



Sun Java™ System  
Messaging Server 6  
관리 설명서

---

2005Q1

Sun Microsystems, Inc.  
4150 Network Circle  
Santa Clara, CA 95054  
U.S.A.

부품 번호: 819-1055

Copyright © 2005 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, U.S.A. 모든 권리는 저작권자의 소유입니다.

Sun Microsystems, Inc.는 본 설명서에 설명된 제품에 포함된 기술 관련 지적 재산권을 소유합니다. 특히, 이 지적 재산권에는 <http://www.sun.com/patents>에 나열된 하나 이상의 미국 특허권이 포함될 수 있으며 미국 및 다른 국가에서 하나 이상의 추가 특허권 또는 출원 중인 특허권이 제한 없이 포함될 수 있습니다.

이 제품에는 Sun Microsystems, Inc.의 기업 기밀 정보가 포함되어 있습니다. Sun Microsystems, Inc.의 명시적인 사전 서면 승인 없이 사용, 공개 또는 복제하는 것을 금합니다.

미국 정부의 권리 상용 소프트웨어. 정부 사용자는 Sun Microsystems, Inc. 표준 사용권 계약과 해당 FAR 규정과 보충 규정을 준수해야 합니다.

이 배포에는 타사에서 개발한 자료가 포함되어 있을 수 있습니다.

제품 중에는 캘리포니아 대학에서 허가한 Berkeley BSD 시스템에서 파생된 부분이 포함되어 있을 수 있습니다. UNIX는 미국 및 다른 국가에서 X/Open Company, Ltd를 통해 독점적으로 사용권이 부여되는 등록 상표입니다.

Sun, Sun Microsystems, Sun 로고, Java, Solaris, JDK, Java Naming 및 Directory Interface, JavaMail, JavaHelp, J2SE, iPlanet, Duke 로고, Java Coffee Cup logo, Solaris 로고, SunTone Certified 로고 및 Sun ONE 로고는 미국 및 다른 국가에서 Sun Microsystems, Inc.의 상표 또는 등록 상표입니다.

모든 SPARC 상표는 사용 허가를 받았으며 미국 및 다른 국가에서 SPARC International, Inc.의 상표 또는 등록 상표입니다. SPARC 상표를 사용하는 제품은 Sun Microsystems, Inc.에서 개발한 구조에 기반을 두고 있습니다.

Legato 및 Legato 로고는 등록 상표이며 Legato NetWorker는 Legato Systems, Inc의 상표 또는 등록 상표입니다. Netscape Communications Corp 로고는 Netscape Communications Corporation의 상표 또는 등록 상표입니다.

OPEN LOOK 및 Sun(TM) GUI(그래픽 사용자 인터페이스)는 Sun Microsystems, Inc.가 자사의 사용자 및 정식 사용자용으로 개발했습니다. Sun은 컴퓨터 업계를 위한 시각적 또는 그래픽 사용자 인터페이스의 개념을 연구 개발한 Xerox사의 선구적인 노력을 높이 평가하고 있습니다. Sun은 Xerox와 Xerox Graphical User Interface에 대한 비독점적 사용권을 보유하고 있습니다. 이 사용권은 OPEN LOOK GUI를 구현하는 Sun의 정식 사용자에게도 적용되며 그렇지 않은 경우에는 Sun의 서면 사용권 계약을 준수해야 합니다.

이 서비스 설명서에서 다루는 제품과 수록된 정보는 미국 수출 관리법에 의해 규제되며 다른 국가의 수출 또는 수입 관리법의 적용을 받을 수도 있습니다. 이 제품과 정보를 직간접적으로 핵무기, 미사일 또는 생화학 무기에 사용하거나 핵과 관련하여 해상에서 사용하는 것은 엄격하게 금지합니다. 미국 수출 금지 국가 또는 금지된 개인과 특별히 지정된 국민 목록을 포함하여 미국 수출 금지 목록에 지정된 대상으로의 수출이나 재수출은 엄격하게 금지됩니다.

이 제품에는 Carnegie Mellon University의 Computing Services(<http://www.cmu.edu/computing/>)에서 개발한 소프트웨어가 포함되어 있습니다.

설명서는 "있는 그대로" 제공되며 법률을 위반하지 않는 범위 내에서 상품성, 특정 목적에 대한 적합성 또는 비침해에 대한 묵시적인 보증을 포함하여 모든 명시적 또는 묵시적 조건, 표현 및 보증을 배제합니다.

# 목차

<b>표 목차</b> .....	<b>21</b>
<b>그림 목차</b> .....	<b>27</b>
<b>머리말</b> .....	<b>29</b>
대상 .....	29
이 설명서를 읽기 전에 .....	30
설명서 구성 .....	30
이 설명서에 사용된 규칙 .....	32
활자체 규약 .....	32
기호 .....	33
기본 경로 및 파일 이름 .....	33
명령줄 프롬프트 .....	34
관련 설명서 .....	34
Messaging Server 설명서 .....	34
Communications Services 설명서 .....	35
본 설명서의 온라인 버전 .....	36
Sun 자원 온라인 액세스 .....	36
Sun 기술 지원에 문의 .....	36
타사 웹 사이트 관련 참조 사항 .....	37
사용자 의견 환영 .....	37
<b>1장 사후 설치 작업 및 레이아웃</b> .....	<b>39</b>
UNIX 시스템 사용자와 그룹 만들기 .....	40
Messaging Server 구성을 위해 Directory Server 준비 .....	41
comm_dssetup.pl의 위치 .....	41
comm_dssetup.pl 요구 사항 .....	42
comm_dssetup.pl 스크립트 실행 .....	43
Messaging Server 초기 런타임 구성 만들기 .....	51
Messaging Server 전제 조건 .....	51

Messaging Server 구성 확인 목록 .....	52
구성 프로그램 실행 .....	52
자동 설치 수행 .....	57
Directory Server 복제본에 대해 Messaging Server 설치 .....	58
Messaging Server 준비 도구 설치 .....	59
메시징용 Delegated Administrator .....	59
LDAP 준비 도구 .....	61
SMTP 릴레이 차단 .....	62
재부트 후 시작 활성화 .....	64
sendmail 클라이언트 처리 .....	65
Solaris 8 .....	65
Solaris 9 이상 .....	66
Messenger Express 및 Communications Express 메일 필터 구성 .....	67
성능 및 조정 .....	68
사후 설치 디렉토리 레이아웃 .....	68
사후 설치 포트 번호 .....	70
<b>2장 Sun Java Systems Messaging Server로 업그레이드 .....</b>	<b>73</b>
시작하기 전에 .....	73
업그레이드 프로세스 개요 .....	74
구성을 업데이트하도록 업그레이드 파일 만들기 .....	74
업그레이드 파일 정보 .....	74
UpgradeMsg5toMsg6.pl Perl 스크립트 실행 .....	76
업그레이드 유틸리티 실행 .....	78
업그레이드 유틸리티 개요 .....	78
do_the_upgrade.sh 유틸리티 실행 .....	78
MTA 구성 .....	79
configutil 매개 변수 .....	79
백업 구성 .....	80
mboxlist 데이터베이스 .....	80
사용자 메일함 마이그레이션 .....	80
요구 사항 .....	81
마이그레이션 지침 .....	81
<b>3장 고가용성 구성 .....</b>	<b>85</b>
클러스터 에이전트 설치 .....	86
Messaging Server 및 고가용성 지침 .....	86
useconfig 유틸리티 사용 .....	86
Veritas Cluster Server 에이전트 설치 .....	87
Veritas Cluster Server 요구 사항 .....	88
VCS 3.5 설치 및 구성 지침 .....	88
MsgSrv 속성 .....	91

Sun Cluster 에이전트 설치 .....	92
Sun Cluster 요구 사항 .....	92
HASStoragePlus 정보 .....	92
Sun Cluster 및 HA StoragePlus를 사용하여 Messaging Server 구성 .....	93
서버에서 IP 주소 바인딩 .....	97
고가용성 구성 해제 .....	99
Veritas Cluster Server 구성 해제 .....	99
Sun Cluster 3.x에 대한 Messaging Server HA 지원 구성 해제 .....	100

#### **4장 일반 메시징 기능 구성 .....** **103**

비밀번호 수정 .....	104
메일 사용자, 메일 목록 및 도메인 관리 .....	105
Messaging Server에서 사용자 제거 .....	105
Messaging Server에서 도메인 제거 .....	106
Sun ONE 콘솔로 Messaging Server 관리 .....	106
서비스 시작 및 중지 .....	107
HA 환경에서 서비스 시작 및 중지 .....	107
HA가 아닌 환경에서 서비스 시작 및 중지 .....	108
실패했거나 응답이 없는 서비스의 자동 재시작 .....	110
고가용성 배포 시 자동 재시작 .....	112
자동 작업 예약 .....	113
인사 메일 구성 .....	114
도메인별 인사 메일 설정 .....	115
사용자 기본 언어 설정 .....	117
도메인 기본 언어 설정 .....	117
서버 사이트 언어 구성 .....	118
디렉토리 조회 사용자 정의 .....	118
암호화 설정 .....	122
페일오버 LDAP 서버 설정 .....	122

#### **5장 POP, IMAP 및 HTTP 서비스 구성 .....** **123**

일반 구성 .....	124
서비스 사용 가능/불가능하게 하기 .....	124
포트 번호 지정 .....	124
암호화된 통신을 위한 포트 .....	125
서비스 배너 .....	126
로그인 요구 사항 .....	126
POP 클라이언트에 대한 로그인 구분자 설정 .....	126
도메인 이름을 사용하지 않고 로그인 허용 .....	127
비밀번호 기반 로그인 .....	127
인증서 기반 로그인 .....	128
성능 매개 변수 .....	128

프로세스 수	129
프로세스당 연결 수	129
프로세스당 스레드 수	130
유휴 연결 해제	131
HTTP 클라이언트 로그아웃	131
클라이언트 액세스 제어	132
POP 서비스 구성	132
IMAP 서비스 구성	134
HTTP 서비스 구성	136

## **6장 단일 사인 온(SSO) 사용** ..... 141

Sun Java System 서버에 대한 Access Manager SSO	141
SSO 제한 및 알림	142
SSO를 지원하도록 Messaging Server 구성	142
SSO 문제 해결	144
신뢰할 수 있는 원 SSO(레거시)	144
신뢰할 수 있는 원 SSO 개요 및 정의	144
신뢰할 수 있는 원 SSO 응용 프로그램	145
신뢰할 수 있는 원 SSO 제한	146
신뢰할 수 있는 원 SSO 배포 시나리오 예	146
신뢰할 수 있는 원 SSO 설정	148
Messenger Express의 신뢰할 수 있는 SSO 구성 매개 변수	152

## **7장 멀티플렉서 서비스 구성 및 관리** ..... 155

멀티플렉서 서비스	155
멀티플렉서의 장점	156
Messaging Multiplexor 정보	157
Messaging Multiplexor의 작동 방식	158
암호화(SSL) 옵션	159
인증서 기반 클라이언트 인증	159
사용자 사전 인증	160
MMP 가상 도메인	161
SMTP 프록시 정보	162
Messaging Multiplexor 설정	163
MMP를 구성하기 전에	163
Multiplexor 구성	164
Multiplexor 파일	164
Multiplexor 시작	166
기존 MMP 수정	166
SSL로 MMP 구성	166
샘플 토폴로지	168
MMP 작업	171

MMP를 사용하여 메일 액세스 구성 .....	172
페일오버 MMP LDAP 서버 설정 .....	172
Messenger Express Multiplexor 정보 .....	172
Messenger Express Multiplexor의 작동 방식 .....	173
Messenger Express Multiplexor 설정 .....	174
설정 테스트 .....	177
Messenger Express Multiplexor 관리 .....	178
<b>8장 MTA 개념 .....</b>	<b>181</b>
MTA 기능 .....	181
MTA 구조 및 메일 흐름 개요 .....	185
디스패처 .....	187
서버 프로세스 작성 및 만료 .....	187
디스패처 시작 및 중지 .....	188
다시 쓰기 규칙 .....	189
채널 .....	189
마스터 및 슬레이브 프로그램 .....	190
채널 메일 대기열 .....	192
채널 정의 .....	192
MTA 디렉토리 정보 .....	194
Job Controller .....	194
Job Controller 시작 및 중지 .....	195
<b>9장 MTA 주소 변환 및 라우팅 .....</b>	<b>197</b>
Direct LDAP 알고리즘 및 구현 .....	197
도메인의 로컬 여부 확인 .....	197
로컬 주소의 별칭 확장 .....	202
LDAP 결과 처리 .....	207
주소 역방향 .....	221
비동기 LDAP 작업 .....	223
설정 요약 .....	224
<b>10장 MTA 서비스 및 구성 정보 .....</b>	<b>225</b>
MTA 구성 컴파일 .....	226
MTA 구성 파일 .....	226
매핑 파일 .....	229
매핑 파일의 파일 형식 .....	230
매핑 작업 .....	232
기타 MTA 구성 파일 .....	243
별칭 파일 .....	244
TCP/IP(SMTP) 채널 옵션 파일 .....	244
변환 파일 .....	244

디스패처 구성 파일 .....	245
매핑 파일 .....	246
옵션 파일 .....	246
조정 파일 .....	247
Job Controller 파일 .....	247
별칭 .....	254
별칭 데이터베이스 .....	255
별칭 파일 .....	255
별칭 파일에 다른 파일 포함 .....	256
명령줄 유틸리티 .....	256
SMTP 보안 및 액세스 제어 .....	256
로그 파일 .....	257
주소를 내부 형식에서 공용 형식으로 변환 .....	257
주소 역방향 제어 설정 .....	259
정방향 조회 테이블 및 FORWARD 주소 매핑 .....	261
전달 상태 알림 메일 제어 .....	264
상태 알림 생성 및 수정 .....	265
전달 상태 알림 메일 사용자 정의 및 현지화 .....	267
생성된 알림 국제화 .....	270
추가 상태 알림 메일 기능 .....	271
MDN(Message Disposition Notification) 제어 .....	277
MDN(Message Disposition Notification) 메일 사용자 정의 및 현지화 .....	278
<b>11장 다시 쓰기 규칙 구성 .....</b>	<b>281</b>
다시 쓰기 규칙 구조 .....	282
다시 쓰기 규칙 패턴 및 태그 .....	284
백분율 핵과 일치시키는 규칙 .....	286
뱅 스타일(UUCP) 주소와 일치시키는 규칙 .....	286
모든 주소와 일치시키는 규칙 .....	287
태그된 다시 쓰기 규칙 집합 .....	287
다시 쓰기 규칙 템플릿 .....	287
일반 다시 쓰기 템플릿: A%B@C 또는 A@B .....	288
반복되는 다시 쓰기 템플릿: A%B .....	288
지정된 경로 다시 쓰기 템플릿: A@B@C@D 또는 A@B@C .....	289
다시 쓰기 규칙 템플릿의 대소문자 구분 .....	289
MTA가 다시 쓰기 규칙을 주소에 적용하는 방법 .....	290
단계 1. 첫 번째 호스트 또는 도메인 지정 추출 .....	291
단계 2. 다시 쓰기 규칙 스캔 .....	293
단계 3. 템플릿에 따라 주소 다시 쓰기 .....	294
단계 4. 다시 쓰기 프로세스 완료 .....	294
다시 쓰기 규칙 실패 .....	295
다시 쓰기 후의 구문 검사 .....	295
도메인 리터럴 처리 .....	295



템플릿 대체 및 다시 쓰기 규칙 제어 시퀀스	296
아이디 및 하위 주소 대체: \$U, \$0U, \$1U	299
호스트/도메인 및 IP 리터럴 대체: \$D, \$H, \$nD, \$nH, \$L	300
리터럴 문자 대체: \$\$, \$%, \$@	300
LDAP 쿼리 URL 대체: \$]...[	300
일반 데이터베이스 대체: \$(...)	302
지정된 매핑 적용: \${...}	302
사용자 제공 루틴 대체: \$[...]	303
단일 필드 대체: \$&, \$!, \$*, \$#	304
고유 문자열 대체	304
소스 채널 특정 다시 쓰기 규칙: \$M, \$N	305
대상 채널 특정 다시 쓰기 규칙: \$C, \$Q	305
방향 및 위치 특정 다시 쓰기 규칙: \$B, \$E, \$F, \$R	306
호스트 위치별 다시 쓰기: \$A, \$P, \$S, \$X	307
현재 태그 값 변경: \$T	307
다시 쓰기와 관련된 오류 메시지 처리: \$?	308
많은 수의 다시 쓰기 규칙 처리	309
다시 쓰기 규칙 테스트	309
다시 쓰기 규칙 예	310

<b>12장 채널 정의 구성</b>	<b>313</b>
채널 키워드(알파벳순)	314
채널 키워드 범주화(기능별)	317
채널 기본값 구성	332
SMTP 채널 구성	333
SMTP 채널 옵션 구성	334
SMTP 명령 및 프로토콜 지원	335
TCP/IP 연결 및 DNS 조회 지원	343
SMTP 인증, SASL 및 TLS	351
헤더의 SMTP AUTH에서 인증된 주소 사용	352
Microsoft Exchange 게이트웨이 채널 지정	353
전송 계층 보안	354
메일 처리 및 전달 구성	355
채널 방향 설정	357
지연 전달 날짜 구현	358
전달에 실패한 메일에 대한 재시도 간격 지정	358
채널 실행 작업의 처리 풀	360
서비스 작업 제한	360
연결 트랜잭션 제한 설정	362
크기 기반 메일 우선 순위	363
SMTP 채널 스탠드	363
여러 주소 확장	364
서비스 변환 사용	365

주소 처리 구성 .....	365
주소 유형 및 규칙 .....	366
! 및 %를 사용하는 주소 해석 .....	367
주소에 라우팅 정보 추가 .....	368
명시적 라우팅 주소의 다시 쓰기 사용 안 함 .....	369
메일을 대기열에서 제거할 때 주소 다시 쓰기 .....	370
완성되지 않은 주소를 수정할 때 사용할 호스트 이름 지정 .....	370
수신자 헤더 행 없이 메일 적법화 .....	371
잘못된 빈 수신자 헤더 스트라이핑 .....	372
역방향 데이터베이스의 채널별 사용 .....	372
제한된 메일함 인코딩 사용 .....	373
Return-path: 헤더 행 생성 .....	373
봉투의 To: 및 From: 주소에서 Received: 헤더 행 구성 .....	374
주소 헤더 행의 주석 처리 .....	374
주소 헤더 행에서 개인 이름 처리 .....	375
별칭 파일 및 별칭 데이터베이스 검사 지정 .....	376
하위 주소 처리 .....	376
채널별 다시 쓰기 규칙 검사 사용 .....	377
소스 경로 제거 .....	378
반드시 별칭을 통해 주소 지정 .....	378
헤더 처리 구성 .....	378
포함 헤더 다시 쓰기 .....	379
선택한 메일 헤더 행 제거 .....	379
X-Envelope-to: 헤더 행 생성/제거 .....	381
두 자리 또는 네 자리로 날짜 변환 .....	381
날짜의 요일 지정 .....	381
긴 헤더 행 자동 분할 .....	382
헤더 맞춤 및 접기 .....	382
최대 길이 헤더 지정 .....	383
민감도 검사 .....	383
헤더의 기본 언어 설정 .....	384
첨부 파일 및 MIME 처리 .....	384
Encoding: 헤더 행 무시 .....	384
메일/부분 메일 자동 조각 모음 .....	385
대용량 메일 자동 조각화 .....	386
메일 행 길이 제한 적용 .....	387
메일, 할당량, 수신자 및 인증 시도의 제한 .....	387
성공하지 못한 인증 시도에 대한 제한 .....	388
절대 메일 크기 제한 지정 .....	388
크기 제한 또는 수신자 수 제한을 초과하는 메일 대상 다시 지정 .....	389
할당량 사용자에게 대한 메일 전달 처리 .....	391
1000자가 넘는 행이 있는 SMTP 메일 처리 .....	392
일반 및 Filename Content-type 및 Content-disposition 매개 변수의 길이 제어 .....	392

메일 수신자 제한 .....	392
헤더 크기 제한 .....	393
MTA 대기열에서 파일 만들기 .....	393
메일의 여러 주소 처리 방법 제어 .....	393
여러 하위 디렉토리로 채널 메일 대기열 분산 .....	394
세션 제한 설정 .....	395
로그 및 디버깅 구성 .....	395
로그 키워드 .....	395
디버깅 키워드 .....	396
Loopcheck 설정 .....	396
기타 키워드 .....	397
프로세스 채널 대체 .....	397
채널 작업 유형 .....	397
파이프 채널 .....	398
메일함 필터 파일 위치 지정 .....	398
스팸 필터 키워드 .....	399
주소 검증 후와 확장 전의 라우팅 .....	399
NO-SOLICIT SMTP 확장 지원 .....	403
잘못된 RCPT TO: 주소에 대한 제한 설정 .....	403

## **13장 미리 정의된 채널 사용 ..... 405**

파이프 채널을 사용하여 메일을 프로그램에 전달 .....	407
원시(/var/mail) 채널 구성 .....	408
보관 채널을 사용하여 메일을 일시적으로 보관 .....	409
변환 채널 .....	410
MIME 개요 .....	411
변환 처리를 위한 트래픽 선택 .....	413
변환 처리 제어 .....	414
변환 채널 출력을 사용하여 메일 바운스, 삭제 또는 보관 .....	423
변환 채널 예 .....	425
아랍어 문자 세트 자동 감지 .....	425
문자 세트 변환 및 메일 형식 다시 지정 .....	430
문자 세트 변환 .....	432
메일 형식 다시 지정 .....	433
서비스 변환 .....	439

## **14장 Messaging Server에 스팸 및 바이러스 필터링 프로그램 통합 ..... 441**

Messaging Server에 스팸 필터링 프로그램 통합—작동 원리 .....	442
타사 스팸 필터링 프로그램 배포 및 구성 .....	442
스팸 필터링 소프트웨어 클라이언트 라이브러리 로드 및 구성 .....	443
필터링할 메일 지정 .....	444
스팸 메일에 대해 수행할 작업 지정 .....	451

Symantec Brightmail 스팸 방지 사용 .....	455
Brightmail 작업 방법 .....	455
Brightmail 요구 사항 및 성능 고려 사항 .....	457
Brightmail 배포 .....	457
Brightmail 구성 옵션 .....	458
SpamAssassin 사용 .....	459
SpamAssassin 개요 .....	460
SpamAssassin/Messaging Server 작업 이론 .....	460
SpamAssassin 요구 사항 및 사용 시 고려 사항 .....	461
SpamAssassin 배포 .....	462
SpamAssassin 구성 예 .....	462
SpamAssassin 테스트 .....	469
SpamAssassin 옵션 .....	471
SAVSE(Symantec Anti-virus Scanning Engine) 사용 .....	473
SAVSE 개요 .....	474
SpamAssassin 요구 사항 및 사용 시 고려 사항 .....	474
SAVSE 배포 .....	475
SAVSE 구성 예 .....	475
SAVSE 옵션 .....	478
Sieve 확장 지원 .....	480

## **15장 LMTP 전달 .....** **483**

LMTP 전달 기능 .....	484
LMTP를 사용하지 않는 2계층 배포의 메일 처리 .....	484
LMTP를 사용하는 2계층 배포의 메일 처리 .....	486
LMTP 개요 .....	487
LMTP 전달 구성 .....	488
LMTP를 사용하는 인바운드 MTA 릴레이 구성 .....	488
LMTP를 사용하고 MTA 없이 백엔드 저장소 구성 .....	494
LMTP를 통해 메시지 저장소와 전체 MTA를 갖는 백엔드 시스템에 메일을 보내도록 릴레이 구성 .....	496
전체 MTA가 있는 백엔드 메시지 저장소 시스템의 LMTP 구성 .....	497
구현된 LMTP 프로토콜 .....	498

## **16장 휴가 자동 메일 회신 .....** **503**

휴가 자동 회신 개요 .....	503
자동 회신 구성 .....	504
백엔드 시스템에서 자동 회신 구성 .....	505
릴레이에서 자동 회신 구성 .....	505
휴가 자동 회신 작동 원리 .....	506
휴가 자동 회신 속성 .....	508

<b>17장 메일 필터링 및 액세스 제어</b> .....	<b>511</b>
1부. 매핑 테이블 .....	511
매핑 테이블을 사용한 액세스 제어 .....	512
액세스 제어 매핑 테이블—작업 .....	512
액세스 제어 매핑 테이블 플래그 .....	514
SEND_ACCESS 및 ORIG_SEND_ACCESS 테이블 .....	517
MAIL_ACCESS 및 ORIG_MAIL_ACCESS 매핑 테이블 .....	519
FROM_ACCESS 매핑 테이블 .....	521
PORT_ACCESS 매핑 테이블 .....	523
MTA에 대해 지정된 IP 액세스 연결 제한 .....	525
액세스 제어가 적용되는 경우 .....	526
액세스 제어 매핑 테스트 .....	527
SMTP 릴레이 추가 .....	528
외부 사이트에 대한 SMTP 릴레이 허용 .....	530
SMTP 릴레이 차단 구성 .....	531
MTA의 내부 메일과 외부 메일 구분 방법 .....	531
인증된 사용자의 메일 구분 .....	533
메일 릴레이 금지 .....	534
SMTP 릴레이 차단에 RBL 검사를 포함한 DNS 조회 사용 .....	535
많은 수의 액세스 항목 처리 .....	537
2부. 메일함 필터 .....	540
Sieve 필터 지원 .....	540
Sieve 필터링 개요 .....	541
사용자 수준 필터 만들기 .....	542
채널 수준 필터 만들기 .....	542
MTA 차원 필터 만들기 .....	544
제거된 메일을 FILTER_DISCARD 채널 외부로 라우팅 .....	545
사용자 수준 필터 디버그 .....	545
imsimta test -exp 출력 .....	547
imsimta test -exp 구문 .....	549
<b>18장 메시지 저장소 관리</b> .....	<b>551</b>
개요 .....	552
메시지 저장소 디렉토리 레이아웃 .....	553
메시지 저장소에서 메일을 제거하는 방법 .....	556
저장소에 대한 관리자 액세스 지정 .....	557
관리자 추가 .....	558
관리자 항목 수정 .....	558
관리자 항목 삭제 .....	559
공유 폴더 정보 .....	559
공유 폴더 액세스 권한 .....	561
공유 폴더 작업 .....	564
공유 폴더 만들기 .....	564

공용 폴더의 액세스 제어 권한 변경 .....	565
공유 폴더 목록을 사용 가능 또는 사용 불가능하게 하기 .....	566
분산 공유 폴더 설정 .....	566
공유 폴더 데이터 모니터 및 유지 관리 .....	568
메시지 저장소 할당량 정보 .....	570
사용자 할당량 .....	571
도메인 할당량 .....	571
<b>Telephony Application Server</b> 예외 사항 .....	572
메시지 저장소 할당량 구성 .....	573
기본 사용자 할당량 지정 .....	574
개별 사용자 할당량 지정 .....	575
도메인 할당량 지정 .....	575
할당량 알림 배포 .....	575
할당량 적용 활성화 또는 비활성화 .....	577
유예 기간 설정 .....	579
<b>Netscape Messaging Server</b> 할당량 호환 모드 .....	580
자동 메일 제거(만료 및 제거) 기능 설정 .....	581
<b>imexpire</b> 작동 원리 .....	581
자동 메일 제거 기능 배포 .....	582
메시지 저장소 분할 영역 구성 .....	593
분할 영역 추가 .....	594
메일함을 다른 디스크 분할 영역으로 이동 .....	595
기본 메시지 저장소 분할 영역 정의 변경 .....	597
메시지 저장소 유지 관리 절차 수행 .....	597
메일함 관리 .....	597
할당량 제한 모니터 .....	603
디스크 공간 모니터 .....	604
<b>stored</b> 유틸리티 사용 .....	604
동일한 메일의 중복 저장에 따른 저장소 크기 줄이기 .....	606
메시지 저장소 백업 및 복원 .....	610
메일함 백업 정책 만들기 .....	611
백업 그룹 만들기 .....	612
<b>Messaging Server</b> 백업 및 복원 유틸리티 .....	613
백업 수행 시 대량 메일 제외 .....	615
부분 복원 시의 고려 사항 .....	616
중분 백업된 메일함에서 메일 복원 .....	617
<b>Legato Networker</b> 사용 .....	618
<b>Legato</b> 를 제외한 타사 백업 소프트웨어 사용 .....	622
백업 및 복원 문제 해결 .....	623
메시지 저장소 재해 복구 및 복원 .....	623
사용자 액세스 모니터링 .....	624
메시지 저장소 문제 해결 .....	625
표준 메시지 저장소 모니터링 절차 .....	626

메시지 저장소 시작 및 복구 .....	629
메일함 및 메일함 데이터베이스 복구 .....	632
일반 문제 및 해결 방법 .....	637
<b>19장 보안 및 액세스 제어 구성 .....</b>	<b>641</b>
서버 보안 정보 .....	642
HTTP 보안 정보 .....	643
인증 기법 구성 .....	644
일반 텍스트 비밀번호에 대한 액세스 구성 .....	646
사용자 전환 .....	647
사용자 비밀번호 로그인 .....	647
IMAP, POP 및 HTTP 비밀번호 로그인 .....	648
SMTP 비밀번호 로그인 .....	648
암호화 및 인증서 기반 인증 구성 .....	649
관리 콘솔을 통해 인증서 얻기 .....	651
자체 서명된 인증서 만들기 .....	655
SSL 사용 및 암호문 선택 .....	656
인증서 기반 로그인 설정 .....	658
SMTP 프로토콜을 사용하여 SSL 성능을 최적화하는 방법 .....	660
네트워크 보안 서비스 도구 .....	660
인증서 및 키 관리 .....	660
Messaging Server에 대한 관리자 액세스 구성 .....	661
위임된 관리 계층 .....	662
서버 전체에 대한 액세스 제공 .....	663
특정 작업에 대한 액세스 제한 .....	663
POP, IMAP 및 HTTP 서비스에 대한 클라이언트 액세스 구성 .....	664
클라이언트 액세스 필터의 작동 방법 .....	665
필터 문 .....	666
필터 예 .....	671
서비스에 대한 액세스 필터 만들기 .....	672
HTTP 프록시 인증에 대한 액세스 필터 만들기 .....	673
POP before SMTP 사용 .....	675
SMTP 프록시 설치 .....	675
SMTP 서비스에 대한 클라이언트 액세스 구성 .....	679
SSL을 통한 사용자/그룹 디렉토리 조회 .....	679
<b>20장 Communications Express Mail용 S/MIME 관리 .....</b>	<b>681</b>
S/MIME .....	682
알아야 할 개념 .....	682
필수 소프트웨어 및 하드웨어 구성 요소 .....	683
S/MIME 사용을 위한 요구 사항 .....	684
개인 및 공개 키 .....	684

스마트 카드에 저장된 키 .....	685
클라이언트 시스템에 저장된 키 .....	685
LDAP 디렉토리에 공개 키 게시 .....	685
메일 사용자에게 S/MIME 사용 권한 부여 .....	686
여러 언어 지원 .....	686
<b>Messaging Server 설치 후 시작 .....</b>	<b>686</b>
S/MIME 애플릿 .....	687
기본 S/MIME 구성 .....	688
자격 증명을 사용하여 LDAP에서 공개 키, CA 인증서 및 CRL 액세스 .....	693
smime.conf 파일의 매개 변수 .....	694
<b>Messaging Server 옵션 .....</b>	<b>701</b>
SSL을 사용하여 인터넷 연결 보안 .....	702
Messaging Server 및 Communications Express Mail 간의 연결 보안 .....	702
Messaging Server 및 S/MIME 애플릿 간의 연결 보안 .....	703
클라이언트 시스템의 키 액세스 라이브러리 .....	703
예 .....	704
개인 및 공개 키 확인 .....	705
사용자의 개인 또는 공개 키 찾기 .....	705
CRL에 대해 인증서 확인 .....	706
CRL 액세스 .....	706
프록시 서버 및 CRL 확인 .....	708
오래된 CRL 사용 .....	708
사용할 메일 시간 지정 .....	709
CRL 액세스 문제 .....	710
인증서가 해지된 경우 .....	711
S/MIME 기능을 사용할 수 있는 권한 부여 .....	711
S/MIME 권한 예 .....	712
인증서 관리 .....	712
LDAP 디렉토리의 CA 인증서 .....	712
LDAP 디렉토리의 공개 키 및 인증서 .....	714
키와 인증서가 LDAP 디렉토리에 있는지 확인 .....	715
네트워크 보안 서비스 인증서 .....	717
<b>Communications Express S/MIME 최종 사용자 정보 .....</b>	<b>717</b>
처음 로그인 .....	718
서명 및 암호화 설정 .....	719
Java 콘솔 활성화 .....	721
<b>21장 로깅 관리 .....</b>	<b>723</b>
로깅 개요 .....	723
로깅 데이터의 유형 .....	724
Messaging Server 로그 파일의 유형 .....	724
여러 로그 파일에서 메일 추적 .....	726
로깅 관리를 위한 도구 .....	728



MTA 메일 및 연결 로그 관리 .....	728
MTA 로그 항목 형식 이해 .....	729
MTA 로깅 활성화 .....	733
추가 MTA 로깅 옵션 지정 .....	734
MTA 메일 로깅 예 .....	735
디스패처 디버깅 활성화 .....	751
서비스 로그 관리 .....	753
서비스 로그 특징 이해 .....	753
서비스 로그 파일 형식 이해 .....	756
서비스 로깅 옵션 정의 및 설정 .....	757
서비스 로그 검색 및 보기 .....	760
서비스 로그 작업 .....	761
메시지 저장소 로깅에 메일 추적 사용 .....	764
메시지 저장소 로깅 예 .....	766
<b>22장 MTA 문제 해결 .....</b>	<b>769</b>
문제 해결 개요 .....	770
표준 MTA 문제 해결 절차 .....	770
MTA 구성 확인 .....	771
메일 대기열 디렉토리 확인 .....	771
중요 파일의 소유권 확인 .....	771
Job Controller 및 디스패처 실행 확인 .....	772
로그 파일 확인 .....	774
수동으로 채널 프로그램 실행 .....	775
개별 채널 시작 및 중지 .....	775
MTA 문제 해결 예 .....	777
일반 MTA 문제 및 솔루션 .....	781
TLS 문제 .....	782
영향력이 없는 구성 파일 또는 MTA 데이터베이스에 대한 변경 사항 .....	782
MTA에서 보내는 메일은 전송하지만 받는 메일을 수신하지 않음 .....	783
디스패처(SMTP Server)가 시작되지 않음 .....	783
받는 SMTP 연결의 시간 초과 .....	784
메일이 대기열에서 제외되지 않음 .....	785
MTA 메일이 전달되지 않음 .....	787
메일 루핑 .....	789
받은 메일 인코딩 .....	791
서버측 규칙(SSR)이 작동하지 않음 .....	792
받은 필드 또는 주소의 로컬 부분에 있는 별표 .....	793
일반 오류 메시지 .....	793
mm_init 오류 .....	794
컴파일된 구성 버전이 일치하지 않음 .....	797
공간 오류 스왑 .....	798
파일 열기 또는 오류 만들기 .....	798

유효하지 않은 호스트/도메인 오류 .....	799
SMTP 채널 오류: os_smtp_* errors .....	800
<b>23장 Messaging Server 모니터링 .....</b>	<b>801</b>
자동 모니터링 및 재시작 .....	801
일상적인 모니터링 작업 .....	802
포스트마스터 메일 검사 .....	802
로그 파일 모니터링 및 유지 관리 .....	802
msprobe 유틸리티 설정 .....	803
시스템 성능 모니터링 .....	803
중단간 메일 전달 시간 모니터링 .....	803
디스크 공간 모니터링 .....	804
CPU 사용 모니터링 .....	806
MTA 모니터링 .....	807
메일 대기열 크기 모니터링 .....	807
전달 실패 비율 모니터링 .....	808
인바운드 SMTP 연결 모니터링 .....	808
디스패처 및 Job Controller 프로세스 모니터링 .....	809
LDAP Directory Server 모니터링 .....	810
slapd 모니터링 .....	810
메일 액세스 모니터링 .....	810
imspd, popd 및 httpd 모니터링 .....	811
stored 모니터링 .....	812
메시지 저장소 모니터링 .....	813
메시지 저장소 데이터베이스 잠금의 상태 모니터링 .....	814
mboxlist 디렉토리의 데이터베이스 로그 파일 수 모니터링 .....	814
모니터링을 위한 유틸리티와 도구 .....	815
immonitor-access .....	815
stored .....	815
counterutil .....	816
로그 파일 .....	819
imsimta counters .....	819
imsimta qm counters .....	822
SNMP를 사용한 MTA 모니터링 .....	823
메일함 할당량 검사를 위한 imquotacheck .....	823
msprobe 및 watcher 기능을 사용하여 모니터링 .....	824
<b>부록 A SNMP 지원 .....</b>	<b>829</b>
SNMP 구현 .....	830
Messaging Server에서의 SNMP 작업 .....	830
Solaris 8에서 Messaging Server에 대한 SNMP 지원 구성 .....	831
SNMP 클라이언트로부터 모니터링 .....	832
Unix 플랫폼에서 다른 Sun Java System 제품과 공존 .....	833

Messaging Server의 SNMP 정보 .....	833
applTable .....	834
assocTable .....	835
mtaTable .....	836
mtaGroupTable .....	837
mtaGroupAssociationTable .....	839
mtaGroupErrorTable .....	840
<b>부록 B Messaging Server에서 Event Notification Service 관리 .....</b>	<b>843</b>
Messaging Server에서 ENS Publisher 로드 .....	843
Messaging Server에서 ENS Publisher 로드 .....	844
샘플 Event Notification Service 프로그램 실행 .....	844
샘플 ENS 프로그램 실행 .....	845
Event Notification Service 관리 .....	845
ENS 시작 및 중지 .....	845
ENS 시작 및 중지 .....	846
iPlanet Event Notification Service 구성 매개 변수 .....	846
<b>부록 C 콘솔 인터페이스가 있는 메일 사용자 및 메일 목록 관리(권장되지 않음) .....</b>	<b>847</b>
메일 사용자 관리 .....	847
메일 사용자 액세스 .....	847
사용자 전자 메일 주소 지정 .....	849
전달 옵션 구성 .....	851
전달 주소 지정 .....	853
자동 회신 설정 구성 .....	854
허가된 서비스 구성 .....	855
메일 목록 관리 .....	856
메일 목록 액세스 .....	856
메일 목록 설정 지정 .....	858
목록 구성원 지정 .....	860
메일 게시 제한 정의 .....	863
중재자 정의 .....	864
<b>부록 D SMS(Short Message Service) .....</b>	<b>867</b>
소개 .....	867
요구 사항 .....	869
SMS 채널 작동 원리 .....	870
전자 메일을 채널로 전송 .....	870
전자 메일에서 SMS로의 변환 프로세스 .....	872
SMS 메일 전송 프로세스 .....	876
사이트 정의 주소 유효성 검사 및 변환 .....	880
사이트 정의 텍스트 변환 .....	881

SMS 채널 구성 .....	886
SMS 채널 추가 .....	886
SMS 채널 옵션 파일 만들기 .....	889
사용 가능한 옵션 .....	890
SMS 채널 추가 .....	911
전달 재시도 빈도 조정 .....	912
샘플 단방향 구성(MobileWay) .....	912
양방향 SMS를 위한 SMS 채널 구성 .....	914
SMS 게이트웨이 서버 작동 이론 .....	915
SMS 게이트웨이 서버 기능 .....	916
SMPP 릴레이 및 서버의 동작 .....	916
원격 SMPP에서 게이트웨이 SMPP로의 통신 .....	917
SMS 릴레이 및 알림 처리 .....	918
SMS 게이트웨이 서버 구성 .....	920
양방향 SMS 라우팅 설정 .....	921
SMS 게이트웨이 서버 사용 가능/불가능하게 하기 .....	922
SMS 게이트웨이 서버 시작 및 중지 .....	922
SMS 게이트웨이 서버 구성 파일 .....	923
게이트웨이 서버에서 ETM(Email-To-Mobile) 구성 .....	923
MTE(Mobile-To-Email) 작업 구성 .....	926
구성 옵션 .....	927
전역 옵션 .....	928
SMPP 릴레이 옵션 .....	931
SMPP 서버 옵션 .....	934
게이트웨이 프로필 옵션 .....	936
양방향 SMS의 구성 예 .....	941
SMS 게이트웨이 서버 저장소 요구 사항 .....	944
<b>부록 E 설치 워크시트 .....</b>	<b>947</b>
Directory Server 설치 .....	948
Administration Server 초기 런타임 구성 .....	950
Directory Server 설정 스크립트(comm_dssetup.pl) .....	952
Messaging Server 초기 런타임 구성 .....	954
<b>용어집 .....</b>	<b>957</b>
<b>색인 .....</b>	<b>959</b>

# 표 목차

표 1	설명서 구성 .....	30
표 2	활자체 규약 .....	32
표 3	기호 규약 .....	33
표 4	기본 경로 및 파일 이름 .....	34
표 1-1	Messaging Server 구성 프로그램의 옵션 플래그 .....	52
표 1-2	Sun_MsgSvr의 소유권 및 액세스 모드 변경 .....	64
표 1-3	사후 설치 디렉토리 및 파일 .....	68
표 1-4	설치 도중 지정되는 포트 번호 .....	70
표 1-5	잠재적 포트 번호 충돌 .....	71
표 2-1	*.MERGED 또는 *.CHANGES 파일을 생성하는 Messaging Server 구성 파일 .....	75
표 3-1	지원되는 Sun Cluster Server 및 Veritas Cluster Server 버전 .....	85
표 3-2	Veritas Cluster Server 속성 .....	91
표 4-1	Messaging Server 초기 런타임 구성 시 설정된 비밀번호 .....	104
표 4-2	Sun Cluster 3.0/3.1 환경에서 시작, 중지, 다시 시작 .....	107
표 4-3	Veritas 1.3, 2.0, 2.1 및 3.5 환경에서 시작, 중지, 다시 시작 .....	107
표 4-4	watcher 및 msprobe에서 모니터링하는 서비스 .....	111
표 4-5	HA 자동 재시작 매개 변수 .....	112
표 6-1	Access Manager 단일 사인 온(SSO) 매개 변수 .....	143
표 6-2	SSO 상호 운용성 .....	146
표 6-3	신뢰할 수 있는 원 단일 사인 온(SSO) 매개 변수 .....	152
표 7-1	Messaging Multiplexor 구성 파일 .....	165
표 7-2	MMP 명령 .....	166
표 9-1	다양한 schematag 값의 결과인 객체 클래스 .....	207
표 9-2	검사할 속성 .....	208
표 9-3	검색된 디스트 할당량 및 메일 할당량 속성을 설정하는 MTA 옵션 .....	212
표 9-4	MTA 옵션, 기본 속성 및 메타 문자 .....	212
표 9-5	DELIVERY_OPTIONS MTA 옵션에 사용할 수 있는 단일 문자 접두어 .....	214

표 9-6	전달 옵션에서 사용하기 위한 추가 메타 문자 .....	214
표 9-7	\$nI 및 \$nS 메타 문자의 동작 수정을 제어하는 정수 .....	216
표 9-8	특수한 템플릿 문자열 .....	216
표 9-9	설정할 그룹 확장 기본 속성 및 MTA 옵션 .....	218
표 9-10	local.imta.schematag 값과 속성 .....	221
표 9-11	LDAP_USE_ASYNC MTA 옵션에 대한 설정 .....	223
표 10-1	주소 및 관련 채널 .....	228
표 10-2	Messaging Server 매핑 테이블 .....	229
표 10-3	매핑 패턴 와일드카드 .....	232
표 10-4	매핑 템플릿 대체 및 메타 문자 .....	235
표 10-5	MTA 구성 파일 .....	243
표 10-6	Job Controller 구성 파일 옵션 .....	253
표 10-7	REVERSE 매핑 테이블 플래그 .....	258
표 10-8	FORWARD 매핑 테이블 플래그 설명 .....	261
표 10-9	알림 메일 대체 시퀀스 .....	266
표 10-10	DSN(Delivery Status Notification) 및 MDN(Message Disposition Notification) 옵션 .....	270
표 10-11	포스트마스터 및 보낸 사람에게 알림 메일을 보내는 데 사용되는 키워드 .....	276
표 11-1	다시 쓰기 규칙의 특수한 패턴 요약 .....	285
표 11-2	다시 쓰기 규칙의 템플릿 형식 요약 .....	287
표 11-3	추출된 주소 및 호스트 이름 .....	291
표 11-4	다시 쓰기 규칙 템플릿 대체 및 제어 시퀀스 요약 .....	297
표 11-5	LDAP URL 대체 시퀀스 .....	301
표 11-6	단일 필드 대체 .....	304
표 11-7	샘플 주소 및 다시 쓰기 .....	310
표 12-1	채널 키워드(알파벳순) .....	314
표 12-2	채널 키워드 범주화(기능별) .....	317
표 12-3	SMTP 채널 .....	333
표 12-4	SMTP 명령 및 프로토콜 키워드 .....	335
표 12-5	TCP/IP 연결 및 DNS 조회 키워드 .....	344
표 12-6	authrewrite 비트 값 .....	352
표 12-7	메일 처리 및 전달 키워드 .....	356
표 12-8	missingrecipientpolicy 값 .....	371
표 13-1	미리 정의된 채널 .....	405
표 13-2	로컬 채널 옵션 .....	408
표 13-3	변환 채널 환경 변수 .....	418
표 13-4	변환 채널 출력 옵션 .....	421
표 13-5	변환 채널에 일반적으로 사용되는 특수 지시문 .....	423

표 13-6	변환 매개 변수 .....	427
표 13-7	HARSET-CONVERSION 매핑 테이블 키워드 .....	431
표 14-1	스팸 필터를 위한 MTA 채널 키워드 .....	449
표 14-2	MTA 스팸 필터 옵션(option.dat) .....	452
표 14-3	선택된 Brightmail 구성 파일 옵션 .....	458
표 14-4	SpamAssassin 옵션(spamassassin.opt) .....	471
표 14-5	SpamAssassin mode 옵션의 문자열 반환 .....	473
표 14-6	ICAP 옵션 .....	478
표 14-7	ICAP 모드 옵션의 답신 문자열 반환 .....	480
표 15-1	수신자에 대한 LMTP 상태 코드 .....	500
표 16-1	DELIVERY_OPTIONS의 자동 회신 규칙에 사용되는 접두어 문자 .....	504
표 17-1	액세스 제어 매핑 테이블 .....	513
표 17-2	액세스 매핑 플래그 .....	514
표 17-3	PORT_ACCESS 매핑 플래그 .....	524
표 17-4	filter 채널 키워드 URL 패턴 대체 태그(대소문자 무시) .....	543
표 18-1	메시지 저장소 명령줄 유틸리티 .....	552
표 18-2	메시지 저장소 디렉토리 설명 .....	555
표 18-3	ACL 권한 문자 .....	562
표 18-4	분산 공유 폴더 구성을 위한 변수 .....	566
표 18-5	readership 옵션 .....	569
표 18-6	메시지 저장소 할당량 속성 .....	572
표 18-7	메시지 저장소 configutil 매개 변수 .....	573
표 18-8	imexpire 속성 .....	585
표 18-9	정규 표현식을 사용한 imexpire 폴더 패턴 .....	587
표 18-10	만료 및 제거 configutil 로그 및 예약 매개 변수 .....	592
표 18-11	mboxutil 옵션 .....	598
표 18-12	stored 옵션 .....	605
표 18-13	relinker configutil 매개 변수 .....	609
표 18-14	stored 작업 .....	628
표 18-15	메시지 저장소 데이터베이스 스냅샷 매개 변수 .....	632
표 18-16	reconstruct 옵션 .....	633
표 19-1	일부 SASL 및 SASL 관련 configutil 매개 변수 .....	645
표 19-2	Messaging Server의 SSL 암호문 .....	657
표 19-3	서비스 필터의 와일드카드 이름 .....	668
표 20-1	클라이언트 시스템의 필수 하드웨어 및 소프트웨어 .....	683
표 20-2	서버 시스템의 필수 소프트웨어 .....	684
표 20-3	smime.conf 매개 변수 요약 .....	692

표 20-4	smime.conf 파일의 S/MIME 구성 매개 변수	695
표 20-5	클라이언트 시스템의 특수 라이브러리	704
표 20-6	Communications Express Mail의 서명 및 암호화 확인란	720
표 21-1	Messaging Server 로그 파일	725
표 21-2	로그 항목 코드	730
표 21-3	디스패처 디버깅 비트	751
표 21-4	저장소 및 관리 서비스의 로그 수준	754
표 21-5	로그 이벤트가 발생하는 범주	755
표 21-6	저장소 및 관리 로그 파일 구성 요소	756
표 22-1	MTA 로그 파일	774
표 23-1	counterutil alarm 통계	817
표 23-2	counterutil imapstat 통계	818
표 23-3	counterutil diskstat 통계	818
표 23-4	counterutil serverresponse 통계	819
표 23-5	msprobe 및 watcher configutil 옵션	825
표 23-6	유용한 경고 메시지 configutil 매개 변수	827
표 B-1	iBiff 구성 매개 변수	846
표 C-1	LDAP URL 옵션	861
표 D-1	SMS 속성	870
표 D-2	BIND_TRANSMITTER PDU에서 생성되는 필드	877
표 D-3	SUBMIT_SM PDU에서 생성되는 필수 필드	878
표 D-4	SUBMIT_SM PDU에서 생성되는 선택적 필드	879
표 D-5	SMS 채널 옵션	890
표 D-6	USE_HEADER_FROM 값	896
표 D-7	USE_UCS2에 대한 유효 값	897
표 D-8	Numeric Plan Indicator 값	898
표 D-9	일반 TON 값	899
표 D-10	각 SMS 프로필 유형에 대해 해석되는 SMS 우선 순위 값	899
표 D-11	Priority: 헤더를 SMS 우선 순위 플래그로 변환하기 위한 매핑	900
표 D-12	DEFAULT_PRIVACY 및 USE_HEADER_SENSITIVITY에 대한 결과 값	900
표 D-13	개인 정보 값의 SMS 해석	901
표 D-14	Sensitivity: 헤더를 SMS 우선 순위 값으로 변환하기 위한 매핑	901
표 D-15	DEFAULT_VALIDITY_PERIOD의 형식 및 값	902
표 D-16	DEBUG 비트 마스크	909
표 D-17	대체 시퀀스	909
표 D-18	양방향 구성 예외	914
표 D-19	SMPP 서버 PDU(Protocol Data Unit)	917



표 D-20	전역 옵션 .....	928
표 D-21	DEBUG 비트 마스크 .....	931
표 D-22	SMPP 릴레이 옵션 .....	932
표 D-23	SMPP 서버 옵션 .....	934
표 D-24	SMS 게이트웨이 서버 프로필 옵션 .....	936
표 D-25	SMS에서 전자 메일로의 우선 순위 플래그 매핑 .....	940
표 D-26	SMS에서 전자 메일로의 개인 정보 플래그 매핑 .....	941
표 D-27	SMS 게이트웨이 서버 저장소 요구 사항 .....	944
표 E-1	Directory Server 설치 매개 변수 .....	948
표 E-2	Administration Server 초기 런타임 구성 프로그램 매개 변수 .....	950
표 E-3	comm_dssetup.pl 스크립트 매개 변수 .....	952
표 E-4	Messaging Server 초기 런타임 구성 프로그램 매개 변수 .....	954



# 그림 목차

그림 3-3	간단한 Sun Java System Messaging Server HA 구성	93
그림 5-1	HTTP 서비스 구성 요소	136
그림 6-1	단순 SSO 배포	147
그림 6-2	복잡한 SSO 배포	147
그림 7-1	MMP 설치 환경에서의 클라이언트와 서버	158
그림 7-2	여러 Messaging Server를 지원하는 여러 MMP	169
그림 7-3	iPlanet Messenger Express Multiplexor 개요	173
그림 8-1	Messaging Server, 단순화된 구성 요소 보기(Messenger Express는 표시되지 않음)	183
그림 8-2	MTA 구조	184
그림 8-3	마스터 및 슬레이브 프로그램	191
그림 8-4	ims-ms 채널	191
그림 14-1	Brightmail 및 Messaging Server 구조	455
그림 15-1	LMTP를 사용하지 않는 2계층 배포	485
그림 15-2	LMTP를 사용하는 2계층 배포	486
그림 18-1	메시지 저장소 디렉토리 레이아웃	554
그림 18-2	Ed의 클라이언트 공유 메일 폴더 목록의 예	560
그림 18-3	분산 공유 폴더—예	567
그림 18-4	자동 메일 제거(만료/제거) GUI—대략적인 그림	589
그림 18-5	메시지 저장소 다이제스트 저장소	607
그림 18-6	백업 그룹 디렉토리 구조	620
그림 19-1	Messaging Server와의 암호화된 통신	650
그림 20-1	S/MIME 애플릿	687
그림 20-2	개인 및 공개 키 확인	705
그림 A-1	SNMP 정보 흐름	831
그림 D-1	단방향 및 양방향 SMS의 논리적 흐름	868
그림 D-2	SMS 채널 전자 메일 처리	873
그림 D-3	SMS 채널 전자 메일 처리(계속)	874



# 머리말

이 설명서에서는 Sun Java™ System Messaging Server 관련 소프트웨어 구성 요소를 관리하는 방법에 대해 설명합니다. Messaging Server는 개방형 인터넷 표준을 사용하여 모든 규모의 기업과 메시징 호스트의 전자 메일 요구 사항을 충족시키는 강력하고도 유연한 크로스 플랫폼 솔루션을 제공합니다.

이 장은 다음 내용으로 구성되어 있습니다.

- 대상
- 이 설명서를 읽기 전에
- 설명서 구성
- 이 설명서에 사용된 규칙
- 관련 설명서
- 본 설명서의 온라인 버전
- Sun 자원 온라인 액세스
- Sun 기술 지원에 문의
- 타사 웹 사이트 관련 참조 사항
- 사용자 의견 환영

## 대상

이 설명서는 조직의 사이트에서 Messaging Server를 관리하고 배포하는 일을 담당하는 사람을 대상으로 합니다. *Sun Java System Communications Services Deployment Planning Guide*(<http://docs.sun.com/doc/819-0063>)도 함께 참조해야 합니다.

# 이 설명서를 읽기 전에

이 설명서의 내용은 본 설명서를 읽는 사람이 Messaging Server 소프트웨어를 설치하는 일을 담당하며 다음 사항에 대해 잘 알고 있다고 가정합니다.

- 인터넷 및 WWW(World Wide Web)
- Messaging Server 프로토콜
- Sun Java System Administration Server
- Sun Java System Directory Server 및 LDAP
- Sun Java System 콘솔
- 다음 플랫폼에서의 시스템 관리 및 네트워킹 작업
- 일반 배포 구조

## 설명서 구성

이 설명서는 다음 장과 부록으로 구성되어 있습니다.

**표 1** 설명서 구성

장	설명
머리말	이 설명서 사용과 관련된 일반적인 내용입니다.
1장, "사후 설치 작업 및 레이아웃"	Messaging Server 기능을 설정하는 데 필요한 작업에 대해 설명합니다.
2장, "Sun Java Systems Messaging Server로 업그레이드"	Messaging Server 5.2에서 Messaging Server 6 2005Q1로 업그레이드하는 방법에 대해 설명합니다.
3장, "고가용성 구성"	Messaging Server와 함께 사용하기 위해 Veritas Cluster Server 및 Sun Cluster 고가용성 클러스터링 소프트웨어를 구성하는 방법에 대해 설명합니다.
4장, "일반 메시징 기능 구성"	일반적인 Messaging Server 작업에 대해 설명합니다.
5장, "POP, IMAP 및 HTTP 서비스 구성"	Sun ONE 콘솔이나 명령줄 유틸리티를 사용하여 POP, IMAP 및 HTTP 서비스를 지원하도록 서버를 구성하는 방법에 대해 설명합니다.
6장, "단일 사인 온(SSO) 사용"	단일 사인 온(SSO)을 사용하는 방법에 대해 설명합니다.
7장, "멀티플렉서 서비스 구성 및 관리"	표준 메일 프로토콜(POP, IMAP 및 SMTP)용 MMP(Messaging Multiplexor)와 Messenger Express 웹 인터페이스에 사용되는 Messenger Express Multiplexor에 대해 설명합니다.
8장, "MTA 개념"	MTA의 개념에 대해 설명합니다.

**표 1** 설명서 구성

장	설명
9장, "MTA 주소 변환 및 라우팅"	MTA 주소 변환 및 라우팅에 대해 설명합니다.
10장, "MTA 서비스 및 구성 정보"	일반 MTA 서비스와 구성에 대해 설명합니다.
11장, "다시 쓰기 규칙 구성"	imta.cnf 파일에서 다시 쓰기 규칙을 구성하는 방법에 대해 설명합니다.
12장, "채널 정의 구성"	MTA 구성 파일 imta.cnf에서 채널 키워드 정의를 사용하는 방법에 대해 설명합니다.
13장, "미리 정의된 채널 사용"	MTA에서 미리 정의된 채널 정의를 사용하는 방법에 대해 설명합니다.
14장, "Messaging Server에 스팸 및 바이러스 필터링 프로그램 통합"	스팸 및 바이러스 필터링 소프트웨어를 Messaging Server와 통합 및 구성하는 방법에 대해 설명합니다.
15장, "LMTP 전달"	LMTP 작업 및 배포에 대해 설명합니다.
16장, "휴가 자동 메일 회신"	휴가 자동 회신 기법에 대해 설명합니다.
17장, "메일 필터링 및 액세스 제어"	메일의 소스(보낸 사람, IP 주소 등) 또는 헤더 문자열에 기초하여 메일을 필터링하는 방법에 대해 설명합니다.
18장, "메시지 저장소 관리"	메시지 저장소와 해당 관리 인터페이스에 대해 설명합니다.
19장, "보안 및 액세스 제어 구성"	Messaging Server에 대한 보안 및 액세스 제어를 구성하는 방법에 대해 설명합니다.
20장, "Communications Express Mail용 S/MIME 관리"	S/MIME을 관리하는 방법에 대해 설명합니다.
21장, "로깅 관리"	Messaging Server 로깅 기능에 대해 설명합니다.
22장, "MTA 문제 해결"	MTA 문제 해결을 위한 일반 도구, 방법 및 절차에 대해 설명합니다.
23장, "Messaging Server 모니터링"	Messaging Server의 모니터링에 대해 설명합니다.
부록 A, "SNMP 지원"	Messaging Server에서 SNMP 지원을 사용하는 방법에 대해 설명합니다.
부록 B, "Messaging Server에서 Event Notification Service 관리"	Messaging Server에서 ENS Publisher(Event Notification Service Publisher)를 사용하고 ENS(Event Notification Service)를 관리하는 방법에 대해 설명합니다.

**표 1** 설명서 구성

장	설명
부록 C, "콘솔 인터페이스가 있는 메일 사용자 및 메일 목록 관리(권장되지 않음)"	권장되지 않습니다.
부록 D, "SMS(Short Message Service)"	SMS(Short Message Service)를 구현하는 방법에 대해 설명합니다.
부록 E, "설치 워크시트"	설치를 계획할 수 있는 워크시트를 제공합니다.
용어집	이 설명서 세트에 사용되는 전체 용어 목록입니다.
색인	색인

## 이 설명서에 사용된 규칙

이 절의 표에서는 본 설명서에 사용된 규칙을 설명합니다.

### 활자체 규약

다음 표에서는 본 설명서에 사용된 활자체 규약에 대해 설명합니다.

**표 2** 활자체 규약

서체	의미	예
AaBbCc123 (고정 폭)	컴퓨터 화면에 나타나는 텍스트 또는 사용자가 입력해야 하는 텍스트를 나타냅니다. API 및 언어 요소, HTML 태그, 웹 사이트 URL, 명령 이름, 파일 이름, 디렉토리 경로 이름, 화면 상의 컴퓨터 출력, 샘플 코드 등에 사용됩니다.	.login 파일을 편집합니다.  ls -a를 사용하여 모든 파일을 나열합니다.  % You have mail.
<b>AaBbCc123</b> (굵은 고정 폭)	사용자가 입력해야 하는 코드 예 내의 텍스트나 기타 화면 상 컴퓨터 출력을 나타냅니다.	% <b>su</b> Password:



표 2 활자체 규약 (계속)

서체	의미	예
<i>AaBbCc123</i> (기울임꼴)	명령 또는 경로 이름에서 실제 이름이나 값으로 대체해야 하는 자리 표시자(예: 변수)를 나타냅니다. 책 제목, 새 용어, 강조할 단어 등에도 사용됩니다.	파일은 <i>msg_svr_base/bin</i> 디렉토리에 있습니다. <i>User's Guide</i> 의 6장을 읽으십시오. <i>클래스</i> 옵션이라고 합니다. 파일을 저장하지 <i>마십시오</i> .

## 기호

다음 표에서는 본 설명서에 사용된 기호 규칙을 설명합니다.

표 3 기호 규약

기호	설명	예	의미
[ ]	선택적인 명령 옵션입니다.	ls [-1]	-1 옵션은 사용하지 않아도 됩니다.
{   }	필수 명령 옵션에 대한 일련의 선택 항목을 포함합니다.	-d {y n}	-d 옵션에서는 y 인수나 n 인수를 사용해야 합니다.
-	동시에 입력하는 여러 키를 결합합니다.	Control-A	Ctrl 키를 누른 채로 A 키를 누릅니다.
+	연속해서 입력하는 여러 키를 결합합니다.	Ctrl+A+N	Ctrl 키를 눌렀다가 놓은 다음 후속 키들을 누릅니다.
>	그래픽 사용자 인터페이스의 메뉴 항목 선택을 나타냅니다.	파일 > 새로 만들기 > 템플릿	파일 메뉴에서 새로 만들기를 선택합니다. 새로 만들기 하위 메뉴에서 템플릿을 선택합니다.

## 기본 경로 및 파일 이름

다음 표에서는 본 설명서에 사용된 기본 경로와 파일 이름에 대해 설명합니다.

**표 4** 기본 경로 및 파일 이름

용어	설명
<i>msg_svr_base</i>	Messaging Server의 기본 설치 디렉토리를 나타냅니다. <i>msg_svr_base</i> 설치의 기본값은 다음과 같습니다.  Solaris™ 시스템: /opt/SUNWmsgsr  Linux 시스템: /opt/sun/messaging

## 명령줄 프롬프트

명령줄 프롬프트(예: C 셸의 %, Korn 또는 Bourne 셸의 \$)는 대부분의 예에 표시되어 있지 않습니다. 사용 중인 운영 체제에 따라 서로 다른 명령줄 프롬프트가 표시되기 때문입니다. 하지만 명령은 별도로 명시하지 않는 한, 설명서에 나와 있는 대로 입력해야 합니다.

## 관련 설명서

<http://docs.sun.com> 웹 사이트에서 Sun 기술 관련 설명서를 온라인으로 이용할 수 있습니다. 아카이브를 탐색하거나 특정 책 제목 또는 주제를 검색할 수 있습니다.

## Messaging Server 설명서

모든 Messaging Server 설명서에 대한 자세한 내용은 다음 URL을 사용하십시오.

[http://docs.sun.com/coll/MessagingServer\\_05q1](http://docs.sun.com/coll/MessagingServer_05q1) 및  
[http://docs.sun.com/coll/MessagingServer\\_05q1\\_ko](http://docs.sun.com/coll/MessagingServer_05q1_ko)

다음 설명서를 사용할 수 있습니다.

- *Sun Java System Messaging Server 릴리스 노트*(<http://docs.sun.com/doc/819-1051>)
- *Sun Java System Messaging Server 관리 설명서*(<http://docs.sun.com/doc/819-1055>)
- *Sun Java System Messaging Server Administration Reference*(<http://docs.sun.com/doc/819-0106>)

- *Sun Java System Messaging Server MTA Developer's Reference*(<http://docs.sun.com/doc/819-0107>)
- *Sun Java System Messenger Express Customization Guide*(<http://docs.sun.com/doc/819-0108>)

Messaging Server 제품군에는 Sun Java™ System 콘솔, Directory Server, Administration Server 등의 여러 제품이 포함되어 있습니다. 이러한 제품과 기타 제품에 대한 설명서는 다음 URL을 참조하십시오.

<http://docs.sun.com/db/prod/java.sys> 및 <http://docs.sun.com/db/prod/java.sys?l=ko>

소프트웨어 설명서 외에 Messaging Server Software Forum에서는 특정 Messaging Server 제품과 관련된 질문 사항에 대한 기술적 도움을 얻을 수 있습니다. 이 포럼의 URL은 다음과 같습니다.

<http://swforum.sun.com/jive/forum.jsp?forum=15>

## Communications Services 설명서

다음 URL에서 모든 Communications Services 제품과 관련된 설명서를 볼 수 있습니다.

[http://docs.sun.com/coll/MessagingServer\\_05q1](http://docs.sun.com/coll/MessagingServer_05q1) 및  
[http://docs.sun.com/coll/MessagingServer\\_05q1\\_ko](http://docs.sun.com/coll/MessagingServer_05q1_ko)

다음 설명서를 사용할 수 있습니다.

- *Sun Java System Messenger Express Customization Guide*(<http://docs.sun.com/doc/819-0108>)
- *Sun Java System Communications Services Delegated Administrator 설명서* (<http://docs.sun.com/doc/819-1102>)
- *Sun Java System Communications Services Deployment Planning Guide*(<http://docs.sun.com/doc/819-0063>)
- *Sun Java System Communications Services Schema Reference*(<http://docs.sun.com/doc/819-0113>)
- *Sun Java System Communications Services Schema Migration Guide*(<http://docs.sun.com/doc/819-0112>)
- *Sun Java System Event Notification Service Guide*(<http://docs.sun.com/doc/819-0109>)
- *Sun Java System Communications Express Administration Guide*(<http://docs.sun.com/doc/819-1066>)

- *Sun Java System Communications Express Customization Guide*(<http://docs.sun.com/doc/819-0116>)

## 본 설명서의 온라인 버전

*Messaging Server 관리 설명서*는 온라인에서 PDF 및 HTML 형식으로 볼 수 있습니다. 본 설명서를 볼 수 있는 URL은 다음과 같습니다.

(<http://docs.sun.com/doc/819-1055>)

## Sun 자원 온라인 액세스

제품 다운로드, 전문가 서비스, 패치 및 지원, 추가 개발자 정보 등을 얻으려면 다음을 방문하십시오.

- 다운로드 센터  
<http://www.sun.com/software/download/>
- 전문가 서비스  
<http://www.sun.com/service/sunps/sps.html>
- Sun 엔터프라이즈 서비스, Solaris 패치 및 지원  
<http://sunsolve.sun.com/>
- 개발자 정보  
<http://developers.sun.com/prodtech/index.html>

## Sun 기술 지원에 문의

제품 설명서에 나와 있지 않은 본 제품에 대한 기술적 질문 사항이 있을 경우에는 <http://www.sun.com/service/contacting>을 방문하십시오.

## 타사 웹 사이트 관련 참조 사항

Sun은 이 설명서에 언급된 타사 웹 사이트의 가용성에 대해 책임지지 않습니다. Sun은 이러한 사이트나 자원을 통해 사용할 수 있는 내용, 광고, 제품 또는 기타 자료에 대해서는 보증하지 않으며 책임지지 않습니다. Sun은 해당 사이트 또는 자원을 통해 사용 가능한 내용, 제품 또는 서비스의 사용과 관련해 발생하거나 발생했다고 간주되는 손해나 손실에 대해 책임이나 의무를 지지 않습니다.

## 사용자 의견 환영

Sun은 해당 설명서의 내용을 개선하기 위해 노력하고 있으며 사용자의 의견 및 제안을 환영합니다.

의견을 공유하려면 <http://docs.sun.com>으로 이동하여 Send Comments를 누르고 표시되는 온라인 양식에 설명서 제목과 부품 번호를 입력합니다. 부품 번호는 설명서의 제목 페이지나 문서 맨 위에 있는 7자리 또는 9자리 숫자입니다. 예를 들어, 본 설명서의 제목은 *Sun Java System Messaging Server 6 2005Q1 관리 설명서*이고 부품 번호는 819-1055입니다.

사용자 의견을 제출할 때 해당 양식에 영문 설명서의 제목과 부품 번호를 입력해야 할 수도 있습니다. 본 설명서의 영문 제목과 부품 번호는 *Sun Java System Messaging Server 2005Q1 Administration Guide(819-0105)*입니다.

사용자 의견 환영

# 사후 설치 작업 및 레이아웃

이 장의 내용은 *Sun Java System Messaging Server Deployment Planning Guide* (<http://docs.sun.com/doc/819-0063>)를 읽고 Sun Java™ Enterprise System 설치 프로그램을 사용하여 Messaging Server를 설치한 사용자를 대상으로 합니다. 다음 작업을 수행하여 Messaging Server 기능을 설정할 수 있습니다(*Sun Java Enterprise System 설치 설명서* (<http://docs.sun.com/doc/819-0809>) 참조). 사용자와 그룹을 준비 및/또는 마이그레이션 하고 배포를 사용자 정의할 수 있습니다. 사용자 정의는 이 설명서의 뒷 장들에 설명되어 있습니다. 준비는 *Sun Java System Communications Services Delegated Administrator 설명서* (<http://docs.sun.com/doc/819-1102>)에 설명되어 있습니다.

이 장은 다음 내용으로 구성되어 있습니다.

- 40페이지의 "UNIX 시스템 사용자와 그룹 만들기"
- 41페이지의 "Messaging Server 구성을 위해 Directory Server 준비"
- 51페이지의 "Messaging Server 초기 런타임 구성 만들기"
- 58페이지의 "Directory Server 복제본에 대해 Messaging Server 설치"
- 59페이지의 "Messaging Server 준비 도구 설치"
- 62페이지의 "SMTP 릴레이 차단"
- 64페이지의 "재부트 후 시작 활성화"
- 65페이지의 "sendmail 클라이언트 처리"
- 67페이지의 "Messenger Express 및 Communications Express 메일 필터 구성"
- 68페이지의 "성능 및 조정"
- 68페이지의 "사후 설치 디렉토리 레이아웃"

- 70페이지의 "사후 설치 포트 번호"

## UNIX 시스템 사용자와 그룹 만들기

시스템 사용자는 특정 서버 프로세스를 실행합니다. 사용자가 실행할 프로세스에 대한 적절한 권한을 갖도록 해당 사용자에게 권한을 부여해야 합니다.

모든 Sun Java System 서버에 대한 시스템 사용자 계정 및 그룹을 설정하고 해당 사용자가 소유한 디렉토리 및 파일에 대한 권한을 설정합니다. 그렇게 하려면 다음 단계를 수행합니다.

---

**주** 보안 상의 이유로 일부 배포에서는 서버마다 다른 시스템 관리자를 지정하는 것이 좋습니다. 이 작업은 서버마다 다른 시스템 사용자 및 그룹을 만들어 수행합니다. 예를 들어, Messaging Server의 시스템 사용자는 Web Server의 시스템 사용자와 다르고 Messaging Server 시스템 관리자는 Web Server를 관리할 수 없습니다.

---

1. 슈퍼유저로 로그인합니다.
2. 시스템 사용자가 속하게 될 그룹을 만듭니다. 다음 예에서는 mailsrv 그룹을 만듭니다.

```
# groupadd mail
```

3. 시스템 사용자를 만든 다음 방금 전에 만든 그룹과 연결합니다. 또한 해당 사용자의 비밀번호를 설정합니다. 다음 예에서는 mail 사용자를 만들고 이 사용자를 mailsrv 그룹과 연결합니다.

```
# useradd -g mail mailsrv
```

useradd 및 usermod 명령은 /usr/sbin에 있습니다. 자세한 내용은 UNIX 설명서 페이지를 참조하십시오.



4. 또한 `/etc/groups` 및 `/etc/passwd` 파일을 확인하여 앞서 만든 시스템 그룹에 사용자가 추가되었는지 확인합니다.

---

**주** Messaging Server를 설치하기 전에 UNIX 시스템 사용자와 그룹을 설정하지 않기로 한 경우에는 [51페이지의 "Messaging Server 초기 런타임 구성 만들기"](#)를 수행할 때 UNIX 시스템 사용자와 그룹을 지정할 수 있습니다.

---

## Messaging Server 구성을 위해 Directory Server 준비

이 절에서는 LDAP Directory Server가 Messaging Server, Calendar Server 또는 사용자 관리 유틸리티 구성과 함께 동작하도록 구성하는 Directory Server 설정 스크립트 (`comm_dssetup.pl`)를 실행하는 방법에 대해 설명합니다. `comm_dssetup.pl` 스크립트는 Directory Server에 새 스키마, 색인 및 구성 데이터를 설정하여 Directory Server를 준비합니다. 이 작업은 새 Messaging Server 및 Communications Express 설치에 대해 실행해야 합니다. Directory Server에 속한 구성 요소 제품 중 하나를 업그레이드하는 경우에는 최신 `comm_dssetup.pl`을 실행하는 것도 좋습니다.

이 절에서는 다음 항목에 대해 설명합니다.

- [41페이지의 "comm\\_dssetup.pl의 위치"](#)
- [42페이지의 "comm\\_dssetup.pl 요구 사항"](#)
- [43페이지의 "comm\\_dssetup.pl 스크립트 실행"](#)

### comm\_dssetup.pl의 위치

이전 버전의 Java Enterprise System에서 이 유틸리티는 Messaging Server 및 Calendar Server에 번들로 포함되어 있으며 별도로 설치할 필요가 없었습니다. 그러나 Java Enterprise System 2005Q1부터 이 스크립트는 별도로 설치 가능한 공유 구성 요소입니다.

`comm_dssetup.pl`을 설치하려면 다음 방법 중 하나를 선택합니다.

- Java Enterprise System 설치 프로그램을 사용할 경우 구성 요소 선택 패널에서 `comm_dssetup.pl`을 선택합니다. Directory Server를 선택하면 `comm_dssetup.pl`도 자동으로 선택됩니다.

- 이전 버전의 Java Enterprise System에서 업그레이드하는 중이며 Java Enterprise System 설치 프로그램을 사용하지 않는 경우 다음 패치를 다운로드합니다.

Solaris Sparc: 118245 및 118242

Solaris x86: 118256 및 118243

Linux: 118247만

설치된 comm\_dssetup.pl은 다음 디렉토리에서 찾을 수 있습니다.

Solaris: /opt/SUNWcomds/sbin

Linux: /opt/sun/comms/dssetup/sbin

## comm\_dssetup.pl 요구 사항

comm\_dssetup.pl 스크립트를 실행하기 전에 다음 요구 사항을 읽어보십시오.

- comm\_dssetup.pl 스크립트를 실행하기 전에 Directory Server를 설치하고 구성해야 합니다.
- 수퍼유저가 되어 comm\_dssetup.pl 스크립트를 실행합니다.
- Messaging Server, Calendar Server, Communications Express 또는 사용자 관리 유틸리티 초기 런타임 구성 프로그램을 실행하기 전에 comm\_dssetup.pl을 먼저 실행합니다.
  - 한 제품(예: Calendar Server)에 대해 Directory Server에서 comm\_dssetup.pl을 실행하는 경우 같은 Directory Server를 사용하는 다른 제품(예: Messaging Server)에 대해서는 해당 스크립트를 다시 실행하지 않아도 됩니다. comm\_dssetup을 실행할 때 제공한 답변 중 일부를 변경하는 경우 comm\_dssetup을 다시 실행해야 합니다. 예를 들어, commdirmig를 실행(Sun LDAP Schema 1에서 Sun LDAP Schema 2로 마이그레이션)했기 때문에 Messaging Server의 *다음* 구성에 대해 다른 사용자/그룹 접미어를 사용하기를 원할 수 있습니다.
- comm\_dssetup.pl 스크립트는 Directory Server 시스템에서 실행해야 합니다.
- comm\_dssetup.pl을 실행하기 전에 Directory Server가 실행 중인지 확인하십시오.
- Messaging Server의 새 버전을 설치할 때마다 Directory Server 시스템에서 comm\_dssetup.pl의 새 버전을 실행해야 합니다. 각 Messaging Server 배포에 새 스키마와 색인을 추가할 수 있습니다.

- 구성 데이터와 사용자 및 그룹 데이터가 별도의 디렉토리 인스턴스로 나누어지는 경우 두 인스턴스 모두에 `comm_dssetup` 스크립트를 실행해야 합니다.
- Unix 체제에서 버전 문제를 방지하려면 Directory Server와 함께 제공된 Perl 버전 (`dir_server_root/bin/slapd/admin/bin/perl`)을 사용합니다.
- `comm_dssetup.pl`을 원격 Directory Server에서 실행 중인 경우 다음을 수행합니다.
  - `dssetup.zip` 파일을 `msg_svr_base/install` 디렉토리에서 원격 Directory Server로 복사합니다. `/tmp` 또는 `/var/tmp` 등의 디렉토리에 복사할 수 있습니다. 모든 Directory Server 컴퓨터에 `comm_dssetup`을 설치하려는 게 아닐 때는 설치하는 대신 다른 Directory Server 컴퓨터에 `zip` 파일을 복사할 수 있습니다.
  - `dssetup.zip`, `comm_dssetup.pl` 및 필요한 스키마가 포함된 파일의 압축을 풉니다.
  - 원격 Directory Server에서 `comm_dssetup.pl` 스크립트를 실행합니다.
- 복제된 Directory Server를 실행하고 있는 경우 마스터 및 복제본 디렉토리에 대해 `comm_dssetup.pl` 스크립트를 실행해야 합니다.
- Messaging Server 구성을 위한 Directory Server를 준비하기 위해 Directory Server 설정 스크립트(`comm_dssetup.pl`)를 실행하는 경우 952페이지의 표 E-3에 설치 매개 변수를 기록하십시오. Messaging Server 초기 런타임 구성 시 이 매개 변수가 필요합니다.

## comm\_dssetup.pl 스크립트 실행

`comm_dssetup.pl`은 다음 모드 중 하나로 실행할 수 있습니다.

- 43페이지의 "대화식 모드"
- 49페이지의 "자동 설치 모드"

*Sun Java System Messaging Server Deployment Planning*

*Guide*(<http://docs.sun.com/doc/819-0063>)에 있는 설치 워크시트를 사용하여 답변을 기록합니다.

### 대화식 모드

인수 없이 `comm_dssetup.pl`을 지정하면 다음 질문이 표시됩니다.

## 1. 소개

```
# perl comm_dssetup.pl

Welcome to the Directory Server preparation tool for Java Enterprise
Communications Server.
(Version X.X Revision X.X)

This tool prepares your directory server for Sun Java System Messaging
Server install.

The logfile is /var/tmp/dssetup_YYYYMMDDHHSS

Do you want to continue [y]:
```

계속하려면 Enter 키를 누릅니다. 끝내려면 No를 입력합니다.

## 2. Directory Server의 설치 루트

```
Please enter the full path to the directory where the Java
Enterprise Directory Server was installed.

Directory server root [/var/opt/mps/serverroot]
```

Directory Server 시스템에서 Directory Server의 설치 루트 위치를 지정합니다. 이 Directory Server 루트 위치는 Linux의 경우와 다르다는 것에 주의하십시오.

## 3. Directory Server 인스턴스

```
Please select a directory server instance from the following
list:

[1]  slapd-varrius

Which instance do you want [1]:
```

시스템에 Directory Server의 인스턴스가 여러 개 있는 경우 Messaging Server와 함께 구성할 인스턴스를 선택합니다.

#### 4. Directory Manager 고유 이름(DN)

Please enter the directory manager DN [cn=Directory Manager]:  
 Password:

Directory Manager DN(cn=Directory Manager)은 조직 트리에서 사용자 및 그룹 데이터를 담당하는 관리자입니다. 이 스크립트에서 지정하는 Directory Manager DN은 Directory Server 설치 및 Messaging Server 설치에서 설정한 DN과 같아야 합니다.

#### 5. 사용자 및 그룹 Directory Server

Will this directory server be used for users/groups [Yes]:

Yes를 입력하면 사용자/그룹 트리에 관해 더 많은 질문이 제시됩니다.

No를 입력하면 이 디렉토리 인스턴스는 구성 데이터를 저장하는 데에만 사용되는 것으로 간주됩니다. 따라서 스키마 파일 업데이트에 대한 질문은 건너뛴니다. 구성 디렉토리 인스턴스에 대한 이 스크립트의 실행이 끝나면 설치 프로세스에서 다음 단계로 넘어가기 전에 사용자 및 그룹 데이터를 저장하는 디렉토리 인스턴스에 대해 이 스크립트를 실행해야 합니다.

#### 6. 사용자 및 그룹 기본 접미어

Please enter the Users/Groups base suffix [o=usergroup]:

사용자 및 그룹 기본 접미어는 사용자 및 그룹 항목에 대한 이름 공간이 들어 있는 조직 트리의 최상위 항목입니다. Directory Server 설치 및 Messaging Server 설치 도중 지정한 것과 동일한 사용자 및 그룹 기본 접미어를 선택해야 합니다.

**주** Access Manager를 설치한 경우 Access Manager 설치 시 지정한 접미어가 이 질문에 대해 지정한 것과 같아야 합니다. 같은 접미어를 사용하지 않으면 Messaging Server는 Access Manager 설치를 인식하지 못합니다.

조직 트리에 대한 자세한 내용은 *Sun Java Enterprise System 2003Q4 설치 설명서* (<http://docs.sun.com/source/817-4243-10/provisioning-concepts.html>)의 12장, Messaging Server 6.0에 대한 지정 및 스키마 개념을 참조하십시오.

## 7. 스키마 유형

```
There are 3 possible schema types:  
 1 - schema 1 for systems with iMS 5.x data  
 1.5 - schema 2 compatibility for systems with iMS 5.x data  
       that has been converted with commdirmig  
 2 - schema 2 native for systems using Access Manager
```

```
Please enter the Schema Type (1, 1.5, 2) [1]:
```

Sun LDAP Schema 1을 사용할 계획인 경우 옵션 1을 선택합니다.

Sun LDAP Schema 2, 호환 모드를 사용할 계획인 경우 옵션 1.5를 선택합니다. 자세한 내용은 *Sun Java System Communications Services Schema Migration Guide*를 참조하십시오.

Sun LDAP Schema 2, 기본 모드를 사용할 계획인 경우 옵션 2를 선택합니다.

Access Manager가 설치되어 있지 않은 경우 `comm_dssetup.pl`은 더 이상 종료되지 않습니다. 그 대신 Access Manager가 설치되어 있지 않음을 경고하고 Schema 2를 설치하도록 제공합니다. 경고 화면은 다음과 같습니다.

```
Please enter the Schema Type (1, 1.5, 2) [1]: 2  
  
Access Manager has not been configured for this new user/group suffix  
  
You can opt to continue, but you will not be able to use features that  
depend on Access Manager  
  
Are you sure you want this schema type? [n]:
```

스키마 옵션에 대한 자세한 내용은 *Sun Java System Messaging Server Deployment Planning Guide*(<http://docs.sun.com/doc/819-0063>)를 참조하십시오.

**8. 도메인 구성 요소(DC) 트리 기본 접미어**

```
Please enter the DC Tree base suffix [o=internet]:
```

**주**      **단계 7**에서 옵션 1 또는 1.5를 선택한 경우 DC 트리 기본 접미어를 지정해야 합니다. 옵션 2 - Sun ONE LDAP Schema 2 - 기본 모드를 선택한 경우에는 이 질문이 표시되지 않습니다.

DC 트리는 로컬 DNS 구조를 미리하며, 시스템에서 사용자 및 그룹 데이터 항목이 포함된 조직 트리에 대한 색인으로 사용됩니다. DC 트리 기본 접미어는 DC 트리의 최상위 항목의 이름입니다. 기본값인 o=internet이나 다른 이름을 선택할 수 있습니다.

DC 트리 또는 조직 트리에 대한 자세한 내용은 *Sun Java Enterprise System 2003Q4 설치 설명서*(<http://docs.sun.com/source/817-4243-10/provisioning-concepts.html>)의 12장, Messaging Server 6.0에 대한 지정 및 스키마 개념을 참조하십시오.

**9. 스키마 파일 업데이트**

```
Do you want to update the schema files [yes]:
```

Yes로 답하면 스키마에 새 요소가 추가됩니다. Messaging Server의 최신 버전을 설치할 때마다 디렉토리를 새 스키마 파일로 업데이트하는 것이 좋습니다.

**10. 새 색인 구성**

```
Do you want to configure new indexes [yes]:
```

**단계 5**(사용자 및 그룹 Directory Server)에서 Yes로 답한 경우 디렉토리 검색의 효율성을 향상시키기 위해 캐시를 만드는 데 사용되는 새 색인을 구성할 것인지 묻는 메시지가 나타납니다. 이 질문에 Yes로 답할 것을 권장합니다. 색인을 작성하지 않는 여러 가지 조건이 있습니다.

- 복제본에만 사용되는 마스터 사용자/그룹 Directory Server용인 경우 즉, 사용자/그룹 Directory Server에 대해 수행된 직접 쿼리가 없는 경우
- 색인을 만드는 동안 중단 시간이 많아지는 것을 원치 않는 많은 항목이 있는 작업 사용자/그룹 Directory Server를 소유한 경우

## 11. 설정 요약

```
Here is a summary of the settings that you chose:
Server Root                : /var/opt/mps/serverroot/
Server Instance            : slapd-varrius
Users/Groups Directory    : Yes
Update Schema              : yes
Schema Type                : 1
DC Root                    : o=internet
User/Group Root           : o=usergroup
Add New Indexes            : yes
Directory Manager DN      : cn=Directory Manager

Now ready to generate a shell script and ldif file to modify the
Directory.
No changes to the Directory Server will be made this time.

Do you want to continue [y]:
```

디렉토리 구성이 업데이트되기 전에 설정 요약 화면이 표시됩니다. 이번에는 변경이 수행되지 않습니다.

---

**주**            단계 7에서 옵션 2: Sun LDAP Schema 2 - 기본 모드를 선택한 경우 설정 요약의 DC 루트가 사용자/그룹 루트에 입력한 값과 동일합니다.

---

설정을 변경하려면 No를 입력하고 스크립트를 다시 실행합니다.

Yes를 입력하여 계속하면, comm\_dssetup.pl 스크립트는 Directory Server의 색인과 스키마를 업데이트하는 데 사용되는 LDIF 파일과 셸 스크립트를 만듭니다.

```
/var/tmp/dssetup_YYYYMMDDHHMMSS.sh
/var/tmp/dssetup_YYYYMMDDHHMMSS.ldif
```



여기서 YYYYMMDDHHMMSS는 파일이 생성된 시간과 날짜를 나타냅니다.

---

**주** 스크립트는 지금 실행하거나 나중에 실행할 수 있습니다. 스크립트를 지금 실행하려면 계속할 것인지 묻는 메시지에 Yes를 입력합니다. 스크립트를 나중에 실행하려면 /var/tmp/dssetup\_YYYYMMDDHHMMSS.sh를 사용하여 스크립트를 나중에 호출할 수 있습니다.

---

## 자동 설치 모드

자동 설치 모드를 활성화하려면 모든 인수를 한 번에 지정하십시오.

### 구문

```
# perl comm_dssetup.pl -i yes|no -c Directory_Server_Root -d
Directory_instance -r DC_tree -u User_Group_suffix -s yes|no -D
"DirectoryManagerDN" -w password -b yes|no -t 1|1.5|2 -m yes|no [-S
path-to-schema-files]
```

### 옵션

이 명령의 옵션은 다음과 같습니다.

옵션	설명
-i yes no	다음 질문에 답하십시오. "Do you want to configure new indexes?" 새 색인을 구성하려면 yes를 지정합니다. 새 색인을 지정하지 않으려면 no를 지정합니다.
-c Directory_Server_Root	Directory Server 루트 경로 이름 예: /var/opt/mps/serverroot
-d Directory_instance	Directory Server 인스턴스 하위 디렉토리 예: slapd-budgie
-r DC_tree	DC 트리 접미어(예: o=internet)
-u User_Group_suffix	사용자/그룹 접미어(예: o=usergroup)
-s yes no	다음 질문에 답하십시오. "Do you want to update the schema?" 스키마 파일을 업데이트하려면 yes를 지정합니다. 스키마 파일을 업데이트하지 않으려면 no를 지정합니다.
-D DirectoryManagerDN	Directory Manager DN(예: "cn=Directory Manager")

옵션	설명
<code>-w password</code>	Directory Manager 비밀번호
<code>-b yes no</code>	다음 질문에 답하십시오. "Will this directory server be used for users and groups?" Directory Server를 구성 및 사용자/그룹에 사용하려면 <code>yes</code> 를 지정합니다. 디렉토리를 구성 데이터에만 사용하려면 <code>no</code> 를 지정합니다.
<code>-t 1 1.5 2</code>	Messaging Server에 사용할 스키마 버전을 결정합니다. <ul style="list-style-type: none"> <li>• Sun LDAP Schema 1의 경우 1을 선택합니다.</li> <li>• Sun LDAP Schema 2(호환 모드)의 경우 1.5를 선택합니다. 자세한 내용은 <i>Sun Java System Communications Services Schema Migration Guide</i>를 참조하십시오.</li> <li>• Sun LDAP Schema 2(기본 모드)의 경우 2를 선택합니다.</li> </ul>
<code>m yes no</code>	다음 질문에 답하십시오. "Do you want to modify the directory server?" 디렉토리를 수정하려면 <code>yes</code> 를 지정합니다. 디렉토리를 수정하지 않으려면 <code>no</code> 를 지정합니다.
<code>-R &lt;yes no&gt;</code>	새 색인을 찾고 <code>-m yes</code> 가 제공되면 다시 색인화를 실행합니다.
<code>-S path-to-schema-files</code>	스키마 파일에 대한 디렉토리 경로를 지정합니다(예: <code>./schema</code> ).

#### 예

```
# perl comm_dssetup.pl -i yes -c /var/opt/mps/serverroot -d
slapd-budgie
-r o=internet -u o=usergroup -s yes -D "cn=Directory Manager" -w
password -b yes -t 1 -m yes
```

comm\_dssetup.pl 스크립트의 모든 옵션을 설정하고 나면 스크립트가 실제로 실행되기 전에 다음과 같은 요약 화면이 나타납니다.

```
Here is a summary of the settings that you chose:
Server Root                : /var/opt/mps/serverroot/
Server Instance            : slapd-budgie
Users/Groups Directory    : Yes
Update Schema              : yes
Schema Type                : 1
DC Root                    : o=internet
User/Group Root           : o=usergroup
Add New Indexes           : yes
Schema Directory          : ./schema
Directory Manager DN      : "cn=Directory Manager"
```

각 옵션에 대한 자세한 내용은 43페이지의 "대화식 모드" 절을 참조하십시오.

## Messaging Server 초기 런타임 구성 만들기

초기 런타임 구성 프로그램은 Messaging Server를 설정하고 실행하는 데 필요한 구성을 제공합니다. 즉, 기능적 messaging server 구성을 설정하도록 초기 런타임 구성을 만듭니다. 그렇게 하면 특정 사용자 정의를 만들 수 있는 기본 작업 구성이 제공됩니다. 이 프로그램은 한 번만 실행하면 됩니다. 이후에 이 프로그램을 또 실행하면 기존 구성을 덮어씁니다. 초기 런타임 구성을 수정하려면 이 설명서와 *Sun Java System Messaging Server Administration Reference*(<http://docs.sun.com/doc/819-0106>)에 설명되어 있는 구성 유틸리티를 사용하십시오.

## Messaging Server 전제 조건

초기 런타임 구성 프로그램을 실행하기 전에 다음을 수행해야 합니다.

- Administration Server를 설치 및 구성합니다. *Sun Java Enterprise System 설치 설명서*(<http://docs.sun.com/doc/819-0809>)를 참조하십시오. 관리 서버를 구성하지 않아도 Messaging Server를 구성할 수는 있지만 그 Messaging Server를 관리하는 콘솔은 사용할 수 없습니다.

- Directory Server를 설치 및 구성합니다. *Sun Java Enterprise System 설치 설명서*를 참조하십시오.
- comm\_dssetup.pl 프로그램을 실행합니다. 41페이지의 "Messaging Server 구성을 위해 Directory Server 준비"를 참조하십시오.
- 부록 E, "설치 워크시트"에 제공된 확인 목록에 Administration 및 Directory 설치 및 구성 매개 변수를 기록합니다.

## Messaging Server 구성 확인 목록

Messaging Server 초기 런타임 구성 프로그램을 실행하는 경우 설치 매개 변수를 954페이지의 표 E-4에 기록하십시오. 특정 질문에 답하려면 *Messaging Server Deployment Planning Guide*의 Directory 및 Administration Server 설치 확인 목록을 참조하십시오.

## 구성 프로그램 실행

다음은 Messaging Server 초기 런타임 구성을 구성하는 단계입니다.

1. 다음 명령으로 Messaging Server 초기 런타임 구성을 호출합니다.

```
/msg_svr_base/sbin/configure [flag]
```

원격 시스템에서 Messaging Server를 구성하는 경우 xhost(1) 명령을 사용할 수 있습니다.

표 1-1에서는 configure 프로그램에 설정할 수 있는 선택적 플래그에 대해 설명합니다.

**표 1-1** Messaging Server 구성 프로그램의 옵션 플래그

플래그	설명
-nodisplay	명령줄 구성 프로그램을 실행합니다.
-noconsole	GUI 사용자 인터페이스 프로그램을 실행합니다.
-state [statefile]	자동 설치 파일을 사용합니다. -nodisplay 및 -noconsole 플래그와 함께 사용해야 합니다. <a href="#">자동 설치 수행</a> 을 참조하십시오.

configure 명령을 실행하면 구성 프로그램이 시작됩니다.

**2.** 시작합니다.

구성 프로그램의 첫 번째 패널은 저작권 페이지입니다. 다음을 선택하여 계속하거나 취소를 눌러 종료합니다. 경고를 받도록 관리 서버를 구성하지 않은 경우에는 확인을 눌러 계속합니다.

**3.** 정규화된 호스트 이름(FQHN)을 입력합니다.

이 시스템에서 Messaging Server가 작동합니다. Java Enterprise System 설치 프로그램을 사용하여 서버를 설치했을 때는 실제 호스트 이름을 지정했을 수 있습니다. 그러나 클러스터 환경을 설치하는 중이면 논리 호스트 이름을 사용할 수 있습니다. 여기에서 원래 지정한 이름을 변경할 수 있습니다.

**4.** 구성 및 데이터 파일을 저장할 디렉토리를 선택합니다.

Messaging Server 구성 및 데이터 파일을 저장할 디렉토리 `msg_svr_base`에 없는 경로 이름을 지정하십시오. 심볼릭 링크가 구성 및 데이터 디렉토리의 `msg_svr_base`에 생성됩니다. 이러한 심볼릭 링크에 대한 자세한 내용은 [68페이지의 "사후 설치 디렉토리 레이아웃"](#)을 참조하십시오.

이러한 파일을 저장할 충분한 디스크 공간이 있는지 확인합니다.

**5.** 구성 요소를 로드하고 있음을 나타내는 작은 창이 표시됩니다.

몇 분 정도 소요됩니다.

**6.** 구성할 구성 요소를 선택합니다.

구성할 Messaging 구성 요소를 선택합니다.

- **Message Transfer Agent:** 라우팅을 처리하고, 사용자 메일을 전송하고, SMTP 인증을 처리합니다. MTA는 호스트된 도메인, 도메인 별칭 및 서버측 필터에 대한 지원을 제공합니다.
- **메시지 저장소:** 공용 메시지 저장소를 통해 통합된 메시징 서비스를 위한 기반을 제공합니다. 여러 프로토콜(HTTP, POP, IMAP)을 통해 메시지 저장소에 액세스할 수 있습니다. 메시지 저장소만 구성하는 경우에는 MTA도 선택해야 합니다.
- **Messenger Express:** HTTP 프로토콜이 메시지 저장소의 메일을 검색하는 작업을 처리합니다. Messenger Express만 구성하고 있는 경우 메시지 저장소와 MTA도 선택해야 합니다.

- **Messaging Multiplexor:** 조직 내의 여러 메시징 서버 시스템에 대한 프록시 역할을 합니다. 사용자는 각 연결을 적절한 메일 서버로 리디렉션하는 멀티플렉서 (**Multiplexor**) 서버에 연결합니다. 이 구성 요소는 기본적으로 활성화되지 않습니다. MMP와 메시지 저장소를 선택하면 같은 시스템에서 활성화됩니다. 따라서 구성 후 포트 번호를 변경하라는 경고 메시지가 나타납니다. 변경 방법에 대해서는 **70페이지의 "사후 설치 포트 번호"**를 참조하십시오.

MMP를 구성하려면 **7장, "멀티플렉서 서비스 구성 및 관리"** 및 *Sun Java System Messaging Server Administration Reference*(<http://docs.sun.com/doc/819-0106>)를 참조하십시오.

구성할 구성 요소를 선택하고 구성하지 않을 구성 요소의 선택을 취소합니다.

7. 구성된 파일을 소유할 사용자 아이디와 그룹을 입력합니다.

시스템 사용자와 그룹 설정에 대한 자세한 내용은 **40페이지의 "UNIX 시스템 사용자와 그룹 만들기"**를 참조하십시오.

8. Configuration Directory Server 패널

Configuration Directory LDAP URL, 관리자 및 비밀번호를 Administration Server 구성에서 가져와서 입력합니다.

Directory Server 설치에서 구성 서버 LDAP URL을 수집합니다. *Messaging Server Deployment Planning Guide*(<http://docs.sun.com/doc/819-0063/>)에서 Directory Server 설치 워크시트를 참조하십시오.

Directory Manager는 Directory Server 및 이를 활용하는 Sun Java System 서버(예: Messaging Server)에 대해 전반적인 관리자 권한이 있습니다. 또 Directory Server의 모든 항목에 대한 전체 관리 액세스 권한도 있습니다. 기본 및 권장 고유 이름(DN)은 cn=Directory Manager이고 Directory Server 구성 중에 설정됩니다.

---

**주** 기본값이 아닌 다른 값을 선택하면 Administration Server와 구성 Directory Server 사이의 불일치가 발생합니다. 이렇게 되면 사후 구성 단계를 수동으로 수행해야 합니다. 그러므로 확실히 다른 값이 필요한 지 파악한 경우에만 이 항목을 수정하시기 바랍니다.

---

## 9. 사용자/그룹 Directory Server 패널

사용자 및 그룹 디렉토리 LDAP URL, 관리자 및 비밀번호를 입력합니다.

호스트에서 사용자/그룹 서버 LDAP URL 정보를 얻고 Directory Server 설치에서 포트 번호 정보를 얻습니다. *Messaging Server Deployment Planning Guide* (<http://docs.sun.com/doc/819-0063/>)에서 Directory Server 설치 워크시트를 참조하십시오.

Directory Manager는 Directory Server 및 Directory Server를 사용하는 모든 Sun Java System 서버(예: Messaging Server)에 대해 전체적인 관리자 권한을 가지며 Directory Server의 모든 항목에 대해 완전한 관리 액세스 권한을 가집니다. 기본 및 권한 고유 이름(DN)은 cn=Directory Manager이고 Directory Server 구성 중에 설정됩니다.

복제된 Directory Server 인스턴스에 대해 설치를 하는 경우 마스터 디렉토리가 아니라 복제본의 자격 증명을 지정해야 합니다.

## 10. 포스트마스터 전자 메일 주소

포스트마스터 전자 메일 주소를 입력합니다.

관리자가 주로 모니터링할 주소를 선택합니다. 예를 들어, siroe 도메인의 포스트마스터의 경우 pma@siroe.com을 입력합니다. 이 주소의 첫 부분은 "Postmaster"가 될 수 없습니다.

전자 메일 주소의 사용자는 자동으로 생성되지 않습니다. 따라서 준비 도구를 사용하여 직접 만들어야 합니다.

## 11. 관리자 계정의 비밀번호

서비스 관리자, 서버, 사용자/그룹 관리자, 최종 사용자 관리자 권한 및 PAB 관리자와 SSL 비밀번호에 사용될 초기 비밀번호를 입력합니다.

초기 런타임 구성 후 개별 관리자 계정에 대해 이 비밀번호를 변경할 수 있습니다. 자세한 내용은 104페이지의 "비밀번호 수정"을 참조하십시오.

## 12. 기본 전자 메일 도메인

기본 전자 메일 도메인을 입력합니다.

이 전자 메일 도메인은 다른 도메인이 지정되지 않은 경우 사용되는 기본값입니다. 예를 들어, `siroe.com`이 기본 전자 메일 도메인인 경우 도메인 없이 사용자 아이디로 주소 지정된 메일을 보낼 도메인입니다.

Sun LDAP Schema, v.2에 대한 사용자 및 그룹을 준비하기 위한 명령줄 인터페이스인 사용자 관리 유틸리티를 사용하는 경우에는 구성 과정에서 동일한 기본 도메인을 지정합니다. 자세한 내용은 *Sun Java System Communications Services Delegated Administrator 설명서*(<http://docs.sun.com/doc/819-1102>)를 참조하십시오.

## 13. 조직 DN

사용자 및 그룹을 만들 조직 DN을 입력합니다. 기본값은 사용자/그룹 접미어 앞에 놓인 전자 메일 도메인입니다.

예를 들어, 사용자/그룹 접미어가 `o=usergroup`이고 전자 메일 도메인이 `siroe.com`인 경우 기본값은 `o=siroe.com`, `o=usergroup`입니다. 여기서 `o=usergroup`은 41페이지의 "Messaging Server 구성을 위해 Directory Server 준비"에서 지정한 사용자/그룹 디렉토리 접미어입니다.

같은 사용자/그룹 디렉토리 접미어를 조직 DN으로 선택하면 호스트된 도메인을 만들려고 할 때 마이그레이션 문제가 발생할 수 있습니다. 초기 런타임 구성 도중 호스트된 도메인을 설정하려면 사용자/그룹 접미어의 한 수준 아래에 DN을 지정하십시오.

## 14. 구성 준비 완료

구성 프로그램이 시스템의 디스크 공간이 충분한지 확인한 다음 구성할 준비가 된 구성 요소를 개괄적으로 표시합니다.

Messaging 구성 요소를 구성하려면 지금 구성을 선택합니다. 구성 변수를 변경하려면 뒤로를 선택합니다. 구성 프로그램을 종료하려면 취소를 선택합니다.



## 15. 작업 시퀀스 시작, 시퀀스 완료 및 설치 요약 패널

최종 설치 요약 페이지에서 세부 정보를 선택하면 설치 상태를 볼 수 있습니다. 프로그램을 종료하려면 닫기를 선택합니다.

로그 파일이 `/msg_svr_base/install/configure_YYYYMMDDHHMMSS.log`에 생성되며, 여기서 `YYYYMMDDHHMMSS`는 구성의 4자리 연도, 월, 일, 시, 분 및 초입니다.

이제 Messaging Server에 대한 초기 런타임 구성이 설정되었습니다. 구성 매개 변수를 변경하려면 이 설명서의 해당 부분을 참조하십시오.

Messaging Server를 시작하려면 다음 명령을 사용합니다.

```
/opt/SUNWmsgsr/sbin/start-msg
```

## 자동 설치 수행

Messaging Server 초기 런타임 구성 프로그램은 자동 설치 `state` 파일(`saveState`)을 자동으로 만듭니다. 이 파일을 사용하여 Messaging Server Solaris 패키지가 설치된 배포 환경에 추가 Messaging Server 인스턴스를 빠르게 구성할 수 있습니다. 구성 질문에 대한 사용자의 모든 응답이 이 파일에 기록되어 있습니다.

자동 설치를 실행하면 `configure` 프로그램은 자동 설치 `state` 파일을 읽습니다.

`configure` 프로그램은 Messaging Server의 이후 초기 런타임 구성에 대해 같은 설치 질문을 반복하는 것이 아니라 이 파일의 응답을 읽습니다. 새 설치에 `state` 파일을 사용하면 질문이 나타나지 않습니다. 대신 `state` 파일의 모든 응답이 새 설치 매개 변수로 자동으로 제공됩니다.

자동 설치 `saveState state` 파일은

`/msg_svr_base/install/configure_YYYYMMDDHHMMSS` 디렉토리에 저장되어 있으며 여기서 `YYYYMMDDHHMMSS`는 `saveState` 파일의 4자리 연도, 월, 일, 시, 분, 초를 나타냅니다.

자동 설치 `state` 파일을 사용하여 배포 환경 내 다른 시스템에 다른 Messaging Server 인스턴스를 구성하려면 다음 단계를 수행합니다.

1. 자동 설치 `state` 파일을 새 설치를 수행하고 있는 시스템의 임시 영역에 복사합니다.

2. 필요에 따라 자동 설치 *state* 파일을 검토하고 편집합니다.

*state* 파일의 일부 매개 변수와 지정 내용을 변경해야 할 수 있습니다. 예를 들어 새 설치의 기본 전자 메일 도메인은 *state* 파일에 기록된 기본 전자 메일 도메인과 다를 수 있습니다. *state* 파일에 나열된 매개 변수는 이 설치에 자동으로 적용된다는 점에 유의하십시오.

3. 다음 명령을 실행하여 자동 설치 파일로 다른 시스템을 구성합니다.

```
msg_svr_base/sbin/configure -nodisplay -noconsole -state \  
    fullpath/saveState
```

여기서 *fullpath*는 *saveState* 파일이 있는 전체 디렉토리 경로입니다. 이 절의 [단계 1](#)을 참조하십시오.

---

주

자동 설치 프로그램을 실행하면

```
msg_svr_base/install/configure_YYYYMMDDHHMMSS/saveState
```

디렉토리 위치에 새 *state* 파일이 생성됩니다. 여기서 YYYYMMDDHHMMSS는 /*saveState* 파일의 4자리 연도, 월, 일, 시, 분, 초입니다.

---

## Directory Server 복제본에 대해 Messaging Server 설치

다음과 같은 제한 사항으로 인해 Directory Server 복제본에 대해 Messaging Server를 설치하지 못할 수 있습니다.

- Directory Server 마스터 자격 증명이 없는 경우
- Messaging Server가 Directory Server 마스터와 직접 통신할 수 없는 경우

Messaging Server를 Directory Server 복제본에 대해 설치하려면 다음 단계를 수행합니다.

1. [42페이지의 "comm\\_dssetup.pl 요구 사항"](#)에서 설명하는 대로 Directory Server 복제본을 포함한 모든 Directory Server에 대해 *comm\_dssetup.pl* 프로그램을 실행합니다.

2. **Messaging Server 초기 런타임 구성 만들기**의 단계 8 및 단계 9에서 설명하는 대로 복제된 Directory Server 자격 증명을 사용하여 Messaging configure 프로그램 (`msg_svr_base/sbin/configure`에 있음)을 실행합니다.

잘못된 권한 때문에 configure 프로그램은 Directory Server 관리자를 구성하는 시도에 실패하게 됩니다. 하지만 Directory Server 복제본에 올바른 권한을 허용하는 데 필요한 `msg_svr_base/config/*.ldif` 파일이 생성됩니다.

3. \*.ldif 파일을 Directory Server 마스터로 옮깁니다.
4. \*.ldif 파일에 대해 `ldapmodify` 명령을 실행합니다.

`ldapmodify` 또는 `msg_svr_base/install/configure_YYYYMMDDHHMMSS.log`에 대한 자세한 내용은 Sun Java System Directory Server 설명서를 참조하십시오.

5. configure 프로그램을 다시 실행합니다.

이제 Directory Server 복제본(및 마스터)이 Messaging Server와 함께 사용할 수 있도록 구성되었습니다.

## Messaging Server 준비 도구 설치

다음 절에서는 지원되는 준비 도구에 대한 설치 정보를 요약하여 설명합니다.

- 59페이지의 "메시징용 Delegated Administrator"
- 61페이지의 "LDAP 준비 도구"
- 40페이지의 "UNIX 시스템 사용자와 그룹 만들기"

## 메시징용 Delegated Administrator

Messaging Server에 사용할 수 있는 GUI 준비 도구는 두 가지로서 iPlanet Delegated Administrator(Sun LDAP Schema 1)와 Communications Services Delegated Administrator(Sun LDAP Schema 2)입니다. 이 절에서는 iPlanet Delegated Administrator(Sun LDAP Schema 1)에 대해 설명합니다. Communications Services Delegated Administrator(Sun LDAP Schema 2)에 대한 자세한 내용은 *Sun Java System Communications Services Delegated Administrator 설명서* (<http://docs.sun.com/doc/819-1102>)를 참조하십시오.

iPlanet Delegated Administrator(Sun LDAP Schema 1)를 설치하려면 Sun Software 페이지에서 다운로드해야 합니다. 다운로드 위치 정보에 대해서는 Sun Java System 담당자에게 문의하십시오.

---

**주** iPlanet Delegated Administrator는 Messaging Server와 Web Server를 설치 및 구성한 후에만 설치할 수 있습니다. iPlanet Delegated Administrator 설치에 대한 자세한 내용은 iPlanet Delegated Administrator 설명서를 참조하십시오.

iPlanet Delegated Administrator는 기존 Messaging Server 5.x를 설치했고 현재 Messaging Server 6을 설치 중인 고객만 사용할 수 있습니다. Messaging Server 제품을 새로 구입하는 고객은 사용할 수 없습니다.

iPlanet Delegated Administrator는 Sun Java System Web Server 6.0(이전 Messaging Server 5.2에서만 번들로 포함됨)과 함께 사용해야 합니다. Web Server 6.1(Java Enterprise System 설치 프로그램에 포함됨)은 iPlanet Delegated Administrator와 함께 사용할 수 없습니다.

*Sun Java System Messaging Server 릴리스 노트*  
(<http://docs.sun.com/db/doc/819-1051>)를 읽어보십시오.

---

**설치 단계 요약:** Messaging Server를 사용하여 메시징용 iPlanet Delegated Administrator를 설치 및 구성하려면 다음을 수행합니다.

---

**주** 다음 제품을 설치할 때는 Java Enterprise System 설치 프로그램을 사용합니다. 이 제품 중 일부는 고유의 구성을 갖고 있지만 그 밖의 제품의 구성은 Java Enterprise System 설치/구성 프로그램에 포함되어 있습니다. 자세한 내용은 특정 제품 설명서를 참조하십시오.

---

1. Sun Java System 5.2가 설치 및 구성되어야 합니다.  
자세한 내용은 *Sun Java System Directory Server 설치 설명서*를 참조하십시오.
2. Messaging Server를 설치 및 구성합니다.  
Sun Java System Access Manager가 설치되지 않을 것이기 때문에 Messaging Server는 Sun LDAP Schema 1을 사용 중이라는 것을 감지합니다.

3. 이전 Messaging Server 5.2 번들에서 Sun Java System Web Server 6.0을 설치합니다.  
Sun Java System Web Server 설명서 및 Sun Java System Delegated Administrator 설명서를 참조하십시오.
4. 메시징용 iPlanet Delegated Administrator 1.2 Patch 2를 설치합니다. 최신 버전을 구하려면 Sun 기술 지원 담당자에게 문의하십시오.  
iPlanet Delegated Administrator 설명서를 참조하십시오.

## LDAP 준비 도구

Sun LDAP Schema 1 사용자 및 그룹은 LDAP Directory 도구를 사용하여 준비할 수 있습니다. Schema 2는 지원되지 않습니다.

### 설치 단계 요약:

1. Directory Server가 아직 설치되어 있지 않은 경우에는 해당 서버를 설치하고 구성해야 합니다.  
자세한 내용은 *Sun Java Enterprise System 설치 설명서* (<http://docs.sun.com/doc/819-0809>)를 참조하십시오.
2. Access Manager가 Directory Server의 데이터를 인식하도록 구성합니다.  
Access Manager가 LDAP 디렉토리의 데이터를 인식하도록하려면 Access Manager가 관리할 모든 조직, 그룹 및 사용자에 대한 항목에 특별한 객체 클래스를 추가해야 합니다. 아직 이렇게 하지 않은 경우 새 계정 준비를 시작하기 전에 먼저 이 작업을 수행하십시오. 이러한 객체 클래스를 디렉토리에 자동으로 추가하는 것을 돕기 위해 Access Manager 제품에는 샘플 스크립트가 포함되어 있습니다. 이러한 설치 사후 단계에 대한 자세한 내용은 *Sun Java System Access Manager Migration Guide*(<http://docs.sun.com/doc/819-7645>)를 참조하십시오.
3. 이 설명서의 지침에 따라 Messaging Server를 설치 및 구성합니다.  
Messaging Server는 Access Manager가 설치되어 있는지 여부에 따라 현재 사용 중인 Sun Java System LDAP Schema를 식별합니다.
4. Messenger Express의 메일 필터링을 활성화하려면 Sun Java System Web Server 6.1을 설치 및 구성하십시오. 메일 필터링 활성화에 대한 자세한 내용은 [67페이지](#)의 "Messenger Express 및 Communications Express 메일 필터 구성"을 참조하십시오. Web Server를 설치하려면 *Sun Java Enterprise System 설치 설명서*를 참조하십시오.  
메일 필터링은 준비 도구는 아니지만 그 기능은 메시징용 Delegated Administrator의 이전 GUI 버전에 포함되어 있습니다.

5. Sun Java System Messaging Server 설명서를 참조하여 LDAP 준비를 수행합니다.

Sun LDAP Schema 1 LDAP 준비에 대해서는 *Messaging Server 5.2 Provisioning Guide* 및 *Sun Java System Communications Services Schema Reference Manual*을 참조하십시오. (*Sun Java System Schema Reference Manual*에는 Sun LDAP Schema 1 및 v.2에 대한 개체 클래스와 속성이 있습니다.)

## SMTP 릴레이 차단

기본적으로 Messaging Server는 SMTP 릴레이 시도를 차단하도록 구성되어 있습니다. 즉, 인증되지 않은 외부 소스의 외부 주소로의 메일 전송 시도를 거부합니다. 외부 시스템이란 서버가 있는 호스트가 아닌 다른 모든 시스템을 말합니다. 이 기본 구성은 다른 모든 시스템을 외부 시스템으로 간주하기 때문에 과도하게 SMTP 릴레이를 차단합니다.

설치한 뒤에는 사이트의 필요에 맞게 구성을 수동으로 수정하는 것이 중요합니다. 특히 Messaging Server가 SMTP 릴레이를 항상 허용해야 하는 자체 내부 시스템과 서브넷을 인식해야 합니다. 이 구성을 업데이트하지 않으면 MTA 구성을 테스트할 때 문제가 발생할 수 있습니다.

Messaging Server 시스템의 SMTP 서버를 통해 외부 주소로 지정된 메일을 전송하려고 시도하는 IMAP 및 POP 클라이언트, 그리고 SMTP AUTH(SASL)를 사용하여 인증하지 않는 클라이언트의 전송 시도는 거부됩니다. 내부로 인식되는 시스템 및 서브넷은 `msg_svr_base/config/mappings` 파일에 포함되어 있는 INTERNAL\_IP 매핑 테이블을 통해 제어됩니다.

예를 들어, IP 주소가 192.45.67.89인 Messaging Server 시스템의 경우 기본 INTERNAL\_IP 매핑 테이블은 다음과 같습니다.

```
INTERNAL_IP

$(192.45.67.89/24)  $Y
127.0.0.1  $Y
*  $N
```

첫 번째 항목은 \$(IP-pattern/significant-prefix-bits) 구문을 사용하여 192.45.67.89의 24비트와 완전히 일치하는 모든 IP 주소를 내부로 인식하도록 지정합니다. 두 번째 항목은 루프백 IP 주소 127.0.0.1을 내부로 인식합니다. 마지막 항목은 다른 모든 IP 주소가 내부로 인식되지 않도록 지정합니다.

마지막 \$N 항목 앞에 추가 IP 주소 또는 서브넷을 지정하여 항목을 추가할 수 있습니다. 이러한 항목은 왼쪽에 IP 주소나 서브넷(\$.../...) 구문을 사용하여 서브넷 지정)을 지정하고 오른쪽에 \$Y를 지정합니다. 또는 기존 \$(.../...) 항목을 수정하여 더 일반적인 서브넷을 허용할 수 있습니다.

예를 들어, 동일한 샘플 사이트의 네트워크가 클래스 C 네트워크, 즉 192.45.67.0 서브넷을 모두 소유하는 네트워크인 경우 해당 사이트에서는 첫 번째 항목을 수정하여 매핑 테이블이 다음과 같도록 해야 합니다.

```
INTERNAL_IP

$(192.45.67.89/24) $Y
127.0.0.1 $Y
* $N
```

또는 사이트가 192.45.67.80-192.45.67.99 범위 내의 IP 주소만 소유하는 경우 해당 사이트에서는 다음과 같은 매핑 테이블을 사용할 수 있습니다.

```
INTERNAL_IP

! Match IP addresses in the range 192.45.67.80-192.45.67.95
$(192.45.67.80/28) $Y
! Match IP addresses in the range 192.45.67.96-192.45.67.99
$(192.45.67.96/30) $Y
127.0.0.1 $Y
* $N
```

`msg_svr_base/sbin/imsimta test -match` 유틸리티는 IP 주소가 특정 \$(.../...) 테스트 조건에 일치하는지 여부를 검사할 때 유용하게 사용할 수 있습니다. `imsimta test -mapping` 유틸리티는 INTERNAL\_IP 매핑 테이블이 다양한 IP 주소 입력에 대해 원하는 결과를 반환하는지 검사할 때 매우 유용합니다.

INTERNAL\_IP 매핑 테이블을 수정한 뒤에는 `msg_svr_base/sbin/imsimta cnbuild` 및 `msg_svr_base/sbin/imsimta restart` 유틸리티를 실행해야 변경 사항이 적용됩니다.

매핑 파일 및 일반 매핑 테이블 형식과 `imsimta` 명령줄 유틸리티에 대한 자세한 내용은 *Sun Java System Messaging Server Administration*

*Reference*(<http://docs.sun.com/doc/819-0106>)를 참조하십시오. INTERNAL\_IP 매핑 테이블에 대한 자세한 내용은 528페이지의 "SMTP 릴레이 추가"를 참조하십시오.

## 재부트 후 시작 활성화

부트 스크립트인 `msg_svr_base/lib/Sun_MsgSvr`을 사용하여 시스템 재부트 후에 Messaging Server 시작을 활성화할 수 있습니다. 기본적으로 Messaging Server는 이 스크립트를 실행하지 않기 때문에 시스템 재부트 후에 다시 시작되지 않습니다. 또한 이 스크립트는 사용되었을 때 MMP에서 시작합니다.

`Sun_MsgSvr`을 활성화하려면 다음을 수행합니다.

1. `Sun_MsgSvr` 스크립트를 `/etc/init.d` 디렉토리에 복사합니다.
2. `Sun_MsgSvr` 스크립트에 대한 다음 소유권 및 액세스 모드를 변경합니다.

**표 1-2** `Sun_MsgSvr`의 소유권 및 액세스 모드 변경

소유권(chown(1M))	그룹 소유권(chgrp(1M))	액세스 모드(chmod(1M))
root(수퍼유저)	sys	0744

3. `/etc/init.d/rc0.d` 디렉토리로 이동하여 다음과 같은 링크를 만듭니다.

```
ln /etc/init.d/Sun_MsgSvr S92Sun_MsgSvr
```

4. `/etc/rc0.d` 디렉토리로 이동하여 다음과 같은 링크를 만듭니다.

```
ln /etc/init.d/Sun_MsgSvr K08Sun_MsgSvr
```



# sendmail 클라이언트 처리

최종 사용자가 sendmail 클라이언트를 통해 메일을 보내는 경우 프로토콜을 통해 해당 클라이언트를 지원하도록 Messaging Server를 구성할 수 있습니다. 사용자는 UNIX sendmail 클라이언트를 계속 사용할 수 있습니다.

sendmail 클라이언트와 Messaging Server 사이에 호환성을 만들려면 sendmail 구성 파일을 만들어 수정하면 됩니다.

---

**주** 새 sendmail 패치가 시스템에 적용될 때마다 **Solaris 9 이상** 및 위에 대한 다음 지침의 설명에 따라 submit.cf 파일을 수정해야 합니다. Solaris 8의 경우에는 다음 지침을 따르십시오.

---

이전 버전의 Messaging Server를 업그레이드한 경우 /usr/lib/sendmail 이진 파일이 sendmail 제품의 구성 요소로 교체되었습니다. Messaging Server 6 2005Q1에서는 업그레이드 중에 이 대체가 발생하지 않습니다. 따라서, 최신 sendmail 패치로부터 적절한 /usr/lib/sendmail 이진 파일 버전을 구해야 합니다.

## Solaris 8

Solaris 8 운영 체제에서는 다음 단계를 수행합니다.

1. /usr/lib/mail/cf 디렉토리에서 main-v7sun.mc 파일을 찾아 이 파일의 복사본을 만듭니다.  
이 절의 예에서는 sunone-msg.mc라는 복사본을 만들었습니다.
2. sunone-msg.mc 파일에서 MAILER 매크로 앞에 다음 행을 추가합니다.

```
FEATURE('nullclient', 'smtp:rhino.west.sesta.com')dnl
MASQUERADE_AS('west.sesta.com')dnl
define('confDOMAIN_NAME', 'west.sesta.com')dnl
```

Messaging Server 초기 런타임 구성 만들기의 56페이지의 "기본 전자 메일 도메인"에서 설명하는 것처럼, 여기서 rhino.west.sesta.com은 localhost 이름이고 west.sesta.com은 기본 전자 메일 도메인입니다. HA 환경에서는 논리 호스트 이름을 사용합니다. 고가용성을 위한 논리 호스트 이름에 대한 자세한 내용은 3장, "고가용성 구성"을 참조하십시오.

3. sunone-msg.mc 파일을 컴파일합니다.

```
/usr/ccs/bin/make sunone-msg.cf
```

sunone-msg.mc는 sunone-msg.cf를 출력합니다.

4. /etc/mail 디렉토리에 있는 기존 sendmail.cf 파일의 백업 복사본을 만듭니다.
  - a. /usr/lib/mail/cf/sunone-msg.cf를 복사한 다음 해당 파일의 이름을 sendmail.cf로 변경합니다.
  - b. 새 sendmail.cf 파일을 /etc/mail 디렉토리로 이동합니다.

## Solaris 9 이상

Solaris 9 플랫폼에서는 sendmail은 setuid 프로그램이 아닌 setgid 프로그램입니다.

Solaris 9 플랫폼에서 sendmail 구성 파일을 만들려면 다음을 수행합니다.

1. /usr/lib/mail/cf 디렉토리에서 submit.mc 파일을 찾아 해당 파일의 복사본을 만듭니다.

이 절의 예에서는 sunone-submit.mc라는 복사본을 만들었습니다.

2. sunone-submit.mc 파일에서 다음 행을 변경합니다.

```
FEATURE('msp')dn
```

위 행을 다음과 같이 변경합니다.

```
FEATURE('msp', 'rhino.west.sesta.com')dn1
```

여기서 rhino.west.sesta.com은 localhost 이름입니다.

Messaging Server 초기 런타임 구성 만들기의 56페이지의 "기본 전자 메일 도메인"에서 설명하는 것처럼, 여기서 rhino.west.sesta.com은 localhost 이름이고 west.sesta.com은 기본 전자 메일 도메인입니다. HA 환경에서는 논리 호스트 이름을 사용합니다. 고가용성을 위한 논리 호스트 이름에 대한 자세한 내용은 3장, "고가용성 구성"을 참조하십시오.

3. sunone-submit.mc 파일을 컴파일합니다.

```
/usr/ccs/bin/make sunone-submit.cf
```

sunone-submit.mc는 sunone-submit.cf를 출력합니다.

4. /etc/mail 디렉토리에 있는 기존 submit.cf 파일의 백업 복사본을 만듭니다.
  - a. /usr/lib/mail/cf/sunone-submit.cf 파일을 복사한 다음 해당 파일의 이름을 submit.cf로 변경합니다.
  - b. 새 submit.cf 파일을 /etc/mail 디렉토리로 이동합니다.

## Messenger Express 및 Communications Express 메일 필터 구성

메일 필터는 Messenger Express 및 Communications Express를 통해 액세스할 수 있습니다. Communications Express만 사용할 때는 .war 파일을 배포할 필요가 없지만 Messenger Express 안의 메일 필터를 배포하려면 다음 명령을 실행해야 합니다.

*Web Server를 웹 컨테이너로 사용하는 경우:*

```
# cd web_srv_base/bin/https/httpadmin/bin/
# ./wdeploy deploy -u /MailFilter -i https-srvr_instance -v
https-virtual_srvr_instance msg_srv_base/SUNWmsgmf/MailFilter.war
```

*App Server를 웹 컨테이너로 사용하는 경우:*

```
# cd app_srv_base/sbin
# ./asadmin
asadmin> deploy --user admin msg_srv_base/SUNWmsgmf/MailFilter.war
```

두 경우 모두 다음 configutil 매개 변수를 설정하고 mshttpd를 다시 시작합니다.

```
# cd msg_svr_base/sbin/
# ./configutil -o "local.webmail.sieve.port" -v "WS_port_no|AS_port_no"
# ./stop-msg http
# ./start-msg http
```

Administration Console을 사용하여 .war 파일을 배포할 수도 있습니다. 자세한 내용은 *Sun Java System Web Server 6.1 관리자 설명서*(<http://docs.sun.com/app/doc/819-0825>) 또는 *Sun Java System Application Server Enterprise Edition 8.1 관리 설명서*(<http://docs.sun.com/doc/819-1552>)를 참조하십시오.

최종 사용자에게 대한 메일 필터 관련 정보는 Messenger Express 및 Communications Express 온라인 도움말 파일에서 볼 수 있습니다.

## 성능 및 조정

*Messaging Server Deployment Planning Guide*(<http://docs.sun.com/doc/819-0063>)에서 Messaging Server 구조에 대한 성능 고려 사항 관련 절을 참조하십시오.

## 사후 설치 디렉토리 레이아웃

Sun Java System Messaging Server를 설치하면 디렉토리 및 파일이 표 1-3에 설명된 구조 대로 정렬됩니다. 이 표에는 일반적인 서버 관리 작업에서 가장 많이 사용되는 디렉토리와 파일만 나열되어 있습니다.

**표 1-3**      사후 설치 디렉토리 및 파일

디렉토리	기본 위치 및 설명
Messaging Server 기본 ( <i>msg_svr_base</i> )	<p><code>/opt/SUNWmsgsr/</code> (기본 위치)</p> <p>서버 프로그램, 구성, 유지 관리 및 정보 파일을 저장하는 Messaging Server 시스템의 전용 디렉토리입니다.</p> <p>Messaging Server 기본 디렉토리는 시스템당 하나만 있을 수 있습니다.</p>

표 1-3 사후 설치 디렉토리 및 파일 (계속)

디렉토리	기본 위치 및 설명
구성 config	<p><i>msg_svr_base/config/</i></p> <p>imta.cnf 및 msg.conf와 같은 모든 Messaging Server 구성 파일이 포함되어 있습니다.</p> <p>Solaris 및 Linux 플랫폼의 경우: 이 디렉토리는 초기 런타임 구성에서 지정한 데이터 및 구성 디렉토리의 config 하위 디렉토리(기본값: <i>/var/opt/SUNWmsgsr/</i>)에 심볼릭 링크로 연결됩니다.</p>
로그 log	<p><i>msg_svr_base/log/</i></p> <p>mail.log_current와 같은 Messaging Server 로그 파일이 포함되어 있습니다.</p> <p>Solaris 및 Linux 플랫폼의 경우: 이 디렉토리는 초기 런타임 구성에서 지정한 데이터 및 구성 디렉토리의 log 하위 디렉토리(기본값: <i>/var/opt/SUNWmsgsr/</i>)에 심볼릭 링크로 연결됩니다(UNIX 플랫폼).</p>
데이터 data	<p><i>msg_svr_base/data/</i> (필수 위치)</p> <p>데이터베이스, 구성, 로그 파일, 사이트 프로그램, 대기열, 저장소 및 메일 파일이 포함되어 있습니다.</p> <p>data 디렉토리에는 config 및 log 디렉토리가 포함되어 있습니다.</p> <p>Solaris 및 Linux 플랫폼의 경우: 이 디렉토리는 초기 런타임 구성에서 지정한 데이터 및 구성 디렉토리(기본값: <i>/var/opt/SUNWmsgsr/</i>)에 심볼릭 링크로 연결됩니다(UNIX 플랫폼).</p>
시스템 관리자 프로그램 sbin	<p><i>msg_svr_base/sbin/</i> (필수 위치)</p> <p>imsimta, configutil, stop-msg, start-msg, uninstaller 등과 같은 Messaging Server 시스템 관리자 실행 프로그램 및 스크립트가 포함되어 있습니다.</p>
라이브러리 lib	<p><i>msg_svr_base/lib/</i> (필수 위치)</p> <p>공유 라이브러리, 개인 실행 프로그램과 스크립트, 데몬 및 사용자 정의가 불가능한 내용 데이터 파일이 포함되어 있습니다(예: imapd 및 qm_maint.hlp).</p>
SDK 포함 파일 include	<p><i>msg_svr_base/include/</i> (필수 위치)</p> <p>SDK(Software Development Kit)의 메시징 헤더 파일이 포함되어 있습니다.</p>
예 examples	<p><i>msg_svr_base/examples/</i> (필수 위치)</p> <p>Messenger Express AUTH SDK와 같은 다양한 SDK의 예가 포함되어 있습니다.</p>

**표 1-3** 사후 설치 디렉토리 및 파일 (계속)

디렉토리	기본 위치 및 설명
설치 데이터 install	<i>msg_svr_base/install/</i> (필수 위치)  설치 로그 파일, 자동 설치 파일, 기본 구성 파일 및 초기 런타임 구성 로그 파일 등과 같은 설치 관련 데이터 파일이 포함되어 있습니다.

## 사후 설치 포트 번호

설치 및 초기 런타임 구성 프로그램을 실행하는 도중 다양한 서비스에 대한 포트 번호를 선택하게 됩니다. 이러한 포트 번호는 1부터 65535 사이의 임의의 숫자일 수 있습니다.

표 1-4에는 설치 후 지정되는 포트 번호가 나열되어 있습니다.

**표 1-4** 설치 도중 지정되는 포트 번호

포트 번호	서비스(configutil 매개 변수)
389	Directory Server를 설치하는 시스템의 표준 Directory Server LDAP 포트. 이 포트는 Directory Server 설치 프로그램에 지정되었습니다( <i>local.ugldapport</i> ).
110	표준 POP3 포트. 이 포트는 같은 시스템에 설치될 때 MMP 포트와 충돌을 일으킬 수 있습니다( <i>service.pop.port</i> ).
143	표준 IMAP4 포트. 이 포트는 같은 시스템에 설치될 때 MMP 포트와 충돌을 일으킬 수 있습니다( <i>service.imap.port</i> ).
25	표준 SMTP 포트( <i>service.http.smtpport</i> )
80	Messenger Express HTTP 포트. 이 포트는 같은 시스템에 설치될 때 MMP 포트와 충돌을 일으킬 수 있습니다( <i>service.http.port</i> )
992	SSL에서의 POP3 포트. 암호화된 통신용( <i>service.pop.sslport</i> )
993	SSL에서의 IMAP 포트. 암호화된 통신용으로 이 포트는 같은 시스템에 설치될 때 MMP 포트와 충돌을 일으킬 수 있습니다( <i>service.imap.sslport</i> ).
443	SSL에서의 HTTP 포트. 암호화된 통신용( <i>service.http.sslport</i> )
7997	메시징 및 공동 작업 ENS(Event Notification Service) 포트
27442	내부 제품 통신을 위해 Job Controller에서 사용하는 포트

**표 1-4** 설치 도중 지정되는 포트 번호 (계속)

포트 번호	서비스(configutil 매개 변수)
49994	내부 제품 통신을 위해 Watcher에서 사용하는 포트. Watcher에 대한 자세한 내용은 <i>Sun Java System Messaging Server 관리 설명서</i> 를 참조하십시오 (local.watcher.port).
사용자 지정	Administration Server HTTP 포트(콘솔 요청 수신용)

같은 시스템에 여러 제품이 설치되어 있으면 포트 번호 충돌이 발생할 수 있습니다.

표 1-5는 잠재적인 포트 번호 충돌을 보여줍니다.

**표 1-5** 잠재적 포트 번호 충돌

충돌하는 포트 번호	포트	포트
143	IMAP 서버	MMP IMAP 프록시
110	POP3 서버	MMP POP3 프록시
993	IMAP over SSL	MMP IMAP 프록시(SSL 사용)
80	Web Server 포트	Messenger Express

가능한 한, 포트 번호가 충돌하는 제품은 별도의 시스템에 설치하는 것이 좋습니다. 그렇게 할 수 없는 경우에는 충돌하는 제품 중 하나의 포트 번호를 변경해야 합니다.

포트 번호를 변경하려면 configutil 유틸리티를 사용합니다. 전체 구문과 사용에 대해서는 *Sun Java System Messaging Server Administration Reference*(<http://docs.sun.com/doc/819-0106>)를 참조하십시오.

다음 예에서는 service.http.port configutil 매개 변수를 사용하여 Messenger Express HTTP 포트 번호를 8080으로 변경합니다.

```
configutil -o service.http.port -v 8080
```

사후 설치 포트 번호



# Sun Java Systems Messaging Server로 업그레이드

이 장에서는 Messaging Server 5.2에서 Messaging Server 6 2005Q1로 업그레이드하는 방법에 대해 설명합니다.

## 시작하기 전에

업그레이드를 수행하기 전에 다음을 확인합니다.

- Messaging Server 6 2005Q1을 Messaging Server 5.2 시스템과 같은 시스템 또는 다른 시스템에 설치하고 구성합니다.

---

**주** Messaging Server의 이전 버전과 달리, Messaging Server 6 2005Q1을 먼저 설치하여 구성하지 않고는 기존 Messaging Server를 업그레이드할 수 없습니다.

또한, Messaging Server 5.2 이전 버전에서는 이 업그레이드 프로그램을 사용할 수 없습니다. 따라서 Messaging Server 5.2로 마이그레이션하거나 업그레이드하고 Messaging Server 6 2005Q1을 설치한 다음 이 업그레이드 프로그램을 실행해야 합니다. Messaging Server 5.2로 마이그레이션하는 방법은 iPlanet Messaging Server 5.2 Migration Guide (<http://docs.sun.com/source/816-6017-10/index.html>)를 참조하십시오.

---

- 기존 Messaging Server 5.2 설치는 `imsimta dirsnc`가 아니라 MTA Direct LDAP Lookup에 대해 구성되어 있습니다.

- 또한, Messaging Server 6 2005Q1은 다중 인스턴스를 지원하지 않습니다. Messaging Server 버전 5.2의 인스턴스가 여러 개 있는 경우 Messaging Server 6 2005Q1로 업그레이드할 인스턴스를 하나만 선택할 수 있습니다. 또한 여러 인스턴스를 마이그레이션하기 위해 업그레이드 유틸리티를 두 번 이상 실행하면 구성을 덮어 씩니다.

## 업그레이드 프로세스 개요

Messaging Server 5.2에서 Messaging Server 6 2005Q1로 업그레이드하는 과정은 세 단계로 구성됩니다. 다음 항목에서 이 프로세스를 개략적으로 설명합니다.

1. 74페이지의 "구성을 업데이트하도록 업그레이드 파일 만들기" (UpgradeMsg5toMsg6.pl)
2. 78페이지의 "업그레이드 유틸리티 실행"(do\_the\_upgrade.sh)
  - MTA 구성(make\_mta\_config\_changes.sh)
  - configutil 매개 변수(make\_configutil\_changes.sh)
  - 백업 구성(make\_backup\_config\_changes.sh)
  - mboxlist 데이터베이스(make\_mboxlistdb\_changes.sh)
3. 80페이지의 "사용자 메일함 마이그레이션"(선택 사항)

## 구성을 업데이트하도록 업그레이드 파일 만들기

이 절에서는 Messaging Server 6 2005Q1 시스템의 구성을 업데이트하기 위해 특별한 업그레이드 파일을 만드는 방법에 대해 설명합니다.

- 74페이지의 "업그레이드 파일 정보"
- 76페이지의 "UpgradeMsg5toMsg6.pl Perl 스크립트 실행"

## 업그레이드 파일 정보

Messaging Server 5.2에서 6으로 마이그레이션하기 위한 업그레이드 유틸리티를 실행하기 전에 UpgradeMsg5toMsg6.pl Perl 스크립트(msg\_svr\_base/sbin에 있음)를 먼저 실행해야 합니다.

UpgradeMsg5toMsg6.pl은 5.2 구성 파일을 Messaging Server 6 구성 파일과 비교하고 각 구성 파일에 대해 \*.CHANGES 및 \*.MERGED의 두 파일 세트를 생성합니다.

\*.CHANGES 파일 및 \*.MERGED 파일은 작업 공간 디렉토리인 /var/tmp/UpgradeMsg5toMsg6.ScratchDir에 생성됩니다.

\*.CHANGES 파일은 Messaging Server 5.2와 Messaging Server 6 2005Q1의 구성 파일 간의 중요한 차이점을 보여줍니다. 이 파일에는 Messaging Server 6 2005Q1에만 있는 구성 엔티티, Messaging Server 6 2005Q1에서는 사용되지 않는 Messaging Server 5.2의 구성 엔티티 및 Messaging Server 5.2에만 있는 구성 엔티티가 포함됩니다. 모든 \*.CHANGES 파일이 구성 파일 버전 간의 차이점을 보여주는 것은 아니며, 모든 구성 파일이 \*.CHANGES 파일을 생성하는 것은 아닙니다.

\*.MERGED 파일에는 Messaging Server 5.2와 Messaging Server 6 구성 값 및 설정이 통합되어 있습니다. 일반적으로 Messaging Server 5.2의 구성 매개 변수 값은 다음의 경우 Messaging Server 6 2005Q1 버전에도 유지됩니다.

- Messaging Server 6 2005Q1 버전에 기본값이 없는 경우
- 5.2 구성에 지정된 값이 기본 설정이 아닌 경우

표 2-1은 \*.MERGED 또는 \*.CHANGES 파일을 생성하는 구성 파일의 목록입니다.

**표 2-1** \*.MERGED 또는 \*.CHANGES 파일을 생성하는 Messaging Server 구성 파일

구성 정보	설명	*.MERGED 파일 생성	*.CHANGES 파일 생성
job_controller.cnf	Job Controller 파일	X	X
conversions	변환 파일	X	
channel_option(여기서 channel은 SMTP 채널임)	SMTP 채널 옵션 파일	X	
native_option	원시 채널 옵션 파일 (channel_option 제외)	X	X
channel_headers.opt(여기서 channel은 SMTP 채널임)	헤더 옵션 파일	X	
dispatcher.cnf	디스패처 파일	X	X
imta_tailor	Tailor 파일	X	X

**표 2-1** \*.MERGED 또는 \*.CHANGES 파일을 생성하는 Messaging Server 구성 파일 (계속)

구성 정보	설명	*.MERGED 파일 생성	*.CHANGES 파일 생성
option.dat	전역 MTA 옵션 파일	X	X
aliases	별칭 파일	X	
imta.cnf	MTA 구성 파일. 포함 참조(파일 디렉토리 위치 등)만 변경됩니다. 다시 쓰기 규칙 및 채널 설정은 5.2의 구성을 유지합니다. imta.cnf에 LMTP를 포함시키려면 Messaging Server 6 imta.cnf 파일에서 LMTP 정보를 복사합니다.	X	경우에 따라 *.CHANGES 파일이 생성될 수 있습니다.
mappings	매핑 파일	X	
mappings.locale	현지화된 매핑 파일	X	
internet.rules	인터넷 규칙 구성 파일	X	
backup-groups.conf	백업 그룹 정의	X	X
configutil	local.conf 및 msg.conf 구성 파일의 구성 매개 변수 변경 사항		X

## UpgradeMsg5toMsg6.pl Perl 스크립트 실행

UpgradeMsg5toMsg6.pl을 실행하여 구성을 업데이트할 수 있는 파일 집합을 만들려면 다음 단계를 수행합니다.

1. 이 단계에서는 5.2와 Messaging Server 6 2005Q1 시스템 모두에서 실행할 수 있습니다.
2. Messaging Server 5.2 및 6 버전이 동일한 시스템에 있지 않은 경우 Messaging Server 5.2 *server-root* 디렉토리를 Messaging Server 6 2005Q1 시스템으로 전송, 추출 및 복사합니다. 두 서버 버전이 동일한 시스템에 설치되어 있으면 이 단계를 건너뛴니다.

메시지 저장소가 너무 커서 한 시스템에서 다른 시스템으로 전송할 수 없을 때는 서버 인스턴스의 중요한 부분만 새 시스템으로 전송하면 됩니다. 이에 대한 자세한 내용은 UpgradeMsg5toMsg6.pl을 참조하십시오.

Messaging Server 5.2 저장소 데이터를 Messaging Server 6 2005Q1 시스템으로 복사할 필요는 없지만 업그레이드 프로세스 중 Messaging Server 5.2 *mboxlist* 디렉토리에 액세스할 수 있어야 합니다.

3. UpgradeMsg5toMsg6.pl 업그레이드 스크립트(*msg\_svr\_base*/sbin에 있음)를 5.2 버전의 *msg-instance*와 Messaging Server 6 2005Q1 버전의 *msg\_svr\_base*에 대해 실행합니다. 예를 들면 다음과 같습니다.

```
perl UpgradeMsg5toMsg6.pl /usr/sunone/server5/msg-budgie \
/opt/SUNWmsgsr
```

여기서 */usr/sunone/server5/msg-budgie*는 5.2 Messaging Server의 *msg-instance*이고 */opt/SUNWmsgsr*는 Messaging Server 6 2005Q1의 *msg\_svr\_base*입니다.

\*.MERGED 및 \*.CHANGES 파일(표 2-1의 설명 참조)이 생성됩니다.

4. \*.MERGED 파일을 주의 깊게 살펴봅니다. 제안된 권장 사항을 사용하지 않을 경우에는 설정을 수동으로 변경해야 합니다.

이 유틸리티는 Messenger Express 사용자 정의 파일을 업데이트하지 않습니다. 따라서 Messaging Server 5.2의 관련 정보를 유지하고 Messaging Server 6 2005Q1 설치의 새 정보를 추가하려면 이 파일을 수동으로 변경해야 합니다.

## 업그레이드 유틸리티 실행

이 절에서는 네 개의 하위 스크립트로 구성된 셸 스크립트인 `do_the_upgrade.sh` 유틸리티(`/var/tmp/UpgradeMsg5toMsg6.ScratchDir`에 있음)에 대해 설명합니다. 다음 항목에 대해 설명합니다.

- 78페이지의 "업그레이드 유틸리티 개요"
- 78페이지의 "`do_the_upgrade.sh` 유틸리티 실행" (`do_the_upgrade.sh`)
- 79페이지의 "MTA 구성"(`make_mta_config_changes.sh`)
- 79페이지의 "`configutil` 매개 변수"(`make_configutil_changes.sh`)
- 80페이지의 "백업 구성"(`make_backup_config_changes.sh`)
- 80페이지의 "`mboxlist` 데이터베이스"(`make_mboxlistdb_changes.sh`)

## 업그레이드 유틸리티 개요

`do_the_upgrade.sh` 유틸리티는 네 개의 셸 스크립트로 구성되며, `*.MERGED` 파일을 통해 MTA 구성의 구성 및 파일 디렉토리 위치, `configutil` 매개 변수, 백업 매개 변수 및 Messaging Server 6 2005Q1 시스템의 `mboxlist` 데이터베이스를 업데이트할 수 있습니다.

`do_the_upgrade.sh` 유틸리티를 실행하거나 `do_the_upgrade.sh` 유틸리티를 구성하는 두 개 이상의 스크립트(`make_mta_config_changes.sh`, `make_configutil_changes.sh`, `make_backup_config_changes.sh` 및 `make_mboxlistdb_changes.sh`)를 개별적으로 실행할 수 있습니다.

MTA 릴레이 시스템을 Messaging Server 5.2에서 Messaging Server 6 2005Q1로 업그레이드하려면 `make_mta_config_changes.sh` 및 `make_backup_config_changes.sh`만 실행하면 됩니다(80페이지의 "백업 구성"의 설명 참조).

`do_the_upgrade.sh` 유틸리티 또는 하위 스크립트 중 하나를 실행하려면 Messaging Server 5.2나 6 2005Q1이 실행 중이면 안 됩니다.

## `do_the_upgrade.sh` 유틸리티 실행

`do_the_upgrade.sh` 유틸리티를 실행하려면 다음을 수행합니다.

1. Messaging Server 5.2와 6을 모두 종료합니다.
2. 유틸리티를 실행합니다.

```
# sh /var/tmp/UpgradeMsg5toMsg6.ScratchDir/do_the_upgrade.sh
```

do\_the\_upgrade.sh 스크립트를 실행한 뒤에는 5.2 분할 영역 경로를 계속 참조하거나 (Messaging Server 5.2 *server-root* 디렉토리를 제거할 수 없게 되지만) 5.2 저장소 분할 영역을 적절한 Messaging Server 6 2005Q1 디렉토리 위치로 수동으로 이동할 수 있습니다. Messaging Server를 다시 시작하기 전에 이 단계를 수행해야 합니다.

## MTA 구성

do\_the\_upgrade.sh 유틸리티의 일부를 구성하는 MTA 업그레이드 구성 하위 스크립트를

make\_mta\_config\_changes.sh(/var/tmp/UpgradeMsg5toMsg6.ScratchDir에 있음)라고 합니다.

make\_mta\_config\_changes.sh 스크립트는 \*.MERGED 서버 구성 파일을 Messaging Server 6 2005Q1 파일 디렉토리 구조 내의 원래 이름 및 위치로 백업, 이름 변경 및 이동합니다.

스크립트가 파일 이름 변경 및 이동을 완료한 뒤에는 자동으로 imsimta cnbuild 명령을 실행하여 MTA 구성을 다시 컴파일합니다.

---

**주** MTA 릴레이 시스템을 Messaging Server 5.2에서 Messaging Server 6 2005Q1로 업그레이드하려면 make\_mta\_config\_changes.sh 및 make\_backup\_config\_changes.sh(80페이지의 "백업 구성"의 설명 참조)를 실행하기만 하면 됩니다.

---

## configutil 매개 변수

do\_the\_upgrade.sh 유틸리티의 일부를 구성하는 configutil 업그레이드 구성 하위 스크립트를 make\_configutil\_changes.sh 스크립트

(/var/tmp/UpgradeMsg5toMsg6.ScratchDir에 있음)라고 합니다.

make\_configutil\_changes.sh 스크립트는 새 매개 변수나 업데이트된 매개 변수를 msg.conf 및 local.conf 파일에 통합합니다. Messaging Server 6 2005Q1의 configutil 매개 변수에 기본값이 지정되어 있지 않은 경우 Messaging Server 5.2 값이 Messaging Server 6 2005Q1 버전에 전달됩니다.

## 백업 구성

`do_the_upgrade.sh` 유틸리티의 일부를 구성하는 백업 업그레이드 구성 하위 스크립트를 `make_backup_config_changes.sh` 스크립트

(`/var/tmp/UpgradeMsg5toMsg6.ScratchDir`에 있음)라고 합니다.

`make_backup_config_changes.sh` 스크립트는 `backup-groups.conf` 파일의 구성 등과 같은 백업 서비스의 구성을 업그레이드합니다.

## mboxlist 데이터베이스

`do_the_upgrade.sh` 유틸리티의 일부를 구성하는 `mboxlist` 데이터베이스 업그레이드 구성 하위 스크립트를 `make_mboxlistdb_changes.sh` 스크립트

(`/var/tmp/UpgradeMsg5toMsg6.ScratchDir`에 있음)라고 합니다.

`make_mboxlistdb_changes.sh` 스크립트는 5.2 `mboxlist` 데이터베이스를 전송 및 업그레이드하고 이를 Messaging Server 6 2005Q1 디렉토리 구조로 업그레이드합니다. 이 스크립트는 네 개의 \*.db 파일(`folder.db`, `quota.db`, `peruser.db` 및 `subscr.db`)을 Messaging Server 5.2 시스템의 `server-root/msg-instance/store/mboxlist`에서 Messaging Server 6 2005Q1 시스템의 `msg_svr_base/data/store/mboxlist`로 복사합니다.

# 사용자 메일함 마이그레이션

이 절에서는 사용자 메일함을 Messaging Server 5.2에서 Messaging Server 6 2005Q1 시스템으로 마이그레이션하는 방법을 설명합니다. Messaging Server 5.2를 Messaging Server 6으로 업그레이드하고 전체 메시지 저장소 데이터베이스를 업그레이드할 경우 이 절차를 수행할 필요가 없습니다. 이전 절에서 설명한 `make_mboxlistdb_changes.sh` 스크립트를 사용하여 데이터베이스를 보다 효율적으로 업그레이드할 수 있습니다.

다음 경우에만 이 단계를 수행합니다.

- Windows에서 UNIX 또는 UNIX에서 Windows로 마이그레이션할 경우
- 전체 메시지 저장소를 한 번에 마이그레이션하지 않으려는 경우
- UID, 도메인 이름, 기본 도메인 변경 사항을 비롯하여 사용자 아이디를 변경할 경우

이 절차를 사용하여 메일함을 마이그레이션할 경우 분할 영역 경로를 Messaging Server 5.2 분할 영역에 매핑하지 마십시오. 또한, `make_mboxlist_changes.sh` 스크립트를 실행하지 마십시오.



업그레이드 스크립트에 의해 생성된 `make_configutil_changes.sh` 스크립트는 자동으로 분할 영역 경로를 설정하여 Messaging Server 5.2 분할 영역으로 매핑합니다. 이 작업은 수동으로 변경해야 합니다. 또한, `make_mboxlistdb_changes.sh` 스크립트 호출을 `do_the_upgrade.sh` 스크립트에서 제거해야 합니다.

사용자 메일함 데이터를 온라인을 통해 Messaging Server 5.2에서 Messaging Server 6 2005Q1로 이동하려면 이 절에서 설명하는 단계를 수행하십시오. 데이터를 이동할 때 Messaging Server를 종료하면 안 됩니다.

이 절에서는 다음 항목에 대해 설명합니다.

- 81페이지의 "요구 사항"
- 81페이지의 "마이그레이션 지침"

## 요구 사항

마이그레이션하려면 기존 및 새 Messaging Server가 모두 실행되도록 stored해야 합니다.

## 마이그레이션 지침

사용자 메일함을 5.2 시스템에서 Messaging Server 6 2005Q1 시스템으로 마이그레이션하려면 다음을 수행합니다.

1. 데이터 이동 프로세스가 완료될 때까지 메일함에 액세스할 수 없다는 사실을 사용자에게 미리 알립니다. 데이터 이동을 수행하기 전에 사용자들이 메일 시스템에서 로그아웃하도록 합니다.
2. 5.2 메시지 저장소의 모든 사용자 항목에 대한 `mailUserStatus` 사용자 LDAP 속성을 `active`에서 `hold`로 변경하여, 수신되는 사용자의 메일을 보관 대기열에 보관하고 IMAP, POP 및 HTTP를 통해 메일함에 액세스하지 못하도록 합니다.

`mailUserStatus`에 대한 자세한 내용은 *Sun Java System Communications Services Schema Reference Manual*(<http://docs.sun.com/doc/819-0113>)을 참조하십시오.

3. 이 프로세스 도중 Messaging Server 5.2 및 6 2005Q1이 모두 실행 중이어야 합니다.

4. 모든 사용자 항목의 mailHost 속성을 기존 메일 서버에서 새 메일 서버로 변경합니다.

이렇게 하려면 아래의 ldapsearch 명령을 사용하여 mailHost 속성을 수정해야 하는 사용자 항목을 찾습니다.

```
ldapsearch -h ldap.siroe.com -b "o=internet" \  
"(&(objectclass=maildomain)(mailHost=oldmail.siroe.com))"
```

그런 다음 ldapmodify 명령을 사용하여 항목을 새 메일 서버로 적절하게 변경합니다. Messaging Server 및/또는 Directory Server와 함께 제공된 ldapmodify를 사용합니다. Solaris ldapmodify를 사용하지 마십시오.

mailhost에 대한 자세한 내용은 *Sun Java System Communications Services Schema Reference Manual*을 참조하십시오.

5. 이전 시스템에서는 backup-groups.conf 파일을 사용하여 사용자 항목을 동일한 그룹 수로 분할합니다. 단계 6에서 파일에 사용자 아이디를 넣고 -u 옵션을 사용할 수도 있습니다.
6. Messaging 5.2 메시지 저장소의 사용자 데이터를 Messaging Server 6 2005Q1 메시지 저장소로 이동합니다.

이 단계를 수행하려면 imsbackup 유틸리티를 사용하여 Messaging Server 5.2 메시지 저장소를 백업한 다음 imsrestore 유틸리티를 사용하여 해당 메시지 저장소를 Messaging Server 6 2005Q1에 복원합니다. 예를 들어, 메일함을 oldmail.siroe.com에서 newmail.siroe.com으로 마이그레이션하려면 oldmail.siroe.com에서 다음 명령을 실행합니다.

```
/<server-root>/bin/msg/store/bin/imsbackup -f- /<instance>/<group> \  
| rsh newmail.siroe.com /opt/SUNWmsgsr/lib/msg/imsrestore.sh \  
-f- -cy -v1
```

여러 백업 및 복원 세션(그룹마다 하나씩)을 동시에 실행하여 새 메시지 저장소로의 전송 속도를 최대화할 수 있습니다. imsbackup 및 imsrestore 유틸리티에 대한 자세한 내용은 *Messaging Server Reference Manual*(<http://docs.sun.com/doc/819-0106>)과 610페이지의 "메시지 저장소 백업 및 복원"을 참조하십시오.

7. Messaging Server 6 2005Q1을 시스템의 새 기본 Messaging Server로 설정합니다.  
oldmail.siroe.com의 A 레코드를 변경하여 newmail.siroe.com(이전에 oldmail.siroe.com에서 호스트되던 도메인을 담당하는 서버)을 가리키도록 합니다.
8. 다음 명령을 실행하여 Messaging Server 5.2 시스템의 보관 대기열에 있는 메일을 해제합니다.

```
imsimta process_held -uid=user -domain=domain
```

여기서 *user*는 사용자 아이디이고 *domain*은 사용자가 속해 있는 도메인입니다.

9. 사용자 클라이언트가 새 메일 서버를 가리키는지 확인합니다.  
업그레이드가 끝나면 사용자가 메일 클라이언트 프로그램을 통해 새 서버를 가리키도록 합니다. 이 예에서는 oldmail.siroe.com에서 newmail.siroe.com을 가리킵니다.  
대체 방법인 MMP를 사용하면 사용자가 자신의 클라이언트를 통해 새 메일 서버를 가리키도록 할 필요가 없습니다. MMP는 LDAP 사용자 항목이 저장되어 있는 mailHost 속성에서 정보를 가져와 새 서버로 자동으로 리디렉션합니다.



# 고가용성 구성

이 장에서는 Veritas Cluster Server 또는 Sun Cluster 고가용성 클러스터링 소프트웨어를 구성하고 Messaging Server와 함께 사용할 준비를 하는 데 필요한 정보를 제공합니다. 이 절에서는 *Messaging Server Deployment Planning Guide*(<http://docs.sun.com/doc/819-0063>)의 고가용성에 대한 장 및 Veritas 또는 Sun Cluster Server 설명서에서 세부 계획, 설치 지침, 필수 패치 및 기타 필요한 정보에 대해 읽어본 것으로 간주합니다.

표 3-1은 현재 Messaging Server에서 지원되는 Sun Cluster Server 및 Veritas Cluster Server의 버전 목록을 보여줍니다.

**표 3-1** 지원되는 Sun Cluster Server 및 Veritas Cluster Server 버전

클러스터	지원되는 버전
Sun Cluster Server	Sun Cluster 3.1
Veritas Cluster Server	Veritas Cluster Server 1.3, Veritas Cluster Server 2.0 및 Veritas Cluster Server 3.5

이 장은 다음 내용으로 구성되어 있습니다.

- 86페이지의 "클러스터 에이전트 설치"
- 87페이지의 "Veritas Cluster Server 에이전트 설치"
- 92페이지의 "Sun Cluster 에이전트 설치"
- 99페이지의 "고가용성 구성 해제"

## 클러스터 에이전트 설치

클러스터 에이전트는 클러스터 프레임워크에서 실행되는 Messaging Server 프로그램입니다.

Sun Cluster Messaging Server 에이전트(SUNWscims)는 Java Enterprise System 설치 프로그램을 통해 Sun Cluster 3.1을 선택한 경우에 설치됩니다. Veritas Cluster Messaging Server 에이전트(SUNWmsgvc)는 Java Enterprise System CD의 Messaging Server Product 하위 디렉토리

Solaris\_sparc/Product/messaging\_svr/Packages/SUNWmsgvc에 있습니다. VCS 클러스터 에이전트를 설치하려면 pkgadd(1M) 명령을 사용해야 합니다.

## Messaging Server 및 고가용성 지침

Messaging Server 및 고가용성(Veritas Cluster와 Sun Cluster 모두에 적용됨) 설치와 관련하여 몇 가지 알아두어야 할 사항이 있습니다.

- Messaging Server를 설치 및 구성하기 전에 클러스터링 소프트웨어를 설치해야 합니다. Messaging Server의 HA 논리 호스트 이름이 현재 가리키고 있는 클러스터 노드에서 설치를 실행합니다. 노드 이름을 묻는 메시지가 나타나면 클러스터 별칭을 사용합니다. Messaging Server를 설치할 때 관련된 물리적 시스템에 상관없이 Messaging Server를 설치하는 노드가 클러스터의 논리적 이름이라는 것을 관리 서버에 알립니다.
- Messaging Server 초기 런타임 구성(51페이지의 "[Messaging Server 초기 런타임 구성 만들기](#)" 참조)을 실행할 때 Messaging Server 클러스터의 정규화된 HA 논리 호스트 이름을 지정해야 합니다.
- 클러스터 호스트 이름을 사용하여 Messaging Server를 구성합니다. 그렇게 하지 않으면 클러스터 호스트 이름을 사용하여 또 다시 구성해야 합니다.

## useconfig 유틸리티 사용

useconfig 유틸리티를 사용하면 단일 구성을 HA 환경의 여러 노드에서 공유할 수 있습니다. 이 유틸리티는 기존 구성을 업그레이드하거나 업데이트하는 용도로 사용할 수 없습니다.

예를 들어 첫 번째 노드를 업그레이드하는 경우 Java Enterprise System 설치 프로그램을 통해 설치한 다음 Messaging Server를 구성합니다. 그런 다음 Java Enterprise System 설치 프로그램을 통해 Messaging Server 패키지를 설치할 두 번째 노드로 패일오버합니다. 하지만 초기 런타임 구성 프로그램(configure)을 다시 실행할 필요는 없습니다. 대신 useconfig 유틸리티를 사용할 수 있습니다.

유틸리티를 사용하려면 useconfig 유틸리티를 실행하여 이전 Messaging Server 구성을 가리키도록 합니다.

```
msg_svr_base/sbin/useconfig install/configure_YYYYMMDDHHMMSS
```

여기서 configure\_YYYYMMDDHHMMSS는 이전 구성 설정 파일입니다.

새 노드의 경우 공유 디스크의 msg\_svr\_base/data/setup 디렉토리에서 configure\_YYYYMMDDHHMMSS를 찾을 수 있습니다.

87페이지의 "Veritas Cluster Server 에이전트 설치" 및 92페이지의 "Sun Cluster 에이전트 설치"에 대한 다음 절에서는 useconfig 유틸리티를 사용할 수 있는 시기에 대해 설명합니다.

## Veritas Cluster Server 에이전트 설치

Messaging Server는 Veritas Cluster Server 1.3, 2.0 및 3.5와 함께 작동하도록 구성할 수 있습니다. 이 절에 나와 있는 지침은 Veritas Cluster 3.5만 다룹니다. Veritas 1.3 및 2.0에 대해서는 *Sun ONE Messaging Server 설치 설명서*(<http://docs.sun.com/doc/819-0809>)를 참조하십시오.

이 절차를 따르기 전에 Veritas Cluster Server 설명서를 검토하시기 바랍니다.

- 
- 주**
- Veritas Volume Manager(VxVM)에는 별도의 사용권이 필요한 클러스터 기능이 있습니다. 이 기능은 Sun Cluster 3.0 전역 파일 시스템과 비슷하게, 공유 저장소에 있는 파일 시스템에 대한 전역 보기를 제공합니다. 자세한 내용은 Veritas Cluster Server 설명서를 참조하십시오.
  - FscckOpt는 3.5 이전 버전의 Veritas에서는 선택 사항이었습니다. 하지만 Mount 자원을 구성하려면 이 기능이 필요합니다. FscckOpt에는 -y 또는 -n이 포함되어야 하며 그렇지 않은 경우 자원이 온라인이 되지 않습니다.
  - Veritas Cluster Server 2.0 Explorer는 Veritas Cluster Server 3.5를 관리하는 데 사용할 수 없습니다.
- 

Java Enterprise System 설치 프로그램을 통해 Messaging Server를 설치하고 HA를 구성한 후에는 97페이지의 "서버에서 IP 주소 바인딩"을 검토하여 HA 지원의 구성과 관련된 추가 단계가 있는지 확인하십시오.

## Veritas Cluster Server 요구 사항

- Veritas Cluster 소프트웨어가 이미 설치 및 구성되어 있어야 합니다.
- 다음 절(88페이지의 "VCS 3.5 설치 및 구성 지침")에 설명되어 있듯이 두 개의 노드에 Messaging Server용 Veritas Cluster 에이전트 패키지와 Messaging Server 소프트웨어를 함께 설치합니다.

## VCS 3.5 설치 및 구성 지침

다음은 Veritas Cluster Server 3.5를 사용하여 Messaging Server를 HA 서비스로 구성하는 방법에 대한 설명입니다.

기본 main.cf 구성 파일은 VCSweb 응용 프로그램을 실행하는 ClusterService라는 자원 그룹을 설정합니다. 이 그룹에는 csgnic 및 webip와 같은 네트워크의 논리 호스트 IP 자원이 포함됩니다. 또한 이벤트 알림을 위한 ntfr 자원이 생성됩니다.



1. 노드 중 하나에서 Cluster Explorer를 시작합니다.

이 Veritas Cluster Server 지침에서는 그래픽 사용자 인터페이스를 사용하여 Messaging Server를 HA 서비스로 구성한다고 가정합니다.

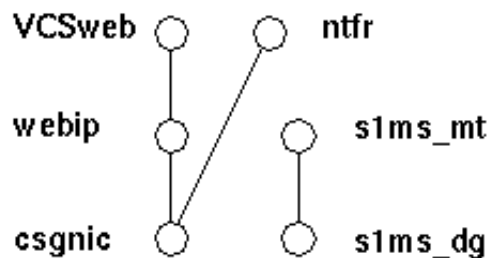
Cluster Explorer를 시작하려면 다음 명령을 실행합니다.

```
# /opt/VRTSvcs/bin/hagui
```

GUI를 사용하려면 VRTScscm 패키지가 설치되어 있어야 합니다.

2. DiskGroup 유형의 s1ms\_dg 디스크 그룹 자원을 추가하고 활성화합니다.
3. Mount 유형의 s1ms\_mt 마운트 자원을 추가합니다.
  - a. Veritas Cluster Server 2.0과는 달리 -y(또는 -n)를 FscckOpt에 추가해야 합니다. 옵션을 지정하지 않으면 Mount가 중지됩니다. fsck\_vxfs에 대한 자세한 내용은 Solaris 설명서 페이지를 참조하십시오.
  - b. 아직 활성화되지 않은 경우 링크 버튼을 눌러 자원 링크를 활성화합니다.
4. s1ms\_mt와 s1ms\_dg 사이에 링크를 만듭니다. s1ms\_mt 자원을 활성화합니다. 그림에서는 종속성 트리를 설명합니다.

그림 3-1 Veritas Cluster Server 종속성 트리



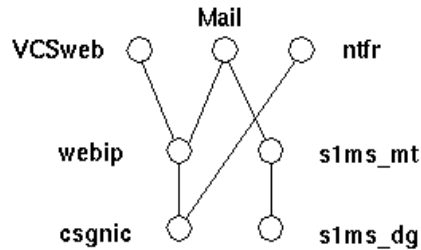
5. Administration Server 및 Messaging Server를 선택하여 Java Enterprise System 설치 프로그램을 실행합니다.

- a. Administration Server 구성 중에 호스트 이름을 제공하라는 메시지가 표시되면 논리 호스트 이름을 지정해야 합니다.
- b. 기본 노드(예: Node\_A)에서 Messaging Server 초기 런타임 구성을 실행하여 Messaging Server를 설치합니다.
- c. pkgadd(1M) 명령을 사용하여 Veritas Cluster Server 에이전트 패키지인 SUNWmsgvc(Java Enterprise System CD의 Messaging Server Product 하위 디렉토리에 있음)를 설치합니다.

이제 Node\_A에 Messaging Server와 Veritas 에이전트가 설치되었습니다.

6. 백업 노드(예: Node\_B)로 전환합니다.
7. Java Enterprise System 설치 프로그램을 실행하여 백업 노드(Node\_B)에 Messaging Server를 설치합니다.
8. Messaging Server를 설치한 다음 useconfig 유틸리티를 사용하면 백업 노드(Node\_B)에 초기 런타임 구성을 추가로 만들 필요가 없습니다. useconfig 유틸리티를 사용하면 단일 구성을 HA 환경의 여러 노드에서 공유할 수 있습니다. 이 유틸리티는 기존 구성을 업그레이드하거나 업데이트하는 용도로 사용할 수는 없습니다. [86페이지의 "useconfig 유틸리티 사용"](#)을 참조하십시오.  
이제 Node\_B에 Veritas 에이전트가 설치되었습니다.
9. Cluster Explorer의 파일 메뉴에서 유형 가져오기...를 선택합니다. 그러면 파일 선택 상자가 표시됩니다.
10. /etc/VRTSvcs/conf/config 디렉토리에서 MsgSrvTypes.cf 유형을 가져옵니다. 이 유형 파일을 가져옵니다. 이 파일을 찾으려면 클러스터 노드에 있어야 합니다.
11. 이제 MsgSrv 유형의 자원(예: Mail)을 만듭니다. 이 자원을 사용하려면 논리 호스트 이름 등록 정보를 설정해야 합니다.
12. Mail 자원은 slms\_mt 및 webip에 종속됩니다. 다음 종속성 트리에 표시되어 있는 것처럼 자원 간에 링크를 만듭니다.

그림 3-2 Veritas Cluster 종속성 트리



- a. 모든 자원을 활성화하고 Mail을 온라인 상태로 만듭니다.
  - b. 모든 서버가 시작됩니다.
13. Node\_A로 전환하여 HA 구성이 작동하는지 확인합니다.
  14. 그룹 속성 OnlineRetryLimit를 3에서 0으로 변경합니다. 이렇게 하지 않으면 페일 오버된 서비스가 같은 노드에서 다시 시작됩니다.

## MsgSrv 속성

이 절에서는 mail 자원의 동작을 제어하는 추가 속성인 MsgSrv에 대해 설명합니다. Messaging Server를 Veritas Cluster Server에 대해 구성하려면 표 3-2를 참조하십시오.

표 3-2 Veritas Cluster Server 속성

속성	설명
FaultOnMonitorTimeouts	설정하지 않으면(=0), 모니터(감시) 시간 초과가 자원 오류로 간주되지 않습니다. 2로 설정할 것을 권장합니다. 모니터가 두 번 시간 초과되면 자원이 다시 시작되거나 페일오버됩니다.
ConfInterval	오류/재시작을 계산하는 시간 간격입니다. 서비스가 이 시간 동안 온라인 상태를 유지하면 이전 기록이 지워집니다. 권장 값은 600초입니다.
ToleranceLimit	모니터가 자원 FAULTED를 선언하기 전에 OFFLINE을 반환하는 횟수입니다. 이 값을 '0'(기본값)에 두는 것이 좋습니다.

# Sun Cluster 에이전트 설치

이 절에서는 Messaging Server를 Sun Cluster 고가용성(HA) 데이터 서비스로 설치 및 구성하는 방법에 대해 설명합니다. 이 설치 지침은 Sun Cluster 3.1에 적용됩니다. 다음 항목에 대해 설명합니다.

- 92페이지의 "Sun Cluster 요구 사항"
- 92페이지의 "HAStoragePlus 정보"
- 93페이지의 "Sun Cluster 및 HA StoragePlus를 사용하여 Messaging Server 구성"
- 97페이지의 "서버에서 IP 주소 바인딩"

Sun Cluster 3.1에 대한 설명서는 다음 위치에서 찾을 수 있습니다.

<http://docs.sun.com/db/prod/cluster#hic> 및  
<http://docs.sun.com/db/prod/cluster?l=ko#hic>

Veritas File System(VxFS)은 Sun Cluster 3.1에서 지원됩니다.

## Sun Cluster 요구 사항

이 절에서는 다음을 가정합니다.

- Sun Cluster 3.1이 Solaris 8 또는 9 운영 체제에 필수 패치와 함께 설치 및 구성되어 있습니다.
- Sun Cluster 에이전트 SUNWscims가 시스템에 설치되어 있습니다.
- 논리적 볼륨을 생성하는 경우 Solstice DiskSuite 또는 Veritas Volume Manager가 사용됩니다.

## HAStoragePlus 정보

HAStoragePlus 자원 유형을 사용하여 Sun Cluster 환경에서 로컬 마운트 파일 시스템의 가용성을 높이는 것이 좋습니다. Sun Cluster 전역 장치 그룹에 있는 모든 파일 시스템을 HAStoragePlus와 함께 사용할 수 있습니다. HAStorage와 같은 전역 마운트 파일 시스템과 달리 HAStoragePlus는 특정 시간에 하나의 클러스터 노드에서만 사용할 수 있습니다. 이러한 로컬 마운트 파일 시스템은 페일오버 모드와 페일오버 자원 그룹에서만 사용할 수 있습니다. HAStoragePlus는 HAStorage의 GFS(전역 파일 시스템)와 반대로 FFS(페일오버 파일 시스템)를 제공합니다.

HAStoragePlus에는 다음과 같은 여러 장점이 있습니다.

- HAStoragePlus는 전역 파일 서비스 계층을 완벽히 우회합니다. 이런 특징은 디스크 입출력 사용량이 많은 데이터 서비스의 경우 성능을 크게 향상시킵니다.
- HAStoragePlus는 전역 파일 서비스 계층에서는 작동하지 않는 파일 시스템을 비롯하여, 모든 파일 시스템(UFS, VxFS 등)과 함께 사용할 수 있습니다. Solaris 운영 체제에서 지원되는 파일 시스템이라면 HAStoragePlus와 함께 사용할 수 있습니다.

HAStoragePlus에 대한 자세한 내용은 *Sun Cluster 3.1 Data Service Planning and Administration Guide*를 참조하십시오.

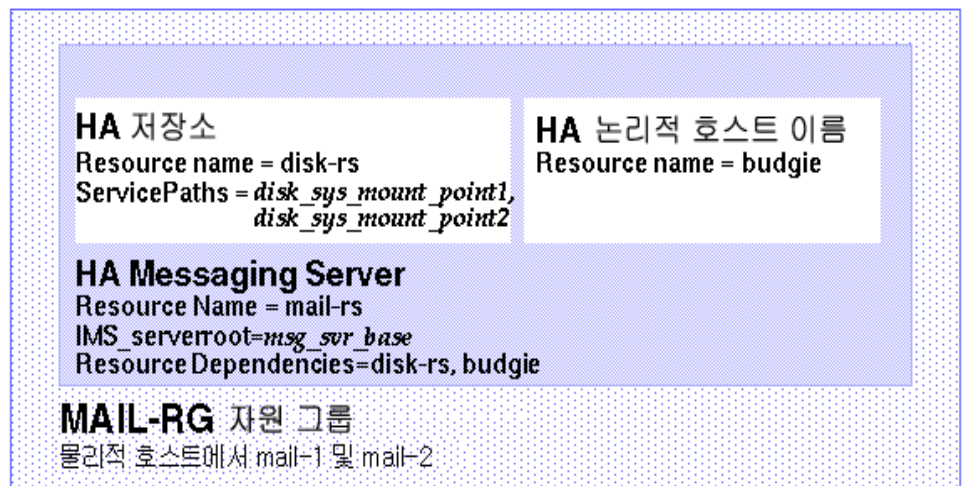
## Sun Cluster 및 HA StoragePlus를 사용하여 Messaging Server 구성

이 절에서는 간단한 예를 통해 Sun Cluster 3.1용 Sun Java System Messaging Server에 대한 HA 지원 및 HA StoragePlus를 구성하는 방법을 설명합니다.

HA를 구성한 뒤에는 97페이지의 "서버에서 IP 주소 바인딩"에서 HA 지원과 관련된 추가 단계를 검토하십시오.

다음 예에서는 Messaging Server가 HA 논리 호스트 이름과 IP 주소로 구성되어 있다고 가정합니다. 물리적 호스트 이름은 HA 논리 호스트 이름인 budgie와 함께 mail-1 및 mail-2인 것으로 가정합니다. **그림 3-3**은 Messaging Server HA 지원을 구성할 때 만들 다른 HA 자원의 중첩된 종속성을 나타냅니다.

**그림 3-3** 간단한 Sun Java System Messaging Server HA 구성



1. 슈퍼유저가 된 다음 콘솔을 엽니다.

아래에 나오는 Sun Cluster 명령을 사용하려면 슈퍼유저로 로그인해야 합니다. 또한 /dev/console에 출력되는 메시지에 대한 자세한 내용은 콘솔이나 창이 필요합니다.

2. 필요한 자원 유형을 추가합니다.

사용할 자원 유형을 Sun Cluster가 인식하도록 구성합니다. `scrgadm -a -t` 명령을 사용하여 이 작업을 합니다.

```
# scrgadm -a -t SUNW.HAStoragePlus
# scrgadm -a -t SUNW.ims
```

3. Messaging Server에 대한 자원 그룹을 만듭니다.

자원 그룹을 만들고 Messaging Server가 실행될 클러스터 노드에 표시되도록 만듭니다. 다음 명령은 MAIL-RG라는 자원 그룹을 만들고 클러스터 노드인 mail-1과 mail-2에 표시되도록 합니다.

```
# scrgadm -a -g MAIL-RG -h mail-1,mail-2
```

물론 자원 그룹에는 원하는 이름을 사용할 수 있습니다.

4. HA 논리 호스트 이름 자원을 만들고 자원 그룹을 시작합니다.

HA 논리 호스트 이름에 대한 자원을 만들고 활성화한 다음 자원 그룹에 추가합니다. 다음 명령은 논리 호스트 이름 budgie를 사용하여 이 작업을 수행합니다. `-j` 스위치를 생략했기 때문에 생성되는 자원의 이름 역시 budgie가 됩니다.

```
# scrgadm -a -L -g MAIL-RG -l budgie
# scswitch -Z -g MAIL-RG
```

## 5. HAStoragePlus 자원을 만듭니다.

그런 다음 Messaging Server가 종속된 파일 시스템에 대한 HA 저장소 자원 유형을 만들어야 합니다. 다음 명령은 disk-rs라는 이름의 HAStoragePlus 자원을 만들고 파일 시스템 `disk_sys_mount_point`는 이 자원의 제어를 받게 됩니다.

```
# scrgadm -a -j disk-rs -g MAIL-RG \
-t SUNW.HAStoragePlus \
-x ServicePaths=disk_sys_mount_point-1,disk_sys_mount_point-2
```

ServicePaths의 쉼표로 분리된 목록은 Messaging Server가 종속된 클러스터 파일 시스템의 마운트 지점입니다. 위의 예에서는 두 개의 마운트 지점 `disk_sys_mount_point-1`과 `disk_sys_mount_point-2`가 지정되었습니다. 서버 중 하나에 해당 서버가 종속된 추가 파일 시스템이 있는 경우 추가 HA 저장소 자원을 만들고 [단계 10](#)에서 해당 추가 종속성을 가리킵니다.

## 6. Administration Server를 설치 및 구성합니다(Sun ONE Messaging Server 설치 설명서 참조).

정규화된 도메인 이름을 지정할 때 [단계 4](#)에서 생성된 HA 로컬 호스트 이름을 사용합니다.

## 7. Messaging Server를 설치 및 구성합니다. 51페이지의 "Messaging Server 초기 런타임 구성 만들기"를 참조하십시오.

- a. 초기 런타임 구성 과정에서 [51페이지](#)의 "Messaging Server 초기 런타임 구성 만들기"에서 지정한 구성 디렉토리를 지정할 것을 요청합니다. HAStoragePlus 자원의 공유 디스크 디렉토리 경로를 사용해야 합니다.
- b. 다음 명령을 실행하여 Sun Cluster에서 watcher 프로세스를 활성화합니다.

```
configutil -o local.autorestart -v 1
```

watcher 프로세스에 대한 자세한 내용은 [110페이지](#)의 "실패했거나 응답이 없는 서비스의 자동 재시작"을 참조하십시오.

8. `ha_ip_config` 스크립트를 실행하여 `service.listenaddr`과 `service.http.smtphost`를 설정하고 `dispatcher.cnf`와 `job_controller.cnf` 파일을 고가용성에 대해 구성합니다. 스크립트를 사용하면 논리적 IP 주소가 물리적 IP 주소가 아니라 이 매개 변수와 파일에 대해 설정됩니다. 또한 `watcher` 프로세스가 활성화(`local.watcher.enable`을 1로 설정)되고 자동 재시작 프로세스가 활성화(`local.auto.restart`를 1로 설정)됩니다.

스크립트 실행에 대한 자세한 내용은 97페이지의 "서버에서 IP 주소 바인딩"을 참조하십시오.

`ha_ip_config` 스크립트는 공유 디스크(구성 및 데이터용)가 있는 시스템에서 한 번만 실행해야 합니다.

9. `imta.cnf` 파일을 수정하고 모든 물리적 호스트 이름을 클러스터의 논리 이름으로 바꿉니다.
10. HA Messaging Server 자원을 만듭니다.

이제 HA Messaging Server 자원을 만들어 자원 그룹에 추가해야 합니다. 이 자원은 HA 논리 호스트 이름과 HA 디스크 자원에 종속됩니다.

HA Messaging Server 자원을 만들 때는 경로를 Messaging Server의 최상위 디렉토리인 `msg_svr_base` 경로로 지정해야 합니다. 이 작업은 다음 명령에 나와 있는 `IMS_serverroot` 확장 등록 정보를 사용하여 수행합니다.

```
# scrgadm -a -j mail-rs -t SUNW.ims -g MAIL-RG \
-x IMS_serverroot=msg_svr_base \
-y Resource_dependencies=disk-rs,budgie
```

위의 명령은 `msg_svr_base` 디렉토리의 `IMS_serverroot`에 설치된 Messaging Server에 대해 `mail-rs`라는 이름의 HA Messaging Server 자원을 만듭니다. HA Messaging Server 자원은 HA 논리 호스트 이름 `budgie`와 HA 디스크 자원 `disk-rs`에 종속적입니다.

Messaging Server에 추가 파일 시스템 종속성이 있는 경우 이러한 파일 시스템에 대해 추가 HA 저장소 자원을 만들 수 있습니다. 추가 HA 저장소 자원 이름이 위 명령의 `Resource_dependencies` 옵션에 포함되도록 합니다.

11. `/etc/vfstab` 파일에서 `global`이라는 단어를 제거합니다. 부트 시 `/etc/vfstab`를 'no..'로 설정해야 합니다. 자세한 내용은 Sun Cluster 3.1 설명서를 참조하십시오.

HAStoragePlus로 `vfstab` 파일이 활성화되기 전에 먼저 현재 전역 파일 시스템인 파일 시스템을 마운트 해제(`umount`)해야 합니다. 그런 다음 HAStoragePlus로 `vfstab` 파일을 활성화하고 파일 시스템을 다시 마운트할 수 있습니다.



**12. Messaging Server 자원을 활성화합니다.**

이제 HA Messaging Server 자원을 활성화하여 Messaging Server를 온라인으로 만듭니다. 이 작업을 수행하려면 다음 명령을 사용합니다.

```
# scswitch -e -j mail-rs
```

위의 명령은 MAIL-RG 자원 그룹의 mail-rs 자원을 활성화합니다. MAIL-RG 자원이 이미 온라인 상태가 되었기 때문에 위의 명령은 mail-rs도 온라인 상태로 만듭니다.

**13. 온라인 상태로 되었는지 확인합니다.**

MAIL-RG 자원 그룹이 온라인인지 확인하려면 scstat 명령을 사용합니다. 콘솔 장치에 표시된 출력에서 진단 정보를 살펴봅니다. 또한 syslog 파일, /var/adm/messages도 살펴봅니다.

**14. 페일오버가 제대로 작동하는지 확인하기 위해 자원 그룹을 다른 클러스터 노드로 페일오버합니다.**

자원 그룹을 다른 클러스터 노드로 수동으로 페일오버합니다. 페일오버를 수행할 노드에 대한 슈퍼유저 권한이 있어야 합니다.

자원 그룹이 현재 어떤 노드에서 실행 중인지("online") 확인하려면 scstat 명령을 사용합니다. 예를 들어 자원 그룹이 mail-1에서 온라인인 경우 다음 명령을 사용하여 mail-2로 페일오버합니다.

```
# scswitch -z -g MAIL-RG -h mail-2
```

첫 번째 노드를 업그레이드하는 경우 Java Enterprise System 설치 프로그램을 통해 설치한 다음 Messaging Server를 구성합니다. 그런 다음 Java Enterprise System 설치 프로그램을 통해 Messaging Server 패키지를 설치할 두 번째 노드로 페일오버합니다. 하지만 초기 런타임 구성 프로그램(configure)을 다시 실행할 필요는 없습니다. 대신 useconfig 유틸리티를 사용할 수 있습니다.

## 서버에서 IP 주소 바인딩

대칭형 또는 N + 1 고가용성 모델을 사용하는 경우 Sun Cluster Server를 Messaging Server와 함께 사용하기 위해 준비하려면 구성 과정에서 알아야 할 몇 가지 사항이 있습니다.

서버에서 실행 중인 Messaging Server에 올바른 IP 주소를 바인딩해야 합니다. 이는 HA 환경에서 Messaging Server를 제대로 구성하기 위해 필요합니다.

HA를 위해 Messaging Server를 구성하려면 Messaging Server가 바인딩하고 연결을 수신하는 인터페이스 주소를 구성해야 합니다. 기본적으로 서버는 사용 가능한 모든 인터페이스 주소에 바인딩합니다. 하지만 HA 환경에서는 서버가 HA 논리 호스트 이름과 연관된 인터페이스 주소에 바인딩되도록 해야 합니다.

따라서 특정 Messaging Server 인스턴스에 속한 서버가 사용하는 인터페이스 주소를 구성하기 위한 스크립트가 제공됩니다. 이 스크립트는 현재 IP 주소 또는 서버가 사용하는 HA 논리 호스트 이름과 연관될 IP 주소를 통해 인터페이스 주소를 식별합니다.

스크립트는 다음 구성 파일을 수정하거나 만들어서 구성을 변경합니다. 다음 파일의 경우 `msg_svr_base/config/dispatcher.cnf`

SMTP 및 SMTP Submit 서버의 `INTERFACE_ADDRESS` 옵션을 추가하거나 변경합니다. 다음 파일의 경우

`msg_svr_base/config/job_controller.cnf`

Job Controller의 `INTERFACE_ADDRESS` 옵션을 추가하거나 변경합니다.

마지막으로 POP, IMAP 및 Messenger Express HTTP 서버에서 사용하는 `configutil service.listenaddr` 및 `service.http.smtphost` 매개 변수를 설정합니다.

원본 구성 파일이 있는 경우 해당 파일의 이름은 `*.pre-ha`로 변경됩니다.

스크립트를 다음과 같이 실행합니다.

1. 슈퍼유저가 됩니다.
2. `msg_svr_base/sbin/ha_ip_config`를 실행합니다.
3. 스크립트에서는 아래와 같은 질문을 합니다. 질문에 대해 `control-d`를 입력하여 응답하면 스크립트 실행이 중단될 수 있습니다. 질문에 대한 기본 답변은 대괄호 [ ] 안에 나타냅니다. 기본 답변을 사용하려면 Enter 키를 누릅니다.
  - a. Logical IP address: Messaging Server에서 논리 호스트 이름에 할당되는 IP 주소를 지정합니다. IP 주소는 123.456.78.90과 같이 점으로 구분된 십진수 형식으로 지정해야 합니다.

논리적 IP 주소는 `configutil` 매개 변수 `service.http.smtphost`에서 자동으로 설정되며 클러스터의 메시징 시스템이 현재 어떤 시스템에서 실행 중인지 확인할 수 있게 해줍니다. 예를 들어 Messenger Express를 사용하는 경우 서버는 보내는 메일을 전송할 메일 호스트를 결정할 수 있습니다.

- b. Messaging Server Base(*msg\_svr\_base*): Messaging Server가 설치되는 최상위 디렉토리의 절대 경로를 지정합니다.
- c. Do you wish to change any of the above choices: 답변을 그대로 적용하고 구성을 변경하려면 "no"로 답합니다. 답변을 변경하려면 "yes"로 답합니다.

---

**주** 또한 `ha_ip_config` 스크립트는 두 개의 새 프로세스인 `watcher`와 `msprobe` 그리고 매개 변수 `local.autorestart`와 `local.watcher.enable`을 자동으로 활성화합니다. 이 새 매개 변수는 Messaging Server의 상태를 모니터링하는 데 도움이 됩니다. 프로세스가 실패하거나 서비스가 응답하지 않으면 해당 오류를 나타내는 로그 메시지가 생성됩니다. 이제 클러스터 에이전트는 종료될 때마다 `watcher` 프로세스와 페일오버를 모니터링합니다. Sun Cluster가 제대로 작동하려면 매개 변수를 활성화해야 합니다.

`watcher` 및 `msprobe` 프로세스에 대한 자세한 내용은 110페이지의 "실패했거나 응답이 없는 서비스의 자동 재시작"을 참조하십시오.

---

## 고가용성 구성 해제

이 절에서는 고가용성의 구성을 해제하는 방법에 대해 설명합니다. 고가용성을 해제하려면 Veritas 또는 Sun Cluster 설명서의 지침을 따르십시오.

고가용성을 구성 해제하는 방법은 Veritas Cluster Server 또는 Sun Cluster 중 어떤 것을 제거하는지에 따라 달라집니다.

다음 항목에 대해 설명합니다.

- 99페이지의 "Veritas Cluster Server 구성 해제"
- 100페이지의 "Sun Cluster 3.x에 대한 Messaging Server HA 지원 구성 해제"

## Veritas Cluster Server 구성 해제

Veritas Cluster Server에 대한 고가용성 구성 요소를 구성 해제하려면 다음을 수행합니다.

1. `iMS5` 서비스 그룹을 오프라인으로 만들고 해당 그룹의 자원을 비활성화합니다.

2. mail 자원, logical\_IP 자원 및 mountshared 자원 간의 종속성을 제거합니다.
3. iMS5 서비스 그룹을 다시 온라인 상태로 전환하여 sharedg 자원을 사용할 수 있도록 합니다.
4. 설치 도중 생성된 모든 Veritas Cluster Server 자원을 삭제합니다.
5. Veritas Cluster Server를 중지하고 두 노드에서 다음 파일을 제거합니다.

```
/etc/VRTSvcs/conf/config/MsgSrvTypes.cf  
/opt/VRTSvcs/bin/MsgSrv/online  
/opt/VRTSvcs/bin/MsgSrv/offline  
/opt/VRTSvcs/bin/MsgSrv/clean  
/opt/VRTSvcs/bin/MsgSrv/monitor  
/opt/VRTSvcs/bin/MsgSrv/sub.pl
```

6. 두 노드의 /etc/VRTSvcs/conf/config/main.cf 파일에서 Messaging Server 항목을 제거합니다.
7. 두 노드에서 /opt/VRTSvcs/bin/MsgSrv/ 디렉토리를 제거합니다.

## Sun Cluster 3.x에 대한 Messaging Server HA 지원 구성 해제

이 절에서는 Sun Cluster에 대한 HA 구성을 취소하는 방법에 대해 설명합니다. 간단한 구성 예(92페이지의 "Sun Cluster 에이전트 설치"에서 설명)를 가정하여 설명합니다. 다른 구성에 대해서는 특정 명령(예: 단계 3)이 다를 수 있지만 논리적 순서는 같습니다.

1. 슈퍼유저가 됩니다.

다음 Sun Cluster 명령을 사용하려면 슈퍼유저가 되어야 합니다.

2. 자원 그룹을 오프라인 상태로 만듭니다.

자원 그룹의 모든 자원을 종료하려면 다음 명령을 실행합니다.

```
# scswitch -F -g MAIL-RG
```

이렇게 하면 자원 그룹 내의 모든 자원(예: Messaging Server 및 HA 논리 호스트 이름)이 종료됩니다.

**3.** 개별 자원을 비활성화합니다.

그런 다음, 아래 명령을 사용하여 자원 그룹에서 자원을 하나씩 제거합니다.

```
# scswitch -n -j mail-rs
# scswitch -n -j disk-rs
# scswitch -n -j budgie
```

**4.** 자원 그룹에서 개별 자원을 제거합니다.

자원이 비활성화되면 다음 명령으로 자원 그룹에서 자원을 하나씩 제거할 수 있습니다.

```
# scrgadm -r -j mail-rs
# scrgadm -r -j disk-rs
# scrgadm -r -j budgie
```

**5.** 자원 그룹을 제거합니다.

자원 그룹에서 모든 자원이 제거되면 다음 명령으로 자원 그룹 자체를 제거할 수 있습니다.

```
# scrgadm -r -g MAIL-RG
```

**6.** 자원 유형을 제거합니다(선택 사항).

클러스터에서 자원을 제거해야 하는 경우 다음 명령을 실행합니다.

```
# scrgadm -r -t SUNW.ims
# scrgadm -r -t SUNW.HAStoragePlus
```

고가용성 구성 해제

## 일반 메시징 기능 구성

이 장에서는 서비스의 시작과 중지 및 디렉토리 액세스 구성 등과 같은 일반적인 Messaging Server 작업에 대해 설명합니다. 이런 작업은 Sun ONE Server Console(이하 콘솔)을 사용하거나 명령줄 유틸리티를 사용하여 수행할 수 있습니다. 개별 Messaging Server 서비스에 한정된 작업(POP, IMAP, HTTP 및 SMTP)은 다음 장에서 설명합니다. 이 장은 다음 내용으로 구성되어 있습니다.

- 104페이지의 "비밀번호 수정"
- 105페이지의 "메일 사용자, 메일 목록 및 도메인 관리"
- 106페이지의 "Sun ONE 콘솔로 Messaging Server 관리"
- 107페이지의 "서비스 시작 및 중지"
- 110페이지의 "실패했거나 응답이 없는 서비스의 자동 재시작"
- 113페이지의 "자동 작업 예약"
- 114페이지의 "인사 메일 구성"
- 117페이지의 "사용자 기본 언어 설정"
- 118페이지의 "디렉토리 조회 사용자 정의"
- 122페이지의 "암호화 설정"
- 122페이지의 "페일오버 LDAP 서버 설정"

## 비밀번호 수정

동일한 비밀번호를 사용하여 여러 관리자를 설정했기 때문에(51페이지의 "[Messaging Server 초기 런타임 구성 만들기](#)" 참조) 각 관리자의 비밀번호를 변경해야 합니다.

표 4-1에는 초기 런타임 구성 시 설정된 기본 비밀번호의 매개 변수와 이를 변경하기 위해 사용할 수 있는 유틸리티가 나열되어 있습니다. `configutil` 유틸리티를 사용하여 비밀번호를 변경하는 매개 변수에 대해서는 전체 구문 및 사용법을 참조하십시오.

**표 4-1** Messaging Server 초기 런타임 구성 시 설정된 비밀번호

매개 변수	설명
<code>local.ugldapbindcred</code>	<code>configutil</code> 유틸리티를 통해 설정된 사용자/그룹 관리자의 비밀번호입니다.
<code>local.service.pab.ldappasswd</code>	<code>configutil</code> 유틸리티를 통해 설정된 PAB 검색용 바인드 DN에 의해 지정된 사용자의 비밀번호입니다.
키 파일의 SSL 비밀번호	<code>sslpassword.conf</code> 파일에 직접 설정된 비밀번호입니다.
서비스 관리자 자격 증명	LDAP 디렉토리에 직접 설정된 자격 증명입니다 (ldapmodify 명령 사용).
Delegated Administrator에 대한 서비스 관리자	Sun LDAP Schema 1을 활성화했고 iPlanet Delegated Administrator 유틸리티를 사용하는 경우 이 관리자의 비밀번호만 변경하면 됩니다.  Delegated Administrator 서비스 관리자의 비밀번호를 변경하려면 Sun ONE 콘솔, LDAP 디렉토리 (ldapmodify 명령 사용) 또는 Delegated Administrator UI에서 변경할 수 있습니다.
저장소 관리자	저장소 관리자의 비밀번호를 변경하려면 Sun ONE 콘솔 또는 LDAP 디렉토리(ldapmodify 명령 사용)에서 변경할 수 있습니다.

다음 예에서는 `local.enduseradmincred` `configutil` 매개 변수를 사용하여 최종 사용자 관리자의 비밀번호를 변경합니다.

```
configutil -o local.enduseradmincred -v newpassword
```



## 메일 사용자, 메일 목록 및 도메인 관리

모든 사용자 및 메일 목록 정보는 LDAP 디렉토리에 항목으로 저장됩니다. LDAP 디렉토리에는 조직의 직원, 구성원, 클라이언트 또는 조직에 여러 방법으로 속해 있는 다양한 유형의 개인에 대한 광범위한 정보가 포함되어 있습니다. 이러한 개인들이 조직의 사용자를 구성합니다.

LDAP 디렉토리에서 사용자에 대한 정보는 효율적인 검색을 위해 구조화되어 있으며 각 사용자 항목은 속성 집합으로 식별됩니다. 사용자와 연관된 디렉토리 속성에는 사용자 아이디와 기타 아이디, 부서, 작업 분류, 물리적 위치, 관리자 이름, 직접 보고자 이름, 조직의 각 부분에 대한 액세스 권한 및 기타 여러 기본 설정 등이 포함될 수 있습니다.

전자 메시징 서비스를 갖춘 조직에서는 대부분의 사용자가 메일 계정을 보유하고 있습니다. Messaging Server의 경우 메일 계정 정보는 서버에 로컬로 저장되는 것이 아니라 LDAP 사용자 디렉토리의 일부입니다. 각 메일 계정에 대한 정보는 디렉토리의 사용자 항목에 첨부된 메일 속성으로 저장됩니다.

메일 사용자와 메일 목록을 만들고 관리하는 작업은 디렉토리에서 사용자와 메일 목록 항목을 만들고 수정하는 작업으로 구성됩니다. 이 작업은 Sun LDAP Schema 2용 Delegated Administrator 및 메시징용 iPlanet Delegated Administrator(Sun LDAP Schema 1용), Delegated Administrator 명령줄 유틸리티를 사용하거나 Sun LDAP Schema 1용 LDAP 디렉토리를 직접 수정하는 방식으로 수행합니다.

## Messaging Server에서 사용자 제거

1. `commadmin user delete` 명령을 실행하여 사용자가 삭제된 것으로 표시합니다. *Sun Java System Communications Services Delegated Administrator 설명서* (<http://docs.sun.com/doc/819-1102>)를 참조하십시오.

2. 사용자로부터 서비스를 제거합니다.

서비스는 메일함 또는 달력일 수 있습니다. Messaging Server에서는 이 프로그램을 `msuserpurge`라 합니다. *Sun Java System Messaging Server Administration Reference*(<http://docs.sun.com/doc/819-0106>)를 참조하십시오. 달력 서비스에서는 프로그램이 `csclean`입니다. *Sun Java System Calendar Server 관리 설명서* (<http://docs.sun.com/doc/819-1477>)를 참조하십시오.

3. `commadmin domain purge` 명령을 호출하여 사용자를 영구히 제거합니다.

## Messaging Server에서 도메인 제거

1. `commadmin domain delete` 명령을 실행하여 도메인이 삭제된 것으로 표시합니다. *Sun Java System Communications Services Delegated Administrator 설명서* (<http://docs.sun.com/doc/819-1102>)를 참조하십시오.
2. 해당 도메인의 사용자로부터 서비스를 제거합니다.  
서비스는 메일함 또는 달력일 수 있습니다. Messaging Server에서는 이 프로그램을 `msuserpurge`라 합니다. *Sun Java System Messaging Server Administration Reference* (<http://docs.sun.com/doc/819-0106>)를 참조하십시오. 달력 서비스에서는 프로그램이 `csclean`입니다. *Sun Java System Calendar Server 관리 설명서* (<http://docs.sun.com/doc/819-1477>)를 참조하십시오.
3. `commadmin domain purge` 명령을 호출하여 도메인을 영구히 제거합니다.

## Sun ONE 콘솔로 Messaging Server 관리

Messaging Server 설치 프로세스 및 초기 런타임 구성 프로그램이 끝나면 관리 콘솔을 통해 Messaging Server를 시작할 수 있습니다. Directory Server와 Messaging Server가 한 시스템에 있는 경우 콘솔 인터페이스를 사용하여 두 서버를 모두 관리할 수 있습니다.

콘솔을 시작하려면 `/var/opt/mps/serverroot/startconsole` 명령을 실행하십시오.

Sun ONE Server Console에서 해당 정보 양식을 보면 현재 설치되어 있는 Messaging Server의 기본 정보 일부를 검토할 수 있습니다.

정보 양식을 표시하려면 다음을 수행합니다.

1. 콘솔에서 정보를 보고자 하는 Messaging Server를 엽니다.
2. 왼쪽 창에서 해당 서버의 아이콘을 선택합니다.
3. 왼쪽 창에서 구성 탭을 누릅니다.
4. 오른쪽 창에서 정보 탭이 맨 앞에 있지 않으면 이 탭을 누릅니다.

정보 양식이 나타납니다. 여기에는 서버 이름, 서버 루트 디렉토리, 설치 디렉토리 및 인스턴스 디렉토리가 표시됩니다.

# 서비스 시작 및 중지

서비스는 HA 환경에 설치되었는지 여부에 따라 다른 방식으로 시작 및 중지됩니다.

## HA 환경에서 서비스 시작 및 중지

Messaging Server가 HA 제어 하에 실행 중일 때는 일반적인 Messaging Server 시작, 다시 시작 및 중지 명령으로 개별 Messaging Server 서비스를 제어할 수 없습니다. HA 환경에서 stop-msg를 시도하면 시스템에는 HA 설정이 감지되었다는 경고 메시지와 함께 시스템을 올바르게 중지하는 방법을 알려줍니다.

시작, 중지 및 다시 시작 명령은 아래 표에서 볼 수 있습니다. 다른 Messaging Server 서비스(예: SMTP)를 개별적으로 시작, 다시 시작 또는 중지시키는 특정 HA 명령은 없습니다. 하지만 stop-msg service 명령을 실행하여 imap, pop 또는 sched 등의 개별 서비스를 중지 및 다시 시작할 수 있습니다.

Sun Cluster에서는 개별 자원을 세부적으로 제어할 수 있습니다. Sun Cluster는 Messaging Server를 자원으로 인식하기 때문에 scswitch 명령은 모든 Messaging Server 서비스에 적용됩니다.

**표 4-2** Sun Cluster 3.0/3.1 환경에서 시작, 중지, 다시 시작

작업	개별 자원	전체 자원 그룹
시작	scswitch -e -j resource	sscswitch -Z -g resource_group
다시 시작	scswitch -n -j resource scswitch -e -j resource	scswitch -R -g resource_group
중지	scswitch -n -j resource	scswitch -F -g resource_group

**표 4-3** Veritas 1.3, 2.0, 2.1 및 3.5 환경에서 시작, 중지, 다시 시작

작업	개별 자원	전체 자원 그룹
시작	hares -online resource -sys system	hagr -online group -sys system
다시 시작	hares -offline resource -sys system hares -online resource -sys system	hagr -offline group -sys system hagr -online group -sys system
중지	hares -offline resource -sys system	hagr -offline group -sys system

## HA가 아닌 환경에서 서비스 시작 및 중지

콘솔이나 명령줄에서 서비스를 시작 및 중지할 수 있습니다. 또한 서버가 실제로 사용할 서비스만 실행하면 됩니다. 예를 들어, **Messaging Server**를 메시지 전송 에이전트(MTA)로만 사용하는 경우에는 MTA만 켤 수 있습니다. 또는 유지 관리, 보수 또는 보안상의 이유로 인해 서버를 종료해야 하는 경우 영향을 받는 서비스만 끌 수 있습니다. 특정 서비스를 실행하지 않으려면 해당 서비스를 끄는 대신 비활성화해야 합니다.

---

**주** POP, IMAP 및 HTTP 등의 서비스를 시작하거나 중지하려면 먼저 해당 서비스들을 활성화해야 합니다. 자세한 내용은 [124페이지의 "서비스 사용 가능/불가능하게 하기"](#)를 참조하십시오.

---

**중요:** 서버 프로세스가 충돌하는 경우 충돌한 서버 프로세스에 의한 잠금을 기다리고 있는 다른 프로세스도 중지될 수 있습니다. 자동 재시작([110페이지의 "실패했거나 응답이 없는 서비스의 자동 재시작"](#) 참조)을 사용하지 않는 경우 서버 프로세스가 충돌하면 모든 프로세스를 중지시킨 다음 모든 프로세스를 다시 시작해야 합니다. 여기에는 stored(메시지 저장소) 프로세스, mboxutil, deliver, reconstruct, readership 또는 upgrade 등과 같이 메시지 저장소를 수정하는 모든 유틸리티와 POP, IMAP, HTTP 및 MTA 프로세스가 포함됩니다.

**콘솔:** 콘솔은 개별 서비스를 시작 및 중지하고 각 서비스에 대한 상태 정보를 볼 수 있는 양식을 제공합니다.

각 서비스(IMAP, POP, SMTP 및 HTTP)에 대해 이 형식에서는 서비스의 현재 상태(켜짐 또는 꺼짐)가 표시됩니다. 서비스가 실행 중인 경우 해당 형식에는 서비스가 마지막으로 시작된 시간이 표시되며 기타 상태 정보도 표시됩니다.

메시징 서비스를 시작, 종료하거나 상태에 대한 자세한 내용은 다음을 수행합니다.

1. 콘솔에서 시작 또는 중지하려는 서비스가 있는 **Messaging Server**를 엽니다.
2. 다음 두 방법 중 하나를 사용하여 서비스 일반 구성 양식으로 이동합니다.
  - a. 태스크 탭을 누른 다음 "서비스 시작/중지"를 누릅니다.
  - b. 구성 탭을 누르고 왼쪽 표시 영역에서 서비스 폴더를 엽니다. 그런 다음 오른쪽 창에서 일반 탭을 누릅니다.

3. 서비스 일반 구성 양식이 나타납니다.

프로세스 제어 필드의 왼쪽 열에는 서버가 지원하는 서비스 목록이 표시되며, 오른쪽 열에는 각 서비스의 기본 상태(켜짐 또는 꺼짐, 켜짐 상태인 경우에는 마지막으로 시작된 시간)가 표시됩니다.

4. 현재 실행 중인 서비스에 대한 상태 정보에 대한 자세한 내용은 프로세스 제어 필드에서 서비스를 선택합니다.

서비스 상태 필드에는 서비스에 대한 상태 정보가 표시됩니다.

POP, IMAP 및 HTTP의 경우 마지막 연결 시간, 총 연결 수, 현재 연결 수, 서비스 시작 후 실패한 연결 수 및 서비스 시작 후 실패한 로그인 수가 필드에 표시됩니다.

이 필드의 정보를 사용하면 서버의 로드와 해당 서비스 안정성 및 서버의 보안에 영향을 미치는 공격을 파악할 수 있습니다.

5. 서비스를 켜려면 프로세스 제어 필드에서 해당 서비스를 선택하고 시작을 누릅니다.

6. 서비스를 끄려면 서비스 제어 필드에서 해당 서비스를 선택하고 중지를 누릅니다.

7. 활성화된 모든 서비스를 동시에 켜거나 끄려면 모두 시작 또는 모두 중지 버튼을 누릅니다.

**명령줄:** start-msg 및 stop-msg 명령을 사용하여 메시징 서비스(smtp, imap, pop, store, http, ens, sched)를 시작하거나 중지할 수 있습니다. 예를 들면 다음과 같습니다.

```
msg_svr_base/sbin/start-msg imap
msg_svr_base/sbin/stop-msg pop
msg_svr_base/sbin/stop-msg sched
msg_svr_base/sbin/stop-msg smtp
```

서비스를 시작하거나 중지하려면 먼저 해당 서비스를 활성화해야 합니다. [110페이지의 "시작할 서비스 지정"](#)을 참조하십시오.

---

**주** start-msg smtp와 stop-msg smtp 명령은 SMTP 서버뿐 아니라 모든 MTA 서비스를 시작 및 중지합니다. MTA 서비스를 시작하거나 중지할 때 보다 세부적으로 제어하려면 디스패처 및 Job Controller에 대해 stoart/stop msg 명령을 사용할 수 있습니다. 자세한 내용은 *Messaging Server Reference Manual*을 참조하십시오.

---

## 시작할 서비스 지정

기본적으로 다음 서비스는 start-msg를 사용하여 시작합니다.

```
# ./start-msg
Connecting to watcher ...
Launching watcher ...
Starting ens server .... 21132
Starting store server .... 21133
checking store server status ... ready
Starting imap server .... 21135
Starting pop server .... 21138
Starting http server .... 21141
Starting sched server .... 21143
Starting dispatcher server .... 21144
Starting job_controller server .... 21146
```

이러한 서비스는 configutil 매개 변수인 service.imap.enable, service.pop.enable, service.http.enable, local.msggateway.enable, local.snmp.enable, local.imta.enable, local.mmp.enable, local.ens.enable 및 local.sched.enable을 활성화하거나 비활성화하여 제어할 수 있습니다. IMAP를 비활성화하려면 service.imap.enable 및 service.imap.enablesslport를 둘 다 0으로 설정해야 합니다. POP 및 HTTP의 경우에도 마찬가지입니다. 자세한 내용은 *Sun Java System Messaging Server Administration Reference*를 참조하십시오.

## 실패했거나 응답이 없는 서비스의 자동 재시작

Messaging Server는 서비스를 투명하게 모니터링하고 서비스가 실패하거나 응답하지 않을 경우 즉, 서비스가 중지된 경우 서비스를 자동으로 다시 시작하는 watcher 및 msprobe라는 두 개의 프로세스를 제공합니다. watcher는 서버 실패를 모니터링하고 msprobe는 서버 응답 시간을 검사하여 서버 중단을 모니터링합니다. 서버가 실패하거나 요청에 대한 응답이 중지되면 자동으로 다시 시작됩니다. 표 4-4를 참조하십시오.

**표 4-4** watcher 및 msprobe에서 모니터링하는 서비스

watcher(크래시)	msprobe(응답하지 않은 보류)
IMAP, POP, HTTP, Job Controller, 디스패처, 메시지 저장소(stored), imsched, MMP. LMTP/SMTP 서버는 디스패처가 모니터링하며 LMTP/SMTP 클라이언트는 job_controller가 모니터링합니다.	IMAP, POP, HTTP, Job Controller, 메시지 저장소(stored), imsched, ENS, LMTP, SMTP

`local.watcher.enable=on`(기본값)으로 설정하면 프로세스 실패와 응답하지 않는 서비스를 모니터링하여 특정 실패를 나타내는 default 로그 파일에 오류 메시지를 기록합니다. 자동 서버 재시작을 활성화하려면 `configutil` 매개 변수 `local.autorestart`를 `yes`로 설정합니다. 기본적으로 이 매개 변수는 `no`로 설정됩니다.

메시지 저장소 서비스 중 하나가 실패하거나 중지되면 시작 시 활성화된 모든 메시지 저장소 서비스가 다시 시작됩니다. 예를 들어 `imapd`가 실패하면 적어도 `stored`와 `imapd`가 다시 시작됩니다. POP 또는 HTTP 서버 등의 다른 메시지 저장소 서비스가 실행 중인 경우 해당 서비스는 그 실패 여부와 관계 없이 다시 시작됩니다.

메시지 저장소 유틸리티가 실패하거나 중지되어도 자동 재시작이 작동합니다. 예를 들어 `mboxutil`이 실패하거나 중지되면 시스템은 모든 메시지 저장소 서버를 자동으로 다시 시작합니다. 하지만 유틸리티는 다시 시작하지 않습니다. `msprobe`는 10분마다 실행됩니다. 서비스 및 프로세스 재시작은 10분 내에 최대 두 번 수행됩니다 (`local.autorestart.timeout`을 사용하여 구성 가능).

`local.autorestart`의 `yes` 설정 여부에 관계 없이 시스템은 서비스를 모니터링하여 실패 또는 무응답 오류 메시지를 해당 콘솔로 전송하고 `msg_svr_base/data/log/watcher`는 기본 포트 49994를 통해 수신하지만 `local.watcher.port`를 사용하여 구성할 수도 있습니다.

`watcher` 로그 파일은 `msg_svr_base/data/log/watcher`에 생성됩니다. 이 로그 파일은 로깅 시스템(롤오버 또는 제거)에서 관리하는 것이 아니며 모든 서버의 시작과 중지를 기록합니다. 로그 예는 다음과 같습니다.

```
watcher process 13425 started at Tue Oct 21 15:29:44 2003

Watched 'imapd' process 13428 exited abnormally
Received request to restart: store imap pop http
Connecting to watcher ...
Stopping http server 13440 .... done
Stopping pop server 13431 ... done
Stopping pop server 13434 ... done
Stopping pop server 13435 ... done
Stopping pop server 13433 ... done
imap server is not running
Stopping store server 13426 .... done
Starting store server .... 13457
checking store server status ..... ready
Starting imap server ..... 13459
Starting pop server ..... 13462
Starting http server ..... 13471
```

이 기능을 구성하는 방법에 대한 자세한 내용은 [824페이지의 "msprobe 및 watcher 기능을 사용하여 모니터링"](#)을 참조하십시오.

msprobe는 imsched로 제어됩니다. imsched가 충돌하면 watcher에서 이 이벤트를 검색하여 다시 시작(autorestart이 사용 가능한 경우)을 트리거합니다. 드물기는 하지만 imsched가 보류되는 경우 watcher에서 다시 시작하도록 하는 kill *imsched\_pid*를 사용하여 imsched를 중지해야 할 수 있습니다.

## 고가용성 배포 시 자동 재시작

고가용성 배포 시 자동 재시작 기능을 사용하려면 다음 configutil 매개 변수를 설정해야 합니다.

**표 4-5** HA 자동 재시작 매개 변수

매개 변수	설명/HA 값
local.watcher.enable	watcher를 활성화합니다. 기본값은 On입니다.
local.autorestart	autorestart를 활성화합니다. (On)



**표 4-5** HA 자동 재시작 매개 변수

매개 변수	설명/HA 값
<code>local.autorestart.time out</code>	재시도 시간 초과 오류. 지정된 시간 내에 서버가 세 번 이상 실패하면 시스템은 서버 재시작 시도를 중지합니다. HA 시스템에서 이런 상황이 발생하면 Messaging Server가 종료되고 다른 시스템으로 페일오버됩니다. 이 값(초)은 msprobe 간격( <code>local.schedule.msprobe</code> )보다 길게 설정해야 합니다.
<code>local.schedule.msprobe</code>	msprobe에서 일정을 실행합니다. crontab 스타일 일정 문자열( <a href="#">592페이지의 표 18-10</a> 참조)로 기본값은 600초입니다.

## 자동 작업 예약

Messaging Server에서는 imsched라는 프로세스를 사용한 일반 작업 예약 기법을 제공합니다. 이는 Messaging Server 프로세스를 예약하기 위한 것입니다. Messaging Server 작업이 아닌 작업은 예약할 수 없습니다. 이 기능은 `local.schedule.taskname` configutil 매개 변수를 설정하여 활성화됩니다. 스케줄을 수정하려면 `stop-msg sched` 및 `start-msg sched` 명령을 사용하여 스케줄러를 다시 시작해야 합니다. 스케줄러 프로세스를 갱신(`refresh sched`)할 수도 있습니다.

이 매개 변수에는 명령과 해당 명령을 실행할 일정이 필요합니다. 형식은 다음과 같습니다.

```
configutil -o local.schedule.taskname -v "schedule"
```

*taskname*은 이 명령/일정 조합의 고유 이름입니다.

*schedule*의 형식은 다음과 같습니다.

```
minute hour day-of-month month-of-year day-of-week command args
```

*command args*는 Messaging Server 명령과 그 인수일 수 있습니다. 정규화된 명령 경로 이름이 필요합니다.

*minute hour day-of-month month-of-year day-of-week*는 명령을 실행하는 일정입니다. UNIX crontab의 형식을 따릅니다.

값은 공백이나 탭으로 구분하며 각각 0-59, 0-23, 1-31, 1-12 또는 0-6(0=일요일)의 값을 사용할 수 있습니다. 각 시간 필드에는 별표(유효한 모든 값), 쉼표로 구분된 값 목록 또는 하이픈으로 구분된 두 값의 범위를 사용할 수 있습니다. 일에는 한 달의 숫자와 요일을 모두 사용할 수 있으며 지정된 경우에는 둘 다 필요합니다. 예를 들어, 17일과 화요일로 설정하면 명령은 17일, 화요일에만 실행됩니다. 일정 매개 변수 설정 방법에 대해서는 [592페이지의 표 18-10](#)을 참조하십시오.

스케줄러를 수정한 경우 stop-msg sched 및 start-msg sched 명령을 사용하여 스케줄러를 다시 시작하거나 다음 스케줄러 프로세스에 SIGHUP을 보낼 수 있습니다.

```
kill -HUP scheduler_pid
```

## 스케줄러의 예

imexpire를 세부 정보 표시 모드로 오전 12시 30분, 오전 8시 30분 및 오후 4시 30분에 실행합니다.

```
configutil -o local.schedule.rm_messages -v 30 0,8,16 * * * *  
/opt/SUNWmsgsr/sbin/imexpire -v
```

20분마다 MTA 채널 대기열 메일 카운터를 표시합니다.

```
configutil -o local.schedule.counters -v 20,40,60 * * * * *  
/opt/SUNWmsgsr/sbin/imsimta qm counters -show > temp.txt
```

월요일부터 금요일까지 오전 12시에 imsbackup을 실행합니다.

```
configutil -o local.schedule.msbackup -v "0 0 * * 1-5"  
/opt/SUNWmsgsr/sbin/imsbackup -f backupfile /primary
```

# 인사 메일 구성

Messaging Server에서는 새 사용자에게 보낼 전자 메일 인사 메시지를 작성할 수 있습니다.

**콘솔.** 콘솔을 사용하여 새 사용자 인사 메일을 만들려면 다음을 수행합니다.

1. 콘솔에서 구성할 새 사용자 인사 메일이 있는 Messaging Server를 엽니다.
2. 구성 탭을 누릅니다. 왼쪽 창에 있는 서버의 아이콘이 아직 강조 표시되어 있지 않으면 이를 선택합니다.
3. 오른쪽 표시 영역에서 기타 탭을 누릅니다.
4. 새 사용자 인사 메일을 만들거나 필요에 따라 변경합니다.

인사 메일은 전자 메일과 같은 형식으로 만듭니다. 즉 최소한 제목 행을 포함하는 헤더, 빈 행 그리고 메시지 본문으로 구성합니다.

메일을 만들 때는 메일 필드 위에 있는 드롭다운 목록을 사용하여 해당 언어를 지정합니다. 원하는 경우 여러 언어로 여러 메일을 만들 수 있습니다.

5. 저장을 누릅니다.

**명령줄:** 명령줄을 사용하여 새 사용자 인사 메일을 만듭니다.

```
configutil -o gen.newuserforms -v Message
```

여기서 *Message*는 최소한 제목 행이 들어있는 헤더를 포함하고 그 뒤에 \$\$와 메일 본문이 와야 합니다. \$는 새 행을 나타냅니다.

예를 들어, 이 매개 변수를 활성화하려면 다음 구성 변수를 설정해야 합니다.

```
configutil -o gen.newuserforms -v "Subject: Welcome!! $$ Sesta.com welcomes  
you to the premier internet experience in Dafandzadgad!"
```

사용 중인 셸에 따라 \$의 특수한 의미를 이스케이프하기 위해 \$ 앞에 특수 문자를 추가해야 할 수 있습니다. \$는 일반적으로 해당 셸의 이스케이프 문자입니다.

## 도메인별 인사 메일 설정

호스팅된 새 도메인을 만들 때마다 지원되는 언어에 대한 도메인별 인사 메일을 만드는 것이 좋습니다. 그렇지 않을 경우 gen.newuserforms에 의해 설정된 일반 인사 메일이 보내집니다.

각 도메인의 새 사용자에게 대해 인사 메일을 설정할 수 있습니다. 인사 메일은 사용자, 도메인 또는 사이트의 기본 언어에 따라 달라질 수 있습니다. 이 작업은 원하는 LDAP 도메인 항목에서 mailDomainWelcomeMessage 속성을 설정하여 수행합니다. 속성 구문은 다음과 같습니다.

```
mailDomainWelcomeMessage;lang-user_prefLang  
mailDomainWelcomeMessage;lang-domain_prefLang  
mailDomainWelcomeMessage;lang-gen.sitelanguage
```

다음 예는 영어를 사용하는 도메인 시작 메일을 설정합니다.

```
mailDomainWelcomeMessage;lang-en: Subject: Welcome!! $$Welcome to the mail  
system.
```

다음 예는 프랑스어를 사용하는 도메인 시작 메일을 설정합니다.

```
mailDomainWelcomeMessage;lang-fr: Subject: Bienvenue!! $$Bienvenue a  
siroe.com!
```

위의 예를 사용할 때 다음을 가정합니다.

- 도메인은 siroe.com임
- 이 도메인에 새 사용자가 소속됨
- 이 사용자의 기본 언어는 LDAP 속성 preferredlanguage에서 지정한 대로 프랑스어임

- siroe.com에서는 위의 영어 및 프랑스어 환영 메일을 사용할 수 있음
- 사이트 언어는 gen.sitelanguage에서 지정한 대로 en임

지원되는 로케일과 해당 언어 값 태그의 목록은 *Directory Server Reference Manual*([http://docs.sun.com/source/816-6699-10/ax\\_inter.html#18744](http://docs.sun.com/source/816-6699-10/ax_inter.html#18744))을 참조하십시오.

사용자가 처음 로그인하면 프랑스어 인사 메일을 받게 됩니다. 프랑스어 시작 메일을 사용할 수 없는 경우에는 영어 메시지가 사용됩니다.

## 인사 메일 작동 원리

인사 메일은 LDAP 속성 mailDomainWelcomeMessage와 configutil 매개 변수 gen.newuserforms를 둘 다 사용하여 설정할 수 있습니다. 다음은 메시지가 선택되는 순서를 가장 높은 우선 순위부터 보여 줍니다.

```
mailDomainWelcomeMessage;lang-user_prefLang
mailDomainWelcomeMessage;lang-domain_prefLang
mailDomainWelcomeMessage;lang-gen.sitelanguage
mailDomainWelcomeMessage
gen.newuserforms;lang-"$user_prefLang"
gen.newuserforms;lang-"$domain_prefLang"
gen.newuserforms;lang-"$gen.sitelanguage"
gen.newuserforms
```

알고리즘은 다음과 같이 실행됩니다. 도메인이 없는 경우(또는 도메인이 있더라도 도메인별 시작 메일이 제공되지 않는 경우)에는 gen.newuserforms 매개 변수로 시작 메일이 지정됩니다. 즉 사용자가 기본 언어를 설정하고(preferredlanguage LDAP 속성으로 설정) gen.newuserforms;lang-user\_prefLang이 설정되어 있으면 사용자가 서버에 처음 로그인할 때 해당 메일을 받게 됩니다. gen.newuserforms;lang-gen.sitelanguage가 설정되어 있고 preferredlanguage는 설정되어 있지 않지만 해당 사이트 언어가 설정된 경우(gen.sitelanguage 매개 변수 사용) 사용자는 해당 메일을 받게 됩니다. 언어 태그 매개 변수가 설정되지 않고 태그되지 않은 gen.newuserforms가 설정된 경우 해당 메일이 사용자에게 보내집니다. 위의 값 중 아무 것도 설정되지 않은 경우 사용자는 시작 메일을 받을 수 없습니다.

사용자가 도메인에 있다고 가정하면 위에 설명된 것과 같이 사용자는 다음 목록 중 사용 가능한 것에 따라 지정된 순서대로 mailDomainWelcomeMessage;lang-xx 중 하나를 받을 수 있습니다.

예를 들어, 도메인은 fantasia.com인 경우 도메인 기본 언어는 독일어(de)입니다. 하지만 이 도메인의 새 사용자 기본 언어는 터키어(tr)이고 사이트 언어는 영어입니다. 다음 값을 사용할 수 있습니다(mailDomainWelcomeMessage는 fantasia.com 도메인 속성).

```
mailDomainWelcomeMessage;lang-fr
mailDomainWelcomeMessage;lang-ja
gen.newuserforms;lang-de
gen.newuserforms;lang-en
gen.newuserforms
```

이 알고리즘에 따라 사용자에게 보내지는 메일은 `gen.newuserforms;lang-de`가 됩니다.

## 사용자 기본 언어 설정

관리자는 사용자의 LDAP 항목에서 `preferredLanguage` 속성을 설정하여 GUI와 서버 생성 메일에 사용할 기본 언어를 설정할 수 있습니다.

서버가 서버의 관리 도메인 외부에 있는 사용자에게 메일을 보내는 경우에는 받는 메일의 헤더에 지정된 기본 언어를 사용하여 응답하는 경우 이외에는 관리 도메인이 해당 사용자의 기본 언어를 알 수 없습니다. 헤더 필드(`accept-language`, `Preferred-Language` 또는 `X-Accept-Language`)는 사용자의 메일 클라이언트에 지정된 속성에 따라 설정됩니다.

기본 언어에 대해 여러 개의 설정이 있는 경우(예: 사용자에게 Directory Server에 저장된 기본 언어 설정도 있고 자신의 메일 클라이언트에 지정된 기본 언어도 있는 경우) 서버는 다음 순서로 기본 언어를 선택합니다.

1. 원본 메일의 `accept-language` 헤더 필드
2. 원본 메일의 `Preferred-Language` 헤더 필드
3. 원본 메일의 `X-Accept-Language` 헤더 필드
4. 보내는 사람의 기본 언어 속성(LDAP 디렉토리에 있는 경우)

## 도메인 기본 언어 설정

도메인 기본 언어는 특정 도메인에 대해 지정된 기본 언어입니다. 예를 들어, `mexico.siroe.com`이라는 도메인에 대해 스페인어를 지정하려 할 수 있습니다. 관리자는 도메인의 LDAP 항목에서 `preferredLanguage` 속성을 설정하여 도메인 기본 언어를 설정할 수 있습니다.

## 서버 사이트 언어 구성

다음과 같이 서버의 기본 사이트 언어를 지정할 수 있습니다. 사이트 언어는 사용자 기본 언어가 설정되어 있지 않은 경우 언어별 메일 버전을 보내는데 사용됩니다.

**콘솔:** 콘솔에서 사이트 언어를 지정하려면 다음을 수행합니다.

1. 구성할 Messaging Server를 엽니다.
2. 구성 탭을 누릅니다.
3. 오른쪽 영역에서 기타 탭을 누릅니다.
4. 사이트 언어 드롭다운 목록에서 사용할 언어를 선택합니다.
5. 저장을 누릅니다.

**명령줄:** 다음과 같이 명령줄에서 사이트 언어를 지정할 수도 있습니다.

```
configutil -o gen.sitelanguage -v value
```

여기서 *value*는 로컬 지원 언어 중 하나입니다. 지원되는 로케일과 언어 값 태그의 목록은 *Directory Server Reference Manual*

([http://docs.sun.com/source/816-6699-10/ax\\_inter.html#18744](http://docs.sun.com/source/816-6699-10/ax_inter.html#18744))을 참조하십시오.

## 디렉토리 조회 사용자 정의

Messaging Server는 Sun Java System Directory Server와 같은 LDAP 기반 디렉토리 시스템이 없는 작동되지 않습니다. Messaging Server와 콘솔에는 여러 가지 목적에 따라 디렉토리 액세스가 필요합니다. 예를 들면 다음과 같습니다.

- Messaging Server를 처음 설치할 때 서버에 대한 구성 설정을 입력합니다. 이 설정은 중앙 구성 디렉토리에 저장됩니다. 설치 프로세스에는 이 디렉토리에 대한 연결을 구성하는 작업도 포함됩니다.
- 메일 사용자 또는 메일 그룹의 계정 정보를 만들거나 업데이트할 때 해당 정보는 사용자 디렉토리라는 디렉토리에 저장됩니다. 서버 그룹의 Administration Server는 설치 시 구성되므로 사용자와 그룹에 액세스할 때 콘솔은 기본적으로 관리 토폴로지(모두 동일한 구성 디렉토리와 사용자 디렉토리를 공유하는 Sun Java System 서버 제품군)를 정의하는 사용자 디렉토리에 연결합니다.

- 메일을 메일함으로 경로 지정하고 메일함으로 전달할 때 Messaging Server는 사용자 디렉토리에서 보내는 사람이나 받는 사람에 대한 정보를 조회합니다. 기본적으로 Messaging Server는 Administration Server가 사용하도록 구성된 사용자 디렉토리에서 찾습니다.

- 메일 라우팅 조회에 대해 사용자를 인증할 때

다음과 같은 방법으로 각 디렉토리의 구성 설정을 수정할 수 있습니다.

- 콘솔의 Administration Server 인터페이스를 사용하여 구성 디렉토리의 연결 설정을 변경할 수 있습니다. 자세한 내용은 *Sun ONE Server Console 5.2 Server Management Guide*의 Administration Server 장을 참조하십시오.
- 콘솔의 사용자 및 그룹 인터페이스를 사용하면 사용자 및 그룹 정보를 변경할 때 기본값과 다른 사용자 디렉토리에 임시로 연결할 수 있습니다. 자세한 내용은 *Sun ONE Server Console 5.2 Server Management Guide*의 Users and Groups 장을 참조하십시오.
- 콘솔의 Messaging Server 인터페이스에서는 Messaging Server가 Administration Server에 의해 정의된 기본값과 다른 사용자 디렉토리에 연결하도록 구성할 수 있습니다. 이 작업이 이 절에서 설명하는 구성 작업입니다.

Messaging Server가 사용자 및 그룹 조회를 위해 다른 사용자 디렉토리에 연결하는 것은 선택 사항입니다. 일반적으로 서버의 관리 도메인을 정의하는 사용자 디렉토리는 도메인의 모든 서버가 사용하는 디렉토리입니다.

---

**주** Messaging Server 조회에 대해 사용자 정의 사용자 디렉토리를 지정하는 경우, 디렉토리의 사용자 또는 그룹 정보를 변경하기 위해 콘솔의 사용자 및 그룹 인터페이스에 액세스할 때마다 동일한 디렉토리를 지정해야 합니다.

---

**콘솔:** 콘솔을 사용하여 Messaging Server LDAP 사용자 조회 설정을 수정하려면 다음을 수행합니다.

1. 콘솔에서 사용자 정의할 LDAP 연결이 있는 Messaging Server를 엽니다.
2. 구성 탭을 누릅니다.
3. 왼쪽 표시 영역에서 서비스 폴더를 선택합니다.

4. 오른쪽 표시 영역에서 LDAP 탭을 누릅니다. LDAP 양식이 나타납니다.

LDAP 형식에는 구성 디렉토리와 사용자 디렉토리 모두에 대한 구성 설정이 표시됩니다. 하지만 구성 디렉토리 설정은 이 형식에서 읽기 전용입니다. 구성 디렉토리 설정을 변경해야 할 경우에는 *Sun ONE Server Console 5.2 Server Management Guide*의 Administration Server 장을 참조하십시오.

5. 사용자 디렉토리 연결 설정을 변경하려면 "Messaging Server별 디렉토리 설정 사용"이라는 레이블이 있는 상자를 누릅니다.
6. 다음 정보를 입력하거나 수정하여 LDAP 구성을 업데이트합니다. 고유 이름 등과 같은 용어 정의를 포함하여 디렉토리 개념에 대한 설명을 보려면 *Directory Server 관리* 설명서를 참조하십시오.

**호스트 이름:** 사용자 설치 시 사용자 정보가 있는 디렉토리의 호스트 시스템 이름을 입력합니다. 대부분 Messaging Server 호스트와는 다르지만 매우 소규모 설치인 경우에는 동일한 호스트일 수 있습니다.

**포트 번호:** Messaging Server가 사용자 조회를 위해 디렉토리에 액세스할 때 사용해야 하는 디렉토리 호스트의 포트 번호입니다. 이 번호는 디렉토리 관리자가 정의하며 반드시 기본 포트 번호(389)일 필요는 없습니다.

**기본 DN:** 검색 기본, 즉 사용자 조회를 위한 시작점을 나타내는 디렉토리 항목의 고유 이름입니다. 조회 프로세스의 속도를 높이려면 검색 기본이 디렉토리 트리에서 검색 중인 정보와 가능한 가까워야 합니다. 사용자 설치 디렉토리 트리에 "사람" 또는 "사용자" 분기가 있는 경우 이것이 좋은 시작점이 될 수 있습니다.

**바인드 DN:** Messaging Server가 조회를 위해 디렉토리 서버에 연결할 때 자신을 나타내기 위해 사용하는 고유 이름입니다. 바인드 DN은 디렉토리의 사용자 부분에 대한 검색 권한을 갖고 있는 사용자 디렉토리 자체에 있는 항목의 고유 이름이어야 합니다. 익명 검색 액세스가 허용되는 디렉토리의 경우에는 이 항목을 비워둘 수 있습니다.



7. Bind DN과 함께 이 Messaging Server를 LDAP 디렉토리에 인증하여 사용자를 조회하기 위해 사용된 비밀번호를 변경하려면 바인드 비밀번호 변경 버튼을 누릅니다. 비밀번호 입력 창이 열리면 여기에 업데이트된 비밀번호를 입력합니다.

이런 경우에 사용할 비밀번호가 무엇인지 결정하는 자체 보안 정책이 있어야 합니다. 초기에는 비밀번호가 설정되어 있지 않습니다. 바인드 DN 필드를 공백으로 비워둠으로써 익명 액세스를 지정한 경우에는 비밀번호가 사용되지 않습니다.

이 단계에서는 서버 구성에 저장된 비밀번호를 업데이트하지만 LDAP 서버의 비밀번호는 변경하지 않습니다. 이 계정은 기본적으로 PAB 조회에도 사용됩니다. 비밀번호를 변경한 후에는 다음 두 단계를 수행해야 합니다.

8. 구성 속성 `local.ugldapbinddn`에 지정된 사용자의 비밀번호를 수정합니다. 이 사용자 계정은 구성 속성 `local.ugdaphost`에 지정된 Directory Server에 있습니다.
9. 속성 `local.service.pab.ldapbinddn` 및 `local.service.pab.ldaphost`에 지정된 동일한 계정을 PAB 액세스에 사용하는 경우에는 `local.service.pab.ldappasswd`에 저장된 비밀번호를 업데이트해야 합니다.

기본 사용자 디렉토리를 다시 사용하려면 "Messaging Server별 디렉토리 설정 사용" 상자의 선택을 취소합니다.

**명령줄:** 다음과 같이 명령줄에 사용자 디렉토리 연결 설정 값을 설정할 수도 있습니다. 위의 단계 8,9에서 설명한 대로 LDAP와 PAB 비밀번호도 설정합니다.

Messaging Server별 디렉토리 설정의 사용 여부를 지정하는 경우

```
configutil -o local.ugldapuselocal -v [ yes | no ]
```

사용자 조회를 위한 LDAP 호스트 이름을 지정하는 경우

```
configutil -o local.ugdaphost -v name[:port_number]
```

사용자 조회를 위한 LDAP 포트 번호를 지정하는 경우

```
configutil -o local.ugdappport -v number
```

사용자 조회를 위한 LDAP 기본 DN을 지정하는 경우

```
configutil -o local.ugldapbasedn -v basedn
```

사용자 조회를 위한 LDAP 바인드 DN을 지정하는 경우

```
configutil -o local.ugldapbinddn -v binddn
```

## 암호화 설정

콘솔을 사용하여 SSL(Secure Sockets Layer) 암호화 및 Messaging Server 인증을 활성화하고 서버가 모든 서비스에 지원할 특정 암호화를 선택할 수 있습니다.

이 작업은 일반 구성 작업이지만 19장, "보안 및 액세스 제어 구성"의 "SSL 활성화" 절에 설명되어 있습니다. 여기에는 Messaging Server의 모든 보안 및 액세스 제어 항목에 대한 배경 정보도 포함되어 있습니다.

## 페일오버 LDAP 서버 설정

하나가 실패하면 다른 하나가 작동하도록 다음과 같이 사용자/그룹 디렉토리에 대한 LDAP 서버를 두 개 이상 지정할 수 있습니다.

1. 여러 LDAP 시스템에 local.ugldaphost를 설정합니다. 예를 들면 다음과 같습니다.

```
configutil -o local.ugldaphost -v "server1 server2 ..."
```

2. local.ugldapuselocal을 yes로 설정합니다. 이 작업은 사용자/그룹 LDAP 구성 데이터가 로컬 구성 파일에 저장되도록 지정합니다. 그렇지 않은 경우에는 LDAP에 저장됩니다. 예를 들면 다음과 같습니다.

```
configutil -o local.ugldapuselocal -v yes
```

목록의 첫 번째 서버가 실패하면 기존 LDAP 연결이 종료된 것으로 인식되어 새 연결이 생성됩니다. 새 ldap 연결이 필요하면 ldap 라이브러리는 모든 ldap 서버를 나열된 순서대로 시도합니다.

사용자/그룹 디렉토리에 대한 페일오버가 있는 것처럼 구성 디렉토리에 대해서도 비슷하게 페일오버 서버를 설정할 수 있습니다. 이 경우 구성 속성은 local.ldaphost입니다.

# POP, IMAP 및 HTTP 서비스 구성

Messaging Server는 메일함에 대한 클라이언트 액세스를 위해 POP3(Post Office Protocol 3), IMAP4(Internet Mail Access Protocol 4) 및 HTTP(HyperText Transfer Protocol)를 지원합니다. IMAP 및 POP는 모두 인터넷 표준 메일함 프로토콜입니다. 웹 사용 가능 전자 메일 프로그램인 Messenger Express를 사용하면 최종 사용자는 HTTP를 사용하는 인터넷에 연결된 컴퓨터 시스템에서 실행 중인 브라우저를 통해 자신의 메일함에 액세스할 수 있습니다.

이 장에서는 Sun ONE 콘솔 또는 명령줄 유틸리티를 사용하여 이러한 서비스를 하나 이상 지원하도록 서버를 구성하는 방법에 대해 설명합니다.

SMTP(Simple Mail Transfer Protocol) 서비스 구성에 대한 자세한 내용은 [10장, "MTA 서비스 및 구성 정보"](#)를 참조하십시오.

이 장은 다음 내용으로 구성되어 있습니다.

- [124페이지의 "일반 구성"](#)
- [126페이지의 "로그인 요구 사항"](#)
- [128페이지의 "성능 매개 변수"](#)
- [132페이지의 "클라이언트 액세스 제어"](#)
- [132페이지의 "POP 서비스 구성"](#)
- [134페이지의 "IMAP 서비스 구성"](#)
- [136페이지의 "HTTP 서비스 구성"](#)

## 일반 구성

Messaging Server POP, IMAP 및 HTTP 서비스의 일반 기능을 구성하는 작업에는 서비스를 사용 가능/불가능하게 하고 포트 번호를 할당하며 선택적으로 연결 클라이언트에 보내진 서비스 배너를 수정하는 것이 포함됩니다. 이 절에서는 이에 대한 배경 정보를 제공합니다. 이러한 설정을 위해 따라야 하는 단계는 [132페이지의 "POP 서비스 구성"](#), [134페이지의 "IMAP 서비스 구성"](#) 및 [136페이지의 "HTTP 서비스 구성"](#)을 참조하십시오.

## 서비스 사용 가능/불가능하게 하기

Messaging Server의 특정 인스턴스가 POP, IMAP 또는 HTTP 서비스를 사용 가능하게 할지 여부를 제어할 수 있습니다. 이것은 서비스를 시작 및 중지하는 것과 다릅니다([107페이지의 "서비스 시작 및 중지"](#) 참조). POP, IMAP 또는 HTTP 서비스가 작동하려면 해당 서비스를 사용 가능하게 한 다음 시작해야 합니다.

서비스를 사용 가능하게 하는 것은 서비스를 시작 또는 중지하는 것보다 "전역적인" 과정입니다. 예를 들어, 사용 가능 설정은 시스템 재부트 후에도 계속 유지되지만 이전에 "중지된" 서비스는 재부트 후에 다시 시작해야 합니다.

사용할 계획이 없는 서비스를 사용 가능하게 할 필요가 없습니다. 예를 들어, Messaging Server 인스턴스를 단지 메일 전송 에이전트(MTA)로 사용할 경우 POP, IMAP 및 HTTP를 사용 불가능하게 해야 합니다. 이 인스턴스가 POP 서비스에만 사용될 경우 IMAP 및 HTTP를 사용 불가능하게 하고 웹 기반 전자 메일에만 사용될 경우 POP 및 IMAP를 사용 불가능하게 해야 합니다.

서버 수준에서 서비스를 사용 가능/불가능하게 할 수 있습니다. 이 프로세스는 이 장과 [110페이지의 "시작할 서비스 지정"](#)에 설명되어 있습니다. 또한 지정된 LDAP 속성 mailAllowedServiceAccess를 설정하여 사용자 수준에서 서비스를 사용 가능/불가능하게 할 수도 있습니다.

## 포트 번호 지정

각 서비스에 대해 서버가 서비스 연결에 사용할 포트 번호를 지정할 수 있습니다.

- POP 서비스를 사용 가능하게 한 경우 서버가 POP 연결에 사용할 포트 번호를 지정할 수 있습니다. 기본값은 110입니다.
- IMAP 서비스를 사용 가능하게 한 경우 서버가 IMAP 연결에 사용할 포트 번호를 지정할 수 있습니다. 기본값은 143입니다.

- HTTP 서비스를 사용 가능하게 한 경우 서버가 HTTP 연결에 사용할 포트 번호를 지정할 수 있습니다. 기본값은 80입니다.

경우에 따라서는 기본값이 아닌 포트 번호를 지정해야 할 수 있습니다. 예를 들어 두 개 이상의 서버 인스턴스가 단일 호스트 시스템에 있거나 IMAP 서버 및 Messaging Multiplexor 서버와 동일한 호스트 시스템을 사용하는 경우 등입니다. Multiplexor에 대한 자세한 내용은 7장, "멀티플렉서 서비스 구성 및 관리"를 참조하십시오.

포트를 지정할 때는 다음 사항을 유의하십시오.

- 포트 번호는 1에서 65535 사이의 모든 숫자가 될 수 있습니다.
- 선택한 포트가 이미 사용 중이거나 다른 서비스에 예약되지 않았는지 확인합니다.

## 암호화된 통신을 위한 포트

Messaging Server는 SSL(Secure Sockets Layer) 프로토콜을 사용하여 IMAP, POP 및 HTTP 클라이언트와의 암호화된 통신을 지원합니다. Messaging Server의 SSL 지원에 대한 일반 정보는 649페이지의 "암호화 및 인증서 기반 인증 구성"을 참조하십시오.

### SSL에서의 IMAP

SSL에서의 IMAP에 대해 기본(권장) 포트 번호(993)를 그대로 사용하거나 다른 포트를 지정할 수 있습니다.

대부분의 현재 IMAP 클라이언트에 다른 포트가 필요하므로 Messaging Server는 IMAP 및 SSL에서의 IMAP에 대해 다른 포트를 사용하는 옵션을 제공합니다. IMAP 및 SSL에서의 IMAP 모두에 동일한 포트를 사용하는 통신은 새로운 표준으로 등장하고 있습니다. Messaging Server에 설치된 SSL 인증서가 있을 경우(651페이지의 "관리 콘솔을 통해 인증서 얻기" 참조) SSL에서의 동일 포트 IMAP를 지원할 수 있습니다.

### SSL에서의 POP

POP에 대한 기본적인 별도 SSL 포트는 995입니다. "STLS" 명령을 사용하여 일반적인 POP 포트를 통해 SSL을 초기화할 수도 있습니다(132페이지의 "POP 서비스 구성" 참조).

### SSL에서의 HTTP

SSL에서의 HTTP에 대해 기본 포트 번호(443)를 그대로 사용하거나 HTTP에 대해 다른 포트를 지정할 수 있습니다.

## 서비스 배너

클라이언트가 POP 또는 IMAP 포트에 처음 연결되면 서버는 식별 텍스트 문자열 클라이언트에게 보냅니다. 일반적으로 클라이언트의 사용자에게 표시되지 않는 이 서비스 배너는 서버를 Sun Java System Messaging Server로 식별하고 서버의 버전 번호를 제공합니다. 이 배너는 대부분 클라이언트 디버깅 또는 문제 해결 목적에 사용됩니다.

연결 클라이언트에 다른 메일을 보내려는 경우 POP 또는 IMAP 서비스의 기본 배너를 바꿀 수 있습니다.

Sun ONE 콘솔 또는 configutil 유틸리티(service.imap.banner, service.pop.banner)를 사용하여 서비스 배너를 설정할 수 있습니다. configutil에 대한 자세한 구문 정보는 *Sun Java System Messaging Server Administration Reference*(<http://docs.sun.com/doc/819-0106>)를 참조하십시오.

## 로그인 요구 사항

메일을 검색하기 위해 POP, IMAP 또는 HTTP 서비스에 로그인하는 사용자를 허용하는 방법을 제어할 수 있습니다. 모든 서비스에 대해 비밀번호 기반 로그인을 허용하거나 IMAP 또는 HTTP 서비스에 대해 인증서 기반 로그인을 허용할 수 있습니다. 이 절에서는 이에 대한 배경 정보를 제공합니다. 이러한 설정을 위해 따라야 하는 단계는 [132페이지의 "POP 서비스 구성"](#), [134페이지의 "IMAP 서비스 구성"](#) 또는 [136페이지의 "HTTP 서비스 구성"](#)을 참조하십시오. 또한 POP 로그인에 대한 유효한 로그인 구분자를 지정할 수도 있습니다.

## POP 클라이언트에 대한 로그인 구분자 설정

일부 메일 클라이언트는 @를 로그인 구분자(즉, uid@domain과 같은 주소의 @)로 허용하지 않습니다. 이러한 클라이언트의 예로는 Netscape Messenger 4.76, Netscape Messenger 6.0, Windows 2000의 Microsoft Outlook Express 등을 들 수 있습니다. 이에 대한 해결 방법은 다음과 같습니다.

1. 다음 명령으로 +를 유효한 구분자로 만듭니다.

```
configutil -o service.loginseparator -v "+@"
```

2. @가 아니라 +를 로그인 구분자로 사용하여 로그인해야 한다는 것을 POP 클라이언트 사용자에게 알립니다.

## 도메인 이름을 사용하지 않고 로그인 허용

일반적인 로그인의 경우 사용자는 사용자 아이디를 입력하고 구분자와 도메인 이름을 입력한 다음 비밀번호를 입력합니다. 그러나 설치 도중에 지정하는 기본 도메인의 사용자는 도메인 이름이나 구분자를 입력하지 않고 로그인할 수 있습니다.

사용자 아이디만 사용하여(즉, 도메인 이름과 구분자를 사용하지 않고) 다른 도메인의 사용자가 로그인할 수 있게 하려면 `sasl.default.ldap.searchfordomain`을 0으로 설정합니다. 사용자 아이디는 전체 디렉토리 트리에서 고유해야 한다는 것에 주의하십시오. 사용자 아이디가 고유하지 않을 경우 도메인 이름 없이 로그인할 수 없습니다.

로그인하기 위해 사용자가 입력해야 하는 속성을 수정할 수 있습니다. 예를 들어, 사용자가 전화 번호(`telephoneNumber`) 또는 직원 번호(`employeeID`)를 사용하여 로그인할 수 있게 하려면 `configutil` 매개 변수 `sasl.default.ldap.searchfilter`에서 정의하는 LDAP 검색을 변경합니다. 이 매개 변수는 `inetdomainsearchfilter` 도메인별 속성의 전역 기본 설정이며 동일한 구문을 사용합니다.

이 매개 변수에 대한 자세한 내용은 *Sun Java System Messaging Server Administration Reference*(<http://docs.sun.com/doc/819-0106>)를 참조하십시오.

## 비밀번호 기반 로그인

일반적인 메시징 설치에서는 사용자가 자신의 POP, IMAP 또는 HTTP 메일 클라이언트에 비밀번호를 입력함으로써 메일함에 액세스합니다. 클라이언트가 비밀번호를 서버에 보내면 서버는 이를 사용하여 사용자를 인증합니다. 사용자가 인증되면 서버는 액세스 제어 규칙에 기초하여 사용자에게 해당 서버에 저장된 특정 메일함에 대한 액세스를 허용할 것인지 결정합니다.

비밀번호 로그인을 허용할 경우 사용자는 비밀번호를 입력하여 POP, IMAP 또는 HTTP에 액세스할 수 있습니다. 비밀번호 기반 또는 SSL 기반 로그인은 POP 서비스를 위한 유일한 인증 방법입니다. 비밀번호는 LDAP 디렉토리에 저장됩니다. 디렉토리 정책에 따라 적용되는 비밀번호 정책(예: 최소 길이)이 결정됩니다.

IMAP 또는 HTTP 서비스에 대한 비밀번호 로그인을 허용하지 않을 경우 비밀번호 기반 인증이 허용되지 않습니다. 이 경우 사용자는 다음 절에 설명된 대로 인증서 기반 로그인을 사용해야 합니다.

IMAP 및 HTTP 서비스에 대한 비밀번호 전송의 보안을 향상시키려면 비밀번호를 서버로 보내기 전에 암호화하도록 요구할 수 있습니다. 이렇게 하려면 로그인에 대한 최소 암호화 길이 요구 사항을 선택합니다.

- 0을 선택한 경우 암호화가 필요하지 않습니다. 비밀번호는 일반 텍스트로 보내지거나 클라이언트 정책에 따라 암호화됩니다.

- 0이 아닌 값을 선택한 경우 클라이언트는 지정된 값 이상의 키 길이를 가진 암호화를 사용하여 서버와의 SSL 세션을 설정해야 합니다. 따라서 클라이언트가 보내는 모든 IMAP 또는 HTTP 사용자 비밀번호가 암호화됩니다.

서버에서 지원하는 최대값보다 큰 키 길이로 암호화하도록 클라이언트가 구성되었거나 클라이언트가 지원하는 최대값보다 큰 키 길이로 암호화하도록 서버가 구성된 경우 비밀번호 기반 로그인을 수행할 수 없습니다. 다양한 암호화 및 키 길이를 지원하도록 서버를 설정하는 방법에 대한 자세한 내용은 [656페이지의 "SSL 사용 및 암호문 선택"](#)을 참조하십시오.

## 인증서 기반 로그인

비밀번호 기반 인증 외에도 Sun Java System 서버는 디지털 인증서 검사를 통한 사용자 인증을 지원합니다. 이 경우, 클라이언트는 서버와의 SSL 세션을 설정할 때 비밀번호를 제공하는 대신 사용자의 인증서를 제공합니다. 인증서가 검증될 경우 사용자는 인증된 것으로 간주됩니다.

IMAP 또는 HTTP 서비스에 대한 인증서 기반 사용자 로그인을 허용하도록 Messaging Server를 설정하는 방법에 대한 자세한 내용은 [658페이지의 "인증서 기반 로그인 설정"](#)을 참조하십시오.

인증서 기반 로그인을 사용 가능하게 하기 위해 IMAP 또는 HTTP 시스템 양식에서 "비밀번호 로그인 허용" 상자를 선택 취소할 필요는 없습니다. 이 상자를 선택한 상태(기본 상태)에서 인증서 기반 로그인을 설정하는 데 필요한 작업을 수행한 경우 비밀번호 기반 로그인 및 인증서 기반 로그인이 모두 지원됩니다. 그런 다음 클라이언트가 SSL 세션을 설정하고 인증서를 제공할 경우 인증서 기반 로그인이 사용됩니다. 클라이언트는 SSL을 사용하지 않으며 클라이언트 인증서를 제공하지 않을 경우에는 대신 비밀번호를 보냅니다.

## 성능 매개 변수

Messaging Server의 POP, IMAP 및 HTTP 서비스에 대한 몇 가지 기본 성능 매개 변수를 설정할 수 있습니다. 하드웨어 용량과 사용자 기반에 따라 이러한 매개 변수를 조정하여 최대한의 서비스 효율성을 실현할 수 있습니다. 이 절에서는 이에 대한 배경 정보를 제공합니다. 이러한 설정을 위해 따라야 하는 단계는 [132페이지의 "POP 서비스 구성"](#), [134페이지의 "IMAP 서비스 구성"](#) 또는 [136페이지의 "HTTP 서비스 구성"](#)을 참조하십시오.



## 프로세스 수

Messaging Server는 여러 실행 프로세스 간에 작업을 분할할 수 있으며 이렇게 하면 경우에 따라 효율성이 향상될 수 있습니다. 이 기능은 특히 서버 프로세스 수를 조정했을 때 하드웨어 프로세서 간에 여러 작업을 더 효율적으로 분산시킬 수 있는 다중 프로세스 서버 시스템에서 유용합니다.

그러나 여러 프로세스 간에 작업을 할당하고 특정 프로세스에서 다른 프로세스로 전환하는 것에는 성능 오버헤드가 존재합니다. 여러 프로세스를 사용하는 자체의 이점은 새 프로세스를 추가할수록 줄어듭니다. 대부분의 구성에 적용되는 간단한 경험상의 규칙은 서버 시스템의 하드웨어 프로세서당 프로세스를 하나씩 가지는 것입니다(최대 한 네 개까지 가능). 실제의 최적 구성이 이와 다를 수 있으므로 이 경험상의 규칙을 단순히 고유한 분석을 위한 지침으로 활용해야 할 것입니다.

**주:** 일부 플랫폼에서는 성능에 영향을 줄 수 있는 플랫폼 특성의 일정한 프로세스별 제한(예: 최대 파일 설명자 수)을 극복하기 위해 프로세스 수를 늘릴 수 있습니다.

각 POP, IMAP 또는 HTTP 서비스에 대한 기본 프로세스 수는 1입니다.

## 프로세스당 연결 수

POP, IMAP 또는 HTTP 서비스가 유지 관리할 수 있는 동시 클라이언트 연결이 많아질수록 클라이언트에게 더 유리합니다. 사용할 수 있는 연결이 없기 때문에 서비스가 거부될 경우 클라이언트는 다른 클라이언트가 연결을 끊을 때까지 기다려야 합니다.

반면, 열려 있는 각 연결은 메모리 자원을 소비하며 서버 시스템의 입출력 하위 시스템에 대한 요청을 하기 때문에 서버가 지원하리라 예상할 수 있는 동시 세션 수에는 실제적인 제한이 있습니다. 서버 메모리나 입출력 용량을 증가시켜 이러한 제한을 늘릴 수도 있습니다.

IMAP, HTTP 및 POP는 이 점에 있어서 다른 요구를 갖고 있습니다.

- IMAP 연결은 일반적으로 POP 및 HTTP 연결과 비교하여 오래 지속됩니다. 사용자가 IMAP에 연결하여 메일을 다운로드할 경우 사용자가 종료하거나 연결 시간이 초과될 때까지 일반적으로 연결이 유지 관리됩니다. 이와 달리 POP 또는 HTTP 연결은 대개 POP 또는 HTTP 요청이 서비스되자마자 닫힙니다.
- IMAP 및 HTTP 연결은 일반적으로 POP 연결과 비교하여 매우 효율적입니다. 각 POP 재연결에는 사용자에게 대한 재인증이 필요합니다. 이와 달리 IMAP 연결은 IMAP 세션 동안(로그인에서 로그아웃까지) 연결이 열려 있기 때문에 단일 인증만 필요합니다. HTTP 연결은 짧지만 각 HTTP 세션(로그인에서 로그아웃까지)에 여러

연결이 허용되므로 각 연결에 대해 사용자의 재인증이 필요하지 않습니다. 이러한 점에서 POP 연결은 IMAP 또는 HTTP 연결보다 훨씬 더 많은 성능 오버헤드를 발생시킵니다. Messaging Server는 특히, 열려 있지만 유휴 상태인 IMAP 연결과 여러 HTTP 연결을 통해 매우 낮은 오버헤드만이 필요하도록 설계되었습니다.

---

**주** HTTP 세션 보안에 대한 자세한 내용은 [643페이지의 "HTTP 보안 정보"](#)를 참조하십시오.

---

따라서 특정 시점의 특정 사용자 요구에 대해 Messaging Server는 POP 연결보다 더 많은 열려 있는 IMAP 및 HTTP 연결을 지원할 수 있습니다.

IMAP의 기본값은 4000이고 HTTP의 기본값은 프로세스당 6000개의 연결이며 POP의 기본값은 600입니다. 이러한 값은 일반적으로 구성된 서버 시스템이 처리할 수 있는 대략적으로 동일한 요구를 나타냅니다. 최적 구성이 이와 다를 수 있으므로 이러한 기본값을 단순히 일반적인 지침으로 사용해야 합니다.

일반적으로 활성 POP 연결은 활성 IMAP 연결보다 서버 리소스와 대역폭이 훨씬 더 많이 요구됩니다. 이는 IMAP 연결이 대부분의 시간에 유휴 상태인 것과 달리 POP 연결은 지속적으로 메일을 다운로드하기 때문입니다. 따라서 POP에 대해 더 적은 수의 세션을 유지하는 것이 적합합니다. 반대로, POP 연결은 전자 메일을 다운로드하는 동안에만 지속되므로 활성 POP 사용자는 짧은 시간 동안만 연결되지만 IMAP 연결은 계속되는 메일 검사에서 연결된 상태로 유지됩니다.

## 프로세스당 스레드 수

여러 프로세스를 지원하는 것 외에도 Messaging Server는 여러 스레드 간에 작업을 분할하여 성능을 더욱 향상시킵니다. 서버의 스레드 사용은 실행 효율성을 크게 향상시키는데 이는 진행 중인 명령이 다른 명령의 실행을 저해하지 않기 때문입니다. 실행하는 동안에 필요에 따라 스레드는 설정된 최대 개수까지 작성 및 삭제됩니다.

동시에 실행되는 스레드가 많다는 것은 더 많은 클라이언트 요청을 지연 없이 처리할 수 있으며 이에 따라 더 많은 수의 클라이언트에게 신속하게 서비스할 수 있다는 것을 의미합니다. 그러나 스레드 간의 디스패칭으로 인해 성능 오버헤드가 발생하므로 서버가 사용할 수 있는 스레드 수에는 실제적인 제한이 존재합니다.

POP, IMAP 및 HTTP의 경우 기본 최대값은 프로세스당 250개의 스레드입니다. IMAP 및 HTTP의 기본 연결이 POP보다 많다는 사실에도 불구하고 이러한 기본값은 동일합니다. 수는 적지만 사용량이 많은 POP 연결과 동일한 최대 스레드 수를 사용하여 POP 연결보다 많은 수의 IMAP 및 HTTP 연결을 효율적으로 처리할 수 있는 것으로 알려져 있습니다. 실제의 최적 구성이 이와 다를 수 있지만 이러한 기본값으로 충분하기 때문에 값을 늘릴 필요는 없을 것입니다. 즉, 대부분의 설치에서 이러한 기본값은 적절한 성능을 제공합니다.

## 유휴 연결 해제

응답하지 않는 클라이언트의 연결에 사용된 시스템 자원을 재이용하기 위해 IMAP4, POP3 및 HTTP 프로토콜은 일정 시간 동안 유휴 상태였던 연결을 일반적으로 해제할 수 있는 기능을 서버에 제공합니다.

각 프로토콜 사양에서는 서버가 최소한의 시간 동안 유휴 연결을 열어두어야 합니다. 기본 시간은 POP는 10분, IMAP는 30분, HTTP는 3분입니다. 유휴 시간을 기본값보다 큰 값으로 늘릴 수 있지만 줄일 수는 없습니다.

POP 또는 IMAP 연결이 해제될 경우 새 연결을 설정하기 위해 사용자는 재인증되어야 합니다. 이와 달리 HTTP 연결이 해제될 경우 HTTP 세션이 계속 열려 있으므로 사용자를 재인증할 필요가 없습니다. HTTP 세션 보안에 대한 자세한 내용은 [643페이지의 "HTTP 보안 정보"](#)를 참조하십시오.

유휴 POP 연결은 일반적으로 클라이언트를 응답하지 않게 만드는 일부 문제(예: 충돌 또는 중지)로 인해 발생합니다. 반면, 유휴 IMAP 연결은 정상적인 상태입니다. IMAP 사용자가 일반적으로 연결이 끊기는 것을 방지하기 위해 IMAP 클라이언트는 일반적으로 30초 미만의 일정한 간격으로 IMAP 서버에 명령을 보냅니다.

## HTTP 클라이언트 로그아웃

HTTP 세션은 여러 연결에서 지속될 수 있습니다. 연결이 해제될 때 HTTP 클라이언트는 로그아웃되지 않습니다. 그러나 지정된 기간(기본적으로 2시간) 동안 HTTP 세션이 유휴 상태이면 서버는 자동으로 HTTP 세션을 해제하고 클라이언트는 로그아웃됩니다. 세션이 해제되면 클라이언트의 세션 아이디가 더 이상 유효하지 않으므로 다른 세션을 설정하기 위해 클라이언트는 재인증되어야 합니다. HTTP 보안 및 세션 아이디에 대한 자세한 내용은 [643페이지의 "HTTP 보안 정보"](#)를 참조하십시오.

## 클라이언트 액세스 제어

Messaging Server에는 POP, IMAP 또는 HTTP 메시징 서비스와 SMTP에 대한 액세스를 어떤 클라이언트가 얻을 수 있는지 결정하는 액세스 제어 기능이 포함되어 있습니다. 다양한 기준에 기초하여 클라이언트에 대한 액세스를 허용 또는 거부하는 유연한 액세스 필터를 만들 수 있습니다.

클라이언트 액세스 제어는 Messaging Server의 중요한 보안 기능입니다. 클라이언트 액세스 제어 필터 작성에 대한 자세한 내용과 그 사용 예는 [664페이지의 "POP, IMAP 및 HTTP 서비스에 대한 클라이언트 액세스 구성"](#) 및 [679페이지의 "SMTP 서비스에 대한 클라이언트 액세스 구성"](#)을 참조하십시오.

## POP 서비스 구성

configutil 명령이나 Sun ONE 콘솔을 사용하여 Messaging Server POP 서비스의 기본 구성을 수행할 수 있습니다. 이 장에서는 더 일반적인 몇 가지 POP 서비스 옵션이 제공됩니다. 전체 목록은 *Sun Java System Messaging Server Administration Reference*에서 확인할 수 있습니다.

자세한 내용은 다음을 참조하십시오.

- [124페이지의 "서비스 사용 가능/불가능하게 하기"](#)
- [126페이지의 "POP 클라이언트에 대한 로그인 구분자 설정"](#)
- [124페이지의 "포트 번호 지정"](#)
- [129페이지의 "프로세스당 연결 수"](#)
- [131페이지의 "유휴 연결 해제"](#)
- [130페이지의 "프로세스당 스레드 수"](#)
- [129페이지의 "프로세스 수"](#)

**콘솔.** 콘솔을 사용하여 POP 서비스를 구성하려면 다음을 수행합니다.

1. Sun ONE 콘솔에서 구성할 Messaging Server를 엽니다.
2. 구성 탭을 누르고 왼쪽 표시 영역에서 서비스 폴더를 엽니다.
3. POP를 선택합니다.
4. 오른쪽 표시 영역에서 시스템 탭을 누릅니다.
5. 서비스를 사용하려면 "포트에서 POP 서비스 사용" 상자를 선택하고 포트 번호를 할당합니다.

6. 다음과 같이 연결 설정을 지정합니다.
  - 프로세스당 최대 네트워크 연결 수를 설정합니다. 자세한 내용은 [129페이지의 "프로세스당 연결 수"](#)를 참조하십시오.
  - 연결의 최대 유휴 시간을 설정합니다. 자세한 내용은 [131페이지의 "유휴 연결 해제"](#)를 참조하십시오.
7. 다음과 같이 프로세스 설정을 지정합니다.
  - 프로세스스레드 수를 설정합니다. 자세한 내용은 [130페이지의 "프로세스당 스레드 수"](#)를 참조하십시오.
  - 최대 프로세스 수를 설정합니다. 자세한 내용은 [129페이지의 "프로세스 수"](#)를 참조하십시오.
8. 원할 경우 POP 서비스 배너 필드에서 서비스 배너를 지정합니다.
9. 저장을 누릅니다.

---

**주** POP 서비스의 경우 비밀번호 기반 로그인 이 자동으로 사용 가능하게 됩니다.

---

**명령줄.** 다음과 같이 명령줄에서 POP 속성에 대한 값을 설정할 수 있습니다.

POP 서비스를 사용 또는 사용하지 않으려면 다음을 수행합니다.

```
configutil -o service.pop.enable -v [ yes | no ]
```

포트 번호를 지정하려면 다음을 수행합니다.

```
configutil -o service.pop.port -v number
```

프로세스당 최대 네트워크 연결 수를 설정하려면 다음을 수행합니다.

```
configutil -o service.pop.maxsessions -v number
```

연결의 최대 유휴 시간을 설정하려면 다음을 수행합니다.

```
configutil -o service.pop.idletimeout -v number
```

프로세스당 최대 스레드 수를 설정하려면 다음을 수행합니다.

```
configutil -o service.pop.maxthreads -v number
```

최대 프로세스 수를 설정하려면 다음을 수행합니다.

```
configutil -o service.pop.numprocesses -v number
```

SSL에서의 POP를 사용하려면 다음을 수행합니다.

```
configutil -o service.pop.enablesslport -v 1
configutil -o service.pop.sslport -v 995
```

SSL이 올바르게 구성된 경우 TLS도 지원된다는 것에 주의합니다.

프로토콜 시작 배너를 지정하려면 다음을 수행합니다.

```
configutil -o service.pop.banner -v banner
```

## IMAP 서비스 구성

configutil 명령이나 Sun ONE 콘솔을 사용하여 Messaging Server IMAP 서비스의 기본 구성을 수행할 수 있습니다. 이 절에서는 더 일반적인 몇 가지 IMAP 서비스 옵션이 제공 됩니다. 전체 목록은 *Sun Java System Messaging Server Administration Reference*에서 확인할 수 있습니다. 자세한 내용은 다음을 참조하십시오.

- 124페이지의 "서비스 사용 가능/불가능하게 하기"
- 124페이지의 "포트 번호 지정"
- 127페이지의 "비밀번호 기반 로그인"
- 129페이지의 "프로세스당 연결 수"
- 131페이지의 "유휴 연결 해제"
- 130페이지의 "프로세스당 스레드 수"
- 129페이지의 "프로세스 수"

**콘솔.** 콘솔에서 IMAP 서비스를 구성하려면 다음을 수행합니다.

1. Sun ONE 콘솔에서 구성할 Messaging Server를 엽니다.
2. 구성 탭을 누르고 왼쪽 표시 영역에서 서비스 폴더를 엽니다.
3. IMAP를 선택합니다.
4. 오른쪽 표시 영역에서 시스템 탭을 누릅니다.
5. 서비스를 사용하려면 "포트에서 IMAP 서비스 사용" 상자를 선택하고 포트 번호를 할당합니다.
6. 원할 경우 비밀번호 기반 로그인을 사용 가능하게 합니다.
7. 다음과 같이 연결 설정을 지정합니다.
  - 프로세스당 최대 네트워크 연결 수를 설정합니다. 자세한 내용은 129페이지의 "프로세스당 연결 수"를 참조하십시오.

- 연결의 최대 유휴 시간을 설정합니다. 자세한 내용은 [131페이지](#)의 "유휴 연결 해제"를 참조하십시오.
8. 다음과 같이 프로세스 설정을 지정합니다.
- 프로세스레드 수를 설정합니다. 자세한 내용은 [130페이지](#)의 "프로세스당 스레드 수"를 참조하십시오.
  - 최대 프로세스 수를 설정합니다. 자세한 내용은 [129페이지](#)의 "프로세스 수"를 참조하십시오.
9. 원할 경우 IMAP 서비스 배너 필드에서 서비스 배너를 지정합니다.
10. 저장을 누릅니다.

**명령줄.** 다음과 같이 명령줄에서 IMAP 속성에 대한 값을 설정할 수 있습니다.

IMAP 서비스를 사용 또는 사용하지 않으려면 다음을 수행합니다.

```
configutil -o service.imap.enable -v [ yes | no ]
```

포트 번호를 지정하려면 다음을 수행합니다.

```
configutil -o service.imap.port -v number
```

SSL에서의 IMAP에 다른 포트를 사용하려면 다음을 수행합니다.

```
configutil -o service.imap.enablesslport -v [ yes | no ]
```

SSL에서의 IMAP에 대한 포트 번호를 지정하려면 다음을 수행합니다.

```
configutil -o service.imap.sslport -v number
```

IMAP 서비스에 대한 비밀번호 로그인을 사용 또는 사용하지 않으려면 다음을 수행합니다.

```
configutil -o service.imap.plaintextmncipher -v value
```

여기에서 *value*는 다음 중 하나입니다.

- 1 - 비밀번호 로그인을 사용 불가능하게 합니다.
- 0 - 암호화 없이 비밀번호 로그인을 사용 가능하게 합니다.
- 40 - 비밀번호 로그인을 사용하여 암호화 강도를 지정합니다.
- 128 - 비밀번호 로그인을 사용하여 암호화 강도를 지정합니다.

프로세스당 최대 네트워크 연결 수를 설정하려면 다음을 수행합니다.

```
configutil -o service.imap.maxsessions -v number
```

연결의 최대 유휴 시간을 설정하려면 다음을 수행합니다.

```
configutil -o service.imap.idletimeout -v number
```

프로세스당 최대 스레드 수를 설정하려면 다음을 수행합니다.

```
configutil -o service.imap.maxthreads -v number
```

최대 프로세스 수를 설정하려면 다음을 수행합니다.

```
configutil -o service.imap.numprocesses -v number
```

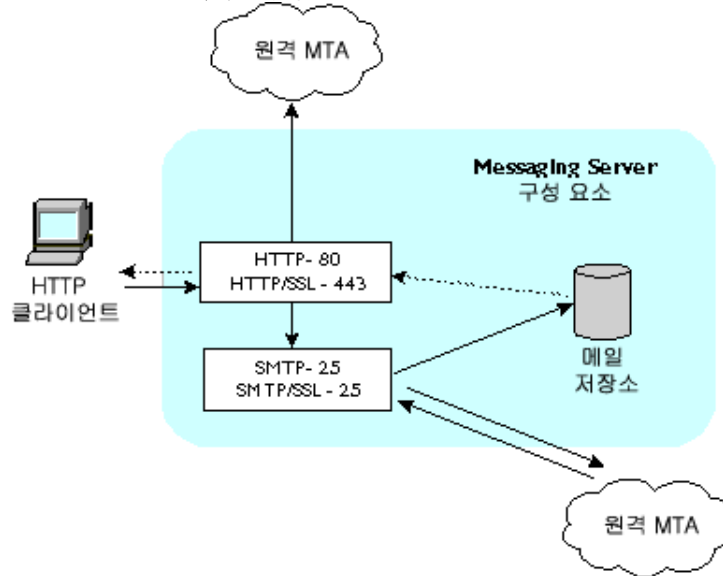
프로토콜 시작 배너를 지정하려면 다음을 수행합니다.

```
configutil -o service.imap.banner -v banner
```

## HTTP 서비스 구성

POP 및 IMAP 클라이언트는 라우팅 또는 전달을 위해 메일을 Messaging Server MTA로 직접 보냅니다. 이와 달리 HTTP 클라이언트는 Messaging Server의 일부인 특수한 웹 서버로 메일을 보냅니다. 그런 다음 HTTP 서비스는 그림 5-1에 나온 것처럼 라우팅 또는 전달을 위해 메일을 로컬 MTA나 원격 MTA로 보냅니다. Messaging Server가 웹 기반 전자 메일용으로만 사용될 경우 POP와 IMAP를 모두 사용 불가능하게 합니다.

그림 5-1 HTTP 서비스 구성 요소





대부분의 HTTP 구성 매개 변수는 POP 및 IMAP 서비스에 사용할 수 있는 매개 변수와 비슷합니다. 여기에는 연결 설정 및 프로세스 설정을 위한 매개 변수가 포함됩니다. 이 절에서는 더 일반적인 몇 가지 HTTP 서비스 옵션이 제공됩니다. 전체 목록은 *Sun Java System Messaging Server Administration Reference*에서 확인할 수 있습니다. 자세한 내용은 다음을 참조하십시오.

- 124페이지의 "서비스 사용 가능/불가능하게 하기"
- 124페이지의 "포트 번호 지정"
- 127페이지의 "비밀번호 기반 로그인"
- 129페이지의 "프로세스당 연결 수"
- 131페이지의 "유휴 연결 해제"
- 131페이지의 "HTTP 클라이언트 로그아웃"
- 130페이지의 "프로세스당 스레드 수"
- 129페이지의 "프로세스 수"

메일 설정 및 MTA 설정을 위한 매개 변수를 비롯한 일부 매개 변수는 HTTP 서비스에만 해당합니다.

**메일 설정.** HTTP 클라이언트가 첨부 파일이 있는 메일을 생성하면 첨부 파일은 서버로 업로드되어 파일에 저장됩니다. HTTP 서비스는 라우팅 또는 전달을 위해 메일을 MTA로 보내기 전에 첨부 파일을 검색하고 메일을 생성합니다. 기본 첨부 파일 스푼 디렉토리를 사용하거나 대체 디렉토리를 지정할 수 있습니다. 또한 첨부 파일에 허용되는 최대 크기를 지정할 수도 있습니다.

**MTA 설정.** 기본적으로 HTTP 서비스는 라우팅 또는 전달을 위해 보내는 웹 메일을 로컬 MTA로 전송합니다. 예를 들어, 사이트가 호스팅 서비스이며 대부분의 수신자가 로컬 호스트 시스템과 다른 도메인에 있을 경우 메일을 원격 MTA로 보내도록 HTTP 서비스를 구성할 수 있습니다. 웹 메일을 원격 MTA로 보내려면 원격 호스트의 이름과 SMTP 포트 번호를 지정해야 합니다.

**콘솔.** Sun ONE 콘솔을 사용하여 HTTP 서비스를 구성하려면 다음을 수행합니다.

1. Sun ONE 콘솔에서 구성할 Messaging Server를 엽니다.
2. 구성 탭을 누르고 왼쪽 표시 영역에서 서비스 폴더를 엽니다.
3. HTTP를 선택합니다.
4. 오른쪽 표시 영역에서 시스템 탭을 누릅니다.

5. 서비스를 사용하려면 "포트에서 HTTP 서비스 사용" 상자를 선택하고 포트 번호를 할당합니다.
  6. 원할 경우 비밀번호 기반 로그인을 사용 가능하게 합니다.
  7. 다음과 같이 연결 설정을 지정합니다.
    - 프로세스당 최대 네트워크 연결 수를 설정합니다. 자세한 내용은 [129페이지의 "프로세스당 연결 수"](#)를 참조하십시오.
    - 연결의 최대 유휴 시간을 설정합니다. 자세한 내용은 [131페이지의 "유휴 연결 해제"](#)를 참조하십시오.
    - 클라이언트 세션의 최대 유휴 시간을 설정합니다. 자세한 내용은 [131페이지의 "HTTP 클라이언트 로그아웃"](#)를 참조하십시오.
  8. 다음과 같이 프로세스 설정을 지정합니다.
    - 프로세스레드 수를 설정합니다. 자세한 내용은 [130페이지의 "프로세스당 스레드 수"](#)를 참조하십시오.
    - 최대 프로세스 수를 설정합니다. 자세한 내용은 [129페이지의 "프로세스 수"](#)를 참조하십시오.
  9. 다음과 같이 메일 설정을 지정합니다.
    - 원할 경우 첨부 파일 스푼 디렉토리를 지정합니다.
    - 원할 경우 최대 보내는 메일 크기를 지정합니다. 여기에는 base64로 인코딩된 모든 첨부 파일이 포함되며 base64 인코딩은 33%의 추가 공간이 필요하다는 점을 유의하십시오. 따라서 콘솔의 제한이 5MB일 경우 메일 하나와 첨부 파일의 최대 크기는 약 3.75MB가 됩니다.  
  
자세한 내용은 [137페이지의 "메일 설정"](#)를 참조하십시오.
  10. 다음과 같이 MTA 설정을 지정합니다.
    - 원할 경우 대체 MTA 호스트 이름을 지정합니다.
    - 원할 경우 대체 MTA 포트를 지정합니다.  
  
자세한 내용은 [137페이지의 "MTA 설정"](#)를 참조하십시오.
  11. 저장을 누릅니다.
- 명령줄.** 명령줄에서 HTTP 속성 값을 다음과 같이 설정할 수 있습니다. 자세한 내용은 *Sun Java System Messaging Server Administration Reference*(<http://docs.sun.com/doc/819-0106>)를 참조하십시오.
- HTTP 서비스를 사용 또는 사용하지 않으려면 다음을 수행합니다.

```
configutil -o service.http.enable -v [ yes | no ]
```

포트 번호를 지정하려면 다음을 수행합니다.

```
configutil -o service.http.port -v number
```

SSL에서의 HTTP에 다른 포트를 사용하려면 다음을 수행합니다.

```
configutil -o service.http.enablesslport -v [ yes | no ]
```

SSL에서의 HTTP에 대한 포트 번호를 지정하려면 다음을 수행합니다.

```
configutil -o service.http.sslport -v number
```

비밀번호 로그인을 사용 또는 사용하지 않으려면 다음을 수행합니다.

```
configutil -o service.http.plaintextmncipher -v value
```

여기에서 *value*는 다음 중 하나입니다.

- 1 - 비밀번호 로그인을 사용 불가능하게 합니다.
- 0 - 암호화 없이 비밀번호 로그인을 사용 가능하게 합니다.
- 40 - 비밀번호 로그인을 사용하여 암호화 강도를 지정합니다.
- 128 - 비밀번호 로그인을 사용하여 암호화 강도를 지정합니다.

프로세스당 최대 네트워크 연결 수를 설정하려면 다음을 수행합니다.

```
configutil -o service.http.maxsessions -v number
```

연결의 최대 유휴 시간을 설정하려면 다음을 수행합니다.

```
configutil -o service.http.idletimeout -v number
```

클라이언트 세션의 최대 유휴 시간을 설정하려면 다음을 수행합니다.

```
configutil -o service.http.sessiontimeout -v number
```

프로세스당 최대 스레드 수를 설정하려면 다음을 수행합니다.

```
configutil -o service.http.maxthreads -v number
```

최대 프로세스 수를 설정하려면 다음을 수행합니다.

```
configutil -o service.http.numprocesses -v number
```

클라이언트에 보내는 메일의 첨부 파일 스폴 디렉토리를 지정하려면 다음을 수행합니다.

```
configutil -o service.http.spooldir -v dirpath
```

최대 메일 크기를 지정하려면 다음을 수행합니다.

```
configutil -o service.http.maxmessagesize -v size
```

여기에서 *size*는 바이트 수입니다. 여기에는 **base64**로 인코딩된 모든 첨부 파일이 포함되며 **base64** 인코딩은 33%의 추가 공간이 필요하다는 점을 유의하십시오. 따라서 콘솔의 제한이 5MB일 경우 메일 하나와 첨부 파일의 최대 크기는 약 3.75MB가 됩니다.

대체 MTA 호스트 이름을 지정하려면 다음을 수행합니다.

```
configutil -o service.http.smtphost -v hostname
```

대체 MTA 호스트 이름의 포트 번호를 지정하려면 다음을 수행합니다.

```
configutil -o service.http.smtpport -v portnum
```

## 단일 사인 온(SSO) 사용

단일 사인 온(SSO)은 최종 사용자가 한 번의 인증(사용자 아이디와 비밀번호를 사용하여 로그인)으로 여러 응용 프로그램에 액세스할 수 있는 기능입니다. Sun Java System Access Manager(이전 명칭은 Identity Server임)는 Sun Java System 서버에 대한 SSO에 사용되는 공식적인 게이트웨이입니다. 즉, 사용자가 다른 SSO 구성 서버에 액세스하려면 Access Manager에 로그인해야 합니다.

예를 들어, 제대로 구성된 경우 사용자는 Sun Java System Access Manager 로그인 화면에서 서명한 후 다른 창에서 다시 서명하지 않고도 Messenger Express에 액세스할 수 있습니다. 마찬가지로 Sun Java System Calendar Server를 제대로 구성한 경우 사용자는 Sun Java System Access Manager 로그인 화면에서 서명한 후 다른 창에서 다시 서명하지 않고도 해당 Calendar Server에 액세스할 수 있습니다.

Messaging Server에서는 SSO를 배포하는 두 가지 방법을 제공합니다. 첫 번째 방법은 Sun Java System Access Manager를 통한 방법이고 두 번째 방법은 통신 서버의 신뢰할 수 있는 원 기술을 통한 방법입니다. 신뢰할 수 있는 원을 사용하는 것은 레거시 SSO 구현 방법입니다. 이 방법에는 Access Manager SSO에서는 사용할 수 없는 여러 기능이 있지만 향후 모든 기능이 Access Manager에 배포될 때까지는 사용하지 않는 것이 좋습니다. 하지만 다음 절에서는 두 가지 방법을 모두 설명합니다.

- [141페이지의 "Sun Java System 서버에 대한 Access Manager SSO"](#)
- [144페이지의 "신뢰할 수 있는 원 SSO\(레거시\)"](#)

## Sun Java System 서버에 대한 Access Manager SSO

이 절에서는 Access Manager를 사용하는 SSO에 대해 설명합니다. 이 절은 다음 내용으로 구성되어 있습니다.

- 142페이지의 "SSO 제한 및 알림"
- 142페이지의 "SSO를 지원하도록 Messaging Server 구성"
- 144페이지의 "SSO 문제 해결"

## SSO 제한 및 알림

- Messenger Express 세션은 Access Manager 세션이 유효한 경우에만 유효합니다. 사용자가 Access Manager에서 로그아웃하면 웹 메일 세션이 자동으로 닫힙니다(단일 사인 오프).
- 함께 작동하는 SSO 응용 프로그램은 동일한 DNS 도메인에 있어야 합니다. 이러한 도메인을 쿠키 도메인이라고도 합니다.
- SSO 응용 프로그램은 Access Manager 확인 URL(이름 지정 서비스)에 액세스해야 합니다.
- 브라우저에 쿠키가 있어야 합니다.

## SSO를 지원하도록 Messaging Server 구성

네 개의 `configutil` 매개 변수가 Messaging Server SSO를 지원합니다. 이 네 개 중 `local.webmail.sso.amnamingurl` 하나만 Messaging Server에서 SSO를 사용하는 데 필요 합니다. SSO를 사용하려면 이 매개 변수를 Access Manager에서 이름 지정 서비스를 실행 하는 URL로 설정합니다. 일반적으로 이 URL은 `http://server/amserver/namingservice` 입니다. 예를 들면 다음과 같습니다.

```
configutil -o local.webmail.sso.amnamingurl -v  
http://sca-walnut:88/amserver/namingservice
```

---

**주** Access Manager SSO는 이전 SSO 기법을 사용하는 `local.webmail.sso.enable`을 확인하지 않습니다. `local.webmail.sso.enable`을 off 또는 설정되지 않은 상태로 두어야 합니다. 그렇지 않으면 이전 SSO 기법에 필요한 구성 매개 변수가 없다는 경고 메일이 기록됩니다.

---

`configutil` 명령을 사용하여 표 6-3에 표시된 SSO 구성 매개 변수를 수정할 수 있습니다.

표 6-1 Access Manager 단일 사인 온(SSO) 매개 변수

매개 변수	설명
<code>local.webmail.sso.amnamingurl</code>	<p>Access Manager가 이름 지정 서비스를 실행하는 URL입니다. Access Manager를 통해 단일 사인 온(SSO)하기 위한 필수 변수입니다. 일반적으로 이 URL은 <code>http://server/amserver/namingservice</code>입니다.</p> <p>기본값: 설정 안 함</p>
<code>local.webmail.sso.amcookieName</code>	<p>Access Manager 쿠키 이름입니다. Access Manager가 다른 쿠키 이름을 사용하도록 구성된 경우 Messaging Server에서 단일 사인 온(SSO) 수행 시 확인할 대상을 알 수 있도록 Messaging Server에서 해당 이름을 <code>local.webmail.sso.amcookieName</code>으로 구성해야 합니다. 기본값은 <code>iPlanetDirectoryPro</code>이며 Access Manager가 기본 구성으로 구성된 경우 이 값을 변경할 수 없습니다.</p> <p>기본값: <code>iPlanetDirectoryPro</code></p>
<code>local.webmail.sso.amloglevel</code>	<p>AMSDK 로깅 수준입니다. Messaging Server에 사용되는 SSO 라이브러리에는 Messaging Server와는 별도로 자체 로깅 기법이 있습니다. <code>msg_svr_base/log</code>의 <code>http_sso</code>라는 파일에 메일이 기록됩니다. 기본적으로 <code>info</code> 이상의 로깅 수준을 가진 메일만 기록되지만 로깅 수준을 1부터 5까지의 값(1 = errors, 2 = warnings, 3 = info, 4 = debug, 5 = maxdebug)으로 설정하여 로깅 수준을 높일 수 있습니다. 이 라이브러리에는 Messaging Server와 동일한 메일 중요도 개념이 없으므로 수준을 <code>debug</code>로 설정하면 많은 의미 없는 데이터가 생성될 수 있습니다. 또한 <code>http_sso</code> 로그 파일이 일반 Messaging Server 로깅 코드에 의해 관리되지 않으며 정리 또는 롤오버되지 않습니다. 로그 수준을 기본값보다 높게 설정하는 경우 정리 작업은 시스템 관리자의 책임입니다.</p> <p>기본값: 3</p>
<code>local.webmail.sso.singlesignoff</code>	<p>Messaging Server에서 Access Manager로의 단일 사인 오프입니다. Access Manager는 중앙 인증 기관이며 단일 사인 오프는 항상 Access Manager로부터 Messaging Server로 사용됩니다. 이 옵션을 사용하면 사이트에서 사용자가 웹 메일의 <i>로그아웃</i> 버튼을 눌러 Access Manager에서도 로그아웃할지 여부를 구성할 수 있습니다(일부 사용자 정의 작업 생략). 이 옵션은 기본적으로 사용됩니다. 이 옵션을 사용하지 않는 경우에는 로그아웃이 루트 문서를 참조하고 해당 루트 문서는 Access Manager 쿠키가 존재하고 유효한 이상 받은 메일함 디스플레이를 참조하기 때문에 사용자가 기본 웹 메일 클라이언트에서 로그아웃하면 자동으로 다시 로그인됩니다. 따라서, 사이트에서 이 옵션을 사용하지 않도록 선택하면 웹 메일 로그아웃시 발생하는 내용을 사용자 정의해야 합니다.</p> <p>기본값: yes</p>

## SSO 문제 해결

SSO에 문제가 있는 경우 처음 수행할 작업은 오류에 대한 웹 메일 로그 파일 `msg_svr_base/log/http`를 검사하는 것입니다. 로깅 수준을 높이는 것도 유용할 수 있습니다(`configutil -o logfile.http.loglevel -v debug`). 이 작업이 도움이 되지 않는 경우 `msg_svr_base/log/http_sso`에서 `amsdk` 메일을 검사한 다음 `amsdk` 로깅 수준을 높입니다(`configutil -o local.webmail.sso.amloglevel -v 5`). 새 로깅 수준을 적용하려면 서버를 다시 시작해야 합니다.

SSO에 여전히 문제가 있을 경우 로그인하는 동안 **Access Manager**와 **Messaging Server** 모두에서 정규화된 호스트 이름을 사용하는지 확인합니다. 쿠키는 동일한 도메인의 서버 간에만 공유되며 브라우저는 로컬 서버 이름에 대한 도메인이 무엇인지 알지 못하므로 브라우저에서 정규화된 이름을 사용해야 SSO가 작동합니다.

## 신뢰할 수 있는 원 SSO(레거시)

이 절에서는 신뢰할 수 있는 원 SSO에 대해 설명합니다. 이후의 모든 개발에서 **Access Manager**를 사용하게 될 것이므로 이 SSO 방법을 사용하지 않는 것이 좋습니다. 그러나 신뢰할 수 있는 원 SSO에서 사용할 수 있는 기능 중 일부는 현재 **Access Manager SSO**에서 사용할 수 없습니다. 이 절은 다음 내용으로 구성되어 있습니다.

- 144페이지의 "신뢰할 수 있는 원 SSO 개요 및 정의"
- 145페이지의 "신뢰할 수 있는 원 SSO 응용 프로그램"
- 146페이지의 "신뢰할 수 있는 원 SSO 제한"
- 146페이지의 "신뢰할 수 있는 원 SSO 배포 시나리오 예"
- 148페이지의 "신뢰할 수 있는 원 SSO 설정"
- 152페이지의 "Messenger Express의 신뢰할 수 있는 SSO 구성 매개 변수"

## 신뢰할 수 있는 원 SSO 개요 및 정의

SSO를 배포하기 전에 다음 용어에 대해 잘 알고 있어야 합니다.

- **단일 사인 온(SSO)**. 하나의 응용 프로그램에 로그인하여 다른 응용 프로그램에 액세스할 수 있는 기능입니다. 사용자 아이디가 모든 응용 프로그램에서 동일합니다.



- **신뢰할 수 있는 응용 프로그램.** SSO 스키마(SSO 접두어)를 공유하고 서로 간에 쿠키 및 확인을 신뢰하는 응용 프로그램입니다. *피어 SSO 응용 프로그램*이라고도 합니다.
- **신뢰할 수 있는 원.** 신뢰할 수 있는 응용 프로그램 원입니다. 서로 동일한 SSO 접두어를 공유합니다.
- **SSO 접두어.** 동일한 신뢰할 수 있는 원 내의 다른 응용 프로그램이 생성한 쿠키를 찾는 데 사용할 수 있도록 SSO를 배포하는 개인이 정의하고 각 응용 프로그램에 알려진 문자열입니다. 다른 접두어를 사용하는 응용 프로그램은 동일한 원 내에 있지 않으므로 그러한 응용 프로그램 간에 이동하는 경우 다시 인증해야 합니다. 항상 그렇지는 않지만 구성 설정에서 접두어에 후행 "-"가 명시되는 경우가 있습니다.
- **응용 프로그램 아이디.** (appid). SSO 원 내의 각 응용 프로그램에 대해 SSO를 배포하는 개인이 정의한 고유한 문자열입니다.
- **SSO 쿠키.** 브라우저에서 사용자가 일부 응용 프로그램에 인증되었음을 기억하는 데 사용하는 토큰입니다. 쿠키 이름 형식은 *SSO\_prefix-application ID*입니다. 쿠키 값은 일반적으로 응용 프로그램에서 생성되는 세션 아이디인 SSO 키입니다.
- **쿠키 도메인.** 응용 프로그램이 쿠키를 보낼 수 있도록 제한된 도메인입니다. DNS 관점의 도메인입니다.
- **확인 URL.** 한 응용 프로그램에서 다른 응용 프로그램에 있는 쿠키를 확인하는 데 사용되는 URL입니다.

## 신뢰할 수 있는 원 SSO 응용 프로그램

SSO를 구현하기 전에 먼저 이 신뢰할 수 있는 원에 속하는 응용 프로그램을 고려해야 합니다. 이 신뢰할 수 있는 원에 포함될 수 있는 응용 프로그램은 Messenger Express(Messenger Express Multiplexor 사용 또는 사용 안 함), Calendar Express 및 이전 메시징용 iPlanet Delegated Administrator(Sun LDAP Schema 1만 지원하므로 권장되지 않음)입니다.

표 6-2에서는 SSO를 통해 서로 액세스할 수 있는 응용 프로그램을 보여 줍니다. 사용자의 관점에서 첫 번째 열의 응용 프로그램 중 하나에 로그인한 다음 사용자 아이디와 비밀번호를 다시 입력하지 않고 맨 위의 행에 있는 응용 프로그램에 액세스할 수 있다면 SSO가 적용되는 것입니다.

