Sun Java System Web Proxy Server 4.0.8 관리 설명서

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

부품 번호: 820–6316
2008년 8월

081015@21288

목차

머리말 19

1 Sun Java System Web Proxy Server 소개 25
Sun Java System Web Proxy Server 정보 25
이 릴리스의 새로운 기능 25
시작하기 26
Administration Server 개요 26
Server Manager 개요 27
구성 파일 28
정규 표현식 29

2 Sun Java System Web Proxy Server 관리 31
Administration Server 시작 31
UNIX 또는 Linux에서 Administration Server를 시작하는 방법 31
Windows에서 Administration Server를 시작하는 방법 32
Administration Server 중지 32
UNIX 또는 Linux에서 Administration Server를 중지하는 방법 32
Windows에서 Administration Server를 중지하는 방법 33
여러 Proxy Server 실행 33
▼ 여러 서버 인스턴스를 설치하는 방법 33
서버 인스턴스 제거 33
▼ 서버 인스턴스를 제거하는 방법 34
Proxy Server 3.6에서 마이그레이션 34

3 관리 기본 설정 35
청취 소켓 만들기 및 관리 35
▼ 청취 소켓을 추가하는 방법 36

▼ 청취 소켓을 편집하는 방법 36
▼ 청취 소켓을 삭제하는 방법 36
수퍼유저 설정 변경 37
▼ Administration Server에 대한 수퍼유저 설정을 변경하는 방법 37
▼ 수퍼유저 비밀번호를 변경하는 방법 37
여러 관리자 허용 38
▼ 분산 관리를 사용 설정하는 방법 38
로그 파일 옵션 지정 39
로그 파일 확인 39
디렉토리 서비스 사용 40
서버 액세스 제한 40
SNMP 마스터 에이전트 설정 41

4 사용자 및 그룹 관리 43
사용자 및 그룹에 대한 정보 액세스 43
디렉토리 서비스 설명 44
LDAP 디렉토리 서비스 44
키 파일 디렉토리 서비스 44
다이제스트 파일 디렉토리 서비스 45
디렉토리 서비스 구성 45
▼ 디렉토리 서비스를 만드는 방법 45
▼ 디렉토리 서비스 편집 방법 46
DN(Distinguished Name) 이해 46
LDIF 사용 47
사용자 생성 47
LDAP 기반 인증 데이터베이스에 사용자 만들기 47
키 파일 인증 데이터베이스에 사용자 생성 49
▼ 키 파일 인증 데이터베이스에 사용자를 만드는 방법 50
다이제스트 파일 인증 데이터베이스에 사용자 만들기 50
▼ 다이제스트 파일 인증 데이터베이스에 사용자를 만드는 방법 50
사용자 관리 51
사용자 정보 찾기 51
사용자 정보 편집 53
사용자 비밀번호 관리 54
사용자 이름 변경 54

사용자 제거 55
그룹 생성 55
정적 그룹 정보 56
동적 그룹 정보 57
그룹 관리 60
그룹 항목 찾기 60
그룹 항목 편집 62
그룹 구성원 추가 62
그룹 구성원 목록에 그룹 추가 63
그룹 구성원 목록에서 항목 제거 63
소유자 관리 64
추가 참조 관리 64
그룹 이름 변경 65
그룹 제거 65
조직 단위 만들기 66
▼ 조직 단위를 만드는 방법 66
조직 단위 관리 66
조직 단위 찾기 66
조직 단위 속성 편집 68
조직 단위 이름 변경 69
조직 단위 제거 69

5 인증서 및 키 사용 71
Administration Server 액세스 보안 72
인증서 기반 인증 72
트러스트 데이터베이스 생성 73
▼ 트러스트 데이터베이스를 만드는 방법 73
password.conf 사용 74
SSL 사용 서버 자동 시작 74
Sun Crypto Accelerator 키 저장소 사용 75
▼ Sun Crypto Accelerator를 사용하도록 Proxy Server를 구성하려면 75
▼ Proxy Server에서 Sun Crypto Accelerator 4000 보드를 활성화하려면 75
VeriSign 인증서 요청 및 설치 76
▼ VeriSign 인증서 요청 방법 76
▼ VeriSign 인증서 설치 방법 76

기타 서버 인증서 요청 및 설치 77
필수 CA 정보 77
기타 서버 인증서 요청 78
기타 서버 인증서 설치 79
이전 버전의 인증서 마이그레이션 81
▼ 인증서 마이그레이션 방법 81
내장 루트 인증서 모듈 사용 82
인증서 관리 82
▼ 인증서 관리 방법 82
CRL 및 KRL 설치/관리 83
▼ CRL 또는 CKL 설치 방법 83
▼ CRL 및 CKL 관리 방법 84
보안 기본 설정 84
SSL 및 TLS 프로토콜 85
SSL을 사용하여 LDAP와 통신 86
Proxy Server를 통해 SSL 터널링 86
SSL 터널링 구성 87
청취 소켓용 보안 사용 설정 89
전역적 보안 구성 91
외부 암호화 모듈 사용 92
PKCS #11 모듈 설치 92
FIPS 140 표준 96
클라이언트 보안 요구 사항 설정 97
클라이언트 인증 요구 97
역방향 프록시에서의 클라이언트 인증 98
역방향 프록시에서의 클라이언트 인증 설정 99
클라이언트 인증서를 LDAP로 매핑 100
`certmap.conf` 파일 사용 102
고급 암호 설정 106
▼ 고급 암호 설정 방법 106
기타 보안 고려 사항 107
실제 액세스 제한 107
관리 액세스 제한 107
고급 비밀번호 선택 108
비밀번호 또는 PIN 변경 108
서버에서 기타 응용 프로그램 제한 109

클라이언트가 SSL 파일을 캐시하지 못하도록 방지 110
포트 제한 110
서버의 한계 파악 110

6 서버 클러스터 관리 111
서버 클러스터 정보 111
클러스터 사용에 대한 지침 112
클러스터 설정 112
클러스터에 서버 추가 113
▼ 원격 서버를 클러스터에 추가하는 방법 113
서버 정보 수정 114
▼ 클러스터의 서버에 대한 정보를 수정하는 방법 114
클러스터에서 서버 제거 114
▼ 클러스터에서 서버를 제거하는 방법 114
서버 클러스터 제어 114
▼ 클러스터의 서버를 제어하는 방법 115

7 서버 기본 설정 구성 117
Proxy Server 시작 117
▼ 관리 인터페이스에서 Proxy Server를 시작하는 방법 118
UNIX 또는 Linux에서 Proxy Server를 시작하는 방법 118
Windows에서 Proxy Server를 시작하는 방법 118
SSL 사용 서버 시작 118
Proxy Server 중지 119
▼ 관리 인터페이스에서 Proxy Server를 중지하는 방법 119
UNIX 또는 Linux에서 Proxy Server를 중지하는 방법 119
Windows에서 Proxy Server를 중지하는 방법 120
Proxy Server 다시 시작 120
서버 다시 시작(UNIX 또는 Linux) 120
서버 다시 시작(Windows) 121
종료 시간 초과 설정 122
서버 설정 보기 122
▼ Proxy Server에 대한 설정을 보는 방법 122
구성 파일의 백업 보기 및 복원 123
▼ 이전 구성을 보는 방법 123

▼ 구성 파일의 백업 사본을 복원하는 방법 123
▼ 표시되는 백업 수 설정 방법 123
시스템 기본 설정 구성 124
▼ 시스템 기본 설정 수정 방법 125
Proxy Server 조정 125
▼ 기본 조정 매개 변수 변경 방법 126
청취 소켓 추가 및 편집 126
▼ 청취 소켓을 추가하는 방법 128
▼ 청취 소켓을 편집하는 방법 128
▼ 청취 소켓을 삭제하는 방법 129
디렉토리 서비스 선택 129
▼ 디렉토리 서비스 선택 방법 130
MIME 유형 130
MIME 유형 만들기 130
▼ MIME 유형 편집 방법 131
▼ MIME 유형 제거 방법 131
액세스 제어 관리 131
▼ 액세스 제어 목록 관리 방법 132
ACL 캐시 구성 132
▼ ACL 캐시 구성 방법 132
DNS 캐시 이해 133
DNS 캐시 구성 133
DNS 하위 도메인 구성 134
▼ 프록시 조회를 위한 하위 도메인의 수준 설정 방법 134
HTTP 연결 유지 구성 135
▼ HTTP 연결 유지 구성 방법 135

8 서버 액세스 제어 137
액세스 제어란 137
사용자 그룹용 액세스 제어 138
호스트-IP용 액세스 제어 145
액세스 제어 파일 사용 145
ACL 사용자 캐시 구성 146
클라이언트 인증서로 액세스 제어 146
액세스 제어 작동 방법 147

액세스 제어 설정 149
전역 액세스 제어 설정 149
서버 인스턴스용 액세스 제어 설정 151
액세스 제어 옵션 선택 153
작업 설정 153
사용자 및 그룹 지정 154
송신 호스트 지정 155
프로그램에 대한 액세스 제한 156
액세스 권한 설정 157
사용자 정의 표현식 작성 157
액세스 제어 사용 안 함 158
액세스가 거부된 경우의 응답 158
서버의 영역에 대한 액세스 제한 159
전체 서버에 대한 액세스 제한 159
디렉토리에 대한 액세스 제한 160
파일 유형에 대한 액세스 제한 160
하루 중 시간을 기준으로 액세스 제한 161
보안을 기준으로 액세스 제한 162
자원에 대한 액세스 보안 162
서버 인스턴스에 대한 액세스 보안 162
IP 기반 액세스 제어 사용 163
파일 기반 인증용 ACL 생성 163
파일 인증을 기반으로 디렉토리 서비스용 ACL 생성 164
Digest 인증을 기반으로 디렉토리 서비스용 ACL 생성 165

9 로그 파일 사용 167
로그 파일 정보 167
UNIX 및 Windows 플랫폼에서의 로깅 168
기본 오류 로깅 168
`syslog`를 사용하여 로깅 168
로그 수준 169
로그 파일 보관 170
내부 데몬 로그 교체 170
스케줄러 기반 로그 교체 171
액세스 로그 기본 설정 지정 171

▼ Administration Server용 액세스 로그 기본 설정을 지정하는 방법 173
서버 인스턴스에 대한 액세스 로그 기본 설정 지정 174
용이한 쿠키 로깅 177
오류 로깅 옵션 설정 178
▼ 오류 로깅 옵션 설정 방법 178
LOG 요소 구성 178
액세스 로그 파일 보기 179
오류 로그 파일 보기 180
로그 분석기로 작업 181
전송 시간 분산 보고서 182
데이터 흐름 보고서 182
상태 코드 보고서 183
요청 및 연결 보고서 183
캐시 성능 보고서 184
전송 시간 보고서 186
시간별 작동 보고서 186
▼ Server Manager에서 로그 분석기를 실행하는 방법 187
명령줄에서 로그 분석기 실행 방법 188
이벤트 보기(Windows) 190
▼ 이벤트 뷰어 사용 방법 190

10 서버 모니터링 191
통계를 사용하여 서버 모니터링 192
Proxy Server 통계 처리 192
통계 사용 설정 193
통계 사용 194
perfdump 유틸리티를 사용하여 현재 활동 모니터링 196
성능 버킷 사용 199
SNMP 기초 201
MIB(Management Information Base) 202
SNMP 설정 203
프록시 SNMP 에이전트 사용(UNIX) 204
프록시 SNMP 에이전트 설치 204
Proxy SNMP 에이전트 시작 205
원시 SNMP 데몬 다시 시작 205

SNMP 원시 에이전트 재구성 205
SNMP 마스터 에이전트 설치 206
▼ 마스터 SNMP 에이전트를 설치하는 방법 206
SNMP 마스터 에이전트 사용 설정 및 시작 207
다른 포트에서 마스터 에이전트 시작 207
SNMP 마스터 에이전트 직접 구성 208
마스터 에이전트 CONFIG 파일 편집 208
`sysContact` 및 `sysLocation` 변수 정의 208
SNMP 하위 에이전트 구성 209
SNMP 마스터 에이전트 시작 210
SNMP 마스터 에이전트 구성 211
커뮤니티 문자열 구성 211
트랩 대상 구성 211
하위 에이전트 사용 설정 212
SNMP 메시지 이해 212

11 URL 프록싱 및 라우팅 215
자원에 대한 프록싱 활성화/비활성화 215
▼ 자원에 대해 프록싱을 활성화하는 방법 216
다른 프록시를 통한 라우팅 216
자원에 대한 라우팅 구성 217
프록시 서버 체인 218
SOCKS 서버를 통해 라우팅 218
클라이언트 IP 주소를 서버로 전달 219
▼ 클라이언트 IP 주소를 전송하도록 프록시를 구성하는 방법 220
클라이언트의 IP 주소 확인 허용 223
▼ Java IP 주소 확인 방법 223
클라이언트 자동 구성 224
네트워크 연결 모드 설정 224
▼ Proxy Server의 실행 모드 변경 방법 225
기본 FTP 전송 모드 변경 225
▼ FTP 모드 설정 방법 226
SOCKS 이름 서버 IP 주소 지정 226
▼ SOCKS 이름 서버 IP 주소 지정 방법 227
HTTP 요청 로드 균형 조정 구성 227

▼ HTTP 요청 로드 균형 조정 구성 방법 227
URL 및 URL 매핑 관리 228
URL 매핑 만들기 및 수정 229
▼ 기존 매핑 변경 방법 231
▼ 매핑 제거 방법 231
URL 리디렉션 232

12 캐시 233
캐시 작동 방법 234
캐시 구조 이해 234
캐시에 파일 배포 235
캐시 사양 설정 236
▼ 캐시 사양 설정 방법 236
캐시 작업 디렉토리 만들기 238
캐시 크기 설정 238
HTTP 문서 캐시 238
FTP 및 Gopher 문서 캐시 240
캐시 만들기 및 수정 241
▼ 캐시 파티션 추가 방법 241
▼ 캐시 파티션 수정 방법 242
캐시 용량 설정 242
▼ 캐시 용량 설정 방법 242
캐시 섹션 관리 243
▼ 캐시 섹션 관리 방법 243
가비지 컬렉션 기본 설정 지정 244
가비지 컬렉션 예약 244
▼ 가비지 컬렉션 설정 방법 244
캐시 구성 244
▼ 캐시를 구성하는 방법 245
구성 요소 캐시 245
로컬 호스트 캐시 247
▼ 로컬 호스트 캐시를 활성화하는 방법 247
파일 캐시 구성 248
▼ 파일 캐시 구성 방법 248
URL 데이터베이스 보기 250

▼ 데이터베이스에서 URL 보는 방법 250
▼ 캐시된 URL을 통해 캐시된 URL을 만료 또는 제거하는 방법 250
캐시 일괄 업데이트 사용 251
일괄 업데이트 만들기 251
일괄 업데이트 구성 편집 또는 삭제 253
▼ 일괄 업데이트 구성을 편집하거나 삭제하는 방법 253
▼ 일괄 업데이트 구성을 삭제하는 방법 253
캐시 명령줄 인터페이스 사용 254
▼ 명령줄 유틸리티 실행 방법 254
캐시 디렉토리 구조 구축 254
캐시 URL 목록 관리 255
캐시 가비지 컬렉션 관리 259
일괄 업데이트 관리 259
ICP(Internet Cache Protocol) 사용 260
ICP 환경을 통한 라우팅 260
ICP 설정 262
▼ ICP 환경에 상위 또는 동급 프록시 추가 263
▼ ICP 환경에서 구성을 편집하는 방법 264
▼ ICP 환경에서 프록시를 제거하는 방법 265
▼ ICP 환경에서 로컬 Proxy Server를 구성하는 방법 265
▼ ICP를 활성화하는 방법 266
▼ ICP 환경을 통한 라우팅을 활성화하는 방법 267
프록시 배열 사용 268
프록시 배열을 통한 라우팅 268
프록시 배열 구성원 목록 만들기 272
프록시 배열 구성원 목록 정보 편집 274
▼ 구성원 목록 정보를 편집하는 방법 274
프록시 배열 구성원 삭제 275
프록시 배열 구성원 구성 275
프록시 배열을 통한 라우팅 활성화 276
프록시 배열 활성화 또는 비활성화 277
프록시 배열의 요청 리디렉션 278
PAT 파일에서 PAC 파일 생성 278
상위 배열을 통한 라우팅 280

13 프록시를 통한 컨텐트 필터링 283
URL 필터링 284
URL 필터 파일 만들기 284
필터 파일에 대한 기본 액세스 설정 285
컨텐트 URL 다시 작성 286
▼ URL 다시 작성 패턴을 만드는 방법 286
▼ URL 다시 작성 패턴 편집 방법 287
▼ URL 다시 작성 패턴 삭제 방법 287
특정 웹 브라우저에 대한 액세스 제한 287
▼ 클라이언트의 웹 브라우저를 기준으로 프록시에 대한 액세스 제한 방법 288
요청 차단 288
▼ MIME 유형을 기반으로 요청을 차단하는 방법 288
전송 헤더 억제 289
▼ 전송 헤더 억제 방법 290
MIME 유형별 필터링 290
▼ MIME 유형별 필터링 방법 290
HTML 태그별 필터링 291
▼ HTML 태그 필터링 방법 291
컨텐트 압축용으로 서버 구성 292
요청 시 컨텐트를 압축하도록 서버 구성 292

14 역방향 프록시 사용 295
역방향 프록싱 작동 방식 295
서버의 대역 역할을 하는 프록시 295
로드 균형 조정을 위한 프록싱 299
역방향 프록시 설정 301
▼ 정방향 또는 역방향 매핑을 만드는 방법 301
보안 역방향 프록시 설정 302
역방향 프록시의 가상 멀티호스팅 305

15 SOCKS 사용 309
SOCKS 정보 309
번들로 제공되는 SOCKS v5 서버 사용 310
▼ SOCKS 사용 방법 310
socks5.conf 정보 311

SOCKS v5 서버 시작 및 중지 312
▼ Server Manager에서 SOCKS 서버를 시작 및 중지하는 방법 312
명령줄에서 SOCKS 서버를 시작 및 중지하는 방법 312
SOCKS v5 서버 구성 312
▼ SOCKS 서버 구성 방법 312
SOCKS v5 인증 항목 구성 314
▼ SOCKS 인증 항목을 만드는 방법 314
▼ 인증 항목 편집 방법 315
▼ 인증 항목 삭제 방법 315
▼ 인증 항목 이동 방법 316
SOCKS v5 연결 항목 구성 316
▼ 연결 항목 만드는 방법 316
▼ 연결 항목 편집 방법 318
▼ 연결 항목 삭제 방법 318
▼ 연결 항목 이동 방법 319
SOCKS v5 서버 체인 구성 319
▼ SOCKS 서버 체인 구성 방법 319
라우팅 항목 구성 319
▼ 라우팅 항목 만드는 방법 320
▼ 프록시 라우팅 항목 만드는 방법 321
▼ 라우팅 항목 편집 방법 322
▼ 라우팅 항목 삭제 방법 322
▼ 라우팅 항목 이동 방법 322

16 템플리트 및 자원 관리 325
템플리트 정보 325
정규 표현식 이해 326
와일드카드 패턴 이해 327
템플리트 작업 328
▼ 템플리트 만드는 방법 328
▼ 템플리트 적용 방법 328
▼ 템플리트 제거 방법 329
▼ 템플리트 편집 방법 329
자원 제거 330
▼ 자원 제거 330

17 클라이언트 자동 구성 파일 사용 331
자동 구성 파일 이해 332
자동 구성 파일의 기능 332
Web Server로 프록시에 액세스 332
Server Manager 페이지를 사용하여 자동 구성 파일 만들기 334
▼ Server Manager를 사용하여 자동 구성 파일을 만드는 방법 334
수동으로 자동 구성 파일 만들기 336
`FindProxyForURL()` 함수 336
JavaScript 함수 및 환경 338

18 ACL 파일 구문 351
ACL 파일 및 ACL 파일 구문 정보 351
인증문 352
권한 부여문 353
기본 ACL 파일 355
obj.conf 파일 내의 ACL 파일 참조 356

19 서버 성능 조정 357
일반 성능 고려 사항 357
액세스 로깅 358
ACL 캐시 조정 358
버퍼 크기 359
연결 시간 초과 359
오류 로그 수준 359
보안 요구 사항 359
Solaris 파일 시스템 캐싱 359
시간 초과 값 360
`init-proxy()` SAF(`obj.conf` 파일) 360
`http-client-config()` SAF(`obj.conf` 파일) 361
`KeepAliveTimeout()` SAF(`magnus.conf` 파일) 361
최신 여부 확인 362
마지막으로 수정된 요소 362
DNS 설정 363
스레드 수 363
인바운드 연결 풀 364

FTP 목록 너비 365
캐시 아키텍처 365
캐시 일괄 업데이트 365
가비지 컬렉션 366
gc hi margin percent 변수 366
gc lo margin percent 변수 366
gc extra margin percent 변수 366
gc leave fs full percent 변수 367
Solaris 성능 조정 367

색인 369

머리말

이 설명서에서는 이전에는 Sun ONE™ Web Proxy Server 및 iPlanet™ Web Proxy Server였던 Sun Java ™ System Web Proxy Server 4(이하 Sun Java System Web Proxy Server 또는 Proxy Server)를 구성 및 관리하는 방법에 대해 설명합니다.

본 설명서의 대상

이 설명서는 프로덕션 환경에서의 정보 기술 관리자를 대상으로 합니다. 이 설명서에서는 사용자가 다음 영역에 대해 잘 알고 있다고 가정합니다.

- 기본 시스템 관리 작업 수행
- 소프트웨어 설치
- 웹 브라우저 사용
- 단말기 창에서 명령 실행

본 설명서를 읽기 전에

Sun Java System Web Proxy Server는 개별 제품으로 구입하거나, 네트워크 또는 인터넷 환경에 배포된 엔터프라이즈 응용 프로그램을 지원하는 소프트웨어 인프라인 Sun Java Enterprise System의 구성 요소로 구입할 수도 있습니다. Sun Java System Web Proxy Server를 Java Enterprise System의 구성 요소로 구입한 경우 `http://docs.sun.com/coll/1286.2` 및 `http://docs.sun.com/coll/1397.2`의 시스템 설명서에 익숙해야 합니다.

본 설명서의 구성

이 설명서는 특정 영역 및 작업을 다루는 여러 부분으로 나누어져 있습니다. 다음 표에는 설명서의 각 부분과 내용이 나열되어 있습니다.

표 P–1 설명서 구성

부	설명

표 P–1 설명서 구성 (계속)

1부 서버 기본	Proxy Server 및 해당 관리에 대한 개요를 제공합니다. ■ 1 장, “Sun Java System Web Proxy Server 소개” ■ 2 장, “Sun Java System Web Proxy Server 관리”
2부 Administration Server 사용	Administration Server 기본 설정의 구성, 사용자 및 그룹 관리, Proxy Server 보안 및 클러스터를 사용하여 서버 사이에서 구성을 공유하는 방법에 대해 자세히 설명합니다. ■ 3 장, “관리 기본 설정” ■ 4 장, “사용자 및 그룹 관리” ■ 5 장, “인증서 및 키 사용” ■ 6 장, “서버 클러스터 관리”
3부 Proxy Server 구성 및 모니터링	서버 기본 설정 구성, 액세스 제어 설정 및 서버 활동 모니터링에 대해 자세히 설명합니다. ■ 7 장, “서버 기본 설정 구성” ■ 8 장, “서버 액세스 제어” ■ 9 장, “로그 파일 사용” ■ 10 장, “서버 모니터링”
4부 Proxy Server 관리	Proxy Server가 요청을 처리하는 방법과 관련된 개념 및 작업에 대해 자세히 설명합니다. ■ 11 장, “URL 프록싱 및 라우팅” ■ 12 장, “캐시” ■ 13 장, “프록시를 통한 컨텐트 필터링” ■ 14 장, “역방향 프록시 사용” ■ 15 장, “SOCKS 사용” ■ 16 장, “템플리트 및 자원 관리” ■ 17 장, “클라이언트 자동 구성 파일 사용”
5부 부록	액세스 제어 목록(ACL) 파일 구문과 서버 성능 조정에 대해 설명합니다. ■ 18 장, “ACL 파일 구문” ■ 19 장, “서버 성능 조정”

Proxy Server 설명서 세트

설명서 세트에는 Proxy Server와 관련된 Sun 설명서가 나열됩니다. Proxy Server 설명서의 URL은 `http://docs.sun.com/coll/1311.8`입니다. Proxy Server에 대한 소개는 다음 표에 나열된 설명서를 순서대로 참조하십시오.

표 P–2 Sun Java System Web Proxy Server 설명서

설명서 제목	내용
Sun Java System Web Proxy Server 4.0.8 릴리스 노트	Proxy Server 릴리스: ■ 소프트웨어 및 설명서에 대한 최신 정보 ■ 새로운 기능 ■ 지원되는 플랫폼 및 환경 ■ 시스템 요구 사항 ■ 알려진 문제점 및 해결 방법
Sun Java System Web Proxy Server 4.0.8 Installation and Migration Guide	설치 및 마이그레이션 작업 수행: ■ Sun Java System Web Proxy Server 설치 ■ 버전 3.6에서 버전 4로 마이그레이션
Sun Java System Web Proxy Server 4.0.8 관리 설명서	관리 작업 수행: ■ 관리 및 명령줄 인터페이스 사용 ■ 서버 기본 설정 구성 ■ 사용자 및 그룹 관리 ■ 서버 작동 모니터링 및 로깅 ■ 서버 보안을 위한 인증서 및 공용 키 암호화 사용 ■ 서버 액세스 제어 ■ URL 프록싱 및 라우팅 ■ 캐시 ■ 컨텐트 필터링 ■ 역방향 프록시 사용 ■ SOCKS 사용
Sun Java System Web Proxy Server 4.0.8 Configuration File Reference	구성 파일 편집
Sun Java System Web Proxy Server 4.0.8 NSAPI Developer's Guide	사용자 정의 NSAPI(Netscape Server Application Programming Interface) 플러그인 만들기

관련 설명서

Sun Java Enterprise System(Java ES) 및 구성 요소에 대한 모든 설명서의 URL은 `http://docs.sun.com/prod/entsys.5` 및 `http://docs.sun.com/prod/entsys.5?l=ko`입니다.

기본 경로 및 파일 이름

다음 표에서는 이 설명서에서 사용되는 기본 경로와 파일 이름에 대해 설명합니다.

표 P–3 기본 경로 및 파일 이름

자리 표시자	설명	기본값
install-dir	Sun Java System Web Proxy Server의 기본 설치 디렉토리를 나타냅니다.	Solaris 및 Linux 설치: /opt/sun/proxyserver40 Windows 설치: \Sun\ProxyServer40

활자체 규약

이 표에서는 본 설명서에서 사용된 여러 활자체 변경 사항에 대해 설명합니다.

표 P–4 활자체 규약

서체	의미	예
`AaBbCc123`	명령, 파일 및 디렉토리 이름과 화면상의 컴퓨터 출력	`.login` 파일을 편집합니다. `ls -a`를 사용하여 모든 파일을 나열합니다. `machine_name% you have mail.`
`AaBbCc123`	화면상의 컴퓨터 출력과는 반대로 사용자가 직접 입력하는 사항입니다.	`machine_name%` **`su`** `Password:`
AaBbCc123	실제 이름이나 값으로 대체해야 하는 자리 표시자입니다.	파일을 제거하는 명령은 `rm` *filename*입니다.
AaBbCc123	설명서 제목, 새로운 용어 및 강조 표시할 용어(일부 강조 항목은 온라인에서 굵게 표시됨)에 사용됩니다.	**사용자 설명서**의 6장을 참조하십시오. **캐시**는 로컬에 저장된 사본입니다. 파일을 저장하지 **마십시오**.

명령 쉘 프롬프트 예

다음 표에서는 기본 시스템 프롬프트 및 수퍼유저 프롬프트를 보여 줍니다.

표 P–5 쉘 프롬프트

쉘	프롬프트
UNIX 및 Linux 시스템의 C 쉘	`machine_name%`
UNIX 및 Linux 시스템의 C 쉘 수퍼유저	`machine_name#`
UNIX 및 Linux 시스템의 Bourne 쉘 및 Korn 쉘	`$`
UNIX 및 Linux 시스템의 Bourne 쉘 및 Korn 쉘 수퍼유저	`#`
Microsoft Windows 명령줄	`C:\`

기호 규칙

다음 표에서는 본 설명서에서 사용되는 기호에 대해 설명합니다.

표 P–6 기호 규칙

기호	설명	예	의미
`[ ]`	선택적 인수 및 명령 옵션을 포함합니다.	`ls [-l]`	`-l` 옵션은 사용하지 않아도 됩니다.
`{ | }`	필수 명령 옵션에 대한 일련의 선택 사항을 포함합니다.	`-d {y|n}`	`-d` 옵션에서는 `y` 인수나 `n` 인수를 사용해야 합니다.
`${ }`	변수 참조를 나타냅니다.	`${com.sun.javaRoot}`	`com.sun.javaRoot` 변수의 값을 나타냅니다.
-	동시에 입력하는 여러 키를 결합합니다.	Ctrl-A	Ctrl 키를 누른 채로 A 키를 누릅니다.
+	연속해서 입력하는 여러 키를 결합합니다.	Ctrl+A+N	Ctrl 키를 눌렀다가 놓은 다음 후속 키를 누릅니다.
→	그래픽 사용자 인터페이스의 메뉴 항목 선택을 나타냅니다.	Fil → New → Templates	File 메뉴에서 New를 선택합니다. New 하위 메뉴에서 Templates를 선택합니다.

설명서, 지원 및 교육

Sun 웹 사이트에서는 다음의 추가 자원에 대한 내용을 제공합니다.

- 설명서(`http://www.sun.com/documentation/`)
- 지원(`http://www.sun.com/support/`)
- 교육(`http://www.sun.com/training/`)

Sun 제품 설명서 검색

docs.sun.com℠ 웹 사이트에서 Sun 제품 설명서를 검색하거나 검색 엔진을 사용하여 검색 필드에 다음 구문을 입력할 수도 있습니다.

search-term `site:docs.sun.com`

예를 들어 “broker” 를 검색하려면 다음을 입력합니다.

```
broker site:docs.sun.com
```

검색에 다른 Sun 웹 사이트를 포함하려면(예: java.sun.com, www.sun.com 및 developers.sun.com), 검색 필드에 `docs.sun.com` 대신 `sun.com`을 사용하십시오.

타사 웹 사이트 참조

이 설명서에 언급된 타사 URL을 통해 관련된 추가 정보를 얻을 수 있습니다.

주 – Sun은 이 설명서에 언급된 타사 웹 사이트의 가용성에 대해 책임지지 않습니다. 또한 해당 사이트나 리소스를 통해 제공되는 내용, 광고, 제품 및 기타 자료에 대해 어떠한 보증도 하지 않으며 그에 대한 책임도 지지 않습니다. 따라서 타사 웹 사이트의 내용, 제품 또는 리소스의 사용으로 인해 발생한 실제 또는 주장된 손상이나 피해에 대해서도 책임을 지지 않습니다.

Sun은 여러분의 의견을 환영합니다

Sun은 설명서의 내용 개선에 노력을 기울이고 있으며, 여러분의 의견과 제안을 환영합니다. 사용자 의견을 보내시려면 `http://docs.sun.com`에서 "의견 보내기"를 누릅니다. 온라인 양식에 전체 설명서 제목과 부품 번호를 입력합니다. 부품 번호는 해당 설명서의 제목 페이지나 문서의 URL에 있는 7자리 또는 9자리 숫자입니다. 예를 들어 이 설명서의 부품 번호는 820–6316입니다. 사용자 의견을 제출할 때 해당 양식에 영문 설명서 제목과 부품 번호를 입력해야 할 수도 있습니다. 본 설명서의 영문 부품 번호와 제목은 820–5723, Sun Java System Web Proxy Server 4.0.8 Administration Guide입니다.

◆ ◆ ◆ 1 장

1 Sun Java System Web Proxy Server 소개

이 장에서는 이 릴리스의 새로운 기능에 대한 간략한 설명과 Proxy Server를 관리 및 구성하는 데 사용된 웹 기반 사용자 인터페이스의 개요를 포함하여 Sun Java System Web Proxy Server의 일반적인 개요를 제공합니다.

이 장은 다음 내용으로 구성되어 있습니다.

- 25 페이지 “Sun Java System Web Proxy Server 정보”
- 25 페이지 “이 릴리스의 새로운 기능”
- 26 페이지 “시작하기”

Sun Java System Web Proxy Server 정보

Sun Java System Web Proxy Server는 고성능 인터넷 및 인트라넷 환경을 위한 HTTP 캐싱 및 가속 기반을 나타냅니다. Proxy Server는 웹 컨텐트를 캐싱 및 필터링하고 네트워크 성능을 향상시키며 전체 네트워크 인프라와의 통합, 교차 플랫폼 지원 및 중앙 집중식 관리 기능을 제공하는 시스템입니다. 네트워크 트래픽 관리자 역할을 수행하여 정보를 효율적으로 배포 및 관리하기 때문에 네트워크 트래픽 및 사용자 대기 시간이 줄어듭니다. 또한 Proxy Server는 컨텐트 배포를 위한 보안 게이트웨이를 제공하고 인터넷 트래픽을 위한 제어 지점 역할을 수행하여 사용자가 네트워크 자원에 안전하고 효율적으로 액세스할 수 있도록 합니다.

이 릴리스의 새로운 기능

Sun Java System Web Proxy Server 4에는 다음과 같은 향상된 기능이 포함되어 있습니다.

- 최신 HTTP 코어
- Linux 및 Solaris™ x86 플랫폼 지원
- 모든 플랫폼에서 최신 SSL(Secure Sockets Layer) 지원
- 모든 플랫폼에서 다중 스레드 아키텍처
- 관리 향상, 그래픽 사용자 인터페이스 및 관리의 용이성

- 새로운 NSAPI(Netscape Server Application Programming Interface) 필터
- 향상된 LDAP(Lightweight Directory Access Protocol) 성능
- 향상된 확장성 및 성능
- 향상된 컨텐트 필터링
- `server.xml` 구성 파일의 구현

새로운 기능 및 향상된 기능에 대한 자세한 내용은 다음 사이트에서 Sun Java System Web Proxy Server **릴리스 노트**를 참조하십시오. `http://docs.sun.com/coll/1311.8`.

시작하기

Sun Java System Web Proxy Server는 Administration Server 및 Server Manager 웹 기반 사용자 인터페이스를 통해 관리 및 구성됩니다. Administration Server는 시스템에 설치된 모든 Proxy Server 인스턴스에 공통적인 구성을 관리하는 데 사용되는 반면 Server Manager는 개별 서버 인스턴스의 설정을 구성하는 데 사용됩니다.

이 절은 다음 내용으로 구성되어 있습니다.

- 26 페이지 “Administration Server 개요”
- 27 페이지 “Server Manager 개요”
- 28 페이지 “구성 파일”
- 29 페이지 “정규 표현식”

주 – 서버를 구성하는 데 필요한 CGI 프로그램을 실행하려면 브라우저에서 쿠키를 활성화해야 합니다.

Administration Server 개요

Administration Server는 시스템에 설치된 모든 Sun Java System Web Proxy Server 인스턴스에 공통적인 구성을 관리하는 데 사용되는 웹 기반 사용자 인터페이스입니다.

Administration Server를 시작한 후 브라우저를 실행하고 URL을 입력하여 Administration Server에 액세스합니다. URL은 설치 시 지정한 호스트 이름 및 포트 번호에 의해 결정됩니다(예: `http://myserver.mycorp.com:1234`).

둘 이상의 관리자에게 Administration Server에 대한 액세스 권한을 부여할 수 있습니다. 분산 관리에 대한 자세한 내용은 38 페이지 “여러 관리자 허용”을 참조하십시오.

Administration Server 설정은 특정 작업에 해당하는 탭으로 구성됩니다. 다음 표에서는 Administration Server 탭과 함께 해당 탭이 제공하는 작업에 대해 간단히 설명합니다.

- Servers - 프록시 서버 관리, 추가, 제거, 마이그레이션
- Preferences - Administration Server 종료, 청취 소켓 편집, 수퍼유저 액세스 구성, 여러 관리자를 허용하는 분산 관리 구성, 액세스 및 오류 로그 사용자 정의 및 보기

- Global Settings - 디렉토리 서비스 구성, 액세스 제어 지정, SNMP 마스터 에이전트 설정 구성
- Users and Groups - 사용자, 그룹 및 조직 구성 단위 추가 및 관리
- Security - 새 트러스트 데이터베이스 만들기, VeriSign 및 기타 인증서 요청 및 설치, 키 쌍 파일 비밀번호 변경, 설치된 인증서 보기 및 관리, CRL(Certificate Revocation List) 및 CKL(Compromised Key List) 추가 또는 교체, CRL 및 CKL 관리, 3.x 인증서 마이그레이션
- Cluster - 클러스터에서 원격 서버 제어, 원격 서버 추가 및 제거, 서버 정보 수정

다음 버튼은 현재 탭 또는 페이지에 관계없이 표시됩니다.

- Version - Sun Java System Web Proxy Server에 대한 버전 정보 표시
- Refresh - 현재 페이지 새로 고침
- Help - 현재 페이지에 대한 온라인 도움말 표시

▼ Administration Server에 액세스하는 방법

1 **브라우저를 시작하고 설치 시 Administration Server에 대해 지정한 호스트 이름 및 포트 번호를 반영하는 URL로 이동합니다(예:** `http://myserver.mycorp.com:1234`**).**

2 **프롬프트가 표시되면 설치 시 지정한 사용자 이름 및 비밀번호를 입력합니다.**

Administration Server의 사용자 인터페이스가 표시됩니다.

Administration Server 사용에 대한 자세한 내용은 2 장, “Sun Java System Web Proxy Server 관리”을 참조하십시오. 또한 Administration Server 탭 및 페이지에 대한 온라인 도움말을 참조하십시오.

Server Manager 개요

Server Manager는 Sun Java System Web Proxy Server의 개별 인스턴스를 시작, 중지 및 구성하는 데 사용되는 웹 기반 사용자 인터페이스입니다.

Server Manager 설정은 특정 작업에 해당하는 탭으로 구성됩니다. 다음은 Server Manager 탭 목록을 나열하고 탭이 제공하는 작업에 대해 간단히 설명합니다.

- Preferences - 서버 시작 및 중지, 서버 설정 보기, 구성 정보 복원, 시스템 기본 설정 구성, Proxy Server 성능 조정, 청취 소켓 추가 및 편집, MIME 유형 관리, 액세스 제어 관리, ACL 및 DNS 캐시 구성, DNS 로컬 하위 도메인 구성, HTTP 연결 유지 설정 구성, 암호 크기 설정
- Routing - 프록시 활성화 및 비활성화, 라우팅 기본 설정 지정, 클라이언트 자격 증명 전달, Java IP 주소 확인 활성화, 자동 구성 파일 만들기 및 편집, 연결 모드 설정, 기본 FTP 전송 모드 변경, SOCKS 이름 서버 IP 주소 설정, HTTP 요청 로드 균형 조정 구성
- SOCKS - SOCKS 서버 시작 및 중지, SOCKS 인증, 연결 및 라우팅 항목 만들기 및 관리

- URLs - URL 매핑 및 리디렉션 보기, 만들기 및 관리
- Caching - 캐시 사양 설정, 캐시 파티션 추가 및 수정, 기존 파티션 사이 섹션 이동, 캐시 용량 설정, 가비지 컬렉션 모드 설정, 캐시 조정, 가비지 컬렉션 예약, 가비지 컬렉션 설정 조정, 특정 자원에 대한 캐싱 구성, 로컬 호스트의 캐싱 활성화, 파일 캐시 설정 변경, 캐시 배치 업데이트 설정, 캐시된 URL 기록에 대한 정보 보기, ICP 환경에 프록시 구성, 프록시 배열 구성원 목록 만들기 및 업데이트, 프록시 배열 구성원 구성, PAT 파일의 정보 보기
- Filters - 필터 파일 만들기, 컨텐트 URL 다시 작성 설정, 사용자 에이전트 제한 및 요청 차단 설정, 전송 헤더 억제, MIME 필터 및 HTML 태그 필터 설정, 요청 시 컨텐트 압축
- Server Status - 로그 파일 보기, 로그 보관, 로그 기본 설정 지정, 보고서 생성, 현재 작동 모니터링, SNMP 하위 에이전트 구성 및 제어
- Security - 새 트러스트 데이터베이스 만들기, VeriSign 및 기타 인증서 요청 및 설치, 키 쌍 파일 비밀번호 변경, 설치된 인증서 보기 및 관리, CRL(Certificate Revocation List) 및 CKL(Compromised Key List) 추가 및 대체, CRL 및 CKL 관리, 3.x 인증서 마이그레이션
- Templates - 템플리트 만들기, 제거, 적용 및 보기, 자원 제거

다음 버튼은 현재 탭 또는 페이지에 관계없이 표시됩니다.

- Version - Sun Java System Web Proxy Server에 대한 버전 정보 표시
- Refresh - 현재 페이지 새로 고침
- Help - 현재 페이지에 대한 온라인 도움말 표시

  경우에 따라 Refresh 버튼 아래에 Restart Required 링크가 표시될 수 있습니다. 이 링크는 변경 사항이 발생하여 서버를 다시 시작해야 함을 나타냅니다. 변경 사항을 적용하려면 링크를 누르고 원하는 작업을 지정합니다.

  Server Manager 사용에 대한 자세한 내용은 이 설명서의 관련 작업을 참조하십시오. 또한 Server Manager 탭 및 페이지의 온라인 도움말을 참조하십시오.

▼ Server Manager에 액세스하는 방법

1 **26 페이지 "Administration Server 개요"에 설명된 대로 Administration Server에 액세스합니다.**

Servers 탭에 Administration Server가 나타납니다.

2 **Manage Servers 페이지에서 관리할 서버 인스턴스의 링크를 누릅니다.**

Server Manager 사용자 인터페이스가 나타납니다.

구성 파일

Sun Java System Web Proxy Server의 구성 및 동작은 구성 파일 집합에 의해 결정됩니다. 관리 인터페이스에서 구성된 설정은 구성 파일에 반영됩니다. 파일은 수동으로도 편집할 수 있습니다.

구성 파일은 *instance-dir* /config 디렉토리에 있으며 여기서 *instance-dir*은 서버 인스턴스입니다. config 디렉토리에는 서로 다른 구성 요소를 제어하는 다양한 구성 파일이 포함되어 있습니다. 구성 파일의 수 및 이름은 활성화 또는 로드된 구성 요소에 따라 다릅니다. 이 디렉토리에는 항상 서버 작동에 필수적인 네 가지 구성 파일이 포함되어 있습니다. 다음 표에는 네 가지 필수 구성 파일 및 해당하는 내용이 나열되어 있습니다.

표 1–1 필수 구성 파일

파일	포함된 내용
server.xml	대부분의 서버 구성(이 Proxy Server 릴리스의 새로운 기능)
magnus.conf	전역 서버 초기화 정보
obj.conf	클라이언트의 요청을 처리하기 위한 지침
mime.types	요청된 자원의 컨텐트 유형을 결정하기 위한 정보

이러한 파일 및 기타 구성 파일에 대한 자세한 내용은 Proxy Server 4.0.8 *Configuration File Reference*를 참조하십시오.

정규 표현식

정규 표현식을 사용하여 자원을 식별하고 여러 URL의 요청을 다르게 처리하도록 Proxy Server를 구성할 수 있습니다. Administration Server 및 Server Manager 사용자 인터페이스를 사용하여 다양한 작업을 수행할 때 정규 표현식을 지정할 수 있습니다. 정규 표현식 사용에 대한 자세한 내용은 16 장, “템플리트 및 자원 관리”을 참조하십시오.

◆ ◆ ◆ 2 장

2 Sun Java System Web Proxy Server 관리

이 장에서는 Administration Server를 사용하여 Sun Java System Web Proxy Server를 관리하기 위한 기본 사항에 대해 설명합니다. Administration Server는 서버를 관리, 추가, 제거 및 마이그레이션하는 데 사용되는 웹 기반 사용자 인터페이스입니다.

이 장은 다음 내용으로 구성되어 있습니다.

- 31 페이지 "Administration Server 시작"
- 32 페이지 "Administration Server 중지"
- 33 페이지 "여러 Proxy Server 실행"
- 33 페이지 "서버 인스턴스 제거"
- 34 페이지 "Proxy Server 3.6에서 마이그레이션"

Administration Server 기본 설정 구성에 대한 자세한 내용은 3 장, "관리 기본 설정"을 참조하십시오. 서버 클러스터를 사용하여 여러 Proxy Server를 관리하는 데 대한 자세한 내용은 6 장, "서버 클러스터 관리"을 참조하십시오.

Administration Server 시작

이 절에서는 다른 플랫폼에서 Administration Server를 시작하는 방법에 대해 설명합니다. Administration Server 중지에 대한 자세한 내용은 32 페이지 "Administration Server 중지"를 참조하십시오.

UNIX 또는 Linux에서 Administration Server를 시작하는 방법

1. 명령줄에서 *server-root*/proxy-admserv로 이동한 다음
2. ./start를 입력하여 Administration Server를 시작합니다(또는 Administration Server를 다시 시작하려면 ./restart를 입력함).

Windows에서 Administration Server를 시작하는 방법

Windows에서 Administration Server는 다음 중 한 가지 방법으로 시작할 수 있습니다.

- 시작->프로그램->Sun Microsystems->Sun Java System Web Proxy Server *version*->Start Admin을 사용합니다.
- 제어판->관리 도구->서비스->Sun Java System Web Proxy Server 4.0 Administration Server->시작을 사용합니다.
- 명령 프롬프트에서 *server-root*\proxy-admserv로 이동한 다음 startsvr.bat를 입력하여 Administration Server를 시작합니다(또는 ./restart를 입력하여 Administration Server를 다시 시작함).

Administration Server를 시작한 후 브라우저를 시작하고, 설치하는 동안 Administration Server에 대해 지정한 호스트 이름과 포트 번호를 반영하는 URL을 제공하여 액세스할 수 있습니다. 예를 들면 http://myserver.mycorp.com:1234와 같이 URL을 입력합니다. 설치하는 동안 지정한 사용자 이름과 비밀번호를 묻는 메시지가 표시됩니다.

둘 이상의 관리자에게 Administration Server에 대한 액세스 권한을 부여할 수 있습니다. 분산 관리에 대한 자세한 내용은 38 페이지 “여러 관리자 허용”을 참조하십시오.

Administration Server 중지

이 절에서는 다른 플랫폼에서 Administration Server를 중지하는 방법에 대해 설명합니다. Administration Server 시작에 대한 자세한 내용은 31 페이지 “Administration Server 시작”을 참조하십시오.

UNIX 또는 Linux에서 Administration Server를 중지하는 방법

다음 중 한가지 방법으로 UNIX 또는 Linux에서 Administration Server를 중지할 수 있습니다.

- 관리 인터페이스 사용:
  1. Administration Server로 액세스합니다.
  2. Preferences 탭을 선택합니다.
  3. Shutdown Server 링크를 누릅니다.
  4. OK를 누릅니다.
- 명령줄에서 *server-root*/proxy-admserv/로 이동한 다음 ./stop을 입력합니다.

Windows에서 Administration Server를 중지하는 방법

Windows에서 Administration Server는 다음 중 한 가지 방법으로 중지할 수 있습니다.

- 다음과 같이 서비스 창에서 Sun Java System Proxy Server 4.0 Administration Server 서비스를 사용합니다. 제어판->관리 도구->서비스->Sun Java System Web Proxy Server 4.0 Administration Server> 중지
- 명령 프롬프트에서 *server-root*\proxy-admserv로 이동한 다음 stopsvr.bat를 입력합니다.

여러 Proxy Server 실행

시스템에서 여러 Proxy Server를 실행하려면 서버 인스턴스를 여러 개 설치 및 구성해야 합니다. 다음 절차에서 서버 인스턴스를 추가하는 방법에 대해 설명합니다.

▼ 여러 서버 인스턴스를 설치하는 방법

1. **Administration Server로 액세스합니다.**
2. **Servers 탭에서 Add Server를 누릅니다.**
3. **요청된 정보를 제공하고 OK를 누릅니다.**
   특정 필드에 대한 자세한 내용은 온라인 도움말을 참조하십시오.
4. **원하는 경우 새 서버 인스턴스를 성공적으로 추가한 후 표시되는 성공 페이지에서 Configure Your New Server 링크를 누릅니다.**
   Server Manager 인터페이스가 표시됩니다. 이 인터페이스를 사용하여 서버 인스턴스를 구성할 수 있습니다.

서버 인스턴스 제거

Administration Server를 사용하여 Proxy Server 인스턴스를 제거할 수 있습니다. 이 프로세스는 실행 취소할 수 없기 때문에 다음 절차를 수행하기 전에 서버 인스턴스를 제거할지 여부를 확인해야 합니다.

▼ 서버 인스턴스를 제거하는 방법

1. Administration Server로 액세스합니다.
2. Servers 탭에서 Remove Server를 누릅니다.
3. 드롭다운 목록에서 제거할 서버 인스턴스를 선택합니다.
4. Confirming Server Removal 확인란을 선택하고 OK를 누릅니다.

Proxy Server 3.6에서 마이그레이션

Sun One Web Proxy Server 3.6(iPlanet Web Proxy Server라고도 함)을 Sun Java System Web Proxy Server 4로 마이그레이션할 수 있습니다. 3.6 서버는 보존되고 동일한 설정을 가진 새 버전 4가 만들어집니다. 버전 3.6에서 버전 4로의 서버 마이그레이션에 대한 자세한 내용은 **Sun Java System Web Proxy Server 4.0.8 Installation and Migration Guide**를 참조하십시오. 또한 Proxy Server 사용자 인터페이스의 마이그레이션 관련 페이지에 대해서는 온라인 도움말을 참조하십시오. 인증서 마이그레이션에 대한 자세한 내용은 이 설명서의 81 페이지 “이전 버전의 인증서 마이그레이션”을 참조하십시오.

◆ ◆ ◆ 3 장

3 관리 기본 설정

이 장에서는 Administration Server를 사용하여 관리 기본 설정을 구성하는 방법에 대해 설명합니다. 서버 구성에 필요한 CGI 프로그램을 실행하려면 브라우저에서 쿠기를 사용하도록 설정해야 합니다.

이 장은 다음 내용으로 구성되어 있습니다.

- 35 페이지 "청취 소켓 만들기 및 관리"
- 37 페이지 "수퍼유저 설정 변경"
- 38 페이지 "여러 관리자 허용"
- 39 페이지 "로그 파일 옵션 지정"
- 40 페이지 "디렉토리 서비스 사용"
- 40 페이지 "서버 액세스 제한"
- 41 페이지 "SNMP 마스터 에이전트 설정"

청취 소켓 만들기 및 관리

서버가 요청을 처리하기 전에 요청은 청취 소켓에 의해 수락된 다음 올바른 서버로 전달되어야 합니다. Proxy Server를 설치하면 청취 소켓(`ls1`)이 자동으로 만들어집니다. 이 청취 소켓은 IP 주소 `0.0.0.0` 및 설치하는 동안 Administration Server 포트 번호로 지정된 포트 번호를 사용합니다.

청취 소켓은 Administration Server의 Edit Listen Sockets 페이지를 사용하여 추가, 편집 및 삭제합니다. 서버에 액세스하기 위해서는 최소 하나의 청취 소켓이 있어야 합니다. 청취 소켓이 하나만 나열된 경우 청취 소켓을 삭제할 수 없습니다.

이 절에서는 청취 소켓을 추가, 편집 및 삭제하는 방법에 대해 설명합니다.

▼ 청취 소켓을 추가하는 방법

1. **Administration Server에 액세스하고 Preferences 탭을 선택합니다.**
2. **Edit Listen Sockets 링크를 누릅니다.**
3. **New 버튼을 누릅니다.**
4. **설정을 지정하고 OK를 누릅니다.**
   특정 필드에 대한 자세한 내용은 온라인 도움말을 참조하십시오.

▼ 청취 소켓을 편집하는 방법

1. **Administration Server에 액세스하고 Preferences 탭을 선택합니다.**
2. **Edit Listen Sockets 링크를 누릅니다.**
3. **편집할 청취 소켓의 링크를 누릅니다.**
4. **원하는 사항을 변경한 다음 OK를 누릅니다.**

▼ 청취 소켓을 삭제하는 방법

1. **Administration Server에 액세스하고 Preferences 탭을 선택합니다.**
2. **Edit Listen Sockets 링크를 누릅니다.**
3. **삭제할 청취 소켓 옆에 있는 확인란을 선택하고 OK를 누릅니다.**
4. **삭제를 확인하는 메시지가 표시되면 OK를 누릅니다.**
   서버에 액세스하기 위해서는 최소 하나의 청취 소켓이 있어야 합니다. 청취 소켓이 하나만 나열된 경우 청취 소켓을 삭제할 수 없습니다.

수퍼유저 설정 변경

Administration Server에 대해 수퍼유저 액세스를 구성할 수 있습니다. 이 설정은 오직 수퍼유저 계정에만 적용됩니다. Administration Server가 분산 관리를 사용하는 경우 허용된 관리자에 대해 추가 액세스 제어를 구성해야 합니다.

주의 – Sun Java System Directory Server를 사용하여 사용자와 그룹을 관리하는 경우 수퍼유저 사용자 이름 또는 비밀번호를 변경하기 **전에** 디렉토리에서 수퍼유저 항목을 업데이트해야 합니다. 디렉토리를 먼저 업데이트하지 않으면 Administration Server의 사용자 및 그룹 인터페이스에 액세스할 수 없게 됩니다. 그러면 디렉토리에 대한 액세스 권한이 없는 관리자 계정으로 Administration Server에 액세스하거나 Directory Server의 콘솔 또는 구성 파일을 사용하여 디렉토리를 업데이트해야 합니다.

▼ Administration Server에 대한 수퍼유저 설정을 변경하는 방법

1. **Administration Server에 액세스하고 Preferences 탭을 선택합니다.**
2. **Control Superuser Access 링크를 누릅니다.**
3. **원하는 사항을 변경한 다음 OK를 누릅니다.**
   특정 필드에 대한 자세한 내용은 온라인 도움말을 참조하십시오.

   수퍼유저의 사용자 이름과 비밀번호는 *server-root*`/proxy-admserv/config`에 있는 `admpw`라는 파일에 보관되어 있습니다. 파일의 형식은 *username*:*password*입니다. 이 파일을 보고 사용자 이름을 확인할 수 있지만 비밀번호는 암호화되어 읽을 수 없습니다. 비밀번호를 잊어 버린 경우 새 비밀번호로 변경할 수 있습니다.

▼ 수퍼유저 비밀번호를 변경하는 방법

1. `admpw` **파일을 편집하고 암호화된 비밀번호를 삭제합니다.**
2. **비밀번호 없이 사용자 이름으로 Administration Server에 액세스합니다.**
3. **Preferences 탭을 누릅니다.**
4. **Control Superuser Access 링크를 누릅니다.**
5. **새 비밀번호를 제공하고 OK를 누릅니다.**

주의 – admpw 파일을 편집할 수 있기 때문에 서버 컴퓨터를 안전한 장소에 보관하고 파일 시스템에 대한 액세스를 제한해야 합니다.

UNIX 및 Linux 시스템의 경우 파일의 소유권을 변경하여 루트나 Administration Server 데몬을 실행하는 시스템 사용자만 쓸 수 있도록 합니다. Windows 시스템의 경우 파일의 소유권을 Administration Server가 사용하는 사용자 계정으로 제한합니다.

여러 관리자 허용

여러 관리자가 분산 관리를 통해 서버의 특정 부분을 변경할 수 있습니다. 분산 관리를 사용하도록 설정하기 전에 디렉토리 서버를 설치해야 합니다. 기본 디렉토리 서버는 LDAP 기반이어야 합니다.

분산 관리를 위한 두 가지 사용자 수준은 수퍼유저와 관리자입니다.

- 수퍼유저는 *server-root*/proxy-admserv/config/admpw에 나열된 사용자입니다. 이는 설치하는 동안 지정한 사용자 이름 및 비밀번호입니다. 이 사용자는, 수퍼유저가 LDAP 서버에서 유효한 계정을 가지는지 여부에 따라 달라지는 액세스인 사용자 및 그룹 형식을 제외한, Administration Server의 모든 형식에 대한 전체 액세스 권한을 가집니다.
- 관리자는 Administration Server를 포함하여 특정 서버의 Server Manager 형식으로 직접 이동할 수 있습니다. 표시되는 형식은 관리자용으로 구성된 액세스 제어 규칙에 따라 다르며, 보통 수퍼유저가 설정합니다. 관리자는 제한된 관리 작업을 수행하며 사용자 추가나 액세스 제어 변경 등 다른 사용자에게 영향을 미치는 사항을 변경할 수도 있습니다.

액세스 제어에 대한 자세한 내용은 8 장, “서버 액세스 제어”을 참조하십시오.

▼ 분산 관리를 사용 설정하는 방법

1. **디렉토리 서버가 설치되어 있는지 확인합니다.**
2. **Administration Server로 액세스합니다.**
3. **(선택 사항) 디렉토리 서버를 설치했지만 관리 그룹을 아직 만들지 않은 경우 관리 그룹을 만들어야 합니다. 그룹을 만드는 방법:**

   a. **Users and Groups 탭을 누릅니다.**

   b. **Create Group 링크를 누릅니다.**

c. LDAP 디렉토리에 관리자 그룹을 만들고 Administration Server 또는 해당 서버 루트에 설치된 서버의 구성 권한을 부여하려는 사용자의 이름을 추가합니다.

특정 필드에 대한 자세한 내용은 온라인 도움말을 참조하십시오.

관리자 그룹의 모든 사용자는 Administration Server 전체에 액세스할 수 있지만 액세스 제어를 사용하여 구성할 수 있는 서버 및 양식을 제한할 수 있습니다.

액세스 제어 목록을 만들면 분산 관리 그룹이 목록에 추가됩니다. 관리자 그룹의 이름을 변경하는 경우 직접 액세스 제어를 편집하여 제어가 참조하는 그룹을 변경해야 합니다.

4 Preferences 탭을 누릅니다.

5 Configure Distributed Administration 링크를 누릅니다.

6 Yes를 선택하고 관리자 그룹을 지정한 다음 OK를 누릅니다.

로그 파일 옵션 지정

Administration Server 로그 파일은 발생한 오류 유형 및 서버 액세스에 대한 정보를 포함하여 Administration Server에 대한 데이터를 기록합니다. 로그 정보를 사용하여 서버 작동을 모니터링하고 문제를 해결할 수 있습니다. 로그 기본 설정 페이지의 여러 옵션을 사용하여 Administration Server 로그에 기록되는 데이터의 유형과 형식을 지정할 수 있습니다. Common Logfile Format을 선택할 수 있는데, 이는 서버에 대한 고정된 양의 정보를 제공하거나 요구 사항에 맞추어 사용자 정의 로그 파일 형식을 만들 수 있습니다.

Administration Server Log Preferences 페이지에 액세스하려면 Preferences 탭을 누른 다음 Set Access Log Preferences 또는 Set Error Log Preferences 링크를 누릅니다. 로그 파일 및 로그 파일 옵션 설정에 대한 자세한 내용은 9 장, “로그 파일 사용”을 참조하십시오. 온라인 도움말도 참조하십시오.

로그 파일 확인

Administration Server 로그 파일은 *server-root*/proxy-admserv/logs에 있습니다. Proxy Serve 관리 콘솔 또는 텍스트 편집기를 통해 오류 및 액세스 로그를 모두 볼 수 있습니다.

액세스 로그 파일

액세스 로그 파일에는 서버로 전송되는 요청 및 서버에서 보내는 응답에 대한 정보가 기록됩니다.

▼ 액세스 로그 파일을 보는 방법

1 **Administration Server에 액세스하고 Preferences 탭을 누릅니다.**

2 **View Access Log 링크를 누릅니다.**
특정 필드에 대한 자세한 내용은 온라인 도움말을 참조하십시오. 9 장, "로그 파일 사용"도 참조하십시오.

오류 로그 파일

오류 로그에는 로그 파일이 작성된 이후 발생한 서버의 모든 오류가 나열됩니다. 또한 서버가 시작된 시간 및 서버에 로그인을 시도했으나 실패한 사용자 등 서버에 대한 정보 메시지가 포함되어 있습니다.

▼ 오류 로그 파일을 보는 방법

1 **Administration Server에 액세스하고 Preferences 탭을 누릅니다.**

2 **View Error Log 링크를 누릅니다.**
특정 필드에 대한 자세한 내용은 온라인 도움말을 참조하십시오. 9 장, "로그 파일 사용"도 참조하십시오.

디렉토리 서비스 사용

LDAP를 사용하는 단일 디렉토리 서버의 사용자 이름 및 비밀번호와 같은 정보를 저장하고 관리할 수 있습니다. 또한 사용자가 쉽게 액세스할 수 있는 여러 네트워크 위치에서 디렉토리 정보를 검색할 수 있도록 서버를 구성할 수 있습니다. 디렉토리 서비스 사용에 대한 자세한 내용은 4 장, "사용자 및 그룹 관리"을 참조하십시오.

서버 액세스 제한

Proxy Server는 수신된 요청을 평가할 때 ACE(Access Control Entries)라고 하는 규칙 계층에 따라 액세스를 결정하며 그런 다음 일치되는 항목을 사용하여 요청의 허가 또는 거부 여부를 결정합니다. 각 ACE는 서버가 계층의 다음 ACE로 계속할 것인지 여부를 지정합니다. ACE의 컬렉션은 ACL(Access Control List)이라고 합니다.

파일, 디렉토리 및 파일 형식과 같이 서버 인스턴스 내에서 Administration Server 및 특정 자원의 액세스에 대해 액세스 제어를 구성할 수 있습니다. Administration Server에 대한 액세스 제어는 Administration Server의 Global Settings 탭에서 구성됩니다. 서버 인스턴스 내에서 자원에 대한 액세스 제어는 Server Manager의 Preferences 탭에서 구성됩니다. 액세스 제어 설정에 대한 자세한 내용은 8 장, "서버 액세스 제어"을 참조하십시오.

주 – 서버 액세스를 제한하기 전에 분산 관리를 사용하도록 설정해야 합니다. 자세한 내용은 38 페이지 "여러 관리자 허용"을 참조하십시오.

SNMP 마스터 에이전트 설정

SNMP(Simple Network Management Protocol)는 네트워크 작동에 대한 데이터를 교환하는 데 사용하는 프로토콜입니다. 이 정보는 하위 에이전트 및 마스터 에이전트를 사용하여 네트워크 관리 스테이션과 서버 간에 전송됩니다.

SNMP 마스터 에이전트 설정은 Administration Server의 Global Settings 탭을 사용하여 구성됩니다. 마스터 에이전트는 Administration Server에 설치됩니다. SNMP 및 에이전트 설정에 대한 자세한 내용은 10 장, "서버 모니터링"을 참조하십시오. 또한 Administration Server의 Global Settings 탭에 있는 마스터 에이전트 페이지 및 Server Manager의 Server Status 탭에 있는 하위 에이전트 페이지에 대해서는 온라인 도움말을 참조하십시오.

◆ ◆ ◆ 4 장

4 사용자 및 그룹 관리

이 장에서 Proxy Server에 액세스할 수 있는 사용자 및 그룹을 추가, 삭제, 수정 및 관리하는 방법에 대해 설명합니다.

이 장은 다음 내용으로 구성되어 있습니다.

- 43 페이지 “사용자 및 그룹에 대한 정보 액세스”
- 44 페이지 “디렉토리 서비스 설명”
- 45 페이지 “디렉토리 서비스 구성”
- 47 페이지 “사용자 생성”
- 51 페이지 “사용자 관리”
- 55 페이지 “그룹 생성”
- 60 페이지 “그룹 관리”
- 66 페이지 “조직 단위 만들기”
- 66 페이지 “조직 단위 관리”

사용자 및 그룹에 대한 정보 액세스

Administration Server에서 사용자 계정, 그룹 목록, 액세스 권한, 조직 단위, 기타 사용자 및 그룹 특정 정보에 대한 응용 프로그램 데이터에 액세스할 수 있습니다.

사용자 및 그룹 정보는 텍스트 형식으로 보통 파일에 저장되거나 Sun Java System Directory Server와 같이 LDAP(Lightweight Directory Access Protocol)를 지원하는 디렉토리 서버에 저장됩니다. LDAP는 개방형 디렉토리 액세스 프로토콜로 TCP/IP(Transmission Control Protocol/Internet Protocol)에서 실행되며 전역적 규모의 수백만 항목을 수용하도록 확장될 수 있습니다.

디렉토리 서비스 설명

디렉토리 서비스를 통해 단일 소스에서 모든 사용자 정보를 관리할 수 있습니다. Proxy Server를 사용하여 세 가지 유형(LDAP, 키 파일 및 다이제스트 파일)의 디렉토리 서비스를 구성할 수 있습니다.

다른 디렉토리 서비스가 구성되지 않은 경우 디렉토리 서비스를 새로 만들면 해당 유형에 상관 없이 `default` 값으로 설정됩니다. 디렉토리 서비스를 만들면 *server-root* `/userdb/dbswitch.conf` 파일이 디렉토리 서비스 세부 정보를 포함하여 업데이트됩니다.

이 절에서는 LDAP, 키 파일 및 다이제스트 파일에 대한 디렉토리 서비스에 대해 설명합니다.

LDAP 디렉토리 서비스

LDAP 디렉토리 서비스에서 사용자 및 그룹 정보는 LDAP 기반 디렉토리 서버에 저장됩니다.

LDAP 서비스가 기본 서비스인 경우 `dbswitch.conf` 파일이 아래의 예와 같이 업데이트됩니다.

```
directory default
ldap://test22.india.sun.com:589/dc%3Dindia%2Cdc%3Dsun%2Cdc%3Dcomdefault:binddn
cn=Directory Managerdefault:encoded bindpw YWRtaW5hZG1pbg==
```

LDAP 서비스가 기본 서비스가 아닌 경우 `dbswitch.conf` 파일이 아래의 예와 같이 업데이트됩니다.

```
directory ldap
ldap://test22.india.sun.com:589/dc%3Dindia%2Cdc%3Dsun%2Cdc%3Dcomldap:binddn
cn=Directory Managerldap:encoded bindpw YWRtaW5hZG1pbg==
```

키 파일 디렉토리 서비스

키 파일은 해시 형식의 사용자 비밀번호와 사용자가 속한 그룹 목록이 포함된 텍스트 파일입니다. 키 파일 형식은 HTTP Basic 인증을 사용할 때만 사용할 수 있습니다. 이 인증 방법에 대한 자세한 내용은 154 페이지 “사용자 및 그룹 지정”을 참조하십시오.

키 파일 기반 데이터베이스를 만들면 `dbswitch.conf` 파일이 다음 예와 같이 업데이트됩니다.

```
directory keyfile filekeyfile:syntax keyfilekeyfile:keyfile
D:\\test22\\keyfile\\keyfiledb
```

다이제스트 파일 디렉토리 서비스

다이제스트 파일은 암호화된 사용자 이름 및 비밀번호를 기반으로 사용자 및 그룹 정보를 저장합니다.

다이제스트 파일 형식은 HTTP Digest 인증뿐만 아니라 Basic 인증도 지원하기 때문에 두 가지 인증 방법 모두에 대해 사용할수 있습니다. 이 방법에 대한 자세한 내용은 154 페이지 "사용자 및 그룹 지정"을 참조하십시오.

다이제스트 기반 데이터베이스를 만들면 `dbswitch.conf` 파일이 다음 예와 같이 업데이트됩니다.

```
directory digest filedigest:syntax digestdigest:digestfile
D:\\test22\\digest\\digestdb
```

주 – 분산 관리를 구성하려면 기본 디렉토리 서비스가 LDAP 기반 디렉토리 서비스여야 합니다.

디렉토리 서비스 구성

Administration Server의 Global Settings 탭에서 디렉토리 서비스를 만들고 구성합니다. 그런 다음 Administration Server의 Users and Groups 탭에서 사용자, 그룹 및 조직 단위를 만들고 관리합니다.

이 절에서는 디렉토리 서비스를 만들고 편집하는 방법에 대해 설명합니다.

▼ 디렉토리 서비스를 만드는 방법

1. **Administration Server에 액세스하고 Global Settings 탭을 누릅니다.**
2. **Configure Directory Service 링크를 누릅니다.**
3. **Create New Service of Type 드롭다운 목록에서 만들려는 디렉토리 서비스 유형을 선택하고 New를 누릅니다.**

   해당 디렉토리 서비스의 구성 페이지가 나타납니다.
4. **구성 정보를 입력한 다음 Save Changes를 누릅니다.**

   특정 필드에 대한 자세한 내용은 온라인 도움말을 참조하십시오.

주 – 다른 디렉토리 서비스가 구성되지 않은 경우 디렉토리 서비스를 새로 만들면 해당 유형에 상관 없이 `default` 값으로 설정됩니다.

▼ 디렉토리 서비스 편집 방법

1. **Administration Server에 액세스하고 Global Settings 탭을 누릅니다.**
2. **Configure Directory Service 링크를 누릅니다.**
3. **편집할 디렉토리 서비스에 대한 링크를 누릅니다.**
4. **원하는 사항을 변경하고 Save Changes를 누릅니다.**
   특정 필드에 대한 자세한 내용은 온라인 도움말을 참조하십시오.

DN(Distinguished Name) 이 해

Administration Server의 Users and Groups 탭은 사용자, 그룹 또는 조직 단위를 만들거나 수정할 때 사용합니다. 사용자는 회사 고용인 등의 LDAP 데이터베이스에 있는 개인입니다. 그룹은 공통 속성을 공유하는 둘 이상의 사용자입니다. 조직 단위는 회사 내의 하위 부서로, `organizationalUnit` 객체 클래스를 사용합니다. 사용자, 그룹 및 조직 단위는 이 장의 뒷 부분에서 자세히 설명합니다.

기업의 각 사용자와 그룹은 DN(고유 이름) 속성으로 구분됩니다. DN 속성은 연결된 사용자, 그룹 또는 객체에 대한 구분 정보가 있는 문자열입니다. 사용자 또는 그룹 디렉토리 항목을 변경할 때마다 DN을 사용합니다. 예를 들어, 디렉토리 항목을 만들거나 수정하고 액세스 제어 구성, 전자 메일이나 게시와 같이 응용 프로그램용 사용자 계정을 구성할 때 항상 DN 정보를 입력해야 합니다. Proxy Server의 Users and Groups 인터페이스는 DN을 만들거나 수정하는 데 사용됩니다.

다음의 예는 SunMicrosystems 직원의 일반적 DN입니다.

```
uid=doe,e=doe@sun.com,cn=John Doe,o=Sun Microsystems Inc.,c=US
```

이 예에서 사용된 약어의 의미는 다음과 같습니다.

- `uid`는 사용자 아이디입니다.
- `e`는 전자 메일 주소입니다.
- `cn`은 사용자의 공통 이름입니다.
- `o`는 조직입니다.
- `c`는 국가입니다.

DN은 다양한 이름-값 쌍을 포함할 수 있으며 LDAP를 지원하는 디렉토리의 인증서 주제와 항목을 식별하는 데 사용됩니다.

LDIF 사용

현재 디렉토리가 없거나 기존 디렉토리에 새 하위 트리를 추가하려는 경우 디렉토리 서버의 LDIF(Lightweight Directory Interchange Format) 가져오기 기능을 사용할 수 있습니다. 이 기능은 LDIF가 포함된 파일을 받아서 LDIF 항목에서 디렉토리를 구축하거나 새 하위 트리를 만듭니다. 또한 디렉토리 서버의 LDIF 내보내기 기능을 사용하여 현재 디렉토리를 LDIF로 내보낼 수 있습니다. 이 기능은 디렉토리에 대한 LDIF 형식 파일을 만듭니다. 사용 가능한 경우 `ldapmodify` 명령줄 유틸리티에 적절한 LDIF 업데이트문을 사용하여 항목을 추가하거나 편집할 수 있습니다.

LDIF를 사용하여 데이터베이스에 항목을 추가하려면 먼저 LDIF 파일에서 항목을 정의한 다음 디렉토리 서버에서 LDIF 파일을 가져옵니다.

사용자 생성

사용자 항목을 만들거나 수정하려면 Administration Server의 Users and Groups 탭을 사용합니다. 사용자 항목에는 데이터베이스의 개인 또는 객체에 대한 정보가 포함됩니다.

주 – 자원에 대한 사용자의 무단 액세스를 차단하여 서버 보안을 유지해야 합니다. Proxy Server는 ACL 기반 인증 및 인증 모델을 사용합니다. ACL 기반 보안에 대한 자세한 내용은 8 장, “서버 액세스 제어”를 참조하십시오. 보안 정보에 대한 자세한 내용은 5 장, “인증서 및 키 사용”을 참조하십시오.

이 절에서는 LDAP 기반 인증 데이터베이스, 키 파일 인증 데이터베이스 및 다이제스트 파일 인증 데이터베이스에 사용자를 만드는 방법에 대해 설명합니다.

LDAP 기반 인증 데이터베이스에 사용자 만들기

LDAP 기반 디렉토리 서비스에 사용자 항목을 추가하는 경우 배후의 LDAP 기반 디렉토리 서버의 서비스가 사용자를 인증하고 권한을 부여하는 데 사용됩니다. 이 절에서는 LDAP 기반 인증 데이터베이스를 사용할 때 고려해야 할 지침을 나열하고 Proxy Server Administration Server를 통해 사용자를 추가하는 방법에 대해 설명합니다.

LDAP 기반 사용자 항목 생성에 대한 지침

Proxy Server 관리 콘솔을 사용하여 LDAP 기반 디렉토리 서비스에 새 사용자 항목을 만드는 경우 다음 지침을 고려하십시오.

- 이름 및 성을 입력하면 사용자의 전체 이름과 사용자 아이디가 자동으로 완료됩니다. 사용자 아이디는 사용자 이름의 첫 자와 사용자 성을 조합하여 만듭니다. 예를 들어, 사용자의 이름이 Billie Holiday인 경우 사용자 아이디는 자동으로 `bholiday`가 됩니다. 원하는 경우 이 사용자 아이디는 원하는 아이디로 바꿀 수 있습니다.

- 사용자 아이디는 반드시 고유해야 합니다. Administration Server는 검색 기반(기본 DN)에서 시작하여 전체 디렉토리에서 해당 사용자 아이디가 사용되는지 검색하여 해당 사용자 아이디가 고유한지 확인합니다. 그러나 사용자를 만들 때 디렉토리 서버 `ldapmodify` 명령줄 유틸리티를 사용하는 경우(사용 가능한 경우) 고유한 사용자 아이디가 보장되지 않습니다. 디렉토리의 사용자 아이디가 중복되는 경우 관련 사용자는 디렉토리에 대해 인증되지 않습니다.
- 기본 DN은 디렉토리 조회가 기본적으로 수행되고 디렉토리 트리에서 모든 Proxy Server Administration Server 항목이 배치되는 고유 이름을 지정합니다. DN(고유 이름)은 디렉토리 서버에 있는 항목 이름을 문자열로 나타낸 것입니다.
- 최소한 새 사용자 항목을 만들 때 반드시 다음 사용자 정보를 지정해야 합니다.
  - 성
  - 전체 이름
  - 사용자 아이디

  디렉토리에 대해 조직 단위가 정의된 경우 Administration Server의 Create User 페이지에 있는 Add New User To 목록을 사용하여 새 사용자를 배치할 위치를 지정할 수 있습니다. 기본 위치는 디렉토리의 기본 DN 또는 루트 지점입니다.

디렉토리 서버 사용자 항목

디렉토리 서버 사용자 항목에 대해 다음 정보를 참조하십시오.

- 사용자 항목은 `inetOrgPerson`, `organizationalPerson` 및 `person` 객체 클래스를 사용합니다.
- 기본적으로 사용자의 고유 이름 형식은 다음과 같습니다.

  `cn=`*full name* `,ou=`*organization*`,...,o=`*base organization*`,c=` *country*

  예를 들어, Billie Holiday에 대한 사용자 항목이 조직 단위 Marketing 안에 만들어졌으며 디렉토리의 기본 DN이 `o=Ace Industry`, `c=US`인 경우 DN은 다음과 같습니다.

  ```
  cn=Billie Holiday,ou=Marketing,o= Ace Industry,c=US
  ```

  이 형식은 사용자 아이디(uid) 기반 고유 이름으로 변경될 수 있습니다.
- 사용자 양식 필드의 값은 LDAP 속성으로 저장됩니다.

  다음 표에서는 Proxy Server 인터페이스에서 새 사용자를 만들거나 편집할 때 표시되는 필드와 해당 LDAP 속성을 나열합니다.

표 4–1 LDAP 속성 - 사용자 항목 만들기 또는 편집

사용자 필드	LDAP 속성
이름	`givenName`
성	`sn`

표 4–1 LDAP 속성 - 사용자 항목 만들기 또는 편집 *(계속)*

사용자 필드	LDAP 속성
전체 이름	cn
사용자 아이디	uid
비밀번호	userPassword
전자 메일 주소	mail
제목	title
전화 번호	telephoneNumber

LDAP 기반 사용자 항목 만들기

사용자 항목을 만들려면 47 페이지 "LDAP 기반 사용자 항목 생성에 대한 지침"의 지침을 읽은 후 다음 절차를 수행합니다.

▼ LDAP 기반 인증 데이터베이스에 사용자를 만드는 방법

1. **Administration Server에 액세스하고 Users and Groups 탭을 선택합니다.**
2. **Create User 링크를 누릅니다.**
3. **드롭다운 목록에서 LDAP 디렉토리 서비스를 선택하고 Select를 누릅니다.**
4. **표시되는 페이지에 정보를 입력합니다.**
   특정 필드에 대한 자세한 내용은 온라인 도움말을 참조하십시오.

   48 페이지 "디렉토리 서버 사용자 항목"을 참조하십시오.
5. **Create를 눌러 사용자 항목을 만들거나 Create and Edit를 눌러 사용자 항목을 만든 다음 해당 항목의 편집 페이지로 이동합니다.**

키 파일 인증 데이터베이스에 사용자 생성

키 파일은 해시 형식의 사용자 비밀번호와 사용자가 속한 그룹 목록이 포함된 텍스트 파일입니다.

▼ 키 파일 인증 데이터베이스에 사용자를 만드는 방법

1. **Administration Server에 액세스하고 Users and Groups 탭을 선택합니다.**
2. **Create User 링크를 누릅니다.**
3. **드롭다운 목록에서 키 파일 기반 디렉토리 서비스를 선택하고 Select를 누릅니다.**
4. **표시되는 페이지에서 정보를 입력한 다음 Create User를 누릅니다.**
   특정 필드에 대한 자세한 내용은 온라인 도움말을 참조하십시오.

다이제스트 파일 인증 데이터베이스에 사용자 만들기

다이제스트 파일 인증 데이터베이스는 사용자 및 그룹 정보를 암호화된 형식으로 저장합니다.

▼ 다이제스트 파일 인증 데이터베이스에 사용자를 만드는 방법

1. **Administration Server에 액세스하고 Users and Groups 탭을 선택합니다.**
2. **Create User 링크를 누릅니다.**
3. **드롭다운 목록에서 다이제스트 파일 기반 디렉토리 서비스를 선택하고 Select를 누릅니다.**
4. **표시되는 페이지에서 정보를 입력한 다음 Create User를 누릅니다.**
   특정 필드에 대한 자세한 내용은 온라인 도움말을 참조하십시오.

주 – Proxy Server ACL 사용자 인터페이스를 사용하여 Digest 인증을 사용하는 ACL을 만드는 경우 동일한 영역 문자열을 지정해야 합니다. 자세한 내용은 149 페이지 “액세스 제어 설정”을 참조하십시오.

사용자 관리

Administration Server Users and Groups 탭의 Manage Users 페이지에서 사용자 속성을 편집할 수 있습니다. 이 페이지에서 사용자 항목을 검색, 변경, 이름 변경 및 삭제할 수 있습니다.

이 절에서는 다음 항목에 대해 설명합니다.

- 51 페이지 "사용자 정보 찾기"
- 53 페이지 "사용자 정보 편집"
- 54 페이지 "사용자 비밀번호 관리"
- 54 페이지 "사용자 이름 변경"
- 55 페이지 "사용자 제거"

사용자 정보 찾기

사용자 항목을 편집하려면 반드시 항목을 찾아 표시해야 합니다. LDAP 기반 디렉토리 서비스의 경우 편집하려는 항목에 대한 기술적인 값을 입력할 수 있습니다.

다음 정보를 제공할 수 있습니다.

- 이름. 이름의 전체 또는 부분을 입력합니다. 검색 문자열과 일치되는 모든 항목이 검색됩니다. 해당 항목을 찾을 수 없는 경우 검색 문자열을 포함하는 모든 항목이 검색됩니다. 해당 항목을 찾을 수 없는 경우 검색 문자열과 소리가 유사한 모든 항목이 검색됩니다.
- 사용자 아이디. 사용자 아이디를 부분적으로 입력하면 문자열을 포함하는 모든 항목이 검색됩니다.
- 전화번호. 번호를 부분적으로 입력하면 검색 번호로 끝나는 전화번호를 포함하는 모든 항목이 검색됩니다.
- 전자 메일 주소. @ 기호를 포함하는 모든 검색 문자열은 전자 메일 주소인 것으로 가정합니다. 정확한 일치가 검색되지 않는 경우 검색은 검색 문자열로 시작하는 모든 전자 메일 주소를 찾습니다.
- LDAP 검색 필터. 등호(=)가 포함된 문자열은 검색 필터로 간주됩니다.
- 디렉토리에 있는 모든 항목을 보려면 별표(*)를 사용합니다. 필드에 아무런 값을 입력하지 않아도 동일한 결과를 얻을 수 있습니다.

사용자 정의 검색 쿼리 만들기

LDAP 서비스의 경우 Find All Users Whose 섹션에서 사용자 정의 검색 필터를 만들 수 있습니다. 이 필드를 사용하면 Find User 필드의 검색 범위를 좁힐 수 있습니다.

왼쪽의 드롭다운 목록에서 검색 기준으로 사용할 속성을 지정합니다. 다음 표에는 사용 가능한 검색 속성 옵션이 정리되어 있습니다.

표 4–2 검색 속성 옵션

옵션	검색 대상
Full name	각 항목의 전체 이름
Last name	각 항목의 성
User ID	각 항목의 사용자 아이디
Phone number	각 항목의 전화 번호
E-mail address	각 항목의 전자 메일 주소

가운데 드롭다운 목록에서 수행할 검색의 유형을 지정합니다. 다음 표에는 사용 가능한 검색 유형 옵션이 정리되어 있습니다.

표 4–3 검색 유형 옵션

옵션	설명
Contains	하위 문자열 검색이 수행되도록 합니다. 지정한 검색 문자열을 포함하는 속성 값 항목이 반환됩니다. 예를 들어, 사용자의 이름에 "Dylan" 단어가 포함되어 있음을 알고 있는 경우 이 옵션에 검색 문자열 "Dylan"을 사용하여 사용자 항목을 찾을 수 있습니다.
Is	정확하게 일치하는 항목을 검색합니다(일치 검색 지정). 사용자 속성의 값을 정확히 아는 경우 이 옵션을 사용합니다. 예를 들어, 사용자 이름의 정확한 철자를 아는 경우입니다.
Isn't	검색 문자열과 정확히 일치하지 않는 속성값의 모든 항목을 검색합니다. 디렉토리에서 이름이 "John Smith"가 아닌 모든 사용자를 찾을 때 이 옵션을 사용합니다.그러나 이 옵션을 사용하면 지나치게 많은 수의 항목이 검색될 수 있습니다.
Sounds like	근사치 또는 발음에 의한 검색이 수행됩니다. 속성의 값은 알지만 철자가 확실하지 않은 경우 이 옵션을 사용합니다. 예를 들어, 사용자의 이름 철자가 "Sarret", "Sarette" 또는 "Sarett" 인지 확실하지 않은 경우입니다.
Starts with	하위 문자열 검색이 수행되도록 합니다. 지정된 검색 문자열로 시작하는 속성 값을 갖는 모든 항목을 검색합니다. 예를 들어, 사용자의 이름이 "Miles"로 시작되지만 나머지 이름은 알지 못하는 경우입니다.
Ends with	하위 문자열 검색이 수행되도록 합니다. 지정된 검색 문자열로 끝나는 속성 값을 갖는 모든 항목을 반환합니다. 예를 들어, 사용자의 이름이 "Dimaggio"로 끝나지만 나머지 이름은 알지 못하는 경우입니다.

오른쪽 텍스트 필드는 검색 문자열을 입력하는 데 사용됩니다. Look Within 필드에 지정된 디렉토리에 포함된 모든 사용자 항목을 표시하려면 별표(*)를 입력하거나 이 필드를 공란으로 남겨둡니다.

▼ 사용자 정보를 찾는 방법

1. **Administration Server에 액세스하고 Users and Groups 탭을 선택합니다.**
2. **Manage Users 링크를 누릅니다.**
3. **드롭다운 목록에서 디렉토리 서비스를 선택하고 Select를 누릅니다.**
   키 파일 또는 다이제스트 파일 디렉토리 서비스의 경우 사용자 목록이 표시됩니다. LDAP 기반 디렉토리 서비스의 경우 검색 필드가 표시됩니다.
4. **사용자 정보 찾기**
   키 파일 또는 다이제스트 파일 디렉토리 서비스의 경우 편집 페이지를 표시할 사용자의 링크를 누르고 변경합니다. 특정 필드에 대한 자세한 내용은 온라인 도움말을 참조하십시오.

   LDAP 기반 디렉토리 서비스의 경우 다음을 수행합니다.

   a. **Find User 필드에 편집하려는 항목에 대한 기술적인 값을 입력합니다.**
      다른 방법으로 Find All Users Whose 섹션의 드롭다운 메뉴를 사용하여 검색 범위를 좁힐 수 있습니다. 자세한 내용은 51 페이지 “사용자 정의 검색 쿼리 만들기”를 참조하십시오.

   b. **Look Within 필드에서 검색하려는 항목의 조직 단위를 선택합니다.**
      기본값은 디렉토리의 루트 지점(최상단 항목)입니다.

   c. **Format 필드에서 출력을 화면에 표시하거나 프린터로 인쇄할 수 있도록 포맷할 것인지 지정합니다.**

   d. **이 프로세스의 아무 단계에서나 Find 버튼을 누릅니다.**
      검색 기준과 일치하는 모든 사용자가 표시됩니다.

   e. **표시할 항목에 대한 링크를 누릅니다.**

사용자 정보 편집

▼ 사용자 항목 편집 방법

1. **Administration Server에 액세스하고 Users and Groups 탭을 선택합니다.**
2. **Manage Users 링크를 누릅니다.**

3 51 페이지 "사용자 정보 찾기"에서 설명한 것과 같이 사용자 항목을 표시합니다.

4 원하는 사항을 변경합니다.
특정 필드에 대한 자세한 내용은 온라인 도움말을 참조하십시오.

주 – 사용자 편집 페이지에서 표시되지 않는 속성 값을 변경하려면 디렉토리 서버 `ldapmodify` 명령줄 유틸리티(사용 가능한 경우)를 사용합니다.

사용자 아이디 변경에 대한 자세한 내용은 54 페이지 "사용자 이름 변경"을 참조하십시오.

사용자 비밀번호 관리

다음 절차에서는 사용자 비밀번호를 변경하고 만드는 방법에 대해 설명합니다.

▼ 사용자 비밀번호 변경 또는 만드는 방법

1 Administration Server에 액세스하고 Users and Groups 탭을 선택합니다.

2 Manage Users 링크를 누릅니다.

3 51 페이지 "사용자 정보 찾기"에서 설명한 것과 같이 사용자 항목을 표시합니다.

4 원하는 사항을 변경합니다.
특정 필드에 대한 자세한 내용은 온라인 도움말을 참조하십시오.

LDAP 데이터베이스의 경우 Manage Users 페이지에서 액세스하여 사용자 비밀번호 정보를 편집하는 데 사용하는 페이지에서 Disable Password 버튼을 눌러 사용자의 비밀번호를 비활성화할 수도 있습니다. 이렇게 하면 사용자의 디렉토리 항목을 삭제할 필요 없이 서버에 로그인할 수 없도록 방지합니다. 새 비밀번호를 입력하면 사용자가 다시 액세스할 수 있습니다.

사용자 이름 변경

LDAP 데이터베이스의 경우 이름 변경 기능은 사용자 아이디만 변경합니다. 다른 모든 필드는 그대로 유지됩니다. 이름 변경 기능을 사용하여 항목을 하나의 조직 단위에서 다른 단위로 이동할 수는 없습니다.

▼ 사용자 항목 이름 변경 방법

1. **Administration Server에 액세스하고 Users and Groups 탭을 선택합니다.**
2. **Manage Users 링크를 누릅니다.**
3. **51 페이지 "사용자 정보 찾기"에서 설명한 것과 같이 사용자 항목을 표시합니다.**
4. **사용자 편집 페이지의 Rename User 버튼을 누릅니다.**
5. **표시되는 페이지에서 사용자 아이디를 입력하고 Save Changes를 누릅니다.**

주 – Administration Server는 `keepOldValueWhenRenaming` 매개 변수를 `false`(기본값)로 설정하면 항목 이름을 변경할 때 이전 값을 보존하지 않도록 지정할 수 있습니다. 이 매개 변수는 다음 파일에 있습니다.

server-root `/proxy-admserv/config/dsgw-orgperson.conf`

사용자 제거

▼ 사용자 항목 제거 방법

1. **Administration Server에 액세스하고 Users and Groups 탭을 선택합니다.**
2. **Manage Users 링크를 누릅니다.**
3. **51 페이지 "사용자 정보 찾기"에서 설명한 것과 같이 사용자 항목을 표시합니다.**
4. **적절한 버튼을 누릅니다.**
   - LDAP 서버의 경우 Delete User를 누릅니다.
   - 키 파일 및 다이제스트 파일 데이터베이스의 경우 Remove User를 누릅니다.

그룹 생성

그룹은 LDAP 데이터베이스에 있는 일련의 객체를 기술하는 객체입니다. Sun Java System 서버 그룹은 공통 속성을 공유하는 사용자로 구성됩니다. 예를 들어, 일련의 객체는 회사의 마케팅 부서에서 일하는 다수의 고용인일 수 있습니다. 이들 고용인은 Marketing이라는 이름의 그룹에 속할 수 있습니다.

LDAP 서버의 경우 정적 및 동적의 두 가지 방법으로 그룹 구성원을 정의합니다. 정적 그룹은 구성원 개체를 명시적으로 열거합니다. 정적 그룹은 공통 이름(CN)이며

uniqueMembers 또는 memberURLs 또는 memberCertDescriptions를 포함합니다. 정적 그룹의 경우 구성원은 cn=groupname 속성을 제외한 공통 속성을 공유하지 않습니다.

동적 그룹을 사용하면 LDAP URL을 사용하여 그룹 구성원에만 적용되는 일련의 규칙을 정의할 수 있습니다. 동적 그룹의 경우 구성원은 공통 속성 또는 memberURL 필터에 정의된 일련의 속성을 공유합니다. 예를 들어, 이미 LDAP 데이터베이스의 ou=Sales,o=Airius.com 에 있는 Sales의 모든 직원이 포함된 그룹이 필요한 경우 다음 구성원 URL로 동적 그룹을 정의할 수 있습니다.

```
ldap:///ou=Sales,o=sun??sub?(uid=*)
```

이 그룹에는 ou=Sales,o=sun 지점 아래의 트리에 있는 uid 속성을 가진 모든 객체가 포함됩니다.

정적 및 동적 그룹의 경우 memberCertDescription을 사용하면 구성원이 인증서에 있는 공통 속성을 공유할 수 있습니다. 이러한 공통 속성 공유는 ACL이 SSL 메소드를 사용하는 경우에만 적용됩니다.

새 그룹을 만든 후에는 사용자(구성원)를 해당 그룹에 추가할 수 있습니다.

이 절은 다음 내용으로 구성되어 있습니다.

- 56 페이지 “정적 그룹 정보”
- 57 페이지 “동적 그룹 정보”

정적 그룹 정보

LDAP 서비스의 경우 Administration Server를 사용하면 사용자 수에 상관없이 DN에서 동일한 그룹 속성을 지정하여 정적 그룹을 만들 수 있습니다. 정적 그룹은 그룹에 대해 사용자를 추가하거나 제거하지 않는 한 변경되지 않습니다.

정적 그룹 생성을 위한 지침

Administration Server 인터페이스를 사용하여 새 정적 그룹을 만들 때 다음 지침을 고려하십시오.

- 정적 그룹에는 다른 정적 또는 동적 그룹이 포함될 수 있습니다.
- 디렉토리에 대해 조직 단위가 정의된 경우 Administration Server 인터페이스에서 Create Group 페이지의 Add New Group To 목록을 사용하여 새 그룹을 배치할 위치를 지정할 수 있습니다. 기본 위치는 디렉토리의 루트 지점인 최상위 항목입니다.
- 그룹 편집에 대한 자세한 내용은 62 페이지 “그룹 항목 편집”을 참조하십시오.

▼ 정적 그룹을 만드는 방법

1. **Administration Server에 액세스하고 Users and Groups 탭을 선택합니다.**
2. **Create Group 링크를 누릅니다.**
3. **Type of Group 드롭다운 목록에서 New Group을 선택한 다음 Go를 누릅니다.**
4. **Create Group 페이지에 정보를 입력합니다.**
   특정 필드에 대한 자세한 내용은 온라인 도움말을 참조하십시오.
5. **Create를 눌러 그룹을 만들거나 Create and Edit를 눌러 그룹을 만들고 해당 그룹의 편집 페이지를 표시합니다.**

동적 그룹 정보

LDAP 서비스의 경우 Proxy Server를 사용하면 그룹 사용자가 자동으로 임의의 속성에 기반하도록 하거나 일치하는 DN이 있는 특정 그룹에 ACL을 적용하려는 경우 동적 그룹을 만들 수 있습니다. 예를 들어, `department=marketing` 속성이 있는 DN이 자동으로 포함되도록 그룹을 만들 수 있습니다. `department=marketing` 검색 필터를 적용하면 `department=marketing` 속성이 있는 모든 DN을 포함하는 그룹이 검색됩니다. 그 후, 이 필터에 기반하여 검색 결과에서 동적 그룹을 정의할 수 있습니다. 따라서 결과의 동적 그룹에 대한 ACL을 정의할 수 있습니다.

동적 그룹의 구현 방법

Proxy Server는 LDAP 서버 스키마에서 `objectclass=groupOfURLs`로 동적 그룹을 구현합니다. `groupOfURLs` 클래스는 0개 이상의 `memberURL` 속성을 포함할 수 있으며 각 속성은 디렉토리에 있는 일련의 객체를 기술하는 LDAP URL입니다. 그룹의 구성원은 이 세트의 조합이 됩니다. 예를 들어 다음 그룹은 하나의 구성원 URL만 포함합니다.

```
ldap:///o=mcom.com??sub?(department=marketing)
```

이 예는 부서가 `marketing`인 `o=mcom.com` 아래의 모든 객체로 구성되는 세트를 설명합니다. LDAP URL은 검색 기반 DN, 범위 및 필터를 포함하지만 호스트 이름과 포트는 포함하지 않습니다. 따라서 동일한 LDAP 서버에 있는 객체만 참조할 수 있습니다. 범위는 모두 지원됩니다. LDAP URL에 대한 자세한 내용은 58 페이지 “동적 그룹 생성을 위한 지침”을 참조하십시오.

DN은 자동으로 포함되므로 직접 개인을 그룹에 추가할 필요가 없습니다. ACL 검증을 위하여 그룹 조회가 필요할 때마다 Proxy Server가 LDAP 서버 검색을 수행하므로 그룹은 동적으로 변경됩니다. ACL 파일에서 사용된 사용자 및 그룹 이름은 LDAP 데이터베이스에 있는 객체의 `cn` 속성에 대응됩니다.

주 – Proxy Server는 ACL의 그룹 이름으로 `cn` 속성을 사용합니다.

ACL에서 LDAP 데이터베이스로의 매핑은 `dbswitch.conf` 파일(실제 LDAP 데이터베이스 URL로 ACL 데이터베이스 이름과 연결) 및 ACL 파일(ACL에 사용할 데이터베이스 정의) 모두에 정의됩니다. 예를 들어, `staff`라는 이름의 그룹 구성원에게 기본 액세스 권한을 부여하는 경우 ACL 코드는 객체 클래스가 `groupOf` *anything*이며 CN이 `staff`로 설정된 객체를 조회합니다. 객체는 구성원 ND를 직접 나열(정적 그룹용 `groupOfUniqueNames`와 동일)하거나 또는 LDAP URL을 지정(예: `groupOfURLs`)하여 그룹의 구성원을 정의합니다.

주 – 그룹은 정적 및 동적이 될 수 있습니다. 그룹 객체는 `objectclass=groupOfUniqueMembers` 및 `objectclass=groupOfURL s`를 모두 가질 수 있습니다. 따라서 `uniqueMember` 및 `memberURL` 속성이 모두 유효합니다. 그룹의 구성원은 정적 및 동적 구성원의 조합입니다.

서버 성능에 미치는 동적 그룹의 영향

동적 그룹을 사용하면 서버 성능에 영향을 미칩니다. 그룹 구성원을 시험하며 DN이 정적 그룹의 구성원이 아닌 경우 Proxy Server는 데이터베이스의 기본 DN에 있는 모든 동적 그룹을 확인합니다. Proxy Server는 기본 DN과 범위를 사용자의 DN에 비교하여 각 `memberURL`이 일치하는지 결정합니다. 그런 다음 Proxy Server는 사용자 DN을 기본 DN으로 사용하고 `memberURL`의 필터를 통해 기본 검색을 수행합니다. 이 절차에는 많은 수의 개별 검색이 관련될 수 있습니다.

동적 그룹 생성을 위한 지침

Administration Server 인터페이스를 사용하여 새 동적 그룹을 만드는 경우 다음의 지침을 고려하십시오.

- 동적 그룹에는 다른 그룹이 포함될 수 없습니다.
- LDAP URL은 이러한 매개 변수가 무시되므로 호스트 및 포트 정보를 생략하고 다음 형식을 사용합니다.

  `ldap:///` *base-dn*`?`*attributes*`?` *scope*`?(`*filter*`)`

`attributes`, `scope` 및 `(filter)` 매개 변수는 URL에서의 위치에 따라 구분됩니다. 속성을 지정하지 않는 경우에도 해당 필드를 구분하는 물음표(?)를 포함해야 합니다.

- 디렉토리에 대해 조직 단위가 정의된 경우 Administration Server 인터페이스에서 Create Group 페이지의 Add New Group To 목록을 사용하여 새 그룹을 배치할 위치를 지정할 수 있습니다. 기본 위치는 디렉토리의 루트 지점인 최상위 항목입니다.

그룹 편집에 대한 자세한 내용은 62 페이지 “그룹 항목 편집”을 참조하십시오.

다음 표에는 LDAP URL의 필수 매개 변수가 정리되어 있습니다.

표 4–4 LDAP URL의 필수 매개 변수

매개 변수 이름	설명
base_dn	검색 기반의 DN 또는 LDAP 디렉토리에서 검색이 수행되는 지점. 이 매개 변수는 때로 o=mcom.com과 같이 디렉토리의 접미사 또는 루트로 설정됩니다.
attributes	검색이 반환할 수 있는 속성 목록. 둘 이상을 지정하려면 쉼표를 사용하여 속성을 구분합니다(예: cn,mail,telephoneNumber). 속성을 지정하지 않으면 모든 속성이 반환됩니다. 동적 그룹 구성원 확인의 경우 이 매개 변수는 무시됩니다.
scope	이 매개 변수는 필수입니다. 검색의 범위로 다음 중 한 가지 값을 가집니다. ■ base는 URL에 지정된 고유 이름(base_dn)에 대한 정보만 검색합니다. ■ one은 URL에 지정된 고유 이름(base_dn)보다 한 수준 아래의 항목에 대한 정보를 검색합니다. 기본 항목은 이 범위에 포함되지 않습니다. ■ sub는 URL에 지정된 고유 이름(base_dn)보다 아래인 모든 수준의 항목에 대한 정보를 검색합니다. 기본 항목은 이 범위에 포함되지 않습니다.
(filter)	이 매개 변수는 필수입니다. 검색의 지정된 범위 안에 있는 항목에 적용되는 검색 필터. Administration Server 인터페이스를 사용하는 경우 반드시 이 속성을 지정해야 합니다. 괄호는 필수입니다.

동적 그룹 만들기

▼ 동적 그룹을 만드는 방법

1 Administration Server에 액세스하고 Users and Groups 탭을 선택합니다.

2 Create Group 링크를 누릅니다.

3 Type of Group 드롭다운 목록에서 Dynamic Group을 선택하고 Go를 누릅니다.

4 Create Group 페이지에 정보를 입력합니다.
특정 필드에 대한 자세한 내용은 온라인 도움말을 참조하십시오.

5 Create를 눌러 그룹을 만들거나 Create and Edit를 눌러 그룹을 만들고 해당 그룹의 편집 페이지를 표시합니다.

그룹 관리

LDAP 서비스의 경우 Administration Server의 Administration Server Users and Groups 탭에 있는 Manage Groups 페이지에서 그룹을 편집하고 그룹 구성원을 관리할 수 있습니다.

이 절에서는 다음 작업에 대해 설명합니다.

- 60 페이지 “그룹 항목 찾기”
- 62 페이지 “그룹 항목 편집”
- 62 페이지 “그룹 구성원 추가”
- 63 페이지 “그룹 구성원 목록에 그룹 추가”
- 63 페이지 “그룹 구성원 목록에서 항목 제거”
- 64 페이지 “소유자 관리”
- 64 페이지 “추가 참조 관리”
- 65 페이지 “그룹 이름 변경”
- 65 페이지 “그룹 제거”

그룹 항목 찾기

그룹 항목을 편집하려면 다음 절차에 설명된 대로 반드시 해당 항목을 찾아 표시해야 합니다.

▼ 그룹 항목을 찾는 방법

1 Administration Server에 액세스하고 Users and Groups 탭을 선택합니다.

2 Manage Groups 링크를 누릅니다.

3 Find Group 필드에 찾으려는 그룹 이름을 입력합니다.

다음을 입력할 수 있습니다.

- 디렉토리에 있는 그룹을 모두 보려면 별표(*)를 사용합니다. 필드에 아무런 값을 입력하지 않아도 동일한 결과를 얻을 수 있습니다.
- LDAP 검색 필터. 등호(=)가 있는 모든 문자열은 검색 필터로 간주됩니다.

  다른 방법으로 Find All Groups Whose 섹션을 사용하여 사용자 정의 검색 필터를 만들어 검색 결과를 좁힙니다. 자세한 내용은 61 페이지 “Find All Groups Whose”를 참조하십시오.
- 이름. 이름의 전체 또는 부분을 입력합니다. 검색 문자열과 일치되는 모든 항목이 검색됩니다. 해당 항목을 찾을 수 없는 경우 검색 문자열을 포함하는 모든 항목이 검색됩니다. 해당 항목을 찾을 수 없는 경우 검색 문자열과 소리가 유사한 모든 항목이 검색됩니다.

4 **Look Within 필드에서 검색하려는 항목의 조직 단위를 선택합니다.**
기본값은 디렉토리의 루트 지점(최상단 항목)입니다.

