그램은 이러한 서브세트 간의 관계를 설명합니다.



IBM MQ 8.0.0 Fix Pack 3 에서 지원되는 CipherSpecs 수가 감소되었습니다.

V 9.1.1 기본 CipherSpec 구성에 대한 정보는 380 페이지의 『IBM MQ에서 사용으로 설정된 기본 CipherSpec 값』의 내용을 참조하십시오. MQ 채널과 함께 사용할 수 있는 대체 CipherSpec 세트를 제공할 수도 있습니다. 381 페이지의 『멀티플랫폼에 사용 가능한 CipherSpec의 사용자 정의 목록 제공』을 참조하십시오.

더 이상 사용되지 않는 CipherSpec을 사용으로 설정하는 것에 관한 정보는 381 페이지의 『멀티플랫폼에서 CipherSpec 사용』 또는 382 페이지의 『z/OS에서 더 이상 사용되지 않는 CipherSpec 사용』의 내용을 참조하십시오. IBM MQ와 함께 사용하기 위해 다시 사용으로 설정할 수 있는 CipherSpec의 목록의 경우, 384 페이지의 『더 이상 사용되지 않는 CipherSpec』의 내용을 참조하십시오.

ULW **V 9.1.4** IBM MQ 9.1.4부터, IBM MQ는 UNIX, Linux, and Windows에서 TLS 1.3 보안 프로토콜을 지원합니다. 이러한 CipherSpec을 사용하는 데 대한 정보는 379 페이지의 『IBM MQ에서 TLS 1.3 사용』 및 380 페이지의 『IBM MQ MQI client와 TLS 1.3』의 내용을 참조하십시오.

IBM MQ TLS 지원과 함께 사용할 수 있는 CipherSpec

IBM MQ 큐 관리자와 함께 사용할 수 있는 암호 스펙은 다음 테이블에 자동으로 나열됩니다. 개인 인증서를 요청할 때 공용 및 개인 키 쌍의 키 크기를 지정합니다. TLS 데이터 교환 동안에 사용되는 키 크기는 인증서에 저장된 크기입니다(표에 명시된 것처럼 CipherSpec으로 판별되는 경우는 제외).

표 74. IBM MQ TLS 지원과 함께 사용할 수 있는 CipherSpec

플랫폼 지원 379 페이지의 『1』	CipherSpec 이름	16진 코드	사용되는 프로토콜	데이터 무결성	암호화 알고리즘 (암호화 비트)	FIPS 379 페이지의 『2』	스위트 B
▶ V 9.1.4 ▶ V 9.1.4 알리어스 CipherSpec							
모두	ANY_TLS13_OR_HIGHER 379 페이지의 『3』 379 페이지의 『4』 379 페이지의 『5』	해당사항 없음	조정됨	조정됨	조정됨	조정됨	조정됨
모두	ANY_TLS13 379 페이지의 『4』 379 페이지의 『5』 379 페이지의 『6』	해당사항 없음	TLS 1.3	조정됨	조정됨	조정됨	조정됨
모두	ANY_TLS12_OR_HIGHER 379 페이지의 『4』 379 페이지의 『5』 379 페이지의 『7』	해당사항 없음	조정됨	조정됨	조정됨	조정됨	조정됨
모두	ANY_TLS12 379 페이지의 『8』	해당사항 없음	TLS 1.2	조정됨	조정됨	조정됨	조정됨
모두	ANY 379 페이지의 『9』	해당사항 없음	조정됨	조정됨	조정됨	조정됨	조정됨
▶ V 9.1.4 ▶ V 9.1.4 CipherSpecs for TLS 1.3							
모두	TLS_AES_128_GCM_SHA256 379 페이지의 『4』	1301	TLS 1.3	GCM	AES-128 (GCM 포함)	예	아니오
모두	TLS_AES_256_GCM_SHA384 379 페이지의 『4』	1302	TLS 1.3	GCM	AES-256 (GCM 포함) (256)	예	아니오
모두	TLS_CHACHA20_POLY1305_SHA256 379 페이지의 『4』	1303	TLS 1.3	POLY1305	CHACHA20 (256)	아니오	아니오
▶ ULW	TLS_AES_128_CCM_SHA256	1304	TLS 1.3	CBC-MAC	CTR (128) 이 있는 AES-128	예	아니오
▶ ULW	TLS_AES_128_CCM_8_SHA256 379 페이지의 『11』	1305	TLS 1.3	CBC-MAC	CTR (128) 이 있는 AES-128	예	아니오
CipherSpecs for TLS 1.2							
모두	TLS_RSA_WITH_AES_128_CBC_SHA256 379 페이지의 『10』	003C	TLS 1.2	SHA-256	AES (128)	예	아니오
모두	TLS_RSA_WITH_AES_256_CBC_SHA256 379 페이지의 『10』 379 페이지의 『12』	003D	TLS 1.2	SHA-256	AES (256)	예	아니오
모두	TLS_RSA_WITH_AES_128_GCM_SHA256 379 페이지의 『10』 379 페이지의 『13』	009C	TLS 1.2	SHA-256 과 AEAD GCM	AES (128)	예	아니오
모두	TLS_RSA_WITH_AES_256_GCM_SHA384 379 페이지의 『10』 379 페이지의 『12』 379 페이지의 『13』	009D	TLS 1.2	SHA-384 와 AEAD GCM	AES (256)	예	아니오
모두	ECDHE_ECDSA_AES_128_CBC_SHA256 379 페이지의 『10』	C023	TLS 1.2	SHA-256	AES (128)	예	아니오

표 74. IBM MQ TLS 지원과 함께 사용할 수 있는 CipherSpec (계속)

플랫폼 지원 379 페이지의 『1』	CipherSpec 이름	16진 코드	사용되는 프로토콜	데이터 무결성	암호화 알고리즘 (암호화 비트)	FIPS 379 페이지의 『2』	스위트 B
모두	ECDHE_ECDSA_AES_256_CBC_SHA384 379 페이지의 『10』 379 페이지의 『12』	C024	TLS 1.2	SHA-384	AES (256)	예	아니오
모두	ECDHE_RSA_AES_128_CBC_SHA256 379 페이지의 『10』	C027	TLS 1.2	SHA-256	AES (128)	예	아니오
모두	ECDHE_RSA_AES_256_CBC_SHA384 379 페이지의 『10』 379 페이지의 『12』	C028	TLS 1.2	SHA-384	AES (256)	예	아니오
Multi	ECDHE_ECDSA_AES_128_GCM_SHA256 379 페이지의 『12』 379 페이지의 『13』	C02B	TLS 1.2	SHA-256 과 AEAD GCM	AES (SHA384)	예	128 비트
Multi	ECDHE_ECDSA_AES_256_GCM_SHA384 379 페이지의 『12』 379 페이지의 『13』	C02C	TLS 1.2	SHA-384 와 AEAD GCM	AES (SHA384)	예	192 비트
모두	ECDHE_RSA_AES_128_GCM_SHA256 379 페이지의 『13』	C02F	TLS 1.2	SHA-256 과 AEAD GCM	AES (128)	예	아니오
모두	ECDHE_RSA_AES_256_GCM_SHA384 379 페이지의 『12』 379 페이지의 『13』	C030	TLS 1.2	AEAD AES-128 GCM	AES (SHA384)	예	아니오

표 74. IBM MQ TLS 지원과 함께 사용할 수 있는 CipherSpec (계속)

플랫폼 지원 379 페이지의 『1』	CipherSpec 이름	16진 코드	사용되는 프로토콜	데이터 무결성	암호화 알고리즘 (암호화 비트)	FIPS 379 페이지의 『2』	스위트 B
---------------------------	---------------	--------	-----------	---------	-------------------	----------------------	-------

참고:

1. 각 플랫폼 아이콘에서 다루는 플랫폼 목록은 제품 문서의 릴리스 및 플랫폼 아이콘의 내용을 참조하십시오.
2. FIPS 인증 플랫폼에서 CipherSpec이 FIPS 인증 CipherSpec인지 여부를 지정합니다. FIPS에 대한 설명은 FIPS(Federal Information Processing Standards)를 참조하십시오.
3. **ULW** ANY_TLS13_OR_HIGHER 알리어스 CipherSpec은 원격 끝이 허용할 것이나 TLS 1.3 이상의 프로토콜을 사용해서만 연결되는 최상위 레벨의 보안을 협상합니다.
4. **z/OS** IBM MQ for z/OS에서 TLS 1.3 또는 ANY CipherSpec을 사용하려면 운영 체제가 z/OS 2.4 이상이어야 합니다.
5. **IBM i** IBM i에서 TLS 1.3 또는 ANY CipherSpec을 사용하려면 기반 운영 체제 버전이 TLS 1.3을 지원해야 합니다. 자세한 정보는 TLSv1.3에 대한 시스템 TLS 지원을 참조하십시오.
6. **ULW** ANY_TLS13 알리어스 CipherSpec은 각 플랫폼에 대해 이 표에 나열된 대로 TLS 1.3 프로토콜을 사용하는 허용 가능한 CipherSpec의 서브세트를 나타냅니다.
7. **ULW** ANY_TLS12_OR_HIGHER 알리어스 CipherSpec은 원격 끝이 허용할 것이나 TLS 1.2 이상의 프로토콜을 사용해서만 연결되는 최상위 레벨의 보안을 협상합니다.
8. ANY_TLS12 CipherSpec은 각 플랫폼에 대해 이 표에 나열된 대로 TLS 1.2 프로토콜을 사용하는 허용 가능한 CipherSpec의 서브세트를 나타냅니다.
9. **ULW** ANY 알리어스 CipherSpec은 원격 끝이 허용할 최상위 레벨의 보안을 협상합니다.
10. **IBM i** 이러한 CipherSpec은 시스템 값 QSSLCSLCTL이 *OPSSYS로 설정된 IBM i 7.4 시스템에서 사용 가능하지 않습니다.
11. **ULW** 이러한 CipherSpec은 16-옥텟 무결성 검사 값(ICV) 대신에 8-옥텟 ICV를 사용합니다.
12. 탐색기가 사용하는 JRE에 제한 없는 적절한 정책 파일이 적용되지 않는 한, 이 CipherSpec을 사용하여 IBM MQ Explorer에서 큐 관리자로의 연결을 보호할 수 없습니다.
13. **Windows Linux** GSKit의 권장사항에 따라 TLS 1.2 GCM CipherSpecs에는 동일한 세션 키를 사용하여 2점두부24.5 TLS 레코드가 전송된 후 연결이 종료되고 AMQ9288E 메시지가 표시됩니다. 이 GCM 제한사항은 사용된 니다 니다 the 니다 (FIPS 모드에 관계없이).

이 오류가 발생하지 않도록 하려면 TLS 1.2 GCM 암호를 사용하지 않고 비밀 키 재설정을 사용으로 설정하거나 환경 변수 GSK_ENFORCE_GCM_RESTRICTION=GSK_FALSE가 설정된 IBM MQ 큐 관리자 또는 클라이언트를 시작하십시오. GSKit 라이브러리의 경우, 연결의 양쪽에서 이 환경 변수를 설정하고 이를 클라이언트 대 큐 관리자 연결 및 큐 관리자 대 큐 관리자 연결 모두에 적용해야 합니다. 이 설정은 비관리 .NET 클라이언트에는 영향을 주지 않지만 Java 또는 관리 .NET 클라이언트에는 영향을 주지 않습니다. 자세한 정보는 AES-GCM 암호 제한을 참조하십시오.

이 제한은 IBM MQ for z/OS에는 적용되지 않습니다.

IBM MQ에서 TLS 1.3 사용

ULW V 9.1.4

IBM MQ 9.1.4부터, IBM MQ는 UNIX, Linux, and Windows에서 TLS 1.3을 지원합니다. 지원되는 설치에서는 다음과 같은 qm.ini 파일의 SSL 스탠자로 된 항목을 사용하여 새 큐 관리자가 작성됩니다.

```
SSL:
  AllowTLSV13=TRUE
```

참고: `qm.ini` 파일은 `<data directory>/qmgrs/<qmgr name>` 디렉토리에서 찾을 수 있습니다.

큐 관리자가 IBM MQ 9.1.4 이전의 IBM MQ 버전을 사용하여 작성되었지만 나중에 IBM MQ 9.1.4 이상을 사용하여 시작되는 경우, **AllowTLSV13** 특성 세트가 없습니다. TLS 1.3을 사용하려면 `qm.ini` file 를 편집하고 예제에 표시된 대로 특성에 추가해야 합니다 (" SSL: 스탠자가 아직 없는 경우에는 스탠자 포함).

이 `.ini` 파일 특성은 TLS 1.3을 사용으로 설정하며, 이는 TLS 1.3 CipherSpec을 사용할 수 있도록 합니다. TLS 1.3 스펙에 따라, 약한 CipherSpec을 사용한 통신 시도는 IBM MQ에서의 사용 설정 여부와 상관없이 거부됩니다. TLS 1.3이 약한 것으로 간주하는 CipherSpec은 다음 기준을 하나 이상 충족합니다.

- SSL 3.0 프로토콜을 사용합니다.
- RC4 또는 RC2를 암호화 알고리즘으로 사용합니다.
- 암호화 키 크기(비트)가 112 이하입니다.

이러한 제한은 더 이상 사용되지 않는 CipherSpec에 대한 표 1에서 참고 [10]으로 플래그 지정되어 있습니다.

이러한 CipherSpec을 계속해서 사용해야 하는 경우에는 TLS 1.3 모드를 사용 안함으로 설정해야 합니다. 큐 관리자의 `qm.ini` 파일을 편집하고 **AllowTLSV13** 특성의 설정을 다음과 같이 변경하여 이를 수행합니다.

```
SSL:
  AllowTLSV13=FALSE
```

참고: 이 설정이 완료되면 TLS 1.3 CipherSpec을 사용할 수 없습니다.

IBM MQ MQI client와 TLS 1.3

ULW V 9.1.4

IBM MQ MQI client 클라이언트를 사용하는 경우, **AllowTLSV13**의 값은 애플리케이션에서 사용 중인 `mqclient.ini` 파일의 SSL 스탠자에 명시적으로 지정되지 않은 한 다음과 같이 추정됩니다.

- 약한 CipherSpec이 사용으로 설정된 경우에는 **AllowTLSV13**이 FALSE로 설정되며 TLS 1.3 CipherSpec을 사용할 수 없습니다.
- 그 외의 경우에는 **AllowTLSV13**이 TRUE로 설정되며 새 TLS 1.3 CipherSpec 및 알리어스 CipherSpec을 사용할 수 있습니다.

IBM MQ에서 사용으로 설정된 기본 CipherSpec 값

V 9.1.1 Multi

기본 구성에서, IBM MQ는 CipherSpec을 사용하는 TLS 1.2 프로토콜과 다양한 암호화 알고리즘을 지원합니다. 호환성을 목적으로 IBM MQ가 SSL 3.0 및 TLS 1.0 프로토콜과 보안 취약성에 민감하거나 취약하다고 알려진 여러 암호화 알고리즘을 사용하도록 구성할 수도 있습니다. 기본 구성에서 사용으로 설정된 CipherSpec의 목록은 유지보수를 적용하여 변경할 수도 있습니다.

다음 제어를 사용하여 CipherSpec의 사용을 제한하거나 허용하기 위해 IBM MQ를 구성할 수 있습니다.

- SSLFIPS를 사용하는 FIPS 140-2 준수 CipherSpec만 허용.
- **ULW** SUITEB를 사용하는 NSA Suite B 준수 CipherSpec만 허용.
- **ULW** **AllowedCipherSpecs** 또는 **AMQ_ALLOWED_CIPHERS** 환경 변수를 사용하여 사용자 정의 CipherSpec 목록을 허용합니다.
- **ULW** **AllowWeakCipher** 또는 **AMQ_SSL_WEAK_CIPHER_ENABLE** 환경 변수를 사용하여 더 이상 사용되지 않는 CipherSpec의 사용을 허용합니다.
- **z/OS** CHINIT JCL의 DD 문을 사용하여 더 이상 사용되지 않는 CipherSpec의 사용을 허용.

참고: **AllowedCipherSpecs** 또는 **AMQ_ALLOWED_CIPHERS**를 사용하여 CipherSpec의 사용자 정의 목록을 지정하면 이는 더 이상 사용되지 않는 CipherSpec의 사용을 대체합니다. 사용자 정의 CipherSpec 목록과 함께 NSA Suite B 또는 FIPS 140-2 제한사항을 사용할 경우, 사용자 정의 목록에 Suite B 또는 FIPS 140-2 설정에서 허용하는 CipherSpec만 포함되어 있는지 확인하십시오.

멀티플랫폼에 사용 가능한 CipherSpec의 사용자 정의 목록 제공

V 9.1.1

Multi

AMQ_ALLOWED_CIPHERS 환경 변수 또는 `.ini` 파일의 **AllowedCipherSpecs** SSL 스탠자 속성을 사용하여 IBM MQ 채널에서 사용할 수 있는 대체 CipherSpec 세트를 제공할 수 있습니다. 이 설정을 사용하여, IBM MQ 리스너가 이름 지정된 CipherSpec을 사용하는 경우를 제외하고 수신 채널 시작 요청을 승인하지 않도록 제한할 수 있습니다. 이 기능은 ANY* CipherSpec에 포함되는 CipherSpec을 제어하는 데 사용할 수 있습니다.

AMQ_ALLOWED_CIPHERS 환경 변수 또는 **AllowedCipherSpecs** SSL 스탠자 속성은 다음 항목을 값으로 허용합니다.

- 단일 CipherSpec 이름 또는
- 다시 사용으로 설정할 IBM MQ CipherSpec 이름의 쉼표로 구분된 목록 또는
- 모든 CipherSpec을 나타내는 특수 값 ALL(권장되지 않음).

참고: ALL CipherSpec은 SSL 3.0 및 TLS 1.0 프로토콜과 다수의 약한 암호화 알고리즘을 사용으로 설정할 수 있기 때문에 사용하지 않는 것이 좋습니다.

이 설정이 구성된 경우 이는 기본 CipherSpec 목록을 대체하며 IBM MQ가 약한 암호 사용 중단 설정을 무시하도록 합니다(아래 내용 참조).

- IBM MQ 리스너가 이름 지정된 CipherSpec 중 하나를 사용하는 SSL/TLS 제안만 허용합니다.
- IBM MQ 채널이 공백 SSLCIPH 값, 또는 이름 지정된 CipherSpec 중 하나만 허용합니다.
- SSLCIPH 값에 대해 **runmqsc**의 Tab 키를 사용한 자동 완성 기능을 사용하면 해당 값이 이름 지정된 CipherSpec 중 하나로 제한됩니다.

예를 들어, 채널이 정의/변경되고 리스너가 ECDHE_RSA_AES_128_GCM_SHA256 또는 ECDHE_ECDSA_AES_256_GCM_SHA384를 허용하도록 하려는 경우 `qm.ini` 파일에서 다음을 설정할 수 있습니다.

```
SSL:
  AllowedCipherSpecs=ECDHE_RSA_AES_128_GCM_SHA256, ECDHE_ECDSA_AES_256_GCM_SHA384
```

`java.security` 파일 설정을 사용하여 AMQP 또는 MQTT 채널에서 사용되는 암호를 제한할 수 있습니다.

멀티플랫폼에서 CipherSpec 사용

Multi

기본적으로 채널 정의에 더 이상 사용되지 않는 CipherSpec을 지정하도록 허용되지 않습니다. 멀티플랫폼에서 더 이상 사용되지 않는 CipherSpec을 지정하려 시도하면 `AMQ8242: SSLCIPH definition wrong` 메시지가 수신되며 PCF가 `MQRCCF_SSL_CIPHER_SPEC_ERROR`를 리턴합니다.

더 이상 사용되지 않는 CipherSpec으로 채널을 시작할 수 없습니다. 더 이상 사용되지 않는 CipherSpec을 사용하여 수행하려고 하면 시스템에서 `MQCC_FAILED (2)`와 `MQRC_SSL_INITIALIZATION_ERROR (2393)`의 **Reason** 을(를) 클라이언트에 리턴합니다.

환경 변수 **AMQ_SSL_WEAK_CIPHER_ENABLE**을(를) 설정하여 서버에서 런타임 시 채널을 정의하기 위해 더 사용되지 않는 하나 이상의 CipherSpec을 다시 사용할 수 있습니다.

AMQ_SSL_WEAK_CIPHER_ENABLE 환경 변수는 다음을 승인합니다.

- 단일 CipherSpec 이름 또는
- 다시 사용으로 설정할 IBM MQ CipherSpec 이름의 쉼표로 구분된 목록 또는
- 모든 CipherSpec을 나타내는 특수 값 ALL(권장되지 않음).

참고: ALL CipherSpec을 사용으로 설정하는 경우 SSL 3.0 및 TLS 1.0 프로토콜과 다수의 취약한 암호화 알고리즘이 사용 설정되므로 이는 권장되지 않습니다.

예를 들어, `ECDHE_RSA_RC4_128_SHA256`을 다시 사용으로 설정하려면 다음 환경 변수를 설정하십시오.


```
export AMQ_SSL_WEAK_CIPHER_ENABLE=ECDHE_RSA_RC4_128_SHA256
```

또는 다음과 같이 설정하여 qm.ini 파일에서 SSL 스탠자를 변경하십시오.

```
SSL:
  AllowTLSV1=Y
  AllowWeakCipherSpec=ECDHE_RSA_RC4_128_SHA256
```

z/OS에서 더 이상 사용되지 않는 CipherSpec 사용

z/OS

기본적으로 채널 정의에 더 이상 사용되지 않는 CipherSpec을 지정하도록 허용되지 않습니다. z/OS에서 더 이상 사용되지 않는 CipherSpec을 지정하려고 시도하면 CSQM102E 또는 CSQX674E 메시지를 수신합니다.

약한(더 이상 사용되지 않는) Cipherspecs를 사용하려면 CHINIT JCL에 다음 DD 명령문을 정의해야 합니다.

```
JCL: //CSQXWEAK DD DUMMY
```

참고: 더 이상 사용되지 않는 CipherSpecs 가 이 DD 명령문을 사용해야 하는 것은 아닙니다. [384 페이지의 『더 이상 사용되지 않는 CipherSpec』](#)에 있는 표의 참고 11을 참조하십시오.

더 이상 사용되지 않는 SSL 3.0 프로토콜을 사용으로 설정하려면 CHINIT JCL에서 다음 DD 명령문도 정의해야 합니다.

```
JCL: //CSQXSSL3 DD DUMMY
```

V 9.1.0 더 이상 사용되지 않는 TLS 1.0 프로토콜을 사용으로 설정하려면 CHINIT JCL에서 다음 DD 명령문도 정의해야 합니다.

```
JCL: //TLS100N DD DUMMY
```

DD 카드의 이름은 TLS100N이며 TLS100N이 아닌 TLS10이 켜져 있음을 의미합니다.

TLS 1.0을 끄려면 다음 명령문을 사용하십시오.

```
JCL: //TLS100FF DD DUMMY
```

취약하거나 중단된 암호 스펙을 사용하여 리스너와 협상하지 않으려면 CHINIT JCL에서 다음 DD 문을 정의해야 합니다.

```
JCL: //WCIPSOFF DD DUMMY
```

System SSL 기본 암호 스펙 목록에 나열된 암호 스펙을 사용하여 리스너와 협상만 수행하려는 경우 CHINIT JCL에서 다음 DD 문을 정의해야 합니다.

```
JCL: //GSKDCIPS DD DUMMY
```

최소 레벨 대 고정 레벨 CipherSpec

ULW V 9.1.4

IBM MQ는 두 가지 서로 다른 CipherSpec 유형을 지원합니다.

- **최소 레벨 CipherSpec**은 상한을 설정하지 않는 유형입니다(예: ANY, ANY_TLS12_OR_HIGHER 또는 ANY_TLS13_OR_HIGHER).
- **고정 레벨 CipherSpec**은 특정 프로토콜(예: ANY_TLS12 및 ANY_TLS13) 또는 특정 알고리즘(예: ECDHE_ECDSA_3DES_EDE_CBC_SHA256)을 식별하는 유형입니다.

구성을 최대한 단순하게 하면서 보안을 유지하려면 채널 양측에서 **최소 레벨 CipherSpec**을 사용하는 것이 좋습니다. 이는 통신의 양측이 더 높은 TLS 프로토콜 버전을 지원하는 경우 양측의 구성을 변경할 필요없이 자동으로 새 버전을 지원하고 사용할 수 있도록 합니다.

시작 측에서 **최소 레벨 CipherSpec** 을 사용하여 수신측의 **고정 레벨 CipherSpec** 을 사용하면 연결이 거부되고 AMQ9631 및 AMQ9641 메시지가 발행될 수 있습니다.

별명 CipherSpec 설정에 대해 다른 결과를 포함하는 테이블은 [387 페이지의 『알리어스 CipherSpec 설정 간 관계』](#) 를 참조하십시오.

관련 개념

[40 페이지의 『IBM MQ에서 디지털 인증서와 CipherSpec의 호환성』](#)

이 토픽은 IBM MQ에서 CipherSpec과 디지털 인증서 사이의 관계를 소개하여 보안 정책에 대해 적합한 CipherSpec 및 디지털 인증서를 선택하는 방법에 대한 정보를 제공합니다.

[17 페이지의 『CipherSpecs 및 CipherSuites』](#)

암호화 보안 프로토콜은 안전 연결에서 사용되는 알고리즘에 동의해야 합니다. CipherSpec 및 CipherSuite는 특정 알고리즘 결합을 정의합니다.

[38 페이지의 『스위트 B에 대해 IBM MQ 구성』](#)

IBM MQ는 Windows, UNIX and Linux 플랫폼에서 NSA 스위트 B 표준을 준수하여 작동하도록 구성 가능합니다.

[29 페이지의 『FIPS\(Federal Information Processing Standard\)』](#)

이 주제에서는 미국 국립 표준 기술국의 FIPS(Federal Information Processing Standard) Cryptomodule Validation Program 및 TLS 채널에서 사용할 수 있는 암호화 기술을 소개합니다.

관련 태스크

[NY TLS12_OR_HIGHER CipherSpec을 사용하도록 기존 보안 구성 마이그레이션](#)

관련 참조

[DEFINE CHANNEL](#)

[ALTER CHANNEL](#)

[채널 변경, 복사 및 작성](#)

ULW AES-GCM 암호 제한

TLS 암호화에 사용될 때 AES-GCM 암호에 부과되는 제한사항에 대한 안내서입니다. 이러한 제한사항은 IETF 및 NIST 조직에 의해 부과되며 AES-GCM 암호를 사용할 때 3개이상의^{24.5} TLS 레코드를 안전하게 전송하는 데 동일한 세션 키를 사용하지 않아야 합니다.

이러한 제한사항에 대한 자세한 정보는 [RFC 9325](#) 섹션 4.4 키 사용 한계 및 [RFC 8446](#) 섹션 5.5를 참조하십시오.

IBM MQ 는 암호화 기능을 직접 구현하지 않습니다. 대신 여러 다른 암호화 라이브러리를 사용하여 TLS 및 Advanced Message Security 기능을 제공합니다. Windows, Linux 및 AIX 운영 체제에서 IBM MQ 가 사용하는 암호화 라이브러리는 GSKit입니다. 애플리케이션의 경우 C 및 비관리 .NET 라이브러리는 암호화 기능을 위해 GSKit 를 사용합니다. GSKit 에 의한 AES-GCM 암호화 알고리즘의 구현에는 표준 그룹에 의해 지정되는 제한사항이 포함됩니다. 또한 이러한 제한사항은 기본적으로 사용 가능합니다. 이와 같이 IBM MQ TLS 통신은 AES-GCM 암호를 사용할 때 동일한 세션 키를 사용하여 3개이상의^{24.5} TLS 레코드가 전송되면 종료됩니다.

참고: 다른 암호화 라이브러리가 사용되고 이러한 라이브러리가 동일한 제한사항을 구현하지 않았기 때문에 IBM i, IBM Z 또는 IBM MQ for HPE NonStop 플랫폼 또는 Java/JMS 관리 .NET 애플리케이션에는 이 제한사항이 없습니다.

IBM MQ 채널이 동일한 세션 키를 사용하여 3개이상의^{24.5} TLS 레코드가 전송될 수 있을 정도로 오랫동안 실행 중인 상태로 남아 있는 경우 기본 암호화 라이브러리가 연결을 종료합니다. 이로 인해 채널이 종료되고 AMQ9288E 오류 메시지가 생성됩니다. 이러한 방식으로 통신이 종료된 애플리케이션은 수행 중인 IBM MQ 조각에서 MQRC_CONNECTION_BROKEN 리턴 코드를 수신합니다.

연결 종료는 통신의 양쪽 끝에서 수행할 수 있지만 암호화 기능을 위해 GSKit 를 사용하는 끝에서만 수행할 수 있습니다.

제한사항 완화를 위한 조언

이 제한사항으로 인해 종료되는 통신을 방지하거나 처리하는 방법에 대한 일부 옵션은 다음과 같습니다.

다시 연결 가능한 클라이언트 사용

연결이 실패하는 경우 자동으로 다시 연결을 시도하도록 애플리케이션을 구성할 수 있습니다. 여기에는 GCM 제한사항으로 인해 종료된 연결이 포함됩니다. 다시 연결하도록 구성된 경우, 클라이언트 애플리케이션은 임의의 실패 지점에서 자동으로 복원되고 오브젝트를 열기 위한 모든 핸들이 복원됩니다. 이는 애플리케이션 코드로 돌아가지 않고 수행됩니다.

자세한 정보는 [자동 클라이언트 다시 연결을 참조하십시오](#).

비밀 키 재설정 값 설정

IBM MQ 는 구성 가능한 바이트 수가 채널을 통해 전송된 후 세션 키 재설정을 요청하도록 구성될 수 있습니다. 이 한계에 도달하면 IBM MQ 는 암호화 계층이 세션 키 재설정을 수행하여 새 세션 키가 되도록 요청합니다.

지정된 값은 전송되는 바이트 수이며, 이는 IBM MQ에서 전송되는 메시지의 크기와 관련됩니다. 전송되는 TLS 레코드 수에 대한 제한이 있습니다. TLS 레코드는 네트워크의 최대 전송 단위 (MTU) 에 따라 최대 바이트 수를 전송할 수 있으므로 메시지 바이트와 TLS 레코드 간에 직접 매핑이 없습니다. 이 값보다 큰 전송된 메시지는 다중 TLS 레코드로 전송됩니다. MTU값은 네트워크 간에 다양합니다. 또한 IBM MQ 메시지 데이터 전송 외부에서 TLS 레코드를 전송해야 하는 다른 이유가 있습니다 (예: IBM MQ 하트비트 검사, TLS 경보, 기타 IBM MQ 프로토콜 메시지). 이러한 추가 TLS 레코드는 최대 TLS 레코드 수에 계수되지만 IBM MQ 비밀 키 재설정 값에서 계수되지 않습니다.

비밀 키 재설정을 사용하여 정기적으로 세션 키를 재설정하면 AES-GCM 제한으로 인해 채널이 종료되지 않을 수 있습니다.

자세한 정보는 [SSL 및 TLS 비밀 키 재설정을 참조하십시오](#).

V9.1.4 TLS 1.3 cipherspecs 사용

TLS 1.3 프로토콜을 사용할 때 AES-GCM 제한사항이 여전히 존재하는 반면, TLS 1.3 프로토콜은 TLS 통신을 인터럽트할 필요 없이 자동으로 세션 키 재설정을 수행하도록 지원합니다. 이를 통해 GSKit 는 IBM MQ 에서 비밀 키 재설정을 요청하지 않고도 필요한 경우 세션 키 재설정을 관리할 수 있습니다.

자세한 정보는 376 페이지의 『CipherSpec 사용 가능』의 IBM MQ 에서 TLS 1.3 사용의 내용을 참조하십시오.

AES-GCM 제한 사용 안함

필요한 경우 AES-GCM 제한을 사용하지 않도록 환경 변수

GSK_ENFORCE_GCM_RESTRICTION=GSK_FALSE 를 설정하여 제한을 사용 안함으로 설정할 수 있습니다. 이를 수행하면 동일한 세션 키를 사용하여 임의의 수의 TLS 레코드를 전송할 수 있습니다. 이 완화를 선택하는 경우 보안 통신을 위해 GSKit 를 사용하는 통신의 각 끝에 환경 변수를 설정해야 합니다.



경고: 이 옵션은 세 개 이상의^{24.5} TLS 레코드가 전송된 후에는 공격자가 전송된 레코드에 대한 분석을 수행하여 사용 중인 세션 키를 판별할 수 있으므로 권장되지 않습니다. 세션 키가 판별되면 해당 세션 키를 사용하는 모든 기존 및 향후 통신이 손상됩니다.

더 이상 사용되지 않는 CipherSpec

필요한 경우 IBM MQ와 함께 사용할 수 있는 더 이상 사용되지 않는 CipherSpec 목록입니다.

더 이상 사용되지 않는 CipherSpec을 사용으로 설정하는 것에 관한 정보는 381 페이지의 『멀티플랫폼에서 CipherSpec 사용』 또는 382 페이지의 『z/OS에서 더 이상 사용되지 않는 CipherSpec 사용』의 내용을 참조하십시오.

IBM MQ TLS 지원과 함께 사용할 수 있는 더 이상 사용되지 않는 CipherSpec은 다음 표에 나열되어 있습니다.

표 75. 더 이상 사용되지 않는 CipherSpec을 IBM MQ와 함께 다시 사용으로 설정할 수 있습니다.

플랫폼 지원 387 페이지의 『1』	CipherSpec 이름	16진 코드	사용되는 프로토콜	데이터 무결성	암호화 알고리즘 (암호화 비트)	FIPS 387 페이지의 『2』	스위트 B	더 이상 사용되지 않는 경우 업데이트
CipherSpecs for SSL 3.0								
IBM I	AES_SHA_US 387 페이지의 『3』	002F	SSL 3.0	SHA-1	AES (128)	아니오	아니오	9.0.0.0
모두	DES_SHA_EXPORT 387 페이지의 『3』 387 페이지의 『4』 387 페이지의 『5』	0009	SSL 3.0	SHA-1	DES (56)	아니오	아니오	9.0.0.0
ULW	DES_SHA_EXPORT1024 387 페이지의 『3』 387 페이지의 『6』	0062	SSL 3.0	SHA-1	DES (56)	아니오	아니오	9.0.0.0
ULW	FIPS_WITH_DES_CBC_SHA 387 페이지의 『3』	FEFE	SSL 3.0	SHA-1	DES (56)	387 페이지의 『7』 없음	아니오	9.0.0.0
ULW	FIPS_WITH_3DES_EDE_CBC_SHA 387 페이지의 『3』	FEFF	SSL 3.0	SHA-1	3DES (168)	387 페이지의 『8』 없음	아니오	9.0.0.1 및 9.0.1
모두	NULL_MD5 387 페이지의 『3』	0001	SSL 3.0	MD5	없음	아니오	아니오	9.0.0.1
모두	NULL_SHA 387 페이지의 『3』	0002	SSL 3.0	SHA-1	없음	아니오	아니오	9.0.0.1
모두	RC2_MD5_EXPORT 387 페이지의 『3』 387 페이지의 『4』 387 페이지의 『5』	0006	SSL 3.0	MD5	RC2 (40)	아니오	아니오	9.0.0.0
모두	RC4_MD5_EXPORT 387 페이지의 『4』 387 페이지의 『3』	0003	SSL 3.0	MD5	RC4 (40)	아니오	아니오	9.0.0.0
모두	RC4_MD5_US 387 페이지의 『3』	0004	SSL 3.0	MD5	RC4 (128)	아니오	아니오	9.0.0.0
모두	RC4_SHA_US 387 페이지의 『3』 387 페이지의 『5』	0005	SSL 3.0	SHA-1	RC4 (128)	아니오	아니오	9.0.0.0
ULW	RC4_56_SHA_EXPORT1024 387 페이지의 『3』 387 페이지의 『6』	0064	SSL 3.0	SHA-1	RC4 (56)	아니오	아니오	9.0.0.0
모두	TRIPLE_DES_SHA_US 387 페이지의 『3』 387 페이지의 『5』	000A	SSL 3.0	SHA-1	3DES (168)	아니오	아니오	9.0.0.1 및 9.0.1
CipherSpecs for TLS 1.0								
IBM I	TLS_RSA_EXPORT_WITH_RC2_40_MD5 387 페이지의 『3』	0006	TLS 1.0	MD5	RC2 (40)	아니오	아니오	9.0.0.0
IBM I	TLS_RSA_EXPORT_WITH_RC4_40_MD5 387 페이지의 『3』 387 페이지의 『4』	0003	TLS 1.0	MD5	RC4 (40)	아니오	아니오	9.0.0.0

표 75. 더 이상 사용되지 않는 CipherSpec을 IBM MQ와 함께 다시 사용으로 설정할 수 있습니다. (계속)


















플랫폼 지원 387 페이지의 『1』	CipherSpec 이름	16진 코드	사용되는 프로토콜	데이터 무결성	암호화 알고리즘 (암호화 비트)	FIPS 387 페이지의 『2』	스위트 B	더 이상 사용되지 않는 경우 업데이트
모두	TLS_RSA_WITH_DES_CBC_SHA 387 페이지의 『3』	0009	TLS 1.0	SHA-1	DES (56)	387 페이지의 『9』 없음	아니오	9.0.0.0
	TLS_RSA_WITH_NULL_MD5 387 페이지의 『3』	0001	TLS 1.0	MD5	없음	아니오	아니오	9.0.0.1
	TLS_RSA_WITH_NULL_SHA 387 페이지의 『3』	0002	TLS 1.0	SHA-1	없음	아니오	아니오	9.0.0.1
	TLS_RSA_WITH_RC4_128_MD5 387 페이지의 『3』	0004	TLS 1.0	MD5	RC4 (128)	아니오	아니오	9.0.0.0
 	TLS_RSA_WITH_AES_128_CBC_SHA 387 페이지의 『10』	002F	TLS 1.0	SHA-1	AES (128)	예	아니오	9.0.5
 	TLS_RSA_WITH_AES_256_CBC_SHA 387 페이지의 『6』 387 페이지의 『10』	0035	TLS 1.0	SHA-1	AES (256)	예	아니오	9.0.5
모두	TLS_RSA_WITH_3DES_EDE_CBC_SHA	000A	TLS 1.0	SHA-1	3DES (168)	예	아니오	9.0.0.1 및 9.0.1
CipherSpecs for TLS 1.2								
	ECDHE_ECDSA_NULL_SHA256 387 페이지의 『3』	C006	TLS 1.2	SHA-1	없음	아니오	아니오	9.0.0.1
	ECDHE_ECDSA_RC4_128_SHA256 387 페이지의 『3』	C007	TLS 1.2	SHA-1	RC4 (128)	아니오	아니오	9.0.0.0
 	ECDHE_RSA_NULL_SHA256 387 페이지의 『3』	C010	TLS 1.2	SHA-1	없음	아니오	아니오	9.0.0.1
 	ECDHE_RSA_RC4_128_SHA256 387 페이지의 『3』	C011	TLS 1.2	SHA-1	RC4 (128)	아니오	아니오	9.0.0.0
	TLS_RSA_WITH_NULL_NULL 387 페이지의 『3』	0000	TLS 1.2	없음	없음	아니오	아니오	9.0.0.1
모두	TLS_RSA_WITH_NULL_SHA256 387 페이지의 『3』	003B	TLS 1.2	SHA-256	없음	아니오	아니오	9.0.0.1
	TLS_RSA_WITH_RC4_128_SHA256 387 페이지의 『3』	0005	TLS 1.2	SHA-1	RC4 (128)	아니오	아니오	9.0.0.0
	ECDHE_ECDSA_3DES_EDE_CBC_SHA256	C0008	TLS 1.2	SHA-1	3DES (168)	예	아니오	9.0.0.1 및 9.0.1
 	ECDHE_RSA_3DES_EDE_CBC_SHA256	C012	TLS 1.2	SHA-1	3DES (168)	예	아니오	9.0.0.1 및 9.0.1

표 75. 더 이상 사용되지 않는 CipherSpec을 IBM MQ와 함께 다시 사용으로 설정할 수 있습니다. (계속)

플랫폼 지원 387 페이지의 『1』	CipherSpec 이름	16진 코드	사용되는 프로토콜	데이터 무결성	암호화 알고리즘 (암호화 비트)	FIPS 387 페이지의 『2』	스위트 B	더 이상 사용되지 않는 경우 업데이트
---------------------	---------------	--------	-----------	---------	-------------------	-------------------	-------	----------------------

참고:

1. 각 플랫폼 아이콘에서 다루는 플랫폼 목록은 [제품 문서의 릴리스 및 플랫폼 아이콘의 내용](#)을 참조하십시오.
2. FIPS 인증 플랫폼에서 CipherSpec이 FIPS 인증 CipherSpec인지 여부를 지정합니다. FIPS에 대한 설명은 [FIPS\(Federal Information Processing Standards\)](#)를 참조하십시오.
3. **ULW** TLS 1.3이 사용으로 설정되면([qm.ini](#)의 AllowTLSV13 특성을 통해) 이러한 CipherSpec이 사용 안함으로 설정됩니다.
z/OS IBM MQ for z/OS 9.2.0 이상에서 작성된 큐 관리자는 기본적으로 TLS 1.3 을 사용으로 설정하며, 이는 이러한 CipherSpecs를 사용 안함으로 설정합니다. 필요한 경우 TLS V1.3을 해제하여 이러한 CipherSpec을 사용으로 설정할 수 있습니다. 이는 큐 관리자 JCL에 있는 QMINI 데이터 세트의 TransportSecurity 스탠자에 **AllowTLSV13==FALSE**를 추가하여 수행됩니다. 이전 버전에서 IBM MQ for z/OS 9.2.0 으로 마이그레이션된 큐 관리자는 기본적으로 TLS 1.3 이 사용으로 설정되어 있지 않으므로 이러한 CipherSpecs 가 사용으로 설정되어 있습니다.
4. 최대 데이터 교환 키 크기는 512비트입니다. SSL 데이터 교환 중에 교환된 인증서 중 한 개의 키 크기가 512비트를 초과할 경우, 데이터 교환 중에 사용할 수 있도록 임시 512비트 키가 생성됩니다.
5. 이 CipherSpec은 IBM MQ classes for Java 또는 IBM MQ classes for JMS에서 더 이상 지원되지 않습니다. 자세한 정보는 [IBM MQ classes for Java의 SSL/TLS 암호 스펙 및 암호 스위트](#) 또는 [IBM MQ classes for JMS의 SSL/TLS 암호 스펙 및 암호 스위트](#)를 참조하십시오.
6. 데이터 교환 키 크기는 1024비트입니다.
7. 이 CipherSpec은 2007년 5월 19일 이전에 FIPS 140-2 인증되었습니다. 이름 FIPS_WITH_DES_CBC_SHA은(는) 히스토리아며 이 CipherSpec이 이전에(더 이상) FIPS를 준수하지 않는다는 사실을 반영합니다. 이 CipherSpec은 더 이상 사용되지 않으므로 앞으로는 사용하지 않는 것이 좋습니다.
8. 이름 FIPS_WITH_3DES_EDE_CBC_SHA은(는) 히스토리아며 이 CipherSpec이 이전에(더 이상) FIPS를 준수하지 않는다는 사실을 반영합니다. 이 CipherSpec은 더 이상 사용되지 않습니다.
9. 이 CipherSpec은 2007년 5월 19일 이전에 FIPS 140-2 인증되었습니다.
10. **z/OS** 이러한 CipherSpec만 다시 사용하는 경우 CSQXWEAK DD문을 사용할 필요가 없습니다.

관련 개념

40 페이지의 『[IBM MQ에서 디지털 인증서와 CipherSpec의 호환성](#)』

이 토픽은 IBM MQ에서 CipherSpec과 디지털 인증서 사이의 관계를 소개하여 보안 정책에 대해 적합한 CipherSpec 및 디지털 인증서를 선택하는 방법에 대한 정보를 제공합니다.

관련 참조

- [DEFINE CHANNEL](#)
- [ALTER CHANNEL](#)

알리어스 CipherSpec 설정 간 관계

다음 테이블은 클라이언트, 큐 관리자 또는 둘 다에서 TLS1.3 이 사용 가능하지 않은 경우 및 TLS1.3 이 클라이언트 및 큐 관리자 둘 다에서 사용 가능한 경우에 예상되는 동작을 보여줍니다.

다음 표에서는 서로 다른 알리어스 CipherSpec 설정 및 예상되는 결과 사이의 관계를 보여줍니다. 388 페이지의 표 76 는 클라이언트, 서버 또는 둘 다에서 TLS 1.3 을 사용할 수 없는 경우 예상되는 작동을 표시합니다. 388 페이지의 표 77 는 TLS 1.3 이 클라이언트와 서버 모두에서 사용 가능한 경우 예상되는 동작을 보여줍니다. 두 경우 모두 클라이언트의 CipherSpecs 가 테이블의 Y축에 표시되고 서버의 CipherSpecs 가 테이블의 X축에 표시됩니다.

참고: 항목 상태가 실패할 수 있음 상태인 경우, 이는 특정 TLS 1.3 또는 TLS 1.2 CipherSpec 이 클라이언트 및 큐 관리자에 가장 강력한 CipherSpec 이 되는 경우, TLS 핸드셰이크가 이를 사용하도록 분석되고 채널 SSCIPH 값과 일치하기 때문입니다.

표 76. 클라이언트, 서버 또는 둘 다에서 TLS 1.3 을 사용할 수 없는 경우의 예상 작동

	서버			
클라이언트	특정 TLS 1.2 CipherSpec	ANY	ANY_TLS12	ANY_TLS12_OR_HIGHER
특정 TLS 1.2 CipherSpec	연결	연결	연결	연결
모두	실패할 수 있음	연결	연결	연결
ANY_TLS12	실패할 수 있음	연결	연결	연결
ANY_TLS12_OR_HIGHER	실패할 수 있음	연결	연결	연결

표 77. TLS 1.3 이 클라이언트와 서버 모두에서 사용 가능한 경우의 예상 작동

	서버						
클라이언트	특정 TLS 1.2 CipherSpec	특정 TLS 1.3 CipherSpec	ANY	ANY_TLS12	ANY_TLS13	ANY_TLS12_OR_HIGHER	ANY_TLS13_OR_HIGHER
특정 TLS 1.2 CipherSpec	연결	실패	연결	연결	실패	연결	실패
특정 TLS 1.3 CipherSpec	실패	연결	연결	실패	연결	연결	연결
모두	실패	실패할 수 있음	연결	실패	연결	연결	연결
ANY_TLS12	실패할 수 있음	실패	연결	연결	실패	연결	실패
ANY_TLS13	실패	실패할 수 있음	연결	실패	연결	연결	연결
ANY_TLS12_OR_HIGHER	실패	실패할 수 있음	연결	실패	연결	연결	연결
ANY_TLS13_OR_HIGHER	실패	실패할 수 있음	연결	실패	연결	연결	연결

관련 개념

40 페이지의 『IBM MQ에서 디지털 인증서와 CipherSpec의 호환성』

이 토픽은 IBM MQ에서 CipherSpec과 디지털 인증서 사이의 관계를 소개하여 보안 정책에 대해 적합한 CipherSpec 및 디지털 인증서를 선택하는 방법에 대한 정보를 제공합니다.

17 페이지의 『CipherSpecs 및 CipherSuites』

암호화 보안 프로토콜은 안전 연결에서 사용되는 알고리즘에 동의해야 합니다. CipherSpec 및 CipherSuite는 특정 알고리즘 결합을 정의합니다.

376 페이지의 『CipherSpec 사용 가능』

DEFINE CHANNEL MQSC 명령 또는 **ALTER CHANNEL** MQSC 명령에서 **SSLCIPH** 매개변수를 사용하여 CipherSpec을 사용 가능으로 설정하십시오.

관련 태스크

[NY_TLS12_OR_HIGHER CipherSpec을 사용하도록 기존 보안 구성 마이그레이션](#)

IBM MQ Explorer를 사용하여 CipherSpec에 대한 정보 확보

IBM MQ Explorer를 사용하여 CipherSpec의 설명을 표시할 수 있습니다.

[376 페이지의 『CipherSpec 사용 가능』](#)에 있는 CipherSpec에 대한 정보를 확보하려면 다음 프로시저를 사용하십시오.

1. IBM MQ Explorer를 열고 **큐 관리자** 폴더를 펼치십시오.
2. 큐 관리자를 시작했는지 확인하십시오.
3. 작업하려는 큐 관리자를 선택하고 **채널**을 클릭하십시오.
4. 작업하려는 채널을 마우스 오른쪽 단추로 클릭하고 **특성**을 선택하십시오.
5. **SSL** 특성 페이지를 선택하십시오.
6. 작업하려는 CipherSpec을 목록에서 선택하십시오. 설명이 목록 아래의 창에 표시됩니다.

CipherSpec을 지정하기 위한 대안

운영 체제가 TLS 지원을 제공하는 플랫폼의 경우 시스템이 새 CipherSpec을 지원할 수도 있습니다. 새 CipherSpec을 SSLCIPH 매개변수에 지정할 수 있으나, 제공하는 값은 플랫폼에 따라 다릅니다.

참고: 이 절은 UNIX, Linux 또는 Windows 시스템에 적용되지 않습니다. CipherSpec에는 IBM MQ 제품이 지원되므로 새 CipherSpec이 운송 후에 사용 가능하게 되지 않습니다.

운영 체제가 TLS 지원을 제공하는 플랫폼에서는, [376 페이지의 『CipherSpec 사용 가능』](#)에 포함되지 않은 새 CipherSpec을 시스템이 지원할 수도 있습니다. 새 CipherSpec을 SSLCIPH 매개변수에 지정할 수 있으나, 제공하는 값은 플랫폼에 따라 다릅니다. 모든 경우에 스펙은 올바르게 시스템이 실행 중인 TLS 버전에 의해 지원되는 TLS CipherSpec에 해당해야 합니다.

IBM i

16진 값을 나타내는 2자의 문자열.

허용되는 값에 대한 자세한 정보는 [보안 세션을 위한 문자 정보 설정의 사용법 참고사항 절](#)에서 3번 항목을 참조하십시오.



주의: 16진 암호 값에서는 사용되는 암호가 명확하지 않으며, 사용되는 프로토콜의 선택이 불확실하므로 SSLCIPH에는 이러한 값을 지정하지 않아야 합니다. 16진 암호 값을 사용하면 CipherSpec 불일치 오류가 발생할 수 있습니다.

CHGMQMCHL 또는 CRTMQMCHL 명령을 사용하여 값을 지정할 수 있습니다. 예를 들어, 다음과 같습니다.

```
CRTMQMCHL CHLNAME(' channel name ') SSLCIPH(' hexadecimal value ')
```

ALTER QMGR MQSC 명령을 사용하여 **SSLCIPH** 매개변수를 설정할 수도 있습니다.

z/OS

16진 값을 나타내는 4문자의 문자열입니다. 16진 코드는 TLS 프로토콜에 정의된 값에 해당합니다.

자세한 정보는 [암호 스위트 정의](#)를 참조하십시오. 여기에는 4자리 16진 코드 양식의 지원되는 모든 TLS 1.0, TLS 1.2 및 TLS 1.3 암호 스펙의 목록이 있습니다.

IBM MQ 클러스터에 대한 고려사항

IBM MQ 클러스터를 사용하면 [376 페이지의 『CipherSpec 사용 가능』](#)에서 CipherSpec 이름을 사용하는 것이 가장 안전합니다. 대체 스펙을 사용하는 경우 스펙이 다른 플랫폼에서는 유효하지 않을 수도 있음을 유의하십시오. 자세한 정보는 [415 페이지의 『SSL/TLS 및 클러스터』](#)의 내용을 참조하십시오.

IBM MQ MQI client를 위해 CipherSpec 지정

IBM MQ MQI client를 위해 CipherSpec을 지정하기 위한 세 가지 옵션이 있습니다.

해당 옵션은 다음과 같습니다.

- 채널 정의 테이블 사용
- MQCD 구조, MQCD_VERSION_7 이상 또는 MQCONNX 호출에서 SSLCipherSpec 필드 사용.
- Active Directory를 지원하는 Windows 시스템에서 Active Directory 사용

IBM MQ classes for Java 및 IBM MQ classes for JMS를 사용하여 CipherSuite 지정

IBM MQ classes for Java 및 IBM MQ classes for JMS는 다른 플랫폼에서와 다르게 CipherSuite를 지정합니다.

IBM MQ classes for Java에서 CipherSuite 지정에 대한 정보는 [Java에 대한 TLS\(Transport Layer Security\) 지원을 참조하십시오.](#)

IBM MQ classes for JMS에서 CipherSuite 지정에 대한 정보는 [IBM MQ classes for JMS에서 TLS\(Transport Layer Security\) 사용을 참조하십시오.](#)

IBM MQ.NET용 CipherSpec 지정

IBM MQ.NET의 경우 MQEnvironment 클래스를 사용하거나 연결 특성의 해시 테이블에서 MQC.SSL_CIPHER_SPEC_PROPERTY를 사용하여 CipherSpec을 지정할 수 있습니다.

.NET 비관리 클라이언트를 위한 CipherSpec 지정에 대한 정보는 [비관리 .NET 클라이언트에 TLS 사용을 참조하십시오.](#)

.NET 관리 클라이언트를 위한 CipherSpec 지정에 대한 정보는 [관리 .NET 클라이언트에 대한 CipherSpec 지원을 참조하십시오.](#)

IBM MQ for z/OS와 함께 AT-TLS 사용

AT-TLS(Application Transparent Transport Layer Security)는 해당 애플리케이션에서 TLS 지원을 구현하거나 TLS가 사용 중임을 인식할 필요 없이 z/OS 애플리케이션에 대한 TLS 지원을 제공합니다. AT-TLS는 z/OS에서만 사용할 수 있습니다.

AT-TLS는 모든 버전의 IBM MQ for z/OS에서 사용할 수 있습니다.

IBM MQ for z/OS에서 AT-TLS를 사용하기 전에 관련된 392 페이지의 『제한』을 이해해야 합니다.

AT-TLS(Application Transparent Transport Layer Security)를 사용하려면 z/OS Communications Server에서 TLS가 투명하게 사용으로 설정된 TCP/IP 연결을 결정하는 데 사용하는 규칙 세트가 포함된 정책문을 정의합니다.

IBM MQ for z/OS에는 채널에 CipherSpec으로 구성된 SSLCIPH 매개변수가 있어야 하는 자체 TLS 구현이 있습니다.

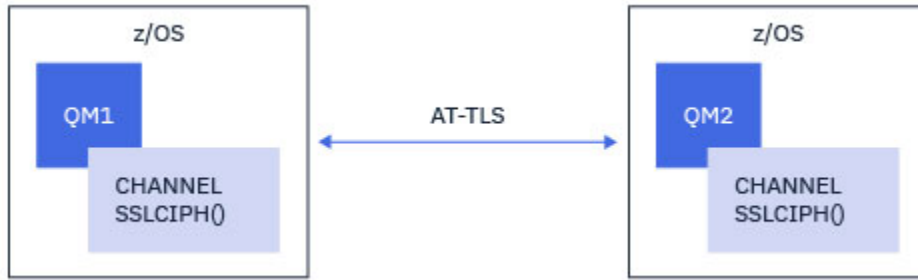
채널에서 TLS를 사용하도록 결정할 때 IBM MQ 관리자가 AT-TLS 또는 IBM MQ TLS를 사용하도록 결정할 수 있습니다. AT-TLS가 다른 미들웨어에 사용되는지 여부 또는 성능 영향으로 인해 결정되는 경우가 많습니다. AT-TLS 및 IBM MQ TLS의 성능에 대한 기본 비교는 [MP16: IBM MQ for z/OS 용량 계획 및 성능 조정을 참조하십시오.](#)

시나리오

IBM MQ에서 AT-TLS 사용은 다음 시나리오에서 지원됩니다.

시나리오 1

채널의 양쪽에서 AT-TLS를 사용하는 두 개의 IBM MQ for z/OS 큐 관리자 사이. 즉, 두 채널 모두 SSLCIPH 속성을 지정하지 않습니다. 이 접근 방식은 모든 메시지 채널에서 사용할 수 있습니다.

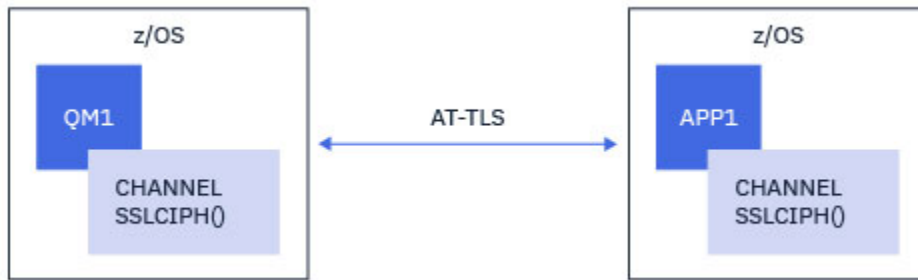


이 시나리오의 구현은 채널의 한쪽마다 하나씩, 두 개의 AT-TLS 정책을 정의하는 것으로 구성됩니다. 이러한 정책은 시나리오 3에서 사용된 정책과 동일합니다.

예를 들어, 채널이 이름 지정된 단일 CipherSpec 사용에서 AT-TLS 사용으로 변경된 경우 아웃바운드 채널은 393 페이지의 『이름 지정된 단일 CipherSpec을 사용하여 IBM MQ for Multiplatforms 큐 관리자로의 아웃바운드 채널에 AT-TLS 구성』의 정책을 사용하고 인바운드 채널은 396 페이지의 『이름 지정된 단일 CipherSpec을 사용하여 IBM MQ for Multiplatforms 큐 관리자로부터의 인바운드 채널에 AT-TLS 구성』의 정책을 사용합니다.

시나리오 2

채널의 양쪽에서 AT-TLS를 사용하는 IBM MQ for z/OS 큐 관리자와 z/OS에서 실행 중인 IBM MQ Java 클라이언트 애플리케이션 사이, 즉, 서버 연결 채널과 클라이언트 연결 채널 모두 SSLCIPH 속성을 지정하지 않습니다.

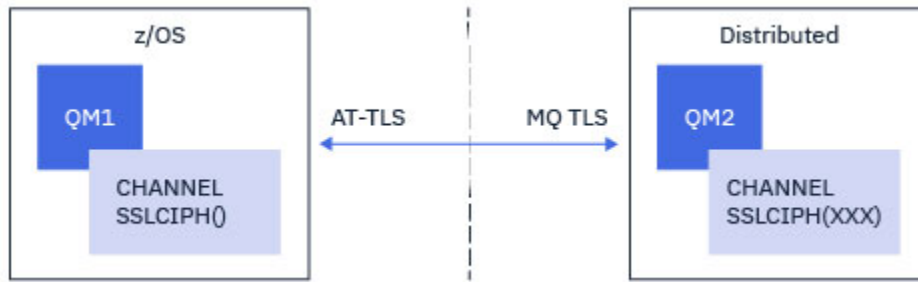


이 시나리오의 구현은 채널의 한쪽마다 하나씩, 두 개의 AT-TLS 정책을 정의하는 것으로 구성됩니다. 이러한 정책은 시나리오 3에서 사용된 정책과 동일합니다.

예를 들어, 채널이 이름 지정된 단일 CipherSpec 사용에서 AT-TLS 사용으로 변경된 경우 클라이언트 연결 채널은 393 페이지의 『이름 지정된 단일 CipherSpec을 사용하여 IBM MQ for Multiplatforms 큐 관리자로의 아웃바운드 채널에 AT-TLS 구성』의 정책을 사용하고 서버 연결 채널은 396 페이지의 『이름 지정된 단일 CipherSpec을 사용하여 IBM MQ for Multiplatforms 큐 관리자로부터의 인바운드 채널에 AT-TLS 구성』의 정책을 사용합니다.

시나리오 3

IBM MQ for z/OS 큐 관리자 및 IBM MQ for Multiplatforms에서 실행 중인 큐 관리자 사이, 여기서 IBM MQ for z/OS 큐 관리자는 AT-TLS를 사용하고 IBM MQ for Multiplatforms 큐 관리자는 IBM MQ TLS를 사용합니다. 이는 클러스터 송신자 및 클러스터 수신자 이외의 모든 메시지 채널 유형에 적용됩니다.

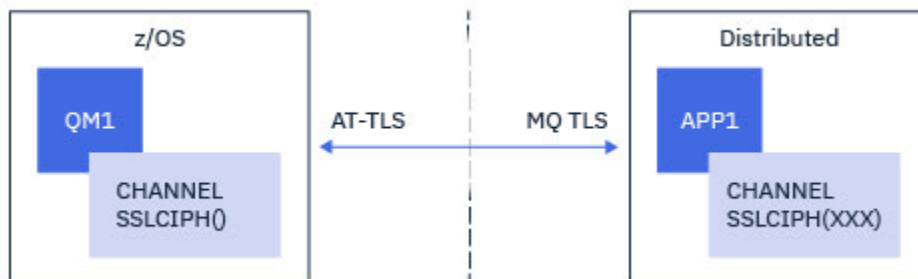


IBM MQ for z/OS 관리자에서 IBM MQ for Multiplatforms로의 아웃바운드 채널에 대한 AT-TLS 구성 예는 393 페이지의 『이름 지정된 단일 CipherSpec을 사용하여 IBM MQ for Multiplatforms 큐 관리자로의 아웃바운드 채널에 AT-TLS 구성』을 참조하고 IBM MQ for Multiplatforms 큐 관리자에서 IBM MQ for z/OS 큐 관리자로의 인바운드 연결에 대한 AT-TLS 구성 예는 396 페이지의 『이름 지정된 단일 CipherSpec을 사용하여 IBM MQ for Multiplatforms 큐 관리자로부터의 인바운드 채널에 AT-TLS 구성』을 참조하십시오.

두 큐 관리자가 모두 z/OS에 있는 경우 동일한 AT-TLS 구성을 사용할 수 있지만 오른쪽의 큐 관리자가 AT-TLS를 사용하도록 구성되지 않았습니다.

시나리오 4

IBM MQ for z/OS 큐 관리자와 IBM MQ for Multiplatforms에서 실행 중인 클라이언트 애플리케이션 사이, 여기서 IBM MQ for z/OS 큐 관리자는 AT-TLS를 사용하고 클라이언트 애플리케이션은 이름 지정된 단일 CipherSpec으로 SSLCIPH 속성을 지정하여 IBM MQ TLS를 사용합니다.



이 시나리오에는 인바운드 메시지 채널에서 사용되는 것과 동일한 요구사항을 충족하는 단일 AT-TLS 정책이 필요합니다. 396 페이지의 『이름 지정된 단일 CipherSpec을 사용하여 IBM MQ for Multiplatforms 큐 관리자로부터의 인바운드 채널에 AT-TLS 구성』을 참조하십시오.

클라이언트 애플리케이션이 Java 애플리케이션이고 z/OS에서 실행 중인 경우 동일한 AT-TLS 구성을 사용할 수 있지만 AT-TLS를 사용하도록 구성되지 않았습니다.

제한

IBM MQ for z/OS는 AT-TLS를 인식하지 않으므로 이전 시나리오에 적용되는 몇 가지 제한사항이 있습니다.

- IBM MQ TLS와 결합된 AT-TLS는 클러스터 송신자 및 클러스터 수신자 채널에서 작동하지 않습니다.
- IBM MQ for z/OS 큐 관리자는 AT-TLS를 사용 중임을 인식하지 못하고 파트너 큐 관리자 또는 클라이언트로부터 인증서 정보를 수신하지 않습니다. 따라서 다음 속성은 AT-TLS를 사용하는 채널의 z/OS 측에 영향을 미치지 않습니다.
 - SSLCAUTH 및 SSLPEER 채널 속성
 - SSLRKEYC 큐 관리자 속성
 - CHLAUTH 규칙의 SSLPEERMAP 속성

- TLS 비밀 키 재협상을 사용하려면 채널의 양쪽에서 IBM MQ TLS를 사용해야 합니다. 따라서 AT-TLS를 사용하여 IBM MQ for z/OS 큐 관리자에 연결하는 경우 IBM MQ for Multiplatforms 큐 관리자 또는 클라이언트에서 TLS 비밀 키 재협상이 사용으로 설정되지 않아야 합니다.

큐 관리자에 대한 TLS 시크릿 키 재조정을 사용하지 않으려면 큐 관리자 SSLRKEYC 매개변수를 0(으)로 설정하십시오. 클라이언트의 경우, 클라이언트 유형에 따라 관련 매개변수를 0(으)로 설정하십시오. 이를 수행하는 방법에 대한 세부사항은 400 페이지의 『SSL 및 TLS 비밀 키 재설정』을 참조하십시오.

AT-TLS 구성 명령문

AT-TLS는 명령문 세트를 사용하여 구성됩니다. 이 주제에 설명된 시나리오에서 사용되는 명령문은 다음과 같습니다.

TTLRule

TCP/IP 연결을 TLS 구성과 일치시키기 위한 기준 세트를 지정합니다. 이는 다시 다른 명령문 유형을 참조합니다.

TTLGroupAction

참조하는 TTLRule이 사용으로 설정되었는지 여부를 지정합니다.

TTLEnvironmentAction

참조하는 TTLRule에 대한 자세한 구성을 지정하고 여러 가지 다른 명령문을 참조합니다.

TTLKeyringParms

AT-TLS에서 사용할 키 링을 참조합니다.

TTLCipherParms

사용될 암호 스위트를 정의합니다.

TTLEnvironmentAdvancedParms

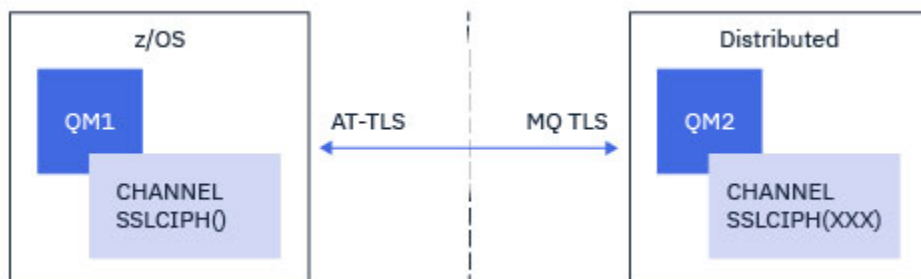
사용으로 설정된 TLS 또는 SSL 프로토콜을 정의합니다.



주의: 여기에 문서화되지 않은 AT-TLS를 사용하는 다른 AT-TLS 정책문이 있으며 필요에 따라 IBM MQ와 함께 사용할 수 있습니다. 그러나 IBM MQ는 이 주제에 설명된 정책으로만 테스트되었습니다.

이름 지정된 단일 CipherSpec을 사용하여 IBM MQ for Multiplatforms 큐 관리자로의 아웃바운드 채널에 AT-TLS 구성

IBM MQ for z/OS 큐 관리자에서 IBM MQ for Multiplatforms 큐 관리자로의 아웃바운드 채널에 AT-TLS를 설정하는 방법입니다. 이 경우 z/OS 큐 관리자의 채널은 SSLCIPH 속성이 설정되지 않은 송신자 채널이고 비z/OS 큐 관리자의 채널은 SSLCIPH 속성이 이름 지정된 단일 CipherSpec으로 설정된 수신자 채널입니다.



이 예에서 TLS 1.2 TLS_RSA_WITH_AES_256_GCM_SHA384 CipherSpec 을 사용하는 기존 송신자-수신자 채널 쌍은 송신자 채널이 IBM MQ TLS 대신 AT-TLS를 사용하도록 조정됩니다.

구성을 약간 조정하여 다른 TLS 프로토콜 및 CipherSpec을 사용할 수 있습니다. 클러스터 송신자 및 클러스터 수신자 채널 이외의 다른 메시지 채널 유형은 AT-TLS 구성을 변경하지 않고 사용할 수 있습니다.

프로시저

1단계: 채널 중지

2단계: AT-TLS 정책 작성 및 적용

이 시나리오를 위해 다음 AT-TLS문을 작성해야 합니다.

1. 채널 시작기 주소 공간에서 대상 수신자 채널의 IP 주소 및 포트 번호로의 아웃바운드 연결을 일치시키는 **TTLRule**문. 이러한 값은 송신자 채널의 CONNAME에 사용된 정보와 일치해야 합니다. 여기서는 특정 채널 시작기 작업 이름과 일치시키기 위한 추가 필터링이 포함되었습니다.

```
TTLRule                CSQ1-T0-REMOTE
{
  LocalAddr             ALL
  RemoteAddr           123.456.78.9
  RemotePortRange     1414
  Jobname              CSQ1CHIN
  Direction            OUTBOUND
  TTLGroupActionRef   CSQ1-GROUP-ACTION
  TTLEnvironmentActionRef CSQ1-OUTBOUND-ENVIRONMENT-ACTION
}
```

앞의 규칙은 CSQ1CHIN 작업에서 포트 1414의 IP 주소 123.456.78.9로 이동하는 연결과 일치합니다.

고급 필터링 옵션은 **TTLRule**에 설명되어 있습니다.

2. 규칙을 사용으로 설정하는 **TTLGroupAction**문. **TTLRule** 는 **TTLGroupActionRef** 특성을 사용하여 **TTLGroupAction** 를 참조합니다.

```
TTLGroupAction        CSQ1-GROUP-ACTION
{
  TTLEnabled          ON
}
```

3. **TTLEnvironmentActionRef** 특성에 의해 **TTLRule** 와 연관된 **TTLEnvironmentAction** 문. **TTLEnvironmentAction**은 TLS 환경을 구성하고 사용할 키 링을 지정합니다.

```
TTLEnvironmentAction  CSQ1-OUTBOUND-ENVIRONMENT-ACTION
{
  HandshakeRole       CLIENT
  TTLKeyringParmsRef  CSQ1-KEYRING
  TTLCipherParmsRef   CSQ1-CIPHERPARM
  TTLEnvironmentAdvancedParmsRef CSQ1-ENVIRONMENT-ADVANCED
}
```

4. **TTLKeyringParms** 문은 **TTLKeyringParmsRef** 특성에 의해 **TTLEnvironmentAction** 와 연관되며 AT-TLS에서 사용되는 키 링을 정의합니다.

키 링에는 원격 비즈/OS 큐 관리자가 신뢰하는 인증서가 포함되어야 합니다. 이 키 링은 채널 시작기에서 사용되는 키 링과 동일한 방식으로 정의할 수 있습니다. 228 페이지의 『TLS를 사용하도록 z/OS 시스템 구성』의 내용을 참조하십시오.

```
TTLKeyringParms       CSQ1-KEYRING
{
  Keyring             MQCHIN/CSQ1RING
}
```

5. **TTLCipherParmsRef** 특성에 의해 **TTLEnvironmentAction** 와 연관된 **TTLCipherParms** 문.

이 명령문에는 대상 수신자 채널에 사용된 IBM MQ CipherSpec 이름과 동일해야 하는 단일 암호 스위트 이름이 포함되어야 합니다.

참고: AT-TLS 암호 스위트 이름이 IBM MQ CipherSpec 이름과 반드시 일치하는 것은 아닙니다. 그러나 다음 표에서 IBM MQ CipherSpec 이름을 찾고 **TTLCipherParms** 주제의 표 2에서 확장된 문자 열이 있는 4자 코드 열을 교차 참조하여 IBM MQ CipherSpec 이름과 일치하는 AT-TLS 암호 스위트 이름을 찾을 수 있습니다.

표 78. 4자 코드에서 CipherSpec 이름으로 변환

4자 코드	프로토콜	기본적으로 사용 됨	CipherSpec 이름
0001	SSL 3.0	아니오	NULL_MD5
0002	SSL 3.0	아니오	NULL_SHA
0003	SSL 3.0	아니오	RC4_MD5_EXPORT
0004	SSL 3.0	아니오	RC4_MD5_US
0005	SSL 3.0	아니오	RC4_SHA_US
0006	SSL 3.0	아니오	RC2_MD5_EXPORT
0008	SSL 3.0	아니오	DES_SHA_EXPORT
0009	TLS 1.0	예	TLS_RSA_WITH_DES_CBC_SHA
000A	SSL 3.0	아니오	TRIPLE_DES_SHA_US
000A	TLS 1.0	예	TLS_RSA_WITH_3DES_EDE_CBC_SHA
002F	TLS 1.0	예	TLS_RSA_WITH_AES_128_CBC_SHA
0035	TLS 1.0	예	TLS_RSA_WITH_AES_256_CBC_SHA
003B	TLS 1.2	예	TLS_RSA_WITH_NULL_SHA256
003C	TLS 1.2	예	TLS_RSA_WITH_AES_128_CBC_SHA256
003D	TLS 1.2	예	TLS_RSA_WITH_AES_256_CBC_SHA256
C023	TLS 1.2	예	ECDHE_ECDSA_AES_128_CBC_SHA256
C024	TLS 1.2	예	ECDHE_ECDSA_AES_256_CBC_SHA384
C027	TLS 1.2	예	ECDHE_RSA_AES_128_CBC_SHA256
C028	TLS 1.2	예	ECDHE_RSA_AES_256_CBC_SHA384

```
TTLSCipherParms CSQ1-CIPHERPARM
{
  V3CipherSuites TLS_RSA_WITH_AES_256_GCM_SHA384
}
```

6. **TTLSEnvironmentAdvancedParms** 문은 **TTLSEnvironmentAdvancedParmsRef** 특성에 의해 **TTLSEnvironmentAction** 와 연관됩니다.

이 명령문을 사용하여 사용 가능한 SSL 및 TLS 프로토콜을 지정할 수 있습니다. IBM MQ 를 사용하면 **TTLSCipherParms** 문에서 사용되는 암호 스위트 이름과 일치하는 단일 프로토콜만 사용해야 합니다.

```
TTLSEnvironmentAdvancedParms CSQ1-ENVIRONMENT-ADVANCED
{
  SSLv3 OFF
  TLSv1 OFF
  TLSv1.1 OFF
  SecondaryMap OFF
  TLSv1.2 ON
  TLSv1.3 OFF
}
```

전체 명령문 세트는 다음과 같으며 정책 에이전트에 적용되어야 합니다.

```

TTLRule CSQ1-T0-REMOTE
{
  LocalAddr ALL
  RemoteAddr 123.456.78.9
  RemotePortRange 1414
  Jobname CSQ1CHIN
  Direction OUTBOUND
  TLSGroupActionRef CSQ1-GROUP-ACTION
  TLSEnvironmentActionRef CSQ1-OUTBOUND-ENVIRONMENT-ACTION
}

TLSGroupAction CSQ1-GROUP-ACTION
{
  TLSEnabled ON
}

TLSEnvironmentAction CSQ1-OUTBOUND-ENVIRONMENT-ACTION
{
  HandshakeRole CLIENT
  TLSKeyringParmsRef CSQ1-KEYRING
  TLSCipherParmsRef CSQ1-CIPHERPARM
  TLSEnvironmentAdvancedParmsRef CSQ1-ENVIRONMENT-ADVANCED
}

TLSKeyringParms CSQ1-KEYRING
{
  Keyring MQCHIN/CSQ1RING
}

TLSCipherParms CSQ1-CIPHERPARM
{
  V3CipherSuites TLS_RSA_WITH_AES_256_GCM_SHA384
}

TLSEnvironmentAdvancedParms CSQ1-ENVIRONMENT-ADVANCED
{
  SSLv3 OFF
  TLSv1 OFF
  TLSv1.1 OFF
  SecondaryMap OFF
  TLSv1.2 ON
  TLSv1.3 OFF
}

```

단계 3: z/OS 채널에서 SSLCIPH 제거

다음 명령을 사용하여 z/OS 채널에서 CipherSpec 을 제거하십시오.

```
ALTER CHANNEL(channel-name) CHLTYPE(SDR) SSLCIPH(' ')
```

4단계: 채널 시작

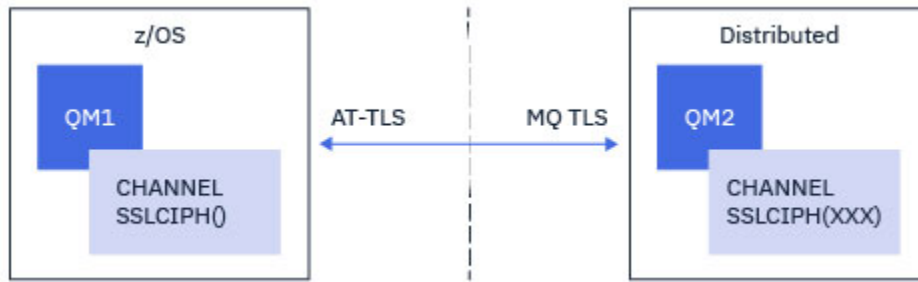
채널이 시작되면 AT-TLS와 IBM MQ TLS의 조합을 사용하게 됩니다.



주의: 앞의 AT-TLS 명령문은 최소 구성일 뿐입니다. 여기에 문서화되지 않은 AT-TLS를 사용하는 다른 AT-TLS 정책문이 있으며 필요에 따라 IBM MQ와 함께 사용할 수 있습니다. 그러나 IBM MQ 는 설명된 정책으로만 테스트되었습니다.

이름 지정된 단일 CipherSpec을 사용하여 IBM MQ for Multiplatforms 큐 관리자로부터의 인바운드 채널에 AT-TLS 구성

IBM MQ for Multiplatforms 큐 관리자에서 IBM MQ for z/OS 큐 관리자로의 인바운드 채널에 AT-TLS를 설정하는 방법입니다. 이 경우 z/OS 큐 관리자의 채널은 SSLCIPH 속성이 설정되지 않은 수신자 채널이고 비z/OS 큐 관리자의 채널은 SSLCIPH 속성이 이름 지정된 단일 CipherSpec으로 설정된 송신자 채널입니다.



이 예에서 TLS 1.2 TLS_RSA_WITH_AES_256_GCM_SHA384 CipherSpec 를 사용하는 기존 송신자-수신자 채널 쌍은 수신자 채널이 IBM MQ TLS 대신 AT-TLS를 사용하도록 조정됩니다.

구성을 약간 조정하여 다른 TLS 프로토콜 및 CipherSpec을 사용할 수 있습니다. 클러스터 송신자 및 클러스터 수신자 채널 이외의 다른 메시지 채널 유형은 AT-TLS 구성을 변경하지 않고 사용할 수 있습니다.

프로시저

1단계: 채널 중지

2단계: AT-TLS 정책 작성 및 적용

이 시나리오를 위해 다음 AT-TLS문을 작성해야 합니다.

1. 송신자 채널의 IP 주소에서 채널 시작기 주소 공간으로의 인바운드 연결을 일치시키는 **TTLRule**문. 여기서는 특정 채널 시작기 작업 이름과 일치시키기 위한 추가 필터링이 포함되었습니다.

```
TTLRule REMOTE-T0-CSQ1
{
  LocalAddr ALL
  LocalPortRange 1414
  RemoteAddr 123.456.78.9
  Jobname CSQ1CHIN
  Direction INBOUND
  TTLGroupActionRef CSQ1-GROUP-ACTION
  TTLEnvironmentActionRef CSQ1-INBOUND-ENVIRONMENT-ACTION
}
```

앞의 규칙은 원격 IP 주소 123.456.78.9에서 로컬 포트 1414의 CSQ1CHIN 작업으로 들어오는 연결과 일치합니다.

고급 필터링 옵션은 **TTLRule**에 설명되어 있습니다.

2. 규칙을 사용으로 설정하는 **TTLGroupAction**문. **TTLRule** 는 **TTLGroupActionRef** 특성을 사용하여 **TTLGroupAction** 를 참조합니다.

```
TTLGroupAction CSQ1-GROUP-ACTION
{
  TTLEnabled ON
}
```

3. **TTLEnvironmentAction** 문은 **TTLEnvironmentActionRef** 특성에 의해 **TTLRule** 와 연관됩니다. **TTLEnvironmentAction**은 TLS 환경을 구성하고 사용할 키 링을 지정합니다.

```
TTLEnvironmentAction CSQ1-INBOUND-ENVIRONMENT-ACTION
{
  HandshakeRole SERVER
  TLSKeyringParmsRef CSQ1-KEYRING
  TTLCipherParmsRef CSQ1-CIPHERPARM
  TTLEnvironmentAdvancedParmsRef CSQ1-ENVIRONMENT-ADVANCED
}
```

AT-TLS는 SSLCAUTH 채널 속성을 사용하는 것과 동일한 상호 인증을 제공하는 기능을 제공합니다. 이는 인바운드 TTLSEnvironmentAction 문에 대해 **HandshakeRole** 값이 *ServerWithClientAuth* 인 TTLSEnvironmentAction 문을 사용하여 수행됩니다.

4. **TTLSKeyringParms** 문은 **TTLSKeyringParmsRef** 특성에 의해 TTLSEnvironmentAction 와 연관되며 AT-TLS에서 사용되는 키 링을 정의합니다.

키 링에는 원격 비z/OS 큐 관리자가 신뢰하는 인증서가 포함되어야 합니다. 이 키 링은 채널 시작기에서 사용되는 키 링과 동일한 방식으로 정의할 수 있습니다. 228 페이지의 『TLS을 사용하도록 z/OS 시스템 구성』의 내용을 참조하십시오.

```
TTLSKeyringParms          CSQ1-KEYRING
{
  Keyring                  MQCHIN/CSQ1RING
}
```

5. **TTLSCipherParmsRef** 특성에 의해 TTLSEnvironmentAction 와 연관된 **TTLSCipherParms** 문.

이 명령문에는 원격 송신자 채널에 사용된 IBM MQ CipherSpec 이름과 동일해야 하는 단일 암호 스위트 이름이 포함되어야 합니다.

참고: AT-TLS 암호 스위트 이름이 IBM MQ CipherSpec 이름과 반드시 일치하는 것은 아닙니다. 그러나 다음 표에서 IBM MQ CipherSpec 이름을 찾고 **TTLSCipherParms** 주제의 표 2에서 확장된 문자 열이 있는 4자 코드 열을 교차 참조하여 IBM MQ CipherSpec 이름과 일치하는 AT-TLS 암호 스위트 이름을 찾을 수 있습니다.

표 79. 4자 코드에서 *CipherSpec* 이름으로 변환

4자 코드	프로토콜	기본적으로 사용됨	CipherSpec 이름
0001	SSL 3.0	아니오	NULL_MD5
0002	SSL 3.0	아니오	NULL_SHA
0003	SSL 3.0	아니오	RC4_MD5_EXPORT
0004	SSL 3.0	아니오	RC4_MD5_US
0005	SSL 3.0	아니오	RC4_SHA_US
0006	SSL 3.0	아니오	RC2_MD5_EXPORT
0008	SSL 3.0	아니오	DES_SHA_EXPORT
0009	TLS 1.0	예	TLS_RSA_WITH_DES_CBC_SHA
000A	SSL 3.0	아니오	TRIPLE_DES_SHA_US
000A	TLS 1.0	예	TLS_RSA_WITH_3DES_EDE_CBC_SHA
002F	TLS 1.0	예	TLS_RSA_WITH_AES_128_CBC_SHA
0035	TLS 1.0	예	TLS_RSA_WITH_AES_256_CBC_SHA
003B	TLS 1.2	예	TLS_RSA_WITH_NULL_SHA256
003C	TLS 1.2	예	TLS_RSA_WITH_AES_128_CBC_SHA256
003D	TLS 1.2	예	TLS_RSA_WITH_AES_256_CBC_SHA256
C023	TLS 1.2	예	ECDHE_ECDSA_AES_128_CBC_SHA256
C024	TLS 1.2	예	ECDHE_ECDSA_AES_256_CBC_SHA384
C027	TLS 1.2	예	ECDHE_RSA_AES_128_CBC_SHA256
C028	TLS 1.2	예	ECDHE_RSA_AES_256_CBC_SHA384

```
TTLSCipherParms          CSQ1-CIPHERPARM
{
  V3CipherSuites         TLS_RSA_WITH_AES_256_GCM_SHA384
}
```

6. [TTLSEnvironmentAdvancedParms](#) 문은 **TTLSEnvironmentAdvancedParmsRef** 특성에 의해 [TTLSEnvironmentAction](#) 와 연관됩니다.

이 명령문을 사용하여 사용 가능한 SSL 및 TLS 프로토콜을 지정할 수 있습니다. IBM MQ 를 사용하면 [TTLSCipherParms](#) 문에서 사용되는 암호 스위트 이름과 일치하는 단일 프로토콜만 사용해야 합니다.

```
TTLSEnvironmentAdvancedParms CSQ1-ENVIRONMENT-ADVANCED
{
  SSLv3          OFF
  TLSv1          OFF
  TLSv1.1        OFF
  SecondaryMap   OFF
  TLSv1.2        ON
  TLSv1.3        OFF
}
```

전체 명령문 세트는 다음과 같으며 정책 에이전트에 적용되어야 합니다.

```
TTLSSRule                REMOTE-T0-CSQ1
{
  LocalAddr              ALL
  LocalPortRange         1414
  RemoteAddr              123.456.78.9
  Jobname                 CSQ1CHIN
  Direction               INBOUND
  TTLSSGroupActionRef     CSQ1-GROUP-ACTION
  TTLSEnvironmentActionRef CSQ1-INBOUND-ENVIRONMENT-ACTION
}

TTLSSGroupAction         CSQ1-GROUP-ACTION
{
  TTLS-enabled           ON
}

TTLSEnvironmentAction    CSQ1-INBOUND-ENVIRONMENT-ACTION
{
  HandshakeRole          CLIENT
  TTLSKeyringParmsRef    CSQ1-KEYRING
  TTLSCipherParmsRef     CSQ1-CIPHERPARM
  TTLSEnvironmentAdvancedParmsRef CSQ1-ENVIRONMENT-ADVANCED
}

TTLSSKeyringParms        CSQ1-KEYRING
{
  Keyring                 MQCHIN/CSQ1RING
}

TTLSCipherParms          CSQ1-CIPHERPARM
{
  V3CipherSuites         TLS_RSA_WITH_AES_256_GCM_SHA384
}

TTLSEnvironmentAdvancedParms CSQ1-ENVIRONMENT-ADVANCED
{
  SSLv3          OFF
  TLSv1          OFF
  TLSv1.1        OFF
  SecondaryMap   OFF
  TLSv1.2        OFF
  TLSv1.3        ON
}
```

단계 3: z/OS 채널에서 SSLCIPH 제거

다음 명령을 사용하여 z/OS 채널에서 CipherSpec 을 제거하십시오.

```
ALTER CHANNEL(channel-name) CHLTYPE(RCVR) SSLCIPH(' ')
```

4단계: 채널 시작

채널이 시작되면 AT-TLS와 IBM MQ TLS의 조합을 사용하게 됩니다.



주의: 앞의 AT-TLS 명령문은 최소 구성일 뿐입니다. 여기에 문서화되지 않은 AT-TLS를 사용하는 다른 AT-TLS 정책문이 있으며 필요에 따라 IBM MQ와 함께 사용할 수 있습니다. 그러나 IBM MQ 는 설명된 정책으로만 테스트되었습니다.

SSL 및 TLS 비밀 키 재설정

IBM MQ는 큐 관리자 및 클라이언트에서 보안 키의 재설정을 지원합니다.

보안 키는 암호화되지 않은 데이터 바이트의 지정된 수가 채널을 통해 흐를 때 재설정됩니다. 채널 하트비트가 사용 가능하면 채널 하트비트 후에 데이터를 송신하거나 수신하기 전에 보안 키가 재설정됩니다.

이 키 재설정 값은 항상 IBM MQ 채널의 한쪽을 시작하여 설정됩니다.

큐 관리자

큐 관리자의 경우 **ALTER QMGR** 명령을 **SSLRKEYC** 매개변수와 함께 사용하여 키 재협상 동안에 사용된 값을 설정합니다.

 IBM i에서 **CHGMQM**을 **SSLRSTCNT** 매개변수와 함께 사용하십시오.

MQI 클라이언트

기본적으로 MQI 클라이언트는 보안 키를 재협상하지 않습니다. 세 가지 방법 중 하나를 사용하여 MQI 클라이언트가 키를 재협상하게 만들 수 있습니다. 다음 목록에서 방법은 우선순위의 순서대로 표시됩니다. 여러 값을 지정하는 경우에는 우선순위가 가장 높은 값이 사용됩니다.

1. MQCONNX 호출에서 MQSCO 구조에서 KeyResetCount 필드를 사용하여
2. 환경 변수 MQSSLRESET를 사용하여
3. MQI 클라이언트 구성 파일에 SSLKeyResetCount 속성을 설정하여

이 변수는 0에서 999 999 999까지의 정수로 설정할 수 있으며 이 숫자는 TLS 보안 키가 재조정되기 전에 TLS 대화 내에서 송신 및 수신된 암호화되지 않은 바이트 수를 나타냅니다. 0 값을 지정하면 TLS 보안 키가 재조정되지 않음을 나타냅니다. TLS 비밀 키 재설정 계수를 1B - 32KB 범위로 지정하는 경우 TLS 채널은 32KB의 비밀 키 재설정 계수를 사용합니다. 이는 작은 TLS 보안 키 재설정 값으로 인해 발생할 수 있는 지나친 키 재설정을 피하기 위한 것입니다.

0보다 큰 값이 지정되고 채널 하트비트가 채널에 사용되는 경우 보안 키는 메시지 데이터가 채널 하트비트 후에 송신 또는 수신되기 전에도 재설정됩니다.

각각의 재조정이 이루어지면 다음 비밀 키 재조정까지의 바이트 수가 재설정됩니다.

MQSCO 구조에 대한 전체 세부사항은 [KeyResetCount\(MQLONG\)](#)를 참조하십시오. MQSSLRESET의 전체 세부사항은 [MQSSLRESET](#)의 내용을 참조하십시오. 클라이언트 구성 파일에서 TLS 사용에 대한 자세한 정보는 [클라이언트 구성 파일의 SSL 스탠자를 참조하십시오](#).

Java

IBM MQ classes for Java의 경우 애플리케이션은 다음 방법으로 보안 키를 재설정할 수 있습니다.

- MQEnvironment 클래스에 sslResetCount 필드 설정
- 해시 테이블 오브젝트에 환경 특성 MQC.SSL_RESET_COUNT_PROPERTY 설정. 그러면 애플리케이션이 해시 테이블을 MQEnvironment 클래스의 properties 필드에 지정하거나 해시 테이블을 해당 구성자의 MQQueueManager 오브젝트로 전달합니다.

애플리케이션이 이러한 방법 중 하나 이상을 사용하는 경우 일반 서열 규칙이 적용됩니다. 서열 규칙에 대해서는 클래스 `com.ibm.mq.MQEnvironment`를 참조하십시오.

`sslResetCount` 필드 또는 환경 변수 `MQC.SSL_RESET_COUNT_PROPERTY`의 값은 비밀 키를 협상하기 전에 IBM MQ classes for Java 클라이언트 코드가 송신하고 수신한 총 바이트 수를 나타냅니다. 송신된 바이트 수는 암호화 전의 바이트 수이며, 수신된 바이트 수는 복호화 후의 바이트 수입니다. 바이트 수에는 IBM MQ classes for Java 클라이언트가 송신하고 수신한 제어 정보도 포함됩니다.

재설정 수가 기본값인 0인 경우 비밀 키는 재협상되지 않습니다. CipherSuite가 지정되지 않으면 재설정 수가 무시됩니다.

JMS

IBM MQ classes for JMS의 경우 SSLRESETCOUNT 특성은 암호화에 사용된 보안 키가 재협상되기 전에 연결에 의해 전송 및 수신된 총 바이트 수를 나타냅니다. 송신된 바이트 수는 암호화 전의 바이트 수이며, 수신된 바이트 수는 복호화 후의 바이트 수입니다. 바이트 수에는 IBM MQ classes for JMS에 의해 송신되거나 수신된 제어 정보도 포함됩니다. 예를 들어, 4MB 데이터가 플로우된 후 재조정되는 비밀 키가 포함된 SSL 또는 TLS 사용 MQI 채널을 통한 연결을 작성하는 데 사용될 수 있는 ConnectionFactory 오브젝트를 구성하려면 JMSAdmin에 다음 명령을 실행하십시오.

```
ALTER CF(my.cf) SSLRESETCOUNT(4194304)
```

SSLRESETCOUNT 값이 기본값인 0인 경우 비밀 키가 재협상되지 않습니다. SSLCIPHERSUITE를 설정하지 않으면 SSLRESETCOUNT 특성이 무시됩니다.

.NET

.NET 비관리 클라이언트의 경우 정수 특성 `SSLKeyResetCount`는 보안 키가 재협상되기 전에 TLS 대화 내에서 전송 및 수신된 암호화되지 않은 바이트의 수를 나타냅니다.

IBM MQ classes for .NET에서 오브젝트 특성의 사용에 대한 자세한 정보는 [속성 값 가져오기 및 설정을 참조하십시오](#).

.NET 관리 클라이언트의 경우, `SSLStream` 클래스가 비밀 키 재설정/재협상을 지원하지 않습니다. 그러나 기타 IBM MQ 클라이언트와의 일관성을 유지하기 위해 IBM MQ 관리 대상 .NET 클라이언트는 애플리케이션이 `SSLKeyResetCount`를 설정하도록 허용합니다. 자세한 정보는 [비밀 키 재설정 또는 재협상을 참조하십시오](#).

XMS .NET

XMS .NET 비관리 클라이언트의 경우 [IBM MQ 큐 관리자에 대한 보안 연결을 참조하십시오](#).

관련 참조

[ALTER QMGR](#)

[DISPLAY QMGR](#)

[메시지 큐 관리자 변경\(CHGMQM\)](#)

[메시지 큐 관리자 표시\(DSPMQM\)](#)

사용자 엑시트 프로그램에서 기밀성 구현

보안 엑시트에서 기밀성 구현

보안 엑시트가 채널에서 플로우되는 데이터를 암호화하고 해독하기 위해 대칭 키를 생성하고 분배하여 기밀성 서비스에서 역할을 할 수 있습니다. 이것을 수행하는 공통적인 기술은 PKI 기법을 사용합니다.

한 보안 엑시트가 무작위 데이터 값을 생성하고, 파트너 보안 엑시트가 나타내고 있는 큐 관리자나 사용자의 공개 키로 그것을 암호화하며, 암호화된 데이터를 보안 메시지로 그 파트너에게 송신합니다. 파트너 보안 엑시트가 그것이 나타내고 있는 큐 관리자나 사용자의 개인 키로 무작위 데이터 값을 해독합니다. 각 보안 엑시트가 이제 그들 모두에게 알려져 있는 알고리즘을 사용하여 다른 엑시트와 독립적으로 대칭 키를 도출하는 데 무작위 데이터 값을 사용할 수 있습니다. 또는 무작위 데이터 값을 키로 사용할 수도 있습니다.

첫 번째 보안 엑시트가 이 때에 그 파트너를 인증하지 않으면, 파트너에 의해 송신되는 다음 보안 메시지가 대칭 키로 암호화된 예상 값을 가질 수 있습니다. 첫 번째 보안 엑시트가 이제 파트너 보안 엑시트가 예상한 값을 제대로 암호화할 수 있었는지를 검사하여 그 파트너를 인증할 수 있습니다.

둘 이상의 알고리즘이 사용 가능한 경우, 이 기회를 사용하여 보안 엑시트가 채널에서 플로우되는 데이터를 암호화하고 암호를 해독하기 위한 알고리즘에 동의할 수 있습니다.

메시지 엑시트에서 기밀성 구현

채널의 송신 측에 있는 메시지 엑시트가 메시지에 있는 응용프로그램 데이터를 암호화하고 채널의 수신 측에 있는 다른 메시지 엑시트가 데이터를 해독할 수 있습니다. 성능을 이유로 보통 대칭 키 알고리즘이 이 목적으로 사용됩니다. 대칭 키가 생성되고 분배될 수 있는 방법에 대한 자세한 정보는 [401 페이지의 『사용자 엑시트 프로그램에서 기밀성 구현』](#)의 내용을 참조하십시오.

임베드된 메시지 설명자를 포함하는 트랜스미션 큐 헤더인 MQXQH 등의 메시지 헤더는 메시지 엑시트에 의해 암호화되지는 않습니다. 이것은 메시지 엑시트가 송신 측에 의해 호출된 후, 또는 메시지 엑시트가 수신 측에 의해 호출되기 전에 메시지 헤더의 데이터 변환이 일어나기 때문입니다. 헤더가 암호화되면, 데이터 변환이 실패하고 채널이 중지됩니다.

송신 및 수신 엑시트에서 기밀성 구현

송신과 수신 엑시트는 채널에서 플로우되는 데이터를 암호화하고 해독하는 데 사용될 수 있습니다. 다음과 같은 이유로 인해 이 서비스를 제공하기 위해서는 메시지 엑시트보다 이들이 더 적합합니다.