**표 6-2** SSO 상호 운용성

대상:	Calendar Express	Messenger Express	Messenger Express Multiplexor	Delegated Administrator
시작:				
Calendar Express	SSO	SSO	SSO	SSO
Messenger Express	SSO	해당 없음	해당 없음	SSO
Messenger Express Multiplexor	SSO	해당 없음	해당 없음	SSO
Delegated Administrator	SSO	SSO	SSO	해당 없음

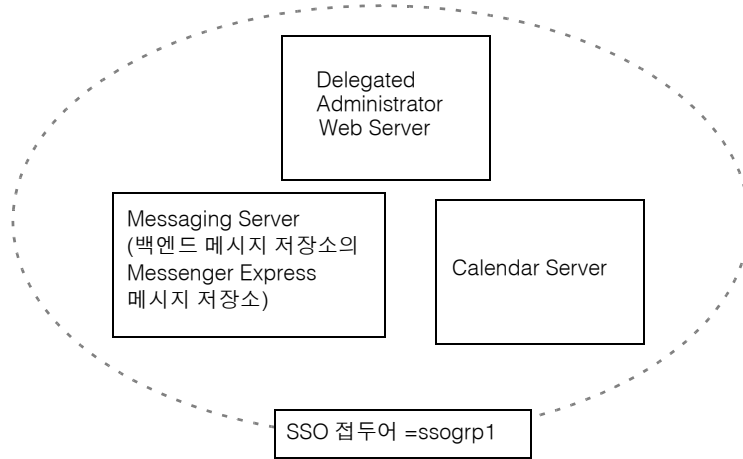
## 신뢰할 수 있는 원 SSO 제한

- 함께 작동하는 SSO 응용 프로그램은 동일한 도메인에 있어야 합니다.
- SSO 응용 프로그램은 서로의 SSO 확인 URL에 액세스할 수 있어야 합니다.
- 브라우저에서 쿠키를 지원해야 합니다.
- 보안상 브라우저가 실행되는 시스템에서는 SSO를 사용하지 마십시오.
- 다른 아이디로 전환하려면 브라우저를 다시 시작해야 합니다.
- Messenger Express와 Sun Java System Calendar Server 모두에서 단일 사인 오프가 사용된다고 가정할 때 Sun Java System Calendar Server에서 로그아웃한 경우에는 Messenger Express에 다시 로그인해야 합니다. Messenger Express에서 로그아웃한 경우에는 Sun Java System Calendar Server에 다시 로그인해야 합니다. 그러나 현재는 이 방법이 적용되지 않으므로 둘 중 하나에서 로그아웃한 후에도 다른 하나에서는 로그인한 상태를 유지할 수 있습니다.

## 신뢰할 수 있는 원 SSO 배포 시나리오 예

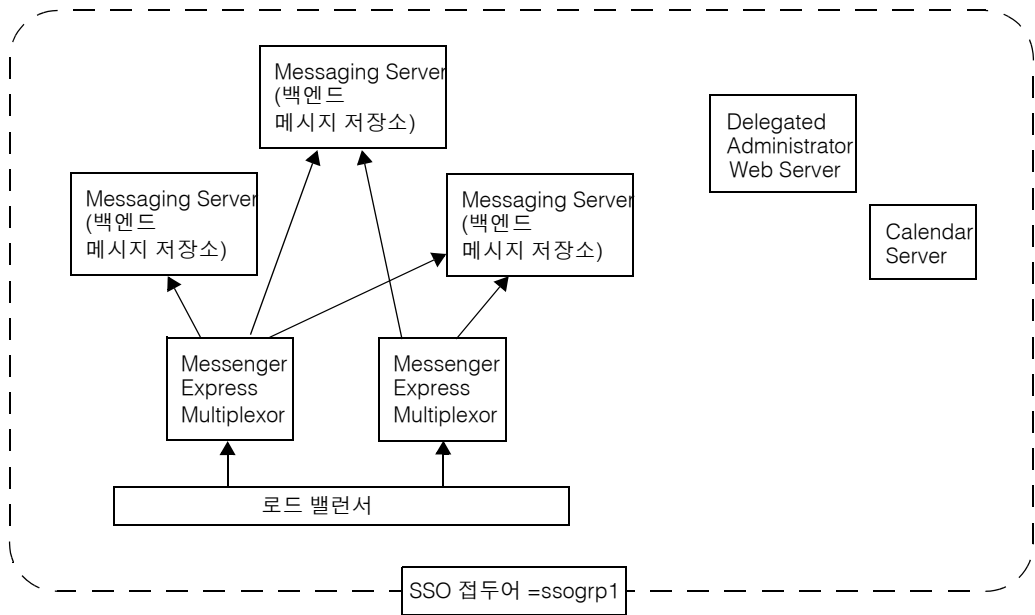
가장 단순한 SSO 배포 시나리오는 Messenger Express와 iPlanet Delegated Administrator for Messaging으로만 구성됩니다. 동일한 신뢰할 수 있는 원 내에 포함되도록 동일한 SSO 접두어를 사용하여 동일한 시스템이나 다른 시스템에 Calendar Express를 추가하여 보다 복잡한 시나리오를 만들 수 있습니다. 이 시나리오는 [그림 6-1](#)에 나와 있습니다.

그림 6-1 단순 SSO 배포



보다 복잡한 배포에는 Messenger Express Multiplexors와 로드 밸런서가 있습니다.

그림 6-2 복잡한 SSO 배포



## 신뢰할 수 있는 원 SSO 설정

이 절에서는 Messenger Express, iPlanet Delegated Administrator for Messaging 및 Calendar Manager에 대한 SSO 설정에 대해 설명합니다.

1. SSO에 대해 Messenger Express를 구성합니다.
  - a. 적절한 SSO `configutil` 매개 변수를 설정합니다.

Delegated Administrator가 있는 Messenger Express에 대해 단일 사인 온(SSO)을 사용하려면 구성 매개 변수를 다음과 같이 설정합니다(기본 도메인을 `siroe.com`으로 가정). 이러한 매개 변수는 표 6-3에 설명되어 있습니다. 루트 사용자가 되어야 합니다(`cd`에서 `instance_root`).

```
configutil -o local.webmail.sso.enable -v 1
configutil -o local.webmail.sso.prefix -v ssogrp1
    ssogrp1 is the default SSO Prefix used by iDA, although you can choose a different prefix,
    using the default would save a little typing when configuring iDA and iCS.
configutil -o local.webmail.sso.id -v ims5
    ims5 is a name you pick to identify Messenger Express (ME) to other applications.
configutil -o local.webmail.sso.cookieDomain -v "siroe.com"
    The above domain must match the domain used by the ME/browser client to connect to
    the servers. Thus, although the hosted domain on this server may be called xyz.com, we
    must use a real domain in the DNS. This value must start with a period.
configutil -o local.webmail.sso.singleSignoff -v 1
configutil -o local.sso.ApplicationID.verifyurl -v \
"http://ApplicationHost:port/verifySSO?"
    ApplicationID is a name we give to the SSO application (example: ida for Delegated
    Administrator, ics50 for Calendar Server). ApplicationHost:port is the host and port number of the
    application. You will have one of these lines for each non-Messaging Server application. Example:
configutil -o local.sso.ida.verifyurl -v \
"http://siroe.com:8080/verifySSO?"
```

- b. 구성을 변경한 후 Messenger Express http 서버를 다시 시작합니다.

```
cd instance_root
./stop-msg http
./start-msg http
```

2. SSO에 대해 Directory Server를 구성합니다.
  - a. 디렉토리에 프록시 사용자 계정을 만듭니다.

프록시 사용자 계정을 사용하면 Delegated Administrator에서 프록시 인증을 위해 Directory Server에 바인드할 수 있습니다. 다음 LDIF 코드(proxy.ldif)를 사용하면 ldapadd를 통해 프록시 사용자 계정 항목을 만들 수 있습니다.

```
dn: uid=proxy, ou=people, o=siroe.com, o=isp
objectclass: top
objectclass: person
objectclass: organizationalperson
objectclass: inetorgperson
uid: proxy
givenname: Proxy
sn: Auth
cn: Proxy Auth
userpassword: proxypassword
```

```
ldapadd -h mysystem.siroe.com -D "cn=Directory Manager" -w
password -v -f proxy.ldif
```

- b. 프록시 사용자 계정 인증을 위해 해당 ACI를 만듭니다.

ldapmodify 유틸리티를 사용하여 Delegated Administrator를 설치할 때 만든 각 접미어에 대한 ACI를 만듭니다.

osiroot - 사용자 데이터를 저장하기 위해 입력한 접미어입니다(기본값: o=isp). osiroot는 조직 트리의 루트입니다.

dcroot - 도메인 정보를 저장하기 위해 입력한 접미어입니다. 기본값은 o=internet입니다.

osiroot - 구성 정보를 저장하기 위해 입력한 접미어이며 사용자 데이터를 저장하기 위해 입력한 값과 동일해야 합니다.

다음은 앞에서 작성한 프록시 사용자의 osiroot에 대한 ACI 항목(aci1.ldif) 예입니다.

```
dn: o=isp
changetype: modify
add:aci
aci: (target="ldap:///o=isp")(targetattr="*")(version 3.0; aci
"proxy";allow (proxy) userdn="ldap:///uid=proxy, ou=people,
o=siroe.com, o=isp");)
```

```
ldapmodify -h siroe.com -D "cn=Directory Manager" -w password  
-v -f aci1.ldif
```

다음과 같이 dcroot에 대해 비슷한 ACI 항목(aci2.ldif)을 만듭니다.

```
dn: o=internet  
changetype: modify  
add:aci  
aci: (target="ldap:///o=internet") (targetattr="*") (version 3.0; acl  
"proxy";allow (proxy) userdn="ldap:///uid=proxy, ou=people, o=siroe.com,  
o=isp");)
```

```
ldapmodify -h siroe.com -D "cn=Directory Manager" -w password  
-v -f aci2.ldif
```

### 3. Delegated Administrator를 구성합니다.

- a. Delegated Administrator resource.properties 파일에 컨텍스트에 대한 프록시 사용자 자격 증명과 쿠키 이름을 추가합니다.

#### Delegated Administrator

*iDA\_server\_root/nda/classes/netscape/nda/servlet/resource.properties*  
파일에서 다음 항목에 대한 주석 처리를 취소하고 수정합니다.

```
LDAPDatabaseInterface-ldapauthdn=Proxy_Auth_DN  
LDAPDatabaseInterface-ldapauthpw=Proxy_Auth_Password  
NDAAuth-singleSignOnId=SSO_Prefix-  
NDAAuth-applicationId=DelAdminID
```

예를 들면 다음과 같습니다.

```
LDAPDatabaseInterface-ldapauthdn=  
uid=proxy, ou=people, o=siroe.com, o=isp  
LDAPDatabaseInterface-ldapauthpw=proxypassword  
NDAAuth-singleSignOnId=ssogrp1-  
NDAAuth-applicationId=id
```

- b. 참여하는 서버의 확인 URL을 추가합니다.

수신하는 단일 사인 온(SSO) 쿠키를 확인하려면 Delegated Administrator에서 연결할 사람을 알고 있어야 합니다. 알려진 모든 참여 서버에 대한 확인 URL을 제공해야 합니다.

다음 예에서는 Messenger Express를 설치하고 해당 응용 프로그램 아이디가 msg5라고 가정합니다. Delegated Administrator `iDA_server_root/nda/classes/netcape/nda/servlet/resource.properties` 파일을 편집하고 다음 항목을 추가합니다.

```
verificationurl-ssogrp1-msg5=http://webmail_hostname:port/VerifySSO?
verificationurl-ssogrp1-ida=http://iDA_hostname:port/VerifySSO?
verificationurl-ssogrp1-ics50=http://iCS_hostname:port/VerifySSO?
```

4. Delegated Administrator 단일 사인 온(SSO) 쿠키 정보를 추가하고 UTF8 매개 변수 인코딩을 사용합니다.
  - a. Delegated Administrator에 대한 컨텍스트 식별자를 정의합니다.
 

`Web_Server_Root/https-instanceName/config/servlets.properties`를 편집하고 `servlet.*.context=ims50` 텍스트에 포함된 모든 행의 주석을 취소합니다. 여기서 \*는 모든 문자열입니다.
  - b. Enterprise Server 구성에서 해당 컨텍스트에 대한 쿠키 이름을 지정합니다.
 

Enterprise Server 파일 `Web_Server_Root/https-instanceName/config/contexts.properties`를 편집하고 파일의 맨 아래쪽에 있는 `#IDACONF-Start` 행 앞에 다음을 추가합니다.

```
context.ims50.sessionCookie=ssogrp1-ida
```
  - c. ims5 컨텍스트에 대해 UTF8 매개 변수 인코딩을 사용합니다.
 

Enterprise Server 구성에서 ims5 컨텍스트에 대해 UTF8 매개 변수 인코딩을 사용하려면 Enterprise Server `WebServer_Root/https-instanceName/config/contexts.properties` 파일에 다음 항목을 추가합니다.

```
context.ims50.parameterEncoding=utf8
```
5. Messenger Express를 다시 시작합니다.

단계 1a에서 2c에 설명된 대로 구성을 변경한 후에는 Messenger Express를 다시 시작해야 변경 내용이 적용됩니다.

```
WebServer_Root/https-instance_name/stop
WebServer_Root/https-instanceName/start
```

- 이 SSO 그룹에서 Calendar를 배포하려면 Calendar Server를 구성합니다.

ics.conf를 편집하고 다음을 추가합니다.

```
sso.appid = "ics50"
sso.appprefix = "ssogrp1"
sso.cookieDomain = ".red.ipplanet.com"
sso.enable = "1"
sso.singlesignoff = "true"
sso.userdomain = "mysystem.red.ipplanet.com"
sso.ims5.url="http://mysystem.red.ipplanet.com:80/VerifySSO?"
sso.ida.url=http://mysystem.red.ipplanet.com:8080/VerifySSO?
```

- Calendar Server를 다시 시작합니다.

```
start-cal
```

- Messenger Express http 서버를 다시 시작합니다.

```
msg_srv_base/sbin/stop-msg http
msg_srv_base/sbin/start-msg http
```

## Messenger Express의 신뢰할 수 있는 SSO 구성 매개 변수

표 6-3에 표시된 것처럼 configutil 명령을 사용하여 Messenger Express에 대한 단일 사인 온(SSO) 구성 매개 변수를 수정할 수 있습니다. configutil에 대한 자세한 내용은 *Messaging Server Reference Manual*을 참조하십시오.

**표 6-3** 신뢰할 수 있는 원 단일 사인 온(SSO) 매개 변수

매개 변수	설명
local.sso.appid.verifyurl	<p>피어 SSO 응용 프로그램에 대한 확인 URL 값을 설정합니다. <i>appid</i>는 해당 SSO 쿠키를 수락하는 피어 SSO 응용 프로그램의 응용 프로그램 아이디입니다. 예를 들어, Delegated Administrator에 대한 기본 <i>appid</i>는 nda45이고 실제 값은 Delegated Administrator resource.properties 파일 항목 NDAAuth-applicationID에 의해 지정됩니다.</p> <p>신뢰할 수 있는 각 피어 SSO 응용 프로그램에 대해 정의된 하나의 매개 변수가 있어야 합니다. 확인 URL의 표준 형식은 다음과 같습니다.</p> <pre>http://nda-host:port/VerifySSO?</pre> <p>여러 Messenger Express Multiplexors 및 Message Store 서버(Messenger Express 실행) 또는 Calendar 프런트 엔드 앞에 로드 밸런서를 사용할 경우 verifyurl에 실제 호스트 이름을 사용하여 각 물리적 시스템에 대해 서로 다른 <i>appid</i>를 지정해야 합니다. 그렇게 하면 쿠키를 확인하는 데 올바른 시스템이 사용됩니다.</p>



**표 6-3** 신뢰할 수 있는 원 단일 사인 온(SSO) 매개 변수

매개 변수	설명
<code>local.webmail.sso.cookieDomain</code>	<p>이 매개 변수의 문자열 값은 Messenger Express HTTP 서버에서 설정한 모든 SSO 쿠키의 쿠키 도메인 값을 설정하는 데 사용됩니다. 기본값은 null입니다.</p> <p>이 도메인은 Messenger Express 브라우저에서 서버에 액세스하는 데 사용한 DNS 도메인과 일치해야 합니다. 호스트된 도메인 이름이 아닙니다.</p>
<code>local.webmail.sso.enable</code>	<p>로그인 페이지를 가져올 때 클라이언트가 표시한 SSO 쿠키 허용 및 확인, 로그인에 성공한 경우 클라이언트에 SSO 쿠키 반환 및 쿠키 확인을 위해 다른 SSO 파트너의 요청에 회신 등을 포함하여 모든 단일 사인 온(SSO) 기능을 사용하거나 사용하지 않습니다.</p> <p>0이 아닌 값을 설정하면 서버에서 모든 SSO 기능을 수행합니다.</p> <p>0을 설정하면 서버에서 이러한 SSO 기능을 수행하지 않습니다.</p> <p>기본값은 0입니다.</p>
<code>local.webmail.sso.id</code>	<p>Messenger Express HTTP 서버에서 설정한 SSO 쿠키의 서식을 지정할 때 이 매개 변수 문자열 값이 응용 프로그램 아이디 값으로 사용됩니다. 기본값은 null입니다.</p> <p>이 값은 임의의 문자열입니다. 이 값은 <code>resource.properties</code> 파일에서 Delegated Administrator에 대해 지정한 값과 일치해야 합니다. <code>resource.properties</code> 의 해당 항목은 다음과 같습니다.</p> <p><code>Verifcationurl-XXX-YYY=http://webmailhost:webmailport/VerifySSO?</code></p> <p>여기서 <code>XXX</code>는 위에서 설정한 <code>local.webmail.sso.prefix</code> 값이고 <code>YYY</code>는 여기서 설정한 <code>local.webmail.sso.id</code> 값입니다.</p>
<code>local.webmail.sso.prefix</code>	<p>Messenger Express HTTP 서버에서 설정한 SSO 쿠키의 서식을 지정할 때 이 매개 변수 문자열 값이 접두어 값으로 사용됩니다. 이 접두어가 있는 SSO 쿠키만 서버에 인식되며 다른 SSO 쿠키는 모두 무시됩니다.</p> <p>이 매개 변수에 null 값을 설정하면 서버에서 모든 SSO 기능을 효과적으로 비활성화할 수 있습니다.</p> <p>기본값은 null입니다.</p> <p>이 문자열은 후행 -가 없는 <code>resource.properties</code> 파일에서 iPlanet Delegated Administrator for Messaging에 사용된 문자열과 일치해야 합니다. 예를 들면 다음과 같습니다.</p> <p><code>NDAAuth-singleSignOnID=ssogrp1-</code></p> <p>이 값을 <code>ssogrp1</code>로 설정해야 합니다.</p>

**표 6-3** 신뢰할 수 있는 원 단일 사인 온(SSO) 매개 변수

매개 변수	설명
local.webmail.sso. singlesignoff	0이 아닌 값으로 설정한 경우 이 매개 변수의 정수 값은 클라이언트가 로그아웃할 때 local.webmail.sso.prefix에 구성된 값과 일치하는 접두어 값을 갖는 클라이언트의 모든 SSO 쿠키를 지웁니다.  0으로 설정하면 Messenger Express는 클라이언트가 로그아웃할 때 해당 클라이언트의 SSO 쿠키만 지웁니다.  기본값은 0입니다.

## 멀티플렉서 서비스 구성 및 관리

이 장에서는 Messaging Server에 포함된 두 멀티플렉서인 표준 메일 프로토콜(POP, IMAP 및 SMTP) Messaging Multiplexor(MMP)와 Messenger Express 웹 인터페이스에 사용되는 Messenger Express Multiplexor에 대해 설명합니다.

이 장에서는 다음 항목에 대해 설명합니다.

- [155페이지의 "멀티플렉서 서비스"](#)
- [157페이지의 "Messaging Multiplexor 정보"](#)
- [163페이지의 "Messaging Multiplexor 설정"](#)
- [166페이지의 "SSL로 MMP 구성"](#)
- [172페이지의 "페일오버 MMP LDAP 서버 설정"](#)
- [172페이지의 "Messenger Express Multiplexor 정보"](#)

### 멀티플렉서 서비스

멀티플렉서는 여러 메시지 저장소에 간접적으로 연결하는 데 사용할 수 있는 하나의 도메인 이름을 제공하기 때문에 수평 확장성(시스템을 추가하면 더 많은 사용자를 지원할 수 있는 기능)을 확보하는 데 필수적입니다. 멀티플렉서는 보안 이점도 제공할 수 있습니다.

MMP는 Messaging Server와 별도로 관리되지만 Messenger Express Multiplexor는 메시지 저장소 및 메일 액세스 설치에 포함되어 있는 HTTP 서비스(mshttpd)에 내장되어 있습니다.

## 멀티플렉서의 장점

사용량이 많은 Messaging Server의 메시지 저장소는 크기가 매우 커질 수 있습니다. 따라서 사용자 메일함과 사용자 연결을 여러 서버로 분산시키면 용량과 성능을 향상시킬 수 있습니다. 또한 하나의 고용량의 큰 다중 프로세서 시스템보다는 여러 대의 작은 서버 시스템을 사용하는 것이 보다 비용면에서 효율적입니다.

메일 서버 설치의 크기가 커서 여러 메시지 저장소를 사용해야 하는 경우 멀티플렉서를 사용하면 여러 가지 장점이 있습니다. 사용자와 메시지 저장소를 간접적으로 연결하고 Messaging Server 간의 사용자 계정을 간단하게 재구성할 수 있으므로 다음과 같은 장점을 제공합니다.

- **간단한 사용자 관리**

모든 사용자는 하나의 서버에 연결하기 때문에(POP, IMAP, SMTP 또는 웹 액세스용 멀티플렉서 시스템을 각각 분리하는 경우에는 하나 이상) 전자 메일 클라이언트를 미리 구성하고 일정한 로그인 정보를 모든 사용자에게 배포할 수 있습니다. 이를 통해 관리 작업이 단순화하고 오류가 발생할 수 있는 로그인 정보가 배포되는 가능성을 줄일 수 있습니다.

특히 로드가 많은 상황에서는 여러 대의 멀티플렉서 서버를 동일한 구성으로 실행하고 DNS 라운드 로빈이나 로드 균형 조정 시스템을 사용하여 연결을 관리할 수 있습니다.

멀티플렉서는 LDAP 디렉토리에 저장된 정보를 사용하여 각 사용자의 Messaging Server를 찾기 때문에 시스템 관리자는 사용자를 새 서버로 간단하게 옮길 수 있으며 사용자도 쉽게 알 수 있습니다. 관리자는 사용자의 메일함을 한 Messaging Server에서 다른 Messaging Server로 옮긴 다음 LDAP 디렉토리에서 사용자 항목을 업데이트할 수 있습니다. 사용자의 메일 주소, 메일함 액세스 및 기타 클라이언트 기본 설정은 변경되지 않습니다.

- **향상된 성능**

메시지 저장소가 너무 커서 단일 시스템에 저장할 수 없는 경우 일부 메시지 저장소를 다른 시스템으로 옮겨서 로드의 균형을 조정할 수 있습니다.

각 시스템마다 다른 클래스의 사용자를 할당할 수 있습니다. 예를 들어 프리미엄 사용자는 용량이 크고 성능도 강력한 시스템에 위치시킬 수 있습니다.

멀티플렉서는 버퍼링을 수행하기 때문에 클라이언트 연결 속도가 늦더라도(예: 모뎀 사용) Messaging Server의 속도가 느려지지 않습니다.

- **비용 절감**  
멀티플렉서로 여러 Messaging Server를 효율적으로 관리할 수 있기 때문에 하나의 대형 시스템보다는 여러 대의 작은 서버 시스템을 구입하면 전체 비용을 줄일 수 있습니다.
- **뛰어난 확장성**  
멀티플렉서를 사용하면 구성을 쉽게 확장할 수 있습니다. 성능이나 저장소 용량의 필요가 증가하면 기존 투자를 교체할 필요 없이 시스템을 계속 추가할 수 있습니다.
- **사용자 중단 시간 최소화**  
멀티플렉서를 사용하여 여러 소형 저장소 시스템에서 대규모 사용자 기반으로 분산하면 사용자 중단 시간을 차단합니다. 즉, 개별 서버가 실패하더라도 해당 서버의 사용자에게만 영향이 미칩니다.
- **향상된 보안**  
멀티플렉서가 설치된 서버 시스템을 방화벽 시스템으로 사용할 수 있습니다. 모든 클라이언트 연결을 이 시스템을 통해 경로 지정하면 외부 컴퓨터가 내부 메시지 저장소 시스템에 액세스하는 것을 제한할 수 있습니다. 멀티플렉서는 클라이언트와 암호화된 통신 및 암호화되지 않은 통신을 모두 지원합니다.

## Messaging Multiplexor 정보

Sun Java System Messaging Multiplexor(MMP)는 여러 개의 백엔드 Messaging Server에 대한 연결의 단일 지점 역할을 하는 특수 Messaging Server입니다. Messaging Multiplexor를 사용하여 대규모 메시징 서비스 공급자는 POP 및 IMAP 사용자 메일함을 여러 시스템에서 분산시켜 메시지 저장소 용량을 늘릴 수 있습니다. 모든 사용자가 하나의 멀티플렉서 서버에 연결하고 이 서버가 각 연결을 적절한 Messaging Server로 리디렉션합니다.

여러 사용자에게 전자 메일 서비스를 제공하는 경우 Messaging Multiplexor를 설치 및 구성하여 전체 Messaging Server의 배열이 메일 사용자에게는 하나의 호스트로 표시되도록 할 수 있습니다.

Messaging Multiplexor는 Messaging Server의 일부로 제공됩니다. MMP는 Messaging Server 또는 기타 Sun Java System 서버를 설치할 때 함께 설치하거나 나중에 MMP만 따로 설치할 수 있습니다. MMP 지원 기능은 다음과 같습니다.

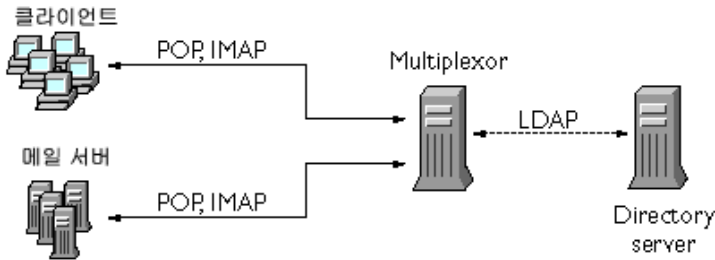
- 메일 클라이언트와의 암호화(SSL)된 통신 및 암호화되지 않은 통신 모두
- 클라이언트 인증서 기반 인증(159페이지의 "인증서 기반 클라이언트 인증"에서 설명함)
- 사용자 사전 인증(160페이지의 "사용자 사전 인증"에서 설명함)

- 다른 IP 주소에 수신하고 도메인 이름을 사용자 아이디에 자동으로 추가하는 가상 도메인(161페이지의 "MMP 가상 도메인"에서 설명함)
- 다른 서버에 MMP 다중 설치(Sun Java Enterprise System 설치 설명서 참조)
- 향상된 LDAP 검색
- 레거시 POP 클라이언트용 POP before SMTP 서비스. 자세한 내용은 675페이지의 "POP before SMTP 사용"을 참조하십시오.

## Messaging Multiplexor의 작동 방식

MMP는 메일 사용자를 여러 서버 시스템으로 분산시키는 다중 스레드 서버입니다. MMP는 다른 서버 시스템(사용자 메일함이 있는 시스템)으로 지정된 수신 클라이언트 연결을 처리합니다. 클라이언트는 MMP 자체에 연결하며, MMP는 사용자에게 대한 적절한 서버를 결정하고 해당 서버에 연결한 다음 클라이언트와 서버 사이에 데이터를 전달합니다. 이 기능을 통해 인터넷 서비스 공급자 및 기타 대규모 설치 조직에서는 메시지 저장소를 여러 시스템에 분산시킬 수 있으며(용량 증가), 사용자(효율성 증가)와 외부 클라이언트(보안 증가)에게는 하나의 메일 호스트로 보이게 할 수 있습니다. 그림 7-1은 MMP 설치에서 서버와 클라이언트가 상호간 어떻게 관련되어 있는지 보여 줍니다.

그림 7-1 MMP 설치 환경에서의 클라이언트와 서버



모든 POP, IMAP 및 SMTP 클라이언트를 Messaging Multiplexor와 함께 사용할 수 있습니다. MMP는 연결을 수용하고, LDAP 디렉토리 조회를 수행하고, 연결을 적절하게 경로 지정합니다. 다른 메일 서버 설치와 마찬가지로 각 사용자에게는 특정 주소와 특정 Messaging Server의 메일함이 할당됩니다. 하지만 모든 연결은 MMP를 통해 경로가 지정됩니다.

다음은 사용자 연결을 설정하는 세부 단계입니다.

1. 사용자의 클라이언트가 MMP에 연결합니다. MMP는 예비 인증 정보(아이디)를 받습니다.
2. MMP는 Directory Server에 쿼리하여 사용자의 메일함이 포함된 Messaging Server를 결정합니다.
3. MMP는 적절한 Messaging Server에 연결하여 인증을 재수행한 다음 연결 기간 동안 전달 파이프 역할을 합니다.

## 암호화(SSL) 옵션

Messaging Multiplexor는 Messaging Server와 메일 클라이언트 사이의 암호화(SSL)된 통신 및 암호화되지 않은 통신을 모두 지원합니다. Messaging Server는 새 인증서 데이터베이스 형식(cert8.db)을 지원합니다.

SSL이 활성화된 경우 MMP는 STARTTLS를 지원하며 MMP가 SSL IMAP, POP 및 SMTP 연결에 대한 추가 포트에서 수신하도록 구성할 수도 있습니다.

IMAP, POP 및 SMTP 서비스에 대해 SSL 암호화를 활성화하려면

ImapProxyAService.cfg, PopProxyAService.cfg 및 SmtproxyAService.cfg 파일을 각각 편집합니다. 또한 IMAP, POP 및 SMTP 서버 포트의 보안 여부에 관계 없이 이러한 모든 서버 포트 목록이 포함되게 하려면 AService.cfg 파일의 default:ServiceList 옵션을 수정해야 합니다. 자세한 내용은 [166페이지의 "SSL로 MMP 구성"](#)을 참조하십시오.

기본적으로 SSL 구성 매개 변수는 주석 처리되어 있으므로 SSL이 활성화되어 있지 않습니다. SSL을 활성화하려면 SSL 서버 인증서를 설치해야 합니다. 그런 다음 SSL 매개 변수의 주석 처리를 제거하고 적절하게 설정해야 합니다. SSL 매개 변수의 목록을 보려면 *Sun Java System Messaging Server Administration Reference*(<http://docs.sun.com/doc/819-0106>)를 참조하십시오.

## 인증서 기반 클라이언트 인증

MMP는 인증서 매핑 파일(certmap)을 사용하여 클라이언트의 인증을 사용자/그룹 Directory Server의 올바른 사용자와 일치시킬 수 있습니다.

인증서 기반 클라이언트 인증을 사용하려면 [159페이지의 "암호화\(SSL\) 옵션"](#)에 설명된 대로 SSL 암호화도 활성화해야 합니다.

또한 저장소 관리자도 구성해야 합니다. 메일 관리자를 사용할 수는 있지만 필요에 따라 사용 권한을 설정할 수 있도록 `mmpstore` 등의 고유한 사용자 아이디를 만드는 것이 좋습니다.

MMP는 `certmap` 플러그인을 지원하지 않습니다. 대신 MMP에서는 `certmap.conf` 파일에 향상된 `DNComps` 및 `FilterComps` 속성 값 항목을 사용할 수 있습니다. 이러한 향상된 형식의 항목은 다음 형식을 사용합니다.

```
mapname:DNComps FROMATTR=TOATTR
mapname:FilterComps FROMATTR=TOATTR
```

인증서의 `subjectDN`에 있는 `FROMATTR` 값은 `TOATTR=value` 요소와 함께 LDAP 쿼리를 구성하는 데 사용할 수 있습니다. 예를 들어 `subjectDN`이 `"cn=Pilar Lorca, ou=pilar, o=siroe.com"`인 인증서는 다음 행을 사용하여 `"(uid=pilar)"`의 쿼리에 매핑할 수 있습니다.

```
mapname:FilterComps ou=uid
```

IMAP 또는 POP 서비스에 대한 인증서 기반 인증을 활성화하려면 다음을 수행합니다.

1. 저장소 관리자로 사용할 사용자 아이디를 결정합니다.  
메일 관리자가 이 용도로 사용할 수 있는 경우 저장소 관리자의 고유한 사용자 아이디 (예: `mmpstore`)를 만드는 것이 좋습니다.
2. 159페이지의 "암호화(SSL) 옵션"에 설명된 대로 SSL 암호화가 활성화되었는지 확인합니다.
3. 구성 파일에 `certmap.conf` 파일의 위치를 지정하여 MMP가 인증서 기반 클라이언트 인증을 사용하도록 구성합니다.
4. 653페이지의 "신뢰할 수 있는 CA의 인증서 설치"에 설명된 대로 적어도 하나의 신뢰할 수 있는 CA 인증서를 설치합니다.

## 사용자 사전 인증

MMP는 수신되는 사용자로 디렉토리에 바인딩하고 결과를 로깅하여 사용자를 사전 인증할 수 있는 옵션을 제공합니다.

---

**주**                      사용자 사전 인증을 활성화하면 서버 성능이 저하됩니다.

---

로그 항목의 형식은 다음과 같습니다.

```
date time (sid 0xhex) user name pre-authenticated - client IP address, server IP address
```



여기서 *date*는 `yyyymmdd`의 형식이고, *time*은 `hhmmss` 형식으로 서버에서 구성된 시간이고, *hex*는 16진수로 표시되는 세션 식별자(`sid`)이며, *user name*에는 가상 도메인(있는 경우)이 포함되며, IP 주소는 점으로 구분된 네 개의 번호 형식으로 되어 있습니다.

## MMP 가상 도메인

MMP 가상 도메인은 서버 IP 주소와 연관된 구성 설정 세트입니다. 이 기능의 기본 용도는 각 서버 IP 주소에 대해 서로 다른 기본 도메인을 제공하는 것입니다.

사용자는 짧은 형식의 `userID` 또는 `user@domain` 형식의 정규화된 `userID`로 MMP에 인증할 수 있습니다. 짧은 형식의 `userID`를 제공하면 MMP는 지정된 경우 `DefaultDomain` 설정을 추가합니다. 그 결과 여러 개의 호스트된 도메인을 지원하는 사이트는 서버 IP 주소와 MMP 가상 도메인을 각 호스트된 도메인에 연결시켜 짧은 사용자 아이디를 사용할 수 있게 할 수 있습니다.

특정 호스트된 도메인에 대한 사용자 하위 트리를 찾는 경우 해당 도메인의 LDAP 도메인 트리 항목에서 `inetDomainBaseDN` 속성을 찾는 것이 좋습니다. 백엔드 메시지 저장소도 LDAP에서 사용자를 조회해야 하고 가상 도메인을 지원하지 않기 때문에 MMP의 `LdapUrl` 설정은 이러한 검색에 적합하지 않습니다.

Sun LDAP Schema 2가 활성화된 경우(*Sun Java Enterprise System 설치 설명서* 및 *Sun Java System Communications Services Schema Reference Manual* 참조) 지정된 도메인의 사용자 하위 트리는 해당 도메인의 조직 노드 아래에 있는 하위 트리의 모든 사용자입니다.

가상 도메인을 활성화하려면 `VirtualDomainFile` 설정이 가상 도메인 매핑 파일에 대한 전체 경로를 지정하는 인스턴스 디렉토리에서 `ImapProxyAService.cfg`, `PopProxyAService.cfg` 또는 `SmtpproxyAService.cfg` 파일을 편집합니다.

가상 도메인 파일의 각 항목에 대한 구문은 다음과 같습니다.

```
vimap name IPaddr
name:parameter value
```

여기서 *name*은 IP 주소를 구성 매개 변수와 연결시키는 데만 사용되며 원하는 모든 이름을 사용할 수 있습니다. 또한 *IPaddr*은 점으로 구분된 네 개의 번호 형식이며 *parameter* 및 *value* 쌍은 가상 도메인을 구성합니다. 설정 시 가상 도메인 구성 매개 변수 값은 전역 구성 매개 변수 값보다 우선합니다.

다음은 가상 도메인에 지정할 수 있는 구성 매개 변수입니다.

AuthCacheSize 및 AuthCacheSizeTTL  
AuthService  
BindDN 및 BindPass  
CertMap  
ClientLookup  
CRAMs  
DefaultDomain  
DomainDelim  
HostedDomains  
LdapCacheSize 및 LdapCacheTTL  
LdapURL  
MailHostAttrs  
PreAuth  
ReplayFormat  
RestrictPlainPasswords  
StoreAdmin 및 StoreAdminPass  
SearchFormat  
TCPAccess  
TCPAccessAttr

---

**주** LdapURL이 제대로 설정되어 있지 않으면 BindDN, BindPass, LdapCacheSize 및 LdapCacheTTL 설정이 무시됩니다.

---

이러한 구성 매개 변수에 대한 자세한 내용은 *Messaging Server Reference Manual*을 참조하십시오.

## SMTP 프록시 정보

MMP에는 기본적으로 비활성화되어 있는 SMTP 프록시가 포함되어 있습니다. 인터넷 메일 표준이 이미 SMTP(DNS MX 레코드)의 수평 확장을 위한 적절한 기법을 제공하므로 대부분의 사이트에는 SMTP 프록시가 필요하지 않습니다.

SMTP 프록시는 유용한 보안 기능을 제공합니다. 우선 SMTP 프록시는 POP 프록시와 통합되어 일부 레거시 POP 클라이언트에 필요한 POP before SMTP 인증 기능을 구현합니다. 자세한 내용은 [675페이지](#)의 "POP before SMTP 사용"을 참조하십시오. 또한 SMTP 프록시를 사용하여 SSL 가속 하드웨어에 대한 투자를 최대화할 수 있습니다. [660페이지](#)의 "SMTP 프록시를 사용하여 SSL 성능을 최적화하는 방법"을 참조하십시오.

# Messaging Multiplexor 설정

Messaging Server의 초기 런타임 구성 중에 시스템에서 MMP를 구성할 것인지 여부를 결정하였습니다. Messaging Server와 같은 시스템에 설정하거나 별도의 시스템에 설정할 수 있습니다.

---

**주** MMP는 DNS 결과를 캐시하지 않습니다. Messaging Server 제품을 배포하려면 로컬 네트워크에 고품질 캐싱 DNS 서버가 필요합니다.

---

다음 절에서는 MMP의 설정 방법에 대해 설명합니다.

- 163페이지의 "MMP를 구성하기 전에"
- 164페이지의 "Multiplexor 구성"
- 164페이지의 "Multiplexor 파일"
- 166페이지의 "Multiplexor 시작"
- 166페이지의 "기존 MMP 수정"

다음에서 MMP에 대한 추가 정보를 볼 수 있습니다.

- *Sun Java System Messaging Server Administration Reference: MMP Syntax and Structure*(<http://docs.sun.com/doc/819-0106>)

## MMP를 구성하기 전에

MMP를 구성하기 전에 다음을 수행합니다.

1. MMP를 구성할 시스템을 선택합니다. MMP 전용 시스템을 사용하는 것이 가장 좋습니다.

---

**주** POP 또는 IMAP 서버가 실행 중인 시스템에서는 MMP를 활성화하지 않는 것이 좋습니다.

Messaging Server와 같은 시스템에 MMP를 설치한 경우 POP와 IMAP 서버를 비표준 포트로 설정해야 합니다. 이렇게 하면 MMP와 Messaging Server 포트가 서로 충돌하지 않습니다.

---

2. MMP를 구성할 시스템에서 MMP가 사용할 UNIX 시스템 사용자를 만듭니다. 이 새 사용자는 UNIX 시스템 그룹에 속해야 합니다. [40페이지의 "UNIX 시스템 사용자와 그룹 만들기"](#)를 참조하십시오.
3. 아직 설정하지 않은 경우 Messaging Server에 사용할 Directory Server와 호스트 시스템을 설정합니다. [41페이지의 "Messaging Server 구성을 위해 Directory Server 준비"](#)를 참조하십시오.
4. 백엔드 서버에 앞서 MMP를 업그레이드할 경우 ImapProxyAService.cfg에서 Capability 옵션을 다음과 같이 설정하여 이전 백엔드의 capability 명령에 대한 응답과 일치시켜야 합니다.

```
IMAP4 IMAP4rev1 ACL QUOTA LITERAL+ NAMESPACE UIDPLUS CHILDREN
LANGUAGE XSENDER X-NETSCAPE XSERVERINFO
```

위에서 편의상 줄 바꿈이 되었지만 실제 구성 값은 한 줄로 되어 있어야 합니다.

## Multiplexor 구성

MMP를 구성하려면 Messaging Multiplexor를 활성화하는 옵션이 있는 Messaging Server 구성 프로그램을 사용해야 합니다. 구성 프로그램에 대한 자세한 내용은 [51페이지의 "Messaging Server 초기 런타임 구성 만들기"](#)를 참조하십시오.

MMP를 구성하려면 다음을 수행합니다.

1. MMP를 설치 및 구성하려는 시스템에 Sun Java System Messaging Server를 설치합니다.
2. Messaging Server 초기 런타임 구성을 만들어 MMP를 구성합니다. [51페이지의 "Messaging Server 초기 런타임 구성 만들기"](#)를 참조하십시오.  
다음과 같은 예외가 있습니다. Messaging Server를 설치할 때 Messaging Multiplexor 옵션만 확인합니다.

## Multiplexor 파일

Messaging Multiplexor 파일은 `msg_svr_base/config` 구성 파일 디렉토리에 저장됩니다. 표 7-1에 나열된 Messaging Multiplexor 구성 파일의 구성 매개 변수를 수동으로 편집해야 합니다. 모든 MMP 구성 매개 변수에 대한 자세한 내용은 *Sun Java System Messaging Server Administration Reference*를 참조하십시오.

표 7-1 Messaging Multiplexor 구성 파일

파일	설명
PopProxyAService.cfg	POP 서비스에 사용되는 구성 변수를 지정하는 구성 파일
PopProxyAService-def.cfg	POP 서비스 구성 템플릿. 파일은 start-msg mmp로 초기 MMP가 시작되고 난 후에만 만들어집니다.
ImapProxyAService.cfg	IMAP 서비스에 사용되는 구성 변수를 지정하는 구성 파일
ImapProxyAService-def.cfg	IMAP 서비스 구성 템플릿. 파일은 start-msg mmp로 초기 MMP가 시작되고 난 후에만 만들어집니다.
AService.cfg	시작할 서비스를 지정하고 POP 및 IMAP 서비스 모두가 공유하는 몇 가지 옵션을 지정하는 구성 파일
AService-def.cfg	시작할 서비스를 지정하고 POP 및 IMAP 서비스가 공유하는 몇 가지 옵션을 지정하는 구성 템플릿. 파일은 MMP start-msg mmp로 초기 MMP가 시작되고 난 후에만 만들어집니다.
SmtProxyAService.cfg	SMTP Proxy 서비스에 사용되는 구성 변수를 지정하는 선택적 구성 파일. POP before SMTP를 활성화하는 경우에 필요합니다. POP before SMTP가 활성화되지 않은 경우에도 SSL 하드웨어를 최대한 지원하려는 경우 유용합니다. POP before SMTP에 대한 자세한 내용은 675페이지의 "POP before SMTP 사용"을 참조하십시오.
SmtProxyAService-def.cfg	SMTP 프록시 서비스에 사용되는 구성 변수를 지정하는 구성 템플릿. 파일은 start-msg mmp로 초기 MMP가 시작되고 난 후에만 만들어집니다.

예를 들어 LogDir 및 LogLevel 매개 변수는 모든 구성 파일에서 찾을 수 있습니다. ImapProxyAService.cfg에서는 IMAP 관련 이벤트의 로깅 매개 변수를 지정하는 데 사용되며, 이와 유사하게 PopProxyAService.cfg의 해당 매개 변수는 POP 관련 이벤트의 로깅 매개 변수 구성에 사용됩니다. SmtProxyAService.cfg에서는 SMTP 프록시 관련 이벤트에 대한 로깅을 지정하는 데 사용됩니다.

하지만 AService.cfg에서는 LogDir 및 LogLevel이 POP, IMAP 또는 SMTP 서비스를 시작하는 데 실패하는 경우와 같은 MMP 실패를 로깅하는 데 사용됩니다.

**주** MMP를 구성하거나 업그레이드하면 구성 템플릿 파일을 덮어씁니다.

## Multiplexor 시작

Messaging Multiplexor의 인스턴스를 시작, 중지 또는 갱신하려면 *msg\_svr\_base*/sbin 디렉토리에 있는 표 7-2의 다음 명령 중 하나를 사용합니다.

**표 7-2** MMP 명령

옵션	설명
start-msg mmp	MMP를 시작합니다(다른 MMP가 이미 실행 중인 경우에도 시작).
stop-msg mmp	최근 시작한 MMP를 중지합니다.
refresh mmp	활성 연결을 중단하지 않고 이미 실행 중인 MMP의 구성을 새로 고칩니다.

## 기존 MMP 수정

MMP의 기존 인스턴스를 수정하려면 필요에 따라 *ImapProxyAService.cfg* 및 *PopProxyAService.cfg* 구성 파일을 편집합니다. 이러한 구성 파일은 *msg\_svr\_base*/config 하위 디렉토리에 있습니다.

## SSL로 MMP 구성

SSL을 사용하기 위해 MMP를 구성하려면 다음을 수행합니다.

---

**주** 여기서는 MMP가 메시지 저장소 또는 MTA가 없는 시스템에 설치되어 있는 것으로 가정합니다.

---

1. Admin Server가 설치되어 있는 경우에는 Admin Console을 사용하여 SSL 서버 인증서를 설치하십시오. Admin Server가 설치되어 있지 않으면 인증서 설치에 NSS 도구를 사용합니다. 660페이지의 "네트워크 보안 서비스 도구"를 참조하십시오.

<http://docs.sun.com/db/doc/816-5572-10>을 참조하십시오.

2. Admin Server 서버가 설치되어 있는 경우에는 명령줄에서 다음 심볼릭 링크를 통해 간단히 처리할 수 있습니다.

```
cd msg_svr_base/config
ln -s /var/mps/serverroot/alias/admin-serv-instance-cert7.db cert7.db
ln -s /var/mps/serverroot/alias/admin-serv-instance-key3.db key3.db
```

또한 MMP가 실행될 시스템 ID에서 해당 파일을 소유해야 합니다. Messaging Server는 새 인증서 데이터베이스 형식(cert8.db)을 지원합니다.

3. `sslpassword.conf` 파일은 초기 Messaging Server 런타임 구성 중에 설정하므로 설정할 필요가 없습니다. 51페이지의 "Messaging Server 초기 런타임 구성 만들기"를 참조하십시오.

---

**주**            단계 1-8에 해당하는 대체 방법은 기존 Messaging 또는 Directory Server에서 `cert7.db`, `key3.db`, `secmod.db` 및 `sslpassword.conf` 파일을 복사하는 것입니다. 이러한 서버에는 이미 설치된 동일한 도메인에 적합한 서버 인증서와 키가 있어야 합니다.

---

4. `ImapProxyAService.cfg` 파일을 편집하고 관련 SSL 설정의 주석 처리를 제거합니다.
5. SSL 및 POP를 사용하려면 `PopProxyAService.cfg` 파일을 편집하고 관련 SSL 설정의 주석 처리를 제거합니다.  
  
또는 `AService.cfg` 파일을 편집하고 `ServiceList` 설정의 110 뒤에 |995를 추가해야 합니다.
6. `BindDN` 및 `BindPass` 옵션이 `ImapProxyAService.cfg`와 `PopProxyAService.cfg` 파일에 설정되어 있는지 확인합니다.  
  
또한 `DefaultDomain` 옵션을 기본 도메인(정규화되지 않은 아이디에 사용할 도메인)으로 설정해야 합니다.

서버측 SSL 지원만 필요한 경우에는 이로써 작업이 끝났습니다. `msg_svr_base/sbin` 디렉토리에서 다음 명령으로 MMP를 시작합니다.

```
start-msg mmp
```

클라이언트 인증서 기반 로그인을 사용하려면 다음을 수행합니다.

1. 클라이언트 인증서 복사본과 이 복사본을 서명한 CA 인증서를 얻습니다.
2. 이전과 같이 MMP와 같은 시스템에서 Sun ONE 콘솔을 시작하지만 이번에는 CA 인증서를 Trusted Certificate Authority로 가져옵니다.
3. Messaging Server 설치 도중 만든 저장소 관리자를 사용합니다.  
  
자세한 내용은 557페이지의 "저장소에 대한 관리자 액세스 지정"을 참조하십시오.

4. MMP에 대한 `certmap.conf` 파일을 만듭니다. 예를 들면 다음과 같습니다.

```
certmap default default
default:DNComps
default:FilterComps e=mail
```

이것은 LDAP 서버에서 메일 속성을 찾아서 인증서 DN의 `e` 필드와 일치하는 항목을 찾는다는 의미입니다.

5. `ImapProxyAService.cfg` 파일을 편집하고 다음을 설정합니다.
- `CertMapFile`을 `certmap.conf`로 설정합니다.
  - `StoreAdmin` 및 `StorePass`를 단계 3의 값으로 설정합니다.
  - `UserGroupDN`을 사용자 및 그룹 트리의 루트로 설정합니다.
6. POP3을 사용한 클라이언트 인증서가 필요한 경우 `PopProxyAService.cfg` 파일에 대해 단계 5를 반복합니다.
7. MMP가 이미 실행 중이 아닌 경우 `msg_svr_base/sbin` 디렉토리에서 다음 명령을 사용하여 실행합니다.
- ```
start-msg mmp
```
8. 클라이언트 인증서를 클라이언트로 가져옵니다. Netscape™ Communicator에서 자물쇠(보안) 아이콘을 누른 다음 인증서 아래에서 사용자를 선택하고 인증서 가져 오기...를 선택합니다. 그런 다음 지시에 따릅니다.

---

주                    어느 곳에서나 클라이언트 인증서를 사용하려면 모든 사용자가 이 단계를 수행해야 합니다.

---

## 샘플 토폴로지

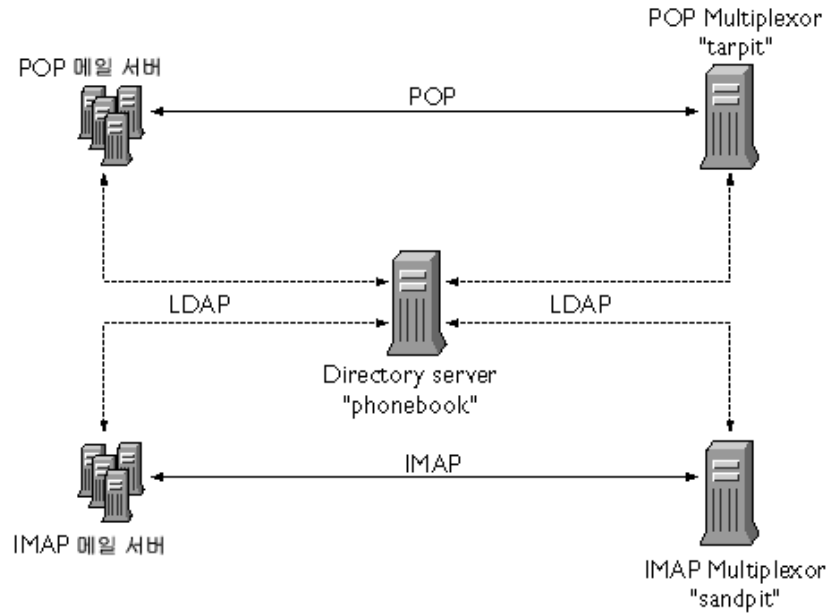
가상의 Siroe Corporation에는 별도의 시스템에 두 개의 Messaging Multiplexor가 있으며 각각 여러 Messaging Server를 지원합니다. POP 및 IMAP 사용자 메일함은 Messaging Server 시스템에서 분산되어 있으며, 각 서버는 POP 또는 IMAP 전용 서버입니다.

`ImapProxyAService` 항목을 `ServiceList` 설정에서 제거하면 POP 서비스에 대한 클라이언트 액세스를 제한할 수 있습니다. 마찬가지로 `ServiceList` 설정에서 `PopProxyAService` 항목을 제거하면 IMAP 서비스에 대한 클라이언트 액세스를 제한할 수 있습니다. 각 Messaging Multiplexor는 POP만 지원하거나 IMAP만 지원합니다. LDAP 디렉토리 서비스는 별도의 전용 시스템에 있습니다.

이 토폴로지는 그림 7-2에서 볼 수 있습니다.



그림 7-2 여러 Messaging Server를 지원하는 여러 MMP



### IMAP 구성 예

그림 7-2의 IMAP Messaging Multiplexor는 두 개의 프로세서가 있는 시스템인 sandpit에 설치되어 있습니다. 이 Messaging Multiplexor는 표준 포트에서 IMAP 연결(143)에 대기합니다. Messaging Multiplexor는 호스트 phonebook의 LDAP 서버와 사용자 메일함 정보를 통신하며, 적절한 IMAP 서버로 연결의 경로를 지정합니다. 이것은 IMAP 기능 문자열을 대체하고, 가상 도메인 파일을 제공하며, SSL 통신을 지원합니다.

ImapProxyAService.cfg 구성 파일은 다음과 같습니다.

```

default:LdapUrl          ldap://phonebook.siroe.com/o=internet
default:LogDir           /opt/SUNWmsgsr/config/log
default:LogLevel         5
default:BindDN           "cn=Directory Manager"
default:BindPass         secret
default:BacksidePort     143
default:Timeout          1800
default:Capability       "IMAP4 IMAP4rev1 ACL QUOTA LITERAL+ NAMESPACE UIDPLUS CHILDREN
BINARY LANGUAGE XSENDER X-NETSCAPE XSERVERINFO"
default:SearchFormat     (uid=%s)
default:SSEnable         yes
default:SSLPorts         993
default:SSLSecmodFile    /opt/SUNWmsgsr/config/secmod.db
default:SSLCertFile      /opt/SUNWmsgsr/config/cert7.db
default:SSLKeyFile       /opt/SUNWmsgsr/config/key3.db
default:SSLKeyPasswdFile ""
default:SSLCipherSpecs   all
default:SSLCertNicknames Siroe.com Server-Cert
default:SSLCacheDir      /opt/SUNWmsgsr/config
default:SSLBacksidePort  993
default:VirtualDomainFile /opt/SUNWmsgsr/config/vdmap.cfg
default:VirtualDomainDelim @
default:ServerDownAlert  "your IMAP server appears to be temporarily out of service"
default:MailHostAttrs    mailHost
default:PreAuth          no
default:CRAMs            no
default:AuthCacheSize    10000
default:AuthCacheTTL     900
default:AuthService      no
default:AuthServiceTTL   0
default:BGMax            10000
default:BGPenalty        2
default:BGMaxBadness     60
default:BGDecay          900
default:BGLinear         no
default:BGExcluded       /opt/SUNWmsgsr/config/bgexcl.cfg
default:ConnLimits       0.0.0.0|0.0.0.0:20
default:LdapCacheSize    10000
default:LdapCacheTTL     900
default:HostedDomains    yes
default:DefaultDomain    Siroe.com

```

## POP 구성 예

그림 7-2에서 예로 든 POP Messaging Multiplexor는 4개의 프로세서가 있는 tarpit 시스템에 설치되어 있습니다. 이 Messaging Multiplexor는 표준 포트에서 POP 연결(110)을 수신합니다. Messaging Multiplexor는 호스트 phonebook의 LDAP 서버와 사용자 메일함 정보를 통신하며, 적절한 POP 서버로 연결의 경로를 지정합니다. 또한 스푸핑 메일 파일도 제공합니다.

해당 PopProxyAService.cfg 구성 파일은 다음과 같습니다.

```

default:LdapUrl          ldap://phonebook.siroe.com/o=internet
default:LogDir           /opt/SUNWmsgsr/config/log
default:LogLevel        5
default:BindDN           "cn=Directory Manager"
default:BindPass         password
default:BacksidePort     110
default:Timeout          1800
default:SearchFormat     (uid=%s)
default:SslEnable        no
default:VirtualDomainFile /opt/SUNWmsgsr/config/vdmap.cfg
default:VirtualDomainDelim @
default:MailHostAttrs    mailHost
default:PreAuth          no
default:CRAMS            no
default:AuthCacheSize    10000
default:AuthCacheTTL     900
default:AuthService      no
default:AuthServiceTTL   0
default:BGMax            10000
default:BGPenalty        2
default:BGMaxBadness     60
default:BGDecay          900
default:BGLinear         no
default:BGExcluded       /opt/SUNWmsgsr/config/bgexcl.cfg
default:ConnLimits       0.0.0.0|0.0.0.0:20
default:LdapCacheSize    10000
default:LdapCacheTTL     900
default:HostedDomains    yes
default:DefaultDomain    Siroe.com

```

## MMP 작업

이 절에서는 기타 MMP 구성 작업을 설명합니다. 다음 사항이 추가되었습니다.

- 172페이지의 "MMP를 사용하여 메일 액세스 구성"
- 172페이지의 "페일오버 MMP LDAP 서버 설정"

## MMP를 사용하여 메일 액세스 구성

MMP는 자동으로 구성되지 않기 때문에 명시적으로 구성해야 합니다. 또한, MMP는 PORT\_ACCESS 매핑 테이블을 사용하지 않습니다. 특정 IP 주소의 SMTP 연결을 거부하기를 원하고 MMP를 사용하는 경우 TCPAccess 옵션을 사용해야 합니다. 이 옵션 구문은 mailDomainAllowedServiceAccess와 동일합니다. *Sun Java System Communications Services Schema Reference Manual*(<http://docs.sun.com/doc/819-0113>)을 참조하십시오. 이 항목은 666페이지의 "필터 문"에도 설명되어 있습니다.

## 페일오버 MMP LDAP 서버 설정

하나의 LDAP 서버가 실패하면 다른 서버가 처리하도록 MMP에 대한 LDAP 서버를 두 개 이상 지정할 수 있습니다. PopProxyAservice.cfg 또는 IMAPProxyAservice.cfg를 다음과 같이 수정합니다.

```
default:LdapUrl "ldap://ldap01.yourdomain ldap02.yourdomain/o=INTERNET"
```

# Messenger Express Multiplexor 정보

Sun Java System Messenger Express Multiplexor는 HTTP 액세스 서비스에 대한 단일 연결 지점의 역할을 하는 특수한 서버입니다. Messenger Express는 Sun Java System Messaging Server HTTP 서비스에 대한 클라이언트 인터페이스입니다. 모든 사용자는 하나의 메시징 프록시 서버에 연결하고 이 서버가 사용자를 적절한 메일함으로 지정합니다. 따라서 전체 Messaging Server가 메일 사용자에게는 하나의 호스트로 표시됩니다.

Messaging Multiplexor(MMP)가 POP 및 IMAP 서버에 연결하는 반면 Messenger Express Multiplexor는 HTTP 서버에 연결합니다. 즉, Messenger Express Multiplexor와 Messenger Express의 관계는 MMP와 POP 및 IMAP의 관계와 같습니다.

Messenger Express Multiplexor는 MMP와 같이 다음을 지원합니다.

- 메일 클라이언트와의 비암호화 및 암호화(SSL) 통신  
SSL 구성에 대한 자세한 내용은 19장, "보안 및 액세스 제어 구성"의 *보안 및 액세스 제어*를 참조하십시오.

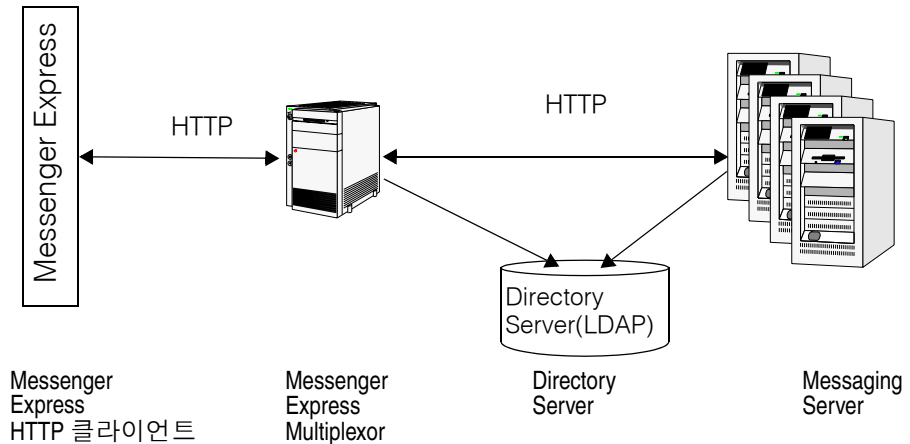
- 호스트된 도메인

Messenger Express Multiplexor는 MMP와는 달리 mshttpd 서비스에 내장되어 있으며, 따라서 같은 로깅 및 구성 기법을 사용합니다.

## Messenger Express Multiplexor의 작동 방식

Messenger Express Multiplexor는 멀티플렉서 역할을 하는 프록시 Messaging Server로 구성됩니다. 이를 통해 Messaging Server의 HTTP 서비스(Messenger Express)에 연결할 수 있습니다. Messenger Express Multiplexor는 메일함을 여러 서버 시스템으로 분산시킵니다. 클라이언트는 Messenger Express에 로그인할 때 멀티플렉서에 연결합니다. 이 때 Messenger Express는 사용자에게 대한 올바른 서버를 결정하고, 그 서버에 연결한 다음 클라이언트와 서버 사이에 데이터를 전달합니다. 이 기능을 사용하여 대규모 설치에서는 메시지 저장소를 여러 시스템에 분산시킬 수 있으며(용량 증가), 사용자(효율성 증가)와 외부 클라이언트(보안 증가)에게는 하나의 메일 호스트로 보이게 합니다. [173페이지의 그림 7-3](#)은 Messaging Server 설치에서 Messenger Express Multiplexor가 상주하는 위치를 설명합니다.

그림 7-3 iPlanet Messenger Express Multiplexor 개요



Messenger Express Multiplexor는 연결을 설정하여 적절히 경로를 지정함으로써 Messenger Express 클라이언트와 Messaging Servers 사이에서 인터페이스 역할을 합니다. 다른 메일 서버 설치와 마찬가지로 각 사용자에게는 특정 주소와 특정 Messaging Server의 메일함이 할당됩니다. 하지만 모든 HTTP 연결은 Messenger Express Multiplexor를 통해 경로가 지정됩니다.

다음은 사용자 연결을 설정할 때 수행되는 단계입니다.

1. 사용자의 클라이언트가 Messenger Express Multiplexor에 연결하면 Messenger Express Multiplexor는 임시 인증 정보를 받습니다.
2. Messenger Express Multiplexor는 Directory Server에 쿼리하여 사용자의 메일함이 포함된 Messaging Server를 확인합니다.
3. Messenger Express Multiplexor는 연관된 Messaging Server로 연결하고, 인증을 다시 수행한 다음 세션 기간 동안 통과 파이프의 역할을 합니다.

## Messenger Express Multiplexor 설정

이 절에서는 Messenger Express Multiplexor를 설정 및 구성하는 단계를 안내하며 다음 항목에 대해 설명합니다.

- 174페이지의 "프록시 시스템에 Messaging Server 설치"
- 174페이지의 "Messenger Express Multiplexor 매개 변수 구성"
- 176페이지의 "Messenger Express Multiplexor 활성화"

### 프록시 시스템에 Messaging Server 설치

첫 번째 단계는 Messenger Express Multiplexor가 될 프록시 시스템에 Messaging Server를 설치하는 것입니다. 구체적인 설치 지침에 대해서는 *Sun Java Enterprise System 설치 설명서*를 참조하십시오.

Messaging Server를, 백엔드 Messaging Server를 가리키는 사용자 및 그룹 디렉토리 서버로 구성합니다. 이 디렉토리 서버는 Messenger Express Multiplexor를 통해 사용자를 Messaging Server에 인증하는 데 사용됩니다.

### Messenger Express Multiplexor 매개 변수 구성

프록시 시스템에 Messaging Server를 설치한 뒤에는 다음과 같이 Messenger Express Multiplexor 매개 변수를 구성합니다.

1. 필요한 백엔드 Messaging Server 정보를 수집합니다.

백엔드 Messaging Server의 디렉토리에서 `configutil` 명령을 실행하여 이 절 뒤에 서 설명하는 매개 변수의 값을 결정합니다. 올바르게 설정하려면 프록시 시스템(멀티플렉서가 활성화되는 위치)의 구성이 백엔드 Messaging Server와 일치해야 합니다.

2. Messenger Express Multiplexor에 대한 구성 매개 변수를 설정합니다.

프록시 시스템 Messaging Server의 `msg_srv_base/sbin/configutil` 디렉토리에서 `configutil` 명령을 실행하여 구성 값을 설정합니다. 이러한 값은 백엔드 Messaging Server의 값과 일치해야 합니다.

다음 절에서는 Messenger Express Multiplexor를 설정하는 데 필요한 `configutil` 매개 변수에 대해 설명합니다.

- [175페이지의 "LDAP 매개 변수"](#)
- [176페이지의 "dcroot"](#)
- [176페이지의 "기본 도메인"](#)
- [176페이지의 "로그인 구분자"](#)

### LDAP 매개 변수

Messenger Express Multiplexor를 활성화하기 전에 Directory Server 매개 변수가 올바르게 지정되었는지 확인해야 합니다. LDAP 매개 변수를 결정하려면 적절한 백엔드 Messaging Server 인스턴스 디렉토리에서 다음 명령을 실행합니다.

- `configutil -o local.ugldaphost`

이 매개 변수는 백엔드 Messaging Server가 사용하는 사용자 및 그룹 LDAP Directory Server를 표시합니다. `ldaphost`가 백엔드 Messaging Server가 사용하는 것과 같은 값으로 설정되었는지(또는 복제된 LDAP 서버에 같은 데이터가 포함되었는지) 확인합니다.

- `configutil -o local.ugldapbinddn`  
`configutil -o local.ugldapbindcred`

이 매개 변수는 사용자 및 그룹 Directory Server 관리자의 DN과 비밀번호를 표시합니다. `ldapbinddn` 및 `ldapbindcred` 모두가 백엔드 Messaging Server 사양과 동일해야 합니다.

### ***dcroot***

*dcroot*가 올바르게 지정되었는지 확인해야 합니다. *dcroot*를 결정하려면 적절한 Messaging Server 인스턴스 디렉토리에서 다음 명령을 실행합니다.

```
configutil -o service.dcroot
```

### ***기본 도메인***

Messaging Server 기본 도메인(*defaultdomain*)이 올바르게 지정되었는지 확인해야 합니다. Messaging Server 기본 도메인을 결정하려면 적절한 Messaging Server 인스턴스 디렉토리에서 다음 *configutil* 명령을 실행합니다.

```
configutil -o service.defaultdomain
```

### ***로그인 구분자***

로그인 구분자(*loginseparator*)가 백엔드 Messaging Server에 의해 사용되는 로그인 구분자와 일치하는지 확인합니다. Messaging Server 로그인 구분자를 결정하려면 적절한 백엔드 Messaging Server 인스턴스 디렉토리에서 *configutil* 명령을 실행합니다.

```
configutil -o service.loginseparator
```

## **Messenger Express Multiplexor 활성화**

구성 매개 변수를 설정한 뒤에는 프록시 시스템에서 Messenger Express Multiplexor를 활성화할 수 있습니다. 이렇게 하려면 프록시 서버에 있는 Messaging Server 인스턴스의 *msg\_svr\_base/sbin/configutil* 디렉토리에서 다음 *configutil* 명령을 실행합니다.

```
configutil -o local.service.http.proxy -v 1
```

여기서 1은 Messenger Express Multiplexor를 활성화합니다(기본값 0).

로컬이 아닌 사용자(로그인한 서버에 해당 메일 호스트가 없음)가 로그인하고 *local.service.http.proxy*의 값이 0인 경우, 사용자는 자신의 호스트로 지정되고 호스트 이름 변경을 볼 수 있게 되므로 멀티플렉서가 활성화되지 않았습니다.

*local.service.http.proxy*의 값이 1로 설정되어 있고 멀티플렉서가 활성화되어 있으면, 호스트 이름이 변경되지 않고 전체 Messaging Server 배열이 로컬이 아닌 메일 사용자에게 하나의 호스트로 나타납니다.

로컬 사용자(로그인한 서버가 메일 호스트가 아님)의 경우 서버는

*local.service.http.proxy* 매개 변수 값에 관계 없이 로컬 메시지 저장소를 사용합니다. 프록시와 로컬 사용자가 같은 Messaging Server에 있을 수 있습니다.



## 설정 테스트

이 절에서는 Messenger Express Multiplexor 설정을 테스트하는 방법과 로그 파일에서 메일을 찾는 방법에 대해 설명합니다. 여기서는 Messenger Express Multiplexor를 구성하고 활성화한 것으로 가정합니다.

### Messenger Express 클라이언트에 액세스

설치를 테스트하기 전에 Messenger Express 제품에 대해 잘 알고 있어야 합니다. 또한 이전에 만든 테스트 계정이 있어야 합니다.

Messenger Express Multiplexor 프록시를 테스트하려면 다음 단계를 수행합니다.

1. Messenger Express Multiplexor를 통해 다음 브라우저 위치에 입력하여 Messenger Express에 연결합니다.  
`http://msgserver_name`  
예를 들면 다음과 같습니다.  
`http://budgie.sesta.com`
2. 이전에 만든 테스트 계정을 사용하여 Messenger Express에 로그인합니다.
3. 성공적으로 로그인할 수 있고 백엔드 Messaging Server의 메일에 액세스할 수 있어야 합니다.
4. Messenger Express를 통해 로그인한 뒤 Messaging Server 이름이 변경되면 `local.service.http.proxy`가 1로 설정되었으며 메시징 프록시 서버를 다시 시작했는지 확인합니다. Messenger Express Multiplexor는 사용자에게 하나의 메일 호스트 모양을 제공해야 합니다.

### 오류 메시지

사용자 아이디, 비밀번호를 입력하고 Connect를 누르면 오류 메시지를 받는 경우 프록시 시스템의 HTTP 로그 파일을 검토해야 합니다. 오류 메시지에 대한 자세한 내용은 `msg_svr_base/log` 디렉토리로 이동합니다. 일반적으로 오류 메시지에는 문제를 진단할 수 있는 충분한 정보가 포함되어 있습니다. 문제 진단에 필요한 정보가 부족한 경우에는 고객 지원 센터에 문의하십시오.

## Messenger Express Multiplexor 관리

이 절에서는 Messenger Express Multiplexor의 기본 관리 기능에 대해 설명합니다.

### SSL 구성 및 관리

Messenger Express Multiplexor에 대한 SSL(Secure Sockets Layer)을 구성 및 관리하려면 [656페이지의 "SSL 사용 및 암호문 선택"](#)을 참조하십시오.

### 여러 프록시 서버 설정

하나의 이름으로 주소 지정되는 여러 개의 Messenger Express Multiplexor를 설정하려면 세션 인식 로드 균형 조정 장치를 사용할 수 있습니다. 이 장치를 사용하면 특정 클라이언트에서 고유 서버로 모든 요청을 경로 지정할 수 있습니다.

### 여러 버전의 Messaging Server 및 Messenger Express Multiplexor 관리

Messenger Express Multiplexor와 백엔드 메일 호스트에 대해 여러 버전의 Messaging Server를 사용하는 경우 Messenger Express 정적 파일을 업데이트하여 서버 간의 호환성을 확인할 수 있습니다.

Messenger Express 인터페이스를 구성하는 정적 파일은 사용자의 메일 호스트가 아니라 Messenger Express Multiplexor에서 직접 제공됩니다. 멀티플렉서는 이러한 파일을 `msg_svr_base/config/html` 디렉토리에서 찾습니다.

서버 간의 호환성을 위해 이러한 파일을 업데이트하려면 새 버전의 Messaging Server에 있는 `msg_svr_base/config/html` 디렉토리의 전체 내용(Messenger Express 인터페이스를 구성하는 정적 파일로 구성됨)을 기존 버전의 Messaging Server의 동일한 디렉토리의 내용으로 대체합니다.

예를 들어 백엔드 Messaging Server가 Messaging Server 6을 사용하고 Messaging Server 6 2005Q1을 Messenger Express Multiplexor로 설치한 경우, Messenger Express Multiplexor의 `msg_svr_base/config/html` 디렉토리 전체 내용을 Messaging Server 6 2003Q4 백엔드 서버의 같은 디렉토리 내용으로 대체해야 합니다. Messaging Server 6 2003Q4을 Messaging Server 6 2005Q1로 업그레이드하는 경우 Messenger Express Multiplexor 서버에 대한 `msg_svr_base/config/html` 디렉토리의 이러한 정적 파일도 함께 업데이트할 수 있습니다.

## Messenger Express Multiplexor로 백엔드 Messaging Server의 포트 구성

Messenger Express Multiplexor로 HTTP Messaging Server의 포트를 구성하려면 Multiplexor 시스템에서 다음 `configutil` 명령을 사용합니다.

```
local.service.http.proxy.port.hostname
```

여기서 `hostname`은 백엔드 HTTP Messaging Server의 호스트입니다.

예를 들어 백엔드 Messaging Server의 호스트 이름이 `sesta.com`이고 포트 번호가 8888인 경우 명령의 형식은 다음과 같습니다.

```
configutil -o local.service.http.proxy.port.store.sesta.com -v 8888
```

`local.service.proxy.port`는 자체 포트가 있는 경우(예: `local.service.proxy.admin`)를 제외하고 모든 백엔드 메시지 저장소에 적용됩니다.

## 단일 사인 온(SSO) 구성

단일 사인 온(SSO)은 Messenger Express Multiplexor 시스템에서 다음의 추가 구성을 사용하여 Messaging(HTTP) 서버와 동일한 방법으로 구성해야 합니다.

```
configutil -o local.service.http.proxy.admin -v store_administrator
```

여기서 `store_administrator`는 백엔드 Messaging Server 설치 중에 지정한 백엔드 저장소 관리자입니다.

```
configutil -o local.service.http.proxy.adminpass -v store_admin_password
```

여기서 `store_admin_password`는 백엔드 Messaging Server 설치 중에 지정한 백엔드 저장소 관리자 비밀번호입니다.

서로 다른 저장소 관리자와 비밀번호를 사용하는 여러 백엔드 Messaging Server가 있는 경우, 정규화된 호스트 이름을 Messenger Express Multiplexor의 각 구성 변수에 추가하여 개별적으로 구성할 수 있습니다.

```
configutil -o local.service.http.proxy.admin.hostname -v store_administrator
```

```
configutil -o local.service.http.proxy.adminpass.hostname -v store_admin_password
```

여기서 `hostname`은 백엔드 HTTP Messaging Server의 호스트이고, `store_administrator` 및 `store_admin_password`는 백엔드 Messaging Server 설치 중에 지정한 백엔드 저장소 관리자 및 비밀번호입니다.

사용자가 백엔드 서버에 로그인할 수 있도록 하기 위해 Messenger Express Multiplexor는 proxyauth 로그인 명령을 사용합니다. proxyauth를 활성화하려면 백엔드 메시지 저장소에서 다음 configutil 매개 변수를 사용합니다.

```
configutil -o service.http.allowadminproxy -v 1
```

---

**주** Messenger Express Multiplexor를 통해 단일 사인 온(SSO)이 활성화된 경우에는 백엔드 HTTP Messaging Server에서 구성할 필요가 없습니다.

---

Identity Server에서 Messenger Express Multiplexor SSO를 구성하려면 다음 configutil 매개 변수를 활성화합니다.

```
./configutil -o local.webmail.sso.amcookieName -v iPlanetDirectoryPro  
./configutil -o local.webmail.sso.amNamingURL -v \  
    http://identity host: identity port/amserver/namingservice
```

# MTA 개념

이 장에서는 MTA의 개념에 대해 설명합니다. 이 장은 다음 내용으로 구성되어 있습니다.

- 181페이지의 "MTA 기능"
- 185페이지의 "MTA 구조 및 메일 흐름 개요"
- 187페이지의 "디스패처"
- 189페이지의 "다시 쓰기 규칙"
- 189페이지의 "채널"
- 194페이지의 "MTA 디렉토리 정보"
- 194페이지의 "Job Controller"

## MTA 기능

Message Transfer Agent 또는 MTA는 Messaging Server의 구성 요소입니다(183페이지의 그림 8-1). 가장 기본적인 수준에서 MTA는 메일 라우터입니다. MTA는 다른 서버에서 메일을 수락하여 주소를 읽은 다음 최종 대상(일반적으로 사용자의 메일함)으로 가는 도중에 있는 다음 서버로 라우팅합니다.

수년 동안 많은 기능이 MTA에 추가되었으며 이에 따라서 MTA의 크기, 기능 및 복잡도가 증가했습니다. 이러한 MTA 기능은 중복되기는 하지만 일반적으로 다음과 같이 분류할 수 있습니다.

- **라우팅.** 메일을 수락하여 필요에 따라(예: 별칭인 경우) 확장 또는 변환한 후에 다음 서버, 채널, 프로그램, 파일 등에 라우팅합니다. 라우팅 기능은 관리자가 메시지가 라우팅되는 방법에 대한 내부 및 외부 기법을 지정하는 수준까지 확장되었습니다. 예를 들어, SMTP 인증 사용, 다양한 SMTP 명령 및 프로토콜 사용, TCP/IP 또는 DNS 조회 지원, 작업 제출, 프로세스 제어 및 메시지 대기열 등을 지정할 수 있게 된 것입니다.

- **주소 다시 쓰기.** 봉투 주소는 흔히 라우팅 프로세스의 일부로 다시 쓰여지지만 봉투 또는 헤더 주소를 더 적절하거나 원하는 형태로 다시 쓸 수 있습니다.
- **필터링.** MTA는 주소, 도메인, 가능한 바이러스 및 스팸 내용, 크기, IP 주소, 헤더 내용 등에 기초하여 메일을 필터링할 수 있습니다. 필터링된 메일은 삭제, 거부 또는 수정되거나, 파일 또는 프로그램으로 보내지거나, 사용자 메일함으로 가는 도중의 다음 서버로 보내질 수 있습니다.
- **내용 수정.** 메일 헤더와 내용을 수정할 수 있습니다. 예를 들어 메일을 특정 클라이언트나 특수한 문자 세트에서 읽을 수 있게 만들거나 스팸 또는 바이러스를 검사합니다.
- **감사.** 누가 언제, 어디서, 무엇을 제출했는지 추적합니다.

184페이지의 그림 8-2에 나온 여러 하위 구성 요소와 프로세스가 이러한 기능을 지원합니다. 이 장에서는 이러한 하위 구성 요소와 프로세스에 대해 설명합니다. 또한 시스템 관리자는 여러 도구를 사용하여 이러한 기능을 활성화하고 구성할 수 있습니다. 이러한 도구에는 MTA 옵션, configutil 매개 변수, 매핑 테이블, 키워드, 채널, 다시 쓰기 규칙 등이 포함됩니다. 이러한 도구에 대해서는 MTA 다음 장에서 설명합니다.

- 9장, "MTA 주소 변환 및 라우팅"
- 10장, "MTA 서비스 및 구성 정보"
- 11장, "다시 쓰기 규칙 구성"
- 12장, "채널 정의 구성"
- 13장, "미리 정의된 채널 사용"
- 14장, "Messaging Server에 스팸 및 바이러스 필터링 프로그램 통합"
- 15장, "LMTP 전달"
- 16장, "휴가 자동 메일 회신"
- 17장, "메일 필터링 및 액세스 제어"
- 19장, "보안 및 액세스 제어 구성"
- 21장, "로깅 관리"

- 22장, "MTA 문제 해결"
- 23장, "Messaging Server 모니터링"

그림 8-1 Messaging Server, 단순화된 구성 요소 보기(Messenger Express는 표시되지 않음)

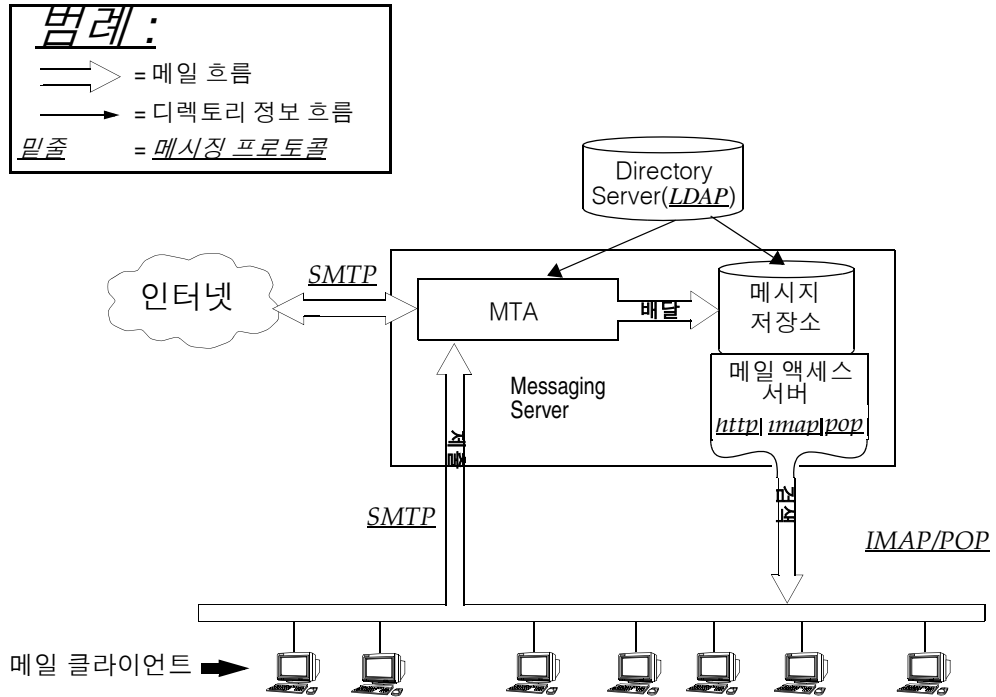
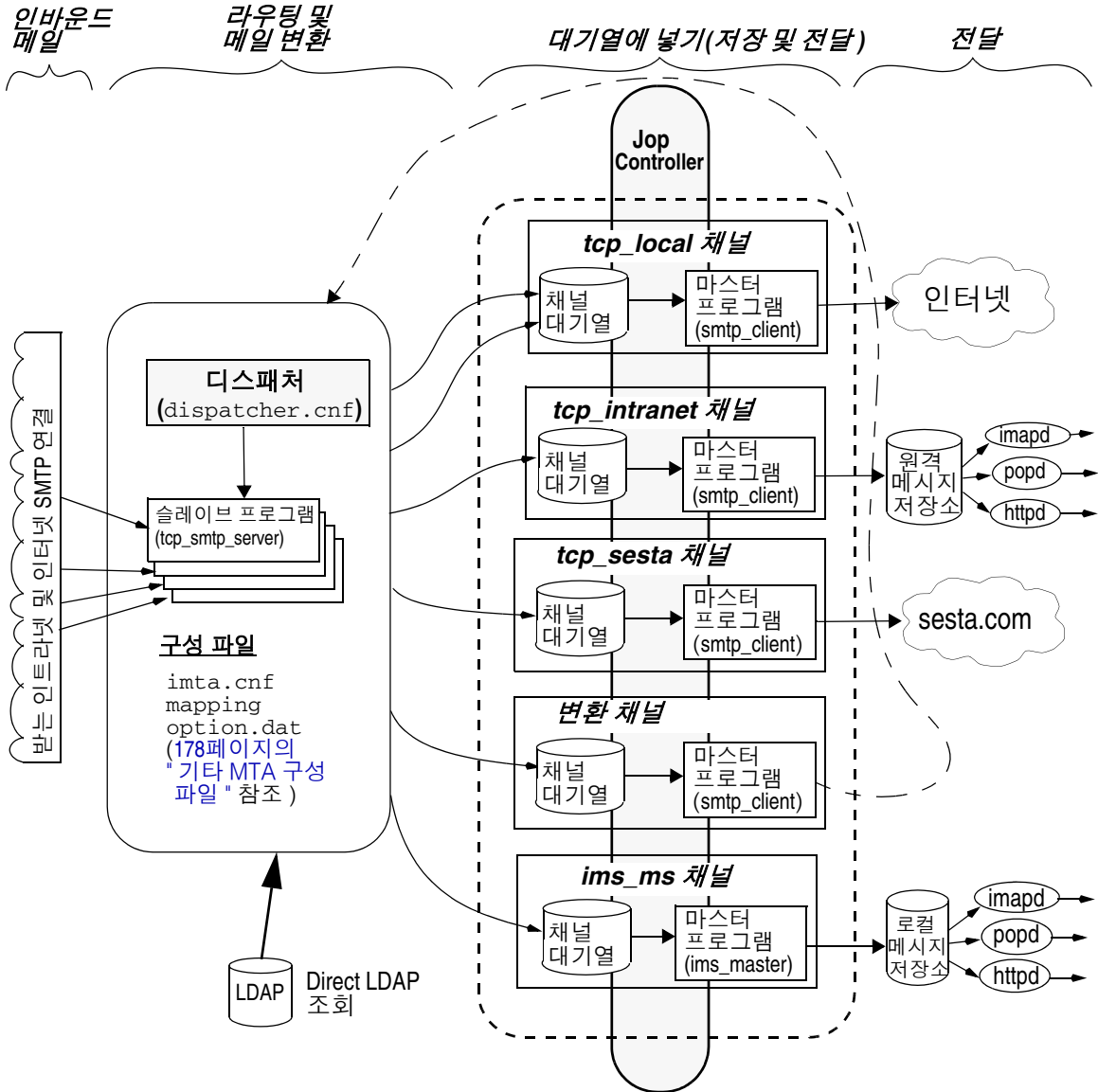


그림 8-2 MTA 구조





# MTA 구조 및 메일 흐름 개요

이 절에서는 MTA 구조 및 메일 흐름(그림 8-2)의 개요를 설명합니다. MTA는 상당히 복잡한 구성 요소이며 그림 8-2는 시스템을 통과하는 메일 흐름을 *단순하게* 표현한 것임을 유의하십시오. 실제로 이 그림은 시스템을 통과하는 모든 메일 흐름을 정확하게 나타내지 않습니다. 그러나 개념적 논의를 위해서는 이 그림으로 충분할 것입니다.

## 디스패처 및 SMTP 서버(슬레이브 프로그램)

메일은 SMTP 세션을 통해 인터넷 또는 인트라넷에서 MTA로 들어옵니다. MTA가 SMTP 연결에 대한 요청을 받으면 MTA *디스패처*(다중 스레드 연결 디스패칭 에이전트)는 SMTP 세션을 처리하기 위해 *슬레이브* 프로그램(tcp\_smtp\_server)을 실행합니다. 디스패처는 각 서비스에 대한 다중 스레드 프로세스 풀을 유지 관리합니다. 추가 세션이 요청되면 디스패처는 각 세션을 처리하기 위해 SMTP 서버 프로그램을 활성화합니다. 디스패처 프로세스 풀의 프로세스는 동시에 여러 연결을 처리할 수 있습니다. 디스패처와 슬레이브 프로그램은 서로 협력하여 각각의 받는 메일에 대한 여러 다른 기능을 수행합니다. 세 가지 기본 기능은 다음과 같습니다.

- 메일 차단 - 지정된 IP 주소, 메일 주소, 포트, 채널, 헤더 문자열 등에 기초하여 메일을 차단할 수 있습니다(17장, "메일 필터링 및 액세스 제어").
- 주소 변경 - 받는 From: 또는 To: 주소를 다른 형식으로 다시 쓸 수 있습니다.
- 채널 대기열에 포함 - 메일을 보내야 하는 채널을 결정하기 위해 다시 쓰기 규칙을 통해 주소가 실행됩니다.

자세한 내용은 187페이지의 "디스패처"를 참조하십시오.

## 라우팅 및 주소 다시 쓰기

SMTP 서버가 메일을 대기열에 포함시키지만 변환 채널 및 재처리 채널을 비롯한 여러 다른 채널도 이를 수행할 수 있습니다. 이 전달 단계가 진행되는 동안에 여러 작업이 수행되지만 기본 작업은 다음과 같습니다.

- 별칭 확장
- 메일을 대기열에 포함시켜야 하는 채널을 결정하기 위해 다시 쓰기 규칙을 통한 주소 실행 및 주소의 도메인 부분을 적절한 또는 원하는 형식으로 다시 쓰기
- 채널 키워드 처리
- 적절한 채널 대기열로 메일 보내기

## 채널

채널은 메일 처리에 사용되는 기본 MTA 구성 요소입니다. 채널은 다른 시스템(예: 다른 MTA, 다른 채널 또는 로컬 메시지 저장소)과의 메일 연결을 나타냅니다. 메일이 들어오면 메일의 소스 및 대상에 따라 각기 다른 메일에 다른 라우팅 및 처리가 필요합니다. 예를 들어, 로컬 메시지 저장소로 전달할 메일, 인터넷에 전달할 메일, 메일 시스템 내의 다른 MTA로 전달할 메일 등은 서로 다른 방식으로 처리됩니다. 채널은 각 연결에 필요한 처리 및 라우팅을 사용자 정의하기 위한 기법을 제공합니다. 기본 설치에서 대부분의 메일은 인터넷, 인트라넷 및 로컬 메일을 처리하는 채널로 이동합니다.

특정 상황을 위한 특수한 채널을 만들 수도 있습니다. 예를 들어, 특정 인터넷 도메인이 메일을 매우 느린 속도로 처리하기 때문에 이 도메인으로 주소 지정된 메일이 MTA의 성능을 저하시킨다고 가정해 봅시다. 이 경우 느린 도메인으로 주소 지정된 메일을 위한 특수한 처리를 제공하는 특정 채널을 만들어 이 도메인 병목 현상을 줄일 수 있습니다.

주소의 도메인 부분은 메일을 대기열에 포함시킬 채널을 결정합니다. 도메인을 읽고 적절한 채널을 결정하는 기법을 다시 쓰기 규칙이라고 부릅니다(189페이지의 "다시 쓰기 규칙" 참조).

채널은 일반적으로 채널 대기열과 *마스터 프로그램*이라고 부르는 채널 처리 프로그램으로 구성됩니다. 슬레이브 프로그램이 메일을 적절한 채널 대기열로 전달한 후 마스터 프로그램은 원하는 처리 및 라우팅을 수행합니다. 다시 쓰기 규칙과 마찬가지로 채널은 `imta.cnf` 파일에서 지정 및 구성합니다. 채널 항목의 예는 다음과 같습니다.

```
tcp_intranet smtp mx single_sys subdirs 20 noreverse maxjobs 7 SMTP_POOL
maytlssserver allowswitchchannel saslswitchchannel tcp_auth
tcp_intranet-daemon
```

이 경우에 첫 번째 단어 `tcp_intranet`은 채널 이름입니다. 마지막 단어는 채널 태그라고 부릅니다. 그 사이에 있는 단어는 채널 키워드라고 부르며 메일이 처리되는 방법을 지정합니다. 수백 개의 다른 키워드를 사용하여 메일을 다양한 방법으로 처리할 수 있습니다. 채널 키워드에 대한 자세한 내용은 *Sun Java System Messaging Server Administration Reference* 및 12장, "채널 정의 구성"에 설명되어 있습니다.

## 메일 전달

메일이 처리된 후 마스터 프로그램은 메일의 전달 경로를 따라 다음 정지 위치로 메일을 보냅니다. 이 위치는 의도한 수신자의 메일함, 다른 MTA 또는 심지어 다른 채널이 될 수 있습니다. 다른 채널로 전달하는 것은 이 그림에 나와 있지 않지만 실제로는 흔히 볼 수 있습니다.

주소와 수신된 필드의 로컬 부분이 일반적으로 7비트 문자라는 점을 주의하시기 바랍니다. MTA는 이러한 필드에서 8비트 문자를 읽을 경우 각 8비트 문자를 별표로 바꿉니다.

## 디스패처

디스패처는 여러 다중 스레드 서버 프로세스가 SMTP 연결 서비스에 대한 역할을 공유할 수 있게 하는 다중 스레드 디스패칭 에이전트입니다. 디스패처를 사용하면 모두 동일한 포트에 대한 연결을 처리하는 여러 다중 스레드 SMTP 서버 프로세스를 동시에 실행할 수 있습니다. 또한 각 서버는 하나 이상의 활성 연결을 가질 수 있습니다.

디스패처는 자체 구성에 나열된 TCP 포트에 대한 중앙 수신기의 역할을 수행합니다. 연결이 설정된 후 디스패처는 정의된 각 서비스에 대해 하나 이상의 SMTP 서버 프로세스를 만들어 연결을 처리할 수 있습니다.

일반적으로 정의된 TCP 포트에 대한 연결을 수신하면 디스패처는 해당 포트의 사용 가능한 작업자 프로세스 풀에서 서비스를 검사하고 새 연결을 위한 최적의 후보를 선택합니다. 적절한 후보를 사용할 수 없는 경우 디스패처는 구성에서 허용하는 경우에 한하여 새 작업자 프로세스를 만들어 새 연결과 후속 연결을 처리할 수 있습니다. 또한 디스패처는 이후의 받는 연결을 예상하여 새 작업자 프로세스를 만들 수도 있습니다. 디스패처의 다양한 서비스 제어를 조정하고 특히 작업자 프로세스 수와 각 작업자 프로세스가 처리하는 연결 수를 제어하는 데 사용할 수 있는 여러 구성 옵션이 존재합니다.

자세한 내용은 [245페이지](#)의 "디스패처 구성 파일"을 참조하십시오.

## 서버 프로세스 작성 및 만료

디스패처 내의 자동 작업 관리 기능은 새 서버 프로세스의 작성과 오래된 또는 유향 서버 프로세스의 만료를 제어합니다. 디스패처의 동작을 제어하는 기본 옵션은 MIN\_PROCS 및 MAX\_PROCS입니다. MIN\_PROCS는 여러 서버 프로세스를 준비하고 받는 연결을 대기하여 보충된 서비스 수준을 제공합니다. 반면, MAX\_PROCS는 주어진 서비스에 대해 동시에 활성화할 수 있는 서버 프로세스 수에 대한 상한값을 설정합니다.

최대한의 연결을 이미 처리하고 있거나 프로세스의 종료가 예약되었기 때문에 현재 실행 중인 서버 프로세스가 연결을 수락하지 못할 수 있습니다. 이 경우 디스패처는 이후의 연결을 지원하기 위해 추가 프로세스를 만들 수 있습니다.

MIN\_CONNS 및 MAX\_CONNS 옵션은 서버 프로세스 간에 연결을 분산시킬 수 있는 기법을 제공합니다. MIN\_CONNS는 서버 프로세스를 "busy enough"(충분히 사용 중)로 플래그 지정하는 연결 수를 지정하고 MAX\_CONNS는 서버 프로세스에 적용할 수 있는 "busiest"(최대한 사용 중)로 지정합니다.

일반적으로 디스패처는 현재 서버 프로세스 수가 MIN\_PROCS보다 작거나 모든 기존 서버 프로세스가 "busy enough"(충분히 사용 중)이고 현재 활성화된 연결의 각 수가 최소한 MIN\_CONNS인 경우 새 서버 프로세스를 만듭니다.

예를 들어, UNIX 시스템 kill 명령에 의해 서버 프로세스가 예기치 않게 종료할 경우 디스패처는 새 연결이 들어올 때와 마찬가지로 새 서버 프로세스를 만듭니다.

디스패처 구성에 대한 자세한 내용은 [245페이지의 "디스패처 구성 파일"](#)을 참조하십시오.

## 디스패처 시작 및 중지

디스패처를 시작하려면 다음 명령을 실행합니다.

```
start-msg dispatcher
```

이 명령은 디스패처가 관리하도록 구성된 MTA 구성 요소를 시작하기 위해 이전에 사용되던 다른 모든 start-msg 명령을 포함하므로 이러한 이전 명령은 더 이상 사용되지 않습니다. 특히 imsimta start smtp를 더 이상 사용하지는 안 됩니다. 폐기된 명령을 실행하려고 하면 MTA는 경고를 표시합니다.

디스패처를 종료하려면 다음 명령을 실행합니다.

```
stop-msg dispatcher
```

디스패처 종료 시에 서버 프로세스에서 수행되는 작업은 기본 TCP/IP 패키지에 따라 달라집니다. 디스패처에 적용되는 MTA 구성 또는 옵션을 수정할 경우 새 구성 또는 옵션이 적용되도록 디스패처를 다시 시작해야 합니다.

디스패처를 다시 시작하려면 다음 명령을 실행합니다.

```
imsimta restart dispatcher
```

디스패처를 다시 시작하면 현재 실행 중인 디스패처가 종료되고 새 디스패처가 즉시 시작됩니다.

## 다시 쓰기 규칙

다시 쓰기 규칙은 다음을 결정합니다.

- 주소의 도메인 부분을 적절한 또는 원하는 형식으로 다시 쓰는 방법
- 주소를 다시 쓴 후에 메일을 대기열에 포함시켜야 하는 채널

각 다시 쓰기 규칙은 *패턴* 및 *템플릿*으로 구성됩니다. 패턴은 주소의 도메인 부분에 대해 일치하는 문자열입니다. 템플릿은 도메인 부분이 패턴과 일치할 경우 수행되는 작업을 지정합니다. 두 가지로 구성된 경우 1) 주소를 다시 쓰는 방법을 지정하는 명령 집합(즉, 제어 문자열) 및 2) 메일을 보내야 하는 채널 이름의 두 부분으로 구성됩니다. 주소가 다시 작성된 후 의도한 수신자에게 전달되도록 메일이 대상 채널의 대기열에 포함됩니다.

다시 쓰기 규칙의 예는 다음과 같습니다.

```
siroe.com          $U%$D@tcp_siroe-daemon
```

siroe.com은 도메인 패턴입니다. siroe.com을 포함하는 주소를 가진 모든 메일은 템플릿 명령(\$U%\$D)에 따라 다시 작성됩니다. \$U는 다시 작성된 주소가 같은 아이디를 사용하도록 지정합니다. %는 다시 작성된 주소가 같은 도메인 구분자를 사용하도록 지정합니다. \$D는 다시 작성된 주소가 패턴에서 일치했던 같은 도메인 이름을 사용하도록 지정합니다. @tcp\_siroe-daemon은 다시 작성된 주소를 가진 메일이 tcp\_siroe-daemon이라는 채널로 보내지도록 지정합니다. 자세한 내용은 [11장, "다시 쓰기 규칙 구성"](#)을 참조하십시오.

다시 쓰기 규칙의 구성에 대한 자세한 내용은 [226페이지의 "MTA 구성 파일"](#) 및 [11장, "다시 쓰기 규칙 구성"](#)을 참조하십시오.

## 채널

채널은 메일을 처리하는 기본 MTA 구성 요소입니다. 채널은 다른 컴퓨터 시스템 또는 시스템 그룹과의 연결을 나타냅니다. 실제 하드웨어 연결 및/또는 소프트웨어 전송은 채널마다 크게 다를 수 있습니다.

채널은 다음 기능을 수행합니다.

- 메일을 원격 시스템으로 전송하고 전송 후에는 대기열에서 메일을 삭제합니다.

- 원격 시스템의 메일을 수락하고 적절한 채널 대기열에 넣습니다.
- 메일을 로컬 메시지 저장소에 전달합니다.
- 특수한 처리를 위해 메일을 프로그램에 전달합니다.

메일은 MTA로 들어올 때 채널에 의해 대기열에 포함되고, 나갈 때 대기열에서 제외됩니다. 일반적으로 메일은 특정 채널을 통해 들어가고 다른 채널에 의해 나옵니다. 채널은 메일을 대기열에서 제외하거나, 메일을 처리하거나, 메일을 다른 MTA 채널의 대기열에 포함시킬 수 있습니다.

## 마스터 및 슬레이브 프로그램

항상 그런 것은 아니지만 채널은 일반적으로 마스터 및 슬레이브의 두 프로그램과 관련됩니다. 슬레이브 프로그램은 다른 시스템에서 메일을 수락하고 채널의 메일 대기열에 추가합니다. 마스터 프로그램은 채널에서 다른 시스템으로 메일을 전송합니다.

예를 들어, SMTP 채널은 메일을 전송하는 마스터 프로그램과 메일을 받는 슬레이브 프로그램을 가집니다. 이러한 프로그램은 각각 SMTP 클라이언트 및 서버입니다.

마스터 채널 프로그램은 일반적으로 MTA가 작업을 시작했던 보내는 연결을 담당합니다. 마스터 채널 프로그램은 다음을 수행합니다.

- 처리를 위해 로컬 요청에 응답하여 실행됩니다.
- 채널 메일 대기열에서 메일을 뽑습니다.
- 대상 형식이 대기열에 넣은 메일의 형식과 같지 않을 경우 필요에 따라 주소, 헤더 및 내용 변환을 수행합니다.
- 메일의 네트워크 전송을 시작합니다.

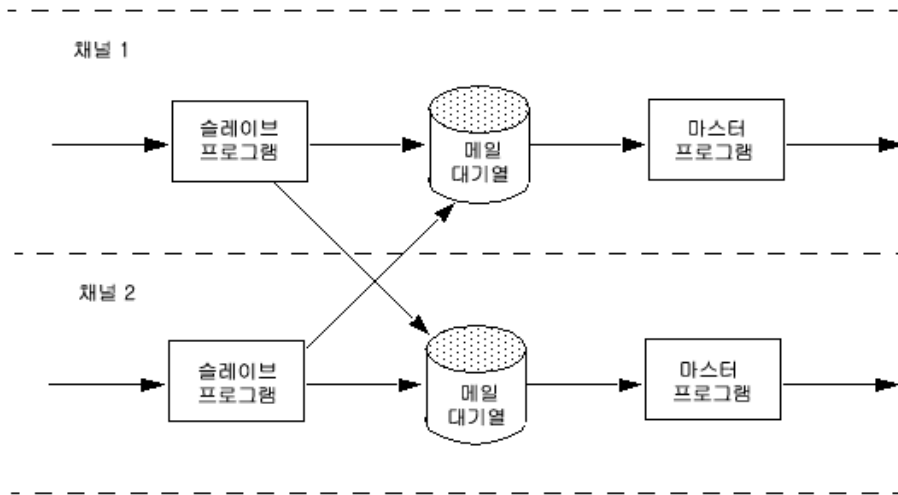
슬레이브 채널 프로그램은 일반적으로 MTA가 외부 요청에 응답하는 받는 연결을 수락합니다. 슬레이브 채널 프로그램을 다음을 수행합니다.

- 외부 이벤트에 응답하여 또는 로컬 요청에 따라 실행됩니다.
- 메일을 채널의 대기열에 넣습니다. 다시 쓰기 규칙을 통해 봉투 주소를 전달하는 방법으로 대상 채널이 결정됩니다.

예를 들어, [그림 8-3](#)에는 두 개의 채널 프로그램(채널 1 및 채널 2)이 나와 있습니다. 채널 1의 슬레이브 프로그램은 원격 시스템으로부터 메일을 받습니다. 이 프로그램은 주소를 확인하고 필요에 따라 다시 쓰기 규칙을 적용한 다음 다시 작성된 주소에 기초하여 해당 채널 메일 대기열에 메일을 포함시킵니다.

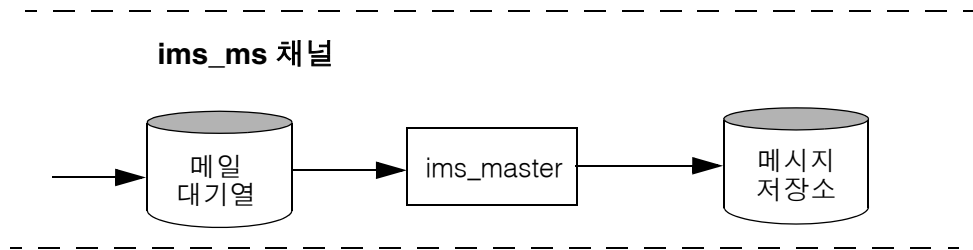
마스터 프로그램은 대기열에서 메일을 제외시키고 메일의 네트워크 전송을 시작합니다. 마스터 프로그램이 자신의 채널 대기열에서만 메일을 제외시킬 수 있다는 것을 유의하십시오.

그림 8-3 마스터 및 슬레이브 프로그램



일반 채널이 마스터 및 슬레이브 프로그램을 모두 가지지만 경우에 따라서는 슬레이브 프로그램 또는 마스터 프로그램만 포함할 수도 있습니다. 예를 들어, Messaging Server와 함께 제공되는 ims-ms 채널은 그림 8-4에 나온 것처럼 로컬 메시지 저장소에 대해서만 메일을 대기열에서 제외시키기 때문에 마스터 프로그램만 포함합니다.

그림 8-4 ims-ms 채널



## 채널 메일 대기열

모든 채널은 연관된 메일 대기열을 가집니다. 메일이 메시징 시스템으로 들어가면 슬레이브 프로그램은 메일을 포함시킬 메일 대기열을 결정합니다. 대기열에 넣은 메일은 채널 대기열 디렉토리의 메일 파일에 저장됩니다. 기본적으로 이러한 디렉토리는 `msg_svr_base/data/queue/channel/*` 위치에 저장됩니다.

---

**주의** 문제가 발생할 수 있으므로 MTA 대기열 디렉토리에서 파일이나 디렉토리(즉, `imta_tailor` 파일의 `IMTA_QUEUE` 값)를 추가하지 않도록 합니다. MTA 대기열 디렉토리에 대해 별개의 파일 시스템을 사용할 경우 해당 마운트 지점 아래에 하위 디렉토리를 만들고 이 하위 디렉토리를 `IMTA_QUEUE` 값으로 지정합니다.

---

## 채널 정의

채널 정의는 다시 쓰기 규칙에 뒤이어 MTA 구성 파일 `imta.cnf`의 하단부에 표시됩니다 (226페이지의 "MTA 구성 파일" 참조). 이 파일에 있는 첫 번째 빈 행은 다시 쓰기 규칙 섹션의 끝 부분이자 채널 정의의 시작 부분을 나타냅니다.

채널 정의는 채널 이름을 포함하며 이어서 채널 구성을 정의하는 선택적 키워드 목록과 메일을 채널로 라우팅하기 위해 다시 쓰기 규칙에서 사용되는 고유한 채널 태그를 포함합니다. 채널 정의는 하나의 빈 행으로 구분됩니다. 채널 정의 안에 주석이 나타날 수 있지만 빈 행을 포함할 수는 없습니다.

```
[blank line]
! sample channel definition
Channel_Name keyword1 keyword2
Channel_Tag
[blank line]
```



채널 정의를 통틀어서 채널 호스트 테이블이라고 하며 개별 채널 정의를 채널 블록이라고 합니다. 예를 들어, 아래 예에서 채널 호스트 테이블은 세 개의 채널 정의 또는 블록을 포함합니다.

```
! test.cnf - An example configuration file.
!
! Rewrite Rules
.
.
.

! BEGIN CHANNEL DEFINITIONS
! FIRST CHANNEL BLOCK
1
local-host

! SECOND CHANNEL BLOCK
a_channel defragment charset7 usascii
a-daemon

! THIRD CHANNEL BLOCK
b_channel noreverse notices 1 2 3
b-daemon
```

일반 채널 항목은 다음과 같이 나타납니다.

```
tcp_intranet smtp mx single_sys subdirs 20 noreverse maxjobs 7 SMTP_POOL
maytlssserver allowswitchchannel sasls witchchannel tcp_auth
tcp_intranet-daemon
```

이 경우 첫 번째 단어 `tcp_intranet`은 채널 이름이며 마지막 단어 `tcp_intranet-daemon`을 *채널 태그*라고 부릅니다. 채널 태그는 메일을 전송하기 위해 다시 쓰기 규칙에 사용되는 이름입니다. 채널 이름과 채널 태그 사이의 단어를 채널 *키워드*라고 하며, 메일이 처리되는 방법을 지정합니다. 수백 개의 다른 키워드를 사용하여 메일을 다양한 방법으로 처리할 수 있습니다. 채널 키워드의 전체 목록과 자세한 내용은 *Sun Java System Messaging Server Administration Reference* 및 12장, "채널 정의 구성"을 참조하십시오.

채널 호스트 테이블은 Messaging Server가 사용할 수 있는 채널과 각 채널에 연관되는 시스템의 이름을 정의합니다.

UNIX 시스템에서 파일의 첫 번째 채널 블록은 항상 로컬 채널 1을 설명합니다. (로컬 채널 앞에 놓일 수 있는 defaults 채널은 예외입니다.) 로컬 채널은 라우팅 결정을 내리고 UNIX 메일 도구에 의해 보내진 메일을 전송하는 데 사용됩니다.

MTA 옵션 파일 option.dat에서 채널에 대한 전역 옵션을 설정하거나 채널 옵션 파일의 특정 채널에 대한 옵션을 설정할 수도 있습니다. 옵션 파일에 대한 자세한 내용은 [246페이지](#)의 "옵션 파일" 및 [244페이지](#)의 "TCP/IP(SMTP) 채널 옵션 파일"을 참조하십시오. 채널 구성에 대한 자세한 내용은 [12장](#), "채널 정의 구성"을 참조하십시오. MTA 채널 작성에 대한 자세한 내용은 [226페이지](#)의 "MTA 구성 파일"을 참조하십시오.

## MTA 디렉토리 정보

MTA는 각 메일을 처리할 때 지원되는 사용자, 그룹 및 도메인에 대한 디렉토리 정보에 액세스해야 합니다. 이 정보는 LDAP 디렉토리 서비스에 저장됩니다. MTA는 LDAP 디렉토리에 직접 액세스합니다. 이에 대한 자세한 내용은 [9장](#), "MTA 주소 변환 및 라우팅"에 설명되어 있습니다.

## Job Controller

메일이 채널의 대기열에 포함될 때마다 Job Controller는 메일 전달을 위해 실행 중인 작업이 있는지 확인합니다. 여기에는 새 작업 프로세스를 시작하거나, 스레드를 추가하거나, 단순히 작업이 이미 실행 중인지 확인하는 것이 포함됩니다. 채널 또는 풀에 대한 작업 제한에 도달하여 작업을 시작할 수 없을 경우 Job Controller는 다른 작업이 종료할 때까지 기다립니다. 작업 제한을 더 이상 초과하지 않으면 Job Controller는 다른 작업을 시작합니다.

채널 작업은 Job Controller 내의 처리 풀 안에서 실행됩니다. 풀은 채널 작업이 실행되는 "장소"로 생각할 수 있습니다. 풀은 작업 세트가 풀 외부의 작업과 자원을 놓고 경쟁하지 않고도 작동할 수 있는 컴퓨팅 영역을 제공합니다. 풀에 대한 자세한 내용은 [247페이지](#)의 "Job Controller 파일" 및 [360페이지](#)의 "채널 실행 작업의 처리 풀"을 참조하십시오.

채널에 대한 작업 제한은 maxjobs 채널 키워드에 의해 결정되며 풀에 대한 작업 제한은 풀의 JOB\_LIMIT 옵션에 의해 결정됩니다.

Messaging Server는 일반적으로 모든 메일을 즉시 전달하려고 시도합니다. 그러나 첫 번째 시도에서 메일을 전달할 수 없는 경우 해당 `backoff` 키워드에 지정된 기간 동안 메일이 지연됩니다. `backoff` 키워드에 지정된 시간이 경과하자마자 지연된 메일을 전달할 수 있으며 필요한 경우 메일을 처리하기 위해 채널 작업이 시작됩니다.

현재 처리 중인 메일과 처리 대기 중인 메일에 대한 Job Controller의 메모리 내장 데이터 구조는 일반적으로 MTA 대기열 영역의 디스크에 저장된 전체 메일 파일 집합을 반영합니다. 그러나 디스크의 메일 파일 백로그가 Job Controller의 메모리 내장 데이터 구조 크기 제한을 초과하기에 충분할 만큼 작성될 경우 Job Controller는 디스크의 전체 메일 파일 중 일부만 메모리에서 추적합니다. Job Controller는 메모리에서 추적 중인 메일만 처리합니다. 메모리 내장 저장소를 비워야 할 정도로 많은 메일이 전달될 경우 Job Controller는 MTA 대기열 영역을 스캔하여 메일 목록을 업데이트함으로써 메모리 내장 저장소를 자동으로 갱신합니다. 그런 다음 Job Controller는 디스크에서 방금 검색한 추가 메일 파일의 처리를 시작합니다. Job Controller는 MTA 대기열 영역에 대한 이러한 스캔 작업을 자동으로 수행합니다.

사이트에서 과도한 메일 백로그가 정기적으로 발생할 경우 `MAX_MESSAGES` 옵션을 사용하여 Job Controller를 조정할 수 있습니다. Job Controller가 더 많은 메모리를 사용할 수 있게 `MAX_MESSAGES` 옵션 값을 늘리면 메일 백로그가 Job Controller의 메모리 내장 캐시를 초과하는 경우를 줄일 수 있습니다. 또한 이 경우 Job Controller가 MTA 대기열 디렉토리를 스캔해야 할 때와 관련된 오버헤드가 줄어듭니다. 그러나 Job Controller가 메모리 내장 캐시를 다시 작성해야 할 경우 캐시가 더 크기 때문에 프로세스에 더 많은 시간이 걸린다는 것을 유의하십시오. 또한 Job Controller는 시작 또는 재시작될 때마다 MTA 대기열 디렉토리를 스캔해야 하므로 과도한 메일 백로그가 있다는 것은 그렇지 않을 때보다 Job Controller를 시작 또는 재시작할 때 많은 오버헤드가 발생한다는 것을 의미합니다.

풀과 Job Controller 구성에 대한 자세한 내용과 [247페이지의 "Job Controller 파일"](#) 및 [355페이지의 "메일 처리 및 전달 구성"](#)을 참조하십시오.

## Job Controller 시작 및 중지

Job Controller를 시작하려면 다음 명령을 실행합니다.

```
start-msg job_controller
```

Job Controller를 종료하려면 다음 명령을 실행합니다.

```
stop-msg job_controller
```

Job Controller를 다시 시작하려면 다음 명령을 실행합니다.

```
imsimta restart job_controller
```

Job Controller를 다시 시작하면 현재 실행 중인 Job Controller가 종료되고 새 Job Controller가 바로 시작됩니다.

## MTA 주소 변환 및 라우팅

Messaging Server 6 2003Q4 이전에 Messaging Server는 LDAP 서버에 저장된 정보로 컴파일된 데이터베이스에서 모든 사용자, 도메인 및 그룹 데이터에 액세스했습니다. LDAP 서버에서 디렉토리 정보가 업데이트되면 데이터베이스 정보는 `dirsync`라는 프로그램과 동기화되었습니다. Messaging Server MTA는 이제 LDAP 디렉토리에 직접 액세스합니다. 이 장에서는 Direct LDAP 데이터 액세스를 사용한 MTA의 데이터 흐름에 대해 설명합니다. 이 장은 다음 내용으로 구성되어 있습니다.

- 197페이지의 "Direct LDAP 알고리즘 및 구현"
- 221페이지의 "주소 역방향"
- 223페이지의 "비동기 LDAP 작업"
- 224페이지의 "설정 요약"

### Direct LDAP 알고리즘 및 구현

다음 절에서는 Direct LDAP 처리에 대해 설명합니다.

#### 도메인의 로컬 여부 확인

`user@domain` 형식의 주소에서 시작되는 주소 변환 및 라우팅 프로세스는 우선 `domain`이 로컬인지 여부를 검사합니다.

## 다시 쓰기 규칙 방법

주어진 문자열을 검사하여 로컬로 처리해야 하는 도메인인지 여부를 확인하는 기능이 MTA 다시 쓰기 규칙 방법에 추가되었습니다. 이 새 기능은 \$v 또는 \$z 메타 문자에 의해 활성화됩니다. 이러한 새 메타 문자는 기존 \$N, \$M, \$Q 및 \$C 메타 문자와 구문적으로 유사합니다. 즉, 뒤에 패턴 문자열이 옵니다. \$N, \$M, \$Q 및 \$C의 경우 소스 또는 대상 채널에 대해 패턴이 일치됩니다. \$v 및 \$z의 경우 패턴은 도메인이며 로컬인지 여부를 확인하는 검사가 수행됩니다. \$v의 경우 로컬이 아닌 도메인에 대해 규칙이 실패하며 \$z의 경우 로컬 도메인에 대해 규칙이 실패합니다.

이러한 메타 문자의 처리는 다음 절차에 따라 구현됩니다.

1. Messaging Server는 현재 도메인이 디렉토리의 유효한 도메인 항목과 일치하는지 여부를 확인합니다. 항목이 없으면 단계 3으로 가십시오.
2. 도메인에 디렉토리의 항목이 있을 때는 LDAP\_DOMAIN\_ATTR\_ROUTING\_HOSTS MTA 옵션에서 지정한 속성(기본 mailRoutingHosts)이 해당 도메인 항목에서 검색됩니다. 이 속성이 존재할 경우 이 도메인의 사용자를 처리할 수 있는 호스트 집합이 나열됩니다. 이 목록은 local.hostname configutil 매개 변수에 지정된 호스트 및 local.imta.hostnamealiases configutil 매개 변수에 지정된 호스트 목록과 비교됩니다. 이러한 옵션은 각각 LDAP\_LOCAL\_HOST 및 LDAP\_HOST\_ALIAS\_LIST MTA 옵션으로 무시할 수 있습니다. 일치하는 항목이 있거나 도메인에 속성이 존재하지 않을 경우 도메인은 로컬입니다. 일치하는 항목이 없으면 도메인은 로컬이 아닙니다.

mailRoutingHosts 속성으로 인해 로컬이 아닌 것으로 간주되는 도메인의 처리는 ROUTE\_TO\_ROUTING\_HOST MTA 옵션의 설정에 따라 달라집니다. 이 옵션이 0(기본 값)으로 설정된 경우 주소는 단순히 로컬이 아닌 것으로 간주되며 MTA 다시 쓰기 규칙을 사용하여 라우팅을 결정합니다. 이 옵션이 1로 설정된 경우 LDAP\_DOMAIN\_ATTR\_ROUTING\_HOSTS MTA 옵션에 나열된 첫 번째 값으로 구성된 소스 경로가 주소의 앞에 놓입니다.

3. 도메인 항목을 찾을 수 없는 경우 도메인의 왼쪽에서 구성 요소를 제거하고 단계 1로 이동합니다. 구성 요소가 남아 있지 않으면 단계 4를 진행합니다.

도메인 트리를 거슬러 올라가는 이 방법은 결과적으로 domain.com이 로컬로 인식될 경우 domain.com의 모든 하위 도메인이 로컬로 인식되게 합니다. 이 동작이 바람직하지 않은 상황이 발생할 수 있으므로 동작을 제어하기 위한 MTA 옵션 DOMAIN\_UPLEVEL이 제공됩니다. 특히 DOMAIN\_UPLEVEL의 비트 0(값 = 1)이 지워진 경우 제거된 도메인 구성 요소로 채시도할 수 없게 됩니다. DOMAIN\_UPLEVEL의 기본 값은 0입니다.

4. 이제 부속 도메인 검사를 수행해야 합니다. 부속 도메인에는 도메인 항목이 없고, 오히려 하나 이상의 사용자 항목에 특별한 도메인 속성을 추가함으로써 지정됩니다. 후속 도메인 검사는 `DOMAIN_MATCH_URL` MTA 옵션에 지정된 LDAP URL을 사용하여 LDAP 검색을 시작하는 방법으로 수행됩니다. 이 옵션의 값은 다음과 같이 설정해야 합니다.

```
ldap:/// $B?msgVanityDomain?sub?(msgVanityDomain=$D)
```

\$B는 `local.ugldapbasedn configutil` 매개 변수의 값을 대체합니다(이는 디렉토리에서 사용자 트리의 기반임). `LDAP_USER_ROOT` MTA 옵션을 사용하여 특히 MTA에 대해 이 `configutil` 옵션의 값을 무시할 수 있습니다.

이 검색의 실제 반환 값은 중요하지 않습니다. 중요한 것은 반환할 값이 존재하는지 여부입니다. 반환 값이 존재할 경우 도메인은 로컬로 간주되며 그렇지 않을 경우 도메인은 로컬이 아닌 것으로 간주됩니다.

## 도메인 로컬 여부의 도메인 맵 확인

디렉토리에서 유효한 도메인 항목을 찾기 위해 수행되는 단계가 무엇인지 잘 기억하는 것이 좋습니다. 이러한 단계는 스키마 수준별로 다릅니다. Sun LDAP Schema, v.1의 경우 이러한 단계는 다음과 같습니다.

1. 도메인을 도메인 트리의 기본 DN으로 변환합니다. 이 작업은 도메인을 일련의 `dc` 구성 요소로 변환한 다음 도메인 루트 접미어를 추가하는 방법으로 수행합니다. 기본 접미어는 `service.dccroot configutil` 매개 변수에서 얻습니다. 기본 접미어는 `o=internet`입니다. 따라서 `a.b.c.d` 형식의 도메인은 일반적으로 `dc=a,dc=b,dc=c,dc=d,o=internet`으로 변환됩니다. `service.dccroot configutil` 매개 변수는 `LDAP_DOMAIN_ROOT` MTA 옵션을 설정하여 무시할 수 있습니다.
2. 단계 1에서 발견된 기본 DN과 `inetDomain` 또는 `inetDomainAlias` 객체 클래스를 가진 항목을 찾습니다. 이 목적에 사용되는 검색 필터는 `LDAP_DOMAIN_FILTER_SCHEMA1` MTA 옵션을 설정하여 무시할 수 있습니다. 이 옵션의 기본값은 `(|(objectclass=inetDomain)(objectclass=inetdomainalias))`입니다.
3. 아무 것도 발견되지 않을 경우 실패와 함께 종료합니다.
4. 항목의 객체 클래스를 `inetDomain`에서 찾은 경우, 해당 도메인 항목에 관련된 `inetDomainBaseDn` 속성이 있는지 확인하십시오. 이 속성이 있으면 사용자 항목에 대한 후속 검색에 사용되도록 저장한 다음 처리가 종료됩니다. 이 속성이 없으면 해당 항목은 도메인 별칭으로 가정되고 단계 5로 처리가 계속됩니다. `inetDomainBaseDN` 대신 MTA 옵션 `LDAP_DOMAIN_ATTR_BASEDN`을 사용할 수 있습니다.

5. 항목은 도메인 별칭이어야 합니다. `aliasedObjectName` 속성에서 참조한 새 항목을 찾아 단계 4로 돌아가십시오. `aliasedObjectName` 속성이 없으면 오류와 함께 처리가 종료됩니다. MTA 옵션 `LDAP_DOMAIN_ATTR_ALIAS`를 사용하여 `aliasedObjectName` 속성 사용을 대체할 수 있습니다.

처리가 단계 4로 돌아가는 일은 한 번 정도만 발생할 수 있다는 점을 주의하십시오. 도메인 별칭에서 도메인 별칭을 가리키는 일은 허용되지 않습니다.

Sun LDAP Schema 2에서는 수행되는 작업이 훨씬 더 간단합니다. 디렉토리에서 도메인이 `sunPreferredDomain` 또는 `associatedDomain` 속성 값으로 표시되는 `sunManagedOrganization` 객체 클래스가 있는 항목을 검색합니다. 필요한 경우 `sunPreferredDomain` 및 `associatedDomain` 속성의 사용을 각각 MTA 옵션 `LDAP_ATTR_DOMAIN1_SCHEMA2` 및 `LDAP_ATTR_DOMAIN2_SCHEMA2`를 사용하여 무시할 수 있습니다. 검색은 `service.dcroot configutil` 매개 변수로 지정된 루트 하에서 수행됩니다. `service.dcroot configutil` 매개 변수는 `LDAP_DOMAIN_ROOT` MTA 옵션을 설정하여 무시할 수 있습니다. 아울러 스키마 2의 도메인 항목은 `inetDomainBaseDn` 속성을 가지지 않아도 됩니다. 해당 속성을 가지지 않은 경우 사용자 트리의 기본이 도메인 항목 자체인 것으로 간주됩니다.

## 도메인 로컬 여부 정보의 캐싱

도메인 다시 쓰기 작업이 수행되는 빈도와 디렉토리 쿼리(특히 부속 도메인 검사)의 비용으로 인해 도메인에 대한 부정적 및 긍정적 표시를 모두 캐시해야 합니다. 이 작업은 동적으로 확장되는 메모리 내장의 개방형 체인 해시 테이블을 통해 구현됩니다. 캐시의 최대 크기는 `DOMAIN_MATCH_CACHE_SIZE` MTA 옵션(기본값 100000)으로 설정하며 캐시의 항목에 대한 시간 초과는 `DOMAIN_MATCH_CACHE_TIMEOUT` MTA 옵션(기본값 600초)으로 설정합니다.

## 오류 처리

이 프로세스 도중에 발생하는 임시 서버 오류를 신중하게 처리해야 하는데 이는 이 오류가 발생할 경우 주어진 도메인이 로컬인지 여부를 알 수 없기 때문입니다. 기본적으로 이러한 경우에는 두 가지 결과가 가능합니다.

1. 주소를 나중에 다시 시도하라는 임시(4xx) 오류를 클라이언트에게 반환합니다.
2. 주소를 수락하지만 재처리 채널에서 주소를 대기시켜 나중에 로컬로 다시 시도할 수 있게 합니다.

이러한 두 옵션이 모든 경우에 적합한 것은 아닙니다. 예를 들어, 결과 1은 원격 SMTP 릴레이와 통신할 때 적합합니다. 그러나 결과 2는 로컬 사용자로부터의 SMTP 제출을 처리할 때 적합합니다.



동일한 패턴을 가진 여러 규칙을 사용하여 일시적인 오류를 처리하는 것이 이론적으로 가능하지만 이러한 쿼리를 반복할 경우 발생하는 오버헤드는 캐시로도 처리할 수 없는 큰 부담이 됩니다. 이러한 이유로 도메인 다시 쓰기의 다음 규칙까지의 성공/실패 일치 모델은 적합하지 않습니다. 대신 MTA 옵션 DOMAIN\_FAILURE에 지정된 특수한 템플리트가 도메인 조회 실패의 경우에 사용됩니다. \$v 작업이 실패하면 이 템플리트는 처리 중인 현재 다시 쓰기 규칙 템플리트의 나머지 부분을 대체합니다.

## 도메인 검사 다시 쓰기 규칙을 위한 패턴

다른 다시 쓰기 규칙이 수행되기 전에 이 도메인 검사를 수행해야 합니다. 이 순서는 규칙의 왼쪽에서 특수한 \$\*를 사용하여 지정합니다. \$\* 패턴은 다른 모든 규칙에 앞서 검사됩니다.

## 모든 방법 사용

지금까지 설명된 모든 방법을 고려할 때 imta.cnf에서 필요한 새 다시 쓰기 규칙은 다음과 같습니다.

```
$*          $E$F$U%$H$V$H@localhost
```

또한 option.dat 파일에서 DOMAIN\_FAILURE MTA 옵션 값은 다음과 같아야 합니다.

```
reprocess-daemon$Mtcp_local$1M$1--error$4000000?Temporary lookup failure
```

이 다시 쓰기 규칙에서 localhost는 로컬 채널과 연관된 호스트 이름입니다. 여기에 표시된 DOMAIN\_FAILURE 옵션 값이 기본값이므로 정상적인 환경에서 option.dat에 표시될 필요가 없습니다.

여기에서 순서는 특히 까다롭습니다. MTA는 주소가 재작성되었지만 경로가 아직 추가되기 전에 \$v를 검사합니다. 따라서 일시적인 조회 실패가 발생할 경우에 MTA에서 경로를 변경할 수 있습니다. 보류 중인 채널 일치 검사는 삽입 지점이 변경될 때마다 적용되므로 \$H초 후에 @가 검사를 호출합니다. 이 검사에 성공할 경우 템플리트의 나머지 부분이 적용되며 다시 쓰기 처리가 완료됩니다. 검사에 실패할 경우 다시 쓰기는 실패하며 적용 가능한 다음 다시 쓰기 규칙을 사용하여 다시 쓰기가 계속됩니다. 일시적인 오류로 인해 검사를 수행할 수 없는 경우 DOMAIN\_FAILURE MTA 옵션에 지정된 값에서 템플리트 처리가 계속됩니다. 이 템플리트 값은 우선 라우팅 호스트를 reprocess-daemon으로 설정합니다. 그런 다음 템플리트는 MTA가 동일한 종류 또는 tcp\_local의 재처리 채널을 처리하고 있는지 여부를 확인합니다. MTA가 이러한 채널을 처리하는 중이면 규칙이 계속 진행되어 라우팅 호스트를 잘못된 것으로 만들고 일시적인 오류를 결과로 지정합니다. MTA가 이러한 채널을 처리하는 중이 아니면 규칙이 잘리고 성공적으로 종료하므로 재처리 채널에 주소가 다시 쓰여집니다.

## 로컬 주소의 별칭 확장

주소가 로컬 채널과 연관된 것으로 확인되고 나면 해당 주소에 자동으로 별칭 확장이 적용됩니다. 별칭 확장 프로세스는 다음을 비롯하여 여러 정보 소스를 검사합니다.

1. 별칭 파일(컴파일된 구성의 일부)
2. 별칭 데이터베이스
3. 별칭 URL

검사되는 정확한 별칭 소스와 별칭 소스가 검사되는 순서는 option.dat 파일의 ALIAS\_MAGIC MTA 옵션 설정에 따라 달라집니다. Direct LDAP의 경우 이 옵션을 8764로 설정합니다. 이것은 ALIAS\_URL0 MTA 옵션에 지정된 URL이 우선적으로 검사되고 ALIAS\_URL1 MTA 옵션에 지정된 URL이 검사된 다음 ALIAS\_URL2 MTA 옵션에 지정된 URL이 검사되고 마지막으로 별칭 파일이 검사된다는 것을 의미합니다. 이 설정이 활성화되면 별칭 데이터베이스는 검사되지 않습니다.

### LDAP URL을 사용한 별칭 검사

LDAP에서 별칭을 검사하는 것은 두 개의 특수한 LDAP URL을 별칭 URL로 지정하여 구현합니다. 첫 번째 URL은 일반 사용자와 그룹을 처리하며 부속 도메인은 후속 별칭 URL에 의해 처리됩니다. 첫 번째 URL은 다음과 같이 ALIAS\_URL0으로 지정됩니다.

```
ALIAS_URL0=ldap:///?$V?*?sub?$R
```

### \$V 메타 문자

메타 문자 확장은 URL 조회 전에 발생합니다. ALIAS\_URL0 값에 사용되는 두 개의 메타 문자는 \$V 및 \$R입니다.

\$V 메타 문자는 주소의 도메인 부분을 기본 DN으로 변환합니다. 이것은 앞의, "[다시 쓰기 규칙 방법](#)" 절에서 설명한 \$V 다시 쓰기 규칙 메타 문자에 의해 수행되는 초기 단계와 비슷합니다. \$V 처리는 다음 단계로 구성됩니다.

1. 현재 도메인의 사용자 항목에 대한 기본 DN을 가져옵니다.
2. 현재 도메인과 연결된 정규 도메인을 가져옵니다. Sun LDAP Schema 1에서 정규 도메인 이름은 도메인 항목의 inetCanonicalDomainName 속성에 의해 제공됩니다 (이 속성이 존재할 경우). 이 속성이 없을 경우 정규 이름은 실제 도메인 항목의 DN에서 명시적인 방식으로 생성되는 이름입니다. 현재 도메인이 별칭일 경우 이것은 현재 도메인과 다릅니다. 정규 이름을 저장하는 데 사용되는 이름 속성은 option.dat 파일의 LDAP\_DOMAIN\_ATTR\_CANONICAL MTA 옵션으로 무시할 수 있습니다.

Sun LDAP Schema, v.2에서 정규 이름은 단순히 SunPreferredDomain 속성 값입니다.

3. 기본 DN이 존재할 경우 이를 \$v 대신에 URL로 대체합니다.
4. 이제 이 항목에 대한 적용 가능한 모든 호스트된 도메인이 확인됩니다. 이 작업은 정규 도메인(DOMAIN\_Uplevel의 비트 2(값 = 4)가 지워진 경우) 또는 현재 도메인(DOMAIN\_Uplevel의 비트 2(값 = 4)가 설정된 경우)과 service.defaultdomain configutil 매개 변수를 비교하는 방법으로 수행됩니다. 서로 일치하지 않을 경우 해당 항목은 호스트된 도메인의 구성원입니다. service.defaultdomain configutil 매개 변수는 option.dat 파일에서 LDAP\_DEFAULT\_DOMAIN MTA 옵션을 설정하여 무시할 수 있습니다.
5. 기본 DN 확인이 실패할 경우 도메인의 왼쪽에서 구성 요소를 제거하고 단계 1로 이동합니다. 구성 요소가 남아 있지 않을 경우 대체는 실패합니다.

\$v는 또한 선택 사항인 숫자 인수를 허용합니다. 1로 설정된 경우(예: \$1v) 도메인 트리의 도메인 확인 실패가 무시되고 local.ugldapbasedn configutil 옵션에서 지정한 사용자 트리의 기반이 반환됩니다.

도메인의 기본 DN을 검색하려는 시도가 성공할 경우 MTA는 또한 나중에 필요한 여러 유용한 도메인 속성을 검색합니다. 검색된 속성의 이름은 option.dat 파일의 다음 MTA 옵션에 의해 설정됩니다.

- LDAP\_DOMAIN\_ATTR\_UID\_SEPARATOR(기본값: domainUIdSeparator)
- LDAP\_DOMAIN\_ATTR\_SMARTHOST(기본값: mailRoutingSmartHost)
- LDAP\_DOMAIN\_ATTR\_CATCHALL\_ADDRESS(기본값: mailDomainCatchallAddress)
- LDAP\_DOMAIN\_ATTR\_BLOCKLIMIT(기본값: mailDomainMsgMaxBlocks)
- LDAP\_DOMAIN\_ATTR\_REPORT\_ADDRESS(기본값: mailDomainReportAddress)
- LDAP\_DOMAIN\_ATTR\_STATUS(기본값: inetDomainStatus)
- LDAP\_DOMAIN\_ATTR\_MAIL\_STATUS(기본값: mailDomainStatus)
- LDAP\_DOMAIN\_ATTR\_CONVERSION\_TAG(기본값: mailDomainConversionTag)
- LDAP\_DOMAIN\_ATTR\_FILTER(기본값: mailDomainSieveRuleSource)
- LDAP\_DOMAIN\_ATTR\_DISK\_QUOTA(기본값: 없음)

- LDAP\_DOMAIN\_ATTR\_MESSAGE\_QUOTA(기본값: 없음)
- LDAP\_DOMAIN\_ATTR\_AUTOREPLY\_TIMEOUT(기본값: 없음)
- LDAP\_DOMAIN\_ATTR\_NOSOLICIT(기본값: 없음)
- LDAP\_DOMAIN\_ATTR\_OPTIN(기본값: 없음)
- LDAP\_DOMAIN\_ATTR\_RECIPIENTLIMIT(기본값: 없음)
- LDAP\_DOMAIN\_ATTR\_RECIPIENTCUTOFF(기본값: 없음)
- LDAP\_DOMAIN\_ATTR\_SOURCEBLOCKLIMIT(기본값: 없음)

## URL에서 매핑 호출

간혹 도메인에서 기본 DN으로의 매핑이 다른 방식으로 수행되기도 합니다. 이러한 설정을 수용하기 위해 URL 확인 프로세스는 MAT 매핑을 호출하는 기능을 가집니다. 이 작업은 다음과 같은 일반적인 형식의 메타 문자 시퀀스를 통해 수행됩니다.

`$|/mapping-name/mapping-argument|`

큰따옴표("")는 콜아웃을 시작 및 종료합니다. \$의 바로 뒤에 오는 문자는 매핑 이름과 인수의 구분자이며 이 문자는 매핑 이름이나 인수에 사용되는 예상된 문자 값과 충돌하지 않도록 선택해야 합니다.

## \$R 메타 문자

\$R 메타 문자는 URL을 위한 적절한 필터를 제공합니다. 이 메타 문자의 목적은 특정 사용자나 그룹에 대한 전자 메일 주소를 포함할 수 있는 모든 속성을 검색하는 필터를 생성하는 것입니다. 검색할 속성 목록은 `configutil` 매개 변수에서 제공됩니다. 이 매개 변수를 설정하지 않을 경우 `local.imta.schematag configutil` 매개 변수가 검사되며 다음과 같이 이 매개 변수의 값에 따라 적절한 기본 속성 집합이 선택됩니다.

```
sims401      mail,rfc822mailalias
nms41       mail,mailAlternateAddress
ims50       mail,mailAlternateAddress,mailEquivalentAddress
```

`local.imta.schematag`의 값은 쉼표로 구분된 목록이 될 수 있습니다. 둘 이상의 스키마가 지원될 경우 중복 항목이 제거된 결합된 속성 목록이 사용됩니다. LDAP\_SCHEMATAG MTA 옵션을 사용하여 특히 MTA에 대한 `local.imta.schematag`의 설정을 무시할 수 있습니다.

또한 이 필터는 원래 제공되었던 주소뿐만 아니라 로컬 부분이 동일하지만 실제로 도메인 트리에서 발견된 도메인("\$V 메타 문자" 절의 단계 2에서 저장)을 가진 주소를 검색합니다. 도메인 트리 조회의 반복 특성은 두 개의 주소가 다를 수 있다는 것을 의미합니다. 이 추가 검사는 option.dat 파일에서 DOMAIN\_UPLEVEL MTA 옵션의 비트 1(값 = 2)을 통해 제어합니다. 이 비트를 설정하면 추가 주소 검사가 활성화됩니다. DOMAIN\_UPLEVEL의 기본값은 0입니다.

예를 들어, 도메인 siroe.com이 도메인 트리에 있다고 가정해 봅시다. Sun LDAP Schema, v.1을 사용 중이라고 가정하면 주소 조회는 다음과 같습니다.

```
u@host1.siroe.com
```

\$R 및 ims50 schematag의 확장 결과로 얻어지는 필터는 다음과 같습니다.

```
( | (mail=u@siroe.com)
      (mail=u@host1.siroe.com)
      (mailAlternateAddress=u@siroe.com)
      (mailAlternateAddress=u@host1.siroe.com)
      (mailEquivalentAddress=u@siroe.com)
      (mailEquivalentAddress=u@host1.siroe.com) )
```

반면, DOMAIN\_UPLEVEL이 3이 아니라 1로 설정된 경우 필터는 다음과 같을 것입니다.

```
( | (mail=u@host1.siroe.com)
      (mailAlternateAddress=u@host1.siroe.com)
      (mailEquivalentAddress=u@host1.siroe.com) )
```

## 가져올 속성 결정

반환할 속성 목록에 대해 URL에서 \*가 지정된 경우 이 별표는 MTA가 사용할 수 있는 속성 목록으로 대체됩니다. 이 목록은 MTA가 사용하는 옵션을 지정하는 다양한 MTA 옵션 설정으로부터 동적으로 만들어집니다.

## LDAP 오류 처리

이 시점에서 결과 URL은 LDAP 검색을 수행하는 데 사용됩니다. 일정한 LDAP 오류가 발생한 경우 일시적인 오류 표시(SMTP의 4xx 오류)와 함께 처리가 종료됩니다. LDAP 작업이 성공적이지만 결과를 생성하지 못한 경우

LDAP\_DOMAIN\_ATTR\_CATCHALL\_ADDRESS MTA 옵션에서 검색된 도메인에 대한 catchall 주소 속성이 검사됩니다. 이 속성이 설정된 경우 해당 값이 현재 주소를 대체합니다.

catchall 주소 속성이 설정되지 않은 경우 LDAP\_DOMAIN\_ATTR\_SMARTHOST MTA 옵션에서 검색된 도메인에 대한 smarthost 속성이 검사됩니다. 이 속성이 설정된 경우 다음 형식의 주소가 작성되고

```
@smarthost:user@domain
```

이 결과와 함께 별칭 처리가 성공적으로 종료합니다. 또한

LDAP\_DOMAIN\_ATTR\_CONVERSION\_TAG MTA 옵션에서 얻은 도메인에 대한 변환 태그 (있을 경우)가 주소에 추가되어 smarthost로 전달하기 전에 변환이 수행될 수 있게 합니다. 도메인에 대해 catchall 주소나 smarthost가 존재하지 않을 경우 이 별칭 URL의 처리가 실패로 종료합니다.

## LDAP 결과에 대한 유효성 검사

LDAP 검색이 결과를 반환한 후에 항목이 하나만 존재하는지 확인하기 위해 결과가 검사됩니다. 둘 이상의 항목이 존재할 경우 사용자 또는 그룹에 대한 올바른 객체 클래스, 삭제되지 않은 상태 및 UID(사용자인 경우)를 가지는지 확인하기 위해 각 항목이 검사됩니다. 이 검사를 통과하지 않은 항목은 무시됩니다. 이 검사에 의해 여러 항목이 하나로 줄어들 경우 처리가 계속 진행됩니다. 그렇지 않을 경우에는 중복 또는 모호한 디렉토리 오류가 반환됩니다.

## 부속 도메인 지원

ALIAS\_URL0 검사는 기본 사용자나 호스트된 도메인의 사용자에 대해 수행됩니다. 이 검사가 실패할 경우 또한 부속 도메인 검사가 수행됩니다. 부속 도메인 검사에는 다음 별칭 URL이 사용됩니다.

```
ALIAS_URL1=ldap:/// $B?*?sub? (&(msgVanityDomain=$D)$R)
```

## Catchall 주소 지원

마지막으로 @host 형식의 catchall 주소에 대한 검사가 mailAlternateAddress 속성에서 수행되어야 합니다. 이 와일드카드 지정 형식은 호스트된 도메인과 부속 도메인 모두에서 허용되므로 이에 대한 적절한 별칭 URL은 다음과 같습니다.

```
ALIAS_URL2=ldap:/// $1V?*?sub?(mailAlternateAddress=@$D)
```

---

**주**      +\* 하위 주소 대체 기법은 항상 Direct LDAP 모드에서 catch-all 주소를 사용하지만 문자열 대체는 전체 로컬 부분이 아닌 하위 주소에서만 이루어집니다. 이것은 이러한 구성을 사용할 때 원래 주소의 전체 로컬 부분이 catch-all 주소에 하위 주소로 연결되도록 변경되었습니다.

예를 들어, 주소 형식이 foo+bar@domain.com인 경우 domain.com 도메인에 로컬 사용자 foo가 없고 domain.com의 catch-all 주소가 bletch+\*@example.com이면 결과 주소는 bletch+foo+bar@example.com이 됩니다. 이전에는 bletch+bar@example.com이 사용되었습니다.

---

## LDAP 결과 처리

LDAP 별칭 결과 처리는 순서가 정해진 여러 단계를 통해 수행됩니다. 이러한 단계는 다음 절에서 설명됩니다.

### 객체 클래스 검사

별칭 검색에 성공할 경우 사용자나 그룹에 대한 적절한 객체 클래스 집합이 포함되었는지 확인하기 위해 항목의 객체 클래스가 검사됩니다. 사용자 및 그룹에 대한 필수 객체 클래스의 가능한 집합은 일반적으로 활성화된 `schemata`에 따라 달라지며 이것은 `local.imta.schematag` 설정에 의해 결정됩니다.

표 9-1은 다양한 `schematag` 값의 결과인 사용자 및 그룹 객체 클래스를 보여 줍니다.

**표 9-1** 다양한 `schematag` 값의 결과인 객체 클래스

| <code>schematag</code> | 사용자 객체 클래스                                             | 그룹 객체 클래스                                         |
|------------------------|--------------------------------------------------------|---------------------------------------------------|
| <code>sims40</code>    | <code>inetMailRouting+inetmailuser</code>              | <code>inetMailRouting+inetmailgroup</code>        |
| <code>nms41</code>     | <code>mailRecipient +<br/>nsMessagingServerUser</code> | <code>mailGroup</code>                            |
| <code>ims50</code>     | <code>inetLocalMailRecipient+inetma<br/>iluser</code>  | <code>inetLocalMailRecipient+inetmailgroup</code> |

이 표의 정보는 스키마 태그 처리의 나머지 부분과 마찬가지로 하드 코딩됩니다. 그러나 `option.dat` 파일에는 또한 사용자와 그룹에 대해 각각 다른 객체 클래스 집합을 지정하도록 설정할 수 있는 두 개의 MTA 옵션인 `LDAP_USER_OBJECT_CLASSES`와 `LDAP_GROUP_OBJECT_CLASSES`가 존재합니다.

예를 들어, `ims50`, `nms41`의 스키마 태그 설정은 다음 옵션 설정과 동등합니다.

```
LDAP_USER_OBJECT_CLASSES=inetLocalMailRecipient+inetmailuser,  
mailRecipient+nsMessagingServerUser
```

```
LDAP_GROUP_OBJECT_CLASSES=inetLocalMailRecipient+inetmailgroup,mail  
Group
```

사용자나 그룹에 적합한 올바른 객체 클래스 집합이 없을 경우 LDAP 결과는 간단하게 무시됩니다. 또한 MTA는 사용자나 그룹을 처리하고 있는지 확인하여 이 정보를 저장합니다. 저장된 이 정보는 나중에 반복적으로 사용됩니다.

여기에 설명된 객체 클래스 설정이 또한 실제 LDAP 검색 필터를 생성하는 데 사용되며 이 필터는 사용자나 그룹에 대한 올바른 객체 클래스를 항목이 갖고 있는지 확인하는 데 사용될 수 있다는 것에 주의합니다. 이 필터는 \$K 메타 문자를 통해 액세스할 수 있습니다. 또한 이 필터는 채널 프로그램에서 사용할 수 있도록 MTA의 구성에 내부적으로 저장되며 `imsimta cnbuild -option` 명령이 사용되면 MTA 옵션 파일 `option.dat`에 `LDAP_UG_FILTER` 옵션으로 기록됩니다. 이 옵션은 단지 이 파일에 기록만 되며 MTA는 옵션 파일에서 절대로 이 옵션을 읽지 않습니다.

## 항목 상태 검사

다음은 항목의 상태가 검사됩니다. 두 가지 상태 속성이 존재하는데 하나는 항목에 대한 일반 속성이며 다른 하나는 메일 서비스에 대한 특수한 속성입니다.

**표 9-2**는 유효한 `schemata`에 따라 검사되는 `schematag` 항목의 일반 및 메일별 사용자 또는 그룹 속성을 보여 줍니다.

**표 9-2** 검사할 속성

| schematag            | 유형  | General              | 메일                  |
|----------------------|-----|----------------------|---------------------|
| sims40               | 사용자 | inetsubscriberstatus | mailuserstatus      |
| sims40               | 그룹  | none                 | inetmailgroupstatus |
| nms41                | 사용자 | none                 | mailuserstatus      |
| nms41                | 그룹  | none                 | none                |
| Messaging Server 5.0 | 사용자 | inetuserstatus       | mailuserstatus      |
| Messaging Server 5.0 | 그룹  | none                 | inetmailgroupstatus |

필요한 경우 `option.dat` 파일의 `LDAP_USER_STATUS` 및 `LDAP_GROUP_STATUS` MTA 옵션을 각각 사용하여 사용자와 그룹에 대한 대체 일반 상태 속성을 선택할 수 있습니다. 메일별 사용자 및 그룹 상태 속성은 `LDAP_USER_MAIL_STATUS` 및 `LDAP_GROUP_MAIL_STATUS` MTA 옵션으로 제어합니다.

이와 관련된 또 다른 요소는 도메인 자체에 대한 상태(`LDAP_DOMAIN_ATTR_STATUS` 및 `LDAP_DOMAIN_ATTR_MAIL_STATUS`)입니다. 모두 합쳐서 네 개의 상태 속성이 존재하며 이러한 상태 속성은 다음 순서로 고려되어 결합됩니다.

1. 도메인 상태
2. 도메인 메일 상태
3. 사용자 또는 그룹 상태



#### 4. 메일 사용자 또는 그룹 상태

"active" 이외의 상태를 지정하는 첫 번째 속성은 다른 모든 것보다 우선합니다. 가능한 기타 상태 값은 "inactive", "deleted", "removed", "disabled", "hold" 및 "overquota"입니다. "hold", "disabled" 및 "removed" 상태는 메일 도메인이나 메일 사용자, 메일 그룹에만 지정될 수 있습니다. "overquota" 상태는 메일 도메인 또는 메일 사용자 상태로만 지정할 수 있습니다.

특정 상태 속성이 존재하지 않을 경우 모든 상태는 기본적으로 "active"입니다. 알 수 없는 상태 값은 "inactive"로 해석됩니다.

네 가지 상태가 결합되면 사용자나 그룹은 "active", "inactive", "deleted", "removed", "disabled", "hold", 및 "overquota"라는 상태가 될 수 있습니다. active 상태는 별칭 처리가 계속되도록 합니다. inactive 또는 overquota 상태의 경우 4xx(임시) 오류와 함께 주소가 즉시 거부됩니다. deleted, removed 및 disabled 상태의 경우 5xx(영구) 오류와 함께 주소가 즉시 거부됩니다. hold 상태는 상태 처리와 관련해서는 active로 처리되지만 나중에 전달 옵션이 고려될 때 단일 "hold" 항목을 포함하는 옵션 목록이 존재하는 모든 옵션보다 우선하도록 내부 플래그가 설정됩니다.

#### UID 검사

다음 단계는 항목의 UID를 고려하는 것입니다. 다양한 목적에 사용되는 UID는 모든 사용자 항목의 일부여야 하며 그룹 항목에 포함될 수 있습니다. UID가 없는 사용자 항목은 무시되며 이 별칭 URL의 처리가 실패로 종료합니다. 호스트된 도메인의 항목에 대한 UID는 실제 UID, 구분자 문자 및 도메인으로 구성될 수 있습니다. MTA는 실제 UID만을 원하기 때문에 나머지 항목은 제거되며 이 제거 작업에는 option.dat 파일의 LDAP\_DOMAIN\_ATTR\_UID\_SEPARATOR MTA 옵션에서 얻은 도메인 구분자 문자가 사용됩니다.

uid가 아닌 속성이 UID를 저장하는 데 사용된 드문 경우에는 LDAP\_UID MTA 옵션을 사용하여 다른 속성을 사용하도록 강제할 수 있습니다.

#### 메일 캡처

다음은 하나 이상의 메일 캡처 주소를 지정하는 데 사용되는 LDAP 속성이 검사됩니다. 이 목적에 사용되는 속성은 LDAP\_CAPTURE MTA 옵션을 사용하여 지정해야 합니다. 기본값은 없습니다. 이 속성 값은 주소로 간주되며 특수한 "캡처" 알림이 생성되어 현재 메일을 첨부 파일로 포함하는 이러한 주소로 보내집니다. 또한 캡처 주소는 이후에 주소가 봉투의 From: 주소로 표시되는 경우에 주소 역방향 캐시를 시드하는 데 사용됩니다.

## 역방향 캐시 시드

다음은 사용자 항목에 추가된 주 주소와 모든 별칭이 고려됩니다. 이 정보는 주소 역방향 캐시를 시드하는 데 사용되며 현재의 주소 변환 프로세스에서 특정한 역할을 수행하지는 않습니다. 우선 주 주소, 개인 이름, 수신자 제한, 수신자 경계 및 소스 블록 제한 속성이 고려됩니다. 주 주소는 일반적으로 "mail" 속성에 저장되지만 LDAP\_PRIMARY\_ADDRESS MTA 옵션을 적절하게 설정하여 다른 속성을 지정할 수 있습니다. (물론, 주 주소는 그 자체에 대해 반전됩니다.) 다른 모든 속성의 경우에는 기본 속성이 존재하지 않습니다. 이러한 속성을 사용하려면 LDAP\_PERSONAL\_NAME(508페이지의 "휴가 자동 회신 속성" 참조), LDAP\_RECIPIENTLIMIT, LDAP\_RECIPIENTCUTOFF(392페이지의 "메일 수신자 제한" 참조) 및 LDAP\_SOURCEBLOCKLIMIT(388페이지의 "절대 메일 크기 제한 지정" 참조) MTA 옵션으로 해당 속성을 지정해야 합니다. 또한 해당하는 도메인 수준 수신자 제한, 수신자 경계 및 소스 블록 제한 속성도 이 시점에서 고려됩니다. 사용자 수준 설정은 모든 도메인 수준 설정보다 우선합니다.

다음은 모든 보조 주소가 고려되고 각 보조 주소에 대한 캐시 항목이 작성됩니다. 보조 주소에는 역방향으로 진행되는 주소와 그렇지 않은 주소의 두 종류가 있습니다. 메일 캡처 요청을 모든 경우에 검사해야 하기 때문에 주소 역방향 캐시를 적절하게 시드하려면 두 종류를 모두 고려해야 합니다.

역방향이 적용되는 보조 주소는 일반적으로 mailAlternateAddress 속성에 저장되며 LDAP\_ALIAS\_ADDRESSES MTA 옵션을 설정하여 다른 옵션을 지정할 수 있습니다. 역방향이 적용되지 않는 보조 주소는 일반적으로 mailEquivalentAddress 속성에 저장되며 LDAP\_EQUIVALENCE\_ADDRESSES MTA 옵션으로 다른 속성을 지정할 수 있습니다.

## 메일 호스트 및 라우팅 주소

이제 mailhost 및 mailRoutingAddress 속성을 고려할 차례입니다. 고려되는 실제 속성은 각각 LDAP\_MAILHOST 및 LDAP\_ROUTING\_ADDRESS MTA 옵션을 사용하여 무시할 수 있습니다. 이러한 속성은 서로 합쳐져서 주소를 지금 실행해야 하는지 아니면 다른 시스템으로 전달해야 하는지 여부를 결정합니다.

첫 번째 단계는 이 항목에 대해 mailhost가 의미가 있는지 여부를 확인하는 것입니다. 항목이 mailhost 특정 항목인지 여부를 확인하기 위해 해당 항목에 대해 활성화된 전달 옵션의 예비 검사가 수행됩니다. mailhost 특정 항목이 아닐 경우 mailhost 검사가 생략됩니다. 이 검사가 수행되는 방법을 이해하려면 213페이지의 "전달 옵션 처리"에 설명된 내용을 특히 # 플래그를 중심으로 참조하십시오.

사용자 항목의 경우 `mailhost` 속성은 로컬 시스템을 식별할 경우에만 실행됩니다. `mailhost` 속성은 `local.hostname configutil` 매개 변수의 값과 `local.imta.hostnamealiases configutil` 매개 변수에 지정된 값 목록에 대해 비교됩니다. 일치하는 항목이 있을 경우 `mailhost` 속성은 로컬 호스트를 식별하는 것으로 간주됩니다.

일치에 성공할 경우 별칭이 로컬로 실행될 수 있으며 별칭 처리가 계속된다는 것을 의미합니다. 일치에 실패할 경우에는 `mailhost`로 전달해야만 메일이 작동한다는 것을 의미합니다. 다음 형식의 새 주소가 생성되며

`@mailhost:user@domain`

별칭 확장 작업의 결과가 됩니다.

누락된 `mailhost` 속성의 처리는 항목이 사용자인지 아니면 그룹인지 여부에 따라 달라집니다. 사용자인 경우 `mailhost`가 필수적이므로 `mailhost` 속성이 존재하지 않을 경우 다음 형식의 새 주소가

`@smarthost:user@domain`

`LDAP_DOMAIN_ATTR_SMARTHOST MTA` 옵션에 지정된 도메인에 대한 스마트 호스트를 사용하여 생성됩니다. 도메인에 대한 스마트 호스트가 존재하지 않을 경우 오류가 보고됩니다.

반면, 그룹의 경우에는 `mailhost`가 필요하지 않으므로 누락된 `mailhost`는 그룹을 어디에서나 확장할 수 있다는 것을 의미하는 것으로 해석됩니다. 따라서 별칭 처리가 계속 진행됩니다.

`mailRoutingAddress` 속성은 유용한 최종 기능 하나를 추가합니다. 이 속성이 존재할 경우 별칭 처리는 결과적으로 `mailRoutingAddress`와 함께 종료합니다. 그러나 `mailhost`가 존재할 경우 해당 `mailhost`는 `mailRoutingAddress`에 소스 경로로 추가됩니다.

## 기타 속성 지원

다음은 `mailMsgMaxBlocks` 속성이 고려됩니다. 우선 이 속성은

`LDAP_DOMAIN_ATTR_BLOCKLIMIT MTA` 옵션에서 반환된 도메인 블록 제한에 따라 최소화됩니다. 현재 메일의 크기가 이 제한을 초과하는 것으로 확인될 경우 별칭 처리는 크기 초과 오류와 함께 종료합니다. 크기가 알려지지 않거나 제한을 초과하지 않을 경우에는 제한이 저장되며 나중에 메일 자체가 검사될 때 해당 제한이 다시 검사됩니다.

`mailMsgMaxBlocks` 사용은 `LDAP_BLOCKLIMIT MTA` 옵션을 사용하여 무시할 수 있습니다.

다음은 여러 속성이 평가 및 저장됩니다. 결국 이러한 속성은 `ims_master` 채널 프로그램에 사용되도록 대기열 파일 항목에 기록되며 이 채널 프로그램은 이러한 속성을 사용하여 저장소의 사용자 정보 캐시를 업데이트합니다. 개별 사용자에게 대한 속성이 발견되지 않을 경우 도메인 수준 속성을 사용하여 기본값을 설정할 수 있습니다.

LDAP 항목이 사용자가 아니라 그룹에 대한 것이거나 LDAP 항목을 LDAP 디렉토리가 아니라 별칭 캐시에서 가져온 경우 이 단계를 건너뛰게 됩니다. 후자의 조건에 담겨 있는 논리는 이 정보를 자주 업데이트하는 것이 불필요하며 별칭 캐시를 사용하면 업데이트를 수행해야 할 경우에 대한 적절한 기준이 제공된다는 점입니다. 검색된 속성의 이름은 다양한 MTA 옵션에 의해 설정됩니다.

**표 9-3**은 검색된 디스크 할당량 및 메일 할당량 속성을 설정하는 MTA 옵션을 보여 줍니다.

**표 9-3** 검색된 디스크 할당량 및 메일 할당량 속성을 설정하는 MTA 옵션

| MTA 옵션             | 속성           |
|--------------------|--------------|
| LDAP_DISK_QUOTA    | mailQuota    |
| LDAP_MESSAGE_QUOTA | mailMsgQuota |

다음은 나중에 메타 문자 대체와 함께 사용할 수 있도록 여러 속성이 저장됩니다.

**표 9-4**는 MTA 옵션, 기본 속성 및 메타 문자를 보여 줍니다.

**표 9-4** MTA 옵션, 기본 속성 및 메타 문자

| MTA 옵션             | 기본 속성                   | 메타 문자         |
|--------------------|-------------------------|---------------|
| LDAP_PROGRAM_INFO  | mailProgramDeliveryInfo | \$P           |
| LDAP_DELIVERY_FILE | mailDeliveryFileURL     | \$F           |
| LDAP_SPARE_1       | 기본값 없음                  | \$1E \$1G \$E |
| LDAP_SPARE_2       | 기본값 없음                  | \$2E \$2G \$G |
| LDAP_SPARE_3       | 기본값 없음                  | \$3E \$3G     |
| LDAP_SPARE_4       | 기본값 없음                  | \$4E \$4G     |
| LDAP_SPARE_5       | 기본값 없음                  | \$5E \$5G     |

추가 속성을 위한 예비 슬롯이 포함되는데 이러한 슬롯을 사용하여 사용자 정의된 주소 확장 기능을 작성할 수 있습니다.

다음은 `mailconversiontag` 속성과 연관된 모든 값이 현재의 변환 태그 집합에 추가됩니다. 이 속성의 이름은 `LDAP_CONVERSION_TAG` MTA 옵션을 사용하여 변경할 수 있습니다. 또한 도메인의 `mailDomainConversionTag` 속성과 연관된 모든 값도 추가됩니다.

## 전달 옵션 처리

다음은 mailDeliveryOption 속성이 검사됩니다. 이 속성의 이름은 LDAP\_DELIVERY\_OPTION MTA 옵션을 사용하여 변경할 수 있습니다. 이 속성은 여러 값을 가지며 별칭 변환 프로세스에 의해 생성되는 주소가 이 속성 값에 의해 결정됩니다. 또한 사용자와 그룹에 대해 허용되는 값이 다릅니다. 일반적으로 허용되는 값은 program, forward 및 hold입니다. 사용자 전용 값은 mailbox, native, unix 및 autoreply이며 그룹 전용 값은 members, members\_offline 및 file입니다.

mailDeliveryOption 속성이 적절한 주소로 변환되는 작업은 DELIVERY\_OPTIONS MTA 옵션에 의해 제어됩니다. 이 옵션은 허용되는 각 mailDeliveryOption 값이 생성하는 주소뿐만 아니라 허용되는 mailDeliveryOption 값과 각 값이 사용자, 그룹 또는 둘 다에 적용될 수 있는지 여부를 지정합니다.

이 옵션 값은 deliveryoption=template 쌍의 쉼표로 구분된 목록으로 구성되며 각 쌍은 하나 이상의 선택적 단일 문자 접두어를 가집니다.

DELIVERY\_OPTIONS 옵션의 기본값은 다음과 같습니다.

```
DELIVERY_OPTIONS=*mailbox=$M%\$2I$_+$2S@ims-ms-daemon, \
    &members=*, \
    *native=$M@native-daemon, \
    /hold=@hold-daemon:$A, \
    *unix=$M@native-daemon, \
    &file=+$F@native-daemon, \
    &@members_offline=*, \
    program=$M%$P@pipe-daemon, \
    #forward=**, \
    *^!autoreply=$M+$D@bitbucket
```

각 전달 옵션은 가능한 mailDeliveryOption 속성 값에 해당하며 해당 템플릿은 URL 처리에 사용되는 것과 동일한 메타 문자 대체 방법을 사용하여 결과 주소를 지정합니다.

[표 9-5](#)는 DELIVERY\_OPTIONS 옵션에 사용할 수 있는 단일 문자 접두어를 보여 줍니다.

**표 9-5** DELIVERY\_OPTIONS MTA 옵션에 사용할 수 있는 단일 문자 접두어

| 접두어 문자 | 설명                                                                                                                                                                                                                    |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| @      | 메일이 프로세스 채널에 리디렉션되어야 한다는 사실을 보여주도록 플래그를 설정하십시오. 현재 사용자/그룹의 처리는 금지되어 있습니다. 플래그는 재처리 채널에서 보내지는 메일에 대해서는 무시됩니다.                                                                                                          |
| *      | 전달 옵션이 사용자에게 적용됩니다.                                                                                                                                                                                                   |
| &      | 전달 옵션이 그룹에 적용됩니다.                                                                                                                                                                                                     |
| \$     | 이 사용자 또는 그룹의 확장이 지연된다는 것을 나타내는 플래그를 설정합니다.                                                                                                                                                                            |
| ^      | 휴가 시작 및 종료 시간을 검사하여 이 전달 옵션이 실제로 유효한지 확인해야 한다는 것을 나타내는 플래그를 설정합니다.                                                                                                                                                    |
| #      | 이 전달 옵션의 확장이 항목의 지정된 메일 호스트에서 발생할 필요가 없다는 것을 나타내는 플래그를 설정합니다. 즉, 다음 항목은 메일 호스트에 독립적입니다. 이렇게 하면 MTA는 주어진 사용자 또는 그룹의 모든 전달 옵션이 메일 호스트에 독립적인지 확인할 수 있습니다. 이 조건이 충족되면 MTA는 메일을 메일 호스트에 전달하지 않고도 즉시 항목에 대한 작업을 수행할 수 있습니다. |
| /      | 이 전달 옵션에 의해 생성된 모든 주소가 보관된다는 것을 나타내는 플래그를 설정합니다. 이러한 수신자 주소를 포함하는 메일 파일은 .HELD 확장자를 가집니다.                                                                                                                             |
| !      | MTA가 자동 회신 작업을 내부적으로 처리해야 한다는 것을 나타내는 플래그를 설정합니다. 이 접두어는 자동 회신 전달 옵션에서만 사용되어야 합니다. 옵션 값은 메일을 bitbucket 채널로 전송해야 합니다.                                                                                                  |

\* 및 &가 모두 존재하지 않을 경우 전달 옵션은 사용자 및 그룹 모두에 적용됩니다.

### 전달 옵션에 사용할 추가 메타 문자

MTA의 새로운 URL 템플릿 기능 사용을 지원하기 위해 여러 추가 메타 문자가 다음 사항이 추가되었습니다.

**표 9-6**은 전달 옵션에서 사용하기 위한 추가 메타 문자와 그 설명을 보여 줍니다.

**표 9-6** 전달 옵션에서 사용하기 위한 추가 메타 문자

| 메타 문자 | 설명                 |
|-------|--------------------|
| \$\   | 후속 텍스트를 소문자로 바꿉니다. |
| \$\$  | 후속 텍스트를 대문자로 바꿉니다. |

**표 9-6** 전달 옵션에서 사용하기 위한 추가 메타 문자 (계속)

| 메타 문자 | 설명                                                                                                       |
|-------|----------------------------------------------------------------------------------------------------------|
| \$_   | 후속 텍스트에 대해 대소문자 변환을 수행하지 않습니다.                                                                           |
| \$nA  | 주소의 $n$ 번째 문자를 삽입합니다. 첫 번째 문자는 문자 0입니다. $n$ 이 생략될 경우 전체 주소가 대체됩니다. 이 메타 문자는 자동 회신 디렉토리 경로를 생성하는 데 사용됩니다. |
| \$D   | 주소의 도메인 부분을 삽입합니다.                                                                                       |
| \$nE  | $n$ 번째 예비 속성의 값을 삽입합니다. $n$ 이 생략될 경우 첫 번째 속성이 사용됩니다.                                                     |
| \$F   | 전달 파일의 이름(mailDeliveryFileURL 속성)을 삽입합니다.                                                                |
| \$nG  | $n$ 번째 예비 속성의 값을 삽입합니다. $n$ 이 생략될 경우 두 번째 속성이 사용됩니다.                                                     |
| \$nH  | 원래 주소에서 0부터 시작하는 도메인의 $n$ 번째 구성 요소를 삽입합니다. $n$ 이 생략될 경우 기본값은 0입니다.                                       |
| \$nI  | 별칭과 연관된 호스트된 도메인을 삽입합니다. 이 메타 문자는 표 9-7에 의미가 설명되어 있는 정수 매개 변수 $n$ 을 허용합니다.                               |
| \$nJ  | 0부터 시작하는 호스트 도메인의 $n$ 번째 부분을 삽입합니다. $n$ 의 기본값은 0입니다.                                                     |
| \$nO  | 현재 주소와 연관된 소스 루트를 삽입합니다. 이 메타 문자는 표 9-7에 의미가 설명되어 있는 정수 매개 변수 $n$ 을 허용합니다.                               |
| \$K   | 사용자 또는 그룹에 대한 객체 클래스와 일치하는 LDAP 필터를 삽입합니다. LDAP_UG_FILTER 출력 전용 MTA 옵션의 설명을 참조하십시오.                      |
| \$L   | 주소의 로컬 부분을 삽입합니다.                                                                                        |
| \$nM  | UID의 $n$ 번째 문자를 삽입합니다. 첫 번째 문자는 문자 0입니다. $n$ 이 생략될 경우 전체 UID가 대체됩니다.                                     |
| \$P   | 프로그램 이름(mailProgramDeliveryInfo 속성)을 삽입합니다.                                                              |
| \$nS  | 현재 주소와 연관된 하위 주소를 삽입합니다. 이 메타 문자는 표 9-7에 의미가 설명되어 있는 정수 매개 변수 $n$ 을 허용합니다.                               |
| \$nU  | 현재 주소의 메일함 부분에서 따옴표가 없는 형식의 $n$ 번째 문자를 삽입합니다. 첫 번째 문자는 문자 0입니다. $n$ 이 생략될 경우 따옴표가 없는 전체 메일함이 대체됩니다.      |
| \$nX  | 메일 호스트의 $n$ 번째 구성 요소를 삽입합니다. $n$ 이 생략될 경우 전체 메일 호스트가 삽입됩니다.                                              |

표 9-7은 정수 매개 변수가 \$nI 및 \$nS 메타 문자의 동작을 수정하는 방법을 보여 줍니다.

**표 9-7** \$nI 및 \$nS 메타 문자의 동작 수정을 제어하는 정수

| 정수 | 동작 설명                                                                                      |
|----|--------------------------------------------------------------------------------------------|
| 0  | 사용할 수 있는 값이 없을 경우 실패합니다(기본값).                                                              |
| 1  | 사용할 수 있는 값이 있을 경우 해당 값을 삽입하고 없을 경우에는 아무 것도 삽입하지 않습니다.                                      |
| 2  | 사용할 수 있는 값이 있을 경우 해당 값을 삽입하고 없을 경우에는 아무 것도 삽입하지 않고 앞의 문자를 삭제합니다(이 특수한 동작은 ims-ms 채널에 필요함). |
| 3  | 사용할 수 있는 값이 있을 경우 해당 값을 삽입하고 없을 경우에는 아무 것도 삽입하지 않고 다음 문자를 무시합니다.                           |

표 9-8은 메타 문자 외에 두 개의 특수한 템플릿 문자열을 보여 줍니다.

**표 9-8** 특수한 템플릿 문자열

| 특수한 템플릿 문자열 | 설명                                                                               |
|-------------|----------------------------------------------------------------------------------|
| *           | 그룹 확장을 수행합니다. 사용자 항목의 경우에는 이 값이 유효하지 않습니다.                                       |
| **          | LDAP_FORWARDING_ADDRESS MTA 옵션에 의해 명명된 속성을 확장합니다. 기본값은 mailForwardingAddress입니다. |

그룹 확장의 경우 예를 들어, 사용자의 mailDeliveryOption 값이 mailbox로 설정되면 스트라이프된 UID, 백분율 기호 다음의 호스트된 도메인(적용 가능한 경우), 더하기 기호 다음의 하위 주소(지정된 경우), 마지막으로 @ims-ms-daemon으로 구성된 새 주소가 생성됩니다.

### 전달 옵션 기본값

이 시점에서 활성 전달 옵션의 목록이 비어 있을 경우 목록의 첫 번째 옵션(일반적으로 메일함)이 사용자에게 대해 활성화되고 목록의 두 번째 옵션(일반적으로 구성원)이 그룹에 대해 활성화됩니다.

### 시작 및 종료 날짜 검사

전달 옵션 목록을 읽은 후에 시작 및 종료 날짜가 검사됩니다. 두 가지 속성이 존재하며 이러한 속성의 이름은 각각 LDAP\_START\_DATE(기본값 vacationStartDate) 및 LDAP\_END\_DATE(기본값 vacationEndDate) MTA 옵션에 의해 제어됩니다.



하나 이상의 활성 전달 옵션이 ^ 접두어 문자를 지정한 경우 이러한 옵션의 값이 현재 날짜에 대해 검사됩니다. 현재 날짜가 이러한 옵션에 지정된 범위를 벗어날 경우 ^ 접두어를 가진 전달 옵션이 활성 집합에서 제거됩니다. 자세한 내용은 [508페이지의 "휴가 자동 회신 속성"](#)을 참조하십시오.

## Optin 및 Presence 속성

LDAP\_OPTIN MTA 옵션을 사용하면 스팸 필터 수신 선택 기능 값의 목록을 포함하는 LDAP 속성을 지정할 수 있습니다. 이 옵션이 지정되고 속성이 존재할 경우 현재의 스팸 필터 수신 선택 기능 목록에 해당 속성이 추가됩니다. 또한 LDAP\_DOMAIN\_ATTR\_OPTIN MTA 옵션에 의해 설정된 도메인 수준 속성이 설정하는 모든 값도 이 목록에 추가됩니다.

LDAP\_PRESENCE MTA 옵션을 사용하면 사용자에게 대한 존재 여부 정보를 반환하기 위해 확인할 수 있는 URL을 지정할 수 있습니다. 이 옵션이 지정되고 속성이 존재할 경우 시브(sieve) 존재 여부 테스트와 함께 사용할 수 있도록 속성 값이 저장됩니다. 사용자 항목에 대한 값이 존재하지 않을 경우 LDAP\_DOMAIN\_ATTR\_PRESENCE MTA 옵션에 의해 설정된 도메인 수준 속성이 이 URL의 소스로 사용됩니다.

## 시브(Sieve) 필터 처리

다음은 이 항목에 적용되는 시브(sieve) 필터에 대해 mailSieveRuleSource 속성이 검사됩니다. 이 속성은 존재할 경우 이 시점에서 구문 분석 및 저장됩니다. 이 속성 값에 대한 두 가지 가능한 형식으로는 완전한 시브(sieve) 스크립트를 포함하는 단일 값 형식과 각 값이 시브(sieve) 스크립트를 포함하는 다중 값 형식이 있습니다. 후자의 형식은 웹 필터 생성 인터페이스에 의해 생성됩니다. 값의 순서를 지정하고 적절하게 값을 결합하기 위해 특수한 코드가 사용됩니다.

mailSieveRuleSource 속성 사용을 특별히 LDAP\_FILTER MTA 옵션을 사용하여 무시할 수 있습니다.

## 지연된 처리 제어

다음은 mailDeferProcessing 속성이 검사됩니다. 이 속성은 LDAP\_REPROCESS MTA 옵션을 사용하여 변경할 수 있습니다. 이 속성이 존재하고 no로 설정된 경우 처리는 정상적으로 처리됩니다. 그러나 이 속성이 yes로 설정되고 현재 소스 채널이 재처리 채널이 아닐 경우 이 항목의 확장이 중지되며 원래 `user@domain` 주소가 단순히 재처리 채널의 대기열에 포함됩니다. 이 속성이 존재하지 않을 경우 전달 옵션 처리와 연관된 지연된 처리 문자 접두어의 설정이 검사됩니다. 이에 대한 예는 [전달 옵션 처리](#) 절을 참조하십시오. 이 접두어가 설정된 경우 처리가 지연되고 설정되지 않은 경우 사용자에게 대한 기본값은 no입니다. 그룹에 대한 기본값은 DEFER\_GROUP\_PROCESSING MTA 옵션에 의해 제어되며 이 옵션의 기본값은 1(yse)입니다. 사용자 항목의 경우 이 시점에서 별칭 처리가 완료됩니다.

## 그룹 확장 속성

여러 추가 속성이 그룹 확장과 연관되며 이 시점에서 처리되어야 합니다. 이러한 속성의 이름은 모두 다양한 MTA 옵션을 통해 구성할 수 있습니다.

**표 9-9**에서는 기본 속성 이름, 속성 이름을 설정하기 위한 MTA 옵션을 나열합니다. MTA가 속성을 처리하는 방법이 나열되어 있습니다. 이 표에 있는 요소의 순서는 다양한 그룹 속성이 처리되는 순서를 보여 줍니다. 정확한 작업을 위해서는 이 순서가 필수적입니다.

**표 9-9** 설정할 그룹 확장 기본 속성 및 MTA 옵션

| 기본 속성                 | (속성 이름을 설정하기 위한 MTA 옵션)<br>속성이 처리되는 방법                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| mgrpMsgRejectAction   | (LDAP_REJECT_ACTION) 후속 액세스 검사가 실패할 경우 발생하는 작업을 제어하는 단일 값 속성입니다. TOMODERATOR 하나만 정의되며 이 값은 설정된 경우 모든 액세스 실패를 mgrpModerator 속성에 의해 지정된 중재자로 리디렉션하도록 MTA에 지시합니다. 이 속성에 값(기본값 및 다른 모든 값)이 지정되면 오류가 보고되며 메일이 거부됩니다.                                                                                                                                                                                                                                                                                                                                                |
| mailRejectText        | (LDAP_REJECT_TEXT) 이 속성의 첫 번째 값에 저장된 텍스트의 첫 번째 행이 저장됩니다. 다음 인증 속성 중 하나로 인해 메일이 거부될 경우 이 텍스트가 반환됩니다. 이것은 텍스트가 SMTP 응답에 나타날 수 있으므로 값을 US-ASCII로 제한하여 현재 메시징 표준을 따르도록 해야 한다는 것을 의미합니다.                                                                                                                                                                                                                                                                                                                                                                            |
| mgrpBroadcasterPolicy | (LDAP_AUTH_POLICY) 그룹에 보내는 데 필요한 인증 수준을 지정합니다. 가능한 토큰은 SMTP_AUTH_REQUIRED 또는 AUTH_REQ(두 가지 모두 SMTP AUTH 명령을 사용하여 그룹에 보내는 순서대로 보내는 사람을 식별해야 함을 의미), PASSWORD_REQUIRED, PASSWD_REQUIRED 또는 PASSWD_REQ(이 세 가지는 mgrpAuthPassword 속성에 지정된 목록의 비밀번호가 메일의 Approved: 헤더 필드에 표시되어야 함을 의미), OR(이 목록에 대해 OR_CLAUSES MTA 옵션 설정을 1로 변경), AND(이 목록에 대해 OR_CLAUSES MTA 옵션 설정을 0으로 변경), NO_REQUIREMENTS(no-op) 등입니다. 여러 값이 허용되고 각 값은 쉼표로 구분된 토큰 목록으로 구성될 수 있습니다.<br><br>SMTP AUTH가 호출된 경우에는 또한 MAIL FROM 주소가 아니라 SASL 계층에 의해 제공된 전자 메일 주소에 대해 이후의 모든 권한 부여 검사가 수행된다는 것을 의미합니다. |
| mgrpAllowedDomain     | (LDAP_AUTH_DOMAIN) 이 그룹에 메일을 제출하는 것이 허용된 도메인입니다. 0(기본값)으로 설정된 OR_CLAUSES MTA 옵션과의 일치 실패는 액세스 검사가 실패했고 모든 후속 테스트를 수행하지 않는다는 의미입니다. 1로 설정된 OR_CLAUSES MTA 옵션과의 일치 실패는 "failure pending" 플래그를 설정합니다. 즉, 액세스 검사를 계속하려면 다른 액세스 검사가 성공해야 합니다. 전송자가 이미 LDAP_AUTH_URL와 일치된 경우에는 이 검사를 수행하지 않습니다. 값이 여러 개일 수 있고 글롭 와일드카드가 허용됩니다.                                                                                                                                                                                                                                        |

**표 9-9** 설정할 그룹 확장 기본 속성 및 MTA 옵션 (계속)

| 기본 속성                     | (속성 이름을 설정하기 위한 MTA 옵션)<br>속성이 처리되는 방법                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|---------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| mgrpDisallowedDomain      | (LDAP_CANT_DOMAIN) 이 그룹에 메일을 제출하는 것이 허용되지 않는 도메인입니다. 일치하는 액세스 검사가 실패했고 모든 후속 검사를 수행하지 않음을 의미합니다. 전송자가 이미 LDAP_AUTH_URL과 일치되어 있으면 이러한 검사를 수행하지 않습니다. 값이 여러 개일 수 있고 그룹 와일드카드가 허용됩니다.                                                                                                                                                                                                                                                                                                                             |
| mgrpAllowedBroadcaster    | (LDAP_AUTH_URL) 이 그룹에 메일을 전송하는 것이 허용된 메일 주소를 식별하는 URL입니다. 값이 여러 개일 수 있습니다. 각 URL은 주소 목록으로 확장되며 현재 봉투의 보낸 사람 주소에 대해 각 주소가 검사됩니다. 0(기본값)으로 설정된 OR_CLAUSES MTA 옵션과의 일치 실패는 액세스 검사가 실패했고 모든 후속 테스트를 수행하지 않는다는 의미입니다. 1로 설정된 OR_CLAUSES MTA 옵션과의 일치 실패는 "failure pending" 플래그를 설정합니다. 즉, 액세스 검사가 성공하기 위해서는 다른 액세스 검사가 성공해야 합니다. 일치하는 경우에도 후속 도메인 액세스 검사는 비활성화됩니다. 수행되는 확장은 모든 액세스 제어 검사를 비활성화하는 SMTP EXPN와 비슷합니다.                                                                                                   |
| mgrpDisallowedBroadcaster | (LDAP_CANT_URL) 메일을 이 그룹에 전송하는 것이 허용되지 않는 메일 주소를 식별하는 URL입니다. 값이 여러 개일 수 있습니다. 각 URL은 주소 목록으로 확장되며 현재 봉투의 보낸 사람 주소에 대해 각 주소가 검사됩니다. 일치하는 액세스 검사가 실패했고 모든 후속 검사가 수행되지 않는다는 의미입니다. 수행되는 확장은 모든 액세스 제어 검사를 비활성화하는 SMTP EXPN와 비슷합니다.                                                                                                                                                                                                                                                                               |
| mgrpMsgMaxSize            | (LDAP_ATTR_MAXIMUM_MESSAGE_SIZE) 그룹에 전송할 수 있는 최대 메일 크기(바이트)입니다. 이 속성은 폐기되었지만 이전 버전과의 호환성을 위해 계속 지원됩니다. 대신, 새 mailMsgMaxBlocks 속성을 사용해야 합니다.                                                                                                                                                                                                                                                                                                                                                                    |
| mgrpAuthPassword          | (LDAP_AUTH_PASSWORD) 목록에 게시하는 데 필요한 비밀번호를 지정합니다. mgrpAuthPassword 속성이 존재하면 재처리 통과가 강제됩니다. 메일이 재처리 채널의 대기열에 포함되면 헤더에서 가져온 비밀번호가 봉투에 포함됩니다. 그런 다음 재처리 도중에 해당 비밀번호는 봉투에서 가져와 이 속성에 대해 검사됩니다. 또한 실제로 사용되는 비밀번호만 헤더 필드에서 제거됩니다.<br><br>이 속성에서 OR_CLAUSES MTA 옵션은 다른 액세스 검사 속성의 경우와 같은 방식으로 작동됩니다.                                                                                                                                                                                                                   |
| mgrpModerator             | (LDAP_MODERATOR_URL) 일련의 주소로 확장될 이 속성에 의해 제공된 URL 목록입니다. 이 주소 목록의 해석은 LDAP_REJECT_ACTION MTA 옵션의 설정에 따라 달라집니다. LDAP_REJECT_ACTION이 TOMODERATOR로 설정된 경우 이 속성은 액세스 검사 중 하나가 실패할 경우에 메일을 전송할 중재자 주소를 지정합니다. LDAP_REJECT_ACTION이 누락되거나 다른 값을 가진 경우 이 주소 목록은 봉투의 보낸 사람 주소와 비교됩니다. 일치하는 항목이 있을 경우 처리가 계속됩니다. 일치하는 항목이 없을 경우 이 속성에 지정된 모든 주소로 메일이 다시 전송됩니다. 이 속성을 확장하는 작업은 이 속성 값을 그룹에 대한 URL 목록으로 만드는 방법으로 구현됩니다. 그룹과 연관된 RFC822 주소 또는 DN의 모든 목록이 지워지며 그룹에 대한 전달 옵션은 members로 설정됩니다. 마지막으로 이 표에 나열된 후속 그룹 속성이 무시됩니다. |

**표 9-9** 설정할 그룹 확장 기본 속성 및 MTA 옵션 (계속)

| 기본 속성                | (속성 이름을 설정하기 위한 MTA 옵션)<br>속성이 처리되는 방법                                                                                                                                                                                                                |
|----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| mgrpDeliverTo        | (LDAP_GROUP_URL1) 확장될 경우 메일 목록 구성원 주소의 목록을 제공하는 URL 목록입니다.                                                                                                                                                                                            |
| memberURL            | (LDAP_GROUP_URL2) 확장될 경우 메일 목록 구성원 주소의 또 다른 목록을 제공하는 URL의 다른 목록입니다.                                                                                                                                                                                   |
| uniqueMember         | (LDAP_GROUP_DN) 그룹 구성원의 DN 목록입니다. DN은 전체 하위 트리를 지정할 수 있습니다. 고유한 구성원 DN은 LDAP URL에 이러한 DN을 내장하는 방법으로 확장됩니다. 사용할 정확한 URL은 GROUP_DN_TEMPLATE MTA 옵션에 의해 지정됩니다. 이 옵션에 대한 기본값은 ldap:/// \$A?mail?sub?(mail=*)입니다.<br>\$A는 uniqueMember DN이 삽입되는 지점을 지정합니다. |
| mgrpRFC822MailMember | (LDAP_GROUP_RFC822) 이 목록에 있는 구성원의 메일 주소입니다.                                                                                                                                                                                                           |
| rfc822MailMember     | (LDAP_GROUP_RFC822) rfc822MailMember는 이전 버전과의 호환성을 위해 지원됩니다. rfc822MailMember와 mgrpRFC822MailMember 중에서 하나를 주어진 모든 그룹에 사용할 수 있습니다.                                                                                                                    |
| mgrpErrorsTo         | (LDAP_ERRORS_TO) 봉투의 메일 발송자(MAIL FROM) 주소를 속성이 지정하는 주소로 설정합니다.                                                                                                                                                                                        |
| mgrpAddHeader        | (LDAP_ADD_HEADER) 속성에 지정된 헤더를 헤더 자르기 ADD 옵션으로 변환합니다.                                                                                                                                                                                                  |
| mgrpRemoveHeader     | (LDAP_REMOVE_HEADER) 지정된 헤더를 헤더 자르기 MAXLINES=-1 옵션으로 변환합니다.                                                                                                                                                                                           |
| mgrpMsgPrefixText    | (LDAP_PREFIX_TEXT) 지정된 텍스트를 메일 텍스트(있을 경우)의 시작 부분에 추가합니다.                                                                                                                                                                                              |
| mgrpMsgSuffixText    | (LDAP_SUFFIX_TEXT) 지정된 텍스트를 메일 텍스트(있을 경우)의 끝 부분에 추가합니다.                                                                                                                                                                                               |
| No Default           | (LDAP_ADD_TAG) 지정된 텍스트의 제목을 검사하며 없을 경우 제목 필드의 첫 부분에 텍스트가 추가됩니다.                                                                                                                                                                                       |

SMTP EXPN 명령: mgmanMemberVisibility 또는 확장의 일부인 특수한 그룹 확장에서는 최종 속성 하나가 검사됩니다. LDAP\_EXPANDABLE MTA 옵션을 사용하여 검사할 다른 속성을 선택할 수 있습니다. 가능한 값에는 anyone(누구나 그룹을 확장할 수 있다는 것을 의미), all 또는 true(확장이 허용되려면 사용자가 SASL로 성공적으로 인증되어야 한다는 것을 의미), 그리고 none(확장이 허용되지 않는다는 것을 의미)이 있습니다. 인식되지 않는 값은 none으로 해석됩니다. 이 속성이 존재하지 않을 경우 EXPANDABLE\_DEFAULT MTA 옵션은 확장이 허용되는지 여부를 제어합니다.

별칭 항목은 도메인 항목과 비슷한 방식으로 캐시됩니다. 별칭 캐시를 제어하는 MTA 옵션은 `ALIAS_ENTRY_CACHE_SIZE`(기본값은 1000개 항목) 및 `ALIAS_ENTRY_CACHE_TIMEOUT`(기본값은 600초)입니다. 주어진 별칭에 대한 전체 LDAP 반환 값은 캐시에 보관됩니다.

별칭 항목의 네거티브 캐싱은 `ALIAS_ENTRY_CACHE_NEGATIVE` MTA 옵션에 의해 제어됩니다. 0이 아닌 값은 별칭 일치 실패의 캐싱을 활성화하고 값 0은 이 캐싱을 비활성화합니다. 별칭 항목의 네거티브 캐싱은 기본적으로 비활성화되는데 이것은 잘못된 주소가 실제로 반복적으로 지정될 가능성이 별로 없기 때문입니다. 또한 네거티브 캐싱은 디렉토리에 추가된 새 사용자를 제때에 인식하는 데 방해가 될 수 있습니다. 그러나 부속 도메인이 많이 사용될 경우 사이트는 별칭의 네거티브 캐싱을 다시 활성화하는 것을 고려해야 합니다. `ALIAS_URL0`에 지정된 URL에 의해 수행되는 검색은 성공할 가능성이 적습니다.

## 주소 역방향

Direct LDAP를 사용한 주소 역방향은 `USE_REVERSE_DATABASE` 값 4로 시작되며 이 값은 역방향 데이터베이스를 사용하지 않도록 설정합니다. 그런 다음 주소 역방향은 앞에서 설명한 라우팅 기능을 토대로 작성됩니다. 특히 이전 버전에서는 다음 형식의 역방향 URL 지정으로 시작되었습니다.

```
REVERSE_URL=ldap:/// $V?mail?sub?$Q
```

`$V` 메타 문자는 별칭 URL과 관련하여 이미 설명되었습니다. 그러나 `$Q` 메타 문자는 별칭 URL에 사용되는 `$R` 메타 문자와 기능이 비슷하지만 특별히 주소 역방향에 사용하도록 되어 있습니다. `$R`과 달리 이 메타 문자는 주소 역방향을 후보인 주소가 포함된 속성을 검색하는 필터를 생성합니다. 검색할 속성 목록은 MTA 옵션 `LDAP_MAIL_REVERSES`에서 가져옵니다. 이 옵션이 설정되지 않은 경우 `local.imta.schematag configutil` 매개 변수가 검사되고 그 값에 따라 적절한 기본 속성 집합이 선택됩니다.

표 9-10에서는 `local.imta.schematag` 값과 선택된 기본 속성을 보여 줍니다.

**표 9-10** `local.imta.schematag` 값과 속성

| 스키마 태그 값 | 속성                        |
|----------|---------------------------|
| sims40   | mail,rfc822mailalias      |
| nms41    | mail,mailAlternateAddress |
| ims50    | mail,mailAlternateAddress |

그러나 \$Q는 사용하기에 더 이상 적합하지 않습니다. 메일 캡처와 다른 기능이 제대로 작동하도록 하기 위해 일치하는 항목이 발생했다는 사실 외에도 일치한 속성에 주의하도록 주소 역방향이 향상되었습니다. 이것은 \$Q 대신에 \$R을 사용하여 필터를 지정해야 한다는 것을 의미합니다. 또한 주소 역방향이 필요할 수 있는 속성 목록을 반환하는 \$N 메타 문자가 추가되었습니다. 결과 옵션 값은 다음과 같습니다.

```
REVERSE_URL=ldap:///SV?$N?sub?$R
```

항상 그랬던 것처럼 local.imta.schematag는 쉽표로 구분된 목록이 될 수 있습니다. 둘 이상의 스키마가 지원될 경우 중복 항목이 제거된 결합된 속성 목록이 사용됩니다.

또한 이 필터는 원래 제공되었던 주소뿐만 아니라 로컬 부분이 동일하지만 실제로 도메인 트리에서 발견된 도메인(198페이지의 단계 2에서 저장)을 가진 주소를 검색합니다. 도메인 트리 조회의 반복 특성은 두 개의 주소가 다를 수 있다는 것을 의미합니다.

예를 들어, 도메인 siroe.com이 도메인 트리에 표시되며 MTA가 다음 주소를 찾는다고 가정해 봅시다.

```
u@host1.siroe.com
```

\$R 및 ims50 schematag의 확장 결과로 얻어지는 필터는 다음과 같습니다.

```
(|(mail=u@siroe.com)
(mail=u@host1.siroe.com)
(mailAlternateAddress=u@siroe.com)
(mailAlternateAddress=u@host1.siroe.com)
(mailEquivalentAddress=u@siroe.com)
(mailEquivalentAddress=u@host1.siroe.com))
```

역방향 URL이 정규화된 주소를 포함하는 속성을 명시적으로 지정한다는 것에 주의합니다. 일반적으로 이 속성은 메일 속성입니다.

URL이 생성된 후 LDAP 검색이 수행됩니다. 검색이 성공적이면 반환된 첫 번째 속성 값이 원래 주소를 대체합니다. 검색에 실패하거나 오류가 발생하면 원래 주소가 변경되지 않습니다.

주소 역방향 작업이 수행되는 빈도(특히 메일 헤더에 표시될 수 있는 주소 수가 지정된 경우)와 관련 디렉토리 쿼리의 비용으로 인해 부정적 및 긍정적 결과를 모두 캐시해야 합니다. 이 작업은 동적으로 확장되는 메모리 내장의 개방형 체인 해시 테이블을 통해 구현됩니다. 캐시의 최대 크기는 REVERSE\_ADDRESS\_CACHE\_SIZE MTA 옵션(기본값 100000)으로 설정하며 캐시의 항목에 대한 시간 초과는 REVERSE\_ADDRESS\_CACHE\_TIMEOUT MTA 옵션(기본값 600초)으로 설정합니다. 캐시는 실제로 LDAP URL 및 LDAP 결과가 아니라 주소 자체를 저장합니다.

## 비동기 LDAP 작업

비동기 조회는 경우에 따라 성능 문제를 야기할 수 있는 큰 LDAP 결과 전체를 메모리에 저장할 필요가 없게 만듭니다. MTA는 MTA에 의한 다양한 유형의 조회를 비동기식으로 수행하는 기능을 제공합니다.

비동기 LDAP 조회의 사용은 LDAP\_USE\_ASYNC MTA 옵션에 의해 제어됩니다. 이 옵션은 비트 인코딩 값입니다. 각 비트는 설정된 경우 MTA 내의 특정 LDAP 사용과 함께 비동기 LDAP 조회 사용을 활성화합니다.

표 9-11에서는 option.dat 파일의 LDAP\_USE\_ASYNC MTA 옵션에 대한 비트 및 값 설정을 보여 줍니다.

**표 9-11** LDAP\_USE\_ASYNC MTA 옵션에 대한 설정

| 비트 | 값    | 특정 LDAP 사용                                                                                 |
|----|------|--------------------------------------------------------------------------------------------|
| 0  | 1    | LDAP_GROUP_URL1(mgrpDeliverTo) URL                                                         |
| 1  | 2    | LDAP_GROUP_URL2(memberURL) URL                                                             |
| 2  | 4    | LDAP_GROUP_DN(UniqueMember) DNS                                                            |
| 3  | 8    | auth_list, moderator_list, sasl_auth_list 및 sasl_moderator_list nonpositional 목록 매개 변수 URL |
| 4  | 16   | cant_list, sasl_cant_list nonpositional 목록 매개 변수 URL                                       |
| 5  | 32   | originator_reply nonpositional 목록 매개 변수 URL                                                |
| 6  | 64   | deferred_list, direct_list, hold_list, nohold_list nonpositional 목록 매개 변수 URL              |
| 7  | 128  | username_auth_list, username_moderator_list, username_cant_list nonpositional 목록 매개 변수 URL |
| 8  | 256  | 별칭 파일 목록 URL                                                                               |
| 9  | 512  | 별칭 데이터베이스 목록 URL                                                                           |
| 10 | 1024 | LDAP_CANT_URL(mgrpDisallowedBroadcaster) 외부 수준 URL                                         |
| 11 | 2048 | LDAP_CANT_URL 내부 수준 URL                                                                    |

**표 9-11** LDAP\_USE\_ASYNC MTA 옵션에 대한 설정 (계속)

| 비트 | 값     | 특정 LDAP 사용                                      |
|----|-------|-------------------------------------------------|
| 12 | 4096  | LDAP_AUTH_URL(mgrpAllowedBroadcaster) 외부 수준 URL |
| 13 | 8192  | LDAP_AUTH_URL 내부 수준 URL                         |
| 14 | 16384 | LDAP_MODERATOR_URL(mgrpModerator) URLs          |

LDAP\_USE\_ASYNC MTA 옵션의 기본값은 0이며 이것은 비동기 LDAP 조회가 기본적으로 비활성화된다는 것을 의미합니다.

## 설정 요약

Direct LDAP를 활성화하려면 다음 MAT 옵션을 설정해야 합니다.

```
ALIAS_MAGIC=8764
ALIAS_URL0=ldap:/// $V?*?sub?$R
USE_REVERSE_DATABASE=4
USE_DOMAIN_DATABASE=0
REVERSE_URL=ldap:/// $V?mail?sub?$Q
```

부속 도메인을 지원하려는 경우 다음 추가 옵션을 설정해야 합니다.

```
DOMAIN_MATCH_URL=ldap:/// $B?msgVanityDomain?sub?(msgVanityDomain=$D)
ALIAS_URL1=ldap:/// $B?*?sub? (&(msgVanityDomain=$D) $R)
ALIAS_URL2=ldap:/// $1V?*?sub?(mailAlternateAddress=@$D)
```

이러한 옵션의 마지막 부분은 호스트된 도메인과 부속 도메인 모두에서 와일드카드로 지정된 로컬 부분의 대소문자를 처리합니다. 와일드카드로 지정된 로컬 부분에 대한 지원은 필요하지만 부속 도메인 지원이 필요하지 않은 경우에는 다음 옵션을 사용해야 합니다.

```
ALIAS_URL1=ldap:/// $V?*?sub?&(mailAlternateAddress=@$D)
```

filter ssrd:\$A 절을 MTA 구성 파일(imta.cnf)의 ims-ms 채널 정의에서 제거해야 합니다.



## MTA 서비스 및 구성 정보

이 장에서는 일반 MTA 서비스 및 구성에 대해 설명합니다. 더 구체적이고 자세한 설명은 다른 장에서 확인할 수 있습니다. 이 장은 다음 내용으로 구성되어 있습니다.

- 226페이지의 "MTA 구성 컴파일"
- 226페이지의 "MTA 구성 파일"
- 229페이지의 "매핑 파일"
- 243페이지의 "기타 MTA 구성 파일"
- 254페이지의 "별칭"
- 256페이지의 "명령줄 유틸리티"
- 256페이지의 "SMTP 보안 및 액세스 제어"
- 257페이지의 "로그 파일"
- 257페이지의 "주소를 내부 형식에서 공용 형식으로 변환"
- 264페이지의 "전달 상태 알림 메일 제어"
- 277페이지의 "MDN(Message Disposition Notification) 제어"

## MTA 구성 컴파일

`imta.cnf`, `mappings`, `aliases` 또는 `option.dat`와 같은 MTA 구성 파일이 수정될 때마다 구성을 다시 컴파일해야 합니다(*Sun Java System Messaging Server Administration Reference*에서 `imsimta refresh` 명령 참조). 이 명령은 구성 파일을 공유 메모리(UNIX) 또는 동적 링크 라이브러리(NT)의 단일 이미지로 컴파일합니다.

컴파일된 구성은 재로드 가능한 정적 및 동적 부분을 가집니다. 동적 부분이 변경되고 `imsimta reload`를 실행하면 실행 중인 프로그램에서 동적 데이터를 재로드합니다. 동적 부분은 매핑 테이블, 별칭 및 조회 테이블입니다.

구성 정보를 컴파일하는 주된 이유는 성능 때문입니다. 또한 컴파일된 구성이 사용 중일 때 구성 파일 자체가 "live" 상태가 아니므로 컴파일된 구성을 사용하면 구성 변경 사항을 더 편리하게 테스트할 수 있습니다.

MTA의 구성 요소(예: 채널 프로그램)는 구성 파일을 읽어야 할 때마다 컴파일된 구성이 존재하는지 먼저 확인합니다. 컴파일된 구성이 존재할 경우 실행 중인 프로그램에 이미지가 추가됩니다. 이미지 추가 작업이 실패할 경우 MTA는 텍스트 파일을 읽는 이전의 방법으로 돌아갑니다.

## MTA 구성 파일

주 MTA 구성 파일은 `imta.cnf`입니다. 기본적으로 이 파일은 `msg_svr_base/config/imta.cnf`에 위치합니다. 이 파일은 채널 다시 쓰기 규칙뿐만 아니라 MTA 채널 정의를 포함합니다. 다시 쓰여진 대상 주소와 관련된 채널은 대상 채널이 됩니다. 일반적으로 기본 `imta.cnf`를 사용하면 시스템이 적절하게 작동합니다.

이 절에서는 MTA 구성 파일에 대한 간단한 소개를 제공합니다. MTA 구성 파일을 구성하는 다시 쓰기 규칙과 채널 정의를 구성하는 방법에 대한 자세한 내용은 [11장, "다시 쓰기 규칙 구성"](#) 및 [12장, "채널 정의 구성"](#)을 참조하십시오.

MTA 구성 파일을 수정하여 사이트에서 사용되는 채널을 설정하고 어떤 채널이 다시 쓰기 규칙을 통해 어떤 종류의 주소를 담당하는지 지정합니다. 이 구성 파일은 주소 유형을 적절한 채널과 연관시키는 전송 경로(다시 쓰기 규칙)와 사용 가능한 전송 방법(채널)을 지정하여 전자 메일 시스템의 레이아웃을 설정합니다.

구성 파일은 도메인 다시 쓰기 규칙과 채널 정의의 두 부분으로 구성됩니다. 도메인 다시 쓰기 규칙은 파일에서 앞 부분에 나타나며 빈 행으로 채널 정의와 구분됩니다. 채널 정의는 통틀어서 채널 테이블이라고 합니다. 개별 채널 정의는 채널 블록을 구성합니다.

imta.cnf 구성 파일의 다음 예는 메일을 적절한 채널로 라우팅하는 데 다시 쓰기 규칙이 사용되는 방법을 보여 줍니다. 가능한 한 간단하게 하기 위해 도메인 이름은 사용되지 않았습니다. 다시 규칙은 구성 파일의 상반부에 나타나며 채널 정의는 그 뒤를 이어 구성 파일의 하반부에 나타납니다.

```

! test.cnf - An example configuration file. (1)
!
! This is only an example of a configuration file. It serves
! no useful purpose and should not be used in a real system.
!
! Part I: Rewrite rules
a    $U@a-daemon (2)
b    $U@b-daemon
c    $U%c@b-daemon
d    $U%d@a-daemon
      (3)
! Part II: Channel definitions
l    (4)
local-host

a_channel defragment charset7 usascii (5)
a-daemon

b_channel noreverse notices 1 2 3
b-daemon

</opt/SUNWmsgsr/msg-tango/table/internet.rules (6)

```

다음 목록에는 위 구성 파일의 주요 항목(괄호로 묶인 굵은체의 숫자가 표시된)이 설명되어 있습니다.

1. 느낌표(!)는 주석 행을 포함하는 데 사용됩니다. 느낌표는 첫 번째 열에 표시되어야 합니다. 그 밖의 다른 위치에 표시된 느낌표는 *리터럴* 느낌표로 해석됩니다.

2. 다시 쓰기 규칙은 구성 파일의 상반부에 나타납니다. 다시 쓰기 규칙의 행에는 빈 행이 포함될 수 없습니다. 첫 번째 열에서 느낌표로 시작되는 주석 행은 허용됩니다.
3. 구성 파일에 나타나는 첫 번째 빈 행은 다시 쓰기 섹션의 끝이자 채널 블록의 시작임을 의미합니다. 이러한 정의를 통틀어서 MTA가 사용할 수 있는 채널 및 각 채널과 연관된 이름을 정의하는 *채널 호스트 테이블*이라고 합니다.
4. 처음에 표시되는 채널 블록은 일반적으로 로컬 또는 1 채널입니다. 그런 다음 빈 행으로 각 채널 블록이 서로 분리됩니다. (1 채널 앞에 나타날 수 있는 defaults 채널은 예외입니다.)
5. 일반 채널 정의는 채널 이름(a\_channel), 채널 구성을 정의하는 일부 키워드 (defragment charset7 usascii) 및 *채널 태그*라고도 부르는 라우팅 시스템 (a-daemon)으로 구성됩니다.
6. 구성 파일에는 다른 파일의 내용이 포함될 수 있습니다. 첫 번째 열에 보다 작음(<) 기호가 있을 경우 해당 행의 나머지 부분은 파일 이름으로 간주되며 파일 이름은 항상 절대 및 전체 파일 경로여야 합니다. 이 경우 파일이 열리고 파일의 내용이 해당 지점에서 구성 파일에 결합됩니다. 포함 파일은 최대 3개 수준 깊이까지 중첩될 수 있습니다. 구성 파일이 세계 공용인 것처럼 구성 파일에 포함된 모든 파일도 세계 공용이어야 합니다.

표 10-1에서는 앞의 구성에 의해 일부 예제 주소가 라우팅되는 방법을 보여 줍니다.

**표 10-1** 주소 및 관련 채널

| 주소  | 다음 채널의 대기열에 넣음 |
|-----|----------------|
| u@a | a_channel      |
| u@b | b_channel      |
| u@c | b_channel      |
| u@d | a_channel      |

MTA 구성 파일에 대한 자세한 내용은 189페이지의 "다시 쓰기 규칙", 192페이지의 "채널 정의" 및 11장, "다시 쓰기 규칙 구성"을 참조하십시오.

**주** imta.cnf 파일이 변경될 때마다 MTA 구성을 다시 컴파일해야 합니다. 226페이지의 "MTA 구성 컴파일"을 참조하십시오.

## 매핑 파일

MTA의 구성 요소는 대부분 테이블 조회 지향의 정보를 사용합니다. 이 유형의 테이블은 입력 문자열을 출력 문자열로 변환, 즉 *매핑*하는 데 사용됩니다. *매핑 테이블*이라고 부르는 이러한 테이블은 대개 두 개의 열로 제공됩니다. 첫 번째(왼쪽) 열은 일치시킬 가능한 입력 문자열(패턴)을 제공하며 두 번째(오른쪽) 열은 입력 문자열이 매핑되는 결과 출력 문자열(템플릿)을 제공합니다.

대부분의 MTA 데이터베이스(다른 유형의 MTA 데이터를 포함하는 데이터베이스로서 매핑 테이블과 혼동해서는 안 됨)는 바로 이 테이블 유형의 인스턴스입니다. 그러나 MTA 데이터베이스 파일은 와일드카드 조회 기능을 제공하지 않으므로 와일드카드 일치를 위해 전체 데이터베이스를 스캔해야 한다는 점에서 본질적으로 비효율적입니다.

MTA mappings 파일은 여러 매핑 테이블을 지원합니다. 와일드카드 기능뿐만 아니라 다단계 및 반복 매핑 방법이 제공됩니다. 이 방식은 특히 항목 수가 많을 경우에 데이터베이스를 사용하는 것보다 컴퓨팅 작업이 많이 요구됩니다. 그러나 동일한 데이터베이스에서 대부분의 항목을 불필요하게 만드는 유연성이 있기 때문에 결과적으로 전체 오버헤드가 줄어들 수 있습니다.

매핑 테이블은 MTA mappings 파일에 저장됩니다. 이 파일은 MTA tailor 파일에서 IMTA\_MAPPING\_FILE 옵션으로 지정되며 기본적으로 *msg\_svr\_base/config/mappings*입니다. mappings 파일의 내용은 재로드 가능한 섹션의 일부로 컴파일된 구성에 통합됩니다(226페이지의 "MTA 구성 컴파일" 참조). mappings 파일은 세계 공용이어야 합니다. 세계 공용 액세스를 허용하지 않을 경우 오류 동작이 발생합니다. mappings 파일이 변경될 때마다 MTA 구성을 다시 컴파일해야 합니다. 226페이지의 "MTA 구성 컴파일"을 참조하십시오.

표 10-2에서는 이 책에서 설명된 매핑 테이블이 나열되어 있습니다.

**표 10-2** Messaging Server 매핑 테이블

| 매핑 테이블             | 페이지 | 설명                                                                                          |
|--------------------|-----|---------------------------------------------------------------------------------------------|
| AUTH_REWRITE       | 352 | 인증 작업(SASL)에서 얻은 주소 지정 정보를 사용하여 헤더 및 봉투 주소를 수정하기 위해 <code>authrewrite</code> 키워드와 함께 사용됩니다. |
| CHARSET-CONVERSION | 430 | 어떤 종류의 채널 간 문자 세트 변환 및 메일 서식 재설정을 수행해야 하는지 지정하는 데 사용됩니다.                                    |
| COMMENT_STRINGS    | 374 | 주소 헤더 주석(괄호로 묶인 문자열)을 수정하는 데 사용됩니다.                                                         |

**표 10-2** Messaging Server 매핑 테이블

| 매핑 테이블                | 페이지 | 설명                                                                         |
|-----------------------|-----|----------------------------------------------------------------------------|
| CONVERSIONS           | 413 | 변환 채널에 대한 메일 트래픽을 선택하는 데 사용됩니다.                                            |
| FORWARD               | 261 | 별칭 파일이나 별칭 데이터베이스를 사용하여 수행하는 것과 비슷한 전달을 수행하는 데 사용됩니다.                      |
| FROM_ACCESS           | 513 | 봉투의 보낸 사람 주소에 기초하여 메일을 필터링하는 데 사용됩니다. To 주소가 부적절한 경우 이 테이블을 사용합니다.         |
| INTERNAL_IP           | 528 | 내부의 시스템과 서버넷을 인식하는 데 사용됩니다.                                                |
| MAIL_ACCESS           | 513 | SEND_ACCESS 및 PORT_ACCESS 테이블에서 발견한 결합된 정보에 기초하여 받는 연결을 차단하는 데 사용됩니다.      |
| NOTIFICATION_LANGUAGE | 264 | 알림 메일을 사용자 정의 또는 현지화하는 데 사용됩니다.                                            |
| ORIG_MAIL_ACCESS      | 513 | ORIG_SEND_ACCESS 및 PORT_ACCESS 테이블에서 발견한 결합된 정보에 기초하여 받는 연결을 차단하는 데 사용됩니다. |
| ORIG_SEND_ACCESS      | 513 | 봉투의 보낸 사람 주소, 봉투의 받는 사람 주소, 소스 및 대상 채널에 기초하여 받는 연결을 차단하는 데 사용됩니다.          |
| PERSONAL_NAMES        | 375 | 개인 이름(꺾쇠로 구분된 주소 앞의 문자열)을 수정하는 데 사용됩니다.                                    |
| PORT_ACCESS           | 513 | IP 번호를 기준으로 받는 연결을 차단하는 데 사용됩니다.                                           |
| REVERSE               | 257 | 주소를 내부 형식에서 공용 광고 형식으로 변환하는 데 사용됩니다.                                       |
| SEND_ACCESS           | 513 | 봉투의 보낸 사람 주소, 봉투의 받는 사람 주소, 소스 및 대상 채널에 기초하여 받는 연결을 차단하는 데 사용됩니다.          |
| SMS_Channel_TEXT      | 881 | 사이트 정의 텍스트 변환에 사용됩니다.                                                      |
| X-ATT-NAMES           | 421 | 매핑 테이블에서 매개 변수 값을 검색하는 데 사용됩니다.                                            |
| X-REWRITE-SMS-ADDRESS | 880 | 로컬 SMS 주소 유효성 검사에 사용됩니다.                                                   |

## 매핑 파일의 파일 형식

mappings 파일은 일련의 개별 테이블로 구성됩니다. 각 테이블은 이름으로 시작되며 이름의 첫 번째 열에는 항상 알파벳 문자가 옵니다. 테이블 이름 뒤에는 필수적으로 빈 행이 오고 이어서 테이블의 항목이 나타납니다. 항목은 0개 이상의 들여쓰기 행으로 구성되며 각 항목 행은 하나 이상의 공백 또는 탭으로 구분된 두 개의 열로 구성됩니다. 항목 안의 모든 공백은 \$ 문자를 사용하여 인용해야 합니다. 각 매핑 테이블 이름 뒤와 각 매핑 테이블 사이에 빈 행이 있어야 하며 단일 테이블의 항목 사이에는 빈 행이 표시될 수 없습니다. 주석은 첫 번째 열에서 느낌표(!)로 시작해야 합니다.

결과 형식은 다음과 같이 나타납니다.

|                    |                    |
|--------------------|--------------------|
| <i>TABLE1_NAME</i> |                    |
| <i>pattern1-1</i>  | <i>template1-1</i> |
| <i>pattern1-2</i>  | <i>template1-2</i> |
| <i>pattern1-3</i>  | <i>template1-3</i> |
| .                  | .                  |
| .                  | .                  |
| <i>pattern1-n</i>  | <i>template1-n</i> |
| <i>TABLE2_NAME</i> |                    |
| <i>pattern2-1</i>  | <i>template2-1</i> |
| <i>pattern2-2</i>  | <i>template2-2</i> |
| <i>pattern2-3</i>  | <i>template2-3</i> |
| .                  | .                  |
| .                  | .                  |
| <i>pattern2-n</i>  | <i>template2-n</i> |
| .                  | .                  |
| .                  | .                  |
| <i>TABLE3_NAME</i> |                    |
| .                  | .                  |
| .                  | .                  |
| .                  | .                  |

매핑 테이블 *TABLE2\_NAME*을 사용하는 응용 프로그램은 *pattern2-2* 문자열을 *template2-2*에 지정된 것으로 매핑합니다. 각 패턴이나 템플릿은 최대 252자를 포함할 수 있습니다. 과도한 수의 항목이 막대한 양의 CPU와 메모리를 소비할 수 있지만 매핑에 표시될 수 있는 항목 수에는 제한이 없습니다. 252자를 초과하는 긴 행은 끝에 백슬래시를 포함하여 계속 이어질 수 있습니다. 두 열 사이의 공백과 첫 번째 열 앞에 있는 공백은 생략할 수 없습니다.

중복된 매핑 테이블 이름은 *mappings* 파일에서 허용되지 않습니다.

## 매핑 파일에 다른 파일 포함

mappings 파일에 다른 파일이 포함될 수 있습니다. 이렇게 하려면 다음 형식의 행을 사용합니다.

```
<file-spec
```

이 행을 사용하면 포함이 나타나는 지점에서 file-spec 파일의 내용이 mappings 파일에 포함됩니다. 파일 지정은 전체 파일 경로(디렉토리 등)를 지정해야 합니다. 이 방식으로 포함된 모든 파일은 세계 공용이어야 합니다. 또한 이러한 포함된 mappings 파일에는 주석이 허용됩니다. 포함은 최대 3개 수준 깊이까지 중첩될 수 있습니다. 포함 파일은 mappings 파일이 로드될 때 동시에 로드됩니다. 즉, 포함 파일은 요청 시 로드되지 않으므로 포함 파일 사용과 관련하여 성능 또는 메모리가 절약되지는 않습니다.

## 매핑 작업

mappings 파일의 모든 매핑은 일관된 방식으로 적용됩니다. 특정 매핑과 다음 매핑 사이에서 변경되는 유일한 사항은 입력 문자열의 소스와 매핑 출력이 사용되는 대상입니다.

매핑 작업은 항상 입력 문자열과 매핑 테이블로부터 시작됩니다. 매핑 테이블의 항목은 테이블에 표시된 순서대로 위에서 아래로 한 번에 하나씩 스캔됩니다. 각 항목의 왼쪽은 패턴으로 사용되며 입력 문자열은 대소문자를 구분하지 않는 방식으로 해당 패턴과 비교됩니다.

## 매핑 항목 패턴

패턴은 와일드카드 문자를 포함할 수 있습니다. 특히 일반적인 와일드카드 문자가 허용됩니다. 별표(\*)는 0개 이상의 문자와 일치하며 각 백분율 기호(%)는 하나의 문자와 일치합니다. 별표, 백분율 기호, 공백 및 탭은 앞에 달러 기호(\$)를 추가하여 인용할 수 있습니다. 별표 또는 백분율 기호를 인용하면 특별한 의미가 사라집니다. 영구적으로 패턴이나 템플릿으로 끝나는 것을 방지하기 위해 공백과 탭을 인용해야 합니다. 리터럴 달러 기호 문자는 이중(\$\$)으로 표시해야 하며 첫 번째 달러 기호가 두 번째 기호를 인용합니다.

**표 10-3** 매핑 패턴 와일드카드

| 와일드카드 | 설명                                        |
|-------|-------------------------------------------|
| %     | 정확하게 하나의 문자와 일치합니다.                       |
| *     | 왼쪽에서 오른쪽으로의 최대 일치를 사용하여 0개 이상의 문자와 일치합니다. |



**표 10-3** 매핑 패턴 와일드카드(계속)

| 뒤로 일치                                                 | 설명                                                                    |
|-------------------------------------------------------|-----------------------------------------------------------------------|
| \$n*                                                  | n번째 와일드카드 또는 그룹과 일치합니다.                                               |
| <b>수정자</b>                                            | <b>설명</b>                                                             |
| \$_                                                   | 왼쪽에서 오른쪽으로의 최소 일치를 사용합니다.                                             |
| \$@                                                   | 이어지는 와일드카드 또는 그룹의 "저장"을 해제합니다.                                        |
| \$^                                                   | 이어지는 와일드카드 또는 그룹의 "저장"을 설정합니다. 기본값입니다.                                |
| <b>그룹 와일드카드</b>                                       | <b>설명</b>                                                             |
| \$A%                                                  | 하나의 알파벳 문자(A-Z 또는 a-z)와 일치합니다.                                        |
| \$A*                                                  | 0개 이상의 알파벳 문자(A-Z 또는 a-z)와 일치합니다.                                     |
| \$B%                                                  | 하나의 이진수(0 또는 1)와 일치합니다.                                               |
| \$B*                                                  | 0개 이상의 이진수(0 또는 1)와 일치합니다.                                            |
| \$D%                                                  | 하나의 십진수(0-9)와 일치합니다.                                                  |
| \$D*                                                  | 0개 이상의 십진수(0-9)와 일치합니다.                                               |
| \$H%                                                  | 하나의 16진수(0-9 또는 A-F)와 일치합니다.                                          |
| \$H*                                                  | 0개 이상의 16진수(0-9 또는 A-F)와 일치합니다.                                       |
| \$O%                                                  | 하나의 8진수(0-7)와 일치합니다.                                                  |
| \$O*                                                  | 0개 이상의 8진수(0-7)와 일치합니다.                                               |
| \$S%                                                  | 하나의 기호 집합 문자(예: 0-9, A-Z, a-z, _, \$)와 일치합니다.                         |
| \$S*                                                  | 0개 이상의 기호 집합 문자(예: 0-9, A-Z, a-z, _, \$)와 일치합니다.                      |
| \$T%                                                  | 하나의 탭 또는 세로 탭이나 공백 문자와 일치합니다.                                         |
| \$T*                                                  | 0개 이상의 탭 또는 세로 탭이나 공백 문자와 일치합니다.                                      |
| \$X%                                                  | \$H%의 동의어입니다.                                                         |
| \$X*                                                  | \$H*의 동의어입니다.                                                         |
| \$[c]%                                                | 문자 c와 일치합니다.                                                          |
| \$[c]*                                                | 문자 c의 모든 경우와 일치합니다.                                                   |
| \$[c <sub>1</sub> c <sub>2</sub> ...c <sub>n</sub> ]% | 문자 c <sub>1</sub> , c <sub>2</sub> 또는 c <sub>n</sub> 과 정확하게 한번 일치합니다. |
| \$[c <sub>1</sub> c <sub>2</sub> ...c <sub>n</sub> ]* | 문자 c <sub>1</sub> , c <sub>2</sub> 또는 c <sub>n</sub> 의 모든 경우와 일치합니다.  |
| \$[c <sub>1</sub> -c <sub>n</sub> ]%                  | c <sub>1</sub> 에서 c <sub>n</sub> 범위에 있는 문자 하나와 일치합니다.                 |
| \$[c <sub>1</sub> -c <sub>n</sub> ]*                  | c <sub>1</sub> 에서 c <sub>n</sub> 범위에 있는 모든 문자와 일치합니다.                 |
| \$<IPv4>                                              | IPv4 주소와 일치하며 비트를 무시합니다.                                              |
| \$(IPv4)                                              | IPv4 주소와 일치하며 접두어 비트를 유지합니다.                                          |

|                       |                 |
|-----------------------|-----------------|
| <b>표 10-3</b>         | 매핑 패턴 와일드카드(계속) |
| <code>\$(IPv6)</code> | IPv6 주소와 일치합니다. |

그룹 내에서, 즉 `$[...]` 구조 내에서 백슬래시 문자 `\`는 인용 문자입니다. 그룹 내에서 리터럴 하이픈(-) 또는 오른쪽 대괄호(])를 나타내려면 하이픈이나 오른쪽 대괄호를 백슬래시로 인용해야 합니다.

패턴의 다른 모든 문자는 해당 문자 자체를 표시 및 일치시킵니다. 특히 작은따옴표 및 큰따옴표 문자와 괄호는 매핑 패턴이나 템플릿에서 특별한 의미가 없는 보통 문자에 불과합니다. 따라서 유효하지 않은 주소나 부분 주소에 해당하는 항목을 쉽게 작성할 수 있습니다.

여러 수정자를 지정하거나 수정자와 뒤로 일치를 지정하려면 단지 하나의 달러 기호가 구문에 사용됩니다. 예를 들어, 뒤로 일치 자체를 저장하지 않고 처음 와일드카드를 뒤로 일치시키려면 `$$0`이 아니라 `$@0`을 사용합니다.

`imsimta test -match` 유틸리티를 사용하여 매핑 패턴을 테스트하고 특히 패턴에서의 와일드카드 동작을 테스트할 수 있다는 점을 유의하십시오.

별표 와일드카드는 패턴의 왼쪽에서 오른쪽으로 작동하여 항목을 최대한 일치시킵니다. 예를 들어, 문자열 `a/b/c`가 패턴 `*/*`와 비교되면 왼쪽 별표는 `a/b`와 일치하고 오른쪽 별표는 나머지 `c`와 일치합니다.

`_` 수정자는 패턴에서 왼쪽에서 오른쪽으로 작동하여 와일드카드 일치를 최소화하므로 최소한의 가능한 일치만 일치로 간주됩니다. 예를 들어, 문자열 `a/b/c`가 패턴 `$_*/$_*`와 비교되면 왼쪽 `$_*`는 `a`와 일치하고 오른쪽 `$_*`는 `b/c`와 일치합니다.

### IP 일치

IPv4 접두어 일치의 경우 IP 주소나 서브넷이 지정되며 선택적으로 슬래시와 접두어의 비트 수(일치하는 항목을 비교할 때 고려되는)가 뒤에 올 수 있습니다. 예를 들어, 다음은 `123.45.67.0` 서브넷의 모든 항목과 일치합니다.

```
$(123.45.67.0/24)
```

IPv4 무시 비트 일치의 경우 IP 주소나 서브넷이 지정되며 선택적으로 슬래시와 비트 수(일치하는 항목을 검사할 때 무시되는)가 뒤에 올 수 있습니다. 예를 들어, 다음은 `123.45.67.0` 서브넷의 모든 항목과 일치합니다.

```
$<123.45.67.0/8>
```

다음 예는 `123.45.67.4`에서 `123.45.67.7`까지의 범위에 속한 모든 항목과 일치합니다.

<123.45.67.4/2>

IPv6 일치는 IPv6 주소 또는 서브넷과 일치합니다.

### 매핑 항목 템플리트

주어진 항목의 패턴 비교에 실패할 경우 어떠한 작업도 수행되지 않으며 다음 항목의 스캔이 진행됩니다. 비교에 성공할 경우 항목의 오른쪽이 출력 문자열을 생성하기 위한 템플리트로 사용됩니다. 템플리트가 사용되면 입력 문자열은 템플리트에 제공된 지침으로부터 생성된 출력 문자열로 효과적으로 대체됩니다.

템플리트의 거의 모든 문자는 단순히 그대로 출력됩니다. 단, 달러 기호(\$)의 경우는 예외입니다.

달러 기호 뒤에 달러 기호, 공백 또는 탭이 오면 출력 문자열에 달러 기호, 공백 또는 탭이 생성됩니다. 이러한 문자는 모두 출력 문자열에 삽입하기 위해 인용해야 한다는 점을 유의하십시오.

달러 기호 뒤에 오는 숫자  $n$ 은 대체를 요청하며 달러 기호 뒤에 알파벳 문자는 "메타 문자"라고 부릅니다. 메타 문자 자체는 템플리트가 생성한 출력 문자열에 나타나지 않지만 특수한 일부 대체 또는 처리를 생성합니다. 특수한 대체 또는 표준 처리 메타 문자의 목록은 [표 10-4](#)를 참조하십시오. 그 밖의 다른 메타 문자는 매핑 특정 응용 프로그램용으로 예약됩니다.

\$C, \$E, \$L 또는 \$R 메타 문자는 일치하는 패턴의 템플리트에 존재할 경우 매핑 프로세스에 영향을 주고 프로세스의 계속 또는 종료를 제어한다는 점을 유의하십시오. 즉, 한 항목의 출력이 다른 항목의 입력이 되는 반복 매핑 테이블 항목을 설정할 수 있습니다. 일치하는 패턴의 템플리트가 \$C, \$E, \$L 또는 \$R 메타 문자를 포함하지 않을 경우 \$E(매핑 프로세스의 즉시 종료)가 가정됩니다.

무한 루프를 방지하기 위해 매핑 테이블의 반복 통과 횟수가 제한됩니다. 이전 통과보다 길거나 같은 패턴으로 통과가 다시 시작될 때마다 카운터가 증가합니다. 문자열의 길이가 이전 것보다 짧을 경우 카운터는 0으로 재설정됩니다. 카운터가 10을 초과하면 매핑을 반복하려는 요청은 무시됩니다.

**표 10-4** 매핑 템플리트 대체 및 메타 문자

| 대체 시퀀스  | 대체 대상                                   |
|---------|-----------------------------------------|
| \$n     | 0부터 시작하여 왼쪽에서 오른쪽으로 계산된 $n$ 번째 와일드카드 필드 |
| \$#...# | 일련 번호 대체                                |
| \$]...[ | LDAP 검색 URL 조회(결과에서 대체)                 |

**표 10-4** 매핑 템플릿 대체 및 메타 문자 (계속)

| 대체 시퀀스                | 대체 대상                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| \$ ...                | 지정된 매핑 테이블을 제공된 문자열에 적용                                                                                                                                                                                                                                                                                                                                                                                                                |
| \${...}               | 일반 데이터베이스 대체                                                                                                                                                                                                                                                                                                                                                                                                                           |
| }\${domain,attribute{ | <p>도메인별 속성에 액세스하는 기능을 추가합니다. <i>domain</i>은 해당 도메인이고 <i>attribute</i>는 도메인과 연관된 속성입니다. 도메인이 있고 속성을 가지고 있는 경우 초기 값이 매핑 결과로 대체됩니다. 하지만 속성이나 도메인이 없으면 매핑 항목이 실패합니다.</p> <p><i>attributes</i>는 도메인 LDAP 속성이거나 아래에 정의되어 있는 특수한 속성일 수 있습니다.</p> <p><i>_base_dn_</i> - 도메인의 사용자 항목에 대한 기본 DN</p> <p><i>_domain_dn_</i> - 도메인 항목의 DN 그 자체</p> <p><i>_domain_name_</i> - 도메인의 이름(별칭의 반대 개념)</p> <p><i>_canonical_name_</i> - 도메인과 관련된 정규 이름</p> |
| \$[...]               | 사이트 제공 루틴 호출(결과에서 대체)                                                                                                                                                                                                                                                                                                                                                                                                                  |
| 메타 문자                 | 설명                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| \$C                   | 다음 테이블 항목에서 시작하는 매핑 프로세스를 계속합니다. 이 항목의 출력 문자열을 매핑 프로세스의 새 입력 문자열로 사용합니다.                                                                                                                                                                                                                                                                                                                                                               |
| \$E                   | 지금 매핑 프로세스를 종료합니다. 이 항목의 출력 문자열을 매핑 프로세스의 최종 결과로 사용합니다.                                                                                                                                                                                                                                                                                                                                                                                |
| \$L                   | 다음 테이블 항목에서 시작하는 매핑 프로세스를 계속합니다. 이 항목의 출력 문자열을 매핑 프로세스의 새 입력 문자열로 사용합니다. 테이블의 모든 항목이 사용되고 나면 첫 번째 테이블 항목에서 시작하는 통과를 하나 더 만듭니다. 이후의 일치하는 항목에서는 \$C, \$E 또는 \$R 메타 문자를 사용하여 이 조건을 무시할 수 있습니다.                                                                                                                                                                                                                                            |
| \$R                   | 매핑 테이블의 첫 번째 항목에서 시작하는 매핑 프로세스를 계속합니다. 이 항목의 출력 문자열을 매핑 프로세스의 새 입력 문자열로 사용합니다.                                                                                                                                                                                                                                                                                                                                                         |
| \$nA                  | 위치 0에서 시작하여 현재 주소의 n번째 왼쪽 문자를 삽입합니다. n을 생략하면 전체 주소가 삽입됩니다.                                                                                                                                                                                                                                                                                                                                                                             |
| \$nX                  | 0에서 시작하여 메일 호스트의 n번째 왼쪽 구성 요소를 삽입합니다. n을 생략하면 전체 메일 호스트가 삽입됩니다.                                                                                                                                                                                                                                                                                                                                                                        |
| \$?x?                 | 매핑 항목이 x%의 시간 동안 성공합니다.                                                                                                                                                                                                                                                                                                                                                                                                                |
| \$\                   | 후속 텍스트를 소문자로 강제합니다.                                                                                                                                                                                                                                                                                                                                                                                                                    |
| \$\$                  | 후속 텍스트를 대문자로 강제합니다.                                                                                                                                                                                                                                                                                                                                                                                                                    |
| \$_                   | 후속 텍스트를 원래 대소문자로 유지합니다.                                                                                                                                                                                                                                                                                                                                                                                                                |

**표 10-4** 매핑 템플릿 대체 및 메타 문자 (계속)

| 대체 시퀀스 | 대체 대상                                                      |
|--------|------------------------------------------------------------|
| \$=    | 대체된 후속 문자가 LDAP 검색 필터에 삽입하기 적합하게 인용되도록 합니다. 모두 대문자로 적용합니다. |
| \$.x   | 지정된 플래그가 설정된 경우에만 일치합니다.                                   |
| \$.x   | 지정된 플래그가 지워진 경우에만 일치합니다.                                   |

**와일드카드 필드 대체(\$n)**

숫자 n이 뒤에 오는 달러 기호는 패턴의 n번째 와일드카드와 일치했던 항목으로 대체됩니다. 와일드카드는 0부터 시작하여 번호가 매겨집니다. 예를 들어, 다음 항목은 입력 문자열 `PSI%A::B`와 일치하며 결과 출력 문자열 `b@a.psi.siroe.com`을 생성합니다.

```
PSI$%*::* $1@$0.psi.siroe.com
```

또한 입력 문자열 `PSI%1234::USER`도 일치하여 `USER@1234.psi.siroe.com`을 결과 문자열로 생성합니다. 입력 문자열 `PSIABC::DEF`는 이 항목의 패턴과 일치하지 않으며 어떤 작업도 발생하지 않습니다. 즉, 이 항목으로부터 출력 문자열이 생성되지 않습니다.

**텍스트 대소문자 제어(\$\, \$^, \$\_)**

메타 문자 `$$`는 후속 텍스트를 소문자로 강제하고 `$$^`는 후속 텍스트를 대문자로 강제하며 `$$_`는 후속 텍스트를 원래 대소문자로 유지합니다. 예를 들어, 이러한 메타 문자는 매핑을 사용하여 대소문자가 중요한 주소를 변환할 경우에 유용할 수 있습니다.

**처리 제어(\$C, \$L, \$R, \$E)**

`$C`, `$L`, `$R` 및 `$E` 메타 문자는 매핑 프로세스의 종료 여부와 종료 시기를 제어하여 매핑 프로세스에 영향을 줍니다. 각 메타 문자는 다음과 같습니다.

- `$C`를 사용하면 매핑 프로세스가 다음 항목에서 계속되며 현재 항목의 출력 문자열이 매핑 프로세스의 새 입력 문자열로 사용됩니다.

- \$L을 사용하면 매핑 프로세스가 다음 항목에서 계속되며 현재 항목의 출력 문자열이 매핑 프로세스의 새 입력 문자열로 사용됩니다. 일치하는 항목이 없을 경우 항목을 하나 더 만들어 첫 번째 테이블 항목에서 시작하는 테이블을 통과하도록 합니다. \$C, \$E 또는 \$R 메타 문자를 가진 이후의 일치하는 항목은 이 조건을 무시합니다.
- \$R을 사용하면 매핑 프로세스가 테이블의 첫 번째 항목에서 계속되며 현재 항목의 출력 문자열이 매핑 프로세스의 새 입력 문자열로 사용됩니다.
- \$E를 사용하면 매핑 프로세스가 종료하며 이 항목의 출력 문자열이 최종 출력이 됩니다. \$E가 기본값입니다.

매핑 테이블 템플리트는 왼쪽에서 오른쪽으로 스캔됩니다. "성공" 또는 "실패"할 수 있는 항목(예: 일반 데이터베이스 대체 또는 임의 값 제어 항목)에 \$C, \$L 또는 \$R 플래그를 설정하려면 해당 항목의 왼쪽에 \$C, \$L 또는 \$R 메타 문자를 추가합니다. 그렇지 않을 경우 항목의 나머지 부분이 실패하면 플래그가 표시되지 않습니다.

### 특수 플래그 검사

일부 매핑 검사에서는 특수한 플래그를 설정합니다. 이러한 플래그를 설정한 다음 \$:, \$; 테스트의 일반 매핑 테이블 기능을 사용하여 플래그의 존재/부재를 테스트할 수 있습니다. \$:x는 플래그 x가 설정된 경우에만 항목이 일치하게 합니다. \$;x는 플래그 x가 없는 경우에만 항목이 일치하게 합니다. 매핑 테이블에 적용될 수 있는 특수 플래그는 해당 매핑 테이블에 대한 설명을 참조하십시오. [514페이지의 표 17-2](#)에서 \$A, \$T, \$S, \$F 및 \$D를 참조하십시오.

플래그 검사가 성공하면 항목이 계속되고 종료되도록 하고 플래그 검사가 실패하면 매핑 프로세스가 계속되도록 하려는 경우 항목에서는 플래그 검사 왼쪽에 \$C 메타 문자를 사용하고 플래그 검사 오른쪽에 \$E 플래그를 사용해야 합니다.

### 임의로 성공 또는 실패하는 항목(\$?x?)

매핑 테이블 항목의 \$?x? 메타 문자를 사용하면 x%의 시간 동안 항목이 "성공"합니다. 나머지 시간에는 항목이 "실패"하며 매핑 항목의 입력에 대한 출력이 변경되지 않은 채로 출력으로 사용됩니다. (매핑에 따라 항목 실패의 결과가 처음에 일치하지 않은 항목과 반드시 같은 것은 아닙니다.) x는 성공 비율을 지정하는 실수여야 합니다.

예를 들어, IP 주소가 123.45.6.78인 시스템이 많은 양의 SMTP 전자 메일을 사이트로 전송하고 있으며 관리자가 그 속도를 줄이려는 경우 다음과 같은 방법으로 PORT\_ACCESS 매핑 테이블을 사용할 수 있습니다. 여기에서 연결 시도의 25%만 허용하고 나머지 75%의 시도를 거부해야 한다고 가정해 봅니다. 다음 PORT\_ACCESS 매핑 테이블은 \$Y(연결 허용)

를 가진 항목이 25%의 시간 동안만 성공하도록 \$?25?를 사용합니다. 나머지 75%의 시간 동안 이 항목이 실패하면 맨 앞의 \$C로 인해 MTA는 다음 항목에서 매핑을 계속합니다. 결과적으로 SMTP 오류가 발생하고 Try again later 메시지가 표시되면서 연결 시도가 거부됩니다.

```

PORT_ACCESS

TCP|*|25|123.45.6.78|*          $C$?25?$Y
TCP|*|25|123.45.6.78|*          $N45s$ 4.40$ Try$ again$ later
    
```

**일련 번호 대체(\$#...#)**

\$#...# 대체는 MTA 시퀀스 파일에 저장된 값을 증가시키고 해당 값을 템플릿으로 대체합니다. 매핑 테이블 출력에 고유한 한정자가 존재하는 것이 바람직한 경우(예: 매핑 테이블을 사용하여 파일 이름을 생성하는 경우) 이 대체를 사용하여 증가하는 고유 문자열을 생성할 수 있습니다.

다음 구문 중 하나를 사용할 수 있습니다.

```
$#seq-file-spec|radix|width|m#
```

```
$#seq-file-spec|radix|width#
```

```
$#seq-file-spec|radix#
```

```
$#seq-file-spec#
```

필수 *seq-file-spec* 인수는 이미 존재하는 MTA 시퀀스 파일에 대한 전체 파일 지정입니다. 선택적 *radix* 및 *width* 인수는 각각 시퀀스 값을 출력하는 데 적용할 기수와 출력할 자릿수를 지정합니다. 기본 기수는 10이며 허용 범위는 -36에서 36까지입니다.

예를 들어, 기수 36은 숫자 0,...,9,A,...,Z로 표현되는 값을 제공합니다. 기본적으로 시퀀스 값은 본래 너비로 인쇄되지만 지정된 너비에 더 많은 자릿수가 요구될 경우 올바른 자릿수가 되도록 출력의 왼쪽 부분이 0으로 채워집니다. 너비가 명시적으로 지정된 경우 기수도 명시적으로 지정되어야 한다는 점을 유의하십시오.

선택적  $m$  인수는 모듈러스입니다. 이 네 번째 인수를 지정하면 삽입되는 값은 파일 `mod m`에서 검색되는 시퀀스 번호입니다. 기본값은 모듈러스 작업을 수행하지 않는 것입니다.

위에서 언급한 것처럼 매핑에서 참조되는 MTA 시퀀스 파일은 이미 존재해야 합니다. MTA 시퀀스 파일을 만들려면 다음 UNIX 명령을 사용합니다.

```
touch seq-file-spec
```

또는

```
cat >seq-file-spec
```

매핑 테이블을 사용하여 액세스하는 일련 번호 파일은 세계 공용일 경우에만 제대로 작동합니다. 또한 이러한 일련 번호 파일을 사용하려면 `imta_tailor` 파일에서 `nobody`로 구성된 MTA 사용자 계정이 있어야 합니다.

### LDAP 쿼리 URL 대체(\$...)

`$(ldap-url [ 형식 ])`의 대체는 특수하게 처리됩니다. `ldap-url`은 LDAP 쿼리 URL로 해석되며 LDAP 쿼리 결과가 대체됩니다. 호스트와 포트가 생략된 표준 LDAP URL이 사용되며 대신 `LDAP_HOST` 및 `LDAP_PORT` 옵션을 사용하여 호스트와 포트를 지정합니다. 즉, LDAP URL은 다음과 같이 지정해야 합니다.

```
ldap:///dn[?attributes[?scope?filter]]
```

여기에서 대괄호 문자 [ 및 ]는 URL의 선택적 부분을 나타냅니다. `dn`은 필수 항목으로서 검색 기준을 지정하는 고유 이름입니다. 선택 항목인 URL의 `attributes`, `scope` 및 `filter` 부분은 반환할 정보를 더 구체화합니다. 즉, `attributes`는 이 LDAP 쿼리와 일치하는 LDAP 디렉토리 항목에서 반환될 속성을 지정합니다. `scope`은 `base`(기본값), `one` 또는 `sub`가 될 수 있습니다. `filter`는 일치하는 항목의 특성을 설명합니다.



특정 LDAP URL 대체 시퀀스를 LDAP 쿼리 URL 내에서 사용할 수 있습니다.

### **매핑 테이블 대체(\$...)**

`$(mapping;argument)` 형식의 대체는 특수하게 처리됩니다. MTA는 MTA mappings 파일에서 *mapping*이라는 보조 매핑 파일을 찾은 후 *argument*를 명명된 이 보조 매핑 테이블에 대한 입력으로 사용합니다. 명명된 보조 매핑 테이블은 존재해야 하며 성공할 경우 해당 출력에서 `$Y` 플래그를 설정해야 합니다. 명명된 보조 매핑 테이블이 존재하지 않거나 `$Y` 플래그를 설정하지 않을 경우 해당 보조 매핑 대체가 실패하고 원래 매핑 항목이 실패로 간주되어 원래 입력 문자열이 출력 문자열로 사용됩니다.

매핑 테이블 대체를 수행하는 매핑 테이블 항목에서 `$C`, `$R` 또는 `$L`과 같은 처리 제어 메타 문자를 사용하려는 경우 매핑 테이블 템플릿에서 매핑 테이블 대체의 왼쪽에 처리 제어 메타 문자를 두어야 한다는 점을 유의하십시오. 그렇지 않을 경우 매핑 테이블 대체가 "실패"하면 처리 제어 메타 문자가 표시되지 않습니다.

### **일반 조회 테이블 또는 데이터베이스 대체(\$...)**

`$(text)` 형식의 대체는 특수하게 처리됩니다. *text* 부분은 일반 조회 테이블이나 데이터베이스에 액세스하기 위한 키로 사용됩니다. 데이터베이스는 `imsimta crdb` 유틸리티를 사용하여 생성합니다. 테이블에서 *text*가 발견될 경우 테이블의 해당 템플릿이 대체됩니다. *text*가 테이블의 항목과 일치하지 않을 경우 입력 문자열이 변경되지 않은 채로 출력 문자열로 사용됩니다.

일반 조회 테이블을 사용하는 중이면 MTA 옵션 `use_text_databases`의 낮은 순서 하위 비트를 설정해야 합니다. 즉 기수로 설정합니다. `imsimta cnbuild`를 사용하여 컴파일 작업을 수행하고 `imsimta reload`를 사용하여 재로드 가능한 데이터를 재로드함으로써 `general.txt`에 대한 변경 사항을 MTA 구성으로 컴파일해야 합니다.

일반 데이터베이스를 사용하는 경우 데이터베이스는 제대로 작동하기 위해 세계 공용이어야 합니다.

일반 테이블 대체를 수행하는 매핑 테이블 항목에서 `$C`, `$R` 또는 `$L`과 같은 처리 제어 메타 문자를 사용하려는 경우 매핑 테이블 템플릿에서 일반 테이블 대체의 왼쪽에 처리 제어 메타 문자를 두어야 합니다. 그렇지 않을 경우 일반 테이블 대체가 "실패"하면 처리 제어 메타 문자가 표시되지 않습니다.

### 사이트 제공 루틴 대체(\$[...])

`$(image, routine, argument)` 형식의 대체는 특수하게 처리됩니다. `image`, `routine`, `argument` 부분은 사용자 제공 루틴을 검색 및 호출하는 데 사용됩니다. UNIX의 런타임에서 MTA는 `dlopen` 및 `dlsym`을 사용하여 공유 라이브러리 `image`에서 `routine` 루틴을 동적으로 로드 및 호출합니다. 이어서 `routine` 루틴은 다음 인수 목록을 가진 함수로 호출됩니다.

```
status = routine (argument, arglength, result, reslength)
```

`argument` 및 `result`는 252바이트 길이의 문자열 버퍼입니다. `argument` 및 `result`는 포인터로 문자열에 전달됩니다(예: C에서는 `char*`로). `arglength` 및 `reslength`는 참조에 의해 전달되는 서명된 정수(Long)입니다. 입력의 경우, `argument`는 매핑 테이블 템플릿의 `argument` 문자열을 포함하고 `arglength`는 해당 문자열의 길이를 포함합니다. 반환 시에 결과 문자열은 `result`에 포함되고 그 길이는 `reslength`에 포함되어야 합니다. 그런 다음 이 결과 문자열은 매핑 테이블 템플릿에서 `$(image, routine, argument)`를 대체합니다. `routine` 루틴은 매핑 테이블 대체가 실패할 경우에는 0을 반환하고 성공할 경우에는 1을 반환해야 합니다. 대체가 실패할 경우 일반적으로 원래 입력 문자열이 그대로 출력 문자열로 사용됩니다.

사이트 제공 루틴 대체를 수행하는 매핑 테이블 항목에서 `$C`, `$R` 또는 `$L`과 같은 제어 메타 문자를 사용하려는 경우 매핑 테이블 템플릿에서 사이트 제공 루틴 대체의 왼쪽에 제어 메타 문자를 두어야 합니다. 그렇지 않을 경우 매핑 테이블 대체가 "실패"하면 제어 메타 문자가 표시되지 않습니다.

사이트 제공 루틴 설명선 기법을 사용하면 MTA의 매핑 프로세스를 모든 종류의 복잡한 방법으로 확장할 수 있습니다. 예를 들어, `PORT_ACCESS` 또는 `ORIG_SEND_ACCESS` 매핑 테이블에서 특정한 유형의 로드 모니터링 서비스를 호출할 수 있으며 결과를 사용하여 연결이나 메일을 수락할지 여부를 결정할 수 있습니다.

사이트 제공 공유 라이브러리 이미지 `image`는 세계 공용이어야 합니다.

### UTF-8 문자열 생성

일반 매핑 테이블 기능의 유니코드 문자 값에서 UTF-8 문자열을 만들 수 있습니다. 유니코드 메타 문자의 순서는 다음 형식으로 나타냅니다.

```
$&A0A0, 20, A1A1&
```

이 형식에서 `A0A0, 20` 및 `A1A1` 위치에 문자가 포함되는 UTF-8 문자열을 만들어냅니다.

## 기타 MTA 구성 파일

imta.cnf 파일 외에 Messaging Server는 MTA 서비스를 구성하는 데 도움이 되는 다른 여러 구성 파일을 제공합니다. 표 10-5에는 이러한 파일이 요약되어 있습니다. imta.cnf, mappings, aliases 또는 option.dat과 같은 MTA 구성 파일을 수정할 때마다 구성을 다시 컴파일해야 한다는 점을 유의하십시오(*Sun Java System Messaging Server Administration Reference*에서 imsimta refresh 명령 참조).

**표 10-5** MTA 구성 파일

| 파일                                               | 설명                                                                                                                                              |
|--------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| 별칭 파일(필수)                                        | 디렉토리에 존재하지 않는 별칭을 구현합니다.<br><code>msg_svr_base/config/aliases</code>                                                                            |
| TCP/IP(SMTP) 채널 옵션 파일<br>(SMTP 옵션 파일이라고도 부<br>름) | 채널 특정 옵션을 설정합니다.<br><code>msg_svr_base/config/channel_option</code>                                                                             |
| 변환 파일                                            | 메일 본문 부분의 변환을 제어하기 위해 변환 채널에 사용됩니다.<br><code>msg_svr_base/config/conversions</code>                                                             |
| 디스패처 구성 파일(필수)                                   | 디스패처를 위한 구성 파일입니다.<br><code>msg_svr_base/config/dispatcher.cnf</code>                                                                           |
| Job Controller 파일(필수)                            | Job Controller에 사용되는 구성 파일입니다.<br><code>/msg_svr_base/config/job_controller.cnf</code>                                                          |
| MTA 구성 파일(필수)                                    | 채널 정의뿐만 아니라 주소 다시 쓰기 및 라우팅에 사용됩니다.<br><code>/msg_svr_base/config/imta.cnf</code>                                                                |
| 매핑 파일(필수)                                        | 매핑 테이블의 저장소입니다.<br><code>/msg_svr_base/config/mappings</code>                                                                                   |
| 옵션 파일                                            | 전역 MTA 옵션 파일입니다.<br><code>/msg_svr_base/config/option.dat</code>                                                                                |
| 조정 파일(필수)                                        | 위치와 일부 조정 매개 변수를 지정하기 위한 파일입니다.<br><code>/msg_svr_base/config/imta_tailor</code>                                                                |
| 일반 조회 테이블(선택 사항)                                 | 일반 조회 기능은 일반 데이터베이스와 동일합니다. 재로드 가능<br>한 컴파일된 구성의 일부입니다.<br><br>위치와 일부 조정 매개 변수를 지정하기 위한 파일입니다.<br><code>/msg_svr_base/config/general.txt</code> |
| 정방향 조회 테이블(선택 사항)                                | To: 주소에 대한 역방향 조회 기능입니다. 정방향 데이터베이스와<br>동일하며 재로드 가능한 컴파일된 구성의 일부입니다.<br><br><code>/msg_svr_base/config/forward.txt</code>                       |

표 10-5 MTA 구성 파일

| 파일                | 설명                                                                                                                   |
|-------------------|----------------------------------------------------------------------------------------------------------------------|
| 역방향 조회 테이블(선택 사항) | From: 주소에 대한 역방향 조회 기능입니다. 역방향 데이터베이스와 동일하며 재로드 가능한 컴파일된 구성의 일부입니다.<br><code>/msg_svr_base/config/reverse.txt</code> |

## 별칭 파일

별칭 파일 `aliases`는 디렉토리에서 설정되지 않은 별칭을 설정합니다. 특히 루트의 주소를 좋은 예로 들 수 있습니다. 이 파일에 설정된 별칭은 디렉토리에 동일한 별칭이 존재할 경우 무시됩니다. 별칭 및 `aliases` 파일에 대한 자세한 내용은 [254페이지의 "별칭"](#)을 참조하십시오.

`aliases` 파일을 변경한 후 MTA를 다시 시작하거나 `imsimta reload` 명령을 실행해야 합니다.

## TCP/IP(SMTP) 채널 옵션 파일

TCP/IP 채널 옵션 파일은 TCP/IP 채널의 다양한 특성을 제어합니다. 채널 옵션 파일은 MTA 구성 디렉토리에 저장하고 `x_option`으로 이름을 지정해야 합니다. 여기서 `x`는 채널의 이름입니다. 예를 들어, `msg_svr_base/config/imta/tcp_local_option`입니다. 자세한 내용은 [334페이지의 "SMTP 채널 옵션 구성"](#)을 참조하십시오. 모든 채널 옵션 키워드와 구문에 대한 전체 정보는 *Messaging Server Reference Manual*을 참조하십시오.

## 변환 파일

변환 파일 `conversions`는 변환 채널이 MTA를 통과하는 메일에 대한 변환을 수행하는 방법을 지정합니다. MTA 트래픽의 모든 하위 집합을 변환하도록 선택할 수 있으며 임의의 프로그램 또는 명령 프로시저 집합을 사용하여 변환 처리를 수행할 수 있습니다. MTA는 각 본문 부분에 대한 적절한 변환을 선택하기 위해 변환 파일을 확인합니다.

이 파일의 구문에 대한 자세한 내용은 [410페이지의 "변환 채널"](#)을 참조하십시오.

## 디스패처 구성 파일

디스패처 구성 파일 `dispatcher.cnf`는 디스패처 구성 정보를 지정합니다. 기본 구성 파일은 설치 시 작성되며 변경 없이 사용할 수 있습니다. 그러나 보안이나 성능상의 이유로 기본 구성 파일을 수정하려는 경우 `dispatcher.cnf` 파일을 편집하여 원하는 사항을 수정할 수 있습니다(이에 대한 개념적 정보는 [187페이지의 "디스패처"](#)를 참조).

디스패처 구성 파일 형식은 다른 MTA 구성 파일의 형식과 비슷합니다. 옵션을 지정하는 행은 다음 형식을 가집니다.

*option=value*

*option*은 옵션의 이름이며 *value*는 옵션이 설정되는 문자열 또는 정수입니다. *option*이 정수 값을 가질 경우 *b%v* 형식의 표기법을 사용하여 기수를 지정할 수 있습니다. 여기에서 *b*는 기수 10으로 표현되는 기수이며 *v*는 기수 *b*로 표현되는 실제 값입니다. 이러한 옵션 지정은 다음 형식의 행을 사용하여 다음 옵션 설정이 적용되는 서비스에 해당하는 섹션으로 그룹화됩니다.

[SERVICE=*service-name*]

*service-name*은 서비스의 이름입니다. 이러한 섹션 태그 앞에 표시되는 초기 옵션 지정은 모든 섹션에 전역적으로 적용됩니다.

다음은 샘플 디스패처 구성 파일(`dispatcher.cnf`)입니다.

```
! The first set of options, listed without a [SERVICE=xxx]
! header, are the default options that will be applied to all
! services.
!
MIN_PROCS=0
MAX_PROCS=5
MIN_CONNS=5
MAX_CONNS=20
MAX_LIFE_TIME=86400
MAX_LIFE_CONNS=100
MAX_SHUTDOWN=2
!
! Define the services available to Dispatcher
!
[SERVICE=SMTP]
PORT=25
IMAGE=msg_svr_base/lib/tcp_smtp_server
LOGFILE=msg_svr_base/log/tcp_smtp_server.log
```

이 파일의 매개 변수에 대한 자세한 내용은 *Messaging Server Reference Manual*을 참조하십시오.

## 매핑 파일

mappings 파일은 MTA가 입력 문자열을 출력 문자열로 매핑하는 방법을 정의합니다.

MTA의 구성 요소는 대부분 테이블 조회 지향 정보를 사용합니다. 일반적으로 이러한 종류의 테이블은 입력 문자열을 출력 문자열로 변환(즉, 매핑)하는 데 사용됩니다. 매핑 테이블이라고 부르는 이러한 테이블은 두 개의 열, 즉 가능한 입력 문자열을 제공하는 첫 번째(왼쪽) 열과 연관된 입력에 대한 결과 출력 문자열을 제공하는 두 번째(오른쪽) 열로 제공됩니다. 대부분의 MTA 데이터베이스는 이러한 매핑 테이블 유형의 인스턴스입니다. 그러나 MTA 데이터베이스 파일은 와일드카드 조회 기능을 제공하지 않으므로 와일드카드 일치를 위해 전체 데이터베이스를 스캔해야 한다는 점에서 본질적으로 비효율적입니다.

mappings 파일은 여러 매핑 테이블을 지원하기 위한 기능을 MTA에 제공합니다. 완전한 와일드카드 기능이 제공되는 것 외에도 다단계 및 반복 매핑 방법을 사용할 수 있습니다. 이 방식은 특히 항목 수가 많은 경우에 데이터베이스를 사용하는 것보다 컴퓨팅 작업이 많이 요구됩니다. 그러나 동일한 데이터베이스에서 대부분의 항목을 불필요하게 만드는 유연성이 있기 때문에 결과적으로 전체 오버헤드가 줄어들 수 있습니다.

imsimta test -mapping 명령을 사용하여 매핑 테이블을 테스트할 수 있습니다. mappings 파일 및 test -mapping 명령의 구문에 대한 자세한 내용은 [229페이지의 "매핑 파일"](#) 및 *Messaging Server Reference Manual*을 참조하십시오.

mappings 파일을 변경한 후 MTA를 다시 시작하거나 imsimta reload 명령을 실행해야 합니다.

## 옵션 파일

옵션 파일 option.dat는 채널 특정 옵션과 달리 전역 MAT 옵션을 지정합니다.

옵션 파일을 사용하면 MTA에 전체적으로 적용되는 다양한 매개 변수의 기본값을 무시할 수 있습니다. 특히 옵션 파일은 구성 및 별칭 파일을 읽어오는 다양한 테이블의 크기를 설정하는 데 사용됩니다. 또한 옵션 파일을 사용하여 MTA가 수락하는 메일의 크기를 제한하고 MTA 구성에 허용되는 채널 수를 지정하며 허용되는 다시 쓰기 규칙 수를 설정하는 등의 작업을 수행할 수 있습니다.

option.dat에서 #, ! 또는 ;으로 시작하는 행은 행이 계속된다는 것을 의미하는 후행 \가 바로 앞 행에 있는 경우에도 주석 행으로 처리됩니다. 이것은 이러한 문자를 포함할 수 있는 긴 옵션(특히 전달 옵션)에서 주의해야 한다는 것을 의미합니다.

일반적으로 # 또는 !로 시작하는 연속 행을 가지는 전달 옵션의 경우 이를 처리할 수 있는 안전하고 간단한 방법이 존재합니다.

옵션 파일의 구문에 대한 자세한 내용은 *Messaging Server Reference Manual*을 참조하십시오.

## 조정 파일

조정 파일 `imta_tailor`는 다양한 MTA 구성 요소의 위치를 설정합니다. MTA가 제대로 작동하려면 `imta_tailor` 파일이 항상 `msg_svr_base/config` 디렉토리에 상주해야 합니다.

이 파일을 편집하여 특정 설치의 변경 사항을 반영할 수 있지만 이렇게 하려면 주의를 기울여야 합니다. 이 파일을 변경한 후에는 MTA를 다시 시작해야 합니다. MTA를 종료한 상태에서 변경을 수행하는 것이 더 바람직합니다.

---

**주**                      꼭 필요한 경우가 아니면 이 파일을 편집해서는 안 됩니다.

---

이 파일에 대한 자세한 내용은 *Messaging Server Reference Manual*을 참조하십시오.

## Job Controller 파일

Job Controller는 메일 전달을 위해 채널 작업을 작성 및 관리합니다. 이러한 채널 작업은 Job Controller 내의 처리 풀 안에서 실행됩니다. 풀은 채널 작업이 실행되는 "장소"로 생각할 수 있습니다. 풀은 작업 세트가 풀 외부의 작업과 자원을 놓고 경쟁하지 않고도 작동할 수 있는 컴퓨팅 영역을 제공합니다(Job Controller의 개념과 채널 키워드 구성에 대한 자세한 내용은 [194페이지의 "Job Controller"](#), [360페이지의 "채널 실행 작업의 처리 풀"](#) 및 [360페이지의 "서비스 작업 제한"](#) 참조).

Job Controller 파일 `job_controller.cnf`는 다음 채널 처리 정보를 지정합니다.

- 다양한 풀을 정의합니다.

- 모든 채널, 마스터 프로그램 이름 및 슬레이브 프로그램 이름(해당 사항이 있을 경우)을 지정합니다.

imta.cnf 파일에서 pool 키워드를 사용하여 job\_controller.cnf에서 정의된 프로세스 풀의 이름을 지정할 수 있습니다. 예를 들어, 샘플 job\_controller.cnf 파일의 다음 단편은 MY\_POOL 풀을 정의합니다.

```
[POOL=MY_POOL]
job_limit = 12
```

샘플 imta.cnf 파일의 다음 단편은 채널 블록에서 MY\_POOL 풀을 지정합니다.

```
channel_x pool MY_POOL
channel_x-daemon
```

기본 풀 구성과 관련된 매개 변수를 수정하거나 추가 풀을 추가하려는 경우 job\_controller.cnf 파일을 편집한 다음 Job Controller를 중지했다가 다시 시작할 수 있습니다.

Job Controller 구성 파일의 첫 번째 풀은 풀 이름을 지정하지 않는 모든 요청에 사용됩니다. MTA 구성 파일(imta.cnf)에 정의된 MTA 채널은 pool 채널 키워드 뒤에 풀 이름을 사용하여 처리 요청을 특정 풀을 향하도록 할 수 있습니다. 풀 이름은 Job Controller 구성의 풀 이름과 일치해야 합니다. Job Controller가 요청된 풀 이름을 인식하지 않을 경우 요청은 무시됩니다.

초기 구성에서는 DEFAULT, LOCAL\_POOL, IMS\_POOL, SMTP\_POOL 풀이 정의됩니다.

## 사용 예

일반적으로 일부 채널의 처리를 다른 채널의 처리와 차별화하려는 경우 추가 풀 정의를 Job Controller 구성에 추가합니다. 또한 다른 특성을 가진 풀을 사용할 수도 있습니다. 예를 들어, 일부 채널에서 처리하도록 허용된 동시 요청의 개수를 제어해야 할 수 있습니다. 이렇게 하려면 작업 제한을 가진 새 풀을 만든 다음 pool 채널 키워드를 사용하여 이러한 채널을 더 적절한 새 풀로 향하게 합니다.

풀 정의 외에도 Job Controller 구성 파일은 각 채널에 대해 Job Controller가 요청을 처리하는 데 사용해야 하는 MTA 채널 및 명령 테이블을 포함합니다. 요청의 두가지 유형은 "마스터"와 "슬레이브"로 한정됩니다. 일반적으로 채널 마스터 프로그램은 채널에 대한 대기열 호출됩니다. 마스터 프로그램은 메일을 대기열에서 제외시킵니다.



슬레이브 프로그램은 채널을 풀하고 해당 채널에 대한 모든 인바운드 메일을 가져오기 위해 호출됩니다. 거의 모든 MTA 채널이 마스터 프로그램을 갖고 있지만 대부분은 경우 슬레이브 프로그램은 갖고 있지 않거나 불필요합니다. 예를 들어, TCP/IP를 통해 SMTP를 처리하는 채널은 슬레이브 프로그램을 사용하지 않는데 이는 임의 SMTP 서버에서 요청할 경우 네트워크 서비스인 SMTP 서버가 받는 SMTP 메일을 수신하기 때문입니다. SMTP 채널의 마스터 프로그램은 MTA의 SMTP 클라이언트입니다.

채널과 관련된 대상 시스템이 한 번에 하나의 메일만 처리할 수 있는 경우 작업 제한이 1인 새로운 유형의 풀을 만들어야 합니다.

```
[POOL=single_job]
job_limit=1
```

이와 달리 대상 시스템에 충분한 병행성이 있을 경우 작업 제한을 더 높은 값으로 설정할 수 있습니다.

**코드 예 10-1**은 샘플 Job Controller 구성 파일을 보여 줍니다. 사용 가능한 옵션은 [표 10-6](#)에 나와 있습니다.

**코드 예 10-1** UNIX의 샘플 Job Controller 구성 파일

```

!MTA Job Controller configuration file
!
!Global defaults
tcp_port=27442          (1)
secret=never mind
slave_command=NULL     (2)
max_life_age=3600     (3)
!
!
!Pool definitions
!
[POOL=DEFAULT]        (4)
job_limit=10         (5)
!
[POOL=LOCAL_POOL]
job_limit=10
!
[POOL=IMS_POOL]
job_limit=1
!
[POOL=SMTP_POOL]
job_limit=1
!
!Channel definitions
!
!
[CHANNEL=1]           (6)
master_command=msg_svr_base/lib/l_master
!
[CHANNEL=ims-ms]
master_command=msg_svr_base/lib/ims_master
!
[CHANNEL=tcp_*]      (7)
anon_host=0
master_command=msg_svr_base/lib/tcp_smtp_client

```

위 예의 괄호로 묶인 굵은체의 숫자가 표시된 주요 항목은 다음과 같습니다.

1. 이 전역 옵션은 Job Controller가 요청을 수신하는 TCP 포트 번호를 정의합니다.

2. 후속 [CHANNEL] 섹션에 대한 기본 SLAVE\_COMMAND를 설정합니다.
3. 후속 [CHANNEL] 섹션에 대한 기본 MAX\_LIFE\_AGE를 설정합니다.
4. 이 [POOL] 섹션은 DEFAULT라는 풀을 정의합니다.
5. 이 풀의 JOB\_LIMIT를 10으로 설정합니다.
6. 이 [CHANNEL] 섹션은 1이라는 UNIX 로컬 채널에 적용됩니다. 이 섹션에 필요한 유일한 정의는 Job Controller가 이 채널을 실행하기 위해 사용하는 master\_command입니다. 채널 이름에 와일드카드가 없기 때문에 채널은 정확하게 일치해야 합니다.
7. 이 [CHANNEL] 섹션은 이름이 tcp\_\*로 시작하는 모든 채널에 적용됩니다. 이 채널 이름은 와일드카드를 포함하므로 이름이 tcp\_\*로 시작하는 모든 채널과 일치합니다.

### 추가 풀을 추가하는 예

Job Controller는 메일 전달을 위해 채널 작업을 작성 및 관리합니다. 이러한 채널 작업은 Job Controller 내의 처리 풀 안에서 실행됩니다. 풀은 채널 작업이 실행되는 "장소"로 생각할 수 있습니다. 풀은 작업 세트가 풀 외부의 작업과 자원을 놓고 경쟁하지 않고도 작동할 수 있는 컴퓨팅 영역을 제공합니다. job\_controller에서 설정된 작업 제한이 해당 풀에만 적용된다는 점을 유의하십시오. 따라서 예를 들어, job\_limit가 10으로 설정된 SMTP\_POOL을 정의할 경우 특정 시점에 10개의 tcp\_smtp 클라이언트 프로세스만 해당 풀에서 실행될 수 있습니다.

경우에 따라서는 추가 tcp\_\* 채널을 만드는 것이 필요할 수 있습니다(예: 특히 느린 메일 사이트를 위한 tcp 채널). 이러한 채널은 다른 풀에서 실행하는 것이 좋습니다. 이는 예를 들어, 10개의 다른 tcp\_\* 채널을 만들어 SMTP\_POOL에서 모두 실행할 경우 특정 시점에 각 tcp\_\* 채널에 대해 하나의 tcp\_smtp 클라이언트만 실행될 수 있기 때문입니다 (job\_limit가 10인 SMTP\_POOL을 정의한 경우에 해당하며 메일이 모든 tcp\_\* 채널을 대상으로 하는지 여부에 따라 달라짐). 시스템의 로드량이 많고 다양한 tcp\_\* 채널로 나가길 기다리는 메일을 모든 대기열이 갖고 있다고 가정하면 이는 비효율적입니다. 이러한 경우에는 경합이 발생하지 않도록 추가 tcp\_\* 채널에 대한 추가 풀을 정의할 수 있습니다.

예를 들어, 다음 tcp\_\* 채널을 설정한다고 가정해 봅니다.

```
tcp_tcp_yahoo smtp mx pool yahoo_pool keyword keyword keyword
tcp-yahoo-daemon

tcp_aol smtp mx keyword keyword keyword pool aol_pool
tcp-aol-daemon

tcp_hotmail smtp mx pool hotmail_pool keyword keyword keyword tcp-hotmail-daemon

...

tcp_sun smtp mx pool sun_pool keyword keyword keyword
tcp-sun-daemon
```

각각의 새 채널에 대해 10개의 tcp\_smtp\_client 프로세스를 추가하기 위해 job\_controller.cnf 파일에 다음을 추가할 수 있습니다.

```
[POOL=yahoo_pool]
job_limit=10

[POOL=aol_pool]
job_limit=10

[POOL=hotmail_pool]
job_limit=10

...

[POOL=sun_pool]
job_limit=10
```

풀에 대한 자세한 내용은 360페이지의 "채널 실행 작업의 처리 풀"을 참조하십시오. Job Controller 파일의 구문에 대한 자세한 내용은 *Messaging Server Reference Manual*을 참조하십시오.

표 10-6 Job Controller 구성 파일 옵션

| 옵션                                     | 설명                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|----------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 일반 옵션                                  | 설명                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <code>INTERFACE_ADDRESS=adapter</code> | Job Controller가 바인드해야 하는 IP 주소 인터페이스를 지정합니다. 지정된 값(어댑터)은 ANY, ALL, LOCALHOST 또는 IP 주소 중 하나가 될 수 있습니다. 기본적으로 Job Controller는 모든 주소에 바인드됩니다(ALL 또는 ANY를 지정하는 것과 동일). <code>INTERFACE_ADDRESS=LOCALHOST</code> 를 지정하면 Job Controller는 로컬 시스템 내의 연결만 수락합니다. 이 경우 Job Controller에 의해 지원되는 시스템 간 작업이 없이 때문에 정상적인 작업에 영향을 주지 않습니다. 그러나 이 지정은 Job Controller의 응답 여부를 HA 에이전트가 검사할 수 있는 HA 환경에서는 적합하지 않을 수 있습니다. Messaging Server가 실행 중인 시스템이 HA 환경에 있으며 "내부 네트워크" 어댑터 및 "외부 네트워크" 어댑터가 사용 중이고 높은 포트 번호에 대한 연결을 방화벽에서 차단할 수 있는지 확실하지 않을 경우, "내부 네트워크" 어댑터의 IP 주소를 지정하는 것을 고려해야 합니다. |
| <code>MAX_MESSAGES=integer</code>      | Job Controller는 메일에 대한 정보를 메모리 내장 구조에서 유지합니다. 대량의 백로그가 작성될 경우에 대비하여 이 구조의 크기를 제한해야 할 수 있습니다. 백로그의 메일 수가 여기에서 지정된 매개 변수를 초과할 경우 후속 메일에 대한 정보를 메모리에 저장되지 않습니다. 메일 메시지는 항상 디스크에 기록되므로 손실되지 않지만 Job Controller가 알고 있는 메일 수가 이 숫자의 절반으로 줄어 들 때까지 메일 전달이 고려되지 않습니다. 이 시점에서 Job Controller는 <code>imsimta cache -sync</code> 명령을 모방하는 대기열 디렉토리의 스캔을 수행합니다.<br><br>기본값은 100000입니다.                                                                                                                                                                                                 |
| <code>SECRET=file_spec</code>          | Job Controller로 보내진 요청을 보호하는 데 사용되는 공유 비밀입니다.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <code>SYNCH_TIME=time_spec</code>      | Job Controller는 가끔씩 디스크상의 대기열 파일을 스캔하여 누락된 파일을 검사합니다. 기본적으로 이 작업은 Job Controller가 시작되고 4시간 후부터 4시간마다 수행됩니다. <code>time_spec</code> 의 형식은 <code>HH:MM/hh:mm</code> 또는 <code>/hh:mm</code> 입니다. 변수 <code>hh:mm</code> 은 이벤트 사이의 간격을 나타내는 시간( <code>h</code> )과 분( <code>m</code> )입니다. 변수 <code>HH:MM</code> 은 이벤트가 처음 발생해야 하는 시간입니다. 예를 들어, <code>15:45/7:15</code> 은 15시 45분에 이벤트를 시작하고 그 이후부터 7시간 15분마다 이벤트를 반복합니다.                                                                                                                                                       |
| <code>TCP_PORT=integer</code>          | Job Controller가 요청 패킷을 수신해야 하는 TCP 포트를 지정합니다. 기본값이 시스템의 다른 TCP 응용 프로그램과 충돌하지 않을 경우 이 옵션을 변경하지 않습니다. 이 옵션을 변경할 경우 MTA 조정 파일 <code>msg_svr_base/config/imta_tailor</code> 에서 해당 <code>IMTA_JBC_SERVICE</code> 옵션을 변경하여 일치시켜야 합니다. <code>TCP_PORT</code> 옵션은 전역적으로 적용되며 <code>[CHANNEL]</code> 또는 <code>[POOL]</code> 섹션에 있을 경우 무시됩니다.                                                                                                                                                                                                                                        |

**표 10-6** Job Controller 구성 파일 옵션(계속)

| 옵션                                    | 설명                                                                                                                                                                                                                                                                                                                                                |
|---------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>풀 옵션</b>                           | <b>설명</b>                                                                                                                                                                                                                                                                                                                                         |
| <code>JOB_LIMIT=integer</code>        | 풀이 동시에(병렬로) 사용할 수 있는 최대 프로세스 수를 지정합니다. <code>JOB_LIMIT</code> 는 각 풀에 개별적으로 적용되므로 작업의 최대 총 개수는 모든 풀의 <code>JOB_LIMIT</code> 매개 변수를 더한 값입니다. 이 옵션은 기본적으로 섹션 외부에 설정된 경우 <code>JOB_LIMIT</code> 를 지정하지 않는 모든 <code>[POOL]</code> 섹션에 사용됩니다. <code>[CHANNEL]</code> 섹션 안에 있을 경우 이 옵션은 무시됩니다.                                                           |
| <b>채널 옵션</b>                          | <b>설명</b>                                                                                                                                                                                                                                                                                                                                         |
| <code>MASTER_COMMAND=file_spec</code> | 채널을 실행하고 해당 채널에 대한 아웃바운드 메일을 대기열에서 제외시키기 위해 Job Controller가 작성한 UNIX 시스템 프로세스에 의해 실행되는 명령의 전체 경로를 지정합니다. 이 옵션은 기본적으로 섹션 외부에 설정된 경우 <code>MASTER_COMMAND</code> 를 지정하지 않는 모든 <code>[CHANNEL]</code> 섹션에 사용됩니다. <code>[POOL]</code> 섹션 안에 있을 경우 이 옵션은 무시됩니다.                                                                                        |
| <code>MAX_LIFE_AGE=integer</code>     | 채널 마스터 작업의 최대 수명 시간을 초 단위로 지정합니다. 채널에 이 매개 변수가 지정되지 않은 경우 전역 기본값이 사용됩니다. 기본값이 지정되지 않은 경우 1800(30분)이 사용됩니다.                                                                                                                                                                                                                                        |
| <code>MAX_LIFE_CONNS=integer</code>   | 최대 수명 매개 변수 외에 메일이 있는지 Job Controller에 물어볼 수 있는 횟수에 따라 채널 마스터 작업의 기대 수명이 제한됩니다. 채널에 이 매개 변수가 지정되지 않은 경우 전역 기본값이 사용됩니다. 기본값이 지정되지 않은 경우 300이 사용됩니다.                                                                                                                                                                                                |
| <code>SLAVE_COMMAND=file_spec</code>  | 채널을 실행하고 해당 채널에 대한 모든 인바운드 메일을 풀하기 위해 Job Controller가 작성한 UNIX 시스템 프로세스에 의해 실행되는 명령의 전체 경로를 지정합니다. 대부분의 MTA 채널은 <code>SLAVE_COMMAND</code> 를 갖지 않습니다. 이러한 경우 예약된 값 <code>NULL</code> 을 지정해야 합니다. 이 옵션은 기본적으로 섹션 외부에 설정된 경우 <code>SLAVE_COMMAND</code> 를 지정하지 않는 모든 <code>[CHANNEL]</code> 섹션에 사용됩니다. <code>[POOL]</code> 섹션 안에 있을 경우 이 옵션은 무시됩니다. |

## 별칭

MTA는 실제 사용자와 반드시 일치할 필요가 없는 로컬 시스템과 연관된 메일함 이름, 즉 **별칭**을 지원하는 기능을 제공합니다. 별칭은 메일 목록 생성, 메일 전달 및 아이디어에 대한 동의어 제공 등에 유용합니다. 별칭 지정이 처리되는 방법에 대한 자세한 내용은 [202 페이지의 "\\$V 메타 문자"](#)를 참조하십시오.

`aliases` 파일 또는 별칭 데이터베이스에 정의되어 있는 이전 스타일의 메일 목록은 이제 `nonpositional [capture]` 매개 변수를 가집니다. `[capture]` 매개 변수가 사용되는 경우, 이 매개 변수는 LDAP의 사용자나 그룹에 적용되는 `LDAP_CAPTURE` 속성에서 지정한 캡처 주소와 같은 의미의 캡처 주소를 지정합니다.

## 별칭 데이터베이스

별칭 데이터베이스 사용은 권장되지 않습니다. 대신, `imsimta reload` 명령을 사용하여 동적으로 재로드할 수 있는 `aliases` 파일을 사용합니다.

MTA는 디렉토리의 정보를 사용하여 별칭 데이터베이스를 만듭니다. 일반 별칭 파일이 참조될 때마다 별칭 데이터베이스가 한 번씩 참조됩니다. 그러나 별칭 데이터베이스는 일반 별칭 파일이 사용되기 전에 검사됩니다. 실제로 별칭 데이터베이스는 별칭 파일을 사용하기 전에 호출되는 일종의 주소 재작성기의 역할을 수행합니다.

---

**주** 데이터베이스 자체 형식은 개인적입니다. 데이터베이스를 직접 편집하려고 해서는 안 되며 필요한 모든 사항을 디렉토리에서 변경합니다.

---

## 별칭 파일

`aliases` 파일은 디렉토리에 설정되지 않은 별칭을 설정하는 데 사용됩니다. 특히 포스트마스터 별칭을 좋은 예로 들 수 있습니다. 이 파일에 설정된 별칭은 디렉토리에 동일한 별칭이 존재할 경우 무시됩니다. `imsimta reload` 명령을 실행하거나 MTA를 다시 시작하여 변경 사항을 활성화할 수 있습니다. 느낌표로 시작되는 모든 행은 주석으로 간주되어 무시됩니다. 또한 빈 행도 무시됩니다.

---

**주** Messaging Server는 주소 역방향 데이터베이스 및 특수한 매핑 테이블과 같은 주소 조작을 위한 다른 기능을 제공합니다. 그러나 최상의 성능을 위해서는 주소 조작을 수행할 수 있을 때마다 다시 쓰기 규칙을 사용하는 것이 좋습니다. [11장, "다시 쓰기 규칙 구성"](#)을 참조하십시오.

---

이 파일의 물리적 행은 1024자로 제한됩니다. 백슬래시(\) 연속 문자를 사용하여 논리적 행을 여러 물리적 행으로 분할할 수 있습니다.

이 파일의 형식은 다음과 같습니다.

```
user@domain: <address> (호스트된 도메인의 사용자인 경우)
```

```
user@domain: <address> (호스트되지 않은 도메인의 사용자인 경우. 예: default-domain)
```

예를 들면 다음과 같습니다.

```
! A /var/mail/ user
inetmail@siroe.com: inetmail@native-daemon

! A message store user
ms_testuser@siroe.com: mstestuser@ims-ms-daemon
```

## 별칭 파일에 다른 파일 포함

주 `aliases` 파일에 다른 파일을 포함할 수 있습니다. 다음 형식의 행은 `file-spec` 파일을 읽도록 MTA에 지시합니다.

```
<file-spec
```

파일 지정은 완전한 파일 경로 지정이어야 하며 파일은 주 `aliases` 파일과 동일한 보호를 가져야 합니다. 예를 들어, 세계 공용이어야 합니다.

포함 파일의 내용은 해당 참조 지점에서 `aliases` 파일에 삽입됩니다. 포함 파일에 대한 참조를 파일의 실제 내용으로 대체하여 동일한 결과를 얻을 수 있습니다. 포함 파일의 형식은 주 `aliases` 파일 자체의 형식과 같습니다. 실제로 포함 파일 자체에 다른 파일이 포함될 수 있습니다. 최대 세 개 수준까지의 포함 파일 중첩이 허용됩니다.

## 명령줄 유틸리티

Messaging Server는 MAT에 대한 다양한 유지 관리, 테스트 및 관리 작업을 수행할 수 있는 여러 명령줄 유틸리티를 제공합니다. 예를 들어, `imsimta cnbuild` 명령을 사용하여 MTA 구성, 별칭, 매핑, 보안, 시스템 전체 필터 및 옵션 파일을 컴파일할 수 있습니다.

MTA command-line utilities에 대한 자세한 내용은 *Messaging Server Reference Manual*을 참조하십시오.

## SMTP 보안 및 액세스 제어

SMTP 보안 및 액세스 제어에 대한 자세한 내용은 17장, "메일 필터링 및 액세스 제어" 및 19장, "보안 및 액세스 제어 구성"을 참조하십시오.



## 로그 파일

모든 MTA 특정 로그 파일은 로그 디렉토리(*msg\_svr\_base/log*)에 저장됩니다. 이 디렉토리는 MTA를 통과하는 메일 트래픽을 설명하는 로그 파일과 특정 마스터 또는 슬레이브 프로그램에 대한 정보를 설명하는 로그 파일을 포함합니다.

MTA 로그 파일에 대한 자세한 내용은 [21장, "로그 관리"](#)를 참조하십시오.

## 주소를 내부 형식에서 공용 형식으로 변환

주소 역방향 데이터베이스(*역방향 데이터베이스*라고도 부름)와 REVERSE 매핑 테이블을 사용하여 주소를 내부 형식에서 공용 광고 형식으로 변환할 수 있습니다. 예를 들어, `uid@mailhost.siroe.com`은 `siroe.com` 도메인 내에서 유효 주소일 수 있지만 외부에 공개하기에는 적합하지 않을 수 있습니다. 이 경우에는 내부 주소 대신에 `firstname.lastname@siroe.com`과 같은 공용 주소를 사용하는 것이 필요합니다.

---

**주** Messaging Server는 `aliases` 파일 및 특수한 매핑 테이블과 같은 주소 조작을 위한 다른 기능을 제공합니다. 그러나 최상의 성능을 위해서는 주소 조작을 수행할 수 있을 때마다 다시 쓰기 규칙을 사용하는 것이 좋습니다. [11장, "다시 쓰기 규칙 구성"](#)을 참조하십시오.

---

역방향 데이터베이스에서 각 사용자의 공용 주소는 디렉토리에 있는 사용자 항목의 `mail` 속성에 의해 지정됩니다. 개인 또는 내부 주소는 `mailAlternativeAddress` 속성에 의해 지정됩니다. 이는 배포 목록의 경우에도 마찬가지입니다.

역방향 데이터베이스는 임의 유효 주소와 이 공용 주소 간의 매핑을 포함합니다. 역방향 데이터베이스는 일반적으로 MTA 데이터베이스 디렉토리에 위치합니다. 역방향 데이터베이스는 `msg_svr_base/config/imta_tailor` 파일에서 `IMTA_REVERSE_DATABASE` 옵션을 사용하여 이름을 지정하는 파일이며 기본적으로 `msg_svr_base/data/db/reversedb.*`입니다.

데이터베이스에서 주소가 발견될 경우 데이터베이스의 해당 오른쪽 부분이 주소로 대체됩니다. 주소가 발견되지 않을 경우 mappings 파일에서 REVERSE라는 매핑 테이블을 찾으려는 시도가 수행됩니다. 테이블이 존재하지 않거나 테이블의 항목이 일치하지 않을 경우 대체가 수행되지 않으며 다시 쓰기가 정상적으로 종료됩니다.

mappings 파일에서 REVERSE 매핑 테이블이 발견되고 주소가 매핑 항목과 일치할 경우 결과 문자열이 주소를 대체합니다(항목에서 \$Y를 지정한 경우). \$N이 지정된 경우에는 매핑 결과가 무시됩니다. 매핑 항목에서 \$Y 외에 \$D가 지정된 경우 결과 문자열은 역방향 데이터베이스에서 한 번 더 실행됩니다. 여기에서 일치하는 항목이 발생하면 데이터베이스의 템플릿이 매핑 결과(즉, 주소)를 대체합니다. 아래에는 일반 REVERSE 매핑 테이블 항목(즉, 모든 채널에 적용되는 항목)의 형식이 나와 있습니다. 플래그는 새 주소의 앞이나 끝에 올 수 있다는 점을 유의하십시오.

```
REVERSE

    OldAddress          $Y[Flags]NewAddress
```

아래에는 *channel-specific* 항목(즉, 특정 채널을 통과하는 메일에서만 발생하는 매핑)의 형식이 나와 있습니다. 채널 특정 항목이 작동하려면 option.dat에서 use\_reverse\_database를 13으로 설정해야 한다는 점을 유의하십시오.

```
REVERSE

    source-channel|destination-channel|OldAddress  $Y[Flags]NewAddress
```

표 10-7은 REVERSE 매핑 테이블 플래그를 보여 줍니다.

**표 10-7** REVERSE 매핑 테이블 플래그

| 플래그 | 설명                         |
|-----|----------------------------|
| \$Y | 출력을 새 주소로 사용합니다.           |
| \$N | 주소가 변경되지 않고 그대로 유지됩니다.     |
| \$D | 역방향 데이터베이스를 통해 출력을 실행합니다.  |
| \$A | 역방향 데이터베이스 항목으로 패턴을 추가합니다. |
| \$F | 정방향 데이터베이스 항목으로 패턴을 추가합니다. |

**표 10-7** REVERSE 매핑 테이블 플래그(계속)

| 플래그    | 설명                |
|--------|-------------------|
| 플래그 비교 | 설명                |
| \$.B   | 헤더(본문) 주소만 일치합니다. |
| \$.E   | 봉투 주소만 일치합니다.     |
| \$.F   | 정방향 지정 주소만 일치합니다. |
| \$.R   | 역방향 지정 주소만 일치합니다. |
| \$.I   | 메일 아이디만 일치합니다.    |

## 주소 역방향 제어 설정

reverse 및 noreverse 채널 키워드와 MTA 옵션 USE\_REVERSE\_DATABASE 및 REVERSE\_ENVELOPE을 사용하여 주소 역방향을 적용할 시기와 방법에 대한 세부 사항을 제어합니다. 기본적으로 주소 역방향 작업은 단지 역방향 지정 주소가 아니라 모든 주소에 적용됩니다.

주소 역방향은 REVERSE\_ENVELOPE 시스템 옵션 값(기본값: 1-on, 0-off)의 설정에 따라서 활성화 또는 비활성화됩니다.

대상 채널의 noreverse는 메일의 주소에 주소 역방향이 적용되지 않도록 지정합니다. reverse는 주소 역방향을 적용하도록 지정합니다. 자세한 내용은 *Sun Java System Messaging Server Administration Reference*를 참조하십시오.

USE\_REVERSE\_DATABASE는 MTA가 주소 역방향 데이터베이스와 REVERSE 매핑을 대체 주소의 소스로 사용하는지 여부를 제어합니다. 값 0은 채널에서 주소 역방향이 사용되지 않는다는 것을 의미합니다. 기본값인 5는 단지 역방향 지정 주소가 아니라 모든 주소(MTA 주소 다시 쓰기 프로세스에 의해 재작성된 후)에 주소 역방향을 적용하도록 지정합니다. 값 13은 단지 역방향 지정 주소가 아니라 reverse 채널 키워드를 가진 주소(MTA 주소 다시 쓰기 프로세스에 의해 재작성된 후)에 주소 역방향을 적용하도록 지정합니다. 더 세부적인 주소 역방향 작업은 USE\_REVERSE\_DATABASE 옵션의 비트 값을 설정하여 지정할 수 있습니다. 자세한 내용은 *Sun Java System Messaging Server Administration Reference*를 참조하십시오.

REVERSE\_ENVELOPE 옵션은 주소 역방향이 메일 헤더 주소뿐만 아니라 봉투의 From 주소에 적용되는지 여부를 제어합니다.

구체적인 효과에 대해서는 *Sun Java System Messaging Server Administration Reference*에서 이러한 옵션과 키워드에 대한 자세한 설명을 참조하십시오.

## 일반 역방향 매핑 예

다음 예는 일반 REVERSE 매핑을 보여 줍니다. 여기에서는 `siroe.com`의 내부 주소가 `user@mailhost.siroe.com` 형식을 가진다고 가정합니다. 그러나 아이디 공간은 `user@host1.siroe.com` 및 `user@host2.siroe.com`이 `siroe.com`의 모든 호스트에 대해 동일한 사용자를 지정하는 것으로 간주됩니다. 다음 REVERSE 매핑은 주소 역방향 데이터베이스와 함께 사용될 수 있습니다.

```
REVERSE
    *@*.siroe.com      $0@siroe.com$Y$D
```

이 예에서 `name@anyhost.siroe.com` 형식의 주소는 `name@siroe.com`으로 변경됩니다. `$D` 메타 문자는 주소 역방향 데이터베이스를 참조하도록 합니다. 주소 역방향 데이터베이스는 다음 형식의 항목을 포함해야 합니다.

```
user@mailhost.siroe.com      first.last@siroe.com
```

## 채널 특정 역방향 매핑 예

기본적으로 주소 역방향 데이터베이스는 라우팅 가능성 범위가 메일 서버 도메인으로 설정된 경우에 사용됩니다. 채널 특정 REVERSE 매핑 테이블 항목의 예는 다음과 같습니다.

```
REVERSE
    tcp_*|tcp_local|binky@macho.siroe.com      $D$YRebecca.Woods@siroe.com
```

이 항목은 `tcp_local`의 대상 채널에서 나가는 `tcp_*` 소스 채널을 가진 모든 메일에 대해 `binky@macho.siroe.com` 형식의 주소를 `Rebecca.Woods@siroe.com`으로 변경하도록 MTA에 지시합니다.

---

**주** 채널 특정 역방향 매핑을 사용하려면 `option.dat`에서 `USE_REVERSE_DATABASE` 옵션을 13(기본값=3)으로 설정해야 합니다.

---

## 정방향 조회 테이블 및 FORWARD 주소 매핑

주소 역방향은 봉투의 To: 주소에 적용되지 않습니다. 이는 메일이 메일 시스템을 통과할 때 봉투의 To: 주소가 계속해서 재작성 및 수정된다는 확실한 이유가 있기 때문입니다. 라우팅의 전체 목표는 봉투의 To: 주소를 점차적으로 시스템 및 메일함 특정 형식으로 변환하는 것입니다. 주소 역방향을 정형화 기능은 전반적으로 봉투의 To: 주소에 적합하지 않습니다.

어떠한 경우든 MTA에서 풍부한 기능을 사용하여 봉투의 To: 주소에 대한 대체를 수행할 수 있습니다. 별칭 파일, 별칭 데이터베이스 및 일반 조회 테이블이 바로 이 기능을 정확하게 제공합니다.

MTA에서는 또한 패턴 기반 전달, 소스 고유 전달 또는 주소 자동 등록과 같은 특수한 전달 목적에 사용되는 정방향 조회 테이블과 FORWARD 매핑을 사용할 수 있습니다. 정방향 조회 테이블과 FORWARD 매핑은 주로 특수한 종류의 주소 전달에 사용하도록 되어 있다는 점을 유의하십시오. 즉, 대부분의 주소 전달은 MTA의 다른 전달 기법 중 하나를 사용할 때 더 효율적으로 수행됩니다.

봉투의 To: 주소에 대한 다양한 대체 기법은 역방향 조회 테이블과 동일한 기능을 제공하지만 역방향 매핑과 동일한 기능에 대해서는 아직 언급된 것이 없습니다. 경우에 따라서는 봉투의 To: 주소에 대한 매핑 기능이 유용하고 바람직할 수 있습니다.

### FORWARD 매핑 테이블

FORWARD 매핑 테이블은 패턴을 기반으로 하는 전달 기능을 제공하며 소스 고유 전달을 위한 기법도 제공합니다. FORWARD 매핑 테이블이 매핑 파일에 있으면 각 봉투의 To: 주소에 적용됩니다. 이 매핑이 존재하지 않거나 매핑의 항목이 일치하지 않을 경우 변경이 수행되지 않습니다.

주소가 매핑 항목과 일치할 경우 매핑 결과가 테스트됩니다. 항목에 \$Y가 지정될 경우 결과 문자열이 봉투의 To: 주소를 대체하며 \$N이 지정될 경우 매핑 결과를 무시합니다. 추가 플래그 목록은 표 10-8을 참조하십시오.

**표 10-8** FORWARD 매핑 테이블 플래그 설명

| 플래그 | 설명                           |
|-----|------------------------------|
| \$D | 다시 쓰기 프로세스를 통해 출력을 다시 실행합니다. |

**표 10-8** FORWARD 매핑 테이블 플래그 설명

| 플래그 | 설명                                                  |
|-----|-----------------------------------------------------|
| \$G | 정방향 조회 테이블을 통해 출력을 실행합니다(정방향 조회 테이블이 사용 가능하게 된 경우). |
| \$H | 추가 정방향 조회 테이블이나 FORWARD 매핑 조회를 사용 불가능하게 합니다.        |
| \$I | 메일을 .HELD 파일로 보관합니다.                                |
| \$N | 주소가 변경되지 않고 그대로 유지됩니다.                              |
| \$Y | 출력을 새 주소로 사용합니다.                                    |

FORWARD 매핑(있을 경우)은 정방향 조회 테이블이 조회되기 전에 참조됩니다. FORWARD 매핑이 일치하고 플래그 \$G가 있을 경우 정방향 조회 테이블에 대해 FORWARD 매핑의 결과가 검사됩니다(USE\_FORWARD\_DATABASE의 적절한 설정을 통해 정방향 조회 테이블이 사용 가능하게 된 경우). 채널 고유 정방향 조회 테이블 사용이 지정된 경우 정방향 조회 테이블에서 조회하기 전에 FORWARD 매핑의 결과에 소스 주소와 소스 채널이 접두어로 추가된다는 점을 유의하십시오. 일치하는 FORWARD 매핑 항목에 \$D가 지정된 경우 FORWARD 매핑의 결과와 선택적 정방향 테이블 조회가 MTA 주소 다시 쓰기 프로세스를 통해 다시 실행됩니다. 일치하는 FORWARD 매핑 항목에 \$H가 지정된 경우 \$D 사용으로 인해 발생하는 후속 주소 다시 쓰기 프로세스 동안에 추가 FORWARD 매핑이나 데이터베이스 조회가 수행되지 않습니다.