5 **Format 필드에서 출력을 화면에 표시하거나 프린터로 인쇄할 수 있도록 포맷할 것인지 지정합니다.**

6 **이 프로세스의 모든 단계에서 조건에 맞는 모든 그룹을 표시하려면 Find 버튼을 누릅니다.**

7 **표시할 항목에 대한 링크를 누릅니다.**

Find All Groups Whose

LDAP 서비스의 경우 Find All Groups Whose 섹션에서 사용자 정의 검색 필터를 만들 수 있습니다. 이 섹션의 필드를 사용하여 Find Group에서 반환되는 검색 결과를 더욱 좁힐 수 있습니다.

왼쪽의 드롭다운 목록에서 검색 기준으로 사용할 속성을 지정합니다. 다음 옵션을 사용할 수 있습니다.

- **Name.** 각 항목의 전체 이름이 일치하도록 검색합니다.
- **Description.** 각 그룹 항목의 설명이 일치하도록 검색합니다.

가운데 드롭다운 목록에서 수행할 검색의 유형을 지정합니다. 다음 옵션을 사용할 수 있습니다.

- **Contains.** 하위 문자열 검색이 수행되도록 합니다. 지정한 검색 문자열을 포함하는 속성 값 항목이 반환됩니다. 예를 들어, 그룹 이름에 "Administrator"라는 단어가 포함된 것을 알고 있는 경우 이 옵션에 검색 문자열 "Administrator"을 사용하여 해당 그룹 항목을 찾을 수 있습니다.
- **Is.** 정확히 일치되는 항목을 검색합니다. 그룹 속성의 값을 정확히 아는 경우 이 옵션을 사용합니다. 예를 들어, 그룹 이름의 정확한 철자를 아는 경우입니다.
- **Isn't.** 검색 문자열과 정확히 일치하지 않는 속성값의 모든 항목을 검색합니다. 디렉토리에서 이름에 "administrator"가 포함되지 않는 모든 그룹을 찾으려면 이 옵션을 사용합니다.그러나 이 옵션을 사용하면 지나치게 많은 수의 항목이 검색될 수 있습니다.
- **Sounds like.** 근사치 또는 발음에 의한 검색이 수행됩니다. 속성의 값은 알지만 철자가 확실하지 않은 경우 이 옵션을 사용합니다. 예를 들어, 그룹 이름의 철자가 "Sarret's list", "Sarette's list" 또는 "Sarett's list" 인지 확실하지 않은 경우입니다.
- **Starts with.** 하위 문자열 검색이 수행되도록 합니다. 지정된 검색 문자열로 시작하는 속성 값을 갖는 모든 항목을 검색합니다. 예를 들어, 그룹 이름이 "Product"로 시작되지만 나머지 이름은 알지 못하는 경우입니다.
- **Ends with.** 하위 문자열 검색이 수행되도록 합니다. 지정된 검색 문자열로 끝나는 속성 값을 갖는 모든 항목을 반환합니다. 예를 들어, 그룹 이름이 "development"로 끝나지만 나머지 이름은 알지 못하는 경우입니다.

오른쪽 텍스트 입력란에 검색 문자열을 입력합니다. 검색 위치 디렉토리에 포함된 모든 그룹 항목을 표시하려면 별표(*)를 입력하거나 이 필드를 공란으로 남겨둡니다.

그룹 항목 편집

▼ 그룹 항목 편집 방법

다음 절차는 LDAP 서비스에만 적용됩니다.

1. **Administration Server에 액세스하고 Users and Groups 탭을 선택합니다.**
2. **Manage Groups 링크를 누릅니다.**
3. **60 페이지 "그룹 항목 찾기"에 설명된 대로 편집할 그룹을 찾습니다.**
4. **원하는 사항을 변경합니다.**
   특정 필드 및 버튼에 대한 자세한 내용은 온라인 도움말을 참조하십시오.

주 – 그룹 편집 페이지에 표시되지 않는 속성 값을 변경해야 할 수 있습니다. 이런 경우 디렉토리 서버 `ldapmodify` 명령줄 유틸리티(사용 가능한 경우)를 사용하십시오.

그룹 구성원 추가

▼ 그룹에 구성원을 추가하는 방법

다음 절차는 LDAP 서비스에만 적용됩니다.

1. **Administration Server에 액세스하고 Users and Groups 탭을 선택합니다.**
2. **Manage Groups 링크를 누릅니다.**
3. **60 페이지 "그룹 항목 찾기"에 설명된 대로 관리할 그룹을 찾아 표시한 다음 Group Members 옆에 있는 Edit 버튼을 누릅니다.**
   표시되는 페이지에 기존 그룹 구성원이 나열됩니다. 검색 필드도 표시됩니다.
   - 구성원 목록에 사용자 항목을 추가하려면 Find 드롭다운 목록에서 Users를 선택해야 합니다.
   - 그룹에 그룹 항목을 추가하려면 Groups을 선택해야 합니다.
4. **Matching 텍스트 필드에 검색 문자열을 입력합니다. 다음 옵션에 대한 정보를 입력합니다.**

- 이름. 이름의 전체 또는 부분을 입력합니다. 검색 문자열과 일치하는 이름의 항목이 모두 검색됩니다. 해당 항목을 찾을 수 없는 경우 검색 문자열을 포함하는 모든 항목이 검색됩니다. 해당 항목을 찾을 수 없는 경우 검색 문자열과 소리가 유사한 모든 항목이 검색됩니다.
- 사용자 아이디. 사용자 아이디를 부분적으로 입력하면 문자열을 포함하는 모든 항목이 검색됩니다.
- 전화번호. 번호를 부분적으로 입력하면 검색 번호로 끝나는 전화번호를 포함하는 모든 항목이 검색됩니다.
- 전자 메일 주소. @ 기호를 포함하는 모든 검색 문자열은 전자 메일 주소인 것으로 가정합니다. 정확히 일치하는 검색 결과가 없는 경우 검색 문자열로 시작하는 모든 전자 메일 주소를 찾는 검색이 수행됩니다.
- 현재 디렉토리에 있는 모든 항목이나 그룹을 보려면 이 필드에 별표(*)를 입력하거나 이 필드를 공란으로 남겨둡니다.
- 모든 LDAP 검색 필터. 등호(=)가 있는 모든 문자열은 검색 필터로 간주됩니다.

5 **Add를 눌러 LDAP 데이터베이스에서 일치하는 모든 항목을 찾아 그룹에 추가합니다.**

6 **(선택 사항) 그룹에 추가하지 않으려는 항목이 검색된 경우 Remove From List 열에서 해당 확인란을 누릅니다. 또한 그룹에서 제거하려는 항목과 일치하는 검색 필터를 만든 후 Remove를 누르면 됩니다. 자세한 내용은 63 페이지 "그룹 구성원 목록에서 항목 제거"를 참조하십시오.**

7 **그룹 구성원 목록이 완료되었으면 Save Changes를 누릅니다. 항목이 그룹 구성원 목록에 추가됩니다.**

그룹 구성원 목록에 그룹 추가

LDAP 서비스의 경우 그룹의 구성원 목록에 개별 구성원 대신 그룹을 추가할 수 있습니다. 이렇게 하면 포함된 그룹에 속한 모든 사용자가 수신 그룹의 구성원이 됩니다. 예를 들어 Neil Armstrong이 Engineering Managers 그룹의 구성원이며 Engineering Managers 그룹을 Engineering Personnel 그룹의 구성원으로 추가하면 Neil Armstrong 또한 Engineering Personnel 그룹의 구성원이 됩니다.

그룹을 다른 그룹의 구성원 목록에 추가하려면 그룹이 사용자 항목인 것처럼 추가합니다. 자세한 내용은 62 페이지 "그룹 구성원 추가"를 참조하십시오.

그룹 구성원 목록에서 항목 제거

이 절차는 LDAP 서비스에만 적용됩니다.

▼ 그룹 구성원 목록에서 항목을 제거하는 방법

1 **Administration Server에 액세스하고 Users and Groups 탭을 선택합니다.**

2 **Manage Groups 링크를 누릅니다.**

3 **관리할 그룹을 찾습니다.**
자세한 내용은 60 페이지 "그룹 항목 찾기"를 참조하십시오. Group Members 옆에 있는 Edit 버튼을 누릅니다.

4 **제거할 구성원을 표시합니다.**
- 일부 구성원만 제거하려면 Remove From List 열에서 해당 확인란을 누릅니다.
- 공통 기준에 따라 구성원을 제거하려면 그룹에서 제거할 항목과 일치하는 검색 필터를 만든 다음 Remove를 누릅니다.

검색 필터 만들기에 대한 자세한 내용은 62 페이지 "그룹 구성원 추가"를 참조하십시오.

5 **Save Changes를 누릅니다.**
그룹 구성원 목록에서 해당 항목이 삭제됩니다.

소유자 관리

LDAP 서비스의 경우 그룹 소유자 목록은 그룹 구성원 목록과 같은 방식으로 관리됩니다.

자세한 내용을 제공하는 이 설명서의 항목 목록은 다음과 같습니다.

표 4–5 소유자 관리

수행 작업	참조
그룹에 소유자 추가	62 페이지 "그룹 구성원 추가"
소유자 목록에 그룹 추가	63 페이지 "그룹 구성원 목록에 그룹 추가"
소유자 목록에서 항목 제거	63 페이지 "그룹 구성원 목록에서 항목 제거"

추가 참조 관리

추가 참조는 현재 그룹과 관련되었을 수 있는 기타 디렉토리 항목에 대한 참조입니다. 이러한 참조를 통해 현재 그룹과 관련된 사용자 및 기타 그룹의 항목을 쉽게 찾을 수 있습니다. 그룹 구성원 목록을 관리하는 것과 마찬가지로 추가 참조를 관리할 수 있습니다.

자세한 내용을 제공하는 이 설명서의 항목 목록은 다음과 같습니다.

표 4–6 추가 참조 관리

수행 작업	참조
추가 참조에 사용자 추가	62 페이지 “그룹 구성원 추가”
추가 참조에 그룹 추가	63 페이지 “그룹 구성원 목록에 그룹 추가”
추가 참조에서 항목 제거	63 페이지 “그룹 구성원 목록에서 항목 제거”

그룹 이름 변경

이 절차는 LDAP 서비스에만 적용됩니다. 그룹 항목의 이름을 변경하면 그룹의 이름만 변경됩니다. 그룹 이름 변경 기능을 사용하여 항목을 하나의 조직 단위에서 다른 단위로 이동할 수는 없습니다. 예를 들어 회사에 다음과 같은 조직이 있는 것으로 가정합니다.

- Marketing 및 Product Management를 위한 조직 단위
- Marketing 조직 단위 아래의 Online Sales 그룹

이 예에서 그룹의 이름을 Online Sales에서 Internet Investments로 변경할 수 있으나 Marketing 조직 단위 아래에 있는 Online Sales가 Product Management 조직 단위 아래의 Online Sales로 되도록 항목의 이름을 변경할 수는 없습니다.

▼ 그룹 이름 변경 방법

1. **Administration Server에 액세스하고 Users and Groups 탭을 선택합니다.**
2. **Manage Groups 링크를 누르고 60 페이지 “그룹 항목 찾기”에 설명된 대로 관리할 그룹을 찾습니다.**
3. **Rename Group 버튼을 누릅니다.**
4. **표시되는 페이지에 새 그룹 이름을 지정하고 Save Changes를 누릅니다.**

그룹 제거

이 절차는 LDAP 서비스에만 적용됩니다.

▼ 그룹 제거 방법

1. **Administration Server에 액세스하고 Users and Groups 탭을 선택합니다.**
2. **Manage Groups 링크를 누릅니다.**
3. **60 페이지 “그룹 항목 찾기”에 설명된 대로 관리할 그룹을 찾고 Delete Group을 누릅니다.**

주 – 그룹의 개별 구성원은 제거되지 않습니다. 그룹 항목만 제거됩니다.

조직 단위 만들기

LDAP 서비스의 경우 조직 단위에는 여러 그룹이 포함될 수 있으며 보통 사업 단위, 부서 또는 기타 명확히 구분되는 엔티티를 나타냅니다. DN은 하나 이상의 조직 단위에 존재할 수 있습니다.

- 새 조직 단위는 `organizationalUnit` 객체 클래스를 사용하여 만들어집니다.
- 새 조직 단위용 고유 이름의 형식은 다음과 같습니다.

  `ou=`*new organization* `,ou=`*parent organization*`,...,o=` *base organization*`,c=`*country*

▼ 조직 단위를 만드는 방법

1. **Administration Server에 액세스하고 Users and Groups 탭을 선택합니다.**
2. **Create Organizational Unit 링크를 누릅니다.**
3. **정보를 입력하고 Create를 누릅니다.**

   특정 필드에 대한 자세한 내용은 온라인 도움말을 참조하십시오.

   예를 들어, Accounting이라는 이름의 새 조직을 West Coast라는 이름의 조직 단위 내에 만들고 기본 DN이 `o=Ace Industry, c=US`인 경우, 새 조직 단위의 DN은 다음과 같습니다.

   ```
   ou=Accounting,ou=West Coast,o=Ace Industry,c=US
   ```

조직 단위 관리

LDAP 서비스의 경우 조직 단위는 Administration Server Users and Groups 탭의 Manage Organizational Units 페이지에서 편집하고 관리합니다.

이 절은 다음 내용으로 구성되어 있습니다.

- 66 페이지 “조직 단위 찾기”
- 68 페이지 “조직 단위 속성 편집”
- 69 페이지 “조직 단위 이름 변경”
- 69 페이지 “조직 단위 제거”

조직 단위 찾기

이 절차는 LDAP 서비스에만 적용됩니다.

▼ 조직 단위를 검색하는 방법

1 **Administration Server에 액세스하고 Users and Groups 탭을 선택합니다.**

2 **Manage Organizational Units 링크를 누릅니다.**

3 **Find Organizational Unit 필드에 찾으려는 단위의 이름을 입력합니다.**
다음을 입력할 수 있습니다.

- 이름. 이름의 전체 또는 부분을 입력합니다. 검색 문자열과 일치되는 모든 항목이 검색됩니다. 해당 항목을 찾을 수 없는 경우 검색 문자열을 포함하는 모든 항목이 검색됩니다. 해당 항목을 찾을 수 없는 경우 검색 문자열과 소리가 유사한 모든 항목이 검색됩니다.
- 디렉토리에 있는 그룹을 모두 보려면 별표(*)를 사용합니다. 필드에 아무런 값을 입력하지 않아도 동일한 결과를 얻을 수 있습니다.
- 모든 LDAP 검색 필터. 등호(=)가 있는 모든 문자열은 검색 필터로 간주됩니다.

  다른 방법으로 Find All Units Whose 필드의 드롭다운 메뉴를 사용하여 검색 범위를 좁힐 수 있습니다. 자세한 내용은 67 페이지 “Find All Units Whose ”를 참조하십시오.

4 **Look Within 필드에서 검색하려는 항목의 조직 단위를 선택합니다.**
기본값은 디렉토리의 루트 지점(최상위 항목)입니다.

5 **Format 필드에서 출력을 화면에 표시하거나 프린터로 인쇄할 수 있도록 포맷할 것인지 지정합니다.**

6 **이 프로세스의 아무 단계에서나 Find 버튼을 누릅니다.**
검색 조건과 일치하는 조직 단위가 모두 표시됩니다.

7 **표시할 항목에 대한 링크를 누릅니다.**

Find All Units Whose

LDAP 서비스의 경우 Find All Units Whose 섹션에서 사용자 정의 검색 필터를 만들 수 있습니다. 이 섹션의 필드를 사용하여 Find Organizational Unit에서 반환되는 검색 결과를 더욱 좁힐 수 있습니다.

왼쪽의 드롭다운 목록에서 검색 기준으로 사용할 속성을 지정합니다. 다음 옵션을 사용할 수 있습니다.

- **Unit name.** 각 항목의 전체 이름이 일치하도록 검색합니다.
- **Description.** 각 조직 단위 항목의 설명이 일치하도록 검색합니다.

가운데 드롭다운 목록에서 수행할 검색의 유형을 지정합니다. 다음 옵션을 사용할 수 있습니다.

- **Contains.** 하위 문자열 검색이 수행되도록 합니다. 지정한 검색 문자열을 포함하는 속성 값 항목이 반환됩니다. 예를 들어, 조직 단위의 이름에 “Administrator” 단어가 포함되어 있음을 알고 있는 경우 이 옵션에 검색 문자열 “Administrator”를 사용하여 조직 단위 항목을 찾을 수 있습니다.
- **Is.** 정확히 일치되는 항목을 검색합니다. 조직 단위 속성의 값을 정확히 아는 경우 이 옵션을 사용합니다. 예를 들어, 조직 단위 이름의 정확한 철자를 아는 경우입니다.
- **Isn’t.** 검색 문자열과 정확히 일치하지 않는 속성값의 모든 항목을 검색합니다. 디렉토리에서 이름에 "administrator"가 포함되지 않는 모든 조직 단위를 찾으려면 이 옵션을 사용합니다. 그러나 이 옵션을 사용하면 지나치게 많은 수의 항목이 검색될 수 있습니다.
- **Sounds like.** 근사치 또는 발음에 의한 검색이 수행됩니다. 속성의 값은 알지만 철자가 확실하지 않은 경우 이 옵션을 사용합니다. 조직 단위 이름의 철자가 "Sarret’s list", "Sarette’s list" 또는 "Sarett’s list" 인지 확실하지 않은 경우입니다.
- **Starts with.** 하위 문자열 검색이 수행되도록 합니다. 지정된 검색 문자열로 시작하는 속성 값을 갖는 모든 항목을 검색합니다. 예를 들어, 조직 단위의 이름이 "Product"로 시작되지만 나머지 이름은 알지 못하는 경우입니다.
- **Ends with.** 하위 문자열 검색이 수행되도록 합니다. 지정된 검색 문자열로 끝나는 속성 값을 갖는 모든 항목을 반환합니다. 예를 들어, 조직 단위의 이름이 "development"로 끝나지만 나머지 이름은 알지 못하는 경우입니다.

오른쪽 텍스트 입력란에 검색 문자열을 입력합니다. 검색 위치 디렉토리에 포함된 모든 조직 단위 항목을 표시하려면 별표(*)를 입력하거나 이 필드를 공란으로 남겨둡니다.

조직 단위 속성 편집

이 절차는 LDAP 서비스에만 적용됩니다.

▼ 조직 단위 항목 편집 방법

1. **Administration Server에 액세스하고 Users and Groups 탭을 선택합니다.**
2. **Manage Organizational Units 링크를 누릅니다.**
3. **66 페이지“조직 단위 찾기”에 설명된 대로 편집할 조직 단위를 찾습니다.**
4. **원하는 사항을 변경합니다.**
   특정 필드에 대한 자세한 내용은 온라인 도움말을 참조하십시오.

주 – 조직 단위 편집 페이지에서 표시되지 않는 속성 값을 변경하려면 디렉토리 서버 `ldapmodify` 명령줄 유틸리티(사용 가능한 경우)를 사용합니다.

조직 단위 이름 변경

이 절차는 LDAP 서비스에만 적용됩니다. 조직 단위 항목의 이름을 변경하면 조직 단위의 이름만 변경됩니다. 이름 변경 기능을 사용하여 항목을 하나의 조직 단위에서 다른 단위로 이동할 수는 없습니다.

▼ 조직 단위 이름 변경 방법

1. **Administration Server에 액세스하고 Users and Groups 탭을 선택합니다.**
2. **Manage Organizational Units 링크를 누릅니다.**
3. **66 페이지 "조직 단위 찾기"에 설명된 대로 편집할 조직 단위를 찾습니다.**
4. **Rename 버튼을 누릅니다.**
5. **표시되는 페이지에 새 조직 단위 이름을 입력하고 Save Changes를 누릅니다.**

조직 단위 제거

이 절차는 LDAP 서비스에만 적용됩니다.

▼ 조직 단위 삭제 방법

1. **Administration Server에 액세스하고 Users and Groups 탭을 선택합니다.**
2. **Manage Organizational Units 링크를 누릅니다.**
3. **66 페이지 "조직 단위 찾기"에 설명된 대로 삭제할 조직 단위를 찾습니다.**
4. **Delete 버튼을 누르고 표시되는 확인 상자에서 OK를 누릅니다.**

◆ ◆ ◆ 5 장

5 인증서 및 키 사용

이 장에서는 인증서와 키 인증을 사용하여 Sun Java System Web Proxy Server의 보안을 강화하는 방법에 대해 설명합니다. Proxy Server에는 모든 Sun Java System 서버의 보안 아키텍처가 포함되어 있으며, 최대의 상호 운영성과 일관성을 위해 업계 표준 및 공용 프로토콜을 기반으로 구축되었습니다.

이 장에서는 암호화 및 복호화, 공용 및 개인 키, 디지털 인증서 및 암호화 프로토콜과 같은 공용 키 암호화에 대한 기본 개념을 이해하는 것으로 가정합니다.

이 장은 다음 내용으로 구성되어 있습니다.

- 72 페이지 “Administration Server 액세스 보안”
- 72 페이지 “인증서 기반 인증”
- 73 페이지 “트러스트 데이터베이스 생성”
- 75 페이지 “Sun Crypto Accelerator 키 저장소 사용”
- 76 페이지 “VeriSign 인증서 요청 및 설치”
- 77 페이지 “기타 서버 인증서 요청 및 설치”
- 81 페이지 “이전 버전의 인증서 마이그레이션”
- 82 페이지 “인증서 관리”
- 83 페이지 “CRL 및 KRL 설치/관리”
- 84 페이지 “보안 기본 설정”
- 92 페이지 “외부 암호화 모듈 사용”
- 97 페이지 “클라이언트 보안 요구 사항 설정”
- 106 페이지 “고급 암호 설정”
- 107 페이지 “기타 보안 고려 사항”

Administration Server 액세스 보안

서버의 관리, 추가, 제거 및 마이그레이션에 사용되는 웹 기반 사용자 인터페이스인 Administration Server에는 보안이 필요합니다.

기본 Administration Server 페이지는 HTTP 모드에서 시작됩니다. 사용 가능한 Proxy Server 인스턴스가 Manage Servers의 제목 아래에 목록으로 표시됩니다. Proxy Server 인스턴스를 관리하려면 목록에서 이름을 누릅니다. Proxy Server 인스턴스의 이름을 누르면 해당 인스턴스의 Server Manager 페이지가 표시됩니다.

Server Manager 페이지에서 왼쪽 상단에 있는 Manage Servers 링크를 눌러 Administration Server 페이지로 돌아갈 수 있습니다.

인증서 기반 인증, 트러스트 데이터베이스 만들기, SSL 구성, 인증서 요청 및 설치, 보안 기본 설정 지정과 같은 보안 기능은 Administration Server와 개별 Proxy Server 인스턴스 모두에 적용됩니다. Administration Server의 보안 관련 구성의 경우 Preferences 탭과 Administration Server 페이지의 Security 탭을 사용합니다. Proxy Server 인스턴스와 관련된 보안 구성의 경우 Preferences 탭과 해당 프록시 인스턴스의 Server Manager 페이지에 나타나는 Security 탭을 사용합니다.

Administration Server를 보안 모드에서 시작하려면 기본 HTTP가 아닌 HTTPS를 사용하여 액세스해야 합니다.

보안 기능은 다음 절에서 자세히 설명합니다.

인증서 기반 인증

인증은 아이디를 확인하는 과정입니다. 네트워크 상호작용이라는 맥락에서 인증은 한 쪽이 다른 쪽의 아이디를 명확히 확인하는 것입니다. 인증서는 인증을 지원하는 방법 중 한 가지입니다.

인증서는 개인, 회사 또는 기타 엔티티의 이름을 지정하며 인증서에 포함된 공용 키가 해당 엔티티에 속한다는 것을 인증하는 디지털 데이터로 구성됩니다.

클라이언트와 서버 모두 인증서를 가질 수 있습니다. 서버 인증이란 클라이언트가 서버의 아이디를 확인하는 것을 말합니다. 즉, 특정 네트워크의 주소에서 서버에 대한 책임이 있는 조직의 아이디를 확인하는 것입니다. 클라이언트 인증이란 서버가 클라이언트의 아이디를 확인하거나 클라이언트 소프트웨어를 사용하는 사람의 아이디를 확인하는 것입니다. 개인이 여러 개의 신분증을 가질 수 있는 것처럼 클라이언트에는 여러 개의 인증서가 있을 수 있습니다.

인증서는 인증 기관(또는 CA)이 발행하고 전자적으로 서명합니다. CA는 인증서를 판매하는 회사이거나 회사의 인트라넷 또는 익스트라넷용으로 인증서를 발행하는 부서일 수 있습니다. 다른 사람의 아이디를 확인하는 데 충분히 신뢰할 수 있는 CA를 선택합니다.

인증서에는 다음 정보가 포함됩니다.

- 공용 키
- 인증서로 식별되는 엔티티의 이름
- 만료일
- 인증서를 발행한 CA의 이름
- CA 발행의 전자 서명

주 – 서버 인증서는 반드시 암호화 기능을 사용하기 전에 설치되어야 합니다.

트러스트 데이터베이스 생성

서버 인증서를 요청하기 전에 트러스트 데이터베이스를 만들어야 합니다. Proxy Server에서는 Administration Server 및 각 서버 인스턴스에 자체 트러스트 데이터베이스가 있을 수 있습니다. 트러스트 데이터베이스는 로컬 컴퓨터에만 만들 수 있습니다.

트러스트 데이터베이스를 만들 때 키 쌍 파일용으로 사용할 비밀번호를 지정합니다. 또한 암호화된 통신을 사용하여 서버를 시작할 때에도 이 비밀번호가 필요합니다. 비밀번호를 선택하는 경우 고려해야 할 지침은 108 페이지 “고급 비밀번호 선택”을 참조하십시오.

트러스트 데이터베이스에서 공용 및 개인 키를 만들고 저장할 수 있습니다. 이는 키 쌍 파일이라고 합니다. 키 쌍 파일은 SSL 암호화에 사용됩니다. 키 쌍 파일은 서버 인증서를 요청하고 설치할 때 사용합니다. 인증서가 설치되면 트러스트 데이터베이스에 저장됩니다.

키 쌍 파일은 다음 디렉토리에 암호화되어 저장됩니다.

server-root/alias/proxy-**serverid**-key3.db

Administration Server에는 하나의 트러스트 데이터베이스만 있을 수 있습니다. 각 서버 인스턴스에는 자체의 트러스트 데이터베이스를 부여할 수 있습니다.

▼ 트러스트 데이터베이스를 만드는 방법

1. **Administration Server 또는 Server Manager에 액세스하고 Security 탭을 누릅니다.**
2. **Create Database 링크를 누릅니다.**
3. **트러스트 데이터베이스의 비밀번호를 입력합니다.**
4. **비밀번호를 다시 입력하고 OK를 누릅니다.**

password.conf 사용

기본적으로 시작하기 전에 관리자에게 키 데이터베이스 비밀번호를 입력하라는 프롬프트가 Proxy Server에 표시됩니다. 무인 작업으로 Proxy Server를 다시 시작하려면 비밀번호를 `password.conf` 파일에 저장해야 합니다. 시스템이 적절히 보호되어 이 파일과 키 데이터베이스가 조작되지 않을 경우에만 이 기능을 사용하십시오.

일반적으로 UNIX SSL 사용 서버의 경우 시작하기 전에 비밀번호가 필요하므로 `/etc/rc.local` 또는 `/etc/inittab` 파일을 사용할 수 없습니다. 비밀번호를 일반 텍스트 파일에 저장하여 SSL 사용 서버를 자동으로 시작할 수는 있지만 안전하지 않습니다. 서버의 `password.conf` 파일은 루트 또는 서버를 설치한 사용자의 소유여야 하며 소유자만 파일을 읽고 쓸 수 있어야 합니다.

UNIX의 경우 SSL 사용 서버의 비밀번호를 `password.conf` 파일에 남겨두면 보안상의 위험이 커집니다. 파일에 액세스할 수 있는 사용자는 모두 SSL 사용 서버의 비밀번호를 알 수 있습니다. SSL 사용 서버의 비밀번호를 `password.conf` 파일에 보관하기 전에 보안 위험에 대해 고려해야 합니다.

Windows의 경우 NTFS 파일 시스템이 있으면 파일을 사용하지 않더라도 액세스를 제한하여 `password.conf` 파일이 포함된 디렉토리를 보호해야 합니다. 디렉토리에는 Administration Server 사용자와 Proxy Server 사용자에 대해 읽기 및 쓰기 권한이 있어야 합니다. 디렉토리를 보호하면 다른 사람이 잘못된 `password.conf` 파일을 만들 수 없도록 방지합니다. FAT 파일 시스템의 경우 액세스를 제한하는 경우에도 디렉토리나 파일을 보호할 수 없습니다.

SSL 사용 서버 자동 시작

▼ SSL 사용 서버 자동 시작 방법

1 SSL이 활성화되어 있는지 확인합니다.

2 Proxy Server 인스턴스의 `config` 하위 디렉토리에 새 `password.conf` 파일을 만듭니다.

- Proxy Server와 함께 제공되는 내부 PKCS #11 소프트웨어 암호화 모듈을 사용하는 경우 다음 정보를 입력합니다.`internal:` *your-password*
  - 하드웨어 암호화 또는 하드웨어 가속기용의 다른 PKCS #11 모듈을 사용하는 경우에는 해당 PKCS #11 모듈의 이름과 비밀번호를 지정합니다. 예를 들면 다음과 같습니다.`nFast:` *your-password*

    `password.conf` 파일을 만든 후에도 Proxy Server를 시작할 때 항상 비밀번호를 입력하라는 프롬프트가 표시됩니다.

Sun Crypto Accelerator 키 저장소 사용

Sun Crypto Accelerator 4000 카드는 시스템 CPU가 낼 수 있는 속도보다 훨씬 빠른 속도로 확장 가능하고 최적화된 SSL 작업을 제공합니다.

▼ Sun Crypto Accelerator를 사용하도록 Proxy Server를 구성하려면

1. **Sun Crypto Accelerator 4000 보드를 설치합니다.**
2. **Sun Crypto Accelerator 4000 보드를 초기화합니다.**
3. **Proxy Server 4.0.8을 설치합니다(루트로 설치하는 것이 좋음).**
4. **프록시 인스턴스에 트러스트 데이터베이스를 만듭니다.**
   트러스트 데이터베이스를 만드는 방법에 대한 자세한 내용은 73 페이지 “트러스트 데이터베이스 생성”를 참조하십시오.
5. **Sun Crypto Accelerator 4000 보드를 활성화합니다.**

▼ Proxy Server에서 Sun Crypto Accelerator 4000 보드를 활성화하려면

1. **`secadm` 명령을 사용하여 사용자와 영역을 설정합니다.**
2. **"*server-root*`/bin/proxy`" 디렉토리를 "*server-root*`/bin/https`" 디렉토리에 복사합니다.**
   이 단계에서는 `ipsslcfg` 스크립트를 사용하여 `modutil` 명령을 찾아야 합니다.
3. **`/opt/SUNWconn/bin/iplsslcfg` 스크립트를 편집하여 `modutil` 경로를 지정합니다.**
4. **`/opt/SUNWconn/bin/iplsslcfg`를 실행합니다.**
5. **옵션 `1. Configure Sun ONE Web Server for SSL`을 선택합니다.**

주 – 옵션 1은 SSL에 대한 Web Server의 구성을 나타냅니다. Proxy Server 구성에 대해서도 같은 **옵션** 1을 선택합니다.

---

6. **Proxy Server 4.0.8 설치 디렉토리를 지정하고 y 를 선택하여 계속 진행합니다.**
   모듈 Sun Crypto Accelerator가 데이터베이스에 추가됩니다.

7 **관리 서버를 다시 시작합니다.**

8 **다시 시작한 후 Security->Request Certificate->Cryptographic Module을 선택합니다.**
그러면 목록에 SUNW acceleration only, Internal 및 keystore_name 등이 표시됩니다. 각 키 저장소는 목록에 자체 항목이 있습니다.

9 **해당 키 저장소를 선택합니다.**
서버 인증서를 만드는 동안에는 SUNW acceleration only 옵션을 선택하지 마십시오.

VeriSign 인증서 요청 및 설치

VeriSign은 Proxy Server의 기본 인증 기관입니다. 이 회사의 기술은 인증서 요청 프로세스를 간소화합니다. VeriSign에는 인증서를 사용자의 서버로 직접 회신할 수 있다는 장점이 있습니다.

서버용 인증서 트러스트 데이터베이스를 만든 후 인증서를 요청하고 인증 기관(CA)에 제출할 수 있습니다. 회사에 내부 CA가 있는 경우에는 해당 부서로 인증서를 요청합니다. 상용 CA로부터 인증서를 구매할 계획인 경우에는 CA를 선택하고 필요한 정보 형식이 있는지 문의합니다.

Administration Server에는 오직 하나의 서버 인증서만 부여할 수 있습니다. 각 서버 인스턴스에는 자체의 서버 인증서를 부여할 수 있습니다.

▼ VeriSign 인증서 요청 방법

1 **Administration Server 또는 Server Manager에 액세스하고 Security 탭을 누릅니다.**

2 **Request VeriSign Certificate 링크를 누릅니다.**

3 **표시되는 페이지에 나열된 단계를 검토하고 OK를 누릅니다.**
VeriSign Enrollment Wizard가 과정을 안내합니다.

▼ VeriSign 인증서 설치 방법

1 **Administration Server 또는 Server Manager에 액세스하고 Security 탭을 누릅니다.**

2 **Install VeriSign Certificate 링크를 누릅니다.**

3 **외부 암호화 모듈을 사용하지 않는 한 Cryptographic Module 드롭다운 목록에서 Internal을 선택합니다.**

4 **키 쌍 파일 비밀번호 또는 PIN을 입력합니다.**

5 **드롭다운 목록에서 검색할 Transaction ID를 선택하고 OK를 누릅니다.**

기타 서버 인증서 요청 및 설치

VeriSign 외에도 다른 인증 기관에 인증서를 요청하여 설치할 수 있습니다. 회사나 조직에서 자체의 내부 인증서를 제공할 수도 있습니다. 이 절에서는 여러 유형의 서버 인증서를 요청하고 설치하는 방법에 대해 설명합니다.

이 절은 다음 내용으로 구성되어 있습니다.

- 77 페이지 "필수 CA 정보"
- 78 페이지 "기타 서버 인증서 요청"
- 79 페이지 "기타 서버 인증서 설치"

필수 CA 정보

요청 프로세스를 시작하기 전에 CA가 요구하는 정보가 무엇인지 알아야 합니다. 요청되는 정보의 형식은 CA에 따라 다르지만 일반적으로 아래 나열된 정보를 제공해야 합니다. 이 정보의 대부분은 인증서를 갱신할 때는 필요하지 않습니다.

- **Requestor name.** 인증서가 발행될 이름
- **Telephone number.** 요청자의 전화 번호
- **Common name.** DNS 조회에 사용되는 정규화된 호스트 이름(예: `www.example.com`)
- **Email address.** 업체와 CA 사이의 통신용으로 사용할 사업용 전자 메일 주소
- **Organization.** 회사, 교육 기관, 조직 등의 공식적, 법적 이름. 대부분의 CA는 정보에 대해 법적 서류(예: 사업자 등록)로 확인할 것을 요구합니다.
- **Organizational unit.** 회사 내 조직 단위의 설명
- **Locality.** 조직이 위치한 국가 또는 시/도에 대한 설명
- **State or Province.** 회사가 위치한 시/도
- **Country.** 국가 이름의 두자리 약자(ISO 형식. 예를 들어, 미국의 국가 코드는 US입니다.

모든 정보는 고유 이름(DN)이라고 하는 일련의 속성 값 쌍으로 조합되어 인증서의 개체를 고유하게 구분합니다.

상용 CA에서 인증서를 구매하는 경우에는 반드시 CA에 연락하여 인증서를 발행하기 위하여 필요한 추가 정보가 있는지 확인해야 합니다. 대부분의 CA는 아이디에 대한 증명을 요구합니다. 예를 들어, 회사 이름 및 회사가 서버를 관리하도록 지정한 사용자를 확인하고 사용자가 제공하는 정보를 사용할 법적 권한이 있는지 확인할 수 있습니다.

일부 상용 CA는 완벽한 아이디를 제공하는 조직이나 개인에게 더 자세하고 정확한 인증서를 제공합니다. 예를 들어, 사용자에게 www.example.com 컴퓨터에 대한 관리의 권한이 있으며 3년간 경영해온 회사로 유의할 고객 소송이 없었다는 사실을 표시하는 인증서를 구매할 수 있습니다.

기타 서버 인증서 요청

▼ 기타 서버 인증서 요청 방법

1. **Administration Server 또는 Server Manager에 액세스하고 Security 탭을 누릅니다.**
2. **Request a Certificate 링크를 누릅니다.**
3. **신규 인증서인지 또는 인증서 갱신인지 지정합니다.**
   인증서는 대부분 6개월이나 1년 등, 일정 시간이 경과하면 무효화됩니다. CA에 따라 자동으로 갱신을 송신하는 경우도 있습니다.
4. **인증서 요청을 제출할 방법을 지정합니다.**
   - 전자 메일을 사용하여 요청을 제출하려면 CA Email Address를 선택하고 해당 요청에 적절한 전자 메일 주소를 입력합니다.
   - CA의 웹 사이트를 사용하여 요청을 제출하려면 CA URL을 선택하고 해당 요청에 적절한 URL을 입력합니다.
5. **Cryptographic Module 드롭다운 목록에서 인증서 요청 시 키 쌍 파일에 사용될 암호화 모듈을 선택합니다.**
6. **키 쌍 파일용 비밀번호를 입력합니다.**
   Internal이 아닌 암호화 모듈을 선택하지 않는 한 이 비밀번호는 트러스트 데이터베이스를 만들 때 지정됩니다. 서버는 비밀번호를 사용하여 개인 키를 구하고 CA로 전송되는 메시지를 암호화합니다. 그런 다음 서버는 공용 키와 암호화된 메시지를 모두 CA로 전송합니다. CA는 공용 키를 사용하여 메시지를 해독합니다.
7. **이름 및 전화 번호와 같은 아이디 정보를 입력합니다.**
   이 정보의 형식은 CA에 따라 다릅니다. 이 정보의 대부분은 인증서를 갱신할 때는 필요하지 않습니다.
8. **입력한 사항이 정확한지 다시 한 번 확인한 다음 OK를 누릅니다.**
   정보가 정확할 수록 인증서가 더욱 빨리 승인될 수 있습니다. 인증 서버에 대한 요청인 경우 요청을 제출하기 전에 양식 정보를 확인하라는 프롬프트가 표시됩니다.

서버가 정보를 포함하는 인증서 요청을 생성합니다. 요청에는 개인 키를 사용하여 만든 전자 서명이 포함됩니다. CA는 전자 서명을 사용하여 요청이 서버 컴퓨터에서 CA로 라우팅되는 동안 조작되지 않았는지 검사합니다. 드물지만 요청이 조작된 경우에는 보통 CA가 전화를 통하여 사용자에게 문의합니다.

요청을 전자 메일로 보내는 경우 서버는 요청이 포함된 전자 메일 메시지를 CA로 전송합니다. 이후 대개 인증서는 전자 메일로 전달됩니다. 인증 서버에 대한 URL을 지정한 경우 서버가 URL을 사용하여 요청을 인증 서버에 제출합니다. CA에 따라 전자 메일 또는 다른 방법을 통해 회신을 받을 수 있습니다.

CA가 인증서 발행에 동의하는 경우 해당 사실을 통지합니다. 대부분의 경우 CA는 전자 메일을 사용하여 인증서를 전송합니다. 조직에서 인증 서버를 사용하는 경우 인증서 서버의 형식을 사용하여 인증서를 검색할 수 있습니다.

주 – 상용 CA로 인증서를 요청하는 모든 사람에게 인증서가 발행되는 것은 아닙니다. 많은 CA가 인증서를 발행하기 전에 아이디 증명을 요구합니다. 또한 승인에는 하루에서 몇 주까지 걸릴 수 있습니다. CA에 필요한 모든 정보를 신속하게 제공할 책임이 있습니다.

인증서를 받으면 설치합니다. 그 동안에는 SSL 없이 Proxy Server를 계속 사용할 수 있습니다.

기타 서버 인증서 설치

CA의 인증서는 공용 키로 암호화되므로 오직 해당 사용자만 해독할 수 있습니다. 정확한 트러스트 데이터베이스용 비밀번호를 입력해야만 인증서를 해독하고 설치할 수 있습니다.

인증서에는 세 가지 유형이 있습니다.

- 클라이언트에게 제시할 자체 서버의 인증서
- 인증 체인에 사용할 CA의 자체 인증서
- 신뢰할 수 있는 CA의 인증서

인증서 체인이란 연속적인 인증 기관이 서명한 일련의 계층적 인증서를 말합니다. CA 인증서는 인증 기관을 확인하고 해당 기관이 발행한 인증서에 서명하는 데 사용됩니다. 이 CA 인증서는 다시 상위 CA의 CA 인증서에 의하여 서명되는 과정을 되풀이하여 루트 CA의 서명까지 이어집니다.

주 – CA가 자동으로 인증서를 보내지 않는 경우에는 요청해야 합니다. 많은 CA가 커사의 인증서가 있는 전자 메일에 자체의 인증서를 포함하며 서버는 이 두 인증서를 동시에 설치합니다.

CA의 인증서는 공용 키로 암호화되므로 오직 해당 사용자만 해독할 수 있습니다. 인증서를 설치하면 Proxy Server는 지정한 키 쌍 파일 비밀번호를 사용하여 이를 해독합니다. 다음 절차에 설명된 대로 전자 메일을 서버에 액세스할 수 있는 다른 위치에 저장하거나 전자 메일의 텍스트를 복사한 후 Install Certificate 형식에 붙여넣을 수 있도록 합니다.

▼ 기타 서버 인증서 설치 방법

1 Administration Server 또는 Server Manager에 액세스하고 Security 탭을 누릅니다.

2 Install Certificate 링크를 누릅니다.

3 Certificate For 옆에서 설치할 인증서 유형을 선택합니다.

- This Server
  - Server Certificate Chain
  - Certification Authority

  특정 설정에 대한 자세한 내용은 온라인 도움말을 참조하십시오.

4 드롭다운 목록에서 암호화 모듈을 선택합니다.

5 키 쌍 파일 비밀번호를 입력합니다.

6 단계 3에서 Server Certificate Chain 또는Certification Authority를 선택한 경우에만 인증서 이름을 입력합니다.

7 다음 중 하나를 수행하여 인증서 정보를 입력합니다.

- Message Is In This File을 선택한 다음 CA 인증서가 포함된 파일의 전체 경로 이름을 입력합니다.
  - Message Text(헤더 포함)를 선택한 다음 CA 인증서의 컨텐트를 복사하여 붙여넣습니다. Begin Certificate 및 End Certificate 헤더를 시작 및 끝 하이픈과 함께 포함해야 합니다.

8 OK를 누릅니다.

9 새 인증서를 추가하는지 기존 인증서를 갱신하는지 여부를 지정합니다.

- Add Certificate. 새 인증서를 설치하는 경우
  - Replace Certificate. 인증서 갱신을 설치하는 경우

  인증서는 서버의 인증서 데이터베이스에 저장됩니다. 예:

  server-root/alias/ proxy-*serverid*-cert8.db

이전 버전의 인증서 마이그레이션

Sun ONE Web Proxy Server 3.6(iPlanet Web Proxy Server라고도 함)에서 Sun Java System Web Proxy Server 4로 마이그레이션하는 경우 트러스트 및 인증서 데이터베이스를 포함한 파일이 자동으로 업데이트됩니다.

Proxy Server 4 Administration Server가 이전 3.x 데이터베이스 파일에 대한 읽기 권한이 있는지 확인해야 합니다. 파일은 *alias*-`cert.db` 및 *alias*-`key.db`이며 *3.x-server-root*/`alias` 디렉토리에 있습니다.

키 쌍 파일 및 인증서는 서버에 보안이 활성화된 경우에만 마이그레이션됩니다. 또한 Administration Server 및 Server Manager의 Security 탭에서 Migrate 3.x Certificates 옵션을 사용하여 키와 인증서를 자체적으로 마이그레이션할 수 있습니다. 특정 설정에 대한 자세한 내용은 온라인 도움말을 참조하십시오.

이전 버전의 경우 인증서와 키 쌍 파일은 여러 서버 인스턴스가 사용할 수 있는 별칭에 의하여 참조되었습니다. Administration Server가 모든 별칭과 해당 구성 인증서를 관리했습니다. Sun Java System Web Proxy Server 4의 경우 Administration Server와 각 서버 인스턴스에는 자체 인증서 및 키 쌍 파일이 있으며 이는 별칭이 아닌 트러스트 데이터베이스라고 합니다.

트러스트 데이터베이스 및 해당 구성 인증서는 Administration Server 자체에 대해서는 Administration Server에서 관리되고 서버 인스턴스에 대해서는 Server Manager에서 관리됩니다. 인증서와 키 쌍 데이터베이스 파일은 이를 사용하는 서버 인스턴스의 이름을 따라 이름이 지정됩니다. 이전 버전에서 여러 서버 인스턴스가 동일한 별칭을 공유한 경우, 마이그레이션된 인증서와 키 쌍 파일의 이름은 새로운 서버 인스턴스용으로 변경됩니다.

서버 인스턴스와 연결된 트러스트 데이터베이스 전체가 마이그레이션됩니다. 이전 데이터베이스에 나열된 모든 CA가 Proxy Server 4 데이터베이스로 마이그레이션됩니다. CA가 중복되는 경우 유효 기간 동안 이전 CA를 사용합니다. 중복되는 CA를 삭제하면 안 됩니다.

Proxy Server 3.x 인증서는 지원되는 NSS(Network Security Services) 형식으로 마이그레이션됩니다. 인증서의 이름은 해당 인증서가 액세스된 Proxy Server 페이지에 따라 지정됩니다. 즉, Administration Server Security 탭 또는 Server Manager Security 탭에서 액세스되었는지에 따라 달라집니다.

▼ 인증서 마이그레이션 방법

1. **로컬 컴퓨터에서 Administration Server 또는 Server Manager에 액세스하고 Security 탭을 선택합니다.**
2. **Migrate 3.x Certificates 링크를 누릅니다.**

3. **3.6 서버가 설치된 루트 디렉토리를 지정합니다.**
4. **이 컴퓨터의 별칭을 지정합니다.**
5. **관리자의 비밀번호를 입력하고 OK를 누릅니다.**

내장 루트 인증서 모듈 사용

동적으로 로드할 수 있는 루트 인증서 모듈이 Proxy Server에 포함되어 있으며, 여기에는 VeriSign을 비롯하여 많은 CA용 루트 인증서가 있습니다. 루트 인증서 모듈을 사용하면 이전보다 훨씬 쉽게 루트 인증서를 신규 버전으로 업그레이드할 수 있습니다. 이전에는 오래된 루트 인증서를 한 번에 하나씩 삭제하고 새 인증서를 한 번에 하나씩 설치해야 했습니다. 이제 잘 알려진 CA 인증서를 설치하는 경우, 간단히 Proxy Server의 신규 버전이 발표될 때 루트 인증서 모듈 파일을 신규 버전으로 업데이트하면 됩니다.

루트 인증서는 PKCS #11 암호화 모듈로 구현되기 때문에 포함된 루트 인증서는 삭제할 수 없습니다. 이러한 인증서를 관리하는 경우 삭제 옵션은 제공되지 않습니다. 서버 인스턴스에서 루트 인증서를 제거하려면 서버의 `alias` 디렉토리에서 다음 항목을 삭제하여 루트 인증서 모듈을 비활성화합니다.

- `libnssckbi.so`(대부분의 UNIX 플랫폼)
- `nssckbi.dll`(Windows)

루트 인증서 모듈을 복원하려면 *server-root*`/bin/proxy/lib` (UNIX) 또는 *server-root*`\\bin\\proxy\\bin`(Windows)에서 확장자를 `alias` 하위 디렉토리로 복사할 수 있습니다.

루트 인증서의 트러스트 정보를 수정할 수 있습니다. 트러스트 정보는 루트 인증서 모듈 그 자체가 아니라 편집하는 서버 인스턴스용 인증서 데이터베이스에 기록되어 있습니다.

인증서 관리

서버에 설치된 CA 및 자체 인증서의 트러스트 설정을 보고, 삭제 또는 편집할 수 있습니다.

▼ 인증서 관리 방법

1. **Administration Server 또는 Server Manager에 액세스하고 Security 탭을 누릅니다.**
2. **Manage Certificates 링크를 누릅니다.**
   - 내부 암호화 모듈을 사용하는 기본 구성용 인증서를 관리하는 경우에는 설치된 모든 인증서의 목록이 해당 유형 및 유효 기간과 함께 표시됩니다. 모든 인증서는 *server-root*`/alias` 디렉토리에 저장됩니다.

- 하드웨어 가속기 등의 외부 암호화 모듈을 사용하는 경우에는 우선 해당 모듈용 비밀번호를 입력하고 OK를 눌러야 합니다. 인증서 목록이 해당 모듈에 있는 인증서를 포함하여 업데이트됩니다.

3 **관리할 인증서의 이름을 누릅니다.**

해당 인증서 유형에 대한 관리 옵션을 표시하는 페이지가 나타납니다. CA 인증서의 경우에만 클라이언트 트러스트를 설정 또는 해제할 수 있습니다. 외부 암호화 모듈에 따라 인증서를 삭제할 수 없는 경우도 있습니다.

4 **원하는 작업을 지정합니다.**

다음 옵션을 사용할 수 있습니다.

- Delete certificate 또는 Quit - 내부 인증서용
- Set client trust, Unset server trust 또는 Quit - CA 인증서용

  인증서 정보에는 소유자와 발행자가 표시됩니다. 트러스트 설정을 이용하여 클라이언트 신뢰를 설정하거나 서버 트러스트를 해제할 수 있습니다. LDAP 서버 인증서의 경우 서버가 반드시 신뢰되어야 합니다.

CRL 및 KRL 설치/관리

인증서 해지 목록(CRL) 및 변조된 키 목록(CKL)은 클라이언트 또는 서버 사용자가 더 이상 신뢰해서는 안 되는 모든 인증서와 키를 알려줍니다. 예를 들어, 인증서의 유효 기간이 끝나기 전에 사용자가 사무실을 이전하거나 퇴사하는 등 인증서의 데이터가 변경되면 인증서는 취소되며 CRL에 해당 데이터가 표시됩니다. 키가 조작 또는 변형되는 경우 해당 키와 데이터가 CKL에 표시됩니다. CRL과 CKL은 모두 CA에 의하여 만들어지고 주기적으로 업데이트됩니다. 이 목록을 얻으려면 특정 CA에 문의하십시오.

이 절에서는 CRL 및 CKL을 설치하고 관리하는 방법에 대해 설명합니다.

▼ CRL 또는 CKL 설치 방법

1 **CA에서 CRL 또는 CKL을 구하여 로컬 디렉토리에 다운로드합니다.**

2 **Administration Server 또는 Server Manager에 액세스하고 Security 탭을 누릅니다.**

3 **Install CRL/CKL 링크를 누릅니다.**

4 **다음 중 한 가지를 선택합니다.**

- Certificate Revocation List
- Compromised Key List

5 **연결된 파일의 전체 경로 이름을 입력하고 OK를 누릅니다.**

CRL 또는 CKL 정보가 나열된 Add Certificate Revocation List 또는 Add Compromised Key List 페이지가 표시됩니다. 데이터베이스에 이미 CRL 또는 CKL이 있는 경우에는 Replace Certificate Revocation List 또는 Replace Compromised Key List 페이지가 나타납니다.

6 **CRL 또는 CKL을 추가하거나 교체합니다.**

▼ CRL 및 CKL 관리 방법

1 **Administration Server 또는 Server Manager에 액세스하고 Security 탭을 누릅니다.**

2 **Manage CRL/CKL 링크를 누릅니다.**

설치된 모든 CRL과 CKL 및 만료일이 나열된 Manage Certificate Revocation List/Compromised Key List 페이지가 표시됩니다.

3 **Server CRL 또는 Server CKL 목록에서 인증서를 선택합니다.**

4 **CRL 또는 CKL을 삭제하려면 Delete CRL이나 Delete CKL을 선택합니다.**

5 **관리 페이지로 돌아가려면 Quit를 누릅니다.**

보안 기본 설정

인증서를 만든 후, 서버의 보안 작업을 시작할 수 있습니다. Sun Java System Web Proxy Server는 이 절에서 설명하는 여러 보안 요소를 제공합니다.

암호화는 정보를 변환하여 의도된 수신자 외에 아무도 알아볼 수 없도록 하는 프로세스입니다. 암호 해독은 암호화된 정보를 변환하여 다시 알아볼 수 있도록 하는 프로세스입니다. Proxy Server는 SSL(Secure Sockets Layer) 및 TLS(Transport Layer Security) 암호화 프로토콜을 지원합니다.

암호는 암호화 또는 암호 해독에 사용되는 암호화 알고리즘(수학 함수)입니다. SSL 및 TLS 프로토콜에는 다양한 암호 제품군이 포함됩니다. 보안의 안전성과 강도는 암호마다 다릅니다. 일반적으로 암호가 사용하는 비트의 수가 많을수록 데이터를 해독하는 것이 어렵습니다.

양방향 암호화 프로세스에서 양쪽에는 반드시 동일한 암호가 있어야 합니다. 다양한 암호를 사용할 수 있으므로 서버를 가장 공통적으로 사용되는 암호용으로 활성화해야 합니다.

보안 연결에서 클라이언트와 서버는 양쪽이 통신에 사용할 수 있는 가장 강력한 암호화를 사용하도록 동의합니다. SSL 2.0, SSL 3.0 및 TLS 프로토콜에서 암호를 선택할 수 있습니다.

주 – SSL 버전 2.0 이후 보안과 성능이 향상되었으므로 SSL 3.0을 사용할 수 있는 클라이언트가 아닌 경우에는 SSL 2.0을 사용하면 안 됩니다. 클라이언트 인증서가 SSL 2.0 암호와 작동되도록 보장되지 않습니다.

암호화 프로세스 그 자체로는 서버의 비밀 정보를 보안하는 데 충분하지 않습니다. 실제의 암호화 결과를 생성하거나 이전에 암호화된 정보를 해독하려면 키를 암호화 암호와 함께 사용해야 합니다. 이를 위해서 암호화 프로세스에는두 가지 키(공용 키와 개인 키)가 사용됩니다. 공용 키로 암호화된 정보는 오직 연결된 개인 키로만 해독할 수 있습니다. 공용 키는 인증서의 일부로 게시됩니다. 연결된 개인 키만 보호할 수 있습니다.

다양한 암호 제품군에 대한 설명과 키 및 인증서에 대한 자세한 내용은 **SSL 개요**를 참조하십시오.

서버에서 사용할 수 있는 암호를 지정할 수 있습니다. 암호화 성능이 최적인 암호를 활성화하려면 특정 암호를 사용하면 안 되는 충분한 이유가 있지 않는 한,모두 선택해야 합니다.

주의 – Enable No Encryption, Only MD5 Authentication을 선택하지 마십시오. 클라이언트 측에 사용 가능한 다른 암호가 없는 경우 서버는 이 설정을 기본값으로 사용하며 암호화가 수행되지 않습니다.

이 절은 다음 내용으로 구성되어 있습니다.

- 85 페이지 “SSL 및 TLS 프로토콜”
- 86 페이지 “SSL을 사용하여 LDAP와 통신”
- 86 페이지 “Proxy Server를 통해 SSL 터널링”
- 87 페이지 “SSL 터널링 구성”
- 89 페이지 “청취 소켓용 보안 사용 설정”
- 91 페이지 “전역적 보안 구성”

SSL 및 TLS 프로토콜

프록시 서버는 암호화 통신에 SSL 및 TLS 프로토콜을 지원합니다. SSL 및 TLS는 응용 프로그램에 독립적이며 더 높은 수준의 프로토콜과 함께 투명하게 계층을 이룰 수 있습니다.

SSL과 TLS 프로토콜은 서버와 클라이언트가 서로를 인증하고, 인증서를 전송하며 세션 키를 설정하는 등의 작업에 사용되는 다양한 암호를 지원합니다. 클라이언트와 서버는 지원하는 프로토콜, 암호화 정도에 대한 회사 정책, 암호화된 소프트웨어의 수출에 대한 정부 규제 등, 다양한 요인에 따라 지원하는 암호 제품군이 달라집니다. 다른 기능 중 SSL과 TLS 핸드셰이크 프로토콜에 따라 서버와 클라이언트가 통신에 사용할 암호 제품군을 선택하는 방식을 결정됩니다.

SSL을 사용하여 LDAP와 통신

Administration Server는 SSL을 사용하여 LDAP와 통신하도록 해야 합니다.

주 – 이 경우 Proxy Server는 SSL 클라이언트 역할을 하며 SSL 서버 LDAP 인증서를 서명한 루트 CA 인증서를 가져와야 합니다. LDAP에 대한 SSL 인증서가 잘 알려진 CA에서 발행되지 않은 경우 사용된 CA 루트 키를 Proxy Server 키 저장소로 가져와야 합니다.

▼ Administration Server에서 SSL 연결로 LDAP를 활성화하는 방법

1. **Administration Server에 액세스하고 Global Settings 탭을 누릅니다.**
2. **Configure Directory Service 링크를 누릅니다.**
3. **나타나는 표에서 디렉토리 서비스에 대한 링크를 누릅니다.**

   Configure Directory Service 페이지가 표시됩니다. LDAP 기반 디렉토리 서비스를 아직 만들지 않은 경우 Create New Service of Type 드롭다운 목록에서 LDAP Server를 선택한 다음 New를 눌러 디렉토리 서비스를 구성합니다. LDAP 기반 디렉토리 서비스에 대해 표시되는 특정 필드에 대한 자세한 내용은 온라인 도움말을 참조하십시오.
4. **연결에 SSL을 사용하도록 Yes를 선택한 다음 Save Changes를 누릅니다.**

Proxy Server를 통해 SSL 터널링

Proxy Server(프록시)를 정방향으로 실행할 때 클라이언트가 프록시를 통해 보안 서버에 대한 SSL 연결을 요청하면, 프록시는 보안 서버에 대한 연결을 연 다음 보안 트랜잭션에 관여하지 않고 양방향으로 데이터를 복사합니다. 이 프로세스를 SSL 터널링이라고 하며 아래 그림에서 설명합니다.

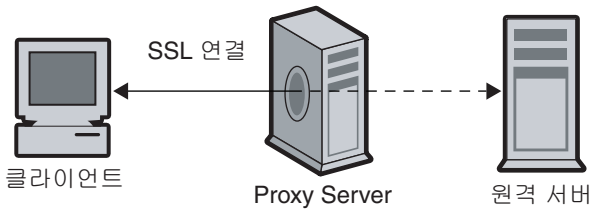

그림 5–1 SSL 연결

HTTPS URL에 SSL 터널링을 사용하려면 클라이언트는 SSL과 HTTPS를 모두 지원해야 합니다. HTTPS는 일반 HTTP에 SSL을 사용하여 구현됩니다. HTTPS 지원이 없는 클라이언트도 Proxy Server의 HTTPS 프록싱 기능을 사용하여 HTTPS 문서에 액세스할 수 있습니다.

SSL 터널링은 응용 프로그램 수준(HTTPS)에 영향을 미치지 않는 더 낮은 수준의 작동입니다. SSL 터널링은 프록싱이 없는 SSL만큼 안전합니다. 사이에 프록시가 있어도 보안이 손상되거나 SSL 기능이 저하되지 않습니다.

SSL을 통해 데이터 스트림이 암호화되므로 프록시가 실제 트랜잭션에 액세스할 수 없습니다. 따라서 액세스 로그가 원격 서버에서 수신된 상태 코드나 헤더 길이를 나열할 수 없습니다. 또한 이 프로세스를 통해 프록시 또는 다른 제 3자가 트랜잭션을 도청하는 것을 방지할 수 있습니다.

프록시는 데이터를 볼 수 없으므로 클라이언트와 원격 서버 사이에 사용되는 프로토콜이 SSL인지 확인할 수 없습니다. 따라서 프록시도 다른 프로토콜이 통과되는 것을 차단할 수 없습니다. IANA(Assigned Numbers AuthorityIANA)에 의해 할당된 HTTPS용 포트 443 및 SNEWS용 포트 563과 같이 잘 알려진 SSL 포트로만 SSL 연결을 제한해야 합니다. 다른 포트에서 보안 서버를 실행하는 사이트가 있는 경우 `connect://.*` 자원을 사용하여 명시적으로 예외를 지정하여 특정 호스트에 있는 다른 포트에 대한 연결을 허용할 수 있습니다.

SSL 터널링 기능은 실제로 프로토콜에 독립적인 일반 SOCKS의 기능과 유사하기 때문에 다른 서비스에도 이 기능을 사용할 수 있습니다. 프록시 서버는 HTTPS 및 SNEWS 프로토콜뿐만 아니라 SSL을 지원하는 모든 응용 프로그램에 대한 SSL 터널링을 처리할 수 있습니다.

SSL 터널링 구성

다음 절차에서는 SSL을 터널링하도록 Proxy Server를 구성하는 방법에 대해 설명합니다.

▼ SSL 터널링 구성 방법

1 **서버 인스턴스에 대해 Server Manager에 액세스하고 Routing 탭을 누릅니다.**

2 **Enable/Disable Proxying 링크를 누릅니다.**

3 **드롭다운 목록에서 `connect://.*:443` 자원을 선택합니다.**

`connect://` 메소드는 내부 프록시 표기법으로 프록시의 외부에는 존재하지 않습니다. `connect`에 대한 자세한 내용은 88 페이지 "SSL 터널링에 대한 기술적 세부 정보"를 참조하십시오.

다른 포트에 대한 연결을 허용하려면 템플리트에 비슷한 URL 패턴을 사용합니다. 템플리트에 대한 자세한 내용은 16 장, "템플리트 및 자원 관리"을 참조하십시오.

4 **Enable Proxying Of This Resource를 선택하고 OK를 누릅니다.**

주의 – 프록시가 잘못 구성되면 이 프록시를 사용하여 telnet 연결이 실제 연결하는 호스트가 아닌 프록시 호스트에서 들어오는 것처럼 나타나게 할 수 있습니다. 따라서 절대적으로 필요하지 않은 포트는 허용하지 말고 프록시에서 액세스 제어를 사용하여 클라이언트 호스트를 제한해야 합니다.

SSL 터널링에 대한 기술적 세부 정보

내부적으로 SSL 터널링은 `CONNECT` 메소드를 사용하고 대상 호스트 이름과 포트 번호를 매개 변수로 지정한 다음 빈 행을 추가합니다.

```
CONNECT energy.example.com:443 HTTP/1.0
```

Proxy Server의 성공적인 응답은 다음과 같으며 뒤에 빈 줄이 옵니다.

```
HTTP/1.0 200 Connection establishedProxy-agent:
Sun-Java-System-Web-Proxy-Server/4.0
```

그러면 클라이언트와 원격 서버 사이에 연결이 설정됩니다. 한 쪽 연결이 닫히기 전까지 데이터를 양방향으로 전송할 수 있습니다.

내부적으로는 URL 패턴에 따라 일반적인 구성 메커니즘을 활용하려면 다음과 같이 호스트 이름 및 포트 번호를 자동으로 URL에 매핑해야 합니다.

```
connect://energy.example.com:443
```

`connect://`는 구성을 용이하게 하고 다른 URL 패턴과 일치하도록 Proxy Server에서 사용하는 내부 표기법입니다. Proxy Server 외부에는 `connect` URL이 존재하지 않습니다. Proxy Server가 네트워크에서 이런 URL을 수신하면 URL을 유효하지 않은 것으로 표시하고 해당 요청에 대한 서비스를 거부합니다.

청취 소켓용 보안 사용 설정

다음을 수행하여 서버의 청취 소켓을 보안할 수 있습니다.

- 보안 기능 사용
- 청취 소켓용 서버 인증서 선택
- 암호 선택

주 – 역방향 프록시 모드에서만 보안을 사용할 수 있으며 순방향 프록시 모드에서는 사용할 수 없습니다.

보안 기능 사용

청취 소켓용으로 다른 보안 설정을 구성하기 전에 반드시 보안을 사용하도록 설정해야 합니다. 새 청취 소켓을 만들거나 기존 청취 소켓을 편집할 때 보안을 사용하도록 설정할 수 있습니다.

▼ 청취 소켓을 만들 때 보안을 사용하도록 설정하는 방법

1. **Administration Server 또는 Server Manager에 액세스하고 Preferences 탭을 누릅니다.**
2. **Add Listen Socket 링크를 누릅니다.**
3. **필요한 정보를 입력합니다.**

주 – 청취 소켓을 만든 후 보안 설정을 구성하려면 Edit Listen Sockets 링크를 사용합니다.

---

4. **보안을 사용하도록 설정하려면 Security 드롭다운 목록에서 Enabled를 선택한 다음 OK를 누릅니다.**

   서버 인증서가 설치되지 않은 경우에는 Disabled만 선택할 수 있습니다. 특정 설정에 대한 자세한 내용은 온라인 도움말을 참조하십시오.

▼ 청취 소켓을 편집할 때 보안을 사용하도록 설정하는 방법

1. **Administration Server 또는 Server Manager에 액세스하고 Preferences 탭을 누릅니다.**
2. **Edit Listen Sockets 링크를 누릅니다.**
3. **편집할 청취 소켓의 링크를 누릅니다.**
4. **Security 드롭다운 목록에서 Enabled를 선택한 다음 OK를 누릅니다.**

   서버 인증서가 설치되지 않은 경우에는 Disabled만 선택할 수 있습니다.

청취 소켓용 서버 인증서 선택

Administration Server나 Server Manager에서 청취 소켓을 구성하여 요청 및 설치한 서버 인증서를 사용할 수 있습니다.

주 – 인증서를 한 개 이상 설치해야 합니다.

▼ 청취 소켓용 서버 인증서를 선택하는 방법

1. **Administration Server 또는 Server Manager에 액세스하고 Preferences 탭을 누릅니다.**
2. **Edit Listen Sockets 링크를 누릅니다.**
3. **편집할 청취 소켓의 링크를 누릅니다.**
4. **Security 드롭다운 목록에서 Enabled를 선택한 다음 OK를 누릅니다.**
   서버 인증서가 설치되지 않은 경우에는 Disabled만 선택할 수 있습니다.
5. **Server Certificate Name 드롭다운 목록에서 해당 청취 소켓의 서버 인증서를 선택하고 OK를 누릅니다.**

암호 선택

Proxy Server의 보안을 보호하려면 SSL을 활성화해야 합니다. SSL 2.0, SSL 3.0 및 TLS 암호화 프로토콜을 활성화하고 다양한 암호 제품군을 선택할 수 있습니다. SSL 및 TLS 프로토콜은 Administration Server용 청취 소켓에서 활성화할 수 있습니다. Server Manager용 청취 소켓에서 SSL 및 TLS를 활성화하면 특정 서버 인스턴스에 대한 해당 보안 기본 설정이 지정됩니다. 인증서를 한 개 이상 설치해야 합니다.

주 – 청취 소켓에서 SSL를 활성화하는 것은 Proxy Server가 역방향 프록싱을 수행하도록 구성된 경우에만 적용됩니다.

기본 설정의 경우 가장 많이 사용되는 암호를 허용합니다. 특정 암호 제품군을 사용하면 안 되는 충분한 이유가 있지 않는 한, 모두 선택해야 합니다.

TLS Rollback에 대한 기본 및 권장 설정은 Enabled입니다.이 설정은 “중간개입자(man-in-the-middle) 버전 롤백” 공격 시도를 감지하도록 서버를 구성합니다. TLS 사양을 잘못 구현한 일부 클라이언트와의 상호 운영성을 위해 TLS Rollback을 Disabled로 설정해야 할 수 있습니다.

TLS Rollback을 비활성화하면 연결이 버전 롤백 공격에 취약해집니다. 버전 롤백 공격은 클라이언트와 서버가 SSL 2.0과 같이 보안이 약한 이전 프로토콜을 사용하도록 제 3자가

강제로 조정할 수 있는 메커니즘입니다. SSL 2.0 프로토콜에는 알려진 결함이 있으므로 "버전 롤백" 공격을 감지하지 못하면 제 3자가 더 쉽게 암호화된 연결을 가로채어 해독할 수 있습니다.

▼ SSL 및 TLS 활성화 방법

1. **Administration Server 또는 Server Manager에 액세스하고 Preferences 탭을 누릅니다.**
2. **Edit Listen Sockets 링크를 누른 다음 편집할 청취 소켓의 링크를 누릅니다.**
   보안 청취 소켓의 경우 사용 가능한 암호 설정이 표시됩니다.

   청취 소켓에서 보안을 활성화하지 않은 경우 SSL 및 TLS 정보가 나열되지 않습니다. 암호를 사용하려면 선택한 청취 소켓에서 보안이 사용되도록 설정해야 합니다. 자세한 내용은 89 페이지 "청취 소켓용 보안 사용 설정"을 참조하십시오.
3. **필요한 암호화 설정에 해당하는 확인란을 선택하고 OK를 누릅니다.**
4. **Netscape Navigator 6.0의 경우 TLS 및 SSL 3.0을 모두 선택합니다. TLS Rollback의 경우에는 TLS를 선택하고 SSL 3.0 및 SSL 2.0을 모두 비활성화해야 합니다.**
   서버에서 SSL을 활성화하면 URL은 `http`가 아닌 `https`를 사용합니다. SSL 사용 서버의 문서를 가리키는 URL의 형식은 다음과 같습니다. `https://`*servername* `.`*domain*`.dom:`*port*, 예: `https://admin.example.com:443`

   기본 보안 HTTP 포트(443)를 사용하는 경우 URL에 포트 번호를 입력하지 않아도 됩니다.

전역적 보안 구성

SSL 사용 서버를 설치하면 `magnus.conf` 파일(서버의 기본 구성 파일)에 전역 보안 매개변수용 지시문 항목이 만들어집니다.

SSLSessionTimeout

`SSLSessionTimeout` 지시문은 SSL 2.0 세션 캐시를 제어합니다. 구문:

`SSLSessionTimeout` *seconds*

여기서 *seconds*는 캐시된 SSL 세션의 유효 시간(초)입니다. 기본값은 100입니다. `SSLSessionTimeout` 지시문이 지정되면 초 단위 값은 자동으로 5에서 100초로 제한됩니다.

SSLCacheEntries

캐시할 수 있는 SSL 세션의 수를 지정합니다.

SSL3SessionTimeout

`SSL3SessionTimeout` 지시문은 3.0 및 TLS 세션 캐시를 제어합니다. 구문:

`SSL3SessionTimeout` *seconds*

여기서 *seconds*는 캐시된 SSL 3.0 세션의 유효한 시간(초)입니다. 기본값은 86400(24시간)입니다. `SSL3SessionTimeout` 지시문이 지정되면 초 단위 값은 자동으로 5초에서 86400초 사이로 제한됩니다.

▼ SSL 구성 파일 지시문에 대한 값을 설정하는 방법

1. **서버 인스턴스에 대한 Sever Manager에 액세스합니다.**
2. **구성하려는 청취 소켓에서 보안을 사용하는지 확인하십시오.**
   자세한 내용은 89 페이지 "청취 소켓용 보안 사용 설정"을 참조하십시오.
3. **`magnus.conf` 파일을 수동으로 편집하여 다음 설정에 대한 값을 제공합니다.**
   - `SSLSessionTimeout`
   - `SSLCacheEntries`
   - `SSL3SessionTimeout`

   `magnus.conf`에 대한 자세한 내용은 **Sun Java System Web Proxy Server 4.0.8 Configuration File Reference**를 참조하십시오.

외부 암호화 모듈 사용

Proxy Server는 다음과 같이 스마트 카드나 토큰 링 등 외부 암호화 모듈을 사용하는 방법을 지원합니다.

- PKCS #11
- FIPS 140

FIPS 140 암호화 표준을 사용하기 전에 PKCS#11 모듈을 추가해야 합니다.

이 절은 다음 내용으로 구성되어 있습니다.

- 92 페이지 "PKCS #11 모듈 설치"
- 96 페이지 "FIPS 140 표준"

PKCS #11 모듈 설치

Proxy Server는 SSL과 PKCS #11 모듈 사이의 통신에 사용되는 인터페이스를 정의하는 PKCS(Public Key Cryptography Standard) #11을 지원합니다. PKCS #11 모듈은 SSL

하드웨어 가속기에 대한 표준 기반 연결용으로 사용됩니다. 외부 하드웨어 가속기용으로 가져온 인증서 및 키는 secmod.db 파일에 저장되며 이 파일은 PKCS #11 모듈을 설치할 때 생성됩니다. 이 파일은 *server-root*/alias 디렉토리에 있습니다.

modutil 도구를 사용하여 PKCS #11 모듈 설치

modutil 도구를 사용하여 PKCS #11 모듈을 .jar 파일 또는 객체 파일의 형태로 설치할 수 있습니다.

▼ modutil 도구를 사용하여 PKCS #11 모듈을 설치하는 방법

1. **Administration Server를 포함한 모든 서버를 중지해야 합니다.**
2. **데이터베이스가 포함된** *server-root*/alias **디렉토리로 이동합니다.**
3. **PATH에** *server-root*/bin/proxy/admin/bin**을 추가합니다.**
4. *server-root* /bin/proxy/admin/bin**에서** modutil**을 찾습니다.**
5. **환경을 설정합니다.**
   - UNIX: setenv

     LD_LIBRARY_PATH *server-root*/bin/proxy/lib:${LD_LIBRARY_PATH}
   - Windows의 경우 이를 PATH에 추가합니다.

     LD_LIBRARY_PATH *server-root*/bin/proxy/bin

     server-root/proxy-admserv/start에서 나열된 컴퓨터에 대한 PATH를 찾을 수 있습니다.
6. **단말기 창에서** modutil**을 입력합니다.**
   옵션이 나열됩니다.
7. **필요한 조치를 수행합니다.**
   예를 들어, UNIX에서 PKCS #11 모듈을 추가하려면 다음을 입력합니다.

   modutil -add (*PKCS#11* **파일의 이름**) -libfile (*PKCS #11***에 대한** *libfile*) -nocertdb -dbdir . (*db* **디렉토리**)

pk12util 도구를 사용하여 내보내기

pk12util을 사용하면 내부 데이터베이스에서 인증서와 키를 내보내고 이를 내부 또는 외부 PKCS #11 모듈로 가져올 수 있습니다. 언제라도 인증서와 키를 내부 데이터베이스로 내보낼 수 있으나, 외부 토큰의 경우 대부분 인증서와 키를 내보낼 수 없습니다. 기본적으로 pk12util은 cert8.db와 key3.db라는 이름의 인증서 및 키 데이터베이스를 사용합니다.

▼ 내부 데이터베이스에서 인증서 및 키를 내보내는 방법

1. **데이터베이스가 포함된** *server-root*/alias **디렉토리로 이동합니다.**
2. **PATH에** *server-root*/bin/proxy/admin/bin**을 추가합니다.**
3. *server-root* /bin/proxy/admin/bin**에서** pk12util**을 찾습니다.**
4. **환경을 설정합니다.**
   - UNIX:

     setenv LD_LIBRARY_PATH/ *server-root*/bin/proxy/lib:${LD_LIBRARY_PATH}
   - Windows의 경우 이를 PATH에 추가합니다.

     LD_LIBRARY_PATH *server-root*/bin/proxy/bin

     아래 나열된 컴퓨터에 대한 PATH를 찾을 수 있습니다.
     server-root/proxy-admserv/start.
5. **터미널 창에서** pk12util**을 입력합니다.**
   옵션이 나열됩니다.
6. **필요한 조치를 수행합니다.**
   예를 들어, UNIX의 경우 다음을 입력합니다.

   ```
   pk12util -o certpk12 -n Server-Cert [-d /server/alias] [-P https-test-host]
   ```
7. **데이터베이스 비밀번호를 입력합니다.**
8. pkcs12 **비밀번호를 입력합니다.**

▼ 인증서 및 키를 내부 또는 외부 PKCS #11 모듈로 가져오는 방법

1. **데이터베이스가 포함된** *server-root*/alias **디렉토리로 이동합니다.**
2. **PATH에** *server-root*/bin/proxy/admin/bin**을 추가합니다.**
3. *server-root* /bin/proxy/admin/bin**에서** pk12util**을 찾습니다.**
4. **환경을 설정합니다.**
   예:
   - UNIX:

     setenv LD_LIBRARY_PATH/ *server-root*/bin/proxy/lib:${LD_LIBRARY_PATH}

- Windows의 경우 이를 PATH에 추가합니다.

  LD_LIBRARY_PATH *server-root*/bin/proxy/bin

  server-root/proxy-admserv/start에 나열된 컴퓨터에 대한 PATH를 찾을 수 있습니다.

5 **터미널 창에서 pk12util을 입력합니다.**
옵션이 나열됩니다.

6 **필요한 조치를 수행합니다.**
예를 들어, UNIX의 경우 다음을 입력합니다.

```
pk12util -i pk12_sunspot [-d certdir][-h   nCipher  ][-P
https-jones.redplanet.com-jones-]
```

-P는 반드시 -h 뒤에 있어야 하며 마지막 인수여야 합니다.

대문자와 인용 부호 사이의 공백을 포함하여 토큰 이름을 정확히 입력합니다.

7 **데이터베이스 비밀번호를 입력합니다.**

8 **pkcs12 비밀번호를 입력합니다.**

외부 인증서를 사용하여 서버 시작

서버용 인증서를 하드웨어 가속기와 같은 외부 PKCS #11 모듈에 설치한 경우 server.xml 파일을 편집하거나 아래에 설명된 대로 인증서 이름을 지정하지 않으면 해당 인증서를 사용하여 서버를 시작할 수 없습니다.

서버는 항상 이름이 Server-Cert인 인증서를 사용하여 시작하려고 합니다. 그러나 외부 PKCS #11 모듈의 인증서는 해당 식별자에 모듈의 토큰 이름 중 하나를 포함합니다. 예를 들어, smartcard0라는 외부 스마트 카드 판독기에 설치된 서버 인증서의 이름은 smartcard0:Server-Cert가 됩니다.

외부 모듈에 설치된 인증서를 사용하여 서버를 시작하려면 서버가 실행되는 청취 소켓용 인증서 이름을 지정해야 합니다.

▼ 청취 소켓용 인증서 이름을 선택하는 방법

청취 소켓에서 보안이 활성화되지 않는 경우에는 인증서 정보가 표시되지 않습니다. 청취 소켓용 인증서 이름을 선택하려면 먼저 청취 소켓에서 보안을 활성화해야 합니다. 자세한 내용은 89 페이지 “청취 소켓용 보안 사용 설정”을 참조하십시오.

1 **Administration Server 또는 Server Manager에 액세스하고 Preferences 탭을 누릅니다.**

2 **Edit Listen Sockets 링크를 누릅니다.**

3. **인증서와 연결할 청취 소켓에 대한 링크를 누릅니다.**

4. **청취 소켓에 대한 Server Certificate Name 드롭다운 목록에서 서버 인증서를 선택하고 OK를 누릅니다.**

   이 목록에는 설치된 모든 내부 및 외부 인증서가 표시됩니다.

   또한 `server.xml` 파일을 수동으로 편집하여 서버가 해당 서버 인증서를 사용하여 시작하도록 할 수 있습니다. `SSLPARAMS`의 `servercertnickname` 속성을 다음으로 변경합니다.

   ```
   $TOKENNAME:Server-Cert
   ```

   `$TOKENNAME`용으로 사용할 값을 찾으려면 서버의 Security 탭으로 이동하여 Manage Certificate 링크를 선택합니다. Server-Cert가 저장된 외부 모듈로 로그인하면 해당 인증서가 `$TOKENNAME:$NICKNAME` 형식의 목록에 표시됩니다.

   트러스트 데이터베이스를 만들지 않은 경우, 외부 PKCS #11 모듈에 대한 인증서를 요청하거나 설치하면 자동으로 만들어집니다. 만들어진 기본 데이터베이스에는 비밀번호가 없으며 액세스할 수 없습니다. 외부 모듈은 작동하지만 서버 인증서를 요청하거나 설치할 수는 없습니다. 기본 데이터베이스가 비밀번호 없이 만들어진 경우 Security 탭의 Create Database 페이지를 사용하여 비밀번호를 설정합니다.

FIPS 140 표준

PKCS #11 API를 사용하면 암호화 작업을 수행하는 소프트웨어 또는 하드웨어 모듈과 통신할 수 있습니다. PKCS #11을 Proxy Server에 설치한 후 서버를 FIPS 140과 호환되도록 구성할 수 있습니다. FIPS는 Federal Information Processing Standards를 나타냅니다. 이 라이브러리는 SSL 3.0에만 포함되어 있습니다.

▼ FIPS 140 활성화 방법

1. **FIPS 140의 설명을 따라 플러그인을 설치합니다.**

2. **Administration Server 또는 Server Manager에 액세스하고 Preferences 탭을 누릅니다.**

3. **Edit Listen Sockets 링크를 누릅니다.**

   보안 청취 소켓에 대해 Edit Listen Socket 페이지에 사용 가능한 보안 설정이 표시됩니다.

   FIPS 140을 사용하려면 선택한 청취 소켓에서 보안이 사용되도록 설정해야 합니다. 자세한 내용은 89 페이지 “청취 소켓용 보안 사용 설정”을 참조하십시오.

4. **Enable이 선택되어 있지 않으면 SSL Version 3 드롭다운 목록에서 선택합니다.**

5. **적절한 FIPS 140 암호 제품군을 선택하고 OK를 누릅니다.**

   - 168비트 암호화 및 SHA 인증이 포함된 Triple DES(FIPS) 활성화

- 56비트 암호화 및 SHA 인증이 포함된 DES(FIPS) 활성화

클라이언트 보안 요구 사항 설정

서버 보안 단계를 모두 수행한 후, 클라이언트에 대한 추가 보안 요구 사항을 설정할 수 있습니다.

클라이언트 인증이 SSL 연결에 반드시 필요한 것은 아니지만 암호화된 정보를 올바른 대상에게 전송하는 데 도움이 될 수 있습니다. 역방향 프록시에서 클라이언트 인증을 사용하여 내용 서버가 권한이 없는 프록시나 클라이언트와 정보를 공유하지 않도록 할 수 있습니다.

이 절은 다음 내용으로 구성되어 있습니다.

- 97 페이지 “클라이언트 인증 요구”
- 98 페이지 “역방향 프록시에서의 클라이언트 인증”
- 99 페이지 “역방향 프록시에서의 클라이언트 인증 설정”
- 100 페이지 “클라이언트 인증서를 LDAP로 매핑”
- 102 페이지 “certmap.conf 파일 사용”

클라이언트 인증 요구

Administration Server용 청취 소켓을 사용하도록 설정하고 각 서버 인스턴스가 클라이언트 인증을 요청하도록 할 수 있습니다. 클라이언트 인증을 활성화하면 서버가 쿼리에 대한 응답을 전송하기 전에 클라이언트에 인증서를 요구합니다.

Proxy Server는 클라이언트 인증서에 있는 CA와 클라이언트 인증서 서명용으로 신뢰된 CA를 비교하여 클라이언트 인증서를 인증합니다. 클라이언트 인증서 서명용으로 신뢰된 CA의 목록은 Security 탭을 통해 Manage Certificates 페이지에서 볼 수 있습니다.

신뢰할 수 있는 CA의 클라이언트 인증서를 보유하지 않은 클라이언트를 거부하도록 프록시 서버를 구성할 수 있습니다. 신뢰할 수 있는 CA를 수락하거나 거부하려면 CA에 대해 클라이언트 트러스트를 설정해야 합니다. 자세한 내용은 82 페이지 “인증서 관리”를 참조하십시오.

인증서의 유효 기간이 만료된 경우 프록시 서버는 오류를 기록하고 인증서를 거부하며 클라이언트에게 메시지를 반송합니다. 또한 Manage Certificates 페이지에서 만료된 인증서를 볼 수 있습니다.

서버가 인증서 클라이언트에서 정보를 수집하여 이를 LDAP 디렉토리에 있는 사용자 항목과 비교하도록 구성할 수 있습니다. 이 프로세스는 클라이언트에 유효한 인증서가 있고 LDAP 디렉토리에 항목이 있는지 확인합니다. 또한 클라이언트 인증서가 LDAP 디렉토리의 항목 중 하나와 일치되도록 합니다. 이에 대한 방법은 100 페이지 “클라이언트 인증서를 LDAP로 매핑”을 참조하십시오.

클라이언트 인증서를 액세스 제어와 조합할 수 있으므로 신뢰된 CA의 요구 사항 이외에 인증서에 연결된 사용자는 반드시 액세스 제어 규칙(ACL)과 일치되어야 합니다. 자세한 내용은 145 페이지 "액세스 제어 파일 사용"을 참조하십시오.

▼ 클라이언트 인증 요구 방법

1. **Administration Server 또는 Server Manager에 액세스하고 Preferences 탭을 누릅니다.**
2. **Edit Listen Sockets 링크를 누릅니다.**
3. **클라이언트 인증을 요구할 청취 소켓에 대한 링크를 누릅니다.**
4. **Client Authentication 드롭다운 목록을 사용하여 청취 소켓에 대한 클라이언트 인증을 요구하고 OK를 누릅니다.**

역방향 프록시에서의 클라이언트 인증

역방향 프록시에서는 다음 시나리오 중 하나에 따라 클라이언트 인증을 구성할 수 있습니다.

- **Proxy-Authenticates-Client.** 이 시나리오에서는 사용 가능한 인증서가 있는 모든 클라이언트에 대한 액세스를 허용하거나, 사용 가능한 인증서가 있고 Proxy Server의 액세스 제어 목록에서 인식된 사용자인 클라이언트에 대한 액세스만 허용할 수 있습니다.

  주 – 프록시에 CA의 사용자 루트 키 또는 사용자 인증서에 서명한 자체 서명 응용 프로그램이 있어야 합니다. 사용자는 CA 또는 Proxy Server 인증서에 서명한 자체 서명 응용 프로그램의 프록시 서버 루트 키를 로드해야 합니다.

- **Content-Server-Authenticates-Proxy.** 이 시나리오에서는 내용 서버가 실제로 Proxy Server와 연결 중이며 다른 서버와는 연결하고 있지 않음을 확인할 수 있습니다.

  주 – 프록시에 CA 또는 내용 서버 인증서에 서명한 자체 서명 응용 프로그램의 내용 서버 루트 키가 있어야 합니다. 내용 서버에 CA 또는 Proxy Server 인증서에 서명한 자체 서명 응용 프로그램의 Proxy Server 루트 키가 있어야 합니다.

- **Proxy-Authenticates-Client and Content-Server-Authenticates-Proxy.** 이 시나리오는 역방향 프록시에 대해 최대 보안 및 인증을 제공합니다.

이러한 시나리오를 구성하는 방법에 대한 자세한 내용은 99 페이지 "역방향 프록시에서의 클라이언트 인증 설정"을 참조하십시오.

역방향 프록시에서의 클라이언트 인증 설정

보안 역방향 프록시에서의 클라이언트 인증은 연결의 보안을 더욱 강화할 수 있습니다. 다음 지침에서는 선택한 시나리오에 따라 클라이언트 인증을 구성하는 방법에 대해 설명합니다.

주 – 각 시나리오에서는 보안 클라이언트-프록시 연결 및 보안 프록시-내용 서버 연결을 모두 사용한다고 가정합니다.

▼ Proxy-Authenticates-Client 시나리오 구성 방법

1 **14 장,"역방향 프록시 사용"의 "역방향 프록시 설정"에 있는 보안 클라이언트-프록시 및 보안 프록시-내용 서버 시나리오 구성 지침을 따릅니다.**

2 **서버 인스턴스에 대한 Server Manager에 액세스하고 Preferences 탭을 누릅니다.**

3 **Edit Listen Sockets 링크를 누른 다음 나타나는 표에서 원하는 청취 소켓에 대한 링크를 누릅니다.**

청취 소켓을 구성하고 추가하려면 Add Listen Socket 링크를 사용합니다.

4 **클라이언트 인증 요구 사항을 지정합니다.**

a. **유효한 인증서가 있는 모든 사용자에게 액세스를 허용하는 방법**

Security 섹션에서 Client Authentication 설정을 사용하여 이 청취 소켓에 대해 클라이언트 인증을 요구합니다. 서버 인증서가 설치되어 있지 않으면 이 설정이 표시되지 않습니다.

b. **두 개의 유효한 인증서가 모두 있고 액세스 제어에 승인된 사용자로 지정된 사용자에게만 액세스를 허용하는 방법**

i. **Security 섹션에서 Client Authentication 설정을 off로 유지합니다. 서버 인증서가 설치되어 있지 않으면 이 설정이 표시되지 않습니다.**

ii. **이 서버 인스턴스에 대한 Server Manager Preferences 탭에서 Administer Access Control 링크를 누릅니다.**

iii. **ACL을 선택한 다음 Edit 버튼을 누릅니다.**

Access Control Rules For 페이지가 표시됩니다(프롬프트가 표시되면 인증 필요).

iv. **액세스 제어를 사용하도록 설정합니다(아직 선택되어 있지 않으면 Access control Is On 확인란 선택).**

v. **역방향 프록시로 인증하도록 Proxy Server를 설정합니다.**
자세한 내용은 301 페이지 "역방향 프록시 설정"을 참조하십시오.

vi. **원하는 액세스 제어 규칙에 대한 Rights 링크를 누르고 아래 창에서 액세스 권한을 지정한 다음 Update를 눌러 이 항목을 업데이트합니다.**

vii. **Users/Groups 링크를 누릅니다. 아래 창에서 사용자 및 그룹을 지정하고 인증 방법으로 SSL을 선택한 다음 Update를 눌러 이 항목을 업데이트합니다.**

viii. **위 창에서 Submit를 눌러 항목을 저장합니다.**
액세스 제어 설정에 대한 자세한 내용은 8 장, "서버 액세스 제어"를 참조하십시오.

▼ Content Server-Authenticates-Proxy 시나리오를 구성하는 방법

1 **301 페이지 "역방향 프록시 설정"의 보안 클라이언트-프록시 및 프록시-내용 서버 시나리오를 구성하는 지침을 따릅니다.**

2 **내용 서버에서 클라이언트 인증을 사용하도록 설정합니다.**
Proxy Server에 대한 비보안 클라이언트 연결 및 내용 서버에 대한 보안 연결을 수행하고 내용 서버가 프록시 서버를 인증하도록 이 시나리오를 수정할 수 있습니다. 이렇게 하려면 다음 절차에 설명된 대로 암호화의 사용 설정을 해제하고 프록시가 인증서만 초기화하도록 해야 합니다.

▼ Proxy-Authenticates-Client and Content Server-Authenticates-Proxy 시나리오를 구성하는 방법

1 **99 페이지 "Proxy-Authenticates-Client 시나리오 구성 방법"의 프록시-인증-클라이언트 시나리오를 구성하는 방법에 대한 지침을 따릅니다.**

2 **내용 서버에서 클라이언트 인증을 사용하도록 설정합니다.**

클라이언트 인증서를 LDAP로 매핑

이 절에서는 Proxy Server가 클라이언트 인증서를 LDAP 디렉토리의 항목으로 매핑하는 프로세스에 대해 설명합니다. 클라이언트 인증서를 LDAP에 매핑하기 전에 필수 ACL을 구성해야 합니다. 자세한 내용은 8 장, "서버 액세스 제어"를 참조하십시오.

서버가 클라이언트의 요청을 수신하면 이를 처리하기 전에 클라이언트의 인증서를 요구합니다. 클라이언트에 따라 서버에 요청과 함께 클라이언트를 전송하는 경우도 있습니다.

서버는 CA를 Administration Server에 있는 신뢰할 수 있는 CA의 목록과 일치시키려 합니다. 일치 항목이 없으면 Proxy Server는 연결을 종료합니다. 일치 항목이 있으면 서버가 요청 처리를 계속합니다.

신뢰할 수 있는 CA의 인증서임을 확인한 후 서버는 다음과 같이 인증서를 LDAP 항목으로 매핑합니다.

- 클라이언트 인증서에 있는 발행자와 대상 DN을 LDAP 디렉토리의 분기점에 매핑합니다.
- LDAP 디렉토리에 클라이언트 인증서의 대상(최종 사용자)에 대한 정보와 일치하는 항목이 있는지 검색합니다.
- (선택 사항) 클라이언트 인증서를 DN에 해당하는 LDAP 항목 중 하나와 확인합니다.

서버는 `certmap.conf`라는 인증서 매핑 파일을 사용하여 LDAP 검색이 수행되는 방법을 결정합니다. 서버는 매핑 파일에 따라 클라이언트 인증서에서 가져올 값(예: 최종 사용자의 이름, 전자 메일 주소 등)을 결정합니다. 서버는 이 값을 사용하여 LDAP 디렉토리에서 사용자 항목을 검색하지만, 우선 서버가 LDAP 디렉토리에서 검색을 시작할 위치를 결정해야 합니다. 서버는 또한 인증서 매핑 파일에서 시작 위치를 알 수 있습니다.

서버가 검색을 시작할 위치와 검색할 항목을 결정하면 LDAP 디렉토리에서 검색을 수행합니다(두 번째 지점). 일치 항목이 없거나 일치 항목이 여러 개인 경우 인증서를 확인하도록 매핑이 설정되지 **않고** 검색은 실패합니다.

예상되는 검색 결과의 목록은 다음 표와 같습니다. ACL에서 예상 동작을 지정할 수 있습니다. 예를 들어, 인증서 일치에 실패하면 Proxy Server가 해당사용자만 허용하도록 지정할 수 있습니다. ACL 기본 설정을 지정하는 방법에 대한 자세한 내용은 145 페이지 “액세스 제어 파일 사용”을 참조하십시오.

표 5–1 LDAP 검색 결과

LDAP 검색 결과	인증서 검증 ON	인증서 검증 OFF
검색된 항목 없음	인증 실패	인증 실패
정확히 한 개 항목 일치	인증 실패	인증 성공
여러 항목 일치	인증 실패	인증 실패

서버가 LDAP 디렉토리에서 일치 항목과 인증서를 찾으면 서버는 해당 정보를 사용하여 트랜잭션을 처리할 수 있습니다. 예를 들어 서버에 따라 인증서 LDAP 매핑을 사용하여 서버에 대한 액세스를 결정합니다.

certmap.conf 파일 사용

인증서 매핑에 따라 서버가 LDAP 디렉토리에서 사용자 항목을 찾는 방법이 결정됩니다. certmap.conf 파일을 사용하여 이름으로 명시된 인증서를 LDAP 항목에 매핑하는 방법을 구성할 수 있습니다. 이 파일을 편집하고 항목을 추가하여 LDAP 디렉토리의 조직과 일치시키고 사용자에게 부여할 인증서 목록을 표시할 수 있습니다. 사용자는 사용자 아이디, 전자 메일 주소 또는 subjectDN에 사용되는 다른 모든 값을 기반으로 인증될 수 있습니다. 특히, 매핑 파일에는 다음의 정보가 정의됩니다.

- 서버가 검색을 시작하는 LDAP 트리 내의 위치
- LDAP 디렉토리에서 항목을 검색할 때 서버가 검색 범주로 사용할 인증서 속성
- 서버가 추가적인 검증 과정을 수행할 것인지 여부

인증서 매핑 파일은 다음에 있습니다.

server-root/userdb/certmap.conf

파일에는 하나 이상의 이름 매핑이 있으며, 각각의 매핑은 서로 다른 CA에 적용됩니다. 매핑의 구문은 다음과 같습니다.

certmap *name issuerDNname* :*property* [*value*]

첫 번째 줄은 항목의 이름과 CA 인증서에 있는 고유 이름을 구성하는 속성을 지정합니다. *name*은 임의이며 원하는 값으로 정의할 수 있습니다. 그러나 *issuerDN*은 클라이언트 인증서를 발행한 CA의 발행자 DN과 정확하게 일치해야 합니다. 예를 들어, 아래의 발행자 DN 행의 차이는 단지 속성을 구분하는 공백이지만 서버는 이 두 항목을 서로 다른 것으로 처리합니다.

```
certmap sun1 ou=Sun Certificate Authority,o=Sun,c=UScertmap sun2 ou=Sun
Certificate Authority, o=Sun, c=US
```

주 – Sun Java System Directory Server를 사용하고 발행자 DN을 일치시키는 데 문제가 발생하는 경우에는 디렉토리 서버 오류 로그에 유용한 정보가 있는지 확인하십시오.

이름 매핑의 두 번째 및 이후 줄은 등록 정보를 값과 매핑합니다. certmap.conf 파일에는 6개의 기본 등록 정보가 있습니다. 인증서 API를 사용하여 자체 등록 정보를 직접 사용자 정의할 수도 있습니다. 기본 등록 정보는 다음과 같습니다.

- DNComps는 쉼표로 분리된 속성 목록으로, LDAP 디렉토리에서 사용자의 정보(즉, 클라이언트 인증서의 소유자)와 일치하는 항목 검색을 시작할 위치를 결정하는 데 사용합니다. 서버는 클라이언트 인증서에서 이들 속성 값을 수집하고 값을 사용하여 LDAP DN을 구성합니다. 그런 후 LDAP 디렉토리에서 서버가 검색을 시작할 위치를 결정합니다. 예를 들어, DNComps가 DN의 o 및 c 속성을 사용하도록 설정된 경우 서버는 LDAP 디렉토리의 o=*org*, c= *country* 항목부터 검색을 시작합니다. 여기서 *org* 및 *country*는 인증서의 DN에 있는 값으로 대체됩니다.

  다음 상황에 유의하십시오.

- 매핑에 DNComps 항목이 없는 경우 서버는 CmapLdapAttr 설정을 사용하거나 클라이언트 인증서에 있는 전체 대상 DN(즉, 최종 사용자의 정보)을 사용합니다.
- DNComps 항목은 있으나 값이 없는 경우, 서버는 전체 LDAP 트리에서 필터와 일치하는 항목을 검색합니다.

FilterComps는 쉼표로 분리된 속성 목록으로 클라이언트 인증서에 있는 사용자의 DN에서 정보를 수집하여 필터를 만드는 데 사용합니다. 서버는 이들 속성용 값을 사용하여 LDAP 디렉토리에서 항목을 비교하는데 사용할 검색 범주를 구성합니다. LDAP에서 인증서에서 수집한 사용자의 정보와 일치하는 항목이 하나 이상 검색되는 경우 검색은 성공적이며 서버는 선택적으로 검증을 수행합니다.

예를 들어, FilterComps를 전자 메일과 사용자 아이디 속성을 사용하도록 설정하는 경우(FilterComps=e,uid), 서버는 디렉토리에서 전자 메일과 사용자 아이디 값이 클라이언트 인증서에서 수집한 사용자 정보와 일치하는 항목을 검색합니다. 전자 메일 주소와 사용자 아이디는 일반적으로 디렉토리에서 고유한 항목이므로 좋은 필터가 될 수 있습니다. LDAP 데이터베이스에서 오직 하나의 항목만 검색하려면 필터가 구체적이어야 합니다.

필터용 속성 이름은 LDAP 디렉토리가 아닌 인증서의 속성 이름이어야 합니다. 예를 들어, 일부 인증서에는 사용자의 전자 메일 주소용 속성으로 e가 있는 반면 LDAP에서 이 속성의 이름은 mail 입니다.

x509v3 인증서 속성의 목록은 다음 표와 같습니다.

표 5–2 x509v3 인증서의 속성

속성	설명
c	국가
o	조직
cn	공통 이름
l	위치
st	상태
ou	조직 단위
uid	UNIX/Linux 사용자 아이디
email	전자 메일 주소

- 서버는 verifycert에 따라 클라이언트의 인증서를 LDAP 디렉토리에서 발견된 인증서와 비교할지 여부를 결정합니다. 등록 정보는두 가지 값(on 및 off)을 사용합니다. 이 등록 정보는 LDAP 디렉토리에 인증서가 있는 경우에만 사용합니다. 이 기능은 최종 사용자의 인증서가 유효하며 취소되지 않았는지 확인하는 데 유용합니다.

- CmapLdapAttr은 LDAP 디렉토리에 있는 속성 이름으로 사용자에게 속한 모든 인증서의 대상 DN을 포함합니다. 이 등록 정보의 기본값은 certSubjectDN입니다. 이 속성은 표준 LDAP 속성이 아니므로 이 등록 정보를 사용하려면 반드시 LDAP 스키마를 확장해야 합니다. 자세한 내용은 **SSL 개요**를 참조하십시오.

  certmap.conf 파일에 이 등록 정보가 있으면 서버는 전체 LDAP 디렉토리에서 속성이 대상의 전체 DN(인증서에서 가져온 DN)과 일치하는 항목을 검색합니다. 발견된 항목이 없으면 서버는 DNComps 및 FilterComps 매핑을 사용하여 검색을 재시도합니다.

  인증서를 LDAP 항목과 일치시키는 이러한 방식의 접근은 DNComps 및 FilterComps를 사용하여 항목을 일치시키기 어려운 경우에 유용합니다.
- Library는 공유 라이브러리 또는 DLL에 대한 경로 이름입니다. 이 등록 정보는 인증서 API를 사용하여 자체 등록 정보를 만든 경우에만 사용합니다.
- InitFn은 사용자 정의 라이브러리의 init 함수의 이름입니다. 이 등록 정보는 인증서 API를 사용하여 자체 등록 정보를 만든 경우에만 사용합니다.

이러한 등록 정보에 대한 자세한 내용은 104 페이지 "매핑 예제"에 설명된 예를 참조하십시오.

사용자 정의 등록 정보 생성

클라이언트 인증서 API는 자체 등록 정보를 만드는 데 사용할 수 있습니다. 사용자 정의 매핑이 있는 경우 매핑은 다음과 같이 참조합니다.

name:library *path_to_shared_libraryname* :InitFN *name_of_ init_function*

예:

```
certmap default1 o=Sun Microsystems, c=US default1:library
/usr/sun/userdb/plugin.so default1:InitFn plugin_init_fn default1:DNComps ou o
c default1:FilterComps l default1:verifycert on
```

매핑 예제

certmap.conf 파일에는 항목이 한 개 이상 있어야 합니다. 다음 예는 certmap.conf를 사용할 수 있는 다양한 방법을 보여줍니다.

예제 #1 한 개의 기본 매핑만 포함된 certmap.conf 파일

```
certmap default defaultdefault:DNComps ou, o, cdefault:FilterComps e,
uiddefault:verifycert on
```

이 예제를 사용하면 서버는 ou=*orgunit*, o=*org*, c=*country* 항목을 포함하는 LDAP 분기점에서 검색을 시작하며, 여기서 기울임체로 표시된 텍스트는 클라이언트 인증서에 있는 대상 DN의 값으로 대체됩니다.

이후, 서버는 인증서에 있는 전자 메일 주소와 사용자 아이디 값을 사용하여 LDAP 디렉토리에 일치하는 항목이 있는지 검색합니다. 항목이 검색되면 서버는 클라이언트가 전송한 인증서와 디렉토리에 있는 인증서를 비교하여 인증서를 검증합니다.