- 메시지 채널에서는 메시지의 응용프로그램 데이터뿐만 아니라 메시지 헤더도 암호화될 수 있습니다.
- 송신과 수신 엑시트는 메시지 채널뿐만 아니라 MQI 채널에서도 사용될 수 있습니다. MQI 호출의 매개변수들에는 MQI 채널에서 플로우되는 동안에 보호되어야 하는 민감한 응용프로그램 데이터가 있을 수 있습니다. 그러므로 두 종류의 채널 모두에서 동일한 송신 및 수신 엑시트를 사용할 수 있습니다.

API 엑시트 및 API 교차 엑시트에서 기밀성 구현

메시지의 애플리케이션 데이터는 메시지가 송신 애플리케이션에 의해 놓일 때 API 또는 API 교차 엑시트에 의해 암호화될 수 있고 메시지가 수신 애플리케이션에 의해 검색될 때 두 번째 엑시트에 의해 복호화될 수 있습니다. 성능을 이유로 보통 대칭 키 알고리즘이 이 목적으로 사용됩니다. 그러나, 애플리케이션 레벨에서는 많은 사용자가 서로 메시지를 송신할 수도 있는 상황에서, 문제는 의도된 메시지 수신자만이 메시지의 암호를 해독할 수 있게 보장하는 방법입니다. 한 가지 솔루션은 메시지를 서로 송신하는 사용자의 각 쌍에 다른 대칭 키를 사용하는 것입니다. 그러나, 이 솔루션은 관리하기에 어렵고 시간이 많이 소요될 수 있습니다. 특히, 사용자가 다른 조직에 속하는 경우가 그렇습니다. 이 문제점을 해결하는 표준 방법은 디지털 봉합으로 알려져 있으며 PKI 기술을 사용합니다.

애플리케이션이 메시지를 큐에 넣을 때 API 또는 API 교차 엑시트는 임의의 대칭 키를 생성하고 메시지에서 애플리케이션 데이터를 암호화하기 위해 키를 사용합니다. 엑시트는 대칭 키를 의도한 수신자의 공개 키로 암호화합니다. 그런 후, 메시지의 애플리케이션 데이터를 암호화된 애플리케이션 데이터와 암호화된 대칭 키로 바꿉니다. 이런 식으로, 의도된 수신자만이 대칭 키, 즉 애플리케이션 데이터의 암호를 해독할 수 있습니다. 암호화된 메시지에 둘 이상의 의도된 수신자가 있는 경우 엑시트는 각 의도한 수신자의 대칭 키의 사본을 암호화할 수 있습니다.

애플리케이션 데이터를 암호화하고 복호화하기 위한 서로 다른 알고리즘을 사용할 수 있는 경우 엑시트에는 사용된 알고리즘의 이름을 포함할 수 있습니다.

z/OS V 9.1.4 데이터 세트 암호화를 사용한 IBM MQ for z/OS의 저장 데이터 기밀성

IBM MQ for z/OS에서는 데이터를 활성 로그 데이터 세트, 아카이브 로그 데이터 세트, 페이지 세트, 부트스트랩 데이터 세트 및 **V 9.1.5** 공유 메시지 데이터 세트(SMDS)에 기록하여 고객 및 구성 데이터를 디스크에 기록합니다.

z/OS는 데이터 세트에 대한 효율적인 정책 기반 암호화를 제공합니다. IBM MQ for z/OS는 다음 항목에 대해 z/OS 데이터 세트 암호화를 지원합니다.

- 활성 로그 데이터 세트의 경우 참고 403 페이지의 『1』의 내용을 참조하십시오.
- 아카이브 로그 데이터 세트의 경우 참고 403 페이지의 『2』의 내용을 참조하십시오.
- 페이지 세트의 경우 참고 403 페이지의 『1』의 내용을 참조하십시오.
- BSDS의 경우 참고 403 페이지의 『2』의 내용을 참조하십시오.
- CSQINP* 데이터 세트의 경우 참고 403 페이지의 『2』의 내용을 참조하십시오.
- **V 9.1.5** SMDS의 경우 참고 403 페이지의 『3』의 내용을 참조하십시오.

이는 개별 z/OS 큐 관리자의 저장 데이터에 대한 기밀성을 제공합니다.

참고사항:

1. IBM MQ 9.1.4부터는 IBM MQ for z/OS에서 활성 로그 및 페이지 세트에 대한 z/OS 데이터 세트 암호화를 지원합니다.
2. 아카이브 로그, BSDS 및 CSQINP* 데이터 세트에 대한 데이터 세트 암호화는 모든 IBM MQ for z/OS 버전에서 지원됩니다.
3. **V 9.1.5** IBM MQ 9.1.5부터는 IBM MQ for z/OS에서 SMDS에 대한 z/OS 데이터 세트 암호화를 지원합니다.
4. IBM MQ Advanced Message Security는 저장 데이터를 보호하는 다른 메커니즘을 제공합니다. AMS 또한 메모리에 저장된 데이터 및 전송 중인 데이터를 보호합니다.

z/OS 데이터 세트 암호화에 대한 자세한 정보는 [z/OS 데이터 세트 암호화 개선사항 사용](#)을 참조하십시오.

z/OS 데이터 세트 암호화의 구성은 IBM MQ for z/OS 제어 하에 수행되는 작업이 아닙니다. 암호화 설정은 데이터 세트가 작성될 때 적용됩니다.

이는 새 데이터 세트 암호화 정책을 사용하려면 먼저 기존의 모든 데이터 세트를 다시 작성해야 함을 의미합니다.

IBM MQ for z/OS는 암호화된 데이터 세트와 암호화되지 않은 데이터 세트가 혼합된 경우에도 실행될 수 있으나, 표준 구성은 사용되는 데이터 세트를 모두 암호화하거나 전혀 암호화하지 않습니다.

z/OS V 9.1.4 IBM MQ for z/OS 데이터 세트 암호화 단계의 개요

IBM MQ for z/OS 데이터 세트를 암호화하는 방법에 대해 설명합니다.

시작하기 전에

엔터프라이즈에서 z/OS 데이터 세트 암호화를 올바르게 구성했는지 확인해야 합니다. 큐 공유 그룹에서의 데이터 세트 암호화를 설정하는 경우에는 데이터 공유에 대해 z/OS 데이터 세트 암호화를 구성해야 합니다.

참고: z/OS 암호화된 데이터 세트는 확장된 형식의 데이터 세트여야 합니다.

프로시저

1. RACF에서 데이터 세트를 암호화하는 데 사용할 암호화 키 및 key-label을 설정하십시오.
2. key-label에 대한 프로파일을 RACF CSFKEYS 클래스로 작성하십시오.
3. 큐 관리자의 사용자 ID, 그리고 암호화된 않은 데이터에 액세스해야 하는 다른 모든 사용자 ID에 READ 액세스 권한을 부여하십시오.
여기에는 데이터 세트에 대해 인쇄 유틸리티를 실행하는 데 사용되는 사용자 ID가 포함될 수 있습니다. 예를 들어, CSQUTIL SCOPY를 실행하는 사용자는 관련 페이지 세트를 복호화해야 합니다.
4. 암호화 key-label을 데이터 세트 이름과 연관시키십시오.
데이터 세트 이름 또는 상위 레벨 규정자에 대해 SMS 데이터 클래스 또는 RACF DFP 세그먼트를 사용하여 이를 수행할 수 있습니다.
데이터 세트가 할당되는 경우에도 key-label을 데이터 세트와 연관시킬 수 있습니다.
5. IDCAMS ALTER를 사용하여 기존 데이터 세트의 이름을 바꾸십시오.
6. 적절한 속성을 사용하여 데이터 세트를 재할당하십시오.
7. IDCAMS REPRO를 사용하여 이름을 바꾼 데이터 세트의 콘텐츠를 새 데이터 세트에 복사하십시오.

데이터는 데이터를 데이터 세트에 복사하는 조치에 의해 암호화됩니다.

8. 암호화되어야 하는 다른 모든 데이터 세트에 대해 403 페이지의 『4』 - 403 페이지의 『6』 단계를 반복하십시오.

z/OS V 9.1.4 큐 관리자 활성화 로그 암호화 방법 예

다음 주제에서는 기존 활성화 로그에서 데이터 세트 암호화를 사용하는 프로세스 전체를 안내합니다.

참고: 다른 데이터 세트에 대한 프로세스는 활성화 로그에 대한 프로세스와 비슷합니다.

이 예제에서

- 큐 관리자 CSQ1은 사용자 QMCSQ1에 의해 실행되며, 활성화 데이터 로그 세트 CSQ1.LOGS.LOGCOPY1.DS001, CSQ1.LOGS.LOGCOPY1.DS002, ...를 보유하고 있습니다.
- z/OS 데이터 세트 암호화를 사용할 수 있는 하드웨어 및 소프트웨어 환경입니다.
- RACF가 SAF로 사용됩니다.
- 큐 관리자가 중지되었습니다.

다음 순서대로 프로시저를 수행하십시오.

1. 404 페이지의 『큐 관리자에 대한 데이터 세트 암호화 키 구성』
2. 404 페이지의 『로그 데이터 세트에 대한 데이터 세트 암호화 구성』

z/OS V 9.1.4 큐 관리자에 대한 데이터 세트 암호화 키 구성

큐 관리자에 대한 데이터 세트 암호화 키를 구성하는 방법

이 태스크 정보

이 태스크는 404 페이지의 『로그 데이터 세트에 대한 데이터 세트 암호화 구성』의 필수조건입니다.

프로시저

1. z/OS 키 생성기 유틸리티 프로그램 (KGUP)을 사용하여 레이블 (예: CSQ1DSKY) 을 사용하여 AES-256 비트 암호화 DATA키를 설정하십시오.
2. 다음 명령을 실행하여 CSQ1DSKY 암호화 키에 대한 RACF CSFKEYS 프로파일을 정의하십시오.

```
RDEFINE CSFKEYS CSQ1DSKY UACC(NONE)
```

3. 다음 명령을 실행하여, 키를 보호된 키로 사용할 수 있도록 프로파일의 ICSF 세그먼트를 구성하십시오.

```
RALTER CSFKEYS CSQ1DSKY ICSF(SYMCPACFWRAP(YES) SYMCPACFRET(YES))
```

4. 다음 명령을 실행하여 QMCSQ1에 READ 액세스 권한을 부여함으로써 큐 관리자가 암호화 키를 사용할 수 있도록 하십시오.

```
PERMIT CSQ1DSKY CLASS(CSFKEYS) ID(QMCSQ1) ACCESS(READ)
```

암호화된 데이터 세트를 읽고 써야 하는 다른 관리자에게도 동일한 액세스 권한을 부여하십시오.

5. 다음 명령을 실행하여 CSFKEYS 클래스를 새로 고치십시오.

```
SETROPTS RACLIST(CSFKEYS) REFRESH
```

다음에 수행할 작업

404 페이지의 『로그 데이터 세트에 대한 데이터 세트 암호화 구성』에 설명되어 있는 바와 같이 데이터 세트에 대한 데이터 세트 암호화를 구성하십시오.

z/OS V 9.1.4 로그 데이터 세트에 대한 데이터 세트 암호화 구성

로그 데이터 세트에 대해 암호화를 구성하는 방법입니다.

시작하기 전에

다음 항목을 읽었는지 확인하십시오.

[IBM MQ for z/OS 데이터 세트 암호화 단계의 개요](#). 그리고 다음 항목에 있는 프로시저를 수행했는지 확인하십시오.

[404 페이지의 『큐 관리자에 대한 데이터 세트 암호화 키 구성』](#)

이 태스크 정보

이 방법은 RACF 일반 프로파일의 DFP 세그먼트를 사용하므로, 이 프로파일과 일치하는 모든 데이터 세트에 대한 암호화 키를 사용할 수 있습니다.

또는 SMS 데이터 클래스를 구성하고 사용할 수 있으며, 데이터 세트를 할당할 때 직접 키 레이블을 지정할 수도 있습니다.

이전에 설명한 바와 같이, 이 예에서 큐 관리자 CSQ1은 사용자 QMCSQ1에 의해 실행되며, 활성 데이터 로그 세트 CSQ1.LOGS.LOGCOPY1.DS001, CSQ1.LOGS.LOGCOPY1.DS002, ...를 보유하고 있습니다.

프로시저

1. 일반 프로파일이 없는 경우에는 다음 명령을 실행하여 이를 작성하십시오.

```
ADDSD 'CSQ1.LOGS.*' UACC(NONE)
```

2. 다음 명령을 실행하여 프로파일에 대한 큐 관리자 사용자의 대체 액세스를 허용하십시오.

```
PERMIT 'CSQ1.LOGS.*' ID(QMCSQ1) ACCESS(ALTER)
```

다른 관리자가 필요로 하는 적절한 액세스 또한 허용하십시오.

3. 다음 명령을 실행하여 암호화 키 레이블을 포함하는 DFP 세그먼트를 추가하십시오.

```
ALTDSD 'CSQ1.LOGS.*' DFP(RESOWNER(QMCSQ1) DATAKEY(CSQ1DSKY))
```

참고: [큐 관리자에 대한 데이터 세트 암호화 키 구성](#)에서 사용한 것과 동일한 암호화 키를 사용해야 합니다.

4. 다음 명령을 실행하여 일반 데이터 세트 프로파일을 새로 고치십시오.

```
SETROPTS GENERIC(DATASET) REFRESH
```

5. 백업할 각 로그 데이터 세트의 이름을 바꾼 후 IDCAMS를 사용하여 데이터를 다시 작성하고 복원하십시오. 다음 JCL 파편은 CSQ1.LOGS.LOGCOPY1.DS001을 변환합니다.

- a) 백업할 데이터 세트의 이름을 바꾸십시오.

```
//RENAME EXEC PGM=IDCAMS,REGION=0M
//SYSPRINT DD SYSOUT=*
//SYSIN DD *
/*-----*/
/* RENAME DATASET TO BACKUP */
/*-----*/
ALTER 'CSQ1.LOGS.LOGCOPY1.DS001' -
      NEWNAME('CSQ1.BAK.LOGS.LOGCOPY1.DS001')
```

- b) 데이터 세트를 재정의하십시오.

새 데이터 세트는 RACF 프로파일에 따라 암호화됩니다.

참고: ++EXTDCLASS++를 데이터 세트에 대해 사용할 확장 형식 데이터 클래스의 이름으로 대체하십시오.

```
//REDEFINE EXEC PGM=IDCAMS,REGION=0M
//SYSPRINT DD SYSOUT=*
//SYSIN DD *
/*-----*/
/* REDEFINE THE DATASET */
/*-----*/
DEFINE CLUSTER -
```



```
(NAME(CSQ1.LOGS.LOGCOPY1.DS001) -
LINEAR -
SHAREOPTIONS(2 3) -
MODEL(CSQ1.BAK.LOGS.LOGCOPY1.DS001) -
DATACLAS(++EXTDCLASS++))
```

- c) 백업의 데이터를 재작성된 데이터 세트에 복사하십시오.
이 단계는 데이터를 암호화합니다.

```
//RESTORE EXEC PGM=IDCAMS,REGION=0M
//SYSPRINT DD SYSOUT=*
//SYSIN DD *
/*-----*/
/* RESTORE DATA INTO ENCRYPTED LOG */
/*-----*/
REPRO INDATASET(CSQ1.BAK.LOGS.LOGCOPY1.DS001) -
      OUTDATASET(CSQ1.LOGS.LOGCOPY1.DS001)
```

다음에 수행할 작업

모든 활성 로그 데이터 세트에 대해 405 페이지의 『5』 단계를 반복하십시오.

하나의 암호화 키만 필요하며, 모든 데이터 세트는 동일한 키 레이블과 연관시킬 수 있습니다.

큐 관리자 CSQ1을 재시작하십시오. `DISPLAY LOG` 명령의 출력을 사용하여 로그 데이터 세트가 암호화되었는지 확인하십시오.

z/OS V 9.1.4 큐 공유 그룹에서의 z/OS 데이터 세트 암호화에 대한 고려사항

큐 공유 그룹(QSG)의 각 큐 관리자는 QSG에 있는 다른 모든 큐 관리자의 로그, BSDS V 9.1.5 및 공유 메시지 데이터 세트(SMDS)를 읽을 수 있어야 합니다.

이는 QSG의 멤버가 실행될 수 있는 각 시스템이 z/OS 데이터 세트 암호화에 대한 요구사항을 충족해야 하며, 각 큐 관리자에 대한 데이터 세트를 보호하는 데 사용되는 모든 키 레이블 및 암호화 키가 각 시스템에서 사용 가능해야 함을 의미합니다.

IBM MQ for z/OS 9.1.3 이전 큐 관리자는 암호화된 활성 로그 데이터 세트에 액세스할 수 없습니다.

V 9.1.5 IBM MQ for z/OS 9.1.3 이전의 큐 관리자는 암호화된 SMDS에 액세스할 수 없습니다.

V 9.1.5 z/OS 데이터 세트 암호화를 이용하기 전에 QSG에 있는 모든 큐 관리자를 IBM MQ for z/OS 9.1.3 이상으로 마이그레이션해야 합니다.

QSG의 한 큐 관리자가 암호화된 활성 로그를 지원하는 IBM MQ for z/OS 버전으로 시작되지 않은 상태에서 QSG의 다른 큐 관리자가 암호화된 활성 로그 데이터 세트를 사용하여 시작되는 경우, 암호화된 활성 로그가 있는 큐 관리자가 이상종료 코드 5C6-00F50033을 출력하며 비정상 종료됩니다.

V 9.1.5 다음을 통해 전체를 중지시키지 않고도 암호화된 활성 로그와 SMDS를 사용하도록 QSG를 변환할 수 있습니다.

1. 각 큐 관리자를 IBM MQ 9.1.5 이상으로 차례대로 마이그레이션합니다.
2. 각 큐 관리자에 대해 활성 로그를 암호화된 데이터 세트로 차례대로 변환합니다. 이 작업을 하려면 큐 관리자를 종료한 다음 재시작해야 합니다.

보통 이와 동시에 페이지 세트 및 아카이브 로그 또한 암호화된 데이터 세트로 사용할 수 있도록 설정되지만, 이는 QSG 마이그레이션에 영향을 주지 않습니다.

각 데이터 세트를 변환하기 위한 프로시저는 404 페이지의 『큐 관리자 활성 로그 암호화 방법 예』에 설명되어 있습니다.

3. 다음을 통해 각 개별 CF 구조에 대해 SMDS를 암호화된 데이터 세트로 차례대로 변환합니다.
 - a. `RESET SMDS(*) ACCESS(DISABLED) CFSTRUCT(structure-name)` 명령을 발행하여 SMDS에 대한 큐 관리자 액세스를 일시중단합니다.

일시중단된 동안에는 SMDS와 연관된 공유 큐의 데이터가 임시적으로 사용 불가능함을 참고하십시오.

- b. 404 페이지의 『큐 관리자 활성화 로그 암호화 방법 예』에 설명된 프로시저를 사용하여 SMDS를 구성하는 각 데이터 세트를 암호화된 데이터 세트로 변환합니다.
- c. RESET SMDS(*) ACCESS(ENABLED) CFSTRUCT(structure-name) 명령을 발행하여 SMDS에 대한 큐 관리자 액세스를 재개합니다.



주의: 로그를 변환하기 전에는 큐 관리자를 올바르게 종료해야 하며, 변환 중에는 활성화 로그 데이터 세트가 임시로 사용 불가능하게 되므로 커플링 기능 구조 복구가 불가능할 수 있습니다.

z/OS V 9.1.4 z/OS 데이터 세트 암호화 사용 시 역방향 마이그레이션 고려사항

하나 이상의 암호화된 데이터 세트를 가지고 있는 큐 관리자를 역방향으로 마이그레이션할 때 다음을 고려해야 합니다.

z/OS 데이터 세트 암호화는 다음 IBM MQ for z/OS 데이터 세트에서 지원됩니다.

- 활성화 로그 데이터 세트
- 아카이브 로그 데이터 세트
- 페이지 세트
- BSDS
- **V 9.1.5** SMDS
- CSQINP* 데이터 세트

BSDS, 아카이브 로그 또는 CSINP* 데이터 세트에 대한 역방향 마이그레이션 고려사항은 없습니다.

그러나 다음에 대한 고려사항이 있습니다.

- **V 9.1.5** SMDS
- 페이지 세트 및
- 활성화 로그

z/OS 데이터 세트 암호화와 함께 이를 사용하는 것과 같은 데이터 세트는 IBM MQ for z/OS 9.1.0 및 이전의 장기 지원 릴리스에서 지원되지 않습니다.

역방향 마이그레이션 전에 **V 9.1.5** SMDS, 페이지 세트 및 활성화 로그 데이터 세트에 대한 모든 암호화 정책은 제거되고 데이터는 복호화되어야 합니다. 이 프로세스는 407 페이지의 『데이터 세트에서 데이터 세트 암호화 제거』에 설명되어 있습니다.



주의: 역방향으로 마이그레이션할 큐 관리자가 큐 공유 그룹(QSG)에 속하는 경우 먼저 409 페이지의 『큐 공유 그룹 고려사항』 절을 읽으십시오.

데이터 세트에서 데이터 세트 암호화 제거

이 예에서는 로그 데이터 세트 CSQ1.LOGS.LOGCOPY1.DS001에서 데이터 세트 암호화를 제거하는 방법을 설명합니다. **V 9.1.5** SMDS 및 페이지 세트에 동일한 프로세스를 사용할 수 있습니다.

이 예에서는 다음과 같이 가정합니다.

- RACF가 SAF임
- 데이터 세트를 사용하는 큐 관리자가 중지되었음
- 암호화 키 레이블이 일반 RACF 프로파일 CSQ1.LOGS.*와 연관되었음

다음 프로시저를 수행하십시오.

1. 데이터 세트의 데이터를 백업 데이터 세트에 복사하십시오.
 - a. 암호화 키 레이블과 연관되지 않은 백업 데이터 세트를 정의하십시오.

참고: ++EXTDCLASS++를 데이터 세트에 대해 사용할 확장 형식 데이터 클래스의 이름으로 대체하십시오.

```
//DEFINE EXEC PGM=IDCAMS,REGION=0M
//SYSPRINT DD SYSOUT=*
//SYSIN DD *
/*-----*/
/* DEFINE UNENCRYPTED DATA SET */
/*-----*/
DEFINE CLUSTER -
      (NAME(CSQ1.BAK.LOGS.LOGCOPY1.DS001) -
      LINEAR -
      SHAREOPTIONS(2 3) -
      MODEL(CSQ1.LOGS.LOGCOPY1.DS001) -
      DATACLASS(++EXTDCLASS++))
/*
```

b. 원래 데이터 세트의 데이터를 백업에 복사하십시오. 이 단계에서는 데이터를 복호화합니다.

```
//COPY EXEC PGM=IDCAMS,REGION=0M
//SYSPRINT DD SYSOUT=*
//SYSIN DD *
/*-----*/
/* COPY DATA INTO UNENCRYPTED DATA SET */
/*-----*/
REPRO INDATASET(CSQ1.LOGS.LOGCOPY1.DS001) -
      OUTDATASET(CSQ1.BAK.LOGS.LOGCOPY1.DS001)
/*
```

c. 원래 데이터 세트를 삭제하십시오.

```
//DELETE EXEC PGM=IDCAMS,REGION=0M
//SYSPRINT DD SYSOUT=*
//SYSIN DD *
/*-----*/
/* DELETE ORIGINAL */
/*-----*/
DELETE ('CSQ1.LOGS.LOGCOPY1.DS001')
/*
```

d. 백업의 이름을 원래 데이터 세트 이름으로 바꾸십시오. 데이터는 암호화되지 않은 상태로 유지됩니다.

```
//RENAME EXEC PGM=IDCAMS,REGION=0M
//SYSPRINT DD SYSOUT=*
//SYSIN DD *
/*-----*/
/* RENAME UNENCRYPTED DATA SET */
/*-----*/
ALTER CSQ1.BAK.LOGS.LOGCOPY1.DS001 -
      NEWNAME('CSQ1.LOGS.LOGCOPY1.DS001')
ALTER 'CSQ1.BAK.LOGS.LOGCOPY1.DS001.*' -
      NEWNAME('CSQ1.LOGS.LOGCOPY1.DS001.*')
/*
```

2. 선택적으로 CSQ1.LOGS.* 일반 프로파일.
3. 선택적으로 CSQ1.LOGS.* 일반 프로파일이 암호 해독되었습니다. 다음 명령을 실행하여 일반 프로파일과 연관된 DATAKEY를 제거하십시오.

```
ALTDSO 'CSQ1.LOGS.*' DFP(RESOWNER(QMCSQ1) DATAKEY(CSQ1DSKY))
```

4. 다음 명령을 실행하여 일반 데이터 세트 프로파일을 새로 고치십시오.

```
SETROPTS GENERIC(DATASET) REFRESH
```

5. 큐 관리자를 재시작하십시오.
6. 암호화 키가 더 이상 필요하지 않은 경우 삭제하고 CSFKEYS 클래스로부터 그와 연관된 RACF 프로파일을 삭제하십시오.

큐 공유 그룹 고려사항

큐 공유 그룹에 속하는 큐 관리자가 데이터 세트 암호화를 지원하지 않는 IBM MQ for z/OS 버전으로 역방향 마이그레이션될 예정인 경우 QSG 내 모든 큐 관리자의 모든 활성 로그 데이터 세트 **V 9.1.5** 및 SMDS에 포함된 데이터 세트 암호화 정책은 제거되어야 하고 데이터는 복호화되어야 합니다.

이는 역방향으로 마이그레이션되는 멤버가 QSG의 단일 멤버인지 또는 QSG의 모든 멤버인지에 상관없이 적용됩니다.

다음을 통해 전체 QSG를 중지하지 않고도 데이터의 복호화 및 암호화 정책의 제거를 수행할 수 있습니다.

1. QSG에서 각 큐 관리자를 순서대로 종료시키고, 활성 로그에서 암호화 정책 제거 및 데이터 복호화를 수행하고 407 페이지의 『데이터 세트에서 데이터 세트 암호화 제거』에서 설명한 프로세스를 사용.

큐 관리자를 역방향으로 마이그레이션하려는 경우 해당 페이지 세트도 이 때 복호화해야 합니다. 그런 다음 큐 관리자를 재시작하십시오.

2. **V 9.1.5** 다음을 수행하여 각 개별 CF 구조의 SMDS에 대해 순서대로 암호화 정책을 제거하고 데이터를 복호화합니다.

- a. 다음 명령을 발행하여

```
RESET SMDS(*) ACCESS(DISABLED) CFSTRUCT(structure-name)
```

SMDS에 대한 큐 관리자 액세스를 일시중단시키십시오. 일시중단된 동안에는 SMDS와 연관된 공유 큐의 데이터는 임시적으로 사용 불가능하게 됩니다.

- b. SMDS를 구성하는 각 데이터 세트의 407 페이지의 『데이터 세트에서 데이터 세트 암호화 제거』에 있는 프로세스를 수행합니다.

- c. 다음 명령을 발행하여

```
RESET SMDS(*) ACCESS(ENABLED) CFSTRUCT(structure-name)
```

SMDS에 대한 큐 관리자 액세스를 재개하십시오.

z/OS 데이터 세트 암호화를 지원하지 않는 큐 관리자에서 이 암호화 사용

실수로 큐 관리자를 데이터 세트 암호화를 지원하지 않는 IBM MQ for z/OS 버전으로 역방향 마이그레이션하고 암호화 정책 제거 및 데이터 복호화를 수행하지 않은 경우 큐 관리자가 데이터 세트에 액세스하려고 시도하면 오류가 발생합니다.

이 오류는 데이터 세트 유형에 따라 다르고 다음 테이블에 표시됩니다.

참고: 이러한 오류 중 하나 이상이 발생하는 경우 영향을 받는 데이터 세트에 대해 407 페이지의 『데이터 세트에서 데이터 세트 암호화 제거』에 설명된 프로세스를 따라야 합니다. 이러한 프로세스는 IBM MQ for z/OS의 버전을 변경하지 않고도 수행할 수 있습니다.

데이터 세트	큐 관리자가 z/OS 데이터 세트 암호화를 지원하지 않는 경우 오류가 발생함
페이지 세트 0	큐 관리자 시작 시 이상종료 5C6-00C91400이 발생함
페이지 세트 1 - 99	페이지 세트에 액세스할 때(예를 들어, MQPUT에서) MQRC 2193 “페이지 세트 오류”가 발생함
활성 로그	큐 관리자 시작 시 이상종료 5C6-00E80084가 발생함
V 9.1.5 SMDS	Message IEC161I-122 logged “데이터 세트에 키 레이블이 있지만 사용자가 애플리케이션이 암호화를 처리할 수 있도록 지정하지 않았습니다.” 메시지 IEC161I-122가 로깅됩니다. SMDS가 AVAIL(ERROR)로 표시됩니다.

메시지의 데이터 무결성

데이터의 무결성을 유지보수하기 위해 다양한 유형의 사용자 엑시트 프로그램을 사용하여 메시지의 메시지 요약 또는 디지털 서명을 제공할 수 있습니다.

데이터 무결성

메시지에서 데이터 무결성 구현

TLS를 사용할 때 선택한 CipherSpec는 엔터프라이즈에서 데이터 무결성의 레벨을 판별합니다. IBM MQ 고급 메시지 서비스(AMS)를 사용하는 경우에는 고유한 메시지의 무결성을 지정할 수 있습니다.

메시지 엑시트에서 데이터 무결성 구현

메시지는 채널의 송신 측에 있는 메시지 엑시트에 의해 디지털로 서명될 수 있습니다. 그런 후, 메시지가 의도적으로 수정되었는지를 감지하기 위해 채널의 수신 측에 있는 메시지 엑시트에 의해 디지털 서명이 검사될 수 있습니다.

디지털 서명 대신에 메시지 요약을 사용하여 일부 보호가 제공될 수 있습니다. 약식 또는 무차별 도용에 대해서는 메시지 요약이 효율적일 수 있으나, 경험이 많은 사람이 메시지를 변경하거나 바꾸고, 그것에 대한 완전히 새로운 축약을 생성하는 것을 막지는 못합니다. 메시지 요약을 생성하는 데 사용되는 알고리즘이 잘 알려진 것이라면 더욱 그렇습니다.

송신 및 수신 엑시트에서 데이터 무결성 구현

메시지 채널에서는 메시지 엑시트가 전체 메시지에 액세스할 수 있기 때문에 이 서비스를 제공하는 데는 메시지 엑시트가 더 적합합니다. MQI 채널에서는 MQI 호출의 매개변수들에 보호되어야 하는 애플리케이션 데이터가 있을 수 있고 송신과 수신 엑시트만이 이 보호를 제공할 수 있습니다.

API 엑시트 또는 API 교차 엑시트에서 데이터 무결성 구현

메시지가 송신 애플리케이션에 의해 놓일 때 메시지는 API 또는 API 교차 엑시트에 의해 디지털적으로 서명될 수 있습니다. 그런 다음 디지털 서명은 메시지가 의도적으로 수정되었는지 여부를 감지하기 위해 수신 애플리케이션에 의해 검색될 때 두 번째 엑시트에 의해 검사될 수 있습니다.

디지털 서명 대신에 메시지 요약을 사용하여 일부 보호가 제공될 수 있습니다. 약식 또는 무차별 도용에 대해서는 메시지 요약이 효율적일 수 있으나, 경험이 많은 사람이 메시지를 변경하거나 바꾸고, 그것에 대한 완전히 새로운 축약을 생성하는 것을 막지는 못합니다. 메시지 요약을 생성하는 데 사용되는 알고리즘이 잘 알려진 것이라면 더욱 그렇습니다.

추가 정보

데이터 무결성을 확인하는 방법에 대한 자세한 정보는 [376 페이지의 『CipherSpec 사용 가능』](#)에 대한 절을 참조하십시오.

관련 태스크

[TLS를 사용하여 두 개의 큐 관리자 연결](#)
[클라이언트를 큐 관리자에 안전하게 연결](#)

감사

이벤트 메시지를 사용하여 보안 침입 또는 침입 시도를 확인할 수 있습니다. IBM MQ Explorer를 사용하여 시스템의 보안을 확인할 수도 있습니다.

큐 관리자에 연결 또는 메시지를 큐에 놓기 등과 같은 권한 없는 조치를 수행하려는 시도를 감지하려면 큐 관리자가 생성한 이벤트 메시지, 특히 권한 이벤트 메시지를 검사하십시오. 큐 관리자 이벤트 메시지에 대한 자세한 정보는 [큐 관리자 이벤트](#)를, 이벤트 모니터링 일반에 대한 자세한 정보는 [이벤트 모니터링](#)을 참조하십시오.

클러스터 보안 유지

큐 관리자에게 클러스터를 조인하거나 클러스터 큐에 메시지를 넣도록 권한 부여하거나 금지하십시오. 강제로 큐 관리자가 클러스터를 나가도록 하십시오. 클러스터에 대해 TLS를 구성할 때 몇 가지 추가 고려사항을 고려하십시오.

권한 없는 큐 관리자가 메시지를 전송하는 것을 중지

채널 보안 엑시트를 사용하여 권한 없는 큐 관리자가 큐 관리자에 메시지를 전송하는 것을 방지하십시오.

시작하기 전에

클러스터링은 보안 엑시트가 작동하는 방법에는 영향을 미치지 않습니다. 분산 큐잉 환경에서와 같은 방법으로 큐 관리자에 대한 액세스를 제한할 수 있습니다.

이 태스크 정보

선택된 큐 관리자가 큐 관리자에 메시지를 전송하는 것을 방지하십시오.

프로시저

1. CLUSRCVR 채널 정의에 채널 보안 엑시트 프로그램을 정의하십시오.
2. 클러스터 수신자 채널에서 메시지를 전송하려고 시도하는 큐 관리자를 인증하고 권한이 없는 경우 액세스를 거부하는 프로그램을 작성하십시오.

다음에 수행할 작업

채널 보안 엑시트 프로그램은 MCA 시작 및 종료 시에 호출됩니다.

권한 없는 큐 관리자가 메시지를 사용자의 큐에 넣는 것을 중지

권한 없는 큐 관리자가 메시지를 큐에 넣는 것을 중지하려면 클러스터 수신자 채널에서 채널 넣기 권한 속성을 사용하십시오. z/OS에서 RACF를 사용하여 메시지의 사용자 ID를 확인하거나 기타 플랫폼의 경우 OAM을 사용하여 리모트 큐 관리자에 권한을 부여하십시오.

이 태스크 정보

큐에 대한 액세스를 제어하려면 IBM MQ에서 플랫폼의 보안 기능 및 액세스 제어 메커니즘을 사용하십시오.

프로시저

1. 특정 큐 관리자가 메시지를 큐에 넣는 것을 방지하려면 플랫폼에서 사용 가능한 보안 기능을 사용하십시오.
예를 들면, 다음과 같습니다.
 - RACF or other external security managers on IBM MQ for z/OS
 - 다른 플랫폼의 오브젝트 권한 관리자(OAM).
2. CLUSRCVR 채널 정의에서 넣기 권한, PUTAUT 속성을 사용하십시오.

PUTAUT 속성을 사용하면 메시지를 큐에 넣기 위해 권한을 설정하기 위해 어떤 사용자 ID가 사용되는지를 지정할 수 있습니다.

PUTAUT 속성의 옵션은 다음과 같습니다.

DEF

기본 사용자 ID를 사용하십시오. z/OS에서 검사는 네트워크에서 수신한 사용자 ID 및 MCAUSER에서 파생된 사용자 ID 둘 모두를 사용하는 것과 관련될 수 있습니다.

CTX

메시지와 연관된 컨텍스트 정보에서 사용자 ID를 사용하십시오. z/OS에서 검사는 네트워크에서 수신한 사용자 ID 또는 MCAUSER에서 파생된 사용자 ID 또는 둘 모두의 사용과 관련될 수도 있습니다. 링크가 신뢰되고 인증되는 경우 이 옵션을 사용하십시오.

ONLYMCA (z/OS 만 해당)

DEF에 대해서는 네트워크에서 수신한 모든 사용자 ID가 사용되지 않습니다. 링크가 신뢰되지 않은 경우에 이 옵션을 사용하십시오. MCAUSER에 정의된 특정 조치 세트만을 허용하고 싶습니다.

ALTMCA(z/OS에만 해당)

CTX에 대해서는 네트워크에서 수신한 모든 사용자 ID가 사용되지 않습니다.

리모트 클러스터 큐에 메시지를 넣는 권한 부여

z/OS에서 RACF를 사용하여 클러스터에 넣기 위한 권한을 설정하십시오. 다른 플랫폼에서 큐 관리자에 연결하기 위한 액세스의 권한을 부여하고 큐를 이러한 큐 관리자에 놓으십시오.

이 태스크 정보

기본 동작은 SYSTEM.CLUSTER.TRANSMIT.QUEUE에 대한 액세스 제어를 수행하는 것입니다. 이 작동은 여러 전송 큐를 사용 중인 경우에도 적용된다는 점을 유의하십시오.

이 주제에 설명된 특정 동작은 보안 스탠자 주제에 설명된 대로 `qm.ini` 파일에서 **ClusterQueueAccessControl** 속성을 `RQMName`으로 구성하고 큐 관리자를 재시작한 경우에만 적용됩니다.

프로시저

- z/OS의 경우 다음 명령을 실행하십시오.

```
RDEFINE MQQUEUE QMgrName.QUEUE. QueueName UACC(NONE)
PERMIT QMgrName.QUEUE. QueueName CLASS(MQADMIN) ID(GroupName) ACCESS(UPDATE)
```

- UNIX, Linux, and Windows 시스템의 경우 다음 명령을 실행하십시오.

```
setmqaut -m QMgrName -t qmgr -g GroupName +connect
setmqaut -m QMgrName -t queue -n QueueName -g GroupName -all +put
```

- IBM i의 경우 다음 명령을 실행하십시오.

```
GRTMQMAUT OBJ(' QMgrName ') OBJTYPE(*MQM) USER(GroupName) AUT(*CONNECT)
GRTMQMAUT OBJ(' QueueName ') OBJTYPE(*Q) USER(GroupName) AUT(*PUT) MQMNAME(' QMgrName ')
```

사용자는 다른 클러스터 큐가 아닌 지정된 클러스터 큐에만 메시지를 넣을 수 있습니다.

변수 이름에는 다음과 같은 의미가 있습니다.

QMGrName

큐 관리자 이름. z/OS에서 이 값은 또한 큐 공유 그룹의 이름일 수도 있습니다.

GroupName

액세스가 부여될 그룹의 이름입니다.

QueueName

권한 부여를 변경할 큐 또는 일반 프로파일의 이름입니다.

다음에 수행할 작업

클러스터 큐에 메시지를 넣을 때 응답 대상 큐를 지정하면 처리 애플리케이션에 응답을 송신할 수 있는 권한이 있어야 합니다. 356 페이지의 『메시지를 리모트 클러스터 큐에 넣기 위한 권한 부여』의 지시사항에 따라 이 권한을 설정하십시오.

관련 개념

[qm.ini의 보안 스탠자](#)

큐 관리자가 클러스터에 조인하는 것을 방지

악한 큐 관리자가 클러스터에 조인하면 사용자가 수신하고 싶지 않은 메시지를 큐 관리자가 수신하는 것을 방지하기 어렵게 됩니다.

프로시저

특정 권한 있는 큐 관리자만이 클러스터에 조인하게 하려면 다음 세 개의 방법을 선택할 수 있습니다.

- 채널 인증 레코드를 사용하면 원격 시스템이 제공하는 원격 IP 주소, 리모트 큐 관리자 이름 또는 TLS 식별 이름을 기반으로 클러스터 채널 연결을 차단할 수 있습니다.
- 권한 없는 큐 관리자가 SYSTEM.CLUSTER.COMMAND.QUEUE에 쓰는 것을 막는 엑시트 프로그램을 작성하십시오. 큐 관리자가 여기에 쓸 수 없도록 SYSTEM.CLUSTER.COMMAND.QUEUE에 대한 액세스를 제한하지 마십시오. 그렇지 않으면 큐 관리자가 클러스터에 조인하는 것을 막게 됩니다.
- CLUSRCVR 채널 정의에서 보안 엑시트 프로그램.

클러스터 채널에서 보안 엑시트

클러스터 채널에서 보안 엑시트를 사용할 때 추가 고려사항

이 태스크 정보

클러스터-송신자 채널이 처음 시작될 때 이는 시스템 관리자가 수동으로 정의한 속성을 사용합니다. 채널이 중지된 후 다시 시작되면 이는 해당하는 클러스터-수신자 채널 정의로부터 속성을 선택합니다. 원본 클러스터-송신자 채널 정의는 SecurityExit 속성을 포함하여 새 속성으로 덮어쓰기됩니다.

프로시저

1. 채널의 클러스터-송신자 끝 및 클러스터-수신자 끝 둘 모두에서 보안 엑시트를 정의해야 합니다.
보안 엑시트 이름이 클러스터-수신자 정의로부터 전송되더라도 초기 연결은 보안-엑시트 데이터 교환을 사용하여 작성되어야 합니다.
2. 보안 엑시트에서 MQCXP 구조에서 PartnerName을 유효성 검증하십시오.
엑시트는 파트너 큐 관리자가 권한 부여된 경우에만 채널이 시작하도록 허용해야 합니다.
3. 클러스터-수신자 정의에서 보안 엑시트가 시작된 수신자가 되도록 설계하십시오.
4. 이를 시작된 송신자로서 설계하는 경우에는 보안 검사가 수행되지 않으므로 보안 엑시트가 없는 권한 없는 큐 관리자는 클러스터에 조인할 수 있습니다.
채널이 중지되고 다시 시작될 때까지는 SCYEXIT 이름이 클러스터-수신자 정의로부터 전송되고 전체 보안 검사가 수행될 수 없습니다.
5. 현재 사용 중인 클러스터-송신자 채널 정의를 보려면 다음 명령을 사용하십시오.

```
DISPLAY CLUSQMGR( queue manager ) ALL
```

명령은 클러스터-수신자 정의로부터 전송된 속성을 표시합니다.

6. 원본 정의를 보려면 다음 명령을 사용하십시오.

```
DISPLAY CHANNEL( channel name ) ALL
```

7. 큐 관리자가 다른 플랫폼에 있는 경우 클러스터-송신자 큐 관리자에서 채널 자동 정의 엑시트, CHADEXIT를 정의해야 할 수도 있습니다.
채널 자동 정의 엑시트를 사용하여 SecurityExit 속성을 대상 플랫폼에 적합한 형식으로 설정하십시오.
8. 보안 엑시트를 배치하고 구성하십시오.

 z/OS

보안 엑시트 로드 모듈은 채널 시작기 주소 공간 프로시저의 CSQXLIB DD문에 지정된 데이터 세트에 있어야 합니다.

 Windows, UNIX and Linux 시스템

- 보안 엑시트 동적 링크 라이브러리는 채널 정의의 SCYEXIT 속성에 지정된 경로에 있어야 합니다.

- 채널 자동 정의 엑시트 동적 링크 라이브러리는 큐 관리자 정의의 CHADEXIT 속성에 지정된 경로에 있어야 합니다.

필요하지 않은 큐 관리자는 클러스터에서 강제로 제거

전체 저장소 큐 관리자에서 RESET CLUSTER 명령을 실행하여 필요하지 않은 큐 관리자는 클러스터에서 강제로 제거하십시오.

이 태스크 정보

필요하지 않은 큐 관리자는 클러스터에서 강제로 제거할 수 있습니다. 예를 들어, 큐 관리자가 삭제되었지만 해당 클러스터 수신자 채널이 여전히 클러스터에 정의되어 있습니다. 이를 정돈하고 싶을 수도 있습니다.

전체 저장소 큐 관리자만이 큐 관리자를 클러스터에서 배출하기 위한 권한이 부여됩니다.

참고: RESET CLUSTER 명령을 사용하면 큐 관리자를 강제로 클러스터에서 제거하지만 RESET CLUSTER를 사용하는 것만으로는 큐 관리자가 나중에 클러스터에 다시 조인하는 것을 방지할 수 없습니다. 큐 관리자가 클러스터에 다시 조인하지 않게 하려면 [412 페이지의 『큐 관리자가 클러스터에 조인하는 것을 방지』](#)에 설명된 단계를 따르십시오.

큐 관리자 OSLO를 클러스터 NORWAY에서 배출하려면 이 프로시저를 따르십시오.

프로시저

1. 전체 저장소 큐 관리자에서 명령을 실행하십시오.

```
RESET CLUSTER(NORWAY) QMNAME(OSLO) ACTION(FORCEREMOVE)
```

2. 명령에서 QMNAME 대신에 QMID를 사용하십시오.

```
RESET CLUSTER(NORWAY) QMID(qmid) ACTION(FORCEREMOVE)
```

참고: QMID는 문자열이므로 qmid의 값은 작은따옴표로 묶어야 합니다 (예: QMID('FR01_2019-07-15_14.42.42')).

결과

강제로 제거된 큐 관리자는 변경되지 않습니다. 해당 로컬 클러스터 정의는 이것이 클러스터에 있는 것으로 표시합니다. 다른 모든 큐 관리자에서의 정의는 이를 클러스터에 표시하지 않습니다.

큐 관리자가 메시지 수신하는 것을 방지

엑시트 프로그램을 사용하여 클러스터 큐 관리자가 수신할 권한이 없는 메시지를 수신하는 것을 막을 수 있습니다.

이 태스크 정보

클러스터의 멤버인 큐 관리자가 큐를 정의하지 못하도록 막는 것은 어렵습니다. 악한 큐 관리자가 클러스터에 조인하고 클러스터에 큐 중 하나의 자체 인스턴스를 정의할 위험이 있습니다. 이는 이제 수신할 권한이 없는 메시지를 수신할 수 있습니다. 큐 관리자가 메시지를 수신하는 것을 방지하려면 프로시저에 제공된 다음 옵션 중 하나를 사용하십시오.

프로시저

- 각 클러스터 송신자 채널에서 채널 엑시트 프로그램. 엑시트 프로그램은 연결 이름을 사용하여 메시지를 전송할 목적지 큐 관리자의 적합성을 판별합니다.
- 메시지가 전송될 목적지 큐 및 큐 관리자의 적합성을 판별하기 위해 목적지 레코드를 사용하는 클러스터 워크로드 엑시트 프로그램.

SSL/TLS 및 클러스터

클러스터에 대한 TLS를 구성할 때 CLUSRCVR 채널 정의가 자동 정의된 CLUSSDR 채널로 다른 큐 관리자에 전파됨을 유의하십시오. CLUSRCVR 채널이 TLS를 사용하는 경우 채널을 사용하여 통신하는 모든 큐 관리자에서 TLS를 구성해야 합니다.

TLS에 대한 자세한 정보는 21 페이지의 『IBM MQ의 TLS 보안 프로토콜』의 내용을 참조하십시오. 이 참고는 일반적으로 클러스터 채널에 적용 가능하지만 다음에 일부 특수 고려사항을 제공하고 싶을 수도 있습니다.

IBM MQ 클러스터에서 특별 CLUSRCVR 채널 정의는 종종 자동 정의된 CLUSSDR로 변환되는 다른 많은 큐 관리자로 전파됩니다. 이후에 자동 정의된 CLUSSDR이 채널을 CLUSRCVR에 시작하는 데 사용됩니다. CLUSRCVR이 TLS 연결성을 위해 구성된 경우에는 다음 고려사항이 적용됩니다.

- 이 CLUSRCVR과 통신하려는 모든 큐 관리자에게는 TLS 지원에 대한 액세스가 있어야 합니다. 이 TLS 프로비저닝은 채널의 CipherSpec을 지원해야 합니다.
- 자동 정의된 클러스터 송신자 채널이 전파된 다른 큐 관리자에게는 각각 서로 다른 식별 이름이 연관됩니다. 식별 이름 피어 검사가 CLUSRCVR에서 사용될 예정이면 수신할 수 있는 모든 식별 이름이 성공적으로 일치할 수 있도록 설정되어야 합니다.

예를 들어, 특정 CLUSRCVR에 연결할 클러스터-송신자 채널을 호스팅하는 모든 큐 관리자에 연관된 인증서가 가정해 보겠습니다. 또한 이러한 모든 인증서에서 식별 이름은 국가를 UK, 조직을 IBM, 조직 단위를 IBM MQ 부서로 정의하고, 모두 DEVT.QMnnn 양식으로 된 공통 이름(여기서, nnn은 숫자)을 가지고 있다고 가정합니다.

이 경우 CLUSRCVR에서 C=UK, O=IBM, OU=IBM MQ Development, CN=DEVT.QM*의 SSLPEER 값을 통해 필요한 모든 클러스터 송신자 채널은 성공적으로 연결하되 원하지 않는 클러스터 송신자 채널은 연결되지 않도록 할 수 있습니다.

- 사용자 정의 CipherSpec 문자열이 사용된 경우에는 사용자 정의 문자열 형식이 모든 플랫폼에서 허용되지는 않음을 유의하십시오. 예를 들어, CipherSpec 문자열 RC4_SHA_US 값 05는 IBM i에서 허용되지만 UNIX, Linux 또는 Windows 시스템에서는 올바른 스펙이 아닙니다. 따라서 사용자 정의 SSLCIPH 매개변수가 CLUSRCVR에서 사용되는 경우에는 결과로 나오는 모든 자동 정의된 클러스터 송신자 채널은 기본 TLS 지원이 이 CipherSpec을 구현하고 사용자 정의 값으로 지정될 수 있는 플랫폼에 상주해야 합니다. 클러스터 전체에 걸쳐 이해될 SSLCIPH 매개변수의 값을 선택할 수 없는 경우 이를 이해될 사용 중인 플랫폼으로 변경하기 위해 채널 자동 정의 엑시트가 필요합니다. 가능한 경우 텍스트 CipherSpec 문자열(예: TLS_RSA_WITH_AES_128_CBC_SHA)을 사용하십시오.

SSLCRLNL 매개변수는 개별 큐 관리자에 적용되고 클러스터 내에 다른 큐 관리자에게 전파되지 않습니다.

클러스터된 큐 관리자 및 채널을 SSL/TLS로 업그레이드

클러스터 채널을 한 번에 하나씩 업그레이드하여 CLUSSDR 채널 전에 모든 CLUSRCVR 채널을 변경하십시오.

시작하기 전에

클러스터를 위한 CipherSpec 선택에 영향을 미칠 수 있으므로 다음 고려사항을 고려하십시오.

- 일부 CipherSpec은 모든 플랫폼에서 사용 가능하지는 않습니다. 클러스터에 있는 모든 큐 관리자에 의해 지원되는 CipherSpec을 주의해서 선택하십시오.
- 일부 CipherSpec은 현재 IBM MQ 릴리스에서는 신규일 수도 있고 이전 릴리스에서는 지원되지 않을 수도 있습니다. 다른 MQ 릴리스에서 실행 중인 큐 관리자를 포함하는 클러스터는 각 릴리스가 지원하는 CipherSpec만을 사용할 수 있습니다.

클러스터 내에서 새 CipherSpec을 사용하려면 먼저 모든 클러스터 큐 관리자를 현재 릴리스로 마이그레이션해야 합니다.

- 일부 CipherSpec에는 사용할 디지털 인증서의 특정 유형이 필요한데, 특히, 타원 곡선 암호법을 사용하는 유형입니다.



주의: 클러스터의 일부로 함께 조인할 큐 관리자에서 Elliptic Curve 서명 인증서와 RSA 서명 인증서를 혼합해서 사용하는 것은 불가능합니다.

클러스터의 큐 관리자는 모두 RSA 서명 인증서를 사용하거나 모두 EC 서명 인증서를 사용해야 합니다. 이 둘을 혼합해서 사용할 수는 없습니다.

자세한 정보는 40 페이지의 『IBM MQ에서 디지털 인증서와 CipherSpec의 호환성』의 내용을 참조하십시오.

클러스터에 있는 모든 큐 관리자가 아직 IBM MQ V8 이상 레벨에 있지 않으면 업그레이드하십시오. TLS가 이들 각각에서 작동할 수 있도록 인증서 및 키를 분배하십시오.

톰을 업그레이드하거나 ANY_TLS12 CipherSpecs를 사용하려면 클러스터의 모든 큐 관리자를 IBM MQ 9.1.2 이상으로 업그레이드해야 합니다.

다른 별명 CipherSpecs (ANY_TLS13, ANY_TLS12, ANY_TLS12_OR_HIGHER 등) 중 하나를 업그레이드하거나 사용하려는 경우, 클러스터의 모든 큐 관리자를 IBM MQ 9.1.4 이상으로 업그레이드해야 합니다.

이 태스크 정보

CLUSDR 채널 전에 CLUSRCVR 채널을 변경하십시오.

프로시저

1. CLUSRCVR 채널을 원하는 순서로 TLS로 전환하여 한 번에 하나의 CLUSRCVR를 변경하고, 다음을 변경하기 전에 변경사항이 클러스터를 통해 플로우할 수 있게 허용하십시오.

중요사항: 현재 채널이 변경사항이 클러스터 전체에 분배될 때까지 역방향 경로를 변경하지 않았는지 확인하십시오.

2. 옵션: 모든 수동 CLUSDR 채널을 TLS로 전환하십시오.

이는 REFRESH CLUSTER 명령을 REPOS (YES) 옵션과 함께 사용하지 않는 한 클러스터의 조작에 영향을 미치지 않습니다.

참고: 큰 클러스터의 경우, REFRESH CLUSTER 명령을 사용하면 진행 중인 클러스터에 지장을 줄 수 있으며, 클러스터 오브젝트가 모든 관심있는 큐 관리자에게 자동으로 상태 업데이트를 보내는 경우에는 27일 간격으로 다시 사용할 수 있습니다. 대형 클러스터를 새로 고치면 클러스터의 성능 및 가용성에 영향을 줄 수 있음을 참조하십시오.

3. DISPLAY CLUSQMGR 명령을 사용하여 새 보안 구성이 클러스터 전체에 걸쳐 전파되었는지 확인하십시오.
4. TLS를 사용하도록 채널을 재시작한 후 REFRESH SECURITY(SSL)를 실행하십시오.

관련 개념

376 페이지의 『CipherSpec 사용 가능』

DEFINE CHANNEL MQSC 명령 또는 ALTER CHANNEL MQSC 명령에서 SSLCIPH 매개변수를 사용하여 CipherSpec을 사용 가능으로 설정하십시오.

40 페이지의 『IBM MQ에서 디지털 인증서와 CipherSpec의 호환성』

이 토픽은 IBM MQ에서 CipherSpec과 디지털 인증서 사이의 관계를 소개하여 보안 정책에 대해 적합한 CipherSpec 및 디지털 인증서를 선택하는 방법에 대한 정보를 제공합니다.

관련 정보

클러스터링: REFRESH CLUSTER 사용 우수 사례

클러스터된 큐 관리자 및 채널에서 SSL/TLS를 사용 안함으로 설정

TLS를 끄려면 SSLCIPH 매개변수를 ' ' 로 설정하십시오. 클러스터 채널에서 개별적으로 TLS를 사용 안함으로 설정하여 클러스터 송신자 채널 전에 클러스터 수신자 채널을 모두 변경하십시오.

이 태스크 정보

한 번에 하나의 클러스터 수신자 채널을 변경하고 다음을 변경하기 전에 변경사항이 클러스터를 통해 플로우하게 허용하십시오.

중요사항: 현재 채널이 변경사항이 클러스터 전체에 분배될 때까지 역방향 경로를 변경하지 않았는지 확인하십시오.

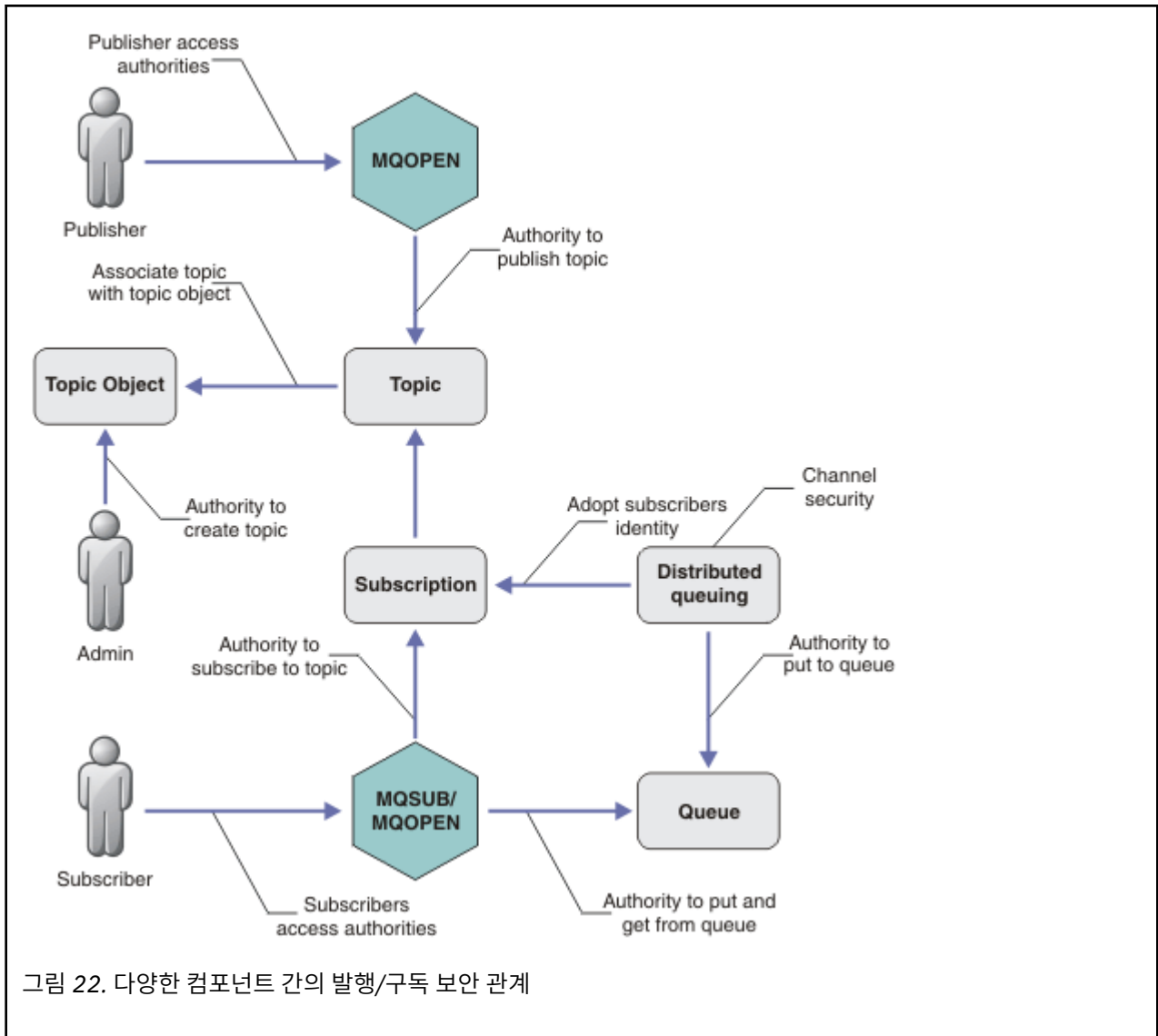
프로시저

1. SSLCIPH 매개변수의 값을 ' ', 비어 있는 문자열, 작은따옴표 **IBM i** 또는 IBM i의 *NONE 로 설정하십시오.
클러스터 수신자 채널에서 원하는 순서대로 TLS를 끌 수 있습니다.
변경사항이 TLS를 활성화된 채로 남겨두는 채널을 통해 반대 방향으로 플로우함을 유의하십시오.
2. **DISPLAY CLUSQMGR(*)** ALL 명령을 사용하여 다른 큐 관리자 모두에서 새 값이 반영되는지 확인하십시오.
3. 모든 매뉴얼 클러스터 송신자 채널에서 TLS를 끄십시오.
이는 **REFRESH CLUSTER** 명령을 REPOS(YES) 옵션과 함께 사용하지 않는 한 클러스터의 조작에 영향을 미치지 않습니다.
대형 클러스터의 경우 **REFRESH CLUSTER** 명령 사용은 진행 중에, 그리고 클러스터 오브젝트가 모든 관련 큐 관리자에 대한 상태 업데이트를 자동으로 전송한 후 주기적인 간격으로 클러스터에 지장을 줄 수 있습니다. 자세한 내용은 [대형 클러스터의 새로 고침이 클러스터의 성능과 가용성에 영향을 줄 수 있음](#)을 참조하십시오.
4. 클러스터 송신자 채널을 중지하고 다시 시작하십시오.

발행/구독 보안

발행/구독에 관련된 컴포넌트 및 상호작용은 다음에 나오는 보다 자세한 설명과 예에 대한 소개로서 설명되어 있습니다.

토픽 발행 및 구독에 관련된 여러 컴포넌트가 있습니다. 이들 간의 일부 보안 관계는 [418 페이지의 그림 22](#)에 표시되고 다음 예에 설명됩니다.



토픽

토픽은 토픽 문자열로 식별되며, 일반적으로 트리로 구성됩니다(토픽 트리참조). 토픽에 대한 액세스를 제어하려면 토픽을 토픽 오브젝트와 연관시켜야 합니다. 420 페이지의 『토픽 보안 모델』에서는 토픽 오브젝트를 사용하여 토픽을 보안 설정하는 방법을 설명합니다.

관리 토픽 오브젝트

관리 토픽 오브젝트 목록과 함께 **setmqaut** 명령을 사용하여 누가 어떤 용도로 토픽에 대한 액세스를 가지는지를 제어할 수 있습니다. 예 424 페이지의 『토픽 구독을 위해 사용자에게 액세스 부여』 및 431 페이지의 『토픽에 발행을 위해 사용자에게 액세스 부여』의 내용을 참조하십시오. **z/OS** z/OS에서 토픽 오브젝트에 대한 액세스 제어는 토픽 보안을 위한 프로파일을 참조하십시오.

구독

토픽 문자열을 제공하는 구독을 작성하여 하나 이상의 토픽을 구독하십시오. 여기에는 토픽 문자열을 발행물의 토픽 문자열과 일치시키기 위한 와일드카드가 포함될 수 있습니다. 자세한 내용은 다음을 참조하십시오.

토픽 오브젝트를 사용하여 구독

421 페이지의 『토픽 오브젝트 이름을 사용하여 구독』

토픽을 사용하여 구독

422 페이지의 『토픽 노드가 없는 토픽 문자열을 사용한 구독』

와일드카드와 함께 토픽을 사용하여 구독

422 페이지의 『와일드카드 문자가 포함된 토픽 문자열을 사용한 구독』

구독에는 구독자의 ID와 발행물 배치될 목적지 큐의 ID에 대한 정보가 포함됩니다. 또한 목적지 큐에 발행을 배치하는 방법에 대한 정보가 있습니다.

특정 토픽을 구독하는 권한이 있는 구독자를 정의하고 개별 구독자가 사용하는 구독을 제한할 수 있습니다. 또한 발행이 목적지 큐에 있을 때 큐 관리자가 사용하는 구독자 정보를 제어할 수 있습니다. [436 페이지의 『구독 보안』](#)의 내용을 참조하십시오.

큐

목적지 큐는 보안을 설정할 중요한 큐입니다. 이 큐는 구독자에 대해 로컬이며 구독과 일치한 발행이 해당 큐에 배치됩니다. 두 가지 관점에서 목적지 큐에 대한 액세스를 고려해야 합니다.

1. 발행을 목적지 큐에 넣습니다.
2. 목적지 큐에서 발행을 가져옵니다.

큐 관리자가 구독자가 제공한 ID를 사용하여 목적지 큐에 발행을 넣습니다. 구독자, 또는 발행을 가져오는 태스크를 위임받은 프로그램이 큐에서 메시지를 가져옵니다. [422 페이지의 『목적지 큐에 대한 권한』](#)의 내용을 참조하십시오.

토픽 오브젝트 알리어스가 없지만 알리어스 큐를 토픽 오브젝트의 알리어스로 사용할 수 있습니다. 사용하는 경우, 큐 관리자는 발행 또는 구독에 토픽을 사용할 수 있는 권한 및 큐 사용 권한을 검사합니다.

438 페이지의 『큐 관리자 간의 발행/구독 보안』

토픽 발행 또는 구독 권한은 로컬 ID 및 권한을 사용하여 로컬 큐 관리자에서 검사합니다. 권한은 토픽을 정의하는지의 여부나 정의된 위치에 관계없이 사용합니다. 그 결과 클러스터된 토픽을 사용할 때 클러스터의 모든 큐 관리자에서 토픽 권한을 수행해야 합니다.

참고: 토픽의 보안 모델은 큐의 보안 모델과는 다릅니다. 클러스터된 모든 큐에 로컬로 큐 알리어스를 정의하여 큐에 대한 동일한 결과를 얻을 수 있습니다.

큐 관리자는 클러스터에서 구독을 교환합니다. 대부분의 IBM MQ 클러스터 구성에서 채널은 채널 프로세스의 권한을 사용하여 메시지를 대상 큐에 놓기 위해 PUTAUT=DEF로 구성됩니다. PUTAUT=CTX를 사용하여 구독 중인 사용자가 클러스터에 있는 또 다른 큐 관리자에 구독을 전달하는 권한을 갖도록 채널 구성을 수정할 수 있습니다.

[438 페이지의 『큐 관리자 간의 발행/구독 보안』](#)에서는 클러스터의 다른 서버에 구독을 전파할 수 있는 사용자를 제어하도록 채널 정의를 변경하는 방법에 대해 설명합니다.

권한 부여

큐 및 다른 오브젝트와 같은 토픽 오브젝트에 권한을 적용할 수 있습니다. 토픽에만 적용할 수 있는 세 가지 권한 부여 조작 pub, sub 및 resume이 있습니다. 세부사항은 [여러 오브젝트 유형에 권한 지정에 설명되어](#) 있습니다.

합수 호출

큐된 프로그램과 같은 발행 및 구독 프로그램에서, 오브젝트를 열거나, 작성하거나, 변경하거나, 삭제할 때 권한 검사가 이루어집니다. 발행을 넣고 가져오도록 MQPUT 또는 MQGET MQI 호출이 이루어지는 경우에는 검사가 수행되지 않습니다.

토픽을 발행하려면 권한 검사를 수행하는 토픽에서 MQOPEN을 수행하십시오. 권한 검사를 수행하지 않는 MQPUT 명령을 사용하여 토픽 핸들에 메시지를 발행합니다.

토픽을 구독하려면 일반적으로 MQSUB 명령을 수행하여 구독을 작성하거나 재개하고, 발행을 수신하기 위해 목적지 큐를 엽니다. 또는 개별 MQOPEN을 수행하여 목적지 큐를 연 다음 MQSUB를 수행하여 구독을 작성하거나 재개합니다.

사용하는 호출에 관계없이 큐 관리자는 사용자가 토픽을 구독할 수 있고 목적지 큐에서 결과 발행을 가져올 수 있음을 확인합니다. 목적지 큐가 관리되지 않는 경우, 큐 관리자가 목적지 큐에 발행을 배치할 수 있는 권한 검사도 수행되며 이 큐 관리자는 일치하는 구독에서 채택한 ID를 사용합니다. 큐 관리자는 항상 관리 대상 목적지 큐에 발행을 배치할 수 있다고 가정합니다.

역할

사용자는 실행 중인 발행/구독 애플리케이션의 네 가지 역할에 관련되어 있습니다.

1. 발행자

- 2. 구독자
- 3. 토픽 관리자
- 4. IBM MQ 관리자 - 그룹 mqm의 멤버

발행, 구독 및 토픽 관리 역할에 해당하는 적절한 권한을 가진 그룹을 정의하십시오. 그 다음 특정 발행 및 구독 태스크를 수행하도록 권한을 부여하여 프린시펄을 이러한 그룹에 지정할 수 있습니다.

또한 관리 조작 권한을 발행 및 구독을 이동시키는 큐 및 채널의 관리자로 확장해야 합니다.

토픽 보안 모델

정의된 토픽 오브젝트에만 연관된 보안 속성이 있습니다. 토픽 오브젝트에 대한 설명은 [관리 토픽 오브젝트](#)를 참조하십시오. 보안 속성은 지정된 사용자 ID 또는 보안 그룹이 각 토픽 오브젝트에서 구독 또는 발행 조작을 수행할 수 있는지의 여부를 지정합니다.

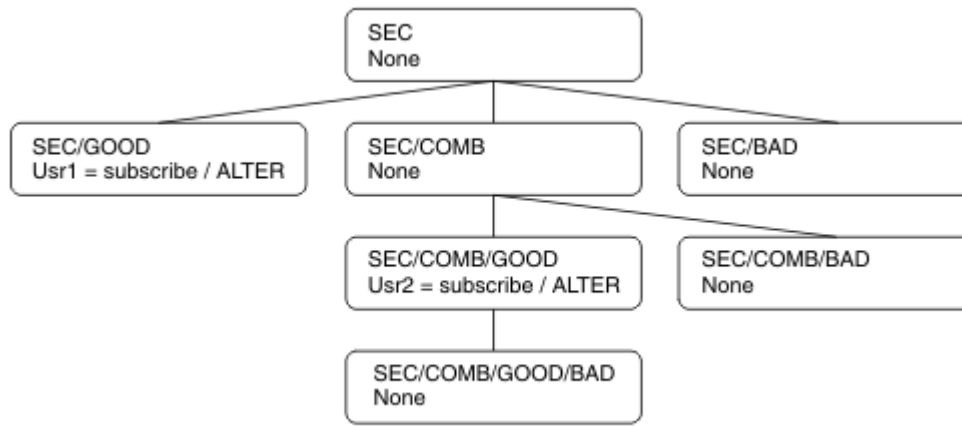
보안 속성은 토픽 트리의 적절한 관리 노드와 연관되어 있습니다. 구독 또는 발행 조작 중에 특정 사용자 ID에 대한 권한 검사가 이루어지는 경우, 부여된 권한은 연관된 토픽 트리 노드의 보안 속성을 기반으로 합니다.

보안 속성은 특정 운영 체제 사용자 ID 또는 보안 그룹이 토픽 오브젝트에 대해 가진 권한을 나타내는 액세스 제어 목록입니다.

표시된 보안 속성 또는 권한으로 토픽 오브젝트를 정의한 다음 예를 고려하십시오.

표 80. 토픽 오브젝트 권한의 예			
토픽 이름	토픽 문자열	권한 - z/OS가 아님	z/OS 권한
SECR00T	SEC	없음	없음
SECGOOD	SEC/GOOD	usr1+subscribe	ALTER HLQ.SUBSCRIBE.SECGOOD
SECBAD	SEC/BAD	없음	없음 HLQ.SUBSCRIBE.SECBAD
SECCOMB	SEC/COMB	없음	없음 HLQ.SUBSCRIBE.SECCOMB
SECCOMBB	SEC/COMB/ GOOD/BAD	없음	없음 HLQ.SUBSCRIBE.SECCOMBB
SECCOMBG	SEC/COMB/GOOD	usr2+subscribe	ALTER HLQ.SUBSCRIBE.SECCOMBG
SECCOMBN	SEC/COMB/BAD	없음	없음 HLQ.SUBSCRIBE.SECCOMBN

각 노드에 있는 연관된 보안 속성을 가진 토픽 트리를 다음과 같이 표시할 수 있습니다.



나열된 예에서는 다음 권한을 제공합니다.

- 트리 /SEC의 루트 노드에서 사용자에게 해당 노드의 권한이 없습니다.
- `usr1`에는 오브젝트 /SEC/GOOD에 대한 구독 권한이 부여되었습니다.
- `usr2`에는 오브젝트 /SEC/COMB/GOOD에 대한 구독 권한이 부여되었습니다.

토픽 오브젝트 이름을 사용하여 구독

MQCHAR48 이름을 지정하여 토픽 오브젝트를 구독할 때 토픽 트리의 해당 노드를 찾았습니다. 노드와 연관된 보안 속성이 사용자에게 구독 권한이 있음을 나타내면, 액세스가 부여됩니다.

사용자에게 액세스가 부여되지 않은 경우, 트리의 상위 노드가 사용자에게 상위 노드 레벨에서 구독할 수 있는 권한이 있는지의 여부를 판별합니다. 권한이 있는 경우, 액세스가 부여됩니다. 권한이 없는 경우에는 해당 노드의 상위 노드가 고려됩니다. 사용자에게 구독 권한을 부여하는 노드를 찾을 때까지 순환이 계속됩니다. 권한이 부여되지 않고 루트 노드를 고려하는 경우에는 순환이 중지됩니다. 후자의 경우, 액세스가 거부됩니다.

즉, 경로에 있는 임의의 노드가 사용자 또는 애플리케이션에 구독 권한을 부여하는 경우, 구독자는 해당 노드 또는 토픽 트리의 해당 노드 아래에서 구독할 수 있습니다.

예의 루트 노드는 SEC입니다.

액세스 제어 목록이 사용자 ID에 권한이 있거나 사용자 ID가 구성원인 운영 체제 보안 그룹에 권한이 있음을 나타내는 경우 사용자에게 구독 권한이 부여됩니다.

예:

- `usr1`이 토픽 문자열 SEC/GOOD을 사용하여 구독하려는 경우, 사용자 ID에 해당 토픽과 연관된 노드에 대한 액세스 권한이 있으므로 구독이 허용됩니다. 하지만, `usr1`이 토픽 문자열 SEC/COMB/GOOD을 사용하여 구독하려는 경우, 사용자 ID에 연관된 노드에 대한 액세스 권한이 없으므로 구독이 허용되지 않습니다.
- `usr2`가 토픽 문자열 SEC/COMB/GOOD을 사용하여 구독하려는 경우, 사용자 ID에 토픽과 연관된 노드에 대한 액세스 권한이 있으므로 구독이 허용됩니다. 하지만, `usr2`가 SEC/GOOD을 구독하려는 경우, 사용자 ID에 연관된 노드에 대한 액세스 권한이 없으므로 구독이 허용되지 않습니다.
- `usr2`가 토픽 문자열 SEC/COMB/GOOD/BAD를 사용하여 구독하려는 경우, 사용자 ID에 상위 노드 SEC/COMB/GOOD에 대한 액세스 권한이 있으므로 구독이 허용됩니다.
- `usr1` 또는 `usr2`가 토픽 문자열 /SEC/COMB/BAD를 사용하여 구독하려는 경우, 연관된 토픽 노드 또는 해당 토픽의 상위 노드에 대한 액세스 권한이 없으므로 두 구독 모두 허용되지 않습니다.

존재하지 않는 토픽 오브젝트의 이름을 지정하는 구독 조작으로 인해 MQRC_UNKNOWN_OBJECT_NAME 오류가 발생합니다.

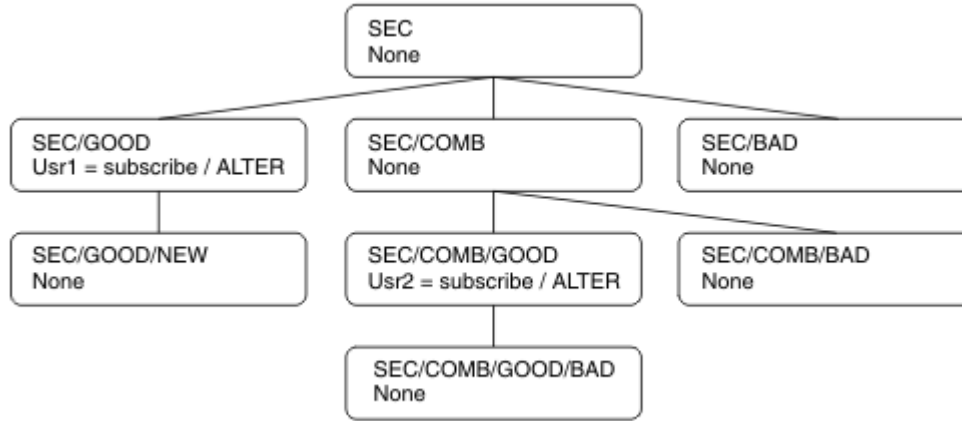
토픽 노드가 있는 토픽 문자열을 사용한 구독

작동은 토픽을 MQCHAR48 오브젝트 이름으로 지정할 때와 동일합니다.

토픽 노드가 없는 토픽 문자열을 사용한 구독

토픽 트리에 현재 없는 토픽 노드를 나타내는 토픽 문자열을 지정하여 구독하는 애플리케이션의 경우를 고려하십시오. 이전 절에 간단하게 설명된 대로 권한 검사를 수행합니다. 검사는 토픽 문자열로 표시되는 토픽의 상위 노드에서 시작합니다. 권한이 부여되는 경우, 토픽 문자열을 표시하는 새 노드가 토픽 트리에서 작성됩니다.

예를 들어, `usr1`은 토픽 `SEC/GOOD/NEW`를 구독하려 합니다. `usr1`에 상위 노드 `SEC/GOOD`에 대한 액세스 권한이 있으므로 권한이 부여됩니다. 새 토픽 노드는 다음 다이어그램에 표시된 대로 트리에 작성됩니다. 새 토픽 노드는 보안 속성이 직접 연관되지 않은 토픽 오브젝트가 아닙니다. 속성은 상위에서 상속됩니다.



와일드카드 문자가 포함된 토픽 문자열을 사용한 구독

와일드카드 문자가 포함된 토픽 문자열을 사용한 구독의 경우를 고려하십시오. 토픽 문자열의 완전히 규정된 부분과 일치하는 토픽 트리의 노드에서 권한 검사가 수행됩니다.

애플리케이션이 `SEC/COMB/GOOD/*`를 구독하는 경우, 토픽 트리의 노드 `SEC/COMB/GOOD`에 있는 두 개의 이전 절에 설명된 대로 권한 검사를 수행합니다.

이와 유사하게 애플리케이션이 `SEC/COMB/*/GOOD`를 구독해야 하는 경우, 노드 `SEC/COMB`에서 권한 검사가 수행됩니다.

목적지 큐에 대한 권한

토픽을 구독할 때 매개변수 중 하나는 발행물을 수신하기 위해 출력을 위해 열려 있는 큐의 핸들 `hobj`입니다.

`hobj`가 지정되지 않았지만 공백인 경우 다음 조건이 적용되면 관리 대상 큐가 작성됩니다.

- `MQSO_MANAGED` 옵션을 지정했습니다.
- 구독이 없습니다.
- 작성이 지정되어 있습니다.

`hobj`가 공백이고 기존 구독을 변경하거나 재개하는 경우, 이전에 제공된 목적지 큐는 관리되거나 관리되지 않는 큐일 수 있습니다.

`MQSUB` 요청을 작성하는 애플리케이션 또는 사용자에게 제공된 목적지 큐에 메시지를 넣을 수 있는 권한(사실상 해당 큐에 넣은 메시지를 발행하는 권한)이 있어야 합니다. 권한 검사는 큐 보안 검사에 대한 기존 규칙을 따릅니다.

보안 검사에는 필요에 따라 대체 사용자 ID 및 컨텍스트 보안 검사가 포함됩니다. ID 컨텍스트 필드 중 하나를 설정할 수 있도록 `MQSO_SET_IDENTITY_CONTEXT` 옵션 및 `MQSO_CREATE` 또는 `MQSO_ALTER` 옵션을 지정해야 합니다. `MQSO_RESUME` 요청에서 ID 컨텍스트 필드 중 하나를 설정할 수 없습니다.

목적지가 관리 대상 큐인 경우, 관리 대상 목적지에 대해 보안 검사가 수행되지 않습니다. 토픽을 구독할 수 있는 경우 관리 대상 목적지를 사용할 수 있다고 가정합니다.

토픽 노드가 있는 토픽 이름 또는 토픽 문자열을 사용한 발행

발행을 위한 보안 모델은 와일드카드 문자를 제외하고는 구독을 위한 보안 모델과 동일합니다. 발행에는 와일드카드 문자가 포함되지 않으므로 와일드카드 문자가 포함된 토픽 문자열을 고려하는 경우는 없습니다.

발행할 권한과 구독할 권한은 별개입니다. 사용자 또는 그룹에는 발행 또는 구독 중 하나를 수행할 수 없어도 다른 하나를 수행할 수 있는 권한이 있습니다.

MQCHAR48 이름 또는 토픽 문자열을 지정하여 토픽 오브젝트를 발행할 때 토픽 트리의 해당 노드를 찾았습니다. 토픽 노드와 연관된 보안 속성이 사용자에게 발행 권한이 있음을 나타내면, 액세스가 부여됩니다.

액세스가 부여되지 않은 경우, 트리의 상위 노드가 사용자에게 해당 레벨에서 발행할 수 있는 권한이 있는지의 여부를 판별합니다. 권한이 있는 경우, 액세스가 부여됩니다. 권한이 없는 경우, 사용자에게 발행 권한을 부여하는 노드를 찾을 때까지 순환이 계속됩니다. 권한이 부여되지 않고 루트 노드를 고려하는 경우에는 순환이 중지됩니다. 후자의 경우, 액세스가 거부됩니다.

즉, 경로에 있는 임의의 노드가 사용자 또는 애플리케이션에 발행할 권한을 부여하는 경우, 발행자는 해당 노드 또는 토픽 트리의 해당 노드 아래에서 발행할 수 있습니다.

토픽 노드가 없는 토픽 이름 또는 토픽 문자열을 사용한 발행

구독 조작에서와 같이, 애플리케이션이 토픽 트리에 현재 없는 토픽 노드를 나타내는 토픽 문자열을 지정하여 발행할 때 토픽 문자열로 표시되는 노드의 상위부터 시작하여 보안 검사를 수행합니다. 권한이 부여되는 경우, 토픽 문자열을 표시하는 새 노드가 토픽 트리에서 작성됩니다.

토픽 오브젝트로 해석되는 알리어스 큐를 사용한 발행

토픽 오브젝트로 해석되는 알리어스 큐를 사용하여 발행하는 경우, 알리어스 큐 및 이 큐가 해석되는 기본 토픽 모두에서 보안 검사가 수행됩니다.

알리어스 큐에서 보안 검사를 수행하면 사용자에게 해당 알리어스 큐에 메시지를 넣을 수 있는 권한이 있는지 확인 가능하고, 토픽에 대한 보안 검사를 수행하면 사용자가 해당 토픽을 발행할 수 있는지 확인 가능합니다. 알리어스 큐가 다른 큐로 해석되는 경우, 기본 큐에서는 검사를 수행하지 않습니다. 토픽에 대한 권한 검사와 큐에 대한 권한 검사는 서로 다르게 수행됩니다.

구독 종료

이 핸들에서 구독을 작성하지 않으면 MQCO_REMOVE_SUB 옵션을 사용하여 구독을 종료하는 경우 추가 보안 검사가 수행됩니다.

조치로 인해 구독이 제거되므로 이를 수행할 수 있는 올바른 권한이 있는지 확인하기 위해 보안 검사를 수행합니다. 토픽 노드와 연관된 보안 속성이 사용자에게 권한이 있음을 나타내는 경우, 액세스가 부여됩니다. 권한이 없는 경우, 트리의 상위 노드가 사용자에게 구독을 종료할 수 있는 권한이 있는지의 여부를 판별합니다. 권한이 부여되거나 루트 노드에 도달할 때까지 순환이 계속됩니다.

구독 정의, 대체 및 삭제

MQSUB API 요청을 사용하지 않고 구독이 관리 면에서 작성되는 경우 구독 보안 검사가 수행되지 않습니다. 관리자는 이미 명령을 통해 해당 권한을 받았습니다.

구독과 연관된 목적지 큐에 발행을 넣을 수 있는지 확인하기 위해 보안 검사를 수행합니다. 검사는 MQSUB 요청의 경우와 동일한 방식으로 수행됩니다.

이러한 보안 검사에 사용된 사용자 ID는 발행될 명령에 따라 달라집니다. **SUBUSER** 매개변수를 지정한 경우, 424 페이지의 표 81에 표시된 대로 검사 수행 방식에 영향을 줍니다.

명령	SUBUSER 지정 및 공백	SUBUSER 지정 및 완료	SUBUSER가 지정되지 않음
	관리자 ID 사용		LIKE 구독으로부터 사용자 ID 사용
	관리자 ID 사용		SYSTEM.DEFAULT.SUB 구독으로부터 사용자 ID 사용 - 공백이면 관리자 ID 사용
	관리자 ID 사용		기존 구독에서 사용자 ID 사용

DELETE SUB 명령을 사용하여 구독을 삭제할 때 수행된 보안 검사만 명령 보안 검사입니다.

발행/구독 보안 설정 예

이 절에서는 보안 제어를 필요에 따라 적용할 수 있는 방식으로 토픽에 대해 액세스 제어가 설정되어 있는 시나리오에 대해 설명합니다.

토픽 구독을 위해 사용자에게 액세스 부여

이 주제는 두 명 이상의 사용자에게 의해 토픽에 대한 액세스를 부여하는 방법을 설명하는 태스크 목록의 첫 번째 항목입니다.

이 태스크 정보

이 태스크는 관리 토픽 오브젝트가 존재하지 않으며 구독 또는 발행용으로 정의된 프로파일도 없다고 가정합니다. 애플리케이션은 기존 구독을 계속하기보다 새 구독을 작성하며 토픽 문자열만을 사용하여 이를 수행합니다.

애플리케이션은 토픽 오브젝트, 토픽 문자열 또는 둘의 조합을 제공하여 구독을 작성할 수 있습니다. 애플리케이션이 선택하는 어떤 방법이든지 그 영향은 토픽 트리의 특정 지점에서 구독을 작성하는 것입니다. 토픽 트리의 이 지점이 관리 토픽 오브젝트에 의해 표시될 경우 보안 프로파일은 해당 토픽 오브젝트의 이름을 기반으로 선택됩니다.

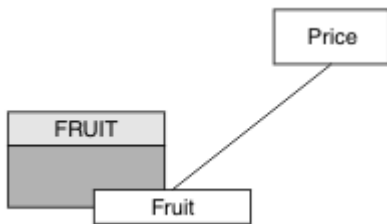


그림 23. 토픽 오브젝트 액세스의 예

주제	필요한 구독 액세스	토픽 오브젝트
Price	사용자 없음	없음
Price/Fruit	USER1	과일

다음과 같이 새 토픽 오브젝트를 정의하십시오.

프로시저

1. MQSC 명령 `DEF TOPIC(FRUIT) TOPICSTR('Price/Fruit')`를 발행하십시오.
2. 다음과 같이 액세스를 부여하십시오.

- **z/OS** z/OS :

hlq.SUBSCRIBE.FRUIT 프로파일에 대한 사용자 액세스를 부여하여 "Price/Fruit" 토픽을 구독하기 위해 USER1에 액세스를 부여하십시오. 이를 수행하려면 다음 RACF 명령을 사용하여 다음을 수행하십시오.

```
RDEFINE MXTOPIC hlq.SUBSCRIBE.FRUIT UACC(NONE)
PERMIT hlq.SUBSCRIBE.FRUIT CLASS(MXTOPIC) ID(USER1) ACCESS(ALTER)
```

- 기타 플랫폼의 경우:

FRUIT 오브젝트에 대한 사용자 액세스를 부여하여 "Price/Fruit" 토픽을 구독하기 위해 USER1에 액세스를 부여하십시오. 플랫폼에 대한 권한 부여 명령을 사용하여 다음을 수행하십시오.

- **ULW** Windows, UNIX and Linux 시스템

```
setmqaut -t topic -n FRUIT -p USER1 +sub
```

- **IBM i** IBM i

```
GRTRMQUAUT OBJ(FRUIT) OBJTYPE(*TOPIC) USER(USER1) AUT(*SUB)
```

결과

USER1이 토픽 "Price/Fruit"를 구독하려고 시도하면 결과는 성공입니다.

USER2가 토픽 "Price/Fruit"를 구독하려고 시도할 때 결과는 다음 및 MQRC_NOT_AUTHORIZED 메시지와 함께 실패합니다.

- **z/OS** z/OS에서는 시도한 토픽 트리를 통해 전체 보안 경로를 표시하는 콘솔에 다음 메시지가 표시됩니다.

```
ICH408I USER(USER2 ) ...
hlq.SUBSCRIBE.FRUIT ...

ICH408I USER(USER2 ) ...
hlq.SUBSCRIBE.SYSTEM.BASE.TOPIC ...
```

- **ULW** 기타 플랫폼에서는 다음 권한 부여 이벤트가 제공됩니다.

```
MQRC_NOT_AUTHORIZED
ReasonQualifier      MQRC_SUB_NOT_AUTHORIZED
UserIdentifier       USER2
AdminTopicNames     FRUIT, SYSTEM.BASE.TOPIC
TopicString          "Price/Fruit"
```

- **IBM i** IBMi에서는 다음 권한 부여 이벤트가 제공됩니다.

```
MQRC_NOT_AUTHORIZED
ReasonQualifier      MQRC_SUB_NOT_AUTHORIZED
UserIdentifier       USER2
```

```
AdminTopicNames    FRUIT, SYSTEM.BASE.TOPIC
TopicString        "Price/Fruit"
```

이는 전체 필드가 아닌 사용자에게 표시되는 그림입니다.

트리 내에서 더 깊은 토픽을 구독할 수 있는 액세스를 사용자에게 부여

이 주제는 두 명 이상의 사용자에게 의해 토픽에 대한 액세스를 부여하는 방법을 설명하는 태스크 목록의 두 번째 항목입니다.

시작하기 전에

이 주제에서는 424 페이지의 『토픽 구독을 위해 사용자에게 액세스 부여』에 설명된 설정을 사용합니다.

이 태스크 정보

애플리케이션이 구독을 작성하는 토픽 트리에서의 지점이 관리 토픽 오브젝트에 의해 표시되지 않으면 가장 가까운 상위 관리 토픽 오브젝트를 찾을 때까지 트리 위로 이동하십시오. 보안 프로파일은 해당 토픽 오브젝트의 이름을 기반으로 검사됩니다.

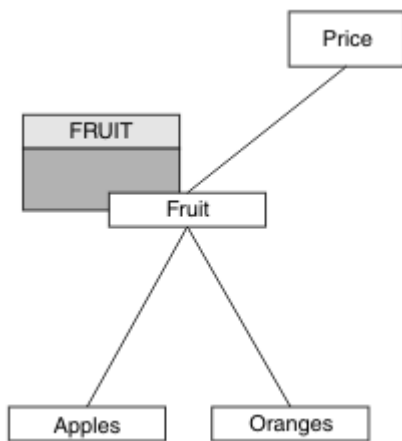


그림 24. 토픽 트리 내에서 토픽에 대한 액세스 부여의 예

표 83. 예제 토픽 및 토픽 오브젝트에 대한 액세스 요구사항		
주제	필요한 구독 액세스	토픽 오브젝트
Price	사용자 없음	없음
Price/Fruit	USER1	과일
Price/Fruit/ Apples	USER1	
Price/Fruit/ Oranges	USER1	

이전 태스크 USER1에서 z/OS의 hlq.SUBSCRIBE.FRUIT 프로파일에 대한 액세스 권한을 부여하고 다른 플랫폼의 FRUIT 프로파일에 대한 등록 액세스 권한을 부여하여 "Price/Fruit" 토픽에 대한 등록에 대한 액세스가 부여되었습니다. 이 단일 프로파일은 또한 "Price/Fruit/Apples", "Price/Fruit/Oranges" 및 "Price/Fruit/#"를 구독하기 위한 USER1 액세스를 부여합니다.

USER1이 토픽 "Price/Fruit/Apples"를 구독하려고 시도하면 결과는 성공입니다.

USER2가 토픽 "Price/Fruit/Apples"를 구독하려고 시도할 때 결과는 다음 및 MQRC_NOT_AUTHORIZED 메시지와 함께 실패합니다.

- z/OS에서는 시도한 토픽 트리를 통해 전체 보안 경로를 표시하는 콘솔에 다음 메시지가 표시됩니다.

```

ICH408I USER(USER2 ) ...
hlq.SUBSCRIBE.FRUIT ...

ICH408I USER(USER2 ) ...
hlq.SUBSCRIBE.SYSTEM.BASE.TOPIC ...

```

- 기타 플랫폼에서는 다음 권한 부여 이벤트가 제공됩니다.

```

MQRC_NOT_AUTHORIZED
ReasonQualifier      MQRC_SUB_NOT_AUTHORIZED
UserIdentifier       USER2
AdminTopicNames     FRUIT, SYSTEM.BASE.TOPIC
TopicString          "Price/Fruit/Apples"

```

다음에 유의하십시오.

- z/OS에서 수신한 메시지는 이전 태스크에서 수신한 메시지와 동일합니다. 동일한 토픽 오브젝트 및 프로파일 이 액세스를 제어 중이기 때문입니다.
- 다른 플랫폼에서 수신한 이벤트 메시지는 이전 태스크에서 수신한 메시지와 유사하지만 실제 토픽 문자열은 다릅니다.

트리 내에서 더 깊은 토픽만 구독할 수 있는 또 다른 사용자 액세스 부여

이 주제는 두 명 이상의 사용자가 토픽을 구독할 수 있는 액세스를 부여하는 방법을 설명하는 태스크 목록의 세 번째 항목입니다.

시작하기 전에

이 주제에서는 426 페이지의 『트리 내에서 더 깊은 토픽을 구독할 수 있는 액세스를 사용자에게 부여』에 설명된 설정을 사용합니다.

이 태스크 정보

이전 태스크에서 USER2가 토픽 "Price/Fruit/Apples"에 대한 액세스가 거부되었습니다. 이 주제에서는 다른 토픽이 아닌 해당 토픽에 대한 액세스를 부여하는 방법을 알려줍니다.

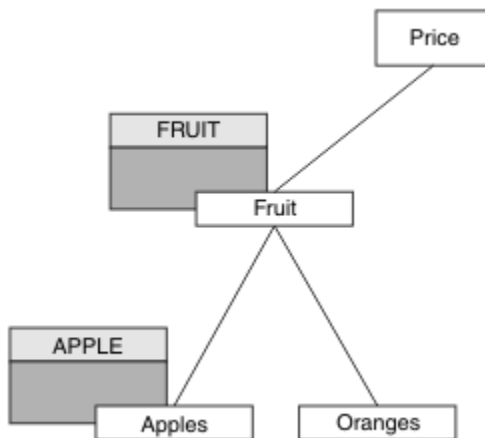


그림 25. 토픽 트리 내에서 특정 토픽에 대한 액세스 부여

표 84. 예제 토픽 및 토픽 오브젝트에 대한 액세스 요구사항		
주제	필요한 구독 액세스	토픽 오브젝트
Price	사용자 없음	없음

표 84. 예제 토픽 및 토픽 오브젝트에 대한 액세스 요구사항 (계속)		
주제	필요한 구독 액세스	토픽 오브젝트
Price/Fruit	USER1	과일
Price/Fruit/ Apples	USER1 및 USER2	APPLE
Price/Fruit/ Oranges	USER1	

다음과 같이 새 토픽 오브젝트를 정의하십시오.

프로시저

- MQSC 명령 `DEF TOPIC(APPLE) TOPICSTR('Price/Fruit/Apples')`을 실행하십시오.
- 다음과 같이 액세스를 부여하십시오.

- ▶ **z/OS** **z/OS :**

이전 태스크에서 USER1는 `hlq.SUBSCRIBE.FRUIT` 프로파일에 대한 사용자 액세스를 부여하여 토픽 "Price/Fruit/Apples"를 구독할 수 있는 액세스가 부여되었습니다.

이 단일 프로파일에는 또한 "Price/Fruit/Oranges" "Price/Fruit/#"를 구독할 수 있는 USER1 액세스가 부여되고 이 액세스는 새 토픽 오브젝트 및 이와 연관된 프로파일을 추가하는 경우에도 남습니다.

`hlq.SUBSCRIBE.APPLE` 프로파일에 대한 사용자 액세스를 부여하여 "Price/Fruit/Apples" 토픽을 구독하기 위해 USER2에 액세스를 부여하십시오. 이를 수행하려면 다음 RACF 명령을 사용하여 다음을 수행하십시오.

```
RDEFINE MXTOPIC hlq.SUBSCRIBE.APPLE UACC(NONE)
PERMIT hlq.SUBSCRIBE.FRUIT APPLE(MXTOPIC) ID(USER2) ACCESS(ALTER)
```

- 기타 플랫폼의 경우:

이전 태스크 USER1는 FRUIT 프로파일에 대한 사용자 구독 액세스를 부여하여 토픽 "Price/Fruit/Apples"를 구독할 수 있는 액세스가 부여되었습니다.

이 단일 프로파일에는 또한 "Price/Fruit/Oranges" 및 "Price/Fruit/#"을 구독할 수 있는 USER1 액세스가 부여되고 이 액세스는 새 토픽 오브젝트 및 이와 연관된 프로파일을 추가하는 경우에도 남습니다.

APPLE 프로파일에 대한 사용자 구독 액세스를 부여하여 "Price/Fruit/Apples" 토픽을 구독하기 위해 USER2에 액세스를 부여하십시오. 플랫폼에 대한 권한 부여 명령을 사용하여 다음을 수행하십시오.