아래 예는 복잡한 REVERSE 및 FORWARD 매핑의 사용을 보여 줍니다. 여기에서는 mr\_local 채널과 연관된 am.sigurd.innosoft.com이라는 시스템 또는 의사 도메인이 일반적인 형식의 RFC 822 주소를 생성한다고 가정합니다.

```
"lastname, firstname"@am.sigurd.example.com
```

또는

```
"lastname,firstname"@am.sigurd.example.com
```

이러한 주소는 완전히 유효하지만 RFC 822 구문 규칙을 완벽하게 따르지 않는 전자 메일 프로그램(예: 인용된 주소를 제대로 처리하지 않은 전자 메일 프로그램)에서는 흔히 혼동을 일으킵니다. 결과적으로 인용이 필요하지 않는 주속 형식이 더 많은 전자 메일 프로그램에서 작동합니다. 이러한 형식 중 하나는 다음과 같습니다.

```
firstname.lastname@am.sigurd.example.com
```

## 복잡한 FORWARD 및 REVERSE 매핑 예

## REVERSE

```
* |mr_local| "*", $ "*"@am.sigurd.innosoft.com $Y"$1, $ 2"@am.sigurd.innosoft.com
* |mr_local| "*", "*"@am.sigurd.innosoft.com $Y"$1, $ 2"@am.sigurd.innosoft.com
* |*| "*", $ "*"@am.sigurd.innosoft.com $Y"$3.$2@am.sigurd.innosoft.com
* |*| "*", "*"@am.sigurd.innosoft.com $Y"$3.$2@am.sigurd.innosoft.com
* |mr_local|*.*@am.sigurd.innosoft.com $Y"$2, $ 1"@am.sigurd.innosoft.com
* |*|*.*@am.sigurd.innosoft.com $Y"$2.$3@am.sigurd.innosoft.com
```

## FORWARD

```
"*, $ "*"@am.sigurd.innosoft.com $Y"$0, $ 1"@am.sigurd.innosoft.com
"*,*"@am.sigurd.innosoft.com $Y"$0, $ 1"@am.sigurd.innosoft.com
*.*@am.sigurd.innosoft.com $Y"$1, $ 0"@am.sigurd.innosoft.com
```

따라서 위 예에 나온 샘플 매핑 테이블은 (1) 이러한 세 개의 주소 형식을 모두 사용할 수 있도록 허용하고, (2) 원래 형식의 주소만 `mr_local` 채널에 제공하고 필요에 따라 형식을 변환하며, (3) 인용되지 않은 새 형식의 주소만 다른 모든 채널에 제공하고 필요에 따라 형식을 변환하는 세 가지 목적을 가집니다. (위의 REVERSE 매핑에서는 MTA 옵션 `USE_REVERSE_DATABASE`에 비트 3이 설정되었다고 가정합니다.)

## 정방향 조회 테이블

주소 전달이 자동 등록되거나 소스별로 고유해야 할 경우 정방향 조회 테이블을 사용할 수 있습니다. 간단한 메일 전달에는 일반적으로 정방향 조회 테이블을 사용하는 것이 적합하지 않으며 `aliases` 파일 또는 별칭 조회 테이블이 이러한 전달을 수행하는 데 더 효율적인 방법이라는 점을 유의하십시오. 기본적으로 정방향 조회 테이블은 전혀 사용되지 않으므로 `USE_FORWARD_DATABASE` 옵션을 통해 명시적으로 사용 가능하게 해야 합니다. 정방향 테이블 조회는 주소 다시 쓰기 이후, 별칭 확장이 수행된 후, 그리고 임의의 FORWARD 매핑이 검사된 후에 수행됩니다. 정방향 테이블 조회에 성공할 경우 MTA 주소 다시 쓰기 프로세스를 통해 대체된 결과 주소가 다시 실행됩니다.

정방향 조회 테이블에는 메모리 내장 해시 테이블과 기본 데이터베이스의 두 가지 기법을 사용할 수 있습니다. 테이블의 크기가 너무 크지 않을 경우 해시 테이블이 권장됩니다. (1,000은 너무 큰 것이 아니지만 100,000은 너무 크다고 할 수 있습니다.) 해시 테이블은 `use_text_database` 옵션에서 비트 3(값 34)을 설정하고 `use_forward_database`를 설정하여 활성화합니다.

해시 테이블은 `msg_svr_base/configure/forward.txt`에서 읽어오고 구성의 재로드 가능 부분으로 컴파일되며 `imsimta reload` 명령에 의해 강제로 활성화 MTA 프로세스로 재로드될 수 있습니다.

정방향 데이터베이스는 소스 텍스트 파일에서 `crdb` 유틸리티를 사용하여 만든 MTA `crdb` 데이터베이스입니다. 소스 텍스트 파일의 형식은 기본적으로 다음과 같습니다.

```
user1@domain1    changedmailbox1@changeddomain1
user2@domain2    changedmailbox@changeddomain2
```

그러나 `USE_FORWARD_DATABASE` 옵션의 비트 3을 설정하여 정방향 데이터베이스의 소스별 사용을 가능하게 한 경우 소스 텍스트 파일 형식은 다음과 같습니다.

```
source-channel|source-address|original-address  changed-address
```

예를 들어, 다음과 같은 항목은

```
tcp_limited|bob@blue.com|helen@red.com  "helen of troy"@siroe.com
```

`bob@blue.com`에서 메일이 오고 대기열 넣기 채널이 `tcp_limited`인 경우에만 To: 주소 `helen@red.com`을 "helen of troy" `siroe.com`에 매핑합니다.

## 전달 상태 알림 메일 제어

전달 상태 알림 또는 *상태 알림*은 MTA가 보낸 사람이나 선택적으로 포스트마스터로 보내는 전자 메일 상태 메일입니다. Messaging Server를 사용하면 내용이나 언어별로 알림 메일을 사용자 정의할 수 있습니다. 또한 각 유형의 전달 상태(예: FAILED, BOUNCED, TIMEDOUT 등)에 대해 다른 메일을 만들 수 있습니다. 이외에도 특정 채널에서 보내지는 메일에 대한 상태 알림을 만들 수 있습니다.

기본적으로 상태 알림은 `msg_svr_base/config/locale/C` 디렉토리에 저장됩니다 (`msg_svr_base/config/imta_tailor` 파일의 `IMTA_LANG` 설정에서 지정됨). 파일 이름은 다음과 같습니다.

```
return_bounced.txt, return_delivered.txt return_header.opt,
return_timedout.txt, return_deferred.txt, return_failed.txt,
return_prefix.txt, return_delayed.txt, return_forwarded.txt,
return_suffix.txt.
```



\*.txt 파일의 메일 텍스트는 한 행당 78자로 제한되어야 합니다. Messaging Server를 업그레이드할 때 이러한 파일을 덮어쓰므로 이러한 파일을 직접 변경하면 안 됩니다. 이러한 파일을 수정하고 유일한 알림 메일 템플릿 집합(return\_\*.txt)으로 사용하려면 파일을 새 디렉토리로 복사하여 해당 위치에서 편집합니다. 그런 다음 이러한 템플릿을 포함하는 새 디렉토리를 가리키도록 imta\_tailor 파일에서 IMTA\_LANG 옵션을 설정합니다. 각 언어에 대한 집합이 필요한 경우처럼 여러 집합의 알림 파일을 원할 경우 NOTIFICATION\_LANGUAGE 매핑 테이블을 설정해야 합니다.

## 상태 알림 생성 및 수정

단일 알림 메일은 세 파일 집합 return\_prefix.txt + return\_ActionStatus.txt + return\_suffix.txt로부터 생성됩니다.

알림을 사용자 정의하거나 현지화하려면 각 로캘 및/또는 사용자 정의에 대해 완전한 return\_\*.txt 파일 집합을 만들어서 별도의 디렉토리에 저장합니다. 예를 들어 프랑스어 알림 파일을 한 디렉토리에 저장해 놓고 스페인어 알림 파일을 또 다른 디렉토리에 저장하고 원치 않는 대량 전자 메일 채널에 대한 알림을 다른 디렉토리에 저장할 수 있습니다.

---

**주** 이 릴리스에는 프랑스어, 독일어, 스페인어 샘플 파일이 포함되어 있습니다. 자신의 고유한 요구에 맞도록 이러한 파일을 수정할 수 있습니다.

일본어와 같은 더블바이트 언어의 경우 텍스트를 일본어로 생성한 다음 해당 텍스트를 ASCII인 것처럼 표시하여 % 문자를 검사합니다. % 문자가 잘못 들어가 있을 경우 이를 %%로 대체합니다.

---

상태 알림 메일 집합의 형식과 구조는 다음과 같습니다.

1. return\_prefix.txt는 본문의 소개 부분뿐만 아니라 해당하는 헤더 텍스트를 제공합니다. 미국 영어 로캘에 대한 기본값은 다음과 같습니다.

```
Content-type: text/plain; charset=us-ascii
Content-language: EN-US
```

```
This report relates to a message you sent with the following
header fields: %H
```

미국 ASCII가 아닌 상태 알림 메일의 경우 charset 매개 변수와 Content-Language 헤더 값을 적절하게 변경해야 합니다. 예를 들어, 현지화된 프랑스어 파일의 경우 이러한 값은 ISO-8859-1 및 fr입니다. %H는 [표 10-9](#)에 정의된 헤더 대체 시퀀스입니다.

2. `return_<ActionStatus>.txt`는 상태 특정 텍스트를 포함합니다. *ActionStatus*는 메일의 MTA 상태 유형을 나타냅니다. 예를 들어, `return_failed.txt`의 기본 텍스트는 다음과 같습니다.

```
Your message cannot be delivered to the following recipients:
%R
```

`return_bounced.txt`의 기본 텍스트는 다음과 같습니다.

```
Your message is being returned. It was forced to return by
the postmaster.
```

```
The recipient list for this message was:
%R
```

3. `return_suffix.txt`는 결과 텍스트를 포함합니다. 기본적으로 이 파일은 비어 있습니다.

**표 10-9**      알림 메일 대체 시퀀스

| 대체                                                                           | 정의                                                                                                                                                                                                                                                                                                                                                                                                                          |
|------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| %H                                                                           | 메일의 헤더로 확장됩니다.                                                                                                                                                                                                                                                                                                                                                                                                              |
| %C                                                                           | 메일을 대기열에 포함했던 단위 수 <sup>1</sup> 로 확장됩니다.                                                                                                                                                                                                                                                                                                                                                                                    |
| %L                                                                           | 메일이 반환되기 전에 대기열에 남아 있었던 메일의 단위 수 <sup>1</sup> 로 확장됩니다.                                                                                                                                                                                                                                                                                                                                                                      |
| %F                                                                           | 메일이 대기열에 머무르는 것이 허용되는 단위 수 <sup>1</sup> 로 확장됩니다.                                                                                                                                                                                                                                                                                                                                                                            |
| %S [%s]                                                                      | 이전에 확장된 숫자 값이 1이 아닐 경우 문자 S 또는 s로 확장됩니다. 메일이 대기열에 포함되었던 일 수에 따라 "%C day%s"는 "1 day" 또는 "2 days"로 확장될 수 있습니다.                                                                                                                                                                                                                                                                                                                |
| %U [%u]                                                                      | 사용 중인 시간 단위 <sup>1</sup> Hour [hour] 또는 Day [day]로 확장됩니다. 메일이 대기열에 포함되었던 일 또는 시간과 MTA 옵션 RETURN_UNITS의 값에 따라 "%C %U%s"가 "2 days" 또는 "1 hour"로 확장됩니다. RETURN_UNITS=1(시간)을 설정했으며 사이트에서 현지화된 상태 알림 메일을 사용할 경우 <code>return_delayed.txt</code> 및 <code>return_timedout.txt</code> 를 편집하여 영어가 아닌 모든 언어에 대해 "days" 단어를 hours로 대체해야 합니다. 예를 들어, 프랑스어는 jour(s)를 heure(s)로, 독일어는 Tag(e)를 Stunde(n)로, 스페인어는 día(s)를 hora(s)로 바꿔야 합니다. |
| %R                                                                           | 메일 수신자의 목록으로 확장됩니다.                                                                                                                                                                                                                                                                                                                                                                                                         |
| %%                                                                           | % (텍스트는 문자 세트에 상관 없이 대체 시퀀스에 대해 바이트 단위로 스캔된다는 것에 주의합니다. 더블바이트 문자 세트를 사용하는 중이면 % 기호가 잘못 들어가 있지 않은지 검사합니다.)                                                                                                                                                                                                                                                                                                                   |
| <sup>1</sup> 단위는 MTA 옵션 파일의 RETURN_UNITS 옵션에 의해 정의되며 시간 또는 일(기본값)이 될 수 있습니다. |                                                                                                                                                                                                                                                                                                                                                                                                                             |

## 전달 상태 알림 메일 사용자 정의 및 현지화

전달 상태 알림 메일을 현지화하여 여러 다른 언어로 여러 사용자에게 메일을 반환할 수 있습니다. 예를 들어, 프랑스어를 선호하는 사용자에게 프랑스어 알림을 반환할 수 있습니다.

상태 알림 메일을 현지화 또는 사용자 정의하는 것은 다음 두 단계로 구성됩니다.

1. 현지화된/사용자 정의된 `return_*.txt` 메일 파일 집합을 만들어 각 집합을 별도의 디렉토리에 저장합니다. 이에 대해서는 [265페이지의 "상태 알림 생성 및 수정"](#)에 설명되어 있습니다.
2. `NOTIFICATION_LANGUAGE` 매핑 테이블을 설정합니다.

`msg_svr_base/config/mappings`에 있는 `NOTIFICATION_LANGUAGE` 매핑 테이블은 *원본 메일*(알림을 보내는 원인이 되는 메일)의 속성에 따라 현지화되거나 사용자 정의된 알림 메일 파일을 사용하도록 지정합니다.

상태 알림 유형, 소스 채널, 기본 언어, 반송 주소 및 첫 번째 수신자를 결정하기 위해 원래 보낸 사람의 메일이 구문 분석됩니다. 테이블의 구성 방법에 따라 이러한 속성 중 하나 이상에 기초하여 알림 파일 집합이 선택됩니다.

`NOTIFICATION_LANGUAGE` 매핑 테이블의 형식은 다음과 같습니다.

```
NOTIFICATION_LANGUAGE
```

```
dsn-type-list | source-channel | preferred-language | return-address | first-recipient
$Idirectory-spec
```

`dsn-type-list`는 쉼표로 구분된 전달 상태 알림 유형의 목록입니다. 여러 유형을 지정할 경우 공백 없이 쉼표로 이러한 유형을 구분해야 합니다(공백을 사용할 경우 매핑 테이블 항목의 패턴이 종료됨). 이러한 유형은 다음과 같습니다.

`failed` - 일반 영구 오류 메일(예: 해당 사용자 없음)입니다. `return_failed.txt` 파일이 사용됩니다.

`bounced` - 수동 "바운스"와 함께 사용되는 알림 메일입니다. 포스트마스터에 의해 수행됩니다. `return_bounced.txt` 파일이 사용됩니다.

`timedout` - MTA가 전달이 허용되는 시간 내에 메일을 전달하지 못했습니다. 메일을 반환하고 있습니다. `return_timedout.txt` 파일이 사용됩니다.

`delayed` - MTA가 메일을 전달하지 못했지만 계속해서 전달을 시도할 것입니다. `return_delayed.txt` 파일이 사용됩니다.

`deferred` - "`delayed`"와 비슷한 전달 실패 알림이지만 MTA가 전달 시도를 계속할 시간이 표시되지 않습니다. `return_deferred.txt` 파일이 사용됩니다.

`forwarded` - 메일에 대한 전달 수신 확인이 요청되었지만 이러한 수신 확인을 지원하지 않는 시스템에 메일이 전달되었습니다. `return_forwarded.txt` 파일이 사용됩니다.

`source-channel`은 알림 메일을 생성하는 채널(즉, 메일이 현재 대기열이 포함된 채널)입니다. 예를 들어, 메시지 저장소의 전달 대기열에 대한 `ims-ms`, 아웃바운드 SMTP 대기열에 대한 `tcp_local` 등이 있습니다.

`preferred-language`는 처리할 메일(알림이 생성된 메일)이 표현되는 언어입니다. 이 정보의 소스는 우선적으로 `accept_language` 필드입니다. 해당 필드가 없는 경우 `Preferred-language`: 헤더 필드와 `X-Accept-Language`: 헤더 필드가 사용됩니다. 표준 언어 코드 값의 목록은 `msg_svr_base/config/languages.txt` 파일을 참조하십시오.

이 필드는 비어 있지 않을 경우 `Preferred-language`: 또는 `X-Accept-language`: 헤더 행에 지정된 메일의 메일 발송자가 됩니다. 이에 따라 이 필드에 무의미한 문자가 나타날 수 있습니다.

`return-address`는 원래 메일의 봉투 `From`: 주소입니다. 이 주소는 알림 메일이 보내지는 봉투 주소이므로 사용할 언어를 나타내는 표시 기호일 수 있습니다.

`first-recipient`는 원래 메일을 보내도록 지정된 봉투 `To`: 주소(메일이 여러 수신자에 대해 실패한 경우 첫 번째 주소)입니다. 예를 들어, "our message to dan@siroe.com could not be delivered" 알림에서 보고되는 봉투의 `To`: 주소는 dan@siroe.com입니다.

`directory-spec`은 매핑 테이블 검사가 일치할 경우 사용할 `return_*.txt` 파일을 포함하는 디렉토리입니다. 디렉토리 지정 앞에 `$I`가 와야 한다는 것에 주의합니다.

예를 들어, 프랑스어 알림 파일(return\_\*.txt)을 /lc\_messages/table/notify\_french/ 디렉토리에 저장하고 스페인어 알림 파일을 /lc\_messages/table/notify\_spanish/ 디렉토리의 return\_\*.txt 파일에 저장하는 사이트는 아래와 같은 테이블을 사용할 수 있습니다. 각 항목이 하나 이상의 공백으로 시작해야 하며 항목 간에 빈 행이 올 수 없다는 것에 주의합니다.

**코드 예 10-2**

알림 언어 매핑 테이블—예

```

NOTIFICATION_LANGUAGE

! Preferred-language: header value specified
!
*|*|fr|*|*   $I/lc_messages/table/notify_french/
*|*|es|*|*   $IIMTA_TABLE/notify_spanish/
*|*|en|*|*   $I/imta/lang/
!
! If no Preferred-language value, then select notification based on the
! country code in the domain name. EX: PF=French Polynesia; BO=Bolivia
!
*|*|*|.fr|*   $I/imta/table/notify_french/
*|*|*|.fx|*   $I/imta/table/notify_french/
*|*|*|.pf|*   $I/imta/table/notify_french/
*|*|*|.tf|*   $I/imta/table/notify_french/
*|*|*|.ar|*   $I/imta/table/notify_spanish/
*|*|*|.bo|*   $I/imta/table/notify_spanish/
*|*|*|.cl|*   $I/imta/table/notify_spanish/
*|*|*|.co|*   $I/imta/table/notify_spanish/
*|*|*|.cr|*   $I/imta/table/notify_spanish/
*|*|*|.cu|*   $I/imta/table/notify_spanish/
*|*|*|.ec|*   $I/imta/table/notify_spanish/
*|*|*|.es|*   $I/imta/table/notify_spanish/
*|*|*|.gp|*   $I/imta/table/notify_spanish/
*|*|*|.gt|*   $I/imta/table/notify_spanish/
*|*|*|.gy|*   $I/imta/table/notify_spanish/
*|*|*|.mx|*   $I/imta/table/notify_spanish/
*|*|*|.ni|*   $I/imta/table/notify_spanish/
*|*|*|.pa|*   $I/imta/table/notify_spanish/
*|*|*|.ve|*   $I/imta/table/notify_spanish/

```

---

**주** 알림 언어 매핑이 사용 가능하도록 기본 `mappings.locale` 파일이 설치 시 함께 제공되어 `mappings` 파일에 포함됩니다. 알림 언어 매핑을 사용 불가능하게 하려면 다음과 같이 포함 줄을 주석 처리합니다.

```
! <IMTA_TABLE:mappings.locale
```

(파일에서 주석을 읽은 다음 자신의 요구에 맞게 적절하게 수정합니다.)

---

## 생성된 알림 국제화

DSN(Delivery Status Notification) 및 MDN(Message Disposition Notification)을 위한 두 개의 옵션 파일을 사용할 수 있습니다. 생성된 알림의 국제화를 더 유연하게 수행할 수 있게 하는 이러한 파일은 다음과 같습니다.

```
IMTA_LANG:return_option.dat (DSN)
IMTA_LANG:disposition_option.dat (MDN)
```

표 10-10에는 이러한 파일에 사용할 수 있는 옵션이 설명되어 있습니다.

**표 10-10** DSN(Delivery Status Notification) 및 MDN(Message Disposition Notification) 옵션

| 옵션                    | 설명                                                                                                                                                                 |
|-----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DAY(DSN)              | RETURN_UNITS=0(기본값)을 설정하는 경우 %U 또는 %u 대체에 대해 삽입되는 텍스트입니다. 영어의 "Day" 또는 "day" 각각을 대체하는 기본적인 경우와는 달리 %U 및 %u 간에는 차이점이 없습니다.                                          |
| DIAGNOSTIC_CODE(DSN)  | DSN의 첫 번째 부분에서 수신자별 섹션의 구성에 사용되는 "Diagnostic code:" 텍스트보다 우선합니다. 이 필드는 DSN의 첫 번째 부분에 사용되는 문자 세트와 같은 문자 세트로 지정해야 합니다.                                               |
| HOURL(DSN)            | RETURN_UNITS=1을 설정하는 경우 %U 또는 %u 대체에 대해 삽입되는 텍스트입니다. 영어의 "Hour" 또는 "hour" 각각을 대체하는 기본적인 경우와는 달리 %U 및 %u 간에는 차이점이 없습니다.                                             |
| n.n.n(DSN)            | DSN의 수신자별 부분을 구성할 때 이름이 수신자별 숫자 상태와 일치하는 옵션이 있는지 확인하는 검사가 수행됩니다. 일치하는 항목이 있는 경우 해당 텍스트가 DSN에 삽입됩니다. 또한 위에서 설명한 REASON 옵션이 길이가 0인 결과를 생성하는 경우 REASON 필드는 삽입되지 않습니다. |
| ORIGINAL_ADDRESS(DSN) | DSN의 첫 번째 부분에서 수신자별 섹션의 구성에 사용되는 "Original address:" 텍스트보다 우선합니다. 이 필드는 DSN의 첫 번째 부분에 사용되는 문자 세트와 같은 문자 세트로 지정해야 합니다.                                              |

**표 10-10** DSN(Delivery Status Notification) 및 MDN(Message Disposition Notification) 옵션

| 옵션                         | 설명                                                                                                                                         |
|----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| REASON(DSN)                | DSN의 첫 번째 부분에서 수신자별 섹션의 구성에 사용되는 "Reason:" 텍스트보다 우선합니다. 이 필드는 DSN의 첫 번째 부분에 사용되는 문자 세트와 같은 문자 세트로 지정해야 합니다.                                |
| RECIPIENT_ADDRESS(DSN)     | DSN의 첫 번째 부분에서 수신자별 섹션의 구성에 사용되는 "Recipient address:" 텍스트보다 우선합니다. 이 필드는 DSN의 첫 번째 부분에 사용되는 문자 세트와 같은 문자 세트로 지정해야 합니다.                     |
| RETURN_PERSONAL(DSN 및 MDN) | From: 필드와 함께 사용되는 개인 이름 필드보다 우선합니다. 이 필드는 RFC 2047로 인코딩되어야 합니다. 이 옵션을 지정하지 않을 경우 RETURN_PERSONAL MTA 옵션에 설정된 값이 사용됩니다.                     |
| SUBJECT(DSN 및 MDN)         | Subject: 필드보다 우선합니다. 이 값은 알림에서 자체의 제목 필드를 제공하지 않은 경우에만 사용됩니다. 이 필드는 RFC 2047로 인코딩되어야 합니다. 이 옵션을 사용하지 않고 알림에서 제목을 제공하지 않은 경우 적절한 제목이 생성됩니다. |
| TEXT_CHARSET(MDN)          | MDN의 첫 번째 부분과 제목의 문자 세트 텍스트를 변환해야 합니다. 기본값은 변환을 수행하지 않는 것입니다.                                                                              |

## 추가 상태 알림 메일 기능

앞의 절에서는 상태 알림 메일을 설정하기 위한 필수 절차에 대해 설명했습니다. 다음 절에서는 추가 기능에 대해 설명합니다.

### 큰 메일의 내용 반환 차단

일반적으로 메일이 바운스 또는 차단되면 메일 내용이 보낸 사람과 알림 메일의 로컬 도메인 포스트마스터에게 반환됩니다. 이것은 매우 큰 여러 메일이 반환될 경우 자원에 적지 않은 부담이 될 수 있습니다. 일정 크기 이상의 메일 내용이 반환되는 것을 차단하려면 MTA 옵션 파일에서 CONTENT\_RETURN\_BLOCK\_LIMIT 옵션을 설정합니다.

### 상태 알림 메일의 포함 헤더에서 미국 ASCII가 아닌 문자 제거

인터넷 메일 헤더의 원시 형식은 미국 ASCII가 아닌 문자를 허용하지 않습니다. 미국 ASCII가 아닌 문자가 메일 헤더에 사용된 경우 이러한 문자는 RFC 2047에 설명된 "MIME 헤더 인코딩"을 통해 인코딩됩니다. 따라서 전자 메일의 중국어 "Subject" 행은 실제로 다음과 같이 나타납니다.

```
Subject: =?big5?Q?=A4j=AB=AC=A8=B1=AD=B1=B0=D3=F5=A5X=AF=B2?=
```

이 경우 헤더를 표시할 때 인코딩을 제거하는 작업을 전자 메일 클라이언트가 수행합니다.

%H 템플릿이 헤더를 알림 메일의 본문에 복사하므로 인코딩된 헤더 텍스트가 정상적으로 표시됩니다. 그러나 제목의 문자 세트(이 경우에는 "big5")가 return\_prefix.txt의 Content-Type 헤더 문자 세트 매개 변수에 있는 문자 세트와 일치할 경우 Messaging Server는 인코딩을 제거합니다. 이러한 문자 세트가 일치하지 않을 경우 Messaging Server는 인코딩을 그대로 둡니다.

## 알림 메일 전달 간격 설정

키워드: notices, nonurgentnotices, normalnotices, urgentnotices

전달할 수 없는 메일은 보낸 사람에게 반환하기 전에 지정된 시간 동안 주어진 채널 대기열에 보관됩니다. 또한 Messaging Server가 전달을 시도하는 동안에 일련의 상태/경고 메일이 보낸 사람에게 반환될 수 있습니다. 메일 간의 시간 및 간격은 notices, nonurgentnotices, normalnotices 또는 urgentnotices 키워드를 사용하여 지정할 수 있습니다. 예를 들면 다음과 같습니다.

notices 1 2 3

모든 메일에 대해 1 및 2일 후에 일시적인 실패 상태 알림 메일이 보내집니다. 3일 후에도 여전히 전달되지 않은 경우 해당 메일은 메일 발송자에게 반환됩니다.

urgentnotices 2, 4, 6, 8

높은 우선 순위를 가진 메일에 대해 2, 4 및 6일 후에 일시적인 실패 알림이 보내집니다. 8일 후에도 여전히 전달되지 않은 경우 해당 메일은 메일 발송자에게 반환됩니다.

MTA에 옵션 파일의 RETURN\_UNITS 옵션에서는 시간(1) 또는 일(0) 단위를 지정할 수 있다는 것에 주의합니다. 기본값은 일(0)입니다. RETURN\_UNITS=1을 설정할 경우 반송 작업을 1시간마다 실행하고 알림을 1시간마다 가져오도록 예약해야 합니다. 반송 작업이 1시간마다 실행되면 또한 1시간마다 mail.log\* 파일을 롤오버합니다. mail.log 파일이 1시간마다 롤오버되는 것을 방지하려면 imta.tailor 파일의 IMTA\_RETURN\_SPLIT\_PERIOD 조정 파일 옵션을 24로 설정합니다. 반송 작업 예약은 local.schedule.return\_job configutil 매개 변수에 의해 제어됩니다.

notices 키워드가 지정되지 않은 경우 기본값은 로컬 1 채널에 대한 notices 설정을 사용하는 것입니다. 로컬 채널에 대한 설정이 없을 경우 notices 3, 6, 9, 12가 기본값으로 사용됩니다.

## 상태 알림 메일에 변경된 주소 포함

키워드: includefinal, suppressfinal, useintermediate



MTA가 알림 메일(바운스 메일, 전달 수신 확인 메일 등)을 생성할 때 "원래" 형식의 수신자 주소와 MTA에서 사용할 수 있는 변경된 "최종" 형식의 수신자 주소가 모두 존재할 수 있습니다. 알림 메일의 수신자(알림 메일이 관련된 원래 메일을 보낸 사람)가 대개 원래 형식을 인식하므로 MTA는 항상 원래 형식(존재할 경우)을 알림 메일에 포함합니다.

`includefinal` 및 `suppressfinal` 채널 키워드는 MTA가 또한 최종 형식의 주소를 포함하는지 여부를 제어합니다. 내부 메일함 이름을 외부에서 볼 수 없도록 "숨기는" 사이트에서는 최종 형식의 주소를 포함하지 않을 수 있습니다. 이러한 사이트는 원래 "외부" 형식의 주소만 상태 알림 메일에 포함하기를 원할 것입니다. 기본값은 최종 형식의 수신자 주소를 포함하는 `includefinal`입니다. `suppressfinal`을 사용하면 원래 주소 형식이 존재할 경우 최종 주소 형식이 상태 알림 메일에 표시되지 않습니다.

`useintermediate` 키워드는 목록이 확장되었지만 사용자 메일함 이름이 생성되기 전에 만들어진 중간 형식의 주소를 사용합니다. 이 정보를 사용할 수 없는 경우 최종 형식이 사용됩니다.

## 포스트마스터에 대해 상태 알림 메일을 전송, 차단 및 지정

기본적으로 실패 및 경고 상태 알림 메일의 복사본은 오류 반환 및 경고가 빈

`Errors-to:` 헤더 행 또는 빈 봉투 `From:` 주소로 완전히 억제되지 않은 경우 포스트마스터에게 보내집니다. 다음 절과 표 10-11에 설명된 여러 채널 키워드를 사용하면 포스트마스터에 대한 알림 메일 전달을 더 세부적으로 제어할 수 있습니다.

### 반환되는 실패 메일

키워드: `sendpost`, `nosendpost`, `copysendpost`, `errsendpost`

채널 프로그램은 장기적인 서비스 실패나 잘못된 주소로 인해 메일을 전달하지 못할 수 있습니다. 이 경우 MTA 채널 프로그램은 메일을 전달할 수 없는 이유에 대한 설명과 함께 메일을 보낸 사람에게 반환합니다. 또한 선택적으로 모든 실패 메일의 복사본이 로컬 포스트마스터에게 보내집니다. 이것은 메일 실패를 모니터링하는 데 유용하지만 포스트마스터가 처리해야 하는 과도한 양의 트래픽을 발생시킬 수 있습니다. 표 10-11을 참조하십시오.

### 경고 메일

키워드: `warnpost`, `nowarnpost`, `copywarnpost`, `errwarnpost`

메일을 반환하는 것 외에도 MTA는 전달되지 않은 메일에 대한 자세한 경고를 보낼 수 있습니다. 경우에 따라 채널 프로그램이 실패한 전달 시도 이후에 경고 메일을 생성할 수 있지만 이러한 경고는 일반적으로 `notices` 채널 키워드 설정에 기초한 시간 초과로 인해 발생합니다. 경고 메일은 무엇이 잘못되었는지와 전달 시도가 얼마나 오랫동안 계속되었는지에 대한 설명을 포함합니다. 또한 대부분의 경우 경고 메일은 문제가 된 메일의 헤더와 처음 몇 개의 행을 포함합니다.

선택적으로 모든 경고 메일의 복사본을 로컬 포스트마스터에게 보낼 수 있습니다. 이것은 포스트마스터가 처리해야 하는 많은 양의 트래픽을 발생시키지만 다양한 대기열의 상태를 모니터링하는 데 유용할 수 있습니다. 경고 메일을 포스트마스터에게 보내는 것을 제어하기 위해 `warnpost`, `copywarnpost`, `errwarnpost` 및 `nowarnpost` 키워드가 사용됩니다. 표 10-11을 참조하십시오.

### 빈 봉투 반송 주소

키워드: `returnenvelope`

`returnenvelope` 키워드는 비트 플래그 집합으로 해석되는 단일 정수 값을 가집니다. 비트 0(값 = 1)은 MTA에 의해 생성된 반송 알림이 빈 봉투 주소 또는 로컬 포스트마스터의 주소로 작성되는지 여부를 제어합니다. 이 비트를 설정하면 로컬 마스터 주소가 사용되고 이 비트를 지우면 빈 주소가 사용됩니다.

---

**주** RFC 1123에는 빈 주소를 사용하도록 명시되어 있지만 일부 시스템은 빈 봉투의 `From:` 주소를 적절하게 처리하지 않으므로 이 옵션을 사용하는 것이 필요할 수 있습니다.

---

비트 1(값 = 2)은 MTA가 모든 빈 봉투 주소를 로컬 포스트마스터의 주소로 대체하는지 여부를 제어합니다. 이 비트는 RFC 821, RFC 822 또는 RFC 1123을 따르지 않는 비호환 시스템을 수용하는 데 사용됩니다.

비트 2(값 = 4)는 구문적으로 잘못된 반송 주소를 사용할 수 없게 합니다.

비트 3(값 = 8)은 `mailfromdnsverify` 키워드와 동일합니다.

### 포스트마스터에게 반환되는 메일 내용

키워드: `postheadonly`, `postheadbody`

채널 프로그램이나 정기적인 메일 반송 작업이 포스트마스터와 원래의 보낸 사람 모두에게 메일을 반환할 경우 포스트마스터 복사본은 전체 메일이나 헤더가 될 수 있습니다. 포스트마스터 복사본을 단지 헤더로 제한하면 사용자 메일의 프라이버시 수준이 향상됩니다. 그러나 일반적으로 포스트마스터와 시스템 관리자는 원할 경우 root 시스템 권한을 사용하여 메일 내용을 읽을 수 있으므로 이러한 제한만으로 메일 보안이 보장되지는 않습니다. 표 10-11을 참조하십시오.

### 채널별 포스트마스터 주소 설정

키워드: `aliaspostmaster`, `returnaddress`, `noreturnaddress`, `returnpersonal`, `noreturnpersonal`

기본적으로 MTA가 바운스 또는 상태 알림 메일을 생성할 때 사용되는 포스트마스터의 반송 주소는 `postmaster@local-host`, 여기서 `local-host`는 공식 로컬 호스트 이름(로컬 채널에 있는 이름)이고 포스트마스터 개인 이름은 "MTA e-Mail Interconnect"입니다. 잘못된 포스트마스터 주소를 선택할 경우 급격한 메일 루핑과 많은 오류 메시지가 발생할 수 있으므로 주의해야 합니다.

`RETURN_ADDRESS` 및 `RETURN_PERSONAL` 옵션을 사용하면 포스트마스터 주소 및 개인 이름에 대한 MTA 시스템 기본값을 설정할 수 있습니다. 또는 채널별 제어를 원할 경우 `returnaddress` 및 `returnpersonal` 채널 키워드를 사용할 수 있습니다.

`returnaddress` 및 `returnpersonal`은 각각 포스트마스터 주소와 포스트마스터 개인 이름을 지정하는 필수 인수를 가집니다. 기본적으로 `noreturnaddress`와 `noreturnpersonal`이 지정되며 이것은 기본값이 사용되어야 한다는 것을 의미합니다. 기본값은 `RETURN_ADDRESS` 및 `RETURN_PERSONAL` 옵션을 통해 지정하거나 이러한 옵션이 설정되지 않은 경우 보통의 기본값으로 지정됩니다.

`aliaspostmaster` 키워드가 채널에 있을 경우 공식 채널 이름의 아이디 `postmaster`(소문자, 대문자 또는 대소문자 혼합)로 주소 지정된 모든 메일은 `postmaster@local-host`로 리디렉션됩니다. 여기서 `local-host`는 공식 로컬 호스트 이름(로컬 채널의 이름)입니다. 인터넷 표준에 따르면 메일을 수락하는 DNS의 모든 도메인이 메일을 수신하는 유효한 포스트마스터 계정을 가져야 한다는 것에 주의합니다. 따라서 여러 다른 도메인에 대해 별개의 포스트마스터 계정을 설정하는 대신 포스트마스터의 책임을 중앙 집중화하려는 경우 이 키워드가 유용할 수 있습니다. 즉, `returnaddress`가 MTA에서 포스트마스터의 알림 메일을 생성할 때 사용되는 반송 포스트마스터 주소를 제어하는 것과 달리 `aliaspostmaster`는 포스트마스터로 주소 지정된 메일을 MTA에서 처리하는 방법에 영향을 줍니다.

**표 10-11**                      포스트마스터 및 보낸 사람에게 알림 메일을 보내는 데 사용되는 키워드

| 키워드               | 설명                                                                                                                                                              |
|-------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>반환되는 메일 내용</b> | <b>알림에 대한 주소 지정</b>                                                                                                                                             |
| notices           | 알림을 보낸 후 메일을 반환되기 전에 경과할 수 있는 시간을 지정합니다.                                                                                                                        |
| nonurgentnotices  | 낮음 우선 순위를 갖는 메일에 대해 알림을 보낸 후 메일을 반환되기 전에 경과할 수 있는 시간을 지정합니다.                                                                                                    |
| normalnotices     | 중간 우선 순위를 갖는 메일에 대해 알림을 보낸 후 메일을 반환되기 전에 경과할 수 있는 시간을 지정합니다.                                                                                                    |
| urgentnotices     | 높음 우선 순위를 갖는 메일에 대해 알림을 보낸 후 메일을 반환되기 전에 경과할 수 있는 시간을 지정합니다.                                                                                                    |
| <b>반환되는 메일</b>    | <b>반환되는 메일에 대한 실패 알림 처리 방법</b>                                                                                                                                  |
| sendpost          | 실패한 모든 메일의 복사본을 포스트마스터에게 보냅니다.                                                                                                                                  |
| copysendpost      | 전송 실패 메일에서 메일 발송자 주소가 비어 있지 않는 한 실패 알림 복사본을 포스트마스터에게 보냅니다. 이 경우 포스트마스터는 실제로 바운스 또는 알림인 메일을 제외하고 실패한 모든 메일의 복사본을 갖게 됩니다.                                         |
| errsendpost       | 메일 발송자에게 알림을 보낼 수 없는 경우 실패 알림 복사본을 포스트마스터에게 보냅니다. nosendpost가 지정된 경우 실패한 메일은 포스트마스터에게 보내지지 않습니다.                                                                |
| nosendpost        | 전달이 실패한 모든 메일의 복사본을 포스트마스터에게 보내지 않습니다.                                                                                                                          |
| <b>경고 메일</b>      | <b>경고 메일 처리 방법</b>                                                                                                                                              |
| warnpost          | 경고 메일의 복사본을 포스트마스터에게 보냅니다. 빈 Warnings-to: 헤더 또는 빈 봉투 From: 주소로 경고가 완전히 억제되지 않은 경우 기본값은 경고 복사본을 포스트마스터에게 보내는 것입니다.                                               |
| copywarnpost      | 전달되지 않은 메일에서 보낸 사람 주소가 비어 있지 않는 한 경고 메일 복사본을 포스트마스터에게 보냅니다.                                                                                                     |
| errwarnpost       | 메일 발송자에게 알림을 보낼 수 없는 경우 경고 메일 복사본을 포스트마스터에게 보냅니다.                                                                                                               |
| nowarnpost        | 경고 메일의 복사본을 포스트마스터에게 보내지 않습니다.                                                                                                                                  |
| <b>반환되는 메일 내용</b> | <b>포스트마스터에게 전체 메일을 보낼 것인지 아니면 단순히 헤더만 보낼 것인지 지정</b>                                                                                                             |
| postheadonly      | 헤더만 포스트마스터에게 반환됩니다. 포스트마스터 복사본을 단지 헤더로 제한하면 사용자 메일의 프라이버시 수준이 향상됩니다. 그러나 포스트마스터와 시스템 관리자는 원할 경우 root 시스템 권한을 사용하여 메일 내용을 읽을 수 있으므로 이러한 제한만으로 메일 보안이 보장되지는 않습니다. |
| postheadbody      | 헤더와 메일 내용을 모두 반환합니다.                                                                                                                                            |

표 10-11 포스트마스터 및 보낸 사람에게 알림 메일을 보내는 데 사용되는 키워드

| 키워드                                | 설명                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 반환되는 메일 내용                         | 알림에 대한 주소 지정                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| includefinal<br>returnenvelope     | <p>전달 알림에 최종 수신자 주소 형식을 포함합니다.</p> <p>빈 봉투 반송 주소 사용을 제어합니다. returnenvelope 키워드는 비트 플래그 집합으로 해석되는 단일 정수 값을 가집니다.</p> <p>비트 0(값 = 1)은 MTA에 의해 생성된 반송 알림이 빈 봉투 주소 또는 로컬 포스트마스터의 주소로 작성되는지 여부를 제어합니다. 이 비트를 설정하면 로컬 마스터 주소가 사용되고 이 비트를 지우면 빈 주소가 사용됩니다.</p> <p>비트 1(값 = 2)은 MTA가 모든 빈 봉투 주소를 로컬 포스트마스터의 주소로 대체하는지 여부를 제어합니다. 이 비트는 RFC 821, RFC 822 또는 RFC 1123을 따르지 않는 비호환 시스템을 수용하는 데 사용됩니다.</p> <p>비트 2(값 = 4)는 구문적으로 잘못된 반송 주소를 사용할 수 없게 합니다.</p> <p>비트 3(값 = 8)은 mailfromdnsverify 키워드와 동일합니다.</p> |
| suppressfinal<br>useintermediate   | <p>원본 주소 형식이 있는 경우 알림 메일에서 최종 주소 형식을 생략합니다.</p> <p>목록을 확장한 이후 사용자 메일할 이름이 생성되기 이전에 생성되는 중간 주소 형식을 사용합니다. 이 정보를 사용할 수 없는 경우 최종 형식이 사용됩니다.</p>                                                                                                                                                                                                                                                                                                                                                        |
| 반환되는 메일 내용                         | 알림에 대한 주소 지정                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| aliaspostmaster                    | 공식 채널 이름에서 포스트마스터 아이디로 주소 지정된 메일은 postmaster@local-host로 리디렉션됩니다. 여기서 local-host는 로컬 호스트 이름(로컬 채널에 있는 이름)입니다.                                                                                                                                                                                                                                                                                                                                                                                       |
| returnaddress<br>noreturnaddress   | <p>로컬 포스트마스터에 대한 반송 주소를 지정합니다.</p> <p>RETURN_ADDRESS 옵션 값을 포스트마스터 주소 이름으로 사용합니다.</p>                                                                                                                                                                                                                                                                                                                                                                                                                |
| returnpersonal<br>noreturnpersonal | <p>로컬 포스트마스터에 대한 개인 이름을 설정합니다.</p> <p>RETURN_PERSONAL 옵션 값을 포스트마스터 개인 이름으로 사용합니다.</p>                                                                                                                                                                                                                                                                                                                                                                                                               |

## MDN(Message Disposition Notification) 제어

MDN(Message Disposition Notification)은 MTA가 보낸 사람 및/또는 포스트마스터에게 보내는 전자 메일 보고서로서 메일의 전달 처리를 보고합니다. 예를 들어, Sieve 필터에 의해 메일이 거부된 경우 MDN이 보낸 사람에게 보내집니다. MDN은 또한 읽음 확인, 확인, 수신 알림 또는 전달 확인이라고도 합니다. Sieve 스크립트 언어는 일반적으로 메일 필터링 및 휴가 메일에 사용됩니다.

## MDN(Message Disposition Notification) 메일 사용자 정의 및 현지화

MDN을 수정 및 현지화하기 위한 지침은 여기에 설명된 약간의 차이점을 제외하고 전달 상태 알림 메일을 사용자 정의 및 현지화하기 위한 지침과 비슷합니다. [267페이지의 "전달 상태 알림 메일 사용자 정의 및 현지화"](#) 및 [270페이지의 "생성된 알림 국제화"](#)를 참조하십시오.

매핑(DISPOSITION\_LANGUAGE 매핑이라고 부름)은 상태 알림을 국제화하는 데 사용되는 `notification_language` 매핑 테이블([269페이지의 코드 예 10-2](#))과 비슷합니다.

그러나 이 매핑에 대한 MDN 검사는 다음 형식을 가집니다.

```
type|modifiers|source-channel|header-language|return|recipient
```

여기서

`type`은 배포 유형이며 `displayed`, `dispatched`, `processed`, `deleted`, `denied` 또는 `failed` 중 하나를 사용할 수 있습니다.

`modifiers`는 쉼표로 구분된 처리 수정자 목록입니다. 현재 목록은 `error`, `warning`, `superseded` 및 `expired`입니다.

`source-channel`은 MDN을 생성하는 소스 채널입니다.

`header-language`는 `accept-language`, `preferred-language` 또는 `x-accept-language` 중 하나에 지정된 언어입니다. (MTA는 이러한 옵션 중에서 존재하는 첫 번째 옵션을 사용합니다.)

`return`은 알림이 반환되는 주소입니다.

`recipient`는 처리와 관련된 주소입니다.

처리 매핑의 결과는 세로 막대(|)로 구분되는 둘 또는 세 개의 정보로 구성됩니다. 첫 번째 정보는 배포 알림의 템플릿 파일이 있는 디렉토리입니다. 두 번째 정보는 독립형 배포 텍스트에 적용될 문자 세트입니다. 이 정보가 필요한 것은 특히 휴가 Sieve 작업에 대한 `:mime` 매개 변수 사용이나 자동 회신 예코에 의해 생성된 처리를 비롯한 일부 처리가 템플릿 파일을 사용하지 않으며 결과적으로 이러한 파일로부터 문자 세트를 상속할 수 없기 때문입니다. 마지막으로 세 번째 정보는 알림에 대한 대체 제목 행입니다. 이 정보는 매핑에 의해 또한 `$T` 플래그가 설정된 경우에만 사용됩니다.

다음의 추가 템플릿 파일이 MDN을 구성하는 데 사용됩니다.

```
disposition_deleted.txt disposition_failed.txt  
disposition_denied.txt disposition_prefix.txt  
disposition_dispatched.txt disposition_processed.txt  
disposition_displayed.txt disposition_suffix.txt  
disposition_option.opt
```

이러한 템플릿 파일은 상태 알림 메일에 대한 다양한 `return_*.txt` 파일과 비슷한 방식으로 사용됩니다. `*.txt` 파일의 메일 텍스트는 한 행당 78자로 제한되어야 합니다.

MDN(Message Disposition Notification) 제어



## 다시 쓰기 규칙 구성

이 장에서는 `imta.cnf` 파일에서 다시 쓰기 규칙을 구성하는 방법에 대해 설명합니다. 아직 읽지 않은 경우, 이 장을 진행하기 전에 [10장, "MTA 서비스 및 구성 정보"](#)를 읽어야 합니다.

이 장은 다음 내용으로 구성되어 있습니다.

- [282페이지의 "다시 쓰기 규칙 구조"](#)
- [284페이지의 "다시 쓰기 규칙 패턴 및 태그"](#)
- [287페이지의 "다시 쓰기 규칙 템플릿"](#)
- [290페이지의 "MTA가 다시 쓰기 규칙을 주소에 적용하는 방법"](#)
- [296페이지의 "템플릿 대체 및 다시 쓰기 규칙 제어 시퀀스"](#)
- [309페이지의 "많은 수의 다시 쓰기 규칙 처리"](#)
- [309페이지의 "다시 쓰기 규칙 테스트"](#)
- [310페이지의 "다시 쓰기 규칙 예"](#)

**Messaging Server**의 주소 다시 쓰기 기능은 주소의 호스트 또는 도메인 부분을 조작 및 변경하기 위한 기본 기능입니다. **Messaging Server**는 별칭, 주소 역방향 데이터베이스 및 특수한 매핑 테이블과 같은 주소 조작을 위한 다른 기능을 제공합니다. 그러나 최상의 성능을 위해서는 주소 조작을 수행할 수 있을 때마다 다시 쓰기 규칙을 사용하는 것이 좋습니다.

---

**주** imta.cnf 파일의 다시 쓰기 규칙을 변경하면 시작 시에 구성 데이터를 한 번만 로드하는 모든 프로그램이나 채널(예: SMTP 서버)을 `imsimta restart` 명령을 사용하여 다시 시작해야 합니다. 컴파일된 구성을 사용하는 경우 재컴파일을 수행한 다음 다시 시작해야 합니다.

구성 정보 컴파일과 프로그램 시작에 대한 자세한 내용은 *Messaging Server Reference Manual*을 참조하십시오.

---

## 다시 쓰기 규칙 구조

다시 쓰기 규칙은 MTA 구성 파일 `imta.cnf`의 상반부에 표시됩니다. 구성 파일의 각 규칙은 하나의 행으로 나타납니다. 규칙 사이에 주석이 올 수 있지만 빈 행은 허용되지 않습니다. 다시 쓰기 규칙은 빈 행으로 끝나며 그 뒤에 채널 정의가 옵니다. 아래 예는 구성 파일의 다시 쓰기 규칙 섹션을 보여 줍니다.

```
! test.cnf - An example configuration file.
!
! This is only an example of a configuration file. It serves
! no useful purpose and should not be used in a real system.
!
a.com    $U@a-host
b.org    $U@b-host
c.edu    $U%c@b-daemon
d.com    $U%d@a-daemon

! Begin channel definitions
```

다시 쓰기 규칙은 해당 문자열이나 *템플릿*가 뒤에 오는 패턴인 두 부분으로 구성됩니다. 두 부분을 공백으로 구분해야 하며 각 부분 내에서는 공백이 허용되지 않습니다. 다시 쓰기 규칙의 구조는 다음과 같습니다.

```
pattern template
```

*pattern*

도메인 이름에서 검색할 문자열을 나타냅니다. 표 11-3에서 패턴은 a.com, b.org, c.edu 및 d.com입니다.

패턴이 주소의 도메인 부분과 일치할 경우 다시 쓰기 규칙이 주소에 적용됩니다. 패턴과 템플릿 사이를 공백으로 구분해야 합니다. 패턴 구문에 대한 자세한 내용은 284페이지의 "다시 쓰기 규칙 패턴 및 태그"를 참조하십시오.

*template*

다음 중 하나입니다.

*UserTemplate@DomainTemplate@ChannelTag* [controls]

*UserTemplate@ChannelTag* [controls]

*UserTemplate@DomainTemplate* [controls]

*UserTemplate@DomainTemplate@ChannelTag* [controls]

*UserTemplate@DomainTemplate@SourceRoute@ChannelTag* [controls]

여기서

*UserTemplate*는 주소의 사용자 부분이 다시 작성되는 방법을 지정합니다. 대체 시퀀스를 사용하여 원래 주소의 일부나 데이터베이스 조회의 결과를 나타낼 수 있습니다. 대체 시퀀스는 다시 작성된 주소를 생성하기 위해 자신이 나타내는 대상으로 대체됩니다.

표 11-4에서는 \$U 대체 시퀀스가 사용됩니다. 자세한 내용은 296페이지의 "템플릿 대체 및 다시 쓰기 규칙 제어 시퀀스"를 참조하십시오.

*DomainTemplate*는 주소의 도메인 부분이 다시 작성되는 방법을 지정합니다.

*UserTemplate*와 마찬가지로 *DomainTemplate*는 대체 시퀀스를 포함할 수 있습니다.

*ChannelTag*는 이 메일이 전송될 채널을 나타냅니다. 모든 채널 정의는 채널 이름뿐만 아니라 채널 태그를 포함해야 합니다. 채널 태그는 일반적으로 다시 쓰기 규칙과 채널 정의에 모두에 표시됩니다.

*controls*(제어)를 사용하여 규칙의 적용 가능성을 제한할 수 있습니다. 일부 제어 시퀀스는 규칙의 시작 부분에 있어야 하며 다른 제어는 규칙의 끝 부분에 있어야 합니다. 제어에 대한 자세한 내용은 296페이지의 "템플릿 대체 및 다시 쓰기 규칙 제어 시퀀스"를 참조하십시오.

템플릿 구문에 대한 자세한 내용은 287페이지의 "다시 쓰기 규칙 템플릿"를 참조하십시오.

## 다시 쓰기 규칙 패턴 및 태그

이 절은 다음과 같은 하위 절로 구성되어 있습니다.

- [286페이지의 "백분율 핵과 일치시키는 규칙"](#)
- [286페이지의 "뱅 스타일\(UUCP\) 주소와 일치시키는 규칙"](#)
- [287페이지의 "모든 주소와 일치시키는 규칙"](#)
- [287페이지의 "태그된 다시 쓰기 규칙 집합"](#)

대부분의 다시 쓰기 규칙 패턴은 해당 호스트와만 일치하는 특정 호스트 이름이나 전체 하위 도메인의 모든 호스트/도메인과 일치하는 하위 도메인 패턴으로 구성됩니다.

예를 들어, 다음 다시 쓰기 규칙 패턴은 지정된 호스트와만 일치하는 특정 호스트 이름을 포함합니다.

```
host.siroe.com
```

다음 다시 쓰기 규칙 패턴은 전체 하위 도메인의 모든 호스트 또는 도메인과 일치하는 하위 도메인 패턴을 포함합니다.

```
.siroe.com
```

그러나 이 패턴은 정확한 호스트 이름 `siroe.com`과 일치하지 않습니다. 정확한 호스트 이름 `siroe.com`과 일치하려면 별개의 `siroe.com` 패턴이 필요합니다.

MTA는 특정 호스트 이름부터 시작한 다음 특수성을 줄이기 위해 이름을 점차적으로 일반화하여 호스트/도메인 이름의 다시 쓰기를 시도합니다. 이것은 더 특수한 다시 쓰기 규칙 패턴의 사용이 더 일반적인 다시 쓰기 규칙 패턴 사용보다 선호된다는 것을 의미합니다. 예를 들어, 다음 다시 쓰기 규칙 패턴이 구성 파일에 존재한다고 가정해 봅니다.

```
hosta.subnet.siroe.com
```

```
.subnet.siroe.com
```

```
.siroe.com
```

다시 쓰기 규칙 패턴에 기초하여 `jdoue@hosta.subnet.siroe.com` 주소는

`hosta.subnet.siroe.com` 다시 쓰기 규칙 패턴과 일치하고

`jdoue@hostb.subnet.siroe.com` 주소는 `.subnet.siroe.com` 다시 쓰기 규칙 패턴과 일치하며 `jdoue@hostc.siroe.com` 주소는 `.siroe.com` 다시 쓰기 규칙 패턴과 일치합니다.

특히 하위 도메인 다시 쓰기 규칙 패턴을 통합하는 다시 쓰기 규칙이 인터넷상의 사이트에서 일반적으로 사용됩니다. 이러한 사이트는 일반적으로 고유한 내부 호스트와 서브넷을 위한 여러 다시 쓰기 규칙을 가지며 최상위 인터넷 도메인에 대한 다시 쓰기 규칙을 `internet.rules(msg_svr_base/config/internet.rules)` 파일의 구성에 포함합니다.

특정 다시 쓰기 규칙을 통해 처리되는 내부 호스트 대상이 아니라 인터넷 대상에 대한 메일이 제대로 재작성되고 보내는 TCP/IP 채널로 라우팅되도록 `imta.cnf` 파일이 다음을 포함하는지 확인합니다.

- 최상위 인터넷 도메인과 일치하는 패턴이 포함된 다시 쓰기 규칙
- 이러한 패턴과 일치하는 주소를 보내는 TCP/IP 채널로 다시 쓰는 템플릿

```
! Ascension Island
.AC          $U%$H$D@TCP-DAEMON
. [text
.   removed for
.   brevity]
! Zimbabwe
.ZW         $U%$H$D@TCP-DAEMON
```

IP 도메인 리터럴은 비슷한 계층 일치 패턴을 따르지만 왼쪽에서 오른쪽이나 아니라 오른쪽에서 왼쪽으로 일치합니다. 예를 들어, 다음 패턴은 정확하게 IP 리터럴 [1.2.3.4]와만 일치합니다.

[1.2.3.4]

다음 패턴은 1.2.3.0 서브넷의 모든 항목과 일치합니다.

[1.2.3.]

이미 설명했던 더 일반적인 종류의 호스트 또는 하위 도메인 다시 쓰기 규칙 패턴 외에도 다시 쓰기 규칙은 또한 표 11-1에 요약되어 있으며 다음 하위 절에서 설명할 여러 특수한 패턴을 사용할 수 있습니다.

**표 11-1** 다시 쓰기 규칙의 특수한 패턴 요약

| 패턴  | 설명/사용                                                   |
|-----|---------------------------------------------------------|
| \$* | 모든 주소와 일치합니다. 이 규칙은 지정된 경우 파일에서의 위치에 상관 없이 가장 먼저 시도됩니다. |
| \$% | 백분을 핵 규칙입니다. A%B 형식의 모든 호스트/도메인 지정과 일치합니다.              |

**표 11-1** 다시 쓰기 규칙의 특수한 패턴 요약

| 패턴  | 설명/사용                                            |
|-----|--------------------------------------------------|
| \$! | 뱅 스타일 규칙입니다. B!A 형식의 모든 호스트/도메인 지정과 일치합니다.       |
| [ ] | IP 리터럴 모두 일치 규칙입니다. 모든 IP 도메인 리터럴과 일치합니다.        |
| .   | 모든 호스트/도메인 지정과 일치합니다<br>(예: joe@[129.165.12.11]) |

이러한 특수한 패턴 외에도 **Messaging Server**는 또한 다시 쓰기 규칙 패턴에 표시될 수 있는 *태그*의 개념을 가집니다. 이러한 태그는 주소를 여러 번 다시 쓸 수 있으며 이전 다시 쓰기에 기초하여 주소와 일치할 다시 쓰기 규칙을 제어함으로써 후속 다시 쓰기를 구별해야 하는 경우에 사용됩니다. 자세한 내용은 [287페이지의 "태그된 다시 쓰기 규칙 집합"](#)을 참조하십시오.

## 백분율 핵과 일치시키는 규칙

MTA는 A%B 형식의 주소를 다시 쓰려는 시도가 실패할 경우 해당 주소를 A%B@localhost 형식으로 처리하기 전에 하나의 추가 규칙을 시도합니다. (이러한 주소 형식에 대한 자세한 내용은 [287페이지의 "다시 쓰기 규칙 템플릿"](#)을 참조하십시오.) 이 추가 규칙은 *백분율 핵* 규칙입니다. 패턴은 %이며 절대 변경되지 않습니다. 이 규칙은 백분율 기호를 포함하는 로컬 부분의 다시 쓰기가 다른 방법(아래 설명된 모두 일치 규칙 포함)으로 실패할 경우에만 활성화됩니다.

백분율 핵 규칙은 특수한 내부 의미를 백분율 핵 주소에 할당하는 데 유용합니다.

## 뱅 스타일(UUCP) 주소와 일치시키는 규칙

MTA는 B!A 형식의 주소를 다시 쓰려는 시도가 실패할 경우 해당 주소를 B!A@localhost 형식으로 처리하기 전에 하나의 추가 규칙을 시도합니다. 이 추가 규칙은 *뱅 스타일* 규칙입니다. 패턴은 \$!이며 절대 변경되지 않습니다. 이 규칙은 느낌표를 포함하는 로컬 부분의 다시 쓰기가 다른 방법(아래 설명된 기본 규칙 포함)으로 실패할 경우에만 활성화됩니다.

뱅 스타일 규칙은 UUCP 시스템과 라우팅에 대한 포괄적인 지식을 바탕으로 UUCP 스타일 주소를 시스템으로 라우팅하도록 강제 지정하는 데 사용할 수 있습니다.

## 모든 주소와 일치시키는 규칙

특수한 패턴 "."(마침표)는 다른 규칙이 일치하지 않거나 호스트/도메인 지정을 채널 테이블에서 찾을 수 없을 경우 모든 호스트/도메인 지정과 일치합니다. 다시 말해서 "." 규칙은 주소 다시 쓰기가 다른 방법으로 실패한 경우 마지막 수단으로 사용됩니다.

---

**주** 대체 시퀀스와 관련하여 모두 일치 규칙이 일치하고 해당 템플리트가 확장되면 \$H는 전체 호스트 이름으로 확장하고 \$D는 마침표 "."로 확장됩니다. 따라서 \$D는 모두 일치 규칙 템플리트에서 제한적으로 사용됩니다.

---

## 태그된 다시 쓰기 규칙 집합

다시 쓰기 프로세스가 진행되면서 다른 규칙 집합을 적용하는 것이 적합할 수 있습니다. 이렇게 하려면 다시 쓰기 규칙 태그를 사용합니다. 현재 태그는 구성 파일 또는 도메인 데이터베이스에서 패턴이 조회되기 전에 각 패턴의 앞에 놓입니다. 다시 쓰기 규칙 템플리트의 \$T 대체 문자열을 사용하여 일치하는 임의의 다시 쓰기 규칙에 의해 태그가 변경될 수 있습니다(아래에 설명됨).

태그는 다소 고정적일 수 있습니다. 즉, 설정된 태그는 단일 주소에서 추출되는 모든 호스트에 계속 적용됩니다. 이것은 임의의 태그를 사용한 후에 적절한 태그 값으로 시작하는 대체 규칙을 제공할 때 신중해야 한다는 것을 의미합니다. 일반적으로 태그는 매우 전문화된 응용 프로그램에서만 사용되므로 이것은 실제로 거의 문제가 되지 않습니다. 주소 다시 쓰기가 끝나면 태그는 기본 태그(빈 문자열)로 재설정됩니다.

기본적으로 모든 태그 값은 세로 막대(|)로 끝납니다. 이 문자는 일반 주소에서 사용되지 않으므로 패턴의 나머지 부분에서 태그를 자유롭게 나타냅니다.

## 다시 쓰기 규칙 템플리트

다음 절에서는 다시 쓰기 규칙의 템플리트 형식에 대해 더욱 자세하게 설명합니다.

표 11-2에는 템플리트 형식이 요약되어 있습니다.

**표 11-2** 다시 쓰기 규칙의 템플리트 형식 요약

| 템플리트 | 페이지 | 사용                                                       |
|------|-----|----------------------------------------------------------|
| A%B  | 288 | A는 새 사용자/메일함 이름이 되고 B는 새 호스트/도메인 지정이 되며 다시 쓰기를 다시 수행합니다. |
| A@B  | 288 | A%B@B로 처리됩니다.                                            |

표 11-2 다시 쓰기 규칙의 템플리트 형식 요약

| 템플리트    | 페이지 | 사용                                                                            |
|---------|-----|-------------------------------------------------------------------------------|
| A%B@C   | 288 | A는 새 사용자/메일함 이름이 되고 B는 새 호스트/도메인 지정이 되며 호스트 C와 연관된 채널로 라우팅합니다.                |
| A@B@C   | 288 | A@B@C@C로 처리됩니다.                                                               |
| A@B@C@D | 288 | A는 새 사용자/메일함 이름이 되고 B는 새 호스트/도메인 지정이 되며 C를 소스 경로로 삽입하고 호스트 D와 연관된 채널로 라우팅합니다. |

## 일반 다시 쓰기 템플리트: A%B@C 또는 A@B

다음 템플리트는 가장 일반적인 형식의 템플리트입니다. 주소의 사용자 부분과 주소의 도메인 부분에 규칙이 적용된 다음 새 주소를 사용하여 메일을 특정 채널(*ChannelTag*에 의해 표시된)로 라우팅합니다.

*UserTemplate%DomainTemplate@ChannelTag* [controls]

다음 형식의 템플리트는 그 적용에 있어 가장 일반적인 형식의 템플리트와 동일합니다. 그러나 이 형식의 템플리트는 *DomainTemplate* 및 *ChannelTag*가 동일한 경우에만 가능합니다.

*UserTemplate@ChannelTag* [controls]

## 반복되는 다시 쓰기 템플리트: A%B

다음 템플리트 형식은 규칙이 적용된 후에 추가 다시 쓰기가 필요한 메타 규칙에 사용됩니다. 규칙이 적용된 후 전체 다시 쓰기 프로세스가 새 결과 주소에서 반복됩니다. (다른 모든 다시 쓰기 규칙 형식은 규칙이 적용된 후 프로세스를 종료합니다.)

*UserTemplate%DomainTemplate* [controls]

예를 들어, 다음 규칙은 주소 끝에서 모든 *.removable* 도메인을 제거합니다.

*.removable*      \$U%\$H



이러한 반복 규칙을 사용할 때는 매우 주의해서 다루어야 합니다. 함부로 사용하면 "규칙 루프"가 발생하기 때문입니다. 따라서 메타 규칙은 반드시 필요한 경우에만 사용해야 합니다. `imsimta test -rewrite` 명령을 사용하여 메타 규칙을 테스트합니다. `test -rewrite` 명령에 대한 자세한 내용은 *Messaging Server Reference Manual*을 참조하십시오.

## 지정된 경로 다시 쓰기 템플리트: A@B@C@D 또는 A@B@C

*ChannelTag*가 주소에 소스 경로로 삽입된다는 점을 제외하고 다음 템플리트 형식은 더 일반적인 *UserTemplate%DomainTemplate@ChannelTag* 템플리트와 같은 방식으로 작동합니다(첫 번째 구분자 문자가 다르다는 점에 주의). 그런 다음 메일이 *ChannelTag*로 라우팅 됩니다.

```
UserTemplate@DomainTemplate@Source-Route
    @ChannelTag [controls]
```

다시 작성된 주소는 `@route:user@domain`이 됩니다. 또한 다음 템플리트도 유효합니다.

```
UserTemplate@DomainTemplate@ChannelTag [controls]
```

예를 들어, 다음 규칙은 `jdooe@com1` 주소를 `@siroe.com:jdooe@com1` 소스 라우팅 주소로 다시 씁니다. 채널 태그는 `siroe.com`이 됩니다.

```
com1 $U@com1@siroe.com
```

## 다시 쓰기 규칙 템플리트의 대소문자 구분

다시 쓰기 규칙의 패턴과 달리 템플리트의 대소문자는 유지됩니다. 이것은 다시 쓰기 규칙을 사용하여 대소문자를 구분하는 메일 시스템에 인터페이스를 제공할 때 필요합니다. 주소에서 추출된 자료를 대체하는 `$U` 및 `$D`와 같은 대체 시퀀스도 원래 대소문자를 유지한다는 것에 주의합니다.

대체된 자료에 특정 대소문자를 사용하도록 강제하는 것이 바람직한 경우(예: UNIX 시스템에서 메일함에 소문자를 사용하도록 강제하는 경우) 특수한 대체 시퀀스를 템플리트에 사용하여 대체된 자료에 원하는 대소문자를 적용할 수 있습니다. 특히, `$\`는 대체된 이후의 자료를 소문자로 강제하고 `$^`는 대문자로 강제하며 `$_`는 원래 대소문자를 사용하도록 지정합니다.

예를 들어, 다음 규칙을 사용하여 `unix.siroe.com` 주소에 대해 메일함을 소문자로 강제 지정할 수 있습니다.

```
unix.siroe.com    $\$U$_%unix.siroe.com
```

## MTA가 다시 쓰기 규칙을 주소에 적용하는 방법

다음 단계는 MTA가 다시 쓰기 규칙을 특정 주소에 적용하는 방법을 설명합니다.

1. MTA는 주소에서 첫 번째 호스트 또는 도메인 지정을 추출합니다.

주소는 다음과 같이 둘 이상의 호스트 또는 도메인 이름을 지정할 수 있습니다.

```
jdoe%hostname@siroe.com
```

2. 첫 번째 호스트 또는 도메인 이름을 식별한 후에 MTA는 패턴이 호스트 또는 도메인 이름과 일치하는 다시 쓰기 규칙을 스캔하는 검색을 수행합니다.
3. 일치하는 다시 쓰기 규칙이 발견되면 MTA는 해당 규칙의 템플릿 부분에 따라 주소를 다시 씁니다.
4. 마지막으로 MTA는 채널 태그를 각 채널과 연관된 호스트 이름과 비교합니다.

일치하는 항목이 발견된 경우 MTA는 연관된 채널의 대기열에 메일을 넣고, 그렇지 않을 경우 다시 쓰기 프로세스가 실패합니다. 일치하는 채널이 로컬 채널일 경우 별칭 데이터베이스와 별칭 파일을 조회하여 주소의 일부 추가 다시 쓰기가 발생할 수 있습니다.

이러한 단계는 다음 하위 절에 더욱 자세하게 설명되어 있습니다.

---

**주**            기존 채널에 속하지 않은 채널 태그를 사용하면 주소가 이 규칙과 일치하는 메일이 바운스됩니다. 즉, 일치하는 메일을 라우팅할 수 없게 됩니다.

---

## 단계 1. 첫 번째 호스트 또는 도메인 지정 추출

주소 다시 쓰기 프로세스는 첫 번째 호스트나 도메인 지정을 주소에서 추출하는 것으로 시작됩니다. (RFC 822 주소 규칙에 익숙하지 않은 경우에는 다음 내용을 이해할 수 있도록 이 표준을 읽어보는 것이 좋습니다.) 주소의 호스트/도메인 지정이 스캔되는 순서는 다음과 같습니다.

1. 소스 경로의 호스트(왼쪽에서 오른쪽으로 읽음)
2. "at" 기호(@)의 오른쪽에 있는 호스트
3. 마지막 단일 백분율 기호(%) 오른쪽에 있는 호스트
4. 첫 번째 느낌표(!)의 왼쪽에 있는 호스트

주소 다시 쓰기를 수행하는 채널에서 bangoverpercent 키워드가 적용될 경우(즉, 메일을 대기열에 넣으려고 시도하는 채널 자체가 bangoverpercent 채널 키워드로 표시된 경우) 마지막 두 개 항목의 순서가 바뀝니다.

표 11-3에는 몇 개의 주소와 첫 번째로 추출할 수 있는 호스트 이름의 예가 나와 있습니다.

**표 11-3** 추출된 주소 및 호스트 이름

| 주소                    | 첫 번째 호스트<br>도메인 지정 | 설명                                        |
|-----------------------|--------------------|-------------------------------------------|
| user@a                | a                  | "단순 형식"의 도메인 이름입니다.                       |
| user@a.b.c            | a.b.c              | "정규화된" 도메인 이름(FQDN)입니다.                   |
| user@[0.1.2.3]        | [0.1.2.3]          | "도메인 리터럴"입니다.                             |
| @a:user@b.c.d         | a                  | 단순 형식 도메인 이름, 즉 "route"를 가진 소스 라우팅 주소입니다. |
| @a.b.c:user@d.e.f     | a.b.c              | 소스 라우팅 주소입니다. 경로 부분이 정규화됩니다.              |
| @[0.1.2.3]:user@d.e.f | [0.1.2.3]          | 소스 라우팅 주소입니다. 경로 부분이 도메인 리터럴입니다.          |
| @a,@b,@c:user@d.e.f   | a                  | a, b, c 순서의 라우팅을 가진 소스 라우팅 주소입니다.         |
| @a,@[0.1.2.3]:user@b  | a                  | 경로 부분에 도메인 리터럴이 있는 소스 라우팅 주소입니다.          |
| user%A@B              | B                  | 이 비표준 라우팅 형식은 "백분율 핵"이라고 합니다.             |
| user%A                | A                  |                                           |

**표 11-3** 추출된 주소 및 호스트 이름(계속)

| 주소         | 첫 번째 호스트<br>도메인 지정 | 설명                                     |
|------------|--------------------|----------------------------------------|
| user%A%B   | B                  |                                        |
| user%%A%B  | B                  |                                        |
| A!user     | A                  | "뱅 스타일" 주소 지정입니다. 일반적으로 UUCP에 사용됩니다.   |
| A!user@B   | B                  |                                        |
| A!user%B@C | C                  |                                        |
| A!user%B   | B                  | nobangoverpercent 키워드가 활성화됩니다. 기본값입니다. |
| A!user%B   | A                  | bangoverpercent 키워드가 활성화됩니다.           |

RFC 822는 주소에 있는 느낌표(!)와 백분율 기호(%)의 해석을 다루지 않습니다. at 기호 (@)가 존재하지 않을 경우 백분율 기호는 관례상 at 기호와 동일한 방식으로 해석되며 따라서 Messaging Server MTA에 이 규칙이 적용됩니다.

반복되는 백분율 기호의 특수한 해석은 백분율 기호를 로컬 아이디의 일부로 허용하는 데 사용됩니다. 이것은 일부 외국 메일 시스템 주소를 처리하는 데 유용할 수 있습니다. 느낌표에 대한 해석은 RFC 976의 "뱅 스타일" 주소 규칙을 따르며 Messaging Server MTA에서 UUCP 주소를 사용할 수 있게 합니다.

이러한 해석의 순서는 RFC 822 또는 RFC 976에 지정되어 있지 않으므로 bangoverpercent 및 nobangoverpercent 키워드를 사용하여 다시 쓰기를 수행하는 채널에 의해 적용되는 순서를 제어할 수 있습니다. 대체 설정이 유용할 경우가 있긴 해도 기본값은 "표준"입니다.

---

**주** 주소에서는 느낌표(!) 또는 백분율 기호(%)를 사용하지 않는 것이 좋습니다.

---

## 단계 2. 다시 쓰기 규칙 스캔

첫 번째 호스트 또는 도메인 지정이 주소에서 추출된 후 MTA는 다시 쓰기 규칙을 참조하여 그 처리 방법을 결정합니다. 호스트/도메인 지정은 각 규칙의 패턴 부분(즉, 각 규칙의 왼쪽)과 비교됩니다. 이 비교는 RFC 822에 명시된 대로 대소문자를 구분하지 않습니다. MTA에서는 대소문자를 구분하지 않지만 가능하면 대소문자를 유지합니다.

호스트 또는 도메인 지정이 어떠한 패턴과도 일치하지 않으면(이러한 경우를 "어떠한 규칙과도 일치하지 않음"이라고 함) 호스트 또는 도메인 지정의 첫 번째 부분, 즉 첫 번째 마침표의 앞 부분(대개 호스트 이름)이 제거되고 별표(\*)로 대체된 다음, 구성 파일 다시 쓰기 규칙에서만 결과 호스트 또는 도메인 지정을 찾으려는 또 다른 시도가 수행됩니다(도메인 데이터베이스는 참조되지 않음).

이 시도가 실패하면 첫 번째 부분이 제거되고 프로세스가 반복됩니다. 또 다시 실패할 경우에는 다음 부분(일반적으로 하위 도메인)이 제거되고 다시 쓰기 프로세스가 처음에는 별표를 사용하고 그 다음에는 별표 없이 다시 시도됩니다. 별표를 포함하는 모든 검사는 구성 파일 다시 쓰기 규칙 테이블에서만 수행되며 도메인 데이터베이스는 검사되지 않습니다. 이 프로세스는 일치하는 항목이 발견되거나 전체 호스트 또는 도메인 지정이 사용될 때까지 계속됩니다. 이 절차는 가장 구체적인 도메인을 우선 일치시키고 점차 덜 구체적이면서 더 일반적인 도메인을 일치시키는 방향으로 진행됩니다.

일치 절차의 알고리즘에 대한 자세한 내용은 다음과 같습니다.

- 호스트/도메인 지정이 비교 문자열 spec\_1 및 spec\_2의 초기 값으로 사용됩니다(예: spec\_1 = spec\_2 = a.b.c).
- 일치하는 항목이 발견될 때까지 비교 문자열 spec\_1이 구성 파일에 이어 도메인 데이터베이스에 있는 각 다시 쓰기 규칙의 패턴 부분과 비교됩니다. 일치하는 항목이 발견되면 일치 절차가 종료합니다.
- 일치하는 항목이 발견되지 않을 경우 spec\_2의 별표가 아닌 맨 왼쪽 부분이 별표로 변환됩니다. 예를 들어, spec\_2는 a.b.c인 경우 \*.b.c로 변경되고 \*.b.c인 경우 \*.\*.c로 변경됩니다. 일치하는 항목이 발견되면 일치 절차가 종료합니다.
- 일치하는 항목이 발견되지 않을 경우 선행 마침표를 포함한 비교 문자열 spec\_1의 첫 번째 부분이 제거됩니다. spec\_1이 한 부분으로만 구성된 경우(예: .c 또는 c) 문자열은 마침표"."로 바꿉니다. 결과 문자열 spec\_1의 길이가 0이 아닌 경우 단계 1로 돌아갑니다. 결과 문자열의 길이가 0인 경우(예: 이전에 "."경우) 조회 프로세스가 실패하고 일치 절차가 종료됩니다.

예를 들어, dan@sc.cs.siroe.edu 주소를 다시 작성한다고 가정해 봅시다. 이 경우 MTA는 다음 패턴을 주어진 순서대로 찾습니다.

```
sc.cs.siroe.edu
*.cs.siroe.edu
.cs.siroe.edu
*.*.siroe.edu
.siroe.edu
*.*.*.edu
.edu
*.*.*.*
.
```

### 단계 3. 템플릿에 따라 주소 다시 쓰기

호스트/도메인 지정은 다시 쓰기 규칙과 일치할 경우 규칙의 템플릿 부분에 따라 다시 작성됩니다. 템플릿은 다음 세 가지 정보를 지정합니다.

1. 주소의 새 아이디
2. 주소의 새 호스트/도메인 지정
3. 이 주소에 대한 메일을 보내야 하는 기존 MTA 채널을 식별하는 채널 태그

### 단계 4. 다시 쓰기 프로세스 완료

호스트/도메인 지정이 다시 작성된 후 다음 작업 중 하나가 수행될 수 있습니다.

- 채널 태그가 로컬 채널 및 routelocal 채널 키워드로 표시된 채널과 관련이 없거나 주소에 추가 호스트/도메인 지정이 없을 경우 다시 작성된 지정은 다시 쓰기를 위해 추출된 원래 지정을 대체하는 주소로 대체되고 다시 쓰기 프로세스가 종료합니다.
- 채널 태그가 로컬 채널이나 routelocal로 표시된 채널과 일치하거나 주소에 추가 호스트/도메인 지정이 있을 경우 다시 작성된 주소를 버리고 원래(초기) 호스트/도메인 지정이 주소에서 제거되며 새 호스트/도메인 지정이 주소에서 추출된 후 전체 프로세스가 반복됩니다. 다시 쓰기는 모든 호스트/도메인 지정이 사라지거나 로컬이 아닌 채널 또는 routelocal이 아닌 채널을 통한 경로가 발견될 때까지 계속됩니다.

이 반복 기법은 MTA가 소스 라우팅에 대한 지원을 제공하는 방법입니다. 실제로 로컬 시스템 및 `routelocal` 시스템을 통과하는 여분의 경로는 이 프로세스에 의해 주소에서 제거됩니다.

## 다시 쓰기 규칙 실패

호스트 도메인 지정이 다시 쓰기 규칙과 일치하는 데 실패하거나 기본 규칙이 존재하지 않을 경우 MTA는 지정을 "있는 그대로" 사용합니다. 예를 들어, 원래 지정은 새 지정과 라우팅 시스템 모두가 됩니다. 주소에 유효하지 않은 호스트/도메인 지정이 있을 경우 라우팅 시스템이 임의 채널과 연관된 어떠한 시스템 이름과도 일치하지 않을 때 이점이 감지되며 메일이 바운스됩니다.

## 다시 쓰기 후의 구문 검사

다시 쓰기 규칙이 주소에 적용된 후 추가 구문 검사가 수행되지 않습니다. RFC 822를 따르지 않는 형식으로 주소를 변환하는 데 다시 쓰기 규칙이 사용될 수 있다는 점에서 일부러 이러한 검사가 수행되지 않는 것입니다. 그러나 이것은 또한 구성 파일의 실수로 인해 MTA에서 잘못된 또는 유효하지 않은 주소를 가진 메일이 보내질 수 있다는 것을 의미합니다.

## 도메인 리터럴 처리

도메인 리터럴은 다시 쓰기 프로세스 동안 특수하게 처리됩니다. 주소의 도메인 부분에 있는 도메인 리터럴이 다시 쓰기 규칙 패턴과 일치하지 않을 경우 이러한 리터럴은 마침표로 구분하고 대괄호로 묶은 문자열 그룹으로 해석됩니다. 맨 오른쪽의 문자열이 제거되며 검색이 반복됩니다. 이 작업이 수행되지 않을 경우 빈 대괄호만 남을 때까지 다음 문자열이 제거됩니다. 빈 대괄호에 대한 검색이 실패하면 전체 도메인 리터럴이 제거되고 도메인 주소의 다음 섹션(있을 경우)에서 다시 쓰기가 진행됩니다. 도메인 리터럴의 내부 처리에서 별표는 사용되지 않습니다. 전체 도메인 리터럴이 별표로 대체될 경우 별표 수는 도메인 리터럴의 요소 수에 해당합니다.

일반 도메인 또는 호스트 지정과 마찬가지로 도메인 리터럴은 또한 가장 구체적인 순서에서 가장 일반적인 순서로 시도됩니다. 해당 패턴이 일치하는 첫 번째 규칙은 호스트 또는 도메인 지정을 다시 쓰는 데 사용되는 규칙입니다. 규칙 목록에 두 개의 동일한 패턴이 있을 경우 먼저 표시된 규칙이 사용됩니다.

예를 들어, dan@[128.6.3.40] 주소를 다시 작성한다고 가정해 봅니다. 다시 쓰기 프로세스는 [128.6.3.40], [128.6.3.], [128.6.], [128.], [], [\*.\*.\*.\*]를 차례로 찾은 다음 마지막으로 모두 일치 규칙 "."를 찾습니다.

## 템플릿 대체 및 다시 쓰기 규칙 제어 시퀀스

대체는 문자열을 다시 작성된 주소(사용된 특정 대체 시퀀스에 의해 결정되는 값)에 삽입하여 아이디나 주소를 다시 쓰는 데 사용됩니다. 이 절은 다음과 같은 하위 절로 구성되어 있습니다.

- 299페이지의 "아이디 및 하위 주소 대체: \$U, \$OU, \$1U"
- 300페이지의 "호스트/도메인 및 IP 리터럴 대체: \$D, \$H, \$nD, \$nH, \$L"
- 300페이지의 "리터럴 문자 대체: \$\$, \$%, \$@"
- 300페이지의 "LDAP 쿼리 URL 대체: \$]...["
- 302페이지의 "일반 데이터베이스 대체: \$(...)"
- 302페이지의 "지정된 매핑 적용: \${...}"
- 303페이지의 "사용자 제공 루틴 대체: \$[...]"
- 304페이지의 "단일 필드 대체: \$&, \$!, \$\*, \$#"
- 304페이지의 "고유 문자열 대체"
- 305페이지의 "소스 채널 특정 다시 쓰기 규칙: \$M, \$N"
- 305페이지의 "대상 채널 특정 다시 쓰기 규칙: \$C, \$Q"
- 307페이지의 "호스트 위치별 다시 쓰기: \$A, \$P, \$S, \$X"
- 307페이지의 "현재 태그 값 변경: \$T"
- 308페이지의 "다시 쓰기와 관련된 오류 메시지 처리: \$?"

예를 들어, 다음 템플릿에서 \$U는 대체 시퀀스입니다. 이 대체 시퀀스는 템플릿의 출력에서 다시 쓰는 주소의 *username* 부분을 대체시킵니다. 따라서 이 템플릿으로 jdoe@mailhost.siroe.com이 다시 작성된 경우 \$U가 원래 주소의 *username* 부분인 jdoe로 대체되어 결과 출력은 jdoe@siroe.com이 됩니다.

\$U@siroe.com



제어 시퀀스는 특정 다시 쓰기 규칙의 적용 가능성에 추가 조건을 부과합니다. 다시 쓰기 규칙의 패턴 부분이 검사되는 호스트 또는 도메인 지정과 일치해야 할 뿐만 아니라 다시 쓰는 주소의 다른 측면에서 제어 시퀀스에 의해 설정된 조건을 충족해야 합니다. 예를 들어, 다시 쓰는 주소는 \$E 제어 시퀀스가 있을 경우 봉투 주소여야 하며 \$F 제어 시퀀스가 있을 경우 정방향 지정 주소여야 합니다. 다음 다시 쓰기 규칙은 user@siroe.com 형식의 (다시 쓰기) 봉투의 To: 주소에만 적용됩니다.

siroe.com \$U@mail.siroe.com\$E\$F

도메인 또는 호스트 지정이 다시 쓰기 규칙의 패턴 부분과 일치하지만 규칙 템플릿의 제어 시퀀스가 부과한 모든 조건을 충족하지 않을 경우 다시 쓰기 규칙은 실패하고 다른 적용 가능한 규칙을 찾기 위해 다시 쓰기 프로세스가 계속됩니다.

표 11-4에는 템플릿 대체와 제어 시퀀스가 요약되어 있습니다.

**표 11-4** 다시 쓰기 규칙 템플릿 대체 및 제어 시퀀스 요약

| 대체 시퀀스 | 대체 대상                                                           |
|--------|-----------------------------------------------------------------|
| \$D    | 일치한 도메인 지정 부분                                                   |
| \$H    | 호스트/도메인 지정의 일치하지 않는 부분(패턴에 있는 점의 왼쪽)                            |
| \$L    | 도메인 리터럴의 일치하지 않는 부분(패턴 리터럴에 있는 점의 오른쪽)                          |
| \$U    | 원래 주소의 아이디                                                      |
| \$nA   | 위치 0에서 시작하여 현재 주소의 n번째 왼쪽 문자를 삽입합니다. n을 생략하면 전체 주소가 삽입됩니다.      |
| \$nX   | 0에서 시작하여 메일 호스트의 n번째 왼쪽 구성 요소를 삽입합니다. n을 생략하면 전체 메일 호스트가 삽입됩니다. |
| \$0U   | 원래 주소에서 모든 하위 주소를 뺀 로컬 부분(아이디)                                  |
| \$1U   | 원래 주소의 로컬 부분(아이디)에 있는 하위 주소(있을 경우)                              |
| \$\$   | 리터럴 달러 기호(\$) 삽입                                                |
| \$\$   | 리터럴 백분율 기호(%) 삽입                                                |
| \$@    | 리터럴 at 기호(@) 삽입                                                 |
| \$\$   | 모두 소문자로 적용                                                      |
| \$\$   | 모두 대문자로 적용                                                      |
| \$_    | 원래 대소문자 사용                                                      |
| \$=    | 대체된 후속 문자가 LDAP 검색 필터에 삽입하기 적합하게 인용되도록 합니다. 모두 대문자로 적용합니다.      |

**표 11-4** 다시 쓰기 규칙 템플릿 대체 및 제어 시퀀스 요약(계속)

| 대체 시퀀스             | 대체 대상                                                                  |
|--------------------|------------------------------------------------------------------------|
| \$W                | 임의의 고유 문자열로 대체                                                         |
| \$]...[            | LDAP 검색 URL 조회                                                         |
| \$(text)           | 일반 데이터베이스 대체(조회에 실패할 경우 규칙이 실패함)                                       |
| \${...}            | 지정된 매핑을 제공된 문자열에 적용                                                    |
| \$[...]            | 사용자 제공 루틴 호출(결과로 대체)                                                   |
| \$&n               | 일치하지 않는(와일드카드로 표시된) 호스트의 <i>n</i> 번째 부분(0부터 시작하여 왼쪽에서 오른쪽으로 계산)        |
| !\$n               | 일치하지 않는(와일드카드로 표시된) 호스트의 <i>n</i> 번째 부분(0부터 시작하여 오른쪽에서 왼쪽으로 계산)        |
| *\$n               | 일치하는 패턴의 <i>n</i> 번째 부분(0부터 시작하여 왼쪽에서 오른쪽으로 계산)                        |
| #n                 | 일치하는 패턴의 <i>n</i> 번째 부분(0부터 시작하여 오른쪽에서 왼쪽으로 계산)                        |
| \$nD               | 일치한 도메인 지정 부분(0부터 시작하는 <i>n</i> 번째 맨 왼쪽 부분부터 대체)                       |
| \$nH               | 일치하지 않는 호스트/도메인 지정 부분(0부터 시작하는 <i>n</i> 번째 맨 왼쪽 부분부터 대체)               |
| 제어 시퀀스             | 다시 쓰기 규칙에 미치는 영향                                                       |
| \$!M               | 채널이 내부 재처리 채널일 경우에만 적용됩니다.                                             |
| \$!N               | 채널이 내부 재처리 채널이 아닐 경우에만 적용됩니다.                                          |
| \$!~               | 보류 중인 모든 채널 일치 검사를 수행합니다. 검사가 실패할 경우 현재 다시 쓰기 규칙 템플릿의 처리가 성공적으로 종료합니다. |
| \$A                | 호스트가 at 기호의 오른쪽에 있을 경우 적용됩니다.                                          |
| \$B                | 헤더/본문 주소에만 적용됩니다.                                                      |
| \$C <i>channel</i> | <i>channel</i> 로 보낼 경우 실패합니다.                                          |
| \$E                | 봉투 주소에만 적용됩니다.                                                         |
| \$F                | 정방향 지정(예: To:) 주소                                                      |
| \$M <i>channel</i> | <i>channel</i> 이 주소를 다시 쓰는 경우에만 적용됩니다.                                 |
| \$N <i>channel</i> | <i>channel</i> 이 주소를 다시 쓰는 경우 실패합니다.                                   |
| \$P                | 호스트가 백분율 기호의 오른쪽에 있을 경우 적용됩니다.                                         |
| \$Q <i>channel</i> | <i>channel</i> 로 보낼 경우 적용됩니다.                                          |
| \$R                | 역방향 지정(예: From:) 주소                                                    |
| \$S                | 호스트가 소스 경로에서 온 경우 적용됩니다.                                               |
| \$T <i>newtag</i>  | 다시 쓰기 규칙 태그를 <i>newtag</i> 로 설정합니다.                                    |

**표 11-4** 다시 쓰기 규칙 템플리트 대체 및 제어 시퀀스 요약(계속)

| 대체 시퀀스                       | 대체 대상                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>\$Vhost</code>         | 호스트 이름이 LDAP 디렉토리(DC 트리에 있거나 가상 도메인으로 존재)에 정의되지 않은 경우 실패합니다. LDAP 검색의 시간이 초과되면 호스트 이름 다음의 문자 바로 뒤부터 시작하는 다시 쓰기 패턴의 나머지 부분은 MTA 옵션 문자열 <code>DOMAIN_FAILURE</code> 로 대체됩니다.                                                                                                                                                                                                                                                                   |
| <code>\$X</code>             | 호스트가 느낌표의 왼쪽에 있을 경우 적용됩니다.                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <code>\$Zhost</code>         | 호스트 이름이 LDAP 디렉토리(DC 트리에 있거나 가상 도메인으로 존재)에 정의된 경우 실패합니다. LDAP 검색의 시간이 초과되면 호스트 이름 다음의 문자 바로 뒤부터 시작하는 다시 쓰기 패턴의 나머지 부분은 MTA 옵션 문자열 <code>DOMAIN_FAILURE</code> 로 대체됩니다.                                                                                                                                                                                                                                                                       |
| <code>\$?errmsg</code>       | 다시 쓰기가 실패할 경우 기본 오류 메시지 대신에 <code>errmsg</code> 를 반환합니다. 오류 메시지는 US ASCII여야 합니다.                                                                                                                                                                                                                                                                                                                                                             |
| <code>\$number?errmsg</code> | 다시 쓰기가 실패할 경우 기본 오류 메시지 대신에 <code>errmsg</code> 를 반환하고 SMTP 확장 오류 코드를 <code>a.b.c</code> 로 설정합니다. <ul style="list-style-type: none"> <li><code>a</code>는 <code>number/1000000</code>(첫 번째 자리 값)</li> <li><code>b</code>는 <code>(number/1000)</code> 나머지 1000(두 번째에서 네 번째 자리의 값)</li> <li><code>c</code>는 <code>number</code> 나머지 1000(마지막 세 개 자리의 값)</li> </ul> 다음 예는 오류 코드를 3.45.89로 설정합니다.<br><code>\$3045089?the snark is a boojum</code> |

## 아이디 및 하위 주소 대체: \$U, \$0U, \$1U

템플리트의 모든 \$U는 원래 주소의 아이디(RFC 822 "로컬 부분")로 대체됩니다. a."b" 형식의 아이디가 "a.b"로 대체된다는 것에 주의합니다. 이는 RFC2822에서 RFC 822에 명시된 전자의 형식을 반대하고 있으며 앞으로 후자의 형식이 필수 형식이 될 것으로 예상되기 때문입니다.

템플리트의 모든 \$0U는 하위 주소 및 하위 주소 표시 문자(+)를 빼고 원래 주소의 아이디로 대체됩니다. 템플리트의 모든 \$1U는 원래 주소의 하위 주소 및 하위 주소 표시 문자(있을 경우)로 대체됩니다. 따라서 \$0U 및 \$1U가 아이디의 보완적 부분이며 \$0U\$1U는 \$U와 동일하다는 것에 주의합니다.

## 호스트/도메인 및 IP 리터럴 대체: \$D, \$H, \$nD, \$nH, \$L

모든 \$H는 규칙에 의해 일치되지 않은 호스트/도메인 지정 부분으로 대체됩니다. 모든 \$D는 다시 쓰기 규칙에 의해 일치된 호스트/도메인 지정 부분으로 대체됩니다. \$nH 및 \$nD 문자는 0부터 계산되는 n번째 맨 왼쪽 부분에서 일반 \$H 또는 \$D 부분을 대체합니다. 즉, \$nH 및 \$nD는 각각 \$H 또는 \$D 대체의 맨 왼쪽에서 1부터 계산되는 n개의 부분을 생략합니다. 특히, \$0H는 \$H와 동일하며 \$0D는 \$D와 동일합니다.

예를 들어, jdoe@host.siroe.com 주소가 다음 다시 쓰기 규칙과 일치한다고 가정해 봅니다.

```
host.siroe.com    $U%$1D@TCP-DAEMON
```

결과 주소는 TCP-DAEMON을 보내는 채널로 사용하는 jdoe@siroe.com입니다. 여기에서 \$D는 일치한 전체 도메인 host.siroe.com으로 대체될 것이지만 \$1D는 첫 번째 항목 (siroe)으로부터 일치하는 부분으로 대체되므로 siroe.com으로 대체됩니다.

\$L은 다시 쓰기 규칙에 의해 일치되지 않은 도메인 리터럴 부분을 대체합니다.

## 리터럴 문자 대체: \$\$, \$%, \$@

\$, % 및 @ 문자는 일반적으로 다시 쓰기 규칙 템플릿에서 메타 문자입니다. 이러한 문자의 리터럴 삽입을 수행하려면 달러 문자 \$를 사용하여 해당 문자를 인용합니다. 즉, \$\$는 단일 달러 기호 \$로 확장되고 \$%는 단일 백분율 %(이 경우 백분율은 템플릿 필드 구분자로 해석되지 않음)로 확장되며 \$@은 단일 at 기호 @(마찬가지로 필드 구분자로 해석되지 않음)으로 확장됩니다.

## LDAP 쿼리 URL 대체: \$]...[

\$]ldap-ur1[ 형식의 대체는 LDAP 쿼리 URL로 해석되며 LDAP 쿼리 결과가 대체됩니다. 표준 LDAP URL은 호스트와 포트가 생략된 채로 사용됩니다. 호스트와 포트는 대신 msg.conf 파일(local.ldaphost 및 local.ldapport 속성)에서 지정됩니다.

즉, LDAP URL은 다음과 같이 지정해야 하며 여기에서 대괄호 문자 [ ]는 URL의 선택적 부분을 나타냅니다.

ldap:///dn[?attributes[?scope?filter]]

dn은 필수 항목으로서 검색 기준을 지정하는 고유 이름입니다. URL의 선택적 속성, 범위 및 필터 부분은 반환할 정보를 더욱 구체화합니다. 다시 쓰기 규칙의 경우 반환 지정을 위한 속성은 mailRoutingSystem 속성(또는 이와 유사한 속성)이 될 수 있습니다. 범위는 base(기본값), one 또는 sub가 될 수 있으며 필터는 mailDomain 값이 다시 쓰는 도메인과 일치하는 객체의 반환을 요청하는 것이 될 수 있습니다.

LDAP 디렉토리 스키마가 mailRoutingSystem 및 mailDomain 속성을 포함할 경우 주어진 주소를 라우팅할 시스템을 결정하기 위한 다시 쓰기 규칙은 다음과 같이 나타날 수 있습니다. 여기에서 LDAP URL 대체 시퀀스 \$D는 현재 도메인 이름을 생성된 LDAP 쿼리로 대체하는 데 사용됩니다.

```
.siroe.com \
  $U%$H$D@$]ldap:///o=siroe.com?mailRoutingSystem?sub? \
  (mailDomain=$D)
```

백슬래시 문자는 쉽게 알아볼 수 있도록 하나의 논리적 다시 쓰기 규칙 행을 계속해서 두 번째 물리적 행으로 이어주는 데 사용됩니다. 표 11-5에는 LDAP URL 대체 시퀀스가 나열되어 있습니다.

**표 11-5** LDAP URL 대체 시퀀스

| 대체 시퀀스             | 설명                           |
|--------------------|------------------------------|
| \$\$               | 리터럴 \$ 문자                    |
| \$~ <i>account</i> | 사용자 계정의 홈 디렉토리               |
| \$A                | 주소                           |
| \$D                | 도메인 이름                       |
| \$H                | 호스트 이름(정규화된 도메인 이름의 첫 번째 부분) |
| \$L                | ~ 또는 _와 같은 특수한 선행 문자를 뺀 아이디  |
| \$S                | 하위 주소                        |
| \$U                | 아이디                          |

MTA는 이제 다시 쓰기 규칙 및 매핑에서 수행된 조회에서 URL 결과를 캐시합니다. 이 새 URL 결과 캐시는 두 개의 새로운 MTA 옵션, 즉 URL\_RESULT\_CACHE\_SIZE(기본값은 10000개 항목) 및 URL\_RESULT\_CACHE\_TIMEOUT(기본값은 600초)에 의해 제어됩니다.

## 일반 데이터베이스 대체: \$(...)

\$(텍스트) 형식의 대체는 특수하게 처리됩니다. 텍스트 부분은 특수한 일반 데이터베이스에 액세스하기 위한 키로 사용됩니다. 이 데이터베이스는 /imta/config/imta\_tailor 파일의 IMTA\_GENERAL\_DATABASE 옵션으로 지정하는 파일(일반적으로 /imta/db/generaldb.db)로 구성됩니다.

이 데이터베이스는 imsimta crdb 유틸리티를 사용하여 생성합니다. 데이터베이스에서 "text-string"이 발견될 경우 데이터베이스의 해당 템플릿이 대체됩니다. "text-string" 데이터베이스의 항목과 일치하지 않을 경우 다시 쓰기 프로세스는 실패합니다(다시 쓰기 규칙이 처음에 일치하지 않은 것과 같음). 대체에 성공할 경우 추가 대체를 위해 데이터베이스에서 추출된 템플릿이 다시 스캔됩니다. 그러나 참조가 무한대로 반복되는 것을 방지하기 위해 추출된 템플릿의 추가 \$(텍스트) 대체는 금지됩니다.

예를 들어, jdoe@siroe.siroenet 주소가 다음 다시 쓰기 규칙과 일치한다고 가정해 봅시다.

```
.SIROENET $(SH)
```

이 경우 텍스트 문자열 siroe가 일반 데이터베이스에서 조회되고 조회 결과(있을 경우)가 다시 쓰기 규칙의 템플릿에 사용됩니다. siroe를 조회한 결과는 \$u%eng.siroe.com@siroenet이라고 가정해 봅시다. 그러면 템플릿 출력은 jdoe@eng.siroe.com(즉, 아이디 = jdoe, 호스트/도메인 지정 = eng.siroe.com)이 되고 라우팅 시스템은 siroenet이 됩니다.

일반 데이터베이스(존재할 경우)는 제대로 작동하려면 세계 공용이어야 합니다.

## 지정된 매핑 적용: \${...}

.SIROENET \$(SH) \${mapping, argument} 형식의 대체는 MTA 매핑 파일에서 매핑을 찾아 적용하는 데 사용됩니다. mapping 필드는 사용할 매핑 테이블의 이름을 지정하며 argument는 매핑에 전달할 문자열을 지정합니다. 매핑은 존재해야 하며 성공적일 경우 해당 출력에 \$Y 플래그를 설정해야 합니다. 매핑이 존재하지 않거나 \$Y를 설정하지 않을 경우 다시 쓰기가 실패합니다. 성공적일 경우 매핑 결과가 현재 위치에서 템플릿에 병합되고 다시 확장됩니다.

이 기법을 통해 MTA 다시 쓰기 프로세스는 복잡한 여러 방법으로 확장될 수 있습니다. 예를 들어, 주소의 아이디 부분을 선택적으로 분석 및 수정할 수 있습니다(일반적으로 MTA 다시 쓰기 프로세스에서 불가능한 기능임).

## 사용자 제공 루틴 대체: \$[...]

$\$(image, routine, argument)$  형식의 대체는 사용자 제공 루틴을 검색 및 호출하는 데 사용됩니다. UNIX의 런타임에서 MTA는 `dlopen` 및 `dlsym`을 사용하여 공유 라이브러리 이미지에서 지정된 루틴을 동적으로 로드 및 호출합니다. 그런 다음 루틴은 다음 인수 목록과 함께 함수로 호출됩니다.

```
status := routine (argument, arglength, result, reslength)
```

*argument* 및 *result*는 252바이트 길이의 문자열 버퍼입니다. UNIX에서 *argument* 및 *result*는 문자열에 대한 포인터로 전달됩니다(예: C에서는 `char*`로 전달됨). *arglength* 및 *reslength*는 참조에 의해 전달되는 서명된 정수(Long)입니다. 입력 시에 *argument*는 다시 쓰기 규칙 템플릿의 인수 문자열을 포함하며 *arglength*는 해당 문자열의 길이를 포함합니다. 반환 시에 결과 문자열은 *result*에 포함되고 그 길이는 *reslength*에 포함되어야 합니다. 그런 다음 해당 결과 문자열은 다시 쓰기 규칙 템플릿의  $\$(image, routine, argument)$ 를 대체합니다. 루틴은 다시 쓰기 규칙이 실패할 경우 0을 반환하고 성공할 경우 -1을 반환합니다.

이 기법을 통해 다시 쓰기 프로세스는 모든 종류의 복잡한 방법으로 확장될 수 있습니다. 예를 들어, 일부 유형의 이름 서비스에 대한 호출을 수행하고 그 결과를 사용하여 주소를 일정한 방식으로 변경할 수 있습니다. 호스트 `siroe.com`에 대한 정방향 지정 주소(예: To: 주소)에 대해 다음 다시 쓰기 규칙을 사용하여 디렉토리 서비스 조회를 수행할 수 있습니다. 306페이지의 "방향 및 위치 특정 다시 쓰기 규칙: \$B, \$E, \$F, \$R"에 설명된 \$F는 정방향 지정 주소에 대해서만 이 규칙이 사용되도록 합니다.

```
siroe.com $F$[LOOKUP_IMAGE,LOOKUP,$U]
```

정방향 지정 주소 `jdoe@siroe.com`은 이 다시 쓰기 규칙과 일치할 경우 `LOOKUP_IMAGE`(UNIX의 공유 라이브러리)가 메모리에 로드된 다음 `LOOKUP` 루틴이 인수 매개 변수로 `jdoe`와 함께 호출되게 합니다. 그런 다음 `LOOKUP` 루틴은 결과 매개 변수에서 다른 주소, 즉 `John.Doe@eng.siroe.com`과 다시 쓰기 규칙이 성공했음을 나타내는 값 -1을 반환할 수 있습니다. 결과 문자열의 백분율 기호(288페이지의 "반복되는 다시 쓰기 템플릿: A%B" 참조)는 `John.Doe@eng.siroe.com`을 다시 쓸 주소로 사용하여 다시 쓰기 프로세스가 다시 시작되게 합니다.

UNIX 시스템에서 사이트 제공 공유 라이브러리 이미지는 세계 공용이어야 합니다.

## 단일 필드 대체: \$&, \$!, \$\*, \$#

단일 필드 대체는 다시 쓰는 호스트/도메인 지정에서 단일 하위 도메인 부분을 추출합니다. 표 11-6에는 사용 가능한 단일 필드 대체가 나와 있습니다.

**표 11-6** 단일 필드 대체

| 제어 시퀀스 | 사용                                                                                                                                |
|--------|-----------------------------------------------------------------------------------------------------------------------------------|
| \$&n   | 호스트 지정에서 n번째 요소(n=0,1,2,...,9)를 대체합니다(일정한 와일드카드와 일치하지 않았거나 일치한 부분). 요소는 점으로 구분되며 왼쪽의 첫 번째 요소가 요소 0입니다. 요청한 요소가 없으면 다시 쓰기가 실패합니다.  |
| \$!n   | 호스트 지정에서 n번째 요소(n=0,1,2,...,9)를 대체합니다(일정한 와일드카드와 일치하지 않았거나 일치한 부분). 요소는 점으로 구분되며 오른쪽의 첫 번째 요소가 요소 0입니다. 요청한 요소가 없으면 다시 쓰기가 실패합니다. |
| \$*n   | 도메인 지정에서 n번째 요소(n=0,1,2,...,9)를 대체합니다(패턴의 명시적 텍스트와 일치하지 않은 부분). 요소는 점으로 구분되며 왼쪽의 첫 번째 요소가 요소 0입니다. 요청한 요소가 없으면 다시 쓰기가 실패합니다.      |
| \$#n   | 도메인 지정에서 n번째 요소(n=0,1,2,...,9)를 대체합니다(패턴의 명시적 텍스트와 일치하지 않은 부분). 요소는 점으로 구분되며 오른쪽의 첫 번째 요소가 요소 0입니다. 요청한 요소가 없으면 다시 쓰기가 실패합니다.     |

jdoh@eng.siroe.com 주소가 다음 다시 쓰기 규칙과 일치한다고 가정해 봅시다.

```
*.SIROE.COM $U%$&0.siroe.com@mailhub.siroe.com
```

이 경우 템플릿의 결과는 jdoh@eng.siroe.com이 되며 mailhub.siroe.com이 라우팅 시스템으로 사용됩니다.

## 고유 문자열 대체

\$W 제어 시퀀스를 사용할 때마다 대문자 및 숫자로 구성된 반복되지 않는 고유한 텍스트 문자열이 삽입됩니다. 반복되지 않는 주소 정보를 생성해야 할 경우에 \$W가 유용합니다.



## 소스 채널 특정 다시 쓰기 규칙: \$M, \$N

특정 소스 채널에 대해서만 작동하는 다시 쓰기 규칙을 지정할 수 있습니다. 이것은 단순 형식의 이름이 다음과 같이 두 개의 의미를 가질 경우에 유용합니다.

1. 특정 채널에 도착하는 메일에 나타날 경우
2. 다른 채널에 도착하는 메일에 나타날 경우

소스 채널 특정 다시 쓰기는 사용 중인 채널 프로그램과 rules 및 norules 채널 키워드와 연관됩니다. 다시 쓰기를 수행 중인 MTA 구성 요소와 연관된 채널에서 norules가 지정된 경우 채널 특정 다시 쓰기 검사가 수행되지 않습니다. 이러한 채널에 rules가 지정된 경우에는 채널 특정 규칙 검사가 적용됩니다. rules 키워드가 기본값입니다.

소스 채널 특정 다시 쓰기는 주어진 주소와 일치하는 채널과 연관되지 않으며 다시 쓰기를 수행하는 MTA 구성 요소와 이 구성 요소의 채널 테이블 항목에만 의존합니다.

채널 특정 다시 쓰기 검사는 규칙의 템플릿 부분에 있는 \$N 또는 \$M 제어 시퀀스의 존재에 의해 트리거됩니다. \$N 또는 \$M 뒤에서부터 at 기호(@), 백분율 기호(%) 또는 후속 \$N, \$M, \$Q, \$C, \$T 또는 \$?의 앞 부분에 있는 문자는 채널 이름으로 해석됩니다.

예를 들어, \$Mchannel의 경우 channel이 현재 다시 쓰기를 수행 중이 아니면 규칙이 실패하고 \$Nchannel의 경우 channel이 다시 쓰기를 수행 중이면 규칙이 실패합니다. 여러 \$M 및 \$N 절을 지정할 수 있습니다. 여러 \$M 절 중 하나가 일치하면 규칙이 성공하며 여러 \$N 절 중 하나가 일치하면 규칙이 실패합니다.

## 대상 채널 특정 다시 쓰기 규칙: \$C, \$Q

메일을 대기열에 넣는 채널에 의존하여 다시 쓰기 규칙이 적용될 수 있습니다. 이것은 일부 호스트에 대한 두 개의 이름, 즉 특정 호스트 그룹에 알려진 이름과 다른 호스트 그룹에 알려진 이름이 존재할 경우에 유용합니다. 다른 채널을 사용하여 메일을 각 그룹에 보내면 주소를 다시 작성하여 각 그룹에 알려진 이름으로 호스트를 참조할 수 있습니다.

대상 채널 특정 다시 쓰기는 메일을 대기열에서 빼고 처리하는 채널과 해당 채널의 rules 및 norules 채널 키워드와 연관됩니다. 대상 채널에 norules가 지정된 경우 채널 특정 다시 쓰기 검사가 수행되지 않습니다. 대상 채널에 rules가 지정된 경우 채널 특정 규칙 검사가 적용됩니다. rules 키워드가 기본값입니다.

대상 채널 특정 다시 쓰기는 주어진 주소와 일치하는 채널과 연관되지 않습니다. 대상 채널 특정 다시 쓰기는 메일의 봉투 To:주소에만 의존합니다. 메일을 대기열에 넣을 때 대상 채널을 결정하기 위해 메일 봉투의 To:주소가 우선적으로 다시 작성됩니다. envelope To:주소를 다시 쓰는 동안 \$C 및 \$Q 제어 시퀀스는 무시됩니다. envelope To:주소가 다시 작성되고 대상 채널이 결정되면 메일과 연관된 다른 주소가 다시 작성될 때 \$C 및 \$Q 제어 시퀀스가 적용됩니다.

대상 채널 특정 다시 쓰기 검사는 규칙의 템플릿 부분에 있는 \$C 또는 \$Q 제어 시퀀스의 존재에 의해 트리거됩니다. \$C 또는 \$Q 뒤에서부터 at 기호(@), 백분율 기호(%) 또는 후속 \$N, \$M, \$C, \$Q, \$T 또는 \$?의 앞 부분에 있는 문자는 채널 이름으로 해석됩니다.

예를 들어, \$Qchannel의 경우 channel이 대상이 아니면 규칙이 실패하고 \$Cchannel의 경우 channel이 대상이면 규칙이 실패합니다. 여러 \$Q 및 \$C 절을 지정할 수 있습니다. 여러 \$Q 절 중 하나가 일치하면 규칙이 성공하며 여러 \$C 절 중 하나가 일치하면 규칙이 실패합니다.

## 방향 및 위치 특정 다시 쓰기 규칙: \$B, \$E, \$F, \$R

경우에 따라 봉투 주소 또는 헤더 주소에만 적용되는 다시 쓰기 규칙을 지정해야 합니다. 제어 시퀀스 \$B는 다시 쓰는 주소가 봉투 주소가 아닐 경우 다시 쓰기가 실패하도록 지정하며 \$B는 다시 쓰는 주소가 메일 헤더나 본문에서 오지 않은 경우 다시 쓰기가 실패하도록 지정합니다. 이러한 시퀀스는 다시 쓰기에 다른 영향을 미치지 않으며 다시 쓰기 규칙 템플릿의 임의 위치에 나타날 수 있습니다.

주소를 또한 방향별로 범주화할 수 있습니다. 정방향 지정 주소는 To:, Cc:, Resent-to: 또는 대상을 나타내는 다른 헤더 또는 봉투 행에서 시작되는 주소입니다. 역방향 지정 주소는 소스를 나타내는 From:, Sender: 또는 Resent-From: 과 같은 주소입니다. 제어 시퀀스 \$F는 주소가 정방향 지정일 경우에 다시 쓰기를 적용하도록 지정하며 \$R은 주소가 역방향 지정일 경우에 다시 쓰기를 적용하도록 지정합니다.

## 호스트 위치별 다시 쓰기: \$A, \$P, \$S, \$X

경우에 따라 주소에서 호스트 이름이 나타나는 위치가 중요한 다시 쓰기가 필요할 수 있습니다. 호스트 이름은 다음과 같이 주소의 여러 다른 컨텍스트에 나타날 수 있습니다.

- 소스 경로 내
- at 기호(@)의 오른쪽
- 로컬 부분에 있는 백분율 기호(%)의 오른쪽
- 로컬 부분에 있는 느낌표의 왼쪽

정상적인 경우라면 호스트 이름은 표시 위치에 상관 없이 동일하게 처리되어야 합니다. 일부 상황에서는 특수한 처리가 필요할 수 있습니다.

주소에서의 호스트 위치에 기초한 일치를 제어하기 위해 네 개의 제어 시퀀스가 사용됩니다.

- \$s는 규칙이 소스 경로에서 추출된 호스트와 일치할 수 있도록 지정합니다.
- \$A는 규칙이 @ 기호의 오른쪽에 있는 호스트와 일치할 수 있도록 지정합니다.
- \$P는 규칙이 % 기호의 오른쪽에 있는 호스트와 일치할 수 있도록 지정합니다.
- \$X는 규칙이 느낌표(!)의 왼쪽에 있는 호스트와 일치할 수 있도록 지정합니다.

호스트가 지정된 위치와 다른 위치에 있을 경우 규칙은 실패합니다. 이러한 시퀀스는 하나의 다시 쓰기 규칙에서 결합될 수 있습니다. 예를 들어, \$s 및 \$A가 지정된 경우 규칙은 소스 경로나 at 기호의 오른쪽에 지정된 호스트와 일치합니다. 이러한 시퀀스를 전혀 지정하지 않는 것은 시퀀스를 모두 지정되는 것과 같습니다. 즉, 위치에 상관 없이 규칙이 일치할 수 있습니다.

## 현재 태그값 변경: \$T

\$T 제어 시퀀스는 현재 다시 쓰기 규칙 태그를 변경하는 데 사용됩니다. 구성 파일과 도메인 데이터베이스에서 다시 쓰기 규칙 패턴이 조회되기 전에 다시 쓰기 규칙 태그가 모든 다시 쓰기 규칙 패턴의 앞에 놓입니다. \$T의 뒤에서부터 at 기호, 백분율 기호, \$N, \$M, \$Q, \$C, \$T 또는 \$?의 앞 부분에 있는 텍스트는 새 태그로 간주됩니다.

태그는 특정 구성 요소가 발견되었을 때 주소의 전체 특성이 변경되는 특수한 주소 지정 형식을 처리하는 데 유용합니다. 예를 들어, 소스 경로에서 발견될 경우 특정 호스트 이름 **internet**을 주소에서 제거해야 하며 TCP-DAEMON 채널에 대해 결과 주소를 강제로 일치시켜야 한다고 가정해 봅니다.

이것은 다음과 같은 규칙으로 구현할 수 있습니다(localhost가 로컬 호스트의 공식 이름이라고 가정함).

```
internet                $$U@localhost$Tmtcp-force|
mtcp-force|.           $U%H@TCP-DAEMON
```

첫 번째 규칙은 특정 호스트 이름 **internet**과 일치합니다(소스 경로에 표시될 경우). 이 규칙은 **internet**을 로컬 채널에 대해 강제로 일치시켜 주소에서 제거되도록 합니다. 그런 다음 다시 쓰기 태그가 설정됩니다. 다시 쓰기가 진행되지만 태그로 인해 일반 규칙은 일치하지 않습니다. 마지막으로 태그와 함께 기본 규칙이 시도되고 이 집합의 두 번째 규칙이 적용되어 다른 조건에 상관 없이 TCP-DAEMON 채널에 대해 주소를 강제로 일치시킵니다.

## 다시 쓰기와 관련된 오류 메시지 처리: \$?

MTA는 다시 쓰기 및 채널 일치 실패할 경우 기본 오류 메시지를 제공합니다. 특별한 상황에서는 이러한 메시지를 변경하는 기능이 유용할 수 있습니다. 예를 들어, 누군가가 이더넷 라우터 상자에 메일을 보내려고 시도할 경우 일반적인 "illegal host/domain specified"라는 메시지보다 "our routers cannot accept mail"이라는 메시지가 더 정확하게 의미를 전달합니다.

특수한 제어 시퀀스를 사용하여 규칙이 실패할 경우 인쇄할 오류 메시지를 변경할 수 있습니다. \$? 시퀀스는 오류 메시지를 지정하는 데 사용됩니다. \$?의 뒤에서부터 at 기호(@), 백분율 기호(%), \$N, \$M, \$Q, \$C, \$T 또는 \$?의 앞 부분에 있는 텍스트는 다시 쓰기의 결과가 임의의 채널과 일치하는 데 실패할 경우 인쇄될 오류 메시지의 텍스트로 간주됩니다. 오류 메시지의 설정은 "고정적"이며 다시 쓰기 프로세스 동안 계속 적용됩니다.

\$?를 포함하는 규칙은 다른 규칙과 마찬가지로 작동합니다. \$?만 포함하는 특수한 규칙의 경우 다른 방식으로 처리됩니다. 즉, 주소의 메일함 또는 호스트 부분을 변경하지 않고 다시 쓰기 프로세스가 종료하며 호스트는 채널 테이블에서 있는 그대로 조회됩니다. 이 조회는 실패할 것이며 이에 따라 오류 메시지가 결과로 반환됩니다.

예를 들어, MTA 구성 파일의 최종 다시 쓰기 규칙이 다음과 같다고 가정해 봅니다.

. \$?Unrecognized address; contact postmaster@siroe.com

이 예에서 실패할 수 있는 인식되지 않은 호스트 또는 도메인 지정은 실패하는 과정에서 오류 메시지 Unrecognized address; contact postmaster@siroe.com을 생성합니다.

## 많은 수의 다시 쓰기 규칙 처리

MTA는 항상 `imta.cnf` 파일에서 모든 다시 쓰기 규칙을 읽어 해시 테이블의 메모리에 저장합니다. 컴파일된 구성을 사용하면 정보가 필요할 때마다 구성 파일을 읽는 것과 관련된 오버헤드가 사라집니다. 해시 테이블은 여전히 모든 다시 쓰기 규칙을 메모리에 저장하는 데 사용됩니다. 이 방법은 다시 쓰기 규칙 수가 적거나 보통인 경우에 적합합니다. 그러나 일부 사이트에는 10,000개 이상의 다시 쓰기 규칙이 필요할 수 있으며 이로 인해 과도한 양의 메모리가 소비될 수 있습니다.

MTA는 보조 색인 데이터 파일에 많은 수의 다시 쓰기 규칙을 저장하기 위한 선택적 기능을 제공하여 이 문제를 해결합니다. 일반 구성 파일을 읽을 때마다 MTA는 도메인 데이터베이스의 존재를 확인합니다. 도메인 데이터베이스가 존재할 경우 구성 파일에서 발견된 규칙에서 시도된 일치가 실패할 때마다 이 데이터베이스가 열리고 참조됩니다. 구성 파일에서 특정 규칙이 발견되지 않을 경우에만 도메인 데이터베이스가 검사되므로 규칙을 항상 구성 파일에 추가하여 데이터베이스에서 이를 무시할 수 있습니다. 기본적으로 도메인 데이터베이스는 호스트 도메인과 연관된 다시 쓰기 규칙을 저장하는 데 사용됩니다.

IMTA\_DOMAIN\_DATABASE 속성은 `imta_tailor` 파일에 저장됩니다. 데이터베이스의 기본 위치는 `msg_svr_base/data/db/domaindb.db`입니다.

---

주 이 필드를 수동으로 편집해서는 안 됩니다.

---

## 다시 쓰기 규칙 테스트

`imsimta test -rewrite` 명령을 사용하여 다시 쓰기 규칙을 테스트할 수 있습니다.

`-noimage` 한정자를 사용하면 새 구성을 다시 컴파일하기 전에 구성 파일의 변경 사항을 테스트할 수 있습니다.

이 유틸리티를 `-debug` 한정자와 함께 사용하여 몇 개의 주소를 다시 쓰는 것이 유용할 수 있습니다. 이 작업은 주소를 다시 쓰는 방법을 단계별로 보여 줍니다. 예를 들어, 다음 명령을 실행합니다.

```
% imsimta test -rewrite -debug joe@siroe.com
```

imsimta test -rewrite 유틸리티에 대한 자세한 내용은 *Messaging Server Reference Manual*을 참조하십시오.

## 다시 쓰기 규칙 예

다음 예는 샘플 다시 쓰기 규칙과 샘플 주소가 이러한 규칙에 의해 다시 작성되는 방법을 보여 줍니다.

다음 예에 나온 다시 쓰기 규칙이 시스템 SC.CS.SIROE.EDU에 대한 구성 파일에 포함되었다고 가정해 봅니다.

```

sc                $U@sc.cs.siroe.edu
sc1              $U@sc1.cs.siroe.edu
sc2              $U@sc2.cs.siroe.edu
*                $U%$&0.cs.siroe.edu
*.cs             $U%$&0.cs.siroe.edu
*.cs.siroe      $U%$&0.cs.siroe.edu
*.cs.siroe.edu  $U%$&0.cs.siroe.edu@ds.adm.siroe.edu
sc.cs.siroe.edu $U@$D
sc1.cs.siroe.edu $U@$D
sc2.cs.siroe.edu $U@$D
sd.cs.siroe.edu  $U@sd.cs.siroe.edu
.siroe.edu      $U%$H.siroe.edu@cads.adm.siroe.edu
.edu            $U@$H$D@gate.adm.siroe.edu
[]              $U@[L]@gate.adm.siroe.edu
    
```

표 11-7은 몇 가지 샘플 주소와 다시 쓰기 규칙에 따라 이러한 주소가 다시 작성 및 라우팅 되는 방법을 보여 줍니다.

**표 11-7**      샘플 주소 및 다시 쓰기

| 초기 주소            | 다시 작성된 주소             | 라우팅 대상           |
|------------------|-----------------------|------------------|
| user@sc          | user@sc.cs.siroe.edu  | sc.cs.siroe.edu  |
| user@sc1         | user@sc1.cs.siroe.edu | sc1.cs.siroe.edu |
| user@sc2         | user@sc2.cs.siroe.edu | sc2.cs.siroe.edu |
| user@sc.cs       | user@sc.cs.siroe.edu  | sc.cs.siroe.edu  |
| user@sc1.cs      | user@sc1.cs.siroe.edu | sc1.cs.siroe.edu |
| user@sc2.cs      | user@sc2.cs.siroe.edu | sc2.cs.siroe.edu |
| user@sc.cs.siroe | user@sc.cs.siroe.edu  | sc.cs.siroe.edu  |

표 11-7 샘플 주소 및 다시 쓰기

| 초기 주소                 | 다시 작성된 주소             | 라우팅 대상                                |
|-----------------------|-----------------------|---------------------------------------|
| user@sc1.cs.siroe     | user@sc1.cs.siroe.edu | sc1.cs.siroe.edu                      |
| user@sc2.cs.siroe     | user@sc2.cs.siroe.edu | sc2.cs.siroe.edu                      |
| user@sc.cs.siroe.edu  | user@sc.cs.siroe.edu  | sc.cs.siroe.edu                       |
| user@sc1.cs.siroe.edu | user@sc1.cs.siroe.edu | sc1.cs.siroe.edu                      |
| user@sc2.cs.siroe.edu | user@sc2.cs.siroe.edu | sc2.cs.siroe.edu                      |
| user@sd.cs.siroe.edu  | user@sd.cs.siroe.edu  | sd.cs.siroe.edu                       |
| user@aa.cs.siroe.edu  | user@aa.cs.siroe.edu  | ds.adm.siroe.edu                      |
| user@a.eng.siroe.edu  | user@a.eng.siroe.edu  | cds.adm.siroe.edu                     |
| user@a.cs.sesta.edu   | user@a.cs.sesta.edu   | gate.adm.siroe.edu<br>—route inserted |
| user@b.cs.sesta.edu   | user@b.cs.sesta.edu   | gate.adm.siroe.edu<br>—route inserted |
| user@[1.2.3.4]        | user@[1.2.3.4]        | gate.adm.siroe.edu<br>—route inserted |

호스트 이름이 단순 형식 이름(sc, sc1 또는 sc2) 중 하나이거나 전체 이름(sc.cs.siroe.edu 등) 중 하나일 경우 이를 전체 이름으로 확장하고 대상으로 라우팅합니다. 한 부분으로 된 단순 형식 이름에 cs.cmu.edu를 추가하고 다시 시도합니다. 뒤에 .cs가 오는 한 부분을 뒤에 .cs.siroe.edu가 오는 한 부분으로 변환하고 다시 시도합니다. 또한 .cs.siroe를 .cs.siroe.edu로 변환하고 다시 시도합니다.

이름이 sd.cs.siroe.edu(직접 연결되는 일부 시스템)인 경우 이를 다시 작성하고 자체에서 라우팅합니다. 호스트 이름이 .cs.siroe.edu 하위 도메인에 있는 것이면 이를 ds.cs.siroe.edu(.cs.siroe.edu 하위 도메인의 게이트웨이)로 라우팅합니다. 호스트 이름이 .siroe.edu 하위 도메인에 있는 것이면 이를 cds.adm.siroe.edu(.siroe.edu 하위 도메인의 게이트웨이)로 라우팅합니다. 호스트 이름이 .edu 최상위 도메인 있는 것이면 이를 gate.adm.siroe.edu(메일을 적절한 대상으로 라우팅할 수 있음)로 라우팅합니다. 도메인 리터럴이 사용될 경우 이를 또한 gate.adm.siroe.edu로 보냅니다.

앞의 예와 마찬가지로 대부분의 다시 쓰기 규칙 적용은 주소의 아이디 또는 메일함 부분을 변경하지 않습니다. 주소의 아이디 부분을 변경하는 기능은 RFC 822를 따르지 않는 전자 메일 프로그램(즉, 호스트/도메인 지정의 일부로 주소의 아이디 부분을 채워야 하는 전자 메일 프로그램)과 인터페이스하기 위해 MTA를 사용할 때 사용됩니다. 이 기능을 사용할 때는 매우 주의해야 합니다.

다시 쓰기 규칙 예



## 채널 정의 구성

이 장에서는 MTA 구성 파일 `imta.cnf`에서 채널 키워드 정의를 사용하는 방법에 대해 설명합니다. 이 장을 읽기 전에 10장, "MTA 서비스 및 구성 정보", 192페이지의 "채널 정의" 및 226페이지의 "MTA 구성 파일"을 읽어 보십시오. 이 장은 다음 내용으로 구성되어 있습니다.

- 채널 키워드(알파벳순)
- 채널 키워드 범주화(기능별)
- 채널 기본값 구성
- SMTP 채널 구성
- 메일 처리 및 전달 구성
- 주소 처리 구성
- 헤더 처리 구성
- 첨부 파일 및 MIME 처리
- 메일, 할당량, 수신자 및 인증 시도의 제한
- MTA 대기열에서 파일 만들기
- 메일함 필터 파일 위치 지정
- 로깅 및 디버깅 구성
- 기타 키워드

**주** imta.cnf에서 채널 정의를 변경하는 경우 `imsimta restart` 명령을 사용하여 시작할 때 한 번만 구성 데이터를 로드하는 프로그램 또는 채널(예: SMTP 서버)을 다시 시작해야 합니다. 컴파일된 구성을 사용하는 경우 재 컴파일을 수행한 다음 다시 시작해야 합니다. 구성 정보 컴파일과 프로그램 시작에 대한 자세한 내용은 *Messaging Server Reference Manual*을 참조하십시오.

## 채널 키워드(알파벳순)

다음 표는 알파벳순으로 나열된 키워드 목록입니다.

**표 12-1** 채널 키워드(알파벳순)

| 키워드                     | 페이지 | 키워드                    | 페이지 | 키워드                              | 페이지 | 키워드                   | 페이지 |
|-------------------------|-----|------------------------|-----|----------------------------------|-----|-----------------------|-----|
| 733                     | 366 | 822                    | 366 | addrreturnpath                   | 373 | addrspersfile         | 391 |
| Aliasdetourhost         | 399 | aliaslocal             | 376 | aliaspostmaster                  | 274 | allowetrn             | 338 |
| allowswitchchannel      | 350 | alternatchannel        | 389 | alternateblocklimit              | 389 | alternatelinelimit    | 389 |
| alternaterecipientlimit | 389 | authrewrite            | 352 | backoff                          | 358 | bangoverpercent       | 368 |
| bangstyle               | 366 | bidirectional          | 357 | blocketrn                        | 338 | blocklimit            | 388 |
| cacheeverything         | 346 | cachefailures          | 346 | cachesuccesses                   | 346 | channelfilter         | 398 |
| charset7                | 341 | charset8               | 341 | charsetesc                       | 341 | checkehlo             | 337 |
| commentinc              | 374 | commentmap             | 374 | commentomit                      | 374 | commentstrip          | 374 |
| commenttotal            | 374 | connectalias           | 370 | connectcanonical                 | 370 | copysendpost          | 273 |
| copywarnpost            | 273 | daemon                 | 350 | datefour                         | 381 | datetwo               | 381 |
| dayofweek               | 381 | defaulthost            | 370 | defaultmx                        | 348 | defaultnameservers    | 349 |
| deferralrejectlimit     | 403 | deferred               | 358 | defragment                       | 385 | dequeue_remove<br>ute | 378 |
| destinationfilter       | 398 | destinationnosolicit   | 403 | destinationspamfilter<br>rXoptin | 399 | disableetrn           | 338 |
| dispositionchannel      | 397 | disconnectbadauthlimit | 388 | disconnectbadcom<br>mandlimit    | 395 | domainetrn            | 338 |
| domainvrfy              | 339 | dropblank              | 372 | ehlo                             | 337 | eightbit              | 341 |

표 12-1 채널 키워드(알파벳순)

| 키워드              | 페이지 | 키워드                 | 페이지 | 키워드                 | 페이지 | 키워드                    | 페이지 |
|------------------|-----|---------------------|-----|---------------------|-----|------------------------|-----|
| eightnegotiate   | 341 | eightstrict         | 341 | errsendpost         | 273 | errwarnpost            | 273 |
| expandchannel    | 364 | expandlimit         | 364 | expnallow           | 340 | expndisable            | 340 |
| expndefault      | 340 | exproute            | 368 | fileinto            | 398 | filesperjob            | 360 |
| filter           | 398 | forwardcheckdelete  | 346 | forwardchecknone    | 346 | forwardchecktag        | 346 |
| header_733       | 366 | header_822          | 366 | header_uucp         | 366 | headerlabelalign       | 382 |
| headerlimit      | 393 | headerlinelength    | 382 | headerread          | 379 | headertrim             | 379 |
| holdexquota      | 391 | holdlimit           | 364 | identnone           | 347 | identnonelimited       | 347 |
| identnonenumeric | 347 | identnon symbolic   | 347 | identtcp            | 347 | identtcp limited       | 347 |
| identtcpsymbolic | 347 | ignoreencoding      | 384 | imnnonurgent        | 358 | improute               | 368 |
| includefinal     | 272 | indenttcpnumeric    | 347 | inner               | 379 | innertrim              | 379 |
| interfaceaddress | 345 | interpretencoding   | 384 | language            | 384 | lastresort             | 349 |
| linelength       | 387 | linelimit           | 388 | localvrfy           | 339 | 로깅                     | 395 |
| logheader        | 395 | loopcheck           | 396 | mailfromdnsverify   | 340 | master                 | 357 |
| master_debug     | 396 | maxblocks           | 386 | maxheaderaddrs      | 382 | maxheaderchars         | 382 |
| maxjobs          | 360 | maxlines            | 386 | maxprocchars        | 382 | maysaslserver          | 351 |
| maytls           | 354 | maytlsclient        | 354 | maytlsserver        | 354 | missingrecipientpolicy | 371 |
| msexchange       | 353 | multiple            | 391 | mustsaslserver      | 351 | musttls                | 354 |
| musttlsclient    | 354 | musttlsserver       | 354 | mx                  | 348 | namelengthlimit        | 392 |
| nameservers      | 349 | noaddreturnpath     | 373 | nobangoverpercent   | 368 | noblocklimit           | 388 |
| nocache          | 346 | nochannelfilter     | 398 | nodayofweek         | 381 | nodefaulthost          | 370 |
| nodeferred       | 358 | nodefragment        | 385 | nodestinationfilter | 398 | nodropblank            | 372 |
| noehlo           | 337 | noexproute          | 368 | noexquota           | 391 | nofileinto             | 398 |
| nofilter         | 398 | noheaderread        | 379 | noheadertrim        | 379 | noimproute             | 368 |
| noinner          | 379 | noinnertrim         | 379 | nolinelimit         | 388 | nologging              | 395 |
| noloopcheck      | 396 | nomailfromdnsverify | 340 | nomaster_debug      | 396 | nomsexchange           | 352 |
| nomx             | 348 | nonrandomemx        | 348 | nonurgentbackoff    | 358 | nonurgentblocklimit    | 363 |
| nonurgentnotices | 272 | noreceivedfor       | 374 | noreceivedfrom      | 374 | noremotehost           | 370 |
| norestricted     | 373 | noreturnaddress     | 274 | noreturnpersonal    | 274 | noreverse              | 372 |
| normalbackoff    | 358 | normalblocklimit    | 363 | normalnotices       | 272 | norules                | 377 |

표 12-1 채널 키워드(알파벳순)

| 키워드                        | 페이지 | 키워드                 | 페이지 | 키워드                  | 페이지 | 키워드                                | 페이지 |
|----------------------------|-----|---------------------|-----|----------------------|-----|------------------------------------|-----|
| nosasl                     | 351 | nosaslserver        | 351 | nosaslswitchchannel  | 351 | nosendetrn                         | 338 |
| nosendpost                 | 273 | noservice           | 365 | noslave_debug        | 396 | nosmtp                             | 337 |
| nosourcefilter             | 398 | noswitchchannel     | 350 | notices              | 272 | notificationchannel                | 397 |
| notls                      | 354 | notlsclient         | 354 | notlsserver          | 354 | novrfy                             | 339 |
| nowarnpost                 | 273 | nox_env_to          | 381 | parameterlengthlimit | 392 | percentonly                        | 368 |
| percents                   | 366 | personalinc         | 375 | personalmap          | 375 | personalomit                       | 375 |
| personalstrip              | 375 | pool                | 360 | port                 | 345 | postheadbody                       | 274 |
| postheadonly               | 274 | randommx            | 348 | receivedfor          | 374 | receivedfrom                       | 374 |
| recipientcutoff            | 392 | recipientlimit      | 392 | rejectsmtpplonglines | 392 | remotehost                         | 370 |
| restricted                 | 373 | returnaddress       | 274 | returnenvelope       | 274 | returnpersonal                     | 274 |
| reverse                    | 372 | routelocal          | 369 | rules                | 377 | rules                              | 377 |
| saslswitchchannel          | 351 | sendetrn            | 338 | sendpost             | 273 | sensitivitycompany<br>confidential | 383 |
| sensitivitynormal          | 383 | sensitivitypersonal | 383 | sensitivityprivate   | 383 | service                            | 365 |
| sevenbit                   | 341 | silentetrn          | 338 | single               | 391 | single_sys                         | 350 |
| slave                      | 357 | slave_debug         | 396 | smtp                 | 337 | smtp_cr                            | 337 |
| smtp_crlf                  | 337 | smtp_crorlf         | 337 | smtp_lf              | 337 | sourceblocklimit                   | 388 |
| sourcecommentinc           | 374 | sourcecommentmap    | 374 | sourcecommentomit    | 374 | sourcecommentstri<br>p             | 374 |
| sourcecommenttotal         | 374 | sourcefilter        | 398 | sourcenosolicit      | 403 | sourcepersonalinc                  | 375 |
| sourcepersonalmap          | 375 | sourcepersonalomit  | 375 | sourcepersonalstrip  | 375 | sourceroute                        | 366 |
| sourcespamfilterXopt<br>in | 399 | streaming           | 343 | subaddressexact      | 376 | subaddressrelaxed                  | 376 |
| subaddresswild             | 376 | subdirs             | 394 | submit               | 397 | suppressfinal                      | 272 |
| switchchannel              | 350 | threaddepth         | 363 | tlsswitchchannel     | 354 | transactionlimit                   | 362 |
| truncatesmtpplonglines     | 392 | unrestricted        | 373 | urgentbackoff        | 358 | urgentblocklimit                   | 363 |
| urgentnotices              | 272 | useintermediate     | 272 | user                 | 398 | uucp                               | 366 |
| viaaliasoptional           | 378 | viaaliasrequired    | 378 | vrifyallow           | 339 | vrifydefault                       | 339 |
| vrifyhide                  | 339 | warnpost            | 273 | wrapsmtpplonglines   | 392 | x_env_to                           | 381 |

## 채널 키워드 범주화(기능별)

다음 표는 범주화한 키워드 목록입니다. 범주는 다음과 같습니다.

- 317의 "주소 처리"
- 319의 "첨부 파일 및 MIME 처리"
- 319의 "문자 세트 및 8비트 데이터"
- 319의 "MTA 대기열 영역에서 파일 만들기"
- 320의 "헤더"
- 322의 "받는 채널 일치 및 전환"
- 323의 "로깅 및 디버깅"
- 323의 "긴 주소 목록 또는 헤더"
- 323의 "메일함 필터"
- 324의 "NO-SOLICIT SMTP 확장 지원"
- 324의 "알림 및 포스트마스터 메일"
- 325의 "제어 및 작업 전송 처리"
- 326의 "민감도 제한"
- 326의 "메일, 사용자 할당량, 권한 및 인증 시도의 제한"
- 327의 "SMTP 인증, SASL 및 TLS"
- 328의 "SMTP 명령 및 프로토콜"
- 330의 "TCP/IP 연결 및 DNS 조회 지원"
- 331의 "기타"

**표 12-2** 채널 키워드 범주화(기능별)

| 키워드            | 페이지 | 정의                                         |
|----------------|-----|--------------------------------------------|
| 주소 처리          |     |                                            |
| 733            | 366 | 봉투에 percents와 동의어인 % 라우팅을 사용합니다.           |
| 822            | 366 | 봉투에 sourceroute와 동일한 소스 루트를 사용합니다.         |
| addrreturnpath | 373 | Return-path: 헤더를 이 채널의 대기열에 포함된 메일에 추가합니다. |

**표 12-2** 채널 키워드 범주화(기능별)

| 키워드                    | 페이지 | 정의                                                             |
|------------------------|-----|----------------------------------------------------------------|
| aliaslocal             | 376 | 별칭 파일 및 별칭 데이터베이스에서 다시 쓴 주소를 조회합니다.                            |
| authrewrite            | 352 | MTA에서 인증된 메일 발송자 정보(사용 가능한 경우)를 헤더로 전파하도록 하기 위해 소스 채널에서 사용됩니다. |
| bangoverpercent        | 368 | A!B%C를 A!(B%C)로 그룹화합니다.                                        |
| bangstyle              | 366 | 봉투에 uucp와 동의어인 UUCP! 라우팅을 사용합니다.                               |
| defaulthost            | 370 | 주소를 완성하기 위해 사용할 도메인 이름을 지정합니다.                                 |
| dequeue_removalroute   | 378 | 봉투의 T <sub>0</sub> : 주소에서 소스 경로를 제거합니다.                        |
| exproute               | 368 | 주소가 원격 시스템에 전달될 때 명시적 라우팅이 필요합니다.                              |
| holdlimit              | 364 | 봉투의 수신자 주소 수가 이 제한을 초과할 경우 메일을 보관합니다.                          |
| improute               | 368 | 이 채널 주소에 대한 암시적 라우팅이 필요합니다.                                    |
| missingrecipientpolicy | 371 | 수신자 헤더가 없는 메일을 적법화(헤더 추가)하는 방법에 대한 정책을 설정합니다.                  |
| noaddreturnpath        | 373 | 메일을 대기열에 포함할 때 Return-path: 헤더를 추가하지 않습니다.                     |
| nobangoverpercent      | 368 | A!B%C를 (A!B)%C로 그룹화합니다.                                        |
| nodefaulthost          | 370 | 주소를 완성하기 위해 사용할 도메인 이름을 지정하지 않습니다.                             |
| noexproute             | 368 | 이 채널의 주소에 대한 명시적 라우팅이 필요하지 않습니다.                               |
| noimproute             | 368 | 이 채널의 주소에 대한 암시적 라우팅이 필요하지 않습니다.                               |
| noreceivedfrom         | 374 | 원본 봉투의 From: 주소를 포함하지 않고 Received: 헤더 행을 구성합니다.                |
| noremotehost           | 370 | 주소를 완성하기 위해 로컬 호스트의 도메인 이름을 기본 도메인 이름으로 사용합니다.                 |
| norestricted           | 373 | unrestricted와 동일합니다.                                           |
| noreverse              | 372 | 메일의 주소를 역방향 주소 처리에서 제외합니다.                                     |
| norules                | 377 | 이 채널에 대해 채널별 다시 쓰기 규칙 검사를 실행하지 않습니다.                           |
| percentonly            | 368 | 뱅 경로를 무시합니다. 봉투에 % 라우팅을 사용합니다.                                 |
| percents               | 366 | 봉투에 733과 동의어인 % 라우팅을 사용합니다.                                    |
| remotehost             | 370 | 주소를 완성하기 위해 원격 호스트의 이름을 기본 도메인 이름으로 사용합니다.                     |
| restricted             | 373 | 채널이 인코딩을 필요로 하는 메일 시스템에 연결됩니다.                                 |
| reverse                | 372 | 주소를 주소 역방향 데이터베이스 또는 REVERSE 매핑에 대해 검사합니다.                     |
| routelocal             | 369 | 채널에 주소를 다시 쓸 때 MTA가 주소의 명시적 라우팅을 "단락화"하게 합니다.                  |
| rules                  | 377 | 이 채널에 대해 채널별 다시 쓰기 규칙 검사를 실행합니다.                               |

표 12-2 채널 키워드 범주화(기능별)

| 키워드                        | 페이지 | 정의                                                                                   |
|----------------------------|-----|--------------------------------------------------------------------------------------|
| sourceroute                | 366 | 822와 동의어입니다.                                                                         |
| subaddressexact            | 376 | 항목 일치 작업 중에 특수 하위 주소 처리를 수행하지 않습니다. 하위 주소를 포함하여 전체 메일함이 항목과 일치해야 별칭이 일치하는 것으로 간주됩니다. |
| subaddressrelaxed          | 376 | MTA는 전체 일치와 name+* 형식의 일치를 차례로 조사한 다음 이름 부분에 대한 일치를 추가로 확인해야 합니다.                    |
| subaddresswild             | 376 | MTA는 전체 하위 주소를 포함한 정확한 일치를 조사한 다음 name+* 형식의 항목을 조사해야 합니다.                           |
| unrestricted               | 373 | MTA에 RFC 1137 인코딩 및 디코딩을 수행하지 않도록 지시합니다.                                             |
| uucp                       | 366 | 봉투에 bangstyle과 동의어인 UUCP! 라우팅을 사용합니다.                                                |
| viaaliasoptional           | 378 | 채널과 일치하는 최종 수신자 주소를 별칭을 통해 생성할 필요가 없습니다.                                             |
| viaaliasrequired           | 378 | 채널과 일치하는 최종 수신자 주소를 별칭을 통해 생성해야 합니다.                                                 |
| <b>첨부 파일 및 MIME 처리</b>     |     |                                                                                      |
| defragment                 | 385 | 채널에 대기 중인 부분 메일을 조각 모음 채널 대기열에 대신 넣습니다.                                              |
| ignoreencoding             | 384 | 받는 메일에서 Encoding: 헤더를 무시합니다.                                                         |
| interpretencoding          | 384 | 필요한 경우 받는 메일에서 Encoding: 헤더를 해석합니다.                                                  |
| nodefragment               | 385 | 조각 모음을 사용하지 않습니다.                                                                    |
| <b>문자 세트 및 8비트 데이터</b>     |     |                                                                                      |
| charset7                   | 341 | 7비트 텍스트 메일과 관련된 기본 문자 세트입니다.                                                         |
| charset8                   | 341 | 8비트 텍스트 메일과 관련된 기본 문자 세트입니다.                                                         |
| charsetesc                 | 341 | 이스케이프 문자를 포함하는 7비트 텍스트 메일과 관련된 기본 문자 세트입니다.                                          |
| eightbit                   | 341 | 채널에서 8비트 문자를 지원합니다.                                                                  |
| eightnegotiate             | 341 | 채널에서 가능할 경우 8비트 전송 사용을 협상합니다.                                                        |
| eightstrict                | 341 | 협상되지 않은 8비트 데이터를 포함하는 메일을 거부합니다.                                                     |
| sevenbit                   | 341 | 8비트 문자를 지원하지 않으므로 8비트 문자를 인코딩해야 합니다.                                                 |
| <b>MTA 대기열 영역에서 파일 만들기</b> |     |                                                                                      |
| addrspfile                 | 391 | 채널 대기열에서 단일 메일 파일과 연결될 수 있는 최대 수신자 수를 제한합니다.                                         |
| expandchannel              | 364 | expandlimit 적용으로 인해 지연된 확장을 수행할 채널을 지정합니다.                                           |

표 12-2 채널 키워드 범주화(기능별)

| 키워드              | 페이지 | 정의                                                                                   |
|------------------|-----|--------------------------------------------------------------------------------------|
| expandlimit      | 364 | 주소 수가 이 제한을 초과할 경우 받는 메일을 "오프라인"으로 처리합니다.                                            |
| multiple         | 391 | 메일 파일의 수신자 수를 제한하지 않습니다. SMTP 채널의 기본값은 99입니다.                                        |
| single           | 391 | 채널의 각 대상 주소에 대해 별도의 메일 복사본을 만듭니다.                                                    |
| single_sys       | 391 | 사용된 각 대상 시스템에 대해 단일 메일 복사본을 만듭니다.                                                    |
| subdirs          | 394 | 채널 대기열의 메일을 분산시킬 하위 디렉토리 수를 지정합니다.                                                   |
| <b>헤더</b>        |     |                                                                                      |
| authrewrite      | 352 | MTA에서 인증된 메일 발송자 정보(사용 가능한 경우)를 헤더로 전파하도록 하기 위해 소스 채널에서 사용됩니다.                       |
| commentinc       | 374 | 메일 헤더 행의 주석을 그대로 둡니다.                                                                |
| commentmap       | 374 | COMMENT_STRINGS 매핑 테이블을 통해 메일 헤더 행에 주석 문자열을 실행합니다.                                   |
| commentomit      | 374 | 메일 헤더 행에서 주석을 제거합니다.                                                                 |
| commentstrip     | 374 | 메일 헤더 행의 주석 필드에서 문자가 있는 문자를 제거합니다.                                                   |
| commenttotal     | 374 | Received: 헤더 행을 제외한 모든 헤더 행에서 주석(괄호 안의 내용)을 제거합니다. 권장되지 않습니다.                        |
| datefour         | 381 | 모든 연도 필드를 네 자리로 확장합니다.                                                               |
| datetwo          | 381 | 네 자리 날짜에서 앞의 두 자리를 제거하여 두 자리 날짜를 사용해야 하는 메일 시스템과 호환되게 합니다. 그 밖의 다른 목적으로 사용해서는 안 됩니다. |
| dayofweek        | 381 | 요일 정보를 보존하고 이 정보를 날짜 및 시간 헤더에 추가합니다(없는 경우).                                          |
| defaulthost      | 370 | 주소를 완성하기 위해 사용할 도메인 이름을 지정합니다.                                                       |
| dropblank        | 372 | 받는 메일에서 잘못된 빈 헤더를 제거합니다.                                                             |
| header_733       | 366 | 메일 헤더에 % 라우팅을 사용합니다.                                                                 |
| header_822       | 366 | 메일 헤더에 소스 경로를 사용합니다.                                                                 |
| headerlabelalign | 382 | 이 채널의 대기열에 포함된 메일 헤더에 대한 맞춤 점을 제어합니다. 맞춤 점은 정수 값 인수를 가집니다.                           |
| headerlinelength | 382 | 이 채널의 대기열에 포함된 헤더 행의 길이를 제어합니다.                                                      |
| headerread       | 379 | 원본 메일 헤더를 처리하기 전에 옵션 파일의 헤더 자르기 규칙을 메일 대기열에 포함된 메일 헤더에 적용합니다.                        |



표 12-2 채널 키워드 범주화(기능별)

| 키워드                    | 페이지 | 정의                                                                               |
|------------------------|-----|----------------------------------------------------------------------------------|
| headertrim             | 379 | 원본 메일 헤더를 처리한 후에 옵션 파일의 헤더 자르기 규칙을 메일 헤더에 적용합니다.                                 |
| header_uucp            | 366 | 헤더에 ! 라우팅을 사용합니다.                                                                |
| inner                  | 379 | 메일을 구문 분석하고 내부 헤더를 다시 씁니다.                                                       |
| innertrim              | 379 | 옵션 파일의 헤더 자르기 규칙을 내부 메일 헤더에 적용합니다.                                               |
| language               | 384 | 헤더에 기본 언어를 지정합니다.                                                                |
| maxheaderaddrs         | 382 | 한 행에 표시할 수 있는 주소 수를 제어합니다.                                                       |
| maxheaderchars         | 382 | 한 행에 표시할 수 있는 문자 수를 제어합니다.                                                       |
| missingrecipientpolicy | 371 | 수신자 헤더가 없는 메일을 적법화(헤더 추가)하는 방법에 대한 정책을 설정합니다.                                    |
| nodayofweek            | 381 | 날짜 및 시간 헤더에서 요일을 제거하여 이 정보를 처리할 수 없는 메일 시스템과 호환되게 합니다. 그 밖의 다른 목적으로 사용해서는 안 됩니다. |
| nodefaulthost          | 370 | 주소를 완성하기 위해 사용할 도메인 이름을 지정하지 않습니다.                                               |
| nodropblank            | 372 | 받는 메일에서 잘못된 빈 헤더를 제거하지 않습니다.                                                     |
| noheaderread           | 379 | 옵션 파일의 헤더 자르기 규칙을 적용하지 않습니다.                                                     |
| noheadertrim           | 379 | 옵션 파일의 헤더 자르기 규칙을 적용하지 않습니다.                                                     |
| noinner                | 379 | 내부 메일 헤더 행을 다시 쓰지 않습니다.                                                          |
| noinnertrim            | 379 | 내부 메일 헤더에 헤더 자르기를 적용하지 않습니다.                                                     |
| noreceivedfor          | 374 | 봉투 수신자 정보를 포함하지 않고 Received: 헤더 행을 구성합니다.                                        |
| noreceivedfrom         | 374 | 원본 봉투의 From: 주소를 포함하지 않고 Received: 헤더 행을 구성합니다.                                  |
| noremotehost           | 370 | 주소를 완성하기 위해 로컬 호스트의 도메인 이름을 기본 도메인 이름으로 사용합니다.                                   |
| noreverse              | 372 | 채널에 대기 중인 메일에서 역방향 주소 처리를 사용하지 않습니다.                                             |
| norules                | 377 | 이 채널에 대해 채널별 다시 쓰기 규칙 검사를 실행하지 않습니다.                                             |
| nox_env_to             | 381 | X-Envelope-to 헤더 행을 제거합니다.                                                       |
| personalinc            | 375 | 메일 헤더 행의 개인 이름 필드를 그대로 둡니다.                                                      |
| personalmap            | 375 | PERSONAL_NAMES 매핑 테이블을 통해 개인 이름을 실행합니다.                                          |
| personalomit           | 375 | 메일 헤더 행에서 개인 이름 필드를 제거합니다.                                                       |
| personalstrip          | 375 | 헤더 행의 개인 이름 필드에서 문제가 있는 문자를 제거합니다.                                               |

**표 12-2** 채널 키워드 범주화(기능별)

| 키워드                            | 페이지 | 정의                                                                                  |
|--------------------------------|-----|-------------------------------------------------------------------------------------|
| receivedfor                    | 374 | 메일의 주소가 한 명의 봉투 수신자로 지정된 경우 해당 봉투의 To: 주소를 메일이 구성하는 Received: 헤더 행에 포함합니다.          |
| receivedfrom                   | 374 | MTA에서 봉투의 From: 주소를 변경한 경우, 받는 메일에 대한 Received: 헤더 행을 구성할 때 봉투의 원래 From: 주소를 포함합니다. |
| remotehost                     | 370 | 주소를 완성하기 위해 원격 호스트의 이름을 기본 도메인 이름으로 사용합니다.                                          |
| restricted                     | 373 | 채널이 이 인코딩을 필요로 하는 메일 시스템에 연결됩니다.                                                    |
| reverse                        | 372 | 주소를 주소 역방향 데이터베이스 또는 REVERSE 매핑에 대해 검사합니다.                                          |
| rules                          | 377 | 이 채널에 대해 채널별 다시 쓰기 규칙 검사를 실행합니다.                                                    |
| sensitivitycompanyconfidential | 383 | Companyconfidential이 메일에 대한 최대 민감도 제한으로 적용됩니다.                                      |
| sensitivitynormal              | 383 | Normal이 메일에 대한 최대 민감도 제한으로 적용됩니다.                                                   |
| sensitivitypersonal            | 383 | Personal이 메일에 대한 최대 민감도 제한으로 적용됩니다.                                                 |
| sensitivityprivate             | 383 | Private이 메일에 대한 최대 민감도 제한으로 적용됩니다.                                                  |
| sourcecommentinc               | 374 | 받는 메일 헤더 행의 주석을 그대로 둡니다.                                                            |
| sourcecommentmap               | 374 | 소스 채널을 통해 헤더 행에 주석 문자열을 실행합니다.                                                      |
| sourcecommentomit              | 374 | 받는 메일 헤더 행(예: To:, From:, Cc: 등과 같은 주소 지정 헤더)에서 주석을 제거합니다.                          |
| sourcecommentstrip             | 374 | 받는 헤더 행의 주석 필드에서 문제가 있는 문자를 제거합니다.                                                  |
| sourcecommenttotal             | 374 | 받는 메일에서 주석(괄호 안의 내용)을 제거합니다.                                                        |
| sourcepersonalinc              | 375 | 받는 메일 헤더 행의 개인 이름을 그대로 둡니다.                                                         |
| sourcepersonalmap              | 375 | 소스 채널을 통해 개인 이름을 실행합니다.                                                             |
| sourcepersonalomit             | 375 | 받는 메일 헤더 행에서 개인 이름 필드를 제거합니다.                                                       |
| sourcepersonalstrip            | 375 | 받는 메일 헤더 행의 개인 이름 필드에서 문제가 있는 문자를 제거합니다.                                            |
| unrestricted                   | 373 | MTA에 RFC 1137 인코딩 및 디코딩을 수행하지 않도록 지시합니다.                                            |
| X_env_to                       | 381 | X-Envelope-to 헤더 행을 생성합니다.                                                          |
| <b>받는 채널 일치 및 전환</b>           |     |                                                                                     |
| allowswitchchannel             | 350 | switchchannel 채널에서 이 채널로 전환을 허용합니다.                                                 |
| nosaslsupportchannel           | 351 | SASL 인증에 성공할 때 이 채널로 전환하지 않습니다.                                                     |
| noswitchchannel                | 350 | 채널 전환을 수행하지 않습니다.                                                                   |
| switchchannel                  | 350 | 서버 채널에서 원본 호스트와 연결된 채널로 전환합니다.                                                      |

표 12-2 채널 키워드 범주화(기능별)

| 키워드                          | 페이지 | 정의                                                          |
|------------------------------|-----|-------------------------------------------------------------|
| saslswitchchannel            | 351 | 클라이언트가 SASL을 성공적으로 사용하면 받는 연결이 지정한 채널로 전환되게 합니다.            |
| tlsswitchchannel             | 354 | TLS 협상이 성공하면 다른 채널로 전환합니다.                                  |
| <b>로깅 및 디버깅</b>              |     |                                                             |
| 로깅                           | 395 | 로그 파일에 대기열에서 제거되거나 포함된 메일에 대해 기록하고 특정 채널에 대한 로깅을 활성화합니다.    |
| loopcheck                    | 396 | MTA가 자체적으로 통신하는지 확인하도록 SMTP EHLO 응답 배너에 문자열을 넣습니다.          |
| master_debug                 | 396 | 채널의 마스터 프로그램 출력에 디버깅 출력을 만듭니다.                              |
| nologging                    | 395 | 로그 파일에 대기열에 포함되거나 대기서 제거된 메일에 대해 기록하지 않습니다.                 |
| noloopcheck                  | 396 | SMTP EHLO 응답 배너에 문자열을 넣지 않습니다.                              |
| nomaster_debug               | 396 | 채널의 마스터 프로그램 출력에 디버깅 출력을 만들지 않습니다.                          |
| noslave_debug                | 396 | 슬레이브 디버깅 출력을 생성하지 않습니다.                                     |
| slave_debug                  | 396 | 슬레이브 디버깅 출력을 생성합니다.                                         |
| <b>긴 주소 목록 또는 헤더</b>         |     |                                                             |
| expandchannel                | 364 | expandlimit 적용으로 인해 지연된 확장을 수행할 채널을 지정합니다.                  |
| expandlimit                  | 364 | 주소 수가 이 제한을 초과할 경우 받는 메일을 "오프라인"으로 처리합니다.                   |
| holdlimit                    | 364 | 주소 수가 이 제한을 초과할 경우 메일을 보관합니다.                               |
| maxprocchars                 | 382 | 처리 및 다시 쓰기 가능한 최대 길이 헤더입니다.                                 |
| <b>메일함 필터</b>                |     |                                                             |
| channelfilter                | 398 | 채널 필터 파일의 위치이며 destinationfilter와 동일합니다.                    |
| destinationfilter            | 398 | 보내는 메일에 적용되는 채널 필터 파일의 위치입니다.                               |
| destinationspamfilter Xoptin | 399 | 스팸 필터링 소프트웨어 X를 통해 이 채널을 대상으로 하는 메일을 실행합니다.                 |
| fileinto                     | 398 | 메일함 필터 fileinto 작업을 적용할 때 주소에 미치는 영향을 지정합니다.                |
| filter                       | 398 | 사용자 필터 파일의 위치를 지정합니다.                                       |
| nochannelfilter              | 398 | 보내는 메일에 대해 채널 필터링을 수행하지 않습니다. nodeestinationfilter 라고도 합니다. |
| nodeestinationfilter         | 398 | 보내는 메일에 대해 채널 필터링을 수행하지 않습니다.                               |
| nofileinto                   | 398 | 메일함 필터 fileinto 연산자가 영향을 미치지 않습니다.                          |
| nofilter                     | 398 | 사용자 메일함 필터링을 수행하지 않습니다.                                     |

**표 12-2** 채널 키워드 범주화(기능별)

| 키워드                                             | 페이지 | 정의                                                                                                             |
|-------------------------------------------------|-----|----------------------------------------------------------------------------------------------------------------|
| nosourcefilter                                  | 398 | 받는 메일에 대해 채널 필터링을 수행하지 않습니다.                                                                                   |
| sourcefilter                                    | 398 | 받는 메일에 대해 채널 필터 파일의 위치를 지정합니다.                                                                                 |
| sourcespamfilterXoptin                          | 399 | 스팸 필터링 소프트웨어 X를 통해 이 채널에서 수신한 메일을 실행합니다.                                                                       |
| <b>NO-SOLICIT SMTP 확장 지원</b>                    |     |                                                                                                                |
| sourcenosolicit                                 | 403 | 이 채널이 전송하는 메일에서 차단될 요청 필드 값의 범위로 구분된 목록을 지정합니다.                                                                |
| destinationnosolicit                            | 403 | 이 채널의 대기열에 포함된 메일에서 허용되지 않는 요청 필드 값의 범위로 구분된 목록을 지정합니다.                                                        |
| <b>알림 및 포스트마스터 메일<br/>(전체 알림 절차는 264페이지 참조)</b> |     |                                                                                                                |
| aliaspostmaster                                 | 274 | 공식 채널 이름에서 포스트마스터 아이디로 주소 지정된 메일은 postmaster@local-host로 리디렉션됩니다. 여기서 local-host는 로컬 호스트 이름 (로컬 채널에 있는 이름)입니다. |
| copysendpost                                    | 273 | 전송 실패 메일에서 보낸 사람 주소가 비어 있지 않는 한 실패 알림 복사본을 포스트마스터에게 보냅니다.                                                      |
| copywarnpost                                    | 273 | 전달되지 않은 메일에서 보낸 사람 주소가 비어 있지 않는 한 경고 메일 복사본을 포스트마스터에게 보냅니다.                                                    |
| errsendpost                                     | 273 | 메일 발송자에게 알림을 보낼 수 없는 경우 실패 알림 복사본을 포스트마스터에게 보냅니다.                                                              |
| errwarnpost                                     | 273 | 메일 발송자에게 알림을 보낼 수 없는 경우 경고 메일 복사본을 포스트마스터에게 보냅니다.                                                              |
| includefinal                                    | 272 | 전달 알림에 최종 수신자 주소 형식을 포함합니다.                                                                                    |
| nonurgentnotices                                | 272 | 우선 순위가 낮은 메일에 대해 알림을 보내고 메일을 반환하기 전에 경과할 수 있는 시간을 지정합니다.                                                       |
| noreturnaddress                                 | 274 | RETURN_ADDRESS 옵션 값을 포스트마스터 주소 이름으로 사용합니다.                                                                     |
| noreturnpersonal                                | 274 | RETURN_PERSONAL 옵션 값을 포스트마스터 개인 이름으로 사용합니다.                                                                    |
| normalnotices                                   | 272 | 우선 순위가 중간인 메일에 대해 알림을 보내고 메일을 반환하기 전에 경과할 수 있는 시간을 지정합니다.                                                      |
| nosendpost                                      | 273 | 전달이 실패한 모든 메일의 복사본을 포스트마스터에게 보내지 않습니다.                                                                         |
| notices                                         | 272 | 알림을 보낸 후 메일이 반환되기 이전에 경과할 수 있는 시간을 지정합니다.                                                                      |
| nowarnpost                                      | 273 | 경고 메일의 복사본을 포스트마스터에게 보내지 않습니다.                                                                                 |
| postheadbody                                    | 274 | 헤더와 메일 내용을 모두 반환합니다.                                                                                           |

표 12-2 채널 키워드 범주화(기능별)

| 키워드                                                        | 페이지 | 정의                                                                                            |
|------------------------------------------------------------|-----|-----------------------------------------------------------------------------------------------|
| postheadonly                                               | 274 | 헤더만 포스트마스터에게 반환됩니다.                                                                           |
| returnaddress                                              | 274 | 로컬 포스트마스터에 대한 반송 주소를 지정합니다.                                                                   |
| returnenvelope                                             | 274 | 빈 봉투 반송 주소 사용을 제어합니다.                                                                         |
| returnpersonal                                             | 274 | 로컬 포스트마스터에 대한 개인 이름을 설정합니다.                                                                   |
| sendpost                                                   | 273 | 실패한 모든 메일의 복사본을 포스트마스터에게 보냅니다.                                                                |
| suppressfinal                                              | 272 | 원본 주소 형식이 있는 경우 알림 메일에서 최종 주소 형식을 생략합니다.                                                      |
| urgentnotices                                              | 272 | 우선 순위가 높은 메일에 대해 알림을 보내고 메일을 반환하기 전에 경과할 수 있는 시간을 지정합니다.                                      |
| useintermediate                                            | 272 | 목록을 확장한 이후 사용자 메일함 이름이 생성되기 이전에 생성되는 중간 주소 형식을 사용합니다.                                         |
| warnpost                                                   | 273 | 경고 메일의 복사본을 포스트마스터에게 보냅니다.                                                                    |
| <b>제어 및 작업 전송 처리</b><br>(기능에 대한 자세한 내용은 356페이지의 표 12-7 참조) |     |                                                                                               |
| backoff                                                    | 358 | 전달되지 않은 메일의 재전달 시도 간격입니다. normalbackoff, nonurgentbackoff, urgentbackoff 키워드로 대체될 수 있습니다.     |
| bidirectional                                              | 357 | 마스터 및 슬레이브 프로그램에서 사용되는 채널입니다.                                                                 |
| deferred                                                   | 358 | Deferred-delivery: 헤더 행을 인식하고 수락합니다.                                                          |
| expandchannel                                              | 364 | expandlimit 적용으로 인해 지연된 확장을 수행할 채널을 지정합니다.                                                    |
| expandlimit                                                | 364 | 주소 수가 이 제한을 초과할 경우 받는 메일을 "오프라인"으로 처리합니다.                                                     |
| filesperjob                                                | 360 | 단일 작업에서 처리할 대기열 항목의 수입입니다.                                                                    |
| immonurgent                                                | 358 | 높음, 중간 및 낮음 우선 순위 메일을 제출하면 바로 전달을 시작합니다.                                                      |
| master                                                     | 357 | 마스터 프로그램에서 사용되는 채널(master)입니다.                                                                |
| maxjobs                                                    | 360 | 채널에 대해 동시에 실행될 수 있는 최대 작업 수입입니다.                                                              |
| nodeferred                                                 | 358 | Deferred-delivery: 헤더 행을 수락하지 않음을 지정합니다.                                                      |
| nonurgentbackoff                                           | 358 | 낮음 우선 순위 메일의 재전달 시도 간격입니다.                                                                    |
| nonurgentblocklimit                                        | 363 | 이 크기 이상인 메일의 우선 순위를 낮음(두 번째 우선 순위 클래스) 이하로 지정합니다. 즉, 해당 메일은 항상 다음 정기 작업이 처리되는 동안 대기한 후 처리됩니다. |
| normalbackoff                                              | 358 | 중간 우선 순위 메일의 재전달 시도 간격입니다.                                                                    |
| normalblocklimit                                           | 363 | 이 크기 이상인 메일의 우선 순위를 낮음으로 지정합니다.                                                               |

**표 12-2** 채널 키워드 범주화(기능별)

| 키워드                                | 페이지 | 정의                                                                                                      |
|------------------------------------|-----|---------------------------------------------------------------------------------------------------------|
| noservice                          | 365 | 이 채널로 받는 메일에 대한 서비스 변환을 CHARSET-CONVERSION을 통해 활성화해야 합니다.                                               |
| pool                               | 360 | 채널에 대한 풀을 지정합니다. 현재 채널에 대한 전달 작업을 풀링해야 하는 풀 이름이 뒤에 와야 합니다.                                              |
| service                            | 365 | CHARSET-CONVERSION 항목에 관계 없이 서비스 변환을 무조건적으로 사용합니다.                                                      |
| slave                              | 357 | 슬레이브 프로그램에서 사용되는 채널(slave)입니다.                                                                          |
| threaddepth                        | 363 | 다중 스레드 SMTP 클라이언트를 사용하여 새 스레드를 트리거하는 메일 수입니다.                                                           |
| transactionlimit                   |     | 연결당 허용되는 메일 수를 제한합니다.                                                                                   |
| urgentbackoff                      | 358 | 높음 우선 순위 메일의 재전달 시도 간격입니다.                                                                              |
| urgentblocklimit                   | 363 | 이 크기 이상인 메일의 우선 순위를 중간으로 지정합니다.                                                                         |
| user                               | 398 | 파이프 채널에서 실행할 아이디를 나타내는 데 사용됩니다.                                                                         |
| <b>민감도 제한</b>                      |     |                                                                                                         |
| sensitivitycompanyconfidential     | 383 | 메일에 적용되는 최대 민감도 제한입니다.                                                                                  |
| sensitivitynormal                  | 383 | Normal이 메일에 대한 최대 민감도 제한으로 적용됩니다.                                                                       |
| sensitivitypersonal                | 383 | Personal이 메일에 대한 최대 민감도 제한으로 적용됩니다.                                                                     |
| sensitivityprivate                 | 383 | Private이 메일에 대한 최대 민감도 제한으로 적용됩니다.                                                                      |
| <b>메일, 사용자 할당량, 권한 및 인증 시도의 제한</b> |     |                                                                                                         |
| alternatechannel                   | 389 | alternateblocklimit, alternateblocklimit, alternatelinelimit 및 alternaterecipientlimit에 대한 대체 대상 채널입니다. |
| alternateblocklimit                | 389 | 메일을 alternativechannel로 보내기 이전에 메일의 블록 수 제한을 지정합니다.                                                     |
| alternatelinelimit                 | 389 | 메일을 alternativechannel로 보내기 이전에 메일의 행 수 제한을 지정합니다.                                                      |
| alternaterecipientlimit            | 389 | 메일을 alternativechannel로 보내기 이전에 메일의 수신자 수 제한을 지정합니다.                                                    |
| blocklimit                         | 388 | 각 메일에 허용되는 최대 MTA 블록 수입니다.                                                                              |
| disconnectbadauthlimit             | 388 | 세션의 연결이 끊어지기 전에 세션에 허용되는 인증 시도의 실패 횟수를 제한합니다.                                                           |
| disconnectbadcommandlimit          | 395 | 잘못된 세션 명령의 수를 제한합니다.                                                                                    |
| disconnectrecipientlimit           | 395 | 세션 수신자의 수를 제한합니다.                                                                                       |

표 12-2 채널 키워드 범주화(기능별)

| 키워드                                                      | 페이지 | 정의                                                                                            |
|----------------------------------------------------------|-----|-----------------------------------------------------------------------------------------------|
| disconnectrejectlimit                                    | 395 | 거부된 수신자의 수를 제한합니다.                                                                            |
| disconnecttransactionlimit                               | 395 | 트랜잭션 수를 제한합니다.                                                                                |
| headerlimit                                              | 393 | 가장 외부에 있는 주 메일 헤더의 최대 크기를 제한합니다.                                                              |
| holdexquota                                              | 391 | 할당량을 초과한 사용자의 메일을 보관합니다.                                                                      |
| holdlimit                                                | 364 | 주소 수가 이 제한을 초과할 경우 받는 메일을 보관합니다.                                                              |
| linelength                                               | 387 | 채널별로 허용되는 최대 메일 행 길이를 제한합니다.                                                                  |
| linelimit                                                | 388 | 각 메일에 허용되는 최대 행 수입니다.                                                                         |
| maxblocks                                                | 386 | 메일에 허용되는 최대 블록 수를 지정합니다.                                                                      |
| maxlines                                                 | 386 | 메일에 허용되는 최대 행 수를 지정합니다.                                                                       |
| nameparameterlengthlimit                                 | 392 | name content-type 및 filename content-disposition 매개 변수가 잘리는 지점을 제어합니다.                        |
| noblocklimit                                             | 388 | 각 메일에 허용되는 MTA 블록 수를 제한하지 않습니다.                                                               |
| noexquota                                                | 391 | 할당량을 초과하는 사용자의 메일을 메일 발송자에게 반환합니다.                                                            |
| nolinelimit                                              | 388 | 각 메일에 허용되는 행 수에 지정된 제한이 없습니다.                                                                 |
| nonurgentblocklimit                                      | 363 | 이 크기 이상인 메일의 우선 순위를 낮음(두 번째 우선 순위 클래스) 이하로 지정합니다. 즉, 해당 메일은 항상 다음 정기 작업이 처리되는 동안 대기한 후 처리됩니다. |
| normalblocklimit                                         | 363 | 이 크기 이상인 메일의 우선 순위를 낮음으로 지정합니다.                                                               |
| parameterlengthlimit                                     | 392 | 일반 content-type 및 content-disposition 매개 변수가 잘리는 지점을 조절합니다.                                   |
| recipientcutoff.                                         | 392 | 수신자가 이 값을 초과할 경우 메일을 거부합니다.                                                                   |
| recipientlimit                                           | 392 | 메일에 허용되는 수신자 주소 수를 제한합니다.                                                                     |
| rejectsmtplonglines                                      | 392 | 1000자(CRLF 포함)보다 긴 행을 포함하는 메일을 거부합니다.                                                         |
| sourceblocklimit                                         | 388 | 각 받는 메일에 허용되는 최대 MTA 블록 수입니다.                                                                 |
| truncatesmtplonglines                                    | 392 | 1000자를 초과하는 행을 자릅니다.                                                                          |
| wrapsmtplonglines                                        | 392 | 1000자를 초과하는 행을 줄 바꿈합니다.                                                                       |
| urgentblocklimit                                         | 363 | 이 크기 이상인 메일의 우선 순위를 중간으로 지정합니다.                                                               |
| <b>SMTP 인증, SASL 및 TLS</b><br>(기능에 대한 자세한 내용은 351페이지 참조) |     |                                                                                               |
| authrewrite                                              | 352 | MTA에서 인증된 메일 발송자 정보(사용 가능한 경우)를 헤더로 전파하도록 하기 위해 소스 채널에서 사용됩니다.                                |

**표 12-2** 채널 키워드 범주화(기능별)

| 키워드                                                         | 페이지 | 정의                                                                                      |
|-------------------------------------------------------------|-----|-----------------------------------------------------------------------------------------|
| maysaslserver                                               | 351 | 클라이언트가 SASL 인증 사용을 시도하도록 허용합니다.                                                         |
| maytls                                                      | 354 | MTA가 받는 연결에 TLS를 제공하고 보내는 연결에 TLS를 시도하도록 합니다.                                           |
| maytlsclient                                                | 354 | TLS를 지원하는 SMTP 서버에 메일을 보낼 경우 MTA SMTP 클라이언트가 TLS 사용을 시도합니다.                             |
| maytsserver                                                 | 354 | MTA SMTP 서버에서 STARTTLS 확장 지원을 광고하고 메일을 받을 때 TLS 사용을 허용합니다.                              |
| msexchange                                                  | 353 | TCP/IP 채널에서 사용되며 이 채널이 Microsoft Exchange 게이트웨이 및 클라이언트와 통신하는 채널임을 MTA에 알려줍니다.          |
| mustsaslserver                                              | 351 | SMTP 서버는 원격 클라이언트가 성공적으로 인증되지 않는 경우 메일이 수락되지 않습니다.                                      |
| musttls                                                     | 354 | 보내는 연결과 받는 연결 모두에서 TLS 사용을 강제합니다.                                                       |
| musttlsclient                                               | 354 | MTA SMTP 클라이언트는 메일을 보낼 때 TLS 사용을 강제합니다(MTA가 STARTTLS 명령을 실행하고 해당 명령이 성공해야 함).           |
| musttsserver                                                | 354 | MTA SMTP 서버에서 STARTTLS 확장 지원을 광고하고 메일을 받을 때 TLS 사용을 강제합니다.                              |
| nomsexchange                                                | 352 | 기본값입니다.                                                                                 |
| nosasl                                                      | 351 | SASL 인증이 허용 또는 시도되지 않습니다.                                                               |
| nosaslserver                                                | 351 | SASL 인증이 허용되지 않습니다.                                                                     |
| notls                                                       | 354 | TLS가 허용 또는 시도되지 않습니다.                                                                   |
| notlsclient                                                 | 354 | 보내는 연결에서 MTA SMTP 클라이언트가 TLS 사용을 시도하지 않습니다(보내는 연결 중에 STARTTLS 명령이 실행되지 않음).             |
| nottsserver                                                 | 354 | 받는 연결에서 MTA SMTP 서버의 TLS 사용이 허용되지 않습니다(SMTP 서버에서 STARTTLS 확장을 광고하지 않고 명령 자체가 허용되지도 않음). |
| saslswitchchannel                                           | 351 | 클라이언트가 SASL을 성공적으로 사용하면 받는 연결이 지정한 채널로 전환되게 합니다.                                        |
| tlsswitchchannel                                            | 354 | 클라이언트가 TLS 협상에 성공할 경우 받는 연결이 지정한 채널로 전환되게 합니다. 전환할 채널을 지정하는 필수 값을 사용합니다.                |
| <b>SMTP 명령 및 프로토콜</b><br>(기능에 대한 자세한 내용은 335페이지의 표 12-4 참조) |     |                                                                                         |
| allowetrn                                                   | 338 | ETRN 명령을 수락합니다.                                                                         |
| blocketrn                                                   | 338 | ETRN 명령을 차단합니다.                                                                         |
| checkehlo                                                   | 337 | SMTP 응답 배너를 검사하여 EHLO 또는 HELO 중 어떤 것을 사용할지 여부를 결정합니다.                                   |



표 12-2 채널 키워드 범주화(기능별)

| 키워드                 | 페이지 | 정의                                                                        |
|---------------------|-----|---------------------------------------------------------------------------|
| disableetrn         | 338 | ETRN SMTP 명령 지원을 사용하지 않습니다.                                               |
| domainetrn          | 338 | 도메인을 지정하는 ETRN 명령만 수락합니다.                                                 |
| domainvrfy          | 339 | 전체 주소를 사용하여 VRFY 명령을 실행합니다.                                               |
| ehlo                | 337 | 초기 연결에 SMTP EHLO 명령을 사용합니다.                                               |
| eightbit            | 341 | 채널에서 8비트 문자를 지원합니다.                                                       |
| eightnegotiate      | 341 | 채널에서 가능할 경우 8비트 전송 사용을 협상합니다.                                             |
| eightstrict         | 341 | 협상되지 않은 8비트 데이터를 포함하는 메일을 거부합니다.                                          |
| expnallow           | 340 | DISABLE_EXPAND SMTP 채널 옵션을 사용하여 SMTP 서버 수준에서 사용 불가능으로 설정했다라도 EXPN을 허용합니다. |
| expndisable         | 340 | EXPN을 무조건적으로 사용 불가능하게 합니다.                                                |
| expndefault         | 340 | SMTP 서버에 사용하도록 설정된 경우 EXPN을 허용합니다.                                        |
| localvrfy           | 339 | 로컬 주소를 사용하여 VRFY 명령을 실행합니다.                                               |
| mailfromdnsverify   | 340 | MAIL FROM:명령에 사용된 도메인이 DNS에 있는지 여부를 확인합니다                                 |
| noehlo              | 337 | EHLO 명령을 사용하지 않습니다.                                                       |
| nomailfromdnsverify | 340 | MAIL FROM:명령에 사용된 도메인이 DNS에 있는지 여부를 확인하지 않습니다.                            |
| nosendetrn          | 338 | ETRN 명령을 보내지 않습니다.                                                        |
| nosmtp              | 337 | SMTP 프로토콜을 지원하지 않습니다. 기본값입니다.                                             |
| novrfy              | 339 | VRFY 명령을 실행하지 않습니다.                                                       |
| sendetrn            | 338 | ETRN 명령을 보냅니다.                                                            |
| sevenbit            | 341 | 8비트 문자를 지원하지 않으므로 8비트 문자를 인코딩해야 합니다.                                      |
| silentetrn          | 338 | 채널 정보를 에코하지 않고 ETRN 명령을 수락합니다.                                            |
| smtp                | 337 | SMTP 프로토콜을 지원합니다. smtp 키워드는 모든 SMTP 채널에 필수입니다(이 키워드는 smtp_crorlf와 동일함).   |
| smtp_cr             | 337 | 후행 줄 바꿈(LF) 없이 캐리지 리턴(CR)을 사용하여 행을 종료합니다.                                 |
| smtp_crlf           | 337 | 행을 캐리지 리턴(CR) 줄 바꿈(LF) 시퀀스로 종료해야 합니다.                                     |
| smtp_crorlf         | 337 | 행을 캐리지 리턴(CR), 줄 바꿈(LF) 시퀀스 또는 전체 CRLF를 사용하여 종료해야 합니다.                    |
| smtp_lf             | 337 | 선행 CR 없이 줄 바꿈(LF)을 사용하여 행을 종료합니다.                                         |
| streaming           | 343 | 채널에 연결된 프로토콜에 사용되는 프로토콜 스트리밍의 범위를 제어합니다.                                  |

표 12-2 채널 키워드 범주화(기능별)

| 키워드                                                                | 페이지 | 정의                                                                                                            |
|--------------------------------------------------------------------|-----|---------------------------------------------------------------------------------------------------------------|
| vrifyallow                                                         | 339 | VERFY 명령에 대한 정보 응답을 제공합니다.                                                                                    |
| vrifydefault                                                       | 339 | 채널의 HIDE_VERIFY 옵션 설정에 따라 VRFY 명령에 대한 기본 응답을 제공합니다.                                                           |
| vrifyhide                                                          | 339 | SMTP VRFY 명령에 대한 위장 응답을 제공합니다.                                                                                |
| <b>TCP/IP 연결 및 DNS 조회 지원</b><br>(기능에 대한 자세한 내용은 344페이지의 표 12-5 참조) |     |                                                                                                               |
| cacheeverything                                                    | 346 | 모든 연결 정보를 캐시합니다.                                                                                              |
| cachefailures                                                      | 346 | 연결 실패 정보만 캐시합니다.                                                                                              |
| cachesuccesses                                                     | 346 | 연결 성공 정보만 캐시합니다.                                                                                              |
| connectalias                                                       | 370 | 수신자 주소에 나열된 모든 호스트에 전달합니다.                                                                                    |
| connectcanonical                                                   | 370 | MTA가 연결되는 시스템에 대한 호스트 별칭에 연결합니다.                                                                              |
| daemon                                                             | 350 | 봉투 주소에 관계 없이 특정 호스트 시스템에 연결합니다.                                                                               |
| defaultmx                                                          | 348 | 채널이 네트워크에서 MX 조회를 수행할지 여부를 결정합니다.                                                                             |
| defaultnameservers                                                 | 349 | TCP/IP 스택의 이름 서버 선택을 참조합니다.                                                                                   |
| forwardcheckdelete                                                 | 346 | 역방향 DNS 조회를 수행한 경우 반환된 이름에 대한 정방향 조회를 수행하여 반환된 IP 번호가 원본과 일치하는지 확인합니다. 원본과 일치하지 않는 경우 이름을 삭제하고 IP 주소를 사용합니다.  |
| forwardchecknone                                                   | 346 | DNS 역방향 조회 후 정방향 조회를 수행하지 않습니다.                                                                               |
| forwardchecktag                                                    | 346 | 역방향 DNS 조회를 수행한 경우 반환된 이름에 대한 정방향 조회를 수행하여 반환된 IP 번호가 원본과 일치하는지 확인합니다. 원본과 일치하지 않는 경우 이름에 * 태그를 붙입니다.         |
| identnone                                                          | 347 | IDENT 조회를 수행하지 않고, IP를 호스트 이름으로 변환하고, 호스트 이름과 IP 주소를 모두 Received: 헤더에 포함합니다.                                  |
| identnonelimited                                                   | 347 | IDENT 조회를 수행하지 않고, IP를 호스트 이름으로 변환하지만 채널 전환 중에 호스트 이름을 사용하지 않고, 호스트 이름과 IP 주소를 모두 Received: 헤더에 포함합니다.        |
| identnonenumeric                                                   | 347 | IDENT 조회를 수행하지 않거나 IP를 호스트 이름으로 변환하지 않습니다.                                                                    |
| identnon symbolic                                                  | 347 | IDENT 조회를 수행하지 않고 IP를 호스트 이름으로 변환하고 호스트 이름만 Received: 헤더에 포함합니다.                                              |
| identtcp                                                           | 347 | 받는 SMTP 연결에서 IDENT 조회를 수행하고 IP를 호스트 이름으로 변환하고 호스트 이름과 IP 주소를 모두 Received: 헤더에 포함합니다.                          |
| identtcp limited                                                   | 347 | 받는 SMTP 연결에 IDENT 조회를 수행하고 IP를 호스트 이름으로 변환하지만 채널 전환 중에 호스트 이름을 사용하지 않습니다. 호스트 이름과 IP 주소를 Received: 헤더에 포함합니다. |

표 12-2 채널 키워드 범주화(기능별)

| 키워드                 | 페이지 | 정의                                                                                                     |
|---------------------|-----|--------------------------------------------------------------------------------------------------------|
| indentnumeric       | 347 | 받는 SMTP 연결에서 IDENT 조회를 수행하지만 IP를 호스트 이름으로 변환하지 않습니다.                                                   |
| identsymbolic       | 347 | 받는 SMTP 연결에서 IDENT 조회를 수행하고 IP를 호스트 이름으로 변환하고 호스트 이름만 Received: 헤더에 포함합니다.                             |
| interfaceaddress    | 345 | 지정된 TCP/IP 인터페이스 주소에 바인딩합니다.                                                                           |
| lastresort          | 349 | 마지막 호스트를 지정합니다.                                                                                        |
| mailfromdnsverify   | 340 | MAIL FROM: 명령에 사용된 도메인이 DNS에 있는지 여부를 확인합니다.                                                            |
| mx                  | 348 | TCP/IP 네트워크 및 소프트웨어가 MX 레코드 조회를 지원합니다.                                                                 |
| nameservers         | 349 | TCP/IP 스택의 자체 이름 서버 선택을 참조하는 대신 참조할 이름 서버 목록을 지정합니다. nameservers에는 이름 서버에 대한 공백으로 구분된 IP 주소 목록이 필요합니다. |
| nocache             | 346 | 연결 정보를 캐시하지 않습니다.                                                                                      |
| nomailfromdnsverify | 340 | MAIL FROM: 명령에 사용된 도메인이 DNS에 있는지 여부를 확인하지 않습니다.                                                        |
| nomx                | 348 | TCP/IP 네트워크가 MX 조회를 지원하지 않습니다.                                                                         |
| nonrandommx         | 348 | MX 조회를 수행하고 반환된 항목을 같은 우선 순위로 임의화하지 않습니다.                                                              |
| port                | 345 | SMTP 연결에 대한 기본 포트 번호를 지정합니다. 표준 포트는 25입니다.                                                             |
| randommx            | 348 | MX 조회를 수행하고 반환된 항목을 같은 우선 순위로 임의화합니다.                                                                  |
| single              | 350 | 채널의 각 대상 주소에 대해 별도의 메일 복사본을 만들도록 지정합니다.                                                                |
| single_sys          | 350 | 사용된 각 대상 시스템에 대해 단일 메일 복사본을 만듭니다.                                                                      |
| threaddepth         | 363 | 다중 스레드 SMTP 클라이언트를 사용하여 새 스레드를 트리거하는 메일 수입니다.                                                          |
| <b>기타</b>           |     |                                                                                                        |
| deferralrejectlimit | 403 | 잘못된 RCPT TO: 주소 수에 제한을 설정합니다.                                                                          |
| dispositionchannel  | 397 | 처음에 전달 상태 알림(DSN)을 대기열에 포함하기 위한 장소로 프로세스 채널을 대체합니다.                                                    |
| destinationfilter   | 398 | 보내는 메일에 적용할 채널 수준 필터를 지정하기 위해 일반 MTA 채널에서 사용됩니다.                                                       |
| filter              | 398 | 필터 파일 위치를 설명하는 필수 URL 인수를 가집니다.                                                                        |
| nodestinationfilter | 398 | 어느 채널 방향에 대해서도 채널 메일함 필터를 사용하지 않습니다.                                                                   |
| nosourcefilter      | 398 | 소스 채널에 대해 채널 메일함 필터를 사용하지 않습니다.                                                                        |
| nofilter            | 398 | 기본값이며 채널에 대해 사용자 메일함 필터를 사용하지 않는다는 것을 의미합니다.                                                           |

**표 12-2** 채널 키워드 범주화(기능별)

| 키워드                 | 페이지 | 정의                                                                          |
|---------------------|-----|-----------------------------------------------------------------------------|
| notificationchannel | 397 | 처음에 MDN(Message Disposition Notification)을 대기열에 포함하기 위한 장소로 프로세스 채널을 대체합니다. |
| sourcefilter        | 398 | 받는 메일에 적용할 채널 수준 필터를 지정하기 위해 일반 MTA 채널에서 사용됩니다.                             |
| submit              | 397 | 채널을 제출 전용 채널로 표시하는 데 사용됩니다.                                                 |
| user                | 398 | 파이프 채널에서 실행할 아이디를 나타내는 데 사용됩니다.                                             |

## 채널 기본값 구성

많은 구성은 모든 채널 또는 거의 모든 채널에서 다양한 채널 키워드 반복을 포함합니다. 그러한 구성의 유지 관리는 귀찮고 오류가 발생하기 쉽습니다. 일부 구성을 단순화하기 위해 다양한 채널의 기본값으로 사용할 키워드를 지정할 수 있습니다.

예를 들어, 구성 파일의 다음 행은 해당 행 다음에 있는 모든 채널 블록이 해당 행에 지정된 키워드를 상속함을 나타냅니다.

```
defaults keyword1 keyword2 keyword3 ...
```

defaults 행은 실제로 채널을 지정하지 않은 채 키워드 기본값을 변경하는 특수 채널 블록으로 간주할 수 있습니다. 또한, defaults 행에는 추가 채널 블록 정보 행이 필요하지 않습니다(무시하도록 지정된 경우).

지정 가능한 defaults 행 수에 대한 제한이 없습니다. 즉, 여러 기본값 행의 효과가 최근에 발생한 앞 행(위에서 아래로 읽음)에 누적됩니다.

구성 파일의 특정 지점(예: 외부 파일에 있는 채널 블록의 독립형 섹션의 시작 부분)에서 시작하여 defaults 행의 효과를 무조건적으로 제거하는 것이 좋을 수도 있습니다.

nodefaults 행이 이러한 목적으로 제공됩니다. 예를 들어, 구성 파일에 다음 행을 삽입하면 이전의 기본값 채널에서 지정된 모든 설정이 무효화되고 구성이 기본값을 지정하지 않은 경우에 적용되는 상태로 돌아갑니다.

```
nodefaults
```

일반 채널 블록과 마찬가지로 빈 행을 사용하여 각 `defaults` 또는 `nodefaults` 채널 블록을 다른 채널 블록과 구분해야 합니다. `defaults` 및 `nodefaults` 채널 블록은 구성 파일에서 로컬 채널 앞에 표시될 수 있는 유일한 채널 블록입니다. 그러나, 다른 채널 블록과 마찬가지로 이 채널 블록도 마지막 다시 쓰기 규칙 뒤에 표시해야 합니다.

## SMTP 채널 구성

설치 유형에 따라 **Messaging Server**는 설치 시 여러 SMTP 채널을 제공합니다(아래 표 참조). 이러한 채널은 SMTP over TCP/IP를 구현합니다. 다중 스레드 TCP SMTP 채널은 디스패처의 제어에 따라 실행되는 다중 스레드 SMTP 서버를 포함합니다. 보내는 SMTP 메일은 `tcp_smtp_client` 채널 프로그램에서 처리되고 필요한 경우 Job Controller의 제어에 따라 실행됩니다.

**표 12-3** SMTP 채널

| 채널                        | 정의                                                                                                            |
|---------------------------|---------------------------------------------------------------------------------------------------------------|
| <code>tcp_local</code>    | 원격 SMTP 호스트로부터 인바운드 메일을 받습니다. 스마트 호스트/방화벽 구성을 사용하는지 여부에 따라 아웃바운드 메일을 원격 SMTP에 직접 보내거나 스마트 호스트/방화벽 시스템으로 보냅니다. |
| <code>tcp_intranet</code> | 인트라넷 내에서 메일을 주고 받습니다.                                                                                         |
| <code>tcp_auth</code>     | <code>tcp_local</code> 에 대한 전환 채널로 사용되며 릴레이 차단 제한을 피하도록 인증된 사용자를 <code>tcp_auth</code> 채널로 전환합니다.             |
| <code>tcp_submit</code>   | 예약된 제출 포트 587에서 메일 제출(일반적으로 사용자 에이전트로부터)을 수락합니다(RFC 2476 참조).                                                 |
| <code>tcp_tas</code>      | IA 특수 채널이 통합 메시징을 수행하는 사이트에서 사용됩니다.                                                                           |

이 절에 설명된 대로 채널 키워드를 추가하거나 제거하여 이러한 채널의 정의를 수정하거나 새 채널을 만들 수 있습니다. 또한, 옵션 파일을 사용하여 TCP/IP 채널의 다양한 특성을 제어할 수 있습니다. 옵션 파일은 MTA 구성 디렉토리(`msg_svr_base/config`)에 저장하고 `x_option`으로 이름을 지정해야 합니다. 여기서 `x`는 채널의 이름입니다. 자세한 내용은 *Sun Java System Messaging Server Administration Reference*를 참조하십시오.

이 절은 다음 내용으로 구성되어 있습니다.

- 334페이지의 "SMTP 채널 옵션 구성"

- 335페이지의 "SMTP 명령 및 프로토콜 지원"
- 343페이지의 "TCP/IP 연결 및 DNS 조회 지원"
- 351페이지의 "SMTP 인증, SASL 및 TLS"
- 352페이지의 "헤더의 SMTP AUTH에서 인증된 주소 사용"
- 352페이지의 "헤더의 SMTP AUTH에서 인증된 주소 사용"
- 353페이지의 "Microsoft Exchange 게이트웨이 채널 지정"
- 354페이지의 "전송 계층 보안"

## SMTP 채널 옵션 구성

TCP/IP 채널 옵션 파일은 TCP/IP 채널의 다양한 특성을 제어합니다. 채널 옵션 파일은 MTA 구성 디렉토리에 저장하고 `x_option`으로 이름을 지정해야 합니다. 여기서 `x`는 채널의 이름입니다. 예를 들어, `/msg_svr_base/config/tcp_local_option`입니다.

옵션 파일은 하나 이상의 키워드와 관련 값으로 구성됩니다. 예를 들어, 옵션 파일에 `DISABLE_EXPAND` 키워드를 포함시키고 값을 1로 설정하여 메일 목록 확장을 비활성화할 수 있습니다.

다른 옵션 파일 키워드를 사용하여 다음을 수행할 수 있습니다.

- 메일당 허용되는 수신자 수에 대한 제한 설정 (`ALLOW_RECIPIENTS_PER_TRANSACTION`)
- 연결당 허용되는 메일 수에 대한 제한 설정 (`ALLOW_TRANSACTIONS_PER_SESSION`)
- MTA 로그 파일에 기록되는 정보 유형 세부 조정 (`LOG_CONNECTION`, `LOG_TRANSPORTINFO`)
- 클라이언트 채널 프로그램에 허용되는 최대 동시 아웃바운드 연결 수 지정 (`MAX_CLIENT_THREADS`)

모든 채널 옵션 키워드 및 구문에 대한 자세한 내용은 *Messaging Server Reference Manual*을 참조하십시오.

## SMTP 명령 및 프로토콜 지원

SMTP 채널이 EHLO, ETRN, EXPN, VRFY 등과 같은 특정 SMTP 명령을 지원하는지 여부를 지정할 수 있습니다. 또한, 채널이 DNS 도메인 확인을 지원하는지 여부, 채널에서 행 종결 기호로 사용되는 문자 등을 지정할 수 있습니다. 이 절은 다음 내용으로 구성되어 있습니다.

- 337페이지의 "채널 프로토콜 선택 및 행 종결 기호"
- 337페이지의 "EHLO 명령 지원"
- 338페이지의 "ETRN 명령 지원"
- 339페이지의 "VRFY 명령 지원"
- 340페이지의 "DNS 도메인 확인"
- 341페이지의 "문자 세트 레이블링 및 8비트 데이터"
- 343페이지의 "프로토콜 스트리밍"

표 12-4는 이 절에서 설명하는 키워드를 요약해서 보여 줍니다.

표 12-4 SMTP 명령 및 프로토콜 키워드

| 채널 키워드                   | 설명                                                                      |
|--------------------------|-------------------------------------------------------------------------|
| <b>프로토콜 선택 및 행 종결 기호</b> | <b>채널이 SMTP 프로토콜을 지원하는지 여부를 지정하고 행 종결 기호로 사용되는 문자 시퀀스를 지정합니다.</b>       |
| smtp                     | SMTP 프로토콜을 지원합니다. smtp 키워드는 모든 SMTP 채널에 필수입니다(이 키워드는 smtp_crorlf와 동일함). |
| nosmtp                   | SMTP 프로토콜을 지원하지 않습니다. 기본값입니다.                                           |
| smtp_cr                  | 후행 줄 바꿈(LF) 없이 캐리지 리턴(CR)을 사용하여 행을 종료합니다.                               |
| smtp_crlf                | 행을 캐리지 리턴(CR) 줄 바꿈(LF) 시퀀스로 종료해야 합니다.                                   |
| smtp_lf                  | 선행 CR 없이 줄 바꿈(LF)을 사용하여 행을 종료합니다.                                       |
| smtp_crorlf              | 행을 캐리지 리턴(CR), 줄 바꿈(LF) 시퀀스 또는 전체 CRLF를 사용하여 종료해야 합니다.                  |
| <b>EHLO 키워드</b>          | <b>채널에서 EHLO 명령을 처리하는 방법을 지정합니다.</b>                                    |
| ehlo                     | 초기 연결에 SMTP EHLO 명령을 사용합니다.                                             |
| checkehlo                | SMTP 응답 배너를 검사하여 EHLO 또는 HELO 중 어떤 것을 사용할지 여부를 결정합니다.                   |
| noehlo                   | EHLO 명령을 사용하지 않습니다.                                                     |

표 12-4 SMTP 명령 및 프로토콜 키워드

| 채널 키워드                 | 설명                                                                                                  |
|------------------------|-----------------------------------------------------------------------------------------------------|
| <b>ETRN 키워드</b>        | <b>채널에서 ETRN 명령(대기열 처리 요청)을 처리하는 방법을 지정합니다.</b>                                                     |
| allowetrn              | ETRN 명령을 수락합니다.                                                                                     |
| blocketrn              | ETRN 명령을 차단합니다.                                                                                     |
| domainetrn             | 도메인을 지정하는 ETRN 명령만 수락합니다.                                                                           |
| silentetrn             | 채널 정보를 에코하지 않고 ETRN 명령을 수락합니다.                                                                      |
| sendetrn               | ETRN 명령을 보냅니다.                                                                                      |
| nosendetrn             | ETRN 명령을 보내지 않습니다.                                                                                  |
| <b>VRFY 키워드</b>        | <b>채널에서 VRFY 명령을 처리하는 방법을 지정합니다.</b>                                                                |
| domainvrfy             | 전체 주소를 사용하여 VRFY 명령을 실행합니다.                                                                         |
| localvrfy              | 로컬 주소를 사용하여 VRFY 명령을 실행합니다.                                                                         |
| novrfy                 | VRFY 명령을 실행하지 않습니다.                                                                                 |
| vrfyallow              | VRFY 명령에 대한 정보 응답을 제공합니다.                                                                           |
| vrfydefault            | 채널의 HIDE_VERIFY 옵션 설정에 따라 VRFY 명령에 대한 기본 응답을 제공합니다.                                                 |
| vrfyhide               | SMTP VRFY 명령에 대한 위장 응답을 제공합니다.                                                                      |
| <b>EXPN 키워드</b>        | <b>채널에서 EXPN 키워드를 처리하는 방법을 지정합니다.</b>                                                               |
| expnallow              | DISABLE_EXPAND SMTP 채널 옵션을 사용하여 SMTP 서버 수준에서 사용 불가능으로 설정했더라도 EXPN을 허용합니다.                           |
| expndisable            | EXPN을 무조건적으로 사용 불가능하게 합니다.                                                                          |
| expndefault            | SMTP 서버에 사용하도록 설정된 경우 EXPN을 허용합니다. 기본값입니다.                                                          |
| <b>DNS 도메인 확인</b>      | <b>채널에서 DNS 도메인 확인을 수행하는지 여부를 지정합니다.</b>                                                            |
| mailfromdnsverify      | MAIL FROM:명령에 사용된 도메인이 DNS에 있는지 여부를 확인합니다.                                                          |
| nomailfromdnsverify    | MAIL FROM:명령에 사용된 도메인이 DNS에 있는지 여부를 확인하지 않습니다.                                                      |
| <b>문자 세트 및 8비트 데이터</b> | <b>채널에서 8비트 데이터를 처리하는 방법을 지정합니다.<br/>(주: 이러한 키워드는 일반적으로 SMTP 채널에서 사용되지만 모든 종류의 채널과 관련될 수 있습니다.)</b> |
| charset7               | 7비트 텍스트 메일과 관련된 기본 문자 세트입니다.                                                                        |
| charset8               | 8비트 텍스트 메일과 관련된 기본 문자 세트입니다.                                                                        |



표 12-4 SMTP 명령 및 프로토콜 키워드

| 채널 키워드           | 설명                                          |
|------------------|---------------------------------------------|
| charsetesc       | 이스케이프 문자를 포함하는 7비트 텍스트 메일과 관련된 기본 문자 세트입니다. |
| eightbit         | 채널에서 8비트 문자를 지원합니다.                         |
| eightnegotiate   | 채널에서 가능할 경우 8비트 전송 사용을 협상합니다.               |
| eightstrict      | 채널은 잘못된 8비트 데이터를 포함하는 메일을 거부해야 합니다.         |
| sevenbit         | 채널에서 8비트 문자를 지원하지 않으므로 8비트 문자를 인코딩해야 합니다.   |
| <b>프로토콜 스트리밍</b> | <b>사용할 채널에 대한 프로토콜 스트리밍 범위를 지정합니다.</b>      |
| streaming        | 채널에 연결된 프로토콜에 사용되는 프로토콜 스트리밍의 범위를 제어합니다.    |

## 채널 프로토콜 선택 및 행 종결 기호

키워드: smtp, nosmtp, smtp\_crlf, smtp\_cr, smtp\_crorlf, smtp\_lf

smtp 및 nosmtp 키워드는 채널이 SMTP 프로토콜을 지원하는지 여부를 지정합니다.

smtp 키워드 또는 이 키워드의 변형 중 하나가 모든 SMTP 채널에 필수입니다.

smtp\_crlf, smtp\_cr, smtp\_crorlf 및 smtp\_lf 키워드는 SMTP에서 MTA가 행 종결 기호로 사용하는 문자 시퀀스를 지정하는 데 사용될 수 있습니다. smtp\_crlf 키워드는 행을 캐리지 리턴(CR) 줄 바꿈(LF) 시퀀스로 종료해야 함을 의미합니다. smtp\_lf 또는 smtp 키워드는 선행 CR 없이 LF를 사용할 수 있음을 의미합니다. 마지막으로 smtp\_cr은 후행 LF 없이 CR을 사용할 수 있음을 의미합니다. 이러한 옵션은 받는 메일의 처리에만 영향을 미칩니다.

SMTP 표준은 행 종결 기호로 CRLF를 필요로 하기 때문에 MTA는 항상 표준 CRLF 시퀀스를 생성합니다. 여러 가지 smtp 키워드는 MTA에서 추가 비표준 행 종결 기호를 수락할지 여부만 제어합니다. 예를 들어, MTA가 적절한 SMTP 메일만 수락하고 비표준행 종결 기호가 있는 메일을 거부하게 하려면 smtp\_crlf를 지정할 수 있습니다.

## EHLO 명령 지원

키워드: ehlo, noehlo, checkehlo

추가 명령 협상을 허용하도록 SMTP 프로토콜이 확장되었습니다(RFC 1869). 이를 위해 RFC 821의 HELO 명령을 대체하는 새 EHLO 명령이 사용됩니다. 확장 SMTP 서버는 지원하는 확장 목록을 제공하여 EHLO에 응답합니다. 확장되지 않은 서버가 알 수 없는 명령 오류를 반환하면 클라이언트는 이전의 HELO 명령을 대신 보냅니다.

이 폴백 전략은 일반적으로 확장된 서버와 확장되지 않은 서버 모두에 잘 적용됩니다. 그러나 RFC 821에 따라 SMTP를 구현하지 않은 서버에서는 문제가 발생할 수 있습니다. 특히, 일부 비호환 서버에서는 알 수 없는 명령을 수신할 경우 연결을 끊는 것으로 알려져 있습니다.

SMTP 클라이언트는 서버에서 EHLO를 수신할 때 연결을 끊는 경우 다시 연결한 다음 HELO를 사용하는 전략을 구현합니다. 원격 서버에서 EHLO를 수신할 때 연결을 끊고 문제 상태로 전환하는 경우에는 이 전략을 적용할 수 없습니다.

그런 상황에 대처하도록 ehlo, noehlo 및 checkehlo 채널 키워드가 제공됩니다. ehlo 키워드는 모든 초기 연결 시도에서 EHLO 명령을 사용하도록 MTA에 지시합니다. noehlo 키워드는 모든 EHLO 명령 사용을 비활성화합니다. checkehlo 키워드는 문자열 "ESMTP"에 대해 원격 SMTP 서버가 반환하는 응답 배너를 테스트합니다. 이 문자열이 있는 경우 EHLO가 사용되고, 없는 경우 HELO가 사용됩니다. 기본 동작은 모든 초기 연결 시도에서 EHLO를 사용하는 것입니다. 배너 행에 문자열 "fire away"가 없는 경우에는 HELO가 사용됩니다. ehlo 및 checkehlo 키워드로부터 발생하는 동작 사이에 위치하는 이 기본 동작에 해당하는 키워드가 없습니다.

## ETRN 명령 지원

키워드: allowetrn, blocketrn, disableetrn, domainetrn, silentetrn, sendetrn, nosendetrn, novrfy

RFC 1985에 정의되어 있는 ETRN 명령은 SMTP 클라이언트와 서버가 상호 작용하여 서버에서 지정된 호스트로 보낼 메일 대기열 처리를 시작할 수 있도록 SMTP 서비스를 확장합니다.

SMTP 클라이언트는 ETRN을 사용하여 원격 SMTP 서버에서 SMTP 클라이언트에 보낼 메일 대기열의 처리를 시작하도록 요청할 수 있습니다. 즉, ETRN을 사용하면 원격 SMTP 시스템에서 수신하는 메일에 대해 원격 SMTP 시스템 "폴링"을 구현할 수 있습니다. 이 방법은 서로 일시적으로만 연결하는 시스템에 유용할 수 있습니다. 예를 들어, 전화 접속을 통해서만 인터넷에 연결하는 다른 사이트에 대해 보조 MX(Mail eXchange) 호스트로 설정되는 사이트가 있습니다. 이 명령을 사용하여 원격 전화 접속 서버의 메일 전달 요청을 허용합니다.

SMTP 클라이언트는 SMTP ETRN 명령줄에서 메일을 보낼 시스템의 이름(일반적으로 SMTP 클라이언트 시스템 자체 이름)을 지정합니다. 원격 SMTP 서버가 ETRN 명령을 지원하는 경우 해당 서버는 개별 프로세스를 트리거하여 명명된 시스템에 다시 연결하고 해당 명명된 시스템에 대해 전달 대기 중인 메일을 보냅니다.

### **ETRN 명령에 대한 응답**

allowetrn, blocketrn, domainetrn 및 silentetrn 키워드는 보내는 SMTP 클라이언트가 MTA에 MTA 대기열의 메일을 전달하도록 요청하는 ETRN 명령을 실행할 때 MTA 응답을 제어합니다.

기본적으로 MTA는 모든 ETRN 명령을 수락하려고 시도합니다. 즉, allowetrn 키워드가 사용됩니다. 채널 정의에 blocketrn 키워드를 포함하여 MTA에서 ETRN 명령을 수락하지 않도록 지정할 수 있습니다.

silentetrn 키워드를 포함하여 도메인과 일치하고 MTA에서 실행할 채널의 이름을 에코하지 않고 모든 ETRN 명령을 수락하도록 지정할 수 있습니다. domainetrn 키워드는 MTA가 도메인을 지정하는 ETRN 명령만 사용하도록 지정합니다. 또한, 도메인과 일치하고 MTA에서 실행할 채널의 이름을 에코하지 않도록 지정합니다.

disableetrn은 ETRN 명령을 전혀 지원하지 않습니다. ETRN은 SMTP 서버에서 지원되는 명령으로 광고되지 않습니다.

### **ETRN 명령 보내기**

sendetrn 및 nosendetrn 채널 키워드는 MTA가 SMTP 연결을 시작할 때 ETRN 명령을 보내는지 여부를 제어합니다. 기본값은 nosendetrn이며 MTA가 ETRN 명령을 보내지 않음을 의미합니다. sendetrn 키워드는 원격 SMTP 서버가 ETRN을 지원할 경우 ETRN 명령을 보내도록 MTA에 지시합니다. sendetrn 키워드는 메일이 전달 시도를 받도록 요청하는 시스템 이름 앞에 입력해야 합니다.

### **VRFY 명령 지원**

키워드: domainvrfy, localvrfy, vrfyallow, vrfydefault, vrfyhide

VRFY 명령을 사용하면 SMTP 클라이언트가 SMTP 서버에 특정 아이디에 대한 메일이 있는지 확인하라는 요청을 서버에 보낼 수 있습니다. VRFY 명령은 RFC 821에 정의되어 있습니다.

서버는 사용자가 로컬 사용자인지 여부, 메일 전달 여부 등을 나타내는 응답을 보냅니다. 250 응답은 아이디가 로컬임을 나타내고, 251 응답은 아이디가 로컬이 아니지만 서버가 메일을 전달할 수 있음을 나타냅니다. 서버 응답에는 메일함 이름이 포함되어 있습니다.

## VERFY 명령 보내기

정상적인 환경에서는 VRFY 명령을 SMTP 대화 상자의 일부로 실행할 이유가 없습니다. SMTP RCPT TO 명령은 VRFY 명령과 동일한 기능을 수행하고 해당 오류를 반환해야 합니다. RCPT TO에 주소를 받아들이는 다음 나중에 바운스할 수 있는 서버가 존재하지만, 이러한 서버는 VRFY 명령의 일부로 보다 집중적인 검사를 수행합니다.

기본적으로 MTA는 VRFY 명령을 보내지 않습니다(novrfy 키워드 사용).

필요한 경우 채널 정의에 domainvrfy 또는 localvrfy 키워드를 포함하여 SMTP VRFY 명령을 실행하도록 MTA를 구성할 수 있습니다. domainvrfy 키워드는 전체 주소 (user@host)를 인수로 갖는 VRFY 명령이 실행되게 합니다. localvrfy 키워드는 MTA에서 주소의 로컬 부분(user) 만 사용하여 VRFY 명령이 실행되게 합니다.

## VERFY 명령에 대한 응답

vrfyallow, vrfydefault 및 vrfyhide 키워드는 보내는 SMTP 클라이언트가 SMTP VRFY 명령을 실행할 때 SMTP 서버의 응답을 제어합니다.

vrfyallow 키워드는 자세한 정보 응답을 실행하도록 MTA에 지시합니다.

vrfydefault는 HIDE\_VERIFY=1 채널 옵션이 지정되어 있지 않은 경우 자세한 정보 응답을 제공하도록 MTA에 지시합니다. vrfyhide 키워드는 모호한 응답만 생성하도록 MTA에 지시합니다. 이러한 키워드는 동일한 SMTP 서버를 통해 처리되는 모든 받는 TCP/IP 채널에 일반적으로 적용되는 HIDE\_VERIFY 옵션과 달리 VRFY 응답을 채널 단위로 제어할 수 있습니다.

## EXPN 지원

키워드: expnallow, expndisable, expndefault

expnallow는 DISABLE\_EXPAND SMTP 채널 옵션을 사용하여 SMTP 서버 수준에서 사용 불가능으로 설정했다라도 EXPN을 허용합니다. expndisable은 EXPN을 무조건적으로 사용 불가능하게 합니다. expndefault는 SMTP 서버에 사용하도록 설정된 경우 EXPN을 허용합니다(기본값). 확장은 목록 단위로 비활성화할 수 있지만 서버 수준에서 비활성화하면 목록별 설정이 부적절하게 됩니다.

## DNS 도메인 확인

키워드: mailfromdnsverify, nomailfromdnsverify

받는 TCP/IP 채널에서 mailfromdnsverify를 설정하면 MTA가 DNS의 항목이 SMTP MAIL FROM 명령에 사용된 도메인에 있는지 확인하여 해당 항목이 없는 경우 메일을 거부합니다. 기본값인 nomailfromdnsverify는 확인이 수행되지 않음을 의미합니다. 반송 주소 도메인에 대해 DNS 확인을 수행하면 일부 유효한 메일이 거부될 수 있습니다. 예를

들어, 도메인 이름을 아직 등록하지 않은 합법적인 사이트에서 또는 DNS에 잘못된 정보가 있는 경우 거부됩니다. 이는 RFC 1123, *Requirements for Internet Hosts*에 명시되어 있는 전자 메일 수락 및 전달에 있어 관대함을 요구하는 조항에 위반됩니다. 그러나 몇몇 사이트에서는 존재하지 않는 도메인으로부터 위조된 전자 메일 주소로 UBE(Unsolicited Bulk Email)를 받는 경우 그러한 검사를 수행할 수 있습니다.

COM 및 ORG 최상위 도메인에서 DNS 와일드카드 항목이 소개되어 mailfromdnsverify가 별로 유용하지 않게 되었기 때문에 mailfromdnsverify 코드가 수정되었습니다.

DNS가 하나 이상의 A 레코드를 반환하면 이러한 값은 새 MTA 옵션

BLOCKED\_MAIL\_FROM\_IPS에 지정된 도메인 리터럴과 비교됩니다. 일치하는 값이 발견되면 도메인은 유효하지 않은 것으로 간주됩니다. 올바른 동작을 복원하기 위한 현재의 올바른 설정은 다음과 같습니다.

```
BLOCKED_MAIL_FROM_IPS=[64.94.110.11]
```

이 옵션의 기본값은 빈 문자열입니다.

## 문자 세트 레이블링 및 8비트 데이터

키워드: charset7, charset8, charsetesc, sevenbit, eightbit, eightnegotiate, eightstrict

### *문자 세트 레이블링*

MIME 사양은 일반 텍스트 메일에 사용되는 문자 세트를 레이블링하는 기법을 제공합니다. 특히 charset= 매개 변수를 Content-type:의 헤더 행으로 지정할 수 있습니다.

US-ASCII(기본값), ISO-8859-1, ISO-8859-2 등을 포함하여 다양한 문자 세트 이름이 MIME에 정의되어 있습니다.

일부 기존 시스템과 사용자 에이전트는 이러한 문자 세트 레이블 생성을 위한 기법을 제공하지 않기 때문에 일반 텍스트 메일이 제대로 레이블링되지 않을 수 있습니다. charset7, charset8 및 charsetesc 채널 키워드는 문자 세트 레이블링이 부족한 메일 헤더에 삽입할 문자 세트 이름을 지정할 수 있도록 채널 단위 기법을 제공합니다. 각 키워드에는 문자 세트 이름을 지정하는 단일 인수가 필요합니다. 이름의 유효성은 검사하지 않습니다. MTA 테이블 디렉토리에 있는 charsets.txt 문자 세트 정의 파일에 지정된 문자 세트에 대해서만 문자 세트 변환을 수행할 수 있습니다. 가능하면 이 파일에 정의된 이름을 사용해야 합니다.

charset7 문자 세트 이름은 메일에 7비트 문자만 포함되어 있는 경우에 사용되고, charset8 문자 세트 이름은 메일에 8비트 데이터가 있는 경우에 사용되고, charsetesc는 7비트 데이터만 포함하는 메일에 이스케이프 문자가 함께 되어 있는 경우에 사용됩니다. 해당 키워드를 지정하지 않으면 Content-type: 헤더 행으로 어떤 문자 세트도 지정되지 않습니다.

또한, `charset8` 키워드는 8비트 문자는 무조건적으로 부적합한 메일 헤더에서 8비트 문자의 MIME 인코딩을 제어합니다. MTA는 일반적으로 `charset8` 값이 지정되어 있지 않은 경우 메일 헤더에 있는(잘못된) 8비트 데이터를 UNKNOWN charset으로 레이블링하여 MIME 인코딩합니다.

이러한 문자 세트 사양은 기존 레이블을 대체하지 않습니다. 즉, 메일에 문자 세트 레이블이 이미 있거나 메일 유형이 텍스트가 아닌 경우에는 적용되지 않습니다. 이 문자 세트 사양은 MTA 로컬 채널을 다음과 같이 레이블링하는 데 적합합니다.

```
1 ... charset7 US-ASCII charset8 ISO-8859-1 ...
hostname
```

메일에 Content-type 헤더가 없는 경우에 추가됩니다. 또한, 이 키워드는 MIME-version: 헤더 행을 추가합니다(없는 경우).

`charsetesc` 키워드는 이스케이프 문자를 포함하는 일본어 또는 한국어 문자 세트를 사용하는 레이블링되지 않은 메일을 받는 채널에서 특히 유용합니다.

### **8비트 데이터**

일부 전송에서는 127(십진수)보다 더 큰 서수 값을 갖는 문자의 사용을 제한합니다. 일부 SMTP 서버는 높은 비트를 제거하기 때문에 이 8비트 범위에 속하는 문자를 사용하는 메일을 제대로 해석하지 못합니다.

Messaging Server는 문제가 있는 8비트 문자가 메일에 직접 표시되지 않도록 해당 메일을 자동으로 인코딩하는 기능을 제공합니다. 이 인코딩은 `sevenbit` 키워드를 지정하여 지정된 채널의 대기열에 포함된 모든 메일에 적용할 수 있습니다. 이러한 제한이 없는 경우 채널에 `eightbit` 표시를 해야 합니다.

"원격 SMTP 서버가 8비트를 허용하는 SMTP 확장을 지원한다고 명시하지 않은 경우" SMTP 프로토콜에서 8비트를 사용할 수 없습니다. 확장 SMTP와 같은 일부 전송에서는 8비트 문자를 전송할 수 있는지 확인할 수 있도록 협상을 지원하는 경우도 있습니다. 따라서 협상에 실패할 경우 `eightnegotiate` 키워드를 사용하여 메일을 인코딩하도록 채널에 지시하는 것이 좋습니다. 이 키워드는 모든 채널의 기본값입니다. 이 경우 협상을 지원하지 않는 채널에서는 8비트 데이터를 전송할 수 없는 것으로 간주합니다.

`eightstrict` 키워드는 협상되지 않은 8비트 데이터가 포함된 받는 메일을 거부하도록 Messaging Server에 지시합니다.

## 프로토콜 스트리밍

키워드: streaming

일부 메일 프로토콜에서는 스트리밍 작업을 지원합니다. 이것은 MTA가 한 번에 여러 작업에 대한 명령을 실행하고 각 작업에 대한 응답이 일괄적으로 도착할 때까지 기다릴 수 있음을 의미합니다. streaming 키워드는 채널과 연결된 프로토콜에서 사용되는 프로토콜 스트리밍의 범위를 제어합니다. 이 키워드에는 정수 매개 변수가 필요합니다. 매개 변수를 해석하는 방법은 사용 중인 프로토콜에 따라 다릅니다.

정상적인 환경에서는 SMTP 파이프라인 확장을 사용하여 사용 가능한 스트리밍 범위를 협상합니다. 따라서, 정상적인 환경에서는 이 키워드를 절대 사용하지 마십시오.

사용 가능한 스트리밍 값의 범위는 0부터 3까지입니다. 값 0은 스트리밍을 지정하지 않고, 값 1은 RCPT TO 명령 그룹을 스트리밍하고, 값 2는 MAIL FROM/RCPT TO를 스트리밍하고, 값 3은 HELO/MAIL FROM/RCPT TO 또는 RSET/MAIL FROM/RCPT TO 스트리밍을 사용합니다. 기본값은 0입니다.

## TCP/IP 연결 및 DNS 조회 지원

서버에서 TCP/IP 연결 및 주소 조회를 처리하는 방법에 대한 정보를 지정할 수 있습니다. 이 절은 다음 내용으로 구성되어 있습니다.

- 345페이지의 "TCP/IP 포트 번호 및 인터페이스 주소"
- 346페이지의 "채널 연결 정보 캐싱"
- 346페이지의 "역방향 DNS 조회"
- 347페이지의 "IDENT 조회"
- 348페이지의 "TCP/IP MX 레코드 지원"
- 349페이지의 "이름 서버 조회"
- 349페이지의 "마지막 호스트"
- 350페이지의 "받는 메일을 위한 대체 채널(전환 채널)"
- 350페이지의 "대상 호스트 선택"

표 12-5에는 이 절에서 설명하는 TCP/IP 연결 및 DNS 조회 키워드가 나열되어 있습니다.

**표 12-5** TCP/IP 연결 및 DNS 조회 키워드

| 채널 키워드                     | 설명                                                                                                               |
|----------------------------|------------------------------------------------------------------------------------------------------------------|
| <b>포트 선택 및 인터페이스 주소</b>    | <b>SMTP 연결에 대한 기본 포트 번호 및 인터페이스 주소를 지정합니다.</b>                                                                   |
| port                       | SMTP 연결에 대한 기본 포트 번호를 지정합니다. 표준 포트는 25입니다.                                                                       |
| interfaceaddress           | 지정된 TCP/IP 인터페이스 주소에 바인딩합니다.                                                                                     |
| <b>캐시 키워드</b>              | <b>연결 정보를 캐시하는 방법을 지정합니다.</b>                                                                                    |
| cacheeverything            | 모든 연결 정보를 캐시합니다.                                                                                                 |
| cachefailures              | 연결 실패 정보만 캐시합니다.                                                                                                 |
| cachesuccesses             | 연결 성공 정보만 캐시합니다.                                                                                                 |
| nocache                    | 연결 정보를 캐시하지 않습니다.                                                                                                |
| <b>역방향 DNS 조회</b>          | <b>받는 SMTP 연결에서 역방향 DNS 조회를 처리하는 방법을 지정합니다.</b>                                                                  |
| forwardcheckdelete         | 역방향 DNS 조회를 수행한 경우 반환된 이름에 대한 정방향 조회를 수행하여 반환된 IP 번호가 원본과 일치하는지 확인합니다. 원본과 일치하지 않는 경우 이름을 삭제하고 IP 주소를 사용합니다.     |
| forwardchecknone           | DNS 역방향 조회 후 정방향 조회를 수행하지 않습니다.                                                                                  |
| forwardchecktag            | 역방향 DNS 조회를 수행한 경우 반환된 이름에 대한 정방향 조회를 수행하여 반환된 IP 번호가 원본과 일치하는지 확인합니다. 원본과 일치하지 않는 경우 이름에 * 태그를 붙입니다.            |
| <b>IDENT 조회/DNS 역방향 조회</b> | <b>받는 SMTP 연결에서 IDENT 조회 및 DNS 역방향 조회를 처리하는 방법을 지정합니다.</b>                                                       |
| identnone                  | IDENT 조회를 수행하지 않고 IP를 호스트 이름으로 변환하고 호스트 이름과 IP 주소를 모두 Received: 헤더에 포함합니다.                                       |
| identnonelimited           | IDENT 조회를 수행하지 않고 IP를 호스트 이름으로 변환하지만 채널 전환 중에 호스트 이름을 사용하지 않고 호스트 이름과 IP 주소를 모두 Received: 헤더에 포함합니다.             |
| identnonenumeric           | IDENT 조회를 수행하지 않거나 IP를 호스트 이름으로 변환하지 않습니다.                                                                       |
| identnonesymbolic          | IDENT 조회를 수행하지 않고 IP를 호스트 이름으로 변환하고 호스트 이름만 Received: 헤더에 포함합니다.                                                 |
| identtcp                   | 받는 SMTP 연결에서 IDENT 조회를 수행하고 IP를 호스트 이름으로 변환하고 호스트 이름과 IP 주소를 모두 Received: 헤더에 포함합니다.                             |
| identtcplimited            | 받는 SMTP 연결에 IDENT 조회를 수행하고 IP를 호스트 이름으로 변환하지만 채널 전환 중에 호스트 이름을 사용하지 않습니다. 호스트 이름과 IP 주소를 모두 Received: 헤더에 포함합니다. |
| identtcpnumeric            | 받는 SMTP 연결에서 IDENT 조회를 수행하지만 IP를 호스트 이름으로 변환하지 않습니다.                                                             |



표 12-5 TCP/IP 연결 및 DNS 조회 키워드

| 채널 키워드                          | 설명                                                                                                     |
|---------------------------------|--------------------------------------------------------------------------------------------------------|
| identtcpsymbolic                | 받는 SMTP 연결에서 IDENT 조회를 수행하고 IP를 호스트 이름으로 변환하고 호스트 이름만 Received:헤더에 포함합니다.                              |
| <b>MX 레코드 지원 및 TCP/IP 이름 서버</b> | <b>채널에서 MX 레코드 조회를 지원하는지 여부와 지원 방법을 지정합니다.</b>                                                         |
| mx                              | TCP/IP 네트워크 및 소프트웨어가 MX 레코드 조회를 지원합니다.                                                                 |
| nomx                            | TCP/IP 네트워크가 MX 조회를 지원하지 않습니다.                                                                         |
| defaultmx                       | 채널이 네트워크에서 MX 조회를 수행할지 여부를 결정합니다.                                                                      |
| randommx                        | MX 조회를 수행하고 반환된 항목을 같은 우선 순위로 임의화합니다.                                                                  |
| nonrandommx                     | MX 조회를 수행하고 반환된 항목을 같은 우선 순위로 임의화하지 않습니다.                                                              |
| nameservers                     | TCP/IP 스택의 자체 이름 서버 선택을 참조하는 대신 참조할 이름 서버 목록을 지정합니다. nameservers에는 이름 서버에 대한 공백으로 구분된 IP 주소 목록이 필요합니다. |
| defaultnameservers              | TCP/IP 스택의 이름 서버 선택을 참조합니다.                                                                            |
| lastresort                      | 마지막 호스트를 지정합니다.                                                                                        |
| <b>전환 키워드</b>                   | <b>받는 메일에 대한 대체 채널 선택을 제어합니다.</b>                                                                      |
| allowswitchchannel              | switchchannel 채널에서 이 채널로 전환을 허용합니다.                                                                    |
| noswitchchannel                 | 서버 채널을 유지합니다. 원본 호스트와 연결된 채널을 전환하지 않고, 채널 전환을 허용하지 않습니다.                                               |
| switchchannel                   | 서버 채널에서 원본 호스트와 연결된 채널로 전환합니다.                                                                         |
| tlsswitchchannel                | TLS 협상이 성공하면 다른 채널로 전환합니다.                                                                             |
| saslswitchchannel               | SASL 인증이 성공할 경우 다른 채널로 전환합니다.                                                                          |
| <b>대상 호스트 선택 및 메일 복사본 저장소</b>   | <b>대상 호스트 시스템과 메일 복사본의 저장 방법을 지정합니다.</b>                                                               |
| daemon                          | 봉투 주소에 관계 없이 특정 호스트 시스템에 연결합니다.                                                                        |
| single                          | 채널의 각 대상 주소에 대해 별도의 메일 복사본을 만들도록 지정합니다.                                                                |
| single_sys                      | 사용된 각 대상 시스템에 대해 단일 메일 복사본을 만듭니다.                                                                      |

## TCP/IP 포트 번호 및 인터페이스 주소

키워드: port, interfaceaddress

SMTP over TCP/IP 채널은 메일을 보낼 때 일반적으로 포트 25에 연결합니다. port 키워드를 사용하여 비표준 포트에 연결하도록 SMTP over TCP/IP 채널에 지시할 수 있습니다. 이 키워드는 SMTP 연결을 위해 MTA가 수신하는 포트를 제어하는 PORT 디스패처 옵션을 보완합니다.

interfaceaddress 키워드는 TCP/IP 채널이 아웃바운드 연결에 대한 소스 주소로 바인딩하는 주소를 제어합니다. 즉, 여러 인터페이스 주소를 갖는 시스템에서 이 키워드는 MTA가 SMTP 메일을 보낼 때 소스 IP 주소로 사용하는 주소를 제어합니다. 이 키워드는 받는 연결 및 메일을 받기 위해 TCP/IP 채널이 수신하는 인터페이스 주소를 제어하는 INTERFACE\_ADDRESS 디스패처 옵션을 보완합니다.

## 채널 연결 정보 캐싱

키워드: cacheeverything, nocache, cachefailures, cachesuccesses

SMTP 프로토콜을 사용하는 채널은 이전 연결 시도 내역이 들어 있는 캐시를 유지 관리합니다. 이 캐시를 사용하면 액세스할 수 없는 호스트에 여러 번 다시 연결할 필요가 없으므로 시간이 낭비되거나 다른 메일이 지연되지 않습니다. 캐시는 프로세스 단위 캐시이며 아웃바운드 SMTP 전달 채널을 한 번 실행하는 동안에만 지속됩니다.

캐시는 일반적으로 연결 성공과 연결 실패를 모두 기록합니다. 성공한 연결 시도는 후속 실패를 오프셋하기 위해 기록됩니다. 그러나, 이전에는 성공했으나 지금은 실패한 호스트에서는 연결을 시도한 적이 없거나 이전에 실패했던 호스트에서처럼 다른 연결을 시도하기 이전에 지연 기간이 보장되지 않습니다.

MTA에 사용되는 캐싱 전략이 모든 상황에 적합한 것은 아닙니다. 따라서 MTA 캐시 조정을 위해 채널 키워드가 제공됩니다.

cacheeverything 키워드는 모든 형식의 캐싱을 사용하며 기본값입니다. nocache 키워드는 모든 캐싱을 사용하지 않습니다.

cachefailures 키워드는 연결 실패 캐싱만 사용하며 cacheeverything 키워드의 경우보다 재시도가 제한됩니다. 마지막으로 cachesuccesses는 연결 성공만 캐시합니다. 이 마지막 키워드는 SMTP 채널의 nocache 키워드와 효과가 동일합니다.

## 역방향 DNS 조회

키워드: forwardchecknone, forwardchecktag, forwardcheckdelete

`forwardchecknone`, `forwardchecktag` 및 `forwardcheckdelete` 채널 키워드는 역방향 DNS 조회 수행 효과를 수정할 수 있습니다. 이러한 키워드는 MTA가 DNS 역방향 조회를 사용하여 찾은 IP 이름에 대해 정방향 조회를 수행하는지 여부를 제어할 수 있으며, 그러한 정방향 조회를 요청받을 경우 IP 이름 정방향 조회가 연결의 원본 IP 번호와 일치하지 않을 때 MTA에서 수행할 작업을 지정합니다.

`forwardchecknone` 키워드는 기본값이며 정방향 조회가 수행되지 않음을 의미합니다. `forwardchecktag` 키워드는 각 역방향 조회 이후에 정방향 조회를 수행하고, 정방향 조회를 사용하여 찾은 IP 번호가 원본 연결의 IP 번호와 일치하지 않을 경우 해당 IP 이름에 별표(\*) 태그를 붙이도록 MTA에 지시합니다. `forwardcheckdelete` 키워드는 각 역방향 조회 이후에 정방향 조회를 수행하고 해당 이름에 대한 정방향 조회가 원본 연결 IP 주소와 일치하지 않는 경우 역방향 조회에서 반환된 이름을 무시(삭제)하도록 MTA에 지시합니다. 이 경우 MTA는 원본 IP 주소를 대신 사용합니다.

---

**주** 정방향 조회가 원본 IP 주소와 일치하지 않는 것이 정상인 사이트가 있습니다. 이러한 사이트에서는 여러 IP 주소에 보다 "일반적인" IP 이름을 사용합니다.

---

## IDENT 조회

키워드: `identnone`, `identnonelimited`, `identttnonnumeric`, `identnonesymbolic`, `identtcp`, `identtcpnumeric`, `identtcpsymbolic`, `identtcplimited`

IDENT 키워드는 MTA에서 IDENT 프로토콜을 사용하여 연결 및 조회를 처리하는 방법을 제어합니다. IDENT 프로토콜은 RFC 1413에 설명되어 있습니다.

`identtcp`, `identtcpsymbolic` 및 `identtcpnumeric` 키워드는 IDENT 프로토콜을 사용하여 연결 및 조회를 수행하도록 MTA에 지시합니다. IDENT 프로토콜에서 가져온 정보(일반적으로 SMTP에 연결한 아이디)는 메일의 Received: 헤더에 다음과 같이 삽입됩니다.

- `identtcp`는 받는 IP 번호에 해당하는 호스트 이름(DNS 역방향 조회에서 보고됨)과 IP 번호 자체를 삽입합니다.
- `identtcpsymbolic`은 받는 IP 번호에 해당하는 호스트 이름(DNS 역방향 조회에서 보고됨)을 삽입합니다. IP 번호 자체는 Received: 헤더에 포함되지 않습니다.
- `identtcpnumeric`은 실제 받는 IP 번호를 삽입합니다. IP 번호에 대한 DNS 역방향 조회는 수행되지 않습니다.

---

**주** identtcp, identtcpsymbolic 또는 identtcpnumeric에 의한 IDENT 조희가 유효하려면 원격 시스템에서 IDENT 서버를 실행해야 합니다.

---

IDENT 쿼리를 시도하면 성능이 감소될 수 있음에 유의하십시오. 점차적으로 라우터는 자신이 구성하지 않은 포트에 대해 시도된 연결에 "블랙홀"을 생성합니다. IDENT 쿼리에서 이러한 현상이 발생할 경우 MTA는 연결 시간 초과(TCP/IP 스택 제어 시간 초과, 일반적으로 1분 또는 2분)가 발생할 때까지는 다시 수신하지 않습니다.

identtcp, identtcpplimited 또는 identtcpsymbolic을 identtcpnumeric과 비교하는 경우 또 다른 성능 요소가 있습니다. identtcp, identtcpplimited 또는 identtcpsymbolic으로 호출되는 DNS 역방향 조희는 사용자에게 보다 친숙한 호스트 이름을 가져오기 위해 추가 오버헤드를 발생시킵니다.

identnone 키워드는 IDENT 조희를 사용하지 않지만 IP를 호스트 이름으로 변환하도록 지정하고 IP 번호와 호스트 이름 모두 메일의 Received: 헤더에 포함합니다.

identnonenumeric 키워드는 IDENT 조희를 사용하지 않지만 IP를 호스트 이름으로 변환하며 호스트 이름만 메일의 Received: 헤더에 포함합니다.

identnonenumeric 키워드는 이 IDENT 조희를 사용하지 않고 일반 DNS 역방향 조희에서 IP 번호를 호스트 이름으로 변환하지 못하게 합니다. 또한, Received: 헤더에 포함합니다. 기본값입니다.

identtcpplimited 및 identnonelimited 키워드는 IDENT 조희, 역방향 DNS 조희 및 Received: 헤더에 표시되는 정보에 있어서 각각 identtcp 및 identnone와 동일한 효과를 가집니다. identtcpplimited 또는 identnonelimited에서는 DNS 역방향 조희의 호스트 이름 확인 성공 여부에 관계 없이 switchchannel 키워드의 사용에 따른 채널 전환의 기초로 항상 IP 문자 주소를 사용한다는 점만 다릅니다.

## TCP/IP MX 레코드 지원

키워드: mx, nomx, defaultmx, randommx, nonrandommx

TCP/IP 네트워크에서 MX(메일 전달) 레코드 사용을 지원하는 경우도 있고 지원하지 않는 경우도 있습니다. 일부 TCP/IP 채널 프로그램에서는 MTA 시스템이 연결된 네트워크에서 MX 레코드를 제공하지 않는 경우 MX 레코드를 사용하지 않도록 구성할 수 있습니다. mx, nomx, defaultmx, randommx, nonrandommx 키워드는 MX 레코드 지원을 제어합니다.

randommx 키워드는 MX 조회를 수행하고 우선 순위가 동일한 MX 레코드 값을 임의의 순서로 처리하도록 지정합니다. nonrandommx 키워드는 MX 조회를 수행하고 우선 순위가 동일한 MX 레코드 값을 받은 순서대로 처리하도록 지정합니다.

mx 키워드는 nonrandommx 키워드에 해당하며 이후의 릴리스에서는 randommx에 해당하는 키워드로 변경될 수 있습니다. nomx 키워드는 MX 조회를 사용하지 않습니다. defaultmx 키워드는 네트워크에서 MX 레코드를 지원할 경우 mx를 사용하도록 지정합니다. defaultmx 키워드는 MX 조회를 지원하는 채널의 기본값입니다.

## 이름 서버 조회

키워드: nameservers, defaultnameservers

이름 서버 조회를 수행할 경우 TCP/IP 스택의 자체 이름 서버 선택을 참조하는 대신 nameservers 채널 키워드를 사용하여 이름 서버 목록을 지정할 수 있습니다.

nameservers 키워드에는 다음 예에 표시된 것처럼 이름 서버에 대한 공백으로 구분된 IP 주소 목록이 필요합니다.

```
nameservers 1.2.3.1 1.2.3.2
```

기본값인 defaultnameservers는 TCP/IP 스택의 자체 이름 서버 선택을 사용함을 의미합니다.

UNIX에서 이름 서버 조회를 수행하지 않게 하려면 nsswitch.conf 파일을 수정하면 됩니다. NT에서는 TCP/IP 구성을 수정하십시오.

## 마지막 호스트

키워드: lastresort

lastresort 키워드는 다른 모든 연결 시도가 실패할 경우에 연결할 호스트를 지정하는 데 사용됩니다. 실제로 이 키워드는 마지막 MX 레코드 역할을 합니다. 또한 SMTP 채널에서만 유효합니다.

이 키워드에는 "마지막 시스템"의 이름을 지정하는 단일 매개 변수가 필요합니다. 예를 들면 다음과 같습니다.

```
tcp_local single_sys smtp mx lastresort mailhub.siroe.com
TCP-DAEMON
```

## 받는 메일을 위한 대체 채널(전환 채널)

키워드: `switchchannel`, `allowswitchchannel`, `noswitchchannel`.

351페이지의 `saslswitchchannel` 및 354페이지의 `tlsswitchchannel`을 참조하십시오.

`switchchannel`, `allowswitchchannel` 및 `noswitchchannel` 키워드는 받는 메일을 위한 대체 채널 선택을 제어합니다.

MTA는 원격 시스템으로부터 받는 연결을 수락할 때 연결에 사용할 채널을 선택해야 합니다. 일반적으로 이 결정은 사용된 전송을 기반으로 합니다. 예를 들어, 받는 SMTP over TCP/IP 연결은 `tcp_local` 채널에 자동으로 연결됩니다.

서로 다른 특성을 갖는 여러 보내는 채널을 사용하여 동일한 전송을 통해 서로 다른 여러 시스템을 처리할 경우에는 이 규칙이 적용되지 않습니다. 이러한 경우 받는 연결은 보내는 연결과 동일한 채널에 연결되지 않기 때문에 해당 채널 특성이 원격 시스템과 연결되지 않습니다.

`switchchannel` 키워드를 사용하면 이 문제를 해결할 수 있습니다. 서버가 사용하는 초기 채널에서 `switchchannel`을 지정하면 연결(원본) 호스트의 IP 주소가 채널 테이블에 일치되고 그에 따라 원본 채널이 적절하게 변경됩니다. IP 주소가 일치하지 않거나 원래의 기본 받는 채널에 대한 일치가 발견되는 경우 MTA는 DNS 역방향 조회를 통해 찾은 호스트 이름을 사용하여 선택적으로 일치를 시도할 수 있습니다. 소스 채널이 `switchchannel` 또는 `allowswitchchannel`(기본값) 표시가 있는 채널로 변경될 수 있습니다. `noswitchchannel` 키워드는 채널 전환이 수행되지 않음을 지정합니다.

서버가 연결하는 채널이 아닌 다른 채널에 지정한 `switchchannel` 키워드는 기본적으로 적용되지 않습니다. 현재는 `switchchannel` 키워드가 SMTP 채널에만 적용되며 `switchchannel`을 적용할 수 있는 다른 채널이 없습니다.

## 대상 호스트 선택

키워드: `daemon`, `single`, `single_sys`

`daemon` 키워드의 해석과 사용은 적용되는 채널의 유형에 따라 다릅니다.

`daemon` 키워드는 SMTP 채널에서 대상 호스트 선택을 제어하는 데 사용됩니다.

일반적으로 채널은 처리할 메일의 봉투 주소에 나열되는 모든 호스트에 연결됩니다. daemon 키워드는 봉투 주소에 관계 없이 특정 원격 시스템(일반적으로 방화벽 또는 메일 허브 시스템)에 대신 연결하도록 채널에 지시하는 데 사용됩니다. 실제 원격 시스템 이름은 다음 예에 표시된 것처럼 daemon 키워드 바로 뒤에 표시되어야 합니다.

```
tcp_firewall smtp mx daemon firewall.acme.com
TCP-DAEMON
```

daemon 키워드 뒤의 인수가 정규화된 도메인 이름이 아닌 경우 해당 인수가 무시되고 채널이 해당 채널의 공식 호스트에 연결됩니다. 공식 호스트는 채널과 연관된 정규화된 호스트 이름이며 세 개 행 채널 블록의 두 번째 행에서 지정할 수 있습니다.

```
tcp_firewall smtp mx daemon router
firewall.acme.com
TCP-DAEMON
```

또한 공식 호스트를 두 개 행 채널 블록에서 TCP-DAEMON 뒤에 지정하여 아웃바운드 연결이 자체를 특정 호스트로 식별하게 할 수 있습니다.

```
tcp_firewall smtp mx daemon router
TCP-DAEMON firewall.acme.com
```

방화벽 또는 게이트웨이 시스템 이름을 공식 호스트 이름으로 지정할 경우 다음 예에 표시된 것처럼 daemon 키워드에 지정된 인수가 일반적으로 라우터로 지정됩니다.

```
tcp_firewall smtp mx daemon router
firewall.acme.com
TCP-DAEMON
```

기타 관련 키워드로는 single 및 single\_sys가 있습니다. single 키워드는 채널의 각 대상 주소에 대해 별도의 메일 복사본을 만들도록 지정합니다. single\_sys 키워드는 사용된 각 대상 시스템에 대해 단일 메일 복사본을 만듭니다. 사용된 키워드에 관계 없이 메일이 대기열에 있는 각 채널에 대해 해당 메일 복사본을 하나 이상 만듭니다.

## SMTP 인증, SASL 및 TLS

키워드: maysaslserver, mustsaslseserver, nosasl, nosaslserver, saslswitchchannel, nosaslswitchchannel

Messaging Server가 SASL(Simple Authentication and Security Layer)을 사용한 SMTP 서버 인증을 지원하는지 여부를 제어할 수 있습니다. SASL은 RFC 2222에 정의되어 있습니다. SASL, SMTP 인증 및 보안에 대한 자세한 내용은 19장, "보안 및 액세스 제어 구성"을 참조하십시오.

maysaslserver, mustsaslserver, nosasl, nosaslserver, switchchannel 및 saslswitchchannel 채널 키워드는 TCP/IP 채널과 같은 SMTP 채널이 SMTP 프로토콜에서 SASL(SMTP AUTH)을 사용하도록 구성하는 데 사용됩니다.

nosasl이 기본값이며 SASL 인증이 허용 또는 시도되지 않음을 의미합니다. 또한, SASL 인증이 허용되지 않음을 의미하는 nosaslserver를 포함합니다. maysaslserver를 지정하면 SMTP 서버에서 클라이언트가 SASL 인증 사용을 시도하도록 허용합니다.

mustsaslserver를 지정하면 SMTP 서버에서 클라이언트가 SASL 인증을 사용하려고 시도하지만 SMTP 서버는 원격 클라이언트가 성공적으로 인증되지 않는 경우 메일을 수락하지 않습니다.

saslswitchchannel을 사용하면 클라이언트가 SASL을 성공적으로 사용할 경우에 받는 연결이 지정한 채널로 전환되게 합니다. 전환할 채널을 지정하는 필수 값을 사용합니다.

## 헤더의 SMTP AUTH에서 인증된 주소 사용

키워드: authrewrite

authrewrite 채널 키워드 및 관련 AUTH\_REWRITE 매핑 테이블을 사용하면 인증 작업에서 얻은 주소 지정 정보를 사용하여 헤더 및 봉투 주소를 수정할 수 있습니다. 특히 인증된 전자 메일 주소를 제공하도록 SASL 인증을 구성할 수 있습니다. 일반적으로 SMTP AUTH 정보가 사용되지만 이 정보는 FROM\_ACCESS 매핑을 통해 대체될 수 있습니다.

authrewrite 키워드는 표 12-6에 따라 필수 비트 값을 가집니다.

**표 12-6** authrewrite 비트 값

| 비트 | 값 | 설명                                                                                                   |
|----|---|------------------------------------------------------------------------------------------------------|
| 0  | 1 | 아무것도 변경하지 않습니다(기본값).                                                                                 |
| 1  | 2 | 인증 작업에서 제공된 주소를 포함하는 Sender: 또는 Resent-sender: 헤더 필드를 추가합니다. 다른 resent- 필드가 있는 경우 Resent- 변형이 사용됩니다. |
| 2  | 4 | 인증 작업에서 제공된 주소를 포함하는 Sender: 헤더 필드를 추가합니다.                                                           |



표 12-6 authrewrite 비트 값

| 비트 | 값  | 설명                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|----|----|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 3  | 8  | <p>다음과 같은 형태의 AUTH_REWRITE라는 매핑 테이블에서 검사를 생성합니다.</p> <p><i>mail-from   sender   from   auth-sender</i></p> <p>여기서 <i>mail-from</i>은 봉투의 <i>From:</i> 주소이고 <i>sender</i>는 <i>Sender:</i> 또는 <i>Resent-sender:</i> 헤더 필드의 주소이며 <i>from</i>은 <i>From:</i> 또는 <i>Resent-From:</i> 헤더 필드의 주소이고 <i>auth-sender</i>는 인증 작업에서 제공된 주소입니다.</p> <p>결과는 AUTH_REWRITE 매핑을 통해 실행됩니다. 매핑은 세로 막대(   )로 구분된 항목 목록을 반환합니다. 이러한 항목은 다음 플래그를 설정하여 순서대로 사용됩니다.</p> <p>\$J \$K 메일의 봉투 <i>From:</i> 주소를 바꿉니다.</p> <p>\$Y \$T 적절한 <i>Sender:</i> 또는 <i>Resent-sender:</i> 헤더 필드를 추가합니다.</p> <p>\$N 메일을 거부합니다. 결과를 매핑하면 오류 메시지의 텍스트가 제공됩니다. 텍스트가 제공되지 않으면 <i>invalid originator address used</i>라는 오류 메시지가 표시됩니다.</p> <p>\$Z 적절한 <i>From:</i> 또는 <i>Resent-from:</i> 헤더 필드를 추가합니다. (일반적으로 <i>From:</i> 필드를 대체하는 것은 아주 나쁜 방법입니다.)</p> <p>헤더에 다른 <i>Resent-</i> 필드가 있는 경우 <i>Resent-</i> 변형이 사용됩니다.</p> |
| 4  | 16 | <p>인증에서 인증된 주소를 제공하지 않은 경우라도 AUTH_REWRITE 매핑을 적용합니다. 비트가 지워지면 인증된 주소를 사용할 수 있을 경우 매핑만 적용됩니다.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| 5  | 32 | <p>AUTH_REWRITE 매핑 검사의 시작 부분에 소스 채널을 포함합니다. 이 부분과 남은 정보는  로 구분됩니다. 비트가 지워지면 채널이 포함되지 않습니다.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

---

**경고** \$Z 플래그는 봉투와 헤더 주소를 수정하기 위해 합법적으로 사용하는 경우는 적으므로 높은 수준으로 제한되어야 합니다.

---

## Microsoft Exchange 게이트웨이 채널 지정

키워드: msexchange, nomsexchange

TCP/IP 채널에서 `msexchange` 채널 키워드를 사용하여 이 채널이 Microsoft Exchange 게이트웨이 및 클라이언트와 통신하는 채널임을 MTA에 알려줄 수 있습니다. 이 채널 키워드를 `maysaslserver` 또는 `mustsaslsrver` 키워드를 통해 SASL을 사용하는 받는 TCP/IP 채널에 넣을 경우 MTA의 SMTP 서버가 "잘못된" 형식(새로 수정된 AUTH 사양 대신 올바른 ESMTP 사용과 호환되지 않는 원본의 ESMTP AUTH 사양을 기반으로 함)을 사용하여 AUTH를 광고하게 합니다. 예를 들어, 일부 Microsoft Exchange 클라이언트는 올바른 AUTH 형식을 인식하지 않고 잘못된 AUTH 형식만 인식합니다.

또한, `msexchange` 채널 키워드는 끊어진 TLS 명령을 광고 및 인식하게 합니다.

기본값은 `nomsexchange`입니다.

## 전송 계층 보안

키워드: `maytls`, `maytlsclient`, `maytlsserver`, `musttls`, `musttlsclient`, `musttlsserver`, `notls`, `notlsclient`, `notlsserver`, `tlsswitchchannel`

`maytls`, `maytlsclient`, `maytlsserver`, `musttls`, `musttlsclient`, `musttlsserver`, `notls`, `notlsclient`, `notlsserver` 및 `tlsswitchchannel` 채널 키워드는 TCP/IP 채널과 같은 SMTP 기반 채널에 의한 SMTP 프로토콜에서 TLS 사용을 구성하는 데 사용됩니다.

기본값은 `notls`이고 TLS가 허용 또는 시도되지 않음을 의미합니다. 보내는 연결에서 MTA SMTP 클라이언트가 TLS 사용을 시도하지 않음(보내는 연결 중에 `STARTTLS` 명령 실행 안 됨)을 의미하는 `notlsclient` 키워드와 받는 연결에서 MTA SMTP 서버의 TLS 사용이 허용되지 않음(SMTP 서버에서 `STARTTLS` 확장을 광고하지 않고 명령 자체도 허용 안 됨)을 의미하는 `notlsserver` 키워드를 포함합니다.

`maytls`를 지정하면 MTA가 받는 연결에 TLS를 제공하고 보내는 연결에서 TLS를 시도합니다. TLS를 지원하는 SMTP 서버에 메일을 보낼 때 MTA SMTP 클라이언트가 TLS 사용을 시도함을 의미하는 `maytlsclient` 키워드와 MTA SMTP 서버가 `STARTTLS` 확장 지원을 광고하고 메일을 받을 때 TLS 사용을 허용함을 의미하는 `maytlsserver` 키워드를 포함합니다.

TLS로 작업할 경우 다음 조건을 충족시켜야 합니다.

- `mailsrv` 계정에서 파일에 액세스할 수 있도록 인증서의 보호/소유권을 설정해야 합니다.

- mailsrv 계정에서 인증서가 저장되는 디렉토리 내의 파일에 액세스할 수 있도록 해당 디렉토리에서 보호/소유권을 설정해야 합니다.

musttls를 지정하면 MTA가 보내는 연결과 받는 연결 모두에서 TLS 사용을 주장하게 되므로 TLS 사용 협상에 실패할 경우 원격 시스템과 전자 메일을 교환할 수 없습니다. MTA SMTP 클라이언트가 메일을 보낼 때 TLS 사용을 주장하고 TLS 사용 협상(MTA가 STARTTLS 명령을 실행하고 해당 명령이 성공해야 함)에 실패한 SMTP 서버에 메일을 보내지 않음을 의미하는 musttlsclient를 포함합니다. 또한, MTA SMTP 서버가 STARTTLS 확장 지원을 광고하고 메일을 받을 때 TLS 사용을 강제하고 TLS 사용 협상에 실패한 클라이언트에서 보낸 메일을 받지 않음을 의미하는 musttlsxserver를 포함합니다.

tlsswitchchannel 키워드를 사용하면 클라이언트가 SASL 협상에 성공할 경우 받는 연결이 지정한 채널로 전환됩니다. 전환할 채널을 지정하는 필수 값을 사용합니다.

## 메일 처리 및 전달 구성

서버가 특정 기준에 따라 메일 전달을 시도하도록 구성할 수 있습니다. 또한, 서비스 작업 처리 제한, 새 SMTP 채널 스레드 생성 시기 등과 같은 작업 처리 매개 변수를 지정할 수 있습니다. 이 절은 다음 내용으로 구성되어 있습니다.

- [357페이지의 "채널 방향 설정"](#)
- [358페이지의 "지연 전달 날짜 구현"](#)
- [358페이지의 "전달에 실패한 메일에 대한 재시도 간격 지정"](#)
- [360페이지의 "채널 실행 작업의 처리 풀"](#)
- [360페이지의 "서비스 작업 제한"](#)
- [363페이지의 "크기 기반 메일 우선 순위"](#)
- [363페이지의 "SMTP 채널 스레드"](#)
- [364페이지의 "여러 주소 확장"](#)
- [365페이지의 "서비스 변환 사용"](#)

메일 처리 및 전달에 대한 개념 정보는 194페이지의 "Job Controller" 및 247페이지의 "Job Controller 파일"을 참조하십시오.

표 12-7은 이 절에서 설명하는 키워드를 요약해서 보여 줍니다.

**표 12-7** 메일 처리 및 전달 키워드

| 키워드                   | 정의                                                                                            |
|-----------------------|-----------------------------------------------------------------------------------------------|
| <b>즉시 전달</b>          | <b>메일 즉시 전달에 대한 사양을 정의합니다.</b>                                                                |
| immonurgent           | 높음, 중간 및 낮음 우선 순위 메일을 제출하면 바로 전달을 시작합니다.                                                      |
| <b>채널 방향</b>          | <b>채널을 사용하는 프로그램 유형을 지정합니다.</b>                                                               |
| bidirectional         | 마스터 및 슬레이브 프로그램에서 사용되는 채널입니다.                                                                 |
| master                | 마스터 프로그램에서 사용되는 채널(master)입니다.                                                                |
| slave                 | 슬레이브 프로그램에서 사용되는 채널(slave)입니다.                                                                |
| <b>지연 전달</b>          | <b>지연 작업 전달에 대한 사양을 정의합니다.</b>                                                                |
| backoff               | 지연 메일의 재전달 시도 간격을 지정합니다. normalbackoff, nonurgentbackoff, urgentbackoff에 의해 대체될 수 있습니다.       |
| deferred              | Deferred-delivery: 헤더 행을 수락하고 인식합니다.                                                          |
| nodeferred            | 기본값입니다. Deferred-delivery: 헤더 행을 수락하지 않음을 지정합니다.                                              |
| nonurgentbackoff      | 낮음 우선 순위 메일의 재전달 시도 간격입니다.                                                                    |
| normalbackoff         | 중간 우선 순위 메일의 재전달 시도 간격입니다.                                                                    |
| urgentbackoff         | 높음 우선 순위 메일의 재전달 시도 간격입니다.                                                                    |
| <b>크기 기반 메일 우선 순위</b> | <b>메일 크기를 기반으로 메일의 우선 순위를 정의합니다.</b>                                                          |
| nonurgentblocklimit   | 이 크기 이상인 메일의 우선 순위를 낮음(두 번째 우선 순위 클래스) 이하로 지정합니다. 즉, 해당 메일은 항상 다음 정기 작업이 처리되는 동안 대기한 후 처리됩니다. |
| normalblocklimit      | 이 크기 이상인 메일의 우선 순위를 낮음으로 지정합니다.                                                               |
| urgentblocklimit      | 이 크기 이상인 메일의 우선 순위를 중간으로 지정합니다.                                                               |
| <b>채널 실행 작업의 처리 풀</b> | <b>작업 우선 순위와 지연 수준이 서로 다른 메일 처리를 위한 풀을 지정합니다.</b>                                             |
| pool                  | 채널이 실행되는 풀을 지정합니다.                                                                            |
| after                 | 채널이 실행되기 이전의 시간 지연을 지정합니다.                                                                    |

**표 12-7** 메일 처리 및 전달 키워드

| 키워드                   | 정의                                                        |
|-----------------------|-----------------------------------------------------------|
| <b>서비스 작업 제한</b>      | <b>서비스 작업 수와 작업당 처리할 최대 메일 파일 수를 지정합니다.</b>               |
| maxjobs               | 채널에 대해 동시에 실행될 수 있는 최대 작업 수를 지정합니다.                       |
| filesperjob           | 단일 작업에서 처리할 대기열 항목 수를 지정합니다.                              |
| <b>SMTP 채널 스레드</b>    |                                                           |
| threaddepth           | 다중 스레드 SMTP 클라이언트를 사용하여 새 스레드를 트리거하는 메일 수입니다.             |
| <b>다중 주소 확장</b>       | <b>수신자가 여러 명인 메일의 처리를 정의합니다.</b>                          |
| expandlimit           | 주소 수가 이 제한을 초과할 경우 받는 메일을 "오프라인"으로 처리합니다.                 |
| expandchannel         | expandlimit 적용으로 인해 지연된 확장을 수행할 채널을 지정합니다.                |
| holdlimit             | 주소 수가 이 제한을 초과할 경우 받는 메일을 보관합니다.                          |
| <b>트랜잭션 제한</b>        | <b>연결 트랜잭션 제한을 지정합니다.</b>                                 |
| transactionlimit      | 연결당 허용되는 메일 수를 제한합니다.                                     |
| <b>전달할 수 없는 메일 알림</b> | <b>전달할 수 없는 메일 알림을 보내는 시기를 지정합니다.</b>                     |
| notices               | 알림을 보낸 후 메일이 반환되기 이전에 경과할 수 있는 시간을 지정합니다.                 |
| nonurgentnotices      | 우선 순위가 낮은 메일에 대해 알림을 보내고 메일을 반환하기 전에 경과할 수 있는 시간을 지정합니다.  |
| normalnotices         | 우선 순위가 중간인 메일에 대해 알림을 보내고 메일을 반환하기 전에 경과할 수 있는 시간을 지정합니다. |
| urgentnotices         | 우선 순위가 높은 메일에 대해 알림을 보내고 메일을 반환하기 전에 경과할 수 있는 시간을 지정합니다.  |

## 채널 방향 설정

키워드: master, slave, bidirectional

세 키워드를 사용하여 채널이 마스터 프로그램(master), 슬레이브 프로그램(slave) 또는 두 프로그램 모두(bidirectional)에서 사용되는지 여부를 지정합니다. 이 키워드를 지정하지 않을 경우 기본값은 bidirectional입니다. 이러한 키워드는 메일을 채널의 대기열에 넣을 때 MTA가 전달 작업을 시작하는지 여부를 지정합니다.

이러한 키워드의 사용은 해당 채널 프로그램의 기본 특성을 반영합니다. MTA가 지원하는 다양한 채널 설명은 이러한 키워드를 사용해야 하는 시기와 위치를 나타냅니다.

## 지연 전달 날짜 구현

키워드: deferred, nodeferred, immmnonurgent

deferred 채널 키워드는 Deferred-delivery: 헤더 행을 인식하고 준수합니다. deferred 전달 날짜가 미래 날짜인 메일은 해당 날짜가 만료되어 반환되거나 지연 전달 날짜가 될 때까지 채널 대기열에 보관됩니다. Deferred-delivery: 헤더 행의 형식 및 작업에 대한 자세한 내용은 RFC 1327을 참조하십시오.

기본값은 nodeferred 키워드입니다. 지연 메일 처리에 대한 지원이 RFC 1327에 규정되어 있지만 지연 메일 처리를 실제로 구현하면 메일 시스템을 디스크 할당량의 확장으로 효과적으로 사용할 수 있습니다.

키워드 immmnonurgent는 높음, 중간 및 낮음 우선 순위 메일을 제출하면 바로 전달을 시작합니다.

## 전달에 실패한 메일에 대한 재시도 간격 지정

키워드: backoff, nonurgentbackoff, normalbackoff, urgentbackoff, notices

기본적으로 전달에 실패한 메일에 대한 전달 재시도 간격은 메일의 우선 순위에 따라 다릅니다. 전달 시도 사이의 기본 간격(분)은 아래에 나와 있습니다. 우선 순위 뒤의 첫 번째 숫자는 최초 전달 실패 후 첫 번째 전달 재시도가 시도될 때까지의 시간(분)을 나타냅니다.

높음: 30, 60, 60, 120, 120, 240

보통: 60, 120, 120, 240, 240, 480

낮음: 120, 240, 240, 480, 480, 960

우선 순위가 높은 메일의 경우 최초 전달 실패 후 30분 뒤, 첫 번째 전달 재시도 후 60분 뒤, 두 번째 재시도 후 60분 뒤, 세 번째 재시도 후 120분 뒤 등의 간격으로 재시도가 시도됩니다. 지정된 마지막 시도 이후의 재시도는 동일한 간격으로 반복됩니다. 따라서, 우선 순위가 높은 메일은 이러한 전달 재시도가 240분 간격으로 수행됩니다.

전달 시도는 `notices`, `nonurgentnotices`, `normalnotices` 또는 `urgentnotices` 키워드에 지정된 기간 동안 계속됩니다. 전달이 성공적으로 이루어질 수 없으면 **전달 실패 알림**이 생성되고 메일은 보낸 사람에게 반환됩니다. `notices` 키워드에 대한 자세한 내용은 272페이지의 "**알림 메일 전달 간격 설정**"을 참조하십시오.

`backoff` 키워드를 사용하면 다양한 우선 순위를 갖는 메일에 대한 전달 재시도 간격 설정을 사용자 정의할 수 있습니다. `nonurgentbackoff`는 우선 순위가 낮은 메일에 대한 간격을 지정하고, `normalbackoff`는 우선 순위가 보통인 메일에 대한 간격을 지정하고, `urgentbackoff`는 우선 순위가 높은 메일에 대한 간격을 지정합니다. 이러한 키워드를 지정하지 않으면 우선 순위와 관계 없이 `backoff`에 의해 모든 메일에 대한 간격이 지정됩니다.

예를 들면 다음과 같습니다.

```
urgentbackoff "pt30m" "pt1h" "pt2h" "pt3h" "pt4h" "pt5h" "pt8h"
"pt16h"
```

여기서 우선 순위가 높은 메일의 경우 최초 전달 실패 후 30분 뒤, 첫 번째 전달 시도 후 1시간 뒤(최초 실패 후 1시간 30분 뒤), 두 번째 전달 시도 후 2시간 뒤, 세 번째 시도 후 3시간 뒤, 네 번째 시도 후 4시간 뒤, 다섯 번째 시도 후 5시간 뒤, 여섯 번째 시도 후 8시간 뒤, 일곱 번째 전달 시도 후 16시간 뒤에 각각 전달 재시도가 수행됩니다. 후속 시도는 `notices` 키워드에 지정된 기간까지 16시간마다 수행됩니다. 전달이 성공적으로 이루어질 수 없으면 전달 실패 알림이 생성되고 메일은 보낸 사람에게 반환됩니다. 간격 구문은 ISO 8601P에 나와 있으며 *Sun Java System Messaging Server Administration Reference*에도 설명되어 있습니다.

다음 예에서,

```
normalbackoff "pt30m" "pt1h" "pt8h" "p1d" "p2d" "p1w"
```

우선 순위가 보통인 메일의 경우 최초 전달 실패 후 30분 뒤, 첫 번째 전달 시도 후 1시간 뒤, 두 번째 시도 후 8시간 뒤, 세 번째 시도 후 1일 뒤, 네 번째 시도 후 2일 뒤, 다섯 번째 시도 후 1주일 뒤에 전달 재시도가 각각 수행되고 이후에는 `notices` 키워드에 지정된 기간까지 1주일마다 전달 재시도가 반복됩니다. 전달이 성공적으로 이루어질 수 없으면 전달 실패 알림이 생성되고 메일은 보낸 사람에게 반환됩니다.

마지막 예에서,

```
backoff "pt30m" "pt120m" "pt16h" "pt36h" "p3d"
```

모든 실패한 메일의 경우 `nonurgentbackoff`, `normalbackoff` 또는 `urgentbackoff` 키워드에 의해 대체되지 않는 한, 메일 우선 순위에 관계 없이 최초 전달 실패 후 30분 뒤, 첫 번째 재시도 후 2시간 뒤, 두 번째 재시도 후 16시간 뒤, 세 번째 재시도 후 36시간 뒤, 네 번째 재시도 후 3일 뒤에 전달 재시도가 각각 수행되고 이후에는 `notices` 키워드에 지정된 기간까지 3일마다 전달 재시도가 수행됩니다. 전달이 성공적으로 이루어질 수 없으면 전달 실패 알림이 생성되고 메일은 보낸 사람에게 반환됩니다.

## 채널 실행 작업의 처리 풀

키워드: `pool`

채널을 동일한 풀 내에서 실행하여 여러 채널이 자원을 공유하도록 구성할 수 있습니다. 다른 채널을 특정 채널에 전용인 풀에서 실행하도록 구성할 수 있습니다. 각 풀 내에서 메일은 메일 우선 순위에 따라 서로 다른 처리 대기열에 자동으로 정렬됩니다. 풀 내에서 우선 순위가 높은 메일이 우선 순위가 낮은 메일보다 먼저 처리됩니다. [363페이지의 "크기 기반 메일 우선 순위"](#)를 참조하십시오.

`pool` 키워드를 사용하면 작업이 만들어지는 풀을 채널 단위로 선택할 수 있습니다. `pool` 키워드는 현재 채널에 대한 전달 작업을 풀링해야 하는 풀 이름 앞에 와야 합니다. 풀 이름은 11자를 초과할 수 없습니다.

Job Controller 개념 및 구성에 대한 자세한 내용은 [247페이지의 "Job Controller 파일"](#), [194페이지의 "Job Controller"](#) 및 [360페이지의 "서비스 작업 제한"](#)을 참조하십시오.

## 서비스 작업 제한

키워드: `maxjobs`, `filesperjob`

메일이 채널의 대기열에 배치될 때마다 Job Controller는 해당 메일을 전달하기 위해 실행 중인 작업이 있는지 확인합니다. 여기에는 새 작업 프로세스를 시작하거나, 스레드를 추가하거나, 단순히 작업이 이미 실행 중인지 확인하는 것이 포함됩니다. 단일 서비스 작업으로 모든 메일 전달을 확인하지 못할 수도 있습니다. Job Controller 개념 및 구성에 대한 자세한 내용은 [247페이지의 "Job Controller 파일"](#), [360페이지의 "채널 실행 작업의 처리 풀"](#) 및 [194페이지의 "Job Controller"](#)를 참조하십시오.



특정 설치의 경우 메일 전달을 위해 시작할 프로세스 및 스레드에 대한 합리적인 최대 수가 있습니다. 이 최대 수는 프로세서 수, 디스크 속도, 연결 특징 등의 요인에 따라 다릅니다. MTA 구성에서는 다음을 제어할 수 있습니다.

- 지정된 채널에 대해 실행할 최대 프로세스 수(maxjobs 채널 키워드)
- 채널 집합에 대해 시작할 최대 프로세스 수(Job Controller 구성 파일의 관련 폴 섹션에 있는 JOB\_LIMIT 매개 변수)
- 새 스레드 또는 프로세스를 시작하기 전에 받은 대기열에 포함된 메일 수 (threaddepth 채널 키워드)
- 일부 채널의 경우 지정된 전달 프로그램 내에서 실행되는 최대 스레드 수(채널 옵션 파일에 있는 max\_client\_threads 매개 변수)

지정된 채널에 대해 실행을 시작하는 최대 프로세스 수는 채널에 설정된 maxjobs의 최대 값이며 채널이 실행되는 폴에 대해 설정된 JOB\_LIMIT입니다.

메일을 처리해야 한다고 가정합니다. 일반적으로 Job Controller는 새 프로세스를 다음과 같이 시작합니다.

- 채널에 대해 실행 중인 프로세스가 없고 폴 작업 제한에 도달하지 않은 경우 Job Controller는 새 프로세스를 시작합니다.
- 채널 프로그램이 단일 스레드이거나 스레드 제한에 도달하고 백로그가 threaddepth에 지정된 스레드 수의 배 이상으로 증가하고 채널 및 폴 작업 제한에 도달하지 않은 경우 Job Controller는 새 프로세스를 시작합니다.
- 채널 프로그램이 다중 스레드이고 스레드 제한에 도달하지 않고 메일 백로그가 threaddepth의 배 이상으로 증가한 경우 새 스레드가 시작됩니다.

특히, SMTP 채널의 경우 서로 다른 호스트에 대한 대기열에 메일이 포함될 경우 새 스레드 또는 프로세스가 시작됩니다. 따라서, SMTP 채널의 경우 Job Controller는 새 프로세스를 다음과 같이 시작합니다. 메일을 처리해야 한다고 가정합니다.

- SMTP 채널에 대해 실행 중인 프로세스가 없고 폴 제한에 도달하지 않은 경우 Job Controller는 새 프로세스를 시작합니다.
- 스레드 제한(MAX\_CLIENT\_THREADS)에 도달하고, 아직 사용되고 있지 않은 호스트의 대기열에 메일이 포함되고, 채널(maxjobs) 및 폴 작업 제한(JOB\_LIMIT)에 도달하지 않은 경우 새 프로세스가 시작됩니다.

- 스레드 제한에 도달하지 않고 아직 사용되고 있지 않은 호스트의 대기열에 메일이 포함될 경우 새 스레드가 시작됩니다.
- 스레드 제한에 도달하지 않고 메일이 대기열에 포함되어 해당 호스트에 대한 메일 백로그가 `threaddepth`의 배 이상으로 증가할 경우 새 스레드가 시작됩니다.

363페이지의 "SMTP 채널 스레드"도 참조하십시오.

`filesperjob` 키워드를 사용하여 MTA에서 추가 서비스 작업을 만들 수 있습니다. 이 키워드는 여러 서비스 작업을 만들어 처리하기 전에 연결된 채널로 보내야 하는 대기열 항목(파일) 수를 지정하는 단일의 양의 정수 매개 변수를 가집니다. 0보다 작거나 같은 값을 지정하면 하나의 서비스 작업만 대기열에 포함하라는 요청으로 해석됩니다. 키워드를 지정하지 않으면 0의 값을 지정한 것과 같습니다. 이 키워드의 효과는 최대화됩니다. 즉, 계산된 높은 숫자가 실제로 만들어지는 서비스 작업 수가 됩니다.

`filesperjob` 키워드는 실제 대기열 항목 또는 파일 수를 지정된 값으로 나눕니다. 지정된 메일의 대기열 항목 수는 `single` 및 `single_sys` 키워드의 사용, 메일 목록의 헤더 수정 작업 사양 등 많은 요소에 의해 제어됩니다.

`maxjobs` 키워드는 동시에 실행될 수 있는 총 서비스 작업 수에 대한 최대값을 지정합니다. 이 키워드는 정수 값이 뒤에 와야 합니다. 계산된 서비스 작업 수가 이 값보다 더 큰 경우 `maxjobs` 작업만 실제로 만들어집니다. `maxjobs`를 지정하지 않은 경우 이 값의 기본 값은 100입니다. 일반적으로 `maxjobs`는 채널이 사용되는 서비스 풀에 관계 없이 동시에 실행될 수 있는 총 작업 수보다 작거나 같은 값으로 설정됩니다.

## 연결 트랜잭션 제한 설정

키워드: `transactionlimit`

`transactionlimit`는 연결당 허용되는 메일 수를 제한합니다. 이 키워드를 사용하여 다음과 같은 방법으로 공격자를 차단할 수 있습니다.

공격자가 SMTP를 통해 연결한 다음 많은 RCPT TO 명령을 보내 합법적인 전자 메일 주소를 추측하려고 시도할 수 있습니다. 트랜잭션에 허용되는 유효하지 않은 RCPT TO 수를 제한하여 그런 공격을 차단할 수 있습니다. 공격자는 SMTP 세션에 허용되는 트랜잭션 수를 제한할 수 있는 `transactionlimit`가 있는 여러 트랜잭션을 사용하여 응답할 수 있습니다. 공격자가 여러 세션을 사용할 수 있지만 과도한 비용이 듭니다. 연결 억제를 사용하여 대부분의 경우에 실제로 많은 비용이 들게 하는 다양한 방법으로 세션 수를 제한할 수 있습니다.

이 비용은 우리 쪽에 부과되는 비용이지만, 일부 SMTP 클라이언트는 수신자 제한, 트랜잭션 제한 또는 두 가지 모두에 잘못된 반응을 나타내는 경우도 있습니다. 이러한 클라이언트에 대한 예외를 만들어야 합니다. 그러나, TCP 채널 옵션은 SMTP 서버에 무조건적으로 적용됩니다. 솔루션은 채널 키워드와 switchchannel을 사용하여 문제가 있는 에이전트의 경로를 더 큰 제한이 있는 채널로 지정하는 것입니다.

## 크기 기반 메일 우선 순위

키워드: urgentblocklimit, normalblocklimit, nonurgentblocklimit

urgentblocklimit, normalblocklimit 및 nonurgentblocklimit 키워드를 사용하여 MTA에 크기 기반 메일의 우선 순위를 낮추도록 지시할 수 있습니다. 이러한 키워드는 메일을 처리할 때 Job Controller가 적용하는 우선 순위에 영향을 미칩니다.

## SMTP 채널 스레드

키워드: threaddepth

다중 스레드 SMTP 클라이언트는 각 스레드에 대한 대상별로 보내는 메일을 정렬합니다. threaddepth 키워드를 사용하면 다중 스레드 SMTP 클라이언트에 한 스레드에서 지정된 수의 메일만 처리하도록 지시하여 대상이 같은 메일(일반적으로 한 스레드에서 모두 처리됨)일 경우에도 추가 스레드를 사용하게 할 수 있습니다. 이 키워드의 기본값은 10입니다.

채널의 백로그가 threaddepth의 배 이상으로 증가할 때마다 Job Controller는 해당 채널의 대기열에 포함된 메일 처리를 전담하는 처리량을 높이려고 시도합니다. 다중 스레드 채널의 경우 Job Controller는 해당 채널에 대한 메일을 처리하는 작업에서 새 스레드를 시작하게 합니다. 또는 모든 작업이 해당 채널에 대해 허용된 최대 수의 스레드(tcp\_\* 채널에 대한 옵션의 MAX\_CLIENT\_THREADS)를 갖는 경우 새 프로세스를 시작합니다. 단일 스레드 채널의 경우 새 프로세스를 시작합니다. 채널에 대한 작업 제한(maxjobs) 또는 풀에 대한 작업 제한(JOB\_LIMIT)에 도달한 경우 Job Controller는 새 작업을 시작하지 않습니다.

기본적으로 threaddepth는 적극적인 작업을 예약하는 방법을 제어합니다. 다음의 두 가지 다른 상황을 고려해 보겠습니다.

(1) 일반(아웃바운드) SMTP 채널

(2) 스마트 호스트에 전달하는 SMTP 채널

Job Controller는 특정 채널을 대상으로 하는 메일을 대상 호스트별로 정렬하고 이러한 대상 호스트의 백로그에 기초하여 메일을 처리하기 위한 작업을 예약합니다.

첫 번째 경우는 많은 수의 대상 호스트가 있고 대상 호스트의 백로그가 대부분 작습니다. 실행되는 스레드의 수가 많으며 aol, yahoo, hotmail 등과 같이 대량의 트래픽이 있을 수 있는 대상 호스트를 제외하고는 모두 제대로 작동합니다. 스레드 깊이가 128인 경우 백로그가 128에 도달하면 yahoo에 전달되는 두 번째 스레드만 가져오게 됩니다. 이는 바람직하지 않습니다.

두 번째 경우는 대상 호스트가 하나만 존재하며 해당 호스트에 많은 수의 스레드를 전달하는 것이 바람직합니다. 어느 경우든 기본값 10은 너무 작을 수 있습니다.

threaddepth를 사용하면 채널이 연결하는 SMTP 서버에서 여러 동시 연결을 처리할 수 있을 때 데몬 라우터 TCP/IP 채널(단일의 특정 SMTP에 연결하는 TCP/IP 채널)에서 다중 스레딩을 수행하는 데 특히 유용합니다.

## 여러 주소 확장

키워드: expandlimit, expandchannel, holdlimit

대부분의 채널은 각 인바운드 메일 전송에서 여러 수신자 주소 사양을 지원합니다. 단일 메일에 많은 수신자 주소가 있는 사양에서는 메일 전송 처리가 지연될 수 있습니다(온라인 지연). 너무 오래 지연될 경우 네트워크 시간 초과가 발생하여 메일 제출 시도가 반복되거나 기타 문제가 발생할 수 있습니다.

MTA는 단일 메일에 대해 지정된 수보다 더 많은 주소를 지정할 경우 지연(오프라인) 처리를 강제하는 특수 기능을 제공합니다. 메일 처리 지연은 온라인 지연을 대폭 줄일 수 있습니다. 그러나 처리 오버헤드가 지연되지만 완전히 제거되지는 않습니다.

예를 들어, 일반 reprocessing 채널과 expandlimit 키워드를 함께 사용하면 이 특수 기능이 활성화됩니다. expandlimit 키워드는 지연 처리 이전에 채널에서 받은 메일에 허용되는 주소 수를 지정하는 정수 인수를 가집니다. expandlimit 키워드를 지정하지 않은 경우 기본값은 무제한입니다. 값이 0이면 채널에서 수신하는 모든 주소에서 지연 처리를 수행합니다.

로컬 채널 또는 reprocessing 채널 자체에는 expandlimit 키워드를 지정하면 안 됩니다. 이러한 키워드를 지정하면 예상치 못한 결과가 발생할 수 있습니다.

지연 처리를 수행하는 데 실제로 사용되는 채널은 expandchannel 키워드를 사용하여 지정할 수 있습니다. expandchannel을 지정하지 않은 경우 reprocessing 채널이 기본적으로 사용되지만 다른 reprocessing 또는 processing 채널을 사용하는 것이 유용한 경우도 있습니다. expandchannel을 통해 지연 처리를 위한 채널을 지정하는 경우 해당 채널이 reprocessing 또는 processing 채널이어야 합니다. 다른 종류의 채널 사양은 예측할 수 없는 결과를 초래할 수 있습니다.

expandlimit 키워드를 적용하려면 reprocessing 채널이나 지연 처리를 수행하는 데 사용되는 모든 채널을 MTA 구성 파일에 추가해야 합니다. MTA 구성 유틸리티를 사용하여 구성을 작성한 경우 reprocessing 채널이 이미 있어야 합니다.

지나치게 큰 수신자 주소 목록은 UBE(Unsolicited Bulk Email) 특성을 가질 수 있습니다. holdlimit 키워드는 수신자가 지정된 수보다 많은 채널에서 수신하는 메일에 .HELD 메일 표시를 하고 reprocess 채널 또는 expandchannel 키워드를 통해 지정한 모든 채널의 대기열에 포함하도록 MTA에 지시합니다. 이러한 파일은 MTA 포스트마스터가 수동으로 처리할 때까지 reprocess 대기열에 처리되지 않은 상태로 유지됩니다.

## 서비스 변환 사용

키워드: service, noservice

service 키워드는 CHARSET-CONVERSION 항목에 관계 없이 서비스 변환을 무조건적으로 사용합니다. noservice 키워드를 설정하면 이 채널에 수신되는 메일에 대해 CHARSET-CONVERSION을 통해 서비스 변환을 사용해야 합니다.

## 주소 처리 구성

이 절에서는 주소 처리를 수행하는 키워드에 대해 설명합니다. 이 절은 다음 내용으로 구성되어 있습니다.

- 365페이지의 "서비스 변환 사용"
- 366페이지의 "주소 유형 및 규칙"
- 367페이지의 "! 및 %를 사용하는 주소 해석"
- 368페이지의 "주소에 라우팅 정보 추가"

- 369페이지의 "명시적 라우팅 주소의 다시 쓰기 사용 안 함"
- 370페이지의 "메일을 대기열에서 제거할 때 주소 다시 쓰기"
- 370페이지의 "완성되지 않은 주소를 수정할 때 사용할 호스트 이름 지정"
- 371페이지의 "수신자 헤더 행 없이 메일 적법화"
- 372페이지의 "잘못된 빈 수신자 헤더 스트라이핑"
- 372페이지의 "역방향 데이터베이스의 채널별 사용"
- 373페이지의 "제한된 메일함 인코딩 사용"
- 373페이지의 "Return-path: 헤더 행 생성"
- 374페이지의 "봉투의 To: 및 From: 주소에서 Received: 헤더 행 구성"
- 374페이지의 "주소 헤더 행의 주석 처리"
- 375페이지의 "주소 헤더 행에서 개인 이름 처리"
- 376페이지의 "별칭 파일 및 별칭 데이터베이스 검사 지정"
- 376페이지의 "하위 주소 처리"
- 377페이지의 "채널별 다시 쓰기 규칙 검사 사용"
- 378페이지의 "소스 경로 제거"
- 378페이지의 "반드시 별칭을 통해 주소 지정"

## 주소 유형 및 규칙

키워드: 822, 733, uucp, header\_822, header\_733, header\_uucp

이 키워드 그룹은 채널에서 지원하는 주소 유형을 제어합니다. 전송 계층(메일 봉투)에 사용되는 주소와 메일 헤더에 사용되는 주소를 구분합니다.

### 822(sourceroute)

소스 경로 봉투 주소입니다. 이 채널은 소스 경로를 포함하여 전체 RFC 822 형식의 봉투 주소 지정 규칙을 지원합니다. sourceroute 키워드를 822와 동의어로 사용할 수도 있습니다. 이 키워드는 다른 봉투 주소 유형 키워드를 지정하지 않은 경우의 기본값입니다.

## 733(percents)

백분율(%) 기호 봉투 주소입니다. 이 채널은 소스 경로를 제외한 전체 RFC 822 형식의 봉투 주소 지정을 지원합니다. 소스 경로는 백분율(%) 기호 규칙을 대신 사용하여 다시 작성해야 합니다. percents 키워드는 733에 대한 동의어로 사용될 수 있습니다.

---

**주** SMTP 채널에서 733 주소 규칙을 사용하면 이러한 규칙이 SMTP 봉투의 전송 계층 주소에 적용됩니다. 그렇게 하면 RFC 821을 위반할 수 있습니다. 733 주소 규칙은 반드시 필요한 경우에만 사용하십시오.

---

## uucp(bangstyle)

뱅 스타일 봉투 주소입니다. 이 채널은 RFC 976 뱅 스타일의 주소 규칙을 준수하는 주소를 봉투에 사용합니다. 이 채널의 예로는 UUCP 채널이 있습니다. bangstyle 키워드는 uucp에 대한 동의어로 사용될 수 있습니다.

## header\_822

소스 경로 헤더 주소입니다. 이 채널은 소스 경로를 포함하여 전체 RFC 822 형식의 헤더 주소 지정 규칙을 지원합니다. 다른 헤더 주소 유형 키워드를 지정하지 않을 경우의 기본값입니다.

## header\_733

백분율(%) 기호 헤더 주소입니다. 이 채널은 소스 경로를 제외한 RFC 822 형식의 헤더 주소 지정을 지원합니다. 소스 경로는 백분율(%) 기호 규칙을 대신 사용하여 다시 작성해야 합니다.

---

**주** 메일 헤더에 733 주소 규칙을 사용하면 RFC 822 및 RFC 976 위반입니다. 채널이 소스 경로 주소를 처리할 수 없는 시스템에 연결된다고 확신하는 경우에만 이 키워드를 사용하십시오.

---

## header\_uucp

UUCP 또는 뱅 스타일의 헤더 주소입니다. 이 키워드를 사용하면 RFC 976 위반이므로 이 키워드는 사용하지 않는 것이 좋습니다.

# ! 및 %를 사용하는 주소 해석

키워드: bangoverpercent, nobangoverpercent, percentonly

주소는 항상 RFC 822 및 RFC 976에 따라 해석되지만 이러한 표준에 맞게 주소가 지정되지 않은 복합 주소를 처리할 경우 애매할 수 있습니다. 특히 A!B%C 형식 주소는 다음과 같이 해석될 수 있습니다.

- A는 라우팅 호스트로 해석되고 C는 최종 대상 호스트로 해석됩니다.

또는

- C는 라우팅 호스트로 해석되고 A는 최종 대상 호스트로 해석됩니다.

RFC 976은 메일 프로그램이 두 번째 규칙을 사용하여 주소를 해석할 수 있음을 의미하지만 그런 해석이 반드시 필요하다는 의미는 아닙니다. 첫 번째 해석 방법이 더 좋은 경우도 있습니다.

bangoverpercent 키워드는 첫 번째 A!(B%C) 해석을 수행하게 합니다.

nobangoverpercent 키워드는 두 번째(A!B)%C 해석을 수행하게 합니다. 기본값은 nobangoverpercent입니다.

---

**주** 이 키워드는 A!B@C 형식 주소 처리에 영향을 미치지 않습니다. 이러한 주소는 항상 (A!B)@C로 처리됩니다. 이러한 처리는 RFC 822와 RFC 976 모두에서 필수입니다.

---

percentonly 키워드는 뱅 경로를 무시합니다. 이 키워드를 설정하면 %이 라우팅으로 해석됩니다.

## 주소에 라우팅 정보 추가

키워드: `exproute`, `noexproute`, `improute`, `noimproute`

MTA가 처리하는 주소 지정 모델에서는 모든 시스템이 다른 나머지 시스템의 주소와 다른 시스템에 연결하는 방법을 알고 있는 것으로 가정합니다. 불행하게도 이러한 가정이 모든 경우에 적용되는 것은 아닙니다. 채널이 다른 나머지 시스템에서는 알지 못하는 하나 이상의 시스템(예: 개인 TCP/IP 네트워크의 내부 시스템)에 연결하는 경우가 있습니다. 이 채널의 시스템 주소는 사이트 외부의 원격 시스템에는 적합하지 않을 수 있습니다. 그러한 주소에 회신할 수 있으려면 로컬 시스템을 통해 메일 경로를 지정하도록 원격 시스템에 알려주는 소스 경로가 해당 주소에 포함되어 있어야 합니다. 그러면 로컬 시스템이 메일의 경로를 이러한 시스템으로 (자동) 지정할 수 있습니다.



`exproute` 키워드("explicit routing"의 약어)는 주소를 원격 시스템에 전달할 때 연결된 채널에 명시적 라우팅이 필요함을 MTA에 알려 줍니다. 이 키워드를 한 채널에서 지정하면 MTA가 해당 채널과 일치하는 모든 헤더 주소와 모든 봉투의 From: 주소에 로컬 시스템의 이름 또는 로컬 시스템의 현재 별칭을 포함하는 라우팅 정보를 추가합니다. 기본값인 `noexproute`는 라우팅 정보를 추가하지 않도록 지정합니다.

`EXPROUTE_FORWARD` 옵션을 사용하여 `exproute` 작업을 역방향 주소로 제한할 수 있습니다. 다른 시나리오는 MTA가 자체적으로 라우팅을 수행할 수 없는 채널을 통해 시스템에 연결하는 경우입니다. 이 경우 부적합한 시스템에 연결되는 채널에 보낸 메일에 해당 주소가 사용되는 시기를 나타내는 라우팅이 다른 채널과 연결된 모든 주소에 있어야 합니다.

암시적 라우팅과 `improute` 키워드는 이 상황을 처리하는 데 사용됩니다. MTA는 다른 채널과 일치하는 모든 주소가 `improute` 표시 채널에 보낸 메일에 사용될 경우 라우팅이 필요함을 알고 있습니다. 기본값인 `noimproute`는 지정된 채널에서 보내는 메일의 주소에 라우팅 정보를 추가하지 않도록 지정합니다. `IMPROUTE_FORWARD` 옵션을 사용하여 `improute` 작업을 역방향 주소로 제한할 수 있습니다.

`exproute` 및 `improute` 키워드의 사용을 절제해야 합니다. 이러한 키워드는 길고 복잡한 주소를 만들기 때문에 다른 시스템에 사용되는 지능적인 라우팅 체계를 손상시킬 수 있습니다. 명시적 라우팅과 암시적 라우팅을 지정된 경로와 혼동해서는 안 됩니다. 지정된 루트는 라우팅 정보를 다시 쓰기 규칙에서 주소로 삽입하는 데 사용됩니다. 이 키워드는 특수 `A@B@C` 다시 쓰기 규칙 템플릿에 의해 활성화됩니다.

지정된 경로를 활성화하면 헤더와 봉투에 있는 모든 주소에 적용됩니다. 지정된 경로는 특정 다시 쓰기 규칙에 의해 활성화되며 일반적으로 현재 사용 중인 채널과는 관련이 없습니다. 다시 말해서 명시적 라우팅과 암시적 라우팅은 채널 단위로 제어되며 삽입된 경로 주소는 항상 로컬 시스템입니다.

## 명시적 라우팅 주소의 다시 쓰기 사용 안 함

키워드: `routelocal`

`routelocal` 채널 키워드는 채널에 주소를 다시 쓸 때 MTA가 주소에 명시적 라우팅을 "단락화"하게 합니다. 명시적 라우팅 주소(!, % 또는 @ 문자 사용)는 단순화됩니다.

내부 TCP/IP 채널과 같은 "내부" 채널에 이 키워드를 사용하면 SMTP 릴레이 차단 구성을 단순화할 수 있습니다.

명시적 % 또는 다른 라우팅이 필요한 채널에서는 이 키워드를 사용하지 마십시오.

## 메일을 대기열에서 제거할 때 주소 다시 쓰기

키워드: `connectalias`, `connectcanonical`

MTA는 일반적으로 채널 대기열에 메일을 넣을 때 주소를 다시 씁니다. 메일을 대기열에서 제거하는 동안에는 추가 다시 쓰기를 수행하지 않습니다. 그렇게 하면 채널 대기열에 이전 이름으로 주소가 지정된 메일이 있을 경우 호스트 이름을 변경하면 문제가 발생할 수 있습니다.

`connectalias` 키워드는 수신자 주소에 나열된 모든 호스트에 전달하도록 MTA에 지시하는 기본값입니다. `connectcanonical` 키워드는 MTA가 연결되는 시스템의 호스트 별칭에 연결하도록 MTA에 지시합니다.

## 완성되지 않은 주소를 수정할 때 사용할 호스트 이름 지정

키워드: `remotehost`, `noremotehost`, `defaulthost`, `nodefaulthost`

MTA는 잘못 구성되거나 호환되지 않는 메일 프로그램 및 SMTP 클라이언트로부터 도메인 이름이 포함되지 않은 주소를 받는 경우가 있습니다. 이 경우 MTA는 이러한 주소를 올바른 주소로 만든 후에 전달을 시도합니다. 이를 위해 MTA는 주소에 도메인 이름을 추가(예: `@siroe.com`을 `mrochek`에 추가)합니다.