예제 #2 두 가지 매핑이 있는 certmap.conf 파일

다음 예제 파일에는기본값 및 미국 우편 서비스에 대한 두 가지 매핑이 있습니다.

```
certmap default defaultdefault:DNCompsdefault:FilterComps e, uid

certmap usps ou=United States Postal Service, o=usps, c=USusps:DNComps
ou,o,cusps:FilterComps eusps:verifycert on
```

서버에 미국 우편 서비스가 아닌 다른 인증서가 수신되면 기본 매핑을 사용합니다. 이 경우 LDAP 트리의 상단에서 시작하여 클라이언트의 전자 메일 및 사용자 아이디와 일치하는 항목을 검색합니다. 미국 우편 서비스의 인증서인 경우 서버는 조직 단위를 포함하는 LDAP 분기에서 검색을 시작하며 일치하는 전자 메일 주소를 검색합니다. 또한 서버는 인증서를 확인합니다. 다른 인증서는 확인되지 않습니다.

주의 – 인증서의 발행자 DN(즉, CA 정보)은 반드시 매핑의 첫 번째 행 목록에 있는 발행자 DN과 동일해야 합니다. 앞의 예제에서 `o=United States Postal Service, c=US`인 발행자 DN의 인증서는 `o`와 `c` 속성 사이에 공백이 없으므로 일치되지 않습니다.

예제 #3 LDAP 데이터베이스 검색

다음 예제에서는 `CmapLdapAttr` 등록 정보를 사용하여 LDAP 데이터베이스에서 `certSubjectDN`이라는 속성을 검색합니다. 이 속성의 값은 클라이언트 인증서에서 가져온 전체 대상 DN과 정확하게 일치합니다. 이 예제에서는 LDAP 디렉토리에 `certSubjectDN` 속성이 있는 항목이 포함된 것으로 가정합니다.

```
certmap myco ou=My Company Inc, o=myco, c=USmyco:CmapLdapAttr
certSubjectDNmyco:DNComps o, c myco:FilterComps mail, uid myco:verifycert on
```

클라이언트 인증서 대상이 다음인 경우,

```
uid=Walt Whitman, o=LeavesOfGrass Inc, c=US
```

서버는 우선 다음 정보를 포함한 항목을 검색합니다.

```
certSubjectDN=uid=Walt Whitman, o=LeavesOfGrass Inc, c=US
```

일치하는 항목이 하나 이상인 경우에는 서버가 항목을 검증합니다. 일치 항목이 없는 경우 서버는 `DNComps` 및 `FilterComps`를 사용하여 일치하는 항목을 검색합니다. 이 예제에서 서버는 `o=LeavesOfGrass Inc, c=US`의 모든 항목에서 `uid=Walt Whitman`을 검색합니다.

고급 암호 설정

Server Manager Preferences 탭의 Set Cipher Size 옵션에서는 액세스용으로 168비트, 128비트 또는 56비트 비밀 키 크기를 선택하거나 제한을 설정하지 않을 수 있습니다. 제한에 맞지 않는 경우 서비스될 파일을 지정할 수 있습니다. 파일을 지정하지 않으면 Proxy Server는 Forbidden 상태를 반환합니다.

선택한 액세스용 키 크기가 Security Preferences의 현재 비밀번호 설정과 맞지 않는 경우 Proxy Server에 더 큰 비밀 키로 암호를 활성화해야 한다는 경고가 표시됩니다.

키 크기 제한은 `Service fn=key-toosmall`이 아니라 `obj.conf`의 NSAPI `PathCheck` 지시문을 기준으로 구현됩니다. 지시문은 다음과 같습니다.

```
PathCheck fn="ssl-check" [secret-keysize=nbits ] [bong-file=filename ]
```

여기서 *nbits*는 비밀 키에 필요한 최소 비트 수이며 *filename*은 제한을 만족하지 않는 경우 서비스될 파일의 이름(URL 아님)입니다.

SSL이 활성화되지 않았거나 `secret-keysize` 매개 변수가 지정되지 않은 경우 `PathCheck`는 `REQ_NOACTION`을 반환합니다. 현재 세션의 비밀 키 크기가 지정된 `secret-keysize`보다 작은 경우, `bong-file`이 지정되지 않으면 이 함수는 `REQ_ABORTED`를 `PROTOCOL_FORBIDDEN` 상태와 함께 반환합니다. `bong-file`이 지정된 경우 함수는 `REQ_PROCEED`를 반환하고 경로 변수가 `bong-file` *filename*으로 설정됩니다. 또한 키 크기 제한을 만족하지 않은 경우 현재 세션용 SSL 세션 캐시가 무효화되어 다음 번 클라이언트가 서버로 연결하면 전체 SSL 핸드셰이크가 발생합니다.

주 – Set Cipher Size 형식을 사용하면 `PathCheck fn=ssl-check`를 추가할 때 객체에서 검색되는 모든 `Service fn=key-toosmall` 지시문을 제거합니다.

▼ 고급 암호 설정 방법

1. **서버 인스턴스에 대한 Server Manager에 액세스하고 Preferences 탭을 누릅니다.**
2. **Set Cipher Size 링크를 누릅니다.**
3. **드롭다운 목록에서 고급 암호를 적용할 자원을 선택하고 Select를 누릅니다. 정규 표현식도 지정할 수 있습니다.**
   자세한 내용은 16 장, “템플리트 및 자원 관리”를 참조하십시오.
4. **비밀 키 크기 제한을 선택합니다.**
   - 168비트 이상
     - 128비트 이상

- 56비트 이상
- 제한 없음

5 **액세스를 거부할 메시지의 파일 위치를 지정하고 OK를 누릅니다.**

암호화에 대한 자세한 내용은 **SSL 개요**를 참조하십시오.

기타 보안 고려 사항

누군가 암호를 해독하려는 시도 외에도 다른 보안 위험이 있습니다. 네트워크는 서버와 서버의 정보에 액세스하려는 다양한 방법을 사용하는 외부 및 내부 해커의 위험에 직면해 있습니다. 서버 암호화 활성화 외에도 추가적인 보안 조치가 필요합니다. 예를 들어, 서버 컴퓨터를 안전한 곳에 배치하거나 신뢰할 수 없는 개인이 서버에 프로그램을 업로드하지 못하도록 해야 합니다다. 이 절에서는 서버의 보안을 강화하기 위해 취할 수 있는 몇 가지 주요 사항에 대해 설명합니다.

이 절은 다음 내용으로 구성되어 있습니다.

- 107 페이지 “실제 액세스 제한”
- 107 페이지 “관리 액세스 제한”
- 108 페이지 “고급 비밀번호 선택”
- 108 페이지 “비밀번호 또는 PIN 변경”
- 109 페이지 “서버에서 기타 응용 프로그램 제한”
- 110 페이지 “클라이언트가 SSL 파일을 캐시하지 못하도록 방지”
- 110 페이지 “포트 제한”
- 110 페이지 “서버의 한계 파악”

실제 액세스 제한

이 간단한 보안 수단이 종종 잊혀지고 있습니다. 서버 컴퓨터를 잠금 장치가 있는 곳에 보관하고 권한이 있는 사람만 출입할 수 있도록 합니다. 이 정책을 사용하면 서버 컴퓨터 자체를 해킹할 수 없도록 방지합니다. 또한 컴퓨터의 관리(루트) 비밀번호(있는 경우)를 보호하십시오.

관리 액세스 제한

원격 구성을 사용하는 경우 오직 몇몇의 사용자와 컴퓨터에만 관리를 허용하도록 액세스 제어를 설정해야 합니다. Administration Server가 최종 사용자에게 LDAP 서버나 로컬 디렉토리 정보에 대한 액세스를 제공하도록 하는 경우 두 대의 Administration Server를 유지하고 클러스터 관리를 사용하는 것을 고려하십시오. 그러면 SSL 사용 Administration Server가 마스터 서버 역할을 하고 최종 사용자가 다른 Administration Server에 액세스할 수 있습니다. 클러스터에 대한 자세한 내용은 6 장, “서버 클러스터 관리”을 참조하십시오.

또한 Administration Server에서 암호화를 사용하도록 설정해야 합니다. 관리용 SSL 연결을 사용하지 않는 경우에는 보안되지 않은 네트워크를 통하여 원격 서버 관리를 수행할 때 조심해야 합니다. 누구라도 관리 비밀번호를 가로채어 서버를 재구성할 수 있습니다.

고급 비밀번호 선택

서버에는관리 비밀번호, 개인 키 비밀번호, 데이터베이스 비밀번호 등 여러 개의 비밀번호를 사용합니다. 관리 비밀번호가 있으면 누구라도 컴퓨터에 있는 모든 서버를 구성할 수 있으므로 가장 중요한 비밀번호입니다. 개인 키 비밀번호는 다음으로 중요한 비밀번호입니다. 개인 키와 개인 키 비밀번호가 있으면 사용자의 것으로 보이는 가짜 서버를 만들거나 서버로 오고 가는 통신을 가로채고 변경할 수 있습니다.

좋은 비밀번호는 자신은 기억할 수 있지만 다른 사람은 추측할 수 없는 비밀번호입니다. 예를 들어, *MCi12!mo*를 "My Child is 12 months old!"로 기억할 수 있습니다. 자녀의 이름이나 생일은 비밀번호로 적합하지 않습니다.

해독하기 어려운 비밀번호

다음 지침을 사용하여 고급 비밀번호를 만드십시오. 하나의 비밀번호에 다음의 규칙을 모두 적용해야 하는 것은 아니지만 더 많은 규칙을 적용할수록 비밀번호를 알아내기가 더욱 어려워질 것입니다. 몇 가지 팁은 다음과 같습니다.

- 비밀번호 길이는 6-14자여야 합니다.
- 잘못된 문자인*, “ 또는 공백을 사용하지 마십시오.
- 사전의 단어를 사용하면 안 됩니다(모든 언어).
- E를 3으로, L을 1로 하는 등의 일반적인 문자 대체를 사용하지 마십시오.
- 다음 종류의 문자를 가능한 한 많이 포함시킵니다.
  - 대문자
  - 소문자
  - 숫자
  - 기호

비밀번호 또는 PIN 변경

트러스트 데이터베이스/키 쌍 파일 비밀번호나 PIN을 주기적으로 변경합니다. Administration Server에서 SSL을 사용하는 경우 서버를 시작할 때 이 비밀번호가 필요합니다. 주기적으로 비밀번호를 변경하면 서버 보호를 한 단계 높일 수 있습니다.

이 비밀번호는 로컬 컴퓨터에서만 변경해야 합니다. 비밀번호를 변경할 때 고려해야 하는 지침 목록은 108 페이지 “해독하기 어려운 비밀번호”를 참조하십시오.

▼ 트러스트 데이터베이스/키 쌍 파일 비밀번호 변경 방법

1. **Administration Server 또는 Server Manager에 액세스하고 Security 탭을 누릅니다.**
2. **Change Key Pair File Password 링크를 누릅니다.**
3. **Cryptographic Module 드롭다운 목록에서 비밀번호를 변경할 보안 토큰을 선택합니다.**
   기본적으로 내부 키 데이터베이스용 내부 토큰입니다. PKCS #11 모듈이 설치된 경우 모든 보안 토큰이 나열됩니다.
4. **현재 비밀번호를 입력합니다.**
5. **새 비밀번호를 입력합니다.**
6. **새 비밀번호를 다시 입력하고 OK를 누릅니다.**
   키 쌍 파일이 보호되는지 확인합니다. Administration Server는 키 쌍 파일을 *server-root*/alias 디렉토리에 저장합니다.

   파일이 백업 테이프에 저장되어 있는지 또는 다른 사람이 가로챌 수 있는지 확인합니다. 이 경우 백업을 서버와 마찬가지로 완벽하게 보호해야 합니다.

서버에서 기타 응용 프로그램 제한

서버와 동일한 컴퓨터에서 실행되는 모든 응용 프로그램을 신중하게 고려해야 합니다. 서버에서 실행되는 다른 프로그램의 취약점을 악용하여 서버의 보안을 우회할 수 있습니다. 필요하지 않은 모든 프로그램과 서비스를 종료합니다. 예를 들어, UNIX sendmail 데몬은 안전하게 구성하는 것이 어려우며 서버 컴퓨터에서 해로운 프로그램을 실행하도록 프로그램될 수 있습니다.

UNIX 및 Linux

inittab 및 rc 스크립트에서 시작하는 프로세스를 신중하게 선택합니다. 서버 컴퓨터에서 telnet 또는 rlogin을 실행하지 마십시오. 서버 컴퓨터에 rdist가 있으면 안 됩니다. 파일을 분산할 수는 있지만 서버 컴퓨터의 파일을 업데이트하는 데도 사용될 수 있습니다.

Windows

다른 컴퓨터와 공유할 드라이브 및 디렉토리를 신중히 고려합니다. 또한 계정이나 Guest 권한을 부여할 사용자를 고려합니다. 서버에 설치하거나 다른 사람이 설치할 수 있도록 허용할 프로그램을 신중하게 고려합니다. 다른 사람의 프로그램에는 보안 취약점이 있을 수 있습니다. 또한 특히 보안을 손상시키도록 디자인된 악의적 프로그램을 업로드할 수도 있습니다. 서버에서 프로그램을 허용하기 전에 신중하게 프로그램을 평가해야 합니다.

클라이언트가 SSL 파일을 캐시하지 못하도록 방지

HTML 파일의 <HEAD> 부분에 다음 행을 추가하여 클라이언트가 미리 암호화된 파일을 캐시할 수 없도록 방지할 수 있습니다.

```
<meta http-equiv="pragma" content="no-cache">
```

포트 제한

컴퓨터에서 사용되지 않는 포트는 모두 비활성화합니다. 라우터 또는 방화벽 구성을 사용하여 절대적인 최소 포트 이외로 들어오는 연결을 차단합니다. 이 보호 기능을 적용하면 이미 제한된 영역에 위치한 서버의 컴퓨터를 사용할 때에만 컴퓨터에서 쉘을 사용할 수 있게 됩니다.

서버의 한계 파악

서버는 서버와 클라이언트 사이에 안전한 연결을 제공합니다. 클라이언트가 일단 정보를 보유하면 정보의 보안을 제어할 수 없으며 서버 컴퓨터 자체와 해당 디렉토리 및 파일에 대한 액세스를 제어할 수 없습니다.

이러한 제한을 알고 있으면 피해야 할 상황을 이해하는 데 도움이 됩니다. 예를 들어, SSL 연결을 통해 신용 카드 번호를 구할 수 있으나 이 번호가 서버 컴퓨터의 보안 파일에 저장되어 있을까요? SSL 연결이 종료된 후 이 번호는 어떻게 될까요? 클라이언트가 SSL을 통해 전송하는 모든 정보를 보안해야 합니다.

◆ ◆ ◆ 6 장

6 서버 클러스터 관리

이 장에서는 Sun Java System Web Proxy Server 클러스터링의 개념 및 클러스터를 사용하여 서버에서 구성을 공유하는 방법에 대해 설명합니다.

이 장은 다음 내용으로 구성되어 있습니다.

- 111 페이지 “서버 클러스터 정보”
- 112 페이지 “클러스터 사용에 대한 지침”
- 112 페이지 “클러스터 설정”
- 113 페이지 “클러스터에 서버 추가”
- 114 페이지 “서버 정보 수정”
- 114 페이지 “클러스터에서 서버 제거”
- 114 페이지 “서버 클러스터 제어”

서버 클러스터 정보

클러스터는 단일 Administration Server에서 관리할 수 있는 Sun Java System Web Proxy Server 그룹입니다. 각 클러스터에는 반드시 마스터 Administration Server로 지정된 서버가 하나 있어야 합니다.

서버를 클러스터로 구성하면 다음을 수행할 수 있습니다.

- 모든 프록시 서버를 관리하는 중앙 위치 만들기
- 서버 사이에서 하나 이상의 구성 파일 공유
- 하나의 마스터 Administration Server에서 모든 서버를 시작 및 종료
- 특정 서버에 대한 액세스 및 오류 로그 보기

클러스터 사용에 대한 지침

프록시 서버 그룹을 클러스터로 구성하려면 다음 지침을 수행해야 합니다.

- 클러스터를 만들기 전에 특정 클러스터에 포함할 모든 서버를 설치해야 합니다.
- 클러스터에 포함된 모든 서버는 반드시 같은 유형(UNIX 또는 Windows)이어야 합니다. 클러스터는 반드시 같은 종류여야 합니다.
- 클러스터의 모든 서버는 Proxy Server 버전 4이어야 합니다. Proxy Server 버전 4 서버만 클러스터에 대한 추가를 지원합니다.
- 모든 Administration Server가 동일한 프로토콜, HTTP 또는 HTTPS를 사용해야 합니다. 클러스터에 있는 Administration Server 중 하나의 프로토콜을 변경한 경우 모든 Administration Server의 프로토콜을 변경해야 합니다. 자세한 내용은 114 페이지 “서버 정보 수정”을 참조하십시오.
- 모든 클러스터 특정 Administration Server에 마스터 Administration Server와 동일한 사용자 이름 및 비밀번호가 부여되어야 합니다. 각 Administration Server에 여러 관리자를 구성하기 위해 분산 관리를 사용할 수 있습니다.
- 선택한 서버에 관계 없이 하나의 클러스터 특정 Administration Server를 마스터 Administration Server로 지정해야 합니다.
- 마스터 Administration Server는 반드시 각 클러스터 특정 Administration Server에 대한 액세스 권한이 있어야 합니다. 마스터 Administration Server는 설치된 모든 Sun Java System Web Server에 대한 정보를 검색합니다.

클러스터 설정

Proxy Server 클러스터를 설정하는 일반적인 단계는 다음과 같습니다.

1. 클러스터에 포함하려는 프록시 서버를 설치합니다.

   클러스터용 Administration Server에 마스터 Administration Server가 인증용으로 사용할 수 있는 사용자 이름 및 비밀번호가 있어야 합니다. 이런 경우 기본 사용자 이름 및 비밀번호를 사용하거나 분산 관리를 구성하면 됩니다.
2. 마스터 Administration Server가 포함될 Proxy Server를 설치하고 사용자 이름과 비밀번호가 단계 1에서 설정한 사항과 일치하는지 확인합니다.
3. 클러스터 목록에 서버를 추가합니다.

   자세한 내용은 113 페이지 “클러스터에 서버 추가”를 참조하십시오.
4. Control Cluster 페이지에서 Server Manager 인터페이스에 액세스하거나 클러스터에 있는 한 서버의 구성 파일을 다른 서버로 복사하여 원격 서버를 관리합니다.

클러스터에 서버 추가

Proxy Server를 클러스터에 추가하면 Administration Server 및 포트 번호가 지정됩니다. 이 Administration Server에 하나 이상의 서버에 대한 정보가 있는 경우 해당 서버 모두가 클러스터에 추가됩니다. 개별 서버는 나중에 제거할 수 있습니다.

원격 Administration Server에 클러스터에 대한 정보가 있는 경우 원격 클러스터에 있는 서버는 추가되지 않습니다. 마스터 Administration Server는 원격 컴퓨터에 실제로 설치된 서버만 추가합니다.

▼ 원격 서버를 클러스터에 추가하는 방법

1. **마스터 Administration Server가 사용하도록 설정되었는지 확인합니다.**
2. **마스터 Administration Server에 액세스하고 Cluster 탭을 선택합니다.**
3. **Add Server 링크를 누릅니다.**
4. **원격 Administration Server가 사용하는 프로토콜을 선택합니다.**
   - 일반 Administration Server의 경우 HTTP
   - 보안 Administration Server의 경우 HTTPS
5. **예를 들어, `plaza.example.com`과 같이 `magnus.conf` 파일에 표시된 대로 원격 Administration Server의 정규화된 호스트 이름을 입력합니다.**
6. **원격 Administration Server의 포트 번호를 입력합니다.**
7. **원격 Administration Server의 관리자 이름 및 비밀번호를 입력하고 OK를 누릅니다.**
   마스터 Administration Server가 원격 서버와의 연결을 시도합니다. 성공적으로 연결될 경우 클러스터에 대한 서버 추가를 확인하는 프롬프트가 표시됩니다.

주 – 클러스터 제어가 활성화되면 클러스터의 마스터가 클러스터의 각 슬레이브용 `proxy-`*serverid* `/config/cluster/`*server-name*`/proxy-` *serverid* 디렉토리에 여러 개의 파일을 만듭니다. 이 파일의 구성은 변경할 수 없습니다.

서버 정보 수정

Administration Server의 Cluster 탭에 있는 Modify Server 옵션은 슬레이브 서버에서 슬레이브 관리 포트 정보를 변경한 후 이를 업데이트하는 경우에만 사용합니다. 클러스터에 있는 원격 Administration Server의 포트 번호를 변경하는 경우 클러스터에 저장된 Administration Server의 정보도 수정해야 합니다. 슬레이브 Administration Server에 대한 기타 사항을 변경하려면 서버를 삭제한 다음 변경 사항이 적용된 후 해당 서버를 클러스터에 다시 추가해야 합니다.

▼ 클러스터의 서버에 대한 정보를 수정하는 방법

1. **마스터 Administration Server에 액세스하고 Cluster 탭을 선택합니다.**
2. **Modify Server 링크를 누릅니다. 서버 목록이 고유 서버 식별자별로 표시됩니다.**
3. **수정할 서버를 선택하고 원하는 변경 사항을 수행한 다음 OK를 누릅니다.**

클러스터에서 서버 제거

▼ 클러스터에서 서버를 제거하는 방법

1. **마스터 Administration Server에 액세스하고 Cluster 탭을 선택합니다.**
2. **Remove Server 링크를 누릅니다.**
3. **클러스터에서 제거할 원격 서버를 선택하고 OK를 누릅니다.**
   제거된 서버는 더 이상 클러스터를 통해 액세스할 수 없습니다. 자체 Administration Server를 통해서만 액세스할 수 있습니다.

서버 클러스터 제어

Proxy Server를 사용하면 다음 작업을 통해 클러스터의 원격 서버를 제어할 수 있습니다.

- 서버 시작 및 정지
- 액세스 및 오류 로그 확인
- 구성 파일 전송마스터 Administration Server에 둘 이상의 Proxy Server 인스턴스가 있는 경우 이러한 서버에서 클러스터에 추가된 슬레이브로 파일을 전송할 수 있습니다. 클러스터는 반드시 같은 종류여야 합니다. 클러스터에 포함된 모든 서버는

반드시 같은 유형(UNIX 또는 Windows)이어야 합니다. 서로 다른 플랫폼으로 구성 파일을 전송하면 서버가 중단되거나 손상됩니다. 구성 파일은 다음과 같습니다.

- `server.xml`
- `magnus.conf`
- `obj.conf`
- `mime.types`
- `socks5.conf`
- `bu.conf`
- `icp.conf`
- `parray.pat`
- `parent.pat`

▼ 클러스터의 서버를 제어하는 방법

1 마스터 Administration Server에 액세스하고 Cluster 탭을 선택합니다.

2 Control Cluster 링크를 누릅니다.

3 제어할 서버를 선택하고 원하는 항목을 선택합니다.

요소를 변경이 수행되기 전에 있었던 값으로 재설정하려면 언제든지 Reset 버튼을 누릅니다.

- 드롭다운 목록에서 Start, Stop 또는 Restart를 선택하고 Go를 누릅니다. 작업을 확인하는 프롬프트가 표시됩니다.
- 드롭다운 목록에서 View Access 또는 View Error를 선택하고 로그 파일에 표시할 줄의 마지막 번호를 입력합니다. Go를 눌러 정보를 표시합니다. 표시된 Cluster Execution Report에서 View 버튼을 누릅니다.
- 다음과 같이 구성 파일을 전송합니다.
  - 전송할 구성 파일 선택
  - 파일이 있는 서버 선택
  - Go를 눌러 정보 전송

◆ ◆ ◆ 7 장

7 서버 기본 설정 구성

이 장에서는 Proxy Server의 시스템 설정 및 구성 방법을 설명합니다. 시스템 설정은 Proxy Server 전체에 영향을 미칩니다. 설정에는 프록시 서버가 사용하는 사용자 계정 및 해당 서버가 청취하는 포트와 같은 옵션이 포함됩니다.

이 장은 다음 내용으로 구성되어 있습니다.

- 117 페이지 “Proxy Server 시작”
- 119 페이지 “Proxy Server 중지”
- 120 페이지 “Proxy Server 다시 시작”
- 122 페이지 “서버 설정 보기”
- 123 페이지 “구성 파일의 백업 보기 및 복원”
- 124 페이지 “시스템 기본 설정 구성”
- 125 페이지 “Proxy Server 조정”
- 126 페이지 “청취 소켓 추가 및 편집”
- 129 페이지 “디렉토리 서비스 선택”
- 130 페이지 “MIME 유형”
- 131 페이지 “액세스 제어 관리”
- 132 페이지 “ACL 캐시 구성”
- 133 페이지 “DNS 캐시 이해”
- 134 페이지 “DNS 하위 도메인 구성”
- 135 페이지 “HTTP 연결 유지 구성”

Proxy Server 시작

이 절에서는 다양한 플랫폼에서 Proxy Server를 시작하는 방법을 설명합니다. 서버가 설치되면 요청을 청취하고 수락합니다.

▼ 관리 인터페이스에서 Proxy Server를 시작하는 방법

1 **Server Manager에 액세스하고 Preferences 탭을 누릅니다.**

2 **Start/Stop Server 링크를 누릅니다.**
Start/Stop Server 페이지가 표시됩니다.

3 **On 버튼을 누릅니다.**
Start/Stop Server 페이지에 서버의 상태가 나타납니다.

UNIX 또는 Linux에서 Proxy Server를 시작하는 방법

다음 중 한 가지 방법으로 UNIX 또는 Linux에서 Proxy Server를 시작할 수 있습니다.

- 명령줄에서 *server-root* `/proxy-server`*id*로 이동하고 `./start`를 입력하여 Proxy Server를 시작합니다.
- `start`를 사용합니다. 이 스크립트를 `init`와 함께 사용하려면 시작 명령 `prxy:2:respawn:`*server-root*`/proxy-server`*id*`/start -start -i`가 `/etc/inittab`에 포함되어야 합니다.

Windows에서 Proxy Server를 시작하는 방법

다음과 같이 Windows에서 Proxy Server를 시작할 수 있습니다.

- 시작 > 프로그램 > Sun Microsystems > Sun Java System Web Proxy Server **버전** > Start Proxy Server를 사용합니다.
- 제어판 > 관리 도구 > 서비스 > Sun Java System Web Proxy Server 4.0(proxy-server*id*) > 시작을 사용합니다.
- 명령 프롬프트에서 *server-root* `\proxy-server`*id*로 이동하고 `startsvr.bat`를 입력하여 Proxy Server를 시작합니다.

SSL 사용 서버 시작

SSL 사용 서버를 시작하려면 비밀번호가 필요합니다. 비밀번호를 일반 텍스트 파일에 저장하여 SSL 사용 서버를 자동으로 시작할 수는 있지만 보안 위험이 매우 큽니다. 파일에 액세스할 수 있는 사용자는 모두 SSL 사용 서버의 비밀번호를 알 수 있습니다. SSL 사용 서버의 비밀번호를 일반 텍스트로 보관하기 전에 보안의 위험에 대해 고려해야 합니다.

서버의 시작 스크립트, 키 쌍 파일 및 키 비밀번호는 루트가 소유해야 하며 (루트가 아닌 사용자가 서버를 설치한 경우에는 해당 사용자 계정) 이에 대한 읽기 및 쓰기 액세스 권한은 소유자에게만 부여되어야 합니다.

Proxy Server 중지

이 절에서는 다양한 플랫폼에서 Proxy Server를 중지하는 여러 가지 방법에 대해 설명합니다.

▼ 관리 인터페이스에서 Proxy Server를 중지하는 방법

1 **Server Manager에 액세스하고 Preferences 탭을 누릅니다.**

2 **Start/Stop Server 링크를 누릅니다.**
Start/Stop Server 페이지가 표시됩니다.

3 **Off 버튼을 누릅니다.**
Start/Stop Server 페이지에 서버의 상태가 나타납니다.

UNIX 또는 Linux에서 Proxy Server를 중지하는 방법

다음 중 한 가지 방법으로 UNIX 또는 Linux에서 Proxy Server를 중지할 수 있습니다.

- 명령줄에서 *server-root*/proxy-server*id*로 이동하고 ./stop을 입력합니다.

주 – etc/inittab 파일을 사용하여 서버를 다시 시작한 경우에는 /etc/inittab 에서 서버를 시작하는 행을 제거하고 kill -1 1을 입력한 다음 서버를 중지해야 합니다. 그렇지 않으면 서버가 정지된 후 자동으로 재시작하게 됩니다.

- stop을 사용하면 서버가 완전히 종료되며 서버가 다시 시작할 때까지 서비스가 중단됩니다. respawn을 사용하여 자동으로 다시 시작하도록 etc/inittab 파일을 설정한 경우 서버를 종료하기 전에 etc/inittab에서 프록시 서버에 관련된 행을 제거해야 합니다. 그렇지 않으면 서버가 자동으로 다시 시작됩니다.

서버를 종료하면 서버가 완료되고 종료 프로세스 및 해당 상태가 Off로 변경되는 데 약간의 시간이 걸릴 수 있습니다.

시스템이 중단되거나 오프라인이 되는 경우에는 서버가 중단되며 서비스하는 모든 요청을 잃게 됩니다.

주 – 서버에 보안 모듈이 설치된 경우 서버를 시작 또는 중지하기 전에 적절한 비밀번호를 입력해야 합니다.

Windows에서 Proxy Server를 중지하는 방법

다음과 같이 Windows에서 Proxy Server를 중지할 수 있습니다.

- 시작 > 프로그램 > Sun Microsystems > Sun Java System Web Proxy Server **버전** > Stop Proxy Server를 사용합니다.
- 명령 프롬프트에서 *server-root*\proxy-server*id*로 이동하고 `stopsvr.bat`를 입력하여 Proxy Server를 중지합니다.
- 서비스 창에서 Sun Java System Proxy Server 4.0(proxy-server *id*) 서비스를 사용합니다. 제어판 > 관리 도구 > 서비스

Proxy Server 다시 시작

이 절에서는 다양한 플랫폼에서 Proxy Server를 다시 시작하는 여러 가지 방법에 대해 설명합니다.

서버 다시 시작(UNIX 또는 Linux)

다음 중 한 가지 방법으로 서버를 다시 시작할 수 있습니다.

- 서버를 수동으로 다시 시작합니다.
- `inittab` 파일에서 서버를 자동으로 다시 시작합니다.

  System V에서 유도되지 않은 UNIX 또는 Linux 버전을 사용하는 경우(예: SunOS™ 4.1.3) `inittab` 파일을 사용할 수 없습니다.
- 시스템이 재부팅될 때 `/etc/rc2.d`의 데몬을 사용하여 서버를 자동으로 다시 시작합니다.

설치 스크립트는 `/etc/rc.local` 또는 `/etc/inittab` 파일을 편집할 수 없으므로 반드시 텍스트 편집기에서 이 파일을 편집해야 합니다. 이 파일의 편집 방법을 모르는 경우에는 시스템 관리자에게 문의하거나 시스템 설명서를 참조하십시오.

▼ 명령줄에서 Proxy Server를 다시 시작하는 방법

1. **서버가 1024보다 낮은 번호의 포트에서 실행되는 경우 루트로 로그인합니다. 그렇지 않은 경우에는 루트 또는 서버 사용자 계정으로 로그인합니다.**

2. **명령줄 프롬프트에서 다음 행을 입력하고 Enter를 누릅니다.**

   server-root`/proxy-server`*id*`/restart`

   여기서 *server-root*는 서버가 설치된 디렉토리입니다.

- 행의 마지막에 선택 매개 변수인 -i를 사용할 수 있습니다. -i 옵션을 사용하면 서버가 inittab 모드로 실행되므로 서버 프로세스가 종료 또는 중단되는 경우inittab가 서버를 자동으로 다시 시작합니다. 또한 이 옵션을 사용하면 서버가 자체를 배경 프로세스로 전환할 수 없도록 방지합니다.

inittab를 사용하여 서버를 다시 시작하는 방법

/etc/inittab 파일의 한 행에 다음 텍스트를 추가합니다.

prxy:23:respawn:*server-root*/proxy-server*id*/start -start -i

여기서 *server-root*는 서버가 설치된 디렉토리이고 proxy-server*id*는 서버의 디렉토리입니다.

-i 옵션을 사용하면 서버가 자체를 배경 프로세스로 전환할 수 없도록 방지합니다.

서버를 중지하기 전에 반드시 이 행을 제거해야 합니다.

시스템 RC 스크립트를 사용하여 서버를 다시 시작하는 방법

/etc/rc.local 또는 시스템의 해당 파일을 사용하는 경우 /etc/rc.local에 다음 행을 추가합니다.

server-root/proxy-server*id*/start

*server-root*를 서버를 설치한 디렉토리로 대체합니다.

서버 다시 시작(Windows)

서비스 제어판을 사용하거나 다음 작업을 완료하여 서버를 다시 시작할 수 있습니다.

▼ Windows에서 서버를 다시 시작하는 방법

1. **제어판 > 관리 도구 > 서비스를 사용합니다.**
2. **서비스 목록에서 Sun Java System Web Proxy Server 4.0(proxy-server*id*)을 선택합니다.**
3. **속성 창에서 시작 유형을 자동으로 변경합니다. 컴퓨터가 시작되거나 재부팅할 때마다 시스템이 서버를 시작합니다.**
4. **OK를 누릅니다.**

종료 시간 초과 설정

서버가 정지되면 새 연결을 받지 않습니다. 또한 모든 기존 연결이 완료되도록 대기합니다. 서버가 제한 시간이 만료되기 전까지 대기하는 시간은 `magnus.conf` 파일에서 구성할 수 있습니다. 기본값은 30초로 설정됩니다. 값을 변경하려면 `magnus.conf` 파일에 다음 행을 추가합니다.

`TerminateTimeout` *seconds*

여기에서 *seconds*는 서버가 시간 초과 동안 대기하는 초 단위 시간입니다.

이 값을 구성하면 서버가 연결이 완료될 때까지 더 긴 시간 동안 대기하는 장점이 있습니다. 그러나 서버에 응답하지 않는 클라이언트의 연결이 있을 수 있으므로 종료 시간 초과를 크게 하면 서버가 종료되는 시간이 더 오래 걸릴 수 있습니다.

서버 설정 보기

설치 중 Proxy Server의 일부 설정을 구성합니다. 이러한 설정 및 기타 시스템 설정을 Server Manager에서 볼 수 있습니다. View Server Settings 페이지에 Proxy Server의 모든 설정이 나열됩니다. 또한 저장되지 않았거나 적용되지 않은 변경 사항이 있는지 여부를 표시합니다. 저장되지 않은 변경 사항이 있는 경우 해당 사항을 저장하고 Proxy Server를 다시 시작해야 새 구성으로 시작할 수 있습니다.

서버 설정에는 두 가지 유형(기술적 설정 및 컨텐트 설정)이 있습니다. 서버의 컨텐트 설정은 서버를 구성한 방식에 따라 다릅니다. 일반적으로 프록시는 모든 템플리트, URL 매핑 및 액세스 제어를 나열합니다. 개별 템플리트에 대해 View Server Settings 페이지에 템플리트 이름, 정규 표현식 및 템플리트 설정(예: 캐시 설정)이 나열됩니다.

프록시 서버의 기술적 설정은 `magnus.conf` 파일과 `server.xml` 파일에서 컨텐트 설정은 `obj.conf` 파일에서 찾을 수 있습니다. 이 파일은 서버 루트 디렉토리의 `proxy-`*id*`/config` 하위 디렉토리에 있습니다.

▼ Proxy Server에 대한 설정을 보는 방법

1. **Server Manager에 액세스하고 Preferences 탭을 누릅니다.**
2. **View Server Settings 링크를 누릅니다.**
   View Server Settings 페이지가 표시됩니다.

구성 파일의 백업 보기 및 복원

구성 파일의 백업 사본을 보거나 복원할 수 있으며, 이러한 구성 파일에는`server.xml`, `magnus.conf`, `obj.conf`, `mime` **유형**, `server.xml.clfilter`, `magnus.conf.clfilter`, `obj.conf.clfilter`, `socks5.conf`, `bu.conf`, `icp.conf`, `parray.pat`, `parent.pat`, `proxy-id.acl` 등이 있습니다. 이 기능을 사용하면 현재 구성에 문제가 있을 때 기존 구성을 사용할 수 있습니다. 예를 들어, 프록시의 구성을 몇 가지 변경한 후에 프록시가 올바르게 작동하지 않는 경우(예: URL에 대한 액세스를 거부했지만 프록시가 요청을 서비스하는 경우), 이전 구성으로 돌아가서 구성 변경을 재실행할 수 있습니다.

▼ 이전 구성을 보는 방법

1. **Server Manager에 액세스하고 Preferences 탭을 누릅니다.**
2. **Restore Configuration 링크를 누릅니다.**
   Restore Configuration 페이지가 표시됩니다. 이 페이지는 일자 및 시간 순으로 이전의 모든 구성을 나열합니다.
3. **View 링크를 누르면 특정 버전의 기술적 및 컨텐트 설정 목록이 표시됩니다.**

▼ 구성 파일의 백업 사본을 복원하는 방법

1. **Server Manager에 액세스하고 Preferences 탭을 누릅니다.**
2. **Restore Configuration 링크를 누릅니다.**
   Restore Configuration 페이지가 표시됩니다. 이 페이지는 일자 및 시간 순으로 이전의 모든 구성을 나열합니다.
3. **복원할 버전의 Restore 링크를 누릅니다.**
   모든 파일을 특정 시간의 해당 상태로 복원하려면 테이블 왼쪽 열에서 Restore to *time* 링크를 누릅니다. *time*은 복원할 일자 및 시간입니다.

▼ 표시되는 백업 수 설정 방법

1. **Server Manager에 액세스하고 Preferences 탭을 누릅니다.**
2. **Restore Configuration 링크를 누릅니다.**
   Restore Configuration 페이지가 표시됩니다.

3 **Set Number Of Sets Of Backups 필드에 표시할 백업의 수를 입력합니다.**

4 **Change 버튼을 누릅니다.**

시스템 기본 설정 구성

Configure System Preferences 페이지에서 서버의 기본적인 측면을 설정하거나 변경할 수 있습니다. 이 페이지에서는 다음 작업을 수행할 수 있습니다.

- 서버 사용자, 프로세스 수, 청취 대기열 크기, 프록시 시간 초과 및 프록시 서버의 인터럽트 후 시간 초과 변경
- DNS, ICP, 프록시 배열 및 상위 배열 활성화

기본 설정 옵션은 다음과 같습니다.

- **Server User**. Server User는 프록시가 사용하는 사용자 계정입니다. 프록시 서버 사용자로 입력하는 사용자 이름은 이미 정상적인 사용자 계정으로 존재해야 합니다. 서버를 시작하면 이 사용자에 의해 시작된 것처럼 실행됩니다.

  새 사용자 계정을 만들지 않으려면 동일한 호스트에서 실행되는 다른 서버가 사용하는 계정을 선택하거나, UNIX 프록시를 실행하는 경우에는 `nobody` 사용자를 선택할 수 있습니다. 그러나 일부 시스템에서는 `nobody` 사용자가 파일을 소유할 수만 있고 프로그램은 실행할 수 없기 때문에 프록시 사용자 이름으로 적합하지 않습니다.

  UNIX 시스템에서는 프록시가 사용하는 모든 프로세스가 서버 사용자 계정에 할당됩니다.
- **Processes**. Processes 필드는 서비스 요청에 사용 가능한 프로세스 수를 표시합니다. 기본값은 1입니다. 필요하지 않는 이상 이 설정을 수정하지 마십시오.
- **Listen Queue Size**. Listen Queue Size 필드는 청취 소켓에서 대기하는 연결의 최대 수를 지정합니다.
- **DNS**. DNS(Domain Name Service)는 IP 주소를 호스트 이름으로 복원합니다. 웹 브라우저가 서버에 연결되면 서버는 클라이언트의 IP 주소(예: `198.18.251.30`)만 가져옵니다. 서버에는 `www.example.com`과 같은 호스트 이름 정보가 없습니다. 서버는 액세스 로깅 및 액세스 제어를 위해 IP 주소를 호스트 이름으로 변환할 수 있습니다. Configure System Preferences 페이지에서 IP 주소를 호스트 이름으로 변환할 것인지 여부를 지정할 수 있습니다.
- **ICP**. ICP(Internet Cache Protocol)는 캐시가 서로 통신할 수 있도록 해주는 메시지 전달 프로토콜입니다. 캐시는 ICP를 사용하여 쿼리를 전송하고 캐시된 URL의 존재 및 이러한 URL을 검색하기 위한 최상의 위치 정보에 대해 응답합니다. Configure System Preferences 페이지에서 ICP를 활성화할 수 있습니다. ICP에 대한 자세한 내용은 260 페이지 “ICP 환경을 통한 라우팅”을 참조하십시오.
- **Proxy Array**. 프록시 배열은 분산 캐시를 위해 하나의 캐시 역할을 하는 여러 프록시의 배열입니다. Configure System Preferences 페이지에서 프록시 배열 옵션을 활성화하면, 구성하는 프록시 서버가 프록시 배열의 구성원이 되고 해당 배열의 다른

모든 구성원이 동급이 됩니다. 프록시 배열 사용에 대한 자세한 내용은 268 페이지 “프록시 배열을 통한 라우팅”을 참조하십시오.

- **Parent Array**. 상위 배열은 프록시 또는 프록시 배열 구성원이 라우팅하는 프록시 배열입니다. 따라서 프록시가 원격 서버에 액세스하기 전에 업스트림 프록시 배열을 라우팅하는 경우, 해당 업스트림 프록시 배열이 상위 배열로 간주됩니다. 프록시 서버에서의 상위 배열 사용에 대한 자세한 내용은 280 페이지 “상위 배열을 통한 라우팅”을 참조하십시오.
- **Proxy Timeout**. 프록시 시간 초과는 프록시 서버가 요청을 시간 초과로 처리하기 전에 원격 서버에서 전송되는 연속적인 네트워크 데이터 패킷 간 최대 시간입니다. 프록시 시간 초과의 기본값은 5분입니다.

주 – 원격 서버가 server-push를 사용하고 페이지 간의 지연이 프록시 시간 초과보다 긴 경우, 전송이 완료되기 전에 연결이 종료될 수 있습니다. 대신 여러 요청을 프록시로 전송하는 client-pull을 사용합니다.

▼ 시스템 기본 설정 수정 방법

1. **Server Manager에 액세스하고 Preferences 탭을 누릅니다.**
2. **Configure System Preferences 링크를 누릅니다.**
   Configure System Preferences 페이지가 표시됩니다.
3. **옵션을 변경한 다음 OK를 누릅니다.**
4. **Restart Required를 누릅니다.**
   Apply Changes 페이지가 표시됩니다.
5. **Restart Proxy Server 버튼을 눌러 변경 사항을 적용합니다.**

Proxy Server 조정

Tune Proxy 페이지에서는 기본 매개 변수를 변경하여 프록시 서버의 성능을 조정할 수 있습니다.

▼ 기본 조정 매개 변수 변경 방법

1. **Server Manager에 액세스하고 Preferences 탭을 누릅니다.**
2. **Tune Proxy 링크를 누릅니다.**
   Tune Proxy 페이지가 표시됩니다.
3. **(선택 사항) 긴 파일 이름을 사용할 수 있도록 FTP 목록의 너비를 수정하여 파일 이름이 잘리는 현상을 줄입니다.**
   기본 너비는 80자입니다.
4. **OK를 누릅니다.**
5. **Restart Required를 누릅니다.**
   Apply Changes 페이지가 표시됩니다.
6. **Restart Proxy Server 버튼을 눌러 변경 사항을 적용합니다.**

청취 소켓 추가 및 편집

서버가 요청을 처리하려면 청취 소켓을 통해 요청을 수락한 다음 올바른 서버로 요청을 전달해야 합니다. Proxy Server를 설치하면 청취 소켓 한 개(ls1)가 자동으로 만들어집니다. 이 청취 소켓은 IP 주소 `0.0.0.0` 및 설치 중 프록시 서버 포트 번호로 지정한 포트 번호를 사용합니다. 기본 청취 소켓은 삭제할 수 없습니다.

- **General**
  - **Listen Socket ID.** 청취 소켓용 내부 이름입니다. 청취 소켓을 만든 후에는 이 이름을 변경할 수 없습니다.
  - **IP Address.** 청취 소켓의 IP 주소입니다. 이 주소는 점으로 연결된 쌍(dotted-pair) 또는 IPv6 표기법일 수 있습니다. 또한 `0.0.0.0`, any, `ANY` 또는 `INADDR_ANY`(모든 IP 주소)일 수 있습니다.
  - **Port.** 청취 소켓을 만들 포트 번호입니다. 허용되는 값은 1-65535입니다. UNIX에서 포트 1-1024를 청취하는 소켓을 만들려면 수퍼유저 권한이 필요합니다. 포트 443을 청취하도록 SSL 청취 소켓을 구성합니다.
  - **Server Name.** 이 청취 소켓의 기본 서버입니다.

  Security

보안을 비활성화하면 다음 매개 변수만 표시됩니다.

- **Security.** 선택한 청취 소켓용 보안을 사용 또는 사용하지 않도록 설정합니다.

보안을 활성화하면 다음 매개 변수가 표시됩니다.

- **Security.** 선택한 청취 소켓용 보안을 사용 또는 사용하지 않도록 설정합니다.
  - **Server Certificate Name.** 드롭다운 목록에서 설치된 인증서를 선택하여 이 청취 소켓용으로 사용할 수 있습니다.
  - **Client Authentication.** 이 청취 소켓에 클라이언트 인증이 필요한지 여부를 지정합니다. 이 설정의 기본값은 Optional입니다.
  - **SSL Version 2.** SSL 버전 2를 활성화하거나 비활성화합니다. 기본적으로 이 설정은 비활성화됩니다.
  - **SSL Version 2 Ciphers.** 이 제품군에 있는 모든 암호화 목록이 표시됩니다. 상자를 선택하거나 선택 해제하여 편집하는 청취 소켓에 대해 활성화할 암호화를 선택합니다. 기본 버전은 선택 해제되어 있습니다.
  - **SSL Version 3.** SSL 버전 3을 활성화하거나 비활성화합니다. 기본적으로 이 설정은 활성화됩니다.
  - **TLS.** 암호화된 통신을 위한 TLS(Transport Layer Security) 프로토콜을 활성화하거나 비활성화합니다. 기본적으로 활성화됩니다.
  - **TLS Rollback.** TLS 롤백을 활성화하거나 비활성화합니다. TLS 롤백을 비활성화하면 연결이 버전 롤백 공격에 취약해진다는 점에 유의하십시오. 기본적으로 활성화됩니다.
  - **SSL Version 3 and TLS Ciphers.** 이 제품군에 있는 모든 암호화 목록이 표시됩니다. 상자를 선택하거나 선택 해제하여 편집하는 청취 소켓에 대해 활성화할 암호화를 선택합니다. 기본 버전이 선택되어 있습니다.

  Advanced

  - **Number Of Acceptor Threads.** 청취 소켓용 승인자 스레드의 수입니다. 권장값은 컴퓨터에 있는 프로세서의 수입니다. 기본값은 1입니다. 유효한 값은 1-1024입니다.

    Protocol Family. 소켓군 유형입니다. 허용되는 값은 `inet`, `inet6` 및 `nca`입니다. IPv6 청취 소켓의 경우 `inet6` 값을 사용합니다. Solaris Network Cache와 Accelerator를 사용할 수 있도록 하려면 `nca`를 지정합니다.

Server Manager의 Add Listen Socket 및 Edit Listen Sockets 페이지를 사용하여 청취 소켓을 추가, 편집 및 삭제합니다.

청취 소켓에 대한 보안은 필요한 인증서가 설치된 뒤에만 옵션으로 활성화되며 그 전까지는 드롭다운 상자에 Disabled만 표시됩니다.

이 절은 다음 내용으로 구성되어 있습니다.

- 99 페이지 “Proxy-Authenticates-Client 시나리오 구성 방법”
- 100 페이지 “Content Server-Authenticates-Proxy 시나리오를 구성하는 방법”
- 100 페이지 “Proxy-Authenticates-Client and Content Server-Authenticates-Proxy 시나리오를 구성하는 방법”

▼ 청취 소켓을 추가하는 방법

1. **Server Manager에 액세스하고 Preferences 탭을 누릅니다.**
2. **Add Listen Socket 링크를 누릅니다.**
   Add Listen Socket 페이지가 표시됩니다.
3. **청취 소켓의 내부 이름을 지정합니다.**
   청취 소켓을 만든 후에는 이 이름을 변경할 수 없습니다.
4. **청취 소켓의 IP 주소를 지정합니다.**
   IP 주소는 점으로 연결된 쌍(dotted-pair) 또는 IPv6 표기법일 수 있습니다. 또한 `0.0.0.0`, any, `ANY` 또는 `INADDR_ANY`(모든 IP 주소)일 수 있습니다.
5. **청취 소켓을 만들 포트 번호를 지정합니다. 허용되는 값은 1 - 65535입니다.**
   UNIX에서 포트 1 - 1024를 청취하는 소켓을 만들려면 수퍼유저 권한이 필요합니다. 포트 443을 청취하도록 SSL 청취 소켓을 구성합니다.
6. **서버가 클라이언트로 전송하는 모든 URL의 호스트 이름 부분에 사용될 서버 이름을 지정합니다.**
   이 설정에 따라 서버가 자동으로 생성하는 URL이 달라지지만 서버에 저장된 디렉토리 및 파일용 URL에는 영향을 미치지 않습니다. 서버에서 별칭을 사용하는 경우 이 이름은 별칭이어야 합니다.
7. **드롭다운 목록에서 청취 소켓에 대해 보안을 활성화할 것인지 비활성화할 것인지 여부를 지정합니다.**
8. **OK를 누릅니다.**
9. **Restart Required를 누릅니다.**
   Apply Changes 페이지가 표시됩니다.
10. **Restart Proxy Server 버튼을 눌러 변경 사항을 적용합니다.**

▼ 청취 소켓을 편집하는 방법

1. **Server Manager에 액세스하고 Preferences 탭을 누릅니다.**
2. **Edit Listen Sockets 링크를 누릅니다.**
   Edit Listen Sockets 페이지가 표시됩니다.

3. **Configured Sockets 표에서 편집할 청취 소켓에 대한 링크를 누릅니다.**
   Edit Listen Sockets 페이지가 표시됩니다.
4. **원하는 옵션을 변경합니다.**
   옵션에 대한 설명은 이 절의 시작 부분을 참조하십시오.
5. **OK를 누릅니다.**
6. **Restart Required를 누릅니다.**
   Apply Changes 페이지가 표시됩니다.
7. **Restart Proxy Server 버튼을 눌러 변경 사항을 적용합니다.**

▼ 청취 소켓을 삭제하는 방법

1. **Server Manager에 액세스하고 Preferences 탭을 누릅니다.**
2. **Edit Listen Sockets 링크를 누릅니다.**
3. **삭제할 청취 소켓 옆의 확인란을 선택하고 OK를 누릅니다.**
   삭제를 확인하라는 프롬프트가 나타납니다. 해당 인스턴스의 유일한 청취 소켓이 아닌 경우 모든 청취 소켓을 삭제할 수 있습니다.
4. **Restart Required를 누릅니다.**
   Apply Changes 페이지가 표시됩니다.
5. **Restart Proxy Server 버튼을 눌러 변경 사항을 적용합니다.**

디렉토리 서비스 선택

Select Directory Services 페이지는 지정된 프록시 서버 인스턴스에 대한 모든 디렉토리 서비스를 나열합니다. 이 페이지에서 특정 프록시 서버 인스턴스와 함께 사용할 디렉토리 서비스를 선택할 수 있습니다. 자세한 내용은 45 페이지 “디렉토리 서비스 구성”을 참조하십시오.

▼ 디렉토리 서비스 선택 방법

1 **Server Manager에 액세스하고 Preferences 탭을 누릅니다.**

2 **Select Directory Services 링크를 누릅니다.**
Select Directory Services 페이지에 지정된 프록시 서버 인스턴스에 대한 모든 디렉토리 서비스가 표시됩니다.

3 **목록에서 디렉토리 서비스를 선택합니다.**

4 **OK를 누릅니다.**

5 **Restart Required를 누릅니다.**
Apply Changes 페이지가 표시됩니다.

MIME 유형

MIME(Multi-purpose Internet Mail Extension) 유형은 멀티미디어 전자 메일 및 메시징의 표준입니다. MIME 유형에 따라 파일을 필터링할 수 있도록 프록시 서버는 서버에 사용할 새 MIME 유형을 만들 수 있는 페이지를 제공합니다. 프록시는 새 유형을 `mime.types` 파일에 추가합니다. MIME 유형에 따라 파일을 차단하는 방법에 대한 자세한 내용은 290 페이지 “MIME 유형별 필터링”을 참조하십시오.

이 절에서는 MIME 유형을 만들거나, 편집 또는 제거하는 방법을 설명합니다.

MIME 유형 만들기

▼ MIME 유형을 만드는 방법

1 **Server Manager에 액세스하고 Preferences 탭을 누릅니다.**

2 **Create/Edit MIME Types 링크를 누릅니다.**
Create/Edit MIME Types 페이지에 프록시의 `mime.types` 파일에 나열된 모든 MIME 유형이 표시됩니다.

3 **드롭다운 목록에서 MIME 유형의 범주를 지정합니다.** `type`, **enc 또는** `lang` **일 수 있습니다.** `type`**은 파일 또는 응용 프로그램 유형,** `enc`**는 압축에 사용되는 인코딩,** `lang`**은 언어 인코딩입니다.**
범주에 대한 자세한 내용은 온라인 도움말을 참조하십시오.

4. **HTTP 헤더에 표시되는 컨텐트 유형을 지정합니다.**

5. **파일 접미어를 지정합니다.**
   파일 접미어는 MIME 유형에 매핑되는 파일 확장자를 나타냅니다. 하나 이상의 확장자를 지정하려면 항목을 쉼표로 분리합니다. 파일 확장자는 고유해야 합니다. 즉, 하나의 파일 확장자를 두 개의 MIME 유형에 매핑할 수 없습니다.

6. **New 버튼을 눌러 MIME 유형을 추가합니다.**

▼ MIME 유형 편집 방법

1. **Server Manager에 액세스하고 Preferences 탭을 누릅니다.**

2. **Create/Edit MIME Types 링크를 누릅니다.**
   Create/Edit MIME Types 페이지에 프록시의 `mime.types` 파일에 나열된 모든 MIME 유형이 표시됩니다.

3. **편집할 MIME 유형의 Edit 링크를 누릅니다.**

4. **원하는 사항을 변경합니다. Change MIME Type 버튼을 누릅니다.**

▼ MIME 유형 제거 방법

1. **Server Manager에 액세스하고 Preferences 탭을 누릅니다.**

2. **Create/Edit MIME Types 링크를 누릅니다.**
   Create/Edit MIME Types 페이지에 프록시의 `mime.types` 파일에 나열된 모든 MIME 유형이 표시됩니다.

3. **제거할 MIME 유형의 Remove 링크를 누릅니다.**

액세스 제어 관리

Administer Access Control 페이지에서는 액세스 제어 목록(ACL)을 관리할 수 있습니다. ACL을 사용하면 서버에 액세스할 수 있는 클라이언트를 제어할 수 있습니다. ACL은 특정 사용자, 그룹 또는 호스트를 검사하여 서버의 일부분에 대한 액세스를 허용 또는 거부할 수 있습니다. 또한 올바른 사용자와 그룹만 서버의 일부분에 액세스할 수 있도록 인증을 설정할 수도 있습니다. 액세스 제어에 대한 자세한 내용은 8 장, “서버 액세스 제어”을 참조하십시오.

▼ 액세스 제어 목록 관리 방법

1 **Server Manager에 액세스하고 Preferences 탭을 누릅니다.**

2 **Administer Access Control 링크를 누릅니다.**
Administer Access Control 페이지가 표시됩니다.

3 **자원 또는 기존 ACL을 선택하거나 ACL 이름을 입력하고 Edit 버튼을 누릅니다.**
Access Control Rules 페이지가 표시됩니다.

4 **원하는 사항을 변경한 다음 Submit을 누릅니다.**
액세스 제어에 대한 자세한 내용은 8 장, “서버 액세스 제어”의 "서버 인스턴스에 대한 액세스 제어 설정"을 참조하십시오.

ACL 캐시 구성

Configure ACL Cache 페이지는 프록시 인증 캐시 활성화 또는 비활성화, 프록시 인증 캐시 디렉토리 설정, 캐시 테이블 크기 구성 및 항목 유효 시간 설정에 사용됩니다.

▼ ACL 캐시 구성 방법

1 **Server Manager에 액세스하고 Preferences 탭을 누릅니다.**

2 **Configure ACL Cache 링크를 누릅니다.**
Configure ACL Cache 페이지가 표시됩니다.

3 **프록시 인증 캐시를 활성화하거나 비활성화합니다.**

4 **Proxy Auth User Cache Size 드롭다운 목록에서 사용자 캐시의 사용자 수를 선택합니다.**
기본 크기는 200입니다.

5 **Proxy Auth Group Cache Size 드롭다운 목록에서 단일 UID/캐시 항목에 대해 캐시할 수 있는 그룹 아이디의 수를 선택합니다.**
기본 크기는 4입니다.

6 **캐시 항목이 만료되기 전 시간(초)을 선택합니다.**
캐시에 있는 항목이 참조될 때마다 시간이 계산되고 이 값과 비교됩니다. 항목 시간이 Proxy Auth Cache Expiration 값보다 크거나 같으면 해당 항목이 사용되지 않습니다. 이 값을 0으로 설정하면 캐시가 해제됩니다.

이 값에 큰 수를 사용하면 LDAP 항목을 변경할 때 Proxy Server를 다시 시작해야 합니다. 예를 들어, 이 값을 120초로 설정하면 Proxy Server가 최대 2분까지 LDAP 서버와 동기화되지 않을 수 있습니다. LDAP 항목이 자주 변경되지 않으면 큰 값을 사용하십시오. 기본 유효 시간 값은 2분입니다.

7 **OK를 누릅니다.**

8 **Restart Required를 누릅니다.**
Apply Changes 페이지가 표시됩니다.

9 **Restart Proxy Server 버튼을 눌러 변경 사항을 적용합니다.**

DNS 캐시 이해

Proxy Server는 DNS 호스트 이름을 IP 주소로 변환할 때 프록시에서 수행하는 DNS 조회 수를 줄이기 위해 DNS 캐시를 지원합니다.

DNS 캐시 구성

Configure DNS Cache 페이지는 DNS 캐시 활성화 또는 비활성화, DNS 캐시 크기 및 DNS 캐시 항목의 유효 시간 설정, 네거티브 DNS 캐시 활성화 또는 비활성화에 사용됩니다.

▼ DNS 캐시 구성 방법

1 **Server Manager에 액세스하고 Preferences 탭을 누릅니다.**

2 **Configure DNS Cache 링크를 누릅니다.**
Configure DNS Cache 페이지가 표시됩니다.

3 **DNS 캐시를 활성화하거나 비활성화합니다.**

4 **DNS Cache Size 드롭다운 목록에서 DNS 캐시에 저장할 수 있는 항목 수를 선택합니다.**
기본 크기는 1024입니다.

5 **DNS 캐시 유효 시간을 설정합니다.**
Proxy Server는 사전 설정된 유효 시간이 되면 캐시에서 DNS 캐시 항목을 제거합니다. 기본 DNS 유효 시간은 20분입니다.

6 **호스트 이름을 찾을 수 없는 경우 오류 캐시를 활성화하거나 비활성화합니다.**

7 **OK를 누릅니다.**

8 **Restart Required를 누릅니다.**
Apply Changes 페이지가 표시됩니다.

9 **Restart Proxy Server 버튼을 눌러 변경 사항을 적용합니다.**

DNS 하위 도메인 구성

일부 URL에는 여러 수준의 하위 도메인이 있는 호스트 이름이 포함되어 있습니다. 첫 번째 DNS 서버가 호스트 이름을 확인할 수 없는 경우 프록시 서버가 DNS 검사를 수행하는 데 시간이 오래 걸릴 수 있습니다. 클라이언트에 "host not found" 메시지를 반환하기 전에 Proxy Server가 검사할 수준의 수를 설정할 수 있습니다.

예를 들어, 클라이언트가 `http://www.sj.ca.example.com/index.html`을 요청하면 프록시는 호스트 컴퓨터의 IP 주소를 가져오기 위해 4개의 DNS 서버를 통과해야 할 수 있으므로 호스트 이름을 IP 주소로 변환하는 데 시간이 오래 걸릴 수 있습니다. 이러한 조회에는 상당히 오랜 시간이 소요될 수 있기 때문에 프록시가 특정 수 이상의 DNS 서버를 사용해야 하는 경우에는 IP 주소 조회를 종료하도록 구성할 수 있습니다.

▼ 프록시 조회를 위한 하위 도메인의 수준 설정 방법

1 **Server Manager에 액세스하고 Preferences 탭을 누릅니다.**

2 **Configure DNS Subdomains 링크를 누릅니다.**
Configure DNS Subdomains 페이지가 표시됩니다.

3 **드롭다운 목록에서 자원을 선택하거나 정규 표현식을 지정합니다.**

4 **Local Subdomain Depth 드롭다운 목록에서 수준 수를 선택합니다.**

5 **OK를 누릅니다.**

6 **Restart Required를 누릅니다.**
Apply Changes 페이지가 표시됩니다.

7 **Restart Proxy Server 버튼을 눌러 변경 사항을 적용합니다.**

HTTP 연결 유지 구성

Configure HTTP Client 페이지를 사용하여 프록시 서버에서 연결 유지를 활성화할 수 있습니다.

연결 유지는 클라이언트가 열린 연결을 신속하게 다시 사용할 수 있도록 요청이 완료된 후에도 연결을 열어두는 TCP/IP 기능입니다. 기본적으로 프록시는 연결 유지 연결을 사용하지 않지만 일부 시스템에서는 연결 유지 기능을 사용하여 프록시 성능을 향상시킬 수 있습니다.

웹의 정상적인 클라이언트-서버 트랙잭션에서 클라이언트는 서버로 여러 문서를 요청하는 여러 개의 연결을 만들 수 있습니다. 예를 들어, 클라이언트가 다양한 그래픽 이미지가 있는 웹 페이지를 요청하는 경우 클라이언트는 각 그래픽 파일에 대해 별도의 요청을 만들어야 합니다. 연결을 다시 설정하는 데 많은 시간이 소요될 수 있습니다. 따라서 연결 유지 패킷이 유용할 수 있습니다.

▼ HTTP 연결 유지 구성 방법

1 **Server Manager에 액세스하고 Preferences 탭을 누릅니다.**

2 **Configure HTTP Client 링크를 누릅니다.**

Configure HTTP Client 페이지가 표시됩니다.

3 **드롭다운 목록에서 자원을 선택합니다.**

Proxy Server에서 연결 유지를 구성할 HTTP 또는 HTTPS 자원을 선택하거나 정규 표현식을 지정합니다.

4 **적절한 Keep Alive 옵션을 선택하여 HTTP 클라이언트가 지속적인 연결을 사용해야 하는지 여부를 지정합니다.**

5 **Keep Alive Timeout 필드에 지속적인 연결을 열어 두어야 하는 최대 시간(초)을 지정합니다.**

기본값은 29입니다.

6 **적절한 Persistent Connection Reuse 옵션을 선택하여 HTTP 클라이언트가 모든 유형의 요청에 대해 기존의 지속적인 연결을 다시 사용할 수 있는지 여부를 지정합니다.**

기본값은 off이며, 이 경우 GET이 아닌 요청이나 본문이 있는 요청에 대해 지속적인 연결을 다시 사용할 수 없습니다.

7 **HTTP Version String 필드에 HTTP 프로토콜 버전 문자열을 지정합니다.**

특정한 프로토콜 상호 운영성 문제가 발생하지 않는 한 이 매개 변수를 지정하지 마십시오.

8. **Proxy Agent Header 필드에 Proxy Server 제품 이름 및 버전을 지정합니다.**

9. **SSL Client Certificate Nickname 필드에 원격 서버에 제시할 클라이언트 인증서의 별명을 지정합니다.**

10. **적절한 SSL Server Certificate Validation 옵션을 선택하여 Proxy Server가 원격 서버에서 제시한 인증서를 검증해야 하는지 여부를 표시합니다.**

11. **OK를 누릅니다.**

12. **Restart Required를 누릅니다.**
    Apply Changes 페이지가 표시됩니다.

13. **Restart Proxy Server 버튼을 눌러 변경 사항을 적용합니다.**

◆ ◆ ◆ 8 장

8 서버 액세스 제어

이 장에서는 Administration Server 및 Proxy Server에서 제공하는 데이터에 대한 액세스를 제어하는 방법에 대해 설명합니다. 서버에서 제공하는 모든 데이터 또는 특정 URL에 대한 액세스를 제한할 수 있습니다. 예를 들어 특정 사용자만 특정 URL에 액세스하거나 이러한 사용자를 제외한 모든 사용자가 파일을 볼 수 있도록 지정할 수 있습니다. 모든 클라이언트에 대해 HTTP URL에는 액세스할 수 있지만 FTP에 대해서는 제한된 액세스만 허용할 수 있습니다. 또한 Proxy Server가 여러 내부 웹 서버에 서비스를 제공하고 이러한 서버 중 하나에 저장된 기밀 연구 프로젝트에 특정 사용자만 액세스할 수 있게 하려는 경우와 같이 호스트 이름 또는 도메인 이름을 기준으로 URL을 제한할 수 있습니다.

Administration Server에서 액세스 제어를 사용하기 전에 분산 관리 기능을 활성화하고 LDAP 데이터베이스에 관리 그룹을 구성해야 합니다. 이 장의 정보는 이러한 작업이 이미 수행되었다는 가정하에 제공됩니다.

이 장은 다음 내용으로 구성되어 있습니다.

- 137 페이지 “액세스 제어란”
- 149 페이지 “액세스 제어 설정”
- 153 페이지 “액세스 제어 옵션 선택”
- 159 페이지 “서버의 영역에 대한 액세스 제한”
- 162 페이지 “자원에 대한 액세스 보안”
- 163 페이지 “파일 기반 인증용 ACL 생성”

액세스 제어란

액세스 제어를 통해 Proxy Server에 액세스할 수 있는 사용자와 이러한 사용자가 액세스할 수 있는 서버의 부분을 결정할 수 있습니다. 전체 서버 또는 서버의 일부분(디렉토리, 파일, 파일 유형 등)에 대한 액세스를 제어할 수 있습니다. 수신 요청을 평가할 때 액세스는 액세스 제어 항목(ACE)이라는 규칙의 계층을 기준으로 결정됩니다. Proxy Server는 액세스를 허용할지 또는 거부할지 결정하기 위해 일치하는 항목을 찾습니다. 각 ACE는 서버가 계층의 다음 항목을 계속할 것인지의 여부를 지정합니다.

ACE의 컬렉션은 ACL(Access Control List)이라고 합니다. 요청을 수신하면 `obj.conf` 파일이 ACL에 대한 참조로 확인된 다음 액세스 여부를 결정하는 데 사용됩니다. 기본으로 서버에는 하나의 ACL 파일이 있으며 여기에는 여러 개의 ACL이 있습니다.

액세스는 다음 항목을 기준으로 허용 또는 거부됩니다.

- 요청하는 사용자 (사용자 그룹)
- 요청의 출처(호스트-IP)
- 요청이 발생한 시간(예: 하루 중 시간)
- 사용되는 연결의 종류(SSL)

이 절은 다음 내용으로 구성되어 있습니다.

- 138 페이지 “사용자 그룹용 액세스 제어”
- 145 페이지 “호스트-IP용 액세스 제어”
- 145 페이지 “액세스 제어 파일 사용”
- 146 페이지 “ACL 사용자 캐시 구성”
- 146 페이지 “클라이언트 인증서로 액세스 제어”

사용자 그룹용 액세스 제어

서버에 대한 액세스를 특정 사용자 또는 그룹으로 제한할 수 있습니다. 사용자 그룹 액세스 제어를 사용하려면 사용자가 해당 서버에 액세스하기 전에 사용자 이름과 비밀번호를 제공해야 합니다. 서버는 클라이언트 인증서에 있는 정보 또는 클라이언트 인증서 자체를 디렉토리 서버 항목과 비교합니다.

Administration Server는 오직 Basic 인증만 사용합니다. Administration Server에 클라이언트 인증이 필요하도록 하려면 반드시 `obj.conf`의 ACL 파일을 직접 편집하여 인증 방법을 SSL로 변경해야 합니다.

사용자 그룹 인증은 서버에 구성된 디렉토리 서비스에 의해 수행됩니다. 자세한 내용은 45 페이지 “디렉토리 서비스 구성”을 참조하십시오.

디렉토리 서비스가 액세스 제어를 구현하는데 사용하는 정보는 다음 중 한 가지 소스에서 구합니다.

- 내부 보통 파일 유형 데이터베이스
- 외부 LDAP 데이터베이스

서버가 외부 LDAP 기반 디렉토리 서비스를 사용하는 경우 서버 인스턴스용으로 다음 유형의 사용자 그룹 인증 방법을 지원합니다.

- Default
- Basic
- SSL
- Digest
- Other

서버가 내부 파일 기반 디렉토리 서비스를 사용하는 경우 서버 인스턴스용으로 다음 유형의 사용자 그룹 인증 방법을 지원합니다.

- Default
- Basic
- Digest

사용자 그룹 인증의 경우 사용자가 액세스 권한을 얻기 전에 자신의 아이디를 증명합니다. 인증 과정에서 사용자는 사용자 이름과 비밀번호를 제공하거나 클라이언트 인증서 또는 Digest 인증 플러그인을 사용하여 자신의 아이디를 증명합니다. 클라이언트 인증서를 사용하려면 암호화가 필요합니다.

Default 인증

Default 인증은 가장 많이 사용되는 방법입니다. Default 설정은 `obj.conf` 파일에서 기본적인 방법을 사용하거나 `obj.conf`에 설정이 없는 경우 Basic을 사용합니다. Default가 선택된 경우 ACL 규칙은 ACL 파일에서 방법을 지정하지 않습니다. Default를 선택하면 `obj.conf` 파일에서 한 줄만 편집하여 모든 ACL에 대한 인증 방법을 쉽게 변경할 수 있습니다.

Basic 인증

Basic 인증의 경우 사용자가 서버에 액세스하기 위해 사용자 이름과 비밀번호를 제공해야 합니다. Basic 인증은 기본 설정입니다. 사용자 및 그룹 목록을 만들어 Sun Java System Directory Server 같은 LDAP 데이터베이스 또는 파일에 저장해야 합니다. Proxy Server와는 다른 서버 루트에 설치된 디렉토리 서버 또는 원격 컴퓨터에 설치된 디렉토리 서버를 사용해야 합니다.

사용자가 사용자 그룹 인증이 있는 자원에 액세스하려는 경우 사용자 이름과 비밀번호를 입력하라는 메시지가 표시됩니다. 서버에서 암호화 기능이 사용되는지의 여부에 따라 이 정보는 암호화 또는 암호화되지 않은 형태로 서버에 입력됩니다(SSL 사용).

주 – SSL 암호화가 없는 Basic 인증을 사용하는 경우 사용자 이름과 비밀번호가 암호화되지 않은 텍스트로 네트워크에 전송됩니다. 이 네트워크 패킷은 포착될 수 있으며 사용자 이름과 비밀번호가 도용될 수 있습니다. Basic 인증은 SSL 암호화나 호스트-IP 인증 또는 이 두 가지를 함께 사용할 때 가장 효과적입니다. Digest 인증을 사용하면 이 문제를 피할 수 있습니다.

인증에 성공하면 사용자에게 요청된 자원이 표시됩니다. 사용자 이름 또는 비밀번호가 잘못된 경우 액세스를 거부하는 메시지가 표시됩니다.

권한 없는 사용자에 의해 수신된 메시지를 사용자 정의할 수 있습니다. 자세한 내용은 158 페이지 “액세스가 거부된 경우의 응답”을 참조하십시오.

SSL 인증

서버가 보안 인증서가 있는 사용자의 아이디를 확인하는 방법은 두 가지입니다.

- 클라이언트 인증서의 정보를 아이디 증명으로 사용
- LDAP 디렉토리에 게시된 클라이언트 인증서 확인 (추가)

클라이언트 인증을 위해 인증서 정보를 사용하도록 서버를 구성한 경우 서버는 다음 작업을 수행합니다.

- 인증서가 신뢰할 수 있는 인증 기관으로부터 제공되는지 여부를 확인합니다. 그렇지 않은 경우 인증이 실패하며 트랜잭션이 종료됩니다. 클라이언트 인증 사용 방법에 대한 자세한 내용은 84 페이지 "보안 기본 설정"을 참조하십시오.
- 인증서가 신뢰할 수 있는 인증 기관에서 제공된 경우 `certmap.conf` 파일을 사용하여 인증서를 사용자 항목에 매핑합니다. 인증서 매핑 파일을 구성하는 방법에 대해서는 102 페이지 "certmap.conf 파일 사용"을 참조하십시오.
- 인증서가 올바로 매핑된 경우 해당 사용자에 대해 설정된 ACL 규칙을 확인합니다. 인증서가 올바로 매핑된 경우라도 ACL 규칙에 따라 사용자 액세스를 거부할 수 있습니다.

특정 자원에 대한 액세스를 제어하기 위해 클라이언트 인증을 요구하는 경우는 서버에 대한 모든 연결에 대해 클라이언트 인증을 요구하는 경우와 다릅니다. 모든 연결에 대해 서버가 클라이언트 인증을 요구하도록 구성된 경우 클라이언트는 신뢰할 수 있는 인증 기관에서 발행한 유효한 인증서만 제시하면 됩니다. 서버가 SSL 방법을 사용하여 사용자 및 그룹을 인증하도록 구성된 경우 다음 작업을 수행해야 합니다.

- 클라이언트는 신뢰할 수 있는 인증 기관에서 발행한 유효한 인증서를 제공해야 합니다.
- 인증서는 반드시 LDAP의 유효한 사용자와 매핑되어야 합니다.
- 액세스 제어 목록이 반드시 적절히 평가해야 합니다.

액세스 제어와 함께 클라이언트 인증이 필요한 경우 Proxy Server용 SSL 암호를 사용하도록 설정해야 합니다. SSL 사용에 대한 자세한 내용은 5 장, "인증서 및 키 사용"을 참조하십시오.

SSL 인증이 요구되는 자원에 성공적으로 액세스하려면 Proxy Server가 신뢰할 수 있는 인증 기관으로부터 클라이언트 인증서가 발급되어야 합니다. Proxy Server의 `certmap.conf` 파일이 브라우저에 있는 클라이언트 인증서를 디렉토리 서버에 있는 클라이언트 인증서와 비교하도록 구성된 경우에는 클라이언트 인증서가 디렉토리 서버 내에 게시되어야 합니다. 그러나 `certmap.conf` 파일은 인증서의 선택된 정보만 디렉토리 서버 항목과 비교되도록 구성할 수 있습니다. 예를 들어 브라우저 인증서에 있는 사용자 아이디와 전자 메일 주소만 디렉토리 서버 항목과 비교하도록 `certmap.conf` 파일을 구성할 수 있습니다. `certmap.conf` 및 인증서 매핑에 대한 자세한 내용은 5 장, "인증서 및 키 사용"을 참조하십시오. 또한 **Sun Java System Web Proxy Server 4.0.8 Configuration File Reference**를 참조하십시오.

Digest 인증

Proxy Server가 LDAP 기반 또는 파일 기반 디렉토리 서비스를 사용하여 Digest 인증을 수행하도록 구성할 수 있습니다.

Digest 인증을 통해 사용자는 사용자 이름과 비밀번호를 일반 텍스트로 보내지 않고 사용자 이름과 비밀번호를 기반으로 인증할 수 있습니다. 브라우저는 MD5 알고리즘을 사용하여 Proxy Server가 제공하는 사용자 비밀번호와 일부 정보를 사용하는 다이제스트 값을 만듭니다.

서버가 LDAP 기반 디렉토리 서비스를 사용하여 Digest 인증을 수행하는 경우 이 다이제스트 값은 또한 Digest 인증 플러그인을 사용하는 서버 측에서 컴퓨팅되며 클라이언트가 제공하는 다이제스트 값과 비교됩니다. 다이제스트 값이 일치하면 사용자가 인증됩니다. 이렇게 하려면 디렉토리 서버가 일반 텍스트의 사용자 비밀번호에 액세스해야 합니다. Sun Java System Directory Server에는 역변환 가능한 비밀번호 플러그인이 있으며, 이는 데이터를 암호화된 형태로 저장하여 나중에 원래의 형태로 해독할 수 있는 대칭 암호화 알고리즘을 사용합니다. 오직 Directory Server만이 데이터의 키를 보유합니다.

LDAP 기반 인증의 경우 Proxy Server에 포함된 역변환 가능한 비밀번호 플러그인과 Digest 인증 관련 플러그인을 사용하도록 설정해야 합니다. Digest 인증을 처리하도록 Proxy Server를 구성하려면 *server-root*`/userdb/`에 있는 `dbswitch.conf` 파일에서 데이터베이스 정의의 `digestauth` 등록 정보를 설정합니다.

여기서는 샘플 dbswitch.conf 파일입니다.

```
directory default ldap://<host_name>:<port>
default:binddn cn=Directory Manager
default:encoded bindpw ***********
default:digestauth on
```

또는

```
directory default ldap://<host_name>:<port>/
default:binddn cn=Directory Manager
default:encoded bindpw ***********
default:digestauthstate on
```

서버는 141 페이지 “Digest 인증”에 보이는 것과 같이 지정된 ACL 방법에 기반하여 LDAP 데이터베이스에 대한 인증을 시도합니다. ACL 방법을 지정하지 않으면, 서버는 인증이 요구되는 경우 Digest 또는 Basic을 사용하며 인증이 요구되지 않는 경우 Basic을 사용합니다.

다음 표에서는 인증 데이터베이스에서 지원하거나 지원하지 않는 Digest 인증에 대해 나열합니다.

표 8–1 Digest 인증 질문 생성

ACL 방법	인증 데이터베이스에서 지원	인증 데이터베이스에서 지원하지 않음
Default 지정된 사항 없음	Digest 및 Basic	Basic
Basic	Basic	Basic
Digest	Digest	ERROR

`method=digest`로 설정된 ACL을 처리하는 경우 서버는 다음 작업을 수행하여 인증을 시도합니다.

- 인증 요청 헤더 확인. 헤더가 없는 경우 다이제스트 시도를 포함하는 401 응답이 생성되며 프로세스가 중지됩니다.
- 인증 유형 확인. 인증 유형이 Digest인 경우 서버는 다음 작업을 수행합니다.
  - nonce를 확인합니다. nonce가 유효하지 않은 경우 이 서버에서 새 nonce를 생성하고 401 응답이 생성되며 프로세스가 중지됩니다. nonce가 오래된 경우 `stale=true`로 설정된 401 응답이 생성되며 프로세스가 중지됩니다.

    server-root`/proxy-server_name/config/`에 위치한 `magnus.conf` 파일에 있는 `DigestStaleTimeout` 매개 변수의 값을 변경하여 nonce가 새로운 상태를 유지하는 시간을 구성할 수 있습니다. 이 값을 설정하려면 `magnus.conf`에 다음과 같은 줄을 추가합니다.

    `DigestStaleTimeout` *seconds*

    여기에서 *seconds*는 nonce가 새로운 상태를 유지하는 초 단위 시간입니다. 지정된 시간이 경과하면 nonce가 만기되며 사용자에 대한 새로운 인증이 요구됩니다.
  - 영역 확인. 영역이 일치하지 않는 경우 401 응답이 생성되며 프로세스가 중지됩니다.
  - 인증 디렉토리가 LDAP 기반인 경우 LDAP 디렉토리에 사용자가 있는지 확인하거나, 인증 디렉토리가 파일 기반인 경우 파일 데이터베이스에 사용자가 있는지 확인합니다. 사용자를 찾을 수 없는 경우 401 응답이 생성되며 프로세스가 중지됩니다.
  - 디렉토리 서버 또는 파일 데이터베이스에서 `request-digest` 값을 가져오고 클라이언트의 `request-digest` 와 일치하는지 확인합니다. 일치하지 않는 경우 401 응답이 생성되며 프로세스가 중지됩니다.
  - `Authorization-Info` 헤더를 만들고 이 헤더를 서버 헤더에 삽입합니다.

Digest 인증 플러그인 설치

LDAP 기반 디렉토리 서비스를 사용하는 Digest 인증의 경우 Digest 인증 플러그인을 설치해야 합니다. 이 플러그인은 서버 측에서 다이제스트 값을 계산하고 이 값을 클라이언트에서 제공하는 다이제스트 값과 비교합니다. 다이제스트 값이 일치하면 사용자가 인증됩니다.

파일 기반 인증 데이터베이스를 사용하는 경우 Digest 인증 플러그인을 설치할 필요는 없습니다.

UNIX에 Digest 인증 플러그인 설치

Digest 인증 플러그인은 다음 공유 라이브러리와 ldif 파일로 구성됩니다.

- `libdigest-plugin.lib`
- `libdigest-plugin.ldif`

▼ UNIX에 Digest 인증 플러그인을 설치하는 방법

시작하기 전에

- 이 공유 라이브러리가 Sun Java System Directory Server를 설치한 동일한 서버 컴퓨터에 있는지 확인합니다.
- Directory Manager 비밀번호가 올바른지 확인합니다.
- `libdigest-plugin.ldif` 파일의 `/path/to`에 대한 모든 참조를 다이제스트 플러그인 공유 라이브러리를 설치한 위치로 변경합니다.

● **플러그인을 설치하려면 다음 명령을 입력합니다.**

```
% ldapmodify -D "cn=Directory Manager" -w password -a < libdigest-plugin.ldif
```

Windows에 Digest 인증 플러그인 설치

Directory Server가 다이제스트 플러그인과 함께 제대로 시작되려면 여러 개의 `.dll` 파일을 프록시 서버 설치 위치에서 Directory Server용 Sun Java System Directory Server 서버 컴퓨터로 복사해야 합니다.

▼ Windows에 Digest 인증 플러그인을 설치하는 방법

1. ***server-root*`\bin\proxy\bin`에 있는 Proxy Server의 공유 라이브러리에 액세스합니다.**
2. **`nsldap32v50.dll`, `libspnr4.dll` 및 `libplds4.dll` 파일을 해당 디렉토리에 복사합니다.**
3. **복사한 파일을 다음 중 한 곳에 붙여넣습니다.**
   - `\Winnt\system32`
   - Sun Java System Directory Server 설치 디렉토리: *server-root*`\bin\sldap\server`

DES 알고리즘 사용을 위한 Sun Java System Directory Server 설정

DES 알고리즘을 위해 다이제스트 비밀번호가 저장된 속성을 암호화해야 합니다.

▼ DES 알고리즘을 사용하도록 Directory Server를 설정하는 방법

1. **Sun Java System Directory Server 콘솔을 시작합니다.**
2. **Sun ONE Directory Server 5.1 SP1 이상 버전의 인스턴스를 엽니다.**
3. **Configuration 탭을 선택합니다.**
4. **플러그인 옆의 + 기호를 누릅니다.**
5. **DES 플러그인을 선택합니다.**
6. **Add를 선택하여 새 속성을 추가합니다.**
7. **`iplanetReversiblePassword`를 입력합니다.**
8. **Save를 누릅니다.**
9. **Digest 인증 비밀번호를 설정합니다.**

주 – 서버는 객체 클래스 iplanetReversiblePassword에 있는 iplanetReversiblePassword 속성을 사용합니다. 사용자의 `iplanetReversiblePassword` 속성에서 Digest 인증 비밀번호를 사용하려면 항목에 `iplanetReversiblePasswordobject` 객체가 포함되어야 합니다.

`ldapmodify`를 사용하거나 Directory Server 관리 인터페이스를 사용하여 이를 수행할 수 있습니다.

`ldapmodify` 사용—

`digest.ldif` 파일을 만들어 LDAP 명령을 저장합니다. 비밀번호 추가 프로세스는 2단계로 구성되어 있습니다.

a. **객체 클래스를 `digest.ldif`에 추가합니다.**

   파일이 다음과 유사하게 표시됩니다(Directory Server 사용자 및 ACL을 기준으로 추가 `ldif` 파일을 가질 수 있음).

```
dn:uid=user1,dc=india,dc=sun,dc=com
changetype:modify
add:objectclass
objectclass:iplanetReversiblePasswordobject
```

```
dn:uid=user1,dc=india,dc=india,dc=sun,dc=com
changetype:modify
add:iplanetReversiblePassword
iplanetReversiblePassword:user1
```

b. `# ldapmodify -D  cn={CN_Value}  -w <password> -a <ldif_file_name>`

10 Sun Java System Directory Server 인스턴스를 다시 시작하고 사용자 속성이 Directory Server 데이터베이스에 추가되었는지 확인합니다.

기타 인증

액세스 제어 API를 사용하여 사용자 정의 인증 방법을 만들 수 있습니다.

호스트-IP용 액세스 제어

Administration Server와 해당 파일 및 디렉토리를 특정 컴퓨터를 이용하는 클라이언트만 사용할 수 있도록 설정하여 이에 대한 액세스를 제한할 수 있습니다. 허용 또는 거부하려는 컴퓨터의 호스트 이름 또는 IP 주소를 지정합니다. 호스트-IP 인증을 사용하는 파일 또는 디렉토리 액세스는 사용자가 알 수 없게 진행됩니다. 사용자는 사용자 이름 또는 비밀번호를 입력하지 않고 즉시 파일과 디렉토리에 액세스할 수 있습니다.

여러 사람이 특정 컴퓨터를 사용할 수 있으므로 호스트-IP 인증은 사용자 그룹 인증과 함께 사용할 때 더 효과적입니다. 두 가지 인증 방법이 모두 사용되는 경우 액세스할 때 사용자 이름과 비밀번호가 필요합니다.

호스트-IP 인증의 경우 서버에서 DNS(Domain Name Service)를 구성할 필요가 없습니다. 호스트-IP 인증을 선택한 경우 반드시 DNS가 네트워크에서 실행되어야 하며 서버가 이를 사용하도록 구성되어야 합니다. DNS를 사용하도록 설정하려면 서버의 Server Manager에 액세스하고 Preferences 탭을 누른 다음 Configure System Preferences를 누릅니다. DNS 설정을 확인합니다.

DNS를 사용하도록 설정하면 서버가 DNS 조회를 수행해야 하므로 Proxy Server의 성능이 저하됩니다. DNS 조회가 서버 성능에 미치는 영향을 줄이려면 모든 요청에 대해 IP 주소를 확인하는 대신 액세스 제어 및 CGI의 IP 주소만 확인합니다. 이러한 제한을 설정하려면 `obj.conf`에서 다음을 지정합니다.

```
AddLog fn="flex-log" name="access" iponly=1
```

액세스 제어 파일 사용

Administration Server 또는 서버의 파일이나 디렉토리에서 액세스 제어를 사용하는 경우 해당 설정은 확장자가 `.acl`인 파일에 저장됩니다. 액세스 제어 파일이 디렉토리

server-root/httpacl에 저장되며 여기서 *server-root*는 서버가 설치된 위치입니다. 예를 들어 서버를 /usr/Sun/Servers에 설치한 경우 Administration Server와 서버에 구성된 각 서버 인스턴스용 ACL 파일의 위치는 /usr/Sun/Servers/httpacl/입니다.

기본 ACL 파일은 generated-proxy-*serverid* .acl입니다. 임시 작업 파일은 genwork-proxy-*serverid* .acl입니다. Administration Server를 사용하여 액세스를 구성하는 경우 이 두 파일이 만들어집니다. 그러나 제한을 더욱 복잡하게 하려면 여러 개의 파일을 만들고 server.xml 파일에서 이러한 파일을 참조할 수 있습니다. 또한 하루 중 시간 또는 요일을 기준으로 서버에 대한 액세스를 제한하는 등, 파일을 편집할 때에만 사용할 수 있는 몇 가지 기능이 있습니다.

액세스 제어 파일 및 구문에 대한 자세한 내용은 18 장, “ACL 파일 구문”을 참조하십시오. server.xml에 대한 자세한 내용은 **Sun Java System Web Proxy Server 4.0.8 Configuration File Reference**를 참조하십시오.

ACL 사용자 캐시 구성

기본적으로 Proxy Server는 ACL 사용자 캐시에서 사용자 및 그룹 인증 결과를 캐시합니다. magnus.conf 파일에서 ACLCacheLifetime 지시문을 사용하여 ACL 사용자 캐시의 유효 시간을 제어할 수 있습니다. 캐시에 있는 항목이 참조될 때마다 시간이 계산되고 ACLCacheLifetime과 비교됩니다. 항목의 시간이 ACLCacheLifetime과 같거나 크면 해당 항목은 사용되지 않습니다. 기본값은 120초입니다. 값을 0으로 설정하면 캐시가 Off로 설정됩니다. 이 값에 큰 값을 사용하면 LDAP 항목을 변경할 때마다 Proxy Server를 다시 시작해야 합니다. 예를 들어 이 값을 120초로 설정하는 경우 최대 2분까지 Proxy Server가 LDAP 디렉토리와 동기화되지 않을 수 있습니다. LDAP 디렉토리가 자주 변경되지 않는 경우에만 큰 값을 사용하십시오.

ACLUserCacheSize의 magnus.conf 매개 변수를 사용하여 캐시에 유지할 항목의 최대 수를 구성할 수 있습니다. 이 매개 변수의 기본값은 200입니다. 새 항목은 목록의 앞에 추가되며 목록의 끝에 있는 항목은 캐시가 최대 크기에 도달하면 재활용되어 새로운 항목이 됩니다.

또한 magnus.conf 매개 변수 ACLGroupCacheSize를 사용하여 사용자 항목당 캐시할 수 있는 최대 그룹 구성원 수를 설정할 수 있습니다.. 이 매개 변수의 기본값은 4입니다. 그룹에 있는 사용자가 구성원이 아닌 경우 캐시되지 않으며, 요청마다 여러 LDAP 디렉토리 액세스가 발생하게 됩니다.

클라이언트 인증서로 액세스 제어

서버에서 SSL을 사용하도록 설정하면 액세스 제어와 함께 클라이언트 인증서를 사용할 수 있습니다. 특정 자원에 액세스하려면 클라이언트 인증서가 필요하도록 지정해야 합니다. 이 기능을 서버에서 사용하도록 설정하면 인증서가 있는 사용자는 처음으로 제한된 자원에 액세스하는 경우에만 사용자 이름과 비밀번호를 입력합니다. 아이디가

설정되면 서버는 사용자의 로그인 이름과 비밀번호를 관련 인증서에 매핑합니다. 이 때부터 사용자는 클라이언트 인증이 필요한 자원에 액세스할 때 더 이상 로그인 이름 또는 비밀번호를 입력할 필요가 없습니다.

사용자가 제한된 자원에 액세스하려는 경우 클라이언트는 서버에 클라이언트 인증서를 보내고 서버는 이를 매핑 목록과 비교하여 확인합니다. 인증서가 액세스 권한이 부여된 사용자에 속한 경우 자원이 제공됩니다.

특정 자원에 대한 액세스를 제어하는 용도로 필요한 클라이언트 인증은 서버에 대한 모든 연결에 대해 클라이언트 인증을 요구하는 것과는 다릅니다. 또한 모든 SSL 연결에 대해 클라이언트 인증서를 요구하는 경우 자동으로 인증서가 데이터베이스의 사용자에게 매핑되지 않습니다. 이 매핑을 설정하려면 특정 자원에 액세스하기 위해 클라이언트 인증서가 필요하도록 지정해야 합니다.

액세스 제어 작동 방법

서버가 페이지에 대한 요청을 수신하면 ACL 파일의 규칙을 사용하여 액세스 권한을 부여해야 하는지 여부를 결정합니다. 규칙은 요청을 보내는 컴퓨터의 호스트 이름 또는 IP 주소를 참조할 수 있습니다. 또한 LDAP 디렉토리에 저장된 사용자 및 그룹을 참조할 수 있습니다.

다음 예에서는 ACL 파일의 가능한 내용을 표시하고 액세스 제어 규칙에 대한 예를 제공합니다.

```
version 3.0;
# The following "es-internal" rules protect files such
# as icons and images related to Sun Java System Web Proxy Server.
# These "es-internal" rules should not be modified.
  acl "es-internal";
  allow (read, list, execute,info) user = "anyone";
  deny (write, delete) user = "anyone";

# The following rules deny access to the directory "web"
# to everyone not in the directory server and deny everyone
# in the directory server who is not in GroupB.
# Only the users in GroupB are allowed read, execute, list,
# and info permissions. GroupA cannot gain access to the
# directory "web" even though (in the ACL rule below) they
# can access the directory   my_stuff  . Furthermore, members
# of GroupB cannot write or delete files.
  acl "path=/export/user/990628.1/docs/my_stuff/web/";
  authenticate (user,group) {
     database = "default";
     method = "basic";
  };
  deny (all)
```

```
  (user = "anyone");

  allow (read,execute,list,info)
  (group = "GroupB");

# The following rule denies everyone not in the directory
# server and denies everyone in the directory server except
# users with the ID of "SpecificMemberOfGroupB". The ACL rule
# in this setting also has a requirement that the user
# connect from a specific IP address. The IP address setting
# in the rule is optional, and has been added for extra
# security. Also, this ACL rule has a Customized prompt
# of "Presentation Owner". This Customized prompt appears
# in the username and password dialog box in the client's
# browser.

  acl "path=/export/user/990628.1/docs/my_stuff/web/presentation.html";
  authenticate (user,group) {
     database = "default";
     method = "basic";
     prompt = "Presentation Owner";
  };
  deny (all)
  (user = "anyone" or group = "my_group");
  allow (all)
  (user = "SpecificMemberOfGroupB") and
  (ip = "208.12.54.76");

# The following ACL rule denies everyone not in the directory
# server and everyone in the directory server except for
# GroupA and GroupB access to the directory   my_stuff
  acl "path=/export/user/990628.1/docs/my_stuff/";
  authenticate (user,group) {
     database = "default";
     method = "basic";
  };
  deny (all)
  (user = "anyone");
  allow (read,execute,list,info)
  (group = "GroupA,GroupB");
```

예를 들어 사용자가 URL `http://server_name/my_stuff/web/presentation.html` 을 요청하면 Proxy Server는 먼저 전체 서버에 대한 액세스 제어를 확인합니다. 전체 서버용 ACL이 계속으로 설정된 경우 서버는 `my_stuff` 디렉토리용 ACL을 확인합니다. ACL이 존재하면 서버는 ACL에 있는 ACE를 확인한 후, 다음 디렉토리로 이동합니다. 이

프로세스는 액세스를 거부하는 ACL이 발견되거나 요청된 URL에 대한 마지막 ACL(이 경우에는 `presentation.html` 파일)에 도달할 때까지 계속됩니다.

Server Manager를 사용하여 이 예에서의 액세스 제어를 설정하려면 파일 전용 또는 파일로 유도되는 각 자원용 ACL을 만들 수 있습니다. 즉, 전체 서버용 1개, `my_stuff` 디렉토리용 1개, `my_stuff/web` 디렉토리용 1개 및 해당 파일용 1개를 만들 수 있습니다.

일치되는 ACL이 둘 이상인 경우 서버는 일치되는 마지막 ACL문을 사용합니다.

액세스 제어 설정

이 절에서는 액세스를 제한하는 프로세스에 대해 설명합니다. 모든 서버에 대한 전역 액세스 제어 규칙을 설정할 수도 있고 특정 서버에 대한 개별 규칙을 설정할 수도 있습니다. 예를 들어 인력 관리 부서에서는 모든 인증된 사용자가 자신의 연봉 데이터를 볼 수 있으나 오직 인력 관리 부서의 연봉을 담당하는 직원만 데이터를 업데이트할 수 있도록 제한하는 ACL을 만들 수 있습니다.

이 절은 다음 내용으로 구성되어 있습니다.

- 149 페이지 “전역 액세스 제어 설정”
- 151 페이지 “서버 인스턴스용 액세스 제어 설정”

주 – 전역 액세스 제어를 설정하기 전에 반드시 분산 관리를 구성하고 사용해야 합니다.

전역 액세스 제어 설정

▼ 모든 서버에 대해 액세스 제어를 설정하는 방법

1 Administration Server에 액세스하고 Global Settings 탭을 누릅니다.

2 Administer Access Control 링크를 누릅니다.

3 드롭다운 목록에서 관리 서버(`proxy-admserv`)를 선택하고 Go to load data를 누른 다음 New ACL(또는 Edit ACL)을 누릅니다.

4 메시지가 표시되면 인증합니다.

Access Control Rules For 페이지가 표시됩니다. Administration Server에는 편집할 수 없는 기본 액세스 제어 규칙이 두 줄 있습니다.

5 아직 선택되지 않았으면 Access Control Is On을 선택합니다.

6 **표의 하단에 기본 ACL 규칙을 추가하려면 New Line 버튼을 누릅니다.**
액세스 제어 제한 위치를 변경하려면 위쪽 또는 아래쪽 화살표를 누릅니다.

7 **Users/Groups 열에서 Anyone을 누릅니다.**
User/Group 페이지가 아래의 창에 표시됩니다.

8 **액세스를 허용할 사용자 및 그룹을 선택하고 Update를 누릅니다.**
그룹 또는 사용자에 대해 List 버튼을 누르면 선택할 목록이 표시됩니다. 설정에 대한 자세한 내용은 온라인 도움말을 참조하십시오. 또한 154 페이지 "사용자 및 그룹 지정"을 참조하십시오.

9 **From Host 열에서 아무 곳이나 누릅니다.**
From Host 페이지가 아래의 창에 표시됩니다.

10 **액세스가 허용된 호스트 이름 및 IP 주소를 지정한 후 Update를 누릅니다.**
설정에 대한 자세한 내용은 온라인 도움말을 참조하십시오. 또한 155 페이지 "송신 호스트 지정"을 참조하십시오.

11 **Programs 열에서 All을 누릅니다.**
Programs 페이지가 아래의 창에 표시됩니다.

12 **액세스를 허용할 Program Groups를 선택하거나 Program Items 필드에 특정 파일 이름을 입력하고 Update를 누릅니다.**
설정에 대한 자세한 내용은 온라인 도움말을 참조하십시오. 또한 156 페이지 "프로그램에 대한 액세스 제한"을 참조하십시오.

13 **(선택 사항) 사용자 정의 ACL 표현식을 추가하려면 Extra 열 아래의 X를 누릅니다.**
Customized Expressions 페이지가 아래의 창에 표시됩니다. 자세한 내용은 157 페이지 "사용자 정의 표현식 작성"을 참조하십시오.

14 **아직 선택하지 않은 경우 Continue 열에서 확인란을 선택합니다.**
서버는 사용자의 액세스 허용 여부를 결정하기 전에 다음 줄을 확인합니다. 여러 줄을 만드는 경우에는 가장 일반적인 제한에서 가장 국부적인 제한으로 진행합니다.

15 **(선택 사항) 액세스 제어 규칙에서 해당 라인을 삭제하려면 휴지통 아이콘을 누릅니다.**

16 **(선택 사항) 액세스가 거부되었을 때 사용자가 수신하는 응답을 지정하려면 Response When Denied 링크를 누릅니다.**
Access Deny Response 페이지가 아래의 창에 표시됩니다.

a. **원하는 응답을 선택합니다.**

b. 해당하는 경우 추가 정보를 지정합니다.

c. Update를 누릅니다.

설정에 대한 자세한 내용은 158 페이지 "액세스가 거부된 경우의 응답"을 참조하십시오.

17 ACL 파일에서 새 액세스 제어 규칙을 저장하려면 Submit를 누르고 변경을 적용하기 전에 포함된 값으로 페이지의 요소를 재설정하려면 Revert를 누릅니다.

서버 인스턴스용 액세스 제어 설정

Server Manager를 사용하여 특정 서버 인스턴스용 액세스 제어를 만들거나 편집 또는 삭제할 수 있습니다. 삭제하는 경우 ACL 파일에서 ACL 규칙을 모두 삭제하면 안 됩니다. 서버를 시작하려면 ACL 규칙을 한 개 이상 포함하는 ACL 파일이 적어도 하나 이상 있어야 합니다. ACL 규칙을 모두 삭제하고 서버를 재시작하면 구문 오류가 발생합니다.

▼ 서버 인스턴스용 액세스 제어를 설정하는 방법

1 서버 인스턴스에 대한 Server Manager에 액세스하고 Preferences 탭을 누릅니다.

2 Administer Access Control 링크를 누릅니다.

3 다음 방법 중 하나를 사용하여 ACL을 선택합니다.

- Select A Resource 드롭다운 목록에서 액세스를 제한하기 위해 ACL을 사용하는 자원을 선택하거나 Regular Expression을 눌러 정규 표현식을 지정합니다. 자세한 내용은 Proxy Server **관리 설명서**에서 16 장, "템플리트 및 자원 관리"를 참조하십시오.
- 사용하도록 설정된 모든 ACL을 나열하는 기존 ACL 목록을 선택합니다.

  사용하도록 설정하지 않은 기존 ACL은 목록에 표시되지 않습니다. 드롭다운 목록에서 ACL을 선택합니다.
- Type In The ACL Name . 이 옵션을 사용하여 명명된 ACL을 작성할 수 있습니다. 이 옵션은 ACL 파일에 익숙한 경우에만 사용하십시오. 명명된 ACL을 자원에 적용하려는 경우에는 `obj.conf`를 직접 편집해야 합니다. 자세한 내용은 18 장, "ACL 파일 구문"을 참조하십시오.

4 해당 Edit 버튼을 누릅니다.

Access Control Rules For 페이지가 표시됩니다.

5 아직 선택되지 않았으면 Access Control Is On을 선택합니다.

6 표의 하단에 기본 ACL 규칙을 추가하려면 New Line 버튼을 누릅니다.

액세스 제어 제한 위치를 변경하려면 위쪽 또는 아래쪽 화살표를 누릅니다.

7 **이 서버 인스턴스용 ACL을 편집하려면 Action 열에서 작업을 누릅니다.**
Allow/Deny 페이지가 아래의 창에 표시됩니다.

8 **Allow가 아직 기본값으로 선택되지 않았으면 선택하고 Update를 누릅니다.**
Allow 또는 Deny에 대한 자세한 내용은 153 페이지 "작업 설정"을 참조하십시오.

9 **Users/Groups 열에서 Anyone을 누릅니다. User/Group 페이지가 아래의 창에 표시됩니다.**

10 **액세스를 허용할 사용자와 그룹을 선택하고 인증 정보를 지정한 다음 Update를 누릅니다.**
그룹 또는 사용자에 대한 List 버튼을 누르면 선택할 목록이 표시됩니다. 설정에 대한 자세한 내용은 온라인 도움말을 참조하십시오. 또한 154 페이지 "사용자 및 그룹 지정"을 참조하십시오.

11 **From Host 열에서 아무 곳이나 누릅니다.**
From Host 페이지가 아래의 창에 표시됩니다.

12 **액세스가 허용된 호스트 이름 및 IP 주소를 지정한 후 Update를 누릅니다.**
설정에 대한 자세한 내용은 온라인 도움말을 참조하십시오. 또한 155 페이지 "송신 호스트 지정"을 참조하십시오.

13 **Rights 열에서 All을 누릅니다.**
Access Rights 페이지가 아래의 창에 표시됩니다.

14 **이 사용자에 대한 액세스 권한을 지정하고 Update를 누릅니다.**
자세한 내용은 156 페이지 "프로그램에 대한 액세스 제한"을 참조하십시오.