- ▶ **ULW** **Windows, UNIX and Linux 시스템**

```
setmqaut -t topic -n APPLE -p USER2 +sub
```

- ▶ **IBM i** **IBM i**

```
GRTRMQUAUT OBJ(APPLE) OBJTYPE(*TOPIC) USER(USER2) AUT(*SUB)
```

결과

z/OS에서, USER1이 토픽 "Price/Fruit/Apples"를 구독하려고 시도할 때 hlq.SUBSCRIBE.APPLE 프로파일에서 첫 번째 보안 검사는 실패하지만 트리 위로 이동할 때 hlq.SUBSCRIBE.FRUIT 프로파일은 USER1이 구독하도록 허용하므로 구독은 성공하고 리턴 코드가 MQSUB에 전송되지 않습니다. 그러나 RACF ICH 메시지가 첫 번째 검사에 대해 생성됩니다.

```
ICH408I USER(USER1 ) ...
hlq.SUBSCRIBE.APPLE ...
```

USER2가 토픽 "Price/Fruit/Apples"를 구독하려고 시도할 때 보안 검사가 첫 번째 프로파일에 전달되므로 결과는 성공적입니다.

USER2가 토픽 "Price/Fruit/Oranges"를 구독하려고 시도할 때 결과는 다음 및 MQRC_NOT_AUTHORIZED 메시지와 함께 실패합니다.

- ▶ **z/OS** z/OS에서는 시도한 토픽 트리를 통해 전체 보안 경로를 표시하는 콘솔에 다음 메시지가 표시됩니다.

```
ICH408I USER(USER2 ) ...
hlq.SUBSCRIBE.FRUIT ...

ICH408I USER(USER2 ) ...
hlq.SUBSCRIBE.SYSTEM.BASE.TOPIC ...
```

- ▶ **ULW** Windows, UNIX and Linux 플랫폼에서는 다음 권한 부여 이벤트가 제공됩니다.

```
MQRC_NOT_AUTHORIZED
ReasonQualifier      MQRC_SUB_NOT_AUTHORIZED
UserIdentifier       USER2
AdminTopicNames     FRUIT, SYSTEM.BASE.TOPIC
TopicString          "Price/Fruit/Oranges"
```

- ▶ **IBMi** IBMi에서는 다음 권한 부여 이벤트가 제공됩니다.

```
MQRC_NOT_AUTHORIZED
ReasonQualifier      MQRC_SUB_NOT_AUTHORIZED
UserIdentifier       USER2
AdminTopicNames     FRUIT, SYSTEM.BASE.TOPIC
TopicString          "Price/Fruit/Oranges"
```

이 설정의 단점은 z/OS에서는 콘솔에서 추가 ICH 메시지를 받는다는 점입니다. 토픽 트리를 다른 방법으로 보안 설정하면 이를 피할 수 있습니다.

추가 메시지를 방지하기 위한 액세스 제어 변경

이 주제는 둘 이상의 사용자가 토픽을 구독하기 위해 액세스를 부여하고 z/OS에서 추가 RACF ICH408I 메시지를 피하는 방법을 설명하는 태스크 목록에서 네 번째입니다.

시작하기 전에

이 주제는 추가 오류 메시지를 방지할 수 있도록 427 페이지의 『트리 내에서 더 깊은 토픽만 구독할 수 있는 또 다른 사용자 액세스 부여』에 설명된 설정을 개선합니다.

이 태스크 정보

이 주제에서는 트리에서 더 깊은 토픽에 대한 액세스를 부여하는 방법과 이를 필요로 하는 사용자가 없을 때 트리의 더 아래쪽 토픽에 대한 액세스를 제거하는 방법을 알려줍니다.

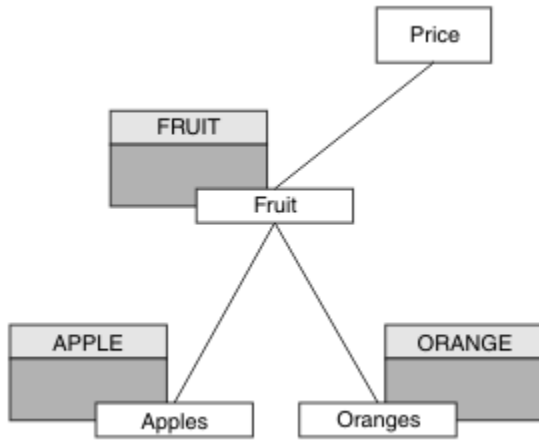


그림 26. 추가 메시지를 방지하기 위해 액세스 제어를 부여하는 예
다음과 같이 새 토픽 오브젝트를 정의하십시오.

프로시저

1. MQSC 명령 `DEF TOPIC(ORANGE) TOPICSTR('Price/Fruit/Oranges')`을 실행하십시오.
2. 다음과 같이 액세스를 부여하십시오.

z/OS z/OS :

새 프로파일을 정의하고 해당 프로파일 및 기존 프로파일에 대한 액세스를 추가하십시오. 이를 수행하려면 다음 RACF 명령을 사용하여 다음을 수행하십시오.

```
RDEFINE MXTOPIC h1q.SUBSCRIBE.ORANGE UACC(NONE)
PERMIT h1q.SUBSCRIBE.ORANGE CLASS(MXTOPIC) ID(USER1) ACCESS(ALTER)
PERMIT h1q.SUBSCRIBE.APPLE CLASS(MXTOPIC) ID(USER1) ACCESS(ALTER)
```

기타 플랫폼의 경우:

플랫폼의 권한 부여 명령을 사용하여 동등한 액세스를 설정하십시오.

ULW Windows, UNIX and Linux 시스템

```
setmqaut -t topic -n ORANGE -p USER1 +sub
setmqaut -t topic -n APPLE -p USER1 +sub
```

IBM i IBM i

```
GRTMQAUT OBJ(ORANGE) OBJTYPE(*TOPIC) USER(USER1) AUT(*SUB)
GRTMQAUT OBJ(APPLE) OBJTYPE(*TOPIC) USER(USER1) AUT(*SUB)
```

결과

z/OS에서 USER1이 토픽 "Price/Fruit/Apples"를 구독하기 위해 시도할 때 h1q.SUBSCRIBE.APPLE 프로파일에서 첫 번째 보안 검사가 성공합니다.

마찬가지로, USER2가 토픽 "Price/Fruit/Apples"를 구독하려고 시도할 때 보안 검사가 첫 번째 프로파일에 전달되므로 결과는 성공적입니다.

USER2가 토픽 "Price/Fruit/Oranges"를 구독하려고 시도할 때 결과는 다음 및 MQRC_NOT_AUTHORIZED 메시지와 함께 실패합니다.

- ▶ **z/OS** z/OS에서는 시도한 토픽 트리를 통해 전체 보안 경로를 표시하는 콘솔에 다음 메시지가 표시됩니다.

```

ICH408I USER(USER2 ) ...
hlq.SUBSCRIBE.ORANGE ...

ICH408I USER(USER2 ) ...
hlq.SUBSCRIBE.FRUIT ...

ICH408I USER(USER2 ) ...
hlq.SUBSCRIBE.SYSTEM.BASE.TOPIC ...

```

- ▶ **ULW** 기타 플랫폼에서는 다음 권한 부여 이벤트가 제공됩니다.

```

MQRC_NOT_AUTHORIZED
ReasonQualifier      MQRC_SUB_NOT_AUTHORIZED
UserIdentifier       USER2
AdminTopicNames     ORANGE, FRUIT, SYSTEM.BASE.TOPIC
TopicString          "Price/Fruit/Oranges"

```

- ▶ **IBMi** IBMi에서는 다음 권한 부여 이벤트가 제공됩니다.

```

MQRC_NOT_AUTHORIZED
ReasonQualifier      MQRC_SUB_NOT_AUTHORIZED
UserIdentifier       USER2
AdminTopicNames     ORANGE, FRUIT, SYSTEM.BASE.TOPIC
TopicString          "Price/Fruit/Oranges"

```

토픽에 발행을 위해 사용자에게 액세스 부여

이 주제는 두 명 이상의 사용자가 토픽을 발행할 수 있는 액세스를 부여하는 방법을 설명하는 태스크 목록의 첫 번째 항목입니다.

이 태스크 정보

이 태스크는 관리 토픽 오브젝트가 토픽 트리의 오른쪽에 존재하지 않으며 발행용으로 정의된 프로파일도 없다고 가정합니다. 여기서는 발행자가 토픽 문자열만 사용한다는 가정이 사용됩니다.

애플리케이션은 토픽 오브젝트, 토픽 문자열 또는 둘의 조합을 제공하여 토픽을 발행할 수 있습니다. 애플리케이션이 선택하는 어떤 방법이든 그 영향은 토픽 트리의 특정 지점에서 발행하는 것입니다. 토픽 트리의 이 지점이 관리 토픽 오브젝트에 의해 표시될 경우 보안 프로파일은 해당 토픽 오브젝트의 이름을 기반으로 선택됩니다. 예를 들면, 다음과 같습니다.

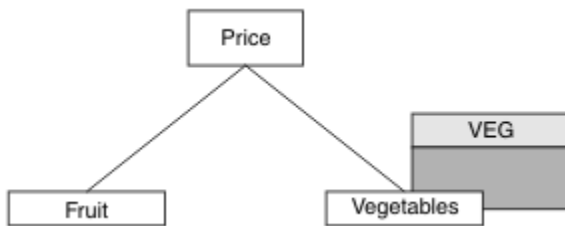


그림 27. 토픽에 대한 발행 액세스 권한 부여

표 85. 발행 액세스 요구사항의 예			
주제	필요한 발행 액세스	토픽 오브젝트	
Price	사용자 없음	없음	
Price/Vegetables	USER1	VEG	

다음과 같이 새 토픽 오브젝트를 정의하십시오.

프로시저

1. MQSC 명령 DEF TOPIC(VEG) TOPICSTR('Price/Vegetables')를 발행하십시오.
2. 다음과 같이 액세스를 부여하십시오.

- **z/OS** z/OS :

hlq.PUBLISH.VEG 프로파일에 대한 사용자 액세스를 부여하여 "Price/Vegetables" 토픽을 발행하기 위해 USER1에 액세스를 부여하십시오. 이를 수행하려면 다음 RACF 명령을 사용하여 다음을 수행하십시오.

```
RDEFINE MXTOPIC hlq.PUBLISH.VEG UACC(NONE)
PERMIT hlq.PUBLISH.VEG CLASS(MXTOPIC) ID(USER1) ACCESS(UPDATE)
```

- 기타 플랫폼의 경우:

VEG 프로파일에 대한 사용자 액세스를 부여하여 "Price/Vegetables" 토픽을 발행하기 위해 USER1에 액세스를 부여하십시오. 플랫폼에 대한 권한 부여 명령을 사용하여 다음을 수행하십시오.

- **ULW** Windows, UNIX and Linux 시스템

```
setmqaut -t topic -n VEG -p USER1 +pub
```

- **IBM i** IBM i

```
GRTMQAUT OBJ(VEG) OBJTYPE(*TOPIC) USER(USER1) AUT(*PUB)
```

결과

USER1이 토픽 "Price/Vegetables"을 발행하려고 시도하면 결과는 성공적입니다. 즉, MQOPEN 호출이 성공합니다.

USER2가 토픽 "Price/Vegetables"을 발행하려고 시도할 때 MQOPEN 호출은 다음 및 MQRC_NOT_AUTHORIZED 메시지와 함께 실패합니다.

- **z/OS** z/OS에서는 시도한 토픽 트리를 통해 전체 보안 경로를 표시하는 콘솔에 다음 메시지가 표시됩니다.

```
ICH408I USER(USER2 ) ...
hlq.PUBLISH.VEG ...

ICH408I USER(USER2 ) ...
hlq.PUBLISH.SYSTEM.BASE.TOPIC ...
```

- **ULW** 기타 플랫폼에서는 다음 권한 부여 이벤트가 제공됩니다.

```
MQRC_NOT_AUTHORIZED
ReasonQualifier      MQRC_OPEN_NOT_AUTHORIZED
UserIdentifier       USER2
AdminTopicNames     VEG, SYSTEM.BASE.TOPIC
TopicString          "Price/Vegetables"
```

- **IBM i** IBMi에서는 다음 권한 부여 이벤트가 제공됩니다.

```
MQRC_NOT_AUTHORIZED
ReasonQualifier      MQRC_OPEN_NOT_AUTHORIZED
UserIdentifier       USER2
AdminTopicNames     VEG, SYSTEM.BASE.TOPIC
TopicString          "Price/Vegetables"
```

이는 전체 필드가 아닌 사용자에게 표시되는 그림입니다.

트리 내에서 더 깊은 토픽에 발행할 수 있는 액세스를 사용자에게 부여

이 주제는 두 명 이상의 사용자가 토픽을 발행할 수 있는 액세스를 부여하는 방법을 설명하는 태스크 목록의 두 번째 항목입니다.

시작하기 전에

이 주제에서는 [431 페이지의 『토픽에 발행을 위해 사용자에게 액세스 부여』](#)에 설명된 설정을 사용합니다.

이 태스크 정보

애플리케이션이 발행하는 토픽 트리에서의 지점이 관리 토픽 오브젝트에 의해 표시되지 않으면 가장 가까운 상위 관리 토픽 오브젝트를 찾을 때까지 트리 위로 이동하십시오. 보안 프로파일은 해당 토픽 오브젝트의 이름을 기반으로 검사됩니다.

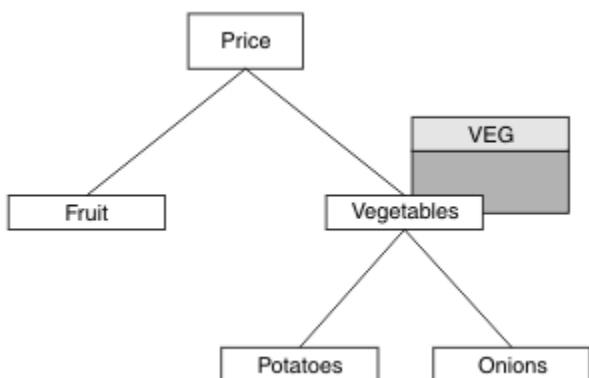


그림 28. 토픽 트리 내에서 토픽에 대한 발행 액세스 부여

표 86. 발행 액세스 요구사항의 예		
주제	필요한 구독 액세스	토픽 오브젝트
Price	사용자 없음	없음
Price/Vegetables	USER1	VEG
Price/ Vegetables/ Potatoes	USER1	
Price/ Vegetables/ Onions	USER1	

In the previous task USER1 was granted access to publish topic "Price/Vegetables/Potatoes" by granting it access to the hlq . PUBLISH . VEG profile on z/OS or publish access to the VEG profile on other platforms. 또한 이 단일 프로파일은 "Price/Vegetables/Onions"에 공개할 수 있는 USER1 액세스 권한을 부여합니다.

USER1이 "Price/Vegetables/Potatoes" 토픽을 발행하려고 시도하면 결과는 성공적입니다. 즉, MQOPEN 호출이 성공합니다.

USER2가 "Price/Vegetables/Potatoes" 토픽을 구독하려고 시도하면 결과는 실패입니다. 즉, MQOPEN 호출은 다음과 함께 MQRC_NOT_AUTHORIZED 메시지와 함께 실패합니다.

- z/OS에서는 시도한 토픽 트리를 통해 전체 보안 경로를 표시하는 콘솔에 다음 메시지가 표시됩니다.

```

ICH408I USER(USER2  ) ...
hlq.PUBLISH.VEG ...

ICH408I USER(USER2  ) ...
hlq.PUBLISH.SYSTEM.BASE.TOPIC ...

```

- 기타 플랫폼에서는 다음 권한 부여 이벤트가 제공됩니다.

```

MQRC_NOT_AUTHORIZED
ReasonQualifier      MQRC_OPEN_NOT_AUTHORIZED
UserIdentifier       USER2
AdminTopicNames     VEG, SYSTEM.BASE.TOPIC
TopicString          "Price/Vegetables/Potatoes"

```

다음에 유의하십시오.

- z/OS에서 수신한 메시지는 이전 태스크에서 수신한 메시지와 동일합니다. 동일한 토픽 오브젝트 및 프로파일 이 액세스를 제어 중이기 때문입니다.
- 다른 플랫폼에서 수신한 이벤트 메시지는 이전 태스크에서 수신한 메시지와 유사하지만 실제 토픽 문자열은 다릅니다.

발행 및 구독을 위한 액세스 부여

이 주제는 두 명 이상의 사용자가 토픽을 발행 및 구독할 수 있는 액세스를 부여하는 방법을 설명하는 태스크 목록의 마지막 항목입니다.

시작하기 전에

이 주제에서는 433 페이지의 『트리 내에서 더 깊은 토픽에 발행할 수 있는 액세스를 사용자에게 부여』에 설명된 설정을 사용합니다.

이 태스크 정보

이전 태스크에서 USER1에게 토픽 "Price/Fruit"를 구독할 수 있는 액세스가 제공되었습니다. 이 주제에서는 사용자에게 해당 토픽에 발행하기 위한 액세스를 부여하는 방법을 알려줍니다.

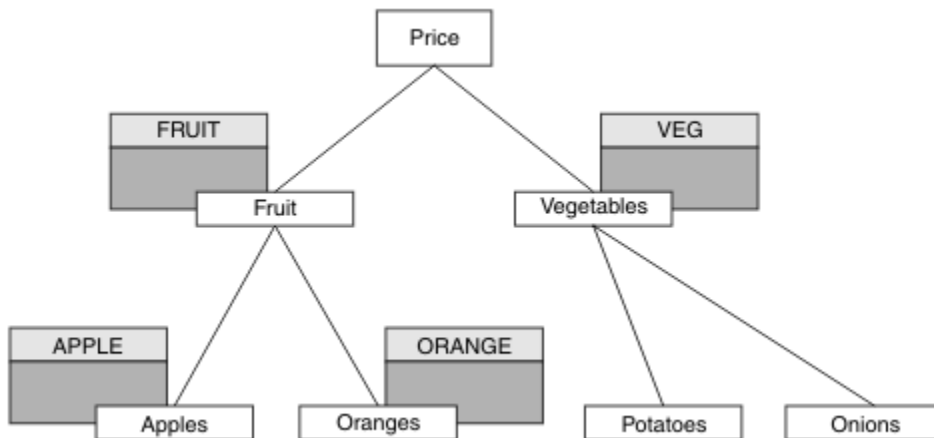


그림 29. 발행 및 구독을 위한 액세스 부여

표 87. 액세스 요구사항 발행 및 구독 예				
주제	필요한 구독 액세스	필요한 발행 액세스	토픽 오브젝트	
Price	사용자 없음	사용자 없음	없음	

표 87. 액세스 요구사항 발행 및 구독 예 (계속)

주제	필요한 구독 액세스	필요한 발행 액세스	토픽 오브젝트
Price/Fruit	USER1	USER1	과일
Price/Fruit/Apples	USER1 및 USER2		APPLE
Price/Fruit/Oranges	USER1		ORANGE

프로시저

다음과 같이 액세스를 부여하십시오.

z/OS z/OS :

이전 태스크에서 USER1는 h1q.SUBSCRIBE.FRUIT 프로파일에 대한 사용자 액세스를 부여하여 토픽 "Price/Fruit"를 구독할 수 있는 액세스가 부여되었습니다.

"Price/Fruit" 토픽에 발행하기 위해 USER1에게 h1q.PUBLISH.FRUIT 프로파일에 대한 액세스를 부여하십시오. 이를 수행하려면 다음 RACF 명령을 사용하여 다음을 수행하십시오.

```
RDEFINE MXTOPIC h1q.PUBLISH.FRUIT UACC(NONE)
PERMIT h1q.PUBLISH.FRUIT CLASS(MXTOPIC) ID(USER1) ACCESS(ALTER)
```

기타 플랫폼의 경우:

FRUIT 프로파일에 대한 사용자 발행 액세스를 부여하여 "Price/Fruit" 토픽을 발행하기 위해 USER1에 액세스를 부여하십시오. 플랫폼에 대한 권한 부여 명령을 사용하여 다음을 수행하십시오.

ULW Windows, UNIX and Linux 시스템

```
setmqaut -t topic -n FRUIT -p USER1 +pub
```

IBM i IBM i

```
GRTMQAUT OBJ(FRUIT) OBJTYPE(*TOPIC) USER(USER1) AUT(*PUB)
```

결과

z/OS에서 USER1이 "Price/Fruit" 토픽에 발행하려고 시도하면 MQOPEN 호출에서 보안 검사가 통과됩니다.

USER2가 토픽 "Price/Fruit"에서 발행하려고 시도하면 결과는 다음 및 MQRC_NOT_AUTHORIZED 메시지와 함께 실패합니다.

z/OS z/OS에서는 시도한 토픽 트리를 통해 전체 보안 경로를 표시하는 콘솔에 다음 메시지가 표시됩니다.

```
ICH408I USER(USER2 ) ...
h1q.PUBLISH.FRUIT ...

ICH408I USER(USER2 ) ...
h1q.PUBLISH.SYSTEM.BASE.TOPIC ...
```


- ▶ **ULW** Windows, UNIX 및 Linux 플랫폼에서는 다음 권한 부여 이벤트가 제공됩니다.

```
MQRC_NOT_AUTHORIZED
ReasonQualifier      MQRC_OPEN_NOT_AUTHORIZED
UserIdentifier       USER2
AdminTopicNames     FRUIT, SYSTEM.BASE.TOPIC
TopicString          "Price/Fruit"
```

- ▶ **IBM i** IBMi에서는 다음 권한 부여 이벤트가 제공됩니다.

```
MQRC_NOT_AUTHORIZED
ReasonQualifier      MQRC_OPEN_NOT_AUTHORIZED
UserIdentifier       USER2
AdminTopicNames     FRUIT, SYSTEM.BASE.TOPIC
TopicString          "Price/Fruit"
```

이러한 태스크의 전체 세트를 뒤따라 USER1 및 USER2에 나열된 토픽을 발행하고 구독하기 위한 다음과 같은 액세스 권한을 제공합니다.

표 88. 보안에서 발생하는 액세스 권한의 전체 목록 예

주제	필요한 구독 액세스	필요한 발행 액세스	토픽 오브젝트
Price	사용자 없음	사용자 없음	없음
Price/Fruit	USER1	USER1	과일
Price/Fruit/Apples	USER1 및 USER2		APPLE
Price/Fruit/Oranges	USER1		ORANGE
Price/Vegetables		USER1	VEG
Price/Vegetables/Potatoes			
Price/Vegetables/Onions			

토픽 트리 내에서 서로 다른 레벨에 있는 보안 액세스에 대해 다른 요구사항이 있는 경우에는 주의깊게 계획하면 z/OS 콘솔 로그에서 추가로 보안 경고를 받지 않도록 해줍니다. 트리 내에서 올바른 레벨에 보안을 설정하면 잘못된 보안 메시지를 피할 수 있습니다.

구독 보안

MQSO_ALTERNATE_USER_AUTHORITY

AlternateUserId 필드는 이 MQSUB 호출을 유효성 검증하는 데 사용할 사용자 ID를 포함합니다. 애플리케이션을 실행 중인 사용자 ID가 토픽을 구독하는 권한이 있는지에 관계없이 이 AlternateUserId에 지정된 액세스 옵션을 사용하여 토픽을 구독할 수 있는 권한이 있는 경우에만 호출이 성공할 수 있습니다.

MQSO_SET_IDENTITY_CONTEXT

구독은 PubAccountingToken 및 PubApplIdentityData 필드에 제공된 계정 토큰 및 애플리케이션 ID 데이터를 사용하는 것입니다.

이 옵션을 지정하면 MQOO_SET_IDENTITY_CONTEXT와 함께 MQOPEN 호출을 사용하여 목적지 큐에 액세스한 경우와 동일한 권한 검사가 수행됩니다(목적지 큐에서 권한 검사를 수행하지 않는 경우 MQSO_MANAGED 옵션을 사용하는 경우 제외).

이 옵션을 지정하지 않으면 다음과 같이 이 구독자에게 전송된 발행에 연관된 기본 컨텍스트 정보가 있습니다.

표 89. 기본 발행 컨텍스트 정보	
MQMD의 필드	사용된 값
<i>UserIdentifier</i>	발행이 작성된 시간에 구독과 연관된 사용자 ID(DISPLAY SBSTATUS의 SUBUSER 필드 참조)입니다.
<i>AccountingToken</i>	가능한 경우 환경에서 결정됩니다. 그렇지 않으면 MQACT_NONE으로 설정됩니다.
<i>ApplIdentityData</i>	공백으로 설정합니다.

이 옵션은 MQSO_CREATE 및 MQSO ALTER에서만 유효합니다. MQSO_RESUME와 함께 사용하면 PubAccountingToken 및 PubApplIdentityData 필드가 무시되고 따라서 이 옵션은 적용되지 않습니다.

이전에 구독이 ID 컨텍스트 정보를 제공한 경우 해당 옵션을 사용하지 않고 구독을 대체하면 대체된 구독에 대한 기본 컨텍스트 정보가 생성됩니다.

여러 사용자 ID가 MQSO_ANY_USERID 옵션과 함께 이 옵션을 사용할 수 있게 하는 구독이 다른 사용자 ID에 의해 재개되는 경우 구독을 소유한 새 사용자 ID에 대한 기본 ID 컨텍스트가 생성되고 새 ID 컨텍스트가 포함된 후속 발행물이 전달됩니다.

AlternateSecurityId

적절한 권한 검사를 수행할 수 있도록 AlternateUserId와 함께 권한 서비스에 전달되는 보안 ID입니다. AlternateSecurityId는 MQSO_ALTERNATE_USER_AUTHORITY가 지정된 경우에만 사용되며, AlternateUserId 필드는 첫 번째 널 문자 또는 필드의 끝까지 전체적으로 비어있지 않습니다.

MQSO_ANY_USERID subscription 옵션

MQSO_ANY_USERID가 지정된 경우 구독자의 ID는 단일 사용자 ID로 제한되지 않습니다. 이로 인해 적절한 권한이 있을 때 사용자가 구독을 대체하거나 재개할 수 있습니다. 단일 사용자에 한해서 언제든지 구독 가능합니다. 또 다른 애플리케이션이 현재 사용 중인 구독을 재개하기 위한 시도는 호출을 MQRC_SUBSCRIPTION_IN_USE로 실패하게 만듭니다.

이 옵션을 기존 구독에 추가하려면 MQSUB 호출(MQSO ALTER 사용)은 원본 구독과 같은 사용자 ID로부터 나와야 합니다.

MQSUB 호출이 MQSO_ANY_USERID가 설정된 기존 구독을 참조하고 사용자 ID가 원래 구독과 다른 경우 새 사용자 ID에 토픽을 구독할 수 있는 권한이 있을 때에만 호출에 성공합니다. 성공적인 완료 후에 이 구독자에 대한 추가 발행은 발행에 설정된 새 사용자 ID와 함께 구독자 큐에 놓입니다.

MQSO_FIXED_USERID

MQSO_FIXED_USERID가 지정될 때 구독은 단일 소유 사용자 ID에 의해서만 변경되거나 재개될 수 있습니다. 이 사용자 ID는 이 옵션을 설정하여 MQSO_ANY_USERID 옵션을 제거한 구독을 변경하기 위한 마지막 사용자 ID이거나, 변경이 발생하지 않으면 구독을 작성한 사용자 ID입니다.

MQSUB 동사가 MQSO_ANY_USERID가 설정된 기존 구독을 가리키고 MQSO_FIXED_USERID 옵션을 사용하기 위해 구독(MQSO ALTER 사용)을 변경하는 경우, 구독의 사용자 ID는 이제 이 새 사용자 ID로 고정됩니다. 새 사용자 ID에 토픽을 구독할 수 있는 권한이 있는 경우에만 호출에 성공합니다.

구독을 소유한 것으로 기록된 사용자 ID 이외의 사용자 ID가 MQSO_FIXED_USERID 구독을 재개하거나 변경하려고 시도하는 경우 호출은 MQRC_IDENTITY_MISMATCH와 함께 실패합니다. DISPLAY SBSTATUS 명령을 사용하여 구독에 대한 소유 사용자 ID를 볼 수 있습니다.

MQSO_ANY_USERID 또는 MQSO_FIXED_USERID가 지정되지 않은 경우에는 기본값인 MQSO_FIXED_USERID입니다.

큐 관리자 간의 발행/구독 보안

프록시 구독 및 발행물과 같은 발행/구독 내부 메시지는 정상적인 채널 보안 규칙을 사용하여 발행/구독 시스템 큐에 놓입니다. 이 토픽에 있는 정보 및 다이어그램은 메시지 전달에 포함되는 다양한 프로세스 및 사용자 ID를 강조표시합니다.

로컬 액세스 제어

발행물 및 구독에 대한 토픽의 액세스는 발행/구독 보안에 설명된 로컬 보안 정의 및 규칙으로 관리됩니다. z/OS에서는 액세스 제어를 설정하기 위해 로컬 토픽 오브젝트가 필요하지 않습니다. 다른 플랫폼에서 액세스 제어에 필요한 로컬 토픽도 없습니다. 관리자는 클러스터된 토픽 오브젝트가 클러스터에 아직 존재하는지 여부와 관계 없이 이에 대한 액세스 제어를 적용하도록 선택할 수 있습니다.

시스템 관리자는 로컬 시스템에서의 액세스 제어를 담당합니다. 이러한 관리자는 액세스 제어 정책을 담당할 클러스터 집합 또는 계층의 다른 멤버의 관리자를 신뢰해야 합니다. 액세스 제어가 별도의 각 시스템에 대해 정의되어 있으므로 상세 레벨 제어가 필요한 경우 번거로운 일이 될 수 있습니다. 액세스 제어를 부여하는 데 필요하지 않거나 액세스 제어가 토픽 트리의 상위 레벨 오브젝트에서 정의될 수 있습니다. 상세 레벨 액세스 제어는 토픽 네임스페이스의 각 세분화를 위해 정의할 수 있습니다.

프록시 구독 작성

조직이 큐 관리자에 해당 큐 관리자를 연결하기 위한 신뢰는 정상 채널 인증 수단으로 확인됩니다. 또한 신뢰되는 조직이 분산 발행/구독을 수행하도록 허용되는 경우 권한 검사가 수행됩니다. 이 검사는 채널이 분산된 발행/구독 큐에 메시지를 넣을 때 수행됩니다. 예를 들어, 메시지를 SYSTEM.INTER.QMGR.CONTROL 큐에 넣는 경우입니다. 큐 권한 검사를 위한 사용자 ID는 수신 채널의 PUTAUT 값에 따라 달라집니다. 예를 들어, 값 및 플랫폼에 따라 채널의 사용자 ID, MCAUSER, 메시지 컨텍스트. 채널 보안에 대한 자세한 정보는 [채널 보안](#)을 참조하십시오.

프록시 구독은 리모트 큐 관리자에서 분배된 발행/구독 에이전트의 사용자 ID로 작성됩니다. 예를 들어, 438 페이지의 [그림 30](#)의 QM2입니다. 그러면 사용자 ID가 시스템에 정의되어 있고 따라서 도메인 충돌이 없으므로 이 사용자는 쉽게 로컬 토픽 오브젝트 프로파일에 대한 액세스 권한을 부여받게 됩니다.

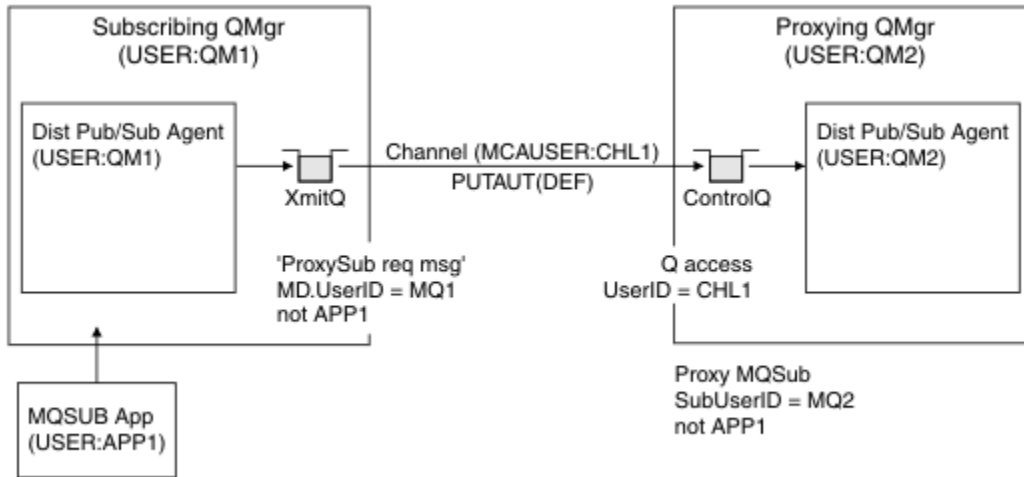


그림 30. 프록시 구독 보안, 구독 작성

원격 발행물 다시 송신

구독 큐 관리자에서 발행물이 작성되면 발행물의 사본이 프록시 구독용으로 작성됩니다. 복사된 발행물의 컨텍스트에는 구독한 사용자 ID의 컨텍스트를 포함합니다(439 페이지의 [그림 31](#)의 QM2). 프록시 구독은 리모트 큐인 목적지 큐와 함께 작성되므로 발행 메시지는 전송 큐에서 해결됩니다.

큐 관리자, QM2을(를) 다른 큐 관리자, QM1에 연결하는 조직에 대한 신뢰는 정상적인 채널 인증 수단을 통해 확인합니다. 신뢰할 수 있는 조직이 분배된 발행/구독을 수행할 수 있는 경우, 채널이 발행 메시지를 분산 발행/구독 발행 큐 SYSTEM.INTER.QMGR.PUBS에 넣을 때 권한 검사가 수행됩니다. 큐 권한 검사에 대한 사용자 ID는 수신 채널의 PUTAUT 값에 의존합니다(예를 들어, 값과 플랫폼에 따라 채널, MCAUSER, 메시지 컨텍스트 등의 사용자 ID). 채널 보안에 대한 자세한 정보는 [채널 보안](#)을 참조하십시오.

발행 메시지가 구독 큐 관리자에 도달할 때, 토픽에 대한 다른 MQPUT는 해당 큐 관리자의 권한 하에 수행되고, 메시지가 있는 컨텍스트는 로컬 구독자에게 각각 메시지가 제공되는 대로 각 로컬 구독자의 컨텍스트에 의해 대체됩니다.

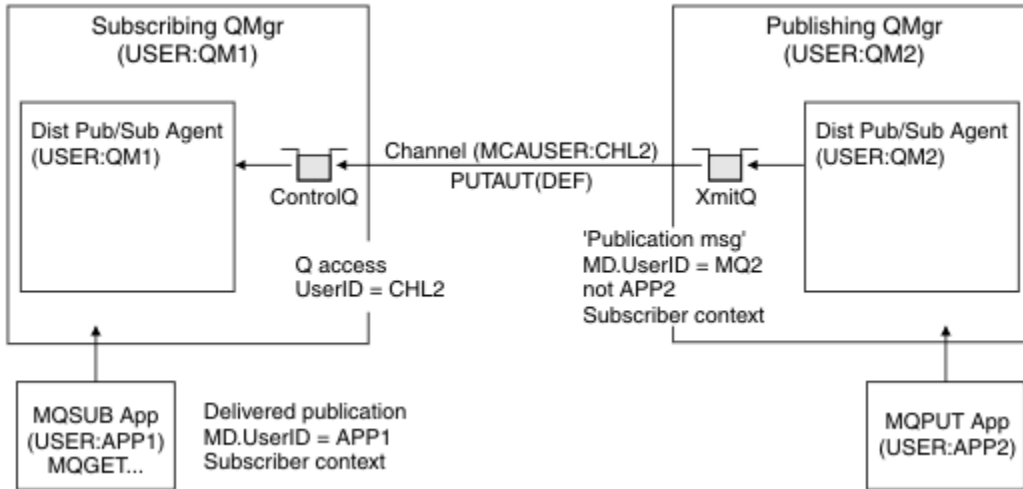


그림 31. 프록시 구독 보안, 발행물 전달

보안과 관련하여 거의 고려되지 않은 시스템에서 분산 발행/구독 프로세스는 mqm 그룹의 사용자 ID로 실행될 수 있으며 채널의 MCAUSER 매개변수는 공백(기본값)이고 메시지는 필요에 따라 다양한 시스템 큐로 전달됩니다. 안전하지 않은 시스템은 분배된 발행/구독을 시연하기 위한 개념 증명을 설정하기가 쉽습니다.

보안이 보다 심각하게 고려되는 시스템에서는 이러한 내부 메시지가 채널을 통해 이동하는 메시지와 동일한 보안 제어의 영향을 받습니다.

채널을 비어 있지 않은 MCAUSER 및 PUTAUT 값으로 설정하여 MCAUSER를 확인해야 함을 지정하는 경우 문제의 MCAUSER에 SYSTEM.INTER.QMGR.* 큐에 대한 액세스 권한이 부여되어야 합니다. 다른 MCAUSER ID로 실행되는 채널이 있는 다른 리모트 큐 관리자가 여러 개이면 해당 모든 사용자 ID에 SYSTEM.INTER.QMGR.* 큐에 액세스할 수 있는 권한을 부여해야 합니다. 다른 MCAUSER ID에서 실행 중인 채널은 예를 들어 다중 계층 구조 연결이 단일 큐 관리자에 구성된 경우 발생할 수 있습니다.

메시지의 컨텍스트를 사용하도록 지정하는 PUTAUT 값을 사용하여 채널이 설정된 경우 내부 메시지 내부의 사용자 ID를 기반으로 SYSTEM.INTER.QMGR.* 큐에 대한 액세스 권한이 확인됩니다. 이 메시지 모두 내부 메시지 또는 발행물 메시지를 송신하는 큐 관리자의 분산 발행/구독 에이전트의 사용자 ID로 넣어지기 때문에(439 페이지의 [그림 31](#) 참조) 이런 방식으로 분산 발행/구독 보안을 설정하면 사용자 ID 세트가 너무 크지 않기 때문에 다양한 시스템 큐에 액세스를 부여할 수 있습니다(리모트 큐 관리자별로 한 개). 채널 컨텍스트 보안이 항상 가지고 있는 동일한 문제 모두를 계속 가지고 있습니다. 다양한 사용자 ID 도메인의 문제와 메시지의 사용자 ID가 수신 시스템에서 정의되지 않을 수 있다는 문제입니다. 그러나 이는 필요한 경우 완벽히 허용되는 실행 방법입니다.

z/OS 시스템 큐 보안은 분산 발행/구독 환경을 안전하게 설정하기 위해 필요한 큐 및 액세스 목록을 제공합니다. 보안 파기로 인해 내부 메시지 또는 발행물 저장에 실패할 경우 채널은 정상 방법으로 로그에 메시지를 기록하며 이 메시지는 정상 채널 오류 처리에 따라 데드-레터 큐로 송신될 수 있습니다.

분산 발행/구독을 위해 모든 내부 큐 관리자 메시징은 정상 채널 보안을 사용하여 실행됩니다.

토픽 레벨에서 발행물 및 프록시 구독을 제한하는 방법에 대한 정보는 [발행/구독 보안](#)을 참조하십시오.

큐 관리자 계층으로 기본 사용자 ID 사용

다른 플랫폼에서 실행 중인 큐 관리자의 계층이 있고 기본 사용자 ID를 사용 중인 경우 이러한 기본 사용자 ID는 플랫폼 간에 다를 수 있고 대상 플랫폼에서 인식되지 않을 수 있습니다. 따라서 한 플랫폼에서 실행 중인 큐 관리자는 이유 코드가 MQRC_NOT_AUTHORIZED인 다른 플랫폼의 큐 관리자로부터 수신된 메시지를 거부합니다.

메시지가 거부되지 않도록 하려면 최소한 다른 플랫폼에서 사용되는 기본 사용자 ID에 다음 권한을 추가해야 합니다.

- SYSTEM.BROKER의 *PUT *GET 권한. 큐
- SYSTEM.BROKER의 *PUB *SUB 권한. 토픽
- SYSTEM.BROKER.CONTROL.QUEUE 큐의 *ADMCRT *ADMDLT *ADMCHG 권한.

큐 관리자 계층 구조가 있는 기본 사용자 ID는 다음과 같습니다.

플랫폼	기본 사용자 ID
Windows	MUSR_MQADMIN
UNIX and Linux 시스템	mqm
IBM i	QMQM
z/OS	채널 시작기 주소 공간 사용자 ID

Windows, UNIX, Linux 및 z/OS 플랫폼의 큐 관리자에 대해 IBM i의 큐 관리자에 계층적으로 연결된 경우 'qmqm' 사용자 ID에 대한 액세스를 작성하고 부여하십시오.

IBM i 및 z/OS 플랫폼의 큐 관리자에 대해 Windows, UNIX 또는 Linux의 큐 관리자에 계층적으로 연결된 경우 'mqm' 사용자 ID에 대한 액세스를 작성하고 부여하십시오.

Windows, UNIX, Linux 및 IBM i 플랫폼의 큐 관리자에 대해 z/OS의 큐 관리자에 계층적으로 연결된 경우 z/OS 채널 시작기 주소 공간 사용자 ID에 대한 사용자 액세스 권한을 작성하고 부여하십시오.

사용자 ID는 대소문자가 구별될 수 있습니다. 원래 큐 관리자(IBM i, Windows, UNIX 또는 Linux 시스템의 경우)에서는 사용자 ID가 모두 대문자여야 합니다. 수신 큐 관리자(Windows, UNIX 또는 Linux 시스템의 경우)에서는 사용자 ID가 모두 소문자여야 합니다. 따라서 UNIX and Linux 시스템에서 작성된 모든 사용자 ID는 소문자 양식으로 작성되어야 합니다. 메시지 엑시트가 설치된 경우 사용자 ID를 대문자 또는 소문자로 강제 실행하는 작업이 발생하지 않습니다. 메시지 엑시트가 사용자 ID를 처리하는 방법을 이해하려면 경우에는 주의하십시오.

사용자 ID의 변환에 관련된 잠재적인 문제점을 방지하려면 다음을 수행하십시오.

- UNIX, Linux, and Windows 시스템에서는 사용자 ID가 소문자로 지정되었는지 확인하십시오.
- IBM i 및 z/OS에서는 사용자 ID가 대문자로 지정되었는지 확인하십시오.

V 9.1.0 IBM MQ Console 및 REST API 보안

IBM MQ Console 및 REST API에 대한 보안은 mqwebuser.xml 파일에서 mqweb 서버 구성을 편집하여 구성됩니다.

이 태스크 정보

mqweb 서버의 로그 파일을 검사하여 사용자 조치를 추적하고 IBM MQ Console 및 REST API 사용을 감사할 수 있습니다.

IBM MQ Console 및 REST API의 사용자는 다음을 통해 인증될 수 있습니다.

- Basic registry
- LDAP 레지스트리
- 로컬 OS 레지스트리
- z/OS의 SAF
- WebSphere Liberty에서 지원하는 다른 레지스트리 유형

역할을 IBM MQ Console 사용자 및 REST API 사용자에게 지정하여 IBM MQ 오브젝트에 대해 해당 사용자에게 부여되는 액세스 권한 레벨을 판별할 수 있습니다. 예를 들어, 메시지를 수행하려면 사용자에게 MQWebUser 역할을 지정해야 합니다. 사용 가능한 역할에 대한 자세한 정보는 [451 페이지의 『IBM MQ Console 및 REST API의 역할』](#)의 내용을 참조하십시오.

사용자에게 역할이 지정되고 나면 다수의 방법을 사용하여 사용자를 인증할 수 있습니다. IBM MQ Console을 사용하는 경우 사용자는 사용자 이름 및 비밀번호를 사용하여 로그인하거나 클라이언트 인증서 인증을 사용할 수 있습니다. REST API를 사용하는 경우 사용자는 기본 HTTP 인증, 토큰 기반 인증 또는 클라이언트 인증서 인증을 사용할 수 있습니다.

프로시저

1. 사용자 레지스트리를 정의하여 사용자를 인증하고 각 사용자 또는 그룹에 역할을 지정하여 사용자 및 그룹에 IBM MQ Console 또는 REST API를 사용할 수 있는 권한을 부여하십시오. 자세한 정보는 다음 항목을 참조하십시오. [442 페이지의 『사용자 및 역할 구성』](#)
2. IBM MQ Console의 사용자가 mqweb 서버에 대해 인증되는 방식을 선택하십시오. 모든 사용자에게 대해 동일한 방법을 사용하지 않아도 됩니다.
 - 사용자가 토큰 인증을 사용하여 인증하게 합니다. 이 경우 사용자는 IBM MQ Console 로그인 화면에서 사용자 ID 및 비밀번호를 입력합니다. 사용자가 설정된 시간 동안 로그인되어 권한 부여된 상태를 유지할 수 있게 하는 LTPA 토큰이 생성됩니다. 이 인증 옵션을 사용하기 위해 추가 구성은 필요하지 않지만 선택적으로 LTPA 토큰의 만기 시간을 구성할 수 있습니다. 자세한 정보는 [LTPA 토큰 만기 간격 구성](#)을 참조하십시오.
 - 사용자가 클라이언트 인증서를 사용하여 인증하게 합니다. 이 경우 사용자는 사용자 ID 또는 비밀번호를 사용하여 IBM MQ Console에 로그인하지 않고 클라이언트 인증서를 대신 사용합니다. 자세한 정보는 [452 페이지의 『REST API 및 IBM MQ Console과 함께 클라이언트 인증서 인증 사용』](#)의 내용을 참조하십시오.
3. REST API의 사용자가 mqweb 서버에 대해 인증되는 방식을 선택하십시오. 모든 사용자에게 대해 동일한 방법을 사용하지 않아도 됩니다.
 - 사용자가 HTTP 기본 인증을 사용하여 인증하게 합니다. 이 경우 사용자 이름 및 비밀번호가 인코딩되지만 암호화되지는 않으며 각각의 REST API 요청과 함께 전송되어 해당 요청에 대해 사용자를 인증하고 사용자에게 권한을 부여합니다. 이 인증에 보안을 설정하려면 보안 연결을 사용해야 합니다. 즉, HTTPS를 사용해야 합니다. 자세한 정보는 [456 페이지의 『REST API로 HTTP 기본 인증 사용』](#)의 내용을 참조하십시오.
 - 사용자가 토큰 인증을 사용하여 인증하게 합니다. 이 경우 사용자는 HTTP POST 메소드를 사용하여 사용자 ID 및 비밀번호를 REST API login 자원에 제공합니다. 사용자가 설정된 시간 동안 로그인되어 권한 부여된 상태를 유지할 수 있게 하는 LTPA 토큰이 생성됩니다. 추가 정보는 [457 페이지의 『REST API로 토큰 기반 인증 사용』](#)의 내용을 참조하십시오.

이 인증에 보안을 설정하려면 보안 연결을 사용해야 합니다. 즉, HTTPS를 사용해야 합니다. 하지만 HTTP 연결을 사용하는 경우 HTTP 연결을 위해 발행되는 LTPA 토큰을 HTTP 연결에 사용할 수 있도록 합니다. 자세한 정보는 [LTPA 토큰 구성](#)을 참조하십시오.
 - 사용자가 클라이언트 인증서를 사용하여 인증하게 합니다. 이 경우 사용자는 사용자 ID 또는 비밀번호를 사용하여 REST API에 로그인하지 않고 클라이언트 인증서를 대신 사용합니다. 자세한 정보는 [452 페이지의 『REST API 및 IBM MQ Console과 함께 클라이언트 인증서 인증 사용』](#)의 내용을 참조하십시오.
4. 옵션: REST API에 대한 CORS(Cross Origin Resource Sharing)를 공유하십시오.

기본적으로 웹 브라우저는 스크립트(예: JavaScript)가 REST API와 동일한 원본에서 제공되지 않는 경우 스크립트가 REST API를 호출하도록 허용하지 않습니다. 즉, 원본 간 요청이 사용으로 설정되지 않습니다. 지정된 URL로부터의 원본 간 요청을 허용하도록 CORS(Cross Origin Resource Sharing)를 구성할 수 있습니다. 추가 정보는 [459 페이지의 『REST API에 대해 CORS 구성』](#)의 내용을 참조하십시오.
5. 옵션: IBM MQ Console 및 REST API에 대한 호스트 헤더 유효성 검증을 구성하십시오.

호스트 헤더 유효성 검증을 구성하고 호스트 이름 및 포트의 허용 목록을 작성하여 특정 호스트 헤더를 포함하는 요청만 IBM MQ Console 및 REST API에 의해 처리되도록 할 수 있습니다. 추가 정보는 [460 페이지의 『IBM MQ Console 및 REST API에 대한 호스트 헤더 유효성 검증 구성』](#)의 내용을 참조하십시오.

IBM MQ Console 또는 REST API를 사용하려면 사용자가 mqweb 서버에 정의된 사용자 레지스트리에 대해 인증해야 합니다.

이 태스크 정보



인증된 사용자는 IBM MQ Console 및 REST API의 기능에 대한 액세스 권한을 부여하는 그룹 중 하나의 구성원이어야 합니다. 기본적으로 사용자 레지스트리에는 사용자가 포함되지 않습니다. mqwebuser.xml 파일을 편집하여 이를 추가해야 합니다.

사용자 및 그룹을 구성할 때는 먼저 사용자 및 그룹을 인증할 사용자 레지스트리를 구성합니다. 이 사용자 레지스트리는 IBM MQ Console과 REST API 사이에서 공유됩니다. 사용자 및 그룹에 대한 역할을 구성할 때 사용자 및 그룹에 IBM MQ Console, REST API 또는 둘 다에 대한 액세스 권한이 있는지 여부를 제어할 수 있습니다.

사용자 레지스트리를 구성한 후 사용자 및 그룹에 대한 역할을 구성하여 사용자 및 그룹에 권한을 부여합니다. Managed File Transfer에 REST API를 사용하는 것에 특정한 역할을 포함하여 여러 가지 역할을 사용할 수 있습니다. 각 역할은 서로 다른 레벨의 액세스 권한을 부여합니다. 추가 정보는 [451 페이지의 『IBM MQ Console 및 REST API의 역할』](#)의 내용을 참조하십시오.

사용자 및 그룹의 구성을 더 단순하게 하기 위해 다수의 샘플 XML 파일이 mqweb 서버와 함께 제공됩니다. WebSphere Liberty(WLP)에서의 보안 구성에 익숙한 사용자는 샘플 사용을 선호하지 않습니다. WLP는 여기서 설명한 기능 외에 다른 권한 부여 기능을 제공합니다.

프로시저

- basic_registry.xml 파일을 사용하여 기본 레지스트리로 사용자 및 그룹을 구성하십시오.
레지스트리에 있는 사용자 이름 및 비밀번호는 IBM MQ Console 및 REST API의 사용자를 인증하고 이 사용자에게 권한을 부여하는 데 사용됩니다.
basic_registry.xml 샘플 파일을 사용하여 기본 레지스트리를 구성하려면 [443 페이지의 『IBM MQ Console 및 REST API에 대한 기본 레지스트리 구성』](#)의 내용을 참조하십시오.
- ldap_registry.xml 파일을 사용하여 LDAP 레지스트리로 사용자 및 그룹을 구성하십시오.
LDAP 레지스트리에 있는 사용자 이름 및 비밀번호는 IBM MQ Console 및 REST API의 사용자를 인증하고 이 사용자에게 권한을 부여하는 데 사용됩니다.
ldap_registry.xml 샘플 파일을 사용하여 LDAP 레지스트리를 구성하려면 [447 페이지의 『IBM MQ Console 및 REST API에 대한 LDAP 레지스트리 구성』](#)의 내용을 참조하십시오.
-  local_os_registry.xml 파일을 사용하여 로컬 운영 체제 레지스트리로 사용자 및 그룹을 구성하십시오.
운영 체제 레지스트리에 있는 사용자 이름 및 비밀번호는 IBM MQ Console 및 REST API의 사용자를 인증하고 이 사용자에게 권한을 부여하는 데 사용됩니다.
local_os_registry.xml 샘플 파일을 사용하여 로컬 OS 레지스트리를 구성하려면 [446 페이지의 『IBM MQ Console 및 REST API에 대한 로컬 OS 레지스트리 구성』](#)의 내용을 참조하십시오.
-  zos_saf_registry.xml 파일을 사용하여 z/OS에서 SAF (System Authorization Facility) 인터페이스를 사용하여 사용자 및 그룹을 구성하십시오.
RACF 또는 기타 보안 제품의 경우 프로파일을 사용하여 사용자 및 그룹에 역할에 대한 액세스 권한을 부여합니다. RACF 데이터베이스의 사용자 이름 및 비밀번호는 IBM MQ Console 및 REST API의 사용자를 인증하고 권한을 부여하는 데 사용됩니다.
zos_saf_registry.xml 샘플 파일을 사용하여 SAF 인터페이스를 구성하려면 [448 페이지의 『IBM MQ Console 및 REST API에 대한 SAF 레지스트리 구성』](#)의 내용을 참조하십시오.

- no_security.xml 파일을 사용하여 IBM MQ Console 또는 HTTPS를 사용하는 REST API에 액세스하는 기능을 포함하여 보안을 사용 불가능하게 하십시오.

다음에 수행할 작업

사용자 인증 방법을 선택하십시오.

IBM MQ Console 인증 옵션

- 사용자가 토큰 인증을 사용하여 인증하게 합니다. 이 경우 사용자는 IBM MQ Console 로그인 화면에서 사용자 ID 및 비밀번호를 입력합니다. 사용자가 설정된 시간 동안 로그인되어 권한 부여된 상태를 유지할 수 있게 하는 LTPA 토큰이 생성됩니다. 이 인증 옵션을 사용하기 위해 추가 구성은 필요하지 않지만 선택적으로 LTPA 토큰의 만기 간격을 구성할 수 있습니다. 자세한 정보는 [LTPA 토큰 만기 간격 구성을 참조하십시오](#).
- 사용자가 클라이언트 인증서를 사용하여 인증하게 합니다. 이 경우 사용자는 사용자 ID 또는 비밀번호를 사용하여 IBM MQ Console에 로그인하지 않고 클라이언트 인증서를 대신 사용합니다. 자세한 정보는 [452 페이지의 『REST API 및 IBM MQ Console과 함께 클라이언트 인증서 인증 사용』의 내용을 참조하십시오](#).

REST API 인증 옵션



- 사용자가 HTTP 기본 인증을 사용하여 인증하게 합니다. 이 경우 사용자 이름 및 비밀번호가 인코딩되지만 암호화되지는 않으며 각각의 REST API 요청과 함께 전송되어 해당 요청에 대해 사용자를 인증하고 사용자에게 권한을 부여합니다. 이 인증에 보안을 설정하려면 보안 연결을 사용해야 합니다. 즉, HTTPS를 사용해야 합니다. 자세한 정보는 [456 페이지의 『REST API로 HTTP 기본 인증 사용』의 내용을 참조하십시오](#).
- 사용자가 토큰 인증을 사용하여 인증하게 합니다. 이 경우 사용자는 HTTP POST 메소드를 사용하여 사용자 ID 및 비밀번호를 REST API login 자원에 제공합니다. 사용자가 설정된 시간 동안 로그인되어 권한 부여된 상태를 유지할 수 있게 하는 LTPA 토큰이 생성됩니다. 추가 정보는 [457 페이지의 『REST API로 토큰 기반 인증 사용』의 내용을 참조하십시오](#). LTPA 토큰의 만기 간격을 구성할 수 있습니다. 자세한 정보는 [LTPA 토큰 구성을 참조하십시오](#).
- 사용자가 클라이언트 인증서를 사용하여 인증하게 합니다. 이 경우 사용자는 사용자 ID 또는 비밀번호를 사용하여 REST API에 로그인하지 않고 클라이언트 인증서를 대신 사용합니다. 자세한 정보는 [452 페이지의 『REST API 및 IBM MQ Console과 함께 클라이언트 인증서 인증 사용』의 내용을 참조하십시오](#).

V9.1.0 IBM MQ Console 및 REST API에 대한 기본 레지스트리 구성

mqwebuser.xml 파일 내에서 기본 레지스트리를 구성할 수 있습니다. xml 파일에 있는 사용자 이름, 비밀번호 및 역할은 IBM MQ Console 및 REST API의 사용자를 인증하고 권한 부여하는 데 사용됩니다.



시작하기 전에

- 기본 레지스트리 내에 사용자를 구성할 때 각 사용자에게 역할을 지정해야 합니다. 각 역할은 IBM MQ Console 및 REST API에 액세스하는 데 필요한 다양한 레벨의 권한을 제공하고 허용된 조작이 시도될 때 사용되는 보안 컨텍스트를 판별합니다. 기본 레지스트리를 구성하기 전에 이러한 역할을 이해해야 합니다. 각 역할에 대한 자세한 정보는 [451 페이지의 『IBM MQ Console 및 REST API의 역할』의 내용을 참조하십시오](#).
- 이 작업을 완료하려면 mqwebuser.xml 파일을 편집할 수 있는 충분한 권한이 있는 사용자여야 합니다.

-  z/OS에서는 mqwebuser.xml 파일에 대한 쓰기 액세스 권한이 있어야 합니다.
-  다른 모든 운영 체제에서는 [권한이 있는 사용자여야 합니다](#).

프로시저

1. 다음 경로 중 하나에서 샘플 XML 파일 basic_registry.xml을 복사하십시오.

-  UNIX, Linux, and Windows: MQ_INSTALLATION_PATH /web/mq/samp/configuration
-  z/OS: PathPrefix /web/mq/samp/configuration

여기서 PathPrefix는 IBM MQ Unix System Services 컴포넌트 설치 경로입니다.

2. 샘플 파일을 적절한 디렉토리에 배치하십시오.



UNIX, Linux, and Windows: `MQ_DATA_PATH/web/installations/installationName/servers/mqweb`



z/OS: `WLP_user_directory/servers/mqweb`

여기서 `WLP_user_directory`는 mqweb 서버 정의를 작성하기 위해 `crtmqweb` 스크립트를 실행할 때 지정된 디렉토리입니다.

3. 옵션: `mqwebuser.xml`에서 구성 설정을 변경한 경우 이를 샘플 파일에 복사하십시오.

4. 기존 `mqwebuser.xml` 파일을 삭제하고 샘플 파일 이름을 `mqwebuser.xml`로 변경하십시오.

5. **basicRegistry** 태그 내에 사용자 및 그룹을 추가하도록 새 `mqwebuser.xml` 파일을 편집하십시오.

MQWebUser 역할이 지정된 사용자는 큐 관리자에서 수행하도록 사용자 ID가 제공된 조작만 수행할 수 있습니다. 따라서 레지스트리에 정의된 사용자 ID는 IBM MQ가 설치된 시스템의 사용자 ID와 동일해야 합니다. 이러한 사용자 ID는 동일한 대소문자로 되어 있어야 합니다. 그렇지 않을 경우 사용자 ID 간 맵핑이 실패합니다.

기본 사용자 레지스트리 구성에 대한 자세한 정보는 WebSphere Liberty 문서의 [Liberty에 대한 기본 사용자 레지스트리 구성](#)을 참조하십시오.

6. `mqwebuser.xml` 파일을 편집하여 사용자 및 그룹에 역할을 지정하십시오.

사용자 및 그룹에 IBM MQ Console 및 REST API를 사용할 수 있는 권한을 부여할 수 있는 몇 가지 역할이 있습니다. 각 역할은 서로 다른 레벨의 액세스 권한을 부여합니다. 추가 정보는 [451 페이지의 『IBM MQ Console 및 REST API의 역할』](#)의 내용을 참조하십시오.

- IBM MQ Console에 역할을 지정하고 액세스 권한을 부여하려면 **<enterpriseApplication id="com.ibm.mq.console">** 태그 내의 해당 **security-role** 태그 사이에 사용자 및 그룹을 추가하십시오.

- REST API에 역할을 지정하고 액세스 권한을 부여하려면 **<enterpriseApplication id="com.ibm.mq.rest">** 태그 내의 해당 **security-role** 태그 사이에 사용자 및 그룹을 추가하십시오.

security-role 태그 내에서 사용자 및 그룹 정보의 형식에 대한 도움말은 [예](#)를 참조하십시오.

7. `mqwebuser.xml`의 사용자에게 비밀번호를 제공한 경우 WebSphere Liberty에서 제공하는 **securityUtility encoding** 명령을 사용하여 이러한 비밀번호를 더 안전하게 설정해야 합니다. 자세한 정보는 WebSphere Liberty 제품 문서의 [Liberty:securityUtility 명령](#)을 참조하십시오.

예

다음 예제에서는 MQWebAdminGroup 그룹에 MQWebAdmin 역할을 가진 IBM MQ Console에 대한 액세스가 부여됩니다. 사용자 `reader`에게는 MQWebAdminRO 역할과 함께 액세스 권한이 부여되고 사용자 `guest`에게는 MQWebUser 역할과 함께 액세스 권한이 부여됩니다.

```
<enterpriseApplication id="com.ibm.mq.console">
  <application-bnd>
    <security-role name="MQWebAdmin">
      <group name="MQWebAdminGroup" realm="defaultRealm"/>
    </security-role>
    <security-role name="MQWebAdminRO">
      <user name="reader" realm="defaultRealm"/>
    </security-role>
    <security-role name="MQWebUser">
      <user name="guest" realm="defaultRealm"/>
    </security-role>
  </application-bnd>
</enterpriseApplication>
```

다음 예에서는 사용자 reader 및 guest에게 IBM MQ Console에 대한 액세스 권한이 부여됩니다. 사용자 user에게는 REST API에 대한 액세스 권한이 부여되고 MQAdmin 그룹 내의 모든 사용자에게는 IBM MQ Console 및 REST API에 대한 액세스 권한이 부여됩니다. mftadmin 사용자는 MFT에 대한 REST API에 대한 액세스 권한이 부여됩니다.

```
<enterpriseApplication id="com.ibm.mq.console">
  <application-bnd>
    <security-role name="MQWebAdmin">
      <group name="MQAdmin" realm="defaultRealm"/>
    </security-role>
    <security-role name="MQWebAdminRO">
      <user name="reader" realm="defaultRealm"/>
    </security-role>
    <security-role name="MQWebUser">
      <user name="guest" realm="defaultRealm"/>
    </security-role>
  </application-bnd>
</enterpriseApplication>

<enterpriseApplication id="com.ibm.mq.rest">
  <application-bnd>
    <security-role name="MQWebAdmin">
      <group name="MQAdmin" realm="defaultRealm"/>
    </security-role>
    <security-role name="MQWebUser">
      <user name="user" realm="defaultRealm"/>
    </security-role>
    <security-role name="MFTWebAdmin">
      <user name="mftadmin" realm="defaultRealm"/>
    </security-role>
  </application-bnd>
</enterpriseApplication>
```

다음에 수행할 작업

사용자 인증 방법을 선택하십시오.

IBM MQ Console 인증 옵션

- 사용자가 토큰 인증을 사용하여 인증하게 합니다. 이 경우 사용자는 IBM MQ Console 로그인 화면에서 사용자 ID 및 비밀번호를 입력합니다. 사용자가 설정된 시간 동안 로그인되어 권한 부여된 상태를 유지할 수 있게 하는 LTPA 토큰이 생성됩니다. 이 인증 옵션을 사용하기 위해 추가 구성은 필요하지 않지만 선택적으로 LTPA 토큰의 만기 간격을 구성할 수 있습니다. 자세한 정보는 [LTPA 토큰 만기 간격 구성을 참조하십시오](#).
- 사용자가 클라이언트 인증서를 사용하여 인증하게 합니다. 이 경우 사용자는 사용자 ID 또는 비밀번호를 사용하여 IBM MQ Console에 로그인하지 않고 클라이언트 인증서를 대신 사용합니다. 자세한 정보는 [452 페이지의 『REST API 및 IBM MQ Console과 함께 클라이언트 인증서 인증 사용』의 내용을 참조하십시오](#).

REST API 인증 옵션

- 사용자가 HTTP 기본 인증을 사용하여 인증하게 합니다. 이 경우 사용자 이름 및 비밀번호가 인코딩되지만 암호화되지는 않으며 각각의 REST API 요청과 함께 전송되어 해당 요청에 대해 사용자를 인증하고 사용자에게 권한을 부여합니다. 이 인증에 보안을 설정하려면 보안 연결을 사용해야 합니다. 즉, HTTPS를 사용해야 합니다. 자세한 정보는 [456 페이지의 『REST API로 HTTP 기본 인증 사용』의 내용을 참조하십시오](#).
- 사용자가 토큰 인증을 사용하여 인증하게 합니다. 이 경우 사용자는 HTTP POST 메소드를 사용하여 사용자 ID 및 비밀번호를 REST API login 자원에 제공합니다. 사용자가 설정된 시간 동안 로그인되어 권한 부여된 상태를 유지할 수 있게 하는 LTPA 토큰이 생성됩니다. 추가 정보는 [457 페이지의 『REST API로 토큰 기반 인증 사용』의 내용을 참조하십시오](#). LTPA 토큰의 만기 간격을 구성할 수 있습니다. 자세한 정보는 [LTPA 토큰 구성을 참조하십시오](#).
- 사용자가 클라이언트 인증서를 사용하여 인증하게 합니다. 이 경우 사용자는 사용자 ID 또는 비밀번호를 사용하여 REST API에 로그인하지 않고 클라이언트 인증서를 대신 사용합니다. 자세한 정보는 [452 페이지의 『REST API 및 IBM MQ Console과 함께 클라이언트 인증서 인증 사용』의 내용을 참조하십시오](#).

성

mqwebuser.xml 파일 내에서 로컬 운영 체제 레지스트리를 구성할 수 있습니다. 로컬 운영 체제의 사용자 이름 및 비밀번호는 IBM MQ Console 및 REST API의 사용자를 인증하고 이 사용자에게 권한을 부여하는 데 사용됩니다.

시작하기 전에

- 로컬 OS 인증 기능을 사용하는 클라이언트 인증서 인증의 경우, 사용자 ID는 클라이언트 인증서의 식별 이름 (DN)에 있는 공통 이름(CN)입니다. 사용자 ID가 운영 체제 사용자로 존재하지 않는 경우 클라이언트 인증서로 그인이 실패하고 비밀번호 기반 인증으로 대체됩니다.
- 이 태스크를 완료하려면 권한이 있는 사용자여야 합니다.

이 태스크 정보

로컬 운영 체제 레지스트리를 사용하면 사용자 및 그룹에 자동으로 역할이 지정됩니다.

- IBM i의 'QMOMADM' 또는 'mqm' 그룹의 부분인 모든 사용자에게 MQWebAdmin 및 MFTWebAdmin 역할이 부여됩니다.
- 다른 모든 사용자에게 MQWebUser 역할이 부여됩니다.

이러한 역할에 대한 자세한 정보는 451 페이지의 『IBM MQ Console 및 REST API의 역할』의 내용을 참조하십시오.

로컬 운영 체제 레지스트리는 UNIX, Linux, and Windows에서만 사용할 수 있습니다. SAF 레지스트리를 구성하여 이에 해당하는 기능을 z/OS에 제공할 수 있습니다. 추가 정보는 448 페이지의 『IBM MQ Console 및 REST API에 대한 SAF 레지스트리 구성』의 내용을 참조하십시오.

프로시저

1. 다음 경로에서 샘플 XML 파일 local_os_registry.xml을 복사하십시오.
MQ_INSTALLATION_PATH/web/mq/samp/configuration
2. 다음 디렉토리에 샘플 파일을 배치하십시오.
MQ_DATA_PATH/web/installations/installationName/servers/mqweb
3. 옵션: mqwebuser.xml에서 구성 설정을 변경한 경우 이를 샘플 파일에 복사하십시오.
4. 기존 mqwebuser.xml 파일을 삭제하고 샘플 파일 이름을 mqwebuser.xml로 변경하십시오.

다음에 수행할 작업

사용자 인증 방법을 선택하십시오.

IBM MQ Console 인증 옵션

- 사용자가 토큰 인증을 사용하여 인증하게 합니다. 이 경우 사용자는 IBM MQ Console 로그인 화면에서 사용자 ID 및 비밀번호를 입력합니다. 사용자가 설정된 시간 동안 로그인되어 권한 부여된 상태를 유지할 수 있게 하는 LTPA 토큰이 생성됩니다. 이 인증 옵션을 사용하기 위해 추가 구성은 필요하지 않지만 선택적으로 LTPA 토큰의 만기 간격을 구성할 수 있습니다. 자세한 정보는 LTPA 토큰 만기 간격 구성을 참조하십시오.
- 사용자가 클라이언트 인증서를 사용하여 인증하게 합니다. 이 경우 사용자는 사용자 ID 또는 비밀번호를 사용하여 IBM MQ Console에 로그인하지 않고 클라이언트 인증서를 대신 사용합니다. 자세한 정보는 452 페이지의 『REST API 및 IBM MQ Console과 함께 클라이언트 인증서 인증 사용』의 내용을 참조하십시오.

REST API 인증 옵션

- 사용자가 HTTP 기본 인증을 사용하여 인증하게 합니다. 이 경우 사용자 이름 및 비밀번호가 인코딩되지만 암호화되지는 않으며 각각의 REST API 요청과 함께 전송되어 해당 요청에 대해 사용자를 인증하고 사용자

에게 권한을 부여합니다. 이 인증에 보안을 설정하려면 보안 연결을 사용해야 합니다. 즉, HTTPS를 사용해야 합니다. 자세한 정보는 456 페이지의 『REST API로 HTTP 기본 인증 사용』의 내용을 참조하십시오.

- 사용자가 토큰 인증을 사용하여 인증하게 합니다. 이 경우 사용자는 HTTP POST 메소드를 사용하여 사용자 ID 및 비밀번호를 REST API login 자원에 제공합니다. 사용자가 설정된 시간 동안 로그인되어 권한 부여된 상태를 유지할 수 있게 하는 LTPA 토큰이 생성됩니다. 추가 정보는 457 페이지의 『REST API로 토큰 기반 인증 사용』의 내용을 참조하십시오. LTPA 토큰의 만기 간격을 구성할 수 있습니다. 자세한 정보는 LTPA 토큰 구성을 참조하십시오.
- 사용자가 클라이언트 인증서를 사용하여 인증하게 합니다. 이 경우 사용자는 사용자 ID 또는 비밀번호를 사용하여 REST API에 로그인하지 않고 클라이언트 인증서를 대신 사용합니다. 자세한 정보는 452 페이지의 『REST API 및 IBM MQ Console과 함께 클라이언트 인증서 인증 사용』의 내용을 참조하십시오.

V9.1.0 IBM MQ Console 및 REST API에 대한 LDAP 레지스트리 구성

mqwebuser.xml 파일 내에서 LDAP 레지스트리를 구성할 수 있습니다. LDAP 레지스트리에 있는 사용자 이름 및 비밀번호는 IBM MQ Console 및 REST API의 사용자를 인증하고 이 사용자에게 권한을 부여하는 데 사용됩니다.

시작하기 전에

- LDAP 레지스트리를 구성할 때 각 사용자에게 역할을 지정해야 합니다. 각 역할은 IBM MQ Console 및 REST API에 액세스하는 데 필요한 다양한 레벨의 권한을 제공하고 허용된 조작이 시도될 때 사용되는 보안 컨텍스트를 판별합니다. 레지스트리를 구성하기 전에 이러한 역할을 이해해야 합니다. 각 역할에 대한 자세한 정보는 451 페이지의 『IBM MQ Console 및 REST API의 역할』의 내용을 참조하십시오.

MQWebUser 역할이 지정된 사용자는 큐 관리자에서 수행하도록 사용자 ID가 제공된 조작만 수행할 수 있습니다. 따라서 LDAP 서버에 정의된 사용자 ID는 IBM MQ가 설치된 시스템의 사용자 ID와 동일해야 합니다. 이러한 사용자 ID는 동일한 대소문자로 되어 있어야 합니다. 그렇지 않을 경우 사용자 ID 간 맵핑이 실패합니다.

- 이 작업을 완료하려면 mqwebuser.xml 파일을 편집할 수 있는 충분한 권한이 있는 사용자여야 합니다.
 - **z/OS** z/OS에서는 mqwebuser.xml 파일에 대한 쓰기 액세스 권한이 있어야 합니다.
 - **Multi** 다른 모든 운영 체제에서는 [권한이 있는 사용자](#)여야 합니다.

프로시저

1. 다음 경로 중 하나에서 샘플 XML 파일 ldap_registry.xml을 복사하십시오.

- **ULW** UNIX, Linux, and Windows: MQ_INSTALLATION_PATH /web/mq/samp/configuration
- **z/OS** z/OS: PathPrefix /web/mq/samp/configuration

여기서 PathPrefix는 IBM MQ Unix System Services 컴포넌트 설치 경로입니다.

2. 샘플 파일을 적절한 디렉토리에 배치하십시오.

- **ULW**
UNIX, Linux, and Windows: MQ_DATA_PATH/web/installations/installationName/servers/mqweb
- **z/OS**
z/OS: WLP_user_directory/servers/mqweb

여기서 WLP_user_directory는 mqweb 서버 정의를 작성하기 위해 **crtmqweb** 스크립트를 실행할 때 지정된 디렉토리입니다.

3. 옵션: mqwebuser.xml에서 구성 설정을 변경한 경우 이를 샘플 파일에 복사하십시오.

4. 기존 mqwebuser.xml 파일을 삭제하고 샘플 파일 이름을 mqwebuser.xml로 변경하십시오.

5. 새 mqwebuser.xml 파일을 편집하여 **ldapRegistry** 및 **idsLdapFilterProperties** 태그 내에서 LDAP 레지스트리 설정을 변경하십시오.

LDAP 레지스트리 구성에 대한 자세한 정보는 WebSphere Liberty 문서의 [Liberty의 LDAP 사용자 레지스트리 구성](#) 을 참조하십시오.

6. mqwebuser.xml 파일을 편집하여 사용자 및 그룹에 역할을 지정하십시오.

사용자 및 그룹에 IBM MQ Console 및 REST API를 사용할 수 있는 권한을 부여할 수 있는 몇 가지 역할이 있습니다. 각 역할은 서로 다른 레벨의 액세스 권한을 부여합니다. 추가 정보는 [451 페이지의 『IBM MQ Console 및 REST API의 역할』](#) 의 내용을 참조하십시오.

- IBM MQ Console에 역할을 지정하고 액세스 권한을 부여하려면 **<enterpriseApplication id="com.ibm.mq.console">** 태그 내의 해당 **security-role** 태그 사이에 사용자 및 그룹을 추가하십시오.
- REST API에 역할을 지정하고 액세스 권한을 부여하려면 **<enterpriseApplication id="com.ibm.mq.rest">** 태그 내의 해당 **security-role** 태그 사이에 사용자 및 그룹을 추가하십시오.

다음에 수행할 작업

사용자 인증 방법을 선택하십시오.

IBM MQ Console 인증 옵션

- 사용자가 토큰 인증을 사용하여 인증하게 합니다. 이 경우 사용자는 IBM MQ Console 로그인 화면에서 사용자 ID 및 비밀번호를 입력합니다. 사용자가 설정된 시간 동안 로그인되어 권한 부여된 상태를 유지할 수 있게 하는 LTPA 토큰이 생성됩니다. 이 인증 옵션을 사용하기 위해 추가 구성은 필요하지 않지만 선택적으로 LTPA 토큰의 만기 간격을 구성할 수 있습니다. 자세한 정보는 [LTPA 토큰 만기 간격 구성](#) 을 참조하십시오.
- 사용자가 클라이언트 인증서를 사용하여 인증하게 합니다. 이 경우 사용자는 사용자 ID 또는 비밀번호를 사용하여 IBM MQ Console에 로그인하지 않고 클라이언트 인증서를 대신 사용합니다. 자세한 정보는 [452 페이지의 『REST API 및 IBM MQ Console과 함께 클라이언트 인증서 인증 사용』](#) 의 내용을 참조하십시오.

REST API 인증 옵션

- 사용자가 HTTP 기본 인증을 사용하여 인증하게 합니다. 이 경우 사용자 이름 및 비밀번호가 인코딩되지만 암호화되지는 않으며 각각의 REST API 요청과 함께 전송되어 해당 요청에 대해 사용자를 인증하고 사용자에게 권한을 부여합니다. 이 인증에 보안을 설정하려면 보안 연결을 사용해야 합니다. 즉, HTTPS를 사용해야 합니다. 자세한 정보는 [456 페이지의 『REST API로 HTTP 기본 인증 사용』](#) 의 내용을 참조하십시오.
- 사용자가 토큰 인증을 사용하여 인증하게 합니다. 이 경우 사용자는 HTTP POST 메소드를 사용하여 사용자 ID 및 비밀번호를 REST API login 자원에 제공합니다. 사용자가 설정된 시간 동안 로그인되어 권한 부여된 상태를 유지할 수 있게 하는 LTPA 토큰이 생성됩니다. 추가 정보는 [457 페이지의 『REST API로 토큰 기반 인증 사용』](#) 의 내용을 참조하십시오. LTPA 토큰의 만기 간격을 구성할 수 있습니다. 자세한 정보는 [LTPA 토큰 구성](#) 을 참조하십시오.
- 사용자가 클라이언트 인증서를 사용하여 인증하게 합니다. 이 경우 사용자는 사용자 ID 또는 비밀번호를 사용하여 REST API에 로그인하지 않고 클라이언트 인증서를 대신 사용합니다. 자세한 정보는 [452 페이지의 『REST API 및 IBM MQ Console과 함께 클라이언트 인증서 인증 사용』](#) 의 내용을 참조하십시오.

IBM MQ Console 및 REST API에 대한 SAF 레지스트리 구성

SAF(System Authorization Facility) 인터페이스에서는 mqweb 서버가 인증 및 권한 부여 검사를 위해 ESM(External Security Manager)을 호출할 수 있습니다. 그런 다음 사용자는 z/OS 사용자 ID 및 비밀번호를 사용하여 IBM MQ Console 및 REST API 에 로그인할 수 있습니다.

시작하기 전에

- SAF 레지스트리를 구성할 때 사용자에게 역할을 지정해야 합니다. 각 역할은 IBM MQ Console 및 REST API 에 액세스하는 데 필요한 다양한 레벨의 권한을 제공하고 허용된 조작이 시도될 때 사용되는 보안 컨텍스트를

판별합니다. 레지스트리를 구성하기 전에 이러한 역할을 이해해야 합니다. 각 역할에 대한 자세한 정보는 [451 페이지의 『IBM MQ Console 및 REST API의 역할』](#)의 내용을 참조하십시오.

- SAF에 대해 권한 부여된 인터페이스를 사용하려면 WebSphere Liberty Angel 프로세스가 실행 중이어야 합니다. 자세한 정보는 [Liberty for z/OS에서 z/OS 권한 부여 서비스 사용](#) 을 참조하십시오.
- 이 태스크를 완료하려면 mqwebuser.xml 파일에 대한 쓰기 액세스 권한 및 보안 관리자 프로파일을 정의할 수 있는 권한이 있어야 합니다.

참고: **V9.1.0.20** IBM MQ 9.1.0 Fix Pack 20에서 샘플 구성 파일 zos_saf_registry.xml 가 중복된 safAuthorization 항목을 제거하도록 업데이트되었습니다.

이 업데이트는 z/OS 의 MQ Console 가 WebSphere Liberty Profile 22.0.0.12 이상을 제공하는 레벨 (즉, IBM MQ 9.1.0 Fix Pack 15에서) 로 업그레이드될 때 ICH408I 오류가 발생할 수 있는 문제를 수정합니다. 둘 이상의 safAuthorization 문이 지원되지 않으며 EBJROLE 클래스에서 MQWebAdmin 또는 MQWebAdminRO 역할에 없는 사용자가 MQ Console를 통해 z/OS 큐 관리자에 액세스하려는 경우 ICH408I 오류가 발생할 수 있습니다.

로그할 액세스 시도 유형을 지정하는 **racRouteLog**의 기본값은 NONE입니다. 보안 감사를 위해 추가 보고서 또는 레코드가 필요한 경우 자세한 정보는 [SAF 권한 \(safAuthorization\)](#) 을 참조하십시오.

이 태스크 정보

SAF 인터페이스에서는 mqweb 서버가 IBM MQ Console과 REST API 모두에 대한 인증 및 권한 부여 검사를 위해 ESM(External Security Manager)을 호출할 수 있습니다.

프로시저

1. z/OS용 Liberty에서 [z/OS 권한 부여 서비스 사용](#)의 단계에 따라 mqweb 서버에 z/OS 권한 부여 서비스를 사용할 수 있는 액세스 권한을 부여하십시오.
angel 프로세스를 시작하는 샘플 JCL은 USS_ROOT/web/templates/zos/procs/bbgzang1.jcl에 있습니다. 여기서, USS_ROOT는 IBM MQ for z/OS USS 컴포넌트가 설치된 UNIX System Services의 경로입니다.

bbgzang1.jcl에서 USS_ROOT/web를 가리키도록 SET ROOT문을 변경하십시오.
(예: /usr/lpp/mqm/V9R1M0/web).

angel 프로세스 중지 및 시작에 대한 추가 정보는 [z/OS에서 Liberty 관리를 참조하십시오](#).
2. [Liberty: SAF\(System Authorization Facility\) 인증되지 않은 사용자 설정](#)의 단계에 따라 Liberty에 필요한 인증되지 않은 사용자를 작성하십시오.
3. PathPrefix /web/mq/samp/configuration 경로에서 zos_saf_registry.xml 파일을 복사하십시오. 여기서 PathPrefix 는 IBM MQ Unix System Services 컴포넌트 설치 경로입니다.
4. 샘플 파일을 WLP_user_directory/servers/mqweb 디렉토리에 배치하십시오. 여기서 WLP_user_directory는 mqweb 서버 정의를 작성하기 위해 **crtmqweb** 스크립트를 실행할 때 지정된 디렉토리입니다.
5. 옵션: 이전에 mqwebuser.xml에서 구성 설정을 변경한 경우 이를 샘플 파일에 복사하십시오.
6. 기존 mqwebuser.xml 파일을 삭제하고 샘플 파일 이름을 mqwebuser.xml로 변경하십시오.
7. mqwebuser.xml의 **safCredentials** 요소를 사용자 정의하십시오.
 - a. **profilePrefix**를 Liberty 서버에 고유한 이름으로 설정하십시오. 둘 이상의 mqweb 서버가 단일 시스템에서 실행 중인 경우 서버마다 다른 이름을 선택해야 합니다(예: MQWEB910 및 MQWEB905).
 - b. **unauthenticatedUser**는 [449 페이지의 『2』](#) 단계에서 작성한 인증되지 않은 사용자의 이름으로 설정하십시오.
8. RACF에 대한 mqweb 서버 APPLID를 정의하십시오.
APPLID 자원 이름은 [449 페이지의 『7』](#) 단계에서 **profilePrefix** 속성에 지정한 값입니다. 다음 예에서는 RACF의 mqweb 서버 APPLID를 정의합니다.

```
RDEFINE APPL profilePrefix UACC(NONE)
```

9. MQ Console 또는 REST API에서 인증할 모든 사용자 또는 그룹에게 APPL 클래스의 mqweb 서버 APPLID에 대한 읽기 액세스 권한을 부여하십시오.

449 페이지의 『2』 단계에서 정의한 인증되지 않은 사용자에게 대해서도 이를 수행해야 합니다. 다음 예에서는 RACF의 mqweb 서버 APPLID에 대한 읽기 액세스 권한을 사용자에게 부여합니다.

```
PERMIT profilePrefix CLASS(APPL) ACCESS(READ) ID(userID)
```

10. MQ Console 및 REST API에서 사용자에게 역할에 대한 액세스 권한을 제공하기 위해 필요한 EJBROLE 클래스에 프로파일을 정의하십시오.

다음 예제는 RACF에서 프로파일을 정의합니다. 여기서 **profilePrefix** 은 449 페이지의 『7』 단계에서 **profilePrefix** 속성에 지정된 값입니다.

```
RDEFINE EJBROLE profilePrefix.com.ibm.mq.console.MQWebAdmin UACC(NONE)
RDEFINE EJBROLE profilePrefix.com.ibm.mq.console.MQWebAdminRO UACC(NONE)
RDEFINE EJBROLE profilePrefix.com.ibm.mq.console.MQWebUser UACC(NONE)
RDEFINE EJBROLE profilePrefix.com.ibm.mq.rest.MQWebAdmin UACC(NONE)
RDEFINE EJBROLE profilePrefix.com.ibm.mq.rest.MQWebAdminRO UACC(NONE)
RDEFINE EJBROLE profilePrefix.com.ibm.mq.rest.MQWebUser UACC(NONE)
RDEFINE EJBROLE profilePrefix.com.ibm.mq.rest.MFTWebAdmin UACC(NONE)
RDEFINE EJBROLE profilePrefix.com.ibm.mq.rest.MFTWebAdminRO UACC(NONE)
```

11. MQ Console 및 REST API에서 역할에 대해 사용자에게 액세스 권한을 부여하십시오.

이를 수행하려면 450 페이지의 『10』 단계에서 작성된 EJBROLE 클래스의 하나 이상 프로파일에 대해 사용자 또는 그룹이 읽기 액세스 권한을 제공하십시오. 역할에 대한 자세한 정보는 451 페이지의 『IBM MQ Console 및 REST API의 역할』의 내용을 참조하십시오.

다음 예제는 RACF에서 REST API의 MQWebAdmin 역할에 대한 사용자 액세스를 제공합니다. 여기서 **profilePrefix** 는 449 페이지의 『7』 단계에서 **profilePrefix** 속성에 지정된 값입니다.

```
PERMIT profilePrefix.com.ibm.mq.rest.MQWebAdmin CLASS(EJBROLE) ACCESS(READ) ID(userID)
```

결과

IBM MQ Console 및 REST API에 대해 SAF 인증을 설정했습니다.

다음에 수행할 작업

사용자 인증 방법을 선택하십시오.

IBM MQ Console 인증 옵션

- 사용자가 토큰 인증을 사용하여 인증하게 합니다. 이 경우 사용자는 IBM MQ Console 로그인 화면에서 사용자 ID 및 비밀번호를 입력합니다. 사용자가 설정된 시간 동안 로그인되어 권한 부여된 상태를 유지할 수 있게 하는 LTPA 토큰이 생성됩니다. 이 인증 옵션을 사용하기 위해 추가 구성은 필요하지 않지만 선택적으로 LTPA 토큰의 만기 간격을 구성할 수 있습니다. 자세한 정보는 [LTPA 토큰 만기 간격 구성을 참조하십시오](#).
- 사용자가 클라이언트 인증서를 사용하여 인증하게 합니다. 이 경우 사용자는 사용자 ID 또는 비밀번호를 사용하여 IBM MQ Console에 로그인하지 않고 클라이언트 인증서를 대신 사용합니다. 자세한 정보는 452 페이지의 『REST API 및 IBM MQ Console과 함께 클라이언트 인증서 인증 사용』의 내용을 참조하십시오.

REST API 인증 옵션

- 사용자가 HTTP 기본 인증을 사용하여 인증하게 합니다. 이 경우 사용자 이름 및 비밀번호가 인코딩되지만 암호화되지는 않으며 각각의 REST API 요청과 함께 전송되어 해당 요청에 대해 사용자를 인증하고 사용자에게 권한을 부여합니다. 이 인증에 보안을 설정하려면 보안 연결을 사용해야 합니다. 즉, HTTPS를 사용해야 합니다. 자세한 정보는 456 페이지의 『REST API로 HTTP 기본 인증 사용』의 내용을 참조하십시오.
- 사용자가 토큰 인증을 사용하여 인증하게 합니다. 이 경우 사용자는 HTTP POST 메소드를 사용하여 사용자 ID 및 비밀번호를 REST API login 자원에 제공합니다. 사용자가 설정된 시간 동안 로그인되어 권한 부여된 상태를 유지할 수 있게 하는 LTPA 토큰이 생성됩니다. 추가 정보는 457 페이지의 『REST API로 토큰 기반 인증 사용』의 내용을 참조하십시오. LTPA 토큰의 만기 간격을 구성할 수 있습니다. 자세한 정보는 [LTPA 토큰 구성을 참조하십시오](#).

- 사용자가 클라이언트 인증서를 사용하여 인증하게 합니다. 이 경우 사용자는 사용자 ID 또는 비밀번호를 사용하여 REST API에 로그인하지 않고 클라이언트 인증서를 대신 사용합니다. 자세한 정보는 [452 페이지](#)의 『REST API 및 IBM MQ Console과 함께 클라이언트 인증서 인증 사용』의 내용을 참조하십시오.

V 9.1.0 IBM MQ Console 및 REST API의 역할

IBM MQ Console 또는 REST API을(를) 사용하도록 사용자와 그룹에 권한을 부여하는 경우 사용 가능한 **MQWebAdmin**, **MQWebAdminRO**, **MQWebUser**, **MFTWebAdmin** 및 **MFTWebAdminRO** 역할 중 하나를 사용자와 그룹에 지정해야 합니다. 각 역할은 IBM MQ Console 및 REST API에 액세스하는 데 필요한 다양한 레벨의 권한을 제공하고 허용된 조작이 시도될 때 사용되는 보안 컨텍스트를 판별합니다.

참고: **MQWebUser** 역할을 제외하고 사용자 ID는 대소문자를 구분하지 않습니다. 이 역할에 대한 특정 요구사항은 [451 페이지](#)의 『MQWebUser』의 내용을 참조하십시오.

MQWebAdmin

이 역할이 지정된 사용자 및 그룹은 모든 관리 조작을 수행할 수 있고 mqweb 서버를 시작하는 데 사용된 운영 체제 사용자 ID의 보안 컨텍스트에서 작업합니다.

이 역할의 사용자 또는 그룹에 다음 REST 서비스에 대한 액세스 권한이 없습니다.

- MFT의 REST API입니다. 이러한 서비스를 사용하려면 사용자 또는 그룹에도 **MFTWebAdmin** 또는 **MFTWebAdminRO** 역할이 지정되어야 합니다.
- messaging REST API입니다. messaging REST API을(를) 사용하려면 사용자에게 **MQWebUser** 역할이 지정되어야 합니다.

MQWebAdminRO

이 역할은 IBM MQ Console 또는 REST API에 대한 읽기 전용 액세스 권한만 제공합니다. 이 역할이 지정된 사용자 및 그룹은 다음 조작을 수행할 수 있습니다.

- 큐 및 채널과 같은 IBM MQ 오브젝트에서 조작을 표시 및 조회합니다.
- 큐에서 메시지를 찾아봅니다.

이 역할이 지정된 사용자 또는 그룹은 mqweb 서버를 시작하는 데 사용된 운영 체제 사용자 ID의 보안 컨텍스트에서 작업합니다.

이 역할의 사용자 또는 그룹에 다음 REST 서비스에 대한 액세스 권한이 없습니다.

- MFT의 REST API입니다. 이러한 서비스를 사용하려면 사용자 또는 그룹에도 **MFTWebAdmin** 또는 **MFTWebAdminRO** 역할이 지정되어야 합니다.
- messaging REST API입니다. messaging REST API을(를) 사용하려면 사용자에게 **MQWebUser** 역할이 지정되어야 합니다.

MQWebUser

이 역할이 지정된 사용자 또는 그룹은 큐 관리자에서 수행하도록 사용자 ID에 부여된 모든 조작을 수행할 수 있습니다. 예를 들면, 다음과 같습니다.

- 채널과 같은 IBM MQ 오브젝트에서 조작을 시작 및 중지합니다.
- 큐 및 채널 같은 IBM MQ 오브젝트에서 조작을 정의 및 설정합니다.
- 큐 및 채널과 같은 IBM MQ 오브젝트에서 조작을 표시 및 조회합니다.
- messaging REST API를 사용하여 메시지를 넣고 가져옵니다.

이 역할이 지정된 사용자 또는 그룹은 프린시펄의 보안 컨텍스트에서 작업하고, 큐 관리자에서 수행하기 위해 사용자 ID가 제공된 조작만 수행할 수 있습니다.

따라서 mqweb 사용자 레지스트리에서 정의되는 사용자 또는 그룹이 조작을 수행하려면 먼저 해당 사용자 또는 그룹에 IBM MQ 내의 권한을 부여해야 합니다. 이 역할을 사용하면 IBM MQ Console 및 REST API를 사용할 때 특정 IBM MQ 자원에 대한 액세스 유형이 있는 사용자를 정교하게 제어할 수 있습니다.

참고:

- 이 역할이 지정된 사용자 ID의 최대 길이는 12자입니다.

- 사용자 ID의 대소문자는 mqweb 사용자 레지스트리와 IBM MQ 시스템에서 동일해야 합니다. 사용자 ID의 대소문자가 서로 다르면 사용자는 IBM MQ Console 및 REST API에서 인증될 수 있지만 IBM MQ 자원을 사용하는 권한을 부여받지는 않습니다.

이 역할이 있는 사용자 또는 그룹은 MFT 서비스에 대한 REST API에 대한 액세스 권한이 없습니다. 이러한 서비스를 사용하려면 사용자 또는 그룹에도 **MFTWebAdmin** 또는 **MFTWebAdminRO** 역할이 지정되어야 합니다.

MFTWebAdmin

이 역할이 지정된 사용자 또는 그룹은 모든 MFT REST 조작을 수행할 수 있으며 mqweb 서버를 시작하는 데 사용되는 운영 체제 사용자 ID의 보안 컨텍스트에서 작동합니다.

이 역할의 사용자 또는 그룹에 IBM MQ REST API 서비스에 대한 액세스 권한이 없습니다. 이러한 서비스를 사용하려면 사용자 또는 그룹에도 **MQWebAdmin**, **MQWebAdminRO** 또는 **MQWebUser** 역할이 지정되어야 합니다.

MFTWebAdminRO

이 역할은 MFT에 대한 REST API에 대한 읽기 전용 액세스를 제공합니다. 이 역할이 지정된 사용자 또는 그룹은 전송 나열 또는 에이전트 나열과 같이 읽기 전용 조작(GET 요청)만 수행할 수 있습니다.

이 역할이 지정된 사용자 또는 그룹은 mqweb 서버를 시작하는 데 사용된 운영 체제 사용자 ID의 보안 컨텍스트에서 작업합니다.

이 역할의 사용자 또는 그룹에 IBM MQ REST API 서비스에 대한 액세스 권한이 없습니다. 이러한 서비스를 사용하려면 사용자 또는 그룹에도 **MQWebAdmin**, **MQWebAdminRO** 또는 **MQWebUser** 역할이 지정되어야 합니다.

이 역할을 사용하도록 사용자 및 그룹을 구성하는 자세한 정보는 [442 페이지의 『사용자 및 역할 구성』](#)의 내용을 참조하십시오.

역할 겹침

사용자 또는 그룹에 두 개 이상의 역할이 지정될 수 있습니다. 이런 상황에서 사용자가 조작을 수행하면 조작에 적용되는 가장 높은 권한 역할이 사용됩니다. 예를 들어, 역할이 **MQWebAdminRO**이고 **MQWebUser**에서 조회 쿼리 조작을 수행하는 경우 **MQWebAdminRO** 역할이 사용되고 웹 서버를 시작한 시스템 사용자 ID의 컨텍스트에서 조작을 시도합니다. 동일한 사용자가 정의 조작을 수행하는 경우 **MQWebUser** 역할이 사용되고 프린시펄의 컨텍스트에서 조작을 시도합니다.

ULW V9.1.0 REST API 및 IBM MQ Console과 함께 클라이언트 인증서 인증 사용

클라이언트 인증서를 프린시펄에 맵핑하여 IBM MQ Console 및 REST API 사용자를 인증할 수 있습니다.

시작하기 전에

- IBM MQ Console 및 REST API를 사용할 수 있는 권한이 부여되도록 사용자, 그룹 및 역할을 구성하십시오. 추가 정보는 [442 페이지의 『사용자 및 역할 구성』](#)의 내용을 참조하십시오.
- REST API를 사용하는 경우 login 자원에서 HTTP GET 메소드를 사용하여 현재 사용자의 신임 정보를 조회하여 클라이언트 인증서를 제공하여 요청을 인증할 수 있습니다. 이 요청은 사용자 이름 및 사용자에게 지정된 역할에 대한 정보를 리턴합니다. 자세한 정보는 [GET /login](#)을 참조하십시오.
- 클라이언트 인증서를 프린시펄에 맵핑하여 사용자를 인증할 경우 클라이언트 인증서의 식별 이름을 사용하여 구성된 사용자 레지스트리의 사용자와 비교합니다.
 - 기본 레지스트리의 경우 공통 이름(CN)을 사용자와 비교합니다. 예를 들어, CN=Fred, O=IBM, C=GB는 Fred 사용자 이름과 비교합니다.
 - LDAP 레지스트리의 경우 기본적으로 전체 식별 이름을 LDAP과 비교합니다. 필터 및 맵핑을 설정하여 비교를 사용자 정의할 수 있습니다. 자세한 정보는 WebSphere Liberty 문서의 [Liberty :LDAP 인증 맵 모드](#)를 참조하십시오.

이 태스크 정보

클라이언트 인증서를 사용하여 사용자가 인증되는 경우 사용자 이름 및 비밀번호 대신 인증서가 사용됩니다. REST API의 경우, 클라이언트 인증서가 사용자 인증을 위해 각 REST 요청과 함께 제공됩니다. IBM MQ Console의 경우 사용자가 인증서를 사용하여 로그인하면 사용자가 로그아웃할 수 없습니다.