도메인 이름이 없는 봉투의 `To:` 주소의 경우 MTA는 항상 로컬 호스트 이름을 추가해야 한다고 가정합니다. 그러나 `From:` 주소와 같은 다른 주소에서는 MTA SMTP 서버의 경우 두 가지 이상의 도메인 이름 선택 항목(로컬 MTA 호스트 이름과 클라이언트 SMTP가 보고한 원격 호스트 이름)이 있습니다. 세 번째 선택 항목(해당 채널에서 수신하는 메일에 추가할 특정 도메인 이름)이 있는 경우도 있습니다. 처음 두 선택 항목이 특정 빈도로 계속 해서 발생할 경우 그 중 하나가 올바른 수 있습니다. 잘못 구성된 SMTP 클라이언트를 처리할 경우 원격 호스트 도메인 이름을 사용하는 것이 좋습니다. SMTP가 메일을 게시하는데 사용하는 POP 또는 IMAP 클라이언트와 같은 경량 원격 메일 클라이언트를 처리할

경우 로컬 호스트 도메인 이름을 사용하면 안 됩니다. POP 또는 IMAP와 같은 경량 원격 메일 클라이언트의 경우 클라이언트에 로컬 호스트의 도메인 이름이 아닌 해당 클라이언트의 특정 도메인 이름이 있어야 합니다. 그런 다음 다른 특정 도메인 이름을 추가할 수 있습니다. MTA가 채널 단위로 선택하도록 허용하는 것이 가장 좋습니다.

noremotehost 채널 키워드는 로컬 호스트 이름을 사용하도록 지정합니다. 기본값은 noremotehost 키워드입니다.

defaultthost 채널 키워드는 받는 사용자 아이디에 추가할 특정 호스트 이름을 지정하는데 사용됩니다. 또한, 해당 채널에서 수신하는 주소(봉투의 From: 및 헤더)를 완성하는데 사용할 도메인 이름이 뒤에 와야 합니다. 제출 채널의 경우 defaultthost 키워드의 첫 번째 인수가 봉투의 To: 주소에도 적용됩니다. 선택적 두 번째 도메인 이름(하나 이상의 점이 있음)을 봉투의 To: 주소를 완성하는데 사용하도록 지정할 수 있습니다. 기본값은 nodefaultthost입니다.

350페이지의 "받는 메일을 위한 대체 채널(전환 채널)"에서 설명한 것처럼 switchchannel 키워드를 사용하여 받는 SMTP 연결을 특정 채널에 연결할 수 있습니다. 이 기능을 사용하면 원격 메일 클라이언트를 적절하게 처리될 수 있는 특정 채널에서 그룹화할 수 있습니다. 또한, MTA 호스트에서 네트워크 차원 문제를 해결하려고 시도하는 것보다는 비호환 클라이언트를 여러 개 사용 중인 경우에도 표준 호환 원격 메일 클라이언트를 배포하는 것이 더 간단합니다.

## 수신자 헤더 행 없이 메일 적법화

키워드: missingrecipientpolicy

RFC 822(인터넷) 메일에는 To:, Cc: 또는 Bcc: 헤더 행과 같은 수신자 헤더 행이 있어야 합니다. 이러한 헤더 행이 없는 메일은 잘못된 것입니다. 그럼에도 불구하고 sendmail의 많은 이전 버전과 같은 일부 손상된 사용자 에이전트 및 메일 프로그램에서는 잘못된 메일을 생성합니다.

missingrecipientpolicy 키워드는 그러한 메일을 사용하는 방법을 지정하는 정수 값을 취합니다. 기본값은 이 키워드가 명백히 표시되지 않은 경우 1(잘못된 메일을 변경하지 않고 전달)이 됩니다.

**표 12-8** missingrecipientpolicy 값

| 값 | 작업                           |
|---|------------------------------|
| 0 | 봉투의 To: 수신자를 To: 헤더 행에 넣습니다. |
| 1 | 잘못된 메일을 변경하지 않은 상태로 전달합니다.   |

표 12-8 missingrecipientpolicy 값

| 값 | 작업                                                               |
|---|------------------------------------------------------------------|
| 2 | 봉투의 To: 수신자를 To: 헤더 행에 넣습니다.                                     |
| 3 | 모든 봉투의 To: 수신자를 한 Bcc: 헤더 행에 넣습니다.                               |
| 4 | 그룹 구조(예: ",") To: 헤더 행을 "To: Recipients not specified.;"로 생성합니다. |
| 5 | 빈 Bcc: 헤더 행을 생성합니다.                                              |
| 6 | 메일을 거부합니다.                                                       |

MISSING\_RECIPIENT\_POLICY 옵션을 사용하여 이 동작에 대한 MTA 시스템 기본값을 설정할 수 있습니다. 초기 Messaging Server 구성에서는 MISSING\_RECIPIENT\_POLICY 가 1로 설정됩니다.

## 잘못된 빈 수신자 헤더 스트라이핑

키워드: dropblank, nodropblank

RFC 822(인터넷) 메일에서 To:, Resent-To:, Cc: 또는 Resent-Cc: 헤더에는 하나 이상의 주소가 포함되어 있어야 합니다. 이러한 헤더는 빈 값을 가질 수 없습니다. 그럼에도 불구하고 일부 메일 프로그램은 잘못된 헤더를 생성할 수 있습니다. dropblank 채널 키워드를 소스 채널에 지정한 경우 MTA는 받는 메일에서 그러한 잘못된 빈 헤더를 스트라이프합니다.

## 역방향 데이터베이스의 채널별 사용

키워드: reverse, noreverse

reverse 키워드는 채널 대기열에 포함된 메일의 주소를 주소 역방향 데이터베이스 또는 REVERSE 매핑을 통해 검색하여 수정(있는 경우)하도록 지시합니다. noreverse는 채널 대기열에 포함된 메일의 주소를 주소 역방향 처리에서 제외합니다. 기본값은 reverse 키워드입니다. 자세한 내용은 257페이지의 "주소를 내부 형식에서 공용 형식으로 변환"을 참조하십시오.

## 제한된 메일함 인코딩 사용

키워드: `restricted`, `unrestricted`

일부 메일 시스템에서는 RFC 822에서 허용하는 모든 형식의 주소를 처리하는 데 어려움이 있습니다. 이러한 공통된 예로는 잘못된 구성 파일을 갖는 `sendmail` 기반 메일 프로그램이 있습니다. 따옴표가 있는 로컬 부분 또는 메일함 사양이 문제의 원인이 되는 경우가 많습니다.

```
"smith, ned"@siroe.com
```

이러한 것이 문제의 주된 원인이며 RFC 1137에는 이러한 문제를 해결하기 위한 방법론이 나와 있습니다. 기본적인 방법은 주소에서 따옴표를 제거한 다음 따옴표가 필요한 문자를 `atom`에 허용된 문자로 매핑하는 변환을 적용하는 것입니다. 여기에 사용되는 `atom`에 대한 정의는 RFC 822를 참조하십시오. 예를 들어, 선행 주소가 다음과 같습니다.

```
smith#m#_ned@siroe.com
```

`restricted` 채널 키워드는 채널이 이 인코딩을 필요로 하는 메일 시스템에 연결됨을 MTA에 알려줍니다. 그러면 MTA는 채널에 메일이 기록될 때 헤더와 봉투 주소 모두에서 따옴표가 있는 로컬 부분을 인코딩합니다. 채널의 받는 주소는 자동으로 디코딩됩니다. `unrestricted` 키워드는 MTA에 RFC 1137 인코딩 및 디코딩을 수행하지 않도록 지시합니다. 기본값은 `unrestricted` 키워드입니다.

---

**주** 따옴표가 있는 로컬 부분을 적용할 수 없는 시스템에 연결하는 채널에는 `restricted` 키워드를 적용해야 합니다. 따옴표가 있는 로컬 부분을 실제로 생성하는 채널에는 이 키워드를 적용할 수 없습니다. 그런 주소를 생성할 수 있는 채널은 해당 주소를 처리할 수 있다고 가정합니다.

---

## Return-path: 헤더 행 생성

키워드: `addreturnpath`, `noaddreturnpath`

일반적으로 `Return-path:` 헤더 행을 추가하는 것은 최종 전달을 수행하는 채널에서 담당합니다. `ims-ms` 채널과 같은 일부 채널의 경우 채널에서 `Return-path:` 헤더를 추가하는 것보다 MTA에서 추가하는 것이 더 효과적입니다. `addreturnpath` 키워드는 `Return-path:` 헤더가 이 채널의 대기열에 포함될 때 이 경로를 추가합니다.

## 봉투의 To: 및 From: 주소에서 Received: 헤더 행 구성

키워드: `receivedfor`, `noreceivedfor`, `receivedfrom`, `noreceivedfrom`

`receivedfor` 키워드는 메일의 주소가 한 명의 봉투 수신자로만 지정된 경우 해당 봉투의 To: 주소를 Received: 헤더 행에 포함하도록 MTA에 지시합니다. 기본값은 `receivedfor` 키워드입니다. `noreceivedfor` 키워드는 봉투 주소 정보를 포함하지 않고 Received: 헤더 행을 구성하도록 MTA에 지시합니다.

`receivedfrom` 키워드는 특정 종류의 메일 목록 확장으로 인해 MTA에서 봉투의 From: 주소를 변경한 경우, 받는 메일에 대한 Received: 헤더 행을 구성할 때 원래의 From: 주소를 포함하도록 MTA에 지시합니다. 기본값은 `receivedfrom`입니다.

`noreceivedfrom` 키워드는 원래 From: 주소를 포함하지 않고 Received: 헤더 행을 구성하도록 MTA에 지시합니다.

## 주소 헤더 행의 주석 처리

키워드: `commentinc`, `commentmap`, `commentomit`, `commentstrip`, `commenttotal`, `sourcecommentinc`, `sourcecommentmap`, `sourcecommentomit`, `sourcecommentstrip`, `sourcecommenttotal`

MTA는 필요한 경우에만 헤더 행의 내용을 해석합니다. 그러나 주소를 포함하는 모든 등록된 헤더 행의 구문을 분석하여 축약형 주소를 제거한 다음 올바른 주소로 변환해야 합니다. 이 프로세스 중에 헤더 행을 다시 작성할 때 주석(괄호로 묶인 문자열)을 추출하여 수정하거나 제외할 수 있습니다.

이 동작은 `commentinc`, `commentmap`, `commentomit`, `commentstrip` 및 `commenttotal` 키워드를 사용하여 제어합니다. `commentinc` 키워드는 헤더 행에 주석을 유지하도록 MTA에 지시하는 기본값입니다. `commentomit` 키워드는 To:, From:, Cc: 헤더 행과 같은 주소 지정 헤더에서 주석을 제거하도록 MTA에 지시합니다.

`commenttotal` 키워드는 Received: 헤더 행을 제외한 모든 헤더 행에서 주석을 제거하도록 MTA에 지시합니다. 이 키워드는 대부분 유용하지 않거나 권장되지 않습니다. `commentstrip`은 모든 주석 필드에서 `nonatomic` 문자를 제거하도록 MTA에 지시합니다. `commentmap` 키워드는 COMMENT\_STRINGS 매핑 테이블을 통해 주석 문자열을 실행합니다.

소스 채널에서 이 동작은 `sourcecommentinc`, `sourcecommentmap`, `sourcecommentomit`, `sourcecommentstrip` 및 `sourcecommenttotal` 키워드에 의해 제어됩니다. `sourcecommentinc` 키워드는 헤더 행에 주석을 유지하도록 MTA에 지시하는 기본값입니다. `sourcecommentomit` 키워드는 `To:`, `From:`, `Cc:` 등과 같은 주소 지정 헤더에서 주석을 제거하도록 MTA에 지시합니다. `sourcecommenttotal` 키워드는 `Received:` 헤더를 제외한 모든 헤더에서 주석을 제거하도록 MTA에 지시합니다. 따라서, 이 키워드는 대부분 유용하지 않거나 권장되지 않습니다. 마지막으로 `sourcecommentstrip` 키워드는 모든 주석 필드에서 `nonatomic` 문자를 스트라이프하도록 MTA에 지시합니다. `sourcecommentmap` 키워드는 소스 채널을 통해 주석 문자열을 실행합니다.

이러한 키워드는 모든 채널에 적용될 수 있습니다.

COMMENT\_STRINGS 매핑 테이블의 구문은 다음과 같습니다.

```
(comment_text) | address
```

항목 템플릿가 \$Y 플래그를 설정하는 경우 원래 주석이 지정된 텍스트(괄호로 묶임)로 변경됩니다.

## 주소 헤더 행에서 개인 이름 처리

키워드: `personalinc`, `personalmap`, `personalomit`, `personalstrip`, `sourcepersonalinc`, `sourcepersonalmap`, `sourcepersonalomit`, `sourcepersonalstrip`

다시 쓰기 프로세스 중에 주소를 포함하는 모든 등록된 헤더 행의 구문을 분석하여 축약형 주소를 제거한 다음 올바른 주소로 변환해야 합니다. 이 프로세스 중에 헤더 행을 다시 작성할 때 개인 이름(대괄호로 구분된 주소 앞의 문자열)을 추출하여 선택적으로 수정하거나 제외할 수 있습니다.

이 동작은 `personalinc`, `personalmap`, `personalomit` 및 `personalstrip` 키워드를 사용하여 제어합니다. `personalinc` 키워드는 헤더에 개인 이름을 유지하도록 MTA에 지시하는 기본값입니다. `personalomit` 키워드는 모든 개인 이름을 제거하도록 MTA에 지시합니다. `personalstrip` 키워드는 모든 개인 이름 필드에서 `nonatomic` 문자를 스트라이프하도록 MTA에 지시합니다. `personalmap` 키워드는 PERSONAL\_NAMES 매핑 테이블을 통해 개인 이름을 실행하도록 MTA에 지시합니다.

소스 채널에서 이 동작은 `sourcepersonalinc`, `sourcepersonalmap`, `sourcepersonalomit` 또는 `sourcepersonalstrip` 키워드에 의해 제어됩니다. `sourcepersonalinc` 키워드는 헤더에 개인 이름을 유지하도록 MTA에 지시하는 기본 값입니다. `sourcepersonalomit` 키워드는 모든 개인 이름을 제거하도록 MTA에 지시합니다. 마지막으로 `sourcepersonalstrip`은 모든 개인 이름 필드에서 `nonatomic` 문자를 스트라이프하도록 MTA에 지시합니다. `sourcepersonalmap` 키워드는 소스 채널을 통해 개인 이름을 실행하도록 MTA에 지시합니다.

이러한 키워드는 모든 채널에 적용될 수 있습니다.

`PERSONAL_NAMES` 매핑 테이블 검사 구문은 다음과 같습니다.

```
personal_name | address
```

템플릿에 `$Y` 플래그를 설정하면 원래의 개인 이름이 지정된 텍스트로 변경됩니다.

## 별칭 파일 및 별칭 데이터베이스 검사 지정

키워드: `aliaslocal`

일반적으로 로컬 채널(UNIX의 1 채널)에 다시 작성된 주소만 별칭 파일과 별칭 데이터베이스에서 조회됩니다. `aliaslocal` 키워드를 채널에 배치하여 별칭 파일과 별칭 데이터베이스에서 해당 채널에 다시 작성된 주소를 조회할 수도 있습니다. 만든 조회 검사의 정확한 형식은 `ALIAS_DOMAINS` 옵션에 의해 제어됩니다.

## 하위 주소 처리

키워드: `subaddressexact`, `subaddressrelaxed`, `subaddresswild`

하위 주소의 개념 관련 배경으로 원시 및 `ims-ms` 채널은 주소의 로컬 부분(메일함 부분)에서 + 문자를 해석합니다. `name+subaddress@domain` 형식 주소에서 MTA는 더하기(+) 문자 뒤의 메일함 부분을 하위 주소로 간주합니다. 원시 채널은 하위 주소를 추가 정보로 취급하고 해당 하위 주소에 관계 없이 계정 이름에 실제로 전달합니다. `ims-ms` 채널은 하위 주소를 전달할 폴더 이름으로 해석합니다.



하위 주소는 로컬 채널(UNIX의 L 채널)에 의한 별칭 조회, `aliaslocal` 키워드로 표시한 채널에 의한 별칭 조회, 디렉토리 채널에 의한 메일함 조회 등에도 영향을 미칩니다. 주소를 항목과 비교할 경우 MTA는 항상 하위 주소를 포함한 전체 메일함에서 정확한 일치를 먼저 검사합니다. 그런 다음 MTA가 추가 검사를 수행하는지 여부를 구성할 수 있습니다.

`subaddressexact` 키워드는 항목 일치 중에 특수 하위 주소 처리를 수행하지 않도록 MTA에 지시합니다. 하위 주소를 포함하여 전체 메일함이 항목과 일치해야 별칭이 일치하는 것으로 간주됩니다. 추가 비교(와일드카드 비교 또는 하위 주소를 제외한 비교)가 수행되지 않습니다. `subaddresswild` 키워드는 전체 하위 주소를 포함한 정확한 일치를 조사한 다음 `name+*` 형식 항목을 조사하도록 MTA에 지시합니다. `subaddressrelaxed` 키워드는 정확한 일치를 조사하고 `name+*` 형식 일치를 조사한 다음 이름 부분에 대해서만 일치를 조사하도록 MTA에 지시합니다. `subaddressrelaxed`를 사용하면 다음 형식의 별칭 항목이 `name` 또는 `name+subaddress`와 일치되고, 일반 이름이 새 이름으로 변환되고, `name+subaddress`가 `newname+subaddress`로 변환됩니다. 기본값은 `subaddressrelaxed` 키워드입니다.

`name:` `newname+*`

따라서 `subaddresswild` 키워드 또는 `subaddressrelaxed` 키워드는 별칭 또는 디렉토리 채널이 사용 중이지만 임의의 하위 주소를 사용하여 주소가 지정된 메일을 받으려는 경우에 유용할 수 있습니다. 이러한 키워드를 사용하면 주소에서 단일 하위 주소 변형마다 별도의 항목을 둘 필요가 없습니다.

이러한 키워드는 로컬 채널(UNIX의 L 채널) 또는 `aliaslocal` 키워드로 표시한 채널에만 적용됩니다.

표준 Messaging Server 구성은 실제로 `subaddressrelaxed` 동작을 하는 L 채널에서 릴레이됩니다(기본적으로 다른 키워드를 명시하지 않은 경우).

## 채널별 다시 쓰기 규칙 검사 사용

키워드: `rules, norules`

rules 키워드는 이 채널에 대해 채널별 다시 쓰기 규칙 검사를 실행하도록 MTA에 지시합니다. 기본값입니다. norules 키워드는 이 채널을 검사하지 않도록 MTA에 지시합니다. 이 두 키워드는 일반적으로 디버깅하는 데 사용되고 실제 응용 프로그램에서는 거의 사용되지 않습니다.

## 소스 경로 제거

키워드: `dequeue_removeoute`

`dequeue_removeoute` 키워드는 메일을 대기열에서 제거할 때 소스 경로를 봉투의 To: 주소에서 제거합니다. 이 키워드는 현재 `tcp-*` 채널에서만 구현됩니다. 또한, 소스 경로를 올바르게 처리하지 못하는 시스템에 메일을 전송할 때 유용합니다.

## 반드시 별칭을 통해 주소 지정

키워드: `viaaliasoptional`, `viaaliasrequired`

`viaaliasrequired`는 채널과 일치하는 최종 수신자 주소를 별칭을 통해 생성해야 함을 지정합니다. 최종 수신자 주소는 별칭 확장(해당하는 경우)이 수행된 이후의 일치를 참조합니다. 주소를 MTA에 수신자 주소로 직접 전달할 수 없습니다. 즉, 주소를 채널에 다시 쓰는 것만으로는 부족합니다. 채널에 다시 쓴 후 별칭을 통해 주소를 확장해야 채널과 일치하는 것으로 간주됩니다.

예를 들어, 로컬 채널에서 `viaaliasrequired` 키워드를 사용하여 임의의 계정(예: UNIX 시스템에서 임의의 원시 Berkeley 메일함)에 전달하지 못하게 할 수 있습니다.

기본값은 `viaaliasoptional`이며 별칭을 사용하여 채널과 일치하는 최종 수신자 주소를 생성할 필요가 없음을 의미합니다.

## 헤더 처리 구성

이 절에서는 헤더 및 봉투 정보를 처리하는 키워드에 대해 설명합니다. 이 절은 다음 내용으로 구성되어 있습니다.

- 379페이지의 "포함 헤더 다시 쓰기"
- 379페이지의 "선택한 메일 헤더 행 제거"
- 381페이지의 "X-Envelope-to: 헤더 행 생성/제거"

- 381페이지의 "두 자리 또는 네 자리로 날짜 변환"
- 381페이지의 "날짜의 요일 지정"
- 382페이지의 "긴 헤더 행 자동 분할"
- 382페이지의 "헤더 맞춤 및 접기"
- 383페이지의 "최대 길이 헤더 지정"
- 383페이지의 "민감도 검사"
- 384페이지의 "헤더의 기본 언어 설정"

## 포함 헤더 다시 쓰기

키워드: `noinner`, `inner`

필요한 경우에만 헤더 행의 내용을 해석합니다. MIME 메일은 메일 내부에 메일을 포함하는 기능이 있기 때문에 여러 메일 헤더 집합을 포함할 수 있습니다(메일/RFC822). MTA는 일반적으로 가장 외부에 있는 메일 헤더 집합만 해석하고 다시 씁니다. 메일의 내부 헤더에도 헤더 다시 쓰기를 적용하도록 MTA에 선택적으로 지시할 수 있습니다.

이 동작은 `noinner` 및 `inner` 키워드에 의해 제어됩니다. `noinner` 키워드는 내부 메일 헤더 행을 다시 쓰지 않도록 MTA에 지시하는 기본값입니다. `inner` 키워드는 메일의 구문을 분석하고 내부 헤더를 다시 쓰도록 MTA에 지시합니다. 이러한 키워드는 모든 채널에 적용될 수 있습니다.

## 선택한 메일 헤더 행 제거

키워드: `headertrim`, `noheadertrim`, `headerread`, `noheaderread`, `innertrim`, `noinnertrim`

MTA는 메일에서 선택한 메일 헤더 행을 잘라내거나 제거하기 위한 채널 단위 기능을 제공합니다. 이 작업은 채널 키워드와 관련 헤더 옵션 파일을 조합하거나 두 가지를 모두 사용하여 수행됩니다. 헤더 옵션 파일 형식에 대해서는 *Sun Java System Messaging Server Administration Reference*의 MTA 장에 설명되어 있습니다.

`headertrim` 키워드는 *원본 메일 헤더를 처리한 후에* 채널과 연결된 헤더 옵션 파일을 참조하여 해당 대상 채널의 대기열에 포함된 메일의 헤더를 적절하게 잘라내도록 MTA에 지시합니다. `noheadertrim` 키워드는 헤더 자르기를 수행하지 않습니다. 기본값은 `noheadertrim` 키워드입니다.

`innertrim` 키워드는 내부 메일 부분(내장된 MESSAGE/RFC822 부분)에서도 헤더 자르기를 수행하도록 MTA에 지시합니다. 기본값인 `noinnertrim` 키워드는 내부 메일 부분에서 헤더 자르기를 수행하지 않도록 MTA에 지시합니다.

`headerread` 키워드는 *원본 메일 헤더를 처리하기 전에* 채널과 연결된 헤더 옵션 파일을 참조하여 해당 소스 채널에 의해 대기열에 포함된 메일의 헤더를 적절하게 잘라내도록 MTA에 지시합니다. 반면에 `headertrim` 헤더 자르기는 메일을 처리한 이후에 적용되며 소스 채널이 아니라 대상 채널입니다. `noheaderread` 키워드는 메일 대기열이 포함된 헤더 자르기를 수행하지 않습니다. 기본값은 `noheaderread`입니다.

`headeromit` 및 `headerbottom` 키워드와 달리 `headertrim` 및 `headerread` 키워드는 모든 채널에 적용될 수 있습니다. 메일에서 필수 헤더 정보를 스트라이프하면 MTA 작업이 잘못 수행될 수 있습니다. 따라서 제거하거나 제한할 헤더를 선택할 경우 각별히 주의하십시오. 이 기능은 선택한 헤더 행을 제거하거나 제한해야 할 경우를 위해 제공됩니다.

---

**주의** 메일에서 헤더 정보를 스트라이프하면 MTA 작업이 잘못 수행될 수 있습니다. 따라서 제거하거나 제한할 헤더를 선택할 경우 주의하십시오. 이러한 키워드는 선택한 헤더 행을 제거하거나 제한해야 할 경우를 위해 제공됩니다. 헤더 행을 자르거나 제거하기 전에 해당 헤더의 사용법을 이해하고 제거의 함축된 의미를 고려해야 합니다.

---

`headertrim` 및 `innertrim` 키워드의 헤더 옵션 파일에는 채널이 있는 `channel_headers.opt` 형식 이름과 헤더 옵션 파일이 연결되는 채널 이름이 있습니다. 마찬가지로 `headerread` 키워드의 헤더 옵션 파일에는 `channel_read_headers.opt` 형식의 이름이 있습니다. 이러한 파일은 MTA 구성 디렉토리인 `instance_root/imta/config/`에 저장됩니다.

## X-Envelope-to: 헤더 행 생성/제거

키워드: `x_env_to`, `nox_env_to`

`x_env_to` 및 `nox_env_to` 키워드는 특정 채널의 대기열에 포함된 메일 복사본에서 X-Envelope-to 헤더 행의 생성 또는 억제를 제어합니다. `single` 키워드로 표시한 채널에서 `x_env_to` 키워드는 이러한 헤더를 생성하고 `nox_env_to` 키워드는 대기열에 포함된 메일에서 해당 헤더를 제거합니다. 기본값은 `nox_env_to`입니다.

`x_env_to` 키워드를 적용하려면 `single` 키워드가 필요합니다.

## 두 자리 또는 네 자리로 날짜 변환

키워드: `datefour`, `datetwo`

원본 RFC 822 사양은 메일 헤더의 날짜 필드에서 두 자리 연도를 호출합니다. 이 연도 표시는 이후에 RFC 1123에서 네 자리로 변경되었지만, 일부 이전 메일 시스템에서는 네 자리 날짜를 사용할 수 없습니다. 또한, 일부 최신 메일 시스템에서는 두 자리 날짜를 더 이상 받아들이지 않습니다.

---

**주**            두 형식을 모두 처리할 수 없는 시스템은 표준 위반입니다.

---

`datefour` 및 `datetwo` 키워드는 메일 헤더 날짜에서 MTA의 연도 필드 처리를 제어합니다. 기본값인 `datefour` 키워드는 모든 연도 필드를 네 자리로 확장하도록 MTA에 지시합니다. 50보다 작은 두 자리 날짜에는 2000이 추가되고 50보다 큰 값에는 1900이 추가됩니다.

---

**주의**            `datetwo` 키워드는 네 자리 날짜에서 앞의 두 자리를 제거하도록 MTA에 지시합니다. 이 키워드는 두 자리 날짜를 필요로 하는 호환되지 않는 메일 시스템과 호환성을 제공하기 위한 것입니다. 이외의 다른 목적으로 사용해서는 안 됩니다.

---

## 날짜의 요일 지정

키워드: `dayofweek`, `nodayofweek`

RFC 822 사양은 메일 헤더의 날짜 필드에서 선행 요일 사양에 허용됩니다. 요일 정보를 적용할 수 없는 시스템도 있습니다. 따라서 요일 정보를 헤더에 표시하면 매우 유용하기는 하지만 일부 시스템에서는 이 정보를 포함하기를 꺼리게 됩니다.

dayofweek 및 nodayofweek 키워드는 MTA의 요일 정보 처리를 제어합니다. 기본값인 dayofweek 키워드는 요일 정보를 유지하고 날짜 및 시간 헤더에 이 정보를 추가(없는 경우)하도록 MTA에 지시합니다.

---

**주의** nodayofweek 키워드는 날짜 및 시간 헤더에서 선행 요일 정보를 제거하도록 MTA에 지시합니다. 이 키워드는 이 정보를 제대로 처리할 수 없는 호환되지 않는 메일 시스템과 호환성을 제공하기 위한 것입니다. 이외의 다른 목적으로 사용해서는 안 됩니다.

---

## 긴 헤더 행 자동 분할

키워드: maxheaderaddrs, maxheaderchars

일부 메일 전송 프로그램 특히, 일부 sendmail 구현에서는 긴 헤더 행을 제대로 처리할 수 없습니다. 이로 인해 헤더가 손상되지는 않지만 잘못된 메일 거부를 초래할 수 있습니다. 이는 총체적인 표준 위반이지만 일반적인 문제이기도 합니다.

MTA는 긴 헤더 행을 독립된 여러 헤더 행으로 분할하기 위한 채널 단위 기능을 제공합니다. maxheaderaddrs 키워드는 한 행에 표시할 수 있는 주소 수를 제어합니다.

maxheaderchars 키워드는 한 행에 표시할 수 있는 문자 수를 제어합니다. 두 키워드 모두 연관된 제한을 지정하는 단일 정수 매개 변수를 필요로 합니다. 기본적으로 헤더 행의 길이와 표시할 수 있는 주소 수에는 제한이 적용되지 않습니다.

## 헤더 맞춤 및 접기

키워드: headerlabelalign, headerlinelength

`headerlabelalign` 키워드는 이 채널의 대기열에 포함된 메일 헤더에 대한 맞춤 점을 제어합니다. 맞춤 점은 정수 값 인수를 가집니다. 맞춤 점은 헤더 내용이 정렬되는 여백입니다. 예를 들어, 맞춤 점이 10인 샘플 헤더 행의 모양은 다음과 같습니다.

```
To:      joe@siroe.com
From:    mary@siroe.com
Subject: Alignment test
```

기본 `headerlabelalign`은 0이고 헤더가 정렬되지 않습니다. `headerlinelength` 키워드는 이 채널의 대기열에 포함된 메일 헤더 행의 길이를 제어합니다. 이 키워드보다 더 긴 행은 RFC 822 접기 규칙에 따라 접힙니다.

이러한 키워드는 메일 대기열에 있는 메일 헤더의 형식만 제어합니다. 헤더의 실제 디스플레이는 일반적으로 사용자 에이전트에 의해 제어됩니다. 또한, 인터넷을 통해 전송할 경우 일반적으로 헤더의 형식이 다시 지정되기 때문에 이러한 키워드는 메일 헤더의 형식을 다시 지정하지 못하는 단순 사용자 에이전트와 함께 사용하더라도 가시적인 효과가 없을 수 있습니다.

## 최대 길이 헤더 지정

키워드: `maxprocchars`

많은 주소를 포함하는 긴 헤더 행을 처리하려면 많은 시스템 자원을 사용할 수 있습니다. `maxprocchars` 키워드는 MTA가 처리하고 다시 쓸 수 있는 최대 길이 헤더를 지정하는데 사용됩니다. 이 키워드보다 더 긴 헤더를 지닌 메일도 허용되고 전달됩니다. 긴 헤더 행을 어떠한 식으로도 다시 쓰지 않는다는 점만 차이가 납니다. 단일 정수 인수가 필요하며 기본값은 모든 길이의 헤더를 처리합니다.

## 민감도 검사

키워드: `sensitivitynormal`, `sensitivitypersonal`, `sensitivityprivate`, `sensitivitycompanyconfidential`

민감도 검사 키워드는 채널에 허용될 수 있는 메일 민감도에 대한 최대값을 설정합니다. 기본값은 `sensitivitycompanyconfidential`이며 모든 민감도의 메일이 허용됩니다. `Sensitivity`: 헤더가 없는 메일은 보통(가장 낮은 민감도)으로 간주됩니다. 그런 키워드에 의해 지정된 것보다 더 높은 민감도를 갖는 메일은 채널의 대기열에 포함되면 거부되고 다음과 같은 오류 메시지가 표시됩니다.

```
message too sensitive for one or more paths used
```

MTA는 이러한 민감도 검사를 수신자 단위가 아니라 메일 단위로 수행합니다. 한 수신자의 대상 채널에서 민감도 검사에 실패할 경우 해당 메일은 해당 민감도 채널에 연결된 수신자뿐만 아니라 모든 수신자에게 전달됩니다.

## 헤더의 기본 언어 설정

키워드: `language`

헤더의 인코딩된 단어는 특정 언어를 가질 수 있습니다. `language` 키워드는 기본 언어를 지정합니다.

## 첨부 파일 및 MIME 처리

이 절에서는 첨부 파일 및 MIME 처리를 수행하는 키워드에 대해 설명합니다. 이 장은 다음 내용으로 구성되어 있습니다.

- 384페이지의 "Encoding: 헤더 행 무시"
- 385페이지의 "메일/부분 메일 자동 조각 모음"
- 386페이지의 "대용량 메일 자동 조각화"
- 387페이지의 "메일 행 길이 제한 적용"

## Encoding: 헤더 행 무시

키워드: `ignoreencoding`, `interpretencoding`



MTA는 `yes CHARSET-CONVERSION`을 사용하여 다양한 비표준 메일 형식을 MIME으로 변환할 수 있습니다. 특히, RFC 1154 형식에서는 비표준 `Encoding:` 헤더 행을 사용할 수 있습니다. 일부 게이트웨이에서는 이 헤더 행에 잘못된 정보를 생성하므로 이러한 헤더 행을 무시해야 할 경우도 종종 있습니다. `ignoreencoding` 키워드는 `Encoding:` 헤더 행을 무시하도록 MTA에 지시합니다.

---

**주** MTA에 `CHARSET-CONVERSION`이 사용되지 않는 경우 이러한 헤더는 항상 무시됩니다. `interpretencoding` 키워드가 기본값이며 이 키워드는 `Encoding:` 헤더 행에 주의하도록 MTA에 지시합니다(다르게 지시되지 않을 경우).

---

## 메일/부분 메일 자동 조각 모음

키워드: `defragment`, `nodefragment`

MIME 표준은 메일을 더 작은 여러 부분으로 분할하기 위한 메일/부분 내용 유형을 제공합니다. 이 기능은 크기 제한이 있는 네트워크를 선회하거나 메일 조각화에서 "검사점 지정" 형식을 제공할 수 있는 불안정한 네트워크를 선회해야 하는 경우에 유용합니다. 그렇게 하면 메일 전송 중에 네트워크 오류가 발생하더라도 중복된 작업을 줄일 수 있습니다. 메일이 대상에 도착한 이후에 자동으로 다시 어셈블할 수 있도록 각 부분에 정보가 포함됩니다.

`defragment` 채널 키워드 및 조각 모음 채널을 사용하여 MTA에서 메일을 다시 어셈블할 수 있습니다. 채널에 `defragment` 표시가 있는 경우 채널의 대기열에 포함된 부분 메일이 조각 모음 채널 대기열에 대신 포함됩니다. 모든 부분이 도착하면 메일이 다시 작성되어 대상 위치로 보내집니다. `nodefragment`는 이 특수 처리를 사용하지 않습니다. 기본값은 `nodefragment` 키워드입니다.

### 조각 모음 채널 보존 시간

메일은 제한된 시간 동안만 조각 모음 채널 대기열에 보존됩니다. 첫 번째 배달 실패 알림을 보내도록 지정된 시간의 1/2이 경과하면 메일의 다양한 부분을 다시 어셈블하지 않고 보냅니다. 이 시간 값 선택은 조각 모음 채널 대기열의 메일에 대한 배달 실패 알림을 보내지 않게 합니다.

notices 채널 키워드는 배달 실패 알림을 보내기 전에 경과할 수 있는 시간을 제어하며, 부분적으로 보내기 전에 메일이 보존되는 시간을 제어합니다. notices 키워드 값을 가능한 조각 모음에 대해 메일을 보존하려는 시간의 2배로 설정합니다. 예를 들어, notices 값을 4로 설정하면 메일 조각 모음이 2일 동안 보존됩니다.

```
defragment notices 4
DEFRAGMENT-DAEMON
```

## 대용량 메일 자동 조각화

키워드: maxblocks, maxlines

일부 메일 시스템 또는 네트워크 전송 프로그램은 특정 크기 제한을 초과하는 메일을 처리할 수 없습니다. MTA는 채널 단위로 제한을 적용하는 기능을 제공합니다. 설정된 제한보다 큰 메일은 여러 개의 작은 메일로 자동으로 분할(조각화)됩니다. 그런 조각화에 사용되는 내용 유형은 message/partial이며, 동일한 메일의 각 부분이 서로 연결된 다음 받는 메일 프로그램에 의해 자동으로 다시 어셈블되도록 고유한 아이디 매개 변수가 추가됩니다.

maxblocks 및 maxlines 키워드는 자동 조각화가 활성화되는 크기 제한을 적용하는 데 사용됩니다. 이 두 키워드의 뒤에는 단일의 정수 값이 있어야 합니다. maxblocks 키워드는 메일에 허용되는 최대 블록 수를 지정합니다. MTA 블록은 일반적으로 1024바이트이지만 MTA 옵션 파일의 BLOCK\_SIZE 옵션으로 변경할 수 있습니다. maxlines 키워드는 메일에 허용되는 최대 행 수를 지정합니다. 필요한 경우 이 두 제한을 동시에 적용할 수 있습니다.

메일 헤더는 메일 크기에 어느 정도까지는 포함됩니다. 메일 헤더는 여러 메일로 분할될 수 없고 지정된 크기 제한을 초과할 수 없기 때문에 메일 헤더 크기에는 매우 복잡한 기법이 사용됩니다. 이 논리는 MTA 옵션 파일의 MAX\_HEADER\_BLOCK\_USE 및 MAX\_HEADER\_LINE\_USE 옵션에 의해 제어됩니다.

MAX\_HEADER\_BLOCK\_USE는 0과 1 사이의 실수를 지정하는 데 사용되며 기본값은 0.5입니다. 메일 헤더는 메일이 사용할 수 있는 총 블록 수(maxblocks 키워드에 의해 지정)만큼을 차지할 수 있습니다. 메일 헤더가 긴 경우 MTA는 MAX\_HEADER\_BLOCK\_USE 및 maxblocks를 헤더(헤더 크기는 실제 헤더 크기와 maxblocks 중 더 작은 부분임) \* MAX\_HEADER\_BLOCK\_USE의 크기로 생성합니다.

예를 들어, `maxblocks`가 10이고 `MAX_HEADER_BLOCK_USE`가 기본값 0.5인 경우 5블록보다 더 큰 메일 헤더는 5블록 헤더로 취급되고, 메일의 크기가 5블록 이하일 경우 조각화되지 않습니다. 값이 0인 경우에는 헤더가 메일 크기 제한에서 무시됩니다.

값이 1인 경우 헤더에 사용 가능한 최대 크기까지 사용할 수 있습니다. 각 조각은 제한을 초과하는지 여부에 관계 없이 항상 메일 내용의 한 행 이상을 포함하고 있어야 합니다.

`MAX_HEADER_LINE_USE`는 `maxlines` 키워드와 비슷한 방식으로 동작합니다.

## 메일 행 길이 제한 적용

키워드: `linelength`

SMTP 사양은 최대 1,000바이트를 포함하는 텍스트 행에 사용할 수 있습니다. 보다 엄격한 행 길이 제한이 적용되는 전송 프로그램도 있습니다. `linelength` 키워드는 채널 단위로 최대 허용 가능한 메일 행 길이를 제한하는 기법을 제공합니다. 지정된 채널의 대기열에 포함되고 행 길이가 해당 채널에 지정된 제한보다 더 긴 메일은 자동으로 인코딩됩니다.

MTA에서 사용할 수 있는 다양한 인코딩은 항상 행 길이를 80자 미만으로 줄입니다. 그런 인코딩을 수행한 후 해당 디코딩 필터를 적용하여 원본 메일을 복구할 수 있습니다.

---

**주**            인코딩은 행 길이를 80자 미만으로 줄일 수만 있습니다. 80자 미만의 행 길이가 값을 지정하면 명시된 제한에 맞는 길이의 행이 생성되지 않을 수 있습니다.

---

`linelength` 키워드는 전송을 위해 데이터 인코딩에서 "소프트" 줄 바꿈을 수행하게 합니다. 인코딩은 일반적으로 수신하는 쪽에서 디코딩하여 원래의 "긴" 행을 복구합니다. "하드" 줄 바꿈에 대한 자세한 내용은 "레코드, 텍스트" `CHARSET-CONVERSION`을 참조하십시오.

## 메일, 할당량, 수신자 및 인증 시도의 제한

이 절에서는 메일 크기 제한, 사용자 할당량 및 권한을 설정하는 키워드에 대해 설명합니다. 이 절은 다음 내용으로 구성되어 있습니다.

- 388페이지의 "성공하지 못한 인증 시도에 대한 제한"
- 388페이지의 "절대 메일 크기 제한 지정"
- 389페이지의 "크기 제한 또는 수신자 수 제한을 초과하는 메일 대상 다시 지정"
- 391페이지의 "할당량 사용자에게 대한 메일 전달 처리"
- 392페이지의 "1000자가 넘는 행이 있는 SMTP 메일 처리"
- 392페이지의 "일반 및 Filename Content-type 및 Content-disposition 매개 변수의 길이 제어"
- 392페이지의 "메일 수신자 제한"
- 393페이지의 "헤더 크기 제한"

## 성공하지 못한 인증 시도에 대한 제한

키워드: `disconnectbandauthlimit`

이 키워드는 세션의 연결이 끊어지기 전에 세션에 허용되는 인증 시도의 실패 횟수를 제한하는 데 사용할 수 있습니다. 이 옵션의 기본값은 3입니다.

## 절대 메일 크기 제한 지정

키워드: `blocklimit`, `noblocklimit`, `linelimit`, `nolinelimit`, `sourceblocklimit`

조각화를 사용하면 메일을 작은 여러 조각으로 자동으로 분할할 수 있지만 관리상의 목적(예: 서비스 거부 공격 방지)으로 정의한 제한보다 더 큰 메일은 거부하는 것이 좋은 경우도 있습니다.

`blocklimit`, `linelimit` 및 `sourceblocklimit` 키워드는 절대 크기 제한을 적용하는 데 사용됩니다. 각 키워드의 뒤에는 단일의 정수 값이 있어야 합니다.

`blocklimit` 키워드는 메일에 허용되는 최대 블록 수를 지정합니다. MTA는 이 값보다 더 많은 블록을 포함하는 메일을 채널의 대기열에 넣으려는 시도를 거부합니다. MTA 블록은 일반적으로 1024바이트이지만 MTA 옵션 파일의 `BLOCK_SIZE` 옵션으로 변경할 수 있습니다.

sourceblocklimit 키워드는 받는 메일에 허용되는 최대 블록 수를 지정합니다. MTA는 이 값보다 더 많은 블록을 포함하는 메일을 채널에 제출하려는 시도를 거부합니다. 다시 말해서 blocklimit는 대상 채널에 적용되고 sourceblocklimit는 소스 채널에 적용됩니다. MTA 블록은 일반적으로 1024바이트이지만 MTA 옵션 파일의 BLOCK\_SIZE 옵션으로 변경할 수 있습니다.

사용자 LDAP 속성을 MTA 옵션 LDAP\_SOURCEBLOCKLIMIT에 지정하고 이 속성을 보낸 사람의 LDAP 항목에 추가하여 보낸 사람 단위로 소스 블록 제한을 지정할 수도 있습니다. 또한 소스 블록 제한이 보낸 사람의 도메인을 기반으로 지원되기도 합니다. 도메인 LDAP 속성을 MTA 옵션 LDAP\_DOMAIN\_ATTR\_SOURCEBLOCKLIMIT에 지정하고 이 속성을 보낸 사람의 도메인 LDAP 항목에 추가합니다. 이러한 값은 모두 기본값이 없습니다.

linelimit 키워드는 메일에 허용되는 최대 행 수를 지정합니다. MTA는 이 행 수보다 더 많은 행을 포함하는 메일을 채널의 대기열에 넣으려는 시도를 거부합니다. 필요한 경우 blocklimit 키워드와 linelimit 키워드를 동시에 적용할 수 있습니다.

MTA 옵션 LINE\_LIMIT 및 BLOCK\_LIMIT를 사용하여 모든 채널에 비슷한 제한을 적용할 수 있습니다. 이러한 제한은 모든 채널에 적용할 수 있다는 장점이 있습니다. 따라서 MTA 서버는 메일 수신자 정보를 가져오기 전에 해당 제한을 메일 클라이언트에게 알릴 수 있습니다. 이 기능은 일부 프로토콜에서 메일 거부 프로세스를 단순화합니다.

기본값은 nolinelimit 및 noblocklimit 채널 키워드이며 제한이 적용되지 않음을 의미합니다. 전역 제한은 LINE\_LIMIT 또는 BLOCK\_LIMIT MTA 옵션을 통해 적용됩니다.

## 크기 제한 또는 수신자 수 제한을 초과하는 메일 대상 다시 지정

키워드: alternatechannel, alternateblocklimit, alternatelinelimit, alternaterecipientlimit

MTA는 수신자 수, 메일 크기, 메일 행 수 등에 대한 지정된 제한을 초과하는 메일의 대상을 대체 대상 채널로 다시 지정하는 기능을 제공합니다. 이 기능은 대상 채널에 포함될 수 있는 alternatechannel, alternateblocklimit, alternatelinelimit 및 alternaterecipientlimit 채널 키워드 집합으로 구현됩니다. alternatechannel 키워드는 사용할 대체 채널의 이름을 지정하는 단일 인수를 가집니다. 다른 키워드는 각각 해당 임계값을 지정하는 정수 인수를 갖습니다. 이러한 임계값을 초과하는 메일은 원본 대상 채널 대신 대체 채널의 대기열에 포함됩니다.

다음 채널 블록 예에서는 인터넷의 `tcp_local` 채널로 이동해야 하는 5,000개 이상의 블록을 가진 대용량 메일이 `tcp_big` 채널로 대신 이동됩니다.

```
tcp_local smtp ... rest of keywords ... alternatechannel tcp_big
alternateblocklimit 5
tcp-daemon
```

```
tcp_big smtp ...rest of keywords...
tcp-big-daemon
```

다음 예는 `alternate*` 채널 키워드를 사용하는 방법을 보여 줍니다.

- 대용량 메일을 지연된 시간이나 한가한 시간에 전달하려면 `alternatechannel`(예: `tcp_big`)이 실행되는 시간을 제어할 수 있습니다.

한 가지 방법은 `imsimta qm` 유틸리티의 `STOP channel_name` 및 `START channel_name` 명령을 사용하는 것입니다. 이러한 명령은 **Job Controller**가 실행하는 사용자 정의 정기 작업 또는 `cron` 작업을 통해 주기적으로 실행됩니다.

- **Job Controller**가 대용량 메일이나 많은 수신자를 갖는 메일을 자체 풀에서 처리하려면 `alternatechannel`을 사용할 수도 있습니다.

대용량 메일이나 많은 수신자를 갖는 메일은 원격 **SMTP** 서버에서 처리하고 받는 데 더 많은 시간이 걸리기 때문에 대용량 메일이 작은 메일의 전달을 지연하지 않도록 작은 메일이나 수신자가 적은 메일을 그러한 메일과 구분할 수 있습니다.

**Job Controller**의 정기 메일 일정 예약 및 스레드 및 프로세스에 대한 메일 할당 작업은 대부분의 구성에서 허용됩니다.

- 대용량 메일 또는 수신자가 많은 메일에 대한 특수 **TCP/IP** 채널 시간 초과 값을 설정하려면 `alternatechannel`을 사용할 수 있습니다.

특히, 특수 **TCP/IP** 채널 시간 초과 값 설정은 대용량 메일 또는 수신자가 많은 메일을 받는 데 지나치게 많은 시간이 걸리는 원격 호스트에 메일을 보내려는 경우에 유용할 수 있습니다.

대부분의 구성에서는 기본 자동 시간 초과 조정으로 충분합니다. 사용자는 기본값에서 값을 조정할 수만 있고 특수 채널은 사용할 수 없습니다. **Messaging Server Reference Manual**의 `STATUS_DATA_RECV_PER_ADDR_TIME` 및 `STATUS_DATA_RECV_PER_BLOCK_TIME` 채널 옵션을 참조하십시오.

- 매우 긴 메일에 대해 특수 MIME 메일 조각화를 수행하려면 `alternatechannel` 및 `alternateblocklimit` 채널 키워드를 `maxblocks` 채널 키워드와 함께 사용할 수 있습니다.

일반적으로 지정한 크기를 넘는 메일을 조각화하려면 일반 아웃바운드 TCP/IP 채널에 원하는 `maxblocks` 크기를 입력합니다. `maxblocks` 채널 키워드는 조각화를 수행하는 임계값이자 조각을 만들 크기입니다.

더 큰 임계값을 트리거하고 더 작은 조각을 만들려면 아웃바운드 TCP/IP 채널에서 `alternatechannel` 및 `alternateblocklimit`를 사용할 수 있습니다. 그런 다음 대체 채널에서 `maxblock` 크기를 사용하여 특정 크기를 넘는 메일을 조각화할 수 있습니다.

- `alternatechannel`을 특수 필터링과 함께 사용할 수 있습니다. 예를 들어, 수신자가 많은 메일은 스팸인 경우 내용을 보다 주의깊게 조사해야 합니다. 보내는 채널을 기준으로 서로 다른 필터링을 수행할 수 있습니다(*Sun Java System Messaging Server Administration Reference*의 `destinationfilter` 채널 키워드 참조).

변환 채널을 통해 상대적으로 자원을 많이 사용하는 스캔(예: 바이러스 필터링)을 수행할 경우 매우 큰 메일에서 자원 문제가 발생할 수 있습니다. 대체 변환 채널을 사용할 수 있습니다. 또는 보내는 채널을 기준으로 일반 변환 채널 내에서 특수 변환 절차를 수행할 수 있습니다.

- 대용량의 보내는 메일을 자체 채널로 보내려면 `alternatechannel`을 사용하여 `mail.log*` 파일 분석 또는 카운터 표시에서 제외할 수 있습니다.

또한, 전달 통계를 주의깊게 분석할 경우 자체 채널에서 대용량 메일을 처리하는 것이 좋습니다. 원격 SMTP 호스트에 보내는 대용량 메일이나 수신자가 많은 메일은 처리를 완료하는 데 더 많은 시간이 걸리므로 대용량 메일에 대해서는 일반 메일과 다른 전달 통계를 생성하기 때문입니다.

## 할당량 사용자에 대한 메일 전달 처리

키워드: `holdexquota`, `noexquota`

noexquota 및 holdexquota 키워드는 디스크 할당량이 초과된 Berkeley 메일함 사용자 (UNIX) 즉, uid 대체 채널에 전달되는 사용자로 주소가 지정된 메일의 처리를 제어합니다.

noexquota는 할당량을 초과한 사용자에게 보내는 메일을 메일 발송자에게 반환하도록 MTA에 지시합니다. holdexquota는 할당량을 초과한 사용자에게 보내는 메일을 보관하도록 MTA에 지시합니다. 그런 메일은 전달이 가능할 때까지 또는 시간이 초과되어 메일 반환 작업에 의해 보낸 사람에게 반환될 때까지 MTA 대기열에 남아 있습니다.

## 1000자가 넘는 행이 있는 SMTP 메일 처리

키워드: rejectsmtplonglines, wrapsmtplonglines, truncatesmtplonglines

rejectsmtplonglines는 SMTP에서 허용되는 1000자(CRLF 포함)보다 긴 행이 포함된 메일을 거부하는 옵션을 추가합니다. 이 영역의 다른 옵션에는 아주 긴 행을 줄 바꿈하는 wrapsmtplonglines, 아주 긴 행을 자르는 truncatesmtplonglines 등이 있습니다. 이러한 키워드는 둘 다 제출에 사용되는 초기 채널(예: tcp\_local)에 적용해야 합니다. 이후에 전환되는 채널에는 영향을 주지 않습니다.

## 일반 및 Filename Content-type 및 Content-disposition 매개 변수의 길이 제어

키워드: parameterlengthlimit 및 nameparameterlengthlimit

parameterlengthlimit는 일반 content-type 및 content-disposition 매개 변수가 잘리는 지점을 제어합니다. 기본값은 1024입니다. nameparameterlengthlimit는 name content-type 및 filename content-disposition 매개 변수가 잘리는 지점을 제어합니다. 기본값은 128입니다. 메일에서 MIME 처리가 수행되지 않을 경우 가장 외부에 있는 메일 헤더만 처리됩니다. MIME 처리는 inner 키워드나 문자 세트 변환 사용 등과 같은 다양한 방법으로 사용 가능하게 할 수 있습니다.

## 메일 수신자 제한

키워드: recipientlimit 및 recipientcutoff



`recipientlimit`는 메일에 대해 허용할 총 수신자 주소 수를 지정합니다. `recipientcutoff`는 MTA에 제공된 수신자의 총 수를 지정된 값과 비교합니다. 이 값이 지정된 제한을 초과하면 메일 전달이 허용되지 않습니다. 두 키워드는 모두 단일 정수 인수를 가집니다. 해당 채널 키워드를 지정하지 않은 경우 두 키워드의 기본값은 제한이 없습니다.

보낸 사람이나 보낸 사람의 도메인에 수신자 제한을 설정할 수도 있습니다. 이렇게 하려면 적절한 MTA 옵션(`LDAP_RECIPIENTLIMIT`, `LDAP_RECIPIENTCUTOFF`, `LDAP_DOMAIN_ATTR_RECIPIENTLIMIT`, `LDAP_DOMAIN_ATTR_RECIPIENTCUTOFF`)에 사용자 또는 도메인 LDAP 속성을 지정하고 해당 속성을 보낸 사람의 사용자 항목이나 도메인 항목에 추가합니다.

## 헤더 크기 제한

키워드: `headerlimit`

가장 외부에 있는 주 메일 헤더의 최대 크기에 제한을 부과합니다. 주 메일 헤더가 지정된 한계에 이르면 자동으로 잘립니다. 전역 MTA 옵션 `HEADER_LIMIT`를 설정하면 이 옵션이 이러한 채널 수준 제한을 대체합니다. 기본값은 제한 없음입니다.

# MTA 대기열에서 파일 만들기

이 절에서는 MTA 대기열에서 파일 만들기를 지정하여 디스크 자원을 제어할 수 있는 키워드에 대해 설명합니다. 이 절은 다음 내용으로 구성되어 있습니다.

- [393페이지의 "메일의 여러 주소 처리 방법 제어"](#)
- [394페이지의 "여러 하위 디렉토리로 채널 메일 대기열 분산"](#)

## 메일의 여러 주소 처리 방법 제어

키워드: `multiple`, `addrsperfile`, `single`, `single_sys`

MTA에서는 대기열에 포함된 각 메일에 여러 대상 주소를 표시할 수 있습니다. 일부 채널 프로그램은 수신자가 한 명이거나, 수신자의 수가 제한되었거나, 메일 복사본당 하나의 대상 시스템이 있는 메일만 처리할 수 있습니다. 예를 들어, SMTP 채널 마스터 프로그램은 지정된 트랜잭션에 있는 단일 원격 호스트에 대해서만 연결을 설정하기 때문에 해당 호스트의 주소만 처리할 수 있습니다. 그럼에도 불구하고 모든 SMTP 트래픽에 단일 채널이 일반적으로 사용됩니다.

또 다른 예로 일부 SMTP 서버는 한 번에 처리할 수 있는 수신자 수에 대한 제한을 적용할 수 있지만 이 오류 유형을 처리할 수 없습니다.

`multiple`, `addrsperfile`, `single` 및 `single_sys` 키워드를 사용하여 여러 주소를 처리하는 방법을 제어할 수 있습니다. `single` 키워드는 채널의 각 대상 주소에 대해 별도의 메일 복사본을 만들어야 함을 의미합니다. `single_sys` 키워드는 사용된 각 대상 시스템에 대해 단일의 메일 복사본을 만듭니다. 기본값인 `multiple` 키워드는 전체 채널에 대해 단일의 메일 복사본을 만듭니다.

---

**주**            사용된 키워드에 관계 없이 메일이 대기열에 있는 각 채널에 대해 해당 메일 복사본을 하나 이상 만듭니다.

---

`addrsperfile` 키워드는 채널 대기열의 단일 메일 파일에 연결될 수 있는 최대 수신자 수에 대한 제한을 적용하여 단일 작업에서 처리되는 수신자 수를 제한하는 데 사용됩니다. 이 키워드에는 메일 파일에 허용되는 최대 수신자 주소 수를 지정하는 단일의 정수 인수가 필요합니다. 이 수에 도달하면 MTA는 자동으로 추가 메일 파일을 생성하여 해당 주소를 수용합니다. 기본 `multiple` 키워드는 일반적으로 메일 파일에 수신자 수 제한을 적용하지 않습니다. SMTP 채널의 기본값은 99입니다.

## 여러 하위 디렉토리로 채널 메일 대기열 분산

키워드: `subdirs`

기본적으로 채널의 대기열에 포함된 모든 메일은 `/imta/queue/channel-name` 디렉토리에 파일로 저장됩니다. 여기서 `channel-name`은 채널의 이름입니다. 그러나, 많은 수의 메일을 처리하고 처리 대기 중에 대용량 메일 파일 저장소를 생성하는 채널(예: TCP/IP 채널)의 경우 해당 메일 파일을 여러 하위 디렉토리로 분산하여 파일 시스템의 성능을 향상시킬 수 있습니다. `subdirs` 채널 키워드의 뒤에는 채널에 대한 메일을 분산할 하위 디렉토리의 수를 지정하는 정수가 와야 합니다. 예를 들면 다음과 같습니다.

```
tcp_local single_sys smtp subdirs 10
```

## 세션 제한 설정

키워드: `disconnectbadcommandlimit`, `disconnectrecipientlimit`,  
`disconnectrejectlimit`, `disconnecttransactionlimit`

네 개의 새로운 채널 키워드는 일정한 수의 오류가 감지된 후에 SMTP 서버가 클라이언트와의 연결을 끊을 수 있는 기능을 제공합니다.

`disconnectrecipientlimit` - 세션 수신자의 수를 제한합니다.

`disconnectrejectlimit` - 거부된 수신자의 수를 제한합니다.

`disconnecttransactionlimit` - 트랜잭션 수를 제한합니다.

`disconnectbadcommandlimit` - 잘못된 명령의 수를 제한합니다.

이러한 키워드는 모두 세션 제한입니다. `disconnectbadcommandlimit`를 제외하고 이러한 제한은 모두 MAIL FROM 또는 RSET 명령이 실행될 때 확인됩니다. 이러한 제한 중 하나라도 초과하면 서버는 4xy 오류를 표시하고 연결을 끊습니다. 잘못된 명령 제한은 잘못된 명령이 실행될 때 확인된다는 점만 다릅니다.

## 로깅 및 디버깅 구성

이 절에서는 로깅 및 디버깅 키워드에 대해 설명합니다.

- [395페이지의 "로깅 키워드"](#)
- [396페이지의 "디버깅 키워드"](#)
- [396페이지의 "Loopcheck 설정"](#)

## 로깅 키워드

키워드: `logging`, `nologging`, `logheader`

MTA는 대기열에 포함될 때와 대기열에서 제거될 때 각 메일을 로깅하는 기능을 제공합니다. `logging` 및 `nologging` 키워드는 메일 로깅을 채널 단위로 제어합니다. 기본적으로 초기 구성에서는 모든 채널에 대해 로깅을 설정합니다. 채널 정의에서 `nologging` 키워드를 대체하여 특정 채널에 대해 로깅을 비활성화할 수 있습니다.

`logheader`는 채널 단위로 `LOG_HEADER` MTA 옵션을 무시합니다. 기본값인 0은 메일 헤더 로깅을 사용하지 않도록 설정합니다. 자세한 내용은 *Sun Java System Messaging Server Administration Reference*를 참조하십시오.

로깅에 대한 자세한 내용은 [21장, "로깅 관리"](#)를 참조하십시오.

## 디버깅 키워드

키워드: `master_debug`, `slave_debug`, `nomaster_debug`, `noslave_debug`

일부 채널 프로그램에는 추가 진단 출력을 생성하여 디버깅을 도와주는 선택 코드가 포함되어 있습니다. 채널 단위로 이 디버깅 출력을 생성하는 데 사용하는 두 채널 키워드가 제공됩니다. 마스터 프로그램에서 디버깅 출력을 생성하는 `master_debug` 키워드와 슬레이브 프로그램에서 디버깅 출력을 생성하는 `slave_debug` 키워드입니다.

`nomaster_debug` 및 `noslave_debug`에 따라 두 개 디버깅 출력 유형은 기본적으로 사용되지 않습니다.

활성화된 디버깅 출력은 채널 프로그램과 연결된 로그 파일에서 끝납니다. 로그 파일의 위치는 프로그램에 따라 다릅니다. 로그 파일은 일반적으로 로그 디렉토리에 보관됩니다. 마스터 프로그램의 로그 파일 이름은 일반적으로 `x_master.log` 형식입니다. 여기서 `x`는 채널 이름입니다. 슬레이브 프로그램의 로그 파일 이름은 일반적으로 `x_slave.log` 형식입니다.

UNIX에서 1 채널에 대해 `master_debug` 및 `slave_debug`를 활성화하면 MTA 디버그 정보가 들어 있는 현재 디렉토리(디렉토리에 쓰기 권한이 있는 경우, 쓰기 권한이 없는 경우 디버그 출력이 `stdout`으로 이동됨)에 `imta_sendmail.log-uniqueid` 파일이 생성됩니다.

## Loopcheck 설정

키워드: `loopcheck`, `noloopcheck`

`loopcheck` 키워드는 MTA가 자체적으로 통신하는지 확인하도록 SMTP EHLO 응답 배너에 문자열을 넣습니다. `loopcheck`를 설정하면 SMTP 서버가 XLOOP 확장을 광고합니다.

XLOOP를 지원하는 SMTP 서버와 통신할 때 MTA의 SMTP 클라이언트는 광고된 문자열을 MTA 값과 비교하고 클라이언트가 실제로 SMTP 서버와 통신 중인 경우 메일을 즉시 바운스합니다.

## 기타 키워드

이 절에서는 기타 키워드에 대해 설명합니다. 이 절은 다음 내용으로 구성되어 있습니다.

- 397페이지의 "채널 작업 유형"
- 398페이지의 "파이프 채널"
- 398페이지의 "메일함 필터 파일 위치 지정"
- 399페이지의 "스팸 필터 키워드"
- 399페이지의 "주소 검증 후와 확장 전의 라우팅"
- 403페이지의 "NO-SOLICIT SMTP 확장 지원"
- 403페이지의 "잘못된 RCPT TO: 주소에 대한 제한 설정"

## 프로세스 채널 대체

키워드: `notificationchannel`, `dispositionchannel`

이러한 키워드는 각각 초기에 전달 상태 알림(DSN) 및 MDN(Message Disposition Notification)을 대기열에 포함하기 위한 장소로 프로세스 채널을 대체합니다. 명명된 채널이 없으면 Messaging Server는 다시 프로세스 채널을 사용합니다.

`notificationchannel`은 초기에 전달 상태 알림(DSN)을 대기열에 포함하기 위한 장소로 프로세스 채널을 대체합니다. 명명된 채널이 없으면 Messaging Server는 다시 프로세스 채널을 사용합니다.

`dispositionchannel`은 초기에 MDN(Message Disposition Notification)을 대기열에 포함하기 위한 장소로 프로세스 채널을 대체합니다. 명명된 채널이 없으면 Messaging Server는 다시 프로세스 채널을 사용합니다.

## 채널 작업 유형

키워드: `submit`

Messaging Server는 RFC 2476의 메일 제출 프로토콜을 지원합니다. `submit` 키워드를 사용하여 채널을 제출 전용 채널로 표시할 수 있습니다. 이 키워드는 SMTP 서버가 메일 제출 전용으로 사용되는 특수 포트에서 실행하는 대부분의 TCP/IP 채널에 유용합니다. RFC 2476은 포트 587을 이러한 메일 제출용으로 사용하도록 구성합니다.

## 파이프 채널

키워드: `user`

`user` 키워드는 파이프 채널에서 실행할 아이디를 나타내는 데 사용됩니다.

`user`에 대한 인수는 일반적으로 소문자로 사용되지만 인수가 따옴표로 묶여 있는 경우 원래의 문자가 그대로 유지됩니다.

## 메일함 필터 파일 위치 지정

키워드: `filter`, `nofilter`, `channelfilter`, `nochannelfilter`, `destinationfilter`, `nodestinationfilter`, `sourcefilter`, `nosourcefilter`, `fileinto`, `nofileinto`)

`filter` 키워드는 원시 및 `ims-ms` 채널에서 해당 채널에 대한 사용자 필터 파일의 위치를 지정하는 데 사용됩니다. 이 키워드는 필터 파일 위치를 설명하는 필수 URL 인수를 가집니다. 기본값은 `nofilter`이며 해당 채널에 대해 사용자 메일함 필터가 사용되지 않음을 의미합니다.

`sourcefilter` 및 `destinationfilter` 키워드는 일반 MTA 채널에서 받는 메일과 보내는 메일 각각에 적용할 채널 수준 필터를 지정하는 데 사용할 수 있습니다. 이러한 키워드는 채널 필터 위치를 설명하는 필수 URL 인수를 가집니다. 기본값은 `nosourcefilter` 및 `nodestinationfilter`이고 어느 채널 방향에 대해서도 채널 메일함 필터를 사용하지 않음을 의미합니다.

이전의 `channelfilter` 및 `nochannelfilter` 키워드는 각각 `destinationfilter` 및 `nodestinationfilter`의 동의어입니다.

현재 `ims-ms` 채널과 LMTP 채널에서만 지원되는 `fileinto` 키워드는 메일함 필터 `fileinto` 연산자를 적용할 때 주소를 변경하는 방법을 지정합니다. `ims-ms` 채널에서의 일반적인 사용법은 다음과 같습니다.

```
fileinto $U+$S@$D
```

위의 키워드는 폴더 이름을 원본 주소에 하위 주소로 삽입하여 원래의 하위 주소를 대체하도록 지정합니다.

LMTP 채널에서의 일반적인 사용법은 다음과 같습니다.

```
fileinto @$40:$U+$S@$D
```

여기서 \$40는 4와 영문자 O입니다(숫자 0이 아님).

## 스팸 필터 키워드

키워드: `destinationspamfilterXoptin`, `sourcespamfilterXoptin`

`destinationspamfilterXoptin`은 이 채널을 대상으로 하는 모든 메일이 필터링 소프트웨어 X를 통해 실행되도록 지정합니다. 필터링 소프트웨어 X는 `option.dat`의 `spamfilterX_library`에서 정의합니다. 필터 매개 변수 앞에는 키워드가 오고 사용 가능한 매개 변수는 필터링 프로그램에 따라 다릅니다.

`sourcespamfilterXoptin`은 이 채널로부터 수신된 모든 메일이 스팸 필터링 소프트웨어 X를 통해 실행하도록 지정합니다. 필터링 소프트웨어 X는 `option.dat`의 `spamfilterX_library`에서 정의합니다. 시스템 차원 기본 매개 변수 앞에는 키워드가 오고 사용 가능한 매개 변수는 필터링 프로그램에 따라 다릅니다. `switchchannel`이 적용되는 경우 이 키워드가 `switched-to` 채널에 포함됩니다.

이러한 키워드를 사용하는 방법에 대한 자세한 내용은 [448페이지의 "채널 수준 필터링 지정"](#)을 참조하십시오.

## 주소 검증 후와 확장 전의 라우팅

키워드: `aliasdetourhost`

`aliasdetourhost`는 호스트된 사용자의 `mailHost` 속성 값에 대한 소스 채널별 대체를 허용합니다. 특히 `aliasdetourhost`는 일반적으로 로컬(이 시스템에서 호스팅되는) 사용자를 대상으로 하는 메일을 라우팅할 때 특정 종류의 처리를 위해 별도의 호스트로 "우회"하는 데 사용됩니다. 메일을 원래 호스트에서 확인(해당 주소가 정당한 로컬 주소인지)하고 처리 호스트로 우회한 다음 확장 및 전달을 위해 원래 호스트로 되돌려 보낼 수 있습니다.

`aliasdetourhost`는 채널 및 타사 필터링 호스트를 더 적절하게 구성하고 일종의 "중간 필터링"을 사용할 수 있게 합니다. `aliasdetourhost`는 일반적으로 대체 변환 채널과 함께 사용됩니다. 대체 변환 채널이 원격 수신자의 라우팅에 영향을 주는 데 사용되는 것과 달리 `aliasdetourhost`는 로컬(이 시스템에서 호스팅되는) 사용자의 라우팅에 영향을 주는 데 사용됩니다.

aliasdetourhost의 인수는 호스트 또는 도메인 이름이거나 호스트/도메인 지정입니다. 다시 쓰기 규칙을 사용하여 호스트 이름, IP 리터럴 주소 및 채널 태그(암시적으로 호스트 이름으로 간주되는)를 처리할 수 있습니다. 소스 채널에서 이 키워드를 지정하는 경우 태그 정보가 처리된 후 메일 호스트 정보가 확인되기 직전에 LDAP에 저장된 주소의 별칭 확장이 중지됩니다. 이 때 메일이 aliasdetourhost 값으로 보내지고 처리된 주소가 성공적으로 완료되지만 이러한 작업은 주소 검증이 끝나고 별칭 확장이 수행되기 전에 발생합니다.

aliasdetourhost를 사용하여 변환 채널 필터링과 관련된 다양한 문제를 방지하는 예는 다음과 같습니다. 여기서는 시스템이 프런트엔드 MTA 및 백엔드 메시지 저장소를 사용하여 설정되었다고 가정합니다. 사용자의 전달 옵션은 전달 및 메일함으로 설정되어 있습니다. MTA에서는 바이러스 백신/스팸 시스템을 위해 대체 변환 채널을 사용합니다. 이 사용자에게 메일이 도착하면 MTA 별칭이 확장되고 두 명의 수신자(하나는 로컬, 다른 하나는 원격)가 생성됩니다. 원격 수신자의 복사본은 직접 전송됩니다. 반면, 로컬 수신자의 복사본은 변환 채널로 이동하여 스캔된 다음 반환됩니다. 그런 다음 별칭 확장이 다시 적용되어 원격 수신자의 두 번째 복사본이 생성되며 로컬 수신자의 복사본은 정상적으로 전달됩니다. 최종적으로 원격 수신자에 대한 두 개의 복사본과 로컬 수신자에 대한 하나의 복사본이 생성됩니다.

aliasdetourhost를 사용하는 채널에서는 로컬로 호스트된 사용자에게 대해 대체 변환 채널을 사용하지 않고(단, 다른 수신자에 대해서는 여전히 대체 변환 채널을 사용할 수 있음) 다음 작업을 수행할 수 있습니다.

- 메일을 수락합니다.
- 메일을 외부 스팸/바이러스 필터에 라우팅합니다.
- 주소 확장 및 전달을 위해 메일을 다시 수락합니다.

#### 예 1:

타사 스캐너가 MTA에서 별개의 호스트에 실행 중이라고 가정합니다. 다음 예는 메일을 수락하기 전에 수신자 주소 검증을 수행하는 기능을 유지하면서도 가짜 복제본을 만들지 않고 사용자 항목을 전달할 수 있게 합니다.

1. 새 tcp\_scanner 채널을 만듭니다.

daemon 키워드를 해당 채널에 넣어 필터링 시스템을 가리킵니다.

enqueue\_removertime도 이 채널에 추가합니다. tcp\_scanner 채널은 imta.cnf에서 다음과 같이 표시됩니다.

```
tcp_scanner smtp mx single_sys subdirs 20 noreverse maxjobs 7 pool
SMTP_POOL daemon my_a-v_filter.siroe.com enqueue_removertime
tcp_scanner-daemon
```



2. 스캔할 모든 인바운드 소스 tcp채널(tcp\_local, tcp\_submit, tcp\_intranet 등)에서 aliasDetourHost tcp\_scanner-daemon을 tcp\_local에 추가합니다. 다음은 tcp\_local 및 tcp\_submit에 대한 예입니다.

```
! tcp_local
tcp_local smtp mx single_sys remotehost inner switchchannel
identnonnumeric subdirs 20 maxjobs 7 pool SMTP_POOL maytlserver
maysaslserver sasls witchchannel tcp_auth missingrecipientpolicy 0
aliasdetourhost tcp_scanner-daemon
tcp-daemon
```

```
! tcp_submit
tcp_submit submit smtp mx single_sys mustsasls server maytlserver
missingrecipientpolicy 4 aliasdetourhost tcp_scanner-daemon
tcp_submit-daemon
```

aliasdetourhost(tcp\_scanner-daemon)의 인수는 새 채널 tcp\_scanner의 공식 호스트 이름입니다.

3. tcp\_scanner 채널을 통해 스캔 시스템에서 메일을 다시 수신하기 위해 다시 쓰기 규칙을 작성합니다.

```
[1.2.3.4] $E$R$U[1.2.3.4]@tcp_scanner-daemon
```

여기서 1.2.3.4는 스캐너 시스템의 IP 주소입니다.

이 다시 쓰기 규칙이 없으면 메일이 다른 tcp\* 소스 채널을 통해 들어오며 모든 메일에 aliasdetourhost가 있기 때문에 메일이 다시 스캔됩니다. 루프가 발생합니다.

4. 구성을 다시 컴파일하고 디스패처를 다시 시작합니다.

```
#imsimta cnbuild
#imsimta restart dispatcher
```

## 예 2:

타사 스캐너가 MTA와 동일한 호스트에서 실행 중이지만 다른 포트를 수신한다고 가정합니다. 메일이 포트 10024에서 수락되며 포트 10025에서 릴레이된다고 가정합니다.

1. 새 tcp\_scanner 채널을 만듭니다.

```
! tcp_scanner
tcp_scanner smtp nomx single_sys identnonnumeric subdirs 20 maxjobs 7 pool
SCAN_POOL daemon 127.0.0.1 port 10024 enqueue_remove route
tcp_scanner-daemon
```

- 스캔할 모든 인바운드 소스 tcp 채널(tcp\_local, tcp\_submit, tcp\_intranet 등)에서 aliasDetourHost tcp\_scanner-daemon을 tcp\_local에 추가합니다. 다음은 tcp\_local 및 tcp\_submit에 대한 예입니다.

```
! tcp_local
tcp_local smtp mx single_sys remotehost inner switchchannel
identnonnumeric subdirs 20 maxjobs 7 pool SMTP_POOL maytlsserver
maysaslserver saslswitchchannel tcp_auth missingrecipientpolicy 0
aliasdetourhost tcp_scanner-daemon
tcp-daemon
```

```
! tcp_submit
tcp_submit submit smtp mx single_sys mustsaslsaslserver maytlsserver
missingrecipientpolicy 4 aliasdetourhost tcp_scanner-daemon
tcp_submit-daemon
```

- tcp\_scanner 채널을 통해 아웃바운드 메일을 다시 라우팅하기 위해 mappings 파일에 추가합니다.

CONVERSIONS

```
in-chan=tcp_scanner;out-chan=*;CONVERT          No
in-chan=tcp_*;out-chan=tcp_local;CONVERT       Yes,Channel=tcp_scanner
```

- SMTP\_POOL 아래의 job\_controller.cnf에서 동시 스캔 수에 대한 제한을 추가합니다.

스캔 소프트웨어에도 제한이 있어야 하지만 Messaging Server가 메일을 수락하지 않을 경우에 스캐너로 메일을 전송하지 않도록 하기 위해서 이 설정을 동일하게 유지하는 것이 좋습니다.

```
!
[POOL=SCAN_POOL]
job_limit=2
!
```

- 새 서비스를 dispatcher.cnf에 추가하여 특정 포트에서 스캐너로부터 되돌아오는 메일을 수락하고 메일이 다시 스캔되지 않도록 tcp\_scan에서 메일을 가져옵니다.

```
!
[SERVICE=SMTP_SCANNING]
INTERFACE_ADDRESS=127.0.0.1
PORT=10025
IMAGE=IMTA_BIN:tcp_smtp_server
LOGFILE=IMTA_LOG:tcp_smtp_server.log
STACKSIZE=2048000
PARAMETER=CHANNEL=tcp_scanner
!
```

## 6. 구성을 다시 컴파일하고 디스패처를 다시 시작합니다.

```
# imsimta cnbuild
# imsimta restart job_controller
# imsimta restart dispatcher
```

## NO-SOLICIT SMTP 확장 지원

키워드: `sourcenosolicit` 및 `destinationnosolicit`

**Internet-Draft** `draft-malamud-no-soliciting-07.txt`에 설명된 NO-SOLICIT SMTP 확장은 **Messaging Server**에서 제안된 표준으로 구현되었습니다. 다음 채널 키워드를 사용하여 이 기능을 제어할 수 있습니다.

`sourcenosolicit`는 이 채널이 전송하는 메일에서 차단될 요청 필드 값의 쉽표로 구분된 목록을 지정합니다 이 값 목록은 NO-SOLICIT EHLO 응답에 표시됩니다. 글롭 스타일 와일드카드를 이러한 값에서 사용할 수 있지만 와일드카드를 포함하는 값은 EHLO 알림에 표시되지 않습니다.

`destinationnosolicit`는 이 채널의 대기열에 포함된 메일에서 허용되지 않는 요청 필드 값의 쉽표로 구분된 목록을 지정합니다.

## 잘못된 RCPT TO: 주소에 대한 제한 설정

키워드: `deferralrejectlimit`

단일 세션에서 허용되는 잘못된 RCPT TO: 주소의 수에 제한을 설정합니다. 지정된 수의 To: 주소가 거부되면 모든 후속 수신자(잘못되었는지 여부에 상관없이)는 4xx 오류와 함께 거부됩니다. `ALLOW_REJECTIONS_BEFORE_DEFERRAL` SMTP 채널 키워드와 동일한 기능을 채널 단위로 제공합니다.

기타 키워드

# 미리 정의된 채널 사용

Messaging Server를 처음 설치하면 여러 채널이 미리 정의되어 있습니다(표 13-1 참조). 이 장에서는 MTA에서 미리 정의된 채널 정의를 사용하는 방법에 대해 설명합니다.

10장, "MTA 서비스 및 구성 정보"를 아직 읽지 않은 경우 이 장을 읽기 전에 8장을 읽어 보십시오. imta.cnf 파일의 다시 쓰기 규칙 구성에 대한 자세한 내용은 11장, "다시 쓰기 규칙 구성"을 참조하십시오.

이 장은 다음 내용으로 구성되어 있습니다.

- 407페이지의 "파이프 채널을 사용하여 메일을 프로그램에 전달"
- 408페이지의 "원시(/var/mail) 채널 구성"
- 409페이지의 "보관 채널을 사용하여 메일을 일시적으로 보관"
- 410페이지의 "변환 채널"
- 430페이지의 "문자 세트 변환 및 메일 형식 다시 지정"

defaults 채널에 대해서는 332페이지의 "채널 기본값 구성"에 설명되어 있습니다.

**표 13-1** 미리 정의된 채널

| 채널       | 정의                                                                                                                              |
|----------|---------------------------------------------------------------------------------------------------------------------------------|
| defaults | 여러 채널의 기본값이 되는 키워드를 지정하는 데 사용됩니다. 332페이지의 "채널 기본값 구성"을 참조하십시오.                                                                  |
| l        | UNIX 전용입니다. 라우팅 결정을 내리고 UNIX 메일 도구를 사용하여 메일을 전송하는 데 사용됩니다.                                                                      |
| ims-ms   | 로컬 저장소에 메일을 전달합니다.                                                                                                              |
| native   | UNIX 전용입니다. 메일을 /var/mail에 전달합니다. Messaging Server는 /var/mail 액세스를 지원하지 않습니다. 사용자가 UNIX 도구를 사용하여 /var/mail 저장소에서 메일에 액세스해야 합니다. |

**표 13-1** 미리 정의된 채널

| 채널                                                             | 정의                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|----------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| pipe                                                           | 사이트에서 제공하는 프로그램 또는 스크립트를 통해 전달을 수행하는 데 사용됩니다. pipe 채널에서 실행되는 명령은 imsimta 프로그램 인터페이스를 통해 관리자가 제어합니다.                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| reprocess<br>process                                           | 이러한 채널은 지연된 오프라인 메일을 처리하는 데 사용됩니다. reprocess 채널은 일반적으로 소스 또는 대상 채널로 표시되지 않고 process 채널은 다른 MTA 채널과 마찬가지로 표시됩니다.                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| defragment                                                     | MIME 조각화된 메일을 다시 어셈블할 수 있습니다.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| conversion                                                     | MTA를 통해 주고 받는 메일에 대해 본문 부분 단위 변환을 수행합니다.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| bitbucket                                                      | 삭제해야 하는 메일에 사용됩니다.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| inactive/deleted                                               | 디렉토리에 비활성/삭제됨으로 표시된 사용자의 메일을 처리하는 데 사용됩니다. 일반적으로 메일을 바운스하고 메일을 보낸 사람에게 사용자 정의 바운스 메일을 반환합니다.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| hold                                                           | 사용자의 메일을 보관하는 데 사용됩니다. 예를 들어, 사용자가 한 메일 서버에서 다른 메일 서버로 마이그레이션하는 경우에 이러한 사용자의 메일을 보관합니다.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| sms                                                            | SMS 게이트웨이에 단방향 전자 메일 지원을 제공합니다.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| tcp_local<br>tcp_intranet<br>tcp_auth<br>tcp_submit<br>tcp_tas | TCP/IP를 통해 SMTP를 구현합니다. 다중 스레드 TCP SMTP 채널은 디스패처의 제어에 따라 실행되는 다중 스레드 SMTP 서버를 포함합니다. 보내는 SMTP 메일은 tcp_smtp_client 채널 프로그램에서 처리되고 필요한 경우 Job Controller의 제어에 따라 실행됩니다.<br><br>tcp_local은 원격 SMTP 호스트로부터 인바운드 메일을 받습니다. 스마트 호스트/방화벽 구성을 사용하는지 여부에 따라 아웃바운드 메일을 원격 SMTP에 직접 보내거나 스마트 호스트/방화벽 시스템으로 보냅니다.<br><br>tcp_intranet은 인트라넷에서 메일을 보내고 받습니다.<br><br>tcp_auth는 tcp_local에 대한 전환 채널로 사용되며 인증된 사용자를 tcp_auth 채널로 전환하여 릴레이 차단 제한을 방지합니다.<br><br>tcp_submit은 예약된 제출 포트 587에서 메일 제출(일반적으로 사용자 에이전트로부터)을 허용합니다(RFC 2476 참조).<br><br>tcp_tas는 사이트에서 통합 메시징을 수행하는 데 사용되는 특수 채널입니다. |

## 파이프 채널을 사용하여 메일을 프로그램에 전달

받는 메일이 메일함 대신 프로그램에 전달되게 할 수 있습니다. 예를 들어, 사용자는 받는 메일을 메일 정렬 프로그램으로 보내기를 원할 수 있습니다. pipe 채널은 사이트에서 제공하는 사용자 단위 프로그램을 사용하여 메일 전달을 수행합니다.

프로그램 전달을 쉽게 수행하려면 pipe 채널에서 호출 가능하도록 먼저 프로그램을 등록해야 합니다. `imsimta program` 유틸리티를 사용하여 등록합니다. 이 유틸리티는 pipe 채널에서 호출 가능하도록 등록하는 각 명령에 고유한 이름을 제공합니다. 그런 다음 최종 사용자는 메소드 이름을 해당 `mailprogramdeliveryinfo` LDAP 속성 값으로 지정할 수 있습니다.

예를 들어, UNIX 명령 `myprocmail`을 사용자가 호출할 수 있는 프로그램으로 등록하려면 먼저 다음 예에 표시된 것처럼 `imsimta program` 유틸리티를 사용하여 명령을 등록합니다. 이 예에서는 `-d username` 인수를 사용하여 `procmail` 프로그램을 실행하고 사용자로 실행되는 `myprocmail`이라는 프로그램을 등록합니다.

```
imsimta program -a -m myprocmail -p procmail -g "-d %s" -e user
```

`programs` 디렉토리인 `msg_svr_base/data/site-programs`에 실행 파일이 존재하는지 확인합니다. 또한 실행 권한이 "others"로 설정되었는지도 확인합니다.

사용자가 프로그램에 액세스하려면 해당 사용자의 LDAP 항목에 다음 속성과 값이 포함되어 있어야 합니다.

```
maildeliveryoption: program
mailprogramdeliveryinfo: myprocmail
```

`imsimta program` 유틸리티에 대한 자세한 내용은 *Messaging Server Reference Manual*을 참조하십시오.

대체 전달 프로그램은 다음 종료 코드 및 명령줄 인수 제한을 준수해야 합니다.

**종료 코드 제한.** pipe 채널에서 호출되는 전달 프로그램은 메일을 대기열에서 제외할지, 나중에 처리하도록 전달할지 또는 메일을 반환할지 여부를 채널이 알 수 있도록 의미 있는 오류 코드를 반환해야 합니다.

하위 프로세스가 종료 코드 0(EX\_OK)으로 끝나는 경우 해당 메일이 성공적으로 전달되고 MTA 대기열에서 제거되는 것으로 간주합니다. 하위 프로세스가 종료 코드 71, 74, 75 또는 79(EX\_OSERR, EX\_IOERR, EX\_TEMPFAIL 또는 EX\_DB)로 끝나는 경우 일시적인 오류가 발생하여 메일 전달이 지연되는 것으로 간주합니다. 다른 종료 코드가 반환되는 경우 해당 메일은 메일 발송자에게 전달 불가능 메일로 반환됩니다. 이러한 종료 코드는 `syssexits.h` 시스템 헤더 파일에 정의됩니다.

**명령줄 인수.** 전달 프로그램은 변수 인수 `%s`뿐 아니라 고정 인수를 가질 수 있습니다. 이를 사용하여 사용자가 실행한 프로그램의 아이디를 나타내거나 포스트마스터인 "inetmail"이 실행하는 프로그램의 아이디+도메인을 나타낼 수 있습니다. 예를 들어, 다음 명령줄은 `procmail` 프로그램을 사용하여 수신자의 메일을 전달합니다.

```
/usr/lib/procmail -d %s
```

## 원시(/var/mail) 채널 구성

옵션 파일을 사용하여 원시 채널의 다양한 특성을 제어할 수 있습니다. 이 원시 채널 옵션 파일은 MTA 구성 디렉토리에 저장하고 `native_option`(예: `msg_svr_base/config/native_option`)으로 이름을 지정해야 합니다.

옵션 파일은 여러 행으로 구성됩니다. 각 행에는 하나의 옵션에 대한 설정값이 포함되어 있습니다. 옵션의 형식은 다음과 같습니다.

```
option=value
```

*value*는 옵션의 요구 사항에 따라 문자열 또는 정수일 수 있습니다.

**표 13-2** 로컬 채널 옵션

| 옵션                                        | 설명                                                                                                                                                                                                    |
|-------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| FORCE_CONTENT_LENGTH<br>(0 또는 1, UNIX 전용) | FORCE_CONTENT_LENGTH=1이면 MTA는 원시 채널에 전달된 메일에 Content-length: 헤더 행을 추가하여 "From"이 행의 시작 부분에 있을 경우 채널에서 ">From" 구문을 사용하지 않게 합니다. 그렇게 하면 로컬 UNIX 메일이 Sun의 최신 메일 도구와 호환되지만 다른 UNIX 메일 도구와는 호환되지 않을 수 있습니다. |



표 13-2 로컬 채널 옵션 (계속)

| 옵션                                 | 설명                                                                                                                                                                                                                                                                                                                                                                                                     |
|------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| FORWARD_FORMAT(문자열)                | <p>사용자의 <code>.forward</code> 파일 위치를 지정합니다. <code>%u</code> 문자열은 각 사용자 아이디에서 대체됨을 나타내고, <code>%h</code> 문자열은 각 사용자의 홈 디렉토리에서 대체됨을 나타냅니다. 이 옵션을 명확하게 지정하지 않을 경우 기본 동작은 다음과 같습니다.</p> <pre>FORWARD_FORMAT=%h/.forward</pre>                                                                                                                                                                              |
| REPEAT_COUNT(정수)<br>SLEEP_TIME(정수) | <p>MTA가 새 메일을 전달하려고 시도할 때 다른 프로세스에 의해 사용자의 새 메일 파일이 잠긴 경우 이러한 옵션을 사용하여 원시 채널 프로그램이 수행하는 시도 횟수와 빈도를 제어할 수 있습니다. 지정된 횟수만큼의 시도 후에도 파일을 열 수 없는 경우 메일을 원시 대기열에 그대로 두고 해당 원시 채널이 다음에 실행될 때 새 메일을 다시 전달하려고 시도합니다.</p> <p>REPEAT_COUNT 옵션은 채널 프로그램이 메일 파일을 열기 위해 시도하는 횟수를 제어합니다. REPEAT_COUNT 기본값은 30(30회 시도)입니다.</p> <p>SLEEP_TIME 옵션은 채널 프로그램이 시도 간에 대기하는 시간(초)을 제어합니다. SLEEP_TIME 기본값은 2(시도 간격: 2초)입니다.</p> |
| SHELL_TIMEOUT(정수)                  | <p><code>.forward</code>의 사용자 셸 명령이 완료될 때까지 채널이 대기하는 시간(초)을 제어합니다. 그런 시간 초과가 발생하면 "Time-out waiting for <i>user's</i> shell command <i>command</i> to complete."와 비슷한 오류 메시지와 함께 원래의 보낸 사람에게 메일이 반환됩니다. 기본값은 600(10분)입니다.</p>                                                                                                                                                                          |
| SHELL_TMPDIR(디렉토리별)                | <p>로컬 채널에서 셸 명령에 전달할 때 임시 파일을 만드는 위치를 제어합니다. 기본적으로 그런 임시 파일은 사용자의 홈 디렉토리에 만들어집니다. 관리자는 이 옵션을 사용하여 임시 파일을 다른(단일) 디렉토리에 만들도록 선택할 수 있습니다. 예를 들면 다음과 같습니다.</p> <pre>SHELL_TMPDIR=/tmp</pre>                                                                                                                                                                                                                |

## 보관 채널을 사용하여 메일을 일시적으로 보관

보관 채널은 새 메일 받기가 일시적으로 금지된 수신자의 메일을 보관하는 데 사용됩니다. 사용자의 이름이 변경되었거나 메일함이 다른 메일 호스트 또는 도메인으로 이동된 경우에 메일을 보관할 수 있습니다. 다른 이유로 메일을 일시적으로 보관할 수도 있습니다.

메일을 보관할 경우 메일을 재처리 채널로 이동하는 데 사용되는 것과 동일한 기법으로 메일을 `msg_svr_base/queue/hold` 디렉토리의 보관 채널로 이동합니다. 그렇게 해도 봉투의 To: 주소는 변경되지 않습니다. 메일은 `msg-server/queue/hold` 디렉토리의 보관 채널 대기열에 `ZZxxx.HELD` 파일로 작성됩니다. 이렇게 하면 메일이 Job Controller에 의해 표시되지 않고 "보관"됩니다. `.HELD` 파일의 목록을 보려면 `imsimta qm dir -held` 명령을

사용합니다. 이러한 메일을 선택한 다음 `imsimta qm release` 명령을 사용하여 해제할 수 있습니다. 메일을 해제하면 메일 이름이 `ZZxxx.00`으로 변경되고 **Job Controller**에 알립니다. 그러면 보관 채널과 연결된 마스터 프로그램 `reprocess.exe`에서 해당 메일을 처리합니다. 일반적인 다시 쓰기 방법을 사용하여 메일 및 **To:** 주소를 처리합니다.

`imsimta qm` 명령에 대한 자세한 내용은 *Sun Java System Messaging Server Administration Reference*를 참조하십시오.

## 변환 채널

Conversion 채널을 사용하면 MTA를 통과하는 메일 흐름에서 임의의 본문을 본문 부분 단위로 처리할 수 있습니다. 본문 부분은 메일과 다릅니다. 예를 들어, 메일은 한 첨부 파일에 여러 본문 부분을 포함할 수 있습니다. 또한, 본문 부분은 MIME 헤더에서 지정하고 설명합니다. 이 프로세스는 사이트에서 제공하는 프로그램이나 명령 프롬프트에 의해 수행될 수 있으며 텍스트 또는 이미지를 다른 형식으로 변환, 바이러스 스캔, 언어 변환 등과 같은 작업을 수행할 수 있습니다. 변환할 다양한 메일 유형의 MTA 트래픽을 선택한 다음 각 유형의 메일 본문 부분에 대해 특정 프로세스 및 프로그램을 지정할 수 있습니다.

이 장을 학습하려면 채널 개념을 잘 알고 있어야 합니다(189페이지의 "채널" 참조).

Conversion 채널을 사용한 바이러스 스캔과 관련한 자세한 내용은 **Messaging Server Documentation** 웹 사이트([http://docs.sun.com/db/coll/S1\\_MsgTechNotes](http://docs.sun.com/db/coll/S1_MsgTechNotes))의 아래쪽에 있는 **Messaging Server Technical Notes**를 참조하십시오.

변환 채널 구현은 A) 처리할 메일 트래픽 선택 및 B) 메일 처리 방법 지정으로 구성됩니다. 이러한 절차에 대해서는 나중에 자세히 설명합니다.

---

**주**            기본 변환 채널은 MTA 구성 파일(`imta.cnf`)에 자동으로 만들어집니다. 이 채널을 그대로 사용할 수 있으므로 수정할 필요가 없습니다.

---

이 절은 다음과 같은 하위 절로 구성되어 있습니다.

- 411페이지의 "MIME 개요"
- 413페이지의 "변환 처리를 위한 트래픽 선택"
- 414페이지의 "변환 처리 제어"

- 423페이지의 "변환 채널 출력을 사용하여 메일 바운스, 삭제 또는 보관"
- 425페이지의 "변환 채널 예"

## MIME 개요

변환 채널을 사용하면 MIME(Multipurpose Internet Mail Extensions) 헤더 행을 광범위하게 사용할 수 있습니다. 메일 구성 및 MIME 헤더 필드에 대한 지식이 필요합니다.

MIME에 대한 자세한 내용은 RFCs 1806, 2045 - 2049 및 2183을 참조하십시오. 편의를 위해 여기서는 MIME에 대한 간단한 개요를 제공합니다.

### 메일 구성

간단한 메일은 헤더와 본문으로 구성됩니다. 헤더는 메일의 맨 위쪽에 있으며 날짜, 제목, 보낸 사람, 수신자 등과 같은 특정 제어 정보가 포함되어 있습니다. 본문은 헤더 뒤의 첫 번째 빈 행 다음의 모든 내용입니다. MIME는 여러 본문 부분 및 본문 부분 내에 중첩된 본문 부분을 포함할 수 있는 보다 복잡한 메일을 구성하는 방법을 지정합니다. 이러한 메일을 다중 부분 메일이라 합니다. 앞에서 설명한 것처럼 변환 채널은 메일을 본문 부분 단위로 처리합니다.

### MIME 헤더

MIME 규격은 본문 부분에 대한 헤더 행 집합을 정의합니다. 여기에는 MIME-Version, Content-type, Content-Transfer-Encoding, Content-ID 및 Content-disposition이 포함됩니다. 변환 채널은 Content-type 및 Content-disposition 헤더를 가장 많이 사용합니다. 다음은 일부 MIME 헤더 행의 예입니다.

```
Content-type: APPLICATION/wordperfect5.1;name=Poem.wpc
Content-transfer-encoding: BASE64
Content-disposition: attachment; filename=Poem.wpc
Content-description: "Project documentation Draft1 wordperfect format"
```

---

**주** MIME 헤더 행은 To:, Subject: 및 From: 등과 같은 일반적인 비 MIME 헤더 행과 다릅니다. 변환 채널의 경우 MIME 헤더 행은 기본적으로 Content-.로 시작합니다.

---

### Content-type 헤더

MIME Content-Type 헤더는 본문 부분의 내용을 설명합니다. Content-Type 헤더 형식의 예를 들면 다음과 같습니다.

```
Content-type: type/subtype; parameter1=value; parameter2=value...
```

*type*은 본문 부분의 내용 유형을 설명합니다. 유형의 예로는 Text, Multipart, Message, Application, Image, Audio, Video 등이 있습니다.

*subtype*은 내용 유형을 자세히 설명합니다. 각 Content-type에는 자체 하위 유형 집합이 있습니다. 예를 들어, text/plain, application/octet-stream, image/jpeg 등이 있습니다. MIME 메일에 대한 내용 하위 유형은 IANA(Internet Assigned Numbers Authority)에 의해 지정되고 나열됩니다. 목록 복사본은 <http://www.isi.edu/in-notes/iana/assignments/media-types/media-types>에 있습니다.

*parameter*는 Content-type/subtype 쌍에 한정됩니다. charset 및 name 매개 변수의 예를 들면 다음과 같습니다.

```
Content-type: text/plain; charset=us-ascii
Content-type: application/msword; name=temp.doc
```

charset 매개 변수는 텍스트 메일의 문자 세트를 지정합니다. name 매개 변수는 데이터를 파일로 작성할 경우 사용할 파일 이름을 제안합니다.

---

**주** Content-Type 값, subtypes 및 매개 변수 이름은 대/소문자를 구분합니다.

---

### Content-disposition 헤더

MIME Content-disposition 헤더는 본문 부분에 대한 표시 정보를 제공합니다. 이 헤더를 첨부 파일에 추가하여 첨부 파일의 본문 부분을 표시할지(inline) 복사할 파일 이름으로 표시할지(attachment) 여부를 지정하는 경우도 있습니다. Content-disposition 헤더의 형식은 다음과 같습니다.

```
Content-disposition: disposition_type; parameter1=value; parameter2=value...
```

*disposition\_type*은 일반적으로 inline(본문 부분 표시) 또는 attachment(저장할 파일로 표시)입니다. Attachment에는 일반적으로 저장된 파일에 대한 이름을 제안하는 값이 있는 filename 매개 변수가 있습니다.

Content-disposition 헤더에 대한 자세한 내용은 RFC2183을 참조하십시오.

## 변환 처리를 위한 트래픽 선택

다른 MTA 채널과 달리 변환 채널은 일반적으로 주소 또는 MTA 다시 쓰기 규칙에 지정되어 있지 않습니다. 대신 CONVERSIONS 매핑 테이블(*imta\_tailor* 파일의 *IMTA\_MAPPING\_FILE* 매개 변수에 의해 지정됨)을 사용하여 변환 채널에 메일을 보냅니다. 테이블 항목의 형식은 다음과 같습니다.

```
IN-CHAN=source-channel;OUT-CHAN=destination-channel;CONVERT Yes/No
```

MTA는 각 메일을 처리할 때 CONVERSIONS 매핑 테이블(있는 경우)을 검사합니다. *source-channel*이 메일을 가져온 채널이고 *destination-channel*이 메일을 받을 채널인 경우 CONVERT 앞의 작업이 수행됩니다. Yes일 경우 MTA는 *destination-channel*에서 가져온 메일을 변환 채널로 전환합니다. 일치하는 항목이 발견되지 않는 경우 메일이 일반 대상 채널의 대기열에 포함됩니다.

---

**주** CONVERSIONS 매핑 테이블에 관계 없이 *user@conversion.localhostname* 또는 *user@conversion* 형식 주소가 변환 채널을 통해 라우팅됩니다.

---

다음 예에서는 모든 외부 메일(인터넷을 통해 주고 받는 메일)을 변환 채널로 라우팅합니다.

```
CONVERSIONS
```

```
IN-CHAN=tcp_local;OUT-CHAN=*;CONVERT Yes
IN-CHAN=*;OUT-CHAN=tcp_local;CONVERT Yes
```

첫 번째 행은 *tcp\_local* 채널에서 가져온 메일이 처리됨을 지정합니다. 두 번째 행은 *tcp\_local* 채널로 보낸 메일도 처리됨을 지정합니다. *tcp\_local* 채널은 인터넷을 통해 주고 받는 모든 메일을 처리합니다. 기본값은 변환 채널을 통해 전달하지 않는 것이기 때문에 다른 메일이 변환 채널을 통해 전달되지 않습니다.

이 테이블은 기본적인 테이블이므로 보다 많이 사용자 정의된 구성(예: 다중 *outbound-to-the-Internet tcp\_\** 채널을 사용하거나 다중 *inbound-from-the-Internet tcp\_\** 채널을 사용하는 사이트)이 있는 사이트에는 충분하지 않을 수 있습니다.

## 변환 처리 제어

메일을 변환 채널로 보내면 본문 부분 단위로 처리됩니다. 처리는 `imta_tailor` 파일의 `IMTA_CONVERSION_FILE` 옵션에 지정된 MTA conversions 파일(기본값: `msg_svr_base/conversions`)에 의해 제어됩니다. conversions 파일은 1) 처리할 본문 부분의 유형을 지정하고 2) 처리 방법을 제어하는 항목으로 구성됩니다.

각 항목은 여러 `name=value` 매개 변수 절을 포함하는 하나 이상의 행으로 구성됩니다. 매개 변수 절의 값은 MIME 규칙을 따릅니다. 마지막 행을 제외한 모든 행은 세미콜론(;)으로 끝나야 합니다. 이 파일의 물리적 행은 252자로 제한됩니다. 백슬래시(\) 연결 문자를 사용하여 논리적 행을 여러 물리적 행으로 분할할 수 있습니다. 세미콜론으로 끝나지 않는 행이나 하나 이상의 빈 행 또는 두 가지 모두를 사용하여 항목을 종료합니다.

다음은 conversion 파일 항목의 간단한 예입니다.

**코드 예 13-1** conversion 파일 항목

```
out-chan=ims-ms; in-type=application; in-subtype=wordperfect5.1;
out-type=application; out-subtype=msword; out-mode=block;
command="/usr/bin/convert -in=wordp -out=msword 'INPUT_FILE' \ 'OUTPUT_FILE' "
```

`out-chan=ims-ms; in-type=application; in-subtype=wordperfect5.1` 절은 본문 부분을 규정합니다. 즉, 변환할 부분의 유형을 지정합니다. 각 부분의 헤더를 읽고 해당 헤더의 `Content-Type:` 과 기타 헤더 정보를 추출합니다. 그런 다음 conversion 파일의 항목을 처음부터 끝까지 순서대로 검사하여 `in-*` 매개 변수가 있는지 확인하고, `OUT-CHAN` 매개 변수(있는 경우)를 검사합니다. 이러한 매개 변수가 모두 처리할 본문 부분의 해당 정보와 일치하면 `command=` 또는 `delete=` 절에 지정된 변환이 수행되고 `out-*` 매개 변수가 설정됩니다.

일치하지 않는 경우 해당 부분이 다음에 있는 conversions 파일 항목에 대해 일치됩니다. 모든 본문 부분을 스캔하여 처리한 다음(규정된 일치가 있다고 가정) 메일을 다음 채널로 보냅니다. 일치하지 않는 경우 처리 작업을 수행하지 않고 메일을 다음 채널로 보냅니다.

`out-chan=ims-ms`는 `ims-ms` 채널이 대상인 메일 부분만 변환하도록 지정합니다. `in-type=application` 및 `in-subtype=wordperfect5.1`은 메일 부분에 대한 MIME Content-type 헤더가 `application/wordperfect5.1`이어야 함을 지정합니다.

추가 in-\* 매개 변수를 사용하여 메일 부분을 자세히 규정할 수 있습니다. 표 13-6을 참조하십시오. 위 항목은 다음 MIME 헤더 행이 있는 메일 부분에 대한 변환 작업을 트리거합니다.

```
Content-type: APPLICATION/wordperfect5.1;name=Draft1.wpc
Content-transfer-encoding: BASE64
Content-disposition: attachment; filename=Draft1.wpc
Content-description: "Project documentation Draft1 wordperfect format"
```

코드 예 13-1에서 세 conversion 파일 규정 매개 변수 뒤의 두 매개 변수 out-type=application 및 out-subtype=msword는 "처리된" 본문 부분에 첨부할 대체 MIME 헤더 행을 지정합니다. out-type=application 및 out-subtype=msword는 보내는 메일의 MIME Content-type/subtype이 application/msword임을 지정합니다.

in-type 매개 변수와 out-type 매개 변수가 동일하고 보내는 본문 부분의 원본 MIME 레이블이 변환 채널의 기본값이기 때문에 out-type=application은 필요하지 않습니다. 추가 출력 매개 변수를 사용하여 보내는 본문 부분에 대한 추가 MIME 레이블을 지정할 수 있습니다.

out-mode=block(코드 예 13-1)은 사이트에서 제공하는 프로그램이 반환할 파일 유형을 지정합니다. 즉, 파일 저장 방법과 반환된 파일에서 변환 채널을 다시 읽는 방법을 지정합니다. 예를 들어, html 파일은 텍스트 모드로 저장되고 .exe 프로그램 또는 zip 파일은 블록/이진 모드로 저장됩니다. 모드는 읽을 파일이 특정 저장소 형식에 속하는지를 설명하는 방법입니다.

코드 예 13-1의 마지막 매개 변수인

```
command="/usr/bin/convert -in=wordp -out=msword 'INPUT_FILE' 'OUTPUT_FILE'"
```

은 본문 부분에 대해 수행할 작업을 지정합니다.

command= 매개 변수는 프로그램이 본문 부분에서 실행됨을 지정합니다. /usr/bin/convert는 가상 명령 이름이고 -in=wordp 및 -out=msword는 입력 텍스트 및 출력 텍스트의 형식을 지정하는 가상 명령줄 인수입니다. INPUT\_FILE 및 OUTPUT\_FILE은 원래의 본문 부분이 포함된 파일과 프로그램에서 변환된 본문 부분을 저장하는 파일을 지정하는 변환 채널 환경 매개 변수(416페이지의 "변환 채널 환경 변수 사용" 참조)입니다.

---

**주** 일반 변환 항목에 의해 외부 메일 헤더를 포함하는 파일이 요청되는 경우 봉투 생성자 및 수신자 정보는 x-envelope-from 및 x-envelope-to 필드로 제공됩니다.

---

본문 부분에서 명령을 실행하지 않고 command 매개 변수 대신 DELETE=1을 대체하여 메일 부분을 간단히 삭제할 수 있습니다.

---

**주** conversions 파일을 수정할 때마다 구성을 다시 컴파일해야 합니다(*Sun Java System Messaging Server Administration Reference*의 `imsimta refresh` 명령 참조).

---

## 변환 채널 정보 흐름

정보 흐름은 다음과 같습니다. 본문 부분이 포함된 메일이 변환 채널로 전달됩니다. 변환 채널에서 메일을 구문 분석하여 한 부분씩 처리합니다. 그런 다음 본문 부분을 규정합니다. 즉, MIME 헤더 행을 *규정 매개 변수*와 비교하여 메일을 처리할지 여부를 결정합니다. 본문 부분이 규정되면 변환 처리가 시작됩니다. MIME 또는 본문 부분 정보를 변환 스크립트로 전달해야 할 경우 해당 정보가 *정보 전달 매개 변수*에 지정된 환경 변수(표 13-3)로 저장됩니다.

이 지점에서 *작업 매개 변수*에 지정된 작업이 본문 부분에 대해 수행됩니다. 일반적으로 본문 부분을 삭제하거나 스크립트에 포함된 프로그램으로 전달하는 작업입니다. 스크립트는 본문 부분을 처리한 다음 사후 처리 메일로 다시 어셈블할 수 있도록 변환 채널로 다시 보냅니다. 또한, 변환 채널 *출력 옵션*을 사용하여 정보를 변환 채널로 보낼 수 있습니다. 이 정보는 출력 본문 부분에 추가할 새 MIME 헤더 행, 메일을 보낸 사람에게 반환할 오류 텍스트, 작업(메일 바운스, 삭제, 보관 등)을 시작하도록 MTA에 지시하는 특수 지시문 등입니다.

마지막으로 변환 채널은 출력 본문 부분의 헤더 행을 *출력 매개 변수*에 지정된 대로 바꿉니다.

## 변환 채널 환경 변수 사용

메일 본문 부분에 대한 작업을 수행할 경우 사이트에서 제공하는 프로그램을 통해 MIME 헤더 행 정보 또는 전체 본문 부분을 전달하는 것이 좋습니다. 예를 들어, 프로그램에는 메일 본문 부분 외에도 Content-type 및 Content-disposition 헤더 행 정보가 필요할 수 있습니다. 일반적으로 사이트에서 제공하는 프로그램의 기본 입력은 파일에서 읽은 메일 본문 부분입니다. 본문 부분을 처리한 후 프로그램은 변환 채널에서 읽을 수 있도록 본문 부분을 파일에 기록해야 합니다. 이러한 유형의 정보 전달은 변환 채널 환경 변수를 사용하여 수행됩니다.

parameter-symbol-\* 매개 변수 또는 미리 정의된 채널 환경 변수(421페이지의 표 13-4 참조)를 사용하여 conversions 파일에 환경 변수를 만들 수 있습니다.



다음 conversions 파일 항목 및 수신 헤더는 환경 변수를 사용하여 MIME 정보를 사이트에서 제공하는 프로그램에 전달하는 방법을 나타냅니다.

conversions 파일 항목:

```
in-channel=*; in-type=application; in-subtype=*;
parameter-symbol-0=NAME; parameter-copy-0=*;
dparameter-symbol-0=FILENAME; dparameter-copy-0=*;
message-header-file=2; original-header-file=1;
override-header-file=1; override-option-file=1;
command="/bin/viro-scan500.sh ?NPUT_FILE??UTPUT_FILE?
```

수신 헤더:

```
Content-type: APPLICATION/msword; name=Draft1.doc
Content-transfer-encoding: BASE64
Content-disposition: attachment; filename=Draft1.doc
Content-description: "Project documentation Draft1 msword format"
```

in-channel=\*; in-type=application; in-subtype=\*는 유형이 application인 입력 채널의 메일 본문 부분을 처리하도록 지정합니다.

parameter-symbol-0=NAME은 첫 번째 Content-type 매개 변수 값(이 예의 경우 Draft1.doc)을 NAME이라는 환경 변수에 저장하도록 지정합니다.

parameter-copy-0=\*는 입력 본문 부분의 모든 Content-type 매개 변수를 출력 본문 부분에 복사하도록 지정합니다.

dparameter-symbol-0=FILENAME은 첫 번째 Content-disposition 매개 변수 값(이 예의 경우 Draft1.doc)을 FILENAME이라는 환경 변수에 저장하도록 지정합니다.

dparameter-copy-0=\*는 입력 본문 부분의 모든 Content-disposition 매개 변수를 출력 본문 부분에 복사하도록 지정합니다.

message-header-file=2는 메일의 원본 헤더(가장 외부에 있는 메일 헤더) 전체를 MESSAGE\_HEADERS 환경 변수에 지정된 파일에 기록하도록 지정합니다.

original-header-file=1은 포함된 MESSAGE/RFC822 부분의 원본 헤더를 ORIGINAL\_HEADERS 환경 변수에 기록하도록 지정합니다.

override-header-file=1은 포함된 MIME 부분의 원본 MIME 헤더 행을 무시하고 OUTPUT\_HEADERS 환경 변수에 지정된 파일에서 MIME 헤더를 읽도록 지정합니다. \$OUTPUT\_HEADERS는 변환을 실행할 때 즉석에서 만들어지는 임시 파일입니다. 사이트에서 제공하는 프로그램은 이 파일을 사용하여 변환 프로세스 중에 변경된 MIME 헤더 행을 저장합니다. 그런 다음 변환 채널은 본문 부분을 다시 어셈블할 때 이 파일에서 MIME 헤더 행을 읽습니다. MIME 헤더 행만 수정할 수 있습니다. 다른 일반적인 비MIME 헤더 행은 변환 채널에서 변경할 수 없습니다.

override-option-file=1은 변환 채널이 OUTPUT\_OPTIONS 환경 변수를 통해 명명된 파일에서 *변환 채널 옵션*을 읽도록 지정합니다. 420페이지의 "변환 채널 출력 옵션 사용"을 참조하십시오.

command="msg\_svr\_base/bin/viro-scan500.sh"는 메일 본문 부분에서 실행할 명령을 지정합니다.

**표 13-3** 변환 채널 환경 변수

| 환경 변수             | 설명                                                                                                                |
|-------------------|-------------------------------------------------------------------------------------------------------------------|
| ATTACHMENT_NUMBER | 현재 부분의 첨부 파일 수입니다. ATTACHMENT-NUMBER 변환 일치 매개 변수와 같은 형식을 사용합니다.                                                   |
| CONVERSION_TAG    | 활성 변환 태그의 현재 목록입니다. TAG 변환 일치 매개 변수에 해당합니다.                                                                       |
| INPUT_CHANNEL     | 메일을 변환 채널의 대기열에 포함시킨 채널입니다. IN-CHANNEL 변환 일치 매개 변수에 해당합니다.                                                        |
| INPUT_ENCODING    | 본문 부분에 원래 표시된 부분을 인코딩합니다.                                                                                         |
| INPUT_FILE        | 원본 본문 부분이 포함된 파일 이름입니다. 사이트에서 제공하는 프로그램은 이 파일을 읽어야 합니다.                                                           |
| INPUT_HEADERS     | 본문 부분의 원본 헤더 행이 포함된 파일 이름입니다. 사이트에서 제공하는 프로그램은 이 파일을 읽어야 합니다.                                                     |
| INPUT_TYPE        | 입력 메일 부분의 MIME Content-type입니다.                                                                                   |
| INPUT_SUBTYPE     | 입력 메일 부분의 MIME 내용 하위 유형입니다.                                                                                       |
| INPUT_DESCRIPTION | 입력 메일 부분의 MIME content-description입니다.                                                                            |
| INPUT_DISPOSITION | 입력 메일 부분의 MIME content-disposition입니다.                                                                            |
| MESSAGE_HEADERS   | 포함된 메일의 가장 외부에 있는 원본 헤더(본문 부분 아님) 또는 최신 포함된 MESSAGE/RFC822 부분의 헤더를 포함하는 파일 이름입니다. 사이트에서 제공하는 프로그램은 이 파일을 읽어야 합니다. |
| OUTPUT_CHANNEL    | 메일을 보내는 채널입니다. OUT-CHANNEL 변환 일치 매개 변수에 해당합니다.                                                                    |

**표 13-3** 변환 채널 환경 변수 (계속)

| 환경 변수          | 설명                                                                                                                                                                                                                              |
|----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| OUTPUT_FILE    | 사이트에서 제공하는 프로그램이 출력을 저장하는 파일 이름입니다. 사이트에서 제공하는 프로그램은 이 파일을 만들고 써야 합니다.                                                                                                                                                          |
| OUTPUT_HEADERS | 사이트에서 제공하는 프로그램이 포함 부분에 대한 MIME 헤더 행을 저장하는 파일의 이름입니다. 사이트에서 제공하는 프로그램은 이 파일을 만들고 써야 합니다. 파일에는 마지막 행으로 빈 행이 오는 실제 MIME 헤더 행(option=value 행 아님)이 포함되어 있어야 합니다. 또한, MIME 헤더 행만 수정할 수 있습니다. 다른 일반적인 비MIME 헤더 행은 변환 채널에서 변경할 수 없습니다. |
| OUTPUT_OPTIONS | 사이트에서 제공하는 프로그램이 변환 채널 옵션을 읽어야 하는 파일의 이름입니다. 420페이지의 "변환 채널 출력 옵션 사용"을 참조하십시오.                                                                                                                                                  |
| PART_NUMBER    | 현재 부분의 부품 번호입니다. PART-NUMBER 변환 일치 매개 변수와 같은 형식을 사용합니다.                                                                                                                                                                         |
| PART_SIZE      | 처리할 부분의 크기(바이트)입니다.                                                                                                                                                                                                             |

### 메일 변환 태그

메일 변환 태그는 특정한 받는 사람이나 보낸 사람과 연관된 특수한 태그입니다. 메일이 전달될 때 변환 채널 프로그램에서 변환 태그를 볼 수 있으며 특수한 처리를 위해 변환 태그를 사용할 수 있습니다. 변환 태그는 LDAP 디렉토리에 저장됩니다.

메일 변환 태그를 다음과 같이 사용할 수 있습니다. 관리자는 메일 변환 태그 값이 harmonica인 선택된 사용자를 설정할 수 있습니다. 그런 다음 관리자는 해당 메일 처리 시에 태그와 harmonica 값을 감지하는 변환 채널을 설정합니다. 해당 태그와 값이 감지되면 프로그램에서 몇 가지 임의의 기능을 수행합니다.

메일 변환 태그는 사용자 또는 도메인 단위로 설정할 수 있습니다. 도메인 수준의 수신자 LDAP 속성은 MailDomainConversionTag(MTA 옵션 LDAP\_DOMAIN\_ATTR\_CONVERSION\_TAG를 사용하여 수정할 수 있음)입니다. 사용자 수준의 수신자 LDAP 속성은 MailConversionTag(MTA 옵션 LDAP\_CONVERSION\_TAG를 사용하여 수정할 수 있음)입니다. 이러한 두 속성은 값이 여러 개일 수 있으며 각 값에 다른 태그를 지정할 수 있습니다. 특정 수신자와 연관된 태그 집합은 누적됩니다. 즉, 도메인 수준에서 설정된 태그가 사용자 수준에서 설정된 태그와 결합됩니다.

보낸 사람 기반의 변환 태그는 MTA 옵션 LDAP\_SOURCE\_CONVERSION\_TAG 및 LDAP\_DOMAIN\_ATTR\_SOURCE\_CONVERSION\_TAG를 사용하여 설정할 수 있습니다. 이 옵션은 이러한 소스 주소와 연관된 변환 태그에 대해 각각 사용자 및 도메인 수준 LDAP 속성을 지정합니다. 이러한 옵션에는 기본 속성이 없습니다.

## 변환 채널 출력 옵션 사용

변환 채널 출력 옵션(표 13-4)은 변환 스크립트에서 변환 채널로 정보 및 특수 지시문을 전달하는 데 사용되는 동적 변수입니다. 예를 들어, 본문 부분을 처리하는 동안 스크립트가 메일을 바운스하고 메일에 바이러스가 있다는 오류 텍스트를 반환되는 메일에 추가하도록 요청하는 특수 지시문을 보낼 수 있습니다.

원하는 변환 항목에 `OVERRIDE-OPTION-FILE=1`을 설정하여 출력 옵션을 시작합니다. 그러면 출력 옵션이 필요에 따라 스크립트에서 설정되고 환경 변수 파일 `OUTPUT_OPTIONS`에 저장됩니다. 스크립트가 본문 부분 처리를 완료하면 변환 채널이 `OUTPUT_OPTIONS` 파일에서 옵션을 읽습니다.

`OUTPUT_OPTION` 변수는 변환 채널이 옵션을 읽는 파일의 이름입니다. 일반적으로 이 파일을 즉석에서 만들어지는 임시 파일로 사용하여 정보를 전달합니다. 아래 예는 출력 옵션을 사용하여 바이러스 메일을 보낸 사람에게 오류 메시지를 반환하는 스크립트입니다.

```

/usr/local/bin/viro_screen2k $INPUT_FILE # run the virus screener

if [ $? -eq 1 ]; then
    echo "OUTPUT_DIAGNOSTIC=?irus found and deleted.? > $OUTPUT_OPTIONS
    echo "STATUS=178029946" >> $OUTPUT_OPTIONS
else
    cp $INPUT_FILE $OUTPUT_FILE # Message part is OK
fi
    
```

이 예에서는 시스템 진단 메일과 상태 코드를 `$OUTPUT_OPTIONS`에 정의된 파일에 추가합니다. `$OUTPUT_OPTIONS` 임시 파일에는 다음과 비슷한 내용이 표시됩니다.

```

OUTPUT_DIAGNOSTIC="Virus found and deleted."
STATUS=178029946
    
```

`OUTPUT_DIAGNOSTIC='Virus found and deleted'` 행은 메일에 `Virus found and deleted` 텍스트를 추가하도록 변환 채널에 지시합니다.

178029946은 `msg_svr_base/include/deprecated/pmdf_err.h`에 있는 각 `pmdf_err.h` 파일의 `PMDF_FORCEReturn` 상태입니다. 이 상태 코드는 메일을 보낸 사람에게 다시 바운스하도록 변환 채널에 지시합니다. 특수 지시문 사용에 대한 자세한 내용은 [423페이지의 "변환 채널 출력을 사용하여 메일 바운스, 삭제 또는 보관"](#)을 참조하십시오.

다음은 전체 출력 옵션 목록입니다.

**표 13-4** 변환 채널 출력 옵션

| 옵션                 | 설명                                                                                                                               |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------|
| OUTPUT_TYPE        | 출력 메일 부분의 MIME 내용 유형입니다.                                                                                                         |
| OUTPUT_SUBTYPE     | 출력 메일 부분의 MIME 내용 하위 유형입니다.                                                                                                      |
| OUTPUT_DESCRIPTION | 출력 메일 부분의 MIME 내용 설명입니다.                                                                                                         |
| OUTPUT_DIAGNOSTIC  | 메일이 변환 채널에 의해 강제로 바운스될 경우 보낸 사람에게 전달되는 메일의 일부로 포함되는 텍스트입니다.                                                                      |
| OUTPUT_DISPOSITION | 출력 메일 부분의 MIME content-disposition입니다.                                                                                           |
| OUTPUT_ENCODING    | 출력 메일 부분에 사용할 MIME 내용 전송 encoding입니다.                                                                                            |
| OUTPUT_MODE        | 변환 채널에서 출력 메일 부분을 쓸 때 사용하는 MIME Mode 즉, 수신자가 출력 메일 부분을 읽을 때 사용하는 모드입니다.                                                          |
| STATUS             | 변환기의 종료 상태입니다. 일반적으로 변환 채널에서 일부 작업을 시작하는 특수 지시문입니다. 전체 지시문 목록은 <code>msg_svr_base/include/deprecated/pmdf_err.h</code> 를 참조하십시오. |

### 포함된 MESSAGE/RFC822 부분의 헤더

메일 부분에서 변환을 수행할 때 변환 채널은 포함된 MESSAGE/RFC822 부분의 헤더에 액세스합니다. 포함된 MESSAGE/RFC822 부분이 없는 경우 메일 헤더에 액세스합니다. 헤더의 정보는 사이트에서 제공하는 프로그램에 유용할 수 있습니다.

ORIGINAL-HEADER-FILE=1이 있는 항목을 선택하면 포함된 MESSAGE/RFC822 부분의 모든 원본 헤더 행이 ORIGINAL\_HEADERS 환경 변수에 표시된 파일에 기록됩니다.

OVERRIDE-HEADER-FILE=1인 경우 변환 채널은 ORIGINAL\_HEADERS 환경 변수에 표시된 파일의 내용을 읽어 해당 포함 부분의 헤더로 사용합니다.

### 변환 항목에서 매핑 테이블 호출

out-parameter-\* 값은 이름이 중복 지정된 매핑 테이블에서 저장 및 검색될 수 있습니다. 이 기능은 첨부 파일이 postscript, msword 또는 text인지 여부에 관계 없이 att.dat와 같은 일반적인 이름을 사용하여 모든 첨부 파일을 보내는 클라이언트가 첨부 파일의 이름을 변경하여 보낼 때 유용합니다. 이 방법은 다른 클라이언트(예: Outlook)가 확장명을 읽어 해당 부분을 열 수 있도록 이 부분의 레이블을 다시 지정하는 일반적인 방법입니다.

매핑 테이블에서 매개 변수 값을 검색하는 구문은 다음과 같습니다.

```
'mapping-table-name:mapping-input[$Y,$N]'
```

\$Y는 매개 변수 값을 반환합니다. 일치하는 내용이 없거나 \$N이 반환될 경우 변환 파일 항목의 해당 매개 변수가 무시되거나 빈 문자열로 처리됩니다. 일치 항목이 부족하거나 \$N이 반환될 경우에는 변환 항목이 중지되지 않습니다.

다음 매핑 테이블을 참조하십시오.

| X-ATT-NAMES    |             |
|----------------|-------------|
| postscript     | temp.PS\$Y  |
| wordperfect5.1 | temp.WPC\$Y |
| msword         | temp.DOC\$Y |

위 매핑 테이블에서 첨부 파일에 있는 특정 파일 이름을 일반 파일 이름으로 대체하면 변환 항목이 다음과 같이 표시됩니다.

```
out-chan=tcp_local; in-type=application; in-subtype=*;
in-parameter-name-0=name; in-parameter-value-0=*;
out-type=application; out-subtype='INPUT-SUBTYPE';
out-parameter-name-0=name;
out-parameter-value-0="'X-ATT-NAMES:\\\' INPUT_SUBTYPE\\\'";
command="cp 'INPUT_FILE' 'OUTPUT_FILE'"
```

위 예에서 out-chan=tcp\_local; in-type=application; in-subtype=\*는 application/\*(\*는 하위 유형의 수행 작업을 지정함)의 content-type 헤더를 사용하여 tcp\_local 채널에서 처리할 메일을 가져오도록 지정합니다.

in-parameter-name-0=name; in-parameter-value-0=\*는 메일에 name=\* 매개 변수 유형(\*는 매개 변수 값의 수행 작업을 지정함)이 있어야 함을 지정합니다.

out-type=application;은 사후 처리 메일의 MIME Content-type 매개 변수가 application임을 지정합니다.

out-subtype=?NPUT-SUBTYPE?은 사후 처리 본문 부분의 MIME subtype 매개 변수가 입력 subtype의 원본 값인 INPUT-SUBTYPE 환경 변수임을 지정합니다. 따라서

```
Content-type: application/xxxx; name=foo.doc
```

위 항목을 아래와 같이 변경하려면

```
Content-type: application/msword; name=foo.doc
```

다음을 사용합니다.

```
out-type=application; out-subtype=msword
```

`out-parameter-name-0=name`; 은 출력 본문 부분의 첫 번째 MIME Content-type 매개 변수가 `name=` 유형임을 지정합니다.

`out-parameter-value-0='X-ATT-NAMES:\\INPUT_SUBTYPE\\'`; 은 첫 번째 MIME subtype 매개 변수 값을 사용하여 X-ATT-NAMES 매핑 테이블에서 subtype 일치 항목을 검색하도록 지시합니다. 일치 항목이 발견되면 name 매개 변수는 X-ATT-NAMES 매핑 테이블에 지정된 새 값을 받습니다. 따라서, 매개 변수가 msword 유형인 경우 name 매개 변수는 temp.DOC가 됩니다.

## 변환 채널 출력을 사용하여 메일 바운스, 삭제 또는 보관

이 절에서는 변환 채널 옵션을 사용하여 메일을 바운스, 삭제 또는 보관하는 방법을 설명합니다. 기본 절차는 다음과 같습니다.

1. 해당 변환 파일 항목에서 `OVERRIDE-OPTION-FILE=1`을 설정합니다. 이 설정은 `OUTPUT_OPTIONS` 파일에서 출력 옵션을 읽도록 변환 채널에 지시합니다.
2. 변환 스크립트를 사용하여 특정 메일 본문 부분에 필요한 작업을 결정합니다.
3. 스크립트에서 `OUTPUT_OPTIONS` 파일에 `STATUS=directive_code` 옵션을 작성하여 해당 작업에 대한 특수 지시문을 지정합니다.

전체 특수 지시문 목록은 `msg_svr_base/include/deprecated/pmdf_err.h`를 참조하십시오. 변환 채널에 일반적으로 사용되는 특수 지시문은 다음과 같습니다.

**표 13-5** 변환 채널에 일반적으로 사용되는 특수 지시문

| 이름                | 16진수 값     | 10진수 값    |
|-------------------|------------|-----------|
| PMDF__FORCEHOLD   | 0x0A9C86AA | 178030250 |
| PMDF__FORCERETURN | 0x0A9C857A | 178029946 |
| PMDF__FORCEDELETE | 0x0A9C8662 | 178030178 |

이러한 지시문의 기능의 예는 다음과 같습니다.

## 메일 바운스

변환 채널을 사용하여 메일을 바운스하려면 해당 conversions 파일 항목에서 OVERRIDE-OPTION-FILE=1을 설정하고 변환 스크립트에 다음 행을 추가합니다.

```
echo "STATUS=178029946" >> $OUTPUT_OPTIONS
```

바운스된 메일에 간단한 텍스트 문자열을 추가하려면 변환 스크립트에 다음 행을 추가합니다.

```
echo OUTPUT_DIAGNOSTIC=text-string >> $OUTPUT_OPTIONS
```

여기서 텍스트 문자열은 "The message sent from your machine contained a virus which has been removed. Be careful about executing email attachments."과 같습니다.

## 메일 부분 조건부 삭제

메일 부분을 포함된 내용에 따라 조건적으로 삭제하는 것이 좋을 수 있습니다. 조건적 삭제는 출력 옵션을 사용하여 수행할 수 있습니다. 반대로 DELETE=1 변환 매개 변수 절은 메일 부분을 무조건 삭제합니다.

출력 옵션을 사용하여 메일 부분을 삭제하려면 해당 변환 파일 항목에 OVERRIDE-OPTION-FILE=1을 설정하고 변환 스크립트에 다음 행을 추가합니다.

```
echo "STATUS=178030178" >> $OUTPUT_OPTIONS
```

## 메일 보관

메일 부분을 포함된 내용에 따라 조건적으로 보관하는 것이 좋을 수 있습니다. 출력 옵션을 사용하여 메일 부분을 삭제하려면 해당 변환 파일 항목에 OVERRIDE-OPTION-FILE=1을 설정하고 변환 스크립트에 다음 행을 추가합니다.

```
echo "STATUS=178030250" >> $OUTPUT_OPTIONS
```

이 행은 변환 채널이 메일을 변환 채널 대기열에 .HELD 파일로 보관해야 하도록 요청합니다.



## 변환 채널 예

아래 예에 표시된 CONVERSIONS 매핑 및 변환 규칙 세트는 tcp\_docuprint 가상 채널로 보낸 GIF, JPEG 및 BITMAP 파일을 PostScript로 자동으로 변환하게 합니다. 이러한 여러 변환에서는 가상 /usr/bin/ps-converter.sh를 사용하여 해당 변환을 수행합니다.

WordPerfect 5.1 파일을 Microsoft Word 파일로 변환하는 추가 규칙이 포함되어 있습니다.

```
CONVERSIONS

IN-CHAN=*;OUT-CHAN=tcp_docuprint;CONVERT Yes
```

```
out-chan=ims-ms; in-type=application; in-subtype=wordperfect5.1;
out-type=application; out-subtype=mword; out-mode=block;
command="/bin/doc-convert -in=wp -out=msw ?NPUT_FILE?"

out-chan=tcp_docuprint; in-type=image; in-subtype=gif;
out-type=application; out-subtype=postsript; out-mode=text;
command="/bin/ps-convert -in=gif -out=ps ?NPUT_FILE?"

out-chan=tcp_docuprint; in-type=image; in-subtype=jpeg;
out-type=application; out-subtype=postsript; out-mode=text;
command="/bin/ps-convert -in=jpeg -out=ps ?NPUT_FILE?"

out-chan=tcp_docuprint; in-type=image; in-subtype=bitmap;
out-type=application; out-subtype=postsript; out-mode=text;
command="/bin/ps-convert -in=bmp -out=ps 'INPUT_FILE' 'OUTPUT_FILE'"
```

## 아랍어 문자 세트 자동 감지

아랍어 문자 세트를 자동으로 감지하기 위한 새로운 *auto\_ef* 프로그램이 추가되었습니다.

변환 채널에서 *auto\_ef* 프로그램을 호출하여 레이블링되지 않았거나 잘못 레이블링된 아랍어 문자 세트의 텍스트 메일을 대부분 자동으로 감지하고 레이블링할 수 있습니다. 이러한 레이블링되지 않았거나 잘못 레이블링된 메일은 일반적으로 Yahoo나 Hotmail에서 아랍어로 보낸 메일입니다.

문자 세트 레이블링을 제대로 하지 못하면 많은 메일 클라이언트에서 메일을 올바르게 표시하지 못합니다.

메일에 MIME 내용 유형 헤더가 있으면 `auto_ef` 프로그램은 텍스트/일반 내용 유형의 헤더만 검사하고 처리합니다. 메일이 MIME 내용 유형 헤더로 레이블링되어 있지 않은 경우에는 `auto_ef`는 텍스트/일반 내용 유형을 무조건 추가합니다.

이 프로그램을 활성화하거나 사용 가능하도록 설정하려면 다음을 수행해야 합니다.

1. `msg_svr_base/config` 디렉토리에 있는 매핑 파일을 편집하여 선택에 따라 소스 및 대상 채널에 대해 변환 채널을 활성화합니다. 인터넷에서 로컬 사용자에게 오는 모든 메일에 대해 변환 채널을 활성화하려면 매핑 파일에 다음과 유사한 섹션을 추가합니다.

```
CONVERSIONS
```

```
IN-CHAN=tcp*;OUT-CHAN=ims-ms;CONVERT YES
```

IN 및 OUT 채널은 구성에 따라 다릅니다. 릴레이 MTA에 배포하려면 해당 구성에 맞게 채널을 수정해야 합니다. 예를 들면 다음과 같습니다.

```
IN-CHAN=tcp*;OUT-CHAN=tcp*;CONVERT YES
```

또는 다음과 같이 모든 채널에 대해 설정할 수 있습니다.

```
IN-CHAN=*;OUT-CHAN=*;CONVERT YES
```

2. Messaging Server 사용자가 소유하고 읽을 수 있는 `msg_svr_base/config` 디렉토리에 다음 내용을 포함하는 변환 파일을 만듭니다.

```
!
in-channel=*; out-channel=*;
in-type=text; in-subtype=*;
parameter-copy-0=*; dparameter-copy-0=*;
original-header-file=1; override-header-file=1;
command="msg_svr_base/lib/arabicdetect.sh"
!
```

3. 다음 명령으로 MTA 구성을 컴파일합니다.

```
msg_svr_base/sbin/imsimta cnbuild
```

4. 다음 명령을 사용하여 다시 시작합니다.

```
msg_svr_base/sbin/imsimta restart
```

표 13-6 변환 매개 변수

| 매개 변수                                         | 설명                                                                                                                                                                                 |
|-----------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>매개 변수 규정(변환하기 전에 메일이 일치해야 하는 매개 변수 지정)</b> |                                                                                                                                                                                    |
| OUT-CHAN,<br>OUT-CHANNEL                      | 변환을 위해 일치시킬 출력 채널(와일드카드 허용)입니다. 메일이 해당 채널의 대상으로 지정된 경우에만 이 항목에 지정된 변환이 수행됩니다.                                                                                                      |
| IN-CHAN,<br>IN-CHANNEL                        | 변환을 위해 일치시킬 입력 채널(와일드카드 허용)입니다. 지정된 채널에서 메일이 전달된 경우에만 이 항목에 지정된 변환이 수행됩니다.                                                                                                         |
| IN-TYPE                                       | 변환을 위해 일치시킬 입력 MIME 유형(와일드카드 허용)입니다. 이 필드가 본문 부분의 MIME 유형과 일치하는 경우에만 지정된 변환이 수행됩니다.                                                                                                |
| IN-SUBTYPE                                    | 변환을 위해 일치시킬 입력 MIME 하위 유형(와일드카드 허용)입니다. 이 필드가 본문 부분의 MIME 하위 유형과 일치하는 경우에만 이 항목에 지정된 변환이 수행됩니다.                                                                                    |
| IN-PARAMETER-NAME- <i>n</i>                   | 변환을 위해 일치해야 하는 입력 MIME Content-Type 매개 변수 이름입니다 ( <i>n</i> = 0, 1, 2...) 이 매개 변수를 IN-PARAMETER-VALUE- <i>n</i> 과 함께 사용하여 이름 및 보유한 값을 기준으로 매개 변수를 명확하게 식별할 수 있습니다.                  |
| IN-PARAMETER-VALUE- <i>n</i>                  | 변환을 위해 일치해야 하는 해당 IN-PARAMETER-NAME의 입력 MIME Content-Type 매개 변수 값입니다. 이 필드가 본문 부분의 Content-Type 매개 변수 목록에 있는 해당 매개 변수와 일치하는 경우에만 이 항목에 지정된 변환이 수행됩니다. 와일드카드가 허용됩니다.                |
| IN-PARAMETER-DEFAULT- <i>n</i>                | 매개 변수가 없는 경우 입력 MIME Content-Type 매개 변수의 기본값입니다. 이 값은 해당 매개 변수가 본문 부분에 지정되어 있지 않은 경우 IN-PARAMETER-VALUE- <i>n</i> 테스트를 위한 기본값으로 사용됩니다.                                             |
| IN-DISPOSITION                                | 변환을 위해 일치시킬 입력 MIME Content-Disposition입니다.                                                                                                                                        |
| IN-DPARAMETER-NAME- <i>n</i>                  | 변환을 위해 일치해야 하는 입력 MIME Content-Disposition 매개 변수 이름입니다( <i>n</i> = 0, 1, 2...). 이 매개 변수를 IN-DPARAMETER-VALUE- <i>n</i> 과 함께 사용하여 이름 및 보유한 값을 기준으로 매개 변수를 명확하게 식별할 수 있습니다.          |
| IN-DPARAMETER-VALUE- <i>n</i>                 | 변환을 위해 일치해야 하는 해당 IN-DPARAMETER-NAME의 입력 MIME Content-Disposition 매개 변수 값입니다. 이 필드가 본문 부분의 Content-Disposition 매개 변수 목록에 있는 해당 매개 변수와 일치하는 경우에만 이 항목에 지정된 변환이 수행됩니다. 와일드카드가 허용됩니다. |
| IN-DPARAMETER-DEFAULT- <i>n</i>               | 매개 변수가 없는 경우의 입력 MIME Content-Disposition 매개 변수의 기본값입니다. 이 값은 해당 매개 변수가 본문 부분에 지정되어 있지 않은 경우 IN-DPARAMETER-VALUE- <i>n</i> 테스트를 위한 기본값으로 사용됩니다.                                    |
| IN-DESCRIPTION                                | 변환을 위해 일치시킬 입력 MIME Content-Description입니다.                                                                                                                                        |
| IN-SUBJECT                                    | 포함 MESSAGE/RFC822 부분에서 가져온 입력 Subject입니다.                                                                                                                                          |

**표 13-6** 변환 매개 변수 (계속)

| 매개 변수                                 | 설명                                                                                                                                                                                                                                                                                                   |
|---------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| TAG                                   | 메일 목록 CONVERSION_TAG 매개 변수에 의해 설정되는 입력 태그입니다.                                                                                                                                                                                                                                                        |
| <b>출력 매개 변수(본문 부분의 변환 후 출력 설정 지정)</b> |                                                                                                                                                                                                                                                                                                      |
| OUT-TYPE                              | 입력 유형과 다른 경우의 출력 MIME 유형입니다.                                                                                                                                                                                                                                                                         |
| OUT-SUBTYPE                           | 입력 하위 유형과 다른 경우의 출력 MIME 하위 유형입니다.                                                                                                                                                                                                                                                                   |
| OUT-PARAMETER-NAME- <i>n</i>          | 출력 MIME Content-Type 매개 변수 이름입니다( <i>n</i> = 0, 1, 2...).                                                                                                                                                                                                                                            |
| OUT-PARAMETER-VALUE- <i>n</i>         | OUT-PARAMETER-NAME- <i>n</i> 에 해당하는 출력 MIME Content-Type 매개 변수 값입니다.                                                                                                                                                                                                                                 |
| PARAMETER-COPY- <i>n</i>              | 입력 본문 부분의 Content-Type 매개 변수 목록에서 출력 본문 부분의 Content-Type: 매개 변수 목록에 복사할 Content-Type:매개 변수 목록입니다( <i>n</i> =0, 1, 2...). IN-PARAMETER-NAME- <i>n</i> 절과 일치할 경우 동일한 MIME 매개 변수 이름을 사용하여 복사합니다.                                                                                                        |
| OUT-DISPOSITION                       | 입력 MIME Content-Disposition과 다른 경우의 출력 MIME Content-Disposition입니다.                                                                                                                                                                                                                                  |
| OUT-DPARAMETER-NAME- <i>n</i>         | 출력 MIME Content-Disposition 매개 변수 이름입니다( <i>n</i> =0, 1, 2...).                                                                                                                                                                                                                                      |
| OUT-DPARAMETER-VALUE- <i>n</i>        | OUT-DPARAMETER-NAME- <i>n</i> 에 해당하는 출력 MIME Content-Disposition 매개 변수 값입니다.                                                                                                                                                                                                                         |
| DPARAMETER-COPY- <i>n</i>             | 입력 본문 부분의 Content-Disposition: 매개 변수 목록에서 출력 본문 부분의 Content-Disposition: 매개 변수 목록에 복사할 Content-Disposition: 매개 변수 목록입니다( <i>n</i> = 0, 1, 2,...). IN-PARAMETER-NAME- <i>n</i> 절과 일치할 경우 MIME 매개 변수 이름을 인수로 사용하여 복사합니다. 와일드카드를 인수로 사용할 수 있습니다. 특히 * 인수는 모든 원본 Content-Disposition: 매개 변수를 복사함을 의미합니다. |
| OUT-DESCRIPTION                       | 입력 MIME Content-Description과 다른 경우의 출력 MIME Content-Description입니다.                                                                                                                                                                                                                                  |
| OUT-MODE                              | 변환된 파일을 읽고 저장하는 데 사용하는 모드입니다. BLOCK(이진 및 실행 파일) 또는 TEXT이어야 합니다.                                                                                                                                                                                                                                      |
| OUT-ENCODING                          | 메일을 다시 어셈블할 때 변환된 파일에 적용할 인코딩입니다.                                                                                                                                                                                                                                                                    |
| <b>작업 매개 변수(메일 부분에서 수행할 작업 지정)</b>    |                                                                                                                                                                                                                                                                                                      |
| COMMAND                               | 변환을 수행하기 위해 실행할 명령입니다. 변환을 수행하기 위해 실행할 명령입니다. 이 매개 변수는 필수입니다. 명령을 지정하지 않으면 항목이 무시됩니다. \대신 /를 사용하여 경로를 지정합니다(예: command="D:/tmp/mybat.bat").                                                                                                                                                          |
| DELETE                                | 0 또는 1입니다. 이 플래그를 설정하면 메일 부분이 삭제됩니다. 이 부분이 메일의 유일한 부분인 경우 빈 단일 텍스트 부분이 대체됩니다.                                                                                                                                                                                                                        |

**표 13-6** 변환 매개 변수 (계속)

| 매개 변수                                                  | 설명                                                                                                                                                                                                                                                                                                                                |
|--------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| RELABEL                                                | RELABEL=1인 경우 MIME 레이블을 출력 매개 변수에 지정된 레이블로 다시 지정합니다. Relabel=0인 경우에는 레이블을 다시 지정하지 않습니다. 일반적으로 레이블 다시 지정은 레이블이 잘못 지정된 부분에서 수행됩니다. 예를 들어, Content-type: application/octet-stream에서 Content-type: application/msword로 레이블을 다시 지정합니다. 그렇게 하면 해당 부분을 파일로 저장하여 프로그램에서 열 필요 없이 해당 부분을 "두 번 놀러" 열 수 있습니다.                                 |
| SERVICE-COMMAND                                        | SERVICE-COMMAND=command는 전체 MIME 메일(MIME 헤더 및 내용 본문 부분)에 적용할 사이트에서 제공하는 절차를 실행합니다. 다른 CHARSET-CONVERSION 작업 또는 변환 채널 작업과 달리 service-command는 MIME 디스어셈블리, 디코딩, 재인코딩 및 리어셈블리를 자체적으로 수행합니다. 이 플래그는 변환 채널을 처리하는 동안 항목이 무시되게 합니다. SERVICE-COMMAND 항목은 문자 세트 변환 처리 중에 대신 수행됩니다. \대신 /를 사용하여 경로를 지정합니다(예: command="D: /tmp/mybat.bat"). |
| <b>정보 전달 매개 변수(사이트에서 제공하는 프로그램을 통해 정보를 전달하는 데 사용됨)</b> |                                                                                                                                                                                                                                                                                                                                   |
| DPARAMETER-SYMBOL- <i>n</i>                            | Content-disposition 매개 변수 값(있는 경우)이 저장되는 환경 변수입니다( <i>n</i> = 0, 1, 2,...). 각 DPARAMETER-SYMBOL- <i>n</i> 은 Content-Disposition: 매개 변수 목록에서 순서대로( <i>n</i> =0이 첫 번째 매개 변수, <i>n</i> =2가 두 번째 매개 변수 등) 추출되어 사이트에서 제공하는 프로그램을 실행하기 전에 지정된 환경 변수에 저장됩니다.                                                                             |
| PARAMETER-SYMBOL- <i>n</i>                             | Content-Type 매개 변수 값(있는 경우)이 저장되는 환경 변수입니다( <i>n</i> = 0, 1, 2,...). 각 PARAMETER-SYMBOL- <i>n</i> 은 Content-Type: 매개 변수 목록에서 순서대로( <i>n</i> =0이 첫 번째 매개 변수, <i>n</i> =2가 두 번째 매개 변수, 등) 추출되어 사이트에서 제공하는 프로그램을 실행하기 전에 동일한 이름의 환경 변수에 저장됩니다. IN-PARAMETER-NAME- <i>n</i> 결과 일치할 경우 MIME 매개 변수를 변환할 변수 이름을 인수로 사용합니다.               |
| MESSAGE-HEADER-FILE                                    | 메일 원본 헤더의 모두 또는 일부를 MESSAGE_HEADERS 환경 변수에서 지정한 파일에 쓰거나 전혀 쓰지 않습니다. 이 값을 1로 설정하면 포함된 본문 부분의 원본 헤더를 MESSAGE_HEADERS 환경 변수에서 지정한 파일에 씁니다. 이 값을 2로 설정하면 메일 원본 헤더(가장 바깥에 있는 메일 헤더) 전체를 해당 파일에 씁니다.                                                                                                                                    |
| ORIGINAL-HEADER-FILE                                   | 0 또는 1입니다. 이 값을 1로 설정하면 포함된 MESSAGE/RFC822 부분(본문 부분이 아님)의 원본 헤더를 ORIGINAL_HEADERS 환경 변수에 표시된 파일에 씁니다.                                                                                                                                                                                                                             |
| OVERRIDE-HEADER-FILE                                   | 0 또는 1입니다. 이 값을 1로 설정하는 경우 변환 채널은 포함된 MIME 부분의 원본 헤더 행을 무시하고 OUTPUT_HEADERS 환경 변수에서 MIME 헤더 행을 읽습니다.                                                                                                                                                                                                                              |
| OVERRIDE-OPTION-FILE                                   | OVERRIDE-OPTION-FILE=1인 경우 변환 채널은 OUTPUT_OPTIONS 환경 변수에서 옵션을 읽습니다.                                                                                                                                                                                                                                                                |
| PART-NUMBER                                            | 점으로 구분된 정수( <i>a. b. c...</i> )입니다. MIME 본문 부분의 부품 번호입니다.                                                                                                                                                                                                                                                                         |

## 문자 세트 변환 및 메일 형식 다시 지정

이 절에서는 MTA에서 내부적으로 수행한 문자 집합과 형식 지정, 레이블 지정의 변환에 대해 설명합니다. 이 절에 나와 있는 예 중 일부는 DEC VMS 같이 오래되었거나 더 이상 사용되지 않는 기술 또는 a 채널을 사용합니다. 이러한 기술이 오래된 것이라 해도 DEC 나 a 채널에만 사용되는 예를 제시한 것은 아니며 변환 기술의 작동 방법을 설명하는 데 있어서는 여전히 유효한 예라 할 수 있습니다. 향후 릴리스에서는 이러한 예를 업데이트 할 예정입니다.

Messaging Server의 가장 기본적인 매핑 테이블 중 하나는 문자 세트 변환 테이블입니다. 이 테이블의 이름은 CHARSET-CONVERSION입니다. 이 테이블은 수행할 채널 간 문자 세트 변환 및 메일 형식 다시 지정 종류를 지정하는 데 사용됩니다.

여러 시스템에서는 문자 세트 변환 또는 메일 형식 다시 지정을 수행할 필요가 없으므로 이 테이블이 필요하지 않습니다. 그러나, 문자 변환을 수행해야 하는 상황이 발생할 수 있습니다. 예를 들어 일본어 OpenVMS를 실행하는 사이트는 DEC Kanji와 현재 인터넷에서 사용되는 ISO-2022 Kanji 사이에 변환해야 할 필요가 있습니다. 변환이 사용될 또 다른 경우로서, 다국어 문자가 너무 많이 사용되었기 때문에 DEC 다국어 문자 집합 (DEC-MCS)과 MIME에 사용되도록 지정된 ISO-8859-1 문자 집합 사이에 약간의 차이가 발생할 수 있고 이 두 집합 간에 실제 변환이 필요할 수 있습니다.

또한 CHARSET-CONVERSION 매핑 테이블을 사용하여 메일의 형식을 변경할 수도 있습니다. 많은 비MIME 형식을 MIME 형식으로 변환하는 기능이 제공됩니다. 또한 MIME 인코딩과 구조를 변경할 수 있습니다. 이러한 옵션은 MIME 또는 MIME의 일부 하위 집합만 지원하는 시스템에 메일을 릴레이할 때 사용됩니다. 마지막으로 MIME를 비MIME 형식으로 변환하는 기능이 제공되는 경우도 가끔씩 있습니다.

MTA는 다음과 같은 두 가지 방법으로 CHARSET-CONVERSION 매핑 테이블을 감시합니다. 첫 번째 감시 방법은 MTA가 메일 형식을 다시 지정해야 하는지 여부를 확인하고 그렇게 해야 할 경우 사용할 형식 지정 옵션을 결정하는 데 사용됩니다. 형식 다시 지정을 지정하지 않으면 MTA는 특정 문자 세트 변환을 확인하지 않습니다. 이 첫 번째 감시 방법에 사용되는 입력 문자열의 형식은 일반적으로 다음과 같습니다.

```
IN-CHAN=in-channel; OUT-CHAN=out-channel; CONVERT
```

여기서 *in-channel*은 소스 채널(메일을 가져온 채널)의 이름이고 *out-channel*은 대상 채널(메일이 이동하는 채널)의 이름입니다. 일치가 발생할 경우 쉼표로 구분된 키워드 목록이 결과 문자열로 표시됩니다. 키워드는 표 13-7에 나열되어 있습니다.

표 13-7 HARSET-CONVERSION 매핑 테이블 키워드

| 키워드              | 설명                                                                                                                         |
|------------------|----------------------------------------------------------------------------------------------------------------------------|
| Always           | <i>out-channel</i> 로 이동하기 전에 변환 채널을 통해 메일을 전달하더라도 변환을 수행합니다.                                                               |
| Appledouble      | 다른 MacMIME 형식을 Appledouble 형식으로 변환합니다.                                                                                     |
| Applesingle      | 다른 MacMIME 형식을 Applesingle 형식으로 변환합니다.                                                                                     |
| BASE64           | MIME 인코딩을 BASE64로 전환합니다. 이 키워드는 이미 인코딩된 메일 부분에만 적용됩니다. 7비트 또는 8비트를 가진 메일은 특수한 인코딩이 필요하지 않으므로 이 BASE64 옵션이 아무 영향을 미치지 않습니다. |
| Binhex           | 다른 MacMIME 형식 또는 Macintosh 유형 및 Mac 작성자 정보를 포함하는 부분을 Binhex 형식으로 변환합니다.                                                    |
| Block            | MacMIME 형식 부분에서 데이터 포크만 추출합니다.                                                                                             |
| Bottom           | 메일/rfc822 본문 부분(전달된 메일)을 메일 내용 부분과 헤더 부분으로 "결합"합니다.                                                                        |
| Delete           | 전달된 헤더를 삭제하여 메일/rfc822 본문 부분(전달된 메일)을 메일 내용 부분으로 "결합"합니다.                                                                  |
| 수준               | 메일에서 중복 멀티파트 수준을 제거합니다.                                                                                                    |
| Macbinary        | 다른 MacMIME 형식 또는 Macintosh 유형 및 Macintosh 작성자 정보를 포함하는 부분을 Macbinary 형식으로 변환합니다.                                           |
| 아니요              | 변환을 비활성화합니다.                                                                                                               |
| QUOTED-PRINTABLE | MIME 인코딩을 QUOTED-PRINTABLE로 전환합니다.                                                                                         |
| Record,Text      | 텍스트/일반 부분을 80자에서 줄 바꿈합니다.                                                                                                  |
| Record,Text= n   | 텍스트/일반 부분을 n자에서 줄 바꿈합니다.                                                                                                   |
| RFC1154          | 메일을 RFC 1154 형식으로 변환합니다.                                                                                                   |
| Top              | 메일/rfc822 본문 부분(전달된 메일)을 헤더 부분과 메일 내용 부분으로 "결합"합니다.                                                                        |
| UUENCODE         | MIME 인코딩을 X-UUENCODE로 전환합니다.                                                                                               |
| 예                | 변환을 활성화합니다.                                                                                                                |

## 문자 세트 변환

MTA가 메일 형식을 다시 지정해야 하는지를 감시하여 발견하는 경우 메일의 각 부분을 확인합니다. 텍스트 부분이 있으면 해당 문자 세트 매개 변수를 사용하여 두 번째 감시를 생성합니다. MTA는 변환이 필요하다고 확인된 경우에만 두 번째 감시를 수행합니다. 이 두 번째 감시의 입력 문자열은 다음과 같습니다.

`IN-CHAN=in-channel; OUT-CHAN=out-channel; IN-CHARSET=in-char-set`

`in-channel` 및 `out-channel`은 앞의 예와 동일하고 `in-char-set`은 문제가 있는 특정 부분과 연결된 문자 세트의 이름입니다. 첫 번째 감시에서 키워드가 일치하여 메일 형식이 다시 지정(예: MIME 구조 변경)되더라도 이 두 번째 감시에서 일치 항목이 발견되지 않으면 문자 세트 변환이 수행되지 않습니다. 일치 항목이 발견될 경우 다음과 같은 형식의 문자열이 생성됩니다.

`OUT-CHARSET=out-char-set`

여기서 `out-char-set`은 `in-char-set`를 변환해야 하는 문자 세트의 이름을 지정합니다. 이러한 문자 세트는 모두 MTA 테이블 디렉토리에 있는 문자 세트 정의 테이블 `charsets.txt`에서 정의해야 합니다. 문자 세트를 이 파일에 제대로 정의하지 않으면 변환이 수행되지 않습니다. 이 파일에는 수 백개의 문자 세트가 정의되어 있고 현재 사용 중인 대부분의 문자 세트가 이 파일에 정의되어 있기 때문에 이러한 경우는 흔하지 않습니다. `charsets.txt` 파일에 대한 자세한 내용은 `imsimta chbuild(UNIX 및 NT)` 유틸리티 설명을 참조하십시오.

모든 조건이 충족되면 MTA는 문자 세트 매핑을 작성하고 변환을 수행합니다. 변환된 메일 부분의 레이블은 변환된 문자 세트의 이름으로 다시 지정됩니다.

Charset-conversion 매핑이 확장되어 다음과 같은 여러 추가 기능을 제공합니다.

- IN-CHARSET 옵션은 매핑 항목의 출력 템플릿에서 지정할 수 있습니다. 이 옵션이 있을 경우 인코딩된 단어에서 지정된 문자 세트를 무시합니다.
- 정수 0 또는 1을 가지는 RELABEL-ONLY 옵션을 지정할 수 있습니다. 이 옵션의 값이 1인 경우 OUT-CHARSET은 단순히 IN-CHARSET를 대체하고 레이블을 다시 지정하지는 않습니다.
- IN-CHARSET 옵션을 사용하여 입력 문자 세트를 \*로 설정하면 문자 세트가 "감지되어" 적절한 레이블이 결정됩니다.



## 예: ISO-8859-1과 UTF-8 사이의 변환

로컬로 ISO-8859-1가 사용된다고 할 때, 인터넷에서 사용하기 위해서는 UTF-8로 변환되어야 합니다. 특히, 인터넷 연결이 tcp\_local을 통한 것이라고 가정할 때 tcp\_internal과 ims-ms는 내부 메시지가 만들어져 전달되는 위치입니다. 아래는 그러한 변환을 일으키는 CHARSET-CONVERSION 표입니다.

| CHARSET-CONVERSION                                            |                        |
|---------------------------------------------------------------|------------------------|
| IN-CHAN=tcp_internal;OUT-CHAN=tcp_local;CONVERT               | Yes                    |
| IN-CHAN=tcp_local;OUT-CHAN=tcp_internal;CONVERT               | Yes                    |
| IN-CHAN=tcp_local;OUT-CHAN=ims-ms;CONVERT                     | Yes                    |
| IN-CHAN=*;OUT-CHAN=*;CONVERT                                  | No                     |
| IN-CHAN=tcp_internal;OUT-CHAN=tcp_local;IN-CHARSET=ISO-8859-1 | OUT-CHARSET=UTF-8      |
| IN-CHAN=tcp_local;OUT-CHAN=tcp_internal;IN-CHARSET=UTF-8      | OUT-CHARSET=ISO-8859-1 |
| IN-CHAN=tcp_local;OUT-CHAN=ims-ms;IN-CHARSET=UTF-8            | OUT-CHARSET=ISO-8859-1 |

## 예: EUC-JP와 ISO-2022-JP 사이의 변환

아래 CHARSET-CONVERSION 표는 EUC-JP의 로컬 사용과 ISO 2022 기반 JP 코드 사이의 변환을 지정합니다.

| CHARSET-CONVERSION                                     |                         |
|--------------------------------------------------------|-------------------------|
| IN-CHAN=ims-ms;OUT-CHAN=ims-ms;CONVERT                 | No                      |
| IN-CHAN=tcp_internal;OUT-CHAN=ims-ms;CONVERT           | No                      |
| IN-CHAN=tcp_internal;OUT-CHAN=tcp_internal;CONVERT     | No                      |
| IN-CHAN=tcp_internal;OUT-CHAN=*;CONVERT                | Yes                     |
| IN-CHAN=*;OUT-CHAN=ims-ms;CONVERT                      | YES                     |
| IN-CHAN=*;OUT-CHAN=tcp_internal;CONVERT                | Yes                     |
| IN-CHAN=tcp_internal;OUT-CHAN=*;IN-CHARSET=EUC-JP      | OUT-CHARSET=ISO-2022-JP |
| IN-CHAN=*;OUT-CHAN=ims-ms;IN-CHARSET=ISO-2022-JP       | OUT-CHARSET=EUC-JP      |
| IN-CHAN=*;OUT-CHAN=tcp_internal;IN-CHARSET=ISO-2022-JP | OUT-CHARSET=EUC-JP      |

## 메일 형식 다시 지정

위에서 설명한 것처럼 CHARSET-CONVERSION 매핑 테이블은 MIME과 여러 해당 메일 형식 사이에서 첨부 파일을 변환하는 데도 사용됩니다.

다음 절에서는 CHARSET-CONVERSION 매핑 테이블에서 적용할 수 있는 메일 형식 다시 지정의 몇 가지 다른 예를 제공합니다.

## 비MIME 이진 첨부 파일 변환

특정 형식의 메일 또는 Microsoft Mail(MSMail) SMTP 게이트웨이에서 가져온 메일 등과 같은 특정 비 표준(비MIME) 형식 메일은 메일 처리에 관계된 채널에 대해 CHARSET-CONVERSION을 활성화할 경우 MIME 형식으로 자동으로 변환됩니다. tcp\_local 채널은 일반적으로 Microsoft Mail SMTP 게이트웨이를 통해 가져온 메일에 대한 수신 채널이며, 다음은 로컬 사용자에게 전달된 메일에 대한 변환을 활성화합니다.

CHARSET-CONVERSION

```
IN-CHAN=tcp_local;OUT-CHAN=ims-ms;CONVERT Yes
```

또한 채널에 대한 항목을 다른 로컬 메일 시스템에 추가하려고 할 수 있습니다. 예를 들어 다음은 tcp\_internal 채널에 대한 항목입니다.

CHARSET-CONVERSION

```
IN-CHAN=tcp_local;OUT-CHAN=l;CONVERT Yes
IN-CHAN=tcp_local;OUT-CHAN=tcp_internal;CONVERT Yes
```

모든 채널을 포함하려면 OUT-CHAN=ims-ms 대신 OUT-CHAN=\*를 지정하면 됩니다. 그러나, 이렇게 하면 tcp\_local 채널에 수신되는 모든 메일을 특정 채널에 바운드하지 않고 꼼꼼하게 검사하게 되므로 메일 처리 오버헤드가 증가할 수 있습니다.

무엇보다도 그러한 무분별한 변환은 시스템을 통해 단순히 전달하기만 하면 되는(메일 봉투와 관련 전송 정보 이외에 다른 변환을 수행할 필요 없이 단순히 전송만 하면 되는 상황) 변환 메일로 인해 시스템이 정렬되지 않은 복잡한 상태로 될 수 있습니다(사용자의 시스템은 그렇지 않을 수도 있음).

MIME를 Microsoft Mail SMTP 게이트웨이에서 인식할 수 있는 형식으로 변환하려면 Microsoft Mail SMTP 게이트웨이에 대한 MTA 구성에서 별도의 채널(예: tcp\_msmail)을 사용하고 매핑 파일에 다음을 입력합니다.

CHARSET-CONVERSION

```
IN-CHAN=*;OUT-CHAN=tcp_msmail;CONVERT RFC1154
```

## MIME 헤더 레이블 다시 지정

일부 사용자 에이전트 또는 게이트웨이에서는 내용에 비해 부족하지만 세부 MIME 헤더를 구성하는 데는 충분한 정보를 제공하는 MIME 헤더를 사용하여 메일을 보낼 수 있습니다. 그러한 사용자 에이전트 또는 게이트웨이를 적절하게 구성하는 것이 가장 좋지만 해당 구성을 직접 제어할 수 없는 경우 MIME 헤더를 보다 유용하게 다시 구성하도록 MTA에 요청할 수 있습니다.

CHARSET-CONVERSION 매핑 테이블에 대한 첫 번째 감시에서 Yes 또는 Always 키워드를 생성하는 경우 MTA는 conversions 파일이 있는지를 확인합니다. 변환 파일이 있는 경우 MTA는 해당 파일에서 RELABEL=1인 항목을 조사하여 그런 항목이 있는 경우 해당 항목에 지정된 MIME 레이블 다시 지정을 수행합니다. 변환 파일 항목에 대한 자세한 내용은 [414 페이지](#)의 "변환 처리 제어"를 참조하십시오.

예를 들어 다음과 같은 CHARSET-CONVERSION 테이블과

|                                                 |     |
|-------------------------------------------------|-----|
| CHARSET-CONVERSION                              |     |
| IN-CHAN=tcp_local;OUT-CHAN=tcp_internal;CONVERT | Yes |

### MTA 변환 파일 항목

|                                                                                                                                                                                                                                                                                                                                                                                                           |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre> out-chan=ims-ms; in-type=application; in-subtype=octet-stream; in-parameter-name-0=name; in-parameter-value-0=*.ps; out-type=application; out-subtype=postscript; parameter-copy-0=*; relabel=1  out-chan=ims-ms; in-type=application; in-subtype=octet-stream; in-parameter-name-0=name; in-parameter-value-0=*.msw; out-type=application; out-subtype=msword; parameter-copy-0=* relabel=1 </pre> |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

을 조합하면 tcp\_local 채널에 도착하고 ims-ms 채널에 라우팅된 메일이 나타나게 되는데, 이는 원래 application/octet-stream이라는 MIME 레이블 지정을 사용하여 도착하되 파일 이름 매개 변수에 ps 또는 msw라는 확장명이 있는 메일로서 각각 application/postscript 또는 application/msword라는 레이블이 붙여집니다. 이러한 보다 세부적인 레이블 지정은 원본 사용자 에이전트 또는 게이트웨이에서 수행되었어야 하는 내용입니다. 이러한 레이블 다시 지정은 MIME-CONTENT-TYPES-TO-MR 매핑 테이블과 함께 사용할 때 특히 유용합니다. MIME-CONTENT-TYPES-TO-MR 매핑 테이블은 결과로 나타나는 MIME 형식을 다시 적합한 MRTYPE 태그로 변환하는 데 사용되며 해당 태그가 최적 상태로 기능하기 위해서는 MIME 레이블을 정확히 지정해야 합니다. 모든 내용 유형에 application/octet-stream으로만 레이블이 지정된 경우에는 MIME-CONTENT-TYPES-TO-MR 매핑 테이블은 모든 형식을 무조건 MRTYPE이라는 한 가지 태그로만 변환할 수 있습니다. 위의 예와 함께 다음이 포함된 MIME-CONTENT-TYPES-TO-MR 매핑 테이블 항목을 사용할 때

```
APPLICATION/POSTSCRIPT      PS
APPLICATION/MSWORD           MW
```

레이블 지정을 수행하면

```
Content-type: application/octet-stream; name=stuff.ps
```

다음과 같이 레이블이 다시 지정되고

```
Content-type: application/postscript
```

MRTYPE 태그로 변환됨으로써 PS 메일 라우터가 PostScript를 예상할 수 있게 됩니다.

일반 이진 데이터에 대해 반대 방향으로 레이블 다시 지정(특정 MIME 첨부 파일 레이블 지정을 `application/octet-stream`으로 "다운그레이드")하는 것이 유용할 경우가 있습니다. 특히, 특정 MIME 레이블 지정을 "다운그레이드"하는 것은 `mime_to_x400` 채널 (PMDF-X400) 또는 `xapi_local` 채널 (PMDF-MB400)의 `convert_octet_stream` 채널 키워드와 함께 사용하여 모든 이진 MIME 첨부 파일을 X.400 bodypart 14 형식으로 강제 설정하는 경우가 많습니다.

예를 들어, 아래와 같은 CHARSET-CONVERSION 매핑 테이블과

```
CHARSET-CONVERSION
```

```
IN-CHAN=*;OUT-CHAN=mime_to_x400*;CONVERT      Yes
```

다음 PMDF 변환 파일 항목을

```
out-chan=mime_to_x400*; in-type=application; in-subtype=*;
out-type=application; out-subtype=octet-stream; relabel=1
```

```
out-chan=mime_to_x400*; in-type=audio; in-subtype=*;
out-type=application; out-subtype=octet-stream; relabel=1
```

```
out-chan=mime_to_x400*; in-type=image; in-subtype=*;
out-type=application; out-subtype=octet-stream; relabel=1
```

```
out-chan=mime_to_x400*; in-type=video; in-subtype=*;
out-type=application; out-subtype=octet-stream; relabel=1
```

조합하면 mime\_to\_x400\* 채널로 가는 모든 메일에 대해 특정 MIME 첨부 파일 레이블 지정이 일반 application/octet-stream 레이블 지정으로 다운그레이드되고 그에 따라 convert\_octet\_stream이 적용됩니다.

## MacMIME 형식 변환

Macintosh 파일에는 Macintosh 특정 정보가 들어 있는 자원 포크와 다른 플랫폼에서 사용 가능한 데이터가 들어 있는 데이터 포크의 두 부분이 있습니다. 따라서, Macintosh 파일 전송은 더욱 복잡하게 수행됩니다. Macintosh 파일 부분 전송에는 서로 다른 네 가지 형식이 공통적으로 사용됩니다. Applesingle, Binhex 및 Macbinary의 세 형식은 한 부분으로 함께 인코딩되는 Macintosh 자원 포크와 Macintosh 데이터 포크로 구성됩니다. 네 번째 형식인 Appledouble은 자원 포크와 데이터 포크가 별도의 부분에 존재하는 멀티파트 형식입니다. 따라서, Appledouble이 Macintosh 이외의 플랫폼에 가장 유용한 형식입니다. 이 경우 비 Macintosh 응용 프로그램에서는 자원 포크 부분은 무시하고 데이터 포크 부분만 사용할 수 있습니다. 다른 형식은 Macintoshes에 메일을 보낼 경우에 특히 유용합니다.

MTA는 이러한 다양한 Macintosh 형식을 변환할 수 있습니다. CHARSET-CONVERSION 키워드 Appledouble, Applesingle, Binhex 또는 Macbinary는 다른 MacMIME 구조 부분을 각각 multipart/appledouble, application/applefile, application/mac-binhex40 또는 application/macbinary MIME 구조로 변환하도록 MTA에 지시합니다. 또한 Binhex 또는 Macbinary 키워드는 MIME Content-type: 헤더에 X-MAC-TYPE 및 X-MAC-CREATOR 매개 변수를 포함하는 비 MacMIME 형식 부분의 지정된 형식으로 변환하도록 요청합니다. CHARSET-CONVERSION 키워드 Block은 MacMIME 형식 부분에서 자원 포크는 삭제하고 데이터 포크만 추출하도록 MTA에 지시합니다. 이렇게 하면 정보가 손실되므로 일반적으로 Appledouble을 사용하는 것이 좋습니다.

예를 들어 다음 CHARSET-CONVERSION 테이블은 MTA에게 VMS MAIL 메일함이나 GroupWise 사서함으로 전달할 때는 Appledouble 형식으로 변환하고 메일 라우터 채널로 전달할 때는 Macbinary 형식으로 변환하도록 명령합니다.

CHARSET-CONVERSION

```
IN-CHAN=*;OUT-CHAN=1;CONVERT           Appledouble
IN-CHAN=*;OUT-CHAN=wpo_local;CONVERT    Appledouble
IN-CHAN=*;OUT-CHAN=tcp_internal;CONVERT  Macbinary
```

Appledouble 형식에서의 변환은 이미 MacMIME 형식 중 하나로 된 부분에만 적용됩니다. Macbinary 형식에서의 변환은 이미 MacMIME 형식 중 하나로 된 부분에만 적용되거나 X-MAC-TYPE 및 X-MAC-CREATOR 매개 변수를 MIME Content-type: 헤더에 포함한 비MacMIME 부분에만 적용됩니다.

Appledouble 또는 Block 형식으로 변환할 경우 MAC-TO-MIME-CONTENT-TYPES 매핑 테이블을 사용하여 원본 Macintosh 파일의 Macintosh 작성자 및 Macintosh 입력 정보에 따라 Appledouble 부분 또는 Block 부분의 데이터 포크에 넣을 특정 MIME 레이블을 지정할 수 있습니다. 이 테이블의 검사에는 *format|type|creator|filename*이라는 형식이 사용되는데 여기서 format은 SINGLE, BINHEX 또는 MACBINARY 중 하나이고 type 및 creator는 각각 16진수인 Macintosh 유형 및 Macintosh 작성자 정보이며 filename은 파일 이름입니다.

예를 들어, ims-ms 채널에 보낼 때 MACBINARY 또는 BINHEX 부분에서 변환된 MS Word 또는 PostScript 문서에 대해 특정 MIME 레이블을 사용하도록 Appledouble로 변환하는 테이블은 다음과 같습니다.

|                                   |                           |
|-----------------------------------|---------------------------|
| CHARSET-CONVERSION                |                           |
| IN-CHAN=*;OUT-CHAN=ims-ms;CONVERT | Appledouble               |
| MAC-TO-MIME-CONTENT-TYPES         |                           |
| ! PostScript                      |                           |
| MACBINARY 45505346 76677264 *     | APPLICATION/POSTSCRIPT\$Y |
| BINHEX 45505346 76677264 *        | APPLICATION/POSTSCRIPT\$Y |
| ! Microsoft Word                  |                           |
| MACBINARY 5744424E 4D535744 *     | APPLICATION/MSWORD\$Y     |
| BINHEX 5744424E 4D535744 *        | APPLICATION/MSWORD\$Y     |

매핑 항목의 템플릿(오른쪽)에는 지정된 레이블 지정을 수행하도록 설정된 \$Y 플래그가 있어야 합니다. 추가 첨부 파일 형식에 대한 샘플 항목은 MTA 테이블 디렉토리의 mac\_mappings.sample 파일을 참조하십시오.

비 MacMIME 형식 부분을 Binhex 또는 Macbinary 형식으로 변환하려면 해당 부분은(매개 변수 값이 있을 경우) X-MAC-TYPE 및 X-MAC-CREATOR MIME Content-type:을 가져야 합니다. MIME 레이블 다시 지정을 사용하여 해당 매개 변수가 없는 부분에 이러한 매개 변수를 제공할 수 있습니다.

## 서비스 변환

MTA의 변환 서비스 기능을 사용하면 사이트에서 제공하는 절차에 따라 메일을 처리하여 새로운 형식의 메일을 생성할 수 있습니다. 개별 MIME 메일 부분의 내용에 적용되는 위에서 설명한 CHARSET-CONVERSION 작업 또는 conversion 채널과 달리 변환 서비스는 전체 MIME 메일 부분(MIME 헤더 및 내용)과 전체 MIME 메일에 대해 수행됩니다. 다른 CHARSET-CONVERSION 작업 또는 변환 채널 작업과 달리 변환 서비스는 MIME 디스어셈블리, 디코딩, 재인코딩 및 리어셈블리를 자체적으로 수행합니다.

다른 CHARSET-CONVERSION 작업과 마찬가지로 변환 서비스도 CHARSET-CONVERSION 매핑 테이블을 통해 활성화됩니다. CHARSET-CONVESION 매핑 테이블에 대한 첫 번째 감시에서 Yes 또는 Always 키워드를 생성하는 경우 MTA는 MTA conversions 파일이 있는지를 확인합니다. conversions 파일이 있는 경우 MTA는 해당 파일에서 SERVICE-COMMAND를 지정하는 항목을 조사하여 그러한 항목이 발견되면 해당 항목을 실행합니다.

conversions 파일 항목의 형식은 다음과 같습니다.

```
in-chan=channel-pattern;
in-type=type-pattern; in-subtype=subtype-pattern;
service-command=command
```

핵심적인 사항은 명령 문자열입니다. 명령 문자열은 서비스 변환을 수행하기 위해 실행해야 하는 명령(예: 문서 변환기 호출)입니다. 명령은 서비스를 제공할 메일 텍스트가 들어 있는 입력 파일을 처리하여 새 메일 텍스트가 포함된 출력 파일을 생성해야 합니다. UNIX에서 명령은 성공할 경우 0으로 끝나고 그렇지 않은 경우 0이 아닌 다른 값으로 끝납니다.

예를 들어, 아래와 같은 CHARSET-CONVERSION 테이블과

```
CHARSET-CONVERSION
```

```
IN-CHAN=bsout_*;OUT-CHAN=*;CONVERT Yes
```

다음의 UNIX MTA conversions 파일 항목을

```
in-chan=bsout_*; in-type=*; in-subtype=*;
service-command="/pmdf/bin/compress.sh compress $INPUT_FILE $OUTPUT_FILE"
```

조합하면 BSOUT 채널의 모든 메일이 압축됩니다.

환경 변수는 메일의 봉투 수신자 주소 목록이 포함된 파일 이름과 입력 및 출력 파일의 이름을 전달하는 데 사용됩니다. 이러한 환경 변수의 이름은 다음과 같습니다.

- INPUT\_FILE - 처리할 입력 파일의 이름
- OUTPUT\_FILE - 처리할 출력 파일의 이름
- INFO\_FILE - 봉투 수신자 주소가 포함된 파일의 이름

표준 명령줄 대체를 사용하여 이러한 세 환경 변수 값을 명령줄로 대체할 수 있습니다.

UNIX의 경우 변수 이름 앞에 \$ 문자를 표시합니다. 예를 들어 INPUT\_FILE과 OUTPUT\_FILE에 a.in 및 a.out 값이 있을 때 UNIX에서 다음 선언은

```
in-chan=bsout_*; in-type=*; in-subtype=*;  
service-command="/pmdf/bin/convert.sh $INPUT_FILE $OUTPUT_FILE"
```

다음 명령을 실행합니다.

```
/pmdf/bin/convert.sh a.in a.out
```



# Messaging Server에 스팸 및 바이러스 필터링 프로그램 통합

이 장에서는 스팸 및 바이러스 필터링 소프트웨어를 Messaging Server에 통합하고 구성하는 방법에 대해 설명합니다. 이 장에 설명되어 있는 스팸 및 바이러스 필터링 기술은 변환 채널(410페이지의 "변환 채널" 참조)에서 제공하는 기술보다 훨씬 강력합니다.

Messaging Server는 Symantec Brightmail AntiSpam, SpamAssassin 및 스팸 방지/바이러스 백신 프로그램을 지원합니다. 이러한 프로그램들은 ICAP(Internet Content Adaptation Protocol, RFC 3507), 특히 Symantec AntiVirus Scan Engine을 지원합니다.

---

**주** 이 장에서 스팸 방지 또는 스팸 필터링 기능은 바이러스 백신 또는 바이러스 필터링 기능을 의미하기도 합니다. 일부 제품(Brightmail)은 두 기능을 모두 제공하지만 다른 제품은 스팸 필터링만 제공하거나(SpamAssassin) 바이러스 필터링만 제공합니다(Symantec AntiVirus Scan Engine). 또한 일반적으로 구성 매개 변수에는 spam이 사용된다는 점에 유의하십시오.

---

이 장은 다음 내용으로 구성되어 있습니다.

- 442페이지의 "Messaging Server에 스팸 필터링 프로그램 통합—작동 원리"
- 442페이지의 "타사 스팸 필터링 프로그램 배포 및 구성"
- 455페이지의 "Symantec Brightmail 스팸 방지 사용"
- 459페이지의 "SpamAssassin 사용"
- 473페이지의 "SAVSE(Symantec Anti-virus Scanning Engine) 사용"
- 480페이지의 "Sieve 확장 지원"

# Messaging Server에 스팸 필터링 프로그램 통합—작동 원리

Messaging Server의 관점에서 스팸 방지 솔루션은 거의 동일한 기능을 수행합니다.

1. Messaging Server가 메일 복사본을 스팸 필터링 소프트웨어로 보냅니다.
2. 스팸 필터링 소프트웨어가 메일을 분석하여 스팸인지 여부에 대한 답신을 보냅니다. SpamAssassin과 같은 일부 프로그램은 메일이 스팸일 가능성을 숫자 등급으로 나타낸 스팸 점수를 답신과 함께 보냅니다.
3. Messaging Server가 답신을 읽고 메일에 대한 Sieve 작업을 수행합니다(451페이지의 "스팸 메일에 대해 수행할 작업 지정" 참조).

스팸 필터링 프로그램은 프로토콜을 통해 MTA와 상호 작용합니다. 이러한 프로토콜은 ICAP 기반 프로그램(예: Symantec AntiVirus Scan Engine)에서와 같이 표준 프로토콜이거나, Brightmail에서와 같이 전용 프로토콜이거나, Spam Assassin에서와 같이 표준이 아닌 프로토콜일 수 있습니다. 각 프로토콜에는 MTA와 상호 작용하기 위한 소프트웨어 후크가 필요합니다. Brightmail 및 SpamAssassin은 Messaging Server와 상호 작용할 수 있는 최초의 스팸 필터링 프로그램입니다. 이제 MTA에서는 ICAP를 사용하는 프로그램도 지원합니다.

## 타사 스팸 필터링 프로그램 배포 및 구성

Messaging Server에서 타사 필터링 소프트웨어를 배포하려면 다음의 다섯 가지 작업을 수행해야 합니다.

- **배포할 스팸 필터링 프로그램과 이 스팸 필터링 프로그램을 배포할 서버의 수를 지정합니다.** Messaging Server에서는 최대 네 개의 다른 스팸/바이러스 프로그램을 사용하여 받는 메일을 필터링할 수 있습니다. 이러한 프로그램은 별도의 시스템에서 실행할 수도 있고 단일 시스템 배포에서 Messaging Server와 동일한 시스템에서 실행하거나 2계층 배포에서 MTA와 동일한 시스템에서 실행할 수도 있습니다. 필요한 서버 수는 메일 로드, 하드웨어 성능 및 기타 요인에 따라 달라집니다. 사이트의 하드웨어 요구 사항을 확인하려면 스팸 필터링 소프트웨어 설명서를 참조하거나 담당자에게 문의하십시오.
- **스팸 필터링 소프트웨어를 설치 및 구성합니다.** 자세한 내용은 스팸 필터링 소프트웨어 설명서를 참조하거나 담당자에게 문의하십시오.

- **필터링 클라이언트 라이브러리를 로드하고 구성합니다.** 여기에는 MTA option.dat 파일에서 클라이언트 라이브러리 및 구성 파일을 지정하고 필터링 소프트웨어의 구성 파일에서 원하는 옵션을 설정하는 것이 포함됩니다. [443페이지의 "스팸 필터링 소프트웨어 클라이언트 라이브러리 로드 및 구성"](#)을 참조하십시오.
- **필터링할 메일을 지정합니다.** 사용자, 도메인 또는 채널별로 메일을 필터링할 수 있습니다. [444페이지의 "필터링할 메일 지정"](#)을 참조하십시오.
- **스팸 처리 방법을 지정합니다.** 스팸 삭제, 폴더에 정리, 제목 줄에 태그 지정 등을 수행할 수 있습니다. [451페이지의 "스팸 메일에 대해 수행할 작업 지정"](#)을 참조하십시오.

---

**주**      이전 버전의 Messaging Server에서는 Brightmail 필터링 기술만 지원했기 때문에 키워드와 옵션에 sourcebrightmail 또는 Brightmail\_config\_file과 같은 이름이 붙었습니다. 이러한 키워드와 옵션을 sourcespamfilter 또는 spamfilter\_config\_file과 같은 보다 일반적인 이름으로 변경했습니다. 이전 Brightmail 이름은 호환성을 위해 그대로 유지됩니다.

---

## 스팸 필터링 소프트웨어 클라이언트 라이브러리 로드 및 구성

각 스팸 필터링 프로그램에서 Messaging Server에 클라이언트 라이브러리 파일과 구성 파일을 제공해야 합니다. 클라이언트 라이브러리의 로드 및 구성에는 다음 두 가지 작업이 포함됩니다.

- option.dat 파일에서 스팸 필터링 소프트웨어 라이브러리 경로 (spamfilterX\_library) 및 구성 파일(spamfilterX\_config\_file) 지정. 이러한 옵션 외에도 스팸 필터링 LDAP 속성과 스팸 메일에 대해 사용할 Sieve 작업을 지정하는데 사용되는 여러 다른 옵션이 있습니다.
- 스팸 필터링 소프트웨어 구성 파일에서 원하는 옵션 지정. 각 스팸 필터링 프로그램은 서로 다른 구성 파일 및 구성 옵션을 가집니다. 이에 대해서는 스팸 필터링 소프트웨어 절이나 필터링 소프트웨어 설명서에 설명되어 있습니다. [455페이지의 "Symantec Brightmail 스팸 방지 사용"](#), [459페이지의 "SpamAssassin 사용"](#) 및 [473페이지의 "SAVSE\(Symantec Anti-virus Scanning Engine\) 사용"](#)을 참조하십시오.

## 스팸 필터링 소프트웨어 라이브러리 경로 지정

Messaging Server는 메일에 대해 최대 네 개의 다른 필터링 시스템을 호출할 수 있습니다. 예를 들어, Symantec AntiVirus Scan Engine 및 SpamAssassin을 통해 메일을 실행할 수 있습니다. 각 필터링 소프트웨어는 1에서 4까지의 번호로 식별됩니다. 이 번호는 여러 스팸 필터 옵션, LDAP 속성 및 채널 키워드의 일부로 표시되며 X가 필터 식별 번호로 사용 됩니다(예: sourcespamfilterXoptin 또는 spamfilterX\_config\_file). 키워드나 옵션 이름에서 식별 번호를 생략하면 기본값 1이 됩니다.

다음 option.dat 설정은 Messaging Server가 Symantec AntiVirus Scan Engine 및 SpamAssassin을 통해 메일을 필터링하도록 지정합니다.

```
spamfilter1_library=Symantec_Library_File  
spamfilter1_config_file=Symantec_Config_File  
spamfilter2_library=SpamAssassin_Library_File  
spamfilter2_config_file=SpamAssassin_Config_File
```

다른 옵션이나 키워드를 사용하여 시스템을 구성할 경우 옵션이나 키워드의 끝에서 해당 번호를 사용합니다. 예를 들어, sourcespamfilter2optin은 SpamAssassin을 나타내고 sourcespamfilter1optin은 Symantec AntiVirus Scan Engine을 나타냅니다. 번호를 순서대로 사용할 필요는 없습니다. 예를 들어, Symantec AntiVirus Scan Engine을 일시적으로 사용하지 않으려면 spamfilter1\_library 구성 파일을 주석 처리할 수 있습니다.

## 필터링할 메일 지정

Messaging Server에 스팸 필터링 소프트웨어가 설치되어 실행할 준비가 되면 필터링할 메일을 지정해야 합니다. 사용자, 도메인 또는 채널별로 메시지를 필터링하도록 Messaging Server를 구성할 수 있습니다. 다음 절에는 이러한 각 시나리오가 설명되어 있습니다.

- [445페이지의 "사용자 수준 필터 만들기"](#)
- [446페이지의 "도메인 수준 필터링 지정"](#)
- [448페이지의 "채널 수준 필터링 지정"](#)

---

**주**            *optin* 표현식은 사용자, 도메인 또는 채널이 메일 필터링을 받도록 선택되었음을 의미합니다.

---

## 사용자 수준 필터 만들기

사용자 단위로 필터링을 지정하는 것이 바람직할 수 있습니다. 예를 들어, 스팸이나 바이러스 필터링을 ISP 고객에게 프리미엄 서비스로 제공한 경우 이 서비스를 받을 사용자와 받지 않을 사용자를 지정할 수 있습니다. 사용자 필터링을 위한 일반적인 단계는 다음과 같습니다.

1. 스팸 필터링 소프트웨어를 활성화하는 사용자 LDAP 속성을 지정합니다.

option.dat에서 LDAP\_OPTINX 옵션을 설정합니다. 예를 들면 다음과 같습니다.

```
LDAP_OPTIN1=SymantecAV
LDAP_OPTIN2=SpamAssassin
```

2. 스팸 필터링을 받을 사용자 항목의 필터 속성을 설정합니다.

필터 속성의 값은 다중 값이며 서버에 따라 다릅니다. 단계 1의 예를 사용할 경우 항목은 다음과 같습니다.

```
SymantecAV: virus
SpamAssassin: spam
```

바이러스와 스팸을 모두 필터링할 수 있는 Brightmail과 같은 프로그램의 경우 유효한 값은 spam 및 virus입니다. 다중 값 속성으로 사용되는 각 값에는 개별 속성 항목이 필요합니다. 예를 들어, Brightmail의 필터 속성이 Brightmail로 설정된 경우 항목은 다음과 같습니다.

```
Brightmail: spam
Brightmail: virus
```

## 사용자 수준 필터 예

이 예에서는 Brightmail을 사용한다고 가정합니다. 또한 option.dat 파일에 LDAP\_OPTIN1이 Brightmail로 설정되어 있다고 가정합니다. Otis Fanning이라는 사용자는 자신의 사용자 항목에서 Brightmail 속성을 spam 및 virus로 설정했습니다. 따라서, 그의 메일은 스팸과 바이러스에 대해 필터링됩니다. 코드 예 14-1에서는 Otis Fanning에 대한 Brightmail 사용자 항목을 보여줍니다.

**코드 예 14-1** Brightmail에 대한 LDAP 사용자 항목 예

```
dn: uid=fanning,ou=people,o=sesta.com,o=ISP
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: inetUser
objectClass: ipUser
objectClass: inetMailUser
objectClass: inetLocalMailRecipient
objectClass: nsManagedPerson
objectClass: userPresenceProfile
```

**코드 예 14-1** Brightmail에 대한 LDAP 사용자 항목 예

```
cn: Otis Fanning
sn: fanning
initials: OTF
givenName: Otis
pabURI: ldap://ldap.siroe.com:389/ou=fanning,ou=people,o=sesta.com,o=isp,o=pab
mail: Otis.Fanning@sesta.com
mailAlternateAddress: ofanning@sesta.com
mailDeliveryOption: mailbox
mailHost: manatee.siroe.com
uid: fanning
dataSource: iMS 5.0 @(#)ims50users.sh 1.5a 02/3/00
userPassword: password
inetUserStatus: active
mailUserStatus: active
mailQuota: -1
mailMsgQuota: 100
Brightmail: virus
Brightmail: spam
```

Symantec AntiVirus Scan Engine 및 SpamAssassin을 사용하는 경우 항목은 다음과 같습니다.

```
SymantecAV: virus
SpamAssassin: spam
```

자세한 내용과 추가 예는 "[Symantec Brightmail 스팸 방지 사용](#)", "[SpamAssassin 사용](#)" 또는 "[SAVSE\(Symantec Anti-virus Scanning Engine\) 사용](#)"을 참조하십시오.

## 도메인 수준 필터링 지정

필터링을 받을 도메인을 지정할 수 있습니다. 예를 들어 스팸 방지 또는 바이러스 백신 필터링을 ISP 도메인 고객에게 프리미엄 서비스로 제공한 경우 이 기능을 사용할 수 있습니다. 도메인 필터링을 지정하는 일반적인 단계는 다음과 같습니다.

1. 필터링 소프트웨어를 활성화하는 도메인 LDAP 속성을 지정합니다.

option.dat에서 LDAP\_DOMAIN\_ATTR\_OPTINX 옵션을 설정합니다. 예를 들면 다음과 같습니다.

```
LDAP_DOMAIN_ATTR_OPTIN1=SymantecAV
LDAP_DOMAIN_ATTR_OPTIN2=SpamAssassin
```

## 2. 스팸 필터링을 받을 도메인 항목에서 필터 속성을 설정합니다.

필터 속성의 값은 다중 값이며 서버에 따라 다릅니다. 단계 1의 예를 사용할 경우 항목은 다음과 같습니다.

```
SymantecAV: virus
SpamAssassin: spam
```

바이러스와 스팸을 모두 필터링할 수 있는 **Brightmail**과 같은 프로그램의 경우 유효한 값은 spam 및 virus입니다. 다중 값 속성으로 사용되는 각 값에는 개별 속성 값 항목이 필요합니다. 예를 들어, LDAP\_DOMAIN\_ATTR\_OPTIN1이 Brightmail로 설정된 경우 항목은 다음과 같습니다.

```
Brightmail: spam
Brightmail: virus
```

### 도메인 수준 필터링 예

이 예에서는 Brightmail을 사용한다고 가정합니다. 또한 option.dat 파일에

LDAP\_DOMAIN\_ATTR\_OPTIN1이 Brightmail로 설정되어 있다고 가정합니다. Sun LDAP Schema 1에 대한 DC 트리의 sesta.com 도메인 항목에 Brightmail 속성이 spam 및 virus로 설정되어 있습니다. Sun LDAP Schema 2의 도메인 항목에서도 스팸 필터링을 받도록 Brightmail을 설정합니다.

Brightmail은 sesta.com으로 보낸 모든 메일에서 스팸과 바이러스를 필터링합니다. 코드 예 14-2에서는 도메인 항목을 보여줍니다.

#### 코드 예 14-2 Brightmail에 대한 LDAP 도메인 항목 예

```
dn: dc=sesta,dc=com,o=internet
objectClass: domain
objectClass: inetDomain
objectClass: mailDomain
objectClass: nsManagedDomain
objectClass: icsCalendarDomain
description: DC node for sesta.com hosted domain
dc: sesta
inetDomainBaseDN: o=sesta.com,o=isp
inetDomainStatus: active
mailDomainStatus: active
mailDomainAllowedServiceAccess: +imap, pop3, http:*
mailRoutingHosts: manatee.siroe.com
preferredMailHost: manatee.siroe.com
mailDomainDiskQuota: 10000000
mailDomainMsgQuota: -1
mailClientAttachmentQuota: 5
Brightmail: spam
Brightmail: virus
```

Symantec AntiVirus Scan Engine 및 SpamAssassin을 사용하는 경우 항목은 다음과 같습니다.

```
SymantecAV: virus  
SpamAssassin: spam
```

자세한 내용과 추가 예는 "Symantec Brightmail 스팸 방지 사용", "SpamAssassin 사용" 또는 "SAVSE(Symantec Anti-virus Scanning Engine) 사용"을 참조하십시오.

## 채널 수준 필터링 지정

소스 및 대상 채널별로 필터링을 지정하면 스팸 필터링의 유효성과 세부 수준이 향상됩니다. 예를 들어, 다음과 같이 필터링을 지정할 수 있습니다.

- 특정 MTA 릴레이에서 백엔드 메시지 저장소로 보낸 메일만
- 특정 MTA에서 받는 모든 메일
- 특정 MTA에서 보내는 모든 메일
- 특정 MTA에서 받는 메일과 보내는 메일

Messaging Server에서는 소스 또는 대상 채널을 기준으로 필터링을 지정할 수 있습니다. 이 작업을 수행하는 기법은 표 14-1에 설명된 채널 키워드입니다. 다음 예에서는 채널 수준 필터링을 설정하는 방법을 설명합니다.

1. 백엔드 메시지 저장소 호스트에 메일을 보내는 모든 인바운드 SMTP 서버의 imta.cnf 파일에 다시 쓰기 규칙을 추가합니다. 예를 들면 다음과 같습니다.

```
msg_store1.siroe.com  $U@msg_store1.siroe.com
```

2. destinationspamfilterXoptin 키워드를 사용하여 다시 쓰기 규칙에 해당하는 채널을 추가합니다. 예를 들면 다음과 같습니다.

```
tcp_msg_store1 smtp subdirs 20 backoff "pt5m" "pt10" "pt30" "pt1h" \  
"pt2h" "pt4h" maxjobs 1 pool IMS_POOL fileinto $U+$S@$D \  
destinationspamfilterloptin spam  
msg_store1.siroe.com
```



표 14-1 스팸 필터를 위한 MTA 채널 키워드

| 채널 키워드                       | 설명                                                                                                                                                                                                                                                                                                                                                                                                                 |
|------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| destinationsspamfilterXoptin | <p>사용자 또는 도메인이 LDAP_OPTIN LDAP 속성을 통해 해당 서비스를 지정하지 않은 경우에도 이 채널을 대상으로 하는 모든 메일을 스팸 방지 소프트웨어 X가 필터링하도록 지정합니다. 필터링 소프트웨어 X는 option.dat의 spamfilterX_library에서 정의합니다. 필터 매개 변수는 필터링 프로그램에 따라 다르며 키워드 뒤에 옵니다. 예를 들어, Brightmail 매개 변수는 spam, virus 또는 spam,virus입니다. SpamAssassin 매개 변수는 spam입니다.</p> <p>이 예에서는 메시지 저장소를 대상으로 하는 모든 메일에서 스팸을 스캔합니다.</p> <pre>ims-ms destinationsspamfilterloptin spam,virus. . .</pre> |
| sourcespamfilterXoptin       | <p>사용자 또는 도메인이 LDAP_OPTIN LDAP 속성을 통해 해당 서비스를 지정하지 않은 경우에도 이 채널을 통해 수신하는 모든 메일을 스팸 방지 소프트웨어 X가 필터링하도록 지정합니다. 시스템 차원 기본 매개 변수 앞에는 키워드가 오고 사용 가능한 매개 변수는 필터링 프로그램에 따라 다릅니다. 예를 들어, Brightmail 매개 변수는 spam, virus 또는 spam,virus입니다. SpamAssassin의 경우 매개 변수가 spam입니다. switchchannel이 적용되는 경우 이 키워드가 switched-to 채널에 포함됩니다.</p>                                                                                         |

### 채널 수준 필터링 예

다음 예에서는 필터링 프로그램이 번호 1로 지정되었다고 가정합니다.

**예 1.** MTA 릴레이에서 백엔드 메시지 저장소(msg\_store1.siroe.com)로 오는 모든 메일에서 스팸 및 바이러스를 필터링합니다.

1. 메일을 백엔드 메시지 저장소 호스트로 보내는 다시 쓰기 규칙을 imta.cnf 파일에 추가합니다. 예를 들면 다음과 같습니다.

```
msg_store1.siroe.com    $U@msg_store1.siroe.com
```

2. destinationsspamfilterXoptin 키워드를 사용하여 다시 쓰기 규칙에 해당하는 채널을 추가합니다. 예를 들면 다음과 같습니다.

```
tcp_msg_store1 smtp subdirs 20 backoff "pt5m" "pt10" "pt30" "pt1h" \
"pt2h" "pt4h" maxjobs 1 pool IMS_POOL fileinto $U+$$@$D \
destinationsspamfilterloptin spam,virus
msg_store1.siroe.com
```

**예 2.** MTA를 통해 전달하는 모든 받는 메일에서 스팸을 필터링합니다(일반적으로 모든 받는 메일은 tcp\_local 채널을 통해 전달됨).

```
tcp_local smtp mx single_sys remotehost inner switchchannel \  
identnonelimited subdirs 20 maxjobs 7 pool SMTP_POOL \  
maytlserver maysaslserver saslswitchchannel tcp_auth \  
sourcespamfilterloptin spam  
tcp-daemon
```

**예 3.** MTA를 통해 인터넷으로 전달하는 모든 보내는 메일을 필터링합니다(일반적으로 인터넷으로 보내는 모든 메일은 tcp\_local 채널을 통해 전달됨).

```
tcp_local smtp mx single_sys remotehost inner switchchannel \  
identnonelimited subdirs 20 maxjobs 7 pool SMTP_POOL \  
maytlserver maysaslserver saslswitchchannel tcp_auth \  
destinationsspamfilterloptin spam  
tcp-daemon
```

**예 4.** MTA를 통해 전달하는 모든 받는 메일과 보내는 메일을 필터링합니다.

```
tcp_local smtp mx single_sys remotehost inner switchchannel \  
identnonelimited subdirs 20 maxjobs 7 pool SMTP_POOL \  
maytlserver maysaslserver saslswitchchannel tcp_auth \  
sourcespamfilterloptin spam destinationsspamfilterloptin spam  
tcp-daemon
```

**예 5.** 사용자별 수신 선택 기능을 사용하지 않고 2계층 시스템에서 로컬 메시지 저장소를 대상으로 하는 모든 메일을 필터링합니다.

```
ims-ms smtp mx single_sys remotehost inner switchchannel \  
identnonelimited subdirs 20 maxjobs 7 pool SMTP_POOL \  
maytlserver maysaslserver saslswitchchannel tcp_auth \  
destinationsspamfilterloptin spam  
tcp-daemon
```

**예 6.** 모든 받는 메일과 보내는 메일에서 스팸과 바이러스를 필터링합니다(소프트웨어가 스팸과 바이러스를 모두 필터링하는 것으로 가정).

```
tcp_local smtp mx single_sys remotehost inner switchchannel \  
identnonelimited subdirs 20 maxjobs 7 pool SMTP_POOL \  
maytlserver maysaslserver saslswitchchannel tcp_auth \  
destinationsspamfilterloptin spam,virus sourcespamfilterloptin \  
spam,virus  
tcp-daemon
```

## 스팸 메일에 대해 수행할 작업 지정

스팸 필터링 프로그램은 메일을 분석하여 Messaging Server에 스팸 여부에 대한 답신을 보냅니다. 그러면 Messaging Server에서 해당 메일에 대한 작업을 수행합니다. 작업은 Sieve 메일 필터링 언어를 사용하여 지정됩니다. 메일 삭제, 메일을 폴더에 정리, 헤더 추가, 제목 행에 태그 추가 등과 같은 작업을 수행할 수 있습니다. if-then-else 문이 있는 복잡한 Sieve 스크립트를 사용할 수도 있습니다.

---

**주** 전체 Sieve 구문은 Sieve 사양 3028을 참조하십시오. 또한 <http://www.cyrusoft.com/sieve/>를 참조하십시오.

---

Sieve 스크립트는 표 14-2에서 설명한 MTA 스팸 필터 옵션(option.dat)을 통해 지정됩니다. 기본 스팸 필터 작업 옵션은 SpamfilterX\_null\_action(null 값이 스팸 답신 값으로 반환될 때 실행하도록 Sieve 규칙 지정) 및 SpamfilterX\_string\_action(문자열이 스팸 답신으로 반환될 때 실행하도록 Sieve 규칙 지정)입니다.

스팸 필터링 프로그램은 일반적으로 MTA에 해당 메일이 스팸임을 나타내는 문자열 또는 null 값을 반환합니다. 메일이 스팸일 확률을 나타내는 숫자 등급인 스팸 점수를 반환하는 프로그램도 있습니다. 이 점수는 작업 시퀀스의 일부로 사용될 수 있습니다. 다음 예는 필터링된 메일에 대해 수행할 작업을 지정하는 방법을 보여 줍니다. 각 예에서 필터링 프로그램이 번호 1로 지정되었다고 가정합니다.

**예 1:** 답신 값이 null인 스팸 메일을 SPAM\_CAN 파일로 저장합니다.

```
spamfilter1_null_action=data:,require "fileinto"; fileinto "SPAM_CAN";
```

문자열을 반환하는 스팸 메일에 대해 동일한 작업을 수행할 수 있습니다.

```
spamfilter1_string_action=data:,require "fileinto"; fileinto "SPAM_CAN";
```

**예 2:** 답신이 문자열인 스팸 메일을 MTA에 반환된 해당 답신 문자열로 명명된 파일에 저장합니다(\$U가 수행하는 작업). 즉, 반환된 답신 문자열이 spam일 경우 메일은 spam이라는 파일에 저장됩니다.

```
spamfilter1_null_action=data:,require "fileinto"; fileinto "$U";
```

**예 3:** 답신 값이 문자열인 스팸 메일을 삭제합니다.

```
spamfilter1_string_action=data:,discard
```

null 값을 반환하는 스팸 메일에 대해 동일한 작업을 수행할 수 있습니다.

```
spamfilter1_null_action=data:,require "fileinto"; fileinto "SPAM_CAN";
```

**예 4.** 이 행은 문자열 답신 값을 통해 스팸으로 확인된 각 메일에 Spam-test: FAIL 헤더를 추가합니다.

```
spamfilter1_string_action=data:,require ["addheader"];addheader "Spam-test:
FAIL";
```

**예 5.** 이 행은 문자열을 반환하는 스팸 메일의 제목 행에 [PROBABLE SPAM] 문자열을 추가합니다.

```
spamfilter1_string_action=data:,addtag "[PROBABLE SPAM]";
```

**예 6.** 이 행은 헤더에 resent-from 및 User-1이 포함되어 있는 경우 문자열 답신 값으로 간주하고 스팸 메일을 testspam 메일함에 파일로 저장합니다. 해당 헤더가 없는 경우 메일을 spam 파일에 저장합니다.

```
spamfilter1_string_action=data:,require "fileinto";\
  if header :contains ["resent-from"] ["User-1"] {\
    fileinto "testspam";\
  } else {\
    fileinto "spam";};
```

대부분의 스팸 필터 소프트웨어로 답신 문자열을 구성할 수 있기 때문에 반환되는 문자열에 따라 다른 작업을 지정할 수 있습니다. 이 작업은 일치하는 spamfilterX\_verdict\_n 및 spamfilterX\_action\_n 옵션 쌍을 사용하여 수행할 수 있습니다.

**예 7.** 이 일치 쌍 옵션은 반환된 답신 문자열이 remove인 스팸 메일을 삭제합니다.

```
spamfilter1_verdict_0=remove
spamfilter1_action_0=data:,discard
```

스팸 답신 문자열 지정 방법에 대한 자세한 내용은 해당 스팸 필터링 소프트웨어 절을 참조하십시오.

**표 14-2** MTA 스팸 필터 옵션(option.dat)

| Spam Assassin에 대한 MTA 옵션 설명 |                                                       |
|-----------------------------|-------------------------------------------------------|
| SpamfilterX_config_file     | 필터링 소프트웨어 X 구성 파일의 전체 파일 경로와 이름을 지정합니다.<br>기본값: 없음    |
| SpamfilterX_library         | 필터링 소프트웨어 X 공유 라이브러리의 전체 파일 경로와 이름을 지정합니다.<br>기본값: 없음 |

표 14-2 MTA 스팸 필터 옵션(option.dat)

| Spam Assassin에 대한 MTA 옵션 설명 |                                                                                                                                                                                                                                                                                                                                                                        |
|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SpamfilterX_optional        | <p>필터링 라이브러리 X가 보고한 특정 실패가 일시적인 처리 실패로 간주되는지 무시되는지 여부를 제어합니다. 기본값 0은 스팸 필터링 문제가 일시적인 처리 실패를 발생함을 지정합니다. 값을 1로 변경하면 모든 이벤트가 아니라 일부 이벤트에서 스팸 필터 처리를 건너뛰어 필터링 라이브러리가 실패합니다. 특히, 시스템이 라이브러리 코드에 값을 반환하지 않고 고착 상태가 될 경우 MTA의 일부 부분도 함께 고착될 수 있습니다. -2와 2가 함께 설정될 수 있습니다. 이들은 스팸 필터 플러그인에서 보고한 문제의 이벤트에 syslog 메시지를 보낸다는 점만 제외하고 각각 0 및 1과 같습니다.</p> <p>기본값: 0</p>           |
| LDAP_optinX                 | <p>사용자 단위로 필터링 소프트웨어 X를 활성화하는 데 사용되는 LDAP 속성의 이름을 지정합니다. 이 속성은 inetMailUser objectclass의 속성이어야 합니다.</p> <p>속성 자체는 여러 값을 가질 수 있으며 대/소문자를 구분합니다. SpamAssassin의 경우 이 값은 소문자 spam이어야 합니다.</p> <p>기본값: 없음</p>                                                                                                                                                               |
| LDAP_domain_attr_optinX     | <p>도메인 단위로 필터링 소프트웨어 X를 활성화하는 데 사용되는 LDAP 속성의 이름을 지정합니다. 대상 도메인에 적용됩니다. mailDomain objectclass에 있어야 한다는 점을 제외하고 LDAP_optin과 동일합니다.</p> <p>기본값: 없음</p>                                                                                                                                                                                                                  |
| SpamfilterX_null_optin      | <p>LDAP_optinX 또는 LDAP_domain_attr_optinX에서 정의한 속성 값으로 발견된 경우 MTA에서 해당 속성이 없는 것처럼 간주하는 문자열을 지정합니다. 즉, 해당 항목에 대한 필터링을 비활성화합니다. 자세한 내용은 444페이지의 "필터링할 메일 지정"을 참조하십시오.</p> <p>기본값: 빈 문자열. 빈 optin 속성은 기본적으로 무시됩니다. 빈 optin 속성이 빈 optin 목록을 갖는 필터링을 트리거했던 iPlanet Messaging Server 5.2와 달라진 내용입니다. spamfilterX_null_optin을 실제로 표시된 적이 없는 문자열로 설정하여 5.2 동작을 복원할 수 있습니다.</p> |
| SpamfilterX_null_action     | <p>필터링 소프트웨어 X 답신이 null로 반환될 경우에 메일에서 수행할 작업을 지정하는 Sieve 규칙을 정의합니다. 파일 URL을 사용하여 Sieve 문을 외부적으로 저장할 수 있습니다(예: file:///var/opt/SUNWmsgsr/config/null_action.sieve). 또한, Sieve 거부 작업을 사용하여 스팸을 거부하지 않기 때문에 주소를 사용하여 스팸을 보낸 적이 있는 악의 없는 사용자에게 배달 실패 알림을 전달합니다.</p> <p>기본값: data: ,discard;</p>                                                                            |
| SpamfilterX_string_action   | <p>답신이 문자열일 경우에 메일에서 수행할 작업을 지정하는 SIEVE 규칙을 정의합니다. 파일 URL을 사용하여 Sieve 문을 외부적으로 저장할 수 있습니다(예: file:///var/opt/SUNWmsgsr/config/null_action.sieve). 또한, Sieve reject 작업을 사용하여 스팸을 거부하지 않기 때문에 서버를 사용하여 스팸을 보낸 적이 있는 악의 없는 사용자에게 배달 실패 알림을 전달합니다.</p> <p>Default: data: ,require "fileinto"; fileinto "\$U;</p> <p>\$U는 verdict가 반환한 문자열입니다.</p>                          |

**표 14-2** MTA 스팸 필터 옵션(option.dat)

| <b>Spam Assassin에 대한 MTA 옵션 설명</b> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| spamfilterX_verdict_n              | <p>spamfilterX_verdict_n 및 spamfilterX_action_n 옵션은 일치하는 쌍입니다. 여기서 n은 0에서 9 사이의 숫자입니다. 이러한 옵션을 사용하면 임의의 답신 문자열에 대한 Sieve 필터를 지정할 수 있습니다. 이 작업은 spamfilterX_verdict_n 및 spamfilterX_action_n을 각각 답신 문자열 및 sieve 필터로 설정하여 수행합니다. 여기서 n은 0에서 9 사이의 정수입니다. 예를 들어, 사이트에 "reject" 답신이 있는 경우 다음을 지정하여 sieve 거부 작업을 발생시킵니다.</p> <pre>spamfilter1_verdict_0=reject spamfilter1_action_0=data:,require "reject"; reject "Rejected by spam filter";</pre> <p>모든 spamfilterX_verdict_n 옵션과 해당 작업 옵션의 기본값은 빈 문자열입니다.</p> <p>기본값: 없음</p>                                                                                                                                                                                                                                                                                                                                      |
| spamfilterX_action_n               | <p>spamfilterX_verdict_n을 참조하십시오.</p> <p>기본값: 없음</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| spamfilterX_final                  | <p>일부 필터링 라이브러리에는 수신자 주소를 기반으로 작업을 수행하는 기능이 있습니다. spamfilterX_final은 필터링 라이브러리에 전달되는 수신자 주소의 종류를 지정합니다. 0은 중간 주소가 사용되게 하고 1은 최종 수신자 주소 형식을 보냅니다.</p> <p>기본값: 0</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| optin_user_carryover               | <p>전달은 스팸 필터 처리를 위한 시도입니다. forward 전달 옵션을 지정하고 다른 사용자의 전달 주소를 지정하는 사용자 항목을 고려합니다. 또한, 사용자 항목은 특정 필터링 종류에 대한 optin으로 설정됩니다. 전달된 메일에 필터링을 적용하시겠습니까? 다시 말해서 특정 사용자에게 올바른 필터링 선택이 다른 사용자에게는 올바른 선택이 아닐 수 있습니다. 즉, 필터링 작업 제거가 사이트의 보안 정책을 위반하는 수단으로 사용될 수 있습니다.</p> <p>모든 경우에서 어떤 답변도 옳지 않기 때문에 OPTIN_USER_CARRYOVER는 전달 중에 사용자/별칭 항목의 스팸 필터링 optin 목록이 다른 사용자/별칭 항목에 적용되는 방법을 제어합니다. 이는 비트 인코딩 값입니다. 비트 값의 의미는 다음과 같습니다.</p> <p>비트 0(값 1). 각 LDAP 사용자 항목이 이전의 활성 사용자/도메인 optins를 무조건적으로 대체합니다.</p> <p>비트 1(값 2). 사용자의 도메인에 optin 속성이 있는 경우 활성화된 이전 사용자/도메인/별칭 optins를 대체합니다.</p> <p>비트 2(값 4). 사용자에게 optin 속성이 있는 경우 활성화된 이전 사용자/도메인/별칭 optins를 대체합니다.</p> <p>비트 3(값 8). [optin] non-positional 매개 변수에 지정된 optin이 활성화된 이전 사용자/도메인/별칭 optins를 대체합니다.</p> <p>기본값: 0. 사용자가 다른 사용자에게 전달하는 전달 옵션이 있는 경우 optin이 누락됩니다. 기본값은 전달 중에 사이트 보안 정책을 적용하고 다른 설정은 적용되지 않게 합니다.</p> |

# Symantec Brightmail 스팸 방지 사용

Brightmail 솔루션은 전자 메일 서버에 다운로드되는 실시간 스팸 방지 및 바이러스 백신 규칙 업데이트와 Brightmail Server로 구성됩니다.

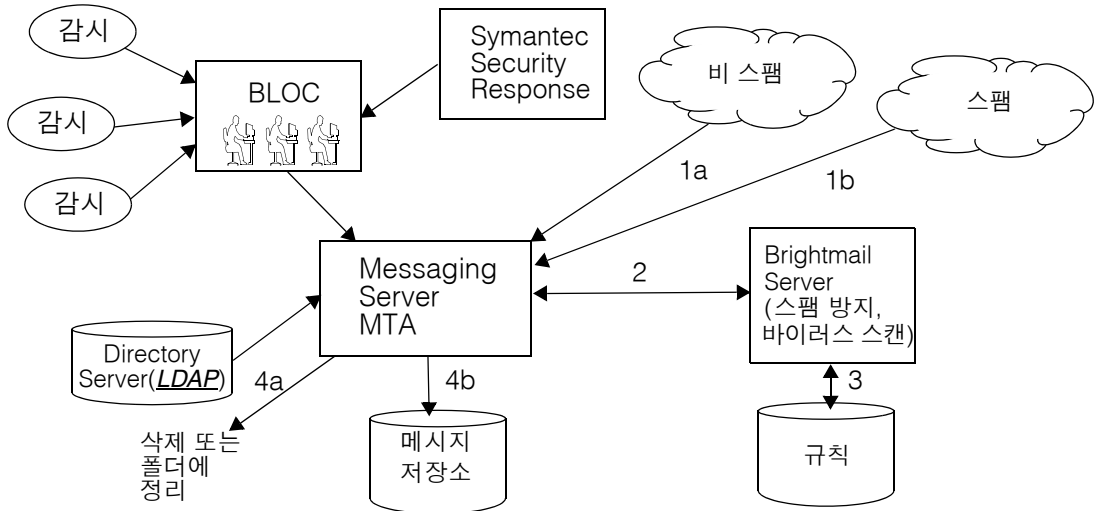
## Brightmail 작업 방법

Brightmail Server는 고객 사이트에 배포됩니다. Brightmail에는 인터넷을 통한 새로운 스팸 감지를 위한 전자 메일 감시 설정이 있습니다. Brightmail 기술자들은 이러한 스팸을 실시간으로 차단하기 위한 사용자 정의 규칙을 작성합니다. 이러한 규칙은 Brightmail Server에 실시간으로 다운로드됩니다. Brightmail 데이터베이스는 업데이트되고 Brightmail Server는 지정된 사용자 또는 도메인의 전자 메일에 대해 이 데이터베이스 필터를 실행합니다.

## Brightmail 구조

그림 14-1에서는 Brightmail 구조에 대해 설명합니다.

그림 14-1 Brightmail 및 Messaging Server 구조



BLOC(Brightmail Logistics and Operations Center)에서 전자 메일 감시를 통해 스팸을 받는 경우 연산자는 해당 스팸 방지 규칙을 즉시 생성하여 Brightmail 고객 시스템에 다운로드되게 합니다. 마찬가지로 Symantec Security Response 실시간 바이러스 규칙을 Brightmail을 통해 받습니다. 이러한 규칙은 고객의 Brightmail Server에서 스팸 및 바이러스를 찾아내는 데 사용됩니다.

MTA는 Brightmail SDK를 사용하여 Brightmail Server와 통신합니다. MTA는 Brightmail의 응답에 따라 메일을 발송합니다. MTA는 메일 (1a) 또는 (1b)를 받은 후 Brightmail Server로 보냅니다. (2) Brightmail Server는 해당 규칙과 데이터를 사용하여 메일이 스팸 또는 바이러스인지 확인하고 (3) MTA에 답신을 보냅니다. 답신에 따라 MTA는 (4a) 폴더에서 메일 또는 파일을 삭제하거나 (4b) 일반적으로 대상에 전달합니다.

Brightmail SDK는 타사 소프트웨어이기 때문에 본사의 설치 키트에는 제공되지 않습니다. Brightmail SDK 및 서버 소프트웨어는 고객이 Brightmail Inc.를 통해 직접 구입해야 합니다. MTA에는 Brightmail 통합을 위해 Brightmail SDK를 로드할지 여부와 로드 위치를 알려주는 구성 설정이 있습니다.

SDK가 로드되면 여러 요소와 세부(*granularity* - Brightmail에서 현재 프로세싱이 *optin*임을 지정하는 데 사용되는 용어) 수준으로 Brightmail 메일 처리를 결정합니다. 이는 다음 기준에 따라 지정됩니다.

- 소스 채널 또는 대상 채널이 Brightmail에 대해 활성화되는지 여부(*imta.cnf*)
- (*imta.cnf*)에서 선택한 서비스에 대한 채널 기본값이 있는지 여부
- 도메인별 수신 선택 기능(*optin*)이 있는지 여부(LDAP)
- 사용자별 수신 선택 기능(*optin*)이 있는지 여부(LDAP)

특정 메일 수신자에 대해 위의 *optin* 값과 기본값을 결합합니다. 그렇게 하면 스팸과 바이러스 모두에 대해 채널 기본값이 이미 지정되어 있는 경우 각 사용자 *optin* 값을 제공할 필요가 없습니다. 즉, 시스템 관리자가 모든 사용자에게 대해 스팸 및 바이러스 필터링을 수행하도록 결정할 경우 스팸 또는 바이러스에 대해 수신 선택 기능(*optin*)을 사용자에게 제공할 필요가 없습니다. 처리를 중단할 수 있는 방법은 없습니다. 즉, 시스템이나 도메인 수신 선택 기능(*optin*)을 통해 이미 선택된 서비스는 취소할 수 없습니다. 이것은 또한 서비스에 대해 수신 선택 기능(*optin*)을 사용하고 메일을 다른 주소로 전달한 경우, 사용자를 대신 하여 필터링이 수행된 후에 해당 주소가 메일을 받게 된다는 것을 의미합니다.

바이러스 감지 또는 스팸 감지의 두 서비스만 제공됩니다. 또한 Brightmail은 "content-filtering" 서비스를 제공하지만 이 기능은 Sieve를 사용하여 제공되므로 Brightmail에서 Sieve 필터링을 수행할 수 있는 추가된 값이 없습니다.



메일이 바이러스 메일인 것으로 확인되면 바이러스를 삭제하고 치료된 메일을 MTA에 다시 제출하도록 **Brightmail Server**를 구성할 수 있습니다. 다시 제출된 치료된 메일에 원본 메일에 대한 정보가 없을 경우 원하지 않은 부작용이 발생하기 때문에 치료된 메일을 다시 MTA로 제출하도록 **Brightmail**을 구성하지 않는 것이 좋습니다. 메일이 스팸인 경우 MTA는 **Brightmail**의 답신과 구성을 함께 사용하여 메일에 표시되는 내용은 결정할 수 있습니다. 메일을 삭제하거나, 폴더에 정리하거나, 제목 행에 스팸 또는 바이러스 태그를 지정하거나, Sieve 규칙에 전달하거나, INBOX에 전달할 수 있습니다.

**Brightmail Server**는 MTA와 동일한 시스템에 위치하거나 별도의 시스템에 위치할 수 있습니다. 실제로, 하나 이상의 MTA에 서비스를 제공하는 **Brightmail Server** 그룹을 가질 수 있습니다. **Brightmail SDK**는 **Brightmail** 구성 파일을 사용하여 사용할 **Brightmail Server**를 결정합니다.

## Brightmail 요구 사항 및 성능 고려 사항

- **Brightmail Server**는 Solaris 운영 체제에서 실행해야 합니다.
- **Brightmail**에서 스팸 검사와 바이러스 검사를 모두 구현하는 경우 MTA 메일 처리 능력이 50%까지 감소될 수 있습니다. MTA 처리 능력을 유지하려면 각 MTA에 대해 두 대의 **Brightmail Server**가 필요합니다.
- **SpamAssassin**에는 사용자 단위로 다양한 필터링을 수행할 수 있는 기능이 있지만 동일한 메일에 한 번에 두 개의 서로 다른 필터링 기준을 적용할 수는 없습니다. 따라서, **SpamAssassin**은 시스템 차원 필터링만 허용합니다. 개별 사용자에 대한 사용자 정의 필터링은 사용할 수 없습니다.

## Brightmail 배포

**Brightmail**을 배포하려면 다음 단계를 수행합니다.

- **Brightmail**을 설치하고 구성합니다. 설치 및 구성 정보는 **Brightmail** 소프트웨어 설명서를 참조하거나 담당자에게 문의하십시오. 선택된 **Brightmail** 구성 옵션은 [458페이지의 "Brightmail 구성 옵션"](#)에 표시되지만 최신 정보는 **Brightmail** 설명서를 참조하십시오.

- **Brightmail 클라이언트 라이브러리를 로드하고 구성합니다.** 이 작업에는 Brightmail 클라이언트 라이브러리 `libbmiclient.so`와 MTA에 대한 구성 파일 `config`를 지정하는 것이 포함됩니다. [443페이지의 "스팸 필터링 소프트웨어 클라이언트 라이브러리 로드 및 구성"](#)을 참조하십시오.
- **스팸을 필터링할 메일을 지정합니다.** 사용자, 도메인 또는 채널별로 메일을 필터링할 수 있습니다. [444페이지의 "필터링할 메일 지정"](#)을 참조하십시오.
- **스팸 메일에 대해 수행할 작업을 지정합니다.** 스팸 삭제, 폴더에 정리, 제목 행에 태그 지정 등의 작업을 수행할 수 있습니다. [451페이지의 "스팸 메일에 대해 수행할 작업 지정"](#)을 참조하십시오.
- **기타 MTA 필터 구성 매개 변수를 원하는 대로 설정합니다.** [452페이지의 "MTA 스팸 필터 옵션\(option.dat\)"](#)을 참조하십시오.

## Brightmail 구성 옵션

선택한 Brightmail 구성 파일 옵션은 [표 14-3](#)에 표시되어 있습니다. Brightmail 구성 파일 환경 옵션의 전체 목록은 Brightmail에서 구할 수 있습니다. 옵션과 값은 대소문자를 구분하지 않습니다.

**표 14-3**      선택된 Brightmail 구성 파일 옵션

| Brightmail 옵션                             | 설명                                                                                                                                                                                                                                                                                                                 |
|-------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>blSWPrecedence</code>               | 지정된 메일에 여러 답신이 있을 수 있습니다. 이 옵션은 우선 순위를 지정합니다. 이 옵션을 <code>virus-spam</code> 으로 지정한 경우 메일에서 바이러스 검사를 먼저 수행한 다음 스팸 검사를 수행합니다. 답신은 하이픈(-)으로 구분됩니다. Sun Java System Messaging Server에서 Brightmail을 사용할 경우에 권장되는 설정입니다.                                                                                                 |
| <code>blSWClientDestinationDefault</code> | 스팸 또는 바이러스 대신 일반적인 메일 전달 방법을 지정하므로 답신이 없습니다. 이 메일을 일반적인 방법으로 전달하려면 <code>inbox</code> 를 값으로 지정합니다. 기본값은 없습니다.                                                                                                                                                                                                      |
| <code>blSWLocalDomain</code>              | 이 속성은 로컬로 간주되는 도메인을 지정합니다. 로컬로 간주되는 여러 도메인을 지정하는 여러 행으로 된 이 속성이 있을 수 있습니다. 로컬 도메인과 외부 도메인은 답신에 대한 서로 다른 두 가지 처리를 지정하기 위해 구분하여 사용됩니다.<br><br>아래의 <code>blSWClientDestinationLocal</code> 및 <code>blSWClientDestinationForeign</code> 을 참조하십시오. 예를 들어, 다음을 지정할 수 있습니다.<br><br><code>blSWLocalDomain=siroe.com</code> |

**표 14-3**     선택된 Brightmail 구성 파일 옵션

| Brightmail 옵션                | 설명                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| blSWClientDestinationLocal   | <p>이 속성은 로컬 도메인에 대한 답신과 작업 쌍을 지정합니다. 일반적으로 스팸과 바이러스에 대해 각각 한 행씩 두 개의 행이 있습니다. 값은 <code>verdict action</code> 형식입니다. 예를 들면 다음과 같습니다.</p> <pre>blSWClientDestinationLocal=spam spambox blSWClientDestinationLocal=virus </pre> <p>기본 Brightmail에서 "null" 작업(!의 오른쪽에 아무 것도 없음)은 메일 삭제를 의미합니다. 따라서, 위의 예에서 <code>virus</code> 답신이 있는 경우 메일이 삭제됩니다. 답신이 <code>spam</code>인 경우 메일을 <code>spambox</code>라는 폴더에 정리합니다. 메일이 스팸 또는 바이러스가 아닌 경우 답신이 일치하지 않고 위의 <code>blSWClientDestinationDefault</code> 설정을 기준으로 메일을 전달합니다.</p> <p>MTA에서 서버를 사용하거나 별도의 Brightmail Server를 사용할 경우 <code>Brightmail_verdict_n/Brightmail_action_n/Brightmail_null_action/Brightmail_string_action</code> MTA 옵션을 사용하여 정의된 작업은 Brightmail Server에서 반환되는 작업 및 답신에 우선합니다. 이 예의 경우 MTA에서 다른 <code>Brightmail_null_action</code>을 사용하여 Virus 작업(삭제)을 대체하거나 <code>Brightmail_verdict_0=spambox</code> 및 <code>Brightmail_action_0=data:,require "fileinto";fileinto "Junk";</code>를 사용하여 메일을 <code>spambox</code> 대신 Junk 폴더에 정리할 수 있습니다.</p> |
| blSWClientDesintationForeign | <p>로컬이 아닌 도메인에 있는 사용자에게 적용된다는 점을 제외하고 위의 <code>blSWClientDestinationLocal</code>과 형식 및 해석이 동일합니다.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| blSWUseClientOptin           | <p>Sun Java System Messaging Server에서 사용할 경우 이 속성을 항상 TRUE로 설정합니다.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| blswcServerAddress           | <p><code>ip:port[,ip:port,...]</code> 형식을 사용하여 하나 이상의 Brightmail Server의 IP 주소와 포트 번호를 지정합니다.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

## SpamAssassin 사용

이 절은 다음과 같은 하위 절로 구성되어 있습니다.

- 460페이지의 "SpamAssassin 개요"
- 460페이지의 "SpamAssassin/Messaging Server 작업 이론"
- 461페이지의 "SpamAssassin 요구 사항 및 사용 시 고려 사항"
- 462페이지의 "SpamAssassin 배포"
- 462페이지의 "SpamAssassin 구성 예"
- 469페이지의 "SpamAssassin 테스트"

- [471페이지의 "SpamAssassin 옵션"](#)

## SpamAssassin 개요

Messaging Server는 스팸을 식별하는 데 사용되는 프리웨어 메일 필터인 SpamAssassin의 사용을 지원합니다. SpamAssassin는 Perl에서 작성된 라이브러리와 SpamAssassin을 메일 시스템에 통합하는 데 사용될 수 있는 일련의 응용 프로그램과 유틸리티로 구성됩니다.

SpamAssassin은 메일 헤더 및 본문 정보에 대한 일련의 테스트를 수행하여 모든 메시지에 대한 점수를 계산합니다. 테스트가 성공하거나 실패할 때마다 true(스팸) 또는 false(스팸 아님) 답신이 렌더링됩니다. 점수는 양의 실수 또는 음의 실수입니다. 점수가 특정 임계값(일반적으로 5.0)을 초과하면 스팸으로 간주됩니다. 다음은 SpamAssassin 결과 문자열의 예입니다.

```
True ; 18.3 / 5.0
```

True는 메일이 스팸임을 나타냅니다. 18.3은 SpamAssassin 점수입니다. 5.0은 임계값입니다.

SpamAssassin은 자세히 구성할 수 있습니다. 언제든지 테스트를 추가하거나 제거하여 기존의 테스트 점수를 조정할 수 있습니다. 이 작업은 다양한 구성 파일을 통해 수행됩니다. SpamAssassin에 대한 자세한 내용은 SpamAssassin 웹 사이트를 참조하십시오.

Brightmail 스팸 및 바이러스 스캔 라이브러리를 호출하는 데 사용한 것과 동일한 기법을 사용하여 SpamAssassin spamd 서버에 연결할 수 있습니다. Messaging Server에 제공되는 모듈을 libspamass.so라 합니다.

## SpamAssassin/Messaging Server 작업 이론

spamd는 SpamAssassin의 데몬 버전이며 MTA에서 호출될 수 있습니다. spamd는 소켓에서 요청을 수신하고 메일 테스트를 위한 하위 프로세스를 생성합니다. 하위 프로세스는 메일을 처리하여 결과를 돌려 보낸 후 종료됩니다. 이론적으로 하위 프로세스 간에 코드 자체가 공유되기 때문에 포크는 효율적인 프로세스이어야 합니다.

SpamAssassin 설치에서 클라이언트 부분인 spamc는 사용되지 않습니다. 이 기능은 Messaging Server의 일부인 libspamass.so라는 공유 라이브러리에 의해 대신 수행됩니다. libspamass.so는 Brightmail SDK에서와 동일한 방법으로 로드됩니다.

MTA의 관점에서 SpamAssassin과 Brightmail을 거의 투명하게 전환하여 스팸을 필터링할 수 있습니다. 그렇지만 서로 간에 기능이 동일하지 않기 때문에 완전히 투명하지는 않습니다. 예를 들어, Brightmail은 바이러스도 필터링할 수 있지만 SpamAssassin은 스팸을 필터링하는 데만 사용됩니다. 또한, 두 소프트웨어 패키지가 반환하는 결과 또는 **답신**도 다릅니다. SpamAssassin은 점수를 제공하는 반면 Brightmail은 답신 이름을 제공하기 때문에 구성 상에 여러 가지 차이점이 있습니다.

MTA와 통합된 SpamAssassin을 사용할 경우 SpamAssassin에서 점수와 답신만 반환됩니다. 메일 자체는 수정되지 않습니다. 즉, 헤더 추가, 제목 행 수정 등과 같은 작업은 Sieve 스크립트를 통해 수행해야 합니다. 또한 mode 옵션을 사용하면 답신을 가리키도록 반환되는 문자열을 지정할 수 있습니다. 문자열로 선택할 수 있는 것은 null이나 기본값, SpamAssassin 결과 문자열, verdict 문자열 등입니다. 자세한 내용은 [471페이지의 표 14-4](#)를 참조하십시오.

## SpamAssassin 요구 사항 및 사용 시 고려 사항

- SpamAssassin은 무료입니다. 소프트웨어와 설명서는 <http://www.spamassassin.org>에서 구할 수 있습니다.
- SpamAssassin을 조정 및 구성하여 스팸을 매우 정확하게 감지할 수 있습니다. 이러한 조정은 사용자와 SpamAssassin 커뮤니티가 직접 수행해야 합니다. Messaging Server는 SpamAssassin에서 수행할 수 있는 작업을 제공하거나 향상시키지 않습니다.
- 특정 번호를 사용할 수 없는 동안 SpamAssassin은 Brightmail보다 처리 능력이 떨어집니다.
- MTA와 통합된 SpamAssassin은 사용자, 도메인 또는 채널에 대해 사용할 수 있습니다.
- Vipul Razor 또는 DCC(Distributed Checksum Clearinghouse)와 같은 다른 온라인 데이터베이스를 사용하도록 SpamAssassin을 구성할 수 있습니다.
- Messaging Server는 SSL(Secure Socket Layer) 버전 libspamass.so를 제공하지 않지만 openssl을 사용하도록 SpamAssassin을 작성할 수 있습니다.
- Perl 5.6 이상이 필요합니다.

## SpamAssassin을 실행하는 장소

SpamAssassin은 자체 시스템, 단일 시스템 배포의 Messaging Server와 동일한 시스템 또는 2계층 배포의 MTA와 동일한 시스템에서 실행할 수 있습니다. LMTP(Local Mail Transfer Protocol)가 MTA와 메시지 저장소 사이에서 사용되는 경우 MTA에서 필터링을 호출해야 합니다. 메시지 저장소에서는 필터링을 호출할 수 없습니다. MTA와 메시지 저장소 간에 SMTP가 사용되는 경우 각 시스템이나 별도의 타사 시스템에서 실행할 수 있습니다.

SpamAssassin을 실행하는 서버 그룹을 사용하려면 해당 그룹의 앞에 로드 밸런서를 사용해야 합니다. MTA는 SpamAssassin 서버에 대해 단일 주소로만 구성됩니다.

## SpamAssassin 배포

SpamAssassin을 배포하려면 다음 단계를 수행합니다.

- **SpamAssassin을 설치하고 구성합니다.** 설치 및 구성 정보는 SpamAssassin 소프트웨어 설명서를 참조하십시오. [471페이지](#)의 "[SpamAssassin 옵션](#)"도 참조하십시오.
- **SpamAssassin 클라이언트 라이브러리를 로드 및 구성합니다.** 이 작업에는 클라이언트 라이브러리 `libspamass.so`와 MTA에 대한 구성 파일(만들어야 함)을 지정하는 것이 포함됩니다. [443페이지](#)의 "[스팸 필터링 소프트웨어 클라이언트 라이브러리 로드 및 구성](#)"을 참조하십시오.
- **스팸을 필터링할 메일을 지정합니다.** 사용자, 도메인 또는 채널별로 메일을 필터링할 수 있습니다. [444페이지](#)의 "[필터링할 메일 지정](#)"을 참조하십시오.
- **스팸 메일에 대해 수행할 작업을 지정합니다.** 스팸 삭제, 폴더에 정리, 제목 행에 태그 지정 등의 작업을 수행할 수 있습니다. [451페이지](#)의 "[스팸 메일에 대해 수행할 작업 지정](#)"을 참조하십시오.
- **기타 필터 구성 매개 변수를 원하는 대로 설정합니다.** [452페이지](#)의 "[MTA 스팸 필터 옵션\(option.dat\)](#)"을 참조하십시오.

## SpamAssassin 구성 예

이 절에서는 일반적인 몇 가지 SpamAssassin 구성 예를 설명합니다.

- [463페이지](#)의 "[스팸을 별도의 폴더에 정리](#)"
- [465페이지](#)의 "[스팸 메일에 SpamAssassin 점수를 포함하는 헤더 추가](#)"

- [467페이지의 "SpamAssassin 결과 문자열을 제목 행에 추가"](#)

**주** 이 예에서는 많은 옵션과 키워드를 사용합니다. 자세한 내용은 [449페이지](#)의 "스팸 필터를 위한 MTA 채널 키워드"와 [452페이지](#)의 "MTA 스팸 필터 옵션(option.dat)"을 참조하십시오.

## 스팸을 별도의 폴더에 정리

이 예에서는 로컬 메시지 저장소에서 받는 메일을 테스트하여 스팸을 spam이라는 폴더에 정리합니다. 처음 세 단계는 순서에 관계없이 수행할 수 있습니다.

### 1. SpamAssassin 구성 파일을 만듭니다.

이 파일의 이름과 위치는 [단계 2](#)에서 지정합니다. spamassassin.opt라는 이름을 사용하는 것이 좋습니다. 이 파일은 다음과 같은 행으로 구성되어 있습니다.

```
host=127.0.0.1
port=2000
mode=0
verdict=spam
debug=1
```

host 및 port는 spamd가 실행 중인 시스템의 이름과 spamd가 받는 요청을 수신하는 포트를 지정합니다. mode=0은 메일이 스팸으로 간주될 때 verdict에 지정된 문자열이 반환되도록 지정합니다. debug=1은 SpamAssassin 라이브러리에서 디버깅을 설정합니다. SpamAssassin 구성 매개 변수에 대한 설명은 [471페이지의 표 14-4](#)를 참조하십시오.

2. option.dat 파일에 다음 행을 추가합니다.

```
! for Spamassassin
spamfilter1_config_file1=/opt/SUNWmsgsr/config/spamassassin.opt
spamfilter1_library1=/opt/SUNWmsgsr/lib/libspamass.so
spamfilter1_optional=1
spamfilter1_string_action=data:,require "fileinto"; fileinto "$U;
```

spamfilter1\_config\_files는 SpamAssassin 구성 파일을 지정합니다.

spamfilter1\_library는 SpamAssassin 공유 라이브러리를 지정합니다.

spamfilter1\_optional=1은 spamd에 의한 실패가 있더라도 MTA가 작업을 계속하도록 지정합니다.

spamfilter1\_string\_action은 스팸 메일에 대해 수행할 Sieve 작업을 지정합니다.

이 예에서는 기본값이 이미 data:,require "fileinto"; fileinto "\$U;로 설정되어 있기 때문에 spamfilter1\_string\_action은 필요하지 않습니다. 이 행은 스팸 메일을 폴더로 보내도록 지정합니다. 폴더 이름은 SpamAssassin에서 반환되는 스팸 답신 값입니다. SpamAssassin에서 반환되는 값은 spamassassin.opt의 verdict 옵션에 의해 지정됩니다. 단계 1을 참조하십시오. 이 경우 폴더 이름은 spam입니다.

3. 필터링할 메일을 지정합니다.

로컬 메시지 저장소로 들어오는 모든 메일을 필터링하려면 ims-ms 채널에 destinationspamfilterXoptin spam 키워드를 추가하여 imta.cnf 파일을 변경합니다.

```
!
! ims-ms
ims-ms defragment subdirs 20 notices 1 7 14 21 28 backoff "pt5m" "pt10m"
"pt30m" "pt1h" "pt2h" "pt4h" maxjobs 4 pool IMS_POOL fileinto
$U+$S@$D destinationspamfilter1optin spam
ims-ms-daemon
```

4. 구성을 다시 컴파일하고 서버를 다시 시작합니다. MTA만 다시 시작해야 합니다. stop-msg는 실행할 필요가 없습니다.

```
# imsimta cnbuild
# imsimta restart
```



5. `spamd` 데몬을 시작합니다. 이 작업은 다음과 같은 일반적인 명령 형식을 사용하여 수행됩니다.

```
spamd -d
```

`spamd` 기본값은 로컬 시스템으로부터의 연결만 허용하는 것입니다. SpamAssassin 과 Messaging Server가 서로 다른 시스템에서 실행 중인 경우 이 구문이 필요합니다.

```
spamd -d -i listen_ip_address -A allowed_hosts
```

여기서 `listen_ip_address`는 수신할 주소이고 `allowed_hosts`는 이 `spamd` 인스턴스에 연결할 수 있는 인증된 호스트 또는 네트워크(IP 주소 사용)의 목록입니다.

---

**주** `spamd`가 모든 주소에서 수신하게 하려면 0.0.0.0을 `-i listen_ip_address`와 함께 사용할 수 있습니다. 시스템의 IP 주소를 변경할 때 `itspamfilterX_verdict_n`으로 인해 명령 스크립트를 변경할 필요가 없기 때문에 모든 주소를 수신하게 하는 것이 좋습니다.

---

## 스팸 메일에 SpamAssassin 점수를 포함하는 헤더 추가

이 예에서는 SpamAssassin에 의해 스팸으로 확인된 메일에 `Spam-test: result string` 헤더를 추가합니다. 다음은 헤더 예입니다.

```
Spam-test: True ; 7.3 / 5.0
```

여기서 `Spam-test:`는 리터럴이고 그 뒤의 모든 항목은 결과 문자열입니다. `True`는 스팸임을 의미하고 `false`는 스팸이 아님을 의미합니다. 7.3은 SpamAssassin 점수입니다. 5.0은 임계값입니다. 이 결과는 특정 점수 이상 또는 사이의 메일을 파일로 저장하거나 삭제할 수 있는 Sieve 필터를 설정할 때 유용합니다.

또한, `USE_CHECK`를 0으로 설정하면 답신 문자열과 함께 일치하는 SpamAssassin 테스트 목록이 반환됩니다. 471페이지의 표 14-4의 `USE_CHECK`를 참조하십시오.

1. 필터링할 메일을 지정합니다. 이 내용은 463페이지의 "스팸을 별도의 폴더에 정리"의 단계 3에 설명되어 있습니다.

## 2. SpamAssassin 구성 파일을 만듭니다.

이 파일의 이름과 위치는 spamfilter\_configX\_file을 사용하여 지정합니다(다음 단계 참조). 이 파일은 다음과 같은 행으로 구성되어 있습니다.

```
host=127.0.0.1
port=2000
mode=1
field=
debug=1
```

host 및 port는 spamd가 실행 중인 시스템 이름과 spamd가 받는 요청을 수신하는 포트를 지정합니다. mode=1은 메일이 스팸으로 확인될 경우에 SpamAssassin 결과 문자열이 반환됨을 지정합니다. field=는 SpamAssassin 결과 문자열의 문자열 접두어를 지정합니다. 이 예에서는 Sieve 스크립트로 지정하기 때문에 접두어가 필요하지 않습니다. debug=1은 SpamAssassin 라이브러리에서 디버깅을 설정합니다.

## 3. option.dat 파일에 다음 행을 추가합니다.

```
!for Spamassassin
spamfilter_config_file=/opt/SUNWmsgsr/config/spamassassin.opt
spamfilter1_library=/opt/SUNWmsgsr/lib/libspamass.so
spamfilter1_optional=1
spamfilter1_string_action=data:,require ["addheader"];addheader "Spam-test: $U";
```

앞의 예와 마찬가지로 처음 세 옵션은 SpamAssassin 구성 파일과 공유 라이브러리를 지정하고 공유 라이브러리에 오류가 있을 경우 MTA 작업을 계속하도록 지정합니다. 다음 행은

```
spamfilter1_string_action=data:,require ["addheader"];addheader "Spam-test:
$U";
```

스팸 메일에 헤더를 추가하도록 지정합니다. 헤더에는 SpamAssassin에서 반환되는 문자열 앞에 Spam-text:라는 문자 접두어가 붙습니다. [단계 2](#)에서 mode=1로 지정했기 때문에 SpamAssassin 결과 문자열이 반환됩니다. 예를 들면 True; 7.3/5.0입니다.

## 4. 구성을 다시 컴파일하고 서버를 다시 시작한 다음 spamd 데몬을 시작합니다.

[463페이지의 "스팸을 별도의 폴더에 정리"](#)를 참조하십시오.

## SpamAssassin 결과 문자열을 제목 행에 추가

SpamAssassin 결과 문자열을 제목 행에 추가하여 SpamAssassin 점수로 메일을 읽을지 여부를 결정할 수 있습니다. 예를 들면 다음과 같습니다.

Subject: [SPAM True ; 99.3 / 5.0] Free Money At Home with Prescription Xanirex!

USE\_CHECK를 0으로 설정하면 답신 문자열과 함께 일치하는 SpamAssassin 테스트 목록이 반환됩니다(471페이지의 표 14-4의 USE\_CHECK 참조). 이 목록의 길이가 매우 길 수 있으므로 USE\_CHECK를 1로 설정하는 가장 것이 좋습니다.

1. 필터링할 메일을 지정합니다. 463페이지의 "스팸을 별도의 폴더에 정리"의 단계 3을 참조하십시오.
2. SpamAssassin 구성 파일을 만듭니다.

이 단계는 463페이지의 "스팸을 별도의 폴더에 정리"에 설명되어 있습니다. mode=1은 메일이 스팸으로 확인되는 경우 SpamAssassin 결과 문자열을 반환하도록 지정합니다.

```
host=127.0.0.1
port=2000
mode=1
debug=1
```

host 및 port는 spamd가 실행 중인 시스템 이름과 spamd가 받는 요청을 수신하는 포트를 지정합니다. mode=1은 메일이 스팸으로 확인될 경우에 SpamAssassin 결과 문자열이 반환되도록 지정합니다. debug=1은 SpamAssassin 라이브러리에서 디버깅을 설정합니다.

3. option.dat 파일에 다음 행을 추가합니다.

```
!for Spamassassin
spamfilter1_config_file=/opt/SUNWmsgsr/config/spamassassin.opt
spamfilter1_library=/opt/SUNWmsgsr/lib/libspamass.so
spamfilter1_optional=1
spamfilter1_string_action=data:;addtag "[SPAM detected: $U]";
```

앞의 예와 마찬가지로 처음 세 옵션은 SpamAssassin 구성 파일과 공유 라이브러리를 지정하고 공유 라이브러리에 오류가 있을 경우 MTA 작업을 계속하도록 지정합니다. 다음 행은

```
spamfilter1_string_action=data:,addtag "[SPAM detected $U]";
```

Subject: 행에 태그를 추가하도록 지정합니다. SpamAssassin에서 반환되는 "[*result string*]" 앞의 field 문자열(기본값: Spam-Test) 앞에 SPAM detected라는 문자 접두어가 있습니다. 단계 2에서 mode=1로 지정했기 때문에 SpamAssassin 결과 문자열이 반환됩니다. 따라서, 제목 행은 다음과 비슷합니다.

```
Subject: [SPAM detected Spam-Test: True ; 11.3 / 5.0] Make Money!
```

addheader와 addtag를 함께 사용하여

```
spamfilter1_string_action=data:,require ["addheader"];addtag "[SPAM detected $U]";addheader "Spamscore: $U";
```

다음과 비슷한 메일을 볼 수도 있습니다.

```
Subject: [SPAM detected Spam-Test: True ; 12.3 / 5.0] Vigarò Now!  
Spamscore: Spam-Test: True ; 12.3 / 5.0
```

spamassassin.opt에서 field=를 설정하여 Spam-Test의 기본값을 제거합니다. 더 명확한 메일이 반환됩니다.

```
Subject: [SPAM True ; 91.3 / 5.0] Vigarò Now!  
Spamscore: True ; 91.3 / 5.0
```

4. 구성을 다시 컴파일하고 서버를 다시 시작한 다음 spamd 데몬을 시작합니다.

[463페이지의 "스팸을 별도의 폴더에 정리"](#)를 참조하십시오.

## SpamAssassin 테스트

SpamAssassin을 테스트하려면 spamassassin.opt 파일에서 debug=1을 설정합니다. imta.cnf에서 채널별 master\_debug 또는 slave\_debug를 설정할 필요는 없습니다. 그런 다음 테스트 사용자에게 테스트 메일을 보냅니다.

msg\_svr\_base/data/tcp\_local\_slave.log\* 파일은 다음과 비슷한 행으로 구성됩니다.

```
15:15:45.44: SpamAssassin callout debugging enabled; config
/opt/SUNWmsgsr/config/spamassassin.opt
15:15:45.44: IP address 127.0.0.1 specified
15:15:45.44: Port 2000 selected
15:15:45.44: Mode 0 selected
15:15:45.44: Field "Spam-Test: " selected
15:15:45.44: Verdict "spam" selected
15:15:45.44: Using CHECK rather than SYMBOLS
15:15:45.44: Initializing SpamAssassin message context
...
15:15:510.42: Creating socket to connect to SpamAssassin
15:15:510.42: Binding SpamAssassin socket
15:15:510.42: Connecting to SpamAssassin
15:15:510.42: Sending SpamAssassin announcement
15:15:510.42: Sending SpamAssassin the message
15:15:510.42: Performing SpamAssassin half close
15:15:510.42: Reading SpamAssassin status
15:15:510.67: Status line: SPAMD/1.1 0 EX_OK
15:15:510.67: Reading SpamAssassin result
15:15:51.67: Result line: Spam: False ; 1.3 / 5.0
15:15:51.67: Verdict line: Spam-Test: False ; 1.3 / 5.0
15:15:510.67: Closing connection to SpamAssassin
15:15:510.73: Freeing SpamAssassin message context
```

로그 파일이 위와 비슷한 행으로 구성되어 있지 않거나 spamd가 실행되고 있지 않은 경우 마지막 마침표(.)가 SMTP 서버로 보내진 후에 SMTP 대화 상자에 다음 오류 메시지가 반환됩니다.

```
452 4.4.5 Error writing message temporaries - Temporary scan failure: End
message status = -1
```

또한, spamfilter1\_optional=1(권장)이 option.dat에 설정되어 있는 경우 메일이 허용되지만 필터링되지는 않습니다. 스팸 필터링이 활성화되지 않은 경우와 동일하며 tcp\_local\_slave.log\*에 다음 행이 나타납니다.

```
15:35:150.69: Creating socket to connect to SpamAssassin
15:35:15.69: Binding SpamAssassin socket
15:35:15.69: Connecting to SpamAssassin
15:35:15.69: Error connecting socket: Connection refused
15:35:15.72: Freeing SpamAssassin message context
```

SMTP 서버에서 전체 메일을 수신한 후(마지막 "."가 SMTP 서버로 보내진 후), SMTP 서버가 메일을 수락했음을 보낸 사람이 알기 전에 SpamAssassin이 호출됩니다.

Mail-SpamAssassin-2.60과 같은 디렉토리에서 sample-spam.txt를 사용하여 샘플 스팸 메일을 보내는 다른 테스트를 수행합니다. 이 메일에는 내부에 다음과 같은 특수 텍스트 문자열이 있습니다.

```
XJS*C4JDBQADN1.NSBN3*2IDNEN*GTUBE-STANDARD-ANTI-UBE-TEST-EMAIL*C.34X
```

해당 tcp\_local\_slave.log\*는 다음과 같은 내용으로 구성되어 있습니다.

```
16:00:08.15: Creating socket to connect to SpamAssassin
16:00:08.15: Binding SpamAssassin socket
16:00:08.15: Connecting to SpamAssassin
16:00:08.15: Sending SpamAssassin announcement
16:00:08.15: Sending SpamAssassin the message
16:00:08.15: Performing SpamAssassin half close
16:00:08.15: Reading SpamAssassin status
16:00:08.43: Status line: SPAMD/1.1 0 EX_OK
16:00:08.43: Reading SpamAssassin result
16:00:08.43: Result line: Spam: True ; 1002.9 / 5.0
16:00:08.43: Verdict line: Spam-Test: True ; 1002.9 / 5.0
16:00:08.43: Closing connection to SpamAssassin
16:00:08.43: Mode 0 verdict of spam
16:00:08.43: Mode 0 verdict of spam
16:00:08.47: Freeing SpamAssassin message context
```

mail.log\_current 파일의 해당 항목은 다음과 비슷합니다. 메일이 spam이라는 폴더에 정리되어 있음을 의미하는 메일 주소의 +spam 부분에 주의하십시오.

```
15-Dec-2003 15:32:17.44 tcp_intranet ims-ms E 1 morchia@siroe.com rfc822;morchia
morchia+spam@ims-ms-daemon
15-Dec-2003 15:32:18.53 ims-ms D 1 morchia@siroe.com rfc822;morchia
morchia+spam@ims-ms-daemon
```

## SpamAssassin 옵션

이 절에는 SpamAssassin 옵션 표가 포함되어 있습니다.

**표 14-4** SpamAssassin 옵션(spamassassin.opt)

| 옵션    | 설명                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 기본값         |
|-------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|
| debug | libspamass.so에서 디버깅을 설정할지 여부를 지정합니다. spamd에 대한 디버깅은 spamd를 호출하는 명령줄에 의해 제어됩니다. 0 또는 1로 설정합니다.                                                                                                                                                                                                                                                                                                                                                                              | 0           |
| field | SpamAssassin 결과 문자열 접두어를 지정합니다. SpamAssassin 결과는 다음과 비슷합니다.<br><br>Spam-Test: False ; 0.0 / 5.0<br>Spam-Test: True ; 27.7 / 5.0<br><br>field 옵션을 사용하면 결과의 Spam-Test: 부분을 변경할 수 있습니다. 빈 field 값을 지정하는 경우 ":"이 제거된다는 점을 유의하십시오.<br><br><a href="#">USE_CHECK</a> 를 0으로 설정하면 다음과 비슷한 결과 문자열이 표시됩니다.<br><br>Spam-test: False ; 0.3 / 4.5 ; HTML_MESSAGE,NO_REAL_NAME<br><br>Spam-test: True ; 8.8 / 4.5 ; NIGERIAN_BODY,<br>NO_REAL_NAME,PLING_PLING,RCVD_IN_SBL,SUBJ_ALL_CAPS | "Spam-test" |
| host  | spamd가 실행 중인 시스템의 이름입니다.                                                                                                                                                                                                                                                                                                                                                                                                                                                   | localhost   |

표 14-4 SpamAssassin 옵션(spamassassin.opt)

| 옵션             | 설명                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | 기본값  |
|----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|
| mode           | <p>SpamAssassin 필터 결과를 답신 정보로 변환하는 것을 제어합니다. 즉, 메일을 처리한 후 반환되는 답신 정보를 지정합니다. 다음과 같은 네 가지 모드를 사용할 수 있습니다. 자세한 내용은 473페이지의 "SpamAssassin mode 옵션"을 참조하십시오.</p> <p>0 - 메일이 스팸일 경우 <i>답신 문자열(verdict 옵션에 의해 지정됨)</i>을 반환합니다. MTA 옵션 <code>spamfilterX_string_action</code>은 <code>verdict</code> 문자열이 반환될 경우 작업할 내용을 지정하는 데 사용될 수 있습니다. 아래에 정의된 <code>verdict</code> 옵션이 비어 있거나 지정되지 않고 메일이 스팸이면 <i>null 답신</i>이 반환됩니다. MTA 옵션 <code>spamfilterX_null_action</code>은 null 답신이 반환될 경우에 수행할 작업을 지정합니다.</p> <p>스팸이 아닌 경우 <i>SpamAssassin 기본 답신 문자열</i>을 반환합니다. 기본 답신은 항상 작업을 수행하지 않고 정상적으로 전달됨을 의미합니다.</p> <p>1 - 메일이 스팸인 경우 SpamAssassin <i>결과 문자열</i>을 반환합니다. 스팸이 아닌 경우 <i>SpamAssassin 기본 답신 문자열</i>을 반환합니다. 여기서도 기본 답신은 항상 작업을 수행하지 않고 정상적으로 전달됨을 의미합니다. SpamAssassin 결과 문자열은 <code>True; 6.5 / 7.3</code>과 비슷합니다.</p> <p>2 - 메일이 스팸인지 여부에 관계 없이 SpamAssassin 결과 문자열이 반환된다는 점을 제외하고 모드 1과 동일합니다. 기본 또는 null 답신이 반환되지 않으며 <code>verdict</code> 옵션이 사용되지 않습니다.</p> <p>3 - 메일이 스팸인 경우에는 SpamAssassin 결과 문자열을 반환하고 스팸이 아닌 경우에는 <code>verdict</code> 옵션에 지정된 <code>verdict</code> 문자열을 반환합니다. <code>spamfilterX_verdict_n</code> 및 <code>spamfilterX_action_n</code> 일치 쌍을 사용하여 SpamAssassin 결과 문자열의 작업을 제어할 수 있습니다. <code>spamfilterX_string_action</code>을 사용하여 <code>verdict</code> 문자열의 작업을 제어할 수 있습니다.</p> | 0    |
| port           | spamd가 수신 요청을 수신하는 포트 번호입니다.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | 783  |
| USE_CHECK      | <p>1 - spamd CHECK 명령을 사용하여 SpamAssassin 점수를 반환합니다.</p> <p>0 - SYMBOLS 명령을 사용하여 일치하는 SpamAssassin 테스트의 점수와 목록을 반환합니다. 2.55 이전 버전 SpamAssassin에서는 이 옵션을 사용하면 시스템이 중단되거나 다른 문제가 발생할 수 있습니다. 위의 <code>field</code>를 참조하십시오.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |      |
| SOCKS_HOST     | 문자열입니다. 중간 SOCKS 서버의 이름을 지정합니다. 이 옵션을 지정하면 ICAP가 직접 연결되지 않고 지정된 SOCKS 서버를 통해 연결됩니다.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | ""   |
| SOCKS_PORT     | 중간 SOCKS 서버가 실행 중인 포트를 지정합니다.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | 1080 |
| SOCKS_PASSWORD | SOCKS 서버를 통해 연결을 설정할 때 사용할 비밀번호(문자열)를 지정합니다. 아이디/비밀번호가 필요한지 여부는 SOCKS 서버 구성에 따라 다릅니다.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | ""   |
| SOCKS_USERNAME | SOCKS 서버를 통해 연결을 설정할 때 사용할 아이디(문자열)를 지정합니다.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | ""   |
| verdict        | MODE 0에 사용되는 답신 문자열을 지정합니다.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | ""   |



## SpamAssassin mode 옵션

메일을 처리한 후, SpamAssassin에서 메일이 스팸인지 아닌지를 파악합니다. mode를 사용하면 답신을 나타내도록 반환되는 문자열을 지정할 수 있습니다. 선택할 수 있는 옵션으로는 null이나 기본값 SpamAssassin 결과 문자열, verdict 옵션으로 지정된 verdict 문자열이 있습니다. (기본값은 null이나 SpamAssassin 결과 문자열, verdict에서 지정한 문자열 중 어느 것도 아니지만 기타 비구성 결과 문자열이라는 점을 유의하십시오.) 아래 테이블은 mode 작업에 대한 개요입니다.

표 14-5 SpamAssassin mode 옵션의 문자열 반환

| verdict 설정              | 스팸  | mode=0         | mode=1             | mode=2             | mode=3             |
|-------------------------|-----|----------------|--------------------|--------------------|--------------------|
| verdict=""<br>(설정되지 않음) | 예   | null           | SpamAssassin<br>결과 | SpamAssassin<br>결과 | SpamAssassin<br>결과 |
|                         | 아니요 | 기본값            | 기본값                | SpamAssassin<br>결과 | 기본값                |
| verdict=string          | 예   | verdict<br>문자열 | SpamAssassin<br>결과 | SpamAssassin<br>결과 | SpamAssassin<br>결과 |
|                         | 아니요 | 기본값            | 기본값                | SpamAssassin<br>결과 | verdict<br>문자열     |

첫 번째 열은 verdict 옵션의 설정 여부를 나타냅니다. 두 번째 열은 해당 메일이 스팸인지 여부를 나타냅니다. 모드 열은 다양한 모드에 반환된 문자열을 나타냅니다. 예를 들어, verdict가 설정되어 있지 않고 mode가 0으로 설정되어 있으며 메일이 스팸이 아닐 때는 기본 문자열이 반환됩니다. verdict가 YO SPAM!으로, mode가 0으로 설정되어 있고 메일이 스팸인 경우에는 YO SPAM! 문자열이 반환됩니다.

## SAVSE(Symantec Anti-virus Scanning Engine) 사용

이 절에서는 SAVSE를 배포하는 방법에 대해 설명하지만 다른 ICAP 지원 스팸 방지/바이러스 백신 프로그램을 배포하는 데에도 도움이 될 것입니다. 이 절은 다음과 같은 하위 절로 구성되어 있습니다.

- 474페이지의 "SAVSE 개요"
- 474페이지의 "SpamAssassin 요구 사항 및 사용 시 고려 사항"

- [475페이지의 "SAVSE 배포"](#)
- [475페이지의 "SAVSE 구성 예"](#)
- [478페이지의 "SAVSE 옵션"](#)

## SAVSE 개요

SAVSE는 TCP/IP 서버 응용 프로그램 및 통신 API(Application Programming Interface)로서, 바이러스 스캐닝 서비스를 제공합니다. 네트워크 인프라 장치를 통해 서비스되거나 저장되는 트래픽을 방지하도록 특별히 설계되었기 때문에 모든 주요 파일 형식(모바일 코드와 압축 파일 형식 포함)에 있는 바이러스와 웜, 트로이 목마 등을 감지하고 방지합니다. 자세한 내용은 Symantec 웹 사이트를 참조하십시오.

---

**주** Messaging Server는 SAVSE 스캔 기능만 지원합니다. 복구를 지원하지하거나 기능을 삭제하지 않습니다.

---

## SpamAssassin 요구 사항 및 사용 시 고려 사항

이는 Symantec으로부터 별도의 라이선스를 받은 제품입니다.

SAVSE 구성에서는 스캔 모드만 지원되며 스캔과 복구 모드 또는 스캔과 삭제 모드는 지원되지 않습니다.

### SAVSE 실행 위치

SAVSE 또는 ICAP를 지원하는 다른 서버는 자체의 별도 시스템, 단일 시스템 배포의 Messaging Server와 동일한 시스템 또는 2계층 배포의 MTA와 동일한 시스템에서 실행할 수 있습니다. LMTP(Local Mail Transfer Protocol)가 MTA와 메시지 저장소 사이에서 사용되는 경우 MTA에서 필터링을 호출해야 합니다. 메시지 저장소에서는 필터링을 호출할 수 없습니다. MTA와 메시지 저장소 간에 SMTP가 사용되는 경우 각 시스템이나 별도의 타사 시스템에서 실행할 수 있습니다.

SAVSE를 실행하는 서버 그룹을 사용하려면 해당 그룹의 앞에 로드 밸런서를 사용해야 합니다. MTA는 SpamAssassin 서버에 대해 단일 주소로만 구성됩니다.

## SAVSE 배포

SAVSE를 배포하려면 다음 단계를 수행합니다.

- **SAVSE를 설치 구성합니다.** 설치 및 구성 정보는 Symantec 소프트웨어 설명서를 참조하십시오. [478페이지](#)의 "[SAVSE 옵션](#)"도 참조하십시오.
- **SAVSE 클라이언트 라이브러리를 로드 및 구성합니다.** 이 작업에는 클라이언트 라이브러리 libicap.so와 MTA에 대한 구성 파일(만들어야 함)을 지정하는 것이 포함됩니다. [443페이지](#)의 "[스팸 필터링 소프트웨어 클라이언트 라이브러리 로드 및 구성](#)"을 참조하십시오.
- **바이러스를 필터링할 메일을 지정합니다.** 사용자, 도메인 또는 채널별로 메일을 필터링할 수 있습니다. [444페이지](#)의 "[필터링할 메일 지정](#)"을 참조하십시오.
- **바이러스 메일에 대해 수행할 작업을 지정합니다.** 바이러스 삭제, 폴더에 정리, 제목 행에 태그 지정 등의 작업을 수행할 수 있습니다. [451페이지](#)의 "[스팸 메일에 대해 수행할 작업 지정](#)"을 참조하십시오.
- **기타 필터 구성 매개 변수를 원하는 대로 설정합니다.** [452페이지](#)의 "[MTA 스팸 필터 옵션\(option.dat\)](#)"을 참조하십시오.

## SAVSE 구성 예

다음 예에서는 로컬 메시지 저장소에서 받는 메일을 테스트하여 바이러스가 첨부된 메일을 삭제합니다. 처음 세 단계는 순서에 관계없이 수행할 수 있습니다.

### 1. SAVSE 구성 파일을 만듭니다.

이 파일의 이름과 위치는 [단계 2](#)에서 지정합니다. 여기에서 사용되는 이름은 SAVSE.opt입니다. 다음은 이 파일의 예입니다.

```
host=127.0.0.1
port=1344
mode=0
verdict=virus
debug=1
```

host 및 port는 SAVSE 프로그램이 실행 중인 시스템의 이름과 이 프로그램이 수신 요청을 수신하는 포트(SAVSE의 기본 포트는 1344임)를 지정합니다. mode=0은 메일이 스팸으로 간주될 때 verdict에 지정된 문자열(이 경우 단어 virus)이 반환되도록 지정합니다. debug=1은 디버깅을 설정합니다. ICAP 구성 매개 변수에 대한 설명은 [478페이지의 표 14-6](#)을 참조하십시오.

- option.dat 파일을 만듭니다. 예를 들면 다음과 같습니다.

```
! for Symantex Anti-virus Scan Engine
spamfilter1_config_file=/opt/SUNWmsgsr/config/SAVSE.opt
spamfilter1_library=/opt/SUNWmsgsr/lib/libicap.so
spamfilter1_optional=1
spamfilter1_string_action=data:,discard
```

spamfilter1\_config\_files는 SAVSE 구성 파일을 지정합니다.

spamfilter1\_library는 SAVSE 공유 라이브러리의 위치를 지정합니다.

spamfilter1\_optional=1은 SAVSE 프로그램에 오류가 있더라도 MTA가 작업을 계속하도록 지정합니다.

spamfilter1\_string\_action은 스팸 메일에 대해 수행할 Sieve 작업을 지정합니다. 이 값은 바이러스가 있는 메일을 삭제하도록 지정하며 이 값은 기본값이기 때문에 값을 바꾸지 않는 한 지정할 필요가 없습니다.

- 필터링할 메일을 지정합니다.

로컬 메시지 저장소로 들어오는 모든 메일을 필터링하려면 ims-ms 채널에 destinationspamfilterloptin spam 키워드를 추가하여 imta.cnf 파일을 변경합니다.

```
!
! ims-ms
ims-ms defragment subdirs 20 notices 1 7 14 21 28 backoff "pt5m" "pt10m"
"pt30m" "pt1h" "pt2h" "pt4h" maxjobs 4 pool IMS_POOL fileinto
$U+$S@$D destinationspamfilterloptin virus
ims-ms-daemon
```

4. 구성을 다시 컴파일하고 서버를 다시 시작합니다. MTA만 다시 시작해야 합니다. stop-msg는 실행할 필요가 없습니다.

```
# imsimta cnbuild
# imsimta restart
```

5. SAVSE가 시작되는지 확인합니다.

자동으로 시작되어야 하지만, 그렇지 않은 경우는 `/etc/init.d/symcscna start`와 같은 `start` 명령을 사용합니다

## 가능한 다른 구성

mode를 0으로 설정하면 spamfilterX\_null\_option을 사용하여 스팸으로 확인된 메일을 특정 폴더에 정리하는 등의 다른 작업을 수행하도록 지정할 수 있습니다. 예를 들면 다음과 같습니다.

```
spamfilter1_null_option=data:,require "fileinto"; fileinto "VIRUS";
```

감염된 메일을 폴더에 정리하는 것은 대부분의 경우 좋지 않습니다.

mode를 1로 설정하여 작업을 시작할 수도 있습니다. 예를 들어, mode를 1로 설정하고 MTA에서 spamfilterX\_string\_action 옵션을 다음과 같이 설정하여 스팸 결과를 거부 메일에 포함할 수 있습니다.

```
spamfilter1_string_action=data:,require "reject"; reject "Message contained a virus [$U]";
```

fileinto와 마찬가지로 reject 작업을 사용하여 바이러스를 처리하는 것은 바이러스가 보낸 사람에게 다시 전송되므로 좋은 방법이 아닙니다.

option.dat 파일에 한 행을 추가하여 스팸 메일 헤더에 태그를 추가할 수도 있습니다. 예를 들면 다음과 같습니다.

```
spamfilter1_string_action=data:,addtag "[SPAM detected!]";
```

메일이 바이러스를 포함하는 것으로 확인되었는지 여부에 상관없이 작업을 수행해야 할 경우에는 mode를 2로 설정할 수 있습니다. 나중에 테스트할 수 있는 헤더 필드를 추가하는 것을 모드 2의 예로 볼 수 있습니다.

```
spamfilterX_string_action=data:,require ["addheader"];addheader "$U"
```

## SAVSE 옵션

SAVSE 옵션 파일은 아주 일반적인 ICAP 옵션 파일입니다. 이 파일의 이름과 위치는 option.dat의 spamfilterX\_config\_file에 설정합니다. 이 파일은 option=value 형태의 행으로 구성됩니다. 유일한 필수 옵션은 HOST입니다. 이 옵션은 ICAP 필터링 서버가 실행 중인 시스템의 이름으로 설정해야 합니다. ICAP 서버가 로컬 호스트에서 실행 중인 경우에도 이 옵션을 설정해야 합니다. 이 옵션 파일은 아래와 같습니다.

**표 14-6** ICAP 옵션

| 옵션    | 설명                                                                                                                                                                                                   | 기본값        |
|-------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|
| debug | ICAP 인터페이스 모듈에서 디버그 출력을 활성화하거나 비활성화합니다. 0 또는 1입니다.                                                                                                                                                   | 0          |
| field | ICAP 결과 접두어를 지정합니다. SAVSE 결과 문자열은 다음과 비슷합니다.<br>Virus-Test: False<br>Virus-Test: True; W32.Mydoom.A@mm.enc<br>이 옵션은 결과의 Virus-Test: 부분을 변경할 수 있는 방법을 제공합니다. 빈 field 값을 지정하는 경우 "."이 제거된다는 점을 유의하십시오. | Virus-test |
| host  | ICAP 필터링 서버가 실행 중인 시스템의 이름입니다.                                                                                                                                                                       | localhost  |

표 14-6 ICAP 옵션

| 옵션             | 설명                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | 기본값  |
|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|
| mode           | <p>ICAP 필터 결과를 답신 정보로 변환하는 것을 제어합니다. 즉, 메일을 처리한 후 반환되는 문자열 정보를 지정합니다. 다음과 같은 네 가지 모드를 사용할 수 있습니다. 자세한 내용은 480페이지의 "ICAP mode 옵션"을 참조하십시오.</p> <p>0 - 메일에 바이러스가 포함된 경우 <i>답신 문자열(verdict 옵션에 의해 지정됨)</i>을 반환합니다. MTA 옵션 <code>spamfilterX_string_action</code>은 <code>verdict</code> 문자열이 반환될 경우 수행할 작업을 지정하는 데 사용될 수 있습니다. <code>verdict</code> 옵션이 비어 있거나 지정되지 않은 경우 <code>null</code> 답신이 반환됩니다. MTA 옵션 <code>spamfilterX_null_action</code>은 기본 작업을 무시함으로써 메일을 버리게 될 경우와 <code>null</code> 답신이 반환될 경우 수행할 작업을 지정하는 데 사용될 수 있습니다.</p> <p>메일에 바이러스가 포함되지 않은 경우 기본 답신이 반환됩니다. 기본 문자열은 구성할 수 없으며 항상 작업을 수행하지 않고 정상적으로 전달됨을 의미합니다.</p> <p>1 - 메일에 바이러스가 있을 경우 ICAP <i>결과 문자열</i>을 반환합니다. 메일에 바이러스가 포함되지 않은 경우 기본 문자열이 반환됩니다. 기본 문자열은 항상 작업을 수행하지 않고 정상적으로 전달됨을 의미합니다. 다음은 SAVSE 결과 문자열의 두 가지 예입니다.</p> <p>VIRUS TEST: FALSE<br/>VIRUS-TEST: TRUE; W32.Mydoom.A@mm.enc</p> <p>2 - 무조건적으로 ICAP 결과 문자열을 답신으로 반환합니다. 기본 또는 <code>null</code> 답신이 반환되지 않으며 <code>verdict</code> 옵션이 사용되지 않습니다. 이 설정은 메일이 바이러스를 포함하는 것으로 확인되었는지 여부에 상관없이 작업을 수행해야 할 경우에 사용됩니다. 나중에 테스트할 수 있는 헤더 필드를 추가하는 것을 모드 2 적용의 예로 볼 수 있습니다.</p> <p><code>spamfilterX_string_action=data:,require ["addheader"];addheader "\$U"</code></p> <p>3 - 메일에 바이러스가 있는 경우 ICAP 결과 문자열이 반환되고 <code>verdict</code> 옵션에서 지정한 <code>verdict</code> 문자열이 반환됩니다. 이 설정은 바이러스가 확인된 경우 특정 작업을 수행하고 그렇지 않은 경우 다른 작업을 수행해야 하는 경우에 사용됩니다. <code>spamfilterX_verdict_n</code> 및 <code>spamfilterX_action_n</code> 일치 쌍을 사용하여 ICAP 결과 문자열의 작업을 제어할 수 있습니다. <code>spamfilterX_string_action</code>을 사용하여 <code>verdict</code> 문자열의 작업을 제어할 수 있습니다.</p> | 0    |
| port           | ICAP 서버가 실행 중인 포트 번호를 지정합니다.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 1344 |
| SOCKS_HOST     | 문자열입니다. 중간 SOCKS 서버의 이름을 지정합니다. 이 옵션을 지정하면 ICAP가 직접 연결되지 않고 지정된 SOCKS 서버를 통해 연결됩니다.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | ""   |
| SOCKS_PORT     | 정수입니다. 중간 SOCKS 서버가 실행 중인 포트를 지정합니다.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 1080 |
| SOCKS_PASSWORD | 문자열입니다. SOCKS 서버를 통해 연결을 설정할 때 사용할 비밀번호를 지정합니다. 아이디/비밀번호가 필요하지 여부는 SOCKS 서버 구성에 따라 다릅니다.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | ""   |
| SOCKS_USERNAME | 문자열입니다. SOCKS 서버를 통해 연결을 설정할 때 사용할 아이디를 지정합니다.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | ""   |
| verdict        | MODE 0과 3에 사용되는 답신 문자열을 지정합니다.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | ""   |

## ICAP mode 옵션

메일을 처리한 후, SASVE와 같은 ICAP 바이러스 방지 프로그램은 메일에 바이러스가 있는지 여부를 파악합니다. mode를 사용하면 이 답신을 나타내는 ICAP 프로그램에서 반환하는 문자열을 지정할 수 있습니다. 선택할 수 있는 옵션으로는 *null*이나 *기본값*, *ICAP 결과 문자열*, *verdict 문자열*(*verdict* 옵션으로 지정) 등이 있습니다. 기본값은 *null*이나 *ICAP 결과 문자열*, *verdict*로 지정된 문자열이 아니지만 프로그램에서 반환한 기타 비구성 문자열이라는 점을 유의하십시오. 아래 테이블은 mode 작업에 대한 개요입니다.

표 14-7 ICAP 모드 옵션의 답신 문자열 반환

| verdict 설정              | 바이러스 | mode=0         | mode=1  | mode=2  | mode=3         |
|-------------------------|------|----------------|---------|---------|----------------|
| verdict=""<br>(설정되지 않음) | 예    | null           | ICAP 결과 | ICAP 결과 | ICAP 결과        |
|                         | 아니요  | 기본값            | 기본값     | ICAP 결과 | 기본값            |
| verdict=string          | 예    | verdict<br>문자열 | ICAP 결과 | ICAP 결과 | ICAP 결과        |
|                         | 아니요  | 기본값            | 기본값     | ICAP 결과 | verdict<br>문자열 |

첫 번째 열은 *verdict* 옵션이 설정되어 있는지 여부를 나타냅니다. 두 번째 열은 메일에 바이러스가 있는지 여부를 나타냅니다. 모드 열은 여러 모드에 문자열이 반환되었음을 나타냅니다. 예를 들어, *verdict*가 설정되어 있지 않고 *mode*가 0으로 설정되어 있으며 메일에 바이러스가 없을 경우 ICAP 프로그램에서 기본값을 반환합니다. *verdict*가 *WARNING VIRUS!*로, *mode*가 0으로 설정되어 있고 메일에 바이러스가 있으면 ICAP 프로그램에서 *WARNING VIRUS!*라는 문자열을 반환합니다.

## Sieve 확장 지원

표준 Sieve 함수 외에도 Messaging Server는 *addheader*, *addtag*, *spamtest* 및 *spamadjust*를 비롯한 여러 확장에 대한 지원을 제공합니다. *addheader* 및 *addtag*는 465 페이지의 "스팸 메일에 SpamAssassin 점수를 포함하는 헤더 추가" 및 467페이지의 "SpamAssassin 결과 문자열을 제목 행에 추가"에 설명되어 있으며 *spamtest* 및 *spamadjust*는 여기에서 설명합니다.

관리자는 이러한 확장을 사용하여 서로 다른 임계값을 설정하고 SpamAssassin 답신을 대체하는 목록을 설정할 수 있습니다. 특정 메일을 보낸 사용자에 따라 두 가지를 결합하여 서로 다른 임계값을 지정할 수 있습니다. *spamadjust*는 비표준 작업입니다. *spamtest*는 <ftp://ftp.isi.edu/in-notes/rfc3685.txt>에 설명되어 있습니다.



spamtest를 사용하면 Sieve [RELATIONAL]을 "i;ascii-numeric" 구분 문자와 함께 사용하여 SpamAssassin 점수를 특정 값과 비교할 수 있습니다. SpamAssassin 점수는 일반적으로 실수이지만 spamtest는 점수를 근사 정수로 반올림하여 0과 10 사이의 정수 값으로 강제합니다. 0 미만인 값은 0으로 반올림되고 10을 초과하는 값은 10으로 내림합니다. Messaging Server에서 유지 관리되는 텍스트 문자열을 첨부하여 spamtest 테스트에 표시되는 테스트 문자열을 생성합니다.

spamadjust는 현재 스팸 점수를 조정하는 데 사용됩니다. 이 작업은 실수 값에 대해 스캔되는 단일 문자열 인수를 가져옵니다. 이 값은 현재 스팸 점수를 조정하는 데 사용됩니다. 전체 문자열이 현재 점수 텍스트 문자열에 첨부됩니다. 아래의 예에서 문자열은 "undisclosed recipients"입니다.

여러 spamadjust 작업이 허용되고 각 작업이 현재 점수에 추가됩니다. 점수 값은 항상 0에서 시작합니다. 서명된 숫자값을 허용하여 현재 점수를 내리거나 높일 수 있습니다. spamadjust에 대한 require 절이 없으므로 spamtest 확장이 대신 나열되어야 합니다.

예를 들어, SpamAssassin MODE 설정 2와 함께 사용할 수 있는 spamadjust는 다음과 같습니다.

```
spamfilterX_string_action=data:,require ["spamtest"];spamadjust "$U";
```

시스템 수준 Sieve 필터는 특정 헤더 유형(있는 경우)을 검사한 다음 SpamAssassin 점수에 5를 더하여 SpamAssassin 점수를 수정할 수 있습니다.

```
spamfilter1_string_action=require "spamtest"; \
if header :contains ["to", "cc", "bcc", "resent-to", "resent-cc", "resent-bcc"] \
    [<undisclosed recipients>, "undisclosed.recipients"] \
{spamadjust "+5 undisclosed recipients";}
```

마지막으로 사용자 수준 Sieve 스크립트는 결과 값을 테스트하고 스팸으로 확인된 메일을 삭제하고, 스팸일 확률이 있는 메일을 파일로 저장하고, 메일을 로컬 도메인의 주소에서 통과하도록 허용할 수 있습니다.

```
spamfilter1_string_action=require ["spamtest", "relational", \
"comparator-i;ascii-numeric", "fileinto"]; \
if anyof (address :matches "from" ["*@siroe.com", \
"*@*.siroe.com"]) \
{keep;} \
elsif spamtest :value "ge" :comparator "i;ascii-numeric" "8" \
{discard;} \
elsif spamtest :value "ge" :comparator "i;ascii-numeric" "5" \
{fileinfo "spam-likely";} \
else \
{keep;}
```

Sieve 확장 지원

# LMTP 전달

Sun Java System Messaging Server MTA는 다중 계층 Messaging Server 배포가 사용되는 상황에서 메시지 저장소로의 전달을 위해 LMTP(RFC 2033에 정의된 Local Mail Transfer Protocol)를 사용할 수 있습니다. 인바운드 릴레이와 백엔드 메시지 저장소를 사용하는 이 시나리오에서는 릴레이가 주소 확장 및 전달 방법(예: 자동 회신, 전달)뿐만 아니라 메일 목록 확장을 담당합니다. 기본적으로 백엔드 저장소에 대한 전달은 백엔드 시스템이 LDAP 디렉토리에서 수신자 주소를 다시 조회해야 하는 SMTP를 통해 이루어지므로 전체 MTA 방법이 사용됩니다. 빠르고 효율적인 전달을 위해 MTA는 SMTP 대신 LMTP를 사용하여 메일을 백엔드 저장소에 전달할 수 있습니다. Sun Java System Messaging Server의 LMTP 서버는 일반적인 용도의 LMTP 서버가 아니라 릴레이와 백엔드 메시지 저장소 사이의 개인 프로토콜 역할을 합니다. 설명의 단순화를 위해 2계층 배포를 포함하는 예를 사용합니다.

---

**주** LMTP는 다중 계층 배포에서 사용하도록 설계되었기 때문에 단일 시스템 배포에서는 사용할 수 없습니다. 또한 Messaging Server의 LMTP 서비스는 다른 LMTP 서버나 다른 LMTP 클라이언트와 함께 작동하도록 설계되지 않았습니다.

---

이 장은 다음 내용으로 구성되어 있습니다.

- 484페이지의 "LMTP 전달 기능"
- 484페이지의 "LMTP를 사용하지 않는 2계층 배포의 메일 처리"
- 486페이지의 "LMTP를 사용하는 2계층 배포의 메일 처리"
- 487페이지의 "LMTP 개요"
- 498페이지의 "구현된 LMTP 프로토콜"

- [488페이지의 "LMTP 전달 구성"](#)

## LMTP 전달 기능

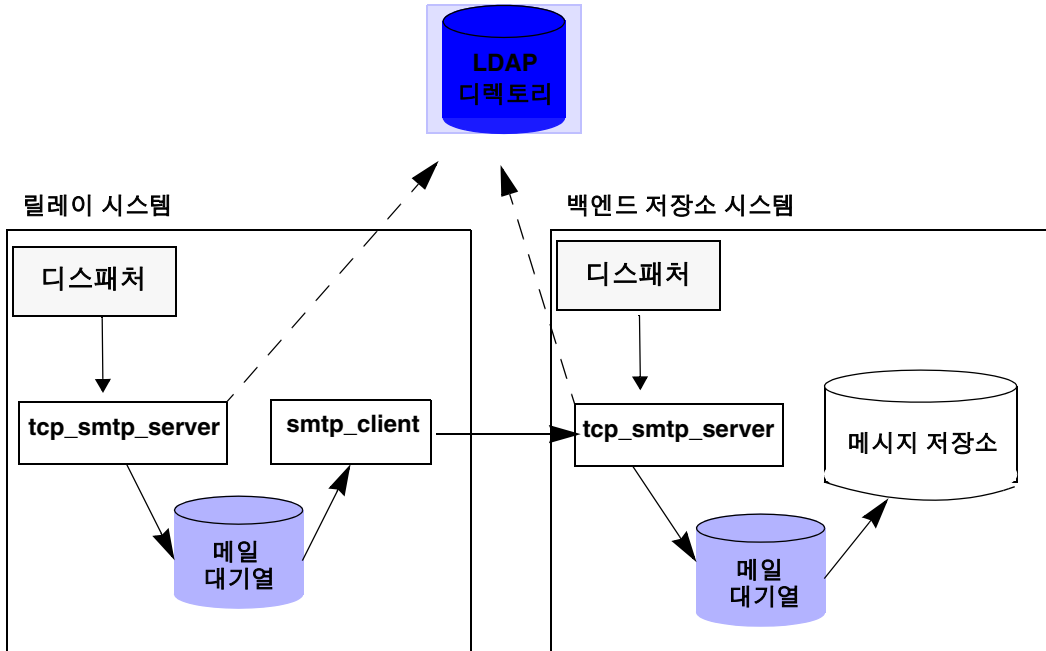
MTA의 LMTP 서버가 백엔드 메시지 저장소에 메일을 전달하는 데 보다 효율적인 이유는 다음과 같습니다.

- 백엔드 저장소의 로드가 감소합니다.  
릴레이는 수평적으로 확장 가능하지만 백엔드 저장소는 그럴 수 없기 때문에 가능한 릴레이에서 프로세스를 처리하는 것이 좋습니다.
- LDAP 서버의 로드가 감소합니다.  
LDAP 인프라가 대용량 메시징 배포의 제한 요소가 되는 경우가 있습니다.
- 메일 대기열의 수가 감소합니다.  
대기열을 릴레이와 백엔드 저장소 모두에 두면 메시징 배포 관리자가 손실된 메일을 찾기가 훨씬 어려워집니다.

## LMTP를 사용하지 않는 2계층 배포의 메일 처리

[그림 15-1](#)은 LMTP를 사용하지 않는 2계층 배포 시나리오의 다음 메일 처리 설명을 그림 형식으로 설명합니다.

그림 15-1 LMTP를 사용하지 않는 2계층 배포



LMTP 없이 저장소 시스템의 앞면에 릴레이가 있는 2수준 배포에서 인바운드 메일 처리는 릴레이 시스템의 디스패처가 선택하고 tcp\_smtp\_server 프로세스에 전달되는 SMTP 포트에 대한 연결에서 시작됩니다. 이 프로세스에서는 인바운드 메일에 대해 다음을 포함한 많은 작업을 수행합니다.

- 디렉토리에서 사용자 조회
- 사용자가 이 전자 메일 배포로 호스팅되는 도메인 내에 있는지 확인
- 사용자가 도메인에 유효한 사용자인지 확인
- 메일 봉투 주소를 @mailhost:user@domain으로 다시 쓰기
- 메일 호스트에 전달할 메일 대기열에 포함시키기

그러면 smtp\_client 프로세스가 대기열에서 메일 메시지를 선택하여 메일 호스트에 보냅니다. 메일 호스트에서도 비슷한 프로세스가 수행됩니다. 디스패처에서 SMTP에 대한 연결을 선택하여 tcp\_smtp\_server 프로세스에 전달합니다. 이 프로세스에서는 다음을 포함하여 많은 메일 작업을 수행합니다.

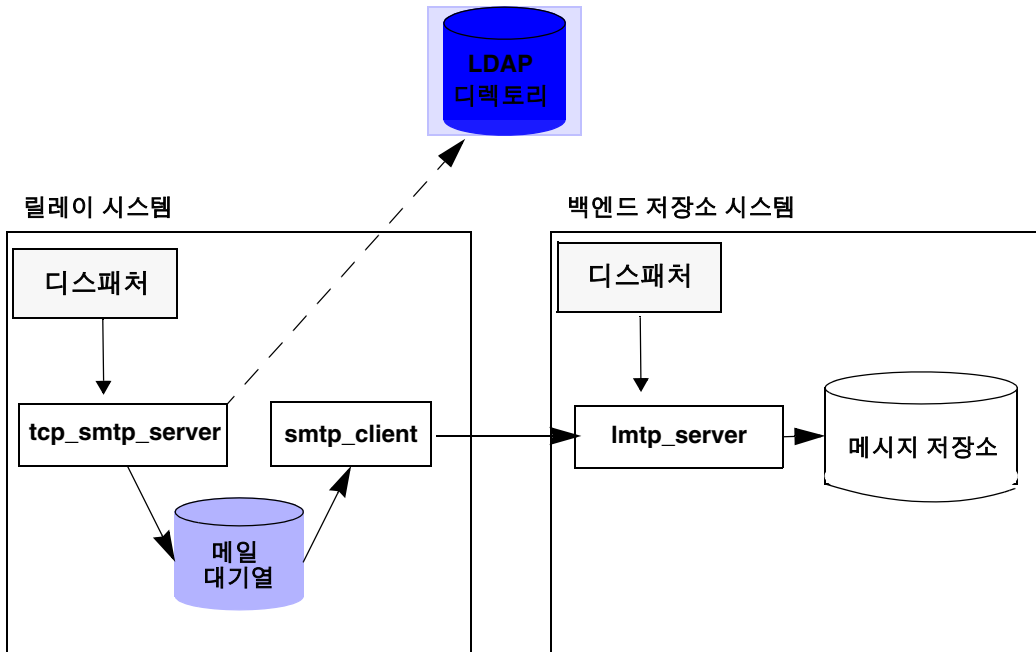
- 디렉토리에서 사용자 조회
- 사용자가 이 전자 메일 배포로 호스팅되는 도메인 내에 있는지 확인
- 사용자가 도메인에 유효한 사용자인지 확인
- 메일을 `ims_ms` 채널에 전달하도록 메일 봉투 주소 다시 쓰기
- 저장소에 전달할 메일 대기열에 포함시키기

그런 다음 `ims_ms` 프로세스가 메일 메시지를 선택하여 저장소에 전달하려고 시도합니다. 이 시나리오에서는 대기열에 포함시키는 프로세스가 두 번 수행되고 각 MTA에서 LDAP 조회를 수행합니다.

## LMTP를 사용하는 2계층 배포의 메일 처리

그림 15-2는 LMTP를 사용하는 2계층 배포 시나리오의 다음 메일 처리 설명을 그림 형식으로 설명합니다.

그림 15-2 LMTP를 사용하는 2계층 배포



LMTP를 배치하고 디스패처에서 릴레이 시스템의 SMTP에 대한 연결을 선택하여 `tcp_smtp_server` 프로세스에 전달합니다. 이 프로세스에서는 인바운드 메일에 대해 다음을 포함한 많은 작업을 수행합니다.

- 디렉토리에서 사용자 조회
- 사용자가 이 전자 메일 배포로 호스팅되는 도메인 내에 있는지 확인
- 사용자가 도메인에 유효한 사용자인지 확인
- 사용자에게 대한 메일함을 호스팅하는 백엔드 메시지 저장소 시스템 결정
- 주소를 `@mailhost:uid@domain.LMTP` 또는 `@mailhost:uid@domain.LMTPNATIVE`로 다시 쓰기
- 메일 호스트에 전달할 메일 대기열에 포함시키기

`user@domain.LMTP` 및 `user@domain.LMTPNATIVE` 형식으로 된 주소가 각각 `tcp_lmtp` 채널 또는 `tcp_lmtpnative` 채널을 통해 메시지 저장소 시스템에 라우팅됩니다. 이러한 채널은 SMTP 대신 LMTP를 사용하여 백엔드 메시지 저장소와 통신합니다. 저장소 시스템에서는 디스패처가 LMTP 포트에 대한 연결을 수신한 다음 `lmtp_server` 프로세스에 전달합니다. 그런 다음 LMTP가 메일을 사용자의 메일함이나 UNIX 원시 메일함에 넣습니다. 메일이 성공적으로 전달되면 메일이 릴레이 시스템의 대기열에서 제거됩니다. 성공적으로 전달되지 않은 경우 메일이 릴레이 시스템에 그대로 남아 있습니다. 메시지 저장소의 LMTP 프로세스에서는 주소 또는 메일 처리를 위해 MTA 방법을 사용하지 않습니다.

## LMTP 개요

대부분의 경우 MTA 자체는 기본적으로 백엔드 서버에 존재하지 않을 수 있습니다. 필요한 유일한 MTA 구성 요소는 다음과 같습니다.

- 디스패처
- `libimta`
- LMTP 서버
- `imta.cnf` 파일
- `mappings` 파일
- `imta.tailor` 파일

디스패처에는 MTA 구성 파일이 필요한데, 이러한 파일은 너무 짧을 수 있습니다. 디스패처를 백엔드 서버에서 실행해야 LMTP 서버를 시작할 수 있습니다. 디스패처와 LMTP 서버는 libimta의 다양한 기능을 사용하기 때문에 백엔드 서버에 위치할 필요가 없습니다.

LMTP 서버는 일반적인 MTA 대기열에 포함 또는 대기열에서 제외 기능, 헤더 처리 또는 주소 변환 작업을 수행하지 않습니다. 릴레이 시스템이 모든 메일 내용 조작을 수행합니다. 이러한 조작을 통해 메일을 메시지 저장소에 전달할 형식으로 표시하고 저장소에 필요한 형식으로 된 전달 주소를 표시합니다. 사용자 할당량과 같이 메일을 저장소에 전달할 때 일반적으로 사용할 수 있는 추가 수신자 정보는 수신자 주소와 함께 LMTP 매개 변수로 표시됩니다. 전달이 실패할 경우 메일이 릴레이 시스템의 LMTP 대기열에 그대로 포함되어 있습니다.

## LMTP 전달 구성

LMTP 전달 기법은 릴레이 시스템과 백엔드 저장소 모두에서 구성해야 합니다. 릴레이 시스템에서는 저장소에 전달할 메일이 LMTP 채널에 전달되도록 DELIVERY\_OPTIONS MTA 옵션(option.dat에서)을 변경해야 합니다. 백엔드 저장소는 디스패처를 사용하여 구성해야 하지만 Job Controller는 필요하지 않습니다. 디스패처는 LMTP 서버를 실행하도록 구성해야 합니다.

일반적인 다중 계층 배포에서는 서로 다른 백엔드 메시지 저장소 시스템에 사용자가 제공됩니다. 이 백엔드 시스템 중 하나 이상에 LMTP가 설정되지 않을 수 있으므로 프론트엔드 릴레이에서는 LMTP를 인식하는 저장소 시스템을 알고 있어야 합니다. 이는 LMTP 전달을 수락하도록 구성된 메시지 저장소를 명시적으로 지정하는 일반 데이터베이스 기능을 사용하면 가능합니다.