15 **(선택 사항) 사용자 정의 ACL 표현식을 추가하려면 Extra 열 아래의 X를 누릅니다.**
Customized Expressions 페이지가 아래의 창에 표시됩니다. 자세한 내용은 157 페이지 "사용자 정의 표현식 작성"을 참조하십시오.

16 **아직 선택하지 않은 경우 Continue 열에서 확인란을 선택합니다.**
서버는 사용자의 액세스 허용 여부를 결정하기 전에 다음 줄을 확인합니다. 여러 줄을 만드는 경우에는 가장 일반적인 제한에서 가장 국부적인 제한으로 진행합니다.

17 **(선택 사항) 액세스 제어 규칙에서 해당 라인을 삭제하려면 휴지통 아이콘을 누릅니다.**
ACL 파일에서 ACL 규칙을 모두 삭제하면 안 됩니다. 서버를 시작하려면 ACL 규칙을 최소한 한 개 이상 포함하는 ACL 파일이 적어도 하나 이상 있어야 합니다. ACL 파일에서 ACL 규칙을 모두 삭제하고 서버를 재시작하면 구문 오류가 발생합니다.

18 (선택 사항) 액세스가 거부되었을 때 사용자가 수신하는 응답을 지정하려면 Response When Denied 링크를 누릅니다.

Access Deny Response 페이지가 아래의 창에 표시됩니다. 원하는 응답을 선택하고 해당하는 경우 추가 정보를 지정한 다음 Update를 누릅니다. 설정에 대한 자세한 내용은 158 페이지 "액세스가 거부된 경우의 응답"을 참조하십시오.

19 ACL 파일에서 새 액세스 제어 규칙을 저장하려면 Submit를 누르고 변경을 적용하기 전에 포함된 값으로 페이지의 요소를 재설정하려면 Revert를 누릅니다.

액세스 제어 옵션 선택

다음 항목에서는 액세스 제어를 설정할 때 선택할 수 있는 다양한 옵션에 대해 설명합니다. Administration Server의 경우 첫 두 줄은 기본으로 설정되며 편집할 수 없습니다.

이 절은 다음 내용으로 구성되어 있습니다.

- 153 페이지 "작업 설정"
- 154 페이지 "사용자 및 그룹 지정"
- 155 페이지 "송신 호스트 지정"
- 156 페이지 "프로그램에 대한 액세스 제한"
- 157 페이지 "액세스 권한 설정"
- 157 페이지 "사용자 정의 표현식 작성"
- 158 페이지 "액세스 제어 사용 안 함"
- 158 페이지 "액세스가 거부된 경우의 응답"

작업 설정

요청이 액세스 제어 규칙과 일치할 때 서버의 작동을 지정할 수 있습니다.

- **Allow**: 사용자 또는 시스템이 요청된 자원에 액세스할 수 있습니다.
- **Deny**: 사용자 또는 시스템이 자원에 액세스할 수 없습니다.

서버는 액세스 제어 항목(ACE) 목록 전체를 확인하여 액세스 권한을 판단합니다. 예를 들어 첫 번째 ACE는 보통 모든 사용자를 거부합니다. 첫 번째 ACE를 Continue로 설정할 경우 서버는 목록에서 두 번째 ACE를 확인합니다. 해당 ACE가 일치하면 다음 ACE가 사용됩니다. Continue가 선택되지 않은 경우 자원에 대한 모든 사용자의 액세스가 거부됩니다. 서버는 일치되지 않는 ACE를 발견하거나 일치되지만 계속으로 설정되지 않은 ACE를 발견할 때까지 계속해서 목록을 검색합니다. 마지막으로 일치되는 ACE에 따라 액세스의 허용 또는 거부가 결정됩니다.

사용자 및 그룹 지정

사용자 및 그룹 인증을 사용하면 사용자가 액세스 제어 규칙에 지정된 자원에 액세스하기 전에 사용자 이름 및 비밀번호를 입력하라는 프롬프트가 표시됩니다.

Proxy Server는 Sun Java System Directory Server 등의 LDAP 서버 또는 내부 파일 기반 인증 데이터베이스에 저장된 사용자 및 그룹 목록을 확인합니다.

데이터베이스에 있는 모든 사용자의 액세스를 허용 또는 거부할 수 있으며, 와일드카드 패턴을 사용하여 특정 사용자를 허용 또는 거부할 수 있습니다. 또는 사용자 및 그룹 목록에서 허용 또는 거부할 사용자를 선택할 수 있습니다.

사용자 인터페이스에서 Access Control Rules For 페이지의 Users/Groups에 다음 요소가 표시됩니다.

- **Anyone (No Authentication)**은 기본값으로, 모든 사용자가 사용자 이름 또는 비밀번호를 제공하지 않고 자원에 액세스할 수 있습니다. 그러나 호스트 이름 또는 IP 주소 등의 기타 설정에 따라 액세스를 거부할 수 있습니다. Administration Server의 경우 이 설정으로 분산 관리로 지정한 관리 그룹의 모든 사용자가 페이지에 액세스할 수 있습니다.
- **Authenticated People Only**
  - **인증 데이터베이스의 모든 사용자**는 데이터베이스에 항목이 있는 임의 사용자를 일치시킵니다.
  - **Only The following People**의 경우 일치하는 사용자 및 그룹을 지정합니다. 사용자 또는 사용자 그룹의 목록을 만들 수 있으며 각 항목을 쉼표로 분리하거나, 와일드카드 패턴을 사용할 수 있습니다. 또는 데이터베이스에 저장된 사용자 및 그룹 목록에서 선택할 수 있습니다. **Group**의 경우 지정한 그룹의 모든 사용자를 검색합니다. **User**는 지정한 개별 사용자를 검색합니다. Administration Server의 경우 사용자는 반드시 분산된 관리용으로 지정한 관리 그룹에 속해야 합니다.

  인증 확인 프롬프트는 인증 대화 상자에 표시된 메시지 텍스트를 지정합니다. 이 텍스트를 사용하여 사용자가 입력해야 하는 내용을 설명할 수 있습니다. 운영 체제에 따라 사용자는 프롬프트의 처음 40자 정도만 볼 수 있습니다. 대부분의 브라우저는 사용자 이름과 비밀번호를 캐시하고 프롬프트 텍스트에 연결합니다. 사용자가 동일한 프롬프트를 가진 서버 파일과 디렉토리의 영역에 액세스하는 경우 사용자는 사용자 이름과 비밀번호를 다시 입력할 필요가 없습니다. 반대로 영역마다 사용자가 인증하도록 하려면 반드시 해당 자원의 ACL용 프롬프트를 변경해야 합니다.
- *Authentication Methods*에서는 클라이언트로부터 인증 정보를 가져오기 위해 서버가 사용할 방법을 지정합니다. Administration Server의 경우 Basic 인증 방법만 제공합니다. Server Manager는 다음 방법을 제공합니다.
  - *Default*는 `obj.conf` 파일에 지정된 기본 방법을 사용하거나 `obj.conf`에 설정이 없는 경우 Basic을 사용합니다. Default를 선택하는 경우 ACL 규칙은 ACL 파일에 방법을 지정하지 않습니다. Default를 선택하면 `obj.conf` 파일에서 한 줄만 편집하여 모든 ACL에 대한 인증 방법을 쉽게 변경할 수 있습니다.

- *Basic*은 HTTP 메소드를 사용하여 클라이언트에서 인증 정보를 가져옵니다. 서버에 대해 암호화를 사용하는 경우(SSL 사용) 사용자 이름과 비밀번호만 암호화됩니다. 그렇지 않을 경우 이름과 비밀번호가 일반 텍스트로 전송되므로 포착될 경우 읽을 수 있습니다.
- *SSL*은 클라이언트 인증서를 사용하여 사용자를 인증합니다. 이 방법을 사용하려면 반드시 서버용에 SSL을 사용해야 합니다. 암호화를 사용하는 경우 Basic과 SSL 방법을 함께 사용할 수 있습니다.

주 – 역방향 프록시 모드에서만 보안을 사용할 수 있으며 순방향 프록시 모드에서는 사용할 수 없습니다.

- *Digest*는 사용자 이름과 비밀번호를 일반 텍스트로 전송하지 않고 브라우저가 사용자 이름과 비밀번호를 기준으로 인증할 수 있게 하는 인증 기법을 사용합니다. 브라우저는 MD5 알고리즘을 이용하여 Proxy Server가 제공하는 사용자의 비밀번호 및 일부 정보를 사용하는 다이제스트 값을 만듭니다. 다이제스트 값은 또한 Digest 인증 플러그인을 사용하는 서버 측에서도 계산되며 이 값은 클라이언트가 제공하는 다이제스트 값과 비교됩니다.

주 – 인증 확인 프롬프트는 Digest 인증에 필요한 매개 변수입니다. 영역과 일치하는 값을 변경합니다(다이제스트 파일의 경우 필수). 예를 들어 다이제스트 파일에서 영역 *test*에 모든 사용자가 있도록 구성한 경우 인증 확인 프롬프트 필드에 텍스트 *test*가 포함되어야 합니다.

- *Other*는 액세스 제어 API를 사용하여 만든 사용자 정의 방법을 사용합니다.

인증 데이터베이스는 서버가 사용자를 인증하는 데 사용할 데이터베이스를 지정합니다. 이 옵션은 오직 Server Manager를 통하여만 사용할 수 있습니다. Default를 선택하는 경우 서버는 기본으로 구성된 디렉토리 서비스에서 사용자 및 그룹을 찾습니다. 개별 ACL이 서로 다른 데이터베이스를 사용하도록 구성하려는 경우 Other를 선택하고 데이터베이스를 지정합니다. 기본이 아닌 데이터베이스와 LDAP 디렉토리는 이미 *server-root*`/userdb/dbswitch.conf`에 지정되어 있어야 합니다. 사용자 정의 데이터베이스에 대해 액세스 제어 API를 사용하는 경우 Other를 선택하고 데이터베이스 이름을 입력합니다.

송신 호스트 지정

요청을 보내는 컴퓨터를 기준으로 Administration Server에 대한 액세스를 제한할 수 있습니다.

사용자 인터페이스의 From Host on the Access Control Rules For 페이지에 다음 요소가 표시됩니다.

- Anyplace는 모든 사용자 및 시스템의 액세스를 허용
- 다음 위치에서만은 특정 호스트 이름 또는 IP 주소로 액세스 제한

다음 위치에서만 옵션을 선택하면 호스트 이름 또는 IP 주소 필드에 와일드카드 패턴 또는 쉼표로 분리된 목록을 입력합니다. 호스트 이름을 기준으로 제한하는 것이 IP 주소를 기준으로 제한하는 것보다 훨씬 유연합니다. 사용자의 IP 주소가 변경되더라도 목록을 업데이트할 필요가 없습니다. 그러나 IP 주소를 기준으로 제한하는 것이 더욱 안전합니다. 연결된 클라이언트에 대한 DNS 조회가 실패하면 호스트 이름 제한은 사용할 수 없습니다.

컴퓨터의 호스트 이름 또는 IP 주소를 검색하는 와일드카드 패턴에는 * 와일드카드만 사용할 수 있습니다. 예를 들어 특정 도메인에 있는 모든 컴퓨터를 허용하거나 거부하려면 해당 도메인에 있는 모든 호스트에 일치하는 와일드카드 패턴(예: `*.example.com`)을 입력합니다. Administration Server에 액세스하는 수퍼유저를 위해 다른 호스트 이름 및 IP 주소를 설정할 수 있습니다.

호스트 이름의 경우 *는 반드시 이름의 전체 구성 요소를 대체해야 합니다. 즉, `*.example.com`은 사용 가능하지만 `*users.example.com`은 사용할 수 없습니다. 호스트 이름에 *를 사용하는 경우 가장 왼쪽에 표시해야 합니다. 예를 들어 `*.example.com`은 사용할 수 있지만 `users.*.com`은 사용할 수 없습니다.

IP 주소의 경우 *는 반드시 주소의 전체 바이트를 대체해야 합니다. 예를 들어 `198.95.251.*`는 사용 가능하지만 `198.95.251.3*`는 사용할 수 없습니다. IP 주소에 *를 사용하는 경우 가장 오른쪽에 표시해야 합니다. 예를 들어 `198.*`는 사용할 수 있지만 `198.*.251.30`은 사용할 수 없습니다.

프로그램에 대한 액세스 제한

프로그램에 대한 액세스는 오직 Administration Server에 의하여 제한될 수 있습니다. 프로그램에 대한 액세스를 제한하면 오직 지정된 사용자만 Server Manager 페이지를 볼 수 있으며 이러한 사용자가 해당 서버를 구성할 수 있는지 판단할 수 있습니다. 예를 들어 일부 관리자가 Administration Server의 Users and Groups 섹션을 구성할 수는 있으나 Global Settings 섹션에는 액세스할 수 없도록 설정할 수 있습니다.

서로 다른 사용자가 서로 다른 기능 영역에 액세스하도록 구성할 수 있습니다. 사용자가 몇 가지 선택된 기능 영역에 액세스하도록 설정되고 해당 사용자가 로그인하면, 오직 해당 사용자에게 액세스를 허용한 기능 영역의 Administration Server 페이지만 볼 수 있습니다.

사용자 인터페이스의 Access Control Rules For 페이지에서 Programs에 대해 다음 요소가 표시됩니다.

- All Programs는 모든 프로그램에 대한 액세스를 허용 또는 거부합니다. 기본적으로 관리자는 서버의 모든 프로그램에 액세스할 수 있습니다.
- Only The Following을 사용하여 사용자가 액세스 권한을 가진 프로그램을 지정할 수 있습니다.

- **Program Groups**는 Preferences 및 Global Settings 등과 같이 Administration Server의 탭으로, 해당 페이지에 대한 액세스를 나타냅니다. 관리자가 Administration Server에 액세스하면 서버는 사용자 이름, 호스트 및 IP 주소를 사용하여 표시할 수 있는 페이지를 결정합니다.
- Program Items를 통해 필드에 페이지 이름을 입력하여 프로그램 내에서 특정 페이지에 대한 액세스를 제어할 수 있습니다.

액세스 권한 설정

액세스 권한은 오직 Server Manager가 서버 인스턴스에 대해 설정합니다. 액세스 권한은 서버의 파일 및 디렉토리에 대한 액세스를 제한합니다. 모든 액세스 권한을 허용 또는 거부하는 것 외에 부분적인 액세스 권한을 허용 또는 거부하는 규칙을 지정할 수 있습니다. 예를 들어 사용자에게 파일에 대한 읽기 전용 액세스 권한을 부여하여 정보를 볼 수는 있지만 파일을 변경할 수는 없도록 할 수 있습니다.

다음 요소는 사용자 인터페이스의 Access Control Rules For 페이지에서 권한에 표시됩니다.

- 모든 액세스 권한은 기본값으로, 모든 권한을 허용 또는 거부합니다.
- **다음 권한만**을 사용하여 허용 또는 거부할 권한을 함께 선택할 수 있습니다.
  - **읽기**는 HTTP 메소드 GET, HEAD, POST 및 INDEX를 포함하여 사용자가 파일을 보도록 허용합니다.
  - **쓰기**는 HTTP 메소드 PUT, DELETE, MKDIR, RMDIR 및 MOVE를 포함하여 사용자가 파일을 변경하거나 삭제하도록 허용합니다. 파일을 삭제하려면 사용자에게 반드시 쓰기 및 삭제 권한이 있어야 합니다.
  - **실행**은 CGI 프로그램, Java 애플릿 및 에이전트와 같이 사용자가 서버 측 응용 프로그램을 실행하도록 허용합니다.
  - **삭제**는 쓰기 권한을 가진 사용자가 파일 또는 디렉토리를 삭제하도록 허용합니다.
  - **목록**은 사용자가 `index.html` 파일을 포함하지 않은 디렉토리의 파일 목록에 액세스하도록 허용합니다.
  - **정보**는 예를 들어 `http_head`와 같은 URI에 대한 정보를 사용자가 수신하도록 허용합니다.

사용자 정의 표현식 작성

ACL용 사용자 정의 표현식을 입력할 수 있습니다. 오직 ACL 파일의 구문과 구조에 익숙한 경우에만 이 옵션을 선택하십시오. ACL 파일을 편집하거나 사용자 정의 표현식을 만들 때에만 사용할 수 있는 몇 가지 기능이 있습니다. 예를 들어 하루 중 시간, 요일 또는 이 둘 모두를 기준으로 서버에 대한 액세스를 제한할 수 있습니다.

다음 사용자 정의 표현식에서는 하루 중 시간 및 요일을 기준으로 액세스를 제한할 수 있는 방법을 보여 줍니다. 이 예에서는 LDAP 디렉토리에 두 개의 그룹이 있는 것으로 가정합니다. Regular 그룹은 월요일부터 금요일까지 오전 8시부터 오후 5시 사이에 액세스할 수 있습니다. Critical 그룹은 항상 액세스할 수 있습니다.

```
allow (read){(group=regular and dayofweek=  mon,tue,wed,thu,fri  );
(group=regular and (timeofday>=0800 and timeofday<=1700));(group=critical)}
```

유효한 구문 및 ACL 파일에 대한 자세한 내용은 18 장, “ACL 파일 구문”을 참조하십시오.

액세스 제어 사용 안 함

Access Control Rules For 페이지에서 Access Control Is On 옵션을 선택 취소하면 ACL에서 레코드를 삭제할지 여부를 묻는 프롬프트가 표시됩니다. 확인을 누르면 해당 자원의 ACL 항목이 ACL 파일에서 삭제됩니다.

ACL을 비활성화하려면 각 줄의 시작 부분에서 # 기호를 사용하여 파일 `generated-proxy-` *serverid* `.acl`에서 ACL 줄을 주석으로 처리합니다.

Administration Server에서 특정 서버 인스턴스에 대한 액세스 제어를 만들어 사용하며 기타 서버에 대해는 사용하지 않도록(기본값) 할 수 있습니다. 예를 들어 Administration Server의 Server Manager 페이지에서 모든 액세스를 거부할 수 있습니다. 기타 서버는 기본적으로 분산 관리를 사용하고 액세스 제어는 사용하지 않으므로 관리자는 다른 서버에 액세스하여 구성할 수 있으나 Administration Server는 구성할 수 없습니다.

액세스가 거부된 경우의 응답

Proxy Server는 액세스가 거부된 경우 기본 메시지를 제공하고 원하는 경우 응답을 사용자 정의할 수 있습니다. 또한 각 액세스 제어 객체마다 서로 다른 메시지를 만들 수 있습니다.

Administration Server의 경우 기본적으로사용자는 *server-root*`/httpacl/admin-denymsg.html` 에서 권한이 거부됨 메시지를 수신합니다.

▼ 액세스 거부 메시지를 변경하는 방법

1. **Access Control Rules For 페이지에서 Response When Denied 링크를 누릅니다.**
2. **원하는 응답을 선택하고 해당하는 경우 추가 정보를 제공한 다음 Update를 누릅니다. 사용자가 리디렉션되는 응답에 대한 액세스 권한이 있는지 확인합니다.**
3. **변경 사항을 저장하려면 Submit를 누르고 변경하기 전에 포함된 값으로 페이지의 요소를 재설정하려면 Revert를 누릅니다.**

서버의 영역에 대한 액세스 제한

이 절에서는 서버 및 해당 컨텐츠에 대한 액세스를 제한하는 데 사용되는 일반적인 제한에 대해 설명합니다. 각 절차에 대한 단계에서는 수행해야 할 특정 작업을 자세하게 설명합니다. 그러나 151 페이지 "서버 인스턴스용 액세스 제어 설정"에서 설명한 단계는 완료해야 합니다.

이 절은 다음 내용으로 구성되어 있습니다.

- 159 페이지 "전체 서버에 대한 액세스 제한"
- 160 페이지 "디렉토리에 대한 액세스 제한"
- 160 페이지 "파일 유형에 대한 액세스 제한"
- 161 페이지 "하루 중 시간을 기준으로 액세스 제한"
- 162 페이지 "보안을 기준으로 액세스 제한"
- 162 페이지 "자원에 대한 액세스 보안"
- 162 페이지 "서버 인스턴스에 대한 액세스 보안"
- 163 페이지 "IP 기반 액세스 제어 사용"

전체 서버에 대한 액세스 제한

하위 도메인의 컴퓨터에서 서버에 액세스하는 그룹의 사용자에게 액세스를 허용하는 경우도 있습니다. 예를 들어 회사 부서 서버의 경우 사용자가 오직 네트워크의 특정 하위 도메인에 있는 컴퓨터에서 액세스하도록 할 수 있습니다.

▼ 전체 서버에 대한 액세스를 제한하는 방법

1. **서버 인스턴스의 Server Manager에 액세스합니다.**
2. **Preferences 탭에서 Administer Access Control 링크를 누릅니다.**
3. **드롭다운 목록에서 전체 서버를 선택하고 Select를 누른 다음 해당 Edit 버튼을 누릅니다.**
   Access Control Rules For 페이지가 표시됩니다.
4. **모든 사용자의 액세스를 거부할 규칙을 추가합니다.**
5. **특정 그룹의 액세스를 허용하는 다른 규칙을 추가합니다.**
6. **시작 호스트를 사용하여 제한할 호스트 이름과 IP 주소를 지정합니다.**
7. **Submit를 눌러 변경 사항을 저장합니다.**

디렉토리에 대한 액세스 제한

사용자가 디렉토리 및 그룹의 소유자가 제어하는 해당 하위 디렉토리와 파일에서 응용 프로그램을 읽거나 실행하도록 허용할 수 있습니다. 예를 들어 프로젝트 관리자는 프로젝트 팀이 검토할 수 있도록 상태 정보를 업데이트할 수 있습니다.

▼ 디렉토리에 대한 액세스를 제한하는 방법

서버 인스턴스의 액세스 제한 설정에 대해 설명된 단계(151 페이지 "서버 인스턴스용 액세스 제어 설정" 참조)를 사용하여 다음을 수행합니다.

1. **서버 인스턴스의 Server Manager에 액세스합니다.**
2. **Preferences 탭에서 Administer Access Control 링크를 누릅니다.**
3. **드롭다운 목록에서 원하는 자원을 선택하고 Edit를 누릅니다.**
4. **모든 위치로부터의 모든 사용자 액세스를 거부하는 기본값으로 규칙을 만듭니다.**
5. **특정 그룹의 사용자에게 오직 읽기 및 실행 권한만 허용하는 다른 규칙을 만듭니다.**
6. **특정 사용자에게 모든 권한을 허용하는 세 번째 규칙을 만듭니다.**
7. **마지막 두 개의 규칙에 대해 Continue 선택을 취소합니다.**
8. **Submit를 눌러 변경 사항을 저장합니다.**

파일 유형에 대한 액세스 제한

파일 유형에 대한 액세스를 제한할 수 있습니다. 예를 들어 지정된 사용자만 서버에서 실행되는 프로그램을 만들 수 있도록 허용할 수 있습니다. 모든 사람이 프로그램을 실행할 수 있으나 그룹의 지정된 사용자만 프로그램을 만들거나 삭제할 수 있습니다.

▼ 파일 유형에 대한 액세스를 제한하는 방법

1. **서버 인스턴스의 Server Manager에 액세스합니다.**
2. **Preferences 탭에서 Administer Access Control 링크를 누릅니다.**
3. **Select A Resource 섹션에서 Regular Expression을 누르고 `*.cgi`와 같은 정규 표현식을 지정합니다.**
4. **Edit를 누릅니다.**

5 **모든 사용자에게 읽기 액세스를 허용하는 규칙을 만듭니다.**

6 **오직 지정된 그룹에게 쓰기 및 삭제 액세스를 허용하는 다른 규칙을 만듭니다.**

7 **Submit를 눌러 변경 사항을 저장합니다.**
파일 유형 제한의 경우 두 개의 Continue 확인란을 모두 선택합니다. 파일에 대한 요청이 수신되면 서버는 우선 해당 파일 유형에 대한 ACL을 확인합니다.

Pathcheck 기능이 `obj.conf`에 만들어지며, 여기에는 파일 또는 디렉토리용 와일드카드 패턴이 포함될 수 있습니다. ACL 파일의 항목은 다음과 같이 표시됩니다. `acl"*.cgi";`

하루 중 시간을 기준으로 액세스 제한

특정 서버에 대해 지정된 시간 동안 또는 특정 일에 쓰기 및 삭제 액세스를 제한할 수 있습니다.

▼ 하루 중 시간을 기준으로 액세스를 제한하는 방법

1 **서버 인스턴스의 Server Manager에 액세스합니다.**

2 **Preferences 탭에서 Administer Access Control 링크를 누릅니다.**

3 **Select A Resource 섹션의 드롭다운 목록에서 전체 서버를 선택하고 Edit를 누릅니다.**

4 **모든 사용자에게 읽기 및 실행 권한을 허용하는 규칙을 만듭니다.**
사용자가 파일이나 디렉토리를 추가, 업데이트 또는 삭제하려 할 때 이 규칙이 적용되지 않으며 서버는 일치되는 다른 규칙을 검색합니다.

5 **모든 사용자의 쓰기 및 삭제 권한을 거부하는 다른 규칙을 만듭니다.**

6 **X 링크를 눌러 사용자 정의 표현식을 만듭니다.**

7 **허용할 주 중 요일과 하루 중 시간을 입력합니다. 예를 들면 다음과 같습니다.**

```
user = "anyone" anddayofweek = "sat,sun" or(timeofday >= 1800
andtimeofday <= 600)
```

8 **Submit를 눌러 변경 사항을 저장합니다.**
사용자 정의 표현식에 오류가 있는 경우 오류 메시지가 생성됩니다. 오류를 수정하고 다시 제출하십시오.

보안을 기준으로 액세스 제한

동일한 서버 인스턴스에 대해 SSL 및 비 SSL 청취 소켓을 구성할 수 있습니다. 보안을 기준으로 액세스를 제한하면 보안 채널을 통해서만 전송되어야 하는 자원을 보호할 수 있습니다.

▼ 보안을 기준으로 액세스를 제한하는 방법

1. **서버 인스턴스의 Server Manager에 액세스합니다.**
2. **Preferences 탭에서 Administer Access Control 링크를 누릅니다.**
3. **Select A Resource 섹션의 드롭다운 목록에서 전체 서버를 선택하고 Edit를 누릅니다.**
4. **모든 사용자에게 읽기 및 실행 권한을 허용하는 규칙을 만듭니다.**
   사용자가 파일이나 디렉토리를 추가, 업데이트 또는 삭제하려 할 때 이 규칙이 적용되지 않으며 서버는 일치되는 다른 규칙을 검색합니다.
5. **모든 사용자의 쓰기 및 삭제 권한을 거부하는 다른 규칙을 만듭니다.**
6. **X 링크를 눌러 사용자 정의 표현식을 만듭니다.**
7. **`ssl="on"`을 입력합니다. 예:**
   ```
   user = "anyone" and ssl="on"
   ```
8. **Submit를 눌러 변경 사항을 저장합니다.**
   사용자 정의 표현식에 오류가 있는 경우 오류 메시지가 생성됩니다. 오류를 수정하고 다시 제출하십시오.

자원에 대한 액세스 보안

이 절에서는 분산 관리를 사용하도록 설정한 후 Proxy Server의 액세스 제어를 보안하기 위해 수행해야 하는 추가 작업에 대해 설명합니다.

서버 인스턴스에 대한 액세스 보안

Proxy Server가 서버 인스턴스에 대한 액세스를 제어하도록 구성하려면 *server-root*`/httpacl/*.proxy-admserv.acl` 파일을 편집하여 액세스 제어 권한을 부여하려는 사용자를 지정합니다. 예:

```
acl "proxy-server_instance "; authenticate (user,group) { database = "default";
method = "basic"; }; deny absolute (all) user != "UserA";
```

IP 기반 액세스 제어 사용

ip 속성을 참조하는 액세스 제어 항목이 Administration Server와 관련된 ACL 파일에 있는 경우(gen*.proxy-admserv.acl) 아래 단계 1 및 2를 완료합니다.

ip 속성을 참조하는 액세스 제어 항목이 서버 인스턴스에 관련된 ACL 파일 안에 있는 경우 해당 ACL에 대해 단계 (1)만 완료합니다.

▼ IP 기반 액세스 제어를 사용 설정하는 방법

1 **아래에 보이는 것과 같이 *server-root*/httpacl/gen*.proxy-admserv.acl 파일을 편집하여 user 및 group 이외에 인증 목록에 ip를 추가합니다.**

```
acl "proxy-admserv"; authenticate (user,group,ip) { database = "default"; method =
"basic"; };
```

2 **다음 액세스 제어 항목을 추가합니다.**

```
deny absolute (all) ip !="ip_for_which_access_is_allowed ";
```

예:

```
acl "proxy-admserv"; authenticate (user,group,ip) { database = "default"; method =
"basic"; }; deny absolute (all) ip !="205.217.243.119";
```

파일 기반 인증용 ACL 생성

Proxy Server에서는 보통 파일에 텍스트 형식으로 사용자 및 그룹 정보를 저장하는 파일 기반 인증 데이터베이스 사용을 지원합니다. ACL 프레임워크는 파일 인증 데이터베이스와 함께 작동하도록 디자인되었습니다.

주 – Proxy Server는 동적 보통 파일을 지원하지 않습니다. 보통 파일 데이터베이스는 서버가 시작할 때 로드됩니다. 파일이 변경되는 경우 오직 서버가 재식작되어야 적용됩니다.

이 절에서는 파일 인증 및 Digest 인증을 기준으로 디렉토리 서비스에 대한 ACL 작성 방법에 대해 설명합니다.

ACL 항목은 database 키워드를 사용하여 사용자 데이터베이스를 참조할 수 있습니다. 예:

```
acl "default";    authenticate (user) {...    database="myfile";...};
```

server-root/userdb/dbswitch.conf 파일에는 파일 인증 데이터베이스와 구성을 정의하는 항목이 포함되어 있습니다. 예:

```
directory myfiledb filemyfiledb:syntax keyfilemyfiledb:keyfile
/path/to/config/keyfile
```

다음 표에서는 파일 인증 데이터베이스에서 지원하는 매개 변수가 나열되어 있습니다.

표 8–2 파일 인증 데이터베이스에서 지원하는 매개 변수

매개 변수	설명
구문	(선택 사항) 값은 `keyfile` 또는 `digest` 중 하나입니다. 지정하지 않는 경우 기본값은 `keyfile`입니다.
`keyfile`	(`syntax=keyfile`인 경우 필요) 사용자 데이터가 있는 파일 경로
`digestfile`	(`syntax=digest`인 경우 필요) Digest 인증용 사용자 데이터가 있는 파일 경로

주의 – 파일 인증 데이터베이스 파일에서 한줄의 최대 길이는 255입니다. 줄이 이 제한을 초과하는 경우 서버를 시작할 수 없으며 오류가 로그 파일에 기록됩니다.

파일 기반 인증 데이터베이스를 사용하여 ACL을 설정하기 전에 파일 기반 인증 디렉토리 서비스가 구성되어 있는지 확인합니다. 자세한 내용은 45 페이지 “디렉토리 서비스 구성”을 참조하십시오.

파일 인증을 기반으로 디렉토리 서비스용 ACL 생성

▼ 파일 인증을 기반으로 디렉토리 서비스용 ACL을 생성하는 방법

1. **서버 인스턴스의 Server Manager에 액세스합니다.**
2. **Preferences 탭에서 Administer Access Control 링크를 누릅니다.**
3. **드롭다운 목록에서 ACL 파일을 선택하고 Edit를 누릅니다.**
4. **Access Control Rules For 페이지에서 편집하려는 ACL의 Users/Groups 링크를 누릅니다.**
   User/Group 페이지가 아래의 창에 표시됩니다.
5. **Authentication Database 아래 드롭다운 목록에서 키 파일 데이터베이스를 지정합니다.**

6 **Update를 누른 다음 Submit를 눌러 변경 사항을 저장합니다.**

아래의 예와 같이 키 파일 기반 파일 인증 데이터베이스에 대한 ACL을 설정하는 경우 `dbswitch.conf` 파일이 ACL 항목을 포함하여 업데이트됩니다.

```
version 3.0;acl "default";authenticate (user) {prompt =
"Sun Java System Proxy Server 4.0";database = "mykeyfile";
method = "basic";};deny (all) user = "anyone";
allow (all) user = "all";
```

Digest 인증을 기반으로 디렉토리 서비스용 ACL 생성

또한 파일 인증 데이터베이스는 각 암호 기반 RFC 2617.A 해시 Digest 인증을 사용하기 적합한 파일 형식을 지원하며, 영역은 저장됩니다. 일반 텍스트 비밀번호는 보관되지 않습니다.

▼ Digest 인증을 기반으로 디렉토리 서비스용 ACL을 생성하는 방법

1 **서버 인스턴스의 Server Manager에 액세스합니다.**

2 **Preferences 탭에서 Administer Access Control 링크를 누릅니다.**

3 **드롭다운 목록에서 ACL 파일을 선택하고 Edit를 누릅니다.**

4 **Access Control Rules For 페이지에서 편집하려는 ACL의 Users/Groups 링크를 누릅니다.**

User/Group 페이지가 아래의 창에 표시됩니다.

5 **Authentication Database 아래 드롭다운 목록에서 다이제스트 데이터베이스를 지정합니다.**

6 **Update를 누른 다음 Submit를 눌러 변경 사항을 저장합니다.**

Digest 인증 기반 파일 인증 데이터베이스에 대한 ACL을 설정하는 경우 `dbswitch.conf` 파일이 아래의 예와 같은 ACL 항목을 포함하여 업데이트됩니다.

```
version 3.0;acl "default";authenticate (user) {prompt = "filerealm";
database = "mydigestfile";method = "digest";}; deny (all) user = "anyone";
allow (all) user = "all";
```

◆ ◆ ◆ 9 장

9 로그 파일 사용

다양한 방법으로 서버의 작동을 모니터할 수 있습니다. 이 장에서는 로그 파일을 기록하고 확인하여 서버를 모니터하는 방법에 대해 설명합니다. 내장 성능 모니터링 서비스 또는 SNMP 사용에 대한 자세한 내용은 10 장, "서버 모니터링"을 참조하십시오.

이 장은 다음 내용으로 구성되어 있습니다.

- 167 페이지 "로그 파일 정보"
- 168 페이지 "UNIX 및 Windows 플랫폼에서의 로깅"
- 169 페이지 "로그 수준"
- 170 페이지 "로그 파일 보관"
- 171 페이지 "액세스 로그 기본 설정 지정"
- 178 페이지 "오류 로깅 옵션 설정"
- 178 페이지 "LOG 요소 구성"
- 179 페이지 "액세스 로그 파일 보기"
- 180 페이지 "오류 로그 파일 보기"
- 181 페이지 "로그 분석기로 작업"
- 190 페이지 "이벤트 보기(Windows)"

로그 파일 정보

서버 로그 파일은 서버의 작동을 기록합니다. 이 로그를 서버를 모니터와 문제 해결에 사용할 수 있습니다. 서버 루트 디렉토리의 `proxy-server_name/logs/errors`에 있는 오류 로그 파일에는 서버에서 발생한 모든 오류가 나열됩니다. 서버 루트 디렉토리의 `proxy-server_name/logs/access`에 있는 액세스 로그에는 서버로의 요청과 서버로부터의 응답에 대한 정보가 기록됩니다. Proxy Server `access` 로그 파일에 기록된 정보를 구성할 수 있습니다. 서버 통계를 생성하려면 로그 분석기를 사용합니다. 서버 오류 및 액세스 로그를 백업하려면 해당 파일을 보관합니다.

주 – 운영 체제의 한계로 인하여 Linux의 경우 Proxy Server는 2GB를 초과하는 로그 파일을 사용할 수 없습니다. 최대 파일 크기가 초과되면 기록이 중단됩니다.

UNIX 및 Windows 플랫폼에서의 로깅

여기에서는 로그 파일이 만들어지는 방법에 대해 설명합니다. 또한 다음 항목에 대해 설명합니다.

- 168 페이지 “기본 오류 로깅”
- 168 페이지 “syslog를 사용하여 로깅”

주 – Windows 운영 체제에서 사용하는 이벤트 로그 기법에 대한 내용은 Windows 도움말에서 Event Logging 키워드로 검색하십시오.

기본 오류 로깅

UNIX 및 Windows 플랫폼 모두의 경우 Administration Server의 로그는 관리 `proxy-admserv/logs/` 디렉토리에서 수집됩니다. 서버 인스턴스의 로그는 `proxy-server_name/logs/` 디렉토리에 수집됩니다.

전체 서버용 기본 로그 수준을 설정할 수 있습니다. `stdout` 및 `stderr`을 서버의 이벤트 로그로 재지정할 수 있으며 로그 출력을 운영 시스템의 시스템 로그로 지정할 수 있습니다. 또한 stdout 및 stderr 컨텐트를 서버의 이벤트 로그로 지정할 수 있습니다. 기본적으로 로그 메시지는 지정된 서버 로그 파일뿐 아니라 stderr로 또한 전송됩니다.

`syslog`를 사용하여 로깅

중앙 집중식 로깅이 필요한 안정된 운영 환경의 경우 `syslog`를 사용하는 것이 더 좋습니다. 진단 및 디버깅용으로 로그 출력이 자주 필요한 환경의 경우 개별 서버 인스턴스 로그가 더 관리하기 쉽습니다.

서버 인스턴스 및 Administration Server에 기록되는 데이터를 하나의 파일에 저장하면 읽고 디버깅하기 어려울 수 있기 때문에 안정적으로 실행되는 배포된 응용 프로그램에서만 `syslog` 마스터 로그 파일을 사용합니다.

기록된 메시지는 Solaris 데몬 응용 프로그램으로부터의 모든 기타 로그와 혼합됩니다.

`syslogd` 및 시스템 로그 데몬과 함께 `syslog` 로그 파일을 사용하면 다음 작업을 수행하도록 `syslog.conf` 파일을 구성할 수 있습니다.

- 적절한 시스템 로그로 메시지 기록

- 시스템 콘솔에 메시지 표시
- 목록에 있는 사용자에게 기록된 메시지를 전달하거나 네트워크를 통해 다른 호스트의 다른 `syslogd`로 기록된 메시지 전달

`syslogd`로의 로깅은 Proxy Server로부터의 로그를 의미하며 기타 데몬 응용 프로그램이 동일한 파일에 수집되므로, 기록된 메시지는 다음 정보를 포함하여 특정 서버 인스턴스로부터의 Proxy Server 관련 메시지를 구분합니다.

- 고유한 메시지 아이디
- 타임스탬프
- 인스턴스 이름
- 프로그램 이름(`proxyd` 또는 `proxyd-wdog`)
- 프로세스 아이디(proxyd 프로세스의 PID)
- 스레드 아이디(선택 사항)
- 서버 아이디

LOG 요소는 `server.xml` 파일에서 Administration Server 및 서버 인스턴스 모두에 대해 구성할 수 있습니다.

UNIX 운영 체제에서 사용되는 `syslog` 로깅 메커니즘에 대한 자세한 내용은 단말기 프롬프트에서 다음 `man` 명령을 사용하십시오.

```
man syslog
man syslogd
man syslog.conf
```

로그 수준

다음 표에는 심각도 순서에 따라 Proxy Server의 로그 수준 및 메시지가 정의되어 있습니다.

표 9–1 로그 수준

로그 수준	설명
`finest`	메시지는 디버그 메시지의 상세 표시 수준을 표시합니다. `finest`는 최대 상세 표시를 제공합니다.
`finer`	
`fine`	
`info`	원래 정보를 제공하는 메시지이며, 보통 서버 구성 또는 서버 상태에 관련된 메시지입니다. 즉각적인 조치가 필요한 오류를 표시하는 메시지는 아닙니다.

표 9–1 로그 수준 *(계속)*

로그 수준	설명
warning	경고를 표시하는 메시지입니다. 이 메시지에는 예외가 포함될 수 있습니다.
failure	정상의 응용 프로그램 실행을 방해할 수 있는 중요한 이상을 표시하는 메시지입니다.
config	다양한 정적 구성 정보에 관련된 메시지로 특정 구성에 관련된 문제를 해결하는데 도움이 됩니다.
security	보안 문제를 표시하는 메시지입니다.
catastrophe	중요한 오류를 표시하는 메시지입니다.

로그 파일 보관

액세스 및 오류 로그 파일이 자동 보관되도록 설정할 수 있습니다. 특정 시간이나 지정된 시간이 경과하면 로그가 교체됩니다. Proxy Server는 이전 로그 파일을 저장하고 파일이 저장된 일자 및 시간이 포함된 이름을 파일에 지정합니다.

예를 들어, 액세스 로그 파일이 매시간 교체되도록 설정할 수 있습니다. Proxy Server는 파일을 "access.200505160000"이라는 이름으로 지정합니다. 여기에서 로그 파일, 년, 월, 일 및 24시간 형식 시간은 단일 문자열로 합쳐집니다. 로그 보관 파일의 형식은 설정한 로그 교체 유형에 따라 달라집니다.

Proxy Server는 파일 보관용으로 두 가지 로그 교체 유형(내부 데몬 로그 교체 및 Cron 기반 로그 교체)을 제공합니다.

내부 데몬 로그 교체

내부 데몬 로그 교체는 HTTP 데몬에서 수행되며 시작 시에만 구성할 수 있습니다. 서버를 다시 시작할 필요 없이 서버가 내부적으로 로그를 교체합니다. 이 방법으로 교체한 로그는 다음의 형식으로 저장됩니다.

```
access.<YYYY><MM><DD><HHMM>

errors.<YYYY><MM><DD><HHMM>
```

로그 파일을 교체하고 새 로그 파일을 시작할 기준으로 사용할 시간을 지정할 수 있습니다. 예를 들어, 교체 시작 시간이 오전 12:00이고 교체 간격이 1440분(1일)인 경우 현재 시간과 관계 없이 변경 사항을 저장 및 적용하는 즉시 새 로그 파일이 만들어집니다. 로그 파일은 매일 오전 12:00에 교체되며 액세스 로그 파일은 오전 12:00으로 스탬프되고 access.200505172400으로 저장됩니다. 마찬가지로 간격을 240분(4시간)으로 설정하고 이 4시간 간격이 오전 12:00에 시작하면 액세스 로그 파일에는 오전 12:00에서 오전 4:00까지, 오전 4:00에서 오전 8:00까지 등의 순서로 정보가 수집됩니다.

로그 교체를 사용하는 경우 로그 교체는 서버가 시작할 때 시작됩니다. 첫 로그 파일은 현재 시간부터 다음 교체 시간까지 정보를 수집합니다. 앞의 예에서 시작 시간을 오전 12:00으로, 교체 간격을 240분으로 설정하며 현재 시간이 오전 6:00이라면, 교체의 첫 번째 로그 파일에는 오전 6:00에서 오전 8:00까지 수집된 정보가 포함되며 다음 로그 파일에는 오전 8:00에서 오후 12:00(정오)까지의 정보가 포함됩니다.

스케줄러 기반 로그 교체

스케줄러 기반 로그 교체는 *server-root*/proxy- *server_name*/config/ 디렉토리의 server.xml 파일에 저장된 시간과 일자를 기준으로 수행됩니다. 이 방법을 사용하면 로그 파일을 즉시 보관하거나 특정 일자의 특정 시간에 서버가 로그 파일을 보관하도록 할 수 있습니다. 서버의 스케줄러 구성 옵션은 server-root/proxy- *server_name*/config/ 디렉토리의 server.xml에 저장됩니다. 스케줄러 기반 방법으로 교체된 로그는 다음의 형식으로 저장됩니다.

<original_filename>.<YYYY><MM><DD><HHMM>

예를 들어, access가 오후 4:30에 교체되면 access.200505171630 이 됩니다.

로그 교체는 서버가 시작할 때 초기화됩니다. 교체를 사용하는 경우 Proxy Server는 타임스탬프 액세스 로그 파일을 만들고 서버가 시작할 때 교체가 시작됩니다.

교체가 시작되면 Proxy Server는 액세스 또는 오류 로그 파일에 기록해야 할 요청 또는 오류가 발생하는 경우 새로운 타임스탬프 로그 파일을 만들며 또한 이 작업은 미리 설정된 "다음 교체 시간"이 경과하면 수행됩니다.

주 – 로그 분석기를 실행하기 전에 서버 로그를 보관합니다.

로그 파일을 보관하고 내부 데몬 방법 또는 스케줄러 기반 방법을 사용할 것인지 지정하려면 Server Manager의 Archive Log Files 페이지를 사용합니다.

액세스 로그 기본 설정 지정

설치하는 동안 access라는 이름의 액세스 로그 파일이 해당 서버용으로 만들어집니다. 액세스 기록 여부, 기록에 사용할 형식 및 자원에 액세스할 때 서버가 클라이언트의 도메인 이름을 조회할 것인지 여부를 지정하여 모든 자원에 대한 액세스 로깅을 사용자 정의할 수 있습니다.

Server Manager의 Set Access Log Preferences 페이지를 사용하여 로깅 기본 설정을 지정하거나 obj.conf 파일에서 직접 지시문을 구성할 수 있습니다. obj.conf에서 서버는 flex-init 함수를 호출하여 유연한 로깅 시스템을 초기화하고 flex-log 함수를 호출하여 요청 관련 데이터를 유연한 로그 형식으로 기록합니다. 공통 로그 파일 형식을

사용하여 요청을 기록하려면 서버가 `init-clf`를 호출하여 `obj.conf`에 사용되는 공통 로그 하위 시스템을 초기화하고 `common-log`를 호출하여 요청에 대한 데이터를 대부분의 HTTP 서버에서 사용되는 공통 로그 형식으로 기록합니다.

자원용 액세스 로그가 일단 만들어지면 해당 로그를 보관하거나 해당 자원용으로 새 액세스 로그 파일을 만들지 않는 한, 이 로그를 변경할 수 없습니다.

표 9–2 Administration Server용 로그 파일 형식

로그 형식 항목	설명
Client Hostname	액세스를 요청하는 클라이언트의 호스트 이름(또는 DNS를 사용하지 않는 경우 IP 주소).
Authenticate User Name	인증이 필요한 경우 액세스 로그에 인증된 사용자 이름을 나열할 수 있습니다.
System Date	클라이언트 요청의 일자 및 시간
Full Request	클라이언트가 수행한 그대로의 요청
상태	서버가 클라이언트에게 반환한 상태 코드
Content Length	클라이언트에게 송신한 문서의 길이(바이트 단위)
HTTP Header, referer	참조자는 클라이언트가 현재 액세스한 페이지의 상위 페이지를 지정합니다. 예를 들어, 사용자가 텍스트 검색 쿼리의 결과를 보려는 경우 참조자는 사용자가 텍스트 검색 엔진에 액세스한 페이지가 됩니다. 서버는 참조자를 통해 역방향 추적 링크 목록을 만듭니다.
HTTP Header, "user-agent"	클라이언트가 사용하는 브라우저 유형, 버전 및 실행되는 운영 체제가 포함된 사용자 에이전트 정보. 이 정보는 클라이언트가 서버에 보내는 HTTP 헤더 정보의 User-agent 필드에서 제공합니다.
Method	GET, PUT 또는 POST와 같은 HTTP 요청 방법이 사용됩니다.
URI	Universal Resource Identifier. 서버의 자원 위치입니다. 예를 들어, `http://www.a.com:8080/special/docs`의 경우 URI는 `special/docs`입니다.
Query String Of The URI	URI의 물음표 뒤에 있는 텍스트. 예를 들어, `http://www.a.com:8080/special/docs?find_this`의 경우 URI의 쿼리 문자열은 `find_this`입니다.
Protocol	사용된 전송 프로토콜 및 버전

기존 로그 파일의 형식을 변경하는 경우 우선 기존 로그 파일을 삭제/이름 변경하거나 다른 파일 이름을 사용해야 합니다.

▼ Administration Server용 액세스 로그 기본 설정을 지정하는 방법

1 **Administration Server에 액세스하고 Preferences 탭을 누릅니다.**

2 **Set Access Log Preferences 링크를 누릅니다.**
Set Access Log Preferences 페이지가 표시됩니다.

3 **드롭다운 목록에서 자원을 선택하거나 Regular Expression 버튼을 눌러 정규 표현식을 입력하고 OK를 누릅니다.**

4 **클라이언트 액세스를 기록할지 여부를 지정합니다.**
이 설정을 사용하려면 DNS(Domain Name Service)를 활성화해야 합니다.

5 **액세스 로그 파일의 절대 경로를 지정합니다.**
기본적으로 로그 파일은 서버 루트의 `logs` 디렉토리에 저장됩니다. 부분적인 경로를 지정하면 서버는 이 경로를 서버 루트의 `logs` 디렉토리에 대한 상대 경로로 가정합니다.

전체 서버를 편집하는 경우 이 필드의 기본값은 `$accesslog`이며, 이 변수는 구성 파일에서 해당 서버의 액세스 로그 파일을 나타냅니다.

6 **액세스 로그에 서버에 액세스하는 시스템의 IP 주소를 기록할 것인지 또는 도메인 이름을 기록할 것인지 선택합니다.**

7 **액세스 로그에 사용할 로그 파일 형식의 유형을 선택합니다.**
다음 옵션을 사용할 수 있습니다.

- **Use Common** *LogFile Format.* 클라이언트의 호스트 이름, 인증된 사용자 이름, 요청 일자 및 시간, HTTP 헤더, 클라이언트에 반환된 상태 코드 및 클라이언트에 전송된 문서의 컨텐트 길이가 포함됩니다.
- **Only Log.** 기록되는 정보를 확인할 수 있습니다. 표 9–2에 나열된 유연한 로그 형식 항목 중에서 선택할 수 있습니다.
- 사용자 정의 형식을 선택한 경우 Custom Format 필드에 입력합니다.

8 **OK를 누릅니다.**

9 **Restart Required를 누릅니다.**
Apply Changes 페이지가 표시됩니다.

10 Restart Proxy Server 버튼을 눌러 변경 사항을 적용합니다.

서버 인스턴스에 대한 액세스 로그 기본 설정 지정

서버 인스턴스에 대한 액세스 로그 기본 설정을 지정하는 데 사용할 수 있는 유연한 로그 형식은 다음 표와 같습니다.

표 9–3 서버 인스턴스에 대한 로그 파일 형식

로그 형식 항목	설명
Client Hostname	액세스를 요청하는 클라이언트의 호스트 이름(또는 DNS를 사용하지 않는 경우 IP 주소).
Authenticate User Name	인증이 필요한 경우 액세스 로그에 인증된 아이디 목록이 표시되도록 할 수 있습니다.
System Date	클라이언트 요청의 일자 및 시간
Full Request	클라이언트가 수행한 그대로의 요청
Status	서버가 클라이언트에게 반환한 상태 코드
Content Length	클라이언트에게 송신한 문서의 길이(바이트 단위)
HTTP Header, referer	참조자는 클라이언트가 현재 액세스한 페이지의 상위 페이지를 지정합니다. 예를 들어, 사용자가 텍스트 검색 쿼리의 결과를 보려는 경우 참조자는 사용자가 텍스트 검색 엔진에 액세스한 페이지가 됩니다. 서버는 참조자를 통해 역방향 추적 링크 목록을 만듭니다.
HTTP Header, "user-agent"	클라이언트가 사용하는 브라우저 유형, 버전 및 실행되는 운영 체제가 포함된 사용자 에이전트 정보. 이 정보는 클라이언트가 서버에 보내는 HTTP 헤더 정보의 User-agent 필드에서 제공합니다.
Method	GET, PUT 또는 POST와 같은 HTTP 요청 방법이 사용됩니다.
URI	Universal Resource Identifier. 서버의 자원 위치입니다. 예를 들어, `http://www.a.com:8080/special/docs`의 경우 URI는 `special/docs`입니다.
Query String Of The URI	URI의 물음표 뒤에 있는 텍스트. 예를 들어, `http://www.a.com:8080/special/docs?find_this`의 경우 URI의 쿼리 문자열은 `find_this`입니다.
Protocol	사용된 전송 프로토콜 및 버전

표 9–3 서버 인스턴스에 대한 로그 파일 형식 (계속)

로그 형식 항목	설명
Cache Finish Status	이 필드는 최신 검사를 통해 캐시 파일이 쓰여졌는지, 새로 고쳐졌는지 또는 반환되었는지 여부를 지정합니다. cs 필드에는 다음과 같은 값 중 하나를 가질 수 있습니다. -는 자원을 캐시할 수 없음을 나타냅니다. WRITTEN은 캐시 파일이 생성되었음을 나타냅니다. REFRESHED는 캐시 파일이 업데이트되었거나 새로 고쳐졌음을 나타냅니다. NO-CHECK는 캐시 파일이 최신 검사 없이 반환되었음을 나타냅니다. UP-TO-DATE는 캐시 파일이 최신 검사 수행 후 반환되었음을 나타냅니다. HOST-NOT-AVAILABLE은 원격 서버에서 최신 검사를 수행할 수 없기 때문에 검사를 수행하지 않고 캐시 파일을 반환했음을 나타냅니다. CL-MISMATCH는 컨텐트 길이가 일치하지 않으므로 캐시 파일 쓰기가 중단되었음을 나타냅니다. ABORTED는 특별한 이유로 캐싱이 중단되었음을 나타냅니다. 예를 들어 유효한 Last-Modified 헤더가 없는 것일 수 있습니다.
Remote Server Finish Status	이 필드는 원격 서버에 대한 요청이 성공적으로 완료되었는지, 브라우저에서 클라이언트가 Stop 버튼을 클릭하여 중단했는지 또는 오류 조건에 의해 중지되었는지 여부를 지정합니다.
Status Code From Server	서버에서 반환된 상태 코드입니다.
Route To Proxy (PROXY, SOCKS, DIRECT)	자원을 검색하는 데 사용된 라우팅입니다. 프록시 또는 SOCKS 서버를 통해 문서를 직접 검색할 수 있습니다.
Transfer Time	전송 시간 길이(초 또는 밀리초)입니다.
Header-length From Server Response	서버 응답의 헤더 길이입니다.
Request Header Size From Proxy To Server	프록시에서 서버로의 요청 헤더 크기입니다.
Response Header Size Sent To Client.	클라이언트에 전송된 응답 헤더의 크기입니다.
Request Header Size Received From Client	클라이언트에서 수신된 요청 헤더의 크기입니다.

표 9–3 서버 인스턴스에 대한 로그 파일 형식 *(계속)*

로그 형식 항목	설명
Content-length From Proxy To Server Request.	프록시에서 서버로 전송된 문서의 길이(바이트)입니다.
Content-length Received From Client	클라이언트의 문서 길이(바이트)입니다.
Content-length From Server Response	서버의 문서 길이(바이트)입니다.
Unverified User From Client	인증 시 원격 서버에 제공된 사용자 이름입니다.

▼ 서버 인스턴스에 대한 액세스 로그 기본 설정을 지정하는 방법

1 Server Manager에 액세스하고 Server Status 탭을 누릅니다.

2 Set Access Log Preferences 링크를 누릅니다.

Set Access Log Preferences 페이지가 표시됩니다.

3 드롭다운 목록에서 자원을 선택하거나 Regular Expression 버튼을 눌러 정규 표현식을 입력하고 OK를 누릅니다.

4 클라이언트 액세스를 기록할지 여부를 지정합니다.

이 설정을 사용하려면 DNS(Domain Name Service)를 활성화해야 합니다.

5 액세스 로그 파일의 절대 경로를 지정합니다.

로그 파일은 기본적으로 서버 루트의 `logs` 디렉토리에 보관됩니다. 부분적인 경로를 지정하면 서버는 이 경로를 서버 루트의 `logs` 디렉토리에 대한 상대 경로로 가정합니다.

전체 서버를 편집하는 경우 이 필드의 기본값은 `$accesslog`이며, 이 변수는 구성 파일에서 해당 서버의 액세스 로그 파일을 나타냅니다.

6 액세스 로그에 서버에 액세스하는 시스템의 IP 주소를 기록할 것인지 또는 도메인 이름을 기록할 것인지 선택합니다.

7 다음 중 로그 파일의 형식을 선택합니다. Common, Extended, Extended-2, 지정된 정보만("Only log" 선택 버튼) 또는 custom.

Only log를 누르면 다음과 같은 유연한 로그 형식 항목을 사용할 수 있습니다.

8 액세스 로그에 사용할 로그 파일 형식의 유형을 선택합니다.

서버 액세스 로그는 Common Logfile Format, Extended Logfile Format, Extended2 Logfile Format, 유연한 로그 형식 또는 사용자 정의 형식을 사용할 수 있습니다. Common LogFile Format은 흔히 지원되는 형식으로 서버에 대한 고정된 양의 정보를 제공합니다. 유연한 로그 형식을 사용하면 기록할 내용을 Proxy Server에서 선택할 수 있습니다. 사용자 정의 형식의 경우 로그할 사항을 조정하는 매개 변수 블록을 사용합니다.

- **Use Common** *LogFile Format*. 클라이언트의 호스트 이름, 인증된 사용자 이름, 요청 일자 및 시간, HTTP 헤더, 클라이언트에 반환된 상태 코드 및 클라이언트에 전송된 문서의 컨텐트 길이가 포함됩니다.
- **Use Extended** *LogFile Format*. 공통 로그 파일 형식의 모든 필드뿐만 아니라 원격 상태, 프록시-클라이언트 컨텐트 길이, 원격-프록시 컨텐트 길이, 프록시-원격 컨텐트 길이, 클라이언트-프록시 헤더 길이, 프록시-클라이언트 헤더 길이, 프록시-원격 헤더 길이, 원격-프록시 헤더 길이 및 전송 시간과 같은 일부 추가 필드를 포함합니다.
- **Use Extended2** *LogFile Format*. 확장된 로그 파일 형식의 모든 필드뿐만 아니라 클라이언트 상태, 서버 상태, 원격 상태, 캐시 완료 상태 및 실제 라우팅과 같은 일부 추가 필드를 포함합니다.
- **Only Log.** 로그할 정보를 선택할 수 있습니다. 표 9–3에 나열된 유연한 로그 형식 항목에서 선택할 수 있습니다.
- 사용자 정의 형식을 선택한 경우 Custom Format 필드에 입력합니다.

9 특정 호스트 이름 또는 IP 주소에서 클라이언트 액세스를 기록하지 않으려면 호스트 이름 및 IP Addresses 필드에 입력합니다.

액세스를 기록하지 않을 호스트의 와일드카드 패턴을 입력합니다. 예를 들어, `*.example.com`은 도메인이 example.com인 사용자의 액세스를 기록하지 않습니다. 호스트 이름, IP 주소 또는 둘 모두에 대한 와일드카드 패턴을 입력할 수 있습니다.

10 로그 파일에 형식 문자열을 포함할지 여부를 선택합니다.

Proxy Server의 로그 분석기를 사용하는 경우 형식 문자열이 포함되어야 합니다. 타사 분석기를 사용하는 경우 로그 파일에 형식 문자열을 포함하지 않을 수 있습니다.

11 OK를 누릅니다.

12 Restart Required를 누릅니다.

Apply Changes 페이지가 나타납니다.

13 Restart Proxy Server 버튼을 눌러 변경 사항을 적용합니다.

용이한 쿠키 로깅

Proxy Server에서는 flexlog 기능을 사용하여 특정 쿠키를 쉽게 기록할 수 있습니다. 구성 파일 `obj.conf`에서 `flex-log` 하위 시스템을 초기화하는 줄에 `Req->headers.cookie.cookie_name`을 추가합니다. 이렇게 하면 쿠키 변수가 요청의 헤더에 있는 경우 쿠키 변수 `cookie_name`의 값을 기록하며, 쿠키 변수가 없는 경우에는 "-"을 기록합니다.

오류 로깅 옵션 설정

서버의 오류 로그에 기록할 정보를 구성할 수 있습니다.

▼ 오류 로깅 옵션 설정 방법

1. **Administration Server에서 오류 로깅 옵션을 설정하려면 Preferences 탭을 선택한 다음 Set Error Log Preferences 링크를 누릅니다.**
   Server Manager에서 서버 인스턴스에 대한 오류 로깅 옵션을 설정하려면 Server Status 탭을 선택한 다음 Set Error Log Preferences 링크를 누릅니다.
2. **Error Log File Name 필드에 서버의 메시지를 저장한 파일을 지정합니다.**
3. **Log Level 드롭다운 목록에서 오류 로그에 기록할 수 있는 정보의 양을 지정합니다. 다음 옵션을 사용할 수 있습니다.**
4. **stdout 출력을 오류 로그로 리디렉션하려면 Log Stdout을 선택합니다.**
5. **stderr 출력을 오류 로그로 리디렉션하려면 Log Stderr을 선택합니다.**
6. **메시지를 콘솔로 리디렉션하려면 Log To Console을 선택합니다.**
7. **UNIX syslog 서비스 또는 Windows 이벤트 로깅을 사용하여 로그를 생성하고 관리하려면 Use System Logging을 선택합니다.**
8. **OK를 누릅니다.**
9. **Restart Required를 누릅니다.**
   Apply Changes 페이지가 나타납니다.
10. **Restart Proxy Server 버튼을 눌러 변경 사항을 적용합니다.**

LOG 요소 구성

다음 표에는 `server.xml` 파일에서 구성할 수 있는 LOG 요소의 속성이 정리되어 있습니다.

표 9–4 LOG 속성

속성	Default	설명
file	errors	서버에서 메시지를 저장하는 파일을 지정합니다.
loglevel	info	다른 요소가 오류 로그에 기록한 메시지의 기본 유형을 제어합니다. 최고에서 최저까지 허용되는 값은 다음과 같습니다. finest, fine, fine, info, warning, failure, config, security, and catastrophe.
logstdout	true	(선택 사항) true인 경우 stdout 출력을 오류 로그로 리디렉션합니다. 유효한 값은 on, off, yes, no, 1, 0, true, false입니다.
logstderr	true	(선택 사항) true인 경우 stderr 출력을 오류 로그로 리디렉션합니다. 유효한 값은 on, off, yes, no, 1, 0, true, false입니다.
logtoconsole	true	(선택, UNIX 전용) true인 경우 로그 메시지를 콘솔로 리디렉션합니다.
createconsole	false	(선택, Windows 전용) true인 경우 stderr 출력용 Windows 콘솔을 만듭니다. 유효한 값은 on, off, yes, no, 1, 0, true, false입니다.
usesyslog	false	(선택 사항) true인 경우 UNIX syslog 서비스 또는 Windows 이벤트 로깅을 사용하여 로그를 생성하고 관리합니다. 유효한 값은 on, off, yes, no, 1, 0, true, false입니다.

액세스 로그 파일 보기

서버의 활성 액세스 로그 파일 및 보관된 액세스 로그 파일을 볼 수 있습니다.

Administration Server에서 Administration Server의 액세스 로그를 보려면 Preference 탭을 선택한 후 View Access Log 링크를 선택합니다.

Server Manager에서 서버 인스턴스의 액세스 로그를 보려면 Server Status 탭을 선택한 다음 View Access Log 링크를 누릅니다.

다음 예에서는 Common Logfile Format의 액세스 로그를 표시합니다.

```
198.18.17.222 - - [20/May/2005:14:15:49 +0530]
"GET http://www.example.com/ HTTP/1.1" 504 622 198.18.17.222 - abc
[20/May/2005:14:16:09 +0530] "GET http://www.test.com/report.zip HTTP/1.1"
504 630
```

다음 표에서는 이 샘플 액세스 로그의 마지막 줄에 대해 설명합니다.

액세스 로그 필드	예
클라이언트의 호스트 이름 또는 IP 주소	198.18.17.222(이 경우 프록시 서버에서 DNS 조회에 대한 설정이 비활성화되어 있기 때문에 클라이언트의 IP 주소가 표시됩니다. DNS 조회가 활성화된 경우 클라이언트의 호스트 이름이 나타납니다.)
IFC 931 정보	- (RFC 931 ID는 구현되지 않음)
사용자 이름	*abc*(클라이언트가 인증용으로 입력한 사용자 이름)
요청 일자/시간	20/May/2005:14:16:09 +0530
요청	GET
프로토콜	HTTP/1.1
상태 코드	504
전송된 바이트	630

오류 로그 파일 보기

오류 로그 파일에는 로그 파일이 만들어진 이후 서버에서 발생한 오류가 기록되어 있습니다. 또한 파일에는 서버를 시작한 시간과 같은 서버에 대한 정보 메시지가 포함되어 있습니다. 성공하지 못한 사용자 인증 또한 오류 로그에 기록됩니다. 오류 로그를 사용하여 끊어진 URL 경로나 누락된 파일을 찾을 수 있습니다.

Administration Server에서 Administration Server의 오류 로그 파일을 보려면 Preferences 탭을 선택하고 View Error Log 링크를 누릅니다.

서버 인스턴스의 오류 로그 파일을 보려면 Server Manager에서 Server Status 탭을 선택하고 View Error Log 링크를 누릅니다.

다음 오류 로그 예에는 다음과 같은 세 가지 항목이 있습니다.

```
20/May/2005:14:08:37] info ( 6141): CORE1116: Sun Java System Web Proxy
Server 4.0 B05/10/2005 01:26 20/May/2005:14:08:37] info ( 6142): CORE3274:
successful server startup 20/May/2005:14:08:37] security (23246):
for host 198.18.148.89 trying to GET /, deny-service reports:
 denying service of /
```

로그 분석기로 작업

server-root/extras/log_anly 디렉토리에는 Server Manager 사용자 인터페이스를 통해 실행할 수 있는 로그 분석 도구가 있습니다. 이 로그 분석기는 오직 공통 로그 형식의 파일만 분석합니다. 도구의 매개 변수를 설명하는 log_anly 디렉토리 내의 HTML 문서입니다. server-install/extras/ flexanlg 디렉토리에는 유연한 로그 파일 형식용 명령줄 로그 분석기가 있습니다. 그러나 Server Manager는 선택한 로그 파일 형식과 관계없이 기본적으로 유연한 로그 파일 보고 도구를 사용합니다.

로그 분석기를 사용하여 작동 요약, 가장 많이 액세스된 URL, 하루 중 서버에 대한 액세스가 가장 많은 시간, 등의 기본 서버에 대한 통계를 생성합니다. 또한 Proxy Server 또는 명령줄에서 로그 분석기를 실행할 수 있습니다.

flexanlg 명령줄 유틸리티를 실행하기 전에 반드시 라이브러리 경로를 설정해야 합니다. 다양한 플랫폼용 설정은 다음과 같습니다.

Solaris 및 Linux:

```
LD_LIBRARY_PATH=server-root/bin/proxy/lib:$LD_LIBRARY_PATH
```

AIX:

```
LIBPATH=server-root/bin/proxy/lib:$LIBPATH
```

HP-UX:

```
SHLIB_PATH=server-root/bin/proxy/lib:$SHLIB_PATH
```

Windows:

```
path=server-root\\bin\\proxy\\bin;%path%
```

주 – 로그 분석기를 실행하기 전에 서버 로그를 보관해야 합니다. 서버 로그 보관에 대한 자세한 내용은 170 페이지 “로그 파일 보관”을 참조하십시오.

또한 라이브러리 경로를 설정하는 대신 server-root/proxy-server*id* 디렉토리로 변경한 후 명령 프롬프트에서 ./start -shell을 입력할 수 있습니다.

Extended 또는 Extended-2 로깅 형식을 사용하는 경우 로그 분석기는 보고하도록 지정한 정보 외에도 출력 파일 내에 여러 보고서를 생성합니다. 다음 절에서는 이러한 보고서에 대해 설명합니다.

전송 시간 분산 보고서

전송 시간 분산 보고서는 프록시 서버가 요청을 전송하는 데 걸린 시간을 표시합니다. 이 보고서에는 서비스 시간 및 완료율(%)을 기준으로 분류된 정보가 표시됩니다. 다음은 전송 시간 분산 보고서의 예입니다.

서비스 시간 기준:

```
< 1 sec [644%] ....................................

< 2 sec [33.3%] ...................

< 3 sec [ 2.7%] .

< 4 sec [ 1.7%] .

< 5 sec [ 0.6%]

< 6 sec [ 0.4%]

< 7 sec [ 0.2%]

< 8 sec [ 0.0%]

< 9 sec [ 0.0%]
```

완료율(%) 기준:

```
< 1 sec [64.4%] ....................................

< 2 sec [97.7%] ..................................

< 3 sec [100.4%].........................................
```

데이터 흐름 보고서

데이터 흐름 보고서는 클라이언트에서 프록시, 프록시에서 클라이언트, 프록시에서 원격 서버 및 원격 서버에서 프록시로의 데이터 흐름(전송된 바이트 수)을 표시합니다. 보고서에는 이러한 각 시나리오에 대해 헤더 및 컨텐트 형식으로 전송된 데이터 양이 표시됩니다. 또한 데이터 흐름 보고서에는 캐시에서 클라이언트로의 데이터 흐름이 표시됩니다. 다음은 데이터 흐름 보고서의 예입니다.

	Headers	Content	Total
- Client -> Proxy.....	0 MB	0 MB	0 MB
- Proxy -> Client.....	0 MB	2 MB	3 MB
- Proxy -> Remote.....	0 MB	0 MB	0 MB
- Remote -> Proxy.....	0 MB	2 MB	2 MB
Approx:			
- Cache -> Client.....	0 MB	0 MB	0 MB

상태 코드 보고서

상태 코드 보고서는 프록시 서버가 원격 서버에서 수신하고 클라이언트로 전송한 상태 코드와 상태 코드 수를 표시합니다. 또한 상태 코드 보고서는 이러한 모든 상태 코드에 대한 설명을 제공합니다. 다음은 상태 코드 보고서의 예입니다.

Code	-From remote-	-To client-	-Explanation-
200	338 [70.7%]	352 [73.6%]	OK
302	33 [6.9%]	36 [7.5%]	Redirect
304	90 [18.8%]	99 [20.7%]	Not modified
404	3 [0.6%]	3 [0.6%]	Not found
407		5 [1.0%]	Proxy authorization required
500		2 [0.4%]	Internal server error
504		6 [1.3%]	Gateway timeout

요청 및 연결 보고서

요청 및 연결 보고서는 프록시 서버가 클라이언트에서 수신한 요청 수, 원격 서버에 대한 프록시 연결 수(초기 검색, 최신 상태 검사 및 새로 고침) 및 캐시된 문서를 사용하여 프록시 서버가 회피한 원격 연결 수를 표시합니다. 다음은 요청 및 연결 보고서의 예입니다.

```
- Total requests.............     478
- Remote connections.........     439
- Avoided remote connects....      39 [ 8.2%]
```

캐시 성능 보고서

캐시 성능 보고서는 클라이언트 캐시, 프록시 서버 캐시 및 직접 연결의 성능을 표시합니다.

클라이언트 캐시

클라이언트 캐시 적중은 클라이언트가 문서에서 최신 상태 검사를 수행하고 원격 서버가 클라이언트 문서가 수정되지 않았음을 알려 주는 304 메시지를 반환하는 경우 발생합니다. 클라이언트에 의해 시작된 최신 상태 검사는 클라이언트의 캐시 내에 고유한 문서 사본이 있음을 표시합니다.

클라이언트 캐시의 경우 보고서는 다음을 표시합니다.

- **Client and proxy cache hits:** 프록시 서버 및 클라이언트에 모두 요청된 문서의 사본이 있으며 프록시 사본과 관련된 최신 상태 검사를 위해 원격 서버를 쿼리한 다음 프록시 사본에 대해 클라이언트 요청을 평가하는 클라이언트 캐시 적중 횟수. 캐시 성능 보고서는 프록시가 처리한 이 유형의 요청 수와 이러한 요청을 처리하는 데 소요된 평균 시간을 표시합니다.
- **Proxy shortcut no-check:** 프록시 서버 및 클라이언트에 모두 요청된 문서의 사본이 있으며 프록시 서버가 원격 서버를 검사하지 않고 클라이언트에게 클라이언트 캐시의 문서가 최신 상태임을 알리는 클라이언트 적중 횟수. 캐시 성능 보고서는 프록시가 처리한 이 유형의 요청 수와 이러한 요청을 처리하는 데 소요된 평균 시간을 표시합니다.
- **Client cache hits only:** 클라이언트에만 요청된 문서의 사본이 있는 클라이언트 캐시 적중 횟수. 이러한 유형의 요청에서 프록시 서버는 직접 클라이언트의 If-modified-since GET 헤더를 터널링합니다. 캐시 성능 보고서는 프록시가 처리한 이 유형의 요청 수와 이러한 요청을 처리하는 데 소요된 평균 시간을 표시합니다.
- **Total client cache hits:** 총 클라이언트 캐시 적중 횟수 및 이러한 요청을 처리하는 데 소요된 평균 시간입니다.

프록시 캐시

프록시 캐시 적중은 클라이언트가 프록시 서버에서 문서를 요청하고 프록시 서버의 캐시에 이미 문서가 있는 경우 발생합니다. 프록시 서버의 캐시 적중 횟수의 경우 보고서는 다음을 표시합니다.

- **Proxy cache hits with check:** 문서에 대한 최신 상태 검사를 위해 프록시 서버가 원격 서버를 쿼리하는 프록시 캐시 적중 횟수. 캐시 성능 보고서는 프록시가 처리한 이 유형의 요청 수와 이러한 요청을 처리하는 데 소요된 평균 시간을 표시합니다.

- **Proxy cache hits without check:**프록시 서버의 프록시 캐시 적중 횟수는 문서에 대한 최신 상태를 검사하기 위해 원격 서버를 쿼리하지 **않습니다**. 캐시 성능 보고서는 프록시가 처리한 이 유형의 요청 수와 이러한 요청을 처리하는 데 소요된 평균 시간을 표시합니다.
- **pure proxy cache hits:**클라이언트에 요청된 문서의 사본이 없는 프록시 캐시 적중 횟수. 캐시 성능 보고서는 프록시가 처리한 이 유형의 요청 수와 이러한 요청을 처리하는 데 소요된 평균 시간을 표시합니다.

결합된 프록시 캐시 적중 횟수

결합된 프록시 캐시 적중 횟수의 경우 보고서는 총 프록시 서버 캐시 적중 횟수 및 이러한 요청을 처리하는 데 소요된 평균 시간을 표시합니다.

직접 트랜잭션

직접 트랜잭션은 캐시 적중 횟수 없이 원격 서버에서 프록시 서버를 통해 클라이언트로 직접 이동하는 트랜잭션입니다. 직접 트랜잭션의 경우 보고서는 다음을 표시합니다.

- **Retrieved documents:**원격 서버에서 직접 검색한 문서입니다. 캐시 성능 보고서는 프록시가 처리한 이러한 유형의 요청, 이러한 요청을 처리하는 데 소요된 평균 시간 및 총 트랜잭션 비율(%)을 표시합니다.
- **Other transactions:**200 또는 304 이외의 상태 코드로 반환된 트랜잭션입니다. 캐시 성능 보고서는 프록시가 처리한 이 유형의 요청 수 및 이러한 요청을 처리하는 데 소요된 평균 시간을 표시합니다.
- **Total direct traffic:**클라이언트에서 원격 서버로 직접 이동한 요청입니다(실패한 요청 및 성공적으로 검색된 문서 모두). 캐시 성능 보고서는 프록시가 처리한 이 유형의 요청, 이러한 요청을 처리하는 데 소요된 평균 시간 및 총 트랜잭션 비율(%)을 표시합니다.

다음은 캐시 성능 보고서의 예입니다.

```
                    CLIENT CACHE:
- Client & proxy cache hits... 86 reqs [18.0%] 0.21 sec/req- Proxy shortcut
no-check........ 13 reqs [ 2.7%] 0.00 sec/req- Client cache hits only.....
- TOTAL client cache hits.......... 99 reqs [20.7%] 0.18 sec/req

                    PROXY CACHE:
- Proxy cache hits w/check........ 4 reqs [ 0.8%] 0.50 sec/req- Proxy cache
hits w/o check.. 10 reqs [ 2.1%] 0.00 sec/req- Pure proxy cache hits......
14 reqs [ 2.9%] 0.14 sec/req

                    PROXY CACHE HITS COMBINED:
- TOTAL proxy cache hits....... 113 reqs [23.6%] 0.18 sec/req

                    DIRECT TRANSACTIONS:
- Retrieved documents..313 reqs [65.5%]  0.90 sec/req 2 MB- Other
```

```
transactions.. 52 reqs [10.9%] 7.79 sec/req- TOTAL direct traffic..
365 reqs [76.4%] 1.88 sec/req 2 MB
```

전송 시간 보고서

전송 시간 보고서는 프록시 서버에서 트랜잭션을 처리하는 데 소요한 시간 정보를 표시합니다. 이 보고서에서는 다음 범주에 대한 값을 표시합니다.

Average transaction time: 기록된 모든 전송 시간의 평균.

Average transfer time without caching: 캐시에서 반환되지 않은 트랜잭션(원격 서버에서 200 응답 반환)의 평균 전송 시간.

Average with caching, without errors: 모든 비오류 트랜잭션(2xx 및 3xx 상태 코드)에 대한 평균 전송 시간.

Average transfer time improvement: 오류 없이 캐시된 평균 전송 시간을 평균 트랜잭션 시간에서 제한 값.

다음은 전송 시간 보고서의 예입니다.

```
- Average transaction time... 1.48 sec/req- Ave xfer time w/o caching..
    0.90 sec/req- Ave w/caching, w/o errors.. 0.71 sec/req - Ave xfer
    time improvement.. 0.19 sec/req
```

시간별 작동 보고서

각 분석된 시간에 대해 시간별 작동 보고서는 다음을 표시합니다.

- 로드 평균
- 원격 서버에 대한 최신 상태 검사가 없는 캐시 적중 횟수
- 문서가 최신 상태이고 문서가 클라이언트 캐시에 있음을 증명하는 원격 서버에 대한 최신 상태 검사를 포함한 프록시 서버의 캐시 적중 횟수
- 문서가 최신 상태이고 문서가 클라이언트 캐시에 **없음**을 증명하는 원격 서버에 대한 최신 상태 검사를 포함한 프록시 서버의 캐시 적중 횟수
- 문서 일부가 업데이트되도록 하는 원격 서버에 대한 최신 상태 검사를 포함한 프록시 서버의 캐시 적중 횟수
- 요청된 문서의 새 사본을 200 상태 코드로 반환한 원격 서버에 대한 최신 상태 검사를 포함한 프록시 서버의 캐시 적중 횟수
- 프록시 서버의 캐시 적중 횟수 없이 원격 서버에서 직접 문서를 검색한 요청 수

▼ Server Manager에서 로그 분석기를 실행하는 방법

1. **Server Manager에 액세스하고 Server Status 탭을 누릅니다.**
2. **Generate Report 링크를 누릅니다.**
   Generate Report 페이지가 표시됩니다.
3. **서버 이름을 입력합니다. 이 이름은 생성된 보고서에 나타납니다.**
4. **보고서를 HTML 또는 ASCII 형식으로 표시할지 여부를 선택합니다.**
5. **분석할 로그 파일을 선택합니다.**
6. **결과를 파일로 저장하려면 Output File 필드에 출력 파일 이름을 입력합니다.**
   필드를 비워두면 보고서 결과가 화면으로 출력됩니다. 로그 파일이 큰 경우 출력을 화면에 표시하는 데 시간이 많이 걸릴 수 있으므로 결과를 저장해야 합니다.
7. **특정 서버 통계에 대한 총계 생성 여부를 선택합니다.**
   다음 총계를 생성할 수 있습니다.
   - **Total Hits**- 액세스 로깅을 활성화한 이후 서버가 수신한 총 적중 횟수.
   - **304 (Not Modified) Status Codes**- 페이지를 반환하는 서버가 아니라 요청한 문서의 로컬 복사본이 사용된 횟수.
   - **302 (Redirects) Status Codes**- 원래 URL이 이동하여 서버가 새 URL로 리디렉션한 횟수.
   - **404 (Not Found) Status Codes**- 서버가 요청된 문서를 찾을 수 없거나 클라이언트가 인증된 사용자가 아니므로 문서를 서비스하지 않은 횟수.
   - **500 (Server Error) Status Codes**- 서버 관련 오류가 발생한 횟수.
   - **Total Unique URLs**- 액세스 로그를 활성화한 후 액세스된 고유 URL의 수.
   - **Total Unique Hosts**- 액세스 로그를 활성화한 후 서버에 액세스한 고유 호스트의 수.
   - **Total Kilobytes Transferred**- 액세스 로그를 활성화한 후부터 서버가 전송한 데이터 양(KB).
8. **일반 통계 생성 여부를 선택합니다. 일반 통계를 생성하는 경우 다음 옵션을 선택합니다.**
   - **Find Top** *Number* **Seconds Of Log**- 가장 최신 초 단위 수의 정보를 기반으로 통계를 생성합니다.
   - **Find Top** *Number* **Minutes Of Log**-
   - 가장 최신 분 단위 수의 정보를 기반으로 통계를 생성합니다.
   - **Find Top** *Number* **Hours Of Log**- 가장 최신 시간 단위 수의 정보를 기반으로 통계를 생성합니다.

- **Find** *Number* **Users (If Logged)**- 사용자 수의 정보를 기반으로 통계를 생성합니다.
- **Find Top** *Number* **Referers (If Logged)**- 참조자 수의 정보를 기반으로 통계를 생성합니다.
- **Find Top** *Number* **User Agents (If Logged)**- 브라우저 유형, 버전 및 운영 체제 등의 사용자 에이전트에 대한 정보를 기반으로 통계를 생성합니다.
- **Find Top** *Number* **Miscellaneous Logged Items (If Logged)**- 사용자 수의 정보를 기반으로 통계를 생성합니다.

9 목록 생성 여부를 선택합니다.

목록을 생성하는 경우 목록을 생성하려는 대상 항목을 다음 목록에서 지정합니다.

- **URLs Accessed**- 액세스한 URL을 표시합니다.
- *Number* **Most Commonly Accessed URL**- 가장 많이 액세스된 URL 또는 지정된 횟수보다 많이 액세스된 URL을 표시합니다.
- **URLs That Were Accessed More Than** *Number* **Times**- 지정된 횟수보다 많이 액세스된 URL을 표시합니다.
- **Hosts Accessing Your Server**- Proxy Server에 액세스한 호스트를 표시합니다.
- *Number* **Hosts Most Often Accessing Your Server**- 서버에 가장 자주 액세스한 호스트 또는 지정된 횟수보다 많이 서버에 액세스한 호스트를 표시합니다.
- **Hosts That Accessed Your Server More Than** *Number* **Times**- 지정된 횟수보다 많이 서버에 액세스한 호스트를 표시합니다.

10 결과를 표시할 순서를 지정합니다.

우선 순위를 1에서 3까지 지정하여 각 세션이 보고서에 표시될 순서를 정합니다. 특정 세션을 생성하지 않기로 하면 해당 세션은 자동으로 무시됩니다. 각 섹션은 다음과 같습니다.

- Find Totals
- General Statistics
- Make Lists

11 OK를 누릅니다.

새 창에 보고서가 표시됩니다.

명령줄에서 로그 분석기 실행 방법

명령줄에서 액세스 로그 파일을 분석하려면 `flexanlg` 도구를 실행합니다. 이 도구는 `server-install/extras/flexanlg` 디렉토리에 있습니다.

`flexanlg`를 실행하려면 명령 프롬프트에서 다음 명령 및 옵션을 입력합니다.

```
./flexanlg [-n name] [-x] [-r] [-p order] [-i file]* [ -m metafile ]* [-o
file][-c opts] [-t opts] [-l opts]
```

*가 표시된 옵션은 반복할 수 있습니다.

```
You can display this information online by
typing ./flexanlg -h.

-P: proxy log format                                    Default: no
-n servername: The name of the server
-x : Output in HTML                                     Default: no
-r : Resolve IP addresses to hostnames                  Default: no
-p [c,t,l]: Output order (counts, time stats, lists)  Default: ctl
-i filename: Input log file                             Default: none
-o filename: Output log file                            Default: stdout
-m filename: Meta file                                  Default: none
-c [h,n,r,f,e,u,o,k,c,z]: Count these item(s) -       Default: hnreuokc
    h: total hits
    n: 304 Not Modified status codes (Use Local Copy)
    r: 302 Found status codes (Redirects)
    f: 404 Not Found status codes (Document Not Found)
    e: 500 Server Error status codes (Misconfiguration)
    u: total unique URL's
    o: total unique hosts
    k: total kilobytes transferred
    c: total kilobytes saved by caches
    z: Do not count any items.
-t [sx,mx,hx, xx,z]: Find time stats -      Default:s5m5h10u10a10r10x10
    s(number): Find top (number) seconds of log
    m(number): Find top (number) minutes of log
    h(number): Find top (number) hours of log
    u(number): Find top (number) users of log
    a(number): Find top (number) user agents of log
    r(number): Find top (number) referers of log
    x(number): Find top (number) for miscellaneous keywords
    z: Do not find any time stats.
-l [cx,hx]: Make a list of -                            Default: c+3h5
    c(x,+x): Most commonly accessed URL's
             (x: Only list x entries)
             (+x: Only list if accessed more than x times)
    h(x,+x): Hosts (or IP addresses) most often accessing your server
             (x: Only list x entries)
             (+x: Only list if accessed more than x times)
    z: Do not make any lists.
```

이벤트 보기(Windows)

서버 오류 로그에 오류를 기록하는 것 외에 Proxy Server는 이벤트 뷰어에 심각한 시스템 오류를 기록합니다. 이벤트 뷰어를 사용하여 시스템의 이벤트를 모니터링할 수 있습니다. 이벤트 뷰어를 사용하여 기능적 구성 문제로 인한 오류를 볼 수 있습니다. 이 오류는 오류 로그가 열리기 전에 발생할 수 있습니다.

▼ 이벤트 뷰어 사용 방법

1. **시작 메뉴에서 모든 프로그램을 선택한 후 관리 도구를 선택합니다.**
   관리 도구 프로그램 그룹에서 이벤트 뷰어를 선택합니다.

2. **로그 메뉴에서 응용 프로그램을 선택합니다.**
   이벤트 뷰어에 응용 프로그램 로그가 표시됩니다. Proxy Server의 오류에는 `proxy-server`*id*의 소스 레이블이 포함됩니다.

3. **보기 메뉴에서 찾기를 선택하여 로그에서 이들 레이블 중 한 가지를 검색합니다.**
   로그 항목을 업데이트하려면 보기 메뉴에서 새로 고침을 선택합니다.

   이벤트 뷰어에 대한 자세한 내용은 시스템 설명서를 참조하십시오.

◆ ◆ ◆ 10장

10 서버 모니터링

이 장에서는 내장 모니터링 도구 및 SNMP(Simple Network Management Protocol) 등을 포함하여 서버를 모니터링하는 방법에 대해 설명합니다.

SNMP를 Sun Java System MIB(Management Information Bases) 및 HP OpenView 등의 네트워크 관리 소프트웨어와 함께 사용하여 네트워크의 다른 장치를 모니터링하는 것처럼 서버를 실시간으로 모니터링할 수 있습니다.

주 – Windows의 경우 Proxy Server 4를 설치하기 전에 시스템에 Windows SNMP 구성 요소가 설치되어 있어야 합니다.

서버의 상태는 통계 기능이나 SNMP를 사용하여 실시간으로 확인할 수 있습니다. UNIX나 Linux를 사용하는 경우 SNMP를 사용하려면 Proxy Server를 SNMP에 맞게 구성해야 합니다.

이 장은 다음 내용으로 구성되어 있습니다.

- 192 페이지 “통계를 사용하여 서버 모니터링”
- 201 페이지 “SNMP 기초”
- 203 페이지 “SNMP 설정”
- 204 페이지 “프록시 SNMP 에이전트 사용(UNIX)”
- 205 페이지 “SNMP 원시 에이전트 재구성”
- 206 페이지 “SNMP 마스터 에이전트 설치”
- 207 페이지 “SNMP 마스터 에이전트 사용 설정 및 시작”
- 211 페이지 “SNMP 마스터 에이전트 구성”
- 212 페이지 “하위 에이전트 사용 설정”
- 212 페이지 “SNMP 메시지 이해”

통계를 사용하여 서버 모니터링

통계 기능을 사용하여 서버의 현재 작동을 모니터링할 수 있습니다. 통계에는 서버가 처리하는 요청의 수와 해당 요청을 처리하는 상태 등이 표시됩니다. 대화형 서버 모니터에 서버가 많은 수의 요청을 처리하고 있는 것으로 표시되면 요청을 수용하도록 서버 구성 또는 시스템의 네트워크 커널을 조정할 수 있습니다. 통계를 수집하면 Proxy Server에 오버헤드가 추가되므로 통계는 기본적으로 비활성화되어 있습니다. 통계를 사용 설정하면 서버가 통계 정보를 수집하고 저장하기 시작합니다.

통계를 사용 설정하면 다음 영역에서 통계를 볼 수 있습니다.

- 연결
- DNS
- KeepAlive
- 캐시
- 서버 요청

대화형 서버 모니터가 보고하는 다양한 서버 통계 전체에 대한 설명은 온라인 도움말의 Monitor Current Activity 페이지를 참조하십시오.

Proxy Server 통계 처리

Proxy Server 통계 수집에는 `stats-xml`이라고 하는 내장 함수가 사용됩니다. Server Manager에서 통계를 보거나 `perfdump` 함수를 사용하여 보고서를 생성하려면 이 내장 함수를 사용해야 합니다. 또한 `stats-xml` 함수는 프로필링 사용 설정에도 사용되는데, 이것은 사용자 정의 NSAPI 함수를 사용한 통계 모니터링의 요구 사항입니다. 서버에서 통계와 프로필링을 사용 설정하면 `obj.conf` 파일에서 `stats-init`라는 서버 함수가 초기화되어 통계 수집을 시작합니다.

```
Init profiling="on" fn="stats-init"
```

또한 이 명령은 브라우저 창에서 통계에 액세스할 수 있게 해 주는 `NameTrans` 지시문을 만듭니다.

```
NameTrans fn="assign-name" name="stats-xml" from="(/stats-xml|/stats-xml/.*)
```

마지막으로, 통계를 사용 설정하면 `NameTrans` 지시문이 선택되었을 때 `stats-xml` 함수를 처리하기 위한 `Service` 지시문이 추가됩니다.

```
<Object name="stats-xml">

Service fn="stats-xml"

</Object>
```

통계 수집은 `obj.conf`의 Init 함수를 업데이트합니다. 따라서 이러한 변경 내용을 적용하려면 서버를 중지한 다음 다시 시작해야 합니다.

다음 예는 obj.conf 파일의 stats-init를 보여 줍니다.

```
Init profiling="on" fn="stats-init" update-interval="5"
```

다음 값을 지정할 수도 있습니다.

- **update-interval.**통계 업데이트 간의 기간(초)입니다. 설정이 높을수록(빈도 낮음) 성능이 향상됩니다. 최소값은 1이고 기본값은 5입니다.
- **profiling.**NSAPI 성능 프로필링의 사용 설정 여부입니다. 기본값은 *no*로, 서버 성능이 약간 향상됩니다. 하지만 사용자 인터페이스를 통해 통계를 사용 설정하면 기본적으로 프로필링이 켜집니다.

다음 URL을 사용하여 stats-xml 출력을 검색할 수 있습니다.

```
http://computer_name:proxyport /stats-xml/proxystats.xml
```

이 요청은 Proxy Server 통계가 포함된 XML 페이지를 반환합니다. 일부 브라우저에서는 브라우저 창 안에서 데이터를 볼 수 있지만 다른 일부 브라우저의 경우 데이터를 외부 파일로 저장한 다음 외부 뷰어에서 볼 수 있습니다. 이 정보는 데이터의 다양한 보기에 대한 통계를 분석하기 위해 구문 분석할 수 있어야 유용합니다. 타사 도구를 사용하여 구문 분석 과정에 도움을 받을 수 있습니다. 구문 분석 도구가 없는 경우에는 Server Manager 또는 perfdump SAF를 통해 stats-xml 출력을 가장 잘 확인할 수 있습니다.

stats-xml 출력에 대한 액세스 제한

브라우저에서 서버의 stats-xml 통계를 볼 수 있는 사용자를 제한하려면 /stats-xml URI에 대한 ACL을 만들어야 합니다.

ACL 파일은 obj.conf 파일의 stats-xml 객체 정의에서도 참조되어야 합니다. 예를 들어 /stats-xml URI에 대해 명명된 ACL을 만든 경우 다음과 같이 객체 정의의 PathCheck문에서 ACL 파일을 참조해야 합니다.

```
<Object name="stats-xml">

PathCheck fn="check-acl" acl="stats.acl"

Service fn="stats-xml"

</Object>
```

통계 사용 설정

성능을 모니터링하려면 Proxy Server에서 통계를 사용 설정해야 합니다. Server Manager를 통해 또는 obj.conf 및 magnus.conf 파일을 편집하여 통계를 사용 설정할 수 있습니다. 모니터링 및 조정을 위한 자동화된 도구를 만들거나 사용자 정의된 프로그램을 작성하는 사용자의 경우 stats-xml로 직접 작업할 수도 있습니다.

주의 – 통계/프로필 작성을 사용하는 경우 서버의 모든 사용자가 통계 정보를 사용할 수 있습니다.

▼ Server Manager에서 통계를 사용 설정하는 방법

1. **Server Manager에 액세스하여 Server Status 탭을 누릅니다.**
2. **Monitor Current Activity 링크를 누릅니다.**
   Monitor Current Activity 페이지가 표시됩니다.
3. **Activate Statistics/Profiling에 대해 예 옵션을 선택하여 통계를 사용 설정합니다.**
4. **OK를 누릅니다.**
5. **Restart Required를 누릅니다.**
   Apply Changes 페이지가 나타납니다.
6. **Restart Proxy Server 버튼을 눌러 변경 사항을 적용합니다.**

▼ stats-xml을 사용하여 통계를 사용 설정하는 방법

1. **obj.conf 파일의 기본 객체 아래에 다음 줄을 추가합니다.**

```
NameTrans fn="assign-name" name="stats-xml" from="
(/stats-xml|/stats-xml/.*)"
```

2. **obj.conf에 다음 Service 함수를 추가합니다.**

```
<Object name="stats-xml">

Service fn="stats-xml"

</Object>
```

3. **obj.conf에 stats-init SAF를 추가합니다.**

통계 사용

통계를 활성화하면 서버 인스턴스가 어떻게 실행되고 있는지에 대한 다양한 정보를 얻을 수 있습니다. 통계는 기능적 영역으로 나누어집니다.

Server Manager에 통계 표시

이 절에서는 Server Manager에서 `proxystats.xml` 데이터의 하위 집합을 볼 수 있는 방법에 대해 설명합니다.

Proxy Server 연결, DNS 처리, 연결 유지 값, 캐시 및 서버 요청에 대한 정보의 총계, 최대값, 최고 수 및 막대 그래프를 볼 수 있습니다.

다음 절에서는 이러한 각 영역에 대해 얻을 수 있는 정보의 유형에 대해 설명합니다.

연결 상태

Server Manager에서는 다음 연결 통계를 사용할 수 있습니다.

- 총 연결 수
- 대기열에 있는 연결의 최대 수
- 대기열에 있는 연결의 최고 수
- 현재 대기열에 있는 연결의 수
- 프로세스의 수

DNS 통계

Server Manager에서 사용할 수 있는 DNS 통계는 다음과 같습니다.

- DNS 캐시 최대 항목
- 프로세스의 수
- DNS 캐시 적중 횟수(막대 그래프로도 표시됨)
- DNS 캐시 누락 횟수(막대 그래프로도 표시됨)

연결 유지 통계

Server Manager에서 사용할 수 있는 연결 유지 통계는 다음과 같습니다.

- 최대 연결 유지 연결
- 연결 유지 시간 초과
- 프로세스의 수
- 연결 유지 적중 횟수(막대 그래프로도 표시됨)
- 연결 유지 플러시 횟수(막대 그래프로도 표시됨)
- 연결 유지 거부 횟수(막대 그래프로도 표시됨)
- 연결 유지 시간 초과 횟수(막대 그래프로도 표시됨)

서버 요청 통계

Server Manager에서 사용할 수 있는 서버 통계는 다음과 같습니다.

- 총 요청 수
- 수신된 바이트 수
- 전송된 바이트 수
- 프로세스 수

- HTTP 서버 코드당 요청 내역(막대 그래프로도 표시됨). 예를 들어 HTTP 서버 코드 200은 이행된 요청을 의미합니다.

▼ 통계에 액세스하는 방법

1. **Server Manager에 액세스하여 Server Status 탭을 누릅니다.**
2. **Monitor Current Activity 링크를 누릅니다.**
3. **Select Refresh Interval 드롭다운 목록에서 Refresh Interval을 선택합니다.**
   새로 고침 간격은 표시되는 통계 정보를 업데이트하는 간격(초)입니다.
4. **표시할 통계의 종류를 Select Statistics To Be Displayed 드롭다운 목록에서 선택합니다.**
   통계의 유형에 대한 자세한 내용은 195 페이지 “Server Manager에 통계 표시”를 참조하십시오.
5. **Submit를 누릅니다.**
   서버 인스턴스가 실행 중이며 통계/프로필링을 사용하는 경우 선택한 종류의 통계를 표시하는 페이지가 나타납니다. 페이지는 새로 고침 간격 값에 따라 5-15초마다 업데이트됩니다.
6. **드롭다운 목록에서 프로세스 아이디를 선택합니다.**
   Server Manager를 통해 현재 활동을 볼 수 있지만 이러한 범주가 서버의 조정에 직접 관련된 것은 아닙니다. `perfdump` 통계는 서버를 조정할 때 권장됩니다. 자세한 내용은 다음 절을 참조하십시오.

perfdump 유틸리티를 사용하여 현재 활동 모니터링

`perfdump` 유틸리티는 Proxy Server 내부 통계에서 다양한 성능 데이터를 수집하여 ASCII 텍스트로 표시하는 Proxy Server에 내장된 SAF(Server Application Function)입니다. `perfdump` 유틸리티를 사용하면 Server Manager를 통해 사용 가능한 것보다 훨씬 다양한 통계를 모니터링할 수 있습니다.

`perfdump`를 사용하면 통계가 통합됩니다. 단일 프로세스를 모니터링하는 것이 아니라 프로세스 수에 따라 배가된 통계가 표시되므로 서버 전체를 보다 정확하게 모니터링할 수 있습니다.

perfdump 유틸리티 사용 설정

`perfdump` SAF는 `stats-xml` 함수를 사용한 후에만 사용 설정할 수 있습니다.

▼ perfdump SAF를 사용 설정하는 방법

1 **obj.conf 파일에서 기본 객체 뒤에 다음 객체를 추가합니다.**

```
<Object name="perf">
Service fn="service-dump"
</Object>
```

2 **기본 객체에 다음 줄을 추가합니다.**

```
NameTrans fn=assign-name from="/.perf" name="perf"
```

3 **서버 소프트웨어를 다시 시작합니다.**

4 **http://*computer_name*:*proxyport*/.perf로 이동하여 perfdump에 액세스합니다.**

perfdump 통계를 요청하고 브라우저가 자동으로 새로 고침을 수행할 간격(초)을 지정할 수 있습니다. 다음 예에서는 5초마다 새로 고침을 설정합니다.

```
http://computer_name:proxyport/.perf?refresh=5
```

perfdump 출력 샘플

다음 예는 perfdump 출력 샘플을 보여 줍니다.

```
proxyd pid: 6751

Sun Java System Web Proxy Server 4.0 B05/02/2005 15:32 (SunOS DOMESTIC)

Server started Thu May 19 13:15:14 2005
Process 6751 started Thu May 19 13:15:14 2005

ConnectionQueue:
----------------------------------------
Current/Peak/Limit Queue Length            0/1/4096
Total Connections Queued                   1
Average Queue Length (1, 5, 15 minutes)    0.00, 0.00, 0.00
Average Queueing Delay                     0.09 milliseconds

ListenSocket ls1:
------------------------
Address                    http://0.0.0.0:8081
Acceptor Threads           1

KeepAliveInfo:
--------------------
KeepAliveCount        0/256
```

```
KeepAliveHits         0
KeepAliveFlushes      0
KeepAliveRefusals     0
KeepAliveTimeouts     0
KeepAliveTimeout      30 seconds

SessionCreationInfo:
------------------------
Active Sessions           1
Keep-Alive Sessions       0
Total Sessions Created    48/128

DiskCacheInfo:
------------------
Hit Ratio               0/0 (  0.00%)
Misses                  0
Cache files at startup  0
Cache files created     0
Cache files cleaned up  0

Native pools:
---------------------------
NativePool:
Idle/Peak/Limit               1/1/128
Work Queue Length/Peak/Limit  0/0/0

Server DNS cache disabled

Async DNS disabled

Performance Counters:
-----------------------------------------------
 ......................Average         Total      Percent

Total number of requests:                    1
Request processing time:    0.2559        0.2559

default-bucket (Default bucket)
Number of Requests:                          1    (100.00%)
Number of Invocations:                       7    (100.00%)
Latency:                    0.2483        0.2483    ( 97.04%)
Function Processing Time:   0.0076        0.0076    (  2.96%)
Total Response Time:        0.2559        0.2559    (100.00%)

Sessions:
---------------------------
Process  Status     Function
6751     response   service-dump
```

이 매개 변수에 대한 자세한 내용은 Sun ONE Web Server 6.1 *Performance Tuning, Sizing, and Scaling Guide*의 2장 "Using Statistics to Tune Your Server"를 참조하십시오.

perfdump 출력에 대한 액세스 제한

브라우저에서 서버의 perfdump 통계를 볼 수 있는 사용자를 제한하려면 /.perf URI에 대한 ACL을 만들어야 합니다.

또한 ACL 파일이 obj.conf 파일의 perf 객체 정의에서 참조되어야 합니다. 예를 들어 /.perf URI에 대해 명명된 ACL을 만든 경우 다음과 같이 객체 정의의 PathCheck문에서 ACL 파일을 참조해야 합니다.

```
<Object name="perf">

PathCheck fn="check-acl" acl="perf.acl"

Service fn="service-dump"

</Object>
```

성능 버킷 사용

성능 버킷을 통해 버킷을 정의하여 여러 서버 함수에 연결할 수 있습니다. 이러한 함수 중 하나가 호출될 때마다 서버는 통계 데이터를 수집하여 버킷에 추가합니다. 예를 들어 send-cgi 및 NSServletService는 각각 CGI와 Java 서블릿 요청을 서비스하는 데 사용됩니다. CGI 및 서블릿 요청에 대해 두 개의 버킷을 정의하여 별도의 카운터를 유지하거나 두 가지 동적 컨텐트 유형 모두에 대한 요청을 계산하는 버킷을 하나 만들 수 있습니다. 이러한 정보의 수집 비용은 매우 낮으며 보통 서버 성능에 거의 영향을 미치지 않습니다. 이러한 정보는 나중에 perfdump 유틸리티를 사용하여 액세스할 수 있습니다.

버킷에는 다음 정보가 저장됩니다.

- **버킷의 이름**- 이 이름은 버킷과 함수를 연결시키는 데 사용됩니다.
- **설명**- 버킷이 연결된 함수에 대한 설명입니다.
- **이 함수에 대한 요청 수**- 이 함수를 호출한 요청의 총 수입니다.
- **함수가 호출된 횟수**- 하나의 요청에 대해 두 번 이상 실행되는 함수도 있으므로 이 수는 함수에 대한 요청 수와 일치하지 않을 수 있습니다.
- **함수 대기 또는 디스패치 시간**- 서버가 함수 호출에 사용한 시간입니다.
- **함수 시간**- 함수 자체에 소요된 시간입니다.

default-bucket은 서버에 의해 미리 정의됩니다. 사용자 정의된 버킷에 연결되지 않은 함수의 통계를 기록합니다.