프로시저에서는 다음과 같은 정보를 가정합니다.

- mqwebuser.xml 파일이 다음 샘플 중 하나를 기반으로 합니다.
 - basic_registry.xml
 - local_os_registry.xml
 - ldap_registry.xml
- UNIX, Linux 또는 Windows 시스템을 사용 중입니다.
- 권한이 있는 사용자입니다.

z/OS에서 RACF 키 링을 사용하여 클라이언트 인증서 인증을 구성하려면 [464 페이지의 『Configuring TLS for the REST API and IBM MQ Console on z/OS』](#)의 프로시저를 따르십시오.

참고: 다음 프로시저에서는 IBM MQ Console 및 REST API와 함께 클라이언트 인증서를 사용하기 위해 필요한 단계에 대해 간략하게 설명합니다. 개발자 편의를 위해 단계에서는 자체 서명 인증서를 작성하고 사용하는 방법을 자세히 설명합니다. 하지만 프로덕션의 경우 인증 기관에서 확보한 인증서를 사용하십시오.

프로시저

1. 명령행에서 **strmqweb** 명령을 입력하여 mqweb 서버를 시작하십시오.
2. 클라이언트 인증서를 작성하십시오.
 - a) PKCS#12 키 저장소를 작성하십시오.
 - i) 명령행에서 **strmqikm** 명령을 입력하여 IBM Key Management 도구를 여십시오.
 - ii) IBM Key Management 도구의 **키 데이터베이스 파일** 메뉴에서 **새로 작성**을 클릭하십시오.
 - iii) **키 데이터베이스 유형** 목록에서 **PKCS12**를 선택하십시오.
 - iv) 키 저장소를 저장할 위치를 선택한 후 **파일 이름** 필드에 적절한 이름을 입력하십시오. 예: `user.p12`
 - v) 프롬프트가 표시되면 비밀번호를 설정하십시오.
 - b) 자체 서명 인증서를 작성하거나 인증 기관에서 인증서를 얻어 인증서를 작성하십시오.
 - 자체 서명 인증서를 작성하십시오.
 - i) **새 자체 서명**을 클릭하십시오.
 - ii) **키 레이블** 필드에 `user`를 입력하십시오.
 - iii) 기본 사용자 레지스트리를 사용하는 경우에는 **공용 이름** 필드에 사용자 레지스트리에서 제공된 사용자 이름을 입력하십시오. 예를 들어, `mqadmin`입니다. LDAP 사용자 레지스트리의 경우 인증서에 대한 식별 이름이 LDAP 레지스트리에 있는 식별 이름과 일치하는지 확인하십시오.
 - iv) **확인**을 클릭하십시오.
 - 인증 기관에서 인증서를 확보하십시오. CA 인증서는 식별 이름(DN) 필드의 공용 이름(CN)에 적절한 사용자 이름을 포함해야 합니다.
 - i) 새 인증서를 요청하십시오. **작성** 메뉴에서 **새 인증서 요청**을 클릭하십시오.
 - ii) **키 레이블** 필드에 인증서 레이블을 입력하십시오.
 - iii) 기본 사용자 레지스트리를 사용하는 경우 **공통 이름** 필드에 인증서의 대상이 되는 사용자의 사용자 이름을 입력하십시오.
로컬 OS 레지스트리를 사용하는 경우 **공통 이름** 필드가 로컬 OS 사용자 ID와 일치해야 합니다.
LDAP 사용자 레지스트리의 경우 인증서에 대한 식별 이름이 LDAP 레지스트리에 있는 식별 이름과 일치하는지 확인하십시오.
 - iv) 해당되는 경우 나머지 필드에 대한 값을 입력하거나 선택하십시오.

- v) 인증서 요청을 저장할 위치 및 인증서 요청에 대한 파일 이름을 선택한 후 **확인**을 클릭하십시오.
 - vi) 인증서 요청 파일을 인증 기관(CA)에 전송하십시오.
 - vii) CA에서 제공된 인증서를 가지고 있는 경우 명령행에서 **strmqikm** 명령을 입력하여 IBM Key Management 도구를 여십시오.
 - viii) IBM Key Management 도구의 **키 데이터베이스 파일** 메뉴에서 **열기**를 클릭하십시오.
 - ix) 클라이언트 인증서를 보유하는 PKCS#12 키 저장소를 선택하십시오. 예: `user.p12`
 - x) **수신**을 클릭하고 적절한 인증서를 선택한 후 **확인**을 클릭하십시오.
3. 클라이언트 인증서의 공용 부분을 추출하십시오.
- a) 명령행에서 **strmqikm** 명령을 입력하여 IBM Key Management 도구를 여십시오.
 - b) IBM Key Management 도구의 **키 데이터베이스 파일** 메뉴에서 **열기**를 클릭하십시오.
 - c) 클라이언트 인증서를 보유하는 PKCS#12 키 저장소를 선택하십시오. 예: `user.p12`
 - d) IBM Key Management 도구의 인증서 목록에서 클라이언트 인증서를 선택하십시오.
 - e) **인증서 추출**을 클릭하십시오.
 - f) 인증서를 저장할 위치를 선택한 후 **인증서 파일 이름** 필드에 적절한 파일 이름을 입력하십시오. 예를 들어, `user.arm`입니다.
4. 서버가 클라이언트 인증서를 유효성 검증할 수 있도록 클라이언트 인증서의 공용 부분을 서명자 인증서로서 mqweb 서버 신뢰 키 저장소로 가져오십시오.
- a) mqweb 서버에서 사용할 `trust.jks` 키 저장소가 없는 경우 작성하십시오.
 - i) IBM Key Management 도구의 **키 데이터베이스 파일** 메뉴에서 **새로 작성**을 클릭하십시오.
 - ii) **키 데이터베이스 유형** 목록에서 **JKS**를 선택하십시오.
 - iii) **찾아보기**를 클릭하고 `MQ_DATA_DIRECTORY/web/installations/installationName/servers/mqweb/resources/security`로 이동하십시오.

이 디렉토리에는 `key.jks` 파일이 이미 있어야 합니다. `trust.jks` 파일이 이미 있는 경우 이 파일을 덮어쓰는 대신 기존 파일을 여십시오.
 - iv) **파일 이름** 필드에 `trust.jks`를 입력하십시오.
 - v) 프롬프트가 표시되면 비밀번호를 설정하십시오.
 - b) 드롭 다운 메뉴에서 **서명자 인증서**를 선택하십시오.
 - c) **추가**를 클릭하십시오.
 - d) 적절한 ARM 파일을 선택한 후 **확인**을 클릭하십시오. 예를 들어, `user.arm`을 선택하십시오.
 - e) 인증서에 대한 레이블을 입력하십시오.
5. mqweb 서버 키 저장소의 비밀번호를 변경하십시오.
- a) **키 데이터베이스 파일** 메뉴에서 **열기**를 클릭하십시오.
 - b) **키 데이터베이스 유형** 목록에서 **JKS**를 선택하십시오.
 - c) **찾아보기**를 클릭하고 `MQ_DATA_PATH/web/installations/installationName/servers/mqweb/resources/security`로 이동하십시오.
 - d) `key.jks` 키 저장소를 선택한 후 **열기**를 클릭하십시오.
 - e) 프롬프트가 표시되면 비밀번호를 입력하십시오. 기본 비밀번호는 `password`입니다.
 - f) **키 데이터베이스 파일** 메뉴에서 **비밀번호 변경**을 클릭하십시오.
 - g) 키 저장소의 새 비밀번호를 입력하십시오.
6. `mqwebuser.xml` 파일에서 클라이언트 인증서 인증을 사용으로 설정하십시오.
- `mqwebuser.xml` 파일은 다음 경로에서 찾을 수 있습니다. `MQ_DATA_PATH/web/installations/installationName/servers/mqweb`
- a) 클라이언트 인증서 인증을 사용으로 설정하는 `mqwebuser.xml` 파일의 섹션을 주석 해제하십시오. 섹션에는 다음 텍스트가 포함되어 있습니다.

```
<keyStore id="defaultKeyStore" location="key.jks" type="JKS" password="password"/>
  <keyStore id="defaultTrustStore" location="trust.jks" type="JKS" password="password"/>
  <ssl id="thisSSLConfig" clientAuthenticationSupported="true"
keyStoreRef="defaultKeyStore"
  trustStoreRef="defaultTrustStore" sslProtocol="TLSv1.2"
serverKeyAlias="default"/>
  <sslDefault sslRef="thisSSLConfig"/>
```

- b) **serverKeyAlias** 값이 서버 인증서의 이름과 일치하는지 확인하십시오. 기본 서버 인증서를 사용하는 경우에는 값이 올바릅니다.
- c) defaultKeyStore에 대한 **password**의 값을 key.jks 키 저장소에 대한 비밀번호의 인코딩된 버전으로 변경하십시오.

i) MQ_INSTALLATION_PATH/web/bin 디렉토리에서 명령행에 다음 명령을 입력하십시오.

```
securityUtility encode password
```

ii) defaultKeyStore에 대한 **비밀번호** 필드에 이 명령의 출력을 배치하십시오.

- d) trust.jks 키 저장소에 대한 비밀번호와 일치하도록 defaultTrustStore에 대한 **비밀번호**의 값을 변경하십시오.

i) MQ_INSTALLATION_PATH/web/bin 디렉토리에서 명령행에 다음 명령을 입력하십시오.

```
securityUtility encode password
```

ii) defaultTrustStore에 대한 **비밀번호** 필드에 이 명령의 출력을 배치하십시오.

- e) mqwebuser.xml에서 다음 행을 제거하거나 주석 처리하십시오.

```
<sslDefault sslRef="mqDefaultSSLConfig"/>
```

7. 명령행에서 **endmqweb** 명령을 입력하여 mqweb 서버를 중지하십시오.

8. 명령행에서 **strmqweb** 명령을 입력하여 mqweb 서버를 시작하십시오.

9. 클라이언트 인증서를 사용하여 인증하십시오.

- IBM MQ Console과 함께 클라이언트 인증서를 사용하려면 IBM MQ Console에 액세스하는 데 사용되는 웹 브라우저에 클라이언트 인증서를 설치하십시오. 예를 들어, 클라이언트 인증서 user.p12를 개인 인증서로 설치하십시오.
- REST API에 대해 클라이언트 인증서를 사용하려면 각각의 REST 요청과 함께 클라이언트 인증서를 제공하십시오. HTTP POST, PATCH 또는 DELETE 메소드를 사용하는 경우에는 사이트 간 요청 위조 공격을 방지하기 위해 클라이언트 인증서와 함께 추가 인증을 제공해야 합니다. 즉, 추가 인증은 요청을 인증하는 데 사용 중인 신임 정보가 신임 정보의 소유자에 의해 사용 중인지 확인하는 데 사용됩니다.

이 추가 인증은 **ibm-mq-rest-csrf-token** HTTP 헤더가 있어야 제공됩니다. **ibm-mq-csrf-token** 헤더의 값을 공백을 포함한 임의 값으로 설정한 다음 요청을 제출하십시오.

예

중요사항: 이 예에서 모든 cURL 구현이 자체 서명 인증서를 지원하는 것은 아니므로, 이를 지원하는 cURL 구현을 사용해야 합니다.

다음 cURL 예에서는 클라이언트 인증서 인증을 사용하여 큐 관리자(QM1)에서 새 큐 Q1을 작성하는 방법을 보여줍니다. 이 cURL 명령의 정확한 구성은 cURL이 빌드된 라이브러리에 따라 다릅니다. 이 예는 OpenSSL에 대해 cURL이 빌드된 Windows 시스템을 기반으로 합니다.

- 클라이언트 인증서로 인증하고 임의 값으로 **ibm-mq-rest-csrf-token** HTTP 헤더를 포함하여 큐 자원과 함께 HTTP POST 메소드를 사용하십시오. 이 값은 공백을 포함하여 임의의 값이 될 수 있습니다. **--cert-type** 플래그는 인증서가 PKCS#12 인증서가 되도록 지정합니다. **--cert** 플래그는 콜론(:)이 뒤에 오는 인증서의 위치를 지정한 후 인증서의 비밀번호를 지정합니다.

```
curl -k https://localhost:9443/ibmmq/rest/v1/admin/qmgr/QM1/queue -X POST -
-cert-type P12 --cert c:\user.p12:password
```

```
-H "ibm-mq-rest-csrf-token: value"
-H "Content-Type: application/json" --data "{\"name\":\"Q1\"}"
```

V 9.1.0 REST API로 HTTP 기본 인증 사용

REST API의 사용자는 HTTP 헤더에 사용자 ID 및 비밀번호를 제공하여 인증할 수 있습니다. HTTP 메소드(예: POST, PATCH, DELETE)와 함께 이 인증 방법을 사용하려면 사용자 ID 및 비밀번호와 함께 `ibm-mq-rest-csrf-token` HTTP 헤더도 제공해야 합니다.

시작하기 전에

- REST API를 사용할 수 있는 권한이 부여되도록 사용자, 그룹 및 역할을 구성하십시오. 자세한 정보는 [442 페이지](#)의 『사용자 및 역할 구성』의 내용을 참조하십시오.
- HTTP 기본 인증이 사용으로 설정되어 있는지 확인하십시오. `mqwebuser.xml` 파일에 다음 XML이 제공되며 주석 처리되어 있지 않은지 확인하십시오. 이 XML은 `<featureManager>` 태그 내에 있어야 합니다.

```
<feature>basicAuthenticationMQ-1.0</feature>
```

z/OS z/OS에서 이 파일을 편집하려면 `mqwebuser.xml`에 대한 쓰기 액세스 권한이 있는 사용자여야 합니다.

Multi 다른 모든 운영 체제에서 `mqwebuser.xml` 파일을 편집하려면 권한이 있는 사용자여야 합니다.

- REST 요청을 전송할 때 보안 연결을 사용하고 있는지 확인하십시오. 사용자 이름 및 비밀번호 조합은 인코딩되지만 암호화되지는 않으므로 REST API에 대해 HTTP 기본 인증을 사용하는 경우 보안 연결(HTTPS)을 사용해야 합니다.
- `login` 자원에 대해 HTTP GET 메소드를 사용하여 현재 사용자의 신임 정보를 조회하여 기본 인증 정보를 제공하여 요청을 인증할 수 있습니다. 이 요청은 사용자 이름 및 사용자에게 지정된 역할에 대한 정보를 리턴합니다. 자세한 정보는 [GET /login](#)을 참조하십시오.

프로시저

1. 사용자 이름을 콜론 및 비밀번호와 연결하십시오. 사용자 이름은 대소문자를 구분합니다. 예를 들어, 사용자 이름 `admin`과 비밀번호 `admin`은 다음 문자열이 됩니다.

```
admin:admin
```

2. base64 인코딩으로 사용자 이름 및 비밀번호 문자열을 인코딩하십시오.
3. 이 인코딩된 사용자 이름 및 비밀번호를 HTTP Authorization: Basic 헤더에 포함하십시오. 예를 들어, 인코딩된 사용자 이름이 `admin`이고 비밀번호가 `admin`이면 다음 헤더가 작성됩니다.

```
Authorization: Basic YWRtaW46YWRtaW4=
```

4. HTTP POST, PATCH 또는 DELETE 메소드를 사용하는 경우에는 사용자 이름 및 비밀번호 외에 추가 인증을 제공해야 합니다. 이 추가 인증은 `ibm-mq-rest-csrf-token` HTTP 헤더가 있어야 제공됩니다. `ibm-mq-rest-csrf-token` HTTP 헤더가 요청에 있어야 하지만 해당 값은 공백을 포함한 임의 값이 될 수 있습니다.
5. 적절한 헤더를 사용하여 REST 요청을 IBM MQ에 제출하십시오.

예

다음 예제는 Windows 시스템에서 기본 인증을 사용하여 큐 관리자 QM1에서 새 큐 Q1를 작성하는 방법을 보여줍니다. 예에서는 cURL을 사용합니다.

- 기본 인증으로 인증하고 임의 값으로 `ibm-mq-rest-csrf-token` HTTP 헤더를 포함하여 큐 자원과 함께 HTTP POST 메소드를 사용하십시오. 이 값은 공백을 포함한 임의의 값이 될 수 있습니다.

```
curl -k https://localhost:9443/ibmmq/rest/v1/admin/qmgr/QM1/queue -X POST
-u mqadmin:mqadmin
-H "ibm-mq-rest-csrf-token: value"
-H "Content-Type: application/json" --data "{\"name\":\"Q1\"}"
```

V 9.1.0 REST API로 토큰 기반 인증 사용

REST API의 사용자는 HTTP POST 메소드를 사용하여 사용자 ID 및 비밀번호를 REST API `login` 자원에 제공하여 인증할 수 있습니다. 이 사용자가 향후 요청을 인증할 수 있게 하는 LTPA 토큰이 생성됩니다. 이 LTPA 토큰에는 접두부 `LtpaToken2`가 있습니다. 이 사용자는 HTTP DELETE 메소드를 사용하여 로그아웃할 수 있고 HTTP GET 메소드를 사용하여 현재 사용자의 로그인 정보를 조회할 수 있습니다.

시작하기 전에

- REST API를 사용할 수 있는 권한이 부여되도록 사용자, 그룹 및 역할을 구성하십시오. 자세한 정보는 [442 페이지의 『사용자 및 역할 구성』](#)의 내용을 참조하십시오.
- 기본적으로 LTPA 토큰이 포함된 쿠키 이름은 `LtpaToken2`로 시작되며, `mqweb` 서버가 재시작될 때 변경될 수 있는 접미부를 포함합니다. 이 랜덤화된 쿠키 이름으로 동일한 시스템에서 둘 이상의 `mqweb` 서버를 실행할 수 있습니다. 하지만 쿠키 이름을 일관된 값으로 유지하려면 `setmqweb` 명령을 사용하여 쿠키의 이름을 지정할 수 있습니다. 자세한 정보는 [LTPA 토큰 구성](#)을 참조하십시오.
- 기본적으로 LTPA 토큰 쿠키는 120분 후에 만료됩니다. `setmqweb` 명령을 사용하여 LTPA 토큰 쿠키의 만기 시간을 구성할 수 있습니다. 자세한 정보는 [LTPA 토큰 구성](#)을 참조하십시오.
- REST 요청을 전송할 때 보안 연결을 사용하고 있는지 확인하십시오. `login` 자원에서 HTTP POST 메소드를 사용하는 경우 요청과 함께 전송되는 사용자 이름 및 비밀번호 조합은 암호화되지 않습니다. 따라서 REST API에 대해 토큰 기반 인증을 사용하는 경우 보안 연결(HTTPS)을 사용해야 합니다. 기본적으로 LTPA 토큰 인증으로 HTTP를 사용할 수 없습니다. `secureLTPA`를 `False`로 설정하여 비보안 HTTP 연결에서 사용할 LTPA 토큰을 사용으로 설정할 수 있습니다. 자세한 정보는 [LTPA 토큰 구성](#)을 참조하십시오.
- `login` 자원에서 HTTP GET 메소드를 사용하여 현재 사용자의 신임 정보를 조회하며 LTPA 토큰을 제공하여 요청을 인증할 수 있습니다. 이 요청은 사용자 이름 및 사용자에게 지정된 역할에 대한 정보를 리턴합니다. 자세한 정보는 [GET /login](#)을 참조하십시오.

프로시저

1. 사용자로 로그인하십시오.
 - a) `login` 자원에서 HTTP POST 메소드를 사용하십시오.

```
https://host:port/ibmmq/rest/v1/login
```

다음 형식으로 사용자 이름 및 비밀번호를 JSON 요청의 본문에 포함하십시오.

```
{
  "username" : name,
  "password" : password
}
```

- b) 요청에서 리턴되는 LTPA 토큰을 로컬 쿠키 저장소에 저장하십시오. 기본적으로 이 LTPA 토큰에 `LtpaToken2` 접두부가 있습니다.
2. 모든 요청의 쿠키로서 저장된 LTPA 토큰을 사용하여 REST 요청을 인증하십시오.

HTTP PUT, PATCH 또는 DELETE 메소드를 사용하는 요청의 경우 `ibm-mq-rest-csrf-token` 헤더를 포함하십시오. 이 헤더 값은 공백을 포함하여 임의의 값이 될 수 있습니다.
 3. 사용자로 로그아웃하십시오.
 - a) `login` 자원에서 HTTP DELETE 메소드를 사용하십시오.

```
https://host:9443/ibmmq/rest/v1/login
```

LTPA 토큰을 쿠키로서 제공하여 요청을 인증하고 `ibm-mq-rest-csrf-token` 헤더를 포함해야 합니다. 이 헤더 값은 공백을 포함하여 임의의 값이 될 수 있습니다.

- b) 지시사항을 처리하여 로컬 쿠키 저장소에서 LTPA 토큰을 삭제하십시오.

참고: 지시사항이 처리되지 않고 LTPA 토큰이 로컬 쿠키 저장소에 남는 경우 LTPA 토큰은 이후 REST 요청을 인증하는 데 사용할 수 있습니다. 즉, 사용자가 세션이 종료된 후에 LTPA 토큰으로 인증하려고 시도하는 경우 기존 토큰을 사용하는 새 세션이 작성됩니다.

예

다음 cURL 예제는 Windows 시스템에서 토큰 기반 인증을 사용하여 큐 관리자 QM1에서 새 큐 Q1를 작성하는 방법을 보여줍니다.

- 로그인하여 접두부가 `LtpaToken2`인 LTPA 토큰을 로컬 쿠키 저장소에 추가하십시오. 사용자 이름 및 비밀번호 정보가 JSON 본문에 포함됩니다. `-c` 플래그는 토큰을 저장할 파일의 위치를 지정합니다.

```
curl -k https://localhost:9443/ibmmq/rest/v1/login -X POST
-H "Content-Type: application/json" --data
"{\"username\": \"mqadmin\", \"password\": \"mqadmin\"}"
-c c:\cookiejar.txt
```

- 큐를 작성하십시오. 큐 자원과 함께 HTTP POST 메소드를 사용하여 LTPA 토큰에 대해 인증하십시오. 접두부가 `LtpaToken2`인 LTPA 토큰은 `-b` 플래그를 사용하여 `cookiejar.txt` 파일에서 검색됩니다. CSRF 보호는 `ibm-mq-rest-csrf-token` HTTP 헤더가 있어야 제공됩니다.

```
curl -k https://localhost:9443/ibmmq/rest/v1/admin/qmgr/QM1/queue -X POST -b
c:\cookiejar.txt -H "ibm-mq-rest-csrf-token: value" -H "Content-Type: application/json"
--data "{\"name\": \"Q1\"}"
```

- 로그아웃한 후 로컬 쿠키 저장소에서 LTPA 토큰을 삭제하십시오. LTPA 토큰은 `-b` 플래그를 사용하여 `cookiejar.txt` 파일에서 검색됩니다. CSRF 보호는 `ibm-mq-rest-csrf-token` HTTP 헤더의 존재에 의해 제공됩니다. `cookiejar.txt` 파일의 위치는 `-c` 플래그에 의해 지정되어 LTPA 토큰이 파일에서 삭제됩니다.

```
curl -k https://localhost:9443/ibmmq/rest/v1/admin/qmgr/QM1/queue -X DELETE
-H "ibm-mq-rest-csrf-token: value" -b c:\cookiejar.txt
-c c:\cookiejar.txt
```

관련 참조

[POST/login](#)

[GET/login](#)

[/login 삭제](#)

V 9.1.3 IFrame에 IBM MQ Console 임베드

HTML `<iframe>` 요소는 IFrame(Inline Frame)을 사용하여 한 웹 페이지를 다른 페이지에 임베드할 때 사용할 수 있습니다. 보안 상의 이유로 IBM MQ Console은 기본적으로 IFrame에 임베드할 수 없습니다. 그러나 `mqweb` 서버에서 `mqConsoleFrameAncestors` 구성 특성을 사용하면 IFrame을 사용으로 설정할 수 있습니다.

이 태스크 정보

`mqweb` 서버는 IFrame을 사용하여 IBM MQ Console 를 임베드할 수 있는 웹 페이지의 오리진 목록을 유지합니다. 원본은 URL 설계, 도메인 및 포트의 결합(예: `https://example.com:1234`)입니다.

`mqweb` 서버에서 `mqConsoleFrameAncestors` 구성 특성을 사용하여 목록에서 항목을 지정할 수 있습니다.

기본적으로 `mqConsoleFrameAncestors`는 공백이며, 이는 IBM MQ Console을 IFrame에 임베드할 수 없음을 의미합니다.

프로시저

다음 명령을 입력하여 IFrame에 IBM MQ Console을 임베드할 수 있는 웹 페이지의 원본 목록을 지정하십시오.

```
setmqweb properties -k mqConsoleFrameAncestors -v allowedOrigins
```

여기서 *allowedOrigins*은 쉼표로 구분되는 원본 목록입니다. 각 원본은 다음으로 구성되어야 합니다.

- 호스트 이름 또는 IP 주소
- 선택적 URL 설계
- 선택적 포트 번호

호스트 이름은 와일드카드 문자(*)로 시작할 수 있고 포트 번호에서도 와일드카드 문자(*)를 사용할 수 있습니다.

예제 원본은 다음과 같습니다.

```
https://example.com:1234
```

여기에서는 `https://example.com:1234`에서 제공되는 웹 페이지에서 IBM MQ Console을 IFrame에 임베드할 수 있습니다.

```
https://*.example.com:*
```

여기에서는 호스트 이름이 `example.com`으로 끝나고 포트를 사용하는 HTTPS 웹 페이지가 IFrame에 IBM MQ Console을 임베드할 수 있습니다.

예

다음 예제에서는 IBM MQ Console이 `https://site2.example.com:1234` 또는 `https://site2.example.com:1235`에서 제공되는 웹 페이지에서 IFrame에 임베드될 수 있습니다.

```
setmqweb properties -k mqConsoleFrameAncestors -v  
https://site2.example.com:1234,https://site2.example.com:1235
```

V 9.1.0 REST API에 대해 CORS 구성

기본적으로 웹 브라우저는 스크립트(예: JavaScript)가 REST API와 동일한 원본에서 제공되지 않는 경우 스크립트가 REST API를 호출하도록 허용하지 않습니다. 즉, 원본 간 요청이 사용으로 설정되지 않습니다. 지정된 원본으로부터의 원본 간 요청을 허용하도록 CORS(Cross Origin Resource Sharing)를 구성할 수 있습니다.

이 태스크 정보

웹 브라우저를 통해(예: 스크립트를 통해) REST API에 액세스할 수 있습니다. 이 요청은 다른 원본으로부터 REST API에 제공되는 원본 간 요청이므로 웹 브라우저는 이 요청을 거부합니다. 도메인, 포트 또는 설계가 동일하지 않은 경우에는 원본이 다릅니다.

예를 들어, `http://localhost:1999/`에서 호스팅되는 스크립트가 있으면 `https://localhost:9443/`에서 호스팅되는 웹 사이트에서 HTTP GET을 발행하는 경우 원본 간 요청을 작성합니다. 포트 번호와 설계(HTTP)가 다르기 때문에 이 요청은 원본 간 요청입니다.

CORS를 구성하고 관리 REST API에 액세스하도록 허용되는 원본을 지정하여 원본 간 요청을 사용으로 설정할 수 있습니다.

CORS에 대한 자세한 정보는 <https://www.w3.org/TR/cors/> 및 <https://developer.mozilla.org/en-US/docs/Web/HTTP/CORS>의 내용을 참조하십시오.

프로시저

1. 다음 명령을 입력하여 현재 구성을 보십시오.


```
dspmweb properties -a
```

mqRestCorsAllowedOrigins 입력 항목은 허용되는 원본을 지정합니다.

mqRestCorsMaxAgeInSeconds 입력 항목은 웹 브라우저가 CORS 프리플라이트(pre-flight) 검사의 결과를 캐시할 수 있는 시간(초)을 지정합니다.

2. 다음 명령을 입력하여 REST API에 액세스할 수 있는 원본을 지정하십시오.

```
setmqweb properties -k mqRestCorsAllowedOrigins -v allowedOrigins
```

여기서 *allowedOrigins*는 원본 간 요청을 허용할 원본을 지정합니다. 별표를 큰따옴표로 묶어 모든 원본 간 요청을 허용할 수 있습니다. 둘 이상의 원본을 큰따옴표로 묶어 쉼표로 구분된 목록으로 입력할 수 있습니다. 원본 간 요청을 허용하지 않으려면 *allowedOrigins*의 값으로 비어 있는 따옴표를 입력하십시오.

3. 다음 명령을 입력하여 웹 브라우저에서 CORS 프리플라이트(pre-flight) 검사의 결과를 캐시에 저장할 수 있게 하려는 시간(초)을 지정하십시오.

```
setmqweb properties -k mqRestCorsMaxAgeInSeconds -v time
```

예

다음 예에서는 <http://localhost:9883>, <https://localhost:1999> 및 <https://localhost:9663>에 대해 사용으로 설정된 원본 간 요청을 보여줍니다. CORS 프리플라이트(pre-flight) 검사의 캐시에 저장된 결과의 최대 유효 기간은 90초로 설정됩니다.

```
setmqweb properties -k mqRestCorsAllowedOrigins -v "http://localhost:9883,https://localhost:1999,https://localhost:9663"
setmqweb properties -k mqRestCorsMaxAgeInSeconds -v 90
```



IBM MQ Console 및 REST API에 대한 호스트 헤더 유효성 검증 구성

지정된 허용 목록과 일치하는 호스트 헤더와 함께 송신되는 요청만 처리되도록 IBM MQ Console 및 REST API에 대한 액세스를 제한하도록 mqweb 서버를 구성할 수 있습니다. 허용 목록에 없는 호스트 헤더 값이 사용되는 경우 오류가 리턴됩니다.

이 태스크 정보

mqweb 서버는 허용되는 호스트 헤더의 허용 목록을 정의하는 데 가상 호스트를 사용합니다. 가상 호스트에 관한 자세한 정보는 WebSphere Liberty 문서(https://www.ibm.com/docs/SSEQTP_liberty/com.ibm.websphere.wlp.doc/ae/cwlp_virtual_hosts.html)를 참조하십시오.

이 태스크를 완료하려면 mqwebuser.xml 파일을 편집할 수 있는 충분한 권한이 있는 사용자여야 합니다.

-  z/OS에서는 mqwebuser.xml 파일에 대한 쓰기 액세스 권한이 있어야 합니다.
-  다른 모든 운영 체제에서는 [권한이 있는 사용자](#)여야 합니다.

프로시저

1. mqwebuser.xml 파일을 여십시오. 이 파일은 다음 위치 중 하나에 있습니다.

-  ULW

UNIX, Linux, and Windows: `MQ_DATA_PATH/web/installations/installationName/servers/mqweb`

-  z/OS

z/OS: `WLP_user_directory/servers/mqweb`

여기서 *WLP_user_directory*는 mqweb 서버 정의를 작성하기 위해 `crtmqweb` 스크립트를 실행할 때 지정된 디렉토리입니다.

2. mqwebuser.xml 파일에서 다음 코드를 추가하거나 주석 해제하십시오.

```
<virtualHost allowFromEndpointRef="defaultHttpEndpoint" id="default_host">
  <hostAlias>localhost:9080</hostAlias>
</virtualHost>
```

3. 허용하려는 호스트 이름 및 포트 조합을 삽입하여 **<hostAlias>** 필드를 편집하십시오.

이 조합은 mqweb 서버의 구성에서 사용한 호스트 이름 및 포트 조합일 수 있습니다. 예를 들어, localhost:9443의 기본 구성을 사용하는 경우 **<hostAlias>** 필드에서 localhost:9443을(를) 사용할 수 있습니다.

필요한 경우 **<virtualHost>** 태그에 여러 **<hostAlias>** 필드를 추가하여 더 많은 호스트 이름 및 포트 조합을 허용할 수 있습니다. 예를 들면, HTTPS 포트를 사용하는 호스트 헤더 외에 HTTP 포트를 사용하는 호스트 헤더 또한 허용하려 하는 경우가 있습니다.

V 9.1.0 감사

IBM MQ Console 및 REST API에서 수행되는 조작의 감사 레코드는 큐 관리자 명령 및 구성 이벤트를 사용하여 생성할 수 있으며, UNIX, Linux, and Windows에서 중요한 상태 변경이 발생하면 mqweb 서버의 로그 파일에 기록됩니다.

중요한 상태 변경

ULW

UNIX, Linux, and Windows에서 IBM MQ Console은 중요한 상태 변경을 기록합니다. 각 메시지는 조작을 요청한 인증된 프린시펄 이름을 나타냅니다.

큐 관리자 작성, 시작, 종료 및 삭제 같은 중요한 상태 변경은 mqweb 서버 messages.log 및 console.log 파일에 로깅됩니다. 각 메시지는 조작을 요청한 인증된 프린시펄 이름을 나타냅니다.

messages.log 및 console.log 파일은 다음 위치에 있습니다.

- ULW UNIX, Linux, and Windows:
 MQ_DATA_PATH\web\installations*installationName*\servers\mqweb\logs

mqweb 서버 로깅 레벨 구성에 대한 자세한 정보는 [로깅 구성](#)을 참조하십시오.

명령 및 구성 이벤트

선택적으로 큐 관리자에서 명령 및 구성 이벤트를 활성화하여 대부분의 IBM MQ Console 및 REST API 활동에 대한 정보를 제공할 수 있습니다. 예를 들어, 채널 작성 및 큐 조치는 명령 및 구성 이벤트를 생성합니다. 명령 및 구성 이벤트 활성화에 대한 자세한 정보는 [구성, 명령 및 로거 이벤트 제어](#)를 참조하십시오.

이 명령 및 구성 이벤트 메시지의 경우 MQIACF_EVENT_ORIGIN 필드가 MQEVO_REST로 설정되어 있습니다. 사용자에게 MQWebAdmin 또는 MQWebAdminRO 역할이 있는 경우, MQCACF_EVENT_USER_ID 필드는 명령을 실행한 프린시펄의 사용자 이름이 아닌 mqweb 서버 사용자 ID를 보고합니다. 그러나 사용자에게 MQWebUser 역할이 있는 경우에는 MQCACF_EVENT_USER_ID가 명령을 실행한 프린시펄의 사용자 이름을 보고합니다.

관련 개념

[410 페이지의 『감사』](#)

이벤트 메시지를 사용하여 보안 침입 또는 침입 시도를 확인할 수 있습니다. IBM MQ Explorer를 사용하여 시스템의 보안을 확인할 수도 있습니다.

Security considerations for the IBM MQ Console and REST API on z/OS

IBM MQ Console 및 REST API에는 사용자가 명령을 실행하거나 표시하거나 변경할 수 있는지를 제어하는 보안 기능이 있습니다. 그런 다음 명령이 큐 관리자에게 전달되고 큐 관리자 보안을 사용하여 사용자가 해당 특정 큐 관리자에 대해 명령을 실행할 수 있는지를 제어합니다.

프로시저

1. mqweb 서버의 시작된 태스크 사용자 ID에 특정 PCF 명령을 실행하고 특정 큐에 액세스하는 권한이 있는지 확인하십시오. 자세한 정보는 [462 페이지의 『mqweb 서버의 시작된 태스크 사용자 ID에 필요한 권한』](#)의 내용을 참조하십시오.

2. MQWebUser 역할이 부여된 사용자에게 적절한 권한이 있는지 확인하십시오.

MQWebUser 역할에 지정된 IBM MQ Console 및 REST API 사용자는 프린시펄의 보안 컨텍스트에서 작동합니다. 이 사용자 ID는 큐 관리자에 대해 사용자 ID에 수행 권한이 부여된 조작만 수행할 수 있으며 mqweb 서버 주소 공간과 동일한 시스템 큐에 대한 권한이 부여되어야 합니다.

mqweb 서버의 시작된 태스크 사용자 ID에는 MQWebUser 역할에 지정된 모든 사용자에게 대한 대체 사용자 액세스 권한이 부여되어야 합니다.

MQWebUser 역할을 가진 사용자에게 적절한 권한을 부여하는 방법에 대한 자세한 정보는 [463 페이지의 『MQ Console 또는 REST API 를 사용하는 데 필요한 IBM MQ 자원에 대한 액세스』](#)의 내용을 참조하십시오.

3. 옵션: IBM MQ Console 및 REST API에 대한 TLS를 구성하십시오. 추가 정보는 [464 페이지의 『Configuring TLS for the REST API and IBM MQ Console on z/OS』](#)의 내용을 참조하십시오.

z/OS mqweb 서버의 시작된 태스크 사용자 ID에 필요한 권한

z/OS에서 mqweb 서버의 시작된 태스크 사용자 ID에는 PCF 명령을 실행하고 시스템 자원에 액세스하는 특정 권한이 필요합니다.

mqweb 서버의 시작된 태스크 사용자 ID에 다음이 필요합니다.

- z/OS UNIX System Services를 사용할 수 있는 z/OS UNIX 사용자 ID(UID).
- IBM MQ 설치의 h1q.SCSQAUTH 및 h1q.SCSQANL* 데이터 세트에 대한 액세스 권한.
- z/OS UNIX System Services의 IBM MQ 설치 파일에 대한 읽기 액세스.
- **crtmqweb** 스크립트로 작성된 Liberty 사용자 디렉토리에 대한 읽기 및 쓰기 액세스
- 큐 관리자에 연결할 수 있는 권한. mqweb 서버의 시작된 태스크 사용자 ID에 MQCONN 클래스의 h1q.BATCH 프로파일에 대한 **READ** 액세스 권한을 부여하십시오.
- IBM MQ 명령을 실행하고 특정 큐에 액세스하는 권한. 이러한 세부사항은 [205 페이지의 『IBM MQ Console - 필수 명령 보안 프로파일』](#), [184 페이지의 『시스템 큐 보안』](#) 및 [194 페이지의 『컨텍스트 보안을 위한 프로파일』](#)에 설명되어 있습니다.
- MFT에 REST API 를 사용하기 위해 SYSTEM.FTE 주제에 등록할 권한. mqweb 서버의 시작된 태스크 사용자 ID에 MXTOPIC 클래스의 h1q.SUBSCRIBE.SYSTEM.FTE 프로파일에 대한 **ALTER** 액세스 권한을 부여하십시오.
- SAF 레지스트리를 구성하는 경우 다양한 보안 프로파일에 액세스하십시오. 자세한 정보는 [448 페이지의 『IBM MQ Console 및 REST API에 대한 SAF 레지스트리 구성』](#)의 내용을 참조하십시오.

연결 인증

모든 배치 애플리케이션이 올바른 사용자 ID 및 비밀번호를 제공하도록 큐 관리자가 구성된 경우 CHKLOCL(REQUIRED)을 설정하여 mqweb 서버의 시작된 태스크 사용자 ID에 MQCONN 클래스의 h1q.BATCH 프로파일에 대한 **UPDATE** 액세스 권한을 부여해야 합니다.

이 권한으로 인해 연결 인증이 mqweb 서버의 시작된 태스크 사용자 ID에 대해 CHKLOCL(OPTIONAL) 모드로 작동합니다.

모든 배치 애플리케이션이 올바른 사용자 ID 및 비밀번호를 제공하도록 큐 관리자를 구성하지 경우에는 mqweb 서버 태스크를 시작하는 사용자 ID에 MQCONN 클래스의 h1q.BATCH 프로파일에 대한 **READ** 액세스 권한을 부여하는 것으로 충분합니다.

옵션에 대한 자세한 정보는 [176 페이지의 『로컬에서 바인딩된 애플리케이션 CHKLOCL 사용』](#)의 내용을 참조하십시오.

MQ Console 또는 REST API 를 사용하는 데 필요한 IBM MQ 자원에 대한 액세스

Operations performed in the MQ Console, or REST API, by a user in the MQWebUser role take place under the security context of the user.

이 태스크 정보

MQ Console 및 REST API의 역할에 대한 자세한 정보는 [451 페이지의 『IBM MQ Console 및 REST API의 역할』](#) 를 참조하십시오.

다음 프로시저를 사용하여 MQWebUser 역할의 사용자에게 MQ Console 또는 REST API를 사용하는 데 필요한 큐 관리자 자원에 대한 액세스 권한을 부여하십시오.

프로시저

1. mqweb server started task 사용자 ID에 MQWebUser 역할의 각 사용자 ID에 대한 대체 사용자 액세스 권한을 부여하십시오.

관리자가 MQ Console 또는 REST API를 통해 관리할 모든 큐 관리자에서 이를 수행하십시오.

You can use the following sample RACF commands to grant the mqweb server started task user ID alternate user access to a user in the MQWebUser role:

```
RDEFINE MQADMIN hlq.ALTERNATE.USER.userId UACC(NONE)
PERMIT hlq.ALTERNATE.USER.userId CLASS(MQADMIN) ACCESS(UPDATE) ID(mqwebUserId)
SETROPTS RACLIST(MQADMIN) REFRESH
```

설명:

hlq

프로파일 접두부이며 큐 관리자 이름 또는 큐 공유 그룹 이름이 될 수 있습니다.

userId

MQWebUser 역할의 사용자입니다.

mqwebUserId

mqweb server started task 사용자 ID입니다.

참고: 대소문자 혼용 보안을 사용하는 경우, MQADMIN 클래스가 아닌 MXADMIN 클래스를 사용하십시오.

2. MQWebUser 역할의 각 사용자에게 MQ Console 및 REST API 사용에 필요한 시스템 큐에 대한 액세스 권한을 부여하십시오.

이를 수행하려면 SYSTEM.ADMIN.COMMAND.QUEUE 및 SYSTEM.REST.REPLY.QUEUE 둘 다에 대해, 각 사용자에게 대소문자 혼용 보안을 사용 중인지 여부에 따라 MQQUEUE 또는 MXQUEUE 클래스에 대한 UPDATE 액세스 권한을 제공하십시오.

[administrative REST API 게이트웨이](#)를 통해 관리되는 리모트 큐 관리자를 포함하여 사용자가 REST API를 통해 관리하는 모든 큐 관리자에서 이를 수행해야 합니다.

3. MQWebUser 역할의 사용자가 리모트 큐 관리자를 관리할 수 있게 하려면 리모트 큐 관리자에게 명령을 전송하는 데 사용하는 전송 큐를 보호하여 MQQUEUE 또는 MXQUEUE 클래스의 프로파일에 대한 UPDATE 액세스 권한을 사용자에게 부여하십시오. 참고로 사용자에게 게이트웨이 큐 관리자에서 UPDATE 액세스 권한을 부여해야 합니다.

리모트 큐 관리자에서는 게이트웨이 큐 관리자로부터 명령 응답 메시지를 다시 전송하는 데 사용한 전송 큐에 넣을 수 있는 액세스 권한을 동일한 사용자에게 부여하십시오.

4. Grant the users in the MQWebUser role access to any other resources required to perform the operations supported by the MQ Console and REST API.

액세스 권한은 다음을 수행해야 합니다.

- REST API에서 조작을 수행하려면 개별 [REST API 자원](#)의 보안 요구사항 섹션에 설명되어 있습니다.
- MQ Console로 명령 실행. [205 페이지의 『IBM MQ Console - 필수 명령 보안 프로파일』](#)에 설명되어 있습니다.

z/OS에서 RACF 키 링을 사용하여 클라이언트 인증서 인증 및 TLS를 사용한 보안 연결에 대한 인증서를 저장하도록 mqweb 서버를 구성할 수 있습니다.

시작하기 전에

이 프로시저를 완료하려면 mqwebuser.xml 파일에 대한 쓰기 액세스 권한과 SAF 키 링에 대한 작업을 수행할 권한이 있는 사용자여야 합니다.

이 태스크 정보

기본 mqweb 서버 구성은 신뢰할 수 있는 인증서 및 서버의 Java 키 저장소를 사용합니다. z/OS에서는 Java 키 스토어 대신 RACF 키 링을 사용하도록 mqweb 서버를 구성할 수 있습니다. 또한 서버는 사용자가 클라이언트 인증서를 사용하여 인증할 수 있도록 구성할 수 있습니다.

Liberty에서 RACF 키 링 사용에 대한 정보는 [Liberty: Keystores](#) 를 참조하십시오.

이 프로시저에 따라 RACF 키 링을 사용하도록 mqweb 서버를 구성하고 선택적으로 클라이언트 인증서 인증을 구성하십시오.

프로시저

1. 인증 기관(CA) 인증서를 작성하십시오. 이 인증서는 서버 인증서에 서명하는 데 사용됩니다. 예를 들어, 다음 RACF 명령을 입력하십시오.

```
RACDCERT GENCERT
CERTAUTH
SUBJECTSDN(CN('mqweb Certification Authority')
O('IBM')
OU('MQ'))
SIZE(2048)
WITHLABEL('mqwebCertauth')
```

2. 다음 명령을 입력하여 1단계에서 작성된 CA 인증서로 서명되는 서버 인증서를 작성하십시오.

```
RACDCERT ID(mqwebUserId) GENCERT
SUBJECTSDN(CN('hostname')
O('IBM')
OU('MQ'))
SIZE(2048)
SIGNWITH (CERTAUTH LABEL('mqwebCertauth'))
WITHLABEL('mqwebServerCert')
```

여기서 *mqwebUserId*는 mqweb 서버의 시작된 태스크 사용자 ID이며 *hostname*은 mqweb 서버의 호스트 이름입니다.

3. 다음 명령을 입력하여 CA 인증서 및 서버 인증서를 SAF 키 링에 연결하십시오.

```
RACDCERT ID(mqwebUserId) CONNECT(RING(keyring) LABEL('mqwebCertauth') CERTAUTH)
RACDCERT ID(mqwebUserId) CONNECT(RING(keyring) LABEL('mqwebServerCert'))
```

여기서 *mqwebUserId*는 mqweb 서버의 시작된 태스크 사용자 ID이며 *keyring*은 사용할 키 링의 이름입니다.

4. 다음 명령을 입력하여 CA 인증서를 CER 파일로 내보내십시오.

```
RACDCERT CERTAUTH EXPORT(LABEL('mqwebCertauth'))
DSN('h1q.CERT.MQWEBCA')
FORMAT(CERTDER)
PASSWORD('password')
```

5. 내보낸 CA 인증서를 2진으로 워크스테이션에 FTA를 통해 송신하고 인증 기관 인증서로서 브라우저에 가져 오십시오.
6. 옵션: 클라이언트 인증서 인증을 구성하려면 클라이언트 인증서를 작성하고 내보내십시오.

- a) 인증 기관(CA) 인증서를 작성하십시오. 이 인증서는 클라이언트 인증서에 서명하는 데 사용됩니다. 예를 들어, 다음 RACF 명령을 입력하십시오.

```
RACDCERT GENCERT
CERTAUTH
SUBJECTSDN(CN('mqweb User CA')
O('IBM')
OU('MQ'))
SIZE(2048)
WITHLABEL('mqwebUserCertauth')
```

- b) 다음 명령을 입력하여 CA 인증서를 SAF 키 링에 연결하십시오.

```
RACDCERT ID(mqwebUserId) CONNECT(RING(keyring) LABEL('mqwebUserCertauth') CERTAUTH)
```

여기서 *mqwebUserId*는 mqweb 서버의 시작된 태스크 사용자 ID이며 *keyring*은 사용할 키 링의 이름입니다.

- c) CA 인증서로 서명된 클라이언트 인증서를 작성하십시오. 예를 들어, 다음 명령을 입력하십시오.

```
RACDCERT ID(clientUserId) GENCERT
SUBJECTSDN(CN('clientUserId')
O('IBM')
OU('MQ'))
SIZE(2048)
SIGNWITH (CERTAUTH LABEL('mqwebUserCertauth'))
WITHLABEL('userCertLabel')
```

여기서 *clientUserId*는 사용자 이름입니다.

프린시펄에 인증서를 맵핑하는 데 사용되는 방법은 구성된 사용자 레지스트리의 유형에 따라 다릅니다.

- 기본 레지스트리를 사용하는 경우 인증서의 공통 이름 필드가 레지스트리의 사용자에 대해 일치합니다.
- SAF 레지스트리를 사용하고 있고 인증서가 RACF 데이터베이스에 있으면 인증서 작성 시 **ID** 매개 변수로 지정된 인증서 소유자가 사용됩니다.
- LDAP 레지스트리를 사용하는 경우 인증서의 전체 식별 이름이 LDAP 레지스트리에 대해 일치합니다.

- d) 다음 명령을 사용하여 클라이언트 인증서를 PKCS #12 파일로 내보내십시오.

```
RACDCERT ID(mqwebUserId) EXPORT(LABEL('userCertLabel')) PASSWORD('password')
DSN('hlq.USER.CERT')
```

- e) 내보낸 인증서를 2진으로 워크스테이션에 FTA를 통해 송신하십시오. IBM MQ Console에 클라이언트 인증서를 사용하려면 개인 인증서로서 IBM MQ Console에 액세스하는 데 사용되는 웹 브라우저로 가져오십시오.

7. *WLP_user_directory/servers/mqweb/mqwebuser.xml* 파일을 편집하십시오. 여기서 *WLP_user_directory*는 mqweb 서버 정의를 작성하기 위해 **crtmqweb** 스크립트를 실행할 때 지정된 디렉토리입니다.

RACF 키 링을 사용하도록 mqweb 서버를 구성하려면 다음과 같이 변경하십시오.

- a) 다음 행을 제거하거나 주석 처리하십시오.

```
<sslDefault sslRef="mqDefaultSSLConfig"/>
```

- b) 다음 명령문을 추가하십시오.

```
<keyStore id="defaultKeyStore" filebased="false" location="safkeyring://mqwebUserId/
keyring"
password="password" readOnly="true" type="JCERACFKS" />
<ssl id="thisSSLConfig" keyStoreRef="defaultKeyStore" sslProtocol="TLSv1.2"
serverKeyAlias="mqwebServerCert" clientAuthenticationSupported="true" />
<sslDefault sslRef="thisSSLConfig"/>
```

설명:

- `mqwebUserId`는 mqweb 서버의 시작된 태스크 사용자 ID입니다.
- `keyring`은 RACF 키 링의 이름입니다.
- `mqwebServerCert`는 mqweb 서버 인증서의 레이블입니다.

참고사항: `keyStore password` 값은 무시됩니다.

- mqweb 서버의 시작된 태스크를 중지하고 재시작하여 mqweb 서버를 재시작하십시오.
- 옵션: 클라이언트 인증서를 사용하여 인증하십시오.

- IBM MQ Console에 클라이언트 인증서를 사용하려면 클라이언트 인증서를 설치한 웹 브라우저에 MQ Console의 URL을 입력하십시오.
- REST API에 클라이언트 인증서를 사용하려면 각 REST 요청과 함께 클라이언트 인증서를 제공하십시오.

참고사항:

- 인증서만 사용하여 IBM MQ Console에 대해 인증하는 경우에는 선택할 인증서 목록이 브라우저에 표시됩니다.
- 다른 인증서를 사용하려면 브라우저를 닫은 후 재시작해야 합니다.
- RACF 데이터베이스에 없는 클라이언트 인증서를 사용하는 경우 RACF 인증서 이름 필터링을 사용하여 인증서 속성을 사용자 ID에 맵핑할 수 있습니다. 예를 들면, 다음과 같습니다.

```
RACDCERT ID(DEPT3USR) MAP SDNFILTER(OU=DEPT1.C=US)
```

OU=DEPT1 및 C=US가 포함된 주제 식별 이름이 있는 인증서를 사용자 ID DEPT3USR로 맵핑합니다.

결과

IBM MQ Console 및 REST API에 대해 TLS 인터페이스를 설정했습니다.

ULW UNIX, Linux, and Windows에서 키 및 인증서 관리

`runmqckm` 명령(UNIX 및 Windows)과 `runmqakm` 명령(UNIX, Linux, and Windows)을 사용하여 키, 인증서 및 인증서 요청을 관리합니다.

runmqckm 명령

`runmqckm` 명령은 UNIX 및 Windows에서 사용할 수 있습니다.

`runmqckm` 명령은 5 페이지의 『IBM MQ 보안 설정』에 설명된 iKeyman의 기능과 유사한 기능을 제공합니다.

`runmqckm` 명령을 사용하려면 `setmqenv` 명령을 실행하여 시스템 환경 변수가 올바르게 구성되었는지 확인하십시오.

V9.1.0 `runmqckm` 명령을 사용하려면 IBM MQ JRE 컴포넌트를 설치해야 합니다. 이 컴포넌트가 설치되지 않은 경우에는 `runmqackm` 명령을 대신 사용할 수 있습니다.

runmqakm 명령

`runmqakm` 명령은 UNIX, Linux, Windows에서 사용할 수 있습니다.

`runmqakm` 명령을 사용하려면 `setmqenv` 명령을 실행하여 시스템 환경 변수가 올바르게 구성되었는지 확인하십시오.

FIPS를 준수하는 방식으로 TLS 인증서를 관리해야 하는 경우 `runmqckm` 명령 대신 `runmqakm` 명령을 사용하십시오. 이는 `runmqackm` 명령이 보다 강력한 암호화를 지원하기 때문입니다.

`runmqckm` 및 `runmqakm` 명령을 사용하여 다음을 수행하십시오.

- IBM MQ에 필요한 CMS 키 데이터베이스 파일의 유형 작성
- 인증서 요청 작성
- 개인 인증서 가져오기
- CA 인증서 가져오기

- 자체 서명 인증서 관리

관련 정보

키 도구

ULW UNIX, Linux, and Windows 의 runmqckm 및 runmqakm 명령

이 절에서는 명령의 오브젝트에 따른 runmqckm 및 runmqakm 명령에 대해 설명합니다.

두 명령 간의 주요 차이점은 다음과 같습니다.

ULW runmqakm

- UNIX, Linux, Windows에서 사용 가능합니다.
- Elliptic Curve 공용 키를 사용하는 인증서 요청 및 인증서의 작성을 지원하는 반면 **runmqckm** 명령은 이를 지원하지 않습니다.
- **-strong** 매개변수를 사용하는 **runmqckm** 명령보다 강력한 키 저장소 파일 암호화를 지원합니다.
- FIPS 140-2 준수로 인증되었으며 **runmqckm** 명령과 달리 **-fips** 매개변수를 사용하여 FIPS 준수 방식으로 작동하도록 구성될 수 있습니다.

Windows UNIX runmqckm

- UNIX 및 Windows에서 사용 가능합니다.
- JKS 및 JCEKS 키 저장소 파일 형식을 지원하며 반면 **runmqakm** 명령은 이를 지원하지 않습니다.



주의: **V9.1.0** **runmqckm** 명령을 사용하려면 IBM MQ Java runtime environment(JRE) 기능을 설치해야 합니다.

각각의 명령은 하나 이상의 오브젝트를 지정합니다. PKCS #11 디바이스 조작에 대한 명령은 추가 오브젝트를 지정합니다. 키 데이터베이스, 인증서 및 인증서 요청 오브젝트에 대한 명령은 조치도 지정합니다. 오브젝트는 다음 중 하나일 수 있습니다.

-keydb

조치가 키 데이터베이스에 적용됨

-cert

조치가 인증서에 적용됨

-certreq

조치가 인증서 요청에 적용됨

-help

도움말을 표시함

-버전

버전 정보를 표시함

다음 하위 주제에서는 키 데이터베이스, 인증서 및 인증서 요청 오브젝트에 대해 수행할 수 있는 조치에 대해 설명합니다. 이 명령의 옵션에 대한 설명은 476 페이지의 『UNIX, Linux, and Windows 의 runmqckm 및 runmqakm 옵션』의 내용을 참조하십시오.

ULW UNIX, Linux, and Windows 에서만 CMS키 데이터베이스에 대한 명령

runmqckm 및 **runmqakm** 명령을 사용하여 CMS 키 데이터베이스에 대한 키 및 인증서를 관리할 수 있습니다.

-keydb -changepw

CMS 키 데이터베이스의 비밀번호를 변경합니다.

```
-keydb -changepw -db filename -pw password -new_pw new_password
```

```
-stash
```

-keydb -create

CMS 키 데이터베이스를 작성합니다.

```
-keydb -create -db filename  
-pw password -type cms -expire days -stash
```

-keydb -stashpw

CMS 키 데이터베이스의 비밀번호를 파일에 숨깁니다.

```
-keydb -stashpw -db filename  
-pw password
```

-cert -getdefault

참고: 기본 인증서는 IBM MQ 8.0에서 지원되지 않습니다. 23 페이지의 『[디지털 인증서 레이블, 요구사항 이해](#)』에 설명된 대로 인증서 레이블 구성을 사용해야 합니다.

기본 개인 인증서를 가져옵니다.

```
-cert -getdefault -db filename  
-pw password
```

-cert -modify

인증서를 수정합니다.

참고: 현재 수정할 수 있는 유일한 필드는 인증서 신뢰 필드입니다.

```
-cert -modify -db filename  
-pw password -label label  
-trust enable|disable
```

-cert -setdefault

참고: 기본 인증서는 IBM MQ 8.0 이후에서 지원되지 않습니다. 23 페이지의 『[디지털 인증서 레이블, 요구사항 이해](#)』에 설명된 대로 인증서 레이블 구성을 사용해야 합니다.

기본 개인 인증서를 설정합니다.

```
-cert -setdefault -db filename  
-pw password -label label
```

ULW UNIX, Linux, and Windows 의 CMS 또는 PKCS #12 키 데이터베이스에 대한 명령

runmqckm 및 runmqakm 명령을 사용하여 CMS 키 데이터베이스 또는 PKCS #12 키 데이터베이스에 대한 키 및 인증서를 관리할 수 있습니다.

참고: IBM MQ는 SHA-3 또는 SHA-5 알고리즘을 지원하지 않습니다. 디지털 서명 알고리즘 이름 SHA384WithRSA 및 SHA512WithRSA를 사용할 수 있습니다. 두 알고리즘 모두 SHA-2 제품군의 구성원이기 때문에입니다.

디지털 서명 알고리즘 이름 SHA3WithRSA 및 SHA5WithRSA는 각각 SHA384WithRSA 및 SHA512WithRSA의 축약된 양식이므로 더 이상 사용되지 않습니다.

-keydb -changepw

키 데이터베이스의 비밀번호를 변경합니다.

```
-keydb -changepw -db filename -pw password -new_pw  
new_password -expire days
```

-keydb -convert

키 데이터베이스를 하나의 형식에서 다른 형식으로 변환합니다.

```
-keydb -convert -db filename -pw password  
-old_format cms | pkcs12 -new_format cms
```

-keydb -create

키 데이터베이스를 작성합니다.

```
-keydb -create -db filename -pw password -type cms  
| pkcs12
```

-keydb -delete

키 데이터베이스를 삭제합니다.

```
-keydb -delete -db filename -pw password
```

-keydb -list

현재 지원되는 키 데이터베이스 유형을 나열합니다.

```
-keydb -list
```

-cert -add

파일의 인증서를 키 데이터베이스에 추가합니다.

```
-cert -add -db filename -pw password -label label  
-file filename  
-format ascii | binary
```

-cert -create

자체 서명 인증서를 작성하십시오.

```
-cert -create -db filename -pw password -label label  
-dn distinguished_name  
-size 1024 | 512 -x509version 3 | 1  
| 2  
-expire days -sig_alg MD2_WITH_RSA | MD2WithRSA  
|  
MD5_WITH_RSA | MD5WithRSA  
|  
SHA1WithDSA | SHA1WithRSA  
|  
SHA256_WITH_RSA | SHA256WithRSA  
|  
SHA2WithRSA | SHA384_WITH_RSA  
|  
SHA384WithRSA | SHA512_WITH_RSA  
|  
SHA512WithRSA | SHA_WITH_DSA  
|  
SHA_WITH_RSA | SHAWithDSA  
|  
SHAWithRSA
```

-cert -delete

인증서를 삭제합니다.

```
-cert -delete -db filename -pw password -label label
```

-cert -details

특정 인증서에 대한 자세한 정보를 나열합니다.

```
-cert -details -db filename -pw password -label label
```

-cert -export

개인 인증서 및 해당 연관된 개인 키를 키 데이터베이스에서 PKCS #12 파일 또는 다른 키 데이터베이스로 내보냅니다.

```
-cert -export -db filename -pw password -label label  
-type cms | pkcs12  
-target filename -target_pw password -target_type  
cms | pkcs12
```

-cert -extract

키 데이터베이스에서 인증서를 추출합니다.

```
-cert -extract -db filename -pw password -label label  
-target filename  
-format ascii | binary
```

-cert -import

키 데이터베이스에서 개인 인증서를 가져옵니다.

```
-cert -import -file filename -pw password -type  
pkcs12 -target filename  
-target_pw password -target_type cms -label  
label
```

-label 옵션은 필수이며 소스 키 데이터베이스에서 가져올 인증서의 레이블을 지정합니다.

-new_label 옵션은 선택사항이며 가져온 인증서에 소스 데이터베이스의 레이블과 다른 레이블을 대상 키 데이터베이스에서 지정할 수 있게 합니다.

-cert -list

키 데이터베이스에 있는 모든 인증서를 나열합니다.

```
-cert -list all | personal | CA  
-db filename -pw password
```

-cert -receive

파일에서 인증서를 수신합니다.

```
-cert -receive -file filename -db filename -pw password  
-format ascii | binary -default_cert yes |  
no
```

-cert -sign

인증서에 서명합니다.

```
-cert -sign -db filename -file filename -pw password  
-label label -target filename  
-format ascii | binary -expire days  
-sig_alg MD2_WITH_RSA | MD2WithRSA | MD5_WITH_RSA  
|  
MD5WithRSA | SHA1WithDSA | SHA1WithRSA  
|  
SHA256_WITH_RSA | SHA256WithRSA |  
SHA2WithRSA | SHA384_WITH_RSA |  
SHA384WithRSA | SHA512_WITH_RSA |  
SHA512WithRSA | SHA_WITH_DSA |  
SHA_WITH_RSA | SHAWithDSA |  
SHAWithRSA
```

-certreq -create

인증서 요청을 작성합니다.

```
-certreq -create -db filename -pw password
-label label -dn distinguished_name
-size 1024 | 512 -file filename
-sig_alg MD2_WITH_RSA | MD2WithRSA |
MD5_WITH_RSA | MD5WithRSA |
SHA1WithDSA | SHA1WithRSA |
SHA256_WITH_RSA | SHA256WithRSA |
SHA2WithRSA | SHA384_WITH_RSA |
SHA384WithRSA | SHA512_WITH_RSA |
SHA512WithRSA | SHA_WITH_DSA |
SHA_WITH_RSA | SHAWithDSA |
SHAWithRSA
```

-certreq -delete

인증서 요청을 삭제합니다.

```
-certreq -delete -db filename -pw password -label
label
```

-certreq -details

특정 인증서 요청에 대한 자세한 정보를 나열합니다.

```
-certreq -details -db filename -pw password -label
label
```

인증서 요청에 대한 자세한 정보를 나열하고 전체 인증서 요청을 표시합니다.

```
-certreq -details -showOID -db filename
-pw password -label label
```

-certreq -extract

인증서 요청 데이터베이스의 인증서 요청을 파일에 추출합니다.

```
-certreq -extract -db filename -pw password
-label label -target filename
```

-certreq -list

인증서 요청 데이터베이스에 있는 모든 인증서 요청을 나열합니다.

```
-certreq -list -db filename -pw password
```

-certreq -recreate

인증서 요청을 재작성합니다.

```
-certreq -recreate -db filename -pw password
-label label -target filename
```



UNIX, Linux, and Windows 에서 암호화 디바이스 조작을 위한 명령

runmqckm 및 runmqakm 명령을 사용하여 암호화 디바이스 조작의 키와 인증서를 관리할 수 있습니다.

참고: IBM MQ는 SHA-3 또는 SHA-5 알고리즘을 지원하지 않습니다. 디지털 서명 알고리즘 이름 SHA384WithRSA 및 SHA512WithRSA를 사용할 수 있습니다. 두 알고리즘 모두 SHA-2 제품군의 구성원이기 때 문입니다.

디지털 서명 알고리즘 이름 SHA3WithRSA 및 SHA5WithRSA는 각각 SHA384WithRSA 및 SHA512WithRSA의 축약된 양식이므로 더 이상 사용되지 않습니다.

-keydb -changepw

암호화 디바이스의 비밀번호를 변경합니다.

```
-keydb -changepw -crypto module_name -tokenlabel token_label  
-pw password -new_pw new_password
```

PKCS #11 암호화 하드웨어에 저장된 인증서 또는 키를 사용 중인 경우 **runmqckm** 및 **strmqikm**은 64비트 프로그램입니다. PKCS #11 지원에 필요한 외부 모듈이 64비트 프로세스에 로드되므로 암호화 하드웨어 관리를 위해서는 64비트 PKCS #11 라이브러리를 설치해야 합니다. **strmqikm** 및 **runmqckm** 프로그램은 Windows 및 Linux x86 32비트 플랫폼에서 32비트이므로 이 플랫폼에서는 이 사항이 적용되지 않습니다.

-keydb -list

현재 지원되는 키 데이터베이스 유형을 나열합니다.

```
-keydb -list
```

PKCS #11 암호화 하드웨어에 저장된 인증서 또는 키를 사용 중인 경우 **runmqckm** 및 **strmqikm**은 64비트 프로그램입니다. PKCS #11 지원에 필요한 외부 모듈이 64비트 프로세스에 로드되므로 암호화 하드웨어 관리를 위해서는 64비트 PKCS #11 라이브러리를 설치해야 합니다. **strmqikm** 및 **runmqckm** 프로그램은 Windows 및 Linux x86 32비트 플랫폼에서 32비트이므로 이 플랫폼에서는 이 사항이 적용되지 않습니다.

-cert -add

파일의 인증서를 암호화 디바이스에 추가합니다.

```
-cert -add -crypto module_name -tokenlabel token_label  
-pw password -label label -file filename -format  
ascii | binary
```

PKCS #11 암호화 하드웨어에 저장된 인증서 또는 키를 사용 중인 경우 **runmqckm** 및 **strmqikm**은 64비트 프로그램입니다. PKCS #11 지원에 필요한 외부 모듈이 64비트 프로세스에 로드되므로 암호화 하드웨어 관리를 위해서는 64비트 PKCS #11 라이브러리를 설치해야 합니다. **strmqikm** 및 **runmqckm** 프로그램은 Windows 및 Linux x86 32비트 플랫폼에서 32비트이므로 이 플랫폼에서는 이 사항이 적용되지 않습니다.

-cert -create

암호화 디바이스에서 자체 서명 인증서를 작성합니다.

```
-cert -create -crypto module_name -tokenlabel token_label  
  
-pw password -label label -dn distinguished_name  
-size 1024 | 512  
-x509version 3 | 1 | 2 -default_cert no  
| yes -expire days  
-sig_alg MD2_WITH_RSA | MD2WithRSA |  
MD5_WITH_RSA | MD5WithRSA |  
SHA1WithDSA | SHA1WithRSA |  
SHA256_WITH_RSA | SHA256WithRSA |  
SHA2WithRSA | SHA384_WITH_RSA |  
SHA384WithRSA | SHA512_WITH_RSA |  
SHA512WithRSA | SHA_WITH_DSA |  
SHA_WITH_RSA | SHAWithDSA |  
SHAWithRSA
```

참고: 식별 이름에 여러 개의 OU(조직 단위) 속성이 포함된 인증서는 가져올 수 없습니다.

PKCS #11 암호화 하드웨어에 저장된 인증서 또는 키를 사용 중인 경우 **runmqckm** 및 **strmqikm**은 64비트 프로그램입니다. PKCS #11 지원에 필요한 외부 모듈이 64비트 프로세스에 로드되므로 암호화 하드웨어 관리를 위해서는 64비트 PKCS #11 라이브러리를 설치해야 합니다. **strmqikm** 및 **runmqckm** 프로그램은 Windows 및 Linux x86 32비트 플랫폼에서 32비트이므로 이 플랫폼에서는 이 사항이 적용되지 않습니다.

-cert -delete

암호화 디바이스에서 인증서를 삭제합니다.

```
-cert -delete -crypto module_name -tokenlabel token_label  
-pw password -label label
```

PKCS #11 암호화 하드웨어에 저장된 인증서 또는 키를 사용 중인 경우 **runmqckm** 및 **strmqikm**은 64비트 프로그램입니다. PKCS #11 지원에 필요한 외부 모듈이 64비트 프로세스에 로드되므로 암호화 하드웨어 관리를 위해서는 64비트 PKCS #11 라이브러리를 설치해야 합니다. **strmqikm** 및 **runmqckm** 프로그램은 Windows 및 Linux x86 32비트 플랫폼에서 32비트이므로 이 플랫폼에서는 이 사항이 적용되지 않습니다.

-cert -details

암호화 디바이스의 특정 인증서에 대한 자세한 정보를 나열합니다.

```
-cert -details -crypto module_name -tokenlabel token_label  
-pw password -label label
```

PKCS #11 암호화 하드웨어에 저장된 인증서 또는 키를 사용 중인 경우 **runmqckm** 및 **strmqikm**은 64비트 프로그램입니다. PKCS #11 지원에 필요한 외부 모듈이 64비트 프로세스에 로드되므로 암호화 하드웨어 관리를 위해서는 64비트 PKCS #11 라이브러리를 설치해야 합니다. **strmqikm** 및 **runmqckm** 프로그램은 Windows 및 Linux x86 32비트 플랫폼에서 32비트이므로 이 플랫폼에서는 이 사항이 적용되지 않습니다.

자세한 정보를 나열하고 암호화 디바이스의 특정 인증서에 대한 전체 인증서를 표시합니다.

```
-cert -details -showOID -crypto module_name -tokenlabel  
token_label  
-pw password -label label
```

PKCS #11 암호화 하드웨어에 저장된 인증서 또는 키를 사용 중인 경우 **runmqckm** 및 **strmqikm**은 64비트 프로그램입니다. PKCS #11 지원에 필요한 외부 모듈이 64비트 프로세스에 로드되므로 암호화 하드웨어 관리를 위해서는 64비트 PKCS #11 라이브러리를 설치해야 합니다. **strmqikm** 및 **runmqckm** 프로그램은 Windows 및 Linux x86 32비트 플랫폼에서 32비트이므로 이 플랫폼에서는 이 사항이 적용되지 않습니다.

-cert -extract

키 데이터베이스에서 인증서를 추출합니다.

```
-cert -extract -crypto module_name -tokenlabel token_label  
-pw password -label label -target filename  
-format ascii | binary
```

PKCS #11 암호화 하드웨어에 저장된 인증서 또는 키를 사용 중인 경우 **runmqckm** 및 **strmqikm**은 64비트 프로그램입니다. PKCS #11 지원에 필요한 외부 모듈이 64비트 프로세스에 로드되므로 암호화 하드웨어 관리를 위해서는 64비트 PKCS #11 라이브러리를 설치해야 합니다. **strmqikm** 및 **runmqckm** 프로그램은 Windows 및 Linux x86 32비트 플랫폼에서 32비트이므로 이 플랫폼에서는 이 사항이 적용되지 않습니다.

-cert -import

보조 키 데이터베이스 지원을 가진 암호화 디바이스로 인증서를 가져옵니다.

```
-cert -import -db filename -pw password -label label  
-type cms  
-crypto module_name -tokenlabel token_label -pw  
password  
-secondaryDB filename -secondaryDBpw password
```

PKCS #11 암호화 하드웨어에 저장된 인증서 또는 키를 사용 중인 경우 **runmqckm** 및 **strmqikm**은 64비트 프로그램입니다. PKCS #11 지원에 필요한 외부 모듈이 64비트 프로세스에 로드되므로 암호화 하드웨어 관리를 위해서는 64비트 PKCS #11 라이브러리를 설치해야 합니다. **strmqikm** 및 **runmqckm** 프로그램은 Windows 및 Linux x86 32비트 플랫폼에서 32비트이므로 이 플랫폼에서는 이 사항이 적용되지 않습니다.

```
-cert -import -db filename -pw password -label label  
-type cms  
-crypto module_name -tokenlabel token_label -pw
```

```
password
-secondaryDB filename -secondaryDBpw password -fips
```

보조 키 데이터베이스 지원을 가진 암호화 디바이스로 PKCS #12 인증서 가져오기:

```
-cert -import -file filename -pw password -type pkcs12
-crypto module_name -tokenlabel token_label -pw
password
-secondaryDB filename -secondaryDBpw password
```

PKCS #11 암호화 하드웨어에 저장된 인증서 또는 키를 사용 중인 경우 **runmqckm** 및 **strmqikm**은 64비트 프로그램입니다. PKCS #11 지원에 필요한 외부 모듈이 64비트 프로세스에 로드되므로 암호화 하드웨어 관리를 위해서는 64비트 PKCS #11 라이브러리를 설치해야 합니다. **strmqikm** 및 **runmqckm** 프로그램은 Windows 및 Linux x86 32비트 플랫폼에서 32비트이므로 이 플랫폼에서는 이 사항이 적용되지 않습니다.

```
-cert -import -file filename -pw password -type pkcs12
-crypto module_name -tokenlabel token_label -pw
password
-secondaryDB filename -secondaryDBpw password -fips
```

참고: 식별 이름에 여러 개의 OU(조직 단위) 속성이 포함된 인증서는 가져올 수 없습니다.

-cert -list

암호화 디바이스의 모든 인증서를 나열합니다.

```
-cert -list all | personal | CA
-crypto module_name -tokenlabel token_label -pw
password
```

PKCS #11 암호화 하드웨어에 저장된 인증서 또는 키를 사용 중인 경우 **runmqckm** 및 **strmqikm**은 64비트 프로그램입니다. PKCS #11 지원에 필요한 외부 모듈이 64비트 프로세스에 로드되므로 암호화 하드웨어 관리를 위해서는 64비트 PKCS #11 라이브러리를 설치해야 합니다. **strmqikm** 및 **runmqckm** 프로그램은 Windows 및 Linux x86 32비트 플랫폼에서 32비트이므로 이 플랫폼에서는 이 사항이 적용되지 않습니다.

-cert -receive

보조 키 데이터베이스 지원을 가진 암호화 디바이스로 파일의 인증서를 수신합니다.

```
-cert -receive -file filename -crypto module_name -tokenlabel
token_label
-pw password -default_cert yes | no
-secondaryDB filename -secondaryDBpw password -format
ascii | binary
```

PKCS #11 암호화 하드웨어에 저장된 인증서 또는 키를 사용 중인 경우 **runmqckm** 및 **strmqikm**은 64비트 프로그램입니다. PKCS #11 지원에 필요한 외부 모듈이 64비트 프로세스에 로드되므로 암호화 하드웨어 관리를 위해서는 64비트 PKCS #11 라이브러리를 설치해야 합니다. **strmqikm** 및 **runmqckm** 프로그램은 Windows 및 Linux x86 32비트 플랫폼에서 32비트이므로 이 플랫폼에서는 이 사항이 적용되지 않습니다.

runmqckm 명령 사용:

-certreq -create

암호화 디바이스에서 인증서 요청을 작성합니다.

```
-certreq -create -crypto module_name -tokenlabel token_label

-pw password -label label -dn distinguished_name
-size 1024 | 512 -file filename
-sig_alg MD2_WITH_RSA | MD2WithRSA | MD5_WITH_RSA
|
MD5WithRSA | SHA1WithDSA | SHA1WithRSA
|
SHA256_WITH_RSA | SHA256WithRSA
SHA2WithRSA | SHA384_WITH_RSA |
```

```
SHA384WithRSA | SHA512_WITH_RSA |  
SHA512WithRSA | SHA_WITH_DSA |  
SHA_WITH_RSA | SHAWithDSA |  
SHAWithRSA
```

참고: 식별 이름에 여러 개의 OU(조직 단위) 속성이 포함된 인증서는 가져올 수 없습니다.

PKCS #11 암호화 하드웨어에 저장된 인증서 또는 키를 사용 중인 경우 **runmqckm** 및 **strmqikm**은 64비트 프로그램입니다. PKCS #11 지원에 필요한 외부 모듈이 64비트 프로세스에 로드되므로 암호화 하드웨어 관리를 위해서는 64비트 PKCS #11 라이브러리를 설치해야 합니다. **strmqikm** 및 **runmqckm** 프로그램은 Windows 및 Linux x86 32비트 플랫폼에서 32비트이므로 이 플랫폼에서는 이 사항이 적용되지 않습니다.

-certreq -delete

암호화 디바이스에서 인증서 요청을 삭제합니다.

```
-certreq -delete -crypto module_name -tokenlabel token_label  
-pw password -label label
```

PKCS #11 암호화 하드웨어에 저장된 인증서 또는 키를 사용 중인 경우 **runmqckm** 및 **strmqikm**은 64비트 프로그램입니다. PKCS #11 지원에 필요한 외부 모듈이 64비트 프로세스에 로드되므로 암호화 하드웨어 관리를 위해서는 64비트 PKCS #11 라이브러리를 설치해야 합니다. **strmqikm** 및 **runmqckm** 프로그램은 Windows 및 Linux x86 32비트 플랫폼에서 32비트이므로 이 플랫폼에서는 이 사항이 적용되지 않습니다.

-certreq -details

암호화 디바이스의 특정 인증서 요청에 대한 자세한 정보를 나열합니다.

```
-certreq -details -crypto module_name -tokenlabel token_label  
-pw password -label label
```

PKCS #11 암호화 하드웨어에 저장된 인증서 또는 키를 사용 중인 경우 **runmqckm** 및 **strmqikm**은 64비트 프로그램입니다. PKCS #11 지원에 필요한 외부 모듈이 64비트 프로세스에 로드되므로 암호화 하드웨어 관리를 위해서는 64비트 PKCS #11 라이브러리를 설치해야 합니다. **strmqikm** 및 **runmqckm** 프로그램은 Windows 및 Linux x86 32비트 플랫폼에서 32비트이므로 이 플랫폼에서는 이 사항이 적용되지 않습니다.

인증서 요청에 대한 자세한 정보를 나열하고 암호화 디바이스의 전체 인증서 요청을 표시합니다.

```
-certreq -details -showOID -crypto module_name -tokenlabel  
token_label  
-pw password -label label
```

PKCS #11 암호화 하드웨어에 저장된 인증서 또는 키를 사용 중인 경우 **runmqckm** 및 **strmqikm**은 64비트 프로그램입니다. PKCS #11 지원에 필요한 외부 모듈이 64비트 프로세스에 로드되므로 암호화 하드웨어 관리를 위해서는 64비트 PKCS #11 라이브러리를 설치해야 합니다. **strmqikm** 및 **runmqckm** 프로그램은 Windows 및 Linux x86 32비트 플랫폼에서 32비트이므로 이 플랫폼에서는 이 사항이 적용되지 않습니다.

-certreq -extract

암호화 디바이스의 인증서 요청 데이터베이스의 인증서 요청을 파일에 추출합니다.

```
-certreq -extract -crypto module_name -tokenlabel token_label  
-pw password -label label -target filename
```

PKCS #11 암호화 하드웨어에 저장된 인증서 또는 키를 사용 중인 경우 **runmqckm** 및 **strmqikm**은 64비트 프로그램입니다. PKCS #11 지원에 필요한 외부 모듈이 64비트 프로세스에 로드되므로 암호화 하드웨어 관리를 위해서는 64비트 PKCS #11 라이브러리를 설치해야 합니다. **strmqikm** 및 **runmqckm** 프로그램은 Windows 및 Linux x86 32비트 플랫폼에서 32비트이므로 이 플랫폼에서는 이 사항이 적용되지 않습니다.

-certreq -list

암호화 디바이스의 인증서 요청 데이터베이스에 있는 모든 인증서 요청을 나열합니다.

```
-certreq -list -crypto module_name -tokenlabel token_label
-pw password
```

PKCS #11 암호화 하드웨어에 저장된 인증서 또는 키를 사용 중인 경우 **runmqckm** 및 **strmqikm**은 64비트 프로그램입니다. PKCS #11 지원에 필요한 외부 모듈이 64비트 프로세스에 로드되므로 암호화 하드웨어 관리를 위해서는 64비트 PKCS #11 라이브러리를 설치해야 합니다. **strmqikm** 및 **runmqckm** 프로그램은 Windows 및 Linux x86 32비트 플랫폼에서 32비트이므로 이 플랫폼에서는 이 사항이 적용되지 않습니다.

ULW UNIX, Linux, and Windows 의 runmqckm 및 runmqakm 옵션

runmqckm(iKeycmd) 및 **runmqakm** 명령행 옵션을 사용하여 키, 인증서, 인증서 요청을 관리할 수 있습니다.

ULW **runmqakm** 명령은 UNIX, Linux, and Windows에서 사용할 수 있습니다.

Windows **UNIX** **runmqckm** 명령은 UNIX 및 Windows에서 사용할 수 있습니다.

참고: IBM MQ는 SHA-3 또는 SHA-5 알고리즘을 지원하지 않습니다. 디지털 서명 알고리즘 이름 SHA384WithRSA 및 SHA512WithRSA를 사용할 수 있습니다. 두 알고리즘 모두 SHA-2 제품군의 구성원이기 때 문입니다.

디지털 서명 알고리즘 이름 SHA3WithRSA 및 SHA5WithRSA는 각각 SHA384WithRSA 및 SHA512WithRSA의 축약된 양식이므로 더 이상 사용되지 않습니다.

옵션의 의미는 명령에서 지정된 오브젝트 및 조치에 따라 다를 수 있습니다.

표 90. runmqckm 및 runmqakm 과 함께 사용할 수 있는 옵션	
매개변수	설명
-create	키 데이터베이스를 작성하는 옵션입니다.
-crypto	PKCS #11 암호화 디바이스를 관리할 모듈 수입니다. 특성 파일에서 모듈 이름을 지정하는 경우 -crypto 뒤의 값은 선택사항입니다. PKCS #11 암호화 하드웨어에 저장된 인증서 또는 키를 사용하는 경우, runmqckm 및 strmqikm 는 IBM MQ 설치와 함께 제공되는 JVM (Java Virtual Machine) 을 사용하여 실행됩니다. PKCS #11 지원에 필요한 외부 모듈이 JVM 프로세스로 로드됩니다. 따라서 JVM의 비트 정보와 일치하는 암호화 하드웨어의 관리를 위해 PKCS #11 라이브러리를 설치해야 하며, runmqckm 또는 strmqikm 으로 이 라이브러리를 지정해야 합니다.
-db	키 데이터베이스의 완전한 경로 이름입니다.
-default_cert	인증서를 기본 인증서로 설정합니다. 값은 yes 또는 no일 수 있습니다. 기본값은 no입니다.
-dn	X.500 식별 이름입니다. 값은 큰따옴표로 묶인 문자열입니다 (예: "CN=John Smith,O=IBM,OU=Test,C=GB"). O 및 C 속성만 필수임을 유의하십시오. 공통 이름 (CN) 지정은 선택사항입니다.
-encryption	인증서 내보내기 명령에서 사용되는 암호화의 강도입니다. 값은 strong 또는 weak 일 수 있습니다. 기본값은 strong입니다.
-expire	인증서 또는 데이터베이스 비밀번호의 만기 시간(일)입니다. 인증서 비밀번호에 대한 기본값은 365일입니다. 데이터베이스 비밀번호에 대한 기본 시간은 없습니다. -expire 매개변수를 사용하여 데이터베이스 비밀번호 만기 시간을 명확하게 설정하십시오.
-file	인증서 또는 인증서 요청의 파일 이름입니다.

표 90. *runmqckm* 및 *runmqakm*과 함께 사용할 수 있는 옵션 (계속)

매개변수	설명
-fips	명령이 FIPS 모드에서 실행되도록 지정합니다. FIPS 모드에서 ICC 컴포넌트는 FIPS 140-2 유효성 검증된 알고리즘을 사용합니다. ICC 컴포넌트가 FIPS 모드에서 초기화되지 않는 경우에는 <i>runmqakm</i> 명령이 실패합니다.
-format	인증서의 형식입니다. 값은 <code>ascii</code> (Base64_encoded ASCII의 경우) 또는 <code>binary</code> (2진 DER 데이터의 경우)입니다. 기본값은 <code>ascii</code> 입니다.
-label	인증서 또는 인증서 요청에 첨부된 레이블입니다. 인증서가 IBM MQ 클라이언트 애플리케이션 또는 큐 관리자를 식별하는 데 사용되는 개인 인증서인 경우 레이블은 IBM MQ 인증서 레이블(CERTLABL) 설정에 해당해야 합니다. 자세한 정보는 23 페이지의 『디지털 인증서 레이블, 요구사항 이해』의 내용을 참조하십시오.
-new_format	키 데이터베이스의 새 형식입니다.
-new_label	인증서 가져오기 명령에 사용된 경우 이 옵션은 소스 키 데이터베이스에서의 레이블과 다른 레이블을 사용하여 인증서를 가져올 수 있게 합니다. 인증서가 IBM MQ 클라이언트 애플리케이션 또는 큐 관리자를 식별하는 데 사용되는 개인 인증서인 경우 레이블은 IBM MQ 인증서 레이블(CERTLABL) 설정에 해당해야 합니다. 자세한 정보는 23 페이지의 『디지털 인증서 레이블, 요구사항 이해』의 내용을 참조하십시오.
-new_pw	새 데이터베이스 비밀번호입니다.
-old_format	키 데이터베이스의 이전 형식입니다.
-pw	키 데이터베이스 또는 PKCS #12 파일의 비밀번호입니다.
-secondaryDB	PKCS #11 디바이스 조작에 대한 보조 키 데이터베이스의 이름입니다.
-secondaryDBpw	PKCS #11 디바이스 조작에 대한 보조 키 데이터베이스의 비밀번호입니다.
-showOID	전체 인증서 또는 인증서 요청을 표시합니다.
-sig_alg	<p>인증서 요청, 자체 서명 인증서 또는 인증서 서명 작성 중에 사용되는 해시 알고리즘입니다. 이 해시 알고리즘은 새로 작성된 인증서 또는 인증서 요청과 연관된 서명을 작성하는 데 사용됩니다.</p> <p><i>runmqckm</i>의 경우 값은 다음과 같을 수 있습니다. MD2_WITH_RSA, MD2WithRSA, MD5_WITH_RSA, MD5WithRSA, SHA1WithDSA, SHA1WithECDSA, SHA1WithRSA, SHA2/ECDSA, SHA224WithECDSA, SHA256_WITH_RSA, SHA256WithECDSA, SHA256WithRSA, SHA2WithECDSA, SHA3/ECDSA, SHA384_WITH_RSA, SHA384WithECDSA, SHA384WithRSA, SHA3WithECDSA, SHA5/ECDSA, SHA512_WITH_RSA, SHA512WithECDSA, SHA512WithRSA, SHA5WithECDSA, SHA_WITH_DSA, SHA_WITH_RSA, SHAWithDSA, SHAWithRSA. 기본값은 SHA1WithRSA입니다.</p> <p><i>runmqakm</i>의 경우 값은 md5, MD5_WITH_RSA, MD5WithRSA, SHA_WITH_DSA, SHA_WITH_RSA, sha1, SHA1WithDSA, SHA1WithECDSA, SHA1WithRSA, sha224, SHA224_WITH_RSA, SHA224WithDSA, SHA224WithECDSA, SHA224WithRSA, sha256, SHA256_WITH_RSA, SHA256WithDSA, SHA256WithECDSA, SHA256WithRSA, SHA2WithRSA, sha384, SHA384_WITH_RSA, SHA384WithECDSA, SHA384WithRSA, sha512, SHA512_WITH_RSA, SHA512WithECDSA, SHA512WithRSA, SHAWithDSA, SHAWithRSA, EC_ecdsa_with_SHA1, EC_ecdsa_with_SHA224, EC_ecdsa_with_SHA256, EC_ecdsa_with_SHA384 또는 EC_ecdsa_with_SHA512입니다. 기본값은 SHA1WithRSA입니다.</p>

표 90. *runmqckm* 및 *runmqakm*과 함께 사용할 수 있는 옵션 (계속)

매개변수	설명
-size	키 크기입니다. runmqckm 의 경우 값은 512, 1024 또는 2048입니다. 기본값은 1024비트입니다. runmqakm 의 경우 값은 서명 알고리즘에 따라 다릅니다. <ul style="list-style-type: none"> • RSA 서명 알고리즘(-sig_alg가 지정되지 않은 경우 기본 알고리즘이 사용됨)의 경우 값은 512, 1024, 2048 또는 4096입니다. -fips 매개변수가 사용으로 설정된 경우 RSA 키 크기 512비트는 허용되지 않습니다. 기본 RSA 키 크기는 1024비트입니다. • Elliptic Curve 알고리즘의 경우 값은 256, 384 또는 512입니다. 기본 Elliptic Curve 키 크기는 서명 알고리즘에 따라 다릅니다. SHA256의 경우 값은 256이고 SHA384의 경우 값은 384이고 SHA512의 경우 값은 512입니다.
-stash	키 데이터베이스 비밀번호를 파일에 숨깁니다. CMS 및 PKCS12 유형의 데이터베이스에만 적용 가능합니다. 참고: -stash 는 -keydb -create 명령에서 runmqckm/runmqakm 에 비밀번호를 포함하는 스택쉬 파일을 작성하도록 지시하는 데 유효합니다. \$ runmqakm -help 명령을 실행하면 상위 레벨 도움말 매개변수만 나열됩니다.
-stashed	키 데이터베이스 또는 PKCS #12 파일의 비밀번호가 스택쉬 파일에 있음을 표시합니다. 참고: -stashed 옵션은 -keydb -create 명령과는 별도로 호출에서 유효합니다. 이 옵션을 지정하지 않으면 -pw 를 사용하여 비밀번호를 제공해야 합니다. 또한 수행 중인 조치의 종류를 명령에 지시하는 경우에만 -stashed 를 표시하는 자세한 도움말이 표시됩니다.
-target	대상 파일 또는 데이터베이스입니다.
-target_pw	-target 이 키 데이터베이스를 지정하는 경우 키 데이터베이스의 비밀번호입니다.
-target_type	-target 피연산자에 의해 지정된 데이터베이스의 유형입니다. 허용되는 값은 -type 매개변수를 참조하십시오.
-tokenLabel	PKCS #11 암호화 디바이스의 레이블입니다.
-trust	CA 인증서의 신뢰 상태입니다. 값은 enable 또는 disable입니다. 기본값은 enable입니다.
-type	데이터베이스의 유형입니다. 가능한 값은 다음 값 중 하나입니다. <ul style="list-style-type: none"> • cms(CMS 키 데이터베이스의 경우) • pkcs12(PKCS #12 파일의 경우)
-x509version	작성할 X.509 인증서의 버전입니다. 값은 1, 2 또는 3일 수 있습니다. 기본값은 3입니다.

표 90. **runmqckm** 및 **runmqakm**과 함께 사용할 수 있는 옵션 (계속)

매개변수	설명
-rfc3339	<p>runmqakm -cert -details 명령에 대해 다음과 같은 RFC 3339 형식으로 날짜를 출력하려면 이 매개변수를 사용하십시오.</p> <pre>Not Before : 2015-08-26T08:53:37Z Not After : 2016-08-26T08:53:37Z</pre> <p>-rfc3339 매개변수는 명령에서 추가 매개변수 뒤에 표시되어야 합니다.</p> <pre>runmqakm -cert -details -db exampleDB -stashed -label certificatelabel -rfc3339</pre>

참고: **runmqckm** 유틸리티에서 대칭 키 암호화 **-seckey** 매개변수와 관련하여 IBM Global Security Kit (GSKit) 와 함께 제공되는 특성은 무시되며 IBM MQ에서 지원되지 않습니다.

ULW UNIX, Linux, and Windows 의 runmqakm 오류 코드

runmqakm에 의해 발행된 숫자 오류 코드 및 해당 의미에 대한 표입니다.

오류 코드	오류 메시지
0	성공
1	알 수 없는 오류 발생
2	ASN.1 인코딩/디코딩 오류가 발생했습니다.
3	ASN.1 인코더/디코더를 초기화하는 중에 오류가 발생했습니다.
4	범위를 벗어난 색인 또는 존재하지 않는 선택적 필드로 인해 ASN.1 인코딩/디코딩 오류가 발생했습니다.
5	데이터베이스 오류가 발생했습니다.
6	데이터베이스 파일을 여는 중에 오류가 발생했습니다. 파일 존재 여부 및 권한을 확인하십시오.
7	데이터베이스 파일을 다시 여는 중에 오류가 발생했습니다.
8	데이터베이스 작성에 실패했습니다.
9	데이터베이스가 이미 있습니다.
10	데이터베이스 파일을 삭제하는 중에 오류가 발생했습니다.
11	데이터베이스를 열 수 없습니다.
12	데이터베이스 파일을 읽는 중에 오류가 발생했습니다.
13	데이터베이스 파일에 데이터를 쓰는 중에 오류가 발생했습니다.
14	데이터베이스 유효성 검증 오류가 발생했습니다.
15	올바르지 않은 데이터베이스 버전이 발견되었습니다.
16	올바르지 않은 데이터베이스 비밀번호가 발견되었습니다.

오류 코드	오류 메시지
17	올바르지 않은 데이터베이스 파일 유형이 발견되었습니다.
18	지정된 데이터베이스가 손상되었습니다.
19	올바르지 않은 비밀번호가 제공되었거나 키 데이터베이스가 변조되거나 손상되었습니다.
20	데이터베이스 키 입력 항목 무결성 오류가 발생했습니다.
21	중복 인증서가 이미 데이터베이스에 있습니다.
22	중복 키가 이미 데이터베이스에 있습니다(레코드 ID).
23	동일한 레이블을 가진 인증서가 이미 키 데이터베이스에 있습니다.
24	중복 키가 이미 데이터베이스에 있습니다(서명).
25GB	중복 키가 이미 데이터베이스에 있습니다(서명되지 않은 인증서).
26	중복 키가 이미 데이터베이스에 있습니다(발행자 및 일련 번호).
27	중복 키가 이미 데이터베이스에 있습니다(주제 공개 키 정보).
20	중복 키가 이미 데이터베이스에 있습니다(서명되지 않은 CRL).
29	레이블이 데이터베이스에서 사용되었습니다.
30	비밀번호 암호화 오류가 발생했습니다.
31	LDAP 관련 오류가 발생했습니다. (LDAP은 이 프로그램에서 지원되지 않음)
32	암호화 오류가 발생했습니다.
33	암호화/복호화 오류가 발생했습니다.
34	올바르지 않은 암호화 알고리즘이 발견되었습니다.
35	데이터에 서명하는 중에 오류가 발생했습니다.
36	데이터를 확인하는 중에 오류가 발생했습니다.
37	데이터 요약을 처리하는 중에 오류가 발생했습니다.
38	올바르지 않은 암호화 매개변수가 발견되었습니다.
39	지원되지 않는 암호화 알고리즘이 발견되었습니다.
40	지정된 입력 크기가 지원되는 계수 크기보다 큼니다.
41	지원되지 않는 계수 크기가 발견되었습니다.
42	데이터베이스 유효성 검증 오류가 발생했습니다.
43	키 입력 항목 유효성 검증에 실패했습니다.
44	중복 확장 필드가 존재합니다.
45	키의 버전이 올바르지 않습니다.

오류 코드	오류 메시지
46	필수 확장 필드가 존재하지 않습니다.
47	검증 기간이 오늘을 포함하지 않거나 발행자의 검증 기간에 포함되지 않습니다.
48	검증 기간이 오늘을 포함하지 않거나 발행자의 검증 기간에 포함되지 않습니다.
49	개인 키 사용 확장을 유효성 검증하는 중에 오류가 발생했습니다.
50	키의 발행자를 찾을 수 없습니다.
51	필수 인증서 확장이 누락되었습니다.
52	올바르지 않은 기본 제한조건 확장이 발견되었습니다.
53	키 서명 유효성 검증에 실패했습니다.
54	키의 루트 키를 신뢰할 수 없습니다.
55	키가 취소되었습니다.
56	권한 키 ID 확장을 유효성 검증하는 중에 오류가 발생했습니다.
57	개인 키 사용 확장을 유효성 검증하는 중에 오류가 발생했습니다.
58	주제 대체 이름 확장을 유효성 검증하는 중에 오류가 발생했습니다.
59	발행자 대체 이름 확장을 유효성 검증하는 중에 오류가 발생했습니다.
60	키 사용 확장을 유효성 검증하는 중에 오류가 발생했습니다.
61	알 수 없는 중요한 확장이 발견되었습니다.
62	키 쌍 입력 항목을 유효성 검증하는 중에 오류가 발생했습니다.
63	CRL을 유효성 검증하는 중에 오류가 발생했습니다.
64	Mutex 오류가 발생했습니다.
65	올바르지 않은 매개변수가 발견되었습니다.
66	널 매개변수 또는 메모리 할당 오류가 발견되었습니다.
67	숫자 또는 크기가 너무 크거나 너무 작습니다.
68	이전 비밀번호가 올바르지 않습니다.
69	새 비밀번호가 올바르지 않습니다.
70	비밀번호가 만료되었습니다.
71	스레드 관련 오류가 발생했습니다.
72	스레드를 작성하는 중에 오류가 발생했습니다.
73	스레드가 종료를 대기하는 중에 오류가 발생했습니다.
74	I/O 오류가 발생했습니다.