## LMTP를 사용하는 인바운드 MTA 릴레이 구성

LMTP를 사용하도록 인바운드 MTA 릴레이를 구성하려면 다음을 수행합니다.



1. 다음 행을 `option.dat`에 추가하여 텍스트 데이터베이스를 활성화합니다.

```
USE_TEXT_DATABASES=1
```

이 단계에서는 일반 데이터베이스의 일반적인 텍스트 파일을 MTA에서 사용할 수 있습니다. 이미 일반 데이터베이스를 사용하는 경우에는 이 단계를 건너뛸 수 있습니다.

2. 일반 데이터베이스 텍스트 파일을 만들거나 수정합니다.

```
# cd /opt/SUNWmsgsr/config/
# vi general.txt

LMTP_CS|msg-store.siroe.com lmtpcs-daemon
LMTP_CS|name-1-lmtp-store.siroe.com lmtpcs-daemon
LMTP_CS|name-2-lmtp-store.siroe.com lmtpcs-daemon
..
..
LMTP_CN|Zmar.Talek@siroe.com lmtpcn-daemon
..
LMTP_CN|Fred.Bloggs@siroe.com lmtpcn-daemon

# chown mailsrv general.txt
```

`lmtpnative` 채널에 대한 사용자별 전달을 처리하기 위한 것과 `tcp_lmtpcs` 채널을 통해 전달하기 위해 저장소 전체 설정을 처리하기 위한 두 가지 유형의 항목이 있습니다.

3. options.dat 파일에서 DELIVERY\_OPTIONS 변수를 만들거나 수정합니다.

DELIVERY\_OPTIONS의 값을 변경해야 합니다. 전달 옵션의 현재 값은 다음과 같습니다.

```
DELIVERY_OPTIONS=\
    *mailbox=$M%\$2I$_+$2S@ims-ms-daemon, \
    &members=*, \
    *native=$M@native-daemon, \
    *unix=$M@native-daemon, \
    /hold=$L%D@hold-daemon, \
    &file=+$F@native-daemon, \
    &@members_offline=*, \
    ,program=$M$P@pipe-daemon, \
    #forward=**, \
    **^!autoreply=$M+$D@bitbucket
```

이 값을 다음과 같이 바꿉니다.

```
DELIVERY_OPTIONS=\
    #*mailbox=@$X:$M$_+$2S%\$2I@ims-ms-daemon, \
    &members=*, \
    #*native=@$X:$M, \
    #*unix=@$X:$M, \
    #/hold=$L%D@hold, \
    #*file=@$X:+$F, \
    &@members_offline=*, \
    #program=$M$P@pipe-daemon, \
    #forward=**, \
    #**^!autoreply=$M+$D@bitbucket
```

메일함 전달 옵션의 패턴에 발생한 변경 사항과 함께 이제 자동 회신 전달 옵션 앞에 # 문자가 표시되어 릴레이 시스템에서 작업이 수행되도록 강제한다는 사실에 유의하십시오. \$x 대체로 인해 사용자에 대한 mailhost 속성의 값이 삽입됩니다. 그로 인해 라우트된 원본 주소가 생성됩니다.

원시의 UNIX 파일 및 프로그램 전달 방법이 유용하게 사용되기 위해서는 대상 컴퓨터에서 MTA를 실행하고 있어야 한다는 점도 중요합니다.

#### 4. LMTP 다시 쓰기 규칙을 imta.cnf 파일에 다음과 같이 추가합니다.

```
# cd /opt/SUNWmsgsr/config/
# cp imta.cnf imta.cnf.orig
# vi imta.cnf

!
! pipe
.pipe-daemon $U%H.pipe-daemon@pipe-daemon
!
! tcp_local
! Rules for top level internet domains
<IMTA_TABLE:internet.rules
!
! Do mapping lookup for internal IP addresses
[] $E$R${INTERNAL_IP,$L}$U%[$L]@tcp_intranet-daemon
!
! Do general.txt lookup for lmtp hosts
.domain-name.com $$S$U%$H$D@$(LMTP_CN|$U@$H$D)
.domain-name.com $$S$U%$H$D@$(LMTP_CS|$H$D)
!
! tcp_intranet
! Do mapping lookup for internal IP addresses
[] $E$R${INTERNAL_IP,$L}$U%[$L]@tcp_intranet-daemon
.domain-name.com $U%H.domain-name.com@tcp_intranet-daemon
```

이 단계에서 다시 쓰기 규칙 쌍은 주소의 소스 루트 부분이 LMTP 전달을 수행하기 위한 항목과 일치하는지 확인하기 위해 일반 데이터베이스의 태그된 검사를 수행합니다. 단계 2에서 만든 general.txt 파일에는 적절한 채널을 통해 백엔드 메시지 저장소에 전달을 지정하도록 태그된 항목이 있습니다. 여기서 다시 쓰기 규칙의 \$\$는 주소에 소스 루트가 포함된 경우에만 다시 쓰기 규칙이 적용됨을 의미합니다. 일반 데이터베이스의 항목과 일치하는 항목이 있을 경우 다시 쓰기 규칙이 성공하고 LMTP를 통해 전달을 수행하는 tcp\_lmtpX 채널을 통해 소스 루트 백엔드 호스트에 메시지가 전달됩니다.

일치하는 항목이 없을 경우 다른 다시 쓰기 규칙에 일치하는 항목이 있을 때까지 다시 쓰기 프로세스가 계속됩니다. 대부분의 경우 일반 데이터베이스의 검사를 통해 일치하는 항목을 찾지 못하면 SMTP를 통해 전달을 수행하는 tcp\_intranet 채널을 통해 메시지가 라우팅됩니다.

5. 새로운 채널 블록을 `imta.cnf`에 추가합니다.

`imta.cnf` 파일의 채널 정의 섹션에 `lmtpl` 및 `lmtpln` 채널에 대한 채널 정의도 포함시켜야 합니다. 예를 들면 다음과 같습니다.

```
! tcp_lmtpls (LMTP client - store)
tcp_lmtpls defragment lmtpl port 225 nomx single_sys subdirs 20 maxjobs 7
pool SMTP_POOL dequeue_removeoute
lmtpls-daemon
!
! tcp_lmtpln (LMTP client - native)
tcp_lmtpln defragment lmtpl port 226 nomx single_sys subdirs 20 maxjobs 7
pool SMTP_POOL dequeue_removeoute
!lmtpln-daemon
```

6. 구성 변경 사항을 적용합니다.

```
# cd /opt/SUNWmsgsr/bin
# ./imsimta refresh

Compiled configuration done

Killing Dispatcher : 23021

Dispatcher startup requested

Job Controller shutdown requested

Job Controller startup requested
```

---

**주** LMTP 채널에는 `lmtpl` 채널 키워드를 사용해야 합니다. LMTP 채널에 `smtpl` 및 `lmtpl` 채널 키워드를 함께 사용하지 마십시오. 기본적으로 LMTP 채널 정의는 주석 처리되어 있습니다. LMTP를 작동하려면 LMTP의 주석 처리를 제거해야 합니다.

---

조직에서 Sun Java System Messaging Server 사용자와 비Sun Java System Messaging Server 사용자가 함께 있는 경우, 어떤 사용자가 비Sun Java System Messaging Server 컴퓨터에 있는지 알 수 있어야 합니다. 이들의 delivery 옵션은 mailbox으로 설정할 수 없습니다. 대신 delivery 옵션은 forward로 설정되어야 합니다. 전달 주소는 라우트된 원본 형식이어야 하며 다음 예 중 하나일 수 있습니다(다음 예에만 국한되는 것은 아님).

```
mailForwardingAddress: @nonSJSMSHost.siroe.com:first.last@siroe.com
```

또는

```
mailForwardingAddress: @nonSJSMSHost.siroe.com:login@siroe.com
```

또는

```
mailForwardingAddress:
@nonSJSMSHost.siroe.com:first.last@nonSJSMSHost.siroe.com
```

또는

```
mailForwardingAddress:
@nonSJSMSHost.siroe.com:login@nonSJSMSHost.siroe.com
```

즉, 다음과 같습니다.

```
@nonSJSMSHost.siroe.com:address-which-is-recognized-by-the-nonSJ
SMSHost
```

## LMTP를 사용하고 MTA 없이 백엔드 저장소 구성

LMTP를 통해 메일을 받는 경우 백엔드 저장소에 MTA가 필요하지 않습니다. 이것은 Job Controller가 없고 MTA와 연결된 주소 다시 쓰기 방법이 없음을 의미합니다. 디스패처와 단순 MTA 구성은 여전히 필요합니다. 특히, MTA 구성의 유일한 중요 부분을 구성하는 `dispatcher.cnf` 파일과 `mappings` 파일이 필요합니다.

`dispatcher.cnf` 파일에는 다음이 포함되어 있어야 합니다.

```
! rfc 2033 LMTP server - store
!
[SERVICE=LMPSS]
PORT=225
IMAGE=IMTA_BIN:tcp_lmtp_server
LOGFILE=IMTA_LOG:tcp_lmtpss_server.log
PARAMETER=CHANNEL=tcp_lmtpss
STACKSIZE=2048000
! Uncomment the following line and set INTERFACE_ADDRESS to an
appropriate
! host IP (dotted quad) if the dispatcher needs to listen on a
specific
! interface (e.g. in a HA environment).
!INTERFACE_ADDRESS=
!
! rfc 2033 LMTP server - native
!
[SERVICE=LMPNS]
PORT=226
IMAGE=IMTA_BIN:tcp_lmtpn_server
LOGFILE=IMTA_LOG:tcp_lmtpsn_server.log
PARAMETER=CHANNEL=tcp_lmtpsn
STACKSIZE=2048000
! Uncomment the following line and set INTERFACE_ADDRESS to an
appropriate
! host IP (dotted quad) if the dispatcher needs to listen on a
specific
! interface (e.g. in a HA environment).
!INTERFACE_ADDRESS=
```

기본적으로 `dispatcher.cnf` 파일의 LMTP 서비스는 주석 처리됩니다. LMTP가 작동하려면 이러한 주석 처리를 제거해야 합니다.

`MAX_CONNS`, `MAX_PROCS`, `MAX_LIFE_CONNS` 및 `MAX_LIFE_TIME`의 일반 디스패처 옵션을 지정할 수 있습니다. 그럴 경우 해당 하드웨어에 맞게 설정해야 합니다.

`PORT_ACCESS` 매핑이 중요합니다. 백엔드 서버에 대한 LMTP 구현은 Sun Java System Messaging Server 릴레이 시스템과 백엔드 저장소 사이의 개인 프로토콜로 사용됩니다. `PORT_ACCESS` 매핑을 사용하여 그런 릴레이만 이러한 서비스에 연결될 수 있도록 확인해야 합니다. 매핑 파일의 모양은 다음과 같습니다.

```
PORT_ACCESS

TCP|*|225|1.2.3.4|* $Y
TCP|*|226|1.2.3.4|* $Y
TCP|*|225|1.2.3.5|* $Y
TCP|*|226|1.2.3.5|* $Y
TCP|*|*|*|* $N500$ Do$ not$ connect$ to$ this$ machine
```

이 `PORT_ACCESS` 매핑 테이블에 지정된 샘플 IP 주소를 백엔드 저장소에 연결되는 네트워크에 있는 릴레이 시스템의 IP 주소로 바꾸어야 합니다.

`imta.cnf` 파일이 있어야 하지만 이것만으로 완벽한 구성이 이뤄지지 않습니다. 최소 `imta.cnf` 파일은 다음 채널 정의로 구성됩니다.

```
! tcp_lmtpss (LMTP server - store)
tcp_lmtpss lmtp
tcp_lmtpss-daemon

!
! tcp_lmtpsn (LMTP server - native)
tcp_lmtpsn lmtp
tcp_lmtpsn-daemon
```

기본적으로 LMTP 채널 정의는 주석 처리됩니다. LMTP를 작동하려면 LMTP의 주석 처리를 제거해야 합니다.

## LMTP를 통해 메시지 저장소와 전체 MTA를 갖는 백엔드 시스템에 메일을 보내도록 릴레이 구성

백엔드 저장소에 MTA의 전체 기능을 제공하면서 LMTP를 사용하여 로드를 절약해야 하는 경우가 있습니다. 예를 들어, 백엔드 저장소에서 프로그램을 전달할 수 있습니다. 이 경우에는 위의 [488페이지의 "LMTP를 사용하는 인바운드 MTA 릴레이 구성"](#)에서 설명한 대로 릴레이를 구성해야 합니다.



## 전체 MTA가 있는 백엔드 메시지 저장소 시스템의 LMTP 구성

백엔드 저장소 메시징 시스템 구성은 LMTP를 사용하여 저장소에 직접 전달하는 구성에서 dispatcher.cnf 파일의 끝에 다음 행이 추가되는 점만 다릅니다.

```
! rfc 2033 LMTP server - store
!
[SERVICE=LMTPLSS]
PORT=225
IMAGE=IMTA_BIN:tcp_lmtp_server
LOGFILE=IMTA_LOG:tcp_lmtpss_server.log
PARAMETER=CHANNEL=tcp_lmtpss
STACKSIZE=2048000
! Uncomment the following line and set INTERFACE_ADDRESS to an
appropriate
! host IP (dotted quad) if the dispatcher needs to listen on a specific
! interface (e.g. in a HA environment).
!INTERFACE_ADDRESS=
!
! rfc 2033 LMTP server - native
!
[SERVICE=LMTPLSN]
PORT=226
IMAGE=IMTA_BIN:tcp_lmtpn_server
LOGFILE=IMTA_LOG:tcp_lmtpsn_server.log
PARAMETER=CHANNEL=tcp_lmtpsn
STACKSIZE=2048000
! Uncomment the following line and set INTERFACE_ADDRESS to an
appropriate
! host IP (dotted quad) if the dispatcher needs to listen on a specific
! interface (e.g. in a HA environment).
!INTERFACE_ADDRESS=
!
```

기본적으로 dispatcher.cnf 파일의 LMTP 서비스는 주석 처리됩니다. LMTP가 작동하려면 이러한 주석 처리를 제거해야 합니다. 또한 LMTP 포트 번호는 예일 뿐이므로 사용자가 선택한 임의의 번호가 될 수 있습니다.

백엔드 저장소를 LMTP에 대해서만 구성할 경우에는 위에서 설명한 dispatcher.cnf 파일과 동일합니다. 또한, 매핑 파일에는 LMTP 전용 백엔드 저장소에 대해 설명한 PORT\_ACCESS 매핑이 필요합니다.

## 구현된 LMTP 프로토콜

이 절에서는 샘플 LMTP 대화 상자를 제공하여 해당 대화 상자에 표시되는 내용을 설명합니다. 릴레이 시스템의 LMTP 클라이언트는 표준 LMTP 프로토콜을 사용하여 백엔드 저장소의 LMTP 서버와 대화합니다. 프로토콜은 특정 방법으로 사용됩니다. 예를 들면 다음과 같습니다.

```
----> LHLO
<--- 250 OK
```

LHLO 메일에 대한 작업이 수행되지 않습니다. 회신은 항상 250 OK입니다.

```
----> MAIL FROM: address size=messageSizeInBytes
<--- 250 OK
```

메일 발송자 주소를 검사하거나 변환하지 않습니다. size= 매개 변수는 전달할 메일의 크기(바이트)를 지정합니다. 이 값은 프로토콜에 표시되는 메일의 정확한 크기입니다. 정확한 메일 크기가 꼭 필요한 것은 아니지만 대개 실제 메일 크기는 이 크기를 초과하지 않습니다. LMTP 서버는 메일을 받도록 메모리에 이 크기의 버퍼를 할당합니다.

```
----> RCPT TO: uid+folder@domain xquota=size,number xdfld=xxx
<--- 250 OK
```

받을 때는 수신자 주소를 확인하지 않지만 나중에 사용할 수 있도록 수신자 목록이 작성됩니다. 주소의 @domain 부분은 주 도메인의 uids에서는 생략되고 +folder 부분은 선택 사항입니다. 이 형식은 MTA의 메시지 저장소 채널에 사용되는 것과 동일한 주소 형식입니다.

xquota= 매개 변수는 최대 총 크기와 최대 메일 수로 구성되는 사용자의 메일 할당량을 지정합니다. MTA는 사용자에 대한 LDAP 조회를 통해 주소 변환을 수행하는 동안 검색되는 이 메일 할당량 정보를 제공합니다. 이 정보는 메시지 저장소의 할당량 정보를 디렉토리와 동기화된 상태로 유지하는 데 사용됩니다. 할당량 정보를 가져오는 것은 성능에 영향을 미치지 않습니다.

xdflg= 매개 변수는 비트 필드로 해석되는 숫자를 지정합니다. 이러한 비트 수는 메일이 전달되는 방법을 제어합니다. 예를 들어, 비트 값을 2로 설정하면 사용자에 대해 할당량이 초과하더라도 메일이 전달됩니다. (xdflg는 내부 매개 변수이며 포함된 비트가 예고 없이 변경되거나 추가될 수 있다는 것에 주의합니다. Sun 서버에서 이 확장을 사용하는 다른 클라이언트나 일부 다른 서버에서 이 매개 변수를 사용하는 Sun 클라이언트나 모두 지원되지 않습니다.)

이 상호 작용은 수신자마다 한 번씩 여러 번 반복될 수 있습니다.

```
---->DATA
----> <the message text>
---->.
```

그런 다음 LMTP 클라이언트가 SMTP에서처럼 전체 메일을 점으로 표시하여 보냅니다. 메일은 한 행에 점(.) 하나로 끝납니다. 메일 크기가 초과될 경우 LMTP 서버는 다음을 보냅니다.

```
<--- 500 message too big
```

그런 다음 연결을 종료합니다.

메일이 올바르게 전달되면 LMTP 서버는 RCPT TO: 행에 지정된 각 수신자에 대한 상태를 LMTP 클라이언트에게 다시 보냅니다. 예를 들어, 메일이 성공적으로 전달될 경우 다음과 같은 응답을 받습니다.

```
<--- 250 2.5.0 address OK
```

여기서 address는 RCPT TO: 행에 표시된 주소입니다.

변환은 다른 MAIL FROM: 행에서 반복되거나 다음 상호 작용으로 종료될 수 있습니다.

```
----> quit
<---221 OK
```

표 15-1에서는 각 수신자에 대한 가능한 상태 코드를 나타냅니다. 이 3열 테이블의 첫 번째 열에는 짧은 코드가 표시되고, 두 번째 열에는 긴 코드가 표시되며, 세 번째 열에는 상태 텍스트가 표시됩니다. 2.x.x 상태 코드는 성공 코드이고, 4.x.x 코드는 재시도 가능한 오류이고, 5.x.x 코드는 재시도할 수 없는 오류입니다.

**표 15-1** 수신자에 대한 LMTP 상태 코드

| 짧은 코드 | 긴 코드  | 상태 텍스트        |
|-------|-------|---------------|
| 250   | 2.5.0 | 확인            |
| 420   | 4.2.0 | 메일함 잠김        |
| 422   | 4.2.2 | 할당량 초과        |
| 420   | 4.2.0 | 잘못된 메일함 형식    |
| 420   | 4.2.0 | 메일함 지원 안 함    |
| 430   | 4.3.0 | IMAP IOERROR  |
| 522   | 5.2.2 | 지속적인 할당량 초과   |
| 523   | 5.2.3 | 길이가 너무 긴 메일   |
| 511   | 5.1.1 | 메일함 없음        |
| 560   | 5.6.0 | 메일에 null 포함   |
| 560   | 5.6.0 | 메일에 nl 포함     |
| 560   | 5.6.0 | 메일에 잘못된 헤더 있음 |
| 560   | 5.6.0 | 메일에 빈 행 없음    |

그렇지 않으면 메일함, 원시(UNIX) 및 파일에 대한 전달 옵션이 변경된 것입니다. 이러한 규칙의 목적은 메일이 해당 LMTP 채널을 통해 백엔드 서버에 전달되도록 주소를 생성하는 것입니다. 생성된 주소는 라우팅된 원본 주소이며 그 형식은 다음과 같습니다.

`@sourceroute:localpart@domain`

구현된 LMTP 프로토콜

## 휴가 자동 메일 회신

자동으로 생성된 전자 메일 응답(자동 회신), 특히 휴가 메일에 대해 MTA는 MDN(Message Disposition Notification) 및 Sieve 스크립트 언어를 사용합니다. MDN은 메일의 전달 처리를 보고하기 위해 MTA가 보낸 사람 및/또는 포스트마스터에게 보내는 전자 메일입니다. MDN은 또한 읽음 확인, 확인, 수신 알림 또는 전달 확인이라고도 합니다. Sieve는 메일 필터를 만드는 데 사용되는 간단한 스크립트 언어입니다.

이 장에서는 휴가 자동 회신 기법에 대해 설명합니다. 대부분의 경우 기본 구성은 수정할 필요가 없지만 백엔드 메시지 저장소가 아니라 MTA 회신 시스템에서 휴가 처리를 수행하도록 시스템을 구성해야 할 수 있습니다.

이 장은 다음 내용으로 구성되어 있습니다.

- 503페이지의 "휴가 자동 회신 개요"
- 504페이지의 "자동 회신 구성"
- 506페이지의 "휴가 자동 회신 작동 원리"
- 508페이지의 "휴가 자동 회신 속성"

### 휴가 자동 회신 개요

휴가 Sieve 스크립트는 다양한 LDAP 휴가 속성으로부터 자동으로 생성됩니다(508페이지의 "휴가 자동 회신 속성" 참조). 또한 추가적인 유연성을 위해 이러한 스크립트를 명시적으로 지정할 수도 있습니다. 기본 휴가 추적 기법은 다양한 보낸 사람에게 회신을 보낸 시간을 추적하는 파일 집합(원하는 수신자 당 하나)입니다.

기본적으로 MTA는 백엔드 저장소 시스템에서 휴가를 평가합니다. 그러나 MTA 릴레이가 백엔드 저장소처럼 많은 작업을 처리하는 것은 아니기 때문에 백엔드 저장소 대신 메일 릴레이 시스템에서 휴가 메일을 평가하도록 하여 성능을 높일 수 있습니다. 이 기능을 사용하면 각각의 릴레이에서 서로 다른 메일을 처리하기 때문에 원하는 것보다 더 많은 수의 휴가 응답이 보내질 수 있습니다. 휴가 메일을 원하는 수보다 더 많이 보내지 않게 하려면 릴레이 간에 파일 추적을 공유할 수 있습니다. 이 방법도 충분하지 않다고 생각될 경우에는 휴가 메일이 백엔드 저장소 시스템에서 항상 평가되게 할 수 있습니다.

## 자동 회신 구성

전달 주소가 일련의 패턴을 통해 생성됩니다. 사용되는 패턴은 mailDeliveryOption 속성에 정의된 값에 따라 다릅니다. 전달 주소는 각각의 유효한 mailDeliveryOption에 대해 생성됩니다. 패턴은 MTA 옵션 DELIVERY\_OPTIONS에 의해 option.dat 파일에 정의됩니다. option.dat 파일의 DELIVERY\_OPTIONS에 있는 기본 자동 회신 규칙은 다음과 같습니다.

```
*^!autoreply=$M+$D@bitbucket
```

MTA는 자동 회신 DELIVERY\_OPTION MTA 옵션에 "^" 기호를 기록합니다. 그렇게 하면 MTA가 휴가 날짜를 확인하게 됩니다. 현재 날짜가 휴가 날짜 범위에 속하는 경우 처리가 계속되며, MTA는 자동 회신 DELIVERY\_OPTION에 "!"를 기록합니다. 그런 다음 사용자가 입력하는 다양한 자동 회신 LDAP 속성을 기반으로 휴가 Sieve 스크립트를 만듭니다. 자동 회신 규칙에는 접두어 문자 "!", "#", "^" 및 "\*"가 있습니다.

메일함 전달 옵션에 "!" 플래그를 표시할 수 있습니다. 그럴 경우 휴가 스크립트 생성이 무조건적으로 사용됩니다. "^" 플래그에 의해 추가로 금지할 수 있도록 자동 회신 방법이 별도의 전달 옵션에 의해 활성화됩니다. 이 단계에서 날짜를 확인하는 것이 Sieve 논리를 사용하는 것보다 더 효과적입니다.

표 16-1에는 첫 번째 열의 자동 회신 규칙과 두 번째 열의 해당 정의에 사용되는 접두어 문자가 표시되어 있습니다.

**표 16-1** DELIVERY\_OPTIONS의 자동 회신 규칙에 사용되는 접두어 문자

| 접두어 문자 | 정의                                   |
|--------|--------------------------------------|
| !      | 자동 회신 Sieve 스크립트 생성을 사용합니다.          |
| #      | 릴레이에서 프로세스를 처리하도록 허용합니다.             |
| ^      | 휴가 날짜에 옵션을 평가하도록 표시된 경우에만 옵션을 평가합니다. |



**표 16-1** DELIVERY\_OPTIONS의 자동 회신 규칙에 사용되는 접두어 문자

접두어 문자

정의

\*

사용자에게만 규칙을 적용할 수 있습니다.

자동 회신 규칙은 `bitbucket` 채널의 대상 주소를 지정합니다. 자동 회신이 생성되면 이 방법에 의해 메일이 전달된 것으로 간주되지만 `MTA` 방법을 사용하려면 전달 주소가 필요합니다. `bitbucket` 채널에 전달되는 내용은 삭제됩니다.

## 백엔드 시스템에서 자동 회신 구성

`DELIVERY_OPTIONS`의 기본 자동 회신 규칙은 사용자에게 서비스를 제공하는 메일 서버에서 자동 회신을 처리합니다. 백엔드 저장소 시스템에서 휴가 메일이 평가되도록 하려면 아무 것도 구성할 필요가 없습니다. 기본 동작입니다.

## 릴레이에서 자동 회신 구성

성능 향상을 위해 백엔드 저장소 시스템 대신 릴레이에서 휴가를 평가하려면 `option.dat` 파일을 편집하고 `DELIVERY_OPTIONS`의 자동 회신 규칙 앞에 `#` 문자를 붙입니다. 예를 들면 다음과 같습니다.

1. 편집기를 사용하여 `option.dat` 파일을 엽니다.
2. 자동 회신 규칙이 다음과 같이 표시되도록 `DELIVERY_OPTIONS` 옵션을 추가하거나 변경합니다.

```
##^!autoreply=$M+$D@bitbucket
```

기본 `DELIVERY_OPTIONS` 옵션은 다음과 같습니다.

```
DELIVERY_OPTIONS=*mailbox=$M%\$2I$_+$2S@ims-ms-daemon, \
&members=*, \
*native=$M@native-daemon, \
/hold=@hold-daemon;$A, \
*unix=$M@native-daemon, \
&file=+$F@native-daemon, \
```

```
&@members_offline=* \
,program=$M$P@pipe-daemon, \
#forward=**,\
*^!autoreply=$M+$D@bitbucket
```

이렇게 하면 릴레이에서 프로세스를 처리할 수 있습니다. MTA가 릴레이에서 자동 회신을 수행하도록 지정한 경우 특정 사용자가 최근에 휴가 알림 메일을 보냈는지 여부를 각 릴레이에서 독립적으로 추적하도록 하거나 또는 이 정보를 릴레이 간에 공유하도록 할 수 있습니다. 전자의 경우가 더 간단합니다. 특히, 휴가 알림 메일을 보내는 횟수가 문제가 되지 않는 경우에 그렇습니다. 휴가 알림 메일을 보내는 빈도 규칙을 엄격하게 적용하려면 릴레이 간에 정보를 공유해야 합니다. 릴레이 간에 정보를 공유하려면 파일이 NFS에 마운트되어 있어야 합니다.

이러한 파일의 위치는 VACATION\_TEMPLATE 옵션에 의해 제어됩니다. option.dat 파일에서 이 옵션을 /<path>/%A로 설정해야 합니다. 여기서 <path>는 여러 릴레이 시스템 간에 공유되는 디렉토리의 경로입니다. 템플리트는 file:URL이어야 하며, \$U를 사용하여 사용자 이름을 대체해야 합니다. 기본 설정은 다음과 같습니다.

```
VACATION_TEMPLATE=file:///opt/SUNWmsgsr/data/vacation/$3I/$1U/$2U/$U.vac
```

메타 문자에 대한 설명은 [214페이지의 표 9-6](#)을 참조하십시오.

---

**주** 이제 휴가 파일 템플리트에 UID에 대한 액세스 권한이 있으므로 사용자의 UID를 기반으로 작성될 휴가 파일에 경로를 허용하게 됩니다. 추가적으로, 휴가 파일 경로를 확인하는 데 사용된 주소는 사용자의 메일 속성에 저장된 주소이며, 현재 수신자 주소는 이전에 사용되었습니다.

---

## 휴가 자동 회신 작동 원리

휴가 작업을 호출하면 다음과 같이 작동합니다.

1. Sun Java System Messaging Server에서 휴가 작업이 시스템 수준 Sieve 스크립트가 아니라 사용자 수준으로 수행되었는지 확인합니다. 휴가가 시스템 수준 스크립트에서 사용되는 경우 오류가 발생합니다.
2. "no vacation notice" 내부 MTA 플래그가 선택됩니다. 이 플래그를 설정하면 프로세스가 종료되고 휴가 알림이 보내지지 않습니다.
3. 메일에 대한 반송 주소가 선택됩니다. 이 주소가 비어 있으면 프로세스가 종료되고 휴가 알림이 보내지지 않습니다.

4. MTA가 `:addresses` 태그 인수에 지정된 사용자 주소 또는 추가 주소가 현재 메일의 `To:`, `Cc:`, `Resent-to:` 또는 `Resent-cc:` 헤더 필드에 표시되는지 확인합니다. 헤더 필드에 주소가 없는 경우 프로세스가 종료되고 휴가 알림이 보내지지 않습니다.
5. Messaging Server는 `:subject` 인수와 이유 문자열을 구성합니다. 이 문자열은 현재 메일의 반송 주소와 함께 이전 휴가 응답의 사용자 단위 레코드에 대해 확인됩니다. `:days` 인수에 허용된 시간 내에 응답이 이미 보내진 경우 프로세스가 종료되고 응답이 보내지지 않습니다.
6. Messaging Server는 `:subject` 인수, 이유 문자열 및 `:mime` 인수로부터 휴가 알림을 만듭니다. 이 응답 메일에 다음과 같은 두 기본 형식을 사용할 수 있습니다.
  - RFC 2298에 지정된 형식의 메일 배포 알림(첫 번째 부분에 이유 텍스트가 포함되어 있음)
  - 단일 부분 텍스트 회신. 이 형식은 "회신" 자동 회신 모드 속성 설정을 지원하는 데만 사용됩니다.

Messenger Express를 통해 휴가 메일이 구성된 경우 `mailautoreplymode`가 자동으로 `reply`로 설정된다는 것에 주의합니다.

"no vacation notice" MTA 플래그는 기본적으로 선택되어 있지 않습니다. 이 플래그는 비표준 `novacation` 작업을 사용하여 시스템 수준 Sieve 스크립트로 설정할 수 있습니다. `novacation Sieve` 작업은 시스템 수준 Sieve 스크립트에서만 허용됩니다. 사용자 수준 스크립트에서 이 플래그를 사용하면 오류가 발생합니다. 이 작업을 사용하여 휴가 회신에 대한 사이트 차원 제한(예: 하위 문자열 "MAILER-DAEMON"이 포함된 주소에 대한 회신 차단)을 구현할 수 있습니다.

사용자 단위 응답별 정보는 로컬 사용자 당 하나씩 일반 텍스트 파일에 저장됩니다. 이러한 파일의 위치 및 이름 지정 방법은 `VACATION_TEMPLATE` MTA 옵션 설정에 지정됩니다. 이 옵션을 `file: URL`로 설정해야 합니다.

이러한 파일은 자동으로 유지 관리되며 `VACATION_CLEANUP` 정수 MTA 옵션 설정에 의해 제어됩니다. 이러한 파일 중 하나가 열릴 때마다 현재 시간(초) **modulo** 값이 계산됩니다. 결과가 0이면 파일이 스캔되고 모든 만료된 항목이 제거됩니다. 옵션 기본값은 200이고 200번에 한 번씩 정리가 수행됨을 의미합니다.

이러한 일반 텍스트 파일을 읽고 쓰는 데 사용되는 방법은 NFS에 대해 올바르게 작업을 수행할 수 있는 방식으로 디자인됩니다. 그렇게 하면 여러 MTA에서 공통 파일 시스템에서 단일 파일 집합을 공유할 수 있습니다.

# 휴가 자동 회신 속성

휴가 작업에 사용되는 사용자 LDAP 디렉토리 속성 집합은 다음과 같습니다.

- LDAP\_PERSONAL\_NAME에서 정의한 속성

별칭 처리는 이 속성에 지정된 개인 이름 정보를 추적하며 이 정보를 사용하여 생성되는 모든 MDN 또는 휴가 회신의 From: 필드를 구성합니다. 개인 정보가 노출되지 않도록 주의해서 사용합니다.

- vacationStartDate

휴가 시작 날짜 및 시간입니다. 이 값은 YYYYMMDDHHMMSSZ 형식입니다. 이 값은 GMT로 정규화됩니다. 자동 회신은 현재 시간이 이 속성에 지정된 시간 이후인 경우에만 생성되어야 합니다. 이 속성이 없는 경우 시작 날짜가 적용되지 않습니다.

LDAP\_START\_DATE MTA 옵션을 다른 속성 이름으로 설정하여 이 정보에 대해 다른 속성을 조사하도록 MTA에 명령할 수 있습니다.

Sieve 스크립트를 생성한 코드에서 이 속성을 읽고 확인합니다. 현재 날짜가 휴가 시작 날짜 이전이면 휴가 프로세스가 중지됩니다. 현재 Sieve에 날짜/시간 테스트 및 비교 기능이 없기 때문에 스크립트 자체로는 이 속성을 처리할 수 없습니다.

- vacationEndDate

휴가 종료 날짜 및 시간입니다. 이 값은 YYYYMMDDHHMMSSZ 형식입니다. 이 값은 GMT로 정규화됩니다. 자동 회신은 현재 시간이 이 속성에 지정된 시간 이전인 경우에만 생성되어야 합니다. 이 속성이 없는 경우 종료 날짜가 적용되지 않습니다.

LDAP\_END\_DATE MTA 옵션을 다른 속성 이름으로 설정하여 이 정보에 대해 다른 속성을 조사하도록 MTA에 명령할 수 있습니다.

Sieve 스크립트를 생성한 코드에서 이 속성을 읽고 확인합니다. 현재 날짜가 휴가 종료 날짜 이후이면 휴가 프로세스가 중지됩니다. 현재 Sieve에 날짜/시간 테스트 및 비교 기능이 없기 때문에 스크립트 자체에서는 이 속성을 처리할 수 없습니다.

- mailAutoReplyMode

사용자 메일 계정에 대한 자동 회신 모드를 지정합니다. 이 속성에 유효한 값은 다음과 같습니다.

- echo - 추가된 mailAutoReplyText 또는 mailAutoReplyTextInternal 텍스트와 함께 원본 메일 텍스트를 반환하는 멀티파트을 만듭니다.
- reply - 원래의 보낸 사람에게 mailAutoReplyText 또는 mailAutoReplyTextInternal에 지정된 대로 단일 부분 회신을 보냅니다.

이러한 모드는 Sieve 스크립트에 휴가 작업에 대한 비표준 `:echo` 및 `:reply` 인수로 표시됩니다. `echo`는 원본 메일을 반환된 내용에 포함하는 "처리된" MDN(Message Disposition Notification)을 생성합니다. `reply`는 회신 텍스트만 포함되는 순수 회신을 생성합니다. 잘못된 값이 휴가 작업에 대한 인수로 매니페스트되지 않으므로 원본 메일의 헤더만 포함된 MDN이 생성됩니다. 에코 자동 회신 모드를 선택하면 최근에 회신을 보낸 방법에 관계 없이 모든 메일에 대해 자동 회신을 보냅니다.

`LDAP_AUTOREPLY_MODE` MTA 옵션을 다른 속성 이름으로 설정하여 이 정보에 다른 속성을 사용하도록 MTA에 명령할 수 있습니다.

- `mailAutoReplySubject`

자동 응답에 사용할 제목 필드의 내용을 지정합니다. UTF-8 문자열이어야 합니다. 이 값은 휴가 작업에 `:subject` 인수로 전달됩니다. `LDAP_AUTOREPLY_SUBJECT` MTA 옵션을 다른 속성 이름으로 설정하여 이 정보에 다른 속성을 사용하도록 MTA에 명령할 수 있습니다.

Sieve에는 현재 특정 대체를 수행할 수 있는 기능이 없기 때문에 `$SUBJECT`를 사용하여 헤더에 원본 메일을 삽입할 수 없습니다.

- `mailAutoReplyText`

수신자의 도메인에 있는 사용자를 제외한 모든 보낸 사람에게 자동 회신 텍스트를 보냅니다. 이 옵션을 지정하지 않는 경우 외부 사용자는 휴가 메일을 받지 못합니다.

`LDAP_AUTOREPLY_TEXT` MTA 옵션을 다른 속성 이름으로 설정하여 이 정보에 다른 속성을 사용하도록 MTA에 명령할 수 있습니다.

- `mailAutoReplyTextInternal`

수신자 도메인에 있는 보낸 사람에게 자동 회신 텍스트를 보냅니다. 이 옵션을 지정하지 않는 경우 내부 사용자가 메일 자동 회신 텍스트 메일을 받게 됩니다.

`LDAP_AUTOREPLY_TEXT_INT` MTA 옵션을 다른 속성 이름으로 설정하여 이 정보에 다른 속성을 사용하도록 MTA에 명령할 수 있습니다.

MTA는 `mailAutoReplyText` 또는 `mailAutoReplyTextInternal` 속성 값을 휴가 작업에 이유 문자열로 전달합니다.

- `mailAutoReplyTimeOut`

지정된 메일 보낸 사람에게 연속 자동 응답을 보내는 기간(시간)입니다.

mailAutoReplyMode=reply인 경우에만 사용됩니다. 값이 0이면 메일을 받을 때마다 응답을 보냅니다. 이 값은 휴가 작업에 대한 비표준 :hours 인수로 변환됩니다. 일반적으로 Sieve 휴가 작업은 이러한 목적으로 :days 인수만을 지원하며 0 값을 허용하지 않습니다.

이 속성이 사용자 항목에 표시되지 않으면 AUTOREPLY\_TIMEOUT\_DEFAULT MTA 옵션에서 기본 시간 초과 값을 가져옵니다. LDAP\_AUTOREPLY\_TIMEOUT MTA 옵션을 설정하여 이 정보에 다른 속성을 사용하도록 MTA에 명령할 수 있습니다.

# 메일 필터링 및 액세스 제어

이 장에서는 메일의 소스(보낸 사람, IP 주소 등) 또는 헤더 문자열에 기초하여 메일을 필터링하는 방법에 대해 설명합니다. 두 개의 메일 필터링 기법, 즉 매핑 테이블을 사용한 MTA에 대한 액세스 제어와 Sieve 서버측 규칙(SSR)이 사용됩니다.

매핑 테이블을 사용하여 MTA에 대한 액세스를 제한하면 From: 및 To: 주소, IP 주소, 포트 번호, 소스 또는 대상 채널 등에 기초하여 메일을 필터링할 수 있습니다. 매핑 테이블은 SMTP 릴레이를 활성화 또는 비활성화할 수 있게 합니다. Sieve는 헤더에서 발견된 문자열에 기초하여 메일을 필터링할 수 있게 하는 메일 필터링 스크립트이며 메일 본문에서는 작동하지 않습니다.

봉투 수준 제어가 필요한 경우에는 매핑 테이블을 사용하여 메일을 필터링하고 헤더 기반 제어가 필요한 경우에는 Sieve 서버측 규칙을 사용합니다.

이 장은 다음 두 부분으로 구성됩니다.

**1부. 매핑 테이블** 관리자가 특정 매핑 테이블을 구성하여 MTA 서비스에 대한 액세스를 제어할 수 있게 합니다. 관리자는 Messaging Server를 통해 메일을 주고 받을 수 있는 사람과 그렇지 않은 사람을 제어할 수 있습니다.

**2부. 메일함 필터** 사용자와 관리자가 메일 헤더에서 찾은 문자열을 기초로 메일을 필터링하고, 필터링된 이런 메일에 수행할 작업을 지정할 수 있습니다. Sieve 필터 언어를 사용하여 채널, MTA 또는 사용자 수준에서 필터링할 수 있습니다.

## 1부. 매핑 테이블

1부는 다음 내용으로 구성되어 있습니다.

- 512페이지의 "매핑 테이블을 사용한 액세스 제어"
- 526페이지의 "액세스 제어가 적용되는 경우"
- 527페이지의 "액세스 제어 매핑 테스트"

- 528페이지의 "SMTP 릴레이 추가"
- 531페이지의 "SMTP 릴레이 차단 구성"
- 537페이지의 "많은 수의 액세스 항목 처리"
- 514페이지의 "액세스 제어 매핑 테이블 플러그"

## 매핑 테이블을 사용한 액세스 제어

특정 매핑 테이블을 구성하여 메일 서비스에 대한 액세스를 제어할 수 있습니다. 이러한 매핑 테이블을 사용하면 메일을 전송 및/또는 수신할 수 있거나 그렇게 할 수 없는 사람을 제어할 수 있습니다. 표 17-1에는 이 절에 설명된 매핑 테이블이 나열되어 있습니다. FROM\_ACCESS, MAIL\_ACCESS 및 ORIG\_MAIL\_ACCESS 매핑에 제공되는 응용 프로그램 정보 문자열에는 HELO/EHLO SMTP 명령에서 요구된 시스템 이름도 포함됩니다. 이 이름은 문자열 끝에 표시되며 슬래시(/)로 나머지 문자열(일반적으로 "SMTP")과 구분합니다. 요구된 시스템 이름은 일부 웹과 바이러스를 차단하는 데 유용할 수 있습니다.

### 액세스 제어 매핑 테이블—작업

모든 매핑 테이블과 마찬가지로 액세스 제어 매핑 테이블은 동일한 일반 형식을 가집니다 (229페이지의 "매핑 파일" 참조). 즉, 매핑 테이블 이름이 맨 앞에 오고 그 뒤에 공백이 있으며 맨 뒤에 하나 이상의 매핑 항목이 오는 형식입니다. 매핑 항목은 왼쪽에 있는 *검색 패턴*과 오른쪽에 있는 *템플릿*으로 구성됩니다. 검색 패턴은 특정 메일을 필터링하며 템플릿은 메일에 대해 수행할 작업을 지정합니다. 예를 들면 다음과 같습니다.

SEND\_ACCESS

```
*|Elvis1@sesta.com|*|*      $Y
*|Nelson7@sesta.com|*|*     $Y
*|AkiraK@sesta.com|*|*      $Y
*|*@sesta.com|*|*          $NMail$ Blocked
```

다음 예는 sesta.com 도메인에서 Elvis1, Nelson, AkiraK의 전자 메일을 제외한 모든 전자 메일을 차단합니다.

액세스 제어 매핑 항목의 검색 패턴은 세로 막대(|)로 구분된 여러 검색 기준으로 구성됩니다. 검색 기준의 순서는 액세스 매핑 테이블에 따라 다르며 이후의 절에서 설명합니다. 예를 들어 SEND\_ACCESS 매핑 테이블의 검색 형식은 다음과 같습니다.

```
src-channel|from-address|dst-channel|to-address
```



*src-channel*은 메일이 대기 중인 채널, *from-address*는 메일을 보낸 사람의 주소, *dst-channel*은 메일이 대기될 채널, *to-address*는 메일 주소가 지정된 주소입니다. 이 네 필드에 별표를 사용하면 해당 필드는 모든 채널 또는 주소와 일치하게 됩니다.

---

**주** mappings 파일을 수정할 때마다 구성을 다시 컴파일해야 합니다(*Sun Java System Messaging Server Administration Reference*의 `imsimta refresh` 명령 참조).

---

**표 17-1** 액세스 제어 매핑 테이블

| 매핑 테이블                          | 설명                                                                                                                                                    |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|
| SEND_ACCESS<br>(517페이지 참조)      | 봉투 From 주소와 봉투 To 주소, 소스 및 대상 채널을 기준으로 받는 연결을 차단하는 데 사용됩니다. To 주소는 다시 쓰기, 별칭 확장 등이 수행된 뒤 검사됩니다.                                                       |
| ORIG_SEND_ACCESS<br>(517페이지 참조) | 봉투 From 주소와 봉투 To 주소, 소스 및 대상 채널을 기준으로 받는 연결을 차단하는 데 사용됩니다. To 주소는 다시 쓴 다음, 별칭 확장 전에 검사됩니다.                                                           |
| MAIL_ACCESS<br>(519페이지 참조)      | SEND_ACCESS 및 PORT_ACCESS 테이블에서 발견한 결합된 정보(PORT_ACCESS에서 발견한 IP 주소 및 포트 번호 정보와 결합된 SEND_ACCESS에서 발견된 채널 및 주소 정보)에 기초하여 받는 연결을 차단하는 데 사용됩니다.           |
| ORIG_MAIL_ACCESS<br>(519페이지 참조) | ORIG_SEND_ACCESS 및 PORT_ACCESS 테이블에서 발견한 결합된 정보(PORT_ACCESS에서 발견한 IP 주소 및 포트 번호 정보와 결합된 ORIG_SEND_ACCESS에서 발견된 채널 및 주소 정보)에 기초하여 받는 연결을 차단하는 데 사용됩니다. |
| FROM_ACCESS<br>(521페이지 참조)      | 봉투 From 주소를 기준으로 메일을 필터링하는 데 사용됩니다. To 주소가 부적절한 경우 이 테이블을 사용합니다.                                                                                      |
| PORT_ACCESS<br>(523페이지 참조)      | IP 번호를 기준으로 받는 연결을 차단하는 데 사용됩니다.                                                                                                                      |

SEND\_ACCESS 및 ORIG\_SEND\_ACCESS에 사용 가능한 주소 및 채널 정보와 IP 주소와 포트 번호 정보를 포함하여 PORT\_ACCESS 매핑 테이블을 통해 사용 가능한 모든 정보를 사용할 수 있는 경우 MAIL\_ACCESS 및 ORIG\_MAIL\_ACCESS 매핑이 가장 일반적입니다.

## 액세스 제어 매핑 테이블 플래그

표 17-2는 SEND\_ACCESS, ORIG\_SEND\_ACCESS, MAIL\_ACCESS, ORIG\_MAIL\_ACCESS 및 FROM\_ACCESS 매핑 테이블에 관련된 액세스 매핑 플래그입니다. PORT\_ACCESS 매핑 테이블은 이와 약간 다른 플래그 집합을 지원합니다(표 17-3 참조).

인수가 있는 플래그에서는 인수를 표에 나온 읽기 순서에 따라 정렬해야 합니다. 예를 들면 다음과 같습니다.

ORIG\_SEND\_ACCESS

```
tcp_local|*|tcp_local|*    $N$D30|Relaying$ not$ allowed
```

이 경우에 올바른 순서는 지연 기간 다음에 거부 문자열이 오는 것입니다. 플래그 자체는 임의의 순서가 될 수 있습니다. 따라서 다음 항목의 결과는 동일합니다.

```
30|Relaying$ not$ allowed$D$N
$N30|Relaying$ not$ allowed$D
30|$N$DRelaying$ not$ allowed
```

**표 17-2** 액세스 매핑 플래그

| 플래그 | 설명                                                                            |
|-----|-------------------------------------------------------------------------------|
| \$A | SASL이 사용된 경우 설정합니다. 238페이지의 "특수 플래그 검사"를 참조하십시오.                              |
| \$B | 메일을 bitbucket으로 리디렉션합니다.                                                      |
| \$D | 전달 지연 확인이 요청된 경우(FROM_ACCESS에서는 사용할 수 없음) 설정합니다. 238페이지의 "특수 플래그 검사"를 참조하십시오. |
| \$F | 전달 실패 확인이 요청된 경우(FROM_ACCESS에서는 사용할 수 없음) 설정합니다. 238페이지의 "특수 플래그 검사"를 참조하십시오. |
| \$H | 메일을 .HELD 파일로 보관합니다.                                                          |
| \$S | 전달 성공 확인이 요청된 경우(FROM_ACCESS에서는 사용할 수 없음) 설정합니다. 238페이지의 "특수 플래그 검사"를 참조하십시오. |

**표 17-2** 액세스 매핑 플래그

| 플래그                                                          | 설명                                                                                                                                                                                                                       |
|--------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| \$T                                                          | TLS가 사용된 경우 설정합니다. 238페이지의 "특수 플래그 검사"를 참조하십시오.                                                                                                                                                                          |
| \$U                                                          | ORIG_SEND_ACCESS, SEND_ACCESS, ORIG_MAIL_ACCESS 및 MAIL_ACCESS에서 사용될 경우 매핑의 시작 부분에서 단일 정수 인수를 가져오며 이에 따라 MM_DEBUG 값을 설정합니다. 또한 가능한 경우 채널 수준 디버깅도 사용 가능하게 합니다. 결과적으로 소스 IP 주소, 원래 주소, 수신자 주소 등의 항목에 기초하여 디버깅을 사용 가능하게 합니다. |
| \$Y                                                          | 액세스를 허용합니다.                                                                                                                                                                                                              |
| \$V                                                          | 모든 수신자에 대해 삭제를 수행합니다.                                                                                                                                                                                                    |
| \$Z                                                          | 모든 수신자에 대해 jettison을 수행합니다.                                                                                                                                                                                              |
| <b>인수가 있는 플래그, 인수 읽기 순서에 따라 + (이 목록을 알파벳 순서로 정렬하지 마십시오!)</b> |                                                                                                                                                                                                                          |
| \$Uinteger                                                   | 매핑의 시작 부분에서 단일 정수 인수를 가져오며 이에 따라 MM_DEBUG를 설정합니다. 또한 가능한 경우 채널 수준 디버깅도 사용 가능하게 합니다. 결과적으로 소스 IP 주소, 원래 주소, 수신자 주소 등의 항목에 기초하여 디버깅을 사용 가능하게 할 수 있습니다.                                                                     |
| \$Jaddress                                                   | * 원본 봉투 From: 주소를 지정된 <i>address</i> 로 대체합니다.                                                                                                                                                                            |
| \$Kaddress                                                   | * ++ 원래의 Sender: 주소를 지정된 <i>address</i> 로 대체합니다.                                                                                                                                                                         |
| \$Iuseridentifier                                            | 지정된 사용자의 그룹 아이디를 확인합니다.                                                                                                                                                                                                  |
| \$<string                                                    | +++ 검사가 일치하면 <i>string</i> 을 syslog(UNIX, user.notice 기능 및 심각도) 또는 이벤트 로그(NT)로 보냅니다.+++                                                                                                                                  |
| \$>string                                                    | +++ 액세스가 거부되면 <i>string</i> 을 syslog(UNIX, user.notice 기능 및 심각도) 또는 이벤트 로그(NT)로 보냅니다.                                                                                                                                    |
| \$Ddelay                                                     | <i>delay</i> 시간 간격(1/100초)에 대한 지연 응답입니다. 양수 값을 사용하면 트랜잭션의 각 명령에 지연이 적용되며, 음수 값을 사용하면 주소 전달(FROM_ACCESS 테이블에 대한 SMTP MAIL FROM: 명령, 다른 테이블에 대한 SMTP RCPT TO: 명령)에만 지연이 적용됩니다.                                             |
| \$Ttag                                                       | <i>tag</i> 접두어가 사용됩니다.                                                                                                                                                                                                   |
| \$Aheader                                                    | 메일에 헤더 행 <i>header</i> 를 추가합니다.                                                                                                                                                                                          |

**표 17-2** 액세스 매핑 플래그

| 플래그                | 설명                                                                                                                                                                                                                                                                                           |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| \$Gconversion_tag  | ORIG_SEND_ACCESS, SEND_ACCESS, ORIG_MAIL_ACCESS 및 MAIL_ACCESS에서 사용될 경우 매핑 결과에서 값을 읽고 이를 현재 수신자에게 적용될 변환 태그 집합으로 처리합니다. FROM_ACCESS와 함께 사용될 경우 변환 태그가 모든 수신자에게 적용됩니다. \$G의 위치는 매핑에서 읽은 인수 시퀀스에서 \$A(헤더 주소) 다음입니다. <a href="#">419페이지</a> 의 "메일 변환 태그"를 참조하십시오.                                |
| \$Sx,y,z           | * 세로 막대( )로 구분된 추가 인수를 매핑 결과에서 읽습니다. 이 인수는 쉼표로 구분된 하나에서 세 개의 정수 값으로 구성됩니다. 첫 번째 값은 트랜잭션에 대한 최소 blocklimit를 새로 설정하고, 두 번째 값은 최소 recipientlimit를 새로 설정하며, 세 번째 값은 최소 recipientcutoff를 새로 설정합니다. 이 인수는 모든 캡처 인수를 읽은 후에 매핑 결과에서 읽습니다. 자세한 내용은 <a href="#">388페이지</a> 의 "절대 메일 크기 제한 지정"을 참조하십시오. |
| \$Xerror-code      | 메일 거부 시 지정된 error-code 확장 SMTP 오류 코드를 발행합니다.                                                                                                                                                                                                                                                 |
| \$, spamadjust_arg | 액세스 매핑 테이블에서 sieve spamadjust 작업을 수행할 수 있습니다. 인수는 spamadjust 인수와 동일한 형식을 취합니다. 이러한 매핑의 일부는 수신자별 기준으로 적용된다는 점에 유의하십시오. 수행된 spamadjust 작업은 모든 수신자에 적용됩니다.                                                                                                                                      |
| \$Nstring          | 선택적 오류 텍스트 string을 사용하여 액세스를 거부합니다.                                                                                                                                                                                                                                                          |
| \$Fstring          | \$N string에 대한 동의어, 즉 선택적 오류 텍스트 string을 사용하여 액세스를 거부합니다.                                                                                                                                                                                                                                    |

\* FROM\_ACCESS 테이블에만 사용할 수 있습니다.

+ 인수가 있는 여러 개의 플래그를 사용하려면 인수를 세로 막대 문자 |로 구분하고 이 테이블에 나열된 순서대로 인수를 배치합니다.

++ \$K 플래그가 FROM\_ACCESS 매핑 테이블에 적용되려면 소스 채널에 authrewrite 키워드가 포함되어야 합니다.

+++ 문제가 있는 보낸 사람을 처리할 때는 서비스 거부 공격을 방지하기 위해 \$D 플래그를 사용하는 것이 좋습니다. 특히 모든 \$> 항목 또는 액세스를 거부하는 \$< 항목에는 \$D를 사용하는 것이 좋습니다.

## SEND\_ACCESS 및 ORIG\_SEND\_ACCESS 테이블

SEND\_ACCESS 및 ORIG\_SEND\_ACCESS 매핑 테이블을 사용하여 메일을 송수신할 수 있거나 할 수 없는 사용자 또는 둘 다를 제어할 수 있습니다. 액세스 검사는 메일 봉투 From: 주소와 봉투 To: 주소에서 사용 가능하며 메일을 전송한 채널과 대상 채널을 알 수 있습니다.

SEND\_ACCESS 또는 ORIG\_SEND\_ACCESS 매핑 테이블이 있으면 MTA를 통과하여 전달되는 모든 메일의 각 수신자에 대해 MTA는 다음 형식의 문자열로 테이블을 스캔합니다(세로 막대 문자 | 사용).

```
src-channel|from-address|dst-channel|to-address
```

src-channel은 메일이 대기 중인 채널이고 from-address는 메일을 보낸 사람의 주소, dst-channel은 메일이 대기될 채널, to-address는 메일 주소가 지정된 주소입니다. 이 네 필드에 별표를 사용하면 해당 필드는 모든 채널 또는 주소와 일치하게 됩니다.

여기서 주소는 봉투 주소, 즉 봉투 From: 주소와 봉투 To: 주소입니다. SEND\_ACCESS의 경우 봉투 To:주소는 다시 쓰기, 별칭 확장 등이 수행된 후 검사되고, ORIG\_SEND\_ACCESS의 경우 원래 지정된 봉투 To:주소를 다시 쓴 다음, 그리고 별칭 확장 전에 검사됩니다.

검색 문자열이 패턴(즉, 테이블 항목의 왼쪽)과 일치하면 매핑의 결과 출력이 검사됩니다. 출력에 플래그 \$Y 또는 \$y가 포함된 경우 해당 To:주소에 대한 대기가 허용됩니다. 출력에 플래그 \$N, \$n, \$F 또는 \$f가 포함되어 있으면 해당 주소에 대한 대기가 거부됩니다. 거부된 경우 선택적 거부 텍스트가 매핑 출력에 표시될 수 있습니다. 이 문자열은 MTA가 표시하는 거부 오류에 포함됩니다. 문자열이 출력되지 않으면(\$N, \$n, \$F 또는 \$f 플래그 제외) 기본 거부 텍스트가 사용됩니다. 추가 플래그에 대한 설명은 [514페이지의 "액세스 제어 매핑 테이블 플래그"](#)를 참조하십시오.

MTA 옵션 ACCESS\_ORCPT를 1로 설정하면 원래 수신자(ORCPT) 주소를 포함하는 SEND\_ACCESS, ORIG\_SEND\_ACCESS, MAIL\_ACCESS 및 ORIG\_MAIL\_ACCESS 매핑 테이블로 전달되는 검사 값에 수직 막대로 구분된 필드가 또 하나 추가됩니다. 메일에 ORCPT 주소가 없으면 수정되지 않은 원래 RCPT TO: 주소가 대신 사용됩니다. 기본값은 0이고 검사 값은 마지막에 있습니다.

```
src-channel|from-address|dst-channel|to-address|ORCPT_address
```

다음 예에서는 mail, Pine 등의 UNIX 사용자 에이전트가 보낸 메일(로컬, 1, 채널 및 메일에서 인터넷으로 전송)이 일종의 TCP/IP 채널로 나갑니다. 여기서는 포스트마스터를 제외한 이러한 로컬 사용자가 인터넷으로 메일을 보낼 수 없지만 인터넷에서 메일을 받을 수는 있다고 가정합니다. 이 경우 아래 예에 표시된 SEND\_ACCESS 매핑 테이블을 사용하는 것이 이러한 제한을 적용하는 한 가지 방법이 됩니다. 매핑 테이블에서 로컬 호스트 이름을 sesta.com으로 가정합니다. 채널 이름 tcp\_\*에서 와일드 카드가 사용되어 가능한 모든 TCP/IP 채널 이름(예: tcp\_local)과 일치합니다.

**코드 예 17-1** SEND\_ACCESS 매핑 테이블

```
SEND_ACCESS

*|postmaster@sesta.com|*|*      $Y
*|*|*|postmaster@sesta.com      $Y
1|*@sesta.com|tcp_*|*          $NInternet$ postings$ are$ not$ \
    permitted
```

거부 메일에 공백을 입력하려면 달러 기호를 사용합니다. 달러 기호가 없으면 거부가 일찍 완료되어 "Internet postings are not permitted" 대신 "Internet"만 표시됩니다. 이 예에서는 PC 기반 메일 시스템이나 POP 또는 IMAP 클라이언트 등 "로컬" 게시의 소스에 대한 다른 가능성은 무시합니다.

---

**주** MTA 거부 오류 텍스트를 메일을 보내려는 사용자에게 실제로 표시할 것인지 여부는 메일을 보내려는 클라이언트가 결정합니다. SEND\_ACCESS 를 사용하여 받는 SMTP 메일을 거부하는 경우 MTA는 선택적 거부 텍스트를 비롯하여 SMTP 거부 코드만 발행합니다. 즉, 이 정보를 사용하여 원래 보낸 사람에게 보낼 바운스 메일을 구성할 것인지는 SMTP 클라이언트가 결정합니다.

---

## MAIL\_ACCESS 및 ORIG\_MAIL\_ACCESS 매핑 테이블

MAIL\_ACCESS 매핑 테이블은 SEND\_ACCESS와 PORT\_ACCESS 매핑 테이블의 수퍼 세트입니다. 여기에서는 SEND\_ACCESS의 채널과 주소 정보를 PORT\_ACCESS의 IP 주소 및 포트 번호 정보와 조합합니다. 마찬가지로, ORIG\_MAIL\_ACCESS 매핑 테이블은 ORIG\_SEND\_ACCESS와 PORT\_ACCESS 매핑 테이블의 수퍼 세트입니다. MAIL\_ACCESS에 대한 검사 문자열 형식은 다음과 같습니다.

*port-access-probe-info | app-info | submit-type | send\_access-probe-info*

마찬가지로 ORIG\_MAIL\_ACCESS의 검사 문자열 형식은 다음과 같습니다.

*port-access-probe-info | app-info | submit-type | orig\_send\_access-probe-info*

여기서 받는 SMTP 메일의 경우 *port-access-probe-info*는 보통 PORT\_ACCESS 매핑 테이블 검사에 포함된 모든 정보로 구성되는 반면, 그 외의 경우에는 비어 있는 상태가 됩니다.

*app-info*에는 HELO/EHLO SMTP 명령에서 요구한 시스템 이름이 포함됩니다. 이 이름은 문자열 끝에 표시되며 슬래시(/)로 나머지 문자열(일반적으로 "SMTP")과 구분합니다. 요구된 시스템 이름은 일부 웹 및 바이러스를 차단하는 데 유용하게 사용될 수 있습니다.

*submit-type*은 Messaging Server로 메일이 전송된 방법에 따라 MAIL, SEND, SAML, SOML 중 하나가 될 수 있습니다. 일반적으로 그 값은 MAIL이며 이는 메일로 전송된다는 의미입니다. 즉, 브로드캐스트 요청(또는 조합된 브로드캐스트/메일 요청)이 SMTP 서버로 전송된 경우 SEND, SAML 또는 SOML이 발생할 수 있습니다. 또한 MAIL\_ACCESS 매핑의 경우 *send-access-probe-info*는 일반적으로 SEND\_ACCESS 매핑 테이블 검사에 포함된 모든 정보로 구성됩니다. *orig-send-access-probe-info*는 일반적으로 ORIG\_MAIL\_ACCESS 매핑과 유사하게 ORIG\_SEND\_ACCESS 매핑 테이블 검사에 포함된 모든 정보로 구성됩니다.

MTA 옵션 ACCESS\_ORCPT을 1로 설정하면 원래 수신자(ORCPT) 주소를 포함하는 SEND\_ACCESS, ORIG\_SEND\_ACCESS, MAIL\_ACCESS 및 ORIG\_MAIL\_ACCESS 매핑 테이블로 전달되는 검사 값에 수직 막대로 구분된 필드가 또 하나 추가됩니다. 메일에 ORCPT 주소가 없으면 수정되지 않은 원래 RCPT TO: 주소가 대신 사용됩니다. 기본값은 0이고 검사 값은 마지막에 있습니다. 예를 들면 다음과 같습니다.

*port-access-probe-info | app-info | submit-type | send\_access-probe-info | ORCPT\_address*

받는 TCP/IP 연결 정보를 채널 및 주소 정보와 동일한 매핑 테이블에서 사용할 수 있는 경우에는 특정 IP 주소에서 보낸 메일에 표시되도록 허용되는 봉투 From: 주소를 지정하는 등의 제어를 보다 편리하게 수행할 수 있습니다. 이렇게 하면 전자 메일 위조의 가능성을 줄이거나 사용자가 자신의 POP 및 IMAP 클라이언트의 From: 주소를 적절하게 설정하도

록 유도할 수 있습니다. 예를 들어, 봉투 From:주소 vip@siroe.com이 IP 주소 1.2.3.1 및 1.2.3.2에서 받는 메일에만 나타나도록 하고 1.2.0.0 서브넷에 있는 시스템으로부터 받는 메일의 봉투 From:주소는 siroe.com에서 보낸 것으로 하려면 아래 예에 표시된 대로 MAIL\_ACCESS 매핑 테이블을 사용할 수 있습니다.

**코드 예 17-2** MAIL\_ACCESS 매핑 테이블

```
MAIL_ACCESS

! Entries for vip's two systems
!
TCP|*|25|1.2.3.1|*|SMTP|MAIL|tcp_*|vip@siroe.com|*|* $Y
TCP|*|25|1.2.3.2|*|SMTP|MAIL|tcp_*|vip@siroe.com|*|* $Y
!
! Disallow attempts to use vip's From: address from other
! systems
!
TCP|*|25|*|*|SMTP|MAIL|tcp_*|vip@siroe.com|*|* \
    $N500$ Not$ authorized$ to$ use$ this$ From:$ address
!
! Allow sending from within our subnet with siroe.com From:
! addresses
!
TCP|*|25|1.2.*.*|*|SMTP|MAIL|tcp_*|*@siroe.com|*|* $Y
!
! Allow notifications through
!
TCP|*|25|1.2.*.*|*|SMTP|MAIL|tcp_*||*|* $Y
!
! Block sending from within our subnet with non-siroe.com
! addresses
!
TCP|*|25|1.2.*.*|*|SMTP|MAIL|tcp_*|*|*|* \
    $NOnly$ siroe.com$ From:$ addresses$ authorized
```



## FROM\_ACCESS 매핑 테이블

FROM\_ACCESS 매핑 테이블은 메일을 보낼 수 있는 사용자를 제어하거나 인증된 주소를 가진 From: 주소를 무시하는 데 사용할 수 있습니다.

FROM\_ACCESS 매핑 테이블에 대한 입력 검사 문자열은 MAIL\_ACCESS 매핑 테이블에서 대상 채널과 주소를 제외하고 인증된 보낸 사람 정보(사용 가능한 경우)를 추가한 것과 같습니다. 따라서 FROM\_ACCESS 매핑 테이블이 있는 경우 Messaging Server는 시도되는 각 메일 전송에 대해 다음 형식의 문자열을 가진 테이블을 검색합니다(세로 막대 문자 | 사용 주의).

```
port-access-probe-info | app-info | submit-type | src-channel | from-address | auth-from
```

여기서 받는 SMTP 메일의 경우 *port-access-probe-info*는 보통 PORT\_ACCESS 매핑 테이블 검사에 포함된 모든 정보로 구성되는 반면, 그 외의 경우에는 비어 있는 상태가 됩니다.

*app-info*에는 HELO/EHLO SMTP 명령에서 요구한 시스템 이름이 포함됩니다. 이 이름은 문자열 끝에 표시되며 슬래시(/)로 나머지 문자열(일반적으로 "SMTP")과 구분합니다. 요구된 시스템 이름은 일부 웹 및 바이러스를 차단하는 데 유용하게 사용될 수 있습니다.

*submit-type*은 MTA로 메일이 전송된 방법에 따라 MAIL, SEND, SAML, SOML 중 하나가 될 수 있습니다. 일반적으로 그 값은 MAIL이며 이는 메일로 전송된다는 의미입니다. 즉, 브로드캐스트 요청(또는 조합된 브로드캐스트/메일 요청)이 SMTP 서버로 전송된 경우 SEND, SAML 또는 SOML이 발생할 수 있습니다. *src-channel*은 메일을 보낸(메일을 대기열에 넣는) 채널, *from-address*는 메일을 최초로 보낸 사람의 주소이며 *auth-from*은 인증된 보낸 사람 주소(이 정보가 사용 가능한 경우)이고 인증된 정보를 사용할 수 없는 경우에는 비어 있습니다.

검사 문자열이 패턴(즉, 테이블 항목의 왼쪽)과 일치하면 매핑의 결과 출력이 검사됩니다. 출력에 플래그 \$Y 또는 \$y가 포함된 경우 해당 To: 주소에 대한 대기가 허용됩니다. 출력에 플래그 \$N, \$n, \$F 또는 \$f가 포함되어 있으면 해당 주소에 대한 대기가 거부됩니다. 거부된 경우 선택적 거부 텍스트가 매핑 출력에 표시될 수 있습니다. 이 문자열은 Messaging Server가 표시하는 거부 오류에 포함될 수 있습니다. 문자열이 출력되지 않으면(\$N, \$n, \$F 또는 \$f 플래그 제외) 기본 거부 텍스트가 사용됩니다. 추가 플래그에 대한 설명은 514 페이지의 "액세스 제어 매핑 테이블 플러그"를 참조하십시오.

FROM\_ACCESS는 메일 발송자를 기준으로 전송 가능한 메일을 허용할지 여부를 결정하는 것 외에도 봉투 From: 주소를 \$J 플래그를 통해 변경하거나 authrewrite 채널 키워드(반은 메일의 Sender: 헤더 주소 추가)의 결과를 \$K 플래그를 통해 수정하는 데 사용할 수도 있습니다. 예를 들어, 이 매핑 테이블을 사용하여 다음과 같이 원래의 봉투 From: 주소를 인증된 주소로 바꿀 수 있습니다.

**코드 예 17-3** FROM\_ACCESS 매핑 테이블

```
FROM_ACCESS
* |SMTP|* |tcp_auth|* |      $Y
* |SMTP|* |tcp_auth|* |*    $Y$J$3
```

FROM\_ACCESS 매핑 테이블을 사용하여 일부 소스 채널의 0이 아닌 값에 대해 authrewrite를 설정한 결과를 수정할 때 인증된 주소가 글자 그대로 사용되는 경우에는 FROM\_ACCESS를 사용하지 않아도 됩니다.

예를 들어, tcp\_local 채널에 authrewrite 2를 설정한 경우에는 authrewrite만으로도 이 결과를 얻을 수 있기 때문에(인증된 주소를 그대로 추가) FROM\_ACCESS 매핑 테이블이 필요하지 않습니다.

```
FROM_ACCESS
* |SMTP|* |tcp_auth|* |      $Y
* |SMTP|* |tcp_auth|* |*    $Y$K$3
```

하지만 FROM\_ACCESS의 실제 용도는 아래 예에 표시된 대로 보다 복잡하고 세밀한 변경을 허용하는 것입니다. Sender: 헤더 행(SMTP AUTH 인증 전송자 주소 표시)을 받는 메일에 추가하려는 경우에는 authrewrite만 사용해도 됩니다. 하지만 SMTP AUTH 인증 전송자 주소가 봉투 From: 주소와 다른 경우에만 Sender: 헤더 행 등을 받는 메일에 추가하는(즉, 주소가 일치하는 경우에는 Sender: 헤더 행) 것으로 가정하고, 또한 봉투 From:에 선택적 하위 주소 정보가 포함되어 있다는 이유만으로 SMTP AUTH와 봉투 From:을 서로 다른 것으로 간주하지 않는 것으로 가정합니다.

```

FROM_ACCESS

! If no authenticated address is available, do nothing
*|SMTP|*|tcp_auth|*|          $Y
! If authenticated address matches envelope From:, do nothing
*|SMTP|*|tcp_auth|*|$2*      $Y
! If authenticated address matches envelope From: sans
! subaddress, do nothing
*|SMTP|*|tcp_auth|*+*@*|$2*@$4*  $Y
! Fall though to...
! ...authenticated address present, but didn't match, so force
! Sender: header
*|SMTP|*|tcp_auth|*|*        $Y$K$3
    
```

## PORT\_ACCESS 매핑 테이블

디스패처는 IP 주소와 포트 번호를 기반으로 선택적으로 받는 연결을 수락하거나 거부할 수 있습니다. 디스패처는 시작 시에 PORT\_ACCESS라는 매핑 테이블을 찾습니다. 이 테이블이 있으면 디스패처는 연결 정보를 다음 형식으로 구성합니다.

`TCP|server-address|server-port|client-address|client-port`

디스패처는 모든 PORT\_ACCESS 매핑 항목에 대응시키려 시도합니다. 매핑 결과에 \$N 또는 \$F가 포함되어 있으면 연결이 즉시 닫힙니다. 매핑의 다른 결과는 연결이 수락되는 것을 나타냅니다. 거부 메일 다음에 선택적으로 \$N 또는 \$F가 올 수 있습니다. \$N 또는 \$F가 오는 경우 메일은 닫히기 직전에 해당 연결로 다시 보내질 수 있습니다. CRLF 종결자는 연결로 다시 보내지기 전에 문자열에 추가됩니다.

---

**주** MMP는 PORT\_ACCESS 매핑 테이블을 사용하지 않습니다. 특정 IP 주소의 SMTP 연결을 거부하기를 원하고 MMP를 사용하는 경우 TCPAccess 옵션을 사용해야 합니다. [172페이지의 "MMP를 사용하여 메일 액세스 구성"](#)을 참조하십시오. 매핑 테이블을 사용하여 SMTP 연결을 제어하려면 INTERNAL\_IP 매핑 테이블을 사용합니다([530페이지의 "외부 사이트에 대한 SMTP 릴레이 허용"](#) 참조).

---

\$< 플래그 다음에 선택적 문자열이 있으면 매핑 검사가 일치하는 경우 Messaging Server 는 문자열을 syslog(UNIX) 또는 이벤트 로그(NT)로 보냅니다. \$> 플래그 다음에 선택적 문자열이 오면 액세스가 거부된 경우 Messaging Server는 syslog(UNIX) 또는 이벤트 로그(NT)로 보냅니다. LOG\_CONNECTION MTA 옵션이 비트 1로 설정되고 \$N 플래그가 설정되어 연결이 거부된 경우 \$T 플래그를 지정하면 "T" 항목이 연결 로그에 기록됩니다. LOG\_CONNECTION MTA 옵션이 비트 4로 설정된 경우에는 사이트 제공 텍스트가 PORT\_ACCESS 항목에 제공되어 "C" 연결 로그 항목에 포함될 수 있습니다. 이러한 텍스트를 지정하려면 항목의 오른쪽에 두 개의 세로 막대 문자를 넣고 그 뒤에 원하는 텍스트를 입력합니다. 표 17-3에는 사용 가능한 플래그가 나열되어 있습니다.

**표 17-3** PORT\_ACCESS 매핑 플래그

| 플래그                                                                       | 설명                                                                                                                                                      |
|---------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|
| \$Y                                                                       | 액세스를 허용합니다.                                                                                                                                             |
| <b>인수가 있는 플래그, 인수 읽기 순서에 따라+</b>                                          |                                                                                                                                                         |
| \$< 문자열                                                                   | 검사가 일치하는 경우 syslog(UNIX) 또는 이벤트 로그(NT)에 문자열을 보냅니다.                                                                                                      |
| \$> 문자열                                                                   | 액세스가 거부되는 경우 syslog(UNIX) 또는 이벤트 로그(NT)에 문자열을 보냅니다.                                                                                                     |
| \$N 문자열                                                                   | 선택적 오류 텍스트 문자열을 사용하여 액세스를 거부합니다.                                                                                                                        |
| \$F 문자열                                                                   | \$N 문자열에 대한 동의어, 즉 선택적 오류 텍스트 문자열을 사용하여 액세스를 거부합니다.                                                                                                     |
| \$T 텍스트                                                                   | LOG_CONNECTION MTA 옵션이 비트 1로 설정되고 \$N 플래그가 설정되어 연결이 거부된 경우 \$T 플래그를 지정하면 "T" 항목이 연결 로그에 기록됩니다 선택적 텍스트(두 개의 세로 막대 문자 다음에 표시되어야 함)가 연결 로그 항목에 포함될 수 있습니다. |
| + 인수가 있는 여러 개의 플래그를 사용하려면 인수를 세로 막대 문자  로 구분하고 이 테이블에 나열된 순서대로 인수를 배치합니다. |                                                                                                                                                         |

예를 들어, 다음 매핑은 설명하는 텍스트가 없이 추출되어 거부된 특정 호스트를 제외한 단일 네트워크로부터의 SMTP 연결(포트 25, 일반 SMTP 포트)만 수락합니다.

```

PORT_ACCESS

TCP|*|25|192.123.10.70|* $N500
TCP|*|25|192.123.10.*|* $Y
TCP|*|25|*|* $N500$ Bzzzt$ thank$ you$ for$ \
    playing.
    
```

PORT\_ACCESS 매핑 테이블을 변경한 뒤에는 디스패처를 다시 시작해야 디스패처에 변경 내용이 적용됩니다. 컴파일된 MTA 구성을 사용하는 경우에는 먼저 구성을 다시 컴파일하여 변경 내용을 컴파일된 구성에 통합시켜야 합니다.

PORT\_ACCESS 매핑 테이블은 특별히 IP 기반 거부를 수행하기 위한 것입니다. 메일 주소 수준 일반 제어의 경우 SEND\_ACCESS 또는 MAIL\_ACCESS 매핑 테이블이 보다 적합합니다.

## MTA에 대해 지정된 IP 액세스 연결 제한

Port Access 매핑 테이블에 conn\_throttle.so 공유 라이브러리를 사용하여 특정 IP 주소가 MTA에 연결되는 횟수를 제한할 수 있습니다. 특정 IP 주소로 연결을 제한하는 기능은 서비스 거부 공격에 사용되는 과도한 연결을 방지하는 데 유용합니다.

conn\_throttle.so는 특정 IP 주소가 MTA에 너무 자주 연결하는 것을 제한하기 위해 PORT\_ACCESS 매핑 테이블에 사용되는 공유 라이브러리입니다. 모든 구성 옵션은 다음과 같이 연결 억제 공유 라이브러리에 대한 매개 변수로 지정됩니다.

```
[$msg_svr_base/lib/conn_throttle.so,throttle,IP-address,max-rate]
```

IP-address는 원격 시스템의 점으로 구분된 십진수 형식의 주소이며, max-rate는 이 IP 주소에 대한 최대 분당 연결 비율입니다.

루틴 이름 throttle\_p를 루틴 축소 버전의 throttle 대신 사용할 수 있습니다.

throttle\_p는 향후 기존에 너무 많이 연결했던 연결을 거부하게 됩니다. 최대 비율이 100인데 분당 250번의 연결이 시도된 경우에는 해당 분 내에 처음 100번의 연결 시도 후 원격 사이트가 차단되며 그 다음 1분 동안에도 차단됩니다. 즉, 매 분마다 시도된 전체 연결 수에서 최대 비율을 빼서 전체 연결 수가 최대 비율보다 크면 원격 시스템이 차단됩니다.

지정된 IP 주소가 분당 최대 연결 비율을 초과하지 않으면 공유 라이브러리 호출이 실패합니다.

해당 비율을 초과하면 호출에 성공하지만 아무 것도 반환하지 않습니다. 이 작업은 다음 예와 같이 \$C/\$E 조합으로 수행됩니다.

PORT\_ACCESS

```
TCP|*|25|*|* \
$C$[msg_svr_base/lib/conn_throttle.so,throttle,$1,10] \
$N421$ Connection$ not$ accepted$ at$ this$ time$E
```

여기서

\$C는 다음 테이블 항목에서 시작한 매핑 프로세스를 계속하여 이 항목의 출력 문자열을 매핑 프로세스에 대한 새 입력 문자열로 사용합니다.

\$[msg\_svr\_base/lib/conn\_throttle.so,throttle,\$1,10]은 throttle을 라이브러리 루틴, \$1을 서버 IP 주소, 그리고 10을 분당 연결 임계값으로 사용하는 라이브러리 호출입니다.

\$N421\$ Connection\$ not\$ accepted\$ at\$ this\$ time은 액세스를 거부하고 "Connection not accepted at this time"이라는 메일과 함께 421 SMTP 코드(임시 부정 완료)를 반환합니다.

\$E는 이제 매핑 프로세스를 닫습니다. 이 항목의 출력 문자열을 매핑 프로세스의 최종 결과로 사용합니다.

## 액세스 제어가 적용되는 경우

Messaging Server는 가능한 빨리 액세스 제어 매핑을 검사합니다. 정확한 작업 수행 시기는 사용 중인 전자 메일 프로토콜에 따라 다릅니다(검사해야 하는 정보가 사용 가능한 경우).

SMTP 프로토콜의 경우 MAIL FROM: 명령에 대한 응답으로 FROM\_ACCESS 거부가 수행된 후 보내는 측에서 수신자 정보나 메일 데이터를 보낼 수 있습니다. 보내는 측에서 메일 데이터를 보내기 전에 RCPT TO: 명령에 대한 응답으로 SEND\_ACCESS 또는 MAIL\_ACCESS 거부가 수행됩니다. SMTP 메일이 거부되면 Messaging Server는 메일 데이터를 수락하거나 볼 수 없으므로 이러한 거부 수행으로 인한 오버헤드가 최소화됩니다.

여러 개의 액세스 제어 매핑 테이블이 있으면 Messaging Server는 이들 모두를 검사합니다. 즉, FROM\_ACCESS, SEND\_ACCESS, ORIG\_SEND\_ACCESS, MAIL\_ACCESS 및 ORIG\_MAIL\_ACCESS 매핑 테이블이 모두 영향을 받을 수 있습니다.

# 액세스 제어 매핑 테스트

imsimta test -rewrite 유틸리티(특히 -from, -source\_channel, -sender 및 -destination\_channel 옵션과 함께 사용 시)는 액세스 제어 매핑을 테스트할 때 유용합니다. 자세한 내용은 *Sun Java System Messaging Server Administration Reference*(<http://docs.sun.com/doc/819-0106>)를 참조하십시오. 아래 예는 샘플 SEND\_ACCESS 매핑 테이블 및 그 검사 결과를 보여 줍니다.

## MAPPING TABLE:

SEND\_ACCESS

```
tcp_local|friendly@siroe.com|1|User@sesta.com    $Y
tcp_local|unwelcome@varrius.com|1|User@sesta.com $NGo$ away!
```

## PROBE:

```
$ TEST/REWRITE/FROM="friendly@siroe.com" -
_ $ /SOURCE=tcp_local/DESTINATION=1 User@sesta.com
...
Submitted address list:
  1
    User (SESTA.COM) *NOTIFY FAILURES* *NOTIFY DELAYS* Submitted
notifications list:

$ TEST/REWRITE/FROM="unwelcome@varrius.com" -
_ $ /SOURCE=tcp_local/DESTINATION=1 User@sesta.com
...
Submitted address list:
Address list error -- 5.7.1 Go away! User@sesta.com

Submitted notifications list:
```

## SMTP 릴레이 추가

기본적으로 Messaging Server는 SMTP 릴레이 시도를 차단하도록 구성되어 있습니다. 즉, 인증되지 않은 외부 소스의 외부 주소로의 메일 전송 시도를 거부합니다. 외부 시스템은 서버가 있는 호스트가 아닌 모든 시스템을 말합니다. 이 기본 구성은 다른 모든 시스템을 외부 시스템으로 간주하기 때문에 과도하게 SMTP 릴레이를 차단합니다.

Messaging Server 시스템의 SMTP 서버를 통해 외부 주소로 지정된 메일을 전송하려고 시도하는 IMAP 및 POP 클라이언트, 그리고 SMTP AUTH(SASL)를 사용하여 인증하지 않는 클라이언트의 전송 시도는 거부됩니다. 따라서 사용자 구성을 수정하여 릴레이를 항상 수락하는 자체 내부 시스템과 서브넷을 인식하도록 할 수 있습니다.

내부로 인식되는 시스템과 서브넷은 일반적으로 `msg_svr_base/config/mappings` 파일에 포함된 `INTERNAL_IP` 매핑 테이블을 통해 제어됩니다.

예를 들어, IP 주소가 123.45.67.89인 Messaging Server 시스템에서 기본 `INTERNAL_IP` 매핑 테이블은 다음과 같이 나타납니다.

```
INTERNAL_IP

$(123.45.67.89/32)  $Y
127.0.0.1  $Y
*  $N
```

여기서 첫 번째 항목은 \$(IP-pattern/significant-prefix-bits) 구문을 사용하여 123.45.67.89의 32비트와 완전히 일치하는 모든 IP 주소를 내부로 인식하도록 지정합니다. 두 번째 항목은 루프백 IP 주소 127.0.0.1을 내부로 인식합니다. 마지막 항목은 다른 모든 IP 주소가 내부로 인식되지 않도록 지정합니다. 모든 항목 앞에는 적어도 하나의 공백이 있어야 합니다.

마지막 \$N 항목 앞에 추가 IP 주소 또는 서브넷을 지정하여 항목을 추가할 수 있습니다. 이러한 항목은 왼쪽에 IP 주소나 서브넷(\$(.../...)) 구문을 사용하여 서브넷 지정)을 지정하고 오른쪽에 \$Y를 지정합니다. 또는 기존 \$(.../...) 항목을 수정하여 더 일반적인 서브넷을 허용할 수 있습니다.



예를 들어, 동일한 샘플 사이트의 네트워크가 클래스 C 네트워크, 즉 123.45.67.0 서브넷을 모두 소유하는 네트워크인 경우 해당 사이트에서는 주소 일치에 사용되는 비트 수를 변경하여 첫 번째 항목을 수정해야 합니다. 아래 매핑 테이블에서는 32비트를 24비트로 수정합니다. 이렇게 하면 클래스 C 네트워크의 모든 클라이언트에서 SMTP 릴레이 서버를 통해 메일을 릴레이할 수 있습니다.

```
INTERNAL_IP

$(123.45.67.89/24) $Y
127.0.0.1 $Y
* $N
```

또는 사이트가 123.45.67.80-123.45.67.99 범위 내의 IP 주소만 소유하는 경우 해당 사이트는 다음을 사용할 수 있습니다.

```
INTERNAL_IP

! Match IP addresses in the range 123.45.67.80-123.45.67.95
$(123.45.67.80/28) $Y
! Match IP addresses in the range 123.45.67.96-123.45.67.99
$(123.45.67.96/30) $Y
127.0.0.1 $Y
* $N
```

`imsimta test -match` 유틸리티는 IP 주소가 특정 `$(.../...)` 테스트 조건에 일치하는지 여부를 검사할 때 유용하게 사용할 수 있습니다. `imsimta test -mapping` 유틸리티는 `INTERNAL_IP` 매핑 테이블이 다양한 IP 주소 입력에 대해 원하는 결과를 반환하는지 검사할 때 매우 유용합니다.

`INTERNAL_IP` 매핑 테이블을 수정한 뒤에는 `imsimta restart` 명령(컴파일된 구성을 실행하고 있지 않은 경우) 또는 `imsimta refresh` 명령(컴파일된 구성을 실행하는 경우)을 실행해야 변경 사항이 적용됩니다.

매핑 테이블과 일반적인 매핑 테이블 형식 및 `imsimta` 명령줄 유틸리티에 대한 자세한 내용은 `Messaging Server Reference Manual`을 참조하십시오.

## 외부 사이트에 대한 SMTP 릴레이 허용

위에서 설명한 것처럼 모든 내부 IP 주소를 `INTERNAL_IP` 매핑 테이블에 추가해야 합니다. 다른 시스템/사이트에서 SMTP 릴레이를 허용하려는 경우 가장 간단한 방법은 해당 시스템/사이트를 `INTERNAL_IP` 매핑 테이블에 사용자의 실제 내부 IP 주소와 함께 포함시키는 것입니다.

다른 시스템/사이트를 실제 내부 시스템/사이트로 인식시키지 않으려는 경우(예를 들어 로깅이나 다른 제어 목적을 위해 *실제 내부 시스템과 릴레이 권한을 가진 내부가 아닌 시스템을 구분하려는 경우*) 다른 방법으로 시스템을 구성할 수 있습니다.

한 가지 방법은 다른 시스템에서 보내는 메일을 받는 특별 채널을 설정하는 것입니다. 이렇게 하려면 기존 `tcp_internal`과 유사한 `tcp_friendly` 채널을 공식 호스트 이름 `tcp_friendly-daemon`으로 만들고 다른 시스템 IP 주소가 나열된 `INTERNAL_IP` 매핑 테이블과 유사한 `FRIENDLY_IP` 매핑 테이블을 만듭니다. 그런 후 다음과 같은 현재 다시 쓰기 규칙 바로 뒤에

```
! Do mapping lookup for internal IP addresses
[] $E$R$${INTERNAL_IP,$L}$U%[$L]@tcp_intranet-daemon
```

다음과 같이 다시 쓰기 규칙을 새로 추가합니다.

```
! Do mapping lookup for "friendly", non-internal IP addresses []
$E$R$${FRIENDLY_IP,$L}$U%[$L]@tcp_friendly-daemon
```

또 다른 방법은 위의 `ORIG_SEND_ACCESS` 매핑 테이블에 다음 형식의 새로운 최종 `$N` 항목을 추가하고

```
tcp_local|*@siroe.com|tcp_local|* $Y
```

(여기서 `siroe.com`은 다른 도메인의 이름) 다음 형식의 `ORIG_MAIL_ACCESS` 매핑 테이블을 추가하는 것입니다.

```
ORIG_MAIL_ACCESS
```

```
TCP|*|25|$(match-siroe.com-IP-addresses)|*|SMTP|MAIL| \
tcp_local|*@siroe.com|tcp_local|* $Y
TCP|*|*|*|SMTP|MAIL|tcp_local|*|tcp_local|* $N
```

테이블, 여기서 `$(...)` IP 주소 구문은 이전 절에서 설명한 것과 같은 구문입니다.

`ORIG_SEND_ACCESS` 검사는 주소가 정상인 경우 지속되므로 계속 수행할 수 있으며 또한 IP 주소가 `siroe.com` IP 주소에 해당하는 경우에 한해 보다 엄격한 `ORIG_MAIL_ACCESS` 검사를 수행할 수 있습니다.

## SMTP 릴레이 차단 구성

액세스 제어 매핑을 사용하여 다른 사용자가 Messaging Server 시스템을 통해 SMTP 메일을 릴레이하지 못하도록 할 수 있습니다. 예를 들어, 다른 사용자가 메일 시스템을 사용하여 대량 전자 메일을 수백 수천의 인터넷 메일함으로 릴레이하지 못하도록 할 수 있습니다.

기본적으로 Messaging Server는 로컬 POP 및 IMAP 사용자에 의한 릴레이를 포함하여 모든 SMTP 릴레이 작업을 차단합니다.

적합한 로컬 사용자에게 릴레이를 허용하면서 인증되지 않은 릴레이를 차단하려면 Messaging Server에서 이 두 클래스의 사용자를 서로 구분할 수 있도록 구성해야 합니다. 예를 들어, POP나 IMAP를 사용하는 로컬 사용자의 경우 Messaging Server가 SMTP 릴레이 역할을 수행합니다.

SMTP 릴레이를 차단하려면 다음이 가능해야 합니다.

- 내부 메일과 외부 메일 구분
- [533페이지의 "인증된 사용자의 메일 구분"](#)
- [534페이지의 "메일 릴레이 금지"](#)

내부 호스트 및 클라이언트에서 SMTP 릴레이를 사용하려면 "내부" IP 주소나 서브넷을 INTERNAL\_IP 매핑 테이블에 추가해야 합니다.

## MTA의 내부 메일과 외부 메일 구분 방법

메일 릴레이 작업을 차단하려면 MTA는 먼저 사용자 사이트에서 전송된 내부 메일과 외부 인터넷에서 전송되어 사용자 시스템을 경유하여 다시 인터넷으로 나가는 외부 메일을 구분할 수 있어야 합니다. 내부 메일은 허용하고 외부 메일은 차단하려 합니다. 인바운드 SMTP 채널(일반적으로 tcp\_local 채널이며 기본적으로 설정됨)에서 switchchannel 키워드를 사용하여 구분할 수 있습니다.

switchchannel 키워드를 사용하여 SMTP 서버가 들어오는 SMTP 연결에 연관된 실제 IP 주소를 조사합니다. Messaging Server는 이 IP 주소와 다시 쓰기 규칙을 결합하여 도메인 내에서 보낸 SMTP와 도메인 외부로부터의 연결을 구분합니다. 그런 다음 이 정보는 내부 메일 트래픽과 외부 메일 트래픽을 분리하는 데 사용될 수 있습니다.

아래 설명된 MTA 구성은 기본적으로 서버가 내부 메일 트래픽과 외부 메일 트래픽을 구분할 수 있도록 설정됩니다.

- 구성 파일에서 로컬 채널 바로 앞에 `noswitchchannel` 키워드가 지정된 `defaults` 채널이 옵니다.

```
! final rewrite rules
defaults noswitchchannel
! Local store
ims-ms ...
```

- 받는 TCP/IP 채널은 `switchchannel`과 `remotehost` 키워드를 지정하며, 예를 들면 다음과 같습니다.

```
tcp_local smtp single_sys mx switchchannel remotehost
TCP-DAEMON
```

- 받는 TCP/IP 채널 정의 뒷부분은 이름은 다르지만 비슷한 채널입니다. 예를 들면 다음과 같습니다.

```
tcp_intranet smtp single_sys mx allowswitchchannel routelocal
tcp_intranet-daemon
```

`routelocal` 채널 키워드는 채널에 주소를 다시 쓸 때 MTA가 해당 주소의 모든 명시적 라우팅을 이 채널을 통해 "단락화"하도록 하여 명시적으로 소스 라우팅된 주소를 통해 내부 SMTP 호스트를 거친 루핑 방식으로 릴레이 시도를 차단합니다.

위 구성 설정으로 도메인 내에서 생성된 SMTP 메일은 `tcp_intranet` 채널을 통해 들어옵니다. 다른 모든 SMTP 메일은 `tcp_local` 채널을 통해 들어옵니다. 이렇게 해당 메일이 들어오는 채널을 기준으로 내부 메일과 외부 메일이 구분됩니다.

이 작업의 작동 방식에 대해 알아보겠습니다. 여기서 핵심은 `switchchannel` 키워드이며, `tcp_local` 채널에 적용됩니다. 서버는 메일이 SMTP 서버에 들어오면 키워드를 통해 받는 연결과 연관된 소스 IP 주소를 검사합니다. 서버는 받는 연결의 리터럴 IP 주소에 대해 역방향 지정 봉투 다시 쓰기를 시도하여 연관된 채널을 찾습니다. 소스 IP 주소가 `INTERNAL_IP` 매핑 테이블 내의 IP 주소나 서브넷과 일치하는 경우 해당 매핑 테이블을 호출하는 다시 쓰기 규칙을 통해 해당 주소가 `tcp_intranet` 채널로 다시 쓰여집니다.

`tcp_intranet` 채널은 `allowswitchchannel` 키워드로 표시되기 때문에 메일은 `tcp_intranet` 채널로 전환되어 해당 채널로 들어갑니다. 메일이 `INTERNAL_IP` 매핑 테이블에 없는 IP 주소의 시스템에서 들어오는 경우 역방향 지정 봉투 다시 쓰기로 `tcp_local` 또는 다른 채널로 다시 씁니다.

하지만 `tcp_intranet` 채널로는 다시 쓰지 않으며 다른 모든 채널은 기본적으로 `noswitchchannel`로 표시되어 있으므로 메일은 다른 채널로 전환되지 않고 `tcp_local` 채널로 남아 있게 됩니다.

---

**주**            "`tcp_local`" 문자열을 사용하는 모든 매핑 테이블이나 변환 파일 항목은 사용법에 따라 `tcp_*` 또는 "`tcp_intranet`"으로 변경해야 할 수 있습니다.

---

## 인증된 사용자의 메일 구분

사이트에는 물리적 네트워크의 일부가 아닌 "로컬" 클라이언트 사용자가 있을 수 있습니다. 이러한 사용자가 메일을 전송하면 외부 IP 주소(예: 임의의 인터넷 서비스 제공자)로부터 메일이 전송됩니다. 사용자가 SASL 인증을 수행할 수 있는 메일 클라이언트를 사용하는 경우 이러한 인증된 연결을 다른 외부 연결과 구분할 수 있습니다. 따라서 인증되지 않은 릴레이 전송 시도는 거부되는 반면 인증된 전송은 허용됩니다. 인바운드 SMTP 채널(일반적으로 `tcp_local` 채널)에 `saslswitchchannel` 키워드를 사용하여 인증된 연결과 인증되지 않은 연결을 구분할 수 있습니다.

`saslswitchchannel` 키워드는 전환할 채널을 지정하는 인수를 취합니다. SMTP 보낸 사람이 인증에 성공하면 해당 전송 메일은 지정된 전환 대상 채널에서 오는 것으로 간주됩니다.

추가적으로 인증된 전송을 구분하려면 다음을 수행합니다.

1. 구성 파일에 고유 이름을 가진 새 TCP/IP 채널 정의를 추가합니다. 예를 들면 다음과 같습니다.

```
tcp_auth smtp single_sys mx mustsaslsrv noswitchchannel
TCP-INTERNAL
```

이 채널은 정규 채널 전환을 허용하지 않아야 합니다(즉, 이전 기본 행에서 명시적 또는 암시적으로 `noswitchchannel`이 있어야 함). 이 채널에는 `mustsaslsrv`가 있어야 합니다.

2. 다음 예에 표시된 대로 `maysaslsrv` 및 `saslswitchchannel tcp_auth`를 추가하여 `tcp_local` 채널을 수정합니다.

```
tcp_local smtp mx single_sys maysaslsrv saslswitchchannel tcp_auth \
switchchannel
|TCP-DAEMON
```

이 구성을 사용하면 로컬 비밀번호로 인증할 수 있는 사용자가 보낸 SMTP 메일이 tcp\_auth 채널에 들어갈 수 있습니다. 내부 호스트에서 보낸 인증되지 않은 SMTP 메일은 여전히 tcp\_internal 채널로 들어옵니다. 다른 모든 SMTP 메일은 tcp\_local로 들어옵니다.

## 메일 릴레이 금지

이 예에서는 인증되지 않은 사용자가 시스템을 통해 SMTP 메일을 릴레이하지 못하도록 하는 것을 설명합니다. 우선 로컬 사용자는 SMTP 메일을 릴레이할 수 있어야 합니다. 예를 들어, POP 및 IMAP 사용자는 Messaging Server를 사용하여 메일을 보냅니다. 로컬 사용자는 물리적으로 메일이 내부 IP 주소에서 들어오는 로컬이거나, 물리적으로는 원격이지만 로컬 사용자로 인증이 가능한 사용자일 수 있습니다.

인터넷 상에 있는 임의의 사용자가 해당 서버를 릴레이로 사용하지 못하게 하려 합니다. 다음 절에서 설명하는 구성을 사용하면 이러한 사용자 클래스를 구분하고 올바른 클래스를 차단할 수 있습니다. 특히 tcp\_local 채널을 통해 들어오고 같은 채널을 통해 나가는 메일을 차단하려 합니다. 이를 위해 ORIG\_SEND\_ACCESS 매핑 테이블이 사용됩니다.

ORIG\_SEND\_ACCESS 매핑 테이블을 사용하여 소스 채널과 대상 채널을 기반으로 트래픽을 차단할 수 있습니다. 이 경우 tcp\_local 채널을 통해 송수신되는 트래픽을 차단해야 합니다. 이 기능은 다음 ORIG\_SEND\_ACCESS 매핑 테이블로 구현됩니다.

ORIG\_SEND\_ACCESS

```
tcp_local|*|tcp_local|*          $NRelaying$ not$ permitted
```

이 예에서 해당 항목은 메일이 tcp\_local 채널에 들어가서 바로 해당 채널로 다시 나올 수 없도록 지정합니다. 즉, 이 항목은 외부 메일이 SMTP 서버로 들어와서 곧바로 인터넷으로 릴레이되는 것을 방지합니다.

ims-ms 채널과 일치하는 주소(하지만 별칭이나 메일 목록 정의를 통해 다시 외부 주소로 확장될 수 있는 주소)를 차단할 수 있도록 SEND\_ACCESS 매핑 테이블 대신 ORIG\_SEND\_ACCESS 매핑 테이블이 사용됩니다. SEND\_ACCESS 매핑 테이블을 사용할 때는 외부 사용자가 다시 외부 사용자로 확장되는 메일 목록을 보내거나 메일을 다시 외부 주소로 전달하는 사용자에게 보낼 수 있도록 하려면 길이를 늘려야 합니다.

## SMTP 릴레이 차단에 RBL 검사를 포함한 DNS 조회 사용

Messaging Server에는 유효한 DNS 이름을 가진 주소에서 전송된 메일만 전달되도록 하는 여러 방법이 있습니다. 가장 간단한 방법은 tcp\_local 채널에 mailfromdnsverify 채널 키워드를 지정하는 것입니다.

Messaging Server는 ORIG\_MAIL\_ACCESS에서 다음 규칙을 사용하여 유효한 DNS 이름을 가진 주소에서 전송된 메일만 전달되도록 하는 dns\_verify 프로그램도 제공합니다.

```
ORIG_MAIL_ACCESS

TCP|*|*|*|*|SMTP|MAIL|*|*|*|*|* \
$msg_svr_base/lib/dns_verify.so, \
dns_verify,$6|$$y|$$NInvalid$ host:$ $$6$ -$ %e]
```

위 예에서 줄 바꿈은 이러한 매핑 항목에서 구문적으로 매우 중요합니다. 다음 행으로 진행하려면 백슬래시 문자를 사용해야 합니다.

또한 dns\_verify 이미지를 사용하여 받는 연결을 RBL(Realtime Blackhole List), MAPS(Mail Abuse Prevention System, DUL(Dial-up User List) 또는 ORBS(Open Relay Behavior-modification System) 목록 등에 대해 검사하여 UBE로부터 보호할 수 있습니다. 새 mailfromdnsverify 키워드와 마찬가지로 dns\_verify 콜아웃을 수행하는 대신 "보다 간단한 구성" 방법으로 이러한 검사를 수행할 수도 있습니다. 보다 간단한 방법은 dispatcher.cnf 파일에 DNS\_VERIFY\_DOMAIN 옵션을 사용하는 것입니다. 예를 들어, [SERVICE=SMTP] 섹션에서 검사하려는 다양한 목록에 대한 옵션의 인스턴스를 설정합니다.

```
[SERVICE=SMTP]
PORT=25
! ...rest of normal options...
DNS_VERIFY_DOMAIN=rbl.maps.vix.com
DNS_VERIFY_DOMAIN=dul.maps.vix.com
!...etc...
```

이 경우 메일은 SMTP 수준에서 거부됩니다. 즉 메일은 SMTP 대화 도중 거부되므로 MTA로 전송되지 않습니다. 이 방법의 단점은 내부 사용자가 보낸 메일을 포함하여 모든 받는 SMTP 메일을 검사한다는 것입니다. 따라서 효율성이 떨어지며 인터넷 연결이 끊기 되면 문제가 발생할 수 있습니다. 그 대안은 PORT\_ACCESS 매핑 테이블 또는 ORIG\_MAIL\_ACCESS 매핑 테이블로부터 dns\_verify를 호출하는 것입니다. PORT\_ACCESS 매핑 테이블에는 로컬 내부 IP 주소나 메일 전송자를 검사하지 않는 초기 항목과 다른

모든 사용자에게 대해 원하는 검사를 수행하는 후기 항목을 지정할 수 있습니다. 또는 ORIG\_MAIL\_ACCESS 매핑 테이블에서 `tcp_local` 채널로 받는 메일에만 검사를 적용하려는 경우에는 내부 시스템/클라이언트로부터 받는 메일에 대해 해당 검사를 건너뛸 수 있습니다. `dns_verify`를 가리키는 항목을 사용하는 예는 다음과 같습니다.

PORT\_ACCESS

```
! Allow internal connections in unconditionally
*|*|*|*|* $C$|INTERNAL_IP;$3|$Y$E
! Check other connections against RBL list
TCP|*|25|*|* \
$C${msg_svr_base}/lib/dns_verify.so, \
dns_verify_domain_port,$1,rbl.maps.vix.com.]EXTERNAL$E
```

ORIG\_MAIL\_ACCESS

```
TCP|*|25|*|*|SMTP|*|tcp_local|*@*|*|* \
$C${msg_svr_base}/lib/dns_verify.so, \
dns_verify_domain,$1,rbl.maps.vix.com.]$E
```

## DNS 기반 데이터베이스 지원

`dns_verify` 프로그램은 원치 않는 대량 전자 메일을 보낼 수 있는 받는 SMTP 연결을 확인하는 데 사용되는 DNS 기반 데이터베이스를 지원합니다. 공개적으로 사용 가능한 DNS 데이터베이스 중 일부는 일반적으로 이러한 용도로 사용되는 TXT 레코드를 포함하지 않을 수 있습니다. 대신 A 레코드만 포함합니다.

일반 설정에서 특정 IP 주소에 대한 DNS의 TXT 레코드에는 메일을 거부할 때 SMTP 클라이언트로 반환하기에 적합한 오류 메시지가 포함되어 있습니다. 하지만 TXT 레코드가 없고 A 레코드가 있는 경우 Messaging Server 5.2 이전의 `dns_verify` 버전에서는 "No error text available"이라는 메시지를 반환했습니다.

이제 `dns_verify`에서는 사용 가능한 TXT 레코드가 없는 경우에 사용되는 기본 텍스트를 지정하는 옵션을 제공합니다. 예를 들어, 다음 PORT\_ACCESS 매핑 테이블에서는 이 옵션을 사용하는 방법을 보여 줍니다.

PORT\_ACCESS

```
*|*|*|*|* $C$|INTERNAL_IP;$3|$Y$E \
TCP|*|25|*|* \
```



```
$C$[<msg_svr_base/lib/dns_verify.so \
,dns_verify_domain_port,$1,dnsblock.siroe.com,Your$ host$ ($1)$ \
found$ on$ dnsblock$ list]$E
* $YEXTERNAL
```

이 예에서 원격 시스템이 dnsblock.siroe.com 도메인의 쿼리에 있지만 TXT 레코드를 사용할 수 없는 경우에는 "Your host a.b.c.d found on dnsblock list" 메시지가 반환됩니다.

## 많은 수의 액세스 항목 처리

매핑 테이블에서 많은 수의 항목을 사용하는 사이트는 특정 조회에 대해 일반 데이터베이스를 호출하는 몇 개의 일반적인 와일드카드 항목이 매핑 테이블에 포함되도록 구성해야 합니다. 매핑 테이블에 많은 수의 항목이 직접 존재하는 것보다 특정 조회에 대해 일반 데이터베이스를 호출하는 매핑 테이블 항목이 몇 개 있는 것이 더 효율적입니다.

특별한 경우 인터넷 전자 메일을 보내고 받을 수 있는 사용자별로 제어하려는 사이트가 있을 수 있습니다. 이러한 제어는 ORIG\_SEND\_ACCESS 등의 액세스 매핑 테이블을 사용하여 편리하게 구현될 수 있습니다. 이 때 대량의 특정 정보(예: 특정 주소)를 일반 데이터베이스에 저장하고 매핑 테이블 항목을 일반 데이터베이스로 적절하게 호출할 수 있도록 하면 효율성과 성능이 크게 향상될 수 있습니다.

예를 들어, 다음 ORIG\_SEND\_ACCESS 매핑 테이블을 살펴보십시오.

```
ORIG_SEND_ACCESS

! Users allowed to send to Internet
!
*|adam@siroe.com|tcp_local|*   $Y
*|betty@siroe.com|tcp_local|*   $Y
!...etc...
!
! Users not allowed to send to Internet
!
*|norman@siroe.com|tcp_local|*   $NInternet$ access$ not$ permitted
*|opal@siroe.com|tcp_local|*     $NInternet$ access$ not$ permitted
!...etc...
!
! Users allowed to receive from the Internet
!
tcp_*|*|*|adam@siroe.com        $Y
tcp_*|*|*|betty@siroe.com        $Y
!...etc...
!
! Users not allowed to receive from the Internet
!
tcp_*|*|*|norman@siroe.com       $NInternet$ e-mail$ not$ accepted
tcp_*|*|*|opal@siroe.com         $NInternet$ e-mail$ not$ accepted
!...etc...
```

테이블에 각 사용자가 개별적으로 입력된 매핑 테이블을 사용하는 것보다 더 효율적인 설정(수만 명의 사용자 항목이 있는 경우 특히 더 효율적임)이 아래 예에 나와 있습니다. 이 예에서는 일반 데이터베이스의 샘플 소스 텍스트 파일과 샘플 ORIG\_SEND\_ACCESS 매핑 테이블을 볼 수 있습니다. 이 소스 파일을 데이터베이스 형식으로 컴파일하려면 `imsimta crdb` 명령을 실행합니다.

```
% imsimta crdb input-file-spec output-database-spec
```

imsimta crdb 유틸리티에 대한 자세한 내용은 *Sun Java System Messaging Server Administration Reference*를 참조하십시오.

```

DATABASE ENTRIES

SEND|adam@domain.com    $Y
SEND|betty@domain.com   $Y
!...etc...
SEND|norman@domain.com  $NInternet$ access$ not$ permitted
SEND|opal@domain.com    $NInternet$ access$ not$ permitted
!...etc...
RECV|adam@domain.com    $Y
RECV|betty@domain.com   $Y
!...etc...
RECV|norman@domain.com  $NInternet$ e-mail$ not$ accepted
RECV|opal@domain.com    $NInternet$ e-mail$ not$ accepted

MAPPING TABLE

ORIG_SEND_ACCESS

! Check if may send to Internet
!
! *|*|*|tcp_local      $C${SEND|$1}$E
!
! Check if may receive from Internet
!
! tcp_*|*|*|*          $C${RECV|$3}$E
    
```

이 예에서 일반 데이터베이스 왼쪽에(그리고 이에 따라 매핑 테이블에 의해 생성된 일반 데이터베이스 검사에) 임의 문자열 SEND| 및 RECV|를 사용하면 두 가지 종류의 검사를 구분할 수 있습니다. 표시된 대로 일반 데이터베이스 검사 앞뒤에 \$C와 \$E 플래그를 붙이는 것은 일반 데이터베이스에 대한 일반적인 매핑 테이블 호출입니다.

위의 예에서는 일반 데이터베이스 항목에 대한 간단한 매핑 테이블 검사를 보여 줍니다. 보다 복잡한 검사를 수행하는 매핑 테이블도 일반 테이블을 사용하여 효율성을 높일 수 있습니다.

## 2부. 메일함 필터

메일함 필터(Sieve 필터라고도 함)는 메일 헤더에 지정된 문자열을 포함한 메일을 필터링하고 이러한 메일 메시지에 지정한 작업을 적용합니다. 관리자는 채널이나 MTA를 통해 사용자에게 가는 메일 스트림을 필터링합니다. Messaging Server 필터는 서버에 저장되며 서버에 의해 평가됩니다. 따라서 이를 서버측 규칙(SSR)이라고도 합니다.

이 부분은 다음 내용으로 구성되어 있습니다.

- 541페이지의 "Sieve 필터링 개요"
- 542페이지의 "사용자 수준 필터 만들기"
- 542페이지의 "채널 수준 필터 만들기"
- 544페이지의 "MTA 차원 필터 만들기"
- 545페이지의 "사용자 수준 필터 디버그"

## Sieve 필터 지원

Messaging Server 필터는 Sieve 필터링 언어(Draft 9 of the Sieve Internet Draft)를 기반으로 합니다. Sieve 구문과 의미에 대한 자세한 내용은 RFC3028을 참조하십시오. 또한, Messaging Server는 다음의 Sieve 확장도 지원합니다.

- **jettison.** 메일을 자동으로 삭제된다는 점에서는 discard와 비슷하지만, 암시적 보관을 취소할 뿐 다른 작업을 수행하지 않는 discard와 달리 jettison은 discard가 수행되도록 강제 설정합니다. 이러한 동작상의 차이는 여러 Sieve 필터가 포함된 경우에만 중요합니다. 예를 들어 시스템 수준 discard는 명시적으로 keep을 지정한 사용자 Sieve 필터에 의해 대체될 수 있지만 시스템 수준 jettison은 사용자 Sieve에서 수행한 모든 것을 대체합니다.
- **가장 Sieve 필터** 한 사용자가 다른 사용자에 대해 Sieve 필터를 지정할 수 있는 방법을 제공합니다. 이 LDAP 옵션에서 제어하는 사용자 항목에 두 가지 LDAP 속성을 사용합니다.
  - LDAP\_PARENTAL\_CONTROLS - Yes 또는 No라는 문자열 값을 포함하는 속성을 지정합니다. Yes는 가장 Sieve가 이 항목에 적용됨을 의미하고 No는 그러한 Sieve가 적용되지 않음을 의미합니다. 기본값은 없습니다.
  - LDAP\_FILTER\_REFERENCE - 가장 Sieve를 찾을 수 있는 디렉토리 항목을 가리키는 DN을 포함한 속성을 지정합니다. 기본값은 없습니다.

가장 Sieve가 포함되어 있는 항목에는 다음 MTA 옵션에서 지정한 두 가지 속성이 있어야 합니다.

- LDAP\_HOH\_FILTER - 가장 Sieve을 포함하는 속성을 지정합니다. 이 옵션의 기본값은 mailSieveRuleSource입니다.
- LDAP\_HOH\_OWNER - 가장 소유자 전자 메일 주소를 포함하는 속성을 지정합니다. 이 옵션의 기본값은 mail입니다.

두 속성 모두 가장 Sieve의 작동에 필요합니다.

## Sieve 필터링 개요

Sieve 필터는 메일 헤더에 있는 문자열에 따라 메일에 적용되는 하나 이상의 조건적 작업으로 구성됩니다. 관리자는 채널 수준 필터와 MTA 차원 필터를 만들어서 원하지 않는 메일의 전달을 방지할 수 있습니다. 사용자는 Messenger Express를 사용하여 자신의 메일함에 사용자별 필터를 만들 수 있습니다. 구체적인 지침은 Messenger Express 온라인 도움말을 참조하십시오.

서버는 다음 우선 순위에 따라 필터를 적용합니다.

### 1. 사용자 수준 필터

개인 메일함이 메일을 명시적으로 수락하거나 거부하면 해당 메일에 대한 필터 처리가 종료됩니다. 하지만 수신자에게 메일함 필터가 없거나 사용자의 메일함 필터가 해당 메일에 명시적으로 적용되지 않는 경우에는 Messaging Server가 채널 수준 필터를 적용합니다. 사용자별 필터가 설정됩니다.

### 2. 채널 수준 필터

채널 수준 필터가 메일을 명시적으로 수락하거나 거부하면 해당 메일에 대한 필터 처리가 종료됩니다. 그렇지 않으면 Messaging Server가 MTA 차원 필터(있는 경우)를 적용합니다.

### 3. MTA 차원 필터

기본적으로 각 사용자에게는 메일함 필터가 없습니다. 사용자가 Messenger Express 인터페이스를 사용하여 하나 이상의 필터를 만들면 해당 필터가 디렉토리에 저장되어 디렉토리 동기화 프로세스 도중 MTA에 의해 검색됩니다.

## 사용자 수준 필터 만들기

사용자별 메일 필터는 특정 사용자의 메일함을 대상으로 하는 메일에 적용됩니다. 사용자별 메일 필터는 Messenger Express를 통해서만 만들 수 있습니다.

## 채널 수준 필터 만들기

채널 수준 필터는 채널에 대기된 각 메일에 적용됩니다. 이러한 필터의 일반적 용도는 특정 채널을 통과하는 메일을 차단하는 것입니다.

채널 수준 필터를 만들려면 다음을 수행합니다.

1. Sieve를 사용하여 필터를 작성합니다.
2. 필터를 다음 디렉토리에 있는 파일에 저장합니다.

```
../config/file.filter
```

The file must be world readable and owned by the MTA's uid.

3. 채널 구성에 다음을 포함합니다.

```
destinationfilter file:IMTA_TABLE:file.filter
```

4. 구성을 다시 컴파일하고 디스패처를 다시 시작합니다.

필터 파일의 변경 내용은 다시 컴파일하거나 디스패처를 다시 시작하지 않아도 적용됩니다.

`destinationfilter` 채널 키워드를 통해 해당 채널의 대기열에 포함된 메일에 대한 메일 필터링을 사용할 수 있습니다. `sourcefilter` 채널 키워드를 통해 채널에 의해(로부터) 대기된 메일에 대한 메일 필터링을 사용할 수 있습니다. 이러한 키워드에는 채널과 연관된 해당 채널 필터 파일에 대한 경로를 지정하는 하나의 필수 매개 변수가 있습니다.

`destinationfilter` 채널 키워드 구문은 다음과 같습니다.

```
destinationfilter URL-pattern
```

`sourcefilter` 채널 키워드 구문은 다음과 같습니다.

```
sourcefilter URL-pattern
```

여기서 *URL-pattern*은 해당 채널에 대한 필터의 경로를 지정하는 URL입니다. 다음 예에서 *channel-name*은 채널의 이름입니다.

```
destinationfilter file:///usr/tmp/filters/channel-name.filter
```

filter 채널 키워드를 통해 해당 채널에 대한 메일 필터링을 사용할 수 있습니다. 키워드에는 채널을 통해 메일을 받는 각 봉투 수신자와 연관된 필터 파일의 경로를 지정하는 하나의 필수 매개 변수가 있습니다.

filter 채널 키워드의 구문은 다음과 같습니다.

filter *URL-pattern*

*URL-pattern*은 특별한 대체 시퀀스를 처리한 후 경로를 특정 수신 주소에 대한 필터 파일로 지정하는 URL입니다. *URL-pattern*은 특별 대체 시퀀스 발생 시 이를 포함할 수 있으며, 이 시퀀스는 수신 주소(해당 local-part@host.domain)에서 추출된 문자열로 대체될 수 있습니다. 이러한 대체 시퀀스는 [543페이지의 표 17-4](#)에 나와 있습니다.

fileinto 키워드는 메일함 필터 fileinto 연산자가 적용되었을 때 주소를 변경하는 방법을 지정합니다. 다음 예에서는 폴더 이름이 다음과 같이 원래 있던 하위 주소를 대체하면서 원래 주소의 하위 주소로 삽입되어야 한다는 것을 지정합니다.

```
fileinto $U+$S@$D
```

**표 17-4** filter 채널 키워드 *URL 패턴* 대체 태그(대소문자 무시)

| 태그    | 의미                                                                       |
|-------|--------------------------------------------------------------------------|
| *     | 그룹 확장을 수행합니다.                                                            |
| **    | 속성 mailForwardingAddress를 확장합니다. 여러 전달 주소를 생성할 수 있는 값이 여러 개인 속성일 수 있습니다. |
| \$\$  | \$ 문자 대체입니다.                                                             |
| \$\$\ | 후속 텍스트를 소문자로 바꿉니다.                                                       |
| \$\$^ | 후속 텍스트를 대문자로 바꿉니다.                                                       |
| \$_   | 후속 텍스트에 대해 대소문자 변환을 수행하지 않습니다.                                           |
| \$~   | 주소의 로컬 부분과 연관된 홈 디렉토리에 대한 파일 경로를 대체합니다.                                  |
| \$1S  | \$\$와 비슷하지만 하위 주소를 사용할 수 없는 경우 아무 것도 삽입하지 않습니다.                          |
| \$2S  | \$\$와 비슷하지만 하위 주소를 사용할 수 없는 경우 아무 것도 삽입하지 않으며 선행 문자를 삭제합니다.              |
| \$3S  | \$\$와 비슷하지만 하위 주소를 사용할 수 없는 경우 아무 것도 삽입하지 않으며 후행 문자를 무시합니다.              |
| \$A   | 주소 local-part@host.domain을 대체합니다.                                        |
| \$D   | host.domain을 대체합니다.                                                      |
| \$E   | 두 번째 예비 속성 값, LDAP_SPARE_1을 삽입합니다.                                       |

**표 17-4** filter 채널 키워드 URL 패턴 대체 태그(대소문자 무시)

| 태그   | 의미                                                                                                                                                   |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------|
| \$F  | 전달 파일의 이름(mailDeliveryFileURL 속성)을 삽입합니다.                                                                                                            |
| \$G  | 두 번째 예비 속성 값, LDAP_SPARE_2를 삽입합니다.                                                                                                                   |
| \$H  | 호스트를 대체합니다.                                                                                                                                          |
| \$I  | 호스트된 도메인(domainUidSeparator에 의해 지정된 구분자의 오른쪽에 있는 UID 일부)을 삽입합니다. 호스트된 도메인을 사용할 수 없는 경우 실패합니다.                                                        |
| \$I1 | \$I와 비슷하지만 호스트된 도메인을 사용할 수 없는 경우 아무 것도 삽입하지 않습니다.                                                                                                    |
| \$I2 | \$I와 비슷하지만 호스트된 도메인을 사용할 수 없는 경우 아무 것도 삽입하지 않고 선행 문자를 삭제합니다.                                                                                         |
| \$I3 | \$I와 비슷하지만 호스트된 도메인을 사용할 수 없는 경우 아무 것도 삽입하지 않고 후행 문자를 무시합니다.                                                                                         |
| \$L  | 로컬 부분을 대체합니다.                                                                                                                                        |
| \$M  | 호스트된 도메인을 제거하고 UID를 삽입합니다.                                                                                                                           |
| \$P  | 메소드 이름(mailProgramDeliveryInfo 속성)을 삽입합니다.                                                                                                           |
| \$S  | 현재 주소와 연관된 하위 주소를 삽입합니다. 하위 주소는 하위 주소 구분자 뒤에 있는 원래 주소의 일부 사용자 부분입니다. 여기서 구분자는 일반적으로 +이지만 MTA 옵션 SUBADDRESS_CHAR으로 지정할 수 있습니다. 하위 주소를 지정하지 않으면 실패합니다. |
| \$U  | 현재 주소의 메일함 부분을 삽입합니다. 이것은 @ 기호 왼쪽에 있는 주소 전체이거나 하위 주소 구분자 + 앞에 있는 주소의 왼쪽 부분입니다.                                                                       |

## MTA 차원 필터 만들기

MTA 차원 필터는 MTA에 대해 대기된 모든 메일에 적용됩니다. 이 필터의 일반적 용도는 메일의 대상에 관계 없이 원하지 않는 대량 전자 메일이나 기타 원하지 않는 메일을 차단하는 것입니다. MTA 필터를 만들려면 다음을 수행합니다.

1. Sieve를 사용하여 필터를 작성합니다.
2. 다음 파일에 해당 필터를 저장합니다.

```
../imta/config/imta.filter
```

이 필터는 모두가 읽을 수 있어야 하며 이 파일이 있으면 자동으로 사용됩니다.

3. 구성을 다시 컴파일하고 디스패처를 다시 시작합니다.

컴파일된 구성을 사용하면 MTA 차원 필터 파일은 컴파일된 구성에 통합됩니다.



## 제거된 메일을 FILTER\_DISCARD 채널 외부로 라우팅

기본적으로 메일함 필터를 통해 제거된 메일은 즉시 시스템에서 제거(삭제)됩니다. 하지만 사용자가 처음 메일함 필터를 설정할 때나(또는 실수로) 디버깅을 위해 삭제 작업이 일정 시간 동안 지연되도록 할 수 있습니다.

메일함 필터에 의해 제거된 메일을 시스템에 일시 보관한 후 나중에 삭제하려면 먼저 다음 예에 표시된 대로 삭제할 때까지 메일을 보관할 기간(일반적으로 일 수)을 지정하는 notices 채널 키워드와 함께 filter\_discard 채널을 MTA 구성에 추가합니다.

```
filter_discard notices 7
FILTER-DISCARD
```

그런 다음 MTA 옵션 파일에서 FILTER\_DISCARD=2 옵션을 설정합니다. filter\_discard 대기열에 있는 메일은 사용자의 개인 휴지통 폴더의 확장된 범위에 들어 있는 것으로 간주해야 합니다. 따라서 filter\_discard 대기열에 있는 메일에 대한 경고 메일은 보내지지 않으며 바운스 또는 반환 요청 시에도 해당 보낸 사람에게 반환되지 않습니다. 이러한 메일에 대해 수행 가능한 유일한 작업은 최종 알림 값이 만료되거나 imsimta return 등의 유틸리티를 사용하여 수동 바운스가 요청된 경우 해당 메일을 영구적으로 삭제하는 것입니다.

Messaging Server 6 2004Q2 이전에는 jettison Sieve 작업에서 filter\_discard 채널 사용을 FILTER\_DISCARD MTA 옵션으로 제어했습니다. 이제는 FILTER\_DISCARD 설정에서 기본값을 가져오는 FILTER\_JETTISON 옵션으로 제어합니다. FILTER\_DISCARD의 기본값은 1입니다(discard를 bitbucket 채널로 전달).

## 사용자 수준 필터 디버그

사용자가 Sieve 필터가 제대로 작동하지 않는다고 불평할 경우 여러 단계를 수행하여 필터를 디버깅할 수 있습니다. 여기에서 이러한 단계에 대해 설명합니다.

1. fileinto 필터링이 작동하려면 imta.cnf 파일에서 ims-ms 채널이 다음과 같이 표시되어 있어야 합니다.

```
fileinto $u+$s@$d
```

2. 사용자의 LDAP 항목에서 사용자 수준 필터를 가져옵니다.

사용자 수준 필터는 MailSieveRuleSource 속성 아래의 LDAP 항목에 저장됩니다. ldapsearch 명령을 사용하여 검색하려는 경우 이러한 필터가 base64 인코딩되어 있으므로 -Bo 스위치를 사용하여 출력을 디코딩해야 합니다.

```
./ldapsearch -D "cn=directory manager" -w password -b
"o=alcatraz.sesta.com,o=isp" -Bo uid=test
```

또한 아래 설명된 imsimta test -rewrite 명령을 사용하면 디코딩이 자동으로 수행됩니다.

3. 사용자 필터가 MTA에 표시되는지 확인합니다.

다음 명령을 실행합니다.

```
# imsimta test -rewrite -filter -debug user@sesta.com
```

이렇게 하면 앞 단계에서 검색한 사용자의 sieve 필터가 출력되어야 합니다. 필터가 표시되지 않으면 LDAP 항목이 필터를 반환하지 않는 이유를 찾아야 합니다.

imsimta test -rewrite 출력에 필터가 표시되면 MTA가 사용자의 필터를 인식하는 것입니다. 다음 단계에서는 imsimta test -expression 명령을 사용하여 필터 해석을 테스트합니다.

4. imsimta test -exp를 사용하여 사용자 필터를 디버깅합니다. 다음 정보가 필요합니다.
  - a. mailSieveRuleSource 속성에 있는 사용자의 Sieve 언어 문. 위 단계를 참조하십시오.
  - b. 필터를 트리거한 것으로 여겨지는 rfc2822 메일
  - c. 필터가 메일에 대해 수행할 것으로 예상되는 작업에 대한 설명
5. 사용자의 mailSieveRuleSource: values를 기반으로 Sieve 언어 문을 포함하는 텍스트 파일(예: temp.filter)을 만듭니다. 예를 들면 다음과 같습니다.

```
require "fileinto";
if anyof(header :contains
["To", "Cc", "Bcc", "Resent-to", "Resent-cc",
"Resent-bcc"] "commsqa"){
fileinto "QMSG";
}
```

예상 결과: commsqa가 이 메일의 수신자일 경우 메일을 QMSG라는 폴더에 정리합니다.

6. 사용자가 제공한 rfc2822 메일 파일의 내용을 포함하는 test.msg라는 텍스트 파일을 만듭니다.

사용자 메시지 저장소 영역의 .msg 파일을 사용하거나 사용자가 제공한 rfc2822 메일 파일의 내용을 포함하는 test\_rfc2822.msg라는 텍스트 파일을 만들 수 있습니다.

7. `imsimta test -exp` 명령을 사용합니다.

```
# imsimta test -exp -mm -block -input=temp.filter -message=test_rfc2822.msg
```

8. 출력을 검사합니다.

`imsimta test -exp` 명령의 마지막 줄은 Sieve 해석의 결과를 표시합니다. 이 결과는 다음과 같습니다.

```
Sieve Result: []
또는 다음과 같습니다.
Sieve Result: [action]
```

여기서 *action*은 이 메일에서 Sieve 필터를 적용한 결과로 수행되는 작업입니다.

필터 기준이 일치하면 몇 가지 작업이 결과로 표시됩니다. 필터 기준이 일치하지 않으면 빈 Sieve 결과가 표시되며 Sieve 필터에 논리적 오류가 있거나 .msg 파일에 일치하는 정보가 포함되지 않은 것입니다. 다른 오류가 발생할 경우에는 Sieve 스크립트에 구문 오류가 있는 것이므로 이를 디버깅해야 합니다.

출력에 대한 자세한 내용은 547페이지의 "`imsimta test -exp` 출력"을 참조하십시오.

9. 필터 구문이 유효하고 결과가 올바른 경우 다음 단계는 `tcp_local_slave.log` 디버그 로그 파일을 검사하는 것입니다.

테스트하는 메일 파일과 전송되는 메일 파일이 다를 수 있습니다. 무엇이 수신되는지 확인하는 방법은 `tcp_local_slave.log` 파일을 검사하는 것입니다. 이 로그에는 MTA로 보내는 메일과 이 메일에 필터를 적용하는 방법이 표시되어 있습니다.

`tcp_local_slave.log` 디버그 파일을 가져오는 방법은 396페이지의 "디버깅 키워드"에서 `slave_debug` 키워드를 참조하십시오.

## imsimta test -exp 출력

`imsimta test -exp`의 전체 명령은 다음과 같습니다.

```
# imsimta test -exp -mm -block -input=temp.filter -message=rfc2822.msg
```

출력 예는 다음과 같습니다.

**코드 예 17-4**                      `imsimta test -exp` 출력

```
# imsimta test -exp -mm -block -input tmp.filter -message=rfc2822.msg
Expression: if header :contains ["to"] ["pamw"]                      (1)
Expression: {
Expression: redirect "usr3@sesta.com";
Expression: keep;
Expression: }
Expression:
Expression: Dump: header:2000114;0 3 1 :contains 1 "to" 1
"pamw" if 8 ;
Dump: redirect:2000121;0 1 1 "usr3@sesta.com" ; keep:2000117;0        (2)
Dump: 0
Result: 0
Filter result: [ redirect "usr3@sesta.com" keep ]                      (3)
```

**1) Expression:** 출력 행은 `tmp.filter` 텍스트 파일에서 읽고 구문 분석될 필터를 표시합니다. 이러한 행은 스크립트를 디버깅하는 데 그다지 유용하지 않습니다.

**2) Dump:** 출력 행은 Sieve 문을 해석하는 컴퓨터의 결과입니다. 오류가 표시되지 않아야 하며 출력이 입력과 일치하는 것으로 보여야 합니다. 예를 들어, 이 덤프에서 필터 파일 `redirect "usr3@sesta.com";`의 행과 같은 단어 `redirect,usr3@sesta.com`을 표시해야 합니다.

일치하는 텍스트가 표시되지 않은 경우에는 신경을 써야 합니다. 그렇지 않은 경우에는 스크립트를 디버깅하는 데 그다지 유용하지 않습니다.

**3) 출력의 맨 아래에 Filter result:** 문이 나타납니다. 앞에서 언급한 것처럼 다음과 같은 두 가지 결과가 가능합니다.

Sieve Result: []                      또는                      Sieve Result: [*action*]

여기서 *action*은 Sieve 스크립트가 수행하는 작업입니다. 경우에 따라서는 빈 결과를 예상할 수도 있습니다. 예를 들어, `discard` 필터의 경우에는 테스트하는 모든 `.msg` 파일을 항상 삭제하지 않는지 테스트해야 합니다. 예를 들어 대괄호 사이에 작업이 있는 경우

Filter result: [ fileinto "QMSG" keep]

`rfc2822.msg` 파일의 텍스트가 필터 기준과 일치했다는 것을 의미합니다. 이 특수한 예에서 필터는 메일을 `QMSG` 폴더에 정리하고 복사본을 받은 메일함에 보관합니다. 이 경우의 결과 작업은 `fileinto` 및 `keep`입니다.

필터를 테스트할 때 두 결과 모두에 대해 여러 .msg 파일을 테스트해야 합니다. 필터와 일치하는 메일이 필터링되는지, 일치시키지 않으려는 메일이 필터링되지 않는지 항상 테스트해야 합니다.

와일드카드 일치 경우에는 :contains가 아니라 :matches 테스트를 사용해야 한다는 것에 주의합니다. 예를 들어, from=\*@sesta.com을 일치시키려면 :matches를 사용해야 합니다. 그렇지 않으면 테스트 조건을 전혀 만족하지 않으므로 테스트가 실패합니다.

## imsimta test -exp 구문

imsimta test -exp는 지정된 RFC2822 메일에 대해 Sieve 언어 문을 테스트하고 필터 결과를 표준 출력으로 보냅니다.

구문은 다음과 같습니다.

```
imsimta test -exp -mm -block -input=Sieve_language_scriptfile
-message=rfc2822_message_file
```

여기서

-block은 전체 입력을 단일 Sieve 스크립트로 처리합니다. 기본값은 각 행을 별개의 스크립트로 처리하고 별개로 평가하는 것입니다. Sieve는 파일의 끝에 도달한 경우에만 평가됩니다.

-input=Sieve\_file은 Sieve 스크립트를 포함하는 파일입니다. 기본값은 stdin에서 테스트 스크립트 행이나 스크립트 블록을 읽는 것입니다.

-message=message\_file은 Sieve 스크립트를 테스트할 RFC 2822 메일을 포함하는 텍스트 파일입니다. 이 파일은 반드시 RFC 2822 메일이어야 하며 대기열 파일이 될 수 없습니다 (zz\*.00 파일이 아님).

이 명령은 활성화될 경우 스크립트 정보를 읽어 테스트 메일의 컨텍스트에서 평가한 다음 결과를 기록합니다. 결과에는 스크립트의 최종 문을 평가한 결과뿐만 아니라 수행되는 작업도 표시됩니다.

유용한 추가 한정자는 다음과 같습니다.

-from=address는 봉투 테스트에 사용할 봉투의 from: 주소를 지정합니다. 기본값은 RETURN\_ADDRESS MTA 옵션에 지정된 값을 사용하는 것입니다.

-output=file은 결과를 file에 기록합니다. 기본값은 스크립트 평가 결과를 stdout에 기록하는 것입니다.

사용자 수준 필터 디버그

# 메시지 저장소 관리

이 장에서는 메시지 저장소와 메시지 저장소의 관리 인터페이스에 대해 설명합니다. 이 장은 다음 내용으로 구성되어 있습니다.

- 552페이지의 “개요”
- 553페이지의 “메시지 저장소 디렉토리 레이아웃”
- 556페이지의 “메시지 저장소에서 메일을 제거하는 방법”
- 557페이지의 “저장소에 대한 관리자 액세스 지정”
- 559페이지의 “공유 폴더 정보”
- 564페이지의 “공유 폴더 작업”
- 570페이지의 “메시지 저장소 할당량 정보”
- 573페이지의 “메시지 저장소 할당량 구성”
- 581페이지의 “자동 메일 제거(만료 및 제거) 기능 설정”
- 593페이지의 “메시지 저장소 분할 영역 구성”
- 597페이지의 “메시지 저장소 유지 관리 절차 수행”
- 610페이지의 “메시지 저장소 백업 및 복원”
- 624페이지의 “사용자 액세스 모니터링”
- 625페이지의 “메시지 저장소 문제 해결”

# 개요

메시지 저장소는 특정 **Messaging Server** 인스턴스에 대한 사용자 메일함을 포함합니다. 메일함, 폴더 및 로그 파일 수가 늘어나면 메시지 저장소의 크기가 늘어납니다. 메일함의 크기(디스크 할당량)를 제한하고 허용되는 총 메일 수의 한도를 지정하며 저장소의 메일에 대한 에이징 정책을 설정하여 저장소 크기를 제어할 수 있습니다.

시스템에 다른 사용자를 추가하면 디스크 저장소 요구 사항이 증가합니다. 서버가 지원하는 사용자 수에 따라 메시지 저장소는 하나 또는 여러 개의 물리적 디스크가 필요할 수 있습니다. 이러한 추가 디스크 공간을 시스템에 통합하는 방법에는 두 가지가 있습니다. 가장 쉬운 방법은 메시지 저장소 분할 영역을 추가하는 것입니다(593페이지의 [“메시지 저장소 분할 영역 구성”](#) 참조).

마찬가지로 여러 호스트된 도메인을 지원하는 경우 하나의 큰 도메인에서 서버 인스턴스를 전담하도록 할 수 있습니다. 이 구성을 사용하면 특정 도메인에 대한 저장소 관리자를 지정할 수 있습니다. 또한 다른 분할 영역을 추가하여 메시지 저장소를 확장할 수 있습니다.

메시지 저장소를 관리하기 위해 **Messaging Server**는 **Sun Java System** 콘솔 인터페이스 외에 명령줄 유틸리티 집합을 제공합니다. 표 18-1에서는 이러한 명령줄 유틸리티를 설명합니다. 이러한 유틸리티 사용에 대한 자세한 내용은 597페이지의 [“메시지 저장소 유지 관리 절차 수행”](#) 및 *Messaging Server Reference Manual*을 참조하십시오.

**표 18-1** 메시지 저장소 명령줄 유틸리티

| 유틸리티        | 설명                                                     |
|-------------|--------------------------------------------------------|
| configutil  | 저장소의 구성 매개 변수를 설정 및 수정합니다.                             |
| deliver     | 메일을 IMAP 또는 POP 메일 클라이언트가 액세스할 수 있는 메시지 저장소로 직접 전달합니다. |
| hashdir     | 특정 사용자의 메시지 저장소를 포함하는 디렉토리를 식별합니다.                     |
| imsconnutil | 메시지 저장소의 사용자 액세스를 모니터링합니다.                             |
| imexpire    | 관리자가 지정한 기준(예: 기간)에 따라 메시지 저장소에서 메일을 자동으로 제거합니다.       |
| iminitquota | LDAP 디렉토리에서 할당량 제한을 다시 초기화하고 사용 중인 디스크 공간을 다시 계산합니다.   |
| imsasm      | 사용자 메일함의 저장과 복구를 처리합니다.                                |



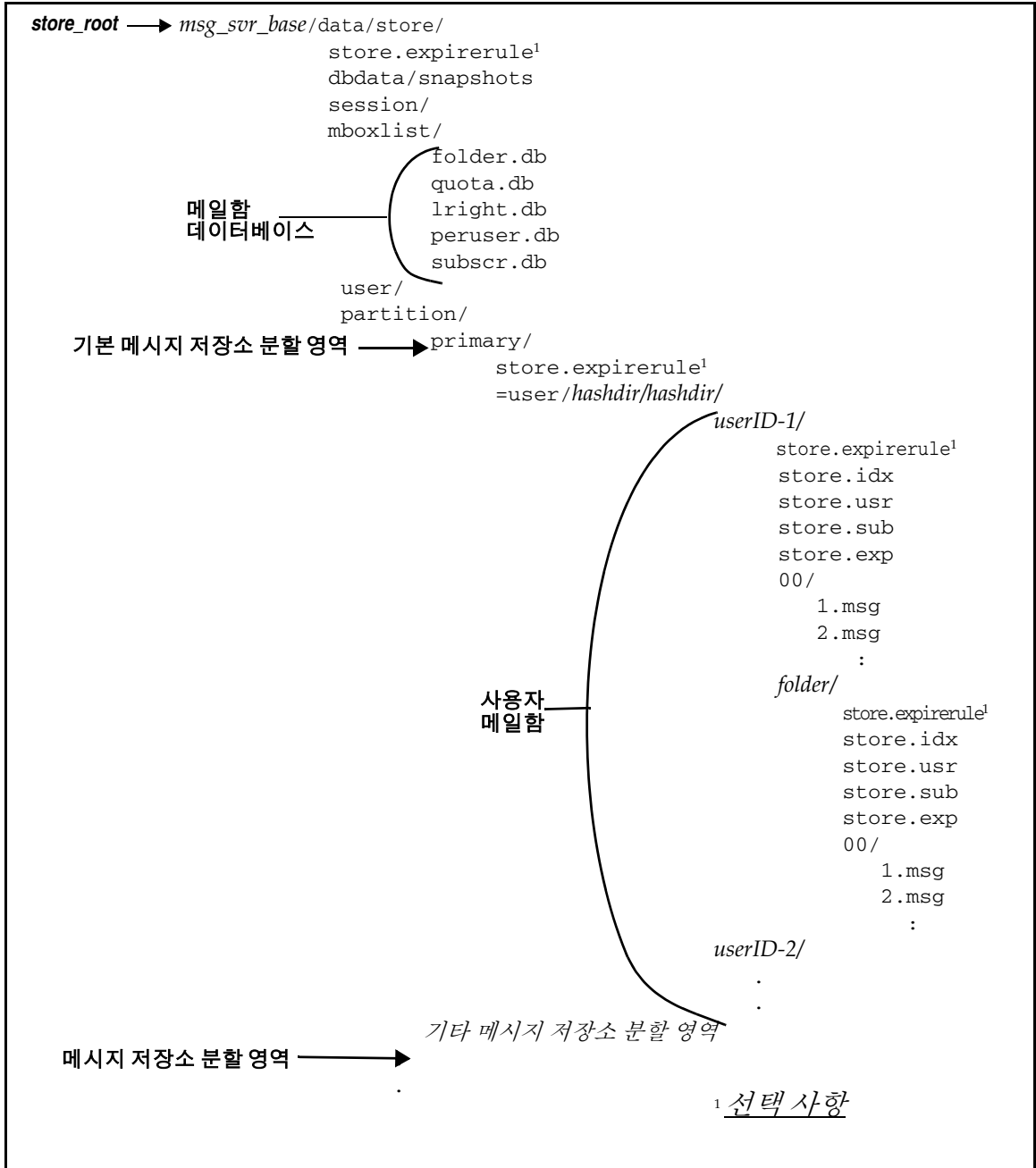
**표 18-1** 메시지 저장소 명령줄 유틸리티

| 유틸리티         | 설명                                                                                                                                                     |
|--------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| imsbackup    | 저장된 메일을 백업합니다.                                                                                                                                         |
| imsexport    | Certificate Management System 메일함을 UNIX /var/mail 형식 폴더로 내보냅니다.                                                                                        |
| imsrestore   | 백업된 메일을 복원합니다.                                                                                                                                         |
| imscripter   | IMAP 서버 프로토콜 스크립트 도구입니다. 명령이나 명령 시퀀스를 실행합니다.                                                                                                           |
| mboxutil     | 메일함을 나열, 작성, 삭제, 이름 변경 또는 이동을 수행하고 할당량 사용을 보고합니다.                                                                                                      |
| mkbackupdir  | 백업 디렉토리를 만들어 메시지 저장소의 정보와 동기화합니다.                                                                                                                      |
| MoveUser     | 한 메시징 서버에서 다른 메시징 서버로 사용자의 계정을 이동합니다.                                                                                                                  |
| imquotacheck | 메시지 저장소의 각 사용자에 대한 총 메일함 크기를 계산하고 이 크기를 지정된 할당량과 비교합니다. 현지화된 버전의 imquotacheck 알림은 % 및 \$ 기호를 잘못 변환합니다. 인코딩을 수정하려면 메일 파일에서 모든 \$와 %을 각각 \24와 \25로 바꿉니다. |
| readership   | 공유 IMAP 폴더에서 readership 정보를 수집합니다.                                                                                                                     |
| reconstruct  | 손상된 메일함을 다시 구성합니다.                                                                                                                                     |
| stored       | 백그라운드 및 일상 작업을 수행하고 디스크에 저장된 메일을 정리 및 삭제합니다.                                                                                                           |

## 메시지 저장소 디렉토리 레이아웃

그림 18-1은 서버 인스턴스에 대한 메시지 저장소 디렉토리 레이아웃을 보여 줍니다. 메시지 저장소는 메일함 내용을 신속하게 액세스할 수 있도록 설계되었습니다. 저장소 디렉토리는 표 18-2에 설명되어 있습니다.

그림 18-1 메시지 저장소 디렉토리 레이아웃



메시지 저장소는 여러 메일함 데이터베이스 및 사용자 메일함으로 구성됩니다. 메일함 데이터베이스는 사용자, 메일함, 분할 영역, 할당량 및 기타 메시지 저장소 관련 데이터에 대한 정보로 구성됩니다. 사용자 메일함은 사용자의 메일과 폴더를 포함합니다. 메일함은 전적으로 메시지 저장소를 저장하는 *디스크 분할 영역*의 한 영역인 *메시지 저장소 분할 영역*에 저장됩니다. 자세한 내용은 [593페이지의 “메시지 저장소 분할 영역 구성”](#)을 참조하십시오. 메시지 저장소 분할 영역은 디스크 분할 영역과 다르지만 유지 관리가 용이하도록 각 메시지 저장소 분할 영역에 대해 하나의 디스크 분할 영역을 가지는 것이 좋습니다.

INBOX와 같은 메일함은 *store\_root*에 위치합니다. 예를 들어, 샘플 디렉토리 경로는 다음과 같을 수 있습니다.

```
store_root/partition/primary/=user/53/53/=mack1
```

아래 표에서는 메시지 저장소 디렉토리를 설명합니다.

**표 18-2** 메시지 저장소 디렉토리 설명

| 위치                                  | 내용/설명                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>msg_svr_base</i>                 | 기본값: /opt/SUNWmsgsr<br>서버 프로그램, 구성, 유지 관리 및 정보 파일을 포함하는 Messaging Server 시스템상의 디렉토리입니다.                                                                                                                                                                                                                                                                                                                                                   |
| <i>store_root</i>                   | <i>msg_svr_base</i> /data/store<br>메시지 저장소의 최상위 디렉토리입니다. mboxlist, user 및 partition 하위 디렉토리를 포함합니다.                                                                                                                                                                                                                                                                                                                                       |
| ./store.expirerule                  | 자동 메일 제거 규칙(만료 규칙)을 포함합니다. 이 선택적 파일의 위치는 다를 수 있습니다. <a href="#">581페이지의 “자동 메일 제거(만료 및 제거) 기능 설정”</a> 을 참조하십시오.                                                                                                                                                                                                                                                                                                                           |
| <i>store_root</i> /dbdata/snapshots | 메시지 저장소 데이터베이스 백업 스냅샷입니다.                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <i>store_root</i> /mboxlist/        | 메일함 및 할당량 관련 정보를 저장하는 메일함 데이터베이스(Berkeley DB)를 포함합니다.<br><br>folder.db는 메일함이 저장된 분할 영역의 이름, ACL, store.idx의 일부 정보 복사본 등을 비롯하여 메일함에 대한 정보를 포함합니다. folder.db에는 각 메일함별로 한 개의 항목이 있습니다.<br><br>quota.db는 할당량 및 할당량 사용에 대한 정보를 포함합니다. quota.db에는 각 사용자별로 한 개의 항목이 있습니다.<br><br>lright.db는 acl 조회 권한별 폴더에 대한 색인입니다.<br><br>peruser.db는 사용자별 플래그에 대한 정보를 포함합니다. 이 플래그는 특정 사용자가 메일을 보았거나 삭제했는지 여부를 나타냅니다.<br><br>subscr.db는 사용자 가입에 대한 정보를 포함합니다. |
| <i>store_root</i> /session/         | 활성 메시지 저장소 프로세스 정보를 포함합니다.                                                                                                                                                                                                                                                                                                                                                                                                                |

**표 18-2** 메시지 저장소 디렉토리 설명

| 위치                                                           | 내용/설명                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>store_root/user/</code>                                | 사용되지 않습니다.                                                                                                                                                                                                                                                                                                                                                                                                          |
| <code>store_root/partition/</code>                           | 메시지 저장소 분할 영역을 포함합니다. 기본 <code>primary</code> 분할 영역이 만들어 집니다. 정의하는 다른 모든 분할 영역을 이 디렉토리에 넣습니다.                                                                                                                                                                                                                                                                                                                       |
| <code>store_root/partition/primary/<br/>=user/</code>        | 분할 영역의 하위 디렉토리에 모든 사용자 메일함을 포함합니다. 메일함은 빠른 검색을 위해 해시 구조에 저장됩니다. 특정 사용자의 메일함을 포함하는 디렉토리를 찾으려면 <code>hashdir</code> 유틸리티를 사용합니다.                                                                                                                                                                                                                                                                                      |
| <code>.../=user/hashdir/hashdir/<br/>userid/</code>          | 아이디가 <code>userid</code> 인 사용자에 대한 최상위 메일 폴더이며, 사용자의 INBOX입니다. 기본 도메인의 경우 <code>userid</code> 는 <code>uid</code> 이고 호스트된 도메인의 경우 <code>userid</code> 는 <code>uid@domain</code> 입니다. 받는 메일은 이 메일 폴더로 전달됩니다.                                                                                                                                                                                                          |
| <code>.../userid/folder</code>                               | Messaging Server의 사용자 정의 메일함입니다.                                                                                                                                                                                                                                                                                                                                                                                    |
| <code>.../userid/store.idx</code>                            | <code>/userid/</code> 디렉토리에 저장된 메일에 대한 메일 수, 이 메일함에 사용된 디스크 할당량, 메일함이 마지막으로 추가된 시간, 메일 플래그, 헤더 및 MIME 구조를 비롯한 각 메일의 변수 길이 정보, 각 메일의 크기 등과 같은 정보를 제공하는 색인입니다. 이 색인은 또한 각 사용자에 대한 <code>mboxlist</code> 정보와 할당량 정보의 백업 복사본을 포함합니다.                                                                                                                                                                                    |
| <code>.../userid/store.usr</code>                            | 폴더에 액세스한 사용자 목록을 포함합니다. 목록의 각 사용자에게 대해 사용자가 폴더에 액세스한 마지막 시간, 사용자가 본 메일 목록 및 사용자가 삭제한 메일 목록에 대한 정보를 포함합니다.                                                                                                                                                                                                                                                                                                           |
| <code>.../userid/store.sub</code>                            | 사용자 가입에 대한 정보를 포함합니다.                                                                                                                                                                                                                                                                                                                                                                                               |
| <code>.../userid/store.exp</code>                            | 정리되었지만 디스크에서 제거되지 않는 메일 파일의 목록을 포함합니다. 이 파일은 정리된 메일이 있는 경우에만 나타납니다.                                                                                                                                                                                                                                                                                                                                                 |
| <code>.../userid/nn/<br/>또는<br/>.../userid/folder/nn/</code> | <code>nn</code> 은 <code>message_id.msg</code> 형식의 메일을 포함하는 해시 디렉토리입니다. <code>nn</code> 은 00에서 99 사이의 숫자가 될 수 있으며 <code>message_id</code> 도 숫자입니다. 예를 들어 1에서 99 사이의 메일은 <code>.../00</code> 디렉토리에 저장됩니다. 첫 번째 메일은 <code>1.msg</code> 이고 두 번째 메일은 <code>2.msg</code> , 세 번째 메일은 <code>3.msg</code> 입니다. 100에서 199 사이의 메일은 01 디렉토리에 저장되고 9990에서 9999 사이의 메일은 99 디렉토리에 저장되며 이와 같이 10000에서 10099 사이의 메일은 00 디렉토리에 저장됩니다. |

## 메시지 저장소에서 메일을 제거하는 방법

메일은 메시지 저장소에서 다음 세 단계를 거쳐 제거됩니다.

1. **삭제.** 클라이언트는 메일 플래그를 **삭제**로 설정합니다. 이 시점에 메일이 제거 표시되지만 클라이언트는 삭제 플래그를 제거하여 메일을 복원할 수 있습니다. 두 번째 클라이언트가 있을 경우 삭제된 플래그는 바로 두 번째 클라이언트부터 표시되지 않을 수 있습니다. `configutil` 매개 변수 `local.imap.immediateflagupdate`를 설정하여 즉시 플래그 업데이트를 사용할 수 있습니다.
2. **정리.** 메일함에서 메일이 제거됩니다. 기술적으로는 메일이 메시지 저장소 색인 파일 `store.idx`에서 제거되는 것입니다. 메일 자체는 여전히 디스크상에 존재하지만 메일이 정리되고 나면 클라이언트가 더 이상 메일을 복원할 수 없습니다.  
  
**만료**는 특수한 경우의 정리를 의미합니다. 메일 크기, 기간 등과 같은 관리자가 정의한 일련의 제거 기준을 따르는 메일이 정리됩니다. [581페이지의 “자동 메일 제거\(만료 및 제거\) 기능 설정”](#)을 참조하십시오.
3. **제거.** `stored` 유틸리티는 기본적으로 메일 오후 11시에 정리된 모든 메일을 디스크에서 제거합니다. 이는 메일 제거 일정을 제어하는 `local.schedule.purge`와 제거 유예 기간(그 전까지 메일이 제거되지 않는 기간)을 제어하는 `store.cleanup`으로 구성할 수 있습니다.

## 저장소에 대한 관리자 액세스 지정

메시지 저장소 관리자는 사용자 메일함을 확인 및 모니터링하고 메시지 저장소에 대한 액세스 제어를 지정할 수 있습니다. 저장소 관리자는 모든 서비스(POP, IMAP, HTTP 또는 SMTP)에 대한 프록시 인증 권한을 가지므로 모든 사용자의 권한을 사용하여 모든 서비스에 인증될 수 있습니다. 이러한 권한을 사용하여 저장소 관리자는 저장소 관리를 위한 일정한 유틸리티를 실행할 수 있습니다. 예를 들어, 저장소 관리자는 `MoveUser`를 사용하여 사용자 계정과 메일함을 특정 시스템에서 다른 시스템으로 이동할 수 있습니다.

이 절에서는 **Messaging Server** 설치의 메시지 저장소에 대한 저장소 권한을 허가하는 방법에 대해 설명합니다.

---

**주**                    다른 사용자가 저장소에 대한 관리자 권한을 가질 수도 있습니다. 예를 들어, 일부 관리자가 이러한 권한을 가질 수 있습니다.

---

다음 하위 절에 설명된 대로 관리자 작업을 수행할 수 있습니다.

- [관리자 추가](#)
- [관리자 항목 수정](#)
- [관리자 항목 삭제](#)

## 관리자 추가

**콘솔.** 콘솔에서 관리자 항목을 추가하려면 다음을 수행합니다.

1. 콘솔에서 구성할 **Messaging Server**를 엽니다.
2. 구성 탭을 누르고 왼쪽 표시 영역에서 메시지 저장소를 선택합니다.
3. 관리자 탭을 누릅니다.

이 탭에는 기존 관리자 아이디 목록이 포함되어 있습니다.

4. 관리자 UID 창 옆의 추가 버튼을 누릅니다.
5. 관리자 UID 필드에서 추가할 관리자의 사용자 아이디를 입력합니다.  
Sun Java System Directory Server에 알려져 있는 사용자 아이디를 입력해야 합니다.
6. 확인을 눌러 관리자 아이디를 관리자 탭에 표시된 목록에 추가합니다.
7. 관리자 탭에서 저장을 눌러 새로 수정한 관리자 목록을 저장합니다.

**명령줄.** 명령줄에서 관리자 항목을 추가하려면 다음을 수행합니다.

```
configutil -o store.admins -v "adminlist"
```

여기서 *adminlist*는 관리자 아이디의 공백으로 구분된 목록입니다. 여러 관리자를 지정할 경우 목록을 따옴표로 묶어야 합니다. 또한, 관리자는 서비스 관리자 그룹의 구성원이어야 합니다(LDAP 사용자 항목에서:memberOf: cn=Service Administrators,ou=Groups,o=usergroup).

## 관리자 항목 수정

**콘솔.** 콘솔에서 메시지 저장소 관리자 UID 목록의 기존 항목을 수정하려면 다음을 수행합니다.

1. 관리자 탭을 누릅니다.
2. 관리자 UID 창 옆의 편집 버튼을 누릅니다.
3. 관리자 UID 필드에 대한 변경 사항을 입력합니다.
4. 확인을 눌러 변경 사항을 제출하고 관리자 편집 창을 닫습니다.

5. 관리자 탭에서 저장을 눌러 수정된 관리자 목록을 제출하고 보존합니다.

**명령줄.** 명령줄에서 메시지 저장소 관리자 UID 목록의 기존 항목을 수정하려면 다음을 수행합니다.

```
configutil -o store.admins -v "adminlist"
```

## 관리자 항목 삭제

**콘솔.** 콘솔을 사용하여 메시지 저장소 관리자 UID 목록에서 항목을 삭제하려면 다음을 수행합니다.

1. 관리자 탭을 누릅니다.
2. 관리자 UID 목록에서 항목을 선택합니다.
3. 삭제를 눌러 항목을 삭제합니다.
4. 저장을 눌러 관리자 목록에 대한 변경 사항을 제출하고 보존합니다.

**명령줄.** 명령줄에서 저장소 관리자를 삭제하려면 다음과 같이 관리자 목록을 편집할 수 있습니다.

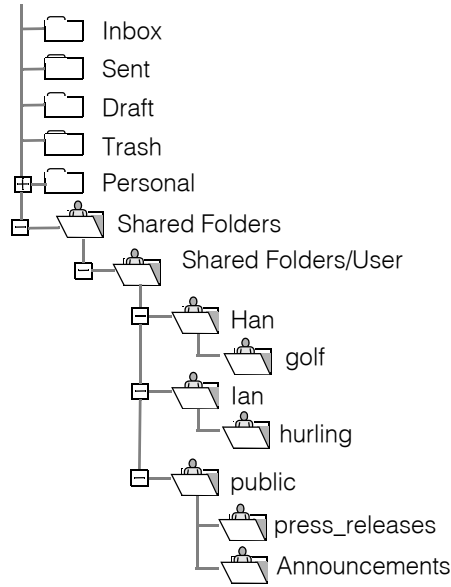
```
configutil -o store.admins -v "adminlist"
```

## 공유 폴더 정보

**공유 폴더**는 사용자 그룹이 액세스하고 읽을 수 있는 폴더입니다. 다시 말해서 공유 폴더에 대한 액세스 권한은 여러 사용자에게 허가됩니다. 예를 들어, 한 사용자가 golf라는 폴더를 만들어 이 폴더의 내용을 다른 사용자가 볼 수 있게 허용할 수 있습니다.

기본적으로 **Messaging Server**는 모든 전자 메일 계정에서 Shared Folders/Users라는 폴더를 만듭니다. 사용자는 이 폴더에서 공유 폴더를 만들고 액세스합니다. 공유 폴더가 클라이언트에서 표시되는 방법을 보여 주는 한 예가 [그림 18-2](#)에 나와 있습니다. 이 예는 [566페이지의 “분산 공유 폴더 설정”](#)에서 자세하게 설명됩니다.

그림 18-2 Ed의 클라이언트 공유 메일 폴더 목록의 예



사용자는 개인 공유 폴더를 만들고 공유 폴더를 지원하는 전자 메일 클라이언트를 사용하여 이러한 폴더에 대한 액세스 권한을 제공할 수 있습니다. 이러한 공유 폴더는 액세스 권한이 주어진 다른 사용자의 Shared Folders에 표시됩니다.

공유 폴더는 특정 주제에 대한 지속적인 대화를 시작, 공유 및 보관하는 데 유용합니다. 예를 들어, 소프트웨어 개발자 그룹은 특정 프로젝트의 개발을 논의하기 위해 공유 폴더를 만들 수 있습니다. 메일을 공유 폴더로 보내면 공유 폴더에 가입한 모든 사람(개별 주소 또는 그룹 주소별로 가입자 추가 가능)이 메일함을 열고 메일을 읽을 수 있습니다.

공유 폴더에는 다음 두 종류가 있습니다.

- **개인** - 개인 공유 폴더는 특정 사용자가 소유하는 공유 폴더입니다. 폴더 소유자는 다른 사용자에게 액세스 권한을 부여합니다.
- **공용** - 공용 공유 폴더에는 소유자가 없습니다. 관리자는 공용 폴더를 호스트하는 데 사용될 수 있는 공용 사용자 계정을 만듭니다. 공용 폴더의 전자 메일 주소는 다음과 같습니다.

`public+foldername@domain`



예를 들어, 회사 내의 특정 이익 집단에 대한 정보를 게시하기 위해 public+software\_dev@siroe.com과 같은 폴더를 필요로 할 수 있습니다. 관련 직원에게 이 공용 폴더에 대한 액세스 권한이 부여됩니다.

일반적으로 공유 폴더는 특정 메시지 저장소의 사용자만 사용할 수 있습니다. 그러나 Messaging Server에서는 여러 메시지 저장소에서 액세스할 수 있는 특수한 공유 폴더를 만들 수 있습니다. 이러한 폴더를 *분산 공유 폴더*라고 부릅니다. 자세한 내용은 [566페이지](#)의 “[분산 공유 폴더 설정](#)”을 참조하십시오.

## 공유 폴더 액세스 권한

액세스 권한은 folder.db에 저장되는 ACL(액세스 제어 목록)에서 유지 관리됩니다. readership 명령줄 유틸리티와 함께 -s 옵션을 사용하여 IMAP SETACL 명령을 사용하거나([565페이지](#)의 “[공용 폴더의 액세스 제어 권한 변경](#)” 참조) Messenger Express 인터페이스를 사용하여 ACL을 설정하는 방법으로 액세스 권한을 부여합니다.

### ACL 식별자

각 ACL 항목은 항목이 적용되는 사용자 또는 사용자 그룹을 지정하는 식별자를 가집니다. 대시("-")로 시작되는 식별자는 허용되지 않는 권한(사용자 또는 그룹에 대해 거부된 권한)을 나타냅니다.

anyone은 특수 식별자입니다. anyone에 대한 액세스 권한은 모든 사용자에게 적용됩니다. 마찬가지로 anyone@domain에 대한 액세스 권한은 동일한 도메인의 모든 사용자에게 적용됩니다.

그룹 식별자는 group=으로 시작됩니다.

### ACL 권한 문자

각 ACL 항목에는 문자열로 표시되는 권한 집합이 있습니다. 이러한 문자열은 RFC 2086에 의해 정의됩니다. 사용자의 권한 집합을 계산하기 위해 서버는 해당 사용자와 사용자가 속한 모든 그룹에 허가된 모든 권한을 더한 다음 해당 사용자와 사용자가 속한 그룹을 거부한 모든 권한을 뺍니다.

다음 표에는 Messaging Server에 의해 인식되는 문자 목록이 그 이름 및 간단한 설명과 함께 나열되어 있습니다. 또한 해당 권한을 가진 사용자가 실행할 수 있는 IMAP 명령이 나와 있습니다.

**표 18-3** ACL 권한 문자

| 문자 | 설명                                                                                            |
|----|-----------------------------------------------------------------------------------------------|
| l  | lookup – 사용자는 공유 폴더를 보고 가입할 수 있습니다(허용되는 IMAP 명령: LIST 및 LSUB).                                |
| r  | read – 사용자는 공유 폴더를 읽을 수 있습니다(허용되는 IMAP 명령: 폴더에서 SELECT, CHECK, FETCH, PARTIAL, SEARCH, COPY). |
| s  | seen – 세션에서 사용자가 본 정보를 보관하도록 시스템에 지시합니다(IMAP STORE SEEN 플래그 설정)                               |
| w  | write – 사용자가 메일을 읽은 것으로 표시하고 삭제할 수 있습니다(SEEN 및 DELETED가 아닌 IMAP STORE 플래그 설정)                 |
| i  | insert – 사용자가 전자 메일을 한 폴더에서 다른 폴더로 복사 및 이동할 수 있습니다(허용되는 IMAP 명령: 폴더로 APPEND, COPY).           |
| p  | post – 사용자가 공유 폴더 전자 메일 주소로 메일을 보낼 수 있습니다(IMAP 명령이 필요하지 않음).                                  |
| c  | create – 사용자가 새 하위 폴더를 만들 수 있습니다(허용되는 IMAP 명령: CREATE).                                       |
| d  | delete – 사용자가 공유 폴더에서 항목을 삭제할 수 있습니다(허용되는 IMAP 명령: EXPUNGE, set STORE DELETED 플래그 설정).        |
| a  | administer – 사용자가 관리 권한을 가집니다(허용되는 IMAP 명령: SETACL).                                          |

## 그룹 ACL

ACL 항목의 식별자는 그룹 이름을 지정할 수 있습니다. 이 항목의 액세스 권한은 해당 그룹의 모든 구성원에게 적용됩니다. 서버는 inetMailUser 객체 클래스의 aclGroupAddr 속성으로 그룹 멤버십을 결정합니다. 그룹은 aclGroupAddr 속성에 대한 필터를 가진 동적 메일 목록으로 나타납니다. 다음 예에서는 aclGroupAddr 속성을 비롯하여 그룹을 정의하는 LDIF 레코드를 보여 줍니다.

```
dn: cn=lee-staff,ou=Groups, o=sesta.com
cn: lee-staff
mailHost: mail.sesta.com
inetMailGroupStatus: active
mgrpErrorsTo: lee.jones@sesta.com
description: Dynamic Group of Lee's staff
objectClass: top
objectClass: groupofuniquenames
objectClass: inetmailgroup
objectClass: inetmailgroupmanagement
objectClass: inetlocalmailrecipient
objectClass: groupofurls
mail: lee-staff@sesta.com
memberURL: ldap:///o=sesta.com??sub?
(&(aclGroupAddr=lee-staff@sesta.com)(objectclass=inetmailuser))
```

그룹 전자 메일 주소를 폴더의 ACL에서 사용하기 위해 그룹을 만들 필요는 없습니다. 실제로는 그룹에 구성원을 추가할 때 이러한 동적 그룹을 만들어 사용자 항목에서 aclGroupAddr 속성을 설정해야 합니다. 이러한 그룹이 만들어지면 mgrpRfc822MailMember 속성에서 해당 전자 메일 주소를 사용하여 정적 외부 구성원을 추가할 수 있습니다. uniqueMember 속성을 사용하거나 memberURL 속성의 추가 값을 만들어 구성원을 추가해서는 안 됩니다. 이렇게 하면 MTA가 메일 목록의 구성원으로 보는 것과 IMAP가 그룹 구성원으로 보는 것 사이의 연결이 끊어집니다.

사용자가 IMAP 서버에 로그인하거나 Messenger Express와 같은 HTTP 액세스 서비스 클라이언트로 로그인하면 서버는 다른 메시지 저장소 관련 속성과 함께 aclGroupAddr 속성을 가져오고 그룹 이름을 메모리에 캐시합니다. 클라이언트가 액세스 권한 확인을 요구하는 명령(예: LIST 또는 SELECT)을 실행할 때마다 서버는 이 정보를 사용하여 사용자의 액세스 권한을 결정합니다.

# 공유 폴더 작업

이 절에서는 공유 폴더와 관련된 다음 관리자 작업에 대해 설명합니다.

- 564페이지의 “공유 폴더 만들기”
- 565페이지의 “공용 폴더의 액세스 제어 권한 변경”
- 566페이지의 “공유 폴더 목록을 사용 가능 또는 사용 불가능하게 하기”
- 566페이지의 “분산 공유 폴더 설정”
- 568페이지의 “공유 폴더 데이터 모니터 및 유지 관리”

## 공유 폴더 만들기

공용 폴더는 LDAP 데이터베이스와 `readership` 명령에 대한 액세스가 필요하기 때문에 시스템 관리자에 의해 작성되어야 합니다.

1. 다음과 같이 모든 공유 폴더(예: `public`)의 컨테이너 역할을 수행하는 LDAP 사용자 항목을 추가합니다.

```
dn: cn=public,ou=people,o=sesta.com,o=ISP
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: inetUser
objectClass: ipUser
objectClass: inetMailUser
objectClass: inetLocalMailRecipient
objectClass: nsManagedPerson
objectClass: userPresenceProfile
cn: public
mail: public@sesta.com
mailDeliveryOption: mailbox
mailHost: manatee.siroe.com
uid: public
inetUserStatus: active
mailUserStatus: active
mailQuota: -1
mailMsgQuota: 100
```

2. `mboxutil` 명령줄 유틸리티를 사용하여 공용 계정 내에 폴더를 만듭니다. 예를 들면 다음과 같습니다.

```
mboxutil -c user/public/golftournament
```

3. `readership` 명령줄 유틸리티를 사용하여 이 폴더에 대해 적절한 ACL을 설정합니다. 이 폴더를 공용으로 만들려면 액세스 권한이 있는 사용자 그룹을 이 폴더에 할당해야 합니다. 이렇게 하려면 `readership` 명령을 사용하여 ACL을 설정합니다. ACL 설정 방법에 대한 지침은 다음에 나오는 565페이지의 “공용 폴더의 액세스 제어 권한 변경”을 참조하십시오.

## 공용 폴더의 액세스 제어 권한 변경

경우에 따라 공용 폴더에 대한 액세스 제어를 변경하거나 새로 만든 공용 폴더에 대한 액세스 제어를 설정해야 할 수 있습니다.

그러려면 `readership` 명령줄 유틸리티를 사용합니다. 이 명령의 형식은 다음과 같습니다.

```
readership -s foldername identifier rights_chars
```

여기서 `foldername`은 권한을 설정할 공용 폴더의 이름이고 `userid`는 권한을 할당하는 개인 또는 그룹이며 `rights_chars`는 할당할 권한(RFC 2086 호환 액세스 권한 문자)입니다. 각 문자의 의미는 561페이지의 “ACL 권한 문자”를 참조하십시오. 또한 Messenger Express 인터페이스를 사용하여 공용 폴더에 대한 액세스 제어를 변경할 수도 있습니다.

### 예

예를 들어, `golftournament` 공용 폴더에 대한 조회, 읽기 및 전자 메일 표시 권한(게시 권한 제외)을 `sesta` 도메인의 모든 사용자에게 할당하려는 경우 다음 명령을 실행합니다.

```
readership -s User/public/golftournament anyone@sesta lwr
```

조회, 읽기, 전자 메일 표시 및 게시 권한을 그룹에 할당하려면 다음 명령을 실행합니다.

```
readership -s User/public/golftournament group=golffinterest lwrp
```

이 폴더에 대한 관리자 및 게시 권한을 개별 사용자 `jdoe`에게 할당하려는 경우 다음 명령을 실행합니다.

```
readership -s User/public/golftournament jdoe lwrpa
```

공용 폴더에 대한 개별 사용자 또는 그룹 액세스를 거부하려면 `userid`에 접두어 대시를 사용합니다. 예를 들어, `jsmith`에 대한 조회, 읽기 및 쓰기 권한을 거부하려면 다음 명령을 실행합니다.

```
readership -s User/public/golftournament -jsmith lwr
```

## 공유 폴더 목록을 사용 가능 또는 사용 불가능하게 하기

서버는 구성 옵션 `local.store.sharedfolders`의 설정에 따라 `LIST` 명령에 응답할 때 공유 폴더를 반환하거나 반환하지 않습니다. 이 옵션을 비활성화하려면 `off`로 설정합니다. 기본적으로 이 옵션은 활성화됩니다(`on`으로 설정).

`SELECT` 및 `LSUB` 명령은 이 옵션의 영향을 받지 않습니다. `LSUB` 명령은 공유 폴더를 비롯하여 가입한 모든 폴더를 반환합니다. 사용자는 자신이 소유하거나 가입한 공유 폴더를 `SELECT`할 수 있습니다.

## 분산 공유 폴더 설정

일반적으로 공유 폴더는 특정 메시지 저장소의 사용자만 사용할 수 있습니다. 그러나 `Messaging Server`에서는 여러 메시지 저장소에서 액세스할 수 있는 *분산 공유 폴더*를 만들 수 있습니다. 즉, 분산 공유 폴더에 대한 액세스 권한은 메시지 저장소 그룹 내의 모든 사용자에게 부여될 수 있습니다. 단, 웹 메일 클라이언트(`Messenger Express`와 같은 `HTTP` 액세스 클라이언트)는 원격 공유 폴더 액세스를 지원하지 않습니다. 사용자는 폴더를 나열하여 가입할 수 있지만 내용을 보거나 변경할 수는 없습니다.

분산 공유 폴더는 다음이 필요합니다.

- 메시지 저장소 `userid`가 메시지 저장소 그룹에서 고유해야 합니다.
- 배포에서 디렉토리 데이터가 동일해야 합니다.

원격 메시지 저장소(공유 폴더를 보유하지 않는 메시지 저장소)는 [566페이지의 표 18-4](#)에 나열된 구성 변수를 설정하여 프록시 서버로 구성해야 합니다.

**표 18-4** 분산 공유 폴더 구성을 위한 변수

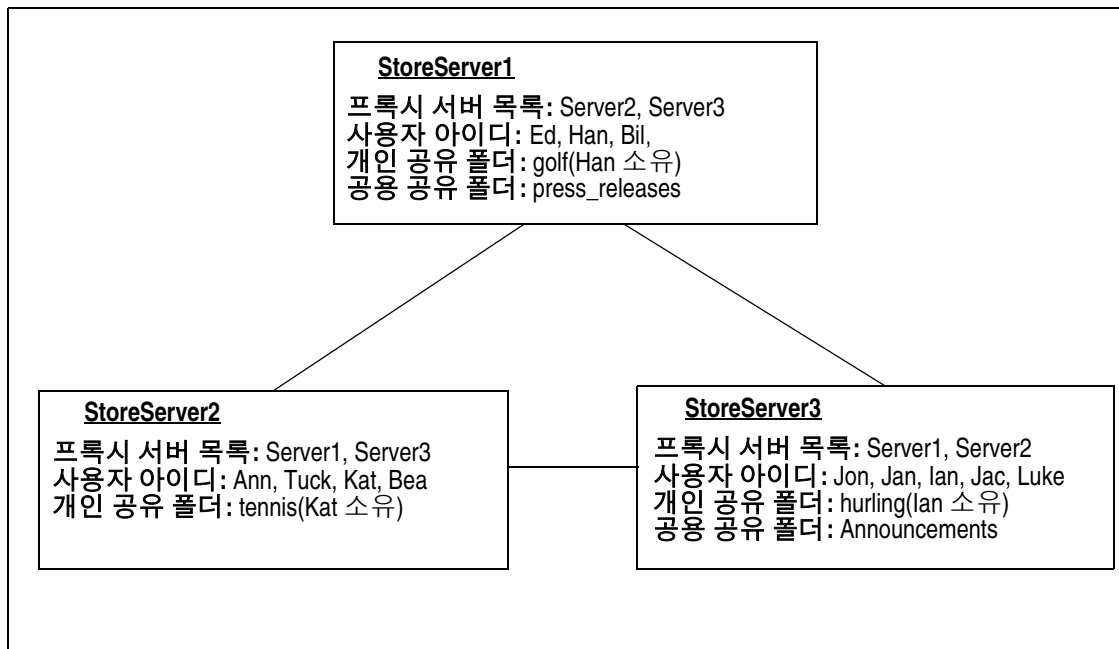
| 이름                                          | 값                 | 데이터 형식       |
|---------------------------------------------|-------------------|--------------|
| <code>local.service.proxy.serverlist</code> | 메시지 저장소 서버 목록     | 공백으로 구분된 문자열 |
| <code>local.service.proxy.admin</code>      | 기본 저장소 관리자 로그인 이름 | 문자열          |

**표 18-4** 분산 공유 폴더 구성을 위한 변수

| 이름                                                  | 값                      | 데이터 형식 |
|-----------------------------------------------------|------------------------|--------|
| <code>local.service.proxy.adminpass</code>          | 기본 저장소 관리자 비밀번호        | 문자열    |
| <code>local.service.proxy.admin.hostname</code>     | 특정 호스트의 저장소 관리자 로그인 이름 | 문자열    |
| <code>local.service.proxy.adminpass.hostname</code> | 특정 호스트의 저장소 관리자 비밀번호   | 문자열    |

## 분산 공유 폴더 설정—예

그림 18-3은 StoreServer1, StoreServer2 및 StoreServer3이라는 세 개의 메시지 저장소 서버의 분산 폴더 예를 보여 줍니다.

**그림 18-3** 분산 공유 폴더—예

이러한 서버는 표 18-4에 나온 변수의 설정을 통해 서로 간에 피어 프록시 메시지 저장소로 연결됩니다. 각 서버는 개인 공유 폴더, 즉 *golf*(Han 소유), *tennis*(Kat 소유) 및 *hurling*(Luke 소유)을 가집니다. 또한 *press\_releases* 및 *Announcements*라는 두 개의 공용 공유 폴더가 존재합니다. 이러한 세 서버의 사용자는 이러한 세 개의 공유 폴더에 액세스할 수 있습니다. 560페이지의 그림 18-2는 Ed의 공유 폴더 목록을 보여 줍니다. 다음은 이 구성의 각 서버에 대한 ACL의 예입니다.

```
$ StoreServer1 :> readership -l
Ed: user/Han/golf
Ian: user/Han/golf
anyone: user/public/press_releases
```

```
$ StoreServer2 :> readership -l
Jan: user/Kat/tennis
Ann: user/Kat/tennis
anyone: user/public+Announcements user/public+press_releases
```

```
$ StoreServer3 :> readership -l
Tuck: user/Ian/hurling
Ed: user/Ian/hurling
Jac: user/Ian/hurling
anyone: user/public/Announcements
```

## 공유 폴더 데이터 모니터 및 유지 관리

`readership` 명령줄 유틸리티를 사용하면 `folder.db`, `peruser.db` 및 `lright.db` 파일에 보관되는 공유 폴더 데이터를 모니터 및 유지 관리할 수 있습니다. `folder.db`는 ACL의 복사본을 보유하는 각 폴더에 대한 레코드를 가집니다. `peruser.db`는 각 사용자 및 메일함에 대한 항목을 가지며 이 항목은 다양한 플래그 설정과 사용자가 임의 폴더를 마지막으로 액세스한 날짜를 나열합니다. `lright.db`는 모든 사용자와 사용자가 조회 권한을 가진 공유 폴더를 나열합니다.



readership 명령줄 유틸리티에는 다음 옵션이 있습니다.

**표 18-5** readership 옵션

| 옵션                                 | 설명                                                           |
|------------------------------------|--------------------------------------------------------------|
| -d days                            | 지정된 날짜 동안 해당 폴더를 선택한 사용자 수에 대한 보고서를 공유 폴더별로 반환합니다.           |
| -p months                          | 지정된 개월 수 동안 공유 폴더를 선택하지 않는 사용자에게 대해 peruser.db에서 데이터를 제거합니다. |
| -l                                 | lright.db의 데이터를 나열합니다.                                       |
| -s <i>folder_identifier_rights</i> | 지정된 폴더에 대한 액세스 권한을 설정합니다. folder.db와 lright.db를 업데이트합니다.     |

다양한 옵션을 사용하여 다음 기능을 수행할 수 있습니다.

- [569페이지의 “공유 폴더 사용 모니터”](#)
- [569페이지의 “사용자 및 사용자의 공유 폴더 나열”](#)
- [570페이지의 “비활성 사용자 제거”](#)
- [570페이지의 “액세스 권한 설정”](#)

## 공유 폴더 사용 모니터

공유 폴더에 액세스하는 활성 사용자 수를 확인하려면 다음 형식의 명령을 실행합니다.

```
readership -d days
```

여기서 *days*는 검사할 일 수입니다. 이 옵션은 활성 사용자 목록이 아니라 그 수를 반환한다는 점에 주의하십시오.

예를 들어, 마지막 30일 이내에 공유 폴더를 선택한 사용자 수를 확인하려면 다음 명령을 실행합니다.

```
readership -d 30
```

## 사용자 및 사용자의 공유 폴더 나열

사용자와 사용자가 액세스할 수 있는 공유 폴더를 나열하려면 다음 명령을 실행합니다.

```
readership -l
```

출력 예는 다음과 같습니다.

```
$ readership -l
group=lee-staff@siroe.com: user/user2/lee-staff
richb: user/golf user/user10/Drafts user/user2/lee-staff user/user10/Trash
han1: user/public+hurling@siroe.com user/golf
gregk: user/public+hurling@siroe.com user/heaving user/tennis
```

## 비활성 사용자 제거

지정된 기간 동안 공유 폴더에 액세스하지 않은 비활성 사용자를 제거하려면 다음 명령을 실행합니다.

```
readership -p months
```

여기서 *months*는 검사할 개월 수입니다.

예를 들어, 지난 6개월 동안 공유 폴더에 액세스하지 않은 사용자를 제거합니다.

```
readership -p 6
```

## 액세스 권한 설정

새 공유 폴더에 대한 액세스 권한을 할당하거나 현재 공유 폴더에서 액세스 권한을 변경할 수 있습니다.

이 명령으로 액세스 권한을 설정하는 방법의 예는 [565페이지의 “공용 폴더의 액세스 제어 권한 변경”](#)을 참조하십시오.

# 메시지 저장소 할당량 정보

메시지 저장소 할당량은 사용자 또는 도메인이 사용할 수 있는 디스크 공간 또는 메일 수에 대한 제한 또는 할당량을 설정하는 한 가지 방법입니다. 이 절은 다음 내용으로 구성되어 있습니다.

- [571페이지의 “사용자 할당량”](#)
- [571페이지의 “도메인 할당량”](#)
- [572페이지의 “Telephony Application Server 예외 사항”](#)

자세한 내용은 [603페이지의 “할당량 제한 모니터”](#)를 참조하십시오.

## 사용자 할당량

디스크 공간 또는 메일 수를 기준으로 사용자 할당량을 지정할 수 있습니다. 디스크 공간 할당량은 각 사용자에게 대한 디스크 공간량을 바이트로 지정합니다. 디스크 할당량은 사용자가 갖고 있는 메일 폴더의 수나 사용자 메일의 총 개수에 상관 없이 모든 사용자 메일의 총 크기에 적용됩니다. 메일 할당량을 사용하면 사용자의 메일함에 저장되는 메일 수를 제한할 수 있습니다.

할당량 정보는 사용자 LDAP 속성(표 18-6) 및 configutil 변수(표 18-7)에 저장됩니다. 최신 정보에 대한 자세한 내용은 *Sun Java System Communications Services Schema Reference Manual*(<http://docs.sun.com/doc/819-0113>)을 참조하십시오. 할당량 자체를 설정하는 외에도 Messaging Server를 사용하여 다음 기능을 제어할 수 있습니다.

- **할당량 알림**은 디스크 할당량 임계값에 도달할 경우에 사용자에게 경고 메일을 보냅니다.
- **할당량 적용**은 할당량이 초과할 경우 메시지 저장소에 대한 메일 전달을 중지하거나, 할당량이 초과하더라도 메일 전달을 허용합니다.

할당량 초과로 인해 메일 전달이 중지되는 경우 받는 메일은 다음 중 하나가 발생할 때까지 MTA 대기열에 남아 있습니다.

- MTA가 메일을 사용자에게 전달하는 시점에 사용자 메일의 크기나 수가 더 이상 할당량을 초과하지 않습니다.
- 메일이 보낸 사람에게 반환되는 시점에 전달되지 않은 메일이 지정된 유예 기간보다 오래 대기열에 남아 있습니다. 579페이지의 “유예 기간 설정”을 참조하십시오.

사용자가 메일을 삭제 또는 정리하거나 설정된 에이징 정책에 따라 서버에서 메일을 삭제하면 디스크 공간을 사용할 수 있게 됩니다.

- **할당량 기본값**은 모든 사용자에게 대한 기본 할당량을 설정하거나 특정 사용자에게 대해 다른 할당량을 설정합니다. 사용자가 할당량을 초과하는지 확인하기 위해 Messaging Server는 우선 개별 사용자에게 대한 할당량이 설정되었는지 검사합니다. 할당량이 설정되지 않은 경우 Messaging Server는 모든 사용자에게 설정된 기본 할당량을 확인합니다.

## 도메인 할당량

사용자의 경우처럼 도메인에 대해서도 바이트 수 또는 메일 수를 기준으로 할당량을 설정할 수 있습니다. 이 할당량은 특정 도메인에 있는 모든 사용자에게 대한 바이트 또는 메일 수를 모두 누적한 값입니다.

## Telephony Application Server 예외 사항

통합 메시징 요구 사항을 지원하기 위해 Messaging Server는 메시지 저장소에서 부과한 할당량 제한을 무시하는 기능을 제공합니다. 이 기능은 Telephony Application Server(TAS)라는 특정 에이전트에서 받은 메일이 전달되도록 합니다. TAS가 받은 메일은 할당량 제한에 상관 없이 메일이 저장소로 전달되도록 하는 특수한 MTA 채널을 통해 라우팅됩니다. TAS 채널 구성에 대한 자세한 내용은 12장, “채널 정의 구성” 을 참조하십시오.

표 18-6에서는 할당량 사용자 LDAP 속성을 표시합니다. 최신 정보에 대한 자세한 내용은 *Sun Java System Communications Services Schema Reference Manual*(<http://docs.sun.com/doc/819-0113>)을 참조하십시오.

**표 18-6** 메시지 저장소 할당량 속성

| 속성                  | 설명                                                                                                                                                                                                                                                                                                                                                               |
|---------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| mailQuota           | 사용자의 메일함에 허용되는 디스크 공간(바이트)입니다. 특수 값은 다음과 같습니다.<br>0 - 사용자의 메일함에 허용되는 공간이 없습니다.<br>-1 - 허용되는 공간 사용량 제한이 없습니다.<br>-2 - 시스템 기본 할당량을 사용합니다(configutil 매개 변수 store.defaultmailboxquota).                                                                                                                                                                              |
| mailMsgQuota        | 사용자에게 허용되는 최대 메일 수입니다. 이 값은 저장소에 있는 모든 폴더에 대한 누적 개수입니다. 특수 값은 다음과 같습니다.<br>0 - 사용자의 메일함에 허용되는 메일이 없습니다.<br>-1 - 허용되는 메일 수 제한이 없습니다.<br>-2 - 시스템 기본 할당량을 사용합니다(configutil 매개 변수 store.defaultmessage.quota).                                                                                                                                                      |
| mailUserStatus      | 메일 사용자의 상태입니다. 다음 값 중 하나일 수 있습니다.<br>active - 메일이 정상적으로 처리됩니다. 기본값은 active입니다.<br>inactive - 사용자의 메일 계정이 비활성 상태입니다. 임시 실패가 반환됩니다.<br>deleted - 계정에 삭제됨 표시를 하고 삭제 준비를 합니다. 영구 실패가 반환됩니다. 메일함 액세스가 차단됩니다.<br>hold - 메일을 보관 대기열로 보내고 메일함 액세스를 허용하지 않습니다.<br>overquota - MTA는 이 상태의 메일함에 메일을 전달하지 않습니다. 이 상태는 configutil 매개 변수 store.overquotastatus가 on일 경우에 설정됩니다. |
| mailDomainDiskQuota | 허용되는 디스크 공간(바이트)으로 도메인에 있는 모든 메일함에 대한 누적 개수입니다. 값 -1은 공간 사용량 제한이 없음을 의미합니다. (기본값) 도메인 디스크 할당량을 적용하려면 다음 명령을 실행합니다.<br>imquotacheck -f -d domain                                                                                                                                                                                                                  |
| mailDomainMsgQuota  | 도메인에 허용되는 최대 메일 수 즉, 저장소에 있는 모든 메일함에 대한 개수 합계입니다. 값 -1은 제한이 없음을 의미합니다. (기본값) 도메인 메일 할당량을 적용하려면 다음 명령을 실행합니다.<br>imquotacheck -f -d domain                                                                                                                                                                                                                        |
| mailDomainStatus    | 메일 도메인의 상태입니다. 값 및 기본값은 mailUserStatus와 동일합니다.                                                                                                                                                                                                                                                                                                                   |

표 18-7 메시지 저장소 configutil 매개 변수

| 매개 변수                          | 설명                                                                                                                                                                                                                                                                                                                                        |
|--------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| store.quotaenforcement         | 할당량 적용을 활성화합니다. Off이면 할당량 데이터베이스가 계속 업데이트되지만 메일이 항상 전달됩니다. 기본값은 On입니다.                                                                                                                                                                                                                                                                    |
| store.quotanotification        | 할당량 알림을 활성화 합니다. 기본값은 On입니다.                                                                                                                                                                                                                                                                                                              |
| store.defaultmailboxquota      | 저장소 기본 할당량(바이트)입니다. 기본값은 -1(제한 없음)입니다.                                                                                                                                                                                                                                                                                                    |
| store.defaultmessagequota      | 저장소 기본 할당량(메일 수)입니다. 숫자로 기본값은 -1(제한 없음)입니다.                                                                                                                                                                                                                                                                                               |
| store.quotaexceededmsg         | 할당량 경고 메일입니다. 이 값이 없으면 알림을 보내지 않습니다. 기본값은 없습니다.                                                                                                                                                                                                                                                                                           |
| store.quotaexceededmsginterval | 할당량 초과 알림을 보내는 간격(일)입니다. 기본값은 7입니다.                                                                                                                                                                                                                                                                                                       |
| store.quotagraceperiod         | 메일함이 할당량 초과된 후 메일함의 메일을 보낸 사람에게 돌려보낼 때까지 허용된 시간(시)입니다. 시간 수입니다. 기본값은 120입니다.                                                                                                                                                                                                                                                              |
| store.quotawarn                | 할당량 경고 임계값. 클라이언트에게 할당량 경고를 보내기 전에 초과한 할당량 비율입니다. 기본값: 90                                                                                                                                                                                                                                                                                 |
| local.store.quotaoverdraft     | Netscape Messaging Server에서 마이그레이션된 시스템과의 호환성을 제공하는 데 사용됩니다. ON인 경우 디스크 사용량이 할당량을 초과하는 메일 전달을 허용합니다. 사용자가 할당량을 초과하면 메일이 지연되거나 바운스되고 할당량 경고 메일이 발송되며 할당량 유예 기간 타이머가 시작됩니다. 기본값은 메시지 저장소가 임계값에 도달할 때 할당량 경고 메일을 보냅니다. 기본값은 Off입니다. 그러나 store.overquotastatus가 설정된 경우에는 on으로 간주되며 그렇지 않은 경우에는 사용자가 할당량을 초과할 수 없고 overquotastatus가 사용되지 않습니다. |
| local.store.overquotastatus    | 메일이 MTA의 대기열에 포함되기 전에 할당량 적용을 활성화합니다. 그렇게 하면 MTA 대기열이 가득 차지 않습니다. 설정하는 경우 사용자가 아직 할당량을 초과하지 않았지만 받는 메일로 인해 사용자가 할당량을 초과하게 되면 메일이 전달되지만 mailuserstatus LDAP 속성이 overquota로 설정되므로 MTA에서 더 이상의 메일을 수락하지 않습니다. 기본값은 Off입니다.                                                                                                                   |

## 메시지 저장소 할당량 구성

이 절에서는 다음 작업에 대해 설명합니다.

- 574페이지의 “기본 사용자 할당량 지정”
- 575페이지의 “개별 사용자 할당량 지정”
- 575페이지의 “도메인 할당량 지정”
- 575페이지의 “할당량 알림 배포”
- 577페이지의 “할당량 적용 활성화 또는 비활성화”

- 579페이지의 “유예 기간 설정”

## 기본 사용자 할당량 지정

개인 할당량 설정이 없는 사용자에게 적용되는 기본 할당량을 설정하려면 다음 단계를 수행합니다.

**콘솔.** 콘솔에서 기본 사용자 할당량을 지정하려면 다음을 수행합니다.

1. 구성 탭을 누르고 왼쪽 표시 영역에서 메시지 저장소를 선택합니다.
2. 할당량 탭을 누릅니다.
3. 기본 사용자 디스크 할당량을 지정하려면 "기본 사용자 디스크 할당량" 필드에서 다음 옵션 중 하나를 선택합니다.

**제한 없음.** 기본 디스크 할당량을 설정하지 않으려는 경우 이 옵션을 선택합니다.

**크기 지정.** 기본 사용자 디스크 할당량을 특정 크기로 제한하려는 경우 이 옵션을 선택합니다. 버튼 옆의 필드에 숫자를 입력하고 드롭다운 목록에서 KB 또는 MB를 선택합니다.

4. 메일 수 할당량을 지정하려면 "기본 사용자 메일 할당량" 상자에 숫자를 입력합니다.
5. 저장을 누릅니다.
6. 기본 메시지 저장소 할당량을 사용하는 사용자 항목에서 Mbytes 속성을 -1로 설정합니다. 표 18-6을 참조하십시오.

**명령줄.** 명령줄에서 할당량을 지정하려면 다음을 수행합니다.

전체 메일 크기에 대한 기본 사용자 디스크 할당량을 지정하려면 다음을 수행합니다.

```
configutil -o store.defaultmailboxquota -v [ -1 | number ]
```

여기서 -1은 할당량 없음을 나타내고 *number*는 바이트 수를 나타냅니다.

전체 메일 수에 대한 기본 사용자 디스크 할당량을 지정하려면 다음을 수행합니다.

```
configutil -o store.defaultmessagequota -v [ -1 | number ]
```

여기서 -1은 할당량 없음을 나타내고 *number*는 메일 수를 나타냅니다.

기본 메시지 저장소 할당량을 사용하는 사용자 항목에서 mailQuota 속성을 -2로 설정합니다. 표 18-6을 참조하십시오.

## 개별 사용자 할당량 지정

각 사용자가 개별 할당량을 가질 수 있습니다. 사용자별 할당량을 설정하려면 사용자의 LDAP 항목에서 `mailQuota` 또는 `mailmsgquota` 속성을 설정합니다. 표 18-6을 참조하십시오. 할당량을 적용하려면 `configutil store.quotaenforcement`를 `on`으로 설정합니다.

## 도메인 할당량 지정

특정 도메인에 대한 디스크 공간 할당량 또는 메일 할당량을 설정할 수 있습니다. 이 할당량은 특정 도메인에 있는 모든 사용자에게 대한 바이트 또는 메일 수를 모두 누적한 값입니다. 도메인 할당량을 설정하려면 사용자의 LDAP 항목에서 `mailDomainDiskQuota` 또는 `mailDomainMsgQuota` 속성을 설정하고(표 18-6 참조) `imquotacheck -f`를 실행합니다.

## 할당량 알림 배포

할당량 알림은 할당량에 가까워질 때 사용자에게 경고 메일을 보내는 프로세스입니다. 이 기능을 사용하려면 다음 세 가지 절차를 수행해야 합니다.

- 575페이지의 “할당량 알림 사용”
- 576페이지의 “할당량 경고 메일 정의”
- 577페이지의 “할당량 임계값 지정”

## 할당량 알림 사용

**콘솔.** 콘솔에서 할당량 알림을 활성화하려면 다음을 수행합니다.

1. 할당량 탭을 누릅니다.
2. "할당량 알림 사용 가능" 상자를 선택합니다. 할당량 알림을 비활성화하려면 이 상자를 선택 취소합니다.
3. 할당량 경고 메일을 정의합니다. 576페이지의 “할당량 경고 메일 정의”를 참조하십시오.
4. 저장을 누릅니다.

**명령줄.** 명령줄에서 할당량 적용을 사용 또는 사용하지 않으려면 다음을 수행합니다.

```
configutil -o store.quotanotification -v [ yes | no ]
```

메일이 설정되지 않은 경우 할당량 경고 메일이 사용자에게 보내지지 않습니다. 할당량 경고 메일 형식의 예는 다음 절을 참조하십시오.

## 할당량 경고 메일 정의

디스크 할당량에 가까워진 사용자에게 보낼 메일을 다음과 같이 정의합니다. 메일은 사용자의 메일함으로 보내집니다.

**콘솔.** 콘솔에서 할당량 경고 메일을 정의하려면 다음을 수행합니다.

1. 할당량 탭을 누릅니다.
2. 드롭다운 목록에서 사용할 언어를 선택합니다.
3. 드롭다운 목록 아래의 메일 텍스트 필드에 보낼 메일을 입력합니다.
4. 저장을 누릅니다.

**명령줄.** 명령줄에서 할당량 경고 메일을 정의하려면 다음을 수행합니다.

```
configutil -o store.quotaexceededmsg -v 'message'
```

메일은 RFC 822 형식이어야 합니다. 즉, 메일은 최소한 제목 행이 들어있는 헤더를 포함하고 그 뒤에 \$\$와 메일 본문이 와야 합니다. "\$"는 새 행을 나타냅니다. 사용 중인 셸에 따라 \$의 특수한 의미를 이스케이프하기 위해 \$ 앞에 \를 추가해야 할 수 있습니다. (\$는 일반적으로 해당 셸의 이스케이프 문자입니다.) 예를 들면 다음과 같습니다.

```
configutil -o store.quotaexceededmsg -v 'Subject: WARNING: User quota exceeded$$User quota threshold exceeded - reduce space used.'
```

또한 다음 변수가 지원됩니다.

[ID] - 사용자 아이디

[DISKUSAGE] - 디스크 사용량

[NUMMSG] - 메일 수

[PERCENT] - store.quotawarn 비율

[QUOTA] - mailquota 속성

[MSGQUOTA] - mailmsgquota 속성

다음은 이러한 변수를 사용한 예입니다.

```
configutil -o store.quotaexceededmsg -v 'Subject: Overquota Warning$$[ID],$$Your mailbox size has exceeded [PERCENT] of its allotted quota.$Disk Usage: [DISKUSAGE]$Number of Messages: [NUMMSG]$Mailquota: [QUOTA]$Message Quota: [MSGQUOTA]$$-Postmaster'
```

경고 메일을 보내는 빈도를 정의하려면 다음을 수행합니다.



```
configutil -o store.quotaexceededmsginterval -v number
```

여기서 *number*는 일 수를 나타냅니다. 예를 들어, 3은 메일이 3일마다 보내진다는 것을 의미합니다.

## 할당량 임계값 지정

할당량 임계값은 클라이언트에게 경고를 보내기 전에 초과된 할당량 비율입니다. 사용자의 디스크 사용량이 지정된 임계값을 초과하면 서버는 사용자에게 경고 메일을 보냅니다.

---

**주** `local.store.quotaoverdraft=on`이면 `store.quotawarn`으로 설정한 임계값에 상관없이 사용자의 디스크 사용량이 할당량의 100%를 초과할 때까지 전자 메일 알림이 트리거되지 않습니다.

---

클라이언트가 IMAP ALERT 기법을 지원하는 IMAP 사용자의 경우 사용자가 메일함을 선택할 때마다 사용자의 화면에 메일이 표시됩니다(또한 IMAP 로그에 메일이 작성됨).

**콘솔.** 콘솔에서 할당량 임계값을 지정하려면 다음을 수행합니다.

1. 할당량 탭을 누릅니다.
2. "할당량 경고 임계값" 필드에 경고 임계값에 해당하는 수를 입력합니다.  
 이 값은 허용되는 할당량의 비율을 나타냅니다. 예를 들어, 90%를 지정할 경우 허용되는 디스크 할당량의 90%를 사용하면 사용자에게 경고 메일이 보내집니다. 기본값은 90%입니다. 이 기능을 해제하려면 100%를 입력합니다.
3. 저장을 누릅니다.

**명령줄.** 명령줄에서 할당량 임계값을 지정하려면 다음을 수행합니다.

```
configutil -o store.quotawarn -v number
```

여기서 *number*는 허용되는 할당량의 비율을 나타냅니다.

## 할당량 적용 활성화 또는 비활성화

기본적으로 사용자 또는 도메인은 할당량을 초과할 수 있으며 할당량 초과 알림(설정된 경우)을 받습니다. 할당량 적용은 디스크 사용량이 할당량 수준 이하로 떨어질 때까지 추가 메일을 받지 않도록 메일함을 잠급니다.

## 사용자 수준으로 할당량 적용 활성화

**콘솔.** 콘솔에서 할당량 적용을 활성화하려면 다음을 수행합니다.

1. 할당량 탭을 누릅니다.
2. "할당량 적용 사용 가능" 상자를 선택합니다. 할당량 적용을 비활성화하려면 이 상자를 선택 취소합니다.
3. 저장을 누릅니다.

**명령줄.** 할당량 적용을 활성화하거나 비활성화하려면 다음을 수행합니다.

```
configutil -o store.quotaenforcement -v [ on | off]
```

할당량 초과 메일이 MTA 대기열에 저장되고 보낸 사람에게 메일이 배달되지 않았지만 나중에 다시 배달 시도가 있을 것임을 나타내는 알림이 전송됩니다. 유예 기간이 만료되어 모든 메일이 보낸 사람에게 되돌아가거나, 디스크 사용량이 할당량 아래로 떨어지고 메일이 MTA 대기열에서 제외되고 메시지 저장소로 배달될 수 있을 때까지 배달 재시도가 계속됩니다. 메일 대기열로 보내기 전에 할당량을 초과한 메일을 돌려보내려면 다음 명령줄을 사용합니다.

```
configutil -o store.overquotastatus -v on
```

## 도메인 수준으로 할당량 적용 활성화

특정 도메인에 대해 할당량을 적용하려면 다음 명령을 사용합니다.

```
imquotacheck -f -d domain
```

모든 도메인에 대해 사용하려면 `-d` 옵션을 제외합니다. 도메인이 할당량을 초과하면 `maildomainstatus` 속성이 `overquota`으로 설정되어 해당 도메인에 대한 모든 전달이 중지됩니다. 도메인이 `overquota`가 아닐 경우 값은 `active`로 설정됩니다.

## 할당량 적용 비활성화

할당량을 비활성화했지만 사용자 할당량이 적용되는 것으로 표시되는 경우 다음 매개 변수를 확인합니다.

다음 `configutil` 매개 변수가 `off`이거나 설정되어 있지 않아야 합니다.

- `store.quotaenforcement`
- `local.store.overquotastatus`
- `local.store.quotaoverdraft`

`store.overquotastatus`가 on일 경우 `store.quotaoverdraft`는 항상 on인 것으로 간주됩니다. 그렇지 않을 경우 사용자가 할당량을 초과하여 거부를 트리거하는 일이 없습니다. 또한 `store.quotaoverdraft`가 on이면 할당량보다 작은 하나의 메일만 사용자에게 허용됩니다. 즉, 사용자의 할당량보다 큰 메일은 허용되지 않습니다.

이 매개 변수를 변경한 후에는 메시징 서비스를 다시 시작해야 합니다.

다음 메시지 저장소 속성을 활성화해야 합니다.

- `maildomainstatus`
- `mailuserstatus`

할당량 적용 구성에 상관없이 메일함 할당량보다 큰 메일은 바운스됩니다.

## 유예 기간 설정

유예 기간은 메일을 보낸 사람에게 다시 바운스하기 전까지 메일함이 할당량(디스크 공간 또는 메일 수)을 초과할 수 있는 기간을 지정합니다. MTA가 메일을 수락하지만 다음 중 하나에 해당할 때까지 메일은 MTA 대기열에 보관되며 메시지 저장소에 전달되지 않습니다.

- 메일이 메일함에 전달되는 시점에 메일함이 더 이상 할당량을 초과하지 않습니다.
- 사용자가 지정된 유예 기간보다 오래 할당량을 초과한 상태로 있습니다. 이 유예 기간이 지나면 서버는 대기열에 포함된 것을 비롯한 모든 메일을 바운스합니다. 이 시간 제한은 `quotagraceperiod configutil` 매개 변수에 의해 제어됩니다.
- 메일이 최대 메일 대기 시간보다 오래 메일 대기열에 남아 있습니다. 이 값은 `notices MTA` 채널 키워드(272페이지의 “알림 메일 전달 간격 설정” 참조)에 의해 제어됩니다.

예를 들어, 유예 기간이 2일로 설정되어 있고 할당량을 1일 동안 초과한 경우 새 메일은 계속 들어와 메일 대기열에 보관되며 전달 시도도 계속됩니다. 2일 이후에 메일이 보낸 사람에게 바운스됩니다.

---

**주** 유예 기간은 메일이 메일 대기열에 보관되는 기간이 아니라 메일 대기열에 있는 메일을 비롯하여 모든 받는 메일이 바운스되기 전까지 메일함의 할당량을 초과할 수 있는 기간입니다. 사용자가 할당량 임계값에 도달하면 유예 기간이 시작됩니다. [577페이지의 “할당량 임계값 지정”](#)을 참조하십시오.

---

**콘솔.** 콘솔에서 메일이 대기열에 보관되는 기간에 대한 유예 기간을 설정하려면 다음을 수행합니다.

1. 할당량 탭을 누릅니다.
2. "할당량 유예 기간 초과" 필드에 숫자를 입력합니다.
3. 드롭다운 목록에서 Day(s) 또는 Hour(s)를 지정합니다.
4. 저장을 누릅니다.

**명령줄.** 명령줄에서 할당량 유예 기간을 지정하려면 다음을 수행합니다.

```
configutil -o store.quotagraceperiod -v number
```

여기서 *number*는 시간을 나타냅니다.

## Netscape Messaging Server 할당량 호환 모드

Netscape Messaging Server에서는 디스크 사용량이 할당량을 초과한 경우 메일 전달을 지연 또는 바운스하고 할당량 초과 알림을 보낸 다음 유예 기간을 시작했습니다.

Messaging Server는 이 동작을 유지하는 `local.store.quotaoverdraft` 매개 변수를 제공합니다.

ON으로 설정하면 디스크 사용량이 할당량을 초과할 때까지 메일이 전달됩니다. 할당량을 초과하면 메일이 지연되고(메일은 MTA 메일 대기열에 보관되지만 메시지 저장소로 전달되지 않음) 할당량 초과 경고 메일이 사용자에게 보내지며 유예 기간이 시작됩니다. 유예 기간은 할당량 초과 메일이 바운스될 때까지 메일함의 할당량이 초과되어 있는 기간을 결정합니다. 기본값은 메시지 저장소가 임계값에 도달할 때 할당량 경고 메일을 보냅니다. 이 매개 변수의 기본값은 off입니다.

## 자동 메일 제거(만료 및 제거) 기능 설정

자동 메일 제거 기능(만료 및 제거라고도 함)은 관리자가 정의한 일련의 기준을 기반으로 메시지 저장소에서 메일을 자동으로 제거합니다. 이전 메일이나 과도하게 큰 메일, 보았거나 삭제한 메일, 특정 제목을 가진 메일 등을 자동으로 제거하는 데 자동으로 제거하는 데 이 기능을 사용할 수 있습니다. 이 기능은 다음 제거 기준을 허용합니다.

- 폴더(메일함), 사용자, 도메인, 전체 메시지 저장소 또는 특정 분할 영역별
- 메일함의 메일 수
- 메일함의 총 크기
- 메일이 메일함에 남아 있는 기간(일)
- 메일 크기와 유예 기간(크기를 초과한 메일이 제거되기 전에 메시지 저장소에 남아 있는 일 수)
- 메일에 *조회* 또는 *삭제됨* 플래그가 지정되었는지 여부
- 헤더 문자열

이 기능은 메일을 정리 및 제거하는 `imexpire` 유틸리티에 의해 수행됩니다. 메일 제거 프로세스에 대한 자세한 내용은 [556페이지](#)의 “메시지 저장소에서 메일을 제거하는 방법”을 참조하십시오.

---

**주** 서버는 경고 없이 메일을 제거하므로 자동 메일 제거 정책을 사용자에게 알리는 것이 중요합니다. 메일이 갑작스럽게 제거되면 사용자와 관리자가 매우 당황할 수 있습니다.

---

### `imexpire` 작동 원리

`imexpire`는 명령줄에서 호출하거나 `imsched` 데몬에 의해 자동으로 실행되도록 예약할 수 있습니다. 관리자는 콘솔이나 `configutil` 명령줄 유틸리티를 사용하여 전역 만료 규칙(전체 메시지 저장소에 대한 규칙)을 구성합니다. 로컬 만료 규칙(폴더나 사용자에게 적용되는 규칙)은 메시지 저장소 분할 영역, 사용자 또는 메일함 디렉토리에서 만료 규칙 파일(`store.expire`)을 만들어 구성할 수 있습니다.

imexpire는 시작 시에 모든 만료 규칙을 로드합니다. 기본적으로 imexpire는 분할 영역당 하나의 스레드를 만듭니다. 각 스레드는 할당된 분할 영역 아래의 사용자 폴더 목록을 거치는 과정에서 로컬 만료 규칙 파일을 로드합니다. 이 만료 기능은 각 폴더에 적용 가능한 만료 규칙에 대해 해당 폴더를 검사하고 필요에 따라 메일을 정리합니다. 메일함 디렉토리에 store.exp 파일이 있고 store.cleanupage 구성 매개 변수에 지정된 시간보다 오랫동안 정리/만료된 메일이 있을 경우 제거 기능은 메일 해시 디렉토리의 모든 메일 파일을 영구적으로 제거하고 store.exp 파일에서 uid 레코드를 제거합니다.

또한 msg\_svr\_base/config/의 expire\_exclude\_list라는 파일에 한 행에 하나씩 사용자 아이디를 추가하여 지정된 사용자를 만료 규칙에서 제외할 수 있습니다.

## 자동 메일 제거 기능 배포

자동 메일 제거는 명령줄이나 콘솔 GUI를 사용하여 배포할 수 있습니다. 이 프로세스는 다음 세 단계로 구성됩니다.

1. 자동 메일 제거 정책을 정의합니다. 자동으로 제거할 메일은 무엇입니까? 메일이 자동으로 제거될 사용자, 도메인 및 분할 영역은 무엇입니까? 제거 기준을 정의하는 크기, 메일 기간 및 헤더는 무엇입니까? [582페이지의 “자동 메일 제거 정책 정의”](#)를 참조하십시오.
2. 이 정책을 구현하기 위한 imexpire 규칙을 지정합니다. [583페이지의 “자동 메일 제거 정책을 구현하는 규칙 설정”](#)을 참조하십시오.
3. imexpire 일정을 지정합니다. [591페이지의 “자동 메일 제거 및 로깅 수준 예약”](#)을 참조하십시오.

### 자동 메일 제거 정책 정의

제거 기준을 지정하여 자동 메일 제거 정책을 정의합니다. imexpire에서는 다음 기준을 제거에 사용할 수 있습니다.

**메일 기간.** X일보다 오래된 메일을 자동으로 제거합니다(속성: messagedays).

**메일 수.** X개의 메일을 초과하는 폴더의 메일을 자동으로 제거합니다(속성: messagecount).

**크기를 초과하는 메일의 기간.** Y일의 유예 기간 후에 X바이트를 초과한 메일을 자동으로 제거합니다(속성: messagesize 및 messagesizedays).

**조회 및 삭제됨 메일 플래그.** *조회* 또는 *삭제됨* 플래그가 설정된 메일을 자동으로 제거합니다. 이러한 기준은 "and" 또는 "or"로 설정될 수 있습니다. or로 설정될 경우 메일의 조회/삭제 플래그는 다른 기준에 상관 없이 메일을 자동으로 삭제합니다. and로 설정된 경우 지정된 다른 모든 기준을 충족하면서 메일의 조회/삭제 플래그를 설정해야 합니다(속성: seen 및 deleted).

**메일의 헤더 필드.** 메일 제거 기준으로 사용할 헤더와 문자열을 지정할 수 있습니다(예: "Subject: Work from Home!"이라는 헤더를 가진 모든 메일 제거).

**메일 폴더.** 메일을 제거할 폴더를 지정할 수 있습니다(속성: folderpattern).

---

**주** imexpire에서는 메일을 읽은 후로 경과한 시간에 따라 메일을 삭제하거나 보존하도록 허용하지 않습니다. 예를 들어, 200일 동안 읽지 않은 메일을 제거하도록 지정할 수 없습니다.

---

### 자동 메일 제거 정책의 예

예 1: 1,000개의 메일을 초과하는 폴더에서 365일이 지난 모든 메일을 제거합니다.

예 2: siroe.com 도메인에서 180일이 지난 메일을 제거합니다.

예 3: *삭제됨*으로 표시된 모든 메일을 제거합니다.

예 4: *조회*표시가 있고 30일이 지났으며 100KB보다 크고 폴더의 메일 수가 1,000개를 초과하며 x-spam 헤더가 있는 메일을 sesta.com에서 제거합니다.

### 자동 메일 제거 정책을 구현하는 규칙 설정

이전 절에서 정의한 자동 메일 제거 정책을 구현하려면 imexpire 규칙을 설정해야 합니다. 규칙은 다음과 같이 설정됩니다.

- GUI 사용([589페이지의 그림 18-4](#) 참조)

- `store.expirerule` 파일에 규칙 포함. 다음은 두 개의 `store.expirerule` 규칙을 보여주는 예입니다.

```
Rule1.folderpatter: user/.*/trash
Rule1.messagedays: 2
Rule2.folderpattern: user/.*
Rule2.messagedays: 14
```

이 예에서 Rule 1은 휴지통 폴더의 모든 메일이 2일 후에 제거되도록 지정합니다. Rule 2는 메시지 저장소의 모든 메일이 14일 후에 제거되도록 지정합니다.

이 절은 다음과 같은 하위 절로 구성되어 있습니다.

- [584페이지의 “만료 규칙 지침”](#)
- [586페이지의 “텍스트 형식으로 imexpire 규칙 설정”](#)
- [587페이지의 “imexpire 폴더 패턴 설정”](#)
- [588페이지의 “콘솔을 사용하여 자동 메일 제거 규칙 설정”](#)

### 만료 규칙 지침

이 절에서는 `store.expirerule` 파일 규칙에 대한 지침을 설정합니다.

---

**주** 이전의 Messaging Server 릴리스에서는 `configutil` 매개 변수 `store.expirerule.attribute`를 사용하여 만료 규칙을 설정할 수 있었습니다 (*Sun Java System Messaging Server Administration Reference* 참조). 이는 여전히 유효하지만 헤더 제약 조건을 사용하는 만료 규칙(예: 특정 제목 행을 가진 메일을 만료하는 것)은 지원되지 않습니다. 이러한 이유 때문에 콘솔 GUI나 `store.expirerule` 파일 규칙을 사용하는 것이 더 나을 수 있습니다.

---

- 규칙은 `store.expirerule`이라는 파일에 지정됩니다.
- 동일한 규칙을 사용하여 여러 만료 기준을 지정할 수 있습니다(위의 예를 참조).
- 규칙은 전체 메시지 저장소(전역 규칙), 메시지 저장소 분할 영역, 사용자 또는 폴더에 적용할 수 있습니다. 비전역 규칙은 `store.expirerule` 규칙을 통해서만 만들 수 있습니다.
  - 전역 규칙은 `configutil` 매개 변수 `store.expirerule.rulename.attribute`를 사용하거나 `msg_svr_base/config/store.expirerule`에서 규칙을 지정하여 만듭니다.



- 분할 영역 규칙은 `store_root/partition/partition_name/store.expirerule`에서 규칙을 지정하여 만들 수 있습니다.
- 사용자 규칙은 `store_root/partition/partition_name/userid/store.expirerule`에서 규칙을 지정하거나 `folderpattern` 규칙이 `user/userid/.*`가 되도록 지정하여 만들 수 있습니다.
- 폴더 규칙은 `store_root/partition/partition_name/userid/folder/store.expirerule`에서 규칙을 지정하거나 `folderpattern` 규칙이 `user/userid/folder`가 되도록 지정하여 만들 수 있습니다.

**주** 또한 `folderpattern` 속성을 지정하여 사용자와 폴더 규칙을 전역 만료 파일(`msg_svr_base/config/store.expirerule`)에 포함시킬 수도 있습니다.

- 여러 만료 규칙을 메일함에 동시에 적용할 수 있습니다. 메일함에 대한 만료 규칙은 전역 규칙 및 로컬 규칙으로 구성됩니다. 로컬 규칙은 같은 디렉토리외 해당하는 모든 하위 폴더의 메일함에 적용됩니다.
- `imexpire`는 이 메일함에 대해 지정된 배타적 규칙이 없을 경우 메일함에 적용되는 모든 만료 규칙을 통합합니다(표 18-8 참조). 결과 규칙 집합은 적용 가능한 모든 규칙을 기반으로 하는 가장 제한적인 만료 정책을 나타냅니다. 예를 들어, 메일이 만료되는 최대 메일 기간을 규칙 X가 10일로 지정하고 규칙 Y가 5일로 지정할 경우 통합 결과는 5일이 됩니다.

**표 18-8** `imexpire` 속성

| 속성                         | 설명(속성 값)                                                                                                                                                                                                                                                                |
|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>exclusive</code>     | 해당 규칙이 배타적인지 여부를 지정합니다. <code>exclusive</code> 로 지정된 경우 해당 규칙만 지정된 메일함에 적용되며 다른 모든 규칙은 무시됩니다. 둘 이상의 배타적인 규칙이 존재할 경우 마지막으로 로드된 규칙이 사용됩니다. 예를 들어, 전역 및 로컬 배타적인 규칙을 지정할 경우 로컬 규칙이 사용됩니다. 둘 이상의 배타적인 전역 규칙이 있을 경우 <code>configutil</code> 에서 나열한 마지막 전역 규칙이 사용됩니다. (yes/no) |
| <code>folderpattern</code> | 해당 규칙의 영향을 받는 폴더를 지정합니다. 형식은 <code>store_root/partition/*/</code> 디렉토리를 나타내는 <code>user/</code> 로 시작해야 합니다. 589페이지의 그림 18-4 및 587페이지의 표 18-9를 참조하십시오(POSIX 정규 표현식).                                                                                                     |
| <code>messagecount</code>  | 폴더의 최대 메일 수입니다. 추가 메일이 전달되면 가장 오래된 메일이 정리됩니다. (정수)                                                                                                                                                                                                                      |
| <code>foldersize</code>    | 추가 메일이 전달되었을 때 가장 오래된 메일이 정리되기 전까지의 최대 폴더 크기입니다. (바이트 단위 정수)                                                                                                                                                                                                            |
| <code>messagedays</code>   | 메일이 정리되기 전까지의 메일 기간(일)입니다. (정수)                                                                                                                                                                                                                                         |
| <code>messagesize</code>   | 메일이 정리되는 것으로 표시되기 전까지의 메일의 최대 크기(바이트)입니다. (정수)                                                                                                                                                                                                                          |

**표 18-8** imexpire 속성

| 속성                          | 설명(속성 값)                                                                                                                                                                                                                                                                               |
|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| messagesize                 | 유예 기간입니다. 크기를 초과한 메일이 폴더에 남아 있어야 하는 일 수입니다. (정수)                                                                                                                                                                                                                                       |
| <i>message header field</i> | 제거할 메일을 표시하는 헤더 필드와 문자열을 지정합니다. 값은 대소문자를 구분하지 않으며 정규 표현식은 인식되지 않습니다.<br>예: Rule1.Subject: Get Rich Now!<br><br><i>Expires</i> 및 <i>Expiry-Date</i> 헤더의 경우 imexpire는 이러한 헤더 필드로 지정한 날짜 값이 <i>messagedays</i> 속성보다 오래 되었으면 메일을 제거합니다. 여러 개의 만료 헤더 필드를 지정한 경우에는 가장 이른 만료 날짜가 사용됩니다. (문자열) |
| regex                       | 규칙 작성에 UNIX 정규 표현식을 사용 가능하게 합니다. (1 또는 0) 지정하지 않으면 IMAP 표현식이 사용됩니다.                                                                                                                                                                                                                    |
| seen                        | seen은 사용자가 메일을 열었을 때 시스템에 의해 설정되는 메일 상태 플래그입니다. seen 속성이 and로 설정된 경우 메일을 보는 것 <b>외에도</b> 다른 기준을 충족해야 규칙이 적용됩니다. seen 속성이 or로 설정된 경우 메일을 보았거나 <b>또는</b> 다른 기준을 충족하면 규칙이 적용됩니다. (and/or)                                                                                                 |
| deleted                     | deleted는 사용자가 메일을 삭제했을 때 시스템에 의해 설정되는 메일 상태 플래그입니다. deleted 속성이 and로 설정된 경우 메일을 삭제한 것 <b>외에도</b> 다른 기준을 충족해야 규칙이 적용됩니다. deleted 속성이 or로 설정된 경우 메일을 삭제했거나 <b>또는</b> 다른 기준을 충족하면 규칙이 적용됩니다. ( <b>and/or</b> )                                                                            |

### 텍스트 형식으로 imexpire 규칙 설정

자동 메일 제거 규칙은 store.expirerule 파일에서 규칙을 지정하여 설정합니다. store.expirerule 파일에는 한 행에 하나씩 만료 기준이 있습니다. 전역 규칙 구성 파일 (*msg\_svr\_base/data/store/store.expirerule*)의 만료 기준의 형식은 다음과 같습니다.

*rule\_name.attribute: value*

**코드 예 18-1**에서는 *msg\_svr\_base/config/store.expirerule*의 만료 규칙 집합을 보여줍니다.

Rule 1은 다음과 같이 전역 만료 정책(즉, 모든 메일에 적용되는 정책)을 설정합니다.

- 규칙 작성에 UNIX 정규 표현식을 사용 가능하게 합니다.
- 3일이 지난 100,000바이트를 초과하는 메일을 제거합니다.
- 사용자가 삭제한 메일을 제거합니다.
- Subject: 헤더에 "Vigara Now!" 또는 "XXX Porn!"라는 문자열이 있는 메일을 제거합니다.

- 모든 폴더의 메일 수를 1,000개로 제한합니다. 메일이 1,000개를 넘으면 시스템은 폴더에서 가장 오래된 메일을 제거하여 합계를 1,000개로 유지합니다.
- 365일이 지난 모든 메일을 제거합니다.

Rule 2는 호스트된 도메인 `siroe.com`에서 사용자에게 대한 자동 메일 제거 정책을 설정합니다. 이 규칙은 메일함 크기를 1MB로 제한하고 삭제된 메일을 제거하며 14일이 지난 메일을 제거합니다.

Rule 3은 `f.dostoevski` 사용자의 `inbox` 폴더에 있는 메일에 대한 자동 메일 제거 정책을 설정합니다. 이 규칙은 제목행에 "On-line Casino" 표현이 있는 메일을 제거합니다.

**코드 예 18-1** imexpire 규칙 예

```
Rule1.regex: 1
Rule1.folderpattern: user/. *
Rule1.messagesize: 100000
Rule1.messagesizedays: 3
Rule1.deleted: or
Rule1.Subject: Vigara Now!
Rule1.Subject: XXX Porn!
Rule1.messagecount: 1000
Rule1.messagedays: 365
Rule2.regex: 1
Rule2.folderpattern: user/. *@siroe.com/. *
Rule2.exclusive: yes
Rule2.deleted: or
Rule2.messagedays: 14
Rule2.messagecount: 1000
Rule3.folderpattern: user/f.dostoevski/inbox
Rule3.Subject: *On-line Casino*
```

### imexpire 폴더 패턴 설정

POSIX 정규 표현식을 사용하여 `imexpire` 속성 `regex`를 1로 설정함으로써 폴더 패턴을 지정할 수 있습니다. 지정하지 않으면 IMAP 표현식이 사용됩니다. `user/`로 시작되고 뒤에 패턴이 나오는 형식이어야 합니다. 표 18-9에서는 여러 폴더에 대한 폴더 패턴을 보여줍니다.

**표 18-9** 정규 표현식을 사용한 `imexpire` 폴더 패턴

| 폴더 패턴                         | 범위                                               |
|-------------------------------|--------------------------------------------------|
| <code>user/userid/. *</code>  | <code>userid</code> 의 모든 폴더에 있는 모든 메일에 적용됩니다.    |
| <code>user/userid/Sent</code> | Sent 폴더에 있는 <code>userid</code> 의 메일에 규칙을 적용합니다. |
| <code>user/. *</code>         | 메시지 저장소 전체에 규칙을 적용합니다.                           |
| <code>user/. */trash</code>   | 모든 사용자의 <code>trash</code> 폴더에 규칙을 적용합니다.        |

**표 18-9** 정규 표현식을 사용한 imexpire 폴더 패턴

| 폴더 패턴                             | 범위                                 |
|-----------------------------------|------------------------------------|
| <code>user/.*@siroe.com/.*</code> | 호스트된 도메인 siroe.com의 폴더에 규칙을 적용합니다. |
| <code>user/[^@]*/.*</code>        | 기본 도메인에 있는 폴더에 규칙을 적용합니다.          |

### 콘솔을 사용하여 자동 메일 제거 규칙 설정

1. 다음과 같이 자동 메일 제거 GUI를 엽니다.

주 콘솔 > 서버 그룹 > Messaging Server (열기) > Messaging Server 콘솔 > 구성 탭 > 메시지 저장소 > 만료/제거 > 추가

그림 18-4에는 대략적인 GUI 그림이 나와 있습니다.

그림 18-4 자동 메일 제거(만료/제거) GUI—대략적인 그림

이름 :

다음 패턴과 일치하는 폴더에 적용됩니다.

배타적  
위에서 지정한 패턴과 일치하는 폴더에 대한 배타적인 규칙을 만드십시오.

폴더 크기 제약 조건  
다음 조건이 true인 경우 가장 오래된 메일을 제거하십시오.  
 메일 수 :   
 폴더 크기 :

메일 기간 제약 조건  
다음 조건이 true인 경우 가장 오래된 메일을 제거하십시오.  
 일 수 :  일

메일 크기 제약 조건  
지정된 크기보다 크거나 유예 기간보다 오래된  
폴더의 메일을 제거하십시오.  
 메일 크기 제한 :    
 유예 기간 :  일

메일 플래그 제약 조건  
다음 플래그 값에 따라 메일을 제거하십시오.  
 조회 :   
 삭제됨 :

헤더 제약 조건  
선택으로 구분된 사용자 정의 헤더 값을 입력하십시오.

2. 새 규칙의 이름을 입력합니다.
3. 메일이 자동으로 제거될 폴더를 입력합니다.

587페이지의 “imexpire 폴더 패턴 설정”을 참조하십시오.

4. 이 규칙이 지정된 기준과 일치하는 폴더에 대한 배타적인 규칙일 경우 *배타적* 상자를 선택합니다.  
이 상자를 선택한 경우 지정된 패턴과 일치하는 다른 모든 규칙보다 이 규칙이 우선합니다. 배타적 확인란에 대한 자세한 내용은 [585페이지의 표 18-8](#)을 참조하십시오.
5. 폴더 크기에 기반한 규칙을 만들려면 다음을 수행합니다.
  - 폴더 크기 제약 조건 확인란을 선택합니다. 메일 수 필드에 가장 오래된 메일이 제거되기 전에 폴더에 남아 있는 최대 메일 수를 지정합니다. 폴더 크기 필드에서 가장 오래된 메일이 제거되기 전의 최대 폴더 크기를 바이트로 지정합니다.
6. 메일 기간에 기반한 규칙을 만들려면 메일 기간 제약 조건 확인란을 선택합니다.  
일 수 필드에 메일이 폴더에 남아 있어야 하는 기간(일)을 지정합니다.
7. 메일 크기를 기반으로 규칙을 만들려면 다음을 수행합니다.
  - 메일 크기 제한 제약 조건 확인란을 선택합니다. 메일 크기 제한 필드에 폴더에 허용되는 최대 메일 크기를 입력합니다. "유예 기간" 필드에 크기를 초과한 메일이 제거되기 전에 폴더에 남아 있는 기간을 입력합니다.
8. 조회 또는 삭제됨 메일 플래그가 설정되었는지에 기초하여 규칙을 만들려면 다음을 수행합니다.
  - 메일 플래그 제약 조건 확인란을 선택합니다.
  - 조회: 필드의 경우 메일을 보는 것 **및** 다른 기준을 충족해야 규칙이 적용되도록 지정하려면 "및"을 선택합니다. 메일을 보았거나 **또는** 다른 기준을 충족하면 규칙이 적용되도록 지정하려면 "또는"을 선택합니다.
  - 삭제됨: 필드의 경우 메일을 삭제한 것 **및** 다른 기준을 충족해야 규칙이 적용되도록 지정하려면 "또는"을 선택합니다. 메일을 삭제했거나 **또는** 다른 기준을 충족하면 규칙이 적용되도록 지정하려면 "또는"을 선택합니다.
9. 헤더 필드와 그 값에 기초하여 규칙을 만들려면 다음을 수행합니다.
  - 헤더 제약 조건 확인란을 선택합니다.

- 선택표로 구분된 헤더 및 값 목록을 다음 형식으로 입력합니다.

*header1: value1, header2: value2*

예: Subject: Work at Home!, From: virus@sesta.com

*Expires*와 *Expiry-Date* 헤더의 경우 시스템은 해당 날짜 값이 메일 기간 제약 조건보다 오래된 경우 메일을 제거합니다. 여러 개의 만료 헤더 필드를 지정한 경우에는 가장 이른 만료 날짜가 사용됩니다. (문자열)

10. 확인을 눌러 새 규칙을 자동 메일 제거 목록에 추가합니다.

## 자동 메일 제거 및 로깅 수준 예약

자동 메일 제거는 `imsched` 예약 데몬에 의해 활성화됩니다. 기본적으로 `imsched`는 매일 23시에 `imexpire`를 호출하여 메일을 정리 및 제거합니다. 표 18-10에 설명된 `configutil` 매개 변수 `local.schedule.expire`, `local.schedule.purge` 및 `store.cleanuppage`를 설정하여 이 일정을 사용자 정의할 수 있습니다.

메시지 저장소가 큰 경우 만료와 제거를 완료하는 데 시간이 걸릴 수 있으므로 이러한 프로세스를 실행하는 빈도를 실험하여 결정하는 것이 필요할 수 있습니다. 예를 들어, 만료/제거 주기가 10시간일 경우 만료 및 제거를 하루에 한 번씩 실행하도록 기본 일정을 세우는 것을 잊을 것입니다. `local.schedule.purge`를 사용하여 별개의 제거 일정을 지정하는 방법으로 만료 및 제거를 예약합니다. `local.schedule.purge`를 설정하지 않을 경우 `imexpire`는 만료 후에 제거를 수행합니다.

**표 18-10** 만료 및 제거 configutil 로그 및 예약 매개 변수

| 매개 변수                       | 설명                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| local.schedule.expire       | <p>imexpire를 실행하는 간격입니다. 다음 UNIX crontab 형식을 사용합니다.<br/><i>minute hour day-of-month month-of-year day-of-week</i></p> <p>값은 공백이나 탭으로 구분하며 각각 0-59, 0-23, 1-31, 1-12 또는 0-6(0=일요일)의 값을 사용할 수 있습니다. 각 시간 필드에는 별표(유효한 모든 값), 쉼표로 구분된 값 목록 또는 하이픈으로 구분된 두 값의 범위를 사용할 수 있습니다. 날짜는 일과 요일 모두를 사용하여 지정할 수 있지만 둘 다 일치하는 경우가 매우 드물기 때문에 일반적이지 않습니다. 일과 요일을 모두 지정한 경우에는 둘 다 필요합니다. 예를 들어, 17일과 화요일을 설정하면 두 값이 모두 true가 되어야 합니다.</p> <p><b>간격 예:</b></p> <ol style="list-style-type: none"> <li>오전 12:30, 8:30 및 오후 4:30에 imexpire를 실행합니다.<br/>30 0,8,16 * * * /opt/SUNWmsgsr/lib/imexpire</li> <li>주중 아침 3:15에 imexpire를 실행합니다.<br/>15 3 * * 1-5 /opt/SUNWmsgsr/lib/imexpire</li> <li>월요일에만 imexpire를 실행합니다.<br/>0 0 * * 1 /opt/SUNWmsgsr/lib/imexpire</li> </ol> <p>기본값: 0 23 * * * /opt/SUNWmsgsr/lib/imexpire</p> |
| local.schedule.purge        | <p>purge를 실행하는 간격입니다. 다음 UNIX crontab 형식을 사용합니다.<br/><i>minute hour day-of-month month-of-year day-of-week</i></p> <p>기본값: 0 0,4,8,12,16,20 * * * /opt/SUNWmsgsr/lib/purge -num=5 (4시간마다)</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| store.cleanupage            | <p>만료 또는 정리된 메일이 purge에 의해 영구적으로 제거된 전까지의 기간(시간)입니다.</p> <p>기본값: 없음</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| local.store.expire.loglevel | <p>다음과 같이 로그 수준을 지정합니다.</p> <ol style="list-style-type: none"> <li>전체 만료 세션의 요약을 기록합니다.</li> <li>만료된 메일함별로 하나씩 메일을 기록합니다.</li> <li>만료된 메일별로 하나씩 메일을 기록합니다.</li> </ol> <p>기본값: 1</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

### 콘솔을 사용하여 imexpire 예약

다음과 같이 자동 메일 제거 GUI를 엽니다.

주 콘솔 > 서버 그룹 > Messaging Server (열기) > Messaging Server 콘솔 > 구성 탭 > 메시지 저장소 > 만료/제거



이 콘솔 페이지의 위쪽에는 만료 규칙이, 아래쪽에는 만료 및 제거 일정이 나열됩니다. 만료 및 제거를 예약하려면 만료/제거 일정의 풀다운 메뉴를 사용하여 만료 및 제거의 월, 일, 요일(0=일요일), 시간 및 분을 설정합니다.

---

**주** 일 값은 일과 요일을 모두 사용하여 설정할 수 있습니다. 일과 요일을 모두 설정하면 둘 다 적용됩니다. 예를 들어, 수요일과 17일을 설정하면 제거/만료는 각 달의 17일 중에서 수요일에 해당하는 날짜에만 발생합니다.

---

### *imexpire* 로깅 수준 설정

*imexpire*는 완료 시에 기본 로그 파일에 대한 요약を 기록합니다. 명령줄에서 만료가 호출 될 경우 `-v(verbose)` 및 `-d(debug)` 옵션을 사용하여 자세한 상태/디버그 메시지를 `stderr` 에 기록하도록 *imexpire*에 지시할 수 있습니다. *imexpire*가 *imsched*에 의해 호출될 경우 `configutil` 매개 변수 `local.store.expire.loglevel`를 여러 다른 로깅 수준에 대해 1, 2 또는 3으로 설정할 수 있습니다. `Loglevel 1`은 기본값으로 전체 만료 세션의 요약을 기록합니다. `Loglevel 2`는 만료된 메일함별로 하나씩의 메일을 기록합니다. 마지막으로 `Loglevel 3`은 만료된 메일별로 하나씩의 메일을 기록합니다.

### 자동 메일 제거에서 지정된 사용자 제외

`msg_svr_base/config/`의 `expire_exclude_list`라는 파일에 한 행에 하나씩 사용자 아이디를 추가하여 지정된 사용자를 만료 규칙에서 제외합니다.

## 메시지 저장소 분할 영역 구성

메일함은 전적으로 메시지 저장소를 저장하는 디스크 분할 영역의 한 영역인 메시지 저장소 분할 영역에 저장됩니다. 메시지 저장소 분할 영역은 디스크 분할 영역과 다르지만 유지 관리가 용이하도록 각 메시지 저장소 분할 영역에 대해 하나의 디스크 분할 영역과 하나의 파일 시스템을 가지는 것이 좋습니다. 메시지 저장소 분할 영역은 특별히 메시지 저장소로 지정된 디렉토리입니다.

사용자 메일함은 기본적으로 `store_root/partition/` 디렉토리에 저장됩니다([554페이지의 그림 18-1](#) 참조). `partition` 디렉토리는 하나 또는 여러 개의 분할 영역을 포함할 수 있는 논리 디렉토리입니다. 시작 시에 `partition` 디렉토리는 `primary` 분할 영역이라는 하나의 하위 분할 영역을 포함합니다.

필요에 따라 분할 영역을 `partition` 디렉토리에 추가할 수 있습니다. 예를 들어, 단일 디스크를 분할하여 다음과 같이 사용자를 구성할 수 있습니다.

```
store_root/partition/mkting/  
store_root/partition/eng/  
store_root/partition/sales/
```

디스크 저장소 요구 사항이 늘어나면 이러한 분할 영역을 다른 물리적 디스크 드라이브에 매핑할 수 있습니다.

한 디스크의 메일함 수를 제한해야 합니다. 여러 디스크로 메일함을 분산시키면 메일 전달 시간이 향상됩니다(SMTP 수락율을 변경할 필요는 없음). 디스크별로 할당하는 메일함 수는 디스크 용량과 각 사용자에게 할당되는 디스크 공간에 따라 다릅니다. 예를 들어, 사용자별로 더 적은 디스크 공간을 할당할 경우 디스크별로 더 많은 메일함을 할당할 수 있습니다.

메시지 저장소에 여러 디스크가 필요한 경우 RAID(Redundant Array of Inexpensive Disks) 기술을 사용하여 편리하게 여러 디스크를 관리할 수 있습니다. RAID 기술을 사용하면 일련의 디스크에서 데이터를 분산시킬 수 있지만 디스크가 하나의 논리 볼륨으로 나타나므로 관리가 간단해집니다. 또한 오류 복구 목적으로 저장소를 복제하기 위해(즉, 중복을 위해) RAID 기술을 사용할 수도 있습니다.

---

**주** 디스크 액세스를 향상시키려면 메시지 저장소와 메일 대기열이 별개의 디스크에 상주해야 합니다.

---

## 분할 영역 추가

분할 영역을 추가할 때는 디스크상에 분할 영역이 저장되는 절대 물리 경로와 논리 이름(분할 영역 별명이라고 함)을 지정합니다.

분할 영역 별명을 사용하면 물리 경로에 상관 없이 사용자를 논리 분할 영역 이름에 매핑할 수 있습니다. 사용자 계정을 설정하고 사용자의 메시지 저장소를 지정할 때 분할 영역 별명을 사용할 수 있습니다. 입력하는 이름은 소문자를 사용하는 알파벳 이름이어야 합니다.

분할 영역을 작성 및 관리하려면 서버를 실행하는 데 사용되는 사용자 아이디가 물리 경로에 지정된 위치에 쓸 수 있는 권한을 가져야 합니다.

---

**주** 분할 영역을 추가한 후에 서버를 중지했다가 다시 시작하여 구성 정보를 갱신해야 합니다.

---

**콘솔.** 콘솔을 사용하여 분할 영역을 저장소에 추가하려면 다음을 수행합니다.

1. 콘솔에서 구성할 Messaging Server를 엽니다.

2. 구성 탭을 누르고 왼쪽 표시 영역에서 메시지 저장소를 선택합니다.
3. 오른쪽 표시 영역에서 분할 영역 탭을 누릅니다.
4. 추가 버튼을 누릅니다.
5. 분할 영역 별명을 입력합니다.  
이 이름은 지정된 분할 영역의 논리 이름입니다.
6. 분할 영역 경로를 입력합니다.  
이 경로는 지정된 분할 영역의 절대 경로 이름입니다.
7. 이 경로를 *기본 메시지 저장소 분할 영역*으로 지정하려면 여기를 기본 분할 영역으로 선택 상자를 누릅니다.

---

**주** 기본 분할 영역은 사용자를 만들 때 사용자 항목에 `mailMessageStore` LDAP 속성을 지정하지 않는 경우에 사용되는 분할 영역입니다. 기본 분할 영역이 필요하지 않도록 `mailMessageStore` LDAP 속성을 모든 사용자 항목에 지정해야 합니다.

---

8. 확인을 눌러 이 분할 영역 구성 항목을 제출하고 창을 닫습니다.
9. 저장을 눌러 현재 분할 영역 목록을 제출하고 보존합니다.

**명령줄.** 명령줄에서 분할 영역을 저장소에 추가하려면 다음을 수행합니다.

```
configutil -o store.partition.nickname.path -v path
```

여기서 `nickname`은 분할 영역의 논리 이름이고 `path`는 분할 영역이 저장되는 절대 경로 이름을 나타냅니다.

기본 주 분할 영역의 경로를 지정하려면 다음을 수행합니다.

```
configutil -o store.partition.primary.path -v path
```

## 메일함을 다른 디스크 분할 영역으로 이동

기본적으로 메일함은 `primary` 분할 영역에 만들어집니다. 분할 영역이 가득 차면 추가 메일을 저장할 수 없습니다. 이 문제는 다음의 여러 방법으로 해결할 수 있습니다.

- 사용자 메일함의 크기를 줄입니다.
- 볼륨 관리 소프트웨어를 사용하는 경우 디스크를 추가합니다.

- 추가 분할 영역을 만들고(594페이지의 “분할 영역 추가” 참조) 메일함을 새 분할 영역으로 이동합니다.

볼륨 관리 소프트웨어를 사용하여 시스템에 다른 디스크 공간을 추가하는 것이 사용자에게 가장 투명한 절차이기 때문에 가능하면 이 방법을 사용하는 것이 좋습니다. 그러나 다음을 수행하여 메일함을 다른 분할 영역으로 이동할 수도 있습니다.

1. 마이그레이션하는 도중에 사용자가 메일함과 연결되지 않게 합니다. 이렇게 하려면 사용자에게 로그오프하고 메일함을 이동하는 동안 메일함을 사용하지 않도록 지시하거나 사용자가 로그오프한 후에 POP, IMAP 및 HTTP 서비스를 허용하지 않도록 `mailAllowedServiceAccess` 속성을 설정합니다. *Sun Java System Communications Services Schema Reference Manual*을 참조하십시오.

---

**주** POP, IMAP 및 HTTP 액세스를 허용하지 않도록 `mailAllowedServiceAccess`를 설정해도 메일함에 대한 열린 연결이 끊기지 않습니다. 따라서 메일함을 이동하기 전에 모든 연결이 닫혔는지 확인해야 합니다.

---

2. 다음 명령을 사용하여 사용자 메일함을 이동합니다.

```
mboxutil -r user/<userid>/INBOX user/<userid>/INBOX <partition_name>
```

```
mboxutil -r user/ofanning/INBOX user/ofanning/INBOX secondary
```

3. 이동한 사용자의 LDAP 항목에서 `mailMessageStore` 속성을 새 분할 영역의 이름으로 설정합니다.

예를 들면 다음과 같습니다.

```
mailMessageStore: secondary
```

4. 이제 메시지 저장소 연결이 허용된다는 것을 사용자에게 알립니다. 해당하는 경우 `mailAllowedServiceAccess` 속성을 변경하여 POP, IMAP 및 HTTP 서비스를 허용합니다.

## 기본 메시지 저장소 분할 영역 정의 변경

기본 분할 영역은 사용자를 만들 때 사용자 항목에 `mailMessageStore LDAP` 속성을 지정하지 않는 경우에 사용되는 분할 영역입니다. 기본 분할 영역이 필요하지 않도록 사용자의 메시지 저장소 분할 영역을 지정하는 `mailMessageStore LDAP` 속성을 모든 사용자 항목에 지정해야 합니다. 또한 로드 균형 조정이나 기타 이유 때문에 기본 분할 영역을 변경하면 **안 됩니다**. 기본 분할 영역 정의에 의존하는 사용자가 있는 상태에서 기본 분할 영역을 변경하는 것은 적절하지 않으며 위험합니다.

기본 분할 영역을 꼭 변경해야 할 경우에는 `configutil` 매개 변수 `store.defaultpartition`을 사용하여 기본값 정의를 변경하기 전에 이전의 기본 분할 영역(남겨진 것)의 모든 사용자가 `mailMessageStore` 속성을 현재 분할 영역(더 이상 기본값이 아닌)으로 설정해야 합니다.

## 메시지 저장소 유지 관리 절차 수행

이 절에서는 메시지 저장소의 유지 관리 및 복구 작업을 수행하는 데 사용되는 유틸리티에 대해 설명합니다. 관리자는 항상 포스트마스터 메일을 읽어 서버가 보낼 수 있는 주의와 경고를 확인해야 합니다. 또한 로그 파일에서 서버의 작동 상태에 대한 정보를 모니터링해야 합니다. 로그 파일에 대한 자세한 내용은 [21장](#), “[로그 관리](#)” 를 참조하십시오.

이 절은 다음 내용으로 구성되어 있습니다.

- [597페이지](#)의 “[메일함 관리](#)”
- [603페이지](#)의 “[할당량 제한 모니터](#)”
- [604페이지](#)의 “[디스크 공간 모니터](#)”
- [604페이지](#)의 “[stored 유틸리티 사용](#)”

### 메일함 관리

이 절에서는 `mboxutil`, `hashdir`, `readership`과 같은 메일함 관리 및 모니터링 유틸리티에 대해 설명합니다.

## mboxutil 유틸리티

mboxutil 명령을 사용하여 메일함에 대한 일반적인 유지 관리 작업을 수행하십시오. mboxutil 작업은 다음을 포함됩니다.

- 메일함 나열
- 고아 및 비활성 메일함 나열 및 제거
- 메일함 작성
- 메일함 이름 바꾸기
- 한 분할 영역에서 다른 분할 영역으로 메일함 이동
- 연결되지 않은 또는 비활성 메일함 삭제
- 또한 mboxutil 명령을 사용하여 할당량에 대한 정보를 볼 수 있습니다. 자세한 내용은 603페이지의 “할당량 제한 모니터”를 참조하십시오.

**주** mboxutil 프로세스를 실행 도중에 종료해서는 안 된다는 것을 유의하십시오. SIGKILL(kill -9)을 사용하여 중지할 경우 모든 서버를 다시 시작하고 복구를 수행해야 할 수 있습니다.

표 18-11에서는 mboxutil 명령을 나열합니다. 자세한 구문 및 사용 요구 사항에 대해서는 *Messaging Server Reference Manual*을 참조하십시오.

**표 18-11** mboxutil 옵션

| 옵션         | 설명                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| -a         | 폐기되었습니다. 모든 사용자 할당량 정보를 나열하는 데 사용됩니다. imquotacheck을 사용합니다.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| -c mailbox | 지정된 메일함을 만듭니다. -f와 함께 사용될 수 있습니다. 메일함이 있어야 보조 메일함을 만들 수 있습니다.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| -d mailbox | 지정된 메일함을 삭제합니다. 메시지 저장소에서 사용자를 삭제하려면 -d mailbox에 대해 다음 값을 사용합니다. <code>user/userid/INBOX</code><br>예를 들어, 메시지 저장소에서 사용자 john을 삭제하려면 -d user/john/INBOX를 사용합니다. 사용자 john의 메일함에서 mm 폴더를 삭제하려면 -d user/john/mm을 사용합니다.<br>사용자를 삭제하기 위한 좋은 방법은 Delegated Administrator 유틸리티 <code>comadmin user delete</code> 명령이나 Delegated Administrator 콘솔을 사용하여 사용자 상태를 LDAP 디렉토리에서 삭제된 것으로 표시하는 것입니다. 그런 다음 <code>comadmin user purge</code> 명령을 사용하여 지정된 일 수보다 긴 기간 동안 삭제된 것으로 표시된 사용자를 제거합니다.<br>앞 단락에 설명한 대로 Delegated Administrator 유틸리티를 사용할 경우에는 <code>mboxutil -d</code> 명령을 사용하여 메일함을 삭제할 필요가 없습니다. |

**표 18-11** mboxutil 옵션

| 옵션                           | 설명                                                                                                                                                                                                                                                                                                                                             |
|------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| -e                           | 메시지 저장소에서 삭제된 메일을 모두 정리합니다. 또한 이 옵션을 <i>-p pattern</i> 옵션과 함께 사용하면 삭제된 메일함 중에서 이름이 <i>pattern</i> 과 일치하는 메일함을 모두 정리할 수 있습니다.                                                                                                                                                                                                                   |
| -f <i>file</i>               | <p>메일함 이름을 저장하는 파일을 지정합니다. <i>-f</i> 옵션은 <i>-c</i>, <i>-d</i> 또는 <i>-r</i> 옵션과 함께 사용할 수 있습니다.</p> <p>이 파일에는 <i>mboxutil</i> 명령이 실행되는 메일함 목록이 포함됩니다. 다음은 데이터 파일의 항목 예입니다.</p> <pre>user/daphne/INBOX user/daphne/projx user/daphne/mm</pre>                                                                                                     |
| -k <i>mailbox cmd</i>        | 폐기되었습니다. 지정된 메일함을 폴더 수준에서 잠그고 지정된 명령을 실행하며 명령이 완료된 후 메일함의 잠금을 해제합니다.                                                                                                                                                                                                                                                                           |
| -l                           | <p>서버의 모든 메일함을 나열합니다.</p> <p>다른 언어 로케일에 대한 다중 바이트 폴더를 만들 경우 <i>msg_svr_base/bin/msg/bundles/encbylang.properties</i>를 편집하여 해당 문자 세트를 LANG 환경 변수에 연결해야 합니다.</p>                                                                                                                                                                                 |
| -o                           | <p>고아 계정을 검사합니다. 이 옵션은 LDAP에 해당 항목이 없는 현재 메시징 서버 호스트에서 받은 메일함을 검색합니다. 예를 들어, <i>-o</i> 옵션은 LDAP에서 삭제되었거나 다른 서버 호스트로 이동한 소유자의 받은 메일함을 찾습니다. 발견된 각 고아 계정에 대해 <i>mboxutil</i>은 다음 명령을 표준 출력에 기록합니다.</p> <pre>mboxutil-d user/userid/INBOX</pre> <p>단, <i>-w</i>를 지정하지 않아야 합니다.</p>                                                                |
| -p <i>MUTF7_IMAP_pattern</i> | <p><i>-l</i> 옵션과 함께 사용될 경우 <i>MUTF7_IMAP_pattern</i>과 일치하는 이름을 가진 메일함만 나열합니다.</p> <p>또한 <i>-d</i> 또는 <i>-e</i> 옵션과 함께 사용하여 <i>MUTF7_IMAP_pattern</i>과 일치하는 이름을 가진 메일함을 삭제 또는 정리할 수 있습니다.</p> <p>IMAP 와일드카드를 사용할 수 있습니다. 이 옵션에는 IMAP M-UTF-7 형식의 패턴이 필요합니다. ASCII가 아닌 메일함의 경우 이 검색 방법은 권장되지 않습니다. ASCII가 아닌 메일함을 검색하려면 <i>-P</i> 옵션을 사용합니다.</p> |
| -P <i>regexp</i>             | 지정된 POSIX 정규 표현식과 일치하는 이름을 가진 메일함만 나열합니다. 이 옵션에서는 <i>regexp</i> 를 로컬 언어로 지정해야 합니다.                                                                                                                                                                                                                                                             |
| -q <i>domain</i>             | 폐기되었습니다. <i>imquotacheck -d domain</i> 을 사용합니다.                                                                                                                                                                                                                                                                                                |

**표 18-11** mboxutil 옵션

| 옵션                                                | 설명                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|---------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| -r <i>oldname newname</i><br>[ <i>partition</i> ] | <p>메일함의 이름을 <i>oldname</i>에서 <i>newname</i>으로 바꿉니다. 폴더를 특정 분할 영역에서 다른 분할 영역으로 이동하려면 <i>partition</i> 옵션으로 새 분할 영역을 지정합니다. 파일을 사용하기 위해 -f 플래그와 함께 사용될 수 있습니다.</p> <p>이 옵션을 사용하여 사용자를 바꿀 수 있습니다. 예를 들어, <code>mboxutil -r user/user1/INBOX user/user2/INBOX</code>는 모든 메일과 메일함을 user1에서 user2로 이동하며 새 INBOX에 새 메일이 나타납니다. (user2가 이미 존재할 경우 이 작업은 실패합니다.)</p>                                                                                                                                                                 |
| -R <i>mailbox</i>                                 | <p>아직 제거되지 않은 삭제된 메일을 복원합니다.</p> <p>메일함이 정리되거나 만료되면 삭제된 메일의 uid가 <code>store.exp</code> 파일에 저장됩니다. 메일은 정리 페이지가 전달된 후 <code>imexpire</code>에 의해 실제로 제거됩니다. 실수로 정리나 만료를 실행한 경우에는 <code>imexpire</code>에 의해 제거되지 않은 삭제된 메일을 이 옵션을 사용하여 원래 메일함으로 복원할 수 있습니다.</p>                                                                                                                                                                                                                                                                |
| -s                                                | <p>-l 옵션과 함께 사용될 경우 메일함 이름만 표시합니다. 다른 데이터는 표시되지 않습니다.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| -t <i>num</i>                                     | <p>지정된 일 수(<i>num</i>) 동안 액세스되지 않은 메일함을 나열합니다. -t 옵션은 고아 메일함을 식별하는 -o 옵션과 함께 사용해야 합니다.</p> <p>따라서 -t 옵션은 고아 메일함(LDAP 디렉토리에 해당 사용자 항목이 없는 메일함)과 함께 비활성 메일함(마지막 액세스 날짜를 기초로)을 식별합니다.</p> <p>고아 및 비활성 메일함을 식별(나열)하려면 <code>mboxutil -o -w file -t num</code>을 사용합니다.</p> <p>이러한 연결되지 않은 및 비활성 메일함을 삭제 표시하려면 <code>mboxutil -d -f file</code>을 사용합니다. 여기서 <i>file</i>은 앞의 -w <i>file</i>에 사용된 것과 동일한 파일입니다.</p> <p>이 기능을 사용하려면 최소한 -t 옵션에 지정된 일 수 동안 <code>config</code> 변수 <code>local.enablelastaccess</code>를 활성화해야 합니다.</p> |
| -u <i>user</i>                                    | <p>폐기되었습니다. 사용자 정보를 나열하는 데 사용됩니다. <code>imquotacheck -u user</code>를 사용합니다.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| -w <i>file</i>                                    | <p>-o 옵션과 함께 사용됩니다. 고아 계정을 식별하는 -o 옵션에 의해 생성된 메일함 이름을 파일에 기록합니다.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| -x                                                | <p>-l 옵션과 함께 사용될 경우 메일함에 대한 경로와 액세스 제어를 표시합니다.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

**주** POSIX 정규식을 `mboxutil` 명령에서 사용할 수 있습니다.



## 메일함 이름 지정 규칙

메일함 이름을 `user/userid/mailbox` 형식으로 지정해야 합니다. 여기서 `userid`는 메일함을 소유한 사용자이고 `mailbox`는 메일함 이름입니다. 호스트된 도메인의 경우 `userid`는 `uid@domain`입니다.

예를 들어, 다음 명령은 사용자 아이디가 `crowe`인 사용자에게 대해 `INBOX`라는 메일함을 만듭니다. `INBOX`는 사용자 `crowe`에게 전달되는 메일의 기본 메일함입니다.

```
mbxutil -c user/crowe/INBOX
```

**중요:** `INBOX`라는 이름은 각 사용자의 기본 메일함으로 준비되어 있습니다. `INBOX`는 대소문자를 구분하지 않는 유일한 폴더 이름입니다. 다른 모든 폴더 이름은 대소문자를 구분합니다.

## 예

모든 사용자의 모든 메일함을 나열하려면 다음을 수행합니다.

```
mbxutil -l
```

모든 메일함을 나열하고 또한 경로와 `ACL` 정보를 포함하려면 다음을 수행합니다.

```
mbxutil -l -x
```

사용자 `daphne`에 대해 `INBOX`라는 기본 메일함을 만들려면 다음을 수행합니다.

```
mbxutil -c user/daphne/INBOX
```

사용자 `delilah`에 대해 `projx`라는 메일 폴더를 삭제하려면 다음을 수행합니다.

```
mbxutil -d user/delilah/projx
```

사용자 `druscilla`에 대해 `INBOX`라는 기본 메일함과 모든 메일 폴더를 삭제하려면 다음을 수행합니다.

```
mbxutil -d user/druscilla/INBOX
```

사용자 `desdemona`에 대해 메일 폴더 `memos`의 이름을 `memos-april`로 바꾸려면 다음을 수행합니다.

```
mbxutil -r user/desdemona/memos user/desdemona/memos-april
```

사용자 `dimitria`에 대한 메일 계정을 새 분할 영역으로 이동하려면 다음을 수행합니다.

```
mbxutil -r user/dimitria/INBOX user/dimitria/INBOX partition
```

여기서 `partition`은 새 분할 영역의 이름을 지정합니다.

사용자 `dimitria`에 대해 `personal`이라는 메일 폴더를 새 분할 영역으로 이동하려면 다음을 수행합니다.

```
mbxutil -r user/dimitria/personal user/dimitria/personal partition
```

## 고아 계정 제거

고아 계정(LDAP에 해당 항목이 없는 메일함)을 검색하려면 다음 명령을 사용합니다.

**mboxutil -o**

명령 출력은 다음과 같습니다.

```
mboxutil: Start checking for orphaned mailboxes
user/annie/INBOX
user/oliver/INBOX
mboxutil: Found 2 orphaned mailbox(es)
mboxutil: Done checking for orphaned mailboxes
```

고아 메일함을 삭제하여 스크립트 파일로 변환될 수 있는 고아 메일함을 나열하는 orphans.cmd라는 이름의 파일을 만들려면 다음 명령을 사용합니다.

**mboxutil -o -w orphans.cmd**

명령 출력은 다음과 같습니다.

```
mboxutil: Start checking for orphaned mailboxes
mboxutil: Found 2 orphaned mailbox(es)
mboxutil: Done checking for orphaned mailboxes
```

다음 명령을 사용하여 고아 파일을 삭제합니다.

**mboxutil -d -f orphans.cmd**

## hashdir 유틸리티

메시지 저장소의 메일함은 빠른 검색을 위해 해시 구조에 저장됩니다. 결과적으로 특정 사용자의 메일함을 포함하는 디렉토리를 찾으려면 hashdir 유틸리티를 사용합니다.

이 유틸리티는 특정 계정의 메시지 저장소를 포함하는 디렉토리를 식별합니다. 이 유틸리티는 메시지 저장소에 상대적인 경로(예: d1/a7/)를 보고합니다. 이 경로는 사용자 아이디 기반 디렉토리의 바로 앞에 있는 디렉토리 수준에 상대적입니다. 이 유틸리티는 경로 정보를 표준 출력으로 보냅니다.

예를 들어, 사용자 crowe에 대한 메일함의 상대 경로를 찾으려면 다음을 수행합니다.

hashdir crowe

## readership 유틸리티

readership 유틸리티는 공유 IMAP 폴더의 메일을 읽은 메일함 소유자 이외의 사용자 수를 보고합니다.

IMAP 폴더 소유자는 폴더의 메일을 읽는 권한을 다른 사용자에게 부여할 수 있습니다. 다른 사용자가 액세스하도록 허가된 폴더를 *공유 폴더*라고 합니다. 관리자는 readership 유틸리티를 사용하여 공유 폴더에 액세스하는 소유자 이외의 사용자 수를 확인할 수 있습니다.

이 유틸리티는 모든 메일함을 스캔한 후 공유 폴더별로 한 행씩의 출력을 생성하여 읽은 사람 수(뒤에 공백과 메일함 이름이 옴)를 보고합니다.

각 읽은 사람은 이전의 지정된 일 수 동안 공유 폴더를 선택했던 고유한 인증 아이디입니다. 자신의 고유한 메일함을 읽을 때는 사용자가 계산되지 않습니다. 폴더 소유자 외에 최소 한 명 이상의 읽은 사람이 존재하지 않을 경우 개인 메일함은 보고되지 않습니다.

예를 들어, 다음 명령은 마지막 15일 동안에 공유 IMAP 폴더를 선택한 모든 아이디를 읽은 사람으로 계산합니다.

```
readership -d 15
```

## 할당량 제한 모니터

imquotacheck를 사용하여 할당량 사용 및 제한을 모니터링한 다음 정의된 할당량과 제한을 나열하는 보고서를 생성하고 할당량 사용과 관련한 정보를 제공합니다. 할당량과 사용량 수치는 KB로 보고됩니다. 이 유틸리티는 메일함 크기를 사용자의 할당량과 비교할 수도 있습니다. 옵션으로 지정된 할당량 비율을 초과한 사용자에게 전자 메일 알림을 보낼 수 있습니다.

---

**주** imquotacheck에서 일부 기능이 변경되었습니다. (Messaging Server 6.x에서는 imquotacheck 유틸리티가 quotacheck 유틸리티 대신 사용되었습니다.) Messaging Server 5.x에서는 quotacheck 유틸리티를 사용하여 사용자 목록을 검색할 때 quotacheck는 로컬 mboxlist 데이터베이스를 검색했습니다. 이 기능은 mboxutil 유틸리티의 검색 기능과 중복되었습니다.

Messaging Server 6.x에서는 이 중복된 기능이 imquotacheck 유틸리티에서 제거되었습니다. imquotacheck를 사용하여 사용자 검색을 수행할 경우 로컬 mboxlist 데이터베이스가 아닌 LDAP 디렉토리에 대해 검색이 수행됩니다. 로컬 mboxlist 데이터베이스에서 사용자 목록을 검색하려면 mboxutil 유틸리티를 사용합니다.

---

할당량이 규칙 파일의 최소 임계값을 초과하는 모든 사용자에 대한 사용량을 나열하려면 다음을 수행합니다.

```
imquotacheck
```

도메인 `siroe.com`에 대한 할당량 정보를 나열합니다.

```
imquotacheck -d siroe.com
```

기본 규칙 파일에 따라 모든 사용자에게 알림을 보내려면 다음을 수행합니다.

```
imquotacheck -n
```

지정된 `rulefile`, `myrulefile` 및 지정된 메일 템플릿 파일 `mytemplate.file`에 따라 모든 사용자에게 알림을 보내려면 다음을 수행합니다(자세한 내용은 *Sun Java System Messaging Server Administration Reference* 참조).

```
imquotacheck -n -r myrulefile -t mytemplate.file
```

모든 사용자에게 대한 사용량을 나열하고 규칙 파일을 무시하려면 다음을 수행합니다.

```
imquotacheck -i
```

사용자 `user1`에 대한 폴더별 사용량을 나열하려면 다음을 수행합니다(규칙 파일 무시).

```
imquotacheck -u user1 -e
```

## 디스크 공간 모니터

시스템이 디스크 공간과 분할 영역 사용을 모니터해야 하는 빈도와 경고를 보내야 하는 상황을 지정할 수 있습니다. 자세한 내용은 [804페이지의 “디스크 공간 모니터링”](#)을 참조하십시오.

## stored 유틸리티 사용

`stored` 유틸리티는 서버에 대한 다음 모니터링 및 유지 관리 작업을 수행합니다.

- 백그라운드 및 일상적인 메시징 작업
- 교착 상태 감지 및 교착 상태에 빠진 데이터베이스 트랜잭션의 롤백
- 시작 시 임시 파일 정리
- 에이징 정책 구현
- 서버 상태, 디스크 공간, 서비스 응답 시간 등의 정기적인 모니터링([815페이지의 “stored”](#) 참조)
- 필요한 경우 경보 발생

- 필요에 따른 데이터베이스 복구(629페이지의 “메시지 저장소 시작 및 복구” 참조)  
stored 유틸리티는 매일 오후 11시에 정리 및 만료 작업을 자동으로 수행합니다. 추가 정리 및 만료 작업을 실행하도록 선택할 수 있습니다.

표 18-12에는 일부 stored 옵션이 나열되어 있습니다. 다음 표에는 몇 가지 일반적인 사용 예가 나와 있습니다. 자세한 구문 및 사용 요구 사항에 대해서는 *Messaging Server Reference Manual*을 참조하십시오.

| 표 18-12 stored 옵션 |                                                                                                     |
|-------------------|-----------------------------------------------------------------------------------------------------|
| 옵션                | 설명                                                                                                  |
| -d                | 폐기되었습니다. start-msg store를 사용하여 데몬으로 실행될 stored를 시작하여 시스템 검사를 수행하고 경보, 교착 상태 감지 및 데이터베이스 복구를 활성화합니다. |
| -t                | stored의 상태를 검사합니다. 이 명령의 반환 코드는 상태를 나타냅니다.                                                          |
| -v                | 세부 정보를 출력합니다.                                                                                       |
| -v -v             | 보다 세부적인 정보를 출력합니다.                                                                                  |

상태를 출력하려면 다음을 입력합니다.

```
stored -t -v
```

자동 정리 및 만료 작업 시간을 변경하려면 다음과 같이 configutil 유틸리티를 사용합니다.

```
configutil -o store.expirestart -v 21
```

경우에 따라 stored 유틸리티를 다시 시작해야 할 수 있습니다(예: 메일함 목록 데이터베이스가 손상된 경우). UNIX에서 stored를 다시 시작하려면 명령줄에서 다음 명령을 사용합니다.

```
msg_svr_base/sbin/stop-msg store
msg_svr_base/sbin/start-msg store
```

입의의 서버 데몬이 충돌된 경우 stored를 비롯한 모든 데몬을 중지했다가 다시 시작해야 합니다.

## 동일한 메일의 중복 저장에 따른 저장소 크기 줄이기

하나의 메일이 여러 수신자에 전송될 때 해당 메일은 각 수신자의 메일함에 다 놓이게 됩니다. 일부 메시징 시스템에서는 각 수신자의 메일함에 같은 메일의 사본을 별도로 저장합니다. 그러나 이와 반대로, Sun Java System Messaging Server에서는 해당 메일이 있는 메일함의 수에 관계 없이 메일 사본을 하나만 유지합니다. 이는 해당 메일을 포함하는 메일함에 메일에 대한 하드 링크를 작성하는 방법으로 이루어집니다.

다른 메시징 시스템을 Sun Java Messaging Server로 마이그레이션할 때는 마이그레이션 과정을 통해 이러한 여러 메일 사본이 복사될 수 있습니다. 이는 규모가 큰 메시지 저장소의 경우 불필요하게 많은 메일이 중복되는 것을 의미합니다. 또한 일반적인 서버 작업(예: IMAP append 작업이나 기타 소스의 작업)에 같은 메일 사본이 여러 개 누적될 수 있습니다.

Messaging Server는 `relinker`라는 이름의 새 명령을 제공하는데, 이 명령은 과도한 메일 사본을 제거하고 하나의 사본에 대한 하드 링크로 대체합니다.

### relinker 작동 원리

재연결 기능은 이 명령이나 실시간 모드에서 실행할 수 있습니다. `relinker` 명령을 실행할 때는 이 명령이 메시지 저장소 분할 영역 전체를 스캔하고 MD5 메일 다이제스트 저장소(하드 링크에 해당)를 작성 또는 업데이트하며 필요한 하드 링크를 만듭니다.

다이제스트 저장소는 메시지 저장소의 메일에 대한 하드 링크로 이루어져 있습니다. 이는 디렉토리 계층 `partition_path/=md5`에 저장됩니다. 이 디렉토리는 사용자 메일함 계층 `partition_path/=user`(554페이지의 그림 18-1 참조)과 병행합니다. 다이제스트 저장소의 메일은 MD5 다이제스트에서 고유하게 식별합니다. 예를 들어, `fredb/00/1.msg`의 다이제스트가 `4F92E5673E091B43415FFFA05D2E47`인 경우

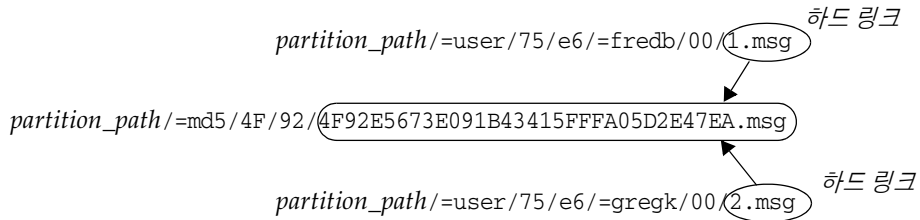
`partition/=user/hashdir/hashdir/=fredb/00/1.msg`는  
`partition/=md5/hashdir/hashdir/4F92E5673E091B43415FFFA05D2E47EA.msg`에 링크됩니다.

다른 메일함에 이와 같은 메일이 있을 때(예:

`partition_path/=user/hashdir/hashdir/gregk/00/17.msg`) 해당 메일은

`partition_path/=md5/4F/92/4F92E5673E091B43415FFFA05D2E47EA.msg`에 대해 하드 링크로 연결됩니다. 이 시나리오는 607페이지의 그림 18-5에 나와 있습니다.

**그림 18-5** 메시지 저장소 다이제스트 저장소



이 메일의 경우 링크 수는 3이 됩니다. 두 메일 모두 fredb 및 gregk의 메일함에서 삭제 되면 링크 수는 하나가 되고 해당 메일을 삭제할 수 있습니다.

relinker 프로세스는 같은 기능에 대해 실시간으로 실행될 수 있습니다. 자세한 내용은 609페이지의 “실시간 모드에서 relinker 사용”을 참조하십시오.

### 명령줄 모드에서 relinker 사용

relinker는 메시지 저장소 분할 영역 전체를 스캔하고 MD5 메시지 저장소(하드 링크에 해당)를 작성 또는 업데이트하며 과도한 메일 파일을 삭제합니다. relinker가 저장소 분할 영역을 스캔한 후에는 재연결 이전과 이후 해당 분할 영역의 크기와 고유한 메일의 수에 대한 통계를 산출합니다. 이미 해시된 저장소에 대한 실행 속도를 높이기 위해 relinker는 아직 =md5에 없는 메일의 다이제스트만 계산합니다. 또한 전체 다이제스트 저장소(사용자 메일함에 영향을 주지 않는 범위에서)를 지우는 옵션도 있습니다.

이 명령의 구문은 다음과 같습니다.

```
relinker [-p partitionname] [-d]
```

여기서 *partitionname*은 처리될 분할 영역(기본값: 모든 분할 영역)을 지정하고 -d는 다이제스트 저장소가 삭제됨을 지정합니다. 출력 예는 다음과 같습니다.

#### # relinker

```
Processing partition: primary
Scanning digest repository...
Processing user directories.....
-----
Partition statistics          Before      After
```

```

-----
Total messages                4531898        4531898
Unique messages              4327531        3847029
Message digests in repository      0            3847029
Space used                   99210Mb        90481Mb
Space savings from single-copy    3911Mb        12640Mb
-----

```

**# relinker -d**

```

Processing partition: primary
Purging digest repository...

```

```

-----
Partition statistics          Before         After
-----
Message digests in repository 3847029         0
-----

```

특히 저장소에 메일이 하나도 없는 처음에는 **relinker** 실행에 시간이 많이 걸릴 수 있습니다. 이는 모든 메일마다 다이제스트를 계산(**relinker** 기준이 모든 메일을 포함하도록 구성된 경우)해야 하기 때문입니다. **relinker** 기준 구성에 대한 자세한 내용은 [609페이지의 “relinker 구성”](#)을 참조하십시오. 예를 들어, 100GB의 메시지 저장소를 처리하는 데는 6 시간 정도가 걸립니다. 그러나 런타임 재연결을 활성화한 경우([609페이지의 “실시간 모드에서 relinker 사용”](#) 참조)에는 **relinker** 명령을 실행할 필요가 없습니다.

**relinker** 명령줄 모드가 예외적으로 사용되고 런타임 옵션이 아닌 경우에는 다이제스트 저장소(=md5)를 삭제할 필요가 있습니다. 그 외의 경우에는 저장소에서 삭제된 메일(=user)에 해당 다이제스트 저장소의 연결이 그대로 있으므로(고아 메일이 됨) 사용 가능한 디스크 공간이 되지 않습니다. **relinker**를 한 번만 실행할 수 있는 저장소의 일회 최적화를 수행하는 경우(예: 마이그레이션 후)에는 **relinker -d**를 사용하여 전체 저장소를 삭제하십시오. 반복된 삭제의 경우(마이그레이션 도중)에는 **relinker** 명령을 반복적으로 수행하는 것만으로도 충분합니다. 이 명령을 실행할 때마다 만료된 메일이나 고아 메일을 저장소에서 삭제하기 때문입니다.

처리되는 다른 분할 영역마다 병행하여 **relinker**의 여러 인스턴스를 실행(-p 옵션 사용)하는 것이 안전합니다. 메일은 같은 파티션 안에서만 재연결됩니다.



## 실시간 모드에서 relinker 사용

relinker 기능은 configutil 매개 변수 local.store.relinker.enabled를 yes로 설정함으로써 실시간 모드에서 활성화될 수 있습니다. 실시간 모드에서 relinker를 사용하면 구성된 relinker 기준(609페이지의 “relinker 구성”)에 맞게 배달된(또는 복원되거나 IMAP 추가된) 모든 메일의 다이제스트를 계산한 다음 해당 다이제스트가 이미 존재하는지 여부를 저장소에서 확인하게 됩니다. 이 다이제스트가 존재하는 경우에는 해당 메일의 새 사본을 만들지 않고 그에 대한 링크를 대상 메일함에 만듭니다. 다이제스트가 없을 때는 메일을 만들고 나중에 그에 대한 링크를 저장소에 추가합니다.

stored는 각 분할 영역의 다이제스트 저장소를 스캔하고 링크 수가 한 개인 메일(즉, relinker 기준에 맞지 않는 메일)을 삭제합니다. 스캔은 구성 가능한 시간 동안 한 번에 한 디렉토리씩 수행됩니다. 이로써 I/O 로드가 공평하게 분산되고 다른 서버 작업에 별다른 영향을 주지 않게 됩니다. 기본적으로 삭제 주기는 24시간이며 이는 저장소에서 메일이 삭제되거나 구성된 최대 캐시 사용 기간을 초과해도 최대 24시간까지는 그대로 남아 있다는 의미입니다. 이 작업은 relinker 실시간 모드가 활성화되어 있는 경우 사용 가능합니다.

## relinker 구성

표 18-13은 relinker 기준을 설정하는 데 사용된 매개 변수를 보여줍니다.

**표 18-13** relinker configutil 매개 변수

| 매개 변수                        | 설명                                                                                                                                                                                                                                                                                                                                                      |
|------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| local.store.relinker.enabled | <p>추가 코드 및 stored 삭제에서 메일의 실시간 재연결을 활성화합니다. 이 옵션이 설정 해제되어 있는 경우에도 relinker 명령줄 도구를 실행할 수는 있지만, stored가 저장소를 삭제하지 않기 때문에 이 작업에는 relinker -d를 사용해야 합니다. 이 옵션을 설정하면 디스크 공간이 절감되는 대신 메일 배달 성능이 떨어집니다.</p> <p>기본값: no</p>                                                                                                                                    |
| local.store.relinker.maxage  | <p>저장소에 메일이 저장될 최대 캐시 사용 기간(시간)으로서 relinker 명령줄에서 고려합니다. -1은 제한이 없다는 뜻으로 저장소에서 고아 메일만 삭제합니다. relinker의 경우 이는 캐시 사용 기간에 관계 없이 기존 메일을 처리한다는 의미가 됩니다. 값을 적게 할수록 저장소가 작아지므로 relinker 또는 stored 삭제가 더 빨리 실행되고 디스크 공간을 더 빨리 재생 이용할 수 있습니다. 반면, 값을 크게 할수록 긴 시간(예를 들어, 사용자가 같은 메일을 며칠 간격으로 저장하거나 며칠 또는 몇 주에 걸쳐 이전을 실행할 때)에 걸쳐 메일 재연결이 중복됩니다.</p> <p>기본값: 24</p> |
| local.store.relinker.minsize | <p>런타임 또는 명령줄 relinker에서 고려하는 메일의 최소 크기(KB). 0이 아닌 값을 설정하면 저장소는 작아지는 대신 규모가 작은 메일에 대한 relinker 혜택은 늘어납니다.</p> <p>기본값: 0</p>                                                                                                                                                                                                                             |

**표 18-13** relinker configutil 매개 변수

| 매개 변수                           | 설명                                                                                                                                                                                                                                                                            |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| local.store.relinker.purgecycle | <p>전체 stored 삭제 주기의 대략적인 지속 시간. 실제 지속 시간은 저장소의 각 디렉토리를 스캔하는 데 걸리는 시간에 따라 달라집니다. 값이 적을수록 더 많은 I/O를 사용하게 되고 값이 클수록 디스크 공간의 재생 이용이 느려집니다. 0은 디렉토리 사이에 일시 중지 없이 계속적으로 삭제가 실행된다는 의미입니다. -1은 stored에서 삭제가 실행되지 않는다는 뜻입니다. 따라서 삭제는 relinker -d 명령을 사용하여 수행해야 합니다.</p> <p>기본값: 24</p> |

## 메시지 저장소 백업 및 복원

메시지 저장소 백업 및 복원은 가장 일반적이고 중요한 관리 작업 중 하나입니다. 이 작업은 메시지 저장소의 모든 메일과 폴더를 백업하는 것으로 구성됩니다. 다음과 같은 문제가 발생했을 때 데이터가 손실되지 않도록 메시지 저장소에 대한 백업 및 복원 정책을 구현해야 합니다.

- 시스템 충돌
- 하드웨어 오류
- 메일 또는 메일함의 우발적 삭제
- 시스템 재설치 또는 업그레이드 시의 문제
- 자연 재해(예: 지진, 화재, 태풍)
- 사용자 마이그레이션

imsbackup 및 imsrestore 명령줄 유틸리티나 Legato Networker®를 사용하는 통합 솔루션을 사용하여 메시지 저장소 백업 및 복원을 수행할 수 있습니다.

Messaging Server는 단일 복사본 백업 절차를 제공합니다. 특정 메일을 포함하는 사용자 폴더 수에 상관 없이 백업 도중 메일 파일은 처음 발견된 메일 파일을 사용하여 한 번만 백업됩니다. 두 번째 메일 복사본은 첫 번째 메일 파일의 이름에 대한 링크로 백업되며 그 다음 복사본도 마찬가지입니다. imsbackup은 메일 파일의 장치와 색인 노드를 색인으로 사용하여 모든 메일의 해시 테이블을 유지 관리합니다. 단, 이 방법은 데이터 복원 시 고려해야 할 사항이 있습니다. 자세한 내용은 [616페이지의 “부분 복원 시의 고려 사항”](#)을 참조하십시오.

**주** 모든 메일 파일과 디렉토리를 백업함으로써 메시지 저장소 백업과 복원을 수행할 수도 있습니다. [623페이지의 “메시지 저장소 재해 복구 및 복원”](#)을 참조하십시오.

이 절에는 다음과 같은 하위 절이 포함됩니다.

- 611페이지의 “메일함 백업 정책 만들기”
- 612페이지의 “백업 그룹 만들기”
- 613페이지의 “Messaging Server 백업 및 복원 유틸리티”
- 616페이지의 “부분 복원 시의 고려 사항”
- 617페이지의 “중분 백업된 메일함에서 메일 복원”
- 618페이지의 “Legato Networker 사용”
- 622페이지의 “Legato를 제외한 타사 백업 소프트웨어 사용”
- 623페이지의 “메시지 저장소 재해 복구 및 복원”
- 623페이지의 “백업 및 복원 문제 해결”
- 623페이지의 “메시지 저장소 재해 복구 및 복원”

## 메일함 백업 정책 만들기

백업 절차는 다음과 같은 여러 요소에 따라 달라집니다.

- 작업량이 가장 많은 시간대
- 전체 및 증분 백업
- 병렬 또는 직렬 백업

### 작업량이 가장 많은 시간대

시스템에 대한 백업 일정을 예약할 때는 작업량이 가장 많은 시간대에 시스템 로드를 줄일 수 있도록 작업량이 가장 많은 시간대를 피해야 합니다. 예를 들어, 백업은 오전 2시와 같은 새벽에 실행되도록 예약하는 것이 가장 적합합니다.

### 전체 및 증분 백업

증분 백업(614페이지의 “증분 백업” 참조)은 변경된 데이터의 저장소를 스캔하고 변경된 사항만 백업합니다. 전체 백업은 전체 메시지 저장소를 백업합니다. 증분 백업과 달리 전체 백업은 시스템이 전체 백업을 수행하는 빈도를 결정해야 합니다. 일반적으로 증분 백업을 일상적인 유지 관리 절차로 수행하면서 일주일에 한 번씩 전체 백업을 수행합니다.

## 병렬 또는 직렬 백업

사용자 데이터를 여러 디스크에 저장할 경우 필요에 따라 사용자 그룹을 병렬로 백업할 수 있습니다. 시스템 자원에 따라 병렬 백업은 전반적인 백업 절차의 속도를 높일 수 있습니다. 그러나 백업이 서버 성능에 미치는 영향을 최소화하려는 경우 직렬 백업을 사용할 수 있습니다. 병렬 백업 또는 직렬 백업 사용 여부는 시스템 로드, 하드웨어 구성, 사용 가능한 테이프 드라이브 수 등에 따라 달라질 수 있습니다.

## 백업 그룹 만들기

백업 그룹은 정규식에 의해 정의되는 임의의 사용자 메일함 집합입니다. 사용자 메일함을 그룹으로 구성하여 보다 유연한 백업 관리를 정의할 수 있습니다.

예를 들어, 사용자 아이디가 A-L로 시작하는 사용자를 포함하는 첫 번째 백업 그룹, 사용자 아이디가 M-Z로 시작하는 사용자를 포함하는 두 번째 백업 그룹, 사용자 아이디가 숫자로 시작하는 사용자를 포함하는 세 번째 백업 그룹의 세 가지 백업 그룹을 만들 수 있습니다. 관리자는 이러한 백업 그룹을 사용하여 메일함을 병렬로 백업하거나 특정 날짜에 일정 그룹만 백업하고 다른 날짜에 다른 그룹을 백업할 수 있습니다.

백업 그룹과 관련하여 다음 몇 가지 사항에 유의해야 합니다.

1. 백업 그룹은 메일 사용자의 임의 *가상* 그룹이며 보기와 달리 메시지 저장소 디렉토리 (554페이지의 [그림 18-1](#))에 정확하게 매핑되지 않습니다.
2. 관리자가 UNIX 정규식을 사용하여 백업 그룹을 정의합니다.
3. 정규식은 다음 구성 파일에 정의됩니다.  
`msg_svr_base/config/backup-groups.conf`
4. 백업 그룹은 `imsbackup` 및 `imsrestore`에서 참조될 경우 `/partition_name/backup_group` 경로 형식을 사용합니다.

`backup-groups.conf`의 형식은 다음과 같습니다.

```
group_name=definition
group_name=definition
.
.
.
```

위 단락에 설명된 예에 따라 다음 정의를 사용하여 세 개의 백업 그룹을 만듭니다.

```
groupA=[a-l].*
groupB=[m,-z].*
groupC=[0-9].*
```

이제 `imsbackup` 및 `imsrestore`를 여러 수준에서 사용할 수 있습니다. 다음과 같이 백업 명령을 사용하여 전체 메시지 저장소를 백업/복원할 수 있습니다.

```
imsbackup -f device /
```

groupA의 모든 사용자에게 대한 모든 메일함을 백업하려면 다음 명령을 사용합니다.

```
imsbackup -f device /partition/groupA
```

기본 분할 영역을 `primary`라고 합니다.

## 미리 정의된 백업 그룹

Messaging Server에는 `backup-groups` 구성 파일을 만들지 않고 사용할 수 있는 하나의 미리 정의된 백업 그룹이 포함되어 있습니다. 이 그룹은 `user`라고 불리며 모든 사용자를 포함합니다. 예를 들어, 다음 명령은 `primary` 분할 영역의 모든 사용자를 백업합니다.

```
imsbackup -f backupfile /primary/user
```

## Messaging Server 백업 및 복원 유틸리티

데이터를 백업 및 복원하기 위해 Messaging Server는 `imsbackup` 및 `imsrestore` 유틸리티를 제공합니다. `imsbackup` 및 `imsrestore` 유틸리티는 Legato Networker와 같은 일반 용도의 도구에 있는 고급 기능을 포함하지 않습니다. 예를 들어, 이러한 유틸리티는 테이프 자동 변환기에 대한 매우 제한적인 지원을 제공하고 단일 저장소를 동시에 여러 장치에 기록할 수 없습니다. 포괄적인 백업은 Legato Networker와 같은 일반화된 도구에 대한 플러그인을 통해 실현됩니다. Legato Networker 사용에 대한 자세한 내용은 [618페이지의 “Legato Networker 사용”](#)을 참조하십시오.

### imsbackup 유틸리티

`imsbackup`을 사용하면 메시지 저장소의 원하는 내용을 자기 테이프, UNIX 파이프 또는 일반 파일을 비롯한 모든 직렬 장치에 기록할 수 있습니다. 백업이나 백업의 일부를 나중에 `imsrestore` 유틸리티를 사용하여 복구할 수 있습니다. `imsbackup`의 출력을 `imsrestore`로 파이프할 수 있습니다.

다음 예에서는 전체 메시지 저장소를 /dev/rmt/0으로 백업합니다.

```
imsbackup -f /dev/rmt/0 /
```

여기에서는 사용자 아이디 joe의 메일함을 /dev/rmt/0으로 백업합니다.

```
imsbackup -f /dev/rmt/0 /primary/user/joe
```

다음 예에서는 백업 그룹 groupA에 정의된 모든 사용자의 모든 메일함을 backupfile로 백업합니다(612페이지의 “백업 그룹 만들기” 참조).

```
imsbackup -f- /primary/groupA > backupfile
```

### 증분 백업

다음 예는 2004년 5월 1일 1:10 PM부터 현재까지 저장된 메일을 백업합니다. 기본값은 날짜에 상관없이 모든 메일을 백업하는 것입니다.

```
imsbackup -d 20040501:13100
```

이 명령은 기본 차단 요소 20을 사용합니다. imsbackup 명령의 전체 구문 설명은 *Messaging Server Reference Manual*을 참조하십시오.

### imsrestore 유틸리티

백업 장치에서 메일을 복원하려면 imsrestore 명령을 사용합니다. 예를 들어, 다음 명령은 backupfile 파일에서 user1에 대한 메일을 복원합니다.

```
imsrestore -f backupfile /primary/user1
```

imsbackup 명령의 전체 구문 설명은 *Messaging Server Reference Manual*을 참조하십시오.

## 백업 수행 시 대량 메일 제외

백업 작업을 수행할 때 백업에서 제외할 메일함을 지정할 수 있습니다. 중요하지 않은 메일을 늘릴 수 있는 대량 또는 휴지통 메일함을 제외함으로써 백업 세션을 단순화하고 작업을 완료하는 데 필요한 시간을 줄이며 백업 데이터를 저장하는 데 필요한 디스크 공간을 최소화할 수 있습니다.

메일함을 제외하려면 `configutil` 매개 변수 `local.store.backup.exclude`에 대한 값을 지정합니다.

하나의 메일함이나 '%' 문자로 구분된 메일함 목록을 제외할 수 있습니다. '%'는 메일함 이름에 사용할 수 없는 문자입니다. 예를 들어, 다음 값을 지정할 수 있습니다.

```
Trash
```

```
Trash%Bulk Mail%Third Class Mail
```

첫 번째 예에서는 폴더 `Trash`가 제외됩니다. 두 번째 예에서는 폴더 `Trash`, `Bulk Mail` 및 `Third Class Mail`이 제외됩니다.

백업 유틸리티는 `local.store.backup.exclude` 매개 변수에 지정된 폴더를 제외하고 사용자 메일함의 모든 폴더를 백업합니다.

이 기능은 `Messaging Server` 백업 유틸리티, `Legato Networker` 및 타사 백업 소프트웨어와 함께 작동합니다.

작업 도중에 전체 논리 이름을 지정하여 `local.store.backup.exclude` 설정을 대체하거나 제외된 메일함을 백업할 수 있습니다. 휴지통 폴더가 제외되었다고 가정합니다. 다음을 지정하여 휴지통도 백업할 수 있습니다.

```
/primary/user/user1/trash
```

그러나 다음과 같이 지정할 경우에는

```
/primary/user/user1
```

휴지통 폴더가 제외됩니다.

## 부분 복원 시의 고려 사항

부분 복원은 메시지 저장소의 일부만 복원하는 것이고 전체 복원은 전체 메시지 저장소를 복원하는 것입니다. 메시지 저장소는 단일 복사본 메일 시스템을 사용합니다. 즉, 메일의 단일 복사본만 단일 파일로 저장소에 저장됩니다. 메일을 여러 메일함으로 보낼 때와 같은 메일의 다른 인스턴스는 해당 복사본에 대한 링크로 저장됩니다. 따라서 메일을 복원할 때 고려해야 할 사항이 있습니다. 예를 들면 다음과 같습니다.

- **전체 복원.** 전체 복원 도중에 연결된 메일은 계속해서 연결된 메일 파일과 동일한 색인 노드를 가리킵니다.
- **부분 백업/복원.** 부분 백업 및 복원 도중에는 메시지 저장소의 단일 복사본 특성이 유지되지 않을 수 있습니다.

다음 예에서는 부분 복원 작업을 수행할 때 여러 사용자가 사용하는 메일에 발생하는 변화를 보여 줍니다. 세 명의 사용자 A, B 및 C에 속하는 모두 동일한 다음 세 개의 메일이 있다고 가정합니다.

A/INBOX/1  
B/INBOX/1  
C/INBOX/1

**예 1.** 첫 번째 예에서는 시스템이 다음과 같이 부분 백업 및 전체 복원 절차를 수행합니다.

1. 사용자 B 및 C의 메일함을 백업합니다.
2. 사용자 B 및 C의 메일함을 삭제합니다.
3. 단계 1의 백업 데이터를 복원합니다.

이 예에서는 B/INBOX/1 및 C/INBOX/1에 새 색인 노드 번호가 할당되며 메일 데이터가 디스크의 새 위치에 기록됩니다. 하나의 메일만 복원되며 두 번째 메일은 첫 번째 메일에 대한 하드 링크입니다.

**예 2.** 이 예에서는 시스템이 다음과 같이 전체 백업 및 부분 복원 작업을 수행합니다.

1. 전체 백업을 수행합니다.
2. 사용자 A의 메일함을 삭제합니다.
3. 사용자 A의 메일함을 복원합니다.

A/INBOX/1에 새 색인 노드 번호가 할당됩니다.

**예 3.** 이 예에서는 여러 번의 부분 복원 시도가 필요할 수 있습니다.



1. 전체 백업을 수행합니다.  
B/INBOX/1 및 C/INBOX/1은 A/INBOX/1에 대한 링크로 백업됩니다.
2. 사용자 A 및 B의 메일함을 삭제합니다.
3. 사용자 B의 메일함을 복원합니다.  
복원 유틸리티는 관리자에게 A/INBOX를 먼저 복원할 것을 요청합니다.
4. 사용자 A 및 B의 메일함을 복원합니다.
5. 사용자 A의 메일함을 삭제합니다(선택 사항).

---

**주**           부분 복원으로 모든 메일이 복원되도록 하려면 `imsbackup` 명령을 `-i` 옵션과 함께 실행합니다. `-i` 옵션은 필요한 경우 모든 메일을 여러 번 백업합니다.

백업 장치를 검색할 수 있는 경우(예: 드라이브 또는 테이프) `imsrestore`는 A/INBOX/1을 포함하는 위치를 검색하여 B/INBOX/1으로 복원합니다. 백업 장치를 검색할 수 없는 경우(예: UNIX 파이프) `imsrestore`는 객체 아이디와 파일에 의존하는(연결된) 객체의 아이디를 기록하며 관리자는 `-r` 옵션과 함께 `imsrestore`를 다시 호출하여 누락된 메일 참조를 복원해야 합니다.

---

## 증분 백업된 메일함에서 메일 복원

증분 백업된 메일함에서 메일을 복원할 때 해당 메일함이 메일을 복원할 서버에 있는 경우 간단하게 `imesrestore`를 실행하여 메일을 복원할 수 있습니다. 그러나 증분 백업된 메일함에서 메일을 복원할 때 해당 메일함이 더 이상 없는 경우에는 다른 복원 절차를 따라야 합니다.

메시지 저장소 서버에 없는 메일함에 메일을 복원하려면 다음 절차 중 하나를 사용합니다.

- 복원 작업 도중에 사용자에게 대한 메일 전달을 비활성화합니다. 이렇게 하려면 LDAP 속성 `mailDeliveryOption`을 `hold`로 설정합니다.
- `imesrestore`를 사용하기 전에 `mboxutil -c` 명령을 사용하여 메일함을 만듭니다.

중분 백업을 복원할 때 이러한 지침을 따라야 하는 이유는 다음과 같습니다. 메일함이 삭제되거나 마이그레이션되면 `imsrestore` 유틸리티는 백업 아카이브에 저장된 메일함 고유 아이디 유효성과 메일 고유 아이디(UID)를 사용하여 메일함을 다시 만듭니다.