구성

성능 버킷 magnus.conf 및 obj.conf 파일의 모든 구성 정보를 지정해야 합니다. 기본 버킷만 자동으로 사용 설정됩니다.

먼저 196 페이지 “perfdump 유틸리티를 사용하여 현재 활동 모니터링”의 설명에 따라 성능 측정을 활성화해야 합니다.

다음 예는 magnus.conf 파일에서 새 버킷을 정의하는 방법을 보여 줍니다.

```
Init fn="define-perf-bucket" name="acl-bucket" description="ACL bucket"

Init fn="define-perf-bucket" name="file-bucket" description="Non-cached
responses"

Init fn="define-perf-bucket" name="cgi-bucket" description="CGI Stats"
```

이 예에서는 acl-bucket, file-bucket 및 cgi-bucket의 세 가지 버킷을 만듭니다. 이 버킷을 함수와 연결하려면 성능을 측정할 obj.conf 함수에 bucket=*bucket-name*을 추가합니다.

예

```
PathCheck fn="check-acl" acl="default" bucket="acl-bucket"

...

Service method="(GET|HEAD|POST)" type="*~magnus-internal/*" fn="send-file"
bucket="file-bucket"

...

<Object name="cgi">

ObjectType fn="force-type" type="magnus-internal/cgi"

Service fn="send-cgi" bucket="cgi-bucket"

</Object>
```

성능 보고서

버킷의 서버 통계는 perfdump 유틸리티를 사용하여 액세스할 수 있습니다. 성능 버킷 정보는 perfdump에서 반환된 보고서의 마지막 섹션에 있습니다.

보고서에는 다음 정보가 포함되어 있습니다.

- 요청된 각 통계의 평균, 총계 및 백분율 열
- Request Processing Time은 서버가 지금까지 수신한 모든 요청을 처리하는 데 소요된 총 시간입니다.

- Number of Requests는 함수에 대한 요청의 총 수입니다.
- Number of Invocations는 함수가 호출된 총 횟수입니다. 하나의 요청을 처리하는 동안 함수가 여러 번 호출될 수 있기 때문에 이 값은 요청 수와 다릅니다. 이 행의 백분율 열은 모든 버킷의 총 호출 수를 참조하여 계산됩니다.
- Latency는 Proxy Server가 함수 호출을 준비하는 데 사용하는 시간(초)입니다.
- Function Processing Time은 Proxy Server가 함수 내에서 소비한 시간(초)입니다. Function Processing Time 및 Total Response Time의 백분율은 총 Request Processing Time을 참조하여 계산됩니다.
- Total Response Time은 Function Processing Time 및 Latency의 시간(초)의 합계입니다.

다음 예는 `perfdump`를 통해 사용할 수 있는 샘플 성능 버킷 정보를 보여 줍니다.

```
Performance Counters:
------------------------------------------------
                            Average         Total      Percent

Total number of requests:                       1
Request processing time:    0.2559        0.2559

default-bucket (Default bucket)
Number of Requests:                             1    (100.00%)
Number of Invocations:                          7    (100.00%)
Latency:                    0.2483        0.2483    ( 97.04%)
Function Processing Time:   0.0076        0.0076    (  2.96%)
Total Response Time:        0.2559        0.2559    (100.00%)
```

SNMP 기초

SNMP는 네트워크 작동에 대한 데이터를 교환하는 데 사용되는 프로토콜입니다. SNMP를 사용하면 데이터가 관리 대상 장치와 네트워크 관리 스테이션(NMS) 사이를 이동합니다. 관리 대상 장치는 호스트, 라우터, 프록시 서버 및 네트워크의 기타 서버 등과 같이 SNMP를 실행하는 모든 장치입니다. NMS는 해당 네트워크를 원격으로 관리하는 데 사용되는 시스템입니다. 일반적으로 NMS 소프트웨어는 수집된 데이터를 표시하는 그래프를 제공하거나 해당 데이터를 사용하여 서버가 특정 허용 한계 내에서 작동하는지 확인합니다.

NMS는 일반적으로 하나 이상의 네트워크 관리 응용 프로그램이 설치된 강력한 워크스테이션입니다. HP OpenView와 같은 네트워크 관리 응용 프로그램은 웹 서버 등의 관리 대상 장치에 대한 정보를 그래픽으로 표시합니다. 이 정보에는 회사에서 작동 또는 중지된 서버를 표시하거나 수신된 오류 메시지의 수와 유형이 포함될 수 있습니다. 프록시 서버에서 SNMP를 사용하는 경우 이 정보는 하위 에이전트와 마스터 에이전트의 두 가지 에이전트 유형을 통해 NMS와 서버 사이에 전송됩니다.

하위 에이전트는 서버에 대한 정보를 수집하고 정보를 서버의 마스터 에이전트로 전달합니다. Administration Server를 제외한 모든 서버에는 하위 에이전트가 있습니다.

주 – SNMP 구성을 변경한 후에는 Apply Required를 눌러 SNMP 하위 에이전트를 다시 시작해야 합니다.

마스터 에이전트는 NMS와 통신합니다. 마스터 에이전트는 Administration Server에 설치됩니다.

호스트 컴퓨터에 여러 개의 하위 에이전트가 있을 수 있으나 마스터 에이전트는 하나만 있어야 합니다. 예를 들어 동일한 호스트에 Directory Server, Proxy Server 및 Messaging Server가 설치된 경우 각 서버의 하위 에이전트가 동일한 마스터 에이전트와 통신합니다.

MIB(Management Information Base)

Proxy Server는 네트워크 관리에 관련된 변수를 저장합니다. 마스터 에이전트가 액세스할 수 있는 변수를 관리된 객체라고 합니다. 이러한 객체는 MIB(Management Information Base)라고 하는 트리 형태 구조로 정의됩니다. MIB는 Proxy Server 네트워크 구성, 상태 및 통계에 대한 액세스를 제공합니다. SNMP를 사용하면 NMS에서 이 정보를 볼 수 있습니다.

MIB 트리의 최상위 수준에는 인터넷 객체 아이디가 표시되며, 여기에는 directory, mgmt, experimental 및 private의 하위 트리가 있습니다. private 하위 트리에는 enterprises 노드가 있습니다. enterprises의 각 하위 트리는 개별 엔터프라이즈에 지정되며, 해당 엔터프라이즈는 자체 특정 MIB 확장자를 등록한 조직입니다. 따라서 엔터프라이즈는 자체의 하위 트리에 제품 특정 하위 트리를 만들 수 있습니다. 회사가 만든 MIB는 enterprises 노드 아래에 위치합니다. Sun Java System 서버 MIB는 enterprises 노드 아래에도 있습니다. 각 Sun Java System 서버 하위 에이전트는 SNMP 통신에 사용할 MIB를 제공합니다. 서버는 이러한 변수가 포함된 트랩 또는 메시지를 전송하여 중요 이벤트를 NMS에 보고합니다. 또한 NMS는 서버 MIB에서 데이터를 쿼리하거나 MIB의 변수를 원격으로 변경할 수 있습니다. 각 Sun Java System 서버마다 자체 MIB가 있습니다. 모든 Sun Java System 서버 MIB는

`server-root/plugins/snmp`에 있습니다.

Proxy Servers MIB는 `proxyserv40.mib`라는 이름의 파일입니다. 이 MIB에는 Proxy Server용 네트워크 관리에 관련된 다양한 변수의 정의가 포함됩니다. Proxy Server MIB를 사용하여 실시간으로 Proxy Server에 대한 관리 정보를 보거나 서버를 모니터링할 수 있습니다.

SNMP 설정

SNMP를 사용하려면 마스터 에이전트 및 최소 하나의 하위 에이전트가 시스템에 설치되어 실행되고 있어야 합니다. 마스터 에이전트를 설치해야 하위 에이전트를 사용할 수 있습니다.

SNMP를 설정하는 방법은 시스템에 따라 다릅니다.

시작하기 전에 두 가지를 확인해야 합니다.

- 시스템에 SNMP 에이전트(운영 체제의 원시 에이전트)가 실행되고 있는지 여부
- 실행 중인 경우 원시 SNMP 에이전트가 SMUX 통신을 지원하는지 여부(AIX 플랫폼을 사용하는 경우 시스템이 SMUX 지원)

이 정보를 확인하는 방법은 시스템 설명서를 참조하십시오.

주 – Administration Server에서 SNMP 설정을 변경하거나, 새 서버를 설치하거나, 기존 서버를 삭제한 후에는 다음 단계를 수행해야 합니다.

- (Windows) Windows SNMP 서비스를 다시 시작하거나 시스템을 재부팅합니다.
- (UNIX) Administration Server를 사용하여 SNMP 마스터 에이전트를 다시 시작합니다.

표 10–1 SNMP 마스터 에이전트 및 하위 에이전트 사용 설정을 위한 절차 개요

시스템의 전제 조건	...수행할 작업.(다음 절에서 자세히 설명)
■ 현재 실행되는 원시 에이전트 없음	1. 마스터 에이전트를 시작합니다. 2. 서버에 설치된 각 서버용 하위 에이전트를 사용하도록 설정합니다.
■ 현재 원시 에이전트 실행 ■ SMUX 없음 ■ 원시 에이전트를 사용하여 계속할 필요 없음	1. Administration Server용 마스터 에이전트를 설치할 때 원시 에이전트를 중지합니다. 2. 마스터 에이전트를 시작합니다. 3. 서버에 설치된 각 서버용 하위 에이전트를 사용하도록 설정합니다.
■ 현재 원시 에이전트 실행 ■ SMUX 없음 ■ 원시 에이전트를 사용하여 계속	1. 프록시 SNMP 에이전트를 설치합니다. 2. 마스터 에이전트를 시작합니다. 3. 해당 프록시 SNMP 에이전트를 시작합니다. 4. 마스터 에이전트 포트 번호가 아닌 포트 번호를 사용하여 원시 에이전트를 다시 시작합니다. 5. 서버에 설치된 각 서버용 하위 에이전트를 사용하도록 설정합니다.

표 10–1 SNMP 마스터 에이전트 및 하위 에이전트 사용 설정을 위한 절차 개요 *(계속)*

시스템의 전제 조건	...수행할 작업.(다음 절에서 자세히 설명)
■ 현재 원시 에이전트 실행 ■ SMUX 지원	1. SNMP 원시 에이전트를 재구성합니다. 2. 서버에 설치된 각 서버용 하위 에이전트를 사용하도록 설정합니다.

프록시 SNMP 에이전트 사용(UNIX)

원시 에이전트를 이미 실행 중이며 Proxy Server 마스터 에이전트와 함께 계속 사용하려는 경우 프록시 SNMP 에이전트를 사용해야 합니다. 시작하기 전에 원시 마스터 에이전트가 중단되었는지 확인합니다. 자세한 내용은 시스템 설명서를 참조하십시오.

주 – 프록시 에이전트를 사용하려면 이를 설치한 다음 시작해야 합니다. 또한 Proxy Server 마스터 에이전트가 실행되고 있는 포트 번호가 아닌 다른 포트 번호를 사용하여 원시 SNMP 마스터 에이전트를 다시 시작해야 합니다.

이 절에서는 다음 항목에 대해 설명합니다.

- 204 페이지 “프록시 SNMP 에이전트 설치”
  - 205 페이지 “Proxy SNMP 에이전트 시작”
  - 205 페이지 “원시 SNMP 데몬 다시 시작”

프록시 SNMP 에이전트 설치

SNMP 에이전트가 시스템에서 실행되며 원시 SNMP 데몬을 계속 사용하려면 다음과 같이 합니다.

▼ 프록시 SNMP 에이전트를 설치하는 방법

1 **SNMP 마스터 에이전트를 설치합니다.**
206 페이지 “SNMP 마스터 에이전트 설치”를 참조하십시오.

2 **프록시 SNMP를 설치 및 시작하고 원시 SNMP 데몬을 재시작합니다.**
204 페이지 “프록시 SNMP 에이전트 사용(UNIX)”을 참조하십시오.

3 **SNMP 마스터 에이전트를 시작합니다.**
207 페이지 “SNMP 마스터 에이전트 사용 설정 및 시작”을 참조하십시오.

4 **하위 에이전트를 사용하도록 설정합니다.**
212 페이지 “하위 에이전트 사용 설정”을 참조하십시오.

SNMP 프록시 에이전트를 설치하려면 CONFIG 파일을 편집합니다. 이 파일은 서버 루트 디렉토리의 plugins/snmp/sagt에 있습니다. SNMP 데몬이 수신할 포트를 추가합니다. 이 파일에는 MIB 트리와 프록시 SNMP 에이전트가 전달할 트랩도 포함되어야 합니다.

다음은 CONFIG 파일의 예입니다.

```
AGENT AT PORT 1161 WITH COMMUNITY public
SUBTREES       1.3.6.1.2.1.1,
               3.6.1.2.1.2,
               1.3.6.1.2.1.3,
               1.3.6.1.2.1.4,
               1.3.6.1.2.1.5,
               1.3.6.1.2.1.6,
               1.3.6.1.2.1.7,
               1.3.6.1.2.1.8
FORWARD ALL TRAPS;
```

Proxy SNMP 에이전트 시작

프록시 SNMP 에이전트를 시작하려면 명령 프롬프트에서 다음을 입력합니다.

```
# sagt -c CONFIG&
```

원시 SNMP 데몬 다시 시작

프록시 SNMP 에이전트를 시작한 후 CONFIG 파일에서 지정한 포트에서 원시 SNMP 데몬을 다시 시작해야 합니다. 원시 SNMP 데몬을 다시 시작하려면 명령 프롬프트에서 다음을 입력합니다.

```
# snmpd -P port-number
```

여기서 *port-number*는 CONFIG 파일에 지정된 포트 번호입니다. 예를 들어 Solais 플랫폼에서는 앞에서 언급한 CONFIG 파일의 예에 나온 포트를 사용하는 경우 다음을 입력합니다.

```
# snmpd -P 1161
```

SNMP 원시 에이전트 재구성

SNMP 데몬이 AIX에서 실행되는 경우 SMUX가 지원됩니다. 따라서 마스터 에이전트를 설치할 필요는 없습니다. 그러나 AIX SNMP 데몬 구성을 변경해야 합니다.

AIX는 여러 구성 파일을 사용하여 통신을 검사합니다. SNMP 데몬이 SMUX 하위 에이전트에서 수신되는 메시지를 받도록 snmpd.conf 파일을 편집해야 합니다. 자세한 내용은 snmpd.conf의 온라인 설명서 페이지를 참조하십시오. 이 파일에 줄을 추가하여 각 하위 에이전트를 정의합니다.

예를 들어 다음 줄은 snmpd.conf에 추가할 수 있습니다.

```
smux 1.3.6.1.4.1.1.1450.1        IP-address net-mask
```

IP_address는 하위 에이전트가 실행되는 호스트의 IP 주소이며 net_mask는 이 호스트의 네트워크 마스크입니다.

주 – 루프백 주소 127.0.0.1을 사용하면 안 되며, 실제 IP 주소를 사용해야 합니다.

SNMP 마스터 에이전트 설치

SNMP 마스터 에이전트를 구성하려면 반드시 Administration Server 인스턴스를 root 사용자로 설치해야 합니다. 그러나 root가 아닌 사용자라도 웹 서버 인스턴스에서 SNMP 하위 에이전트가 마스터 에이전트와 함께 작동하도록 구성하여 MIB 찾아보기 등의 기본적인 SNMP 작업을 수행할 수 있습니다.

▼ 마스터 SNMP 에이전트를 설치하는 방법

1. **루트로 로그인합니다.**
2. **포트 161에서 SNMP 데몬(snmpd)이 실행되고 있는지 확인합니다.**
   - **실행되고 있는 SNMP 데몬이 없으면 206 페이지 "SNMP 마스터 에이전트 설치"로 이동합니다.**
   - **SnMP 데몬이 실행 중이면 데몬을 시작하는 방법과 지원하는 MIB을 확인합니다. 그런 다음 해당 프로세스를 종료합니다.**
3. **Administration Server에서 Global Settings 탭의 Set SNMP Master Agent Trap 링크를 누릅니다.**
4. **네트워크 관리 소프트웨어를 실행하는 시스템의 이름을 입력합니다.**
5. **네트워크 관리 시스템이 트랩을 청취할 포트 번호를 입력합니다. 주로 사용하는 포트는 162입니다.**
   트랩에 대한 자세한 내용은 211 페이지 "트랩 대상 구성"을 참조하십시오.
6. **트랩에서 사용할 커뮤니티 문자열을 입력합니다.**
   커뮤니티 문자열에 대한 자세한 내용은 211 페이지 "커뮤니티 문자열 구성"을 참조하십시오.
7. **OK를 누릅니다.**

8. **Administration Server에서 Global Settings 탭의 Set SNMP Master Agent Community 링크를 누릅니다.**
9. **마스터 에이전트용 커뮤니티 문자열을 입력합니다.**
10. **커뮤니티용 작업을 선택합니다.**
11. **New를 누릅니다.**

SNMP 마스터 에이전트 사용 설정 및 시작

마스터 에이전트의 작동은 이름이 `CONFIG`인 에이전트 구성 파일에서 정의됩니다. Server Manager를 사용하여 `CONFIG` 파일을 편집하거나 또는 파일을 직접 편집할 수 있습니다. SNMP 하위 에이전트를 사용 설정하기 전에 반드시 마스터 SNMP 에이전트를 설치해야 합니다.

마스터 에이전트를 다시 시작할 때 `System Error: Could not bind to port`와 같은 바인딩 오류 메시지가 나타나면 `ps -ef | grep snmp`를 사용하여 `magt`가 실행 중인지 확인합니다. 실행 중인 경우 명령 `kill -9 pid`를 사용하여 프로세스를 종료합니다. SNMP용 CGI가 다시 작동을 시작할 것입니다.

이 절에서는 다음 항목에 대해 설명합니다.

- 207 페이지 "다른 포트에서 마스터 에이전트 시작"
- 208 페이지 "SNMP 마스터 에이전트 직접 구성"
- 208 페이지 "마스터 에이전트 CONFIG 파일 편집"
- 208 페이지 "`sysContact` 및 `sysLocation` 변수 정의"
- 209 페이지 "SNMP 하위 에이전트 구성"
- 210 페이지 "SNMP 마스터 에이전트 시작"

다른 포트에서 마스터 에이전트 시작

Administration Interface는 161이 아닌 다른 포트에서 SNMP 에이전트를 시작하지 않을 것입니다.

▼ 다른 포트에서 마스터 에이전트를 수동으로 시작하는 방법

1. **/*server-root*/plugins/snmp/magt/CONFIG 파일에 원하는 포트를 지정합니다.**
2. **다음과 같은 시작 스크립트를 실행합니다.**

```
cd / server-root/proxy-admserv

./start -shell /server-root/plugins/snmp/magt/magt
```

/server-root /plugins/snmp/magt/CONFIG

/ server-root/plugins/snmp/magt/INIT

마스터 에이전트가 원하는 포트에서 시작될 것입니다. 사용자 인터페이스는 마스터 에이전트가 실행 중인지 감지할 수 있습니다.

SNMP 마스터 에이전트 직접 구성

▼ 마스터 SNMP 에이전트를 수동으로 구성하는 방법

1 **수퍼유저로 로그인합니다.**

2 **포트 161에서 SNMP 데몬(snmpd)이 실행되고 있는지 확인합니다.**
SnMP 데몬이 실행 중이면 데몬을 시작하는 방법과 지원하는 MIB을 확인합니다. 해당 프로세스를 종료합니다.

3 **서버 루트 디렉토리의 plugins/snmp/magt 에 있는 CONFIG 파일을 편집합니다.**

4 **(선택 사항) CONFIG 파일에서 sysContact 및 sysLocation 변수를 정의합니다.**

마스터 에이전트 CONFIG 파일 편집

▼ 마스터 SNMP 에이전트를 수동으로 구성하는 방법

1 **수퍼유저로 로그인합니다.**

2 **포트 161에서 SNMP 데몬(snmpd)이 실행되고 있는지 확인합니다.**
SnMP 데몬이 실행 중이면 데몬을 시작하는 방법과 지원하는 MIB을 확인합니다. 해당 프로세스를 종료합니다.

3 **서버 루트 디렉토리의 plugins/snmp/magt 에 있는 CONFIG 파일을 편집합니다.**

4 **(선택 사항) CONFIG 파일에서 sysContact 및 sysLocation 변수를 정의합니다.**

sysContact 및 sysLocation 변수 정의

CONFIG 파일의 sysContact 및 sysLocation 항목은 sysContact 및 sysLocation MIB-II 변수를 지정합니다. 이 예에서 sysContact 및 sysLocation 문자열은 큰따옴표 안에 넣습니다. 공백, 줄바꿈, 탭 등을 포함하는 문자열은 인용 부호 안에 넣어야 합니다. 또한 16진수 표기법으로 값을 지정할 수 있습니다.

다음 예는 sysContract 및 sysLocation 변수가 정의된 CONFIG 파일을 보여 줍니다.

```
COMMUNITY public

ALLOW ALL OPERATIONS

MANAGER nms2

SEND ALL TRAPS TO PORT 162

WITH COMMUNITY public

INITIAL sysLocation "Server room

987 East Cannon RoadMountain View, CA 94043 USA" INITIAL sysContact "Jill Dawson
email: jdawson@example.com"
```

SNMP 하위 에이전트 구성

SNMP 하위 에이전트를 구성하여 서버를 모니터링할 수 있습니다.

▼ SNMP 하위 에이전트를 구성하는 방법

1. **Server Manager에 액세스하여 Server Status 탭을 누릅니다.**
2. **Configure SNMP Subagent 링크를 누릅니다.**
   Configure SNMP Subagent 페이지가 표시됩니다.
3. **마스터 호스트 필드에 서버의 이름과 도메인을 입력합니다.**
4. **운영 체제 정보를 포함하여 서버에 대한 설명을 입력합니다.**
5. **서버를 담당하는 조직을 입력합니다.**
6. **위치 필드에 서버의 절대 경로를 입력합니다.**
7. **연락처 필드에 서버를 담당하는 담당자의 이름과 연락처 정보를 입력합니다.**
8. **Enable the SNMP Statistics Collection에 On을 선택합니다.**
9. **OK를 누릅니다.**
10. **Restart Required를 누릅니다.**
    Apply Changes 페이지가 나타납니다.

11 Restart Proxy Server 버튼을 눌러 변경 사항을 적용합니다.

SNMP 마스터 에이전트 시작

SNMP 마스터 에이전트를 설치하면 에이전트를 직접 시작하거나 Administration Server를 이용하여 시작할 수 있습니다.

SNMP 마스터 에이전트를 수동으로 시작하는 방법

마스터 에이전트를 수동으로 시작하려면 명령 프롬프트에서 다음 명령을 입력합니다.

```
# magt CONFIG INIT&
```

INIT 파일은 MIB-II 시스템 그룹의 정보를 포함하는 비휘발성 파일로, 여기에는 시스템 위치와 연락처 정보가 포함되어 있습니다. INIT가 존재하지 않는 경우 마스터 에이전트를 처음 시작할 때 만들어집니다. CONFIG 파일에 잘못된 관리자 이름이 있는 경우 마스터 에이전트 시작 프로세스가 실패합니다.

비표준 포트에서 마스터 에이전트를 시작하려면 다음 두 가지 방법 중 하나를 사용합니다.

방법 1: CONFIG 파일에서 마스터 에이전트가 관리자의 SNMP 요청을 수신할 각 인터페이스에 대한 전송 매핑을 지정합니다. 전송 매핑을 사용하면 마스터 에이전트가 표준 포트뿐 아니라 비표준 포트의 연결을 수락합니다. 마스터 에이전트는 또한 비표준 포트의 SNMP 트래픽을 수락합니다. 대상 시스템의 한계에 따라 정해진 동시 SNMP의 최대 수에 따라 각 프로세스에 대한 개방 소켓 또는 파일 설명자의 수가 제한됩니다. 다음은 전송 매핑 항목의 예입니다.

```
TRANSPORT extraordinary SNMP

OVER UDP SOCKET

AT PORT 11161
```

CONFIG 파일을 직접 편집한 후 명령 프롬프트에서 다음 명령을 입력하여 마스터 에이전트를 직접 시작해야 합니다.

```
# magt CONFIG INIT&
```

방법 2: 마스터 에이전트가 비표준 포트와 표준 포트에서 연결을 수용하도록 /etc/services 파일을 편집합니다.

▼ Administration Server를 사용하여 SNMP 마스터 에이전트를 시작하는 방법

1 Administration Server에 로그인합니다.

2. **Administration Server에서 Global Settings 탭의 Control SNMP Master Agent 링크를 누릅니다.**

3. **Start를 누릅니다.**

   또한 Control SNMP Master Agent 페이지에서 SNMP 마스터 에이전트를 중지하고 다시 시작할 수 있습니다.

SNMP 마스터 에이전트 구성

마스터 에이전트를 사용 설정하고 호스트 컴퓨터의 하위 에이전트를 사용 설정했으면 호스트의 Administration Server를 구성해야 합니다. 이 구성에서는 커뮤니티 문자열 및 트랩 대상을 지정합니다.

커뮤니티 문자열 구성

커뮤니티 문자열은 SNMP 에이전트가 인증에 사용하는 텍스트 문자열입니다. 네트워크 관리 스테이션은 에이전트에 보내는 각 메시지에 커뮤니티 문자열을 함께 보냅니다. 그런 후 에이전트는 네트워크 관리 스테이션이 정보에 대해 인증되었는지 확인합니다. 커뮤니티 문자열은 SNMP 패킷에서 전송될 때 숨겨져 있지 않습니다. 문자열은 ASCII 텍스트로 전송됩니다.

Administration Server의 Set SNMP Master Agent Community 페이지에서 SNMP 마스터 에이전트의 커뮤니티 문자열을 구성할 수 있습니다. 또한 특정 커뮤니티가 수행할 수 있는 SNMP 관련 작업을 정의합니다. 또한 Administration Server에서 이미 구성한 커뮤니티를 확인, 편집 및 제거할 수 있습니다.

트랩 대상 구성

SNMP 트랩은 SNMP 에이전트가 네트워크 관리 스테이션으로 보내는 메시지입니다. 예를 들어 SNMP 에이전트는 인터페이스의 상태가 작동에서 중지로 변경될 때 트랩을 보냅니다. SNMP 에이전트는 반드시 네트워크 관리 스테이션의 주소를 알고 있어야 트랩을 보낼 위치를 알 수 있습니다. Proxy Server에서 SNMP 마스터 에이전트용 트랩 대상을 구성할 수 있습니다. 또한 이미 구성한 트랩 대상을 확인, 편집 및 제거할 수 있습니다. Proxy Server를 사용하여 트랩 대상을 구성할 때 실제로는 `CONFIG` 파일을 편집하는 것입니다.

하위 에이전트 사용 설정

Administration Server와 함께 제공되는 마스터 에이전트를 설치한 후에는 반드시 에이전트를 시작하기 전에 서버 인스턴스용 하위 에이전트를 사용하도록 설정해야 합니다. 자세한 내용은 206 페이지 "SNMP 마스터 에이전트 설치"를 참조하십시오. Server Manager를 사용하여 하위 에이전트를 사용하도록 설정할 수 있습니다.

UNIX 또는 Linux 플랫폼에서 SNMP 기능을 중지하려면 먼저 하위 에이전트를 중지한 다음 마스터 에이전트를 중지합니다. 마스터 에이전트를 먼저 중지하는 경우 하위 에이전트를 중지할 수 없게 됩니다. 이러한 경우 마스터 에이전트를 다시 시작하고 하위 에이전트를 정지한 후, 마스터 에이전트를 정지시킵니다.

SNMP 하위 에이전트를 사용 설정하려면 Server Manager에서 Configure SNMP Subagent 페이지를 사용하여 Control SNMP Subagent 페이지에서 하위 에이전트를 시작합니다. 자세한 내용은 온라인에서 도움말의 해당 부분을 참조하십시오.

하위 에이전트를 사용 설정한 후에는 *Control SNMP Subagent* **페이지**나 Windows의 서비스 제어판에서 하위 에이전트를 중지 또는 다시 시작할 수 있습니다.

주 – SNMP 구성을 변경한 후에는 Apply Required를 눌러 SNMP 하위 에이전트를 다시 시작해야 합니다.

SNMP 메시지 이해

GET 및 SET은 SNMP에 의해 정의되는 두 가지 메시지 유형입니다. GET과 SET 메시지는 NMS(Network Management Station)가 마스터 에이전트로 보내는 메시지입니다. Administration Server에서 이러한 메시지를 사용할 수 있습니다.

SNMP는 네트워크 정보를 프로토콜 데이터 단위(PDU)의 형식으로 교환합니다. 이 단위에는 웹 서버 등의 관리된 장치에 저장된 변수에 대한 정보가 들어 있습니다. 관리된 객체라고도 하는 이러한 변수에는 필요한 경우 NMS로 보고되는 값과 제목이 포함되어 있습니다. 서버가 NMS로 보내는 프로토콜 데이터 단위를 트랩이라고 합니다. 다음 예는 NMS 또는 서버에서 시작된 통신의 GET, SET 및 트랩 메시지의 용도를 보여 줍니다.

NMS에서 시작된 통신NMS는 서버에 정보를 요청하거나 서버의 MIB에 저장된 변수의 값을 변경합니다. 예:

1. NMS는 Administration Server 마스터 에이전트에 메시지를 보냅니다. 메시지는 데이터에 대한 요청(GET 메시지)일 수 있으며 MIB의 변수를 설정하는 지시문(SET 메시지)일 수 있습니다.
2. 마스터 에이전트는 메시지를 적절한 하위 에이전트로 전달합니다.
3. 하위 에이전트는 데이터를 수신하거나 MIB의 변수를 변경합니다.
4. 하위 에이전트는 데이터 또는 상태를 마스터 에이전트에 보고하고 마스터 에이전트는 GET 메시지를 다시 NMS로 전달합니다.

5. NMS는 네트워크 관리 응용 프로그램을 통하여 데이터를 텍스트 또는 그래픽으로 표시합니다.

   서버에서 시작된 통신중요한 이벤트가 발생하면 서버 하위 에이전트는 메시지 또는 트랩을 NMS로 보냅니다. 예:

6. 하위 에이전트는 마스터 에이전트에게 서버가 정지되었음을 알립니다.
7. 마스터 에이전트는 메시지 또는 트랩을 보내 NMS에 해당 이벤트를 보고합니다.
8. NMS는 네트워크 관리 응용 프로그램을 통하여 정보를 텍스트 또는 그래픽으로 표시합니다.

◆ ◆ ◆ 11 장

11 URL 프록싱 및 라우팅

이 장에서는 프록시 서버가 요청을 처리하는 방법에 대해 설명합니다. 또한 특정 자원에 대해 프록싱을 활성화하는 방법과URL을 다른 URL이나 서버로 라우팅하도록 프록시 서버를 구성하는 방법에 대해서도 설명합니다.

이 장은 다음 내용으로 구성되어 있습니다.

- 215 페이지 “자원에 대한 프록싱 활성화/비활성화”
- 216 페이지 “다른 프록시를 통한 라우팅”
- 219 페이지 “클라이언트 IP 주소를 서버로 전달”
- 223 페이지 “클라이언트의 IP 주소 확인 허용”
- 224 페이지 “클라이언트 자동 구성”
- 224 페이지 “네트워크 연결 모드 설정”
- 225 페이지 “기본 FTP 전송 모드 변경”
- 226 페이지 “SOCKS 이름 서버 IP 주소 지정”
- 227 페이지 “HTTP 요청 로드 균형 조정 구성”
- 228 페이지 “URL 및 URL 매핑 관리”

자원에 대한 프록싱 활성화/비활성화

자원에 대해 프록싱을 켜거나 끌 수 있습니다. 자원은 개별 URL, 공통 사항이 있는 URL 그룹 또는 전체 프로토콜일 수 있습니다. 전체 서버, 다양한 자원 또는 템플리트 파일에 지정된 자원에 대해 프록싱을 사용할 것인지 여부를 제어할 수 있습니다. 해당 자원에 대한 프록싱 사용을 중지하여 하나 이상의 URL에 대한 액세스를 거부할 수 있습니다. 이 설정은 자원에 대한 모든 액세스를 거부하거나 허용할 수 있는 전역적인 방법입니다. 또한 URL 필터를 사용하여 자원에 대한 액세스를 허용하거나 거부할 수도 있습니다. URL 필터에 대한 자세한 내용은 284 페이지 “URL 필터링”을 참조하십시오.

▼ 자원에 대해 프록싱을 활성화하는 방법

1. **Server Manager에 액세스하고 Routing 탭을 누릅니다.**
2. **Enable/Disable Proxying 링크를 누릅니다.**
   Enable/Disable Proxying 페이지가 표시됩니다.
3. **드롭다운 목록에서 자원을 선택하거나 Regular Expression 버튼을 눌러 정규 표현식을 입력하고 OK를 누릅니다.**
4. **지정한 자원에 대해 기본 설정을 선택할 수 있습니다.**
   - **Use Default Setting Derived From A More General Resource.** 이 항목이 포함된 더 일반적인 자원의 설정이 이 자원에 사용됩니다.
   - **Do Not Proxy This Resource.** 프록시를 통해 이 자원에 액세스할 수 없습니다.
   - **Enable Proxying Of This Resource.** 프록시에서 클라이언트가 이 자원에 액세스하도록 허용합니다(다른 보안 및 인증 검사를 통과한 경우). 자원에 대해 프록싱을 활성화하면 모든 메소드가 활성화됩니다. GET, HEAD, INDEX, POST 및 SSL 터널링을 위한 CONNECT를 포함한 읽기 메소드와 PUT, MKDIR, RMDIR, MOVE 및 DELETE를 포함한 쓰기 메소드가 해당 자원에 대해 모두 활성화됩니다. 다른 보안 검사가 없다면 클라이언트는 모두 읽기 및 쓰기 액세스 권한을 갖게 됩니다.
5. **OK를 누릅니다.**
6. **Restart Required를 누릅니다.**
   Apply Changes 페이지가 표시됩니다.
7. **Restart Proxy Server 버튼을 눌러 변경 사항을 적용합니다.**

다른 프록시를 통한 라우팅

Set Routing Preferences 페이지는 파생된 기본 구성이나 직접 연결을 사용하거나 프록시 배열, ICP 환경, 다른 프록시 서버 또는 SOCKS 서버를 사용하여 특정 자원을 라우팅하도록 프록시 서버를 구성하는 데 사용됩니다.

자원에 대한 라우팅 구성

▼ 자원에 대한 라우팅 구성 방법

1 **Server Manager에 액세스하고 Routing 탭을 누릅니다.**

2 **Set Routing Preferences 링크를 누릅니다.**
Set Routing Preferences 페이지가 표시됩니다.

3 **드롭다운 목록에서 자원을 선택하거나 Regular Expression 버튼을 누르고 정규 표현식을 입력한 다음 OK를 누릅니다.**

4 **구성하는 자원에 대해 원하는 라우팅 유형을 선택합니다.**
사용 가능한 옵션은 다음과 같습니다.

- **Derived Default Configuration.** 프록시 서버는 더 일반적인 템플리트, 즉 더 짧고 정규 표현식과 일치하는 템플리트를 사용하여 원격 서버나 다른 프록시를 사용해야 하는지 여부를 결정합니다. 예를 들어, 프록시가 모든 `http://.*` 요청을 다른 프록시 서버로 라우팅하고 모든 `http://www.*` 요청을 원격 서버로 라우팅하는 경우, `http://www.example.*` 요청에 대해 파생된 기본 구성 라우팅을 만들 수 있습니다. 이렇게 하면 `http://www.*` 템플리트에 대한 설정이 적용되어 원격 서버로 직접 라우팅됩니다.
- **Direct Connections.** 요청이 프록시를 통하지 않고 항상 원격 서버로 직접 이동합니다.
- **Route Through A SOCKS Server.** 지정된 자원에 대한 요청이 SOCKS 서버를 통해 라우팅됩니다. 이 옵션을 선택한 경우 프록시 서버가 라우팅할 SOCK 서버의 이름이나 IP 주소 및 포트 번호를 지정합니다.
- **Route Through.** 프록시 배열, ICP 환경, 상위 배열 또는 프록시 서버를 통해 라우팅할지 여부를 지정할 수 있습니다. 여러 개의 라우팅 방법을 선택하는 경우 프록시는 양식에 표시된 계층 구조(프록시 배열, 리디렉션, ICP, 상위 배열 또는 다른 프록시)를 따릅니다. 프록시 서버를 통한 라우팅에 대한 자세한 내용은 218 페이지 “프록시 서버 체인”을 참조하십시오.

  SOCKS 서버를 통한 라우팅에 대한 자세한 내용은 218 페이지 “SOCKS 서버를 통해 라우팅”을 참조하십시오. 프록시 배열, 상위 배열 또는 ICP 환경을 통한 라우팅에 대한 자세한 내용은 12 장, “캐시”을 참조하십시오.

주 – 443 이외의 포트에서 연결 요청의 라우팅을 활성화하려면 `obj.conf` 파일에서 `ppath` 매개 변수를 `connect://.*`로 변경합니다.

---

5 **OK를 누릅니다.**

6 **Restart Required를 누릅니다.**
Apply Changes 페이지가 표시됩니다.

7 **Restart Proxy Server 버튼을 눌러 변경 사항을 적용합니다.**

프록시 서버 체인

일부 자원에 대해 프록시가 원격 서버에 액세스하지 않고 다른 프록시에 액세스하도록 설정할 수 있습니다. 체인은 방화벽 뒤에 여러 프록시를 구성하는 좋은 방법입니다. 또한 체인을 통해 계층적 캐시를 만들 수도 있습니다.

▼ 다른 Proxy Server를 통해 라우팅하는 방법

1 **Server Manager에 액세스하고 Routing 탭을 누릅니다.**

2 **Set Routing Preferences 링크를 누릅니다.**
Set Routing Preferences 페이지가 표시됩니다.

3 **드롭다운 목록에서 자원을 선택하거나 Regular Expression 버튼을 눌러 정규 표현식을 입력하고 OK를 누릅니다.**

4 **페이지의 Routing Through Another Proxy 섹션에서 Route Through 옵션을 선택합니다.**

5 **Another Proxy 확인란을 선택합니다.**

6 **Another Proxy 필드에 라우팅할 프록시 서버의 서버 이름과 포트 번호를 입력할 수 있습니다.**
서버 이름:포트의 형식으로 서버 이름과 포트 번호를 입력합니다.

7 **OK를 누릅니다.**

8 **Restart Required를 누릅니다.**
Apply Changes 페이지가 표시됩니다.

9 **Restart Proxy Server 버튼을 눌러 변경 사항을 적용합니다.**

SOCKS 서버를 통해 라우팅

네트워크에서 이미 원격 SOCKS 서버를 실행 중인 경우 특정 자원에 대해 SOCKS 서버로 연결하도록 프록시를 구성할 수 있습니다.

▼ SOCKS 서버를 통해 라우팅하는 방법

1 **Server Manager에 액세스하고 Routing 탭을 누릅니다.**

2 **Set Routing Preferences 링크를 누릅니다.**
Set Routing Preferences 페이지가 표시됩니다.

3 **드롭다운 목록에서 자원을 선택하거나 Regular Expression 버튼을 눌러 정규 표현식을 입력하고 OK를 누릅니다.**

4 **페이지의 Routing Through Another Proxy 섹션에서 Route Through 옵션을 선택합니다.**

5 **Route Through SOCKS Server 옵션을 선택합니다.**

6 **프록시 서버가 라우팅할 SOCK 서버의 이름이나 IP 주소 및 포트 번호를 지정합니다.**

7 **OK를 누릅니다.**

8 **Restart Required를 누릅니다.**
Apply Changes 페이지가 표시됩니다.

9 **Restart Proxy Server 버튼을 눌러 변경 사항을 적용합니다.**

다음 단계

SOCKS 서버를 통한 라우팅을 활성화한 후 SOCKS v5 Routing 페이지를 사용하여 프록시 라우팅을 만들어야 합니다. 프록시 라우팅은 프록시가 라우팅하는 SOCKS 서브를 통해 액세스할 수 있는 IP 주소를 식별합니다. 또한 프록시 라우팅은 SOCKS 서버가 호스트에 직접 연결할 것인지 여부를 지정합니다.

클라이언트 IP 주소를 서버로 전달

Forward Client Credentials 페이지는 클라이언트 자격 증명을 원격 서버로 전송하도록 프록시를 구성하는 데 사용됩니다.

▼ 클라이언트 IP 주소를 전송하도록 프록시를 구성하는 방법

1 **Server Manager에 액세스하고 Routing 탭을 누릅니다.**

2 **Forward Client Credentials 링크를 누릅니다.**
Forward Client Credentials 페이지가 표시됩니다.

3 **드롭다운 목록에서 자원을 선택하거나 Regular Expression 버튼을 눌러 정규 표현식을 입력하고 OK를 누릅니다.**

4 **전달 옵션을 설정합니다.**

- **Client IP Addressing Forwarding.** 문서에 대한 요청 시 Proxy Server는 클라이언트의 IP 주소를 원격 서버로 전송하지 않습니다. 대신 프록시가 클라이언트의 역할을 하여 자신의 IP 주소를 원격 서버로 전송합니다. 그러나 다음과 같은 경우 클라이언트의 IP 주소를 전달할 수 있습니다.
  - 프록시가 내부 프록시 체인에 있는 경우
  - 클라이언트가 액세스해야 하는 서버에서 클라이언트의 IP 주소를 알아야 하는 경우 템플리트를 사용하여 특정 서버에만 클라이언트의 IP 주소를 전송할 수 있습니다.

  클라이언트의 IP 주소를 전송하도록 프록시를 구성하는 옵션을 설정합니다.
  - **Default.** Proxy Server가 클라이언트의 IP 주소를 전달할 수 있습니다.
  - **Blocked.** 프록시가 클라이언트의 IP 주소를 전달할 수 없습니다.
  - **Enabled Using HTTP Header.** IP 주소를 전달할 때 사용할 프록시의 HTTP 헤더를 지정할 수 있습니다. 기본 HTTP 헤더의 이름은 `Client-ip`이지만 어떤 헤더를 선택해도 IP 주소를 전송할 수 있습니다.
- **Client Proxy Authentication Forwarding.** 클라이언트의 인증 세부 정보를 전송하도록 프록시를 구성하는 옵션을 설정합니다.
  - **Default.** Proxy Server가 클라이언트의 인증 세부 정보를 전달할 수 있습니다.
  - **Blocked.** 프록시가 클라이언트의 인증 세부 정보를 전달할 수 없습니다.
  - **Enabled Using HTTP Header.** 인증 세부 정보를 전달할 때 사용할 프록시의 HTTP 헤더를 지정할 수 있습니다.
- **Client Cipher Forwarding.** 클라이언트의 SSL/TLS 암호화 제품군 이름을 원격 서버로 전송하도록 프록시를 구성하는 옵션을 설정합니다.
  - **Default.** Proxy Server가 클라이언트의 SSL/TLS 암호화 제품군 이름을 원격 서버로 전달할 수 있습니다.
  - **Blocked.** 프록시가 클라이언트의 SSL/TLS 암호화 제품군 이름을 원격 서버로 전달할 수 없습니다.

  - **Enabled Using HTTP Header.** 클라이언트의 SSL/TLS 암호화 제품군 이름을 원격 서버로 전달할 때 사용할 프록시의 HTTP 헤더를 지정할 수 있습니다. 기본 HTTP 헤더의 이름은 `Proxy-cipher`이지만 어떤 헤더를 선택해도 클라이언트의 SSL/TLS 암호화 제품군 이름을 전송할 수 있습니다.
- **Client Keysize Forwarding.** 클라이언트의 SSL/TLS 키 크기를 원격 서버로 전송하도록 프록시를 구성하는 옵션을 설정합니다.
  - **Default.** Proxy Server가 클라이언트의 SSL/TLS 키 크기를 원격 서버로 전달할 수 있습니다.
  - **Blocked.** 프록시가 클라이언트의 SSL/TLS 키 크기를 원격 서버로 전달할 수 없습니다.
  - **Enabled Using HTTP Header.** 클라이언트의 SSL/TLS 키 크기를 원격 서버로 전달할 때 사용할 프록시의 HTTP 헤더를 지정할 수 있습니다. 기본 HTTP 헤더의 이름은 `Proxy-keysize`이지만 어떤 헤더를 선택해도 클라이언트의 SSL/TLS 키 크기를 전송할 수 있습니다.
- **Client Secret Keysize Forwarding.** 클라이언트의 SSL/TLS 비밀 키 크기를 원격 서버로 전송하도록 프록시를 구성하는 옵션을 설정합니다.
  - **Default.** Proxy Server가 클라이언트의 SSL/TLS 비밀 키 크기를 원격 서버로 전달할 수 있습니다.
  - **Blocked.** 프록시가 클라이언트의 SSL/TLS 비밀 키 크기를 원격 서버로 전달할 수 없습니다.
  - **Enabled Using HTTP Header.** SSL/TLS 비밀 키 크기를 원격 서버로 전달할 때 사용할 프록시의 HTTP 헤더를 지정할 수 있습니다. 기본 HTTP 헤더의 이름은 `Proxy-secret-keysize`이지만 어떤 헤더를 선택해도 클라이언트의 SSL/TLS 비밀 키 크기를 전송할 수 있습니다.
- **Client SSL Session ID Forwarding.** 클라이언트의 SSL/TLS 세션 ID를 원격 서버로 전송하도록 프록시를 구성하는 옵션을 설정합니다.
  - **Default.** Proxy Server가 클라이언트의 SSL/TLS 세션 ID를 원격 서버로 전달할 수 있습니다.
  - **Blocked.** 프록시가 클라이언트의 SSL/TLS 세션 ID를 원격 서버로 전달할 수 없습니다.
  - **Enabled Using HTTP Header.** 클라이언트의 SSL/TLS 세션 ID를 원격 서버로 전달할 때 사용할 프록시의 HTTP 헤더를 지정할 수 있습니다. 기본 HTTP 헤더의 이름은 `Proxy-ssl-id`이지만 어떤 헤더를 선택해도 클라이언트의 SSL/TLS 세션 아이디를 전송할 수 있습니다.
- **Client Issuer DN Forwarding.** 클라이언트의 SSL/TLS 인증서에 대한 발급자의 고유 이름을 원격 서버에 전송하도록 프록시를 구성하는 옵션을 설정합니다.
  - **Default.** Proxy Server가 클라이언트의 SSL/TLS 인증서에 대한 발급자의 고유 이름을 원격 서버로 전달할 수 있습니다.
  - **Blocked.** 프록시가 클라이언트의 SSL/TLS 인증서에 대한 발급자의 고유 이름을 원격 서버로 전달할 수 없습니다.

  - **Enabled Using HTTP Header.** 클라이언트의 SSL/TLS 인증서에 대한 발급자의 고유 이름을 원격 서버로 전달할 때 사용할 프록시의 HTTP 헤더를 지정할 수 있습니다. 기본 HTTP 헤더의 이름은 `Proxy-issuer-dn`이지만 어떤 헤더를 선택해도 클라이언트의 SSL/TLS 인증서에 대한 발급자의 이름을 전송할 수 있습니다.
- **Client User DN Forwarding.** 클라이언트의 SSL/TLS 인증서에 대한 주제의 고유 이름을 원격 서버에 전송하도록 프록시를 구성하는 옵션을 설정합니다.
  - **Default.** Proxy Server가 클라이언트의 SSL/TLS 인증서에 대한 주제의 고유 이름을 원격 서버로 전달할 수 있습니다.
  - **Blocked.** 프록시가 클라이언트의 SSL/TLS 인증서에 대한 주제의 고유 이름을 원격 서버로 전달할 수 없습니다.
  - **Enabled Using HTTP Header.** 클라이언트의 SSL/TLS 인증서에 대한 주제의 고유 이름을 원격 서버로 전달할 때 사용할 프록시의 HTTP 헤더를 지정할 수 있습니다. 기본 HTTP 헤더의 이름은 `Proxy-user-dn`이지만 어떤 헤더를 선택해도 클라이언트의 SSL/TLS 인증서에 대한 주제의 이름을 전송할 수 있습니다.
- **Client SSL/TLS Certificate Forwarding.** 클라이언트의 SSL/TLS 인증서를 원격 서버로 전송하도록 프록시를 구성하는 옵션을 설정합니다.
  - **Default.** Proxy Server가 클라이언트의 SSL/TLS 인증서를 원격 서버로 전달할 수 있습니다.
  - **Blocked.** 프록시가 클라이언트의 SSL/TLS 인증서를 원격 서버로 전달할 수 없습니다.
  - **Enabled Using HTTP Header.** 클라이언트의 SSL/TLS 인증서를 원격 서버로 전달할 때 사용할 프록시의 HTTP 헤더를 지정할 수 있습니다. 기본 HTTP 헤더의 이름은 `Proxy-auth-cert`이지만 어떤 헤더를 선택해도 클라이언트의 SSL/TLS 인증서를 전송할 수 있습니다.
- **Client Cache Information Forwarding.** 다음 옵션 중 하나를 선택하여 로컬 캐시 적중 횟수에 대한 정보를 원격 서버로 전송하도록 프록시를 구성합니다.
  - **Default.** Proxy Server가 로컬 캐시 적중 횟수에 대한 정보를 원격 서버로 전송할 수 있습니다.
  - **Blocked.** 프록시가 로컬 캐시 적중 횟수에 대한 정보를 원격 서버로 전송할 수 없습니다.
  - **Enabled Using HTTP Header.** 로컬 캐시 적중 횟수에 대한 정보를 원격 서버로 전달할 때 사용할 프록시의 HTTP 헤더를 지정할 수 있습니다. 기본 HTTP 헤더의 이름은 `Cache-info`이지만 어떤 헤더를 선택해도 로컬 캐시 적중 횟수에 대한 정보를 전송할 수 있습니다.
- **Set Basic Authentication Credentials.** HTTP 요청을 전송하도록 프록시를 구성하는 옵션을 설정합니다.
  - **User.** 인증할 사용자를 지정합니다.
  - **Password.** 사용자의 비밀번호를 지정합니다.

- **Using HTTP Header.** 프록시가 자격 증명을 통신할 때 사용할 HTTP 헤더를 지정할 수 있습니다.

5 **OK를 누릅니다.**

6 **Restart Required를 누릅니다. Apply Changes 페이지가 표시됩니다.**

7 **Restart Proxy Server 버튼을 눌러 변경 사항을 적용합니다.**

클라이언트의 IP 주소 확인 허용

네트워크 보안을 유지하기 위해 클라이언트에 특정 IP 주소에 대한 액세스만 제한하는 기능이 있을 수 있습니다. 클라이언트가 이 기능을 사용할 수 있도록 Proxy Server에서 Java IP 주소 확인을 지원합니다.

Java IP 주소를 확인하면 클라이언트가 자원을 다시 라우팅하는 데 사용할 IP 주소를 확인하기 위해 Proxy Server를 쿼리할 수 있습니다. Java 애플릿에서는 DNS 스푸핑이 자주 발생하므로 이 기능을 사용하면 클라이언트가 원본 서버의 올바른 IP 주소를 확인할 수 있습니다.

이 기능을 사용할 경우 Proxy Server는 대상 원본 서버에 연결하는 데 사용된 IP 주소가 있는 헤더를 첨부합니다. 예를 들어 이 기능을 사용하는 경우 해당 요청에 "Pragma: dest-ip" 헤더가 포함되어 있으면 Proxy Server에 원본 서버의 IP 주소가 "Dest-ip:" 헤더 값으로 포함됩니다.

Java IP 주소 확인에 사용되는 SAF(Server Application Function)에 대한 자세한 내용은 **Sun Java System Web Proxy Server 4.0.8 Configuration File Reference**의 "ObjectType" 섹션에서 `java-ip-check`를 참조하십시오.

▼ Java IP 주소 확인 방법

1 **Server Manager에 액세스하고 Routing 탭을 누릅니다.**

2 **Check Java IP Address 링크를 누릅니다.**
Check Java IP Address 페이지가 표시됩니다.

3 **드롭다운 목록에서 자원을 선택하거나 Regular Expression 버튼을 눌러 정규 표현식을 입력하고 OK를 누릅니다.**

4 **Java IP 주소 확인의 기본 구성을 활성화하거나, 비활성화하거나 사용합니다.**

주 – 기본 옵션은 더 일반적인 템플리트에서 파생된 기본 구성을 사용합니다. 일반 템플리트에는 Java IP 주소 확인의 활성화 여부를 결정하기 위한 더 짧은 정규 표현식이 있습니다.

5 **OK를 누릅니다.**

6 **Restart Required를 누릅니다.**
Apply Changes 페이지가 표시됩니다.

7 **Restart Proxy Server 버튼을 눌러 변경 사항을 적용합니다.**

클라이언트 자동 구성

프록시 서버가 여러 클라이언트를 지원하는 경우 클라이언트 자동 구성 파일을 사용하여 모든 브라우저 클라이언트를 구성할 수 있습니다. 자동 구성 파일에는 브라우저가 다양한 URL에 액세스하는 데 사용할 프록시(있을 경우)를 결정하는 JavaScript™ 함수가 포함되어 있습니다. 이 기능에 대한 자세한 내용은 17 장, “클라이언트 자동 구성 파일 사용”을 참조하십시오.

네트워크 연결 모드 설정

네트워크에서 프록시 서버 컴퓨터를 연결하거나 연결 해제할 수 있습니다. 이 기능을 사용하여 데모용으로 사용할 수 있는 휴대용 컴퓨터에 프록시를 쉽게 설치할 수 있습니다.

프록시가 네트워크에서 연결 해제되면 문서가 캐시에서 직접 반환됩니다. 프록시가 최신 상태 검사를 수행할 수 없기 때문에 문서가 매우 신속하게 검색됩니다. 그러나 문서가 최신이 아닐 수 있습니다. 캐시에 대한 자세한 내용은 12 장, “캐시”를 참조하십시오.

네트워크에 연결되지 않은 경우, 프록시 서버가 네트워크 연결이 없음을 인식하고 원격 서버로의 연결을 시도하지 않기 때문에 연결이 중지되지 않습니다. 네트워크가 중단된 상태에서 프록시 서버 컴퓨터를 실행하는 경우 이 네트워크 없음 설정을 사용할 수 있습니다. 네트워크에 연결되지 않은 프록시를 실행하면 캐시에 있는 오래된 데이터에 액세스하게 됩니다. 또한 네트워크 없이 실행하는 경우에는 프록시 보안 기능이 불필요합니다.

Proxy Server는 4개의 네트워크 연결 모드를 제공합니다.

- Default 모드는 일치하는 가장 일반적인 객체의 구성에서 파생됩니다.
- Normal 모드는 프록시의 정상 작동 모드입니다. 프록시는 문서가 캐시에 없는 경우 컨텐트 서버에서 검색합니다. 문서가 캐시에 있으면 컨텐트 서버와 확인하여 최신 상태인지 확인합니다. 캐시된 파일이 변경된 경우에는 최신 사본으로 대체됩니다.

- Fast-demo 모드는 네트워크를 사용할 수 있는 경우 데모를 원활하게 제공할 수 있습니다. 문서가 캐시에 있으면 컨텐트 서버에 연결하지 않으며 문서 변경 여부도 확인하지 않습니다. 이 모드에는 컨텐트 서버의 응답을 기다리는 데 소요되는 대기 시간이 없습니다. 문서가 캐시에 없으면 컨텐트 서버에서 검색하여 캐시합니다. fast-demo 모드는 일반 모드보다 대기 시간이 짧지만 서버에 문서의 사본이 있으면 문서에 대한 최신 상태 검사를 수행하지 않기 때문에 오래된 데이터를 반환할 수도 있습니다.
- No-network 모드는 휴대용 컴퓨터에서 네트워크에 연결되지 않는 동안 사용할 수 있도록 설계되었습니다. 프록시는 문서가 캐시에 있으면 해당 문서를 반환하고 그렇지 않으면 오류를 반환합니다. 프록시는 컨텐트 서버에 연결하려고 시도하지 않으며 따라서 존재하지 않는 연결을 찾는 동안 대기하는 시간이 발생하지 않습니다.

▼ Proxy Server의 실행 모드 변경 방법

1. **Server Manager에 액세스하고 Routing 탭을 누릅니다.**
2. **Set Connectivity Mode 링크를 누릅니다. Set Connectivity Mode 페이지가 표시됩니다.**
3. **드롭다운 목록에서 자원을 선택하거나 Regular Expression 버튼을 눌러 정규 표현식을 입력하고 OK를 누릅니다.**
4. **원하는 모드를 선택합니다.**
5. **OK를 누릅니다.**
6. **Restart Required를 누릅니다. Apply Changes 페이지가 표시됩니다.**
7. **Restart Proxy Server 버튼을 눌러 변경 사항을 적용합니다.**

기본 FTP 전송 모드 변경

FTP에는 FTP 서버와 클라이언트(프록시가 클라이언트 역할) 간에 데이터 연결을 설정하는 두 가지 방법이 있습니다. 두 모드를 각각 PASV 및 PORT 모드 FTP라고 합니다.

- *Passive Mode(PASV).* 프록시 서버에서 데이터 연결을 시작하고 FTP 서버가 이 연결을 수락합니다. 서버가 인바운드 연결을 수락할 필요가 없기 때문에 프록시 서버를 실행하는 사이트의 경우 이 모드가 더 안전합니다.
- *Active Mode(PORT).* 원격 FTP 서버에서 데이터 연결을 시작하고 프록시가 들어오는 연결을 수락합니다. 프록시 서버가 방화벽 내에 있으면 방화벽이 FTP 서버에서 들어오는 FTP 데이터 연결을 차단할 수 있으며 이 경우 PORT 모드가 작동하지 않을 수 있습니다.

일부 FTP 사이트는 방화벽을 실행하기 때문에 프록시 서버에서 PASV 모드가 작동하지 않을 수 있습니다. 따라서 PORT 모드 FTP를 사용하도록 프록시 서버를 구성할 수 있습니다. 전체 서버에 대해 PORT 모드를 사용하거나 특정 FTP 서버에 대해서만 사용할 수 있습니다.

PASV 모드가 On인 경우에도 원격 FTP 서버가 PASV 모드를 지원하지 않으면 프록시 서버는 PORT 모드를 사용합니다.

프록시 서버가 방화벽 뒤에 있어서 PORT 모드 FTP가 작동하지 않는 경우에는 PORT 모드를 활성화할 수 없습니다. 자원에 대해 기본값이 선택된 경우 프록시 서버는 더 일반적인 자원의 모드를 사용합니다. 아무것도 지정하지 않으면 PASV 모드가 사용됩니다.

▼ FTP 모드 설정 방법

1. **Server Manager에 액세스하고 Routing 탭을 누릅니다.**
2. **Set FTP Mode 링크를 누릅니다. Set FTP Mode 페이지가 표시됩니다.**
3. **드롭다운 목록에서 자원을 선택하거나 Regular Expression 버튼을 눌러 정규 표현식을 입력하고 OK를 누릅니다.**
4. **FTP 전송 모드를 선택합니다.**
5. **OK를 누릅니다.**
6. **Restart Required를 누릅니다. Apply Changes 페이지가 표시됩니다.**
7. **Restart Proxy Server 버튼을 눌러 변경 사항을 적용합니다.**

SOCKS 이름 서버 IP 주소 지정

SOCKS 서버를 통해 아웃바운드 연결을 만들도록 프록시를 구성한 경우, SOCKS에 사용할 이름 서버의 IP 주소를 명시적으로 지정해야 할 수 있습니다.

방화벽 내에 있는 내부 DSN 서비스가 아닌 DNS 서버로 외부 호스트 이름을 확인하는 경우에는 이름 서버 IP 주소를 지정해야 합니다.

▼ SOCKS 이름 서버 IP 주소 지정 방법

1 **Server Manager에 액세스하고 Routing 탭을 누릅니다.**

2 **Set SOCKS Name Server 링크를 누릅니다.**
Set SOCKS Name Server 페이지가 표시됩니다.

3 **필드에 DNS 이름 서버의 IP 주소를 입력합니다.**

4 **OK를 누릅니다.**

주 – 한번에 SOCKS 이름 서버 IP 주소를 지정할 수 있는 기능은 SOCKS_NS 환경 변수를 통해서만 액세스할 수 있습니다. 환경 변수를 설정하고 SOCKS Name Server Setting 양식을 사용하여 이름 서버 IP 주소를 지정하면 프록시는 환경 변수 대신 양식에 지정된 IP 주소를 사용합니다.

---

5 **Restart Required를 누릅니다.**
Apply Changes 페이지가 표시됩니다.

6 **Restart Proxy Server 버튼을 눌러 변경 사항을 적용합니다.**

HTTP 요청 로드 균형 조정 구성

Configure HTTP Request Load Balancing 페이지는 지정된 원래 서버에 로드를 분산시키는 데 사용됩니다.

▼ HTTP 요청 로드 균형 조정 구성 방법

1 **Server Manager에 액세스하고 Routing 탭을 누릅니다.**

2 **Configure HTTP Request Load Balancing 링크를 누릅니다.**
Configure HTTP Request Load Balancing 페이지가 표시됩니다.

3 **드롭다운 목록에서 자원을 선택하거나 Regular Expression 버튼을 눌러 정규 표현식을 입력하고 OK를 누릅니다.**

4 **Server 필드에 원래 서버의 URL을 지정합니다. 여러 서버 매개 변수가 제공된 경우 Proxy Server는 지정된 원래 서버에 로드를 분산시킵니다.**

5. **응답에 존재할 경우 Sticky Cookie 필드에 후속 요청이 해당 원래 서버에 고정되도록 하는 쿠키의 이름을 지정합니다. 기본값은 JSESSIONID입니다.**

6. **Sticky Parameter 필드에 라우팅 정보를 조사할 URI 매개 변수의 이름을 지정합니다. URI 매개 변수가 요청 URI에 있고 해당 값에 순서대로 콜론과 라우팅 ID가 있는 경우 요청은 해당 라우팅 ID로 식별된 원래 서버에 "고정"됩니다. 기본값은 jsessionid입니다.**

7. **Route Header 필드에 라우팅 ID를 원래 서버로 전달하는 데 사용되는 HTTP 요청 헤더의 이름을 지정합니다. 기본값은 proxy-jroute입니다.**

8. **응답에서 고정 쿠키가 발견된 경우 Route Cookie 필드에 프록시 서버에 의해 생성되는 쿠키 이름을 지정합니다.**
   기본값은 JROUTE입니다.

9. **Rewrite Host 옵션을 설정하여 서버 매개 변수로 지정된 호스트와 일치하도록 Host HTTP 요청 헤더를 다시 작성할 것인지 여부를 지정합니다.**

10. **Rewrite Location 옵션을 설정하여 서버 매개 변수와 일치하도록 Location HTTP 응답 헤더를 다시 작성할 것인지 여부를 지정합니다.**

11. **Rewrite Content Location 옵션을 설정하여 서버 매개 변수와 일치하도록 Content Location HTTP 응답 헤더를 다시 작성할 것인지 여부를 지정합니다.**

12. **서버 매개 변수와 일치하는 *headername* HTTP 응답 헤더를 다시 작성할 것인지 여부를 지정합니다. 여기서 *headername*은 사용자 정의 헤더 이름입니다. Headername 필드에 헤더 이름을 지정합니다.**

13. **OK를 누릅니다.**

14. **Restart Required를 누릅니다.**
    Apply Changes 페이지가 표시됩니다.

15. **Restart Proxy Server 버튼을 눌러 변경 사항을 적용합니다.**

URL 및 URL 매핑 관리

Server Manager를 사용하여 URL을 다른 서버(때로는 미러 서버라고도 함)로 매핑합니다. 클라이언트가 미러링된 URL이 있는 프록시에 액세스하면 프록시는 URL에서 지정한 서버가 아니라 미러링된 서버에서 요청된 문서를 검색합니다. 클라이언트는 이 요청이 다른 서버로 전달된다는 것을 인식할 수 없습니다. URL을 리디렉션할 수도 있습니다. 이 경우 프록시가 리디렉션된 URL만 클라이언트로 반환하고 문서는 반환하지 않기 때문에 클라이언트가 새 문서를 요청할 수 있습니다. 매핑을 사용하면 PAC 및 PAT 매핑에서처럼 URL을 파일로 매핑할 수도 있습니다.

URL 매핑 만들기 및 수정

URL을 매핑하려면 URL 접두어 및 매핑 위치를 지정합니다. 다음 절에서는 다양한 유형의 URL 매핑에 대해 설명합니다. 다음 유형의 URL 매핑을 만들 수 있습니다.

- 정상 매핑은 URL 접두어를 다른 URL 접두어로 매핑합니다. 예를 들어, `http://www.example.com`으로 시작하는 요청을 받을 때마다 특정 URL로 이동하도록 프록시를 구성할 수 있습니다.
- 역방향 매핑은 리디렉션된 URL 접두어를 다른 URL 접두어로 매핑합니다. 이 매핑은 내부 서버가 문서 대신 리디렉션된 응답을 프록시로 전송할 때 역방향 프록시와 함께 사용됩니다. 자세한 내용은 14 장, “역방향 프록시 사용”을 참조하십시오.
- 정규 표현식은 표현식과 일치하는 모든 URL을 하나의 URL로 매핑합니다. 예를 들어 .*job.*과 일치하는 모든 URL을 특정 URL로 매핑할 수 있습니다. 이 URL은 사용자가 특정 URL로 이동할 수 없는 이유를 설명하는 내용일 수 있습니다.
- 클라이언트 자동 구성은 URL을 프록시 서버에 저장된 특정 `.pac` 파일로 매핑합니다. 자동 구성 파일에 대한 자세한 내용은 17 장, “클라이언트 자동 구성 파일 사용”을 참조하십시오.
- PAT(프록시 배열 테이블)는 URL을 프록시 서버에 저장된 특정 `.pat` 파일로 매핑합니다. 이 유형의 매핑은 마스터 프록시에서만 만들어야 합니다. PAT 파일 및 프록시 배열에 대한 자세한 내용은 268 페이지 “프록시 배열을 통한 라우팅”을 참조하십시오.

URL에 액세스하는 클라이언트는 같은 서버의 다른 위치나 다른 서버로 보내집니다. 이 기능은 자원이 이동되었거나 끝에 슬래시 없이 디렉토리에 액세스할 때 관련 링크의 무결성을 유지하는 데 유용합니다.

예를 들어, `hi.load.com`이라고 하는 로드가 심한 웹 서버를 `mirror.load.com`이라고 하는 다른 서버로 미러링한다고 가정합니다. `hi.load.com` 컴퓨터로 이동하는 URL의 경우, `mirror.load.com` 컴퓨터를 사용하도록 프록시 서버를 구성할 수 있습니다.

소스 URL 접두어는 이스케이프하면 안 됩니다. 대상(미러) URL에서는 HTTP 요청에 잘못된 문자만 이스케이프해야 합니다.

접두어 끝에는 슬래시를 사용하지 마십시오.

▼ URL 매핑 만드는 방법

1 Server Manager에 액세스하고 URL 탭을 누릅니다.

2 Create Mapping 링크를 누릅니다.

Create Mapping 페이지가 표시됩니다.

3 만들 매핑 유형을 선택합니다.

- **Regular Mappings**. 이 옵션을 선택하면 페이지의 아래 부분에 다음 옵션이 표시됩니다.
  - *Rewrite Host.*Host HTTP 헤더를 `to` 매개 변수로 지정된 호스트와 일치하도록 다시 작성해야 하는지 여부를 지정합니다.
  - **Reverse Mappings.**리디렉션된 URL 접두어를 다른 URL 접두어로 매핑합니다. 이 옵션을 선택하면 페이지의 아래 부분에 다음 옵션이 표시됩니다.
    - *Rewrite Location.*Location HTTP 응답 헤더를 다시 작성해야 하는지 여부를 지정합니다.
    - *Rewrite Content Location.*Content-location HTTP 응답 헤더를 다시 작성해야 하는지 여부를 지정합니다.
    - *Rewrite Headername.*확인란을 선택하여 *headername* HTTP 응답 헤더를 다시 작성해야 하는지 여부를 나타냅니다. 여기서 *headername*은 사용자 정의 헤더 이름입니다.

    Regular Expressions.표현식과 일치하는 모든 URL을 하나의 URL로 매핑합니다. 정규 표현식에 대한 자세한 내용은 16 장, “템플리트 및 자원 관리”을 참조하십시오.
  - **Client Autoconfiguration.**URL을 Proxy Server에 저장된 특정 `.pac` 파일로 매핑합니다. 자동 구성 파일에 대한 자세한 내용은 17 장, “클라이언트 자동 구성 파일 사용”을 참조하십시오.
  - **PAT(Proxy Array Table).**URL을 Proxy Server에 저장된 특정 `.pat` 파일로 매핑합니다. 이 유형의 매핑은 마스터 프록시에서만 만들어야 합니다. PAT 파일 및 프록시 배열에 대한 자세한 내용은 12 장, “캐시”의 "프록시 배열을 통한 라우팅"을 참조하십시오.

4 매핑 소스 접두어를 입력합니다.

정상 및 역방향 매핑의 경우 이 접두어는 대체할 URL의 일부여야 합니다.

정규 표현식 매핑의 경우 URL 접두어는 일치시킬 모든 URL에 대한 정규 표현식이어야 합니다. 매핑에 대한 템플리트를 선택한 경우에는 정규 표현식이 템플리트의 정규 표현식에 있는 URL에 대해서만 작동합니다.

클라이언트 자동 구성 매핑과 프록시 배열 테이블 매핑의 경우 URL 접두어는 클라이언트가 액세스하는 전체 URL이어야 합니다.

5 매핑 대상을 입력합니다.

클라이언트 자동 구성 및 프록시 배열 테이블을 제외한 모든 매핑 유형에서 이 선언은 매핑할 전체 URL이어야 합니다. 클라이언트 자동 구성 매핑의 경우 이 값은 프록시 서버의 하드 디스크에 있는 `.pac` 파일에 대한 절대 경로여야 합니다. 프록시 배열 테이블 매핑의 경우 이 값은 마스터 프록시의 로컬 디스크에 있는 `.pat` 파일에 대한 절대 경로여야 합니다.

6. **드롭다운 목록에서 템플리트 이름을 선택하거나 템플리트를 적용하지 않으려면 NONE 값을 그대로 둡니다.**

7. **OK를 눌러 매핑을 만듭니다.**

8. **Restart Required를 누릅니다.**
   Apply Changes 페이지가 표시됩니다.

9. **Restart Proxy Server 버튼을 눌러 변경 사항을 적용합니다.**

▼ 기존 매핑 변경 방법

1. **Server Manager에 액세스하고 URL 탭을 누릅니다.**

2. **View/Edit Mappings 링크를 누릅니다.**
   View/Edit Mappings 페이지가 표시됩니다.

3. **수정할 매핑 옆에 있는 Edit 링크를 누릅니다. 매핑의 영향을 받는 접두어, 매핑된 URL 및 템플리트를 편집할 수 있습니다. OK를 눌러 변경 사항을 확인합니다.**

4. **Restart Required를 누릅니다. Apply Changes 페이지가 표시됩니다.**

5. **Restart Proxy Server 버튼을 눌러 변경 사항을 적용합니다.**

▼ 매핑 제거 방법

1. **Server Manager에 액세스하고 URL 탭을 누릅니다.**

2. **View/Edit Mappings 링크를 누릅니다.**
   View/Edit Mappings 페이지가 표시됩니다.

3. **제거할 매핑을 선택한 다음 옆에 있는 Remove 링크를 누릅니다.**

4. **Restart Required를 누릅니다. Apply Changes 페이지가 표시됩니다.**

5. **Restart Proxy Server 버튼을 눌러 변경 사항을 적용합니다.**

URL 리디렉션

문서를 가져와 반환하는 대신 리디렉션된 URL을 클라이언트에 반환하도록 프록시 서버를 구성할 수 있습니다. 리디렉션을 사용하면 클라이언트는 원래 요청한 URL이 다른 URL로 리디렉션되었음을 인식합니다. 일반적으로 클라이언트는 즉시 리디렉션된 URL을 요청합니다. Netscape Navigator는 리디렉션된 URL을 자동으로 요청합니다. 다음에 사용자가 문서를 명시적으로 요청할 필요가 없습니다.

액세스가 거부된 이유를 설명하는 URL로 사용자를 리디렉션할 수 있기 때문에 특정 영역에 대한 액세스를 거부하는 경우 URL 리디렉션이 유용합니다.

▼ 하나 이상의 URL 리디렉션 방법

1. **Server Manager에 액세스하고 URL 탭을 누릅니다.**
2. **Redirect URLs 링크를 누릅니다. Redirect URLs 페이지가 표시됩니다.**
3. **URL 접두어인 소스 URL을 입력합니다.**
4. **리디렉션할 URL을 입력합니다. 이 URL은 URL 접두어 또는 고정 URL일 수 있습니다.**
   - 리디렉션할 URL로 URL 접두어를 사용하는 경우, URL prefix 필드 옆에 있는 선택 버튼을 선택하고 URL 접두어를 입력합니다.
   - 고정 URL을 사용하는 경우 Fixed URL 필드 옆에 있는 선택 버튼을 선택하고 고정 URL을 입력합니다.
5. **OK를 누릅니다.**
6. **Restart Required를 누릅니다.**
   Apply Changes 페이지가 표시됩니다.
7. **Restart Proxy Server 버튼을 눌러 변경 사항을 적용합니다.**

◆ ◆ ◆ 12 장

12 캐시

이 장에서는 Sun Java System Web Proxy Server가 문서를 캐시하는 방법에 대해 설명합니다. 또한 온라인 페이지를 사용하여 캐시를 구성할 수 있는 방법에 대해 설명합니다.

이 장은 다음 내용으로 구성되어 있습니다.

- 234 페이지 “캐시 작동 방법”
- 234 페이지 “캐시 구조 이해”
- 235 페이지 “캐시에 파일 배포”
- 236 페이지 “캐시 사양 설정”
- 241 페이지 “캐시 만들기 및 수정”
- 242 페이지 “캐시 용량 설정”
- 243 페이지 “캐시 섹션 관리”
- 244 페이지 “가비지 컬렉션 기본 설정 지정”
- 244 페이지 “가비지 컬렉션 예약”
- 244 페이지 “캐시 구성”
- 247 페이지 “로컬 호스트 캐시”
- 248 페이지 “파일 캐시 구성”
- 250 페이지 “URL 데이터베이스 보기”
- 251 페이지 “캐시 일괄 업데이트 사용”
- 254 페이지 “캐시 명령줄 인터페이스 사용”
- 260 페이지 “ICP(Internet Cache Protocol) 사용”
- 268 페이지 “프록시 배열 사용”

캐시 작동 방법

캐시는 네트워크 트래픽을 줄이고 원격 서버로 직접 이동하지 않고 프록시 서버를 사용하는 클라이언트에게 신속한 응답 시간을 제공합니다.

클라이언트가 프록시 서버에 웹 페이지 또는 문서를 요청할 경우 프록시 서버는 문서를 클라이언트에 보내는 동시에 원격 서버의 문서를 로컬 캐시 디렉토리 구조로 복사합니다.

클라이언트가 이전에 요청하여 프록시 캐시에 복사한 문서를 요청하는 경우 프록시는 다음 그림에 표시된 대로 원격 서버에서 문서를 다시 검색하는 대신 캐시에서 문서를 반환합니다. 프록시에서 파일이 최신 상태가 아님을 확인한 경우 프록시는 문서를 클라이언트에 보내기 전에 원격 서버의 문서를 새로 고치고 해당 캐시를 업데이트합니다.

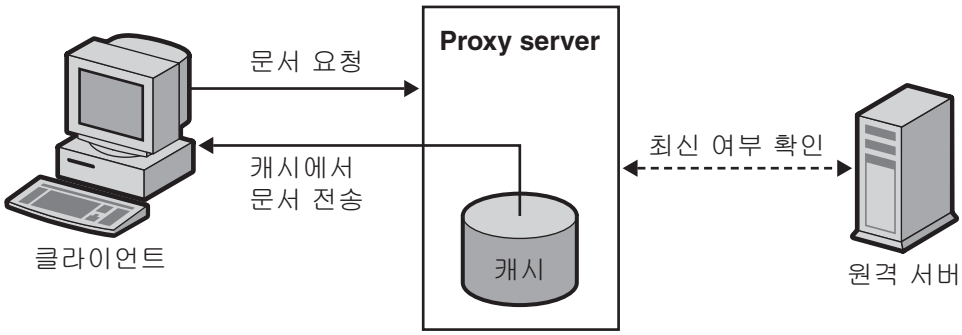

그림 12–1 프록시 문서 검색

캐시의 파일은 Sun Java System Web Proxy Server 가비지 컬렉션 유틸리티(CacheGC)에 의해 자동으로 유지 관리됩니다. CacheGC는 정기적으로 캐시를 자동 삭제하여 캐시에 오래된 문서가 남아 있지 않도록 합니다.

캐시 구조 이해

캐시는 하나 이상의 파티션으로 구성되어 있습니다. 이론적으로 파티션은 캐시용으로 설정한 디스크의 저장 영역입니다. 캐시 범위를 여러 디스크로 확장하려면 각 디스크에 대해 최소 하나 이상의 캐시 파티션을 구성합니다. 각 파티션을 독립적으로 관리할 수 있습니다. 즉, 모든 다른 파티션과 별도로 특정 파티션을 활성화, 비활성화 및 구성할 수 있습니다.

캐시된 여러 파일을 단일 위치에 저장할 경우 성능이 느려질 수 있기 때문에 각 파티션마다 여러 디렉토리 또는 섹션을 만듭니다. 섹션은 캐시 구조에서 파티션 다음

수준입니다. 모든 파티션에서 캐시에 최대 256개의 섹션을 포함할 수 있습니다. 캐시 섹션 수는 2의 거듭제곱이어야 합니다(예를 들어 1, 2, 4, 8, 16, ..., 256).

캐시 구조 계층의 최종 수준은 하위 구역입니다. 하위 구역은 섹션 내의 디렉토리입니다. 각 섹션에는 64개의 하위 구역이 있습니다. 캐시된 파일은 캐시의 최하위 수준인 하위 구역에 저장됩니다.

다음 그림에서는 파티션 및 섹션을 포함한 캐시 구조의 예를 보여 줍니다. 이 그림에서 캐시 디렉토리 구조는 전체 캐시를 세 개의 파티션으로 나눕니다. 첫 번째 파티션에는 4개의 캐시 섹션이 있으며 다른 2개의 파티션에는 각각 2개의 섹션이 있습니다.

각 캐시 섹션에는 섹션을 의미하는 "s" 다음에 섹션 번호가 지정됩니다. s3.4로 표시된 섹션의 경우 3은 캐시 섹션 수에 대해 2의 거듭제곱($2^3 = 8$)을 나타내고 4는 섹션 번호를 의미합니다(8개의 섹션에 0-7 레이블 지정). 따라서 s3.4는 8개의 섹션 중 5번째 섹션을 의미합니다.

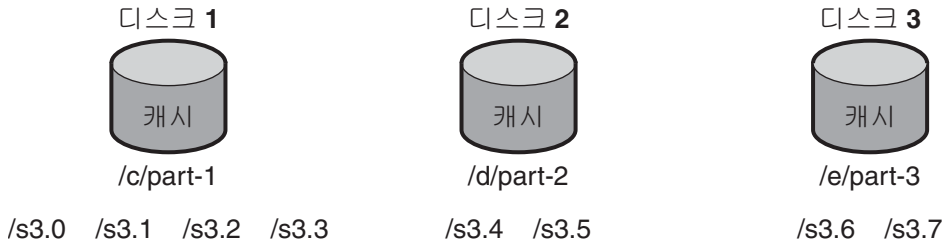

그림 12–2 캐시 구조의 예

캐시에 파일 배포

Proxy Server는 특정 알고리즘을 사용하여 문서를 저장해야 할 디렉토리를 결정합니다. 이 알고리즘을 통해 디렉토리 내에 문서를 동일하게 배포합니다. 문서의 수가 많은 디렉토리의 경우 성능 문제를 일으킬 수 있기 때문에 반드시 동일하게 배포해야 합니다.

Proxy Server는 RSA MD5 알고리즘(메시지 다이제스트 5)을 사용하여 URL을 16바이트의 이진 데이터로 줄이고 이 데이터의 8바이트를 사용하여 캐시에 문서를 저장하는 데 사용되는 16자의 16진수 파일 이름을 계산합니다.

캐시 사양 설정

캐시를 활성화하고 캐시 사양 설정을 통해 Proxy Server가 캐시하는 프로토콜 유형을 제어할 수 있습니다. 캐시 사양은 다음 항목으로 구성되어 있습니다.

- 캐시 활성화 또는 비활성화 여부
- 캐시가 임시 파일을 저장하는 작업 디렉토리
- 캐시된 URL을 기록할 디렉토리 이름
- 캐시 크기
- 캐시 용량
- 캐시될 프로토콜의 유형
- 캐시된 문서의 새로 고침 시기
- 프록시가 문서의 액세스 횟수를 추적하고 이 값을 원격 서버에 다시 보고해야 하는지 여부

주 – 대용량 캐시에 대한 사양을 설정하는 데 많은 시간이 소요되며 관리 인터페이스 시간이 초과될 수 있습니다. 따라서 대용량 캐시를 만드는 경우 명령줄 유틸리티를 사용하여 캐시 사양을 설정합니다. 캐시 명령줄 유틸리티에 대한 자세한 내용은 254 페이지 “캐시 명령줄 인터페이스 사용”을 참조하십시오.

▼ 캐시 사양 설정 방법

1 **Server Manager에 액세스하고 Caching 탭을 누릅니다.**

2 **Set Cache Specifics 링크를 누릅니다.**

Set Cache Specifics 페이지가 표시됩니다.

3 **적절한 옵션을 선택하여 캐시를 활성화하거나 비활성화할 수 있습니다.**

기본적으로 캐시는 활성화되어 있습니다.

4 **작업 디렉토리를 제공합니다.**

기본적으로 작업 디렉토리는 프록시 인스턴스 아래 표시됩니다. 이 위치를 변경할 수 있습니다. 자세한 내용은 238 페이지 “캐시 작업 디렉토리 만들기”를 참조하십시오.

5 **Partition Configuration 링크를 누릅니다.**

Add/Edit Cache Partitions 페이지가 표시됩니다. 새 캐시 파티션을 추가하거나 기존 캐시 파티션을 편집할 수 있습니다. 캐시 크기는 캐시가 증가할 수 있는 최대 크기입니다. 최대 캐시 크기는 32GB입니다. 자세한 내용은 238 페이지 “캐시 크기 설정”을 참조하십시오.

6 **Cache Capacity Configuration 링크를 누릅니다.**

Set Cache Capacity 페이지가 표시됩니다. Set Cache Capacity 페이지에서 캐시 용량을 설정할 수 있습니다.

7 **HTTP 문서 캐시를 활성화하려면 Cache HTTP를 선택합니다.**

프록시 서버가 HTTP 문서를 캐시하도록 결정한 경우 캐시의 문서에 대해 항상 최신 검사를 수행해야 하는지 또는 일정한 간격을 기준으로 검사를 수행해야 하는지 여부를 결정합니다. 또한 Proxy Server가 캐시 적중 횟수를 원격 서버에 보고하는 기능을 활성화 또는 비활성화할 수 있습니다. 자세한 내용은 238 페이지 "HTTP 문서 캐시"를 참조하십시오. 사용 가능한 옵션은 다음과 같습니다.

- HTTP 문서를 항상 최신 상태로 유지하려면 Always Check That The Document Is Up To Date 옵션을 선택합니다.
  - Check Only If Last Check More Than 드롭다운 목록에서 시간을 선택하여 프록시 서버의 새로 고침 간격을 지정합니다. 다음 옵션 중 하나를 사용하여 최신 여부 확인을 수행합니다.
    - **마지막으로 수정된 요소 사용.**마지막으로 수정된 헤더는 원래 서버에서 문서와 함께 전송됩니다.
    - **Only Explicit Expiration Information 사용.**프록시 서버가 Expires 헤더를 사용하여 캐시 항목이 새로 고침 또는 오래된 상태인지 여부를 확인합니다.

    프록시 서버가 액세스 횟수를 원격 서버에 보고하는 것을 방지하려면 Never Report Accesses To Remote Server 옵션을 선택합니다.
  - 문서에 액세스한 횟수를 추적하여 원격 서버에 다시 보고하려면 Report Cache Hits To Remote Server 옵션을 선택합니다.

8 **Yes, Reload If Older Than 확인란을 선택하여 캐시된 FTP 문서의 새로 고침 간격을 설정하고 드롭다운 목록에서 해당 값을 선택하여 시간 간격을 설정할 수도 있습니다. 자세한 내용은 240 페이지 "FTP 및 Gopher 문서 캐시"를 참조하십시오.**

9 **캐시된 Gopher 문서의 갱신 간격을 설정할 수 있습니다. Yes, Reload If Older Than 확인란을 선택하고 드롭다운 목록에서 값을 선택하여 시간 간격을 설정합니다. 자세한 내용은 240 페이지 "FTP 및 Gopher 문서 캐시"를 참조하십시오.**

10 **OK를 누릅니다.**

11 **Restart Required를 누릅니다. Apply Changes 페이지가 표시됩니다.**

12 **Restart Proxy Server 버튼을 눌러 변경 사항을 적용합니다.**

캐시 작업 디렉토리 만들기

캐시 파일은 캐시 파티션에 있습니다. Set Cache Specifics 페이지에서 지정한 작업 디렉토리는 대부분 캐시의 상위 디렉토리입니다. 캐시된 모든 파일이 캐시 디렉토리 아래 구성된 디렉토리 구조에 나타납니다. 캐시 디렉토리 이름을 변경하거나 다른 위치로 이동하는 경우 프록시에 새 위치를 제공해야 합니다.

대용량 캐시 구조를 하나의 대용량 디스크에 모두 보관하는 대신 여러 소용량 디스크에 나누어 보관할 수 있도록 캐시 디렉토리 구조를 여러 파일 시스템으로 확장할 수 있습니다. 각 프록시 서버에 자체 캐시 디렉토리 구조가 있어야 합니다. 즉 캐시 디렉토리를 여러 프록시 서버에서 동시에 공유할 수 없습니다.

캐시 크기 설정

캐시 크기는 파티션 크기를 나타냅니다. 캐시 크기는 캐시가 증가할 수 있는 최대 크기이기 때문에 항상 캐시 용량보다 작아야 합니다. 모든 파티션 크기의 합계는 캐시 크기보다 작거나 같아야 합니다.

프록시 캐시에 사용 가능한 디스크 공간의 크기는 캐시 성능에 중요한 영향을 줍니다. 캐시가 너무 작으면 디스크에 공간을 만들기 위해 Cache GC가 더 자주 캐시된 문서를 제거해야 하며 컨텐트 서버에서 문서를 검색하는 횟수도 늘어나야 합니다. 이러한 작업으로 인해 성능이 느려질 수 있습니다.

캐시 크기가 클수록 더 많은 문서가 캐시되어 네트워크 트래픽 부하가 줄어들고 프록시의 응답 시간이 더 빨라지기 때문에 효율적입니다. 또한 캐시된 문서가 더 이상 필요하지 않은 경우 GC가 해당 문서를 제거합니다. 다른 파일 시스템 제한이 없다면 캐시 크기는 클수록 좋습니다. 초과 공간은 사용되지 않은 상태로 남아 있습니다.

또한 캐시를 여러 디스크 파티션에 분할할 수 있습니다.

HTTP 문서 캐시

HTTP 문서는 다른 프로토콜의 문서에서 제공하지 않는 캐시 기능을 제공합니다. 그러나 캐시를 제대로 설정 및 구성하면 Proxy Server가 HTTP, FTP 및 Gopher 문서를 효과적으로 캐시할 수 있습니다.

주 – Proxy Server 4는 HTTPS 문서를 캐시하지 않습니다.

모든 HTTP 문서에는 Proxy Server가 프록시 캐시의 문서 및 원격 서버의 문서를 비교하고 평가하는 데 사용하는 설명 헤더 섹션이 있습니다. 프록시가 HTTP 문서에 대한 최신 검사를 수행할 때 캐시 버전이 오래된 경우 서버에 문서를 반환하라는 요청을 보냅니다. 대개 마지막 요청 이후 문서가 변경되지 않기 때문에 전송되지 않습니다. HTTP 문서가 최신 상태인지 여부를 확인하기 위한 이러한 검사 방법은 대역폭을 절약하고 대기 시간을 단축합니다.

원격 서버와의 트랜잭션을 줄이기 위해 Proxy Server를 사용하여 HTTP 문서에 대한 캐시 만료 설정을 지정할 수 있습니다. 캐시 만료 설정에서는 HTTP 문서가 서버에 요청을 보내기 전에 최신 여부 확인이 필요한지 여부를 평가하기 위해 프록시에 정보를 제공합니다. 프록시는 헤더에 있는 HTTP 문서의 마지막으로 수정된 날짜를 기준으로 평가를 수행합니다.

또한 HTTP 문서를 통해 캐시 새로 고침 설정을 사용할 수 있습니다. 이 옵션은 프록시가 만료 설정을 대체할 수 있는 최신 여부 확인을 항상 수행하거나 검사를 수행하기 전에 프록시가 특정 시간 동안 대기할지 여부를 지정합니다. 다음 표는 만료 설정 및 새로 고침 설정이 모두 지정된 경우 프록시가 수행하는 작업을 보여줍니다. 새로 고침 설정을 사용하면 대기 시간이 단축되고 대역폭이 크게 줄어 듭니다.

표 12–1 HTTP를 통해 캐시 만료 및 캐시 새로 고침 설정 사용

Refresh 설정	Expiration 설정	Results
Always do an up-to-date check	(해당 없음)	항상 최신 여부 확인 수행
User-specified interval	Use document's "expires" header	간격이 만료된 경우 최신 여부 확인 수행
	Estimate with document's Last-Modified header	측정 및 만료 헤더의 최소값*

주 – * 최소값을 사용하면 자주 변경되는 문서에 대해 캐시에서 오래된 데이터를 가져오는 것을 방지합니다.

HTTP 캐시 새로 고침 간격 설정

Proxy Server에서 HTTP 문서를 캐시하도록 결정하는 경우 캐시의 문서에 대해 항상 최신 여부 확인을 수행해야 하는지 여부 또는 캐시 새로 고침 설정(최신 여부 확인 간격)을 기준으로 검사해야 하는지 여부를 결정합니다. 예를 들어, HTTP 문서의 경우 적절한 새로 고침 간격은 4-8시간입니다. 새로 고침 간격이 길어질수록 프록시가 원격 서버와 연결되는 횟수가 줄어듭니다. 새로 고침 간격 동안 프록시가 최신 여부 확인을 수행하지 않더라도 클라이언트에서 Reload 버튼을 눌러 새로 고침을 강제로 수행할 수 있습니다. 이 작업을 통해 프록시가 원격 서버로 최신 여부 확인을 강제 수행합니다.

Set Cache Specifics 페이지 또는 Set Caching Configuration 페이지에서 HTTP 문서에 대한 새로 고침 간격을 설정할 수 있습니다. Set Cache Specifics 페이지에서 전역 캐시 절차를 구성할 수 있으며 Set Caching Configuration 페이지에서 특정 URL 및 자원에 대한 캐시 절차를 제어할 수 있습니다.

HTTP 캐시 만료 정책 설정

또한 마지막으로 수정된 요소 또는 명시적 만료 정보만 사용하여 캐시된 문서가 최신 상태인지 여부를 검사하도록 서버를 설정할 수 있습니다.

명시적 만료 정보는 해당 파일이 만기가 되는 날짜와 시간을 지정하는 일부 HTTP 문서에 있는 헤더입니다. HTTP 문서에서 명시적 만료 헤더를 사용하는 경우가 많지 않기 때문에 마지막으로 수정된 헤더를 기준으로 측정해야 합니다.

마지막으로 수정된 헤더를 기준으로 HTTP 문서를 캐시하도록 결정한 경우 만료 측정에 사용할 분율을 선택해야 합니다. LM 요소라고 하는 이 분율은 마지막 수정 시간과 문서에 대해 마지막 최신 여부 확인을 수행한 시간 사이의 간격을 곱한 값입니다. 결과 값을 마지막 최신 여부 확인 이후 시간과 비교합니다. 이 수치가 시간 간격보다 작은 경우 문서는 만료되지 않습니다. 분율이 작을수록 프록시가 문서를 검사하는 빈도가 높아집니다.

예를 들어, 10일 전에 마지막으로 변경한 문서가 있다고 가정합니다. 마지막으로 수정된 요소를 0.1로 설정하면 프록시는 이 요소를 문서가 하루 동안(10 * 0.1 = 1) 변경되지 않은 상태를 유지하는 것으로 해석합니다. 이러한 경우 프록시는 하루 이내에 검사된 문서가 있으면 캐시에서 문서를 반환합니다.

동일한 예에서 HTTP 문서의 캐시 새로 고침 설정을 1일 이하로 설정하면 프록시는 하루에 1회 이상 최신 여부 확인을 수행합니다. 프록시는 항상 값, 캐시 새로 고침 또는 캐시 만료를 사용하고 이를 위해 업데이트를 더 자주 수행해야 합니다.

Set Cache Specifics 페이지 또는 Set Caching Configuration 페이지에서 HTTP 문서에 대한 만료 설정을 설정할 수 있습니다. Set Cache Specifics 페이지에서 전역 캐시 절차를 구성할 수 있으며 Set Caching Configuration 페이지에서 특정 URL 및 자원에 대한 캐시 절차를 제어할 수 있습니다.

원격 서버에 HTTP 액세스 보고

문서가 Sun Java System Web Proxy Server에 의해 캐시된 경우 다시 새로 고치기 전에 여러 번 액세스할 수 있습니다. 원격 서버의 경우 캐시할 프록시에 하나의 복사본을 보내면 하나의 액세스 또는 "적중 횟수"만 표시합니다.Proxy Server는 최신 여부 확인 간격 사이에 프록시 캐시에서 제공된 문서에 액세스한 횟수를 계산한 후 다음에 문서를 새로 고칠 때 추가 HTTP 요청 헤더(Cache-Info)에서 해당 적중 횟수를 원격 서버에 다시 보낼 수 있습니다. 이와 같이 원격 서버가 이러한 유형의 헤더를 인식하도록 구성된 경우 문서에 액세스한 더욱 정확한 횟수 정보가 수신됩니다.

FTP 및 Gopher 문서 캐시

FTP 및 Gopher에는 문서가 최신 상태인지 여부를 확인하는 검사 방법이 없습니다. 따라서 FTP 및 Gopher 문서의 캐시를 최적화하는 유일한 방법은 캐시 새로 고침 간격을 설정하는 것입니다. 캐시 새로 고침 간격은 원격 서버에서 최신 버전의 문서를 검색하기 전에 Proxy Server가 대기하는 시간입니다. 캐시 새로 고침 간격을 설정하지 않는 경우 프록시는 캐시 버전이 최신 상태이더라도 이러한 문서를 검색합니다.

FTP 및 Gopher에 대한 캐시 새로 고침 간격을 설정하는 경우 프록시가 가져오는 문서가 안전한지 여부를 고려해야 합니다. 예를 들어, 거의 변경되지 않는 정보를 저장하는 경우 몇 일에 해당하는 높은 값을 사용합니다. 데이터를 지속적으로 변경하는 경우 최소 몇 시간마다 파일을 검색하도록 합니다. 새로 고침 시간 동안 오래된 파일이 클라이언트에 전송될 수 있습니다. 간격이 짧은 경우(예:몇 시간) 이러한 위험의 대부분이 제거되는 동시에 응답 시간이 상당히 빨라집니다.

Set Cache Specifics 페이지 또는 Set Caching Configuration 페이지에서 FTP 및 Gopher 문서에 대한 캐시 새로 고침 간격을 설정할 수 있습니다. Set Cache Specifics 페이지에서 전역 캐시 절차를 구성할 수 있으며 Set Caching Configuration 페이지에서 특정 URL 및 자원에 대한 캐시 절차를 제어할 수 있습니다. Set Cache Specifics 페이지 사용에 대한 자세한 내용은 236 페이지 “캐시 사양 설정”을 참조하십시오. Set Caching Configuration 페이지 사용에 대한 자세한 내용은 244 페이지 “캐시 구성”을 참조하십시오.

주 – FTP 및 Gopher 문서가 크게 다른 경우(일부는 자주 변경되고 나머지는 거의 변경되지 않음) Set Caching Configuration 페이지를 사용하여 각 유형별 문서에 대한 개별 템플리트를 만든 다음(예: `ftp://.*.gif`자원을 사용하여 템플리트 만들기) 해당 자원에 적합한 새로 고침 간격을 설정합니다.

캐시 만들기 및 수정

캐시 파티션은 캐시를 위해 설정된 디스크 또는 메모리의 예약 부분입니다. 캐시 용량이 변경될 경우 파티션을 변경하거나 추가할 수 있습니다.

▼ 캐시 파티션 추가 방법

1. **Server Manager에 액세스하고 Caching 탭을 누릅니다.**
2. **Add/Edit Cache Partitions 링크를 누릅니다.**
   Add/Edit Cache Partitions 페이지가 표시됩니다.
3. **Add Cache Partition 버튼을 누릅니다.**
   Cache Partition Configuration 페이지가 표시됩니다.
4. **새 파티션에 적절한 값을 제공합니다.**
5. **OK를 누릅니다.**
6. **Restart Required를 누릅니다.**
   Apply Changes 페이지가 표시됩니다.

7 **Restart Proxy Server 버튼을 눌러 변경 사항을 적용합니다.**

▼ 캐시 파티션 수정 방법

1 **Server Manager에 액세스하고 Caching 탭을 누릅니다.**

2 **Add/Edit Cache Partitions 링크를 누릅니다.**
Add/Edit Cache Partitions 페이지가 표시됩니다.

3 **변경할 파티션의 이름을 클릭합니다.**

4 **정보를 편집합니다.**

5 **OK를 누릅니다.**

6 **Restart Required를 누릅니다.**
Apply Changes 페이지가 표시됩니다.

7 **Restart Proxy Server 버튼을 눌러 변경 사항을 적용합니다.**

캐시 용량 설정

캐시 용량 값은 캐시 디렉토리 구조를 파생하는 데 사용합니다. 캐시 디렉토리가 포함할 수 있는 섹션 수는 캐시 용량에서 파생됩니다. 캐시 용량은 캐시 디렉토리의 캐시 계층과 직접 관련됩니다. 용량이 클수록 계층이 커집니다. 캐시 용량은 캐시 크기와 같거나 커야 합니다. 나중에 캐시 크기를 증가할 계획이 있는 경우(예: 외부 디스크 추가) 용량을 캐시 크기보다 크게 설정하는 것이 좋습니다. 최대 캐시 용량은 32GB이며 256개의 섹션을 만들 수 있습니다.

▼ 캐시 용량 설정 방법

1 **Server Manager에 액세스하고 Caching 탭을 누릅니다.**

2 **Set Cache Capacity 링크를 누릅니다.**
Set Cache Capacity 페이지가 표시됩니다.

3 **New Capacity Range 드롭다운 목록에서 용량을 선택합니다.**

4 **OK를 누릅니다.**

5 **Restart Required를 누릅니다.**
Apply Changes 페이지가 표시됩니다.

6 **Restart Proxy Server 버튼을 눌러 변경 사항을 적용합니다.**

캐시 섹션 관리

프록시 캐시는 하나 이상의 캐시 섹션으로 구분됩니다. 최대 256개의 섹션으로 구성할 수 있습니다. 캐시 섹션의 값은 2의 거듭제곱이어야 합니다(예: 1, 2, 4, 8, 16, ..., 256). 최대 용량은 32GB(최적)이며 256개의 섹션을 포함할 수 있습니다.

캐시 용량으로 500MB를 선택할 경우 설치 프로그램은 4개의 캐시 섹션(500 d6 125 = 4)을 만들고 2GB를 선택하면 16개의 섹션(2000 d6 125 = 16)을 만듭니다. 각 섹션에 대한 최적값이 125MB로 선택되어 이와 같은 섹션 수를 얻을 수 있습니다. 섹션 수가 많을수록 저장되고 배포되는 URL 수도 증가합니다.

▼ 캐시 섹션 관리 방법

1 **Server Manager에 액세스하고 Caching 탭을 누릅니다.**

2 **Manage Sections 링크를 누릅니다.**
Manage Sections 페이지가 표시됩니다.

3 **테이블에서 정보를 변경합니다.**
섹션을 기존 파티션 사이에서 이동할 수 있습니다.

4 **OK를 누릅니다.**

5 **Restart Required를 누릅니다.**
Apply Changes 페이지가 표시됩니다.

6 **Restart Proxy Server 버튼을 눌러 변경 사항을 적용합니다.**

가비지 컬렉션 기본 설정 지정

캐시 가비지 컬렉터를 사용하여 캐시에서 파일을 삭제할 수 있습니다. 가비지 컬렉션을 자동 모드 또는 명시적 모드에서 수행할 수 있습니다. 명시적 모드는 관리자에 의해 외부에서 예약됩니다. 모드 중 하나를 선택하고 OK를 누릅니다. Restart Required를 누릅니다. Apply Changes 페이지가 표시됩니다. Restart Proxy Server 버튼을 눌러 변경 사항을 적용합니다.

가비지 컬렉션 예약

Schedule Garbage Collection 페이지에서 가비지 컬렉션이 수행되는 요일 및 시간을 지정할 수 있습니다.

▼ 가비지 컬렉션 설정 방법

1. **Server Manager에 액세스하고 Caching 탭을 누릅니다.**
2. **Schedule Garbage Collection 링크를 누릅니다.**
   Schedule Garbage Collection이 표시됩니다.
3. **Schedule Garbage Collection At 목록에서 가비지 컬렉션을 수행할 시간을 선택합니다.**
4. **가비지 컬렉션을 수행할 요일을 지정합니다.**
5. **OK를 누릅니다.**
6. **Restart Required를 누릅니다.**
   Apply Changes 페이지가 표시됩니다.
7. **Restart Proxy Server 버튼을 눌러 변경 사항을 적용합니다.**

캐시 구성

지정한 정규 표현식 패턴과 일치하는 URL에 대해 여러 구성 매개 변수 값을 지정할 수 있습니다. 이 기능을 통해 캐시된 문서 유형을 기준으로 프록시 캐시를 미세 조정할 수 있습니다. 캐시 구성에서 다음 항목을 식별할 수 있습니다.

- 캐시 기본값
- 인증이 필요한 페이지 캐시 방법
- 쿼리 캐시 방법

- 최소 및 최대 캐시 파일 크기
- 캐시된 문서의 새로 고침 시기
- 캐시 만료 정책
- 클라이언트 중단 시 캐시 동작
- 원래 서버와 연결 실패 시 캐시 동작

주 – 특정 자원의 캐시 기본값을 Derived configuration 또는 Don't cache로 설정할 경우 캐시 구성 옵션이 Set Caching Configuration 페이지에 표시되지 않습니다. 그러나 캐시 기본값으로 Cache for a resource를 선택할 경우 여러 다른 구성 항목을 지정할 수 있습니다.

▼ 캐시를 구성하는 방법

1 **Server Manager에 액세스하고 Caching 탭을 누릅니다.**

2 **Set Caching Configuration 페이지를 누릅니다.**
Set Caching Configuration 페이지가 표시됩니다.