오류 코드	오류 메시지
75	CMS를 로드하는 중에 오류가 발생했습니다.
76	암호화 하드웨어 관련 오류가 발생했습니다.
77	라이브러리 초기화 루틴이 성공적으로 호출되지 않았 습니다.
78	내부 데이터베이스 핸들 테이블이 손상되었습니다.
79	메모리 할당 오류가 발생했습니다.
80	인식되지 않는 옵션이 발견되었습니다.
81	시간 정보를 가져오는 중에 오류가 발생했습니다.
82	Mutex 작성 오류가 발생했습니다.
83	메시지 카탈로그를 여는 중에 오류가 발생했습니다.
84	오류 메시지 카탈로그를 여는 중에 오류가 발생했습니 다.
85	널 파일 이름이 발견되었습니다.
86	파일을 여는 중에 오류가 발생했습니다. 파일 존재 여 부 및 권한을 확인하십시오.
87	읽을 파일을 여는 중에 오류가 발생했습니다.
88	쓸 파일을 여는 중에 오류가 발생했습니다.
89	해당 파일이 없습니다.
90	권한 설정으로 인해 파일을 열 수 없습니다.
91	파일에 데이터를 쓰는 중에 오류가 발생했습니다.
92	파일을 삭제하는 중에 오류가 발생했습니다.
93	올바르지 않은 Base64 인코딩된 데이터가 발견되었습 니다.
94	올바르지 않은 Base64 메시지 유형이 발견되었습니 다.
95	Base64 인코딩 규칙을 사용하여 데이터를 인코딩하는 중에 오류가 발생했습니다.
96	Base64 인코딩된 데이터를 디코딩하는 중에 오류가 발생했습니다.
97	식별 이름 태그를 가져오는 중에 오류가 발생했습니다.
98	필수 공용 이름 필드가 비어 있습니다.
99	필수 국가 또는 지역 이름 필드가 비어 있습니다.
100	올바르지 않은 데이터베이스 핸들이 발견되었습니다.
101	키 데이터베이스가 없습니다.
102	요청 키 쌍 데이터베이스가 없습니다.
103	비밀번호 파일이 없습니다.
104	새 비밀번호가 이전 비밀번호와 동일합니다.
105	키 데이터베이스에 키가 없습니다.

오류 코드	오류 메시지
106	요청 키가 없습니다.
107	신뢰할 수 있는 CA가 없습니다.
108	인증서에 대한 요청 키가 없습니다.
109	키 데이터베이스에 개인 키가 없습니다.
110	키 데이터베이스에 기본 키가 없습니다.
111	키 레코드에 개인 키가 없습니다.
112	키 레코드에 인증서가 없습니다.
113	CRL 입력 항목이 없습니다.
114	올바르지 않은 키 데이터베이스 파일 이름이 발견되었습니다.
115	인식되지 않는 개인 키 유형이 발견되었습니다.
116	올바르지 않은 식별 이름 입력이 발견되었습니다.
117	지정된 키 레이블을 가진 키 입력 항목이 없습니다.
118	키 레이블 목록이 손상되었습니다.
119	입력 데이터가 올바른 PKCS12 데이터가 아닙니다.
120	비밀번호가 올바르지 않거나 PKCS12 데이터가 손상되었거나 PKCS12의 이후 버전을 사용하여 작성되었습니다.
121	인식되지 않는 키 내보내기 유형이 발견되었습니다.
122	지원되지 않는 비밀번호 기반 암호화 알고리즘이 발견되었습니다.
123	키 링 파일을 CMS 키 데이터베이스로 변환하는 중에 오류가 발생했습니다.
124	CMS 키 데이터베이스를 키 링 파일로 변환하는 중에 오류가 발생했습니다.
125	인증서 요청에 대한 인증서를 작성하는 중에 오류가 발생했습니다.
126	완전한 발행자 체인을 빌드할 수 없습니다.
127	올바르지 않은 WEBDB 데이터가 발견되었습니다.
128	키 링 파일에 기록할 데이터가 없습니다.
129	입력한 일 수가 허용된 검증 기간을 벗어났습니다.
130	비밀번호가 너무 짧습니다. 비밀번호는 {0}자 이상으로 구성되어야 합니다.
131	비밀번호는 하나 이상의 숫자를 포함해야 합니다.
132	비밀번호에 있는 모든 문자는 영문자 또는 숫자여야 합니다.
133	인식되지 않거나 지원되지 않는 서명 알고리즘이 지정되었습니다.
134	올바르지 않은 데이터베이스 유형이 발견되었습니다.

오류 코드	오류 메시지
135	지정된 보조 키 데이터베이스를 다른 PKCS#11 디바이스가 사용 중입니다.
136	보조 키 데이터베이스가 지정되지 않았습니다.
137	레이블이 PKCS#11 디바이스에 존재하지 않습니다.
138	PKCS#11 디바이스에 액세스하려면 비밀번호가 필요합니다.
139	PKCS#11 디바이스에 액세스하려면 비밀번호가 필요하지 않습니다.
140	암호화 라이브러리를 로드할 수 없습니다.
141	이 조작에 대해 PKCS#11이 지원되지 않습니다.
142	PKCS#11 디바이스에 대한 조작이 실패했습니다.
143	LDAP 사용자가 올바른 사용자가 아닙니다. (LDAP은 이 프로그램에서 지원되지 않음)
144	LDAP 사용자가 올바른 사용자가 아닙니다. (LDAP은 이 프로그램에서 지원되지 않음)
145	LDAP 조회에 실패했습니다. (LDAP은 이 프로그램에서 지원되지 않음)
146	올바르지 않은 인증서 체인이 발견되었습니다.
147	루트 인증서를 신뢰할 수 없습니다.
148	폐기된 인증서가 발견되었습니다.
149	암호화 오브젝트 기능이 실패했습니다.
150	사용 가능한 인증서 폐기 목록 데이터 소스가 없습니다.
151	사용 가능한 암호화 토큰이 없습니다.
152	FIPS 모드를 사용할 수 없습니다.
153	FIPS 모드 설정과 충돌이 발생했습니다.
154	입력한 비밀번호가 최소 필수 강도를 충족하지 않습니다.
200	프로그램을 초기화하는 중에 장애가 발생했습니다.
201	runmqakm 프로그램에 전달된 인수의 토큰화에 실패했습니다.
202	명령에서 식별된 오브젝트가 인식되는 오브젝트가 아닙니다.
203	전달된 조치가 알려진 -keydb 조치가 아닙니다.
204	전달된 조치가 알려진 -cert 조치가 아닙니다.
205	전달된 조치가 알려진 -certreq 조치가 아닙니다.
206	요청된 명령에 대한 태그가 누락되었습니다.
207	-version 태그와 함께 전달된 값이 인식되는 값이 아닙니다.

오류 코드	오류 메시지
208	-size 태그와 함께 전달된 값이 인식되는 값이 아닙니다.
209	-dn 태그와 함께 전달된 값이 올바른 형식으로 되어 있지 않습니다.
210	-format 태그와 함께 전달된 값이 인식되는 값이 아닙니다.
211	파일 열기와 연관된 오류가 발생했습니다.
212	이 단계에서는 PKCS12가 지원되지 않습니다.
213	비밀번호를 변경하려고 하는 암호화 토큰이 비밀번호로 보호되어 있지 않습니다.
214	이 단계에서는 PKCS12가 지원되지 않습니다.
215	입력한 비밀번호가 최소 필수 강도를 충족하지 않습니다.
216	FIPS 모드를 사용할 수 없습니다.
217	만기 날짜로 입력한 일 수가 허용된 범위를 벗어났습니다.
218	비밀번호 강도가 최소 요구사항을 충족하지 않습니다.
219	요청된 키 데이터베이스에 기본 인증서가 없습니다.
220	올바르지 않은 신뢰 상태가 발견되었습니다.
221	지원되지 않는 서명 알고리즘이 발견되었습니다. 이 단계에서는 MD5 및 SHA1만 지원됩니다.
222	해당 특정 조작에는 PCKS11이 지원되지 않습니다.
223	전달된 조치가 알려진 -random 조치가 아닙니다.
224	0(영)보다 짧은 길이는 허용되지 않습니다.
225	-strong 태그를 사용하는 경우 비밀번호 최소 길이는 14자입니다.
226	-strong 태그를 사용하는 경우 비밀번호 최대 길이는 300자입니다.
227	FIPS 모드에서는 MD5 알고리즘이 지원되지 않습니다.
228	-cert -list 명령에는 사이트 태그가 지원되지 않습니다. 이 속성은 역호환성 및 잠재적 향후 개선을 위해 추가됩니다.
229	-ca 태그와 연관된 값이 인식되지 않습니다. 값은 'true' 또는 'false'여야 합니다.
230	-type 태그와 함께 전달된 값이 올바르지 않습니다.
231	-expire 태그와 함께 전달된 값이 허용된 범위보다 아래에 있습니다.
232	사용되거나 요청된 암호화 알고리즘이 지원되지 않습니다.
233	대상이 이미 있습니다.

데이터베이스 인증의 보호 세부사항

사용자 이름 및 비밀번호 인증을 사용하여 데이터베이스 관리자에 연결하는 경우에는 비밀번호를 `qm.ini` 파일에 일반 텍스트로 저장하지 않도록 MQ XA 인증서 저장소에 저장할 수 있습니다.

자원 관리자를 위해 XAOpenString 업데이트

신임 정보 저장소를 사용하려면 `qm.ini` 파일에서 `XAOpenString`을 수정해야 합니다. 문자열은 데이터베이스 관리자에 연결하는 데 사용됩니다. `XAOpenString` 문자열 내에서 사용자 이름 및 비밀번호가 대체되는 위치를 식별하기 위해 대체 가능한 필드를 지정합니다.

- `+USER+` 필드는 `XACredentials` 저장소에 저장된 사용자 이름 값으로 대체됩니다.
- `+PASSWORD+` 필드는 `XACredentials` 저장소에 저장된 비밀번호 값으로 대체됩니다.

다음 예는 데이터베이스에 연결하기 위해 신임 정보 파일을 사용하기 위해 `XAOpenString`을 수정하는 방법을 보여줍니다.

Db2 데이터베이스에 연결

```
XAResourceManager:  
Name=mydb2  
SwitchFile=db2swit  
XAOpenString=db=mydbname,uid=+USER+,pwd=+PASSWORD+,toc=t  
ThreadOfControl=THREAD
```

Oracle 데이터베이스에 연결

```
XAResourceManager:  
Name=myoracle  
SwitchFile=oraswit  
XAOpenString=Oracle_XA+Acc=P/+USER+/+PASSWORD++SesTm=35  
+LogDir=/tmp+threads=true  
ThreadOfControl=THREAD
```

MQ XA 신임 정보 저장소에 대한 데이터베이스의 신임 정보에 대한 작업

교체 가능한 신임 문자열로 `qm.ini` 파일을 업데이트한 후에는 `setmqxacred` 명령을 사용하여 MQ 신임 정보 저장소에 사용자 이름 및 비밀번호를 추가해야 합니다. `setmqxacred`를 사용하여 기존 신임 정보를 수정하고, 신임 정보를 삭제하거나 신임 정보를 나열할 수도 있습니다. 다음 예는 일부 일반적 유스 케이스를 제공합니다.

신임 정보 추가

다음 명령은 자원 `mqdb2`에 대해 큐 관리자 `QM1`의 사용자 이름 및 비밀번호를 안전하게 저장합니다.

```
setmqxacred -m QM1 -x mydb2 -u user1 -p Password2
```

신임 정보 업데이트

데이터베이스에 연결하는 데 사용되는 사용자 이름 및 비밀번호를 업데이트하려면 `setmqxacred` 명령을 새 사용자 이름 및 비밀번호로 재발행하십시오.

```
setmqxacred -m QM1 -x mydb2 -u user3 -p Password4
```

변경사항을 적용하려면 큐 관리자를 재시작해야 합니다.

신임 정보 삭제

다음 명령은 신임 정보를 삭제합니다.

```
setmqxacred -m QM1 -x mydb2 -d
```

신입 정보 나열

다음 명령은 신입 정보를 나열합니다.

```
setmqxacred -m QM1 -1
```

관련 참조

[setmqxacred](#)

Managed File Transfer 보호

설치 직후 수정되지 않은 상태에서 Managed File Transfer는 보호된 환경에서 테스트 또는 평가 목적에 적합할 수 있는 보안 레벨을 가지고 있습니다. 하지만 프로덕션 환경에서는 파일 전송 작업을 시작할 수 있는 사용자, 전송 중인 파일을 읽고 쓸 수 있는 사용자 및 파일의 무결성을 보호하는 방법에 대한 적절한 제어를 고려해야 합니다.

관련 태스크

[MFT 고유 자원에 대한 그룹 권한 제한](#)

[MFT 고유 자원에 대한 권한 관리](#)

[544 페이지의 『Managed File Transfer과\(와\) 함께 Advanced Message Security 사용』](#)

이 시나리오에서는 Managed File Transfer를 통해 전송되는 데이터에 대해 메시지 개인정보 보호정책을 제공하도록 Advanced Message Security 를 구성하는 방법에 대해 설명합니다.

관련 참조

[파일 시스템에 액세스하기 위한 MFT의 권한](#)

[commandPath MFT 특성](#)

[MFT 에이전트 로그 및 상태 메시지를 발행할 수 있는 권한](#)

MFT 및 IBM MQ 연결 인증

연결 인증을 사용하면 큐 관리자가 제공된 사용자 ID 및 비밀번호를 사용하여 애플리케이션을 인증하도록 구성될 수 있습니다. 연관된 큐 관리자에서 보안이 사용되고 신입 정보 세부사항(사용자 ID 및 비밀번호)이 필요한 경우, 큐 관리자에 연결하려면 연결 인증 기능이 사용으로 설정되어야 합니다. 연결 인증은 호환 모드 또는 MQCSP 인증 모드에서 실행할 수 있습니다.

신입 정보 세부사항을 제공하는 메소드

많은 Managed File Transfer 명령에서 신입 정보 세부사항을 제공하는 다음 방법을 지원합니다.

세부사항을 명령행 인수에서 제공

신입 정보 세부사항은 **-mquserid** 및 **-mqpassword** 매개변수를 사용하여 지정할 수 있습니다.

-mqpassword가 제공되지 않으면, 사용자는 입력이 표시되지 않는 위치에서 비밀번호를 입력하도록 요청합니다.

세부사항을 신입 정보 파일 MQMFTCredentials.xml에서 제공

MQMFTCredentials.xml 파일에서 신입 정보 세부사항을 일반 텍스트 또는 난독화된 텍스트로 사전 정의할 수 있습니다.

IBM MQ for Multiplatforms 에서 MQMFTCredentials.xml 파일 설정에 대한 정보는 [488 페이지의 『멀티플랫폼에서 MQMFTCredentials.xml 구성』](#)의 내용을 참조하십시오.

IBM MQ for z/OS 에서 MQMFTCredentials.xml 파일 설정에 대한 정보는 [489 페이지의 『z/OS 에서 MQMFTCredentials.xml 구성』](#)의 내용을 참조하십시오.

우선순위

신입 정보 세부사항 판별 우선순위는 다음과 같습니다.

1. 명령행 인수
2. 연관된 큐 관리자 및 명령을 실행하는 사용자별 MQMFTCredentials.xml 색인

3. 연관된 큐 관리자별 MQMFTCredentials.xml 색인
4. IBM MQ 또는 IBM WebSphere MQ 의 이전 릴리스와의 호환성을 허용하기 위해 신임 정보 세부사항이 제공되지 않는 기본 역호환성 모드

참고:

- **fteStartAgent** 및 **fteStartLogger** 명령은 명령행 인수 **-mquserid** 또는 **-mqpassword**를 지원하지 않으며 MQMFTCredentials.xml 파일을 사용하는 경우에만 신임 정보 세부사항을 지정할 수 있습니다.

▶ **z/OS**

z/OS에서는 사용자의 비밀번호가 소문자를 갖는 경우에도 비밀번호가 대문자여야 합니다. 예를 들어 사용자 비밀번호가 "password"인 경우 "PASSWORD"로 입력해야 합니다.

관련 참조

[MFT 명령과 큐 관리자의 연결 조합](#)

[MFT 신임 정보 파일 형식](#)

멀티플랫폼에서 MQMFTCredentials.xml 구성

Managed File Transfer (MFT) 가 보안 사용으로 구성된 경우, 연결 인증에는 큐 관리자와 연결하여 사용자 ID 및 비밀번호 신임 정보를 제공하는 모든 MFT 명령이 필요합니다. 마찬가지로, MFT 로거는 데이터베이스에 연결할 때 사용자 ID 및 비밀번호를 지정해야 합니다. 이 신임 정보는 MFT 신임 정보 파일에 저장될 수 있습니다.

이 태스크 정보

MQMFTCredentials.xml 파일의 요소는 MQMFTCredentials.xsd 스키마를 따라야 합니다.

MQMFTCredentials.xml 형식에 대한 정보는 [MFT 권한 정보 파일 형식](#)을 참조하십시오.

MQ_INSTALLATION_PATH/mqft/samples/credentials 디렉토리에서 샘플 신임 정보 파일을 찾을 수 있습니다.

MFT 신임 정보 파일은 조정 큐 관리자, 명령 큐 관리자, 개별 에이전트 및 개별 로거에 대해 각각 하나씩 있을 수 있습니다. 또는 토폴로지의 모든 항목이 사용하는 하나의 파일을 가질 수 있습니다.

MFT 신임 정보 파일의 기본 위치는 다음과 같습니다.

Linux > UNIX **UNIX and Linux**
\$HOME

Windows **Windows**
%USERPROFILE% 또는 %HOMEDRIVE%\%HOMEPATH%

신임 정보 파일이 다른 위치에 저장되는 경우, 다음 특성을 사용하여 명령이 검색해야 하는 위치를 지정할 수 있습니다.

표 91. : 다양한 명령에 대한 MQMFTCredentials.xml 파일의 위치를 정의하는 특성.		
명령어 유형	특성 파일	특성 이름
조정 큐 관리자에 연결하는 명령	coordination.properties	coordinationQMGrAuthenticationCredentialsFile
명령 큐 관리자에 연결하는 명령	connection.properties	connectionQMGrAuthenticationCredentialsFile
에이전트 프로세스에 연결하는 명령	agent.properties	agentQMGrAuthenticationCredentialsFile
로거 프로세스에 연결하는 명령	logger.properties	loggerQMGrAuthenticationCredentialsFile

표 92. : 에이전트 및 로거 프로세스에 대한 MQMFTCredentials.xml .		
명령어 유형	특성 파일	특성 이름
MFT 에이전트	agent.properties	agentQMGrAuthenticationCredentialsFile
MFT loggers	logger.properties	loggerQMGrAuthenticationCredentialsFile

큐 관리자에 연결하는 명령 및 프로세스에 대한 자세한 내용은 어떤 MFT 명령과 프로세스가 어떤 큐 관리자에 연결됩니다.의 내용을 참조하십시오.

신입 정보 파일에는 사용자 ID 및 비밀번호 정보가 포함되어 있으므로 권한이 부여되지 않은 액세스를 방지하려면 특수 권한이 필요합니다.

Linux > UNIX UNIX and Linux

```
chown <agent owner userid>
chmod 600
```

Windows Windows

상속이 사용 가능하지 않은지 확인한 후 신입 정보 파일을 사용할 에이전트 또는 로거를 실행하는 권한을 제외한 모든 사용자 ID를 제거하십시오.

The credential details used to connect to an MFT coordination queue manager, in the IBM MQ Explorer Managed File Transfer plug-in for , depends on the type of configuration:

글로벌(로컬 디스크의 구성)

글로벌 구성은 조정 및 명령 특성에 지정된 신입 정보 파일을 사용합니다.

로컬(IBM MQ Explorer 내에서 정의됨):

로컬 구성은 IBM MQ Explorer에 있는 연관 큐 관리자의 연결 세부사항 특성을 사용합니다.

관련 태스크

491 페이지의 『MFT의 연결 인증 사용』

조정 큐 관리자 또는 명령 큐 관리자와 연결하는 IBM MQ Explorer MFT 플러그인의 연결 인증, 그리고 조정 큐 관리자 또는 명령 큐 관리자와 연결하는 Managed File Transfer 에이전트의 연결 인증은 호환 모드 또는 MQCSP 인증 모드로 실행될 수 있습니다.

관련 참조

MFT 신입 정보 파일 형식

fteObfuscate: 민감한 데이터 암호화

z/OS z/OS 에서 MQMFTCredentials.xml 구성

Managed File Transfer (MFT) 가 보안이 사용 가능한 상태로 구성된 경우, 연결 인증에는 모든 MFT 에이전트 및 큐 관리자에 연결하는 명령이 사용자 ID 및 비밀번호 신입 정보를 제공해야 합니다.

마찬가지로, MFT 로거는 데이터베이스에 연결할 때 사용자 ID 및 비밀번호를 지정해야 할 수 있습니다.

이 신입 정보는 MFT 신입 정보 파일에 저장할 수 있습니다. 신입 정보 파일은 선택사항이지만 환경을 사용자 정의하기 전에 필요한 파일을 정의하는 것이 더 쉽습니다.

또한 신입 정보 파일이 있는 경우 더 적은 경고 메시지를 수신합니다. MFT에서 큐 관리자 보안이 해제된 것으로 간주되면 경고 메시지로 알려져 사용자가 인증 세부사항을 제공하지 않도록 합니다.

MQ_INSTALLATION_PATH/mqft/samples/credentials 디렉토리에서 샘플 신입 정보 파일을 찾을 수 있습니다.

다음은 MQMFTCredentials.xml 파일의 예제입니다.

```
<?xml version="1.0" encoding="IBM-1047"?>
<tns:mqmftCredentials xmlns:tns="http://wmqfte.ibm.com/MFTCredentials"
xmlns:xsi="https://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://wmqfte.ibm.com/MFTCredentials MFTCredentials.xsd">
  <tns:qmgr name="MQPH" user="ADMIN" mqUserId="JOHNDOEH" mqPassword="cXXXX" />
```



```

<tns:qmgr name="MQPI" user="ADMIN" mqUserId="JOHNDOEI" mqPassword="yXXXX" />
<tns:qmgr name="MQPH" mqUserId="NONEH" mqPassword="yXXXX" />
<tns:qmgr name="MQPI" mqUserId="NONEI" mqPassword="yXXXX" />
</tns:mqmftCredentials>

```

사용자 ID가 ADMIN인 작업은 큐 관리자 MQPH에 연결해야 할 때 사용자 ID JOHNDOEH를 전달하고 비밀번호 cXXXX를 사용합니다.

작업이 다른 사용자 ID로 실행되어 MQPH를 연결하는 경우, 해당 작업은 사용자 ID NONEH 및 비밀번호 yXXXX를 전달합니다.

MQMFTCredentials.xml 파일의 기본 위치는 USS (z/OS UNIX System Services) 에서 사용자의 홈 디렉토리입니다. USS의 다른 위치 또는 파티션된 데이터 세트 내의 멤버에 파일을 저장할 수도 있습니다.

신임 정보 파일이 다른 위치에 저장된 경우 다음 특성을 사용하여 명령이 검색해야 하는 위치를 지정할 수 있습니다.

표 93. : 다양한 명령에 대한 MQMFTCredentials.xml 파일의 위치를 정의하는 특성입니다.		
명령 유형	특성 파일	특성 이름
조정 큐 관리자에 연결하는 명령	coordination.properties	coordinationQMGrAuthenticationCredentialsFile
명령 큐 관리자에 연결하는 명령	connection.properties	connectionQMGrAuthenticationCredentialsFile
에이전트 프로세스에 연결하는 명령	agent.properties	agentQMGrAuthenticationCredentialsFile
로거 프로세스에 연결하는 명령	logger.properties	loggerQMGrAuthenticationCredentialsFile

표 94. : 에이전트 및 로거 프로세스에 대한 MQMFTCredentials.xml 파일의 위치를 정의하는 특성입니다.		
명령 유형	특성 파일	특성 이름
MFT 에이전트	agent.properties	agentQMGrAuthenticationCredentialsFile
MFT loggers	logger.properties	loggerQMGrAuthenticationCredentialsFile

어떤 명령 및 프로세스가 어떤 큐 관리자에 연결되는지에 대한 세부사항은 [어떤 MFT 명령 및 프로세스가 어떤 큐 관리자에 연결되는지](#)를 참조하십시오.

파티션된 데이터 세트 내에서 신임 정보 파일을 작성하려면 다음 단계를 수행하십시오.

- 형식이 VB이고 논리 레코드 길이(Lrecl)가 200인 PDSE를 작성하십시오.
- 데이터 세트 내에 멤버를 작성하고, 데이터 세트 및 멤버를 기록해 두고, 다음 코드를 멤버에 추가하십시오.

```

<?xml version="1.0" encoding="IBM-1047"?>
<tns:mqmftCredentials xmlns:tns="http://wmqfte.ibm.com/MQMFTCredentials"
xmlns:xsi="https://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://wmqfte.ibm.com/MFTCredentials MQMFTCredentials.xsd">
  <!--credentials information goes here-->
</tns:mqmftCredentials>

```

보안 제품 (예: RACF) 을 사용하여 신임 정보 파일을 보호할 수 있지만 Managed File Transfer 명령을 실행하고 에이전트 및 로거 프로세스를 관리하는 사용자 ID는 이 파일에 대한 읽기 액세스 권한이 필요합니다.

멤버 BFGCROBS의 JCL을 사용하여 이 파일에서 정보를 숨길 수 있습니다. 이는 파일을 가져와서 IBM MQ 사용자 ID 및 비밀번호를 암호화합니다. 예를 들어, 멤버 BFGCROBS는 다음 행을 가져와서

```

<tns:qmgr name="MQPI" user="JOHNDOE2" mqUserId="JOHNDOE1" mqPassword="yXXXX" />

```

다음을 작성합니다.

```
<tns:mqgr mqPasswordCipher="e977c61e9b9c363c" mqUserIdCipher="c394c5887867157c"
name="MQPI" user="JOHND0E2"/>
```

사용자 ID 대 IBM MQ 사용자 ID 매핑을 보관하려면 파일에 주석을 추가할 수 있습니다. 예:

```
<!-- name="MQPI" user="ADMIN" mqUserId="JOHND0E1" -->
```

이러한 주석은 숨기기 프로세스에 의해 변경되지 않습니다.

컨텐츠는 강력하게 암호화되지 않고 이해하기 힘들게 되어 있다는 점을 유의하십시오. 파일에 액세스할 수 있는 사용자 ID를 제한해야 합니다.

관련 태스크

488 페이지의 『멀티플랫폼에서 MQMFTCredentials.xml 구성』

Managed File Transfer (MFT) 가 보안 사용으로 구성된 경우, 연결 인증에는 큐 관리자와 연결하여 사용자 ID 및 비밀번호 신임 정보를 제공하는 모든 MFT 명령이 필요합니다. 마찬가지로, MFT 로거는 데이터베이스에 연결할 때 사용자 ID 및 비밀번호를 지정해야 합니다. 이 신임 정보는 MFT 신임 정보 파일에 저장될 수 있습니다.

MFT의 연결 인증 사용

조정 큐 관리자 또는 명령 큐 관리자와 연결하는 IBM MQ Explorer MFT 플러그인의 연결 인증, 그리고 조정 큐 관리자 또는 명령 큐 관리자와 연결하는 Managed File Transfer 에이전트의 연결 인증은 호환 모드 또는 MQCSP 인증 모드로 실행될 수 있습니다.

이 태스크 정보

IBM MQ 9.1.1 이전 버전에서는 호환 모드가 연결 인증에 대한 기본 설정입니다. 그러나 사용자는 기본 호환 모드를 사용 안함으로 설정하고 MQCSP 인증 모드를 사용으로 설정할 수 있습니다.

V 9.1.1 IBM MQ 9.1.1부터, MQCSP 인증 모드가 기본값입니다.

CLIENT 전송을 사용하여 큐 관리자에 연결하는 IBM MQ Explorer Managed File Transfer 플러그인 또는 Managed File Transfer 에이전트의 연결 인증에서, 12자보다 긴 비밀번호는 MQCSP 인증 모드에서만 지원됩니다. 호환 모드를 사용한 권한 부여에서 12자보다 긴 비밀번호를 지정하는 경우에는 오류가 발생하며 큐 관리자에 인증되지 않습니다. 진단 메시지: BFGAG0001 - BFGAG9999에서 BFGAG0187E 메시지를 참조하십시오.

프로시저

- IBM MQ Explorer에서 조정 큐 관리자 또는 명령 큐 관리자의 연결 인증 모드를 선택하려면 다음 단계를 완료하십시오.
 - a) 연결하려는 큐 관리자를 선택하십시오.
 - b) 마우스의 오른쪽 단추를 클릭하고 팝업 메뉴에서 **연결 세부사항->특성**을 선택하십시오.
 - c) **사용자 ID** 탭을 클릭하십시오.
 - d) 사용할 연결 인증 모드에 대한 선택란이 선택되었는지 확인하십시오.
 - **V 9.1.0** IBM MQ 9.1.0부터는 기본적으로 **사용자 ID 호환 모드** 선택란이 선택 취소되어 있습니다. 이는 **사용자 ID 사용** 선택란이 선택된 경우 IBM MQ Explorer가 큐 관리자에 연결하는 데 MQCSP 인증을 사용함을 의미합니다. IBM MQ Explorer가 MQCSP 인증이 아니라 호환 모드를 사용하여 큐 관리자에 연결해야 하는 경우에는 **사용자 ID 사용** 및 **사용자 ID 호환 모드** 선택란이 둘 다 선택되어 있는지 확인하십시오.
 - IBM MQ 9.1.0 이전에는 기본적으로 **사용자 ID 호환 모드** 선택란이 선택되어 있습니다. 이는 **사용자 ID 사용** 선택란이 선택된 경우 IBM MQ Explorer가 큐 관리자에 연결하는 데 호환 모드를 사용함을 의미합니다. IBM MQ Explorer가 MQCSP 인증을 사용하여 큐 관리자에 연결해야 하는 경우에는 **사용자 ID 사용** 선택란은 선택되어 있고 **사용자 ID 호환 모드** 선택란은 선택 취소되어 있는지 확인하십시오.
- MQMFTCredentials.xml 파일을 사용하여 Managed File Transfer 에이전트에 대해 MQCSP 인증 모드를 사용하거나 사용하지 않으려면 **useMQCSPAuthentication** 매개변수를 관련 사용자의 MQMFTCredentials.xml 파일에 추가하십시오.

useMQCSPAAuthentication 매개변수는 다음 값을 갖습니다.

true

큐 관리자에 사용자를 인증하는 데 MQCSP 인증 모드가 사용됩니다.

V 9.1.1 IBM MQ 9.1.1부터는 true가 기본값입니다. **useMQCSPAAuthentication** 매개변수가 지정되지 않은 경우 이는 기본적으로 true로 설정되며 큐 관리자에 사용자를 인증하는 데 MQCSP 인증 모드가 사용됩니다.

false

큐 관리자에 사용자를 인증하는 데 호환 모드가 사용됩니다.

IBM MQ 9.1.1 이전에는 **useMQCSPAAuthentication** 매개변수가 지정되지 않은 경우 이는 기본적으로 false로 설정되며 큐 관리자에 사용자를 인증하는 데 호환 모드가 사용됩니다.

다음 예는 MQMFTCredentials.xml 파일에서 **useMQCSPAAuthentication** 매개변수를 설정하는 방법을 보여줍니다.

```
<tns:qmgr name="CoordQueueMgr" user="ernest" mqUserId="ernest"
mqPassword="AveryL0ngPassw0rd2135" useMQCSPAAuthentication="true"/>
```

관련 개념

26 페이지의 『MQCSP 비밀번호 보호』

IBM MQ 8.0에서 IBM MQ 기능을 사용하여 보호되거나 TLS 암호화를 사용하여 암호화된 MQCSP 구조에 포함된 비밀번호를 전송할 수 있습니다.

관련 참조

487 페이지의 『MFT 및 IBM MQ 연결 인증』

연결 인증을 사용하면 큐 관리자가 제공된 사용자 ID 및 비밀번호를 사용하여 애플리케이션을 인증하도록 구성될 수 있습니다. 연관된 큐 관리자에서 보안이 사용되고 신임 정보 세부사항(사용자 ID 및 비밀번호)이 필요한 경우, 큐 관리자에 연결하려면 연결 인증 기능이 사용으로 설정되어야 합니다. 연결 인증은 호환 모드 또는 MQCSP 인증 모드에서 실행할 수 있습니다.

MFT 신임 정보 파일 형식

MFT 샌드박스

전송 과정에서 에이전트가 액세스할 수 있는 파일 시스템의 영역을 제한할 수 있습니다. 에이전트의 액세스가 제한되는 영역을 샌드박스라고 합니다. 전송을 요청하는 사용자 또는 에이전트에 제한을 적용할 수 있습니다.

에이전트가 프로토콜 브릿지 에이전트이거나 Connect:Direct® 브릿지 에이전트인 경우 샌드박스는 지원되지 않습니다. IBM MQ 큐로나 큐로부터 전송해야 할 에이전트에는 에이전트 샌드박싱을 사용할 수 없습니다.

관련 참조

492 페이지의 『MFT 에이전트 샌드박스에 대한 작업』

Managed File Transfer에 추가 보안 레벨을 추가하기 위해 에이전트가 액세스할 수 있는 파일 시스템 영역을 제한할 수 있습니다.

494 페이지의 『MFT 사용자 샌드박스에 대한 작업』

전송을 요청한 사용자의 MQMD 사용자 이름에 기반하여 파일을 송수신할 수 있는 파일 시스템의 영역을 제한할 수 있습니다.

MFT 에이전트 샌드박스에 대한 작업

Managed File Transfer에 추가 보안 레벨을 추가하기 위해 에이전트가 액세스할 수 있는 파일 시스템 영역을 제한할 수 있습니다.

IBM MQ 큐로나 큐로부터 전송하는 에이전트에는 에이전트 샌드박싱을 사용할 수 없습니다. 대신 모든 샌드박스 요구사항에 대한 권장 솔루션인 사용자 샌드박싱을 사용하여 샌드박싱의 IBM MQ 큐에 대한 액세스 제한을 구현할 수 있습니다. 사용자 샌드박싱에 대한 자세한 정보는 494 페이지의 『MFT 사용자 샌드박스에 대한 작업』의 내용을 참조하십시오.

에이전트 샌드박싱을 사용으로 설정하려면 제한하려는 에이전트의 `agent.properties` 파일에 다음 특성을 추가하십시오.

```
sandboxRoot=[!]restricted_directory_nameseparator...separator[!]restricted_directory_name
```

설명:

- `restricted_directory_name`은 허용하거나 거부할 디렉토리 경로입니다.
- `!`는 선택사항이며 `restricted_directory_name`에 대한 다음 값이 거부(제외)되도록 지정합니다. `!`를 지정하지 않으면 `restricted_directory_name`은 허용(포함) 경로입니다.
- `separator`는 플랫폼별 구분 기호입니다.

예를 들어, AGENT1이 소유하는 액세스 권한을 `/tmp` 디렉토리만으로 제한하지만 `private` 서브디렉토리에 대한 액세스는 허용하지 않으려는 경우 AGENT1에 속하는 `agent.properties` 파일에서 `sandboxRoot=/tmp:!/tmp/private`과 같이 특성을 설정하십시오.

`sandboxRoot` 특성에 대해서는 [고급 에이전트 특성에](#) 설명되어 있습니다.

에이전트 및 사용자 샌드박싱은 둘 다 프로토콜 브릿지 에이전트 또는 Connect:Direct 브릿지 에이전트에서 지원되지 않습니다.

UNIX, Linux 및 Windows 플랫폼에서의 샌드박스 작업

ULW UNIX, Linux 및 Windows 플랫폼에서 샌드박싱은 Managed File Transfer Agent가 읽고 쓸 수 있는 디렉토리를 제한합니다. 샌드박싱이 활성화된 경우, Managed File Transfer Agent는 허용된 것으로 지정된 디렉토리와 지정된 디렉토리에 들어 있는 서브디렉토리(서브디렉토리가 `sandboxRoot`에서 거부된 것으로 지정되지 않은 경우)만 읽고 쓸 수 있습니다. Managed File Transfer 샌드박싱은 운영 체제 보안에서 우선권이 없습니다. Managed File Transfer Agent를 시작한 사용자에게는 디렉토리를 읽고 쓸 수 있는 디렉토리에 대한 적절한 운영 체제 레벨의 액세스 권한이 있어야 합니다. 지정된 `sandboxRoot` 디렉토리(및 서브디렉토리) 외부로 디렉토리가 링크되면 해당 디렉토리로 링크되는 기호 링크가 작동되지 않습니다.

z/OS에서의 샌드박스 작업

z/OS z/OS에서 샌드박싱은 Managed File Transfer Agent가 읽고 쓸 수 있는 데이터 세트 이름 규정을 제한합니다. Managed File Transfer Agent를 시작한 사용자에게는 관련된 모든 데이터 세트에 대한 올바른 운영 체제 권한이 있어야 합니다. `sandboxRoot` 데이터 세트 이름 규정자 값을 큰따옴표로 묶으면 이 값은 일반적인 z/OS 규칙을 따르며 완전한 값으로 처리됩니다. 큰따옴표를 생략하면 `sandboxRoot`의 접두부에 현재 사용자 ID가 추가됩니다. 예를 들어, `sandboxRoot=//test`로 설정하면 에이전트가 표준 z/OS 표기법으로 `//username.test.**` 인 데이터 세트에 액세스할 수 있습니다. 런타임 시 완전히 해석된 데이터 세트 이름의 초기 레벨이 `sandboxRoot`와 일치하지 않는 경우에는 전송 요청이 거부됩니다.

IBM i 시스템에서의 샌드박스 작업

IBM i IBM i 시스템에서 통합 파일 시스템에 있는 파일의 경우, 샌드박싱은 Managed File Transfer Agent가 읽고 쓸 수 있는 디렉토리를 제한합니다. 샌드박싱이 활성화된 경우, Managed File Transfer Agent는 허용된 것으로 지정된 디렉토리와 지정된 디렉토리에 들어 있는 서브디렉토리(서브디렉토리가 `sandboxRoot`에서 거부된 것으로 지정되지 않은 경우)만 읽고 쓸 수 있습니다. Managed File Transfer 샌드박싱은 운영 체제 보안에서 우선권이 없습니다. Managed File Transfer Agent를 시작한 사용자에게는 디렉토리를 읽고 쓸 수 있는 디렉토리에 대한 적절한 운영 체제 레벨의 액세스 권한이 있어야 합니다. 지정된 `sandboxRoot` 디렉토리(및 서브디렉토리) 외부로 디렉토리가 링크되면 해당 디렉토리로 링크되는 기호 링크가 작동되지 않습니다.

관련 참조

[497 페이지의 『와일드카드 전송 시의 추가 점검사항』](#)

에이전트가 파일을 주고 받을 수 있는 위치를 제한하기 위해 사용자 또는 에이전트 샌드박싱을 사용하여 에이전트를 구성하는 경우 해당 에이전트에 대한 와일드카드 전송 시 추가적인 검사가 이루어지도록 지정할 수 있습니다.

[492 페이지의 『MFT 에이전트 샌드박싱에 대한 작업』](#)

Managed File Transfer에 추가 보안 레벨을 추가하기 위해 에이전트가 액세스할 수 있는 파일 시스템 영역을 제한할 수 있습니다.

MFT 사용자 샌드박스에 대한 작업

전송을 요청한 사용자의 MQMD 사용자 이름에 기반하여 파일을 송수신할 수 있는 파일 시스템의 영역을 제한할 수 있습니다.

에이전트가 프로토콜 브릿지 에이전트이거나 Connect:Direct 브릿지 에이전트인 경우에는 사용자 샌드박스가 지원되지 않습니다.

사용자 샌드박스를 사용으로 설정하려면 제한하려는 에이전트의 agent.properties 파일에 다음 특성을 추가하십시오.

```
userSandboxes=true
```

이 특성이 있고 true로 설정된 경우 에이전트는 MQ_DATA_PATH/mqft/config/coordination_qmgr_name/agents/agent_name/UserSandboxes.xml 파일에 있는 정보를 사용하여 전송을 요청하는 사용자가 액세스할 수 있는 파일 시스템의 부분을 판별합니다.

UserSandboxes.xml XML은 0개 이상의 <sandbox> 요소를 포함하는 <agent> 요소로 구성됩니다. 이러한 요소가 어떤 규칙이 어떤 사용자에게 적용되는지를 기술합니다. <sandbox> 요소의 user 속성은 요청의 MQMD 사용자를 찾는 데 사용되는 패턴입니다.

UserSandboxes.xml 파일은 에이전트가 주기적으로 다시 로드하며 이 파일에 대한 유효한 변경사항은 에이전트의 작동에 영향을 미칩니다. 기본 다시 로드 간격은 30초입니다. 이 간격은 agent.properties 파일에서 xmlConfigReloadInterval 에이전트 특성을 지정하여 변경할 수 있습니다.

userPattern="regex" 속성 또는 값을 지정하면, user 속성은 Java 정규식으로 해석됩니다. 자세한 정보는 MFT에서 사용하는 정규식을 참조하십시오.

userPattern="regex" 속성이나 값을 지정하지 않으면 user 속성은 다음 와일드카드 문자를 가진 패턴으로 해석됩니다.

- 별표(*) - 0개 이상의 문자를 표시
- 물음표(?) - 정확히 하나의 문자를 표시

<sandbox> 요소가 파일에 나열된 순서대로 일치가 수행됩니다. 첫 번째 일치만 사용되며 파일에서 이후 모든 잠재적 일치는 무시됩니다. 파일에 지정된 <sandbox> 요소 중 전송 요청 메시지와 연관된 MQMD 사용자와 일치하는 항목이 없을 경우 전송 시 파일 시스템에 액세스할 수 없습니다. MQMD 사용자 이름과 user 속성 사이에서 일치 발견되면 해당 일치는 <sandbox> 요소 내에서 전송에 적용되는 규칙 세트를 식별합니다. 이 규칙 세트는 전송 중에 읽거나 쓸 수 있는 파일 또는 데이터 세트 항목을 판별하는 데 사용됩니다.

각 규칙 세트는 읽을 수 있는 파일을 식별하는 <read> 요소와 쓸 수 있는 파일을 식별하는 <write> 요소를 지정할 수 있습니다. 규칙 세트에서 <read> 또는 <write> 요소를 생략하면 해당 규칙 세트와 연관된 사용자는 적절하게 읽기 또는 쓰기를 수행할 수 없는 것으로 간주됩니다.

참고: UserSandboxes.xml 파일에서 <read> 요소는 <write> 요소 앞에 있어야 하고 <include> 요소는 <exclude> 요소 앞에 있어야 합니다.

각 <read> 또는 <write> 요소에는 파일이 샌드박스에 있고 전송될 수 있는지 여부를 판별하는 데 사용되는 하나 이상의 패턴이 포함되어 있습니다. <include> 및 <exclude> 요소를 사용하여 이러한 패턴을 지정하십시오. <include> 또는 <exclude> 요소의 name 속성은 일치시킬 패턴을 지정합니다. 선택적인 type 속성은 이름 값이 파일인지 또는 큐 패턴인지 여부를 지정합니다. type 속성이 지정되지 않은 경우에는 에이전트가 패턴을 파일 또는 디렉토리 경로 패턴으로 취급합니다. 예를 들면, 다음과 같습니다.

```
<tns:read>
  <tns:include name="/home/user/**"/>
  <tns:include name="USER.**" type="queue"/>
  <tns:exclude name="/home/user/private/**"/>
</tns:read>
```


<include> 및 <exclude> name 패턴은 에이전트에서 파일, 데이터 세트 또는 큐를 읽거나 쓸 수 있는지 판별하는 데 사용됩니다. 표준 파일 경로, 데이터 세트 또는 큐 이름이 하나 이상의 포함 패턴과 일치하고 제외 패턴과는 일치하지 않는 경우 조작이 허용됩니다. <include> 및 <exclude> 요소의 name 속성을 사용하여 지정된 패턴은 에이전트가 실행 중인 플랫폼에 적합한 경로 구분 기호 및 규칙을 사용합니다. 상대 파일 경로를 지정하는 경우, 에이전트의 transferRoot 특성과 관련하여 경로가 해석됩니다.

큐 제한을 지정하면 QUEUE@QUEUEMANAGER 구문이 지원되고 다음과 같은 규칙이 적용됩니다.

- at 문자(@)가 항목에서 누락된 경우 패턴을 모든 큐 관리자에서 액세스할 수 있는 큐 이름으로 처리합니다. 예를 들어, 패턴이 name인 경우 이는 name@**와 동일한 방법으로 처리됩니다.
- at 문자(@)가 항목의 첫 번째 문자인 경우 패턴을 큐 관리자 이름으로 처리하며 큐 관리자의 모든 큐에 액세스할 수 있습니다. 예를 들어, 패턴이 @name인 경우 이는 **@name과 동일한 방법으로 처리됩니다.

다음 와일드카드 문자는 <include> 및 <exclude> 요소의 name 속성의 부분으로 지정하는 경우 특별한 의미를 갖습니다.


단일 별표는 디렉토리 이름 또는 데이터셋명 또는 큐 이름의 규정자에서 0개 이상의 문자와 일치합니다.

?

물음표는 디렉토리 이름의 정확히 한 문자 또는 데이터셋명 또는 큐 이름의 규정자와 일치합니다.

두 개의 별표 문자가 0개 이상의 디렉토리 이름과 일치하거나 데이터 세트 이름 또는 큐 이름에 0개 이상의 규정자가 있습니다. 또한 경로 구분 기호로 끝나는 경로에는 암시적 "*"가 경로의 끝에 추가됩니다. 따라서 /home/user/는 /home/user/**와 동일합니다.

예를 들면, 다음과 같습니다.

- /**/test/**는 경로에 test 디렉토리가 있는 모든 파일과 일치합니다.
- /test/file?는 file 문자열로 시작하고 뒤에 하나의 문자가 오는 /test 디렉토리 내의 모든 파일과 일치합니다.
- c:\test*.txt는 .txt 확장자가 있는 c:\test 디렉토리 내의 모든 파일과 일치합니다.
- c:\test***.txt는 .txt 확장자가 있는 'c:\test 디렉토리 또는 서브디렉토리 중 하나의 모든 파일과 일치합니다.
-  // 'TEST.*.DATA'는 첫 번째 규정자가 TEST이고 임의의 두 번째 규정자와 세 번째 규정자가 DATA인 모든 데이터 세트와 일치합니다.
- *@QM1는 단일 규정자가 있는 큐 관리자 QM1의 모든 큐와 일치합니다.
- TEST.*.QUEUE@QM1는 첫 번째 규정자가 TEST이고 임의의 두 번째 규정자와 세 번째 규정자가 QUEUE인 큐 관리자 QM1의 모든 큐와 일치합니다.
- **@QM1는 큐 관리자 QM1의 모든 큐와 일치합니다.

기호 링크

<include> 및 <exclude> 요소에 하드 링크를 지정하여 UserSandboxes.xml 파일의 파일 경로에 사용하는 모든 기호 링크를 완전히 해석해야 합니다. 예를 들어, /var 가 /SYSTEM/var로 맵핑되는 기호 링크가 있는 경우 이 경로를 <tns:include name="/SYSTEM/var"/>로 지정해야 합니다. 그렇지 않으면 사용자 샌드박스 보안 오류로 인해 의도한 전송이 실패합니다.

예

이 예제는 AGENT_JUPITER의 구성 디렉토리에 있는 UserSandboxes.xml 파일에 다음 <sandbox> 요소를 추가하여 MQMD 사용자 이름이 guest 인 사용자가 /home/user/public 디렉토리 또는 에이전트

AGENT_JUPITER가 실행 중인 시스템의 서브디렉토리에서 임의의 파일을 전송할 수 있도록 하는 방법을 보여줍니다.

```
<?xml version="1.0" encoding="UTF-8"?>
<tns:userSandboxes
  xmlns:tns="http://wmqfte.ibm.com/UserSandboxes"
  xmlns:xsi="https://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://wmqfte.ibm.com/UserSandboxes UserSandboxes.xsd">
  <tns:agent>
    <tns:sandbox user="guest">
      <tns:read>
        <tns:include name="/home/user/public/**"/>
      </tns:read>
    </tns:sandbox>
  </tns:agent>
</tns:userSandboxes>
```

예

이 예는 MQMD 사용자 이름 account 뒤에 한 자리 숫자가 있는 사용자(예: account4)가 다음 조치를 어떻게 완료하는지 보여줍니다.

- AGENT_SATURN 에이전트가 실행 중인 시스템에서 /home/account/private 디렉토리는 제외하고 /home/account 디렉토리 또는 이의 서브디렉토리에서 파일을 전송합니다.
- AGENT_SATURN 에이전트가 실행 중인 시스템에서 /home/account/output 디렉토리 또는 이의 서브디렉토리로 파일을 전송합니다.
- 로컬 큐 관리자의 큐에서 접두부 ACCOUNT.로 시작하는 메시지를 읽습니다(메시지가 ACCOUNT.PRIVATE.으로 시작하는 경우(즉, 두 번째 레벨에 PRIVATE이 있음) 제외).
- 모든 큐 관리자에서 접두부 ACCOUNT.OUTPUT.으로 시작하는 큐에 데이터를 전송합니다.

MQMD 사용자 이름이 account 인 사용자가 이러한 조치를 완료할 수 있도록 하려면 AGENT_SATURN의 구성 디렉토리에 있는 UserSandboxes.xml파일에 다음 <sandbox> 요소를 추가하십시오.

```
<?xml version="1.0" encoding="UTF-8"?>
<tns:userSandboxes
  xmlns:tns="http://wmqfte.ibm.com/UserSandboxes"
  xmlns:xsi="https://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://wmqfte.ibm.com/UserSandboxes UserSandboxes.xsd">
  <tns:agent>
    <tns:sandbox user="account[0-9]" userPattern="regex">
      <tns:read>
        <tns:include name="/home/account/**"/>
        <tns:include name="ACCOUNT.**" type="queue"/>
        <tns:exclude name="ACCOUNT.PRIVATE.**" type="queue"/>
        <tns:exclude name="/home/account/private/**"/>
      </tns:read>
      <tns:write>
        <tns:include name="/home/account/output/**"/>
        <tns:include name="ACCOUNT.OUTPUT.**" type="queue"/>
      </tns:write>
    </tns:sandbox>
  </tns:agent>
</tns:userSandboxes>
```

관련 참조

497 페이지의 『와일드카드 전송 시의 추가 점검사항』

에이전트가 파일을 주고 받을 수 있는 위치를 제한하기 위해 사용자 또는 에이전트 샌드박스를 사용하여 에이전트를 구성하는 경우 해당 에이전트에 대한 와일드카드 전송 시 추가적인 검사가 이루어지도록 지정할 수 있습니다.

[MFTagent.properties 파일](#)

와일드카드 전송 시의 추가 점검사항

에이전트가 파일을 주고 받을 수 있는 위치를 제한하기 위해 사용자 또는 에이전트 샌드박스를 사용하여 에이전트를 구성하는 경우 해당 에이전트에 대한 와일드카드 전송 시 추가적인 검사가 이루어지도록 지정할 수 있습니다.

additionalWildcardSandboxChecking 특성

와일드카드 전송에 대한 추가 검사를 사용으로 설정하려면 검사하려는 에이전트에 대한 `agent.properties` 파일에 다음 특성을 추가하십시오.

```
additionalWildcardSandboxChecking=true
```

이 특성이 `true`로 설정되어 있는 경우 에이전트가 와일드카드의 일치하는 파일을 찾기 위해 정의된 샌드박스의 외부 위치를 읽으려고 시도하는 전송 요청을 작성하면 전송이 실패합니다. 한 전송 요청에 여러 개의 전송이 포함되어 있고 이들 요청 중 하나가 샌드박스 외부 위치를 읽으려다 실패하는 경우 전체 전송이 실패합니다. 검사에 실패하면 실패 이유가 오류 메시지로 제공됩니다.

`additionalWildcardSandboxChecking` 특성이 에이전트의 `agent.properties` 파일에서 생략되거나 `false`로 설정된 경우 해당 에이전트의 와일드카드 전송에 대한 추가 검사가 수행되지 않습니다.

와일드카드 검사의 오류 메시지

구성된 샌드박스 위치의 외부로 와일드카드 전송 요청을 보내는 경우 보고되는 메시지는 다음과 같습니다.

다음 메시지는 전송 요청의 와일드카드 파일 경로가 제한된 샌드박스 외부에 있는 경우 발생합니다.

BFGSS0077E: 파일 경로 *path*을(를) 읽으려는 시도가 거부되었습니다.
파일 경로가 제한된 전송 샌드박스 외부에 있습니다.

여러 전송 요청 내의 한 전송에 와일드카드 전송 요청이 포함되어 있으며 해당 요청의 경로가 제한된 샌드박스 외부에 있는 경우 다음 메시지가 발생합니다.

BFGSS0078E: 파일 경로 읽기 시도: *path*가 다른 전송으로 무시됨
제한된 전송 샌드박스 외부에서 읽기를 시도했기 때문입니다.

다음 메시지는 파일이 제한된 샌드박스 외부에 있는 경우 발생합니다.

BFGSS0079E: 파일 *file path*을(를) 읽으려는 시도가 거부되었습니다.
파일이 제한된 전송 샌드박스 외부에 있습니다.

다음 메시지는 다른 와일드카드 전송 요청으로 인해 이 요청이 무시되는 여러 전송 요청에서 발생합니다.

BFGSS0080E: 파일 *file path*을(를) 읽으려는 시도가 거부되었습니다.
제한된 전송 샌드박스 외부에서 읽기를 시도했기 때문입니다.

와일드카드를 포함하지 않는 단일 파일 전송에서, 샌드박스 외부에 있는 파일이 전송에 관련되는 경우 보고되는 메시지는 이전 릴리스에서 변경되지 않았습니다.

BFGI00056E: "FILE" 파일을 읽으려는 시도가 거부되었습니다.
파일이 제한된 전송 샌드박스 외부에 있습니다.

관련 참조

[494 페이지의 『MFT 사용자 샌드박스에 대한 작업』](#)

전송을 요청한 사용자의 MQMD 사용자 이름에 기반하여 파일을 송수신할 수 있는 파일 시스템의 영역을 제한할 수 있습니다.

[492 페이지의 『MFT 에이전트 샌드박스에 대한 작업』](#)

Managed File Transfer에 추가 보안 레벨을 추가하기 위해 에이전트가 액세스할 수 있는 파일 시스템 영역을 제한할 수 있습니다.

[MFTagent.properties 파일](#)

MFT의 SSL 또는 TLS 암호화 구성

IBM MQ Managed File Transfer 와 함께 SSL 또는 TLS를 사용하여 에이전트와 해당 에이전트 큐 관리자, 명령 및 연결되는 큐 관리자 및 토폴로지 내의 큐 관리자 연결에 대한 다양한 큐 관리자 간의 통신을 보안할 수 있습니다.

시작하기 전에

SSL 또는 TLS 암호화를 사용하여 IBM MQ Managed File Transfer 토폴로지를 통해 플로우되는 메시지를 암호화할 수 있습니다. 다음이 포함됩니다.

- 에이전트와 해당 에이전트 큐 관리자 사이에 전달되는 메시지입니다.
- 연결되어 있는 명령 및 큐 관리자에 대한 메시지입니다.
- 에이전트 큐 관리자, 명령 큐 관리자 및 토폴로지 내의 조정 큐 관리자 간에 플로우되는 내부 메시지입니다.

이 태스크 정보

IBM MQ에서 SSL 사용에 대한 일반 정보는 244 페이지의 『SSL/TLS에 대한 작업』의 내용을 참조하십시오. IBM MQ 용어에서 Managed File Transfer는 표준 Java 클라이언트 애플리케이션입니다.

다음 단계를 수행하여 Managed File Transfer에 SSL을 사용하십시오.

프로시저

1. 신뢰 저장소 파일을 작성하고 선택적으로 키 저장소 파일을 작성하십시오(이들 파일이 동일할 수 있음). 클라이언트 인증(즉, 채널의 SSLCAUTH=OPTIONAL)이 필요하지 않은 경우 키 저장소를 제공하지 않아도 됩니다. 큐 관리자의 인증서를 인증하려면 신뢰 저장소가 필요합니다.
신뢰 저장소 및 키 저장소에 대한 인증서를 작성하는 데 사용되는 키 알고리즘은 IBM MQ와 작동하려면 RSA 이어야 합니다.
2. SSL을 사용하도록 IBM MQ 큐 관리자를 설정하십시오.
SSL을 사용하도록 큐 관리자를 설정하는 방법(예: IBM MQ Explorer 사용)에 대한 정보는 [큐 관리자의 SSL 구성을 참조하십시오](#).
3. 신뢰 저장소 파일 및 키 저장소 파일(있을 경우)을 적당한 위치에 저장하십시오. 제안된 위치는 `config_directory/coordination_qmgr/agents/agent_name` 디렉토리입니다.
4. 해당 Managed File Transfer 특성 파일에서 필요에 따라 각 SSL 사용 큐 관리자에 대한 SSL 특성을 설정하십시오. 하나의 큐 관리자가 두 개 이상의 역할을 수행할 수도 있지만 각 특성 세트는 개별 큐 관리자(에이전트, 조정 및 명령)를 참조합니다.

CipherSpec 또는 **CipherSuite** 특성 중 하나는 필수입니다. 이 특성이 없으면 클라이언트가 SSL 없이 연결을 시도합니다. Both the **CipherSpec** or **CipherSuite** properties are provided because of the terminology differences between IBM MQ and Java. Managed File Transfer에서는 특성 및 필수 변환을 승인하므로, 두 특성 모두 설정하지 않아도 됩니다. **CipherSpec** 또는 **CipherSuite** 특성을 모두 지정하는 경우, **CipherSpec**이 사용됩니다.

PeerName 특성은 선택적입니다. 연결할 큐 관리자의 식별 이름에 특성을 설정할 수 있습니다. Managed File Transfer는 일치하지 않는 식별 이름이 있는 올바른지 않은 SSL 서버에 대한 연결을 거부합니다.

SslTrustStore 및 **SslKeyStore** 특성을 신뢰 저장소 및 키 저장소 파일을 가리키는 파일 이름으로 설정하십시오. 이미 실행 중인 에이전트의 특성을 설정하는 경우, 에이전트를 중지시키고 재시작하여 SSL 모드에서 다시 연결하십시오.

특성 파일에 일반 텍스트 비밀번호가 포함되므로 해당 파일 시스템 권한 설정을 고려하십시오.

SSL 특성에 대한 자세한 정보는 [MFT의 SSL 특성](#)을 참조하십시오.

5. 에이전트 큐 관리자가 SSL을 사용하는 경우 사용자는 에이전트 작성 시 필수 세부사항을 제공할 수 없습니다. 다음 단계를 수행하여 에이전트를 작성하십시오.
 - a) **fteCreateAgent** 명령을 사용하여 에이전트를 작성하십시오. 에이전트의 존재를 조정 큐 관리자에게 발행할 수 없음에 대한 경고가 수신됩니다.

- b) 이전 단계에서 작성된 `agent.properties` 파일을 편집하여 SSL 정보를 추가하십시오. 에이전트가 시작되면 발행이 다시 시도됩니다.
- 6. `agent.properties` 파일 또는 `coordination.properties` 파일의 SSL 특성이 변경되는 동안 IBM MQ 탐색기의 에이전트 또는 인스턴스가 실행 중인 경우 에이전트 또는 IBM MQ Explorer를 재시작해야 합니다.

관련 참조

[MFTagent.properties 파일](#)

채널 인증으로 클라이언트 모드의 큐 관리자에 연결

IBM WebSphere MQ 7.1에서는 채널 레벨에서 더 정확하게 액세스를 제어하기 위해 채널 인증 레코드를 도입했습니다. 이와 같은 작동 변경은 기본적으로 새로 작성된 IBM WebSphere MQ 7.1 이상 큐 관리자가 Managed File Transfer 컴포넌트의 클라이언트 연결을 거부함을 의미합니다.

채널 인증에 대한 자세한 정보는 43 페이지의 『[채널 인증 레코드](#)』의 내용을 참조하십시오.

Managed File Transfer에서 사용한 SVRCONN에 대한 채널 인증 구성이 권한 없는 MCAUSER ID를 지정하는 경우, Managed File Transfer Agent 및 명령이 올바르게 작동할 수 있도록 큐 관리자, 큐 및 토픽에 대한 특정 권한 레코드를 부여해야 합니다. MQSC 명령 `SET CHLAUTH` 또는 PCF 명령 [채널 인증 레코드 설정](#)을 사용하여 채널 인증 레코드를 작성, 수정 또는 제거하십시오. IBM WebSphere MQ 7.1 또는 이후 큐 관리자에 연결하려는 모든 Managed File Transfer 에이전트의 경우, 모든 에이전트에 사용할 MCAUSER ID를 설정하거나 각 에이전트에 대해 별도의 MCAUSER ID를 설정할 수 있습니다.

각 MCAUSER ID에 다음 권한을 부여하십시오.

- 큐 관리자에 필요한 권한 레코드
 - connect
 - setid
 - inq
- 큐에 필요한 권한 레코드.

모든 에이전트 특정 큐(다음 목록에서 `agent_name`으로 끝나는 큐 이름)의 경우, 클라이언트 연결을 사용하여 IBM WebSphere MQ 7.1 이상 큐 관리자에 연결하려는 각 에이전트에 대해 해당 큐 권한 레코드를 작성해야 합니다.

- put, get, dsp(SYSTEM.DEFAULT.MODEL.QUEUE)
- put, get, setid, browse(SYSTEM.FTE.COMMAND.agent_name)
- put, get(SYSTEM.FTE.DATA.agent_name)
- put, get(SYSTEM.FTE.REPLY.agent_name)
- put, get, inq, browse(SYSTEM.FTE.STATE.agent_name)
- put, get, browse(SYSTEM.FTE.EVENT.agent_name)
- put, get(SYSTEM.FTE)
- 토픽에 필요한 권한 레코드.
 - sub, pub(SYSTEM.FTE)
- 파일 전송에 필요한 권한 레코드.

소스 및 대상 에이전트에 대해 개별 MCAUSER ID가 있는 경우 소스 및 대상 둘 다의 에이전트 큐에서 권한 레코드를 작성하십시오.

예를 들어, 소스 에이전트의 MCAUSER ID가 `user1`이고 대상 에이전트 MCAUSER ID가 `user2`인 경우 에이전트 사용자에게 다음 권한을 설정하십시오.

에이전트 사용자	큐	필요한 권한
user1	SYSTEM.FTE.DATA.destination_agent_name	put

에이전트 사용자	큐	필요한 권한
user1	SYSTEM.FTE.COMMAND.destination_agent_name	put
user2	SYSTEM.FTE.REPLY.source_agent_name	put
user2	SYSTEM.FTE.COMMAND.source_agent_name	put

Connect:Direct 브릿지 에이전트와 Connect:Direct 노드 사이에서 SSL 또는 TLS 구성

Connect:Direct 브릿지 에이전트 특성 파일에서 특성을 설정하고 키 저장소와 신뢰 저장소를 작성하여 SSL 프로토콜을 통해 서로 연결하도록 Connect:Direct 브릿지 에이전트와 Connect:Direct 노드를 구성하십시오.

이 태스크 정보

이러한 단계에는 인증 기관에서 서명한 키를 가져오기 위한 지시사항이 포함되어 있습니다. 인증 기관을 사용하지 않는 경우 자체 서명된 인증서를 생성할 수 있습니다. 자체 서명된 인증서 생성에 대한 자세한 정보는 [255 페이지](#)의 『UNIX, Linux, and Windows에서 SSL/TLS에 대한 작업』의 내용을 참조하십시오.

이러한 단계에는 Connect:Direct 브릿지 에이전트의 새 키 저장소 및 신뢰 저장소 작성에 대한 지시사항이 포함되어 있습니다. Connect:Direct 브릿지 에이전트에 IBM MQ 큐 관리자에 안전하게 연결하는 데 사용하는 키 저장소와 신뢰 저장소가 이미 있는 경우 Connect:Direct 노드에 안전하게 연결할 때 기존 키 저장소와 신뢰 저장소를 사용할 수 있습니다. 자세한 정보는 [498 페이지](#)의 『MFT의 SSL 또는 TLS 암호화 구성』의 내용을 참조하십시오.

프로시저

Connect:Direct 노드의 경우 다음 단계를 완료하십시오.

1. Connect:Direct 노드에 대해 서명된 인증서와 키를 생성하십시오.
IBM MQ와 함께 제공되는 IBM 키 관리 도구를 사용하여 이를 수행할 수 있습니다. 추가 정보는 [244 페이지](#)의 『SSL/TLS에 대한 작업』의 내용을 참조하십시오.
2. 서명된 키를 가지려면 인증 기관에 요청을 송신하십시오. 그러면 인증서를 받습니다.
3. 인증 기관의 공개 키를 포함하는 텍스트 파일을 작성하십시오(예: /test/ssl/certs/CAcert).
4. Connect:Direct 노드에서 Secure+ Option을 설치하십시오.
노드가 이미 있는 경우 설치 프로그램을 다시 실행하고 기존 설치의 위치를 지정하고 Secure+ Option만 설치하도록 선택하여 Secure+ Option을 설치할 수 있습니다.
5. 새 텍스트 파일을 작성하십시오(예: /test/ssl/cd/keyCertFile/node_name.txt).
6. 인증 기관에서 받은 인증서 및 /test/ssl/cd/privateKeys/node_name.key에 있는 개인 키를 텍스트 파일로 복사하십시오.

/test/ssl/cd/keyCertFile/node_name.txt의 콘텐츠는 다음 형식이어야 합니다.

```
-----BEGIN CERTIFICATE-----
MIIcCzCCAgigAwIBAgIBGjANBgkqhkiG9w0BAQUFADBEMQswCQYDVQQGEwJHqjES
MBAGA1UECBMJSjGFtcHNoaXJlMRAwDgYDVQOHEwdIdXJzbGV5MQwwCgYDVQKEwNJ
Qk0xOjAMBGNVBAStBU1RSVBUMQswCQYDVQQDEwJDDQTAeFw0xMTAzMDExNjIwNDZa
Fw0yMTAyMjYxNjIwNDZaMFAXCzAJBgNVBAYTAkdCMRlEAYDVQQIEw1IYyW1wc2hp
cmUxDDAKBgNVBAoTA01CTTEOMAwGA1UECxMFTVFGVUxZzANBgNVBAMTBmJpbmJh
ZzCBnzANBgkqhkiG9w0BAQEFAA0BjQAwgYkCgYEAvgP1QIk1U9ypSKD1Xo0Do1yk
EyMFXB0UpZr1DVxjoSEC0vtWncJ199e+Vc4UpNybdyBu+Nkd1MNOF40xeQcLAFj
WnhakqCiQ+JIAD5AurhnrwChe0MV3kjA84GKH/r0SVqt1984mu/1DyS819XcfSSn
c00MsK1KbneVSCIV2XECaWEAAa7MHkwcQYDVR0TBAlwADAsBg1ghkgBhvhCAQ0E
HxYdT3B1b1NTTCBHZW51cmF0ZWQgQ2VydG1maWNhdGUwHQYDVR00BBYEFNXXIpSc
csBXUniW4A3UrzNCRsv3MB8GA1UdIwQYMBaAFDXY8rmj41Vz5+FVAoQb++cns+B4
MA0GCSqGSIb3DQEBBQUAA4GBAFc7k1Xa4pGKYgwhcxKpE3ZF6FNWY4vBXS216/ja
8h/v18+iv010CL8t0ZOKSU95fyZLz0PKnCH7v+ItFSE3CIIEk9D1z2U6W091ICwn
17PL72Tdfal3kabwHYVf17IVcuL+VZsZ3HjLggP2qH09ZuJPspeT9+AxFVMLiaAb
8eHw
-----END CERTIFICATE-----
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4, ENCRYPTED
```

```
DEK-Info: DES-EDE3-CBC,64A02DA15B6B6EF9
```

```
57kqxL0J/gRU0IQ6hVK2YN13B4E1jAi1gSme0I5ZpEIG8CHXISKB7/0cke2FTqsV
lvI99QyCxsDwoMnt5fj51v7aPmVeS60b0m+UlGre8B/Ze18JVj204K2Uh72rDCXE
5e6eFxsDUM207sQDy20euBVELJtM2k0kL1R0doQQS1U3XQNgJw/t3ZIx5hPXWEQT
rjRQ064BEhb+PzzxPF8uwzZ9IrkUK9BJ/UUnqC6OdBR87IeA4pnJD1Jvb2ML7EN9Z
5Y+50hTKI80GvBvWX04fHyvIX5aslwhBoArXIS1AtNtrptPvoaP1zyIAeZ60Cvo/
Sfo+A2UhmTEJe0JaZG2XZ3H495fAw/EHmjehzIACwukQ9nSIETgu4A1+CV64RJED
aYBCM8UjaAkBZDH5gn7+eBov0ssXAXWdyJBVhU0jXjvAj/e1h+kcSF1hax5D//AI
66nRMZzboSxNqkjcVd8wfdWp+bEjDzUaaarJTS71IFeLlw7eJ8MNAkMGicDkycL0
EPBU9X5QnHKLK0fYHN/1WgUk8qt3UytFXXfzTXGF3EbsWbBupkT5e5+1YcX80VZ6
sHFPN1HluCny/riUcBy9iviVeodX8Iom0chSy05DK18bwZNjYtUP+CtYHNFU5BaD
I+1uU0AeJ+wjQYKT1WaeIGZ3VxuNITJul8y5qDTXXfX7vxM50owXa6U5+AYuGUMg
/itPZmUmNrhjTk7ghT6i1IQ0aBowXXKJB1Mmq/6BQXN2IhkD9ys2qrvM1hdi5nAf
egmdiG50l0LnBRqWbfr+DykpAhK4SaDi2F52Uxovw3Lhwi8dQP7lzQ==
-----END RSA PRIVATE KEY-----
```

7. Secure+ Admin 도구를 시작하십시오.

- Linux 또는 UNIX 시스템에서 **spadmin.sh** 명령을 실행하십시오.
- Windows 시스템에서 시작 > 프로그램 > **Sterling Commerce Connect:Direct > CD Secure+ Admin** 도구를 클릭하십시오.

CD Secure+ Admin 도구를 시작합니다.

8. CD Secure+ Admin 도구에서 **.Local** 행을 두 번 클릭하여 기본 SSL 또는 TLS 설정을 편집하십시오.

- a) 사용 중인 프로토콜에 따라 **Enable SSL Protocol** 또는 **Enable TLS Protocol**을 선택하십시오.
- b) **대체 사용 불가능**을 선택하십시오.
- c) 최소 하나의 암호 스위트를 선택하십시오.
- d) 양방향 인증을 원하는 경우 **Enable Client Authentication**의 값을 Yes로 변경하십시오.
- e) **Trusted Root Certificate** 필드에 인증 기관의 공용 인증서 파일에 대한 경로(/test/ssl/certs/CAcert)를 입력하십시오.
- f) **Key Certificate File** 필드에 사용자가 작성한 파일의 경로(/test/ssl/cd/keyCertFile/node_name.txt)를 입력하십시오.

9. **.Client** 행을 두 번 클릭하여 기본 SSL 또는 TLS 설정을 편집하십시오.

- a) 사용 중인 프로토콜에 따라 **Enable SSL Protocol** 또는 **Enable TLS Protocol**을 선택하십시오.
- b) **대체 사용 불가능**을 선택하십시오.

Connect:Direct 브릿지 에이전트의 경우 다음 단계를 수행하십시오.

10. 신뢰 저장소를 작성하십시오. 더미 키를 작성한 후 더미 키를 삭제하여 이를 수행할 수 있습니다. 다음 명령을 사용할 수 있습니다.

```
keytool -genkey -alias dummy -keystore /test/ssl/fte/stores/truststore.jks
```

```
keytool -delete -alias dummy -keystore /test/ssl/fte/stores/truststore.jks
```

11. 인증 기관의 공용 인증서를 신뢰 저장소로 가져오십시오.

다음 명령을 사용할 수 있습니다.

```
keytool -import -trustcacerts -alias myCA
-file /test/ssl/certs/CAcert
-keystore /test/ssl/fte/stores/truststore.jks
```

12. Connect:Direct 브릿지 에이전트 특성 파일을 편집하십시오.

파일에 다음 행을 포함시키십시오.

```
cdNodeProtocol=protocol
cdNodeTruststore=/test/ssl/fte/stores/truststore.jks
cdNodeTruststorePassword=password
```


이 단계의 예에서 *protocol*은 사용 중인 프로토콜(SSL 또는 TLS)이며 *password*는 신뢰 저장소를 작성할 때 지정한 비밀번호입니다.

13. 양방향 인증을 원하는 경우 Connect:Direct 브릿지 에이전트의 키와 인증서를 작성하십시오.

a) 키 저장소와 키를 작성하십시오.

다음 명령을 사용할 수 있습니다.

```
keytool -genkey -keyalg RSA -alias agent_name
        -keystore /test/ssl/fte/stores/keystore.jks
        -storepass password -validity 365
```

b) 서명 요청을 생성하십시오.

다음 명령을 사용할 수 있습니다.

```
keytool -certreq -v -alias agent_name
        -keystore /test/ssl/fte/stores/keystore.jks -storepass password
        -file /test/ssl/fte/requests/agent_name.request
```

c) 선행 단계에서 수신하는 인증서를 키 저장소로 가져오십시오. 인증서는 x.509 형식이어야 합니다.

다음 명령을 사용할 수 있습니다.

```
keytool -import -keystore /test/ssl/fte/stores/keystore.jks
        -storepass password -file certificate_file_path
```

d) Connect:Direct 브릿지 에이전트 특성 파일을 편집하십시오.

파일에 다음 행을 포함시키십시오.

```
cdNodeKeystore=/test/ssl/fte/stores/keystore.jks
cdNodeKeystorePassword=password
```

이 단계의 예에서 *password*는 키 저장소를 작성할 때 지정한 비밀번호입니다.

관련 태스크

Connect:Direct 브릿지 구성

ULW AMQP 클라이언트 보안 설정

일정 범위의 보안 메커니즘을 사용하여 AMQP 클라이언트에서의 연결에 대해 보안을 설정하고 데이터가 네트워크에서 안전하게 보호되도록 할 수 있습니다. MQ Light 애플리케이션에 보안을 빌드할 수 있습니다. 또한 기능이 다른 애플리케이션에 사용되는 것과 동일한 방식으로 AMQP 클라이언트에서 IBM MQ의 기존 보안 기능을 사용할 수도 있습니다.

채널 인증 규칙(CHLAUTH)

채널 인증 규칙을 사용하여 큐 관리자에 대한 TCP 연결을 제한할 수 있습니다. AMQP 채널은 사용자 큐 관리자에 대해 구성되는 채널 인증 규칙 사용을 지원합니다. 사용자 큐 관리자에서 AMQP 채널과 일치하는 프로파일로 채널 인증 규칙이 정의되면 이러한 규칙은 해당 채널에 적용됩니다. 기본적으로 채널 인증은 새 IBM® MQ 큐 관리자에서 사용으로 설정되므로 AMQP 채널을 사용하기 전에 일부 구성을 완료해야 합니다.

AMQP가 사용자 큐 관리자에 연결할 수 있도록 채널 인증 규칙 구성 방법에 대한 자세한 정보는 [AMQP 채널 작성 및 사용](#)을 참조하십시오.

연결 인증(CONNAUTH)

연결 인증을 사용하여 큐 관리자에 대한 연결을 인증할 수 있습니다. AMQP 채널은 AMQP 애플리케이션에서 큐 관리자에 대한 액세스를 제어하기 위한 연결 인증 사용을 지원합니다.

AMQP 프로토콜은 SASL(Simple Authentication and Security Layer) 프레임워크를 사용하여 연결 인증 방법을 지정합니다. 여기에는 다양한 SASL 메커니즘이 있고 IBM MQ는 두 가지 SASL 메커니즘(ANONYMOUS 및 PLAIN)을 지원합니다.

ANONYMOUS의 경우 인증을 위해 클라이언트에서 큐 관리자 신임 정보가 전달되지 않습니다. CONNAUTH 속성에서 지정되는 MQ AUTHINFO 오브젝트의 CHCKCLNT 값이 REQUIRED 또는 REQDADM(관리자로서 연결되는 경우)인 경우, 연결은 거부됩니다. CHCKCLNT 값이 NONE 또는 OPTIONAL인 경우 연결은 허용됩니다.

PLAIN의 경우 인증을 위해 클라이언트에서 큐 관리자에게 사용자 이름 및 비밀번호가 전달됩니다. CONNAUTH 속성에서 지정되는 MQ AUTHINFO 오브젝트의 CHCKCLNT 값이 NONE이면 연결은 거부됩니다. CHCKCLNT 값이 OPTIONAL, REQUIRED 또는 REQDADM(관리자로서 연결되는 경우)인 경우, 큐 관리자는 사용자 이름 및 비밀번호를 검사합니다. 큐 관리자는 운영 체제(AUTHINFO 오브젝트가 IDPWOS 유형인 경우) 또는 LDAP 저장소(AUTHINFO 오브젝트가 IDPWLDPAP 유형인 경우)를 검사합니다.

다음 테이블은 이 인증 작동을 요약한 것입니다.

표 95. SASL 메커니즘 및 연결 인증 요약		
SASL 메커니즘	클라이언트에서 큐 관리자 신임 정보 전달 여부	CHCKCLNT 값
ANONYMOUS	아니오	REQUIRED 또는 REQDADM - 연결 거부됨 NONE 또는 OPTIONAL - 연결 허용됨
PLAIN	예, 사용자 이름 및 비밀번호	REQUIRED, REQDADM 또는 OPTIONAL - 큐 관리자가 사용자 이름 및 비밀번호를 검사함 NONE - 연결이 거부됨

MQ Light 클라이언트를 사용 중인 경우 연결하는 AMQP 주소에 이를 포함시켜 신임 정보를 지정할 수 있습니다.
예:

```
amqp://mwhitehead:mYp4ssw0rd@localhost:5672/sports/football
```

채널에서의 MCAUSER 설정

AMQP 채널에는 MCAUSER 속성이 있고, 이는 해당 채널에 대한 모든 연결에 권한을 부여하는 IBM MQ 사용자 ID를 설정할 때 사용할 수 있습니다. AMQP 클라이언트에서 해당 채널로의 모든 연결에서는 사용자가 구성된 MCAUSER ID를 채택합니다. 해당 사용자 ID는 다른 토픽에 대한 메시징의 권한 부여에 사용됩니다.

큐 관리자에 대한 연결의 보안을 설정하려면 채널 인증(CHLAUTH)을 사용하도록 권장합니다. 채널 인증을 사용 중인 경우 MCAUSER 값을 권한이 없는 사용자로 구성하도록 권장합니다. 그러면 채널 연결이 CHLAUTH 규칙에 일치하지 않는 경우 연결에는 큐 관리자에서 메시징을 수행할 권한이 부여되지 않습니다.

참고: **Windows** Windows의 경우 IBM MQ 9.1.1 이전에는 MCAUSER 사용자 ID 설정이 길이가 최대 12자인 사용자 ID에 대해서만 지원됩니다.

V 9.1.1 IBM MQ 9.1.1부터, 12자 제한이 제거됩니다.

SSL/TLS 지원

AMQP 채널은 사용자 큐 관리자에서 구성된 키 저장소에서 키를 사용한 SSL/TLS 암호화를 지원합니다. SSL/TLS 암호화를 위한 AMQP 채널 구성 옵션에서는 다른 MQ 채널 유형과 동일한 옵션을 지원합니다. 암호 스펙 및 큐 관리자에게 AMQP 클라이언트 연결에서의 인증서가 필요한지 여부를 지정할 수 있습니다.

큐 관리자의 FIPS 속성을 사용하면 SSL/TLS 암호 스위트를 제어할 수 있고, 이는 AMQP 클라이언트로부터의 연결에 대한 보안을 설정할 때 사용할 수 있습니다.

큐 관리자의 키 저장소 설정 방법에 대한 정보는 [UNIX, Linux 및 Windows 시스템에서의 SSL 또는 TLS에 대한 작업을 참조하십시오.](#)

AMQP 클라이언트 연결에 대한 SSL/TLS 지원 구성 방법에 대한 정보는 [AMQP 채널 작성 및 사용을 참조하십시오.](#)

JAAS(Java Authentication and Authorization Service)

선택적으로 JAAS 로그인 모듈이 있는 AMQP 채널을 구성할 수 있습니다. 이는 AMQP 클라이언트가 제공하는 사용자 이름 및 비밀번호를 확인할 수 있습니다. [505 페이지의 『AMQP 채널용 JAAS 구성』](#)의 내용을 참조하십시오.

관련 태스크

[AMQP 클라이언트 애플리케이션 개발](#)

[AMQP 채널 작성 및 사용](#)

ULW AMQP 클라이언트 인계 제한

AMQP 클라이언트 연결이 기존 AMQP 클라이언트 연결과 동일한 클라이언트 ID를 갖도록 하는 경우, 기본적으로 기존 클라이언트의 연결이 끊어집니다. 그러나 특정 조건을 충족할 때에만 인계가 가능하도록 클라이언트 인계 작동을 제한하는 큐 관리자를 구성할 수 있습니다.

예를 들어 기존 클라이언트의 연결을 끊는 것은 다른 팀에서 개발 중인 AMQP 애플리케이션이 있고 여기에서 동일한 클라이언트 ID를 사용하는 경우 적절하지 않습니다. 이 문제를 해결하기 위해 사용 중인 AMQP 채널의 이름, 클라이언트의 IP 주소 및 클라이언트 사용자 ID(SASL 인증이 사용되는 경우)를 기반으로 클라이언트 인계를 제한할 수 있습니다.

다음 테이블에서 자세히 설명한 대로 큐 관리자 속성 **AdoptNewMCA** 및 **AdoptNewMCACheck**의 설정을 사용하여 클라이언트 인계 제한의 필수 레벨을 지정하십시오.

표 96. 클라이언트 인계를 제한하는 AdoptNewMCA 및 AdoptNewMCACheck 설정		
AdoptNewMCA	AdoptNewMCACheck	클라이언트 인계가 허용되기 전 검사하는 기준
NO 또는 정의되지 않음	적용할 수 없음	없음 인증되고 모든 CHLAUTH 규칙을 통과한 모든 클라이언트 연결에 대해 클라이언트 인계가 허용됩니다.
ALL(또는 NO 이외의 값)	QM 또는 정의되지 않음	없음 인증되고 모든 CHLAUTH 규칙을 통과한 모든 클라이언트 연결에 대해 클라이언트 인계가 허용됩니다.
ALL(또는 NO 이외의 값)	이름	사용자 ID(SASL이 사용되는 경우) 채널 이름
ALL(또는 NO 이외의 값)	ADDRESS	사용자 ID(SASL이 사용되는 경우) IP 주소
ALL(또는 NO 이외의 값)	모두	사용자 ID(SASL이 사용되는 경우) 채널 이름 IP 주소

큐 관리자 속성 **AdoptNewMCA** 및 **AdoptNewMCACheck**는 CHANNELS 스탠자에 정의되는 큐 관리자 구성의 일부입니다. On IBM MQ for Windows and IBM MQ for Linux x86-64 systems, modify configuration

information using the IBM MQ Explorer. 기타 시스템에서는 `qm.ini` 구성 파일을 편집하여 정보를 수정하십시오. 큐 관리자 채널 정보를 수정하는 방법에 대한 정보는 [채널의 속성을 참조하십시오](#).

관련 태스크

[AMQP 클라이언트 애플리케이션 개발](#)

[AMQP 채널 작성 및 사용](#)

ULW AMQP 채널용 JAAS 구성

JAAS(Java Authentication and Authorization Service) 사용자 정의 모듈은 연결할 때 AMQP 클라이언트가 AMQP 채널에 전달하는 사용자 이름 및 비밀번호 신임 정보를 인증할 때 사용할 수 있습니다.

이 태스크 정보

기타 Java 기반의 시스템에서 인증에 JAAS 모듈을 이미 사용하고 있고 MQ에 대한 AMQP 연결의 인증에 해당 모듈을 다시 사용하려는 경우 사용자 정의 JAAS 모듈을 사용하려 합니다. 또는 MQ에 빌드된 인증 기능이 사용하려는 인증 메커니즘을 지원하지 않는 경우 사용자 정의 JAAS 모듈을 작성하려 할 수 있습니다.



AMQP 채널에 대한 JAAS 모듈 구성은 큐 관리자 레벨에서 수행됩니다. 이는 큐 관리자에 대한 AMQP 연결 인증에 JAAS 모듈이 구성되는 경우, 모듈은 모든 AMQP 채널에 적용됩니다. JAAS 모듈을 호출한 채널의 이름은 모듈로 전달되어 사용자가 다른 채널을 위해 다른 JAAS 로그를 코딩할 수 있습니다.

다음과 같은 다른 정보도 JAAS 모듈로 전달됩니다.

- 인증을 시도하는 AMQP 클라이언트의 클라이언트 ID.
- AMQP 클라이언트의 네트워크 주소.
- JAAS 모듈을 호출한 채널의 이름.

프로시저

다음 단계를 완료하여 AMQP 채널의 JAAS 구성 모듈을 구성합니다.

1. 하나 이상의 JAAS 모듈 구성 스탠자를 포함하는 `jaas.config` 파일을 정의하십시오. 스탠자는 `javax.security.auth.spi.LoginModule` 인터페이스를 구현하는 Java 클래스의 완전한 이름을 지정해야 합니다.
 - 기본 `jaas.config` 파일은 제품과 함께 제공되며 `QM_data_directory/amqp/jaas.config`에 있습니다.
 - 사전 구성된 `MQXRConfig` 스탠자는 이미 기본 `jaas.config` 파일에 정의되어 있습니다.
2. AMQP 채널에 사용할 스탠자의 이름을 지정하십시오.
 -  `amqp_unix.properties` 파일에 특성을 추가하십시오.
 -  `amqp_win.properties` 파일에 특성을 추가하십시오.

특성의 양식은 다음과 같습니다.

```
com.ibm.mq.MQXR.JAASConfig=JAAS_stanza_name
```

for example:

```
com.ibm.mq.MQXR.JAASConfig=MQXRConfig
```

3. 사용자 정의 모듈의 클래스를 포함하도록 큐 관리자 환경을 구성하십시오. AMQP 서비스에는 JAAS 구성 스탠자에서 구성되는 Java 클래스에 대한 액세스가 있어야 합니다.

JAAS 클래스에 대한 경로를 MQ `service.env` 파일에 추가하여 이를 수행합니다. MQ 구성 디렉토리 (`MQ_config_directory`) 또는 큐 관리자 구성 디렉토리 (`QM_config_directory`)에 있는 `service.env` 파일을 편집하여 `CLASSPATH` 변수를 JAAS 모듈 클래스의 위치로 설정하십시오.

다음에 수행할 작업

샘플 JAAS 로그인 모듈은 제품과 함께 `mq_installation_directory/amqp/samples` 디렉토리에 제공됩니다. 샘플 JAAS 로그인 모듈은 클라이언트가 연결하는 사용자 이름 또는 비밀번호에 관계없이 모든 클라이언트 연결을 인증합니다.

사용자는 샘플의 소스 코드를 수정하고 이를 다시 컴파일하여 특정 비밀번호를 갖는 특정 사용자만 인증하도록 시도할 수 있습니다. 제품에서 제공하는 샘플 JAAS 로그인 모듈을 사용하도록 UNIX 시스템에서 AMQP 채널을 구성하려면 다음을 수행하십시오.

1. `/var/mqm/qmgrs/QMNAME/amqp/amqp_unix.properties` 파일을 편집하고 특성 `com.ibm.mq.MQXR.JAASConfig=MQXRConfig`를 설정하십시오.
2. `/var/mqm/service.env` 파일을 편집하고 `CLASSPATH=mq_installation_location/amqp/samples` 특성을 설정하십시오.

`jaas.config` 파일에는 샘플 클래스 `samples.JAASLoginModule` 를 로그인 모듈 클래스로 지정하는 `MQXRConfig` 스탠자가 이미 포함되어 있습니다. 샘플 모듈을 시도하기 전에 `jaas.config`를 변경할 필요는 없습니다.

관련 태스크

[AMQP 클라이언트 애플리케이션 개발](#)

[AMQP 채널 작성 및 사용](#)

Advanced Message Security

Advanced Message Security(AMS)는 엔드 애플리케이션에 영향을 미치지 않으면서 IBM MQ 네트워크를 통해 플로우는 민감한 데이터에 대한 높은 레벨의 보호를 제공하는 IBM MQ의 컴포넌트입니다.

Advanced Message Security의 개요

IBM MQ 애플리케이션은 가치가 높은 금융 거래 및 개인 정보 등과 같은 민감한 데이터를 공개 키 암호화 모델을 사용하여 서로 다른 보호 레벨을 사용하여 전송하기 위해 Advanced Message Security를 사용할 수 있습니다.



관련 참조

[GSKit는 AMS 메시지에 사용된 코드를 리턴합니다.](#)

Advanced Message Security의 기능 및 특징

Advanced Message Security는 메시지 레벨에서 데이터 서명 및 암호화를 제공하기 위해 IBM MQ 보안 서비스를 확장합니다. 확장된 서비스는 메시지 데이터가 원래 큐에 놓인 때와 검색된 때 사이에 수정되지 않았음을 보장합니다. 또한, AMS는 메시지 데이터 송신자가 서명된 메시지를 대상 큐에 배치할 권한이 있는지 확인합니다.

AMS는 다음 기능을 제공합니다.

- IBM MQ가 처리하는 민감하거나 가치가 높은 트랜잭션을 보안합니다.
- 악하거나 권한 없는 메시지가 수신 애플리케이션에 의해 처리되기 전에 감지하고 제거합니다.
- 메시지가 큐에서 큐로 이동 중에 수정되지 않았는지 확인합니다.
- 데이터가 네트워크 전체에 걸쳐 흐를 때뿐만 아니라 큐에 놓일 때에도 보호합니다.
- IBM MQ에 대한 기존 독점 및 고객 작성 애플리케이션의 보안을 설정합니다.
-  IBM MQ 9.1.3부터 IBM MQ for z/OS는 네트워크를 통해 전달되는 메시지서 AMS 보호를 선택적으로 제거 및 추가하는 기능을 제공합니다. 이 기능을 서버 대 서버 메시지 채널 에이전트 (MCA) 인터셉션이라고 합니다.
-  IBM MQ 9.1.4 및 IBM MQ 9.1.0 Fix Pack 4부터는 IBM MQ 라이 브러리 코드에 고객의 애플리케이션 프로그램에서 실행되는 검사가 추가되었습니다. 이 검사는 환경 변수 `AMQ_AMS_FIPS_OFF`의 값을 읽어들이기 위해 해당 초기화의 초반에 실행되며 임의의 값으로 설정된 경우 해당 애플리케이션에서 GSKit 코드가 비FIPS 모드로 실행됩니다.

AMS에서 사용 가능한 QoP(Quality of Protection)

Advanced Message Security, Integrity, Privacy 및 Confidentiality에 대한 보호 품질은 세 가지가 있습니다.

Integrity 보호는 디지털 서명을 통해 제공되며, 이 서명을 통해 메시지를 작성한 사용자 및 메시지가 변경되거나 변경되지 않았는지 보증합니다.

Privacy 보호는 디지털 서명 및 암호화의 조합으로 제공됩니다. 암호화는 의도된 하나 이상의 수신인만 메시지 데이터를 볼 수 있도록 보장합니다. 권한이 없는 수신인이 암호화된 메시지 데이터의 사본을 확보해도 실제 메시지 데이터를 볼 수 없습니다.

Confidentiality 보호는 선택적 키 재사용으로만 암호화를 통해 제공됩니다.

성능에 미치는 효과

AMS는 대칭 및 비대칭 암호화 루틴의 조합을 사용하여 디지털 서명 및 암호화를 제공합니다. 대칭 키 조작은 비대칭 키 조작에 비해 매우 빠릅니다. 비대칭 키 조작은 CPU 집중적이기 때문에 AMS에서 많은 수의 메시지를 보호하는 비용에 큰 영향을 미칠 수 있습니다.

비대칭 암호화 루틴

예를 들어, 서명된 메시지를 넣으면 비대칭 키 조작을 사용하여 메시지 해시에 서명합니다.

서명된 메시지를 가져올 때 서명된 해시를 확인하기 위해 추가적인 비대칭 키 조작을 사용합니다.

따라서 메시지당 메시지 데이터에 서명하고 이를 확인하기 위해 적어도 두 개의 비대칭 키 조작이 필요합니다.

비대칭 및 대칭 암호화 루틴

암호화된 메시지를 넣을 때 대칭 키가 생성되고 의도된 각 메시지 수신인에 대해 비대칭 키 조작을 사용하여 해당 대칭 키를 암호화합니다.

그러면 대칭 키를 사용하여 메시지 데이터가 암호화됩니다. 암호화된 메시지를 가져올 때 의도된 수신인은 메시지에서 사용할 대칭 키를 검색하기 위해 비대칭 키 조작을 사용해야 합니다.

따라서 세 가지 QoP(Quality of Protection)는 모두 CPU 집중적인 비대칭 키 조작의 여러 요소를 포함하여, 이로 인해 메시지를 넣고 가져오는 애플리케이션에서 도달 가능한 최대 메시징 비율에 큰 영향을 줍니다.

그러나 **Confidentiality** 정책은 일련의 메시지에 대해 대칭 키 재사용을 허용합니다. 대칭 키 재사용을 통해 **Confidentiality** 정책을 사용하여 CPU 비용을 크게 절감할 수 있습니다. 이 조작 모드에서는 PKCS#7 형식을 사용하여 대칭 암호화 키를 공유합니다. 하지만 디지털 서명이 없으며, 이로 인해 메시지별 비대칭 키 조작의 일부가 제거됩니다. 대칭 키는 여전히 수신인마다 비대칭 키 조작을 사용하여 암호화되어야 하지만 선택적으로 동일 수신인을 대상으로 하는 여러 메시지에 반복적으로 재사용될 수 있습니다. 키 재사용이 정책에서 허용되면 첫 번째 메시지에만 비대칭 키 조작이 필요합니다. 후속 메시지는 대칭 키 조작만 사용해야 합니다.

키 재사용


Confidentiality 정책을 사용하면 대칭 키 재사용 접근법을 사용하여 동일한 큐에 넣고 동일한 수신인 또는 수신인을 대상으로 하는 여러 메시지를 암호화하는 데 소요되는 비용을 크게 줄일 수 있습니다.

예를 들어, 동일한 수신인에 10개의 암호화된 메시지를 넣는 경우 대칭 키가 생성되고 의도된 각 메시지 수신인에 대해 비대칭 키 조작을 사용하여 첫 번째 메시지에 대해 암호화됩니다.

정책에서 제어하는 한계에 기반하여 암호화된 대칭 키는 동일한 수신인에 대해 의도된 후속 메시지에서 재사용할 수 있습니다. 암호화된 메시지를 가져오는 애플리케이션은 대칭 키가 변경되지 않아서 대칭 키를 검색하는 비용이 들지 않는 경우 애플리케이션에서 감지할 수 있는 동일한 최적화를 적용할 수 있습니다.

이 예에서 비대칭 키 조작의 90%는 동일한 키를 재사용하여 메시지를 넣고 가져오는 애플리케이션 모두에서 피할 수 있습니다.

키 재사용 방법에 대한 추가적인 정보는 다음을 참조하십시오.

- MQSC 명령 [SET POLICY](#)
- 제어 명령 [setmqspl](#)
-  IBM i 명령 [SETMQMSPL](#)

AMS의 키 개념

도구가 작동하는 방법 및 이를 효율적으로 사용하는 방법을 이해하려면 Advanced Message Security에서 키 개념에 대해 배우십시오.

PKI(Public Key Infrastructure) 및 Advanced Message Security

PKI(Public Key Infrastructure)는 안전한 통신을 확보하기 위해 공개 키 암호화의 사용을 지원하는 기능, 정책 및 서비스의 시스템입니다.

PKI(Public Key Infrastructure)의 컴포넌트를 정의하는 단일 표준은 없지만 PKI는 일반적으로 공개 키 인증서의 사용과 관련되고 다음 서비스를 제공하는 인증 기관(CA) 및 기타 등록대행 기관(RA)으로 구성됩니다.

- 디지털 인증서 발행
- 디지털 인증서 유효성 검증
- 디지털 인증서 폐기
- 인증서 분배

사용자와 애플리케이션 ID는 서명되고 암호화된 메시지와 연관된 인증서에서 **식별 이름(DN)** 필드로 표시됩니다. Advanced Message Security는 이 ID를 사용하여 사용자 또는 애플리케이션을 나타냅니다. 이 ID를 인증하기 위해 사용자 또는 애플리케이션은 인증서 및 연관된 개인 키가 저장되는 키 저장소에 대한 액세스가 있어야 합니다. 각 인증서는 키 저장소에서 레이블로 표시됩니다.