이전에는 `imsrestore`가 삭제되었거나 마이그레이션된 메일함을 다시 만들 때 새 UID 유효성을 메일함에 할당하고 새 UID를 메일에 할당했습니다. 이 경우 캐시된 메일을 가진 클라이언트는 메일함 UID 유효성과 메일 UID를 다시 동기화해야 합니다. 클라이언트가 새 데이터를 다시 다운로드해야 하므로 서버에서 작업 로드가 증가합니다.

새 `imsrestore` 동작의 경우에는 클라이언트 캐시가 동기화된 상태로 유지되며 복원 프로세스가 투명하게 작동하므로 성능에 부정적인 영향이 없습니다.

메일함이 있는 경우 `imsrestore`는 새 UID를 복원된 메일에 할당하므로 새 UID와 이미 기존 메일에 할당된 UID의 일관성이 유지됩니다. UID 일관성을 보장하기 위해 `imsrestore`는 복원 작업 도중에 메일함을 잠급니다. 그러나 `imsrestore`는 이제 새 UID 값을 할당하는 대신에 백업 아카이브의 메일함 UID 유효성과 메일 UID를 사용하므로 중분 백업 및 복원을 수행할 경우 UID가 일관되지 않을 수 있습니다.

`imsbackup` 유틸리티의 `-d` 날짜 옵션을 사용하여 중분 백업을 수행할 경우 복원 작업을 완료하기 위해 `imsrestore`를 여러 번 호출해야 할 수 있습니다. 중분 백업이 수행되었으면 최신 전체 백업과 이후의 모든 중분 백업을 복원해야 합니다.

복원 작업 사이에 새 메일을 메일함에 전달할 수 있지만 이 경우에는 메일 UID가 일관되지 않을 수 있습니다. UID의 비일관성을 방지하려면 위에 설명된 작업 중 하나를 수행해야 합니다.

## Legato Networker 사용

Messaging Server에는 Legato Networker와 같은 타사 백업 도구와의 인터페이스를 제공하는 백업 API가 포함되어 있습니다. 물리적 메시지 저장소 구조와 데이터 형식은 백업 API 내에서 캡슐화됩니다. 메시지 저장소와 직접 상호 작용하는 백업 API는 메시지 저장소의 논리적 뷰를 백업 서비스에 제공합니다. 백업 서비스는 메시지 저장소의 개념적 표시를 사용하여 백업 객체를 저장 및 복원합니다.

Messaging Server는 Legato Networker의 `save` 및 `recover` 명령으로 호출하여 메시지 저장소 데이터를 백업 및 복원할 수 있는 ASM(Application Specific Module)을 제공합니다. 호출된 ASM은 이어서 Messaging Server `imsbackup` 및 `imsrestore` 유틸리티를 호출합니다.

---

**주** 이 절에서는 Messaging Server 메시지 저장소와 함께 Legato Networker를 사용하는 방법에 대해 설명합니다. Legato Networker 인터페이스를 이해하려면 Legato 설명서를 참조하십시오.

---

## Legato Networker를 사용하여 데이터 백업

Legato Networker를 사용하여 Messaging Server 메시지 저장소의 백업을 수행하려면 Legato 인터페이스를 호출하기 전에 다음 예비 단계를 수행해야 합니다.

1. `/usr/lib/nsr/imsasm`에서 `msg_srv_base/lib/msg/imsasm`에 대한 심볼릭 링크를 만듭니다.
2. Sun 또는 Legato에서 `nsrfile` 이진 파일의 복사본을 얻어 다음 디렉토리에 복사합니다.

```
/usr/bin/nsr
```

이전 버전 Networker(5.x)를 사용 중인 경우에만 필요합니다. Networker 6.0 이상에서는 `nsrfile`이 `/usr/bin/nsr`에 자동으로 설치됩니다.

3. 그룹별로 사용자를 백업하려면 다음 단계를 수행합니다.
  - a. 612페이지의 “백업 그룹 만들기”에 설명된 대로 백업 그룹 파일을 만듭니다.
  - b. 구성을 확인하려면 `mkbackupdir.sh`를 실행합니다.

`mkbackupdir.sh`에 의해 작성된 디렉터리 구조를 확인합니다. 이 구조는 표 18-4에 나온 것과 비슷해야 합니다.

`backup-groups.conf` 파일을 지정하지 않을 경우 백업 프로세스는 모든 사용자에게 기본 백업 그룹 ALL을 사용합니다.

4. 백업 전에 `mkbakupdir.sh` 스크립트를 호출하기 위해 `/nsr/res/` 디렉토리에서 저장 그룹에 대한 `res` 파일을 만듭니다. 그 예는 [표 18-4](#)에 나와 있습니다.

---

**주** 이전 버전의 Legato Networker에서는 `saveset` 이름이 64자로 제한됩니다. 이 디렉토리 이름과 메일함의 논리 이름을 합친 것(예: `/primary/groupA/fred`)이 64자 이상인 경우 `mkbakupdir.sh -p`를 실행해야 합니다. 따라서 `mkbakupdir.sh`의 `-p` 옵션에 짧은 경로 이름을 사용해야 합니다. 예를 들어, 다음 명령은 `/backup` 디렉토리 아래에 백업 이미지를 만듭니다.

```
mkbakupdir.sh -p /backup
```

중요: 백업 디렉토리는 메시지 저장소 소유자(예: `inetuser`)가 쓸 수 있어야 합니다.

---

[그림 18-6](#)에서는 샘플 백업 그룹 디렉토리 구조를 보여 줍니다.

**그림 18-6** 백업 그룹 디렉토리 구조

```
/backup/primary/groupA/amy
                        /bob
                        /carly
/groupB/mary
                        /nancy
                        /zelda
/groupC/123go
                        /1bill
                        /354hut
```

아래 예에서는 `/nsr/res` 디렉토리에 있는 `IMS.res`라는 샘플 `res` 파일을 보여 줍니다.

```
type: savepnpc;
precmd: "echo mkbakupdir started",
        "/usr/siroe/server5/msg-siroe/bin/mkbakupdir.sh -p /backup";
pstcmd: "echo imsbakup Completed";
timeout: "12:00 pm";
```

이제 다음과 같이 Legato Networker 인터페이스를 실행할 준비가 되었습니다.

1. 필요한 경우 Messaging Server 저장 그룹을 만듭니다.
  - a. `nwadmin`을 실행합니다.
  - b. 사용자 정의 | 그룹 | 만들기를 선택합니다.
2. 다음과 같이 `savepnpc`를 백업 명령으로 사용하여 백업 클라이언트를 만듭니다.

- a. `saveset`를 `mkbackupdir`로 만든 디렉토리로 설정합니다.

단일 세션 백업의 경우 `/backup`을 사용합니다.

병렬 백업의 경우 `/backup/server/group`을 사용합니다.

612페이지의 “백업 그룹 만들기”에 정의된 대로 이미 `group`이 만들어졌는지 확인합니다.

백업 세션 수에 대해서도 병렬을 설정해야 합니다.

621페이지의 “예: Networker에서 백업 클라이언트 만들기”를 참조하십시오.

3. 그룹 제어 | 시작을 선택하여 백업 구성을 테스트합니다.

예: Networker에서 백업 클라이언트 만들기

Networker에서 백업 클라이언트를 만들려면 `nwadmin`에서 클라이언트 | 클라이언트 설치 | 만들기를 선택합니다.

```
Name: siroe
Group: IMS
Savesets: /backup/primary/groupA
          /backup/secondary/groupB
          /backup/tertiary/groupC
          .
          .
Backup Command: savepnpc
Parallelism: 4
```

## Legato Networker를 사용하여 데이터 복원

Legato Networker `nwrecover` 인터페이스나 `recover` 명령줄 유틸리티를 사용하여 데이터를 복구할 수 있습니다. 다음 예에서는 사용자 `a1`의 INBOX를 복구합니다.

```
recover -a -f -s siroe /backup/siroe/groupA/a1/INBOX
```

다음 예에서는 전체 메시지 저장소를 복구합니다.

```
recover -a -f -s siroe /backup/siroe
```

## Legato를 제외한 타사 백업 소프트웨어 사용

Messaging Server는 두 개의 메시지 저장소 백업 솔루션인 명령줄 `imsbackup`과 Solstice Backup(Legato Networker)을 제공합니다. 단일 `imsbackup`을 실행하여 전체 메시지 저장소를 백업하는 대량 메시지 저장소는 매우 많은 시간이 소요될 수 있습니다. Legato 솔루션은 여러 백업 장치에서의 동시 백업 세션을 지원합니다. 동시 백업으로 백업 시간을 대폭 단축시킬 수 있습니다(시간당 25GB의 데이터 백업 가능).

타사 동시 백업 소프트웨어(예: Netbackup)를 사용하는 경우 다음 방법을 사용하여 백업 소프트웨어를 Messaging Server와 통합할 수 있습니다.

1. 사용자를 그룹으로 분할하고(612페이지의 “백업 그룹 만들기” 참조)  
`msg_svr_base/config/` 디렉토리 아래에 `backup-groups.conf` 파일을 만듭니다.

---

**주** 이 백업 솔루션에는 추가 디스크 공간이 필요합니다. 모든 그룹을 동시에 백업하려는 경우 디스크 공간 요구 사항은 메시지 저장소 크기의 2배입니다. 디스크 공간이 충분치 않을 경우에는 사용자를 더 작은 그룹으로 분할한 다음 그룹 집합을 한꺼번에 백업합니다(예: `group1 - group5, group6 - group10`). 백업 후에는 그룹 데이터 파일을 제거합니다.

---

2. `imsbackup`을 실행하여 스테이징 영역에서 각 그룹을 파일로 백업합니다.  
명령은 `imsbackup -f <device> /<instance>/<group>`입니다.  
여러 `imsbackup` 프로세스를 동시에 실행할 수 있습니다. 예를 들면 다음과 같습니다.  

```
# imsbackup -f- /primary/groupA > /bkdata/groupA &  
# imsbackup -f- /primary/groupB > /bkdata/groupB &  
...
```

  
`imsbackup`은 큰 파일을 지원하지 않으므로 백업 데이터가 2GB 이상일 경우 `-f-` 옵션을 사용하여 데이터를 `stdout`에 기록한 다음 출력을 파일로 파이프해야 합니다.
3. 타사 백업 소프트웨어를 사용하여 스테이징 영역(이 예에서는 `/bkdata`)에서 그룹 데이터 파일을 백업합니다.

4. 사용자를 복원하려면 사용자의 그룹 파일 이름을 식별하고 테이프에서 해당 파일을 복원한 다음 `imsrestore`를 사용하여 데이터 파일에서 사용자를 복원합니다.

`imsrestore`는 큰 파일을 지원하지 않습니다. 데이터 파일이 2GB 이상일 경우 다음 명령을 사용합니다.

```
# cat /bkdata/groupA | imsrestore -f- /primary/groupA/andy
```

## 백업 및 복원 문제 해결

이 절에서는 일반적인 백업 및 복원 문제와 그 해결 방법에 대해 설명합니다.

- **문제:** `imsrestore` 또는 `imsasm`을 사용하여 폴더 또는 받은 메일함을 복원할 때 해당 폴더의 모든 메일이 현재 폴더에 추가됩니다. 이로 인해서 해당 폴더에 메일의 복사본이 여러 개 있게 됩니다.

**해결 방법:** `imsrestore`의 `-i` 플래그가 `imsasm` 스크립트에 설정되어 있지 않도록 하십시오.

- **문제:** 메일 폴더에 추가된 새 메일만 증분 백업하려고 하는데 전체 폴더가 백업됩니다. 새 메일만 백업하려면 어떻게 해야 합니까?

**해결 방법:** `imsbackup`에 `-d datetime` 플래그를 설정합니다. 이렇게 하면 지정된 날짜 및 시간에서 현재까지 저장된 메일이 백업됩니다. 기본값은 날짜와 상관없이 모든 메일을 백업하는 것입니다.

## 메시지 저장소 재해 복구 및 복원

재해란 전체 메시지 저장소에 매우 심각한 문제가 발생했음을 말합니다. 즉, 메시지 저장소 서버의 모든 데이터가 손실되는 경우가 이에 해당합니다. 다음의 손실 데이터를 복원하면 메시지 저장소 재해를 완전히 복원할 수 있습니다.

- 모든 메시지 저장소 데이터. 이 데이터는 [610페이지의 “메시지 저장소 백업 및 복원”](#)에서 설명하는 절차를 사용하여 백업할 수 있습니다. 파일 시스템 백업 방법을 사용하는 경우에는 다음 데이터를 백업해야 합니다.
  - 모든 메시지 저장소 분할 영역
  - `msg_svr_base/data/store/mboxlist`에 있는 메시지 저장소 데이터베이스 파일
- `msg_svr_base/data/store/dbdata/snapshots`에 있는 메시지 저장소 데이터베이스 스냅샷(메시지 저장소 데이터베이스 스냅샷 파일의 위치는 `configutil` 매개 변수로 구성할 수 있음). 파일 시스템 백업을 사용하는 경우에는 이 데이터가 복원된 후 `reconstruct -m after`를 실행하십시오.

- 다음을 포함하는 모든 구성 데이터
  - msg\_svr\_base/data/config에 있는 로컬 구성 파일
  - LDAP Directory Server의 Messaging Server 구성 데이터

## 사용자 액세스 모니터링

Messaging Server는 IMAP, POP 및 http를 통해 사용자의 메시지 저장소 액세스를 모니터링할 수 있는 `imsconnutil` 명령을 제공합니다. 또한 사용자의 마지막 로그인 및 로그아웃을 확인할 수 있습니다. 이 명령은 메시지 저장소별로 작동하므로 여러 메시지 저장소에 대해 사용할 수 없습니다.

---

**주** 이 기능 또는 기타 Messaging Server 기능을 사용하여 사용자의 전자 메일을 모니터링, 읽기 또는 액세스할 때 해당 법률이나 규칙을 위반하거나 고객 정책 또는 계약을 위반할 경우 책임이 따를 수 있습니다.

---

이 명령을 사용하려면 시스템 사용자(기본값: `inetuser`)가 루트로 액세스해야 하며 구성 변수 `local.imap.enableuserlist`, `local.http.enableuserlist`, `local.enablelastaccess`를 1로 설정해야 합니다.

IMAP 또는 웹 메일 클라이언트를 통해 현재 로그인한 사용자를 나열하려면 다음 명령을 사용합니다.

```
# imsconnutil -c
```

메시지 저장소에 있는 모든 사용자의 마지막 IMAP, POP 또는 Messenger Express 액세스(로그인 및 로그아웃)를 나열하려면 다음 명령을 사용합니다.

```
# imsconnutil -a
```

다음 명령은 1) 지정된 사용자가 IMAP나 Messenger Express 또는 `mshttp`를 통해 연결된 임의의 클라이언트(POP 사용자는 대개 연결 상태를 유지하지 않으므로 POP는 해당되지 않음)를 사용하여 현재 로그인했는지 확인하고 2) 사용자가 마지막으로 로그인 및 로그오프한 시간을 나열하는 두 가지 작업을 수행합니다.

```
# imsconnutil -c -a -u user_ID
```

다음 명령을 사용하여 사용자 목록이 파일에 한 행당 하나씩 입력될 수 있습니다.

```
# imsconnutil -c -a -f filename
```



또한 `-s` 플래그를 사용하여 특정 서비스(imap 또는 http)를 지정할 수도 있습니다. 예를 들어, 특정 사용자 아이디가 IMAP에 로그인했는지 여부를 나열하려면 다음 명령을 사용합니다.

```
# imskonutil -c -s imap -u user_ID
```

imskonutil 구문의 전체 설명은 *Sun Java System Messaging Server Administration Reference*를 참조하십시오.

다음은 몇 가지 출력 예입니다.

```
$ ./imskonutil -a -u soroork
UID IMAP last access HTTP last access POP last access
=====
soroork 08/Jul/2003:10:49:0510/Jul/2003:14:55:52----NOT-RECORDED----

$ ./imskonutil -c
IMAP
UID TIME AUTH          TO          FROM
=====
ed 17/Jun/2003:11:24:03plain172.58.73.45:193129.157.12.73:2631
bill17/Jun/2003:04:28:43plain172.58.73.45:193129.158.16.34:2340
mia 17/Jun/2003:09:36:54plain172.58.73.45:193192.18.184.103:3744
jay 17/Jun/2003:05:38:46plain172.58.73.45:193129.159.18.123:3687
paul17/Jun/2003:12:23:28plaintext172.58.73.45:193192.18.194.83:2943
tony17/Jun/2003:05:38:46plain172.58.73.45:193129.152.18.123:3688
anil17/Jun/2003:12:26:40plaintext172.58.73.45:193192.18.164.17:1767
anil17/Jun/2003:12:25:17plaintext172.58.73.45:193129.150.17.34:3117
jack17/Jun/2003:12:26:32plaintext172.58.73.45:193129.150.17.34:3119
toni17/Jun/2003:12:25:32plaintext172.58.73.45:193192.18.148.17:1764
=====
10 users were logged in to imap.
Feature is not enabled for http.
-----
```

## 메시지 저장소 문제 해결

이 절에서는 메시지 저장소를 능동적으로 유지 관리하기 위한 지침을 제공합니다. 또한 이 절에서는 메시지 저장소가 손상되었거나 예기치 않게 종료된 경우 사용할 수 있는 다른 메시지 저장소 복구 절차에 대해 설명합니다. 이 추가 메시지 저장소 복구 절차에 대한 절은 [632페이지의 “메일함 및 메일함 데이터베이스 복구”](#)를 확장한 것입니다.

이 절을 읽기 전에 이 장과 함께 *Sun Java System Messaging Server Administration Reference*의 명령줄 유틸리티 및 `configutil`에 대한 장을 검토하는 것이 좋습니다. 이 절은 다음 내용으로 구성되어 있습니다.

- [626페이지의 “표준 메시지 저장소 모니터링 절차”](#)
- [637페이지의 “일반 문제 및 해결 방법”](#)
- [629페이지의 “메시지 저장소 시작 및 복구”](#)
- [632페이지의 “메일함 및 메일함 데이터베이스 복구”](#)

## 표준 메시지 저장소 모니터링 절차

이 절에서는 메시지 저장소의 표준 모니터링 절차에 대해 개괄적으로 설명합니다. 이러한 절차는 일반적인 메시지 저장소 검사, 테스트 및 표준 유지 관리에 유용합니다.

자세한 내용은 [813페이지의 “메시지 저장소 모니터링”](#)을 참조하십시오.

### 하드웨어 공간 검사

메시지 저장소에는 충분한 추가 디스크 공간과 하드웨어 자원이 있어야 합니다. 메시지 저장소가 디스크 및 하드웨어 공간의 최대 한도에 가까이 도달하면 메시지 저장소 내에 문제가 발생할 수 있습니다.

디스크 공간 부족은 메일 서버 문제 및 오류의 가장 일반적인 원인 중 하나입니다. 메시지 저장소에 쓰기 위한 공간이 없을 경우 메일 서버에서 오류가 발생합니다. 또한 사용 가능한 디스크 공간이 일정한 임계값 아래로 내려가면 메일 전달, 로깅 등과 관련된 문제가 발생합니다. `stored` 프로세스의 정리 기능이 실패하고 삭제된 메일이 메시지 저장소에서 정리되지 않으면 디스크 공간이 급속도로 줄어들 수 있습니다.

디스크 공간 모니터링에 대한 자세한 내용은 [604페이지의 “디스크 공간 모니터”](#) 및 [813페이지의 “메시지 저장소 모니터링”](#)을 참조하십시오.

### 로그 파일 검사

로그 파일을 검사하여 메시지 저장소 프로세스가 구성된 대로 실행되는지 확인합니다. `Messaging Server`는 지원되는 각각의 주요 프로토콜 또는 서비스(SMTP, IMAP, POP 및 HTTP)에 대한 별도의 로그 파일 집합을 만듭니다. 이러한 로그 파일은 콘솔을 통해서나 `msg_svr_base/log/` 디렉토리에서 확인할 수 있습니다. 정기적으로 로그 파일을 모니터링해야 합니다.

로깅이 서버 성능에 영향을 줄 수 있다는 것을 유의하십시오. 더 자세한 로깅을 지정할수록 일정한 시간 동안 로그 파일이 차지하는 디스크 공간이 더 많아집니다. 따라서 효과적이면서 실제적인 로그 회전, 만료 및 백업 정책을 서버에 정의해야 합니다. 서버의 로깅 정책 정의에 대한 자세한 내용은 [21장](#), “[로깅 관리](#)” 를 참조하십시오.

## 사용자 IMAP/POP 세션 검사

Messaging Server는 사용자의 전체 IMAP 또는 POP 세션을 파일로 캡처할 수 있는 원격 측정이라는 기능을 제공합니다. 이 기능은 클라이언트 문제를 디버깅하는 데 유용합니다. 예를 들어, 사용자가 메일 액세스 클라이언트가 제대로 작동하지 않는다고 불평할 경우 이 기능을 사용하여 액세스 클라이언트와 Messaging Server 사이의 상호 작용을 추적할 수 있습니다.

세션을 캡처하려면 다음 디렉토리를 만들기만 하면 됩니다.

```
msg_svr_base/data/telemetry/pop_or_imap/userid
```

Messaging Server는 이 디렉토리에서 세션당 하나의 파일을 만듭니다. 출력 예는 다음과 같습니다.

```
LOGIN redb 2003/11/26 13:03:21
>0.017>1 OK User logged in
<0.047<2 XSERVERINFO MANAGEACCOUNTURL MANAGELISTSURL MANAGEFILTERSURL
>0.003>* XSERVERINFO MANAGEACCOUNTURL {67}
http://redb@cuisine.blue.planet.com:800/bin/user/admin/bin/enduser
MANAGELISTSURL NIL MANAGEFILTERSURL NIL
2 OK Completed
<0.046<3 select "INBOX"
>0.236>* FLAGS (\Answered flagged #raft #eleted \Seen $MDNSent Junk)
* OK [PERMANENTFLAGS (\Answered flagged #raft #eleted \Seen $MDNSent Junk \*)]
* 1538 EXISTS
* 0 RECENT
* OK [UNSEEN 23]
* OK [UIDVALIDITY 1046219200]
* OK [UIDNEXT 1968]
3 OK [READ-WRITE] Completed
<0.045<4 UID fetch 1:* (FLAGS)
>0.117>* 1 FETCH (FLAGS (\Seen) UID 330)
* 2 FETCH (FLAGS (\Seen) UID 331)
* 3 FETCH (FLAGS (\Seen) UID 332)
* 4 FETCH (FLAGS (\Seen) UID 333)
* 5 FETCH (FLAGS (\Seen) UID 334)
<etc>
```

## stored 프로세스 검사

stored 함수는 메일 데이터베이스의 교착 상태 및 트랜잭션 작업, 에이징 정책 적용, 디스크에 저장된 메일 정리 및 삭제와 같은 여러 중요한 작업을 수행합니다. stored의 실행이 중지되면 Messaging Server에서 문제가 발생합니다. start-msg가 실행될 때 stored가 시작되지 않을 경우 다른 프로세스는 시작되지 않습니다.

- stored 프로세스가 실행 중인지 확인합니다. `stored -t -v`를 실행합니다.
- `store_root/mbolist`에서 작성된 로그 파일을 확인합니다.
- 기본 로그 파일 `msg_svr_base/log/default/default`에서 stored 메일을 확인합니다.
- stored 프로세스에서 다음 기능 중 하나를 시도할 때마다 `msg_svr_base/config/` 디렉토리에 있는 다음 파일의 타임스탬프가 업데이트되는지 확인합니다.

**표 18-14** stored 작업

| stored 작업  | 기능                                                |
|------------|---------------------------------------------------|
| stored.ckp | 데이터베이스 검사점이 시작될 때 수정됩니다. 약 1분마다 시간이 기록됩니다.        |
| stored.lcu | 데이터베이스 로그가 정리될 때마다 수정됩니다. 약 5분마다 시간이 기록됩니다.       |
| stored.per | 사용자 단위 db 쓰기가 생성될 때마다 수정됩니다. 1시간에 한 번씩 시간이 기록됩니다. |

stored 프로세스에 대한 자세한 내용은 604페이지의 “stored 유틸리티 사용”과 *Messaging Server Reference Manual*의 Messaging Server Command-line Utilities 장에서 stored 유틸리티를 참조하십시오.

stored 기능 모니터링에 대한 자세한 내용은 813페이지의 “메시지 저장소 모니터링”을 참조하십시오.

## 데이터베이스 로그 파일 검사

데이터베이스 로그 파일은 `store_root/mbolist` 디렉토리에 있는 `sleepycat` 트랜잭션 검사점 지정 로그 파일을 나타냅니다. 로그 파일이 누적될 경우 데이터베이스 검사점 지정이 발생하지 않습니다. 일반적으로 단일 기간 동안 둘 또는 세 개의 데이터베이스 로그 파일이 존재합니다. 파일이 더 많이 있을 경우는 문제가 발생한 것일 수 있습니다.

## 사용자 폴더 검사

사용자 폴더를 검사하려는 경우 모든 사용자 폴더를 검토하고 오류를 보고하는 `reconstruct -r -n`(재귀적 수정 없음) 명령을 실행할 수 있습니다. `reconstruct` 명령에 대한 자세한 내용은 [632페이지의 “메일함 및 메일함 데이터베이스 복구”](#)를 참조하십시오.

## 코어 파일 검사

코어 파일은 프로세스가 예기치 않게 종료된 경우에만 존재합니다. 특히 메시지 저장소에 문제가 있을 경우 이러한 파일을 검토하는 것이 중요합니다. Solaris에서는 `coreadm`을 사용하여 `core` 파일 위치를 구성합니다.

## 메시지 저장소 시작 및 복구

메시지 저장소 데이터는 메일, 색인 데이터 및 메시지 저장소 데이터베이스로 구성됩니다. 이 데이터는 상당히 견고하지만 가끔 시스템에 메시지 저장소 데이터 문제가 발생할 수 있습니다. 이러한 문제는 기본 로그 파일에서 나타나며 그 대부분이 항상 투명하게 수정됩니다. 아주 드물게 로그 파일의 오류 메시지가 `reconstruct` 유틸리티를 실행해야 한다는 것을 나타낼 수 있습니다. 또한 메일을 보호하기 위한 마지막 수단으로 [610페이지의 “메시지 저장소 백업 및 복원”](#)에 설명된 백업 및 복원 프로세스가 사용됩니다. 이 절에서는 `stored`의 자동 시작 및 복구 프로세스를 중심으로 설명합니다.

메시지 저장소는 이전에 관리자가 담당하던 많은 복구 작업을 자동화합니다. 이러한 작업은 시작 시에 메시지 저장소 데몬 `stored`에 의해 수행되며 필요에 따라 데이터베이스 스냅샷 및 자동 고속 복구를 포함합니다. `stored`는 메시지 저장소의 데이터베이스를 철저히 검사하여 문제가 감지된 경우 이를 자동으로 복구합니다.

`stored`는 또한 상태 메시지를 통해 포괄적인 데이터베이스 상태 분석을 기본 로그에 제공하여 메시지 저장소에 대해 수행된 복구 작업과 메시지 저장소를 작동시키기 위한 자동 시도를 보고합니다.

## 자동 시작 및 복구 — 작동 원리

`stored` 데몬은 다른 메시지 저장소 프로세스보다 먼저 시작됩니다. 이 데몬은 메시지 저장소 데이터베이스를 초기화하고 필요한 경우 복구합니다. 메시지 저장소 데이터베이스는 폴더, 할당량, 가입 및 메일 플래그 정보를 보관합니다. 데이터베이스는 로깅 및 트랜잭션 가능하여 이미 복구가 내장되어 있습니다. 또한 일부 데이터베이스 정보는 각 폴더의 메일 색인 영역에서 중복하여 복사됩니다.

데이터베이스는 상당히 견고하지만 가끔씩 손상될 수 있으며 stored는 대부분의 경우 이 문제를 투명하게 복구합니다. 그러나 stored를 다시 시작할 때마다 기본 로그 파일을 검사하여 추가 관리 개입이 필요하지 않은지 확인해야 합니다. 데이터베이스의 추가 재작성이 필요한 경우 로그 파일의 상태 메시지에 reconstruct를 실행하라는 내용이 나타납니다.

메시지 저장소 데이터베이스를 열기 전에 stored는 무결성을 분석하고 경고 범주에 속하는 상태 메시지를 기본 로그로 보냅니다. 일부 메시지는 관리자에게 유용하며 다른 일부는 내부 분석에 사용되는 코딩된 데이터로 구성됩니다. stored는 문제를 감지하면 데이터베이스를 수정하고 재시작을 시도합니다.

데이터베이스가 열리면 stored는 나머지 서비스를 시작할 수 있다는 것을 알립니다. 자동 수정이 실패할 경우 기본 로그의 메시지는 수행할 작업을 지정합니다. 자세한 내용은 630 페이지의 **“reconstruct -m이 필요하다는 것을 지정하는 오류 메시지”**를 참조하십시오.

이전 릴리스에서는 stored에서 복구 프로세스를 구현하는 데 매우 오래 걸려서 관리자가 stored를 "중단"된 것으로 여기기도 했습니다. 이제 이러한 긴 복구 유형은 제거되었으며 stored는 1분 이내에 최종 상태를 확인해야 합니다. 그러나 stored가 스냅샷 복구와 같은 복구 기술을 사용해야 할 경우 프로세스는 몇 분 정도가 소요될 수 있습니다.

대부분의 경우 복구가 수행된 후에 데이터베이스는 최신 상태로 업데이트되며 다른 작업은 필요하지 않습니다. 그러나 일부 복구는 메시지 저장소의 중복 데이터를 동기화하기 위해 reconstruct -m이 필요합니다. 이러한 내용도 기본 로그에 표시되므로 시작 후에 기본 로그를 모니터링하는 것이 중요합니다. 메시지 저장소가 시작되어 정상적으로 실행되는 것처럼 보이는 경우에도 reconstruct와 같은 요청된 모든 작업을 실행해야 합니다.

로그 파일을 읽어야 하는 또 다른 이유는 처음에 데이터베이스를 손상시킨 원인을 확인하는 데 있습니다. stored는 시스템상의 문제와 무관하게 메시지 저장소를 사용하도록 설계되었지만 데이터베이스 손상이 숨겨진 더 큰 문제의 일부일 수 있으므로 그 원인을 확인하는 것이 필요합니다.

### **reconstruct -m이 필요하다는 것을 지정하는 오류 메시지**

이 절에서는 reconstruct -m을 실행해야 하는 오류 메시지 유형에 대해 설명합니다.

오류 메시지가 메일함 오류를 나타내면 reconstruct <mailbox>를 실행합니다. 예를 들면 다음과 같습니다.

```
"Invalid cache data for msg 102 in mailbox user/joe/INBOX. Needs reconstruct"
```

```
"Mailbox corrupted, missing fixed headers: user/joe/INBOX"
```

```
"Mailbox corrupted, start_offset beyond EOF: user/joe/INBOX"
```

오류 메시지가 데이터베이스 오류를 나타내면 `reconstruct -m`을 실행합니다. 예를 들면 다음과 같습니다.

```
"Removing extra database logs. Run reconstruct -m soon after startup to resync redundant data"
```

```
"Recovering database from snapshot. Run reconstruct -m soon after startup to resync redundant data"
```

## 데이터베이스 스냅샷

스냅샷은 데이터베이스의 핫 백업으로 `stored`에서 손상된 데이터베이스를 몇 분 안에 투명하게 복원하기 위해 사용합니다. 이것은 다른 영역에 저장된 중복된 정보에 의존하는 `reconstruct`를 사용하는 것보다 훨씬 더 빠릅니다.

## 메시지 저장소 데이터베이스 스냅샷 – 작동 원리

`mboxlist` 디렉토리에 있는 데이터베이스의 스냅샷은 기본적으로 24시간에 한 번씩 자동으로 생성됩니다. 스냅샷은 기본적으로 `store` 디렉토리의 하위 디렉토리에 복사됩니다. 언제든지 기본적으로 다섯 개의 스냅샷(라이브 데이터베이스 하나, 스냅샷 세 개, 데이터베이스/제거된 복사본 하나)이 있습니다. 데이터베이스/제거된 복사본이 가장 최신 버전이며 `mboxlist` 데이터베이스 디렉토리의 `removed` 하위 디렉토리로 보내지는 데이터베이스의 긴급 복사본입니다.

현재 데이터베이스가 손상된 것으로 확인되어 복구 프로세스에서 이를 제거하기로 결정한 경우 `stored`는 가능한 경우 해당 데이터베이스를 `removed` 디렉토리로 이동합니다. 이렇게 하면 필요에 따라 데이터베이스를 분석할 수 있습니다.

데이터 이동은 일주일에 한 번만 발생합니다. 따라서 이미 데이터베이스 복사본이 있는 경우에는 `stored`에서 저장소를 만들 때마다 데이터베이스 복사본을 교체하지 않습니다. `stored`는 `removed` 디렉토리의 데이터가 1주일보다 오래된 경우에만 교체를 수행합니다. 이것은 문제가 있는 원래 데이터베이스가 계속적인 시작으로 인해 너무 빨리 대체되는 것을 방지합니다.

## 메시지 저장소 데이터베이스 스냅샷 간격 및 위치 지정

결합된 데이터베이스와 스냅샷의 5배에 해당하는 공간이 있어야 합니다. 관리자는 스냅샷을 별개의 디스크에서 실행되도록 다시 구성하고 시스템 요구에 맞게 조정하는 것이 좋습니다.

`stored`가 시작 시에 데이터베이스 문제를 감지할 경우 최적의 스냅샷이 자동으로 복구됩니다. 세 개의 스냅샷 변수는 스냅샷 파일 위치, 스냅샷 촬영 간격, 저장되는 스냅샷 수 등과 같은 매개 변수를 설정할 수 있습니다. 이러한 `configutil` 매개 변수는 표 18-15에 나와 있습니다.

스냅샷 간격이 너무 작으면 시스템에 자주 부담을 주게 되며 데이터베이스의 문제가 스냅샷으로 복사될 가능성이 더 커집니다. 스냅샷 간격이 너무 크면 스냅샷을 가져왔을 때 갖고 있던 상태를 데이터베이스가 계속 보유하는 상황이 발생할 수 있습니다.

스냅샷 간격으로 1일이 권장되지만 시스템상에 문제가 수일 동안 지속되거나 문제가 존재하기 전의 시점으로 되돌아가려는 경우 일주일 이상의 간격이 유용할 수 있습니다.

stored는 데이터베이스를 모니터링하여 데이터베이스가 완전하지 않다고 의심될 경우 최신 스냅샷을 거부하며 그 대신에 가장 안정적인 최신 스냅샷을 검색합니다. 하루 전의 스냅샷을 검색할 수 있다는 사실에도 불구하고 시스템은 보다 최신의 중복 데이터가 있는 경우 이를 사용하며 이전 스냅샷 데이터를 무시합니다.

따라서 스냅샷의 궁극적인 역할은 시스템을 가능한 최신 상태로 유지하고 데이터를 즉석에서 재작성하려고 시도하는 시스템의 나머지 부분에 대한 부담을 줄여 주는 것입니다.

**표 18-15** 메시지 저장소 데이터베이스 스냅샷 매개 변수

| 매개 변수                        | 설명                                                                                          |
|------------------------------|---------------------------------------------------------------------------------------------|
| local.store.snapshotpath     | 메시지 저장소 데이터베이스 스냅샷 파일의 위치입니다. 기존 절대 경로 또는 store 디렉토리에 대한 상대 경로입니다.<br>기본값: dbdata/snapshots |
| local.store.snapshotinterval | 스냅샷 간격(분)입니다. 유효 값: 1 - 46080<br>기본값: 1440(1440분 = 1일)                                      |
| local.store.snapshotdirs     | 보관되는 다른 스냅샷 수입니다. 유효 값: 2 - 367<br>기본값: 3                                                   |

## 메일함 및 메일함 데이터베이스 복구

하나 이상의 메일함이 손상되면 reconstruct 유틸리티를 사용하여 메일함 또는 메일함 데이터베이스를 다시 작성하고 모든 불일치를 복구할 수 있습니다.



reconstruct 유틸리티는 하나 이상의 메일함 또는 마스터 메일함 파일을 다시 작성하고 모든 불일치를 복구합니다. 이 유틸리티를 사용하면 메시지 저장소에서 거의 모든 형태의 데이터 손상을 복구할 수 있습니다. [630페이지의 “reconstruct -m이 필요하다는 것을 지정하는 오류 메시지”](#)를 참조하십시오.

**주** 트랜잭션 완료나 불완전한 트랜잭션 롤백과 같은 저급 데이터베이스 복구는 시작 시에 자동으로 수행됩니다.

표 18-16에는 reconstruct 옵션이 나열되어 있습니다. 구문 및 사용 요구 사항에 대한 자세한 내용은 *Sun Java System Messaging Server Administration Reference*(<http://docs.sun.com/doc/819-0106>)를 참조하십시오.

**표 18-16** reconstruct 옵션

| 옵션 | 설명                                                                                                                                                                                                                                                                                                              |
|----|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| -e | 재구성하기 전에 store.exp 파일을 제거합니다. 이렇게 하면 저장 프로세스에서 정리하지 않은 제거된 메일에 대한 모든 내부 저장소 레코드가 제거됩니다. -i 또는 -e 옵션은 폴더가 실제로 재구성될 때만 작동하므로 이러한 옵션을 사용할 때 -f 옵션을 사용하는 것도 유용합니다. 마찬가지로 재구성이 아닌 검사를 수행하는 -n 옵션을 사용할 경우 -i 및 -e 옵션이 작동하지 않습니다. reconstruct가 손상을 감지하지 못하는 경우 reconstruct -e를 실행하면 제거된 메일이 복구되지 않습니다. -f는 재구성을 실행합니다. |
| -i | 재구성 전에 store.idx 파일 길이를 0으로 설정합니다. -i 또는 -e 옵션은 폴더가 실제로 재구성될 때만 작동하므로 이러한 옵션을 사용할 때 -f 옵션을 사용하는 것도 유용합니다. 마찬가지로 재구성이 아닌 검사를 수행하는 -n 옵션을 사용할 경우 -i 및 -e 옵션이 작동하지 않습니다.                                                                                                                                           |
| -f | reconstruct를 수행하여 메일함을 수정합니다.                                                                                                                                                                                                                                                                                   |
| -l | lright.db를 재구성합니다.                                                                                                                                                                                                                                                                                              |
| -m | 일관성 검사를 수행하고 필요한 경우 메일함 데이터베이스를 복구합니다. 이 옵션은 스펠 영역에서 찾은 모든 메일함을 검사하고 메일함 데이터베이스에서 적절하게 항목을 추가 또는 제거합니다. 데이터베이스에서 항목을 추가 또는 제거할 때마다 표준 출력 파일에 메일이 인쇄됩니다. 특히 folder.db, quota.db 및 lright.db를 수정합니다.                                                                                                              |
| -n | 메일함을 수정하지 않고 메시지 저장소만 검사합니다. 메일함 이름을 제공하지 않을 경우 -n 옵션을 단독으로 사용할 수 없습니다. 메일함 이름을 제공하지 않을 때는 -n 옵션을 -r 옵션과 함께 사용해야 합니다. -r 옵션은 -p 옵션과 함께 사용할 수 있습니다. 예를 들어, 다음 명령은 모두 유효합니다.                                                                                                                                      |
|    | <pre>reconstruct -n user/dulcinea/INBOX reconstruct -n -r reconstruct -n -r -p primary reconstruct -n -r user/dulcinea/</pre>                                                                                                                                                                                   |

**표 18-16** reconstruct 옵션

| 옵션                    | 설명                                                                                                                                                                                                                                                                                                                                                          |
|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| -o                    | 폐기되었습니다. mboxutil -o를 참조하십시오.                                                                                                                                                                                                                                                                                                                               |
| -o -d <i>filename</i> | 폐기되었습니다. mboxutil -o를 참조하십시오.                                                                                                                                                                                                                                                                                                                               |
| -p <i>partition</i>   | -p 옵션은 -m 옵션과 함께 사용되며 재구성의 범위를 지정한 분할 영역으로 제한합니다. -p 옵션을 지정하지 않을 경우 reconstruct에서 모든 분할 영역이 기본값이 됩니다. 구체적으로 이 옵션은 folder.db 및 quota.db를 수정하지만 lright.db는 수정하지 않습니다. 이는 lright.db를 수정하려면 메시지 저장소의 모든 사용자에게 acl을 스캔해야 하기 때문입니다. 모든 분할 영역에 대해 이 작업을 수행하는 것은 그리 효율적이지 않습니다. lright.db를 수정하려면 reconstruct -l을 실행합니다.<br><br>분할 영역 이름을 지정하며 전체 경로 이름을 사용하면 안 됩니다. |
| -q                    | 할당량 하위 시스템의 모든 불일치(예: 잘못된 할당량 루트를 가진 메일함 또는 잘못된 할당량 사용이 보고된 할당량 루트)를 수정합니다. 다른 서버 프로세스가 실행되는 동안 -q 옵션을 실행할 수 있습니다.                                                                                                                                                                                                                                          |
| -r [ <i>mailbox</i> ] | 지정된 메일함의 분할 영역에 대한 일관성 검사를 복구 및 수행합니다. -r 옵션은 또한 지정된 메일함 내의 모든 하위 메일함을 복구합니다. 메일함 인수 없이 -r을 지정할 경우 사용자 분할 영역 디렉토리에 있는 모든 메일함의 스푼 영역이 복구됩니다.                                                                                                                                                                                                                 |
| -u <i>user</i>        | -u 옵션은 -m 옵션과 함께 사용되며 재구성의 범위를 지정한 사용자로 제한합니다. -u 옵션은 -p 옵션과 함께 사용해야 합니다. -u 옵션을 지정하지 않을 경우 모든 분할 영역이나 -p 옵션을 사용하여 지정한 분할 영역이 reconstruct에서 기본값이 됩니다.<br><br>분할 영역 이름을 지정하며 전체 경로 이름을 사용하면 안 됩니다.                                                                                                                                                           |

## 메일함 재작성

메일함을 다시 작성하려면 -r 옵션을 사용합니다. 다음 경우에 이 옵션을 사용해야 합니다.

- 메일함에 액세스하면 "System I/O error" 또는 "Mailbox has an invalid format" 중 하나의 오류가 발생하는 경우
- 메일함에 액세스할 때 서버 충돌이 발생하는 경우
- 스푼 디렉토리에서 파일이 추가 또는 제거된 경우

reconstruct -r은 우선 일관성 검사를 실행합니다. 이 검사는 모든 일관성을 보고하며 문제가 감지된 경우에만 재작성을 수행합니다. 결과적으로 이 릴리스에서 reconstruct 유틸리티의 성능이 향상됩니다.

다음 예에 설명된 대로 reconstruct를 사용할 수 있습니다.

사용자 daphne에 속하는 메일함의 스푼 영역을 다시 작성하려면 다음 명령을 사용합니다.

```
reconstruct -r user/daphne
```

메일함 데이터베이스에 나열된 모든 메일함의 스폴 영역을 다시 작성하려면 다음 명령을 사용합니다.

```
reconstruct -r
```

대용량 메시지 저장소의 경우 메일함 데이터베이스에 나열된 모든 메일함의 스폴 영역을 다시 작성하는 것이 아주 오래 걸릴 수 있으므로 이 옵션은 신중하게 사용해야 합니다.

[636페이지의 “reconstruct 성능”](#)을 참조하십시오. 저장소에 여러 디스크를 사용하는 것이 보다 나은 오류 복구 방법일 수 있습니다. 디스크가 하나가 중지되었다고 전체 저장소가 중지되지는 않습니다. 디스크가 손상된 경우 다음과 같이 `-p` 옵션을 사용하여 저장소의 일부만 다시 작성하면 됩니다.

```
reconstruct -r -p subpartition
```

`primary` 분할 영역에 있을 경우에만 명령줄 인수에 나열된 메일함을 다시 작성하려면 다음 명령을 수행합니다.

```
reconstruct -p primary mbox1 mbox2 mbox3
```

`primary` 분할 영역에 있는 모든 메일함을 다시 작성할 필요가 없을 경우 다음 명령을 사용합니다.

```
reconstruct -r -p primary
```

`reconstruct`를 실행하여 일관성 검사를 수행하지 않고 폴더를 다시 작성하려면 `-f` 옵션을 사용합니다. 예를 들어, 다음 명령을 실행하여 사용자 폴더 `daphne`를 다시 구성합니다.

```
reconstruct -f -r user/daphne
```

모든 메일함을 수정하지 않고 검사하려면 다음과 같이 `-n` 옵션을 사용합니다.

```
reconstruct -r -n
```

## 메일함 검사 및 복구

메일함 데이터베이스의 고급 일관성 검사와 복구를 수행하려면 다음 명령을 사용합니다.

```
reconstruct -m
```

기본 분할 영역의 일관성 검사와 복구를 수행하려면 다음 명령을 사용합니다.

```
reconstruct -p primary -m
```

---

**주** `reconstruct`를 `-p` 및 `-m` 플래그와 함께 실행하면 `light.db`가 수정되지 않습니다. 이는 `light.db`를 수정하려면 메시지 저장소의 모든 사용자에게 대한 ACL을 스캔해야 하기 때문입니다. 모든 분할 영역에 대해 이 작업을 수행하는 것은 그리 효율적이지 않습니다. `light.db`를 수정하려면 `reconstruct -l`을 실행합니다.

---

`john`이라는 개별 사용자의 메일함에 대한 일관성 검사와 복구를 수행하려면 다음 명령을 사용합니다.

```
reconstruct -p primary -u john -m
```

다음 경우에 `-m` 옵션을 사용해야 합니다.

- 하나 이상의 디렉토리가 저장소 스푼 영역에서 제거되어 메일함 데이터베이스 항목 또한 제거해야 하는 경우
- 하나 이상의 디렉토리가 저장소 스푼 영역에서 복원되어 메일함 데이터베이스 항목을 또한 추가해야 하는 경우
- `stored -d` 옵션으로 데이터베이스의 일관성을 유지할 수 없는 경우  
stored -d 옵션으로 데이터베이스의 일관성을 유지할 수 없는 경우에는 다음 단계를 나열된 순서대로 수행합니다.
  - 모든 서버를 종료합니다.
  - `store_root/mboxlist`의 모든 파일을 제거합니다.
  - 서버 프로세스를 다시 시작합니다.
  - `reconstruct -m`을 실행하여 스푼 영역 내용에서 새 메일함 데이터베이스를 작성합니다.

## reconstruct 성능

reconstruct가 작업을 수행하는 데 걸리는 시간은 다음 요소에 따라 달라집니다.

- 수행하는 작업의 종류 및 선택한 옵션
- 디스크 성능
- `reconstruct -m` 실행 시의 폴더 수
- `reconstruct -r` 실행 시의 메일 수
- 메시지 저장소의 전체 크기
- 시스템이 실행 중인 다른 프로세스 및 시스템 사용량
- 진행 중인 POP, IMAP, HTTP 또는 SMTP 활동이 있는지 여부

`reconstruct -r` 옵션은 초기 일관성 검사를 수행합니다. 이 검사는 다시 작성해야 하는 폴더 수에 따라 reconstruct 성능을 향상시킵니다.

약 2400명의 사용자와 85GB의 메시지 저장소가 있으며 서버에 동시 POP, IMAP 또는 SMTP 활동이 있는 시스템에서 다음 성능이 확인되었습니다.

- `reconstruct -m`은 약 1시간이 걸렸습니다.

- `reconstruct -r -f`는 약 18시간이 걸렸습니다.

---

**주**            진행 중인 POP, IMAP, HTTP 또는 SMTP 활동을 서버에서 수행하지 않을 경우 `reconstruct` 작업에는 훨씬 더 적은 시간이 소요될 수 있습니다.

---

## 일반 문제 및 해결 방법

이 절에서는 다음과 같은 일반적인 메시지 저장소 문제와 해결 방법에 대해 설명합니다.

- 637페이지의 “메일 페이지를 로드하지 않는 Messenger Express 또는 Communications Express”
- 637페이지의 “와일드카드 패턴을 사용하는 명령이 작동하지 않음”
- 638페이지의 “알 수 없거나 잘못된 분할 영역”
- 638페이지의 “사용자 메일함 디렉토리 문제”

### 메일 페이지를 로드하지 않는 Messenger Express 또는 Communications Express

사용자가 Messenger Express 페이지 또는 Communications Express 메일 페이지를 로드할 수 없는 경우 압축 후에 데이터가 손상되었을 수 있습니다. 이 문제는 시스템에서 오래된 프록시 서버를 배포한 경우에 종종 발생할 수 있습니다. 이 문제를 해결하려면 `local.service.http.gzip.static` 및 `local.service.http.gzip.dynamic`을 0으로 설정하여 데이터 압축을 비활성화해 보십시오. 문제가 해결되면 프록시 서버를 업데이트할 수 있습니다.

### 와일드카드 패턴을 사용하는 명령이 작동하지 않음

UNIX 셸의 경우 일부는 와일드카드 매개 변수에 따옴표가 필요하지만 일부는 그렇지 않습니다. 예를 들어, C 셸은 와일드카드(\*, ?)를 파일로 포함하는 인수 확장을 시도하며 일치하는 항목이 없으면 실패합니다. 이러한 패턴 일치 인수를 `mbxutil`과 같은 명령에 전달하려면 따옴표로 묶어야 할 수 있습니다.

예를 들면 다음과 같습니다.

```
mbxutil -l -p user/usr44*
```

Bourne 셸에서 작동하지만 `tsch` 및 C 셸에서는 실패합니다. 이러한 셸에는 다음이 필요합니다.

```
mbxutil -l -p "user/usr44*"
```

와일드카드 패턴을 사용하는 명령이 작동하지 않을 경우 해당 셸의 와일드카드를 따옴표로 묶어야 하는지 여부를 확인합니다.

## 알 수 없거나 잘못된 분할 영역

메일함을 방금 만든 새 분할 영역으로 이동했거나 Messaging Server를 갱신 또는 다시 시작하지 않은 경우 Messenger Express에서 "Unknown/invalid partition"이라는 메시지가 표시될 수 있습니다. 이 문제는 새 분할 영역에서만 발생합니다. 이제 추가 사용자 메일함을 이 새 분할 영역에 추가할 경우 Messaging Server를 갱신 또는 다시 시작할 필요가 없습니다.

## 사용자 메일함 디렉토리 문제

메시지 저장소 손상이 몇몇의 사용자로 제한되고 시스템에 대한 전역 손상이 없을 경우 사용자 메일함 문제가 발생합니다. 다음 지침은 사용자 메일함 디렉토리 문제를 식별, 분석 및 해결하기 위한 프로세스를 제시합니다.

1. 로그 파일, 오류 메시지 또는 관찰된 모든 비정상적인 동작을 검토합니다.
2. 정보와 기록을 계속 디버깅하려면 전체 `store_root/mboxlist/` 사용자 디렉토리를 메시지 저장소 외부의 다른 위치로 복사합니다.
3. 문제를 일으키는 사용자 폴더를 찾으려면 `reconstruct -r -n` 명령을 실행합니다. `reconstruct`를 사용하여 폴더를 찾을 수 없는 경우 `folder.db`에 폴더가 존재할 수 있습니다.

`reconstruct -r -n` 명령을 사용하여 폴더를 찾을 수 없는 경우 `hashdir` 명령을 사용하여 위치를 확인합니다. `hashdir`에 대한 자세한 내용은 602페이지의 “[hashdir 유틸리티](#)”와 *Messaging Server Reference Manual*의 Messaging Server Command-line Utilities 장에서 `hashdir` 유틸리티를 참조하십시오.

4. 폴더를 찾은 후에는 파일과 권한을 검사하고 적절한 파일 크기를 확인합니다.
5. `reconstruct -r(-n 옵션 없이)`을 사용하여 메일함을 다시 작성합니다.
6. 사용자가 관찰한 문제를 `reconstruct`에서 감지하지 않을 경우 `reconstruct -r -f` 명령을 실행하여 메일 폴더를 다시 구성할 수 있습니다.
7. 폴더가 `mboxlist` 디렉토리(`store_root/mboxlist`)에 존재하지 않지만 `partition` 디렉토리(`store_root/partition`)에 존재할 경우 전역 불일치가 존재할 수 있습니다. 이 경우 `reconstruct -m` 명령을 실행해야 합니다.

8. 이전 단계들로 문제가 해결되지 않을 경우 `store.idx` 파일을 제거하고 `reconstruct` 명령을 다시 실행할 수 있습니다.

---

**주의** `reconstruct` 명령으로 검색할 수 없는 파일에 문제가 있다고 확신하는 경우에만 `store.idx` 파일을 제거해야 합니다.

---

9. 문제가 특정 메일로 한정된 경우 해당 메일 파일을 메시지 저장소 외부의 다른 위치로 복사하고 `mailbox/` 디렉토리에서 `reconstruct -r` 명령을 실행해야 합니다.
10. 폴더가 디스크(`store_root/partition/` 디렉토리)에 존재하지만 데이터베이스(`store_root/mboxlist/` 디렉토리)에는 확실하게 없을 경우 `reconstruct -m` 명령을 실행하여 메시지 저장소 일관성을 확인합니다.

`reconstruct` 명령에 대한 자세한 내용은 [632페이지의 “메일함 및 메일함 데이터베이스 복구”](#)를 참조하십시오.

## 저장소 데몬이 시작되지 않음

다음 오류 메시지와 함께 `stored`가 시작되지 않을 수 있습니다.

```
# msg_svr_base/sbin/start-msg
```

```
msg_svr_base: Starting STORE daemon ...Fatal error: Cannot find group in name
service
```

이 오류 메시지는 `local.servergid`에 구성된 UNIX 그룹을 찾을 수 없다는 것을 나타냅니다. `stored` 및 다른 유틸리티에서는 해당 `gid`가 이 그룹으로 설정되어야 합니다. 경우에 따라 실수로 `local.servergid`에 의해 정의된 그룹이 삭제될 수 있습니다. 이런 경우에는 삭제된 그룹을 만들고 `inetuser`를 그룹에 추가한 다음 `instance_root`와 해당 파일의 소유권을 `inetuser` 및 해당 그룹으로 변경합니다.





## 보안 및 액세스 제어 구성

Messaging Server는 메일을 가로챌 수 없게 하고 침입자가 사용자 또는 관리자로 가장하는 것을 금지하며 특정 사용자에게만 메시징 시스템의 특정 부분에 대한 액세스를 허용할 수 있는 다양하고 유연한 보안 기능을 지원합니다.

Messaging Server 보안 구조는 Sun Java System 서버 전체의 보안 구조 중 일부입니다. 이 구조는 최대한의 상호 운용성과 일관성을 위해 업계 표준 및 공용 프로토콜에 기반을 둡니다. 따라서 Messaging Server 보안 정책을 구현하려면 이 장의 내용뿐만 아니라 여러 다른 문서를 읽어야 합니다. 특히 Messaging Server 보안을 설정하려면 *Sun ONE Server Console 5.2 Server Management Guide*에 설명된 정보가 필요합니다.

이 장은 다음 내용으로 구성되어 있습니다.

- 642페이지의 "서버 보안 정보"
- 643페이지의 "HTTP 보안 정보"
- 644페이지의 "인증 기법 구성"
- 647페이지의 "사용자 비밀번호 로그인"
- 649페이지의 "암호화 및 인증서 기반 인증 구성"
- 661페이지의 "Messaging Server에 대한 관리자 액세스 구성"
- 664페이지의 "POP, IMAP 및 HTTP 서비스에 대한 클라이언트 액세스 구성"
- 675페이지의 "POP before SMTP 사용"
- 679페이지의 "SMTP 서비스에 대한 클라이언트 액세스 구성"

## 서버 보안 정보

서버 보안에는 광범위한 주제가 포함됩니다. 대부분의 기업에서는 허가된 사용자만 서버에 액세스하고, 비밀번호나 아이디의 손상을 방지하며, 사용자가 통신 중에 다른 사람을 나타내지 않도록 하고, 필요 시 비밀리에 통신이 이루어지도록 보장하는 것이 메시징 시스템의 중요한 요구 사항입니다.

서버 통신의 보안이 다양한 방식으로 손상될 수 있기 때문에 보안을 향상시키는 여러 방법이 존재합니다. 이 장에서는 암호화, 인증 및 액세스 제어를 설정하는 방법에 대해 중점적으로 설명합니다. 다음과 같은 Messaging Server의 보안 관련 주제가 이 장에서 다루어 집니다.

- **사용자 아이디 및 비밀번호 로그인:** IMAP, POP, HTTP 또는 SMTP에 로그인하려면 사용자 아이디와 비밀번호를 입력해야 하며 보낸 사람 인증을 메일 수신자에게 전송하려면 SMTP 비밀번호 로그인을 사용해야 합니다.
- **암호화 및 인증:** 통신 및 인증 클라이언트를 암호화하기 위해 TLS 및 SSL 프로토콜을 사용하도록 서버를 설정합니다.
- **관리자 액세스 제어:** 콘솔의 액세스 제어 기능을 사용하여 Messaging Server 및 일부 개별 작업에 대한 액세스를 위임합니다.
- **TCP 클라이언트 액세스 제어:** 필터링 기술을 사용하여 서버의 POP, IMAP, HTTP 및 인증된 SMTP 서비스에 연결할 수 있는 클라이언트를 제어합니다.

Messaging Server와 관련된 모든 보안 및 액세스 문제가 이 장에서 설명되지는 않습니다. 다른 곳에서 다루어지는 보안 주제는 다음과 같습니다.

- **물리적 보안:** 서버 시스템의 보안을 물리적으로 유지하기 위한 준비가 없을 경우 소프트웨어 보안은 무의미할 수 있습니다.
- **메시지 저장소 액세스:** Messaging Server에 대한 메시지 저장소 관리자를 정의할 수 있습니다. 이러한 관리자는 메일함을 확인 및 모니터링하고 메일함에 대한 액세스를 제어할 수 있습니다. 자세한 내용은 18장, "메시지 저장소 관리"를 참조하십시오.
- **최종 사용자 계정 구성:** 최종 사용자 계정 정보는 주로 Delegated Administrator 제품을 사용하여 유지 관리할 수 있습니다(Sun LDAP Schema 1에만 해당). 또한 콘솔 인터페이스를 사용하여 최종 사용자 계정을 관리할 수도 있습니다.
- **원하지 않는 대량 전자 메일 필터링(UBE):** 17장, "메일 필터링 및 액세스 제어"를 참조하십시오.

다양한 보안 주제를 다루는 매우 많은 문서가 존재합니다. 여기에 언급된 주제에 대한 추가 배경 정보와 다른 보안 관련 정보는 <http://docs.sun.com>의 설명서 웹 사이트를 참조하십시오.

## HTTP 보안 정보

Messaging Server는 사용자 아이디/비밀번호 인증, 클라이언트 인증서 인증 및 Access Manager를 지원합니다. 그러나 클라이언트와 서버 간의 네트워크 연결을 프로토콜이 처리하는 방법에서 몇 가지 차이점이 있습니다.

POP, IMAP 또는 SMTP 클라이언트가 Messaging Server에 로그인하면 연결이 설정되고 세션이 만들어집니다. 세션이 끝날 때까지, 즉 로그인에서 로그아웃까지 연결이 지속됩니다. 새 연결을 설정할 때 클라이언트는 서버에 대해 재인증되어야 합니다.

HTTP 클라이언트가 Messaging Server에 로그인할 때 서버는 고유한 세션 아이디를 클라이언트에게 제공합니다. 클라이언트는 이 세션 아이디를 사용하여 세션 도중에 여러 연결을 설정합니다. HTTP 클라이언트는 각 연결에 대해 재인증될 필요가 없습니다. 즉, 세션이 해제되고 새 세션을 설정하려는 경우에만 클라이언트 재인증이 필요합니다. (지정된 기간 동안 HTTP 세션이 유희 상태일 경우 서버가 자동으로 HTTP 세션을 해제하며 클라이언트는 자동으로 로그아웃됩니다. 이 기간의 기본값은 2시간입니다.)

HTTP 세션의 보안을 향상시키기 위해 다음 기술이 사용됩니다.

- 세션 아이디는 특정 IP 주소로 바인드됩니다.
- 각 세션 아이디는 관련된 시간 초과 값을 가집니다. 세션 아이디는 지정된 기간 동안 사용되지 않을 경우 무효화됩니다.
- 서버가 열려 있는 모든 세션 아이디의 데이터베이스를 보유하므로 클라이언트가 아이디를 위조할 수 없습니다.
- 세션 아이디는 URL에 저장되지만 쿠키 파일에는 저장되지 않습니다.

향상된 연결 성능을 위한 구성 매개 변수 지정에 대한 자세한 내용은 5장, "POP, IMAP 및 HTTP 서비스 구성"을 참조하십시오.

Access Manager에 대한 자세한 내용은 141페이지의 6장, "단일 사인 온(SSO) 사용"을 참조하십시오.

## 인증 기법 구성

인증 기법은 클라이언트가 자신의 아이디를 서버에 대해 입증하는 특정 방법입니다. Messaging Server는 SASL(Simple Authentication and Security Layer) 프로토콜에 정의된 인증 방법과 인증서 기반 인증을 지원합니다. SASL 기법은 이 절에 설명되어 있습니다. 인증서 기반 인증에 대한 자세한 내용은 [649페이지의 "암호화 및 인증서 기반 인증 구성"](#)을 참조하십시오.

Messaging Server는 비밀번호 기반 인증을 위한 다음 SASL 인증 방법을 지원합니다.

- **PLAIN** - 이 기법은 사용자의 일반 비밀번호를 네트워크를 통해 전달하므로 도청에 취약합니다.  
SSL을 사용하여 도청 문제를 줄일 수 있다는 것에 주의합니다. 자세한 내용은 [649페이지의 "암호화 및 인증서 기반 인증 구성"](#)을 참조하십시오.
- **DIGEST-MD5** - RFC 2831에 정의된 챌린지/응답 인증 기법입니다. (DIGEST-MD5는 아직 Messaging Multiplexor에서 지원하지 않습니다.)
- **CRAM-MD5** - APOP와 비슷하지만 다른 프로토콜에서 사용하기에도 적합한 챌린지/응답 인증 기법입니다. RFC 2195에 정의되어 있습니다.
- **APOP** - POP3 프로토콜에만 사용할 수 있는 챌린지/응답 인증 기법입니다. RFC 1939에 정의되어 있습니다.
- **LOGIN** - PLAIN과 동일하며 SMTP 인증의 예비 표준 구현과의 호환성을 위해서만 존재합니다. 기본적으로 이 기법은 SMTP에 대해서만 사용 가능하게 됩니다.

챌린지/응답 인증 기법을 사용하면 서버는 요청 문자열을 클라이언트에게 보냅니다. 클라이언트는 사용자의 비밀번호와 해당 챌린지의 해시로 응답합니다. 클라이언트의 응답이 서버의 고유한 해시와 일치할 경우 사용자가 인증됩니다. 해시는 취소할 수 없으므로 사용자의 비밀번호가 네트워크를 통해 보내질 때 공개되지 않습니다.

---

**주** POP, IMAP 및 SMTP 서비스는 모든 SASL 기법을 지원합니다. HTTP 서비스는 일반 텍스트 비밀번호 기법만 지원합니다.

---

[표 19-1](#)은 몇 개의 SALS 및 SASL 관련 configutil 매개 변수를 보여 줍니다. configutil 매개 변수의 최신 전체 목록은 *Sun Java System Messaging Server Administration Reference*를 참조하십시오.

표 19-1 일부 SASL 및 SASL 관련 configutil 매개 변수

| 매개 변수                                       | 설명                                                                                                                                                                                                                                                                                                                                      |
|---------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| sasl.default.ldap.has_plain_passwords       | 디렉토리에 일반 텍스트 비밀번호가 저장되는지 나타내며 APOP, CRAM-MD5 및 DIGEST-MD5를 사용 가능하게 하는 부울입니다.<br>기본값: False                                                                                                                                                                                                                                              |
| sasl.default.transition_criteria            | 더 이상 지원 또는 사용되지 않습니다. sasl.default.auto_transition을 참조하십시오.                                                                                                                                                                                                                                                                             |
| sasl.default.auto_transition                | 부울입니다. 이 매개 변수가 설정되고 사용자가 일반 텍스트 비밀번호를 제공할 경우 비밀번호 저장 형식이 Directory Server에 대한 기본 비밀번호 저장 방법으로 전환됩니다. 일반 텍스트 비밀번호를 APOP, CRAM-MD5 또는 DIGEST-MD5로 마이그레이션하는 데 사용할 수 있습니다.<br>기본값: False                                                                                                                                                   |
| service.imap.allowanonymouslogin            | IMAP에 사용하기 위해 SASL ANONYMOUS 기법을 사용 가능하게 합니다.<br>기본값: False                                                                                                                                                                                                                                                                             |
| service.{imap pop http}.plaintextmimicipher | 이 매개 변수가 > 0이면 보안 계층(SSL 또는 TLS)이 활성화되지 않은 경우 일반 텍스트 비밀번호를 사용할 수 없게 됩니다. 사용자는 로그인하려면 네트워크상에서 비밀번호가 공개되는 것을 방지하는 SSL 또는 TLS를 클라이언트에서 사용 가능하게 해야 합니다. MMP는 동일한 옵션 "RestrictPlainPasswords"를 가집니다.<br>주의: Messaging Server의 5.2 릴리스는 SSL 또는 TLS에 의해 협상된 암호문 강도에 대해 실제로 값을 검사합니다. 이 옵션을 단순화하고 일반적인 사용을 더 잘 반영하기 위해 이 기능이 제거되었습니다.<br>기본값: 0 |
| sasl.default.mech_list                      | 사용 가능하게 할 SASL 기법의 공백으로 구분된 목록입니다. 비어 있지 않을 경우 이 옵션은 sasl.default.ldap.has_plain_passwords 및 service.imap.allowanonymouslogin 옵션을 모두 무시합니다. 이 옵션은 모든 프로토콜(imap, pop, smtp)에 적용됩니다.<br>기본값: False                                                                                                                                        |
| sasl.default.ldap.searchfilter              | 도메인의 inetDomainSearchFilter에 지정되지 않은 경우 사용자를 조회하는 데 사용되는 기본 검색 필터입니다. 구문은 inetDomainSearchFilter(스키마 설명서 참조)와 동일합니다.<br>기본값: (&(uid=%U)(objectclass=inetmailuser))                                                                                                                                                                      |
| sasl.default.ldap.searchfilterdomain        | 기본적으로 인증 시스템은 도메인 조회 규칙에 따라(즉, 필요에 따라) LDAP에서 도메인을 조회한 다음 사용자를 조회합니다. 그러나 이 옵션이 기본값 "1"이 아니라 "0"으로 설정된 경우 도메인 조회는 수행되지 않으며 sasl.default.ldap.searchfilter를 사용한 사용자 검색이 local.ugldapbasedn에 지정된 LDAP 트리에서 직접 수행됩니다. 이것은 레거시 단일 도메인 스키마와의 호환성을 위해 제공되지만 심지어 소규모 회사에서도 여러 도메인에 대한 지원이 필요한 합병이나 사명 변경이 발생할 수 있으므로 새 배포에는 사용하지 않는 것이 좋습니다.   |

## 일반 텍스트 비밀번호에 대한 액세스 구성

CRAM-MD5, DIGEST-MD5 또는 APOP SASL 인증 방법을 사용하려면 사용자의 일반 텍스트 비밀번호에 대한 액세스가 필요합니다. 다음 단계를 수행해야 합니다.

1. 비밀번호를 일반 텍스트로 저장하도록 Directory Server를 구성합니다.
2. Directory Server가 일반 텍스트 비밀번호를 사용한다는 것을 인식하도록 Messaging Server를 구성합니다.

### Directory Server를 구성하여 비밀번호 저장

CRAM-MD5, DIGEST-MD5 또는 APOP 기법을 사용하려면 다음과 같이 Directory Server를 구성하여 비밀번호를 일반 텍스트로 저장하게 해야 합니다.

1. 콘솔에서 구성할 Directory Server를 엽니다.
2. 구성 탭을 누릅니다.
3. 왼쪽 표시 영역에서 데이터를 엽니다.
4. 오른쪽 표시 영역에서 비밀번호를 누릅니다.
5. 비밀번호 암호화 드롭다운 목록에서 "일반 텍스트"를 선택합니다.

---

**주** 이 변경 사항은 앞으로 만들 사용자에게만 영향을 줍니다. 이 변경 이후에 기존 사용자는 자신의 비밀번호를 전환하거나 재설정해야 합니다.

---

### Messaging Server 구성

이제 Messaging Server를 구성하여 Directory Server가 일반 텍스트 비밀번호를 검색할 수 있다는 것을 인식하도록 할 수 있습니다. 이렇게 하면 Messaging Server는 APOP, CRAM-MD5 및 DIGEST-MD5를 안전하게 광고할 수 있습니다.

```
configutil -o sasl.default.ldap.has_plain_passwords -v 1
```

값을 0으로 설정하여 이러한 챌린지/응답 SASL 기법을 사용 불가능하게 할 수 있습니다.

---

**주** 기존 사용자는 비밀번호를 재설정하거나 마이그레이션할 때까지 APOP, CRAM-MD5 또는 DIGEST-MD5를 사용할 수 없습니다(사용자 전환 참조).

---

MMP는 CRAM과 동등한 옵션을 가집니다.

## 사용자 전환

configutil을 사용하여 사용자 전환에 대한 정보를 지정할 수 있습니다. 적절한 항목을 갖고 있지 않은 기법으로 클라이언트가 인증을 시도하거나 사용자 비밀번호가 변경되는 경우를 예로 들 수 있습니다.

```
configutil -o sasl.default.auto_transition -v value
```

value의 경우 다음 중 하나를 지정할 수 있습니다.

- no 또는 0 - 비밀번호를 전환하지 않습니다. 기본값입니다.
- yes 또는 1 - 비밀번호를 전환합니다.

사용자를 성공적으로 전환하려면 사용자 비밀번호 속성에 대한 쓰기 권한을 Messaging Server에 허용하는 ACI를 Directory Server에서 설정해야 합니다. 이렇게 하려면 다음 단계를 수행합니다.

1. 콘솔에서 구성할 Directory Server를 엽니다.
2. 디렉토리 탭을 누릅니다.
3. 사용자/그룹 트리의 기본 접미어를 선택합니다.
4. 객체 메뉴에서 액세스 권한을 선택합니다.
5. "Messaging Server 최종 사용자 관리자 쓰기 액세스 권한"에 대한 ACI를 선택(두 번 누름)합니다.
6. ACI 속성을 누릅니다.
7. userpassword 속성을 기존 속성 목록에 추가합니다.
8. 확인을 누릅니다.

sasl.default.mech\_list를 사용하여 SASL 기법의 목록을 사용 가능하게 할 수 있습니다. 비어 있지 않을 경우 이 옵션은 sasl.default.ldap.has\_plain\_passwords 및 service.imap.allowanonymouslogin 옵션을 모두 무시합니다. 이 옵션은 모든 프로토콜(imap, pop, smtp)에 적용됩니다.

## 사용자 비밀번호 로그인

Messaging Server에 로그인하여 메일을 주고 받으려는 사용자에게 비밀번호 제출을 요구하는 것은 무단 액세스를 방지하는 첫 번째 방법입니다. Messaging Server는 IMAP, POP, HTTP 및 SMTP 서비스에 대한 비밀번호 기반 로그인을 지원합니다.

## IMAP, POP 및 HTTP 비밀번호 로그인

기본적으로 내부 사용자는 Messaging Server에서 메일을 검색하기 위해 비밀번호를 제출해야 합니다. 관리자는 POP, IMAP 및 HTTP 서비스에 대한 비밀번호 로그인을 별개로 사용 가능 또는 불가능하게 합니다. POP IMAP 및 HTTP 서비스의 비밀번호 로그인에 대한 자세한 내용은 [127페이지의 "비밀번호 기반 로그인"](#)을 참조하십시오.

사용자 비밀번호는 사용자의 클라이언트 소프트웨어에서 서버로 일반 텍스트 또는 암호화된 형식으로 전송할 수 있습니다. 클라이언트와 서버가 둘 다 SSL을 사용 가능하게 구성되고 [656페이지의 "SSL 사용 및 암호문 선택"](#)에 설명된 것처럼 필요한 강도의 암호화를 지원할 경우 암호화가 수행됩니다.

사용자 아이디와 비밀번호는 설치 시 LDAP 사용자 디렉토리에 저장됩니다. 최소 길이와 같은 비밀번호 보안 조건은 디렉토리 정책 요구 사항에 의해 결정되며 Messaging Server 관리의 일부가 아닙니다.

인증서 기반 로그인은 비밀번호 기반 로그인의 대안입니다. 이 장에서 SSL의 나머지 내용을 다루면서 인증서 기반 로그인이 설명됩니다. [658페이지의 "인증서 기반 로그인 설정"](#)을 참조하십시오.

첼린지/응답 SASL 기법은 일반 텍스트 비밀번호 로그인의 또 다른 대안입니다.

## SMTP 비밀번호 로그인

기본적으로 사용자는 메일을 보내기 위해 Messaging Server의 SMTP 서비스에 연결할 때 비밀번호를 제출할 필요가 없습니다. 그러나 관리자는 인증된 SMTP를 사용할 수 있도록 SMTP에 대한 비밀번호 로그인을 사용 가능하게 할 수 있습니다.

*인증된 SMTP*는 클라이언트를 서버에 대해 인증할 수 있는 SMTP 프로토콜의 확장입니다. 이 인증에는 메일이 수반됩니다. 인증된 SMTP는 주로 이동 중이거나 홈 ISP를 사용하는 로컬 사용자가 열린 릴레이(다른 사용자가 남용할 수 있는)를 만들지 않고 메일을 전달하도록 허용하기 위해 사용됩니다. 클라이언트는 서버에 대해 인증되도록 "AUTH" 명령을 사용합니다.

SMTP 비밀번호 로그인과 이에 따라 인증된 SMTP를 사용 가능하게 하는 방법은 [351페이지의 "SMTP 인증, SASL 및 TLS"](#)를 참조하십시오.

SSL 암호화를 함께 사용하거나 사용하지 않으면서 인증된 SMTP를 사용할 수 있습니다.



## 암호화 및 인증서 기반 인증 구성

이 절에는 다음과 같은 하위 절이 포함됩니다.

- 651페이지의 "관리 콘솔을 통해 인증서 얻기"
- 656페이지의 "SSL 사용 및 암호문 선택"
- 658페이지의 "인증서 기반 로그인 설정"
- 660페이지의 "SMTP 프로кси를 사용하여 SSL 성능을 최적화하는 방법"

Messaging Server는 클라이언트 및 서버의 암호화된 통신과 인증서 기반 인증을 위해 TLS(Transport Layer Security) 프로토콜(또는 SSL(Secure Sockets Layer) 프로토콜로 알려져 있음)을 사용합니다. Messaging Server는 SSL 버전 3.0 및 3.1을 지원합니다. TLS는 SSL과 완전히 호환되며 필요한 모든 SSL 기능을 포함합니다.

SSL에 대한 배경 정보는 *Introduction to SSL(Managing Servers with iPlanet Console*의 부록으로 제공됨)을 참조하십시오. SSL은 *Introduction to Public-Key Cryptography(Managing Servers with iPlanet Console*의 부록으로 제공됨)에 설명되어 있는 공개 키 암호화의 개념에 기초합니다.

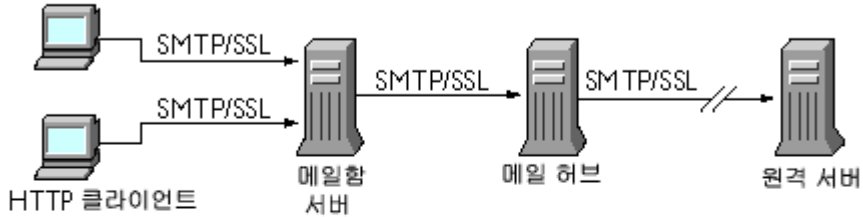
Messaging Server와 클라이언트 간의 메일이나 Messaging Server와 다른 서버 간의 메일 전송이 암호화될 경우 통신에서 도청이 발생할 가능성이 거의 없습니다. 또한 연결하는 클라이언트가 인증될 경우 침입자가 클라이언트를 가장(스푸핑)할 가능성이 거의 없습니다.

SSL은 IMAP4, HTTP, POP3 및 SMTP의 응용 프로그램 계층 아래에 있는 프로토콜 계층의 기능을 수행합니다. SMTP 및 SMTP/SSL은 같은 포트를 사용하고 HTTP 및 HTTP/SSL에는 다른 포트가 필요하며 IMAP 및 IMAP/SSL과 POP 및 POP/SSL은 같은 포트나 다른 포트를 사용할 수 있습니다. 그림 19-1에 나온 것처럼 SSL은 보내는 메일과 받는 메일 모두에 대해 특정 메일 통신 단계에서 작동합니다.

그림 19-1 Messaging Server와의 암호화된 통신

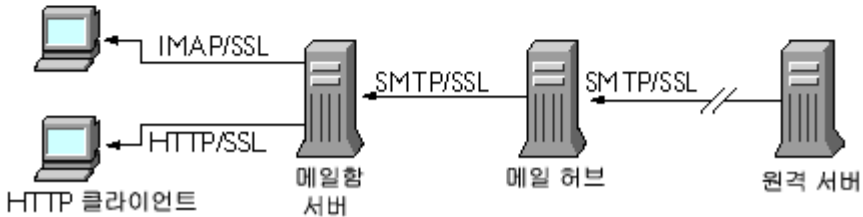
**A. 보내는 메일**

IMAP 클라이언트



**B. 받는 메일**

IMAP 클라이언트



SSL은 홉 간의 암호화를 제공하지만 메일은 각 중간 서버에서 암호화되지 않습니다.

---

**주** 보내는 메일에 대한 암호화를 사용하려면 maytls, musttls 등의 tls 채널 키워드를 포함하도록 채널 정의를 수정해야 합니다. 자세한 내용은 [354 페이지의 "전송 계층 보안"](#) 및 *Messaging Server Reference Manual*을 참조하십시오.

---

SSL 연결을 설정하는 과정에서 발생하는 추가 오버헤드가 서버의 성능에 부담을 줄 수 있다는 것에 주의합니다. 따라서 메시징 설치를 디자인하고 성능을 분석할 경우 서버 용량과 보안 요구 사항 간에 적절히 균형을 맞추는 것이 필요합니다.

---

**주** 모든 Sun Java System 서버가 SSL을 지원하며 콘솔을 통해 SSL을 사용 가능하게 하고 구성하기 위한 인터페이스가 대부분의 서버에서 거의 동일하기 때문에 이 절에 설명된 여러 작업은 *Managing Servers with iPlanet Console*의 SSL 장에 더 자세하게 설명되어 있습니다. 이 장에서는 이러한 작업에 대한 요약 정보만 제공합니다.

---

## 관리 콘솔을 통해 인증서 얻기

SSL을 암호화에 사용하는지 아니면 인증에 사용하는지 여부에 상관 없이 Messaging Server에 대한 서버 인증서를 얻어야 합니다. 인증서는 해당 서버를 클라이언트와 다른 서버에 대해 식별합니다. 관리 콘솔을 통해 인증서를 얻으려면 이 절의 단계를 수행합니다. 명령줄 모드에서 자체 서명된 인증서를 만들려면 [655페이지의 "자체 서명된 인증서 만들기"](#)를 참조하십시오.

### 내부 및 외부 모듈 관리

서버 인증서는 데이터를 암호화 및 해독하는 데 사용되는 숫자인 키 쌍의 소유권과 유효성을 설정합니다. 서버 인증서와 키 쌍은 서버의 신원을 나타내며 서버 내부이거나 외부의 이동식 하드웨어 카드(스마트 카드)가 될 수 있는 인증서 데이터베이스에 저장됩니다.

Sun Java System 서버는 PKCS(Public-Key Cryptography System) #11 API를 따르는 모듈을 사용하여 키 및 인증서 데이터베이스에 액세스합니다. 특정 하드웨어 장치의 PKCS #11 모듈은 일반적으로 해당 제공자로부터 얻을 수 있으며 Messaging Server에 설치한 후에만 Messaging Server에서 해당 장치를 사용할 수 있습니다. 미리 설치된 "Netscape Internal PKCS # 11 Module"은 서버 내부의 인증서 데이터베이스를 사용하는 단일 내부 소프트웨어 토큰을 지원합니다.

인증서 사용을 위해 서버를 설정하는 작업에는 인증서와 해당 키를 위한 데이터베이스를 만들고 PKCS #11 모듈을 설치하는 것이 포함됩니다. 외부 하드웨어 토큰을 사용하지 않을 경우 서버에서 내부 데이터베이스를 만들고 Messaging Server의 일부인 내부 기본 모듈을 사용합니다. 외부 토큰을 사용할 경우 하드웨어 스마트 카드 판독기를 연결하고 해당 PKCS #11 모듈을 설치합니다.

내부 및 외부 PKCS #11 모듈을 모두 콘솔을 통해 관리할 수 있습니다. PKCS #11 모듈을 설치하려면 다음을 수행합니다.

1. 하드웨어 카드 판독기를 Messaging Server 호스트 시스템에 연결하고 드라이버를 설치합니다.
2. 콘솔에서 PKCS #11 관리 인터페이스를 사용하여 설치된 드라이버를 위한 PKCS #11 모듈을 설치합니다.

보다 자세한 지침은 *Managing Servers with iPlanet Console*에서 SSL 장을 참조하십시오.

**하드웨어 암호화 가속기 설치.** 암호화를 위해 SSL을 사용할 경우 하드웨어 암호화 가속기를 설치하여 메일을 암호화 및 해독하는 서버의 성능을 향상시킬 수 있습니다. 일반적으로 암호화 가속기는 서버 시스템에 영구적으로 설치된 하드웨어 보드와 소프트웨어 드라이버로 구성됩니다. Messaging Server는 PKCS #11 API를 따르는 가속기 모듈을 지원합니다. (이러한 모듈은 기본적으로 고유한 키를 저장하지 않으며 이를 위한 내부 데이터베이스를 사용하는 하드웨어 토큰입니다.) 가속기를 설치하려면 우선 하드웨어와 드라이버를 제조업체에서 지정한 대로 설치한 다음 하드웨어 인증서 토큰과 마찬가지로 PKCS #11 모듈을 설치하여 설치를 완료합니다.

## 서버 인증서 요청

콘솔에서 서버를 열고 인증서 설정 마법사를 실행하여 서버 인증서를 요청합니다. 이 마법사는 콘솔 메뉴나 Messaging Server 암호화 탭에서 액세스할 수 있습니다. 이 마법사를 사용하여 다음 작업을 수행합니다.

1. 인증서 요청을 생성합니다.
2. 인증서를 발급한 인증 기관(CA)에 전자 메일로 요청을 보냅니다.

CA로부터 전자 메일 응답이 도착하면 이를 텍스트 파일로 저장하고 인증서 설정 마법사를 사용하여 설치합니다.

보다 자세한 지침은 *Managing Servers with iPlanet Console*에서 SSL 장을 참조하십시오.

## 인증서 설치

설치는 요청 생성과 별개의 프로세스입니다. 인증서 요청에 대한 전자 메일 응답이 CA로부터 도착했으며 이를 텍스트 파일로 저장한 후에는 인증서 설정 마법사를 한 번 더 실행하여 다음과 같이 파일을 인증서로 설치합니다.

1. 이미 얻은 인증서를 설치하고 있다는 것을 지정합니다.
2. 인증서의 텍스트를 필드에 붙여넣습니다(그렇게 하라는 메일이 나타났을 때).

### 3. 인증서 별명을 `server-cert`에서 `Server-Cert`로 변경합니다.

인증서 별명을 변경하지 않으려면 `configutil` 매개 변수 `encryption.rsa.nssslpersonalityssl`을 설정하여 시스템에서 원하는 인증서 별명을 변경할 수 있습니다.

보다 자세한 지침은 *Managing Servers with iPlanet Console*에서 SSL 장을 참조하십시오.

---

**주** 이것은 또한 다음에 설명하는 CA 인증서를 설치할 때 따르는 프로세스입니다. 서버는 CA 인증서를 사용하여 클라이언트가 제공한 인증서를 신뢰할지 여부를 결정합니다.

---

## 신뢰할 수 있는 CA의 인증서 설치

또한 인증서 설정 마법사를 사용하여 인증 기관의 인증서를 설치할 수 있습니다. CA 인증서는 CA 자체의 신원을 검증합니다. 서버는 클라이언트 및 다른 서버를 인증하는 과정에서 이러한 CA 인증서를 사용합니다.

예를 들어, 비밀번호 기반 인증 외에 인증서 기반 클라이언트 인증이 가능하도록 설정한 경우(157페이지의 "인증 기반 로그인 설정" 참조) 클라이언트가 제공할 수 있는 인증서를 발급하는 신뢰할 수 있는 모든 CA의 CA 인증서를 설치해야 합니다. 이러한 CA는 조직 내부에 대한 것이거나 민간 또는 정부 기관이나 다른 회사 등 외부에 대한 것일 수 있습니다. (인증을 위한 CA 인증서 사용에 대한 자세한 내용은 *Managing Servers with iPlanet Console*에서 *Introduction to Public-Key Cryptography*를 참조하십시오.)

`Messaging Server`를 설치하면 여러 상용 CA에 대한 CA 인증서가 기본적으로 포함되어 있습니다. 다른 상용 CA를 추가해야 하거나 회사에서 내부 용도의 고유한 CA를 개발(`Sun Java System Certificate Server` 사용)하는 중이면 추가 CA 인증서를 얻어 설치해야 합니다.

---

**주** `Messaging Server`에서 자동으로 제공되는 CA 인증서는 처음에 클라이언트 인증서에 대해 신뢰할 수 있는 것으로 표시되지 않습니다. 따라서 이러한 CA에 의해 발급된 클라이언트 인증서를 신뢰하려면 트러스트 설정을 편집해야 합니다. 자세한 지침은 153페이지의 "인증 및 신뢰할 수 있는 CA 관리"를 참조하십시오.

---

새 CA 인증서를 요청하여 설치하려면 다음을 수행합니다.

1. 인증 기관에 문의하여(대부분의 웹 또는 전자 메일을 통해) 해당 CA 인증서를 다운로드합니다.
2. 받은 인증서의 텍스트를 텍스트 파일로 저장합니다.

3. 앞의 절에 설명된 대로 인증서 설정 마법사를 사용하여 인증서를 설치합니다.

보다 자세한 지침은 *Managing Servers with iPlanet Console*에서 SSL 장을 참조하십시오.

### 인증서 및 신뢰할 수 있는 CA 관리

서버는 신뢰할 수 있는 CA의 여러 인증서를 클라이언트 인증에 사용할 수 있습니다.

콘솔에서 서버를 열고 콘솔 메뉴에서 인증서 관리 명령을 선택하여 **Messaging Server**에 설치된 모든 인증서를 확인하거나, 해당 트러스트 설정을 편집하거나, 인증서 자체를 삭제할 수 있습니다. 자세한 지침은 *Managing Servers with iPlanet Console*에서 SSL 장을 참조하십시오.

### 비밀번호 파일 만들기

모든 Sun Java System 서버에서 인증서 설정 마법사를 사용하여 인증서를 요청하면 마법사는 내부 모듈의 데이터베이스나 스마트 카드의 외부 데이터베이스에 저장되는 키 쌍을 만듭니다. 그런 다음 이 마법사는 개인 키를 암호화하는 데 사용되는 비밀번호를 묻는 메시지를 표시합니다. 나중에 이와 동일한 비밀번호를 통해서만 키를 해독할 수 있습니다. 이 마법사는 비밀번호를 보유하거나 임의의 위치에 저장하지 않습니다.

SSL이 사용 가능하게 되는 대부분의 Sun Java System 서버에서는 키 쌍을 해독하는 데 필요한 비밀번호를 제공하라는 메시지가 시작 시에 관리자에게 표시됩니다. 그러나 **Messaging Server**에서는 비밀번호를 여러 번 입력(최소한 세 개의 서버 프로세스에 필요함)하는 불편함을 없애고 무인 서버의 다시 시작을 용이하게 만들기 위해 비밀번호를 비밀번호 파일에서 읽습니다.

비밀번호 파일의 이름은 `sslpassword.conf`이며 `msg_svr_base/config/` 디렉토리에 위치합니다. 이 파일의 항목은 다음 형식을 갖는 개별 행입니다.

```
moduleName:password
```

여기에서 `moduleName`은 사용할 내부 또는 외부 PKCS #11 모듈의 이름이며 `password`는 모듈의 키 쌍을 해독하는 비밀번호입니다. 비밀번호는 일반(암호화되지 않은) 텍스트로 저장됩니다.

**Messaging Server**는 내부 모듈 및 기본 비밀번호를 위한 다음과 같은 단일 항목을 가지는 기본 버전의 비밀번호 파일을 제공합니다.

```
Internal (Software) Token:netscape!
```

내부 인증서를 설치할 때 기본값이 아닌 비밀번호를 지정할 경우 비밀번호 파일의 위 행을 편집하여 지정된 비밀번호를 반영해야 합니다. 외부 모듈을 설치할 경우 이에 대해 지정한 모듈 이름과 비밀번호를 포함하는 새 행을 파일에 추가해야 합니다.

---

**주의** 서버 시작 시에 모듈 비밀번호를 묻는 메시지가 관리자에게 표시되지 않으므로 서버에 대한 관리자 액세스 제어와 서버 호스트 시스템 및 해당 백업의 물리적 보안을 적절하게 하는 것이 특히 중요합니다.

---

## 자체 서명된 인증서 만들기

명령줄 모드에서 자체 서명된 인증서를 만들려면 이 절의 지침을 따릅니다. 인증서 마법사를 사용하여 인증서를 만들려면 [651페이지의 "관리 콘솔을 통해 인증서 얻기"](#)를 참조하십시오.

1. 슈퍼유저로 로그인하거나 슈퍼유저(root)가 됩니다.
2. `/opt/SUNWmsgsr/config/sslpassword`에서 `certutil`에 대한 인증서 데이터베이스 비밀번호를 지정합니다. 예를 들면 다음과 같습니다.
 

```
# echo "password" > /opt/SUNWmsgsr/config/sslpassword
```

 여기서 `password`는 해당 비밀번호입니다.
3. `sbin` 디렉토리로 이동하여 인증서 데이터베이스(`cert8.db`) 및 키 데이터베이스(`key3.db`)를 생성합니다. 예를 들면 다음과 같습니다.
 

```
# cd /opt/SUNWmsg/sbin
# ./certutil -N -d /opt/SUNWmsgsr/config -f /opt/SUNWmsgsr/config/sslpassword
```
4. 자동 서명된 기본 루트 인증 기관 인증서를 생성합니다. 예를 들면 다음과 같습니다.

```
# ./certutil -S -n SampleRootCA -x -t "CTu,CTu,CTu"
-s "CN=My Sample Root CA, O=sesta.com" -m 25000
-o /opt/SUNWmsgsr/config/SampleRootCA.crt
-d /opt/SUNWmsgsr/config
-f /opt/SUNWmsgsr/config/sslpassword -z /etc/passwd
```

5. 호스트에 대한 인증서를 생성합니다. 예를 들면 다음과 같습니다.

```

./certutil -S -n Server-Cert -c SampleRootCA -t "u,u,u"
-s "CN=hostname.sesta.com, o=sesta.com" -m 25001
-o /opt/SUNWmsgsr/config/SampleSSLServer.crt
-d /opt/SUNWmsgsr/config -f /opt/SUNWmsgsr/config/sslpassword
-z /etc/passwd
    
```

여기서 *hostname.sesta.com*은 서버 호스트 이름입니다.

6. 인증서의 유효성을 검사합니다. 예를 들면 다음과 같습니다.

```

# ./certutil -V -u V -n SampleRootCA -d /opt/SUNWmsgsr/config
# ./certutil -V -u V -n Server-Cert -d /opt/SUNWmsgsr/config
    
```

7. 인증서를 나열합니다. 예를 들면 다음과 같습니다.

```

# ./certutil -L -d /opt/SUNWmsgsr/config
# ./certutil -L -n Server-Cert -d /opt/SUNWmsgsr/config
    
```

8. modutil을 사용하여 사용 가능한 보안 모듈(secmod.db)을 나열합니다. 예를 들면 다음과 같습니다.

```

# ./modutil -list -dbdir /opt/SUNWmsgsr/config
    
```

9. 예에 나온 것처럼 인증서 데이터베이스 파일의 소유자를 메일 서버 사용자 및 그룹으로 변경합니다.

```

chown mail:mailserv /opt/SUNWmsgsr/config/cert8.db
chown mail:mailserv /opt/SUNWmsgsr/config/key3.db
    
```

10. 메시징 서비스를 다시 시작하여 SSL을 활성화합니다.

**주** 이전에는 인증서와 키 파일이 항상 Messaging Server 구성 디렉토리에 있었습니다. 이제는 이러한 파일의 위치를 *local.ssldbpath*(인증서 및 키 파일의 위치 지정) 및 *local.ssldbprefix*(인증서 및 키 파일의 접두어 지정)를 사용하여 지정하는 일이 가능합니다.

## SSL 사용 및 암호문 선택

콘솔을 사용하여 SSL을 사용 가능하게 하고 Messaging Server가 클라이언트와의 암호화된 통신에 사용할 수 있는 암호화 암호문 집합을 선택할 수 있습니다.



## 암호문 정보

암호문은 암호화 프로세스에서 데이터를 암호화 및 해독하는 데 사용되는 알고리즘입니다. 일부 암호문은 다른 암호문보다 강력한데 이는 이러한 암호문으로 스크램블된 메일을 권한 없는 사용자가 푸는 것이 더 어렵다는 것을 의미합니다.

암호문은 키(긴 번호)를 데이터에 적용하는 방법으로 데이터에서 작동합니다. 일반적으로 암호문이 암호화 도중에 사용하는 키가 더 길수록 적절한 암호화 키 없이 데이터를 해독하는 것이 어려워집니다.

클라이언트는 Messaging Server와의 SSL 연결을 시작할 때 암호화에 사용할 선호되는 암호문과 키 길이를 서버에 알려줍니다. 모든 암호화된 통신에서 클라이언트와 서버는 동일한 암호문을 사용해야 합니다. 일반적으로 다양한 암호문 및 키 조합이 사용되기 때문에 서버는 암호화를 유연하게 지원해야 합니다. Messaging Server는 암호문 및 키 길이 조합을 최대 6개까지 지원할 수 있습니다.

표 6-1에는 SSL 3.0과 함께 사용하는 Messaging Server에서 지원하는 암호문을 나열합니다. 이 표에 요약된 정보의 자세한 내용은 *Managing Servers with iPlanet Console의 Introduction to SSL* 절에서 확인할 수 있습니다.

**표 19-2** Messaging Server의 SSL 암호문

| 암호문                                    | 설명                                                      |
|----------------------------------------|---------------------------------------------------------|
| 128비트 암호화 및 MD5 메일 인증을 사용하는 RC4        | 가장 빠른 암호화 암호문(RSA에 의한)이며 강도가 매우 높은 암호문 및 암호화 키의 조합입니다.  |
| 168비트 암호화 및 SHA 메일 인증을 사용하는 Triple DES | 더 느린 암호화 암호문(미국 정보 표준)이지만 강도가 가장 높은 암호문 및 암호화 키의 조합입니다. |
| 56비트 암호화 및 SHA 메일 인증을 사용하는 DES         | 더 느린 암호화 암호문(미국 정보 표준)이며 강도가 보통인 암호문 및 암호화 키의 조합입니다.    |
| 40비트 암호화 및 MD5 메일 인증을 사용하는 RC4         | 가장 빠른 암호화 암호문(RSA에 의한)이며 강도가 낮은 암호문 및 암호화 키의 조합입니다.     |
| 40비트 암호화 및 MD5 메일 인증을 사용하는 RC2         | 더 느린 암호화 암호문(RSA에 의한)이며 강도가 낮은 암호문 및 암호화 키의 조합입니다.      |
| 암호화 없음, MD5 메일 인증만 사용                  | 암호화가 없으며 메일 다이제스트만 인증에 사용됩니다.                           |

특정 암호문을 사용하지 않을 중요한 이유가 없을 경우 모든 암호문을 지원해야 합니다. 그러나 일부 국가에서는 수출법에 따라 특정 암호화 암호문의 사용이 제한된다는 것에 주의합니다. 또한 미국 수출 제한법이 완화되기 전에 만들어진 일부 클라이언트 소프트웨어는 더 높은 강도의 암호화를 사용할 수 없습니다. 40비트 암호문이 우발적인 도청을 방지할 수 있지만 보안되지는 않으므로 적극적인 공격을 차단하지 않는다는 것에 주의합니다.

SSL을 사용 가능하게 하고 암호화 암호문을 선택하려면 다음 명령줄 단계를 따릅니다.

SSL을 사용 또는 사용하지 않으려면 다음을 수행합니다.

```
configutil -o nssserversecurity -v [ on | off ]
```

RSA 암호문을 사용 또는 사용하지 않으려면 다음을 수행합니다.

```
configutil -o encryption.rsa.nssslactivation -v [ on | off ]
```

토큰을 지정하려면 다음을 수행합니다.

```
configutil -o encryption.rsa.nsssltoken -v tokename
```

인증서를 지정하려면 다음을 수행합니다.

```
configutil -o encryption.rsa.nssslpersonalityssl -v certname
```

RSA 암호문을 사용 가능하게 할 경우 또한 토큰과 인증서를 지정해야 한다는 것에 주의합니다.

암호문 기본 설정을 선택하려면 다음을 수행합니다.

```
configutil -o encryption.nsssl3ciphers -v cipherlist
```

여기에서 *cipherlist*는 쉼표로 구분된 암호문 목록입니다.

---

**주** 보내는 메일에 대해 SSL 암호화를 사용하려면 채널 정의를 수정하여 `maytls`, `musttls` 등의 `tls` 채널 키워드를 포함해야 합니다. 자세한 내용은 *354 페이지의 "전송 계층 보안"* 및 *Messaging Server Reference Manual*을 참조하십시오.

---

## 인증서 기반 로그인 설정

비밀번호 기반 인증 외에도 Sun Java System 서버는 디지털 인증서 검사를 통한 사용자 인증을 지원합니다. 인증서 기반 인증에서 클라이언트는 서버와의 SSL 세션을 설정하고 사용자의 인증서를 서버로 제출합니다. 그런 다음 서버는 제출된 인증서가 진짜인지 여부를 평가합니다. 인증서가 검증될 경우 사용자는 인증된 것으로 간주됩니다.

인증서 기반 로그인을 사용하도록 Messaging Server를 설정하려면 다음을 수행합니다.

1. 서버의 서버 인증서를 얻습니다. 자세한 내용은 [651페이지](#)의 "[관리 콘솔을 통해 인증서 얻기](#)"를 참조하십시오.
2. 인증서 설정 마법사를 실행하여 서버가 인증할 사용자에게 인증서를 발급하는 신뢰할 수 있는 모든 인증 기관의 인증서를 설치합니다. 자세한 내용은 [653페이지](#)의 "[신뢰할 수 있는 CA의 인증서 설치](#)"를 참조하십시오.

서버의 데이터베이스에 최소한 하나 이상의 신뢰할 수 있는 CA가 있을 경우 서버는 각 연결 클라이언트로부터 클라이언트 인증서를 요청한다는 것에 주의합니다.

3. SSL을 설정합니다. 자세한 내용은 [656페이지](#)의 "[SSL 사용 및 암호문 선택](#)"을 참조하십시오.
4. (선택 사항) 제출된 인증서의 정보에 기초하여 서버가 LDAP 사용자 디렉토리를 적절하게 검색하도록 서버의 certmap.conf 파일을 편집합니다.

사용자의 인증서에 있는 전자 메일 주소가 사용자의 디렉토리 항목에 있는 전자 메일 주소와 일치하며 검색을 최적화하거나 사용자 항목의 인증서에 대해 제출된 인증서를 검증할 필요가 없을 경우에는 certmap.conf 파일을 편집할 필요가 없습니다.

certmap.conf의 형식과 변경할 수 있는 사항에 대한 자세한 내용은 *Managing Servers with iPlanet Console*에서 SSL 장을 참조하십시오.

이러한 단계를 수행하고 나면 사용자가 IMAP 또는 HTTP에 로그인할 수 있도록 클라이언트가 SSL 세션을 설정할 때 Messaging Server는 클라이언트로부터 사용자의 인증서를 요청합니다. 클라이언트에 의해 제출된 인증서가 서버에서 신뢰할 수 있는 것으로 설정한 CA가 발급했으며 인증서의 아이디가 사용자 디렉토리의 항목과 일치할 경우 사용자가 인증되며 액세스가 허가됩니다(해당 사용자를 제어하는 액세스 제어 규칙에 따라).

인증서 기반 로그인을 사용 가능하게 하기 위해 비밀번호 기반 로그인을 허용하지 않을 필요는 없습니다. 비밀번호 기반 로그인이 허용되는 기본 상태에서 이 절에 설명된 작업을 수행할 경우 비밀번호 기반 및 인증서 기반 로그인이 모두 지원됩니다. 이 경우 클라이언트가 SSL 세션을 설정하고 인증서를 제공할 경우 인증서 기반 로그인이 사용됩니다. 클라이언트가 SSL을 사용하지 않거나 인증서를 제공하지 않을 경우 서버는 비밀번호를 요청합니다.

## SMTP 프록시를 사용하여 SSL 성능을 최적화하는 방법

SMTP 프록시는 SMTP 프로토콜에 추가 대기 시간을 야기하므로 대부분의 사이트는 SMTP 프록시를 사용해서는 안 됩니다. 그러나 SMTP 연결을 보호하기 위해 SSL에 많이 의존하는 대규모 사이트는 SSL 및 프록시 외에는 일체 수행하지 않는 서버에서 모든 프로토콜에 대해 모든 SSL 작업을 수행하여 SSL 가속기 하드웨어에 대한 투자를 극대화할길 원할 수 있습니다. SMTP 프록시를 사용하면 메일 대기열을 별개의 MTA 시스템에 두면서 SSL을 프런트엔드 프록시 서버에서 처리할 수 있습니다. 이러한 방법으로 각 작업에 대해 최적화된 하드웨어를 별도로 구성 및 구입할 수 있습니다.

SMTP 프록시를 설치하는 방법에 대한 지침은 [675페이지의 "SMTP 프록시 설치"](#)를 참조하십시오.

## 네트워크 보안 서비스 도구

네트워크 보안 서비스는 개방형 표준을 기반으로 하는 인터넷 보안 응용 프로그램을 구현 및 배포하는 데 사용되는 오픈 소스 라이브러리 및 도구 집합입니다. 이러한 보안 도구는 진단을 수행하고 인증서, 키 및 암호화 모듈을 관리하며 SSL 및 TLS 기반 응용 프로그램을 디버깅하는 데 도움이 됩니다. 이러한 도구는 `/usr/sfw/bin`에 있습니다.

### 인증서 및 키 관리

이 절에 설명된 도구는 암호화와 식별에 사용되는 키와 인증서를 저장, 검색 및 보호합니다.

#### certutil

인증서 데이터베이스 도구인 certutil은 cert8.db 및 key3.db 데이터베이스 파일을 작성 및 수정할 수 있는 명령줄 유틸리티입니다. 키와 인증서 관리 프로세스는 일반적으로 키 데이터베이스에서 키를 만든 다음 인증서 데이터베이스에서 인증서를 생성 및 관리합니다. certutil에 대한 자세한 내용은 다음 URL을 참조하십시오.

<http://www.mozilla.org/projects/security/pki/nss/tools/certutil.html>

## cmsutil

cmsutil 명령줄 유틸리티는 S/MIME 툴킷을 사용하여 CMS(Cryptographic Message Syntax) 메일에 대한 암호화 및 해독과 같은 기본 작업을 수행합니다. 이 유틸리티는 메일 암호화, 해독, 서명 등의 기본 인증서 관리 작업을 수행합니다. cmsutil에 대한 자세한 내용은 다음 URL을 참조하십시오.

<http://www.mozilla.org/projects/security/pki/nss/tools/cmsutil.html>

## modutil

보안 모듈 데이터베이스 도구인 modutil은 PKCS #11 모듈(secmod.db 파일)의 데이터베이스를 관리하기 위한 명령줄 유틸리티입니다. 이 도구를 사용하면 PKCS #11 모듈 추가 및 삭제, 암호 변경, 기본값 설정, 모듈 내용 나열, 슬롯 활성화 또는 비활성화, FIPS-140-1 확인 활성화 또는 비활성화, 암호화 작업을 위한 기본 공급자 할당 등을 수행할 수 있습니다. modutil에 대한 자세한 내용은 다음 URL을 참조하십시오.

<http://www.mozilla.org/projects/security/pki/nss/tools/modutil.html>

## pk12util

pk12util 명령줄 유틸리티는 PKCS #12 표준에 의해 정의된 키와 인증서를 해당 데이터베이스 및 파일 형식으로 가져오거나 내보냅니다. pk12util에 대한 자세한 내용은 다음 URL을 참조하십시오.

<http://www.mozilla.org/projects/security/pki/nss/tools/pk12util.html>

## ssltap

SSL 디버깅 도구인 ssltap은 SSL 인식 명령줄 프록시입니다. 이 도구는 SSL 서버에 대한 요청을 프록시하고 클라이언트 및 서버 간에 교환되는 메일의 내용을 표시할 수 있습니다. 이 도구는 TCP 연결을 감시하여 전송되는 데이터를 표시합니다. 연결이 SSL인 경우에는 해석된 SSL 레코드와 핸드셰이킹이 데이터 표시에 포함됩니다. 자세한 내용은 다음 URL을 참조하십시오.

<http://www.mozilla.org/projects/security/pki/nss/tools/ssltap.html>

# Messaging Server에 대한 관리자 액세스 구성

이 절의 내용은 주로 Sun Java System LDAP Schema v. 1과 관련됩니다. 이 절은 다음과 같은 하위 절로 구성되어 있습니다.

- 662페이지의 "위임된 관리 계층"
- 663페이지의 "서버 전체에 대한 액세스 제공"
- 663페이지의 "특정 작업에 대한 액세스 제한"

이 절에서는 Messaging Server에 대한 액세스 권한을 서버 관리자가 어떻게 얻을 수 있는지 제어하는 방법에 대해 설명합니다. 주어진 Messaging Server와 특정 Messaging Server 작업에 대한 관리 액세스는 위임된 서버 관리의 컨텍스트 내에서 발생합니다.

*위임된 서버 관리*는 대부분의 Sun Java System 서버가 갖고 있는 기능으로서 특정 관리자가 개별 서버 또는 서버 기능에 대한 선택적 액세스를 다른 관리자에게 제공하는 기능을 말합니다. 이 장에서는 위임된 서버 작업을 간단하게 요약하여 설명합니다. 자세한 내용은 *Managing Servers with iPlanet Console*에서 서버 관리 위임에 대한 장을 참조하십시오.

## 위임된 관리 계층

네트워크에 Sun Java System 서버를 처음 설치하면 설치 프로그램은 LDAP 사용자 디렉토리에 구성 관리자 그룹이라는 그룹을 자동으로 만듭니다. 기본적으로 구성 관리자 그룹의 구성원은 네트워크의 모든 호스트와 서버에 대한 무제한적인 액세스 권한을 가집니다.

구성 관리자 그룹은 Messaging Server에 대한 위임된 관리를 구현(Sun Java System Sun ONE LDAP Schema v. 1이 사용될 경우)하기 위해 작성할 수 있는 다음과 같은 액세스 계층의 최상위에 위치합니다.

1. **구성 관리자.** Sun Java System 서버의 네트워크에 대한 "수퍼유저"입니다. 모든 자원에 대한 전체 액세스 권한을 가집니다.
2. **서버 관리자.** 도메인 관리자는 각 유형의 서버를 관리하기 위해 그룹을 만들 수 있습니다. 예를 들어, 관리 도메인이나 전체 네트워크에서 모든 Messaging Server를 관리하기 위해 메시징 관리자 그룹을 만들 수 있습니다. 이러한 그룹의 구성원은 다른 서버는 제외하고 해당 관리 도메인의 모든 Messaging Server에 액세스할 수 있습니다.
3. **작업 관리자.** 마지막으로 위 관리자는 모두 단일 Messaging Server 또는 Messaging Server 집합에 대한 제한된 액세스 권한을 가진 그룹을 만들거나 개별 사용자를 지정할 수 있습니다. 이러한 작업 관리자는 서버를 시작 또는 중지하거나 특정 서비스의 로그에 액세스하는 등의 제한된 특정 서버 작업만 수행할 수 있습니다.

콘솔은 관리자가 다음 작업을 수행할 수 있는 편리한 인터페이스를 제공합니다.

- "서버 전체에 대한 액세스 제공"(다음)에 설명된 대로 특정 Messaging Server에 대한 액세스를 그룹이나 개인에게 허가합니다.
- 663페이지의 "특정 작업에 대한 액세스 제한"에 설명된 대로 특정 Messaging Server의 특정 작업에 대한 액세스를 제한합니다.

## 서버 전체에 대한 액세스 제공

특정 Messaging Server 인스턴스에 대한 액세스 권한을 사용자나 그룹에 제공하려면 다음을 수행합니다.

1. 액세스를 제공할 Messaging Server에 액세스할 수 있는 관리자로서 콘솔에 로그인합니다.
2. 콘솔 창에서 해당 서버를 선택합니다.  
콘솔 메뉴에서 객체를 선택한 다음 액세스 권한 설정을 선택합니다.
3. 서버에 액세스할 수 있는 사용자 및 그룹 목록을 추가하거나 편집합니다.

보다 자세한 지침은 *Managing Servers with iPlanet Console*에서 서버 관리 위임에 대한 장을 참조하십시오.

특정 Messaging Server에 액세스할 수 있는 개인 및 그룹 목록을 설정한 후에는 다음에 설명된 것처럼 ACI를 사용하여 특정 서버 작업을 해당 목록의 특정 개인 또는 그룹에 위임할 수 있습니다.

## 특정 작업에 대한 액세스 제한

관리자는 일반적으로 하나 이상의 관리 작업을 수행하기 위해 서버에 연결합니다. 일반 관리 작업은 콘솔에서 Messaging Server 작업 양식에 나열됩니다.

기본적으로 특정 Messaging Server에 대한 액세스는 모든 해당 작업에 대한 액세스를 의미합니다. 그러나 작업 양식의 각 작업은 추가된 액세스 제어 명령(ACI) 집합을 가질 수 있습니다. 서버는 작업에 대한 액세스를 연결된 사용자(서버 전체에 대한 액세스 권한을 이미 갖고 있는 사용자)에게 제공하기 전에 이러한 ACI를 참조합니다. 실제로 서버는 사용자가 권한을 갖고 있는 작업만 작업 양식에 표시합니다.

Messaging Server에 액세스할 수 있는 경우 임의의 작업(즉, 액세스할 수 있는 작업)에 대한 ACI를 작성 및 편집함으로써 다른 사용자나 그룹이 가질 수 있는 작업 액세스 권한을 제한할 수 있습니다.

연결된 사용자나 그룹이 가질 수 있는 작업 액세스 권한을 제한하려면 다음을 수행합니다.

1. 제한된 액세스를 제공할 Messaging Server에 액세스할 수 있는 관리자로서 콘솔에 로그인합니다.
2. 서버를 열고 작업 텍스트를 눌러 서버의 작업 양식에서 작업을 선택합니다.
3. 편집 메뉴에서 액세스 권한 설정을 선택하고 액세스 규칙 목록을 추가 또는 편집하여 사용자나 그룹에 원하는 종류의 액세스를 제공합니다.
4. 다른 작업에 대해 적절하게 이 과정을 반복합니다.

보다 자세한 지침은 *Managing Servers with iPlanet Console*에서 서버 관리 위임에 대한 장을 참조하십시오.

ACI와 ACI 작성 방법에 대한 자세한 내용은 *Managing Servers with iPlanet Console*에서 서버 관리 위임에 대한 장에 자세히 설명되어 있습니다.

## POP, IMAP 및 HTTP 서비스에 대한 클라이언트 액세스 구성

이 절에는 다음과 같은 하위 절이 포함됩니다.

- 665페이지의 "클라이언트 액세스 필터의 작동 방법"
- 666페이지의 "필터 문"
- 671페이지의 "필터 예"
- 672페이지의 "서비스에 대한 액세스 필터 만들기"
- 673페이지의 "HTTP 프록시 인증에 대한 액세스 필터 만들기"
- 665페이지의 "클라이언트 액세스 필터의 작동 방법"

Messaging Server는 서버에 액세스할 수 있는 클라이언트를 광범위하고 세부적으로 제어할 수 있도록 IMAP, POP 및 HTTP 서비스에 대한 정교한 서비스별 액세스 제어를 지원합니다.



대기업이나 인터넷 서비스 공급자에 대한 메시징 서비스를 관리하는 중이면 이러한 기능은 시스템에서 스팸 발송자 및 DNS 스푸퍼를 차단하고 네트워크의 일반 보안을 향상시키는 데 도움을 줄 수 있습니다. 특히 원하지 않은 대량 전자 메일을 제어하는 방법은 [17장, "메일 필터링 및 액세스 제어"](#)를 참조하십시오.

---

**주** IP 주소별로 액세스를 제어하는 것이 기업의 중요한 문제가 아닐 경우 이 절에 설명된 필터를 만들 필요가 없습니다. 단지 최소한의 액세스 제어만 필요한 경우에는 [671페이지의 "대부분 허용"](#) 절에서 이를 설정하는 방법에 대한 지침을 참조하십시오.

---

## 클라이언트 액세스 필터의 작동 방법

Messaging Server 액세스 제어 기능은 서비스되는 TCP 데몬과 동일한 포트에서 수신하는 프로그램입니다. 즉, 이 기능은 액세스 필터를 사용하여 클라이언트 신원을 확인하며 클라이언트가 필터링 프로세스를 통과할 경우 데몬에 대한 액세스 권한을 클라이언트에게 제공합니다.

Messaging Server TCP 클라이언트 액세스 제어 시스템은 필요한 경우 처리 과정의 일부로서 소켓 종점 주소에 대한 다음 분석을 수행합니다.

- 두 종점 모두에 대한 역방향 DNS 조회(이름 기반 액세스 제어를 수행하기 위해)
- 두 종점 모두에 대한 정방향 DNS 조회(DNS 스푸핑을 감지하기 위해)
- Identd 콜백(클라이언트 종점의 사용자가 클라이언트 호스트에 알려져 있는 검사하기 위해)

시스템은 *필터*라고 부르는 액세스 제어문에 대해 이 정보를 비교하여 액세스를 허가 또는 거부할지 여부를 결정합니다. 각 서비스에 대해 별도의 허용 필터 및 거부 필터 집합이 액세스를 제어합니다. 허용 필터는 액세스를 명시적으로 허가하며 거부 필터는 액세스를 명시적으로 금지합니다.

클라이언트가 서비스에 대한 액세스를 요청하면 액세스 제어 시스템은 다음 조건을 사용하여 각 서비스의 필터에 대해 클라이언트의 주소 또는 이름 정보를 순서대로 비교합니다.

- 일치하는 첫 번째 항목에서 검색이 중지됩니다. 허용 필터는 거부 필터 이전에 처리되므로 허용 필터가 우선 순위를 가집니다.
- 클라이언트 정보가 해당 서비스의 허용 필터와 일치할 경우 액세스가 허가됩니다.
- 클라이언트 정보가 해당 서비스의 거부 필터와 일치할 경우 액세스가 거부됩니다.

- 허용 또는 거부 필터와 일치하는 항목이 없을 경우 액세스가 허가됩니다. 단, 허용 필터만 있고 거부 필터가 없을 경우 일치하는 항목이 없으면 액세스가 거부됩니다.

여기에서 설명된 필터 구문은 간단한 방식으로 여러 다른 종류의 액세스 제어 정책을 구현할 수 있을 정도로 충분히 유연합니다. 거의 배타적인 허용 또는 거부를 사용하여 대부분의 정책을 구현할 수 있지만 허용 필터와 거부 필터를 둘 다 임의로 조합하여 사용할 수 있습니다.

다음 절에서는 필터 구문을 자세하게 설명하고 사용 예를 제공합니다. [672페이지의 "서비스에 대한 액세스 필터 만들기"](#) 절에서는 액세스 필터를 만들기 위한 절차에 대해 설명합니다.

## 필터 문

필터 문은 서비스 정보와 클라이언트 정보를 모두 포함합니다. 서비스 정보는 서비스 이름, 호스트 이름 및 호스트 주소를 포함할 수 있습니다. 클라이언트 정보는 호스트 이름, 호스트 주소 및 아이디를 포함할 수 있습니다. 서버 및 클라이언트 정보는 둘 다 와일드카드 이름이나 패턴을 포함할 수 있습니다.

가장 간단한 형식의 필터는 다음과 같습니다.

```
service: hostSpec
```

여기에서 *service*는 서비스 이름(예: smtp, pop, imap 또는 http)이고 *hostSpec*은 호스트 이름, IP 주소 또는 액세스를 요청하는 클라이언트는 나타내는 와일드카드 이름 또는 패턴입니다. 필터가 처리될 때 액세스를 요구하는 클라이언트가 *client*와 일치할 경우 *service*에 지정된 서비스에 대한 액세스가 해당 필터 유형에 따라 허용되거나 거부됩니다. 다음은 몇 가지 예입니다.

```
imap: roberts.newyork.siroe.com
```

```
pop: ALL
```

```
http: ALL
```

이러한 필터가 허용 필터일 경우 첫 번째 필터는 IMAP 서비스에 대한 액세스를 roberts.newyork.siroe.com 호스트에 허가하고 두 번째 및 세 번째 필터는 각각 POP 및 HTTP 서비스에 대한 액세스를 모든 클라이언트에게 허가합니다. 이러한 필터가 거부 필터일 경우 이러한 클라이언트는 서비스에 대한 액세스가 거부됩니다. ALL과 같은 와일드카드 이름에 대한 자세한 내용은 [668페이지의 "와일드카드 이름"](#)을 참조하십시오.

필터가 더 일반적인 형식을 가질 경우 필터의 서버 또는 클라이언트 정보는 다음과 같이 다소 복잡할 수 있습니다.

*serviceSpec*: *clientSpec*

여기에서 *serviceSpec*은 *service* 또는 *service@hostSpec*이 될 수 있고 *clientSpec*은 *hostSpec* 또는 *user@hostSpec*이 될 수 있습니다. *user*는 액세스를 요구하는 클라이언트 호스트와 연관된 사용자 아이디 또는 와일드카드 이름입니다. 다음 두 개의 예를 가령해 봅니다.

pop@mailServer1.siroe.com: ALL

imap: srashad@xyz.europe.siroe.com

여기에서 이러한 필터가 거부 필터일 경우 첫 번째 필터는 mailServer1.siroe.com 호스트에서 SMTP 서비스에 대한 액세스를 모든 클라이언트에 대해 거부합니다. 두 번째 필터는 xyz.europe.siroe.com 호스트에서 사용자 srashad의 IMAP 서비스에 대한 액세스를 거부합니다. 이러한 확장된 서버 및 클라이언트 지정은 사용하는 시기에 대한 자세한 내용은 [669페이지의 "서버 호스트 지정"](#) 및 [670페이지의 "클라이언트 사용자 아이디 지정"](#)을 참조하십시오.

마지막으로 가장 일반적인 형식의 필터는 다음과 같습니다.

*serviceList*: *clientList*

여기에서 *serviceList*는 하나 이상의 *serviceSpec* 항목으로 구성되며 *clientList*는 하나 이상의 *clientSpec* 항목으로 구성됩니다. *serviceList* 및 *clientList* 내의 개별 항목은 공백 및/또는 쉼표로 구분됩니다.

여기에서는 필터가 처리될 때 액세스를 요구하는 클라이언트가 *clientList*의 *clientSpec* 항목 중 하나와 일치할 경우 *serviceList*에 지정된 모든 서비스에 대한 액세스가 해당 필터 유형에 따라 허용되거나 거부됩니다. 다음은 이에 대한 한 예입니다.

pop, imap, http: .europe.siroe.com .newyork.siroe.com

이 필터가 허용 필터일 경우 europe.siroe.com 또는 newyork.siroe.com 도메인에 있는 모든 클라이언트는 POP, IMAP 및 HTTP 서비스에 대한 액세스가 허가됩니다. 선행 점이나 다른 패턴을 사용하여 도메인 또는 서브넷을 지정하는 방법에 대한 자세한 내용은 [668페이지의 "와일드카드 패턴"](#)을 참조하십시오.

또한 다음 구문을 사용할 수도 있습니다.

"+" 또는 "-" *serviceList*: \*\$next\_rule

+(허용 필터)는 클라이언트 목록에 대해 데몬 목록 서비스가 허가된다는 것을 의미합니다.

-(거부 필터)는 클라이언트 목록에 대해 서비스가 거부된다는 것을 의미합니다.

\*(와일드카드 필터)는 모든 클라이언트가 이러한 서비스를 사용하도록 허용합니다.

\$는 규칙을 구분합니다.

다음 예는 모든 클라이언트에서 여러 서비스를 사용 가능하게 합니다.

+imap,pop,http:\*

다음 예는 여러 규칙을 표시하지만 각 규칙은 서비스 이름을 하나만 가지도록 단순화되며 클라이언트 목록에 와일드카드를 사용합니다. 이는 LDIF 파일에서 액세스 제어를 지정하기 위해 가장 일반적으로 사용되는 방법입니다.

+imap:ALL\$+pop:ALL\$+http:ALL

다음 예는 사용자에게 대해 모든 서비스를 거부하는 방법을 보여 줍니다.

-imap:\*\$-pop:\*\$-http:\*

## 와일드카드 이름

다음 와일드카드 이름을 사용하여 서비스 이름, 호스트 이름이나 주소, 또는 아이디를 나타낼 수 있습니다.

**표 19-3** 서비스 필터의 와일드카드 이름

| 와일드카드 이름   | 설명                                                                                                                                                                                                                                                                                                   |
|------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ALL, *     | 범용 와일드카드입니다. 모든 이름과 일치합니다.                                                                                                                                                                                                                                                                           |
| LOCAL      | 모든 로컬 호스트(이름에 점 문자가 포함되지 않은 호스트)와 일치합니다. 그러나 설치가 정규 이름만 사용할 경우 로컬 호스트 이름은 점을 포함하므로 이 와일드카드와 일치하지 않습니다.                                                                                                                                                                                               |
| UNKNOWN    | 이름이 알려지지 않은 모든 사용자나 이름이나 주소가 알려지지 않은 모든 호스트와 일치합니다.<br>다음과 같이 이 와일드카드 이름을 신중하게 사용합니다.<br>임시 DNS 서버 문제로 인해 호스트 이름을 사용하지 못할 수 있습니다. 이러한 경우 UNKNOWN을 사용하는 모든 필터는 모든 클라이언트 호스트와 일치합니다.<br>통신하는 네트워크 유형을 소프트웨어에서 식별할 수 없으면 네트워크 주소를 사용할 수 없습니다. 이러한 경우 UNKNOWN을 사용하는 모든 필터는 해당 네트워크의 모든 클라이언트 호스트와 일치합니다. |
| KNOWN      | 이름이 알려진 모든 사용자나 이름 및 주소가 알려진 모든 호스트와 일치합니다.<br>다음과 같이 이 와일드카드 이름을 신중하게 사용합니다.<br>일시적인 DNS 서버 문제로 인해 호스트 이름을 사용하지 못할 수 있습니다. 이러한 경우 KNOWN을 사용하는 모든 필터를 모든 클라이언트 호스트에서 실패합니다.<br>통신하는 네트워크 유형을 소프트웨어에서 식별할 수 없으면 네트워크 주소를 사용할 수 없습니다. 이러한 경우 KNOWN을 사용하는 모든 필터는 해당 네트워크의 모든 클라이언트 호스트에서 실패합니다.         |
| DNSSPOOFER | DNS 이름이 고유한 IP 주소와 일치하는 않는 모든 호스트와 일치합니다.                                                                                                                                                                                                                                                            |

## 와일드카드 패턴

다음 패턴을 서비스나 클라이언트 주소에서 사용할 수 있습니다.

- 점 문자(.)로 시작하는 문자열. 이름의 마지막 구성 요소가 지정된 패턴과 일치할 경우 호스트 이름이 일치합니다. 예를 들어, 와일드카드 패턴 `.siroe.com`은 도메인 `siroe.com`의 모든 호스트와 일치합니다.
- 점 문자(.)로 끝나는 문자열. 첫 번째 숫자 필드가 지정된 패턴과 일치할 경우 호스트 주소가 일치합니다. 예를 들어, 와일드카드 패턴 `123.45.`는 서브넷 `123.45.0.0`에 있는 모든 호스트의 주소와 일치합니다.
- `n.n.n.n/m.m.m.m` 형식의 문자열. 이 와일드카드 패턴은 `net/mask` 쌍으로 해석됩니다. `net`이 주소 및 `mask`의 비트 AND와 같은 경우 호스트 주소가 일치합니다. 예를 들어, 패턴 `123.45.67.0/255.255.255.128`은 `123.45.67.0`에서 `123.45.67.127`까지의 모든 주소와 일치합니다.

## EXCEPT 연산자

액세스 제어 시스템은 단일 연산자를 지원합니다. EXCEPT 연산자를 사용하면 `serviceList` 또는 `clientList`에 여러 항목이 있을 경우 일치하는 이름이나 패턴에 대한 예외를 만들 수 있습니다. 예를 들어, 다음 표현식은

```
list1 EXCEPT list2
```

`list1`과 일치하는 항목이 또한 `list2`와 일치하지 않을 경우에 일치한다는 것을 의미합니다.

다음은 이에 대한 한 예입니다.

```
ALL: ALL EXCEPT issserver.siroe.com
```

이 예는 거부 필터인 경우 `issserver.siroe.com` 호스트 시스템에 있는 것을 제외하고 모든 클라이언트에 대해 모든 서비스의 액세스를 거부합니다.

EXCEPT 절은 중복될 수 있습니다. 다음 표현식은

```
list1 EXCEPT list2 EXCEPT list3
```

다음과 같은 것으로 평가됩니다.

```
list1 EXCEPT (list2 EXCEPT list3)
```

## 서버 호스트 지정

서버 호스트 이름이나 주소 정보를 `serviceSpec` 항목에 포함하여 요청되는 특정 서비스를 필터에서 추가로 식별할 수 있습니다. 이러한 경우 항목의 형식은 다음과 같습니다.

```
service@hostSpec
```

Messaging Server 호스트 시스템이 다른 인터넷 호스트 이름을 가진 여러 인터넷 주소에 대해 설정된 경우 이 기능을 사용할 수 있습니다. 서비스 공급자인 경우에는 이 기능을 사용하여 다른 액세스 제어 규칙을 가진 여러 도메인을 단일 서버 인스턴스에서 호스트할 수 있습니다.

## 클라이언트 사용자 아이디 지정

RFC 1413에 설명된 대로 `identd` 서비스를 지원하는 클라이언트 호스트 시스템의 경우 클라이언트의 사용자 아이디를 필터의 `clientSpec` 항목에 포함하여 특정 클라이언트 요청 서비스를 추가로 식별할 수 있습니다. 이러한 경우 항목의 형식은 다음과 같습니다.

```
user@hostSpec
```

여기에서 `user`는 클라이언트의 `identd` 서비스(또는 와일드카드 이름)에 의해 반환되는 사용자 아이디입니다.

필터에서 클라이언트 아이디를 지정하는 것은 유용할 수 있지만 다음과 같은 사항에 주의해야 합니다.

- `identd` 서비스는 인증이 아닙니다. 클라이언트 시스템이 손상된 경우 이 서비스가 반환하는 클라이언트 사용자 아이디를 신뢰할 수 없습니다. 일반적으로 특정 사용자 아이디를 사용하지 않으며 ALL, KNOWN 또는 UNKNOWN 와일드카드 이름만 사용합니다.
- `identd`는 대부분의 최신 클라이언트 시스템에서 지원되지 않으므로 현대적인 배포에서는 거의 가치가 없습니다. 이후 버전에서는 `identd` 지원을 제거하는 것이 고려되고 있으므로 이 기능이 필요한 경우 Sun Java System에 따로 알릴 필요가 있을 것입니다.
- 사용자 아이디 조회는 시간이 걸립니다. 따라서 모든 사용자에게 대한 조회를 수행하면 `identd`를 지원하지 않는 클라이언트의 액세스가 느려질 수 있습니다. 선택적 사용자 아이디 조회로 이 문제를 줄일 수 있습니다. 예를 들어, 다음과 같은 규칙은

```
serviceList: @xyzcorp.com ALL@ALL
```

사용자 아이디 조회를 수행하지 않고 도메인 xyzcorp.com의 사용자와 일치하지만 다른 모든 시스템에서는 사용자 아이디 조회를 수행합니다.

경우에 따라 사용자 아이디 조회 기능은 클라이언트 호스트에서 권한 없는 사용자의 공격으로부터 보호하는 데 도움이 될 수 있습니다. 예를 들어, 일부 TCP/IP 구현에서는 rsh(원격 셸 서비스)를 사용하는 침입자가 신뢰할 수 있는 클라이언트 호스트를 가장할 수 있습니다. 클라이언트 호스트가 `ident` 서비스를 지원할 경우 사용자 아이디 조회를 사용하여 이러한 공격을 감지할 수 있습니다.

## 필터 예

이 절의 예는 액세스 제어의 다양한 방법을 보여 줍니다. 이러한 예에서는 허용 필터가 거부 필터보다 먼저 처리되고 일치하는 항목이 발견될 때 검색이 종료하며 일치하는 항목이 전혀 없을 경우 액세스가 허가된다는 것에 주의합니다.

여기에 나열된 예는 IP 주소가 아니라 호스트 및 도메인 이름을 사용합니다. 주소와 넷마스크 정보를 필터에 포함하여 이름 서비스 실패를 대비한 안정성을 향상시킬 수 있다는 것에 주의합니다.

### 대부분 거부

이 경우에는 액세스가 기본적으로 거부됩니다. 명시적으로 허가된 호스트만 액세스가 허용됩니다.

기본 정책(액세스 없음)은 다음과 같은 평범하고 단순한 거부 파일을 통해 구현됩니다.

```
ALL: ALL
```

이 필터는 허용 필터에 의해 액세스가 명시적으로 허가되지 않은 모든 클라이언트에 대한 모든 서비스를 거부합니다. 그런 다음 허용 필터는 다음과 같을 수 있습니다.

```
ALL: LOCAL @netgroup1
```

```
ALL: .siroe.com EXCEPT externalserver.siroe.com
```

첫 번째 규칙은 로컬 도메인(즉, 호스트 이름에 점이 없는 모든 호스트)의 모든 호스트와 netgroup1 그룹의 구성원에 대해 액세스를 허가합니다. 두 번째 규칙은 선행 점 와일드카드 패턴을 사용하여 externalserver.siroe.com 호스트를 제외하고 siroe.com 도메인에 있는 모든 호스트의 액세스를 허가합니다.

### 대부분 허용

이 경우에는 액세스가 기본적으로 허가됩니다. 명시적으로 지정된 호스트만 액세스가 거부됩니다.

기본 정책(액세스 허가)은 허용 필터를 불필요하게 만듭니다. 원하지 않는 클라이언트는 다음과 같이 거부 필터에 명시적으로 나열됩니다.

```
ALL: externalserver.siroe1.com, .siroe.asia.com
```

```
ALL EXCEPT pop: contractor.siroe1.com, .siroe.com
```

첫 번째 필터는 특정 호스트와 특정 도메인에 대해 모든 서비스를 거부합니다. 두 번째 필터는 특정 호스트와 특정 도메인의 POP 액세스만 허가합니다.

## 스푸핑된 도메인에 대한 액세스 거부

필터에서 DNSSPOOFER 와일드카드 이름을 사용하여 호스트 이름 스푸핑을 감지할 수 있습니다. DNSSPOOFER를 지정하면 액세스 제어 시스템은 정방향 또는 역방향 DNS 조회를 수행하여 클라이언트가 제공한 호스트 이름이 실제 IP 주소와 일치하는지 확인합니다. 다음은 거부 필터의 예입니다.

```
ALL: DNSSPOOFER
```

이 필터는 IP 주소가 해당 DNS 호스트 이름과 일치하지 않는 모든 원격 호스트에 대한 모든 서비스를 거부합니다.

## 가상 도메인에 대한 액세스 제어

단일 서버 인스턴스가 여러 IP 주소 및 도메인 이름과 연관된 가상 도메인을 메시징 설치에서 사용할 경우 허용 및 거부 필터를 조합하여 각 가상 도메인에 대한 액세스를 제어할 수 있습니다. 예를 들어, 다음 허용 필터를

```
ALL@msgServer.siroe1.com: @.siroe1.com
```

```
ALL@msgServer.siroe2.com: @.siroe2.com
```

```
...
```

다음 거부 필터와 결합하여 사용할 수 있습니다.

```
ALL: ALL
```

각 허용 필터는 domainN 내의 호스트만 IP 주소가 msgServer.siroeN.com에 해당하는 서비스에 연결되도록 허용합니다. 다른 모든 연결은 거부됩니다.

## 서비스에 대한 액세스 필터 만들기

IMAP, POP 또는 HTTP 서비스에 대한 허용 및 거부 필터를 만들 수 있습니다. 또한 이러한 필터를 SMTP 서비스에 대해 만들 수 있지만 인증된 SMTP 세션에만 적용된다는 점에서 이것은 거의 가치가 없습니다. 인증되지 않은 SMTP 세션에 대한 액세스를 제어하는 방법은 17장, "메일 필터링 및 액세스 제어"를 참조하십시오.

**콘솔.** 콘솔을 사용하여 필터를 만들려면 다음 단계를 따릅니다.

1. 콘솔에서 액세스 필터를 만들려는 Messaging Server를 엽니다.
2. 구성 탭을 누릅니다.
3. 왼쪽 표시 영역에서 서비스 폴더를 열고 서비스 폴더 아래에서 IMAP, POP 또는 HTTP를 선택합니다.



#### 4. 오른쪽 표시 영역에서 액세스 탭을 누릅니다.

이 탭의 허용 및 표시 필드에는 해당 서비스에 대한 기존의 허용 및 거부 필터가 표시됩니다. 필드의 각 행은 하나의 필터를 나타냅니다. 이러한 필드 중 하나에서 다음 작업을 지정할 수 있습니다.

- a. 추가를 눌러 새 필터를 만듭니다. 필터 허용 또는 필터 거부 창이 열리면 새 필터의 텍스트를 창에 입력하고 확인을 누릅니다.
- b. 필터를 선택하고 편집을 눌러 필터를 수정합니다. 필터 허용 또는 필터 거부 창이 열리면 창에 표시된 필터의 텍스트를 편집하고 확인을 누릅니다.
- c. 필터를 선택하고 삭제를 눌러 필터를 제거합니다.

필요한 경우 일련의 삭제 및 추가 작업을 수행하여 허용 또는 거부 필터의 순서를 재정렬할 수 있다는 것에 주의합니다.

필터 구문 지정과 다양한 예는 [666페이지의 "필터 문"](#)을 참조하십시오. 추가 예는 [671페이지의 "필터 예"](#)를 참조하십시오.

**명령줄.** 다음과 같이 명령줄에서 액세스 및 거부 필터를 지정할 수도 있습니다.

서비스에 대한 액세스 필터를 작성 또는 편집하려면 다음을 수행합니다.

```
configutil -o service.service.domainallowed -v filter
```

여기에서 *service*는 pop, imap 또는 http이고 *filter*는 [666페이지의 "필터 문"](#)에 설명된 구문 규칙을 따릅니다.

서비스에 대한 거부 필터를 작성 또는 편집하려면 다음을 수행합니다.

```
configutil -o service.service.domainnotallowed -v filter
```

여기에서 *service*는 pop, imap 또는 http이고 *filter*는 [666페이지의 "필터 문"](#)에 설명된 구문 규칙을 따릅니다.

## HTTP 프록시 인증에 대한 액세스 필터 만들기

모든 저장소 관리자는 모든 서비스에 대해 프록시 인증을 수행할 수 있습니다. 저장소 관리자에 대한 자세한 내용은 [557페이지의 "저장소에 대한 관리자 액세스 지정"](#)을 참조하십시오. 모든 사용자는 해당 클라이언트 호스트가 프록시 인증 액세스 필터를 통해 액세스가 허가된 경우 HTTP 서비스에 한하여 프록시 인증을 수행할 수 있습니다.

프록시 인증을 사용하면 포털 사이트 등의 다른 서비스에서 사용자를 인증하고 인증서를 HTTP 로그인 서비스로 전달할 수 있습니다. 예를 들어, 포털 사이트가 여러 서비스를 제공하며 그 중 하나가 Messenger Express 웹 기반 전자 메일이라고 가정해 봅니다. 이 경우 최종 사용자는 HTTP 프록시 인증 기능을 사용하여 포털 서비스에 한 번만 인증되면 됩니다. 즉, 전자 메일에 액세스하기 위해 다시 인증될 필요가 없습니다. 포털 사이트는 클라이언트와 서비스 간의 인터페이스로 작동하는 로그인 서버를 구성해야 합니다. Messenger Express 인증을 위한 로그인 서버의 구성을 돕기 위해 Sun Java System은 Messenger Express용 인증 SDK를 제공합니다.

이 절에서는 IP 주소별로 HTTP 프록시 인증을 허용하기 위해 허용 필터를 만드는 방법에 대해 설명합니다. 로그인 서버를 설정하는 방법이나 Messenger Express 인증 SDK를 사용하는 방법은 이 절에서 설명하지 않습니다. Messenger Express에 맞게 로그인 서버를 설정하고 인증 SDK를 사용하는 방법에 대한 자세한 내용은 Sun Java System 담당자에게 문의하십시오.

**콘솔.** HTTP 서비스에 대한 프록시 인증을 위한 액세스 필터를 만들려면 다음을 수행합니다.

1. 콘솔에서 액세스 필터를 만들려는 Messaging Server를 엽니다.
2. 구성 탭을 누릅니다.
3. 왼쪽 표시 영역에서 서비스 폴더를 열고 서비스 폴더 아래에서 HTTP를 선택합니다.
4. 오른쪽 표시 영역에서 프록시 탭을 누릅니다.  
이 탭의 허용 필드에는 프록시 인증에 대한 기존의 허용 필터가 표시됩니다.
5. 새 필터를 만들려면 추가를 누릅니다.  
허용 필터 창이 열리면 새 필터의 텍스트를 창에 입력하고 확인을 누릅니다.
6. 기존 필터를 편집하려면 필터를 선택하고 편집을 누릅니다.  
허용 필터 창이 열리면 창에 표시된 필터의 텍스트를 편집하고 확인을 누릅니다.
7. 기존 필터를 삭제하려면 허용 필드에서 필드를 선택하고 삭제를 누릅니다.
8. 프록시 탭에 대한 변경이 끝나면 저장을 누릅니다.

허용 필터 구문에 대한 자세한 내용은 [666페이지의 "필터 문"](#)을 참조하십시오.

**명령줄.** 다음과 같이 명령줄에서 HTTP 서비스에 대한 프록시 인증을 위한 액세스 필터를 지정할 수도 있습니다.

```
configutil -o service.service.proxydomainallowed -v filter
```

여기에서 *filter*는 666페이지의 "필터 문"에 설명된 구문 규칙을 따릅니다.

## POP before SMTP 사용

SMTP 인증 또는 *SMTP Auth*(RFC 2554)는 SMTP 릴레이 서버 보안을 제공하는 데 선호되는 방법입니다. *SMTP Auth*는 인증된 사용자만 MTA를 통해 메일을 보낼 수 있도록 허용합니다. 그러나 일부 레거시 클라이언트는 *POP before SMTP*에 대한 지원만 제공합니다. 이러한 시스템에서는 아래 설명된 것처럼 *POP before SMTP*를 사용 가능하게 할 수 있습니다. 그러나 가능하면 사용자에게 *POP before SMTP*를 사용하는 대신 POP 클라이언트를 업그레이드하도록 권장하는 것이 좋습니다. 사이트에서 *POP before SMTP*가 배포되고 나면 사용자는 인터넷 보안 표준을 따르지 못하는 클라이언트에 의존하게 됩니다. 따라서 최종 사용자가 해킹의 위협에 노출될 뿐만 아니라 성공적인 최근 POP 세션의 IP 주소를 추적 및 조정하면서 발생하는 불가피한 성능 저하로 인해 사이트 속도가 느려집니다.

Messaging Server의 *POP before SMTP* 구현은 SIMS 또는 Netscape Messaging Server에서와 완전히 다릅니다. POP 및 SMTP 프록시 모두를 가지도록 MMP(Messaging Multiplexor)를 구성하여 *POP before SMTP*를 지원합니다. SMTP 클라이언트가 SMTP 프록시에 연결하면 프록시는 최근 POP 인증의 메모리 내장 캐시를 검사합니다. 동일한 클라이언트 IP 주소의 POP 인증이 발견되면 SMTP 프록시는 메일을 로컬 및 비로컬 수신자 모두에게 보낼 수 있게 허용해야 한다는 것을 SMTP 서버에 알립니다.

## SMTP 프록시 설치

1. *Sun ONE Messaging Server 설치 설명서*에 설명된 대로 MMP(Messaging Multiplexor)를 설치합니다.

2. MMP에서 SMTP 프록시를 사용 가능하게 합니다.

다음 문자열을

```
msg_svr_base/lib/SmtProxyAService@25|587
```

msg\_svr\_base/config/AService.cfg 파일의 ServiceList 옵션에 추가합니다. 이 옵션은 길이가 한 줄이며 줄 바꿈을 포함할 수 없습니다.

---

**주** MMP가 업그레이드되면 MMP에 대한 네 개의 기존 구성 파일에 해당하는 네 개의 새 파일이 만들어집니다. 이러한 새 파일은 다음과 같습니다.

```
AService-def.cfg, ImapProxyAService-def.cfg,  
PopProxyAService-def.cfg 및 SmtProxyAService-def.cfg
```

이러한 파일은 설치 프로그램에 의해 만들어지며 문서에 설명된 네 개의 구성 파일은 설치하는 동안에 만들어지거나 영향을 받지 않습니다.

MMP는 시작되면 일반 구성 파일(현재 문서화되어 있는)을 찾습니다. 일반 구성 파일을 찾지 못한 경우 MMP는 각 \*AService-def.cfg 파일을 해당 \*AService.cfg 파일 이름에 복사하는 것을 시도합니다.

---

3. 각 SMTP 릴레이 서버에서 SMTP 채널 옵션 파일 tcp\_local\_option의 PROXY\_PASSWORD 옵션을 설정합니다.

SMTP 프록시는 SMTP 서버에 연결되면 실제 클라이언트 IP 주소와 다른 연결 정보를 SMTP 서버에 알려 SMTP 서버가 릴레이 차단 및 다른 보안 정책(POP before SMTP 인증 포함)을 제대로 적용할 수 있게 해야 합니다. 이것은 보안에 민감한 작업으로서 반드시 인증되어야 합니다. MMP SMTP 프록시 및 SMTP 서버 모두에서 구성되는 프록시 비밀번호는 다른 사람이 기능을 남용할 수 없게 합니다.

**예:** PROXY\_PASSWORD=A\_Password

4. MMP에서 SMTP 서버에 연결하기 위해 사용하는 IP 주소가 INTERNAL\_IP 매핑 테이블에서 "내부" 주소로 처리되지 않는지 확인합니다.

INTERNAL\_IP 매핑 테이블에 대한 자세한 내용은 17장, "메일 필터링 및 액세스 제어"에서 528페이지의 "SMTP 릴레이 추가"를 참조하십시오.

5. POP before SMTP를 지원하도록 SMTP 프록시를 구성합니다.

- a. `msg_svr_base/config/SmtproxyAService.cfg` 구성 파일을 편집합니다.

다음 SMTP 프록시 옵션은 IMAP 및 POP 프록시 옵션(155페이지의 7장, "멀티플렉서 서비스 구성 및 관리" 및 *Sun Java System Messaging Server Administration Reference*(<http://docs.sun.com/doc/819-0106>)에서 Encryption(SSL) Option 절의 이러한 옵션에 대한 설명 참조)과 똑같이 작동합니다.

```
LdapURL, LogDir, LogLevel, BindDN, BindPass, Timeout, Banner, SSLEnable,
SSLSecmodFile, SSLCertFile, SSLKeyFile, SSLKeyPasswdFile,
SSLCipherSpecs, SSLCertNicknames, SSLCacheDir, SSLPorts, CertMapFile,
CertmapDN, ConnLimits, TCPAccess
```

위에 나열되지 않은 다른 MMP 옵션(BacksidePort 옵션 포함)은 현재 SMTP 프록시에 적용되지 않습니다.

다음 다섯 개의 옵션을 추가합니다.

`SmtRelays`는 라운드 로빈 릴레이에 사용할 SMTP 릴레이 서버 호스트 이름(선택적 포트 포함)의 공백으로 구분된 목록입니다. 이러한 릴레이는 `XPROXYEHLO` 확장을 지원해야 합니다. 이 옵션은 필수이며 기본값은 없습니다.

예: `default:SmtRelays manatee:485 gonzo mothra`

`SmtProxyPassword`는 SMTP 릴레이 서버에 대한 소스 채널 변경 사항을 허가하는 데 사용되는 비밀번호입니다. 이 옵션은 필수이고 기본값은 없으며 SMTP 서버의 `PROXY_PASSWORD` 옵션과 일치해야 합니다.

예: `default:SmtProxyPassword A_Password`

`EhloKeywords` 옵션은 기본 집합 외에 클라이언트에게 전달할 프록시에 대한 EHLO 확장 키워드 목록을 제공합니다. MMP는 SMTP 릴레이에 의해 반환된 EHLO 목록에서 인식되지 않은 모든 EHLO 키워드를 제거합니다.

`EhloKeywords`는 이 목록에서 제거하지 않아야 하는 추가 EHLO 키워드를 지정합니다. 기본값은 비어 있지만 `8BITMIME`, `PIPELINING`, `DSN`,

`ENHANCEDSTATUSCODES`, `EXPN`, `HELP`, `XLOOP`, `ETRN`, `SIZE`, `STARTTLS`, `AUTH` 키워드는 SMTP 프록시에서 지원되므로 이 옵션에 나열할 필요가 없습니다.

다음은 드물게 사용되는 "TURN" 확장을 사용하는 사이트에서 사용할 수 있는 예입니다.

예: default: EhloKeywords TURN

PopBeforeSmtplKludgeChannel 옵션은 허가된 POP before SMTP 연결에 사용할 MTA 채널의 이름으로 설정됩니다. 기본값은 비어 있으며 POP before SMTP를 사용 가능하게 하려는 사용자에게 대한 일반 설정은 tcp\_intranet입니다. 이 옵션은 SSL 성능을 최적화하는 데 필요하지 않습니다(660페이지의 "SMTP 프록시를 사용하여 SSL 성능을 최적화하는 방법" 참조).

예: default: PopBeforeSmtplKludgeChannel tcp\_intranet

ClientLookup 옵션은 기본적으로 no입니다. yes로 설정된 경우 클라이언트 IP 주소에 대한 DNS 역방향 조회가 무조건 수행되므로 SMTP 릴레이 서버에서 이 작업을 수행할 필요가 없습니다. 이 옵션은 호스트된 도메인별로 설정할 수 있습니다.

예: default: ClientLookup yes

- b. PopProxyAService.cfg 구성 파일에서 PreAuth 및 AuthServiceTTL 옵션을 설정합니다. 이 옵션은 SSL 성능을 최적화하는 데 필요하지 않습니다. 660페이지의 "SMTP 프록시를 사용하여 SSL 성능을 최적화하는 방법"을 참조하십시오.

---

**주** POP before SMTP가 작동하려면 IMAP 또는 SMTP 프록시 구성 파일에서 AuthServiceTTL을 설정하면 **안 됩니다**.

---

이러한 옵션은 POP 인증 후에 사용자가 메일을 전달할 수 있도록 허가된 시간(초)을 지정합니다. 일반 설정은 900-1800(15-30분)입니다.

예:

```
default:PreAuth    yes
default:AuthServiceTTL  900
```

- c. 목록에서 다음 항목을 시도하기 전에 MMP가 SMTP 릴레이의 응답을 대기하는 시간(초)을 선택적으로 지정할 수 있습니다.

기본값은 10(초)입니다. SMTP 릴레이에 대한 연결이 실패한 경우 MMP는 페일 오버 시간 초과에 해당하는 시간(분) 동안 해당 릴레이를 시도하지 않습니다(따라서 페일오버 시간 초과가 10초이고 릴레이가 실패한 경우 MMP는 해당 릴레이를 10분 동안 다시 시도하지 않음).

예: `default:FailoverTimeout 10`

## SMTP 서비스에 대한 클라이언트 액세스 구성

SMTP 서비스에 대한 클라이언트 액세스 구성에 대한 자세한 내용은 [17장, "메일 필터링 및 액세스 제어"](#)를 참조하십시오.

## SSL을 통한 사용자/그룹 디렉토리 조회

MTA, MMP 및 IMAP/POP/HTTP 서비스를 위해 SSL을 통한 사용자/그룹 디렉토리 조회를 수행할 수 있습니다. 전제 조건은 Messaging Server가 SSL 모드에서 구성되어야 한다는 것입니다. 이 기능을 활성화하려면 `configutil` 매개 변수를 설정해야 합니다. 즉, `local.service.pab.ldapport`는 636으로, `local.ugldapport`는 636으로, `local.ugldapussl`은 1로 설정합니다.





# Communications Express Mail용 S/MIME 관리

S/MIME(Secure/Multipurpose Internet Mail Extension)을 Sun Java System Communications Express Mail에서 사용할 수 있습니다. S/MIME을 사용하도록 설정한 Communications Express Mail 사용자는 Communications Express Mail, Microsoft Outlook Express 및 Mozilla 메일 시스템의 다른 사용자와 서명되었거나 암호화된 메일을 교환할 수 있습니다.

Communications Express Mail에서 S/MIME을 사용하는 방법에 대한 자세한 내용은 온라인 도움말을 참조하십시오. 이 장에서는 S/MIME을 관리하는 방법에 대해 설명합니다. 이 장은 다음 내용으로 구성되어 있습니다.

- [682페이지의 "S/MIME"](#)
- [683페이지의 "필수 소프트웨어 및 하드웨어 구성 요소"](#)
- [684페이지의 "S/MIME 사용을 위한 요구 사항"](#)
- [686페이지의 "Messaging Server 설치 후 시작"](#)
- [694페이지의 "smime.conf 파일의 매개 변수"](#)
- [701페이지의 "Messaging Server 옵션"](#)
- [702페이지의 "SSL을 사용하여 인터넷 연결 보안"](#)
- [703페이지의 "클라이언트 시스템의 키 액세스 라이브러리"](#)
- [705페이지의 "개인 및 공개 키 확인"](#)
- [711페이지의 "S/MIME 기능을 사용할 수 있는 권한 부여"](#)
- [712페이지의 "인증서 관리"](#)
- [717페이지의 "Communications Express S/MIME 최종 사용자 정보"](#)

# S/MIME

S/MIME은 Communications Express Mail 사용자에게 다음 기능을 제공합니다.

- 보내는 메일에 대한 디지털 서명을 만들어 메일을 받는 사람이 메일이 손상되지 않았으며 메일을 보낸 사람으로부터 받았음을 확인할 수 있게 합니다.
- 메일이 수신자의 메일함에 도착하기 전에 다른 사람이 메일 내용을 확인, 변경 또는 사용하는 것을 방지하기 위해 나가는 메일 메시지를 암호화합니다.
- 인증서 해지 목록(CRL)을 포함하는 프로세스를 사용하여 서명된 받는 메일의 디지털 서명을 확인합니다.
- 수신자가 메일의 내용을 읽을 수 있도록 암호화된 받는 메일을 자동으로 해독합니다.
- 서명 및 암호화된 메시지를 Communications Express Mail 및 Mozilla 메일 시스템 같은 S/MIME 호환 클라이언트를 사용하는 다른 사용자와 교환합니다.

## 알아야 할 개념

S/MIME을 올바르게 관리하려면 다음 개념에 익숙해야 합니다.

- 플랫폼의 기본 관리 절차
- LDAP(Lightweight Directory Access Protocol) 디렉토리의 구조 및 사용
- LDAP 디렉토리의 항목 추가 또는 수정
- Sun Java System Directory Server의 구성 프로세스
- 다음에 대한 개념 및 용도
  - 보안 통신 회선을 위한 SSL(Secure Socket Layer)
  - 디지털 서명된 전자 메일 메시지
  - 암호화된 전자 메일 메시지
  - 브라우저의 로컬 키 저장소
  - 스마트 카드와 이를 사용하기 위한 소프트웨어 및 하드웨어
  - 개인 공개 키 쌍 및 해당 인증서

- 인증 기관(CA)
- 키와 해당 인증서 확인
- 인증서 해지 목록(CRL). 이에 대한 소개는 [706페이지의 "CRL에 대해 인증서 확인"](#)을 참조하십시오.

## 필수 소프트웨어 및 하드웨어 구성 요소

이 절에서는 S/MIME과 함께 Communications Express Mail을 사용하기 위한 필수 하드웨어 및 소프트웨어에 대해 설명합니다. S/MIME 구성을 시도하기 전에 서버와 클라이언트 시스템에 올바른 버전의 소프트웨어를 모두 설치해야 합니다.

**표 20-1**에는 Communications Express Mail에 액세스하는 클라이언트 시스템의 필수 소프트웨어 및 하드웨어가 나열되어 있습니다.

**표 20-1** 클라이언트 시스템의 필수 하드웨어 및 소프트웨어

| 구성 요소                                      | 설명                                                                                                                                                                                                                                                                                                                                                                                    |
|--------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 운영 체제                                      | <ul style="list-style-type: none"> <li>• Microsoft Windows 98, 2000 또는 XP</li> </ul>                                                                                                                                                                                                                                                                                                  |
| 브라우저                                       | <ul style="list-style-type: none"> <li>• Windows용 Microsoft Internet Explorer 버전 6 SP2</li> <li>• Windows 2000 및 Windows 98용 Microsoft Internet Explorer 버전 6 SP1(2004년 12월 1일 당시의 최신 패치 포함)</li> </ul>                                                                                                                                                                               |
| Sun 소프트웨어                                  | Sun Java 2 Runtime Environment, Standard Edition, 버전 1.4.2_03 이상(1.5는 아님)                                                                                                                                                                                                                                                                                                             |
| 인증서가 포함된 개인-공개 키                           | <p>인증서가 포함된 하나 이상의 개인-공개 키 쌍. 인증서가 필요하며 표준 X.509 v3 형식이어야 합니다. S/MIME 기능을 사용하게 될 각 Communications Express Mail 사용자에게 대해 CA로부터 키와 인증서를 얻습니다. 키와 해당 인증서는 클라이언트 시스템이나 스마트 카드에 저장됩니다. 공개 키와 인증서는 Directory Server가 액세스할 수 있는 LDAP 디렉토리에 저장됩니다.</p> <p>키 인증서를 CA가 유지 관리하는 인증서 해지 목록(CRL)과 비교하여 키의 유효성을 추가로 확인하려면 CRL이 시스템의 일부여야 합니다. <a href="#">706페이지의 "CRL에 대해 인증서 확인"</a>을 참조하십시오.</p> |
| 스마트 카드 소프트웨어(키와 인증서를 스마트 카드에 저장할 경우에만 필요함) | <ul style="list-style-type: none"> <li>• ActivCard Gold 버전 2.1 또는 3.0</li> <li>• NetSign 버전 3.1</li> </ul>                                                                                                                                                                                                                                                                            |
| 스마트 카드 판독기                                 | 클라이언트 시스템 및 스마트 카드 소프트웨어가 지원하는 스마트 카드 판독 장치 모델                                                                                                                                                                                                                                                                                                                                        |

표 20-2에는 서버 시스템의 필수 Sun Microsystems 소프트웨어가 나열되어 있습니다.

**표 20-2** 서버 시스템의 필수 소프트웨어

| Sun 구성 요소 | 설명                                                                                                                                        |
|-----------|-------------------------------------------------------------------------------------------------------------------------------------------|
| 메일 서버     | Sun Java System Messaging Server 6 2005Q1 릴리스(Solaris 버전 8 또는 9 및 Sun SPARC 시스템)                                                          |
| LDAP 서버   | Sun Java System Directory Server 5 2004Q2 이상                                                                                              |
| Java      | Java 2 Runtime Environment, Standard Edition, 버전 1.4.2 이상                                                                                 |
| 액세스 관리자   | (Schema 2에서 배포하는 경우) - Sun Java System Access Manager 6 2005Q1 및 Communications Express - Sun Java System Communications Express 6 2005Q1 |

## S/MIME 사용을 위한 요구 사항

Messaging Server를 설치한 후 Communications Express Mail 사용자가 서명 및 암호화 기능을 즉시 사용할 수 있는 것은 아닙니다. 사용자가 S/MIME을 사용할 수 있으려면 이 절에서 설명하는 요구 사항이 충족되어야 합니다.

### 개인 및 공개 키

S/MIME을 사용할 각 Communications Express Mail 사용자에게 표준 X.509 v3 형식의 인증서를 포함하여 하나 이상의 개인 및 공개 키 쌍을 발급해야 합니다. 확인 프로세스에 사용되는 인증서는 다른 메일 사용자에게 키가 실제로 키를 사용하는 사람에게 속해 있다는 것을 보장합니다. 사용자는 둘 이상의 키 쌍과 관련 인증서를 가질 수 있습니다.

키와 해당 인증서는 조직 내에서 발급 받거나 타사 공급업체에게 구입합니다. 키와 인증서 발급 방법에 상관없이 발급하는 조직을 인증 기관(CA)이라고 합니다.

키 쌍과 해당 인증서는 다음 두 가지 방법으로 저장됩니다.

- 스마트 카드라고 부르는 일반 액세스 카드(CAC)에 저장
  - 이러한 카드는 일반 신용 카드와 비슷하며 신용 카드를 사용할 때와 마찬가지로 메일 사용자가 적절하게 보호해야 합니다. 스마트 카드에서 개인 키 정보를 읽으려면 메일 사용자의 컴퓨터(클라이언트 시스템)에 연결된 특수한 카드 판독기가 필요합니다. 자세한 내용은 685페이지의 "스마트 카드에 저장된 키"를 참조하십시오.
- 메일 사용자 컴퓨터(클라이언트 시스템)의 로컬 키 저장소에 저장

메일 사용자의 브라우저에는 키 저장소가 있습니다. 또한 브라우저는 키 쌍과 인증서를 키 저장소로 다운로드하기 위한 명령도 제공합니다. 자세한 내용은 [685페이지](#)의 "[클라이언트 시스템에 저장된 키](#)"를 참조하십시오.

## 스마트 카드에 저장된 키

인증서를 포함하는 개인 공개 키 쌍을 스마트 카드에 저장할 경우 카드 판독기를 메일 사용자의 컴퓨터에 올바르게 연결해야 합니다. 또한 카드 판독 장치에는 소프트웨어가 필요합니다. 카드 판독 장치와 해당 소프트웨어는 장비를 판매하는 공급업체가 제공합니다.

판독 장치가 적절하게 설치되면 메일 사용자는 보내는 메일에 대한 디지털 서명을 만들려는 경우에 스마트 카드를 판독 장치에 삽입합니다. 스마트 카드 비밀번호가 확인되면 **Communications Express Mail**에서 메일에 서명하기 위해 개인 키에 액세스할 수 있습니다. 지원되는 스마트 카드와 판독 장치에 대한 자세한 내용은 [683페이지](#)의 "[필수 소프트웨어 및 하드웨어 구성 요소](#)"를 참조하십시오.

스마트 카드 공급업체가 제공하는 라이브러리가 사용자의 컴퓨터에 있어야 합니다. 자세한 내용은 [703페이지](#)의 "[클라이언트 시스템의 키 액세스 라이브러리](#)"를 참조하십시오.

## 클라이언트 시스템에 저장된 키

키 쌍과 인증서를 스마트 카드에 저장하지 않을 경우 메일 사용자의 컴퓨터(클라이언트 시스템)에 있는 로컬 키 저장소에 보관해야 합니다. 메일 사용자의 브라우저에서 키 저장소를 제공하고 키 쌍과 인증서를 키 저장소에 다운로드하기 위한 명령도 제공합니다. 브라우저에 따라 키 저장소를 비밀번호로 보호하기도 합니다.

로컬 키 저장소를 지원하려면 브라우저 공급업체가 제공하는 라이브러리가 사용자의 컴퓨터에 있어야 합니다. 자세한 내용은 [703페이지](#)의 "[클라이언트 시스템의 키 액세스 라이브러리](#)"를 참조하십시오.

## LDAP 디렉토리에 공개 키 게시

모든 공개 키와 인증서는 Sun Java System Directory Server가 액세스할 수 있는 LDAP 디렉토리에 저장해야 합니다. 이러한 작업을 S/MIME 메일을 작성하는 다른 메일 사용자가 사용할 수 있도록 공개 키를 게시한다고 합니다.

보낸 사람과 받는 사람의 공개 키는 암호화된 메일의 암호화/해독 프로세스에 사용됩니다. 공개 키 인증서는 디지털 서명에 사용된 공개 키를 검증하는 데 사용됩니다.

ldapmodify를 사용하여 공개 키와 인증서를 게시하는 방법은 [712페이지의 "인증서 관리"](#)를 참조하십시오.

## 메일 사용자에게 S/MIME 사용 권한 부여

서명된 또는 암호화된 메일을 작성하려면 유효한 Communications Express Mail 사용자에게 그렇게 할 수 있는 권한이 있어야 합니다. 이 작업을 수행하려면 사용자의 LDAP 항목에 대한 mailAllowedServiceAccess 또는 mailDomainAllowedServiceAccess LDAP 속성을 사용합니다. 이러한 속성을 사용하여 개인 또는 도메인 단위로 S/MIME의 메일 사용자를 포함시키거나 제외시킬 수 있습니다.

자세한 내용은 [711페이지의 "S/MIME 기능을 사용할 수 있는 권한 부여"](#)를 참조하십시오.

## 여러 언어 지원

메일 메시지에 영어만 사용하는 Communications Express Mail 사용자는 라틴어가 아닌 언어(예: 중국어)의 문자를 포함하는 S/MIME 메일을 읽지 못할 수 있습니다. 이러한 상황이 발생하는 한 가지 이유는 사용자 시스템에 설치된 JRE(Java 2 Runtime Environment)의 /lib 디렉토리에 charsets.jar 파일이 없기 때문입니다.

기본 JRE 설치 프로세스를 사용하여 영어 버전의 JRE를 다운로드한 경우 charsets.jar 파일이 설치되지 않습니다. 그러나 기본 설치의 다른 모든 언어 항목을 선택하면 charsets.jar가 설치됩니다.

charsets.jar 파일이 /lib 디렉토리에 설치되게 하려면 사용자 정의 설치를 사용하여 영어 버전의 JRE를 설치하라고 사용자에게 알립니다. 설치 중에 사용자가 "추가 언어 지원" 옵션을 선택해야 합니다.

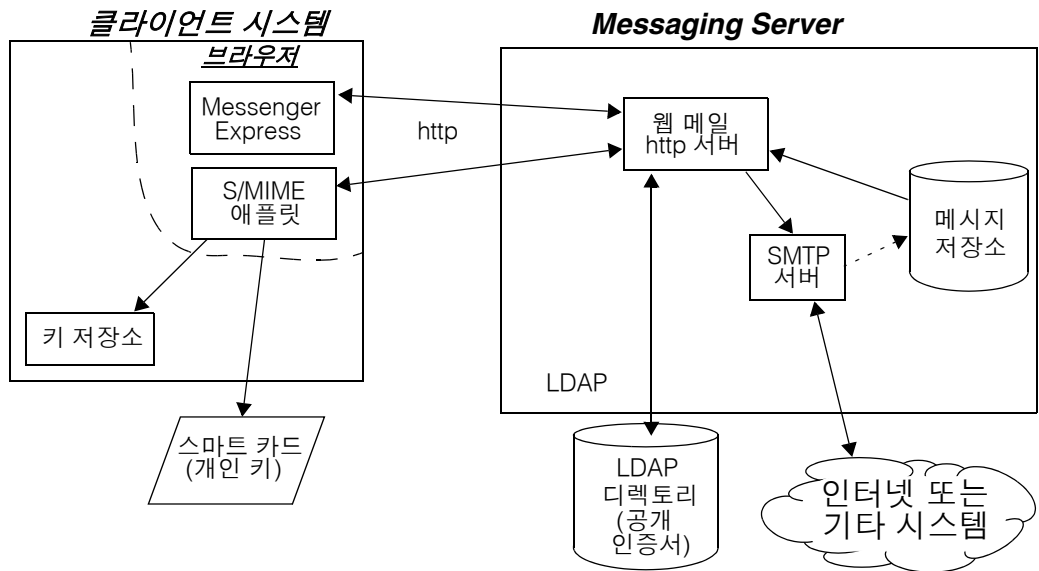
## Messaging Server 설치 후 시작

이 절에서는 S/MIME 애플릿이란 무엇이며 Communications Express Mail의 S/MIME을 설정하는 기본 구성 절차에 대해 설명합니다. 구성 프로세스에는 S/MIME 애플릿의 매개 변수와 Messaging Server의 옵션을 설정하는 작업이 포함됩니다.

## S/MIME 애플릿

개인 및 공개 키를 확인하는 여러 절차와 함께 메일에 서명하거나, 메일을 암호화하거나, 메일을 해독하는 프로세스는 S/MIME 애플릿이라고 부르는 특수한 애플릿에 의해 처리됩니다. S/MIME 기능을 구성하려면 smime.conf 파일의 매개 변수와 Messaging Server 옵션을 사용합니다. **그림 20-1**에서는 S/MIME 애플릿과 다른 시스템 구성 요소와의 관계를 보여 줍니다.

**그림 20-1** S/MIME 애플릿



### 처음으로 로그인

S/MIME을 사용할 수 있는 권한을 가진 Communications Express Mail 사용자가 Messaging Server에 처음 로그인하면 S/MIME 애플릿에 대한 일련의 특수한 프롬프트가 표시됩니다. 프롬프트에서 Yes 또는 Always를 선택하면 S/MIME 애플릿이 사용자의 컴퓨터에 다운로드됩니다. 사용자가 Communications Express Mail을 로그아웃할 때까지 S/MIME 애플릿이 컴퓨터에 남아 있습니다.

자세한 내용은 **712페이지의 "인증서 관리"**를 참조하십시오.

## S/MIME 애플릿 다운로드

사용자 컴퓨터에서 JRE(Java 2 Runtime Environment)에 대한 캐싱이 활성화되어 있지 않은 경우 사용자가 Communications Express Mail에 로그인할 때마다 S/MIME 애플릿이 다운로드됩니다. 캐싱이 활성화되면 초기 다운로드 후에 S/MIME 애플릿의 복사본이 사용자의 시스템에 저장되므로 사용자가 로그인할 때마다 애플릿이 다운로드되지 않습니다.

캐싱은 성능을 향상시키므로 사용자에게 Java 2 Runtime Environment 버전 1.4.x에 대한 캐싱을 활성화하는 다음 단계를 수행하도록 지시할 수 있습니다.

1. Windows 제어판으로 이동합니다.
2. Java 플러그인 아이콘(Java 2 Runtime Environment)을 두 번 누릅니다.
3. 캐시 탭을 누릅니다.
4. 캐싱 사용 확인란을 선택합니다.
5. 적용을 누릅니다.

S/MIME 애플릿이 다운로드된 후에도 사용자는 이 애플릿을 인식하지 못합니다. 이 애플릿에는 Communications Express Mail에서 메일 서명, 암호화 또는 해독을 수행한다는 것이 표시됩니다. 또한 사용자는 오류 메시지가 나타나지 않는 한 개인 또는 공개 키 확인 프로세스를 인식하지 못합니다. 자세한 내용은 705페이지의 "개인 및 공개 키 확인"을 참조하십시오.

## 기본 S/MIME 구성

S/MIME의 구성 파일인 `smime.conf`에는 각 S/MIME 매개 변수에 대한 설명 주석과 예가 들어 있습니다. `smime.conf` 파일은 Messaging Server의 `msg-svr-base/config/` 디렉토리에 있습니다. 여기서 `msg-svr-base`는 Messaging Server가 설치된 디렉토리입니다.

다음 절차에는 S/MIME 기능을 구성하는 데 필요한 최소한의 단계가 포함되어 있습니다.

1. Messaging Server를 설치한 후 Communications Express Mail의 기본 기능이 작동하고 있는지 확인합니다.
2. 아직 없는 경우, S/MIME 기능을 사용할 권한이 있는 모든 메일 사용자에게 대해 표준 X.509 v3 형식의 인증서와 함께 개인 공개 키 쌍을 만들거나 얻습니다.
3. 키와 인증서를 위해 스마트 카드를 사용할 경우
  - a. 스마트 카드를 메일 사용자에게 배포합니다.



- b. Communications Express Mail에 액세스하는 각 클라이언트 시스템에 스마트 카드 판독 장치와 소프트웨어를 올바르게 설치합니다.
- 4. 브라우저의 로컬 키 저장소를 사용하여 키와 인증서를 저장할 경우 키 쌍과 인증서를 로컬 키 저장소에 다운로드하는 방법을 메일 사용자에게 알려줍니다.
- 5. 스마트 카드나 로컬 키 저장소를 지원하려면 올바른 라이브러리가 클라이언트 시스템에 있어야 합니다. 자세한 내용은 703페이지의 "클라이언트 시스템의 키 액세스 라이브러리"를 참조하십시오.
- 6. S/MIME을 지원하도록 LDAP 디렉토리를 설정합니다.

- a. CA의 모든 인증서를 인증 기관의 고유 이름을 사용하여 Directory Server가 액세스할 수 있는 LDAP 디렉토리에 저장합니다. 이러한 인증서의 LDAP 속성은 cacertificate;binary입니다. 인증서를 저장한 디렉토리 정보를 기록해 둡니다. 이후의 단계에서 이 정보가 필요합니다.

LDAP 디렉토리 정보를 지정하는 예는 700페이지의 "trustedurl"을, LDAP 디렉토리 검색에 대한 자세한 내용은 712페이지의 "인증서 관리"를 참조하십시오.

- b. Directory Server가 액세스할 수 있는 LDAP 디렉토리에 공개 키와 인증서를 저장합니다. 공개 키와 인증서에 대한 LDAP 속성은 usercertificate;binary입니다. 공개 키와 인증서를 저장한 디렉토리에 대한 정보를 기록해 둡니다. 이후의 단계에서 이 정보가 필요합니다.

LDAP 디렉토리 정보를 지정하는 예는 695페이지의 "certurl"을, LDAP 디렉토리 검색에 대한 자세한 내용은 712페이지의 "인증서 관리"를 참조하십시오.

- c. S/MIME 메일을 주고받는 모든 사용자에게 자신의 사용자 항목에서 LDAP 필터와 함께 S/MIME을 사용할 수 있는 권한이 주어졌는지 확인합니다. 필터는 mailAllowedServiceAccess 또는 mailDomainAllowedServiceAccess LDAP 속성을 사용하여 정의합니다.

**주:** 기본적으로 mailAllowedServiceAccess 또는 mailDomainAllowedServiceAccess를 사용하지 않은 경우 smime를 비롯한 모든 서비스가 허용됩니다. 이러한 속성에 서비스를 명시적으로 지정할 경우 메일 사용자에게 S/MIME 기능을 사용할 수 있는 권한을 제공하려면 smime뿐만 아니라 http 및 smtp 서비스도 지정해야 합니다.

자세한 내용은 711페이지의 "S/MIME 기능을 사용할 수 있는 권한 부여"를 참조하십시오.

7. 사용 가능한 텍스트 편집기를 사용하여 `smime.conf` 파일을 편집합니다. 매개 변수 구문은 이 파일의 시작 부분에 있는 주석을 참조하십시오.

`smime.conf`의 모든 텍스트와 매개 변수 예는 주석 문자(#)로 시작됩니다. 필요한 매개 변수를 `smime.conf`에 추가하거나 매개 변수 예들 파일의 다른 부분에 복사하고 해당 값을 변경할 수 있습니다. 예를 복사하여 편집할 경우 행의 시작 부분에 있는 # 문자를 제거해야 합니다.

다음 매개 변수를 각각 하나의 행으로 파일에 추가합니다.

- a. `trustedurl` -- CA의 인증서를 찾기 위한 LDAP 디렉토리 정보로 설정합니다. [6a](#)에서 저장한 정보를 사용합니다.
- b. `certurl` -- 공개 키와 인증서를 찾기 위한 LDAP 디렉토리 정보로 설정합니다. [6b](#)에서 저장한 정보를 사용합니다.

- c. `usercertfilter` -- `smime.conf` 파일의 값 예로 설정합니다. 대부분의 경우 값 예를 사용하면 됩니다. 예를 복사하고 행의 시작 부분에서 # 문자를 삭제합니다.

이 매개 변수는 키 쌍을 다른 메일 주소에 할당할 때 사용자의 모든 개인 공개 키 쌍을 찾을 수 있도록 **Communications Express Mail** 사용자의 주, 대체 및 이와 동일한 전자 메일 주소에 대한 필터 정의를 지정합니다.

- d. `sslrootcacertsurl` -- S/MIME 애플릿과 Messaging Server 사이의 통신 연결에 SSL을 사용하는 경우 Messaging Server의 SSL 인증서를 확인하는 데 사용되는 CA의 인증서를 찾기 위해 LDAP 디렉토리 정보와 함께 `sslrootcacertsurl`을 설정합니다. 자세한 내용은 [702페이지의 "SSL을 사용하여 인터넷 연결 보안"](#)을 참조하십시오.

`checkoverssl` -- S/MIME 애플릿과 Messaging Server 사이의 통신 연결에 SSL을 사용하지 않을 경우 0으로 설정합니다.

- e. `crlenable` -- CRL 확인을 수행하려면 `smime.conf` 파일에 다른 매개 변수를 추가해야 하므로 지금은 0으로 설정하여 CRL 확인을 비활성화합니다.
- f. `logindn` 및 `loginpw` -- 공개 키 및 CA 인증서가 포함된 LDAP 디렉토리에 액세스하기 위해 인증이 필요한 경우 이러한 매개 변수를 읽기 권한을 가진 LDAP 항목의 고유 이름과 비밀번호로 설정합니다.

주: `certurl`, `crlmappingurl`, `sslrootcacertsurl` 또는 `trustedurl` 매개 변수에 지정된 LDAP 정보를 사용하여 LDAP 디렉토리에 액세스할 때마다 `logindn` 및 `loginpw`의 값이 사용됩니다. 자세한 내용은 693페이지의 "자격 증명을 사용하여 LDAP에서 공개 키, CA 인증서 및 CRL 액세스"를 참조하십시오.

LDAP 디렉토리에 액세스하는 데 인증이 필요하지 않은 경우 `logindn` 및 `loginpw`를 설정하지 마십시오.

8. `configutil`을 사용하여 Messaging Server 옵션을 설정합니다.
  - a. `local.webmail.smime.enable` -- 1로 설정합니다.
  - b. `local.webmail.cert.enable` -- CRL에 대해 인증서를 확인하려는 경우 1로 설정합니다.  
 자세한 내용은 701페이지의 "Messaging Server 옵션"을 참조하십시오.
9. 이제 Communications Express Mail이 S/MIME 기능을 사용하도록 구성되었습니다. 다음 단계를 수행하여 S/MIME 기능이 작동하는지 확인합니다.
  - a. Messaging Server를 다시 시작합니다.
  - b. Messaging Server 로그 파일 `msg-svr-base/log/http`에서 S/MIME과 관련된 진단 메시지를 확인합니다.
  - c. S/MIME에 대한 문제가 감지된 경우 진단 메시지를 통해 구성 매개 변수의 문제를 수정하는 방법을 확인할 수 있습니다.
  - d. 필요한 구성 매개 변수를 수정합니다.
  - e. Messaging Server의 로그 파일에 S/MIME에 대한 진단 메시지가 더 이상 존재하지 않을 때까지 단계 a~d까지 반복합니다.
  - f. 다음 단계를 수행하여 S/MIME 기능이 작동하는지 확인합니다.
    - I. 클라이언트 시스템에서 Messaging Server에 로그인합니다. S/MIME 애플릿에 대한 특수 프롬프트에 Yes 또는 Always로 대답합니다. 자세한 내용은 712페이지의 "인증서 관리"를 참조하십시오.
    - II. 자신에게 보내는 짧은 메일을 작성합니다.
    - III. 작성 창의 맨 아래에서 암호화 확인란을 선택하여(선택되어 있지 않은 경우) 메일을 암호화합니다.
    - IV. 보내기를 눌러 암호화된 메일을 자신에게 보냅니다. 이때 키와 인증서 기법이 대부분 작동해야 합니다.

- V. 암호화된 메일에 문제가 있을 경우 대개 `smime.conf` 파일의 LDAP 디렉토리 정보에 사용한 값이나 LDAP 디렉토리에 키와 인증서가 저장된 방법에 문제의 원인이 있을 수 있습니다. Messaging Server 로그에서 추가 진단 메시지를 확인합니다.

표 20-3에 요약되어 있는 나머지 S/MIME 매개 변수는 S/MIME 환경을 추가로 구성하는데 사용할 수 있는 여러 옵션을 제공합니다. 매개 변수에 대한 자세한 내용은 694페이지의 "smime.conf 파일의 매개 변수"를 참조하십시오.

**표 20-3** smime.conf 매개 변수 요약

| S/MIME의 필수 매개 변수             | 스마트 카드 및 로컬 키 저장소를 위한 매개 변수 | CRL 확인을 위한 매개 변수                    | 초기 설정 및 보안 연결을 위한 매개 변수        |
|------------------------------|-----------------------------|-------------------------------------|--------------------------------|
| <code>certurl*</code>        | <code>-p pattern</code>     | <code>checkoverssl</code>           | <code>alwaysencrypt</code>     |
| <code>logindn</code>         |                             | <code>crlaccessfail</code>          | <code>alwaysign</code>         |
| <code>loginpw</code>         |                             | <code>crlidir</code>                | <code>sslrootcacertsurl</code> |
| <code>trustedurl*</code>     |                             | <code>crlenable</code>              |                                |
| <code>usercertfilter*</code> |                             | <code>crlmappingurl</code>          |                                |
|                              |                             | <code>crlurllogindn</code>          |                                |
|                              |                             | <code>crlurlloginpw</code>          |                                |
|                              |                             | <code>crlusepastnextupdate</code>   |                                |
|                              |                             | <code>readsigncert</code>           |                                |
|                              |                             | <code>revocationunknown</code>      |                                |
|                              |                             | <code>sendencryptcert</code>        |                                |
|                              |                             | <code>sendencryptcertrevoked</code> |                                |
|                              |                             | <code>readsigncert</code>           |                                |
|                              |                             | <code>sendsigncertrevoked</code>    |                                |
|                              |                             | <code>timestampdelta</code>         |                                |

\* 이러한 매개 변수에는 기본값이 없기 때문에 값을 지정해야 합니다.

## 자격 증명을 사용하여 LDAP에서 공개 키, CA 인증서 및 CRL 액세스

S/MIME에 필요한 공개 키, CA 인증서 및 CRL을 LDAP 디렉토리에 저장할 수 있습니다 (앞의 절 참조). 키, 인증서 및 CRL은 LDAP의 단일 URL 또는 여러 URL에서 액세스할 수 있습니다. 예를 들어, CRL을 하나의 URL에 저장하고 공개 키와 인증서를 다른 URL에 저장할 수 있습니다. Messaging Server에서는 원하는 CRL이나 인증서 정보를 포함하는 URL과 이러한 URL에 액세스할 수 있는 항목의 DN 및 비밀번호를 지정할 수 있습니다. 이러한 DN/비밀번호 자격 증명은 선택 사항입니다. 아무 것도 지정하지 않을 경우 먼저 HTTP 서버 자격 증명으로 LDAP 액세스를 시도하고 이것이 실패할 경우 anonymous로 액세스를 시도합니다.

두 쌍의 smime.conf 자격 증명 매개 변수, 즉 loginDN 및 loginPW와 cURLloginDN 및 cURLloginPW를 설정하여 원하는 URL에 액세스할 수 있습니다.

loginDN 및 loginPW는 smime.conf의 모든 URL에 사용되는 자격 증명입니다. 이러한 매개 변수는 certURL 및 trustedURL 매개 변수에 지정된 공개 키, 해당 인증서 및 CA 인증서에 대한 읽기 권한이 있는 LDAP 항목의 DN과 비밀번호를 지정합니다.

cURLloginDN 및 cURLloginPW는 매핑 테이블의 결과 URL에 대한 읽기 권한이 있는 LDAP 항목의 DN과 비밀번호를 지정합니다(자세한 내용은 706페이지의 "CRL 액세스" 참조). 이러한 자격 증명이 허용되지 않을 경우 LDAP 액세스가 거부되며 다른 자격 증명으로 다시 시도되지 않습니다. 두 매개 변수를 모두 지정하거나 둘 다 비워두어야 합니다. 이러한 매개 변수는 인증서로부터 직접 가져온 URL에는 적용되지 않습니다.

### 특정 URL의 비밀번호 설정

Messaging Server에서는 smime.conf URL(certURL, trustedURL, cURLmappingURL 및 sslrootcacertsURL)에 액세스하기 위한 DN/비밀번호 쌍을 명시적으로 정의할 수 있습니다.

구문은 다음과 같습니다.

```
url_type    URL[|URL_DN|URL_password]
```

예:

```
trustedurl==ldap://mail.siroe.com:389/cn=Directory Manager, ou=people,
o=siroe.com,o=ugroot?cacertificate?sub?(objectclass=certificationauthority
) | cn=Directory manager | boomshakalaka
```

## LDAP 자격 증명 사용 요약

이 절에서는 LDAP 자격 증명의 사용에 대해 요약합니다.

- 모든 LDAP 자격 증명은 선택 사항입니다. 아무 것도 지정하지 않을 경우 먼저 HTTP 서버 자격 증명으로 LDAP 액세스를 시도하고 이것이 실패할 경우 anonymous 액세스를 시도합니다.

두 쌍의 smime.conf 매개 변수를 지정할 수 있는 두 개의 URL 집합에 대한 자격 증명으로 사용합니다.

logindn 및 loginpw - smime.conf의 모든 URL

crlurllogindn 및 crlurlloginpw - 매핑 테이블의 모든 URL

이것들을 기본 LDAP 자격 증명 쌍이라고 합니다.

- smime.conf 또는 매핑 CRL URL을 통해 지정된 모든 URL에 선택적 로컬 LDAP 자격 증명 쌍을 지정할 수 있습니다.
- 자격 증명은 지정된 순서대로 확인됩니다.
  - 1) 로컬 LDAP 자격 증명 쌍 - 지정된 경우 한 번만 시도됩니다.
  - 2) 기본 LDAP 자격 증명 쌍 - 지정된 경우 로컬 LDAP 자격 증명 쌍이 없으면 한 번만 시도됩니다.
  - 3) 서버 - 로컬 LDAP 자격 증명 쌍과 기본 LDAP 자격 증명 쌍이 모두 지정되지 않은 경우 처음으로 시도됩니다.
  - 4) anonymous - 서버가 실패하거나 아무 것도 지정하지 않은 경우에만 마지막에 시도됩니다.
- URL에 로컬 LDAP 자격 증명 쌍이 지정된 경우 이 자격 증명 쌍이 처음에 사용됩니다. 액세스에 실패하면 액세스가 거부됩니다.
- URL에 로컬 LDAP 자격 증명 쌍이 지정되지 않은 경우 해당하는 기본 LDAP 자격 증명 쌍이 사용됩니다. 액세스에 실패하면 액세스가 거부됩니다.

## smime.conf 파일의 매개 변수

smime.conf 파일은 Messaging Server의 *msg-svr-base/config/* 디렉토리에 있습니다. 여기서 *msg-svr-base*는 Messaging Server가 설치된 디렉토리입니다. 이 파일의 모든 텍스트 및 매개 변수 예는 주석 문자(#)로 시작됩니다.

매개 변수를 원하는 값과 함께 smime.conf에 추가하거나 매개 변수 예를 편집할 수 있습니다. 예를 사용할 경우 파일의 다른 부분에 예를 복사하고 매개 변수의 값을 편집한 다음 행의 시작 부분에 있는 # 문자를 제거합니다.

Messaging Server를 설치한 후에 사용 가능한 텍스트 편집기를 사용하여 smime.conf를 편집합니다. 표 20-4에 설명된 매개 변수는 대소문자를 구분하지 않으며 다른 언급이 없는 한 설정할 필요가 없습니다.

**표 20-4** smime.conf 파일의 S/MIME 구성 매개 변수

| 매개 변수        | 용도                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|--------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| alwayencrypt | <p>S/MIME을 사용할 권한이 있는 모든 Communications Express Mail 사용자에게 대해 모든 보내는 메일을 자동으로 암호화할 것인지 여부에 대한 초기 설정을 제어합니다. 각 Communications Express Mail 사용자는 720페이지의 표 20-6에 설명된 확인란을 사용하여 자신의 메일에 대해 이 매개 변수 값을 무시할 수 있습니다.</p> <p>다음 값 중 하나를 선택합니다.</p> <p>0 - 메일을 암호화하지 않습니다. Communications Express Mail 내의 암호화 확인란이 선택되지 않은 상태로 표시됩니다. 기본값입니다.</p> <p>1 - 메일을 항상 암호화합니다. Communications Express Mail 내의 암호화 확인란이 선택된 상태로 표시됩니다.</p> <p>예:</p> <pre>alwayencrypt==1</pre>                                               |
| alwayssign   | <p>S/MIME을 사용할 권한이 있는 모든 Communications Express Mail 사용자에게 대해 모든 보내는 메일을 자동으로 서명할 것인지 여부에 대한 초기 설정을 제어합니다. 각 Communications Express Mail 사용자는 720페이지의 표 20-6에 설명된 확인란을 사용하여 자신의 메일에 대해 이 매개 변수 값을 무시할 수 있습니다.</p> <p>다음 값 중 하나를 선택합니다.</p> <p>0 - 메일에 서명하지 않습니다. Communications Express Mail 내의 서명 확인란이 선택되지 않은 상태로 표시됩니다. 기본값입니다.</p> <p>1 - 메일에 항상 서명합니다. Communications Express Mail 내의 서명 확인란이 선택된 상태로 표시됩니다.</p> <p>예:</p> <pre>alwayssign==1</pre>                                                      |
| certurl      | <p>Communications Express Mail 사용자의 공개 키와 인증서를 찾기 위한 LDAP 디렉토리 정보를 지정합니다(공개 키의 LDAP 속성은 usercertificate;binary임). 인증서에 대한 자세한 내용은 712페이지의 "인증서 관리"를 참조하십시오.</p> <p>이 매개 변수는 Messaging Server에 의해 서비스되는 모든 사용자가 포함된 LDAP 디렉토리 정보 트리(DIT)의 사용자/그룹에서 최상위 노드를 가리켜야 합니다. 이러한 점은 특히 도메인이 둘 이상인 사이트의 경우 중요합니다. 고유 이름이 단일 도메인의 사용자를 포함하는 하위 트리가 아니라 사용자/그룹 트리의 루트 고유 이름이어야 합니다.</p> <p>이 매개 변수는 반드시 설정해야 하는 필수 매개 변수입니다.</p> <p>예:</p> <pre>certurl==ldap://mail.siroe.com:389/ou=people, o=siroe.com, o=ugroot</pre> |

**표 20-4** smime.conf 파일의 S/MIME 구성 매개 변수(계속)

| 매개 변수         | 용도                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| checkoverssl  | <p>CRL에 대해 키의 인증서를 확인할 때 SSL 통신 연결을 사용하는지 여부를 제어합니다. 자세한 내용은 <a href="#">702페이지의 "SSL을 사용하여 인터넷 연결 보안"</a>을 참조하십시오.</p> <p>다음 값 중 하나를 선택합니다.</p> <p>0 - SSL 통신 연결을 사용하지 않습니다.</p> <p>1 - SSL 통신 연결을 사용합니다. 기본값입니다.</p> <p>CRL 확인이 유효한 상태에서 프록시 서버를 사용하면 문제가 발생할 수 있습니다. 자세한 내용은 <a href="#">708페이지의 "프록시 서버 및 CRL 확인"</a>을 참조하십시오.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| crlaccessfail | <p>Messaging Server가 CRL 액세스를 여러 번 시도했다가 실패한 후에 CRL 액세스를 다시 시도하기까지 기다리는 시간을 지정합니다. 이 매개 변수에는 기본값이 없습니다.</p> <p><b>구문:</b></p> <pre>crlaccessfail==number_of_failures:time_period_for_failures:wait_time_before_retry</pre> <p>여기서</p> <p><i>number_of_failures</i>는 Messaging Server가 <i>time_period_for_failures</i>에 지정된 시간 간격 동안 CRL 액세스에 실패할 수 있는 횟수입니다. 값이 0보다 커야 합니다.</p> <p><i>time_period_for_failures</i>는 Messaging Server가 CRL 액세스 시도에 실패한 횟수를 계산하는 시간(초)입니다. 값이 0보다 커야 합니다.</p> <p><i>wait_time_before_retry</i>는 Messaging Server가 지정된 간격 동안 제한된 실패 횟수에 도달한 후에 CRL에 다시 액세스하려고 시도하기까지 대기하는 시간(초)입니다. 값이 0보다 커야 합니다.</p> <p>예:</p> <pre>crlaccessfail==10:60:300</pre> <p>이 예에서 Messaging Server는 1분 동안 10번까지 CRL 액세스에 실패할 수 있습니다. 그런 다음 5분을 기다렸다가 CRL 액세스를 다시 시도합니다. 자세한 내용은 <a href="#">710페이지의 "CRL 액세스 문제"</a>를 참조하십시오.</p> |
| crlmdir       | <p>Messaging Server가 CRL을 디스크에 다운로드하는 디렉토리 정보를 지정합니다. 기본 값은 <i>msg-svr-base/data/store/mboxlist</i>입니다. 여기서 <i>msg-svr-base</i>는 Messaging Server가 설치된 디렉토리입니다. 자세한 내용은 <a href="#">708페이지의 "오래된 CRL 사용"</a>을 참조하십시오.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| crlenable     | <p>CRL에 대해 인증서를 확인하는지 여부를 제어합니다. CRL에 일치하는 것이 있을 경우 인증서가 해지된 것입니다. smime.conf 파일의 send*revoked 매개 변수 값은 해지된 인증서가 있는 키를 Communications Express Mail이 거부하는지 아니면 사용하는지 여부를 지정합니다. 자세한 내용은 <a href="#">705페이지의 "개인 및 공개 키 확인"</a>을 참조하십시오.</p> <p>다음 값 중 하나를 선택합니다.</p> <p>0- 각 인증서를 CRL에 대해 확인하지 않습니다.</p> <p>1- 각 인증서를 CRL에 대해 확인합니다. 기본값입니다. Messaging Server의 local.webmail.cert.enable 옵션이 1로 설정되었는지 확인합니다. 그렇지 않으면 crlenable을 1로 설정하는 경우에도 CRL 확인이 수행됩니다.</p>                                                                                                                                                                                                                                                                                                                                                                            |



**표 20-4** smime.conf 파일의 S/MIME 구성 매개 변수(계속)

| 매개 변수               | 용도                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|---------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| crlmappingurl       | <p>CRL 매핑 정의를 찾기 위한 LDAP 디렉토리 정보를 지정합니다. 이 매개 변수는 매핑 정의가 있는 경우에만 필요합니다. 자세한 내용은 706페이지의 "CRL 액세스"를 참조하십시오. 이 매개 변수에는 기본값이 없습니다. 또한 URL에 액세스할 수 있는 DN과 비밀번호를 추가할 수도 있습니다.</p> <p>구문:</p> <pre>crlmappingurl URL [URL_DN   URL_password]</pre> <p>예:</p> <pre>crlmappingurl==ldap://mail.siroe.com:389/cn=XYZ Messaging, ou=people, o=mail.siroe.com,o=isp?msgCRLMappingRecord?sub?(objectclass=msg CRLMappingTable) cn=Directory Manager   pAsSwOrD</pre> |
| crlurllogin         | <p>CRL 매핑 정의에 대한 읽기 권한을 가진 LDAP 항목의 고유 이름을 지정합니다. 항목을 인증서에서 직접 가져올 경우에는 지정하지 않습니다. 자세한 내용은 904페이지의 "CRL 액세스"를 참조하십시오.</p> <p>crllogindn 및 crlloginpw의 값을 지정하지 않을 경우 Messaging Server는 HTTP 서버의 로그인 값을 사용하여 LDAP 디렉토리에 액세스합니다. 액세스에 실패할 경우 Messaging Server는 LDAP 디렉토리에 익명으로 액세스를 시도합니다.</p> <p>예:</p> <pre>crllogindn==cn=Directory Manager</pre>                                                                                                        |
| crlurlloginpw       | <p>crllogindn 매개 변수의 고유 이름에 대한 비밀번호를 ASCII 텍스트로 지정합니다.</p> <p>crllogindn 및 crlloginpw의 값을 지정하지 않을 경우 Messaging Server는 HTTP 서버의 로그인 값을 사용하여 LDAP 디렉토리에 액세스합니다. 액세스에 실패할 경우 Messaging Server는 LDAP 디렉토리에 익명으로 액세스를 시도합니다.</p> <p>예:</p> <pre>crlloginpw==zippy</pre>                                                                                                                                                                                      |
| crusepastnextupdate | <p>현재 날짜가 CRL의 next-update 필드에 지정된 날짜 이후인 경우에 CRL을 사용할지 여부를 제어합니다. 자세한 내용은 708페이지의 "오래된 CRL 사용"을 참조하십시오.</p> <p>다음 값 중 하나를 선택합니다.</p> <p>0 - 오래된 CRL을 사용하지 않습니다.</p> <p>1 - 오래된 CRL을 사용합니다. 기본값입니다.</p>                                                                                                                                                                                                                                                  |

**표 20-4** smime.conf 파일의 S/MIME 구성 매개 변수(계속)

| 매개 변수             | 용도                                                                                                                                                                                                                                                                                                                             |
|-------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| logindn           | <p>certurl 및 trustedurl 매개 변수에 지정된 LDAP 디렉토리에 있는 공개 키 및 해당 인증서와 CA 인증서에 대한 읽기 권한을 가진 LDAP 항목의 고유 이름을 지정합니다.</p> <p>logindn 및 loginpw의 값을 지정하지 않을 경우 Messaging Server는 HTTP 서버의 로그인 값을 사용하여 LDAP 디렉토리에 액세스합니다. 액세스에 실패할 경우 Messaging Server는 LDAP 디렉토리에 익명으로 액세스를 시도합니다.</p> <p>예:</p> <pre>logindn==cn=Directory Manager</pre> |
| loginpw           | <p>logindn 매개 변수의 고유 이름에 대한 비밀번호를 ASCII 텍스트로 지정합니다.</p> <p>logindn 및 loginpw의 값을 지정하지 않을 경우 Messaging Server는 HTTP 서버의 로그인 값을 사용하여 LDAP 디렉토리에 액세스합니다. 액세스에 실패할 경우 Messaging Server는 LDAP 디렉토리에 익명으로 액세스를 시도합니다.</p> <p>예:</p> <pre>loginpw==SkyKing</pre>                                                                      |
| -p pattern        | <p>Windows 플랫폼에서 스마트 카드나 로컬 키 저장소를 사용할 때 필요한 하나 이상의 라이브러리 이름을 지정합니다. 클라이언트 시스템에서 기본값이 작동하지 않을 경우에만 이 매개 변수를 변경합니다. 기본값은 다음과 같습니다.</p> <pre>platformwin==CAPI:library=capibridge.dll;</pre> <p>자세한 내용은 703페이지의 "클라이언트 시스템의 키 액세스 라이브러리"를 참조하십시오.</p>                                                                            |
| readsigncert      | <p>메시지를 읽을 때 S/MIME 디지털 서명을 확인하기 위해 공개 키의 인증서를 CRL에 대해 확인할지 여부를 제어합니다. 메일의 디지털 서명을 만들기 위해 개인 키가 사용되지만 개인 키를 CRL에 대해 확인할 수 없습니다. 따라서 개인 키와 연관된 공개 키의 인증서가 CRL에 대해 확인됩니다. 자세한 내용은 705페이지의 "개인 및 공개 키 확인"을 참조하십시오.</p> <p>다음 값 중 하나를 선택합니다.</p> <p>0 - 인증서를 CRL에 대해 확인하지 않습니다.</p> <p>1 - 인증서를 CRL에 대해 확인합니다. 기본값입니다.</p>         |
| revocationunknown | <p>인증서를 CRL에 대해 확인할 때 모호한 상태가 반환될 경우 수행할 작업을 지정합니다. 이 경우에 인증서가 유효한지 아니면 해지된 상태인지는 확실하지 않습니다. 자세한 내용은 705페이지의 "개인 및 공개 키 확인"을 참조하십시오.</p> <p>다음 값 중 하나를 선택합니다.</p> <p>ok - 인증서를 유효한 것으로 간주합니다.</p> <p>revoked - 인증서를 해지된 것으로 간주합니다. 기본값입니다.</p>                                                                                 |

**표 20-4** smime.conf 파일의 S/MIME 구성 매개 변수(계속)

| 매개 변수                  | 용도                                                                                                                                                                                                                                                                                                                                                     |
|------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| sendencryptcert        | <p>보내는 메일을 암호화하는 데 사용되는 공개 키의 인증서를 사용 전에 CRL에 대해 확인하는지 여부를 제어합니다. 자세한 내용은 <a href="#">705페이지의 "개인 및 공개 키 확인"</a>을 참조하십시오.</p> <p>다음 값 중 하나를 선택합니다.</p> <p>0 - 인증서를 CRL에 대해 확인하지 않습니다.</p> <p>1 - 인증서를 CRL에 대해 확인합니다. 기본값입니다.</p>                                                                                                                       |
| sendencryptcertrevoked | <p>보내는 메일을 암호화하는 데 사용되는 공개 키의 인증서가 해지된 경우 수행할 작업을 지정합니다. 자세한 내용은 <a href="#">705페이지의 "개인 및 공개 키 확인"</a>을 참조하십시오.</p> <p>다음 값 중 하나를 선택합니다.</p> <p>allow - 공개 키를 사용합니다.</p> <p>disallow - 공개 키를 사용하지 않습니다. 기본값입니다.</p>                                                                                                                                   |
| sendsigncert           | <p>개인 키를 사용하여 보내는 메일의 디지털 서명을 만들 수 있는지 여부를 결정하기 위해 공개 키의 인증서를 CRL에 대해 확인하는지 여부를 제어합니다. 디지털 서명에 대해 개인 키가 사용되지만 개인 키를 CRL에 대해 확인할 수 없습니다. 따라서 개인 키와 연관된 공개 키의 인증서를 CRL에 대해 확인합니다. 자세한 내용은 <a href="#">705페이지의 "개인 및 공개 키 확인"</a>을 참조하십시오.</p> <p>다음 값 중 하나를 선택합니다.</p> <p>0 - 인증서를 CRL에 대해 확인하지 않습니다.</p> <p>1 - 인증서를 CRL에 대해 확인합니다. 기본값입니다.</p>         |
| sendsigncertrevoked    | <p>개인 키가 해지된 상태인 것으로 확인되었을 때 수행할 작업을 결정합니다. 메일의 디지털 서명을 만들 때 개인 키가 사용되지만 개인 키를 CRL에 대해 확인할 수는 없습니다. 따라서 개인 키와 연관된 공개 키의 인증서를 CRL에 대해 확인합니다. 공개 키 인증서가 해지되면 해당 개인 키도 해지됩니다. 자세한 내용은 <a href="#">705페이지의 "개인 및 공개 키 확인"</a>을 참조하십시오.</p> <p>다음 값 중 하나를 선택합니다.</p> <p>allow - 해지된 상태의 개인 키를 사용합니다.</p> <p>disallow - 해지된 상태의 개인 키를 사용하지 않습니다. 기본값입니다.</p> |

**표 20-4** smime.conf 파일의 S/MIME 구성 매개 변수(계속)

| 매개 변수             | 용도                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| sslrootcacertsurl | <p>Messaging Server의 SSL 인증서를 확인하는 데 사용되는 유효한 CA의 인증서를 찾기 위한 고유 이름과 LDAP 디렉토리 정보를 지정합니다. Messaging Server에서 SSL이 활성화된 경우 이 매개 변수를 반드시 지정해야 합니다. 자세한 내용은 <a href="#">702페이지의 "SSL을 사용하여 인터넷 연결 보안"</a>을 참조하십시오.</p> <p>클라이언트 응용 프로그램에서 모든 요청을 수신하는 프록시 서버에 대한 SSL 인증서가 있을 경우 이러한 SSL 인증서에 대한 CA 인증서도 이 매개 변수가 가리키는 LDAP 디렉토리에 있습니다.</p> <p>또한 이 URL에 액세스할 수 있는 DN과 비밀번호를 추가할 수도 있습니다.</p> <p>구문:</p> <pre>crlmappingurl URL[ URL_DN URL_password]</pre> <p>예:</p> <pre>sslrootcacertsurl==ldap://mail.siroe.com:389/cn=SSL Root CA Certificates, ou=people, o=siroe.com, o=isp? cacertificate;binary?base? (objectclass=certificationauthority) cn=Directory Manager   pAsSwOrD</pre> |
| timestampdelta    | <p>공개 키의 인증서를 CRL에 대해 확인할 때 메일의 보낸 시간이나 받은 시간을 사용할지를 결정하는 데 사용되는 시간 간격(초)을 지정합니다.</p> <p>기본값인 0은 Communications Express Mail에서 항상 받은 시간을 사용하도록 지시합니다. 자세한 내용은 <a href="#">709페이지의 "사용할 메일 시간 지정"</a>을 참조하십시오.</p> <p>예:</p> <pre>timestampdelta==360</pre>                                                                                                                                                                                                                                                                                                                                                                                                                           |
| trustedurl        | <p>유효한 CA의 인증서를 찾기 위한 고유 이름과 LDAP 디렉토리 정보를 지정합니다. 필수 매개 변수입니다.</p> <p>또한 이 URL에 액세스할 수 있는 DN과 비밀번호를 추가할 수도 있습니다.</p> <p>구문:</p> <pre>crlmappingurl URL[ URL_DN URL_password]</pre> <p>예:</p> <pre>trustedurl==ldap://mail.siroe.com:389/cn=Directory Manager, ou=people, o=siroe.com,o=ugroot?cacertificate?sub?(objectclass=certificati onauthority) cn=Directory Manager   pAsSwOrD</pre>                                                                                                                                                                                                                                                                                          |
| usercertfilter    | <p>키 쌍을 다른 메일 주소에 할당할 때 사용자의 모든 개인 공개 키 쌍을 찾을 수 있도록 Communications Express Mail 사용자의 주, 대체 및 이와 동일한 전자 메일 주소에 대한 필터 정의를 지정합니다.</p> <p>이 매개 변수는 필수이며 기본값이 없습니다.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

# Messaging Server 옵션

S/MIME에 적용되는 세 가지 Messaging Server 옵션을 설정하려면 Messaging Server가 설치된 시스템에서 다음 작업을 수행합니다.

1. 루트로 로그인하여 다음을 입력합니다.

```
# cd msg-svr-base/sbin
```

여기서 *msg-svr-base*는 Messaging Server가 설치된 디렉토리입니다.

2. 다음 표에 설명된 Messaging Server 옵션을 시스템에 맞게 설정합니다. `configutil` 유틸리티를 사용하여 이러한 옵션을 설정합니다. 별도의 언급이 없을 경우 옵션을 설정할 필요가 없습니다.

| 매개 변수                                   | 용도                                                                                                                                                                                                                                                                                                                                                         |
|-----------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>local.webmail.cert.enable</code>  | <p>CRL 확인을 처리하는 프로세스가 CRL 확인을 수행해야 하는지 여부를 제어합니다.</p> <p>0 - 프로세스가 인증서를 CRL에 대해 확인하지 않습니다. 기본값입니다.</p> <p>1 - 프로세스가 인증서를 CRL에 대해 확인합니다. 1로 설정할 경우 <code>smime.conf</code> 파일의 <code>crleenable</code> 매개 변수가 1로 설정되었는지 확인합니다.</p>                                                                                                                          |
| <code>local.webmail.cert.port</code>    | <p>CRL 통신에 사용할 Messaging Server가 실행되는 시스템의 포트 번호를 지정합니다. 이 포트는 해당 시스템에서 대해서만 로컬로 사용됩니다. 값은 1024보다 커야 하며 기본값은 55443입니다.</p> <p>기본 포트 번호가 이미 사용 중이면 이 옵션을 반드시 지정해야 합니다.</p>                                                                                                                                                                                  |
| <code>local.webmail.smime.enable</code> | <p>Communications Express Mail 사용자가 S/MIME 기능을 사용할 수 있는지 여부를 제어합니다. 다음 값 중 하나를 선택합니다.</p> <p>0 - 시스템이 올바른 소프트웨어 및 하드웨어 구성 요소로 구성된 경우에도 Communications Express Mail 사용자가 S/MIME 기능을 사용할 수 없습니다. 기본값입니다.</p> <p>1 - 사용 권한이 있는 Communications Express Mail 사용자가 S/MIME 기능을 사용할 수 있습니다.</p> <p>예:</p> <pre>configutil -o local.webmail.smime.enable -v 1</pre> |

# SSL을 사용하여 인터넷 연결 보안

다음 표에 요약된 것처럼 Messaging Server에서는 Communications Express Mail에 영향을 주는 인터넷 연결에 SSL(Secure Socket Layer)을 사용할 수 있습니다.

| 대상 연결                                                | 설명                                                                                                                                                                                                                                                                                       |
|------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Messaging Server 및 Communications Express Mail 간의 연결 | <p>SSL을 사용하여 이 연결을 보안하려면 Messaging Server에 대한 관리 작업이 필요합니다. Communications Express Mail 사용자는 브라우저에서 Messaging Server에 대한 URL 정보를 입력할 때 HTTP가 아니라 HTTPS 프로토콜을 사용해야 합니다.</p> <p>자세한 내용은 <a href="#">702페이지의 "Messaging Server 및 Communications Express Mail 간의 연결 보안"</a>을 참조하십시오.</p>     |
| Messaging Server 및 S/MIME 애플릿 간 연결                   | <p>공개 키 인증서를 CRL에 대해 확인할 경우 S/MIME 애플릿 Messaging Server와 직접 통신해야 합니다. SSL을 사용하여 이 연결을 보안하려면 smime.conf 파일에서 sslrootcacertsurl 및 checkoverssl을 설정하는 것 외에도 Messaging Server에 대한 관리 작업이 필요합니다.</p> <p>자세한 내용은 <a href="#">703페이지의 "Messaging Server 및 S/MIME 애플릿 간의 연결 보안"</a>을 참조하십시오.</p> |

## Messaging Server 및 Communications Express Mail 간의 연결 보안

Messaging Server에서는 Messaging Server와 Communications Express Mail 간의 인터넷 연결에 SSL(Secure Socket Layer)을 사용할 수 있습니다. SSL에 대해 Messaging Server를 설치하고 나면 SSL에 대해 Communications Express를 구성하십시오.

*Communications Express 관리 설명서*(<http://docs.sun.com/doc/819-1066>)를 참조하십시오. Communications Express Mail 사용자는 브라우저에서 HTTPS 프로토콜을 사용하여 Communications Express URL을 지정합니다.

`HTTPS://hostname.domain:secured_port`

즉, HTTP 프로토콜(`HTTP://hostname.domain:unsecure_port`)을 사용하지 않습니다. Communications Express 로그인 창이 표시되면 창 아래의 잠금 위치에 보안 링크가 있음을 나타내는 잠금 아이콘이 보입니다.

Messaging Server에 대한 SSL 구성은 [649페이지의 "암호화 및 인증서 기반 인증 구성"](#) 및 *Communications Express 관리 설명서*(<http://docs.sun.com/doc/819-1066>)를 참조하십시오.

## Messaging Server 및 S/MIME 애플릿 간의 연결 보안

공개 키 인증서를 CRL에 대해 확인할 경우 S/MIME 애플릿이 Messaging Server와 직접 통신해야 합니다. SSL을 사용하여 이 통신 연결을 보안하려면 다음 작업을 수행합니다.

1. 관리 작업을 수행하여 Messaging Server에서 SSL을 구성합니다. [649페이지의 "암호화 및 인증서 기반 인증 구성"](#)을 참조하십시오.
2. `smime.conf` 파일에서 `sslrootcacertsurl` 매개 변수를 설정하여 루트 SSL CA 인증서를 찾기 위한 정보를 지정합니다. 이러한 CA 인증서는 Messaging Server와 S/MIME 애플릿 간에 SSL 연결을 설정할 때 Messaging Server의 SSL 인증서를 확인하는 데 사용됩니다.
3. `smime.conf` 파일에서 `checkoverssl` 매개 변수를 1로 설정합니다. 이 Messaging Server 옵션은 Messaging Server와 S/MIME 애플릿 간의 연결에 SSL이 사용되는지 여부를 지정합니다. `checkoverssl`을 1로 설정하면 Communications Express Mail 사용자가 Messenger Server의 URL을 지정하는 방법(HTTP 또는 HTTPS)에 상관없이 Messaging Server 및 S/MIME 애플릿 간의 연결이 SSL을 사용하여 보안됩니다.

---

**주** Messaging Server와 Communications Express Mail 등의 클라이언트 응용 프로그램 간에 프록시 서버를 사용할 수 있습니다. 프록시 서버를 보안된 통신 연결과 함께 사용하거나 보안된 통신 연결 없이 사용하는 방법은 [708페이지의 "프록시 서버 및 CRL 확인"](#)을 참조하십시오.

---

## 클라이언트 시스템의 키 액세스 라이브러리

메일 사용자가 개인 공개 키 쌍과 인증서를 스마트 카드에 보관하는지 아니면 브라우저의 로컬 키 저장소에 보관하는지 여부에 상관없이 클라이언트 시스템에는 저장 방법을 지원하기 위한 키 액세스 라이브러리가 존재해야 합니다.

이러한 라이브러리는 스마트 카드 및 브라우저 공급업체가 제공합니다. 클라이언트 시스템에 올바른 라이브러리가 있는지 확인하고 `smime.conf` 파일에서 올바른 플랫폼 매개 변수에 라이브러리 이름을 지정해야 합니다. 선택할 수 있는 매개 변수는 다음과 같습니다.

- `platformwin`(PC에서 실행 중인 Microsoft Windows의 경우)

클라이언트 시스템에 설치된 라이브러리를 알고 있는 경우 이러한 라이브러리만 지정하거나 설치된 라이브러리가 확실하지 않을 경우 특정 플랫폼과 공급업체의 모든 라이브러리 이름을 지정할 수 있습니다. S/MIME 애플릿이 지정한 이름 중에서 필요한 라이브러리를 찾지 못할 경우 S/MIME 기능이 작동하지 않습니다.

하나 이상의 라이브러리 파일 이름을 지정하는 구문은 다음과 같습니다.

```
platform_parameter==vendor:library=library_name;...
```

여기서

*platform\_parameter*는 Communications Express Mail에 액세스하는 클라이언트 시스템의 플랫폼에 대한 매개 변수 이름입니다. 다음 이름 중 하나를 선택합니다(platformwin).

*vendor*는 스마트 카드나 브라우저의 공급업체를 지정합니다. 다음 리터럴 중 하나를 선택합니다.

cac(ActivCard 또는 NetSign 스마트 카드의 경우)

capi(CAPI가 포함된 Internet Explorer의 경우)

mozilla(네트워크 보안 서비스가 포함된 Mozilla의 경우)

*library\_name* 라이브러리 파일 이름을 지정합니다. 공급업체 및 운영 체제에 대한 라이브러리 이름은 표 20-5를 참조하십시오.

**표 20-5** 클라이언트 시스템의 특수 라이브러리

| 스마트 카드 또는 브라우저 공급업체                                                          | 운영 체제   | 라이브러리 파일 이름    |
|------------------------------------------------------------------------------|---------|----------------|
|                                                                              | Windows | acpkcs211.dll  |
| CAPI(Cryptographic Application Programming Interface)가 포함된 Internet Explorer | Windows | capibridge.dll |
|                                                                              | Windows | softokn3.dll   |
|                                                                              | Windows | core32.dll     |

## 예

다음 예에서는 Windows 플랫폼에 대한 하나의 스마트 카드 라이브러리, 하나의 Internet Explorer 라이브러리 및 하나의 Mozilla 라이브러리를 지정합니다.

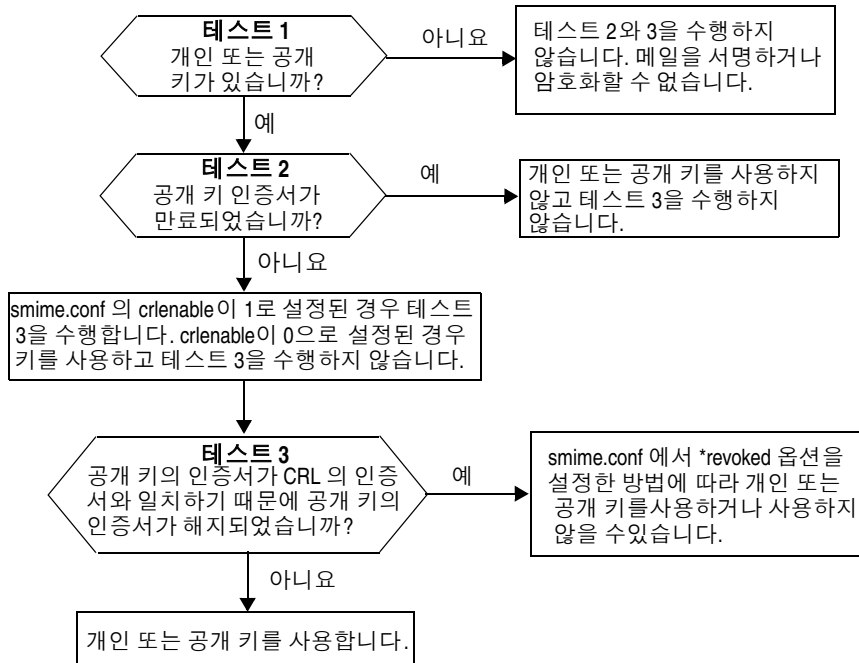
```
platformwin==CAC:library=acpkcs211.dll;CAPI:library=capibridge.dll;
MOZILLA:library=softokn3.dll;
```



## 개인 및 공개 키 확인

Communications Express Mail은 개인 또는 공개 키를 사용하기 전에 [그림 20-2](#)에 표시된 확인 테스트를 통과해야 합니다. 이 절의 나머지 부분에서는 공개 키 인증서를 CRL에 대해 확인하는 작업을 자세히 설명합니다.

**그림 20-2** 개인 및 공개 키 확인



## 사용자의 개인 또는 공개 키 찾기

Communications Express Mail 사용자가 여러 개인 공개 키 쌍과 여러 전자 메일 주소(주, 대체 또는 별칭 주소)를 갖고 있는 경우 키가 이러한 주소와 연결될 수 있습니다. 이 경우 S/MIME 애플릿이 확인을 위해 모든 키를 찾는 것이 중요합니다. smime.conf 파일에서 usercertfilter 매개 변수를 사용하여 공개 키 인증서를 CRL에 대해 확인할 때 키 소유자의 메일 주소 목록을 만드는 필터를 정의합니다. 자세한 내용은 [700페이지](#)의 "usercertfilter"를 참조하십시오.

## CRL에 대해 인증서 확인

인증서 해지 목록(CRL)은 키 쌍과 인증서를 발급하는 CA가 유지 관리하는 해지된 인증서 목록입니다. CRL 확인이 사용 가능한 경우 시스템은 인증서 요청이 있을 때마다 CRL에서 해당 인증서가 해지되었는지 확인합니다.

smime.conf 파일에서 crlenable이 1로 설정되어 있는 경우에는 만료된 키가 발견될 때 CRL 테스트가 수행됩니다. 공개 키의 인증서를 CRL에 대해 확인합니다. 각 CA에 대해 CRL이 하나만 있을 수 있지만 동일한 CRL이 여러 위치에 있을 수 있습니다.

S/MIME 애플릿이 확인을 수행하라는 요청을 보내면 Messaging Server가 인증서를 CRL에 대해 확인합니다. 공개 키 인증서는 공개 키를 검증하기 위해 사용됩니다. 개인 키는 소유자만 사용할 수 있도록 비밀로 유지되기 때문에 개인 키를 CRL에 대해 직접 확인할 수 없습니다. 따라서 개인 키가 올바른지 확인하려면 키 쌍의 공개 키 인증서가 사용됩니다. 공개 키의 인증서가 CRL 테스트를 통과하면 연관된 개인 키도 테스트를 통과합니다.

소유자가 회사를 그만두거나 스마트 카드를 분실할 경우와 같은 다양한 이유 때문에 인증서가 해지될 수 있습니다.

다음과 같은 세 가지 경우에 인증서를 CRL에 대해 확인합니다.

- 보내는 메일이 서명된 경우  
sendsigncert를 0으로 설정하지 않았거나 crlenable를 0으로 설정하지 않은 경우 S/MIME 애플릿은 항상 이 확인을 수행합니다.
- 서명된 받는 메일을 읽을 경우  
readsigncert를 0으로 설정하지 않았거나 crlenable를 0으로 설정하지 않은 경우 S/MIME 애플릿은 항상 이 확인을 수행합니다.
- 보내는 메일이 암호화된 경우  
sendencryptcert을 0으로 설정하지 않았거나 crlenable를 0으로 설정하지 않은 경우 S/MIME 애플릿은 항상 이 확인을 수행합니다.

## CRL 액세스

인증서에는 Messaging Server가 CRL을 찾기 위해 사용하는 0개 이상의 URL(배포 지점이라고도 함)이 포함됩니다. 인증서에 CRL URL이 없을 경우 CRL에 대해 확인할 수 없으며 진짜 상태를 알지 못한 채 개인 또는 공개 키를 사용하여 메일을 서명하거나 암호화하게 됩니다.

Messaging Server가 사용할 수 있는 모든 URL을 시도한 후 CRL을 찾거나 액세스하지 못할 경우 인증서 상태가 알 수 없는 것으로 간주됩니다. 상태를 알 수 없는 개인 또는 공개 키를 사용할지 여부는 `revocationunknown`의 설정에 따라 결정됩니다.

각 CA에 대해 하나의 CRL만 지원되지만 동일한 CRL의 여러 복사본이 사용자의 공개 키 인증서 간에 다른 URL로 표시되는 다른 위치에 존재할 수 있습니다. Messaging Server는 CRL에 액세스할 때까지 인증서의 모든 URL 위치를 시도합니다.

정기적으로 CA에서 최신 CRL을 원하는 위치에 다운로드하여 CRL의 여러 복사본에 최적으로 액세스할 수 있도록 관리할 수 있습니다. 인증서에 포함된 URL을 변경할 수 없지만 인증서의 URL을 CRL 정보가 포함된 새 URL로 매핑하여 새 CRL 위치를 사용하도록 Messaging Server를 리디렉션할 수 있습니다. 다음 구문을 사용하여 LDAP 디렉토리에서 하나 이상의 매핑 정의 목록을 만듭니다([crlmappingurl](#) 참조).

```
msgCRLMappingRecord=url_in_certificate==new_url[|url_login_DN|url_login_password]
```

`url_in_certificate`는 CRL을 찾기 위한 이전 정보가 포함된 인증서의 URL입니다. `new_url`은 새 CRL 정보가 포함된 새 URL입니다. `url_login_DN` 및 `url_login_password`는 `new_url`에 액세스할 수 있는 항목의 DN과 비밀번호입니다. 두 옵션은 모두 선택 사항이며 지정하는 경우 새 URL 액세스에 대해서만 사용됩니다.

DN과 비밀번호가 실패할 경우 LDAP 액세스가 거부되며 다른 자격 증명을 사용하여 다시 시도되지 않습니다. 이러한 로그인 자격 증명은 LDAP URL에 대해서만 유효합니다. `smmime.conf`에서 `crlurl1logindn` 및 `crlurl1loginpw`를 사용할 경우 매핑 레코드에 로그인 DN과 비밀번호를 지정할 필요가 없습니다. [693페이지](#)의 "[자격 증명을 사용하여 LDAP에서 공개 키, CA 인증서 및 CRL 액세스](#)"를 참조하십시오.

한 계층의 매핑만 허용됩니다. 인증서의 다른 URL을 동일한 새 URL에 매핑할 수 있지만 인증서 URL을 여러 새 URL에 할당할 수는 없습니다. 예를 들어, 다음 매핑 목록은 유효하지 않습니다.

```
msgCRLMappingRecord=URL12==URL45
msgCRLMappingRecord=URL12==URL66
msgCRLMappingRecord=URL12==URL88
msgCRLMappingRecord=URL20==URL90
msgCRLMappingRecord=URL20==URL93
```

다음 예는 올바른 매핑 목록입니다.

```
msgCRLMappingRecord=URL12==URL45
msgCRLMappingRecord=URL14==URL66
msgCRLMappingRecord=URL88==URL66
msgCRLMappingRecord=URL201==URL90
msgCRLMappingRecord=URL202==URL93
```

LDAP 디렉토리에서 매핑 정의를 만든 후에 `smime.conf` 파일의 `crlmappingurl`을 사용하여 이러한 정의를 찾기 위한 디렉토리 정보를 지정합니다. [697페이지](#)의 "`crlmappingurl`"을 참조하십시오.

## 프록시 서버 및 CRL 확인

시스템에서 클라이언트 응용 프로그램과 Messaging Server 간에 프록시 서버를 사용할 경우 CRL 확인을 수행하기 위해 S/MIME 애플릿을 올바르게 구성했다라도 CRL 확인이 차단될 수 있습니다. 이러한 문제가 발생하면 유효한 키 인증서가 해지 또는 알 수 없는 상태라는 것을 경고하는 오류 메시지가 Communications Express Mail 사용자에게 표시됩니다.

다음과 같은 상황에서 이 문제가 발생합니다.

- 다음 구성 값을 사용하여 CRL 확인을 요청한 경우
  - `smime.conf` 파일의 `crlenable` 매개 변수를 1로 설정
  - Messaging Server의 `local.webmail.cert.enable` 옵션을 1로 설정
- S/MIME 애플릿과 프록시 서버 간의 통신 연결이 SSL로 보안되지 않았지만 `smime.conf` 파일의 `checkoverssl` 매개 변수가 1로 설정되었기 때문에 S/MIME 애플릿이 보안 연결을 예상하는 경우

이 문제를 해결하려면 다음 작업을 수행합니다.

1. 클라이언트 시스템과 프록시 서버 간의 통신 연결을 SSL을 사용한 보안 연결로 설정하고 모든 구성 값을 그대로 둡니다.  
  
또는
2. 통신 연결을 보안되지 않은 상태로 두고 `checkoverssl`을 0으로 설정합니다.

자세한 내용은 [702페이지](#)의 "[SSL을 사용하여 인터넷 연결 보안](#)"을 참조하십시오.

## 오래된 CRL 사용

S/MIME 애플릿이 확인을 수행하라는 요청을 보내면 Messaging Server가 인증서를 CRL에 대해 확인합니다. Messaging Server는 인증서를 확인할 때마다 CRL을 메모리로부터 다운로드하는 대신 CRL 복사본을 디스크에 다운로드하고 해당 복사본을 인증서 확인에 사용합니다. 모든 CRL에는 지정한 날짜 이후에는 최신 버전의 CRL을 사용하도록 지정

하는 next-update 필드가 있습니다.

next-update 날짜는 CRL 사용의 만료 날짜나 시간 제한으로 간주할 수 있습니다. CRL은 next-update 날짜가 지나면 오래된 것으로 간주되며 Messaging Server는 다음 번에 인증서를 검사할 때 최신 버전의 CRL을 다운로드합니다.

S/MIME 애플릿이 인증서를 CRL에 대해 확인하도록 요청할 때마다 Messaging Server는 다음 작업을 수행합니다.

1. 현재 날짜를 CRL의 next-update 날짜와 비교합니다.
2. CRL이 오래된 경우 Messaging Server는 최신 버전의 CRL을 다운로드하여 디스크의 오래된 CRL을 대체한 다음에 확인 작업을 진행합니다. 그러나 최신 버전의 CRL을 찾을 수 없거나 다운로드할 수 없으면 smime.conf 파일의 crlusepastnextupdate 값에 따라 수행할 작업을 결정합니다.
3. crlusepastnextupdate가 0으로 설정된 경우 오래된 CRL이 사용되지 않으며 해당 인증서는 모호한 상태가 됩니다. S/MIME 애플릿은 smime.conf의 revocationunknown 값에 따라 다음과 같이 수행할 작업을 결정합니다.
  - a. revocationunknown이 ok로 설정된 경우 인증서는 유효한 것으로 간주되며 개인 또는 공개 키를 메일의 서명이나 암호화에 사용합니다.
  - b. revocationunknown이 revoked로 설정된 경우 인증서는 유효하지 않은 것으로 간주되고 개인 또는 공개 키를 메일 서명이나 암호화에 사용하지 않으며 키를 사용할 수 없다는 오류 메시지를 메일 사용자에게 표시됩니다.

crlusepastnextupdate가 1로 설정된 경우 S/MIME 애플릿이 오래된 CRL을 계속 사용하므로 Communications Express Mail 내에서 처리 중단이 발생하지 않지만 이러한 상황을 알리기 위해 Messaging Server 로그 파일에 메시지가 기록됩니다.

인증서를 CRL에 대해 확인할 때 이러한 순서의 이벤트가 계속됩니다. Messaging Server가 최신 버전의 CRL을 제때에 smime.conf 파일의 설정에 따라 다운로드할 수 있으면 메일 처리가 중단 없이 계속됩니다. Messaging Server 로그를 정기적으로 확인하여 오래된 CRL이 사용 중임을 나타내는 메시지가 반복되는지 확인합니다. 최신 CRL을 다운로드할 수 없는 경우 액세스할 수 없는 이유를 조사해야 합니다.

## 사용할 메일 시간 지정

timestampdelta 매개 변수는 주로 다음 용도로 사용됩니다.

1. 메일이 대상에 도착하는 데 오래 걸리는 상황을 처리하는 경우. 이 경우 메일을 보낼 때 키가 유효했다라도 보낸 사람의 키가 잘못된 키로 간주되었을 수 있습니다.

2. 보낸 시간을 속일 수 있으므로 메일의 보낸 시간에 대한 신뢰를 제한하려는 경우 모든 메일은 다음 두 가지 시간과 관련되어 있습니다.

- 메일을 보낸 시간(메일 헤더 세부 정보의 날짜 행에 있음)
- 메일이 대상에 도착한 시간(메일 헤더 세부 정보의 마지막 받은 날짜 행에 있음)

---

**주** 메일의 보낸 사람 필드 오른쪽에 있는 삼각형 아이콘을 누르면 메일 헤더 세부 정보를 볼 수 있습니다.

---

메일을 보낼 때 유효했던 인증서가 메일이 대상에 도착할 때 해지되거나 만료될 수 있습니다. 이 경우에는 인증서의 유효성을 검사할 때 보낸 시간과 받은 시간 중에서 어떤 시간을 사용해야 하는지가 중요합니다. 보낸 시간을 사용하면 메일을 보낼 때 인증서가 유효했는지 여부를 확인합니다. 그러나 항상 보낸 시간을 사용하면 메일이 대상에 도착하는 데 오래 걸릴 수 있다는 사실을 고려하지 못합니다. 이러한 경우에는 받은 시간을 사용하는 것이 낫습니다.

smime.conf 파일의 timestampdelta 매개 변수를 사용하여 CRL 확인에 사용할 시간에 영향을 줄 수 있습니다. 이 매개 변수는 초를 나타내는 양의 정수로 설정합니다. 받은 시간에서 timestampdelta 값을 뺀 시간이 보낸 시간보다 앞설 경우 보낸 시간이 사용됩니다. 그렇지 않을 경우에는 받은 시간이 사용됩니다. timestampdelta의 값이 작을수록 받은 시간이 더 자주 사용됩니다. timestampdelta를 설정하지 않으면 항상 받은 시간이 사용됩니다. [700페이지의 "timestampdelta"](#)를 참조하십시오.

## CRL 액세스 문제

네트워크 또는 서버 문제와 같은 다양한 이유 때문에 Messaging Server가 인증서를 CRL에 대해 확인하려고 할 때 CRL을 사용하지 못할 수 있습니다. 이 경우에 Messaging Server가 계속 CRL에 액세스하려고 시도하느라 시간을 낭비하게 하는 대신 smime.conf 파일의 crlaccessfail 매개 변수를 사용하여 CRL 액세스를 시도하는 빈도를 관리함으로써 Messaging Server가 다른 작업을 수행하게 할 수 있습니다.

crlaccessfail을 사용하여 다음을 정의합니다.

- 실패한 시도의 횟수(시도가 실패할 때마다 Messaging Server 로그에 오류 메시지가 기록됨)

- 실패한 시도 횟수를 세는 기간
  - 새 CRL 액세스 주기를 시도하기 전에 기다리는 시간
- 매개 변수의 구문과 예는 [692페이지](#)의 "crlaccessfail"을 참조하십시오.

## 인증서가 해지된 경우

공개 키의 인증서가 CRL의 항목과 일치하지 않으면 개인 또는 공개 키가 보내는 메일의 서명이나 암호화에 사용됩니다. 인증서가 CRL의 항목과 일치하거나 인증서의 상태를 알 수 없으면 개인 또는 공개 키는 해지된 것으로 간주됩니다. 기본적으로 Communications Express Mail은 해지된 인증서가 포함된 키를 보내는 메일의 서명이나 암호화에 사용하지 않습니다. 수신자가 메일을 읽을 때 서명된 메일의 개인 키가 해지된 경우 수신자에게 서명을 신뢰할 수 없다는 경고 메시지가 표시됩니다.

원할 경우 smime.conf 파일에서 다음 매개 변수를 사용하여 해지된 모든 인증서에 대한 여러 기본 정책을 변경할 수 있습니다.

- sendsigncertrevoked를 allow로 설정하면 공개 키 인증서가 해지되어 해지된 것으로 간주되는 개인 키를 사용하여 보내는 메일에 서명합니다.
- sendcryptcertrevoked를 allow로 설정하면 해지된 인증서가 있는 공개 키를 사용하여 보내는 메일을 암호화합니다.
- revocationunknown을 ok로 설정하면 상태를 알 수 없는 인증서를 유효한 것으로 처리하며 개인 또는 공개 키를 보내는 메일의 서명이나 암호화에 사용합니다.

## S/MIME 기능을 사용할 수 있는 권한 부여

Communications Express Mail을 통해 사용할 수 있는 여러 메일 서비스를 사용할 수 있는 권한을 LDAP 필터를 사용하여 부여하거나 거부할 수 있습니다. 필터는 mailAllowedServiceAccess 또는 mailDomainAllowedServiceAccess LDAP 속성을 사용하여 정의합니다. 일반적으로 필터는 다음 세 가지 방법 중 하나로 작동합니다.

- 필터를 사용하지 않을 경우 모든 서비스에 대한 권한이 모든 사용자에게 부여됨
- 지정된 서비스 이름에 대한 권한이 일련의 사용자에게 명시적으로 부여됨(서비스 이름 목록 앞에 더하기 기호(+))가 있음)
- 지정된 서비스 이름에 대한 권한이 일련의 사용자에게 대해 명시적으로 거부됨(서비스 이름 목록 앞에 음수 기호(-))가 있음)

S/MIME의 필수 메일 서비스 이름은 http, smime 및 smtp입니다. Communications Express Mail 사용자 중에서 S/MIME 사용을 제한해야 하는 경우 적절한 LDAP 속성 구분과 서비스 이름을 사용하여 필터를 만듭니다. 이러한 속성은 LDAP 명령을 사용하여 만들거나 수정합니다.

## S/MIME 권한 예

1. 다음 예는 한 명의 Communications Express Mail 사용자가 S/MIME 기능에 액세스할 수 없게 합니다.

```
mailAllowedServiceAccess: -smime:*$+imap,pop,http,smtp:*
```

또는

```
mailAllowedServiceAccess: +imap,pop,http,smtp:*
```

2. 다음 예는 도메인의 모든 Communications Express Mail 사용자가 S/MIME 기능에 액세스할 수 없게 합니다.

```
mailDomainAllowedServiceAccess: -smime:*$+imap:*$+pop:*$+smtp:*$+http:*
```

또는

```
mailDomainAllowedServiceAccess: +imap:*$+pop:*$+smtp:*$+http:*
```

자세한 내용은 [666페이지의 "필터 문"](#)을 참조하십시오.

## 인증서 관리

다음 예에서는 대부분 ldapsearch 및 ldapmodify 명령을 사용하여 LDAP 디렉토리에 사용자 키와 인증서를 검색합니다. 이러한 명령은 Directory Server와 함께 제공됩니다. 이러한 명령에 대한 자세한 내용은 *Sun ONE Directory Server Resource Kit Tools Reference*(릴리스 5.2)를 참조하십시오.

### LDAP 디렉토리의 CA 인증서

다음 예에서는 인증 기관의 인증서를 LDAP 디렉토리에 추가합니다. 이러한 인증서의 디렉토리 구조는 이미 존재합니다. 인증서와 인증서가 속하는 LDAP 항목은 add-root-CA-cert.ldif라는 .ldif 파일에 입력합니다. Base64 인코딩된 텍스트로 입력해야 하는 인증서 정보를 제외하고 이 파일의 모든 텍스트는 ASCII 텍스트로 입력합니다.



```

dn: cn=SMIME Admin,ou=people,o=demo.siroe.com,o=demo
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: certificationAuthority
cn: RootCACerts
sn: CA
authorityRevocationList: novalue
certificateRevocationList: novalue
cacertificate;binary:: MFU01JTUUEjAQBgNVBAsTCU1zZ1NlcnZlcjMBoGA1UEAxMTydg
QGEwJVUzEOMAwGA1UEMFUJTUUXEjAQBgNVBAsTCU1zZ1NlcnZlcjEMBoGA1UEAxMTQ2Vydg
aFw0wNjAxMwODAwMDBaM267hgbX9FExCzAJByrjgNVBAK9STklBMQwCgYDVQQVHR8EgaQwg
YTA1VMMRQYDVQQIEWpDQXJk9STklBMQwwCgYDVQQKEwww31tgYz111zAdBgNVBpYSE9Vc
5yZWQaddWlm899XBsYW5ldc5jb20wgZ8wDQYJOGBAK1mUTy8vvnOFg4mlHjkgHyTQUR1k8l
5mvWRf77ntm5mGXRd3XMu40ciUq6zUfIg3ngvxlLyERTIqjUS8HQ4R5pvj+rrVgsAGjggE
+FNAJmtOV2A3wMyghqkVPNDP3Aqq2fkcN4va3C5nRNAYxNNVE84J0H3jyPDXhMB1QU6vQn
weMBAAjggEXMIIBEzARBglghkgBhCAQEEBApq1Sai4mfuvjh02SQkoPMNDAGTwMB8GA1UdI
QYMBaAEd38IK05AHreiU9OYc6vNMOWZMIGsBgNVHR8EgaQwgaEwb6BtoGuGaWkYXA6Lyht
bmcucmVklmlbGFuZXQuY29tL1VJd1DXJ0aWZpY2F0ZSBNYW5hZ2VyLE9VPVBlb3BsZSxPPW
aWxxYT9jZXJ0aZpY2jdu2medXR1lkghytQURYFNrkuoCygKoYoaHR0cDovL3Bl1a2kgHyTQU
Zy5yZWQuaXBsYW5ldc5jb20vcGVranLmNybdAeBgNVHREEFzAVGRNwb3J0aWEuc2hhb0BzdW
4uY29tMAOGCXLm78freCxS3Pp078jyTaDci1AudBL8+RrRUQvxsMJfZeFED+Uuf10Ilt6kw
Tc6W5UekbirfEZGAVQIzlt6DQJfgpifGLvtQ60Kw==

```

CA 인증서를 ldapmodify 명령을 사용하여 LDAP 디렉토리에 추가합니다.

```
# ldapmodify -a -h demo.siroe.com -D "cn=Directory Manager" -w mypasswd -v
-f add-root-CA-cert.ldif
```

smime.conf의 trustedurl 매개 변수 값은 LDAP 디렉토리에서 CA 인증서의 위치를 지정합니다. 예 1의 경우 trustedurl은 다음으로 설정됩니다.

```
trustedurl==ldap://demo.siroe.com:389/cn=SMIME Admin, ou=people,
o=demo.siroe.com,o=demo?cacertificate;binary?sub?(objectclass=certificatio
nAuthority)
```



## 키와 인증서가 LDAP 디렉토리에 있는지 확인

다음 예에서는 LDAP 디렉토리에서 CA 인증서와 공개 키 및 해당 인증서를 검색하는 것을 보여 줍니다.

### 하나의 CA 인증서 검색

다음 예에서 `-b` 옵션에 정의된 기본 DN `cn=SMIME admin,`

`ou=people,o=demo.siroe.com,o=demo objectclass=*`는 LDAP 디렉토리에 있는 하나의 CA 인증서를 설명합니다. 디렉토리에서 찾는 경우 `ldapsearch`는 인증서에 대한 정보를 `ca-cert.ldif` 파일에 반환합니다.

```
# ldapsearch -L -h demo.siroe.com -D "cn=Directory Manager" -w mypasswd
-b "cn=SMIME admin, ou=people,o=demo.siroe.com,o=demo"
"objectclass=" > ca-cert.ldif
```

아래 예에서는 `ca-cert.ldif` 파일의 검색 결과를 보여 줍니다. 파일 내용의 형식은 `ldapsearch`의 `-L` 옵션을 사용한 결과입니다.

```
# more ca-cert.ldif
dn: cn=SMIME admin,ou=people,o=demo.siroe.com,o=demo
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: certificationAuthority
cn: RootCACerts
cn: SMIME admin
sn: CA
authorityRevocationList: novalue
certificateRevocationList: novalue
cacertificate;binary:: MFU01JTUUxEjAQBgNVBAsTCU1zZ1N1cnZlcjcmBoGA1UEAxMTyDg
QGEwJVEOMAwGA1UEChMFU0U0UxEjAQBgNVBAsTCU1zZ1N1cnZlcjcmBoGA1UEAxMTQ2VydG
aFw0jAxMTIwODAwMDBaM267X9FExCzAJBgwyrjgNVBAk9STklBMQwwCgYDVQQLVHR8EgaQwg
Y1VzMRMwEQYDVQQIEWpDQUx9STklBMQwwCgYDVQQKEWww3ltgoOYz111zAdBgNVBpYSE9Vc
5yQuaddiiWlm899XBsYW51jb20wgZ8wDQYJcGBAK1mUTy8vv02nOFg4mlHjkgkghytQUR1k81
5mcWRfL77ntm5mGXRD3XMciUq6zUfIg3ngvx1LKLyERTIqjUS8HQU4R5pvj+rrVgsAGjggE
+FNAJmqtOV2A3wMyghqkDP3Aqq2BYfkc4va3C5nRNAyxNnVE84JJ0H3jyPDXhMB1QU6vQn
1NABAAGjggEXMIIBEzglghkgBhvhCAQEEBAPq1Sai4mfuvjh02SQkOPMNDagTwMB8GA1UdI
QYMAFEd38IK05AHreOYc6v+ENMOWZMIGsBgNVHR8EgaQwgaEwb6BtoGuGaWxkYXA6Lyht74
tpbucmVklm1wbGFuZyZy29tL1VJRd1DZXJ0aWZpY2F0ZSBNYW5hZ2VyLE9VPVBlb3BsZSxPPW
1haWYt9jZkxJ0aWZpdu2medXR11HjkgkghytQURYFNrkuoCYgKoYoaHR0cDovL3Bla2kghytQU
luZyZWQuaXBsYW51db20vcGVraW5nLmNybDAeBgNVHREEFzAVgRNwb3J0aWEuc2hhb0BzdW
4uYtMA0GCxLm78Ufre3Pp078jyTaDv2ci1AudBL8+RrRUQvxsmJfZeFED+Uuf101lt6kwhm
Tc6W5UekbirfEZGAVQIz1t6DQJfgpifGLvtQ60Kw==
```

### 여러 공개 키 검색

다음 예에서 `-b` 옵션에 정의된 기본 DN `o=demo.siroe.com,o=demo objectclass=*`는 LDAP 디렉토리의 기본 DN과 그 아래에서 발견된 모든 공개 키와 인증서를 `usergroup.ldif` 파일로 반환하도록 합니다.

```
# ldapsearch -L -h demo.siroe.com -D "cn=Directory Manager" -w
mypasswd
-b "o=demo.siroe.com,o=demo" "objectclass=*" > usergroup.ldif
```

### 하나의 공개 키 검색

다음 예에서 `-b` 옵션에 정의된 기본 DN `uid=JohnDoe, ou=people,o=demo.siroe.com,o=demo objectclass=*`는 LDAP 디렉토리에 있는 하나의 공개 키와 해당 인증서를 설명합니다.

```
# ldapsearch -L -h demo.siroe.com -D "cn=Directory Manager" -w mypasswd
-b "uid=JohnDoe, ou=people,o=demo.siroe.com,o=demo" "objectclass=*" >
public-key.ldif
```

아래 예는 `public-key.ldif` 파일의 검색 결과를 보여 줍니다. 파일 내용의 형식은 `ldapsearch`의 `-L` 옵션을 사용한 결과입니다.

```
# more public-key.ldif
dn: uid=sdemol, ou=people, o=demo.siroe.com, o=demo
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: siroe-am-managed-person
objectClass: inetOrgPerson
objectClass: inetUser
objectClass: ipUser
objectClass: userPresenceProfile
objectClass: inetMailUser
objectClass: inetLocalMailRecipient
objectClass: icsCalendarUser
objectClass: sunUCPreferences
mail: JohnDoe@demo.siroe.com
mailHost: demo.siroe.com
.
.
uid: JohnDoe
.
.
```

```
mailUserStatus: active
inetUserStatus: active
.
.
.
usercertificate;binary:: MFU01JTUUxEjAQBgNBAsTCU1zZ1NlcnZjcMBoGA1UEAxMTYdG
QGEwJEOwGA1UEChMFU01JTUUxEjAQBgNVBAsTCU1zZ1NlcnZlcjEcMBoGA1UEAxMTQ2Vydg
aFw0MTIwODAwMDBaM267hgbX9FExCzAJBgwyrjgNVBAk9STklBMQwwCgYDVQQVHR8EgaQwg
YTA1VEQYDVQQIEWpDQUxJRk9STklBMQwwCgYDVQQKEww31tgoOYz111zAdBgNVBpYSE9Vc
5yZWQdWlM899XBsYW5ldC5jb20wgZ8wDQYJOGBAK1mUTy8vv02nOFg4mlHjkgghytQUR1k8l
5mvgc7ntm5mGXRd3XMU40ciUq6zUfIg3ngvx1LLLyERTIqjUS8HQ4R5pvj+rrVgsAGjggE
+FG9NmV2A3wMyghqkVPNDP3Aqq2BYfkc4va3C5nRNAYxNNVE84JJ0H3jyPDXhMB1QU6vQn
1NAGMAgEXMIIBEzARBglghkgBhvhCAQEEBAPq1Sai4mfuvjh02SQkoPMNDAgTwmB8GA1UdI
QYMBaEdK05AHreiU9OYc6v+ENMOwZMIGsBgnVHR8EgaQwgaEwb6BtoGuGaWxkYXA6Lyht74
tpbucmVkwbgFuZlZlY29tL1VJRd1DZXJ0aWZpY2F0ZSBnYw5hZ2VyLE9VPVBlb3BsZSxPPW
1haxYT9jZaWZpY2Jdu2medXR1lHjkgghytQURYFNrkuoCygKoYoaHR0cDovL3Bl2kgghytQU
luZyZWQuaYW5ldC5jb20vcGVraW5nLmNybDAeBgNVHREEFzAVGRNwb3J0aWEuc2hhb0BzdW
4u9tMA0GC78UfreCxS3Pp078jyTaDv2ci1AudBL8+RrRUQvxsMJfZeFED+Uuf10Ilt6kwhm
Tc6W5UekbirfEZGAVQIzlt6DQJfgpifGLvtQ60Kw==
.
.
```

## 네트워크 보안 서비스 인증서

네트워크 보안 서비스(NSS)에 사용되는 여러 인증서는 LDAP 데이터베이스가 아닌 자체 데이터베이스에 저장됩니다. 이러한 인증서와 관련 CRL을 데이터베이스에 저장하기 위해 Messaging Server에서는 certutil 및 crlutil의 두 가지 유틸리티를 제공합니다. 이러한 유틸리티를 사용하여 데이터베이스를 검색할 수도 있습니다.

certutil에 대한 자세한 내용은 *Sun Java System Directory Server 관리 설명서* (<http://docs.sun.com/doc/819-2012>)를 참조하십시오. 또한 crlutil과 함께 제공되는 도움말 텍스트를 참조하십시오(유틸리티를 인수 없이 실행하면 유틸리티의 온라인 도움말을 볼 수 있음).

# Communications Express S/MIME 최종 사용자 정보

이 절에서는 최종 사용자를 위한 정보를 제공합니다. 이 절은 다음 내용으로 구성되어 있습니다.

- [718페이지의 "처음 로그인"](#)
- [719페이지의 "서명 및 암호화 설정"](#)
- [721페이지의 "Java 콘솔 활성화"](#)

## 처음 로그인

메일 사용자가 Communications Express Mail에 처음으로 로그인하면 S/MIME 애플릿과 관련된 특수한 프롬프트가 표시됩니다.

### Windows용 프롬프트

Windows 98, 2000 또는 XP에서 Communications Express Mail에 처음 로그인하면 다음 프롬프트가 표시됩니다.

1. JRE(Java 2 Runtime Environment)가 컴퓨터(클라이언트 시스템)에 설치되지 않은 경우 다음과 비슷한 프롬프트가 표시됩니다.

```
Do you want to install and run "Java Plug-in 1.4.2_03 signed on
11/20/03 and distributed by Sun Microsystems, Inc."?
Publisher authenticity verified by: VeriSign Class 3 Code Signing
2001 CA
```

Yes를 누르고 다음 프롬프트에 따라 JRE를 설치합니다.

---

**주** 영어 언어 지원을 원하지만 라틴어가 아닌 문자(예: 중국어)를 포함하는 S/MIME 메일도 읽고 싶은 경우에는 컴퓨터의 /lib 디렉토리에 charsets.jar 파일이 있어야 합니다.

charsets.jar 파일이 /lib 디렉토리에 설치되도록 하려면 사용자 정의 설치를 사용하여 영어 버전의 JRE를 설치합니다. 설치 중에 "추가 언어 지원" 옵션을 선택합니다.

자세한 내용은 [686페이지의 "여러 언어 지원"](#)을 참조하십시오.

---

마지막 설치 프롬프트에서 Finish를 누릅니다. 컴퓨터를 다시 시작하고 Communications Express Mail에 다시 로그인합니다.

## 2. 다음과 같은 프롬프트가 표시됩니다.

```
Do you want to trust the signed applet distributed by "Sun
Microsystems, Inc."?
Publisher authenticity verified by: Thawte Consulting cc
```

다음 응답 중 하나를 누릅니다.

- Communications Express Mail 세션에 S/MIME 애플릿을 허용하려면 Yes를 누릅니다. 로그인할 때마다 프롬프트가 표시됩니다.
- S/MIME 애플릿을 거부하려면 No를 누릅니다. S/MIME 기능을 사용할 수 없습니다.
- 현재 및 이후의 모든 Communications Express Mail 세션에 S/MIME 애플릿을 허용하려면 Always를 누릅니다. 프롬프트가 다시 표시되지 않습니다.

## 3. 다음과 같은 프롬프트가 표시됩니다.

```
Do you want to trust the signed applet distributed by "sun
microsystems, inc."?
Publisher authenticity verified by: VeriSign, Inc.
```

다음 응답 중 하나를 누릅니다.

- 현재의 Communications Express Mail 세션에 S/MIME 애플릿을 허용하려면 Yes를 누릅니다. 로그인할 때마다 프롬프트가 표시됩니다.
- S/MIME 애플릿을 거부하려면 No를 누릅니다. S/MIME 기능을 사용할 수 없습니다.
- 현재 및 이후의 모든 Communications Express Mail 세션에 S/MIME 애플릿을 허용하려면 Always를 누릅니다. 프롬프트가 다시 표시되지 않습니다.

## 서명 및 암호화 설정

모든 사용자의 보내는 메일을 다음 중 어떤 방법으로 처리할지 제어하기 위해 설정할 수 있는 초기 서명 및 암호화 설정이 있습니다.

- 자동으로 서명
- 자동으로 암호화
- 자동으로 서명 및 암호화

또한 초기 설정은 Communications Express Mail 창의 맨 아래와 옵션 - 설정 창에 있는 서명 및 암호화 확인란을 선택한(기능 설정) 또는 선택하지 않은(기능 해제) 상태로 표시할지 여부를 제어합니다. smime.conf 파일에서 alwaysencrypt 및 alwayssign 매개변수를 사용하여 이러한 초기 설정을 지정합니다.

메일 사용자에게 메일의 초기 설정을 변경할 수 있다고 알려주십시오. Communications Express Mail에 로그인한 후 사용자는 하나의 메일에 대한 설정을 임시로 대체하거나 모든 메일에 대한 설정을 지속적으로 대체할 수 있습니다.

표 20-6에서는 이 확인란 사용에 대해 요약합니다.

**표 20-6** Communications Express Mail의 서명 및 암호화 확인란

| 확인란 텍스트        | 위치                                                               | Communications Express Mail 사용자가 수행하는 작업                                                                                                                                                      |
|----------------|------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 메시지에 서명        | 메일 작성, 전달 또는 회신에 사용되는 Communications Express Mail 창의 맨 아래에 있습니다. | <ul style="list-style-type: none"> <li>• 현재 메일에 서명하려면 선택합니다.</li> <li>• 현재 메일에 서명하지 않으려면 선택 취소합니다.</li> </ul>                                                                                 |
| 메시지 암호화        | 메일 작성, 전달 또는 회신에 사용되는 Communications Express Mail 창의 맨 아래에 있습니다. | <ul style="list-style-type: none"> <li>• 현재 메일을 암호화하려면 선택합니다.</li> <li>• 현재 메일을 암호화하지 않으려면 선택 취소합니다.</li> </ul>                                                                               |
| 보내는 모든 메시지에 서명 | Communications Express Mail 옵션 설정 창에서 보안 메일 옵션 아래에 있습니다.         | <ul style="list-style-type: none"> <li>• 모든 메일에 자동으로 서명하려면 선택합니다.</li> <li>• 모든 메일에 자동으로 서명하지 않으려면 선택 취소합니다.</li> </ul> <p>주: "메시지에 서명" 확인란을 사용하여 "보내는 모든 메시지에 서명" 설정을 메일별로 대체할 수 있습니다.</p>   |
| 보내는 모든 메시지 암호화 | Communications Express Mail 옵션 설정 창에서 보안 메일 옵션 아래에 있습니다.         | <ul style="list-style-type: none"> <li>• 모든 메일을 자동으로 암호화하려면 선택합니다.</li> <li>• 모든 메일을 자동으로 암호화하지 않으려면 선택 취소합니다.</li> </ul> <p>주: "메시지 암호화" 확인란을 사용하여 "보내는 모든 메시지 암호화" 설정을 메일별로 대체할 수 있습니다.</p> |



## Java 콘솔 활성화

Communications Express Mail 사용자가 서명된 메일과 암호화된 메일을 처리할 때 S/MIME 애플릿에서 다양한 작업 메시지를 Java 콘솔에 기록할 수 있습니다. Java 콘솔 메시지는 메일 사용자가 보고한 문제를 해결하는 데 도움이 될 수 있습니다. 그러나 사용자의 LDAP 항목의 `inetMailUser` 객체 클래스에 `nswmExtendedUserPrefs` 속성을 추가하여 사용자에게 대해 Java 콘솔을 활성화한 경우에만 작업 메시지가 생성됩니다. 예를 들면 다음과 같습니다.

```
nswmExtendedUserPrefs: meSMIMEDebug=on
```

이렇게 하면 Communications Express Mail의 성능이 크게 저하될 수 있으므로 모든 메일 사용자에게 대해 Java 콘솔을 항상 활성화하지는 마십시오.



# 로깅 관리

이 장에서는 Messaging Server MTA, 메시지 저장소 및 서비스의 로깅 기능에 대해 개괄적으로 설명합니다. 또한 이 장에서는 이러한 로깅 기능을 관리하는 방법에 대해 설명합니다.

이 장은 다음 내용으로 구성되어 있습니다.

- [로깅 개요](#)
- [로깅 관리를 위한 도구](#)
- [MTA 메일 및 연결 로그 관리](#)
- [서비스 로그 관리](#)

## 로깅 개요

로깅은 시스템이 시스템 서비스에 대한 시간이 기록되고 레이블이 지정된 정보를 제공하는 수단입니다. 로깅에서는 시스템의 현재 스냅샷뿐 아니라 기록 보기도 제공합니다.

Messaging Server 로그 파일을 이해하고 사용하면 다음을 수행할 수 있습니다.

- 메일 크기, 메일 전달 속도, MTA를 통해 전달되는 메일 수 등의 메일 통계 수집
- 추세 파악
- 용량 계획 상호 연계
- 문제 해결

예를 들어, 사용자 수가 증가하여 더 많은 디스크 저장소를 사이트에 추가해야 할 경우 Messaging Server 로그 파일을 사용하여 시스템 수요의 증가 비율을 확인하고 필요한 새 디스크 저장소의 양을 계획할 수 있습니다.

또한 Messaging Server 로그를 사용하여 하루 동안의 메시징 패턴을 파악할 수 있습니다. 매일 최고 부하가 발생하는 시점을 파악하면 용량 계획을 수행하는 데 도움이 됩니다.

또한 로깅은 사용자 문제를 해결하는 데 도움이 됩니다. 예를 들어, 사용자가 예상한 메일 메시지를 받지 못할 경우 Messaging Server 로깅 기능을 사용하여 사용자의 메일 메시지를 추적할 수 있습니다. 이렇게 함으로써 메일이 자동으로 필터링되어 SPAM 폴더로 보내졌기 때문에 도착하지 않았음을 확인할 수도 있습니다.

## 로깅 데이터의 유형

일반적으로 로깅은 두 가지 유형의 정보를 제공합니다.

- 작업 데이터
- 오류 조건(이벤트 로깅이라고도 함)

대부분의 경우 Messaging Server 로깅에서는 작업 데이터를 제공합니다. 이 작업 데이터에는 메일이 시스템에 들어온 날짜와 시간, 메일의 보낸 사람 및 받는 사람, 메일이 디스크에 기록된 시간, 이후에 메일이 디스크에서 제거되고 사용자의 메일함에 삽입된 시간 등의 정보가 포함됩니다.

또한 Messaging Server 로깅에서는 이벤트 로깅 데이터도 제공합니다. 이벤트 로깅 데이터를 얻으려면 다른 로그 파일에서 여러 항목을 모아야 합니다. 그런 다음 메시지 아이디와 같은 고유한 상수를 사용하여 시스템을 통해 지점 간에 전달된 메일의 주기를 검색하고 연관시킬 수 있습니다.

## Messaging Server 로그 파일의 유형

Messaging Server 로깅은 세 가지 유형의 로그 파일로 구성됩니다.

1. **MTA 로그.** 앞에서 설명한 Message Transfer Agent에 대한 작업 데이터를 제공합니다.
2. **오류 로그.** 이 오류 로그는 MTA 디버그 로그이며 MTA 하위 구성 요소 로그(즉, Job Controller, 디스패처 등)입니다.

### 3. 메시지 저장소 및 서비스 로그. http 서버, mshttpd, imap, pop 서비스 및 Admin 서비스의 메일을 제공합니다. 이 로그의 형식은 처음 두 로그 유형과 다릅니다.

다음 표에는 다양한 유형의 로그 파일이 나열되어 있습니다. 기본적으로 로그 파일은 *msg\_svr\_base/data/logs* 디렉토리에 있습니다. 각 로그 파일의 유형을 개별적으로 사용자 정의하고 볼 수 있습니다.

**표 21-1** Messaging Server 로그 파일

| 로그 파일 유형       | 로그 파일 설명                                                                                                                                         | 기본 이름                                                                                                        |
|----------------|--------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------|
| MTA            | 날짜 및 시간 정보, 대기열에 포함 및 대기열에서 제외 정보 등을 비롯하여 MTA를 통과하는 메일 트래픽에 대한 정보를 보여 줍니다.                                                                       | mail.log, mail.log_current, mail.log_yesterday                                                               |
| 연결             | 전자 메일을 보내기 위해 이 시스템에 연결하는 원격 시스템(MTA)을 포함합니다.                                                                                                    | connection.log                                                                                               |
| 카운터            | 채널별로 송수신된 메일에 관한 메일 추세를 포함합니다.                                                                                                                   | counters                                                                                                     |
| Job Controller | 마스터, Job Controller, 보낸 사람 및 대기열에서 제외 채널 프로그램에 대한 데이터를 포함합니다.                                                                                    | job_controller.log                                                                                           |
| 디스패처           | 디스패처에 관한 오류를 포함합니다. 디스패처 디버깅을 설정하면 정보가 증가합니다.                                                                                                    | dispatcher.log                                                                                               |
| 채널             | 채널에 관한 오류를 기록합니다. master_debug 및 slave_debug 키워드는 채널 디버깅을 설정하여 채널 로그 파일의 자세한 표시 수준을 늘립니다. 정보 수준과 유형은 option.dat에서 여러 *_DEBUG MTA 옵션을 사용하여 제어합니다. | channelname_master.log*<br>(예: tcp_local_master.log*)<br>channelname_slave.log*<br>(예: tcp_local_slave.log*) |
| Admin          | Administration Server에 의해 콘솔과 Messaging Server 사이에 수행되는(대부분 CGI 프로세스를 통해 수행됨) 통신에 관련된 기록 이벤트가 포함됩니다.                                             | admin,<br>admin.sequenceNum.timeStamp                                                                        |
| IMAP           | 이 서버의 IMAP4 활동에 관련된 기록 이벤트가 포함됩니다.                                                                                                               | imap, imap.sequenceNum.timeStamp                                                                             |
| POP            | 이 서버의 POP3 활동에 관련된 기록 이벤트가 포함됩니다.                                                                                                                | pop, pop.sequenceNum.timeStamp                                                                               |
| HTTP           | 이 서버의 HTTP 활동에 관련된 기록 이벤트가 포함됩니다.                                                                                                                | http, http.sequenceNum.timeStamp                                                                             |
| 기본값            | 명령줄 유틸리티 및 기타 프로세스 등과 같은 이 서버의 다른 활동에 관련된 기록 이벤트가 포함됩니다.                                                                                         | default,<br>default.sequenceNum.timeStamp                                                                    |

**표 21-1** Messaging Server 로그 파일

| 로그 파일 유형 | 로그 파일 설명                                                                                    | 기본 이름    |
|----------|---------------------------------------------------------------------------------------------|----------|
| msgtrace | 메시지 저장소에 대한 추적 정보를 포함합니다. 파일이 매우 빠른 속도로 아주 커질 수 있습니다. 적절히 모니터링하십시오.                         | msgtrace |
| watcher  | 프로세스 실패와 응답하지 않는 서비스( <a href="#">111페이지의 표 4-4 참조</a> )를 모니터링하고 특정 실패를 나타내는 오류 메시지를 기록합니다. | watcher  |

여기서

*sequenceNum* - 로그 파일 디렉토리에 있는 다른 로그 파일과 비교하여 이 로그 파일의 생성 순서를 지정하는 정수를 지정합니다. 일련 번호가 높은 로그 파일은 이 번호가 낮은 로그 파일보다 최신 파일입니다. 일련 번호는 롤오버되지 않습니다. 즉 서버 설치부터 시작하여 서버 수명 동안 계속 증가합니다.

*timeStamp* - 파일 생성 날짜 및 시간을 지정하는 큰 정수를 지정합니다. 이 값은 1970년 1월 1일 자정부터 시작하여 계산한 초의 수인 표준 UNIX 시간으로 표시됩니다.

예를 들어 `imap.63.915107696`라는 이름의 로그 파일은 1998년 12월 31일 12:34:56 PM에 생성되었으며 IMAP 로그 파일의 디렉토리에 만들어진 63번째 로그 파일입니다.

타임스탬프를 사용하여 개방형 일련 번호 지정의 조합을 통해, 분석을 위한 파일의 회전, 만료 및 선택에 더 큰 유연성을 가질 수 있습니다. 자세한 내용은 [757페이지의 "서비스 로깅 옵션 정의 및 설정"](#)을 참조하십시오.

## 여러 로그 파일에서 메일 추적

시스템에서 메일이 전달되는 방법과 여러 로그 파일에 정보가 기록되는 시점은 아래에 설명되어 있습니다. 이러한 설명을 통해 Message Server의 로그 파일을 사용하여 문제를 해결하는 방법을 이해할 수 있습니다. [184페이지의 표 8-2](#)를 참조하십시오.

1. 원격 호스트가 메시징 호스트의 TCP 소켓에 연결하여 SMTP 서비스를 요청합니다.

2. MTA 디스패처가 요청에 응답하고 메시징 호스트의 SMTP 서비스에 연결을 넘겨 줍니다.

MTA는 모듈식으로 설계되므로 Job Controller 및 SMTP 서비스 디스패처를 포함하는 일련의 프로세스로 구성됩니다. 디스패처는 받는 TCP 연결을 가져와 SMTP 서비스로 보냅니다. SMTP 서비스는 메일을 디스크의 채널 영역에 기록합니다. SMTP 서비스는 메일의 봉투 매개 변수(예: 보낸 사람 및 받는 사람)를 인식합니다. 시스템의 구성 항목에서 시스템이 속한 대상 채널을 알려줍니다.

3. 디스패처가 스레드를 포크했고 특정 IP 주소에서 받는 연결에 대해 스레드를 사용할 수 있게 만들었다고 dispatcher.log 파일에 기록합니다.
4. SMTP 서버가 원격 호스트에서 SMTP 서버에 연결하여 메일을 보낼 때 발생한 일에 대한 기록을 tcp\_smtp\_server.log 파일에 기록합니다. 이 로그 파일은 디스패처가 호스트 IP의 SMTP 서버로 보낼 때 작성됩니다.
5. SMTP 서버가 tcp\_intranet과 같은 채널 프로그램의 디스크에 있는 대기열 영역에 메일을 기록하고 Job Controller에 알립니다.
6. Job Controller가 채널 프로그램에 연결합니다.
7. 채널 프로그램이 메일을 전달합니다.

채널마다 고유한 로그 파일이 있습니다. 그러나 이러한 로그에서는 일반적으로 채널의 시작 및 중지를 표시합니다. 추가 정보를 얻으려면 채널에 대한 디버그 수준을 활성화해야 합니다. 그러나 이로 인해서 시스템이 느려지고 진행 중인 문제가 더 모호해질 수 있으므로 실제 문제가 발생했을 경우에만 디버그 수준을 활성화해야 합니다.

---

**주**                    효율성을 위해 채널이 기존 프로세스에 대해 이미 실행 중인 경우 시스템은 새 메일이 들어와도 새 채널 프로세스를 만들지 않습니다. 현재 실행 중인 프로세스에서 새 메일을 가져옵니다.

---

8. 메일이 다른 호스트, 다른 TCP 연결 등의 다음 홉으로 전달됩니다. 이 정보는 connection.log 파일에 기록됩니다.

SMTP 서버가 디스크의 대기열 영역에 메일을 기록하는 것과 동시에 메일을 담당하는 채널이 mail.log\_current 또는 mail.log 파일에 레코드를 기록합니다. 이 레코드는 메일이 대기열에 포함된 날짜와 시간, 보낸 사람, 받는 사람 등의 정보를 보여 줍니다. 자세한 내용은 735페이지의 "MTA 메일 로깅 예"를 참조하십시오. 메일을 추적하는 데 가장 유용한 파일은 mail.log\_current 파일입니다.

## 로깅 관리를 위한 도구

콘솔에서 `configutil` 명령을 사용하여 **Messaging Server** 로그 파일 작성 및 관리를 위한 정책을 사용자 정의할 수 있습니다.

메시지 저장소 로그의 경우 콘솔을 사용하여 로그 설정을 지정하고 로그를 볼 수 있습니다. 지정하는 설정은 기록되는 이벤트 및 기록되는 이벤트의 수에 영향을 미칩니다. 로그 파일을 분석할 때 이러한 설정 및 기타 특성을 사용하여 기록되는 이벤트를 자세히 검색할 수 있습니다.

MTA는 별개의 로깅 기능을 사용하기 때문에 콘솔을 사용하여 MTA 로깅 서비스를 구성하거나 로그를 볼 수 없습니다. 대신 구성 파일에 정보를 지정하여 MTA 로깅을 구성할 수 있습니다.

**Messaging Server**에서 제공하지 않는 로그 분석 및 보고서 생성 기능을 사용하려면 다른 도구를 사용해야 합니다. 로그 파일은 텍스트 편집기나 표준 시스템 도구로 조작할 수 있습니다.

정규 표현식 구문 분석을 지원하는 스크립트 가능 텍스트 편집기를 사용하면 이 장에서 설명하는 모든 조건을 기준으로 로그 항목을 추출하고 검색할 수 있으며, 결과를 정렬하거나 합계나 기타 통계를 낼 수도 있습니다.

UNIX 환경에서는 UNIX `syslog` 파일을 조작하기 위해 개발된 기존 보고서 생성 도구를 수정하고 사용할 수도 있습니다. 공개 도메인 `syslog` 조작 도구를 사용하려면 다른 날짜/시간 형식과 **Messaging Server** 로그 항목에는 있지만 `syslog` 항목에는 없는 두 개의 추가 구성 요소(`facility` 및 `logLevel`)를 고려하여 수정해야 합니다.

## MTA 메일 및 연결 로그 관리

MTA는 각 메일이 대기열에 포함되고 제외될 때마다 로깅할 수 있는 기능을 제공합니다. 또한 디스패처 오류 및 디버깅 출력도 제공합니다.

로깅은 채널별로 제어하거나 모든 채널의 메일 활동이 기록되도록 지정할 수 있습니다. 초기 구성에서는 모든 채널에 대해 로깅이 비활성화됩니다.

자세한 내용은 [733페이지](#)의 "[MTA 로깅 활성화](#)"를 참조하십시오.



로깅을 활성화하면 MTA는 메일이 MTA 채널을 통과할 때마다 `msg_svr_base/data/log/mail*` 파일에 항목을 기록합니다. 이러한 로그 항목은 MTA를 통해(또는 특정 채널을 통해) 전달된 메일의 수에 대한 통계를 얻으려는 경우에 유용합니다. 또한 이러한 로그 항목을 사용하여 메일의 전송/전달 여부와 시점 등의 다른 문제를 조사할 수 있습니다.

매일밤 자정 정도에 실행되는 메일 반환 작업은 기존 `mail.log_yesterday`를 누적 로그 파일인 `mail.log`에 추가하고, 현재 `mail.log_current` 파일의 이름을 `mail.log_yesterday`로 바꾼 다음 새 `mail.log_current` 파일을 시작합니다. 또한 메시지 반환 작업은 모든 `connection.log*` 파일에 대해 비슷한 작업을 수행합니다.

MTA는 현재 파일을 유지하기 위해 자동 롤오버를 수행하지만 파일 백업, 파일 자르기, 파일 삭제 등의 작업에 대한 정책을 결정하기 위해 누적 `mail.log` 파일을 관리해야 합니다.

로그 파일 관리 방법에 대해 고려할 때는 MTA의 주기적 반환 작업이 사이트에서 제공하는 `msg_svr_base/bin/daily_cleanup` 프로시저(있을 경우)를 실행한다는 것에 주의합니다. 따라서 일부 사이트는 매주 한 번 기존 `mail.log` 파일의 이름을 바꾸는 등의 자체적인 정리 절차를 제공할 수 있습니다.

---

#### 주의

로깅을 활성화하면 `mail.log`가 지속적으로 증가하므로 확인하지 않는 경우 디스크 공간을 모두 차지해버릴 수 있습니다. 따라서 이 파일의 크기를 주기적으로 모니터링하여 불필요한 내용은 삭제해야 합니다. 또한 필요에 따라 전체 파일을 삭제하여 다른 버전이 생성되도록 할 수도 있습니다.

---

## MTA 로그 항목 형식 이해

MTA 로그 파일은 ASCII 텍스트로 기록됩니다. 기본적으로 각 로그 파일 항목에는 아래 예와 같이 8개나 9개의 필드가 포함됩니다.

```
19-Jan-1998 19:16:57.64 l tcp_local E 1 adam@sesta.com
rfc822;marlowe@siroe.com marlowe@siroe.com
```

로그 항목에는 다음이 표시됩니다.

1. 항목이 작성된 날짜와 시간(예: 19-Jan-1998 19:16:57.64)
2. 소스 채널의 채널 이름(이 예의 경우 l)

3. 대상 채널의 채널 이름(이 예의 경우 tcp\_local) (SMTP 채널의 경우 LOG\_CONNECTION이 활성화되어 있으면, 플러스 기호(+)는 SMTP 서버에 대한 인바운드를 나타내고 마이너스 기호(-)는 SMTP 클라이언트를 통한 아웃바운드를 나타냅니다.)
  4. 항목의 유형(이 예에서는 E). 730페이지의 표 21-2를 참조하십시오.
  5. 메일의 크기(이 예에서는 1). 기본적으로 KB로 표현되지만 MTA 옵션 파일에 BLOCK\_SIZE 키워드를 사용하여 이 기본값을 변경할 수 있습니다.
  6. 봉투의 From: 주소(이 예에서는 adam@sesta.com). 알림 메일과 같이 봉투의 From: 주소가 비어 있는 메일의 경우에는 이 필드가 비어 있습니다.
  7. 봉투의 To: 주소의 원래 형식(이 예에서는 marlowe@siroe.com)
  8. 봉투의 To: 주소의 활성(현재) 형식(이 예에서는 marlowe@siroe.com)
  9. 전달 상태(SMTP 채널 전용)
- 다음 표에서는 로깅 항목 코드를 설명합니다.

**표 21-2** 로깅 항목 코드

| 항목  | 설명                                                                                                                                               |
|-----|--------------------------------------------------------------------------------------------------------------------------------------------------|
| B   | SMTP 서버로 보낸 잘못된 명령. 수신자 주소 필드에는 거부된 명령이 포함되고 진단 필드에는 SMTP 서버가 제공한 응답이 포함됩니다. MTA 채널 옵션 MAX_B_ENTRIES는 지정된 세션에 기록되는 잘못된 명령의 수를 제어합니다. 기본값은 10입니다. |
| BA  | 트랜잭션 초기에 인증이 성공적으로 수행된 후의 잘못된 명령                                                                                                                 |
| BS  | TLS가 성공적으로 시작된 후의 잘못된 명령                                                                                                                         |
| BSA | TLS 및 AUTH를 사용한 잘못된 명령                                                                                                                           |
| D   | 대기열에서 제외 성공                                                                                                                                      |
| DA  | SASL(인증)을 사용한 대기열에서 제외 성공                                                                                                                        |
| DS  | TLS(보안)를 사용한 대기열에서 제외 성공                                                                                                                         |
| DSA | TLS 및 SASL(보안 및 인증)을 사용한 대기열에서 제외 성공                                                                                                             |
| E   | 대기열에 포함                                                                                                                                          |
| EA  | SASL(인증)을 사용한 대기열에 포함 성공                                                                                                                         |
| ES  | TLS(보안)를 사용한 대기열에 포함 성공                                                                                                                          |

표 21-2 로깅 항목 코드

| 항목                                       | 설명                                                                                                                                                                                                                                                                                                                                                   |
|------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ESA                                      | TLS 및 SASL(보안 및 인증)을 사용한 대기열에 포함 성공                                                                                                                                                                                                                                                                                                                  |
| J                                        | 대기열에 포함 시도 거부(슬레이브 채널 프로그램에 의한 거부)                                                                                                                                                                                                                                                                                                                   |
| K                                        | 수신자 메일 거부됨. 보낸 사람이 NOTIFY=NEVER DSN 플래그 설정을 요청하거나 메일이 시간 초과하거나 메일을 수동으로 반환하는 경우(예: <code>imsimta qm "delete"</code> 명령은 각 수신자에 대해 항상 "K" 레코드를 생성하고 <code>qm "return"</code> 명령은 "R" 레코드 대신 "K" 레코드 생성). 보낸 사람의 요청에 따라 보낸 사람에게 알림을 보내지 않았음을 나타냅니다.<br><br>rejection/time-out과 동일한 종류이지만 실패한 메일에 대한 새 알림 메일(원래의 보낸 사람에게 보냄)이 생성되는 "R" 레코드와 비교될 수 있습니다. |
| Q                                        | 대기열에서 제외 일시적으로 실패                                                                                                                                                                                                                                                                                                                                    |
| R                                        | 대기열에서 제외 시도에서 수신자 주소 거부(마스터 채널 프로그램에 의한 거부) 또는 실패/바운스 메일의 생성                                                                                                                                                                                                                                                                                         |
| W                                        | 메일이 아직 전달되지 않았지만 아직 대기열에서 시도 중에 있음을 원래 전송자에게 알려주기 위해 전송되는 경고 메일                                                                                                                                                                                                                                                                                      |
| Z                                        | 일부 수신자는 성공했지만 이 수신자는 일시적으로 성공하지 못했습니다. 모든 수신자의 원본 메일 파일이 대기열에서 제외되었으며 대신 이 수신자와 다른 성공하지 못한 수신자를 위한 새 메일 파일이 곧 대기열에 포함됩니다.                                                                                                                                                                                                                            |
| <b>SMTP 채널의 LOG_CONNECTION + 또는 - 항목</b> |                                                                                                                                                                                                                                                                                                                                                      |
| C                                        | 연결 끊김. 뒤이어 진단 필드가 표시됩니다. <code>connection.log_current</code> (하나의 로그 파일이 사용되는 경우에는 <code>mail.log_current</code> )에 작성됩니다. 연결이 끊긴 이유를 기록하는 데 사용됩니다. 특히, 연결이 끊긴 이유가 일부 세션이 연결 끊기 제한에 도달했기 때문인 경우 이 사실이 진단 필드에 표시됩니다.                                                                                                                                  |
| O                                        | 연결 열림                                                                                                                                                                                                                                                                                                                                                |
| U                                        | SMTP 인증 성공 및 실패를 기록합니다. 형식은 다른 O 항목 및 C 항목의 경우와 같습니다. 특히, 응용 프로그램 필드와 전송 정보 필드가 동일한 순서로 표시됩니다. 사용자 이름이 알려져 있으면 사용자 이름 필드에 기록됩니다. LOG_CONNECTION MTA 옵션의 Bit 7(값 128)이 이를 제어합니다.                                                                                                                                                                      |
| X                                        | 연결 거부됨                                                                                                                                                                                                                                                                                                                                               |
| Y                                        | 연결이 설정되기 전에 연결 시도가 실패했음                                                                                                                                                                                                                                                                                                                              |
| I                                        | ETRN 명령이 수신됨                                                                                                                                                                                                                                                                                                                                         |

MTA 옵션 파일에서 LOG\_CONNECTION, LOG\_FILENAME, LOG\_MESSAGE\_ID, LOG\_NOTARY, LOG\_PROCESS 및 LOG\_USERNAME을 모두 활성화하면 형식은 아래 예와 같이 됩니다. (인쇄상의 이유로 샘플 로그 항목에서는 행이 바뀌어졌지만 실제 로그 항목은 한 행에 표시됩니다.)

```
19-Jan-1998 13:13:27.10 HOSTA 2e2d.2.1 tcp_local 1
E 1 service@siroe.com rfc822;adam@sesta.com
adam 276 /imta/queue/1/ZZ01IWFY9ELGWM00094D.00
<01IWFVYLGTS499EC9Y@siroe.com> inetmail
siroe.com (siroe.com [192.160.253.66])
```

위에서 설명한 것 이외의 추가 필드는 다음과 같습니다.

1. 채널 프로세스가 실행 중인 노드의 이름(이 예의 경우 HOSTA)
2. 점(.) 문자와 카운트가 뒤에 붙은 프로세스 아이디(16진수로 표현됨). 다중 스레드 채널 항목인 경우(예: tcp\_\* 채널 항목) 프로세스 아이디와 카운트 사이에 스레드 아이디도 있습니다. 이 예에서 프로세스 아이디는 2e2d.2.1입니다.
3. 정수로 표현된 메일의 NOTARY(전달 수신 요청) 플래그(이 예의 경우 276)
4. MTA 대기열 영역의 파일 이름(이 예의 경우 /imta/queue/1/ZZ01IWFY9ELGWM00094D.00)
5. 메일 아이디(이 예의 경우 <01IWFVYLGTS499EC9Y@siroe.com>)
6. 실행 프로세스의 이름(이 예의 경우 inetmail). UNIX에서 SMTP 서버 등의 디스패처 프로세스로 일반적으로 inetmail(SASL이 사용되지 않은 경우)입니다.
7. 연결 정보(이 예의 경우 siroe.com (siroe.com [192.160.253.66])). 연결 정보는 HELO/EHLO 행(받는 SMTP 메일)에서 전송 시스템이 나타내는 이름 또는 대기열에 포함 채널의 공식 호스트 이름(다른 종류의 채널) 등의 전송 시스템이나 채널 이름으로 구성됩니다. TCP/IP 채널의 경우 전송 시스템의 "실제" 이름, 즉 DNS 역조회 및 /또는 IP 주소에 의해 보고되는 심볼릭 이름은 ident\* 채널 키워드에 의해 제어되어 괄호 안에 표시될 수 있습니다. **347페이지의 "IDENT 조회"를 참조하십시오.** 이 샘플에서는 이러한 키워드 중 하나를 사용한 것으로 가정합니다. 이 경우 DNS와 IP 주소에서 발견된 이름을 모두 표시하는 기본 identnone 키워드를 사용합니다.

## MTA 로깅 활성화

단지 몇 개의 특정 MTA 채널에 대한 통계만 수집하려면 해당 MTA 채널에 대해서만 로깅 채널 키워드를 활성화합니다. 모든 MTA 채널에 대한 로깅을 활성화하는 사이트가 많이 있습니다. 특히 문제를 추적하는 경우 문제 진단의 첫 번째 단계로 예상하거나 의도한 채널로 메일이 전달되는지 알아내고 모든 채널에 대해 로깅을 활성화하면 이러한 문제의 진단에 도움이 됩니다.

### ▶ 특정 채널에서 MTA 로깅을 활성화하는 방법

1. `imta.cnf` 파일을 편집합니다.

이 파일은 `/opt/SUNWmsgsr/config` 디렉토리에 있습니다.

2. 특정 채널에 대한 로깅을 활성화하려면 `logging` 키워드를 채널 정의에 추가합니다. 예를 들면 다음과 같습니다.

```
channel-name keyword1 keyword2 logging
```

또한 로그 파일의 디렉토리 경로, 로그 수준 등의 여러 구성 매개 변수도 설정할 수도 있습니다. [753페이지의 "서비스 로그 관리"](#)를 참조하십시오.

### ▶ 모든 채널에서 MTA 로깅을 활성화하는 방법

1. `imta.cnf` 파일을 편집합니다.

이 파일은 `/opt/SUNWmsgsr/config` 디렉토리에 있습니다.

2. MTA 구성 파일의 채널 블록 섹션에서 `defaults` 채널([332페이지의 "채널 기본값 구성"](#) 참조)에 `logging` 키워드를 추가합니다. 예를 들면 다음과 같습니다.

```
defaults logging notices 1 2 4 7 copywarnpost copysendpost postheadonly  
noswitchchannel immnonurgent maxjobs 7 defaulthost siroe.com
```

```
1 defragment charset7 us-ascii charset8 iso-8859-01  
siroe.com
```

## 추가 MTA 로깅 옵션 지정

로깅이 활성화되면 기본 정보가 항상 제공될 뿐 아니라 MTA 옵션 파일에 다양한 LOG\_\* MTA 옵션을 구성하여 선택적 정보 필드가 추가로 포함되도록 할 수 있습니다. IMTA 조정 파일(`msg_svr_base/config/imta_tailor`)에서 `IMTA_OPTION_FILE` 옵션을 사용하여 지정한 파일에서 MTA 옵션 파일을 지정합니다. 기본적으로 이 파일은 `msg_svr_base/config/option.dat`입니다.

MTA Option 파일에 대한 자세한 내용은 *Sun Java System Messaging Server Reference*(<http://docs.sun.com/doc/819-0106>)를 참조하십시오.

### ▶ MTA 로그를 syslog에 보내는 방법

1. MTA 옵션 파일을 편집합니다.
2. `LOG_MESSAGES_SYSLOG` 옵션을 1로 설정합니다.  
값 0이 기본값이며 syslog(이벤트 로그) 로깅이 수행되지 않음을 나타냅니다.

### ▶ 로그 메일 항목을 연관시키는 방법

1. MTA 옵션 파일을 편집합니다.
2. `LOG_MESSAGE_ID` 옵션을 1로 설정합니다.  
값 0이 기본값이며 메일 아이디가 `mail.log` 파일에 저장되지 않음을 나타냅니다.

### ▶ 메일 전달 재시도 횟수를 식별하는 방법

1. MTA 옵션 파일을 편집합니다.
2. `LOG_FILENAME` 옵션을 1로 설정합니다.  
이 옵션을 사용하면 특정 메일 파일의 전달이 재시도된 횟수를 곧바로 쉽게 알 수 있습니다. 또한 이 옵션을 사용하면 MTA가 여러 수신자를 대상으로 하는 메일을 디스크 상에서 개별 메일 파일 복사본으로 분할하거나 분할하지 않은 경우를 식별할 수 있습니다.

### ▶ TCP/IP 연결을 기록하는 방법

1. MTA 옵션 파일을 편집합니다.

## 2. LOG\_CONNECTION 옵션을 설정합니다.

이 옵션을 사용하면 MTA는 메일 트래픽 뿐만 아니라 TCP/IP 연결을 기록합니다. 연결 로그 항목은 기본적으로 mail.log\* 파일에 기록됩니다. 또는 연결 로그 항목을 connection.log\* 파일에 기록할 수도 있습니다. 자세한 내용은 SEPARATE\_CONNECTION\_LOG 옵션을 참조하십시오.

### ▶ 항목을 connection.log 파일에 기록하는 방법

1. MTA 옵션 파일을 편집합니다.
2. SEPARATE\_CONNECTION\_LOG 옵션을 1로 설정합니다.

연결 로그 항목을 connection.log 파일에 대신 기록하도록 지정하려면 이 옵션을 사용합니다. 기본값 0을 사용하면 연결 로깅이 MTA 로그 파일에 저장됩니다.

### ▶ 프로세스 아이디로 로그 메시지를 연관시키는 방법

1. MTA 옵션 파일을 편집합니다.
2. LOG\_PROCESS 옵션을 설정합니다.

이 옵션을 LOG\_CONNECTION과 함께 사용하면 연결 항목과 메일 항목을 프로세스 아이디로 연관시킬 수 있습니다.

### ▶ 메일을 대기열에 포함시키는 프로세스에 연관된 사용자 아이디를 mail.log 파일에 저장하는 방법

1. MTA 옵션 파일을 편집합니다.
2. LOG\_USERNAME 옵션을 설정합니다.

이 옵션은 메일을 대기열에 포함시키는 프로세스에 연관된 아이디를 mail.log 파일에 저장할지 여부를 제어합니다. SASL(SMTP AUTH)이 사용된 SMTP 제출의 경우 아이디 필드는 인증된 아이디(앞에 별표 문자가 접두사로 붙음)가 됩니다.

## MTA 메일 로깅 예

MTA 메일 파일에 기록되는 정확한 필드 형식 및 필드 목록은 설정하는 로깅 옵션에 따라 다릅니다. 이 절에서는 일반적인 로그 항목의 몇 가지 예를 보여 줍니다. 추가적인 옵션 필드에 대한 설명은 [734페이지의 "추가 MTA 로깅 옵션 지정"](#)을 참조하십시오.

---

**주** 인쇄상의 이유로 로그 파일 항목이 여러 행으로 표시되어 있지만 실제 로그 파일 항목은 한 항목당 한 행으로 표시됩니다.

---

로그 파일을 검토하는 경우, 일반적인 시스템에서는 많은 메일이 한 번에 처리된다는 점에 유의하십시오. 일반적으로 특정 메일에 관련된 항목은 같은 시간에 처리되고 있는 다른 메일과 관련된 항목 간에 섞여 있습니다. 기본 로깅 정보는 MTA를 통해 이동하는 전체 메일을 이해하는 데 적합합니다.

같은 메일에 관련된 특정 항목을 같은 수신자에게 연관시키려면 LOG\_MESSAGE\_ID를 활성화합니다. 특정 메일을 MTA 대기열 영역의 특정 파일과 연관시키거나, 아직 성공적으로 대기열에서 제외되지 않은 메일의 배달 시도가 몇 번 있었는지 알아내려면 LOG\_FILENAME을 활성화합니다. SMTP 메일의 경우(TCP/IP 채널을 통해 처리됨) 원격 시스템의 TCP 연결을 전송된 메일과 연관시키려면 LOG\_PROCESS와 LOG\_CONNECTION의 몇 가지 수준을 활성화합니다.

### MTA 로깅 예: 사용자가 보내는 메일 전송

아래 예는 로컬 사용자가 보내는 TCP/IP 채널(예: 인터넷)로 메일을 전송하는 경우 볼 수 있는 로그 항목의 기본 예를 보여 줍니다. 이 예에서는 LOG\_CONNECTION이 활성화되어 있습니다. (1)과 (2)로 표시된 행은 하나의 항목입니다. 실제 로그 파일에서는 한 행으로 표시됩니다. 마찬가지로 (3) - (7)로 표시된 행도 하나의 항목이며 실제로 한 행으로 표시됩니다.

#### 코드 예 21-1

로깅: 로컬 사용자가 보내는 메일 전송

```
19-Jan-1998 19:16:57.64 1          tcp_local    E 1 (1)
adam@sesta.com rfc822;marlowe@siroe.com marlowe@siroe.com (2)

19-Jan-1998 19:17:01.16 tcp_local          D 1 (3)
adam@sesta.com rfc822;marlowe@siroe.com marlowe@siroe.com (4)
dns;thor.siroe.com
(TCP|206.184.139.12|2788|192.160.253.66|25) (5)
(THOR.SIROE.COM -- Server ESMTP [iMS V5.0 #8694]) (6)
smtp;250 2.1.5 marlowe@siroe.com and options OK. (7)
```

1. 이 행은 한(1) 블록 메일의 1 채널부터 tcp\_local 채널까지의 대기열에 포함(E) 날짜 및 시간을 표시합니다.



2. 이 부분은 로그 파일에서 (1)과 같은 행의 일부이며 여기서는 인쇄 편의상 별도의 행으로 표시했습니다. 이것은 봉투의 **From:** 주소(이 경우에는 adam@sesta.com)와 봉투의 **From:** 주소의 원래 버전과 현재 버전(이 경우 marlowe@siroe.com)을 나타냅니다.
3. 이 행은 (1) 블록 메일의 tcp\_local 채널의 대기열에서 제외(D) 날짜와 시간을 표시합니다. 즉 tcp\_local 채널에 의한 일부 원격 SMTP 서버로의 성공적 전송을 표시합니다.
4. 봉투의 **From:** 주소, 원래 봉투의 **To:** 주소 및 봉투의 **To:** 주소의 현재 형식을 표시합니다.
5. 연결이 이루어진 실제 시스템의 이름이 DNS에서 thor.siroe.com이며, 로컬 전송 시스템의 IP 주소가 206.184.139.12이고 포트 2788에서 전송되고, 원격 대상 시스템의 IP 주소가 192.160.253.66이고 원격 대상 시스템의 연결 포트는 포트 25임을 보여 줍니다.
6. 원격 SMTP 서버의 SMTP 배너 행을 표시합니다.
7. 이 주소에 대해 반환된 SMTP 상태 코드를 표시합니다. 250은 기본 SMTP 성공 코드이며 이 원격 SMTP 서버는 확장된 SMTP 상태 코드와 추가 텍스트로 응답합니다.

## MTA 로깅 예: 옵션 로깅 필드

코드 예 21-2는 코드 예 21-3과 비슷한 로깅 항목을 보여 주지만, LOG\_FILENAME=1과 LOG\_MESSAGE\_ID=1을 설정하여(파일 이름과 메일 아이디 표시) 기록된 추가 정보를 함께 표시합니다. (1)과 (2)를 참조하십시오. 특히 메일 아이디를 사용하여 항목과 메일을 연관시킬 수 있습니다.

**코드 예 21-2**                      로깅: 옵션 로깅 필드 포함

```
19-Jan-1998 19:16:57.64 1                tcp_local      E 1
adam@sesta.com rfc822;marlowe@siroe.com marlowe@siroe.com
/imta/queue/tcp_local/ZZ01ISKLSK LZLI90N15M.00
<01ISKLSKC2QC90N15M@sesta.com> (1)

19-Jan-1998 19:17:01.16 tcp_local      D 1
adam@sesta.com rfc822;marlowe@siroe.com marlowe@siroe.com
/imta/queue/tcp_local/Z01ISKLSK LZLI90N15M.00
<01ISKLSKC2QC90N15M@sesta.com> (2)
dns;thor.siroe.com (TCP|206.184.139.12|2788|192.160.253.66|25)
(THOR.SIROE.COM -- Server ESMTP [iMS V5.0 #8694])
smtp;250 2.1.5 marlowe@siroe.com and options OK.
```

## MTA 로깅 예: 목록으로 전송

739페이지의 코드 예 21-3은 LOG\_FILENAME=1, LOG\_MESSAGE\_ID=1 및 LOG\_CONNECTION=1을 활성화하여 여러 수신자에게 전송하는 예를 보여 줍니다. 여기서 사용자 adam@sesta.com은 MTA 메일 목록 test-list@sesta.com으로 전송하였고 이 메일 목록은 bob@sesta.com, carol@varrius.com 및 david@varrius.com으로 확장됩니다. 현재 봉투의 To: 주소는 각각의 해당 주소이지만 원래 봉투의 To: 주소는 각 수신자에 대해 test-list@sesta.com이라는 것에 주의합니다. 두 개의 별도 파일(1 채널에 대해 하나, tcp\_local 채널에서 나가는 파일 하나)이 관련되어 있지만 메일 아이디는 동일하게 유지됩니다.