3 **드롭다운 목록에서 자원을 선택하거나 Regular Expression 버튼을 눌러 정규 표현식을 입력하고 OK를 누릅니다.**

4 **구성 정보를 변경합니다.**

5 **OK를 누릅니다.**

6 **Restart Required를 누릅니다.**
Apply Changes 페이지가 표시됩니다.

7 **Restart Proxy Server 버튼을 눌러 변경 사항을 적용합니다.**

구성 요소 캐시

다음 절에서는 사용자의 요구 사항에 가장 적합한 구성을 결정하는 데 도움을 주는 정보에 대해 설명합니다.

캐시 기본값 설정

프록시 서버를 사용하여 특정 자원에 대한 캐시 기본값을 식별할 수 있습니다. 자원은 지정한 특정 기준과 일치하는 파일 유형입니다. 예를 들어, 서버가 `company.com` 도메인의 모든 문서를 자동으로 캐시하도록 하려면 다음 정규 표현식을 만들 수 있습니다.

```
[a-z] *://[^/:]\\.company\\.com.*.
```

Cache 옵션은 기본적으로 선택됩니다. 서버가 해당 도메인에서 캐시 가능한 모든 문서를 자동으로 캐시합니다.

주 – 특정 자원에 대한 캐시 기본값을 Derived configuration 또는 Don't cache로 설정할 경우 해당 자원에 대한 캐시를 구성할 필요가 없습니다. 그러나 캐시 기본값으로 Cache for a resource를 선택할 경우 여러 다른 구성 항목을 지정할 수 있습니다. 이러한 항목에 대한 목록은 244 페이지 "캐시 구성"을 참조하십시오.

또한 HTTP, FTP 및 Gopher에 대한 캐시 기본값을 설정할 수 있습니다.

인증이 필요한 페이지 캐시

서버가 사용자 인증이 필요한 파일을 캐시하도록 할 수 있습니다. Proxy Server는 사용자가 요청하는 경우 원격 서버에서 인증이 필요하도록 캐시의 파일에 태그를 지정합니다.

Proxy Server는 원격 서버의 인증 방법을 결정할 수 없고 사용자 아이디 또는 비밀번호 목록이 없기 때문에 인증이 필요한 문서에 대해 요청이 있을 때마다 원격 서버를 통해 최신 여부 확인을 강제로 수행합니다. 따라서 해당 파일에 대한 액세스 권한을 얻으려면 아이디 및 비밀번호를 입력해야 합니다. 브라우저 세션에서 이전에 이미 해당 서버에 액세스한 경우 브라우저는 사용자에게 메시지를 표시하지 않고 자동으로 인증 정보를 전송합니다.

인증이 필요한 페이지의 캐시를 활성화하지 않는 경우 프록시는 이러한 페이지를 캐시하지 않습니다(기본 동작).

쿼리 캐시

캐시된 쿼리만 HTTP 문서에서 작동합니다. 캐시되는 쿼리의 길이를 제한하거나 쿼리 캐시를 완전히 금지할 수 있습니다. 쿼리가 길수록 반복될 가능성은 줄어들지만 캐시의 유용성도 감소됩니다.

쿼리 시 다음 캐시 제한 사항이 적용됩니다.

- 액세스 메소드가 GET이어야 하고 인증된 페이지 캐시를 활성화하지 않는 한 문서를 보호할 수 없으며 응답에 최소한 마지막으로 수정된 헤더가 있어야 합니다. 따라서 쿼리 엔진이 쿼리 결과 문서를 캐시할 수 있음을 표시해야 합니다.
- 마지막으로 수정된 헤더가 있는 경우 쿼리 엔진은 효과적으로 캐시를 수행하기 위해 조건부 GET 메소드(If-modified-since 헤더 포함)를 지원해야 하며 그렇지 않은 경우 쿼리 엔진이 만료 헤더를 반환해야 합니다.

최소 및 최대 캐시 파일 크기 설정

Proxy Server에 의해 캐시된 파일의 최소 및 최대 크기를 설정할 수 있습니다. 네트워크 연결 속도가 빠른 경우 최소 크기로 설정합니다. 연결 속도가 빠르면, 작은 파일의 경우

신속하게 검색할 수 있기 때문에 서버에서 캐시할 필요가 없습니다. 이런 경우 용량이 큰 파일만 캐시합니다. 최대 파일 크기를 설정하면 큰 파일이 프록시의 디스크 공간을 너무 많이 차지하는 것을 방지할 수 있습니다.

최신 여부 확인 정책 설정

최신 여부 확인 정책은 HTTP 문서가 항상 최신 상태를 유지하도록 합니다. 또한 Proxy Server의 새로 고침 간격을 지정할 수 있습니다.

만료 정책 설정

마지막으로 수정된 요소 또는 명시적 만료 정보를 사용하여 만료 정책을 설정할 수 있습니다.

클라이언트 중단 시 캐시 동작 설정

문서가 일부만 검색된 상태에서 클라이언트가 데이터 전송을 중단하는 경우에도 프록시는 캐시를 위해 해당 문서 검색을 마칠 수 있습니다. 프록시의 기본값은 문서의 최소 25%가 이미 검색된 경우 캐시할 문서의 검색을 마치는 것입니다. 25% 미만인 경우 프록시는 원격 서버 연결을 종료하고 검색된 일부 파일을 제거합니다. 클라이언트 중단율을 높이거나 낮출 수 있습니다.

서버에 대한 연결 실패 시 동작

원래 서버에 연결되지 않아 오래된 문서에 대한 최신 여부 확인이 실패하는 경우 프록시가 캐시의 오래된 문서를 전송할지 여부를 지정할 수 있습니다.

로컬 호스트 캐시

로컬 호스트에서 요청된 URL에 도메인 이름이 없는 경우 Proxy Server는 중복 캐시를 방지하기 위해 이 호스트를 캐시하지 않습니다. 예를 들어, 로컬 서버에서 `http://machine/filename.html` 및 `http://machine.example.com/filename.html` 을 요청하는 경우 두 개의 URL이 모두 캐시에 나타납니다. 이러한 파일은 로컬 서버에서 제공되기 때문에 신속하게 검색할 수 있으며, 따라서 캐시할 필요가 없습니다.

그러나 회사의 여러 원격 위치에 서버가 있는 경우 모든 호스트에서 문서를 캐시하여 네트워크 트래픽을 줄이고 파일에 액세스하는 데 필요한 시간을 단축할 수 있습니다.

▼ 로컬 호스트 캐시를 활성화하는 방법

1 **Server Manager에 액세스하고 Caching 탭을 누릅니다.**

2 **Cache Local Hosts 링크를 누릅니다.**
Cache Local Hosts 페이지가 표시됩니다.

3 **드롭다운 목록에서 자원을 선택하거나 Regular Expression 버튼을 눌러 정규 표현식을 입력하고 OK를 누릅니다.**
정규 표현식에 대한 자세한 내용은 16 장, “템플리트 및 자원 관리”을 참조하십시오.

4 **활성화 버튼을 누릅니다.**

5 **OK를 누릅니다.**

6 **Restart Required를 누릅니다.**
Apply Changes 페이지가 표시됩니다.

7 **Restart Proxy Server 버튼을 눌러 변경 사항을 적용합니다.**

파일 캐시 구성

기본적으로 파일 캐시는 사용하도록 설정됩니다. 파일 캐시 설정은 `server.xml` 파일에 포함되어 있습니다. Server Manager를 사용하여 파일 캐시 설정을 변경할 수 있습니다.

주 – Configure File Cache 페이지는 사용자 인터페이스에 표시되지만 이 Proxy Server 4 릴리스에서는 구현되지 않습니다.

▼ 파일 캐시 구성 방법

1 **Server Manager에서 Caching 탭을 누릅니다.**

2 **File Cache Configuration 링크를 누릅니다.**
File Cache Configuration 페이지가 표시됩니다.

3 **아직 선택하지 않은 경우 Enable File Cache를 선택합니다.**

4 **파일을 전송할지 여부를 선택합니다.**
파일 전송을 활성화하면 서버는 파일 내용이 아닌 파일 캐시에서 파일에 대한 열린 파일 설명자를 캐시합니다. `PR_TransmitFile`은 클라이언트에 파일 내용을 전송하는 데 사용됩니다. 파일 전송을 활성화하면 열린 파일 설명자만 캐시되므로 일반적으로 파일 캐시에서 사용하는 소형, 중형 및 대형 파일 등의 구분 방법은 더 이상 적용되지 않습니다. 기본적으로 파일 전송은 Windows에서는 활성화되고 UNIX에서는 비활성화됩니다. UNIX의 경우 HP-UX 및 AIX를 포함하여 OS 자체에서 PR_TransmitFile을 지원하는 플랫폼에서만 파일 전송을 활성화해야 합니다. UNIX/Linux 플랫폼에서는 사용하지 않는 것이 좋습니다.

5 **해시 테이블의 크기를 입력합니다.**

기본 크기는 최대 파일 수의 두 배에 1을 더한 값입니다. 예를 들어, 최대 파일 수가 1024로 설정된 경우 기본 해시 테이블 크기는 2049입니다.

6 **유효한 캐시 항목의 최대 사용 기간(초)을 입력합니다.**

기본 설정은 30입니다. 이 설정에 따라 파일을 캐시한 후에 캐시된 정보를 계속하여 사용하는 시간이 달라집니다. MaxAge 값보다 오래된 항목은 같은 파일이 캐시를 통해 참조되는 경우 같은 파일에 대한 새 항목으로 대체됩니다. 내용을 일정한 간격으로 업데이트할지 여부에 따라 최대 사용 기간을 설정합니다. 예를 들어, 내용이 일정한 간격으로 하루에 네 번 업데이트되는 경우 최대 사용 기간을 21600초(6시간)로 설정할 수 있습니다. 또는 파일이 수정된 후 내용 파일의 이전 버전을 유지할 수 있는 가장 긴 시간으로 최대 사용 기간을 설정할 수도 있습니다.

7 **캐시할 최대 파일 수를 입력합니다.**

기본 설정은 1024입니다.

8 **중간 및 작은 파일 크기 제한(바이트)을 입력합니다.**

Medium File Size Limit는 기본적으로 537600으로 설정됩니다. Small File Size Limit는 기본적으로 2048로 설정됩니다.

캐시는 소형, 중형 및 대형 파일을 서로 다르게 처리합니다. 중간 파일의 내용은 파일을 UNIX/Linux 플랫폼의 가상 메모리에만 매핑하여 캐시합니다. 작은 파일의 내용은 힙 공간을 할당하고 파일을 이 공간으로 읽어 캐시합니다. 큰 파일에 대한 정보는 캐시되지만 파일 내용은 캐시되지 않습니다. 작은 파일과 중간 파일을 구분하면 작은 파일이 많은 경우 가상 메모리의 여러 페이지가 낭비되는 것을 방지할 수 있습니다. 그러므로 작은 파일 크기 제한 값은 일반적으로 VM 페이지 크기보다 약간 작습니다.

9 **중간 및 작은 파일 공간을 설정합니다.**

중간 파일 공간은 모든 중간 크기 파일을 매핑하는데 사용되는 가상 메모리의 크기(바이트)입니다. 이 크기는 기본적으로 10485760으로 설정됩니다. 작은 파일 공간은 작은 파일을 캐시하는 데 사용되는 힙 공간을 포함하여 캐시에 사용되는 힙 공간 크기(바이트)입니다. UNIX/Linux의 경우 이 크기는 기본적으로 1048576입니다.

10 **OK를 누릅니다.**

11 **Restart Required를 누릅니다.**

Apply Changes 페이지가 표시됩니다.

12 **Restart Proxy Server 버튼을 눌러 변경 사항을 적용합니다.**

URL 데이터베이스 보기

액세스 프로토콜과 사이트 이름별로 그룹화 및 기록한 모든 캐시된 URL의 이름과 속성을 볼 수 있습니다. 이 정보에 액세스하면 캐시에서 문서를 만료 및 제거하는 등 다양한 캐시 관리 기능을 수행할 수 있습니다.

▼ 데이터베이스에서 URL 보는 방법

1. **Server Manager에 액세스하고 Caching 탭을 누릅니다.**
2. **View URL Database 링크를 누릅니다.**
   View URL Database 페이지가 표시됩니다.
3. **현재 캐시된 URL 목록을 생성하려면 Regenerate 버튼을 누릅니다.**
4. **(선택 사항) 특정 URL의 정보를 보려면 Search 필드에 URL 또는 정규 표현식을 입력하고 Search 버튼을 누릅니다.**
5. **도메인 이름과 호스트별로 그룹화된 캐시 데이터베이스 정보를 보려면 다음을 수행합니다.**
   a. **목록에서 도메인 이름을 선택합니다.**
      해당 도메인의 호스트 목록이 나타납니다. 나타난 호스트 이름과 URL 목록을 누릅니다.
   b. **URL 이름을 누릅니다.**
      해당 URL에 대한 자세한 정보가 나타납니다.
   c. **해당 URL에 대한 자세한 정보를 보려면 URL 이름을 누릅니다.**

▼ 캐시된 URL을 통해 캐시된 URL을 만료 또는 제거하는 방법

1. **Server Manager에 액세스하고 Caching 탭을 누릅니다.**
2. **View URL Database 링크를 누릅니다.**
   View URL Database 페이지가 표시됩니다.
3. **캐시 데이터베이스의 스냅샷을 생성하려면 Regenerate 버튼을 누릅니다.**
   이 스냅샷은 나머지 단계에 대한 기본 사항을 구성합니다.

4. **만료 또는 제거하려는 특정 URL을 아는 경우 Search 필드에 해당 URL 또는 해당 URL과 일치하는 정규 표현식을 입력하고 Search 버튼을 누릅니다.**

5. **도메인 이름과 호스트별로 그룹화된 URL로 작업하려는 경우 다음을 수행합니다.**

   a. **목록에서 도메인 이름을 선택합니다.**
   해당 도메인의 호스트 목록이 나타납니다.

   b. **나타난 호스트 이름과 URL 목록을 누릅니다.**

6. **개별 파일을 만료하려면 다음을 수행합니다.**

   a. **해당 파일의 URL 옆에 있는 Ex 옵션을 선택합니다.**

   b. **Exp/Rem Marked 버튼을 누릅니다.**

7. **목록에 있는 모든 파일을 만료하려면 양식의 아래쪽에 있는 Exp All 버튼을 누릅니다.**

8. **캐시에서 개별 파일을 제거하려면 다음을 수행합니다.**

   a. **제거할 파일에 대해 URL 옆에 있는 Rm 옵션을 선택합니다.**

   b. **Exp/Rem Marked 버튼을 누릅니다.**

9. **목록에 있는 모든 파일을 제거하려면 Rem All 버튼을 누릅니다.**

10. **스냅샷을 다시 생성하려면 Regenerate 버튼을 누릅니다.**

주 – Ex 또는 Rm 옵션을 사용하는 경우 연결된 파일이 처리되지만 변경 사항은 스냅샷에 반영되지 않습니다. 변경 사항을 표시하려면 스냅샷을 다시 생성해야 합니다.

캐시 일괄 업데이트 사용

파일을 지정된 웹 사이트에 미리 로드하거나 프록시 서버를 사용하지 않을 때마다 캐시에 이미 있는 문서에 대한 최신 여부 확인을 수행할 수 있습니다. URL 배치를 만들고 편집 및 삭제할 수 있으며 일괄 업데이트를 활성화 및 비활성화할 수 있습니다.

일괄 업데이트 만들기

배치에 업데이트할 파일을 지정하여 파일을 능동적으로 캐시할 수 있습니다. 현재 캐시에 있는 여러 파일에 대해 최신 여부 확인을 수행하거나 특정 웹 사이트에 있는 여러 파일을 미리 로드할 수 있습니다.

▼ 일괄 업데이트 만드는 방법

1 **Server Manager에 액세스하고 Caching 탭을 누릅니다.**

2 **Set Cache Batch Updates 링크를 누릅니다.**
Set Cache Batch Updates 페이지가 표시됩니다.

3 **Create/Select a Batch Update Configuration 옆에 있는 드롭다운 목록에서 New 및 Create를 선택합니다.**

4 **OK를 누릅니다. Set Cache Batch Updates 페이지가 표시됩니다.**

5 **Name 섹션에서 새 일괄 업데이트 항목의 이름을 입력합니다.**

6 **페이지의 Source 섹션에서 만들 일괄 업데이트의 유형을 선택합니다.**
캐시의 모든 문서에 대해 최신 여부 확인을 수행하려면 첫 번째 라디오 버튼을 누릅니다. 제공된 소스 URL에서 시작하여 URL을 재귀적으로 캐시하려면 두 번째 라디오 버튼을 누릅니다.

7 **Source 섹션 필드에서 일괄 업데이트에 사용할 문서를 확인합니다.**

8 **Exceptions 섹션의 일괄 업데이트에서 제외할 파일을 확인합니다.**

9 **Resources 섹션에 최대 동시 연결 수 및 최대 이동 문서 수를 입력합니다.**

10 **OK를 누릅니다.**
새롭게 추가된 배치 이름과 Create/Select a Batch Update Configuration 옆에 있는 드롭다운 목록에서 Schedule을 선택합니다.

11 **OK를 누릅니다.**

주 – 일괄 업데이트를 끈 상태에서 일괄 업데이트 구성을 만들고, 편집 및 삭제할 수 있습니다. 그러나 Set Cache Batch Updates 페이지에서 설정한 시간에 따라 일괄 업데이트를 업데이트하려는 경우 업데이트를 사용하도록 설정해야 합니다.

---

12 **Schedule Batch Updates 페이지가 표시됩니다.**

13 **Update On 또는 Update Off 옵션을 선택합니다.**

14 **드롭다운 목록에서 시간을 선택하고 업데이트를 실행할 날짜를 선택합니다.**

15 **OK를 누릅니다.**

16 **Restart Required를 누릅니다.**
Apply Changes 페이지가 표시됩니다.

17 **Restart Proxy Server 버튼을 눌러 변경 사항을 적용합니다.**

일괄 업데이트 구성 편집 또는 삭제

특정 파일을 제외하거나 일괄 업데이트 빈도를 늘리려는 경우 일괄 업데이트를 편집할 수 있습니다. 또한 일괄 업데이트 구성을 완전히 삭제할 수도 있습니다.

▼ 일괄 업데이트 구성을 편집하거나 삭제하는 방법

1 **Server Manager에 액세스하고 Caching 탭을 누릅니다.**

2 **Set Cache Batch Updates 링크를 누릅니다.**
Set Cache Batch Updates 페이지가 표시됩니다.

3 **배치를 편집하려면 해당 배치 이름을 선택하고 Create/Select a Batch Update Configuration 옆에 있는 드롭다운 목록에서 Edit를 선택합니다.**

4 **OK를 누릅니다.**
Set Cache Batch Updates 페이지가 표시됩니다.

5 **원하는 경우 정보를 수정합니다.**

6 **OK를 누릅니다.**

7 **Restart Required를 누릅니다.**
Apply Changes 페이지가 표시됩니다.

8 **Restart Proxy Server 버튼을 눌러 변경 사항을 적용합니다.**

▼ 일괄 업데이트 구성을 삭제하는 방법

1 **Server Manager에 액세스하고 Caching 탭을 누릅니다.**

2 **Set Cache Batch Updates 링크를 누릅니다.**

3 **배치를 삭제하려면 해당 배치 이름을 선택하고 Create/Select a Batch Update Configuration 옆에 있는 드롭다운 목록에서 Delete를 선택합니다.**

4 **OK를 누릅니다.**

5 **Restart Required를 누릅니다.**
Apply Changes 페이지가 표시됩니다.

6 **Restart Proxy Server 버튼을 눌러 변경 사항을 적용합니다.**

캐시 명령줄 인터페이스 사용

프록시 서버는 캐시 디렉토리 구조를 구성, 변경, 생성 및 복구할 수 있는 다양한 명령줄 유틸리티와 함께 제공합니다. 이러한 유틸리티 대부분은 Server Manager 페이지의 기능과 중복됩니다. 예를 들어, cron 작업과 같은 유지 관리를 예약해야 하는 경우 유틸리티를 사용할 수 있습니다. 모든 유틸리티는 `extras` 디렉토리에 있습니다.

▼ 명령줄 유틸리티 실행 방법

1 **명령줄 프롬프트에서** *server_root* `/proxy-server`*id* **디렉토리로 이동합니다.**

2 **`./start -shell`을 입력합니다.**
다음 절에서는 다양한 유틸리티에 대해 설명합니다.

캐시 디렉토리 구조 구축

`cbuild`라고 하는 프록시 유틸리티는 오프라인 캐시 데이터베이스 관리자입니다. 이 유틸리티를 사용하여 새 캐시 구조를 만들거나 명령줄 인터페이스를 사용하여 기존 캐시 구조를 수정할 수 있습니다. Server Manager 페이지를 사용하여 프록시에서 새롭게 만든 캐시를 사용할 수 있습니다.

주 – 유틸리티는 `server.xml` 파일을 업데이트하지 않습니다. `cbuild`는 파티션이 여러 개인 캐시의 크기를 조정할 수 없습니다. `cbuild`에서 캐시를 만들거나 수정하면 `cachecapacity` 매개 변수를 `server.xml` 파일에서 수동으로 업데이트해야 합니다.

```
<PARTITION partitionname="part1" partitiondir="/home/build/install9
/proxy-server1/cache" maxsize="1600" minspace="5" enabled="true"/>
<CACHE enabled="true" cachecapacity="2000" cachedir="/tmp/cache">
```

두 가지 모드로 `cbuild` 유틸리티를 호출할 수 있습니다. 첫 번째 모드는 다음과 같습니다.

```
cbuild -d conf-dir -c cache-dir -s cache size
cbuild -d conf-dir -c cache-dir -s cache size -r
```

예:

```
cbuild -d server_root/proxy-serverid/config
    -c server_root/proxy-serverid/cache -s 512
cbuild -d server_root/proxy-serverid/config
    -c server_root/proxy-serverid/cache -s 512 -r
```

여기서

- *conf-dir*은 *server_root* /proxy-server*id*/config 디렉토리에 있는 프록시 인스턴스의 구성 디렉토리입니다.
- *cache-dir*은 캐시 구조의 디렉토리입니다.
- *cache size*는 캐시가 증가할 수 있는 최대 크기입니다. 이 옵션은 *cache-dim* 매개 변수와 함께 사용할 수 없습니다. 최대 크기는 65135MB입니다.
- -r은 파티션이 한 개인 경우 기존 캐시 구조의 크기를 조정합니다. 새 캐시를 만드는 데에는 필요하지 않습니다.

두 번째 모드는 다음과 같습니다.

```
cbuild -d conf-dir -c cache-dir -n cache-dim
cbuild -d conf-dir -c cache-dir -n cache-dim -r
```

예:

```
cbuild -d server_root/proxy-serverid/config
    -c server_root/proxy-serverid/cache -n 3
cbuild -d server_root/proxy-serverid/config
    -c server_root/proxy-serverid/cache -n 3 -r
```

여기서

- *conf-dir*은 *server_root* /proxy-server*id*/config 디렉토리에 있는 프록시 인스턴스의 구성 디렉토리입니다.
- *cache-dir*은 캐시 구조의 디렉토리입니다.
- *cache-dim*은 섹션 수를 결정합니다. 예를 들어 그림 12–2에서 s3.4로 표시된 섹션의 경우 3은 크기를 나타냅니다. *cache-dim*의 기본값은 0이고 최대값은 8입니다.
- -r은 파티션이 한 개인 경우 기존 캐시 구조의 크기를 조정합니다. 이 옵션은 새 캐시를 만드는 경우 필요하지 않습니다.

캐시 URL 목록 관리

프록시 유틸리티 urldb는 캐시의 URL 목록을 관리합니다. 이 유틸리티를 사용하여 캐시된 URL을 나열할 수 있습니다. 또한 캐시 데이터베이스에서 캐시된 객체를 선택적으로 만료 및 제거할 수 있습니다.

urldb 명령은 -o 옵션을 기준으로 다음 세 개의 그룹으로 분류할 수 있습니다.

- 도메인
- 사이트
- URL

- 도메인을 나열하려면 명령줄에 다음 명령을 입력합니다.

  ```
  urldb -o matching_domains -e reg-exp -d conf-dir
  ```

  예:

  ```
  urldb -o matching_domains -e .*phoenix.* -d server-root/proxy-serverid/config
  ```

  여기서

  - *matching_domains*는 정규 표현식과 일치하는 도메인을 나열합니다.
  - *reg-exp*는 사용된 정규 표현식입니다.
  - *conf-dir*은 *server-root* /proxy-server*id*/config 디렉토리에 있는 프록시 인스턴스의 구성 디렉토리입니다.

- 도메인에서 일치하는 모든 사이트를 나열하려면 명령줄에 다음 명령을 입력합니다.

  ```
  urldb -o matching_sites_in_domain -e reg-exp -m domain_name -d conf-dir
  ```

  예:

  ```
  urldb -o matching_sites_in_domain -e .*atlas -m phoenix.com
      -d server-root/proxy-serverid/config
  ```

  여기서

  - matching_sites_in_domain은 정규 표현식과 일치하는 도메인의 모든 사이트를 나열합니다.
  - *reg-exp*는 사용된 정규 표현식입니다.
  - *domain_name*은 도메인 이름입니다.
  - *conf-dir*은 *server-root* /proxy-server*id*/config 디렉토리에 있는 프록시 인스턴스의 구성 디렉토리입니다.

- 일치하는 모든 사이트를 나열하려면 명령줄에 다음 명령을 입력합니다.

  ```
  urldb -o all_matching_sites -e reg-exp -d conf-dir
  ```

  예:

  ```
  urldb -o all_matching_sites -e .*atlas.* -d server-root/proxy-serverid/config
  ```

  여기서

  - all_matching_sites는 정규 표현식과 일치하는 모든 사이트를 나열합니다.

- *reg-exp*는 사용된 정규 표현식입니다.
- *conf-dir*은 *server-root* /proxy-server*id*/config 디렉토리에 있는 프록시 인스턴스의 구성 디렉토리입니다.

- 사이트에서 일치하는 URL을 나열하려면 명령줄에 다음 명령을 입력합니다.

```
urldb -o matching_urls_from_site -e reg-exp -s site_name -d conf-dir
```

예:

```
urldb -o matching_urls_from_site -e   http://.*atlas.*   -s atlas.phoenix.com
    -d server-root/proxy-serverid/config
```

여기서

- matching_urls_from_site는 정규 표현식과 일치하는 사이트의 모든 URL을 나열합니다.
- *reg-exp*는 사용된 정규 표현식입니다.
- *site_name*은 사이트의 이름입니다.
- *conf-dir*은 *server-root* /proxy-server*id*/config 디렉토리에 있는 프록시 인스턴스의 구성 디렉토리입니다.

- 사이트에서 일치하는 URL을 만료 또는 제거하려면 명령줄에 다음 명령을 입력합니다.

```
urldb -o matching_urls_from_site -e reg-exp -s site_name -x e -d conf-dir
urldb -o matching_urls_from_site -e reg-exp -s site_name -x r -d conf-dir
```

예:

```
urldb -o matching_urls_from_site -e   http://.*atlas.*   -s atlas.phoenix.com
    -x e -d server-root/proxy-serverid/config
```

여기서

- matching_urls_from_site는 정규 표현식과 일치하는 사이트의 모든 URL을 나열합니다.
- *reg-exp*는 사용된 정규 표현식입니다.
- *site_name*은 사이트의 이름입니다.
- -x e는 캐시 데이터베이스에서 일치하는 URL을 만료하기 위한 옵션입니다. 이 옵션은 도메인 및 사이트 모드와 함께 사용할 수 없습니다.
- -x r은 캐시 데이터베이스에서 일치하는 URL을 제거하기 위한 옵션입니다.
- *conf-dir*은 프록시 인스턴스의 구성 디렉토리입니다. *server-root* /proxy-server*id*/config 디렉토리에 있습니다.

- 일치하는 모든 URL을 나열하려면 명령줄에 다음을 입력합니다.

```
urldb -o all_matching_urls -e reg-exp -d conf-dir
```

예:

```
urldb -o all_matching_urls -e   .*cgi-bin.*   -d
    server-root/proxy-serverid/config
```

여기서

- `all_matching_urls`는 정규 표현식과 일치하는 모든 URL을 나열합니다.
- *reg-exp*는 사용된 정규 표현식입니다.
- *conf-dir*은 *server-root* `/proxy-server`*id*`/config` 디렉토리에 있는 프록시 인스턴스의 구성 디렉토리입니다.

- 일치하는 모든 URL을 만료하거나 제거하려면 명령줄에 다음 명령을 입력합니다.

```
urldb -o all_matching_urls -e reg-exp -x e -d conf-dir
urldb -o all_matching_urls -e reg-exp -x r -d conf-dir
```

예:

```
urldb -o all_matching_urls -e   .*cgi-bin.*   -x e -d server-root/proxy-serverid/config
```

여기서

- `all_matching_urls`는 정규 표현식과 일치하는 모든 URL을 나열합니다.
- *reg-exp*는 사용된 정규 표현식입니다.
- `-x e`는 캐시 데이터베이스에서 일치하는 URL을 만료시키기 위한 옵션입니다.
- `-x r`은 캐시 데이터베이스에서 일치하는 URL을 제거하기 위한 옵션입니다.
- *conf-dir*은 *server-root* `/proxy-server`*id*`/config` 디렉토리에 있는 프록시 인스턴스의 구성 디렉토리입니다.

- URL 목록을 만료하거나 제거하려면 명령줄에서 다음 명령을 입력합니다.

```
urldb -l url-list -x e -e reg-exp -d conf-dir
urldb -l url-list -x r -e reg-exp -d conf-dir
```

예:

```
urldb -l url.lst -x e -e   .*cgi-bin.*   -d server-root/proxy-serverid/config
```

여기서

- `url-list`는 만료해야 할 URL 목록입니다. 이 옵션은 URL 목록을 제공하는 데 사용할 수 있습니다.
- `-x e`는 캐시 데이터베이스에서 일치하는 URL을 만료하기 위한 옵션입니다.
- `-x r`은 캐시 데이터베이스에서 일치하는 URL을 제거하기 위한 옵션입니다.

- *reg-exp*는 사용된 정규 표현식입니다.
- *conf-dir*은 *server-root* /proxy-server*id*/config 디렉토리에 있는 프록시 인스턴스의 구성 디렉토리입니다.

캐시 가비지 컬렉션 관리

cachegc 유틸리티를 사용하여 만료되었거나 캐시 크기 제약 조건으로 인해 너무 오래되어 캐시할 수 없는 캐시 데이터베이스에서 객체를 제거할 수 있습니다.

주 – cachegc 유틸리티를 사용하는 경우 CacheGC가 프록시 인스턴스에서 실행되지 않는지 확인합니다.

---

cachegc 유틸리티는 다음과 같은 방법으로 사용할 수 있습니다.

```
cachegc -f leave-fs-full-percent -u gc-high-margin-percent -l gc-low-margin-percent -e
    extra-margin-percent -d conf-dir
```

예:

```
cachegc -f 50 -u 80 -l 60 -e 5 -d server-root/proxy-serverid/config
```

여기서

- *leave-fs-full-percent*는 가비지 컬렉션이 실행되지 않는 캐시 파티션 크기 백분율 한도를 결정합니다.
- *gc-high-margin-percent*는 최대 캐시 크기 백분율을 제어하고 최대값에 도달하는 경우 가비지 컬렉션을 실행합니다.
- *gc-low-margin-percent*는 가비지 컬렉터가 대상으로 하는 최대 캐시 크기의 백분율을 제어합니다.
- *extra-margin-percent*는 가비지 컬렉터가 제거할 캐시 조각을 결정하는 데 사용합니다.
- *conf-dir*은 *server-root* /proxy-server*id*/config 디렉토리에 있는 프록시 인스턴스의 구성 디렉토리입니다.

일괄 업데이트 관리

bu 유틸리티는 캐시를 업데이트하며 두 가지 모드에서 작동합니다. 첫 번째 모드에서는 캐시 데이터베이스를 통해 반복되고 각각에 대해 HTTP 요청을 전송하여 캐시에 있는 모든 URL을 업데이트합니다. 두 번째 모드에서는 제공된 URL로 시작하여 해당 URL의 모든 링크에 대해 지정한 깊이까지 첫 번째 반복을 수행하고 페이지를 캐시로 가져옵니다. bu는 RFC 호환 로봇입니다.

```
bu -n hostname -p port -t time-lmt -f contact-address -s sleep-time -o object -r n -d conf-dir
```

예:

```
bu -n phoenix -p 80 -t 3600 -f admin@phoenix.com -s 60 -o nova -r n
    -d server-root/proxy-serverid/config
```

여기서

- *hostname*은 프록시가 실행되는 시스템의 호스트 이름입니다. 기본값은 localhost입니다.
- *port*는 프록시 서버가 실행되는 포트입니다. 기본 포트는 `8080`입니다.
- *time-lmt*는 유틸리티가 실행되는 시간 제한입니다.
- *contact-address*는 `bu`에서 전송된 HTTP 요청에서 전송되는 연락처 주소를 결정합니다.기본값은 `worm@proxy-name`입니다.
- *sleep-time*은 연속적인 두 요청 사이의 휴면 시간입니다. 기본값은 5초입니다.
- *object*는 현재 실행 중인 `bu.conf`에서 지정된 객체입니다.
- `-r n` 옵션은 `robot.txt` 정책을 수행할지 여부를 결정합니다. 기본값은 `y`입니다.
- *conf-dir*은 *server-root* `/proxy-server`*id*`/config` 디렉토리에 있는 프록시 인스턴스의 구성 디렉토리입니다.

ICP(Internet Cache Protocol) 사용

ICP(Internet Cache Protocol)는 캐시가 서로 통신할 수 있는 객체 위치 프로토콜입니다. 캐시는 ICP를 사용하여 쿼리를 전송하고 캐시된 URL의 존재 및 이러한 URL을 검색하기 위한 최상의 위치 정보에 대해 응답합니다. 일반적인 ICP 교환의 경우 캐시는 특정 URL에 대한 ICP 쿼리를 인접한 모든 캐시에 전송합니다. 그러면 인접한 모든 캐시는 해당 URL을 포함하는지 여부를 표시하는 ICP 응답을 다시 반환합니다. 캐시에 URL이 없는 경우 적중 실패를 전송합니다. 캐시에 URL이 있는 경우 적중을 전송합니다.

ICP 환경을 통한 라우팅

ICP는 서로 다른 관리 도메인에 있는 프록시 간에 통신하는 데 사용할 수 있습니다. 이를 통해 특정 관리 도메인의 프록시 캐시가 다른 관리 도메인의 프록시 캐시와 통신할 수 있습니다. 여러 프록시 서버에서 통신하는 경우에는 효율적이지만 프록시 배열에 있기 때문에 하나의 마스터 프록시에서 모두 구성할 수는 없습니다. 그림 12–3은 서로 다른 관리 도메인에 있는 프록시 간의 ICP 교환을 보여 줍니다.

ICP를 통해 서로 통신하는 프록시를 **이웃***(neighbor)*이라고 합니다. ICP 환경에서 최대 이웃은 64개입니다. ICP 환경에는 두 가지 유형(**상위***(parent)* 및 **동급***(sibling)*)의 이웃이 있습니다. 다른 이웃에 요청된 URL이 없는 경우 상위만 원격 서버에 액세스할 수 있습니다. ICP 환경에 상위가 없거나 둘 이상의 상위가 있을 수 있습니다. ICP 환경에서 상위가 **아닌** 이웃은 동급으로 간주됩니다. 동급이 ICP의 기본 라우팅으로 표시되고 ICP가 기본값을 사용하지 않는 한 동급은 원격 서버에서 문서를 검색할 수 없습니다.

폴링 라운드를 사용하여 이웃이 쿼리를 수신하는 순서를 결정할 수 있습니다. 폴링 라운드는 ICP 쿼리 주기입니다. 각 이웃에 대해 폴링 라운드를 할당해야 합니다. 모든 이웃을 폴링 라운드 1에 있도록 구성하는 경우 모든 이웃이 동시에 한 주기에서 쿼리됩니다. 일부 이웃을 폴링 라운드 2에 포함되도록 구성하는 경우 폴링 라운드 1의 모든 이웃이 먼저 쿼리되고 어떤 이웃에서도 적중을 반환하지 않으면 폴링 라운드 2의 모든 프록시가 쿼리됩니다. 최대 폴링 라운드 수는 2입니다.

ICP 상위가 네트워크 병목 지점이 될 수 있기 때문에 폴링 라운드를 사용하여 부하를 덜 수 있습니다. 일반 설정은 모든 동급을 폴링 라운드 1에 배치하고 모든 상위를 폴링 라운드 2에 배치하도록 구성하는 것입니다. 이런 경우 로컬 프록시가 URL을 요청하면 해당 요청이 환경에 있는 모든 동급으로 먼저 이동합니다. 동급에 요청된 URL이 없는 경우 해당 요청이 상위로 이동합니다. 상위에 URL이 없는 경우 URL이 원격 서버에서 상위를 검색합니다.

ICP 환경의 각 이웃에는 실행 중인 ICP 서버가 하나 이상 있어야 합니다. 이웃에서 ICP 서버를 실행하지 않는 경우 다른 이웃의 ICP 요청에 응답할 수 없습니다. 프록시 서버에서 ICP를 활성화하면 아직 실행되지 않은 경우 ICP 서버를 시작합니다.

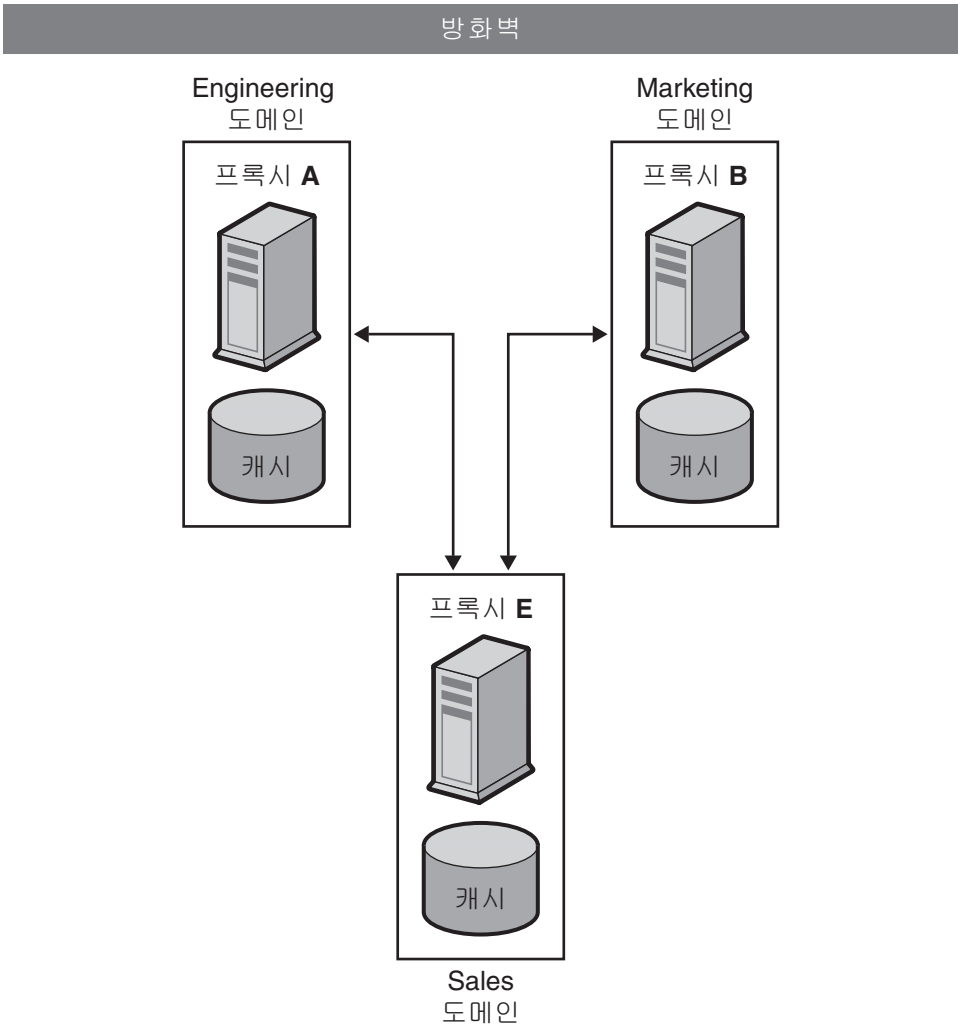

그림 12–3 ICP 교환

ICP 설정

이 절에서는 ICP 설정에 대한 자세한 정보를 제공합니다. ICP 설정에 필요한 일반적인 단계는 다음과 같습니다.

1. (선택 사항) ICP 환경에 상위를 추가합니다.
   자세한 내용은 263 페이지 "ICP 환경에 상위 또는 동급 프록시 추가"을 참조하십시오.
2. ICP 환경에 동급을 추가합니다.
   자세한 내용은 263 페이지 "ICP 환경에 상위 또는 동급 프록시 추가"을 참조하십시오.

3. ICP 환경에서 각 이웃을 구성합니다.
   자세한 내용은 264 페이지 "ICP 환경에서 구성을 편집하는 방법"을 참조하십시오.
4. ICP를 활성화합니다.
   자세한 내용은 266 페이지 "ICP를 활성화하는 방법"을 참조하십시오.
5. 프록시의 ICP 환경에 동급 또는 상위가 있는 경우 ICP 환경을 통한 라우팅을 활성화합니다.
   자세한 내용은 267 페이지 "ICP 환경을 통한 라우팅을 활성화하는 방법"을 참조하십시오.

▼ ICP 환경에 상위 또는 동급 프록시 추가

1 Server Manager에 액세스하고 Caching 탭을 누릅니다.

2 Configure ICP 링크를 누릅니다.
Configure ICP 페이지가 표시됩니다.

3 페이지의 Parent List 섹션에서 Add 버튼을 누릅니다.
ICP Parent 페이지가 표시됩니다.

- 상위 프록시를 추가하려면 페이지의 Parent List 섹션에서 Add를 누릅니다.
  ICP Parent 페이지가 표시됩니다.
- 동급 프록시를 추가하려면 페이지의 Sibling List 섹션에서 Add를 누릅니다.
  ICP Sibling 페이지가 표시됩니다.

4 Machine Address 필드에 ICP 환경에 추가할 프록시의 IP 주소 또는 호스트 이름을 입력합니다.

5 ICP Port 필드에 프록시가 ICP 메시지에 대해 수신할 포트 번호를 입력합니다.

6 (선택 사항) Multicast Address 필드에 상위가 수신할 멀티캐스트 주소를 입력합니다. 멀티캐스트 주소는 여러 서버가 수신할 수 있는 IP 주소입니다.
멀티캐스트 주소를 사용하면 프록시가 해당 멀티캐스트 주소를 수신하는 모든 이웃이 인식할 수 있는 네트워크에 한 개의 쿼리를 전송할 수 있습니다. 이 기법을 사용하면 각 이웃에 개별적으로 쿼리를 전송할 필요가 없습니다. 멀티캐스트 사용은 선택 사항입니다.

주 – 서로 다른 폴링 라운드에 있는 이웃은 동일한 멀티캐스트 주소를 수신할 수 없습니다.

---

7 **TTL 필드에 멀티캐스트 메시지를 전달할 서브넷 수를 입력합니다.**
TTL이 1로 설정된 경우 멀티캐스트 메시지는 로컬 서브넷에만 전달됩니다. TTL이 2인 경우 메시지는 한 레벨을 제외한 모든 서브넷으로 전달됩니다.

주 – 멀티캐스트를 사용하면 관련되지 않은 두 개의 이웃이 서로에게 ICP 메시지를 전송할 수 있습니다. 따라서 관련되지 않은 이웃이 ICP 환경의 프록시로부터 ICP 메시지를 수신하지 않도록 하려면 TTL 필드에 낮은 TTL 값을 설정합니다.

---

8 **Proxy Port 필드에 상위의 프록시 서버에 대한 포트를 입력합니다.**

9 **Polling Round 드롭다운 목록에서 상위가 있어야 할 폴링 라운드를 선택합니다. 기본 폴링 라운드는 1입니다.**

10 **OK를 누릅니다.**

11 **Restart Required를 누릅니다.**
Apply Changes 페이지가 표시됩니다.

12 **Restart Proxy Server 버튼을 눌러 변경 사항을 적용합니다.**

▼ ICP 환경에서 구성을 편집하는 방법

1 **Server Manager에 액세스하고 Caching 탭을 누릅니다.**

2 **Configure ICP 링크를 선택합니다. Configure ICP 페이지가 표시됩니다.**

3 **편집할 프록시 옆에 있는 라디오 버튼을 선택합니다.**

4 **Edit 버튼을 누릅니다.**

5 **해당 정보를 수정합니다.**

6 **OK를 누릅니다.**

7 **Restart Required를 누릅니다.**
Apply Changes 페이지가 표시됩니다.

8 **Restart Proxy Server 버튼을 눌러 변경 사항을 적용합니다.**

▼ ICP 환경에서 프록시를 제거하는 방법

1. **Server Manager에 액세스하고 Caching 탭을 누릅니다.**
2. **Configure ICP 링크를 선택합니다. Configure ICP 페이지가 표시됩니다.**
3. **제거할 프록시 옆에 있는 라디오 버튼을 선택합니다.**
4. **Delete 버튼을 누릅니다.**
5. **Restart Required를 누릅니다.**
   Apply Changes 페이지가 표시됩니다.
6. **Restart Proxy Server 버튼을 눌러 변경 사항을 적용합니다.**

▼ ICP 환경에서 로컬 Proxy Server를 구성하는 방법

ICP 환경에서 각 이웃 또는 로컬 프록시를 구성해야 합니다.

1. **Server Manager에 액세스하고 Caching 탭을 누릅니다.**
2. **Configure ICP 링크를 선택합니다.**
   Configure ICP 페이지가 표시됩니다.
3. **Binding Address 필드에 이웃 서버가 바인드할 IP 주소를 입력합니다.**
4. **Port 필드에 이웃 서버가 ICP에 대해 수신할 포트 번호를 입력합니다.**
5. **Multicast Address 필드에 이웃이 수신할 멀티캐스트 주소를 입력합니다.**
   멀티캐스트 주소는 여러 서버가 수신할 수 있는 IP 주소입니다. 멀티캐스트 주소를 사용하면 프록시가 해당 멀티캐스트 주소를 수신하는 모든 이웃이 인식할 수 있는 네트워크에 한 개의 쿼리를 전송할 수 있습니다. 이 기법을 사용하면 각 이웃에 개별적으로 쿼리를 전송할 필요가 없습니다.

   이웃에 대해 멀티캐스트 주소 및 바인드 주소를 모두 지정한 경우 이웃은 바인드 주소를 사용하여 응답을 전송하고 멀티캐스트를 사용하여 수신합니다. 바인드 주소 또는 멀티캐스트 주소를 지정하지 않은 경우 운영 체제가 데이터를 전송하는 데 사용할 주소를 결정합니다.

6 **인접한 프록시에서 적중으로 응답하지 않는 경우 Default Route 필드에 이웃이 요청을 라우팅할 프록시 이름 또는 IP 주소를 입력합니다.**

이 필드에 단어 "origin"을 입력하거나 필드를 비어두는 경우 기본 라우팅은 원래 서버가 됩니다.

No Hit Behavior 드롭다운 목록에서 "first responding parent"를 선택할 경우 Default Route 필드에 입력한 라우팅이 적용되지 않습니다. 기본 "no hit" 동작을 선택한 경우 프록시는 이 라우팅만 사용합니다.

7 **두 번째 Port 필드에 Default Route 필드에 입력한 기본 라우팅 시스템의 포트 번호를 입력합니다.**

8 **ICP 환경에서 동급의 캐시에 요청된 URL이 없는 경우 On No Hits, Route Through 드롭다운 목록에서 이웃의 동작을 선택합니다.**

사용 가능한 옵션은 다음과 같습니다.

- **first responding parent.** 이웃은 처음에 적중 실패로 응답한 상위를 통해 요청된 URL을 검색합니다.
- **default route**. 이웃은 Default Route 필드에서 지정된 시스템을 통해 요청된 URL을 검색합니다.

9 **Server Count 필드에 ICP 요청을 처리하는 프로세스 수를 입력합니다.**

10 **Timeout 필드에 각 라운드마다 이웃이 ICP 응답을 대기하는 최대 시간을 입력합니다.**

11 **OK를 누릅니다.**

12 **Restart Required를 누릅니다.**

Apply Changes 페이지가 표시됩니다.

13 **Restart Proxy Server 버튼을 눌러 변경 사항을 적용합니다.**

▼ ICP를 활성화하는 방법

1 **Server Manager에 액세스하고 Preferences 탭을 누릅니다.**

2 **Configure System Preferences 링크를 누릅니다.**

Configure System Preferences 페이지가 표시됩니다.

3 **ICP에 대해 Yes 라디오 버튼을 선택하고 OK를 누릅니다.**

4 **Restart Required를 누릅니다.**
Apply Changes 페이지가 표시됩니다.

5 **Restart Proxy Server 버튼을 눌러 변경 사항을 적용합니다.**

▼ ICP 환경을 통한 라우팅을 활성화하는 방법

ICP 환경에서 프록시에 다른 동급 또는 상위가 있는 경우에만 ICP 환경을 통한 라우팅을 활성화해야 합니다. 프록시가 다른 프록시에 대해 상위이고 자체 동급 또는 상위가 없는 경우 해당 프록시에 대해서만 ICP를 활성화해야 합니다. ICP 환경을 통한 라우팅을 활성화할 필요가 없습니다.

1 **Server Manager에 액세스하고 Routing 탭을 누릅니다.**

2 **Set Routing Preferences 링크를 누릅니다.**
Set Routing Preferences 페이지가 표시됩니다.

3 **드롭다운 목록에서 자원을 선택하거나 Regular Expression 버튼을 눌러 정규 표현식을 입력하고 OK를 누릅니다.**

4 **Route Through 옵션 옆에 있는 라디오 버튼을 선택합니다.**

5 **ICP 옆에 있는 확인란을 선택합니다.**

6 **(선택 사항) 클라이언트가 다른 이웃을 통하지 않고 문서가 있는 ICP 이웃에서 문서를 직접 검색할 수 있게 하려면 Text Redirect 옵션 옆에 있는 확인란을 선택합니다.**

7 **OK를 누릅니다.**

주의 – 리디렉션은 현재 클라이언트에서 지원되지 않기 때문에 해당 기능을 사용할 수 없습니다.

8 **Restart Required를 누릅니다.**
Apply Changes 페이지가 표시됩니다.

9 **Restart Proxy Server 버튼을 눌러 변경 사항을 적용합니다.**

프록시 배열 사용

배포된 캐시의 프록시 배열을 사용하여 프록시가 단일 캐시 역할을 수행할 수 있습니다. 배열의 각 프록시에는 브라우저 또는 다운스트림 프록시 서버에서 검색할 수 있는 서로 다른 캐시된 URL이 포함됩니다. 프록시 배열은 여러 프록시 서버에서 자주 발생하는 캐시 중복을 방지합니다. 해시 기반 라우팅을 통해 프록시 배열은 요청을 프록시 배열의 올바른 캐시에 전달합니다.

또한 프록시 배열에서는 증분 확장성을 활성화합니다. 다른 프록시를 프록시 배열에 추가하려는 경우 각 구성원의 캐시가 무효화되지 않습니다. 각 구성원 캐시에서 URL의 1/*n*만 다른 구성원에 다시 지정됩니다. 여기서 *n*은 배열에 있는 프록시 수입니다.

프록시 배열을 통한 라우팅

프록시 배열을 통한 각 요청의 경우 해시 기능으로 배열의 각 프록시에 요청된 URL, 프록시 이름 및 프록시 로드 요소를 기준으로 점수를 지정합니다. 그런 다음 요청은 점수가 가장 높은 프록시로 라우팅됩니다.

URL의 요청은 클라이언트 및 프록시에서 제공될 수 있기 때문에 프록시 배열을 통한 라우팅에는 다음과 같은 두 가지 유형이 있습니다. 클라이언트에서 프록시로의 라우팅 및 프록시에서 프록시로의 라우팅.

클라이언트에서 프록시로의 라우팅에서는 클라이언트가 PAC(Proxy Auto Configuration) 메커니즘을 사용하여 전달될 프록시를 결정합니다. 그러나 표준 PAC 파일을 사용하는 대신 클라이언트는 해시 알고리즘을 계산하는 특수 PAC 파일을 사용하여 요청한 URL에 적합한 라우팅을 결정합니다. 그림 12–4에서는 클라이언트에서 프록시로의 라우팅을 보여줍니다. 이 그림에서 프록시 배열의 각 구성원은 업데이트에 대한 마스터 프록시를 PAT 파일에 로드 및 폴링합니다. 클라이언트에 PAC 파일이 있는 경우 클라이언트는 구성이 변경되면 이 파일만 다시 다운로드해야 합니다. 일반적으로 클라이언트는 다시 시작할 때 PAC 파일을 다운로드합니다.

프록시 서버는 관리 인터페이스를 사용하여 결정한 PAT(Proxy Array Membership Table) 사양에서 특수 PAC 파일을 자동으로 생성할 수 있습니다.

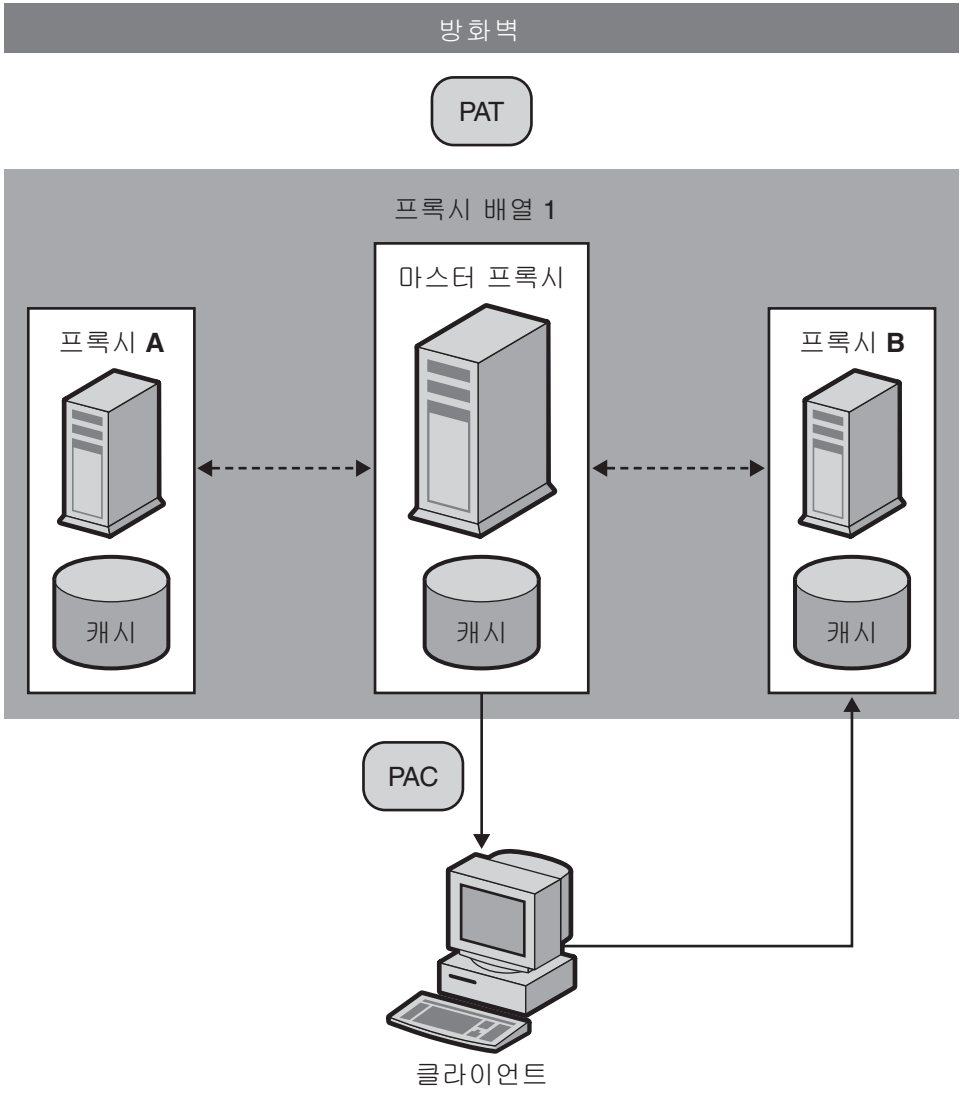

그림 12–4 클라이언트에서 프록시로의 라우팅

프록시에서 프록시로의 라우팅에서 프록시는 PAT(Proxy Array Table) 파일을 사용하여 클라이언트에서 사용되는 PAC 파일 대신 해시 알고리즘을 계산합니다. PAT 파일은 프록시의 시스템 이름, IP 주소, 포트, 로드 요소, 캐시 크기 등을 포함하여 프록시 배열에 대한 정보가 포함된 ASCII 파일입니다. 서버에서 해시 알고리즘을 계산하는 경우 PAT 파일을 사용하면 PAC 파일(런타임 시 해석해야 하는 JavaScript 파일)을 사용하는 것보다

훨씬 효율적입니다. 그러나 대부분의 클라이언트는 PAT 파일 형식을 인식하지 못하기 때문에 PAC 파일을 사용해야 합니다. 그림 12–5에서는 프록시에서 프록시로의 라우팅을 보여 줍니다.

PAT 파일은 프록시 배열의 마스터 프록시에서 만들어집니다. 프록시 관리자는 마스터 프록시가 될 프록시를 결정해야 합니다. 관리자는 이 마스터 프록시 서버에서 PAT 파일을 변경할 수 있습니다. 프록시 배열의 다른 모든 구성원은 이러한 변경 사항에 대해 마스터 프록시를 수동 또는 자동으로 폴링할 수 있습니다. 이러한 변경 사항이 적용된 PAC 파일을 자동으로 생성하도록 각 구성원을 구성할 수 있습니다.

또한 계층적 라우팅을 위해 프록시 배열을 함께 연결할 수 있습니다. 프록시 서버가 업스트림 프록시 배열을 통해 들어 오는 요청을 라우팅하는 경우 업스트림 프록시 배열을 상위 배열이라고 합니다. 즉, 클라이언트가 Proxy X에서 문서를 요청하는 경우 Proxy X에 문서가 없으면 요청을 원격 서버에 직접 전송하는 대신 Proxy Array Y로 전송합니다. 따라서 Proxy Array Y는 상위 배열입니다.

그림 12–5에서 Proxy Array 1은 Proxy Array 2에 대해 상위 배열입니다. Proxy Array 2의 구성원은 상위 배열의 PAT 파일에 대한 업데이트를 로드하고 폴링합니다. 일반적으로 해당 구성원이 상위 배열에서 마스터 프록시를 폴링합니다. 요청된 URL의 해시 알고리즘은 다운로드한 PAT 파일을 사용하여 계산됩니다. 그런 다음 Proxy Array 2의 구성원은 Proxy Array 1 중 점수가 가장 높은 프록시에서 요청된 URL을 검색합니다. 이 그림에서는 Proxy B가 클라이언트에서 요청된 URL에 대해 점수가 가장 높습니다.

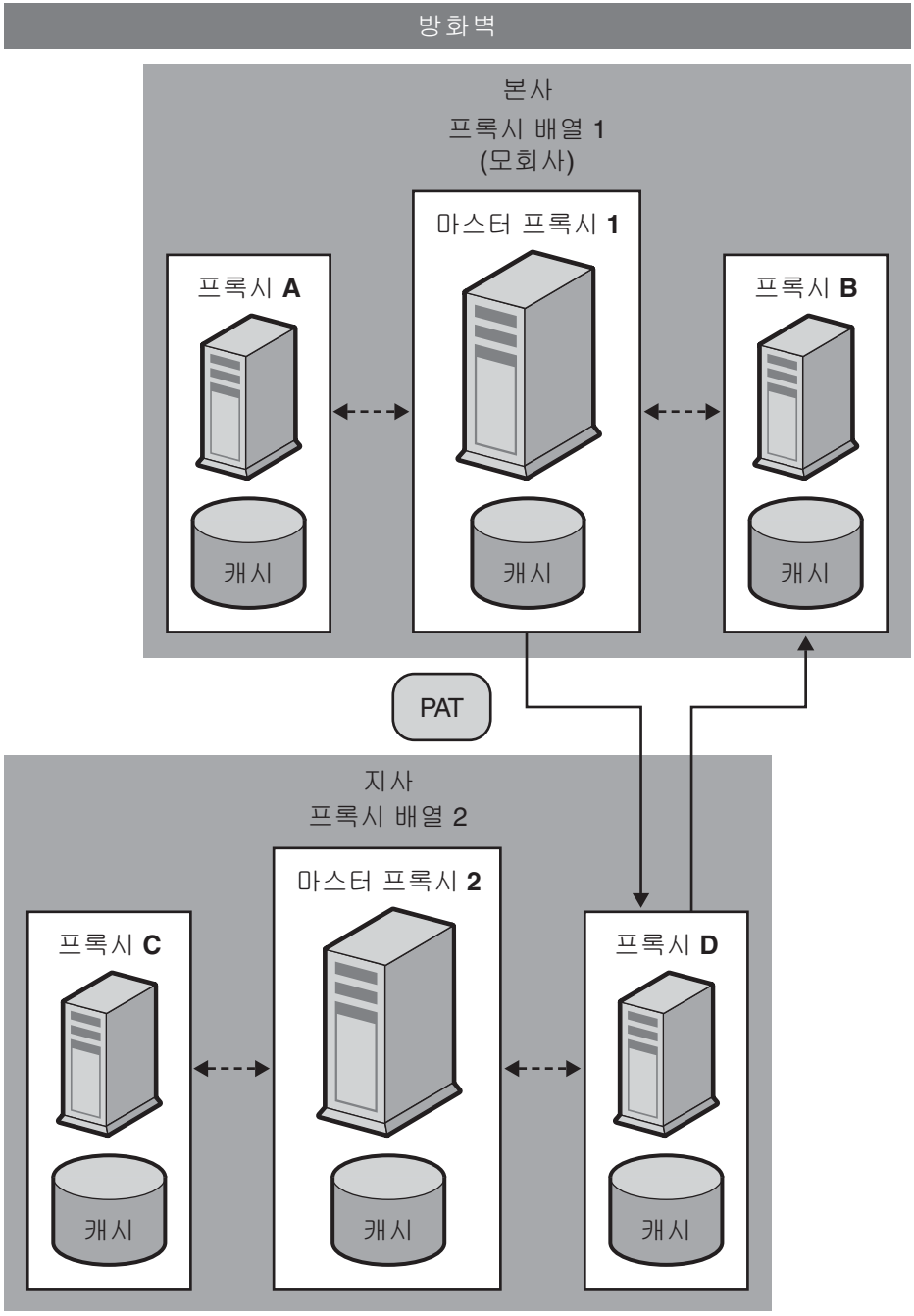

그림 12–5 프록시에서 프록시로의 라우팅

프록시 배열을 설정하는 일반적인 단계는 다음과 같습니다.

마스터 프록시에서 다음 단계를 수행합니다.

1. 프록시 배열을 만듭니다.

   구성원 목록 만들기에 대한 자세한 내용은 272 페이지 "프록시 배열 구성원 목록 만들기"를 참조하십시오.
2. PAT 파일에서 PAC 파일을 생성합니다.

   클라이언트에서 프록시로의 라우팅을 사용하는 경우에만 PAC 파일을 생성해야 합니다. 자세한 내용은 278 페이지 "PAT 파일에서 PAC 파일 생성"을 참조하십시오.
3. 배열의 마스터 구성원을 구성합니다. 자세한 내용은 275 페이지 "프록시 배열 구성원 구성"을 참조하십시오.
4. 프록시 배열을 통한 라우팅을 활성화합니다. 자세한 내용은 276 페이지 "프록시 배열을 통한 라우팅 활성화"를 참조하십시오.
5. URL `/pat`을 PAT 파일에 매핑하도록 PAT 매핑을 만듭니다.
6. 프록시 배열을 활성화합니다.

   자세한 내용은 277 페이지 "프록시 배열 활성화 또는 비활성화"를 참조하십시오.

마스터가 아닌 각 프록시에서 다음 단계를 수행합니다.

1. 배열에서 마스터가 아닌 구성원을 구성합니다.

   자세한 내용은 275 페이지 "프록시 배열 구성원 구성"을 참조하십시오.
2. 프록시 배열을 통한 라우팅을 활성화합니다.

   자세한 내용은 276 페이지 "프록시 배열을 통한 라우팅 활성화"를 참조하십시오.
3. 프록시 배열을 활성화합니다.

   자세한 내용은 277 페이지 "프록시 배열 활성화 또는 비활성화"를 참조하십시오.

주 – 프록시 배열이 상위 배열을 통해 라우팅되는 경우에도 상위 배열을 활성화하고 각 구성원이 원하는 URL에 대해 상위 배열을 통해 라우팅되도록 구성해야 합니다. 자세한 내용은 280 페이지 "상위 배열을 통한 라우팅"을 참조하십시오.

프록시 배열 구성원 목록 만들기

배열의 마스터 프록시에서만 프록시 배열 구성원을 만들고 업데이트해야 합니다. 프록시 배열 구성원 목록은 한 번만 만들면 되지만 언제라도 수정할 수 있습니다. 프록시 배열 구성원 목록을 만들어 배열의 모든 프록시와 다운스트림 프록시에 배포할 PAT 파일을 생성합니다.

주 – 배열의 마스터 프록시를 통해서만 프록시 배열 구성원 목록을 변경하거나 추가해야 합니다. 배열의 다른 모든 구성원은 구성원 목록을 읽을 수만 있습니다.

▼ 프록시 배열 구성원 목록을 만드는 방법

1. **Server Manager에 액세스하고 Caching 탭을 누릅니다.**
2. **Configure Proxy Array 링크를 누릅니다.**
   Configure Proxy Array 페이지가 표시됩니다.
3. **Array name 필드에 배열 이름을 입력합니다.**
4. **Reload Configuration Every 필드에 PAT 파일의 각 폴링 간격(분)을 입력합니다.**
5. **Array Enabled 확인란을 누릅니다.**
6. **Create 버튼을 누릅니다.**
   Create 버튼은 프록시 배열이 만들어진 후 OK 버튼으로 변경됩니다.

주 – 구성원을 구성원 목록에 추가하기 전에 OK를 눌러야 합니다.

7. **OK를 누릅니다.**
8. **Restart Required를 누릅니다.**
   Apply Changes 페이지가 표시됩니다.
9. **프록시 배열의 각 구성원에 대해 다음을 제공한 다음 OK를 누릅니다.**
   먼저 마스터 구성원을 추가한 다음 다른 구성원을 추가해야 합니다.
   - **Name.** 구성원 목록에 추가할 프록시 서버 이름
   - **IP Address.** 구성원 목록에 추가할 프록시의 서버의 IP 주소
   - **Port.** PAT 파일에 대해 구성원이 폴링하는 포트입니다.
   - **Load Factor.** 구성원을 통해 라우팅해야 하는 상대적 부하를 반영하는 정수.
   - **Status.** 구성원 상태. 이 값은 On 또는 Off일 수 있습니다. 프록시 배열 구성원을 비활성화할 경우 구성원의 요청이 다른 구성원을 통해 다시 라우팅됩니다.

주 – 추가할 각 프록시 배열 구성원에 대해 정보를 입력한 후 OK를 눌러야 합니다.

10 **Restart Required를 누릅니다.**
Apply Changes 페이지가 표시됩니다.

11 **Restart Proxy Server 버튼을 눌러 변경 사항을 적용합니다.**

프록시 배열 구성원 목록 정보 편집

언제라도 프록시 배열 구성원 목록의 구성원에 대한 정보를 변경할 수 있습니다. 마스터 프록시에서만 프록시 배열 구성원 목록을 편집할 수 있습니다.

주 – 배열의 마스터 프록시를 통해서만 프록시 배열 구성원 목록을 변경하거나 추가해야 합니다. 배열의 다른 구성원에서 이 목록을 수정하면 모든 변경 사항이 손실됩니다.

▼ 구성원 목록 정보를 편집하는 방법

1 **Server Manager에 액세스하고 Caching 탭을 누릅니다.**

2 **Configure Proxy Array 링크를 누릅니다.**
Configure Proxy Array 페이지가 표시됩니다.

3 **Member List에서 편집할 구성원 옆에 있는 라디오 버튼을 선택합니다.**

4 **Edit 버튼을 누릅니다.**
Configure Proxy Array Member 페이지가 표시됩니다.

5 **해당 정보를 편집합니다.**

6 **OK를 누릅니다.**

7 **Restart Required를 누릅니다.**
Apply Changes 페이지가 표시됩니다.

8 **Restart Proxy Server 버튼을 눌러 변경 사항을 적용합니다.**

주 – 변경 사항을 적용하고 프록시 배열의 구성원에게 배포하려는 경우 Configure Proxy Array 페이지에서 Configuration ID를 업데이트하고 OK를 누릅니다. Configuration ID에 1을 더하면 업데이트됩니다.

프록시 배열 구성원 삭제

프록시 배열 구성원을 삭제하면 프록시 배열에서 제거됩니다. 마스터 프록시에서만 프록시 배열 구성원을 삭제할 수 있습니다.

▼ 프록시 배열의 구성원을 삭제하는 방법

1. **Server Manager에 액세스하고 Caching 탭을 누릅니다.**
2. **Configure Proxy Array 링크를 누릅니다.**
   Configure Proxy Array 페이지가 표시됩니다.
3. **Member List에서 삭제할 구성원 옆에 있는 라디오 버튼을 선택합니다.**
4. **Delete 버튼을 누릅니다.**

주 – 변경 사항을 적용하고 프록시 배열의 구성원에게 배포하려는 경우 Configure Proxy Array 페이지에서 Configuration ID를 업데이트하고 OK를 누릅니다. Configuration ID에 1을 더하면 업데이트됩니다.

---

5. **Restart Required를 누릅니다.**
   Apply Changes 페이지가 표시됩니다.
6. **Restart Proxy Server 버튼을 눌러 변경 사항을 적용합니다.**

프록시 배열 구성원 구성

구성원에서 프록시 배열의 각 구성원을 한 번만 구성해야 합니다. 다른 구성원에서 배열의 구성원을 구성할 수 없습니다. 또한 마스터 프록시를 구성해야 합니다.

▼ 프록시 배열의 각 구성원을 구성하는 방법

1. **Server Manager에 액세스하고 Caching 탭을 누릅니다.**
2. **Configure Proxy Array Member 링크를 누릅니다.**
   Configure Proxy Array Member 페이지가 표시됩니다.
3. **Proxy Array 섹션에서 해당 라디오 버튼을 선택하여 PAT 파일에 대해 구성원이 폴링해야 하는지 여부를 표시합니다.**

- **Non-Master Member.** 구성하는 구성원이 마스터 프록시가 **아닌** 경우 이 옵션을 선택합니다. 마스터 프록시가 아닌 프록시 배열 구성원은 마스터 프록시에서 검색하기 위해 PAT 파일에 대해 폴링해야 합니다.
- **Master Member.** 마스터 프록시를 구성하는 경우 이 옵션을 선택합니다. 마스터 프록시를 구성하는 경우 PAT 파일은 로컬이며 폴링할 필요가 없습니다.

4 **Poll Host 필드에 PAT 파일에 대해 폴링할 마스터 프록시 이름을 입력합니다.**

5 **Port 필드에 마스터 프록시가 HTTP 요청을 수락하는 포트를 입력합니다.**

6 **URL 필드에 마스터 프록시의 PAT 파일에 대한 URL을 입력합니다. PAT 파일을 URL** `/pat` **에 매핑하기 위해 마스터 프록시에서 PAT 매핑을 만든 경우 URL 필드에** `/pat` **를 입력해야 합니다.**

7 **(선택 사항) Headers File 필드에 인증 정보와 같이 PAT 파일의 HTTP 요청을 전송해야 하는 특수 헤더와 함께 파일의 전체 경로 이름을 입력합니다.**

8 **OK를 누릅니다.**

9 **Restart Required를 누릅니다.**
Apply Changes 페이지가 표시됩니다.

10 **Restart Proxy Server 버튼을 눌러 변경 사항을 적용합니다.**

프록시 배열을 통한 라우팅 활성화

▼ 프록시 배열을 통한 라우팅을 활성화하는 방법

1 **Server Manager에 액세스하고 Routing 탭을 누릅니다.**

2 **Set Routing Preferences 링크를 누릅니다.**
Set Routing Preferences 페이지가 표시됩니다.

3 **드롭다운 목록에서 자원을 선택하거나 Regular Expression 버튼을 눌러 정규 표현식을 입력하고 OK를 누릅니다.**

4 **Route Through 옵션을 선택합니다.**

5 **프록시 배열 또는 상위 배열의 확인란을 선택합니다.**

구성하는 프록시 서버가 프록시 배열의 구성원인 경우에만 프록시 배열 라우팅을 활성화할 수 있습니다. 상위 배열이 있는 경우에만 상위 라우팅을 활성화할 수 있습니다. 두 옵션은 서로 독립적입니다.

6 **프록시 배열을 통한 라우팅을 선택하고 요청을 다른 URL로 리디렉션하려면 리디렉션 확인란을 선택합니다.**

리디렉션은 프록시 배열의 구성원이 처리하지 않아야 하는 요청을 받은 경우 클라이언트에게 해당 요청에 대해 연결할 프록시를 알려 주는 기능입니다.

7 **OK를 누릅니다.**

8 **Restart Required를 누릅니다.**

Apply Changes 페이지가 표시됩니다.

9 **Restart Proxy Server 버튼을 눌러 변경 사항을 적용합니다.**

프록시 배열 활성화 또는 비활성화

프록시 배열을 통해 라우팅되지 않는 경우 프록시 배열 옵션을 비활성화하기 전에 모든 클라이언트가 특수 PAC 파일을 사용하여 올바르게 라우팅되는지 확인해야 합니다. 상위 배열 옵션을 비활성화하는 경우 명시적 프록시 또는 직접 연결과 같이 Set Routing Preferences 페이지에서 유효한 대체 라우팅 옵션을 설정해야 합니다.

▼ 프록시 배열을 활성화 또는 비활성화하는 방법

1 **Server Manager에 액세스하고 Preferences 탭을 누릅니다.**

2 **Configure System Preferences 링크를 누릅니다.**

Configure System Preferences 페이지가 표시됩니다.

3 **프록시 배열을 활성화하거나 비활성화합니다.**

- 프록시 배열을 활성화하려면 활성화할 배열의 유형에 대해 Yes 옵션을 누릅니다. 일반 프록시 배열 또는 상위 배열.
- 프록시 배열을 비활성화하려면 No를 누릅니다.

4 **OK를 누릅니다.**

5 **Restart Required를 누릅니다.**

Apply Changes 페이지가 표시됩니다.

6 **Restart Proxy Server 버튼을 눌러 변경 사항을 적용합니다.**

프록시 배열의 요청 리디렉션

프록시 배열을 통한 라우팅을 선택한 경우 요청을 다른 URL로 리디렉션할지 여부를 지정해야 합니다. 리디렉션은 프록시 배열의 구성원이 처리하지 않아야 하는 요청을 받은 경우 클라이언트에게 해당 요청에 대해 연결할 프록시를 알려 주는 기능입니다.

PAT 파일에서 PAC 파일 생성

대부분의 클라이언트는 PAT 파일 형식을 인식하지 못하기 때문에 클라이언트에서 프록시로의 라우팅 시 클라이언트는 PAC(Proxy Auto Configuration) 메커니즘을 사용하여 수행할 프록시에 대한 정보를 수신합니다. 그러나 클라이언트는 표준 PAC 파일 대신 PAT 파일에서 파생된 특수 PAC 파일을 사용합니다. 이 특수 PAC 파일은 해시 알고리즘을 계산하여 요청된 URL에 대해 적절한 라우팅을 결정합니다.

PAT 파일에서 PAC 파일을 수동 또는 자동으로 생성할 수 있습니다. 프록시 배열의 특정 구성원에서 PAC 파일을 수동으로 생성하는 경우 해당 구성원은 PAT 파일에 현재 있는 정보를 기준으로 PAC 파일을 즉시 다시 생성합니다. PAC 파일을 자동으로 생성하도록 프록시 배열 구성원을 구성하는 경우 수정된 버전의 PAT 파일을 감지할 때마다 구성원은 자동으로 파일을 다시 생성합니다.

주 – 프록시 서버의 프록시 배열 기능을 사용하지 않는 경우 Create/Edit Autoconfiguration File 페이지를 사용하여 PAC 파일을 생성합니다. 자세한 내용은 17 장, “클라이언트 자동 구성 파일 사용”을 참조하십시오.

▼ PAT 파일에서 PAC 파일을 수동으로 생성하는 방법

PAC 파일은 마스터 프록시에서만 생성할 수 있습니다.

1 **마스터 프록시의 Server Manager에 액세스하고 Caching 탭을 누릅니다.**

2 **Configure Proxy Array 링크를 누릅니다.**

Configure Proxy Array 페이지가 표시됩니다.

3 **Generate PAC 버튼을 누릅니다.**

PAC Generation 페이지가 표시됩니다.

4 **PAC 파일에서 사용자 정의 로직을 사용하려는 경우 Custom logic file 필드에 PAC 파일 생성 시 포함할 사용자 정의된 로직이 포함된 파일 이름을 입력합니다.**

이 로직은 `FindProxyForURL` 함수에서 프록시 배열 선택 로직 앞에 삽입됩니다. 이 함수는 일반적으로 프록시 배열을 통과하지 않아야 할 로컬 요청에 사용됩니다.

프록시 배열 구성원을 구성할 때 이미 사용자 정의 로직 파일을 제공한 경우 이 필드는 해당 정보로 채워집니다. 여기서 사용자 정의 로직 파일을 편집할 수 있습니다.

5 **배열의 프록시를 사용할 수 없는 경우 Default Route 필드에 클라이언트가 이동해야 할 라우팅을 입력합니다.**
프록시 배열 구성원을 구성할 때 이미 기본 라우팅을 제공한 경우 이 필드는 해당 정보로 채워집니다. 여기서 기본 라우팅을 편집할 수 있습니다.

6 **OK를 누릅니다.**

7 **Restart Required를 누릅니다.**
Apply Changes 페이지가 표시됩니다.

8 **Restart Proxy Server 버튼을 눌러 변경 사항을 적용합니다.**

▼ PAC 파일을 자동으로 생성하는 방법

1 **Server Manager에 액세스하고 Caching 탭을 누릅니다.**

2 **Configure Proxy Array Member 링크를 누릅니다.**
Configure Proxy Array Member 페이지가 표시됩니다.

3 **Auto-generate PAC File 확인란을 선택합니다.**

4 **PAC 파일에서 사용자 정의 로직을 사용하려는 경우 Custom Logic File 필드에 PAC 파일 생성 시 포함할 사용자 정의된 로직이 포함된 파일 이름을 입력합니다.**
이 로직은 `FindProxyFor URL` 함수에서 프록시 배열 선택 로직 앞에 삽입됩니다.

프록시 배열을 구성할 때 이미 사용자 정의 로직 파일을 제공하고 저장한 경우 이 필드는 해당 정보로 채워집니다. 여기서 사용자 정의 로직 파일을 편집할 수 있습니다.

5 **배열의 프록시를 사용할 수 없는 경우 Default Route 필드에 클라이언트가 이동해야 할 라우팅을 입력합니다.**
프록시 배열을 구성할 때 이미 기본 라우팅을 제공한 경우 이 필드는 해당 정보로 채워집니다. 기본 라우팅을 편집할 수 있습니다.

6 **OK를 누릅니다.**

7 **Restart Required를 누릅니다.**
Apply Changes 페이지가 표시됩니다.

8 **Restart Proxy Server 버튼을 눌러 변경 사항을 적용합니다.**

상위 배열을 통한 라우팅

원격 서버로 직접 이동하는 대신 업스트림 상위 배열을 통해 라우팅되도록 프록시 또는 프록시 배열 구성원을 구성할 수 있습니다.

▼ 상위 배열을 통해 라우팅하는 방법

1. **상위 배열을 활성화합니다.**
   자세한 내용은 277 페이지 "프록시 배열 활성화 또는 비활성화"를 참조하십시오.

2. **상위 배열을 통한 라우팅을 활성화합니다.**
   자세한 내용은 276 페이지 "프록시 배열을 통한 라우팅 활성화"를 참조하십시오.

3. **Server Manager에 액세스하고 Caching 탭을 누릅니다.**

4. **Configure Proxy Array Member 링크를 누릅니다.**
   Configure Proxy Array Member 페이지가 표시됩니다.

5. **페이지의 Parent Array 섹션에 있는 Poll Host 필드에 PAT 파일에 대해 폴링할 상위 배열에 있는 프록시의 호스트 이름을 입력합니다.**
   이 프록시는 일반적으로 상위 배열의 마스터 프록시입니다.

6. **페이지의 Parent Array 섹션에 있는 Port 필드에 PAT 파일에 대해 폴링할 상위 배열에 있는 프록시의 포트 번호를 입력합니다.**

7. **URL 필드에 마스터 프록시의 PAT 파일에 대한 URL을 입력합니다.**
   마스터 프록시에서 PAT 매핑을 만든 경우 이 URL 필드에 대한 매핑을 입력합니다.

8. **(선택 사항) 양식의 Parent Array 섹션에 있는 Headers File 필드에 인증 정보와 같이 PAT 파일의 HTTP 요청에 따라 전송해야 하는 특수 헤더를 포함하여 파일의 전체 경로 이름을 입력합니다.**
   이 필드는 선택 사항입니다.

9. **OK를 누릅니다.**

10. **Restart Required를 누릅니다.**
    Apply Changes 페이지가 표시됩니다.

11. **Restart Proxy Server 버튼을 눌러 변경 사항을 적용합니다.**

상위 배열 정보 보기

프록시 배열이 상위 배열을 통해 라우팅되는 경우 상위 배열의 구성원에 대한 정보가 필요합니다. 이 정보는 PAT 파일 양식의 상위 배열에서 전송됩니다.

▼ 상위 배열 정보를 보는 방법

1. **Server Manager에 액세스하고 Caching 탭을 누릅니다.**
2. **View Parent Array Configuration 링크를 누릅니다.**
   View Parent Array Configuration 페이지가 표시됩니다.
3. **정보를 봅니다.**

◆ ◆ ◆ 13장

13 프록시를 통한 컨텐트 필터링

이 장에서는 프록시 서버가 URL에 대한 액세스를 허용하지 않거나 클라이언트에 반환되는 HTML 및 JavaScript 컨텐트를 수정하도록 URL을 필터링하는 방법에 대해 설명합니다. 또한 클라이언트가 사용하는 웹 브라우저(사용자 에이전트)를 기반으로 프록시를 통해 액세스를 제한할 수 있는 방법에 대해 설명합니다.

URL 필터를 사용하여 서버가 지원하는 URL을 결정할 수 있습니다. 예를 들어, 지원할 URL의 와일드카드 패턴을 수동으로 입력하는 대신 제한하려는 URL이 포함된 텍스트 파일 하나를 만들거나 구입할 수 있습니다. 이 기능을 사용하여 다양한 프록시 서버에서 사용할 수 있는 단일 URL 파일을 만들 수 있습니다.

또한 MIME 유형을 기반으로 URL을 필터링할 수 있습니다. 예를 들어, 프록시를 통해 HTML 및 GIF 파일을 캐시하고 전송할 수 있지만 컴퓨터 바이러스 위험이 있는 이진 파일이나 실행 파일을 가져오지 못하게 할 수 있습니다.

이 장은 다음 내용으로 구성되어 있습니다.

- 284 페이지 “URL 필터링”
- 286 페이지 “컨텐트 URL 다시 작성”
- 287 페이지 “특정 웹 브라우저에 대한 액세스 제한”
- 288 페이지 “요청 차단”
- 289 페이지 “전송 헤더 억제”
- 290 페이지 “MIME 유형별 필터링”
- 291 페이지 “HTML 태그별 필터링”
- 292 페이지 “컨텐트 압축용으로 서버 구성”

URL 필터링

URL 파일을 사용하여 프록시 서버가 검색하는 컨텐트를 구성할 수 있습니다. 프록시가 항상 지원하는 URL 목록과 프록시가 지원하지 않는 URL 목록을 설정할 수 있습니다.

예를 들어, 어린이에게 적합한 컨텐트를 제공하는 프록시 서버를 실행하는 인터넷 서비스 제공자는 어린이가 볼 수 있도록 승인된 URL 목록을 설정할 수 있습니다. 그런 다음 프록시 서버가 승인된 URL만 검색하도록 할 수 있습니다. 클라이언트가 지원되지 않는 URL로 이동하려는 경우 프록시가 기본 "Forbidden" 메시지를 반환하게 하거나 클라이언트가 해당 URL에 액세스할 수 없는 이유를 설명하는 사용자 정의 메시지를 만들 수 있습니다.

URL을 기반으로 액세스를 제한하려면 허용하거나 제한할 URL 파일을 만듭니다. Server Manager를 통해 이 작업을 수행할 수 있습니다. 파일이 만들어지면 제한을 설정할 수 있습니다. 다음 절에서 이러한 절차에 대해 설명합니다.

URL 필터 파일 만들기

필터 파일은 URL 목록이 포함된 파일입니다. 프록시 서버가 사용하는 필터 파일은 다음 패턴의 URL 행이 있는 일반 텍스트 파일입니다.

```
protocol://host:port/path/filename
```

다음 세 가지 섹션 모두에서 정규 표현식을 사용할 수 있습니다. `protocol`, `host:port` 및 `path/filename`. 예를 들어, `netscape.com` 도메인으로 이동하는 모든 프로토콜에 대해 URL 패턴을 만드는 경우 해당 파일에 다음 행이 있어야 합니다.

```
.*://.*\\.example\\.com/.*
```

이 행은 포트 번호를 지정하지 않은 경우에만 작동합니다. 정규 표현식에 대한 자세한 내용은 16 장, "템플리트 및 자원 관리"의 "정규 표현식 이해"를 참조하십시오.

Server Manager를 사용하지 않고 고유한 파일을 만드는 경우 Server Manager 페이지를 사용하여 빈 파일을 만든 다음 해당 파일에 텍스트를 추가하거나 파일을 정규 표현식을 포함하는 파일로 바꿉니다.

▼ 필터 파일 만드는 방법

1. **Server Manager에 액세스하고 Filters 탭을 누릅니다.**
2. **Restrict URL Filter Access 링크를 누릅니다.**
   Restrict URL Filter Access 페이지가 표시됩니다.
3. **Create/Edit 버튼 옆에 있는 드롭다운 목록에서 New Filter를 선택합니다.**

4. **드롭다운 목록 오른쪽에 있는 입력란에 필터 파일 이름을 입력한 다음 Create/Edit 버튼을 누릅니다.**

   Filter Editor 페이지가 표시됩니다.

5. **Filter Content 스크롤 가능 입력란을 사용하여 URL 및 URL의 정규 표현식을 입력합니다.**

   Reset 버튼을 누르면 이 필드의 모든 텍스트가 삭제됩니다.

   정규 표현식에 대한 자세한 내용은 16 장, “템플리트 및 자원 관리”의 "정규 표현식 이해"를 참조하십시오.

6. **OK를 누릅니다.**

   프록시 서버가 파일을 만들어 Restrict URL Filter Access 페이지에 반환합니다. 필터 파일은 `proxy-server`*id*`/conf_bk` 디렉토리에서 만들어집니다.

필터 파일에 대한 기본 액세스 설정

사용할 URL이 포함된 필터 파일이 있는 경우 이러한 URL에 대해 기본 액세스를 설정할 수 있습니다.

▼ 필터 파일에 대해 기본 액세스 설정 방법

1. **Server Manager에 액세스하고 Filters 탭을 누릅니다.**

2. **Restrict URL Filter Access 링크를 누릅니다.**

   Restrict URL Filter Access 페이지가 표시됩니다.

3. **필터와 사용할 템플리트를 선택합니다.**

   일반적으로 전체 프록시 서버에 대한 필터 파일을 만들지만 HTTP에 대한 필터 파일 집합과 FTP에 대한 필터 파일 집합을 구분할 수도 있습니다.

4. **URL Filter To Allow 목록을 사용하여 프록시 서버가 지원할 URL이 포함된 필터 파일을 선택합니다.**

5. **URL Filter To Deny 목록을 사용하여 프록시 서버에서 액세스를 거부할 URL이 포함된 필터 파일을 선택합니다.**

6. **프록시 서버에서 거부된 URL을 요청한 클라이언트에 반환할 텍스트를 선택합니다.**

   - 프록시가 생성하는 기본 "Forbidden" 응답을 보냅니다.
   - 텍스트 또는 사용자 정의된 텍스트가 있는 HTML 파일을 보냅니다. 이 파일에 대한 절대 경로를 입력란에 입력합니다.

7. **OK를 누릅니다.**

8 **Restart Required를 누릅니다. Apply Changes 페이지가 표시됩니다.**

9 **Restart Proxy Server 버튼을 눌러 변경 사항을 적용합니다.**

컨텐트 URL 다시 작성

Proxy Server는 클라이언트로 반환되는 컨텐트를 조사하여 URL과 같은 패턴을 다른 문자열로 바꿀 수 있습니다. 다음과 같은 두 가지 매개 변수를 구성할 수 있습니다. 소스 문자열 및 대상 문자열. Proxy Server는 소스 문자열과 일치하는 텍스트를 찾아 대상 문자열에 있는 텍스트로 대체합니다. 이 기능은 역방향 프록시 모드에서만 작동합니다.

▼ URL 다시 작성 패턴을 만드는 방법

1 **Server Manager에 액세스하고 Filters 탭을 누릅니다.**

2 **Set Content URL Rewriting 링크를 누릅니다.**
Set Content URL Rewriting 페이지가 표시됩니다.

3 **드롭다운 목록에서 자원을 선택하거나 정규 표현식을 지정합니다.**
정규 표현식에 대한 자세한 내용은 16 장, “템플리트 및 자원 관리”의 "정규 표현식 이해"를 참조하십시오.

4 **Source Pattern 입력란에 소스 문자열을 지정합니다.**

5 **Destination Pattern 입력란에 대상 문자열을 지정합니다.**

6 **MIME Pattern 입력란에 컨텐트 유형을 지정합니다.**

7 **OK를 누릅니다.**

8 **Restart Required를 누릅니다.**
Apply Changes 페이지가 표시됩니다.

9 **Restart Proxy Server 버튼을 눌러 변경 사항을 적용합니다.**

▼ URL 다시 작성 패턴 편집 방법

1. **Server Manager에 액세스하고 Filters 탭을 누릅니다.**
2. **Set Content URL Rewriting 링크를 누릅니다.**
   Set Content URL Rewriting 페이지가 표시됩니다.
3. **편집할 URL 다시 작성 패턴 옆에 있는 Edit 링크를 누릅니다.**
4. **OK를 누릅니다.**
5. **Restart Required를 누릅니다.**
   Apply Changes 페이지가 표시됩니다.
6. **Restart Proxy Server 버튼을 눌러 변경 사항을 적용합니다.**

▼ URL 다시 작성 패턴 삭제 방법

1. **Server Manager에 액세스하고 Filters 탭을 누릅니다.**
2. **Set Content URL Rewriting 링크를 누릅니다.**
   Set Content URL Rewriting 페이지가 표시됩니다.
3. **삭제할 URL 다시 작성 패턴 옆에 있는 Remove 링크를 누릅니다.**
   OK를 눌러 삭제를 확인합니다.
4. **Restart Required를 누릅니다.**
   Apply Changes 페이지가 표시됩니다.
5. **Restart Proxy Server 버튼을 눌러 변경 사항을 적용합니다.**

특정 웹 브라우저에 대한 액세스 제한

클라이언트의 웹 브라우저 유형 및 버전을 기반으로 프록시 서버에 대한 액세스를 제한할 수 있습니다. 요청 시 모든 웹 브라우저가 서버에 전송하는 사용자 에이전트 헤더를 기반으로 제한이 수행됩니다.

▼ 클라이언트의 웹 브라우저를 기준으로 프록시에 대한 액세스 제한 방법

1. **Server Manager에 액세스하고 Filters 탭을 누릅니다.**
2. **Set User-Agent Restriction 링크를 누릅니다.**
   Set User-Agent Restriction 페이지가 표시됩니다.
3. **드롭다운 목록에서 자원을 선택하거나 Proxy Server가 지원할 브라우저에 대해 사용자 에이전트 문자열과 일치하는 정규 표현식을 입력합니다.**
   둘 이상의 클라이언트를 지정하려는 경우 정규 표현식을 괄호로 묶고 | 문자를 사용하여 여러 항목을 구분합니다. 정규 표현식에 대한 자세한 내용은 16 장, “템플리트 및 자원 관리”의 "정규 표현식 이해"를 참조하십시오.
4. **Allow Only User-Agents Matching 옵션을 선택합니다.**
5. **OK를 누릅니다.**
6. **Restart Required를 누릅니다.**
   Apply Changes 페이지가 표시됩니다.
7. **Restart Proxy Server 버튼을 눌러 변경 사항을 적용합니다.**

요청 차단

업로드 컨텐트 유형을 기반으로 파일 업로드 및 기타 요청을 차단할 수 있습니다.

▼ MIME 유형을 기반으로 요청을 차단하는 방법

1. **Server Manager에 액세스하고 Filters 탭을 누릅니다.**
2. **Set Request Blocking 링크를 누릅니다.**
   Set Request Blocking 페이지가 표시됩니다.
3. **드롭다운 목록에서 자원을 선택하거나 Regular Expression 버튼을 눌러 정규 표현식을 입력하고 OK를 누릅니다.**
4. **원하는 요청 차단 유형을 선택합니다.**
   - Disabled — 요청 차단을 비활성화합니다

- Multipart MIME(File Upload) — 모든 파일 업로드를 차단합니다.
- MIME Types Matching Regular Expression — 입력한 정규 표현식과 일치하는 MIME 유형의 요청을 차단합니다. 정규 표현식에 대한 자세한 내용은 16 장, “템플리트 및 자원 관리”의 "정규 표현식 이해"를 참조하십시오.

5 모든 클라이언트에 대해 요청을 차단할지 또는 입력한 정규 표현식과 일치하는 사용자 에이전트에 대해 요청을 차단할지 여부를 선택합니다.

6 요청을 차단할 메소드를 선택합니다.

옵션은 다음과 같습니다.

- Any Method With Request Body — 메소드와 관계 없이 요청 본문이 있는 모든 요청을 차단합니다.
- Only For:
  - POST — POST 메소드를 사용하여 파일 업로드 요청을 차단합니다.
  - PUT — PUT 메소드를 사용하여 파일 업로드 요청을 차단합니다.
- Methods Matching Regular Expression — 입력한 메소드를 사용하여 모든 파일 업로드 요청을 차단합니다.

7 OK를 누릅니다.

8 Restart Required를 누릅니다.

Apply Changes 페이지가 표시됩니다.

9 Restart Proxy Server 버튼을 눌러 변경 사항을 적용합니다.

전송 헤더 억제

일반적으로 보안 상의 이유로 요청에서 전송 헤더를 표시하지 않도록 프록시 서버를 구성할 수 있습니다. 예를 들어, 사용자의 전자 메일 주소가 표시되는 From 헤더가 표시되지 않도록 할 수 있습니다. 또는 외부 서버가 조직에서 사용하는 웹 브라우저를 확인할 수 없도록 사용자 에이전트 헤더를 필터링할 수 있습니다. 또한 요청이 인터넷으로 전달되기 전에 인트라넷에서만 사용되는 로깅 또는 클라이언트 관련 헤더를 제거할 수 있습니다.

이 기능은 프록시 자체에서 특수하게 처리되거나 생성되는 헤더 또는 If-Modified-Since 및 Forwarded와 같이 프로토콜이 제대로 작동하는 데 필요한 헤더에는 영향을 주지 않습니다.

프록시에서 생성되어 전달된 헤더에는 보안 문제가 없습니다. 원격 서버가 해당 연결에서 연결되는 프록시 호스트를 감지할 수 있습니다. 프록시 체인에서 내부

프록시로부터 전달된 헤더는 외부 프록시에 의해 표시되지 않을 수 있습니다. 내부 프록시 또는 클라이언트 호스트 이름이 원격 서버에 공개되지 않도록 하려면 이 방법을 사용하여 서버를 설정하는 것이 좋습니다.

▼ 전송 헤더 억제 방법

1. **Server Manager에 액세스하고 Filters 탭을 누릅니다.**
2. **Suppress Outgoing Headers 링크를 누릅니다.**
   Suppress Outgoing Headers 페이지가 표시됩니다.
3. **표시하지 않을 요청 헤더 목록을 쉼표로 구분하여 Suppress Headers 입력란에 입력합니다.**
4. **Restart Required를 누릅니다.**
   Apply Changes 페이지가 표시됩니다.
5. **Restart Proxy Server 버튼을 눌러 변경 사항을 적용합니다.**

MIME 유형별 필터링

MIME 유형과 일치하는 특정 파일을 차단하도록 프록시 서버를 구성할 수 있습니다. 예를 들어, 실행 파일 또는 이진 파일을 차단하도록 프록시 서버를 설정하여 프록시 서버를 사용하는 클라이언트가 컴퓨터 바이러스를 다운로드할 수 없도록 합니다.

프록시 서버가 새 MIME 유형을 지원하도록 하려면 Server Manager에서 Preferences > Create/Edit MIME Types를 선택하고 해당 유형을 추가합니다. MIME 유형 만들기에 대한 자세한 내용은 130 페이지 “MIME 유형 만들기”를 참조하십시오.

필터링하는 MIME 유형을 템플리트와 결합하여 특정 URL에 대해 특정 MIME 유형만 차단할 수 있습니다. 예를 들어, `.edu` 도메인의 컴퓨터에서 들어오는 실행 파일을 차단할 수 있습니다.

▼ MIME 유형별 필터링 방법

1. **Server Manager에 액세스하고 Filters 탭을 누릅니다.**
2. **Set MIME Filters 링크를 누릅니다.**
   Set MIME Filters 페이지가 표시됩니다.
3. **MIME 유형 필터링에 사용할 템플리트를 선택하거나 전체 서버를 편집하는 중인지 확인합니다.**

4. **Current filter 입력란에 차단할 MIME 유형과 일치하는 정규 표현식을 입력할 수 있습니다.**
   예를 들어, 모든 응용 프로그램을 필터링하기 위해 정규 표현식에 **application/.***을 입력할 수 있습니다. 이 방법은 모든 응용 프로그램 유형에 대해 각 MIME 유형을 확인하는 것보다 빠릅니다. 정규 표현식은 대소문자를 구분하지 않습니다. 정규 표현식에 대한 자세한 내용은 16 장, "템플리트 및 자원 관리"의 "정규 표현식 이해"를 참조하십시오.

5. **필터링하려는 MIME 유형을 선택합니다.**
   클라이언트가 차단된 파일에 대한 액세스를 시도하는 경우 프록시 서버는 "403 Forbidden" 메시지를 반환합니다.

6. **OK를 누릅니다.**

7. **Restart Required를 누릅니다.**
   Apply Changes 페이지가 표시됩니다.

8. **Restart Proxy Server 버튼을 눌러 변경 사항을 적용합니다.**

HTML 태그별 필터링

파일을 클라이언트로 전달하기 전에 필터링할 HTML 태그를 지정할 수 있습니다. 이 방법을 통해 Java 애플릿 및 HTML 파일에 포함된 JavaScript와 같은 객체를 필터링할 수 있습니다. HTML 태그를 필터링하려면 HTML 태그의 시작과 끝을 지정합니다. 그러면 프록시는 파일을 클라이언트로 전송하기 전에 이러한 태그에 있는 모든 텍스트 및 객체를 공백으로 대체합니다.

프록시가 해당 자원을 캐시하도록 구성된 경우 프록시는 편집되지 않은 원본 파일을 저장합니다.

▼ HTML 태그 필터링 방법

1. **Server Manager에 액세스하고 Filters 탭을 누릅니다.**

2. **Set HTML Tag Filters 링크를 누릅니다.**
   Set HTML Tag Filters 페이지가 표시됩니다.

3. **수정할 템플리트를 선택합니다.**
   HTTP를 선택하거나 .edu 도메인에 있는 호스트의 URL과 같이 특정 URL만 지정하는 템플리트를 선택할 수 있습니다.

4. **필터링할 기본 HTML 태그를 선택합니다.**

- APPLET은 일반적으로 Java 애플릿 주위에 위치합니다.
- SCRIPT는 JavaScript 코드의 시작을 표시합니다.
- IMG는 인라인 이미지 파일을 지정합니다.

5 필터링할 HTML 태그를 입력할 수 있습니다.

HTML 태그의 시작과 끝을 입력합니다.

예를 들어, 양식을 필터링하기 위해 Start Tag 상자에 **FORM**을 입력하고 End Tag 상자에 **/FORM**을 입력할 수 있습니다. HTML 태그는 대소문자를 구분하지 않습니다. 필터링할 태그에 OBJECT 및 IMG와 같은 종료 태그가 없는 경우 End Tag 상자를 비워둘 수 있습니다.

6 OK를 누릅니다.

7 Restart Required를 누릅니다.

Apply Changes 페이지가 표시됩니다.

8 Restart Proxy Server 버튼을 눌러 변경 사항을 적용합니다.

컨텐트 압축용으로 서버 구성

Proxy Server는 HTTP 컨텐트 압축을 지원합니다. 컨텐트 압축을 사용하면 클라이언트로 전달하는 속도가 빨라지고 추가적인 하드웨어 비용 없이 컨텐트 볼륨을 늘릴 수 있습니다. 컨텐트 압축은 다운로드 시간을 단축시키므로 전화 접속 및 높은 수준의 트래픽 연결 사용자는 더 많은 혜택을 누릴 수 있습니다.

컨텐트 압축을 통해 Proxy Server는 압축된 데이터를 전송하고 데이터를 신속하게 압축 해제하도록 브라우저에 지시합니다. 이 압축으로 인해 전송되는 데이터 양은 감소되고 페이지 표시 속도는 빨라집니다.

요청 시 컨텐트를 압축하도록 서버 구성

전송 데이터를 신속하게 압축하도록 Proxy Server를 구성할 수 있습니다. 동적으로 생성된 HTML 페이지는 사용자가 요청할 때까지 존재하지 않습니다.

▼ 요청 시 컨텐트를 압축하도록 서버를 구성하는 방법

1 Server Manager에 액세스하고 Filters 탭을 누릅니다.

2 Compress Content on Demand 링크를 누릅니다.

Compress Content on Demand 페이지가 표시됩니다.

3 **드롭다운 목록에서 자원을 선택하거나 정규 표현식을 입력합니다.**

정규 표현식에 대한 자세한 내용은 16 장, “템플리트 및 자원 관리”의 "정규 표현식 이해"를 참조하십시오.

4 **다음 정보를 지정합니다.**

- **Activate Compress Content on Demand?** 서버가 선택된 자원에 대해 미리 압축된 컨텐트를 서비스해야 하는지 선택합니다.
- **Vary Header.** Vary: Accept-encoding 헤더를 삽입할지 지정합니다. Yes 또는 No를 선택합니다. Yes로 설정하면 파일의 압축된 버전이 선택되는 경우 Vary: Accept-encoding 헤더가 삽입됩니다.

  no로 설정되면 Vary: Accept-encoding 헤더가 삽입되지 않습니다.