관련 개념

547 페이지의 『키 저장소 및 인증서 사용』

IBM MQ 애플리케이션에 투명한 암호 보호를 제공하기 위해 Advanced Message Security는 공개 키 인증서 및 개인 키가 저장되는 키 저장소 파일을 사용합니다. z/OS에서 SAF 키 링이 키 저장소 파일 대신에 사용됩니다.

AMS에서 디지털 인증서

Advanced Message Security는 사용자 및 애플리케이션을 X.509 표준 디지털 인증서와 연관시킵니다. X.509 인증서는 일반적으로 신뢰 인증 기관(CA)에 의해 서명되고 암호화 및 복호화에 사용되는 개인 및 공개 키와 관련됩니다.

디지털 인증서는 공개 키를 해당 소유자가 개인, 큐 관리자 또는 다른 엔티티인지 관계 없이 해당 소유자에게 바인딩하여 위장으로부터 보호를 제공합니다. 비대칭 키 설계를 사용할 때 공개키의 소유권에 대해 보장해줄 때 문에, 디지털 인증서를 공개키 인증서라고도 합니다. 이 스키마에서는 애플리케이션을 위해 공개 키 및 개인 키가 생성되어야 합니다. 공개 키로 암호화된 데이터는 해당하는 개인 키를 사용해서만 복호화될 수 있는 반면 개인 키로 암호화된 데이터는 해당하는 공개 키를 사용해서만 복호화될 수 있습니다. 개인 키는 비밀번호 보호된 키 데이터베이스 파일에 저장됩니다. 해당 소유자만이 해당하는 공개 키를 사용하여 암호화되는 메시지를 복호화하는데 사용되는 개인 키에 대한 액세스가 있습니다.

해당 소유자가 공개 키를 다른 엔티티로 직접 송신하는 경우, 메시지가 인터셉트되고 공개 키는 다른 키로 대체될 위험이 있습니다. 이는 "man-in-the-middle" 공격으로 알려져 있습니다. 해결책은 트러스트되는 Third-Party를 통해 공개키를 교환하는 것이며, 이렇게 하면 공개키가 정말로 사용자가 통신하고 있는 엔티티에 속하는지를 강력하게 보장해줍니다. 공개 키를 직접 송신하는 대신에, 신뢰되는 써드파티에게 그것을 디지털 인증서로 통합하도록 요청합니다. 디지털 인증서를 발행하는 신뢰되는 써드파티는 인증 기관(CA)이라고 불립니다.

디지털 인증서에 대한 자세한 정보는 [디지털 인증서의 내용을 참조하십시오](#).

디지털 인증서에는 엔티티에 대한 공개 키가 있고 공개 키가 그 엔티티에 속한다는 언급이 있습니다.

- 인증서가 개인 엔티티에 대한 것일 때 이는 개인 인증서 또는 사용자 인증서라고 불립니다.
- 인증서가 인증 기관에 대한 것일 때 인증서는 CA 인증서 또는 서명자 인증서라고 불립니다.

참고: Advanced Message Security는 Java 및 고유 애플리케이션 둘 모두에서 자체 서명 인증서를 지원합니다.

관련 개념

7 페이지의 『암호화』

암호화(cryptography)는 읽기 가능한 텍스트인 일반 텍스트와 읽을 수 없는 양식인 암호문 사이에서의 변환 프로세스입니다.

Multi 오브젝트 권한 관리자

멀티플랫폼에서 오브젝트 권한 관리자(OAM)는 IBM MQ 제품과 함께 제공되는 권한 서비스 컴포넌트입니다.

Advanced Message Security 엔티티에 대한 액세스는 IBM MQ 사용자 그룹 및 OAM을 통해 제어됩니다. 관리자는 명령행 인터페이스를 사용하여 필요에 따라 권한 부여를 부여하거나 취소할 수 있습니다. 서로 다른 사용자 그룹은 동일 오브젝트에 대해 서로 다른 종류의 액세스 권한을 가질 수 있습니다. 예를 들어, 한 그룹은 특정 큐에 대해 PUT 및 GET 조작 둘 모두를 수행할 수 있는 반면 다른 그룹은 큐를 찾아보기만이 허용될 수도 있습니다. 마찬가지로, 일부 그룹에는 큐에 대한 GET 및 PUT 권한이 있을 수도 있지만 큐를 변경하거나 삭제는 허용되지 않습니다.

OAM을 통해 다음을 제어할 수 있습니다.

- MQI (Message Queue Interface) 를 통해 Advanced Message Security 오브젝트에 액세스합니다. 애플리케이션 프로그램이 오브젝트에 액세스하려고 시도할 때 OAM은 요청을 하는 사용자 프로파일에 요청된 조작의 권한 부여가 있는지 여부를 검사합니다. 즉, 해당 큐 및 큐의 메시지는 비인가 액세스로부터 보호될 수 있음을 의미합니다.
- PCF 및 MQSC 명령 사용 권한.

관련 개념

[오브젝트 권한 관리자](#)

[MQI\(Message Queue Interface\) 개요](#)

Advanced Message Security에 의해서 지원되는 기술

Advanced Message Security는 보안 인프라를 제공하기 위해 몇몇 기술 컴포넌트에 의존합니다.

Advanced Message Security는 다음 IBM MQ API(Application Programming Interface)를 지원합니다.

- 메시지 큐 인터페이스(MQI)
- IBM MQ Java Message Service(JMS) 1.0.2 및 1.1.
- Java용 IBM MQ 기본 클래스
- 비관리 모드에서 .Net을 위한 IBM MQ 클래스

참고: Advanced Message Security는 X.509 준수 인증 기관을 지원합니다.

AMS의 알려진 제한사항

지원되지 않거나 Advanced Message Security에 대한 제한사항이 있는 많은 IBM MQ 옵션이 있습니다.

- 다음 IBM MQ 옵션은 지원되지 않거나 제한사항이 있습니다.

발행/구독

포인트-투-포인트 모델과 비교하여 발행/구독 메시징 모델의 주요 이점 중 하나는 송신 애플리케이션과 수신 애플리케이션이 데이터 송수신을 위해 서로에 대해 알지 않아도 된다는 점입니다. 그러나 의도한 수신인 또는 권한 있는 서명자를 정의해야 하는 Advanced Message Security 정책의 사용으로 이 이점이 상쇄되었습니다. 애플리케이션은 정책으로 보호되는 알리어스 큐 정의를 통해 토픽에 발행할 수 있고, 구독 애플리케이션은 정책으로 보호된 큐에서 메시지를 가져올 수도 있습니다. 정책은 토픽 문자열에 직접 지정할 수는 없고 큐 정의에만 지정할 수 있습니다.

채널 데이터 변환

Advanced Message Security로 보호되는 메시지의 보호된 페이로드는 2진 형식을 사용하여 전송되므로, 애플리케이션 간 채널에서 데이터 변환을 수행해도 메시지 요약이 무효화되지 않습니다. 정책으로 보호된 큐에서 메시지를 검색하는 애플리케이션이 데이터 변환을 요청해야 합니다. 메시지가 성공적으로 확인 및 보호 해제되면 보호된 페이로드의 변환이 시도됩니다.

분배 목록

목록에 있는 목적지 큐 각각에 동일한 정책이 정의되어 있는 경우 메시지를 분배 목록에 넣는 애플리케이션을 보호할 때 Advanced Message Security 정책을 사용할 수 있습니다. 애플리케이션이 분배 목록을 열 때 일치하지 않은 정책이 식별될 경우 열기 조작이 실패하며 애플리케이션에 보안 오류가 리턴됩니다.

애플리케이션 메시지 세그먼트화.

정책으로 보호된 메시지의 크기는 증가하므로 애플리케이션에서 메시지의 세그먼트 경계를 정확하게 지정할 수 없습니다.

관리 모드(클라이언트 연결)에서 IBM MQ classes for .NET를 사용하는 애플리케이션

IBM MQ classes for .NET를 관리 모드(클라이언트 연결)에서 사용하는 애플리케이션은 지원되지 않습니다.

참고: MCA 인터셉션은 지원되지 않는 클라이언트가 AMS를 사용할 수 있도록 허용할 수 있습니다.

관리 모드의 .NET (XMS)용 메시지 서비스 클라이언트 애플리케이션

.NET(XMS)용 메시지 서비스 클라이언트 애플리케이션은 관리 모드에서 지원되지 않습니다.

참고: MCA 인터셉션을 사용하여 지원되지 않는 클라이언트가 AMS를 사용하도록 허용할 수 있습니다.

IMS 브릿지가 처리한 IBM MQ 큐

IMS 브릿지가 처리한 IBM MQ 큐는 지원되지 않습니다.

참고: AMS는 CICS 브릿지 큐에서 지원됩니다. CICS 브릿지 큐에서 MQPUT(암호화) 및 MQGET(복호화)에 대해 동일 사용자 ID를 사용해야 합니다.

대기 중인 Getter에 넣기

대기 중인 Getter에 넣기는 AMS 정책이 정의되어 있는 큐에 대한 Getter 애플리케이션에서는 지원되지 않습니다.

V 9.1.3 서버 대 서버 MCA 인터셉션

IBM MQ 9.1.3부터 IBM MQ for z/OS에서는 송신자, 서버, 수신자, 및 요청자 채널 유형에 대해서만 서버 대 서버 MCA 인터셉션이 지원됩니다.

- 메시지를 보호할 때 사용할 인증서가 정의되지 않았으므로, 동일한 식별 이름을 사용하는 둘 이상의 인증서를 하나의 키 저장소에 넣으면 안됩니다.
- **WMQ_PROVIDER_VERSION** 특성이 6으로 설정된 경우 AMS는 JMS에서 지원되지 않습니다.
- AMS 인터셉터는 AMQP 또는 MQTT 채널을 지원하지 않습니다.

z/OS V 9.1.3 메시지 채널에서 Advanced Message Security 인터셉션 개요

On z/OS, Advanced Message Security (AMS) interception enhances the existing offering by adding an additional option of security policy protection (SPLPROT) to sender, server, receiver, and requester channels.

현재, 은행과 통신하는 지우기 하우스의 예를 사용하여 시스템의 양쪽 모두가 AMS를 지원해야 합니다 (그림 1 참조).

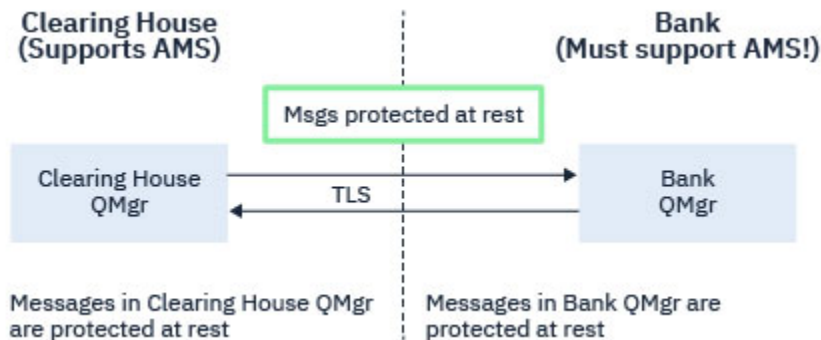


그림 32. AMS의 현재 사용

추가 옵션의 가장 큰 혜택은 엔터프라이즈에 AMS가 구성되어 있고 일부 비즈니스 파트너가 AMS를 지원하지 않는 경우, 아웃바운드 메시지에서 보호를 제거하고 AMS를 지원하지 않는 비즈니스 파트너와의 채널에서 인바운드 메시지를 보호할 수 있는 것입니다.

어음 교환소 및 은행의 예제를 사용하는 이 시나리오는 그림 2에 표시되어 있습니다. 여기에서 일부 기관에는 AMS가 있지만 다른 곳에는 없는 어음 교환소, 은행 및 비즈니스 파트너 사이의 메시지 플로우가 있습니다.

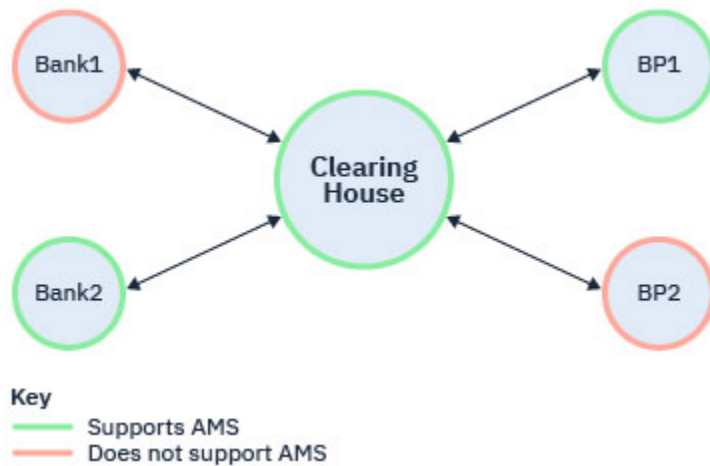


그림 33. 일부 파트너는 AMS를 지원하지만 일부는 지원하지 않음

일반적으로 채널에서는 TLS가 가능합니다.

그러나 일부 은행과 비즈니스 파트너가 AMS를 지원하지 않고 모든 은행과 비즈니스 파트너 사이에서 메시지를 교환할 수 있어야 하는 요구사항이 있을 수 있습니다. 이 시나리오는 그림 3에서 표시되어 있습니다.

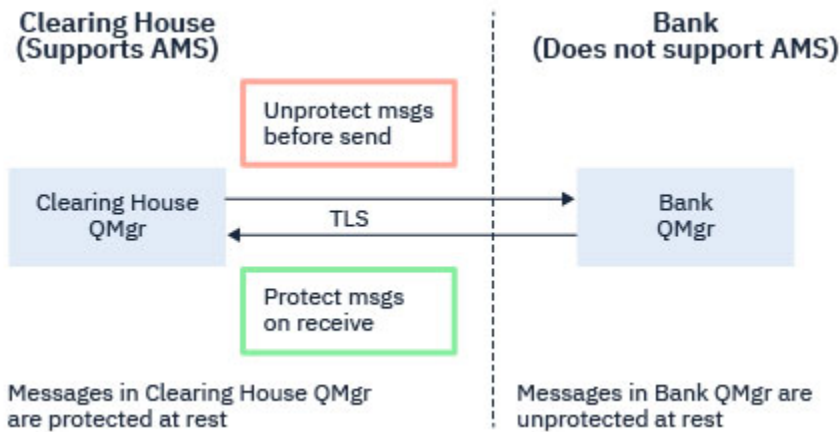


그림 34. 비즈니스 파트너 사이의 메시지 플로우

관련 태스크

서버 대 서버 메시지 채널 인터셉션 예제 구성

z/OS V 9.1.3 서버 대 서버 메시지 채널에서의 AMS 인터셉션

송신자 유형 메시지 채널 에이전트가 전송 큐에서 메시지를 가져오고 수신자 유형 메시지 채널 에이전트가 메시지를 대상 큐에 넣는 경우 서버 대 서버 메시지 채널 인터셉션에서는 메시지에 적용할 수 있는 적용 가능한 Advanced Message Security(AMS) 정책이 있어야 하는지 여부를 제어하는 도구를 제공합니다.

이를 사용하면 송신자, 서버, 수신자 및 요청자 유형의 서버 대 서버 메시지 채널을 사용하여 AMS가 사용으로 설정되지 않은 큐 관리자와 통신할 때 큐 관리자에서 AMS 보호를 사용으로 설정할 수 있습니다.

즉 AMS 가능 큐 관리자에 있는 AMS 보호 메시지는 비AMS 가능 큐 관리자에 전송되기 전 보호 해제될 수 있고, 비AMS 가능 큐 관리자로부터 수신한 비보호 메시지는 AMS 가능 큐 관리자에서 적용 가능한 AMS 정책에 의해 보호될 수 있습니다.

서버 대 서버 메시지 채널 인터셉션 구성

서버 대 서버 메시지 채널 인터셉션은 채널 유형이 송신자, 서버, 수신자 또는 요청자인 채널에서 SPLPROT 속성으로 구성됩니다. 동작 구성에 사용할 수 있는 옵션은 지정된 채널 유형에 따라 다릅니다.

PASSTHRU

이 채널의 메시지 채널 에이전트에서 송신하거나 수신한 변경되지 않은 모든 메시지를 통과합니다.

이 값은 SDR, SVR, RCVR 또는 RQSTR의 채널 유형(**CHLTYPE**)이 있는 채널에 대해 유효하며 기본값입니다.

REMOVE

메시지 채널 에이전트에 의해 전송 큐에서 검색된 메시지에서 모든 AMS 보호를 제거하며 파트너에 메시지를 송신합니다.

메시지 채널 에이전트가 전송 큐에서 메시지를 가져올 때 전송 큐에 대해 AMS 정책이 정의된 경우, 채널을 통해 메시지를 송신하기 전에 메시지에서 AMS 보호를 제거하기 위해 적용됩니다. 전송 큐에 대해 AMS 정책이 정의되지 않은 경우 메시지가 현상태대로 송신됩니다.

이 값은 채널 유형이 SDR 또는 SVR인 채널에 대해서만 유효합니다.

ASPOLICY

대상 큐에 대해 정의된 정책을 기반으로 하여 인바운드 메시지를 대상 큐에 넣기 전에 AMS 보호를 적용합니다.

메시지 채널 에이전트가 인바운드 메시지를 수신할 때 대상 큐에 대해 AMS 정책이 정의된 경우, 메시지를 대상 큐에 넣기 전에 메시지에 AMS 보호가 적용됩니다. 대상 큐에 대한 AMS 정책이 정의되지 않은 경우 메시지를 그대로 대상 큐에 넣습니다.

이 값은 채널 유형이 RCVR 또는 RQSTR인 채널에 대해서만 유효합니다.

메시지 채널 인터셉션을 위한 사용자 ID

서버 대 서버 메시지 채널 인터셉션에 사용되는 사용자 ID의 요구사항은 기존 AMS 가능 애플리케이션에서와 동일합니다. 실행 중인 채널의 경우, 송신 메시지 채널 에이전트는 전송 큐에서 메시지를 가져오고 수신 메시지 채널 에이전트는 메시지를 대상 큐에 넣습니다. 서버 대 서버 채널에서 설정된 메시지 채널 에이전트 사용자 ID(MCAUSER) 필드는 메시지 채널 에이전트가 요청을 넣고 가져오는 사용자 ID를 정의합니다.

서버 대 서버 메시지 채널 인터셉션을 사용하면 기타 AMS 가능 애플리케이션에서와 같이 AMS 기능이 가져오기 및 넣기 요청 도중 수행됩니다. 그러므로 메시지 채널 에이전트 사용자 ID에 대한 요구사항은 AMS 애플리케이션 사용자 ID와 동일합니다.

넣기 및 가져오기를 수행할 때 사용되는 MCAUSER는 구성 가능하며 아웃바운드 채널인지 또는 인바운드 채널인지에 따라 달라집니다. 선택한 사용자 ID가 메시지 채널 에이전트에서 조치를 수행하는 방법에 대한 자세한 내용은 MCAUSER를 참조하십시오. 이와 같이 채널 시작기를 실행 중인 사용자 ID는 서버 대 서버 메시지 채널 인터셉션 도중 수행되는 AMS 기능에 사용되는 사용자 ID입니다. 그러므로 이러한 사용자 ID의 요구사항은 AMS 애플리케이션 사용자 ID의 요구사항과 동일합니다.

PUTAUT 구성이 있는 채널에 대해 세부적으로 설명하는 채널의 기존 규칙을 사용하여 인증을 수행합니다. 자세한 정보는 [채널 시작기에서 사용하는 사용자 ID](#)를 참조하십시오.

참고: 서버 대 서버 메시지 채널 인터셉션에서는 PUTAUT 채널 속성 값을 고려하지 않습니다.

메시지 크기 및 MAXMSGL

AMS 보호로 인해, 보호 메시지의 메시지 크기는 원래 메시지 크기보다 커집니다.

보호 메시지는 비보호 메시지보다 크기가 큼니다. 그러므로 큐와 채널 모두에서 **MAXMSGL** 속성 값은 보호 메시지의 크기를 고려하도록 변경되어야 합니다.

관련 참조

서버 대 서버 메시지 채널 인터셉션 예제 구성

오류 핸들링

IBM MQ Advanced Message Security는 오류가 포함된 메시지 또는 보호할 수 없는 메시지를 관리할 오류 핸들링 큐를 정의합니다.

결함 메시지는 예외적인 케이스로 처리됩니다. 수신된 메시지가 현재 있는 큐의 보안 요구사항을 충족하지 않을 경우, 예를 들어 암호화해야 하는 메시지가 서명되었거나 복호화 또는 서명 확인이 실패한 경우 메시지가 오류 핸들링 큐로 송신됩니다. 다음과 같은 이유로 메시지가 오류 핸들링 큐로 송신될 수 있습니다.

- QoP(Quality of Protection) 불일치 - 수신된 메시지와 보안 정책의 QoP 정의 간에 QOP 불일치가 존재합니다.
- 복호화 오류 - 메시지를 복호화할 수 없습니다.
- PDMQ 헤더 오류 - Advanced Message Security(AMS) 메시지 헤더에 액세스할 수 없습니다.
- 크기 불일치 - 복호화 후 메시지 길이가 예상과 다릅니다.
- 암호화 알고리즘 강도 불일치 - 메시지 암호화 알고리즘이 필요한 것보다 약합니다.
- 알 수 없는 오류 - 예상치 못한 오류가 발생했습니다.

AMS 는 SYSTEM.PROTECTION.ERROR.QUEUE 는 오류 처리 큐로 대기합니다. IBM MQ AMS가 SYSTEM.PROTECTION.ERROR.QUEUE 앞에는 MQDLH 헤더가 있습니다.

IBM MQ 관리자도 SYSTEM.PROTECTION.ERROR.QUEUE 는 다른 큐를 가리키는 알리어스 큐로 설정됩니다.

z/OS V 9.1.3 IBM MQ 9.1.3부터 IBM MQ for z/OS에서 서버 대 서버 메시지 채널 에이전트 (MCA) 인터셉션이 사용 중인 경우 다음과 같이 처리됩니다.

- 앞에서 설명한 이유 중 하나로 IBM MQ AMS가 메시지를 전송 큐에서 오류 핸들링 큐로 이동시킨 경우, 송신자 MCA는 사용 가능한 다음 메시지를 전송 큐에서 계속 처리합니다.
- 일반적으로 기존 채널 규칙은 다음 사항에 적용됩니다.
 - 데드-레터 큐에 메시지 넣기
 - 데드-레터 큐에 넣기가 실패할 경우에 수행할 조치

특정 시나리오에 대한 자세한 정보는 513 페이지의 『z/OS 에서 AMS 에 대한 전달되지 않은 메시지』의 내용을 참조하십시오.

z/OS V 9.1.3 z/OS 에서 AMS 에 대한 전달되지 않은 메시지

IBM MQ for z/OS에서 발생하는 서버 대 서버 메시지 채널 에이전트 인터셉션과 관련된 특정 상황입니다.

IBM MQ 9.1.3부터 IBM MQ for z/OS에서 서버 대 서버 메시지 채널 에이전트(MCA) 인터셉션이 사용 중인 경우 다음과 같이 처리됩니다.

- 메시지를 받아 보호 해제한 후 예를 들어 메시지가 채널에 너무 큰 이유로 송신자 MCA가 메시지 전달에 실패하고 USEDLO 송신자 채널 속성이 YES로 설정되면, 송신자 MCA는 메시지를 로컬 DLQ(Dead Letter Queue)로 이동시킵니다.

로컬 DLQ로서 SYSTEM.DEAD.LETTER.QUEUE를 사용 중인 경우 메시지는 비보호 상태로 배치됩니다.

참고: IBM MQ AMS는 시스템 큐에 넣은 메시지의 보호를 지원하지 않습니다.

이름 지정된 DLQ가 로컬 DLQ로 사용되는 경우, IBM MQ AMS 정책을 이름 지정된 DLQ와 동일한 이름으로 정의했다면 메시지가 보호된 상태로 배치되고, 적합한 정책을 정의하지 않았다면 비보호 상태로 배치됩니다.

- 어떤 이유로 메시지를 로컬 DLQ에 넣을 수 없는 경우, 채널의 NPMSPEED가 NORMAL로 설정되어 있거나 메시지가 지속 메시지이면 메시지의 현재 배치가 백아웃되고 채널이 RETRY 상태가 됩니다. 그렇지 않은 경우 메시지가 제거되고 송신자 MCA가 계속해서 전송 큐의 다음 메시지를 처리합니다.
- 보안 정책은 SYSTEM.DEAD.LETTER.QUEUE 또는 578 페이지의 『AMS의 시스템 큐 보호』에 나열된 다른 SYSTEM 큐에 영향을 미치지 않으므로, SYSTEM.DEAD.LETTER.QUEUE가 사용 중일 경우, MCA가 이 큐에 넣은 메시지는 현재 상태 그대로 배치됩니다. 즉, 이전에 보호된 메시지는 보호된 상태로 배치되고, 그렇지 않은 메시지는 비보호 상태로 배치됩니다.

큐 관리자 DEADQ 속성이 대체(비시스템) 데드-레터 큐의 이름으로 설정되고 동일한 이름의 AMS 정책이 없을 경우, MCA가 이 큐에 넣은 메시지는 현재 상태 그대로 배치됩니다. 즉, 이전에 보호된 메시지는 보호된 상태로 배치되고, 그렇지 않은 메시지는 비보호 상태로 배치됩니다.

큐 관리자 DEADQ 속성이 대체(비시스템) 데드-레터 큐의 이름으로 설정되고 동일한 이름의 AMS 정책이 있을 경우, 해당 정책으로 MCA가 이 큐에 넣은 메시지가 보호됩니다. 이전에 이미 보호된 메시지는 다시 보호되지 않는데, 이는 이중 보호를 방지하기 위한 것입니다. 동일한 이름의 AMS 정책이 없을 경우 메시지는 현재 상태 그대로 배치됩니다.

- setmqspl 명령에 있는 허용 옵션이 오프(-t O)로 설정되어 있는 DLQ에 대한 정책이 있는 경우, 메시지가 AMS 보호 상태가 아니면 DLQ에 넣기는 실패하므로 PDMQ 헤더가 없습니다. 이 상황은 메시지가 PDMQ 헤더 없이

수신자에게 도착한 경우에 발생합니다. 즉, 메시지의 원래 putter에는 목적지에 대한 정책이 없으며, 수신자에게는 SPLPROT(ASPOLICY)가 설정되어 있지 않습니다.

- DLQ에 대해 정의된 AMS 정책이 채널 시작기를 실행 중인 사용자 ID가 메시지를 보호하는 것을 허용하지 않는 경우에는 MCA가 DLQ에 메시지를 넣는 데 실패할 수 있습니다.
- 수신자 채널은 일반적으로 미전달 메시지를 로컬 DLQ에 배치하지만, 송신자 채널은 일반적으로 메시지가 큐에 비해 너무 크거나 잘못된 MQXQH 헤더 등의 어떤 이유로 보호할 수 없는 메시지를 로컬 DLQ에 배치합니다.
- DLQ 핸들러는 일반적으로 메시지 페이로드(payload) 자체가 아니라 DLQ 헤더(DLH)만 검토합니다. 따라서 핸들러는 메시지 페이로드가 보호된다는 사실만으로 메시지가 DLQ에 배치된 이유를 판별할 수 밖에 없습니다.
- DLQ가 정의되지 않은 경우 채널은 다음 상태가 됩니다.
 - 지속 메시지를 전달할 수 없는 경우 비상적으로 종료되고 재시도 상태가 됩니다.
 - 비지속 미전달 메시지를 제거하고 계속 실행됩니다.

관련 개념

512 페이지의 『오류 핸들링』

IBM MQ Advanced Message Security는 오류가 포함된 메시지 또는 보호할 수 없는 메시지를 관리할 오류 핸들링 큐를 정의합니다.

사용자 시나리오

Advanced Message Security로 이룰 수 있는 비즈니스 목적에 대해 이해하려면 가능한 시나리오에 친숙해지십시오.

Windows 플랫폼에서 AMS의 빠른 시작 안내서

Windows 플랫폼에서 메시지 보안을 제공하도록 Advanced Message Security를 신속하게 구성하려면 이 안내서를 사용하십시오. 이를 완료할 때쯤 사용자 ID를 확인하기 위한 키 데이터베이스를 작성하게 될 것이고 큐 관리자의 서명/암호화 정책을 정의했을 것입니다.

시작하기 전에

최소한 다음 기능이 시스템에 설치되어 있어야 합니다.

- SERVER
- 개발 툴킷(샘플 프로그램용)
- Advanced Message Security

세부사항은 [Windows 시스템의 IBM MQ 기능](#) 을 (를) 참조하십시오.

setmqenv 명령을 사용하여 운영 체제에서 적절한 IBM MQ 명령을 찾아 실행할 수 있도록 현재 환경을 초기화하는 방법에 대한 정보는 [setmqenv \(set IBM MQ environment\)](#)를 참조하십시오.

1. 큐 관리자 및 큐 작성

이 태스크 정보

다음 모든 예에서는 애플리케이션 간 메시지를 전달하기 위해 이름이 TEST.Q인 큐를 사용합니다. Advanced Message Security는 표준 IBM MQ 인터페이스를 통해 IBM MQ 인프라에 입력하는 지점에서 메시지에 서명하고 암호화하기 위해 인터셉터를 사용합니다. 이 기본 설정은 IBM MQ에서 수행되고 다음 단계에서 구성됩니다.

You can use IBM MQ Explorer to create the queue manager QM_VERIFY_AMS and its local queue called TEST.Q by using all the default wizard settings, or you can use the commands found in C:\Program Files\IBM\MQ\bin. 다음 관리 명령을 실행하려면 mqm 사용자 그룹의 구성원이어야 함을 기억하십시오.

프로시저

1. 큐 관리자 작성

```
crtmqm QM_VERIFY_AMS
```

2. 큐 관리자 시작

```
strmqm QM_VERIFY_AMS
```

3. 다음 명령을 큐 관리자 QM_VERIFY_AMS의 **runmqsc**에 입력하여 이름이 TEST.Q인 큐를 작성하십시오.

```
DEFINE QLOCAL(TEST.Q)
```

결과

프로시저가 완료되면 **runmqsc**에 입력된 명령이 TEST.Q에 대한 세부사항을 표시합니다.

```
DISPLAY Q(TEST.Q)
```

2. 사용자 작성 및 권한 부여

이 태스크 정보

이 예에는 2명의 사용자가 나타납니다. 송신자 **alice**와 수신자 **bob**입니다. 애플리케이션 큐를 사용하려면 이러한 사용자에게는 이를 사용할 권한이 부여되어야 합니다. 또한 우리가 정의한 보호 정책을 성공적으로 사용하기 위해 이러한 사용자에게는 일부 시스템 큐에 대한 액세스가 부여되어야 합니다. **setmqaut** 명령에 대한 자세한 정보는 **setmqaut**를 참조하십시오.

프로시저

- 2명의 사용자를 작성하고 이러한 두 사용자 모두에게 **HOME**PATH 및 **HOME**DRIVE가 설정되었는지 확인하십시오.
- 사용자에게 큐 관리자에 연결하고 큐에 대해 작업할 수 있는 권한을 부여

```
setmqaut -m QM_VERIFY_AMS -t qmgr -p alice -p bob +connect +inq  
setmqaut -m QM_VERIFY_AMS -n TEST.Q -t queue -p alice +put  
setmqaut -m QM_VERIFY_AMS -n TEST.Q -t queue -p bob +get
```

- 또한 두 사용자가 시스템 정책 큐를 찾아서 메시지를 오류 큐에 넣도록 허용해야 합니다.

```
setmqaut -m QM_VERIFY_AMS -t queue -n SYSTEM.PROTECTION.POLICY.QUEUE -p alice -p bob +browse  
setmqaut -m QM_VERIFY_AMS -t queue -n SYSTEM.PROTECTION.ERROR.QUEUE -p alice -p bob +put
```



주의: IBM MQ는 모든 경우에 **SYSTEM.PROTECTION.POLICY.QUEUE**의 정책 세부사항에 대한 레코드를 찾아볼 필요가 없도록 정책을 캐싱하여 성능을 최적화합니다.

IBM MQ가 사용 가능한 모든 정책을 캐시하지는 않습니다. 정책 수가 많으면 IBM MQ가 제한된 수의 정책을 캐시합니다. 따라서 큐 관리자에 적은 수의 정책이 정의되어 있는 경우 **SYSTEM.PROTECTION.POLICY.QUEUE**에 찾아보기 옵션을 제공할 필요가 없습니다.

그러나 많은 수의 정책이 정의되어 있거나 이전 클라이언트를 사용 중인 경우 이 큐에 대한 찾아보기 권한을 부여해야 합니다. **SYSTEM.PROTECTION.ERROR.QUEUE**는 AMS 코드에서 생성된 오류 메시지를 넣는 데 사용됩니다. 이 큐에 대한 넣기(Put) 권한은 오류 메시지를 큐에 넣으려고 할 때만 확인됩니다. AMS 보호 큐에서 메시지를 가져오거나 넣으려고 할 때는 큐에 대한 넣기(Put) 권한이 확인되지 않습니다.

결과

그러면 사용자가 작성되고 사용자에게 필요한 권한이 부여됩니다.

다음에 수행할 작업

단계가 올바르게 수행되었는지 확인하려면 518 페이지의 『7. 설정 테스트』 섹션에 설명된 대로 amqsput 및 amqsget 샘플을 사용하십시오.

3. 키 데이터베이스 및 인증서 작성

이 태스크 정보

인터셉터에는 메시지를 암호화하기 위해 송신 사용자의 공개 키를 요구합니다. 따라서 공개 및 개인 키에 맵핑된 사용자의 키 데이터베이스가 작성되어야 합니다. 사용자 및 애플리케이션이 여러 컴퓨터에 분산되어 있는 실제 시스템에서는 각 사용자는 고유의 개인용 키 저장소를 가지고 있을 것입니다. 마찬가지로, 이 안내서에서는 alice와 bob을 위한 키 데이터베이스를 작성하고 이들 간에 사용자 인증서를 공유합니다.

참고: 이 안내서에서는 로컬 바인딩을 사용하여 연결하는 C로 작성된 샘플 애플리케이션을 사용합니다. 클라이언트 바인딩을 사용하여 Java 애플리케이션을 사용할 계획이면 JRE의 일부인 **keytool** 명령을 사용하여 JKS 키 저장소 및 인증서를 작성해야 합니다(세부사항은 535 페이지의 『Java 클라이언트가 있는 AMS 에 대한 빠른 시작 안내서』의 내용을 참조하십시오.). 다른 모든 언어 및 로컬 바인딩을 사용하는 Java 애플리케이션의 경우 이 안내서의 단계가 정확합니다.

프로시저

1. IBM 키 관리 GUI (strmqikm.exe) 를 사용하십시오. 사용자 alice에 대한 새 키 데이터베이스를 작성합니다.

```
Type: CMS
Filename: alicekey.kdb
Location: C:/Documents and Settings/alice/AMS
```

참고:

- 데이터베이스를 보안 설정하기 위해 강력한 비밀번호를 사용하는 것이 권장됩니다.
 - **파일에 비밀번호 숨김** 선택란이 선택되어 있는지 확인하십시오.
2. 키 데이터베이스 콘텐츠 보기를 **개인 인증서**로 변경하십시오.
 3. **새 자체 서명**을 선택하십시오. 자체 서명 인증서가 이 시나리오에서 사용됩니다.
 4. 다음 필드를 사용하여 암호화에 사용할 사용자 **alice**를 식별하는 인증서를 작성하십시오.

```
Key label: Alice_Cert
Common Name: alice
Organisation: IBM
Country: GB
```

참고:

- 이 안내서의 용도상 인증 기관을 사용하지 않고 작성할 수 있는 자체 서명 인증서를 사용 중입니다. 프로덕션 시스템의 경우 자체 서명 인증서를 사용하지 않고 대신에 인증 기관이 서명한 인증서에 의존하는 것이 바람직합니다.
 - **Key label** 매개변수는 인터셉터가 필수 정보를 수신하기 위해 찾아볼 인증서의 이름을 지정합니다.
 - **Common Name** 및 선택적 매개변수는 **식별 이름(DN)**의 세부사항을 지정하고 이는 각 사용자에게 고유해야 합니다.
5. 사용자 bob에 대해 1-4단계를 반복하십시오.

결과

2명의 사용자 alice 및 bob은 이제 각각 자체 서명 인증서가 있습니다.

4. keystore.conf 작성

이 태스크 정보

키 데이터베이스 및 인증서가 located.This 인 디렉토리에 대한 Advanced Message Security 인터셉터를 가리켜 일반 텍스트 양식으로 해당 정보를 보유하는 keystore.conf 파일을 통해 수행해야 합니다. 각 사용자에게는 .mqs 폴더에 별도의 keystore.conf 파일이 있어야 합니다. alice 및 bob 모두에 대해 이 단계를 완료해야 합니다.

keystore.conf의 콘텐츠를 다음 양식이어야 합니다.

```
cms.keystore = dir/keystore_file
cms.certificate = certificate_label
```

예

이 시나리오의 경우 keystore.conf의 콘텐츠는 다음과 같습니다.

```
cms.keystore = C:/Documents and Settings/alice/AMS/alicekey
cms.certificate = Alice_Cert
```

참고:

- 키 저장소 파일의 경로는 파일 확장자 없이 제공되어야 합니다.
- 인증서 레이블에는 공백을 포함할 수 있으므로 예를 들어, "Alice_Cert" 및 "Alice_Cert "(끝에 공백 포함)는 두 개의 서로 다른 인증서의 레이블로 인식됩니다. 그러나 혼동을 피하기 위해 레이블의 이름에는 공백을 사용하지 않는 것이 좋습니다.
- CMS(Cryptographic Message Syntax), Java 키 저장소(JKS) 및 JCEKS(Java Cryptographic Extension Keystore)의 키 저장소 형식이 있습니다. 자세한 정보는 547 페이지의 『AMS에 대한 키 저장소 구성 파일(keystore.conf)의 구조』의 내용을 참조하십시오.
- Advanced Message Security가 keystore.conf 파일을 검색하는 기본 위치는 %HOMEDRIVE%\%HOMEPATH%\ .mqs\keystore.conf(예: C:\Documents and Settings\alice\.mqs\keystore.conf)입니다. keystore.conf에 대해 기본이 아닌 위치를 사용하는 방법에 대한 정보는 547 페이지의 『키 저장소 및 인증서 사용』의 내용을 참조하십시오.
- .mqs 디렉토리를 작성하려면 명령 프롬프트를 사용해야 합니다.

5. 인증서 공유

이 태스크 정보

각 사용자가 서로를 올바르게 식별할 수 있도록 두 키 데이터베이스 사이에서 인증서를 공유하십시오. 각 사용자의 공용 인증서를 파일에 내보내면 이 파일이 다른 사용자의 키 데이터베이스에 추가되는 방식으로 수행됩니다.

참고: 신중하게 추출 옵션을 사용하고 내보내기 옵션은 사용하지 마십시오. 추출은 사용자의 공개 키를 가져오지만 내보내기는 공개 키와 개인 키를 모두 가져옵니다. 실수로 추출을 사용하는 경우 개인 키가 누출되어 애플리케이션이 완전히 훼손될 수 있습니다.

프로시저

1. alice를 식별하는 인증서를 외부 파일로 추출하십시오.

```
runmqakm -cert -extract -db "C:/Documents and Settings/alice/AMS/alicekey.kdb" -pw passw0rd -label Alice_Cert -target alice_public.arm
```

2. 인증서를 bob's 키 저장소에 추가하십시오.

```
runmqakm -cert -add -db "C:/Documents and Settings/bob/AMS/bobkey.kdb" -pw passw0rd -label Alice_Cert -file alice_public.arm
```

3. bob에 대해 단계를 반복하십시오.

```
runmqakm -cert -extract -db "C:/Documents and Settings/bob/AMS/bobkey.kdb" -pw passw0rd  
-label Bob_Cert -target bob_public.arm  
  
runmqakm -cert -add -db "C:/Documents and Settings/alice/AMS/alicekey.kdb" -pw passw0rd  
-label Bob_Cert -file bob_public.arm
```

결과

두 명의 사용자 `alice` 및 `bob`은 이제 자체 서명 인증서를 작성하고 공유한 서로를 성공적으로 식별할 수 있습니다.

다음에 수행할 작업

GUI를 사용하여 찾아보거나 자세한 내용을 출력하는 다음 명령을 실행하여 인증서가 키 저장소에 있는지 확인하십시오.

```
runmqakm -cert -details -db "C:/Documents and Settings/bob/AMS/bobkey.kdb" -pw passw0rd -label  
Alice_Cert
```

```
runmqakm -cert -details -db "C:/Documents and Settings/alice/AMS/alicekey.kdb" -pw passw0rd  
-label Bob_Cert
```

6. 큐 정책 정의

이 태스크 정보

큐 관리자가 작성되고 인터셉터가 메시지 및 액세스 암호화 키를 방해할 준비가 된 상태에서 `setmqsp1` 명령을 사용하여 `QM_VERIFY_AMS`에서 보호 정책 정의를 시작할 수 있습니다. 이 명령에 대한 자세한 정보는 `setmqsp1`의 내용을 참조하십시오. 각 정책 이름은 적용되는 큐 이름과 동일해야 합니다.

예

이는 `TEST.Q` 큐에 정의된 정책의 예입니다. 예에서 메시지는 `SHA1` 알고리즘으로 서명되고 `AES256` 알고리즘으로 암호화됩니다. `alice`는 유일한 유효한 송신자이고 `bob`은 이 큐에서 메시지의 유일한 수신자입니다.

```
setmqsp1 -m QM_VERIFY_AMS -p TEST.Q -s SHA1 -a "CN=alice,O=IBM,C=GB" -e AES256 -r  
"CN=bob,O=IBM,C=GB"
```

참고: DN은 키 데이터베이스로부터 각각의 사용자의 인증서에 명시된 것과 정확하게 일치한다.

다음에 수행할 작업

사용자가 정의한 정책을 확인하려면 다음 명령을 실행하십시오.

```
dspmqsp1 -m QM_VERIFY_AMS
```

`setmqsp1` 명령의 세트로 정책 세부사항을 인쇄하려면 `-export` 플래그를 사용하십시오. 이는 이미 정의된 정책을 저장할 수 있게 해줍니다.

```
dspmqsp1 -m QM_VERIFY_AMS -export >restore_my_policies.bat
```

7. 설정 테스트

이 태스크 정보

다른 사용자 하에서 다른 프로그램을 실행하여 애플리케이션이 제대로 구성되었는지 확인할 수 있습니다.

프로시저

1. 사용자 `alice`로서 실행하도록 사용자를 전환하십시오.

`cmd.exe`를 마우스 오른쪽 단추로 클릭하고 **다음으로 실행...**을 선택하십시오. 메시지가 표시되면 사용자 `alice`로 로그인하십시오.

2. `alice` 사용자가 샘플 애플리케이션을 사용하여 메시지를 넣을 때:

```
amqsput TEST.Q QM_VERIFY_AMS
```

3. 메시지의 텍스트를 입력한 다음 `Enter`를 누르십시오.
4. 사용자 `bob`로서 실행하도록 사용자를 전환하십시오.

`cmd.exe`를 마우스 오른쪽 단추로 클릭하고 **다음으로 실행...**을 선택하여 다른 창을 여십시오. 메시지가 표시되면 사용자 `bob`로 로그인하십시오.

5. `bob` 사용자가 샘플 애플리케이션을 사용하여 메시지를 가져올 때:

```
amqsget TEST.Q QM_VERIFY_AMS
```

결과

애플리케이션이 두 사용자에게 모두 적절하게 구성된 경우 사용자 `alice`의 메시지가 `bob`이 가져오기 애플리케이션을 실행할 때 표시됩니다.

8. 암호화 테스트

이 태스크 정보

암호화가 예상대로 발생했는지 확인하려면 원본 큐 `TEST.Q`를 참조하는 알리어스 큐를 작성하십시오. 이 알리어스 큐에는 보안 정책이 없고 메시지를 복호화하기 위한 정보를 가진 사용자가 없으므로, 암호화된 데이터가 표시될 것입니다.

프로시저

1. 큐 관리자 `QM_VERIFY_AMS`에 대해 `runmqsc` 명령을 사용하여 알리어스 큐를 작성하십시오.

```
DEFINE QALIAS(TEST.ALIAS) TARGET(TEST.Q)
```

2. 알리어스 큐에서 찾아보기 위해 `bob`에 액세스를 부여하십시오.

```
setmqaut -m QM_VERIFY_AMS -n TEST.ALIAS -t queue -p bob +browse
```

3. `alice` 사용자로서 방금 것처럼 샘플 애플리케이션을 사용하여 또 다른 메시지를 넣으십시오.

```
amqsput TEST.Q QM_VERIFY_AMS
```

4. `bob` 사용자로서 이번에는 알리어스 큐를 통해 샘플 애플리케이션을 사용하여 메시지를 찾으십시오.

```
amqsbcg TEST.ALIAS QM_VERIFY_AMS
```

5. `bob` 사용자로서 로컬 큐로부터 샘플 애플리케이션을 사용하여 메시지를 가져오십시오.

```
amqsget TEST.Q QM_VERIFY_AMS
```


결과

amqsbcg 애플리케이션의 출력에는 메시지가 암호화되었음을 증명하는 큐에 있는 암호화된 데이터가 표시됩니다.

UNIX의 AMS에 대한 빠른 시작 안내서

UNIX에 메시지 보안을 제공하도록 Advanced Message Security를 신속하게 구성하려면 이 안내서를 사용하십시오. 이를 완료할 때쯤 사용자 ID를 확인하기 위한 키 데이터베이스를 작성하게 될 것이고 큐 관리자의 서명/암호화 정책을 정의했을 것입니다.

시작하기 전에

최소한 다음 컴포넌트가 시스템에 설치되어 있어야 합니다.

- 런타임
- SERVER
- 샘플 프로그램
- IBM 글로벌 보안 키
- Advanced Message Security

각 특정 플랫폼에서 컴포넌트 이름에 대해서는 다음 주제를 참조하십시오.

- **Linux** [Linux 시스템의 IBM MQ 구성요소](#)
- **AIX** [AIX 시스템의 IBM MQ 구성요소](#)
- **Solaris** [Solaris 시스템의 IBM MQ 구성요소](#)

1. 큐 관리자 및 큐 작성

이 태스크 정보

다음 모든 예에서는 애플리케이션 간 메시지를 전달하기 위해 이름이 TEST.Q인 큐를 사용합니다. Advanced Message Security는 표준 IBM MQ 인터페이스를 통해 IBM MQ 인프라에 입력하는 지점에서 메시지에 서명하고 암호화하기 위해 인터셉터를 사용합니다. 이 기본 설정은 IBM MQ에서 수행되고 다음 단계에서 구성됩니다.

IBM MQ 탐색기를 사용하여 모든 기본 마법사 설정을 통해 큐 관리자(QM_VERIFY_AMS) 및 해당 로컬 큐(TEST.Q)를 작성하거나 `MQ_INSTALLATION_PATH/bin`에 있는 명령을 사용할 수 있습니다. 다음 관리 명령을 실행하려면 `mqm` 사용자 그룹의 구성원이어야 함을 기억하십시오.

프로시저

1. 큐 관리자 작성

```
crtmqm QM_VERIFY_AMS
```

2. 큐 관리자 시작

```
strmqm QM_VERIFY_AMS
```

3. 다음 명령을 큐 관리자 QM_VERIFY_AMS의 `runmqsc`에 입력하여 이름이 TEST.Q인 큐를 작성하십시오.

```
DEFINE QLOCAL(TEST.Q)
```

결과

프로시저가 성공적으로 완료되면 `runmqsc`에 입력된 다음 명령이 TEST.Q에 대한 세부사항을 표시합니다.

```
DISPLAY Q(TEST.Q)
```

2. 사용자 작성 및 권한 부여

이 태스크 정보

이 예에는 2명의 사용자가 나타납니다. 송신자 `alice`와 수신자 `bob`입니다. 애플리케이션 큐를 사용하려면 이러한 사용자에게는 이를 사용할 권한이 부여되어야 합니다. 또한 우리가 정의한 보호 정책을 성공적으로 사용하기 위해 이러한 사용자에게는 일부 시스템 큐에 대한 액세스가 부여되어야 합니다. `setmqaut` 명령에 대한 자세한 정보는 [setmqaut](#)를 참조하십시오.

프로시저

1. 2명의 사용자를 작성하십시오

```
useradd alice
useradd bob
```

2. 사용자에게 큐 관리자에 연결하고 큐에 대해 작업할 수 있는 권한을 부여

```
setmqaut -m QM_VERIFY_AMS -t qmgr -p alice -p bob +connect +inq
setmqaut -m QM_VERIFY_AMS -n TEST.Q -t queue -p alice +put
setmqaut -m QM_VERIFY_AMS -n TEST.Q -t queue -p bob +get
```

3. 또한 두 사용자가 시스템 정책 큐를 찾아서 메시지를 오류 큐에 넣도록 허용해야 합니다.

```
setmqaut -m QM_VERIFY_AMS -t queue -n SYSTEM.PROTECTION.POLICY.QUEUE -p alice -p bob +browse
setmqaut -m QM_VERIFY_AMS -t queue -n SYSTEM.PROTECTION.ERROR.QUEUE -p alice -p bob +put
```



주의: IBM MQ는 모든 경우에 SYSTEM.PROTECTION.POLICY.QUEUE의 정책 세부사항에 대한 레코드를 찾아볼 필요가 없도록 정책을 캐싱하여 성능을 최적화합니다.

IBM MQ가 사용 가능한 모든 정책을 캐시하지는 않습니다. 정책 수가 많으면 IBM MQ가 제한된 수의 정책을 캐시합니다. 따라서 큐 관리자에 적은 수의 정책이 정의되어 있는 경우 SYSTEM.PROTECTION.POLICY.QUEUE에 찾아보기 옵션을 제공할 필요가 없습니다.

그러나 많은 수의 정책이 정의되어 있거나 이전 클라이언트를 사용 중인 경우 이 큐에 대한 찾아보기 권한을 부여해야 합니다. SYSTEM.PROTECTION.ERROR.QUEUE는 AMS 코드에서 생성된 오류 메시지를 넣는 데 사용됩니다. 이 큐에 대한 넣기(Put) 권한은 오류 메시지를 큐에 넣으려고 할 때만 확인됩니다. AMS 보호 큐에서 메시지를 가져오거나 넣으려고 할 때는 큐에 대한 넣기(Put) 권한이 확인되지 않습니다.

결과

이제 사용자 그룹이 작성되고 필수 권한이 부여됩니다. 이런 식으로, 사용자 그룹에 지정된 사용자는 큐 관리자에 연결하고 큐에 넣고 큐에서 가져올 권한이 가지게 됩니다.

다음에 수행할 작업

단계가 올바르게 수행되었는지 확인하려면 525 페이지의 『8. 암호화 테스트』 섹션에 설명된 대로 `amqsput` 및 `amqsget` 샘플을 사용하십시오.

3. 키 데이터베이스 및 인증서 작성

이 태스크 정보

메시지를 암호화하기 위해 인터셉터는 송신 사용자의 개인 키와 수신인의 공개 키가 필요합니다. 따라서 공개 및 개인 키에 매핑된 사용자의 키 데이터베이스가 작성되어야 합니다. 사용자 및 애플리케이션이 여러 컴퓨터에 분산되어 있는 실제 시스템에서는 각 사용자는 고유의 개인용 키 저장소를 가지고 있을 것입니다. 마찬가지로, 이 안내서에서는 **alice**와 **bob**을 위한 키 데이터베이스를 작성하고 이들 간에 사용자 인증서를 공유합니다.

참고: 이 안내서에서는 로컬 바인딩을 사용하여 연결하는 C로 작성된 샘플 애플리케이션을 사용합니다. 클라이언트 바인딩을 사용하여 Java 애플리케이션을 사용할 계획이면 JRE의 일부인 **keytool** 명령을 사용하여 JKS 키 저장소 및 인증서를 작성해야 합니다(세부사항은 535 페이지의 『Java 클라이언트가 있는 AMS에 대한 빠른 시작 안내서』의 내용을 참조하십시오.). 다른 모든 언어 및 로컬 바인딩을 사용하는 Java 애플리케이션의 경우 이 안내서의 단계가 정확합니다.

프로시저

1. 사용자 **alice**의 새 키 데이터베이스를 작성하십시오.

```
mkdir /home/alice/.mqs -p
runmqakm -keydb -create -db /home/alice/.mqs/alicekey.kdb -pw passw0rd -stash
```

참고:

- 데이터베이스를 보안 설정하기 위해 강력한 비밀번호를 사용하는 것이 권장됩니다.
 - **stash** 매개변수는 비밀번호를 **key.sth** 파일에 저장하고 이는 인터셉터가 데이터베이스를 열기 위해 사용할 수 있습니다.
2. 키 데이터베이스가 읽기 가능한지 확인하십시오.

```
chmod +r /home/alice/.mqs/alicekey.kdb
```

3. 암호화에 사용하기 위해 **alice** 사용자를 식별하는 인증서를 작성하십시오.

```
runmqakm -cert -create -db /home/alice/.mqs/alicekey.kdb -pw passw0rd
-label Alice_Cert -dn "cn=alice,0=IBM,c=GB" -default_cert yes
```

참고:

- 이 안내서의 용도상 인증 기관을 사용하지 않고 작성할 수 있는 자체 서명 인증서를 사용 중입니다. 프로덕션 시스템의 경우 자체 서명 인증서를 사용하지 않고 대신에 인증 기관이 서명한 인증서에 의존하는 것이 바람직합니다.
 - **label** 매개변수는 인터셉터가 필수 정보를 수신하기 위해 찾아볼 인증서의 이름을 지정합니다.
 - **DN** 매개변수는 **식별 이름(DN)**의 세부사항을 지정하고 이는 각 사용자에게 대해 고유해야 합니다.
4. 이제 키 데이터베이스를 작성했으므로 이에 대한 소유권을 설정하고, 다른 사용자는 이를 읽을 수 없는지 확인하십시오.

```
chown alice /home/alice/.mqs/alicekey.kdb /home/alice/.mqs/alicekey.sth
chmod 600 /home/alice/.mqs/alicekey.kdb /home/alice/.mqs/alicekey.sth
```

5. 사용자 **bob**에 대해 1-4단계를 반복하십시오.

결과

2명의 사용자 **alice** 및 **bob**은 이제 각각 자체 서명 인증서가 있습니다.

4. keystore.conf 작성

이 태스크 정보

Advanced Message Security 인터셉터로 키 데이터베이스 및 인증서가 있는 디렉토리를 가리켜야 합니다. 이는 해당 정보를 일반 텍스트 양식으로 보유하는 keystore.conf 파일을 통해 수행됩니다. 각 사용자에게는 .mqc 폴더에 별도의 keystore.conf 파일이 있어야 합니다. alice 및 bob 모두에 대해 이 단계를 완료해야 합니다.

keystore.conf의 콘텐츠를 다음 양식이어야 합니다.

```
cms.keystore = dir/keystore_file
cms.certificate = certificate_label
```

예

이 시나리오의 경우 keystore.conf의 콘텐츠는 다음과 같습니다.

```
cms.keystore = /home/alice/.mqc/alicekey
cms.certificate = Alice_Cert
```

참고:

- 키 저장소 파일의 경로는 파일 확장자 없이 제공되어야 합니다.
- CMS(Cryptographic Message Syntax), Java 키 저장소(JKS) 및 JCEKS(Java Cryptographic Extension Keystore)의 키 저장소 형식이 있습니다. 자세한 정보는 [547 페이지의 『AMS에 대한 키 저장소 구성 파일\(keystore.conf\)의 구조』](#)의 내용을 참조하십시오.
- HOME/.mqc/keystore.conf는 Advanced Message Security가 keystore.conf 파일을 검색하는 기본 위치입니다. keystore.conf에 대해 기본이 아닌 위치를 사용하는 방법에 대한 정보는 [547 페이지의 『키 저장소 및 인증서 사용』](#)의 내용을 참조하십시오.

5. 인증서 공유

이 태스크 정보

각 사용자가 서로를 올바르게 식별할 수 있도록 두 키 데이터베이스 사이에서 인증서를 공유하십시오. 각 사용자의 공용 인증서를 파일에 내보내면 이 파일이 다른 사용자의 키 데이터베이스에 추가되는 방식으로 수행됩니다.

참고: 신중하게 추출 옵션을 사용하고 내보내기 옵션은 사용하지 마십시오. 추출은 사용자의 공개 키를 가져오지만 내보내기는 공개 키와 개인 키를 모두 가져옵니다. 실수로 추출을 사용하는 경우 개인 키가 누출되어 애플리케이션이 완전히 훼손될 수 있습니다.

프로시저

1. alice를 식별하는 인증서를 외부 파일로 추출하십시오.

```
runmqakm -cert -extract -db /home/alice/.mqc/alicekey.kdb -pw passwd -label Alice_Cert -target alice_public.arm
```

2. 인증서를 bob's 키 저장소에 추가하십시오.

```
runmqakm -cert -add -db /home/bob/.mqc/bobkey.kdb -pw passwd -label Alice_Cert -file alice_public.arm
```

3. bob에 대해 단계를 반복하십시오.

```
runmqakm -cert -extract -db /home/bob/.mqc/bobkey.kdb -pw passwd -label Bob_Cert -target bob_public.arm
```

4. bob의 인증서를 alice's 키 저장소에 추가하십시오.

```
runmqakm -cert -add -db /home/alice/.mqs/alicekey.kdb -pw passwd -label Bob_Cert -file bob_public.arm
```

결과

두 명의 사용자 `alice` 및 `bob`은 이제 자체 서명 인증서를 작성하고 공유한 서로를 성공적으로 식별할 수 있습니다.

다음에 수행할 작업

해당 세부사항을 인쇄하는 다음 명령을 실행하여 인증서가 키 저장소에 있는지 확인하십시오.

```
runmqakm -cert -details -db /home/bob/.mqs/bobkey.kdb -pw passwd -label Alice_Cert  
runmqakm -cert -details -db /home/alice/.mqs/alicekey.kdb -pw passwd -label Bob_Cert
```

6. 큐 정책 정의

이 태스크 정보

큐 관리자가 작성되고 인터셉터가 메시지 및 액세스 암호화 키를 방해할 준비가 된 상태에서 `setmqsp1` 명령을 사용하여 `QM_VERIFY_AMS`에서 보호 정책 정의를 시작할 수 있습니다. 이 명령에 대한 자세한 정보는 [setmqsp1](#)의 내용을 참조하십시오. 각 정책 이름은 적용되는 큐 이름과 동일해야 합니다.

예

이는 `TEST.Q` 큐에 정의된 정책의 예입니다. 이 예에서 메시지는 `SHA1` 알고리즘을 사용하여 `alice` 사용자에 의해 서명되고 256비트 `AES` 알고리즘을 사용하여 암호화됩니다. `alice`는 유일한 유효한 송신자이고 `bob`은 이 큐에서 메시지의 유일한 수신자입니다.

```
setmqsp1 -m QM_VERIFY_AMS -p TEST.Q -s SHA1 -a "CN=alice,O=IBM,C=GB" -e AES256 -r "CN=bob,O=IBM,C=GB"
```

참고: DN은 키 데이터베이스로부터 각각의 사용자의 인증서에 명시된 것과 정확하게 일치한다.

다음에 수행할 작업

사용자가 정의한 정책을 확인하려면 다음 명령을 실행하십시오.

```
dspmqspl -m QM_VERIFY_AMS
```

`setmqsp1` 명령의 세트로 정책 세부사항을 인쇄하려면 `-export` 플래그를 사용하십시오. 이는 이미 정의된 정책을 저장할 수 있게 해줍니다.

```
dspmqspl -m QM_VERIFY_AMS -export >restore_my_policies.bat
```

7. 설정 테스트

이 태스크 정보

다른 사용자 하에서 다른 프로그램을 실행하여 애플리케이션이 제대로 구성되었는지 확인할 수 있습니다.

프로시저

1. 샘플을 포함하는 디렉토리로 변경하십시오. MQ가 비기본 위치에 설치된 경우에는 이는 다른 위치에 있을 수도 있습니다.

```
cd /opt/mqm/samp/bin
```

2. 사용자 **alice**로서 실행하도록 사용자를 전환하십시오.

```
su alice
```

3. **alice** 사용자로서, 샘플 애플리케이션을 사용하여 메시지를 넣으십시오.

```
./amqsput TEST.Q QM_VERIFY_AMS
```

4. 메시지의 텍스트를 입력한 다음 Enter를 누르십시오.
5. 사용자 **alice**로서의 실행을 중지하십시오.

```
exit
```

6. 사용자 **bob**로서 실행하도록 사용자를 전환하십시오.

```
su bob
```

7. **bob** 사용자로서 샘플 애플리케이션을 사용하여 메시지를 가져오십시오.

```
./amqsget TEST.Q QM_VERIFY_AMS
```

결과

애플리케이션이 두 사용자에게 모두 적절하게 구성된 경우 사용자 **alice**의 메시지가 **bob**이 가져오기 애플리케이션을 실행할 때 표시됩니다.

8. 암호화 테스트

이 태스크 정보

암호화가 예상대로 발생했는지 확인하려면 원본 큐 **TEST.Q**를 참조하는 알리어스 큐를 작성하십시오. 이 알리어스 큐에는 보안 정책이 없고 메시지를 복호화하기 위한 정보를 가진 사용자가 없으므로, 암호화된 데이터가 표시 될 것입니다.

프로시저

1. 큐 관리자 **QM_VERIFY_AMS**에 대해 **runmqsc** 명령을 사용하여 알리어스 큐를 작성하십시오.

```
DEFINE QALIAS(TEST.ALIAS) TARGET(TEST.Q)
```

2. 알리어스 큐에서 찾아보기 위해 **bob**에 액세스를 부여하십시오.

```
setmqaut -m QM_VERIFY_AMS -n TEST.ALIAS -t queue -p bob +browse
```

3. **alice** 사용자로서 방금 것처럼 샘플 애플리케이션을 사용하여 또 다른 메시지를 넣으십시오.

```
./amqsput TEST.Q QM_VERIFY_AMS
```

4. **bob** 사용자로서 이번에는 알리어스 큐를 통해 샘플 애플리케이션을 사용하여 메시지를 찾으십시오.

```
./amqsbcg TEST.ALIAS QM_VERIFY_AMS
```

5. **bob** 사용자로서 로컬 큐로부터 샘플 애플리케이션을 사용하여 메시지를 가져오십시오.

```
./amqsget TEST.Q QM_VERIFY_AMS
```


결과


amqsbcg 애플리케이션의 출력에는 메시지가 암호화되었음을 증명하는 큐에 있는 암호화된 데이터가 표시됩니다.

z/OS의 예 구성

이 절에서는 z/OS의 Advanced Message Security 대기열 시나리오에 대한 정책 및 인증의 예제 구성을 제공합니다.

Advanced Message Security 구성 방법에 대한 세부사항은 [Advanced Message Security for z/OS 구성](#) 을 참조하십시오.

예는 필요한 Advanced Message Security 정책 및 사용자 및 키 링과 관련하여 존재해야 하는 디지털 인증서에 대해 다룹니다. 예제에서는 시나리오에 참여하는 사용자가 [Advanced Message Security의 사용자 자원 권한 부여](#)에서 제공하는 지시사항에 따라 설정되었다고 간주합니다.

 또한 IBM MQ 9.1.3 이상부터는 [서버 간 메시지 채널 인터셉션 구성 예제](#)를 참조하십시오.

z/OS에서 무결성 보호된 메시지의 로컬 큐잉

이 예는 무결성 보호된 메시지를 넣기 및 가져오기 애플리케이션의 로컬에서 큐에 전송하고 받는 데 필요한 Advanced Message Security 정책 및 인증서를 설명합니다.

예 큐 관리자 및 큐는 다음과 같습니다.

```
BNK6          - Queue manager
FIN.XFER.Q7   - Local queue
```

다음 사용자가 사용됩니다.

```
WMQBNK6      - AMS task user
TELLER5      - Sending user
FINADM2      - Recipient user
```

사용자 인증서 작성

이 예에서 단 하나의 사용자 인증서만이 필요합니다. 이는 무결성 보호된 메시지에 서명하는 데 필요한 송신 사용자의 인증서입니다. 송신 사용자는 'TELLER5'입니다.

인증 기관(CA) 인증서 또한 필요합니다. CA 인증서는 사용자의 인증서를 발행한 권한의 인증서입니다. 이는 인증서의 체인일 수 있습니다. 그런 경우 체인의 모든 인증서는 Advanced Message Security 태스크 사용자의 키 링에서 필수입니다. 이 경우 사용자 WMQBNK6입니다.

CA 인증서는 RACF RACDCERT 명령을 사용하여 작성할 수 있습니다. 이 인증서는 사용자 인증서를 발행하는 데 사용됩니다. 예를 들면, 다음과 같습니다.

```
RACDCERT CERTAUTH GENCERT SUBJECTSDN(CN('BCOCA') O('BCO') C('US'))
KEYUSAGE(CERTSIGN) WITHLABEL('BCOCA')
```

이 RACDCERT 명령은 사용자 'TELLER5'를 위한 사용자 인증서를 발행하는 데 사용할 수 있는 CA 인증서를 작성합니다. 예를 들면, 다음과 같습니다.

```
RACDCERT ID(TELLER5) GENCERT SUBJECTSDN(CN('Teller5') O('BCO') C('US'))
WITHLABEL('Teller5') SIGNWITH(CERTAUTH LABEL('BCOCA'))
KEYUSAGE(HANDSHAKE DATAENCRYPT DOCSIGN)
```

설치에는 CA 인증서를 선택하고 작성하기 위한 프로시저뿐만 아니라 인증서를 발행하고 이를 관련 시스템에 분배하기 위한 프로시저가 있습니다.

이러한 인증서를 내보내고 가져올 때 Advanced Message Security에는 다음이 필요합니다.

- CA 인증서(체인).

- 사용자 인증서 및 해당 개인 키.

RACF를 사용 중인 경우, RACDCERT EXPORT 명령은 인증서를 데이터 세트에 내보내는 데 사용할 수 있고, RACDCERT ADD 명령은 인증서를 데이터 세트로부터 가져오는 데 사용할 수 있습니다. 이러한 명령 및 다른 RACDCERT 명령에 대한 자세한 정보는 z/OS: 보안 서버 RACF 명령어 참조를 참조하십시오.

이 경우 인증서는 큐 관리자 BNK6을 실행 중인 z/OS 시스템에서 필요합니다.

인증서가 BNK6을 실행 중인 z/OS 시스템에 가져오기되면 사용자 인증서에는 TRUST 속성이 필요합니다. RACDCERT ALTER 명령은 TRUST 속성을 인증서에 추가하는 데 사용할 수 있습니다. 예를 들면, 다음과 같습니다.

```
RACDCERT ID(TELLER5) ALTER (LABEL('Teller5')) TRUST
```

이 예에서는 수신인 사용자에게 어떤 인증서도 필요하지 않습니다.

인증서를 관련 키 링에 연결

필수 인증서가 작성되거나 가져오기되고, 신뢰되는 것으로 설정될 때 이들은 BNK6을 실행 중인 z/OS 시스템에서 적합한 사용자 키 링에 연결되어야 합니다. 키 링을 작성하려면 RACDCERT ADDRING 명령을 사용하십시오.

```
RACDCERT ID(WMQBNK6) ADDRING(drq.ams.keyring)
RACDCERT ID(TELLER5) ADDRING(drq.ams.keyring)
```

이는 Advanced Message Security 태스크 사용자, WMQBNK6을 위한 키 링을 작성하고, 송신 사용자, 'TELLER5'를 위한 키 링을 작성합니다. 키 링 이름 drq.ams.keyring은 필수이고 이름은 대소문자를 구분함을 유의하십시오.

키 링이 작성될 때 관련 인증서를 연결할 수 있습니다.

```
RACDCERT ID(WMQBNK6) CONNECT(CERTAUTH LABEL('BCOCA')
RING(drq.ams.keyring))
RACDCERT ID(TELLER5) CONNECT(ID(TELLER5) LABEL('Teller5')
RING(drq.ams.keyring) DEFAULT USAGE(PERSONAL))
```

송신 사용자 인증서는 DEFAULT로서 연결되어야 합니다. 송신 사용자에게 해당 drq.ams.keyring에 둘 이상의 인증서가 있는 경우에는 서명 용도를 위해 기본 인증서가 사용됩니다.

큐 관리자가 중지되고 다시 시작되거나 z/OS MODIFY 명령이 Advanced Message Security 인증서 구성을 새로 고치기 위해 사용될 때까지 인증서의 작성 및 수정이 Advanced Message Security 에서 인식되지 않습니다. 예를 들면, 다음과 같습니다.

```
F BNK6AMSM,REFRESH KEYRING
```

Advanced Message Security 정책 작성

이 예에서 무결성 보호된 메시지는 사용자 'TELLER5'로서 실행 중인 애플리케이션에 의해 큐 FIN.XFER.Q7에 놓여지고, 사용자 'FINADM2'로서 실행 중인 애플리케이션에 의해 동일 큐에서 검색되므로, 단 하나의 Advanced Message Security 정책만이 필요합니다.

Advanced Message Security 정책은 메시지 보안 정책 유틸리티(CSQOUTIL)에 문서화된 CSQOUTIL 유틸리티를 사용하여 작성됩니다.

다음 명령을 실행하여 CSQOUTIL 유틸리티를 사용하십시오.

```
setmqsp1 -m BNK6 -p FIN.XFER.Q7 -s MD5 -a CN=Teller5,O=BCO,C=US
```

이 정책에서 큐 관리자는 BNK6로 식별됩니다. 정책 이름 및 연관된 큐는 FIN.XFER.Q7입니다. 송신자의 서명을 생성하는 데 사용되는 알고리즘은 MD5이고 송신 사용자의 식별 이름(DN)은 'CN=Teller5,O=BCO,C=US'입니다.

정책을 정의한 후에 BNK6 큐 관리자를 재시작하거나 z/OS **MODIFY** 명령을 사용하여 Advanced Message Security 정책 구성을 새로 고치십시오. 예를 들면, 다음과 같습니다.

```
F BNK6AMSM,REFRESH POLICY
```

z/OS z/OS에서 개인정보 보호된 메시지의 로컬 큐잉
이 예는 개인정보 보호된 메시지를 넣기 및 가져오기 애플리케이션의 로컬에서 큐에 전송하고 받는 데 필요한 Advanced Message Security 정책 및 인증서를 설명합니다. 개인정보 보호된 메시지는 둘 모두 서명되고 암호화됩니다.

예 큐 관리자 및 로컬 큐는 다음과 같습니다.

```
BNK6 - Queue manager  
FIN.XFER.Q8 - Local queue
```

다음 사용자가 사용됩니다.

```
WMQBANK6 - AMS task user  
TELLER5 - Sending user  
FINADM2 - Recipient user
```

이 시나리오를 구성하기 위한 단계는 다음과 같습니다.

사용자 인증서 작성

이 예에서 두 개의 사용자 인증서가 필요합니다. 이들은 메시지에 서명하기 위해 필요한 송신 사용자의 인증서 및 메시지 데이터를 암호화하고 복호화하기 위해 필요한 수신자의 사용자 인증서입니다. 송신 사용자는 'TELLER5'이고 수신 사용자는 'FINADM2'입니다.

인증 기관(CA) 인증서 또한 필요합니다. CA 인증서는 사용자의 인증서를 발행한 권한의 인증서입니다. 이는 인증서의 체인일 수 있습니다. 그런 경우 체인의 모든 인증서는 Advanced Message Security 태스크 사용자의 키 링에서 필수입니다. 이 경우 사용자 WMQBANK6입니다.

CA 인증서는 RACF RACDCERT 명령을 사용하여 작성할 수 있습니다. 이 인증서는 사용자 인증서를 발행하는 데 사용됩니다. 예를 들면, 다음과 같습니다.

```
RACDCERT CERTAUTH GENCERT SUBJECTSDN(CN('BCOCA') O('BCO') C('US'))  
KEYUSAGE(CERTSIGN) WITHLABEL('BCOCA')
```

이 RACDCERT 명령은 사용자 'TELLER5' 및 'FINADM2'를 위한 사용자 인증서를 발행하는 데 사용할 수 있는 CA 인증서를 작성합니다. 예를 들면, 다음과 같습니다.

```
RACDCERT ID(TELLER5) GENCERT SUBJECTSDN(CN('Teller5') O('BCO') C('US'))  
WITHLABEL('Teller5') SIGNWITH(CERTAUTH LABEL('BCOCA'))  
KEYUSAGE(HANDSHAKE DATAENCRYPT DOCSIGN)
```

```
RACDCERT ID(FINADM2) GENCERT SUBJECTSDN(CN('FinAdm2') O('BCO') C('US'))  
WITHLABEL('FinAdm2') SIGNWITH(CERTAUTH LABEL('BCOCA'))  
KEYUSAGE(HANDSHAKE DATAENCRYPT DOCSIGN)
```

설치에는 CA 인증서를 선택하고 작성하기 위한 프로시저뿐만 아니라 인증서를 발행하고 이를 관련 시스템에 분배하기 위한 프로시저가 있습니다.

이러한 인증서를 내보내고 가져올 때 Advanced Message Security에는 다음이 필요합니다.

- CA 인증서(체인).
- 송신 사용자 인증서 및 해당 개인 키.
- 수신 사용자 인증서 및 해당 개인 키.

RACF를 사용 중인 경우, RACDCERT EXPORT 명령은 인증서를 데이터 세트에 내보내는 데 사용할 수 있고, RACDCERT ADD 명령은 인증서를 데이터 세트로부터 가져오는 데 사용할 수 있습니다. 이들 및 기타 RACDCERT 명령에 대한 자세한 정보는 *z/OS: Security Server RACF Command Language Reference*의 [RACDCERT \(RACF 디지털 인증서 관리\)](#)를 참조하십시오.

이 경우 인증서는 큐 관리자 BNK6을 실행 중인 z/OS 시스템에서 필요합니다.

인증서가 BNK6을 실행 중인 z/OS 시스템에 가져오기되면 사용자 인증서에는 TRUST 속성이 필요합니다. RACDCERT ALTER 명령은 TRUST 속성을 인증서에 추가하는 데 사용할 수 있습니다. 예를 들면, 다음과 같습니다.

```
RACDCERT ID(TELLER5) ALTER (LABEL('Teller5')) TRUST
RACDCERT ID(FINADM2) ALTER (LABEL('FinAdm2')) TRUST
```

인증서를 관련 키 링에 연결

필수 인증서가 작성되거나 가져오기되고, 신뢰되는 것으로 설정될 때 이들은 BNK6을 실행 중인 z/OS 시스템에서 적합한 사용자 키 링에 연결되어야 합니다. 키 링을 작성하려면 RACDCERT ADDRING 명령을 사용하십시오.

```
RACDCERT ID(WMQBNK6) ADDRING(drq.ams.keyring)
RACDCERT ID(TELLER5) ADDRING(drq.ams.keyring)
RACDCERT ID(FINADM2) ADDRING(drq.ams.keyring)
```

이는 송신 및 수신 사용자를 위해 Advanced Message Security 태스크 사용자를 위한 키 링을 작성합니다. 키 링 이름 drq.ams.keyring은 필수이고 이름은 대소문자를 구분함을 유의하십시오.

키 링이 작성될 때 관련 인증서를 연결할 수 있습니다.

```
RACDCERT ID(WMQBNK6) CONNECT(CERTAUTH LABEL('BCOCA')
RING(drq.ams.keyring))

RACDCERT ID(WMQBNK6) CONNECT(ID(FINADM2) LABEL('FinAdm2')
RING(drq.ams.keyring) USAGE(SITE))

RACDCERT ID(TELLER5) CONNECT(ID(TELLER5) LABEL('Teller5')
RING(drq.ams.keyring) DEFAULT USAGE(PERSONAL))

RACDCERT ID(FINADM2) CONNECT(ID(FINADM2) LABEL('FinAdm2')
RING(drq.ams.keyring) DEFAULT USAGE(PERSONAL))
```

송신 및 수신 사용자 인증서는 DEFAULT로서 연결되어야 합니다. 사용자에게 해당 drq.ams.keyring에 둘 이상의 인증서가 있는 경우에는 서명 및 복호화 용도를 위해 기본 인증서가 사용됩니다.

수신 사용자의 인증서는 또한 USAGE(SITE)와 함께 Advanced Message Security 태스크 사용자의 키 링에 연결되어야 합니다. 이는 고급 메시지 보안 태스크에 메시지 데이터를 암호화할 때 수신인의 공개 키가 필요하기 때문입니다. USAGE(SITE)는 개인 키가 키 링크에서 액세스 가능하지 못하게 만듭니다.

큐 관리자가 중지되고 다시 시작되거나 z/OS **MODIFY** 명령이 Advanced Message Security 인증서 구성을 새로 고치기 위해 사용될 때까지 인증서의 작성 및 수정이 Advanced Message Security 에서 인식되지 않습니다. 예를 들면, 다음과 같습니다.

```
F BNK6AMSM,REFRESH KEYRING
```

Advanced Message Security 정책 작성

이 예에서 개인정보 보호된 메시지는 사용자 'TELLER5'로서 실행 중인 애플리케이션에 의해 큐 FIN.XFER.Q8에 놓여지고, 사용자 'FINADM2'로서 실행 중인 애플리케이션에 의해 동일 큐에서 검색되므로, 단 하나의 Advanced Message Security 정책만이 필요합니다.

Advanced Message Security 정책은 [메시지 보안 정책 유틸리티\(CSQOUTIL\)](#)에 문서화된 CSQOUTIL 유틸리티를 사용하여 작성됩니다.

다음 명령을 실행하여 CSQOUTIL 유틸리티를 사용하십시오.

```
setmqsp1 -m BNK6 -p FIN.XFER.Q8 -s SHA1 -e 3DES -a CN=Teller5,O=BCO,C=US -r  
CN=FinAdm2,O=BCO,C=US
```

이 정책에서 큐 관리자는 BNK6로 식별됩니다. 정책 이름 및 연관된 큐는 FIN.XFER.Q8입니다. 송신자의 서명을 생성하는 데 사용된 알고리즘은 SHA1이고 송신 사용자의 식별 이름(DN)은 'CN=Teller5,O=BCO,C=US'이고, 수신 사용자는 'CN=FinAdm2,O=BCO,C=US'입니다. 메시지 데이터를 암호화하는 데 사용되는 알고리즘은 3DES입니다.

정책을 정의한 후에 BNK6 큐 관리자를 재시작하거나 **z/OS MODIFY** 명령을 사용하여 Advanced Message Security 정책 구성을 새로 고치십시오. 예를 들면, 다음과 같습니다.

```
F BNK6AMSM,REFRESH POLICY
```

z/OS z/OS에서 무결성 보호된 메시지의 리모트 큐잉

이 예는 두 개의 서로 다른 큐 관리자가 관리하는 큐에 무결성 보호된 메시지를 송신하고 수신하는 데 필요한 Advanced Message Security 정책 및 인증서를 설명합니다. 두 개의 큐 관리자는 동일한 z/OS 시스템 또는 다른 z/OS 시스템에서 실행 중이거나 하나의 큐 관리자가 Advanced Message Security를 실행하는 분산 시스템에 있을 수 있습니다.

예 큐 관리자 및 큐는 다음과 같습니다.

```
BNK6      - Sending queue manager  
BNK7      - Recipient queue manager  
FIN.XFER.Q7 - Remote queue on BNK6  
FIN.RCPT.Q7 - Local queue on BNK7
```

참고: 이 예의 경우 BNK6 및 BNK7은 서로 다른 z/OS 시스템에서 실행 중인 큐 관리자입니다.

다음 사용자가 사용됩니다.

```
WMQBNK6 - AMS task user on BNK6  
WMQBNK7 - AMStask user on BNK7  
TELLER5 - Sending user on BNK6  
FINADM2 - Recipient user on BNK7
```

이 시나리오를 구성하기 위한 단계는 다음과 같습니다.

사용자 인증서 작성

이 예에서 단 하나의 사용자 인증서만이 필요합니다. 이는 무결성 보호된 메시지에 서명하는 데 필요한 송신 사용자의 인증서입니다. 송신 사용자는 'TELLER5'입니다.

인증 기관(CA) 인증서 또한 필요합니다. CA 인증서는 사용자의 인증서를 발행한 권한의 인증서입니다. 이는 인증서의 체인일 수 있습니다. 그런 경우 체인의 모든 인증서는 Advanced Message Security 태스크 사용자의 키 링에서 필수입니다. 이 경우 사용자 WMQBNK7입니다.

CA 인증서는 RACF RACDCERT 명령을 사용하여 작성할 수 있습니다. 이 인증서는 사용자 인증서를 발행하는 데 사용됩니다. 예를 들면, 다음과 같습니다.

```
RACDCERT CERTAUTH GENCERT SUBJECTSDN(CN('BCOCA') O('BCO') C('US'))  
KEYUSAGE(CERTSIGN) WITHLABEL('BCOCA')
```

이 RACDCERT 명령은 사용자 'TELLER5'를 위한 사용자 인증서를 발행하는 데 사용할 수 있는 CA 인증서를 작성합니다. 예를 들면, 다음과 같습니다.

```
RACDCERT ID(TELLER5) GENCERT SUBJECTSDN(CN('Teller5') O('BCO') C('US'))
```

```
WITHLABEL('Teller5') SIGNWITH(CERTAUTH LABEL('BCOCA'))
KEYUSAGE(HANDSHAKE DATAENCRYPT DOCSIGN)
```

설치에는 CA 인증서를 선택하고 작성하기 위한 프로시저뿐만 아니라 인증서를 발행하고 이를 관련 시스템에 분배하기 위한 프로시저가 있습니다.

이러한 인증서를 내보내고 가져올 때 Advanced Message Security에는 다음이 필요합니다.

- CA 인증서(체인).
- 송신 사용자 인증서 및 해당 개인 키.

RACF를 사용 중인 경우, RACDCERT EXPORT 명령은 인증서를 데이터 세트에 내보내는 데 사용할 수 있고, RACDCERT ADD 명령은 인증서를 데이터 세트로부터 가져오는 데 사용할 수 있습니다. 이들 및 기타 RACDCERT 명령에 대한 자세한 정보는 *z/OS: Security Server RACF Command Language Reference*의 [RACDCERT \(RACF 디지털 인증서 관리\)](#) 를 참조하십시오.

이 경우 인증서는 큐 관리자 BNK6 및 BNK7을 실행 중인 z/OS 시스템에서 필요합니다.

이 예에서 송신 인증서는 BNK6을 실행 중인 z/OS 시스템에 가져오기되어야 하고 CA 인증서는 BNK7을 실행 중인 z/OS 시스템에 가져오기되어야 합니다. 인증서가 가져오기되면 사용자 인증서에는 TRUST 속성이 필요합니다. RACDCERT ALTER 명령은 TRUST 속성을 인증서에 추가하는 데 사용할 수 있습니다. 예를 들어, BNK6에서:

```
RACDCERT ID(TELLER5) ALTER (LABEL('Teller5')) TRUST
```

인증서를 관련 키 링에 연결

필수 인증서가 작성되거나 가져오기되고, 신뢰되는 것으로 설정될 때 이들은 BNK6 및 BNK7을 실행 중인 z/OS 시스템에서 적합한 사용자 키 링에 연결되어야 합니다.

키 링을 작성하려면 BNK6에서 RACDCERT ADDRING 명령을 사용하십시오.

```
RACDCERT ID(TELLER5) ADDRING(drq.ams.keyring)
```

이는 BNK6에서 송신 사용자를 위한 키 링을 작성합니다. 키 링 이름 drq.ams.keyring은 필수이고 이름은 대소문자를 구분함을 유의하십시오.

BNK7에서:

```
RACDCERT ID(WMQBNK7) ADDRING(drq.ams.keyring)
```

이는 BNK7에서 Advanced Message Security 태스크에 대한 키 링을 작성합니다. BNK7에서 'TELLER5'에 대한 사용자 키 링이 필요하지 않습니다.

키 링이 작성될 때 관련 인증서를 연결할 수 있습니다.

BNK6에서:

```
RACDCERT ID(TELLER5) CONNECT(ID(TELLER5) LABEL('Teller5')
RING(drq.ams.keyring) DEFAULT USAGE(PERSONAL))
```

BNK7에서:

```
RACDCERT ID(WMQBNK7) CONNECT(CERTAUTH LABEL('BCOCA')
RING(drq.ams.keyring))
```

송신 사용자 인증서는 DEFAULT로서 연결되어야 합니다. 송신 사용자에 해당 drq.ams.keyring에 둘 이상의 인증서가 있는 경우에는 서명 용도를 위해 기본 인증서가 사용됩니다.

큐 관리자가 중지되고 다시 시작되거나 z/OS MODIFY 명령이 Advanced Message Security 인증서 구성을 새로 고치기 위해 사용될 때까지 인증서의 작성 및 수정이 Advanced Message Security 에서 인식되지 않습니다. 예를 들면, 다음과 같습니다.

BNK6에서:

```
F BNK6AMSM,REFRESH,KEYRING
```

BNK7에서:

```
F BNK7AMSM,REFRESH,KEYRING
```

Advanced Message Security 정책 작성

이 예에서 무결성 보호된 메시지는 사용자 'TELLER5'로서 실행 중인 애플리케이션에 의해 BNK6에서 리모트 큐 FIN.XFER.Q7에 놓여지고, 사용자 'FINADM2'로서 실행 중인 애플리케이션에 의해 BNK7에서 로컬 큐 FIN.RCPT.Q7에서 검색되므로, 두 개의 Advanced Message Security 정책이 필요합니다.

Advanced Message Security 정책은 [메시지 보안 정책 유틸리티\(CSQ0UTIL\)](#)에 문서화된 CSQ0UTIL 유틸리티를 사용하여 작성됩니다.

BNK6에서 리모트 큐에 대해 무결성 정책을 정의하려면 CSQ0UTIL 유틸리티를 사용하여 다음 명령을 실행하십시오.

```
setmqsp1 -m BNK6 -p FIN.XFER.Q7 -s MD5 -a CN=Teller5,O=BCO,C=US
```

이 정책에서 큐 관리자는 BNK6로 식별됩니다. 정책 이름 및 연관된 큐는 FIN.XFER.Q7입니다. 송신자의 서명을 생성하는 데 사용되는 알고리즘은 MD5이고 송신 사용자의 식별 이름(DN)은 'CN=Teller5,O=BCO,C=US'입니다.

또한 BNK7에서 로컬 큐에 대해 무결성 정책을 정의하려면 CSQ0UTIL 유틸리티를 사용하여 다음 명령을 실행하십시오.

```
setmqsp1 -m BNK7 -p FIN.RCPT.Q7 -s MD5 -a CN=Teller5,O=BCO,C=US
```

이 정책에서 큐 관리자는 BNK7로 식별됩니다. 정책 이름 및 연관된 큐는 FIN.RCPT.Q7입니다. 송신자의 서명에 예상되는 알고리즘은 MD5이고, 송신 사용자의 식별 이름(DN)은 'CN=Teller5,O=BCO,C=US'로 예상됩니다.

두 개의 정책을 정의한 후에 BNK6 및 BNK7 큐 관리자를 재시작하거나 z/OS **MODIFY** 명령을 사용하여 Advanced Message Security 정책 구성을 새로 고치십시오. 예를 들면, 다음과 같습니다.

BNK6에서:

```
F BNK6AMSM,REFRESH,POLICY
```

BNK7에서:

```
F BNK7AMSM,REFRESH,POLICY
```

z/OS에서 개인정보 보호된 메시지의 리모트 큐링

이 예는 두 개의 서로 다른 큐 관리자가 관리하는 큐에 개인정보 보호된 메시지를 송신하고 수신하는 데 필요한 Advanced Message Security 정책 및 인증서를 설명합니다. 두 개의 큐 관리자는 동일한 z/OS 시스템 또는 다른 z/OS 시스템에서 실행 중이거나 하나의 큐 관리자가 Advanced Message Security를 실행하는 분산 시스템에 있을 수 있습니다.

예 큐 관리자 및 큐는 다음과 같습니다.

```
BNK6      - Sending queue manager
BNK7      - Recipient queue manager
FIN.XFER.Q7 - Remote queue on BNK6
FIN.RCPT.Q7 - Local queue on BNK7
```

참고: 이 예의 경우 BNK6 및 BNK7은 이름이 같은 z/OS 시스템에서 실행 중인 큐 관리자입니다.

다음 사용자가 사용됩니다.

```
WMQBNK6 - AMS task user on BNK6
WMQBNK7 - AMS task user on BNK7
TELLER5 - Sending user on BNK6
FINADM2 - Recipient user on BNK7
```

이 시나리오를 구성하기 위한 단계는 다음과 같습니다.

사용자 인증서 작성

이 예에서 두 개의 사용자 인증서가 필요합니다. 이들은 메시지에 서명하기 위해 필요한 송신 사용자의 인증서 및 메시지 데이터를 암호화하고 복호화하기 위해 필요한 수신자의 사용자 인증서입니다. 송신 사용자는 'TELLER5'이고 수신 사용자는 'FINADM2'입니다.

인증 기관(CA) 인증서 또한 필요합니다. CA 인증서는 사용자의 인증서를 발행한 권한의 인증서입니다. 이는 인증서의 체인일 수 있습니다. 그런 경우 체인의 모든 인증서는 Advanced Message Security 태스크 사용자의 키 링에서 필수입니다. 이 경우 사용자 WMQBNK7입니다.

CA 인증서는 RACF RACDCERT 명령을 사용하여 작성할 수 있습니다. 이 인증서는 사용자 인증서를 발행하는 데 사용됩니다. 예를 들면, 다음과 같습니다.

```
RACDCERT CERTAUTH GENCERT SUBJECTSDN(CN('BCOCA') O('BCO') C('US'))
KEYUSAGE(CERTSIGN) WITHLABEL('BCOCA')
```

이 RACDCERT 명령은 사용자 'TELLER5' 및 'FINADM2'를 위한 사용자 인증서를 발행하는 데 사용할 수 있는 CA 인증서를 작성합니다. 예를 들면, 다음과 같습니다.

```
RACDCERT ID(TELLER5) GENCERT SUBJECTSDN(CN('Teller5') O('BCO') C('US'))
WITHLABEL('Teller5') SIGNWITH(CERTAUTH LABEL('BCOCA'))
KEYUSAGE(HANDSHAKE DATAENCRYPT DOCSIGN)
```

```
RACDCERT ID(FINADM2) GENCERT SUBJECTSDN(CN('FinAdm2') O('BCO') C('US'))
WITHLABEL('FinAdm2') SIGNWITH(CERTAUTH LABEL('BCOCA'))
KEYUSAGE(HANDSHAKE DATAENCRYPT DOCSIGN)
```

설치에는 CA 인증서를 선택하고 작성하기 위한 프로시저뿐만 아니라 인증서를 발행하고 이를 관련 시스템에 분배하기 위한 프로시저가 있습니다.

이러한 인증서를 내보내고 가져올 때 Advanced Message Security에는 다음이 필요합니다.

- CA 인증서(체인).
- 송신 사용자 인증서 및 해당 개인 키.
- 수신 사용자 인증서 및 해당 개인 키.

RACF를 사용 중인 경우, RACDCERT EXPORT 명령은 인증서를 데이터 세트에 내보내는 데 사용할 수 있고, RACDCERT ADD 명령은 인증서를 데이터 세트로부터 가져오는 데 사용할 수 있습니다.

이러한 RACDCERT 명령 및 기타 RACDCERT 명령에 대한 자세한 정보는 *z/OS: Security Server RACF Command Language Reference*의 [RACDCERT \(RACF 디지털 인증서 관리\)](#)를 참조하십시오.

이 경우 인증서는 큐 관리자 BNK6 및 BNK7을 실행 중인 z/OS 시스템에서 필요합니다.

이 예에서 송신 및 수신 인증서는 BNK6을 실행 중인 z/OS 시스템에 가져오기되어야 하고 CA 및 수신 인증서는 BNK7을 실행 중인 z/OS 시스템에 가져오기되어야 합니다. 인증서가 가져오기되면 사용자 인증서에는 TRUST 속성이 필요합니다. RACDCERT ALTER 명령은 TRUST 속성을 인증서에 추가하는 데 사용할 수 있습니다. 예를 들면, 다음과 같습니다.

BNK6에서:

```
RACDCERT ID(TELLER5) ALTER (LABEL('Teller5')) TRUST
RACDCERT ID(FINADM2) ALTER (LABEL('FinAdm2')) TRUST
```

BNK7에서:

```
RACDCERT ID(FINADM2) ALTER (LABEL('FinAdm2')) TRUST
```

인증서를 관련 키 링에 연결

필수 인증서가 작성되거나 가져오기되고, 신뢰되는 것으로 설정될 때 이들은 BNK6 및 BNK7을 실행 중인 z/OS 시스템에서 적합한 사용자 키 링에 연결되어야 합니다.

키 링을 작성하려면 RACDCERT ADDRING 명령을 사용하십시오.

BNK6에서:

```
RACDCERT ID(WMQBNK6) ADDRING(drq.ams.keyring)
RACDCERT ID(TELLER5) ADDRING(drq.ams.keyring)
```

이는 Advanced Message Security 태스크 사용자를 위한 키 링을 작성하고 BNK6에서 송신 사용자를 위한 키 링을 작성합니다. 키 링 이름 drq.ams.keyring은 필수이고 이름은 대소문자를 구분함을 유의하십시오.

BNK7에서:

```
RACDCERT ID(WMQBNK7) ADDRING(drq.ams.keyring)
RACDCERT ID(FINADM2) ADDRING(drq.ams.keyring)
```

이는 Advanced Message Security 태스크 사용자를 위한 키 링을 작성하고 BNK7에서 수신 사용자를 위한 키 링을 작성합니다.

키 링이 작성될 때 관련 인증서를 연결할 수 있습니다.

BNK6에서:

```
RACDCERT ID(WMQBNK6) CONNECT(ID(FINADM2) LABEL('FinAdm2')
RING(drq.ams.keyring) USAGE(SITE))

RACDCERT ID(TELLER5) CONNECT(ID(TELLER5) LABEL('Teller5')
RING(drq.ams.keyring) DEFAULT USAGE(PERSONAL))
```

BNK7에서:

```
RACDCERT ID(WMQBNK7) CONNECT(CERTAUTH LABEL('BCOCA')
RING(drq.ams.keyring))

RACDCERT ID(FINADM2) CONNECT(ID(FINADM2) LABEL('FinAdm2')
RING(drq.ams.keyring) DEFAULT USAGE(PERSONAL))
```

송신 및 수신 사용자 인증서는 DEFAULT로서 연결되어야 합니다. 사용자에게 해당 drq.ams.keyring에 둘 이상의 인증서가 있는 경우에는 서명 및 암호화/복호화 용도를 위해 기본 인증서가 사용됩니다.

BNK6에서 수신 사용자의 인증서는 또한 USAGE(SITE)와 함께 Advanced Message Security 태스크 사용자의 키 링에 연결되어야 합니다. 이는 고급 메시지 보안 태스크에 메시지 데이터를 암호화할 때 수신인의 공개 키가 필요하기 때문입니다. USAGE(SITE)는 개인 키가 키 링크에서 액세스 가능하지 못하게 만듭니다.

큐 관리자가 중지되고 다시 시작되거나 z/OS MODIFY 명령이 Advanced Message Security 인증서 구성을 새로 고치기 위해 사용될 때까지 인증서의 작성 및 수정이 Advanced Message Security 에서 인식되지 않습니다. 예를 들면, 다음과 같습니다.

BNK6에서:

```
F BNK6AMSM,REFRESH,KEYRING
```

BNK7에서:

```
F BNK7AMSM,REFRESH,KEYRING
```

Advanced Message Security 정책 작성

이 예에서 개인정보 보호된 메시지는 사용자 'TELLER5'로서 실행 중인 애플리케이션에 의해 BNK6에서 리모트 큐 FIN.XFER.Q7에 놓여지고, 사용자 'FINADM2'로서 실행 중인 애플리케이션에 의해 BNK7에서 로컬 큐 FIN.RCPT.Q7에서 검색되므로, 두 개의 Advanced Message Security 정책이 필요합니다.

Advanced Message Security 정책은 [메시지 보안 정책 유틸리티\(CSQ0UTIL\)](#)에 문서화된 CSQ0UTIL 유틸리티를 사용하여 작성됩니다.

BNK6에서 리모트 큐에 대해 개인정보 정책을 정의하려면 CSQ0UTIL 유틸리티를 사용하여 다음 명령을 실행하십시오.

```
setmqsp1 -m BNK6 -p FIN.XFER.Q7 -s SHA1 -e 3DES -a CN=Teller5,O=BCO,C=US -r  
CN=FinAdm2,O=BCO,C=US
```

이 정책에서 큐 관리자는 BNK6로 식별됩니다. 정책 이름 및 연관된 큐는 FIN.XFER.Q7입니다. 송신자의 서명을 생성하는 데 사용된 알고리즘은 SHA1이고 송신 사용자의 식별 이름(DN)은 'CN=Teller5,O=BCO,C=US'이고, 수신 사용자는 'CN=FinAdm2,O=BCO,C=US'입니다. 메시지 데이터를 암호화하는 데 사용되는 알고리즘은 3DES입니다.