**코드 예 21-3**

로깅: 목록으로 전송

```

19-Jan-1998 20:01:44.10 1 1 E 1
adam@sesta.com rfc822;test-list@sesta.com bob
imta/queue/1/ZZ01ISKND3DE1K90N15M.00
<01ISKND2H8MS90N15M@sesta.com>

19-Jan-1998 20:01:44.81 1 tcp_local E 1
adam@sesta.com rfc822;test-list@sesta.com carol@varrius.com
imta/queue/tcp_local/ZZ01ISKND2WS1I90N15M.00
<01ISKND2H8MS90N15M@sesta.com>

19-Jan-1998 20:01:44.81 1 tcp_local E 1
adam@sesta.com rfc822;test-list@sesta.com david@varrius.com
imta/queue/tcp_local/ZZ01ISKND2WS1I90N15M.00
<01ISKND2H8MS90N15M@sesta.com>

19-Jan-1998 20:01:50.69 1 D 1
adam@sesta.com rfc822;test-list@sesta.com bob
imta/queue/1/ZZ01ISKND3DE1K90N15M.00
<01ISKND2H8MS90N15M@sesta.com>

19-Jan-1998 20:01:57.36 tcp_local D 1
adam@sesta.com rfc822;test-list@sesta.com carol@varrius.com
imta/queue/tcp_local/ZZ01ISKND2WS1I90N15M.00
<01ISKND2H8MS90N15M@sesta.com>
dns;gw.varrius.com (TCP|206.184.139.12|2788|192.160.253.66|25)
(gw.varrius.com -- SMTP Sendmail)
smtp;250 OK.

19-Jan-1998 20:02:06.14 tcp_local D 1
adam@sesta.com rfc822;test-list@sesta.com david@varrius.com
imta/queue/tcp_local/ZZ01ISKND2WS1I90N15M.00
<01ISKND2H8MS90N15M@sesta.com>
dns;gw.varrius.com (TCP|206.184.139.12|2788|192.160.253.66|25)
(gw.varrius.com -- SMTP Sendmail)
smtp;250 OK.

```

**MTA 로깅 예: 존재하지 않는 도메인으로 전송**

741페이지의 코드 예 21-4는 존재하지 않는 도메인(여기에서는 `very.bogus.com`)으로의 전송 시도를 보여 줍니다. 즉, MTA의 다시 쓰기 규칙에 의해 존재하지 않는 것으로 알려지지 않으며 MTA가 보내는 TCP/IP 채널에 일치하는 도메인 이름으로 전송을 시도합니다. 이 예에서는 MTA 옵션을 `LOG_FILENAME=1` 및 `LOG_MESSAGE_ID=1`로 설정한 것으로 가정합니다.

TCP/IP 채널이 실행되어 DNS에서 도메인 이름을 검사할 때 DNS는 이름이 존재하지 않는다는 오류를 반환합니다. (5)에 있는 "rejection" 항목(R)과 (6)에 있는 유효한 도메인 이름이 아니라는 오류를 반환하는 DNS를 주의하십시오.

메일이 제출된 뒤 주소가 거부되었기 때문에 MTA는 원래 전송자에게 바운스 메일을 생성합니다. MTA는 새 거부 메일을 원래의 전송자(1)에게 보내도록 대기열에 포함시키고 복사본은 포스트마스터에게 전송한 다음(4) 원래의 아웃바운드 메일을 삭제합니다((5)에 있는 R 항목).

바운스 메일 등의 알림 메일에는 봉투의 From: 필드가 빈 공간으로 표시되어 있는 빈 봉투의 From: 주소(2) 및 (8))가 있습니다. MTA가 생성한 바운스 메일의 초기 포함된 대기열은 새 알림 메일의 아이디와 원래 메일의 아이디(3)를 보여 줍니다. 이러한 정보가 항상 MTA에 사용 가능한 것은 아니지만 기록할 수 있는 경우에는 아웃바운드 실패 메일에 해당하는 로그 항목을 결과 알림 메일에 해당하는 로그 항목에 연관시킬 수 있도록 해줍니다. 이러한 알림 메일은 프로세스 채널의 대기열에 포함되고 그런 다음 적절한 대상 채널(7)의 대기열에 포함됩니다.

**코드 예 21-4**

로그: 존재하지 않는 도메인으로 전송

```

19-JAN-1998 20:49:04 1          tcp_local      E 1
adam@sesta.com rfc822;user@very.bogus.com user@very.bogus.com
imta/queue/tcp_local/ZZ01ISKP0S0LVQ94DU0K.00
<01ISKP0RYMAS94DU0K@SESTA.COM>

19-JAN-1998 20:49:33 tcp_local      process      E 1          (1)
rfc822;adam@sesta.com adam@sesta.com          (2)
imta/queue/process/ZZ01ISKP0S0LVQ94DTZB.00
<01ISKP22MW8894DTAS@SESTA.COM>, <01ISKP0RYMAS94DU0K@SESTA.COM> (3)

19-JAN-1998 20:49:33 tcp_local      process      E 1          (4)
rfc822;postmaster@sesta.com postmaster@sesta.com
imta/queue/process/ZZ01ISKP0S0LVQ94DTZB.00
<01ISKP22MW8894DTAS@SESTA.COM>, <01ISKP0RYMAS94DU0K@SESTA.COM>

19-JAN-1998 20:50:07 tcp_local          R 1          (5)
adam@sesta.com rfc822;user@very.bogus.com user@very.bogus.com
imta/queue/tcp_local/ZZ01ISKP0S0LVQ94DU0K.00
<01ISKP0RYMAS94DU0K@SESTA.COM>
Illegal host/domain name found          (6)

19-JAN-1998 20:50:08 process      1          E 3          (7)
rfc822;adam@sesta.com adam          (8)
imta/queue/1/ZZ01ISKP23BUQS94DTYL.00
<01ISKP22MW8894DTAS@SESTA.COM>

19-JAN-1998 20:50:08 process      1          E 3
rfc822;postmaster@sesta.com postmaster
imta/queue/1/ZZ01ISKP23BUQS94DTYL.00
<01ISKP22MW8894DTAS@SESTA.COM>

19-JAN-1998 20:50:12 1          D 3
rfc822;adam@sesta.com adam
imta/queue/1/ZZ01ISKP23BUQS94DTYL.00
<01ISKP22MW8894DTAS@SESTA.COM>

19-JAN-1998 20:50:12 1          D 3
rfc822;postmaster@sesta.com postmaster
imta/queue/1/ZZ01ISKP23BUQS94DTYL.00
<01ISKP22MW8894DTAS@SIROE.COM>

```

### MTA 로깅 예: 존재하지 않는 원격 사용자에게 전송

743페이지의 코드 예 21-5는 원격 시스템의 잘못된 주소로 전송을 시도하는 예입니다. 이 예에서는 MTA 옵션 설정이 LOG\_FILENAME=1 및 LOG\_MESSAGE\_ID=1이고 채널 옵션 설정이 LOG\_BANNER=1 및 LOG\_TRANSPORTINFO=1인 것으로 가정합니다. (1)에 있는 거부 항목 (R)에 주의하십시오. 하지만 741페이지의 코드 예 21-4의 거부 항목과는 대조적으로 여기에 있는 거부 항목은 원격 시스템으로 연결되었음을 보여주고 원격 SMTP 서버, (2) 및 (3)에 의해 발생한 SMTP 오류 코드를 보여 줍니다. (2)에 있는 정보가 포함된 이유는 채널 옵션이 LOG\_BANNER=1 및 LOG\_TRANSPORTINFO=1로 설정되었기 때문입니다.

**코드 예 21-5**

로그: 존재하지 않는 원격 사용자에게 전송

```

20-JAN-1998 13:11:05 1          tcp_local      E 1
adam@sesta.com rfc822;nonesuch@siroe.com nonesuch@siroe.com
imta/queue/tcp_local/ZZ01ISLNBB1JOE94DUWH.00
<01ISLNBAWV3094DUWH@sesta.com>

20-JAN-1998 13:11:08 tcp_local      process      E 1
rfc822;adam@sesta.com adam@sesta.com
imta/queue/process/ZZ01ISLNBB1JOE94DSGB.00
<01ISLNBFKIDS94DUJ8@sesta.com>, <01ISLNBAWV3094DUWH@sesta.com>

20-JAN-1998 13:11:08 tcp_local      process      E 1
rfc822;postmaster@sesta.com postmaster@sesta.com
imta/queue/process/ZZ01ISLNBB1JOE94DSGB.00
<01ISLNBFKIDS94DUJ8@sesta.com>, <01ISLNBAWV3094DUWH@sesta.com>

20-JAN-1998 13:11:11 tcp_local          R 1      (1)
adam@sesta.com rfc822;nonesuch@siroe.com nonesuch@siroe.com
imta/queue/tcp_local/ZZ01ISLNBB1JOE94DUWH.00
<01ISLNBAWV3094DUWH@sesta.com>
dns;thor.siroe.com
(TCP|206.184.139.12|2788|192.160.253.66|25)      (2)
(THOR.SIROE.COM -- Server ESMTP [iMS V5.0 #8694])
smtp; 553 unknown or illegal user: nonesuch@siroe.com      (3)

20-JAN-1998 13:11:12 process      1          E 3
rfc822;adam@sesta.com adam
imta/queue/1/ZZ01ISLNBGND1094DQDP.00
<01ISLNBFKIDS94DUJ8@sesta.com>

20-JAN-1998 13:11:12 process      1          E 3
rfc822;postmaster@sesta.com postmaster
imta/queue/1/ZZ01ISLNBGND1094DQDP.00
<01ISLNBFKIDS94DUJ8@sesta.com>

20-JAN-1998 13:11:13 1          D 3
rfc822;adam@sesta.com adam@sesta.com
imta/queue/1/ZZ01ISLNBGND1094DQDP.00
<01ISLNBFKIDS94DUJ8@sesta.com>

20-JAN-1998 13:11:13 1          D 3
rfc822;postmaster@sesta.com postmaster@sesta.com
imta/queue/1/ZZ01ISLNBGND1094DQDP.00
<01ISLNBFKIDS94DUJ8@sesta.com>

```

## MTA 로깅 예: 원격측의 메일 제출 시도 거부

**코드 예 21-6**은 MTA가 원격 메일 제출 시도를 거부할 때 발생하는 로그 파일 항목을 보여 줍니다. 이 예에서는 선택적인 LOG\_\* 옵션을 활성화하지 않은 것으로 간주하므로 항목에 기본적인 필드가 기록됩니다. 특히 LOG\_CONNECTION 옵션을 활성화하면 J 항목 등과 같은 추가 필드가 표시됩니다. 이 경우에는 다음을 포함하여 ORIG\_SEND\_ACCESS 매핑을 사용하여 SMTP 릴레이 차단을 설정한(531페이지의 "SMTP 릴레이 차단 구성" 참조) MTA에 대한 예입니다.

```
ORIG_SEND_ACCESS
```

```
! ...numerous entries omitted...
!
```

```
tcp_local|*|tcp_local|* $NRelaying$ not$ permitted
```

여기서 alan@very.bogus.com은 내부 주소가 아닙니다. 따라서 원격 사용자 harold@varrius.com이 MTA 시스템을 통해 원격 사용자 alan@very.bogus.com에게 릴레이하려는 시도는 거부됩니다.

### 코드 예 21-6 로깅: 원격측의 메일 제출 시도 거부

|                                                       |     |     |
|-------------------------------------------------------|-----|-----|
| 28-May-1998 12:02:23 tcp_local                        | J 0 | (1) |
| harold@varrius.com rfc822; alan@very.bogus.com        |     | (2) |
| 550 5.7.1 Relaying not permitted: alan@very.bogus.com |     | (3) |

1. 이 로그는 MTA가 원격측의 메일 제출 시도를 거부한 날짜와 시간을 보여 줍니다. 거부는 J 레코드에서 표시합니다. MTA 채널이 거부된 메일을 전송하려고 시도하는 경우는 코드 예 21-4 및 코드 예 21-5에서 볼 수 있는 것처럼 R 레코드에서 표시합니다.

---

**주** 로그에 기록된 마지막 J 레코드에는 지정된 세션에 대한 마지막 레코드는 표시가 있습니다. 또한 현재 버전의 Messaging Server에서는 J 레코드 수에 제한이 없습니다.

---

2. 시도된 봉투의 From: 및 To: 주소가 표시됩니다. 이 경우 원래 봉투의 To: 정보를 사용할 수 없으므로 해당 필드가 비어 있습니다.
3. 해당 항목에는 MTA가 원격측(전송을 시도한 보낸 사람)에게 발행한 SMTP 오류 메시지가 포함됩니다.



## MTA 로깅 예: 복수 전달 시도

**코드 예 21-7**은 첫 번째 시도에서 메일을 배달을 할 수 없어서 MTA가 메일 전송을 여러 번 시도한 경우의 로그 파일 항목입니다. 이 예에서는 옵션이 LOG\_FILENAME=1 및 LOG\_MESSAGE\_ID=1으로 구성되었다고 가정합니다.

**코드 예 21-7**                      로깅: 복수 전달 시도

```

15-Jan-1998 10:31:05.18 tcp_internal tcp_local E 3 (1)
adam@hosta.sesta.com rfc822;user@some.org user@some.org
imta/queue/tcp_local/ZZ01IS3D2ZP7FQ9UN54R.00
<01IRUD7SVA3Q9UN2D4@sesta.com>

15-Jan-1998 10:31:10.37 tcp_local Q 3 (2)
adam@hosta.sesta.com rfc822;user@some.org user@some.org
imta/queue/tcp_local/ZZ01IS3D2ZP7FQ9UN54R.00 (3)
<01IRUD7SVA3Q9UN2D4@sesta.com>
TCP active open: Failed connect() Error: no route to host (4)

...several hours worth of entries...

15-Jan-1998 12:45:39.48 tcp_local Q 3 (5)
adam@hosta.sesta.com rfc822;user@some.org user@some.org
imta/queue/tcp_local/ZY01IS3D2ZP7FQ9UN54R.00 (6)
<01IRUD7SVA3Q9UN2D4@sesta.com>
TCP active open: Failed connect() Error: no route to host

...several hours worth of entries...

15-Jan-1998 16:45:24.72 tcp_local Q 3
adam@hosta.sesta.com rfc822;user@some.org user@some.org
imta/queue/tcp_local/ZX01IS67NY4RRK9UN7GP.00 (7)
<01IRUD7SVA3Q9UN2D4@sesta.com>
TCP active open: Failed connect() Error: connection refused (8)

...several hours worth of entries...

15-Jan-1998 20:45:51.55 tcp_local D 3 (9)
adam@hosta.sesta.com rfc822;user@some.org user@some.org
imta/queue/tcp_local/ZX01IS67NY4RRK9UN7GP.00
<01IRUD7SVA3Q9UN2D4@sesta.com>
dns;host.some.org (TCP|206.184.139.12|2788|192.1.1.1|25)
(All set, fire away)
smtp; 250 Ok

```

1. 메일은 tcp\_internal 채널로 보내집니다. 일반적으로 POP 또는 IMAP 클라이언트 또는 MTA를 SMTP 릴레이로 사용하여 조직 내의 다른 호스트가 보내는 것이며, MTA는 이것을 보내는 tcp\_local 채널의 대기열에 포함시킵니다.
2. Q 항목에 표시되어 있는 것처럼 첫 번째 전달 시도는 실패했습니다.
3. 이는 zz\* 파일 이름에서 볼 수 있는 첫 번째 전달 시도입니다.
4. TCP/IP 패키지가 원격측으로의 경로를 찾을 수 없어서 이 전달 시도는 실패했습니다. [741페이지의 코드 예 21-4](#)와는 반대로 DNS가 대상 도메인 이름인 some.org의 문제를 나타내는 것이 아니라, "no route to host" 오류 메시지가 전송측과 수신측 사이에 어떤 네트워크 문제가 있음을 나타냅니다.
5. MTA 주기적 작업이 다음에 전달을 재시도하면 또 실패하게 됩니다.
6. 이제 파일 이름은 두 번째 시도임을 나타내는 zy\*로 바뀝니다.
7. 세 번째로 시도가 실패한 경우 파일 이름은 zx\*입니다.
8. 다음에 주기적 작업이 재시도하는 전달이 실패하면, 이번에는 TCP/IP 패키지가 원격 SMTP 서버에 도달할 수 없다고 표시하는 것이 아니라 원격 SMTP 서버가 연결을 설정하지 않음을 나타냅니다. 원격측에서 네트워크 문제는 해결했지만 아직 SMTP 서버를 실행하지 않았을 수 있습니다. 즉, 해당 SMTP 서버가 다른 메일을 처리할 수 없어서 MTA가 연결을 시도할 때 그 연결을 설정하지 못했을 수 있습니다.
9. 마지막으로 메일이 대기열에서 제외됩니다.

### MTA 로깅 예: 변환 채널을 통해 라우팅된 받는 SMTP 메일

[747페이지의 코드 예 21-8](#)은 메일이 변환 채널을 통해 경로 지정되는 경우를 보여 줍니다. 해당 사이트에는 다음과 같은 CONVERSIONS 매핑 테이블이 있는 것으로 가정합니다.

CONVERSIONS

```
IN-CHAN=tcp_local;OUT-CHAN=1;CONVERT    Yes
```

이 예에서는 옵션이 LOG\_FILENAME=1 및 LOG\_MESSAGE\_ID=1로 구성되었다고 가정합니다.

**코드 예 21-8**                      로깅: 변환 채널을 통해 라우팅된 받는 SMTP 메일

```

04-Feb-1998 00:06:26.72 tcp_local    conversion    E 9 (1)
amy@siroe.edu rfc822;bert@sesta.com bert@sesta.com
imta/queue/conversion/ZZ01IT5UAMZ4QW985180.00
<01IT5UALL144985180@siroe.edu>

04-Feb-1998 00:06:29.06 conversion    1                E 9 (2)
amy@siroe.edu rfc822;bert@sesta.com bert
imta/queue/1/ZZ01IT5UAOXLDW98509E.00 <01IT5STUMUFO984Z8L@siroe.edu>

04-Feb-1998 00:06:29.31 conversion                D 9 (3)
amy@siroe.edu rfc822;bert@sesta.com bert
imta/queue/conversion/ZZ01IT5UAMZ4QW985180.00
<01IT5UALL144985180@siroe.edu>

04-Feb-1998 00:06:32.62 1                D 9 (4)
amy@siroe.edu rfc822;bert@siroe.com bert
imta/queue/1/ZZ01IT5UAOXLDW98509E.00
<01IT5STUMUFO984Z8L@siroe.edu>

```

1. 외부 사용자 amy@siroe.edu가 보낸 메일은 1 채널 수신자 bert@sesta.com으로 주소 지정됩니다. 하지만 CONVERSIONS 매핑 항목 때문에 메일은 초기에 변환 채널의 대기열에 포함됩니다(1 채널로 직접 전송되지 않음).
2. 변환 채널이 실행되고 메일을 1 채널 대기열에 포함시킵니다.
3. 그런 다음에는 변환 채널이 메일을 대기열에서 제외할 수 있습니다(오래된 메일 파일 삭제).
4. 그리고 마지막으로 1 채널이 메일을 대기열에서 제외(전달)합니다.

**MTA 로깅 예: 아웃바운드 연결 로깅**

748페이지의 코드 예 21-9는 LOG\_CONNECTION=3을 통해 연결 로깅이 활성화된 경우 보내는 메일에 대한 로그 출력을 보여 줍니다. 이 예에서도 LOG\_PROCESS=1, LOG\_MESSAGE\_ID=1, LOG\_FILENAME=1이라고 가정합니다. 이 예는 사용자 adam@sesta.com 이 세 명의 수신자(bobby@hosta.sesta.com, carl@hosta.sesta.com 및 dave@hostb.sesta.com)에게 같은 메일을 보내는 경우를 보여 줍니다(각 메일 사본의 메일 아이디는 동일함). 이 예에서는 일반적으로 채널이 그러하듯이 single\_sys 채널 키워드로 표시된 tcp\_local 채널로 메일이 나가는 것으로 가정합니다. 따라서 (1), (2), (3)에서

볼 수 있듯이 각 수신자 집합에 대해 별도의 메일 파일이 디스크에 별도의 호스트 이름으로 생성됩니다. 여기서 bobby@hosta.sesta.com 및 carl@hosta.sesta.com 수신자는 같은 메일 파일에 저장되지만 dave@hostb.sesta.com 수신자는 다른 메일 파일에 저장됩니다.

**코드 예 21-9**                      로깅: 아웃바운드 연결 로깅

```

19-Feb-1998 10:52:05.41 1e488.0 1          tcp_local    E 1
adam@sesta.com rfc822;bobby@hosta.sesta.com bobby@hosta.sesta.com
imta/queue/tcp_local/ZZ01ITRF7B0388000FCN.00          (1)
<01ITRF7BDHS6000FCN@SESTA.COM>

19-Feb-1998 10:52:05.41 1e488.0 1          tcp_local    E 1
adam@sesta.com rfc822;carl@hosta.sesta.com carl@hosta.sesta.com
imta/queue/tcp_local/ZZ01ITRF7B0388000FCN.00          (2)
<01ITRF7BDHS6000FCN@SESTA.COM>

19-Feb-1998 10:52:05.74 1e488.1 1          tcp_local    E 1
adam@sesta.com rfc822;dave@hostb.sesta.com dave@hostb.sesta.com
imta/queue/tcp_local/ZZ01ITRF7C11FU000FCN.00          (3)
<01ITRF7BDHS6000FCN@SESTA.COM>

19-Feb-1998 10:52:10.79 1f625.2.0 tcp_local    -              O (4)
TCP|206.184.139.12|5900|206.184.139.66|25
SMTP/hostb.sesta.com/mailhub.sesta.com                (5)

19-Feb-1998 10:52:10.87 1f625.3.0 tcp_local    -              O (6)
TCP|206.184.139.12|5901|206.184.139.70|25
SMTP/hosta.sesta.com/hosta.sesta.com                  (7)

19-Feb-1998 10:52:12.28 1f625.3.1 tcp_local    D 1
adam@sesta.com rfc822;bobby@hosta.sesta.com bobby@hosta.sesta.com
imta/queue/tcp_local/ZZ01ITRF7B0388000FCN.00
<01ITRF7BDHS6000FCN@SESTA.COM>
hosta.sesta.com dns;hosta.sesta.com                  (8)
(TCP|206.184.139.12|5901|206.184.139.70|25)
(hosta.sesta.com -- Server ESMTP [ims V5.0 #8790])
(TCP|206.184.139.12|5901|206.184.139.70|25)
smtp;250 2.1.5 bobby@hosta.sesta.com and options OK.

19-Feb-1998 10:52:12.28 1f625.3.1 tcp_local    D 1
adam@sesta.com rfc822;carl@hosta.sesta.com carl@hosta.sesta.com
imta/queue/tcp_local/ZZ01ITRF7B0388000FCN.00
<01ITRF7BDHS6000FCN@SESTA.COM>
hosta.sesta.com dns;hosta.sesta.com
(TCP|206.184.139.12|5901|206.184.139.70|25)
(hosta.sesta.com -- Server ESMTP [ims V5.0 #8790])
(TCP|206.184.139.12|5901|206.184.139.70|25)
smtp;250 2.1.5 carl@hosta.sesta.com and options OK.

19-Feb-1998 10:52:12.40 1f625.3.2 tcp_local    -              C (9)
TCP|206.184.139.12|5901|206.184.139.70|25
SMTP/hosta.sesta.com/hosta.sesta.com

```

```

19-Feb-1998 10:52:13.01 1f625.2.1 tcp_local          D 1
adam@sesta.com rfc822;dave@hostb.sesta.com dave@hostb.sesta.com
imta/queue/tcp_local/ZZ01ITRF7C11FU000FCN.00
<01ITRF7BDHS6000FCN@SESTA.COM>
mailhub.sesta.com dns;mailhub.sesta.com
(TCP|206.184.139.12|5900|206.184.139.66|25)
(MAILHUB.SEESTA.COM -- Server ESMTP [ims V5.0 #8694])
(TCP|206.184.139.12|5900|206.184.139.66|25)
smtp;250 2.1.5 dave@hostb.sesta.com and options OK.

19-Feb-1998 10:52:13.05 1f625.2.2 tcp_local          -          C (10)
TCP|206.184.139.12|5900|206.184.139.66|25
SMTP/hostb.sesta.com/mailhub.sesta.com

```

1. 메일이 첫 번째 수신자의 대기열에 포함됩니다.
2. 그리고 두 번째 수신자의 대기열에 포함됩니다.
3. 그리고 세 번째 수신자의 대기열에 포함됩니다.
4. LOG\_CONNECTION=3으로 설정하면 MTA가 이 항목을 기록합니다. 마이너스 기호(-)는 이 항목이 보내는 연결을 참조한다는 것을 나타냅니다. 0는 이 항목이 연결 열기에 해당한다는 것을 나타냅니다. 이러한 별도의 연결을 열 때 다중 스레드 TCP/IP 채널에 같은 프로세스가 사용되기 때문에(열기는 스레드 2 및 스레드 3에 의해 수행되지만) 여기서 프로세스 아이디는 모두 1f625임을 알 수 있습니다.
5. 두 개의 개별적인 원격 시스템에 연결해야 하기 때문에 별도 스레드의 다중 스레드 SMTP 클라이언트는 각각(이 항목에서는 첫 번째, 7에 표시된 두 번째)에 대한 연결을 엽니다. 이 항목 부분은 전송 및 대상 IP 번호와 포트 번호를 표시하며 초기 호스트 이름 및 DNS 조회로 발견된 호스트 이름을 표시합니다. SMTP/initial-host/dns-host 절에서는 초기 호스트 이름이 모두 표시되며, 초기 호스트 이름에 대한 DNS MX 레코드 조회를 수행한 뒤에 사용된다는 것을 알 수 있습니다. mailhub.sesta.com은 hostb.sesta.com의 MX 서버입니다.
6. 다중 스레드 SMTP 클라이언트는 동일한 프로세스를 통해 별도의 스레드에서 두 번째 시스템에 대한 연결을 엽니다.
7. 두 개의 개별적인 원격 시스템에 연결해야 하기 때문에 별도 스레드의 다중 스레드 SMTP 클라이언트는 각각에 대해(이 항목에서는 두 번째, 5에 표시된 첫 번째) 연결을 엽니다. 이 항목 부분은 전송 및 대상 IP 번호와 포트 번호를 표시하며 초기 호스트 이름 및 DNS 조회로 발견된 호스트 이름을 표시합니다. 이 예에서는 hosta.sesta.com 시스템이 직접 메일을 수신합니다.

8. 특정 연결 항목 이외에도 LOG\_CONNECTION=3으로 설정하면 여기에서 예로 표시하는 대로 정규 메일 항목에 연결 관련 정보가 포함됩니다.
9. LOG\_CONNECTION=3으로 설정하면 MTA는 이 항목을 기록합니다. 메일이 대기열에 포함된 뒤(이 예에서는 bobby와 carl 메일) 이 항목의 c에 표시하는 대로 연결이 닫힙니다.
10. LOG\_CONNECTION=3으로 설정하면 MTA는 이 항목을 기록합니다. 메일이 대기열에서 제외된 후(이 예에서는 dave 메일) 이 항목의 c에서 표시하는 대로 연결이 닫힙니다.

### MTA 로깅 예: 인바운드 연결 로깅

코드 예 21-10은 LOG\_CONNECTION=3을 통해 연결 로깅이 활성화된 경우 받는 SMTP 메일에 대한 로그 출력을 보여 줍니다.

**코드 예 21-10**                      로깅: 인바운드 연결 로깅

```

19-Feb-1998 17:02:08.70 tcp_local  +          O  (1)
TCP|206.184.139.12|25|192.160.253.66|1244 SMTP      (2)

19-Feb-1998 17:02:26.65 tcp_local  l          E 1
service@siroe.com rfc822;adam@sesta.com adam
THOR.SIROE.COM (THOR.SIROE.COM [192.160.253.66])    (3)

19-Feb-1998 17:02:27.05 tcp_local  +          C  (4)
TCP|206.184.139.12|25|192.160.253.66|1244 SMTP

19-Feb-1998 17:02:31.73 l          D 1
service@siroe.com rfc822;adam@sesta.com adam
    
```

1. 원격 시스템이 연결을 엽니다. o 문자는 이 항목이 연결 열기에 관련되어 있음을 나타냅니다. + 문자는 이 항목이 받는 연결에 관련되어 있음을 나타냅니다.
2. 연결에 대한 IP 번호와 포트가 표시됩니다. 이 항목에서 수신 시스템(로그 파일 항목을 만드는 시스템)의 IP 주소는 206.184.139.12이고 포트 25로 연결됩니다. 송신 시스템의 IP 주소는 192.160.253.66이고 포트 1244에서 전송됩니다.

3. 받는 TCP/IP 채널(tcp\_local)에서 1 채널 수신자로 메일을 대기열에 포함하는 항목에서는 LOG\_CONNECTION=3이 활성화되어 있기 때문에 기본값 이외의 정보를 포함할 수 있습니다. 특히 전송 시스템이 HELO 또는 EHLO 행에 표시한 이름, 연결 IP 번호에 대한 DNS 역조회로 발견된 전송 시스템 이름 및 전송 시스템의 IP 주소가 모두 기록되어 있습니다. 이 기능에 영향을 주는 채널 키워드에 대한 설명은 12장, "채널 정의 구성"을 참조하십시오.
4. 인바운드 연결이 닫힙니다. c 문자는 이 항목이 연결 닫기에 관련되어 있음을 나타냅니다. + 문자는 이 항목이 받는 연결에 관련되어 있음을 나타냅니다.

## 디스패처 디버깅 활성화

디스패처 오류 및 디버깅 출력(활성화된 경우)은 MTA 로그 디렉토리의 dispatcher.log 파일에 기록됩니다. 디스패처 구성 정보는 msg\_svr\_base/imta/dispatcher.cnf 파일에 지정됩니다. 기본 구성 파일은 설치 시 작성되며 변경 없이 사용할 수 있습니다. 그러나 보안이나 성능상의 이유로 기본 구성 파일을 수정하려는 경우 dispatcher.cnf 파일을 편집하여 원하는 사항을 수정할 수 있습니다

### ▶ 디스패처 오류 디버깅 출력을 활성화하는 방법

1. dispatcher.cnf 파일을 편집합니다.
2. DEBUG 옵션을 -1로 설정합니다.

또한 32비트 디버그 마스크를 16진수로 정의하는 논리 또는 환경 변수 IMTA\_DISPATCHER\_DEBUG(UNIX)를 FFFFFFFF 값으로 설정할 수 있습니다. 다음 표에는 각 비트의 의미가 설명되어 있습니다.

**표 21-3** 디스패처 디버깅 비트

| 비트 | 16진수 값  | 10진수 값 | 사용                   |
|----|---------|--------|----------------------|
| 0  | x 00001 | 1      | 기본 서비스 디스패처 주 모듈 디버깅 |
| 1  | x 00002 | 2      | 추가 서비스 디스패처 주 모듈 디버깅 |
| 2  | x 00004 | 4      | 서비스 디스패처 구성 파일 로깅    |
| 3  | x 00008 | 8      | 기본 서비스 디스패처 기타 디버깅   |
| 4  | x 00010 | 16     | 기본 서비스 디버깅           |

**표 21-3** 디스패처 디버깅 비트 (계속)

| 비트 | 16진수 값    | 10진수 값   | 사용                                      |
|----|-----------|----------|-----------------------------------------|
| 5  | x 00020   | 32       | 추가 서비스 디버깅                              |
| 6  | x 00040   | 64       | 프로세스 관련 서비스 디버깅                         |
| 7  | x 00080   | 128      | 사용되지 않습니다.                              |
| 8  | x 00100   | 256      | 기본 서비스 디스패처 및 프로세스 통신 디버깅               |
| 9  | x 00200   | 512      | 추가 서비스 디스패처 및 프로세스 통신 디버깅               |
| 10 | x 00400   | 1024     | 패킷 수준 통신 디버깅                            |
| 11 | x 00800   | 2048     | 사용되지 않습니다.                              |
| 12 | x 01000   | 4096     | 기본 작업자 프로세스 디버깅                         |
| 13 | x 02000   | 8192     | 추가 작업자 프로세스 디버깅                         |
| 14 | x 04000   | 16384    | 추가 작업자 프로세스 디버깅(특히 연결 핸드오프)             |
| 15 | x 08000   | 32768    | 사용되지 않습니다.                              |
| 16 | x 10000   | 65536    | 서비스 디스패처 I/O에 대한 기본 작업자 프로세스 디버깅        |
| 17 | x 20000   | 131072   | 서비스 디스패처 I/O에 대한 기타 작업자 프로세스 디버깅        |
| 20 | x 100000  | 1048576  | 기본 통계 디버깅                               |
| 21 | x 200000  | 2097152  | 추가 통계 디버깅                               |
| 24 | x 1000000 | 16777216 | dispatcher.log 파일에 대한 PORT_ACCESS 거부 기록 |

### ▶ 디스패처 매개 변수 설정 방법(Solaris)

디스패처 구성 파일에서 제공되는 디스패처 서비스는 다양한 시스템 매개 변수의 요구 사항에 영향을 미칩니다. 시스템의 힙 크기(datasize)는 디스패처의 스택드 스택을 사용하기에 충분해야 합니다.

1. 힙 크기(기본 datasize)를 표시하려면 다음 중 하나를 사용합니다.

csh 명령:

```
# limit
```

ksh 명령

```
# ulimit -a
```

Solaris 유틸리티

```
# sysdef
```



2. 각 디스패처 서비스에 대해  $STACKSIZE * MAX\_CONN$ s를 계산한 다음 각 서비스에 대해 계산된 값을 모두 더합니다. 시스템의 힙 크기는 이 숫자의 두 배 이상이 되어야 합니다.

## 서비스 로그 관리

이 절에서는 Message Store(POP, IMAP 및 HTTP), Admin 및 Default 서비스에 대한 로깅을 설명합니다. [725페이지의 표 21-1](#)을 참조하십시오.

이 서비스에 대해서는 콘솔을 사용하여 로그 설정을 지정하고 로그를 볼 수 있습니다. 지정하는 설정은 기록되는 이벤트 및 기록되는 이벤트의 수에 영향을 미칩니다. 로그 파일을 분석할 때 이러한 설정 및 기타 특성을 사용하여 기록되는 이벤트를 자세히 검색할 수 있습니다.

이 절에는 다음과 같은 하위 절이 포함됩니다.

- [서비스 로그 특징 이해](#)
- [서비스 로그 파일 형식 이해](#)
- [서비스 로깅 옵션 정의 및 설정](#)
- [서비스 로그 검색 및 보기](#)
- [메시지 저장소 로깅에 메일 추적 사용](#)
- [메시지 저장소 로깅 예](#)

### 서비스 로그 특징 이해

이 절에서는 메시지 저장소 및 관리 서비스에 대한 로깅 수준, 기록되는 이벤트 범주, 로그의 파일 이름 규칙, 로그 파일 디렉토리 등과 같은 로그 특징을 설명합니다.

#### 로깅 수준

로깅의 수준 또는 우선 순위는 로깅 작업 수행의 세밀도를 정의합니다. 우선 순위 수준이 높을수록 세밀도가 떨어집니다. 즉, 우선 순위가 높은(높은 심각도) 이벤트가 기록됩니다. 수준이 낮으면 세밀도가 높아집니다. 즉, 더 많은 이벤트가 로그 파일에 기록됩니다.

logfile.service.loglevel 구성 매개 변수(757페이지의 "서비스 로깅 옵션 정의 및 설정" 참조)를 사용하여 각 서버(POP, IMAP, HTTP, Admin 및 Default)마다 별도의 로깅 수준을 설정할 수 있습니다. 또한 로깅 수준을 사용하여 로그 이벤트에 대한 검색을 필터링할 수도 있습니다. 사용 가능한 수준은 표 21-4에서 설명합니다. 이러한 로깅 수준은 UNIX syslog 기능에 의해 정의된 수준의 하위 집합입니다.

**표 21-4** 저장소 및 관리 서비스의 로깅 수준

| 수준          | 설명                                                                                                       |
|-------------|----------------------------------------------------------------------------------------------------------|
| Critical    | 최소의 로깅 세밀도입니다. 서버 문제 또는 중요한 조건이 발생 (예: 서버가 메일함에 액세스할 수 없거나 서버를 실행하려면 라이브러리가 필요한 경우)할 때마다 이벤트가 로그에 기록됩니다. |
| Error       | 오류 조건(예: 클라이언트나 다른 서버에 대한 연결 시도가 실패한 경우)이 발생할 때마다 이벤트가 로그에 기록됩니다.                                        |
| Warning     | 경고 조건이 발생할 때마다(예: 클라이언트가 보낸 통신을 서버가 인식할 수 없는 경우) 이벤트가 로그에 기록됩니다.                                         |
| Notice      | 알림(일반적이지만 중요한 조건)이 발생할 때마다(예: 사용자 로그인 실패 또는 세션 종료시) 이벤트가 로그에 기록됩니다. 이는 기본 로그 수준입니다.                      |
| Information | 수행되는 모든 중요 작업(예: 사용자가 성공적으로 로그인했거나 메일함을 만들거나 메일함 이름을 변경한 경우)에 대한 이벤트를 로그에 기록합니다.                         |
| Debug       | 가장 세밀한 로깅입니다. 디버깅 용도에만 적합합니다. 문제를 나타내기 위해 각 프로세스나 작업 내의 개별 단계에서 이벤트가 로그에 기록됩니다.                          |

특정 로깅 수준을 선택하면 해당 수준과 그보다 높은(세밀도는 더 낮은) 모든 수준에 해당하는 이벤트가 기록됩니다. 기본 로깅 수준은 Notice입니다.

**주** 로깅을 세밀하게 지정할수록 로그 파일이 차지하는 디스크 공간은 많아 집니다. 이에 대한 지침은 757페이지의 "서비스 로깅 옵션 정의 및 설정"을 참조하십시오.

## 기록되는 이벤트의 범주

지원되는 각 서비스 또는 프로토콜 내에서 Messaging Server는 기능 또는 기능 영역에 따라 기록되는 이벤트를 범주화합니다. 기록되는 모든 이벤트에는 해당 이벤트를 생성한 기능의 이름이 포함됩니다. 이러한 범주는 검색 중에 이벤트를 필터링하는 데 도움이 됩니다. 표 21-5에는 로깅을 위해 Messaging Server가 인식하는 범주가 나열되어 있습니다.

**표 21-5** 로그 이벤트가 발생하는 범주

| 기능       | 설명                                                                     |
|----------|------------------------------------------------------------------------|
| General  | 이 프로토콜 또는 서비스에 관련된 구분되지 않은 작업입니다.                                      |
| LDAP     | LDAP 디렉토리 데이터베이스에 액세스하는 Messaging Server에 관련된 작업입니다.                   |
| Network  | 네트워크 연결에 관련된 작업(소켓 오류가 이 범주에 속함)입니다.                                   |
| Account  | 사용자 계정에 관련된 작업(사용자 로그인 이 범주에 속함)입니다.                                   |
| Protocol | 프로토콜별 명령에 관련된 프로토콜 수준 작업(POP, IMAP 또는 HTTP 기능에서 반환되는 오류가 이 범주에 속함)입니다. |
| Stats    | 서버 통계의 수집에 관련된 작업입니다.                                                  |
| Store    | 메시지 저장소 액세스에 관련된 낮은 수준의 작업(읽기/쓰기 오류가 이 범주에 속함)입니다.                     |

로그 검색에서 범주를 필터로 사용하는 예에 대해서는 [760페이지의 "서비스 로그 검색 및 보기"](#)를 참조하십시오.

## 서비스 로그 파일 디렉토리

기록되는 모든 서비스에는 로그 파일이 저장되는 하나의 디렉토리가 할당됩니다. 모든 POP 로그 파일과 기타 모든 서비스의 로그 파일과 마찬가지로 모든 IMAP 로그 파일이 함께 저장됩니다. 각 디렉토리의 위치를 정의할 수 있으며 디렉토리에 허용되는 로그 파일의 최대 크기와 수를 지정할 수 있습니다.

로그 파일을 모두 저장할 수 있을 만큼 저장소 용량이 충분한지 확인하십시오. 로그 데이터는 용량이 매우 커질 수 있습니다(특히 낮은 로깅 수준에서).

또한 모든 로그 파일 디렉토리가 백업되고 오버로드되지 않도록 로깅 수준, 로그 회전, 로그 만료 및 서버 백업 정책을 적절하게 정의해야 합니다. 그렇지 않으면 정보가 손실될 수 있습니다. [757페이지의 "서비스 로깅 옵션 정의 및 설정"](#)을 참조하십시오.

## 서비스 로그 파일 형식 이해

Messaging Server에 의해 생성된 모든 메시지 저장소와 관리 서비스 로그 파일의 내용 형식은 서로 동일합니다. 로그 파일은 여러 행의 텍스트 파일로, 각 행이 기록된 하나의 이벤트를 설명합니다. 지원되는 각 서비스에 대한 모든 이벤트 설명에는 다음과 같은 일반 형식이 있습니다.

```
dateTime hostName processName [pid] : category logLevel: eventMessage
```

표 21-6에는 로그 파일 구성 요소가 나열되어 있습니다. 이러한 이벤트 설명의 형식은, 날짜/시간 형식이 다르고 형식에 두 개의 추가 구성 요소(*category*와 *logLevel*)가 추가된다는 점을 제외하면 UNIX `syslog` 기능에 의해 정의된 것과 동일합니다.

**표 21-6** 저장소 및 관리 로그 파일 구성 요소

| 구성 요소               | 정의                                                                                                                                                                |
|---------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>dateTime</i>     | 이벤트가 기록된 날짜 및 시간이며, <code>dd/mm/yyyy hh:mm:ss</code> 형식으로 표현됩니다. 여기서 시간대 필드는 GMT로부터의 <code>+/-hhmm</code> 으로 표현됩니다. 예를 들면 다음과 같습니다.<br>02/Jan/1999:13:08:21 -0700 |
| <i>hostName</i>     | 서버가 실행되고 있는 호스트 시스템의 이름입니다(예: showshoe).<br><b>주:</b> 호스트에 두 개 이상의 Messaging Server 인스턴스가 있는 경우 프로세스 아이디(pid)를 사용하여 각 인스턴스의 기록된 이벤트를 구분할 수 있습니다.                  |
| <i>processName</i>  | 이벤트를 생성한 프로세스의 이름입니다(예: <code>cgi_store</code> ).                                                                                                                 |
| <i>pid</i>          | 이벤트를 생성한 프로세스의 프로세스 아이디입니다(예: 18753).                                                                                                                             |
| <i>category</i>     | 이벤트가 속하는 범주(예: <code>General</code> )입니다(755페이지의 표 21-5 참조).                                                                                                      |
| <i>logLevel</i>     | 이벤트가 표시되는 로깅 수준(예: <code>Notice</code> )입니다(754페이지의 표 21-4 참조).                                                                                                   |
| <i>eventMessage</i> | 이벤트별 설명 메일로 길이는 임의적일 수 있습니다(예: <code>Log created (894305624)</code> ).                                                                                            |

다음은 콘솔을 사용하여 표시되는 기록된 세 개의 이벤트입니다.

```
02/May/1998:17:37:32 -0700 showshoe cgi_store[18753]:
General Notice:
    Log created (894155852)
```

```
04/May/1998:11:07:44 -0400 xyzmail cgi_service[343]: General Error:
function=getserverhello|port=2500|error=failed to connect
```

```
03/Dec/1998:06:54:32 +0200 SiroePost imapd[232]: Account Notice:
close [127.0.0.1] [unauthenticated] 1998/12/3 6:54:32
0:00:00 0 115 0
```

IMAP와 POP 이벤트 항목은 세 개의 번호로 끝날 수 있습니다. 위의 예에서는 0 115 0입니다. 첫 번째 번호는 클라이언트가 전송한 바이트 수이고, 두 번째 번호는 서버가 전송한 바이트 수이고, 세 번째 숫자는 선택한 메일함(POP의 경우 항상 1)입니다.

Log Viewer 창에서 로그 파일을 볼 때는 특정 로깅 수준이나 범주 또는 특정 프로세스 아이디 등과 같은 이벤트의 특정 구성 요소를 검색하여, 표시되는 이벤트를 제한할 수 있습니다. 자세한 내용은 [760페이지의 "서비스 로그 검색 및 보기"](#)를 참조하십시오.

각 로그 항목의 이벤트 메일에는 기록되는 이벤트 유형에 한정된 형식이 사용됩니다. 즉, 각 서비스는 이벤트 메일에 표시되는 내용을 정의합니다. 대부분의 이벤트 메일은 간단하며 설명적입니다. 다른 메일은 좀 더 복잡할 수 있습니다.

## 서비스 로깅 옵션 정의 및 설정

관리에 필요한 가장 적합한 메시지 저장소와 관리 서비스 로깅 구성을 정의할 수 있습니다. 이 절에서는 최적의 구성과 정책을 결정하는 데 도움이 되는 문제에 대해 설명하고 이를 구현하는 방법에 대해 설명합니다.

### 유연한 로깅 구조

로그 파일의 이름 지정 스키마(*service.sequenceNum.timeStamp*)는 유연한 로그 회전과 백업 정책을 지정하는 데 도움이 됩니다. 각 서비스에 대한 이벤트가 서로 다른 파일에 기록되기 때문에 문제를 빠르게 차단할 수 있습니다. 또한 파일 이름의 일련 번호가 계속 커지고 타임스탬프가 항상 고유하기 때문에 제한된 일련 번호 집합을 모두 사용한 후 새 로그 파일이 기존 로그 파일을 덮어쓰지 않습니다. 대신 보다 유연한 수명 제한, 파일 수 또는 전체 저장소 용량에 도달하였을 때만 기존 로그 파일을 삭제하거나 덮어쓰게 됩니다.

Messaging Server는 관리 작업을 단순화하고 백업 작업을 수월히 하는 로그 파일의 자동 회전 기능을 지원합니다. 이후의 기록되는 이벤트를 저장하기 위해 수동으로 현재 로그 파일을 지우고 새 파일을 만들 필요가 없습니다. 서버를 중단하거나 새 로그 파일을 시작하도록 서버에 수동으로 알리지 않고도 디렉토리에서 현재 로그 파일을 제외한 모든 파일을 언제든지 백업할 수 있습니다.

로깅 정책 설정 시 전체 로그 저장소 제한, 최대 로그 파일 수, 개별 파일 크기, 최대 파일 수명 및 로그 파일 회전 비율을 제어하는 옵션을 설정할 수 있습니다(각 옵션별).

### 원하는 옵션 계획

로그 파일의 회전이나 삭제를 시작할 수 있는 두 개 이상의 제한을 설정해야 합니다. 먼저 도달한 제한이 작업을 제어합니다. 예를 들어 최대 로그 파일 크기가 3.5MB이고 매일 새 로그가 생성되도록 지정한 경우, 로그 데이터가 24시간 동안 3.5MB 이상 작성되면 매일 하나 이상의 로그 파일이 생성됩니다. 또한 최대 로그 파일 수가 10이고 최대 수명이 8일인 경우, 로그 회전이 더 빠르게 수행되면 8일이 되기 전에 10개의 파일이 생성되므로 로그 파일의 수명 제한에는 도달하지 않게 됩니다.

Messaging Server 관리 로그에 대해 제공되는 다음 기본값을 계획의 시작점으로 사용할 수 있습니다.

디렉토리의 최대 로그 파일 수: 10  
최대 로그 파일 크기: 2MB  
모든 로그 파일에 허용되는 총 최대 크기: 20MB  
허용되는 빈 디스크 최대 공간: 5MB  
로그 롤오버 시간: 1일  
만료 전 최대 수명: 7일  
로깅 수준: Notice

이 구성에서는 서버 관리 로그 데이터가 매일 약 2MB 정도 누적될 것이며, 1주에 한 번 백업하고, 관리 로그의 저장소에 할당된 총 크기는 최소한 25MB가 되는 것으로 가정합니다. 로깅 수준이 더 세밀한 경우 이 설정이 충분하지 않을 수 있습니다.

POP, IMAP 또는 HTTP 로그의 경우에도 처음에는 동일한 값을 사용할 수 있습니다. 모든 서비스에 대략 여기에 표시된 기본값과 동일한 로그 저장소 요구 사항이 있는 경우 처음에는 총 로그 저장소 용량을 약 150MB로 설정해야 합니다. 이는 일반적인 저장소 요구 사항이며 실제 요구 사항은 환경에 따라 크게 다를 수 있습니다.

### 로깅 옵션 이해

콘솔 또는 명령줄을 사용하여 메시지 저장소 로깅 구성을 제어하는 옵션을 구성할 수 있습니다.

이러한 옵션의 최적 설정은 로그 데이터가 누적되는 비율에 따라 다릅니다. 1MB의 저장소 공간에는 4,000개에서 10,000개의 로그 항목이 들어갈 수 있습니다. Notice와 같은 보다 세밀한 로깅 수준에서는, 작업량이 중간 정도인 서버가 매주 수백 MB의 로그 데이터를 생성할 수 있습니다. 이 경우 다음과 같은 방법을 사용할 수 있습니다.

- 저장소 제한에 일치하는 로깅 수준 즉, 평가 수준을 설정하면 로그 데이터는 저장소 제한을 평가하는 데 사용되는 비율과 비슷하게 누적됩니다.
- 검색 성능에 영향이 없도록 로그 파일 크기를 정의합니다. 또한 회전 일정과 총 저장소 제한에 맞게 조정합니다. 로그 항목이 누적되는 비율이 지정되면, 그 최대값은 회전이 자동으로 수행될 때 예상되는 누적 양보다 약간 크게 설정합니다. 그리고 최대 파일 크기와 최대 파일 수를 곱한 값이 전체 저장소 제한과 거의 일치하도록 해야 합니다.

예를 들어 IMAP 로그 회전이 매일 수행되며 IMAP 로그 데이터의 예상 누적량이 일일 3MB이고 IMAP 로그의 전체 저장소 제한이 25MB인 경우, 최대 IMAP 로그 파일 크기는 3.5MB로 설정할 수 있습니다. 이 예에서 일부 로그 데이터가 너무 빠르게 누적되어 모든 로그 파일이 최대 크기에 도달하고 최대 로그 파일 수에 도달하면 일부 로그 데이터가 손실될 수 있습니다.

- 서버 백업이 매주 수행되며 IMAP 로그 파일을 매일 회전하는 경우 최대 IMAP 로그 파일 수를 약 10(개별 로그 크기 제한이 초과되는 경우의 회전을 고려한 값)으로 지정하고 최대 수명은 7-8일로 지정할 수 있습니다.
- 전체 저장소 제한은 하드웨어 용량 내에서 선택하고 해당 서버의 백업 일정에 맞게 조정해야 합니다. 로그 데이터의 예상 누적 비율을 평가하고 안전 계수를 추가한 다음 총 저장소 제한이 서버 백업 사이의 간격을 초과하지 않도록 정의합니다.

예를 들어 매일 평균 3MB의 IMAP 로그 파일 데이터가 누적되고 서버 백업이 매주 수행되는 경우, IMAP 로그의 저장소 제한을 25-30MB로 설정할 수 있습니다(디스크 저장소 용량이 충분한 경우).

- 안전을 위해, 로그 파일이 저장될 볼륨에 허용되는 빈 디스크의 최소 공간을 선택해야 합니다. 이렇게 하면 로그 파일 크기 이외의 요소로 인해 볼륨이 꽉 차게 되면 꽉 찬 디스크에 로그 데이터를 쓰려고 할 때 발생하는 실패가 발생하기 전에 오래된 로그 파일이 삭제됩니다.

## 서비스 로그 검색 및 보기

콘솔에서는 메시지 저장소와 관리 로그 데이터를 볼 수 있는 기본 인터페이스를 제공합니다. 이를 통해 개별 로그 파일을 선택하고 해당 파일 내에서 로그 항목의 필터링된 유연한 검색을 수행할 수 있습니다.

특정 서비스에 대한 로그 파일은 날짜 순으로 나열됩니다. 검색할 로그 파일을 선택한 다음에는 검색 매개 변수를 지정하여 개별 이벤트에 대한 검색 범위를 좁힐 수 있습니다.

### 검색 매개 변수

다음은 로그 데이터를 보기 위해 지정할 수 있는 검색 매개 변수입니다.

- **시간.** 이벤트를 검색할 특정 시간의 시작과 끝을 지정하거나 검색할 일 수(현재 날짜 이전)를 지정할 수 있습니다. 서버 충돌 시간 또는 알고 있는 다른 발생 시간까지 기록된 이벤트를 확인할 시간 범위를 지정할 수 있습니다. 또는 현재 로그 파일 중 오늘의 이벤트만 보도록 범위를 지정할 수도 있습니다.
- **로깅 수준.** 로깅 수준(753페이지의 "로깅 수준" 참조)을 지정할 수 있습니다. 특정 문제를 해결할 특정 수준을 선택할 수 있습니다. 예를 들어 서버 다운의 원인을 알려면 **Critical**을 선택하고 실패한 프로토콜 호출을 찾으려면 **Error**를 선택합니다.
- **기능.** 기능을 지정할 수 있습니다(755페이지의 "기록되는 이벤트의 범주" 참조). 문제가 포함된 기능 영역을 알고 있는 경우 특정 기능을 선택할 수 있습니다. 예를 들어 디스크 오류 때문에 서버가 크래시된 것으로 생각되면 **Store**를 선택하고, IMAP 프로토콜 명령 오류에 문제가 있는 경우 **Protocol**을 선택합니다.
- **텍스트 검색 패턴.** 보다 세밀한 검색을 위해 텍스트 검색 패턴을 지정할 수 있습니다. 알고 있는 이벤트 시간, 프로세스 이름, 프로세스 아이디 및 이벤트 메일의 일부(예: 원격 호스트 이름, 함수 이름, 오류 번호 등) 등과 같이 와일드카드 형식의 검색으로 표현할 수 있는 이벤트의 모든 구성 요소(756페이지의 "서비스 로그 파일 형식 이해" 참조)를 포함시킬 수 있습니다.

검색 패턴에는 다음의 특수 문자 및 와일드카드 문자가 포함될 수 있습니다.



\* 모든 문자 세트(예: \*.com)  
 ? 모든 단일 문자(예:199?)  
 [nmn] nmn 집합에 속하는 모든 문자(예: [aeiou])  
 [^nmn] nmn 집합에 속하지 않는 모든 문자(예: (example: [^aeiou])  
 [n-m] n-m 범위의 모든 문자(예: [A-Z])  
 [^n-m] n-m 범위에 속하지 않는 모든 문자(예: [^0-9])  
 \ 이스케이프 문자: \*, ?, [ 또는 ] 앞에 입력하여 리터럴로 사용

주: 검색은 대소문자를 구분합니다.

로그를 볼 때 로깅 수준과 기능을 조합하는 예는 다음과 같습니다.

- Account 기능(및 Notice 수준)을 지정하여 실패한 로그인을 표시합니다. 그러면 잠재적 보안 침해를 조사할 때 유용합니다.
- Network 기능(및 모든 로깅 수준)을 지정하여 연결 문제를 조사합니다.
- 모든 기능(및 Critical 로깅 수준)을 조사하여 서버의 기능에 관련된 기본적인 문제를 찾습니다.

## 서비스 로그 작업

이 절에서는 configutil 명령과 로그 검색 및 보기를 위한 콘솔을 사용하여 서비스 로그에 대한 작업을 수행하는 방법에 대해 설명합니다.

### ▶ 서비스 로그를 syslog에 전송하는 방법

- configutil 명령을 syslogfacility 옵션과 함께 실행합니다.

```
configutil -o logfile.service.syslogfacility -v value
```

여기서 *service*는 admin, pop, imap, imta 또는 http이며, *value*는 user, mail, daemon, local0 ~ local7 또는 none입니다.

값을 설정하면 메일은 설정 값에 따라 syslog 기능에 기록되며 다른 모든 로그 파일 서비스 옵션은 무시됩니다. 옵션이 설정되지 않았거나 값이 none이면 로깅은 Messaging Server 로그 파일을 사용합니다.

### ▶ 콘솔을 사용하여 로깅 옵션을 설정하는 방법

1. 로그 파일 옵션을 설정할 Messaging Server를 엽니다.
2. 구성 탭을 누르고 왼쪽 창에서 Log Files 폴더를 연 다음 서비스(IMAP, HTTP 또는 Admin 등)의 로그 파일을 선택합니다.
3. "세부 정보 수준" 드롭다운 목록에서 로깅 수준을 선택합니다.

4. "로그 파일에 대한 디렉토리 경로" 필드에서 로그 파일을 저장할 디렉토리의 이름을 입력합니다.
5. "각 로그의 파일 크기" 필드에 최대 로그 파일 크기를 입력합니다.
6. "다음 경우마다 새 로그 만들기" 필드에 로그 회전 일정 수를 입력합니다.
7. "디렉토리당 로그 수" 필드와 "로그 최대 기간" 필드에 백업 일정에 맞는 최대 로그 파일 수와 최대 수명을 입력합니다.
8. "총 로그 크기 초과" 필드에 원하는 총 저장소 제한을 입력합니다.
9. "빈 디스크 공간 부족" 필드에 유지할 빈 디스크 공간의 최소 크기를 입력합니다.

▶ **HTTP 로깅 비활성화 방법**

시스템이 http 메일 액세스 즉, 웹 메일을 지원하지 않는 경우 다음 변수를 설정하여 http 로깅을 비활성화할 수 있습니다. 시스템이 웹 메일을 지원해야 하는 경우(예: Messenger Express) 이 변수를 설정하지 마십시오.

- 다음 configutil 명령을 실행합니다.  

```
configutil -o service.http.enable -v no  
configutil -o service.http.enablesslport -v no
```

▶ **서버 로그 수준을 설정하는 방법**

- 다음 configutil 명령을 실행합니다.  

```
configutil -o logfile.service.loglevel -v level
```

여기서 *service*는 admin, pop, imap, imta 또는 http이며 *loglevel*은 Nolog, Critical, Error, Warning, Notice, Information 또는 Debug입니다.

▶ **서버 로그 파일의 디렉토리 경로를 지정하는 방법**

- 다음 configutil 명령을 실행합니다.  

```
configutil -o logfile.service.logdir -v dirpath
```

▶ **각 서비스 로그의 최대 파일 크기를 지정하는 방법**

- 다음 configutil 명령을 실행합니다.  

```
configutil -o logfile.service.maxlogfilesize -v size
```

여기서 *size*는 바이트 수를 지정합니다.

▶ 서비스 로그 회전 일정을 지정하는 방법

- 다음 `configutil` 명령을 실행합니다.

```
configutil -o logfile.service.rollovertime -v number
```

여기서 `number`는 초를 지정합니다.

▶ 디렉토리당 서비스 로그 파일의 최대 수를 지정하는 방법

- 다음 `configutil` 명령을 실행합니다.

```
configutil -o logfile.service.maxlogfiles -v number
```

▶ 저장소 제한을 지정하는 방법

- 다음 `configutil` 명령을 실행합니다.

```
configutil -o logfile.service.maxlogsize -v number
```

여기서 `number`는 바이트 수를 지정합니다.

▶ 유지할 빈 디스크 공간의 최소 크기를 지정하는 방법

- 다음 `configutil` 명령을 실행합니다.

```
configutil -o logfile.service.minfreediskspace -v number
```

여기서 `number`는 바이트 수를 지정합니다.

▶ 로그 파일이 만료되는 시기를 지정하는 방법

```
configutil -o logfile.service.expirytime -v number
```

여기서 `number`는 초를 지정합니다.

▶ 검색 및 보기 결과를 지정하는 방법

지정된 서비스에 속한 특정 특성으로 기록되는 이벤트를 검색하려면 다음 단계를 수행합니다.

1. 콘솔에서 검사할 로그 파일이 있는 **Messaging Server**를 엽니다.
2. 다음 단계 중 하나를 수행하여 기록되는 해당 서비스에 대한 로그 파일 내용 탭을 표시합니다.
  - 작업 탭을 누른 다음 "서비스 로그 보기"를 누릅니다. 여기서 *서비스*는 기록되는 서비스(예: "IMAP 서비스" 또는 "관리" 등)의 이름입니다.
  - 구성 탭을 누른 다음 왼쪽 창에서 **Log Files** 폴더를 연 다음 서비스(예: **IMAP** 또는 **Admin**)의 로그 파일을 선택합니다. 그런 다음 오른쪽 창에서 내용 탭을 누릅니다.
3. 기록된 해당 서비스의 내용 탭이 표시됩니다.

4. 로그 파일 이름 필드에서 검사할 로그 파일을 선택합니다.
5. 선택한 로그 보기 버튼을 눌러 로그 뷰어 창을 엽니다.
6. 로그 뷰어 창에서 원하는 검색 매개 변수(앞의 "검색 매개 변수" 절에서 설명)를 지정합니다.
7. 업데이트를 눌러 검색을 수행한 다음 그 결과를 로그 항목 필드에 표시합니다.

## 메시지 저장소 로깅에 메일 추적 사용

MTA가 메일을 추적하는 것과 비슷한 방법으로 메시지 저장소 로깅을 사용하여 메일 아이디로 메일을 추적할 수 있습니다. 이 방식으로 메일을 추적하면 메일의 수명 주기의 중요 이벤트를 추적할 수 있습니다.

메시지 저장소 로그의 메일을 추적하려면 일반 로깅 구성 외에도 메일 추적을 구성해야 합니다. 기본적으로 메일 추적은 활성화되지 않습니다.

---

**주** 메일 추적에는 많은 양의 디스크 공간이 필요합니다. 디스크 공간이 충분하지 않을 경우 이 기능을 활성화하지 마십시오.

---

메시지 저장소 로깅에서는 다음 작업을 추적할 수 있습니다.

- 추가 - 메시지 저장소 라이브러리가 메일을 폴더에 추가하는 기본 방법입니다. 추가 추적은 메시지 저장소에 들어오는 메일을 보여 줍니다.
- 가져오기 - 최종 사용자에게 메일이나 메일의 일부분을 검색하는 IMAP 명령입니다. 메일 추적의 경우 서비스에서 최종 사용자가 읽을 메일을 검색하는 경우로까지 그 의미가 확장됩니다.  
메일 추적에서는 종종 메일 헤더를 읽을 때 추적을 사용하지 않을 수 있으므로 본문 가져오기가 메일 본문의 일부를 검색할 때를 나타냅니다.
- 정리: 이 경우 임의의 서비스가 사용자 폴더에서 메일을 제거하는 때를 나타내도록 확장되는 IMAP 용어입니다.

### ▶ 메일 추적을 활성화하는 방법

- 다음 configutil 명령을 실행합니다.

```
configutil -o local.msgrace.active -v "yes"
```

메일 추적 정보는 각 프로세스의 기본 로그에 기록됩니다. IMAP 가져오기는 imap로 그 파일에 표시됩니다. ims\_master 추가는 ims\_master 채널 로그 파일에 표시됩니다.

### ▶ 메일 추적을 단일 로그 파일로 리디렉션하는 방법

- 메일 추적 로깅을 단일 "msgtrace" 로그 파일로 리디렉션하려면 configutil 명령을 사용하여 로그 파일 매개 변수를 구성해야 합니다. 다른 로그 파일과 달리 msgtrace 로그 파일은 로컬로 구성됩니다. 예를 들면 다음과 같습니다.

```
configutil -o "local.logfile.msgtrace.buffersize" -v "0"
configutil -o "local.logfile.msgtrace.expirytime" -v "604800"
configutil -o "local.logfile.msgtrace.flushinterval" -v "60"
configutil -o "local.logfile.msgtrace.logdir" -v "/opt/SUNWmsgsr/data/log"
configutil -o "local.logfile.msgtrace.loglevel" -v "Information"
configutil -o "local.logfile.msgtrace.logtype" -v "NscpLog"
configutil -o "local.logfile.msgtrace.maxlogfiles" -v "10"
configutil -o "local.logfile.msgtrace.maxlogfilesize" -v "2097152"
configutil -o "local.logfile.msgtrace.maxlogsize" -v "20971520"
configutil -o "local.logfile.msgtrace.minfreediskspace" -v "5242880"
configutil -o "local.logfile.msgtrace.rollovertime" -v "86400"
```

### ▶ 메일 추적 로깅을 구성 해제하는 방법

- msgtrace 로그 파일을 구성 해제하려면 configutil 명령을 사용하여 해당 구성에 대한 모든 참조를 제거합니다. 예를 들면 다음과 같습니다.

```
configutil -o "local.logfile.msgtrace.buffersize" -v ""
configutil -o "local.logfile.msgtrace.expirytime" -v ""
configutil -o "local.logfile.msgtrace.flushinterval" -v ""
configutil -o "local.logfile.msgtrace.logdir" -v ""
configutil -o "local.logfile.msgtrace.loglevel" -v ""
configutil -o "local.logfile.msgtrace.logtype" -v ""
configutil -o "local.logfile.msgtrace.maxlogfiles" -v ""
configutil -o "local.logfile.msgtrace.maxlogfilesize" -v ""
configutil -o "local.logfile.msgtrace.maxlogsize" -v ""
configutil -o "local.logfile.msgtrace.minfreediskspace" -v ""
configutil -o "local.logfile.msgtrace.rollovertime" -v ""
```

### ▶ LMTP 로깅을 구성하는 방법

- LMTP를 사용하고 단일 "msgtrace" 로그 파일을 사용하지 않을 경우에는 마찬가지로 tcp\_lmtp\_server 로그 파일을 로컬로 구성해야 합니다. LMTP를 사용하지 않거나, 메일 추적을 사용하지 않거나, "msgtrace" 로그 파일에서 메일 추적을 사용할 경우에는 LMTP 메시지 저장소측 로그를 초기화할 필요가 없습니다. LMTP는 이미 MTA 정보를 별도로 기록합니다. 예를 들면 다음과 같습니다.

```
configutil -o "local.logfile.tcp_lmtp_server.bufferysize" -v "0"
configutil -o "local.logfile.tcp_lmtp_server.expirytime" -v "604800"
configutil -o "local.logfile.tcp_lmtp_server.flushinterval" -v "60"
configutil -o "local.logfile.tcp_lmtp_server.logdir" -v "/opt/SUNWmsgsr/data/log"
configutil -o "local.logfile.tcp_lmtp_server.loglevel" -v "Information"
configutil -o "local.logfile.tcp_lmtp_server.logtype" -v "NscpLog"
configutil -o "local.logfile.tcp_lmtp_server.maxlogfiles" -v "10"
configutil -o "local.logfile.tcp_lmtp_server.maxlogfilesize" -v "2097152"
configutil -o "local.logfile.tcp_lmtp_server.maxlogsize" -v "20971520"
configutil -o "local.logfile.tcp_lmtp_server.minfreediskspace" -v "5242880"
configutil -o "local.logfile.tcp_lmtp_server.rollovertime" -v "86400"
```

## 메시지 저장소 로깅 예

메시지 저장소 로그 파일에 기록되는 정확한 필드 형식 및 필드 목록은 설정하는 로깅 옵션에 따라 다릅니다. 이 절에서는 일반적인 로그 항목의 몇 가지 예를 보여 줍니다.

### 메시지 저장소 로깅 예: 잘못된 비밀번호

사용자가 잘못된 비밀번호를 입력하면 "user not found" 메시지와 달리 "인증" 실패가 기록됩니다. 보안상의 이유 때문에 "user not found" 메시지가 클라이언트에게 전달되지만 기록되는 것은 실제 이유(잘못된 비밀번호)입니다.

#### 코드 예 21-11      메시지 저장소 로깅: 잘못된 비밀번호

```
[30/Aug/2004:16:53:05 -0700] vadar imapd[13027]: Account Notice: badlogin:
[192.18.126.64:40718] plaintext user1 authentication failure
```

### 메시지 저장소 로깅 예: 비활성화된 계정

다음 예는 비활성화된 계정으로 인해 사용자가 로그인할 수 없는 이유를 보여 줍니다. 또한 비활성화된 계정이 "(inactive)" 또는 "(hold)"로 구분됩니다.

**코드 예 21-12**      메시지 저장소 로깅: 비활성화된 계정

```
[30/Aug/2004:16:53:31 -0700] vadar imapd[13027]: Account Notice: badlogin:
[192.18.126.64:40720] plaintext user3 account disabled (hold)
```

**메시지 저장소 로깅 예: 추가된 메일**

다음 예는 메일이 폴더에 추가될 때마다 발생하는 추가 메시지를 보여 줍니다. 메시지 저장소 로고는 ims\_master 및 lmtpl 채널을 통해 메시지 저장소에 들어오는 모든 메일을 기록합니다. 사용자 아이디, 폴더, 메일 크기 및 메일 아이디의 "추가"가 기록됩니다.

**코드 예 21-13**      메시지 저장소 로깅: 추가

```
[31/Aug/2004:16:33:14 -0700] vadar ims_master[13822]: Store Information:
append:user1:user/user1:659:<Roam.SIMC.2.0.6.1093995286.11265.user1@vadar.siroe.com>
```

**메시지 저장소 로깅 예: 클라이언트가 가져온 메일**

클라이언트가 메일을 검색하면 메시지 저장소 로고는 "가져오기" 메시지를 기록합니다. 메시지 저장소 로고는 하나 이상의 본문 부분에 대한 클라이언트의 모든 가져오기를 기록합니다. 사용자 아이디, 폴더 및 메일 아이디의 "가져오기"가 기록됩니다.

**코드 예 21-14**      메시지 저장소 로깅: 클라이언트가 검색한 메일

```
[31/Aug/2004:15:55:26 -0700] vadar imapd[13729]: Store Information:
fetch:user1:user/user1:<Roam.SIMC.2.0.6.1093051161.3655.user1@vadar.siroe.com>
```

**메시지 저장소 로깅 예: 폴더에서 제거된 메일**

IMAP 또는 POP 메일이 폴더에서 제거되지만 시스템에서는 제거되지 않을 경우 메시지 저장소는 "정리" 메시지를 기록합니다. 이 메시지는 사용자가 정리하든 유틸리티가 정리하든 상관없이 기록됩니다. 폴더 및 메일 아이디의 "정리"가 기록됩니다.

**코드 예 21-15**      메시지 저장소 로깅: 폴더에서 제거된 메일

```
31/Aug/2004:16:57:36 -0700] vadar imexpire[13923]: Store Information:
expunge:user/user1:<Roam.SIMC.2.0.6.1090458838.2929.user1@vadar.siroe.com>
```

## 메시지 저장소 로깅 예: 중복된 로그인 메시지

하나의 msgtrace 로그 파일에 대해 메일 추적을 구성할 경우 imap 및 pop 로그 파일에 표시되는 일반 "로그인" 메시지가 msgtrace 파일에서 중복됩니다.

### 코드 예 21-16            메시지 저장소 로깅: 로그인

```
[30/Aug/2004:16:53:13 -0700] vadar imapd[13027]: Account Information: login  
[192.18.126.64:40718] user1 plaintext
```



## MTA 문제 해결

이 장에서는 MTA(Message Transfer Agent) 문제 해결에 대한 일반 도구, 방법 및 절차에 대해 설명합니다. 이 장은 다음 내용으로 구성되어 있습니다.

- 770페이지의 "문제 해결 개요"
- 770페이지의 "표준 MTA 문제 해결 절차"
- 781페이지의 "일반 MTA 문제 및 솔루션"
- 793페이지의 "일반 오류 메시지"
- 632페이지의 "메일함 및 메일함 데이터베이스 복구"(다른 장)

관련 항목인 모니터링 절차는 23장, "[Messaging Server 모니터링](#)"에 설명되어 있습니다.

---

**주** 이 장을 읽기 전에 본 설명서의 5장부터 10장과 *Sun Java System Messaging Server Administration Reference*의 MTA 구성 및 명령줄 유틸리티에 대한 장을 검토하십시오.

---

## 문제 해결 개요

MTA 관련 문제 해결의 첫 단계 중 하나는 진단을 시작할 위치를 결정하는 것입니다. 문제에 따라 로그 파일에서 오류 메시지를 볼 수 있습니다. 다른 상황에서는 모든 표준 MTA 프로세스를 확인하고 MTA 구성을 검토하거나 개별 채널을 시작 및 중지할 수 있습니다. 사용 방법에 상관 없이 MTA 관련 문제 해결 시에는 다음 질문을 고려하십시오.

- 구성 또는 환경 문제(예: 디스크 공간 또는 할당량 문제)로 인해 메일을 받을 수 없었습니까?
- 메일이 메일 대기열에 놓였을 때 디스패처 및 Job Controller와 같은 MTA 서비스가 제공되었습니까?
- 네트워크 연결성 또는 라우팅 문제로 인해 메일이 원격 시스템에 고착되거나 잘못 라우팅되었습니까?
- 메일이 메일 대기열에 놓이기 전후에 문제가 발생했습니까?

위 질문은 이 장의 다음 절에 설명되어 있습니다.

## 표준 MTA 문제 해결 절차

이 절에서는 MTA에 대한 표준 문제 해결 절차에 대해 간략하게 설명합니다. 문제가 오류 메시지를 생성하지 않거나 오류 메시지에서 충분한 진단 정보를 제공하지 않을 경우 또는 MTA의 일반 상태 확인, 테스트 및 표준 유지 관리를 수행할 경우에는 다음 절차를 따릅니다.

- 771페이지의 "MTA 구성 확인"
- 771페이지의 "메일 대기열 디렉토리 확인"
- 771페이지의 "중요 파일의 소유권 확인"
- 772페이지의 "Job Controller 및 디스패처 실행 확인"
- 774페이지의 "로그 파일 확인"
- 775페이지의 "수동으로 채널 프로그램 실행"
- 775페이지의 "개별 채널 시작 및 중지"
- 777페이지의 "MTA 문제 해결 예"

## MTA 구성 확인

`imsimta test -rewrite` 유틸리티를 사용하여 주소 구성을 테스트합니다. 이 유틸리티를 사용하여 실제로 메일을 보내지 않고도 MTA의 주소 재작성 및 채널 매핑을 테스트할 수 있습니다. 자세한 내용은 *Sun Java System Messaging Server Administration Reference*의 *MTA command-line utilities* 장을 참조하십시오.

일반적으로 유틸리티는 메일이 대기할 채널뿐 아니라 적용될 주소 재작성을 표시합니다. 단, MTA 구성에 구문 오류가 있는 경우 유틸리티는 오류 메시지를 발생립니다. 출력이 예상과 다를 경우에는 구성을 수정해야 할 수 있습니다.

## 메일 대기열 디렉토리 확인

일반적으로 `msg_svr_base/data/queue/`와 같은 MTA 메일 대기열 디렉토리에 메일이 있는지 확인합니다. `imsimta qm`과 같은 명령줄 유틸리티를 사용하여 MTA 메일 대기열 디렉토리 아래에 예상한 메일 파일이 있는지 확인합니다. `imsimta qm`에 대한 자세한 내용은 *Sun Java System Messaging Server Administration Reference* *MTA command-line utilities* 장과 [822페이지의 "imsimta qm counters"](#)를 참조하십시오.

`imsimta test -rewrite`의 출력이 올바르게 표시되면 메일이 실제로 MTA 메일 대기열 하위 디렉토리에 놓이는지 확인합니다. 확인 시에는 메일 로깅을 사용 가능하게 합니다 (MTA 로깅에 대한 자세한 내용은 [728페이지의 "MTA 메일 및 연결 로그 관리"](#) 참조). 그런 다음 `msg_svr_base/log/` 디렉토리에서 `mail.log_current` 파일을 확인합니다. 메일이 MTA 메일 대기열 하위 디렉토리에 놓이는지 확인하기 위해 메일 아이디를 사용하여 특정 메일을 추적할 수 있습니다. 메일을 찾을 수 없는 경우에는 파일 디스크 공간 또는 디렉토리 사용 권한에 문제가 있을 수 있습니다.

## 중요 파일의 소유권 확인

Messaging Server를 설치 시에는 메일 서버 사용자 계정(기본값은 `nobody`)을 선택해야 합니다. 다음 디렉토리, 하위 디렉토리 및 파일은 이 계정에서 소유해야 합니다.

```
/msg_svr_base/data/queue/  
/msg_svr_base/log/  
/tmp
```

예를 들어 다음 UNIX 시스템 명령은 이 디렉토리의 보호 및 소유권 확인에 사용될 수 있습니다.

```
ls -l -p -d /opt/SUNWmsgsr/data/queue
drwx----- 6 nobody bin 512 Feb 7 09:32 /opt/SUNWmsgsr/data/queue

ls -l -p -d /opt/SUNWmsgsr/log/imta
drwx----- 2 nobody bin 1536 Mar 10 09:00 /opt/SUNWmsgsr/log/imta

ls -l -p -d /opt/SUNWmsgsr/imta/tmp
drwx----- 2 nobody bin 512 Feb 7 10:00 /opt/SUNWmsgsr/imta/tmp
```

다음과 같은 UNIX 시스템의 명령을 사용하여 MTA 계정이 `/msg_svr_base/data/queue`의 파일을 소유하는지 확인합니다.

```
ls -l -p -R /opt/SUNWmsgsr/data/queue
```

## Job Controller 및 디스패처 실행 확인

MTA Job Controller는 대부분의 보내는(마스터) 채널 작업을 포함하여 MTA 프로세스 작업의 실행을 처리합니다.

MTA의 다중 스레드 SMTP 채널과 같은 일부 MTA 채널은 받는 메일을 처리하는 상주 서버 프로세스를 포함합니다. 이 서버는 채널에 대한 슬레이브(받는) 방향을 처리합니다. MTA 디스패처는 이러한 MTA 서버를 만듭니다. 디스패처 구성 옵션은 서버의 사용 가능성과 만들어진 서버의 수 및 각 서버가 처리할 수 있는 연결 수를 제어합니다.

Job Controller 및 디스패처가 있는지 확인하고 MTA 서버 및 실행 중인 처리 작업이 있는지 보려면 `imsimta process` 명령을 사용합니다. 유휴 상태에서 명령은 `job_controller` 및 `dispatcher` 프로세스를 수행해야 합니다. 예를 들면 다음과 같습니다.

```
imsimta process
```

| USER     | PID  | S | VSZ   | RSS  | STIME    | TIME | COMMAND                            |
|----------|------|---|-------|------|----------|------|------------------------------------|
| inetuser | 9567 | S | 18416 | 9368 | 02:00:02 | 0:00 | /opt/SUNWmsgsr/lib/tcp_smtp_server |
| inetuser | 6573 | S | 18112 | 5720 | Jul_13   | 0:00 | /opt/SUNWmsgsr/lib/job_controller  |
| inetuser | 9568 | S | 18416 | 9432 | 02:00:02 | 0:00 | /opt/SUNWmsgsr/lib/tcp_smtp_server |
| inetuser | 6574 | S | 17848 | 5328 | Jul_13   | 0:00 | /opt/SUNWmsgsr/lib/dispatcher      |

Job Controller가 없는 경우, `/msg_svr_base/data/queue` 디렉토리의 파일은 백업되고 메일이 전달되지 않습니다. 디스패처가 없으면 SMTP 연결을 수신할 수 없습니다.

`imsimta process`에 대한 자세한 내용은 *Sun Java System Messaging Server Administration Reference*를 참조하십시오.

Job Controller 또는 디스패처가 모두 없는 경우에는 `/msg_svr_base/data/log`에서 `dispatcher.log-*` 또는 `job_controller.log-*` 파일을 검토해야 합니다.

로그 파일이 존재하지 않거나 오류가 표시되지 않는 경우에는 `msg-start` 명령을 사용하여 프로세스를 시작합니다. 자세한 내용은 *Sun Java System Messaging Server Administration Reference*의 MTA command-line utilities 장을 참조하십시오.

---

**주** 시스템에서 실행해야 할 프로그램을 수행(`exec()`)하기 전에 먼저 자식 프로세스를 포크(`fork()`) 처리하는 경우가 아닌 경우, `imsimta process`를 실행할 때 디스패처나 Job Controller의 여러 인스턴스가 표시되지 않습니다. 그러나 이러한 중복의 시간 프레임은 매우 작습니다.

---

## 로그 파일 확인

MTA 처리 작업이 제대로 실행되지만 메일이 메일 대기열 디렉토리에 남아 있는 경우 로그 파일에 무슨 문제가 있는지 확인할 수 있습니다. 모든 MTA 로그 파일은 `/msg_svr_base/log` 디렉토리에 만들어집니다. 다양한 MTA 처리 작업에 대한 로그 파일 이름 형식은 표 22-1에 표시됩니다.

표 22-1 MTA 로그 파일

| 파일 이름                                     | 로그 파일 내용                                                                                                                 |
|-------------------------------------------|--------------------------------------------------------------------------------------------------------------------------|
| <code>channel_master.log-uniqueid</code>  | <code>channel</code> 에 대한 마스터 프로그램(주로 클라이언트)의 출력입니다.                                                                     |
| <code>channel_slave.log-uniqueid</code>   | <code>channel</code> 에 대한 슬레이브 프로그램(주로 서버)의 출력입니다.                                                                       |
| <code>dispatcher.log-uniqueid</code>      | 디스패처 디버깅입니다. 이 로그는 디스패처 DEBUG 옵션의 설정과 관계없이 만들어집니다. 하지만 자세한 디버깅 정보를 얻으려면 DEBUG 옵션을 0이 아닌 값으로 설정해야 합니다.                    |
| <code>imta</code>                         | <code>ims-ms</code> 채널 오류 메시지로 전달에 문제가 있는 경우 나타납니다.                                                                      |
| <code>job_controller.log-uniqueid</code>  | Job Controller 로깅입니다. 이 로그는 Job Controller DEBUG 옵션의 설정과 관계없이 만들어집니다. 하지만 자세한 디버깅 정보를 얻으려면 DEBUG 옵션을 0이 아닌 값으로 설정해야 합니다. |
| <code>tcp_smtp_server.log-uniqueid</code> | <code>tcp_smtp_server</code> 에 대한 디버깅입니다. 이 로그에 있는 정보는 메일이 아닌 서버에만 해당됩니다.                                                |
| <code>return.log-uniqueid</code>          | 주기적인 MTA 메일 바운서 작업에 대한 출력을 디버그하며 <code>option.dat</code> 에 <code>return_debug</code> 옵션이 사용되는 경우 이 로그 파일이 만들어집니다.        |

**주** 각 로그 파일은 고유 아이디(*uniqueid*)를 가지도록 만들어져 동일한 채널에서 만든 이전 로그를 덮어쓰지 못하게 합니다. 특정 로그 파일을 찾기 위해 `imsimta view` 유틸리티를 사용할 수 있습니다. 또한 `imsimta purge` 명령을 사용하여 오래된 로그 파일을 제거할 수 있습니다. 자세한 내용은 *Sun Java System Messaging Server Administration Reference*의 MTA *command-line utilities* 장을 참조하십시오.

`channel_master.log-uniqueid` 및 `channel_slave.log-uniqueid` 로그 파일은 다음 상황에서 만들어질 수 있습니다.

- 현재 구성에 오류가 있습니다.
- `master_debug` 또는 `slave_debug` 키워드가 `imta.cnf` 파일의 채널에 설정됩니다.

- `mm_debug`가 0이 아닌 값(`mm_debug > 0`)으로 `option.dat` 파일 (`/msg_svr_base/config/`)에 설정됩니다.

채널 마스터 및 슬레이브 프로그램 디버깅에 대한 자세한 내용은 *Sun Java System Messaging Server Administration Reference*를 참조하십시오.

## 수동으로 채널 프로그램 실행

MTA 전달 문제 진단 시에는 MTA 전달 작업을 수동으로 실행하는 것이 좋으며 특히 하나 이상의 채널에 대한 디버깅을 사용 가능하게 한 후에 유용합니다.

`imsimta submit` 명령은 MTA Job Controller에 채널을 실행할 것을 알립니다. 해당 채널에 대한 디버깅이 사용 가능한 경우에는 표 22-1에 표시된 대로 `imsimta submit`가 `/msg_svr_base/log` 디렉토리에 로그 파일을 만듭니다.

`imsimta run` 명령은 현재 출력이 사용자의 단말기로 전송되는 활성 프로세스 상태의 채널에 대한 아웃바운드 전달을 수행합니다. 이는 작업 전송 자체에 문제가 있다고 의심되는 경우 작업을 전송하는 것보다 편리할 수 있습니다.

---

**주** 채널을 수동으로 실행하려면 Job Controller가 실행 중이어야 합니다.

---

`imsimta submit` 및 `imsimta run` 명령에 대한 구문, 옵션, 매개 변수 및 그 예에 대한 정보는 *Sun Java System Messaging Server Administration Reference*의 MTA command-line utilities 장을 참조하십시오.

## 개별 채널 시작 및 중지

경우에 따라 개별 채널을 시작 및 중지하면 메일 대기열 문제의 진단 및 디버그가 더 쉬워질 수 있습니다. 메일 대기열을 중지하면 대기 메일을 검사하여 루프 또는 스팸 공격의 존재 여부를 확인할 수 있습니다.

### 특정 채널에 대한 아웃바운드 처리(대기열에서 제외) 중지

1. `imsimta qm stop` 명령을 사용하여 특정 채널을 중지합니다. 이렇게 하면 Job Controller를 중지하지 않아도 되며 해당 구성을 다시 컴파일하지 않아도 됩니다. 다음 예에서는 `conversion` 채널이 중지됩니다.

```
imsimta qm stop conversion
```

- 2. 처리를 계속하려면 `imsimta qm start` 명령을 사용하여 채널을 다시 시작합니다. 다음 예에서는 `conversion` 채널이 시작됩니다.

**imsimta qm start conversion**

`imsimta qm start` 및 `imsimta qm stop` 명령에 대한 자세한 내용은 *Sun Java System Messaging Server Administration Reference*의 MTA command-line utilities 장을 참조하십시오.

**특정 도메인 또는 IP 주소에서 인바운드 처리(채널 대기열에 포함) 중지**

클라이언트 호스트에게 임시 SMTP 오류를 반환하면서 특정 도메인 또는 IP 주소에 대한 인바운드 메일 처리를 중지하려면 다음 프로세스 중 하나를 실행할 수 있습니다. 이렇게 하면 메일이 사용자 시스템에 보존되지 않습니다. [511페이지](#)의 "1부. 매핑 테이블"을 참조하십시오.

- 특정 호스트 또는 도메인 이름에 대한 인바운드 처리를 중지하려면 MTA 매핑 파일(보통 `/msg_svr_base/config/mappings`)의 `ORIG_SEND_ACCESS` 매핑 테이블에 다음 액세스 규칙을 추가합니다.

```
ORIG_SEND_ACCESS

*|*@sesta.com|*|*                               $X4.2.1|$NHost$ blocked
```

이 프로세스를 사용하면 보내는 사람의 원격 MTA가 시스템에 메일을 보존하며 인바운드 처리를 다시 시작할 때까지 계속해서 주기적으로 메일을 재전송합니다.

- 특정 IP 주소에 대한 인바운드 처리를 중지하려면 MTA 매핑 파일(보통 `/msg_svr_base/config/mappings`)의 `PORT_ACCESS` 매핑 테이블에 다음 액세스 규칙을 추가합니다.

```
PORT_ACCESS

TCP|*|25|IP_address_to_block|*                 $N500$ unable$ to$ \
connect$ at$ this$ time
```



도메인 또는 IP 주소에서 인바운드 처리를 다시 시작하려면 매핑 테이블에서 이 규칙을 제거하고 구성을 다시 컴파일해야 합니다. 추가로 각 매핑 테이블에 대한 고유 오류 메시지를 만들 수 있습니다. 이렇게 하면 어떤 매핑 테이블이 사용되는지 확인할 수 있습니다.

## MTA 문제 해결 예

이 절에서는 특정 MTA 문제를 단계적으로 해결하는 방법에 대해 설명합니다. 이 예에서 메일을 받는 사람은 전자 메일의 첨부 파일을 받지 못했습니다. 주: MIME 프로토콜 용어와 동일하게 이 절에서는 "첨부 파일"을 "메일 부분"이라고 합니다. 앞서 말한 문제 해결 기술은 메일 부분이 사라진 위치 및 이유를 확인하기 위해 사용됩니다(770페이지의 "[표준 MTA 문제 해결 절차](#)" 참조). 다음 단계를 사용하면 MTA를 통해 메일이 거쳐간 경로를 확인할 수 있습니다. 또한 메일이 메일 대기열에 들어가기 전이나 후에 사라졌는지 여부를 확인할 수 있습니다. 이렇게 하려면 채널을 수동으로 중지 및 실행하여 관련 파일을 캡처해야 합니다.

---

**주** 채널을 통해 메일을 수동으로 실행하는 경우에는 Job Controller가 실행 중이어야 합니다.

---

### 메일 경로에서 채널 확인

메일 경로에 어떤 채널이 있는지 확인하면 `master_debug` 및 `slave_debug` 키워드를 해당 채널에 적용할 수 있습니다. 이 키워드는 채널의 마스터 및 슬레이브 로그 파일에서 디버깅 출력을 생성하고 마스터 및 슬레이브 디버깅 정보는 메일 부분이 사라진 지점을 확인하는 데 도움을 줍니다.

1. `log_message_id=1`을 `/msg_svr_base/config`. 디렉토리의 `option.dat` 파일에 추가합니다. 이 매개 변수와 함께 message ID: 헤더 행이 `mail.log_current` 파일에 표시됩니다.
2. `imsimta cnbuild`를 실행하여 구성을 다시 컴파일합니다.
3. `imsimta restart dispatcher`를 실행하여 SMTP 서버를 다시 시작합니다.
4. 최종 사용자가 메일 부분이 있는 메일을 재전송하도록 합니다.
5. 메일이 통과하는 채널을 결정합니다.

채널을 확인할 수 있는 방법은 많지만 다음 방법을 사용하는 것이 좋습니다.

- a. UNIX 플랫폼의 경우 `grep` 명령을 사용하여 `/msg_svr_base/log` 디렉토리의 `mail.log_current` 파일에서 **message ID**: 헤더 행을 찾습니다.
- b. **message ID**: 헤더 행을 찾은 경우 E(대기열에 포함) 및 D(대기열에서 제외) 레코드를 찾아 메일 경로를 확인합니다. 로깅 입력 코드에 대한 자세한 내용은 [729페이지의 "MTA 로그 항목 형식 이해"](#)를 참조하십시오. 그 예는 다음 E 및 D 레코드를 참조하십시오.

```
29-Aug-2001 10:39:46.44 tcp_local conversion      E 2 ...
29-Aug-2001 10:39:46.44 conversion tcp_intranet  E 2 ...
29-Aug-2001 10:39:46.44 tcp_intranet          D 2 ...
```

왼쪽에 있는 채널이 소스 채널이고 오른쪽에 있는 채널이 대상 채널입니다. 이 예에서 E 및 D 레코드는 메일 경로가 `tcp_local` 채널에서 `conversion` 채널로 이동한 다음 최종적으로 `tcp_intranet` 채널로 이동했음을 나타냅니다.

## 수동으로 채널을 시작 및 중지하여 데이터 수집

이 절에서는 채널을 수동으로 시작 및 중지하는 방법에 대해 설명합니다. 자세한 내용은 [775페이지의 "개별 채널 시작 및 중지"](#)를 참조하십시오. 메일 경로에서 채널을 수동으로 시작 및 중지하면 MTA 프로세스의 각 단계에서 메일 및 로그 파일을 저장할 수 있습니다. 이 파일은 나중에 [780페이지의 "메일 정지 지점 확인"](#)에 사용됩니다.

1. 실질적인 디버깅 정보를 제공하려면 `mm_debug=5`를 `/msg_svr_base/config` 디렉토리의 `option.dat` 파일에 설정합니다.
2. `slave_debug` 및 `master_debug` 키워드를 `/msg_svr_base/config` 디렉토리에 있는 `inta.cnf` 파일의 해당 채널에 추가합니다.
  - a. 메일 부분이 있는 메일을 보내는 원격 시스템에서 인바운드 채널(또는 초기 대화 중에 메일이 전환되는 모든 채널)에 `slave_debug` 키워드를 사용합니다. 이 예에서 `slave_debug` 키워드는 `tcp_local` 채널에 추가됩니다.
  - b. 메일이 통과되고 [777페이지의 "메일 경로에서 채널 확인"](#)에서 확인된 다른 채널에 `master_debug` 키워드를 추가합니다. 이 예에서 `master_debug` 키워드는 `conversion` 및 `tcp_intranet` 채널에 추가됩니다.

- c. `imsimta restart dispatcher` 명령을 실행하여 SMTP 서버를 다시 시작합니다.
3. `imsimta qm stop` 및 `imsimta qm start` 명령을 사용하여 특정 채널을 수동으로 시작 및 중지합니다. 이 키워드 사용에 대한 자세한 내용은 775페이지의 "개별 채널 시작 및 중지"를 참조하십시오.
  4. 메일 파일을 캡처하는 프로세스를 시작하려면 최종 사용자가 메일 부분이 있는 메일을 재전송하도록 합니다.
  5. 메일이 채널에 입력될 때 `imsimta qm stop` 명령에 의해 중지된 경우에는 채널에서 메일이 중지됩니다. 자세한 내용은 단계 3을 참조하십시오.
    - a. 메일 경로에서 다음 채널을 수동으로 실행하기 전에 메일 파일을 복사하고 이름을 바꿉니다. 다음 UNIX 플랫폼 예를 참조하십시오.
 

```
# cp ZZ01K7LXW76T7O9TD0TB.00 ZZ01K7LXW76T7O9TD0TB.KEEP1
```

 일반적으로 메일 파일은 `/msg_svr_base/data/queue/destination_channel/001`과 유사한 디렉토리에 상주합니다. `destination_channel`은 메일이 다음으로 통과 (`:tcp_intranet` 등)하는 채널입니다. 하위 디렉토리(001, 002 등)를 `destination_channel` 디렉토리에 만들려면 채널에 `subdirs` 키워드를 추가합니다.
    - b. 메일이 처리된 순서를 확인하려면 메일을 트랩 및 복사할 때마다 메일 확장자에 번호를 지정하는 것이 좋습니다.
  6. 채널에서 메일 처리를 계속하고 메일 경로에서 다음 대상 채널로 대기열에 포함합니다. 이 작업을 수행하려면 `imsimta qm start` 명령을 사용합니다.
  7. `/msg_svr_base/log` 디렉토리에 있는 해당 채널 로그 파일(예: `tcp_intranet_master.log-*`)을 복사하여 저장합니다. 추적하는 메일에 대한 데이터를 가진 해당 로그 파일을 선택합니다. 복사한 파일을 채널에 넣을 때 해당 메일의 타임스탬프 및 제목 헤더와 일치하도록 합니다. `tcp_intranet_master.log-*`의 예에서는 파일이 삭제되지 않도록 파일을 `tcp_intranet_master.keep`으로 저장할 수 있습니다.
  8. 메일이 해당 최종 대상에 도달할 때까지 단계 5-7을 반복합니다.
 

단계 7에서 복사한 로그 파일은 단계 5에서 복사한 메일 파일과 상관 관계가 있어야 합니다. 예를 들어, 누락된 메일 부분 시나리오에서 모든 채널을 중지한 경우 `conversion_master.log-*` 및 `tcp_intranet_master.log-*` 파일을 저장합니다. 또한 소스 채널 로그 파일인 `tcp_local_slave.log-*`도 저장합니다. 또한, 다음과 같이 각 대상 채널로부터 해당 메일 파일의 복사본을 저장합니다. `conversion` 채널에서 `ZZ01K7LXW76T7O9TD0TB.KEEP1` 및 `tcp_intranet` 채널에서 `ZZ01K7LXW76T7O9TD0TB.KEEP2` 파일을 저장합니다.

9. 메일 및 로그 파일을 복사한 후 디버깅 옵션을 제거합니다.
  - a. `/msg_svr_base/config` 디렉토리에 있는 `imta.cnf` 파일의 해당 채널에서 `slave_debug` 및 `master_debug` 키워드를 제거합니다.
  - b. `/msg_svr_base/config` 디렉토리의 `option.dat` 파일에서 `mm_debug=0`을 재설정하고 `log_message_id=1`을 제거합니다.
  - c. `imsimta cnbuild`를 사용하여 구성을 다시 컴파일합니다.
  - d. `imsimta restart dispatcher` 명령을 실행하여 SMTP 서버를 다시 시작합니다.

### 메일 정지 지점 확인

1. 채널 프로그램 시작 및 중지가 완료되면 문제 해결에 사용할 수 있는 다음과 같은 파일을 가지게 됩니다.
  - a. 각 채널 프로그램에서 메일 파일의 모든 복사본(예: `ZZ01K7LXW76T709TD0TB.KEEP1`)
  - b. `tcp_local_slave.log-*` 파일
  - c. 각 대상 채널에 대한 `channel_master.log-*` 파일 집합
  - d. 메일 경로를 표시하는 `mail.log_current` 레코드 집합

모든 파일은 `mail.log_current` 레코드에서 **message ID**: 헤더 행과 일치하는 타임스탬프 및 메일 아이디가 있어야 합니다. 메일이 보낸 사람에게 다시 튕겨질 경우는 예외이며 튕겨진 메일은 원본 메일과는 다른 아이디 값을 가지게 됩니다.

2. `tcp_local_slave.log-*` 파일을 검사하여 메일이 메일 대기열에 들어갔을 때 메일 부분을 가지고 있었는지 확인합니다.

SMTP 대화 상자 및 데이터를 확인하여 클라이언트 시스템에서 무엇을 보냈는지 봅니다.

메일 부분이 `tcp_local_slave.log-*` 파일에 표시되지 않았다면 메일이 MTA에 놓이기 전에 문제가 발생한 것입니다. 그 결과 메일이 메일 부분 없이 대기열에 포함되었습니다. 이 경우 보낸 사람의 원격 SMTP 서버 또는 보낸 사람의 클라이언트 시스템에서 문제가 발생했을 수 있습니다.

3. 메일 파일의 복사본을 조사하여 메일 부분이 어디서 변경 또는 누락되었는지 확인합니다.

메일 파일에서 메일 부분이 변경 또는 누락되었음이 표시되면 이전 채널의 로그 파일을 검사합니다. 예를 들어, tcp\_intranet 채널에 놓이는 메일의 메일 부분이 변경 또는 누락된 경우 conversion\_master.log-\* 파일을 확인합니다.

4. 메일의 최종 대상을 확인합니다.

tcp\_local\_slave.log, 메일 파일(예: ZZ01K7LXW76T709TD0TB.KEEP1) 및 channel\_master.log-\* 파일에서 메일 부분이 변경되지 않은 것으로 확인되면 MTA는 메일을 변경하지 않았으며 메일 부분은 해당 최종 대상으로 가는 경로의 다음 단계에서 사라진 것입니다.

최종 대상이 ims-ms 채널(메시지 저장소)인 경우, 메일 부분이 전송 과정 도중이나 이후에 누락되는지를 확인하기 위해 메일을 서버에서 클라이언트 시스템으로 다운로드할 수 있습니다. 대상 채널이 tcp\_\* 채널인 경우에는 메일 경로의 MTA로 이동해야 합니다. 이 MTA를 Messaging Server MTA라고 가정하면 전체 문제 해결 프로세스를 반복해야 합니다(777페이지의 "메일 경로에서 채널 확인", 778페이지의 "수동으로 채널을 시작 및 중지하여 데이터 수집" 및 이 절 참조). 사용자가 관리하는 MTA가 아닌 경우 문제를 보고한 사용자가 해당 사이트에 문의해야 합니다.

## 일반 MTA 문제 및 솔루션

이 절에서는 MTA 구성 및 작업에 대한 일반 문제 및 솔루션을 나열합니다.

- 782페이지의 "영향력이 없는 구성 파일 또는 MTA 데이터베이스에 대한 변경 사항"
- 783페이지의 "MTA에서 보내는 메일은 전송하지만 받는 메일을 수신하지 않음"
- 783페이지의 "디스패처(SMTP Server)가 시작되지 않음"
- 784페이지의 "받는 SMTP 연결의 시간 초과"
- 785페이지의 "메일이 대기열에서 제외되지 않음"
- 787페이지의 "MTA 메일이 전달되지 않음"
- 789페이지의 "메일 루핑"

- 791페이지의 "받은 메일 인코딩"
- 792페이지의 "서버측 규칙(SSR)이 작동하지 않음"

## TLS 문제

SMTP 대화 중에 STARTTLS 명령은 다음 오류를 반환합니다.

```
454 4.7.1 TLS library initialization failure
```

pop/imap에 액세스에 대한 인증서를 설치 및 작동 중에 있다면 다음 사항을 확인하십시오.

- mailsrv 계정이 파일에 액세스할 수 있도록 인증서의 보호/소유권을 설정해야 합니다.
- mailsrv 계정에서 인증서가 저장되는 디렉토리 내의 파일에 액세스할 수 있도록 해당 디렉토리에서 보호/소유권을 설정해야 합니다.

보호를 변경하고 인증서를 설치한 후에는 다음을 실행해야 합니다.

```
stop-msg dispatcher  
start-msg dispatcher
```

다시 시작해도 좋지만 시스템을 완전히 종료하고 인증서를 설치한 다음 다시 시작하는 것이 좋습니다.

## 영향력이 없는 구성 파일 또는 MTA 데이터베이스에 대한 변경 사항

구성, 매핑, 전환, 보안, 옵션 또는 별칭 파일에 대한 변경이 적용되지 않는 경우 다음 단계를 수행했는지 확인합니다.

1. 구성을 다시 컴파일합니다(imsimta cnbuild 실행).
2. 적절한 프로세스(예: imsimta restart dispatcher)를 다시 시작합니다.
3. 모든 클라이언트 연결을 다시 설정합니다.

## MTA에서 보내는 메일은 전송하지만 받는 메일을 수신하지 않음

대부분의 MTA 채널은 받는 메일을 수신하는 슬레이브 또는 채널 프로그램에 의존합니다. MTA가 지원하는 일부 전송 프로토콜(TCP/IP 및 UUCP 등)의 경우 해당 표준 서버 대신 MTA 슬레이브 프로그램을 활성화해야 합니다. Messaging Server 설치의 일환으로 원시 sendmail SMTP 서버가 MTA SMTP 서버로 대체됩니다. 자세한 내용은 *Sun Java System 설치 설명서*를 참조하십시오.

다중 스레드 SMTP 서버의 경우 디스패처에서 SMTP 서버의 시작을 제어합니다. 디스패처가 SMTP 서비스에 대해 1 이상의 MIN\_PROCS 값을 사용하도록 구성된 경우, 적어도 하나 이상(가능한 경우 SMTP 서비스에 대한 MAX\_PROCS 값에 따라 그 이상으로)의 SMTP 서버 프로세스가 항상 실행 중이어야 합니다. `imsimta process` 명령을 사용하여 SMTP 서버 프로세스의 존재 여부를 확인할 수 있습니다. 자세한 내용은 *Sun Java System Messaging Server Administration Reference*의 MTA command-line utilities 장을 참조하십시오.

## 디스패처(SMTP Server)가 시작되지 않음

디스패처가 시작되지 않는 경우에는 먼저 `dispatcher.log-*`에서 관련 오류 메시지를 확인합니다. 로그에서 `/tmp/.SUNWmsgsr.dispatcher.socket` 파일을 만들거나 액세스하는 문제를 표시하는 경우, `/tmp` 보호가 1777로 설정되어 있는지 확인합니다. 사용 권한에 다음과 같이 표시됩니다.

```
drwxrwxrwt  8 root  sys          734 Sep 17 12:14  tmp/
```

또한 `.SUNWmsgsr.dispatcher.socket` 파일의 `ls -l`을 수행하고 적합한 소유권을 확인하십시오. 예를 들어, `root`에서 만든 경우에는 `inetmail`에서 액세스할 수 없습니다.

`SUNWmsgsr.dispatcher.file`을 제거하지 말고 누락된 경우에는 만들지 마십시오. 디스패처에서 해당 파일을 만듭니다. 보호가 1777로 설정되지 않은 경우에는 디스패처가 소켓 파일을 만들고 액세스할 수 없기 때문에 시작 또는 다시 시작하지 않습니다. 또한 Messaging Server와 연관되지 않은 다른 문제들이 발생할 수 있습니다.

## 받는 SMTP 연결의 시간 초과

받는 SMTP 연결의 시간 초과는 흔히 시스템 자원 및 해당 할당과 연관되어 있습니다. 다음 기술을 사용하여 받는 SMTP 연결의 시간 초과 원인을 확인할 수 있습니다.

1. 허용된 동시에 받는 SMTP 연결 수를 확인합니다. 이는 SMTP 서비스에 대한 MAX\_PROCS 및 MAX\_CONNS 디스패처 설정이 제어하며 허용된 동시 연결 수는 MAX\_PROCS\*MAX\_CONNS입니다. 시스템 자원이 충분하고 이 수가 사용량에 비해 너무 적은 경우 수를 늘릴 수 있습니다.
2. 다른 기술로는 TELNET 세션을 여는 것이 있습니다. 다음 예에서는 사용자가 127.0.0.1 포트 25에 연결합니다. 연결되면 220 배너가 반환됩니다. 예를 들면 다음과 같습니다.

```
telnet 127.0.0.1 25
Trying 127.0.0.1...
Connected to 127.0.0.1.
Escape character is '^]'.
220 budgie.sesta.com -- Server ESMTP (Sun Java System Messaging Server 6.1
(built May 7 2001))
```

사용자가 해당 포트에 연결되고 220 배너를 수신하지만 추가 명령(예: ehlo 및 mail from)이 응답을 부정하지 않는 경우, imsimta test -rewrite를 실행하여 구성이 올바른지 확인합니다.

3. 220 배너의 응답 시간이 느리고 SMTP 서버에 pstack 명령이 실행 중인 경우 다음 iii\_res\* 함수가 표시됩니다(이 함수는 이름 확인 조회가 수행 중임을 나타냄).

```
febe2c04 iii_res_send (fb7f4564, 28, fb7f4de0, 400, fb7f458c, fb7f4564) + 142c
febdfdcc iii_res_query (0, fb7f4564, c, fb7f4de0, 400, 7f) + 254
```

그런 다음 호스트는 localhost/127.0.0.1과 같은 일반 쌍에서도 역방향 이름 확인 조회를 실행해야 할 수 있습니다. 이와 같은 성능 저하를 방지하려면 /etc/nsswitch.conf 파일에서 사용자 호스트 조회 순서를 다시 정렬해야 합니다. 그러려면 /etc/nsswitch.conf 파일에서 다음 행을

```
hosts: dns nis [NOTFOUND=return] files
```



아래와 같이 변경했습니다.

```
hosts: files dns nis [NOTFOUND=return]
```

/etc/nsswitch.conf 파일에서 이러한 변경 작업을 수행하면 여러 SMTP 서버가 불필요한 조회를 수행하는 대신 더 적은 수의 SMTP 서버에서 메일을 처리하므로 성능이 향상됩니다.

4. 또한 slave\_debug 키워드를 주로 tcp\_local 및 tcp\_intranet과 같은 TCP/IP 메일을 통해 받는 SMTP를 처리하는 채널에 입력할 수 있습니다. 그런 다음 최근의 tcp\_local\_slave.log-uniqueid 파일을 검토하여 시간 초과된 메일의 특성을 확인합니다. 예를 들어, 수신자가 많은 받는 메일이 시간 초과되는 경우 채널에 expandlimit 키워드를 사용하는 것이 좋습니다.

시스템이 오버로드되고 지나치게 확장된 경우 시간 초과를 완전히 방지할 수는 없습니다.

## 메일이 대기열에서 제외되지 않음

TCP/IP 전달 중에 발생하는 오류는 보통 일시적이며 문제가 발생하면 일반적으로 MTA에서 메일을 보관하고 주기적으로 다시 보내려는 시도를 합니다. 다른 호스트 연결이 정상적으로 작동할 때 대규모 네트워크가 특정 호스트에서 주기적으로 중단되는 것은 정상입니다. 문제를 확인하려면 로그 파일에서 전달 시도와 관련된 오류를 검사합니다. "Fatal error from smtp\_open"과 같은 오류 메시지가 표시될 수 있습니다. 이런 오류는 보편적이며 보통 일시적인 네트워크 문제와 연관되어 있습니다. TCP/IP 네트워크 문제를 디버그하려면 PING, TRACEROUTE 및 NSLOOKUP과 같은 유틸리티를 사용합니다.

다음 예는 메일이 xtel.co.uk에 전달 시 대기열에서 대기하는 이유를 확인하기 위해 사용자가 사용할 수 있는 단계를 보여 줍니다. 메일이 대기열에서 제외되지 않는 이유를 확인하려면 MTA가 TCP/IP에서 SMTP 메일 전달에 사용하는 단계를 다시 만들 수 있습니다.

```
% nslookup -query=mx xtel.co.uk (단계 1)

Server: LOCALHOST
Address: 127.0.0.1

Non-authoritative answer:
XTEL.CO.UK preference = 10, mail exchanger = nsfnet-relay.ac.uk (단계 2)

% telnet nsfnet-relay.ac.uk 25 (단계 3)
Trying... [128.86.8.6]
telnet: Unable to connect to remote host: Connection refused
```

1. NSLOOKUP 유틸리티를 사용하여 이 호스트에 어떤 MX 레코드가 있는지(있는 경우) 확인합니다. MX 레코드가 없으면 호스트에 직접 연결해야 합니다. MX 레코드가 있으면 지정된 MX 릴레이에 연결해야 합니다. 명시적으로 연결하지 말도록 구성된 경우를 제외하면 MTA는 우선적으로 MX 정보를 적용합니다. [348페이지의 "TCP/IP MX 레코드 지원"](#)도 참조하십시오.
2. 이 예에서 DNS(도메인 이름 서비스)는 xtel.co.uk에 대해 지정된 MX 릴레이의 이름을 반환합니다. 이 호스트는 MTA가 실제로 연결할 호스트입니다. 둘 이상의 MX 릴레이가 나열된 경우 MTA는 각 MX 레코드를 기본값이 낮은 것부터 오름차순으로 연속해서 시도합니다.

3. 원격 호스트에 연결된 경우 SMTP 서버 포트 25의 TELNET을 사용하여 인바운드 SMTP 연결을 허용하는지 확인합니다.

**주**            포트를 지정하지 않고 TELNET을 사용하는 경우에는 원격 호스트가 일반 TELNET 연결을 허용합니다. 하지만 위의 경우 원격 호스트가 SMTP 연결을 허용한다는 것을 의미하지는 않습니다. 많은 시스템이 일반 TELNET 연결은 허용하지만 SMTP 연결을 거부하며 또한 그 반대로 SMTP 연결을 허용하지만 TELNET 연결은 거부합니다. 따라서 항상 SMTP 포트에 대해 테스트를 수행해야 합니다.

이전 예에서 원격 호스트는 SMTP 포트에 대한 연결을 거부합니다. 이는 MTA가 메일 전달에 실패하는 이유입니다. 원격 호스트의 잘못된 구성 또는 원격 호스트에서의 일부 자원 고갈로 인해 연결이 거부될 수 있습니다. 이런 경우 문제를 로컬에서 해결할 수 없습니다. 일반적으로 MTA가 메일을 계속해서 시도하도록 합니다.

DNS를 사용하지 않는 TCP/IP 네트워크에 Messaging Server가 실행 중인 경우에는 (단계 1) 및 (단계 2)를 건너뛸 수 있습니다. 대신 TELNET을 사용하여 해당 호스트에 직접 액세스할 수 있습니다. 호스트 이름은 MTA에서 사용하는 이름과 같아야 합니다. 호스트 이름을 확인하려면 MTA의 최근 시도에서 관련 로그 파일을 봅니다. 호스트 파일을 사용하는 경우에는 호스트 이름 정보가 올바른지 확인합니다. 호스트 이름 대신 DNS를 사용해야 합니다.

TCP/IP 호스트에 대한 연결을 테스트할 때 대화식 테스트 사용에 문제가 발생하지 않는 경우 문제는 MTA가 마지막 메일 전달을 시도할 때 간단히 해결되었을 수 있습니다. 메일이 대기열에서 제외되는지 확인하려면 적절한 채널에서 `imsimta submit tcp_channel`을 다시 실행합니다.

## MTA 메일이 전달되지 않음

메일 전송 문제 외에도 메일 대기열에서 메일을 처리할 수 없도록 하는 두 가지 일반적인 문제가 있습니다.

1. 대기열 캐시가 대기열 디렉토리의 메일과 동기화되지 않습니다. 전달 대기 중인 MTA 대기열 하위 디렉토리의 메일 파일은 메모리 내장 대기열 캐시에 놓입니다. 채널 프로그램이 실행되는 경우에는 이 대기열 캐시에 문의하여 해당 대기열에서 어떤 메일을 전달할지 결정합니다. 대기열에 메일 파일이 있지만 해당 대기열 캐시 항목이 없는 경우도 있습니다.

- a. 대기열 캐시에 특정 파일이 있는지 확인하려면 `imsimta cache -view` 유틸리티를 사용하고 파일이 대기열 캐시에 없는 경우 대기열 캐시를 동기화해야 합니다.

대기열 캐시는 보통 4시간마다 동기화됩니다. 필요하다면 `imsimta cache -sync` 명령을 사용하여 캐시를 수동으로 다시 동기화할 수 있습니다. 이 채널 프로그램은 일단 동기화되면 새 메일이 처리된 후에도 처리되지 않는 원본 메일을 처리합니다. 기본값(4시간)을 변경하려면 대기열 캐시의 동기화 빈도를 반영하는 `timeperiod`가 있는 `sync_time=timeperiod`를 추가하여 `/msg_svr_base/config` 디렉토리의 `job_controller.cnf` 파일을 수정합니다. `timeperiod`는 30분보다 커야 합니다. 다음 예에서는 `sync_time=02:00`을 `job_controller.cnf`의 전역 기본 섹션에 추가하여 동기화를 2시간으로 수정합니다.

```
! VERSION=5.0
!IMTA job controller configuration file
!
!Global defaults
tcp_port=27442
secret=N1Y9[HzQKW
slave_command=NULL
sync_time=02:00
```

`imsimta cache -sync`를 실행한 후 `imsimta submit channel`을 실행하여 메일의 백로그를 모두 지웁니다. 메일의 백로그가 큰(1000 이상) 경우 채널을 모두 지우는 데 긴 시간이 필요할 수도 있다는 점에 유의해야 합니다.

요약된 대기열 캐시 정보에 대해서는 `imsimta qm -maint dir -database -total`을 실행합니다.

- b. 대기열 캐시를 동기화한 후에도 메일이 전달되지 않으면 **Job Controller**를 다시 시작해야 합니다. 그러려면 `imsimta restart job_controller` 명령을 사용합니다.

**Job Controller**를 다시 시작하면 디스크에서 메일 대기열의 메일 데이터 구조가 재구성됩니다.

---

**주의**            **Job Controller**를 다시 시작하는 것은 최후의 수단으로 다른 방법을 모두 사용해 본 후에 수행되어야 합니다.

---

Job Controller에 대한 자세한 내용은 194페이지의 "Job Controller"를 참조하십시오.

2. 해당 처리 로그 파일을 만들 수 없기 때문에 채널 처리 프로그램을 실행할 수 없습니다. 액세스 권한, 디스크 공간 및 할당량을 확인하십시오.

## 메일 루핑

MTA가 메일 루핑을 감지하면 해당 메일은 .HELD 파일로 취급되어 보류됩니다. 790페이지의 ".HELD 메일 진단 및 정리"를 참조하십시오. 특정 경우에는 MTA에서 감지할 수 없는 메일 루프가 발생할 수 있습니다.

첫 번째 단계로 메일 루핑의 원인을 확인합니다. 해당 채널에 대해 문제 메일 파일이 MTA 대기열 영역, 문제 메일과 연관된 MTA 메일 로그 항목(해당 채널에 대한 MTA 구성 파일에서 logging 채널 키워드를 활성화한 경우) 및 MTA 채널 디버그 로그 파일에 있는 동안 문제 메일 파일의 복사본을 검토해야 합니다. 문제 메일에 대한 From: 및 To: 주소와 Received: 헤더 행 및 메일 구조(메일 내용의 캡슐화 유형)를 확인하는 것은 발생할 수 있는 메일 루프 유형을 정확히 아는데 도움이 됩니다.

보다 일반적인 경우는 다음과 같습니다.

1. 포스트마스터 주소가 손상되었습니다.

MTA는 포스트마스터 주소로 전자 메일을 받도록 합니다. 포스트마스터로 보낸 메일이 루핑되는 경우에는 메일을 받을 수 있는 계정을 가르키는 적절한 포스트마스터 주소가 구성되어 있는지 확인합니다.

2. Received: 헤더 행을 제거하면 MTA에서 메일 루프를 감지할 수 없습니다.

정상적인 메일 루프 감지는 Received: 헤더 행에 매핑하는 데만 사용됩니다.

Received: 헤더 행이 제거되면(해당 MTA 시스템에서 명시적으로 또는 방화벽과 같은 다른 시스템에서) 메일 루프를 적절히 감지하는 것을 방해할 수 있습니다. 이 시나리오에서는 원하지 않는 Received: 헤더 행이 제거되지 않도록 합니다. 또한 근본적인 메일 루핑 원인을 조사합니다. 시스템 이름 할당 문제, 해당 이름의 변형을 인식하지 못하게 구성된 시스템 문제, DNS 문제, 해당 시스템의 인증 주소 지정 정보 없음 또는 사용자 주소 전달 오류 등이 있습니다.

3. 다른 메시징 시스템이 알림 메일을 잘못 처리하면 알림 메일에 대한 응답으로 다시 캡슐화된 메일이 생성됩니다.

인터넷 표준은 메일 루프를 방지하기 위해 알림 메일(전달되는 메일 또는 튕겨지는 메일에 대한 보고서)에 받는 사람 주소가 공백인 봉투를 요구합니다. 하지만 일부 메시징 시스템은 이러한 알림 메일을 제대로 처리하지 않습니다. 알림 메일을 전달 또는 튕기는 경우 이 메시징 시스템은 새 **From:** 주소에서 추출된 SMS 대상 주소의 숫자가 아닌 모든 문자를 스트라이프하려면 이 옵션을 사용합니다. 이 봉투를 삽입하면 메일 루프가 발생할 수 있습니다. 해결책은 알림 메일을 제대로 처리하지 못하는 메시징 시스템을 수정하는 것입니다.

### .HELD 메일 진단 및 정리

MTA에서 메일이 서버 또는 채널 사이에서 튕겨지는 것을 감지하면 전달이 중단되고 메일이 `/msg_svr_base/data/queue/channel`의 `.HELD` 접미어를 가진 파일에 저장됩니다. 일반적으로 각 서버 또는 채널은 메일 전달에 대한 책임이 다른 서버 또는 채널에 있다고 생각하기 때문에 메일 루프가 발생합니다.

예를 들어, 최종 사용자는 서로 다른 두 개의 메일 호스트에서 서로에게 메일을 전달하도록 옵션을 설정할 수 있습니다. 최종 사용자는 `sesta.com` 계정에서 `varrius.com` 계정으로 메일이 전달되도록 합니다. 그 후 최종 사용자가 이 설정을 사용 가능하게 한 사실을 잊고 `varrius.com` 계정에서 `sesta.com` 계정으로 메일이 전달되도록 설정합니다.

또한 MTA 구성 결함으로 인해 루프가 발생할 수 있습니다. 예를 들어, MTA 호스트 X는 `mail.sesta.com`에 대한 메일이 호스트 Y로 간다고 생각합니다. 하지만 호스트 Y는 `mail.sesta.com`에 대한 메일을 호스트 X가 처리해야 한다고 생각하기 때문에 메일을 호스트 X에게 반환합니다.

이런 경우 MTA는 메일을 무시하고 더 이상의 전달을 시도하지 않습니다. 이러한 문제가 발생하면 메일을 튕기는 서버나 채널을 알기 위해 메일의 헤더 행을 확인합니다. 필요에 따라 항목을 수정합니다.

또한 `imsimta qm release`를 실행하거나 다음 단계를 수행하여 `.HELD` 메일을 재시도할 수 있습니다.

1. `.HELD` 확장자 이름을 00위의 두 자리 숫자로 바꿉니다(예: `.HELD`에서 `.06`으로).

---

**주** `.HELD` 파일의 이름을 바꾸기 전에 메일이 루핑을 중단해야 합니다.

---

2. `imsimta cache -sync`를 실행합니다. 이 명령을 실행하면 캐시가 업데이트됩니다.
3. `imsimta submit channel` 또는 `imsimta run channel`을 실행합니다.

Received: 헤더 행이 축적되어 메일이 다시 .HELD로 표시될 수 있으므로 이 단계를 여러 번 수행해야 할 수도 있습니다.

## 받은 메일 인코딩

MTA에서 보낸 메일은 인코딩된 형식으로 수신됩니다. 예를 들면 다음과 같습니다.

```
Date: Wed, 04 Jul 2001 11:59:56 -0700 (PDT)
From: "Desdemona Vilalobos" <Desdemona@sesta.com>
To: santosh@varrius.com
Subject: test message with 8bit data
MIME-Version: 1.0
Content-type: TEXT/PLAIN; CHARSET=ISO-8859-1
Content-transfer-encoding: QUOTED-PRINTABLE

2=00So are the Bo=F6tes Void and the Coal Sack the same?=
```

이러한 메일은 MTA 디코더 명령인 `msmtp decode`를 통해 읽을 때 인코딩되지 않은 상태로 표시됩니다. 자세한 내용은 *Sun Java System Messaging Server Administration Reference*를 참조하십시오.

SMTP 프로토콜은 RFC 821에 설명된 것과 같이 ASCII 문자(7비트 문자 세트)의 전송만을 허용합니다. SMTP를 사용한 8비트 문자의 검토되지 않은 전송은 유효하지 않으며 일부 SMTP 서버에 다양한 문제를 일으키는 것으로 알려져 있습니다. 예를 들어, SMTP 서버는 연산 관련 루프로 이동할 수 있습니다. 메일이 계속해서 다시 보내집니다. 8비트 문자는 서버 충돌을 일으킬 수 있습니다. 마지막으로 8비트 문자 세트는 8비트 데이터를 처리할 수 없는 브라우저 및 메일함을 복잡하게 만들 수 있습니다.

SMTP 클라이언트는 8비트 데이터를 포함하는 메일을 처리할 때 보낸 사람에게 전달할 수 없는 것으로 메일을 반환하거나, 메일을 코드화하거나, RFC 821을 직접 위반하여 메일 보내기와 같은 세 가지 옵션만을 가지고 있습니다. 하지만 MIME 및 SMTP 확장자의 발명으로 이제 ASCII 문자 세트를 사용하여 8비트 데이터 코드화에 사용할 수 있는 표준 인코딩 옵션이 있습니다.

이전 예에서 수신자는 TEXT/PLAIN의 MIME 내용 유형으로 인코딩된 메일을 받았으며, 원격 SMTP 서버(MTA SMTP 클라이언트가 메일을 전송한 서버)는 8비트 데이터의 전송을 지원하지 않았습니다. 하지만 원본 메일이 8비트 문자를 포함하고 있기 때문에 MTA가 메일을 인코딩해야 했습니다.

## 서버측 규칙(SSR)이 작동하지 않음

필터는 메일 메시지에 적용할 하나 이상의 조건부 작업으로 구성되어 있습니다. 필터는 서버에 저장 및 평가되므로 흔히 서버측 규칙(SSR)이라고 합니다.

이 절에서는 다음 SSR 관련 항목에 대해 설명합니다.

- [792페이지의 "사용자 SSR 규칙 테스트"](#)
- [792페이지의 "일반 구문 문제"](#)

[545페이지의 "사용자 수준 필터 디버그"](#)도 참조하십시오.

### 사용자 SSR 규칙 테스트

- MTA의 사용자 필터를 확인하려면 다음 명령을 사용합니다.

```
# imsimta test -rewrite -debug -filter user@domain
```

출력에서는 다음 정보를 찾습니다.

```
mmc_open_url called to open ssrf:user@ims-ms
  URL with quotes stripped: ssrd:user@ims-ms
Determined to be a SSRD URL.
  Identifier: user@ims-ms-daemon
Filter successfully obtained.
```

- 추가로 필터의 적용 방법을 보기 위해 tcp\_local 채널에 slave\_debug 키워드를 추가할 수 있습니다. 결과는 tcp\_local\_slave.log 파일에 표시됩니다. 충분한 디버깅 정보를 얻으려면 /msg\_svr\_base/config 디렉토리의 option.dat 파일에 mm\_debug=5를 추가해야 합니다.

### 일반 구문 문제

- 필터에 구문 문제가 있는 경우 tcp\_local\_slave.log-\* 파일에서 다음 메시지를 찾습니다.

```
Error parsing filter expression:...
```

  - 필터 상태가 양호하면 출력 끝에 필터 정보가 표시됩니다.



- 필터 상태가 양호하지 않으면 출력 끝에 다음 오류가 표시됩니다.  
Address list error -- 4.7.1 Filter syntax error:  
desdaemon@sesta.com

또한 필터 상태가 양호하지 않으면 SMTP RCPT TO 명령에서 다음과 같은 임시 오류 응답 코드를 반환합니다.

```
RCPT TO:user@domain
452 4.7.1 Filter syntax error
```

## 받은 필드 또는 주소의 로컬 부분에 있는 별표

이제 MTA는 구성된 받은 필드뿐만 아니라 주소의 로컬 부분에서 8비트 문자(단순히 ASCII 문자가 아니라)를 검사하고 이 문자를 별표로 바꿉니다.

## 일반 오류 메시지

MTA가 시작되지 않으면 명령줄에 일반 오류 메시지가 표시됩니다. 이 절에서는 일반 오류 메시지를 설명하고 진단합니다.

---

**주**            고유한 사용자 MTA 구성을 진단하려면 `imsimta test -rewrite -debug` 유틸리티를 사용하여 사용자의 MTA 주소 다시 쓰기 및 채널 매핑 프로세스를 검사합니다. 이 유틸리티를 사용하여 메일을 실제로 보내지 않고도 해당 구성을 확인할 수 있습니다. [771페이지의 "MTA 구성 확인"](#)을 참조하십시오.

---

또한 MTA 하위 구성 요소는 이 장에서 설명하지 않은 다른 오류 메시지를 표시할 수도 있습니다. 명령줄 유틸리티 및 구성에 대한 장은 *Sun Java System Messaging Server Administration Reference*를 참조하고 각 하위 구성 요소에 대한 자세한 내용은 5장에서 10장을 참조하십시오. 이 절에서는 다음 오류 유형에 대해 설명합니다.

- [794페이지의 "mm\\_init 오류"](#)
- [797페이지의 "컴파일된 구성 버전이 일치하지 않음"](#)
- [798페이지의 "공간 오류 스왑"](#)

- 798페이지의 "파일 열기 또는 오류 만들기"
- 799페이지의 "유효하지 않은 호스트/도메인 오류"
- 800페이지의 "SMTP 채널 오류: os\_smtp\_\* errors"

## mm\_init 오류

mm\_init 오류는 일반적으로 MTA 구성 문제를 나타냅니다. `imsimta test -rewrite` 유틸리티를 실행하면 이러한 오류가 표시됩니다. `imsimta cnbuild`, 채널, 서버 또는 브라우저와 같은 다른 유틸리티에서도 이와 같은 오류를 반환합니다.

일반적으로 발생하는 mm\_init 오류는 다음과 같습니다.

- 794페이지의 "bad equivalence for alias. . ."
- 794페이지의 "cannot open alias include file . ."
- 795페이지의 "duplicate aliases found . ."
- 795페이지의 "duplicate host in channel table . ."
- 795페이지의 "duplicate mapping name found. . ."
- 795페이지의 "mapping name is too long. ."
- 796페이지의 "error initializing ch\_ facility: compiled character set version mismatch"
- 796페이지의 "error initializing ch\_ facility: no room in. . ."
- 796페이지의 "local host alias or proper name too long for system. . ."
- 796페이지의 "no equivalence addresses for alias. . ."
- 796페이지의 "no official host name for channel. . ."
- 797페이지의 "official host name is too long"

### bad equivalence for alias. . .

별칭 파일 항목의 오른쪽의 서식 지정이 잘못되었습니다.

### cannot open alias include file . .

별칭 파일에 포함된 파일을 열 수 없습니다.

**duplicate aliases found . .**

두 개의 별칭 파일 항목의 왼쪽이 동일합니다. 중복된 별칭을 찾아서 제거해야 합니다. 행 번호 XXX인 `error line #XXX` 오류 메시지를 찾습니다. 해당 행에서 중복된 별칭을 수정할 수 있습니다.

**duplicate host in channel table . .**

이 오류 메시지는 MTA 구성에 공식 호스트 이름이 같은 두 개의 채널 정의가 있다는 것을 표시합니다.

사용자 구성 파일(imta.cnf)의 다시 쓰기 규칙(위쪽)에 추가로 생긴 빈 행으로 인해 MTA는 나머지 구성 파일을 채널 정의로 해석하게 됩니다. 파일의 맨 처음 행이 빈 행이 아니어야 합니다. 동일한 패턴(왼쪽)의 다시 쓰기 규칙이 많으므로 MTA는 이 규칙을 고유하지 않은 공식 호스트 이름을 가진 채널 정의로 해석합니다. 모든 중복된 공식 호스트 이름을 가진 채널 정의 및 파일의 위(다시 쓰기 규칙)쪽에 있는 잘못된 모든 빈 행에 대해 MTA 구성을 확인합니다.

**duplicate mapping name found. . .**

이 메시지는 두 개의 매핑 테이블이 같은 이름을 가지고 있다는 것을 나타내며 중복된 매핑 테이블 중 한 개는 제거되어야 합니다. 하지만 매핑 파일의 서식 지정 오류로 인해 MTA에서 무관한 것을 매핑 테이블 이름으로 잘못 해석할 수도 있습니다. 예를 들어, 매핑 테이블 항목을 적절하게 들여쓰지 않으면 MTA에서 항목의 왼쪽이 실질적인 매핑 테이블 이름인 것으로 잘못 생각할 수 있습니다. 일반 형식 매핑 테이블을 검사하고 매핑 테이블 이름을 확인합니다.

---

**주** 빈 행은 매핑 테이블 이름을 가진 모든 행의 앞뒤에 있어야 합니다. 하지만 어떤 빈 행도 매핑 테이블의 항목 간에 산재해 있으면 안 됩니다.

---

**mapping name is too long. .**

이 오류는 매핑 테이블이 이름이 너무 길어서 줄여야 함을 의미합니다. 매핑 파일의 서식 지정 오류로 인해 MTA에서 무관한 것을 매핑 테이블 이름으로 잘못 해석할 수도 있습니다. 예를 들어, 매핑 테이블 항목을 적절하게 들여쓰지 않으면 MTA에서 항목의 왼쪽이 실질적인 매핑 테이블 이름인 것으로 잘못 생각할 수 있습니다. 매핑 파일 및 매핑 테이블 이름을 확인합니다.

### error initializing ch\_facility: compiled character set version mismatch

이 메시지가 표시되면 `imsimta chbuild` 명령을 통해 컴파일된 문자 세트 테이블을 다시 컴파일하고 다시 설치해야 합니다. 자세한 내용은 *Sun Java System Messaging Server Administration Reference*를 참조하십시오.

### error initializing ch\_facility: no room in. . .

일반적으로 이 오류 메시지는 MTA 문자 세트 내부 테이블의 크기를 조정해야 한다는 것을 의미하며 다음 명령을 통해 컴파일된 문자 세트 테이블을 다시 만듭니다.

```
imsimta chbuild -noimage -maximum -option  
imsimta chbuild
```

위와 같이 변경하기 전에는 아무것도 다시 컴파일하거나 다시 시작하지 않도록 합니다. `imsimta chbuild`에 대한 자세한 내용은 *Sun Java System Messaging Server Administration Reference*의 MTA command-line utilities 장을 참조하십시오.

### local host alias or proper name too long for system. . .

이 오류는 로컬 호스트 별칭 또는 해당 이름이 너무 길다는 것을 나타냅니다(채널 블록에서 두 번째 또는 후속 이름 중 하나의 오른쪽). 하지만 초기 MTA 구성 파일(예: 다시 쓰기 규칙의 추가적인 빈 행)의 일부 구문 오류로 인해 MTA에서 무관한 것을 채널 정의로 잘못 해석할 수도 있습니다. 구성 파일의 표시된 행을 확인하는 것 외에도 다른 구문 오류에 대해 위의 해당 행을 확인합니다. 특히 MTA에서 이 오류를 표시하는 행이 다시 쓰기 규칙으로 사용되는 경우 반드시 그 위의 추가적인 빈 행을 확인해야 합니다.

### no equivalence addresses for alias. . .

별칭 파일에 있는 항목의 오른쪽(번역 값)이 없습니다.

### no official host name for channel. . .

이 오류는 채널 정의 블록에 필수적인 두 번째 행(공식 호스트 이름 행)이 없다는 것을 나타냅니다. 채널 정의 블록에 대한 자세한 내용은 *Sun Java System Messaging Server Administration Reference*의 MTA 구성 및 명령줄 유틸리티 장 및 12장, "채널 정의 구성"을 참조하십시오. 각 채널 정의 블록 전후에는 빈 행이 필요하지만 채널 정의의 채널 이름과 공식 호스트 이름 행 사이에 빈 행이 있어서는 안 됩니다. 또한 빈 행은 MTA 구성 파일의 다시 쓰기 규칙 부분에 허용되지 않습니다.

## official host name is too long

채널(채널 정의 블록의 두 번째 행)의 공식 호스트 이름 길이는 128진수로 제한됩니다. 채널에 더 긴 공식 호스트 이름을 사용하려면 이를 자리 표시자 이름으로 줄인 다음 다시 쓰기 규칙을 사용하여 긴 이름을 짧은 공식 호스트 이름에 일치시킵니다. 1(로컬) 채널 호스트 이름을 사용하면 이 시나리오를 볼 수 있습니다. 예를 들면 다음과 같습니다.

```
Original 1 Channel:
!delivery channel to local /var/mail store
1 subdirs 20 viaaliasrequired maxjobs 7 pool LOCAL_POOL
walleroo.pocofronitas.thisnameismuchtoolongandreallymakesnosense
butitisanexample.monkey.gorilla.orangutan.antidisestablimentari
anism.newt.salamander.lizard.gecko.komododragon.com

Create Place Holder:
!delivery channel to local /var/mail store
1 subdirs 20 viaaliasrequired maxjobs 7 pool LOCAL_POOL
newt

Create Rewrite Rule:
newt.salamander.lizard.gecko.komododragon.com    $U%$D@newt
```

1(로컬) 채널을 사용하는 경우에는 REVERSE 매핑 테이블을 사용해야 합니다. 사용법 및 구문에 대한 자세한 내용은 *Sun Java System Messaging Server Administration Reference*의 MTA configuration 장을 참조하십시오.

초기 MTA 구성 파일의 특정 구문 오류(예: 다시 쓰기 규칙의 추가적인 빈 행)로 인해 MTA에서 무관한 것을 채널 정의로 잘못 해석할 수 있습니다. 이로 인해 의도된 다시 쓰기 규칙이 공식 호스트 이름으로 해석될 수 있습니다. 구성 파일의 표시된 행을 확인하는 것 외에도 다른 구문 오류에 대해 위의 해당 행을 확인합니다. 특히 MTA에서 이 오류를 표시하는 행이 다시 쓰기 규칙으로 사용되는 경우 반드시 그 위의 추가적인 빈 행을 확인해야 합니다.

## 컴파일된 구성 버전이 일치하지 않음

imsimta cnbuild 유틸리티의 기능 중 하나는 신속하게 로드되는 이미지에 MTA 구성 정보를 컴파일하는 것입니다. 컴파일 형식은 엄격히 정의되며 MTA의 버전에 따라 상당한 차이가 있습니다. 사소한 변경 사항이 패치 릴리스의 일부로 발생할 수 있습니다.

이와 같은 변경 사항이 발생하면 호환되지 않는 형식을 감지할 수 있도록 내부 버전 필드도 변경됩니다. 호환되지 않는 형식이 감지되면 MTA 구성 요소가 위의 오류와 같이 정지합니다. 이 문제에 대한 해결책은 `imsimta cnbuild` 명령을 사용하여 새로 컴파일된 구성을 생성하는 것입니다.

또한 업데이트된 구성 정보를 얻을 수 있도록 `imsimta restart` 명령을 사용하여 모든 상주 MTA 서버 프로세스를 다시 시작하는 것도 좋은 방법입니다.

## 공간 오류 스왑

제대로 작동하게 하려면 사용자의 메시징 시스템에 충분한 스왑 공간을 구성하는 것이 중요합니다. 사용자의 구성에 따라 필수 스왑 공간 크기가 다릅니다. 일반적인 조정 권장 사항으로는 스왑 공간의 크기가 적어도 주 기억 장치 크기의 3배여야 합니다.

다음은 스왑 공간이 없음을 알리는 오류 메시지입니다.

```
jbc_channels: chan_execute [1]: fork failed: Not enough space
```

이 오류를 Job Controller 로그 파일에서 볼 수도 있습니다. 다른 스왑 공간 오류는 사용자 구성에 따라 다릅니다.

다음 명령을 사용하여 사용한 스왑 공간과 남은 스왑 공간 크기를 확인할 수 있습니다.

- Solaris 시스템: `swap -s`(MTA 프로세스를 사용 중인 경우) `ps -elf` 또는 `tail /var/adm/messages`
- HP-UX 시스템: `swapinfo` 또는 `tail /var/adm/syslog/syslog.log`

## 파일 열기 또는 오류 만들기

메일을 보내려면 MTA는 MTA 메일 대기열 디렉토리에서 구성 파일을 읽거나 메일 파일을 만듭니다. 구성 파일은 MTA 또는 MTA의 SKD에 대해 쓰여진 모든 프로그램으로 읽을 수 있어야 합니다. 설치하는 동안 적절한 사용 권한이 이 파일에 할당됩니다. 구성 파일을 만드는 MTA 유틸리티 및 절차도 사용 권한을 할당합니다. 시스템 관리자가 해당 파일을 보호하는 경우에는 다른 권한있는 사용자 또는 일부 사이트별 절차를 통해 MTA에서 구성 정보를 읽지 못할 수 있습니다. 이런 경우 "파일 열기" 오류 또는 예기치 않은 동작이 발생합니다. `imsimta test -rewrite` 유틸리티는 구성 파일 읽기에 문제가 발생하면 추가 정보를 보고합니다. *Sun Java System Messaging Server Administration Reference*의 MTA 장에서 `imsimta test -rewrite` 설명을 참조하십시오.

MTA가 권한이 있는 계정에서는 작동하고 권한이 없는 계정에서는 작동하지 않는 것처럼 보이는 경우에는 MTA 테이블 디렉토리의 파일 사용 권한이 문제의 원인일 수 있습니다. 구성 파일 및 해당 디렉토리에서 사용 권한을 확인합니다. [771페이지의 "중요 파일의 소유권 확인"](#)을 참조하십시오.

일반적으로 "파일 만들기" 오류는 MTA 메일 대기열 디렉토리에서 메일 파일을 만드는 중에 발생하는 문제를 나타냅니다. 파일 만들기 문제를 진단하려면 [771페이지의 "메일 대기열 디렉토리 확인"](#)을 참조하십시오.

## 유효하지 않은 호스트/도메인 오류

브라우저를 통해 주소가 MTA에 제공되는 경우 이 오류가 나타날 수 있습니다. 또는, 오류 반환 메일 메시지의 일부로 오류가 지연되고 반환될 수 있습니다. 두 경우 모두 이 오류 메시지는 MTA가 지정된 호스트에게 메일을 전달할 수 없다는 것을 나타냅니다. 지정된 호스트에게 메일을 보낼 수 없는 이유를 확인하려면 다음 문제 해결 절차를 수행해야 합니다.

- 해당 주소가 잘못되었거나, 잘못 옮겨졌거나, 존재하지 않는 호스트 또는 도메인의 이름을 사용하지 않았는지 확인합니다.
- `imsimta test -rewrite` 유틸리티를 통해 해당 주소를 실행합니다. 이 유틸리티에서도 해당 주소에 대해 "유효하지 않은 호스트/도메인" 오류를 반환하는 경우, MTA에는 `imta.cnf` 파일 및 관련 파일에 해당 주소를 처리할 수 있는 규칙이 없는 것입니다. MTA를 올바르게 구성하고 모든 구성 질문에 대해 적절하게 응답했으며 최신 구성 정보를 유지하는지 확인합니다.
- `imsimta test -rewrite`에서 주소에 대한 오류가 발생하지 않으면 MTA는 주소 처리 방법을 결정할 수 있지만 네트워크 전송이 해당 주소를 받아들이지 않습니다. 추가 세부 사항은 전달 시도에서 적절한 로그 파일을 확인할 수 있습니다. 잘못 구성된 도메인 이름 서버가 문제를 발생시킬 수 있지만 일시 네트워크 라우팅 또는 이름 서비스 오류는 오류 메시지를 반환하면 안 됩니다.
- 인터넷을 사용하는 경우 MX 레코드 조회를 지원하는 TCP/IP 채널을 제대로 구성했는지 확인합니다. 인터넷 상에서는 많은 도메인 주소에 직접 액세스할 수 없으며 메일 시스템에서 MX 항목을 제대로 해결해야 합니다. 인터넷을 사용하고 TCP/IP가 MX 레코드를 지원하도록 구성된 경우 MX 지원이 사용 가능하도록 MTA를 구성해야 합니다. 자세한 내용은 [343페이지의 "TCP/IP 연결 및 DNS 조회 지원"](#)을 참조하십시오. TCP/IP 패키지가 MX 레코드 조회를 지원하도록 구성되지 않은 경우에는 MX 전용 도메인에 연결할 수 없습니다.

## SMTP 채널 오류: os\_smtp\_\* errors

os\_smtp\_open, os\_smtp\_read, and os\_smtp\_write 오류 등의 os\_smtp\_\* 오류가 반드시 MTA 오류인 것은 아닙니다. 이러한 오류는 MTA가 네트워크 계층에서 발생한 문제를 보고할 때 생성됩니다. 예를 들어, os\_smtp\_open 오류는 원격측 네트워크 연결을 열 수 없다는 것을 의미합니다. MTA가 주소 지정 오류나 채널 구성 오류로 인해 잘못된 시스템에 연결되도록 구성되어 있을 수 있습니다. 일반적으로 os\_smtp\_\* 오류는 DNS 또는 네트워크 연결 문제로 인해 발생하며 특히, 이전에 작업 채널 또는 주소였다면 os\_smtp\_read 또는 os\_smtp\_write 오류는 보통 다른 쪽에서 연결을 중단하거나 네트워크 문제로 인해 연결이 중단되었다는 것을 나타냅니다.

네트워크 및 DNS 문제는 일시적인 경우가 많습니다. 따라서 가끔 발생하는 os\_smtp\_\* 오류는 신경쓰지 않아도 됩니다. 하지만 이 오류가 지속적으로 나타난다는 것은 기본 네트워크 문제를 나타내는 것일 수 있습니다.

특정 os\_smtp\_\* 오류에 대한 자세한 내용을 얻으려면 해당 채널에서 디버깅을 활성화합니다. 시도된 SMTP 대화의 세부 사항을 표시하는 디버그 채널 로그 파일을 조사합니다. 특히 SMTP 대화 중에 언제 네트워크 문제가 발생했는지 확인합니다. 그 시간으로 네트워크 또는 원격측 문제의 유형을 알 수도 있습니다. 경우에 따라 네트워크 수준 디버깅(예: TCP/IP 패킷 추적)을 수행하여 보내거나 받은 메일을 확인할 수 있습니다.



# Messaging Server 모니터링

일반적으로 제대로 계획 및 구성된 서버는 관리자의 광범위한 개입 없이 작동합니다. 그러나 서버에서 문제의 징후를 모니터링하는 것은 관리자가 해야 할 일입니다. 이 장에서는 Messaging Server의 모니터링에 대해 설명합니다. 이 장은 다음 내용으로 구성되어 있습니다.

- 802페이지의 "일상적인 모니터링 작업"
- 803페이지의 "시스템 성능 모니터링"
- 807페이지의 "MTA 모니터링"
- 810페이지의 "메일 액세스 모니터링"
- 810페이지의 "LDAP Directory Server 모니터링"
- 813페이지의 "메시지 저장소 모니터링"
- 815페이지의 "모니터링을 위한 유틸리티와 도구"

문제 해결 절차는 22장, "MTA 문제 해결"에서 확인할 수 있습니다.

## 자동 모니터링 및 재시작

Messaging Server는 서비스를 투명하게 모니터링하고 서비스가 실패하거나 응답하지 않는 경우(즉, 서비스가 중지되거나 멈춘 경우) 서비스를 자동으로 다시 시작하는 방법을 제공합니다. Messaging Server는 IMAP, POP, HTTP, Job Controller, 디스패처 및 MMP 서버를 비롯한 모든 메시지 저장소, MTA 및 MMP 서비스를 모니터링할 수 있지만 SMS 또는 TCP/SNMP 서버와 같은 다른 서비스는 모니터링하지 않습니다. TCP/SNMP는 Job Controller에서 모니터링합니다. 자세한 내용은 110페이지의 "실패했거나 응답이 없는 서비스의 자동 재시작" 및 824페이지의 "msprobe 및 watcher 기능을 사용하여 모니터링"을 참조하십시오.

## 일상적인 모니터링 작업

일상적으로 수행해야 하는 가장 중요한 작업은 포스트마스터 메일 검사, 로그 파일 모니터링 및 stored 유틸리티 설정입니다. 아래에서는 이러한 작업에 대해 설명합니다.

### 포스트마스터 메일 검사

Messaging Server에는 포스트마스터 전자 메일용으로 설정된 관리 메일 목록이 미리 정의되어 있습니다. 이 메일 목록에 속한 모든 사용자는 포스트마스터로 주소 지정된 메일을 자동으로 받게 됩니다.

포스트마스터 메일에 대한 규칙은 RFC822에서 정의됩니다. RFC822에 따르면 모든 전자 메일 사이트에서 postmaster라는 이름의 사용자 또는 메일 목록으로 주소 지정된 메일을 수락해야 하며 이 주소로 보내진 메일은 실제 당사자에게 전달되어야 합니다.

postmaster@host.domain으로 보내진 모든 메일은 포스트마스터 계정 또는 메일 목록으로 보내집니다.

일반적으로 포스트마스터 주소는 사용자가 메일 서비스에 대한 전자 메일을 보내야 하는 곳입니다. 포스트마스터는 예를 들어, 서버 응답 시간에 대한 메일을 로컬 사용자로부터 받거나 서버로 메일을 보내는 데 문제가 있다는 내용의 메일을 다른 서버 관리자로부터 받을 수 있습니다. 포스트마스터 메일은 메일 확인해야 합니다.

특정 오류 메시지를 포스트마스터 주소로 보내도록 서버를 구성할 수도 있습니다. 예를 들어, MTA가 메일을 라우팅 또는 전달하지 못할 경우 포스트마스터 주소로 보내진 전자 메일을 통해 알림을 받을 수 있습니다. 또한 예외적인 상황에 대한 경고(디스크 공간 부족, 서버 응답 실패 등에 대한)를 포스트마스터에게 보낼 수도 있습니다.

### 로그 파일 모니터링 및 유지 관리

Messaging Server는 지원되는 각각의 주요 프로토콜이나 서비스(SMTP, IMAP, POP 및 HTTP)에 대한 별도의 로그 파일 집합을 생성합니다. 이러한 로그 파일은 *msg\_svr\_base/data/log*에 위치합니다. 로그 파일은 정기적으로 모니터링해야 하며, 특히 서버에 문제가 있는 경우에는 이러한 모니터링이 더욱 필요합니다.

로그가 서버 성능에 영향을 줄 수 있다는 것을 유의하십시오. 더 자세한 로깅을 지정할수록 일정한 시간 동안 로그 파일이 차지하는 디스크 공간이 더 많아집니다. 따라서 효과적이면서 실제적인 로그 회전, 만료 및 백업 정책을 서버에 정의해야 합니다. 서버의 로깅 정책 정의에 대한 자세한 내용은 [21장, "로깅 관리"](#)를 참조하십시오.

## msprobe 유틸리티 설정

msprobe 유틸리티는 자동으로 모니터링을 수행하고 기능을 다시 시작합니다. 자세한 내용은 [824페이지](#)의 "msprobe 및 watcher 기능을 사용하여 모니터링"을 참조하십시오.

## 시스템 성능 모니터링

이 장에서는 Messaging Server 모니터링에 초점을 맞추고 있지만 서버가 상주하는 시스템도 모니터링해야 합니다. 적절하게 구성된 서버는 잘못 구성된 시스템에서 제대로 작동할 수 없으며 하드웨어가 전자 메일 로드를 감당할 만큼 성능이 충분하지 않다는 서버 오류의 증상이 나타날 수 있습니다. 시스템 성능을 모니터링하기 위한 절차가 플랫폼마다 차이가 있고 해당 플랫폼의 시스템 설명서를 참조할 필요가 있다는 점에서 이 장에서 이러한 절차를 자세히 다루지는 않습니다. 여기에서는 성능 모니터링을 위한 다음 절차에 대해 설명합니다.

- [803페이지](#)의 "종단간 메일 전달 시간 모니터링"
- [804페이지](#)의 "디스크 공간 모니터링"
- [806페이지](#)의 "CPU 사용 모니터링"

## 종단간 메일 전달 시간 모니터링

전자 메일은 제때 전달되어야 합니다. 이는 서비스 계약 요구 사항일 뿐 아니라 메일을 가능한 신속하게 전달하는 것은 바람직한 정책입니다. 종단간의 느린 메일 전달은 여러 가지 원인으로 인해 발생할 수 있습니다. 예를 들어, 서버가 제대로 작동하지 않거나, 일정 기간 동안 과도한 메일 로드가 발생했거나, 기존 하드웨어 자원이 용량을 초과했을 수 있습니다.

### 느린 종단간 메일 전달 시간의 증상

메일을 전달하는 데 평소보다 오래 걸립니다.

## 종단간 메일 전달 시간 모니터

- 메일을 보내고 받는 임의의 기능을 사용합니다. 서버 홉 간의 헤더 시간과 출발 시점 및 검색 간의 시간을 비교합니다. 815페이지의 "immonitor-access"를 참조하십시오.

## 디스크 공간 모니터링

부족한 디스크 공간은 메일 서버 문제와 오류의 가장 일반적인 원인 중 하나입니다. MTA 대기열 또는 메시지 저장소에 쓰기 위한 공간이 없을 경우 메일 서버에 오류가 발생합니다. 또한 로그 파일이 모니터링 및 정리되지 않을 경우 모든 디스크 공간이 채워질 때까지 로그 파일의 크기가 증가할 수 있습니다.

새 메일이 메일함에 전달되면 메시지 저장소 분할 영역의 크기가 증가합니다. 예를 들어, 메시지 저장소 할당량이 적용되지 않을 경우 메시지 저장소가 분할 영역에 사용할 수 있는 디스크 공간을 초과할 수 있습니다. 디스크 공간 부족이 발생하는 또 다른 원인으로는 MTA 메일 대기열이 너무 커지는 것을 들 수 있습니다. 또한 로그 파일 모니터링 기능에 문제가 있거나 로그 파일이 관리가 불가능할 정도로 커지는 경우도 원인이 될 수 있습니다. LDAP, MTA 및 Message Access와 같은 다양한 로그 파일이 존재하며 이러한 로그 파일은 각각 다른 디스크에 저장될 수 있다는 것을 유의하십시오.

### 디스크 공간 문제의 증상

공간이 부족해지는 디스크나 분할 영역에 따라 여러 다른 증상이 발생할 수 있습니다. MTA 대기열이 오버플로되고 SMTP 연결을 거부하거나, 메일이 `ims_master` 대기열에 남아 있으면서 메시지 저장소로 전달되지 않거나, 로그 파일이 오버플로될 수 있습니다.

메시지 저장소 분할 영역이 모두 채워지면 메일 액세스 데몬이 실패할 수 있으며 메시지 저장소 데이터가 손상될 수 있습니다. `imexpire` 및 `reconstruct`와 같은 메시지 저장소 유지 보수 유틸리티는 손상을 복구하고 디스크 사용량을 줄일 수 있습니다. 그러나 이러한 유틸리티를 사용하려면 추가 디스크 공간이 필요하며 전체 디스크를 차지하는 분할 영역을 복구하려면 잠재적으로 중단 시간이 발생할 수 있습니다.

### 디스크 공간 모니터

시스템 구성에 따라 다양한 디스크와 분할 영역을 모니터링해야 할 수 있습니다. 예를 들어, MTA 대기열, 메시지 저장소 및 로그 파일이 각기 다른 디스크/분할 영역에 상주할 수 있습니다. 이 경우 각 공간에 대한 모니터링이 필요하며 각 공간을 모니터링하는 방법이 다를 수 있습니다.

Messaging Server는 메시지 저장소 디스크 사용량을 모니터링하고 분할 영역이 사용 가능한 모든 디스크 공간을 차지하는 것을 방지하기 위한 특정 방법을 제공합니다.

다음 단계를 수행하여 메시지 저장소의 디스크 공간 사용을 모니터링할 수 있습니다.

- 메시지 저장소 디스크 사용량을 모니터링하기 위한 매개 변수를 설정합니다.
- 디스크 사용량 임계값에 도달하면 메시지 저장소 분할 영역을 잠급니다.

자세한 내용은 뒤이어 나오는 "메시지 저장소 모니터링" 및 "메시지 저장소 분할 영역 모니터링" 절을 참조하십시오.

### 메시지 저장소 모니터링

메시지 저장소의 디스크 사용은 용량의 75%를 초과하지 않도록 하는 것이 좋습니다. `configutil` 유틸리티로 다음 경보 속성을 구성하여 메시지 저장소 디스크 사용을 모니터링할 수 있습니다.

- `alarm.diskavail.msgalarmstatinterval`
- `alarm.diskavail.msgalarmthreshold`
- `alarm.diskavail.msgalarmwarninginterval`
- `alarm.diskavail.msgalarmdescription`

이러한 매개 변수를 설정함으로써 시스템이 디스크 공간을 모니터링하는 빈도와 경고를 보내야 하는 상황을 지정할 수 있습니다. 예를 들어, 디스크 공간을 600초 간격으로 모니터링하려는 경우 다음 명령을 지정합니다.

```
configutil -o alarm.diskavail.msgalarmstatinterval -v 600
```

사용 가능한 디스크 공간이 20% 이하로 내려갈 때마다 경고를 받으려면 다음 명령을 지정합니다.

```
configutil -o alarm.diskavail.msgalarmthreshold -v 20
```

이러한 매개 변수에 대한 자세한 내용은 [827페이지의 표 23-6](#)을 참조하십시오.

### 메시지 저장소 분할 영역 모니터링

분할 영역이 사용 가능한 디스크 공간의 지정된 비율보다 많은 공간을 차지할 경우 메시지 저장소 분할 영역에 메일이 전달되지 않게 할 수 있습니다. 두 개의 `configutil` 매개 변수를 설정하여 이 기능을 활성화하고 디스크 사용 임계값을 지정합니다.

이 기능을 사용하면 메시지 저장소 데몬이 분할 영역의 디스크 사용량을 모니터링합니다. 디스크 사용량이 증가하면 저장소 데몬은 분할 영역을 더 자주(100분에 한 번에서 1분에 한 번에까지 범위) 동적으로 검사합니다.

디스크 사용이 지정된 임계값보다 높아지면 저장소 데몬은 다음을 수행합니다.

- 분할 영역을 잠급니다. 받는 메일은 MTA 메일 대기열에서 보관되지만 메시지 저장소 분할 영역의 메일함에 전달되지 않습니다.

- 메일을 기본 로그 파일에 기록합니다.
- 전자 메일 알림을 포스트마스터에게 보냅니다. (configutil 매개 변수 alarm.msgalarmnoticercpt를 설정하여 전자 메일의 수신자를 변경할 수 있습니다.)

디스크 사용량이 임계값 아래로 내려가면 분할 영역의 잠금이 해제되고 메일이 다시 저장 소로 전달됩니다.

configutil 매개 변수는 다음과 같습니다.

- local.store.checkdiskusage는 분할 영역 모니터링 기능을 활성화합니다.  
허용되는 값: yes, no  
기본값: yes
- local.store.diskusagethreshold는 디스크 사용량 임계값을 지정합니다.  
local.store.diskusagethreshold의 값은 1 - 99%입니다.  
기본값: 99

분할 영역을 다시 나누거나 로컬 메시지 저장소에 더 많은 디스크 공간을 할당할 수 있는 기회를 얻을 수 있도록 디스크 사용량 임계값의 비율을 충분히 낮게 설정해야 합니다.

예를 들어, 분할 영역이 시간당 2%의 비율로 디스크 공간을 채우며 로컬 메시지 저장소의 추가 디스크 공간을 할당하는 데 1시간이 걸린다고 가정합니다. 이 경우에는 디스크 사용량 임계값을 98%보다 낮은 값으로 설정해야 합니다.

### MTA 대기열 및 로깅 공간 모니터링

MTA 대기열 디스크 및 로깅 공간 디스크 사용을 모니터링해야 합니다.

로깅 공간 관리에 대한 자세한 내용은 21장, "로깅 관리"를 참조하십시오. 예를 들어, mail.log 파일을 모니터링하는 방법을 보려면 728페이지의 "MTA 메일 및 연결 로그 관리"를 참조하십시오.

## CPU 사용 모니터링

CPU 사용량이 많다는 것은 해당 사용 수준에 맞는 CPU 용량이 부족하거나 일부 프로세스가 적절한 한도 이상의 CPU 주기를 사용 중임을 의미합니다.

### CPU 사용 문제의 증상

시스템 응답 시간이 저하되고 사용자가 로그인하는 데 시간이 오래 걸리며 전달 속도가 느려집니다.

## CPU 사용 모니터

CPU 사용을 모니터하는 작업은 플랫폼별로 차이가 있습니다. 관련된 플랫폼 설명서를 참조하십시오.

# MTA 모니터링

이 절은 다음과 같은 하위 절로 구성되어 있습니다.

- [807페이지의 "메일 대기열 크기 모니터링"](#)
- [808페이지의 "전달 실패 비율 모니터링"](#)
- [808페이지의 "인바운드 SMTP 연결 모니터링"](#)
- [809페이지의 "디스패처 및 Job Controller 프로세스 모니터링"](#)

## 메일 대기열 크기 모니터링

메일 대기열이 과도하게 커지는 것은 메일이 전달되지 않거나, 메일의 전달이 지연되거나, 시스템이 전달할 수 있는 것보다 빠른 속도로 메일이 도착하기 때문일 수 있습니다. 이 문제는 시스템에 쇄도하는 막대한 수의 메일로 인한 서비스 거부 공격이나 Job Controller가 실행되지 않는 등의 여러 이유로 발생할 수 있습니다.

메일 대기열에 대한 자세한 내용은 [192페이지의 "채널 메일 대기열"](#), [785페이지의 "메일 이 대기열에서 제외되지 않음"](#) 및 [787페이지의 "MTA 메일이 전달되지 않음"](#)을 참조하십시오.

### 메일 대기열 문제의 증상

- 디스크 공간 사용량이 증가합니다.
- 사용자가 메일을 제때에 받지 못합니다.
- 메일 대기열 크기가 비정상적으로 커집니다.

### 메일 대기열의 크기 모니터

메일 대기열을 모니터하는 최선의 방법은 `imsimta qm`을 사용하는 것입니다. [822페이지의 "imsimta qm counters"](#)를 참조하십시오.

또한 대기열 디렉토리(*msg\_svr\_base/data/queue/*)의 파일 수를 모니터할 수도 있습니다. 파일 수는 사이트마다 차이가 있으므로 "너무 많다"고 판단하는 데 기준이 되는 내역을 작성해야 합니다. 2주 이상 동안에 대기열 파일의 크기를 기록하여 대략적인 평균을 구하는 방법으로 이러한 기준 내역을 작성할 수 있습니다.

## 전달 실패 비율 모니터링

전달 실패는 메일을 외부 사이트로 전달하려는 시도가 실패한 것입니다. 전달 실패 비율이 높다는 것은 DNS 서버를 사용할 수 없거나 원격 서버에서 연결 응답 시간이 초과하는 등의 네트워크 문제가 존재한다는 것을 나타낼 수 있습니다.

### 전달 실패 비율의 증상

외부적인 증상은 없습니다. 다수의 Q 레코드가 *mail.log\_current*에 나타납니다.

### 전달 실패의 비율 모니터

전달 실패는 로깅 항목 코드 Q로 MTA 로그에 기록됩니다.

*msg\_svr\_base/data/log/mail.log\_current* 파일에서 레코드를 확인합니다. 예를 들면 다음과 같습니다.

```
mail.log:06-Oct-2003 00:24:03.66 501d.0b.9 ims-ms    Q 5 durai.balusamy@Sun.COM
rfc822;durai.balusamy@Sun.COM durai@ims-ms-daemon
<00ce01c38bda5c7e2b24056501a8c0@guindy> Mailbox is busy
```

## 인바운드 SMTP 연결 모니터링

특정 IP 주소에서 인바운드 SMTP 연결 수가 비정상적으로 증가한다는 것은 다음을 의미할 수 있습니다.

- 외부 사용자가 메일 전달을 시도하고 있습니다.
- 외부 사용자가 서비스 거부 공격을 시도하고 있습니다.

### 인증되지 않은 SMTP 연결의 증상

- 메일을 전달하는 외부 사용자: 외부적인 증상은 없습니다.
- 서비스 거부 공격: 메일 요청으로 SMTP 서버를 오버로드하려는 외부 시도가 있습니다.



## 인바운드 SMTP 연결 모니터

- **메일 전달 외부 사용자:** `msg_svr_base/log/mail.log_current`에서 로깅 항목 코드 J (거부된 전달)가 있는 레코드를 확인합니다. 원격 IP 주소의 로깅을 설정하려면 다음 행을 `option.dat` 파일에 추가합니다.

```
log_connection=1
```

이 기능을 사용 가능하게 하면 약간의 성능 저하가 발생한다는 점을 유의하십시오.

- **서비스 거부 공격:** `netstat` 명령을 실행하고 SMTP 포트(기본값: 25)에서 연결을 검사하여 어떤 사용자가 얼마나 많이 SMTP 서버에 연결되어 있는지 확인할 수 있습니다. 예를 들면 다음과 같습니다.

| Local address   | Remote address                      | State       |
|-----------------|-------------------------------------|-------------|
| 192.18.79.44.25 | 192.18.78.44.56035 32768 0 32768 0  | CLOSE_WAIT  |
| 192.18.79.44.25 | 192.18.136.54.57390 8760 0 24820 0  | ESTABLISHED |
| 192.18.79.44.25 | 192.18.26.165.48508 33580 0 24820 0 | TIME_WAIT   |

시스템에서 특정 읽기 작업이 비정상적인지 확인할 수 있으려면 우선 적절한 수의 SMTP 연결과 상태(ESTABLISHED, CLOSE\_WAIT 등)를 확인해야 한다는 것을 유의하십시오.

다수의 연결이 SYN\_RECEIVED 상태로 있을 경우 네트워크 연결이 끊어졌거나 서비스 거부 공격이 발생한 것일 수 있습니다. 또한 SMTP 서버 프로세스의 수명이 제한됩니다. 이것은 `dispatcher.cnf` 파일에서 MTA 구성 변수 `MAX_LIFE_TIME`을 통해 제어합니다. 기본값은 86,400초(1일)입니다. 마찬가지로 `MAX_LIFE_CONNS`는 서버 프로세스가 수명 한도 내에서 처리할 수 있는 최대 연결 수를 지정합니다. 특정 SMTP 서버가 오래 지속될 경우 이를 조사하는 것이 필요할 수 있습니다.

## 디스패처 및 Job Controller 프로세스 모니터링

MTA가 작동하려면 디스패처 및 Job Controller 프로세스가 실행 중이어야 합니다. 각 종류의 프로세스는 하나만 존재해야 합니다.

### 디스패처 및 Job Controller 프로세스가 다운된 경우의 증상

디스패처가 다운되었거나 자원이 부족할 경우 SMTP 연결이 거부됩니다.

Job Controller가 다운된 경우 대기열 크기가 증가합니다.

### 디스패처 및 Job Controller 프로세스 모니터

dispatcher 및 job\_controller라는 프로세스가 존재하는지 확인합니다. [772페이지의 "Job Controller 및 디스패처 실행 확인"](#)을 참조하십시오.

## LDAP Directory Server 모니터링

이 절은 다음과 같은 하위 절로 구성되어 있습니다.

- [810페이지의 "slapd 모니터링"](#)

### slapd 모니터링

LDAP Directory Server(slapd)는 메시징 시스템에 대한 디렉토리 정보를 제공합니다. slapd가 다운될 경우 시스템이 제대로 작동하지 않습니다. slapd 응답 시간이 너무 느릴 경우 로그인 속도나 LDAP 조회가 필요한 다른 트랜잭션에 영향을 줍니다.

#### slapd 문제의 증상

- 클라이언트 POP, IMAP 또는 웹 메일 인증이 실패하거나 예상보다 느려집니다.
- MTA가 제대로 작동하지 않습니다.

#### slapd 모니터

- ns-slapd 프로세스가 실행 중인지 확인합니다.
- slapd-*instance*/logs/에서 slapd 로그 파일 access 및 errors를 확인합니다.
- 사용자를 검색하는 동안 ns-slapd 응답 시간을 확인합니다.
- 콘솔을 확인하여 slapd를 모니터링합니다.
- [815페이지의 "immonitor-access"](#)를 참조하십시오.

## 메일 액세스 모니터링

이 절은 다음과 같은 하위 절로 구성되어 있습니다.

- 811페이지의 "imapd, popd 및 httpd 모니터링"
- 812페이지의 "stored 모니터링"

## imapd, popd 및 httpd 모니터링

이러한 프로세스는 IMAP, POP 및 웹 메일 서비스에 대한 액세스를 제공합니다. 이러한 프로세스가 실행 중이 아니거나 응답하지 않을 경우 서비스는 제대로 작동하지 않습니다. 서비스가 실행 중이지만 오버로드된 경우 모니터링을 수행하여 문제를 감지하고 더 적절하게 서비스를 구성할 수 있습니다.

### imapd, popd 및 httpd 문제의 증상

연결이 거부되며 시스템의 연결 속도가 너무 느려집니다. 예를 들어, IMAP가 실행 중이 아닐 때 IMAP에 직접 연결하려고 시도하면 다음과 같은 메시지가 나타납니다.

```
telnet 0 143
Trying 0.0.0.0...
telnet: Unable to connect to remote host: Connection refused
```

클라이언트와의 연결을 시도할 경우에는 다음과 같은 메시지가 표시됩니다.

```
Client is unable to connect to the server at the location you have specified. The
server may be down or busy.
```

### imapd, popd 및 httpd 모니터

- watcher 및 msprobe를 사용하여 모니터할 수 있습니다. 110페이지의 "실패했거나 응답이 없는 서비스의 자동 재시작" 및 824페이지의 "msprobe 및 watcher 기능을 사용하여 모니터링"을 참조하십시오.
- SNMP를 사용하여 모니터할 수 있습니다.

SNMP가 설정된 경우 SNMP는 이러한 프로세스를 모니터하는 매우 적절한 방법이 됩니다. 부록 A, "SNMP 지원"을 참조하십시오. 서버 정보는 네트워크 서비스 모니터링 MIB에 있습니다.

- 로그 파일을 검사합니다.

`msg_svr_base/log/service` 디렉토리를 확인합니다. 여기에서 `service`는 `http`, `IMAP` 또는 `POP`가 될 수 있습니다. 이 디렉토리에는 여러 로그 파일이 존재합니다. 파일 이름 중 하나는 `service`의 이름(`imap`, `pop`, `http`)이며 나머지는 서비스 이름 외에 일련 번호와 날짜가 서비스 이름에 연결되어 있습니다. 예를 들면 다음과 같습니다.

```
imap imap.29.1010221593 imap.31.1010394412 imap.33.1010567224
```

서비스 이름만 가진 파일이 가장 최신 로그입니다. 나머지 파일은 일련 번호(여기에서는 29, 31, 33)로 순서가 정해지며 일련 번호가 가장 높은 파일이 그 다음의 최신 로그입니다. [21장, "로그 관리"](#)를 참조하십시오.

서버가 종료된 경우 다음과 같은 메시지가 나타날 수 있습니다.

```
imap.12.1065431243:[07/Oct/2003:01:15:43 -0700] gotmail-2
imapd[20525]: General Warning: Sun Java System Messaging Server
IMAP4 6.1 (built Sep 24 2003) shutting down
```

- `counterutil`을 사용하여 검사할 수 있습니다. [816페이지의 "counterutil"](#) 및 *Sun Java System Messaging Server Administration Reference*를 참조하십시오.
- 플랫폼 특정 명령을 실행하여 `imapd`, `popd` 및 `httpd` 프로세스가 실행 중인지 확인합니다. 예를 들어, Solaris에서는 `ps` 명령을 사용하여 `imapd`, `popd` 및 `mshttpd`를 찾을 수 있습니다.
- [826페이지의 "정보 메시지"](#)에 설명된 서버 응답 구성 매개 변수를 설정하여 지정된 서버 성능 임계값에 대한 정보를 설정할 수 있습니다.
- [815페이지의 "immonitor-access"](#)를 참조하십시오.

## stored 모니터링

`stored`는 메일 데이터베이스의 교착 상태 및 트랜잭션 작업을 수행하고 에이징 정책을 적용하며 디스크에 저장된 메일을 정리 및 지우는 등의 중요한 여러 작업을 수행합니다.

`stored`의 실행이 중지되면 `Messaging Server`에서 결과적으로 문제가 발생합니다.

`start-msg`가 실행될 때 `stored`가 시작되지 않을 경우 다른 프로세스는 시작되지 않습니다.

`.stored`에 대한 자세한 내용은 *Sun Java System Messaging Server Administration Reference*를 참조하십시오.

### stored 문제의 증상

외부적인 증상은 없습니다.

## stored 모니터

- stored 프로세스가 실행 중인지 확인합니다. stored는 `msg_svr_base/config`에서 `pidfile.store`라는 pid 파일을 작성 및 업데이트합니다. pid 파일은 복구 시에 `init` 상태를 표시하고 준비가 되었을 때 `ready` 상태를 표시합니다. 예를 들면 다음과 같습니다.

```
231: cat pidfile.store
28250
ready
```

첫 번째 행의 숫자는 stored의 프로세스 아이디입니다.

```
232: ps -eaf | grep stored
inetuser 28250      1 0   Jan 05 ?          8:44 /opt/SUNWmsgsr/lib/stored -d
```

- `msg_svr_base/store/mboxlist`에서 작성된 로그 파일을 확인합니다. 모든 로그 파일이 직접적인 stored 문제로 인해 작성된 것은 아니라는 점을 유의하십시오. `imapd`가 중지되거나 데이터베이스 문제가 있을 경우에도 로그 파일이 작성될 수 있습니다.
- `msg_svr_base/config`의 다음 파일에서 타임스탬프를 확인합니다.
  - `stored.ckp` - 검사점 지정 시도가 있을 때마다 수정됩니다. 1분마다 시간이 기록되도록 해야 합니다.
  - `stored.lcu - db` 로그가 정리될 때마다 수정됩니다. 5분마다 시간이 기록되도록 해야 합니다.
  - `stored.per` - 사용자 단위 db 쓰기가 생성될 때마다 수정됩니다. 60분마다 시간이 기록되도록 해야 합니다.
- 기본 로그 파일 `msg_svr_base/log/default/default`에서 stored 메일을 확인합니다.
- `watcher` 및 `msprobe`를 사용하여 모니터할 수 있습니다. 110페이지의 "실패했거나 응답이 없는 서비스의 자동 재시작" 및 824페이지의 "msprobe 및 watcher 기능을 사용하여 모니터링"을 참조하십시오.

## 메시지 저장소 모니터링

메일은 데이터베이스에 저장됩니다. 디스크상의 사용자 배포, 메일함 크기 및 디스크 요구 사항은 저장소 성능에 영향을 미칩니다. 이러한 내용은 다음 절에서 설명합니다.

- 804페이지의 "디스크 공간 모니터"
- 814페이지의 "메시지 저장소 데이터베이스 잠금의 상태 모니터링"
- 814페이지의 "mboxlist 디렉토리의 데이터베이스 로그 파일 수 모니터링"

- 603페이지의 "할당량 제한 모니터"

## 메시지 저장소 데이터베이스 잠금의 상태 모니터링

데이터베이스 잠금의 상태는 다른 서버 프로세스에 의해 유지됩니다. 이러한 데이터베이스 잠금은 메시지 저장소의 성능에 영향을 줄 수 있습니다. 교착 상태의 경우 메일이 적절한 속도로 저장소에 삽입되지 않으며 `ims-ms` 채널 대기열의 크기가 결과적으로 더 증가합니다. 이는 대기열을 백업해야 할 정당한 이유가 되며, 따라서 문제를 진단하기 위해서는 대기열 길이의 내역을 갖고 있는 것이 유용합니다.

### 메시지 저장소 데이터베이스 잠금 문제의 증상

트랜잭션 수가 누적되며 해결되지 않습니다.

### 메시지 저장소 데이터베이스 잠금 모니터

`counterutil -o db_lock` 명령을 사용합니다.

## mboxlist 디렉토리의 데이터베이스 로그 파일 수 모니터링

데이터베이스 로그 파일이란 `sleepycat` 트랜잭션 검사점 지정 로그 파일 (`msg_svr_base/store/mboxlist`)을 말합니다. 로그 파일이 작성되는 것은 데이터베이스 검사점 지정이 발생하지 않았기 때문입니다. 또한 로그 파일은 `stored` 문제로 인해 작성될 수 있습니다.

### 데이터베이스 로그 파일 문제의 증상

2 또는 3개의 로그 파일이 존재해야 합니다. 로그 파일이 더 많을 경우 잠재적으로 심각한 문제가 존재하는 것입니다. 메시지 저장소는 메일과 할당량을 위해 몇 개의 데이터베이스를 사용하며 이와 관련된 문제는 전체 메일 서버에 대한 문제를 일으킬 수 있습니다.

### 데이터베이스 로그 파일 모니터

`msg_svr_base/store/mboxlist` 디렉토리에서 파일이 2 또는 3개만 존재하는지 확인합니다.

## 모니터링을 위한 유틸리티와 도구

다음 도구를 모니터링에 사용할 수 있습니다.

- [815페이지의 "stored"](#)
- [816페이지의 "counterutil"](#)
- [819페이지의 "로그 파일"](#)
- [819페이지의 "imsimta counters"](#)
- [822페이지의 "imsimta qm counters"](#)
- [823페이지의 "SNMP를 사용한 MTA 모니터링"](#)
- [823페이지의 "메일함 할당량 검사를 위한 imquotacheck"](#)
- [824페이지의 "msprobe 및 watcher 기능을 사용하여 모니터링"](#)

### immonitor-access

immonitor-access는 메일 전달(SMTP 서버), 메일 액세스 및 저장(POP 및 IMAP 서버), 디렉토리 서비스(LDAP 서버) 및 HTTP 서버와 같은 Messaging Server 구성 요소/프로세스의 상태를 모니터링합니다. 이 유틸리티는 다양한 서비스의 응답 시간과 메일을 전송 및 검색하는 데 걸린 총 왕복 시간을 측정합니다. 디렉토리 서비스는 디렉토리에서 지정된 사용자를 조회하고 응답 시간을 측정하는 방법으로 모니터링합니다. 메일 전달은 메일(SMTP)을 보내는 방법으로 모니터링하며 메일 액세스 및 저장은 메일을 검색하는 방법으로 모니터링합니다. HTTP 서버에 대한 모니터링은 HTTP 서버가 작동하여 실행 중인지 확인하는 것으로 제한됩니다.

자세한 지침은 *Sun Java System Messaging Server Administration Reference*를 참조하십시오.

### stored

stored 유틸리티는 서버에서 유지 관리 작업을 수행하지만 모니터링을 수행할 수도 있습니다. 그러나 모니터링 작업은 msprobe로 더욱 잘 처리됩니다. [824페이지의 "msprobe 및 watcher 기능을 사용하여 모니터링"](#)을 참조하십시오.

## counterutil

이 유틸리티는 다른 시스템 카운터에서 얻은 통계를 제공합니다. 사용 가능한 카운터 객체의 최신 목록은 다음과 같습니다.

```
# /opt/SUNWmsgsr/sbin/counterutil -l
Listing registry (/opt/SUNWmsgsr/data/counter/counter)
numobjects = 11
refcount = 1
created = 25/Sep/2003:02:04:55 -0700
modified = 02/Oct/2003:22:48:55 -0700
    entry = alarm
    entry = diskusage
    entry = serverresponse
    entry = db_lock
    entry = db_log
    entry = db_mpool
    entry = db_txn
    entry = imapstat
    entry = httpstat
    entry = popstat
    entry = cgimsg
```

각 항목은 카운터 객체를 나타내며 해당 객체에 대해 유용한 여러 카운트를 제공합니다. 이 절에서는 alarm, diskusage, serverresponse, db\_lock, popstat, imapstat 및 httpstat 카운터 객체에 대해서만 설명합니다. counterutil 명령 사용에 대한 자세한 내용은 *Sun Java System Messaging Server Administration Reference*를 참조하십시오.

### counterutil 출력

counterutil은 다양한 플래그를 가집니다. 이 유틸리티의 명령 형식은 다음과 같습니다.

```
counterutil -o CounterObject -i 5 -n 10
```

여기에서

-o CounterObject는 카운터 객체 alarm, diskusage, serverresponse, db\_lock, popstat, imapstat 및 httpstat를 나타냅니다.

-i 5는 5초 간격을 지정합니다.

-n 10은 반복 횟수(기본값: 무한대)를 나타냅니다.

counterutil의 사용 예는 다음과 같습니다.



```
# counterutil -o imapstat -i 5 -n 10
Monitor counterobject (imapstat)
registry /gotmail/iplanet/server5/msg-gotmail/counter/counter opened
counterobject imapstat opened

count = 1 at 972082466 rh = 0xc0990 oh = 0xc0968

global.currentStartTime [4 bytes]: 17/Oct/2000:12:44:23 -0700
global.lastConnectionTime [4 bytes]: 20/Oct/2000:15:53:37 -0700
global.maxConnections [4 bytes]: 69
global.numConnections [4 bytes]: 12480
global.numCurrentConnections [4 bytes]: 48
global.numFailedConnections [4 bytes]: 0
global.numFailedLogins [4 bytes]: 15
global.numGoodLogins [4 bytes]: 10446
...
```

### counterutil을 사용한 경보 통계

이러한 경보 통계는 stored에 의해 보내진 경보를 나타냅니다. 경보 카운터는 다음 통계를 제공합니다.

**표 23-1** counterutil alarm 통계

| 접미어                      | 설명                         |
|--------------------------|----------------------------|
| alarm.countoverthreshold | 임계값을 초과한 횟수입니다.            |
| alarm.countwarningsent   | 보내진 경고 수입니다.               |
| alarm.current            | 현재 모니터링되는 값입니다.            |
| alarm.high               | 기록된 값 중에서 가장 높은 값입니다.      |
| alarm.low                | 기록된 값 중에서 가장 낮은 값입니다.      |
| alarm.timelastset        | 현재 값이 마지막으로 설정된 시간입니다.     |
| alarm.timelastwarning    | 경고가 마지막으로 보내진 시간입니다.       |
| alarm.timereset          | 재설정이 마지막으로 수행된 시간입니다.      |
| alarm.timestatechanged   | 경보 상태가 마지막으로 변경된 시간입니다.    |
| alarm.warningstate       | 경보 상태(yes(1) 또는 no(0))입니다. |

## counterutil을 사용한 IMAP, POP 및 HTTP 연결 통계

현재 IMAP, POP 및 HTTP 연결 수, 실패한 로그인 수, 시작 시점부터의 총 연결 수 등에 대한 정보를 얻으려면 `counterutil -o CounterObject -i 5 -n 10` 명령을 사용합니다. 여기에서 *CounterObject*는 카운터 객체 `popstat`, `imapstat` 또는 `httpstat`를 나타냅니다. `imapstat` 접미어의 의미는 표 23-2에 나와 있습니다. `popstat` 및 `httpstat` 객체는 같은 형식과 구조로 동일한 정보를 제공합니다.

**표 23-2** counterutil imapstat 통계

| 접미어                                | 설명                                  |
|------------------------------------|-------------------------------------|
| <code>currentStartTime</code>      | 현재 IMAP 서버 프로세스의 시작 시간입니다.          |
| <code>lastConnectionTime</code>    | 새 클라이언트가 마지막으로 수락된 시간입니다.           |
| <code>maxConnections</code>        | IMAP 서버에 의해 처리되는 최대 동시 연결 수입니다.     |
| <code>numConnections</code>        | 현재 IMAP 서버에 의해 서비스되는 총 연결 수입니다.     |
| <code>numCurrentConnections</code> | 현재 활성 연결의 수입니다.                     |
| <code>numFailedConnections</code>  | 현재 IMAP 서버에 의해 서비스되는 실패한 연결 수입니다.   |
| <code>numFailedLogins</code>       | 현재 IMAP 서버에 의해 서비스되는 실패한 로그인 수입니다.  |
| <code>numGoodLogins</code>         | 현재 IMAP 서버에 의해 서비스되는 성공적인 로그인 수입니다. |

## counterutil을 사용한 디스크 사용 통계

`counterutil -o diskusage` 명령은 다음 정보를 생성합니다.

**표 23-3** counterutil diskstat 통계

| 접미어                                      | 설명                            |
|------------------------------------------|-------------------------------|
| <code>diskusage.availSpace</code>        | 디스크 분할 영역에서 사용할 수 있는 총 공간입니다. |
| <code>diskusage.lastStatTime</code>      | 마지막으로 통계를 가져온 시간입니다.          |
| <code>diskusage.mailPartitionPath</code> | 메일 분할 영역 경로입니다.               |
| <code>diskusage.percentAvail</code>      | 사용할 수 있는 디스크 분할 영역 공간의 비율입니다. |
| <code>diskusage.totalSpace</code>        | 디스크 분할 영역의 총 공간입니다.           |

## 서버 응답 통계

counterutil -o serverresponse 명령은 다음 정보를 생성합니다. 이 정보는 서버가 실행 중인지 확인하고 서버가 얼마나 빨리 응답하는지 확인하는 데 유용합니다.

**표 23-4** counterutil serverresponse 통계

| 접미어                           | 설명                                       |
|-------------------------------|------------------------------------------|
| http.laststattime             | http 서버 응답이 마지막으로 확인된 시간입니다.             |
| http.responsetime             | http에 대한 응답 시간입니다.                       |
| imap.laststattime             | imap 서버 응답이 마지막으로 확인된 시간입니다.             |
| imap.responsetime             | imap에 대한 응답 시간입니다.                       |
| pop.laststattime              | pop 서버 응답이 마지막으로 확인된 시간입니다.              |
| pop.responsetime              | pop에 대한 응답 시간입니다.                        |
| ldap_host1_389.laststattime   | ldap_host1_389 서버 응답이 마지막으로 확인된 시간입니다.   |
| ldap_host1_389.responsetime   | ldap_host1_389에 대한 응답 시간입니다.             |
| ugldap_host2_389.laststattime | ugldap_host2_389 서버 응답이 마지막으로 확인된 시간입니다. |
| ugldap_host2_389.responsetime | ugldap_host2_389에 대한 응답 시간입니다.           |

## 로그 파일

Messaging Server는 SMTP, IMAP, POP 및 HTTP에 대한 이벤트 레코드를 기록합니다. Messaging Server 로그 파일을 작성 및 관리하기 위한 정책은 사용자 정의할 수 있습니다.

로깅이 서버 성능에 영향을 주므로 서버에 부담을 주기 전에 로깅을 매우 신중하게 고려해야 합니다. 자세한 내용은 [21장](#), "[로깅 관리](#)"를 참조하십시오.

## imsimta counters

MTA는 메일 모니터링 MIB, RFC 1566에 기초하여 각 활성 채널에 대한 메일 트래픽 카운터를 증가시킵니다. 채널 카운터는 전자 메일 시스템의 추세와 상태를 나타내는 데 도움을 줍니다. 채널 카운터는 메일 트래픽의 정확한 계산을 제공하도록 설계되지는 않았습다. 정확한 계산을 보려면 [21장](#), "[로깅 관리](#)"에 설명된 대로 MTA 로깅을 확인합니다.

MTA 채널 카운터는 사용 가능한 최소 경량 기법을 사용하여 구현되므로 가능한 한 실제 작업에 미치는 영향이 최소화됩니다. 채널 카운터는 그 이상을 시도하지 않습니다. 즉, 섹션을 매핑하려는 시도가 실패할 경우 정보가 기록되지 않고 섹션의 잠금 중 하나를 거의 즉각적으로 얻을 수 없을 경우 정보가 기록되지 않으며 시스템이 종료할 경우 메모리 내장 섹션에 포함된 정보가 영원히 손실됩니다.

imsimta counters -show 명령은 MTA 채널 메일 통계(아래 참조)를 제공합니다. 시간이 지나면 최소값에 주의하면서 이러한 카운터를 검사해야 합니다. 일부 채널의 경우 최소값은 실제로 음수일 수 있습니다. 음수 값은 카운터가 0이 되었을 때(클러스터 전반의 카운터 데이터베이스 작성 시) 채널에 대해 대기 중인 메일이 존재했다는 것을 의미합니다. 이러한 메일이 대기열에서 빠지면 채널의 관련 카운터가 감소하므로 결과적으로 음수 최소값이 생성됩니다. 이러한 카운터의 경우 올바른 "절대값"은 초기화 이후부터 카운터가 지니고 있는 최소값이 아니라 현재 값입니다.

| Channel                | Messages | Recipients         | Blocks                    |            |
|------------------------|----------|--------------------|---------------------------|------------|
| -----                  | -----    | -----              | -----                     |            |
| tcp_local              |          |                    |                           |            |
| Received               | 29379    | 79714              | 982252                    | <b>(1)</b> |
| Stored                 | 61       | 113                | -2004                     | <b>(2)</b> |
| Delivered              | 29369    | 79723              | 983903 (29369 first time) | <b>(3)</b> |
| Submitted              | 13698    | 13699              | 18261                     | <b>(4)</b> |
| Attempted              | 0        | 0                  | 0                         | <b>(5)</b> |
| Rejected               | 1        | 10                 | 0                         | <b>(6)</b> |
| Failed                 | 104      | 104                | 4681                      | <b>(7)</b> |
| Queue time/count       |          | 16425/29440 = 0.56 |                           | <b>(8)</b> |
| Queue first time/count |          | 16425/29440 = 0.56 |                           | <b>(9)</b> |
| Total In Assocs        |          | 297637             |                           |            |
| Total Out Assocs       |          | 28306              |                           |            |

**1)** Received는 tcp\_local이라는 채널의 대기열에 포함된 메일 수입입니다. 즉, 다른 채널에 의해 tcp\_local의 대기열에 포함된 메일(mail.log\* 파일의 E 레코드)입니다.

**2)** Stored는 채널 대기열에 저장된 전달할 메일 수입입니다.

3) `Delivered`는 `tcp_local` 채널에 의해 처리된(대기열에서 제외된) 메일 수입입니다. 즉, `mail.log*` 파일의 `D` 레코드입니다. 대기열에서 제외하는 작업은 성공적인 전달(즉, 다른 채널의 대기열에 포함)에 해당하거나 보낸 사람에게 반송되는 메일로 인한 작업에 해당할 수 있습니다. 일반적으로 이 값은 `Received`에서 `Stored`를 뺀 숫자입니다.

MTA는 또한 처음 시도할 때 대기열에서 제외된 메일 수를 추적하며 이 수는 괄호로 표시됩니다.

4) `Submitted`는 `tcp_local` 채널에 의해 다른 채널의 대기열에 포함된 메일 수(`mail.log` 파일의 `E` 레코드)입니다.

5) `Attempted`는 대기열에서 빠는 도중에 일시적인 문제를 경험한 메일 수(즉, `mail.log*` 파일의 `Q` 또는 `Z` 레코드)입니다.

6) `Rejected`는 시도된 대기열에 포함 작업 중에서 거부된 작업 수(즉, `mail.log*` 파일의 `J` 레코드)입니다.

7) `Failed`는 시도된 대기열에서 빠기 작업 중에서 실패한 작업 수(즉, `mail.log*` 파일의 `R` 레코드)입니다.

8) `Queue time/count`는 전달된 메일이 대기열에 있는 평균 시간입니다. 여기에는 처음 시도에서 전달된 메일(9 참조)과 추가 전달 시도가 필요했던 메일(대기열에 여유 공간이 생길 때까지 오랜 시간을 기다린 메일)이 모두 포함됩니다.

9) `Queue first time/count`는 처음 시도에서 전달된 메일이 대기열에 있는 평균 시간입니다.

제출된 메일 수가 전달된 메일 수보다 많을 수 있다는 것을 유의하십시오. 이것은 채널이 대기열에서 제외하는(전달하는) 각 메일이 대기열에 포함되는(제출되는) 최소한 하나 이상의 새 메일이 되기 때문에 흔히 발생하는 일입니다. 예를 들어, 메일에 다른 채널을 통해 도달하는 두 명의 수신자가 있는 경우 대기열에 포함 작업은 두 개가 필요합니다. 또는 메일이 바운스될 경우 복사본 하나가 보낸 사람에게 되돌아가고 다른 복사본 하나가 포스터 마스터에게 보내질 수 있습니다. 이 경우 일반적으로 제출 작업은 두 개가 될 것입니다(두 복사본이 동일한 채널을 통해 도달하지 않을 경우).

`Submitted` 및 `Delivered` 간의 연결은 채널 유형에 따라 바뀌는 것이 더 일반적입니다. 예를 들어, 변환 채널에서는 메일이 일부 다른 임의 채널에 의해 대기열에 포함되고 나면 변환 채널이 해당 메일을 처리하여 또 다른 채널의 대기열에 포함시킨 다음 자신의 대기열에서 제외되었다는 것을 메일에 표시합니다. 각 개별 메일은 다음 경로를 가집니다.

```
elsewhere -> conversion   E record   Received
conversion -> elsewhere  E record   Submitted
conversion                D record   Delivered
```

그러나 "pass through"가 아니라 두 개의 개별 부분(슬레이브 및 마스터)을 가지는 tcp\_local과 같은 채널의 경우 Submitted 및 Delivered 사이에 연결이 없습니다. Submitted 카운터는 tcp\_local 채널의 SMTP 서버 부분과 관련되며 Delivered 카운터는 tcp\_local 채널의 SMTP 클라이언트 부분과 관련됩니다. 이들은 완전히 별개인 두 개의 프로그램이며 각각을 통과하는 메일이 완전히 다를 수 있습니다.

*SMTP 서버로 제출되는 메일:*

```
tcp_local -> elsewhere E record Submitted
```

*SMTP 클라이언트를 통해 다른 SMTP 호스트로 보내지는 메일:*

```
elsewhere -> tcp_local E record Received
tcp_local D record Delivered
```

채널이 대기열에서 제외하는(전달하는) 메일은 대기열에 포함되는(제출되는) 최소한 하나 이상의 새 메일이 됩니다. 예를 들어, 메일에 다른 채널을 통해 도달하는 두 명의 수신자가 있는 경우 대기열에 포함 작업은 두 개가 필요합니다. 또는 메일이 바운스될 경우 복사본 하나가 보낸 사람에게 되돌아가고 다른 복사본 하나가 포스트마스터에게 보내질 수 있습니다. 이 경우에는 일반적으로 두 복사본이 동일한 채널을 통해 도달할 것입니다.

## UNIX 및 NT에서의 구현

성능상의 이유로 인해 MTA를 실행하는 노드는 공유 메모리 섹션(UNIX) 또는 공유 파일 매핑 객체(NT)를 사용하여 채널 카운터 캐시를 메모리에서 유지합니다. 노드의 프로세스가 대기열에서 메일을 포함시키거나 제외시킬 때 이 메모리 내장 캐시의 카운터가 업데이트됩니다. 채널이 실행될 때 내장 메모리 섹션이 존재하지 않을 경우 이 섹션은 자동으로 만들어집니다. (또한 내장 메모리 섹션이 존재하지 않을 경우 imta start 명령은 이 섹션을 만듭니다.)

imta counters -clear 또는 imta qm counters clear 명령을 사용하면 카운터를 0으로 재설정할 수 있습니다.

## imsimta qm counters

imsimta qm counters 유틸리티는 MTA 채널 대기열 메일 카운터를 표시합니다. 이 유틸리티를 실행하려면 루트 또는 inetuser여야 합니다. 출력 필드는 819페이지의 "imsimta counters"에 설명된 것과 동일합니다. 사용 방법에 대한 자세한 내용은 Sun Java System Messaging Server Administration Reference를 참조하십시오.

예를 들면 다음과 같습니다.

```
# imsimta counters -create
# imsimta qm counters show
```

| Channel      | Messages | Recipients | Blocks |
|--------------|----------|------------|--------|
| tcp_intranet |          |            |        |
| Received     | 13077    | 13859      | 264616 |
| Stored       | 92       | 91         | -362   |
| Delivered    | 12985    | 13768      | 264978 |
| Submitted    | 2594     | 2594       | 3641   |
| ...          |          |            |        |

MTA를 다시 시작할 때마다 `# imsimta counters -create`를 실행해야 합니다.

## SNMP를 사용한 MTA 모니터링

Messaging Server는 SNMP(Simple Network Management Protocol)를 통한 시스템 모니터링을 지원합니다. Sun Net Manager 또는 HP OpenView(이 제품에서 제공되지 않음)와 같은 SNMP 클라이언트(경우에 따라 *네트워크 관리자*라고 부름)를 사용하면 Messaging Server의 일정 부분을 모니터링할 수 있습니다. 자세한 내용은 [부록 A, "SNMP 지원"](#)을 참조하십시오.

## 메일함 할당량 검사를 위한 imquotacheck

imquotacheck 유틸리티를 사용하여 메일함 할당량 사용과 제한을 모니터링할 수 있습니다. imquotacheck 유틸리티는 정의된 할당량과 제한을 나열하는 보고서를 생성하며 할당량 사용에 대한 정보를 제공합니다.

예를 들어, 다음 명령은 모든 사용자 할당량 정보를 나열합니다.

```
% imquotacheck
-----
Domain red.siroe.com (diskquota = not set msgquota = not set) quota usage
-----
diskquota      size(K)    %use    msgquota    msgs    %use    user
# of domains = 1
# of users = 705

no quota       50418      no quota  4392        ajonkish
no quota        5         no quota   2          andrewt
no quota      355518     no quota  2500        aniksri
...
```

다음 예에서는 `sorook`이라는 사용자의 할당량 사용을 보여 줍니다.

```
% !quotacheck -u sorook
-----
quota usage for user sorook
-----
diskquota      size(K)      %use      msgquota      msgs      %use      user
no quota       1487                no quota      305                sorook
```

## msprobe 및 watcher 기능을 사용하여 모니터링

Messaging Server는 여러 시스템 서비스를 모니터링하기 위해 `watcher` 및 `msprobe`라는 두 가지 프로세스를 제공합니다. `watcher`는 서버 충돌을 관찰하고 필요에 따라 다시 시작하며 `msprobe`는 서버 중지(응답하지 않음)를 모니터링합니다. 특히 `msprobe`는 다음을 모니터링합니다.

- 서버 응답 시간.** `msprobe`는 프로토콜 명령을 사용하여 활성화된 서버에 연결하고 응답 시간을 측정합니다. 응답 시간이 경고 알림 임계값을 초과하는 경우 경고 메시지가 전송됩니다(826페이지의 "경보 메시지" 참조). `autorestart`가 활성화되어 있고 `msprobe`가 서버에 연결할 수 없거나 서버 응답 시간이 지정한 시간 초과 기간을 넘은 경우에는 서버가 다시 시작됩니다. 서버 응답 시간은 카운터 데이터베이스에 표시되고 기본 로그 파일에 기록됩니다. `counterutil`은 서버 응답 시간 통계를 표시하는 데 사용됩니다(816페이지의 "`counterutil`").

다음 서버는 `msprobe`: `imap`, `pop`, `http`, `cert`, `job_controller`, `smtp`, `lntp`, `mmp` 및 `ens`에서 모니터링합니다. `smtp` 또는 `lntp`이 응답하지 않을 때는 디스패처가 다시 시작됩니다. `ens`는 자동으로 다시 시작되지 않습니다.

- 디스크 사용.** `msprobe`는 모든 메시지 저장소 분할 영역의 디스크 사용을 확인합니다. 특히 메시지 저장소 `mboxlist` 데이터베이스 디렉토리와 MTA 대기열 디렉토리를 검사합니다. 디스크 사용이 구성된 임계값을 초과할 때는 경고 메시지가 전송됩니다. 디스크 크기와 사용은 카운터 데이터베이스에 표시되고 기본 로그 파일에 기록됩니다. 관리자는 `counterutil` 유틸리티(816페이지의 "`counterutil`" 참조)를 사용하여 디스크 사용 통계를 표시할 수 있습니다.



- **메시지 저장소 mboxlist 데이터베이스 로그 파일 누적.** 로그 파일 누적은 mboxlist 데이터베이스 오류를 나타냅니다. msprobe는 활성 로그 파일의 개수를 세고 그 수가 임계값보다 클 경우 msprobe는 default 로그 파일에 중요 오류 메시지를 기록하여 관리자께 서버를 다시 시작하도록 알립니다. autorestart가 활성화되어 있으면 (local.autorestart를 yes로 설정) 저장소 데몬이 다시 시작됩니다.

watcher 및 msprobe는 표 23-5에 있는 configutil 옵션으로 제어됩니다. 자세한 내용은 110페이지의 "실패했거나 응답이 없는 서비스의 자동 재시작"을 참조하십시오.

**표 23-5** msprobe 및 watcher configutil 옵션

| 옵션                                   | 설명                                                                                                                                                                                                                    |
|--------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| local.watcher.enable                 | 서비스 실패를 모니터링하는 watcher를 활성화합니다. IMAP, POP, HTTP, Job Controller, 디스패처, 메시지 저장소(stored), imsched, MMP, LMTP/SMTP 서버는 디스패처가 모니터링하며 LMTP/SMTP 클라이언트는 job_controller가 모니터링합니다. 특정 실패에 대해 오류 메시지를 기본 로그 파일에 기록합니다. 기본값: on |
| local.autorestart                    | 서버 자동 재시작 활성화 실패하거나 중지된 서비스를 자동으로 다시 시작합니다. 기본값: no                                                                                                                                                                   |
| local.autorestart.timeout            | 재시도 시간 초과 오류. 지정된 시간 내에 서버가 세 번 이상 실패하면 시스템은 서버 재시작 시도를 중지합니다. 이 값(초)은 msprobe 간격 (local.schedule.msprobe)보다 길게 설정해야 합니다. 기본값: 600초                                                                                   |
| local.schedule.msprobe               | msprobe에서 일정을 실행합니다. crontab 스타일 일정 문자열(592페이지의 표 18-10 참조)로 기본값은 600초입니다.                                                                                                                                            |
| service.readtimeout                  | 다시 시작하기 전의 기본 서버 응답 시간<br>기본값: (smtp/lmtp에는 120초, 기타 프로토콜에는 30초)                                                                                                                                                      |
| local.probe.service.timeout          | 다시 시작하기 전 특정 서버에 대한 시간 초과. service는 imap, pop, http, cert, job_controller, smtp, lmtp, mmp 또는 ens이 될 수 있습니다.<br>기본값: service.readtimeout 사용                                                                           |
| local.probe.warningthreshold         | 경고 메시지가 기본 로그 파일에 기록되기 전 서버가 응답하지 않는 시간(초)<br>기본값: 5초                                                                                                                                                                 |
| local.probe.service.warningthreshold | 경고 메시지가 default 로그 파일에 기록되기 전 특정 서버가 응답하지 않는 시간(초). service는 imap, pop, http, cert, job_controller, smtp, lmtp, mmp 또는 ens가 될 수 있습니다.<br>기본값: local.probe.warningthreshold 사용                                         |

**표 23-5** msprobe 및 watcher configutil 옵션

| 옵션                     | 설명                                                                                       |
|------------------------|------------------------------------------------------------------------------------------|
| local.queuedir         | 대기열 크기가 alarm.diskavail.msgalarmthreshold에서 정의한 임계값을 초과하는 경우 검사할 MTA 대기열 디렉토리<br>기본값: 없음 |
| local.schedule.msprobe | msprobe에서 일정을 실행합니다. 값은 crontab 스타일의 일정 문자열입니다.<br>기본값: 600초                             |
| service.readtimeout    | 서버를 다시 시작하기 전 해당 서버가 응답하지 않는 시간.<br>local.schedule.msprobe를 참조하십시오.<br>기본값: 10초          |

### 경보 메시지

msprobe는 지정된 조건을 경고하도록 포스트마스터에게 전자 메일 형식으로 경보를 보낼 수 있습니다(812페이지 참조). 다음은 일정한 임계값을 초과할 때 보내지는 샘플 전자 메일 경보입니다.

```

Subject:ALARM: server response time in seconds of "ldap_siroe.com_389" is 10
Date: Tue, 17 Jul 2001 16:37:08 -0700 (PDT)
From: postmaster@siroe.com
To: postmaster@siroe.com

Server instance: /opt/SUNWmsgsr
Alarmid: serverresponse
Instance: ldap_siroe_europa.com_389
Description: server response time in seconds
Current measured value (17/Jul/2001:16:37:08 -0700): 10
Lowest recorded value: 0
Highest recorded value: 10
Monitoring interval: 600 seconds
Alarm condition is when over threshold of 10
Number of times over threshold: 1
    
```

msprobe가 디스크 및 서버 성능을 모니터링하는 빈도와 경보를 보내는 상황을 지정할 수 있습니다. 이렇게 하려면 configutil 명령을 사용하여 경보 매개 변수를 설정합니다.

표 23-6은 기본 설정과 함께 유용한 경보 매개 변수를 보여 줍니다. 전체 목록은 *Sun Java System Messaging Server Administration Reference*를 참조하십시오.

표 23-6 유용한 경고 메시지 configutil 매개 변수

| 매개 변수                                           | 설명(괄호 안의 값이 기본값임)                                                             |
|-------------------------------------------------|-------------------------------------------------------------------------------|
| alarm.msgalarmnoticehost                        | (localhost) 경고 메일을 보낼 시스템입니다.                                                 |
| alarm.msgalarmnoticeport                        | (25) 경고 메일을 보낼 때 연결할 SMTP 포트입니다.                                              |
| alarm.msgalarmnoticercpt                        | (Postmaster@localhost) 경고 알람을 받는 사람입니다.                                       |
| alarm.msgalarmnoticesender                      | (Postmaster@localhost) 경보를 보낸 사람의 주소입니다.                                      |
| alarm.diskavail.msgalarmdescription             | (percentage mail partition disk space available.) 디스크 사용 경보의 설명 필드에 사용되는 문자열. |
| alarm.diskavail.msgalarmstatinterval            | (3600) 디스크 가용성 검사의 간격(초)입니다. 디스크 사용 검사를 사용하지 않으려면 0으로 설정합니다.                  |
| alarm.diskavail.msgalarmthreshold               | (10) 디스크 공간 가용성 비율로서 이 비율 아래로 내려가면 경보가 보내집니다.                                 |
| alarm.diskavail.msgalarmthresholddirection      | (-1) 경보가 디스크 공간 가용성이 임계값보다 작을 때 발생하는지(-1) 아니면 임계값보다 클 때 발생하는지(1) 여부를 지정합니다.   |
| alarm.diskavail.msgalarmwarninginterval         | (24). 디스크 가용성 경보가 반복되는 간격(시간)입니다.                                             |
| alarm.serverresponse.msgalarmdescription        | (server response time in seconds.) 서버 응답 경보의 설명 필드에 사용되는 문자열.                 |
| alarm.serverresponse.msgalarmstatinterval       | (600) 서버 응답 검사의 간격(초)입니다. 서버 응답 검사를 사용하지 않으려면 0으로 설정합니다.                      |
| alarm.serverresponse.msgalarmthreshold          | (10) 서버 응답 시간(초)이 이 값을 초과할 경우 경보가 발생합니다.                                      |
| alarm.serverresponse.msgalarmthresholddirection | (1) 경보가 서버 응답 시간이 임계값보다 클 때 발생하는지(1) 아니면 임계값보다 작을 때 발생하는지(-1) 여부를 지정합니다.      |
| alarm.serverresponse.msgalarmwarninginterval    | (24) 서버 응답 경보가 반복되는 간격(시간)입니다.                                                |



# SNMP 지원

Messaging Server는 SNMP(Simple Network Management Protocol)를 통한 시스템 모니터링을 지원합니다. Sun Net Manager 또는 HP OpenView(이 제품에는 제공되지 않음)와 같은 SNMP 클라이언트(*네트워크 관리자*라고도 함)를 사용하여 Messaging Server의 특정 부분을 모니터링할 수 있습니다. Messaging Server 모니터링에 대한 자세한 내용은 23장, "[Messaging Server 모니터링](#)"을 참조하십시오.

이 장에서는 Messaging Server에서 SNMP 지원을 사용하는 방법에 대해 설명합니다. 또한, SNMP에 의해 제공되는 정보 유형에 대한 개요를 제공합니다. 하지만 SNMP 클라이언트에서 이 정보를 보는 방법에 대해서는 설명하지 않습니다. SNMP 클라이언트를 사용하여 SNMP 기반 정보를 보는 방법에 대한 자세한 내용은 SNMP 클라이언트 설명서를 참조하십시오. 또한, 이 문서에는 Messaging Server SNMP 구현에서 사용 가능한 일부 데이터에 대해 설명되어 있지만 전체 MIB 정보는 RFC 2788 및 RFC 2789에서 이용할 수 있습니다.

이 장은 다음 내용으로 구성되어 있습니다.

- 830페이지의 "[SNMP 구현](#)"
- 831페이지의 "[Solaris 8에서 Messaging Server에 대한 SNMP 지원 구성](#)"
- 832페이지의 "[SNMP 클라이언트로부터 모니터링](#)"
- 833페이지의 "[Unix 플랫폼에서 다른 Sun Java System 제품과 공존](#)"
- 833페이지의 "[Messaging Server의 SNMP 정보](#)"

## SNMP 구현

Messaging Server는 Network Services Monitoring MIB(RFC 2788)과 Mail Monitoring MIB(RFC 2789)의 두 표준화된 MIB을 구현합니다. Network Services Monitoring MIB은 POP, IMAP, HTTP 및 SMTP 서버와 같은 네트워크 서비스 모니터링을 위해 제공됩니다. Mail Monitoring MIB은 MTA 모니터링을 위해 제공됩니다. Mail Monitoring MIB을 사용하면 각 MTA 채널의 활성 상태와 비활성 상태를 모두 모니터링할 수 있습니다. 활성 정보에는 주로 현재 대기열에 포함된 메일과 열린 네트워크 연결(예: 대기열에 있는 메일 개수, 열린 네트워크 연결의 소스 IP 주소)에 대한 정보가 있고, 비활성 정보에는 누적 합계(예: 처리된 총 메일 수, 총 인바운드 연결)가 제공됩니다.

---

**주** 전체 Messaging Server SNMP 모니터링 정보 목록은 RFC 2788 및 RFC 2789를 참조하십시오.

---

SNMP는 Java Enterprise System에서 지원하는 모든 Microsoft Windows 버전뿐만 아니라 Solaris 8 및 9를 실행하는 플랫폼에서 지원됩니다. 다른 플랫폼에 대한 지원은 이후 릴리스에서 제공됩니다. Solaris의 SNMP 지원에서는 원시 Solaris SNMP 기술인 SEA(Solstice Enterprise Agents)를 사용합니다. 고객은 Solaris 8 시스템에 SEA를 설치할 필요가 없습니다. 필수 런타임 라이브러리가 이미 제공되어 있습니다.

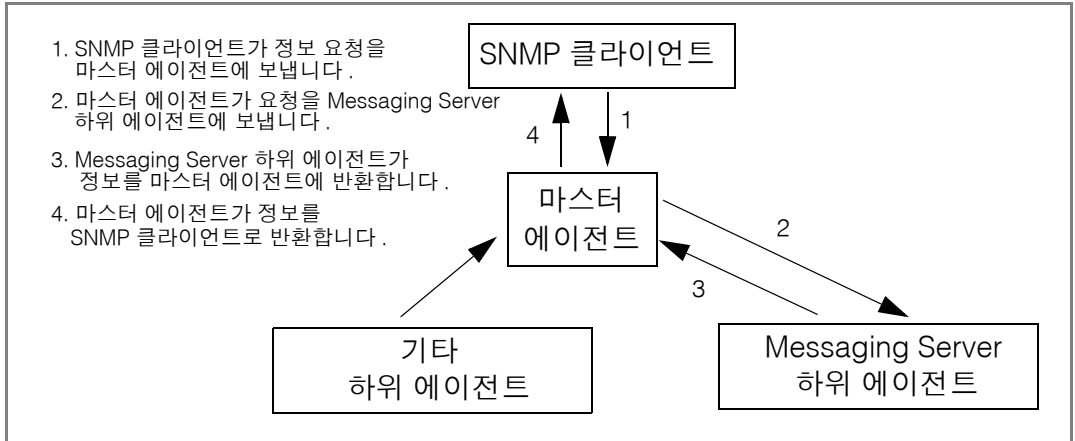
Messaging Server SNMP 지원 제한은 다음과 같습니다.

- 각 호스트 컴퓨터에서는 SNMP를 통해 Messaging Server 인스턴스를 하나씩만 모니터링할 수 있습니다.
- SNMP 지원은 모니터링 전용입니다. SNMP 관리는 지원되지 않습니다.
- SNMP 트랩이 구현되지 않습니다. RFC 2788은 트랩을 사용하지 않는 유사한 기능을 제공합니다.

## Messaging Server에서의 SNMP 작업

Solaris 플랫폼에서 Messaging Server SNMP 프로세스는 시작할 때 플랫폼의 원시 SNMP 마스터 에이전트를 사용하여 자동 등록되는 SNMP 하위 에이전트입니다. 클라이언트의 SNMP 요청은 마스터 에이전트로 전달됩니다. 마스터 에이전트는 Messaging Server가 대상인 모든 요청을 Messaging Server 하위 에이전트 프로세스에 전달합니다. Messaging Server 하위 에이전트 프로세스에서는 해당 요청을 처리하고 마스터 에이전트를 통해 클라이언트에게 응답을 릴레이합니다. 이 프로세스는 [그림 A-1](#)에 표시되어 있습니다.

그림 A-1 SNMP 정보 흐름



## Solaris 8에서 Messaging Server에 대한 SNMP 지원 구성

SNMP 모니터링으로 인한 오버헤드는 매우 작지만 Messaging Server는 SNMP 지원을 비활성화한 상태로 제공됩니다. SNMP 지원을 사용하려면 다음 명령을 실행합니다.

```
# su user-id-for-ims
# configutil -o local.snmp.enable -v 1
# start-msg snmp
```

SNMP를 활성화하면 매개 변수를 지정하지 않더라도 start-msg 명령이 다른 Messaging Server 프로세스와 함께 SNMP 하위 에이전트 프로세스를 자동으로 시작합니다.

Messaging Server SNMP 하위 에이전트를 작동하려면 Solaris 원시 SNMP 마스터 에이전트를 실행해야 합니다. Solaris 원시 SNMP 마스터 에이전트는 일반적으로 Solaris 부트 절차의 일부로 시작되는 snmpdx 데몬입니다.

SNMP 하위 에이전트는 수신할 UDP 포트를 자동으로 선택합니다. 필요한 경우 다음 명령을 사용하여 하위 에이전트에 고정 UDP 포트를 지정할 수 있습니다.

```
# configutil -o local.snmp.port -v port-number
```

나중에 포트 번호로 값 0을 지정하여 이 설정을 취소할 수 있습니다. 기본 설정인 값 0은 Messaging Server에서 하위 에이전트가 사용 가능한 UDP 포트를 자동으로 선택할 수 있도록 합니다.

`/etc/snmp/conf` 디렉토리에 두 SNMP 하위 에이전트 구성 파일이 있습니다. `ims.ac1`에는 SNMP 액세스 제어 정보가 포함되어 있고 `ims.reg`에는 SNMP MIB OID 등록 정보가 포함되어 있습니다.

일반적으로 이러한 파일은 편집할 필요가 없습니다. Messaging Server에서 제공하는 MIB은 읽기 전용이며 `ims.reg` 파일에서 포트 번호를 지정할 필요가 없습니다. 포트 번호를 지정하는 경우 `configutil` 유틸리티를 사용하여 다른 포트를 설정할 때까지는 해당 포트가 적용됩니다. 그럴 경우 하위 에이전트에서는 `configutil`을 사용하여 설정한 포트 번호를 사용합니다. 파일을 편집하는 경우 변경 내용을 적용하려면 SNMP 하위 에이전트를 중지하고 다시 시작해야 합니다.

```
# stop-msg snmp
# start-msg snmp
```

## SNMP 클라이언트로부터 모니터링

RFC 2788 및 RFC 2789의 기본 OID는 다음과 같습니다.

`mib-2.27 = 1.3.6.1.2.1.27`

`mib-2.28 = 1.3.6.1.2.1.28`

이러한 두 OID에서 SNMP 클라이언트를 가리키고 "공용" SNMP 커뮤니티로 액세스합니다.

MIB 복사본을 SNMP 클라이언트에 로드하려는 경우 MIB의 ASCII 복사본은 `msg_svr_base/lib/config-templates` 디렉토리에 `rfc2788.mib` 및 `rfc2789.mib` 파일 이름으로 존재합니다. 이러한 MIB을 SNMP 클라이언트 소프트웨어에 로드하는 것과 관련된 지침은 SNMP 클라이언트 소프트웨어 설명서를 참조하십시오. 일부 이전 SNMP 클라이언트에서는 이러한 MIB에 사용되는 `SnmpAdminString` 데이터 유형을 인식하지 못할 수 있습니다. 그럴 경우 해당 디렉토리에 있는 `rfc2248.mib` 및 `rfc2249.mib` 파일을 사용합니다.



# Unix 플랫폼에서 다른 Sun Java System 제품과 공존

SNMP 지원을 제공하는 다른 Netscape 또는 Sun Java System 제품에서는 플랫폼의 원시 SNMP 마스터 에이전트를 대체하여 이 작업을 수행할 수 있습니다. Messaging Server와 동일한 호스트에서 Sun Java System 제품을 실행하고 SNMP를 통해 모니터링하려면 *Managing Servers with iPlanet Console*([http://docs.sun.com/source/816-5572-10/11\\_snmp.htm](http://docs.sun.com/source/816-5572-10/11_snmp.htm))의 11장에 설명된 대로 Sun Java System 프록시 SNMP 에이전트를 구성합니다. 그러면 Messaging Server SNMP 하위 에이전트(원시 SNMP 하위 에이전트)가 다른 Sun Java System 제품의 비원시 Sun Java System SNMP 하위 에이전트와 공존할 수 있습니다.

## Messaging Server의 SNMP 정보

이 절에서는 SNMP를 통해 제공되는 Messaging Server 정보를 요약합니다. 자세한 내용은 RFC 2788 및 RFC 2789의 개별 MIB 테이블을 참조하십시오. RFC/MIB 용어로 메시징 서비스(MTA, HTTP 등)는 *응용 프로그램*(appl), Messaging Server 네트워크 연결은 *연결*(assoc), MTA 채널은 *MTA 그룹*(mtaGroups)입니다.

여러 Messaging Server 인스턴스를 동시에 모니터링할 수 있는 플랫폼의 경우 applTable에 여러 MTA 및 서버 집합이 있고 다른 테이블에 여러 MTA가 있을 수 있습니다.

---

**주** MIB에 보고되는 누적 값(예: 전달된 총 메일 수, 총 IMAP 연결 수 등)은 재부트 후에 다시 0으로 설정됩니다.

---

사이트별로 임계값과 중요 모니터링 값이 다릅니다. 정상적인 SNMP 클라이언트에서는 추세 분석을 수행하여 기록된 추세와 편차가 발생할 경우 경고를 보냅니다.

## applTable

applTable은 서버 정보를 제공합니다. 이 테이블은 MTA 행 하나와 다음의 각각의 서버에 대한 추가적인 행, 활성화된 경우에는 WebMail HTTP, IMAP, POP, SMTP 및 SMTP Submit 등이 제공됩니다. 이 테이블에서는 버전 정보, 가동 시간, 현재 작업 상태(실행, 중단, 정제), 현재 연결 수, 총 누적 연결 수 및 기타 관련 데이터를 제공합니다.

다음은 applTable(mib-2.27.1.1)의 데이터 예입니다.

### applTable:

```

applName.11 = mailsrv-12 MTA on mailsrv-1.west.sesta.com
applVersion.1 = 5.1
applUptime.1 = 73223
applOperStatus.1 = up4
applLastChange.1 = 74223
applInboundAssociations.1 = 5
applOutboundAssociations.1 = 2
applAccumulatedInboundAssociations.1 = 873
applAccumulatedOutboundAssociations.1 = 234
applLastInboundActivity.1 = 10548223
applLastOutboundActivity.1 = 10542223
applRejectedInboundAssociations.1 = 05
applFailedOutboundAssociations.1 = 17
applDescription.1 = Sun Java System Messaging Server 6.1
applName.21 = mailsrv-1 HTTP WebMail server on mailsrv-1.west.sesta.com
...
applName.3 = mailsrv-1 IMAP server on mailsrv-1.west.sesta.com
...
applName.4 = mailsrv-1 POP server on mailsrv-1.west.sesta.com
...
applName.5 = mailsrv-1 SMTP server on mailsrv-1.west.sesta.com
...
applName.6 = mailsrv-1 SMTP Submit server on mailsrv-1.west.sesta.com
...

```

### 주:

1. 여기서 .1, .2 등의 접미어는 행 번호 applIndex입니다. applIndex에서 값 1은 MTA, 값 2는 HTTP 서버 등을 나타냅니다. 따라서 이 예에서 테이블의 첫 번째 행에는 MTA에 관한 데이터가 제공되고 두 번째 행에는 POP 서버에 관한 데이터가 제공됩니다.
2. 모니터링 Messaging Server 인스턴스 이름입니다. 이 예에서 인스턴스 이름은 mailsrv-1입니다.

3. 이러한 값은 SNMP 타임스탬프 값이고 이벤트 시간의 sysUpTime 값입니다. 즉, sysUpTime은 SNMP 마스터 에이전트가 시작된 후의 시간(1/100초)입니다.
4. HTTP, IMAP, POP, SMTP 및 SMTP Submit 서버의 작업 상태는 구성된 TCP 포트를 통해 해당 서버에 실제로 연결한 다음 해당 프로토콜(예: HTTP의 경우 HEAD 요청 및 응답, SMTP의 경우 HELO 명령 등)을 통해 간단한 작업을 수행하여 확인합니다. 이 연결 시도에서 각 서버의 상태(up(1), down(2), congested(4))가 결정됩니다.

이러한 검사는 서버에 일반 인바운드 연결로 표시되고 각 서버에 대한 applAccumulatedInboundAssociations MIB 변수 값에 포함됩니다.

MTA의 경우 작업 상태는 Job Controller의 작업 상태입니다. MTA가 실행 상태로 표시되면 Job Controller가 실행 중인 것입니다. MTA가 중단 상태로 표시되면 Job Controller가 중단된 것입니다. 이 MTA 작업 상태는 MTA의 서비스 디스패처 상태와는 별개입니다. MTA의 작업 상태는 실행 또는 중단 값으로만 나타납니다. Job Controller에 "congested"(정체)라는 개념은 있지만 MTA 상태에 나타나지는 않습니다.

5. HTTP, IMAP 및 POP 서버의 경우 applRejectedInboundAssociations MIB 변수는 거부된 인바운드 연결 시도 횟수가 아니라 실패한 로그인 시도 횟수를 나타냅니다.

## applTable 사용

나열된 각 응용 프로그램에 대한 서버 상태(applOperStatus) 모니터링은 각 서버 모니터링의 핵심입니다.

applLastInboundActivity가 마지막 MTA 인바운드 작업을 표시한 이후 많은 시간이 경과하면 일부 연결이 끊어져 연결되지 않을 수 있습니다. applOperStatus=2(중단)인 경우 모니터링되는 서비스가 중단 상태입니다. applOperStatus=1(실행)인 경우 다른 곳에 문제가 있을 수 있습니다.

## assocTable

이 테이블은 MTA에 네트워크 연결 정보를 제공합니다. 이 테이블은 각 활성 네트워크 연결에 대한 정보를 제공하는 2차원 테이블입니다. 다른 서버에 대한 연결 정보는 제공되지 않습니다.

다음은 applTable(mib-2.27.2.1)의 데이터 예입니다.

```

assocTable:

    assocRemoteApplication.1.11 = 129.146.198.1672
    assocApplicationProtocol.1.11 = applTCPProtoID.253
    assocApplicationType.1.1 = peerinitiator(3)4
    assocDuration.1.1 = 4005
    ...
    
```

**주:**

1. .x.y 접미어에서 x는 응용 프로그램 색인인 applIndex이며 보고되는 applTable의 응용 프로그램을 나타냅니다. 이 경우에는 MTA입니다. y는 보고되는 응용 프로그램에 대한 각 연결을 나열합니다.
2. 원격 SMTP 클라이언트의 소스 IP 주소입니다.
3. 네트워크 연결에 사용되는 프로토콜을 나타내는 OID입니다. applTCPProtoID는 TCP 프로토콜을 나타냅니다. .n 접미어는 사용 중인 TCP 포트를 나타내고 .25는 TCP 포트 25를 통해 통신하는 프로토콜인 SMTP를 나타냅니다.
4. 원격 SMTP 클라이언트가 사용자 에이전트(UA)인지 다른 MTA인지 알 수 없습니다. 마찬가지로 하위 에이전트는 항상 peer-initiator를 보고하는 반면 ua-initiator는 절대 보고하지 않습니다.
5. 이 값은 SNMP TimeInterval이며 시간 단위(1/100초)를 사용합니다. 이 예에서 연결은 4초 동안 열립니다.

**assocTable 사용**

이 테이블은 활성 문제를 진단하는 데 사용됩니다. 예를 들어, 갑자기 200,000 인바운드 연결이 발생하는 경우 이 테이블을 사용하여 해당 연결의 시작 위치를 알 수 있습니다.

**mtaTable**

applTable의 각 MTA마다 하나의 행을 갖는 1차원 테이블입니다. 각 행에는 mtaGroupTable의 선택 변수에 대한 해당 MTA 내의 모든 채널(그룹이라고 함)의 합계가 제공됩니다.

다음은 `applTable(mib-2.28.1.1)`의 데이터 예입니다.

**mtaTable:**

```

mtaReceivedMessages.11 = 172778
mtaStoredMessages.1 = 19
mtaTransmittedMessages.1 = 172815
mtaReceivedVolume.1 = 3817744
mtaStoredVolume.1 = 34
mtaTransmittedVolume.1 = 3791155
mtaReceivedRecipients.1 = 190055
mtaStoredRecipients.1 = 21
mtaTransmittedRecipients.1 = 3791134
mtaSuccessfulConvertedMessages.1 = 02
mtaFailedConvertedMessages.1 = 0
mtaLoopsDetected.1 = 03

```

**주:**

1. `.x` 접미어는 `applTable`에서 이 응용 프로그램에 대한 행 번호를 제공합니다. 이 예에서 `.1`은 이 데이터가 `applTable`에 있는 첫 번째 응용 프로그램에 대한 데이터임을 나타냅니다. 따라서, 이 데이터는 MTA에 관한 데이터입니다.
2. 변환 채널의 경우 0이 아닌 값만 가집니다.
3. 현재 MTA의 메일 대기열에 저장된 `.HELD` 메일 파일 수를 계산합니다.

### mtaTable 사용

`mtaLoopsDetected`가 0이 아니면 루핑 메일 문제가 있는 것입니다. 그럴 경우 MTA 대기열에서 `.HELD` 파일을 찾아 진단하여 문제를 해결합니다.

시스템에서 변환 채널을 사용하여 바이러스 스캔을 수행하고 감염된 메일을 거부하는 경우 `mtaSuccessfulConvertedMessages`는 다른 변환 오류와 함께 감염된 메일 수를 제공합니다.

## mtaGroupTable

이 2차원 테이블은 `applTable`의 각 MTA에 대한 채널 정보를 제공합니다. 이 정보는 저장(대기열에 포함된) 및 전달된 메일 메시지의 수와 같은 데이터를 포함합니다. 각 채널에 대한 저장된 메일 수 `mtaGroupStoredMessages` 모니터링은 값이 비정상적으로 커서 메일이 대기열에 백업되고 있는 경우에 중요합니다.

다음은 mtaGroupTable(mib-2.28.2.1)의 데이터 예입니다.

**mtaGroupTable:**

```

mtaGroupName.1.11 = tcp_intranet2
...
mtaGroupName.1.21 = ims-ms
...
mtaGroupName.1.31 = tcp_local
  mtaGroupDescription.1.3 = mailsrv-1 MTA tcp_local channel
  mtaGroupReceivedMessages.1.3 = 12154
  mtaGroupRejectedMessages.1.3 = 0
  mtaGroupStoredMessages.1.3 = 2
  mtaGroupTransmittedMessages.1.3 = 12148
  mtaGroupReceivedVolume.1.3 = 622135
  mtaGroupStoredVolume.1.3 = 7
  mtaGroupTransmittedVolume.1.3 = 619853
  mtaGroupReceivedRecipients.1.3 = 33087
  mtaGroupStoredRecipients.1.3 = 2
  mtaGroupTransmittedRecipients.1.3 = 32817
  mtaGroupOldestMessageStored.1.3 = 1103
  mtaGroupInboundAssociations.1.3 = 5
  mtaGroupOutboundAssociations.1.3 = 2
  mtaGroupAccumulatedInboundAssociations.1.3 = 150262
  mtaGroupAccumulatedOutboundAssociations.1.3 = 10970
  mtaGroupLastInboundActivity.1.3 = 1054822
  mtaGroupLastOutboundActivity.1.3 = 1054222
  mtaGroupRejectedInboundAssociations.1.3 = 0
  mtaGroupFailedOutboundAssociations.1.3 = 0
  mtaGroupInboundRejectionReason.1.3 =
  mtaGroupOutboundConnectFailureReason.1.3 =
  mtaGroupScheduledRetry.1.3 = 0
  mtaGroupMailProtocol.1.3 = applTCPProtoID.25
  mtaGroupSuccessfulConvertedMessages.1.3 = 03
  mtaGroupFailedConvertedMessages.1.3 = 0
  mtaGroupCreationTime.1.3 = 0
  mtaGroupHierarchy.1.3 = 0
  mtaGroupOldestMessageId.1.3 = <01IFBV8AT8HYB4T6UA@red.iplanet.com>
  mtaGroupLoopsDetected.1.3 = 04
  mtaGroupLastOutboundAssociationAttempt.1.3 = 1054222
    
```

**주:**

1. .x.y 접미어에서 x는 응용 프로그램 색인인 applIndex이며 보고되는 applTable의 응용 프로그램을 나타냅니다. 이 경우에는 MTA입니다. y는 MTA의 각 채널을 나열합니다. 이 열거 색인 mtaGroupIndex는 mtaGroupAssociationTable 및 mtaGroupErrorTable 테이블에도 사용됩니다.
2. 보고되는 채널의 이름이며 이는 tcp\_intranet 채널입니다.

3. 변환 채널의 경우 0이 아닌 값만 가집니다.
4. 현재 이 채널의 메일 대기열에 저장된 .HELD 메일 파일 수를 계산합니다.

### mtaGroupTable 사용

\*Rejected\* 및 \*Failed\*에 대한 추세 분석은 잠정적인 채널 문제를 확인하는 데 유용할 수 있습니다.

mtaGroupStoredVolume의 비율이 mtaGroupStoredMessages로 갑자기 증가하면 대용량 정크 메일이 해당 대기열 주위로 바운스되는 것을 의미할 수 있습니다.

mtaGroupStoredMessages로 갑자기 증가하는 것은 요청하지 않은 대량 전자 메일을 받거나 어떤 이유로 인해 전달이 실패함을 나타낼 수 있습니다.

mtaGroupOldestMessageStored 값이 전달할 수 없는 메일 알림(notices 채널 키워드)에 사용된 값보다 몇 배 이상 큰 경우 이는 바운스 처리를 통해 처리할 수 없는 메일을 나타낼 수 있습니다. 바운스는

mtaGroupOldestMessageStored > (최대 기간 + 24시간)를 테스트로 사용할 수 있도록 밤에 수행됩니다.

mtaGroupLoopsDetected가 0보다 큰 경우 메일 루프가 감지됩니다.

## mtaGroupAssociationTable

해당 항목이 assocTable에 대한 색인이 되는 3차원 테이블입니다. applTable의 각 MTA에는 2차원 하위 테이블이 있습니다. 이 2차원 하위 테이블에는 해당 MTA의 각 채널에 대한 행이 하나씩 있습니다. 각 채널에는 해당 채널이 현재 진행 중인 각 활성 네트워크 연결에 대한 항목이 있습니다. 해당 항목 값은 assocTable에 대한 색인(항목 값에 의해 색인화되고 MTA의 applIndex 색인이 참조된)입니다. assocTable에 표시된 항목은 채널에 보 관된 네트워크 연결입니다.

즉, mtaGroupAssociationTable 테이블은 assocTable에 표시된 네트워크 연결을 mtaGroupTable의 해당 채널에 연결합니다.

다음은 mtaGroupAssociationTable(mib-2.28.3.1)의 데이터 예입니다.

**mtaGroupAssociationTable:**

```
mtaGroupAssociationIndex.1.3.11 = 12
mtaGroupAssociationIndex.1.3.2 = 2
```

```
mtaGroupAssociationIndex.1.3.3 = 3
mtaGroupAssociationIndex.1.3.4 = 4
mtaGroupAssociationIndex.1.3.5 = 5
mtaGroupAssociationIndex.1.3.6 = 6
mtaGroupAssociationIndex.1.3.7 = 7
```

**주:**

1. .x.y.z 접미어에서 x는 응용 프로그램 색인 applIndex이며 보고되는 applTable의 응용 프로그램을 나타냅니다. 이 경우에는 MTA입니다. y는 보고되는 mtaGroupTable의 채널을 나타냅니다. 이 예에서 3은 tcp\_local 채널을 나타냅니다. z는 채널에(서) 열린 연결을 나열합니다.
2. 여기서 값은 assocTable에 대한 색인입니다. 특히 x와 이 값은 각각 assocTable의 applIndex 및 assocIndex 색인 값이 됩니다. 또는 assocTable(applIndex 무시)의 첫 번째 행은 tcp\_local 채널에 의해 제어되는 네트워크 연결을 설명합니다.

## mtaGroupErrorTable

메일 전달을 시도하는 동안 각 MTA의 각 채널에서 발생된 임시 및 영구 오류의 개수를 제공하는 다른 3차원 테이블입니다. 색인 값이 4000000인 항목은 임시 오류이고 색인 값이 5000000인 항목은 영구 오류입니다. 임시 오류가 발생하면 나중에 전달 시도할 수 있도록 대기열에 메일을 다시 포함하고, 영구 오류가 발생하면 메일은 거부되거나 전달할 수 없는 메일로 반환됩니다.

다음은 mtaGroupErrorTable(mib-2.28.5.1)의 데이터 예입니다.

**mtaGroupErrorTable:**

```
mtaGroupInboundErrorCount.1.1.40000001 = 0
mtaGroupInboundErrorCount.1.1.5000000 = 0
mtaGroupInternalErrorCount.1.1.4000000 = 0
mtaGroupInternalErrorCount.1.1.5000000 = 0
mtaGroupOutboundErrorCount.1.1.4000000 = 0
mtaGroupOutboundErrorCount.1.1.5000000 = 0

mtaGroupInboundErrorCount.1.2.40000001 = 0
...
```



```
mtaGroupInboundErrorCount.1.3.40000001 = 0
...
```

**주:**

1. .x.y.z 접미어에서 x는 응용 프로그램 색인 applIndex이며 보고되는 applTable의 응용 프로그램을 나타냅니다. 이 경우에는 MTA입니다. y는 보고되는 mtaGroupTable의 채널을 나타냅니다. 이 예에서 1은 tcp\_intranet 채널을 지정하고 2는 ims-ms 채널을, 3은 tcp\_local 채널을 지정합니다. 마지막으로 z는 4000000 또는 5000000이며 각각 해당 채널에 대한 메일 전달 시도 중에 발생한 임시 오류 및 영구 오류의 개수를 나타냅니다.

**mtaGroupErrorTable 사용**

오류 개수가 크게 증가하면 비정상적인 전달 문제를 나타낼 수 있습니다. 예를 들어, tcp\_channel이 크게 증가하면 DNS 또는 네트워크 문제를 나타낼 수 있습니다. ims\_ms 채널이 크게 증가할 경우 메일을 메시지 저장소로 전달하는 데 문제(예: 분할 영역이 꽉 참, stored 문제 등)가 있을 수 있습니다.

Messaging Server의 SNMP 정보

# Messaging Server에서 Event Notification Service 관리

이 부록에서는 Messaging Server에서 Event Notification Service Publisher(ENS Publisher)를 사용하고 Event Notification Service(ENS)를 관리할 때 필요한 사항에 대해 설명합니다.

이 장/부록은 다음 내용으로 구성되어 있습니다.

- Messaging Server에서 ENS Publisher 로드
- 샘플 Event Notification Service 프로그램 실행
- Event Notification Service 관리

ENS 및 ENS API에 대한 자세한 내용은 Sun Java System Calendar Server([http://docs.sun.com/db/coll/CalendarServer\\_05q1](http://docs.sun.com/db/coll/CalendarServer_05q1) 및 [http://docs.sun.com/db/coll/CalendarServer\\_05q1\\_ko](http://docs.sun.com/db/coll/CalendarServer_05q1_ko))의 *Event Service Notification Manual for Sun Java System Communications Services* 및 Messaging Server 설명서 웹 페이지([http://docs.sun.com/db/coll/MessagingServer\\_05q1](http://docs.sun.com/db/coll/MessagingServer_05q1) 및 [http://docs.sun.com/db/coll/MessagingServer\\_05q1\\_ko](http://docs.sun.com/db/coll/MessagingServer_05q1_ko))를 참조하십시오.

## Messaging Server에서 ENS Publisher 로드

Event Notification Service(ENS)는 기본 게시 및 가입 서비스입니다. ENS는 Sun Java System 응용 프로그램이 특정 유형의 *이벤트*를 수집하기 위한 중앙 지점으로 사용하는 디스패처 역할을 합니다. 이벤트는 하나 이상의 자원 등록 정보 값에 대한 변경 사항입니다. 이러한 유형의 이벤트가 발생할 때 그 사실을 알고자 하는 모든 응용 프로그램은 이벤트 순서를 식별하고 알림과 가입을 일치시키는 ENS에 등록합니다.

ENS와 iBiff(Messaging Server용 ENS Publisher)는 Messaging Server부터 함께 제공됩니다. ENS는 기본적으로 사용되지만 iBIFF는 로드되지 않습니다. ("[Messaging Server에서 ENS Publisher 로드](#)" 참조)

Messaging Server에서 알림에 가입하려면 Messaging Server 호스트에서 libibiff를 로드한 다음 Messaging Server를 중지했다가 다시 시작해야 합니다.

## Messaging Server에서 ENS Publisher 로드

명령줄에서 다음 단계를 수행합니다. 이 단계에서 Messaging Server 설치 디렉토리의 위치는 `msg_svr_base`이며 Messaging Server 사용자는 `inetuser`입니다. 이 변수의 일반적인 값은 각각 `/opt/SUNWmsgsr` 및 `inetuser`입니다.

1. `inetuser`로 `configutil` 유틸리티를 실행하여 `libibiff` 파일을 로드합니다.

```
cd msg_svr_base
```

```
./configutil -o "local.store.notifyplugin" -v "msg_svr_base/lib/libibiff"
```

2. `root`로 Messaging Server를 중지했다가 다시 시작합니다.

```
cd msg_svr_base/sbin
```

```
./stop-msg
```

```
./start-msg
```

3. 이제 ENS를 통해 알림을 받을 수 있습니다. 자세한 내용은 "[샘플 Event Notification Service 프로그램 실행](#)"을 참조하십시오.

## 샘플 Event Notification Service 프로그램 실행

Messaging Server에는 알림 수신 방법을 익힐 수 있는 샘플 프로그램이 포함되어 있습니다. 이 샘플 프로그램은 `msg_svr_base/examples` 디렉토리에 있습니다.

## 샘플 ENS 프로그램 실행

1. `msg_svr_base/examples` 디렉토리로 이동합니다.
2. `Makefile.sample` 파일을 사용하여 C 컴파일러로 `apub`와 `asub` 예를 컴파일합니다.  
`msg_svr_base/examples` 디렉토리가 포함되도록 라이브러리 검색 경로를 설정합니다.
3. 프로그램 컴파일이 끝나면 별도 창에서 다음과 같이 실행할 수 있습니다.

```
apub localhost 7997
```

```
asub localhost 7997
```

`apub` 창에 입력하는 내용은 모두 `asub` 창에 나타납니다. 또한 기본 설정을 사용할 경우 모든 `iBiff` 알림이 `asub` 창에 나타납니다.

4. `iBiff`에서 발행한 알림을 받으려면 `asub.c`와 유사한 프로그램을 작성합니다.

샘플 프로그램 및 ENS용 프로그램을 직접 작성하는 것에 대한 자세한 내용은 *iPlanet Event Notification Service Messaging and Collaboration Manual*을 참조하십시오.

---

**주** 라이브러리 검색 경로에 `msg_svr_base/lib` 디렉토리가 포함되도록 설정한 다음에는 더 이상 `Directory Server`를 중지하고 시작할 수 없습니다. 해결 방법은 라이브러리 검색 경로에서 해당 항목을 제거하는 것입니다.

---

## Event Notification Service 관리

ENS의 관리 작업에는 서비스의 시작과 중지, ENS용 `iBiff Publisher`의 동작을 제어하기 위한 구성 매개 변수 변경이 포함됩니다.

### ENS 시작 및 중지

`start-msg ens` 및 `stop-message ens` 명령을 사용하여 ENS 서버를 시작 및 중지할 수 있습니다. 이 명령을 실행하려면 `root`가 되어야 합니다.

## ENS 시작 및 중지

- ENS를 시작하려면 다음을 수행합니다.

```
msg_svr_base/sbin/start-msg ens
```

- ENS를 중지하려면 다음을 수행합니다.

```
msg_svr_base/sbin/stop-msg ens
```

## iPlanet Event Notification Service 구성 매개 변수

몇 가지의 구성 매개 변수가 iBiff의 동작을 제어합니다. configutil 유틸리티 프로그램을 사용하여 이러한 매개 변수를 설정합니다.

**표 B-1** iBiff 구성 매개 변수

| 매개 변수                                     | 설명                                                                                                                                                                                                                                                                  |
|-------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| local.store.notifyplugin.maxHeaderSize    | 알림과 함께 전송될 헤더의 최대 크기(바이트)를 지정합니다. 기본값은 0바이트입니다.                                                                                                                                                                                                                     |
| local.store.notifyplugin.maxBodySize      | 알림과 함께 전송될 본문의 최대 크기(바이트)를 지정합니다. 기본값은 0바이트입니다.                                                                                                                                                                                                                     |
| local.store.notifyplugin.eventType.enable | 특정 이벤트 유형이 알림을 생성하는 경우에 지정합니다. ReadMsg, NewMsg 등의 다양한 <i>eventTypes</i> 에 대해서는 <i>Messaging Server for Messaging and Collaboration Manual</i> 을 참조하십시오. 유효한 값은 1(활성화)과 0(비활성화)입니다. 기본값은 1이며, local.store.notifyplugin.ReadMsg.enable을 0으로 설정하면 ReadMsg 알림이 비활성화됩니다. |
| local.store.notifyplugin.ensHost          | ENS 서버의 호스트 이름을 지정합니다. 기본값은 127.0.0.1입니다.                                                                                                                                                                                                                           |
| local.store.notifyplugin.ensPort          | ENS 서버의 TCP 포트를 지정합니다. 기본값은 7997입니다.                                                                                                                                                                                                                                |
| local.store.notifyplugin.ensEventKey      | ENS 알림에 사용할 이벤트 키를 지정합니다. 기본값은 enp://127.0.0.1/store입니다. 이벤트 키의 호스트 이름 부분은 ENS 호스트를 결정하는 데 사용되지 않으며, ENS가 사용하는 고유 식별자일 뿐입니다.<br><br>이 키는 가입자가 이 키에 일치하는 이벤트에 대한 알림을 받기 위해 가입해야 하는 키입니다.                                                                             |

# 콘솔 인터페이스가 있는 메일 사용자 및 메일 목록 관리(권장되지 않음)

이 부록은 참조용입니다. 이 부록에 설명한 대로 사용자 및 메일 목록을 만들고 관리하는데 콘솔 인터페이스를 사용하지 마십시오. 사용자 관리 유틸리티와 같은 다른 승인된 준비 도구를 사용합니다.

---

**주의** 콘솔 인터페이스를 사용하여 사용자 및 그룹을 만들면 여러 가지 문제가 발생할 수 있습니다. 다른 승인 준비 도구(Delegated Administrator)를 사용하십시오. *Sun Java System Messaging Server 관리 설명서* (<http://docs.sun.com/doc/819-1055>)를 참조하십시오.

---

이 부록은 참조용입니다. 사용자의 메일 계정 및 메일 목록을 만들고 관리하는데 있어 콘솔 인터페이스를 사용하지 **않는** 것이 좋습니다.

## 메일 사용자 관리

### 메일 사용자 액세스

이 절에서는 사용자의 메일 관리 인터페이스를 여는 방법에 대해 설명합니다. Messaging Server 메일 계정은 기업의 중앙 LDAP 사용자 디렉토리에 사용자 항목의 속성으로 저장됩니다. 따라서 메일 계정을 관리하려면 해당 디렉토리의 사용자 항목을 수정합니다.

## 새 사용자 만들기

새 메일 계정을 만들려면 디렉토리에서 새 사용자를 만듭니다. 해당 사용자에 대한 메일 계정도 설치해야 합니다. 메일 계정을 설치하지 않으면 해당 사용자가 콘솔의 메일 관리 부분을 사용할 수 없습니다. 사용자를 만들고 다른 유형의 사용자 정보를 지정하는 전체 프로세스에 대한 자세한 내용은 *Sun ONE Server Console 5.2 Server Management Guide*의 사용자 및 그룹 관리에 대한 장에 설명되어 있습니다.

새 메일 사용자를 만들려면 다음을 수행합니다.

1. 콘솔 주 창에서 사용자 및 그룹 탭을 누릅니다.
2. 드롭다운 목록에서 새 사용자를 선택하고 만들기를 누릅니다.
3. 사용자에 대한 조직 단위를 선택하고 확인을 누릅니다. 사용자 만들기 창이 열립니다.
4. *Sun ONE Server Console 5.2 Server Management Guide*의 사용자 및 그룹 관리에 대한 장에 설명된 대로 사용자에 대한 정보를 입력합니다.
5. 사용자 만들기 창을 열어 둔 채로 계정 탭을 누릅니다. 새 사용자 계정에 대해 설치된 제품 목록이 오른쪽 창에 나타납니다.
6. 메일 계정 설치 상자를 누릅니다. 사용자 만들기 창에서 메일 탭을 볼 수 있습니다.
7. 사용자 만들기 창에서 메일 탭을 누른 다음 오른쪽 창에서 원하는 탭을 누릅니다.
8. 변경 사항을 입력한 다음 사용자 만들기 창의 아래쪽에서 확인을 누릅니다.

---

**주**                    확인을 누르기 전에 관련 탭에서 모든 설치 절차를 완료했는지 확인합니다.

---

## 기존 사용자 액세스

기존 메일 계정을 수정하거나 기존 사용자에게 메일 기능을 추가하려면 사용자 디렉토리에서 적합한 사용자에게 액세스한 다음 해당 사용자의 메일 계정 속성을 추가 또는 수정합니다.

기존 사용자에 대한 메일 정보에 액세스하려면 다음을 수행합니다.

1. 콘솔 주 창에서 사용자 및 그룹 탭을 누릅니다.
2. 사용자 및 그룹 주 창에서 검색 또는 고급 검색을 누릅니다.



3. 검색 창에서 검색 조건(예: 사용자 성)을 입력하고 사용자 디렉토리의 검색을 수행합니다.
4. 사용자 및 그룹 주 창으로 돌아가 검색 결과에서 사용자를 선택하고 편집을 누릅니다.
5. 항목 편집 창에 메일 탭이 표시되지 않는 경우 다음을 수행합니다.
  - a. 계정 탭을 누릅니다. 오른쪽 창에 설치된 계정 목록이 나타납니다.
  - b. 메일 계정 상자를 선택합니다. 항목 편집 창에 메일 탭이 표시됩니다.
6. 항목 편집 창에서 메일 탭을 누른 다음 오른쪽 창에서 원하는 탭을 누릅니다.
7. 변경 사항을 입력한 다음 항목 편집 창의 맨 아래에서 확인을 누릅니다.

## 사용자 전자 메일 주소 지정

메일이 사용자에게 성공적으로 전달하려면 먼저 해당 사용자에 대한 메일 주소 지정 정보를 지정해야 합니다. 메일 주소 지정 정보는 Messaging Server 호스트 이름, 사용자의 주 주소 및 모든 대체 주소로 구성됩니다. 호스트 이름 및 주 주소 정보는 필수 사항이며 대체 주소 정보는 선택 사항입니다.

사용자의 메일 주소 지정 정보를 지정하려면 다음을 수행합니다.

1. [847페이지의 "메일 사용자 액세스"](#)에 설명된 대로 콘솔에서 사용자 만들기 또는 항목 편집 창에 액세스합니다.
2. 메일 탭을 누릅니다.
3. 이미 활성화되어 있지 않은 경우 설정 탭을 누릅니다.
4. (필수 사항) Messaging Server 호스트 이름을 입력합니다.

이 사용자의 메일을 처리할 Messaging Server를 호스트하는 시스템입니다. 해당 시스템의 Messaging Server에 알려진 정규화된 도메인 이름(FQDN)입니다.

**5. (필수 사항) 사용자의 주 전자 메일 주소를 입력합니다.**

이 사용자의 메일을 보낼 공용 주소입니다. 사용자는 RFC 821 사양에 맞는 정확한 형식의 유효한 주 주소를 하나만 가질 수 있습니다.

호스트 이름 숨기기(보내는 메일 헤더에 사용자 주소의 호스트 이름이 표시되지 않음)를 구현하려면 주 전자 메일 주소 필드에서 호스트 이름을 지정하지 않습니다. 대신 다음 단계에서 설명하는 대로 호스트 이름을 포함한 대체 주소를 입력합니다.

**6. (선택 사항) 대체 주소 목록에 주소를 추가합니다.**

대체 주소는 사용자의 주 주소에 대해 필수적인 별칭입니다. 이 기능을 사용하여 다음을 수행할 수 있습니다.

- 주소가 잘못된 메일이 올바르게 전달되도록 합니다("Smythe"의 별칭으로 "Smith"를 사용하는 경우 등).
- 보내는 메일 헤더에서 이름 숨기기를 사용 가능하게 합니다. 그러려면 호스트 이름을 포함하고 사용자의 주 전자 메일 주소의 호스트 이름을 포함하지 않는 대체 주소를 제공해야 합니다. 예를 들어, jsmith@siroe.com을 주 전자 메일 주소로 입력한 다음 jsmith@sesta.com을 대체 주소로 입력합니다. 이 사용자가 메일을 보내면 보내는 헤더에 jsmith@siroe.com이 표시되지만 해당 주소로 보낸 모든 메일(회신 포함)은 실제로 jsmith@sesta.com(sesta.com이 유효한 호스트 이름이라고 가정)으로 라우팅됩니다.

각 주소가 고유하다면 특정 사용자에 대한 모든 수의 대체 주소를 지정할 수 있습니다. 이러한 별칭으로 수신되는 메일은 주 주소로 보내집니다.

대체 주소를 입력하려면 다음을 수행합니다.

- a. 대체 주소 필드 아래에 있는 추가 버튼을 누릅니다.
  - b. 대체 주소 창에서 대체 주소를 입력합니다. 원하는 개수만큼 대체 주소를 추가할 수 있지만 이 창을 열 때마다 하나의 주소만 입력할 수 있습니다.
  - c. 확인을 눌러 대체 주소를 추가하고 대체 주소 창을 닫습니다. 다른 대체 주소를 입력하려면 추가를 다시 눌러 대체 주소 창을 다시 엽니다.
- 7. 이 사용자의 메일 정보 변경을 완료했다면 항목 편집 창 맨 아래에서 확인을 누릅니다. 그렇지 않으면 다른 탭을 눌러서 변경 작업을 계속합니다.**

## 전달 옵션 구성

Messaging Server는 각 사용자에게 대해 모든 조합으로 사용 및 구성할 수 있는 세 개의 기본 메일 전달 옵션을 지원합니다. 정규 POP/IMAP 전달, 프로그램 전달 및 UNIX 전달 (UNIX Messaging Server 호스트의 클라이언트에 대한)이 제공됩니다.

메시징용 iPlanet Delegated Administrator는 또한 이러한 옵션을 사용자가 직접 사용 및 구성할 수 있도록 최종 사용자 HTML 인터페이스를 제공합니다. 콘솔 인터페이스와 iPlanet Delegated Administrator 인터페이스는 모두 동일한 디렉토리 속성을 조작합니다. 해당 인터페이스를 열면 관리자와 사용자 중 누가 설정했던 관계없이 각각에 현재 설정이 표시됩니다.

---

**주** Delegated Administrator for Messaging은 Sun Java System LDAP Schema v. 1만 지원하고 v.2는 지원하지 않습니다.

---

사용자에 대한 전달 옵션을 구성하려면 다음을 수행합니다.

1. [847페이지의 "메일 사용자 액세스"](#)에 설명된 대로 콘솔에서 사용자 만들기 또는 항목 편집 창에 액세스합니다.
2. 메일 탭을 누릅니다.
3. 전달 탭을 누릅니다.
4. 이 사용자가 사용할 수 있는 전달 방법을 선택합니다.
  - POP/IMAP 전달을 지정하려면 [851페이지의 "POP/IMAP 전달 지정"](#)의 지침을 따릅니다.
  - 프로그램 전달을 지정하려면 [852페이지의 "프로그램 전달 지정"](#)의 지침을 따릅니다.
  - UNIX 전달을 지정하려면 [853페이지의 "UNIX 전달 지정"](#)의 지침을 따릅니다.
5. 이 사용자의 메일 정보 변경을 완료했다면 항목 편집 창 맨 아래에서 확인을 누릅니다. 그렇지 않으면 다른 탭을 눌러서 변경 작업을 계속합니다.

### POP/IMAP 전달 지정

이 옵션을 지정하면 사용자의 정규 POP3 또는 IMAP4 메일함으로 메일 전달이 가능합니다. 이 사용자에게 대한 POP/IMAP 전달을 사용하려면 다음을 수행합니다.

1. 전달 탭을 누릅니다.

2. POP/IMAP 상자를 선택하고 등록 정보 버튼을 눌러 POP/IMAP 전달 창을 엽니다.
3. (선택 사항) 처리하려는 사용자의 메일이 전달 및 저장되는 메시지 저장소 분할 영역의 별명(경로 이름 또는 물리적 절대 경로가 아닌)을 입력합니다. 이 필드를 비워두면 현재 주 분할 영역이 사용됩니다. 자세한 내용은 [551페이지의 "메시지 저장소 관리"](#)를 참조하십시오.
4. (선택 사항) 사용자에게 할당되는 저장소 제한 또는 디스크 할당량을 입력합니다. 할당량은 지정된 기본값이나([573페이지의 "메시지 저장소 할당량 구성"](#) 참조) 제한 없음(최대 저장소 제한이 없는) 또는 제한(KB 또는 MB)으로 지정할 수 있습니다.
5. (선택 사항) 사용자에게 할당되는 메일 수 제한을 입력합니다. 이 제한은 지정된 기본값이나([573페이지의 "메시지 저장소 할당량 구성"](#) 참조) 제한 없음(최대 저장소 제한이 없는) 또는 제한(숫자)으로 지정할 수 있습니다.

## 프로그램 전달 지정

이 옵션을 지정하면 메일이 사용자에게 전달되기 전에 처리를 위해 외부 응용 프로그램에 전달되는 기법을 제공합니다.

---

**주** 이 절에서는 개별 사용자가 프로그램 전달 옵션을 사용할 수 있도록 하는 방법에 대해서만 설명합니다. 사용자에게 프로그램 전달을 사용 가능하게 하기 전에 먼저 여러 다른 관리 작업을 수행해야 하는 프로그램 전달 모듈을 전체적으로 사용 가능하게 해야 합니다.

---

사용자가 프로그램 전달을 사용할 수 있게 하려면 다음을 수행합니다.

1. 전달 탭을 누릅니다.
2. 프로그램 전달 상자를 선택하고 등록 정보 버튼을 눌러 프로그램 전달 창을 엽니다.
3. 사용자의 메일 처리에 사용될 외부 응용 프로그램 명령을 입력합니다.
4. 확인을 누릅니다.

## UNIX 전달 지정

이 옵션을 지정하면 사용자에게 대한 UNIX 전달이 선택됩니다. UNIX 전달 기능을 사용하면 메일이 사용자의 지정된 UNIX 메일함에 전달됩니다. UNIX 전달은 Messaging Server가 UNIX 호스트 시스템에서 실행되는 사용자만 사용 가능합니다.

사용자가 UNIX 전달을 사용하게 하려면 다음을 수행합니다.

1. 전달 탭을 누릅니다.
2. UNIX 전달 상자를 선택합니다.

---

**주** Messaging Server 사용자에게 UNIX 전달을 제공하려면 일반 UNIX 메일 관리 작업도 수행해야 합니다.

---

## 전달 주소 지정

Messaging Server의 메일 전달 기능을 사용하면 사용자의 메일을 해당 사용자의 주 주소를 대신하여 또는 추가로 다른 주소로 전달할 수 있습니다.

Delegated Administrator for Messaging은 사용자가 전달 주소를 직접 지정할 수 있도록 최종 사용자 HTML 인터페이스를 제공합니다. 콘솔 인터페이스와 Delegated Administrator 인터페이스는 모두 동일한 디렉토리 속성을 조작합니다. 해당 인터페이스를 열면 관리자와 사용자 중 누가 설정했든 관계없이 각각에 현재 설정이 표시됩니다.

---

**주** Delegated Administrator for Messaging은 Sun Java System LDAP Schema v. 1만 지원하고 v.2는 지원하지 않습니다.

---

사용자에 대한 전달 주소 정보를 지정하려면 다음을 수행합니다.

1. [847페이지의 "메일 사용자 액세스"](#)에 설명된 대로 콘솔에서 사용자 만들기 또는 항목 편집 창에 액세스합니다.
2. 메일 탭을 누릅니다.
3. 전달 탭을 누릅니다.  
전달 주소 필드는 사용자의 모든 현재 전달 주소 집합을 표시합니다(있는 경우).
4. 전달 주소를 추가하려면 추가를 누릅니다.
5. 전달 주소 창에서 전달 주소를 입력합니다.

6. 확인을 눌러 메일 전달 탭의 전달 주소 필드에 주소를 추가하고 전달 주소 창을 닫습니다.
7. 이 사용자의 메일 정보 변경을 완료했으면 항목 편집 창 맨 아래에서 확인을 누릅니다. 그렇지 않으면 다른 탭을 눌러서 변경 작업을 계속합니다.

---

**주** 동일한 Messaging Server에 있는 두 사용자 계정 모두 다른 전달 유형을 사용할 수 없는 경우 서로를 지정하는 전달 주소를 설정하지 않습니다. 그렇지 않으면 메일 전달 문제가 발생할 수 있습니다.

---

## 자동 회신 설정 구성

Messaging Server의 자동 회신 기능을 사용하면 사용자의 받는 메일에 대한 자동 회신을 지정할 수 있습니다. 휴가 모드와 자동 응답 모드의 서로 다른 두 가지 자동 응답 모드를 지정할 수 있습니다.

또한 Delegated Administrator for Messaging은 자동 회신 설정을 사용자가 직접 사용 및 구성할 수 있도록 최종 사용자 HTML 인터페이스를 제공합니다. 콘솔 인터페이스와 Delegated Administrator 인터페이스는 모두 동일한 디렉토리 속성을 조작합니다. 해당 인터페이스를 열면 관리자와 사용자 중 누가 설정했든 관계없이 각각에 현재 설정이 표시됩니다.

---

**주** Delegated Administrator for Messaging은 Sun Java System LDAP Schema v. 1만 지원하고 v.2는 지원하지 않습니다.

---

자동 회신 서비스를 사용하려면 다음을 수행합니다.

1. 847페이지의 "메일 사용자 액세스"에 설명된 대로 콘솔에서 사용자 만들기 또는 항목 편집 창에 액세스합니다.
2. 메일 탭을 누릅니다.
3. 자동 회신 탭을 누릅니다.

4. 다음 자동 회신 모드 중 하나를 선택합니다.

**해제:** 자동 회신을 사용할 수 없습니다.

**휴가:** 사용자가 지정한 사람으로부터 받는 첫 번째 메일에 대해 자동 회신 메일을 보냅니다. 보낸 사람의 후속 메일에 대해서는 자동 회신 시간 초과에 도달하기 전까지 회신을 보내지 않습니다. 시간 초과에 도달하면 다음 시간 초과에 도달하기 전까지 새로운 메일이 한번 보내지는 식으로 반복됩니다. 이 모드를 선택하면 휴가 시작/종료 날짜 옵션을 사용하여 회신 텍스트 필드에서 회신 메일을 입력합니다.

5. 휴가 모드를 선택한 경우 자동 회신 메일이 시작되고 종료되는 날짜 및 시간을 지정합니다.
  - 휴가 시작/종료 날짜 확인란을 선택합니다.
  - 시작 및 종료에 대한 편집 버튼을 누른 다음 표시되는 달력을 사용하여 날짜 및 시간을 지정합니다.
6. 시간 또는 일 단위로 자동 회신 시간 초과 값을 지정합니다.
7. 휴가 모드를 선택한 경우 자동 회신 제목 행을 입력하고 보낸 사람에게 반송하는 회신 메일을 입력합니다.
 

내부의 보낸 사람 및 외부의 보낸 사람에 대한 회신 메일을 입력할 수 있습니다. 내부의 보낸 사람에 대한 회신을 입력하면 사용자 도메인 내에 있는 보낸 사람만이 자동 회신을 받게 됩니다.

메일 텍스트 영역 위에 있는 드롭다운 목록에서 사용 가능한 언어를 선택하여 하나의 메일을 여러 언어로 만들 수 있습니다.
8. 이 사용자의 메일 정보 변경을 완료했으면 항목 편집 창 맨 아래에서 확인을 누릅니다. 그렇지 않으면 다른 탭을 눌러서 변경 작업을 계속합니다.

## 허가된 서비스 구성

이 사용자가 메일에 액세스할 수 있도록 메일 서비스를 사용하려면 다음을 수행합니다.

1. [847페이지의 "메일 사용자 액세스"](#)에 설명된 대로 콘솔에서 사용자 만들기 또는 항목 편집 창에 액세스합니다.
2. 메일 탭을 누릅니다.
3. 허가된 서비스 탭을 누릅니다.
 

허가된 서비스 창은 특정 도메인에 적용되는 서비스를 표시합니다.

4. 해당 버튼을 눌러 서비스를 추가, 편집 또는 삭제할 수 있습니다. "허가된 서비스에 대한 수정 규칙" 창이 나타납니다.
5. 서비스 드롭다운 목록에서 규칙을 만들려는 서비스(IMAP, POP, SMTP, HTTP 또는 모두)를 선택합니다.
6. 허용 또는 거부를 지정하고 이 규칙을 적용할 도메인을 지정합니다.
7. 변경 사항을 제출하려면 확인을 누릅니다.

## 메일 목록 관리

### 메일 목록 액세스

이 절에서는 메일 목록의 관리 인터페이스로 이동하는 방법에 대해 설명합니다.

Messaging Server 메일 목록이 LDAP 사용자 디렉토리에 그룹 항목의 속성으로 저장되기 때문에 메일 목록을 관리하는 것은 디렉토리 그룹에 액세스 및 수정하는 것입니다.

### 새 그룹 만들기

새 메일 목록을 만들려면 디렉토리에 새 그룹을 만듭니다. 또한 해당 그룹에 대한 메일 계정도 설치해야 합니다. 메일 계정을 설치하지 않으면 해당 그룹에서 콘솔의 메일 관리 부분을 사용할 수 없습니다. 디렉토리 그룹을 만들고 다른 종류의 그룹 정보를 지정하는 전체 프로세스에 대한 내용은 *Sun ONE Server Console 5.2 Server Management Guide*의 사용자 및 그룹 관리에 대한 장에 자세히 설명되어 있습니다.

새 메일 목록을 만들려면 다음을 수행합니다.

1. 콘솔 주 창에서 사용자 및 그룹 탭을 누릅니다.
2. 드롭다운 목록에서 새 그룹을 선택하고 만들기를 누릅니다.
3. 그룹에 대한 조직 단위를 선택하고 확인을 누릅니다.
4. 그룹 만들기 창에서 *Sun ONE Server Console 5.2 Server Management Guide*의 사용자 및 그룹 관리에 대한 장에 설명된 대로 그룹 항목을 만드는 데 필요한 정보를 입력합니다.

메일 목록 전용인 경우 사용자 및 그룹 구성원 탭을 사용하여 구성원을 추가하지 *않*아도 됩니다. 대신 다음과 같이 메일 계정 전자 메일 전용 구성원 탭을 사용하여 구성원을 추가할 수 있습니다.



- 정규 그룹 구성원은 메일 목록에 대한 전체 권한도 가지고 있지만 해당 그룹 멤버십에 표시된 다른 모든 권한도 가지고 있습니다. 구성원 탭을 사용하여 정규 구성원(정적 또는 동적)을 추가합니다.
  - 메일 목록 구성원은 메일 목록 구성 요소에서 제공하는 제한된 그룹 권한을 가지고 있습니다(이것이 그룹이 존재하는 이유일 수도 있고 아닐 수도 있음). 메일 목록 구성원을 전자 메일 전용 구성원이라고 하며 메일 탭을 사용하여 구성원을 추가합니다.
5. 그룹 만들기 창을 열어 둔 채로 계정 탭을 누릅니다.  
그룹 계정에 대해 설치된 제품 목록이 오른쪽 창에 나타납니다.
  6. 메일 계정 상자를 누릅니다.  
그룹 만들기 창에서 메일 탭을 볼 수 있습니다.
  7. 그룹 만들기 창에서 메일 탭을 누른 다음 오른쪽 창에서 적절한 탭을 누릅니다.
  8. 변경 사항을 입력한 다음 그룹 만들기 창의 맨 아래에서 확인을 누릅니다.  
이 작업을 수행하면 사용자 항목이 제출되고 그룹 만들기 창이 닫힙니다.

---

**주** 모든 메일 관리 창의 맨 아래에서 확인을 누르면 모든 메일 관리 탭에 입력한 모든 현재 메일 구성 정보가 제출됩니다. 확인을 누르기 전에 관련 창에서 모든 설치 절차를 완료했는지 확인합니다.

---

## 기존 그룹 액세스

기존 메일 목록을 수정하거나 기존 그룹에 메일 목록 기능을 추가하려면 사용자 디렉토리에서 적절한 그룹에 액세스한 다음 해당 메일 계정 속성을 추가 또는 수정합니다.

기존 그룹에 대한 메일 목록 정보에 액세스하려면 다음을 수행합니다.

1. 콘솔 주 창에서 사용자 및 그룹 탭을 누릅니다.
2. 사용자 및 그룹 주 창에서 검색 또는 고급 검색을 누릅니다.
3. 검색 창에서 검색 조건(그룹 이름 등)을 입력하고 사용자 디렉토리 검색을 수행합니다.
4. 사용자 및 그룹 주 창으로 돌아가 검색 결과에서 그룹을 선택하고 편집을 누릅니다.
5. 항목 편집 창에 메일 탭이 표시되지 않는 경우 다음을 수행합니다.

- 계정 탭을 누릅니다. 오른쪽 창에 설치된 계정 목록이 나타납니다.
  - 메일 계정 상자를 선택합니다. 항목 편집 창에 메일 탭이 표시됩니다.
6. 항목 편집 창에서 메일 탭을 누른 다음 오른쪽 창에서 원하는 탭을 누릅니다.  
이 탭은 그룹 만들기 창을 통해 액세스한 탭과 동일합니다.
7. 변경 사항을 입력한 다음 항목 편집 창의 맨 아래에서 확인을 눌러 수정 사항을 제출합니다.

## 메일 목록 설정 지정

메일이 성공적으로 메일 목록에 전달되려면 해당 메일 주소 지정 정보를 지정해야 합니다. 이는 그룹에 대한 주 주소와 주 주소의 별칭으로 허용하는 대체 주소로 구성됩니다. 또한 메일 목록의 목록 소유자, 선택적 설명 정보, 구성원, 속성, 제한 사항 및 작업(전자 메일 응답)도 지정할 수 있습니다.

메일 목록 정보를 지정하려면 다음을 수행합니다.

1. 콘솔에서 [856페이지](#)의 "메일 목록 액세스"에 설명된 대로 그룹 만들기 또는 항목 편집 창에 액세스합니다.
2. 메일 탭을 누릅니다.
3. 이미 활성화되어 있지 않은 경우 설정 탭을 누릅니다.
4. (필수 사항) 메일 목록의 주 전자 메일 주소를 입력합니다.  
이 목록의 메일이 전달되는 공용 주소입니다. 하나의 목록은 하나의 주 주소만 가질 수 있습니다. 주 주소는 RFC 821 사양에 맞는 정확한 형식의 SMTP 주소여야 합니다.
5. (선택 사항) 메일 목록에 대한 대체 주소를 지정합니다.  
대체 주소는 그룹의 주 주소에 대한 별칭입니다. 이 기능을 사용하여 다음을 수행할 수 있습니다.
  - 주소가 잘못된 메일이 올바르게 전달되도록 합니다.

- 보내는 메일 헤더에서 이름 숨기기를 사용 가능하게 합니다. 그러면 호스트 이름을 포함하고 그룹의 주 전자 메일 주소의 호스트 이름을 포함하지 않는 대체 주소를 제공해야 합니다.

각 주소가 고유하다면 그룹에 대한 모든 수의 대체 주소를 지정할 수 있습니다. 이러한 별칭으로 수신되는 메일은 주 주소로 보내집니다.

대체 전자 메일 주소를 추가하려면 다음을 수행합니다.

- a. 대체 전자 메일 주소 필드 아래에 있는 추가 버튼을 누릅니다.
  - b. 대체 전자 메일 주소 창에서 대체 주소를 입력합니다. 원하는 개수만큼 대체 주소를 추가할 수 있지만 이 창을 열 때마다 하나의 주소만 입력할 수 있습니다.
  - c. 확인을 눌러 대체 주소를 추가하고 대체 전자 메일 주소 창을 닫습니다. 다른 대체 주소를 입력하려면 추가를 다시 눌러 대체 전자 메일 주소 창을 다시 엽니다.
6. (선택 사항) "오류" 필드에서 목록에 게시된 오류 전달 메일을 보낼 사람의 전자 메일 주소를 입력합니다.

7. (선택 사항) "Messaging Server 호스트 이름" 필드에서 이 메일 목록을 호스트하는 시스템의 호스트 이름을 입력합니다.

이 메일 목록에 대한 "주 전자 메일 주소" 필드에 호스트 이름이 포함된 경우 이 필드를 비워둡니다. 주 전자 메일 주소의 호스트 이름을 지정하지 않는 방법으로 호스트 이름 숨기기를 구현하는 경우 이 필드에서 호스트 이름을 지정합니다.

사용자 메일 계정과는 달리 메일 목록에 대한 호스트 이름을 지정하지 않으면 목록의 LADP 항목에 액세스할 수 있는 모든 호스트에서 해당 목록을 처리할 수 있습니다(대부분 이를 선호). 하나 이상의 특정 호스트로 해당 목록에 대한 처리를 제한하려면 하나 이상의 호스트 이름을 지정해야 합니다. 예를 들어, 과도하게 사용되는 서버의 스트레스를 줄이기 위해 제대로 활용되지 않는 서버에서 큰 그룹을 처리하도록 할 수 있습니다.

이 창에서는 한번에 하나의 호스트 이름만을 입력할 수 있습니다. 여러 호스트 이름을 입력하려면 `ldapmodify` 명령줄 유틸리티를 사용합니다.

8. (선택 사항) 메일 목록 소유자를 입력합니다.

목록 소유자는 사용자 추가 및 제거, 구성 설정 수정 또는 목록 삭제에 대한 관리 권한을 가지고 있습니다.

새 메일 목록 소유자를 지정하려면 소유자 탭을 누른 후 다음 중 하나를 수행합니다.

- 추가를 누른 다음 목록 소유자 DN 입력 창에서 새 메일 목록 소유자(예: uid=jsmith, ou=people, o=siroe.com)의 고유 이름(DN)을 입력하고 확인을 누릅니다.
- 소유자를 찾으려면 검색을 눌러 사용자 및 그룹 검색 창을 엽니다.

사용자 및 그룹 검색 창에서 소유자를 선택하면 DN의 올바른 구문이 자동적으로 추가됩니다. 사용자 및 그룹 검색 창에 대한 자세한 내용은 *Sun ONE Server Console 5.2 Server Management Guide*의 사용자 및 그룹 관리에 대한 장을 참조하십시오.

**9. (선택 사항) 설명 정보를 추가합니다.**

정보 제공용으로만(Messaging Server에서 사용하지 않음) 텍스트 또는 URL을 추가하려면 설명 탭을 누른 후 다음 옵션 중 하나 또는 둘 다를 사용합니다.

- 용도에 대한 설명 또는 메일 목록의 특성을 입력합니다.
- HTML 페이지에서 URL을 입력하여 메일 목록에 대한 추가 정보를 제공합니다. 정보 제공을 위해서만 사용되며 Messaging Server에서 해당 URL을 사용하지 않습니다.

**10. 이 메일 목록 변경을 완료했다면 항목 편집 창 맨 아래에서 확인을 누릅니다. 그렇지 않으면 다른 탭을 눌러서 변경 작업을 계속합니다.**

## 목록 구성원 지정

메일 목록에 전자 메일 전용 구성원을 추가하려면 다음 방법 중 하나 또는 둘 다를 사용합니다.

- 메일 목록에 각 구성원을 명시적으로 추가합니다.
- 그룹 멤버십을 결정하는 필터로 사용자 디렉토리에 적용될 동적 조건을 정의합니다.

여기에 설명된 구성원은 그룹의 메일 목록 요소가 제공하는 제한된 그룹 권한을 가지고 있기 때문에 콘솔의 사용자 및 그룹 인터페이스에서 *전자 메일 전용 구성원*이라고 합니다. 인터페이스(*Sun ONE Server Console 5.2 Server Management Guide*의 사용자 및 그룹 관리에 대한 장 참조)의 다른 부분을 사용하여 추가되는 "일반" 그룹 구성원은 해당 메일 목록 구성원 이상의 추가 권한 또는 책임을 가질 수 있습니다. 그룹에 대한 자세한 내용은 *Sun ONE Server Console 5.2 Server Management Guide*의 사용자 및 그룹 관리에 대한 장을 참조하십시오.

## 동적 멤버십 기준 정의

동적 요소는 멤버십을 결정하는 사용자 디렉토리 검색의 필터로 사용되는 LDAP 검색 URL로 구성됩니다. 이 기법은 그룹에 도착한 메일을 받을 개인을 이름의 정적 목록에 문의하지 않고 디렉토리 검색으로 결정하기 때문에 동적입니다. 따라서 각 구성원을 명시적으로 추적하지 않고도 상당히 크거나 복잡한 그룹을 만들고 유지할 수 있습니다.

LDAP 검색 필터의 형식은 LDAP URL 구문에서 지정되어야 합니다. LDAP 필터 구성에 대한 자세한 내용은 *Sun ONE Server Console 5.2 Server Management Guide*의 사용자 및 그룹 관리에 대한 장을 참조하십시오. 또한 Sun Java System Directory Server 설명서 및 RFC 1959를 참조하십시오.

LDAP URL의 구문은 다음과 같습니다.

```
ldap://hostname:port/base_dn?attributes?scope?filter
```

여기서 URL의 옵션은 다음과 같이 정의됩니다.

**표 C-1** LDAP URL 옵션

| 옵션                | 설명                                                                                                                                                                                            |
|-------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>hostname</i>   | Directory Server의 호스트 이름(Messaging Server가 사용하는 기본 Directory Server 호스트 이름)입니다.                                                                                                               |
| <i>port</i>       | LADP 서버에 대한 포트 번호입니다. 포트를 지정하지 않으면 Messaging Server가 사용하는 표준 LDAP 포트 기본값으로 지정됩니다.                                                                                                             |
| <i>base_dn</i>    | 검색 기준으로 사용될 디렉토리 항목의 고유 이름입니다. 이 구성 요소는 필수입니다.                                                                                                                                                |
| <i>attributes</i> | 반환되는 속성입니다. 이 속성은 Messaging Server가 제공합니다.                                                                                                                                                    |
| <i>scope</i>      | 검색 범위는 다음과 같습니다.<br><br>base의 범위는 검색 기준( <i>base_dn</i> ) 자체로만 정보를 검색합니다.<br><br>one의 범위는 한 수준 아래의 검색 기준으로 정보를 검색합니다(검색 기준 수준은 포함되지 않음).<br><br>sub의 범위는 검색 기준 및 검색 기준 아래의 모든 항목으로 정보를 검색합니다. |
| <i>filter</i>     | 검색의 지정된 범위 내에 있는 항목에 적용될 검색 필터입니다. 필터가 지정되지 않은 경우 (objectclass=*)가 사용됩니다.                                                                                                                     |

다음은 메일 호스트가 Sunnyvale인 사용자를 필터링하는 LDAP 검색 URL의 예입니다.

```
ldap:///o=Siroe Corp,c=US??sub?(&(mailHost=sunnyvale.siroe.com)
(objectClass=inetLocalMailRecipient))
```

위 URL은 미국(c=US)에 있는 Siroe 조직(o=Siroe)의 구성원이고 메일 호스트가 Sunnyvale(mailHost=sunnyvale)인 사용자를 필터링합니다. objectClass 속성은 검색할 항목의 유형을 정의합니다. 이 경우 inetLocalMailRecipient (objectClass=inetLocalMailRecipient)입니다.

콘솔을 사용하여 검색 필터를 만드는 경우 모든 그룹 이름은 무시됩니다. 즉, 아이디만 검색 결과에 포함되고 그룹 구성원은 포함되지 않습니다. 이 설정의 목적은 검색 결과에 그룹의 구성원이기도 한 사용자가 중복되는 것을 방지하기 위해서입니다. 이 설정은 명령줄 구성 유틸리티(configutil)를 사용하여 무시할 수는 있지만 권장되지 않습니다.

다음 절에 설명된 대로 콘솔은 검색 URL 구성에 사용할 수 있는 템플릿 창(LDAP 검색 URL 창)을 제공합니다.

## 메일 목록 구성원 추가

메일 목록에 구성원(전자 메일 전용)을 추가하려면 다음을 수행합니다.

1. 콘솔에서 [856페이지](#)의 "메일 목록 액세스"에 설명된 대로 그룹 만들기 또는 항목 편집 창에 액세스합니다.
2. 메일 탭을 누릅니다.
3. 전자 메일 전용 구성원 탭을 누릅니다.
  - (선택 사항) 멤버십을 결정하는 LDAP 검색 URL을 지정하려면 "전자 메일 전용 구성원의 동적 기준" 필드 아래에 있는 추가 버튼을 누른 다음 동적 기준 추가 창에서 다음을 수행합니다.
  - 필드에서 LDAP 검색 URL을 입력하거나 구성 버튼을 눌러 검색 URL 검색의 구성을 돕는 템플릿인 LDAP 검색 URL 구성 창을 엽니다.
  - 확인을 눌러 "전자 메일 전용 멤버십에 대한 동적 기준" 필드에 항목을 추가하고 동적 기준 추가 창을 닫습니다.

LDAP 검색 URL 만들기에 대한 지침은 [861페이지](#)의 "동적 멤버십 기준 정의"를 참조하십시오.

4. (선택 사항) 메일 목록에 개별 구성원을 추가하려면 "전자 메일 전용 멤버십이 있는 구성원" 필드에서 추가 버튼을 누른 다음 전자 메일 전용 구성원 추가 창에서 다음을 수행합니다.

- 필드에서 새 구성원에 대한 주 주소를 입력합니다. 주 주소는 RFC 821 양식에 맞는 정확한 형식의 SMTP 주소여야 합니다. 특히 그룹에 대한 제한을 지정하는 경우에는 대체 주소를 입력하지 않아야 합니다. 이 창을 열 때마다 하나의 구성원만 추가할 수 있습니다. 이 필드에는 둘 이상의 주소를 보관할 수 없습니다.
  - 확인을 눌러 멤버십 목록에 사용자를 추가하고 전자 메일 전용 구성원 추가 창을 닫습니다. 다른 주소를 입력하려면 추가를 다시 눌러 전자 메일 전용 구성원 추가 창을 다시 엽니다.
5. 이 메일 목록 변경을 완료했으면 항목 편집 창 맨 아래에서 확인을 누릅니다. 그렇지 않으면 다른 탭을 눌러서 변경 작업을 계속합니다.

## 메일 게시 제한 정의

메일 목록에 보내는 메일에 대해 여러 종류의 제한을 부과할 수 있습니다. 메일을 게시할 수 있는 사용자 집합 정의, 보낸 사람의 인증 요구, 게시된 메일의 출처 제한 및 게시된 메일의 크기를 제한할 수 있습니다. 제한을 위반하는 메일은 거부됩니다.

---

**주** 이러한 제한은 그룹이 받는 메일의 여러 사항을 제어하는데 유용하지만 고급 보안 액세스 제어용은 아닙니다.

---

그룹에 대한 메일 게시 제한을 정의하려면 다음을 수행합니다.

1. 콘솔에서 **856페이지**의 "**메일 목록 액세스**"에 설명된 대로 그룹 만들기 또는 항목 편집 창에 액세스합니다.
2. 메일 탭을 누릅니다.
3. 제한 탭을 누릅니다.
4. (선택 사항) 다음 옵션 중 하나를 선택하여 허용된 보낸 사람을 정의합니다.
  - **모든 사용자:** 보낸 사람에 대한 제한이 없습니다. 기본값입니다. 이 옵션을 선택하면 다음 단계에 설명된 SMTP 인증을 선택할 수 없습니다.
  - **메일 목록에 있는 모든 사용자:** 메일 목록 구성원(전자 메일 전용 구성원이 아닌 그룹 구성원 포함)만 메일을 게시할 수 있습니다.

- **다음 목록에 있는 모든 사용자:** 다음 필드에 명시적으로 나열된 사용자만 메일을 게시할 수 있습니다.

"다음 목록에 있는 모든 사용자"를 선택한 경우 보낸 사람을 추가하려면 허용된 보낸 사람 필드 아래에 있는 추가를 누르거나 검색을 눌러 사용자 및 그룹 검색 창을 열 수 있습니다. 추가를 누르면 허용된 보낸 사람 추가 창이 열립니다. 허용된 보낸 사람의 전자 메일 주소 또는 고유 이름(DN)을 필드에 입력합니다. 확인을 눌러 허용된 보낸 사람 필드에 보낸 사람을 추가하고 허용된 보낸 사람 추가 창을 닫습니다. 추가하려는 다른 모든 허용된 보낸 사람에 대해 이 단계를 반복합니다.

사용자 및 그룹 검색 창에 대한 자세한 내용은 *Sun ONE Server Console 5.2 Server Management Guide*의 사용자 및 그룹 관리에 대한 장을 참조하십시오.

5. (선택 사항) 허용된 보낸 사람 도메인을 정의하여 보낸 사람이 게시할 수 있는 메일의 출처를 제한하려면 다음을 수행합니다.
  - 허용된 보낸 사람 도메인 필드 아래에서 추가 버튼을 누릅니다.
  - 허용된 보낸 사람 도메인 추가 창에서 도메인 이름을 입력한 다음 확인을 눌러 목록에 도메인을 추가합니다.

도메인은 자동적으로 모든 해당 하위 도메인을 포함합니다. 예를 들어, `siroe.com`은 `sales.siroe.com`을 포함합니다.

6. (선택 사항) 허용된 메일의 최대 크기를 정의합니다.
 

크기를 입력합니다(바이트).
7. 이 메일 목록 변경을 완료했으면 항목 편집 창 맨 아래에서 확인을 누릅니다. 그렇지 않으면 다른 탭을 눌러서 변경 작업을 계속합니다.

## 중재자 정의

메일 목록에 대해 하나 이상의 중재자를 추가할 수 있습니다.

중재자가 전달된 메일을 받는 경우 해당 중재자가 메일 처리 방법을 결정합니다. 여러 중재자가 있는 경우에는 첫 번째 중재자가 수행한 작업에 따라 메일 처리 방법이 결정됩니다. 해당 처리에는 메일을 승인하고 이를 목록(비밀번호가 있을 수 있음)으로 다시 전달하거나 삭제하는 것이 포함될 수 있습니다.

메일 목록에 대한 중재자를 정의하려면 다음을 수행합니다.



1. 콘솔에서 [856페이지](#)의 "메일 목록 액세스"에 설명된 대로 그룹 만들기 또는 항목 편집 창에 액세스합니다.
2. 메일 탭을 누릅니다.
3. 중재자 탭을 누릅니다.
4. 중재자 목록 필드 아래에서 추가 버튼을 누릅니다.
5. 중재자 추가 창에서 중재자의 주 전자 메일 주소를 입력하거나 필드에 고유 이름 (DN)을 입력합니다. 주소를 찾기 위해 명시적으로 주소를 입력하거나 검색을 눌러 사용자 및 그룹 검색 창을 사용할 수 있습니다. 중재자 추가 창을 열 때마다 하나의 중재자만 입력할 수 있습니다.

사용자 및 그룹 검색 창에 대한 자세한 내용은 *Sun ONE Server Console 5.2 Server Management Guide*의 사용자 및 그룹 관리에 대한 장을 참조하십시오.

6. 확인을 눌러 중재자 목록에 중재자를 추가하고 중재자 추가 창을 닫습니다. 다른 주소를 입력하려면 추가를 다시 눌러 중재자 추가 창을 다시 엽니다.
7. 이 메일 목록 변경을 완료했다면 항목 편집 창 맨 아래에서 확인을 누릅니다. 그렇지 않으면 다른 탭을 눌러서 변경 작업을 계속합니다.



# SMS(Short Message Service)

이 장에서는 Sun™ ONE Messaging Server에서 SMS(Short Message Service)를 구현하는 방법에 대해 설명합니다. 이 장은 다음 내용으로 구성되어 있습니다.

- 867페이지의 "소개"
- 870페이지의 "SMS 채널 작동 원리"
- 886페이지의 "SMS 채널 구성"
- 915페이지의 "SMS 게이트웨이 서버 작동 이론"
- 920페이지의 "SMS 게이트웨이 서버 구성"
- 944페이지의 "SMS 게이트웨이 서버 저장소 요구 사항"

## 소개

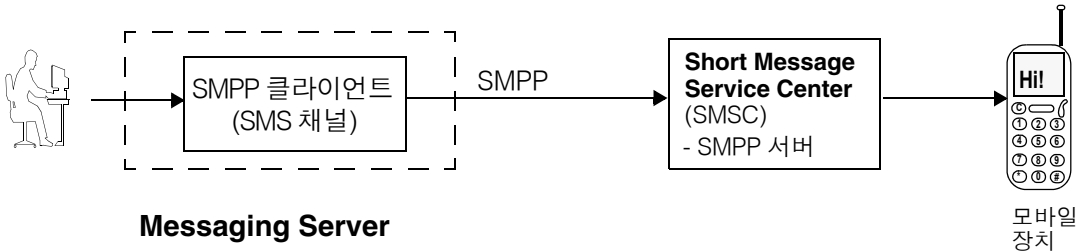
Sun Java System Messaging Server는 SMS(Short Message Service)를 사용하여 ETM(Email-To-Mobile) 및 MTE(Mobile-To-Email) 메시징을 구현합니다. SMS는 단방향(ETM만 해당) 또는 양방향(ETM 및 MTE 모두)이 되도록 구성할 수 있습니다. 단방향 서비스만 사용하려면 SMS 채널을 추가 및 구성해야 합니다. 양방향 서비스를 사용하려면 SMS 채널을 추가 및 구성하는 것 외에도 SMS 게이트웨이 서버를 구성해야 합니다.

단방향 및 양방향 SMS의 경우 생성된 SMS 메일은 SMPP(Short Message Peer to Peer) 프로토콜을 사용하여 SMSC(Short Message Service Center)로 전송됩니다. 특히 SMSC는 TCP/IP를 지원하는 V3.4 이상의 SMPP 서버를 제공해야 합니다.

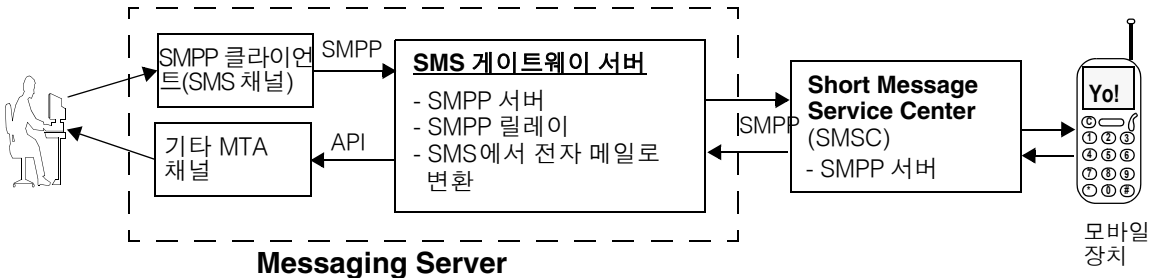
**그림 D-1**은 단방향 및 양방향 SMS의 논리적 메일 흐름을 보여 줍니다.

그림 D-1 단방향 및 양방향 SMS의 논리적 흐름

**단방향 SMS**



**양방향 SMS**



**단방향 SMS**

단방향 서비스를 사용하기 위해 Messaging Server는 원격 SMSC와 통신하는 SMPP 클라이언트(MTA SMS 채널)를 구현합니다. SMS 채널은 872페이지의 "전자 메일에서 SMS로의 변환 프로세스"에 설명된 대로 대기열에 포함된 전자 메일을 SMS 메일로 변환합니다. 이 변환 프로세스는 문자 세트 변환 문제와 멀티파트 MIME 메일 처리를 포함합니다.

SMS 채널은 이러한 방식으로 작동하여(SMPP) ESME(External Short Message Entity)의 기능을 수행합니다.

## 양방향 SMS

양방향 SMS를 사용하여 메일 서버에서 원격 장치로 전자 메일을 보낼 뿐만 아니라 원격 장치로부터 그리고 원격 장치가 보낸 메일 응답을 받을 수 있습니다.

양방향 SMS 서비스를 사용하려면 이전 항목에 설명된 MTA SMS 채널(SMPP 클라이언트)과 SMS 게이트웨이 서버가 모두 필요합니다. Sun Java System Messaging Server는 일반 설치 프로세스의 일부로 SMS 게이트웨이 서버를 설치하며 사용자는 이 서버를 구성해야 합니다. SMS 게이트웨이 서버는 다음 두 가지 기능을 수행합니다.

- SMPP 릴레이

SMS 게이트웨이 서버는 MTA SMS 채널과 SMSC 간의 투명한 SMPP 클라이언트 역할을 수행합니다. SMS 게이트웨이 서버는 또한 릴레이 역할을 수행하면서 릴레이된 메일에 대한 고유한 SMS 주소를 생성하고 원격 SMSC에 의해 반환된 메일 아이디를 저장하여 나중에 SMS 알림 메일과 상호 작용시킵니다.

- SMPP 서버

SMS 게이트웨이 서버는 모바일에서 전송된 SMS 메일, 이전 전자 메일에 대한 응답 및 SMS 알림을 받기 위한 SMTP 서버의 역할을 수행합니다. SMS 게이트웨이 서버는 변환 프로세스를 정의하는 프로필을 사용하여 SMS 메일에서 대상 전자 메일 주소를 추출합니다. 프로필은 또한 이전에 보낸 ETM(Email-To-Mobile) 메일에 응답하여 원격 SMSC가 반환한 알림 메일을 처리하는 방법을 설명합니다.

---

**주** Sun Java System Messaging Server는 Windows 플랫폼에서 양방향 SMS를 지원하지 않습니다.

---

## 요구 사항

이 설명서는 LogicaCMG의 SMPP 사양과 사용자 SMSC용 SMPP 설명서를 읽은 것으로 가정합니다.

SMS를 구현하려면 다음 요구 사항을 충족해야 합니다.

- Sun Java System Messaging Server 6 이상(단방향 SMS는 iPlanet Messaging Server 5.2에서도 구현됩니다.)
- SMSC는 TCP/IP를 통해 SMPP V3.4 이상을 지원해야 하며 Messaging Server를 실행하는 호스트와 SMSC 간에 TCP/IP 연결이 존재해야 합니다.

SMS 게이트웨이 서버에 대한 저장소 계획 정보는 944페이지의 "SMS 게이트웨이 서버 저장소 요구 사항"을 참조하십시오.

## SMS 채널 작동 원리

SMS 채널은 대기 중인 전자 메일을 SMS 메일로 변환한 다음 전달을 위해 SMSC에 전송하는 멀티스레드 채널입니다.

이 절은 다음과 같은 채널 작업 항목으로 구성되어 있습니다.

- 870페이지의 "전자 메일을 채널로 전송"
- 872페이지의 "전자 메일에서 SMS로의 변환 프로세스"
- 876페이지의 "SMS 메일 전송 프로세스"
- 880페이지의 "사이트 정의 주소 유효성 검사 및 변환"
- 881페이지의 "사이트 정의 텍스트 변환"

## 전자 메일을 채널로 전송

886페이지의 "SMS 채널 구성"으로 SMS 채널이 구성되면 하나 이상의 호스트 이름이 해당 채널과 연관됩니다. 여기서는 설명을 위해 호스트 이름 sms.siroe.com을 채널과 연관된 호스트 이름으로 가정합니다. 이 경우 전자 메일은 다음 형식의 주소를 가진 채널로 전송됩니다.

```
local-part@sms.siroe.com
```

여기서 local-part는 SMS 대상 주소(예: 휴대폰 번호, 호출기 아이디 등) 또는 다음 형식의 속성 값 쌍 목록입니다.

```
/attribute1=value1/attribute2=value2/.../@sms.siroe.com
```

인식되는 속성 이름과 그 사용법은 표 D-1에 나와 있습니다. 이러한 속성은 일부 채널 옵션에 대한 수신자별 제어를 허용합니다.

**표 D-1** SMS 속성

| 속성 이름 | 속성 값 및 사용법                                                                |
|-------|---------------------------------------------------------------------------|
| ID    | SMS 메일을 전송할 SMS 대상 주소(예: 휴대폰 번호, 호출기 아이디 등)입니다. 이 속성과 관련 값은 반드시 존재해야 합니다. |
| FROM  | SMS 소스 주소입니다. 옵션 USE_HEADER_FROM=0일 경우 무시됩니다.                             |

표 D-1 SMS 속성

| 속성 이름    | 속성 값 및 사용법                                                                                                                                                                                                    |
|----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| FROM_NPI | <b>NPI</b> . 지정된 NPI 값을 사용합니다. 옵션 USE_HEADER_FROM=0일 경우 무시됩니다.                                                                                                                                                |
| FROM_TON | <b>TON</b> . 지정된 TON 값을 사용합니다. 옵션 USE_HEADER_FROM=0일 경우 무시됩니다.                                                                                                                                                |
| MAXLEN   | 해당 수신자에 대해 생성된 SMS 메일에 포함할 최대 총 바이트(즉, 8비트 바이트)입니다. MAXLEN과 <b>MAX_MESSAGE_SIZE</b> 채널 옵션에 지정된 값 중에서 작은 값이 사용됩니다.                                                                                             |
| MAXPAGES | 해당 수신자에 대해 전자 메일을 분할할 최대 SMS 메일 수입니다. MAXPAGES와 <b>MAX_PAGES_PER_MESSAGE</b> 채널 옵션에 지정된 값 중에서 작은 값이 사용됩니다.                                                                                                    |
| NPI      | ID 속성으로 지정된 대상 SMS 주소에 대한 NPI(Numeric Plan Indicator) 값을 지정합니다. 이 속성에 허용되는 값에 대한 자세한 내용은 <b>DEFAULT_DESTINATION_NPI</b> 채널 옵션의 설명을 참조하십시오. 이 속성을 사용할 경우 이 속성 값은 DEFAULT_DESTINATION_NPI 채널 옵션이 제공한 값보다 우선합니다. |
| PAGELEN  | 해당 수신자에 대해 단일 SMS 메일에 포함할 최대 바이트 수입니다. 이 값과 <b>MAX_PAGE_SIZE</b> 채널 옵션에 지정된 값 중에서 최소값이 사용됩니다.                                                                                                                 |
| TO       | <b>ID</b> 의 동의어입니다.                                                                                                                                                                                           |
| TO_NPI   | <b>NPI</b> 의 동의어입니다.                                                                                                                                                                                          |
| TO_TON   | <b>TON</b> 의 동의어입니다.                                                                                                                                                                                          |
| TON      | ID 속성으로 지정된 대상 SMS 주소에 대한 TON(Type of Number) 값을 지정합니다. 이 속성에 허용되는 값에 대한 자세한 내용은 <b>DEFAULT_DESTINATION_TON</b> 채널 옵션의 설명을 참조하십시오. 이 속성을 사용할 경우 이 속성 값은 DEFAULT_DESTINATION_TON 채널 옵션이 제공한 값보다 우선합니다.         |

다음은 몇 가지 주소 예입니다.

```
123456@sms.siroe.com
/id=123456/@sms.siroe.com
/id=123456/maxlen=100/@sms.siroe.com
/id=123456/maxpages=1/@sms.siroe.com
```

전자 메일 주소의 SMS 대상 주소 부분에 대해 변환, 유효성 검사 및 기타 작업을 수행하는 방법은 880페이지의 "[사이트 정의 주소 유효성 검사 및 변환](#)"을 참조하십시오.

## 전자 메일에서 SMS로의 변환 프로세스

전자 메일을 원격 사이트로 보내려면 전자 메일을 원격 SMSC가 이해할 수 있는 SMS 메일로 변환해야 합니다. 이 절에서는 SMS 채널의 대기열에 포함된 전자 메일을 하나 이상의 SMS 메일로 변환하는 과정에 대해 설명합니다. 아래에 설명된 것처럼 옵션을 사용하여 생성되는 SMS 메일의 최대 개수, 이러한 SMS 메일의 최대 총 길이, 모든 단일 SMS 메일의 최대 크기를 제어할 수 있습니다. 전자 메일의 텍스트 부분(즉, MIME 텍스트 콘텐츠 유형)만 사용되며 변환되는 부분의 최대 개수를 제어할 수도 있습니다.

전자 메일의 헤더 행과 텍스트 부분에 사용된 문자 세트는 모두 유니코드로 변환된 다음 적절한 SMS 문자 세트로 변환됩니다.

SMS\_TEXT 매핑 테이블(881페이지의 "사이트 정의 텍스트 변환" 참조)이 없을 경우 SMS 채널의 대기열에 포함된 전자 메일은 그림 D-2에 설명된 처리를 거칩니다.



그림 D-2 SMS 채널 전자 메일 처리

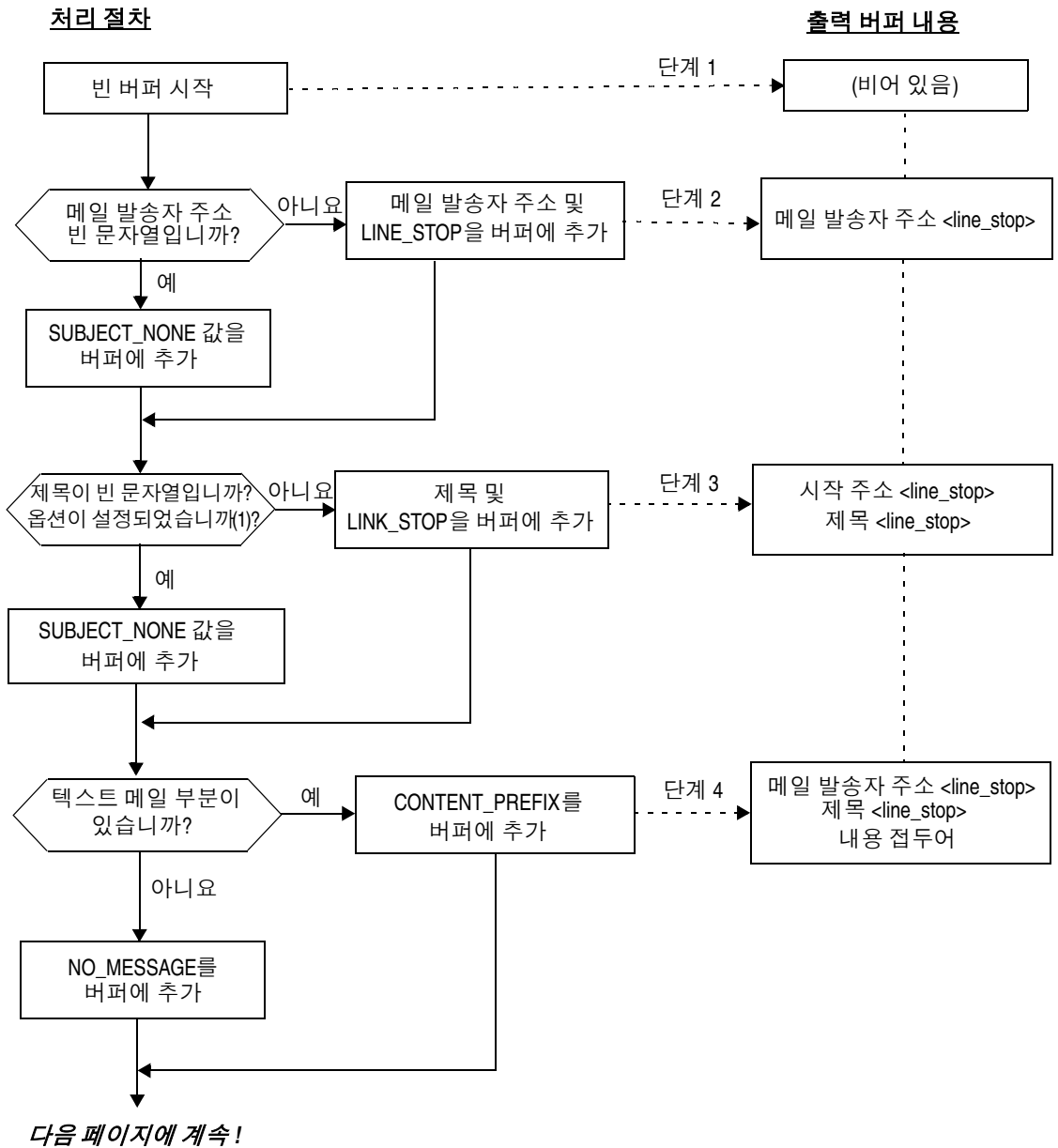
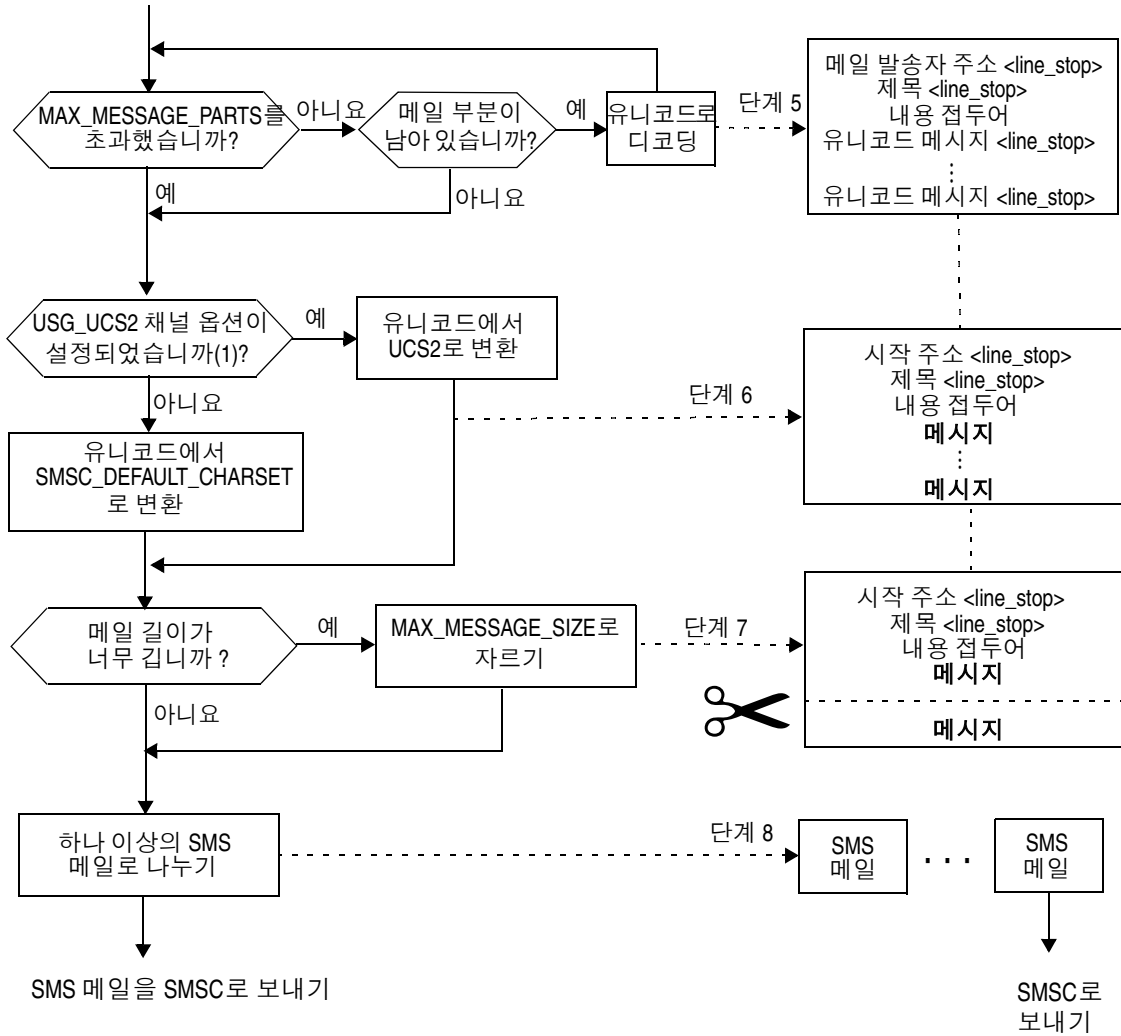


그림 D-3 SMS 채널 전자 메일 처리(계속)

이전 페이지에서 계속!



다음 단계는 번호가 매겨진 그림 D-2의 상자에 해당합니다.

1. 빈 출력 버퍼가 시작됩니다. 버퍼에 사용되는 문자 세트는 유니코드입니다.

2. 전자 메일 발송자 주소를 선호하는 순서로 내림차순으로 나열한 다음 5개의 소스 중 하나에서 가져옵니다.

1. Resent-from:
2. From:
3. Resent-sender:
4. Sender:
5. Envelope From:

메일 발송자 주소가 빈 문자열일 경우 `FROM_NONE` 채널 옵션 값이 대신 버퍼에 추가됩니다.

그러나 메일 발송자 주소가 빈 문자열이 아닐 경우 `FROM_FORMAT` 채널 옵션의 처리 결과와 `LINE_STOP` 채널 옵션 값이 출력 버퍼에 추가됩니다.

Resent-from: 및 Resent-sender: 헤더 행은 `USE_HEADER_RESENT` 옵션 값이 1인 경우에만 고려됩니다. 그렇지 않으면 Resent- 헤더 행은 무시됩니다.

3. Subject: 헤더 행이 존재하지 않거나 비어 있을 경우 `SUBJECT_NONE` 옵션 값이 출력 버퍼에 추가됩니다.

그렇지 않을 경우 `SUBJECT_FORMAT` 옵션의 처리 결과와 `LINE_STOP` 채널 옵션 값이 출력 버퍼에 추가됩니다.

4. 텍스트 메일 부분이 없을 경우 `NO_MESSAGE` 채널 옵션 값이 출력 버퍼에 추가됩니다. 텍스트 메일 부분이 있을 경우 `CONTENT_PREFIX` 채널 옵션 값이 출력 버퍼에 추가됩니다.

텍스트 메일 부분이 아닌 부분은 무시됩니다.

5. 각 텍스트 부분에 대해 `MAX_MESSAGE_PARTS` 한도에 도달하지 않은 동안에 텍스트 부분은 유니코드로 디코딩되고 `LINE_STOP` 채널 옵션 값과 함께 버퍼에 추가됩니다.
6. 그런 다음 결과 출력 버퍼는 유니코드에서 SMSC의 기본 문자 세트 또는 UCS2(UTF-16)로 변환됩니다. SMSC의 기본 문자 세트는 `SMSC_DEFAULT_CHARSET` 옵션으로 지정합니다.
7. 변환된 문자열은 `MAX_MESSAGE_SIZE` 바이트를 초과하지 않도록 잘립니다.

8. 단계 6에서 변환된 문자열은 하나 이상의 SMS 메일로 나뉘며 하나의 SMS 메일은 MAX\_PAGE\_SIZE 바이트를 초과하지 않습니다. 최대한 MAX\_PAGES\_PER\_MESSAGE에 지정된 수만큼 SMS 메일이 생성됩니다.

---

주 전자 메일이 여러 수신자를 가질 수 있으므로 4페이지의 "전자 메일을 채널로 전송"에 설명된 MAXLEN, MAXPAGES 또는 PAGELEN 속성을 사용하는 각 수신자 주소에 대해 단계 6에서 단계 8까지 수행해야 할 수 있습니다.

---

## 샘플 전자 메일 처리

예를 들어, 채널의 기본 설정을 가진 전자 메일은 다음과 같습니다.

```
From: John Doe
To: 1234567@sms.siroe.com
Subject: Today's meeting
Date: Fri, 26 March 2001 08:17
```

The staff meeting is at 14:30 today in the big conference room.

다음 SMS 메일로 변환됩니다.

```
jdoe@siroe.com(Today's meeting) The staff meeting is at 14:30 today in the
big conference room.
```

다음과 같이 일련의 옵션 집합 설정이 다른 경우에는

```
CONTENT_PREFIX=Msg:
FROM_FORMAT=From:${pa}
SUBJECT_FORMAT=Subj:${s}
```

다음 결과가 생성됩니다.

```
From:John Doe Subj:Today's meeting Msg:The staff meeting is at 14:30 today
in the big conference room.
```

## SMS 메일 전송 프로세스

전자 메일이 하나 이상의 SMS 메일로 변환된 후(각 수신자에 대해 다른 집합을 가질 수 있음) SMS 메일은 대상 SMSC로 전송됩니다. 이러한 전송은 TCP/IP를 통한 SMPP V3.4를 사용하여 수행됩니다. SMS 채널과 연관된 공식 호스트 이름으로 사용하기 위해 SMPP 서버의 호스트 이름(SMPP\_SERVER)을 가져오며 사용할 TCP 포트(SMPP\_PORT)가 port 채널 키워드를 통해 지정됩니다.

처리할 메일이 있으면 채널이 시작됩니다. 채널은 송신기로서 SMPP 서버에 바인드하여 904페이지의 "SMPP 옵션"에 설명된 ESME\_ 채널 옵션으로 지정한 자격 증명을 제공합니다. 표 D-2에는 BIND\_TRANSMITTER PDU(Protocol Data Unit)에서 설정되는 필드와 해당 값이 나열되어 있습니다.

**표 D-2** BIND\_TRANSMITTER PDU에서 생성되는 필드

| 필드                | 값                                                 |
|-------------------|---------------------------------------------------|
| system_id         | ESME_SYSTEM_ID 채널 옵션이며 기본값은 빈 문자열입니다.             |
| password          | ESME_PASSWORD 채널 옵션이며 기본값은 빈 문자열입니다.              |
| system_type       | ESME_SYSTEM_TYPE 채널 옵션이며 기본값은 빈 문자열입니다.           |
| interface_version | SMPP V3.4를 나타내는 0x34입니다.                          |
| addr_ton          | ESME_ADDRESS_TON이며 기본값은 알 수 없는 TON을 나타내는 0x00입니다. |
| addr_npi          | ESME_ADDRESS_NPI이며 기본값은 알 수 없는 NPI를 나타내는 0x00입니다. |
| addr_range        | ESME_IP_ADDRESS 채널 옵션이며 기본값은 빈 문자열입니다.            |

채널이 다중 스레드되는 점에 주의하십시오. 보낸 메일의 수에 따라 대기열에서 제외 스레드가 채널에서 여러 개 실행 중일 수 있습니다. (여러 채널 프로세스가 실행 중일 수도 있습니다.) 각 스레드는 BIND\_TRANSMITTER를 수행한 후 해당 TCP/IP 연결에서 전송해야 할 모든 SMS 메일을 보낸 다음 UNBIND를 보내고 연결을 닫습니다. 잠재적 재사용을 위해 유희 기간 동안 연결을 열어두려는 시도는 수행되지 않습니다. 원격 SMPP 서버가 스로틀(throttle) 오류를 되돌려 보낸 경우 UNBIND가 실행되고 TCP/IP 연결이 닫힌 후에 새 연결과 BIND가 설정됩니다. 원격 SMPP 서버가 SMS 메일 전송이 끝나기 전에 UNBIND를 보낸 경우에도 비슷한 동작이 발생합니다.

그런 다음 SMPP SUBMIT\_SM PDU가 사용되어 SMS 메일을 제출합니다. 영구 오류(예: ESME\_RINVDSTADR)가 반환될 경우 전자 메일은 전달할 수 없는 것으로 반환됩니다. 임시 오류가 반환될 경우 전자 메일은 나중에 전달을 시도하기 위해 다시 대기열에 포함됩니다. 영구 오류는 SMS 대상 주소가 잘못된 경우처럼 특정 조건이 무한정 존재하며 반복된 전달 시도가 실제적인 효과가 없는 오류를 말합니다. 이와 달리 임시 오류는 서버 다운이나 서버 정체와 같이 특정 조건이 머지 않아 없어질 것으로 보이는 오류입니다.

USE\_HEADER\_FROM 옵션 값이 1일 경우 제출된 SMS 메일의 소스 주소가 설정됩니다. 사용되는 값은 원본 전자 메일에서 파생되며 모든 응답을 전송해야 할 가장 가능성 있는 (전자 메일) 주소가 선택됩니다. 이에 따라 선호하는 순서로 내림차순으로 나열한 다음 7개의 소스 중 하나에서 소스 주소를 가져옵니다.

1. Resent-reply-to:
2. Resent-from:
3. Reply-to:
4. From:
5. Resent-sender:
6. Sender:
7. Envelope From:

Resent-reply-to: 및 Reply-to: 헤더 행은 [USE\\_HEADER\\_REPLY\\_TO](#) 옵션 값이 1인 경우에만 고려됩니다. Resent-reply-to:, Resent-from: 및 Resent-sender: 헤더 행은 [USE\\_HEADER\\_RESENT](#) 옵션 값이 1인 경우에만 고려됩니다. 이것은 모든 옵션 값이 1이어야 Resent-reply-to: 헤더 행이 고려된다는 의미입니다. 이러한 두 옵션의 기본값은 모두 0입니다. 따라서 4, 6 및 7 항목만 기본 구성에서 고려됩니다. 마지막으로 SMS 메일의 소스 주소가 20바이트로 제한되므로 선택된 소스 주소는 이 제한을 초과할 경우 잘립니다.

[표 D-3](#)은 SUBMIT\_SM PDU에서 설정되는 필수 필드를 보여 줍니다.

**표 D-3** SUBMIT\_SM PDU에서 생성되는 필수 필드

| 필드              | 값                                                                                                                                                                    |
|-----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| service_type    | <a href="#">DEFAULT_SERVICE_TYPE</a> 채널 옵션이며 기본값은 빈 문자열입니다.                                                                                                          |
| source_addr_ton | <a href="#">DEFAULT_SOURCE_TON</a> 채널 옵션이며 <a href="#">USE_HEADER_FROM</a> =1일 경우 이 필드는 일반적으로 영숫자 TON을 나타내는 값 0x05를 가집니다. 그렇지 않을 경우에는 국가별 TON을 나타내는 기본값 0x01이 사용됩니다. |
| source_addr_npi | <a href="#">DEFAULT_SOURCE_NPI</a> 채널 옵션이며 기본값은 0x00입니다.                                                                                                             |
| source_addr     | <a href="#">USE_HEADER_FROM</a> =0일 경우 <a href="#">DEFAULT_SOURCE_ADDRESS</a> 채널 옵션입니다. 그렇지 않을 경우에는 전자 메일 발송자를 나타내는 영숫자 문자열입니다.                                      |
| dest_addr_ton   | TON 주소 지정 속성 또는 <a href="#">DEFAULT_DESTINATION_TON</a> 채널 옵션입니다. 기본값은 국가별 TON을 나타내는 0x01입니다.                                                                        |
| dest_addr_npi   | NPI 주소 지정 속성 또는 <a href="#">DEFAULT_SOURCE_NPI</a> 채널 옵션입니다. 기본값은 알 수 없는 NPI를 나타내는 0x00입니다.                                                                          |
| dest_addr       | 전자 메일 봉투 To: 주소의 로컬 부분에서 파생된 대상 SMS 주소입니다. <a href="#">870 페이지</a> 의 "전자 메일을 채널로 전송"을 참조하십시오.                                                                        |
| esm_class       | 단방향 SMS의 경우 기본 SMSC 메일 유형인 저장 및 전달 모드를 나타내는 0x03으로 설정되며 응답 경로를 설정하지 않습니다. 양방향 SMS 메일의 경우 0x83으로 설정됩니다.                                                               |
| protocol_id     | 0x00이며 CDMA 및 TDMA에 사용되지 않습니다. GSM의 경우 0x00은 인터넷은 연결되어 있지 않지만 SME 간 프로토콜이 있음을 나타냅니다.                                                                                 |
| priority_flag   | GSM 및 CDMA의 경우 0x00이고 TDMA의 경우 0x01입니다. 모두 일반 우선 순위를 나타냅니다. <a href="#">DEFAULT_PRIORITY</a> 채널 옵션에 대한 설명을 참조하십시오.                                                   |

**표 D-3** SUBMIT\_SM PDU에서 생성되는 필수 필드

| 필드                      | 값                                                                                          |
|-------------------------|--------------------------------------------------------------------------------------------|
| schedule_delivery_time  | 즉시 전달을 나타내는 빈 문자열입니다.                                                                      |
| validity_period         | <a href="#">DEFAULT_VALIDITY_PERIOD</a> 채널 옵션이며 기본값은 SMSC의 기본값을 사용해야 한다는 것을 나타내는 빈 문자열입니다. |
| registered_delivery     | 등록된 전달이 없음을 나타내는 0x00입니다.                                                                  |
| replace_if_present_flag | 모든 이전 SMS 메일을 대체해야 한다는 것을 나타내는 0x00입니다.                                                    |
| data_coding             | SMSC 기본 문자 세트의 경우 0x00이며 UCS2 문자 세트의 경우 0x08입니다.                                           |
| sm_default_msg_id       | 미리 정의된 메일을 사용하지 않는다는 것을 나타내는 0x00입니다.                                                      |
| sm_length               | SMS 메일의 길이와 내용입니다. 자세한 내용은 <a href="#">872페이지의 "전자 메일에서 SMS로의 변환 프로세스"</a> 를 참조하십시오.       |
| short_message           | SMS 메일의 길이와 내용입니다. 자세한 내용은 <a href="#">872페이지의 "전자 메일에서 SMS로의 변환 프로세스"</a> 를 참조하십시오.       |

[표 D-4](#)는 SUBMIT\_SM PDU의 선택적 필드를 보여 줍니다.

**표 D-4** SUBMIT\_SM PDU에서 생성되는 선택적 필드

| 필드         | 값                                                                                                                 |
|------------|-------------------------------------------------------------------------------------------------------------------|
| privacy    | <a href="#">DEFAULT_PRIVACY</a> 채널 키워드에 대한 설명을 참조하십시오. 기본값은 전자 메일에 Sensitivity: 헤더 행 값이 없으면 이러한 필드를 제공하지 않는 것입니다. |
| sar_refnum | <a href="#">USE_SAR</a> 채널 키워드에 대한 설명을 참조하십시오. 기본값은 이러한 필드를 제공하지 않는 것입니다.                                         |
| sar_total  | 위의 sar_refnum을 참조하십시오.                                                                                            |
| sar_seqnum | 위의 sar_refnum을 참조하십시오.                                                                                            |

전송할 SMS 메일이 더 이상 없거나(메일 대기열이 비어 있거나) [MAX\\_PAGES\\_PER\\_BIND](#)를 초과할 때까지 채널은 SMPP 서버에 바인드되어 있습니다. 후자의 경우 전송할 추가 SMS 메일이 남아 있으면 새 연결이 설정되고 바인드 작업이 수행됩니다.

SMS 채널이 다중 스레드되는 점에 주의하십시오. 채널의 각 처리 스레드는 SMPP 서버와의 고유한 TCP 연결을 유지 관리합니다. 예를 들어, 각각 전송할 SMS 메일을 가진 세 개의 처리 스레드가 있을 경우 채널은 SMPP 서버에 대한 세 개의 열린 TCP 연결을 가집니다. 각 연결은 송신기로 SMPP 서버에 바인드합니다. 또한 지정된 모든 처리 스레드는 미해결 SMS 전송을 한 번에 하나씩만 가집니다. 즉, 지정된 스레드는 SMS 메일을 전송한 다음 다른 SMS 메일을 전송하기 전에 전송 응답(즉, SUBMIT\_SM\_RESP PDU)을 기다립니다.

## 사이트 정의 주소 유효성 검사 및 변환

사이트는 870페이지의 "전자 메일을 채널로 전송"에 설명된 수신자 전자 메일 주소로 인코딩되는 SMS 대상 주소에 유효성 검사 또는 변환을 적용하려할 수 있습니다. 예를 들어, 사이트에서 다음을 수행할 수 있습니다.

- 숫자가 아닌 문자 스트라이프(예: 800.555.1212를 8005551212로 변환)
- 접두어 추가(예: 8005551212를 +18005551212로 변환)
- 정확성 검증(예: 123은 너무 짧음)

처음 두 개의 작업은 특히 `DESTINATION_ADDRESS_NUMERIC` 및 `DESTINATION_ADDRESS_PREFIX` 채널 옵션으로 수행할 수 있습니다. 일반적으로 이 세 작업 및 기타 작업은 매핑 테이블(다시 쓰기 규칙의 테이블 콜아웃 또는 FORWARD 매핑 테이블)을 사용하여 구현할 수 있습니다. 다시 쓰기 규칙의 매핑 테이블 콜아웃을 사용하면 사이트 정의 오류 응답으로 주소를 거부하는 기능을 비롯하여 가장 뛰어난 유연성이 제공됩니다. 이 절의 나머지 부분에서는 다시 쓰기 규칙의 매핑 테이블 콜아웃을 사용하는 이러한 방식에 대해 설명합니다.

대상 주소가 10 또는 11자리의 숫자로만 되고 문자열 "+1"을 접두어로 붙여야 하는 것으로 가정합니다. 이는 다음 다시 쓰기 규칙을 사용하여 수행할 수 있습니다.

```
sms.siroe.com      ${X-REWRITE-SMS-ADDRESS,$U}@sms.siroe.com
sms.siroe.com      $?Invalid SMS address
```

위에서 첫 번째 다시 쓰기 규칙은 X-REWRITE-SMS-ADDRESS라는 사이트 정의 매핑 테이블로 콜아웃됩니다. 검사를 위해 전자 메일 주소의 로컬 부분이 이 매핑 테이블로 전달됩니다. 매핑 프로세스에서 로컬 부분을 허용할 경우에는 주소가 수락되어 SMS 채널에 다시 기록됩니다. 매핑 프로세스가 로컬 부분을 허용하지 않을 경우에는 다음 다시 쓰기 규칙이 적용됩니다. 다음 다시 쓰기 규칙이 \$? 다시 쓰기 규칙이므로 "Invalid SMS address"라는 오류 텍스트와 함께 주소가 거부됩니다.



아래에는 X-REWRITE-SMS-ADDRESS 매핑 테이블이 나와 있습니다. 이 매핑 테이블은 속성 값 쌍 목록 형식이나 단순히 원시 SMS 대상 주소로 되어 있는 로컬 부분에 대한 필수 검증 단계를 수행합니다.

X-VALIDATE-SMS-ADDRESS

```
! Iteratively strip any non-numeric characters
  $_*[$ -/::~~]* $0$2$R
! Accept the address if it is of the form 1nnnnnnnnnn or nnnnnnnnnn
! In accepting it, ensure that we output +1nnnnnnnnnn
  1%%%%%%%%%      +1$0$1$2$3$4$5$6$7$8$9$Y
  %%%%%%%%%%      +1$0$1$2$3$4$5$6$7$8$9$Y
! We didn't accept it and consequently it's invalid
  *                $N
```

X-REWRITE-SMS-ADDRESS

```
*/id=$_*/*      $C$0/id=$|X-VALIDATE-SMS-ADDRESS;$1|/$2$Y$E
*/id=$_*/*      $N
*                $C$|X-VALIDATE-SMS-ADDRESS;$0|$Y$E
*                $N
```

위와 같이 설정된 경우 `DESTINATION_ADDRESS_NUMERIC` 옵션 값이 0(기본값)인지 확인합니다. 그렇지 않을 경우 "+"가 SMS 대상 주소에서 스트라이프됩니다.

## 사이트 정의 텍스트 변환

사이트는 변환 규칙 테이블을 사용하여 [872페이지의 "전자 메일에서 SMS로의 변환 프로세스"](#)에 설명된 단계 1-6을 사용자 정의할 수 있습니다. 이러한 규칙은 MTA 매핑 파일의 매핑 테이블을 통해 지정됩니다.

매핑 테이블 이름은 `SMS_Channel_TEXT`여야 하며 여기에서 `SMS_Channel`은 SMS 채널의 이름입니다(예: 채널 이름이 `sms`인 경우 `SMS_TEXT` 또는 채널 이름이 `sms_mway`인 경우 `SMS_MWAY_TEXT`).

이 매핑 테이블에서 두 가지 유형의 항목을 만들 수 있습니다. 그러나 이러한 항목의 형식을 설명하기 전에 매핑 파일의 사용 방법을 이해하는 것이 중요합니다. 매핑 파일의 사용 방법을 아는 것은 이러한 항목을 생성 및 사용하는 방법을 이해하는 데 있어 필수적입니다. 이러한 두 유형의 항목이 설명된 후에는 매핑 테이블 예가 제공됩니다.

두 가지 유형의 항목은 다음과 같습니다.

- 메일 헤더 항목
- 메일 본문 항목

## 메일 헤더 항목

이러한 항목은 SMS 메일에 포함해야 하는 메일 헤더 행과 이러한 메일 헤더 행을 축약 또는 변환하는 방법을 지정합니다. 헤더 행은 이러한 항목 중 하나에 의해 길이가 0이 아닌 문자열로 성공적으로 매핑된 경우에만 생성할 SMS 메일에 포함됩니다. 각 항목은 다음 형식을 가집니다.

H|*pattern* *replacement-text*

메일 헤더 행은 패턴과 일치할 경우 매핑 파일의 패턴 일치 및 문자열 교체 기능을 사용하여 교체 텍스트 **replacement-text**로 교체됩니다. 그런 다음 메타 문자 \$Y가 교체 텍스트에 지정된 경우 헤더 행 매핑의 최종 결과는 SMS 메일에 포함됩니다. 헤더 행이 패턴 문자열과 일치하지 않거나 길이가 0인 문자열에 매핑되거나 교체 텍스트에 \$Y 메타 문자가 지정되지 않은 경우 SMS 메일에서 헤더 행이 생략됩니다. 다음 두 항목은

H|From:\* F:\$0\$Y  
H|Subject:\* S:\$0\$Y

From: 및 Subject: 헤더 행을 SMS 메일에 From: 및 Subject:의 약어 F: 및 S:로 포함시킵니다. 다음 항목은

H|Date:\* H|D:\$0\$R\$Y  
H|D:\*,\*%19%\*:\*:\* H|D:\$0\$ \$5:\$6\$R\$Y

Date: 헤더 행을 허용 및 매핑되도록 합니다. 예를 들어, 다음 헤더 행은

Date: Wed, 16 Dec 1992 16:13:27 -0700 (PDT)

다음과 같이 변환됩니다.

D: Wed 16:13

매우 복잡한 반복 매핑을 작성할 수 있습니다. 사용자 정의 필터를 설정하려는 사이트는 우선 매핑 파일의 작동 방법을 이해해야 할 수 있습니다. 항목의 오른쪽에 있는 H|는 원할 경우 생략할 수 있습니다. 반복 매핑 집합에 필요한 테이블 항목 수를 줄이기 위해 오른쪽에 H|가 허용됩니다.

## 메일 본문 항목

이러한 항목은 메일 본문의 각 행에 적용할 매핑을 설정합니다. 메일 본문의 각 행은 작성될 SMS 메일에 통합되기 전에 이러한 매핑을 통해 전달됩니다. 이러한 항목은 다음 형식을 가집니다.

B|*pattern* B|*replacement-text*

메일 본문의 행은 *pattern* 패턴과 일치할 경우 교체 텍스트 *replacement-text*로 교체됩니다. 마찬가지로 이 기능을 사용하여 매우 복잡한 반복 매핑을 생성할 수 있습니다. 항목의 오른쪽에 있는 B|는 원할 경우 생략할 수 있습니다.

## SMS 매핑 테이블 예

코드 예 D-1에는 SMS\_TEXT 매핑 테이블 예가 나와 있습니다. 각 행의 끝에 있는 괄호 안의 숫자는 바로 뒤에 오는 "설명 텍스트" 절의 항목 번호에 해당합니다.

코드 예 D-1 SMS\_TEXT 매핑 테이블 예

| SMS_TEXT     |                            |
|--------------|----------------------------|
| H From:*     | H F:\$0\$R\$Y (1.)         |
| H Subject:*  | H S:\$0\$R\$Y (1.)         |
| H F:<*>*     | H F:\$1\$R\$Y (1.)         |
| H F:*(*)*    | H F:\$0\$2\$R\$Y (2.)      |
| H F:*"*"*    | H F:\$0\$2\$R\$Y (3.)      |
| H F:*@*      | H F:\$0\$R\$Y (4.)         |
| H %:\$ *     | H \$0:\$1\$R\$Y (5.)       |
| H %:*\$      | H \$0:\$1\$R\$Y (5.)       |
| H %:*\$ \$ * | H \$0:\$1\$ \$2\$R\$Y (6.) |
| B *--*       | B \$0-\$1\$R (7.)          |
| B *.*        | B \$0.\$1\$R (7.)          |
| B *!* *      | B \$0!\$1\$R (7.)          |
| B *??*       | B \$0?\$1\$R (7.)          |
| B *\$ \$ *   | B \$0\$ \$1\$R (6.)        |
| B \$ *       | B \$0\$R (5.)              |
| B *\$        | B \$0\$R (5.)              |

## 설명 텍스트

이 절에서는 위의 SMS\_TEXT 매핑 테이블 예에 포함된 항목에 대해 설명합니다.

위 예에서는 매핑의 반복 적용을 구현 및 제어하기 위해 메타 문자 \$R이 사용됩니다. 이러한 매핑을 반복함으로써 강력한 필터링이 수행됩니다. 예를 들어, 단일 선행 또는 후행 공백을 제거하거나(6) 두 개의 공백을 하나의 공백으로 줄이는(7) 간단한 매핑은 서로 결합되어 모든 선행 및 후행 공백을 스트라이프하고 연속된 여러 공백을 모두 하나의 공백으로 줄이는 필터가 됩니다. 이러한 필터링은 각 SMS 메일의 크기를 줄이는 데 도움이 됩니다.

1. 이 두 항목은 From: 및 Subject: 헤더 행을 SMS 메일에 포함시킵니다. From: 및 Subject:는 각각 약어 F: 및 S:로 표시됩니다. 일부 다른 항목이 From: 및 Subject: 헤더 행에 영향을 줄 수 있습니다.

이 항목은 <...> 패턴을 포함하는 From: 헤더 행을 대괄호 안의 텍스트만으로 줄입니다. 예를 들면 다음과 같습니다.

F: "John C. Doe" <jdoe@siroe.com> (Hello)

다음 행으로 교체됩니다.

F: jdoe@siroe.com

2. 이 항목은 From:헤더 행의 (...) 패턴을 포함하여 그 안에 있는 모든 것을 제거합니다. 예를 들면 다음과 같습니다.

F: "John C. Doe" <jdoe@siroe.com> (Hello)

다음 행으로 교체됩니다.

F: "John C. Doe" <jdoe@siroe.com>

3. 이 항목은 From:헤더 행의 "." 패턴을 포함하여 그 안에 모든 것을 제거합니다. 예를 들면 다음과 같습니다.

F: "John C. Doe" <jdoe@siroe.com> (Hello)

다음 행으로 교체됩니다.

F: <jdoe@siroe.com> (Hello)

4. 이 항목은 From:헤더 행의 at 기호(@)를 포함하여 그 오른쪽에 있는 모든 것을 제거합니다. 예를 들면 다음과 같습니다.

F: "John C. Doe" <jdoe@siroe.com> (Hello)

다음 행으로 교체됩니다.

F: "John C. Doe" <jdoe@

5. 이러한 네 개의 항목은 메일 헤더와 본문의 행에서 선행 및 후행 공백을 제거합니다.

6. 이러한 두 개의 항목은 메일 헤더와 본문의 행에서 두 개의 공백을 하나의 공백으로 줄입니다.

7. 이러한 네 개의 항목은 이중 대시, 마침표, 느낌표 및 물음표를 일치하는 문자 하나로 줄입니다. 마찬가지로 이것은 SMS 메일의 바이트를 줄이는 데 도움이 됩니다.

항목의 순서는 매우 중요합니다. 예를 들어, 순서가 정해진 메일에서 메일의 본문은 From: 헤더 행입니다.

From: "John C. Doe" (Hello)

다음과 같이 줄어듭니다.

jdoe

이 작업은 다음과 같은 단계로 수행됩니다.

1. 다음과 같이 **From:** 헤더 행에서 시작합니다.

From: "John C. Doe" (Hello)

첫 번째 매핑 항목의 패턴이 일치하여 다음 결과를 생성합니다.

F: "John C. Doe" (Hello)

결과 문자열의 \$R 메타 문자로 인해 결과 문자열이 다시 매핑됩니다.

2. 마지막 단계의 결과 문자열에 매핑이 적용되어 다음을 생성합니다.

F: jdoe@siroe.com

매핑의 \$R로 인해 전체 매핑 세트가 이 단계의 결과에 다시 적용됩니다.

3. 다음으로 매핑이 적용되어 다음이 생성됩니다.

F: jdoe

매핑의 \$R로 인해 전체 매핑 세트가 이 단계의 결과에 다시 적용됩니다.

4. 다음으로 매핑이 적용되어 다음이 생성됩니다.

F: jdoe

매핑의 \$R로 인해 전체 매핑 세트가 이 단계의 결과에 다시 적용됩니다.

5. 일치하는 다른 항목이 없으므로 다음 최종 결과 문자열이

F: jdoe

SMS 메일에 통합됩니다.

---

**주**      imsimta 테스트 매핑 유틸리티를 사용하여 매핑 테이블을 테스트할 수 있습니다. 예를 들면 다음과 같습니다.

```
# imsimta test -mapping -noimage_file -mapping_file=test.txt
Enter table name: SMS_TEXT
Input string: H|From: "John C. Doe"   (Hello)
Output string: H|F:jdoe
Output flags: [0,1,2,89]
Input string: ^D
#
```

imsimta 유틸리티에 대한 자세한 내용은 *Sun Java System Messaging Server 관리 설명서*(<http://docs.sun.com/doc/819-1055>)를 참조하십시오.

---

## SMS 채널 구성

이 절에서는 단방향(Email-To-Mobile) 및 양방향(Email-To-Mobile 및 Mobile-To-Email) 기능을 모두 사용하도록 SMS 채널을 설정하는 방법에 대해 설명합니다. [914페이지](#)의 "양방향 SMS를 위한 SMS 채널 구성"에 언급된 내용을 제외하고 SMS 채널은 단방향 및 양방향 기능 모두에 대해 동일하게 설정됩니다.

이 절은 다음 내용으로 구성되어 있습니다.

- [886페이지](#)의 "SMS 채널 추가"
- [889페이지](#)의 "SMS 채널 옵션 파일 만들기"
- [890페이지](#)의 "사용 가능한 옵션"
- [911페이지](#)의 "SMS 채널 추가"
- [912페이지](#)의 "전달 재시도 빈도 조정"
- [912페이지](#)의 "샘플 단방향 구성(MobileWay)"
- [914페이지](#)의 "양방향 SMS를 위한 SMS 채널 구성"

## SMS 채널 추가

Messaging Server 구성에 SMS 채널을 추가하려면 다음 두 단계를 수행해야 합니다.

1. 887페이지의 "채널 정의 및 다시 쓰기 규칙 추가"
2. 889페이지의 "SMS 채널 옵션 파일 만들기"

모든 상황에서 설정해야 하는 채널 옵션이 있는 것은 아니지만 `ESME_PASSWORD`, `ESME_SYSTEM_ID`, `MAX_PAGE_SIZE`, `DEFAULT_SOURCE_TON` 및 `DEFAULT_DESTINATION_TON` 또한 설명된 바와 같이 `imta.cnf` 파일의 채널 정의나 채널 옵션 파일을 통해 SMPP 서버의 호스트 이름 또는 IP 주소와 TCP 포트를 설정해야 합니다.

둘 이상의 SMS 채널을 구성하여 다른 SMS 채널에 다른 특성을 제공할 수 있습니다. 여러 SMS 채널 사용에 대한 자세한 내용은 911페이지의 "SMS 채널 추가"를 참조하십시오.

`imta.cnf` 파일을 변경할 경우 다시 컴파일해야 한다는 것입니다. 단순히 채널 옵션 파일을 변경할 경우에는 다시 컴파일할 필요가 없습니다.

또한 채널 변경 사항 적용 시간은 변경 사항에 따라 달라질 수 있다는 점에 주의하십시오. 대부분의 채널 옵션 변경 사항은 변경 이후에 시작된 모든 채널에서 적용되며 Job Controller에서 종종 새 채널을 시작하므로 이것은 거의 즉시 적용되는 것처럼 보일 수 있습니다. 일부 변경 사항은 재컴파일을 수행하고 SMTP 서버를 다시 시작할 때까지 적용되지 않습니다. 이러한 옵션은 채널 자체가 실행될 때가 아니라 메일이 채널의 대기열에 포함될 때 처리됩니다.

## 채널 정의 및 다시 쓰기 규칙 추가

채널 정의 및 다시 쓰기 규칙을 추가하려면 다음을 수행합니다.

1. SMS 채널을 MTA의 구성에 추가하기 전에 채널 이름을 선택해야 합니다. 채널 이름은 `sms` 또는 `sms_x`가 될 수 있으며 여기서 `x`는 1바이트에서 36바이트 사이의 길이를 가진 대소문자가 구분된 임의의 문자열입니다(예: `sms_mway`).
2. 채널 정의를 추가하려면 `installation-directory/config/` 디렉토리에 있는 `imta.cnf` 파일을 편집합니다. 파일의 맨 아래에 빈 행과 다음과 같은 두 행을 추가합니다.

```
channel-name port p threaddepth t \  
  backoff pt2m pt5m pt10m pt30m notices 1  
smpp-host-name
```

여기서 `channel-name`은 사용자가 선택한 채널 이름이고 `p`는 SMPP 서버가 수신하는 TCP 포트이며 `t`는 각 전달 프로세스의 최대 동시 SMPP 서버 연결 수입니다. 마지막으로 `smpp-host-name`은 SMPP 서버를 실행하는 시스템의 호스트 이름입니다.

예를 들어, 다음과 같이 채널 정의를 지정할 수 있습니다.

```
sms_mway port 55555 threaddepth 20 \
  backoff pt2m pt5m pt10m pt30m notices 1
smpp.siroe.com
```

threaddepth를 계산하는 방법에 대한 지침은 [889페이지의 "동시 연결 수 제어"](#)를 참조하십시오.

backoff 및 notices 채널 키워드에 대한 자세한 내용은 [912페이지의 "전달 재시도 빈도 조정"](#)을 참조하십시오.

smpp-host-name에 호스트 이름 대신 IP를 지정하려면 도메인 리터럴을 지정합니다. 예를 들어, IP 주소가 127.0.0.1인 경우 smpp-host-name에 [127.0.0.1]을 지정합니다. 또는 [SMPP\\_SERVER](#) 채널 옵션을 사용할 것을 고려합니다.

---

**주** Sun Java System Messaging Server 6.1의 경우 master 채널 키워드는 더 이상 사용되지 않습니다. 이 키워드가 있을 경우 무시됩니다.

---

3. 채널 정의가 추가된 후에는 파일의 상단 부분으로 가서 다음 형식의 다시 쓰기 규칙을 추가합니다.

```
smpp-host-name $u@smpp-host-name
```

예를 들면 다음과 같습니다.

```
smpp.siroe.com $u@smpp.siroe.com
```

4. imta.cnf 파일을 저장합니다.
5. imsimta cnbuild 명령을 사용하여 구성을 다시 컴파일합니다.
6. imsimta restart dispatcher 명령을 사용하여 SMTP 서버를 다시 시작합니다.
7. 위 구성에서는 전자 메일 주소를 id@smpp-host-name(예: 123456@smpp.siroe.com)으로 지정하여 전자 메일을 채널로 전송합니다. 주소 지정에 대한 자세한 내용은 [872페이지의 "전자 메일에서 SMS로의 변환 프로세스"](#)를 참조하십시오.



8. 선택적으로 SMPP 서버의 호스트 이름을 사용자가 볼 수 없게 하거나 다른 호스트 이름을 동일한 채널과 연관시키려는 경우 다시 쓰기 규칙을 추가합니다. 예를 들어, host-name-1 및 host-name-2를 채널과 연관시키려면 다음을 다시 쓰기 규칙에 추가합니다.

```
host-name-1 $U%host-name-1@smpp-host-name
host-name-2 $U%host-name-2@smpp-host-name
```

예를 들어, SMPP 서버의 호스트 이름이 smpp.siroe.com이지만 사용자에게 전자 메일 주소를 id@sms.sesta.com으로 지정하게 하려면 다음 다시 쓰기 규칙을 추가합니다.

```
sms.sesta.com $U%sms.sesta.com@smpp.siroe.com
```

SMPP\_SERVER 및 SMPP\_PORT 채널 옵션은 채널의 공식 호스트 이름과 port 채널 키워드 설정을 무시합니다. SMPP\_PORT 옵션이 사용되면 또한 port 키워드를 사용할 필요가 없습니다. 이러한 두 옵션은 적용된 후에 구성을 다시 컴파일하지 않고도 변경할 수 있다는 이점이 있습니다. SMPP\_SERVER 옵션의 추가 사용에 대해서는 911페이지의 "SMS 채널 추가"에 설명되어 있습니다.

## 동시 연결 수 제어

threaddepth 채널 키워드는 전달 프로세스 내의 각 전달 스레드에 할당할 메일 수를 제어합니다. 허용되는 동시 연결 수 합계를 계산하려면 SMPP\_MAX\_CONNECTIONS 옵션과 job\_limit(SMPP\_MAX\_CONNECTIONS \* job\_limit) 옵션의 값을 곱합니다.

SMPP\_MAX\_CONNECTIONS 옵션은 전달 프로세스의 최대 전달 스레드 수를 제어합니다.

job\_limit 옵션은 채널이 실행되는 Job Controller 처리 풀에 대해 최대 동시 전달 프로세스 수를 제어합니다.

총 동시 연결 수를 제한하려면 이러한 옵션 중 하나 또는 둘 다를 적절하게 조정해야 합니다. 예를 들어, 원격 SMPP 서버가 단일 연결만 허용할 경우 SMPP\_MAX\_CONNECTIONS 및 job\_limit를 모두 1로 설정해야 합니다. 값을 조정할 때는 job\_limit가 1을 초과하도록 허용하는 것이 좋습니다.

## SMS 채널 옵션 파일 만들기

일반적으로 채널 옵션 파일은 채널 작업에 필요한 사이트별 매개 변수를 포함합니다. SMS에는 채널 옵션 파일이 필요하지 않습니다. 현재 설치에 채널 옵션 파일이 필요한 경우에는 installation-directory/config/ 디렉토리의 텍스트 파일에 이를 저장합니다. 다른 채널 옵션 파일과 마찬가지로 파일 이름의 형식은 다음과 같습니다.

```
channel_name_option
```

예를 들어, 채널 이름이 sms\_mway인 경우 채널 옵션 파일은 다음과 같습니다.

```
installation-directory/config/sms_mway_option
```

각 옵션은 파일에서 다음 형식을 사용하여 단일 행에 포함됩니다.

```
option_name=option_value
```

예를 들면 다음과 같습니다.

```
PROFILE=GSM  
SMSC_DEFAULT_CHARSET=iso-8859-1  
USE_UCS2=1
```

사용 가능한 SMS 채널 옵션 목록과 각 옵션에 대한 설명은 뒤에 나오는 "[사용 가능한 옵션](#)"을 참조하십시오.

## 사용 가능한 옵션

SMS 채널은 넓은 의미에서 다음과 같은 6개의 범주로 구분되는 여러 옵션을 포함합니다.

- *전자 메일에서 SMS로의 변환*: 전자 메일에서 SMS로의 변환 프로세스를 제어하는 옵션입니다.
- *SMS 게이트웨이 서버 옵션*: 게이트웨이 프로필 옵션입니다.
- *SMS 필드*: 생성된 SMS 메일의 SMS별 필드를 제어하는 옵션입니다.
- *SMPP 프로토콜*: TCP/IP를 통한 SMPP 프로토콜 사용과 관련된 옵션입니다.
- *현지화*: SMS 메일에 삽입되는 텍스트 필드의 현지화를 허용하는 옵션입니다.
- *기타*: 디버그 옵션입니다.

이러한 옵션은 아래 표에 요약되어 있으며 이후의 절에 보다 자세하게 설명되어 있습니다.

**표 D-5** SMS 채널 옵션

---

---

### 전자 메일에서 SMS로의 변환 옵션

---

---

표 D-5 SMS 채널 옵션 (계속)

| 옵션(페이지 번호)             | 설명                                          | 기본값      |
|------------------------|---------------------------------------------|----------|
| GATEWAY_NOTIFICATIONS  | 전자 메일 알림 메시지를 SMS 메일로 변환할지 여부를 지정합니다.       | 0        |
| MAX_MESSAGE_PARTS      | 전자 메일에서 추출할 메일 부분의 최대 개수입니다.                | 2        |
| MAX_MESSAGE_SIZE       | 전자 메일에서 추출할 최대 바이트 수입니다.                    | 960      |
| MAX_PAGE_SIZE          | 단일 SMS 메일에 포함할 최대 바이트 수입니다.                 | 160      |
| MAX_PAGES_PER_MESSAGE  | 전자 메일을 분할할 최대 SMS 메일 수입니다.                  | 6        |
| ROUTE_TO               | SMS 메일을 지정된 IP 호스트 이름으로 라우팅합니다.             |          |
| SMSC_DEFAULT_CHARSET   | SMSC에 사용되는 기본 문자 세트입니다.                     | US-ASCII |
| USE_HEADER_FROM        | SMS 소스 주소를 설정합니다.                           | 0        |
| USE_HEADER_PRIORITY    | 전자 메일 헤더에서 우선 순위 정보의 사용을 제어합니다.             | 1        |
| USE_HEADER_REPLY_TO    | SMS 소스 주소를 생성할 때 Reply-to: 헤더 행의 사용을 제어합니다. | 0        |
| USE_HEADER_RESENT      | 발송자 정보를 생성할 때 Resent-*: 헤더 행 사용을 제어합니다.     | 0        |
| USE_HEADER_SENSITIVITY | 전자 메일 헤더에서 개인 정보의 사용을 제어합니다.                | 1        |
| USE_UCS2               | 적용 가능한 경우 SMS 메일에서 UCS2 문자 세트를 사용합니다.       | 1        |

**SMS 게이트웨이 서버 옵션**

|                 |                                                                         |  |
|-----------------|-------------------------------------------------------------------------|--|
| GATEWAY_PROFILE | SMS 게이트웨이 서버의 구성 파일 sms_gateway.cnf에 구성 해당 없음<br>된 게이트웨이 프로필 이름과 일치합니다. |  |
|-----------------|-------------------------------------------------------------------------|--|

**SMS 필드 옵션**

|                         |                                     |                       |
|-------------------------|-------------------------------------|-----------------------|
| DEFAULT_DESTINATION_NPI | SMS 대상 주소의 기본 NPI입니다.               | 0x00                  |
| DEFAULT_DESTINATION_TON | SMS 대상 주소의 기본 TON입니다.               | 0x01                  |
| DEFAULT_PRIORITY        | SMS 메일의 기본 우선 순위 설정입니다.             | 0=GSM, CDMA<br>1=TDMA |
| DEFAULT_PRIVACY         | SMS 메일의 기본 개인 정보 값 플래그입니다.          | -1                    |
| DEFAULT_SERVICE_TYPE    | 전송된 SMS 메일과 연관된 SMS 응용 프로그램 서비스입니다. | 해당 없음                 |

표 D-5 SMS 채널 옵션 (계속)

|                             |                                                                                                                                                                                           |       |
|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| DEFAULT_SOURCE_ADDRESS      | 기본 SMS 소스 주소입니다.                                                                                                                                                                          | 0     |
| DEFAULT_SOURCE_NPI          | SMS 소스 주소의 기본 NPI입니다.                                                                                                                                                                     | 0x00  |
| DEFAULT_SOURCE_TON          | SMS 소스 주소의 기본 TON입니다.                                                                                                                                                                     | 0x01  |
| DEFAULT_VALIDITY_PERIOD     | SMS 메일의 기본 유효 기간입니다.                                                                                                                                                                      | 해당 없음 |
| DESTINATION_ADDRESS_NUMERIC | 대상 SMS 주소를 0 - 9개의 문자로만 구성되도록 줄입니다.                                                                                                                                                       | 0     |
| DESTINATION_ADDRESS_PREFIX  | 대상 SMS 주소의 접두어로 사용할 텍스트 문자열입니다.                                                                                                                                                           | 해당 없음 |
| PROFILE                     | 사용할 SMS 프로필입니다.                                                                                                                                                                           | GSM   |
| USE_SAR                     | SMS sar_필드를 사용하는 여러 SMS 메일의 순서를 정합니다.                                                                                                                                                     | 0     |
| <b>SMPP 프로토콜 옵션</b>         |                                                                                                                                                                                           |       |
| ESME_ADDRESS_NPI            | SMPP 서버에 바인드할 때 지정할 ESME NPI입니다.                                                                                                                                                          | 0x00  |
| ESME_ADDRESS_TON            | SMPP 서버에 바인드할 때 지정할 ESME TON입니다.                                                                                                                                                          | 0x00  |
| ESME_IP_ADDRESS             | Sun Java System Messaging Server를 실행하는 호스트의 IP 주소입니다.                                                                                                                                     | 해당 없음 |
| ESME_PASSWORD               | SMPP 서버에 바인드할 때 제시할 비밀번호입니다.                                                                                                                                                              | 해당 없음 |
| ESME_SYSTEM_ID              | 바인드할 때 SMSC에 제시할 시스템 아이디입니다.                                                                                                                                                              | 해당 없음 |
| ESME_SYSTEM_TYPE            | 바인드할 때 SMSC에 제시할 시스템 유형입니다.                                                                                                                                                               | 해당 없음 |
| MAX_PAGES_PER_BIND          | SMPP 서버와의 단일 세션 도중 전송할 최대 SMS 메일 수입니다.                                                                                                                                                    | 1024  |
| REVERSE_ORDER               | 멀티파트 SMS 메일의 전송 시퀀스입니다.                                                                                                                                                                   | 0     |
| SMPP_MAX_CONNECTIONS        | 최대 동시 SMPP 서버 연결 수입니다.                                                                                                                                                                    | 20    |
| SMPP_PORT                   | 단방향 SMS의 경우 SMPP 서버가 수신하는 TCP 포트입니다. 양방향 SMS의 경우 SMPP 릴레이를 위해 LISTEN_PORT에서 사용하는 것과 동일한 TCP 포트입니다.                                                                                        | 해당 없음 |
| SMPP_SERVER                 | 단방향 SMS의 경우 연결할 SMPP 서버의 호스트 이름입니다. 양방향 SMS의 경우 SMS 게이트웨이 서버의 호스트 이름이나 IP 주소를 가리키도록 설정합니다. SMPP 릴레이의 LISTEN_INTERFACE_ADDRESS 옵션을 사용할 경우 지정된 네트워크 인터페이스 주소와 연관된 호스트 이름이나 IP 주소를 사용해야 합니다. | 해당 없음 |
| TIMEOUT                     | SMPP 서버에서 읽기 및 쓰기 완료 시의 시간 초과입니다.                                                                                                                                                         | 30    |

표 D-5 SMS 채널 옵션 (계속)

| 현지화 옵션             |                                   |                 |
|--------------------|-----------------------------------|-----------------|
| CONTENT_PREFIX     | 전자 메일의 내용을 소개하는 텍스트입니다.           | Msg:            |
| DSN_DELAYED_FORMAT | 전달 지연 알림에 대한 서식 지정 문자열입니다.        | 빈 문자열           |
| DSN_FAILED_FORMAT  | 전달 실패 알림에 대한 서식 지정 문자열입니다.        | 설명 참조           |
| DSN_RELAYED_FORMAT | 릴레이 알림에 대한 서식 지정 문자열입니다.          | 설명 참조           |
| DSN_SUCCESS_FORMAT | 성공한 전달 알림에 대한 서식 지정 문자열입니다.       | 설명 참조           |
| FROM_FORMAT        | 전자 메일 발송자를 나타내기 위해 표시할 텍스트입니다.    | \$a             |
| FROM_NONE          | 메일 발송자가 없을 경우 표시할 텍스트입니다.         | 해당 없음           |
| LANGUAGE           | (i-default) 텍스트 필드를 선택할 언어 그룹입니다. | i-default       |
| LINE_STOP          | 전자 메일에서 추출한 각 행의 끝에 포함할 텍스트입니다.   | 공백 문자           |
| NO_MESSAGE         | 메일에 내용이 없음을 나타내는 텍스트입니다.          | ]no<br>message] |
| SUBJECT_FORMAT     | 전자 메일의 제목을 나타내기 위해 표시할 텍스트입니다.    | \$s             |
| SUBJECT_NONE       | 전자 메일의 제목이 없을 경우 표시할 텍스트입니다.      | 해당 없음           |
| 기타 옵션              |                                   |                 |
| DEBUG              | 세부 정보 디버그 출력을 사용 가능하게 합니다.        | -1              |

### 전자 메일에서 SMS로의 변환 옵션

다음 옵션은 전자 메일에서 SMS 메일로의 변환을 제어합니다. 해당 옵션의 값 범위는 괄호 안에 있습니다. 일반적으로 지정된 전자 메일을 하나 이상의 SMS 메일로 변환할 수 있습니다. 이 변환 프로세스에 대한 자세한 내용은 [872페이지의 "전자 메일에서 SMS로의 변환 프로세스"](#)를 참조하십시오.

#### GATEWAY\_NOTIFICATIONS

(0 또는 1) 전자 메일 알림을 SMS 알림으로 변환할지 여부를 지정합니다. 전자 메일 알림 메시지는 RFC 1892, 1893 및 1894를 준수해야 합니다. 기본값은 0입니다.

GATEWAY\_NOTIFICATIONS=0일 경우 이러한 알림은 무시되며 SMS 알림으로 변환되지 않습니다.

알림을 SMS 알림으로 변환할 수 있게 하려면 GATEWAY\_NOTIFICATIONS=1을 설정합니다. 이 옵션이 1로 설정되면 현지화 옵션(DSN\_\*\_FORMAT)은 SMS 메일로 변환되고 게이트웨이를 통해 전송할 알림 유형(성공, 실패, 지연, 릴레이)을 제어합니다. 알림 유형의 값이 빈 문자열이면 해당 유형 알림이 SMS 메일로 변환되지 않습니다.

### MAX\_MESSAGE\_PARTS

(정수) 멀티파트 전자 메일을 SMS 메일로 변환할 때 텍스트 부분 중에서 MAX\_MESSAGE\_PARTS만큼의 처음 부분만 변환됩니다. 나머지 부분은 무시됩니다. 기본적으로 MAX\_MESSAGE\_PARTS는 2입니다. 메일 부분의 개수를 제한하지 않으려면 -1을 지정합니다. 값이 0으로 지정되면 SMS 메일에 포함되는 메일 내용이 없습니다. 이것은 전자 메일의 헤더 행(예: Subject:)만 사용하여 SMS 메일을 생성하는 효과를 가집니다.

텍스트와 첨부 파일을 모두 포함하는 전자 메일은 일반적으로 두 부분으로 구성됩니다. 또한 일반 텍스트 메일 부분만 변환되며, 다른 모든 MIME 컨텐트 유형은 무시됩니다.

### MAX\_MESSAGE\_SIZE

(정수, >= 10) 이 옵션을 사용하면 전자 메일에서 생성되는 SMS 메일에 포함될 총 바이트 수의 상한값을 지정할 수 있습니다. 특히 하나 이상의 생성된 SMS 메일에 최대 MAX\_MESSAGE\_SIZE 바이트가 사용됩니다. 모든 추가 바이트는 무시됩니다.

기본적으로 960바이트의 상한값이 지정됩니다. 이것은 MAX\_MESSAGE\_SIZE=960에 해당합니다. 임의의 바이트 수를 허용하려면 값을 0으로 지정합니다.

사용되는 바이트 수는 전자 메일을 유니코드에서 SMSC의 기본 문자 세트나 UCS2로 변환한 후에 결정됩니다. 이것은 UCS2의 경우 각 UCS2 문자의 길이가 최소 2바이트 이상이므로 960바이트의 MAX\_MESSAGE\_SIZE는 최대 480개의 문자를 생성한다는 것을 의미합니다.

MAX\_MESSAGE\_SIZE 및 MAX\_PAGES\_PER\_MESSAGE 옵션은 모두 결과 SMS 메일의 전체 크기를 제한하는 동일한 목적으로 사용됩니다. 실제로 MAX\_PAGE\_SIZE=960 및 MAX\_PAGE\_SIZE=160은 MAX\_PAGES\_PER\_MESSAGE=6을 나타냅니다. 서로 다른 두 개의 옵션이 존재하는 이유는 무엇입니까? 그것은 단일 SMS 메일의 최대 크기인 MAX\_PAGE\_SIZE를 고려할 필요 없이 페이지의 전체 크기나 수를 제어할 수 있어야 하기 때문입니다. 이 기능은 채널 옵션 파일에서는 중요하지 않을 수 있지만 870페이지의 "전자 메일을 채널로 전송"에 설명된 MAXPAGES 또는 MAXLEN 주소 지정 속성을 사용하는 경우에는 중요합니다.

마지막으로 MAX\_MESSAGE\_SIZE 및 MAX\_PAGE\_SIZE \* MAX\_PAGES\_PER\_MESSAGE의 두 제한값 중 보다 작은 값이 사용됩니다.

**MAX\_PAGE\_SIZE**

(정수, >= 10) 단일 SMS 메일에서 허용하는 최대 바이트 수는 MAX\_PAGE\_SIZE 옵션을 사용하여 제어합니다. 기본적으로 160바이트가 사용됩니다. 이것은 MAX\_PAGE\_SIZE=160에 해당합니다.

**MAX\_PAGES\_PER\_MESSAGE**

(정수, 1 - 255) 주어진 전자 메일에 대해 생성할 최대 SMS 메일 수를 이 옵션을 사용하여 제어합니다. 실제로 이 옵션은 전자 메일을 잘라 MAX\_PAGES\_PER\_MESSAGE SMS 메일에 들어가는 전자 메일의 해당 부분만 SMS 메일로 변환합니다. 자세한 내용은 MAX\_PAGE\_SIZE 옵션에 대한 설명을 참조하십시오.

기본적으로 MAX\_PAGES\_PER\_MESSAGE는 MAX\_MESSAGE\_SIZE를 MAX\_PAGE\_SIZE로 나눈 값이나 1보다 큰 값으로 설정됩니다.

**ROUTE\_TO**

(문자열, IP 호스트 이름, 1-64바이트) 프로필을 대상으로 하는 모든 SMS 메일은 다음 형식의 전자 메일 주소를 사용하여 지정된 IP 호스트 이름으로 다시 라우팅됩니다.

SMS-destination-address@route-to

여기서 SMS-destination-address는 SMS 메일의 대상 주소이며 route-to는 이 옵션에서 지정되는 IP 호스트 이름입니다. SMS 메일의 전체 내용이 결과 전자 메일의 내용으로 보내집니다. PARSE\_RE\_\* 옵션은 무시됩니다.

---

**주**

PARSE\_RE\_\* 및 ROUTE\_TO 옵션을 동시에 사용할 수 없습니다. 동일한 게이트웨이 프로필에서 두 옵션을 함께 사용하는 것은 구성 오류입니다.

---

**SMSC\_DEFAULT\_CHARSET**

(문자열) 이 옵션을 사용하면 SMSC의 기본 문자 세트를 지정할 수 있습니다. 다음 파일에서 제공되는 문자 세트 이름을 사용합니다.

installation-directory/config/charsets.txt

이 옵션을 지정하지 않을 경우 US-ASCII가 사용됩니다. charsets.txt에 사용되는 니모닉 이름은 동일한 디렉토리의 charnames.txt에 정의됩니다.

전자 메일을 처리할 때 헤더 행과 텍스트 메일 부분은 우선 디코딩된 다음 유니코드로 변환됩니다. 그런 다음 `USE_UCS2` 옵션 값과 SMS 메일이 기본 SMSC 문자 세트에 없는 최소한 하나 이상의 도형 문자를 포함하는지 여부에 따라 데이터는 SMSC의 기본 문자 세트나 UCS2로 변환됩니다. UCS2 문자 세트는 유니코드의 16비트 인코딩으로 흔히 UTF-16으로 불립니다.

### **USE\_HEADER\_FROM**

(정수, 0-2) `From:` 주소를 SMSC에 전달하려면 이 옵션을 설정합니다. 값은 `From:` 주소를 가져온 위치와 형식을 나타냅니다. 표 D-6에서는 허용 가능한 값과 해당 의미를 보여 줍니다.

**표 D-6** USE\_HEADER\_FROM 값

| 값 | 설명                                                                                                                                       |
|---|------------------------------------------------------------------------------------------------------------------------------------------|
| 0 | SMS 소스 주소가 <code>From:</code> 주소에서 설정되지 않습니다. 발견된 속성값 쌍을 사용합니다.                                                                          |
| 1 | SMS 소스 주소를 <code>from-local@from-domain</code> 으로 설정합니다. 여기서 <code>From:</code> 주소는 <code>@from-route:from-local@from-domain</code> 입니다. |
| 2 | SMS 소스 주소를 <code>from-local</code> 로 설정합니다. 여기서 <code>From:</code> 주소는 <code>@from-route:from-local@from-domain</code> 입니다.              |

### **USE\_HEADER\_PRIORITY**

(0 또는 1) 이 옵션은 RFC 822 `Priority:` 헤더 행의 처리를 제어합니다. `Priority:` 헤더 행의 정보는 결과 SMS 메일의 우선 순위 플래그를 설정하여 `DEFAULT_PRIORITY` 옵션에서 지정된 기본 SMS 우선 순위를 무시하는 데 사용됩니다. 이 경우는

`USE_HEADER_PRIORITY=1`에 해당합니다. RFC 822 `Priority:` 헤더 행을 사용하지 않으려면 `USE_HEADER_PRIORITY=0`을 지정합니다.

SMS 우선 순위 플래그 처리에 대한 자세한 내용은 `DEFAULT_PRIORITY` 옵션에 대한 설명을 참조하십시오.

### **USE\_HEADER\_REPLY\_TO**

(0 또는 1) `USE_HEADER_FROM = 1`인 경우 이 옵션은 `Reply-to:` 또는 `Resent-reply-to:` 헤더 행이 SMS 소스 주소를 사용되는지 여부를 제어합니다. 기본적으로 `Reply-to:` 및 `Resent-reply-to:` 헤더 행은 무시됩니다. 이것은 옵션 값 0에 해당합니다. 이러한 헤더 행 사용을 고려하려면 옵션 값 1을 사용합니다.

RFC 2822에서는 `Reply-to:` 및 `Resent-reply-to:` 헤더 행에 매핑하는 데만 사용됩니다.



### USE\_HEADER\_RESENT

(0 또는 1) USE\_HEADER\_FROM =1이면 이 옵션은 Resent- 헤더 행을 SMS 소스 주소로 사용하도록 고려할지 여부를 제어합니다. 기본적으로 Resent- 헤더 행은 무시됩니다. 이것은 옵션 값 0에 해당합니다. 이러한 헤더 행 사용을 고려하려면 옵션 값 1을 사용합니다.

RFC 2822에서는 Resent- 헤더 행을 사용하지 않습니다.

### USE\_HEADER\_SENSITIVITY

(0 또는 1) USE\_HEADER\_SENSITIVITY 옵션은 RFC 822 Sensitivity: 헤더 행의 처리를 제어합니다. 기본적으로, Sensitivity: 헤더 행의 정보는 결과 SMS 메일의 개인 정보 플래그를 설정하여 DEFAULT\_PRIVACY 옵션에서 지정된 기본 SMS 개인 정보를 무시하는 데 사용됩니다. 이것은 기본값이며 USE\_HEADER\_SENSITIVITY=1에 해당합니다. RFC 822 Sensitivity: 헤더 행을 사용하지 않으려면 USE\_HEADER\_SENSITIVITY=0으로 지정합니다.

SMS 개인 정보 플래그 처리에 대한 자세한 내용은 DEFAULT\_PRIVACY 옵션에 대한 설명을 참조하십시오.

### USE\_UCS2

(0 또는 1) 채널은 생성되는 SMS 메일에서 적절한 경우 UCS2 문자 세트를 사용합니다. 이것은 기본 동작이며 USE\_UCS2=1에 해당합니다. UCS2 문자 세트를 사용하지 않으려면 USE\_UCS2=0을 지정합니다. 문자 세트 문제에 대한 자세한 내용은 SMSC\_DEFAULT\_CHARSET 옵션에 대한 설명을 참조하십시오.

**표 D-7** USE\_UCS2에 대한 유효 값

| USE_UCS2 값 | 결과                                                                                         |
|------------|--------------------------------------------------------------------------------------------|
| 1(기본값)     | 가능한 경우 SMSC 기본 문자 세트가 사용됩니다. 원본 전자 메일이 SMSC 기본 문자 세트에 도형 문자를 포함하지 않을 경우 UCS2 문자 세트가 사용됩니다. |
| 0          | 항상 SMSC 기본 문자 세트가 사용됩니다. 해당 문자 세트에서 사용할 수 없는 도형 문자는 니모닉으로 나타냅니다(예: AE-ligature의 경우 "AE").  |

## SMS 게이트웨이 서버 옵션

### GATEWAY\_PROFILE

SMS 게이트웨이 서버 구성 파일 sms\_gateway.cnf에 있는 게이트웨이 프로필의 이름입니다.

## SMS 옵션

다음 옵션을 사용하면 생성된 SMS 메일에서 SMS 필드를 지정할 수 있습니다.

### DEFAULT\_DESTINATION\_NPI

(정수, 0 - 255) 기본적으로 대상 주소에는 NPI(Numeric Plan Indicator) 값으로 0이 할당됩니다. 이 옵션을 사용하면 0부터 255까지 범위의 대체 정수 값이 할당될 수 있습니다. 다음 표 D-8에서는 일반적인 NPI 값을 보여 줍니다.

**표 D-8** Numeric Plan Indicator 값

| 값     | 설명                 |
|-------|--------------------|
| 0     | 알 수 없음             |
| 1     | ISDN(E.163, E.164) |
| 3     | 데이터(X.121)         |
| 4     | 텔렉스(F.69)          |
| 6     | 육상 이동 통신(E.212)    |
| 8     | 국가                 |
| 9     | 비공개                |
| 10    | ERMES              |
| 14    | IP 주소(인터넷)         |
| 18    | WAP 클라이언트 아이디      |
| >= 19 | 정의되지 않음            |

이 옵션 값은 다음 세 가지 방법 중 하나로 지정할 수 있습니다.

- 10진수 값(예: 10)
- 접두어 "0x"가 있는 16진수 값(예: 0x0a)
- 대소문자를 구분하지 않는 다음 텍스트 문자열 중 하나(괄호 안은 연관된 10진수 값): data(3), default(0), e.163(1), e.164(1), e.212(6), ermes(10), f.69(4), Internet(14), ip(14), isdn(1), land-mobile(6), national(8), private(9), telex(4), unknown(0), wap(18), x.121(3)

**DEFAULT\_DESTINATION\_TON**

(정수, 0 - 255) 기본적으로 대상 주소에는 TON(Type of Number) 지정자 값으로 0이 할당됩니다. 이 옵션을 사용하면 0부터 255까지 범위의 대체 정수 값이 할당될 수 있습니다. 다음 표 D-9에서는 일반적인 TON 값을 보여 줍니다.

**표 D-9** 일반 TON 값

| 값   | 설명      |
|-----|---------|
| 0   | 알 수 없음  |
| 1   | 국제      |
| 2   | 국가      |
| 3   | 네트워크별   |
| 4   | 가입자 번호  |
| 5   | 영숫자     |
| 6   | 축약      |
| >=7 | 정의되지 않음 |

이 옵션 값은 다음 세 가지 방법 중 하나로 지정할 수 있습니다.

- 10진수 값(예: 10)
- 접두어 "0x"가 있는 16진수 값(예: 0x0a)
- 대소문자를 구분하지 않는 다음 텍스트 문자열 중 하나(괄호 안은 연관된 10진수 값): abbreviated (6), alphanumeric (5), default (0), international (1), national (2), network-specific (3), subscriber (4), unknown (0)

**DEFAULT\_PRIORITY**

(정수, 0 - 255) SMS 메일은 필수 우선 순위 필드를 가집니다. 다음 표 D-10에서는 SMS 우선 순위 값이 해석되는 방법을 보여 줍니다.

**표 D-10** 각 SMS 프로필 유형에 대해 해석되는 SMS 우선 순위 값

| 값 | GSM   | TDMA  | CDMA |
|---|-------|-------|------|
| 0 | 낮음    | 대량    | 중간   |
| 1 | 우선 순위 | 중간    | 대화식  |
| 2 | 우선 순위 | 높음    | 높음   |
| 3 | 우선 순위 | 매우 높음 | 긴급   |

이 옵션을 사용하면 SMS 메일에 할당되는 기본 우선 순위를 지정할 수 있습니다. 값을 지정하지 않을 경우 기본 우선 순위 0이 PROFILE=GSM 및 CDMA에 사용되며 우선 순위 1이 PROFILE=TDMA에 사용됩니다.

USE\_HEADER\_PRIORITY=1이고 전자 메일에 RFC 822 Priority: 헤더 행이 있는 경우 해당 헤더 행에 지정된 우선 순위를 대신 사용하여 결과 SMS 메일의 우선 순위를 설정합니다. 특히 USE\_HEADER\_PRIORITY=0일 경우에는 SMS 우선 순위 플래그는 항상 DEFAULT\_PRIORITY 옵션에 따라 설정되며 RFC 822 Priority: 헤더 행은 항상 무시됩니다. USE\_HEADER\_PRIORITY=1인 경우 원본 전자 메일의 RFC 822 Priority: 헤더 행을 사용하여 SMS 메일의 우선 순위 플래그를 설정합니다. 해당 헤더 행이 존재하지 않을 경우 DEFAULT\_PRIORITY 옵션을 사용하여 SMS 우선 순위 플래그를 설정합니다.

다음 표는 RFC 822 Priority: 헤더 행 값을 SMS 우선 순위 플래그로 변환하는 데 사용되는 매핑을 보여 줍니다.

**표 D-11** Priority: 헤더를 SMS 우선 순위 플래그로 변환하기 위한 매핑

| RFC 822  | SMS 우선 순위 플래그 |       |       |
|----------|---------------|-------|-------|
| 우선 순위: 값 | GSM           | TDMA  | CDMA  |
| 세 번째     | 낮음(0)         | 대량(0) | 중간(0) |
| 두 번째     | 낮음(0)         | 대량(0) | 중간(0) |
| 낮음       | 낮음(0)         | 대량(0) | 중간(0) |
| 중간       | 낮음(0)         | 중간(1) | 중간(0) |
| 높음       | 우선 순위(1)      | 높음(2) | 높음(2) |

### DEFAULT\_PRIVACY

(경수, -1, 0 - 255) SMS 메일에서 개인 정보 플래그를 설정할지 여부 및 사용할 값은 DEFAULT\_PRIVACY와 USE\_HEADER\_SENSITIVITY 옵션으로 제어합니다. 기본적으로 DEFAULT\_PRIVACY에는 -1 값이 사용됩니다. 다음 표 D-12에서는 DEFAULT\_PRIVACY 및 USE\_HEADER\_SENSITIVITY 옵션을 다양한 값으로 설정한 결과를 보여 줍니다.

**표 D-12** DEFAULT\_PRIVACY 및 USE\_HEADER\_SENSITIVITY에 대한 결과 값

| DEFAULT_PRIVACY | USE_HEADER_SENSITIVITY | 결과                                                                     |
|-----------------|------------------------|------------------------------------------------------------------------|
| -1              | 0                      | SMS 개인 정보 플래그가 SMS 메일에서 절대 설정되지 않습니다.                                  |
| n >= 0          | 0                      | SMS 개인 정보 플래그가 항상 값 n으로 설정됩니다.<br>RFC 822 Sensitivity: 헤더 행은 항상 무시됩니다. |

**표 D-12** DEFAULT\_PRIVACY 및 USE\_HEADER\_SENSITIVITY에 대한 결과 값

| DEFAULT_PRIVACY | USE_HEADER_SENSITIVITY | 결과                                                                                                                                 |
|-----------------|------------------------|------------------------------------------------------------------------------------------------------------------------------------|
| -1(기본값)         | 1(기본값)                 | 원본 전자 메일에 RFC 822 Sensitivity:헤더 행이 있을 경우에만 SMS 메일의 개인 정보 플래그가 설정됩니다. 이 경우 SMS 개인 정보 플래그는 Sensitivity:헤더 행 값에 해당하도록 설정됩니다. 기본값입니다. |
| n >= 0          | 1                      | SMS 메일의 개인 정보 플래그가 원본 전자 메일의 RFC 822 Sensitivity:헤더 행에 해당하도록 설정됩니다. 전자 메일에 Sensitivity: 헤더 행이 없을 경우 SMS 개인 정보 플래그의 값은 n으로 설정됩니다.   |

다음 표 D-13에서는 개인 정보 값의 SMS 해석을 보여 줍니다.

**표 D-13** 개인 정보 값의 SMS 해석

| 값    | 설명      |
|------|---------|
| 0    | 제한 없음   |
| 1    | 제한됨     |
| 2    | 기밀      |
| 3    | 비밀      |
| >= 4 | 정의되지 않음 |

RFC 822 Sensitivity: 헤더 행 값을 SMS 개인 정보 값으로 변환하는 데 사용되는 매핑은 다음 표 D-14에 나와 있습니다.

**표 D-14** Sensitivity: 헤더를 SMS 우선 순위 값으로 변환하기 위한 매핑

| RFC 822 Sensitivity: 값 | SMS 개인 정보 값 |
|------------------------|-------------|
| 개인                     | 1(제한됨)      |
| 비공개                    | 2(기밀)       |
| 회사 기밀                  | 3(비밀)       |

**DEFAULT\_SERVICE\_TYPE**

(문자열, 0 - 5바이트) 채널에 의해 생성되는 SMS 메일과 연관시킬 서비스 유형입니다. 기본적으로 서비스 유형은 지정되지 않습니다(즉, 길이가 0인 문자열이 사용됨). 일반적인 몇 가지 서비스 유형으로는 CMT(Cellular Messaging), CPT(Cellular Paging), VMN(Voice Mail Notification), VMA(Voice Mail Alerting), WAP(Wireless Application Protocol) 및 USSD(Unstructured Supplementary Data Services)가 있습니다.

**DEFAULT\_SOURCE\_ADDRESS**

(문자열, 0 - 20바이트) 전자 메일에서 생성되는 SMS 메일에 사용할 소스 주소입니다. USE\_HEADER\_FROM=1이면 전자 메일 발송자 주소가 이 옵션으로 지정한 값보다 우선한다는 것에 주의합니다. 기본적으로 값을 사용하지 않도록 0이 설정됩니다.

**DEFAULT\_SOURCE\_NPI**

(정수, 0 - 255) 기본적으로 소스 주소에는 NPI 값으로 0이 할당됩니다. 이 옵션을 사용하면 0부터 255까지 범위의 대체 정수 값이 할당될 수 있습니다. 일반 NPI 값을 보여주는 표는 [DEFAULT\\_DESTINATION\\_NPI](#) 옵션 설명을 참조하십시오.

**DEFAULT\_SOURCE\_TON**

(integer, 0 - 255) 기본적으로 소스 주소에는 TON 지정자 값으로 0이 할당됩니다. 이 옵션을 사용하면 0부터 255까지 범위의 대체 정수 값이 할당될 수 있습니다. 일반 TON 값을 보여주는 표는 [DEFAULT\\_DESTINATION\\_TON](#) 옵션 설명을 참조하십시오.

**DEFAULT\_VALIDITY\_PERIOD**

(문자열, 0 - 252바이트) 기본적으로 SMS 메일에는 상대적인 유효 기간이 지정되지 않으며 대신 SMSC의 기본값이 사용됩니다. 상대적인 다른 유효 기간을 지정하려면 이 옵션을 사용합니다. 값은 초, 분, 시 또는 일 단위로 지정할 수 있습니다. 다음 표 D-15에는 이 옵션의 여러 값에 대한 형식과 설명이 나와 있습니다.

**표 D-15** DEFAULT\_VALIDITY\_PERIOD의 형식 및 값

| 형식   | 설명                  |
|------|---------------------|
| mm   | 암시적 초 단위(예: 604800) |
| mmms | 초 단위(예: 604800s)    |
| mmmm | 분 단위(예: 10080m)     |
| mmmh | 시간 단위(예: 168h)      |
| mmnd | 일 단위(예: 7d)         |

0, 0s, 0m, 0h 또는 0d 지정을 사용하여 SMSC의 기본 유효 기간을 선택할 수 있습니다. 즉, 0, 0s, 0m, 0h 또는 0d 지정이 사용되면 생성된 SMS 메일의 유효 기간에 빈 문자열이 지정됩니다.

이 옵션은 UTC 형식의 값을 허용하지 않습니다.

### **DESTINATION\_ADDRESS\_NUMERIC**

(0 또는 1) 전자 메일 봉투 To: 주소에서 추출된 SMS 대상 주소의 숫자가 아닌 모든 문자를 스트라이프하려면 이 옵션을 사용합니다. 예를 들어, 다음 봉투 To: 주소는

"(800) 555-1212"@sms.siroe.com

다음과 같이 줄어듭니다.

8005551212@sms.siroe.com

이 스트라이핑을 사용하려면 해당 옵션의 값을 1로 지정합니다. 기본적으로 이 스트라이핑은 사용 불가능하며 옵션 값 0에 해당합니다. 스트라이핑이 사용 가능한 경우 대상 주소 접두어가 **DESTINATION\_ADDRESS\_PREFIX** 옵션을 통해 추가되기 전에 스트라이핑이 수행됩니다.

### **DESTINATION\_ADDRESS\_PREFIX**

(문자열) 경우에 따라 고정된 텍스트 문자열(예: "+"를 모든 SMS 대상 주소의 접두어로 사용해야 할 수 있습니다. 이 옵션을 사용하면 이러한 접두어를 지정할 수 있습니다. 지정된 접두어는 모든 SMS 대상 주소(해당 접두어가 없는)에 추가됩니다.

**DESTINATION\_ADDRESS\_NUMERIC** 옵션에 의해 스트라이프되는 것을 방지하기 위해 이 옵션은 **DESTINATION\_ADDRESS\_NUMERIC** 옵션 다음에 적용됩니다.

### **PROFILE**

(문자열) SMSC와 함께 사용할 SMS 프로필을 지정합니다. 가능한 값은 GSM, TDMA 및 CDMA입니다. 지정하지 않을 경우 GSM이 사용됩니다. 이 옵션은 **DEFAULT\_PRIORITY** 및 **DEFAULT\_PRIVACY**와 같은 다른 채널 옵션의 기본값을 선택하는 데만 사용됩니다.

### **USE\_SAR**

(0 또는 1) 아주 큰 전자 메일을 여러 SMS 메일로 분리해야 할 수 있습니다. 이 경우 개별 SMS 메일은 선택적으로 SMS sar\_ 필드를 사용하여 순서 지정 정보를 추가할 수 있습니다. 이로 인해 "분할된" SMS 메일이 생성되며 수신 단말기는 이러한 SMS 메일을 단일 SMS 메일로 다시 어셈블할 수 있습니다. 해당되는 경우 **USE\_SAR=1**을 지정하여 이 순서 지정 정보가 추가됨을 나타냅니다. 기본값은 순서 지정 정보를 추가하지 않는 것이며 이것은 **USE\_SAR=0**에 해당합니다.

USE\_SAR=1을 지정하면 REVERSE\_ORDER 옵션이 무시됩니다.

## SMPP 옵션

다음 옵션을 사용하면 SMPP 프로토콜 매개 변수를 지정할 수 있습니다. 문자열 "ESME\_"로 시작하는 이름을 가진 옵션은 MTA가 ESME(External Short Message Entity)로 작동할 때, 즉 MTA가 SMS 메일을 SMPP 서버의 관련 SMSC에 전송하기 위해 SMPP 서버에 바인드할 때 MTA를 식별하는 역할을 수행합니다.

### ESME\_ADDRESS\_NPI

(정수, 0 - 255) 기본적으로 바인드 작업은 ESME NPI 값으로 알 수 없는 NPI를 나타내는 0을 지정합니다. 이 옵션을 사용하면 0부터 255까지 범위의 대체 정수 값이 할당될 수 있습니다. 일반 NPI 값을 보여주는 표는 DEFAULT\_DESTINATION\_NPI 옵션 설명을 참조하십시오.

### ESME\_ADDRESS\_TON

(정수, 0 - 255) 기본적으로 바인드 작업은 ESME TON 값으로 0을 지정합니다. 이 옵션을 사용하면 0부터 255까지 범위의 대체 정수 값이 할당될 수 있습니다. 일반 TON 값을 보여주는 표는 DEFAULT\_DESTINATION\_TON 옵션 설명을 참조하십시오.

### ESME\_IP\_ADDRESS

(문자열, 0 - 15바이트) SMPP 서버에 바인드할 때 BIND PDU는 클라이언트의(즉, ESME) 주소 범위가 IP 주소임을 나타냅니다. 이것은 TON과 NPI를 각각 0x00 및 0x0d로 지정하는 방법으로 수행합니다. 그런 다음 주소 범위 필드의 값이 SMS 채널을 실행하는 호스트의 IP 주소로 설정됩니다. IP 주소를 점으로 구분된 십진수 형식(예: 127.0.0.1)으로 지정합니다.

### ESME\_PASSWORD

(문자열, 0 - 8바이트) SMPP 서버에 바인드할 때 비밀번호가 필요할 수 있습니다. 그럴 경우 이 옵션을 사용하여 비밀번호를 지정합니다. 기본적으로 길이가 0인 비밀번호 문자열이 제공됩니다.

### ESME\_SYSTEM\_ID

(문자열, 0 - 15 바이트) SMPP 서버에 바인드할 때 MTA의 시스템 아이디가 제공될 수 있습니다. 기본적으로 시스템 아이디는 지정되지 않습니다(즉, 길이가 0인 문자열이 사용됨). 시스템 아이디를 지정하려면 이 옵션을 사용합니다.

### ESME\_SYSTEM\_TYPE

(문자열, 0 - 12바이트) SMPP 서버에 바인드할 때 MTA의 시스템 유형이 제공될 수 있습니다. 기본적으로 시스템 유형은 지정되지 않습니다(즉, 길이가 0인 문자열이 사용됨).



**MAX\_PAGES\_PER\_BIND**

(정수, >= 0) 일부 SMPP 서버는 단일 바운드 세션 도중 전송되는 최대 SMS 메일 수를 제한할 수 있습니다. 이러한 상황에서 이 옵션을 사용하면 단일 세션 동안에 전송할 최대 SMS 메일 수를 지정할 수 있습니다. 지정된 한도에 도달하면 채널은 바인드 해제를 수행하고 TCP/IP 연결을 닫았다가 다시 연결한 후에 바인드를 다시 수행합니다.

기본적으로 MAX\_PAGES\_PER\_BIND에 값 1024가 사용됩니다. 채널은 또한 ESME\_RTHROTTLED 오류를 감지하고 이에 따라 채널의 단일 실행 동안에 MAX\_PAGES\_PER\_BIND를 조정합니다.

**REVERSE\_ORDER**

(0 또는 1) 전자 메일에서 둘 이상의 SMS 메일을 생성할 경우 이러한 SMS 메일을 순차적 순서(REVERSE\_ORDER=0) 또는 역순차적 순서(REVERSE\_ORDER=1)로 SMSC에 전송할 수 있습니다. 역순차적 순서는 수신 단말기에서 마지막으로 받은 메일을 가장 먼저 표시할 경우에 유용합니다. 이 경우 마지막으로 받은 메일은 전자 메일의 마지막 부분이 아니라 첫 번째 부분이 됩니다. 기본적으로 REVERSE\_ORDER=1이 사용됩니다.

USE\_SAR=1을 지정하면 이 옵션이 무시됩니다.

**SMPP\_MAX\_CONNECTIONS**

(정수, 1 - 50) 이 옵션은 프로세스당 최대 동시 SMPP 연결 수를 제어합니다. 각 연결에 연관된 스레드가 있으므로 이 옵션은 또한 프로세스당 최대 "작업자" 스레드 수를 제한합니다. 기본적으로 SMPP\_MAX\_CONNECTIONS=20입니다.

**SMPP\_PORT**

(정수, 1 - 65535) SMPP 서버가 수신하는 TCP 포트는 이 옵션이나 port 채널 키워드를 사용하여 지정할 수 있습니다. 이 포트 번호는 이러한 두 기법 중 하나를 통해 지정해야 합니다. 두 기법 모두를 사용하여 지정할 경우 SMPP\_PORT 옵션을 사용하여 설정한 값이 우선합니다. 이 옵션에는 기본값이 없습니다.

양방향 SMS의 경우 SMPP 릴레이를 위한 LISTEN\_PORT와 동일한 포트인지 확인합니다.

**SMPP\_SERVER**

(문자열, 1 - 252 바이트) 단방향 SMS의 경우 연결할 SMPP 서버의 IP 호스트 이름은 채널과 연관된 공식 호스트 이름입니다(즉, MTA 구성에서 채널 정의의 두 번째 행에 표시된 호스트 이름). 이 옵션을 사용하면 채널 정의에 지정된 이름을 무시하는 다른 호스트 이름이나 IP 주소를 지정할 수 있습니다. IP 주소를 지정할 때는 점으로 구분된 십진수 표기법(예: 127.0.0.1)을 사용합니다.

양방향 SMS의 경우 SMS 게이트웨이 서버의 호스트 이름이나 IP 주소를 가리키도록 설정합니다. SMPP 릴레이의 LISTEN\_INTERFACE\_ADDRESS 옵션을 사용할 경우 지정된 네트워크 인터페이스 주소와 연관된 호스트 이름이나 IP 주소를 사용해야 합니다.

### TIMEOUT

(정수, >= 2) SMPP 서버에 데이터를 쓰거나 SMPP 서버로부터 데이터를 받기 위해 기다릴 때 기본적으로 30초의 시간 초과가 사용됩니다. 다른 시간 초과 값을 초 단위로 지정하려면 TIMEOUT 옵션을 사용합니다. 지정된 값은 최소 1초 이상이어야 합니다.

### 현지화 옵션

SMS 메일 구성 시 SMS 채널은 SMS 메일에 포함할 여러 고정 텍스트 문자열을 가집니다. 예를 들어, 이러한 문자열은 전자 메일의 From:주소 및 Subject:헤더 행을 소개합니다. 이 절에 설명된 채널 옵션을 사용하면 이러한 문자열의 버전을 다른 언어로 지정한 다음 채널의 기본 언어를 지정할 수 있습니다. 코드 예 D-2에서는 옵션 파일의 언어 부분을 보여 줍니다.

#### 코드 예 D-2

채널 옵션 파일의 언어 지정 부분

```
LANGUAGE=default-language
```

```
[language=i-default]
FROM_PREFIX=From:
SUBJECT_PREFIX=Subj:
CONTENT_PREFIX=Msg:
LINE_STOP=
NO_MESSAGE=[no message]
REPLY_PREFIX=Re:
```

```
[language=en]
FROM_PREFIX=From:
SUBJECT_PREFIX=Subj:
CONTENT_PREFIX=Msg:
LINE_STOP=
NO_MESSAGE=[no message]
REPLY_PREFIX=Re:
```

```
...
```

각 [language=x] 블록 내에서 해당 언어와 관련된 현지화 옵션을 지정할 수 있습니다. 이 블록 안에 특정 옵션을 지정하지 않을 경우 해당 옵션의 전역 값이 사용됩니다. [language=x] 블록 외부에 지정된 현지화 옵션은 해당 옵션의 전역 값을 설정합니다.

아래 나열된 옵션의 경우 US-ASCII 또는 UTF-8 문자 세트를 사용하여 문자열 값을 지정해야 합니다. US-ASCII 문자 세트는 UTF-8 문자 세트의 특수한 경우입니다.

### ***CONTENT\_PREFIX***

(문자열, 0 - 252 바이트) SMS 메일에서 전자 메일의 내용 앞에 포함되는 텍스트 문자열입니다. 기본 전역 값은 US-ASCII 문자열 "Msg"입니다.

### ***DSN\_DELAYED\_FORMAT***

(문자열, 0-256 자) 전달 지연 알림에 대한 서식 지정 문자열입니다. 기본적으로 이 옵션에는 빈 문자열이 사용되며 이 경우 지연 알림이 SMS로 변환되지 않습니다. 이 옵션을 적용하려면 [GATEWAY\\_NOTIFICATIONS](#)가 1로 설정되어야 합니다. [GATEWAY\\_NOTIFICATIONS](#)=0일 경우 이 옵션은 무시됩니다.

### ***DSN\_FAILED\_FORMAT***

(문자열, 0-256 자) 영구 전달 실패 알림의 서식 지정 문자열입니다. 이 옵션의 기본값은 다음 문자열입니다.

Unable to deliver your message to \$a; no further delivery attempts will be made.

실패한 알림이 변환되는 것을 방지하려면 이 옵션에 빈 문자열을 지정합니다. 이 옵션을 적용하려면 [GATEWAY\\_NOTIFICATIONS](#)가 1로 설정되어야 합니다.

[GATEWAY\\_NOTIFICATIONS](#)=0일 경우 이 옵션은 무시됩니다.

### ***DSN\_RELAYED\_FORMAT***

(문자열, 0-256 자) 릴레이 알림의 서식 지정 문자열입니다. 기본값은 다음 문자열입니다.

Your message to \$a has been relayed to a messaging system which may not provide a final delivery confirmation

릴레이 알림이 변환되는 것을 방지하려면 이 옵션에 빈 문자열을 지정합니다. 이 옵션을 적용하려면 [GATEWAY\\_NOTIFICATIONS](#)가 1로 설정되어야 합니다. [GATEWAY\\_NOTIFICATIONS](#)=0일 경우 이 옵션은 무시됩니다.

### ***DSN\_SUCCESS\_FORMAT***

(문자열, 0-256 자) 성공한 전달 알림의 서식 지정 문자열입니다. 기본값은 다음 문자열입니다.

Your message to \$a has been delivered

성공한 전달 알림이 변환되는 것을 방지하려면 이 옵션에 빈 문자열을 지정합니다. 이 옵션을 적용하려면 [GATEWAY\\_NOTIFICATIONS](#)가 1로 설정되어야 합니다.

[GATEWAY\\_NOTIFICATIONS](#)=0일 경우 이 옵션은 무시됩니다.

**FROM\_FORMAT**

(문자열, 0 - 252 바이트) SMS 메일에 삽입할 메일 발송자 정보의 서식 지정을 위한 서식 지정 템플릿입니다. 기본 전역 값은 메일 발송자의 전자 메일 주소로 대체되는 US-ASCII 문자열 "\$a"입니다. 자세한 내용은 909페이지의 "서식 지정 템플릿"를 참조하십시오.

**FROM\_NONE**

(문자열, 0 - 252 바이트) 표시할 메일 발송자 주소가 없을 경우 SMS 메일에 포함할 텍스트 문자열입니다. 기본 전역 값은 빈 문자열입니다.

사이트는 일반적으로 메일 발송자의 주소가 없는 전자 메일을 거부하므로 이 옵션은 거의 사용되지 않습니다.

**LANGUAGE**

(문자열, 0 - 40 바이트) 텍스트 문자열을 선택할 기본 언어 그룹입니다. 값을 지정하지 않을 경우 호스트의 기본 로캘 지정에서 언어가 파생됩니다. 호스트의 로캘 지정을 사용할 수 없거나 "C"에 해당할 경우 i-default가 사용됩니다. i-default는 "전세계 사용자를 대상으로 하는 영어 텍스트"에 해당합니다.

**LINE\_STOP**

(문자열, 0 - 252 바이트) SMS 메일에서 전자 메일로부터 추출한 행 사이에 포함할 텍스트 문자열입니다. 기본 전역 값은 US-ASCII 공백 문자(" ")입니다.

**NO\_MESSAGE**

(문자열, 0 - 252 바이트) 전자 메일에 내용이 없음을 나타내기 위해 SMS 메일에 포함할 텍스트 문자열입니다. 기본 전역 값은 US-ASCII 문자열 "[no message]"입니다.

**SUBJECT\_FORMAT**

(문자열, 0 - 252 바이트) SMS 메일에 표시할 Subject: 헤더 행 내용의 서식 지정을 위한 서식 지정 템플릿입니다. 이 옵션의 전역 기본값은 US-ASCII 문자열 "(\$s)"입니다. 자세한 내용은 909페이지의 "서식 지정 템플릿"를 참조하십시오.

Subject: 헤더 행이 없거나 해당 헤더 행의 내용이 비어 있는 경우의 처리 방법은 SUBJECT\_NONE 옵션을 참조하십시오.

**SUBJECT\_NONE**

(문자열, 0 - 252 바이트) 원본 전자 메일에 Subject: 헤더 행이 없거나 Subject: 헤더 행의 값이 빈 문자열일 경우 표시할 텍스트 문자열입니다. 이 옵션의 기본 전역 값은 빈 문자열입니다.

## DEBUG

(정수, 비트 마스크) 디버그 출력을 사용 가능하게 합니다. 기본값은 경고 및 오류 메시지를 선택하는 6입니다. 0이 아닌 모든 값은 채널 정의에서 master\_debug를 지정하는 것과 동일하게 채널 자체에 대한 디버그 출력을 사용 가능하게 합니다. 표 D-16에는 DEBUG 비트 마스크의 비트 값이 정의되어 있습니다.

**표 D-16** DEBUG 비트 마스크

| 비트   | 값    | 설명                                   |
|------|------|--------------------------------------|
| 0-31 | -1   | 매우 자세한 출력                            |
| 0    | 1    | 정보 메시지                               |
| 1    | 2    | 경고 메시지                               |
| 3    | 4    | 오류 메시지                               |
| 3    | 8    | 서브루틴 호출 추적                           |
| 4    | 16   | 해시 테이블 진단                            |
| 5    | 32   | I/O 진단, 수신                           |
| 6    | 64   | I/O 진단, 전송                           |
| 7    | 128  | SMS에서 전자 메일로의 변환 진단(모바일 원본 및 SMS 알림) |
| 8    | 256  | PDU 진단, 헤더 데이터                       |
| 9    | 512  | PDU 진단, 본문 데이터                       |
| 10   | 1024 | PDU 진단, 유형 길이 값 데이터                  |
| 11   | 2048 | 옵션 처리(모든 옵션 설정을 로그 파일로 보냄)           |

## 서식 지정 템플릿

FROM\_FORMAT, SUBJECT\_FORMAT 및 모든 DSN\_\* 채널 옵션으로 지정하는 서식 지정 템플릿은 리터럴 텍스트 및 대체 시퀀스의 조합을 포함하는 UTF-8 문자열입니다. 다음과 같은 샘플 전자 메일 주소를 가정합니다.

Jane Doe <user@siroe>

다음 표 D-17에서는 인식되는 대체 시퀀스를 보여 줍니다.

**표 D-17** 대체 시퀀스

| 시퀀스 | 설명                                                         |
|-----|------------------------------------------------------------|
| \$a | 메일 발송자의 전자 메일 주소에 있는 로컬 및 도메인 부분(예: "user@siroe")으로 교체됩니다. |

**표 D-17** 대체 시퀀스

| 시퀀스 | 설명                                                |
|-----|---------------------------------------------------|
| \$d | 메일 발송자의 전자 메일 주소에 있는 도메인 부분(예: "domain")으로 교체됩니다. |
| \$p | 메일 발송자의 전자 메일 주소에 있는 구 부분(예: "Jane Doe")으로 교체됩니다. |
| \$s | Subject: 헤더 행의 내용으로 교체합니다.                        |
| \$u | 메일 발송자의 전자 메일 주소에 있는 로컬 부분(예: "user")으로 교체됩니다.    |
| \x  | 리터럴 문자 "x"로 교체됩니다.                                |

예를 들어, 다음 서식 지정 템플리트는

From: \$a

다음 텍스트 문자열을 생성합니다.

From: user@siroe

다음 구조는

`${xy:alternate text}`

시퀀스 `x`와 연관된 텍스트로 대체하는 데 사용할 수 있습니다. 해당 텍스트가 빈 문자열인 경우 시퀀스 `y`와 연관된 텍스트가 대신 사용됩니다. 또한 위 구조는 해당 텍스트가 빈 문자열인 경우 대체 텍스트로 대체하는 데 사용할 수 있습니다. 예를 들어, 다음과 같은 서식 지정 템플리트를 가정합니다.

From: `${pa:unknown sender}`

구 부분을 포함하는 메일 발송자의 전자 메일 주소의 경우

John Doe <jdoe@siroe.com>

이 템플리트에서는 다음을 생성합니다.

From: John Doe

그러나 구가 없는 다음 주소의 경우

jdoe@siroe.com

이 템플리트는 다음을 생성합니다.

From: jdoe@siroe.com

빈 메일을 보낸 발송자 주소의 경우에는 다음을 생성합니다.

From: unknown sender

## SMS 채널 추가

둘 이상의 SMS 채널을 가지도록 MTA를 구성할 수 있습니다. 이는 일반적으로 다음 두 가지 이유 때문입니다.

### 1. 다른 SMPP 서버와 통신하려는 경우

단순히 추가 SMS 채널을 구성에 추가하면 됩니다. 이 과정에서 추가 SMS 채널에 (a) 다른 채널 이름을 제공하고 (b) 다른 호스트 이름을 연관시킵니다. 예를 들면 다음과 같습니다.

```
sms_mway port 55555 threaddepth 20
smpp.siroe.com
```

```
sms_ace port 777 threaddepth 20
sms.ace.net
```

새로운 다시 쓰기 규칙은 필요하지 않습니다. 직접적으로 일치되는 다시 쓰기 규칙이 없을 경우 **Messaging Server**는 연관된 호스트 이름을 가진 채널을 찾습니다. 예를 들어, `user@host.domain`으로 표시될 경우 **Messaging Server**는 "host.domain"이라는 이름의 채널을 찾습니다. 이러한 채널이 발견되면 메일은 해당 채널로 라우팅됩니다. 그렇지 않을 경우 서버는 다시 쓰기 규칙에서 ".domain"을 찾고, 없을 경우 점(".") 규칙을 찾습니다. 다시 쓰기 규칙에 대한 자세한 내용은 [281페이지의 11장, "다시 쓰기 규칙 구성"](#)을 참조하십시오.

### 2. 다른 채널 옵션을 사용하여 동일한 SMPP 서버와 통신하려는 경우

다른 채널 옵션을 사용하여 동일한 SMPP 서버와 통신하려면 각 채널 정의의 `SMPP_SERVER` 채널 옵션에서 동일한 SMPP 서버를 지정합니다.

이 기법을 사용해야 하는 이유는 두 개의 다른 채널이 동일한 공식 호스트 이름(즉, 채널 정의의 두 번째 행에 나열된 호스트 이름)을 가질 수 없기 때문입니다. 이러한 채널이 동일한 SMPP 서버와 통신할 수 있게 하려면 해당 채널 옵션 파일의 `SMPP_SERVER`에서 동일한 SMPP 서버를 지정하는 별개의 채널 두 개를 정의합니다.

예를 들어, 다음 채널 정의와

```
sms_mway_1 port 55555 threaddepth 20
SMS-DAEMON-1
```

```
sms_mway_2 port 55555 threaddepth 20
SMS-DAEMON-2
```

다음 다시 쓰기 규칙이 있다고 가정합니다.

```
sms-1.siroe.com $u%sms-1.siroe.com@SMS-DAEMON-1
sms-2.siroe.com $U%sms-2.siroe.com@SMS-DAEMON-2
```

이 경우에 동일한 SMPP 서버를 사용하기 위해 이러한 두 채널은 각각 해당 채널 옵션 파일에서 `SMPP_SERVER=smp.1.siroe.com`을 지정합니다.

## 전달 재시도 빈도 조정

SMPP 서버에 도달할 수 없는 경우와 같이 일시적인 오류로 인해 SMS 메일을 전달하지 못하면 전자 메일은 전달 대기열에 남아 있다가 나중에 다시 시도됩니다. 따로 구성하지 않은 경우에는 Job Controller에서 1시간 동안 전달을 다시 시도하지 않습니다. 그러나 SMS 메시징의 경우 1시간은 기다리는 시간으로 너무 깁니다. 이러한 경우에는 SMS 채널과 함께 backoff 채널 키워드를 사용하여 전달 시도에 보다 빠른 일정을 지정하는 것이 좋습니다. 예를 들면 다음과 같습니다.

```
sms_mway port 55555 threaddepth 20 \
  backoff pt2m pt5m pt10m pt30m notices 1
smp.1.siroe.com
```

위 설정에서는 첫 시도가 있은 후 2분, 5분 및 10분 후에 한 번씩 재전달이 시도되며 이러한 시도가 모두 실패할 경우 마지막으로 30분마다 재전달이 시도됩니다. notices 1 채널 키워드는 하루가 지나도록 메일을 전달할 수 없는 경우 해당 메일을 전달할 수 없는 것으로 반환합니다.

## 샘플 단방향 구성(MobileWay)

MTA SMS 채널은 모든 SMPP V3.4 호환 SMPP 서버에서 사용할 수 있습니다. 이 절에서는 구성 예를 제시하기 위해 MobileWay SMPP 서버에서 사용하도록 SMS 채널을 구성하는 방법에 대해 설명합니다. MobileWay(<http://www.mobileway.com/>)는 전역 데이터 및 SMS 연결의 주요 공급업체입니다. MobileWay를 통해 SMS 트래픽을 라우팅하면 전세계 대부분의 주요 SMS 네트워크상에 있는 SMS 가입자에 도달할 수 있습니다.

MobileWay를 통해 SMPP 계정을 요청할 때는 다음 질문에 답하라는 메시지가 나타날 수 있습니다.

- SMPP 클라이언트의 IP 주소: 인터넷 상의 다른 도메인에 표시된 것처럼 Messaging Server 시스템의 IP 주소를 제공합니다.



- 기본 유효 기간: 전송하는 SMS 메일에 유효 기간이 지정되지 않을 경우 MobileWay에서 사용하는 SMS 유효 기간입니다. 이 유효 기간이 만료될 때까지 전달할 수 없는 SMS 메일은 무시됩니다. 적절한 값(예: 2일, 7일 등)을 제공합니다.
- 창 크기: SMPP 클라이언트가 전송하는 최대 SMS 메일 수입니다. SMPP 클라이언트는 이 수를 초과할 경우 추가 SMS 메일을 전송하는 것을 중지하고 SMPP 서버의 응답을 기다립니다. 1의 메일 값을 제공해야 합니다.
- 시간대: Messaging Server 시스템이 작동하는 표준 시간대를 지정합니다. 표준 시간대는 GMT에서 오프셋으로 지정해야 합니다.
- 타임아웃: 단방향 SMS 메시징과는 관련이 없습니다.
- 아웃바운드 요청에 대한 IP 주소 및 TCP 포트: 단방향 SMS 메시징과는 관련이 없습니다.

위 질문에 대한 대답을 MobileWay에 제공하면 SMPP 서버와 통신하는 데 필요한 SMPP 계정 및 정보가 다음과 같이 제공됩니다.

```
Account Address: a.b.c.d:p
Account Login: system-id
Account Passwd: secret
```

계정 주소 필드는 연결할 MobileWay SMPP 서버의 IP 주소 a.b.c.d 및 TCP 포트 번호 p입니다. 이러한 값을 SMPP\_SERVER 및 SMPP\_PORT 채널 옵션에 사용합니다. 계정 로그인 및 비밀번호는 각각 ESME\_SYSTEM\_ID 및 ESME\_PASSWORD 채널 옵션에 사용할 값입니다. 이 정보를 사용하여 채널 옵션 파일에 다음을 포함해야 합니다.

```
SMPP_SERVER=a.b.c.d
SMPP_PORT=p
ESME_SYSTEM_ID=system-id
ESME_PASSWORD=secret
```

이제 MobileWay와 상호 작용하기 위해 다음과 같은 두 개의 추가 옵션 설정이 필요합니다.

```
ESME_ADDRESS_TON=0x01
DEFAULT_DESTINATION_TON=0x01
```

imta.cnf 파일의 다시 쓰기 규칙은 다음과 같이 나타낼 수 있습니다.

```
sms.your-domain $u@sms.your-domain
```

또한 imta.cnf 파일의 채널 정의는 다음과 같이 나타낼 수 있습니다.

```
sms_mobileway
sms.your-domain
```

일단 채널 옵션 파일, 다시 쓰기 규칙 및 채널 정의가 제대로 되면 테스트 메일을 보낼 수 있습니다. MobileWay는 다음과 같은 형식의 국제 주소 지정을 요구합니다.

```
<country-code><subscriber-number>
```

예를 들어, 가입자 번호가 (800) 555-1212인 북미 가입자에게 테스트 메일을 보내려면 전자 메일 주소를 다음과 같이 지정합니다.

```
+18005551212@sms.your-domain
```

## 디버깅

채널을 디버그하려면 채널 정의에서 `master_debug` 채널 키워드를 지정합니다. 예를 들면 다음과 같습니다.

```
sms_mway port 55555 threaddepth 20 \
  backoff pt2m pt5m pt10m pt30m notices 1 master_debug
```

`master_debug` 채널 키워드를 사용하면 채널 작업에 대한 기본 진단 정보가 채널의 로그 파일에 출력됩니다. 채널에서 수행한 SMPP 트랜잭션에 대한 자세한 진단 정보를 원할 경우에는 또한 해당 채널의 옵션 파일에서 다음을

```
DEBUG=-1
```

지정합니다.

## 양방향 SMS를 위한 SMS 채널 구성

SMS 채널 구성에 대한 일반 지침은 이전 [886페이지](#)의 "SMS 채널 구성" 절부터 설명된 항목을 참조하십시오. 다음 표 D-18에 나열된 사항을 제외하고 SMS 채널을 마치 원격 SMSC에 직접 연결하는 것처럼 구성합니다.

**표 D-18** 양방향 구성 예외

| 예외            | 설명                                                                                                                                                                              |
|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| master 채널 키워드 | master 채널 키워드를 제거합니다(있을 경우).<br>SMS 채널 구성에 더 이상 필요하지 않습니다.                                                                                                                      |
| SMPP_SERVER   | SMS 게이트웨이 서버의 호스트 이름이나 IP 주소를 가리키도록 설정합니다. SMPP 릴레이의 LISTEN_INTERFACE_ADDRESS 옵션( <a href="#">927페이지</a> 의 "구성 옵션" 참조)을 사용할 경우 지정된 네트워크 인터페이스 주소와 연관된 호스트 이름이나 IP 주소를 사용해야 합니다. |

**표 D-18** 양방향 구성 예외

| 예외                     | 설명                                                                                                |
|------------------------|---------------------------------------------------------------------------------------------------|
| SMPP_PORT              | SMPP 릴레이(924페이지의 "SMPP 릴레이" 참조)를 인스턴스화하는 데 사용되는 LISTEN_PORT 설정과 동일한 TCP 포트가 사용됩니다.                |
| DEFAULT_SOURCE_ADDRESS | 값을 선택한 다음 이 주소를 다시 게이트웨이 SMPP 서버로 라우팅하도록 원격 SMSC를 구성합니다. SMS 채널의 옵션 파일에서 이 옵션을 사용하여 선택한 값을 지정합니다. |
| GATEWAY_PROFILE        | 게이트웨이 프로필 이름과 일치하도록 설정합니다. 923페이지의 "게이트웨이 프로필"을 참조하십시오.                                           |
| USE_HEADER_FROM        | 0으로 설정합니다.                                                                                        |

다른 모든 채널은 SMS 채널 설명서에 설명된 대로 구성되어야 합니다.

921페이지의 "양방향 SMS 라우팅 설정"에 언급된 대로 원격 SMSC의 경우 LISTEN\_PORT 옵션에 지정된 TCP 포트 번호를 사용하여 DEFAULT\_SOURCE\_ADDRESS 채널 옵션에 정의된 SMS 주소를 게이트웨이의 SMPP 서버에 라우팅하도록 구성해야 합니다. LISTEN\_PORT를 지정하는 방법은 925페이지의 "SMPP 서버"를 참조하십시오.

여러 SMS 채널에서 동일한 SMPP 릴레이를 사용할 수 있습니다. 마찬가지로 여러 SMS 채널의 SMS 응답과 알림을 처리하기 위해 하나의 SMPP 서버 또는 게이트웨이만 필요합니다. 여러 릴레이, 서버 및 게이트웨이 프로필을 구성하는 기능은 구성 옵션을 통해 여러 다른 사용 특성을 구현하는데 필요합니다.

## SMS 게이트웨이 서버 작동 이론

SMS 게이트웨이 서버는 모바일에서 전송된 SMS 메일을 정확한 전자 메일 주소와 일치시키는 기법을 통해 양방향 SMS를 용이하게 합니다. 이 절은 다음과 같은 SMS 게이트웨이 서버 항목으로 구성되어 있습니다.

- 916페이지의 "SMS 게이트웨이 서버 기능"
- 916페이지의 "SMPP 릴레이 및 서버의 동작"
- 918페이지의 "SMS 릴레이 및 알림 처리"

## SMS 게이트웨이 서버 기능

SMS 게이트웨이 서버는 SMPP 릴레이와 서버의 기능을 동시에 수행합니다. SMS 게이트웨이 서버는 각 기능의 여러 "인스턴스화"를 가지도록 구성할 수 있습니다. 예를 들어, 각각 다른 TCP 포트나 네트워크 인터페이스를 수신하고 다른 원격 SMPP 서버로 릴레이하는 세 개의 다른 SMPP 릴레이를 가지도록 구성할 수 있습니다. 마찬가지로 각각 TCP 포트 및 네트워크 인터페이스의 다른 조합을 수신하는 네 개의 다른 SMPP 서버를 가지도록 SMS 게이트웨이 서버를 구성할 수 있습니다.

SMS 게이트웨이 서버는 SMS 메일을 전자 메일로 보내기 위한 0개 이상의 게이트웨이 프로필을 가질 수 있습니다. 각 게이트웨이 프로필은 해당 프로필과 일치하는 대상 SMS 주소, SMS 메일에서 대상 전자 메일 주소를 추출하는 방법, SMS에서 전자 메일로의 변환 프로세스가 가진 다양한 특성 등을 설명합니다. SMS 릴레이 또는 서버를 통해 SMS 게이트웨이 서버에 제공된 각 SMS 메일은 각 프로필과 비교됩니다. 일치하는 항목이 발견되면 해당 메일은 전자 메일로 라우팅됩니다.

마지막으로 게이트웨이 프로필은 또한 이전 ETM(Email-To-Mobile) 메일에 응답하여 원격 SMSC가 반환한 알림 메일을 처리하는 방법을 설명합니다.

## SMPP 릴레이 및 서버의 동작

SMPP 릴레이로 작동할 때 SMS 게이트웨이 서버는 로컬 SMPP 클라이언트의 모든 요청을 원격 SMPP 서버로 릴레이한 다음 원격 서버의 응답을 다시 릴레이하면서 가능한 투명하게 작업을 시도합니다. 그러나 다음 두 가지 경우는 예외입니다.

- 로컬 SMPP 클라이언트가 구성된 게이트웨이 프로필 중 하나와 일치하는 SMS 대상 주소를 가진 메일을 전송하면 전송된 SMS 메일은 직접 전자 메일로 되돌려 보내집니다. 즉, SMS 메일은 원격 SMPP 서버로 릴레이되지 않습니다.
- 로컬 또는 원격 SMPP 클라이언트가 이전에 SMPP 릴레이에 의해 생성된 고유한 SMS 소스 주소와 일치하는 SMS 대상 주소를 가진 메일을 전송하면 해당 SMS 메일은 이전에 릴레이된 메일에 대한 응답입니다. 이 응답은 원본 메일의 발송자에게 다시 전송됩니다.

일반적으로 SMS 게이트웨이 서버는 생성되는 고유한 SMS 소스 주소가 게이트웨이 프로필 중 하나와 일치하도록 구성됩니다.

---

**주** SMS 게이트웨이 서버의 SMPP 릴레이는 정규화된 Sun Java System SMPP 클라이언트, 즉 Sun Java System Messaging Server의 SMS 채널에 서만 사용하도록 되어 있습니다. 따라서 임의의 SMPP 클라이언트에서는 사용되지 않습니다.

---

SMPP 서버로 작동할 때 SMS 게이트웨이 서버는 다음과 같은 세 가지 경우에 SMS 메일을 전자 메일로 전송합니다.

- SMS 메일이 모바일에서 전송되었으며 게이트웨이 프로필과 일치할 경우
- SMS 메일이 모바일에서 전송되었으며 SMS 대상 주소가 이전에 생성된 고유한 SMS 소스 주소와 일치할 경우
- SMS 메일이 이전에 SMS 게이트웨이 서버의 SMPP 릴레이에 의해 릴레이된 ETM(Email-To-Mobile) 메일에 해당하는 SMS 알림인 경우

다른 모든 SMS 메일은 SMPP 서버에 의해 거부됩니다.

## 원격 SMPP에서 게이트웨이 SMPP로의 통신

원격 SMPP 클라이언트는 PDU(Protocol Data Unit)를 사용하여 게이트웨이 SMPP 서버와 통신합니다. 원격 SMPP 클라이언트는 게이트웨이 SMPP 서버가 응답하는 요청 PDU를 보냅니다. 게이트웨이 SMPP 서버는 동기식으로 작동합니다. 게이트웨이 SMPP 서버는 연결된 원격 SMPP 클라이언트의 다음 요청 PDU를 처리하기 전에 요청 PDU에 대한 응답을 완료합니다.

다음 표 D-19에는 게이트웨이 SMPP 서버가 처리하는 요청 PDU와 게이트웨이 SMPP 서버의 응답이 나열되어 있습니다.

**표 D-19** SMPP 서버 PDU(Protocol Data Unit)

| 요청 PDU                                         | SMPP 서버 응답                                                       |
|------------------------------------------------|------------------------------------------------------------------|
| BIND_TRANSMITTER<br>BIND_TRANSCEIVER<br>UNBIND | 적절한 응답 PDU로 응답합니다. 인증 자격 증명은 무시됩니다.                              |
| OUTBIND                                        | 게이트웨이 SMPP 서버가 BIND_RECEIVER PDU를 되돌려 보냅니다. 표시된 인증 자격 증명은 무시됩니다. |

**표 D-19** SMPP 서버 PDU(Protocol Data Unit)

| 요청 PDU               | SMPP 서버 응답                                                                                                              |
|----------------------|-------------------------------------------------------------------------------------------------------------------------|
| SUBMIT_SM<br>DATA_SM | 고유한 SMS 소스 주소나 게이트웨이 프로필의 SELECT_RE 설정을 사용하여 대상 SMS 주소와 일치시키려고 시도합니다. 둘 다 일치하지 않을 경우 ESME_RINVDSTADR 오류와 함께 PDU가 거부됩니다. |
| DELIVER_SM           | 기록 레코드에서 대상 SMS 주소나 수신 확인된 메일 아이디를 찾으려고 시도합니다. 둘 다 일치하지 않을 경우 ESME_RINVMSGID 오류를 반환합니다.                                 |
| BIND_RECEIVER        | 지원되지 않습니다. ESME_RINVCMDID 오류와 함께 GENERIC_NAK PDU를 반환합니다.                                                                |
| SUBMIT_MULTII        | 지원되지 않습니다. ESME_RINVCMDID 오류와 함께 GENERIC_NAK PDU를 반환합니다.                                                                |
| REPLACE_SM           | 지원되지 않습니다. ESME_RINVCMDID 오류와 함께 GENERIC_NAK PDU를 반환합니다.                                                                |
| CANCEL_SM            | 지원되지 않습니다. ESME_RINVCMDID 오류와 함께 GENERIC_NAK PDU를 반환합니다.                                                                |
| QUERY_SM             | 지원되지 않습니다. ESME_RINVCMDID 오류와 함께 GENERIC_NAK PDU를 반환합니다.                                                                |
| QUERY_LAST_MSGS      | 지원되지 않습니다. ESME_RINVCMDID 오류와 함께 GENERIC_NAK PDU를 반환합니다.                                                                |
| QUERY_MSG_DETAILS    | 지원되지 않습니다. ESME_RINVCMDID 오류와 함께 GENERIC_NAK PDU를 반환합니다.                                                                |
| ENQUIRE_LINK         | ENQUIRE_LINK_RESP PDU를 반환합니다.                                                                                           |
| ALERT_NOTIFICATION   | 허용되지만 무시됩니다.                                                                                                            |

## SMS 릴레이 및 알림 처리

SMS 게이트웨이 서버는 해당 SMPP 릴레이를 통해 릴레이된 각 SMS 메일의 기록 레코드를 유지 관리합니다. 기록 데이터를 사용하는 이유는 전자 메일을 SMS로 전송할 때 일반적으로 메일 발송자의 전자 메일 주소를 SMS 소스 주소로 변환할 수 없기 때문입니다. 이 경우 모든 SMS 응답과 알림이 이 SMS 소스 주소로 전송되므로 문제가 발생합니다. 이 문제는 자동으로 생성된 고유한 SMS 소스 주소를 릴레이된 메일에서 사용하는 방법으로 해결합니다. 그런 다음 원격 SMSC는 이러한 SMS 소스 주소를 다시 게이트웨이 SMPP 서버로 라우팅하도록 구성됩니다.

기록 데이터는 메일 아이디와 생성된 고유한 SMS 소스 주소의 메모리 내장 해시 테이블로 표시됩니다. 또한 이 데이터는 연관된 전자 메일 원본 데이터와 함께 디스크에 저장됩니다. 이러한 디스크 기반 저장소는 일련의 파일로써 각 파일은 트랜잭션의 HASH\_FILE\_ROLLOVER\_PERIOD 기간(초 단위이며 기본값은 30분)을 나타냅니다. 각 파일은 RECORD\_LIFETIME 기간(초 단위이며 기본값은 3일) 동안 보관됩니다. 기록 데이터의 메모리 내장 및 디스크 내장 자원 요구 사항에 대한 자세한 내용은 *Sun Java System Messaging Server Deployment Planning Guide*(<http://docs.sun.com/doc/819-0063>)를 참조하십시오.

각 레코드는 다음 세 가지 구성 요소를 가집니다.

- 전자 메일 원본 데이터(예: 봉투 From: 및 To: 주소). MTA SMS 채널에서 메일을 전송할 때 이 데이터를 제공합니다.
- SMPP 릴레이에 의해 생성되며 릴레이된 SMS 메일에 삽입되는 고유한 SMS 소스 주소
- 원격 SMSC의 SMPP 서버에서 전송을 수락할 때 반환하는 수신 확인된 결과 메일 아이디

## SMS 응답의 라우팅 프로세스

게이트웨이 SMPP 릴레이 및 서버는 기록 레코드를 사용하여 SMS 응답, 알림 및 모바일에서 전송된 메일을 처리합니다. SMS 메일이 SMPP 릴레이 또는 서버에 제공될 때 다음 라우팅 프로세스를 따릅니다.

1. SMPP 릴레이가 이전에 생성한 일치하는 고유한 SMS 소스 주소가 있는지 확인하기 위해 SMS 대상 주소가 기록 레코드와 비교됩니다. 일치하는 항목이 발견된 경우 **단계 6**으로 이동합니다.
2. 일치하는 항목이 없지만 메일이 SMS 알림(SMPP DELIVER\_SM PDU)일 경우 수신 확인된 메일 아이디(존재할 경우)가 기록 레코드와 비교됩니다. 일치하는 항목이 발견된 경우 **단계 8**로 이동합니다. [SMS 게이트웨이 서버는 실제로 이러한 항목을 SMPP 릴레이 또는 SMPP 서버에 제공하는 것을 허용합니다.]
3. 일치하는 항목이 없을 경우 대상 SMS 주소가 구성된 각 게이트웨이 프로필의 SELECT\_RE 옵션 표현식과 비교됩니다. 일치하는 항목이 발견된 경우 **단계 9**로 이동합니다.
4. 일치하는 항목이 없고 SMS 메일이 게이트웨이 SMPP 릴레이에 제공된 경우 메일은 원격 SMPP 서버로 릴레이됩니다.
5. 일치하는 항목이 없고 SMS 메일이 게이트웨이 SMPP 서버에 제공된 경우 해당 메일이 잘못된 것으로 결정되어 SMPP 응답 PDU에서 오류 응답이 반환됩니다. 전자 메일에서 SMS로의 경우 최종적으로 NDN(Non Delivery Notification)이 생성됩니다.

6. 일치하는 고유한 SMS 소스 주소가 발견된 경우 SMS 메일을 추가로 검사하여 응답 또는 알림 메일인지 확인합니다. 알림 메일이 되려면 수신 확인된 메일 아이디가 있는 SUBMIT\_SM PDU여야 합니다. 그렇지 않을 경우 해당 메일은 응답으로 간주됩니다.
7. 응답일 경우 SMS 메일은 기록 레코드의 원본 전자 메일 정보를 사용하여 전자 메일로 변환됩니다.
8. 알림일 경우 SMS 메일은 RFC 1892-1894에 따라 전자 메일 DSN(Delivery Status Notification)으로 변환됩니다. 이 때 원본 전자 메일의 ESMTP NOTIFY 플래그(RFC 1891)가 적용됩니다. 예를 들어, SMS 메일이 "성공" DSN이지만 원본 전자 메일이 "실패" 알림만 요청한 경우 SMS 알림은 무시됩니다.
9. 대상 SMS 주소가 구성된 게이트웨이 프로필의 SELECT\_RE 옵션과 일치할 경우 SMS 메일은 모바일에서 전송된 메일로 간주되며 해당 게이트웨이 프로필에 대한 PARSE\_RE\_n 규칙에 따라 다시 전자 메일로 변환됩니다. 변환이 실패할 경우 SMS 메일이 잘못된 것이므로 오류 응답이 반환됩니다.

## SMS 게이트웨이 서버 구성

이 절에서는 ETM(Email-To-Mobile) 및 MTE(Mobile-To-Email) 기능을 모두 사용하도록 SMS 게이트웨이 서버를 설정하는 방법에 대해 설명합니다. 이 절은 다음 내용으로 구성되어 있습니다.

- 921페이지의 "양방향 SMS 라우팅 설정"
- 922페이지의 "SMS 게이트웨이 서버 사용 가능/불가능하게 하기"
- 922페이지의 "SMS 게이트웨이 서버 시작 및 중지"
- 923페이지의 "SMS 게이트웨이 서버 구성 파일"
- 923페이지의 "게이트웨이 서버에서 ETM(Email-To-Mobile) 구성"
- 926페이지의 "MTE(Mobile-To-Email) 작업 구성"
- 927페이지의 "구성 옵션"
- 941페이지의 "양방향 SMS의 구성 예"



## 양방향 SMS 라우팅 설정

MTA와 SMSC 간에 양방향 전자 메일 및 SMS 라우팅을 설정하려면 다음 3단계 과정을 수행하는 것이 좋습니다.

- **SMS 주소 접두어 설정** - SMS 주소 접두어를 선택합니다. 10자 이하인 모든 접두어를 사용할 수 있습니다.
- **게이트웨이 프로파일 설정** - SMS 게이트웨이 서버에 사용하기 위해 접두어를 반전시킵니다(게이트웨이 프로파일을 설정함으로써).
- **SMSC 구성** - 접두어로 시작하는 SMS 대상 주소를 SMS 게이트웨이 SMPP 서버로 라우팅하도록 SMSC를 구성합니다. 모바일에서 전송한 전자 메일은 접두어만 가집니다. 응답과 알림은 정확하게 10개의 십진수가 뒤에 오는 접두어를 가집니다.

### SMS 주소 접두어 설정

MTA SMS 채널에 의해 생성되는 소스 SMS 주소는 선택된 SMS 주소 접두어와 일치하도록 설정해야 합니다. 그러려면 다음을 설정합니다.

- MTA SMS 채널 옵션

```
USE_HEADER_FROM=0
```

```
DEFAULT_SOURCE_ADDRESS=prefix
```

첫 번째 설정은 채널이 전자 메일에 포함된 정보에서 SMS 소스 주소를 설정하지 않도록 합니다. 두 번째 설정은 다른 소스에서 설정되지 않은 경우 SMS 소스 주소가 선택된 접두어로 설정되도록 합니다.

- 해당 접두어를 전자 메일을 수락하여 라우팅할 SMS 대상 주소로 인식합니다. 그러려면 SELECT\_RE 게이트웨이 프로파일 옵션을 다음과 같이 지정합니다.

```
SELECT_RE=prefix
```

### 게이트웨이 프로파일 설정

릴레이된 모든 SMS 소스 주소가 고유하도록 SMS 게이트웨이 서버의 게이트웨이 프로파일을 설정해야 합니다. 이것은 기본 설정이지만 게이트웨이 프로파일 옵션

MAKE\_SOURCE\_ADDRESSES\_UNIQUE=1을 지정하여 명시적으로 설정할 수 있습니다. 결과적으로 다음 형식의 릴레이된 SMS 소스 주소가 만들어집니다.

```
prefixnnnnnnnnnn
```

여기서 *nnnnnnnnnn*은 고유한 10자리 십진수가 됩니다.

## SMSC 구성

마지막으로 접두어(단순히 접두어만 또는 접두어와 10자리 숫자)와 일치하는 모든 SMS 대상 주소를 SMS 게이트웨이 서버의 SMPP 서버로 라우팅하도록 SMSC를 구성해야 합니다. 이러한 라우팅을 위한 정규식은 다음과 유사합니다.

```
prefix([0-9]{10,10}){0,1}
```

여기서 *prefix*는 DEFAULT\_SOURCE\_ADDRESS의 값이고 [0-9]는 10자리 숫자에 허용되는 값이며 {10, 10}은 최소한 10자리 및 최대한 10자리 숫자가 존재한다는 것을 지정하고 마지막으로 {0, 1}은 0개 또는 1개의 10자리 숫자가 존재할 수 있다는 것을 지정합니다.

## SMS 게이트웨이 서버 사용 가능/불가능하게 하기

- SMS 게이트웨이 서버를 사용하려면 **configutil** 매개 변수 `local.msggateway.enable`의 값을 1로 설정해야 합니다. 다음 구성 유틸리티 명령을 사용하여 이 값을 설정합니다.

```
# configutil -o local.msggateway.enable -v 1
```

- 게이트웨이 서버를 사용하지 않으려면 다음 명령을 사용하여 `local.msggateway.enable`의 값을 0으로 설정합니다.

```
# configutil -o local.msggateway.enable -v 0
```

## SMS 게이트웨이 서버 시작 및 중지

SMS 게이트웨이 서버가 사용 가능하게 된 후 다음 명령을 사용하여 서버를 시작 및 중지할 수 있습니다.

```
# start-msg sms
```

및

```
# stop-msg sms
```

## SMS 게이트웨이 서버 구성 파일

SMS 게이트웨이 서버가 작동하려면 구성 파일이 필요합니다. 구성 파일은 UTF-8을 사용하여 인코딩되는 유니코드 텍스트 파일이며 ASCII 텍스트 파일이 될 수 있습니다. 구성 파일의 이름은 다음과 같아야 합니다.

```
installation-directory/config/sms_gateway.cnf
```

구성 파일의 각 옵션 설정은 다음 형식을 가집니다.

```
option-name=option-value
```

옵션 그룹의 일부인 옵션은 다음 형식으로 표시됩니다.

```
[group-type=group-name]
option-name-1=option-value-1
option-name-2=option-value-2
...
option-name-n=option-value-n
```

## 게이트웨이 서버에서 ETM(Email-To-Mobile) 구성

양방향 SMS의 ETM(Email-To-Mobile) 부분을 구현하려면 다음을 구성해야 합니다.

- [923페이지의 "게이트웨이 프로필"](#)
- [924페이지의 "SMPP 릴레이"](#)
- [925페이지의 "SMPP 서버"](#)

### 게이트웨이 프로필

ETM(Email-To-Mobile) 게이트웨이 프로필을 구성하려면 다음 단계를 수행합니다.

1. 게이트웨이 프로필을 SMS 게이트웨이 서버 구성 파일에 추가합니다.

옵션 그룹을 추가하려면 다음 형식을 사용합니다.

```
[GATEWAY_PROFILE=profile_name]
option-name-1=option-value-1
option-name-2=option-value-2a
...
option-name-n=option-value-n
```

위 형식에서 게이트웨이 프로필 이름 `profile_name`의 길이는 11바이트를 초과해서는 안 됩니다. 이 이름은 SMS 채널 옵션 파일의 `GATEWAY_PROFILE` 채널 옵션에 대한 이름과 동일해야 합니다. 이 이름은 대소문자를 구분하지 않습니다. 유효한 채널 옵션 목록은 [890페이지의 "사용 가능한 옵션"](#)을 참조하십시오.

2. 게이트웨이 프로필 옵션(예: `SMSC_DEFAULT_CHARSET`)을 원격 `SMSC`의 특성과 일치하도록 설정합니다.
3. 다른 게이트웨이 프로필 옵션을 SMS 채널의 전자 메일 특성과 일치하도록 설정합니다.

게이트웨이 프로필 옵션에 대한 자세한 내용은 [936페이지의 "게이트웨이 프로필 옵션"](#)을 참조하십시오.

4. `CHANNEL` 옵션을 설정합니다.

해당 값을 MTA SMS 채널 이름으로 설정합니다.

게이트웨이를 통해 알림이 전자 메일로 보내지면 이 채널 이름을 사용하여 결과 전자 메일이 MTA의 대기열에 포함됩니다.

## SMPP 릴레이

SMPP 릴레이를 구성하려면 다음 단계를 완료합니다.

1. SMPP 릴레이 인스턴스화(옵션 그룹)를 SMS 게이트웨이 서버의 구성 파일에 추가합니다.

옵션 그룹을 추가하려면 다음 형식을 사용합니다.

```
[SMPP_RELAY=relay_name]
option-name-1=option-value-1
option-name-2=option-value-2
...
option-name-n=option-value-n
```

임의의 이름을 릴레이 이름으로 사용할 수 있습니다. 단, 해당 이름이 동일한 구성 파일 내의 다른 SMPP 릴레이 인스턴스화에 사용되어서는 안 됩니다.

**2. LISTEN\_PORT 옵션을 설정합니다.**

SMS 채널의 SMPP\_PORT 옵션에 사용되는 값은 릴레이의 LISTEN\_PORT 옵션에 사용되는 것과 일치해야 합니다. LISTEN\_PORT의 경우 다른 SMPP 릴레이 또는 서버 인스턴스화에 사용되지 않으며 동일한 컴퓨터에서 실행 중인 다른 서버에서도 사용되지 않는 TCP 포트 번호를 선택합니다.

**3. SERVER\_HOST 옵션을 설정합니다.**

릴레이의 SERVER\_HOST 옵션은 원격 SMSC의 SMPP 서버에 대한 호스트 이름을 제공해야 합니다. 호스트 이름 대신에 IP 주소를 사용할 수 있습니다.

**4. SERVER\_PORT 옵션을 설정합니다.**

릴레이의 SERVER\_PORT 옵션은 원격 SMSC의 SMPP 서버에 대한 TCP 포트를 제공해야 합니다.

모든 SMPP 릴레이 옵션에 대한 자세한 내용은 [931페이지](#)의 "SMPP 릴레이 옵션"을 참조하십시오.

## SMPP 서버

SMPP 서버를 구성하려면 다음 단계를 완료합니다.

**1. SMPP 서버 인스턴스화(옵션 그룹)를 SMS 게이트웨이 서버의 구성 파일에 추가합니다.**

옵션 그룹을 추가하려면 다음 형식을 사용합니다.

```
[SMPP_SERVER=server_name]
option-name-1=option-value-1
option-name-2=option-value-2
...
option-name-n=option-value-n
```

임의의 이름을 서버 이름으로 사용할 수 있습니다. 단, 해당 이름이 동일한 구성 파일 내의 다른 SMPP 서버 인스턴스화에 사용되어서는 안 됩니다.

**2. LISTEN\_PORT 옵션을 설정합니다.**

다른 서버나 릴레이 인스턴스화에 사용되지 않는 TCP 포트 번호를 선택합니다. 또한 이 포트 번호는 동일한 컴퓨터의 다른 서버에 사용되면 안 됩니다.

이 TCP 포트를 사용하여 SMPP를 통해 알림을 SMS 게이트웨이 서버 시스템으로 라우팅하도록 원격 SMSC를 구성해야 합니다.

모든 SMPP 서버 옵션에 대한 자세한 내용은 [934페이지](#)의 "SMPP 서버 옵션"을 참조하십시오.

## MTE(Mobile-To-Email) 작업 구성

MTE(Mobile-To-Email) 기능을 구성하려면 다음 두 가지 구성 단계를 수행해야 합니다.

- 926페이지의 "MTE(Mobile-To-Email) 게이트웨이 프로필 구성"
- 927페이지의 "MTE(Mobile-To-Email) SMPP 서버 구성"

여러 게이트웨이 프로필을 동일한 SMPP 서버 인스턴스화를 사용할 수 있습니다. 실제로 동일한 SMPP 서버 인스턴스화를 ETM(Email-To-Mobile) 및 MTE(Mobile-To-Email) 응용 프로그램에 모두 사용할 수 있습니다.

### MTE(Mobile-To-Email) 게이트웨이 프로필 구성

모바일 원본의 경우 게이트웨이 프로필은 두 가지 주요 정보 즉, 해당 프로필을 대상으로 하는 SMS 메일을 식별하는 방법과 이러한 메일을 전자 메일로 변환하는 방법을 제공합니다. 이 프로필은 SELECT\_RE 옵션을 추가할 경우 ETM(Email-To-Mobile)에 사용되는 프로필과 동일할 수 있습니다.

게이트웨이 프로필을 구성하려면 다음 단계를 수행합니다.

1. 게이트웨이 프로필(옵션 그룹)을 SMS 게이트웨이 서버의 구성 파일에 추가합니다.

옵션 그룹을 추가하려면 다음 형식을 사용합니다.

```
[GATEWAY_PROFILE=profile_name]
option-name-1=option-value-1
option-name-2=option-value-2
...
option-name-n=option-value-n
```

11자 이하의 모든 이름을 프로필 이름으로 사용할 수 있습니다. 단, 해당 이름을 동일한 구성 파일 내의 다른 게이트웨이 프로필에서 사용해서는 안 됩니다.

2. 각 게이트웨이 프로필에 대해 지정해야 하는 `SELECT_RE` 옵션을 설정합니다.

이 옵션 값은 SMS 대상 주소가 비교되는 ASCII 정규 표현식입니다. SMS 대상 주소가 정규 표현식과 일치할 경우 일치하는 프로필에 설명된 특성을 사용하여 SMS 메일이 게이트웨이를 통해 전자 메일로 보내집니다.

겹치는 SMS 주소 집합을 가진 여러 게이트웨이 프로필(예: 주소 000과 일치하는 프로필과 다른 모든 3자리 주소와 일치하는 또 다른 프로필)을 구성할 수 있습니다. 그러나 SMS 메일이 하나의 게이트웨이 프로필(일치하는 첫 번째 것)로만 전달되므로 여러 게이트웨이 프로필을 구성하는 것을 피해야 합니다. 또한 이러한 프로필이 비교되는 순서는 정의되지 않습니다.

3. CHANNEL 옵션을 설정합니다.

해당 값은 MTA SMS 채널의 이름이어야 합니다.

모든 모바일 원본 옵션에 대한 자세한 내용은 [936페이지의 "게이트웨이 프로필 옵션"](#)을 참조하십시오.

## MTE(Mobile-To-Email) SMPP 서버 구성

SMPP 서버 추가는 ETM(Email-To-Mobile) SMPP 서버의 경우와 같습니다([925페이지의 "SMPP 서버"](#) 참조).

SMS 트래픽을 게이트웨이 SMPP 서버로 라우팅하도록 원격 SMSC를 구성해야 합니다. 이렇게 하려면 MTE(Mobile-To-Email) 트래픽을 라우팅하기 위해 SMSC가 사용하는 SMS 대상 주소가 게이트웨이 프로필 옵션 `SELECT_RE`에 설정된 값이어야 합니다.

예를 들어, SMS 주소 000이 MTE(Mobile-To-Email) 트래픽에 사용될 경우 SMS 대상 주소 000에 대한 트래픽을 게이트웨이 SMPP 서버로 라우팅하도록 SMSC를 구성해야 합니다. 게이트웨이 프로필은 옵션 설정 `SELECT_RE=000`을 사용해야 합니다.

## 구성 옵션

이 절에서는 SMS 게이트웨이 서버 구성 과일 옵션에 대해 자세히 설명합니다. 이 절에 나오는 표에는 사용 가능한 모든 구성 옵션이 간단한 설명과 함께 나열되어 있습니다. 전역 옵션, SMPP 릴레이 옵션, SMPP 서버 옵션 및 SMS 게이트웨이 서버 프로필 옵션에 대한 표가 제공됩니다.

이 절은 사용 가능한 모든 구성 옵션에 대한 자세한 설명을 제공하는 다음 하위 절로 구성되어 있습니다.

- 928페이지의 "전역 옵션"

전역 옵션은 모든 옵션 그룹의 앞에 오도록 구성 파일의 맨 위에 두어야 합니다. 나머지 옵션은 옵션 그룹 안에 있어야 합니다.

- 931페이지의 "SMPP 릴레이 옵션"
- 934페이지의 "SMPP 서버 옵션"
- 936페이지의 "게이트웨이 프로필 옵션"

## 전역 옵션

SMS 게이트웨이 서버에는 현재 다음 세 가지 범주의 전역 옵션이 있습니다.

- 스레드 조정 옵션
- 기록 데이터 조정
- 기타

모든 전역 옵션은 지정된 모든 옵션 그룹의 앞에 오도록 구성 파일의 맨 위에 지정해야 합니다. 표 D-20에는 모든 전역 구성 옵션이 나열되어 있습니다.

**표 D-20** 전역 옵션

| 옵션                           | 기본값  | 설명                                             |
|------------------------------|------|------------------------------------------------|
| DEBUG                        | 6    | 생성된 진단 출력의 유형을 선택합니다.                          |
| HISTORY_FILE_DIRECTORY       |      | 기록 데이터 파일의 절대 디렉토리 경로입니다.                      |
| HISTORY_FILE_MODE            | 0770 | 기록 데이터 파일에 대한 권한입니다.                           |
| HISTORY_FILE_ROLLOVER_PERIOD | 30분  | 기록 데이터의 동일한 파일에 쓸 수 있는 최대 시간입니다.               |
| LISTEN_CONNECTION_MAX        |      | 모든 SMPP 릴레이 및 서버 인스턴스 화에서의 최대 동시 인바운드 연결 수입니다. |
| RECORD_LIFETIME              | 3일   | 기록 데이터 아카이브에 있는 레코드의 수명입니다.                    |
| THREAD_COUNT_INITIAL         | 10개  | 작업자 스레드의 초기 수입니다.                              |
| THREAD_COUNT_MAXIMUM         | 50개  | 작업자 스레드의 최대 수입니다.                              |
| THREAD_STACK_SIZE            | 64KB | 각 작업자 스레드의 스택 크기입니다.                           |



## 스레드 조정 옵션

각 인바운드 TCP 연결은 SMPP 세션을 나타냅니다. 세션 처리는 스레드 풀의 작업자 스레드에 의해 수행됩니다. 세션 처리가 I/O 요청이 완료되기를 기다려야 할 경우 작업 스레드는 세션을 대기시키며 수행할 다른 작업이 작업 스레드에 제공됩니다. I/O 요청이 완료되면 풀의 사용 가능한 작업자 스레드에 의해 세션이 다시 시작됩니다.

다음 옵션을 사용하여 이 작업자 스레드 프로세스 풀을 조정할 수 있습니다.

`THREAD_COUNT_INITIAL`, `THREAD_COUNT_MAXIMUM`, `THREAD_STACK_SIZE`

### `THREAD_COUNT_INITIAL`

(정수, > 0) 초기에 작업자 스레드 풀에 대해 만들어지는 스레드 수입니다. 메모리 내장 기록 데이터를 관리하는 데 사용되는 전용 스레드(두 개의 스레드) 및 받는 TCP 연결을 수신하는 데 사용되는 전용 스레드(SMS 게이트웨이 서버가 수신하는 TCP 포트/인터페이스 주소 쌍마다 스레드 하나씩)는 이 수에 포함되지 않습니다. `THREAD_COUNT_INITIAL`의 기본값은 10개입니다.

### `THREAD_COUNT_MAXIMUM`

(정수, >= `THREAD_COUNT_INITIAL`) 작업자 스레드 풀에 허용되는 최대 스레드 수입니다. 기본값은 50개입니다.

### `THREAD_STACK_SIZE`

(정수, > 0) 작업자 스레드 풀의 각 작업자 스레드에 대한 스택 크기(바이트)입니다. 기본값은 65,536바이트(64KB)입니다.

## 기록 데이터 조정

SMS 메일이 릴레이되면 원격 수신 SMPP 서버에 의해 생성된 메일 아이디가 메모리 내장 해시 테이블에 저장됩니다. 또한 이 메일 아이디와 함께 원래 전자 메일에 대한 정보가 저장됩니다. 그 후에 메일 아이디가 SMS 알림에 의해 참조될 경우 이 정보를 검색할 수 있습니다. 이어서 검색된 정보를 사용하여 SMS 알림을 적절한 전자 메일 수신자에게 보낼 수 있습니다.

메모리 내장 해시 테이블은 전용 스레드에 의해 디스크에 저장됩니다. 결과 디스크 파일은 "기록 파일"이라고 합니다. 이러한 기록 파일은 SMS 게이트웨이 서버를 다시 시작한 후 메모리 내장 해시 테이블을 복원하는 데 필요한 데이터를 비휘발성 형태로 저장하고 잠재적으로 긴 데이터를 디스크에 저장하여 가상 메모리를 절약하는 두 가지 역할을 수행합니다. 각 기록 파일은 `HASH_FILE_ROLLOVER_PERIOD`(초) 동안만 데이터가 기록되며 이 기간 후에는 파일이 닫히고 새 기록 파일이 만들어집니다. 기록 파일은 `RECORD_LIFETIME`(초)을 초과할 경우 디스크에서 삭제됩니다.

다음 옵션을 사용하여 기록 파일을 조정할 수 있습니다.

[HISTORY\\_FILE\\_DIRECTORY](#), [HISTORY\\_FILE\\_MODE](#), [HISTORY\\_FILE\\_ROLLOVER\\_PERIOD](#),  
[RECORD\\_LIFETIME](#)

### **HISTORY\_FILE\_DIRECTORY**

(문자열, 절대 디렉토리 경로) 기록 파일을 기록할 디렉토리의 절대 경로입니다. 디렉토리 경로는 존재하지 않을 경우 새로 만들어집니다. 이 옵션의 기본값은 다음과 같습니다.

```
msg_svr_base/data/sms_gateway_cache/
```

사용할 디렉토리는 충분한 속도의 디스크 시스템에 존재하며 예상 저장소에 충분한 여유 공간을 가져야 합니다. 저장소 계획 정보에 대해서는 [944페이지의 "SMS 게이트웨이 서버 저장소 요구 사항"](#)을 참조하십시오. 해당 사이트에서 이 옵션을 보다 적절한 값으로 변경하는 것이 좋습니다.

### **HISTORY\_FILE\_MODE**

(정수, 8진수 값) 기록 파일과 연관된 파일 권한입니다. 기본값은 0770(8진수)입니다.

### **HISTORY\_FILE\_ROLLOVER\_PERIOD**

(정수, 초) [HASH\\_FILE\\_ROLLOVER\\_PERIOD](#)(초)마다 현재 기록 파일이 닫히고 새 기록 파일이 만들어집니다. 기본값은 1800초(30분)입니다.

### **RECORD\_LIFETIME**

(정수, 초 > 0) 기록 레코드의 수명(초)입니다. 이 수명보다 오래된 레코드는 메모리에서 제거됩니다. 즉, 이 수명보다 오래된 기록 파일은 디스크에서 삭제됩니다. 기본값은 259,200초(3일)입니다. 메모리에 저장된 레코드는 메모리 내장 데이터를 관리하는 전용 스레드에 의해 완전히 제거됩니다. 이러한 제거는 [HASH\\_FILE\\_ROLLOVER\\_PERIOD](#)(초)마다 발생합니다. 디스크의 파일은 새 기록 파일을 여는 것이 필요할 때 제거됩니다.

## **기타**

두 개의 기타 옵션으로 [DEBUG](#) 및 [LISTEN\\_CONNECTION\\_MAX](#)가 있습니다.

### **DEBUG**

(정수, 비트 마스크) 디버그 출력을 사용 가능하게 합니다. 기본값은 경고 및 오류 메시지를 선택하는 6입니다.

표 D-21에는 DEBUG 비트 마스크의 비트 값이 정의되어 있습니다.

표 D-21 DEBUG 비트 마스크

| 비트   | 값    | 설명                                   |
|------|------|--------------------------------------|
| 0-31 | -1   | 매우 자세한 출력                            |
| 0    | 1    | 정보 메시지                               |
| 1    | 2    | 경고 메시지                               |
| 3    | 4    | 오류 메시지                               |
| 3    | 8    | 서브루틴 호출 추적                           |
| 4    | 16   | 해시 테이블 진단                            |
| 5    | 32   | I/O 진단, 수신                           |
| 6    | 64   | I/O 진단, 전송                           |
| 7    | 128  | SMS에서 전자 메일로의 변환 진단(모바일 원본 및 SMS 알림) |
| 8    | 256  | PDU 진단, 헤더 데이터                       |
| 9    | 512  | PDU 진단, 본문 데이터                       |
| 10   | 1024 | PDU 진단, 유형 길이 값 데이터                  |
| 11   | 2048 | 옵션 처리(모든 옵션 설정을 로그 파일로 보냄)           |

### *LISTEN\_CONNECTION\_MAX*

(정수, >= 0) 모든 SMPP 릴레이 및 서버 인스턴스화에서 허용할 최대 동시 인바운드 TCP 연결 수입니다. 값 0은 연결 수에 전역 제한이 없음을 나타냅니다. 그러나 지정된 릴레이 또는 서버 인스턴스화에 의해 릴레이 또는 서버별 제한이 있을 수 있습니다.

## SMPP 릴레이 옵션

SMS 게이트웨이 서버는 해당 SMPP 릴레이의 여러 인스턴스화를 가질 수 있으며 각 인스턴스화는 수신되는 TCP 포트 및 인터페이스에 대해 다른 특성 부분을 가집니다. SMPP 릴레이가 수신하는 각 네트워크 인터페이스 및 TCP 포트 쌍에 대해 다르게 지정함으로써 고유한 특성을 포함시킬 수 있습니다. 이러한 특성은 이 절에 설명된 옵션을 사용하여 지정합니다.

각 인스턴스화는 다음 형식의 옵션 그룹 안에 포함되어야 합니다.

```
[SMPP_RELAY=relay-name]
option-name-1=option-value-1
option-name-2=option-value-2
...
option-name-n=option-value-n
```

문자열 relay-name은 단순히 이 인스턴스화를 다른 인스턴스화와 구별하는 역할을 수행합니다.

표 D-22에는 SMPP 릴레이 구성 옵션이 나열되어 있습니다.

**표 D-22** SMPP 릴레이 옵션

| 옵션                                        | 기본값  | 설명                                    |
|-------------------------------------------|------|---------------------------------------|
| <code>LISTEN_BACKLOG</code>               | 255  | 인바운드 SMPP 클라이언트 연결의 연결 백로그입니다.        |
| <code>LISTEN_CONNECTION_MAX</code>        |      | 동시 인바운드 연결의 최대 수입니다.                  |
| <code>LISTEN_INTERFACE_ADDRESS</code>     |      | 인바운드 SMPP 클라이언트 연결의 네트워크 인터페이스입니다.    |
| <code>LISTEN_PORT</code>                  |      | 인바운드 SMPP 클라이언트 연결의 TCP 포트입니다.        |
| <code>LISTEN_RECEIVE_TIMEOUT</code>       | 600초 | 인바운드 SMPP 클라이언트 연결의 읽기 시간 초과입니다.      |
| <code>LISTEN_TRANSMIT_TIMEOUT</code>      | 120초 | 인바운드 SMPP 클라이언트 연결의 쓰기 시간 초과입니다.      |
| <code>MAKE_SOURCE_ADDRESSES_UNIQUE</code> | 1    | 릴레이된 SMS 소스 주소를 고유하게 만들고 응답 가능하게 합니다. |
| <code>SERVER_HOST</code>                  |      | 릴레이할 SMPP 서버의 호스트 이름 또는 IP 주소입니다.     |
| <code>SERVER_PORT</code>                  |      | 릴레이할 SMPP 서버의 TCP 포트입니다.              |
| <code>SERVER_RECEIVE_TIMEOUT</code>       | 600초 | 아웃바운드 SMPP 서버 연결의 읽기 시간 초과입니다.        |
| <code>SERVER_TRANSMIT_TIMEOUT</code>      | 120초 | 아웃바운드 SMPP 서버 연결의 쓰기 시간 초과입니다.        |

### **LISTEN\_BACKLOG**

([0, 255]의 정수) TCP 스택이 허용하는 인바운드 SMPP 클라이언트 연결의 연결 백로그입니다. 기본값은 255입니다.

***LISTEN\_CONNECTION\_MAX***

(정수,  $\geq 0$ ) 이 SMPP 릴레이 인스턴스화에 허용되는 동시 인바운드 TCP 연결의 최대 수입니다. 이 값은 전역 LISTEN\_CONNECTION\_MAX 설정을 초과할 경우 무시됩니다.

***LISTEN\_INTERFACE\_ADDRESS***

(문자열, "INADDR\_ANY" 또는 점으로 구분된 십진수 IP 주소) 인바운드 SMPP 클라이언트 연결의 수신할 네트워크 인터페이스에 대한 IP 주소입니다. 문자열 "INADDR\_ANY" (사용 가능한 모든 인터페이스)나 점으로 구분된 십진수 형식의 IP 주소(예: 193.168.100.1)가 될 수 있습니다. 기본값은 "INADDR\_ANY"입니다. 클러스터된 HA 구성은 이 값을 HA 논리 IP 주소에 해당하도록 설정해야 합니다.

***LISTEN\_PORT***

(정수, TCP 포트 번호) 인바운드 SMPP 클라이언트 연결을 수락하기 위해 바인드할 TCP 포트입니다. 이 옵션 지정은 필수 사항이며 기본값은 없습니다. 또한 이 서비스에 대한 IANA(Internet Assigned Numbers Authority) 할당이 없습니다.

***LISTEN\_RECEIVE\_TIMEOUT***

(정수, 초  $> 0$ ) SMPP 클라이언트로부터 데이터를 읽는 동안 기다릴 때 허용되는 시간 초과입니다. 기본값은 600초(10분)입니다.

***LISTEN\_TRANSMIT\_TIMEOUT***

(정수, 초  $> 0$ ) 데이터를 SMPP 클라이언트로 보낼 때 허용되는 시간 초과입니다. 기본값은 120초(2분)입니다.

***MAKE\_SOURCE\_ADDRESSES\_UNIQUE***

(0 또는 1) 기본적으로 SMPP 릴레이는 고유한 10자리 문자열을 각 SMS 소스 주소에 추가합니다. 그런 다음 결과 SMS 소스 주소는 다른 기록 데이터와 함께 저장됩니다. 결과는 SMS 사용자가 응답할 수 있는 고유한 SMS 주소입니다. SMPP 서버는 SMS 대상 주소로 사용될 때 이 주소를 감지한 다음 SMS 메일을 올바른 전자 메일 발송자에게 보냅니다.

단방향 SMS에 대해 이러한 고유한 SMS 소스 주소가 생성되지 않게 하려면 이 옵션의 값으로 0을 지정합니다.

***SERVER\_HOST***

(문자열, TCP 호스트 이름 또는 점으로 구분된 십진수 IP 주소) SMPP 클라이언트 트래픽을 릴레이할 SMPP 서버입니다. 호스트 이름이나 IP 주소를 지정할 수 있습니다. 이 옵션 지정은 필수 사항이며 기본값은 없습니다.

**SERVER\_PORT**

(정수, TCP 포트 번호) 릴레이할 원격 SMPP 서버의 TCP 포트입니다. 이 옵션 지정은 필수 사항이며 기본값은 없습니다. 이 서비스에 대한 IANA 할당은 없습니다. 따라서 SNPP에 대한 IANA 할당과 혼동하지 않도록 주의합니다.

**SERVER\_RECEIVE\_TIMEOUT**

(정수, 초 > 0) SMPP 서버로부터 데이터를 읽기 위해 대기할 때 허용되는 시간 초과입니다. 기본값은 600초(10분)입니다.

**SERVER\_TRANSMIT\_TIMEOUT**

(정수, 초 > 0) 데이터를 SMPP 서버로 보낼 때 허용되는 시간 초과입니다. 기본값은 120초(2분)입니다.

## SMPP 서버 옵션

SMS 게이트웨이 서버는 해당 SMPP 서버의 여러 인스턴스화를 가질 수 있으며 각 인스턴스화는 수신되는 TCP 포트 및 인터페이스에 대해 다른 특성 부분을 가집니다. SMPP 서버가 수신하는 각 네트워크 인터페이스 및 TCP 포트 쌍에 대해 다르게 지정함으로써 고유한 특성을 포함할 수 있습니다. 이러한 특성은 이 절에 설명된 옵션을 사용하여 지정합니다.

각 인스턴스화는 다음 형식의 옵션 그룹 안에 포함되어야 합니다.

```
[SMPP_SERVER=server-name]
option-value-1=option-value-1
option-value-2=option-value-2
...
option-name-n=option-value-n
```

문자열 server-name은 단순히 이 인스턴스화를 다른 인스턴스화와 구별하는 역할을 수행합니다.

표 D-23에는 SMPP 서버 구성 옵션이 나열되어 있습니다.

**표 D-23** SMPP 서버 옵션

| 옵션                                       | 기본값 | 설명                              |
|------------------------------------------|-----|---------------------------------|
| <a href="#">LISTEN_BACKLOG</a>           | 255 | 인바운드 SMPP 서버 연결의 연결 백로그입니다.     |
| <a href="#">LISTEN_CONNECTION_MAX</a>    |     | 동시 인바운드 연결의 최대 수입니다.            |
| <a href="#">LISTEN_INTERFACE_ADDRESS</a> |     | 인바운드 SMPP 서버 연결의 네트워크 인터페이스입니다. |

**표 D-23** SMPP 서버 옵션 (계속)

| 옵션                                   | 기본값  | 설명                            |
|--------------------------------------|------|-------------------------------|
| <code>LISTEN_PORT</code>             |      | 인바운드 SMPP 서버 연결의 TCP 포트입니다.   |
| <code>LISTEN_RECEIVE_TIMEOUT</code>  | 600초 | 인바운드 SMPP 서버 연결의 읽기 시간 초과입니다. |
| <code>LISTEN_TRANSMIT_TIMEOUT</code> | 120초 | 인바운드 SMPP 서버 연결의 쓰기 시간 초과입니다. |

***LISTEN\_BACKLOG***

([0,255]의 정수) TCP 스택이 허용하는 인바운드 SMPP 클라이언트 연결의 연결 백로그입니다. 기본값은 255입니다.

***LISTEN\_CONNECTION\_MAX***

(정수  $\geq 0$ ) 이 SMPP 서버 인스턴스화에 허용되는 동시 인바운드 TCP 연결의 최대 수입니다. 이 값은 전역 `LISTEN_CONNECTION_MAX` 설정을 초과할 경우 무시됩니다.

***LISTEN\_INTERFACE\_ADDRESS***

(문자열 "INADDR\_ANY" 또는 점으로 구분된 십진수 IP 주소) 인바운드 SMPP 클라이언트 연결의 수신할 네트워크 인터페이스에 대한 IP 주소입니다. 문자열 "INADDR\_ANY"(사용 가능한 모든 인터페이스)나 점으로 구분된 십진수 형식의 IP 주소(예: 193.168.100.1)가 될 수 있습니다. 기본값은 "INADDR\_ANY"입니다.

***LISTEN\_PORT***

(정수, TCP 포트 번호) 인바운드 SMPP 클라이언트 연결을 수락하기 위해 바인드할 TCP 포트입니다. 이 옵션 지정은 필수 사항이며 기본값은 없습니다. 이 서비스에 대한 IANA 할당이 없습니다.

***LISTEN\_RECEIVE\_TIMEOUT***

(정수, 초  $> 0$ ) SMPP 클라이언트로부터 데이터를 읽는 동안 기다릴 때 허용되는 시간 초과입니다. 기본값은 600초(10분)입니다.

***LISTEN\_TRANSMIT\_TIMEOUT***

(정수, 초  $> 0$ ) 데이터를 SMPP 클라이언트로 보낼 때 허용되는 시간 초과입니다. 기본값은 120초(2분)입니다.

## 게이트웨이 프로필 옵션

0개 이상의 게이트웨이 프로필이 존재할 수 있습니다. SMS 게이트웨이 서버의 구성 파일에서 각 게이트웨이 프로필은 옵션 그룹 내에서 다음 형식으로 선언됩니다.

```
[GATEWAY_PROFILE=profile-name]
option-name-1=option-value-1
option-name-2=option-value-2
...
option-name-n=option-value-n
```

문자열 `profile-name`은 단순히 해당 프로필을 다른 원본 프로필과 구별하는 역할을 수행합니다.

표 D-24에는 SMS 게이트웨이 서버 프로필 옵션이 나열되어 있습니다.

**표 D-24** SMS 게이트웨이 서버 프로필 옵션

| 옵션                                                   | 기본값      | 설명                                   |
|------------------------------------------------------|----------|--------------------------------------|
| <code>CHANNEL</code>                                 | sms      | 메일을 대기열에 포함하는 채널입니다.                 |
| <code>EMAIL_BODY_CHARSET</code>                      | US-ASCII | 전자 메일 본문의 문자 세트입니다.                  |
| <code>EMAIL_HEADER_CHARSET</code>                    | US-ASCII | 전자 메일 헤더의 문자 세트입니다.                  |
| <code>FROM_DOMAIN</code>                             |          | 전자 메일을 다시 SMS로 라우팅하기 위한 도메인 이름입니다.   |
| <code>PARSE_RE_0, PARSE_RE_1, ..., PARSE_RE_9</code> |          | SMS 메일 텍스트를 구문 분석하기 위한 정규 표현식입니다.    |
| <code>PROFILE</code>                                 | GSM      | GSM, TDMA 또는 CDMA에서 작동하는 SMS 프로필입니다. |
| <code>SELECT_RE</code>                               |          | 플러그 인을 선택하기 위한 정규 표현식입니다.            |
| <code>SMSC_DEFAULT_CHARSET</code>                    | US-ASCII | SMSC의 기본 문자 세트입니다.                   |
| <code>USE_SMS_PRIORITY</code>                        | 0        | 전자 메일에 대한 게이트웨이 SMS 우선 순위 플래그입니다.    |
| <code>USE_SMS_PRIVACY</code>                         | 0        | 전자 메일에 대한 게이트웨이 SMS 개인 정보 표시기입니다.    |

### CHANNEL

(문자열, 1-40개 문자) 전자 메일을 대기열에 포함시키는 데 사용되는 MTA 채널의 이름입니다. 지정하지 않을 경우 "sms"가 사용됩니다. 지정된 채널은 MTA의 구성에 정의되어야 합니다.



**EMAIL\_BODY\_CHARSET**

(문자열, 문자 세트 이름) 전자 메일 메시지의 본문에 삽입하기 전에 SMS 텍스트를 변환하기 위한 문자 세트입니다. 필요한 경우 변환된 텍스트는 MIME 인코딩됩니다. 기본값은 US-ASCII입니다. SMS 메일이 charset에서 사용할 수 없는 도형 문자를 포함할 경우 이러한 도형 문자는 수신자에게 의미가 있거나 없을 수 있는 니모닉 문자로 변환됩니다.

MTA에 알려진 문자 세트 목록은 다음 파일에서 확인할 수 있습니다.

`installation-directory/config/charsets.txt`

**EMAIL\_HEADER\_CHARSET**

(문자열, 문자 세트 이름) RFC 822 Subject: 헤더 행에 삽입하기 전에 SMS 텍스트를 변환하기 위한 문자 세트입니다. 필요한 경우 변환된 문자열은 MIME 인코딩됩니다. 기본값은 US-ASCII입니다. SMS 메일이 charset에서 사용할 수 없는 도형 문자를 포함할 경우 이러한 도형 문자는 수신자에게 의미가 있거나 없을 수 있는 니모닉 문자로 변환됩니다.

**FROM\_DOMAIN**

(문자열, IP 호스트 이름, 1-64 개 문자) 봉투를 생성할 때 SMS 소스에 추가되는 도메인 이름 전자 메일의 봉투 From: 주소를 생성할 때 SMS 소스 주소에 추가할 도메인 이름입니다. 지정된 이름은 전자 메일을 다시 SMS로 라우팅하기 위한 올바른 이름이어야 합니다(예: MTA SMS 채널과 연관된 호스트 이름). 지정하지 않을 경우 CHANNEL 옵션으로 지정된 채널의 공식 호스트 이름이 사용됩니다.

**PARSE\_RE\_0, PARSE\_RE\_1, ..., PARSE\_RE\_9**

(문자열, UTF-8 정규 표현식) 전자 메일의 모바일 원본의 경우 게이트웨이 프로파일은 SMS 메일의 텍스트에서 대상 전자 메일 주소를 추출해야 합니다. 이것은 하나 이상의 POSIX 호환 정규 표현식(RE)으로 수행됩니다. 대상 전자 메일 주소를 생성하는 일치하는 항목이 발견되거나 정규 표현식 목록이 모두 사용될 때까지 각 정규 표현식은 SMS 메일의 텍스트를 평가합니다.

---

**주** PARSE\_RE\_\* 및 ROUTE\_TO 옵션을 동시에 사용할 수 없습니다. 동일한 게이트웨이 프로파일에서 두 옵션을 함께 사용하는 것은 구성 오류입니다.

---

각 정규 표현식은 POSIX와 호환되어야 하며 UTF-8 문자 세트로 인코딩되어야 합니다. 정규 표현식은 문자열 0을 대상 주소로 출력해야 합니다. 선택적으로 Subject: 헤더 행에 사용할 텍스트를 문자열 1로 출력하고, 메일 본문에 사용할 텍스트를 문자열 2로 출력할 수 있습니다. 정규 표현식에서 "사용"하지 않는 모든 텍스트는 문자열 2로 출력된 텍스트에 이어서 메일 본문에 사용될 수 있습니다.

정규 표현식은 PARSE\_RE\_0, PARSE\_RE\_1, ..., PARSE\_RE\_9의 순서로 시도됩니다. 지정된 정규 표현식이 없을 경우 다음 기본 정규 표현식이 사용됩니다.

```
[ \t]*([^\( ]*)[ \t]*(?:\((([^\)]*)\))?[ \t]*(.*)
```

이 기본 정규 표현식은 다음 구성 요소로 나뉩니다.

```
[ \t]*
```

선행 공백 문자(SPACE 및 TAB)를 무시합니다.

```
([^\( ]*)
```

대상 전자 메일 주소입니다. 첫 번째로 보고되는 문자열입니다.

```
[ \t]*
```

공백 문자를 무시합니다.

```
(?:\((([^\)]*)\))?)
```

괄호로 묶인 선택적 제목 텍스트입니다. 두 번째로 보고되는 문자열입니다. ?:는 바깥쪽 괄호가 문자열을 보고하지 않게 합니다. 이러한 괄호는 단순히 후행 ?에 대해 해당 내용을 단일 RE로 그룹화하는 데 사용됩니다. 후행 ?는 RE 구성 요소가 0번 또는 1번만 일치하도록 하며 표현식 {0,1}과 같습니다.

```
[ \t]*
```

공백 문자를 무시합니다.

```
(.*)
```

메일 본문에 대한 나머지 텍스트입니다. 세 번째로 보고되는 문자열입니다.

예를 들어, 위 정규 표현식을 사용할 경우 다음 샘플 SMS 메일은

```
dan@sesta.com(Testing)This is a test
```

다음 전자 메일을 생성합니다.

```
To: dan@sesta.com
```

```
Subject: Testing
```

```
This is a test
```

두 번째 예로 다음 SMS 메일은

```
sue@sesta.com This is another test
```

다음을 생성합니다.

```
To: sue@sesta.com
```

```
This is another test
```

SMS 메일은 이러한 정규 표현식으로 평가되기 전에 유니코드의 UTF-16 인코딩으로 변환됩니다. 그런 다음 변환된 텍스트는 이전에 UTF-8에서 UTF-16으로 변환된 정규 표현식으로 평가됩니다. 이어서 평가 결과는 Subject: 텍스트의 대상 전자 메일 주소 EMAIL\_HEADER\_CHARSET(있을 경우)와 메일 본문의 EMAIL\_BODY\_CHARSET(있을 경우)에 대한 US-ASCII로 변환됩니다.

### **PROFILE**

(문자열, "GSM", "TDMA" 또는 "CDMA") 사용할 SMS 프로파일입니다. 현재 이 정보는 SMS 우선 순위 플래그를 RFC 822 Priority: 헤더 행으로 매핑하기 위해 사용됩니다. 결과적으로 USE\_SMS\_PRIORITY가 기본값인 0일 경우 이 옵션은 아무 효과가 없습니다.

### **SELECT\_RE**

(문자열, US-ASCII 정규 표현식) 각 SMS 메일의 SMS 대상 주소와 비교할 US-ASCII POSIX 호환 정규 표현식입니다. SMS 메일의 대상 주소가 이 RE와 일치할 경우 SMS 메일은 이 게이트웨이 프로파일에 따라 게이트웨이를 통해 전자 메일로 보내집니다.

SMS 메일의 대상 주소가 US-ASCII 문자 세트로 지정되므로 이 정규 표현식도 US-ASCII로 표현되어야 합니다.

### **SMSC\_DEFAULT\_CHARSET**

(문자열, 문자 세트 이름) 원격 SMSC에 사용되는 기본 문자 세트의 이름입니다. 이 옵션에는 일반적으로 US-ASCII 및 UTF-16-BE(USC2)가 지정됩니다. 지정하지 않을 경우 US-ASCII가 사용됩니다.

**USE\_SMS\_PRIORITY**

(정수, 0 또는 1) 기본적으로 USE\_SMS\_PRIORITY=0이며 이 경우 SMS 메일의 우선 순위 플래그가 무시되어 전자 메일과 함께 보내지지 않습니다. 우선 순위 플래그를 전자 메일과 함께 전달하려면 USE\_SMS\_PRIORITY=1을 지정합니다. 표 D-25에는 우선 순위 플래그가 전자 메일과 함께 전달될 경우의 SMS에서 전자 메일로의 매핑이 나와 있습니다.

**표 D-25** SMS에서 전자 메일로의 우선 순위 플래그 매핑

| SMS 프로필 | SMS 우선 순위 플래그  | 전자 메일 Priority: 헤더 행 |
|---------|----------------|----------------------|
| GSM     | 0(낮음)          | 헤더 행 없음(Normal을 의미)  |
|         | 1, 2, 3(우선 순위) | Urgent               |
| TDMA    | 0(대량)          | Nonurgent            |
|         | 1(중간)          | 헤더 행 없음(Normal을 의미)  |
|         | 2(높음)          | Urgent               |
|         | 3(매우 높음)       | Urgent               |
| CDMA    | 0(중간)          | 헤더 행 없음(Normal을 의미)  |
|         | 1(대화식)         | Urgent               |
|         | 2(높음)          | Urgent               |
|         | 3(긴급)          | Urgent               |

전자 메일 Priority: 헤더 행 값은 Nonurgent, Normal 및 Urgent입니다.

## USE\_SMS\_PRIVACY

(정수, 0 또는 1) 기본적으로 USE\_SMS\_PRIVACY=0이며 이 경우 SMS 개인 정보 표시가 무시되어 전자 메일과 함께 보내지지 않습니다. 이 정보를 전자 메일과 함께 전달하려면 USE\_SMS\_PRIVACY=1을 지정합니다. 표 D-26에는 개인 정보 플래그가 전자 메일과 함께 전달될 경우 SMS에서 전자 메일로의 매핑이 나와 있습니다.

**표 D-26** SMS에서 전자 메일로의 개인 정보 플래그 매핑

| SMS 개인 정보 플래그 | 전자 메일 Sensitivity: 헤더 행 |
|---------------|-------------------------|
| 0(제한되지 않음)    | 헤더 행 없음                 |
| 1(제한됨)        | Personal                |
| 2(기밀)         | Private                 |
| 3(비밀)         | Company-confidential    |

전자 메일 Sensitivity: 헤더 행 값은 Personal, Private 및 Company-confidential입니다.

## 양방향 SMS의 구성 예

### 동작에 대한 가정

이 예에서는 다음 동작을 원한다고 가정합니다.

- 다음 주소로 지정된 전자 메일이

```
sms-id@sms.domain.com
```

다음 SMS 주소로 전송되고

```
sms-id
```

000nnnnnnnnnn 범위의 고유한 SMS 소스 주소가 주어집니다.

- SMS 주소 000으로 지정된 모바일 SMS 메일을 SMS 메일 텍스트의 시작 부분에서 추출된 전자 메일 주소와 함께 게이트웨이를 통해 전자 메일로 보냅니다.

예를 들어, SMS 메일 텍스트가 다음과 같은 경우

```
jd@domain.com Interested in a movie?
```

"Interested in a movie?" 메일이 jd@domain.com으로 보내집니다.

- 000nnnnnnnnnn으로 보낸 SMS 알림을 게이트웨이를 통해 전자 메일로 보내고 수신 확인되는 메일 발송자에게 전송합니다.

이 동작을 수행하기 위해 다음 가정과 지정이 적용됩니다.

### 추가 가정 및 지정

- MTA의 SMS 채널은 도메인 이름 sms.domain.com을 사용합니다.
- SMS 게이트웨이 서버는 호스트 gateway.domain.com에서 실행되며 다음을 사용합니다.
  - SMPP 릴레이를 위한 TCP 포트 503
  - SMPP 서버를 위한 TCP 포트 504
- 원격 SMSC의 SMPP 서버는 호스트 smpp.domain.com에서 실행되며 TCP 포트 377을 수신합니다.
- 원격 SMSC의 기본 문자 세트는 UCS2(UTF-16이라고도 함)입니다.

### SMS 채널 구성

위 동작을 적용하기 위해 imta.cnf 파일에서 다음 SMS 채널 구성을 사용할 수 있습니다 (다음 행을 파일의 맨 아래에 추가).

```
(blank line)
sms
sms.domain.com
```

### SMS 채널 옵션 파일

그런 다음 채널 옵션 파일 sms\_option은 다음 설정을 포함합니다.

```
SMPP_SERVER=gateway.domain.com
SMPP_PORT=503
USE_HEADER_FROM=0
DEFAULT_SOURCE_ADDRESS=000
GATEWAY_PROFILE=sms1
SMSC_DEFAULT_CHARSET=UCS2
```

### SMS 게이트웨이 서버 구성

마지막으로 게이트웨이 서버 구성 파일 sms\_gateway.cnf는 다음과 같이 표시되어야 합니다.

```
HISTORY_FILE_DIRECTORY=/sms_gateway_cache/
```

```
[SMPP_RELAY=relay1]
LISTEN_PORT=503
SERVER_HOST=smpp.domain.com
SERVER_PORT=377

[SMPP_SERVER=server1]
LISTEN_PORT=504

[GATEWAY_PROFILE=sms1]
SELECT_RE=000 ([0-9]{10,10}){0,1}
SMSC_DEFAULT_CHARSET=UCS2
```

## 이 구성 테스트

테스트할 SMSC가 없을 경우 약간의 루프백 테스트를 수행할 수 있습니다. sms\_option 파일에서 몇 가지 추가 설정을 사용하면 위 구성에 대해 간단한 루프백 테스트를 수행할 수 있습니다.

### 추가 sms\_option 파일 설정

sms\_option 파일의 추가 설정은 다음과 같습니다.

```
! So that we don't add text to the body of the SMS message
FROM_FORMAT=
SUBJECT_FORMAT=
CONTENT_PREFIX=
```

이러한 설정이 없으면 다음을 포함하는 전자 메일은  
user@domain.com (Sample subject) Sample text

다음 SMS 메일로 변환됩니다.

```
From:user@domain.com Subject:Sample Subject Msg:Sample text
```

이것은 다음과 같은 ETM(Email-To-Mobile) 코드에서 예상한 형식이 아닙니다.

```
user@domain.com (Sample subject) Sample text
```

따라서 루프백 테스트를 위해서는 FROM\_FORMAT, SUBJECT\_FORMAT 및 CONTENT\_PREFIX 옵션에 빈 문자열을 지정해야 합니다.

### 루프백 테스트 수행

다음과 같이 000@sms.domain.com으로 주소 지정된 테스트 전자 메일을 보냅니다.

```
user@domain.com (Test message) This is a test message which should loop
back
```

그 결과 이 전자 메일을 전자 메일 수신자 user@domain.com으로 다시 라우팅해야 합니다. 테스트를 위해 DNS 또는 호스트 테이블에 sms.domain.com을 추가했는지 확인합니다.

# SMS 게이트웨이 서버 저장소 요구 사항

SMS 게이트웨이 서버에 필요한 자원의 양을 결정하려면 표 D-27의 요구 사항을 토대로 얻어진 숫자와 함께 초당 예상되는 릴레이 메일 수와 RECORD\_LIFETIME 설정을 사용합니다.

표 D-27에서는 기록 데이터, SMPP 릴레이 및 SMPP 서버에 대한 요구 사항을 보여 줍니다.

**표 D-27** SMS 게이트웨이 서버 저장소 요구 사항

| 구성 요소         | 요구 사항                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 메모리 내장 기록 레코드 | <p>릴레이된 각 메일은 <math>33+m+s</math>바이트의 가상 메모리가 필요합니다. 여기서 <math>m</math>은 메일의 SMS 메일 아이디의 길이(<math>1 \leq m \leq 64</math>)이고 <math>s</math>는 메일의 SMS 소스 주소의 길이(<math>1 \leq s \leq 20</math>)입니다.</p> <p>MAKE_SOURCE_ADDRESS_UNIQUE=0이면 <math>16+m</math>바이트만 사용됩니다. 64비트 운영 체제의 경우 레코드당 <math>49+m+s</math>바이트의 가상 메모리가 사용됩니다(MAKE_SOURCE_ADDRESS_UNIQUE=0일 경우 <math>24+m</math>).</p> <p>또한 힙 할당자가 실제로 각 레코드에 대해 더 큰 가상 메모리를 할당할 수 있습니다.</p> <p>최대 레코드 수는 430억개입니다(<math>2^{32}-1</math>). 해시 테이블은 레코드 수가 1680만개(<math>2^{24}</math>) 이하인 경우 약 16MB를 사용하고 6710만개(<math>2^{26}</math>) 이하인 경우 약 64MB를 사용하며 6710만개 이상인 경우 약 256MB를 사용합니다.</p> <p>64비트 운영 체제의 경우 메모리 소비량을 두 배로 늘립니다.</p> <p>각 레코드 자체에 필요한 메모리 소비량 외에도 이러한 소비량이 요구됩니다.</p> |



**표 D-27** SMS 게이트웨이 서버 저장소 요구 사항 (계속)

| 구성 요소         | 요구 사항                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 디스크 내장 기록 데이터 | <p>릴레이된 각 메일에는 평균적으로 다음 수의 바이트가 필요합니다.</p> $81+m+2s+3a+S+2i$ <p>여기서</p> <ul style="list-style-type: none"> <li>• m는 SMS 메일 아이디의 평균 길이이며 <math>1 \leq m \leq 64</math>입니다.</li> <li>• s는 SMS 소스 주소의 평균 길이이며 <math>1 \leq s \leq 20</math>입니다.</li> <li>• a는 전자 메일 주소의 평균 길이이며 <math>3 \leq a \leq 129</math>입니다.</li> <li>• S는 Subject:헤더 행의 평균 길이이며 <math>0 \leq S \leq 80</math>입니다.</li> <li>• i는 전자 메일 봉투 아이디의 평균 길이이며 <math>0 \leq i \leq 129</math>입니다.</li> </ul> <p>특정 레코드의 크기는 메일의 봉투 From: 및 To: 주소의 길이, 봉투 및 메일 아이디의 길이, Subject:헤더 행의 길이에 따라 달라집니다.</p> <p>최대 레코드 길이는 910바이트입니다.</p> <p>MAKE_SOURCE_ADDRESS_UNIQUE=0이 사용될 때 각 레코드의 크기(바이트)는 다음과 같습니다.</p> $78+m+3a+S+2i$ |
| SMPP 릴레이      | <p>릴레이된 각 SMPP 세션은 두 개의 TCP 소켓 즉, 로컬 SMPP 클라이언트를 가진 TCP 소켓과 원격 SMPP 서버를 가진 TCP 소켓을 사용합니다. 32비트 운영 체제에서는 연결당 약 1KB의 가상 메모리가 사용되고 64비트 운영 체제에서는 약 2KB의 가상 메모리가 사용됩니다.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| SMPP 서버       | <p>각 받는 연결은 하나의 TCP 소켓을 사용합니다. 32비트 운영 체제에서는 연결당 약 1KB의 가상 메모리가 사용되고 64비트 운영 체제에서는 약 2KB의 가상 메모리가 사용됩니다.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

예를 들어, 초당 평균 50개의 메일이 릴레이될 것으로 예상할 경우 SMS 소스 주소의 길이는 13바이트, SMS 메일 아이디의 일반 길이는 12바이트, 전자 메일 주소는 24바이트, Subject: 행은 40바이트, 전자 메일 및 봉투 아이디는 각각 40바이트이고, 기록 데이터는 7일 동안 보관되며, 그 이후에는 다음과 같습니다.

- 저장할 기록 레코드가 3024만개이며 이러한 레코드는 각각 메모리와 디스크에서 평균 58바이트 및 311바이트의 길이를 가집니다.
- 기록 레코드의 메모리 내장 소비량은 약 1.70GB(1.6GB + 64MB)입니다.
- 디스크 내장 저장소는 약 8.76GB입니다.

모든 디스크 내장 요구 사항을 처리하기 위해 충분한 디스크가 제공될 수 있지만 32비트 시스템의 가상 메모리 요구 사항은 약 2GB로 엄격하게 제한됩니다. 필요한 가상 메모리나 디스크 저장소의 양을 줄이려면 RECORD\_LIFETIME 옵션을 사용하여 레코드를 보유하는 시간을 줄입니다.

## 설치 워크시트

이 부록에서는 설치를 계획할 수 있는 워크시트를 제공합니다. 다음 워크시트가 포함되어 있습니다.

- [Directory Server 설치](#)
- [Administration Server 초기 런타임 구성](#)
- [Directory Server 설정 스크립트\(comm\\_dssetup.pl\)](#)
- [Messaging Server 초기 런타임 구성](#)

# Directory Server 설치

Java Enterprise System 설치 프로그램 또는 이전 설치를 통해 Directory Server를 설치했습니다. 표 E-1(*Messaging Server Deployment Planning Guide*에 표시된 워크시트의 복제본)에 Directory Server 설치 및 구성 매개 변수를 기록합니다. Administration Server 및 Messaging Server를 설치하고 구성할 때 이 매개 변수가 필요합니다.

**표 E-1** Directory Server 설치 매개 변수

| 매개 변수:          | 설명:                                                                                                                | 예:                        | 사용:                                                     | 사용자의 답변:                                                                                                |
|-----------------|--------------------------------------------------------------------------------------------------------------------|---------------------------|---------------------------------------------------------|---------------------------------------------------------------------------------------------------------|
| 디렉토리 설치 루트      | 서버 프로그램, 구성, 유지 관리 및 정보 파일을 저장하는 Directory Server 시스템의 전용 디렉토리입니다.                                                 | /var/mps/server<br>root/  | comm_dssetup.pl<br>Perl 스크립트                            |                                                                                                         |
| 호스트             | 호스트 이름은 IP 호스트 이름이며, "짧은 형식" 호스트 이름 (예: fiddle)이거나 정규화된 호스트 이름일 수 있습니다. 정규화된 호스트 이름은 호스트 이름과 도메인 이름의 두 부분으로 구성됩니다. | fiddle.west.ses<br>ta.com | Administration<br>Server 구성                             | 41페이지의 "Messaging Server 구성을 위해 Directory Server 준비"를 참조하십시오.                                           |
| LDAP 디렉토리 포트 번호 | LDAP Directory Server의 기본값은 389입니다.                                                                                | 389                       | Administration<br>Server 구성 및<br>Messaging Server<br>구성 | 41페이지의 "Messaging Server 구성을 위해 Directory Server 준비" 및 51페이지의 "Messaging Server 초기 런타임 구성 만들기"를 참조하십시오. |

| 매개 변수:             | 설명:                                                                                                     | 예:                                      | 사용:                                                                                                                                                                     | 사용자의 답변: |
|--------------------|---------------------------------------------------------------------------------------------------------|-----------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|
| 관리자 아이디 및 비밀번호     | 구성 정보를 담당하는 관리자입니다.<br><br>관리자의 비밀번호입니다.                                                                | Admin<br><br>PaSsWoRd                   | Administration<br>Server 구성<br><br>41페이지의 "Messaging Server 구성을 위해 Directory Server 준비"를 참조하십시오.                                                                        |          |
| 사용자 및 그룹 트리 접미어    | 디렉토리 트리의 최상위에 있는 LDAP 항목의 고유 이름으로서 이 위치 아래에 사용자 및 그룹 데이터가 저장됩니다.                                        | o=usergroup                             | comm_dssetup.pl<br>Perl 스크립트<br><br>41페이지의 "Messaging Server 구성을 위해 Directory Server 준비"를 참조하십시오.                                                                       |          |
| 디렉토리 관리자 DN 및 비밀번호 | UNIX의 슈퍼유저 사용자에게 해당하는 권한 있는 디렉토리 관리자입니다. 일반적으로 이 관리자는 사용자와 그룹 데이터의 관리를 담당합니다.<br><br>디렉토리 관리자의 비밀번호입니다. | cn=Directory<br>Manager<br><br>pAsSwOrD | comm_dssetup.pl<br>Perl 스크립트 및<br>Messaging Server<br>구성<br><br>41페이지의 "Messaging Server 구성을 위해 Directory Server 준비" 및 51페이지의 "Messaging Server 초기 런타임 구성 만들기"를 참조하십시오. |          |
| 관리 도메인             | 관리 제어의 영역입니다.                                                                                           | System Lab                              | Administration<br>Server 구성<br><br>41페이지의 "Messaging Server 구성을 위해 Directory Server 준비"를 참조하십시오.                                                                        |          |

# Administration Server 초기 런타임 구성

Java Enterprise System 설치 프로그램을 통해 Administration Server 초기 런타임 구성 프로그램을 실행할 때 표 E-2(Messaging Server Deployment Planning Guide에 표시된 워크시트의 복제본)에 설치 매개 변수를 기록합니다. Messaging Server 초기 런타임 구성 시 이 매개 변수가 필요합니다. 또한 특정 질문에 답하기 위해 948페이지의 "Directory Server 설치" 확인 목록을 참조해야 할 수 있습니다.

**표 E-2** Administration Server 초기 런타임 구성 프로그램 매개 변수

| 매개 변수                                     | 설명                                                                        | 예                                         | 사용자의 답변: |
|-------------------------------------------|---------------------------------------------------------------------------|-------------------------------------------|----------|
| 정규화된 도메인 이름                               | 호스트 시스템의 정규화된 도메인 이름입니다.                                                  | fiddle.west.sesta.com                     |          |
| 서버 루트 정의                                  | 서버 프로그램, 구성, 유지 관리 및 정보 파일을 저장하는 Administration Server의 전용 설치 루트입니다.      | /var/mps/serverroot                       |          |
| UNIX 시스템 사용자                              | 실행하려는 프로세스에 대해 적절한 권한을 갖도록 하기 위해 시스템 사용자에게 지정되는 특정 권한입니다.                 | inetuser                                  |          |
| UNIX 시스템 그룹                               | 특정 UNIX 시스템 사용자가 속해 있는 그룹입니다.                                             | inetgroup                                 |          |
| Configuration Directory Server            | 948페이지의 "Directory Server 설치" 도중 지정된 호스트와 포트입니다.                          | Host<br>fiddle.west.sesta.com<br>Port 389 |          |
| Configuration Directory Server 관리자 및 비밀번호 | 948페이지의 "Directory Server 설치" 도중 지정된 관리자 아이디입니다.<br><br>관리자 아이디의 비밀번호입니다. | Admin<br>PaSsWoRd                         |          |

표 E-2 Administration Server 초기 런타임 구성 프로그램 매개 변수 (계속)

| 매개 변수                    | 설명                                                                                                                                         | 예           | 사용자의 답변: |
|--------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|-------------|----------|
| 관리 도메인                   | 관리 제어의 영역입니다.<br>Messaging Server와<br>Directory Server를 같은 시<br>스템에 설치한 경우 948페<br>이지의 "Directory Server<br>설치"에서 같은 관리 도메<br>인을 선택해야 합니다. | System Lab2 |          |
| Administrative Server 포트 | Administration Server 전용<br>의 고유 포트 번호입니다.                                                                                                 | 5555        |          |

## Directory Server 설정 스크립트(comm\_dssetup.pl)

Messaging Server 구성을 위한 Directory Server를 준비하기 위해 Directory Server 설정 스크립트(comm\_dssetup.pl)를 실행하는 경우 표 E-3에 설치 매개 변수를 기록하십시오. Messaging Server 초기 런타임 구성 시 이 매개 변수가 필요합니다.

**표 E-3** comm\_dssetup.pl 스크립트 매개 변수

| 매개 변수           | 설명                                                                                                                                             | 예                    | 사용자의 답변: |
|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------|----------------------|----------|
| 서버 루트           | 서버 프로그램, 구성, 유지 관리 및 정보 파일을 저장하는 Directory Server의 전용 설치 루트입니다.                                                                                | /var/mps/serverroot/ |          |
| 서버 인스턴스         | 대부분의 기능을 담당하는 LDAP Directory Server 데몬 또는 서비스입니다. 특정 배포의 경우 사용자와 그룹을 유지 관리하기 위한 전용 인스턴스를 지정하고 구성에 대해서는 별도의 인스턴스를 지정해야 할 수 있습니다.                | slapd-varrius        |          |
| DC 루트           | 2 트리 DIT 준비 모델(Sun LDAP Schema 1 또는 Sun LDAP Schema 2 호환 모드)을 사용하려는 경우 DC 트리는 로컬 DNS 구조를 미리하며, 시스템에서 사용자와 그룹 데이터 항목이 포함된 조직 트리에 대한 색인으로 사용됩니다. | o=internet           |          |
| 사용자 및 그룹 기본 접미어 | 사용자 및 그룹 항목에 대한 이름 공간이 포함된 조직 트리의 최상위 항목입니다.                                                                                                   | o=usergroup          |          |



**표 E-3** comm\_dssetup.pl 스크립트 매개 변수 (계속)

| 매개 변수              | 설명                                                                                                                   | 예                                    | 사용자의 답변: |
|--------------------|----------------------------------------------------------------------------------------------------------------------|--------------------------------------|----------|
| 디렉토리 관리자 DN 및 비밀번호 | 조직 트리의 사용자 및 그룹 데이터를 담당하는 관리자입니다. Sun Java Enterprise System 설치 프로그램에서 지정한 내용과 같아야 합니다.<br><br>디렉토리 관리자 DN의 비밀번호입니다. | cn=Directory Manager<br><br>pAsSwOrD |          |

# Messaging Server 초기 런타임 구성

Messaging Server 초기 런타임 구성 프로그램을 실행하는 경우 설치 매개 변수를 표 E-4에 기록하십시오. 또한 특정 질문에 답하기 위해 948페이지의 "Directory Server 설치" 확인 목록을 참조해야 할 수 있습니다.

**표 E-4** Messaging Server 초기 런타임 구성 프로그램 매개 변수

| 매개 변수                                   | 설명                                                                                                                         | 예                                                                                                           | 사용자의 답변: |
|-----------------------------------------|----------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------|----------|
| 구성 및 데이터 디렉토리                           | 모든 Messaging Server 구성 파일이 포함됩니다.<br><br><i>msg_svr_base/data</i> 디렉토리가 이 디렉토리에 심볼릭 링크됩니다.                                 | <code>/var/opt/SUNWmsgsr</code>                                                                             |          |
| UNIX 시스템 사용자                            | 실행하려는 프로세스에 대해 적절한 권한을 갖도록 하기 위해 시스템 사용자에게 지정되는 특정 권한입니다. 이 시스템 사용자는 Administration Server 초기 런타임 구성에서 지정한 사용자와 같으면 안 됩니다. | <code>mailsrv</code>                                                                                        |          |
| UNIX 시스템 그룹                             | 특정 UNIX 시스템 사용자가 속해 있는 그룹입니다. 이 시스템 그룹은 초기 런타임 구성에서 지정한 그룹과 같으면 안 됩니다.                                                     | <code>mail</code>                                                                                           |          |
| 구성 디렉토리 LDAP URL, 디렉토리 관리자 및 비밀번호       | Configuration Directory Server, LDAP URL, 바인드 DN 및 비밀번호입니다.                                                                | <code>ldap://fiddle.west.sesta.com:389</code><br><code>cn=Directory Manager</code><br><code>PaSsWoRd</code> |          |
| 사용자 및 그룹 디렉토리 LDAP URL, 디렉토리 관리자 및 비밀번호 | 사용자 및 그룹 Directory Server, LDAP URL, 바인드 DN 및 비밀번호입니다.<br><br>사용자 및 그룹 디렉토리와 구성 디렉토리를 별도로 지정하는 것이 좋습니다.                    | <code>ldap://fiddle.west.sesta.com:389</code><br><code>cn=Directory Manager</code><br><code>PaSsWoRd</code> |          |

**표 E-4** Messaging Server 초기 런타임 구성 프로그램 매개 변수 (계속)

| 매개 변수               | 설명                                                                                   | 예                                                                                                                                                                  | 사용자의 답변: |
|---------------------|--------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|
| 포스트마스터 전자 메일 주소     | 포스트마스터 메일을 모니터링할 관리자의 전자 메일 주소입니다. 주소는 정규화된 주소여야 하며 해당 주소와 연결된 메일함이 있는 유효한 주소여야 합니다. | pma@siroe.com                                                                                                                                                      |          |
| 관리자 계정의 비밀번호        | 서비스 관리자, 사용자/그룹 관리자, 최종 사용자 관리자 권한 및 PAB 관리자와 SSL 비밀번호에 사용할 비밀번호입니다.                 | paSSwoRD                                                                                                                                                           |          |
| 기본 전자 메일 도메인        | 지정된 도메인이 없을 때 사용되는 전자 메일 기본값입니다.                                                     | siroe.com                                                                                                                                                          |          |
| 기본 전자 메일 도메인의 조직 이름 | 조직이 속해 있으며 조직 트리를 구성하는 데 사용되는 조직 이름입니다.                                              | 예를 들어, 조직 이름이 Engineering인 경우 siroe.com(기본 전자 메일 도메인)의 모든 사용자는 LDAP DN o=Engineering, o=usergroup 아래에 배치됩니다.<br><br>사용자 및 그룹 디렉토리 접미어는 comm_dssetup.pl에 지정되어 있습니다. |          |



# 용어집

이 설명서 세트에 사용되는 전체 용어 목록은 Java Enterprise System 용어집 (<http://docs.sun.com/doc/819-1934>)을 참조하십시오.



## 기호

228

!(느낌표)

주석 표시 기호 227

\$? 308

\$A 307

\$B 306

\$C 305, 308

\$E 306

\$F 306

\$M 305, 308

\$N 305, 308

\$P 307

\$Q 305, 308

\$R 204, 306

\$S 307

\$T 308

\$U 대체 시퀀스 296

\$V 198

\$V 메타 문자 202

\$X 307

\$Z 198

%(백분율 기호) 305

(A\|B)%C 368

\* 637

\*.CHANGES 파일 75

\*.MERGED 파일 75

+ 126

.HELD 메일 790

.HELD 메일 대기열 파일 790

/ 일치 234

/etc/nsswitch.conf 784

@ 기호 305, 308

@(골뱅이 기호) 308

\! (느낌표)

주소 292

\| 세로 막대 287

## 숫자

220 배너 784

5.2에서 업그레이드 73

733 367

822 366

8비트 데이터 342

8비트 문자 793

## 가

가상 도메인

액세스 제어 672

개별 채널 시작 775

개별 채널 중지 775

개인 및 공개 키를 확인하기 위한 순서도를 보여 주는 그래픽입니다. 705

게시 및 가입 843

경로 지정

명시적 369

암시적 369

경보 속성

디스크 공간 604

고가용성

구성 해제 99

자동 재시작 112

추가 구성 지침 97

클러스터 에이전트 86

IP 주소 바인딩 97

Sun Cluster 93

Sun Cluster 전체 조건 92

useconfig 86

고가용성 구성 해제 99

고아 계정 602

고유 sendmail 구성 파일 사용 65

고정적인 오류 메시지 308

골뱅이 기호(@) 292

공식 호스트 이름이 너무 깁니다.

MTA 오류 메시지 797

공유 폴더 559

공유 폴더 564

데이터 모니터 및 유지 관리 568

분산 561, 566

사용 가능 또는 사용 불가능 566

액세스 제어 목록 565

ACL 565

공유 폴더, IMAP 603

관리

Messenger Express Multiplexor 178

관리 토폴로지 118

관리자 액세스 제어

구성 661

메시지 저장소 557

서버 작업 663

서버 전체 663

구문 문제

SSR 792

구분자, 설정 126

구성

고가용성 93

구성 요소 53

비밀번호 104

선택적 플래그 52

초기 런타임 51

포트 번호 70

Veritas Cluster Server 88

구성 디렉토리 118, 120

구성 요소

구성 53

구성 파일

디스패처 245

빈 행 228

일치 246

조정 247

환경 설정 246

aliases 244

conversion 244

dispatcher.cnf 751

imta.cnf

구조 227

Job Controller 247

MTA 226

nsswitch.conf 349

sslpassword.conf 654

구성원 탭 856

그룹

메일 목록 참조

구성원 탭 856

전자 메일 전용 구성원 857

그룹 확장 속성 218

그룹, 만들기 105

그룹, 작동 원리 218

기본 데이터 크기 752

기본 도메인

Messenger Express Multiplexor 176

기본 언어, 도메인 117

기본 오류 메시지

다시 쓰기 및 채널 일치 실패 308



## 나

날짜

두 자리 381

날짜 변환 381

날짜 사양

요일 381

날짜 필드 381

내부 모듈(PKCS #11) 651

내부 헤더

다시 쓰기 373

내부 헤더 다시 쓰기 373

네 자리 날짜 381

네트워크 문제 808

네트워크 보안 서비스 660

네트워크 서비스 249

느낌표(!) 292

## 다

다른 시스템 구성 요소와 S/MIME 애플릿의 관계를 보여 주는 그래픽입니다. 687

다시 쓰기

내부 헤더 373

다시 쓰기 규칙 198, 228

검사 378

구조 282

다시 쓰기 프로세스 완료 294

다시 쓰기 후의 구문 검사 295

대체, 단일 필드 304

대체, 리터럴 문자 300

대체, 사용자 제공 루틴 303

대체, 아이디 및 하위 주소 299

대체, 일반 데이터베이스 302

대체, 지정된 매핑 302

대체, 호스트/도메인 및 IP 리터럴 300

대체, LDAP 쿼리 URL 300

도메인 리터럴 295

많은 수 처리 309

모든 주소와 일치 287

반복되는 템플릿 A%B 288

방향 특정 306

백분율 핵 286

뱅 스타일 286

빈 행 192, 228

설명 189

스캔 293

실패 295

예 310

위치 특정 306

일반 템플릿 A%B@C 288

작업 290

제어 시퀀스 296

지정된 경로 템플릿 A@B@C 289

태그된 규칙 집합 287

테스트 309

템플릿 287, 294

템플릿 대체 296

템플릿의 대소문자 구분 289

패턴 및 태그 284

패턴 일치 290

호스트 위치 특정 307

UUCP 주소 286

다시 쓰기 규칙 실패 295

다시 쓰기 오류 메시지 308

다시 쓰기 프로세스 실패 290

다시 쓰기 후의 구문 검사 295

다시 쓰기와 관련된 오류 메시지 처리 308

단일 사인 온(SSO)

Messenger Express 구성 매개 변수 152

단일 사인 온(SSO), SSO 참조 141

대기열 807

대기열, 메일 192

대기열에서 제외되지 않은 메일 785

대량 메일 615

대상 주소 394

대용량 메일 자동 조각화 386

대체 변환 채널 399

대체 전자 메일 주소. 850, 858

대체, 다시 쓰기 규칙

## 라

- 고유 문자열 304
- 대화식 모드 43
- 데이터 파일 69
- 데이터베이스
  - 일반 241
- 데이터베이스 로그 파일
  - 메시지 저장소 문제 해결 628
- 도메인
  - 데이터베이스 309
  - 리터럴 295
  - 인바운드 처리 중지 776
  - 제거 106
  - 주소에서의 지정 290
  - DNS 확인 340
- 도메인 기본 언어 117
- 도메인 삭제 106
- 도메인 제거 106
- 동시 연결, 제어 889
- 두 자리 날짜 381
- 두 자리 연도 381
- 디렉토리 194
  - 로그 파일 755
  - 메시지 저장소 553
- 디렉토리 레이아웃 68
- 디버깅 396
  - 디스패처 751
- 디버깅 도구
  - 매핑 테이블 776
  - 메일 파일 780
  - channel\_master.log-\* 파일 780
  - imsimta cache -view 788
  - imsimta process 773
  - imsimta qm 771, 807
  - imsimta qm start 및 stop 775
  - imsimta run 775
  - imsimta test -rewrite 771, 799
  - log\_message\_id 777
  - mail.log\_current 778
  - mail.log\_current 레코드 780
  - master\_debug 778
  - slave\_debug 778
  - subdirs 779

- TCP/IP 네트워크
  - PING, TRACEROUTE, 및 NSLOOKUP 785
  - tcp\_local\_slave.log-\* 파일 780
- 디스크 공간 804
  - 모니터링 604
  - 줄이기 606
  - 할당량 570
- 디스크 사용 824
- 디스패처
  - 구성 파일 245
  - 다시 시작 188
  - 디버깅 및 로그 파일 751
  - 문제 해결 783
  - 설명 187
  - 시작 188
  - 제어 188
  - 중지 188
  - MAX\_CONNS 옵션 188
  - MIN\_CONNS 옵션 188
  - MIN\_PROCS 옵션 187
- 디스패처 구성 파일 245, 751
- 따옴표가 있는 로컬 부분 373

## 라

- 라우팅 주소 210
- 런타임 구성 51
- 로그 파일 69
  - 메시지 저장소 문제 해결 626
  - MTA 관련 문제 해결 774
- 로그인
  - 비밀번호 기반 647
  - 인증서 기반 128, 658
- 로그인 구분자
  - Messenger Express Multiplexor 176
- 로그인 구분자, POP용 126
- 로그인 서비스
  - 비밀번호 기반 로그인 127
- 로깅 395, 723
  - 관리를 위한 도구 728

- 구조 757
- 로그 보기 760
- 로그 분석 728
- 로그 파일 디렉토리 755
- 메시지 저장소 766
- 메시지 저장소 및 관리 서버 753
- 범주 755
- 서비스 로그 관리 753
- 수준 753
- 심각도 수준 753
- 옵션 757
- 유형 724
- 채널 728
- 파일 724
- 파일 형식 756
- 환경 설정 758
- LOG\_CONNECTION 옵션 735
- LOG\_FILENAME 옵션 734
- LOG\_MESSAGE\_ID 옵션 734
- LOG\_MESSAGES\_SYSLOG 옵션 734
- LOG\_PROCESS 옵션 735
- LOG\_USERNAME 옵션 735
- MTA 728, 733
- MTA 메일 및 연결 728
- MTA 예 735
- MTA 항목 코드 730
- MTA 활성화 733
- SEPARATE\_CONNECTION\_LOG 옵션 735
- 로컬 채널
  - 환경 설정 408
- 로컬 호스트가 너무 깁니다.
  - MTA 오류 메시지 796
- 루핑 메일 789
  - 잘못된 알람 메일 처리 789
  - 포스트마스터 주소가 손상되었습니다. 789
- 릴레이
  - 추가 528
- 릴레이 차단 531
- 릴레이 차단, 제거 528
- 링크 수 607

## 마

- 마스터 프로그램 248, 249, 358
- 마이그레이션
  - 메시지 저장소 크기 606
  - 메일함 80
- 마지막 호스트 349
- 만료
- 매핑 검사 238
- 매핑 이름이 너무 깁니다.
  - MTA 오류 메시지 795
- 매핑 이름이 중복되었습니다.
  - MTA 오류 메시지 795
- 매핑 작업 232
- 매핑 테이블 229, 776
  - 많은 수의 항목 처리 537
  - 설명 512
  - 전체 목록 229
- COMMENT\_STRINGS 374
- FROM\_ACCESS 513
- MAIL\_ACCESS 513
- NOTIFICATION\_LANGUAGE 265
- ORIG\_MAIL\_ACCESS 513
- ORIG\_SEND\_ACCESS 513
- PORT\_ACCESS 513, 525
- SEND\_ACCESS 513
- SMS\_Channel\_TEXT 881
- X-REWRITE-SMS-ADDRESS 881
- 매핑 테이블, 액세스 제어 참조
- 매핑 템플릿 대체 및 메타 문자 235
- 매핑 템플릿의 대체 235
- 매핑 템플릿의 메타 문자 235
- 매핑 파일 229, 246
  - 찾기 및 로드 229
  - 파일 형식 230
- 매핑 패턴 와일드카드 232
- 매핑 항목 템플릿 235
- 매핑 항목 패턴 232
- 멀티플렉서. Messaging Multiplexor 참조
- 메시지
  - 대기열에서 제거 370
  - 수신자 헤더 없음 371

- 자동 제거
  - 정리
  - 제거 556
  - 조각화 388
  - 크기 제한 387
- 메시지 저장소 53
  - 개요 552
  - 고아 제거 602
  - 관리자 액세스 557
  - 기본 분할 영역 595
  - 데이터 복원 614
  - 디렉토리 레이아웃 553
  - 디스크 공간 감소 606
  - 디스크 할당량 구성 570
  - 로깅 723, 753
  - 로깅 예 766
  - 메일 삭제 557
  - 메일 정리 557
  - 메일 제거 557
  - 메일 추적 764
  - 메일함 검사 및 복구 635
  - 메일함 재작성 634
  - 명령줄 유틸리티 552
  - 문제 해결 625
  - 백업 그룹 612
  - 백업 정책 611
  - 백업, 휴지통 제외 615
  - 분할 영역 579, 594
  - 분할 영역 구성 593
  - 분할 영역, 기본값 변경 597
  - 액세스 제어 557
  - 에이징 정책 581
  - 유예 기간 579
  - 유지 관리 및 복구 절차 597
  - 일반 문제 및 해결 방법 637
  - 자동 메일 제거
  - 중분 백업 614
  - 타사 소프트웨어 사용 622
  - 할당량(참조, 할당량) 573
  - imsbackup 유틸리티 613
  - imsrestore 유틸리티 614
  - Legato Networker를 백업용으로 사용 618
  - mboxlist 데이터베이스 로그 파일 825
  - primary 분할 영역 593
  - RAID 기술 594
  - reconstruct 유틸리티 633
  - stored 유틸리티 604
  - 메시지 저장소 문제 해결 625, 626
    - 데이터베이스 로그 파일 628
    - 모니터링 626
    - 사용자 폴더 629
    - 일반 문제 및 해결 방법
      - 사용자 메일함 디렉토리 문제 638
    - 코어 파일 629
    - 하드웨어 공간 626
    - stored 작업 628
    - stored 프로세스 628
  - 메시지 저장소 복원 610
  - 메시지 저장소 복원, 고려 사항 616
  - 메시지 저장소의 백업 절차
    - 단일 복사본 절차 610
    - 백업 그룹 만들기 612
    - 백업 유틸리티 613
    - 병렬 백업 612
    - 설명 610
    - 작업량이 가장 많은 시간대 611
    - 전체 백업 611
    - 정책 만들기 611
    - 중분 백업 611
    - 직렬 백업 612
    - 타사 소프트웨어 사용 622
    - Legato Networker 사용 618
  - 메일 거부 389
  - 메일 경로에서 채널 확인
    - 방법 777
  - 메일 대기열 192, 807
  - 메일 대기열 디렉토리
    - 문제 해결 771
  - 메일 대기열, 모니터링 807
  - 메일 만료 581
  - 메일 목록
    - 구성원 탭(그룹) 856
    - 기존 그룹 액세스 857

- 다음에 대한 증재자 864
- 다음에 대한 Netscape Console 액세스 856
- 동적 멤버십 기준 861
- 메일 거부 작업 864
- 메일 게시 제한 863
- 메일 탭 857
- 목록 구성원 860
- 목록 소유자 859
- 목록(전자 메일 전용) 구성원 추가 862
- 새 그룹 만들기 856
- 전자 메일 전용 구성원 857
- 주소(주) 858
- 호스트 이름 숨기기 859
- LDAP 검색 URL 861
- 메일 목록, 만들기 105
- 메일 변환 태그 419
- 메일 복사본당 단일 대상 시스템 394
- 메일 사용자
  - 기존 사용자 액세스 848
  - 다음에 대한 전달 주소 853
  - 다음에 대한 Netscape Console 액세스 847
  - 대체 주소 850
  - 메일 탭 848, 849
  - 새 사용자 만들기 848
  - 자동 회신 설정 854
  - 전달 옵션 구성 851
  - 주소 지정 849
  - 주소(주) 850
  - 프로그램 전달 옵션 852
  - 호스트 이름 숨기기 850
  - 휴가 모드 855
  - POP/IMAP 전달 옵션 851
  - UNIX 전달 옵션 853
- 메일 삭제 556
- 메일 액세스 123
  - 도메인 이름 없이 로그인 127
  - 로그인 요구 사항 126
  - 비밀번호 기반 127
  - 서비스 포트 번호 124
  - 일반 구성 124
  - 포트, 암호화 125
  - HTTP
    - HTTP 서비스 123
    - IMAP
    - POP
    - POP, IMAP 또는 HTTP 124
- 메일 전달 349, 808
- 메일 정리 556
- 메일 정지 780
- 메일 제거 556
- 메일 조각 모음 385
- 메일 처리 410
- 메일 탭 848, 849, 857
- 메일 필터링
  - 매핑 테이블 512
  - 사용자별 필터 541
  - 서버측 규칙 541
  - 설명 511
  - 채널 수준 필터 541
  - MTA 차원 필터 541
- 메일 헤더
  - 날짜 필드 381
- 메일 헤더 행
  - 자르기 381
- 메일 헤더 행 자르기 381
- 메일이 전달되지 않음 787
- 메일함
  - 관리 597
  - 복구 632
  - 이름 지정 규칙 601
  - 자동 메일 제거 581
  - 재구성 633
  - 전달할 기본 메일함 601
  - INBOX 601
  - mboxutil 유틸리티 598
  - reconstruct 유틸리티 632
- 메일함 사양 373
- 메일함 이동 595
- 메일함 인코딩
  - restricted 373
- 명령줄 유틸리티 603
  - mboxutil 598
  - MTA 256

- reconstruct 603
- stored 604
- 명시적 라우팅 369
- 명시적 라우팅, 사용 안 함 369
- 모니터링 801
  - 데이터베이스 로그 파일 814
  - 도구 및 유틸리티 815
  - 디스크 공간 804
  - 디스패처 809
  - 로그 파일 802
  - 메시지 저장소 813
  - 메시지 저장소 데이터베이스 잠금 814
  - 메일 대기열 807
  - 메일 액세스 810
  - 사용자 액세스 624
  - 시스템 성능 803
  - 웹 메일 서비스 811
  - 자동 재시작 110
  - 전달 시간 803
  - 전달 실패 비율 808
  - 포스트마스터 메일 802
- CPU 사용 806
- httpd 811
- imapd 811
- Job Controller 809
- LDAP 서버 815
- LDAP Directory Server 810
- mbxlist 디렉토리 814
- msprobe 803, 824
- MTA 807
- POP 및 IMAP 서버 815
- popd 811
- SMTP 연결 808
- stored 812, 815
- watcher 801, 824
- 모든 주소와 일치 287
- 문자 세트 레이블 생성 341
- 문자 세트 레이블링 341
- 문제 해결
  - 로그인 실패, POP 126
  - 메시지 저장소 637
  - 와일드카드 및 명령 637

## 바

- 바이러스 백신 441, 455, 473
  - 스캐너 399
- 바이러스 스캔 410
- 바이러스 필터링 441
- 반복되는 백분율 기호 292
- 반환되는 메일
  - 내용 274
- 받는 메일 783
- 받는 메일을 위한 대체 채널 350
- 받는 연결 350
- 받은 메일
  - 인코딩 791
- 방향 특정 다시 쓰기 306
- 배너
  - IMAP 126
  - POP 126
- 백분율 기호(%) 305, 308
- 백분율 핵 규칙 286
- 백업 그룹 612
- 뱅 스타일 주소 규칙 292
- 뱅 스타일(UUCP) 주소 286
- 버전이 일치하지 않습니다. 797
- 변환 제어 244
- 변환 채널 410
  - 구성 410, 413
  - 대체 399
  - 매핑 테이블 421
  - 메일 바운스 423
  - 메일 보관 423
  - 메일 삭제 423
  - 변환 제어 244
  - 변환 처리를 위한 트래픽 413
  - 예 425
  - 전달 지시문 420
  - 정보 흐름 416
  - 제어 매개 변수 427
  - 처리 414
  - 출력 옵션 420
  - 헤더 관리 421

변환 처리를 위한 트래픽 413  
 변환 태그 419  
 변환 파일 244, 414  
 별칭 254  
 별칭 데이터베이스 376  
 별칭 파일 263, 376  
 별칭 포함 파일을 열 수 없습니다.  
   MTA 오류 메시지 794  
 별칭 확장 202  
 별칭이 중복되었습니다.  
   MTA 오류 메시지 795  
 별표 793  
 별표, 주소 187  
 보관 채널 409  
 보낸 사람  
   주소 369  
 보다 작음 기호(<) 228  
 보안  
   비밀번호 기반 로그인 127  
   인증 기법 644  
   인증서 기반 로그인 128, 658  
   클라이언트 액세스 제어 132  
   about 642  
   HTTP 서비스 132, 643  
   IMAP 서비스 132  
   POP 서비스 132  
   S/MIME,  
     S/MIME 참조  
   SASL 644  
   SMTP 서비스 648  
   SSL 649  
   TCP 서비스에 대한 클라이언트 액세스 664  
   TLS 649  
 복구 작업  
   메일함 632  
   reconstruct 유틸리티 603  
 복원, Legato Networker 사용 621  
 복제본 58  
 봉투의 To: 주소 306  
 부분 메일 385

부속 도메인 199, 224  
 분할 영역  
   가득 참 595  
   경로 이름 595  
   기본 595  
   메시지 저장소 579  
   메시지 저장소에 대해 구성 593  
   별명 595  
   사이에서 메일함 이동 595  
   추가 594  
   primary 593  
   RAID 기술 594  
 분할 영역, 잘못된 638  
 비밀번호 104  
 비밀번호 로그인 647  
 비밀번호 수정 104  
 비밀번호 인증  
   로그인 참조  
   HTTP 서비스 127  
   IMAP 서비스 127  
   LDAP 사용자 디렉토리 121  
   POP 서비스 127  
   SMTP 서비스 648  
 비밀번호 파일(SSL용) 654  
 비트 플래그 274, 277  
 비표준 메일 형식  
   변환 385  
 빈 봉투 반송 주소 274  
 빈 봉투 주소 274, 277  
 빈 행  
   구성 파일 228

## 사

사용자 관리 유틸리티,  
   Delegated Administrator 참조  
 사용자 구성 변경 782  
 사용자 디렉토리 118  
 사용자 로그인. 로그인 참조

- 사용자 마이그레이션 409
- 사용자 메일함
  - 마이그레이션 80
- 사용자 메일함 디렉토리 문제
  - 메시지 저장소 문제 해결 638
- 사용자 메일함 이동 610
- 사용자 및 그룹
  - UNIX 시스템 40
- 사용자 삭제 105
- 사용자 제거 105
- 사용자 폴더
  - 메시지 저장소 문제 해결 629
- 사용자, 만들기 105
- 사이트 언어 118
- 사전 인증(Messaging Multiplexor) 160
- 사후 설치 디렉토리 레이아웃 68
- 상태 메일
- 상태 알림, 알림 메일 참조
- 서버 시작/중지 107
- 서버 응답 시간. 824
- 서버 인증서
  - 관리 654
  - 설치 652
  - 요청 652
- 서버측 규칙 541
  - 문제 해결 792
  - 작동하지 않음 792
- 서비스
  - 사용 가능/불가능하게 하기 124
  - 시작 및 중지 107
  - HTTP 123
  - IMAP 123
  - MTA 181, 225
  - POP 123
  - SMTP 181, 225
- 서비스 거부 공격 808
- 서비스 매너 126
- 서비스 변환 365
- 선택적 플래그 52
- 설명서
  - 개요 34
  - Communications Services 설명서 위치 35
  - Messaging Server 설명서 위치 34
- 설치 테스트
  - Messenger Express Multiplexor 177
- 설치 프로그램
  - 자동 57
- 설치 후 구성
  - 구성
    - SMTP 차단 62
    - 재부트 간 시작 64
    - 포트 번호 70
- 설치 후 포트 번호 70
- 성능 매개 변수
  - 프로세스 수 129
  - 프로세스당 스레드 130
  - 프로세스당 연결 129
- 성능 및 조정 68
- 성능 향상
  - LMTP 483
- 성능, 릴레이 483
- 세로 막대(\|) 287
- 소스 경로 378
- 소스 라우팅 주소 291
- 소스 채널 특정
  - 다시 쓰기 305
- 소스 파일
  - 포함 228
- 수동으로 채널 프로그램 실행 775
- 수준(로깅) 753
- 스마트 카드 685
- 스왑 공간
  - 명령 798
  - 오류 798
- 스팸 방지 389, 441, 473, 511
  - 도메인 수준 필터링 446
  - 라이브러리 경로 444
  - 사용자 수준 필터 445
  - 수신자 제한 392
  - 스캐너 399
  - 스팸 점수 441, 473



시브(Sieve) 451  
 여러 프로그램 444  
 작동 원리 442  
 작업 451  
 채널 수준 필터링 448, 449  
 클라이언트 라이브러리 443  
 타사 소프트웨어 배포 442  
 필터링할 메일 444  
 Brightmail, Brightmail 참조  
 SpamAssassin,  
   SpamAssassin 참조  
 스팸 필터 541  
 스팸 필터 옵션 452  
 스팸, 스팸 방지 참조  
 스팸,  
   스팸 방지, Brightmail 및 SpamAssassin 참조  
 슬레이브 프로그램 249, 358  
 시브(Sieve) 545  
 시작/중지  
   비 HA 서버 108  
   서버 자동 재시작 110  
   HA 서버 107, 110  
 신뢰할 수 있는 원 145  
 신뢰할 수 있는 응용 프로그램 145  
 실패한 메일 273  
 실패한 전달 358  
 실패한 전달 시도 274  
 심각도 수준(로깅) 753

## 아

아랍어 문자 감지 425  
 알림 메일 ??-272, 273, 276  
   국제화 270  
   내용 반환 차단 271  
   사용자 정의 및 현지화 267  
   생성 및 수정 265  
   전달할 수 없는 메일의 전달 간격 설정 272  
   추가 기능 271

포스트마스터에 대해 전송/차단 273  
 헤더에서 미국 ASCII가 아닌 문자 제거 271  
 알림 메일 참조  
 알림 메일의 변경된 주소 272  
 암시적 라우팅 369  
 암호문  
   about 657  
 암호화  
   가속기 652  
 암호화 설정 122  
 액세스 제어  
   매핑 테스트 527  
   매핑 테이블 512  
   메시지 저장소 557  
   사용자 모니터링 624  
   액세스 필터 만들기 672  
   적용되는 경우 526  
   클라이언트 액세스 132  
   필터 구문 666  
   HTTP 서비스 132, 664  
   IMAP 서비스 132, 664  
   POP 서비스 132, 664  
   SMTP 서비스 512  
   TCP 서비스에 대한 액세스, 개요 664  
 액세스 제어, 매핑 테이블 참조  
 억제 525  
 언어  
   사용자 기본 설정 117  
   서버 사이트 118  
 업그레이드 73  
   메일함 이전 80  
 업데이트  
   구성 74  
 에이징 정책  
   메시지 저장소 581  
   메일 수 581  
   메일함 크기 581  
   지정 581  
 에이징 정책, 자동 메일 제거 참조  
 여러 \$M 절 305  
 여러 대상 주소 394

## 아

- 여러 보내는 채널 350
- 여러 주소 393
- 여러 주소 확장 364
- 여러 프록시 서버
  - Messenger Express Multiplexor 178
- 역방향 데이터베이스 257
  - 채널별 372
- 역방향 매핑 257, 260
- 역방향 주소 369
- 역방향 채널 키워드 259
- 역방향 캐시 210
- 연결 캐싱 346
- 연결, 동시 889
- 오류 메시지
  - 별칭 포함 파일을 열 수 없습니다. 794
  - ch\_facility 초기화 오류 796
  - Messenger Express Multiplexor 177
  - MTA 793
    - 공식 호스트 이름이 너무 깁니다. 797
    - 로컬 호스트가 너무 깁니다. 796
    - 매핑 이름이 너무 깁니다. 795
    - 매핑 이름이 중복되었습니다. 795
    - 별칭이 중복되었습니다. 795
    - 잘못된 별칭입니다. 794
    - 채널 테이블에 중복된 호스트가 있습니다. 795
    - 채널에 대한 공식 호스트 이름이 없습니다. 796
    - 해당 주소가 없습니다. 796
- 오류 알림 메일, 현지화
- 옵션 파일 246
- 와일드카드 637
- 와일드카드 문자, 매핑 232
- 와일드카드 필드 대체 237
- 완성되지 않은 주소 수정 370
- 외부 모듈(PKCS #11) 651
- 외부 사이트에 대한 SMTP 릴레이, NMS에서 허용 530
- 요구 사항
  - comm\_dssetup.pl 42
  - Sun Cluster 92
- 요일
  - 날짜 사양 381
- 워크시트 947
  - Administration Server 950
  - comm\_dssetup.pl 43, 952
  - Directory Server 948
  - Messaging Server 52, 954
- 원격 시스템 350
- 원격 측정 627
- 원래 수신자 517
- 웹 메일
  - HTTP 서비스 136
  - Messenger Express 123
- 위임된 관리 105, 662
- 위치 특정 다시 쓰기 306
- 유휴 연결, 해제 131
- 응용 프로그램 아이디 145
- 이름 서버 조회 349
- 이벤트 알림 서비스(ENS), ENS 참조
- 인사 메일 114
  - 도메인별 115
- 인식되지 않음
  - 도메인 지정 309
  - 호스트 지정 309
- 인증
  - 기법 644
  - 비밀번호 647
  - 인증서 기반 644, 649
  - HTTP 126
  - IMAP 126
  - Messaging Multiplexor 159
  - POP 126
  - SASL 644
  - SMTP 648
- 인증되지 않은 대량 전자 메일 535
- 인증된 주소 352
- 인증서 660
  - 관리 654
  - 설치, 서버 652
  - 설치, 신뢰할 수 있는 CA 653
  - 연기 651
  - 요청, 서버 652
- 인증서 기반 로그인 128, 658

인코딩 387  
 인코딩된 메일 791  
 인코딩된 받은 메일 791  
 일반 데이터베이스 241, 302, 537, 538  
 일반 MTA 오류 메시지 793  
 일치  
 / 일치 234  
 일치 절차, 다시 쓰기 규칙 293

## 자

자동 메일 제거 581  
 규칙 설정 583  
 배포 582  
 사용자 제외 582, 593  
 예약 591  
 예약 GUI 592  
 정책 정의 582, 586  
 GUI 588  
 자동 모드 49  
 자동 설치 57  
 자동 재시작 110  
 자동 재시작, 고가용성 112  
 자동 회신 503  
 설정 854  
 작업 예약 113  
 잘못된 별칭입니다.  
 MTA 오류 메시지 794  
 잘못된 알람 메일 처리  
 루핑 메일 789  
 잘못된 주소 273  
 잘못된 호스트/도메인 오류 799  
 MX 레코드 조회 799  
 장기적인 서비스 실패 273  
 재부트 간 시작 64  
 재검파일, MTA 226, 243  
 전달 보고서, 알람 메일 참조  
 전달 상태 알람, 알람 메일 참조 264  
 전달 실패 808  
 전달 실패 보고서, 알람 메일 참조  
 전달 옵션  
 메일 사용자 851  
 프로그램 전달 852  
 POP/IMAP 전달 851  
 UNIX 전달. 853  
 전달 재시도 간격 358  
 전달 주소 853  
 전달하지 못한 메일 358  
 전자 메일 전용 구성원(그룹) 857  
 정기적인 메일 반송 작업 275  
 정리 557  
 정방향 데이터베이스 261  
 정크 전자 메일  
 제거  
 제거  
 고가용성 99  
 제거된 메일 545  
 보관 545  
 제거된 받은 날짜  
 헤더 행 789  
 제품 버전  
 Messenger Express Multiplexor 178  
 제한  
 행 길이 387  
 제한된 메일함 인코딩 373  
 조각화  
 긴 메일 386  
 조정 파일 247  
 주 전자 메일 주소. 850, 858  
 주석  
 주소 메일 헤더 374  
 주소  
 ! 및 % 사용 367  
 다시 쓰기 370  
 대상 394  
 라우팅 정보 368  
 봉투의 To: 306  
 빈 봉투 반송 274  
 시작

- 369
- 여러 대상 394
- 역방향 369
- 완성되지 않음 370
- 유효하지 않음 273
- 처리 365
- 해석 367, 368
- 주소 다시 쓰기 370
  - 첫 번째 호스트/도메인 지정 추출 291
- 주소 매핑, FORWARD 261
- 주소 메일 헤더
  - 개인 이름 375
  - 주석 374
- 주소 메일 헤더의 개인 이름 375
- 주소 변경 257
- 주소 변환 257
- 주소 역방향 221
- 주소 역방향 데이터베이스 257
- 주소 역방향 제어 259
- 주소 역방향, 채널 특정 260
- 주소 지정 정보
  - 대체 주소 850, 858
  - 메일 목록 858
  - 메일 사용자용 849
  - 전달 주소 853
  - 주 주소 850, 858
- 주소 해석 368
- 주소의 라우팅 정보 368
- 준비 59
- 준비 옵션
  - LDAP 준비 도구 61
- 중재자
  - 메일 목록 864
  - 정의 864
- 중지/시작 107
- 증분 백업 복원 617
- 지연 메일 처리 358
- 지연된 전달 날짜 370
- 지원
  - Solaris 36

## 차

- 채널
  - 8비트 데이터 342
  - 구성 313, 405
  - 구조 192
  - 기본값, 설정 332
  - 대상 호스트 선택 350
  - 대체 350
  - 마스터 프로그램 190
  - 메일 대기열 192
  - 문자 세트 레이블링 341
  - 미리 정의 405
  - 방향 357
  - 설명 186, 189
  - 슬레이브 프로그램 190
  - 역방향 DNS 조회 347
  - 연결 캐싱 346
  - 이름 서버 조회 349
  - 이름 해석 305
  - 작업 처리 풀 360
  - 정의 192
  - 정의의 주석 행 192
  - 제출 전용 398
  - 채널 특정 규칙 검사 305
  - 키워드 335
  - 프로토콜 선택 및 행 종결 기호 337
  - 프로토콜 스트리밍 343
  - IDENT 조회 347
  - SASL 지원 352
  - SMTP 옵션 파일 244
  - SMTP 인증 352
  - TCP/IP 포트 선택 346
  - TCP/IP MX 레코드 지원 349
  - TLS 키워드 354
- 채널 단위 크기 제한 386
- 채널 블록 193
- 채널 처리
  - 동시 요청 248
- 채널 테이블에 중복된 호스트가 있습니다.
  - MTA 오류 메시지 795
- 채널 프로그램

- 문제 해결 775
- 채널 프로그램 수동 실행 방법 775
- 채널 프로토콜 선택 337
- 채널 호스트 테이블 228
- 채널 1 228
- 채널/호스트 테이블 193
- 채널에 대한 공식 호스트 이름이 없습니다.
  - MTA 오류 메시지 796
- 첨부 파일 384
  - 열기 421
- 초기 런타임 구성 51
  - 자동 57
- 최대 길이 헤더 383
- 충돌
  - 포트 번호 70

## 카

- 컴파일된 구성 버전이 일치하지 않습니다. 797
- 코어 파일
  - 메시지 저장소 문제 해결 629
- 콘솔 106
- 클러스터 에이전트 86
- 키워드
  - 표 314, 317

## 타

- 태그된 다시 쓰기 규칙 집합 287
- 특수 지시문 423
- 특정 733
- 특정 도메인 또는 IP 주소에서 인바운드 처리 중
  - 지 776

## 파

- 파이프 채널 398, 407
- 파일
  - 구성 파일에 포함 228
  - 헤더 옵션 380
- 파일 레이아웃 68
- 파일 열기 또는 오류 만들기 798
- 파일의 소유권
  - 문제 해결 771
- 포스트마스터
  - 주소 275
- 포트 번호 70
- 표준 절차
  - MTA 문제 해결 770
- 프로그램
  - master 248
  - slave 249
- 프로그램 전달
  - 설정 407
  - 지정 852
  - 파이프 채널 407
- 프로그램, 메일 보내기 410
- 프로세스
  - 수 129
- 프로세스당 스레드 130
- 프로토콜 스트리밍 343
- 필터 511, 541
  - 사용자 수준 디버깅 545
  - 사용자별 541, 542
  - 시브(Sieve) 217
  - 채널 수준 541
  - IP 주소 525
  - Messenger Express 67
  - MTA 차원 541, 544
  - Sieve 확장 480
- 필터,
  - 메일 필터링 참조

## 하

하드웨어 공간

메시지 저장소 문제 해결 626

하위 주소 376

할당량

경고 575

경고 메일 576

구성 570

기본 574

기본값 571

도메인 571, 575, 578

디스크 571

디스크 공간 570

메시지 571

비활성화 578

사용 603

사용자 575

알림 571, 575, 577

유예 기간 579

임계값, 설정 577

적용 571, 577

적용 사용 578

제품군 그룹 578

attributes 572

configutil 매개 변수 573

Netscape Messaging Server 580

user 571

할당량 검사 보고서 823

해당 주소가 없습니다.

MTA 오류 메시지 796

해당 채널 특성 350

행 길이 제한 387

행 길이 줄이기 387

허가된 서비스 855

헤더

긴 행 분할 382

잘못된 빈 수신자 스트라이핑 372

제거 379

처리 키워드 378

최대 길이 383

language 384

Return-path 373

X-Envelope-to 381

헤더 맞춤 382

헤더 옵션 파일 380

헤더 인코딩 381

헤더 자르기 380

헤더, 정의 411

현지화, 알림 메일

호스트 위치 특정 다시 쓰기 307

호스트 이름

숨기기 850, 859

추출 291

호스트/도메인 지정 291

호스트된 도메인

Messenger Express Multiplexor 173

환경 설정

SLAVE\_COMMAND 254

휴가 메일 503

휴가 모드 855

힙 크기 752

## A

A!B%C 368

A!^ C 368

A@B@C 369

A\!(B%C) 368

Access Manager 141

ACCESS\_ORCPT 517, 519

ACL 561

addheader 466

addrreturnpath 373

addrspfile 393

Administration Server

워크시트 950

after 채널 키워드 356

alarm.diskavail 827

alarm.diskavail.msgalarmdescription 805

alarm.diskavail.msgalarmstatinterval 805, 827

alarm.diskavail.msgalarmthreshold 805, 827  
 alarm.diskavail.msgalarmthresholddirection 827  
 alarm.diskavail.msgalarmwarninginterval 805, 827  
 alarm.msgalarmnoticehost 827  
 alarm.msgalarmnoticeport 827  
 alarm.msgalarmnoticercpt 806, 827  
 alarm.msgalarmnoticesender 827  
 alarm.serverresponse 827  
 alarm.serverresponse.msgalarmstatinterval 827  
 alarm.serverresponse.msgalarmthreshold 827  
 alarm.serverresponse.msgalarmthresholddirection 827  
 alarm.serverresponse.msgalarmwarninginterval 827  
 ALIAS\_DOMAINS 376  
 ALIAS\_ENTRY\_CACHE\_SIZE 221  
 ALIAS\_ENTRY\_CACHE\_TIMEOUT 221  
 ALIAS\_MAGIC 202, 224  
 ALIAS\_URL0 202, 224  
 ALIAS\_URL1 202, 224  
 ALIAS\_URL2 202, 224  
 aliasdetourhost 399  
 aliasedObjectName 200  
 aliases  
   별칭 데이터베이스 255  
   별칭 파일 244, 255  
   별칭 파일에 다른 파일 포함 256  
 aliaslocal 376  
 aliaspostmaster 275  
 ALLOW\_RECIPIENTS\_PER\_TRANSACTION 334  
 ALLOW\_REJECTIONS\_BEFORE\_DEFERRAL 403  
 ALLOW\_TRANSACTIONS\_PER\_SESSION 334  
 allowetrn 338  
 allowetrn 채널 키워드 339  
 allowswitchchannel 채널 키워드 350  
 alternateblocklimit 389  
 alternatechannel 389  
 alternatelinelimit 389  
 alternaterecipientlimit 389  
 alwaysencrypt 695  
 alwaysssign 695  
 AMSDK 143  
 APOP 646

appid 152  
 ASCII가 아닌 문자 793  
 associatedDomain 200  
 authrewrite 352  
 auto\_ef 425

## B

backoff 358  
 backoff 채널 키워드 356  
 bangoverpercent 367  
 bangoverpercent 키워드 292  
 bangstyle 367  
 bidirectional 357  
 BLOCK\_SIZE 386, 388  
 blocketrn 338  
 blocketrn 채널 키워드 339  
 blocklimit 388  
 blSWClientDesintationForeign 459  
 blSWClientDestinationDefault 458  
 blSWClientDestinationLocal 459  
 blswcServerAddress 459  
 blSWLocalDomain 458  
 blSWPrecedence 458  
 blSWUseClientOptin 459  
 Brightmail  
   구성 파일 옵션 458  
   구조 455  
   배포 457  
   요구 사항 및 성능 457  
   MTA 채널 키워드 449

## C

CA 인증서  
   관리 654  
   설치 653  
 cacheeverything 채널 키워드 346

## C

- cachefailures 채널 키워드 346
- cachessuccesses 채널 키워드 346
- cert8.db 159, 167
- certmap.conf 659
- certurl 695
- certutil 660
- ch\_facility 초기화 오류
  - 공간이 없습니다. 796
  - 컴파일된 문자 세트 버전이 일치하지 않습니다 . 796
- charset7 채널 키워드 341
- charset8 채널 키워드 341
- CHARSET-CONVERSION 385
- charsetesc 채널 키워드 341
- checkehlo 337
- checkehlo 채널 키워드 338
- checkoverssl 696
- cmsutil 661
- comm\_dssetup.pl 41
  - 대화식 모드 43
  - 요구 사항 42
  - 워크시트 43, 952
  - 자동 모드 49
- commadmin domain delete 106
- commadmin domain purge 105, 106
- commadmin user delete 105
- COMMENT\_STRINGS 매핑 테이블 374
- commentinc 374
- commentomit 374
- commentstrip 374
- commenttotal 374
- Communications Express
  - 문제 해결 637
- Communications Express Mail 681
- Communications Services
  - 설명서 35
- config 파일 69, 582, 593
- configutil
  - alarm.diskavail 827
  - alarm.msgalarmnoticehost 827
  - alarm.msgalarmnoticeport 827
  - alarm.msgalarmnoticercpt 827
  - alarm.msgalarmnoticesender 827
  - alarm.serverresponse 827
  - encryption.nsssl3ciphers 658
  - encryption.rsa 658
  - gen.newuserforms 115
  - gen.sitelanguage 118
  - local.service.http.proxy 176
  - local.service.pab 121
  - local.sso 152
  - local.store.notifyplugin 846
  - local.ugldapbasedn 121
  - local.ugldapbindcred 175
  - local.ugldapbinddn 121, 175
  - local.ugldaphost 121, 175
  - local.ugldapport 121
  - local.ugldapuselocal 121
  - local.webmail.sso 153
  - logfile.service 761
  - nserversecurity 658
  - sasl.default 647
  - sasl.default.ldap 646
  - service.dccroot 176
  - service.defaultdomai 176
  - service.http 139
  - service.http.plaintextmncipher 135
  - service.imap 135
  - service.imap.banner 126
  - service.loginseparator 126, 176
  - service.pop 133
  - service.pop.banner 126
  - service.service 673
  - store.admins 558
  - store.defaultmailboxquota 574
  - store.partition 595
  - store.quotaenforcement 578
  - store.quotaexceedmsginterval 577
  - store.quotagraceperiod 580
  - store.quotanotification 575
  - store.quotawarn 577
- conn\_throttle.so 525
- connectalias 370
- connectcanonical 370
- copysendpost 273
- copywarnpost 273
- counterutil 816, 824



경보 통계 817  
 출력 816  
 db\_lock 814  
 diskusage 818  
 POP, IMAP, HTTP 818  
 counterutil -l 816  
 CRAM-MD5 646  
 crdb 241, 538  
 crlaccessfail 696  
 crldir 696  
 crlenable 696  
 crlmappingurl 697  
 crlurllogindn 697  
 crlurlloginpw 697  
 crlusepastnextupdate 697  
 crontab 113

## D

daemon 채널 키워드 350  
 datefour 381  
 datetwo 381  
 dayofweek 381  
 dcroot  
   Messenger Express Multiplexor 176  
 debug 471, 478  
 defaultmx 채널 키워드 349  
 defaultnameservers 채널 키워드 349  
 defaults 채널 332  
   구성 파일 194, 228  
 DEFER\_GROUP\_PROCESSING 217  
 deferralrejectlimit 403  
 deferred 356, 358  
 defragment 385  
 Delegated Administrator 59  
 Delegated Administrator for Messaging 105  
 deleted 586  
 DELIVERY\_OPTIONS 213, 504, 505  
 dequeue\_removeoute 378  
 destinationfilter 398, 542  
 destinationnosolicit 403  
 destinationspamfilterXoptin 314, 399, 449  
 DIAGNOSTIC\_CODE 270  
 DIGEST-MD5 646  
 Direct LDAP, 설정 224  
 Direct LDAP, MTA 참조 197  
 Directory Server 118  
   구성 디렉토리 118  
   구성 설정 119  
   사용자 디렉토리 105, 118  
   요구 사항 118  
   워크시트 948  
 Directory Server 복제본 58  
 dirsync 197  
 disableetrn 338  
 disconnectbadauthlimit 388  
 disconnectbadcommandlimit 395  
 disconnectrecipientlimit 395  
 disconnectrejectlimit 395  
 disconnecttransactionlimit 395  
 dispatcher.cnf 파일 751  
 disposition\_option.dat 270  
 dispositionchannel 397  
 DNS  
   도메인 확인 340  
   역방향 조회 347  
   IDENTprotocol 347  
   MX 레코드 349  
 DNS 문제  
   MTA 문제 해결 800  
 DNS 조회 535  
 dns\_verify 535  
 do\_the\_upgrade.sh 78  
 DOMAIN\_FAILURE 201  
 DOMAIN\_MATCH\_URL 199, 224  
 DOMAIN\_UPLEVEL 198, 203, 205  
 domainetrn 338  
 domainetrn 채널 키워드 339  
 domainUIdSeparator 203  
 domainvrfy 340  
 dropblank 372

## E

## E

EHLO 335  
ehlo 337  
EHLO 명령 337  
ehlo 채널 키워드 338  
eightbit 채널 키워드 342  
eightnegotiate 채널 키워드 342  
eightstrict 채널 키워드 342  
encryption.nsssl3ciphers 658  
encryption.rsa 658  
ENS 843  
    관리 845  
    구성 매개 변수 846  
    샘플 프로그램 844  
    시작 및 중지 845  
    활성화 844  
errsendpost 273  
errwarnpost 273  
ETRN 명령 338  
ETRN 명령 지원 338  
Event Notification Service 843  
examples 파일 69  
exclusive 585  
expandchannel 364  
expandchannel 채널 키워드 357  
expandlimit 364  
expandlimit 채널 키워드 357  
expire\_exclude\_list 582, 593  
expnallow 340  
expndefault 340  
expndisable 340  
exproute 368  
EXPROUTE\_FORWARD 옵션 369

## F

field 471, 478  
fileinto 398

filesperjob 360  
filesperjob 채널 키워드 357  
filter 398  
FILTER\_DISCARD 채널 545  
FILTER\_JETTISON 545  
folderpattern 585  
foldersize 585  
FORWARD 주소 매핑 261  
forwardcheckdelete 채널 키워드 347  
forwardchecknone 채널 키워드 347  
forwardchecktag 채널 키워드 347  
FROM\_ACCESS 매핑 테이블 513, 521

## G

gen.newuserforms 115  
gen.sitelanguage 118

## H

hashdir 602  
HASStoragePlus 92  
header\_733 367  
header\_822 367  
HEADER\_LIMIT 393  
header\_uucp 367  
headerlabelalign 382  
headerlimit 393  
headerlinelength 382  
headerread 379  
headerread 키워드 380  
headertrim 379  
HIDE\_VERIFY 340  
holdexquota 391  
holdlimit 364  
holdlimit 채널 키워드 357  
host 471, 478  
http

//www.cyrusoft.com/sieve 451  
//www.mozilla.org/projects/security/pki/nss/  
tools/certutil.html 660  
//www.spamassassin.org 461  
http 로깅, 비활성화 762  
HTTP 메일 액세스, 메일 액세스 참조  
HTTP 서비스  
  구성 136  
  로그인 요구 사항 126  
  메일 설정 137  
  보안 643  
  비밀번호 기반 로그인 138  
  비활성화 138  
  사용 가능 138  
  성능 매개 변수 128  
  세션 아이디 643  
  시작 및 중지 107  
  액세스 제어 필터 672  
  연결 설정 138  
  유휴 연결 해제 131  
  인증서 기반 로그인 128  
  클라이언트 로그아웃 131  
  클라이언트 액세스 제어 132  
  특수 웹 서버 136  
  포트 번호 124  
  프로세스 설정 138  
  프로세스 수 129  
  프로세스당 스레드 130  
  프로세스당 연결 129  
  프록시 인증 673  
  MTA 설정 137  
  SSL 포트 125

iBiffconfiguration 매개 변수 846  
ICAP 442  
  옵션 파일 478  
iddenttcpsymbolic 채널 키워드 347  
IDENT 조회 347

identd 670  
identnone 채널 키워드 348  
identnonelimited 채널 키워드 348  
identnonenumeric 채널 키워드 348  
identnonenumeric 채널 키워드 348  
identntcp 채널 키워드 347  
identntcplimited 채널 키워드 348  
identntcpnumeric 채널 키워드 347  
ignoreencoding 384  
iii\_res\* 기능  
  느린 SMTP 서버 784  
IMAP 서비스  
  공유 폴더 603  
  구성 134  
  로그인 요구 사항 126  
  배너 126, 135  
  비밀번호 기반 로그인 134, 648  
  비활성화 134  
  사용 가능 134  
  사용자 액세스 모니터링 624  
  성능 매개 변수 128  
  시작 및 중지 107  
  액세스 제어 필터 672  
  연결 설정 134  
  유휴 연결 해제 131  
  인증서 기반 로그인 128, 658  
  클라이언트 디버그 627  
  클라이언트 액세스 제어 132  
  포트 번호 124, 125  
  프로세스 설정 135  
  프로세스 수 129  
  프로세스당 스레드 130  
  프로세스당 연결 129  
  readership 유틸리티 603  
  SSL 125, 649  
  SSL 포트 125  
IMAP,  
  메일 액세스 참조  
imesrestore 617  
imexpire  
  배포 582

## J

- 작동 원리 581
- imexpire, 자동 메일 제거 참조
- immonurgent 315, 325, 358
- immonurgent 채널 키워드 356
- immonitor-access 815
- improute 368
- IMPROUTE\_FORWARD 369
- imquotacheck 553, 578, 823
- imqutoacheck 603
- ims50 204, 207
- imsbackup 유틸리티 613
- imsched 113, 581, 591
- imsconnutil 624
- imsimta 갱신 226, 243
- imsimta cache -view 788
- imsimta counters 820
- imsimta crdb 538
- imsimta process 773
- imsimta qm 771, 807
- imsimta qm 409
- imsimta qm counters 822
- imsimta qm stop 및 start 775
- imsimta reload 226
- imsimta run 775
- imsimta test -exp 546, 547, 549
- imsimta test -rewrite 546, 771, 799
  - MTA 문제 해결 771
- imsimta test -rewrite -filter 546
- imsrestore 유틸리티 613, 614
- imta.cnf 201, 226
- imta.cnf 구성 파일
  - 구조 227
- IMTA\_LANG 264
- IMTA\_MAPPING\_FILE 옵션 229
- IMTA\_QUEUE 192
- IMTA\_REVERSE\_DATABASE 257
- INBOX, 기본 메일함 601
- include 파일 69
- includefinal 272, 277
- inetCanonicalDomainName 202
- inetDomainStatus 203

- inner 379
- innertrim 379
- install 파일 70
- INTERFACE\_ADDRESS 346
- interfaceaddress 채널 키워드 346
- INTERNAL\_IP 매핑 테이블 62
- Internet Content Adaptation Protocol 441
- interpretencoding 384
- IP 주소
  - 인바운드 처리 중지 776
- IP 주소 필터링 525
- iPlanetDirectoryPro 143
- IPv4 일치 234

## J

- jettison 545
- Job Controller
  - 개념 194
  - 구성 파일 247
  - 다시 시작 196
  - 명령 248
  - 사용 예 248
  - 시작 195
  - 시작 및 중지 195
  - 중지 195
- JOB\_LIMIT 옵션 251
- JOB\_LIMIT 풀 옵션 194
- limits 키워드 360
- MAX\_MESSAGES 옵션 195
- maxjobs 채널 옵션 194
- SLAVE\_COMMAND 옵션 251
- JOB\_LIMIT 361
- JOB\_LIMIT Job Controller 옵션 194, 251

## L

- language 384

- 사이트 118
- lastresort 채널 키워드 349
- LDAP
  - MTA 인터페이스 197
  - LDAP 디렉토리
    - 구성 디렉토리 118
    - 구성 디렉토리의 설정 보기 120
    - 사용자 디렉토리 105, 118
    - 사용자 디렉토리에서 조회 구성 118
    - 요구 사항 118
    - 조회 사용자 정의 118
    - MTA 194
  - LDAP 매개 변수
    - Messenger Express Multiplexor 175
  - LDAP 서버 페일오버 122
  - LDAP 오류, 처리 205
  - LDAP 준비 도구 61
  - LDAP\_ADD\_HEADER 220
  - LDAP\_ADD\_TAG 220
  - LDAP\_ALIAS\_ADDRESSES 210
  - LDAP\_ATTR\_DOMAIN1\_SCHEMA2 200
  - LDAP\_ATTR\_DOMAIN2\_SCHEMA2 200
  - LDAP\_ATTR\_MAXIMUM\_MESSAGE\_SIZE 219
  - LDAP\_AUTH\_DOMAIN 218
  - LDAP\_AUTH\_PASSWORD 219
  - LDAP\_AUTH\_POLICY 218
  - LDAP\_AUTH\_URL 219
  - LDAP\_AUTOREPLY\_TEXT 509
  - LDAP\_CANT\_DOMAIN 219
  - LDAP\_CANT\_URL 219
  - LDAP\_CONVERSION\_TAG 212, 419
  - LDAP\_DELIVERY\_FILE 212
  - LDAP\_DELIVERY\_OPTION 213
  - LDAP\_DISK\_QUOTA 212
  - LDAP\_DOMAIN\_ATTR\_ALIAS 200
  - LDAP\_DOMAIN\_ATTR\_AUTOREPLY\_TIMEOUT 204
  - LDAP\_DOMAIN\_ATTR\_BASEDN 199
  - LDAP\_DOMAIN\_ATTR\_BLOCKLIMIT 203, 211
  - LDAP\_DOMAIN\_ATTR\_CANONICAL 202
  - LDAP\_DOMAIN\_ATTR\_CATCHALL\_ADDRESS 203, 205
  - LDAP\_DOMAIN\_ATTR\_CONVERSION\_TAG 203, 419
  - LDAP\_DOMAIN\_ATTR\_DISK\_QUOTA 203
  - LDAP\_DOMAIN\_ATTR\_FILTER 203
  - LDAP\_DOMAIN\_ATTR\_MAIL\_STATUS 203
  - LDAP\_DOMAIN\_ATTR\_MESSAGE\_QUOTA 204
  - LDAP\_DOMAIN\_ATTR\_OPTIN 204
  - LDAP\_domain\_attr\_optinX 453
  - LDAP\_DOMAIN\_ATTR\_RECIPIENTCUTOFF 204, 393
  - LDAP\_DOMAIN\_ATTR\_RECIPIENTLIMIT 204, 393
  - LDAP\_DOMAIN\_ATTR\_REPORT\_ADDRESS 203
  - LDAP\_DOMAIN\_ATTR\_ROUTING\_HOSTS 198
  - LDAP\_DOMAIN\_ATTR\_SMARTHOST 203, 205
  - LDAP\_DOMAIN\_ATTR\_SOURCE\_CONVERSION\_TAG 419
  - LDAP\_DOMAIN\_ATTR\_SOURCEBLOCKLIMIT 204, 389
  - LDAP\_DOMAIN\_ATTR\_STATUS 203
  - LDAP\_DOMAIN\_ATTR\_UID\_SEPARATOR 203
  - LDAP\_DOMAIN\_FILTER\_SCHEMA1 199
  - LDAP\_DOMAIN\_ROOT 199
  - LDAP\_END\_DATE 216
  - LDAP\_ERRORS\_TO 220
  - LDAP\_EXPANDABLE 220
  - LDAP\_GROUP\_DN 220
  - LDAP\_GROUP\_OBJECT\_CLASSES 207
  - LDAP\_GROUP\_RFC822 220
  - LDAP\_GROUP\_URL1 220
  - LDAP\_GROUP\_URL2 220
  - LDAP\_HOST\_ALIAS\_LIST 198
  - LDAP\_LOCAL\_HOST 198
  - LDAP\_MAIL\_REVERSES 221
  - LDAP\_MESSAGE\_QUOTA 212
  - LDAP\_MODERATOR\_URL 219
  - LDAP\_OPTIN 217, 445
  - LDAP\_optinX 453
  - LDAP\_PERSONAL\_NAME 508
  - LDAP\_PREFIX\_TEXT 220
  - LDAP\_PRESENCE 217
  - LDAP\_PROGRAM\_INFO 212

## L

- LDAP\_RECIPIENTCUTOFF 393
- LDAP\_RECIPIENTLIMIT 393
- LDAP\_REJECT\_ACTION 218
- LDAP\_REJECT\_TEXT 218
- LDAP\_REMOVE\_HEADER 220
- LDAP\_REPROCESS 217
- LDAP\_SCHEMATAG 204
- LDAP\_SOURCE\_CONVERSION\_TAG 419
- LDAP\_SOURCEBLOCKLIMIT 389
- LDAP\_SPARE\_1 212
- LDAP\_SPARE\_2 212
- LDAP\_START\_DATE 216
- LDAP\_SUFFIX\_TEXT 220
- LDAP\_USE\_ASYNC 223
- LDAP\_USER\_OBJECT\_CLASSES 207
- LDAP\_USER\_ROOT 199
- Legato 618
- lib 파일 69
- libspamass.so 460
- linelength 387
- linelimit 388
- Linux, 기본 디렉토리 34
- LMTP 483
  - 구성 488
  - 릴레이 구성 488
  - 백엔드 저장소, MTA 없음 494, 496
  - 전달 기능 484
  - 프로토콜 498
- Local Mail Transfer Protocol, LMTP [참조](#)
- local.auto.restart 111, 825
- local.autorestart.timeout 113, 825
- local.enablelastaccess 624
- local.ens.enable 110
- local.hostname 198
- local.http.enableuserlist 624
- local.imap.enableuserlist 624
- local.imta.enable 110
- local.imta.hostnamealiases 198
- local.imta.mailaliases 204
- local.imta.schematag 204
- local.ldaphost 122
- local.mmp.enable 110
- local.probe.service.timeout 825
- local.probe.service.warningthreshold 825
- local.probe.warningthreshold 825
- local.queuedir 826
- local.sched.enable 110
- local.schedule.expire 592
- local.schedule.msprobe 113, 825, 826
- local.schedule.purge 592
- local.schedule.taskname 113
- local.service.http.proxy 176
- local.service.http.proxy.port.hostname 179
- local.service.pab 121
- local.smsgateway.enable 110
- local.snmp.enable 110
- local.sso 152
- local.store.checkdiskusage 806
- local.store.expire.loglevel 592, 593
- local.store.notifyplugin 846
- local.store.overquotastatus 573, 578
- local.store.quotaoverdraft 573, 578, 580
- local.store.relinker.enabled 609
- local.store.relinker.maxage 609
- local.store.relinker.minsize 609
- local.store.relinker.purgecycle 610
- local.store.sharedfolders 566
- local.store.snapshotinterval 632
- local.store.snapshotpath 632
- local.ugldapbasedn 121
- local.ugldapbasedn configutil 199
- local.ugldapbindcred 175
- local.ugldapbinddn 121, 175
- local.ugldaphost 121, 122, 175
- local.ugldapport 121
- local.ugldapuselocal 121, 122
- local.watcher.enable 111, 112, 825
- local.webmail.cert.enable 701
- local.webmail.cert.port 701
- local.webmail.smime.enable 701
- local.webmail.sso 153
- local.webmail.sso.amcookieiname 143, 180
- local.webmail.sso.amloglevel 143

local.webmail.sso.amnamingurl 143, 180  
 local.webmail.sso.id 153  
 local.webmail.sso.prefix 153  
 local.webmail.sso.singlesignoff 143  
 localvrfy 채널 키워드 340  
 LOG\_CONNECTION 732  
 LOG\_CONNECTION 옵션 735  
 LOG\_FILENAME 732  
 LOG\_FILENAME 옵션 734  
 LOG\_MESSAGE\_ID 732  
 log\_message\_id 777  
 LOG\_MESSAGE\_ID 옵션 734  
 LOG\_MESSAGES\_SYSLOG 옵션 734  
 LOG\_NOTARY 732  
 LOG\_PROCESS 732  
 LOG\_PROCESS 옵션 735  
 LOG\_TRANSPORTINFO 334  
 LOG\_USERNAME 옵션 735  
 logfile.service 761  
 logfile.service.loglevel 762  
 logheader 395  
 logindn 698  
 loginpw 698  
 loopcheck 396

## M

mail.log\_current 778  
 MAIL\_ACCESS 매핑 테이블 513, 519  
 mailAllowedServiceAccess 712  
 mailAlternateAddress 204  
 mailAutoReplyMode 508  
 mailAutoReplyText 509  
 mailAutoReplyTextInternal 509  
 mailAutoReplyTimeOut 509  
 mailConversionTag 212  
 mailDeferProcessing 217  
 mailDeliveryOption 213, 504  
 mailDomainCatchallAddress 203  
 MailDomainConversionTag 419  
 mailDomainConversionTag 203  
 mailDomainDiskQuota 572  
 mailDomainMsgMaxBlocks 203  
 mailDomainMsgQuota 572  
 mailDomainReportAddress 203  
 mailDomainSieveRuleSource 203  
 mailDomainStatus 203, 572  
 maildomainstatus 579  
 mailEquivalentAddress 204  
 mailfromdnsverify 채널 키워드 340  
 mailMessageStore 597  
 mailMsgMaxBlocks 211  
 mailMsgQuota 572  
 mailQuota 212, 572  
 mailRejectText 218  
 mailRoutingAddress 210  
 mailRoutingHosts 198  
 mailRoutingSmartHost 203  
 MailSieveRuleSource 546  
 mailSieveRuleSource 217  
 mailUserStatus 572  
 mailuserstatus 579  
 make\_backup\_config\_changes.sh 80  
 make\_configutil\_changes.sh 79  
 make\_mboxlistdb\_changes.sh 80  
 make\_mta\_config\_changes.sh 79  
 master 357  
 master\_command 251  
 master\_debug 396, 778  
 MAX\_CLIENT\_THREADS 334  
 max\_client\_threads 361  
 MAX\_CONNS 495  
 MAX\_CONNS 디스패처 옵션 188  
 MAX\_HEADER\_BLOCK\_USE 386  
 MAX\_HEADER\_LINE\_USE 386  
 MAX\_LIFE\_CONNS 495  
 MAX\_LIFE\_TIME 495  
 MAX\_MESSAGES Job Controller 옵션 195  
 MAX\_PROCS 495  
 MAX\_PROCS 디스패처 옵션

- 디스패처
  - MAX\_PROCS 옵션 187
- MAX\_PROCS\*MAX\_CONNS 784
- maxblocks 386
- maxheaderaddrs 382
- maxheaderchars 382
- maxjobs 360
- maxjobs 채널 키워드 194, 357
- maxlines 386
- maxprocchars 383
- maysaslserver 351
- maytls 658
- maytls 채널 키워드 354
- maytlsclient 채널 키워드 354
- maytlsserver 채널 키워드 354
- mboxutil 598
- MD5 607
- MDN 277
- MDN(Message Disposition Notification) 277, 503
- MEM. Messenger Express Multiplexor 참조 172
- memberURL 220
- Message Disposition Notification, 사용자 정의/현지화 278
- message disposition notification, 알림 참조
- Message Transfer Agent MTA 참조
- messagecount 585
- messagedays 585
- messagesize 585
- messagesizedays 586
- Messaging Multiplexor
  - 가상 도메인 161
  - 구성 164, 171
  - 기능 157
  - 미리 구성 163
  - 사전 인증 160
  - 설명 157
  - 설정 163
  - 시작/중지/갱신 166
  - 암호화 159
  - 인증서 기반 인증 160
  - 작동 방식 158
  - 저장소 관리자 160
  - 토폴로지 예 168
  - certmap 플러그인 160
  - DNComps 160
  - FilterComps 160
  - IMAP 예 169
  - POP 예 171
  - SSL, 함께 사용 166
  - vdmap 161
- Messaging Multiplexor, MMP 참조
- Messaging Server
  - 설명서 34
  - 워크시트 52, 954
- Messaging Server 및 Directory Server 복제본 설치 58
- Messaging Server에 대해 LDAP 디렉토리 준비 41
- Messenger Express 53, 123
  - 문제 해결 637
  - 사용자 액세스 모니터링 624
  - 알 수 없거나 잘못된 분할 영역 638
  - debug 627
- Messenger Express 메일 필터 67
- Messenger Express 클라이언트 액세스
  - Messenger Express Multiplexor 177
- Messenger Express Multiplexor
  - 개요 172
  - 관리 178
  - 구성 174
  - 기본 도메인 176
  - 단일 사인온 179
  - 로그인 구분자 176
  - 사용 가능 176
  - 설정 174
  - 여러 프록시 서버 설정 178
  - 연결 설정의 단계 174
  - 오류 메시지 177
  - 작동 방식 173
  - 제품 버전 관리 178
  - 테스트 177
  - 호스트된 도메인 173
  - 활성화 176



- dcroot 176
- LDAP 매개 변수 175
- Messenger Express 클라이언트 액세스 177
- MMP와의 유사성 172
- SSL 172, 178
- Messenger Express Multiplexor 참조 173
- Messenger Express Multiplexor 활성화 176
- Messenger Express Multiplexor와 연결 설정 174
- Messenger Express Multiplexor의 개요 172
- mgmanMemberVisibility 220
- mgrpAddHeader 220
- mgrpAllowedBroadcaster 219
- mgrpAllowedDomain 218
- mgrpAuthPassword 219
- mgrpBroadcasterPolicy 218
- mgrpDeliverTo 220
- mgrpDisallowedBroadcaster 219
- mgrpDisallowedDomain 219
- mgrpErrorsTo 220
- mgrpModerator 218, 219
- mgrpMsgMaxSize 219
- mgrpMsgPrefixText 220
- mgrpMsgRejectAction 218
- mgrpMsgSuffixText 220
- mgrpRemoveHeader 220
- mgrpRFC822MailMember 220
- Microsoft Exchange 353
- MIME
  - 개요 411
  - 메일 구성 411
  - 처리 384
  - 헤더 411
- MIN\_CONNS 디스패처 옵션 188
- MIN\_PROCS 디스패처 옵션 187
- MISSING\_RECIPIENT\_POLICY 372
- missingrecipientpolicy 371
- mm\_debug 778
  - 디버깅 도구
    - mm\_debug 775
- mm\_init 794
- mm\_init 오류 794
- MMP 54, 675
  - 기존 인스턴스 수정 166
  - AService.cfg 파일 165
  - AService-def.cfg 165
  - ImapMMP.config 165
  - ImapProxyAService.cfg 파일 165
  - ImapProxyAService-def.cfg 165
  - LDAP 서버 페일오버 172
  - PopProxyAService.cfg 파일 165
  - PopProxyAService-def.cfg 165
  - SMTP 프록시 162
  - SmtproxyAService.cfg 165
  - SmtproxyAService-def.cfg 165
- MMP 및 Messenger Express Multiplexor의 유사성 172
- MMP. Messaging Multiplexor 참조
- MobileWay 912
- mode 472, 479
- modutil 661
- msexchange 353
- msg\_svr\_base 68, 555
- msprobe 110, 824
- MTA 53, 793
  - 개념 181
  - 구성 파일 226, 243
  - 구조 185
  - 다시 쓰기 규칙 189, 198
  - 데이터 흐름 197
  - 디렉토리 정보 194
  - 디스패처 187
  - 로깅 723, 728
  - 릴레이 차단 531
  - 릴레이 추가 528
  - 메일 대기열 192
  - 메일 흐름 185
  - 명령줄 유틸리티 256
  - 문제 및 솔루션 781
  - 문제 해결 770
  - 별칭 확장 202
  - 서버 프로세스 187
  - 오류 메시지 793
  - 오류 처리 200
  - 작동 원리 197

- 전역 옵션 설정 246
- 채널 186, 189
- imta.cnf 다시 쓰기 규칙 201
- LDAP 인터페이스 197
- MTA 관련 문제 해결
  - .HELD 메일 790
  - 개별 채널 중지 및 시작 방법 775, 778
  - 개요 770
  - 구성 확인 771
  - 로그 파일 774
  - 메일 경로에서 채널 확인 777
  - 메일 대기열 디렉토리 확인 771
  - 메일 정지 지점 확인 780
  - 예 777
  - 일반 문제
    - 구성 파일 변경 782
    - 루핑 메일 789
    - 메일이 대기열에서 제외되지 않음 785
    - 메일이 전달되지 않음 787
    - 받은 메일 인코딩 791
    - 서버측 규칙 792
    - MTA에서 받는 메일을 수신하지 않음 783
    - SMTP 연결의 시간 초과 784
- 일반 오류 메시지 793
  - 버전이 일치하지 않습니다. 797
  - 스왑 공간 798
  - 잘못된 호스트/도메인 오류 799
  - 파일 열기 또는 오류 만들기 798
  - mm\_init 794
  - os\_smtp\_\* 오류 800
- 채널 프로그램 수동 실행 방법 775
- 특정 도메인 또는 IP 주소에서 인바운드 처리 중지 방법 776
- 파일의 소유권 771
- 표준 절차 770
- imsimta qm start 775
- imsimta qm stop 775
- imsimta test-rewrite 771
- Job Controller 및 디스패처 772
- MTA 구성
  - 문제 해결 771
- MTA 구성 컴파일 226
- MTA 구성 파일 226
- MTA 기능
  - MTA 대기열 807
  - MTA 매핑 파일 229-??
  - MTA 문제 해결
    - 네트워크 및 DNS 문제 800
  - MTA 문제 해결 예 777
  - MTA 예
    - 메일 정지 780
    - 채널 시작 및 중지 778
  - MTA 오류 메시지 793
    - 공식 호스트 이름이 너무 길니다. 797
    - 로컬 호스트가 너무 길니다. 796
    - 매핑 이름이 너무 길니다. 795
    - 매핑 이름이 중복되었습니다. 795
    - 별칭 포함 파일을 열 수 없습니다. 794
    - 별칭이 중복되었습니다. 795
    - 잘못된 별칭입니다. 794
    - 채널 테이블에 중복된 호스트가 있습니다. 795
    - 채널에 대한 공식 호스트 이름이 없습니다. 796
    - 해당 주소가 없습니다. 796
  - ch\_facility 초기화 오류
    - 공간이 없습니다. 796
    - 컴파일된 문자 세트 버전이 일치하지 않습니다 . 796
- MTA 채널
  - 시작 및 중지 775
- multiple 393
- mustsaslsrver 351
- musttls 658
- musttls 채널 키워드 354
- musttlsclient 채널 키워드 354
- musttlsserver 채널 키워드 354
- MX 레코드 조회 799
- MX 레코드 지원 349
- mx 채널 키워드 349
- myprocmail, Pipe 채널 사용 407

## N

nameparameterlengthlimit 392

- nameservers 채널 키워드 349
  - NDAAuth-applicationID 152
  - netstat 809
  - nms41 204, 207
  - noaddrreturnpath 373
  - nobangoverpercent 367
  - nobangoverpercent 키워드 292
  - noblocklimit 388
  - nocache 채널 키워드 346
  - nodayofweek 381
  - nodeferred 356, 358
  - nodefragment 385
  - nodestinationfilter 398
  - nodropblank 372
  - noehlo 337
  - noehlo 채널 키워드 338
  - noexproute 368
  - noexquota 391
  - nofileinto 398
  - nofilter 398
  - noheaderread 379
  - noheadertrim 379
  - noimproute 368
  - noinner 379
  - noinnertrim 379
  - nolinelimit 388
  - nologging 395
  - noloopcheck 396
  - nomailfromdnsverify 채널 키워드 340
  - nomaster\_debug 396
  - nomsexchange 353
  - nomx 채널 키워드 349
  - nonrandommx 채널 키워드 349
  - nonurgentbackoff 채널 키워드 356, 358
  - nonurgentblocklimit 363
  - nonurgentblocklimit 채널 키워드 356
  - nonurgentnotices 272
  - nonurgentnotices 채널 키워드 357
  - noreceivedfor 374
  - noreceivedfrom 374
  - noremotehost 370
  - noreturnpersonal 275
  - noreverse 259, 372
  - normalbackoff 358
  - normalbackoff 채널 키워드 356
  - normalblocklimit 363
  - normalblocklimit 채널 키워드 356
  - normalnotices 272
  - normalnotices 채널 키워드 357
  - norules 377
  - norules 채널 키워드 305
  - nosasl 351
  - nosaslserver 351
  - nosaslswitchchannel 351
  - nosendetrn 338, 339
  - nosendpost 273
  - noservice 365
  - noslave\_debug 396
  - nosmtp 채널 키워드 337
  - nosourcefilter 398
  - noswitchchannel 키워드 350
  - notary
    - 알림 메일 참조
  - notices 272, 358
  - notices 채널 키워드 357
  - NOTIFICATION\_LANGUAGE 매핑 테이블 265, 267
  - notificationchannel 397
  - notls 채널 키워드 354
  - notlsclient 채널 키워드 354
  - notlsserver 채널 키워드 354
  - novrfy 338
  - nowarnpost 273
  - nox\_env\_to 381
  - nsserversecurity 658
  - nsswitch.conf 파일 349
- O**
- optin\_user\_carryover 454
  - OR\_CLAUSES 218

## P

ORCPT 517  
ORIG\_MAIL\_ACCESS 매핑 테이블 513, 519  
ORIG\_SEND\_ACCESS 매핑 테이블 513, 517  
ORIGINAL\_ADDRESS 270  
os\_smtp\_\* 오류 800  
os\_smtp\_open 오류 800  
os\_smtp\_read 오류 800  
os\_smtp\_write 오류 800

## P

parameterlengthlimit 392  
PDU 877  
percentonly 367  
percents 367  
personalinc 375  
personalomit 375  
personalstrip 375  
pk12util 661  
PKCS #11  
    내부 및 외부 모듈 651  
platformwin 698  
pool 248, 360  
pool 채널 키워드 356  
POP 서비스  
    구성 132  
    로그인 요구 사항 126  
    배너 126  
    비밀번호 기반 로그인 648  
    사용자 액세스 모니터링 624  
    성능 매개 변수 128  
    시작 및 중지 107  
    액세스 제어 필터 672  
    휴식 연결 해제 131  
    인증서 기반 로그인 658  
    클라이언트 디버그 627  
    클라이언트 액세스 제어 132  
    포트 번호 124  
    프로세스 수 129  
    프로세스당 스레드 130

    프로세스당 연결 129  
    SSL 649  
POP before SMTP 675  
POP,  
    메일 액세스 참조  
PORT 346  
port 472, 479  
port 채널 키워드 346  
PORT\_ACCESS 495, 523  
PORT\_ACCESS 매핑 테이블 513, 523, 525  
postheadbody 274  
postheadbody 채널 키워드 276  
postheadonly 274  
postheadonly 채널 키워드 276  
preferredLanguage 117

## Q

Q 레코드 808

## R

RAID 기술  
    메시지 저장소용 594  
randommx 채널 키워드 349  
RBL 검사 535  
readership 565, 603  
readsigncert 698  
Received: 헤더에 주소 374  
Received: 헤더에 To 주소 374  
receivedfor 374  
receivedfrom 374  
RECIPIENT\_ADDRESS 271  
recipientcutoff 392  
recipientlimit 392  
reconstruct 633, 634  
    성능 636  
rejectsmtpplonglines 392

relinker 606, 607  
   명령줄 모드 607  
   실시간 모드 609  
   작동 원리 606  
 reload 226  
 remotehost 370  
 resource.properties 152  
 restricted 373  
 restricted 채널 키워드 373  
 return\_option 270  
 return\_option.dat 270  
 RETURN\_PERSONAL 271  
 returnaddress 275  
 returnenvelope 274, 277  
 returnpersonal 275  
 reverse 372  
 REVERSE 매핑 테이블 257  
 REVERSE 매핑 테이블 플래그 258  
 REVERSE\_ADDRESS\_CACHE\_SIZE 222  
 REVERSE\_ENVELOPE 259  
 REVERSE\_URL 221, 224  
 revocationunknown 698  
 RFC 2476 398  
 RFC 3507 441  
 rfc822MailMember 220  
 ROUTE\_TO\_ROUTING\_HOST 198  
 routelocal 369  
 rules 377  
 rules 채널 키워드 305

## S

S/MIME 681  
   개념 전체 조건 682  
   개인 및 공개 키 684  
   기본 구성 688  
   사용자 권한 686  
   스마트 카드 685  
   시작 686  
   애플릿 687  
   애플릿 다운로드 688  
   여러 언어 지원 686  
   옵션 701  
   일반 액세스 카드 684  
   정의 682  
   키 쌍 685  
   필수 소프트웨어/하드웨어 683  
   LDAP 디렉토리 693  
   LDAP 디렉토리의 공개 키 685  
   LDAP 비밀번호 쌍 693  
   LDAP 자격 증명 694  
   smime.conf 파일 694  
   SSL 702  
 SASL  
   설명 644  
   채널 키워드 352  
 sasl.default.auto\_transition 645, 647  
 sasl.default.ldap 646  
 sasl.default.ldap.has\_plain\_passwords 645  
 sasl.default.ldap.searchfilter 645  
 sasl.default.ldap.searchfordomain 645  
 sasl.default.mech\_list 645, 647  
 sasl.default.transition\_criteria 645  
 saswitchchannel 350, 351  
 SASVE  
   구성 예 475  
   배포 475  
 SAVSE  
   개요 474  
   배포 474, 475  
   옵션 478  
   요구 사항 및 사용 시 고려 사항 474  
 sbin 파일 69  
 Secure/Multipurpose Internet Mail Extension,  
   S/MIME 참조  
 seen 586  
 SEND\_ACCESS 매핑 테이블 513, 517  
 sendcryptcert 699  
 sendcryptcertrevoked 699  
 sendetrn 338, 339  
 sendmail  
   클라이언트 65

- sendpost 273
- sendsigncert 699
- sendsigncertrevoked 699
- sensitivitycompanyconfidential 383
- sensitivitynormal 383
- sensitivitypersonal 383
- sensitivityprivate 383
- SEPARATE\_CONNECTION\_LOG 옵션 735
- service 365
- service.{imap | pop | http}.plaintextmncipher 645
- service.dccroot 176
- service.defaultdomain 176, 203
- service.http 139
- service.http.enable 110, 762
- service.http.enablesslport 139, 762
- service.http.idletimeout 139
- service.http.maxmessagesize 139
- service.http.maxsessions 139
- service.http.maxthreads 139
- service.http.numprocesses 139
- service.http.plaintextmncipher 135, 139
- service.http.port 139
- service.http.sessiontimeout 139
- service.http.smtphost 140
- service.http.smtpport 140
- service.http.spooldir 139
- service.http.sslport 139
- service.imap 135
- service.imap.allowanonymouslogin 645
- service.imap.banner 126, 136
- service.imap.enable 110
- service.imap.enablesslport 135
- service.imap.idletimeout 135
- service.imap.maxthreads 136
- service.imap.numprocesses 136
- service.imap.port 135
- service.imap.sslport 135
- service.loginseparator 126, 176
- service.pop 133
- service.pop.banner 126, 134
- service.pop.enable 110, 133
- service.pop.enablesslport 134
- service.pop.idletimeout 133
- service.pop.maxsessions 133
- service.pop.maxthreads 133
- service.pop.numprocesses 133
- service.pop.sslport 134
- service.readtimeout 825, 826
- sevenbit 채널 키워드 342
- Short Message Service, 정의 867
- Sieve 필터, 사용자 수준  
참조
- Sieve 필터링 언어 540
- silentetn 338
- silentetn 채널 키워드 339
- sims40 207
- sims401 204
- single 350, 393
- single 채널 키워드 351
- single\_sys 248, 350, 393
- single\_sys 채널 키워드 351
- slapd 810
- slapd 문제 810
- slave 357
- SLAVE\_COMMAND 옵션 254
- SLAVE\_COMMAND Job Controller 옵션 251
- slave\_debug 396, 778
- SMIME
  - 개인 및 공개 키 확인 705
  - 권한 711
  - 네트워크 보안 서비스(NSS) 717
  - 로그인, 처음 718
  - 메일 시간 709
  - 사용자의 개인/공개 키 찾기 705
  - 서명 및 암호화 설정 719
  - 오래된 CRL 708
  - 인증서 관리 712
  - 인증서 해지 711
  - Communications Express S/MIME 최종 사용자  
정보 717
  - CRL 액세스 706
  - CRL 액세스 문제 710

- CRL 확인 706
- CRL 확인 및 프록시 서버 708
- Java 콘솔 활성화 721
- LDAP에서 키/인증서 확인 715
- LDAP의 공개 키 및 인증서 714
- LDAP의 CA 인증서 712
- SMPP V3.4 876
- SMS 867
  - 구성 886
  - 디버깅 914
  - 사이트 정의 텍스트 변환 881
  - 서식 지정 템플릿 909
  - 전달 재시도 912
  - 전자 메일 변환 옵션 893
  - 전자 메일에서 SMS로 변환 872
  - 주소 유효성 검사 880
  - 채널 옵션 890
  - 채널 옵션 파일 889
  - 채널 정의 및 다시 쓰기 규칙 887
  - 채널 추가 911
  - 현지화 옵션 906
  - SMS 옵션 898
- SMS 채널 867
  - 속성 870
  - 요구 사항 869
  - 작업 870
- SMS 채널, 샘플 구성 912
- SMS 채널, 추가 886
- SMS\_Channel\_TEXT 매핑 테이블 881
- SMTP 릴레이 483
  - 추가 528
- SMTP 명령 및 프로토콜 지원 335
- SMTP 서버 속도 저하 784
- SMTP 서비스
  - 로그인 요구 사항 648
  - 릴레이 차단 531
  - 릴레이 추가 528
  - 비밀번호 기반 로그인 648
  - 시작 및 중지 107
  - 액세스 제어 511
  - 인증된 SMTP 648
  - 포트 번호 649
- SMTP 연결 784, 808
- SMTP 오류
  - os\_smtp\_\* 오류 800
- SMTP 인증 675
- SMTP 차단
  - 설치 후 구성 62
- SMTP 차단 구성 62
- SMTP 채널 333
- SMTP 채널 스레드 363
- SMTP 채널 옵션 파일 676
- smtp 채널 키워드 337
- SMTP 프록시 660, 675
  - MMP 162
- SMTP AUTH 528
- SMTP MAIL TO 명령 340
- smtp\_client 프로세스 485
- smtp\_cr 채널 키워드 337
- smtp\_crlf 채널 키워드 337
- smtp\_crorlf 채널 키워드 337
- smtp\_lf 채널 키워드 337
- SNMP 829
  - 구현 830
  - 기타 iPlanet 제품과 공존 833
  - 네트워크 연결 정보 835
  - 서버 정보 834
  - 작업 830
  - 제공된 정보 833
  - 제한 830
  - 채널 네트워크 연결 839
  - 채널 오류 840
  - 채널 정보 837
  - appTable 834
  - appTable 사용 835
  - assocTable 835
  - assocTable 사용 836
  - Messaging Server에 대해 구성 831
  - MIB 지원 830
  - MTA 정보 836
  - mtaGroupAssociationTable 839
  - mtaGroupErrorTable 840

- mtaGroupErrorTable 사용 841
- mtaGroupTable 837
- mtaGroupTable 사용 839
- mtaTable 836
- mtaTable 사용 837
- SOCKS\_HOST 479
- SOCKS\_PASSWORD 479
- SOCKS\_PORT 479
- SOCKS\_USERNAME 479
- Solaris
  - 지원 36
  - 패치 36
- sourceblocklimit 388
- sourcecommentinc 374
- sourcecommentmap 374
- sourcecommentomit 374
- sourcecommentstrip 374
- sourcecommenttota 374
- sourcefilter 398, 542
- sourceenosolicit 403
- sourcepersonalinc 375
- sourcepersonalmap 375
- sourcepersonalomit 375
- sourcepersonalstrip 375
- sourceroute 366
- sourcespamfilterXoptin 399, 449
- spamadjust 480
- SpamAssassin 460
  - 결과 460
  - 배포 462
  - 서버 찾기 462
  - 스팸 파일화 463
  - 옵션(spamassassin.opt) 471
  - 요구 사항 및 성능 461
  - 작동 원리 460
  - 접수 460
  - examples 462
  - mode 473
  - verdict 460
- spamd 460
- spamfilterX\_action\_n 454
- SpamfilterX\_config\_file 452
- spamfilterX\_final 454
- SpamfilterX\_library 452
- SpamfilterX\_null\_action 453
- SpamfilterX\_null\_optin 453
- SpamfilterX\_optional 453
- SpamfilterX\_string\_action 453
- spamfilterX\_verdict\_n 454, 465
- spamttest 480
- SSL
  - 개요 649
  - 내부 및 외부 모듈 651
  - 비밀번호 파일 654
  - 사용 가능 656
  - 서버 인증서 설치 652
  - 서버 인증서 요청 652
  - 성능 최적화 660
  - 암호문 657
  - 인증서 651
  - 인증서 관리 654
  - 하드웨어 암호화 가속기 652
  - CA 인증서 설치 653
  - Messenger Express Multiplexor 172, 178
  - POP 133
- SSL에서의 POP 133
- SSL을 통한 디렉토리 조회 679
- sslpassword.conf 파일 654
- sslrootcacertsurl 700
- ssltap 661
- SSO 141-??
  - 구성 142
  - 문제 해결 144
  - 신뢰할 수 있는 원 144, 146
  - 제한 142
  - 쿠키 145
  - Messenger Express 구성 매개 변수 142
  - Messenger Express Multiplexor 179
- SSR 792
  - 구문 문제 792
- start-msg 109, 110
- stop-msg 109
- store.admins 558
- store.cleanuppage 592



store.defaultmailboxquota 573, 574  
 store.defaultmessagequota 573  
 store.defaultpartition 597  
 store.expirerule 584  
 store.quotaenforcement 573, 578  
 store.quotaexceededmsg 573, 576  
 store.quotaexceededmsginterval 573, 577  
 store.quotagraceperiod 573  
 store.quotanotification 573, 575  
 store.quotawarn 573, 577  
 store\_root 555  
 stored 812  
 stored 작업 628  
 stored 프로세스  
   메시지 저장소 문제 해결 628  
 streaming 채널 키워드 343  
 subaddressexact 376  
 subaddressrelaxed 376  
 subaddresswild 376  
 subdirs 394  
   사용 방법 779  
 subdirs 채널 키워드 394  
 submit 채널 키워드 397, 398  
 Sun Cluster 85  
 Sun ONE 콘솔 106  
 sunManagedOrganization 200  
 SunPreferredDomain 203  
 sunPreferredDomain 200  
 suppressfinal 272, 277  
 switchchannel 371, 531  
 switchchannel 채널 키워드 350  
 Symantec Anti-Virus Scanning Engine,  
   SASVE 참조

## T

TCP 클라이언트 액세스 제어  
   가상 도메인 672  
   개요 664  
   사용자 아이디 조회 670  
   액세스 필터의 작동 방법 665  
   와일드카드 이름 668  
   와일드카드 패턴 668  
   주소 스푸핑 감지 672  
   필터 구문 666  
   호스트 지정 669  
   examples 671  
   EXCEPT 연산자 669  
   identd 서비스 670  
   Netscape Console 인터페이스 672  
 TCP/IP  
   역방향 DNS 조회 347  
   연결 343  
   인터페이스 주소 346  
   채널 244, 334  
   포트 번호 345, 346  
   IDENT 조회 347  
   MX 레코드 지원 348, 349  
 TCP/IP 이름 서버 조회 349  
 TCP/IP 채널 333  
 tcp\_lmtp 채널 487  
 tcp\_lmtpnative 채널 487  
 tcp\_smtp\_server 프로세스 485  
 TEXT\_CHARSET 271  
 threaddepth 363  
 threaddepth 채널 키워드 357  
 timestampdelta 700  
 TLS 134, 354  
   설명 649  
   채널 키워드 354  
 TLS 문제 782  
 tls 채널 키워드 658  
 tlsswitchchannel 키워드 354  
 transactionlimit 362  
 Transport Layer Security (TLS) 649  
 truncatesmtplonglines 392  
 trustedurl 700

## u

## U

UBE(Unsolicited Bulk Email), 스팸 방지 참조  
uniqueMember 220  
UNIX 시스템 사용자 및 그룹 40  
UNIX 전달. 853  
unrestricted 373  
unrestricted 채널 키워드 373  
UpgradeMsg5toMsg6.pl 74, 76  
urgentbackoff 358  
urgentbackoff 채널 키워드 356  
urgentblocklimit 363  
urgentblocklimit 채널 키워드 356  
urgentnotices 272  
urgentnotices 채널 키워드 357  
USE\_CHECK 472  
USE\_DOMAIN\_DATABASE 224  
USE\_FORWARD\_DATABASE 262, 263, 264  
USE\_REVERSE\_DATABASE 221, 224, 259, 263  
USE\_TEXT\_DATABASES 489  
use\_text\_databases 241  
useconfig 유틸리티 86  
useintermediate 277  
user  
    액세스 모니터링 624  
    제거 105  
usercertfilter 700  
uucp 367  
UUCP 주소 다시 쓰기 규칙 286

## V

VACATION\_CLEANUP 507  
VACATION\_TEMPLATE 506, 507  
vacationEndDate 508  
vacationStartDate 508  
vdmap(Messaging Multiplexor) 161  
verdict 472, 479  
VerifySSO 152  
verifyurl 152

Veritas Cluster Server 85

    구성 88

    버전 3.5 88

viaaliasoptional 378

viaaliasrequired 378

VERFY 명령 339

VERFY 명령 지원 339

verfyallow 채널 키워드 340

verfydefault 채널 키워드 340

verfyhide 채널 키워드 340

## W

warnpost 273

watcher 110, 824

wrapsmtplonglines 392

## X

x\_env\_to 381

X-Envelope-to

    헤더 행

    생성 381

X-REWRITE-SMS-ADDRESS 매핑 테이블 881