  기본값은 yes로 설정됩니다.
- **Fragment Size.** 압축 라이브러리(`zlib`)가 한 번에 압축할 양을 제어하는 데 사용하는 메모리 단편 크기(바이트)를 지정합니다. 기본값은 8096입니다.
- **Compression Level.** 압축의 수준을 지정합니다. 1 - 9 사이 값을 선택합니다. 값 1은 속도가 최고이고 9는 압축율이 최고입니다. 기본값은 6으로 속도와 압축율이 조화된 값입니다.

5 **OK를 누릅니다.**

6 **Restart Required를 누릅니다.**

Apply Changes 페이지가 표시됩니다.

7 **Restart Proxy Server 버튼을 눌러 변경 사항을 적용합니다.**

◆ ◆ ◆ 14장

14 역방향 프록시 사용

이 장에서는 Proxy Server를 역방향 프록시로 사용하는 방법에 대해 설명합니다. 역방향 프록시는 외부 클라이언트에 대해 보안 컨텐트 서버를 가정함으로써 회사 외부에서 회사 서버의 데이터에 모니터링되지 않게 직접 액세스하는 것을 방지하기 위해 방화벽 외부에서 사용할 수 있습니다. 역방향 프록시는 복제에도 사용할 수 있습니다. 즉, 로드 균형 조정을 위해 사용량이 많은 서버 앞에서 여러 개의 프로시를 연결할 수 있습니다. 이 장에서는 Proxy Server를 방화벽 내부 또는 외부에서 번갈아 사용할 수 있는 방법에 대해 설명합니다.

이 장은 다음 내용으로 구성되어 있습니다.

- 295 페이지 "역방향 프록싱 작동 방식"
- 301 페이지 "역방향 프록시 설정"

역방향 프록싱 작동 방식

역방향 프록싱은 다음과 같은 두 가지 방법으로 사용할 수 있습니다. 한 가지 방법은 Proxy Server의 보안 기능을 사용하여 트랜잭션을 처리하는 것입니다. 다른 방법은 캐시를 사용하여 사용량이 많은 서버에 로드 균형 조정을 제공하는 것입니다. 두 가지 방법 모두 방화벽에서 엄격하게 작동하지 않기 때문에 일반 프록시 사용과는 다릅니다.

서버의 대역 역할을 하는 프록시

신용 카드 번호 데이터베이스와 같이 보안을 유지해야 하는 중요한 정보가 포함된 컨텐트 서버가 있는 경우 컨텐트 서버의 대역 역할을 할 프록시를 방화벽 외부에 설정할 수 있습니다. 컨텐트 서버에 액세스를 시도하는 외부 클라이언트는 프록시 서버로 보내집니다. 컨텐트 서버에 있는 실제 컨텐트는 안전하게 방화벽 내부에 존재합니다. 프록시 서버는 방화벽 외부에 있으며 클라이언트에게는 컨텐트 서버로 보입니다.

클라이언트가 사이트에 요청을 하면 요청은 프록시 서버로 보내집니다. 그러면 프록시 서버는 클라이언트의 요청을 방화벽의 특정한 경로를 통해 컨텐트 서버로 전송합니다.

컨텐트 서버는 방화벽의 특정 경로를 통해 결과를 다시 프록시로 전달합니다. 프록시는 그림 14–1에 나와 있는 대로 프록시가 실제 컨텐트 서버인 것처럼 검색된 정보를 클라이언트에 보냅니다. 컨텐트 서버가 오류 메시지를 반환하면 프록시 서버는 메시지를 가로채고 헤더에 나열된 모든 URL을 변경한 다음 메시지를 클라이언트에 전송할 수 있습니다. 이 작동 방식은 외부 클라이언트가 내부 컨텐트 서버에 대한 리디렉션 URL을 얻지 못하게 합니다.

이런 방법으로 프록시는 보안 데이터베이스와 악의적 공격의 가능성 사이에 추가적인 보호벽을 제공합니다. 가능성은 별로 없지만 공격에 성공하더라도 공격자는 전체 데이터베이스에 대한 액세스 권한을 얻는 것이 아니라 단일 트랜잭션에 관련된 정보로만 제한될 가능성이 많습니다. 방화벽 통로는 프록시 서버에만 액세스를 허용하기 때문에 인증되지 않은 사용자는 실제 컨텐트 서버에 액세스할 수 없습니다.

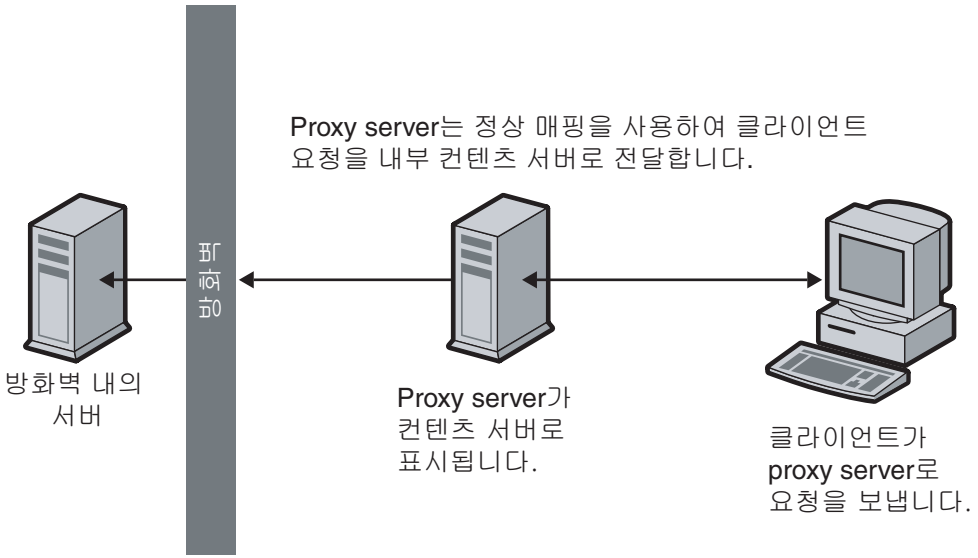

그림 14–1 역방향 프록시 프로세스

다른 시스템의 액세스는 허용하지 않고 특정 포트의 특정 서버(이 경우 할당된 포트의 프록시)만 방화벽을 통해 액세스할 수 있도록 방화벽 라우터를 구성할 수 있습니다.

보안 역방향 프록싱

보안 역방향 프록싱은 프록시 서버와 다른 시스템 간의 하나 이상의 연결이 SSL(Secure Sockets Layer) 프로토콜을 사용하여 데이터를 암호화할 때 수행됩니다.

보안 역방향 프록싱은 다음과 같은 여러 가지 용도로 사용됩니다.

- 방화벽 외부의 프록시 서버에서 방화벽 내부의 보안 컨텐트 서버로 암호화된 연결을 제공
- 클라이언트가 프록시 서버에 안전하게 연결할 수 있도록 하여 신용 카드 번호와 같은 정보의 안전한 전송을 보장

보안 역방향 프록싱이 수행되면 데이터 암호화에 따르는 오버헤드 때문에 각 보안 연결의 속도가 느려집니다. 하지만 SSL은 캐시 메커니즘을 제공하기 때문에 연결의 양측 모두 이전에 협상된 보안 매개 변수를 다시 사용할 수 있어 이후 연결에서는 오버헤드가 크게 줄어듭니다.

다음과 같은 세 가지 방법으로 보안 역방향 프록시를 구성할 수 있습니다.

- **클라이언트와 프록시 간 보안**. 이 시나리오는 다음 그림에서처럼 프록시와 컨텐트 서버 사이에 교환되는 정보가 인증되지 않은 사용자에 의해 액세스될 위험이 없거나 거의 없는 경우에 효과적입니다.

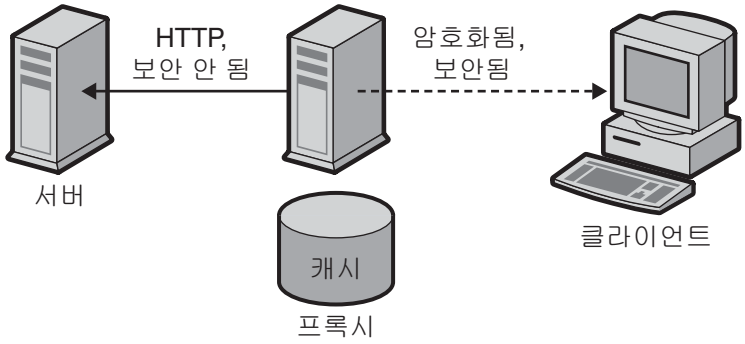

그림 14–2 프록시에 대한 클라이언트 연결 보안

- **프록시와 컨텐트 서버 간 보안**. 이 시나리오는 클라이언트가 방화벽 내부에 있고 컨텐트 서버가 방화벽 외부에 있는 경우에 효과적입니다. 이 시나리오에서는 다음 그림에서처럼 프록시 서버가 사이트 간의 보안 채널 역할을 수행할 수 있습니다.

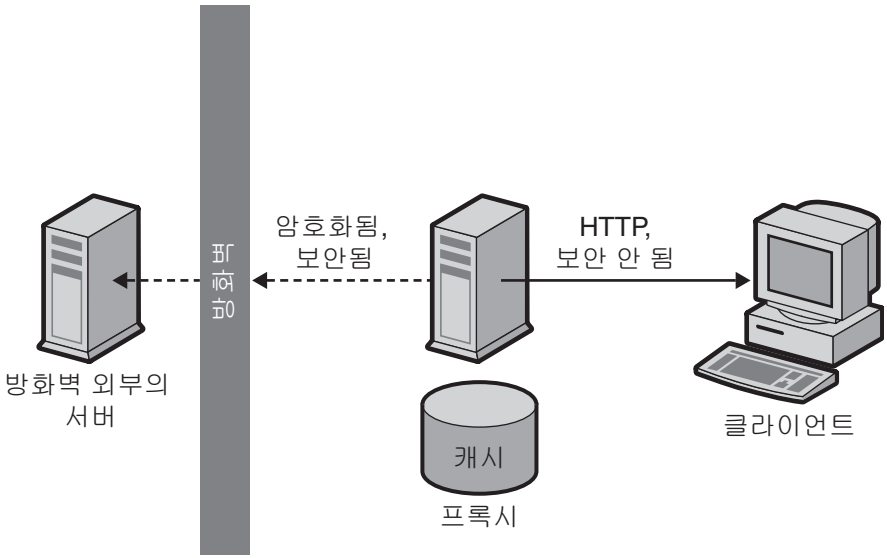

그림 14–3 컨텐트 서버에 대한 프록시 연결 보안

- **클라이언트와 프록시 간 및 프록시와 컨텐트 서버 간 보안**. 이 시나리오는 서버, 프록시 및 클라이언트 간에 교환되는 정보가 보안되어야 하는 경우에 효과적입니다. 이 시나리오에서는 다음 그림에서처럼 프록시 서버가 추가 보안 방법인 클라이언트 인증을 사용하여 사이트 간의 보안 채널 역할을 수행할 수 있습니다.

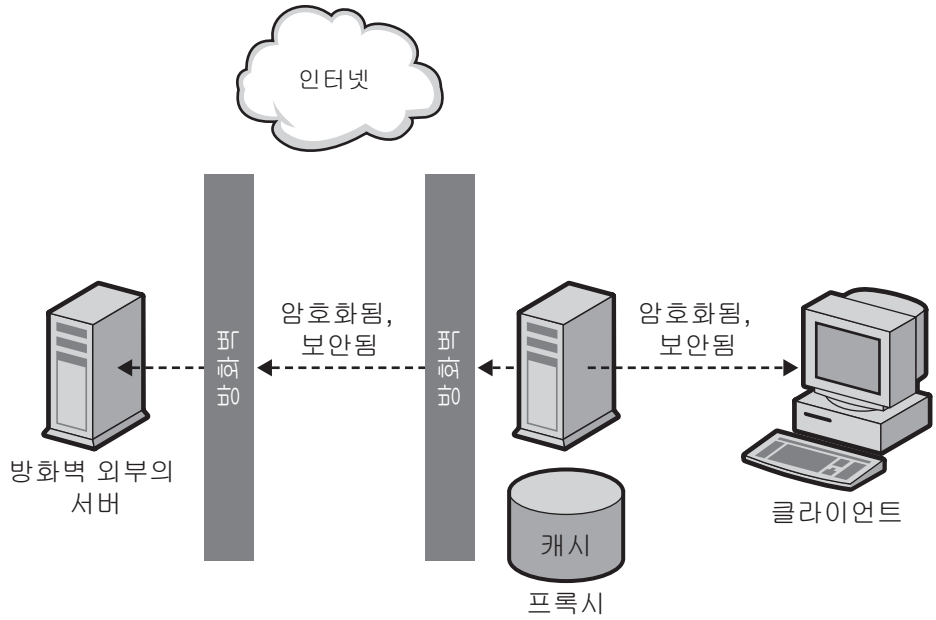

그림 14–4 프록시에 대한 클라이언트 연결 보안 및 컨텐트 서버에 대한 프록시 연결 보안

각 구성을 설정하는 방법에 대해서는 301 페이지 “역방향 프록시 설정”을 참조하십시오.

프록시는 SSL 이외에도 클라이언트 인증을 사용할 수 있는데, 이 경우 프록시에 요청을 하는 컴퓨터는 인증서나 다른 식별 형식을 제공하여 자신의 아이디를 확인할 수 있게 해야 합니다.

로드 균형 조정을 위한 프록싱

조직 내에서 프록시 서버를 여러 개 사용하여 웹 서버 간의 네트워크 로드 균형을 조정할 수 있습니다. 이 모델은 프록시 서버의 캐시 기능을 활용하여 로드 균형 조정을 위한 서버 풀을 만듭니다. 이 경우 프록시 서버는 방화벽의 어느 쪽에도 위치할 수 있습니다. 일별로 많은 양의 요청을 수신하는 웹 서버가 있는 경우 프록시 서버를 사용하여 웹 서버의 로드를 줄이고 네트워크 액세스의 효율성을 높일 수 있습니다.

프록시 서버는 클라이언트 요청을 실제 서버로 전달하는 매개자 역할을 합니다. 프록시 서버는 요청된 문서를 캐시합니다. 프록시 서버가 두 개 이상인 경우 DNS는 프록시 서버의 IP 주소를 "라운드 로빈" 방식으로 선택하여 요청을 임의로 라우팅할 수 있습니다. 클라이언트는 매번 같은 URL을 사용하지만 요청은 매번 다른 프록시를 통해 라우팅될 수 있습니다.

프록시 서버를 여러 개 사용하여 사용량이 많은 컨텐트 서버 하나에 대한 요청을 처리하면 프록시 서버를 한 개 사용할 때보다 서버가 로드를 더 많이 처리할 수 있고

효율성도 더 높아집니다. 프록시가 처음으로 컨텐트 서버에서 문서를 검색하는 초기 시작 기간이 지나면 컨텐트 서버에 대한 요청의 수가 크게 줄어들 수 있습니다.

CGI 요청과 일부 새 요청만 항상 컨텐트 서버로 전달되고 나머지는 프록시가 처리할 수 있습니다. 예를 들어 서버에 대한 요청의 90%가 CGI 요청이 아니어서 캐시가 가능하고 컨텐트 서버는 일별로 2백만 히트를 수신한다고 가정합니다. 이 경우 세 개의 역방향 프록시를 연결하고 각각 일별로 2백만 히트를 처리하면 하루에 약 6백만 히트를 처리할 수 있습니다. 컨텐트 서버에 도달하는 요청의 10%는 각 프록시로부터 일일 약 200,000 히트까지 또는 총 600,000 히트만 추가할 수 있으므로 효율성이 훨씬 높아집니다. 히트 수는 약 2백만에서 6백만으로 증가할 수 있으며 컨텐트 서버의 로드는 이에 따라 2백만에서 600,000으로 줄어들 수 있습니다. 실제 결과는 상황에 따라 다를 수 있습니다.

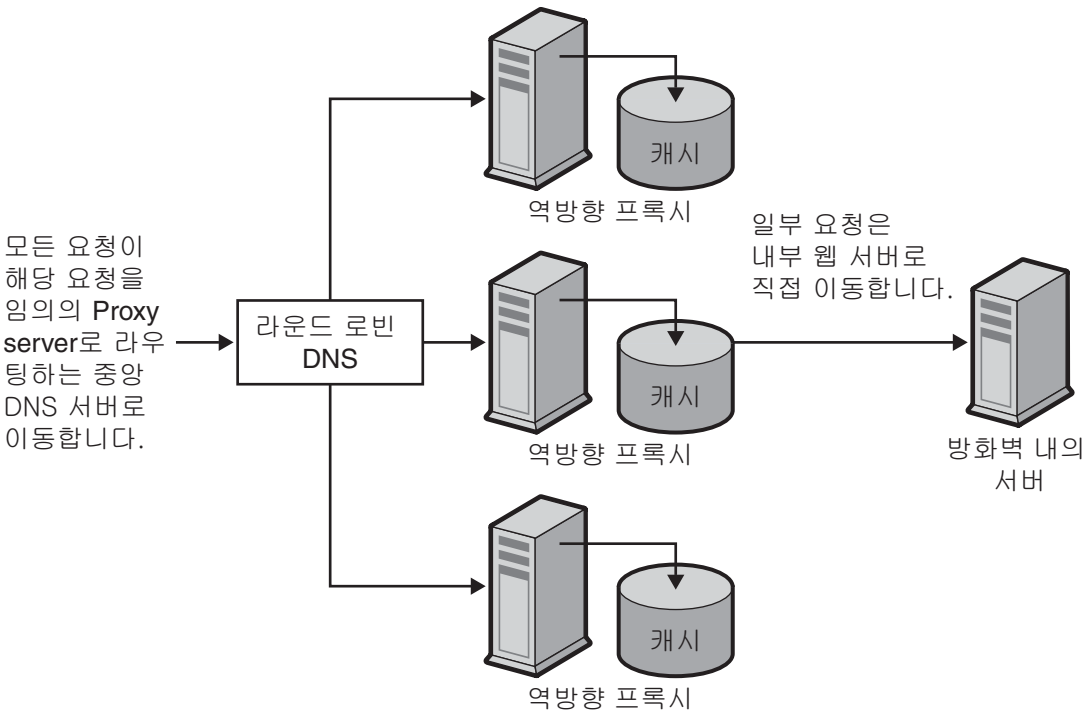

그림 14–5 로드 균형 조정에 사용되는 프록시

역방향 프록시 설정

역방향 프록시를 설정하려면 정방향 매핑과 역방향 매핑의 두 가지 매핑이 필요합니다.

- 정방향 매핑은 요청을 컨텐트 서버로 리디렉션합니다. 클라이언트가 프록시 서버에 문서를 요청하는 경우 프록시 서버에는 실제 문서를 얻을 수 있는 위치를 알려 주는 정방향 매핑이 필요합니다.

주의 – 프록시가 잘못된 결과를 반환할 수 있으므로 자동 구성 파일을 제공하는 프록시에는 역방향 프록시를 사용하지 마십시오.

- 역방향 매핑은 컨텐트 서버로부터 리디렉션을 트랩하도록 프록시 서버에 지시합니다. 프록시는 리디렉션을 가로챈 다음 리디렉션된 URL이 프록시 서버에 매핑되도록 변경합니다. 예를 들어 클라이언트가 이동되었거나 찾을 수 없는 문서를 요청하는 경우 컨텐트 서버는 요청된 URL에서 문서를 찾을 수 없음을 설명하는 메시지를 클라이언트에 반환합니다. 컨텐트 서버는 이 반환 메시지에 이동된 파일을 가져오는 데 사용할 URL이 나열된 HTTP 헤더를 추가합니다. 내부 컨텐트 서버의 개인 정보를 유지 관리하기 위해 프록시는 역방향 매핑을 사용하여 URL을 리디렉션할 수 있습니다.

`http://http.site.com/`이라는 웹 서버가 있고 이 서버에 대해 역방향 프록시 서버를 설정하려는 경우를 가정합니다. 역방향 프록시를 `http://proxy.site.com/`이라고 할 수 있습니다.

▼ 정방향 또는 역방향 매핑을 만드는 방법

1. **Server Manager에 액세스하고 URL 탭을 누릅니다.**
2. **Create Mapping 링크를 누릅니다.**
   Create Mapping 페이지가 표시됩니다.
3. **페이지가 나타나면 정방향 매핑에 대한 소스 접두어 및 대상을 입력합니다.**
   예:

   소스 접두어: `http://proxy.site.com`

   소스 대상: `http://http.site.com/`
4. **OK를 누릅니다.**
   페이지로 돌아가서 역방향 매핑을 만듭니다. 예를 들면 다음과 같습니다.

   역방향 매핑:

   소스 접두어: `http://http.site.com/`

소스 대상: `http://proxy.site.com/`

5 변경 내용을 적용하려면 OK를 누릅니다.

OK 버튼을 누르면 프록시 서버가 하나 이상의 다른 매핑을 추가합니다. 매핑을 보려면 lView/Edit Mappings 링크를 누릅니다. 추가 매핑의 형식은 다음과 같습니다.

from: `/`

to: `http://http.site.com/`

이러한 추가 자동 매핑은 일반 서버로 역방향 프록시에 연결하는 사용자용입니다. 첫 번째 매핑은 정방향 프록시로 역방향 프록시에 연결하는 사용자를 확인하기 위한 것입니다. "/" 매핑은 Administration GUI에서 자동으로 제공하는 Map Source Prefix 입력란의 내용을 사용자가 변경하지 않은 경우에만 추가됩니다. 일반적으로 두 번째 매핑이 유일한 필수 매핑이지만 설정에 따라서는 추가 매핑을 하더라도 프록시에 문제가 발생하지 않습니다.

주 – 웹 서버에 DNS 별칭이 여러 개 있는 경우 각 별칭에는 해당 정방향 매핑이 있어야 합니다. 웹 서버가 여러 개의 DNS 별칭을 사용하여 자신에 대한 리디렉션을 생성하는 경우 각 별칭에는 해당 역방향 매핑이 있어야 합니다.

CGI 응용 프로그램은 여전히 원래 서버에서 실행됩니다. 프록시 서버 자체에서는 CGI 응용 프로그램이 실행되지 않습니다. 하지만 CGI 스크립트에서 마지막으로 수정된 또는 Expires 헤더를 발급하여 0이 아닌 TTL(Timt-to-live)을 의미함으로써 결과가 캐시될 수 있음을 나타내는 경우, 프록시가 결과를 캐시합니다.

웹 서버를 위한 컨텐트를 제작할 때는 컨텐트가 역방향 프록시에 의해서도 서비스된다는 점을 고려하여 웹 서버의 파일에 대한 모든 링크에 상대 링크를 사용해야 합니다. HTML 파일에서 호스트 이름을 참조하지 마십시오. 모든 링크는 페이지로만 구성되어야 합니다.

`/abc/def`

다음과 같은 정규화된 호스트 이름은 사용하지 않아야 합니다.

`http://http.site.com/abc/def`

주 – 역방향 프록시 모드에서 발생하는 오류에 대해 사용자 정의 오류 페이지를 제공할 수 있습니다. 이러한 오류 페이지는 프록시에 의해 생성된 오류를 대체합니다. 이를 통해 클라이언트는 프록시 서버가 구성되어 있다는 것을 알 수 없게 됩니다.

보안 역방향 프록시 설정

보안 역방향 프록싱을 설정하기 전에 디지털 인증서, 인증 기관 및 인증에 대해 충분히 이해해야 합니다.

보안 역방향 프록시를 설정하는 방법은 비보안 역방향 프록시를 설정하는 것과 거의 동일합니다. 유일한 차이는 암호화될 파일에 대해 HTTPS를 프로토콜로 지정해야 한다는 점입니다.

클라이언트-프록시 보안

이 절차에서는 선택한 구성 시나리오에 따라 보안 역방향 프록시를 설정하는 방법을 설명합니다. 매핑을 설정하는 방법을 보여 주기 위해 `http.site.com`이라는 웹 서버가 있고 `proxy.site.com`이라는 보안 역방향 프록시 서버를 설정한다고 가정합니다. 단계를 수행할 때 실제 웹 서버와 프록시 이름을 예에서 사용된 이름으로 바꾸십시오.

▼ 보안 클라이언트-프록시 매핑을 설정하는 방법

1. **Server Manager에 액세스하고 URL 탭을 누릅니다.**
2. **Create Mapping 링크를 누릅니다.**
   Create Mapping 페이지가 표시됩니다.
3. **페이지가 나타나면 다음 방법으로 정방향 및 역방향 매핑을 설정합니다.**
   정방향 매핑:

   소스 접두어: `https://proxy.mysite.com`

   소스 대상: `http://http.mysite.com/`

   역방향 매핑:

   소스 접두어: `http://http.mysite.com/`

   소스 대상: `https://proxy.mysite.com/`
4. **변경 내용을 저장하고 적용합니다.**
   이렇게 만든 매핑을 보려면 View/Edit Mappings 링크를 누릅니다.

주 – 이 구성은 프록시 서버가 보안 모드에서 실행될 경우에만 작동합니다. 즉, 암호화가 활성화되어 있어야 하며 명령줄에서 프록시를 다시 시작해야 합니다. 명령줄에서 프록시를 다시 시작하려면 프록시 디렉토리로 이동하여 **`./start`**를 입력합니다.

▼ 보안 프록시-컨텐트 서버 매핑을 설정하는 방법

1. **Server Manager에 액세스하고 URL 탭을 누릅니다.**
2. **Create Mapping 링크를 누릅니다.**
   Create Mapping 페이지가 표시됩니다.

3 **페이지가 나타나면 다음 방법으로 정방향 및 역방향 매핑을 설정합니다.**
정방향 매핑:

소스 접두어: `http://proxy.mysite.com`

소스 대상: `https://http.mysite.com/`

역방향 매핑:

소스 접두어: `https://http.mysite.com/`

소스 대상: `http://proxy.mysite.com/`

4 **변경 내용을 저장하고 적용합니다.**
이렇게 만든 매핑을 보려면 View/Edit Mappings라는 링크를 누릅니다.

주 – 이 구성은 컨텐트 서버가 보안 모드에서 실행 중인 경우에만 작동합니다.

▼ 보안 클라이언트-프록시 및 보안 프록시-컨텐트 서버를 설정하는 방법

1 **Server Manager에 액세스하고 URL 탭을 누릅니다.**

2 **Create Mapping 링크를 누릅니다.**
Create Mapping 페이지가 표시됩니다.

3 **페이지가 나타나면 다음 방법으로 정방향 및 역방향 매핑을 설정합니다.**
정방향 매핑:

소스 접두어: `https://proxy.mysite.com`

소스 대상: `https://http.mysite.com/`

역방향 매핑:

소스 접두어: `https://http.mysite.com/`

소스 대상: `https://proxy.mysite.com/`

4 **변경 내용을 저장하고 적용합니다.**
이렇게 만든 매핑을 보려면 View/Edit Mappings라는 링크를 누릅니다.

주 – 이 구성은 프록시 서버와 컨텐트 서버가 보안 모드에서 실행 중인 경우에만 작동합니다. 즉, 프록시에 대해 암호화가 활성화되어 있어야 하며 명령줄에서 프록시를 다시 시작해야 합니다. 명령줄에서 프록시를 다시 시작하려면 프록시 디렉토리로 이동하여 **./restart**를 입력합니다.

역방향 프록시 설정 시 정방향 프록시 기능 사용 안 함

프록시 서버가 역방향 프록시 서버로 구성된 경우 기본적으로 해당 프록시 서버 인스턴스는 정방향 프록시 서버로도 계속 작동됩니다. 이러한 서버 인스턴스는 역방향 프록시 요청을 수락하여 서비스를 제공할 뿐만 아니라 정방향 프록시 요청에 대해서도 서비스를 제공합니다. 따라서 정방향 프록시 기능을 사용하지 않으려면 추가적인 구성이 필요합니다. URI가 정방향 프록시 형식과 일치하는 요청을 거부하는 ACL 구성을 설정할 수 있으며,이를 위해 다음과 같은 Client 지시문을 사용할 수 있습니다.

```
<Client uri="http://.*">
PathCheck fn="check-acl" acl="http://.*"
<Client>
.
.
.
The "http://.*" ACL can be a deny all ACL as follows:
.
.
acl "http://.*";
deny (all) user="anyone";
```

역방향 프록시의 가상 멀티호스팅

가상 멀티호스팅은 역방향 프록시 서버 등의 원래 서버가 각 주소에 서로 다른 서버가 설치된 것처럼 여러 DNS 별칭에 응답할 수 있도록 하는 기능입니다. 예를 들어 다음과 같은 이름의 DNS 호스트가 있다고 가정합니다.

- `www`
- `specs`
- `phones`

이 호스트 이름을 각각 같은 IP 주소, 즉 역방향 프록시의 IP 주소에 매핑할 수 있습니다. 그러면 역방향 프록시는 해당 프록시에 액세스하는 데 사용된 DNS 이름에 따라 서로 다르게 작동할 수 있습니다.

가상 멀티호스팅을 사용하면 단일 역방향 프록시 서버에 여러 개의 서로 다른 *도메인*을 호스팅할 수도 있습니다. 예:

- `www.domain-1.com`
- `www.domain-2.com`

- www.domain-3.com

여러 로컬 호스트 이름과 여러 도메인의 조합을 모두 하나의 프록시 서버에서 사용할 수 있습니다.

- www
- specs
- phones
- www.domain-1.com
- www.domain-2.com
- www.domain-3.com

가상 멀티호스팅의 기능 세부 사항

DNS 호스트 이름과 도메인의 이름 또는 별칭을 지정하고 해당 호스트 이름으로 전송된 요청이 전달되어야 하는 대상 URL 접두어를 지정하면 가상 멀티호스팅 기능이 작동합니다. 예를 들어 다음 두 가지 매핑이 있다고 가정합니다.

- engr.domain.com -> http://int-engr.domain.com
- mktg.domain.com -> http://int-mktg.domain.com

매핑이 루트 간 매핑일 필요는 없습니다. 대상 URL에 추가 URL 경로 접두어를 지정할 수 있습니다.

- engr.domain.com -> http://internal.domain.com/engr
- mktg.domain.com -> http://internal.domain.com/mktg

가상 도메인 매핑에도 같은 기법이 적용됩니다. 예를 들어 다음을 사용할 수 있습니다.

- www.domain-1.com -> http://int-engr.domain.com
- www.domain-2.com -> http://int-mktg.domain.com

그러면 시스템은 HTTP "Host:" 헤더를 찾습니다. 시스템은 이 헤더를 기준으로 일치하는 가상 멀티호스팅 매핑을 선택합니다. 일치하는 멀티호스팅 매핑이 없으면 서버는 구성 파일에 나타나는 순서대로 다른 매핑을 찾거나, 찾지 못하는 경우 매핑을 수행하지 않습니다. 일치하는 매핑을 찾지 못한 경우 일반적으로 프록시는 "프록시가 요청 수행 거부" 응답을 발급합니다.

▼ 가상 멀티호스팅을 구성하는 방법

1 Server Manager에 액세스하고 URL 탭을 누릅니다.

2 Configure Virtual Multihosting 링크를 누릅니다.

Configure Virtual Multihosting 페이지가 표시됩니다.

3 Source Hostname (alias) 필드에서 이 매핑이 적용될 로컬 호스트 이름(또는 DNS 별칭)을 지정합니다.

4 **Source Domain Name 필드에서 이 매핑이 적용될 로컬 도메인 이름을 입력합니다.**
여러 개의 서로 다른 DNS 도메인을 멀티호스팅하려는 경우 이외에는 일반적으로 이 이름은 자체 네트워크의 도메인 이름입니다.

5 **호스트와 도메인 이름이 위에서 지정한 내용과 일치하는 경우 요청이 전달될 대상 URL 접두어를 Destination URL Prefix 필드에 입력합니다.**

6 **템플리트를 사용하는 경우에는 Use This Template 드롭다운 목록에서 템플리트 이름을 선택하고, 템플리트를 적용하지 않으려면 NONE의 값을 유지합니다.**

7 **OK를 누릅니다.**

8 **Restart Required를 누릅니다.**
Apply Changes 페이지가 표시됩니다.

9 **Restart Proxy Server 버튼을 눌러 변경 사항을 적용합니다.**
원하는 모든 가상 멀티호스팅 매핑에 대해 위의 단계를 반복합니다.

Configure Virtual Multihosting 페이지 아래쪽에 모든 가상 멀티호스팅 매핑이 나타납니다. Source Hostname (alias) 및 Source Domain Name 필드가 프록시의 포트 번호와 함께 "Host:" 헤더를 찾습니다.

예를 들어 호스트 이름이 `www`이고 도메인이 `example.com`이며 포트 번호가 8080이면 다음과 같은 정규 표현식이 나타납니다.

```
www(|.example.com)(|:8080)
```

이 정규 표현식은 사용자가 입력했거나 클라이언트가 보냈을 수 있는 다음과 같은 모든 가능한 조합과 일치합니다. 일부 클라이언트 소프트웨어에서는 포트 번호가 80이 아닌 경우에도 서버가 해당 포트에서 수신했기 때문에 포트 번호가 생략될 수 있습니다.

- `www`
- `www:8080`
- `www.example.com`
- `www.example.com:8080`

가상 멀티호스팅에 대한 참고 사항

- 역방향 프록시 매핑을 구성하려면 먼저 클라이언트 자동 구성 기능을 비활성화해야 합니다. 클라이언트 자동 구성 기능은 역방향 프록시가 아니라 정방향 프록시 작동을 위한 기능입니다.
- 가상 멀티호스팅 기능은 자동 역방향 매핑을 만듭니다. 가상 멀티호스팅 페이지를 사용하여 제공하는 매핑에 대해 역방향 매핑을 만들지 마십시오.
- 가상 매핑은 `obj.conf` 파일에서 `virt-map` 기능을 사용하여 지정됩니다.

- 가상 매핑은 obj.conf 구성 파일에 지정된 순서대로 일치됩니다. 정방향, 역방향, 정규 표현식 또는 클라이언트 자동 구성 매핑이 가상 매핑 전에 나타나는 경우 먼저 적용됩니다. 마찬가지로, 가상 매핑에 일치하는 매칭이 없으면 obj.conf의 가상 매핑 섹션 뒤의 다음 매핑으로 변환이 계속됩니다.

  주 – 지정 순서에서 역방향 매핑은 다른 매핑보다 먼저 나타나야 합니다.

- 프록시 서버의 포트 번호가 변경되면 가상 멀티호스팅 매핑을 다시 만들어 새 포트 번호를 반영해야 합니다.

◆ ◆ ◆ 15 장

15 SOCKS 사용

이 장에서는 Sun Java System Web Proxy Server에 포함된 SOCKS 서버를 구성하고 사용하는 방법을 설명합니다. Proxy Server는 SOCKS 버전 4 및 5를 지원합니다.

이 장은 다음 내용으로 구성되어 있습니다.

- 309 페이지 “SOCKS 정보”
- 310 페이지 “번들로 제공되는 SOCKS v5 서버 사용”
- 311 페이지 “socks5.conf 정보”
- 312 페이지 “SOCKS v5 서버 시작 및 중지”
- 312 페이지 “SOCKS v5 서버 구성”
- 314 페이지 “SOCKS v5 인증 항목 구성”
- 316 페이지 “SOCKS v5 연결 항목 구성”
- 319 페이지 “SOCKS v5 서버 체인 구성”
- 319 페이지 “라우팅 항목 구성”

SOCKS 정보

SOCKS는 SOCKS 서버 반대쪽에 있는 호스트의 연결 요청을 리디렉션하여 IP에 직접 연결할 필요 없이 한쪽의 호스트가 다른 쪽의 호스트에 완전하게 액세스할 수 있도록 하는 네트워킹 프록시 프로토콜입니다. SOCKS는 인터넷에서 내부 호스트로 무단 액세스할 수 없도록 차단하면서 SOCKS 서버 뒤의 호스트가 인터넷에 완전하게 액세스할 수 있도록 하는 네트워크 방화벽으로 많이 사용됩니다.

SOCKS 서버는 지점간 기반으로 방화벽을 통해 액세스를 제어하는 일반 방화벽 데몬입니다. SOCKS 서버는 요청을 인증 및 권한을 부여하고, 프록시 연결을 설정하고, 데이터를 중계합니다. SOCKS 서버는 응용 프로그램 수준이 아니라 네트워크 수준에서 작동하므로 요청 전송에 사용되는 프로토콜이나 방법에 대해 알지 못합니다. SOCKS 서버가 프로토콜을 알지 못하므로 Telnet과 같이 Proxy Server에서 지원되지 않는 프로토콜을 전달하는 데 사용할 수 있습니다.

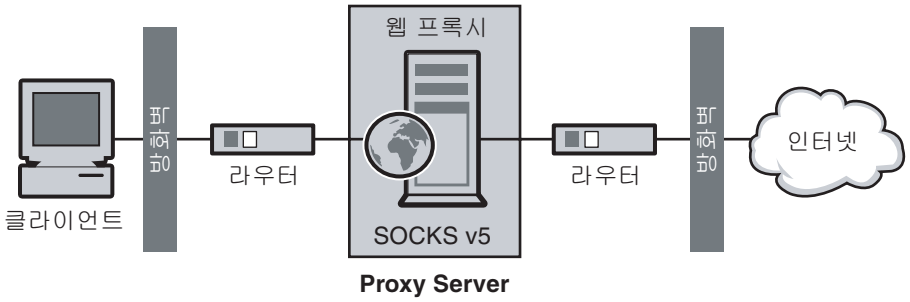

그림 15–1 네트워크에서 SOCKS 서버 위치

번들로 제공되는 SOCKS v5 서버 사용

Sun Java System Web Proxy Server에는 다른 SOCKS 데몬이 사용하는 `socks5.conf` 파일 형식을 이해하는 자체 SOCKS 데몬이 포함되어 있습니다. Proxy Server가 이 데몬을 사용하여 요청을 라우팅하거나 Proxy Server에서 이 데몬을 실행하여 네트워크에 추가 기능을 제공할 수 있습니다. SOCKS 서버를 통해 요청을 라우팅하도록 Proxy Server를 구성하는 방법에 대한 자세한 내용은 319 페이지 “라우팅 항목 구성”을 참조하십시오.

Proxy Server에 포함된 SOCKS 데몬은 기본적으로 비활성화됩니다. Server Manager 인터페이스의 SOCKS 탭이나 명령줄에서 데몬을 활성화할 수 있습니다. 자세한 내용은 312 페이지 “SOCKS v5 서버 시작 및 중지”를 참조하십시오.

주 – Proxy Server 4에서는 SOCKS 데몬의 이름이 `ns-sockd`에서 `sockd`로 변경되었습니다.

다음은 Proxy Server에 포함된 SOCKS 서버를 사용하기 위해 수행해야 하는 전체 단계입니다.

▼ SOCKS 사용 방법

1. **SOCKS 서버를 구성합니다. 312 페이지 “SOCKS v5 서버 구성”을 참조하십시오.**
2. **SOCKS 서버를 여러 인터페이스가 있는 컴퓨터에서 실행하는 경우 SOCKS 라우팅 항목을 만듭니다. 319 페이지 “라우팅 항목 구성”을 참조하십시오.**
3. **인증 항목을 만듭니다. 314 페이지 “SOCKS v5 인증 항목 구성”을 참조하십시오.**
4. **연결 항목을 만듭니다. 316 페이지 “SOCKS v5 연결 항목 구성”을 참조하십시오.**
5. **SOCKS 서버를 활성화합니다. 312 페이지 “SOCKS v5 서버 시작 및 중지”를 참조하십시오.**

socks5.conf 정보

Sun Java System Web Proxy Server는 `socks5.conf` 파일을 사용하여 SOCKS 서버 및 서비스에 대한 액세스를 제어합니다. 각 항목은 항목과 일치하는 요청이 수신될 때 Proxy Server가 수행할 작업을 정의합니다. Server Manager에서 선택한 내용은 `socks5.conf`에 기록됩니다. 파일을 직접 편집할 수도 있습니다. `socks5.conf` 파일은 다음과 같이 설치 루트 디렉토리 *server-root*에 있습니다.

server-root`/proxy-`*serverid*`/config` 디렉토리

이 절에서는 `socks5.conf`에 대한 일반적인 정보를 제공합니다. 파일, 해당 지시문 및 구문에 대한 자세한 내용은 Proxy Server **구성 파일 참조**를 참조하십시오.

인증

서비스 사용 시 인증을 요구하도록 SOCKS 데몬을 구성할 수 있습니다. 인증은 연결되는 클라이언트의 호스트 이름 및 포트를 기반으로 합니다. 사용자 이름 및 비밀번호를 요구하는 경우, `socks5.conf` 파일이 참조하는 사용자 이름 및 비밀번호 파일에 대해 정보를 인증합니다. 제공된 사용자 이름 및 비밀번호가 비밀번호 파일의 목록과 일치하지 않으면 액세스가 거부됩니다. 비밀번호 파일의 사용자 이름 및 비밀번호의 형식은 *username password* 입니다. 여기서 사용자 이름과 비밀번호는 공백으로 구분합니다. .

사용자를 차단할 수도 있습니다. 사용자 이름 및 비밀번호 인증을 요구하려면 `SOCKS5_PWDFILE` 지시문을 `socks5.conf`에 추가해야 합니다. 지시문 및 해당 구문에 대한 자세한 내용은 Proxy Server **구성 파일 참조**의 `socks5.conf` 절을 참조하십시오.

사용자 이름 및 비밀번호 인증은 파일뿐만 아니라 구성된 LDAP 서버에 대해서도 수행할 수 있습니다.

액세스 제어

액세스 제어는 `socks5.conf` 파일의 정렬된 행 세트를 사용하여 수행됩니다. 각 행에는 자원에 대한 액세스를 허용하거나 거부하는 단일 지시문이 포함되어 있습니다. 지시문은 구성 파일에 나타나는 순서대로 처리됩니다. 허용 지시문과 일치하지 않는 요청은 액세스가 거부됩니다.

로깅

SOCKS 데몬은 오류 및 액세스 메시지를 모두 SOCKS 로그 파일에 기록합니다. 로그 파일 위치 및 로깅 유형은 `socks5.conf`에서 지정할 수 있습니다.

또한 SOCKS 데몬은 데몬에 대한 통계를 제공하는 시간별 통계 항목을 생성합니다.

조정

`socks5.conf` 파일을 사용하여 SOCK 서버에 사용되는 작업자 및 승인 스레드의 수를 확인할 수 있습니다. 이러한 수는 SOCKS 서버의 성능에 영향을 미칩니다.

작업자 및 승인 스레드 설정과 성능에 미치는 영향에 대한 자세한 내용은 312 페이지 “SOCKS v5 서버 구성”의 해당 절을 참조하십시오.

SOCKS v5 서버 시작 및 중지

SOCKS 서버는 Server Manager 또는 명령줄에서 시작하고 중지할 수 있습니다.

▼ Server Manager에서 SOCKS 서버를 시작 및 중지하는 방법

1. **서버 인스턴스에 대한 Server Manager에 액세스하고 SOCKS 탭을 누릅니다.**
2. **Start/Stop SOCKS Server 링크를 누릅니다.**
3. **SOCKS 서버를 시작하거나 중지합니다.**

명령줄에서 SOCKS 서버를 시작 및 중지하는 방법

server-root/proxy- *serverid* 디렉토리에 있는 스크립트를 실행합니다. 여기서 *server-root*는 설치 루트입니다.

- `start-sockd`는 SOCKS 데몬을 시작합니다.
- `stop-sockd`는 SOCKS 데몬을 중지합니다.
- `restart-sockd`는 SOCKS 데몬을 다시 시작합니다.

SOCKS v5 서버 구성

▼ SOCKS 서버 구성 방법

1. **서버 인스턴스에 대한 Server Manager에 액세스하고 SOCKS 탭을 누릅니다.**
2. **Configure SOCKS v5 링크를 누릅니다.**
3. **SOCKS Port 필드에 SOCKS 서버가 수신할 포트 번호를 입력합니다. 기본값은 1080입니다.**
4. **사용할 SOCKS 옵션을 선택합니다.**
   다음 옵션을 사용할 수 있습니다.

- *Disable Reverse DNS Lookup.*SOCKS 서버에 대해 역방향 DNS 조회를 비활성화합니다. 역방향 DNS는 IP 주소를 호스트 이름으로 변환합니다. 역방향 DNS 조회를 비활성화하면 네트워크 자원을 절약할 수 있습니다. 기본적으로 DNS 조회는 비활성화되어 있습니다. 역방향 DNS 조회가 비활성화되고 호스트 이름으로 URL이 요청되면 서버는 호스트 이름을 IP 주소에 매핑하지 않습니다. 역방향 DNS 조회가 활성화된 경우 서버는 매핑을 수행하고 항목을 SOCKS 로그 파일에 추가하여 DNS 변환을 나열합니다.
  - **Use Client-specific Bind Port.** 클라이언트가 BIND 요청에서 포트를 지정할 수 있습니다. 이 옵션을 비활성화하면 SOCKS는 클라이언트에서 요청한 포트를 무시하고 임의 포트를 할당합니다. 기본적으로 이 옵션은 비활성화되어 있습니다.
  - **Allow** *Wildcard As Bind IP Address.* 클라이언트가 BIND 요청에서 모두 0으로 구성된 IP 주소(0.0.0.0)를 지정할 수 있습니다. 이는 모든 IP 주소에서 연결할 수 있음을 의미합니다. 이 옵션을 비활성화하면 클라이언트는 바인드 포트에 연결할 IP 주소를 지정해야 하며 SOCKS 서버는 0.0.0.0으로의 바인드 요청을 거부합니다. 기본적으로 이 옵션은 비활성화되어 있습니다.
  - *Quench Updates.* 매시간 작성되는 자동 상태 파일을 비활성화합니다. 비활성화하면 요청마다 쓰기가 수행됩니다. 자세한 내용은 311 페이지 “로깅”을 참조하십시오.

Quench Updates 요소는 사용자 인터페이스에 표시되지만 이 Proxy Server 4 릴리스에서는 구현되지 않습니다.

5 Log File 필드에 SOCKS 로그 파일의 전체 경로 이름을 입력합니다.

기본값은 *server-root*/proxy- *serverid*/logs/socks5.log입니다.

6 Log Level 드롭다운 목록에서 로그 파일에 경고 및 오류만 포함할지, 모든 요청을 포함할지 또는 디버깅 메시지를 포함할지 여부를 선택합니다.

7 RFC 1413 ID 응답을 선택합니다.

SOCKS 서버는 ID를 통해 클라이언트의 사용자 이름을 확인할 수 있습니다. 일반적으로 이 기능은 클라이언트가 일부 UNIX 버전을 실행하는 경우에만 작동합니다. 다음 옵션을 사용할 수 있습니다.

- **Don’t Ask.** ID를 사용하여 클라이언트의 사용자 이름을 확인하지 않습니다. 권장 및 기본 설정입니다.
  - **Ask But Don’t Require.** 모든 클라이언트의 사용자 이름을 요청하지만 생략할 수 있습니다. 이 옵션은 로깅 용도로만 ID를 사용합니다.
  - **Require.** 모든 클라이언트의 사용자 이름을 요청하며 응답이 유효한 경우에만 액세스를 허용합니다.

8 SOCKS Tuning 섹션은 SOCKS 서버가 사용해야 하는 작업자 및 승인 스레드의 수를 지정합니다. 이 수는 SOCKS 서버의 성능에 영향을 줍니다. OK를 누릅니다.

- **Number Of Worker Threads.** 기본값은 40입니다. SOCKS 서버가 너무 느리면 작업자 스레드의 수를 늘리십시오. 서버가 불안정하면 수를 줄이십시오. 이 수를 변경하는 경우 기본값부터 시작하여 필요에 따라 늘리거나 줄입니다. 일반적으로 작업자 스레드의 수는 10과 150 사이입니다. 최대 512까지 설정할 수 있지만 150을 초과하면 효율성이 떨어지고 불안정해집니다.
  - **Number Of Posted Accepts.** 기본값은 1입니다. SOCKS 서버의 연결이 끊어지면 승인 스레드의 수를 늘리십시오. 서버가 불안정하면 서버 수를 줄이십시오. 이 수를 변경하는 경우 기본값부터 시작하여 필요에 따라 늘리거나 줄입니다. 일반적으로 승인 스레드의 수는 1과 10 사이입니다. 최대 512까지 설정할 수 있지만 60을 넘으면 효율성이 떨어지고 불안정해집니다. SOCKS 서버에 부하가 있을 때 요청이 실패하고 연결이 끊기는 경우 이 설정을 조정하십시오.

SOCKS v5 인증 항목 구성

SOCKS 인증 항목은 SOCKS 데몬이 연결을 승인해야 하는 호스트와 SOCKS 데몬이 해당 호스트를 인증할 때 사용할 인증 유형을 식별합니다.

▼ SOCKS 인증 항목을 만드는 방법

1. **서버 인스턴스에 대한 Server Manager에 액세스하고 SOCKS 탭을 누릅니다.**
2. **Set SOCKS v5 Authentication 링크를 누릅니다.**
3. **Add 버튼을 누릅니다.**
4. **Host Mask 필드에 SOCKS 서버가 인증할 호스트의 IP 주소나 호스트 이름을 입력합니다.**

   IP 주소를 입력하는 경우 주소 뒤에 슬래시(/)와 수신 IP 주소에 적용할 마스크를 입력합니다. SOCKS 서버는 이 마스크를 IP 주소에 적용하여 유효한 호스트인지 확인합니다. 호스트 마스크 항목에 공백을 사용하지 마십시오. 호스트 마스크를 입력하지 않으면 모든 호스트에 인증 항목이 적용됩니다.

   예를 들어, 호스트 마스크 필드에 155.25.0.0/255.255.0.0을 입력합니다. 호스트의 IP 주소가 155.25.3.5인 경우 SOCKS 서버는 해당 IP 주소에 마스크를 적용하고 호스트의 IP 주소가 인증 레코드가 적용되는 IP 주소(155.25.0.0)와 일치하는지 확인합니다.
5. **Port Range 필드에 SOCKS 서버가 인증할 호스트 컴퓨터의 포트를 입력합니다.**

   포트 범위 항목에 공백을 사용하지 마십시오. 포트 범위를 제공하지 않으면 모든 포트에 인증 항목이 적용됩니다.

   대괄호 [ ]를 사용하여 범위의 각 끝에 있는 포트를 포함하거나 괄호 ()를 사용하여 각 끝 포트를 제외할 수 있습니다. 예를 들어, [1000-1010]은 1000과 1010 사이(1000 및 1010 포함)의 모든 포트 번호를 의미하고 (1000-1010)은 해당 범위에서 1000과 1010을 제외한

모든 포트 번호를 의미합니다. 대괄호와 괄호를 함께 사용할 수도 있습니다. 예를 들어, (1000-1010]은 1000은 제외하고 1010은 포함한, 1000과 1010 사이의 모든 번호를 의미합니다.

6 **Authentication Type 드롭다운 목록에서 인증 유형을 선택합니다.**

다음 옵션을 사용할 수 있습니다.

- **Require user-password.** SOCKS 서버에 액세스하려면 사용자 이름 및 비밀번호가 필요합니다.
- **User-password, if available.** 사용자 이름 및 비밀번호가 있는 경우에는 이를 사용해야 하지만 없는 경우에도 SOCKS 서버에 액세스할 수 있습니다.
- **Ban.** SOCKS 서버에서 차단됩니다.
- **None.** SOCKS 서버에 액세스하는 데 인증이 필요하지 않습니다.

7 **Insert 드롭다운 목록에서 `socks5.conf` 파일에서 이 항목의 위치를 선택한 다음 OK를 누릅니다.**

여러 인증 방법이 있을 수 있으므로 평가할 순서를 지정해야 합니다. 따라서 클라이언트가 나열된 첫 번째 인증 방법을 지원하지 않으면 두 번째 방법이 대신 사용됩니다. 클라이언트가 나열된 인증 방법을 모두 지원하지 않으면 SOCKS 서버는 요청을 수락하지 않고 연결을 해제합니다.

▼ 인증 항목 편집 방법

1 **서버 인스턴스에 대한 Server Manager에 액세스하고 SOCKS 탭을 누릅니다.**

2 **Set SOCKS v5 Authentication 링크를 누릅니다.**

3 **편집할 인증 항목을 선택하고 Edit 버튼을 누릅니다.**

4 **원하는 대로 변경합니다.**

5 **OK를 누릅니다.**

▼ 인증 항목 삭제 방법

1 **서버 인스턴스에 대한 Server Manager에 액세스하고 SOCKS 탭을 누릅니다.**

2 **Set SOCKS v5 Authentication 링크를 누릅니다.**

3 **삭제할 인증 항목을 선택합니다.**

4 **Delete 버튼을 누릅니다.**

▼ 인증 항목 이동 방법

항목은 `socks5.conf` 파일에 나타나는 순서대로 평가됩니다. 항목을 이동하여 순서를 변경할 수 있습니다.

1 **서버 인스턴스에 대한 Server Manager에 액세스하고 SOCKS 탭을 누릅니다.**

2 **Set SOCKS v5 Authentication 링크를 누릅니다.**

3 **이동할 인증 항목을 선택하고 Move 버튼을 누릅니다.**

4 **Move 드롭다운 목록에서 `socks5.conf` 파일에서 이 항목의 위치를 선택합니다.**

5 **OK를 누릅니다.**

SOCKS v5 연결 항목 구성

SOCKS 연결 항목은 SOCKS 데몬이 요청을 허용할 것인지 거부할 것인지 여부를 지정합니다.

▼ 연결 항목 만드는 방법

1 **서버 인스턴스에 대한 Server Manager에 액세스하고 SOCKS 탭을 누릅니다.**

2 **Set SOCKS v5 Connections 링크를 누릅니다.**

3 **Add 버튼을 누릅니다.**

4 **Authentication Type 드롭다운 목록에서 이 액세스 제어 행을 적용할 인증 방법을 선택합니다.**

5 **Connection Type 드롭다운 목록에서 해당 행과 일치하는 명령의 유형을 선택합니다. 가능한 명령 유형은 다음과 같습니다.**

- **Connect**
  - **Bind**
  - **UDP**
  - **All**

6 Source Host Mask 필드에 연결 제어 항목을 적용할 호스트의 호스트 이름이나 IP 주소를 입력합니다.

IP 주소를 입력하는 경우 주소 뒤에 슬래시(/)와 소스의 IP 주소에 적용할 마스크를 입력합니다. SOCKS 서버는 이 마스크를 소스의 IP 주소에 적용하여 유효한 호스트인지 확인합니다. 호스트 마스크 항목에 공백을 사용하지 마십시오. 호스트 마스크를 입력하지 않으면 모든 호스트에 연결 항목이 적용됩니다.

예를 들어, 호스트 마스크 필드에 155.25.0.0/255.255.0.0을 입력합니다. 호스트의 IP 주소가 155.25.3.5인 경우 SOCKS 서버는 해당 IP 주소에 마스크를 적용하고 호스트의 IP 주소가 연결 제어 항목이 적용되는 IP 주소(155.25.0.0)와 일치하는지 확인합니다.

7 Port Range 필드에 연결 제어 항목을 적용할 소스 컴퓨터의 포트를 입력합니다.

포트 범위 항목에 공백을 사용하지 마십시오. 포트 범위를 지정하지 않으면 모든 포트에 연결 항목이 적용됩니다.

대괄호 [ ]를 사용하여 범위의 각 끝에 있는 포트를 포함하거나 괄호 ()를 사용하여 각 끝 포트를 제외할 수 있습니다. 예를 들어, [1000-1010]은 1000과 1010 사이(1000 및 1010 포함)의 모든 포트 번호를 의미하고 (1000-1010)은 해당 범위에서 1000과 1010을 제외한 모든 포트 번호를 의미합니다. 대괄호와 괄호를 함께 사용할 수도 있습니다. 예를 들어, (1000-1010]은 1000은 제외하고 1010은 포함한, 1000과 1010 사이의 모든 번호를 의미합니다.

8 Destination Host Mask 필드에 연결 항목을 적용할 IP 주소 또는 호스트 이름을 입력합니다.

IP 주소를 입력하는 경우 주소 뒤에 슬래시(/)와 수신 IP 주소에 적용할 마스크를 입력합니다. SOCKS 서버는 이 마스크를 대상 컴퓨터의 IP 주소에 적용하여 유효한 대상 호스트인지 확인합니다. 호스트 마스크 항목에 공백을 사용하지 마십시오. 대상 호스트 마스크를 입력하지 않으면 모든 호스트에 연결 항목이 적용됩니다.

예를 들어, 대상 호스트 마스크 필드에 155.25.0.0/255.255.0.0을 입력합니다. 대상 호스트의 IP 주소가 155.25.3.5인 경우 SOCKS 서버는 해당 IP 주소에 마스크를 적용하고 대상 호스트의 IP 주소가 프록시 항목이 적용되는 IP 주소(155.25.0.0)와 일치하는지 확인합니다.

9 Port Range 필드에 연결 제어 항목을 적용할 대상 호스트 컴퓨터의 포트를 입력합니다.

포트 범위 항목에 공백을 사용하지 마십시오. 포트 범위를 입력하지 않으면 모든 포트에 연결 항목이 적용됩니다.

주 – 대부분의 SOCKS 응용 프로그램은 바인드 요청에 대해 포트 0을 요청합니다. 즉, 포트 기본 설정이 없음을 의미합니다. 따라서 바인드를 위한 대상 포트 범위에는 항상 포트 0이 포함되어야 합니다.

대괄호 [ ]를 사용하여 범위의 각 끝에 있는 포트를 포함하거나 괄호 ()를 사용하여 각 끝 포트를 제외할 수 있습니다. 예를 들어, [1000-1010]은 1000과 1010 사이(1000 및 1010 포함)의 모든 포트 번호를 의미하고 (1000-1010)은 해당 범위에서 1000과 1010을 제외한

모든 포트 번호를 의미합니다. 대괄호와 괄호를 함께 사용할 수도 있습니다. 예를 들어, (1000-1010]은 1000은 제외하고 1010은 포함한, 1000과 1010 사이의 모든 번호를 의미합니다.

10 **User Group 필드에 액세스를 허용하거나 거부할 그룹을 입력합니다.**
그룹을 지정하지 않으면 모든 사용자에게 연결 항목이 적용됩니다.

11 **Action 드롭다운 목록에서 현재 만들고 있는 연결에 대한 액세스를 허용할 것인지 또는 거부할 것인지 여부를 선택합니다.**

12 **Insert 드롭다운 목록에서 `socks5.conf` 파일에서 이 항목의 위치를 선택한 다음 OK를 누릅니다.**
여러 연결 지시문이 있을 수 있으므로 평가할 순서를 지정해야 합니다.

▼ 연결 항목 편집 방법

1 **서버 인스턴스에 대한 Server Manager에 액세스하고 SOCKS 탭을 누릅니다.**

2 **Set SOCKS v5 Connections 링크를 누릅니다.**

3 **편집할 연결 항목을 선택하고 Edit 버튼을 누릅니다.**

4 **원하는 대로 변경합니다.**

5 **OK를 누릅니다.**

▼ 연결 항목 삭제 방법

1 **서버 인스턴스에 대한 Server Manager에 액세스하고 SOCKS 탭을 누릅니다.**

2 **Set SOCKS v5 Connections 링크를 누릅니다.**

3 **삭제할 연결 항목을 선택합니다.**

4 **Delete 버튼을 누릅니다.**

▼ 연결 항목 이동 방법

항목은 socks5.conf 파일에 나타나는 순서대로 평가됩니다. 항목을 이동하여 순서를 변경할 수 있습니다.

1. **서버 인스턴스에 대한 Server Manager에 액세스하고 SOCKS 탭을 누릅니다.**
2. **Set SOCKS v5 Connections 링크를 누릅니다.**
3. **이동할 연결 항목을 선택합니다.**
4. **Move 버튼을 누릅니다.**
5. **Move 드롭다운 목록에서 socks5.conf 파일에서 이 항목의 위치를 선택하고 OK를 누릅니다.**

SOCKS v5 서버 체인 구성

SOCKS 서버는 프록시 서버에서와 같은 방법을 사용하여 체인될 수 있습니다. 즉, SOCKS 서버가 다른 SOCKS 서버를 통해 라우팅할 수 있습니다.

▼ SOCKS 서버 체인 구성 방법

1. **서버 인스턴스에 대한 Server Manager에 액세스하고 SOCKS 탭을 누릅니다.**
2. **Set SOCKS v5 Routing 링크를 누릅니다.**
3. **프록시 체인의 다운스트림 프록시에서 요청을 서비스하기 위해 인증을 요구하는 경우, Server Chaining 섹션에 체인된 프록시 서버를 인증하기 위한 사용자 이름과 비밀번호를 입력합니다. OK를 누릅니다.**

라우팅 항목 구성

라우팅 항목을 사용하면 SOCKS 서버를 통해 요청을 라우팅하도록 Proxy Server를 구성할 수 있습니다. 라우팅 항목에는 두 가지 유형(SOCKS v5 라우팅 및 SOCKS v5 프록시 라우팅)이 있습니다.

- SOCKS v5 라우팅은 SOCKS 데몬이 특정 IP 주소에 사용해야 할 인터페이스를 식별합니다.
- SOCKS v5 프록시 라우팅은 다른 SOCKS 서버를 통해 액세스할 수 있는 IP 주소와 SOCKS 서버가 호스트에 직접 연결되는지 여부를 식별합니다. 프록시 라우팅은 SOCKS 서버를 통해 라우팅할 때 중요합니다.

▼ 라우팅 항목 만드는 방법

1 **서버 인스턴스에 대한 Server Manager에 액세스하고 SOCKS 탭을 누릅니다.**

2 **Set SOCKS v5 Routing 링크를 누릅니다.**

3 **Routing 섹션에서 Add 버튼을 누릅니다.**

4 **Host Mask 필드에 수신 및 전송 연결이 지정된 인터페이스를 통과해야 하는 IP 주소나 호스트 이름을 입력합니다.**

IP 주소를 입력하는 경우 주소 뒤에 슬래시(/)와 수신 IP 주소에 적용할 마스크를 입력합니다. SOCKS 서버는 이 마스크를 IP 주소에 적용하여 유효한 호스트인지 확인합니다. 호스트 마스크 항목에 공백을 사용하지 마십시오. 호스트 마스크를 제공하지 않으면 모든 호스트에 SOCKS v5 항목이 적용됩니다.

예를 들어, 호스트 마스크 필드에 155.25.0.0/255.255.0.0을 입력합니다. 호스트의 IP 주소가 155.25.3.5인 경우 SOCKS 서버는 해당 IP 주소에 마스크를 적용하고 호스트의 IP 주소가 라우팅 항목이 적용되는 IP 주소(155.25.0.0)와 일치하는지 확인합니다.

5 **Port Range 필드에 수신 및 전송 연결이 지정된 인터페이스를 통과해야 하는 포트를 입력합니다. 포트 범위에는 공백이 없어야 합니다.**

포트 범위를 지정하지 않으면 모든 포트에 SOCKS v5 항목이 적용됩니다.

대괄호 [ ]를 사용하여 범위의 각 끝에 있는 포트를 포함하거나 괄호 ()를 사용하여 각 끝 포트를 제외할 수 있습니다. 예를 들어, [1000-1010]은 1000과 1010 사이(1000 및 1010 포함)의 모든 포트 번호를 의미하고 (1000-1010)은 해당 범위에서 1000과 1010을 제외한 모든 포트 번호를 의미합니다. 대괄호와 괄호를 함께 사용할 수도 있습니다. 예를 들어, (1000-1010]은 1000은 제외하고 1010은 포함한, 1000과 1010 사이의 모든 번호를 의미합니다.

6 **Interface/Address 필드에 수신 및 전송 연결이 통과해야 하는 인터페이스의 IP 주소 또는 이름을 입력합니다.**

7 **Insert 드롭다운 목록에서 `socks5.conf` 파일에서 이 항목의 위치를 선택한 다음 OK를 누릅니다.**

여러 라우팅 방법이 있을 수 있으므로 평가할 순서를 지정해야 합니다.

주 – 지정된 인터페이스는 수신 및 전송 연결 모두에 사용되어야 하며, 그렇지 않으면 수신 라우팅과 구성된 인터페이스가 다르기 때문에 오류 메시지가 수신됩니다.

▼ 프록시 라우팅 항목 만드는 방법

1. **서버 인스턴스에 대한 Server Manager에 액세스하고 SOCKS 탭을 누릅니다.**
2. **Set SOCKS v5 Routing 링크를 누릅니다.**
3. **Proxy Routing 섹션에서 Add 버튼을 누릅니다.**
4. **Proxy Type 드롭다운 목록에서 라우팅에 사용할 Proxy Server의 유형을 선택합니다. 다음 옵션을 사용할 수 있습니다.**
   - **SOCKS v5**
     - **SOCKS v4**
     - **Direct connection**
5. **Destination Host Mask 필드에 연결 항목을 적용할 IP 주소 또는 호스트 이름을 입력합니다.**

   IP 주소를 입력하는 경우 주소 뒤에 슬래시(/)와 수신 IP 주소에 적용할 마스크를 입력합니다. SOCKS 서버는 이 마스크를 대상 컴퓨터의 IP 주소에 적용하여 유효한 대상 호스트인지 확인합니다. 호스트 마스크 항목에 공백을 사용하지 마십시오. 대상 호스트 마스크를 제공하지 않으면 모든 호스트에 연결 항목이 적용됩니다.

   예를 들어, 대상 호스트 마스크 필드에 155.25.0.0/255.255.0.0을 입력합니다. 대상 호스트의 IP 주소가 155.25.3.5인 경우 SOCKS 서버는 해당 IP 주소에 마스크를 적용하고 대상 호스트의 IP 주소가 프록시 항목이 적용되는 IP 주소(155.25.0.0)와 일치하는지 확인합니다.
6. **Destination Port Range 필드에 프록시 항목을 적용할 대상 호스트의 포트를 입력합니다.**

   포트 범위 항목에 공백을 사용하지 마십시오. 포트 범위를 지정하지 않으면 모든 포트에 프록시 항목이 적용됩니다.

   대괄호 [ ]를 사용하여 범위의 각 끝에 있는 포트를 포함하거나 괄호 ()를 사용하여 각 끝 포트를 제외할 수 있습니다. 예를 들어, [1000-1010]은 1000과 1010 사이(1000 및 1010 포함)의 모든 포트 번호를 의미하고 (1000-1010)은 해당 범위에서 1000과 1010을 제외한 모든 포트 번호를 의미합니다. 대괄호와 괄호를 함께 사용할 수도 있습니다. 예를 들어, (1000-1010]은 1000은 제외하고 1010은 포함한, 1000과 1010 사이의 모든 번호를 의미합니다.
7. **Destination Proxy Address 필드에 사용할 Proxy Server의 호스트 이름이나 IP 주소를 입력합니다.**
8. **Destination Proxy Port 필드에 프록시 서버가 SOCKS 요청을 수신할 포트 번호를 입력합니다.**

9 **Insert 드롭다운 목록에서 `socks5.conf` 파일에서 이 항목의 위치를 선택한 다음 OK를 누릅니다.**

여러 라우팅 방법이 있을 수 있으므로 평가할 순서를 지정해야 합니다.

▼ 라우팅 항목 편집 방법

1 **서버 인스턴스에 대한 Server Manager에 액세스하고 SOCKS 탭을 누릅니다.**

2 **Set SOCKS v5 Routing 링크를 누릅니다.**

3 **편집할 항목을 선택합니다.**

4 **Edit 버튼을 누릅니다.**

5 **원하는 대로 변경합니다.**

6 **OK를 누릅니다.**

▼ 라우팅 항목 삭제 방법

1 **서버 인스턴스에 대한 Server Manager에 액세스하고 SOCKS 탭을 누릅니다.**

2 **Set SOCKS v5 Routing 링크를 누릅니다.**

3 **삭제할 항목을 선택합니다.**

4 **Delete 버튼을 누릅니다.**

▼ 라우팅 항목 이동 방법

항목은 `socks5.conf` 파일에 나타나는 순서대로 평가됩니다. 항목을 이동하여 순서를 변경할 수 있습니다.

1 **서버 인스턴스에 대한 Server Manager에 액세스하고 SOCKS 탭을 누릅니다.**

2 **Set SOCKS v5 Routing 링크를 누릅니다.**

3 **이동할 항목을 선택합니다.**

4 **Move 버튼을 누릅니다.**

5 **Move 드롭다운 목록에서 `socks5.conf` 파일에서 이 항목의 위치를 선택하고 OK를 누릅니다.**

◆ ◆ ◆ 16 장

16 템플리트 및 자원 관리

템플리트를 사용하면 URL을 함께 그룹화하여 프록시가 해당 URL을 처리하는 방법을 구성할 수 있습니다. 클라이언트가 검색하려는 URL에 따라 프록시가 다르게 동작하도록 구성할 수 있습니다. 예를 들어, 클라이언트가 특정 도메인의 URL에 액세스할 때 사용자 이름 및 비밀번호를 반드시 입력하도록 요구할 수 있습니다. 또는 이미지 파일을 가리키는 URL에 대한 액세스를 거부할 수 있습니다. 파일 유형에 따라 서로 다른 캐시 새로 고침 설정을 구성할 수 있습니다.

이 장은 다음 내용으로 구성되어 있습니다.

- 325 페이지 “템플리트 정보”
- 328 페이지 “템플리트 작업”
- 330 페이지 “자원 제거”

템플리트 정보

템플리트는 URL의 모음이며 자원이라고 합니다. 자원은 단일 URL, 공통 사항이 있는 URL의 그룹 또는 전체 프로토콜일 수 있습니다. 템플리트의 이름을 지정하고 만든 다음 정규 표현식을 사용하여 해당 템플리트에 URL을 할당합니다. 이러한 방법으로 다양한 URL 요청을 서로 다르게 처리하도록 프록시 서버를 구성할 수 있습니다. 정규 표현식으로 만들 수 있는 모든 URL 패턴은 템플리트에 포함할 수 있습니다. 다음 표에서는 기본 자원을 나열하고 다른 템플리트에 대한 몇 가지 아이디어를 제공합니다.

표 16–1 자원 정규 표현식 와일드카드 패턴

정규 표현식 패턴	구성 대상
`ftp://.*`	모든 FTP 요청
`http://.*`	모든 HTTP 요청
`https://.*`	모든 보안 HTTP 요청

표 16–1 자원 정규 표현식 와일드카드 패턴 *(계속)*

정규 표현식 패턴	구성 대상
`gopher://.*`	모든 Gopher 요청
`connect://.*:443`	HTTPS 포트에 대한 모든 SSL(보안) 트랜잭션
`http://home\.example\.com.*`	`home.example.com` 웹 사이트의 모든 문서
`.*\.gif.*`	`.gif` 문자열을 포함하는 모든 URL
`.*\.edu.*`	`.edu` 문자열을 포함하는 모든 URL
`http://.*\.edu.*`	`.edu` 도메인의 컴퓨터로 이동하는 모든 URL

정규 표현식 이해

Proxy Server에서는 정규 표현식을 사용하여 자원을 식별할 수 있습니다. 정규 표현식은 문자열의 패턴을 지정합니다. 프록시 서버에서 정규 표현식은 URL에서 일치하는 패턴을 찾는 데 사용됩니다.

다음은 정규 표현식의 예입니다.

```
[a-z]*://[^:/]*\.abc\.com.*
```

이 정규 표현식은 `.abc.com` 도메인의 모든 문서와 일치합니다. 문서는 모든 프로토콜일 수 있으며 파일 확장자에 제한이 없습니다.

다음 표에서는 정규 표현식 및 해당 의미를 나열합니다.

표 16–2 정규 표현식 및 의미

표현식	의미
.	새 행을 제외하고 모든 단일 문자가 일치합니다.
x?	정규 표현식 *x*가 0 또는 1회 일치합니다.
*x**	정규 표현식 *x*가 0회 이상 일치합니다.
x+	정규 표현식 *x*가 1회 이상 일치합니다.
x{n,m}	*x* 문자가 일치합니다. 여기서 *x*는 최소 *n*회 이상 *m*회 이하 발생합니다.
x{n,}	*x* 문자가 일치합니다. 여기서 *x*는 최소 *n*회 발생합니다.
x{n}	*x* 문자가 일치합니다. 여기서 *x*는 정확하게 *n*회 발생합니다.
[abc]	대괄호 안의 모든 문자가 일치합니다.
[^abc]	대괄호 밖의 모든 문자가 일치합니다.

표 16–2 정규 표현식 및 의미 (계속)

표현식	의미
[a-z]	대괄호의 범위 내에 있는 모든 문자가 일치합니다.
x	*x*문자가 일치합니다. 여기서 *x*는 특수 문자가 아닙니다.
\x	특수 문자 *x*의 의미를 제거합니다.
"x"	특수 문자 *x*의 의미를 제거합니다.
xy	정규 표현식 *x* 발생 및 정규 표현식 *y* 발생이 일치합니다.
x|y	정규 표현식 *x* 또는 정규 표현식 *y*가 일치합니다.
^	문자열의 시작이 일치합니다.
$	문자열의 끝이 일치합니다.
(x)	정규 표현식을 그룹화합니다.

이 예는 326 페이지 "정규 표현식 이해"의 정규 표현식을 사용하는 몇 가지 방법을 보여 줍니다.

```
[a-z]*://([^.:/]*[:/]|.*\.local\.com).*
```

- `[a-z]*`는 모든 프로토콜의 문서와 일치합니다.
- `://`는 (:) 및(//)와 일치합니다.
- `[^.:/]*[:/]`는 (.),(:)또는 (/)를 포함하지 않고 뒤에 (:) 또는 (/)가 있는 모든 문자열과 일치합니다. 따라서 이 표현식은 정규화되지 않은 호스트 이름과 포트 번호가 있는 호스트와 일치합니다.
- `|.*\.local\.com`은 `local.com`과 같은 정규화된 도메인 이름 호스트 이름과 일치하지 않지만 `.local.com` 도메인의 문서와 일치합니다.
- `.*`는 모든 파일 확장자의 문서와 일치합니다.

326 페이지 "정규 표현식 이해"에 언급한 것과 같이 역슬래시(\)를 사용하여 특수 문자의 의미를 이스케이프하거나 제거할 수 있습니다. 마침표나 물음표와 같은 문자에는 특수 의미가 있으므로 자체 의미를 나타내는 경우에는 이스케이프해야 합니다. 특히 마침표는 많은 URL에 사용됩니다. 따라서 정규 표현식에서 마침표의 특수 의미를 제거하려면 앞에 역슬래시를 추가해야 합니다.

와일드카드 패턴 이해

사이트에서 액세스할 수 있는 URL을 지정할 수 있는 와일드카드 패턴 목록을 만들 수 있습니다. 와일드카드는 사용 방법에 따라 정규 표현식 또는 쉘 표현식의 형태가 될 수 있습니다. 일반적인 규칙은 다음과 같습니다.

- 대상 URL과 일치하는 모든 패턴에 정규 표현식을 사용합니다. 여기에는 <Object ppath=...>, URL 필터와 NameTrans, PathCheck 및 ObjectType 함수가 포함됩니다.
- 액세스 제어를 위한 사용자 이름과 그룹 및 들어오는 사용자의 IP 주소나 DNS 이름을포함하여 들어오는 클라이언트 또는 사용자 아이디가 일치하는 모든 패턴에 쉘 표현식을 사용합니다(예: <Client dns=...>).

정규 표현식 와일드카드 패턴을 사용하여 여러 URL을 지정할 수 있습니다. 와일드카드를 사용하면 도메인 이름 또는 URL(URL에 특정 단어 포함)을 기준으로 필터링할 수 있습니다. 예를 들어, "careers" 라는 문자열이 포함된 URL에 대한 액세스를 차단해야 하는 경우가 있습니다. 이렇게 하려면 템플리트에 대한 정규 표현식으로 `http://.*careers.*` 를 지정합니다.

템플리트 작업

▼ 템플리트 만드는 방법

정규 표현식 와일드카드 패턴을 사용하여 템플리트를 만들 수 있습니다. 그런 다음 해당 템플리트에 지정된 URL에만 적용되는 측면을 구성할 수 있습니다. 예를 들어, `.GIF` 이미지에 대해 한 가지 유형의 캐시 구성을 사용하고 일반 `.html` 파일에 대해서는 다른 유형을 사용할 수 있습니다.

1 Server Manager에 액세스하고 Templates 탭을 누릅니다.

Create Template 링크를 누릅니다. Create Template 페이지가 표시됩니다.

2 Template Name 필드에 만들 템플리트의 이름을 입력하고 OK를 누릅니다.

쉽게 기억할 수 있는 이름이어야 합니다. Server Manager에서 변경 사항을 저장하고 적용하도록 프롬프트가 표시됩니다. 나머지 단계에서 설명된 대로 템플리트에 대한 정규 표현식을 만든 후 변경 사항을 저장할 수 있습니다.

▼ 템플리트 적용 방법

1 Server Manager에 액세스하고 Templates 탭을 누릅니다.

2 Apply Template 링크를 누릅니다.

Apply Template 페이지가 표시됩니다.

3 URL Prefix Wildcard 필드에 템플리트에 포함할 모든 URL을 포함하도록 정규 표현식 와일드카드 패턴을 입력합니다.

4 Template 목록에서 방금 추가한 새 템플리트의 이름을 선택합니다.

5 **OK를 누릅니다.**

6 **Restart Required를 누릅니다.**
Apply Changes 페이지가 표시됩니다.

7 **Restart Proxy Server 버튼을 눌러 변경 사항을 적용합니다.**

▼ 템플리트 제거 방법

기존 템플리트를 제거할 수 있습니다. 템플리트를 제거하면 해당 템플리트에 대한 연결 구성이 모두 삭제됩니다. 예를 들어, TEST 템플리트에서 모든 URL에 대해 액세스 제어를 설정한 경우 TEST 템플리트를 제거하면 해당 템플리트에 포함된 URL에 대한 액세스 제어도 제거됩니다.

1 **Server Manager에 액세스하고 Templates 탭을 누릅니다.**

2 **Remove Template 링크를 누릅니다.**
Remove Template 페이지가 표시됩니다.

3 **Remove 목록에서 템플리트를 선택합니다.**

4 **OK를 누릅니다.**

5 **Restart Required를 누릅니다.**
Apply Changes 페이지가 표시됩니다.

6 **Restart Proxy Server 버튼을 눌러 변경 사항을 적용합니다.**

▼ 템플리트 편집 방법

Server Manager에서 만든 템플리트를 보고 편집할 수 있습니다.

1 **Server Manager에 액세스하고 Templates 탭을 누릅니다.**

2 **View Template 링크를 누릅니다.**
View Template 페이지가 표시됩니다. 템플리트 이름 및 템플리트에 대한 정규 표현식이 나열되는 표에 템플리트가 표시됩니다.

3 **기존 템플리트를 편집하려면 Edit Template Assignment 링크를 누릅니다. Apply Template 페이지가 표시됩니다.**

자원 제거

Remove Resource 페이지를 사용하면 전체 정규 표현식 객체 및 해당 구성을 삭제할 수 있습니다. 예를 들어, gopher 자원을 제거하여 해당 자원과 연결된 모든 설정을 프록시 서버의 구성 파일에서 제거되도록 할 수 있습니다.

▼ 자원 제거

1. **Server Manager에 액세스하고 Templates 탭을 누릅니다.**
2. **Remove Resource 링크를 누릅니다.**
   Remove Resource 페이지가 표시됩니다.
3. **Remove 드롭다운 목록에서 제거할 자원을 선택합니다.**
4. **OK를 누릅니다.**
5. **Restart Required를 누릅니다.**
   Apply Changes 페이지가 표시됩니다.
6. **Restart Proxy Server 버튼을 눌러 변경 사항을 적용합니다.**

◆ ◆ ◆ 17 장

17 클라이언트 자동 구성 파일 사용

여러 클라이언트를 지원하는 프록시 서버가 여러 개 있는 경우 클라이언트 자동 구성 파일을 사용하여 브라우저 클라이언트의 모든 항목을 구성할 수 있습니다. 자동 구성 파일에는 브라우저가 다양한 URL에 액세스할 때 사용하는 프록시(있는 경우)를 결정하는 JavaScript 함수가 포함되어 있습니다.

브라우저를 시작하면 자동 구성 파일이 로드됩니다. 사용자가 링크를 누르거나 URL에 입력할 때마다 브라우저는 구성 파일을 사용하여 프록시를 사용해야 하는지 여부를 결정하고 사용해야 하는 경우 사용할 프록시를 결정합니다. 이 기능을 통해 조직의 브라우저에 대한 모든 인스턴스를 쉽게 구성할 수 있습니다. 자동 구성 파일을 클라이언트로 가져올 수 있는 여러 가지 방법이 있습니다.

- 프록시 서버를 자동 구성 파일을 반환하는 웹 서버로 사용할 수 있습니다. 브라우저를 프록시의 URL로 지정합니다. 프록시를 웹 서버로 사용하면 자동 구성 파일을 한 위치에 보관할 수 있으므로 업데이트가 필요한 경우 하나의 파일만 변경하면 됩니다.
- 브라우저가 액세스 권한을 가진 웹 서버, FTP 서버 또는 네트워크 디렉토리에 파일을 저장할 수 있습니다. 일반 URL을 사용할 수 있도록 파일에 URL을 제공하여 브라우저가 파일을 찾도록 구성합니다. 예를 들어 조직에 대용량 프록시 체인이 있는 것과 같이 복잡한 계산을 수행해야 하는 경우 파일에 액세스하는 사용자에 따라 다른 파일을 출력하는 웹 서버 CGI 프로그램을 작성할 수 있습니다.
- 각 브라우저 복사본과 함께 자동 구성 파일을 로컬로 저장할 수 있습니다. 그러나 파일을 업데이트해야 하는 경우 파일 복사본을 각 클라이언트에 배포해야 합니다.

다음과 같이 두 가지 방법으로 자동 구성 파일을 만들 수 있습니다. Server Manager의 페이지를 사용하거나 파일을 직접 만들 수 있습니다. 파일을 만들기 위한 지시문에 대해서는 이 장의 뒷부분에서 설명합니다.

이 장은 다음 내용으로 구성되어 있습니다.

- 332 페이지 “자동 구성 파일 이해”
- 334 페이지 “Server Manager 페이지를 사용하여 자동 구성 파일 만들기”
- 336 페이지 “수동으로 자동 구성 파일 만들기”

자동 구성 파일 이해

또한 Proxy Server를 관리하는 사용자로서 클라이언트 자동 구성 파일을 만들고 배포합니다.

자동 구성 파일의 기능

자동 구성 파일은 클라이언트 및 서버 인터넷 응용 프로그램 개발용 소형 객체 기반 스크립팅 언어인 JavaScript로 작성됩니다. 브라우저는 JavaScript 파일을 해석합니다.

브라우저를 처음으로 로드하면 자동 구성 파일이 다운로드됩니다. 파일은 브라우저가 URL을 사용하여 접근할 수 있는 모든 위치에 보관할 수 있습니다. 예를 들어 파일을 웹 서버에 보관할 수 있습니다. 브라우저가 파일 `://` `URL`을 사용하여 접근할 수 있는 경우 파일을 네트워크 파일 시스템에 보관할 수도 있습니다.

프록시 구성 파일은 JavaScript로 작성됩니다. JavaScript 파일은 브라우저가 각 URL에 대해 사용해야 하는 프록시 서버(있는 경우)를 결정하는 단일 함수(*FindProxyForURL*이라고 함)를 정의합니다. 브라우저는 브라우저가 실행되고 있는 시스템의 호스트 이름 및 가져올 URL의 두 가지 매개 변수를 JavaScript 함수로 보냅니다. JavaScript 함수는 진행 방법을 알려 주는 브라우저에 값을 반환합니다.

자동 구성 파일을 사용하여 다양한 유형의 URL, 여러 서버 또는 하루 중 다양한 시간에 대해 서로 다른 프록시를 지정하거나 프록시를 전혀 지정하지 않을 수 있습니다. 즉, 여러 개의 세분화된 프록시를 가질 수 있는데, 예를 들면 어떤 한 프록시는 `.com` 도메인에 서비스를 제공하고 다른 프록시는 `.edu` 도메인에 서비스를 제공하고 또 다른 프록시는 그 이외의 모든 도메인에 서비스를 제공하는 것과 같습니다. 이 방법을 사용하면 여러 프록시가 모두 동일한 문서를 저장하는 대신 단일 파일 복사본만 캐시에 저장되기 때문에 로드를 나누고 프록시 디스크를 보다 효율적으로 사용할 수 있습니다.

또한 자동 구성 파일은 프록시 페일오버를 지원하기 때문에 프록시 서버를 사용할 수 없는 경우 브라우저가 자연스럽게 다른 프록시 서버로 전환됩니다.

Web Server로 프록시에 액세스

프록시 서버에 하나 이상의 자동 구성 파일을 저장할 수 있으며 프록시 서버가 문서만 자동 구성 파일인 웹 서버의 역할을 수행하게 할 수 있습니다. 이렇게 하면 프록시 관리자가 조직의 클라이언트에 필요한 프록시 자동 구성 파일을 유지 관리할 수 있습니다. 또한 파일을 중앙 위치에 보관할 수 있기 때문에 파일을 업데이트해야 하는 경우 한 번만 업데이트하면 모든 브라우저 클라이언트가 자동으로 업데이트 파일을 얻게 됩니다.

프록시 자동 구성 파일은 *server- root*/proxy-server*id*/pac/ 디렉토리에 보관합니다. 브라우저에서 Proxies 탭에 파일의 URL을 입력하는 프록시 자동 구성 파일에 대한 URL을 입력합니다. 프록시의 URL 형식은 다음과 같습니다.

`http://`*proxy.domain:port/URI*

예를 들어 URL은 `http://proxy.example.com`이 될 수 있습니다. 호스트:포트 조합 다음에 URL의 일부로 URI를 사용하는 경우 템플리트를 사용하여 다양한 자동 구성 파일에 대한 액세스를 제어할 수 있습니다. 예를 들어 `/proxy.pac`라고 하는 자동 구성 파일이 포함된 `/test`라는 URI를 만드는 경우 자원 패턴이 `http://proxy.mysite.com:8080/test/.*`인 템플리트를 만들 수 있습니다. 이 템플리트를 사용하여 해당 디렉토리에 적합한 액세스 제어를 설정할 수 있습니다.

자동 구성 파일을 여러 개 만들고 다른 URL을 통해 액세스할 수 있습니다. 다음 표에는 클라이언트가 액세스할 때 사용하는 URI 및 URL의 몇 가지 예가 나와 있습니다.

표 17–1 샘플 URI 및 해당 URL

URI(경로)	프록시에 대한 URL
/	http://proxy.mysite.com
/employees	http://proxy.mysite.com/employees
/group1	http://proxy.mysite.com/group1
/managers	http://proxy.mysite.com/managers

역방향 프록시에서 PAC 파일 사용

역방향 프록시가 작동하는 방식으로 인해 프록시 서버와 `.pac` 파일 서버를 사용하기가 쉽지 않습니다. 프록시 서버가 파일 요청을 받는 경우 요청이 로컬 `.pac` 파일 또는 원격 문서에 대한 것인지 여부를 결정해야 합니다.

프록시 서버가 `.pac` 파일에 대한 유지 관리 및 서비스를 수행하는 것 이외에 역방향 프록시 역할을 수행하도록 하려면 `obj.conf` 파일을 편집하여 NameTrans 함수 순서가 정확한지 확인합니다.

프록시 서버가 역방향 프록시 역할을 수행하도록 정규 매핑을 만듭니다. 이것은 일반적으로 프록시에게 모든 요청을 원격 컨텐트 서버로 라우팅하도록 지시합니다. 프록시 자동 구성 파일을 추가하여 `/pac` 같은 특정 디렉토리에 매핑할 수 있습니다. 이 경우 `.pac` 파일을 가지는 클라이언트는 다음과 같은 URL을 사용합니다.

```
http://proxy.mysite.com/pac
```

주의 – 이러한 매핑을 통해 원격 컨텐트 서버에 유사한 디렉토리가 없는지 확인합니다.

프록시 자동 구성 파일의 지시문 및 함수가 다른 매핑 이전에 나타나는지 확인하기 위해 `obj.conf` 파일을 편집합니다. 프록시 서버는 일반적으로 요청을 수행하기 전에 모든 NameTrans 함수를 통해 실행되기 때문에 지시문과 함수가 먼저 표시되어야 합니다. 그러나 자동 구성 파일을 통해 프록시는 즉시 경로를 인식하고 `.pac` 파일을 반환합니다.

다음 예는 역방향 프록시를 사용하고 자동 구성 파일을 유지 관리하는 obj.conf 파일입니다.

```
<Object name="default">
NameTrans from="file:" fn="map" to="ftp:"
NameTrans from="/pac" fn="pac-map" name="file"
    to="/ns-home/proxy/pac/proxy.pac"
NameTrans fn="redirect" from="http://foo.*" url="http://www.acme.com"
NameTrans from="/ns-icons" fn="pfx2dir" dir="/ns-home/ns-icons" name="file"
NameTrans fn="reverse-map" from="http://web.acme.com"
    to="http://proxy.acme.com:8080"
NameTrans fn="map" from="http://proxy.acme.com:8080"
    to="http://web.acme.com"
NameTrans fn="map" from="/" to="http://web.acme.com"
PathCheck fn="url-check"
Service fn="deny-service"
AddLog fn="flex-log" name="access"
AddLog fn="urldb-record"
</Object>
```

Server Manager 페이지를 사용하여 자동 구성 파일 만들기

▼ Server Manager를 사용하여 자동 구성 파일을 만드는 방법

1 Server Manager에 액세스하고 Routing 탭을 선택합니다.

2 Create/Edit Autoconfiguration File 링크를 누릅니다.

나타나는 페이지에 프록시 시스템에 있는 자동 구성 파일이 나열됩니다. 자동 구성 파일을 눌러 편집할 수 있습니다. 나머지 단계에서는 새 파일을 만드는 방법에 대해 설명합니다.

3 프록시에서 자동 구성 파일을 가져오는 경우 클라이언트가 사용하는 URL의 경로 부분인 선택적 URI를 입력합니다.

예를 들어 /를 입력하면 클라이언트가 프록시의 기본 문서(웹 서버의 경우 index.html 파일과 유사함)인 파일에 액세스할 수 있습니다. 자동 구성 파일의 프록시에 액세스하는 경우 클라이언트는 도메인 이름만 사용합니다. 여러 URI를 사용하고 각 URI에 대해 별도의 자동 구성 파일을 만들 수 있습니다.

4 .pac 확장자를 사용하여 자동 구성 파일의 이름을 입력합니다.

파일이 하나인 경우 간단하게 `proxy.pac`(pac는 프록시 자동 구성의 줄임말)로 지정합니다. 모든 자동 구성 파일은 단일 JavaScript 함수를 가진 ASCII 텍스트 파일입니다.

5 OK를 누릅니다. 다른 페이지가 나타납니다.

이 페이지를 사용하여 자동 구성 파일을 만듭니다. 페이지의 항목이 클라이언트에 의해 순서대로 수행됩니다. 페이지의 항목은 다음과 같습니다.

- **Never Go Direct To Remote Server**는 브라우저가 항상 프록시를 사용하도록 지시합니다. 프록시 서버가 실행되지 않는 경우 사용할 두 번째 프록시 서버를 지정할 수 있습니다.
- **Go Direct To Remote Server When**은 프록시 서버를 우회할 경우를 결정합니다. 브라우저는 페이지에 옵션이 나열된 순서대로 이러한 경우를 결정합니다.
- **Connecting To Non-fully Qualified Host Names**는 사용자가 컴퓨터 이름만 지정한 경우 브라우저를 직접 서버로 보냅니다. 예를 들어 내부 웹 서버를 `winternal.mysite.com`이라고 할 경우 사용자는 정규화된 도메인 이름 대신 `http://winternal`만 입력할 수 있습니다. 이 경우 브라우저가 프록시 대신 웹 서버로 직접 이동합니다.
- **Connecting To A Host In Domain**을 사용하여 브라우저가 직접 액세스할 수 있는 도메인 이름을 세 개까지 지정할 수 있습니다. 도메인을 지정할 때는 점 문자로 시작합니다. 예를 들어 `.example.com`을 입력할 수 있습니다.
- **Connecting To A Resolvable Host**는 클라이언트가 호스트를 확인할 수 있는 경우 브라우저를 직접 서버로 보냅니다. 이 옵션은 일반적으로 로컬(내부) 호스트만 확인하도록 DNS를 설정한 경우 사용됩니다. 로컬 네트워크 외부의 서버에 연결하는 경우 클라이언트는 프록시 서버를 사용합니다.

주의 – 이 옵션은 클라이언트가 모든 요청에 대해 DNS를 참조해야 하기 때문에 클라이언트에 의해 확인된 성능에 부정적인 영향을 줍니다.

- **Connecting To A Host In Subnet**은 클라이언트가 특정 서브넷의 서버에 액세스하는 경우 브라우저를 직접 서버로 보냅니다. 이 옵션은 조직의 서브넷이 여러 지역에 분포되어 있는 경우 유용합니다. 예를 들어 몇몇 회사가 전 세계의 여러 서브넷에 적용되는 단일 도메인 이름을 가질 수 있지만 각 서브넷은 특정 지역에만 관련됩니다.

주의 – 이 옵션은 클라이언트가 모든 요청에 대해 DNS를 참조해야 하기 때문에 클라이언트에 의해 확인된 성능에 부정적인 영향을 줍니다.

- **Except When Connecting To Hosts**를 사용하여 서버로 직접 이동하는 규칙에 대한 예외를 지정할 수 있습니다. 예를 들어 직접 이동할 도메인으로 `.example.com`을 입력한 경우 `home.example.com`으로 이동하기 위한 예외를 만들 수 있습니다. 그러면 브라우저는 `home.example.com`으로 이동할 때 프록시를 사용하지만 `example.com` 도메인의 다른 서버로 직접 이동합니다.
- **Secondary Failover Proxy**는 프록시 서버가 실행되지 않는 경우 사용할 두 번째 프록시를 지정합니다.
- **Failover Direct**는 프록시 서버가 실행되지 않는 경우 브라우저를 직접 서버로 보냅니다. 보조 페일오버 프록시를 지정한 경우 Navigator는 서버로 직접 이동하기 전에 두 번째 프록시 서버를 시도합니다.

6 OK를 눌러 자동 구성 파일을 만듭니다.

파일은 *server-root*`/proxy-server` *id*`/pac` 디렉토리에 저장됩니다.

파일이 제대로 만들어졌다는 확인 메시지가 나타납니다. 위의 단계를 반복하여 필요한 수만큼 자동 구성 파일을 만듭니다.

자동 구성 파일을 만들었으면 프록시 서버를 사용하는 모든 사용자에게 올바른 자동 구성 파일을 지정하거나 브라우저 복사본을 구성하도록 알려 주어야 합니다.

수동으로 자동 구성 파일 만들기

이 절에서는 수동으로 자동 구성 파일을 만드는 방법에 대해 설명합니다.

프록시 자동 구성 파일은 클라이언트 측 JavaScript를 사용하여 작성됩니다. 각 파일에는 브라우저가 각 URL에 대해 사용해야 하는 프록시 서버(있는 경우)를 결정하는 `FindProxyForURL()`이라고 하는 단일 JavaScript 함수가 포함되어 있습니다. 브라우저는 브라우저가 실행되고 있는 시스템의 호스트 이름 및 두 가지 매개 변수로 보냅니다. JavaScript 함수는 진행 방법을 알려 주는 Navigator에 값을 반환합니다. 다음 절에서는 함수 구문과 가능한 반환 값에 대해 설명합니다.

`FindProxyForURL()` 함수

`FindProxyFor()` URL 함수의 구문은 다음과 같습니다.

```
function FindProxyForURL(url, host){   ...}
```

브라우저가 액세스하는 모든 URL의 경우 다음과 같은 방법으로 *url* 및 *host* 매개 변수를 보내고 함수를 호출합니다.

```
ret = FindProxyForURL(url, host);
```

*url*은 브라우저에서 액세스되는 전체 URL입니다.

*host*는 액세스되는 URL에서 추출된 호스트 이름입니다. 이것은 편의상의 방법일 뿐이며 **://** 및 첫 번째 **:** 또는 그 다음의 **/** 사이의 동일한 문자열입니다. 포트 번호는 이 매개 변수에 포함되지 않으며 필요한 경우 URL에서 추출할 수 있습니다.

ret(반환 값)는 구성을 설명하는 문자열입니다.

함수 반환 값

자동 구성 파일에는 `FindProxyForURL()` 함수가 포함되어 있습니다. 이 함수는 액세스할 클라이언트 호스트 이름과 URL을 매개 변수로 사용합니다. 함수는 브라우저에게 진행 방법을 지시하는 단일 문자열을 반환합니다. 문자열이 null인 경우 프록시를 사용하지 않아야 합니다. 다음 표에 표시된 구성 블록을 세미 콜론으로 구분하여 문자열에 포함시킬 수 있습니다.

표 17–2 `FindProxyForURL()` 반환 값

반환 값	브라우저 결과 작업
`DIRECT`	프록시를 통해 이동하지 않고 서버에 직접 연결합니다.
`PROXY` *host:port*	지정된 프록시와 포트 번호를 사용합니다. 여러 값을 세미 콜론으로 구분한 경우 첫 번째 프록시가 사용됩니다. 해당 프록시가 실패할 경우 다음 프록시가 차례대로 사용됩니다.
`SOCKS` *host:port*	지정된 SOCKS 서버를 사용합니다. 여러 값을 세미 콜론으로 구분한 경우 첫 번째 프록시가 사용됩니다. 해당 프록시가 실패할 경우 다음 프록시가 차례대로 사용됩니다.

브라우저가 사용할 수 없는 프록시 서버에 연결된 경우 브라우저는 자동으로 30분 후, 1시간 후 등과 같이 30분 간격으로 이전에 응답하지 않는 프록시와 연결을 다시 시도합니다. 따라서 일시적으로 프록시 서버를 중단한 경우 클라이언트는 다시 시작한 이후 30분 내에 프록시 사용을 다시 시작합니다.

모든 프록시가 종료되고 DIRECT 반환 값이 지정되지 않을 경우 브라우저는 일시적으로 프록시를 무시하고 대신 직접 연결을 시도할지 여부를 사용자에게 묻는 메시지를 표시합니다. 브라우저는 프록시가 20분 후, 다시 20분 후 등과 같이 20분 간격으로 다시 시도할지 여부를 묻습니다.

다음 예에서 반환 값은 브라우저에게 포트 8080에서 `w3proxy.example.com`이라는 프록시를 사용할 것을 지시합니다. 해당 프록시를 사용할 수 없는 경우 브라우저는 다음과 같이 포트 8080에서 `proxy1.example.com` 이라는 프록시를 사용합니다.

```
PROXY w3proxy.example.com:8080; PROXY proxy1.example.com:8080
```

다음 예에서 기본 프록시는 `w3proxy.example.com:8080` 입니다. 해당 프록시를 사용할 수 없는 경우 브라우저는 `proxy1.example.com:8080`을 사용합니다. 두 개의 프록시를 모두 사용할 수 없는 경우 브라우저가 직접 서버로 이동합니다. 20분 이후 브라우저는 사용자에게 첫 번째 프록시를 다시 시도할지 여부를 묻습니다.

```
PROXY w3proxy.example.com:8080; PROXY proxy1.example.com:8080; DIRECT
```

JavaScript 함수 및 환경

JavaScript 언어에는 프록싱 사용에 유용한 미리 정의된 함수와 환경 조건이 있습니다. 이러한 각 함수는 특정 조건을 만족하는지 여부를 확인한 다음 true 또는 false 값을 반환합니다. 관련 유틸리티 함수는 DNS 호스트 이름 또는 IP 주소를 반환하기 때문에 예외입니다. 기본 `FindProxyForURL ()` 함수에서 이러한 함수를 사용하여 브라우저에 보낼 반환 값을 결정할 수 있습니다. 이 장의 뒷부분에서는 이러한 함수 사용에 대한 개념을 예를 들어 설명합니다.

각 함수 또는 환경 조건에 대해서는 이 절에서 설명합니다. 브라우저와 프록시 통합에 적용된 함수 및 환경 조건은 다음과 같습니다.

- 호스트 이름 함수는 다음과 같습니다.
  - `dnsDomainIs()()`
  - `isInNet()()`
  - `isPlainhost name()()`
  - `isResolvable()()`
  - `localHostOrDomainIs()()`
- 유틸리티 함수:
  - dnsDomainLevels()
  - dnsResolve()
  - myIpAddress()
- URL/host name-based condition:
  - shExpMatch()
- Time-based conditions:
  - dateRange()
  - timeRange()
  - weekdayRange()

호스트 이름 기반 함수

호스트 이름 기반 함수를 통해 호스트 이름 또는 IP 주소를 사용하여 어떤 프록시(있는 경우)를 사용할지 결정할 수 있습니다.

`dnsDomainIs()`(호스트, 도메인)

`dnsDomainIs()()` 함수는 URL 호스트 이름이 지정된 DNS 도메인에 속하는지 여부를 확인합니다. 이 함수는 346 페이지 "예 1: 로컬 호스트를 제외한 모든 서버 프록시" 및 347 페이지 "예 2: 방화벽 외부의 로컬 서버 프록시"에 설명된 대로 로컬 도메인에 대해 프록시를 사용하지 않도록 브라우저를 구성하는 경우 유용합니다.

또한 이 함수는 요청을 수신하는 프록시가 URL이 속한 DNS 도메인을 기준으로 프록시 그룹에서 선택된 경우 로드 균형 조정을 위해 여러 프록시를 사용할 때 유용합니다. 예를 들어 .edu가 포함된 URL을 특정 프록시에 연결하고 .com이 포함된 URL을 다른 프록시로 연결하여 로드 균형을 조정하는 경우 dnsDomainIs()()를 사용하여 URL 호스트 이름을 확인할 수 있습니다.

매개 변수

*host*는 URL의 호스트 이름입니다.

*domain*은 호스트 이름을 테스트하기 위한 도메인 이름입니다.

반환 값

true 또는 false

예

다음 문은 true입니다.

```
dnsDomainIs("www.example.com", ".example.com")
```

다음 문은 false입니다.

```
dnsDomainIs("www", ".example.com") dnsDomainIs("www.mcom.com",
    ".example.com")
```

isInNet()(호스트, 패턴, 마스크)

isInNet()() 함수를 사용하여 IP 주소에 대한 URL 호스트 이름을 확인하고 마스크에 의해 지정된 서브넷에 속하는지 여부를 테스트할 수 있습니다. 이것은 SOCKS가 사용하는 IP 주소 패턴 일치 유형과 동일합니다. 348 페이지 “예 4: 서브넷에 직접 연결”을 참조하십시오.

매개 변수:

*host*는 DNS 호스트 이름 또는 IP 주소입니다. 호스트 이름이 통과되면 이 함수는 호스트 이름을 IP 주소로 확인합니다.

*pattern*은 점으로 구분된 형식의 IP 주소 패턴입니다.

*mask*는 일치해야 하는 IP 주소의 부분을 결정하는 IP 주소 패턴 마스크입니다. 0 값은 무시를, 255는 일치를 의미합니다. 이 함수는 호스트의 IP 주소가 지정된 IP 주소 패턴과 일치할 경우 true입니다.

반환 값

true 또는 false

예

이 문은 호스트의 IP 주소가 정확하게 198.95.249.79와 일치하는 경우에만 true입니다.

```
isInNet(host, "198.95.249.79", "255.255.255.255")
```

이 문은 호스트의 IP 주소가 198.95.*와 일치하는 경우에만 true입니다.*: `isInNet(host, "198.95.0.0", "255.255.0.0")`

isPlainhost name()(호스트)

`isPlainhost name()()` 함수는 요청한 URL의 호스트 이름이 일반 호스트 이름 또는 정규화된 도메인 이름인지 여부를 확인합니다. 이 함수는 346 페이지 "예 1: 로컬 호스트를 제외한 모든 서버 프록시" 및 347 페이지 "예 2: 방화벽 외부의 로컬 서버 프록시"에 설명된 대로 브라우저를 로컬 서버에 직접 연결하려는 경우 유용합니다.

매개 변수

*host*는 호스트 이름에 도메인 이름이 없는 경우(점으로 구분된 세그먼트 없음)에만 포트 번호를 제외하고 URL의 호스트 이름입니다.

반환 값

*host*가 로컬인 경우 true이고 *host*가 원격인 경우 false입니다.

예

```
isPlainhost name("host")
```

*host*가 www와 같은 문자열인 경우 함수는 true를 반환합니다. 호스트가 www.example.com과 같은 문자열인 경우 함수는 false를 반환합니다.

isResolvable()(호스트)

방화벽 내의 DNS가 내부 호스트만 인식하는 경우 `isResolvable()()` 함수를 사용하여 호스트 이름이 네트워크에 대해 내부 또는 외부인지 여부를 테스트할 수 있습니다. 이 함수를 사용하면 내부 서버에 대한 직접 연결을 사용하고 외부 서버에 대해서만 프록시를 사용하도록 브라우저를 구성할 수 있습니다. 이 함수는 방화벽 내의 내부 호스트가 다른 내부 호스트의 DNS 도메인 이름을 확인할 수 있지만 모든 외부 호스트를 확인할 수 없는 사이트에서 유용합니다. `isResolvable()()` 함수는 DNS를 참조하여 호스트 이름을 IP 주소로 확인하려고 합니다. 347 페이지 "예 3: 확인되지 않은 호스트만 프록시"를 참조하십시오.

매개 변수

`host()`는 URL의 호스트 이름입니다.

반환 값

함수가 호스트 이름을 확인할 수 있는 경우 true이고 확인할 수 없으면 false입니다.

예

```
isResolvable("host")
```

host()가 www와 같은 문자열이고 DNS를 통해 확인할 수 있는 경우 이 함수는 true를 반환합니다.

localHostOrDomainIs()(호스트, 호스트 도메인)

localHostOrDomainIs()() 함수는 정규화된 도메인 이름 또는 일반 호스트 이름으로 액세스할 수 있는 로컬 호스트를 지정합니다. 347 페이지 "예 2: 방화벽 외부의 로컬 서버 프록시"를 참조하십시오.

호스트 이름이 지정된 호스트 이름과 정확하게 일치하거나 정규화되지 않은 호스트 이름과 일치하는 호스트 이름에 도메인 이름 부분이 없는 경우 localHostOrDomainIs()() 함수는 true를 반환합니다.

매개 변수

*host*는 URL의 호스트 이름입니다.

*hostdom*은 일치하는 정규화된 호스트 이름입니다.

반환 값

true 또는 false

예

다음 문은 true(정확히 일치)입니다.

```
localHostOrDomainIs("www.example.com", "www.example.com")
```

다음 문은 true(호스트 이름 일치, 도메인 이름 지정되지 않음)입니다.

```
localHostOrDomainIs("www", "www.example.com")
```

다음 문은 false(도메인 이름 불일치)입니다.

```
localHostOrDomainIs("www.mcom.com", "www.example.com")
```

다음 문은 false(호스트 이름 불일치)입니다.

```
localHostOrDomainIs("home.example.com", "www.example.com")
```

유틸리티 함수

유틸리티 함수를 사용하여 도메인 수준, 브라우저가 실행 중인 호스트 또는 호스트의 IP 주소를 찾을 수 있습니다.

dnsDomainLevels()(hot)

dnsDomainLevels()() 함수는 URL 호스트 이름에서 DNS 수준 번호(점의 수)를 찾습니다.

매개 변수

*host*는 URL의 호스트 이름입니다.

반환 값

DNS 도메인 수준의 번호(정수)입니다.

예

dnsDomainLevels("www")는 0을 반환합니다.

dnsDomainLevels("www.example.com")는 2를 반환합니다.

dnsResolve()(host)

dnsResolve()() 함수는 보통 URL로부터 제공되는 호스트의 IP 주소를 확인합니다. 이 함수는 JavaScript 함수가 기존 함수로 수행할 수 있는 것보다 고급 패턴 일치를 수행해야 하는 경우 유용합니다.

매개 변수

*host*는 확인할 호스트 이름입니다. 지정된 DNS 호스트 이름을 IP 주소로 확인하고 점으로 구분된 형식으로 문자열로 반환합니다.

반환 값

문자열 값인 점으로 구분된 네 개의 IP 주소

예

다음 예에서는 문자열 198.95.249.79를 반환합니다.

```
dnsResolve("home.example.com")
```

myIpAddress()()

myIpAddress()() 함수는 브라우저가 실행되는 호스트에 따라 JavaScript 함수가 다르게 동작해야 하는 경우 유용합니다. 이 함수는 브라우저를 실행하는 컴퓨터의 IP 주소를 반환합니다.

반환 값

문자열 값인 점으로 구분된 네 개의 IP 주소

예:

다음 예에서는 컴퓨터 `home.example.com`에서 Navigator를 실행하는 경우 문자열 `198.95.249.79`를 반환합니다.

```
myIpAddress()
```

URL/호스트 이름 기반 조건

로드 균형 조정 및 라우팅을 위해 호스트 이름 또는 URL을 일치시킬 수 있습니다.

`shExpMatch()(str, shexp)`

`shExpMatch()()` 함수는 URL 호스트 이름 또는 URL 자체를 일치시킵니다. 이 함수는 로드 균형 조정 및 서로 다른 프록시 서버에 대한 URL의 지능적 라우팅에 주로 사용됩니다.

매개 변수

*str*은 비교할 문자열입니다(예: URL 또는 호스트 이름).

*shexp*는 비교할 쉘 표현식입니다.

이 표현식은 문자열이 지정된 쉘 표현식과 일치하는 경우 true입니다. 349 페이지 “예 6: `shExpMatch()()`를 통한 프록시 로드 균형 조정”을 참조하십시오.

반환 값

true 또는 false

예

첫 번째 예에서는 true를 반환합니다. 두 번째 예에서는 false를 반환합니다.

```
shExpMatch("http://home.example.com/people/index.html",
           ".*/people/.*")
shExpMatch("http://home.example.com/people/yourpage/index.html",
           ".*/mypage/.*")
```

시간 기반 조건

날짜, 시간 또는 요일에 따라 **FindProxyForURL** 함수가 다르게 동작하도록 할 수 있습니다.

dateRange()(일, 월, 년...)

dateRange()() 함수는 예를 들어 1996년 4월 19일부터 1996년 5월 3일과 같이 특정 날짜 또는 날짜 범위를 검색합니다. 이 함수는 예를 들어 한 프록시에 대해 정기적으로 유지보수 중단 시간이 예약된 경우와 같이 요일에 따라 FindProxyForURL() 함수가 다르게 작동하게 하려는 경우 유용합니다.

날짜 범위는 여러 가지 방법으로 지정할 수 있습니다

```
dateRange(day)dateRange(day1, day2)dateRange(mon)dateRange(month1,
month2)dateRange(year)dateRange(year1, year2)dateRange(day1, month1, day2,
month2)dateRange(month1, year1, month2, year2)dateRange(day1, month1, year1,
day2, month2, year2)dateRange(day1, month1, year1, day2, month2, year2, gmt)
```

매개 변수

*day*는 일에 대한 1에서 31 사이의 정수입니다.

*month*는 다음 월 문자열 중 하나입니다. JAN FEB MAR APR MAY JUN JUL AUG SEP OCT NOV DEC

*year*는 연도 숫자에 대한 네 자리 정수입니다(예: 1996).

*gmt*는 그리니치 표준시에서 시간 비교가 수행되어야 하는 문자열 "GMT" 이거나 시간을 로컬 시간대로 가정하기 위해 비어 있는 상태로 둡니다. GMT 매개 변수는 호출 프로필에서 항상 마지막 매개 변수로 지정할 수 있습니다. 각 범주(일, 월, 년)에서 단일 값만 지정할 경우 함수는 해당 사양과 일치하는 날짜에 대해 true 값만 반환합니다. 두 개의 값을 지정하면 결과는 지정된 첫 번째 시간에서 지정된 두 번째 시간 사이에 true입니다.

예

다음 문은 매월 로컬 시간대의 첫째 날에 대해 true입니다. dateRange(1)

다음 문은 매월 그리니치 표준시의 첫째 날에 대해 true입니다. dateRange(1, "GMT")

다음 문은 매월 상반기에 대해 true입니다. dateRange(1, 15)

다음 문은 매년 12월 24일에 대해 true입니다. dateRange(24, "DEC")

다음 문은 1995년 12월 24일에 대해 true입니다. dateRange(24, "DEC", 1995)

다음 문은 1사분기 동안 true입니다. dateRange("JAN", "MAR")

다음 문은 매년 6월 1일부터 8월 15 사이에 true입니다. dateRange(1, "JUN", 15, "AUG")

다음 문은 1995년 6월 1일부터 1995년 8월 15일 사이에 true입니다. dateRange(1, "JUN", 15, 1995, "AUG", 1995)

다음 문은 1995년 10월부터 1996년 3월 사이에 true입니다. `dateRange("OCT", 1995, "MAR", 1996)`

다음 문은 1995년 동안 계속 true입니다. `dateRange(1995)`

다음 문은 1995년 1월1일부터 1997년 마지막까지 true입니다. `dateRange(1995, 1997)`

timeRange(시, 분, 초...)

`timeRange()` 함수는 예를 들어 오후 9시에서 오전 12 사이와 같이 특정 시간 또는 시간 범위를 검색합니다. 이 함수는 시간에 따라 `FindProxyForURL()` 함수가 다르게 작동하게 하려는 경우 유용합니다.

```
timeRange(hour)timeRange(hour1, hour2)timeRange(hour1, min1, hour2,
min2)timeRange(hour1, min1, sec1, hour2, min2, sec2)
```

매개 변수:

*hour*는 0에서 23 사이의 시간입니다. 0은 자정이고 23은 오후 11시입니다.

*min*은 0에서 59 사이의 분 값입니다.

*sec*는 0에서 59 사이의 초 값입니다.

*gmt*는 GMT 시간대의 GMT 문자열이거나 로컬 시간대에 대해 지정되지 않습니다. 다음 매개 변수는 각 매개 변수 프로필과 함께 사용할 수 있으며 항상 마지막 매개 변수입니다.

반환 값

true 또는 false

예:

다음 문은 정오부터 오후 1시 사이에 true입니다.m: `timerange(12, 13)`

다음 문은 GMT 기준으로 정오부터 오후 12시 59분 사이에 true입니다. `timerange(12, "GMT")`

다음 문은 오전 9시부터 오후 5시 사이에 true입니다.m: `timerange(9, 17)`

다음 문은 자정부터 자정에서 30초 경과한 시간 사이에 true입니다. `timerange(0, 0, 0, 0, 0, 30)`

weekdayRange()(wd1, wd2, gmt)

weekdayRange() 함수는 월요일에서 금요일 사이와 같이 특정 요일 또는 요일 범위를 검색합니다. 이 함수는 요일에 따라 *FindProxyForURL* 함수가 다르게 작동하게 하려는 경우 유용합니다.

매개 변수

*wd1*및 *wd2*는 다음 요일 문자열 중 하나입니다. `SUN MON TUE WED THU FRI SAT`

*gmt*는 그리니치 표준시의 경우 GMT이거나 로컬 시간의 경우 그대로 둡니다.

첫 번째 매개 변수 *wd1*만 필수 사항입니다. *wd2*, *gmt* 또는 두 개 모두 비워 둘 수 있습니다.

하나의 매개 변수만 있는 경우 함수는 매개 변수가 표시하는 요일에 true 값을 반환합니다. 문자열 GMT가 두 번째 매개 변수로 지정된 경우 시간이 GMT로 제공됩니다. 그렇지 않을 경우 시간은 로컬 시간대로 제공됩니다.

*wd1*및 *wd2*가 모두 정의된 경우 조건은 현재 요일이 이 두 요일 사이에 있을 경우 true입니다. 경계값도 포함됩니다. 매개 변수의 순서가 중요합니다. “MON,” “WED”는 월요일부터 수요일 사이지만 “WED,” “MON”은 수요일부터 다음 주 월요일 사이입니다.

예

다음 문은 월요일부터 금요일(로컬 시간대) 사이에 true입니다. `weekdayRange("MON", "FRI")`

다음 문은 그리니치 표준시로 월요일부터 금요일 사이에 true입니다. `weekdayRange("MON", "FRI", "GMT")`

다음 문은 로컬 시간으로 매주 토요일마다 true입니다.`weekdayRange("SAT")`

다음 문은 그리니치 표준 시간으로 매주 토요일마다 true입니다.`weekdayRange("SAT", "GMT")`

다음 문은 금요일부터 월요일 사이에 true입니다(순서가 중요함) `weekdayRange("FRI", "MON")`

함수 예

다음 절에서는 JavaScript 함수에 대해 예를 들어 자세히 설명합니다.

예 1: 로컬 호스트를 제외한 모든 서버 프록시

이 예에서는 브라우저가 정규화되지 않은 모든 호스트와 로컬 도메인에 있는 호스트에 직접 연결합니다. 다른 모든 호스트는 `w3proxy.example.com:8080`이라는 프록시와 연결됩니다.

주 – 프록시가 중단되면 자동으로 직접 연결됩니다.

```
function FindProxyForURL(url, host)
{
    if (isPlainhost name(host) ||
```

```
        dnsDomainIs(host, ".example.com") ||
        dnsDomainIs(host, ".mcom.com"))
        return "DIRECT";
    else
        return "PROXY w3proxy.example.com:8080; DIRECT";
}
```

예 2: 방화벽 외부의 로컬 서버 프록시

이 예는 346 페이지 "예 1: 로컬 호스트를 제외한 모든 서버 프록시"와 비슷하지만 방화벽 외부에 있는 로컬 서버의 프록시를 사용합니다. 기본 웹 서버와 같은 호스트는 로컬 도메인에 속하지만 방화벽 외부에 있어서 프록시 서버를 통해서만 접근할 수 있는 경우 이러한 예외는 `localHostOrDomainIs()()` 함수를 사용하여 처리됩니다.

```
function FindProxyForURL(url, host)
{
    if ((isPlainhost name(host) ||
    dnsDomainIs(host, ".example.com")) &&
    !localHostOrDomainIs(host, "www.example.com") &&
    !localHostOrDoaminIs(host, "merchant.example.com"))
        return "DIRECT";
    else
        return "PROXY w3proxy.example.com:8080; DIRECT";
}
```

이 예에서는 `example.com` 도메인의 로컬 호스트를 제외하고 모든 호스트의 프록시를 사용합니다. 또한 호스트 `www.example.com` 및 `merchant.example.com`도 프록시를 통해 연결됩니다.

예외 순서는 효율성을 향상시킵니다. `localHostOrDomainIs()()` 함수는 모든 URL이 아닌 로컬 도메인에 있는 URL에 대해서만 실행됩니다. 특히 *and* 표현식 앞에 있는 *or* 표현식 주위의 괄호에 주의하십시오.

예 3: 확인되지 않은 호스트만 프록시

이 예는 내부 DNS가 내부 호스트 이름만 확인하는 환경에 대해 설명합니다. 목적은 확인할 수 없는 호스트에 대해서만 프록시를 사용하는 것입니다.

```
function FindProxyForURL(url, host)
{
    if (isResolvable(host))
            return "DIRECT";
        else
            return "PROXY proxy.mydomain.com:8080";
}
```

이 예의 경우 매번 DNS를 참조해야 합니다. 따라서 다른 규칙이 결과를 제공하지 않는 경우에만 DNS를 참조하도록 이 예를 다른 규칙과 함께 그룹화합니다.

```
function FindProxyForURL(url, host)
{
    if (isPlainhost name(host) ||
        dnsDomainIs(host, ".mydomain.com") ||
        isResolvable(host))
        return "DIRECT";
    else
        return "PROXY proxy.mydomain.com:8080";
}
```

예 4: 서브넷에 직접 연결

이 예에서는 지정된 서브넷의 모든 호스트가 직접 연결됩니다. 다른 호스트는 프록시를 통해 연결됩니다.

```
function FindProxyForURL(url, host)
{
    if (isInNet(host, "198.95.0.0", "255.255.0.0"))
        return "DIRECT";
    else
        return "PROXY proxy.mydomain.com:8080";
}
```

이 예에서는 시작 부분에 중복 규칙을 추가하여 DNS 사용을 최소화할 수 있습니다.

```
function FindProxyForURL(url, host)
{
    if (isPlainhost name(host) ||
        dnsDomainIs(host, ".mydomain.com") ||
        isInNet(host, "198.95.0.0", "255.255.0.0"))
        return "DIRECT";
    else
        return "PROXY proxy.mydomain.com:8080";
}
```

예 5: dnsDomainIs()()로 프록시 로드 균형 조정

이 예는 훨씬 복잡합니다. 이 예에서는 4개의 프록시 서버를 사용하며 그 중 하나는 다른 서버에 대해 상시 대기 역할을 수행합니다. 나머지 3개의 프록시 서버가 중단될 경우 네 번째 서버가 역할을 수행합니다. 나머지 3개의 프록시 서버는 URL 패턴을 기준으로 로드를 공유하여 캐싱을 훨씬 효율적으로 수행합니다. 각 서버에 복사본이 하나만 있는 경우와 달리 모든 문서의 복사본이 세 개의 서버에 하나만 존재합니다. 로드는 다음 표에 표시된 것처럼 분산됩니다.

표 17–3 프록시 로드 균형 조정

프록시	용도
#1	.com 도메인
#2	.edu 도메인
#3	기타 모든 도메인
#4	상시 대기

모든 로컬 액세스가 직접 연결되어야 합니다. 모든 프록시 서버가 포트 8080에서 실행됩니다. + 연산자를 사용하여 문자열을 연결할 수 있습니다.

```
function FindProxyForURL(url, host)
{
    if (isPlainhost name(host) || dnsDomainIs(host, ".mydomain.com"))
        return "DIRECT";

    else if (dnsDomainIs(host, ".com"))
        return "PROXY proxy1.mydomain.com:8080; " +
               "PROXY proxy4.mydomain.com:8080";

    else if (dnsDomainIs(host, ".edu"))
        return "PROXY proxy2.mydomain.com:8080; " +
               "PROXY proxy4.mydomain.com:8080";

    else
        return "PROXY proxy3.mydomain.com:8080; " +
               "PROXY proxy4.mydomain.com:8080";
}
```

예 6: shExpMatch()()를 통한 프록시 로드 균형 조정

이 예는 기본적으로 348 페이지 “예 5: dnsDomainIs()()로 프록시 로드 균형 조정”과 동일하지만 dnsDomainIs()()를 사용하는 대신 shExpMatch()()를 사용합니다.

```
    function FindProxyForURL(url, host)
    {
    if (isPlainhost name(host) || dnsDomainIs(host, ".mydomain.com"))
        return "DIRECT";
    else if (shExpMatch(host, "*.com"))
        return "PROXY proxy1.mydomain.com:8080; " +
               "PROXY proxy4.mydomain.com:8080";
    else if (shExpMatch(host, "*.edu"))
        return "PROXY proxy2.mydomain.com:8080; " +
               "PROXY proxy4.mydomain.com:8080";
    else
```

```
        return "PROXY proxy3.mydomain.com:8080; " +
              "PROXY proxy4.mydomain.com:8080";
    }
```

예 7: 특정 프로토콜 프록싱

특정 프로토콜에 대해 프록시를 설정할 수 있습니다. 대부분의 표준 JavaScript 기능은 `FindProxyForURL()()` 함수에서 사용하기 위해 제공됩니다. 예를 들어 프로토콜을 기준으로 다른 프록시를 설정하기 위해 `substring()()` 함수를 사용할 수 있습니다.

```
function FindProxyForURL(url, host)
{
    if (url.substring(0, 5) == "http:") {
        return "PROXY http-proxy.mydomain.com:8080";
    }
    else if (url.substring(0, 4) == "ftp:") {
        return "PROXY ftp-proxy.mydomain.com:8080";
    }
    else if (url.substring(0, 7) == "gopher:") {
        return "PROXY gopher-proxy.mydomain.com:8080";
    }
    else if         (url.substring(0, 6) == "https:" ||
            url.substring(0, 6) == "snews:") {
        return "PROXY security-proxy.mydomain.com:8080";
    }
    else {
        return "DIRECT";
    }
}
```

또한 `shExpMatch()()` 함수를 사용하여 이 구성을 구현할 수 있습니다. 예를 들면 다음과 같습니다.

```
...
if (shExpMatch(url, "http:*")) {
    return "PROXY http-proxy.mydomain.com:8080;
}
...
```

◆ ◆ ◆ 18 장

18 ACL 파일 구문

액세스 제어 목록(ACL) 파일은 텍스트 파일로, Proxy Server 자원에 액세스할 수 있는 사용자를 정의한 목록이 포함되어 있습니다. 기본적으로 Proxy Server는 서버에 액세스할 수 있는 모든 목록이 포함된 한 개의 ACL 파일을 사용하지만, `obj.conf` 파일에 여러 ACL 파일을 만들어 참조할 수도 있습니다.

Proxy Server 4는 Proxy Server 3.x에서 사용했던 구문과는 다른 ACL 파일 구문을 사용합니다. 이 부록에서는 ACL 파일과 해당 구문에 대해 설명합니다. Proxy Server 및 해당 자원의 액세스 제어에 대한 자세한 내용은 8 장, “서버 액세스 제어”을 참조하십시오. 16 장, “템플리트 및 자원 관리”에서 설명한 대로 Proxy Server 4 릴리스에서는 자원 템플리트가 지원됩니다.

이 부록은 다음 내용으로 구성되어 있습니다.

- 351 페이지 “ACL 파일 및 ACL 파일 구문 정보”
- 356 페이지 “obj.conf 파일 내의 ACL 파일 참조”

ACL 파일 및 ACL 파일 구문 정보

모든 ACL 파일은 특정 형식과 구문을 따라야 합니다. ACL 파일은 하나 이상의 ACL이 포함된 텍스트 파일입니다. 모든 ACL 파일은 단일 구문 버전 번호로 시작해야 합니다. 예:

```
version 3.0;
```

버전 줄은 명령줄 다음에 나타날 수 있습니다. Proxy Server는 구문 버전 3.0을 사용합니다. 명령줄 시작 부분에 # 기호를 사용하여 파일에 주석을 포함시킬 수 있습니다.

파일의 각 ACL은 경로, 자원 또는 명명 등 ACL 유형을 정의하는 문으로 시작됩니다.

- 경로 ACL은 영향을 미치는 자원에 대한 절대 경로를 지정합니다.
- 자원 ACL은 `http://`, `https://`, `ftp://` 등과 같이 영향을 미치는 템플리트를 지정합니다. 템플리트에 대한 자세한 내용은 16 장, “템플리트 및 자원 관리”을 참조하십시오.

- 명명된 ACL은 `obj.conf` 파일의 자원에서 참조되는 이름을 지정합니다. 서버에는 기본 이름의 자원이 함께 제공되어 모든 사용자에게 읽기 액세스를 허용하며 LDAP 디렉토리의 사용자에게 쓰기 액세스를 허용합니다. Proxy Server 사용자 인터페이스에서 명명된 ACL을 만들 수는 있지만 명명된 ACL을 `obj.conf` 파일의 자원과 직접 참조해야 합니다.

경로 및 자원 ACL에는 와일드카드가 포함될 수 있습니다. 와일드카드에 대한 자세한 내용은 16 장, "템플리트 및 자원 관리"을 참조하십시오.

유형 줄은 `acl`로 시작하며 큰따옴표로 유형 정보를 표시하고 그 뒤에 세미콜론을 넣습니다. 예:

```
acl "default";acl "http://*.*";
```

모든 ACL의 유형 정보는 서로 다른 ACL 파일인 경우에도 각기 고유한 이름이어야 합니다. ACL의 유형을 정의한 후 ACL과 함께 사용할 메소드를 정의하는 인증문을 하나 이상 추가할 수 있습니다. 또한 액세스를 허용 또는 거부할 사용자 및 컴퓨터를 정의하는 인증문을 포함할 수 있습니다. 다음 절에서는 이러한 인증문 구문에 대해 설명합니다.

인증문

ACL은 선택적으로 ACL을 처리할 때 서버가 반드시 사용해야 하는 인증 방법을 지정할 수 있습니다. 일반적으로 다음 세 가지 방법을 사용합니다.

- Basic(기본값)
- Digest
- SSL

Basic 및 Digest 방법을 사용하려면 사용자가 자원에 액세스하기 전에 사용자 이름과 비밀번호를 입력해야 합니다.

SSL 방법의 경우 사용자에게 클라이언트 인증서가 있어야 합니다. 인증 받으려면 Proxy Server에 대해 암호화를 사용해야 하며 사용자의 인증서 발급자가 신뢰할 수 있는 인증 기관 목록에 있어야 합니다.

기본적으로 서버는 인증 방법을 지정하지 않은 모든 ACL에 대해 Basic 방법을 사용합니다. 서버의 인증 데이터베이스는 사용자가 전송한 Digest 인증을 지원해야 합니다.

각 인증 줄은 서버가 인증하는 속성(사용자, 그룹 또는 사용자 및 그룹 모두)을 지정해야 합니다. 다음은 ACL 유형 줄 다음에 표시되는 인증문으로, 데이터베이스 또는 디렉토리의 개별 사용자와 일치된 사용자에 대해 Basic 인증을 지정합니다.

```
authenticate(user) { method = "basic";};
```

다음 예에서는 SSL을 사용자 및 그룹용 인증 방법으로 사용합니다.

```
authenticate(user, group) { method = "ssl";};
```

다음 예에서는 사용자 이름이 sales로 시작하는 모든 사용자를 허용합니다.

```
allow (all) user = "sales*";
```

마지막 줄을 group = sales로 변경하면 그룹 속성이 인증되지 않으므로 ACL이 실패하게 됩니다.

권한 부여문

각 ACL 항목에는 하나 이상의 권한 부여문이 있습니다. 권한 부여문은 서버 자원에 대한 액세스를 허용 또는 거부할 사용자를 지정합니다.

권한 부여문 작성

권한 부여문을 작성하는 경우 다음 구문을 사용합니다.

```
allow|deny [absolute] (right[,right...]) attribute expression;
```

각 줄은 allow 또는 deny로 시작합니다. 규칙 계층 구조로 인해 첫 번째 규칙에서는 모든 사용자의 액세스를 거부한 다음 이후의 규칙에서는 사용자, 그룹 또는 컴퓨터의 액세스를 구체적으로 허용합니다. 예를 들어 /my_files 라는 디렉토리에 대해 모든 사용자의 액세스를 허용한 후, /my_files/personal 이라는 하위 디렉토리에 대해 일부 사용자에게만 액세스를 허용하는 경우 하위 디렉토리에 대한 액세스 제어가 제대로 적용되지 않습니다. 이는 /my_files 디렉토리에 액세스가 허용된 모든 사용자가 /my_files/personal 디렉토리에 액세스할 수 있기 때문입니다. 이러한 경우를 예방하려면 모든 사용자의 액세스를 거부한 후 일부 사용자에게 액세스를 허용하는 하위 디렉토리용 규칙을 만듭니다.

그러나 모든 사용자의 액세스를 거부하도록 기본 ACL을 설정하면 다른 ACL 규칙에는 "deny all" 규칙이 필요하지 않은 경우도 있습니다.

다음 줄은 모든 사용자의 액세스를 거부합니다.

```
deny (all) user = "anyone";
```

권한 부여문의 계층

ACL 계층은 자원에 따라 다릅니다. 서버는 특정 자원에 대한 요청을 받으면 해당 자원에 적용되는 ACL 목록을 만듭니다. 서버는 우선 obj.conf 파일의 check-acl문에 있는 명명된 ACL 목록을 추가합니다. 그런 다음 일치하는 경로와 자원 ACL을 추가합니다. 이 목록은 동일한 순서로 처리됩니다. "absolute" ACL문이 있지 않는 한 모든 문은 순서대로 평가됩니다. "absolute allow" 또는 "absolute deny"문이 "true"인 경우 서버는 처리를 중단하고 모든 결과를 승인합니다.

일치하는 ACL이 두 개 이상인 경우 서버는 일치하는 마지막 문을 사용합니다. 그러나 absolute문을 사용하는 경우 서버는 다른 일치에 대한 조회를 중단하고 absolute문이 포함된 ACL을 사용합니다. 동일한 자원에 대해 absolute문이 둘인 경우 서버는 파일의 첫 번째 문을 사용하고 일치되는 다른 자원에 대한 조회를 중단합니다.

```
version 3.0;acl "default";authenticate (user,group)
    { prompt="Sun Java System Web Proxy Server";};
    allow (read,execute,list,info) user = "anyone";
    allow (write,delete) user = "all";acl "http://*.*";
    deny (all) user = "anyone";allow (all) user = "joe";
```

속성 표현식

속성 표현식은 사용자 이름, 그룹 이름, 호스트 이름 또는 IP 주소를 기준으로 허용 또는 거부할 사용자를 정의합니다. 다음 줄에서는 다른 사용자 또는 컴퓨터에 액세스 권한을 부여하는 방법에 대해 예를 들어 설명합니다.

- `user = "anyone"`
- `user = "smith*"`
- `group = "sales"`
- `dns = "*.mycorp.com"`
- `dns = "*.mycorp.com,*.company.com"`
- `ip = "198.*"`
- `ciphers = "rc4"`
- `ssl = "on"`

또한 `timeofday` 속성을 사용하여 하루 중 시간(서버의 로컬 시간)에 따라 서버로의 액세스를 제한할 수 있습니다. 예를 들어 `timeofday` 속성을 사용하여 특정 사용자가 정해진 시간에만 액세스하도록 제한할 수 있습니다.

예를 들어 오전 4:00의 경우 0400, 오후 10:30의 경우 2230과 같이 시간을 지정하려면 24시간 형식을 사용합니다. 다음 예에서는 오전 8:00에서 오후 4:59 사이에 `guests`라고 하는 사용자 그룹에 대한 액세스를 제한합니다.

```
allow (read) (group="guests") and (timeofday<0800 or timeofday=1700);
```

또한 주중 요일에 따라 액세스를 제한할 수 있습니다. 다음과 같이 Sun, Mon, Tue, Wed, Thu, Fri, Sat 등의 세 자리 약자를 사용하여 요일을 지정합니다.

다음 문은 `premium` 그룹의 사용자에게 항상 액세스를 허용합니다. `discount` 그룹의 사용자는 주말의 모든 시간과 주 중 오전 8시에서 오후 4:59를 제외한 모든 시간에 액세스할 수 있습니다.

```
allow (read) (group="discount" and dayofweek="Sat,Sun") or (group="discount" and
(dayofweek="mon,tue,wed,thu,fri" and(timeofday<0800 or timeofday=1700)))or
(group="premium");
```

표현식용 연산자

다양한 연산자를 속성 표현식에 사용할 수 있습니다. 괄호는 연산자의 순서를 변경할 때 사용합니다. 다음 연산자를 `user`, `group`, `dns` 및 `ip`와 함께 사용할 수 있습니다.

- and
- or
- not
- =(등호)
- !=(부등호)

다음 연산자를 `timeofday` 및 `dayofweek`와 함께 사용할 수 있습니다.

- greater than
- < 보다 작음
- = 보다 크거나 같음
- <= 보다 작거나 같음

기본 ACL 파일

설치 후 *server_root*`/httpacl/generated.proxy-` *serverid*`.acl` 파일이 서버용 기본 설정을 제공합니다. 사용자 인터페이스에서 설정이 만들어질 때까지 서버는 작업 파일 `genwork.proxy-` *serverid*`.acl`을 사용합니다. ACL 파일을 편집할 때 `genwork` 파일을 변경할 수 있으며, 그런 후 Proxy Server를 사용하여 변경 사항을 저장 및 적용할 수 있습니다.

일반 구문 항목

입력 문자열에는 다음 문자를 포함할 수 있습니다.

- 문자 `a-z`
- 숫자 `0-9`
- 마침표 및 밑줄

그 외 문자는 큰따옴표로 묶어야 합니다.

단일문은 한 줄에 위치해야 하며 세미콜론으로 끝나야 합니다. 복수문은 대괄호([]) 안에 넣습니다. 항목 목록은 반드시 쉼표로 분리하고 인용 부호(") 안에 넣어야 합니다.

obj.conf 파일 내의 ACL 파일 참조

명명된 ACL 또는 별도의 ACL 파일은 `check-acl` 함수를 사용하여 `PathCheck` 지시문의 `obj.conf` 파일에서 참조할 수 있습니다. 이 줄의 구문은 다음과 같습니다.

```
PathCheck fn="check-acl" acl="aclname "
```

여기서 *aclname*은 ACL 파일에 표시되는 ACL의 고유한 이름입니다.

예를 들어 `testacl`이라는 ACL을 사용하여 디렉토리에 대한 액세스를 제한하려면 다음 줄을 `obj.conf` 파일에 추가합니다.

```
<Object ppath="https://"PathCheck fn="check-acl" acl="testacl"</Object>
```

이 예에서 첫 번째 줄은 액세스를 제한하려는 서버 자원을 표시하는 객체입니다. 두 번째 줄은 `PathCheck` 지시문으로, `check-acl` 함수를 사용하여 명명된 ACL(`testacl`)을 지시문이 나타나는 객체에 바인드합니다. `testacl` ACL은 `server.xml`에서 참조된 모든 ACL 파일에 나타날 수 있습니다.

◆ ◆ ◆ 19 장

19 서버 성능 조정

프록시 클라이언트, Proxy Server, 원래 서버 및 네트워크를 포함하여 다양한 요소가 Proxy Server 환경의 성능에 영향을 줍니다. 이 부록에서는 Proxy Server 성능을 향상시킬 수 있는 조정 작업에 대해 설명합니다.

이 부록은 고급 관리자 전용입니다. 서버를 조정하는 경우 변경하기 전에 항상 구성 파일을 백업해야 합니다.

이 부록은 다음 내용으로 구성되어 있습니다.

- 357 페이지 “일반 성능 고려 사항”
- 360 페이지 “시간 초과 값”
- 362 페이지 “최신 여부 확인”
- 363 페이지 “DNS 설정”
- 363 페이지 “스레드 수”
- 364 페이지 “인바운드 연결 풀”
- 365 페이지 “FTP 목록 너비”
- 365 페이지 “캐시 아키텍처”
- 365 페이지 “캐시 일괄 업데이트”
- 366 페이지 “가비지 컬렉션”
- 367 페이지 “Solaris 성능 조정”

일반 성능 고려 사항

이 절에서는 Proxy Server 성능 분석 시 고려해야 할 일반적인 사항에 대해 설명합니다.

이 절은 다음 내용으로 구성되어 있습니다.

- 358 페이지 “액세스 로깅”
- 358 페이지 “ACL 캐시 조정”
- 359 페이지 “버퍼 크기”
- 359 페이지 “연결 시간 초과”

- 359 페이지 "오류 로그 수준"
- 359 페이지 "보안 요구 사항"
- 359 페이지 "Solaris 파일 시스템 캐싱"

액세스 로깅

액세스 로깅을 비활성화하면 Proxy Server의 성능을 향상시킬 수 있습니다. 그러나 Proxy Server에 액세스하는 사용자와 요청 중인 페이지를 직접 확인할 수 없게 됩니다.

obj.conf 파일의 다음 지시문을 주석 처리하여 Proxy Server 액세스 로깅을 비활성화할 수 있습니다.

```
Init fn= flex-init access= $accesslog format.access= %Ses->client.ip% -
%Req->vars.auth-user% [%SYSDATE%] \\ %Req->reqpb.clf-request%\\
%Req->srvhdrs.clf-status% %Req->srvhdrs.content-length% ...AddLog
fn= flex-log name= access
```

ACL 캐시 조정

기본적으로 Proxy Server는 사용자 및 그룹 인증 결과를 ACL 사용자 캐시에 캐시합니다. magnus.conf 파일에서 ACLCacheLifetime 지시문을 사용하여 ACL 사용자 캐시가 유효한 시간을 제어할 수 있습니다. 캐시에 있는 항목이 참조될 때마다 시간이 계산되고 ACLCacheLifetime과 비교됩니다. 항목의 시간이 ACLCacheLifetime과 같거나 크면 해당 항목은 사용되지 않습니다.

ACLCacheLifetime의 기본값은 120초이므로 Proxy Server가 2분 동안 LDAP 서버와 동기화되지 않을 수 있습니다. 값을 0으로 설정하면 캐시가 꺼지고 사용자가 인증할 때마다 Proxy Server가 강제로 LDAP 서버를 쿼리합니다. 이 설정은 액세스 제어를 구현하는 경우 Proxy Server의 성능에 부정적인 영향을 줍니다. ACLCacheLifetime 값을 크게 설정할 경우 이 설정으로 Proxy Server가 LDAP 서버를 강제로 쿼리하기 때문에 LDAP 항목을 변경할 때마다 Proxy Server를 다시 시작해야 합니다. 따라서 LDAP 디렉토리가 자주 변경되지 않는 경우에만 큰 값으로 설정하십시오.

*ACLUserCacheSize*는 캐시에 보관할 수 있는 최대 항목 수를 구성하는 `magnus.conf` 매개변수입니다. 기본값은 200입니다. 새 항목은 목록의 시작 부분에 추가되며 이 목록의 끝에 있는 항목은 캐시가 최대 크기에 도달하면 재활용되어 새로운 항목을 허용합니다.

또한 *ACLGroupCacheSize* 매개 변수를 사용하여 사용자 항목당 캐시할 수 있는 최대 그룹 구성원 수를 설정할 수 있습니다. 기본값은 4입니다. 그룹의 사용자가 구성원이 아닌 경우 캐시되지 않기 때문에 요청 시마다 여러 LDAP 디렉토리가 액세스됩니다.

버퍼 크기

서버 소켓에서 전송 버퍼(SndBufSize) 및 수신 버퍼(RcvBufSize)의 크기를 지정할 수 있습니다. 이러한 매개 변수는 `magnus.conf` 파일에서 구성할 수 있습니다. 권장되는 값은 다양한 UNIX 및 Linux 운영 체제에 따라 다릅니다. 이러한 매개 변수를 제대로 설정하려면 운영 체제 설명서를 참조하십시오.

연결 시간 초과

`magnus.conf` 파일에서 *AcceptTimeout* 매개 변수를 사용하여 연결을 종료하기 전에 서버가 클라이언트로부터 데이터가 도착할 때까지 기다리는 시간(초)을 지정할 수 있습니다. 데이터가 지정된 시간까지 도착하지 않으면 연결이 종료됩니다. 이 매개 변수는 기본적으로 30초로 설정됩니다. 대부분의 환경에서 이 설정을 변경할 필요가 없습니다. 이 매개 변수를 기본값보다 작게 설정하여 스레드 수를 늘릴 수 있지만 연결이 느린 사용자의 경우 연결이 끊길 수도 있습니다.

오류 로그 수준

`server.xml()` 파일의 LOG 태그에서 로그 수준 속성을 높이면 서버가 오류 로그에 더 많은 정보를 생성하고 저장합니다. 그러나 항목을 기록하면 해당 파일이 성능에 영향을 줍니다. 문제를 디버깅하는 동안에만 로깅을 늘리고 문제 해결 모드가 아닌 경우 로깅을 최소화합니다.

보안 요구 사항

SSL을 활성화하면 Proxy Server의 개인 정보와 보안 수준은 강화되지만 패킷의 암호화 및 복호화가 오버헤드의 원인이 되기 때문에 성능에 영향을 줍니다. 하드웨어 가속기 카드에 대한 암호화 및 복호화 처리 로드를 줄이는 것이 좋습니다.

Solaris 파일 시스템 캐싱

Proxy Server 캐시는 RAM(Random Access Memory)에 저장되지 않습니다. 파일에 대한 액세스는 캐시에서 문서를 추출할 때마다 파일 시스템에서 수행됩니다. Solaris 파일 시스템 캐싱을 사용하여 Proxy Server 캐시를 메모리에 사전 로드하는 것이 좋습니다. 그러면 캐시된 파일에 대한 참조가 파일 시스템이 아닌 메모리에서 추출됩니다.

시간 초과 값

시간 초과는 서버 성능에 상당한 영향을 줍니다. Proxy Server에 대해 최적의 시간 초과를 설정하면 네트워크 자원을 유지하는 데 도움이 됩니다.

다음과 같이 인스턴스별 SAF(Server Application Function) 두 개와 전역 매개 변수 한 개를 사용하여 Proxy Server 내에서 시간 초과 값을 구성할 수 있습니다.

- 360 페이지 "init-proxy() SAF(obj.conf 파일)"
- 361 페이지 "http-client-config() SAF(obj.conf 파일)"
- 361 페이지 "KeepAliveTimeout() SAF(magnus.conf 파일)"

init-proxy() SAF(obj.conf 파일)

init-proxy() 함수는 Proxy Server의 내부 설정을 초기화합니다. 이 함수는 Proxy Server가 초기화되는 동안 호출되지만 값이 제대로 초기화되었는지 확인하기 위해 obj.conf 파일에서도 지정해야 합니다.

이 함수의 구문은 다음과 같습니다.

```
Init fn=init-proxy timeout=seconds timeout-2=seconds
```

이전 예에서 다음 매개 변수를 init-proxy SAF의 Proxy Server 시간 초과 설정에 직접 적용할 수 있습니다.

- 시간 초과(프록시 시간 초과)– 프록시 시간 초과 매개 변수는 유휴 연결을 중단하기 전에 기다리는 시간을 서버에 알려 줍니다. 프록시 시간 초과 값을 높이면 중요한 프록시 스레드가 커밋되어 클라이언트가 잠재적으로 오랫동안 중단됩니다. 시간 초과 값을 낮추면 데이터베이스 쿼리 게이트웨이와 같이 결과를 생성하는 데 시간이 오래 걸리는 CGI 스크립트가 중단됩니다.

  서버에 가장 적절한 프록시 시간 초과를 결정하기 위해 다음 사항을 고려합니다.

  - Proxy Server가 많은 수의 데이터베이스 쿼리 또는 CGI 스크립트를 처리합니까?
  - Proxy Server가 지정된 시간에 프로세스가 여분으로 사용할 수 있는 충분한 수의 요청을 처리합니까?

    이러한 질문에 대한 답이 예인 경우 프록시 시간 초과 값을 높게 결정할 수 있습니다. 권장되는 최대 프록시 **시간 초과** 값은 1시간입니다. 기본값은 300초(5분)입니다.

    Server Manager의 Preferences 탭 아래에서 Configure System Preferences 페이지에 액세스하여 프록시 시간 초과 값을 보거나 수정할 수 있습니다. 이 매개 변수는 프록시 시간 초과로 참조됩니다.

  timeout-2(중단 이후 시간 초과)– 중단 이후 시간 초과 값은 클라이언트가 트랜잭션을 중단한 후 캐시 기록을 계속하는 시간을 Proxy Server에 알려 줍니다. 즉, Proxy Server가 문서 캐싱을 거의 완료하고 클라이언트가 연결을 종료한 경우 서버는 중단 이후 시간 초과 값에 도달할 때까지 문서를 계속 캐싱할 수 있습니다.

권장되는 최대 중단 이후 시간 초과 값은 5분입니다. 기본값은 15초입니다.

http-client-config() SAF(obj.conf 파일)

http-client-config 함수는 Proxy Server의 HTTP 클라이언트를 구성합니다.

이 함수의 구문은 다음과 같습니다.

```
Init fn=http-client-config
  keep-alive=(true|false)
  keep-alive-timeout=seconds
  always-use-keep-alive=(true|false)
  protocol=HTTP Protocol
  proxy-agent="Proxy-agent HTTP request header"
```

설정은 다음과 같습니다.

- keep-alive– (선택 사항) HTTP 클라이언트가 지속적인 연결을 사용해야 할지 여부를 나타내는 부울 값입니다. 기본값은 true입니다.
- keep-alive-timeout– (선택 사항) 지속적인 연결을 개방 상태로 유지하는 최대 시간(초)입니다. 기본값은 29입니다.
- always-use-keep-alive– (선택 사항) HTTP 클라이언트가 모든 유형의 요청에 대해 기존의 지속적인 연결을 다시 사용할 수 있는지 여부를 나타내는 부울 값입니다. 기본값은 false이며 non-GET 요청 또는 본문이 있는 요청에 대해 지속적인 연결을 다시 사용하지 않음을 의미합니다.
- protocol– (옵션) HTTP 프로토콜 버전 문자열입니다. 기본적으로 HTTP 클라이언트는 HTTP 요청 내용을 기준으로 HTTP/1.0 또는 HTTP/1.1을 사용합니다. 특정 프로토콜 상호 운용성 문제가 발생하지 않는 한 protocol 매개 변수를 사용하지 마십시오.
- proxy-agent– (선택 사항) Proxy-agent HTTP 요청 헤더의 값입니다. 기본값은 Proxy Server 제품 이름과 버전을 포함하는 문자열입니다.

KeepAliveTimeout() SAF(magnus.conf 파일)

KeepAliveTimeout() 매개 변수는 서버가 HTTP 연결 유지 연결 또는 클라이언트와 Proxy Server 사이의 지속적인 연결을 유지하는 최대 시간(초)을 결정합니다. 기본값은 30초입니다. 유휴 시간이 30초를 넘으면 연결 시간이 초과됩니다. 최대값은 300초(5분)입니다.

주의 – `magnus.conf` 파일에서 시간 초과 설정은 클라이언트와 Proxy Server 간의 연결에 적용됩니다. `obj.conf` 파일의 `http-client-config` SAF에서 시간 초과 설정은 Proxy Server와 원래 서버 간의 연결에 적용됩니다.

최신 여부 확인

Proxy Server는 원래 서버에서 문서를 가져오지 않고 로컬 캐시에서 문서를 제공하여 성능을 향상시킵니다. 이 방법의 한가지 단점은 오래된 문서를 제공할 가능성이 있다는 것입니다.

Proxy Server는 검사를 수행하여 문서가 최신 상태인지 여부를 확인한 다음 문서가 오래된 경우 캐시된 버전으로 새로 고칩니다. 문서 확인을 자주 수행하면 Proxy Server의 전체 성능이 저하될 수 있기 때문에 필요한 경우에만 최신 여부 확인을 수행해야 합니다.

최신 여부 확인은 Caching 탭의 Set Cache Specifics 페이지에 구성됩니다. 기본적으로 2시간마다 새 문서를 검사합니다. 이 정보는 max-uncheck 매개 변수를 사용하여 ObjectType 지시문에 구성됩니다.

문서가 최신 상태인지 확인하는 동안 서버의 성능을 향상시키려면 마지막으로 수정된 요소와 관련하여 적절한 문서 수명을 확인하는 방법으로 최신 여부 확인을 사용자 정의합니다.

마지막으로 수정된 요소

마지막으로 수정된 요소는 통보된 이전 변경 사항을 기준으로 문서가 변경될 가능성을 판단하는 데 도움을 줍니다.

마지막으로 수정된 요소는 .02에서 1.0 사이의 분수입니다. 문서의 실제 마지막 수정 및 문서에 대해 마지막 최신 여부 확인을 수행한 시간 사이의 간격을 이 요소 값과 곱합니다. 결과 값을 마지막 최신 여부 확인 이후 시간과 비교합니다. 값이 시간 간격보다 작은 경우 문서가 만료되지 않았습니다. 그러나 값이 시간 간격보다 클 경우 문서는 만료되고 원래 서버에서 새 버전을 가져옵니다.

마지막으로 수정된 요소를 사용하여 최근에 변경된 문서가 이전 문서보다 자주 검사되는지 확인할 수 있습니다.

마지막으로 수정된 요소를 0.1에서 0.2 사이로 설정해야 합니다.

DNS 설정

DNS는 표준 IP 주소를 호스트 이름과 연결하는 데 사용되는 시스템입니다. 이 시스템은 적절하게 구성되지 않을 경우 중요한 Proxy Server 자원을 독점할 수 있습니다. 성능을 최적화하려면 다음 옵션을 고려하십시오.

- DNS 캐싱 사용

  DNS 캐싱은 Server Manager의 Preferences 탭 아래에서 Configure DNS Cache 링크를 선택하면 활성화됩니다. DNS 캐싱의 Enabled 라디오 버튼을 선택합니다.

- 클라이언트 DNS 이름이 아닌 클라이언트 IP 주소만 기록합니다.

  클라이언트 DNS 이름 로깅은 Server Manager의 Server Status 탭 아래에서 Set Access Log Preferences 링크를 선택하면 비활성화됩니다. 클라이언트 호스트 이름이 아닌 IP 주소를 기록하려면 IP Addresses 라디오 버튼을 선택합니다.

- 역방향 DNS를 비활성화합니다.

  역방향 DNS는 IP 주소를 호스트 이름으로 변환합니다. 역방향 DNS는 Server Manager의 Preferences 탭 아래에서 Configure System Preferences 링크를 선택하면 비활성화됩니다. 역방향 DNS를 비활성화하려면 No 라디오 버튼을 선택합니다.

- 클라이언트 호스트 이름에 기반한 액세스 제어 방지

  가능한 경우 액세스 제어문의 호스트 이름 대신 클라이언트의 IP 주소를 사용합니다.

스레드 수

magnus.conf 파일의 RqThrottle 매개 변수는 Proxy Server가 처리할 수 있는 최대 동시 트랜잭션 수를 지정합니다. 기본값은 128입니다. 서버를 제어하도록 이 값을 변경하여 수행되는 트랜잭션 대기 시간을 최소화합니다.

동시 요청 수를 계산하기 위해 서버는 활성 요청 수를 계산합니다. 서버는 새 요청이 도착하면 값에 1을 더하고 요청이 완료되면 1을 뺍니다. 새 요청이 도착하면 서버가 최대 요청 수를 이미 처리 중인지 여부를 확인합니다. 제한에 도달하면 새 요청 처리는 활성 요청 수가 최대값 이하로 떨어질 때까지 지연됩니다.

perfdump 또는 `proxystats.xml` 데이터에 의해 생성된 데이터의 SessionCreationInfo 부분을 보고 동시 요청 수를 모니터링할 수 있습니다. 이 정보를 통해 총 스레드 수(제한)와 비교하여 동시 최고 요청의 최대 수를 결정할 수 있습니다. 다음은 `perfdump` 출력에서 전달된 정보입니다.

```
SessionCreationInfo:
------------------------
Active Sessions          1
Keep-Alive Sessions      0
Total Sessions Created   48/128
```

Active Sessions에서는 현재 요청을 서비스하는 세션(스레드를 처리 중인 요청) 수를 표시합니다. Keep-Alive Sessions는 Active Sessions와 비슷하지만 연결 유지 연결과 관련됩니다. Total Sessions Created에는 생성된 세션 수와 허용된 최대 세션 수 모두를 표시합니다. 이러한 값은 RqThrottle 값의 최소값 및 최대값입니다.

주의 – RqThrottleMin은 서버가 시작 시 시작하는 최소 스레드 수입니다. 기본값은 48입니다. 또한 이 매개 변수를 `magnus.conf` 파일에서 설정할 수 있지만 기본적으로는 나타나지 않습니다.

구성된 스레드의 최대값에 도달하는 것이 반드시 부정적인 것은 아닙니다. 자동으로 RqThrottle 값을 높일 필요는 없습니다. 이러한 제한에 도달했다는 것은 최고 로드에서 서버에 그만큼의 스레드가 필요했음을 나타냅니다. 서버가 적절한 시기에 요청을 수행할 수 있는 한 서버는 적절하게 조정됩니다. 그러나 이 시점에서 연결은 연결 대기열에 대기하게 되고 이로 인해 잠재적으로 오버플로될 수 있습니다. `perfdump` 출력은 일반적으로 총 세션 생성 값이 거의 RqThrottle 최대값에 도달하는 경우 스레드 제한을 높여야 함을 보여 줍니다.

적절한 RqThrottle 값은 로드에 따라 100에서 500 사이의 범위에 있습니다.

인바운드 연결 풀

인바운드 연결 풀은 다음을 포함하여 KeepAlive* 설정과 magnus.conf의 관련 설정을 사용하여 조정할 수 있습니다.

- MaxKeepAliveConnections
- KeepAliveThreads
- KeepAliveTimeout
- KeepAliveQueryMaxSleepTime
- KeepAliveQueryMeanTime
- ConnQueueSize
- RqThrottle
- acceptorthreads

이러한 매개 변수에 대한 자세한 내용은 다음 사이트에서 Sun ONE Web Server 6.1 SP6 *Performance Tuning, Sizing, and Scaling Guide*의 2장을 참조하십시오.

http://docs.sun.com/app/docs/doc/819-6516/

아웃바운드 연결 풀 설정은 이 릴리스의 Proxy Server에서 구성할 수 없습니다.

FTP 목록 너비

FTP 목록 너비를 늘리면 긴 파일 이름을 사용할 수 있기 때문에 파일 이름이 잘리는 것을 줄여줍니다. 기본 너비는 80자입니다.

FTP 목록 너비는 Server Manager의 Preferences 탭 아래에서 Tune Proxy 링크를 선택하여 수정할 수 있습니다.

캐시 아키텍처

캐시를 적절하게 구성하면 서버 성능을 향상시킬 수 있습니다. 캐시 구성 시 유의해야 할 권장 사항은 다음과 같습니다.

- 로드를 분산시킵니다.
- 여러 프록시 캐시 파티션을 사용합니다.
- 여러 디스크 드라이브를 사용합니다.
- 여러 디스크 컨트롤러를 사용합니다.

적절한 캐시 설정은 Proxy Server 성능에 중요합니다. 프록시 캐시 구성 시 유의해야 할 가장 중요한 규칙은 로드를 분산시키는 것입니다. 캐시를 파티션당 약 1GB로 설정하고 여러 디스크와 디스크 컨트롤러 전체에 분산시켜야 합니다. 이러한 유형의 정렬은 단일 대용량 캐시보다 신속한 파일 생성 및 검색 기능을 제공합니다.

캐시 일괄 업데이트

캐시 일괄 업데이트 기능을 사용하여 지정된 웹 사이트에서 파일을 미리 로드하거나 캐시에 이미 있는 문서에 대한 최신 검사를 수행할 수 있습니다. 이 기능은 일반적으로 Proxy Server의 로드가 가장 낮을 때 시작됩니다. URL의 배치를 생성, 편집 및 삭제할 수 있으며 Cache Batch Updates 페이지에서 일괄 업데이트를 활성화 및 비활성화할 수 있습니다.

요청 시 캐싱과 달리 배치에 업데이트할 파일을 지정하여 적극적으로 내용을 캐시할 수 있습니다. Proxy Server를 사용하여 캐시에서 현재 여러 파일에 대한 최신 검사를 수행하거나 특정 웹 사이트에서 여러 파일을 미리 로드할 수 있습니다.

서버 및 프록시 네트워크가 있는 대형 사이트의 경우 일괄 업데이트를 사용하여 웹의 지정된 영역을 미리 로드할 수 있습니다. 배치 프로세스는 문서의 링크 전체에서 재귀적 하강을 수행하고 내용을 로컬로 캐시합니다. 이 기능은 원격 서버에 부담을 줄 수 있기 때문에 주의해야 합니다. `bu.conf` 구성 파일의 매개 변수는 프로세스가 무제한적으로 재귀를 수행하는 것을 방지하고 이 프로세스에 대한 일부 제어를 제공합니다.

Proxy Server 액세스 로그를 사용하여 가장 일반적으로 활성화된 사이트를 확인하고 성능을 향상시키기 위해 이러한 사이트에 대한 일괄 업데이트를 수행합니다.

가비지 컬렉션

가비지 컬렉션은 Proxy Server 캐시를 검토하고 오래된 파일을 제거하는 프로세스입니다. 가비지 컬렉션은 자원을 집중적으로 사용하는 프로세스입니다. 따라서 성능을 향상시키기 위해 일부 가비지 컬렉션 설정을 조정해야 합니다.

다음 매개 변수는 가비지 컬렉션 프로세스를 미세 조정하기 위한 기능을 제공합니다. Server Manager의 Caching 탭 아래에서 Tune GC를 선택하여 찾을 수 있는 Tune Garbage Collection 양식에서 이러한 매개 변수를 보거나 수정할 수 있습니다. 매개 변수는 다음과 같습니다.

- *gc hi margin percent*
- *gc lo margin percent*
- *gc extra margin percent*
- *gc leave fs full percent*

gc hi margin percent 변수

gc hi margin percent 변수는 최대값에 도달하면 가비지 컬렉션을 트리거하는 최대 캐시 크기의 백분율을 제어합니다.

이 값은 gc lo margin percent 값보다 커야합니다.

gc hi margin percent의 유효한 범위는 10에서 100% 사이입니다. 기본값은 80%로, 캐시 사용률이 80%일 때 가비지 컬렉션이 트리거됩니다.

gc lo margin percent 변수

gc lo margin percent 변수는 가비지 컬렉터가 목표로 하는 최대 캐시 크기의 백분율을 제어합니다.

이 값은 gc hi margin percent 값보다 작아야 합니다.

gc lo margin percent의 유효한 범위는 5에서 100% 사이입니다. 기본값은 70%이며 가비지 컬렉션 후 캐시 사용률 70%를 목표로 합니다.

gc extra margin percent 변수

파티션 크기가 최대 허용 크기(gc hi margin percent)에 도달하는 것 이외의 이유로 가비지 컬렉션이 트리거되는 경우 가비지 컬렉터는 gc extra margin percent 변수에 의해 설정된 백분율을 사용하여 제거할 캐시 부분을 결정합니다.

gc extra margin percent의 유효한 범위는 0에서 100% 사이입니다. 기본값은 30%이며 기존 캐시 파일의 30%를 제거합니다.

gc leave fs full percent 변수

gc leave fs full percent 값은 가비지 컬렉션이 발생하지 않는 캐시 파티션 크기의 백분율을 결정합니다. 이 값은 일부 다른 응용 프로그램이 디스크 공간을 독점하는 경우 가비지 컬렉터가 캐시의 모든 파일을 제거하지 않도록 합니다.

gc leave fs full percent의 유효한 범위는 0(전체 제거 허용)에서 100%(제거하지 않음) 사이입니다. 기본값은 60%이며 캐시 크기를 현재 크기의 60%로 축소할 수 있습니다.

Solaris 성능 조정

Solaris 커널의 다양한 매개 변수를 사용하여 Proxy Server 성능을 미세 조정할 수 있습니다. 다음 표에 이러한 매개 변수 몇 개가 나열되어 있습니다.

표 19–1 Solaris 성능 조정 매개 변수

매개 변수	범위	기본값	조정값	설명
rlim_fd_max	/etc/system	1024	8192	열린 파일 설명자 제한 프로세스입니다. 해당하는 경우 관련 소켓, 파일 및 파이프에 대한 예상 로드를 고려해야 합니다.
rlim_fd_cur	/etc/system	64	8192	
sq_max_size	/etc/system	2	0	스트림 드라이버 대기열 크기를 제어합니다. 이 매개 변수를 0으로 설정하면 성능 실행이 버퍼 공간 부족으로 인한 영향을 받지 않습니다. 클라이언트에서도 이 매개 변수를 설정합니다.
tcp_close_wait_interval	ndd/dev/tcp	240000	60000	클라이언트에서도 이 매개 변수를 설정합니다.
tcp_conn_req_max_q	ndd/dev/tcp	128	1024	
tcp_conn_req_max_q0	ndd/dev/tcp	1024	4096	
tcp_ip_abort_interval	ndd/dev/tcp	480000	60000	
tcp_keepalive_interval	ndd/dev/tcp	7200000	900000	트래픽이 많은 웹 사이트의 경우 이 값을 줄입니다.

표 19–1 Solaris 성능 조정 매개 변수 *(계속)*

매개 변수	범위	기본값	조정값	설명
tcp_rexmit_interval_initial	ndd/dev/tcp	3000	3000	재전송률이 30-40%보다 큰 경우 이 값을 늘립니다.
tcp_rexmit_interval_max	ndd/dev/tcp	240000	10000	
tcp_rexmit_interval_min	ndd/dev/tcp	200	3000	
tcp_smallest_anon_port	ndd/dev/tcp	32768	1024	클라이언트에서도 이 매개 변수를 설정합니다.
tcp_slow_start_initial	ndd/dev/tcp	1	2	데이터 양이 적은 경우 약간 빠르게 전송됩니다.
tcp_xmit_hiwat	ndd/dev/tcp	8129	32768	이 매개 변수를 사용하여 전송 버퍼를 늘립니다.
tcp_recv_hiwat	ndd/dev/tcp	8129	32768	이 매개 변수를 사용하여 수신 버퍼를 늘립니다.

이러한 매개 변수에 대한 자세한 내용은 다음 사이트에서 Sun ONE Web Server 6.1 SP6 *Performance Tuning, Sizing, and Scaling Guide*의 5장을 참조하십시오.

http://docs.sun.com/app/docs/doc/819-6516/

색인

번호와 기호

3.6 서버 마이그레이션, 34

A

acceptorthreads 지시문, 364
AcceptTimeout 지시문, 359
Access Control Rules For 페이지, 옵션, 153-158
ACE, 40-41
ACL
  Digest 인증 절차, 142
  LDAP 데이터베이스로 매핑, 58
  obj.conf, 참조, 356
  경로, 351
  권한 부여문, 353-355
  기본 파일, 355
  명명된, 352
  비활성화, 158
  사용자 캐시, 146
  속성 표현식, 354
  유형, 351
  인증문, 352
  자원, 351
ACL 사용자 캐시 조정, 358
ACL 파일
  구문, 351-356
  기본, 355
  예, 147
  위치, 145
  이름, 146
ACLCacheLifetime 지시문, 146, 358
ACLGroupCacheSize 매개 변수, 146, 358
aclname, PathCheck 지시문, 356
ACLUserCacheSize 매개 변수, 146, 358
Administration Server
  SNMP 마스터 에이전트 시작, 210-211
  URL, 26-27
  개요, 26-27
  로그 파일, 39-40
  사용자 이름 변경 시 이전 값 제거, 55
  사용자 인터페이스, 26-27
  수퍼유저 액세스, 37-38
  시작, 31-32
  액세스, 26-27
  중지, 32-33, 119-120
Administration Server 다시 시작, 31-32
Administration Server 탭
  Cluster, 27
  Global Settings, 27
  Preferences, 26
  Security, 27
  Servers, 26
  Users and Groups, 27
admpw 파일, 37, 38
Allow 또는 Deny, 액세스 제어, 153
always-use-keep-alive 매개 변수, 361
and 연산자, 355
APPLET, 292
attributes, LDAP URL, 59

B

base_dn(LDAP URL 매개 변수), 59
Basic 인증, 44, 139, 155, 352
Basic 인증 및 SSL, 139
bong-file, 106
bu, 259
bu.conf, 123

C

c 속성, 103
Cache-info, 222
cachegc, 259
Caching 탭, 28
cbuild, 254
certmap.conf
  LDAP 검색, 101
  구문, 102
  기본 등록 정보, 102
  매핑 예제, 104
  위치, 102
  정보, 102-105
  클라이언트 인증서, 140
certSubjectDN, 105
CGI 프로그램, 35, 145, 157, 360
check-acl 함수, 356
CKL, 설치 및 관리, 83
Client-ip, 220
client-pull, 125
Cluster 탭, 27
CmapLdapAttr, 104, 105
cn 속성, 49, 58, 103
common-log, 172
common logfile format, 예, 179
CONFIG, 205, 207
config 디렉토리, 29
CONNECT 메소드, 프록싱, 216
ConnQueueSize 지시문, 364
contains, 검색 유형 옵션, 52
CRL, 설치 및 관리, 83
cron 기반 로그 교체, 171
Custom Logic File, 279

D

dayofweek, 355
dbswitch.conf, 44-45, 155
dbswitch.conf 변경 사항
  LDAP, 44
  다이제스트 파일, 45
  키 파일, 44
Default 인증, 139, 154
DELETE 메소드, 157
Deny 또는 Allow, 액세스 제어, 153
DES 알고리즘, Directory Server 설정, 144
Digest 인증
  사용, 141-142
  액세스 제어 옵션, 155
  인증문, 352
  플러그인, 설치, 143-145
digestauth 등록 정보, 141
DigestStaleTimeout 매개 변수, 142
Directory Server, Sun Java System, 37
DN(고유 이름)
  예제, 46
  정보, 46, 48
  형식, 48
DN 이해, 46
DNComps, 102
DNS, 124
  사용 설정, 145
  설정 및 성능, 363
  역방향 DNS 조회, SOCKS 서버, 313
  조회 및 서버 성능, 145
  호스트-IP 인증, 145
DNS 캐시, 133-134

E

e 속성, 103
ends with, 검색 유형 옵션, 52

F

fast-demo 모드, 225
FAT 파일 시스템, 보안, 74
filter, LDAP URL 매개 변수, 59

FilterComps, 103
Filters 탭, 28
FindProxyForURL, 332
FIPS-140, 96
flex-init, 171
flex-log, 171
flexanlg, 181
  사용 및 구문, 188
FTP, 목록 너비, 365
FTP 모드
  능동 모드(PORT), 225
  수동 모드(PASV), 225

G

gc extra margin percent 변수, 366
gc hi margin percent 변수, 366
gc leave fs full percent 변수, 367
gc lo margin percent 변수, 366
generated-proxy-(serverid).acl, 146
genwork-proxy-(serverid).acl, 146
GET 메소드, 157
  쿼리 결과를 캐시해야 함, 246
  프록싱, 216
givenName 속성, 48
Global Settings 탭, 27
groupOfURLs, 57
GUI 개요, 26-29

H

HEAD 메소드, 157
  프록싱, 216
Help 버튼, 27
HP OpenView 네트워크 관리 소프트웨어, SNMP와 함께 사용, 191
HTML 태그 필터링, 291
http-client-config SAF, 361
http_head, 157
HTTP 요청 로드 균형 조정, 227-228
httpacl 디렉토리, 146
HTTPS, SSL, 87

I

ICP, 124
  동급, 260
  상위, 260
  상위 프록시 추가, 263-264
  이웃, 260
  폴링 라운드, 261
icp.conf, 123
ICP(Internet Cache Protocol), 260
ID, 313
IMG, 292
INDEX 메소드, 157
inetOrgPerson, 객체 클래스, 48
INIT, 210
init-clf, 172
init-proxy SAF, 360-361
InitFn, 104
inittab, 74
IP 기반 액세스 제어, 163
iplanetReversiblePassword, 144
iplanetReversiblePasswordobject, 144
is, 검색 유형 옵션, 52
isn't, 검색 유형 옵션, 52
issuerDN, 102

J

Java IP 주소 확인, 223
JavaScript
  반환 값, 337
  프록시 자동 구성 파일, 332
JROUTE, 228
JSESSIONID, 228
jsessionid, 228

K

keep-alive-timeout 매개 변수, 361
keep-alive 매개 변수, 361
KeepAliveQueryMaxSleepTime 지시문, 364
KeepAliveQueryMeanTime 지시문, 364
KeepAliveThreads 지시문, 364
KeepAliveTimeout 지시문, 361-362, 364

keepOldValueWhenRenaming 매개 변수, 55

L

l 속성, 103
LDAP
  Digest 인증, 141-142
  검색 결과, 101
  검색 및 certmap.conf, 101
  검색 필터, 51, 60
  그룹, 만들기, 55
  그룹, 찾기, 60-62
  디렉토리, 액세스 제어, 155
  디렉토리 서비스, 정보, 44
  분산 관리, 사용 설정, 38
  사용자, 만들기, 48-49, 49
  사용자, 찾기, 51-53
  사용자 및 그룹 관리, 43-69
  사용자 이름 및 비밀번호 인증, 139
  사용자 정의 검색 필터, 51-52
  속성, 사용자 항목, 48
  조직 단위, 만들기, 66
  조직 단위, 찾기, 66-68
  클라이언트 인증서 매핑, 100-101
  항목, 46, 47-48, 48-49
LDAP URL
  동적 그룹, 56, 57-58
  필수 매개 변수, 58
  형식, 58
ldapmodify, 고유 UID에 대한 주의 사항, 48
LDIF
  가져오기 및 내보내기 기능, 47
  데이터베이스 항목 추가, 47
libdigest-plugin.ldif, 143
libdigest-plugin.lib, 143
libnssckbi.so, 82
libplds4.dll, 143
Library 등록 정보, 104
libspnr4.dll, 143
log_anly, 181
LOG 요소, 169
ls1 청취 소켓, 35

M

magnus.conf, 123, 200
  내용, 29
  보안 항목, 91
  성능 관련 설정, 357-368
  종료 시간 초과, 142
magnus.conf.clfilter, 123
mail 속성, 49, 103
management information base, 202
max-uncheck 매개 변수, 362
MaxKeepAliveConnections 지시문, 364
MD5 알고리즘, 141
memberCertDescriptions, 56
memberURLs, 56
mime.types, 내용, 29
mime 유형, 123
MIME 유형 범주
  enc, 130
  lang, 130
  type, 130
MIME 필터, 290
MKDIR 메소드, 157
modutil, PKCS#11 설치에 사용, 93
MOVE 메소드, 157

N

NameTrans 지시문, 192
Netscape Navigator, SSL, 87
NMS에서 시작된 통신, 212
no-network 모드, 225
nobody 사용자 계정, 서버 사용자, 124
nonce, 142
not 연산자, 355
NSAPI 플러그인, 사용자 정의, 21
nsldap32v50.dll, 143
NSS, 및 마이그레이션된 인증서, 81
nssckbi.dll, 82
NSServletService, 199
NTFS 파일 시스템, 비밀번호 보호, 74

O

o 속성, 103
obj.conf, 123, 171, 192, 200
  ACL 파일 참조, 356
  Default 인증, 139
  내용, 29
  및 명명된 ACL, 352
  성능 관련 설정, 357-368
obj.conf.clfilter, 123
or 연산자, 355
organizationalPerson, 객체 클래스, 48
organizationalUnit, 객체 클래스, 46
Other, 인증 옵션, 155
ou 속성, 103

P

PAC 파일, 278
  PAT 파일에서 생성
    수동, 278-279
    자동, 279
pac 파일
  만들기, 334-336
  정의, 335
  프록시에서 제공, 331
parent.pat, 123
parray.pat, 123
password.conf, 74
PAT 파일, 269, 278
PathCheck, 키 크기 제한, 106
PathCheck 지시문, 356
perfdump, 363
perfdump 유틸리티
  사용 설정, 196
  성능 보고, 200
  정보, 196
perfdump 출력, 197-199
person, 객체 클래스, 48
pk12util
  인증서 및 키 가져오기, 94-95
  인증서 및 키 내보내기, 94
  정보, 93
PKCS#11
  modutil을 사용하여 설치, 93
PKCS#11 (계속)
  pk12util을 사용하여 인증서 및 키 가져오기, 94-95
  pk12util을 사용하여 인증서 및 키 내보내기, 93
  모듈, 74
POST 메소드, 157
  프록싱, 216
Preferences 탭
  Administration Server, 26
  Server Manager, 27
program no-cache, 110
PROTOCOL_FORBIDDEN, 106
protocol 매개 변수, 361
proxy-agent 매개 변수, 361
Proxy-auth-cert, 222
Proxy Auto Configuration, 278
Proxy-cipher, 221
proxy-id.acl, 123
Proxy-issuer-dn, 222
proxy-jroute, 228
Proxy-keysize, 221
Proxy-secret-keysize, 221
Proxy Server
  개요, 25-29
  관리, 31-34
  구성, 26-29
  기능, 21, 25-26
  마이그레이션, 34
  액세스 제어, 137-165
  정보, 25
  조정, 125-126
Proxy-ssl-id, 221
Proxy-user-dn, 222
proxystats.xml, 195, 363
PUT 메소드, 157

Q

quench updates, 313

R

rc.local, 74

RcvBufSize, 359
Refresh 버튼, 27
REQ_ABORTED, 106
REQ_NOACTION, 106
REQ_PROCEED, 106
request-digest, 142
respawn, 118
Restart Required, 28
RFC 1413 ID 응답, 313
rlim_fd_cur 매개 변수, 367
rlim_fd_max 매개 변수, 367
RMDIR 메소드, 157
Routing 탭, 27
RqThrottle 매개 변수, 363, 364
RqThrottleMin 매개 변수, 364
RSA MD5 알고리즘, 235

S

sagt, 205
sagt, command for starting Proxy SNMP agent, 205
scope, LDAP URL 매개 변수, 59
SCRIPT, 292
secret-keysize, 106
Security 탭
  Administration Server, 27
  Server Manager, 28
send-cgi, 199
Server Manager
  개요, 27-28
  로그 분석기 실행, 187
  사용자 인터페이스, 27-28
  액세스, 27-28
Server Manager 탭
  Caching, 28
  Filters, 28
  Preferences, 27
  Routing, 27
  Security, 28
  Server Status, 28
  SOCKS, 27
  Templates, 28
  URs, 28
server-push, 125
Server Status 탭, 28
server.xml, 122, 123, 169
  내용, 29
  및 액세스 제어, 356
  액세스 제어, 146
  외부 인증서, 95, 96
  자세한 내용, 146
server.xml.clfilter, 123
servercertnickname, 96
Servers 탭, 26
SessionCreationInfo, 363
SET, SNMP 메시지, 212
SMUX, 203
sn 속성, 48
SndBufSize, 359
SNMP
  GET 및 Set 메시지, 212
  기본, 201
  마스터 에이전트, 202
    설치, 204-205
  서버 설정, 203
  실시간으로 서버의 상태 확인, 191
  커뮤니티 문자열, 211
  트랩, 211
  프록시 에이전트, 204
  하위 에이전트, 202
SNMP 마스터 에이전트 및 하위 에이전트, 41
snmpd, command for restarting native SNMP
  daemon, 205
snmpd.conf, 205
SOCKS, 정보, 309
SOCKS 서버
  ID, 313
  Proxy Server에 포함, 310-312
  socks5.conf 파일, 310, 311-312
  구성, 312-314
  라우팅 항목, 319-323
  성능, 311-312, 313
  액세스 제어, 311
  역방향 DNS 조회, 313
  연결 항목, 316-319
  옵션, 312
  인증, 315
  인증 항목, 314-316

SOCKS 서버 *(계속)*
작업자 및 승인 스레드, 311, 313
정보, 309
조정, 311-312, 313
체인, 319
SOCKS 탭, 27
SOCKS 항목 이동, 316, 319
socks5.conf, 123, 310
위치, 311-312
정보, 311-312
추가 정보, 311-312
SOCKS5_PWDFILE 지시문, 311
Solaris
성능 조정 매개 변수, 367-368
파일 시스템 캐싱, 359
sounds like, 검색 유형 옵션, 52
sq_max_size 매개 변수, 367
SSL
2.0 프로토콜, 90
3.0 프로토콜, 84, 90
HTTPS, 87
Netscape Navigator, 87
telnet 홉, 88
데이터 흐름, 86
및 Basic 인증, 139
사용, 89-91
성능 영향, 359
인증 방법, 140, 155, 352
정보, 85
터널링, 86-87, 87-88, 88
프록싱, 86
하드웨어 가속기, 93
활성화에 필요한 정보, 77
SSL/TLS 암호화, 220
SSLPARAMS, 96
st 속성, 103
starts with, 검색 유형 옵션, 52
startsvr.bat, 118
stats-init, 192
stats-xml, 192
stopsvr.bat, 120
Sun Crypto Accelerator 4000, Proxy Server에서
활성화, 75-76
Sun Crypto Accelerator 키 저장소, 75-76
Sun Java System Directory Server, 37
sysContact, 208
sysContract, 209
sysLocation, 208, 209

T

tcp_close_wait_interval 매개 변수, 367
tcp_conn_req_max_q 매개 변수, 367
tcp_conn_req_max_q0 매개 변수, 367
tcp_ip_abort_interval 매개 변수, 367
tcp_recv_hiwat 매개 변수, 368
tcp_rexmit_interval_initial 매개 변수, 368
tcp_rexmit_interval_max 매개 변수, 368
tcp_rexmit_interval_min 매개 변수, 368
tcp_slow_start_initial 매개 변수, 368
tcp_smallest_anon_port 매개 변수, 368
tcp_xmit_hiwat 매개 변수, 368
telephoneNumber 속성, 49
telnet 홉, 보안 위험, 88
Templates 탭, 28
timeofday, 355
timeout-2 매개 변수, 360
title 속성, 49
TLS, 정보, 85, 90
TLS 및 SSL 3.0 암호, Netscape Navigator 6.0, 91
tlsrollback, 90
Transport Layer Security, 85
triple DES 암호, 96

U

uid 속성, 49, 103
uniqueMembers, 56
URL
Administration Server, 26-27
LDAP, 56, 57-58, 58
SSL 사용 서버, 91
매핑 제거, 231
미러 서버로 매핑, 228
요청 처리, 29
URL 요청, 29
URL 요청 처리, 29

urldb, 255
URLs 탭, 28
userPassword 속성, 49
Users and Groups 탭, 27, 46

V
verifycert, 103
VeriSign 인증 기관, 76
VeriSign 인증서
  설치, 76-77
  요청, 76
Version 버튼, 27

X
x509v3 인증서, 속성, 103

가
가비지 컬렉션, 조정, 366-367
가속기, 하드웨어, 93, 95

개
개요
  Administration Server, 26-27
  GUI, 26-29
  Proxy Server, 25-29
  Server Manager, 27-28
  SOCKS 서버, 310-312
개인 키, 85

검
검색
  그룹, 60-62
  사용자, 51
  조직 단위, 66-68
검색 결과
  그룹, 61-62
  사용자, 51-52
  조직 단위, 67-68
검색 결과, LDAP, 101
검색 기반(기본 DN), 48
검색 속성, 51
검색 옵션, 목록, 52
검색 쿼리, LDAP, 51-52
검색 필드, 유효한 항목, 51
검색 필터, LDAP, 51, 60

경
경로 ACL, 351

계
계층, ACL 권한 부여문, 353-354

공
공용 키, 73, 78, 85

관
관리
  CRL 및 CKL, 83-84
  Proxy Server, 26-29, 31-34
  SOCKS 서버, 309-323
  그룹, 60
  그룹 소유자, 64
  사용자, 51
  사용자 및 그룹, 43-69
  사용자 비밀번호, 54
  서버, 26-29
  서버 클러스터, 111-115
  인증서, 82-83
  조직 단위, 66-69
  청취 소켓, 35-36
  추가 참조, 64

관리 *(계속)*
클러스터, 111-115
관리 기본 설정, 35-41
관리된 객체, 212
관리자, 여러, 38-39

구

구문, ACL 파일, 351-356
구성
ACL 사용자 캐시, 146
ACL 캐시, 132-133
DNS 캐시, 133
DNS 하위 도메인, 134
HTTP 연결 유지, 135-136
LOG 요소, 178
Proxy Server, 26-29
SOCKS 서버, 311-312, 312-314
SSL 터널링, 87-88
Sun Crypto Accelerator, 75
가상 멀티호스팅, 306-307
공유, 111
디렉토리 서비스, 45-46
라우팅, 217-218
보안 역방향 프록시, 297
역방향 프록시에서의 클라이언트 인증, 99-100
캐시, 244
구성 파일
essential, 29
magnus.conf, 29
mime.types, 29
obj.conf, 29
server.xml, 29
socks5.conf, 311-312
위치, 29
자세한 정보, 29
정보, 28-29
구성원
그룹 추가, 63
그룹에 대해 정의, 55
추가, 62-63
구성원 URL, 예, 57

권

권한, 액세스, 157
권한 부여문, ACL, 353-355

그

그룹, 61-62
참조 추가, 관리
검색, 60-62
검색 결과 좁히기, 61-62
관리, 60
구성원 정의, 55
구성원 추가, 62-63
그룹을 구성원 목록에 추가, 63
동적, 57-59
만들기, 55-59
만들기 지침, 동적, 58-59
만들기 지침, 정적, 56
정보, 55
정적, 56-57
찾기, 60-62
항목 편집, 62
그룹 구성원
정의, 55
정적 및 동적, 58
그룹 및 사용자
관리, 43-69
인증, 154-155
그룹 소유자, 관리, 64

기

기능, Proxy Server, 21, 25-26
기본
모드, 224
액세스 제어 규칙, 153
기본 DN, 48
기본값, 디렉토리 서비스, 44-45

날

날짜 제한, 액세스 제어, 158, 161

내
내부 데몬 로그 교체, 170

너
너비, FTP 목록, 365

네
네트워크 관리 스테이션(NMS), 201
네트워크 연결 모드
  fast-demo, 225
  no-network, 225
  기본, 224
  일반, 224

다
다이제스트 파일
  사용자 찾기, 51-53
  사용자 항목 만들기, 50

단
단위, 조직, 만들기, 66

대
대역폭, 절약, 238

데
데이터 스트림, SSL, 87
데이터베이스, 인증, 155
데이터베이스, 트러스트
  만들기, 73
  비밀번호, 108
데이터베이스 인증, 163-165
데이터베이스 항목, LDIF를 사용하여 추가, 47

동
동적 그룹
  구현, 57-58
  만들기, 59
  서버 성능에 미치는 영향, 58
  정보, 56, 57-59
  지침, 58-59

디
디렉토리, 액세스 제한, 160
디렉토리 서버
  DES 알고리즘, 144
  ldapmodify 명령줄 유틸리티, 48
  분산 관리, 38-39
  사용자 항목, 48
디렉토리 서비스
  LDAP, 44
  구성, 45-46
  다이제스트 파일, 45
  만들기, 45-46
  유형, 44-45
  정보, 44-45
  키 파일, 44
  편집, 46

라
라우팅, 구성, 217-218
라우팅 항목, SOCKS, 319-323

로
로그, 액세스, 171
로그, 액세스, 위치, 167
로그, 오류
  보기, 180
  위치, 167
로그 교체
  cron 기반, 171
  내부 데몬, 170
로그 분석기, flexanlg, 사용 및 구문, 188

로그 수준, 169
로그 파일
  Administration Server, 39-40
  Linux OS의 경우 2GB 크기 제한, 168
  SOCKS 서버, 311
  구성, 171
  기본 설정, 39-40
  보기, 39-40
  아카이브, 170
  액세스 로그, 39
  오류 로그, 40
  위치, 39-40
  유연한 형식, 176
로그 파일 보기, 39-40
로그 파일 형식
  extended2, 177
  공통, 173, 177
  확장, 177
로드 균형 조정, 299

루

루트 인증서, 제거 및 복원, 82

릴

릴리스 노트, 21

마

마스터 에이전트, 41
  SNMP, 202
  SNMP, 설치, 204-205
  비표준 포트에서 시작, 210
마지막으로 수정된 요소, 362
마지막으로 수정된 헤더, 캐시해야 함, 246

만

만들기
  SOCKS 항목, 314-315, 316-318, 320-321, 321-322
  그룹, 55-59
  동적 그룹, 59
  디렉토리 서비스, 45-46
  사용자 정의 NSAPI 플러그인, 21
  정적 그룹, 57
  조직 단위, 66
  트러스트 데이터베이스, 73-74
만료 정책, 239
만료 헤더, 캐시해야 함, 246

매

매개 변수 중단 이후 시간 초과, 360
매핑
  ACL을 LDAP 데이터베이스로, 58
  URL을 미러 서버로, 228
  클라이언트 인증서를 LDAP 항목으로, 100-101

명

명령줄, flexanlg를 사용하여 액세스 로그 파일 분석, 188
명명된 ACL, 352

모

모듈, PKCS#11, 74, 92
모든 서버, 관리, 26-27

목

목록 권한, 157

문

문서 수명, 확인, 362
문서 수명 확인, 362

미
미러 사이트, URL 매핑, 228

반
반환 값, 자동 구성 파일, 337

버
버퍼 크기, 성능 영향, 359

변
변경
  SOCKS 항목의 위치, 316
  기본 FTP 전송 모드, 225-226
  사용자 항목, 53-54
  수퍼유저 설정, 37-38
  액세스 거부 메시지, 158
  키 쌍 파일 비밀번호, 108
  트러스트 데이터베이스 비밀번호, 108-109
변조된 키 목록(CKL), 83

별
별칭, 및 3.x 인증서, 81
별칭 디렉토리, 81, 82
별칭 파일, 82

보
보고서
  데이터 흐름 보고서, 182-183
  상태 코드 보고서, 183
  시간별 작동 보고서, 186
  요청 및 연결 보고서, 183-184
  전송 시간 보고서, 186
  전송 시간 분산 보고서, 182
  캐시 성능 보고서, 184-186
보고서 생성, 187
보기, 180
보안
  magnus.conf의 보안 매개 변수, 91
  성능 영향, 359
  위험, 88
  증가, 107
  프록시 및 SSL, 87
보안, 액세스 제한 기준, 162
보안 기본 설정, 설정, 84-92

분
분산 관리
  기본 디렉토리 서비스, 45
  사용자 수준, 38
  수퍼유저 액세스, 37
  여러 관리자, 38-39

비
비밀번호
  만들기 지침, 108
  수퍼유저, 37
비밀번호 보호, NTFS 파일 시스템, 74
비밀번호 파일, 311

사
사용
  IP 기반 액세스 제어, 163
  SSL, 89-91
  청취 소켓용 보안, 89-91
사용 설정, DNS, 145
사용자
  DN 형식, 48
  검색, 51
  검색 결과 좁히기, 51-52
  관리, 43-69
  만들기, 47-50
  삭제, 55
  이름 변경, 54-55
  제거, 55

사용자 *(계속)*
편집, 53-54
사용자 검색 필드, 유효한 항목, 51
사용자 계정, 124
사용자 그룹
액세스 제어, 138-145
인증, 138, 145, 146, 154-155
사용자/그룹, 액세스 제어 옵션, 154-155
사용자 및 그룹
관리, 43-69
인증, 154-155
사용자 및 그룹 인증, 캐시된 결과, 146
사용자 이름 및 비밀번호 인증, 139
사용자 이름 및 비밀번호 파일, 311
사용자 정의
NSAPI 플러그인, 21
검색 쿼리, LDAP, 51-52, 61, 67
로그 파일 형식, 39-40
인증 방법, 155
표현식, 액세스 제어, 157-158
사용자 정의 표현식, 액세스 제어, 157-158
사용자 캐시
ACL, 146
조정, 358
사용자 항목
디렉토리 서버, 48
변경, 53-54
삭제, 55
새로 만들기, LDAP, 47-49
새로 만들기, 다이제스트 파일, 50
새로 만들기, 키 파일, 49
속성, 48-49
이름 변경 시 이전 값 제거, 55
참고 정보, 48-49
찾기, 51
필수 정보, 48
사용자 항목 만들기
LDAP 기반, 47, 49
다이제스트 파일, 50
키 파일, 49

삭
삭제
SOCKS 항목, 315-316, 318, 322
사용자, 55
청취 소켓, 36, 126-129
삭제 권한, 157

상
상위 배열, 125, 281
라우팅, 280
정보 보기, 281
상태, 서버 요청 통계, 195

새
새 기능, Proxy Server, 21
새 사용자 항목, 필수 정보, 48
새로 고침 간격, 239
새로운 기능, Proxy Server, 25-26

서
서버
SNMP를 통해 실시간으로 상태 확인, 191
개별 관리, 27-28
로그(로그 분석기를 실행하기 전에 보관), 181
모니터링할 통계 유형, 192
모두 관리, 26-27
체인, 218, 319
클러스터에 추가, 113
클러스터에서 제거, 114
서버, 구성, 28-29
서버, 미러, 228
서버 구성, 공유, 111
서버 구성 공유, 111
서버 설정
공유, 111
마이그레이션, 34
보기, 122
액세스 제한, 156-157

서버 성능 향상
Proxy Server, 357-368
SOCKS 서버, 311-312
서버 액세스 제한, 40-41, 137-165
디렉토리, 160
보안 기준, 162
전체 서버, 159
파일 유형, 160-161
서버 인스턴스
관리, 26-29
마이그레이션, 34
시작 및 중지, 27
액세스 보안, 162
액세스 제어 규칙, 149, 151-153
여러, 33
제거, 33-34
추가, 33
서버 인스턴스에 대한 액세스 보안, 162
서버 인증, 정보, 72
서버 체인
SOCKS 서버, 319
프록시 서버, 218
서버 클러스터, 111
서버에서 시작된 통신, 213
서버의 부분, 액세스 제한, 156-157

설

설정
관리 기본 설정, 35-41
보안 기본 설정, 84-92
액세스 권한, 157
액세스 제어, 149-153, 153-158
역방향 프록시에서의 클라이언트 인증, 99-100
클라이언트 보안 요구 사항, 97-105
설치
Digest 인증 플러그인, 143-145
여러 Proxy Server, 33

성

성능
DNS 조회, 363
성능 *(계속)*
Proxy Server, 357-368
SOCKS 서버, 311-312, 313
Tuning, Sizing, and Scaling Guide, 364
동적 그룹의 영향, 58
및 DNS 조회, 145
성능 버킷, 199
구성, 200
예, 200

소

소유자, 관리, 64

속

속성
LDAP, 48-49
x509v3 인증서, 103
검색 옵션, 51
속성 표현식
액세스 제어 사용, 354
연산자, 355
속성 표현식용 연산자, 355

수

수퍼유저
Administration Server 액세스, 37-38
Sun Java System Directory Server, 37
분산 관리, 38
비밀번호 확인, 37
사용자 이름 및 비밀번호, 37
설정, 37-38

스

스레드
Proxy Server 성능, 363-364
SOCKS 서버 성능, 311-312

스레드 수, 성능
  Proxy Server, 363-364
  SOCKS 서버, 311-312

시
시간 초과, 액세스 제어, 158, 161
시간 초과, 연결, 359
시간 초과 값, 성능 영향, 360-362
시간 초과 매개 변수, 360
시스템 요구 사항, 21
시작
  Administration Server, 31-32
  Proxy Server 인스턴스, 27
  SOCKS 서버, 312
시작 호스트, 액세스 제어 옵션, 155-156
시작하기, 26-29

실
실행 권한, 157

쓰
쓰기 권한, 157

아
아웃바운드 연결 풀, 364
아카이브, 로그 파일, 170

알
알려진 문제점, 추가 정보, 21

암
암호
  Netscape Navigator 6.0의 경우 TLS 및 SSL 3.0, 91
암호 *(계속)*
  정보, 84
암호 해독, 정보, 84
암호화
  양방향, 84
  옵션 설정, 106
  정보, 84
암호화 모듈, 외부, 92-97

액
액세스
  Administration Server, 26-27
  Server Manager, 27-28
  목록 권한, 157
  삭제 권한, 157
  수퍼유저, 37-38
  실행 권한, 157
  쓰기 권한, 157
  읽기 권한, 157
  정보 권한, 157
  제한, 40-41, 137-165
  제한, 디렉토리, 160
  제한, 보안 기준, 162
  제한, 전체 서버, 159
  제한, 파일 유형, 160-161
  클라이언트 인증서로 제어, 146-147
액세스 권한, 157
액세스 로그, 171
  위치, 167
액세스 로그 파일, 구성, 171
액세스 로그 파일, 보기, 39
액세스 로깅, 성능 영향, 358
액세스 제어
  API, 145, 155
  IP 기반, 163
  LDAP 디렉토리 및, 155
  server.xml, 146
  관리, 132
  규칙, 기본, 153
  규칙, 서버 인스턴스, 149-153
  규칙, 전역, 149-153
  기본 규칙, 153
  날짜 제한, 158, 161

액세스 제어 *(계속)*
데이터베이스 및, 155
및 server.xml, 356
방법, 139
사용 안 함 및 사용, 158
사용자 그룹, 138-145, 154-155
사용자 정의 표현식, 157-158
설정, 149-153, 153-158
시간 초과, 158, 161
정보, 137-147
클라이언트 인증서, 146-147
파일, 구문, 351-356
파일, 기본값, 355
파일, 예, 147
파일, 위치, 145
파일, 이름, 146
프로그램, 156-157
필수 요건, 137
항목(ACE), 137
호스트-IP, 145, 155-156
액세스 제한, 149-153
perfdump 출력, 199
stats-xml 출력, 193
목록(ACL), 40-41
브라우저, 287
항목(ACE), 40-41
액세스가 거부된 경우의 응답, 158

양
양방향 암호화, 암호, 84

에
에이전트, SNMP, 41

여
여러
Proxy Server, 33
관리자, 38-39
여러 Proxy Server 실행, 33

역
역방향 DNS 조회, SOCKS 서버, 313
역방향 프록시, 컨텐트 제작, 302
역방향 프록시, 클라이언트 인증, 98, 99-100

연
연결 모드, 224-225
연결 시간 초과, 359
연결 유지 통계, 195
연결 풀
아웃바운드, 364
인바운드, 364
연결 항목, SOCKS, 316-319

오
오류 로그, 180
오류 로그 수준, 성능 영향, 359
오류 로그 파일, 위치, 167
오류 로그 파일, 보기, 40

온
온라인 도움말, 27

와
와일드 카드, 및 SOCKS 서버, 313
와일드카드
및 ACL, 352
및 액세스 제어, 154
액세스 제어, 155-156
와일드카드 패턴, 327

외
외부
암호화 모듈, 92-97
하드웨어 가속기, 93, 95

외부 인증서, 서버 시작, 95
외부 인증서를 사용하여 서버 시작, 95

요
요청 차단, 288

원
원격 서버, 클러스터에 추가, 113

웹
웹 서버, 프록시 실행, 331

위
위치 다시 작성, 230

유
유형
  ACL, 351
  검색 옵션, 52
  디렉토리 서비스, 44-45

이
이름 변경, 이전 값 제거, 55
이벤트 뷰어, 190
이전 값, 사용자 이름 변경 시 제거, 55

인
인바운드 연결 풀, 364
인스턴스
  관리, 27-28
  시작 및 중지, 27-28
인증
  Basic, 44, 139, 155
  Default, 139
  Digest, 141-142
  SOCKS 서버, 315
  데이터베이스, 155, 163-165
  문, ACL 구문, 352
  방법, 액세스 제어, 154
  사용자 그룹, 154-155
  클라이언트, 서버, 72
  클라이언트, 요구, 97-98
  항목, SOCKS, 314-316
  호스트-IP, 145
인증 API, 104
인증 기관
  VeriSign, 76
  승인 프로세스, 79
  정보, 72
인증문, ACL, 352
인증서
  pk12util을 사용하여 가져오기, 94-95
  pk12util을 사용하여 내보내기, 93
  Proxy Server 3.6에서 마이그레이션, 81
  기타 요청, 78-79
  루트 인증서 제거 및 복원, 82
  소개, 72
  속성, 103
  유형, 79
  클라이언트, 97-98
인증서 API, 104
인증서 매핑 파일(certmap.conf)
  구문, 102
  위치, 102
  정보, 102-105
인증서 및 키 내보내기, 93
인증서 요청, 필요한 정보, 77
인증서 체인, 79
인증서 해지 목록(CRL), 83

일
일괄 업데이트, 성능 영향, 365
일반 로그 파일 형식, 39-40
일반 모드, 224

일반 텍스트
  비밀번호 및 Digest 인증, 165
  사용자 이름 및 비밀번호, 141, 155

읽
읽기 권한, 157

잊
잊어 버린 수퍼유저 비밀번호, 37

자
자동 구성 파일, 331
  만들기, 334-336
  반환 값, 337
자동 구성 파일, PAT 파일에서 생성
  수동, 278-279
  자동, 279
자원, 325
자원, 식별, 29
자원 ACL, 351
자원 식별, 29

작
작업자 및 승인 스레드, SOCKS 서버, 311, 313

전
전역
  보안 매개 변수, 91
  액세스 제어 규칙, 149
전체 서버, 액세스 제한, 159

정
정규 표현식, 29, 326
정규 표현식 *(**계속**)*
  의미, 326
정보
  certmap.conf, 102-105
  dbswitch.conf, 44
  DN(고유 이름), 46
  Proxy Server, 25-29
  SOCKS, 309
  SOCKS 서버, 309
  socks5.conf, 311-312
  SSL, 85
  TLS, 85
  공용 및 개인 키, 85
  구성 파일, 28-29
  그룹, 55
  동적 그룹, 57-59
  디렉토리 서비스, 44-45
  서버 관리, 26-29
  서버 구성, 28-29
  서버 액세스 제한, 40-41
  서버 인증, 72
  암호, 84
  암호 해독, 84
  암호화, 84
  액세스 제어, 137-165
  인증 기관(CA), 72
  정적 그룹, 56-57
  청취 소켓, 35-36
  클라이언트 인증, 72
  클러스터, 111
  키 쌍 파일, 73
  프록시 배열, 268-281
정보 권한, 157
정적 그룹
  만들기, 57
  정보, 56-57

제
제거
  사용자, 55
  사용자 이름 변경 시 이전 값, 55
  서버 인스턴스, 33-34
  클러스터에서 서버, 114

제어
서버 액세스, 137-165
수퍼유저 액세스, 37-38

조
조정
ACL 사용자 캐시, 358
Proxy Server, 357-368
SOCKS 서버, 311-312, 313
Solaris 매개 변수, 367-368
가비지 컬렉션, 366-367
조직 단위
관리, 66-69
만들기, 66
정보, 46, 66

종
종료 시간 초과, magnus.conf, 142

중
중지
Administration Server, 32-33, 119-120
Proxy Server 인스턴스, 27
SOCKS 서버, 312

지
지원되는 플랫폼, 21
지침
LDAP 기반 사용자 항목 만들기, 47-48
고급 비밀번호 만들기, 108
동적 그룹 만들기, 58-59
서버 클러스터 사용, 112
정적 그룹 만들기, 56

찾
찾기
그룹, 60-62
사용자 항목, 51

청
청취 대기열 크기, 124
청취 소켓
ls1, 35
삭제, 36, 126-129
외부 인증서 연결, 95-96
정보, 35-36
추가, 36, 126-129
클라이언트 인증 요구, 97-98
편집, 36, 126-129

체
체인
SOCKS 서버, 319
프록시 서버, 218

최
최신 여부 확인, 362

추
추가
Proxy Server, 33
구성원을 그룹에, 62-63
그룹을 그룹 구성원 목록에, 63
청취 소켓, 36, 126-129
클러스터에 서버, 113
추가 참조, 관리, 64

캐

캐시
  가비지 컬렉터, 244
  디렉토리
    구조, 254-255
  만료 정책, 239, 240
  명령줄 유틸리티, 254-255
  명령줄 인터페이스, 254-260
  사양, 236
  새로 고침 간격, 239
  새로 고침 설정, 239
  섹션, 234
  섹션 추가, 수정, 243
  예, 235
  일괄 업데이트, 251
  쿼리, 246
  크기, 238
  크기 변경, 238
  파일 분산, 235
  파티션, 234
  하위 구역, 235
캐시 아키텍처, 성능 영향, 365
캐시 일괄 업데이트, 성능 영향, 365
캐시 조정, 358
캐시 파일, 분산, 235
캐시 파일의 분산, 235
캐시 프로세스, 234
캐시된 URL, 250
캐시된 결과, 사용자 및 그룹 인증, 146
캐시된 문서, 수명, 362
캐시된 파일 만료, 250-251
캐시된 파일 제거, 250-251

커

커뮤니티 문자열, SNMP 에이전트가 인증에
  사용하는 텍스트 문자열, 211

컨

컨텐트 압축, 292
컨텐트 위치 다시 작성, 230
컨텐트 제작, 호스트 이름, 302

쿠

쿠키 및 CGI 프로그램, 35

쿼

쿼리, 캐시, 246

클

클라이언트, 액세스 목록, 171
클라이언트 IP 주소, 219-223
클라이언트 및 프록시 라우팅, 268
클라이언트 보안 요구 사항, 설정, 97-105
클라이언트 인증
  시나리오, 98
  역방향 프록시, 98, 99-100
  요구, 97-98, 140
  정보, 72
클라이언트 인증 요구, 97-98, 140
클라이언트 인증서, 97
  API, 104
  LDAP 항목으로 매핑, 100-101
  액세스 제어, 146-147
클라이언트 자동 구성, 224
클라이언트에서 프록시로의 라우팅, 268
클러스터
  관리, 115
  서버 수정, 114
  서버 제거, 114
  서버 추가, 113
  정보, 111
  지침, 112

키

키
  pk12util을 사용하여 가져오기, 94-95
  pk12util을 사용하여 내보내기, 93
  정보, 85
키 데이터베이스 비밀번호, 74
키 쌍 파일
  보안, 109

키 쌍 파일 *(계속)*
비밀번호 변경, 108
정보, 73
키 크기 제한, PathCheck, 106
키 파일 디렉토리 서비스
사용자 찾기, 51-53
사용자 항목, 49
정보, 44

터
터널링, SSL, 86-87, 87-88, 88

템
템플리트, 325

통
통계
DNS 통계, 195
사용 설정, 193
서버 모니터링에 사용할 수 있는 유형, 192
연결 상태, 195
표시, 195-196

트
트랩, SNMP, 211
트러스트 데이터베이스
만들기, 73
비밀번호, 108
자동 만들기, 외부 PKCS#11 모듈, 96

파
파일, 캐시의 분산, 235
파일 구문, ACL, 351-356
파일 유형, 액세스 제한, 160-161
파일 캐시, 110

페
페이지, 액세스 제한, 156-157

편
편집
SOCKS 항목, 315, 318, 322
그룹 항목, 62
디렉토리 서비스, 46
사용자 항목, 53-54
청취 소켓, 36, 126-129

포
포트, 보안, 위험, 88

폴
폴링 라운드, 261

표
표현식
사용자 정의, ACL, 157-158
속성, 354
정규, 29

프
프로그램, 액세스, 156-157
프로토콜 데이터 단위(PDU), 212
프록시 SNMP 에이전트, 204
프록시 라우팅 항목, SOCKS, 319-323
프록시 배열, 124
PAC 파일 생성
수동, 278-279
자동, 279
구성원 목록 만들기, 272-274
라우팅 활성화, 276-277
상위 배열, 281

프록시 배열 *(계속)*
활성화, 277-278
프록시 배열 테이블, 229
프록시 서버
웹 서버, 331
체인, 218
프록시 서버 그룹, 관리, 111
프록시 서버 다시 시작
inittab 사용, 121
시스템 RC 스크립트 사용, 121
프록시 서버 시작
UNIX 또는 Linux, 118
Windows, 118
프록시 서버 중지
UNIX 또는 Linux, 119-120
Windows, 120
프록시 시간 초과, 125
프록시 시간 초과 매개 변수, 360
프록시에서 프록시로의 라우팅, 268, 269

플
플랫폼, 지원됨, 21

필
필수 매개 변수, LDAP URL, 58
필수 정보
사용자 항목, 48
인증서 요청, 77

하
하드웨어 가속기, 93
하위 에이전트, 41
SNMP, 202

항
항목
LDAP, 46, 47-48, 48-49
항목 *(계속)*
SOCKS, 314-316, 316-318, 319-323

해
해결 방법, 추가 정보, 21

헤
헤더 이름 다시 작성, 230

호
호스트-IP, 액세스 제어, 145, 155-156
호스트 다시 작성, 230

활
활성화
FIPS-140, 96-97
ICP, 266-267
SOCKS 서버, 312
Sun Crypto Accelerator, 75-76