또한 BNK7에서 로컬 큐에 대해 개인정보 정책을 정의하려면 CSQ0UTIL 유틸리티를 사용하여 다음 명령을 실행하십시오.

```
setmqsp1 -m BNK7 -p FIN.RCPT.Q7 -s SHA1 -e 3DES -a CN=Teller5,O=BCO,C=US -r  
CN=FinAdm2,O=BCO,C=US
```

이 정책에서 큐 관리자는 BNK7로 식별됩니다. 정책 이름 및 연관된 큐는 FIN.RCPT.Q7입니다. 송신자의 서명에 예상되는 사용된 알고리즘은 SHA1이고 송신 사용자의 식별 이름(DN)은 'CN=Teller5,O=BCO,C=US'으로 예상되고, 수신 사용자는 'CN=FinAdm2,O=BCO,C=US'입니다. 메시지 데이터를 복호화하는 데 사용되는 알고리즘은 3DES입니다.

두 개의 정책을 정의한 후에 BNK6 및 BNK7 큐 관리자를 재시작하거나 z/OS **MODIFY** 명령을 사용하여 Advanced Message Security 정책 구성을 새로 고치십시오. 예를 들면, 다음과 같습니다.

BNK6에서:

```
F BNK6AMSM,REFRESH,POLICY
```

BNK7에서:

```
F BNK7AMSM,REFRESH,POLICY
```

Java 클라이언트가 있는 AMS 에 대한 빠른 시작 안내서

클라이언트 바인딩을 사용하여 연결하는 Java 애플리케이션에 대한 메시지 보안을 제공하도록 Advanced Message Security 를 신속하게 구성하려면 이 안내서를 사용하십시오. 이를 완료할 때쯤 사용자 ID를 확인하기 위한 키 저장소를 작성하게 될 것이고 큐 관리자의 서명/암호화 정책을 정의했을 것입니다.

시작하기 전에

빠른 시작 안내서([Windows](#) 또는 [UNIX](#))에 설명된 대로 적절한 컴포넌트가 설치되어 있는지 확인하십시오.

1. 큐 관리자 및 큐 작성

이 태스크 정보

다음 모든 예에서는 애플리케이션 간 메시지를 전달하기 위해 이름이 TEST.Q인 큐를 사용합니다. Advanced Message Security는 표준 IBM MQ 인터페이스를 통해 IBM MQ 인프라에 입력하는 지점에서 메시지에 서명하고 암호화하기 위해 인터셉터를 사용합니다. 이 기본 설정은 IBM MQ에서 수행되고 다음 단계에서 구성됩니다.

프로시저

1. 큐 관리자 작성

```
crtmqm QM_VERIFY_AMS
```

2. 큐 관리자 시작

```
strmqm QM_VERIFY_AMS
```

3. 다음 명령을 QM_VERIFY_AMS 큐 관리자의 **runmqsc**에 입력하여 리스너를 작성하고 시작하십시오.

```
DEFINE LISTENER(AMS.LSTR) TRPTYPE(TCP) PORT(1414) CONTROL(QMGR)  
START LISTENER(AMS.LSTR)
```

4. 다음 명령을 QM_VERIFY_AMS 큐 관리자의 **runmqsc**에 입력하여 애플리케이션이 연결할 채널을 작성하십시오.

```
DEFINE CHANNEL(AMS.SVRCONN) CHLTYPE(SVRCONN)
```

5. 다음 명령을 큐 관리자 QM_VERIFY_AMS의 **runmqsc**에 입력하여 이름이 TEST.Q인 큐를 작성하십시오.

```
DEFINE QLOCAL(TEST.Q)
```

결과

프로시저가 성공적으로 완료되면 **runmqsc**에 입력된 다음 명령이 TEST.Q에 대한 세부사항을 표시합니다.

```
DISPLAY Q(TEST.Q)
```

2. 사용자 작성 및 권한 부여

이 태스크 정보

이 시나리오에는 2명의 사용자가 나타납니다. 송신자 alice와 수신자 bob입니다. 애플리케이션 큐를 사용하려면 이러한 사용자에게는 이를 사용할 권한이 부여되어야 합니다. 또한 이 시나리오에 정의된 보호 정책을 성공적으로 사용하기 위해 이러한 사용자에게는 일부 시스템 큐에 대한 액세스가 부여되어야 합니다. **setmqaut** 명령에 대한 자세한 정보는 **setmqaut**를 참조하십시오.

프로시저

1. 사용자 플랫폼의 빠른 시작 안내서(Windows 또는 UNIX)에 설명된 대로 두 사용자를 작성하십시오.
2. 사용자에게 큐 관리자에 연결하고 큐에 대해 작업할 수 있는 권한을 부여

```
setmqaut -m QM_VERIFY_AMS -t qmgr -p alice -p bob +connect +inq  
setmqaut -m QM_VERIFY_AMS -n TEST.Q -t queue -p alice +put  
setmqaut -m QM_VERIFY_AMS -n TEST.Q -t queue -p bob +get +inq +browse
```

3. 또한 두 사용자가 시스템 정책 큐를 찾아서 메시지를 오류 큐에 넣도록 허용해야 합니다.

```
setmqaut -m QM_VERIFY_AMS -t queue -n SYSTEM.PROTECTION.POLICY.QUEUE -p alice -p bob +browse
setmqaut -m QM_VERIFY_AMS -t queue -n SYSTEM.PROTECTION.ERROR.QUEUE -p alice -p bob +put
```



주의: IBM MQ 는 모든 경우에 SYSTEM.PROTECTION.POLICY.QUEUE 의 정책 세부사항에 대한 레코드를 찾아볼 필요가 없도록 정책을 캐싱하여 성능을 최적화합니다.

IBM MQ가 사용 가능한 모든 정책을 캐시하지는 않습니다. 정책 수가 많으면 IBM MQ가 제한된 수의 정책을 캐시합니다. 따라서 큐 관리자에 적은 수의 정책이 정의되어 있는 경우 SYSTEM.PROTECTION.POLICY.QUEUE에 찾아보기 옵션을 제공할 필요가 없습니다.

그러나 많은 수의 정책이 정의되어 있거나 이전 클라이언트를 사용 중인 경우 이 큐에 대한 찾아보기 권한을 부여해야 합니다. SYSTEM.PROTECTION.ERROR.QUEUE는 AMS 코드에서 생성된 오류 메시지를 넣는 데 사용됩니다. 이 큐에 대한 넣기(Put) 권한은 오류 메시지를 큐에 넣으려고 할 때만 확인됩니다. AMS 보호 큐에서 메시지를 가져오거나 넣으려고 할 때는 큐에 대한 넣기(Put) 권한이 확인되지 않습니다.

결과

그러면 사용자가 작성되고 사용자에게 필요한 권한이 부여됩니다.

다음에 수행할 작업

단계가 올바르게 수행되었는지 확인하려면 540 페이지의 『7. 설정 테스트』 섹션에 설명된 대로 JmsProducer 및 JmsConsumer 샘플을 사용하십시오.

3. 키 데이터베이스 및 인증서 작성

이 태스크 정보

메시지를 인터셉터로 암호화하려면 송신 사용자의 공개 키가 필요합니다. 따라서 공개 및 개인 키에 매핑된 사용자의 키 데이터베이스가 작성되어야 합니다. 사용자 및 애플리케이션이 여러 컴퓨터에 분산되어 있는 실제 시스템에서는 각 사용자는 고유의 개인용 키 저장소를 가지고 있을 것입니다. 마찬가지로, 이 안내서에서는 alice와 bob을 위한 키 데이터베이스를 작성하고 이들 간에 사용자 인증서를 공유합니다.

참고: 이 안내서에서는 클라이언트 바인딩을 사용하여 연결하는 Java로 작성된 샘플 애플리케이션을 사용합니다. 로컬 바인딩을 사용하는 Java 애플리케이션 또는 C 애플리케이션을 사용할 계획이면 **runmqakm** 명령을 사용하여 CMS 키 저장소 및 인증서를 작성해야 합니다. **빠른 시작 안내서(Windows 또는 UNIX)**에 표시되어 있습니다.

프로시저

1. 키 저장소를 작성할 디렉토리를 작성하십시오(예: /home/alice/.mqs). 사용자 플랫폼의 **빠른 시작 안내서(Windows 또는 UNIX)**에서 사용하는 것과 같은 디렉토리에 작성할 수 있습니다.

참고: 이 디렉토리는 다음 단계에서 *keystore-dir*로 불립니다.

2. 암호화에 사용하기 위해 alice 사용자를 식별하는 새 키 저장소 및 인증서를 작성하십시오.

참고: **keytool** 명령은 JRE의 일부입니다.

```
keytool -genkey -alias Alice_Java_Cert -keyalg RSA -keystore keystore-dir/keystore.jks
-storepass passw0rd
-dname "CN=alice, O=IBM, C=GB" -keypass passw0rd
```

참고:

- *keystore-dir*에 공백이 포함된 경우에는 키 저장소의 전체 이름 주변에 따옴표를 넣어야 합니다.
- 키 저장소를 보안 설정하기 위해 강력한 비밀번호를 사용하는 것이 권장됩니다.
- 이 안내서의 용도상 인증 기관을 사용하지 않고 작성할 수 있는 자체 서명 인증서를 사용 중입니다. 프로덕션 시스템의 경우 자체 서명 인증서를 사용하지 않고 대신에 인증 기관이 서명한 인증서에 의존하는 것이 바람직합니다.

- **alias** 매개변수는 인터셉터가 필수 정보를 수신하기 위해 찾아볼 인증서의 이름을 지정합니다.
- **dname** 매개변수는 **식별 이름(DN)**의 세부사항을 지정하고 이는 각 사용자에게 고유의 해야 합니다.

3. UNIX에서 키 저장소가 판독 가능한지 확인하십시오.

```
chmod +r keystore-dir/keystore.jks
```

4. 사용자 bob에 대해 1-4단계를 반복하십시오.

결과

2명의 사용자 alice 및 bob은 이제 각각 자체 서명 인증서가 있습니다.

4. *keystore.conf* 작성

이 태스크 정보

Advanced Message Security 인터셉터로 키 데이터베이스 및 인증서가 있는 디렉토리를 가리켜야 합니다. 이는 해당 정보를 일반 텍스트 양식으로 보유하는 *keystore.conf* 파일을 통해 수행됩니다. 각 사용자에게는 별도의 *keystore.conf* 파일이 있어야 합니다. 이 단계는 alice 및 bob 둘 모두에 대해 수행되어야 합니다.

예

이 시나리오의 경우 alice의 *keystore.conf*의 콘텐츠는 다음과 같습니다.

```
JKS.keystore = keystore-dir/keystore
JKS.certificate = Alice_Java_Cert
JKS.encrypted = no
JKS.keystore_pass = passw0rd
JKS.key_pass = passw0rd
JKS.provider = IBMJCE
```

이 시나리오의 경우 bob의 *keystore.conf*의 콘텐츠는 다음과 같습니다.

```
JKS.keystore = keystore-dir/keystore
JKS.certificate = Bob_Java_Cert
JKS.encrypted = no
JKS.keystore_pass = passw0rd
JKS.key_pass = passw0rd
JKS.provider = IBMJCE
```

참고:

- 키 저장소 파일의 경로는 파일 확장자 없이 제공되어야 합니다.
- 빠른 시작 안내서 (Windows 또는 UNIX)의 지시사항을 따랐기 때문에 이미 *keystore.conf* 파일이 있는 경우 기존 파일을 편집하여 이러한 행을 추가할 수 있습니다.
- 자세한 정보는 547 페이지의 『[AMS에 대한 키 저장소 구성 파일 \(keystore.conf\)의 구조](#)』의 내용을 참조하십시오.

5. 인증서 공유

이 태스크 정보

각 사용자가 서로를 성공적으로 식별할 수 있도록 두 개의 키 저장소 간에 인증서를 공유합니다. 이는 각 사용자의 인증서를 추출한 후 다른 사용자의 키 저장소로 가져오는 방식으로 수행됩니다.

참고: 추출 및 내보내기라는 용어는 서로 다른 인증 도구에서 서로 다르게 사용됩니다. 예를 들어, IBM GSKit **strmqikm** 명령(ikeyman) 도구는 인증서(공개 키) 추출과 개인 키 내보내기를 구분합니다. 이 구분은 두 옵션을 모두 제공하는 도구에 아주 중요합니다. 실수로 내보내기를 사용하면 개인 키가 누출되어 애플리케이션이 완전히 훼손될 수 있기 때문입니다. 구분이 이렇게 중요하므로 IBM MQ 문서에서는 이들 용어를 일관되게 사용하도록 노력합니다. 그러나 Java keytool은 공개 키만 추출하는 **exportcert** 명령행 옵션을 제공합니다. 이런 이유로 다음 프로시저에서는 인증서 내보내기를 언급할 때 **exportcert** 옵션을 사용합니다.

프로시저

1. alice를 식별하는 인증서를 추출하십시오.

```
keytool -exportcert -keystore alice-keystore-dir/keystore.jks -storepass passwd0rd  
-alias Alice_Java_Cert -file alice-keystore-dir/Alice_Java_Cert.cer
```

2. alice를 식별하는 인증서를 bob이 사용할 키 저장소로 가져오십시오. 프롬프트되면 이 인증서를 신뢰할 것임을 나타내십시오.

```
keytool -importcert -file alice-keystore-dir/Alice_Java_Cert.cer -alias Alice_Java_Cert  
-keystore bob-keystore-dir/keystore.jks -storepass passwd0rd
```

3. bob에 대해 단계를 반복하십시오.

결과

두 명의 사용자 alice 및 bob은 이제 자체 서명 인증서를 작성하고 공유한 서로를 성공적으로 식별할 수 있습니다.

다음에 수행할 작업

해당 세부사항을 인쇄하는 다음 명령을 실행하여 인증서가 키 저장소에 있는지 확인하십시오.

```
keytool -list -keystore bob-keystore-dir/keystore.jks -storepass passwd0rd -alias Alice_Java_Cert  
keytool -list -keystore alice-keystore-dir/keystore.jks -storepass passwd0rd -alias Bob_Java_Cert
```

6. 큐 정책 정의

이 태스크 정보

큐 관리자가 작성되고 인터프리터가 메시지 및 액세스 암호화 키를 방해할 준비가 된 상태에서 `setmqsp1` 명령을 사용하여 QM_VERIFY_AMS에서 보호 정책 정의를 시작할 수 있습니다. 이 명령에 대한 자세한 정보는 `setmqsp1`의 내용을 참조하십시오. 각 정책 이름은 적용되는 큐 이름과 동일해야 합니다.

예

이는 TEST.Q 큐에 정의되고, SHA1 알고리즘을 사용하여 alice 사용자가 서명하고 bob 사용자에게 대해 256비트 AES 알고리즘을 사용하여 암호화된 정책의 예입니다.

```
setmqsp1 -m QM_VERIFY_AMS -p TEST.Q -s SHA1 -a "CN=alice,O=IBM,C=GB" -e AES256 -r  
"CN=bob,O=IBM,C=GB"
```

참고: DN은 키 데이터베이스로부터 각각의 사용자의 인증서에 명시된 것과 정확하게 일치한다.

다음에 수행할 작업

사용자가 정의한 정책을 확인하려면 다음 명령을 실행하십시오.

```
dspmqsp1 -m QM_VERIFY_AMS
```

`setmqsp1` 명령의 세트로서 정책 세부사항을 인쇄하려면 `-export` 플래그입니다. 이는 이미 정의된 정책을 저장할 수 있게 해줍니다.

```
dspmqsp1 -m QM_VERIFY_AMS -export >restore_my_policies.bat
```

7. 설정 테스트

시작하기 전에

사용 중인 Java 버전에 제한 없는 JCE 정책 파일이 설치되었는지 확인하십시오.

참고: IBM MQ에 제공된 Java의 버전에 이미 이러한 정책 파일이 있습니다. 이는 `MQ_INSTALLATION_PATH/java/bin`에서 찾을 수 있습니다.

이 태스크 정보

다른 사용자 하에서 다른 프로그램을 실행하여 애플리케이션이 제대로 구성되었는지 확인할 수 있습니다. 여러 다른 사용자가 프로그램을 실행하는 데 관한 세부 정보는 사용자 플랫폼의 [빠른 시작 안내서\(Windows 또는 UNIX\)](#)를 참조하십시오.

프로시저

1. 이러한 JMS 샘플 애플리케이션을 실행하려면 **IBM MQ classes for JMS**에서 사용하는 환경 변수에 표시된 대로 사용자 플랫폼에 대한 **CLASSPATH** 설정을 사용하여 샘플 디렉토리가 포함되도록 하십시오.
2. alice 사용자로서 샘플 애플리케이션을 사용하여 클라이언트로서 연결하여 메시지를 넣으십시오.

```
java JmsProducer -m QM_VERIFY_AMS -d TEST.Q -h localhost -p 1414 -l AMS.SVRCONN
```

3. bob 사용자로서 샘플 애플리케이션을 사용하여 클라이언트로서 연결하여 메시지를 가져오십시오.

```
java JmsConsumer -m QM_VERIFY_AMS -d TEST.Q -h localhost -p 1414 -l AMS.SVRCONN
```

결과

애플리케이션이 두 사용자에게 모두 적절하게 구성된 경우 사용자 alice의 메시지가 bob이 가져오기 애플리케이션을 실행할 때 표시됩니다.

리모트 큐 보호

리모트 큐를 완전히 보호하려면 메시지를 전송하는 리모트 큐 및 로컬 큐에서 정책을 설정해야 합니다.

메시지가 리모트 큐에 놓을 때, Advanced Message Security는 조작을 인터셉트하고 리모트 큐에 설정된 정책에 따라 메시지를 처리합니다. 예를 들어, 암호화 정책의 경우 메시지는 이를 처리하기 위해 IBM MQ에 전달되기 전에 암호화됩니다. Advanced Message Security가 리모트 큐에 놓인 메시지를 처리한 후에 IBM MQ는 이를 연관된 전송 큐에 놓고 이를 대상 큐 관리자 및 대상 큐에 전달합니다.

GET 조작이 로컬 큐에서 수행되면 Advanced Message Security는 로컬 큐에 설정된 정책에 따라 메시지를 디코딩하려고 시도합니다. 조작이 성공하려면 메시지를 복호화하는 데 사용된 정책은 이를 암호화하는 데 사용된 것과 동일해야 합니다. 불일치가 있으면 메시지가 거부됩니다.

어떤 이유로든 두 정책이 동시에 설정될 수는 없는 경우에는 스테이지형 롤아웃 지원이 제공됩니다. 정책은 관용 플래그가 있는 로컬 큐에 설정할 수 있고, 이는 큐와 연관된 정책은 큐로부터 메시지를 검색하려는 시도가 보안 정책 세트가 없는 메시지와 관련될 때 무시될 수 있음을 나타냅니다. 이 경우 GET은 메시지를 복호화하려고 시도하지만 암호화되지 않은 메시지가 전달될 수 있도록 허용할 것입니다. 이 방법으로 리모트 큐에 대한 정책은 로컬 큐를 보호하고 테스트한 후에 설정할 수 있습니다.

알아두기: Advanced Message Security 롤아웃이 완료된 후에 관용 플래그를 제거하십시오.

관련 참조

[setmqspl\(보안 정책 설정\)](#)

IBM Integration Bus를 사용하여 보호된 메시지 라우팅

Advanced Message Security는 IBM Integration Bus 또는 WebSphere Message Broker 8.0.0.1 이상이 설치된 인프라에서 메시지를 보호할 수 있습니다. IBM Integration Bus 환경에서 보안을 적용하기 전에 두 제품 모두의 특성을 이해해야 합니다.

이 태스크 정보

Advanced Message Security는 메시지 페이로드(payload)의 엔드-투-엔드 보안을 제공합니다. 이는 메시지의 유효한 송신자와 수신자로 지정된 당사자만이 이를 생성하거나 수신할 수 있음을 의미합니다. 이는 IBM Integration Bus를 통해 메시지 플로우를 보안 설정하기 위해서 IBM Integration Bus가 메시지의 콘텐츠를 모른 채로 처리하거나 의미합니다(시나리오 1) 권한 있는 사용자가 메시지를 받거나 전송할 수 있도록 만들 수 있음(시나리오 2)을 의미합니다.

시나리오 1 - 통합 버스가 메시지 콘텐츠를 볼 수 없음

시작하기 전에

IBM Integration Bus가 기존 큐 관리자에 연결되게 해야 합니다. 다음의 명령에서 *QMgrName*을 이 기존 큐 관리자 이름으로 바꾸십시오.

이 태스크 정보

이 시나리오에서 Alice는 보호된 메시지를 입력 큐 QIN에 넣습니다. 메시지 특성 *routeTo*를 기반으로 메시지가 *bob*(QBOB),¹(QCECIL) 또는 기본(QDEF) 큐로 라우팅됩니다. Advanced Message Security는 메시지 페이로드만을 보호하고 해당 헤더나 특성은 보호하지 않고 보호되지 않은 상태로 남아 있고 IBM Integration Bus에 의해 판독될 수 있으므로 라우팅이 가능합니다. Advanced Message Security는 *alice*, *bob* 및 *cecil*에 의해서만 사용 됩니다. IBM Integration Bus에 대해 설치하거나 구성할 필요가 없습니다.

IBM Integration Bus는 메시지를 복호화하려는 시도를 피하기 위해 보호되지 않는 알리어스 큐로부터 보호된 메시지를 받습니다. 보호된 큐를 직접 사용할 계획이었으면 메시지는 복호화 불가능한 것으로서 DEAD LETTER 큐에 놓일 것입니다. 메시지는 IBM Integration Bus에 의해 라우팅되고 대상 큐에 변경되지 않은 상태로 도착합니다. 그러므로 이는 여전히 원본 작성자(*bob* 및 *cecil* 둘 모두만이 *alice*가 전송한 메시지를 승인함)에 의해 서명되고 이전처럼 보호됩니다(*bob* 및 *cecil*만이 이를 읽을 수 있음). IBM Integration Bus는 라우팅된 메시지를 보호되지 않은 알리어스에 넣습니다. 수신인은 AMS가 메시지를 투명하게 복호화하는 보호된 출력 큐로부터 메시지를 검색합니다.

프로시저

1. **빠른 시작 안내서** ([Windows](#) 또는 [UNIX](#)) 에 설명된 대로 Advanced Message Security 를 사용하도록 *alice*, *bob* 및 *cecil* 을 구성하십시오.
다음 단계가 완료되었는지 확인하십시오.
 - 사용자 작성 및 권한 부여
 - 키 데이터베이스 및 인증서 작성
 - keystore.conf 작성
2. *bob* 및 *cecil*이 메시지에서 디지털 서명을 검사할 때 *alice*를 식별할 수 있도록 *alice*의 인증서를 이들에게 제공하십시오.
*alice*를 식별하는 인증서를 외부 파일로 추출한 다음 추출된 인증서를 *bob* 및 *cecil*의 키 저장소에 추가하여 이를 수행하십시오. **태스크 5. 빠른 시작 안내서 (Windows 또는 UNIX) 의 인증서 공유하기**
3. *alice*가 *bob* 및 *cecil*에 대해 암호화된 메시지를 전송할 수 있도록 *bob* 및 *cecil*의 인증서를 *alice*에게 제공하십시오.
이전 단계에 지정된 방법을 사용하여 이를 수행하십시오.
4. 큐 관리자에서 QIN, QBOB, QCECIL 및 QDEF라는 로컬 큐를 정의하십시오.

```
DEFINE QLOCAL(QIN)
```

5. QIN 큐에 대한 보안 정책을 적합한 구성으로 설정하십시오. QBOB, QCECIL 및 QDEF 큐에 동일한 설정을 사용하십시오.

¹ cecil

```
setmqspl -m QMgrName -p QIN -s SHA1 -a "CN=alice,O=IBM,C=GB"  
-e AES256 -r "CN=bob,O=IBM,C=GB" -r "CN=cecil,O=IBM,C=GB"
```

이 시나리오는 *alice*가 유일한 권한 있는 사용자이고 *bob*과 *cecil*이 수신인인 보안 정책을 가정합니다.

6. 로컬 큐 QIN, QBOB 및 QCECIL을 각각 참조하는 알리어스 큐 AIN, ABOB 및 ACECIL을 정의하십시오.

```
DEFINE QALIAS(AIN) TARGET(QIN)
```

7. 이전 단계에서 지정된 알리어스의 보안 구성이 존재하지 않는지 확인하십시오. 그렇지 않으면 해당 정책을 NONE으로 설정하십시오.

```
dspmqspl -m QMgrName -p AIN
```

8. IBM Integration Bus는 AIN 알리어스 큐에 도착하는 메시지를 메시지의 `routeTo` 특성에 따라 BOB, CECIL 또는 DEF 노드에 라우팅하기 위해 메시지 플로우를 작성합니다. 이를 수행하려면, 다음 단계를 따르십시오.
- a) IN이라는 MQInput 노드를 작성하고 AIN 알리어스를 해당 큐 이름으로 지정하십시오.
 - b) BOB, CECIL 및 DEF라는 MQOutput 노드를 작성하고 알리어스 큐 ABOB, ACECIL 및 ADEF를 각각의 큐 이름으로 지정하십시오.
 - c) 라우트 노드를 작성하고 이를 TEST라고 부르십시오.
 - d) IN 노드를 TEST 노드의 입력 터미널에 연결하십시오.
 - e) TEST 노드를 위한 *bob* 및 *cecil* 출력 터미널을 작성하십시오.
 - f) *bob* 출력 터미널을 BOB 노드에 연결하십시오.
 - g) *cecil* 출력 터미널을 CECIL 노드에 연결하십시오.
 - h) DEF 노드를 기본 출력 터미널에 연결하십시오.
 - i) 다음 규칙을 적용하십시오.

```
$Root/MQRFH2/usr/routeTo/text()="bob"  
$Root/MQRFH2/usr/routeTo/text()="cecil"
```

9. 메시지 플로우를 IBM Integration Bus 런타임 컴포넌트에 배치하십시오.
10. Alice 사용자로서 실행하여 *bob* 또는 *cecil* 값이 있는 `routeTo`라는 메시지 특성을 포함하는 메시지를 넣으십시오. **amqsstm** 샘플 애플리케이션을 실행하면 이를 수행할 수 있게 됩니다.

```
Sample AMQSSTMA start  
target queue is TEST.Q  
Enter property name  
routeTo  
Enter property value  
bob  
Enter property name  
  
Enter message text  
My Message to Bob  
Sample AMQSSTMA end
```

11. *bob* 사용자로서 실행하면 **amqsget** 샘플 애플리케이션을 사용하여 메시지를 큐 QBOB로부터 검색합니다.

결과

*alice*가 메시지를 QIN 큐에 넣으면 메시지가 보호됩니다. 이는 IBM Integration Bus에 의해 AIN 알리어스 큐로부터 보호된 양식으로 검색됩니다. IBM Integration Bus는 `routeTo` 특성을 읽어서(모든 특성처럼 이는 암호화되지 않음) 메시지를 라우트할 위치를 결정합니다. IBM Integration Bus는 메시지를 추가적인 보호를 피하기 위해 적합한 보호되지 않은 알리어스에 놓습니다. 큐로부터 *bob* 또는 *cecil*에 의해 수신되면 메시지를 복호화되고 디지털 서명이 확인됩니다.

이 태스크 정보

이 시나리오에서 개별 그룹은 메시지를 IBM Integration Bus에 보낼 수 있습니다. 또 다른 그룹은 IBM Integration Bus에 의해 작성된 메시지를 받을 권한이 있습니다. 당사자와 IBM Integration Bus 사이의 전송은 도청될 수 없습니다.

IBM Integration Bus는 보호 정책 및 인증서를 큐가 열릴 때에만 판독하므로 보호 정책을 업데이트한 후에 변경 사항을 적용하려면 실행 그룹을 다시 로드해야 함을 기억하십시오.

```
mqsireload execution-group-name
```

IBM Integration Bus가 메시지 페이로드를 읽거나 서명할 수 있는 권한 부여된 당사자로 간주되는 경우, IBM Integration Bus 서비스를 시작하는 사용자에게 대해 Advanced Message Security를 구성해야 합니다. 메시지를 큐에 넣고/가져오는 사용자나 IBM Integration Bus 애플리케이션을 작성하고 배치하는 사용자가 반드시 동일할 필요는 없음을 유의하십시오.

프로시저

1. **빠른 시작 안내서** (Windows 또는 UNIX)에 설명된 대로 Advanced Message Security를 사용하도록 *alice*, *bob*, *cecil* 및 *dave* 및 IBM Integration Bus 서비스 사용자를 구성하십시오.

다음 단계가 완료되었는지 확인하십시오.

- 사용자 작성 및 권한 부여
- 키 데이터베이스 및 인증서 작성
- keystore.conf 작성

2. *alice*, *bob*, *cecil* 및 *dave* 인증서를 IBM Integration Bus 서비스 사용자에게 제공하십시오.

alice, *bob*, *cecil* 및 *dave*를 식별하는 각 인증서를 외부 파일에 추출한 다음 추출된 인증서를 IBM Integration Bus 키 저장소에 추가하여 이를 수행하십시오. **태스크 5. 빠른 시작 안내서 (Windows 또는 UNIX)의 인증서 공유하기**

3. IBM Integration Bus 서비스 사용자의 인증서를 *alice*, *bob*, *cecil* 및 *dave*에게 제공하십시오.

이전 단계에 지정된 방법을 사용하여 이를 수행하십시오.

참고: *Alice* 및 *bob*은 메시지를 올바르게 암호화하기 위해서 IBM Integration Bus 서비스 사용자의 인증서가 필요합니다. IBM Integration Bus 서비스 사용자는 메시지의 작성자를 확인하기 위해 *alice* 및 *bob*의 인증서가 필요합니다. IBM Integration Bus 서비스 사용자는 메시지를 암호화하기 위해 *cecil* 및 *dave*의 인증서가 필요합니다. *cecil* 및 *dave*는 메시지가 IBM Integration Bus에서 오는지를 확인하기 위해 IBM Integration Bus 서비스 사용자의 인증서가 필요합니다.

4. 이름이 IN인 로컬 큐를 정의하고 *alice* 및 *bob*이 작성자로 지정되고 IBM Integration Bus의 서비스 사용자가 수신인으로 지정된 보안 정책을 정의하십시오.

```
setmqspl -m QMgrName -p IN -s MD5 -a "CN=alice,0=IBM,C=GB" -a "CN=bob,0=IBM,C=GB" -e AES256 -r "CN=broker,0=IBM,C=GB"
```

5. 이름이 OUT인 로컬 큐를 정의하고, IBM Integration Bus가 작성자로 지정되고, *cecil* 및 *dave*가 수신인으로 지정된 보안 정책을 정의하십시오.

```
setmqspl -m QMgrName -p OUT -s MD5 -a "CN=broker,0=IBM,C=GB" -e AES256 -r "CN=cecil,0=IBM,C=GB" -r "CN=dave,0=IBM,C=GB"
```

6. IBM Integration Bus에서는 MQInput 및 MQOutput 노드가 있는 메시지 플로우를 작성합니다. IN 큐를 사용하도록 MQInput 노드를 구성하고 OUT 큐를 사용하도록 MQOutput 노드를 구성하십시오.
7. 메시지 플로우를 IBM Integration Bus 런타임 컴포넌트에 배치하십시오.
8. *alice* 또는 *bob* 사용자로서 실행하여 **amqsput** 샘플 애플리케이션을 사용하여 메시지를 IN 큐에 넣으십시오.

9. *cecil* 또는 *dave* 사용자로서 실행하여 **amqsgset** 샘플 애플리케이션을 사용하여 OUT 큐로부터 메시지를 검색합니다.

결과

alice 또는 *bob*이 입력 큐 IN에 전송한 메시지는 암호화되어 IBM Integration Bus만이 이를 읽을 수 있습니다. IBM Integration Bus는 *alice* 및 *bob*으로부터 온 메시지만을 승인하고 나머지는 거부합니다. 승인된 메시지는 적절하게 처리된 다음 출력 큐 OUT에 넣기 전에 *cecil* 및 *dave*의 키로 서명되고 암호화됩니다. *cecil* 및 *dave*만이 이를 읽을 수 있고, IBM Integration Bus에 의해 서명되지 않은 메시지는 거부됩니다.

Managed File Transfer과(와) 함께 Advanced Message Security 사용

이 시나리오에서는 Managed File Transfer를 통해 전송되는 데이터에 대해 메시지 개인정보 보호정책을 제공하도록 Advanced Message Security를 구성하는 방법에 대해 설명합니다.

시작하기 전에

보호하려는 Managed File Transfer에서 사용하는 큐를 호스트하는 IBM MQ 설치에 Advanced Message Security 구성요소가 설치되어 있는지 확인하십시오.

Managed File Transfer 에이전트가 바인딩 모드에서 연결 중인 경우에는 GSKit 컴포넌트가 로컬 설치에 설치되어 있는지 또한 확인하십시오.

이 태스크 정보

데이터를 두 개의 Managed File Transfer 에이전트 사이에서 전송할 때 중단되면 기밀 데이터가 전송을 관리하는 데 사용되는 기본 IBM MQ 큐에 보호되지 않은 상태로 남아 있을 수도 있습니다. 이 시나리오에서는 Managed File Transfer 큐에서 이러한 데이터를 보호하기 위해 Advanced Message Security를 구성하고 사용하는 방법에 대해 설명합니다.

이 시나리오에서는 시나리오 시나리오 개요에 설명된 대로 단일 큐 관리자를 공유하는 두 개의 Managed File Transfer 큐와 두 개의 에이전트 (AGENT1 및 AGENT2)가 있는 하나의 시스템을 포함하는 단순 토폴로지를 고려합니다. 두 에이전트 모두 바인딩 모드 또는 클라이언트 모드에서 동일한 방법으로 연결됩니다.

1. 인증서 작성

시작하기 전에

이 시나리오에서는 FTAGENTS 그룹의 사용자 *ftagent*를 사용하여 Managed File Transfer Agent 프로세스를 실행하는 단순한 모형을 사용합니다. 사용자 고유의 사용자 이름과 그룹 이름을 사용하는 경우 그에 맞게 명령을 변경하십시오.

이 태스크 정보

Advanced Message Security는 보호된 큐에서 메시지를 서명 및/또는 암호화하기 위해 공개 키 암호화를 사용합니다.

참고:

- Managed File Transfer 에이전트가 바인딩 모드에서 실행 중인 경우에는 CMS(Cryptographic Message Syntax) 키 저장소를 작성하는 데 사용하는 명령이 플랫폼별 **빠른 시작 안내서**(Windows 또는 UNIX)에 설명되어 있습니다.
- Managed File Transfer 에이전트가 클라이언트 모드에서 실행 중이면 JKS(Java 키 저장소)를 작성하는 데 필요한 명령은 535 페이지의 『Java 클라이언트가 있는 AMS에 대한 빠른 시작 안내서』에 설명되어 있습니다.

프로시저

- 적합한 빠른 시작 안내서에 설명된 대로 사용자 *ftagent*를 식별하기 위해 자체 서명 인증서를 작성하십시오.
다음과 같이 식별 이름(DN)을 사용하십시오.

```
CN=ftagent, OU=MFT, O=<organisation>, L=<location>, ST=<state>, C=<country>
```

2. 적합한 빠른 시작 안내서에 설명된 대로 키 저장소의 위치와 그 안의 인증서의 위치를 식별하기 위해 `keystore.conf` 파일을 작성하십시오.

2. 메시지 보호 구성

이 태스크 정보

`setmqsp1` 명령을 사용하여 AGENT2가 사용하는 데이터 큐의 보안 정책을 정의해야 합니다. 이 시나리오에서 동일한 사용자가 두 에이전트를 모두 시작하는 데 사용되므로 서명자와 수신자 DN은 동일하고 우리가 생성한 인증서와 일치합니다.

프로시저

1. `fteStopAgent` 명령을 사용하여 보호하기 위해 Managed File Transfer 에이전트를 종료하십시오.
2. `SYSTEM.FTE.DATA.AGENT2` 큐를 보호하기 위해 보안 정책을 작성하십시오.

```
setmqsp1 -m hubQM -p SYSTEM.FTE.DATA.AGENT2 -s SHA1 -a "CN=ftagent, OU=MFT, O=<organisation>, L=<location>, ST=<state>, C=<country>" -e AES128 -r "CN=ftagent, OU=MFT, O=<organisation>, L=<location>, ST=<state>, C=<country>"
```

3. Managed File Transfer Agent 프로세스를 실행 중인 사용자에게 시스템 정책 큐를 찾아보고 메시지를 오류 큐에 넣기 위해 필요한 액세스 권한이 있는지 확인하십시오.

```
setmqaut -m hubQM -t queue -n SYSTEM.PROTECTION.POLICY.QUEUE -p ftagent +browse  
setmqaut -m hubQM -t queue -n SYSTEM.PROTECTION.ERROR.QUEUE -p ftagent +put
```

4. `fteStartAgent` 명령을 사용하여 Managed File Transfer 에이전트를 다시 시작하십시오.
5. `fteListAgents` 명령을 사용하고 에이전트가 READY 상태에 있는지 확인하여 에이전트가 성공적으로 재 시작되었는지 확인하십시오.

결과

이제 전송을 AGENT1에서 AGENT2로 제출할 수 있고, 파일 콘텐츠는 두 에이전트 간에 안전하게 전송됩니다.

Advanced Message Security 설치 개요

Advanced Message Security 컴포넌트를 다양한 플랫폼에 설치하십시오.

이 태스크 정보

설치 프로시저에 대한 정보는 [멀티플랫폼에서 Advanced Message Security 설치](#) 및 [z/OS에 Advanced Message Security 설치](#)를 참조하십시오.

관련 태스크

[Advanced Message Security 설치 제거](#)

z/OS

z/OS에서 감사

z/OS의 Advanced Message Security (AMS)는 정책 보호 큐에 있는 애플리케이션에 의한 조작의 선택적 감사를 위한 수단을 제공합니다. 사용 가능으로 설정된 경우 정책 보호된 큐에서 이러한 조작의 성공과 실패에 대해 IBM 시스템 관리 기능(SMF) 감사 레코드가 생성됩니다. 감사된 조작에는 MQPUT, MQPUT1 및 MQGET가 포함됩니다.

감사는 기본적으로 사용 불가능으로 설정되지만 AMS 주소 공간에 구성된 Language Environment® `_CEE_ENVFILE` 파일에서 `_AMS_SMF_TYPE` 및 `_AMS_SMF_AUDIT`를 구성하여 감사를 활성화할 수 있습니다. 자세한 정보는 [Advanced Message Security의 작성 프로시저](#)를 참조하십시오. `_AMS_SMF_TYPE` 변수는 SMF 레코드 유형을 지정하는 데 사용되고 이는 128과 255 사이의 수입니다. 180의 SMF 레코드 유형이 일반적이지만 필수는 아닙니다. 값 0을 지정하면 감사가 사용 안함으로 설정됩니다. `_AMS_SMF_AUDIT` 변수는 성공적인 조작, 실패한 조작 또는 둘 다에 대한 감사 레코드가 작성되는지 여부를 구성합니다. 조작 명령을 사용하여 AMS가 활성화되는 동안 감사 옵션은 동적으로 변경될 수 있습니다. 자세한 정보는 [Advanced Message Security 작동](#)을 참조하십시오.

SMF 레코드는 하위 유형 1이 일반 감사 이벤트로 사용되는 하위 유형을 사용하여 정의됩니다. SMF 레코드에는 처리 중인 요청과 관련된 모든 데이터가 포함됩니다.

SMF 레코드는 CSQ0KSMF 매크로(매크로 이름에서 0을 참고)에 의해 맵핑되고, 이는 대상 라이브러리 SCSQMACS에서 제공됩니다. SMF 데이터에 대한 데이터 감소 프로그램을 작성 중이면 SMF 포스트 처리 루틴의 개발과 사용자 정의를 지원하기 위해 이 맵핑 매크로를 포함할 수 있습니다.

z/OS에 대해 Advanced Message Security가 생성한 SMF 레코드에서 데이터는 섹션으로 구성됩니다. 레코드는 다음으로 구성됩니다.

- 표준 SMF 헤더
- z/OS용 Advanced Message Security에서 정의된 헤더 확장
- 제품 절
- 데이터 절

SMF 레코드의 제품 섹션은 항상 z/OS에 대해 Advanced Message Security가 생성하는 레코드에 표시됩니다. 데이터 절은 하위 유형에 따라 다릅니다. 현재 하나의 하위 유형이 정의되어 있으므로 단일 데이터 절이 사용됩니다.

SMF는 z/OS 시스템 관리 기능 매뉴얼(SA22-7630)에 설명되어 있습니다. 유효한 레코드 유형은 시스템 PARMLIB 데이터 세트의 SMFPRMxx 구성원에 설명됩니다. 자세한 정보는 SMF 문서를 참조하십시오.

Advanced Message Security 감사 보고서 생성기(CSQ0USMF)

z/OS의 Advanced Message Security는 설치 SCSQAUTH 라이브러리에 제공되는 감사 보고서 생성기 도구 CSQ0USMF를 제공합니다. CSQ40RSM라는 CSQ0USMF 유틸리티를 실행하기 위한 샘플 JCL이 설치 라이브러리 SCSQPROC에 제공됩니다.

CSQ0USMF 유틸리티를 실행하기 전에, SMF 유형 180 레코드는 시스템 SMF 데이터 세트에서 순차 데이터 세트로 덤프해야 합니다. 예를 들어, 이 JCL은 SMF 데이터 세트에서 SMF 유형 180 레코드를 덤프하고 대상 데이터 세트로 전송합니다.

```
//IFAUDUMP EXEC PGM=IFASMFDP
//INDD1 DD DSN=SYSn.MANn.syst,DISP=SHR
//OUTDD1 DD DSN=your.target.dataset,DISP=SHR
//SYSPRINT DD SYSOUT=*
//SYSIN DD *
INDD(INDD1,OPTIONS(DUMP))
OUTDD(OUTDD1,TYPE(180))
/*
```

설치가 사용하는 실제 SMF 데이터 세트 이름을 확인해야 합니다. 버린 레코드의 대상 데이터 세트에는 VBS의 레코드 형식 및 32760의 레코드 길이가 있어야 합니다.

참고: SMF 로그 스트림을 사용 중인 경우 IFASMFDP 프로그램을 사용하여 로그 스트림을 순차 데이터 세트로 덤프해야 합니다. 사용되는 JCL의 예제는 [처리 유형 116 SMF 레코드를 참조하십시오](#).

그런 다음, 대상 데이터 세트는 CSQ0USMF 유틸리티에 입력으로 사용되어 AMS 감사 보고서를 생성할 수 있습니다. 예를 들면, 다음과 같습니다.

```
//STEP1 EXEC PGM=CSQ0USMF,
// PARM=('/' -SMFTYPE 180 -M qmgr')
//STEPLIB DD DSN=thlqual.SCSQANLE,DISP=SHR
// DD DSN=thlqual.SCSQAUTH,DISP=SHR
//SMFIN DD DSN=your.target.dataset,DISP=SHR
//
```

CSQ0USMF 프로그램은 [547 페이지의 표 97](#)에 나열되는 두 개의 선택적 매개변수를 승인합니다.

표 97. CSQOUSMF 선택적 매개변수		
매개변수	가치	설명
SMFTYPE	nnn	감사 보고서에 적용할 수 있는 SMF 레코드 유형입니다. CSQOUSMF 프로그램은 보고서를 생성할 때 SMFTYPE 값과 일치하는 SMF 레코드만을 사용합니다. SMFTYPE을 지정하지 않으면 기본값 180이 사용됩니다.
M	qmgr	감사 보고서에 적용되는 IBM MQ 큐 관리자 이름입니다. -M 매개변수를 지정하지 않으면 감사 보고서에는 SMFIN 데이터 세트에 표시된 모든 큐 관리자의 모든 감사 레코드가 포함됩니다.

키 저장소 및 인증서 사용

IBM MQ 애플리케이션에 투명한 암호 보호를 제공하기 위해 Advanced Message Security는 공개 키 인증서 및 개인 키가 저장되는 키 저장소 파일을 사용합니다. z/OS에서 SAF 키 링이 키 저장소 파일 대신에 사용됩니다.

Advanced Message Security에서 사용자 및 애플리케이션은 PKI(Public Key Infrastructure) ID로 표시됩니다. 이 ID 유형은 메시지를 서명하고 암호화하는 데 사용됩니다. PKI ID는 서명되고 암호화된 메시지와 연관된 인증서에 제목의 **식별 이름(DN)** 필드에 나타납니다. 사용자나 애플리케이션이 이들의 메시지를 암호화하기 위해서는 인증서 및 연관된 개인 및 공개 키가 저장되는 키 저장소 파일에 대한 액세스가 필요합니다.

Windows 및 UNIX에서 키 저장소의 위치는 키 저장소 구성 파일(기본적으로, `keystore.conf`)에 제공됩니다. 각 Advanced Message Security 사용자에게는 키 저장소 파일을 가리키는 키 저장소 구성 파일이 있어야 합니다. Advanced Message Security는 다음 키 저장소 파일 형식을 승인합니다. `.kdb`, `.jceks`, `.jks`.

`keystore.conf` 파일의 기본 위치는 다음과 같습니다.

- ▶ **IBM i** ▶ **UNIX** UNIX 및 IBM i: `$HOME/.mqsc/keystore.conf`
- ▶ **Windows** Windows: `%HOMEDRIVE%%HOMEPATH%\mqsc\keystore.conf`

참고: Windows의 경로는 둘 이상의 드라이브 문자가 사용 가능한 경우 드라이브 이름을 지정할 수 있습니다.

지정된 키 저장소 파일 이름 및 위치를 사용 중인 경우에는 다음 명령을 사용해야 합니다.

- Java의 경우: `java -DMQS_KEYSTORE_CONF=path/filename app_name`
- C 클라이언트 및 서버의 경우
 - UNIX and Linux: `export MQS_KEYSTORE_CONF=path/filename`
 - Windows: `set MQS_KEYSTORE_CONF=path\filename`

관련 개념

571 페이지의 『AMS의 송신자 식별 이름』

송신자 식별 이름(DN)은 메시지를 큐에 배치할 수 있는 권한을 가진 사용자를 식별합니다. 송신자는 메시지를 큐에 배치하기 전에 인증서를 사용하여 메시지에 서명합니다.

572 페이지의 『AMS의 수신인 식별 이름』

수신자 식별 이름(DN)은 큐로부터 메시지를 수신할 권한이 있는 사용자를 식별합니다.

AMS 에 대한 키 저장소 구성 파일 (keystore.conf) 의 구조

키 저장소 구성 파일 (`keystore.conf`) 은 Advanced Message Security 에서 적절한 키 저장소의 위치를 가리킵니다.

다음 구성 파일 유형 각각에는 접두부가 있습니다.

CMS

인증서 관리 시스템(CMS), 구성 항목의 접두부는 `cms`.입니다.

PKCS#11

공개 키 암호 표준(PKCS) #11, 구성 항목의 접두부는 `pkcs11`.입니다.

IBM i PEM

PEM(Privacy Enhanced Mail) 형식, 구성 항목의 접두부는 `pem`.입니다.

JKS

Java 키 저장소, 구성 항목의 접두부는 `jks`.입니다.

JCEKS

Java 암호 암호화 키 저장소, 구성 항목의 접두부는 `jceks`.입니다.

z/OS V 9.1.0 MQ Adv. VUE JCERACFKS

Java 암호 암호화 RACF 키 링 키 저장소, 구성 항목의 접두부는 `jceracfks`입니다.

중요사항: IBM MQ 9.0에서 JCEKS.provider 및 JKS.provider 값이 무시됩니다. Bouncy Castle 제공자는 사용 중 JRE에서 제공하는 JCE/JCE 프로비전과 함께 사용됩니다. 자세한 정보는 551 페이지의 『AMS 가 있는 IBM 이외의 JRE에 대한 지원』의 내용을 참조하십시오.

키 저장소의 구조 예:

CMS

```
cms.keystore = /dir/keystore_file
cms.certificate = certificate_label
```

PKCS#11

```
pkcs11.library = dir\cryptoki.dll
pkcs11.certificate = certificatelabel
pkcs11.token = tokenlabel
pkcs11.token_pin = tokenpin
pkcs11.secondary_keystore = dir\signers
```

IBM i PEM

```
pem.private = /dir/keystore_file_private_key
pem.public = /dir/keystore_file_public_keys
pem.password = password
```

Java JKS

```
jks.keystore = dir/Keystore
jks.certificate = certificate_label
jks.encrypted = no
jks.keystore_pass = password
jks.key_pass = password
jks.provider = IBMJCE
```

Java JCEKS

```
jceks.keystore = dir/Keystore
jceks.certificate = certificate_label
jceks.encrypted = no
jceks.keystore_pass = password
jceks.key_pass = password
jceks.provider = IBMJCE
```

```
jceracfks.keystore = safkeyring://user/keyring
jceracfks.certificate = certificate_label
```

표 98. 각 구성 파일 유형에 필요한 매개변수의 요약

매개변수	필수	구성 파일 유형			
		V 9.1.0 Java (JKS, JCEKS 및 JCERACFKS)	IBM i PEM	PKCS#11	CMS
keystore	✓	✓			✓
IBM i private	✓		IBM i ✓		
IBM i public	✓		IBM i ✓		
IBM i password	✓		IBM i ✓		
library	✓			✓	
certificate	✓	✓		✓	✓
token	✓			✓	
token_pin	✓			✓	
secondary_ke ystore	✓			✓	
encrypted		✓			
keystore_pas s	✓	✓			
key_pass		✓			
provider		✓			

기호를 사용하여 주석을 추가할 수 있습니다.

구성 파일 매개변수는 다음과 같이 정의됩니다.

keystore

CMS 및 Java 구성만. CMS, JKS 및 JCEKS 구성에 대한 키 저장소 파일의 경로입니다.

z/OS **V 9.1.0** **MQ Adv. VUE** JCERACFKS 구성을 위한 RACF 키 링에 대한 URI입니다.

중요사항:

- 키 저장소 파일에 대한 경로는 파일 확장자를 포함하지 않아야 합니다.
- **z/OS** **V 9.1.0** **MQ Adv. VUE** RACF 키 링에 대한 URI는 다음 양식이어야 합니다.

```
safkeyring://user/keyring
```


설명:

- *user*은(는) 키 링을 소유하는 사용자 ID입니다.
- *keyring*은(는) 키링 이름입니다.

IBM i private

PEM 구성만. PEM 형식에 개인 키 및 인증서를 포함하는 파일의 파일 이름.

IBM i public

PEM 구성만. PEM 형식에 신뢰되는 공개 인증서를 포함하는 파일의 파일 이름.

IBM i password

PEM 구성만. 암호화된 개인 키를 복호화하는 데 사용되는 비밀번호입니다.

library

PKCS#11만. PKCS#11 라이브러리의 경로 이름.

certificate

CMS, PKCS#11 및 Java 구성만. 인증서 레이블.

token

PKCS#11만. 토큰 레이블.

token_pin

PKCS#11만. 토큰을 잠금 해제하기 위한 PIN.

secondary_keystore

PKCS#11만. PKCS #11 토큰에 저장된 인증서에 필요한 앵커 인증서(루트 인증서)를 포함하는 CMS 키 저장소의 경로 이름(.kdb 확장자 없이 제공됨). 보조 키 저장소에는 또한 신뢰 체인에서 중간에 있는 인증서뿐만 아니라 개인정보 보안 정책에 정의된 수신인 인증서를 포함할 수 있습니다. 이 CMS 키 저장소는 보조 키 저장소와 같은 디렉토리에 있어야 하는 스테쉬 파일을 동반해야 합니다.

encrypted

Java 구성만. 비밀번호의 상태입니다.

keystore_pass

Java 구성만. 키 저장소 파일의 비밀번호.

참고:

- CMS 키 저장소의 경우 AMS는 스테쉬 파일 (.sth)에 의존하는 반면, JKS 및 JCEKS에는 인증서 및 사용자의 개인 키 둘 모두에 대한 비밀번호가 필요할 수도 있습니다.
- **중요사항:** 비밀번호를 일반 텍스트 양식으로 저장하는 것은 보안 위험입니다.



참고: 액세스가 비밀번호로 제어되지 않으므로 jceracfks에 대해 무시됩니다.

key_pass

Java 구성만. 사용자의 개인 키의 비밀번호입니다.

중요사항: 비밀번호를 일반 텍스트 양식으로 저장하는 것은 보안 위험입니다.



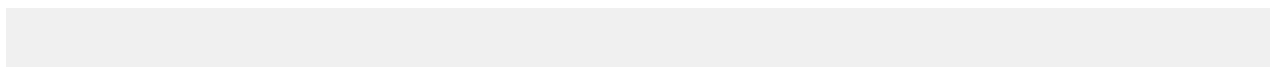
참고: 액세스가 비밀번호로 제어되지 않으므로 jceracfks에 대해 무시됩니다.

provider

Java 구성만. 키 저장소 인증서가 필요로 하는 암호화 알고리즘을 구현하는 Java 보안 제공자.

중요사항: 키 저장소에 저장되는 정보는 IBM MQ를 사용하여 전송되는 데이터의 안전한 플로우를 위해 중요합니다. 보안 관리자는 이들에게 파일 권한을 지정할 때 특히 주의를 기울여야 합니다.

keystore.conf 파일의 예:



```
# Native AMS application configuration
cms.keystore = c:\Documents and Settings\Alice\AliceKeystore
cms.certificate = AliceCert

# Java AMS application configuration
jceks.keystore = c:/Documents and Settings/Alice/
AliceKeystore
jceks.certificate = AliceCert
jceks.encrypted = no
jceks.keystore_pass = passwd
jceks.key_pass = passwd
jceks.provider = IBMJCE
```

관련 태스크

563 페이지의 『Java에서 비밀번호 보호』

키 저장소 및 개인 키 비밀번호를 일반 텍스트로 저장하면 보안 위험이 제기되므로 Advanced Message Security는 키 저장소 파일에서 사용 가능한 사용자 키를 사용하여 이러한 비밀번호를 끊어 모을 수 있는 도구를 제공합니다.

AMS가 있는 IBM 이외의 JRE에 대한 지원

IBM MQ classes for Java and IBM MQ classes for JMS support Advanced Message Security operation when running with non-IBM JREs.

Advanced Message Security(AMS)는 CMS(Cryptographic Message Syntax)를 구현합니다. CMS 구문은 임의의 메시지 콘텐츠에 대한 디지털 서명, 요약, 인증 또는 암호화에 사용됩니다.

IBM MQ 9.0에서 IBM MQ classes for Java 및 IBM MQ classes for JMS의 Advanced Message Security 지원은 오픈 소스 Bouncy Castle 패키지를 사용하여 CMS를 지원합니다. 이는 IBM 이외의 JRE를 사용하여 실행할 때 이 클래스가 Advanced Message Security 조작을 지원할 수 있음을 의미합니다.

Before IBM MQ 9.0, Advanced Message Security was not supported in non-IBM JREs in Java clients. IBM MQ classes for Java 및 IBM MQ classes for JMS의 Advanced Message Security 지원은 Java JCE (Cryptography Extensions)의 IBM 구현에서 특별히 제공하는 CMS 지원에 의존합니다. 이러한 제한사항으로 인해 Java JCE 제공자가 포함된 Java runtime environment (JRE)를 사용하는 경우에만 기능이 사용 가능했습니다.

Solaris 중요한 점은 Solaris와 같은 플랫폼에 대한 지원을 위해서는 IBM에서 제공하는 추가 요소가 있는 플랫폼에 대한 표준 JRE인 하이브리드 JRE가 필요했다는 것입니다. 특히, 플랫폼에 대한 표준 JRE에서 제공한 JCE 제공자가 아닌 IBM JCE 제공자가 필요했습니다.

Bouncy Castle JAR 파일에 대한 위치 및 버전 번호 지정

비IBM JRE에 대한 지원에 필요한 Bouncy Castle JAR 파일은 IBM MQ classes for Java 및 IBM MQ classes for JMS 설치 패키지의 부분으로 포함됩니다.

사용되는 Bouncy Castle JAR 파일은 다음과 같습니다.

Bouncy Castle 조작의 핵심인 제공자 JAR 파일.

이 JAR 파일은 bcprov-jdk15on.jar입니다.

Advanced Message Security에서 사용하는 CMS 조작 지원을 포함하는 "PKIX" JAR 파일.

이 JAR 파일은 bcpkix-jdk15on.jar입니다.

V 9.1.0.9 다른 Bouncy Castle JAR 파일에서 사용하는 클래스를 포함하는 "util" JAR 파일.

이 JAR 파일은 bcutil-jdk15on.jar입니다.

종속성

IBM MQ 9.1 이상 클래스는 IBM JRE 및 Oracle JRE로 테스트되었습니다. 또한 J2SE 준수 JRE에서 성공적으로 실행될 수 있습니다. 그러나 다음 종속성에 주의해야 합니다.

- Advanced Message Security 구성에 대한 변경사항이 없습니다.
- Bouncy Castle 클래스는 CMS 조작에 대해서만 사용됩니다. 다른 모든 보안 관련 조작(예: 키 저장소 액세스), 실제 데이터 암호화, 서명 체크섬 계산은 JRE에서 제공하는 기능을 사용합니다.

중요사항: 이러한 이유로, 사용되는 JRE는 JCE 제공자 구현을 포함해야 합니다.

- 일부 강력한 암호화 알고리즘을 사용하려면 JRE의 JCE 구현에 대해 제한 없는 정책 파일을 설치해야 합니다. 자세한 정보는 JRE 문서를 참조하십시오.
- Java 보안을 사용하는 경우:
 - `java.security.SecurityPermissioninsertProvider.BC`를 애플리케이션에 추가하십시오. 그러면 Bouncy Castle 클래스를 보안 제공자로 사용할 수 있습니다.
 - 다음과 같은 Bouncy Castle JAR 파일에 `java.security.AllPermission`을 부여하십시오.

```
V9.1.0.9 mq_install_dir/java/lib/bcutil-jdk15on.jar
mq_install_dir/java/lib/bcpkix-jdk15on.jar
mq_install_dir/java/lib/bcprov-jdk15on.jar
```

관련 개념

[JMS용 IBM MQ 클래스에 대해 설치되는 항목](#)

[Java용 IBM MQ 클래스에 대해 설치되는 항목](#)

Multi 메시지 채널 에이전트(MCA) 인터셉션

MCA 인터셉션 기능을 사용하면 IBM MQ에서 실행 중인 큐 관리자가 서버 연결 채널에 선택적으로 정책을 적용할 수 있습니다.

AMS 외부에 남아 있는 클라이언트는 MCA 인터셉션을 통해 큐 관리자에 계속 연결되어 있고 메시지를 암호화하고 복호화할 수 있습니다.

MCA 인터셉션은 클라이언트에서 AMS를 사용할 수 없을 때 AMS 기능을 제공하기 위한 것입니다. MCA 인터셉션과 AMS 가능 클라이언트를 사용하면 메시지가 이중으로 보호되어 애플리케이션 수신에 장애가 될 수 있습니다. 자세한 정보는 554 페이지의 『클라이언트에서 Advanced Message Security 사용 안함』의 내용을 참조하십시오.

참고: AMQP 또는 MQTT 채널의 경우 MCA 인터셉터가 지원되지 않습니다.

키 저장소 구성 파일

기본적으로 MCA 인터셉션의 키 저장소 구성 파일은 `keystore.conf`이고 큐 관리자 또는 리스너를 시작한 사용자의 HOME 디렉토리 경로에 `.mq` 디렉토리에 있습니다. 키 저장소는 `MQS_KEYSTORE_CONF` 환경 변수를 사용하여 구성될 수도 있습니다. AMS 키 저장소 구성에 대한 자세한 정보는 547 페이지의 『키 저장소 및 인증서 사용』을 참조하십시오.

MCA 인터셉션을 사용으로 설정하려면 키 저장소 구성 파일에서 사용하고 싶은 채널의 이름을 제공해야 합니다. MCA 인터셉션의 경우 CMS 키 저장소 유형만 사용할 수 있습니다.

553 페이지의 『Advanced Message Security MCA 인터셉션 예』에서 MCA 인터셉션 설정 예를 확인하십시오.



주의: 권한 있는 클라이언트만이 이 기능에 연결하여 사용할 수 있게 하려면 SSL 및 SSLPEER 또는 CHLAUTH TYPE(SSLPEERMAP)을 사용하여 선택된 채널에서 클라이언트 인증 및 암호화를 완료해야 합니다.

IBM i

엔터프라이즈에서 IBM i를 사용하고 인증서에 서명하기 위해 상업 인증 기관(CA)을 선택한 경우 디지털 Certificate Manager 는 PEM (개인정보 보호 강화 메일) 형식으로 인증서 요청을 작성합니다. 요청을 선택한 CA에 전달해야 합니다.

이를 수행하려면 `channelname`에 지정된 채널의 올바른 인증서를 선택하기 위해 다음 명령을 사용해야 합니다.

```
pem.certificate.channel.channelname
```

Advanced Message Security MCA 인터셉션 예

AMS MCA 인터셉션 설정 방법에 대한 태스크 예입니다.

시작하기 전에



주의: 권한 있는 클라이언트만이 이 기능에 연결하여 사용할 수 있게 하려면 SSL 및 SSLPEER 또는 CHLAUTH TYPE(SSLPEERMAP)을 사용하여 선택된 채널에서 클라이언트 인증 및 암호화를 완료해야 합니다.

엔터프라이즈에서 IBM i를 사용하고 인증서에 서명하기 위해 상업 인증 기관 (CA) 을 선택한 경우 디지털 Certificate Manager 는 PEM (개인정보 보호 강화 메일) 형식으로 인증서 요청을 작성합니다. 요청을 선택한 CA 에 전달해야 합니다.

이 태스크 정보

이 태스크는 MCA 인터셉션을 사용하도록 시스템을 설정하고 설정을 확인하는 프로세스를 설명합니다.

참고: IBM WebSphere MQ 7.5 이전의 AMS는 별도로 설치하여, 애플리케이션을 보호하도록 인터셉터를 구성해야 하는 추가 기능 제품이었습니. IBM WebSphere MQ 7.5부터는 인터셉터가 기본으로 포함되오 MQ 클라이언트 및 서버 런타임 환경에서 동적으로 사용됩니다. 이 MCA 인터셉션 예에서는 채널의 서버측에 인터셉터가 제공되며, (12단계에서는) 이전의 클라이언트 런타임을 사용하여 보호되지 않는 메시지가 채널에 배치되게 한 후 MCA 인터셉터가 메시지를 보호하는 과정을 확인할 수 있도록 합니다. 이 예에서 IBM WebSphere MQ 7.5 이상의 클라이언트를 사용하게 되면 MQ 클라이언트 런타임 인터셉터와 MCA 인터셉터가 MQ로 들어오는 메시지를 보호하므로 메시지가 이중으로 보호됩니다.



주의: 코드에서 userID를 사용자의 ID로 바꾸십시오.

프로시저

1. 셸 스크립트를 작성하려면 다음 명령을 사용하여 키 데이터베이스 및 인증서를 작성하십시오.
또한 **INSTLOC** 및 **KEYSTORELOC**를 변경하거나 필수 명령을 실행하십시오. bob의 인증서를 작성할 필요가 없을 수도 있음을 유의하십시오.

```
INSTLOC=/opt/mq90
KEYSTORELOC=/home/testusr/ssl/ams1
mkdir -p $KEYSTORELOC
chmod -R 777 $KEYSTORELOC
chown -R mqm:mqm $KEYSTORELOC
export PATH=$PATH:$INSTLOC/gskit8/bin
echo "PATH = $PATH"
export LD_LIBRARY_PATH=$LD_LIBRARY_PATH:$INSTLOC/gskit8/lib64

gsk8capicmd_64 -keydb -create -db $KEYSTORELOC/alicekey.kdb -pw passw0rd -stash
gsk8capicmd_64 -keydb -create -db $KEYSTORELOC/bobkey.kdb -pw passw0rd -stash
gsk8capicmd_64 -cert -create -db $KEYSTORELOC/alicekey.kdb -pw passw0rd
-label alice_cert -dn "cn=alice,O=IBM,c=IN" -default_cert yes
gsk8capicmd_64 -cert -create -db $KEYSTORELOC/bobkey.kdb -pw passw0rd
-label bob_cert -dn "cn=bob,O=IBM,c=IN" -default_cert yes
```

2. 각 사용자가 서로를 올바르게 식별할 수 있도록 두 키 데이터베이스 사이에서 인증서를 공유하십시오.

태스크 5. 빠른 시작 안내서 (Windows 또는 UNIX) 의 인증서 공유하기

3. 다음 구성으로 keystore.conf를 작성하십시오. Keystore.conf location: /home/
userID/ssl/ams1/

```
cms.keystore = /home/userID/ssl/ams1/alicekey
cms.certificate.channel.SYSTEM.DEF.SVRCONN = alice_cert
```

4. AMSQMGR1 큐 관리자를 작성하고 시작하십시오.
5. port 14567 및 control QMGR로 리스너를 정의하십시오.
6. 채널 권한을 사용 안함으로 설정하거나 채널 권한의 규칙을 설정하십시오.
자세한 정보는 SET CHLAUTH의 내용을 참조하십시오.

- 큐 관리자를 중지합니다.
- 키 저장소를 설정하십시오.

```
export MQS_KEYSTORE_CONF=/home/userID/ssl/ams1/keystore.conf
```

- 동일한 셸에서 큐 관리자를 시작하십시오.
- 보안 정책을 설정하고 다음을 확인하십시오.

```
setmqsp1 -m AMSQMGR1 -s SHA256 -e AES256 -p TESTQ -a "CN=alice,O=IBM,C=IN"
-r "CN=alice,O=IBM,C=IN"
dspmqsp1 -m AMSQMGR1
```

자세한 정보는 [setmqsp1](#) 및 [dspmqsp1](#)의 내용을 참조하십시오.

- 채널 구성을 설정하십시오.

```
export MQSERVER='SYSTEM.DEF.SVRCONN/TCP/127.0.0.1(14567)'
```

- 자동으로 MCA 인터셉터를 사용하지 않는 MQ 클라이언트에서 **amqsputc**를 실행하십시오(예: IBM WebSphere MQ 7.1 또는 이전 클라이언트). 다음 두 메시지를 배치하십시오.

```
/opt/mqm/samp/bin/amqsputc TESTQ TESTQMGR
```

- 보안 정책을 제거하고 결과를 확인하십시오.

```
setmqsp1 -m AMSQMGR1 -p TESTQ -remove
dspmqsp1 -m AMSQMGR1
```

- IBM MQ 9.0 설치에서 큐를 찾아보십시오.

```
/opt/mq90/samp/bin/amqsbcg TESTQ AMSQMGR1
```

찾아보기 출력은 암호화된 형식으로 메시지를 표시합니다.

- 보안 정책을 설정하고 결과를 확인하십시오.

```
setmqsp1 -m AMSQMGR1 -s SHA256 -e AES256 -p TESTQ -a "CN=alice,O=IBM,C=IN"
-r "CN=alice,O=IBM,C=IN"
dspmqsp1 -m AMSQMGR1
```

- IBM MQ 9.0 설치에서 **amqsgetc**를 실행하십시오.

```
/opt/mqm/samp/bin/amqsgetc TESTQ TESTQMGR
```

관련 태스크

535 페이지의 『Java 클라이언트가 있는 AMS에 대한 빠른 시작 안내서』

클라이언트 바인딩을 사용하여 연결하는 Java 애플리케이션에 대한 메시지 보안 제공하도록 Advanced Message Security를 신속하게 구성하려면 이 안내서를 사용하십시오. 이를 완료할 때쯤 사용자 ID를 확인하기 위한 키 저장소를 작성하게 될 것이고 큐 관리자의 서명/암호화 정책을 정의했을 것입니다.

관련 참조

509 페이지의 『AMS의 알려진 제한사항』

지원되지 않거나 Advanced Message Security에 대한 제한사항이 있는 많은 IBM MQ 옵션이 있습니다.

클라이언트에서 Advanced Message Security 사용 안함

제품의 이전 버전에서 큐 관리자에 연결하기 위해 IBM WebSphere MQ 7.5 또는 이후 클라이언트를 사용 중이고 2085 (MQRC_UNKNOWN_OBJECT_NAME) 오류가 보고되는 경우 IBM MQ Advanced Message Security (AMS)를 사용 안함으로 설정해야 합니다.

이 태스크 정보

IBM WebSphere MQ 7.5부터, IBM MQ Advanced Message Security(AMS)는 IBM MQ 클라이언트에서 자동으로 사용 가능하므로 기본적으로 클라이언트는 보안 정책에서 큐 관리자의 오브젝트를 검사하려고 시도합니다.

그러나 IBM WebSphere MQ 7.1과 같이 제품의 이전 버전의 서버는 AMS를 사용으로 설정하지 않았으며 이로 인해 2085 (MQRC_UNKNOWN_OBJECT_NAME) 오류가 보고됩니다.

이 오류가 보고되면 제품의 이전 버전에서 큐 관리자에 연결하려고 할 때 다음과 같이 AMS를 사용 안함으로 설정할 수 있습니다.

- Java 클라이언트의 경우, 다음 방법 중 하나를 사용하십시오.
 - 환경 변수 AMQ_DISABLE_CLIENT_AMS 설정.
 - Java 시스템 특성 com.ibm.mq.cfg.AMQ_DISABLE_CLIENT_AMS 설정.
 - mqclient.ini 파일의 **Security** 스탠자 아래에서 DisableClientAMS 특성 사용.
- C 클라이언트의 경우, 다음 방법 중 하나를 사용하십시오.
 - 환경 변수 MQS_DISABLE_ALL_INTERCEPT 설정.
 - mqclient.ini 파일의 **Security** 스탠자 아래에서 DisableClientAMS 특성 사용.

참고: IBM WebSphere MQ 7.5에서는 AMQ_DISABLE_CLIENT_AMS 환경 변수를 사용할 수도 있습니다. C 클라이언트용. IBM MQ 8.0부터, 더 이상 C 클라이언트용 환경 변수 AMQ_DISABLE_CLIENT_AMS를 사용할 필요가 없습니다. 대신, MQS_DISABLE_ALL_INTERCEPT 환경 변수를 사용해야 합니다.

프로시저

- 클라이언트에서 AMS를 사용 안함으로 설정하려면, 다음 옵션 중 하나를 사용하십시오.

AMQ_DISABLE_CLIENT_AMS 환경 변수

다음의 경우에 이 변수를 설정해야 합니다.

- IBM Java Runtime Environment (JRE) 이외의 Java Runtime Environment (JRE) 를 사용하는 경우
- IBM WebSphere MQ 7.5 또는 이후 IBM MQ classes for JMS 또는 IBM MQ classes for Java 클라이언트를 사용하는 경우

AMQ_DISABLE_CLIENT_AMS 환경 변수를 작성하고 애플리케이션이 실행 중인 환경에서 TRUE로 설정하십시오. 예를 들면, 다음과 같습니다.

```
export AMQ_DISABLE_CLIENT_AMS=TRUE
```

Java 시스템 특성 com.ibm.mq.cfg.AMQ_DISABLE_CLIENT_AMS

IBM MQ classes for JMS 및 IBM MQ classes for Java 클라이언트의 경우 Java 시스템 특성 com.ibm.mq.cfg.AMQ_DISABLE_CLIENT_AMS 를 Java 애플리케이션의 값 TRUE 로 설정할 수 있습니다.

예를 들어, Java 명령이 호출될 때 Java 시스템 특성을 -D 옵션으로 설정할 수 있습니다.

```
java -Dcom.ibm.mq.cfg.AMQ_DISABLE_CLIENT_AMS=TRUE -cp <MQ_INSTALLATION_PATH>/java/lib/com.ibm.mqjms.jar my.java.applicationClass
```

또는 애플리케이션이 이 파일을 사용하는 경우 JMS 구성 파일 jms.config 내에 Java 시스템 특성을 지정할 수 있습니다.

MQS_DISABLE_ALL_INTERCEPT 환경 변수

고유 클라이언트와 함께 IBM MQ 8.0 이상을 사용하고 클라이언트에서 AMS를 사용 안함으로 설정해야 하는 경우 이 변수를 설정해야 합니다.

환경 변수 MQS_DISABLE_ALL_INTERCEPT를 작성하고 클라이언트가 실행 중인 환경에서 TRUE로 설정하십시오. 예를 들면, 다음과 같습니다.

```
export MQS_DISABLE_ALL_INTERCEPT =TRUE
```

C 클라이언트 전용으로 MQS_DISABLE_ALL_INTERCEPT 환경 변수를 사용할 수 있습니다. Java 클라이언트의 경우 AMQ_DISABLE_CLIENT_AMS 환경 변수를 대신 사용해야 합니다.

mqclient.ini 파일의 DisableClientAMS 특성

이 옵션은 IBM MQ classes for JMS 및 IBM MQ classes for Java 클라이언트 그리고 C 클라이언트에 사용할 수 있습니다.

다음 예제에서 표시된 대로 mqclient.ini 파일의 **Security** 스탠자 아래에 특성 이름 **DisableClientAMS**를 추가하십시오.

```
Security:  
DisableClientAMS=Yes
```

다음 예제에 표시된 대로 AMS를 사용으로 설정할 수도 있습니다.

```
Security:  
DisableClientAMS=No
```

다음에 수행할 작업

AMS 보호 큐 열기의 문제점에 대한 자세한 정보는 [JMS와 함께 AMS를 사용할 때 보호된 큐를 여는 중 문제점 발생의 내용을 참조하십시오.](#)

관련 개념

[552 페이지의 『메시지 채널 에이전트\(MCA\) 인터셉션』](#)

MCA 인터셉션 기능을 사용하면 IBM MQ에서 실행 중인 큐 관리자가 서버 연결 채널에 선택적으로 정책을 적용할 수 있습니다.

관련 태스크

[구성 파일을 사용하여 클라이언트 구성](#)

관련 참조

[IBM MQ classes for JMS 구성 파일](#)

AMS의 인증서 요구사항

Advanced Message Security에서 사용하려면 인증서에 RSA 공개 키가 있어야 합니다.

여러 공개 키 유형 및 공개 키를 작성하는 방법에 대한 자세한 정보는 [40 페이지의 『IBM MQ에서 디지털 인증서와 CipherSpec의 호환성』](#)의 내용을 참조하십시오.

키 사용 확장

키 사용 확장은 인증서를 사용할 수 있는 방법에 추가 제한사항을 둡니다.

Advanced Message Security에서, X.509 v3 인증서의 키 사용은 RFC 5280 스펙에 따라 설정되어야 합니다.

QoP(Quality of Protection) 무결성을 위해서는, 인증서 키 사용 확장이 설정된 경우 이 설정이 다음 두 항목 중 하나 이상을 포함해야 합니다.

- **nonRepudiation**
- **digitalSignature**

QoP(Quality of Protection) 개인정보 보호를 위해서는, 인증서 키 사용 확장이 설정된 경우 이 설정이 다음 항목을 포함해야 합니다.

- **keyEncipherment**

QoP(Quality of Protection) 기밀성을 위해서는, 인증서 키 사용 확장이 설정된 경우 이 설정이 다음 항목을 포함해야 합니다.

- **dataEncipherment**

확장 키 사용은 키 사용 확장을 좀 더 세분화합니다. 모든 QoP(Quality of Protection)를 위해서는, 인증서 확장 키 사용이 설정된 경우 이 설정이 다음 항목을 포함해야 합니다.

- **emailProtection**

관련 개념

[574 페이지의 『보호 품질』](#)

Advanced Message Security 데이터 보호 정책은 QoP(Quality of Protection)를 의미합니다.

AMS에서 인증서 유효성 검증 메소드

Advanced Message Security를 사용하여 큐의 메시지가 보안 표준을 충족하지 않는 인증서를 사용하여 보호되지 않도록 폐기된 인증서를 감지하고 거부할 수 있습니다.

AMS를 사용하면 온라인 인증서 상태 프로토콜(OCSP) 또는 인증서 폐기 목록(CRL)을 사용하여 인증서 유효성을 확인할 수 있습니다.

AMS는 OCSP 또는 CRL 검사 또는 둘 모두에 대해 구성될 수 있습니다. 두 메소드 모두가 사용으로 설정되면 성능상의 이유로 AMS는 먼저 폐기 상태를 위해 OCSP를 사용합니다. 인증서의 폐기 상태가 OCSP 검사 후에도 미해결이면 AMS는 CRL 검사를 사용합니다.

참고로, 기본적으로 OCSP 및 CRL 검사를 모두 사용할 수 있습니다.

관련 개념

557 페이지의 『AMS의 온라인 인증서 상태 프로토콜(OCSP)』

온라인 인증서 상태 프로토콜(OCSP)은 인증서가 폐기되었는지 여부를 판별하므로 인증서를 신뢰할 수 있는지 여부를 판별하는 데 도움을 줍니다. OCSP는 기본적으로 사용됩니다.

559 페이지의 『AMS의 인증서 폐기 목록(CRL)』

CRL은 예를 들어, 개인 키가 분실되었거나 손상되었다는 등의 다양한 이유로 더 이상 신뢰되지 않으므로 인증 기관(CA)에 의해 표시된 인증서 목록을 보유하고 있습니다.

AMS의 온라인 인증서 상태 프로토콜(OCSP)

온라인 인증서 상태 프로토콜(OCSP)은 인증서가 폐기되었는지 여부를 판별하므로 인증서를 신뢰할 수 있는지 여부를 판별하는 데 도움을 줍니다. OCSP는 기본적으로 사용됩니다.

OCSP는 IBM i 시스템에서는 지원되지 않습니다.

Advanced Message Security의 기본 인터셉터에서 OCSP 검사 사용

Advanced Message Security의 OCSP(Online Certificate Status Protocol) 검사는 사용되는 인증서의 정보를 기반으로 하여 기본적으로 사용됩니다.

프로시저

키 저장소 구성 파일에 다음 옵션을 추가하십시오.

참고: 모든 OCSP 스탠자는 선택사항이고 독립적으로 지정될 수 있습니다.

옵션	설명
<code>ocsp.enable=off</code>	검사 중인 인증서에 OCSP 응답자가 있는 URI를 포함하는 PKIX_AD_OCSP 액세스 메소드와 함께 권한 정보 액세스(AIA) 확장이 있는 경우 OCSP 검사를 사용으로 설정하십시오. 가능한 값: on 또는 off.
<code>ocsp.url=responder_URL</code>	OCSP 응답자의 URL 주소입니다. 이 옵션이 생략되면 비AIA OCSP 검사가 사용 안함으로 설정됩니다.
<code>ocsp.http.proxy.host=OCSP_proxy</code>	OCSP 프록시 서버의 URL 주소입니다. 이 옵션이 생략되면 프록시는 비AIA 온라인 인증서 검사에 사용되지 않습니다.
<code>ocsp.http.proxy.port=port_number</code>	OCSP 프록시 서버의 포트 번호입니다. 이 옵션이 생략되면 기본 포트 8080이 사용됩니다.
<code>ocsp.nonce.generation=on/off</code>	OCSP를 조회할 때 임시값을 생성합니다. 기본값은 off입니다.

옵션	설명
ocsp.nonce.check=on/off	OCSP로부터 응답을 받은 후 임시값을 검사합니다. 기본값은 off입니다.
ocsp.nonce.size=8	임시값 크기(바이트)입니다.
ocsp.http.get=on/off	요청 메소드로서 HTTP GET을 지정합니다. 이 옵션이 off로 설정되면 HTTP POST가 사용됩니다. 기본값은 off입니다.
ocsp.max_response_size=20480	제공되는 OCSP 응답자로부터의 최대 응답 크기(바이트)입니다.
ocsp.cache_size=100	내부 OCSP 응답 캐싱을 사용으로 설정하고 캐시 항목 수에 대한 한계를 설정합니다.
ocsp.timeout=30	Advanced Message Security 시간 종료 후 서버 응답을 기다리는 시간(초)입니다.
ocsp.unknown=ACCEPT	OCSP 서버가 제한시간 기간 내에 도달할 수 없을 때의 동작을 정의합니다. 가능한 값: <ul style="list-style-type: none"> • ACCEPT 인증서를 허용합니다. • WARN 인증서를 허용하고 경고를 로그합니다. • REJECT 인증서가 사용되는 것을 막고 오류를 로그합니다.

AMS의 Java에서 OCSP 확인 사용

Advanced Message Security에서 Java에 대한 OCSP 검사를 사용으로 설정하려면 `java.security` 파일 또는 키 저장소 구성 파일을 수정하십시오.

이 태스크 정보

Advanced Message Security에서 OCSP 검사를 사용으로 설정하는 데에는 두 가지 방법이 있습니다.

java.security 사용

인증서에 관한 정보 액세스(AIA) 인증서 확장자가 포함되는지 여부를 확인하십시오.

프로시저

1. AIA가 설정되지 않았거나 인증서를 대체하려는 경우 다음 특성으로 `$JAVA_HOME/lib/security/java.security` 파일을 편집하십시오.

```
ocsp.responderURL=http://url.to.responder:port
ocsp.responderCertSubjectName=CN=Example CA,O=IBM,C=US
```

그리고 `$JAVA_HOME/lib/security/java.security` 파일을 다음 행으로 편집하여 OCSP 검사를 사용으로 설정하십시오.

```
ocsp.enable=true
```

2. AIA가 설정된 경우 `$JAVA_HOME/lib/security/java.security` 파일을 다음 행으로 편집하여 OCSP 검사를 사용으로 설정하십시오.

```
ocsp.enable=true
```

다음에 수행할 작업

Java 보안 관리자를 사용 중인 경우에도 구성을 완료하고 다음 Java 권한을 lib/security/java.policy에 추가하십시오.

```
permission java.security.SecurityPermission "getProperty.ocsp.enable";
```

keystore.conf 사용

프로시저

다음 속성을 구성 파일에 추가하십시오.

```
ocsp.enable=true
```

중요사항: 구성 파일에서 이 속성을 설정하면 java.security 설정이 대체됩니다.

다음에 수행할 작업

구성을 완료하려면 다음 Java 권한을 lib/security/java.policy에 추가하십시오.

```
permission java.security.SecurityPermission "getProperty.ocsp.enable";  
permission java.security.SecurityPermission "setProperty.ocsp.enable";
```

AMS의 인증서 폐기 목록(CRL)

CRL은 예를 들어, 개인 키가 분실되었거나 손상되었다는 등의 다양한 이유로 더 이상 신뢰되지 않으므로 인증 기관(CA)에 의해 표시된 인증서 목록을 보유합니다.


인증서를 유효성 검증하기 위해 Advanced Message Security는 서명자의 인증서 및 신뢰 앵커까지 인증 기관(CA)의 인증서 체인으로 구성된 인증서 체인을 구성합니다. 신뢰 앵커는 인증서의 신뢰를 주장하는 데 사용되는 신뢰되는 인증서 또는 신뢰되는 루트 인증서를 포함하는 신뢰되는 키 저장소 파일입니다. AMS는 PKIX 유효성 검증 알고리즘을 사용하여 인증서 경로를 확인합니다. 체인이 작성되고 확인되면, AMS는 인증서 유효성 검사를 완료합니다. 여기에는 체인에서 각 인증서의 발행 및 만기 날짜를 현재 날짜와 비교하여 유효성 검증하고, 키 사용법 확장이 종료 엔티티 인증서에 있는지 여부에 대한 검사가 포함됩니다. 확장이 인증서에 추가된 경우에는 AMS는 **digitalSignature** 또는 **nonRepudiation** 또한 설정되었는지 여부를 확인합니다. 이들이 설정되지 않은 경우에는 MQRC_SECURITY_ERROR가 보고되고 로그됩니다. 그런 다음 AMS는 구성 파일에 지정된 내용에 따라 서 파일 또는 LDAP에서 CRL을 다운로드합니다. AMS에서는 DER 형식으로 인코딩된 CRL만이 지원됩니다. 키 저장소 구성 파일에 CRL 관련 정보를 찾을 수 없는 경우 AMS는 CRL 유효성 검증 검사를 수행하지 않습니다. 각 CA 인증서의 경우 AMS는 해당 CRL을 찾기 위해 CA의 식별 이름을 사용하여 LDAP에서 CRL을 조회합니다. 다음 속성이 LDAP 조회에 포함됩니다.

```
certificateRevocationList,  
certificateRevocationList;binary,  
authorityRevocationList,  
authorityRevocationList;binary  
deltaRevocationList  
deltaRevocationList;binary,
```

참고: deltaRevocationList는 분배 지점으로 지정된 경우에만 지원됩니다.

고유 인터셉터에서 인증서 유효성 검증 및 인증서 폐기 목록 지원 사용으로 설정 Advanced Message Security가 LDAP(Lightweight Directory Access Protocol) 서버로부터 CRL을 다운로드할 수 있도록 키 저장소 구성 파일을 수정해야 합니다.

이 태스크 정보

 기본 인터셉터에서 인증서 유효성 검증 및 인증 취소 목록 지원을 사용하는 것은 IBM i에서 Advanced Message Security에 대해 지원되지 않습니다.

프로시저

다음 옵션을 구성 파일에 추가하십시오.

참고: 모든 CRL 스탠자는 선택사항이고 독립적으로 지정될 수 있습니다.

옵션	설명
<code>crl.ldap.host=host_name</code>	LDAP 서버 호스트 이름
<code>crl.ldap.port=port_number</code>	LDAP 서버 포트 번호. 최대 11개의 서버를 지정할 수 있습니다. 다중 LDAP 호스트는 LDAP 연결 실패 시에 투명한 장애 복구를 보증하는 데 사용됩니다. 모든 LDAP 서버가 복제본이고 동일 데이터를 포함할 것으로 예상됩니다. AMS Java 인터프리터가 LDAP 서버에 성공적으로 연결하면 이는 제공된 나머지 서버에서 CRL을 다운로드하려고 시도하지 않습니다.
<code>crl.cdp=off</code>	이 옵션을 사용하여 인증서에서 CRLDistributionPoints 확장자를 검사하거나 사용하지 않습니다.
<code>crl.ldap.version=3</code>	LDAP 프로토콜 버전 번호. 가능한 값: 2 또는 3.
<code>crl.ldap.user=cn=username</code>	LDAP 서버에 로그인하십시오. 이 값이 지정되지 않으면 LDAP의 CRL은 읽기 쉬워야 합니다.
<code>crl.ldap.pass=password</code>	LDAP 서버에 대한 비밀번호.
<code>crl.ldap.cache_lifetime=0</code>	LDAP 캐시 수명(초 단위). 가능한 값: 0-86400.
<code>crl.ldap.cache_size=50</code>	LDAP 캐시 크기. 이 옵션은 <code>crl.ldap.cache_lifetime</code> 값이 0보다 큰 경우에만 지정할 수 있습니다.
<code>crl.http.proxy.host=some.host.com</code>	CDP CRL 검색을 위한 Http 프록시 서버 포트.
<code>crl.http.proxy.port=8080</code>	Http 프록시 서버 포트 번호.
<code>crl.http.max_response_size=204800</code>	GSKit에서 허용되는 HTTP 서버에서 검색할 수 있는 CRL의 최대 크기(바이트)입니다.
<code>crl.http.timeout=30</code>	AMS 시간 종료 후 서버 응답을 기다리는 시간(초)입니다.
<code>crl.http.cache_size=0</code>	HTTP 캐시 크기(바이트 단위).
<code>crl.unknown=ACCEPT</code>	CRL 서버가 제한시간 기간 내에 도달할 수 없을 때의 동작을 정의합니다. 가능한 값: <ul style="list-style-type: none"> • ACCEPT 인증서를 허용합니다. • WARN 인증서를 허용하고 경고를 로그합니다. • REJECT 인증서가 사용되는 것을 막고 오류를 로그합니다.

AMS의 Java에서 인증 취소 목록 지원 사용

Advanced Message Security에서 CRL 지원을 사용으로 설정하려면 AMS가 LDAP(Lightweight Directory Access Protocol) 서버에서 CRL을 다운로드하고 `java.security` 파일을 구성할 수 있도록 키 저장소 구성 파일을 수정해야 합니다.

프로시저

1. 다음 옵션을 구성 파일에 추가하십시오.

헤더	설명
<code>crl.ldap.host=host_name</code>	LDAP 호스트 이름.
<code>crl.ldap.port=port_number</code>	LDAP 서버 포트 번호. 최대 11개의 서버를 지정할 수 있습니다. 다중 LDAP 호스트는 LDAP 연결 실패 시에 투명한 장애 복구를 보증하는 데 사용됩니다. 모든 LDAP 서버가 복제본이고 동일 데이터를 포함할 것으로 예상됩니다. AMS Java 인터페이스가 LDAP 서버에 성공적으로 연결하면 이는 제공된 나머지 서버에서 CRL을 다운로드하려고 시도하지 않습니다. Java는 <code>crl.ldap.user</code> 및 <code>crl.ldaworldp.pass</code> 값을 사용하지 않습니다. 이는 LDAP 서버에 연결할 때 사용자 및 비밀번호를 사용하지 않습니다. 따라서 LDAP의 CRL 속성은 읽기 쉬워야 합니다.
<code>crl.cdp=on/off</code>	이 옵션을 사용하여 인증서에서 CRLDistributionPoints 확장자를 검사하거나 사용하십시오.

2. 다음 특성으로 JRE/lib/security/java.security 파일을 수정하십시오.

특성 이름	설명
<code>com.ibm.security.enableCRLDP</code>	이 특성은 다음 값 <code>true</code> , <code>false</code> 를 사용합니다. <code>true</code> 로 설정되면 인증서 폐기 검사를 수행할 때 CRL은 인증서의 CRL 분배 지점 확장으로부터 URL을 사용하여 찾습니다. <code>false</code> 로 설정되거나 설정되지 않으면 CRL 분배 지점 확장을 사용하는 CRL 검사는 사용 불가능으로 설정됩니다.
<code>ibm.security.certpath.ldap.cache.lifetime</code>	이 특성은 LDAP CertStore의 메모리 캐시에서 항목의 수명을 초 단위의 값으로 설정하는 데 사용할 수 있습니다. 값 0은 캐시를 사용 불가능으로 설정하고 1은 무제한의 수명을 의미합니다. 설정되지 않으면 기본 수명은 30초입니다.
<code>com.ibm.security.enableAIAEXT</code>	이 특성은 다음 값 <code>true</code> , <code>false</code> 를 사용합니다. <code>true</code> 로 설정되면 빌드 중인 인증서 경로의 인증서 내에서 발견된 권한 정보 액세스 확장은 LDAP URI를 포함하는지 여부를 판별하기 위해 검사됩니다. 발견된 각 LDAP URI에 대해 LDAPCertStore 오브젝트가 작성되고 인증서 경로를 빌드하는 데 필요한 다른 인증서를 찾는 데 사용되는 CertStore의 컬렉션에 추가됩니다. <code>false</code> 로 설정되거나 설정되지 않으면 추가 LDAPCertStore 오브젝트가 작성되지 않습니다.

Advanced Message Security는 데이터 메시지를 보호하는 데 사용되는 디지털 인증서의 인증서 폐기 목록(CRL) 검사를 지원합니다.

이 태스크 정보

사용 가능으로 설정되면, Advanced Message Security는 메시지가 개인정보 보호된 큐에 배치될 때 수신인 인증서를 유효성 검증하고 메시지가 보호된 큐로부터 검색될 때(무결성 또는 개인정보) 송신자 인증서를 유효성 검증합니다. 이 경우 유효성 검증에는 관련 인증서가 관련 CRL에 등록되지 않았다는 확인을 포함합니다.

Advanced Message Security는 IBM 시스템 SSL 서비스를 사용하여 송신자 및 수신인 인증서를 유효성 검증합니다. 시스템 SSL 인증서에 관한 세부사항 문서는 z/OS 암호화 서비스 시스템 보안 소켓 레이어 프로그래밍 매뉴얼(SC24-5901)에서 볼 수 있습니다.

사용 가능해진 CRL 검사에 AMS 주소 공간의 시작된 태스크 JCL에서 CRLFILE DD를 통해 CRL 구성 파일의 위치를 지정합니다. 사용자 정의할 수 있는 샘플 CRL 구성 파일은 *thlqual.SCSQPROC(CSQ40CRL)*에 제공됩니다. 이 파일에 허용된 설정은 다음과 같습니다.

변수	올바른 값	설명
crl.ldap.host[.n]	<i>hostname -or- hostname:port</i>	발행인 인증서의 CRL을 호스트하는 LDAP 서버의 ipaddr/hostname입니다. LDAP 서버의 포트 번호를 지정하지 않는 경우에는 <i>crl.ldap.port</i> 에 의해 지정된 포트 번호가 사용됩니다.
crl.ldap.port	포트	LDAP 서버의 TCP/IP 포트 번호입니다.
crl.ldap.user	<i>ldap_user</i>	LDAP 서버에 연결할 때 사용할 LDAP 사용자 이름입니다.
crl.ldap.pass	<i>ldap_password</i>	<i>crl.ldap.user</i> 와 연관된 LDAP 비밀번호입니다.

다음과 같이 여러 LDAP 서버 호스트 이름 및 포트를 지정할 수 있습니다.

```
crl.ldap.host.1 = hostname -or hostname:port
crl.ldap.host.2 = hostname -or hostname:port
crl.ldap.host.3 = hostname -or hostname:port
```

최대 10개의 호스트 이름을 지정할 수 있습니다. LDAP 서버의 포트 번호를 지정하지 않는 경우에는 *crl.ldap.port*에 의해 지정된 포트 번호가 사용됩니다. 각 LDAP 서버는 액세스를 위해 동일한 *crl.ldap.user/passwd* 결합을 사용해야 합니다.

CRLFILE DD가 지정되면 구성은 Advanced Message Security 주소 공간의 초기화 동안에 로드되고 CRL 검사가 사용 가능으로 설정됩니다. CRLFILE DD가 지정되지 않거나 CRL 구성 파일을 사용할 수 없거나 올바르게 않은 경우 CRL 검사가 사용 안함으로 설정됩니다.

AMS는 IBM 시스템 SSL 인증서 유효성 검증 서비스를 사용하여 다음과 같이 CRL 검사를 수행합니다.

Operation	보호 품질	검사한 인증서
PUT	개인정보	수신자
GET	무결성/개인정보	송신자

메시지 조작이 CRL은 검사에 실패하면 Advanced Message Security는 다음 조치를 수행합니다.

표 101. Advanced Message Security CRL 검사 실패 동작	
Operation	CRL 검사 실패
PUT	메시지가 대상 큐에 놓이지 않습니다. MQCC_FAILED의 완료 코드 및 MQRC_SECURITY_ERROR의 이유 코드가 애플리케이션으로 돌아갑니다.
GET	메시지가 대상 큐에서 제거되고 시스템 보호 오류 큐로 이동됩니다. MQCC_FAILED의 완료 코드 및 MQRC_SECURITY_ERROR의 이유 코드가 애플리케이션으로 돌아갑니다.

AMS for z/OS uses IBM System SSL services to validate certificates, which includes CRL and trust checking. IBM 시스템 SSL은 CRL 검사 조작을 완화하기 위해 환경 변수 GSK_CRL_SECURITY_LEVEL을 제공합니다. 예를 들면, 다음과 같습니다.

```
GSK_CRL_SECURITY_LEVEL=MEDIUM
```

이 변수는 z/OS 암호화 서비스 시스템 보안 소켓 레이어 프로그램 매뉴얼에 문서화되어 있습니다. 유효한 지정은 다음을 포함합니다.

- LOW - LDAP 서버에 접속할 수 없는 경우 인증서 유효성 검증이 실패하지 않습니다.
- MEDIUM- 인증서 유효성 검증을 수행하려면 LDAP 서버에 접속 가능해야 하지만 CRL을 정의할 필요는 없습니다.
- HIGH - 인증서 유효성 검증을 수행하려면 LDAP 서버에 접속 가능하고 CRL을 정의해야 합니다.

IBM 시스템 SSL 기본값은 MEDIUM입니다. AMS 주소 공간의 시작된 태스크 JCL에서 ENVARS DD를 통해 지정된 구성 파일에서 이 변수를 설정할 수 있습니다. 샘플 환경 변수 구성 파일이 *thlqual.SCSQPROC(CSQ40ENV)*에 제공됩니다.

참고: 관련 LDAP 서비스가 사용 가능한지 확인하고 관련 인증 기관을 위해 CRL 항목을 유지보수하는 것은 관리자의 책임입니다.

Java에서 비밀번호 보호

키 저장소 및 개인 키 비밀번호를 일반 텍스트로 저장하면 보안 위험이 제기되므로 Advanced Message Security는 키 저장소 파일에서 사용 가능한 사용자 키를 사용하여 이러한 비밀번호를 끊어 모을 수 있는 도구를 제공합니다.

시작하기 전에

keystore.conf 파일 소유자는 파일 소유자만이 파일을 읽을 권한이 있음을 확실히 해야 합니다. 이 장에서 설명된 비밀번호 보호는 보호의 추가적 측정입니다.

프로시저

1. 키 저장소에 대한 경로 및 사용자 레이블을 포함하도록 keystore.conf 파일을 편집하십시오.

```
jceks.keystore = c:/Documents and Setting/Alice/AliceKeystore
jceks.certificate = AliceCert
jceks.provider = IBMJCE
```

2. 도구를 실행하려면 다음을 실행하십시오.

```
java -cp com.ibm.mq.jmqi.jar com.ibm.mq.es.config.KeyStoreConfigProtector keystore_password private_key_password
```

암호화된 비밀번호가 있는 출력이 생성되고 keystore.conf 파일에 복사될 수 있습니다.

출력을 keystore.conf 파일에 자동으로 복사하려면 다음을 실행하십시오.

```
java -cp com.ibm.mq.jmqi.jar com.ibm.mq.es.config.KeyStoreConfigProtector keystore_password private_key_password >> ~/path_to_keystore/keystore.conf
```

참고:

다양한 플랫폼에서 keystore.conf의 기본 위치의 목록은 [547 페이지의 『키 저장소 및 인증서 사용』](#)의 내용을 참조하십시오.

예

다음은 이러한 출력의 예입니다.

```
#Fri Jul 30 15:20:29 CEST 2010
jceks.key_pass=MMXh997n5Z0r8uR1Jmc5qity9MN2CggGBMKCDxdbn1AyPk1vdgTsOLG6X3C1YT7oDzwaqZF10R4t\r\nm
Zsc7JGAX8nqqxLnAucdGn0NW06xnjZB1n501YGo12k/
PhaQHhFXKMAU9dKg0f8dj0tCA01X4ETe\r\nfy19LBUt2wk87uM7dSs\=
jceks.keystore_pass=0IdeayBnSCfLG4cFuxEVrk6SYyAsdSPpDqgPf16s9s1M04cqZjNbhgjoA2EXonudHZHH+4s2drvQ
\r\nCUvQgu9GuaBMJK2F20jtHJJ1Y4BVeLW2c2okgawo/
W2J1AdUYKkJ0raYTKDouLaTYTQeulyG0xI1\r\niD2si1xUCxhYvvyhbbY\=
jceks.encrypted=yes
```

z/OS z/OS에서 인증서 사용

이 태스크 정보

Advanced Message Security는 무결성, 기밀성 및 개인정보 보호의 세 가지 레벨의 보호를 구현합니다.

무결성 정책을 사용하면 메시지는 진원지(MQPUT을 수행하는 애플리케이션)의 개인 키를 사용하여 서명됩니다. 무결성은 메시지 수정 감지를 제공하지만 메시지 텍스트 자체는 암호화되지 않습니다.

기밀성 정책으로, 메시지는 큐에 넣을 때 암호화됩니다. 메시지는 관련 Advanced Message Security 정책에 지정된 대칭 키 및 알고리즘을 사용하여 암호화됩니다. 대칭 키 자체는 각 수신인의 공개 키로 암호화됩니다 (MQGET을 수행하는 애플리케이션). 공개 키는 키 링에 저장된 인증서와 연관됩니다.

개인정보 보호 정책으로, 메시지는 모두 서명되고 암호화됩니다.

개인정보 보호정책으로 보호되는 메시지가 MQGET을 수행하는 수신인 애플리케이션에 의해 큐에서 해제되면 메시지를 복호화해야 합니다. 이는 수신인의 개인 키를 사용하여 암호화되었으므로 키 링에 있는 수신인의 개인 키를 사용하여 복호화되어야 합니다.

z/OS SAF 키 링 사용

Advanced Message Security(AMS)는 서명과 암호화를 위해 필요한 인증서를 정의하고 관리하기 위해 z/OS SAF 키 링 서비스를 사용합니다. RACF와 기능상으로 동등한 보안 제품이 동일한 지원 레벨을 제공하는 경우 RACF 대신에 사용될 수도 있습니다.

키 링을 효율적으로 사용하면 인증서를 관리하는 데 필요한 관리를 줄일 수 있습니다.

인증서가 생성되거나 가져오기된 후에 이는 액세스 가능하게 되려면 키 링에 연결되어야 합니다. 동일한 인증서를 둘 이상의 키 링에 연결할 수 있습니다.

Advanced Message Security는 두 개의 키 링 세트를 사용합니다. 한 세트는 메시지를 시작하거나 수신한 개별 사용자 ID에 의해 소유되는 키 링 세트로 구성됩니다. 각 키 링에는 소유 사용자 ID의 인증서와 연관된 개인 키가 포함됩니다. 각 인증서의 개인 키는 무결성 보호되거나 개인정보 보호된 큐의 메시지에서 서명하는 데 사용됩니다. 이는 또한 메시지를 수신할 때 개인정보 보호되거나 기밀성 보호된 큐로부터 메시지를 복호화하는 데에도 사용됩니다.

다른 세트는 AMS 주소 공간 사용자에 의해 소유된 단일 키 링입니다. 메시지 진원지와 수신인의 인증서를 유효성 검증하도록 필요한 일련의 서명 CA 인증서를 포함합니다.

개인정보 보호 또는 기밀성 보호를 사용할 때, AMS 주소 공간 사용자가 소유한 키 링은 메시지 수신자의 인증서도 포함합니다. 이러한 인증서의 공개 키는 메시지가 보호된 큐에 놓였을 때 메시지 데이터를 암호화하는 데 사용

되었던 대칭 키를 암호화하는 데 사용됩니다. 이러한 메시지를 검색할 때 관련 수신인의 개인 키는 대칭 키를 복호화하는 데 사용된 다음 메시지 데이터를 복호화하는 데 사용됩니다.

Advanced Message Security는 인증서 및 개인 키를 검색할 때 **drq.ams.keyring**의 키 링 이름을 사용합니다. 이는 사용자 및 AMS 주소 공간 키 링 모두를 위한 경우입니다.

인증서 및 키 링 및 데이터 보호에서 이들에 역할에 대한 설명 및 추가 설명은 [인증서 관련 조작의 요약](#)을 참조하십시오.

서명 및 복호화에 사용되는 개인 키에는 레이블이 있을 수 있지만 기본 인증서로서 연결되어야 합니다.

디지털 인증서 및 키 링은 주로 RACDCERT 명령을 사용하여 RACF에서 관리됩니다.

인증서, 레이블 및 RACDCERT 명령에 대한 자세한 정보는 z/OS: 보안 서버 RACF 명령어 참조 및 z/OS 보안 서버 RACF 보안 관리자 안내서를 참조하십시오.

z/OS RACDCERT 명령에 대한 액세스 권한 부여

RACDCERT 명령을 사용하기 위한 권한 부여는 z/OS 시스템 프로그래머가 완료해야 하는 설치 후 작업입니다. 이 태스크는 Advanced Message Security 보안 관리자에 관련 권한을 부여하는 것과 관련됩니다.

요약하면 이러한 명령은 RACF RACDCERT 명령에 대한 액세스를 허용하기 위해 필요합니다.

```
RDEFINE FACILITY IRR.DIGTCERT.* UACC(NONE)
PERMIT IRR.DIGTCERT.* CLASS(FACILITY) ID( admin ) ACCESS(CONTROL)
SETROPTS RACLIST(FACILITY) REFRESH
```

이 예에서 *admin*은 보안 관리자의 사용자 ID 또는 RACDCERT 명령을 사용하기를 원하는 모든 사용자를 지정합니다.

z/OS 인증서 및 키 링 작성

이 절에서는 RACF CA (Certificate Authority) 를 사용하여 Advanced Message Security 의 z/OS 사용자 (AMS) 에게 필요한 인증서 및 키 링을 작성하는 데 필요한 단계를 설명합니다.

z/OS 에서 Advanced Message Security 를 사용할 때 인증서에 대한 문제점 해결

인증서 관련 문제가 있고 키 저장소에 항목이 누락된 경우 GSKIT 추적을 사용으로 설정할 수 있습니다.

AMS 시작된 태스크 프로시저의 ENVARS DD에서 참조하는 파일에 다음을 추가하십시오.

```
GSK_TRACE_FILE=/u/... /gsktrace
GSK_TRACE=0xff
```

자세한 정보는 [환경 변수](#)를 참조하십시오.

키 저장소에 대한 모든 액세스의 경우 GSK_TRACE_FILE에 지정된 추적 파일에 데이터가 기록됩니다.

추적 파일을 형식화하려면 다음 명령을 사용하십시오.

```
gsktrace inputtrace file > output_file
```

시나리오

송신 애플리케이션 및 수신 애플리케이션의 시나리오가 필수 단계를 설명하는 데 사용됩니다.

다음 예에서 *user1* 은 메시지의 발신자이고 *user2*는 수신인입니다. Advanced Message Security 주소 공간의 사용자 ID는 *WMQAMSD*입니다.

여기에 표시된 예의 모든 명령은 관리 사용자 ID *admin*에 의해 ISPF 옵션 6에서 실행됩니다.

z/OS 로컬 인증 기관 인증서 정의

RACF를 CA로서 사용 중인 경우에는 아직 하지 않은 경우 인증 기관 인증서를 작성해야 합니다. 여기에 표시된 명령은 인증 기관(또는 서명자) 인증서를 작성합니다. 이 예는 Advanced Message Security 사용자 및 애플리케이션의 ID를 반영하는 후속 인증서를 작성할 때 사용될 AMSCA라는 인증서를 작성합니다.

이 명령, 특히 SUBJECTSDN은 설치에 사용된 이름 지정 구조 및 규칙을 반영하기 위해 수정될 수도 있습니다.

```
RACDCERT CERTAUTH GENCERT SUBJECTSDN(CN('AMSCA') O('ibm') C('us'))
KEYUSAGE(CERTSIGN) WITHLABEL('AMSCA')
```

참고: 이 로컬 인증 기관 인증서로 서명되는 인증서는 RACDCERT LIST 명령으로 나열될 때 CN=AMSCA,O=ibm,C=us의 발행인을 표시합니다.

z/OS 개인 키로 디지털 인증서 작성

개인 키가 있는 디지털 인증서는 각 Advanced Message Security 사용자에게 대해 생성되어야 합니다. 여기에 표시된 예에서 RACDCERT 명령은 사용자 user1 및 user2에 대해 인증서를 생성하는 데 사용되고, 이는 레이블 AMSCA에 의해 식별되는 로컬 CA 인증서로 서명됩니다.

```
RACDCERT ID(user1) GENCERT SUBJECTSDN(CN('user1') O('ibm') C('us'))
WITHLABEL('user1') SIGNWITH(CERTAUTH LABEL('AMSCA'))
KEYUSAGE(HANDSHAKE DATAENCRYPT DOCSIGN)

RACDCERT ID(user2) GENCERT SUBJECTSDN(CN('user2') O('ibm') C('us'))
WITHLABEL('user2') SIGNWITH(CERTAUTH LABEL('AMSCA'))
KEYUSAGE(HANDSHAKE DATAENCRYPT DOCSIGN)

RACDCERT ID(user1) ALTER (LABEL('user1')) TRUST
RACDCERT ID(user2) ALTER (LABEL('user2')) TRUST
```

RACDCERT ALTER 명령은 TRUST 속성을 인증서에 추가하는 데 필요합니다. 먼저 인증서가 이 프로시저를 사용하여 작성되면 이는 서명 인증서와는 유효 날짜 범위가 다릅니다. 따라서 RACF는 이를 NOTRUST로 표시하는데 이는 인증서를 사용할 수 없음을 의미합니다. RACDCERT ALTER 명령을 사용하여 TRUST 속성을 설정하십시오.

KEYUSAGE 속성 HANDSHAKE, DATAENCRYPT 및 DOCSIGN은 Advanced Message Security에 의해 사용되는 인증서에 대해 지정되어야 합니다.

표 102. RACDCERT KEYUSAGE 값 및 표시기	
KEYUSAGE 값	표시기 세트
HANDSHAKE	digitalSignature 및 keyEncipherment
DATAENCRYPT	dataEncipherment
DOCSIGN	nonRepudiation
CERTSIGN	keyCertSign 및 cRLSign

z/OS RACF 키 링 작성

여기 표시된 명령은 RACF-정의된 사용자 ID user1, user2 및 Advanced Message Security 주소 공간 태스크 사용자 WMQAMSD를 위해 키 링을 작성합니다. 키 링 이름은 Advanced Message Security에 의해 수정되고 표시된 대로 따옴표 없이 코드화되어야 합니다. 이름은 대소문자를 구분합니다.

```
RACDCERT ID(user1) ADDRING(drq.ams.keyring)
RACDCERT ID(user2) ADDRING(drq.ams.keyring)
RACDCERT ID(WMQAMSD) ADDRING(drq.ams.keyring)
```

z/OS 키 링에 인증서 연결

사용자 및 CA 인증서를 키 링에 연결하십시오.

```
RACDCERT ID(WMQAMSD) CONNECT(CERTAUTH LABEL('AMSCA')
RING(drq.ams.keyring))
RACDCERT ID(user1) CONNECT(ID(user1) LABEL('user1')
RING(drq.ams.keyring) DEFAULT USAGE(PERSONAL))
RACDCERT ID(user2) CONNECT(ID(user2) LABEL('user2')
RING(drq.ams.keyring) DEFAULT USAGE(PERSONAL))
RACDCERT ID(WMQAMSD) CONNECT(ID(user2) LABEL('user2')
RING(drq.ams.keyring) USAGE(SITE))
```

복호화에 사용되는 개인 키를 포함하는 인증서는 사용자의 키 링에 기본 인증서로서 연결되어야 합니다.

RACDCERT USAGE(SITE) 속성은 개인 키가 키 링에 액세스하지 못하도록 하는 반면에 RACDCERT USAGE(PERSONAL) 속성은 개인 키가 사용되도록 허용합니다(있는 경우). 메시지를 큐에 넣을 때 메시지를 암호화하는 데 공용 키가 필요하기 때문에 User2의 인증서는 Advanced Message Security 주소 공간 키 링에 연결되어야 합니다. USAGE(SITE)는 user2의 개인 키의 노출을 제한합니다.

AMSCA 레이블이 있는 CERTAUTH 인증서는 메시지 발신자인 user1의 인증서에 서명하는 데 사용되었기 때문에 Advanced Message Security 주소 공간 키 링에 연결되어야 합니다. user1의 서명 인증서를 유효성 검증하는 데 사용됩니다.

z/OS 키 링 확인

키 링은 모든 명령이 입력된 후에 여기에 표시된 것과 같이 표시되어야 합니다.

```
RACDCERT ID(user1) LISTRING(drq.ams.keyring)
Digital ring information for user USER1:
Ring:>drq.ams.keyring<:

Certificate Label Name      Cert Owner  USAGE      DEFAULT
-----
user1                       ID(USER1)  PERSONAL   YES

RACDCERT ID(user2) LISTRING(drq.ams.keyring)
Digital ring information for user USER2:
Ring:>drq.ams.keyring<:

Certificate Label Name      Cert Owner  USAGE      DEFAULT
-----
user2                       ID(USER2)  PERSONAL   YES

RACDCERT ID(WMQAMSD) LISTRING(drq.ams.keyring)
Digital ring information for user WMQAMSD:
Ring:>drq.ams.keyring<:

Certificate Label Name      Cert Owner  USAGE      DEFAULT
-----
AMSCA                       CERTAUTH   CERTAUTH   NO
user2                       ID(USER2)  SITE       NO
```

개별 인증서 나열은 또한 링 연관을 표시합니다.

```
RACDCERT ID(user2) LIST(label('user2'))
Digital certificate information for user USER2:

***
Label: user2
Certificate ID: 2QfH8Pny9/LzpKKFmFFA
Status: TRUST
Start Date: 2010/05/03 22:59:53
End Date: 2011/05/04 22:59:52
Serial Number:>15<:
Issuer's Name:>OU=AMSCA.O=ibm.C=us<:
Subject's Name:>CN=user2.O=ibm.C=us<:
Key Usage: HANDSHAKE, DATAENCRYPT, DOCSIGN
Private Key Type: Non-ICSF
Private Key Size: 1024
Ring Associations:
```



```

Ring Owner: USER2
Ring:>drq.ams.keyring<:
Ring Owner: WMQAMSD
Ring:>drq.ams.keyring<:

```

성능을 개선하려면 AMS 주소 공간과 연관된 drq.ams.keyring의 콘텐츠가 주소 공간의 수명 동안 캐시됩니다. 해당 키 링의 변경사항은 자동으로 효력이 생기지 않습니다. 관리자는 다음을 수행하여 캐시를 새로 고칠 수 있습니다.

- 큐 관리자를 중지한 후 재시작하십시오.
- z/OS MODIFY 명령 사용:

```
F qmgrAMSM,REFRESH KEYRING
```

관련 태스크

Advanced Message Security 작동

z/OS 인증서 관련 조작 요약

568 페이지의 그림 35에서는 송신 및 수신 애플리케이션과 관련 인증서 사이의 관계를 보여줍니다. 설명된 시나리오는 개인정보의 데이터 보호 정책을 사용하는 두 개의 z/OS 큐 관리자 간의 리모트 큐잉과 관련됩니다. 568 페이지의 그림 35에서, "AMS"는 "Advanced Message Security"를 표시합니다.

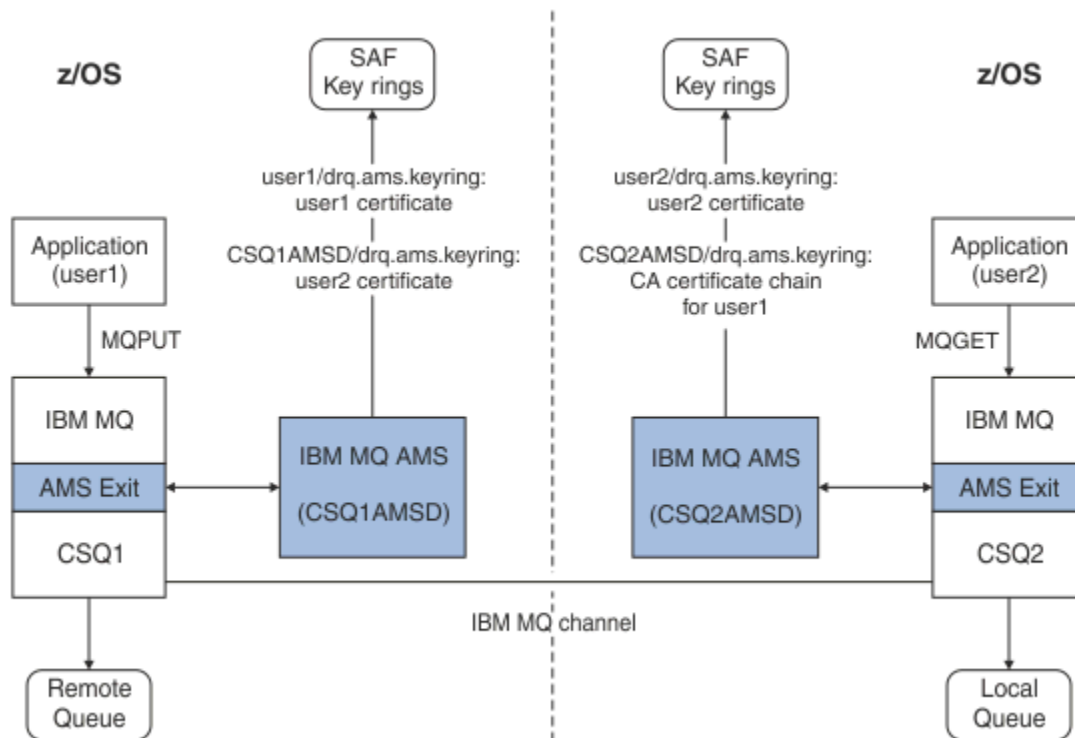


그림 35. 애플리케이션 및 인증서 관계

이 다이어그램에서 'user1'로서 실행 중인 애플리케이션은 CSQ2 큐 관리자가 관리하는 로컬 큐에서 'user2'로서 실행 중인 애플리케이션에 의해 검색될 메시지를 CSQ1 큐 관리자가 관리하는 리모트 큐에 넣습니다. 다이어그램은 개인정보의 Advanced Message Security 정책을 가정하고, 이는 메시지가 서명되고 암호화됨을 의미합니다.

Advanced Message Security는 넣기가 발생할 때 메시지를 인터셉트하고 user2의 인증서(AMS 주소 공간 사용자의 키 링에 저장됨)를 사용하여 메시지 데이터를 암호화하는 데 사용되는 대칭 키를 암호화합니다.

'user2'의 메시지는 옵션 USAGE(SITE)를 사용하여 AMS 주소 공간 사용자 키 링에 연결됨을 유의하십시오. 즉, AMS 주소 공간 사용자는 인증서 및 공개 키에 액세스할 수 있지만 개인 키에는 액세스할 수 없습니다.

수신측에서 Advanced Message Security는 user2에 의해 실행된 가져오기를 인터셉트하고 user2의 인증서를 사용하여 메시지 데이터를 복호화할 수 있도록 대칭 키를 복호화합니다. 그런 다음 AMS 주소 공간 사용자의 키 링에 저장된 user1의 인증서의 CA 인증서 체인을 사용하여 user1의 서명을 유효성 검증합니다.

이 시나리오가 무결성의 데이터 보호 정책과 함께 제공되면 user2의 인증서는 필요하지 않습니다.

Advanced Message Security를 사용하여 개인정보 보호 또는 무결성의 메시지 보호 정책이 있는 IBM MQ 보호 큐에서 메시지를 큐에 삽입하려면 Advanced Message Security에 다음과 같은 데이터 항목에 대한 액세스 권한이 있어야 합니다.

- 사용자가 메시지를 큐에 삽입하기 위한 X.509 V2 또는 V3 인증서 및 개인 키.
- 모든 메시지 서명자의 디지털 인증서에 서명하는 데 사용되는 인증서 체인.
- 데이터 보호 정책이 개인정보 보호인 경우에는 의도한 수신인의 X.509 V2 또는 V3 인증서. 의도된 수신인은 큐와 연관된 Advanced Message Security 정책에 나열되어 있습니다.

z/OS에서 실행되는 프로세스 및 애플리케이션의 경우, Advanced Message Security에는 다음 두 장소에 인증서가 있어야 합니다.

- 송신 애플리케이션(보호된 메시지를 큐에 삽입하는 애플리케이션) 또는 수신 애플리케이션(개인정보 보호를 사용하는 경우)의 RACF ID와 연관된 SAF 관리 키 링.

Advanced Message Security가 찾는 인증서는 기본 인증서이고 개인 키를 포함해야 합니다. Advanced Message Security에서는 송신 애플리케이션의 z/OS 사용자 ID를 가정합니다. 즉, 사용자의 개인 키에 액세스할 수 있도록 대리 역할을 합니다.

- AMS 주소 공간 사용자와 연관된 SAF 관리 키 링.

개인정보 보호로 보호된 메시지를 송신할 때 이 키 링에는 메시지 수신인의 공개 키 인증서가 포함됩니다. 메시지를 수신할 때 이는 메시지 송신자의 서명을 유효성 검증하는 데 필요한 인증 기관 인증서 체인을 포함합니다.

앞서 표시된 예에서는 RACF를 로컬 CA로 사용했습니다. 그러나 또 다른 PKI 제공자(인증 기관)를 사용할 수도 있습니다. If you intend to use another PKI product, remember that the private key and the certificate must be imported into a key ring associated with the z/OS RACF user IDs that originate IBM MQ messages protected by Advanced Message Security.

RACF RACDCERT 명령을 인증서 요청을 생성하기 위해 메커니즘으로 사용할 수 있고, 이는 사용자가 선택하려고 선택한 PKI 제공자로 내보내기되고 전송될 수 있습니다.

다음은 인증서 관련 단계의 요약입니다.

1. RACF가 로컬 CA인 CA 인증서의 작성을 요청하십시오. 또 다른 PKI 제공자를 사용 중인 경우에는 이 단계를 생략하십시오.
2. CA가 서명한 사용자 인증서를 생성하십시오.
3. 사용자 및 Advanced Message Security AMS 주소 공간 ID의 키 링을 작성하십시오.
4. 기본 속성을 사용하여 사용자 인증서를 사용자 키 링에 연결하십시오.
5. 사용법(사이트) 속성을 사용하여 수신인 인증서를 Advanced Message Security AMS 주소 공간 사용자 키 링에 연결하십시오. (이 단계는 궁극적으로 개인정보 보호된 메시지의 수신인이 될 사용자 인증서에만 필수입니다.)
6. 메시지 송신자의 CA 인증서 체인을 Advanced Message Security AMS 주소 공간 사용자 키 링에 연결하십시오. (이 단계는 송신자 서명을 확인할 AMS 태스크에만 필요합니다.)

비z/OS 레지던트 PKI 구성

Advanced Message Security for z/OS, uses X.509 V3 digital certificates in the protection-processing of messages placed on or received from IBM MQ queues. Advanced Message Security 자체는 이러한 인증서의 라이프 사이클을 작성하거나 관리하지 않습니다. 해당 기능은 PKI(Public Key Infrastructure)에 의해 제공됩니다. 인증서의 사용을 설명하는 이 발행물의 예에서는 인증서 요청을 수행하기 위해 z/OS 보안 서버 RACF를 사용합니다.

z/OS 또는 비z/OS 상주 PKI가 사용되는지 여부에 관계없이 z/OS 에 대해 AMS 는 RACF 또는 이와 동등한 것으로 관리되는 키 링만 사용합니다. These key rings are based on Security Authorization Facility (SAF) and are

the repository used by AMS for z/OS to retrieve certificates for originators and recipients of messages placed on or received from IBM MQ queues.

무결성 또는 암호화 정책에 의해 보호되는 z/OS에서 시작되는 메시지의 경우 발신 사용자 ID의 인증서 및 개인 키는 메시지 발신자의 z/OS 사용자 ID와 연관된 SAF 관리 키 링에 저장되어야 합니다.

RACF에는 인증서 및 개인 키를 RACF 관리 키 링으로 가져오기 위한 기능이 포함됩니다. 인증서를 RACF 관리 키 링에 로드하는 방법에 대한 세부사항 및 예제는 z/OS Security Server RACF 서적을 참조하십시오.

설치가 지원되는 PKI 제품 중 하나를 사용 중인 경우에는 이를 배치하는 방법에 대한 정보는 제품과 함께 제공되는 발행물을 참조하십시오.

Advanced Message Security 보안 정책 관리

Advanced Message Security는 보안 정책을 사용하여 큐를 통해 플로우하는 메시지를 암호화 및 인증하기 위한 암호화 및 서명 알고리즘을 지정합니다.

AMS에 대한 보안 정책 개요

Advanced Message Security 보안 정책은 메시지가 암호학적으로 암호화되고 서명되는 방법을 설명하는 개념적 오브젝트입니다.

보안 정책 속성의 세부사항은 다음 하위 주제를 참조하십시오.

관련 개념

[574 페이지의 『보호 품질』](#)

Advanced Message Security 데이터 보호 정책은 QoP(Quality of Protection)를 의미합니다.

[573 페이지의 『AMS의 보안 정책 속성』](#)

Advanced Message Security를 사용하여 데이터를 보호하기 위한 특정 알고리즘 또는 방법을 선택할 수 있습니다.

AMS의 정책 이름

정책 이름은 특정 Advanced Message Security 정책 및 이를 적용하는 큐를 식별하는 고유 이름입니다.

정책 이름은 정책이 적용되는 큐 이름과 같아야 합니다. Advanced Message Security(AMS) 정책 및 큐 간의 일대일 맵핑이 있습니다.

큐와 이름이 같은 정책을 작성함으로써 해당 큐의 정책을 활성화합니다. 일치하는 정책 이름이 없는 큐는 AMS에 의해 보호되지 않습니다.

정책의 범위는 로컬 큐 관리자 및 해당 큐와 관련됩니다. 리모트 큐 관리자에는 이들이 관리하는 큐에 로컬에 정의된 자체 정책이 있어야 합니다..

AMS에서 서명 알고리즘

서명 알고리즘은 데이터 메시지에 서명할 때 사용되어야 하는 알고리즘을 나타냅니다.

유효한 값은 다음을 포함합니다.

- MD5
- SHA-1
- SHA-2 제품군:
 - SHA256
 - SHA384(허용 가능한 최소 키 길이 - 768비트)
 - SHA512(허용 가능한 최소 키 길이 - 768비트)

서명 알고리즘을 지정하지 않거나 NONE의 알고리즘을 지정하는 정책은 정책과 연관된 큐에 배치된 메시지가 서명되지 않음을 암시합니다.

참고: 메시지 넣기 및 가져오기 함수에 사용되는 보호의 품질은 일치해야 합니다. 큐와 큐에 있는 메시지 간의 정책 보호 품질이 불일치하면 메시지는 허용되지 않고 오류 처리 큐로 전송됩니다. 이 규칙은 로컬 및 리모트 큐 둘 모두에 적용됩니다.

AMS에서 암호화 알고리즘

암호화 알고리즘은 암호화 데이터 메시지가 정책과 연관된 큐에 배치될 때 사용되어야 하는 알고리즘을 나타냅니다.

유효한 값은 다음을 포함합니다.

- RC2
- DES
- 3DES
- AES128
- AES256

암호화 알고리즘을 지정하지 않거나 NONE의 알고리즘을 지정하는 정책은 정책과 연관된 큐에 배치된 메시지가 암호화되지 않음을 암시합니다.

NONE이 아닌 암호화 알고리즘을 지정하는 정책은 또한 하나 이상의 수신인 DN 및 서명 알고리즘을 지정해야 합니다. Advanced Message Security 암호화된 메시지 또한 서명되기 때문입니다.

중요사항: 메시지 넣기 및 가져오기 함수에 사용되는 보호의 품질은 일치해야 합니다. 큐와 큐에 있는 메시지 간의 정책 보호 품질이 불일치하면 메시지는 허용되지 않고 오류 처리 큐로 전송됩니다. 이 규칙은 로컬 및 리모트 큐 둘 모두에 적용됩니다.

AMS의 허용

허용 속성은 Advanced Message Security가 보안 정책이 지정되지 않은 메시지를 승인할 수 있는지 여부를 나타냅니다.

메시지를 암호화하기 위한 정책이 있는 큐로부터 메시지를 검색할 때 메시지가 암호화되지 않은 경우에는 이는 호출 애플리케이션으로 돌아갑니다. 유효한 값은 다음을 포함합니다.

0 아니오(기본값).

1 예

허용 값을 지정하지 않거나 0을 지정하는 정책은 정책과 연관된 큐에 배치되는 메시지가 정책 규칙과 일치해야 함을 암시합니다.

허용은 선택사항이고 정책이 큐에 적용되었지만 이러한 큐에 이미 보안 정책이 지정되지 않은 메시지가 포함되어 있는 경우에 구성 공개를 쉽게 하기 위해 존재합니다.

AMS의 송신자 식별 이름

송신자 식별 이름(DN)은 메시지를 큐에 배치할 수 있는 권한을 가진 사용자를 식별합니다. 송신자는 메시지를 큐에 배치하기 전에 인증서를 사용하여 메시지에 서명합니다.

Advanced Message Security(AMS)는 큐가 검색될 때까지 메시지가 올바른 사용자에게 의해 데이터 보호된 큐에 배치되었는지 여부를 검사하지 않습니다. 이때 정책에 하나 이상의 올바른 송신자가 지정되어 있고 큐에 메시지를 배치한 사용자가 올바른 송신자 목록에 없는 경우, AMS는 수신 애플리케이션에 오류를 리턴하고 AMS 오류 큐에 메시지를 배치합니다.

정책에는 0개 이상의 송신자 DN이 지정될 수 있습니다. 정책에 송신자 DN이 지정되지 않은 경우 송신자는 송신자의 인증서가 신뢰되는 경우 데이터 보호 메시지를 큐에 넣을 수 있습니다. 송신자의 인증서는 수신 애플리케이션에 사용 가능한 키 저장소에 공용 인증서를 추가하여 신뢰할 수 있습니다.

송신자 식별 이름의 형식은 다음과 같습니다.

```
CN=Common Name,O=Organization,C=Country
```

중요사항:

- 모든 DN은 대문자여야 합니다. DN의 모든 구성요소 이름 ID는 다음 표에 표시된 순서대로 지정되어야 합니다.

컴포넌트 이름	값
CN	이 DN의 오브젝트의 공통 이름(예: 전체 이름 또는 디바이스의 의도된 용도).
OU	DN의 오브젝트가 가입된 조직 내의 단위(예: 회사 부서 또는 제품 이름).
O	DN의 오브젝트가 가입된 조직(예: 회사).
L	DN의 오브젝트가 위치한 로컬성(시 또는 지자체).
ST	DN의 오브젝트가 위치한 시/도 이름.
C	식별 이름(DN)의 오브젝트가 있는 국가.

- 하나 이상의 송신자 DN이 정책에 지정된 경우 해당 사용자만 정책과 연관된 큐에 메시지를 배치할 수 있습니다.
- 송신자 DN(지정된 경우)은 메시지를 배치하는 사용자와 연관된 디지털 인증서와 정확하게 일치해야 합니다.
- AMS는 라틴-1 문자 세트의 값만 있는 DN을 지원합니다. 이 세트의 문자로 DN을 작성하려면 먼저 UTF-8 코딩이 설정된 UNIX를 사용하거나 **strmqim** GUI를 사용하여 UTF-8 코딩으로 작성되는 DN으로 인증서를 작성해야 합니다. 그런 다음 UTF-8 코딩이 켜진 UNIX 플랫폼에서 정책을 작성하거나 IBM MQ에 대한 AMS 플러그인을 사용해야 합니다.
- AMS가 송신자 이름을 x.509 형식에서 DN 형식으로 변환하기 위해 사용하는 방법은 항상 시/도 값에 ST=를 사용합니다.
- 다음 특수 문자에는 이스케이프 문자가 필요합니다.

```

, (comma)
+ (plus)
" (double quote)
\ (backslash)
< (less than)
> (greater than)
; (semicolon)

```

- 식별 이름에 임베드된 공백이 포함된 경우 DN을 큰따옴표로 묶어야 합니다.

관련 개념

572 페이지의 『AMS의 수신인 식별 이름』

수신자 식별 이름(DN)은 큐로부터 메시지를 수신할 권한이 있는 사용자를 식별합니다.

AMS의 수신인 식별 이름

수신자 식별 이름(DN)은 큐로부터 메시지를 수신할 권한이 있는 사용자를 식별합니다.

정책에는 수신인 DN이 0개 이상 지정될 수 있습니다. 수신자 식별 이름 다음 양식을 가지고 있습니다.

CN=Common Name,O=Organization,C=Country

중요사항:

- 모든 DN은 대문자로 되어 있어야 합니다. 다음 표에 표시된 순서대로 DN에 있는 모든 구성요소 이름 ID를 지정해야 합니다.

컴포넌트 이름	가치
CN	이 DN의 오브젝트의 공통 이름(예: 전체 이름 또는 디바이스의 의도된 용도).
OU	DN의 오브젝트가 가입된 조직 내의 단위(예: 회사 부서 또는 제품 이름).
O	DN의 오브젝트가 가입된 조직(예: 회사).

컴포넌트 이름	가치
L	DN의 오브젝트가 위치한 로컬성(시 또는 지자체).
ST	DN의 오브젝트가 위치한 시/도 이름.
C	식별 이름(DN)의 오브젝트가 있는 국가.

- 정책에 수신인 DN이 지정되지 않으면 어느 사용자나 정책과 연관된 큐에서 메시지를 가져올 수 있습니다.
- 하나 이상의 수신자 DN이 정책에 지정된 경우 해당 사용자만 정책과 연관된 큐에서 메시지를 가져올 수 있습니다.
- 수신자 DN(지정된 경우)은 메시지를 가져오는 사용자와 연관된 디지털 인증서와 정확하게 일치해야 합니다.
- Advanced Message Security는 라틴-1 문자 세트의 값만 있는 DN을 지원합니다. 이 세트의 문자로 DN을 작성하려면 먼저 UTF-8 코딩이 설정된 UNIX를 사용하거나 **strmqikm** GUI를 사용하여 UTF-8 코딩으로 작성되는 DN으로 인증서를 작성해야 합니다. 그런 다음, UTF-8 코딩이 설정된 상태에서 UNIX 플랫폼에서 정책을 작성하거나 Advanced Message Security 플러그인을 IBM MQ에 사용해야 합니다.

관련 개념

571 페이지의 『AMS의 송신자 식별 이름』

송신자 식별 이름(DN)은 메시지를 큐에 배치할 수 있는 권한을 가진 사용자를 식별합니다. 송신자는 메시지를 큐에 배치하기 전에 인증서를 사용하여 메시지에 서명합니다.

AMS의 보안 정책 속성

Advanced Message Security를 사용하여 데이터를 보호하기 위한 특정 알고리즘 또는 방법을 선택할 수 있습니다.

보안 정책은 메시지가 암호학적으로 암호화되고 서명되는 방법을 설명하는 개념적 오브젝트입니다.

표 103. AMS의 보안 정책 속성	
속성	설명
정책 이름	큐 관리자의 정책의 고유 이름.
서명 알고리즘	전송하기 전에 메시지를 서명하는 데 사용되는 암호화 알고리즘.
암호화 알고리즘	전송하기 전에 메시지를 암호화하는 데 사용되는 암호화 알고리즘.
수신인 목록	메시지의 잠재적인 수신자의 인증서 식별 이름(DN) 목록.
서명 DN 체크리스트	메시지 검색 중에 유효성을 검증할 서명 DN 목록.

Advanced Message Security에서 메시지는 대칭 키로 암호화되고, 대칭 키는 수신인의 공개 키로 암호화됩니다. 공개 키는 유효 길이가 최대 2048비트인 키를 사용하여 RSA 알고리즘으로 암호화됩니다. 실제 비대칭 키 암호화는 인증서 키 길이에 따라 다릅니다.

지원되는 대칭-키 알고리즘은 다음과 같습니다.

- RC2
- DES
- 3DES
- AES128
- AES256

Advanced Message Security는 또한 다음과 같은 암호화 해시 함수를 지원합니다.

- MD5
- SHA-1

- SHA-2 제품군:
 - SHA256
 - SHA384(허용 가능한 최소 키 길이 - 768비트)
 - SHA512(허용 가능한 최소 키 길이 - 768비트)

참고: 메시지 넣기 및 가져오기 함수에 사용되는 보호의 품질은 일치해야 합니다. 큐와 큐에 있는 메시지 간의 정책 보호 품질이 불일치하면 메시지는 허용되지 않고 오류 처리 큐로 전송됩니다. 이 규칙은 로컬 및 리모트 큐 둘 모두에 적용됩니다.

보호 품질

Advanced Message Security 데이터 보호 정책은 QoP(Quality of Protection)를 의미합니다.

Advanced Message Security의 세 개의 QoP(Quality of Protection) 레벨은 IBM MQ 9.0이상에서 네 번째 레벨에 의해 보충되며 모두 메시지 서명 및 암호화에 사용되는 암호화 알고리즘에 따라 다릅니다.

- 개인정보 보호 - 큐에 배치된 메시지는 서명되고 암호화되어야 합니다.
- 무결성 - 큐에 배치된 메시지는 서명자에 의해 서명되어야 합니다.
- 기밀성 - 큐에 배치된 메시지는 암호화되어야 합니다. 자세한 정보는 507 페이지의 『AMS에서 사용 가능한 QoP(Quality of Protection)』의 내용을 참조하십시오.
- 없음 - 데이터 보호가 적용 가능하지 않습니다.

메시지는 큐에 배치될 때 서명되어야 함을 규정하는 정책에는 INTEGRITY의 QOP가 있습니다. INTEGRITY의 QOP는 정책이 서명 알고리즘을 규정하지만 암호화 알고리즘을 규정하지는 않음을 의미합니다. 무결성 보호된 메시지는 또한 "SIGNED"라고도 불립니다.

메시지는 큐에 배치될 때 서명되고 암호화되어야 함을 규정하는 정책에는 PRIVACY의 QOP가 있습니다. PRIVACY의 QOP는 정책이 서명 알고리즘 및 암호화 알고리즘을 규정하는 경우를 의미합니다. 개인정보 보호된 메시지는 또한 "SEALED"라고도 불립니다.

큐에 배치할 때 메시지를 암호화하도록 규정하는 정책에는 CONFIDENTIALITY의 QOP가 있습니다. 기밀성 (CONFIDENTIALITY)의 QOP는 정책이 암호화 알고리즘을 규정함을 의미합니다.

서명 알고리즘 또는 암호화 알고리즘을 규정하지 않는 정책에는 NONE의 QOP가 있습니다. Advanced Message Security에서는 NONE의 QOP가 있는 정책이 있는 큐에 대해 데이터 보호를 제공하지 않습니다.

보안 정책 관리

보안 정책은 메시지가 암호학적으로 암호화되고 서명되는 방법을 설명하는 개념적 오브젝트입니다.

보안 정책과 관련된 모든 관리 태스크를 실행하는 위치는 사용 중인 플랫폼 위치에 따라 다릅니다.

- **ULW** UNIX 및 Windows에서는 DELETE POLICY, DISPLAY POLICY 및 SET POLICY(또는 이에 상당하는 PCF) 명령을 사용하여 보안 정책을 관리할 수 있습니다.
 - **UNIX** UNIX에서 관리 태스크는 `MQ_INSTALLATION_PATH/bin`에서 실행될 수 있습니다.
 - **Windows** Windows 플랫폼에서 관리 태스크는 PATH 환경 변수가 설치 시 업데이트되므로 임의 위치에서 실행될 수 있습니다.
- **IBM i** IBM i에서 DSPMQMSPL, SETMQMSPL 및 WRKMQMSPL 명령은 IBM MQ가 설치될 때 시스템의 기본 언어의 QSYS 시스템 라이브러리에 설치됩니다.

추가로 자국어 버전인 언어 피쳐 로드예 따라 QSYS29xx 라이브러리에 설치됩니다. 예를 들어, 미국 영어를 기본 언어로 사용하고 한국어를 2차 언어로 사용하는 시스템에는 QSYS에 미국 영어 명령이 설치되고, 2962가 한국어의 언어 로드이므로 한국어가 QSYS2962에 로드되어 있습니다.
- **z/OS** z/OS에서 관리 명령은 메시지 보안 정책 유틸리티(CSQ0UTIL)를 사용하여 실행됩니다. When policies are created, modified or deleted on z/OS, the changes are not recognized by Advanced Message

Security until the queue manager is stopped and restarted, or the z/OS MODIFY command is used to refresh the Advanced Message Security policy configuration. 예를 들면, 다음과 같습니다.

```
F <qmgr ssid>AMSM,REFRESH POLICY
```

관련 태스크

[575 페이지의 『AMS에서 보안 정책 작성』](#)

보안 정책은 메시지를 놓일 때 메시지가 보호되는 방법 또는 메시지를 수신할 때 메시지를 보호해야 하는 방법을 정의합니다.

[576 페이지의 『AMS에서 보안 정책 변경』](#)

Advanced Message Security를 사용하여 이미 정의한 보안 정책의 세부사항을 변경할 수 있습니다.

[576 페이지의 『AMS의 보안 정책 표시 및 덤프』](#)

dspmqsp1 명령을 사용하여 사용자가 제공하는 명령행 매개변수에 따라 모든 보안 정책 목록 또는 이름 지정된 정책의 세부사항을 표시할 수 있습니다.

[578 페이지의 『AMS에서 보안 정책 제거』](#)

Advanced Message Security에서 보안 정책을 제거하려면 **setmqsp1** 명령을 사용해야 합니다.

Advanced Message Security 작동

관련 참조

[메시지 보안 정책 유틸리티\(CSQOUTIL\)](#)

AMS에서 보안 정책 작성

보안 정책은 메시지를 놓일 때 메시지가 보호되는 방법 또는 메시지를 수신할 때 메시지를 보호해야 하는 방법을 정의합니다.

시작하기 전에

보안 정책을 작성할 때 준수해야 하는 몇 가지 초기 조건이 있습니다.

- 큐 관리자가 실행 중이어야 합니다.
 - 보안 정책의 이름은 **IBM MQ 오브젝트 이름 지정 규칙**을 따라야 합니다.
 - 큐 관리자에 연결하고 보안 정책을 작성하기 위해서는 필수 권한이 있어야 합니다:
 - **z/OS** z/OS에서 [메시지 보안 정책 유틸리티\(CSQOUTIL\)](#)에 문서화된 권한을 부여하십시오.
 - **Multi** z/OS가 아닌 다른 플랫폼에서는 [setmqaut](#) 명령을 사용하여 필수 +connect, +inq 및 +chg 권한을 부여해야 합니다.
- 보안 구성에 대한 자세한 정보는 [112 페이지의 『보안 설정』](#)의 내용을 참조하십시오.
- **z/OS** z/OS에서 필수 시스템 오브젝트가 CSQ4INSM에서 정의에 따라 정의되었는지 확인하십시오.

예

다음은 QMGR 큐 관리자에서 정책 작성의 예입니다. 정책은 SHA256 알고리즘을 사용하여 메시지를 서명하고 DN이 CN=joe, O=IBM, C=US 및 DN: CN=jane, O=IBM, C=US인 인증서에 대해 AES256 알고리즘을 사용하여 암호화하도록 지정합니다. 이 정책은 MY.QUEUE에 첨부됩니다.

```
setmqsp1 -m QMGR -p MY.QUEUE -s SHA256 -e AES256 -r CN=joe,O=IBM,C=US -r CN=jane,O=IBM,C=US
```

다음은 QMGR 큐 관리자에서 정책 작성의 예입니다. 이 정책은 DN이 있는 인증서에 대해 3DES 알고리즘을 사용하여 메시지를 암호화하도록 지정합니다. CN=john, O=IBM, C=US 및 CN=jeff, O=IBM, C=US 및 DN이 있는 인증서에 대한 SHA256 알고리즘: CN=phil, O=IBM, C=US

```
setmqsp1 -m QMGR -p MY.OTHER.QUEUE -s SHA256 -e 3DES -r CN=john,O=IBM,C=US -r CN=jeff,O=IBM,C=US -a CN=phil,O=IBM,C=US
```

참고:

- 메시지 넣기 및 가져오기에 사용되는 보호의 품질은 일치해야 합니다. 메시지에 정의된 정책 보호 품질은 큐에 정의된 것보다 약하고, 메시지는 오류 처리 큐로 전송됩니다. 이 정책은 로컬 및 리모트 큐 둘 모두에 대해 유효합니다.



관련 참조

[setmqspl 명령 속성의 전체 목록](#)

AMS에서 보안 정책 변경

Advanced Message Security를 사용하여 이미 정의한 보안 정책의 세부사항을 변경할 수 있습니다.

시작하기 전에

- 운영하려는 큐 관리자가 실행 중이어야 합니다.
- 큐 관리자에 연결하고 보안 정책을 작성하기 위해서는 필수 권한이 있어야 합니다.
 -  z/OS에서 [메시지 보안 정책 유틸리티\(CSQOUTIL\)](#)에 문서화된 권한을 부여하십시오.
 -  z/OS가 아닌 다른 플랫폼에서는 [setmqaut](#) 명령을 사용하여 필수 +connect, +inq 및 +chg 권한을 부여해야 합니다.

보안 구성에 대한 자세한 정보는 [112 페이지의 『보안 설정』](#)의 내용을 참조하십시오.

이 태스크 정보

보안 정책을 변경하려면 `setmqspl` 명령을 이미 존재하는 정책에 적용하여 새 속성을 제공하십시오.

예

다음은 QMGR이라는 큐 관리자에서 MYQUEUE 정책을 작성하는 예입니다. 이 정책은 CN=alice, O=IBM, C=US의 식별 이름 (DN) 이 있는 인증서를 가지고 있는 작성자 (-a) 의 3DES 알고리즘을 사용하여 암호화되고, DN이 CN=jeff인 인증서가 있는 수신자 (-r) 의 SHA256 알고리즘을 사용하여 서명됩니다 (예:IBM).

```
setmqspl -m QMGR -p MYQUEUE -e 3DES -s SHA256 -a CN=jeff,O=IBM,C=US -r CN=alice,O=IBM,C=US
```

이 정책을 변경하려면 `setmqspl` 명령을 예외 모든 속성과 함께 실행하여 수정하려는 값만을 변경하십시오. 이 예에서 이전에 작성된 정책이 새 큐에 첨부되고 해당 암호화 알고리즘이 AES256으로 변경됩니다.

```
setmqspl -m QMGR -p MYQUEUE -e AES256 -s SHA256 -a CN=jeff,O=IBM,C=US -r CN=alice,O=IBM,C=US
```



관련 참조

[setmqspl\(보안 정책 설정\)](#)

AMS의 보안 정책 표시 및 덤프

`dspmqspl` 명령을 사용하여 사용자가 제공하는 명령행 매개변수에 따라 모든 보안 정책 목록 또는 이름 지정된 정책의 세부사항을 표시할 수 있습니다.

시작하기 전에

- 보안 정책 세부사항을 표시하기 위해서는 큐 관리자가 존재하고 실행 중이어야 합니다.
- 큐 관리자에 연결하고 보안 정책을 작성하기 위해서는 필수 권한이 있어야 합니다.
 -  z/OS에서 [메시지 보안 정책 유틸리티\(CSQOUTIL\)](#)에 문서화된 권한을 부여하십시오.
 -  z/OS가 아닌 다른 플랫폼에서는 [setmqaut](#) 명령을 사용하여 필수 +connect, +inq 및 +chg 권한을 부여해야 합니다.

보안 구성에 대한 자세한 정보는 [112 페이지의 『보안 설정』](#)의 내용을 참조하십시오.

이 태스크 정보

다음은 `dspmqsp1` 명령 플래그의 목록입니다.

표 104. <code>dspmqsp1</code> 명령 플래그.	
명령 플래그	설명
<code>-m</code>	큐 관리자 이름(필수).
<code>-p</code>	정책 이름.
<code>-export</code>	이 플래그를 추가하면 다른 큐 관리자에 쉽게 적용할 수 있는 출력이 생성됩니다.

예

다음 예에서는 `venus.queue.manager`를 위해 두 개의 보안 정책을 작성하는 방법을 보여줍니다.

```
setmqsp1 -m venus.queue.manager -p AMS_POL_04_ONE -s sha256 -a "CN=signer1,O=IBM,C=US" -e NONE
setmqsp1 -m venus.queue.manager -p AMS_POL_06_THREE -s sha256 -a "CN=another signer,O=IBM,C=US"
-e NONE
```

이 예는 `venus.queue.manager`에 대해 정의된 모든 정책 및 생성되는 출력에 대한 세부사항을 표시하는 명령을 보여줍니다.

```
dspmqsp1 -m venus.queue.manager
```

```
Policy Details:
Policy name: AMS_POL_04_ONE
Quality of protection: INTEGRITY
Signature algorithm: SHA256
Encryption algorithm: NONE
Signer DNS:
  CN=signer1,O=IBM,C=US
Recipient DNS: -
Toleration: 0
-----
```

```
Policy Details:
Policy name: AMS_POL_06_THREE
Quality of protection: INTEGRITY
Signature algorithm: SHA256
Encryption algorithm: NONE
Signer DNS:
  CN=another signer,O=IBM,C=US
Recipient DNS: -
Toleration: 0
```

이 예는 `venus.queue.manager`에 대해 정의된 선택된 보안 정책 및 생성되는 출력에 대한 세부사항을 표시하는 명령을 보여줍니다.

```
dspmqsp1 -m venus.queue.manager -p AMS_POL_06_THREE
```

```
Policy Details:
Policy name: AMS_POL_06_THREE
Quality of protection: INTEGRITY
Signature algorithm: SHA256
Encryption algorithm: NONE
Signer DNS:
  CN=another signer,O=IBM,C=US
Recipient DNS: -
Toleration: 0
```

다음 예에서는 먼저, 보안 정책을 작성한 다음에 **-export** 플래그를 사용하여 정책을 내보냅니다.

```
setmqsp1 -m venus.queue.manager -p AMS_POL_04_ONE -s SHA256 -a "CN=signer1,O=IBM,C=US" -e NONE
dspmqsp1 -m venus.queue.manager -export
```

z/OS z/OS에서 내보내기된 정책 정보는 CSQ0UTIL에 의해 EXPORT DD에 작성됩니다.

Multi z/OS 이외의 플랫폼에서 출력을 파일로 경로 재지정하십시오. 예:

```
dspmqspl -m venus.queue.manager -export > policies.[bat|sh]
```

보안 정책을 가져오려면:

- **Windows** Windows에서 policies.bat을(를) 실행하십시오.
- **UNIX** UNIX에서:
 1. mqm IBM MQ 관리 그룹에 속하는 사용자로서 로그인하십시오.
 2. . policies.sh를 실행하십시오.
- **z/OS** z/OS에서 CSQ0UTIL 유틸리티를 사용하여 내보낸 정책 정보를 포함하는 데이터 세트를 SYSIN에 지정하십시오.

관련 참조

[dspmqspl 명령 속성의 전체 목록](#)

AMS에서 보안 정책 제거

Advanced Message Security에서 보안 정책을 제거하려면 setmqspl 명령을 사용해야 합니다.

시작하기 전에

보안 정책을 관리할 때 준수해야 하는 몇 가지 초기 조건이 있습니다.

- 큐 관리자가 실행 중이어야 합니다.
- 큐 관리자에 연결하고 보안 정책을 작성하기 위해서는 필수 권한이 있어야 합니다.
 - **z/OS** z/OS에서 [메시지 보안 정책 유틸리티\(CSQ0UTIL\)](#)에 문서화된 권한을 부여하십시오.
 - **Multi** z/OS가 아닌 다른 플랫폼에서는 [setmqaut](#) 명령을 사용하여 필수 +connect, +inq 및 +chg 권한을 부여해야 합니다.

보안 구성에 대한 자세한 정보는 [112 페이지의 『보안 설정』](#)의 내용을 참조하십시오.

이 태스크 정보

setmqspl 명령을 **-remove** 옵션과 함께 사용하십시오.

예

다음은 정책 제거의 예입니다.

```
setmqspl -m QMGR -remove -p MY.OTHER.QUEUE
```

관련 참조

[setmqspl 명령 속성의 전체 목록](#)

AMS의 시스템 큐 보호

시스템 큐를 사용하면 IBM MQ와 해당 보조 애플리케이션 사이의 통신이 가능합니다. 큐 관리자가 작성될 때마다 시스템 큐 또한 IBM MQ 내부 메시지 및 데이터를 저장하기 위해 작성됩니다. 권한 있는 사용자만이 액세스하거나 복호화할 수 있도록 시스템 큐를 Advanced Message Security로 보호할 수 있습니다.

시스템 큐 보호는 일반 큐의 보호와 같은 패턴을 따릅니다. [575 페이지의 『AMS에서 보안 정책 작성』](#)의 내용을 참조하십시오.

Windows Windows에서 시스템 큐 보호를 사용하려면 keystore.conf 파일을 다음 디렉토리로 복사하십시오.







```
c:\Documents and Settings\Default User\.mq\keystore.conf
```

z/OS z/OS에서 SYSTEM.ADMIN.COMMAND.QUEUE에 대한 보호를 제공하려면 명령 서버가 키 및 구성을 포함하는 keystore 및 keystore.conf에 대한 액세스 권한이 있어야 명령 서버가 키 및 인증서에 액세스할 수 있습니다. SYSTEM.ADMIN.COMMAND.QUEUE의 보안 정책에 작성된 모든 변경사항을 적용하려면 명령 서버를 재시작해야 합니다.

명령 큐로부터 전송되고 수신된 모든 메시지는 정책 설정에 따라 서명되거나 서명된 후 암호화됩니다. 관리자가 권한 있는 서명자를 정의하는 경우, 서명자 식별 이름(DN) 검사를 통과하지 못한 명령 메시지는 명령 서버가 실행하지 않고 Advanced Message Security 오류 처리 큐로 라우트되지 않습니다. IBM MQ 탐색기 임시 동적 큐에 회신으로 전송된 메시지는 AMS에 의해 보호되지 않습니다.

보안 정책에는 다음 SYSTEM 큐에 영향을 미치지 않습니다.

- SYSTEM.ADMIN.ACCOUNTING.QUEUE
- SYSTEM.ADMIN.ACTIVITY.QUEUE
- SYSTEM.ADMIN.CHANNEL.EVENT
- SYSTEM.ADMIN.COMMAND.EVENT
- **z/OS** SYSTEM.ADMIN.COMMAND.QUEUE
- SYSTEM.ADMIN.CONFIG.EVENT
- SYSTEM.ADMIN.LOGGER.EVENT
- SYSTEM.ADMIN.PERFM.EVENT
- SYSTEM.ADMIN.PUBSUB.EVENT
- SYSTEM.ADMIN.QMGR.EVENT
- SYSTEM.ADMIN.STATISTICS.QUEUE
- SYSTEM.ADMIN.TRACE.ROUTE.QUEUE
- SYSTEM.AUTH.DATA.QUEUE
- SYSTEM.BROKER.ADMIN.STREAM
- **z/OS** SYSTEM.BROKER.CLIENTS.DATA
- SYSTEM.BROKER.CONTROL.QUEUE
- SYSTEM.BROKER.DEFAULT.STREAM
- SYSTEM.BROKER.INTER.BROKER.COMMUNICATIONS
- **z/OS** SYSTEM.BROKER.SUBSCRIPTIONS.DATA
- SYSTEM.CHANNEL.INITQ
- SYSTEM.CHANNEL.SYNCQ
- **z/OS** SYSTEM.CHLAUTH.DATA.QUEUE
- SYSTEM.CICS.INITIATION.QUEUE
- SYSTEM.CLUSTER.COMMAND.QUEUE
- SYSTEM.CLUSTER.HISTORY.QUEUE
- SYSTEM.CLUSTER.REPOSITORY.QUEUE
- SYSTEM.CLUSTER.TRANSMIT.QUEUE
- **z/OS** SYSTEM.COMMAND.INPUT
- **z/OS** SYSTEM.DDELAY.LOCAL.QUEUE

- SYSTEM.DEAD.LETTER.QUEUE
- SYSTEM.DURABLE.SUBSCRIBER.QUEUE
- SYSTEM.HIERARCHY.STATE
- SYSTEM.INTER.QMGR.CONTROL
- SYSTEM.INTER.QMGR.FANREQ
- SYSTEM.INTER.QMGR.PUBS
- SYSTEM.INTERNAL.REPLY.QUEUE
-  SYSTEM.JMS.PS.STATUS.QUEUE
-  SYSTEM.JMS.REPORT.QUEUE
- SYSTEM.PENDING.DATA.QUEUE
- SYSTEM.PROTECTION.ERROR.QUEUE
- SYSTEM.PROTECTION.POLICY.QUEUE
-  SYSTEM.QSG.CHANNEL.SYNCQ
-  SYSTEM.QSG.TRANSMIT.QUEUE
-  SYSTEM.QSG.UR.RESOLUTION.QUEUE
- SYSTEM.RETAINED.PUB.QUEUE
-  SYSTEM.RETAINED.PUB.QUEUE
- SYSTEM.SELECTION.EVALUATION.QUEUE
- SYSTEM.SELECTION.VALIDATION.QUEUE

OAM 권한 부여

파일 권한은 모든 사용자가 `setmqsp1` 및 `dspmqspl` 명령을 실행하기 위한 권한을 제공합니다. 그러나 Advanced Message Security는 오브젝트 권한 관리자(OAM)에 의존하고 IBM MQ 관리 그룹인 `mqm` 그룹에 속하지 않는 사용자 또는 부여된 보안 정책 설정을 읽을 권한이 없는 사용자가 이러한 명령을 실행하려고 시도할 때 마다 오류가 발생합니다.

프로시저

사용자에게 필수 권한을 부여하려면 다음을 실행하십시오.

```
setmqaut -m SOME.QUEUE.MANAGER -t qmgr -p SOME.USER +connect +inq
setmqaut -m SOME.QUEUE.MANAGER -t queue -n SYSTEM.PROTECTION.POLICY.QUEUE -p SOME.USER +browse
+put
setmqaut -m SOME.QUEUE.MANAGER -t queue -n SYSTEM.PROTECTION.ERROR.QUEUE -p SOME.USER +put
```

참고: Advanced Message Security 7.0.1을 사용하여 클라이언트를 큐 관리자에 연결하려면 이러한 OAM 권한을 설정하기만 하면 됩니다.



주의: SYSTEM.PROTECTION.POLICY.QUEUE에 대한 찾아보기 권한은 모든 상황에서 필수는 아닙니다. IBM MQ는 모든 경우에 SYSTEM.PROTECTION.POLICY.QUEUE의 정책 세부사항에 대한 레코드를 찾아볼 필요가 없도록 정책을 캐싱하여 성능을 최적화합니다.

IBM MQ가 사용 가능한 모든 정책을 캐시하지는 않습니다. 정책 수가 많으면 IBM MQ가 제한된 수의 정책을 캐시합니다. 따라서 큐 관리자에 적은 수의 정책이 정의되어 있는 경우 SYSTEM.PROTECTION.POLICY.QUEUE에 찾아보기 옵션을 제공할 필요가 없습니다.

그러나 많은 수의 정책이 정의되어 있거나 이전 클라이언트를 사용 중인 경우 이 큐에 대한 찾아보기 권한을 부여해야 합니다. SYSTEM.PROTECTION.ERROR.QUEUE는 AMS 코드에서 생성된 오류 메시지를 넣는 데 사용됩니다. 이 큐에 대한 넣기(Put) 권한은 오류 메시지를 큐에 넣으려고 할 때만 확인됩니다. AMS 보호 큐에서 메시지를 가져오거나 넣으려고 할 때는 큐에 대한 넣기(Put) 권한이 확인되지 않습니다.

보안 권한 부여


명령 자원 보안을 사용할 때 Advanced Message Security가 작동할 수 있도록 권한을 설정해야 합니다. 이 토픽은 예에서 RACF 명령을 사용합니다. 사용자의 엔터프라이즈가 다른 외부 보안 관리자(ESM)를 사용하는 경우에는 해당 ESM에 동등한 명령을 사용해야 합니다.

보안 권한을 부여하는 데에는 세 가지 측면이 있습니다.

- [581 페이지의 『AMSM 주소 공간』](#)
- [581 페이지의 『CSQOUTIL』](#)
- [582 페이지의 『Advanced Message Security 정책이 정의된 큐 사용』](#)

참고사항: 예 명령은 다음 변수를 사용합니다.

1. *QMgrName* - 큐 관리자의 이름.

 z/OS에서 이 값은 또한 큐 공유 그룹의 이름일 수도 있습니다.

2. *username* - 이는 그룹 이름일 수 있습니다.
3. 예는 MQQUEUE 클래스를 보여줍니다. 이는 또한 MXQUEUE, GMQUEUE 또는 GMXQUEUE일 수도 있습니다. 자세한 정보는 [179 페이지의 『큐 보안을 위한 프로파일』](#)의 내용을 참조하십시오.

게다가, 프로파일이 이미 있는 경우 RDEFINE 명령을 필요로 하지 않습니다.

AMSM 주소 공간

일부 IBM MQ 보안을 Advanced Message Security 주소 공간을 실행 중인 사용자 이름에 실행해야 합니다.

- 큐 관리자에 대한 배치 연결을 위해 다음을 실행하십시오.

```
RDEFINE MQCONN QMgrName.BATCH UACC(NONE)
PERMIT QMgrName.BATCH CLASS(MQCONN) ID(username) ACCESS(READ)
```

- SYSTEM.PROTECTION.POLICY.QUEUE에 대한 액세스의 경우 다음을 실행하십시오.

```
RDEFINE MQQUEUE QMgrName.SYSTEM.PROTECTION.POLICY.QUEUE UACC(NONE)
PERMIT QMgrName.SYSTEM.PROTECTION.POLICY.QUEUE CLASS(MQQUEUE)
ID(username) ACCESS(READ)
```

CSQOUTIL

사용자가 **setmqsp1** 및 **dspmqsp1** 명령을 실행하도록 허용하는 유틸리티에는 다음 권한이 필요합니다. 여기서 사용자 이름은 작업 사용자 ID입니다.

- 큐 관리자에 대한 배치 연결을 위해 다음을 실행하십시오.

```
RDEFINE MQCONN QMgrName.BATCH UACC(NONE)
PERMIT QMgrName.BATCH CLASS(MQCONN) ID(username) ACCESS(READ)
```

- **setmqpo1** 명령에 필요한 SYSTEM.PROTECTION.POLICY.QUEUE에 대한 액세스를 위해 다음을 실행하십시오.

```
RDEFINE MQQUEUE QMgrName.SYSTEM.PROTECTION.POLICY.QUEUE UACC(NONE)
PERMIT QMgrName.SYSTEM.PROTECTION.POLICY.QUEUE CLASS(MQQUEUE)
ID(username) ACCESS(ALTER)
```

- **dspmqpo1** 명령에 필요한 SYSTEM.PROTECTION.POLICY.QUEUE에 대한 액세스를 위해 다음을 실행하십시오.

```
RDEFINE MQQUEUE QMgrName.SYSTEM.PROTECTION.POLICY.QUEUE UACC(NONE)
PERMIT QMgrName.SYSTEM.PROTECTION.POLICY.QUEUE CLASS(MQQUEUE)
ID(username) ACCESS(READ)
```

Advanced Message Security 정책이 정의된 큐 사용

애플리케이션이 정책이 정의되어 있는 큐에 대해 작업할 때 해당 애플리케이션에는 Advanced Message Security가 메시지를 보호할 수 있도록 추가 권한이 필요합니다.

애플리케이션에는 다음이 필요합니다.

- SYSTEM.PROTECTION.POLICY.QUEUE에 대한 읽기 액세스. 다음을 실행하여 이를 수행하십시오.

```
RDEFINE MQQUEUE QMgrName.SYSTEM.PROTECTION.POLICY.QUEUE UACC(NONE)
PERMIT QMgrName.SYSTEM.PROTECTION.POLICY.QUEUE CLASS(MQQUEUE)
ID(username) ACCESS(READ)
```

- SYSTEM.PROTECTION.ERROR.QUEUE에 대한 쓰기 액세스. 다음을 실행하여 이를 수행하십시오.

```
RDEFINE MQQUEUE QMgrName.SYSTEM.PROTECTION.ERROR.QUEUE UACC(NONE)
PERMIT QMgrName.SYSTEM.PROTECTION.ERROR.QUEUE CLASS(MQQUEUE)
ID(username) ACCESS(READ)
```

IBM i IBM i에서 인증서 및 키 저장소 구성 파일 설정

Advanced Message Security 보호를 설정할 때 첫 번째 태스크는 인증서를 작성하고, 이를 사용자의 환경과 연관시키는 것입니다. 이 연관은 통합 파일 시스템(IFS)에 보관된 파일을 통해 구성됩니다.

프로시저

1. IBM i와 함께 제공된 OpenSSL 도구를 사용하여 자체 서명 인증서를 작성하려면 QShell에서 다음 명령을 실행하십시오.

```
/QOpenSys/usr/bin/openssl req -x509 -newkey rsa:2048 -keyout
$HOME/private.pem -out $HOME/mycert.pem -nodes -days 365
```

명령은 다음을 포함하여 새 자체 서명 인증서의 다양한 식별 이름 속성에 프롬프트를 표시합니다.

- 공용 이름(CN=)
- 조직(O=)
- 국가(C=)

이는 암호화되지 않은 개인 키 및 일치하는 인증서를 둘 모두 PEM(Privacy Enhanced Mail) 형식으로 작성합니다.

단순성을 위해 공용 이름, 조직 및 국가에 값을 입력하십시오. 이러한 속성 및 값은 정책을 작성할 때 중요합니다.

명령행에서 **-config** 매개변수를 사용해 사용자 정의 openssl 구성을 지정하여 추가 프롬프트 및 속성을 사용자 정의할 수 있습니다. 구성 파일 구문에 대한 자세한 정보는 OpenSSL 문서를 참조하십시오.

예를 들면, 다음 명령은 추가 X.509 v3 인증서 확장을 추가합니다.

```
/QOpenSys/usr/bin/openssl req -x509 -newkey rsa:2048
-keyout $HOME/private.pem -out $HOME/mycert.pem -nodes -days 365 -config myconfig.cnf
```

여기서 myconfig.cnf는 다음 항목을 포함하는 ASCII 스트림 파일입니다.

```
[req]
distinguished_name = req_distinguished_name
x509_extensions = myextensions

[req_distinguished_name]
countryName = Country Name (2 letter code)
countryName_default = GB
stateOrProvinceName = State or Province Name (full name)
stateOrProvinceName_default = Hants
localityName = Locality Name (eg, city)
localityName_default = Hursley
```

```

organizationName = Organization Name (eg, company)
organizationName_default = IBM United Kingdom
organizationalUnitName = Organizational Unit Name (eg, department)
organizationalUnitName_default = IBM MQ Development
commonName = Common Name (eg, Your Name)

[myextensions]
keyUsage = digitalSignature,nonRepudiation,dataEncipherment,keyEncipherment
extendedKeyUsage = emailProtection

```

2. AMS에는 인증서 및 개인 키 둘 모두가 동일 파일에 보관되어야 합니다. 이를 달성하려면 다음 명령을 실행하십시오.

```
cat $HOME/mycert.pem >> $HOME/private.pem
```

\$HOME의 `private.pem` 파일에는 이제 일치하는 개인 키와 인증서가 포함되는 반면, `mycert.pem` 파일에는 메시지를 암호화하고 서명을 유효성 검증할 수 있는 공개 인증서가 모두 포함됩니다.

기본 위치에 키 저장소 구성 파일(`keystore.conf`)을 작성하여 두 파일을 사용자 환경과 연관시켜야 합니다.

기본적으로 AMS는 홈 디렉토리의 `.mqsc` 서브디렉토리에서 키 저장소 구성을 찾습니다.

3. QShell에서 `keystore.conf` 파일을 작성하십시오.

```

mkdir -p $HOME/.mqsc
echo "pem.private = $HOME/private.pem" > $HOME/.mqsc/keystore.conf
echo "pem.public = $HOME/mycert.pem" >> $HOME/.mqsc/keystore.conf
echo "pem.password = unused" >> $HOME/.mqsc/keystore.conf

```

IBM i IBM i에서 정책 작성

정책을 작성하기 전에 보호된 메시지를 보관하기 위해 큐를 작성해야 합니다.

프로시저

1. 명령행 프롬프트에 다음을 입력하십시오.

```
CRTMQMQ QNAME(PROTECTED) QTYPE(*LCL) MQMNAME (mqmname)
```

여기서 `mqmname`은 큐 관리자의 이름입니다.

DSPMQM 명령을 사용하여 큐 관리자가 보안 정책 사용이 가능한지를 확인하십시오. **Security Policy Capability** 가 *YES를 표시하는지 확인하십시오.

정의할 수 있는 가장 단순한 정책은 무결성 정책이고 이는 암호화 알고리즘이 아니라 디지털 서명 알고리즘을 사용하여 정책을 작성하여 달성됩니다.

메시지는 서명되지만 암호화되지 않습니다. 메시지가 암호화될 예정이면 암호화 알고리즘과 하나 이상의 의도된 메시지 수신인을 지정해야 합니다.

의도된 메시지 수신인의 공개 키 저장소의 인증서는 식별 이름을 통해 식별됩니다.

2. QShell에서 다음 명령을 사용하여 \$HOME에서 인증서의 식별 이름을 공개 키 저장소 `mycert.pem`을 표시하십시오.

```
/QOpenSys/usr/bin/openssl x509 -in $HOME/mycert.pem -noout -subject -nameopt RFC2253
```

식별 이름을 의도된 수신인으로 입력해야 하고, 정책 이름은 보호될 큐 이름과 일치해야 합니다.

3. CL 명령 프롬프트에서 예를 들어 다음을 입력하십시오.

```
SETMQMSPL POLICY(PROTECTED) MQMNAME (mqmname) SIGNALG(*SHA256) ENCALG(*AES256) RECIPI('CN=.., O=.., C=..')
```

여기서 `mqmname`은 큐 관리자의 이름입니다.

정책이 작성되면 해당 큐 이름을 통해 놓여지고, 찾거나 파괴적으로 제거된 메시지는 AMS 정책을 따릅니다.

관련 참조

[메시지 큐 관리자 표시\(DSPMQM\)](#)

[MQM 보안 정책 설정\(SETMQMSPL\)](#)

IBM i IBM i에서 정책 테스트

제품과 함께 제공된 샘플 애플리케이션을 사용하여 보안 정책을 테스트하십시오.

이 태스크 정보

IBM MQ와 함께 제공된 샘플 애플리케이션(예: `AMQSPUT4`, `AMQSGET4`, `AMQSGBR4` 및 `WRKMQMMSG` 등과 같은 도구)을 사용하여 `PROTECTED` 큐 이름을 사용하여 메시지를 넣고, 찾고, 가져올 수 있습니다.

모든 것이 올바르게 구성된 경우 애플리케이션의 작동에는 이 사용자의 보호되지 않은 큐의 애플리케이션의 작동과 차이가 있어서는 안 됩니다.

그러나 Advanced Message Security에 대해 설정되지 않은 사용자 또는 메시지를 복호화하는 데 필요한 개인 키가 없는 사용자는 메시지를 볼 수 없습니다. 사용자는 `MQCC_FAILED (2)`와 동등한 `RCFAIL` 완료 코드 및 `RC2063(MQRC_SECURITY_ERROR)` 이유 코드를 수신합니다.

AMS 보호가 유효한지 확인하려면 예를 들어, `AMQSPUT0`를 사용하여 `PROTECTED` 큐에 일부 테스트 메시지를 두십시오. 그런 다음 알리어스 큐를 작성하여 쉬는 중인 원시 보호된 데이터를 찾아볼 수 있습니다.

프로시저

사용자에게 필수 권한을 부여하려면 다음을 실행하십시오.

```
CRTMQMQ QNAME(ALIAS) QTYPE(*ALS) TGTQNAME(PROTECTED) MQMNAME(yourqm)
```

예를 들어, `AMQSBCG4` 또는 `WRKMQMMSG`를 사용하여 `ALIAS` 큐 이름 찾아보기는 `PROTECTED` 큐의 찾아보기가 일반 텍스트 메시지를 표시하는 것보다 더 큰 `scrambled` 메시지를 표시해야 합니다.

스크램블된 메시지는 표시 가능하지만 이 이름과 일치할 강제 실행하는 AMS에 대한 정책이 없으므로 원본 일반 텍스트는 `ALIAS` 큐를 사용하여 해독할 수 없습니다. 따라서 원시 보호된 데이터가 리턴됩니다.

관련 참조

[MQM 보안 정책 설정\(SETMQMSPL\)](#)

[MQ 메시지에 대한 작업\(WRKMQMMSG\)](#)

명령 및 구성 이벤트

Advanced Message Security를 사용하면 로그되고 감사를 위한 정책 변경사항의 레코드로서 사용될 수 있는 명령 및 구성 이벤트 메시지를 생성할 수 있습니다.

IBM MQ에 의해 생성된 명령 및 구성 이벤트는 이벤트가 발생하는 큐 관리자에서 전용 큐로 전송된 PCF 형식의 메시지입니다.

구성 이벤트 메시지는 `SYSTEM.ADMIN.CONFIG.EVENT` 큐에 전송됩니다.

명령 이벤트 메시지는 `SYSTEM.ADMIN.COMMAND.EVENT` 큐에 전송됩니다.

이벤트는 Advanced Message Security 보안 정책을 관리하기 위해 사용 중인 도구와 관계 없이 생성됩니다.

Advanced Message Security에는 보안 정책에서 다른 조치에 의해 생성되는 네 가지 유형의 이벤트가 있습니다.

- 575 페이지의 『[AMS에서 보안 정책 작성](#)』 - 두 개의 IBM MQ 이벤트 메시지를 생성:
 - 구성 이벤트
 - 명령 이벤트
- 576 페이지의 『[AMS에서 보안 정책 변경](#)』 - 세 개의 IBM MQ 이벤트 메시지를 생성:

- 오래된 보안 구성 값을 포함하는 구성 이벤트
- 새 보안 정책 값을 포함하는 구성 이벤트
- 명령 이벤트
- 576 페이지의 『AMS의 보안 정책 표시 및 덤프』 - 한 개의 IBM MQ 이벤트 메시지를 생성:
 - 명령 이벤트
- 578 페이지의 『AMS에서 보안 정책 제거』 - 두 개의 IBM MQ 이벤트 메시지를 생성:
 - 구성 이벤트
 - 명령 이벤트

이벤트 로깅 사용 가능 및 사용 불가능

큐 관리자 속성 **CONFIGEV** 및 **CMDEV**를 사용하여 명령 및 구성 이벤트를 제어합니다. 이들 이벤트를 사용 가능하게 설정하려면 적절한 큐 관리자 속성을 **ENABLED**로 설정하십시오. 이들 이벤트를 사용 불가능하게 설정하려면 적절한 큐 관리자 속성을 **DISABLED**로 설정하십시오.

프로시저

구성 이벤트

구성 이벤트를 사용 가능하게 설정하려면 **CONFIGEV**를 **ENABLED**로 설정하십시오. 구성 이벤트를 사용 불가능하게 설정하려면 **CONFIGEV**를 **DISABLED**로 설정하십시오. 예를 들어, 다음 MQSC 명령을 사용하여 구성 이벤트를 사용 가능으로 설정할 수 있습니다.

```
ALTER QMGR CONFIGEV (ENABLED)
```

명령 이벤트

명령 이벤트를 사용 가능하게 설정하려면 **CMDEV**를 **ENABLED**로 설정하십시오. **DISPLAY MQSC** 명령 및 조회 **PCF** 명령을 제외한 명령에 대한 명령 이벤트를 사용 가능하게 설정하려면 **CMDEV**를 **NODISPLAY**로 설정하십시오. 명령 이벤트를 사용 불가능하게 설정하려면 **CMDEV**를 **DISABLED**로 설정하십시오. 예를 들어, 다음 MQSC 명령을 사용하여 명령 이벤트를 사용 가능으로 설정할 수 있습니다.

```
ALTER QMGR CMDEV (ENABLED)
```

관련 태스크

[IBM MQ에서 구성, 명령, 로거 이벤트 제어](#)

명령 이벤트 메시지 형식

명령 이벤트 메시지는 MQCFH 구조와 이를 뒤따르는 PCF 매개변수로 구성됩니다.

다음은 선택된 MQCFH 값입니다.

```
Type = MQCFT_EVENT;
Command = MQCMD_COMMAND_EVENT;
MsgSeqNumber = 1;
Control = MQCFC_LAST;
ParameterCount = 2;
CompCode = MQCC_WARNING;
Reason = MQRC_COMMAND_PCF;
```

참고: ParameterCount 값은 2입니다. 항상 MQCFGR 유형(그룹)의 두 개의 매개변수가 있기 때문입니다. 각 그룹은 적합한 매개변수로 구성됩니다. 이벤트 데이터는 두 개의 그룹, CommandContext 및 CommandData로 구성됩니다.

CommandContext에는 다음이 포함됩니다.

EventUserID

설명:	이벤트를 생성한 명령 또는 호출을 실행한 사용자 ID입니다. (이는 명령 또는 호출을 실행하기 위한 권한을 검사하는 데 사용된 것과 같은 사용자 ID입니다. 큐로부터 수신한 명령의 경우 이는 또한 명령 메시지의 MD로부터의 사용자 ID(UserIdentifier)입니다).
Identifier:	MQCACF_EVENT_USER_ID.
데이터 유형:	MQCFST.
최대 길이:	MQ_USER_ID_LENGTH.
리턴됨:	항상.

EventOrigin

설명:	이벤트를 초래한 조치의 원본.
Identifier:	MQIACF_EVENT_ORIGIN.
데이터 유형:	MQCFIN.
값:	MQEVO_CONSOLE 콘솔 명령 - 명령행. MQEVO_MSG IBM MQ Explorer 플러그인으로부터의 명령 메시지.
리턴됨:	항상.

EventQMgr

설명:	명령 또는 호출이 입력된 큐 관리자. (명령이 실행되고 이벤트를 생성한 큐 관리자는 이벤트 메시지의 MD에 있습니다.)
Identifier:	MQCACF_EVENT_Q_MGR.
데이터 유형:	MQCFST.
최대 길이:	MQ_Q_MGR_NAME_LENGTH.
리턴됨:	항상.

EventAccountingToken

설명:	메시지(MQEVO_MSG)로서 수신된 명령의 경우 명령 메시지의 MD로부터의 회계 토큰(AccountingToken).
Identifier:	MQBACF_EVENT_ACCOUNTING_TOKEN.
데이터 유형:	MQCFBS.
최대 길이:	MQ_ACCOUNTING_TOKEN_LENGTH.
리턴됨:	EventOrigin이 MQEVO_MSG인 경우에만.

EventIdentityData

설명:	메시지(MQEVO_MSG)로서 수신된 명령의 경우 명령 메시지의 MD로부터의 애플리케이션 ID 데이터(ApplIdentityData).
Identifier:	MQCACF_EVENT_APPL_IDENTITY.
데이터 유형:	MQCFST.
최대 길이:	MQ_APPL_IDENTITY_DATA_LENGTH.
리턴됨:	EventOrigin이 MQEVO_MSG인 경우에만.

EventApplType

설명:	메시지(MQEVO_MSG)로서 수신된 명령의 경우 명령 메시지의 MD로부터의 애플리케이션 유형(PutApplType).
Identifier:	MQIACF_EVENT_APPL_TYPE.
데이터 유형:	MQCFIN.
리턴됨:	EventOrigin이 MQEVO_MSG인 경우에만.

EventApplName

설명:	메시지(MQEVO_MSG)로서 수신된 명령의 경우 명령 메시지의 MD로부터의 애플리케이션 이름(PutApplName).
Identifier:	MQCACF_EVENT_APPL_NAME.
데이터 유형:	MQCFST.
최대 길이:	MQ_APPL_NAME_LENGTH.
리턴됨:	EventOrigin이 MQEVO_MSG인 경우에만.

EventApplOrigin

설명:	메시지(MQEVO_MSG)로서 수신된 명령의 경우 명령 메시지의 MD로부터의 애플리케이션 원본 데이터(ApplOriginData).
Identifier:	MQCACF_EVENT_APPL_ORIGIN.
데이터 유형:	MQCFST.
최대 길이:	MQ_APPL_ORIGIN_DATA_LENGTH.
리턴됨:	EventOrigin이 MQEVO_MSG인 경우에만.

명령

설명:	명령 코드.
Identifier:	MQIACF_COMMAND.
데이터 유형:	MQCFIN.
값:	MQCMD_INQUIRE_PROT_POLICY 숫자 값 205 MQCMD_CREATE_PROT_POLICY 숫자 값 206 MQCMD_DELETE_PROT_POLICY 숫자 값 207 MQCMD_CHANGE_PROT_POLICY 숫자 값 208 이는 IBM MQ 8.0 cmqcfc.h에 정의되어 있습니다.
리턴됨:	항상.

CommandData에는 PCF 명령을 구성하는 PCF 요소가 포함됩니다.

구성 이벤트 메시지 형식

구성 이벤트는 표준 Advanced Message Security 형식의 PCF 메시지입니다.

MQCMD 메시지 디스크립터의 가능한 값은 [이벤트 메시지 MQCMD\(메시지 디스크립터\)](#)에서 볼 수 있습니다.

다음은 선택된 MQCMD 값입니다.

```
Format = MQFMT_EVENT
Persistence = MQPER_PERSISTENCE_AS_Q_DEF
PutApplType = MQAT_QMGR //for both CLI and command server
```

메시지 버퍼는 MQCFH 구조 및 이를 뒤따르는 매개변수 구조로 구성됩니다. 가능한 MQCFH 값은 [이벤트 메시지 MQCFH\(PCF 헤더\)](#)에서 볼 수 있습니다.

다음은 선택된 MQCFH 값입니다.

```
Type = MQCFT_EVENT
Command = MQCMD_CONFIG_EVENT
MsgSeqNumber = 1 or 2 // 2 will be in case of Change Object event
Control = MQCFC_LAST or MQCFC_NOT_LAST //MQCFC_NOT_LAST will be in case of 1 Change Object event
ParameterCount = reflects number of PCF parameters following MQCFH
CompCode = MQCC_WARNING
Reason = one of {MQRC_CONFIG_CREATE_OBJECT, MQRC_CONFIG_CHANGE_OBJECT,
MQRC_CONFIG_DELETE_OBJECT}
```

MQCFH를 뒤따르는 매개변수는 다음과 같습니다.

EventUserID

설명: 이벤트를 생성한 명령 또는 호출을 실행한 사용자 ID입니다. (이는 명령 또는 호출을 실행하기 위한 권한을 검사하는 데 사용된 것과 같은 사용자 ID입니다. 큐로부터 수신한 명령의 경우 이는 또한 명령 메시지의 MD로부터의 사용자 ID(UserIdentifier)입니다).

Identifier: **MQCACF_EVENT_USER_ID**

데이터 유형: MQCFST.

최대 길이: MQ_USER_ID_LENGTH.

리턴됨: 항상.

SecurityId

설명: 명령 서버 메시지 또는 로컬 명령의 Windows SID의 경우에 MQMD.AccountingToken의 값.

Identifier: **MQBACF_EVENT_SECURITY_ID**

데이터 유형: MQCBS.

최대 길이: MQ_SECURITY_ID_LENGTH.

리턴됨: 항상.

EventOrigin

설명: 이벤트를 초래한 조치의 원본.

Identifier: **MQIACF_EVENT_ORIGIN**

데이터 유형: MQCFIN.

값: **MQEVO_CONSOLE**
콘솔 명령 - 명령행.

MQEVO_MSG
IBM MQ 탐색기 플러그인으로부터의 명령 메시지.

리턴됨: 항상.

EventQMgr

설명: 명령 또는 호출이 입력된 큐 관리자. (명령이 실행되고 이벤트를 생성한 큐 관리자는 이벤트 메시지의 MD에 있습니다.)

Identifier: **MQCACF_EVENT_Q_MGR**

데이터 유형: MQCFST

최대 길이: MQ_Q_MGR_NAME_LENGTH
리턴됨: 항상.

ObjectType

설명: 오브젝트 유형.
Identifier: **MQIACF_OBJECT_TYPE**
데이터 유형: MQCFIN
가치: **MQOT_PROT_POLICY**
Advanced Message Security 보호 정책. **1019** - IBM MQ 8.0 또는 cmqc.h 파일에 정의된 숫자 값.
리턴됨: 항상.

PolicyName

설명: Advanced Message Security 정책 이름.
Identifier: **MQCA_POLICY_NAME.**
데이터 유형: MQCFST.
가치: **2112** - IBM MQ 8.0 또는 cmqc.h 파일에 정의된 숫자 값.
최대 길이: MQ_OBJECT_NAME_LENGTH.
리턴됨: 항상.

PolicyVersion

설명: Advanced Message Security 정책 버전.
Identifier: **MQIA_POLICY_VERSION**
데이터 유형: MQCFIN
가치: **238** - IBM MQ 8.0 또는 cmqc.h 파일에 정의된 숫자 값.
리턴됨: Always

TolerateFlag

설명: Advanced Message Security 정책 관용 플래그.
Identifier: **MQIA_TOLERATE_UNPROTECTED**
데이터 유형: MQCFIN
가치: **235** - IBM MQ 8.0 또는 cmqc.h 파일에 정의된 숫자 값.
리턴됨: 항상.

SignatureAlgorithm

설명: Advanced Message Security 정책 서명 알고리즘.
Identifier: **MQIA_SIGNATURE_ALGORITHM**
데이터 유형: MQCFIN
가치: **236** - IBM MQ 8.0 또는 cmqc.h 파일에 정의된 숫자 값.
리턴됨: Advanced Message Security 정책에 정의된 서명 알고리즘이 있을 때마다

EncryptionAlgorithm

설명: Advanced Message Security 정책 암호화 알고리즘.
Identifier: **MQIA_ENCRYPTION_ALGORITHM**
데이터 유형: MQCFIN
가치: **237** - IBM MQ 8.0 또는 cmqc.h 파일에 정의된 숫자 값.
리턴됨: IBM MQ 정책에 정의된 암호화 알고리즘이 있을 때마다

SignerDNs

설명: 허용된 서명자의 제목 식별 이름.
Identifier: **MQCA_SIGNER_DN**
데이터 유형: MQCFSL
가치: **2113** - IBM MQ 8.0 또는 cmqc.h 파일에 정의된 숫자 값.
최대 길이: 정책에서 가장 긴 서명자 DN이지만 MQ_DISTINGUISHED_NAME_LENGTH보다 길지는 않음
리턴됨: IBM MQ 정책에 정의될 때마다.

RecipientDNs

설명: 허용된 서명자의 제목 식별 이름.
Identifier: **MQCA_RECIPIENT_DN**
데이터 유형: MQCFSL
가치: **2114** - IBM MQ 8.0 또는 cmqc.h 파일에 정의된 숫자 값.
최대 길이: 정책에서 가장 긴 수신인 DN이지만 MQ_DISTINGUISHED_NAME_LENGTH보다 길지는 않음
리턴됨: IBM MQ 정책에 정의될 때마다.

주의사항

이 정보는 미국에서 제공되는 제품 및 서비스용으로 작성된 것입니다.

IBM은 다른 국가에서 이 책에 기술된 제품, 서비스 또는 기능을 제공하지 않을 수도 있습니다. 현재 사용할 수 있는 제품 및 서비스에 대한 정보는 한국 IBM 담당자에게 문의하십시오. 이 책에서 IBM 제품, 프로그램 또는 서비스를 언급했다고 해서 해당 IBM 제품, 프로그램 또는 서비스만을 사용할 수 있다는 것을 의미하지는 않습니다. IBM의 지적 재산을 침해하지 않는 한, 기능상으로 동등한 제품, 프로그램 또는 서비스를 대신 사용할 수도 있습니다. 그러나 비IBM 제품, 프로그램 또는 서비스의 운영에 대한 평가 및 검증은 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 라이선스까지 부여하는 것은 아닙니다. 라이선스에 대한 의문사항은 다음으로 문의하십시오.

150-945

서울특별시 영등포구
국제금융로 10, 3IFC
한국 아이.비.엠 주식회사
U.S.A.

2바이트(DBCS) 정보에 관한 라이선스 문의는 한국 IBM에 문의하거나 다음 주소로 서면 문의하시기 바랍니다.

지적 재산권 라이선스 부여
2-31 Roppongi 3-chome, Minato-Ku
IBM Japan, Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

다음 단락은 현지법과 상충하는 영국이나 기타 국가에서는 적용되지 않습니다. IBM은 타인의 권리 비침해, 상품성 및 특정 목적에의 적합성에 대한 묵시적 보증을 포함하여(단, 이에 한하지 않음) 명시적 또는 묵시적인 일체의 보증 없이 이 책을 "현상태대로" 제공합니다. 일부 국가에서는 특정 거래에서 명시적 또는 묵시적 보증의 면책사항을 허용하지 않으므로, 이 사항이 적용되지 않을 수도 있습니다.

이 정보에는 기술적으로 부정확한 내용이나 인쇄상의 오류가 있을 수 있습니다. 이 정보는 주기적으로 변경되며, 변경된 사항은 최신판에 통합됩니다. IBM은 이 책에서 설명한 제품 및/또는 프로그램을 사전 통지 없이 언제든지 개선 및/또는 변경할 수 있습니다.

이 정보에서 언급되는 비IBM의 웹 사이트는 단지 편의상 제공된 것으로, 어떤 방식으로든 이들 웹 사이트를 옹호하고자 하는 것은 아닙니다. 해당 웹 사이트의 자료는 본 IBM 제품 자료의 일부가 아니므로 해당 웹 사이트 사용으로 인한 위험은 사용자 본인이 감수해야 합니다.

IBM은 귀하의 권리를 침해하지 않는 범위 내에서 적절하다고 생각하는 방식으로 귀하가 제공한 정보를 사용하거나 배포할 수 있습니다.

(i) 독립적으로 작성된 프로그램과 기타 프로그램(본 프로그램 포함) 간의 정보 교환 및 (ii) 교환된 정보의 상호 이용을 목적으로 본 프로그램에 관한 정보를 얻고자 하는 라이선스 사용자는 다음 주소로 문의하십시오.

서울특별시 영등포구
서울특별시 강남구 도곡동 467-12,
군인공제회관빌딩
한국 아이.비.엠 주식회사
U.S.A.

이러한 정보는 해당 조건(예를 들면, 사용료 지불 등)하에서 사용될 수 있습니다.

이 정보에 기술된 라이선스가 부여된 프로그램 및 프로그램에 대해 사용 가능한 모든 라이선스가 부여된 자료는 IBM이 IBM 기본 계약, IBM 프로그램 라이선스 계약(IPLA) 또는 이와 동등한 계약에 따라 제공한 것입니다.

본 문서에 포함된 모든 성능 데이터는 제한된 환경에서 산출된 것입니다. 따라서 다른 운영 환경에서 얻어진 결과는 상당히 다를 수 있습니다. 일부 성능은 개발 단계의 시스템에서 측정되었을 수 있으므로 이러한 측정치가 일반적으로 사용되고 있는 시스템에서도 동일하게 나타날 것이라고는 보증할 수 없습니다. 또한 일부 성능은 추정

통해 추측되었을 수도 있으므로 실제 결과는 다를 수 있습니다. 이 책의 사용자는 해당 데이터를 본인의 특정 환경에서 검증해야 합니다.

비IBM 제품에 관한 정보는 해당 제품의 공급업체, 공개 자료 또는 기타 범용 소스로부터 얻은 것입니다. IBM에서는 이러한 제품들을 테스트하지 않았으므로, 비IBM 제품과 관련된 성능의 정확성, 호환성 또는 기타 청구에 대해서는 확신할 수 없습니다. 비IBM 제품의 성능에 대한 의문사항은 해당 제품의 공급업체에 문의하십시오.

IBM이 제시하는 방향 또는 의도에 관한 모든 언급은 특별한 통지 없이 변경될 수 있습니다.

이 정보에는 일상의 비즈니스 운영에서 사용되는 자료 및 보고서에 대한 예제가 들어 있습니다. 이들 예제에는 개념을 가능한 완벽하게 설명하기 위하여 개인, 회사, 상표 및 제품의 이름이 사용될 수 있습니다. 이들 이름은 모두 가공의 것이며 실제 기업의 이름 및 주소와 유사하더라도 이는 전적으로 우연입니다.

저작권 라이선스:

이 정보에는 여러 운영 플랫폼에서의 프로그래밍 기법을 보여주는 원어로 된 샘플 응용프로그램이 들어 있습니다. 귀하는 이러한 샘플 프로그램의 작성 기준이 된 운영 플랫폼의 응용프로그램 프로그래밍 인터페이스(API)에 부합하는 응용프로그램을 개발, 사용, 판매 또는 배포할 목적으로 IBM에 추가 비용을 지불하지 않고 이들 샘플 프로그램을 어떠한 형태로든 복사, 수정 및 배포할 수 있습니다. 이러한 샘플 프로그램은 모든 조건하에서 완전히 테스트된 것은 아닙니다. 따라서 IBM은 이들 샘플 프로그램의 신뢰성, 서비스 가능성 또는 기능을 보증하거나 진술하지 않습니다.

이 정보를 소프트웨어로 확인하는 경우에는 사진과 컬러 삽화가 제대로 나타나지 않을 수도 있습니다.

프로그래밍 인터페이스 정보

프로그래밍 인터페이스 정보는 본 프로그램과 함께 사용하기 위한 응용프로그램 소프트웨어 작성을 돕기 위해 제공됩니다.

이 책에는 고객이 프로그램을 작성하여 WebSphere MQ서비스를 얻을 수 있도록 하는 계획된 프로그래밍 인터페이스에 대한 정보가 포함되어 있습니다.

그러나 본 정보에는 진단, 수정 및 성능 조정 정보도 포함되어 있습니다. 진단, 수정 및 성능 조정 정보는 응용프로그램 소프트웨어의 디버거를 돕기 위해 제공된 것입니다.

중요사항: 이 진단, 수정 및 튜닝 정보는 변경될 수 있으므로 프로그래밍 인터페이스로 사용하지 마십시오.

상표

IBM, IBM 로고, [ibm.com](http://www.ibm.com)®는 전세계 여러 국가에 등록된 IBM Corporation의 상표입니다. 현재 IBM 상표 목록은 웹 "저작권 및 상표 정보"(www.ibm.com/legal/copytrade.shtml)에 있습니다. 기타 제품 및 서비스 이름은 IBM 또는 타사의 상표입니다.

Microsoft 및 Windows는 미국 또는 기타 국가에서 사용되는 Microsoft Corporation의 상표입니다.

UNIX는 미국 또는 기타 국가에서 사용되는 The Open Group의 등록상표입니다.

Linux는 미국 또는 기타 국가에서 사용되는 Linus Torvalds의 등록상표입니다.

이 제품에는 Eclipse 프로젝트 (<http://www.eclipse.org/>)에서 개발한 소프트웨어가 포함되어 있습니다.

Java 및 모든 Java 기반 상표와 로고는 Oracle 및/또는 그 계열사의 상표 또는 등록상표입니다.



부품 번호:

(1P) P/N: