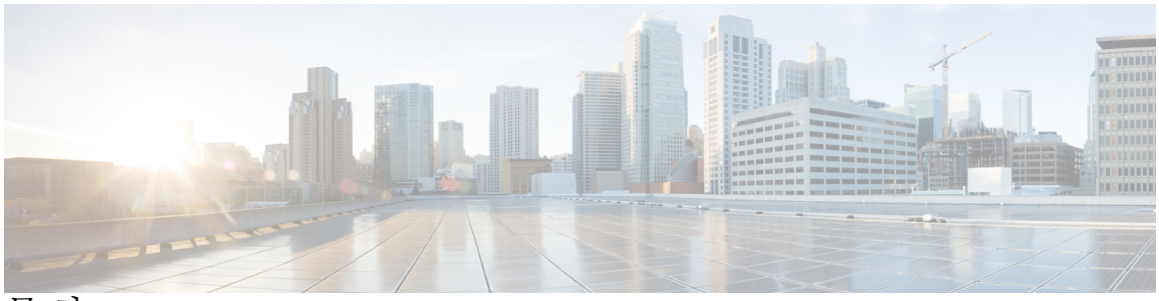
Cisco Unified Communications Manager 관리 설명서, 릴리스 12.5(1)SU3

초판: 2020년 8월 13일

최종 변경: 2024년 2월 13일

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883



목 차

부 I: 관리 개요 25

장 1 관리 개요 1

- Cisco Unified CM 관리 개요 1
- 운영 체제 관리 개요 2
  - 인증 네트워크 시간 프로토콜 지원 4
  - 자동 키 인증 네트워크 시간 프로토콜 지원 4
- Cisco 통합 서비스 가용성 개요 5
- Cisco Unified Reporting 개요 6
- 재해 복구 시스템 개요 6
- 벌크 관리 도구 개요 7

장 2 시작하기 9

- 관리 인터페이스에 로그인 9
- 관리자 또는 보안 암호 재설정 9
- 시스템 종료 또는 다시 시작 11

부 II: 사용자 관리 13

장 3 사용자 액세스 관리 15

- 사용자 액세스 개요 15
  - 액세스 제어 그룹 개요 15
  - 역할 개요 16
  - 사용자 순위 개요 19

사용자 액세스 필수 구성 요소 20
사용자 액세스 구성 작업 흐름 20
사용자 순위 계층 구조 구성 21
사용자 지정 역할 만들기 21
관리자를 위한 고급 역할 구성 22
액세스 제어 그룹 만들기 23
액세스 제어 그룹에 사용자 할당 23
액세스 제어 그룹에 대한 권한 정책 중복 구성 24
사용자 권한 보고서 보기 25
사용자 지정 지원 센터 역할 작업 흐름 만들기 25
사용자 지정 지원 센터 역할 만들기 26
사용자 지정 지원 센터 액세스 제어 그룹 만들기 26
액세스 제어 그룹에 지원 센터 역할 할당 27
액세스 제어 그룹에 지원 센터 구성원 할당 27
액세스 제어 그룹 삭제 28
기존 OAuth 새로 고침 토큰 해지 29
비활성 사용자 계정 비활성화 29
원격 계정 설정 30
표준 역할 및 액세스 제어 그룹 30

장 4

최종 사용자 관리 41
최종 사용자 개요 41
최종 사용자 관리 작업 41
사용자 템플릿 구성 42
범용 회선 템플릿 구성 43
범용 장치 템플릿 구성 44
사용자 프로파일 구성 44
기능 그룹 템플릿 구성 46
LDAP에서 최종 사용자 가져오기 47
최종 사용자를 수동으로 추가 47
최종 사용자를 위한 새 전화기 추가 49

최종 사용자에게 기존 전화기 이동 49
최종 사용자 PIN 변경 50
최종 사용자 암호 변경 50
Cisco Unity Connection 음성 사서함 생성 51

장 5 애플리케이션 사용자 관리 53
애플리케이션 사용자 개요 53
애플리케이션 사용자 작업 흐름 54
새 애플리케이션 사용자 추가 54
애플리케이션 사용자와 장치 연결 55
Cisco Unity 또는 Cisco Unity Connection에 관리자 사용자 추가 55
애플리케이션 사용자 암호 변경 56
애플리케이션 사용자 암호 인증서 정보 관리 57

부 III: 디바이스 관리 59

장 6 전화기 관리 61
전화기 관리 개요 61
전화기 버튼 템플릿 61
전화기 관리 작업 62
전화기를 수동으로 추가 63
최종 사용자를 추가하거나 추가하지 않고 사용자 템플릿에서 새 전화기 추가 64
최종 사용자를 추가하여 사용자 템플릿에서 새 전화기 추가 65
협업 모바일 통합 가상 장치 개요 66
협업 모바일 통합 가상 장치 추가 66
CMC RD 기능 상호 작용 67
CMC RD 기능 제한 72
기존 전화기 이동 72
적극적으로 로그인한 장치 찾기 72
원격으로 로그인된 장치 찾기 73
원격으로 전화기 잠금 74

전화기를 초기 기본값으로 재설정 75
전화기 잠금/삭제 보고서 75
전화기의 LSC 상태 보기 및 CAPF 보고서 생성 76

장 7 장치 펌웨어 관리 79
장치 펌웨어 업데이트 개요 79
장치 팩 또는 개별 펌웨어 설치 80
펌웨어 설치 시 발생할 수 있는 문제 81
시스템에서 사용하지 않는 펌웨어 제거 81
전화기 모델에 대한 기본 펌웨어 설정 82
전화기에 대한 펌웨어 로드 설정 83
로드 서버 사용 83
기본값 이외의 펌웨어 로드가 사용되는 장치 찾기 84

장 8 인프라 장치 관리 87
인프라 관리 개요 87
인프라 필수 구성 요소 관리 87
인프라 작업 흐름 관리 88
인프라 장치에 대한 상태 보기 88
인프라 디바이스에 대한 추적 비활성화 89
비활성화된 인프라 장치에 대한 추적 활성화 89

부 IV: 시스템 관리 91

장 9 시스템 상태 모니터링 93
클러스터 노드 상태 보기 93
하드웨어 상태 보기 93
네트워크 상태 보기 94
설치된 소프트웨어 보기 94
시스템 상태 보기 95
IP 환경 설정 보기 95

마지막 로그인 세부 정보 보기 95
노드 Ping 96
서비스 매개 변수 표시 96
네트워크 DNS 구성 98

장 10 알람 99
개요 99
알람 구성 100
알람 정의 101
알람 정보 102
알람 설정 102
알람 서비스 설정 103
Syslog 에이전트 엔터프라이즈 매개 변수 103
알람 서비스 설정 104
Cisco Tomcat을 사용하는 알람 서비스 설정 105
서비스 그룹 106
알람 구성 설정 107
알람 정의 및 사용자 정의 설명 추가 110
알람 정의 보기 및 사용자 정의 설명 추가 110
시스템 알람 카탈로그 설명 111
CallManager 알람 카탈로그 설명 112
IM and Presence 알람 카탈로그 설명 113
CiscoSyslog 파일의 기본 알람 114

장 11 감사 로그 117
감사 로그 117
감사 로깅 (표준) 117
감사 로깅(자세히) 122
Audit Log Types 122
시스템 감사 로그 122
애플리케이션 감사 로그 122

데이터베이스 감사 로그 122
감사 로그 구성 작업 흐름 122
감사 로그 설정 123
원격 감사 로그 전송 프로토콜 구성 124
경고 알림을 위한 전자 메일 서버 구성 124
이메일 알림 활성화 125
플랫폼 로그에 대해 원격 감사 로깅 구성 125
감사 로그 구성 설정 127

장 12 통화 홈 133
통화 홈 133
통화 홈 133
Smart Call Home 133
익명 통화 홈 136
Smart Call Home 상호 작용 138
통화 홈에 대한 전제 조건 139
통화 홈 액세스 139
통화 홈 설정 140
통화 홈 구성 140
제한 사항 143
통화 홈에 대한 참조 144

장 13 서비스 가용성 커넥터 145
서비스 가용성 커넥터 개요 145
서비스 가용성 서비스 사용의 이점 146
다른 하이브리드 서비스와의 차이 146
작동 방식에 대한 간단한 설명 146
TAC 사례에 대한 구축 아키텍처 147
서비스 가용성 커넥터에 대한 TAC 지원 149

장 14 단순 네트워크 관리 프로토콜 151
SNMP(Simple Network Management Protocol) 지원 151

SNMP 기본 사항 151
SNMP Management Information Base 152
SNMP 구성 요구 사항 167
SNMP 버전 1 지원 167
SNMP 버전 2c 지원 167
SNMP 버전 3 지원 168
SNMP 서비스 168
SNMP 커뮤니티 문자열 및 사용자 169
SNMP 트랩 및 알림 169
SFTP 서버 지원 172
SNMP 구성 작업 흐름 172
SNMP 서비스 활성화 173
SNMP 커뮤니티 문자열 구성 174
커뮤니티 문자열 구성 설정 175
SNMP 사용자 구성 176
SNMP V3 사용자 구성 설정 178
원격 SNMP 엔진 ID 가져오기 180
SNMP 알림 대상 구성 180
SNMP V1 및 V2c에 대한 알림 대상 설정 182
SNMP V3에 대한 알림 대상 설정 183
MIB2 시스템 그룹 구성 185
MIB2 시스템 그룹 설정 185
CISCO-SYSLOG-MIB 트랩 매개 변수 186
CISCO-CCM-MIB 트랩 매개 변수 187
CISCO-UNITY-MIB 트랩 매개 변수 187
SNMP 마스터 에이전트 다시 시작 187
SNMP 트랩 설정 188
SNMP 트랩 구성 188
SNMP 트랩 생성 188
SNMP 추적 구성 192
SNMP 문제 해결 192

장 15 서비스 193
기능 서비스 193
데이터베이스 및 관리 서비스 194
위치 대역폭 관리자 194
Cisco AXL 웹 서비스 195
Cisco UXL 웹 서비스 195
Cisco Bulk Provisioning Service 195
Cisco TAPS 서비스 195
플랫폼 관리 웹 서비스 196
Performance and monitoring services 196
Cisco 서비스 가용성 리포터 196
Cisco CallManager SNMP Service 196
CM 서비스 196
Cisco CallManager 196
Cisco TFTP 197
Cisco Messaging Interface 197
Cisco Unified Mobile Voice Access Service 198
Cisco IP Voice Media Streaming App 198
Cisco CTIManager 198
Cisco Extension Mobility 198
Cisco Dialed Number Analyzer 198
Cisco Dialed Number Analyzer 서버 199
Cisco DHCP 모니터 서비스 199
Cisco 클러스터 간 조회 서비스 199
Cisco UserSync 서비스 199
Cisco UserLookup 웹 서비스 199
Cisco 헤드셋 서비스 200
IM and Presence Service 200
Cisco SIP Proxy 200
Cisco Presence 엔진 200
Cisco XCP 텍스트 전화회의 관리자 200

Cisco XCP Web 연결 관리자 200
Cisco XCP 연결 관리자 200
Cisco XCP SIP 페더레이션 연결 관리자 201
Cisco XCP XMPP 페더레이션 연결 관리자 201
Cisco XCP 메시지 아카이버 201
Cisco XCP 디렉터리 서비스 201
Cisco XCP 인증 서비스 201
CTI 서비스 201
Cisco IP Manager Assistant 201
Cisco WebDialer 웹 서비스 202
셀프 프로비저닝 IVR 202
CDR 서비스 202
CAR 웹 서비스 202
Cisco SOAP - CDROnDemand Service 203
보안 서비스 203
Cisco CTL Provider 203
Cisco Certificate Authority Proxy Function(CAPF) 203
디렉터리 서비스 204
Cisco DirSync 204
위치 기반 추적 서비스 204
Cisco Wireless Controller 동기화 서비스 204
음성 품질 리포터 서비스 205
Cisco Extended Functions 205
네트워크 서비스 205
성능 및 모니터링 서비스 205
백업 및 복원 서비스 206
시스템 서비스 207
플랫폼 서비스 207
보안 서비스 210
데이터베이스 서비스 210
SOAP 서비스 211
CM 서비스 211

IM and Presence Service 서비스 212
CDR 서비스 215
관리 서비스 216
Services setup 217
제어 센터 217
서비스 설정 217
서비스 활성화 218
Cisco Unified Communications Manager에 대한 클러스터 서비스 활성화 권장 사항 218
IM and Presence Service에 대한 클러스터 서비스 활성화 권장 사항 222
기능 서비스 활성화 226
제어 센터 또는 CLI에서 서비스 시작, 중지 및 재시작 227
제어 센터에서 서비스 시작, 중지 및 재시작 227
명령줄 인터페이스를 사용하여 서비스 시작, 중지 및 재시작 228

장 16
추적 229
추적 229
추적 구성 230
추적 설정 230
추적 수집 231
착신자 추적 231
추적 구성 설정 232
추적 구성 233
추적 매개 변수 설정 233
추적 구성의 서비스 그룹 235
디버그 추적 수준 설정 240
추적 필드 설명 241
Database Layer Monitor 추적 필드 242
Cisco RIS Data Collector 추적 필드 242
Cisco CallManager SDI 추적 필드 243
Cisco CallManager SDL 추적 필드 245
Cisco CTIManager SDL 추적 필드 247

Cisco Extended Functions 추적 필드 248
Cisco Extension Mobility 추적 필드 249
Cisco IP Manager Assistant 추적 필드 249
Cisco IP Voice Media Streaming App 추적 필드 250
Cisco TFTP 추적 필드 251
Cisco Web Dialer 웹 서비스 추적 필드 251
IM and Presence SIP 프록시 서비스 추적 필터 설정 252
IM and Presence 추적 필드 설명 253
Cisco Access 로그 추적 필드 253
Cisco Authentication 추적 필드 253
Cisco 달력 추적 필드 253
Cisco CTI 게이트웨이 추적 필드 253
Cisco Database Layer Monitor 추적 필드 254
Cisco Enum 추적 필드 254
Cisco 메서드/이벤트 추적 필드 254
Cisco 번호 확장 추적 필드 254
Cisco 파서 추적 필드 255
Cisco 프라이버시 추적 필드 255
Cisco 프록시 추적 필드 255
Cisco RIS Data Collector 추적 필드 255
Cisco 레지스트리 추적 필드 256
Cisco 라우팅 추적 필드 256
Cisco 서버 추적 필드 256
Cisco SIP 메시지 및 상태 시스템 추적 필드 257
Cisco SIP TCP 추적 필드 257
Cisco SIP TLS 추적 필드 257
Cisco 웹 서비스 추적 필드 257
추적 출력 설정 258
추적 설정 문제 해결 258
추적 설정 문제 해결 창 258
추적 설정 문제 해결 259

장 17 사용 레코드 보기 261
사용 레코드 개요 261
종속성 레코드 261
경로 플랜 보고서 261
사용 보고서 작업 262
경로 플랜 보고서 작업 흐름 262
경로 플랜 레코드 보기 263
경로 플랜 보고서 저장 263
할당되지 않은 디렉토리 번호 삭제 264
할당되지 않은 디렉터리 번호 업데이트 264
종속성 레코드 작업 흐름 265
종속성 레코드 구성 265
종속성 레코드 보기 266

장 18 엔터프라이즈 매개 변수 관리 267
엔터프라이즈 매개변수 개요 267
엔터프라이즈 매개 변수 정보 보기 267
엔터프라이즈 매개 변수 업데이트 268
장치에 구성 적용 268
기본 엔터프라이즈 매개 변수 복원 269

장 19 서버 관리 271
서버 관리 개요 271
서버 삭제 271
클러스터에서 통합 커뮤니케이션 관리자 노드 삭제 273
클러스터에서 IM and Presence 노드 삭제 273
삭제된 서버를 클러스터에 다시 추가 274
설치 전 클러스터에 노드 추가 274
Presence 서버 상태 보기 275
포트 구성 276

포트 설정 276
호스트 이름 구성 277
kerneldump 유틸리티 279
Kerneldump 유틸리티 활성화 280
핵심 덤프에 대한 이메일 경고 활성화 280

부 V: 보고서 관리 283

장 20 Cisco 서비스 가용성 리포터 285
서비스 가용성 보고서 아카이브 285
Cisco 서비스 가용성 리포터 구성 작업 흐름 286
Cisco 서비스 가용성 리포터 활성화 286
Cisco 서비스 가용성 리포터 설정 구성 287
일별 보고서 아카이브 보기 287
일별 보고서 요약 288
장치 통계 보고서 288
서버 통계 보고서 291
서비스 통계 보고서 293
통화 활동 보고서 296
알림 요약 보고서 300
성능 보호 보고서 302

장 21 Cisco Unified Reporting 305
통합 데이터 보고 305
보고서 생성에 사용되는 데이터 소스 306
지원되는 출력 형식 306
시스템 요구 사항 306
필요한 액세스 권한 307
UI 구성 요소 307
관리 인터페이스에서 로그인 308
지원되는 보고서 309

Unified Communications Manager 보고서 309
IM and Presence Service 보고서 311
보고서 설명 보기 312
새 보고서 생성 313
저장된 보고서 보기 314
새 보고서 다운로드 314
저장된 보고서 다운로드 315
보고서 업로드 316

장 22 **Cisco IP** 전화기에 대한 통화 진단 및 품질 보고 구성 317
진단 및 보고 개요 317
통화 진단 개요 317
품질 보고서 도구 개요 318
세부 통화 보고 및 청구 318
Prerequisites 318
통화 진단 필수 조건 318
품질 보고서 도구 필수 조건 319
진단 및 보고 구성 작업 흐름 320
통화 진단 구성 320
품질 보고서 도구 구성 321
QRT 소프트키를 사용하여 소프트키 템플릿 구성 322
QRT 소프트키 템플릿을 일반 장치 구성에 연결 323
전화기에 QRT 소프트키 템플릿 추가 325
Cisco 통합 서비스 가용성에서 QRT 구성 325
품질 보고서 도구에 대한 서비스 매개 변수 구성 328

부 VI: 보안 관리 331

장 23 **SAML Single Sign-On** 관리 333
SAML Single Sign-On 개요 333
iOS에서 Cisco Jabber용 인증서 기반 SSO 인증을 위한 옵트인 제어 333

SAML Single Sign-On 필수 구성 요소 334
SAML Single Sign-On 관리 335
SAML Single Sign-On 활성화 335
iOS에 Cisco Jabber용 SSO 로그인 동작 구성 336
업그레이드한 후 WebDialer에서 SAML Single Sign-on 활성화 336
Cisco WebDialer 서비스 비활성화 337
SAML Single Sign-On 비활성화 337
Cisco WebDialer 서비스 활성화 338
복구 URL에 액세스 338
도메인 또는 호스트 이름 변경 후 서버 메타데이터 업데이트 339
서버를 삭제한 후 서버 메타데이터 업데이트 339
서버 메타데이터 수동 프로비저닝 340

장 24 인증서 관리 343
인증서 개요 343
타사 서명 인증서 또는 인증서 체인 344
타사 인증 기관 인증서 345
인증서 서명 요청 키 사용 확장 346
인증서 표시 347
인증서 다운로드 347
중간 인증서 설치 348
신뢰 인증서 삭제 348
인증서 다시 생성 349
인증서 이름 및 설명 350
OAuth 새로 고침 로그인을 위해 키 다시 생성 351
인증서 또는 인증서 체인 업로드 352
타사 CA(인증기관) 인증서 관리 352
인증서 서명 요청 생성 353
CSR(Certificate Signing Request) 다운로드 354
인증기관 서명 CAPF 루트 인증서를 신뢰 저장소에 추가 354
서비스 다시 시작 355

온라인 인증서 상태 프로토콜을 통한 인증서 해지 355
인증서 모니터링 작업 흐름 356
인증서 모니터 알림 구성 357
OCSP를 통해 인증서 해지 구성 358
인증서 오류 문제 해결 359

장 25 벌크 인증서 관리 361
벌크 인증서 관리 361
인증서 내보내기 361
인증서 가져오기 362

장 26 IPSec 정책 관리 365
IPsec 정책 개요 365
IPsec 정책 구성 365
IPsec 정책 관리 366

장 27 인증 정책 관리 367
인증 정책 및 인증 367
인증 정책에 대한 JTAPI 및 TAPI 지원 368
인증서 정책 구성 368
인증 정책 기본값 구성 369
인증 활동 모니터링 369
인증서 캐시 구성 370
세션 종료 관리 371

부 VII: IP 주소, 호스트 이름 및 도메인 이름 변경 373

장 28 변경 전 작업 및 시스템 상태 검사 375
변경 전 작업 375
IP 주소, 호스트 이름 및 기타 네트워크 식별자 변경 사항 375
IM and Presence Service 노드 이름 및 기본 도메인 이름 변경 사항 376

호스트 이름 구성 376
Procedure workflows 378
Cisco Unified Communications Manager 워크플로우 378
IM and Presence Service 워크플로우 378
Cisco Unified Communications Manager 노드에 대한 변경 전 작업 379
IM and Presence Service 노드에 대한 변경 전 설정 작업 381

장 29
IP 주소 및 호스트 이름 변경 385
IP 주소 및 호스트 이름 작업 목록 변경 385
OS 관리 GUI를 통해 IP 주소 또는 호스트 이름 변경 386
Unified CM Administration GUI를 통해 IP 주소 또는 호스트 이름 변경 387
CLI를 통해 IP 주소 또는 호스트 이름 변경 388
설정된 네트워크 호스트 이름에 대한 CLI 출력 예 389
IP 주소만 변경 390
네트워크 IP 주소 설정에 대한 출력 예 391
CLI를 사용하여 DNS IP 주소 변경 391

장 30
도메인 이름 및 노드 이름 변경 393
도메인 이름 변경 393
IM and Presence Service 기본 도메인 이름 변경 작업 394
DNS 레코드 업데이트 395
FQDN 값의 노드 이름 업데이트 396
DNS 도메인 업데이트 398
클러스터 노드 고려 사항 399
보안 인증서 재생성 400
노드 이름 변경 401
IM and Presence Service 노드 이름 변경 작업 목록 402
노드 이름 업데이트 402
CLI를 사용하여 노드 이름 변경 확인 403
Cisco Unified CM IM and Presence 관리를 사용하여 노드 이름 변경 확인 404
Cisco Unified Communications Manager의 도메인 이름 업데이트 404

장 31 변경 후 작업 및 확인 407
Cisco Unified Communications Manager 노드에 대한 변경 후 작업 407
Cisco Unified Communications Manager 노드에 대한 보안 활성화 클러스터 작업 410
초기 신뢰 목록 및 인증서 재생성 410
단일 서버 클러스터 전화기에 인증서 및 ITL 다시 생성 411
다중 서버 클러스터 전화기에 대한 인증서 및 ITL 재생성 411
IM and Presence Service 노드에 대한 변경 후 작업 411

장 32 주소 변경 문제 해결 415
클러스터 인증 문제 해결 415
데이터베이스 복제 문제 해결 415
데이터베이스 복제 확인 416
데이터베이스 복제 CLI 출력 예 417
데이터베이스 복제 복구 418
데이터베이스 복제 재설정 420
네트워크 문제 해결 420
Network Time Protocol troubleshooting 421
가입자 노드에서 NTP 문제 해결 421
퍼블리셔 노드에서 NTP 문제 해결 421

부 VIII: 재해 복구 423

장 33 시스템 백업 425
백업 개요 425
필수 구성 요소 백업 427
백업 작업 흐름 428
백업 디바이스 구성 428
백업 파일의 크기 계산 429
예약 백업 구성 430
수동 백업 시작 431

현재 백업 상태 보기 432
백업 기록 보기 433
백업 상호 작용 및 제한 사항 433
백업 제한 사항 433
원격 백업용 SFTP 서버 434

장 34 시스템 복원 437
복원 개요 437
마스터 상담원 437
로컬 에이전트 437
필수 구성 요소 복원 438
작업 흐름 복원 439
첫 번째 노드만 복원 439
후속 클러스터 노드 복원 441
게시자를 다시 빌드한 후 한 번에 클러스터 복원 443
전체 클러스터 복원 444
마지막으로 성공한 구성으로 노드 또는 클러스터 복원 445
노드 다시 시작 446
복원 작업 상태 확인 447
복원 기록 보기 447
데이터 인증 448
추적 파일 448
명령줄 인터페이스 448
알람 및 메시지 450
알람 및 메시지 450
라이선스 예약 452
라이선스 예약 452
복원 상호 작용 및 제한 사항 454
복원 제한 사항 454
문제 해결 455
더 작은 가상 시스템으로 DRS 복원 실패 455

부 IX: 문제 해결 457

장 35 문제 해결 개요 459

Cisco 통합 서비스 가용성 459

Cisco Unified Communications 운영 체제 관리 460

문제 해결을 위한 일반 모델 460

네트워크 오류 준비 461

추가 정보 확인 위치 461

장 36 문제 해결 도구 463

Cisco 통합 서비스 가용성 문제 해결 도구 463

명령줄 인터페이스 465

kerneldump 유틸리티 465

Kerneldump 유틸리티 활성화 466

핵심 덤프에 대한 이메일 경고 활성화 467

네트워크 관리 467

시스템 로그 관리 467

Cisco Discovery Protocol 지원 468

SNMP(Simple Network Management Protocol) 지원 468

스니퍼 추적 469

디버그 469

Cisco 보안 텔넷 469

패킷 캡처 470

패킷 캡처 개요 470

패킷 캡처를 위한 구성 검사 목록 471

표준 패킷 스니퍼 액세스 제어 그룹에 최종 사용자 추가 471

패킷 캡처 서비스 매개 변수 구성 472

전화기 구성 창에서 패킷 캡처 구성 472

게이트웨이 및 트렁크 구성 창에서 패킷 캡처 구성 473

패킷 캡처 구성 설정 475

캡처된 패킷 분석 476
일반적인 문제 해결 작업, 도구 및 명령 476
문제 해결 팁 479
시스템 기록 로그 480
시스템 기록 로그 개요 480
시스템 기록 로그 필드 481
시스템 기록 로그 액세스 482
감사 로깅 483
Cisco Unified Communications Manager 서비스가 실행 중인지 확인 488

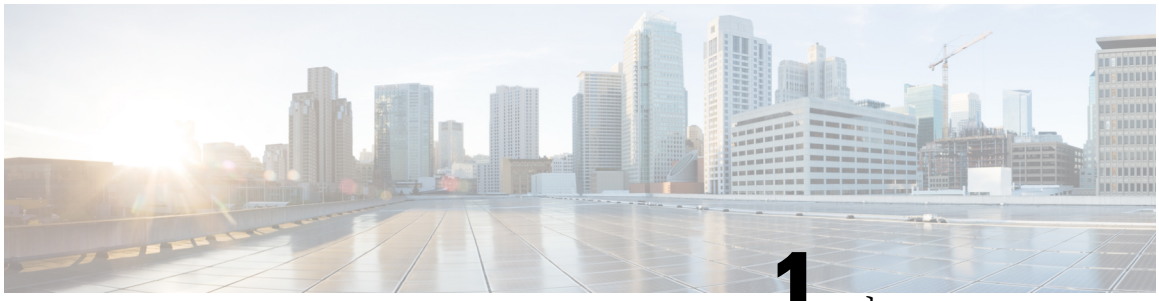
장 37

TAC를 사용하여 케이스 열기 491
필요한 정보 492
필수 예비 정보 492
네트워크 레이아웃 492
문제 설명 493
일반 정보 493
온라인 케이스 494
서비스 가용성 커넥터 494
서비스 가용성 커넥터 개요 494
서비스 가용성 서비스 사용의 이점 495
서비스 가용성 커넥터에 대한 TAC 지원 495
Cisco Live! 495
Remote Access 495
Cisco 보안 텔넷 496
방화벽 보호 496
Cisco 보안 텔넷 설계 496
Cisco 보안 텔넷 구조 497
원격 계정 설정 497

부

관리 개요

- 관리 개요, 1 페이지
- 시작하기, 9 페이지



1 장

관리 개요

- Cisco Unified CM 관리 개요, 1 페이지
- 운영 체제 관리 개요, 2 페이지
- Cisco 통합 서비스 가용성 개요, 5 페이지
- Cisco Unified Reporting 개요, 6 페이지
- 재해 복구 시스템 개요, 6 페이지
- 벌크 관리 도구 개요, 7 페이지

Cisco Unified CM 관리 개요

웹 기반 애플리케이션인 Cisco Unified CM 관리는 Cisco Unified Communications Manager의 기본 관리 및 구성 인터페이스입니다. 일반 시스템 구성 요소, 기능, 서버 설정, 통화 라우팅 규칙, 전화기, 최종 사용자 및 미디어 리소스를 포함하여 시스템에 대한 광범위한 항목을 구성하는 데 Cisco Unified CM 관리를 사용할 수 있습니다.

구성 메뉴

Cisco Unified CM 관리의 [구성] 창은 다음 메뉴로 구성되어 있습니다.

- 시스템—이 메뉴의 구성 창을 사용하여 서버 정보, NTP 설정, 날짜 및 시간 그룹, 지역, DHCP, LDAP 통합 및 엔터프라이즈 매개 변수 등 일반 시스템 설정을 구성합니다.
- 통화 라우팅—이 탭의 구성 창을 사용하여 경로 패턴, 경로 그룹, 헌트 파일럿, 다이얼 규칙, 파티션, 발신 검색 공간, 디렉터리 번호 및 변환 패턴을 포함하여 Cisco Unified Communications Manager가 통화를 전송하는 방식과 관련된 항목을 구성합니다.
- 미디어 리소스—이 탭의 구성 창을 사용하여 미디어 리소스 그룹, 컨퍼런스 브리지, 알림 장치 및 트랜스코더와 같은 항목을 구성합니다.
- 고급 기능—이 탭의 구성 창을 사용하여 음성 메일 파일럿, 메시지 대기 및 통화 제어 에이전트 프로파일 같은 기능을 구성합니다.
- 장치—이 탭의 구성 창을 사용하여 전화기, IP 전화 서비스, 트렁크, 게이트웨이, 소프트키 템플릿 및 SIP 프로파일 등의 장치를 설정합니다.

- 애플리케이션—이 탭의 구성 창을 사용하여 Cisco Unified JTAPI, Cisco Unified TAPI 및 Cisco Unified Real-Time Monitoring Tool 같은 플러그인을 다운로드하고 설치합니다.
- 사용자 관리—사용자 관리 탭의 구성 창을 사용하여 시스템의 최종 사용자와 시스템 애플리케이션 사용자를 구성합니다.
- 벌크 관리—벌크 관리 도구를 사용하여 한 번에 많은 수의 최종 사용자 또는 장치를 가져오고 구성합니다.
- 도움말—이 메뉴를 클릭하여 온라인 도움말 시스템에 액세스합니다. 온라인 도움말 시스템에는 사용자 시스템에서 다양한 구성 창에 대한 설정을 구성하는 데 도움이 되는 설명서가 포함되어 있습니다.

운영 체제 관리 개요

Cisco Unified Communications 운영 체제 관리를 사용하여 운영 체제를 구성 및 관리하고 다음 관리 작업을 수행합니다.

- 소프트웨어 및 하드웨어 상태 확인
- IP 주소 확인 및 업데이트
- 다른 네트워크 장치 Ping
- NTP 서버 관리
- 시스템 소프트웨어 및 옵션 업그레이드
- IPsec 및 인증서를 포함하여 노드 보안 관리
- 원격 지원 계정 관리
- 시스템 다시 시작

운영 체제 상태

다음을 포함한 다양한 운영 체제 구성 요소의 상태를 확인할 수 있습니다.

- 클러스터 및 노드
- 하드웨어
- 네트워크
- 시스템
- 설치된 소프트웨어 및 옵션

운영 체제 설정

다음과 같은 운영 체제 설정을 보고 업데이트할 수 있습니다.

- IP—애플리케이션을 설치할 때 입력한 IP 주소와 DHCP 클라이언트 설정을 업데이트합니다.
- NTP 서버 설정—외부 NTP 서버의 IP 주소를 구성하고 NTP 서버를 추가합니다.
- SMTP 설정—이메일 알림을 보내기 위해 운영 체제가 사용할 SMTP(Simple Mail Transfer Protocol) 호스트를 구성합니다.

운영 체제 보안 구성

보안 인증서와 IPsec 설정을 관리할 수 있습니다. 보안 메뉴에서 다음 보안 옵션을 선택할 수 있습니다.

- 인증서 관리—인증서와 인증서 서명 요청(CSR)을 관리합니다. 인증서를 표시, 업로드, 다운로드, 삭제 및 다시 생성할 수 있습니다. 인증서 관리를 통해 노드에서 인증서의 만료 날짜를 모니터링할 수도 있습니다.
- IPsec 관리—기존 IPsec 정책을 표시하거나 업데이트하고 새 IPsec 정책 및 연결을 설정합니다.

소프트웨어 업그레이드

운영 체제를 실행 중인 소프트웨어 버전을 업그레이드하거나 또는 Cisco Unified Communications 운영 체제 로캘 설치 프로그램, 다이얼 플랜 및 TFTP 서버 파일을 포함한 특정 소프트웨어 옵션을 설치할 수 있습니다.

설치/업그레이드 메뉴 옵션에서 로컬 디스크 또는 원격 서버에서 시스템 소프트웨어를 업그레이드할 수 있습니다. 업그레이드된 소프트웨어가 비활성 파티션에 설치되고 시스템을 다시 시작하고 파티션을 전환할 수 있으므로 시스템은 최신 소프트웨어 버전에서 실행을 시작합니다. 자세한 내용은 http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-guides-list.html에서 *Cisco Unified Communications Manager* 업그레이드 가이드를 참조하십시오.

참고 Cisco Unified Communications Operating System 인터페이스 및 CLI에 포함된 소프트웨어 업그레이드 기능을 통해 모든 소프트웨어 설치와 업그레이드를 수행해야 합니다. 시스템은 Cisco Systems가 승인한 소프트웨어만 업로드 및 처리할 수 있습니다. 승인되지 않은 타사 또는 Windows 기반 소프트웨어 애플리케이션을 설치하거나 사용할 수는 없습니다.

서비스

애플리케이션은 다음과 같은 운영 체제 유틸리티를 제공합니다.

- Ping—다른 네트워크 장치와의 연결을 확인합니다.
- 원격 지원—Cisco 기술 지원 담당자가 시스템에 액세스하는 데 사용할 수 있는 계정을 설정합니다. 이 계정은 사용자가 지정한 일수가 지나면 자동으로 만료됩니다.

CLI

CLI는 운영 체제에서 또는 서버에 대한 보안 셸 연결을 통해 액세스할 수 있습니다. 자세한 내용은 http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html에서 *Cisco Unified Communications Solutions*용 명령줄 인터페이스 설명서를 참조하십시오.

인증 네트워크 시간 프로토콜 지원

Cisco Unified Communications Manager 릴리스 12.0(1)에서는 Unified Communications Manager를 위한 인증된 NTP(Network Time Protocol) 기능이 지원됩니다. 이 지원은 Unified Communications Manager에 대한 보안 NTP 서버 연결에 추가됩니다. 이전 릴리스에서 NTP 서버에 대한 Unified Communications Manager 연결은 보호되지 않았습니다.

이 기능은 대칭 키 기반 인증을 기반으로 하며 NTPv3 및 NTPv4 서버에 의해 지원됩니다. Unified Communications Manager는 SHA1 기반 암호화만 지원합니다. SHA1 기반 대칭 키 지원은 NTP 버전 4.2.6 이상에서 사용할 수 있습니다.

- 대칭 키
- 인증 없음

Cisco Unified OS 관리 애플리케이션의 관리 CLI 또는 **NTP** 서버 목록 페이지를 통해 NTP 서버의 인증 상태를 확인할 수 있습니다.

자동 키 인증 네트워크 시간 프로토콜 지원

Cisco Unified Communications Manager는 자동 키 기능(공개 키 인프라 기반 인증)을 통해 NTP(Network Time Protocol) 인증도 지원합니다. 이 기능은 게시자 노드에만 적용할 수 있습니다.

Redhat에서는 자동 키를 통한 대칭 키 인증을 권장합니다. 자세한 내용은 https://access.redhat.com/support/cases/#/case/01871532의 내용을 참조하십시오.

PKI 기반 인증이 공통 기준 인증에 필수이므로 이 기능이 추가됩니다.

Cisco Unified Communication Manager에서 공통 기준 모드가 활성화된 경우에만 IFF ID 체계를 사용하여 PKI 기반 인증을 구성할 수 있습니다.

Cisco Unified Communications Manager에서 대칭 키 또는 PKI 기반 NTP 인증을 활성화할 수 있습니다.

PKI 활성 서버에서 대칭 키를 활성화하려고 하면 다음 경고 메시지가 표시됩니다.

경고! 자동 키를 사용한 NTP 인증이 현재 활성화되었고 대칭 키를 활성화하기 전에 비활성화해야 합니다. 명령 'utils ntp auth auto-key disable'을 사용하여 NTP 인증을 비활성화한 다음, 이 명령을 재시도합니다.

대칭 키가 활성화된 서버에서 자동 키를 활성화하려고 하면 다음 경고 메시지가 표시됩니다.

경고! 대칭 키를 사용한 NTP 인증이 현재 활성화되었고 자동 키를 활성화하기 전에 비활성화해야 합니다. 명령 'utils ntp auth symmetric-key disable'을 사용하여 NTP 인증을 비활성화한 다음, 이 명령을 재시도합니다.

참고 NTP 서버에는 ntp 버전 4 및 rpm 버전 ntp-4.2.6p5-1.el6.x86_64.rpm 이상이 필요합니다.

Cisco Unified OS 관리 애플리케이션의 관리 CLI 또는 NTP 서버 목록 페이지를 통해 NTP 서버의 인증 상태를 확인할 수 있습니다.

Cisco 통합 서비스 가용성 개요

Cisco 통합 서비스 가용성는 다양한 서비스, 알림 및 관리자의 시스템 관리에 도움이 되는 도구를 제공하는 웹 기반 문제 해결 도구입니다. Cisco 통합 서비스 가용성가 관리자에게 제공하는 기능은 다음과 같습니다.

- 시작 및 중지 서비스 - -관리자가 시스템을 관리하는 데 도움이 되는 서비스를 설정할 수 있습니다. 예를 들어, 관리자가 실시간 모니터링 도구를 사용하여 시스템의 상태를 모니터링할 수 있도록 Cisco CallManager Serviceability RTMT 서비스를 시작할 수 있습니다.
- SNMP—SNMP를 사용하면 노드, 라우터 등과 같은 네트워크 장치 간에 관리 정보를 교환하기 쉽습니다. TCP/IP 프로토콜의 일부로 SNMP를 사용하면 관리자가 네트워크 성능을 원격 관리하고 네트워크 문제를 찾아 해결하며 네트워크 확장을 계획할 수 있습니다.
- 알람—시스템과 관련된 문제를 해결할 수 있도록 알람은 런타임 상태 및 시스템 상태 정보를 제공합니다.
- 추적—추적 도구는 음성 애플리케이션으로 문제를 해결하는 데 도움이 됩니다.
- Cisco Serviceability Reporter—Cisco Serviceability Reporter는 Cisco 통합 서비스 가용성에서 일별 보고서를 생성합니다.
- SNMP—SNMP를 사용하면 노드, 라우터 등과 같은 네트워크 장치 간에 관리 정보를 교환하기 쉽습니다. TCP/IP 프로토콜의 일부로 SNMP를 사용하면 관리자가 네트워크 성능을 원격 관리하고 네트워크 문제를 찾아 해결하며 네트워크 확장을 계획할 수 있습니다.
- CallHome—Cisco Unified Communications Manager가 진단 경고, 재고 및 기타 메시지를 Smart Call Home 백엔드 서버와 통신하고 전송할 수 있도록 Cisco Unified Communications Manager Call Home 기능을 구성합니다.

추가 관리 인터페이스

Cisco 통합 서비스 가용성를 사용하여 다음과 같은 추가 관리 인터페이스를 사용할 수 있는 서비스를 시작할 수 있습니다.

- 실시간 모니터링 도구—실시간 모니터링 도구는 시스템의 상태를 모니터링할 수 있는 웹 기반 인터페이스입니다. RTMT를 사용하여 시스템의 상태에 대한 자세한 정보를 포함하는 알람, 카운터 및 보고서를 볼 수 있습니다.
- Dialed Number Analyzer—Dialed Number Analyzer는 관리자가 다이얼 플랜 문제를 해결하는 데 도움이 되는 웹 기반 인터페이스입니다.

- Cisco Unified CDR Analysis and Reporting-CDR Analysis and Reporting은 시스템에서 건 통화의 세부 정보를 보여주는 통화 상세 내역 레코드를 수집합니다.

Cisco 통합 서비스 가용성를 사용하는 방법에 대한 자세한 내용은 http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html에서 *Cisco* 통합 서비스 가용성 관리 설명서를 참조하십시오.

Cisco Unified Reporting 개요

Cisco Unified Reporting 웹 애플리케이션은 클러스터 데이터 문제 해결 또는 검사에 대한 보고서를 생성합니다. Unified Communications Manager 및 Unified Communications Manager IM and Presence Service 콘솔에서 애플리케이션에 액세스할 수 있습니다.

이 도구는 클러스터 데이터의 스냅샷을 얻는 간단한 방법을 제공합니다. 이 도구는 기존 소스에서 데이터를 수집하고 데이터를 비교하며 불규칙성을 보고합니다. Cisco Unified Reporting에서 보고서를 생성하면 보고서는 하나 이상의 서버에 있는 하나 이상의 소스의 데이터를 하나의 출력 보기로 결합합니다. 예를 들어, 시스템을 관리하는 데 도움이 되는 다음 보고서를 볼 수 있습니다.

- Unified CM 클러스터 개요—이 보고서를 보고 Cisco Unified Communications Manager 및 IM and Presence Service 버전, 서버 호스트 이름 및 하드웨어 세부 사항을 포함하여 클러스터의 스냅샷을 얻을 수 있습니다.
- 전화기 기능 목록—기능을 구성하는 경우 이 보고서를 봅니다. 이 보고서는 전화기가 어느 Cisco Unified Communications Manager 기능을 지원하는지 보여주는 목록을 제공합니다.
- 회선 없는 Unified CM 전화기—클러스터에 있는 전화기에 전화기 회선이 없는지 보려면 이 보고서를 봅니다.

Cisco Unified Reporting을 통해 제공되는 보고서의 전체 목록과 애플리케이션을 사용하는 방법에 대한 지침은 http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html에 있는 *Cisco Unified Reporting* 관리 설명서를 참조하십시오.

재해 복구 시스템 개요

Cisco Unified Communications Manager 관리에서 호출할 수 있는 재난 복구 시스템(DRS)은 전체 데이터 백업 및 복원 기능을 제공합니다. 재해 복구 시스템을 사용하면 정기적으로 예약된 자동 또는 사용자가 호출한 데이터 백업을 수행할 수 있습니다.

DRS은 플랫폼 백업/복원의 일환으로 자체 설정(백업 디바이스 설정 및 예약 설정)을 복원합니다. DRS는 `drfDevice.xml` 및 `drfSchedule.xml` 파일을 백업 및 복원합니다. 이러한 파일로 서버가 복원되면 DRS 백업 디바이스 및 일정을 다시 구성할 필요가 없습니다.

재해 복구 시스템에는 다음과 같은 기능이 포함됩니다.

- 백업 및 복원 작업을 수행하기 위한 사용자 인터페이스.

- 백업 및 복원 기능을 수행하기 위해 분산된 시스템 아키텍처.
- 예약된 백업.
- 실제 테이프 드라이브 또는 원격 SFTP 서버에 백업을 보관합니다.

벌크 관리 도구 개요

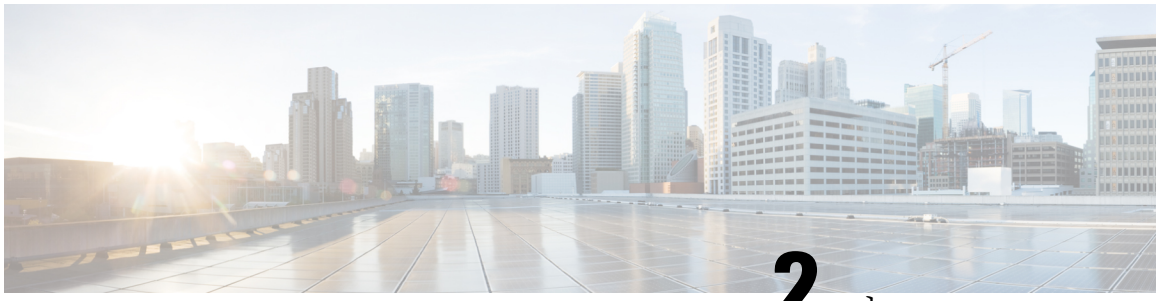
Cisco Unified CM 관리에서 [벌크 관리] 메뉴와 하위 메뉴 옵션을 사용하면 Bulk Administration Tool 사용을 통해 Unified Communications Manager의 항목을 구성할 수 있습니다.

Unified Communications Manager BAT(Bulk Administration Tool)는 웹 기반 애플리케이션으로, 관리자가 Unified Communications Manager 데이터베이스에 대한 벌크 트랜잭션을 수행할 수 있도록 합니다. BAT에서는 다수의 유사한 전화기, 사용자 또는 포트를 동시에 추가, 업데이트 또는 삭제할 수 있습니다. Cisco Unified CM 관리를 사용하는 경우 데이터베이스 트랜잭션마다 개별 수동 작업이 필요한 반면, BAT에서는 프로세스가 자동화되어 추가, 업데이트 및 삭제 작업을 더 빨리 수행할 수 있습니다.

BAT를 사용하여 다음과 같은 유형의 장치 및 레코드 작업을 수행할 수 있습니다.

- Cisco IP 전화기, 게이트웨이, 전화기, CTI(컴퓨터 텔레포니 인터페이스) 포트 및 H.323 클라이언트 추가, 업데이트 및 삭제
- 사용자, 사용자 자치 프로파일, Cisco Unified Communications Manager Assistant 관리자 및 보조자 추가, 업데이트 및 삭제
- 강제 인증 코드(Forced Authorization Code) 및 클라이언트 매터 코드(Client Matter Code) 추가 또는 삭제
- 통화 당겨받기 그룹 추가 또는 삭제
- 지역 매트릭스 채우기/채우기 취소
- 액세스 목록 삽입, 삭제 또는 내보내기
- 원격 대상/원격 대상 프로파일 삽입, 삭제 또는 내보내기
- 인프라 장치 추가

벌크 관리 도구를 사용하는 방법에 대한 자세한 내용은 *Cisco Unified Communications Manager* 벌크 관리 설명서를 참조하십시오.



2 장

시작하기

- 관리 인터페이스에 로그인, 9 페이지
- 관리자 또는 보안 암호 재설정, 9 페이지
- 시스템 종료 또는 다시 시작, 11 페이지

관리 인터페이스에 로그인

이 절차를 수행하여 시스템의 관리 인터페이스 중 하나에 로그인합니다.

프로시저

단계 **1** 웹 브라우저에서 Unified Communications Manager 인터페이스를 엽니다.

단계 **2** 탐색 드롭다운 목록에서 관리 인터페이스를 선택합니다.

단계 **3** 이동을 클릭합니다.

단계 **4** 사용자 이름과 암호를 입력합니다.

단계 **5** 로그인을 클릭합니다.

관리자 또는 보안 암호 재설정

관리자 암호를 잊어버려 시스템에 액세스할 수 없는 경우 다음 절차를 수행하여 암호를 다시 설정할 수 있습니다.

참고 IM and Presence 노드의 암호 변경 사항에 대해 관리자 암호를 재설정하기 전에 모든 IM and Presence 노드에서 Cisco Presence 엔진 서비스를 중지합니다. 암호가 재설정되면 모든 노드에서 Cisco Presence 엔진 서비스를 다시시작합니다. PE가 중지되었을 때 프레즌스 문제가 발생할 수 있으므로 유지 보수 중에 이 작업을 수행해야 합니다.

시작하기 전에

- 이 절차를 수행하는 노드에 실제로 액세스해야 합니다.
- 언제든지, CD 또는 DVD 미디어를 삽입할 것을 요청하면 VMWare 서버용 vSphere Client를 통해 ISO 파일을 마운트해야 합니다. 안내서는 "가상 머신에 DVD 또는 CD 드라이브 추가"https://www.vmware.com/support/ws5/doc/ws_disk_add_cd_dvd.html를 참조하십시오.
- 클러스터의 모든 노드에서 보안 암호가 일치해야 합니다. 모든 시스템의 보안 암호를 변경하십시오. 그렇지 않으면 클러스터 노드가 통신되지 않습니다.

프로시저

단계 **1** 다음과 같은 사용자 이름과 암호로 게시자 노드의 CLI에 로그인합니다.

a) 사용자 이름: **pwrecovery**

b) 암호: **pwreset**

단계 **2** 아무 키나 눌러 계속합니다.

단계 **3** 디스크 드라이브에 올바른 CD/DVD가 있거나 ISO 파일을 마운트했으면 VMWare 클라이언트에서 제거합니다.

단계 **4** 아무 키나 눌러 계속합니다.

단계 **5** 드라이브에 유효한 CD 또는 DVD를 삽입하거나 ISO 파일을 마운트합니다.

참고 이 테스트에는 데이터일 뿐인 ISO 파일이나 디스크를 사용해야 합니다.

단계 **6** 시스템이 마지막 단계를 확인하고 나면 다음 옵션 중 한 가지를 입력하여 계속 진행하라는 메시지가 표시됩니다.

- 관리자 암호를 재설정하려면 **a**를 입력합니다.
- 보안 암호를 재설정하려면 **s**를 입력합니다.

참고 보안 암호를 변경한 후 클러스터에서 각 노드를 재설정해야 합니다. 노드를 재부팅하지 못하면 시스템 서비스 문제 및 가입자 노드의 관리 창에서 문제가 발생합니다.

단계 **7** 새 암호를 입력한 다음 다시 암호를 입력하여 확인합니다.

관리자 자격 증명은 반드시 영문자로 시작해야 하며 최소 여섯 글자 이상이어야 하고 영숫자, 하이픈과 밑줄을 포함할 수 있습니다.

단계 **8** 시스템이 새 암호의 강도를 확인하면 암호가 재설정되고 아무 키나 눌러 암호 재설정 유틸리티를 종료하라는 메시지가 표시됩니다.

다른 관리자 암호를 설정하려면 **set password** CLI 명령을 사용합니다. 자세한 내용은 http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/

products-maintenance-guides-list.html에서 *Cisco Unified Solutions*용 명령줄 인터페이스 설명서를 참조하십시오.

시스템 종료 또는 다시 시작

예를 들어, 구성 변경 사항을 작성한 후, 시스템을 종료하거나 다시 시작해야 할 경우 이 절차를 따르십시오.

시작하기 전에

가상 머신에서 서버를 종료하고 다시 시작해야 하는 경우에는 파일 시스템이 손상된 것일 수 있습니다. 강제 종료를 피합니다. 대신, 이 절차 후 또는 CLI에서 **utils system shutdown**을 실행한 후 서버가 적절하게 종료되기를 기다립니다.

참고 utils system shutdown CLI 명령을 사용하여 가상 시스템을 종료 거나 다시 시작하는 것이 좋습니다. system-history는 명령 항목을 표시하며 정상 종료로 간주됩니다. VSphere 클라이언트에서 종료 또는 재시작을 수행하는 경우 비정상적인 종료로 간주되고 system-history.log에서 해당 항목을 사용할 수 없습니다. VSphere 클라이언트에서 시스템 종료/재부팅은 버전 10.x 이후에서 지원되지 않습니다.

참고 VMware 관리 도구(vCenter 또는 임베디드 호스트 클라이언트)에서 가상 머신을 강제 종료하거나 다시 시작하는 경우:

- 12.5(1)SU3 이전 버전의 경우 이는 비정상적인 종료/다시 시작이며 파일 시스템이 손상될 수 있습니다. 비정상적인 종료는 system-history.log에 표시됩니다. 대신 utils system shutdown CLI 명령을 사용하여 정상적으로 종료하거나 다시 시작하는 것이 좋습니다 .이 명령은 system-history.log에서 정상 종료/재시작으로 표시됩니다.

프로시저

단계 **1** Cisco Unified OS 관리에서 설정 > 버전을 선택합니다.

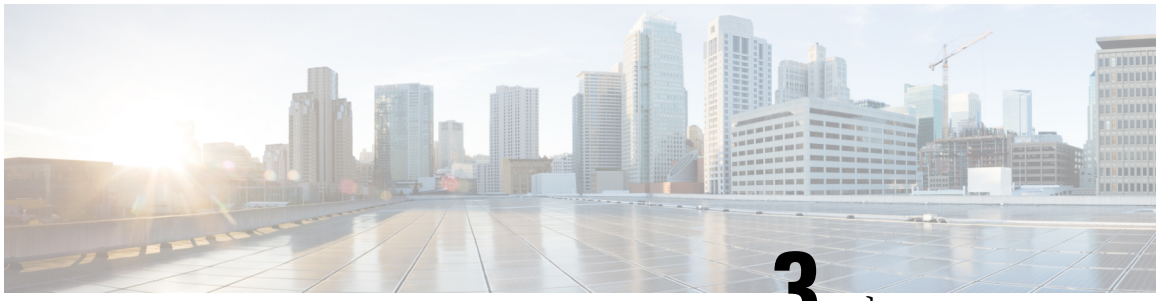
단계 **2** 다음 작업 중 하나를 수행합니다.

- 모든 프로세스를 중지하고 시스템을 종료하려면 종료를 클릭합니다.
- 모든 프로세스를 중지하고 시스템을 다시 시작하려면 다시 시작을 클릭합니다.

II 부

사용자 관리

- 사용자 액세스 관리, 15 페이지
- 최종 사용자 관리, 41 페이지
- 애플리케이션 사용자 관리, 53 페이지



3 장

사용자 액세스 관리

- 사용자 액세스 개요, 15 페이지
- 사용자 액세스 필수 구성 요소, 20 페이지
- 사용자 액세스 구성 작업 흐름 , 20 페이지
- 비활성 사용자 계정 비활성화 , 29 페이지
- 원격 계정 설정, 30 페이지
- 표준 역할 및 액세스 제어 그룹, 30 페이지

사용자 액세스 개요

다음 항목을 구성하여 Cisco Unified Communications Manager에 대한 사용자 액세스를 관리합니다.

- 액세스 제어 그룹
- 역할
- 사용자 순위

액세스 제어 그룹 개요

액세스 제어 그룹은 사용자 및 해당 사용자에게 할당된 역할의 목록입니다. 최종 사용자, 애플리케이션 사용자 또는 관리자 사용자를 액세스 제어 그룹에 할당할 때 사용자는 해당 그룹에 연결된 역할의 액세스 권한을 얻게 됩니다. 필요한 역할과 권한만 있는 액세스 제어 그룹에 비슷한 액세스 요구 사항을 가진 사용자를 할당하여 시스템 액세스를 관리할 수 있습니다.

액세스 제어 그룹에는 다음 두 가지 유형이 있습니다.

- 표준 액세스 제어 그룹 - 일반 배포 요구 사항을 충족하는 역할 할당을 사용하는 미리 정의된 기본 그룹입니다. 표준 그룹에서는 역할 할당을 편집할 수 없습니다. 그러나 사용자를 추가하고 삭제하는 것은 물론 사용자 순위 요구 사항도 편집할 수 있습니다 . 표준 액세스 제어 그룹 목록과 관련 역할에 대한 자세한 내용은 표준 역할 및 액세스 제어 그룹, 30 페이지의 내용을 참조하십시오.

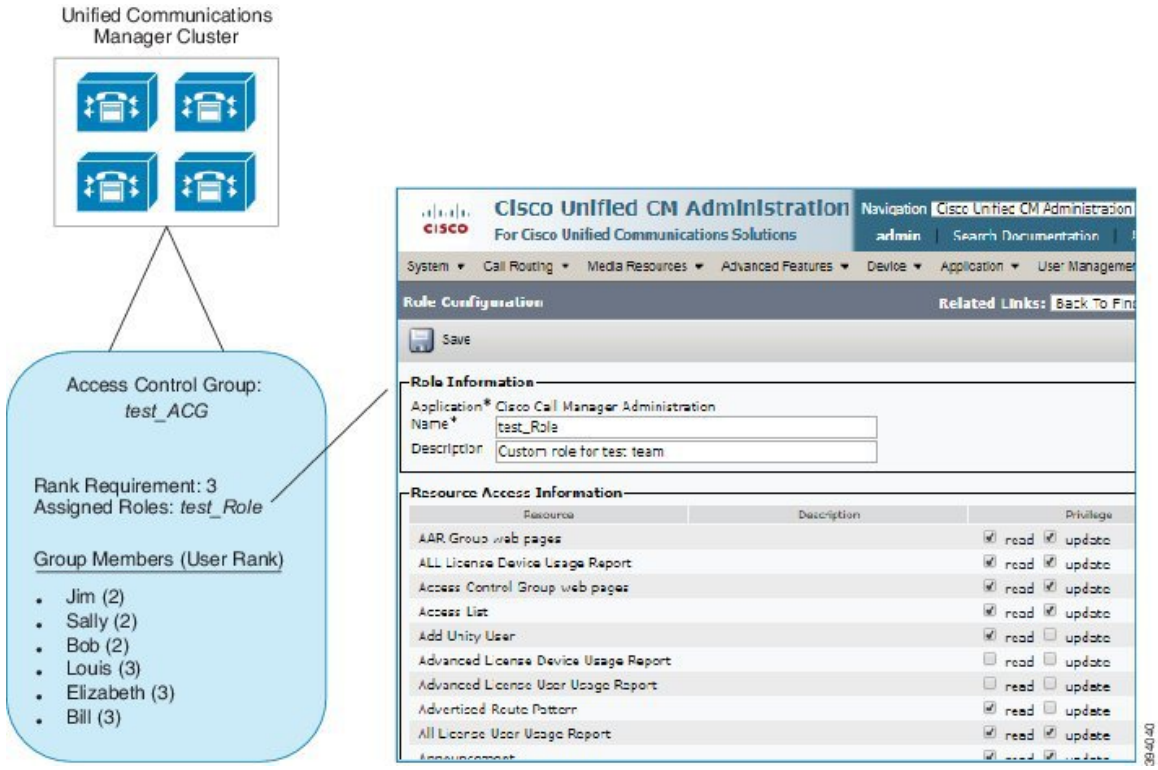
- 사용자 정의 액세스 제어 그룹 - 사용자의 요구에 맞는 역할 권한을 포함하는 표준 그룹이 없는 경우 고유한 액세스 제어 그룹을 생성합니다.

사용자 순위 프레임워크는 사용자에 게 할당할 수 있는 액세스 제어 그룹에 대한 제어 세트를 제공합니다. 액세스 제어 그룹에 할당하려면 사용자가 해당 그룹의 최소 순위 요구 사항을 충족해야 합니다. 예를 들어, 사용자 순위가 4인 최종 사용자는 최소 순위 요구사항이 4~10인 액세스 제어 그룹에만 할당할 수 있습니다. 최소 순위가 1인 그룹에는 할당할 수 없습니다.

예 - 액세스 제어 그룹을 포함한 역할 권한

다음 예는 테스트 팀의 구성원이 액세스 제어 그룹 **test_ACG**에 할당된 클러스터를 보여줍니다. 오른쪽의 화면 캡처에는 액세스 제어 그룹에 연결된 역할인 test_Role의 액세스 설정이 표시됩니다. 또한 액세스 제어 그룹의 최소 순위 요구사항은 3입니다. 모든 그룹 구성원이 1~3등급 사이의 순위를 가지고 있어야 그룹에 참가할 수 있습니다.

그림 ***1:*** 액세스 제어 그룹을 포함한 역할 권한



역할 개요

사용자는 사용자가 구성원인 액세스 제어 그룹에 연결된 역할을 통해 시스템 액세스 권한을 얻습니다. 각 역할에는 특정 리소스나 애플리케이션(예: Cisco Unified CM 관리 또는 CDR 분석 및 보고)에 연결 된 권한 집합이 포함되어 있습니다. Cisco Unified CM 관리 같은 애플리케이션에의 경우 할에는 애플리케이션의 특정 GUI 페이지를 보거나 편집할 수 있는 권한이 포함될 수 있습니다. 리소스 또는 애플리케이션에 할당할 수 있는 권한 수준에는 다음 세 가지가 있습니다.

- 읽기 - 사용자가 리소스에 대한 설정을 볼 수 있습니다.
- 업데이트 — 사용자가 리소스에 대한 설정을 편집할 수 있습니다.
- 액세스 없음 - 사용자가 읽기 또는 업데이트 액세스 권한이 없는 경우에는 사용자가 지정된 리소스에 대한 설정을 보거나 편집할 수 없습니다.

역할 유형

사용자를 프로비저닝하는 경우 적용할 역할을 결정한 다음, 역할을 포함하는 액세스 제어 그룹에 사용자를 할당해야 합니다. Cisco Unified Communications Manager에는 두 가지 기본 역할 유형이 있습니다.

- 표준 역할 — 일반 배포의 요구 사항을 충족하도록 설계된 사전 설치된 기본 역할입니다. 표준 역할에 대한 권한은 편집할 수 없습니다.
- 사용자 정의 역할 — 표준 역할에 필요한 권한이 없을 때 사용자 정의 역할을 만듭니다. 또한 보다 세부적인 수준의 액세스 제어가 필요한 경우에는 고급 설정을 적용하여 관리자가 키 사용자 설정을 편집하는 기능을 제어할 수 있습니다. (자세한 내용은 아래 섹션을 참조하십시오.)

고급 역할 설정

사용자 정의 역할을 생성할 때 애플리케이션 사용자 구성 및 최종 사용자 구성 창에서 선택한 필드에 상세 제어 수준을 추가할 수 있습니다.

고급 역할 구성 창에서는 다음과 같은 작업에 대한 액세스를 제한하면서 Cisco Unified CM 관리에 대한 액세스를 구성할 수 있습니다.

- 사용자 추가
- 암호 편집
- 사용자 순위 편집
- 액세스 제어 그룹 편집

다음 표에는 이 구성으로 적용 할 수 있는 추가 컨트롤이 자세히 나와 있습니다.

표 *1:* 고급 리소스 액세스 정보

고급 리소스	액세스 제어
권한 정보	액세스 제어 그룹 추가 또는 편집 기능 제어: • 보기 - 사용자는 액세스 제어 그룹을 볼 수는 있지만 액세스 제어 그룹을 추가, 편집 또는 삭제할 수는 없습니다. • 업데이트 - 사용자는 액세스 제어 그룹을 추가, 편집 또는 삭제할 수 있습니다. 참고 두 값을 모두 선택하지 않으면 권한 정보섹션을 사용할 수 없습니다. 참고 보기를 선택하면 사용자가 자신의 사용자에 대한 권한 정보를 업데이트할 수 있음 필드가 아니요로 설정되고 비활성화됩니다. 이 필드를 편집할 수 있게 하려면 권한 정보 필드를 업데이트로 설정해야 합니다.
사용자는 자신의 사용자에 대한 권한 정보를 업데이트할 수 있음	사용자가 자신의 액세스 권한을 편집하는 기능을 제어: • 예 - 사용자가 자신의 권한 정보를 업데이트할 수 있습니다. • 아니요 - 사용자가 자신의 권한 정보를 업데이트할 수 없습니다. 그러나 사용자는 동일하거나 더 낮은 사용자에 대한 권한 정보를 보거나 수정할 수 있습니다. 참고 권한 정보업데이트 확인란을 선택하지 않은 경우 사용자가 자신의 사용자에 대한 권한 정보를 업데이트할 수 있음 필드는 아니요로 설정되고 비활성화됩니다.
사용자 순위	사용자 순위를 변경하는 기능을 제어합니다. • 보기 - 사용자는 사용자 등급을 볼 수는 있지만 사용자 등급은 변경할 수 없습니다. • 업데이트 - 사용자는 사용자 순위를 변경할 수 있습니다. 참고 두 값을 모두 선택하지 않으면 사용자 순위 섹션을 사용할 수 없습니다. 참고 보기를 선택하면 사용자가 자신의 사용자에 대한 사용자 순위를 업데이트할 수 있음 필드가 아니요로 설정되고 비활성화됩니다. 이 필드를 편집할 수 있게 하려면 사용자 순위 필드를 업데이트로 설정해야 합니다.

고급 리소스	액세스 제어
사용자가 자신의 사용자에 대한 사용자 순위를 업데이트할 수 있음	사용자가 자신의 사용자 순위를 편집하는 기능을 제어: • 예 - 사용자가 자신의 사용자 순위를 업데이트할 수 있습니다. • 아니요 - 사용자가 자신의 사용자 순위를 업데이트할 수 없습니다. 그러나 사용자는 동일하거나 더 낮은 사용자에 대한 사용자 순위를 보거나 수정할 수 있습니다. 참고 사용자 순위업데이트 확인란을 선택하지 않은 경우 사용자가 자신의 사용자에 대한 사용자 순위를 업데이트할 수 있음 필드는 아니요로 설정되고 비활성화됩니다.
새 사용자 추가	새 사용자를 추가하는 기능을 제어합니다. • 예 - 새 사용자를 추가할 수 있습니다. • 아니요 - 새로 추가 버튼을 사용할 수 없습니다.
암호	암호를 변경하는 기능을 제어합니다. • 예 - 애플리케이션 사용자 정보 섹션 아래에서 사용자 암호를 변경할 수 있습니다. • 아니요 - 애플리케이션 사용자 정보 섹션 아래에서 암호 및 암호 확인을 사용할 수 없습니다.

사용자 순위 개요

사용자 순위 계층은 최종 사용자 또는 애플리케이션 사용자에게 관리자가 할당할 수 있는 제어 그룹에 액세스하는 제어 집합을 제공합니다.

최종 사용자 또는 애플리케이션 사용자를 프로비저닝할 때 관리자는 사용자에 대한 사용자 순위를 할당할 수 있습니다. 또한 관리자는 각 액세스 제어 그룹에 사용자 순위 요구 사항을 할당할 수 있습니다. 사용자를 추가하여 제어 그룹에 액세스하는 경우 관리자는 사용자의 사용자 순위가 그룹의 순위 요구 사항을 충족하는 그룹에만 사용자를 할당할 수 있습니다. 예를 들어, 관리자는 사용자 순위가 3인 사용자를 사용자 순위 요구 사항이 3에서 10 사이인 액세스 제어 그룹에 할당할 수 있습니다. 그러나 관리자는 사용자 순위 요구 사항이 1 또는 2인 액세스 제어 그룹에 해당 사용자를 할당할 수 없습니다.

관리자는 사용자 순위 구성 창 내에서 고유한 사용자 순위 계층 구조를 생성할 수 있으며 사용자 및 액세스 제어 그룹을 프로비저닝할 때 해당 계층 구조를 사용할 수 있습니다. 사용자 순위 계층 구조를 구성하지 않거나 사용자 또는 액세스 제어 그룹을 프로비저닝할 때 사용자 순위 설정을 지정하지 않을 경우 모든 사용자 및 액세스 제어 그룹에는 기본 사용자 순위 1(가능한 가장 높은 순위)이 할당됩니다.

사용자 액세스 필수 구성 요소

사용자의 요구 사항을 검토하여 사용자에 게 필요한 액세스 수준을 확인하십시오. 사용자에게 필요한 액세스 권한을 가지는 역할을 할당하려고 하지만 액세스할 수 없는 시스템의 경우 액세스를 제공하지 않습니다.

새 역할 및 액세스 제어 그룹을 생성하기 전에 표준 역할 및 액세스 제어 그룹 목록을 검토하여 기존 액세스 제어 그룹에 필요한 역할 및 액세스 권한이 있는지 확인합니다. 자세한 내용은 표준 역할 및 액세스 제어 그룹, 30 페이지를 참조하십시오.

사용자 액세스 구성 작업 흐름

사용자 액세스를 구성하려면 다음 작업을 완료합니다.

시작하기 전에

기본 역할 및 액세스 제어 그룹을 사용하려는 경우 사용자 정의된 역할 및 액세스 제어 그룹을 만들기 위한 작업을 건너뛸 수 있습니다. 사용자를 기존 기본 액세스 제어 그룹에 할당할 수 있습니다.

프로시저

	명령 또는 동작	목적
단계 **1**	사용자 순위 계층 구조 구성, 21 페이지	사용자 순위 계층을 설정합니다. 이 작업을 건너뛰는 경우 모든 사용자 및 액세스 제어 그룹에 기본 사용자 순위인 1(최고 순위)이 할당됩니다.
단계 **2**	사용자 지정 역할 만들기, 21 페이지	기본 역할에 필요한 액세스 권한이 없는 경우 사용자 정의 역할을 만듭니다.
단계 **3**	관리자를 위한 고급 역할 구성, 22 페이지	(선택 사항) 사용자 정의 역할에서 고급 권한을 사용하면 관리자가 키 사용자 설정을 편집할 수 있는 기능을 제어할 수 있습니다.
단계 **4**	액세스 제어 그룹 만들기, 23 페이지	기본 그룹에 필요한 역할 할당이 없는 경우 사용자 정의 액세스 제어 그룹을 만듭니다.
단계 **5**	액세스 제어 그룹에 사용자 할당, 23 페이지	표준 또는 사용자 정의 액세스 제어 그룹에서 사용자를 추가하거나 삭제합니다.
단계 **6**	액세스 제어 그룹에 대한 권한 정책 중복 구성, 24 페이지	(선택 사항) 이 설정은 충돌하는 권한이 있는 여러 액세스 제어 그룹에 사용자가 할당된 경우에 사용됩니다.

사용자 순위 계층 구조 구성

이 절차를 사용하여 사용자 정의 사용자 순위 계층 구조를 만듭니다.

참고 사용자 순위 계층 구조를 구성하지 않으면 기본적으로 모든 사용자 및 액세스 제어 그룹에 사용자 순위 1(가능한 가장 높은 순위)이 할당됩니다.

프로시저

단계 **1** [Cisco Unified CM 관리]에서 사용자 관리 > 사용자 설정 > 사용자 순위를 선택합니다.

단계 **2** 새로 추가를 클릭합니다.

단계 **3** 사용자 순위 드롭다운 메뉴에서 1-10 사이의 순위 설정을 선택합니다. 가장 높은 순위는 1입니다.

단계 **4** 순위 이름 및 설명을 입력합니다.

단계 **5** 저장을 클릭합니다.

단계 **6** 이 절차를 반복하여 추가 사용자 순위를 추가합니다.
사용자 순위를 사용자 및 액세스 제어 그룹에 할당하여 사용자에게 할당할 수 있는 그룹을 제어할 수 있습니다.

사용자 지정 역할 만들기

이 절차를 사용하여 사용자 정의된 권한이 있는 새 역할을 만듭니다. 정확히 필요한 권한이 있는 표준 역할이 없는 경우 이 작업을 수행할 수 있습니다. 역할을 만드는 방법은 두 가지가 있습니다.

- 새로 추가 버튼을 사용하여 처음부터 새 역할을 만들고 구성합니다.
- 기존 역할이 필요한 권한과 비슷한 액세스 권한을 가지는 경우 복사 버튼을 사용합니다. 기존 역할의 권한을 편집 가능한 새 역할에 복사할 수 있습니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 사용자 관리 > 사용자 설정 > 역할을 클릭합니다.

단계 **2** 다음 중 하나를 수행합니다.

- 새 역할을 만들려면 새로 추가를 클릭합니다. 이 역할이 연결되는 애플리케이션을 선택하고 다음을 클릭합니다 .
- 기존 역할에서 설정을 복사하려면 찾기를 클릭하고 기존 역할을 엽니다. 복사를 클릭하고 새 역할의 이름을 입력합니다. 확인을 클릭합니다.

단계 **3** 역할에 대한 이름 및 설명을 입력합니다.

단계 **4** 각 리소스에 대해 다음을 적용하는 상자를 선택합니다.

- 사용자가 리소스에 대한 설정을 볼 수 있게 하려면 읽기 확인란을 선택합니다.
- 사용자가 리소스의 설정을 편집할 수 있게 하려면 업데이트 확인란을 선택합니다.
- 리소스에 대한 액세스를 제공하지 않으려면 두 확인란을 선택하지 않은 상태로 둡니다.

단계 **5** 모두에게 액세스 부여**{** 또는 모두에게 액세스 거부 버튼을 클릭하여 이 역할에 대해 페이지에 표시되는 모든 리소스에 대한 권한을 부여 또는 제거합니다.

참고 리소스 목록이 두 페이지 이상 표시되는 경우 이 단추는 현재 페이지에 표시되는 리소스에만 적용됩니다. 기타 페이지에 나열된 리소스의 액세스를 변경하려면 해당 페이지를 표시하고 해당 페이지에 있는 버튼을 사용해야 합니다.

단계 **6** 저장을 클릭합니다.

관리자를 위한 고급 역할 구성

고급 역할 구성을 사용하면 보다 세분화된 수준에서 사용자 지정 역할에 대한 권한을 편집할 수 있습니다. 최종 사용자 구성 및 애플리케이션 사용자 구성 창에서 다음 키 설정을 편집하는 관리자의 기능을 제어할 수 있습니다.

- 사용자 순위 편집
- 액세스 제어 그룹 할당 편집
- 신규 사용자 추가
- 사용자 암호 편집

프로시저

단계 **1** [Cisco Unified CM 관리]에서 사용자 관리 > 사용자 설정 > 역할을 선택합니다.

단계 **2** 찾기를 클릭하고 사용자 지정 역할을 선택합니다.

단계 **3** 관련 링크에서 고급 역할 구성을 선택하고 이동을 클릭합니다.

단계 **4** 리소스 웹 페이지에서 애플리케이션 사용자 웹 페이지 또는 사용자 웹 페이지를 선택합니다.

단계 **5** 설정을 편집합니다. 필드 및 해당 설정에 대한 도움이 필요한 경우 온라인 도움말을 참조하십시오.

단계 **6** 저장을 클릭합니다.

액세스 제어 그룹 만들기

새 액세스 제어 그룹을 생성해야 하는 경우 이 절차를 사용하십시오. 필요한 역할 및 액세스 권한을 가진 표준 그룹이 없는 경우 이 작업을 수행할 수 있습니다. 사용자 정의 그룹을 만드는 방법은 두 가지가 있습니다.

- 새로 추가 버튼을 사용하여 처음부터 새 액세스 제어 그룹을 만들고 구성합니다.
- 기존 그룹이 필요한 그룹과 비슷한 역할 할당을 가지는 경우 복사 버튼을 사용합니다. 기존 그룹의 설정을 새 그룹 및 편집 가능한 그룹으로 복사할 수 있습니다.

프로시저

단계 **1** [Cisco Unified CM 관리]에서 사용자 관리 > 사용자 설정 > 액세스 제어 그룹을 선택합니다

단계 **2** 다음 중 하나를 수행합니다.

- 처음부터 새 그룹을 만들려면 새로 추가를 클릭합니다.
- 기존 그룹의 설정을 복사하려면 찾기를 클릭하고 기존 액세스 제어 그룹을 엽니다. 복사를 클릭하고 새 그룹의 이름을 입력합니다. 확인을 클릭합니다.

단계 **3** 액세스 제어 그룹의 이름을 입력합니다.

단계 **4** 사용자 순위가 다음과 같은 사용자에 사용 가능 드롭다운에서 이 그룹에 할당하기 위해 사용자가 충족해야 하는 최소 사용자 순위를 선택합니다. 기본 사용자 순위는 1입니다.

단계 **5** 저장을 클릭합니다.

단계 **6** 액세스 제어 그룹에 역할을 할당합니다. 선택하는 역할은 그룹 구성원에게 할당됩니다.

a) 관련 링크에서 액세스 제어 그룹에 역할 할당을 선택하고 이동을 클릭합니다.
b) 찾기를 클릭하여 기존 역할을 검색합니다.
c) 추가할 역할을 선택하고 선택한 항목 추가를 클릭합니다.
d) 저장을 클릭합니다.

다음에 수행할 작업

액세스 제어 그룹에 사용자 할당, 23 페이지

액세스 제어 그룹에 사용자 할당

표준 또는 사용자 정의 액세스 제어 그룹에서 사용자를 추가하거나 삭제합니다. .

참고 사용자 순위가 액세스 제어 그룹에 대한 최소 사용자 순위와 같거나 더 높은 사용자만 추가할 수 있습니다.

참고 회사 LDAP 디렉터리에서 새 사용자를 동기화하는 중이거나 적절한 권한으로 순위 계층 및 액세스 제어 그룹이 생성되는 경우 LDAP 동기화의 일부로 해당 그룹을 동기화된 사용자에게 할당할 수 있습니다. LDAP 디렉터리 동기화를 설정하는 방법에 대한 추가 정보는 *Cisco Unified Communications Manager* 시스템 구성 설명서를 참조하십시오.

프로시저

단계 **1** 사용자 관리 > 사용자 설정 > 액세스 제어 그룹을 선택합니다.

액세스 제어 그룹 찾기 및 나열 창이 나타납니다.

단계 **2** 찾기를 클릭하고 사용자 목록을 업데이트할 액세스 제어 그룹의 이름을 선택합니다.

단계 **3** 사용자 순위가 다음과 같은 사용자에 사용 가능 드롭다운에서 이 그룹에 할당하기 위해 사용자가 충족해야 하는 순위 요구 사항을 선택합니다.

단계 **4** 사용자 섹션에서 찾기를 클릭하여 사용자 목록을 표시합니다.

단계 **5** 액세스 제어 그룹에 최종 사용자 또는 애플리케이션 사용자를 추가하려면 다음을 수행합니다.

a) 액세스 제어 그룹에 최종 사용자 추가 또는 액세스 제어 그룹에 애플리케이션 사용자 추가를 클릭합니다.
b) 추가하려는 사용자를 선택합니다.
c) 선택한 항목 추가를 클릭합니다.

단계 **6** 액세스 제어 그룹에서 사용자를 삭제하려면:

a) 삭제하려는 사용자를 선택합니다.
b) 선택한 항목 삭제를 클릭합니다.

단계 **7** 저장을 클릭합니다.

액세스 제어 그룹에 대한 권한 정책 중복 구성

Cisco Unified Communications Manager가 액세스 제어 그룹 할당에서 발생할 수 있는 중복 사용자 권한을 처리하는 방법을 구성합니다. 여기에서는 각각 역할 및 권한 설정이 충돌하는 상태에서 최종 사용자가 여러 액세스 제어 그룹에 할당된 상황을 처리합니다.

프로시저

단계 **1** [Cisco Unified CM 관리]에서 시스템 > 엔터프라이즈 매개 변수를 선택합니다.

단계 **2** 사용자 관리 매개 변수에서 다음과 같이 사용자 그룹 및 역할을 중복하는 유효 액세스 권한에 대해 다음 값 중 하나를 구성합니다.

- 최대—유효 권한은 모든 중첩 액세스 제어 그룹의 최대 권한을 나타냅니다. 이것이 기본 옵션입니다.
- 최소—유효 권한은 모든 중첩 액세스 제어 그룹의 최소 권한을 나타냅니다.

단계 **3** 저장을 클릭합니다.

사용자 권한 보고서 보기

기존 최종 사용자 또는 기존 애플리케이션 사용자에 대한 사용자 권한 보고서를 보려면 다음 절차를 수행합니다. 사용자 권한 보고서는 최종 사용자 또는 애플리케이션 사용자에 할당된 액세스 제어 그룹, 역할 및 액세스 권한을 표시합니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 다음 단계 중 하나를 수행합니다.

- 최종 사용자의 경우 사용자 관리 > 최종 사용자를 선택합니다.
- 애플리케이션 사용자의 경우 사용자 관리 > 애플리케이션 사용자를 선택합니다.

단계 **2** 찾기를 클릭하고 액세스 권한을 보려는 사용자를 선택합니다.

단계 **3** 관련 링크 드롭다운 목록에서 사용자 권한 보고서를 선택한 다음 이동을 클릭합니다.
사용자 권한 창이 표시됩니다.

사용자 지정 지원 센터 역할 작업 흐름 만들기

일부 회사에서는 지원 센터 직원이 특정 관리 작업을 수행할 수 있도록 권한을 부여하기를 원합니다. 전화기를 추가하고 최종 사용자를 추가하는 등의 작업을 수행할 수 있는 지원 센터 팀원을 위한 역할 및 액세스 제어 그룹을 구성하려면 이 작업 흐름의 단계를 수행합니다.

프로시저

	명령 또는 동작	목적
단계 **1**	사용자 지정 지원 센터 역할 만들기, 26 페이지	지원 센터 팀 구성원을 위한 사용자 정의 역할을 만들고 새 전화기 추가 및 새 사용자 추가 같은 항목에 대한 권한을 할당합니다.
단계 **2**	사용자 지정 지원 센터 액세스 제어 그룹 만들기, 26 페이지	지원 센터 역할에 대해 새 액세스 제어 그룹을 만듭니다.
단계 **3**	액세스 제어 그룹에 지원 센터 역할 할당, 27 페이지	지원 센터 액세스 제어 그룹에 지원 센터 역할을 할당합니다. 이 액세스 제어 그룹에 할당된

	명령 또는 동작	목적
		모든 사용자는 지원 센터 역할의 권한이 할당됩니다.
단계 **4**	액세스 제어 그룹에 지원 센터 구성원 할당, 27 페이지	사용자 정의 지원 데스크 역할의 권한을 사용하여 지원 센터 팀 구성원 할당합니다.

사용자 지정 지원 센터 역할 만들기

조직 내의 지원 센터 구성원에 할당할 수 있는 사용자 지정 지원 센터 역할을 만들려면 이 절차를 수행합니다.

프로시저

단계 **1** Cisco Unified Communications Manager 관리에서 사용자 관리 > 사용자 설정 > 역할을 선택합니다.

단계 **2** 새로 추가를 클릭합니다.

단계 **3** 애플리케이션 드롭다운 목록에서 이 역할에 할당하려는 애플리케이션을 선택합니다. 예를 들어, **Cisco CallManager** 관리를 선택합니다.

단계 **4** 다음을 클릭합니다.

단계 **5** 새 역할의 이름을 입력합니다. 예를 들어 지원 센터를 입력합니다.

단계 **6** 권한 읽기 및 업데이트에서 지원 센터 사용자에 할당하려는 권한을 선택합니다. 예를 들어, 지원 센터 구성원이 사용자와 전화기를 추가할 수 있도록 하려면 사용자 웹 페이지와 전화기 웹 페이지에 대해 읽기 및 업데이트 확인란을 선택합니다.

단계 **7** 저장을 클릭합니다.

다음에 수행할 작업

사용자 지정 지원 센터 액세스 제어 그룹 만들기, 26 페이지

사용자 지정 지원 센터 액세스 제어 그룹 만들기

시작하기 전에

사용자 지정 지원 센터 역할 만들기, 26 페이지

프로시저

단계 **1** [Cisco Unified CM 관리]에서 사용자 관리 > 사용자 설정 > 액세스 제어 그룹을 선택합니다.

단계 **2** 새로 추가를 클릭합니다.

단계 **3** 액세스 제어 그룹의 이름을 입력합니다. 예를 들어 지원 센터를 입력합니다.

단계 **4** 저장을 클릭합니다.

다음에 수행할 작업

액세스 제어 그룹에 지원 센터 역할 할당, 27 페이지

액세스 제어 그룹에 지원 센터 역할 할당

지원 센터 역할에서 권한이 있는 지원 센터 액세스 제어 그룹을 구성하려면 다음 단계를 수행합니다.

시작하기 전에

사용자 지정 지원 센터 액세스 제어 그룹 만들기, 26 페이지

프로시저

단계 **1** [Cisco Unified CM 관리]에서 사용자 관리 > 사용자 설정 > 액세스 제어 그룹을 선택합니다.

단계 **2** 찾기를 클릭하고 지원 센터를 위해 사용자가 만든 액세스 제어 그룹을 선택합니다.
액세스 제어 그룹 구성 창이 표시됩니다.

단계 **3** 관련 링크 드롭다운 목록 상자에서 액세스 제어 그룹에 역할 할당 옵션을 선택하고 이동을 클릭합니다.
역할 찾기 및 나열 팝업이 표시됩니다.

단계 **4** 그룹에 역할 할당 버튼을 클릭합니다.

단계 **5** 찾기를 클릭하고 지원 센터 역할을 선택합니다.

단계 **6** 선택한 항목 추가를 클릭합니다.

단계 **7** 저장을 클릭합니다.

다음에 수행할 작업

액세스 제어 그룹에 지원 센터 구성원 할당, 27 페이지

액세스 제어 그룹에 지원 센터 구성원 할당

시작하기 전에

액세스 제어 그룹에 지원 센터 역할 할당, 27 페이지

프로시저

단계 **1** [Cisco Unified CM 관리]에서 사용자 관리 > 사용자 설정 > 액세스 제어 그룹을 선택합니다.

단계 **2** 찾기를 클릭하고 사용자가 만든 사용자 정의 지원 센터 액세스 제어 그룹을 선택합니다.

단계 **3** 다음 단계 중 하나를 수행합니다.

- 지원 센터 팀 구성원이 최종 사용자로 구성된 경우 그룹에 최종 사용자 추가를 클릭합니다.
- 지원 센터 팀 구성원이 애플리케이션 사용자로 구성된 경우 그룹에 앱 사용자 추가를 클릭합니다.

단계 **4** 찾기를 클릭하고 지원 센터 사용자를 선택합니다.

단계 **5** 선택한 항목 추가를 클릭합니다.

단계 **6** 저장을 클릭합니다.

Cisco Unified Communications Manager는 사용자가 만든 사용자 정의 지원 센터 역할의 권한을 사용하여 지원 센터 팀 구성원을 할당합니다.

액세스 제어 그룹 삭제

다음 절차를 사용하여 액세스 제어 그룹을 완전히 삭제합니다.

시작하기 전에

액세스 제어 그룹을 삭제하면 Cisco Unified Communications Manager가 데이터베이스에서 모든 액세스 제어 그룹 데이터를 제거합니다. 어떤 역할이 액세스 제어 그룹을 사용 중인지 확인합니다.

프로시저

단계 **1** 사용자 관리 > 사용자 설정 > 액세스 제어 그룹을 선택합니다.

액세스 컨트롤 그룹 찾기 및 나열 창이 나타납니다.

단계 **2** 삭제할 액세스 제어 그룹을 찾습니다.

단계 **3** 삭제할 액세스 제어 그룹의 이름을 클릭합니다.

선택한 액세스 제어 그룹이 나타납니다. 이 액세스 제어 그룹에 속하는 사용자가 알파벳 순으로 목록에 표시됩니다.

단계 **4** 액세스 제어 그룹을 완전히 삭제하려면 삭제를 클릭합니다.

대화 상자에 액세스 제어 그룹 삭제를 취소할 수 없다는 경고가 표시됩니다.

단계 **5** 액세스 제어 그룹을 삭제하려면 확인을 클릭하거나 작업을 취소하려면 취소를 클릭합니다. 확인을 클릭하는 경우 Cisco Unified Communications Manager가 데이터베이스에서 액세스 제어 그룹을 제거합니다.

기존 OAuth 새로 고침 토큰 해지

AXL API를 사용하여 기존 OAuth 새로 고침 토큰을 해지합니다. 예를 들어, 한 직원이 회사를 퇴사하는 경우 이 API를 사용하여 새 액세스 토큰을 받을 수 없고 더 이상 회사 계정에 로그인 할 수 없도록 해당 직원의 현재 새로 고침 토큰을 해지할 수 있습니다. API는 AXL 인증서에 의해 보호되는 REST 기반 API입니다. API를 호출하려면 명령줄 도구를 사용할 수 있습니다. 다음 명령은 새로 고침 토큰을 해지하는 데 사용할 수 있는 cURL 명령의 예를 제공합니다.

```
curl -k -u "admin:password" https://<UCMaddress:8443/ssosp/token/revoke?user_id=<end_user>
```

여기서:

- `admin:password`는 Cisco Unified Communications Manager 관리자 계정의 로그인 ID와 암호입니다.
- `UCMaddress`는 Cisco Unified Communications Manger 게시자 노드의 FQDN 또는 IP 주소입니다.
- `end_user`는 새로 고침 토큰을 해지하려는 사용자의 사용자 ID입니다.

비활성 사용자 계정 비활성화

다음 절차를 사용하여 Cisco Database Layer Monitor 서비스를 사용하여 비활성 사용자 계정을 비활성화합니다.

지정된 일 수 내에 Cisco Unified Communications Manager에 로그인하지 않은 경우 Cisco Database Layer Monitor는 예약된 유지 보수 작업 중에 사용자 계정 상태를 비활성으로 변경합니다. 비활성화된 사용자는 후속 감사 로그에서 자동으로 감사됩니다.

시작하기 전에

Cisco Database Layer Monitor 서비스(시스템 > 서비스 매개 변수)에서 선택한 서버의 유지 보수 시간을 입력합니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 시스템 > 서비스 매개 변수를 선택합니다.

단계 **2** 서버 드롭다운 목록 상자에서 서버를 선택합니다.

단계 **3** 서비스 드롭다운 목록 상자에서 **Cisco Database Layer Monitor** 매개 변수를 선택합니다.

단계 **4** 고급을 클릭합니다.

단계 **5** 용자 계정 비활성화 미사용 기간**(**일**)** 필드에 일 수를 입력합니다. 예를 들면 90을 입력합니다. 시스템은 입력된 값을 임계값으로 사용하여 계정 상태를 비활성으로 선언합니다. 자동 비활성화를 해제하려면 값을 0으로 입력합니다.

참고 이것은 필수 필드입니다. 기본값 및 최소값은 0이고 단위는 일입니다.

단계 **6** 저장을 클릭합니다.

구성된 일 수 내에 비활성 상태로 남아 있는 경우(예: 90일) 사용자가 비활성화됩니다. 감사 로그에 항목이 생성되고 "< userID > 사용자가 비활성으로 표시됨"이라는 메시지가 표시됩니다.

원격 계정 설정

Cisco 지원이 일시적으로 문제 해결을 위해 시스템에 액세스할 수 있도록 Unified Communications Manager에서 원격 계정을 구성합니다.

프로시저

단계 **1** Cisco Unified Operating System 관리에서 서비스 > 원격 지원을 선택합니다.

단계 **2** 계정 이름 필드에 원격 계정의 이름을 입력합니다.

단계 **3** 계정 기간 필드에 계정 기간(일)을 입력합니다.

단계 **4** 저장을 클릭합니다.
시스템에서 암호화된 암호구를 생성합니다.

단계 **5** Cisco 지원에 연락하여 원격 지원 계정 이름 및 암호를 제공하십시오.

표준 역할 및 액세스 제어 그룹

다음 표는 Cisco Unified Communications Manager에 미리 구성된 표준 역할 및 액세스 제어 그룹을 요약합니다. 표준 역할에 대한 권한은 기본적으로 구성됩니다. 뿐만 아니라 표준 역할에 연결된 액세스 제어 그룹은 기본적으로도 구성됩니다.

표준 역할 및 연결된 액세스 제어 그룹 모두에 대해 권한 또는 역할 할당을 편집할 수 없습니다.

표 *2:* 표준 역할, 권한 및 액세스 제어 그룹

표준 역할	역할에 대한 권한/리소스	연결된 표준 액세스 제어 그룹
표준 AXL API 액세스	AXL 데이터베이스 API에 대한 액세스 허용	표준 CCM 수퍼 사용자
표준 AXL API 사용자	AXL API를 실행할 로그인 권한을 부여합니다.	
표준 AXL 읽기 전용 API 액세스	기본적으로 AXL 읽기 전용 API(list APIs, get APIs, executeSQLQuery API)를 실행할 수 있습니다.	

표준 역할	역할에 대한 권한/리소스	연결된 표준 액세스 제어 그룹
표준 관리 보고 도구 관리	Cisco Unified Communications Manager CDR Analysis and Reporting(CAR)을 보고 구성할 수 있습니다.	표준 CAR 관리 사용자, 표준 CCM 수퍼 사용자
표준 감사 로그 관리	감사 로깅 기능에 대한 다음 작업을 수행할 수 있습니다. • Cisco 통합 서비스 가용성의 감사 로그 구성 창에서 감사 로깅 보기 및 구성 • Cisco 통합 서비스 가용성에서 추적 보기 및 구성과 실시간 모니터링 도구에서 감사 로그 기능에 대한 추적 수집 • Cisco 통합 서비스 가용성에서 Cisco 감사 이벤트 서비스 보기 및 시작/중지 • RTMT에 연결된 경고 보기 및 업데이트	표준 감사 사용자
표준 CCM 관리 사용자	Cisco Unified Communications Manager 관리에 로그인 권한을 부여합니다.	표준 CCM 관리 사용자, 표준 CCM 게이트웨이 관리, 표준 CCM 전화 관리, 표준 CCM 읽기 전용, 표준 CCM 서버 모니터링, 표준 CCM 수퍼 사용자, 표준 CCM 서버 유지 보수, 표준 패킷 스니퍼 사용자
표준 CCM 최종 사용자	Cisco Unified Communications 셀프 케어 포털에 최종 사용자 로그인 권한을 부여합니다	표준 CCM 최종 사용자

표준 역할	역할에 대한 권한/리소스	연결된 표준 액세스 제어 그룹

표준 CCM 기능 관리	Cisco Unified Communications Manager 관리에서 다음 작업을 수행할 수 있습니다.
	• 벌크 관리 도구를 사용하여 다음 항목을 보고, 삭제하고, 삽입합니다.
	  • 클라이언트 매터 코드 및 강제 인증 코드
	  • 통화 당겨받기 그룹
	• Cisco Unified Communications Manager 관리에서 다음 항목을 보고 구성합니다.
	  • 클라이언트 매터 코드 및 강제 인증 코드
	  • 통화 보류
	  • 통화 당겨받기
	  • 강제 인증 코드 번호/패턴
	  • 메시지 대기 중
	  • Cisco Unified IP Phone 서비스
	  • 음성 메일 파일럿, 음성 메일 포트 마법사, 음성 메일 포트 및 음성 메일 프로파일
		표준 CCM 서버 유지 관리

표준 CCM 게이트웨이 관리	Cisco Unified Communications Manager 관리에서 다음 작업을 수행할 수 있습니다. • 벌크 관리 도구에서 게이트웨이 템플릿 보기 및 구성 • 게이트키퍼, 게이트웨이 및 트렁크 보기 및 구성	표준 CCM 게이트웨이 관리

표준 역할	역할에 대한 권한/리소스	연결된 표준 액세스 제어 그룹

표준 CCM 전화 관리	Cisco Unified Communications Manager 관리에서 다음 작업을 수행할 수 있습니다.
	• 벌크 관리 도구에서 전화기 보기 및 내보내기
	• 벌크 관리 도구에서 사용자 장치 프로파일 보기 및 삽입
	• Cisco Unified Communications Manager 관리에서 다음 항목을 보고 구성합니다.
	  • BLF 단축 다이얼
	  • CTI 경로 포인트
	  • 기본 장치 프로파일 또는 기본 프로파일
	  • 디렉터리 번호 및 회선 표시
	  • 펌웨어 로드 정보
	  • 전화기 단추 템플릿 또는 소프트키 템플릿
	  • 전화기
	  • [전화기 구성] 창에서 [단추 항목 수정] 버튼을 클릭하여 특정 전화기에 대한 전화기 단추 정보 순서 바꾸기
		표준 CCM 전화 관리

표준 역할	역할에 대한 권한/리소스	연결된 표준 액세스 제어 그룹
표준 CCM 경로 플랜 관리	Cisco Unified Communications Manager 관리에서 다음 작업을 수행할 수 있습니다. • 애플리케이션 다이얼 규칙 보기 및 구성 • 발신 검색 공간 및 파티션 보기 및 구성 • 다이얼 규칙 패턴을 포함하는 다이얼 규칙 보기 및 구성 • 헌트 목록, 헌트 파일럿 및 회선 그룹 보기 및 구성 • 경로 필터, 경로 그룹, 경로 헌트 목록, 경로 목록, 경로 패턴 및 경로 플랜 보고서 보기 및 구성 • 시간 기간 및 시간 일정 보기 및 구성 • 변환 패턴 보기 및 구성	

표준 CCM 서비스 관리	Cisco Unified Communications Manager 관리에서 다음 작업을 수행할 수 있습니다.
	• 다음 항목을 보고 구성합니다.
	  • 알림 장치, 컨퍼런스 브리지 및 트랜스코더
	  • 오디오 소스 및 MOH 서버
	  • 미디어 리소스 그룹 및 미디어 리소스 그룹 목록
	  • 미디어 종료 지점
	  • Cisco Unified Communications Manager Assistant 마법사
	• 벌크 관리 도구에서 관리자 삭제, 관리자/보조자 삭제 및 관리자/보조자 삽입 창 보기 및 구성
		표준 CCM 서버 유지 관리

표준 역할	역할에 대한 권한/리소스	연결된 표준 액세스 제어 그룹
표준 CCM 시스템 관리	Cisco Unified Communications Manager 관리에서 다음 작업을 수행할 수 있습니다. • 다음 항목을 보고 구성합니다. • AAR(Automate Alternate Routing) 그룹 • Cisco Unified Communications Manager(Cisco Unified CM) 및 Cisco Unified Communications Manager 그룹 • 날짜 및 시간 그룹 • 장치 기본값 • 장치 풀 • 엔터프라이즈 매개 변수 • 엔터프라이즈 전화 구성 • 위치 • NTP(Network Time Protocol) 서버 • 플러그인 • SCCP(Skinny Call Control Protocol) 또는 SIP(Session Initiation Protocol)를 실행하는 전화기의 보안 프로파일, SIP 트렁크의 보안 프로파일 • SRST(Survivable Remote Site Telephony) 참조 • 서버 • 벌크 관리 도구에서 작업 스케줄러 창 보기 및 구성	표준 CCM 서버 유지 관리
표준 CCM 사용자 권한 관리	Cisco Unified Communications Manager 관리에서 애플리케이션 사용자를 보고 구성할 수 있습니다.	
표준 CCMADMIN 관리	CCMAdmin 시스템의 모든 기능에 액세스할 수 있습니다.	

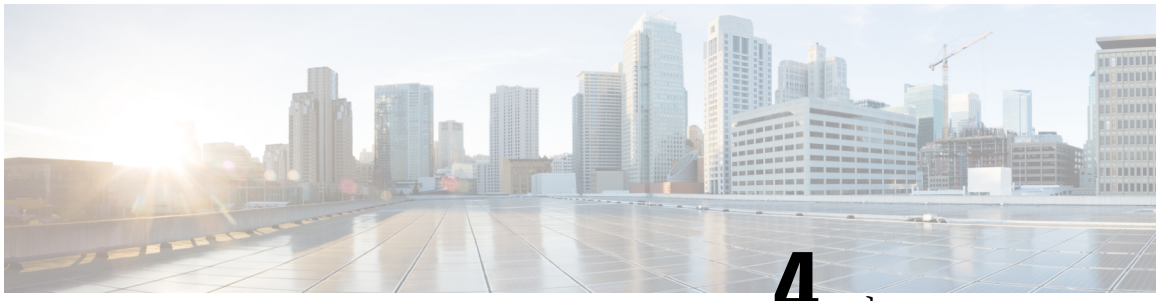
표준 역할	역할에 대한 권한/리소스	연결된 표준 액세스 제어 그룹
표준 CCMADMIN 관리	Cisco Unified Communications Manager 관리 및 벌크 관리 도구에서 모든 항목을 보고 구성할 수 있습니다.	표준 CCM 수퍼 사용자
표준 CCMADMIN 관리	Dialed Number Analyzer에서 정보를 보고 구성할 수 있습니다.	
표준 CCMADMIN 읽기 전용	모든 CCMAdmin 리소스에 읽기 액세스할 수 있습니다.	
표준 CCMADMIN 읽기 전용	Cisco Unified Communications Manager 관리 및 벌크 관리 도구에서 구성을 볼 수 있습니다.	표준 CCM 게이트웨이 관리, 표준 CCM 전화 관리, 표준 CCM 읽기 전용, 표준 CCM 서버 유지 관리, 표준 CCM 서버 모니터링
표준 CCMADMIN 읽기 전용	Dialed Number Analyzer에서 라우팅 구성을 분석할 수 있습니다.	
표준 CCMUSER 관리	Cisco Unified Communications 셀프 케어 포털에 액세스할 수 있습니다.	표준 CCM 최종 사용자
표준 CTI 통화 모니터링 허용	CTI 애플리케이션/장치에서 통화를 모니터링할 수 있습니다.	표준 CTI 통화 모니터링 허용
표준 CTI 통화 지정보류 모니터링 허용	CTI 애플리케이션/장치에서 통화 지정보류를 사용할 수 있습니다. 중요 열려 있는 회선 및 지정 보류 회선의 최대 수는 65000을 초과해서는 안 됩니다. 합계가 65000을 초과하는 경우 애플리케이션 사용자에서 표준 CTI 허용 통화 지정 보류 모니터링 역할을 제거하거나 구성된 지정 보류 회선 수를 줄이십시오.	표준 CTI 통화 지정보류 모니터링 허용
표준 CTI 통화 녹음 허용	CTI 애플리케이션/장치에서 통화를 녹음할 수 있습니다.	표준 CTI 통화 녹음 허용
표준 CTI 발신 번호 수정 허용	CTI 애플리케이션에서 통화 중 발신자 번호를 변환할 수 있습니다.	표준 CTI 발신 번호 수정 허용
표준 CTI 모든 디바이스 제어 허용	모든 CTI 제어 가능 장치 제어 허용	표준 CTI 모든 디바이스 제어 허용

표준 역할	역할에 대한 권한/리소스	연결된 표준 액세스 제어 그룹
연결된 Xfer 및 conf를 지원하는 전화의 표준 CTI 컨트롤 허용	호전환 연결 및 전화회의를 지원하는 모든 CTI 장치 제어 허용	연결된 Xfer 및 conf를 지원하는 전화의 표준 CTI 컨트롤 허용
표준 CTI 롤오버 모드를 지원하는 전화의 컨트롤 허용	롤오버 모드를 지원하는 모든 CTI 장치 컨트롤 허용	표준 CTI 롤오버 모드를 지원하는 전화의 컨트롤 허용
표준 CTI SRTP 키 자료 수신 허용	CTI 애플리케이션에서 SRTP 키 자료에 액세스하고 배포하도록 허용	표준 CTI SRTP 키 자료 수신 허용
표준 CTI 활성화	CTI 애플리케이션 컨트롤 활성화	표준 CTI 활성화
표준 CTI 보안 연결	Cisco Unified Communications Manager에 대한 보안 CTI 연결 활성화	표준 CTI 보안 연결
표준 CUReporting	애플리케이션 사용자가 다양한 소스에서 보고서를 생성하도록 허용	
표준 CUReporting	Cisco Unified Reporting에서 보고서 보기, 다운로드, 생성 및 업로드 허용	표준 CCM 관리 사용자, 표준 CCM 수퍼 사용자
표준 EM 인증 프록시 권한	애플리케이션용 Cisco Extension Mobility(EM) 인증 권한 관리, Cisco Extension Mobility와 상호 작용하는 모든 애플리케이션 필요(예: Cisco Unified Communications Manager Assistant 및 Cisco Web Dialer)	표준 CCM 수퍼 사용자, 표준 EM 인증 프록시 권한
표준 패킷 스니핑	Cisco Unified Communications Manager 관리에 액세스하여 패킷 스니핑(캡처)을 활성화할 수 있습니다.	표준 패킷 스니퍼 사용자

표준 역할	역할에 대한 권한/리소스	연결된 표준 액세스 제어 그룹
표준 RealtimeAndTraceCollection	Cisco 통합 서비스 가용성 및 실시간 모니터링 도구에 액세스하여 다음 항목을 보고 사용할 수 있습니다. • SOAP(Simple Object Access Protocol) 서비스 가용성 AXL API • SOAP 호출 레코드 API • SOAP 진단 포털(Analysis Manager) 데이터베이스 서비스 • 감사 로그 기능에 대한 추적 구성 • 추적 수집을 포함하여 실시간 모니터링 도구 구성	표준 RealtimeAndTraceCollection

표준 역할	역할에 대한 권한/리소스	연결된 표준 액세스 제어 그룹
표준 서비스 가용성	Cisco 통합 서비스 가용성 또는 실시간 모니터링 도구에서 다음 창을 보고 구성할 수 있습니다. • 알람 구성 및 알람 정의(Cisco 통합 서비스 가용성) • 감사 추적(읽기/보기 전용으로 표시됨) • SNMP 관련 창(Cisco 통합 서비스 가용성) • 추적 구성 및 추적 구성 문제 해결(Cisco 통합 서비스 가용성) • 로그 파티션 모니터링 • 경고 구성(RTMT), 프로파일 구성(RTMT) 및 추적 수집(RTMT) SOAP 서비스 가용성 AXL API, SOAP 통화 레코드 API 및 SOAP 진단 포털(Analysis Manager) 데이터베이스 서비스를 보고 사용할 수 있습니다. SOAP 통화 레코드 API의 경우 RTMT Analysis Manager 통화 레코드 권한은 이 리소스를 통해 제어됩니다. SOAP 진단 포털 데이터베이스 서비스의 경우 RTMT Analysis Manager 호스팅 데이터베이스 액세스는 이 리소스를 통해 제어됩니다.	표준 CCM 서버 모니터링, 표준 CCM 수퍼 사용자
표준 SERVICEABILITY 관리	서비스 가용성 관리자는 Cisco Unified Communications Manager 관리에서 플러그인 창에 액세스하여 이 창에서 플러그인을 다운로드할 수 있습니다.	
표준 SERVICEABILITY 관리	Dialed Number Analyzer에 대한 서비스 가용성의 모든 기능을 관리할 수 있습니다.	

표준 역할	역할에 대한 권한/리소스	연결된 표준 액세스 제어 그룹
표준 SERVICEABILITY 관리	Cisco 통합 서비스 가용성 또는 실시간 모니터링 도구에서 모든 창을 보고 구성할 수 있습니다. (감사 추적은 보기만 지원). 모든 SOAP 서비스 가용성 AXL API를 보고 사용할 수 있습니다.	
표준 서비스 가용성 읽기 전용	Dialed Number Analyzer에 있는 구성 요소에 대한 모든 서비스 가용성 관련 데이터를 볼 수 있습니다.	표준 CCM 읽기 전용
표준 서비스 가용성 읽기 전용	Cisco 통합 서비스 가용성 또는 실시간 모니터링 도구에서 구성을 볼 수 있습니다. (표준 감사 로그 관리 역할로 표시되는 감사 구성 창은 제외) 모든 SOAP 서비스 가용성 AXL API, SOAP 통화 레코드 API 및 SOAP 진단 포털(Analysis Manager) 데이터베이스 서비스를 볼 수 있습니다.	
표준 시스템 서비스 관리	Cisco 통합 서비스 가용성에서 서비스를 보고 활성화하고 시작하고 중지할 수 있습니다.	
표준 SSO 구성 관리	SAML SSO 구성의 모든 기능을 관리할 수 있습니다.	
표준 기밀 액세스 수준 사용자	모든 기밀 액세스 수준 페이지에 액세스할 수 있습니다.	표준 Cisco Call Manager 관리
표준 CCMADMIN 관리	CCMAdmin 시스템의 모든 기능을 관리할 수 있습니다.	표준 Cisco Unified CM IM and Presence 관리
표준 CCMADMIN 읽기 전용	모든 CCMAdmin 리소스에 읽기 액세스할 수 있습니다.	표준 Cisco Unified CM IM and Presence 관리
표준 CUReporting	애플리케이션 사용자가 다양한 소스에서 보고서를 생성하도록 허용	표준 Cisco Unified CM IM and Presence 보고



4 장

최종 사용자 관리

- 최종 사용자 개요, 41 페이지
- 최종 사용자 관리 작업, 41 페이지

최종 사용자 개요

실행 중인 시스템을 관리할 때 시스템에 구성된 최종 사용자의 목록을 업데이트해야 할 수 있습니다. 여기에는 다음 항목이 포함됩니다.

- 새 사용자 설정
- 새 최종 사용자를 위해 전화기 설정
- 최종 사용자에 대한 암호 또는 PIN 변경
- IM and Presence Service에 대해 최종 사용자 활성화

관리자는 Cisco Unified CM 관리의 최종 사용자 구성 창을 사용하여 Unified CM 최종 사용자에 대한 정보를 추가, 검색, 표시 및 유지 관리할 수 있습니다. 빠른 사용자/전화기 추가 창을 사용하여 새 최종 사용자를 신속하게 구성하고 해당 최종 사용자에 대해 새 전화기를 구성할 수도 있습니다.

최종 사용자 관리 작업

프로시저

	명령 또는 동작	목적
단계 **1**	사용자 템플릿 구성, 42 페이지	사용자 프로파일 또는 범용 회선과 장치 템플릿을 포함하는 기능 그룹 템플릿으로 시스템을 구성하지 않은 경우 다음 작업을 수행하여 설정합니다.

	명령 또는 동작	목적
		새 사용자 및 전화기를 신속하게 구성하려면 모든 새 최종 사용자에 이러한 템플릿을 적용할 수 있습니다.
단계 **2**	다음 방법 중 하나를 사용하여 새 최종 사용자 추가 • LDAP에서 최종 사용자 가져오기, 47 페이지 • 최종 사용자를 수동으로 추가, 47 페이지	시스템이 회사 LDAP 디렉터리와 동기화하도록 구성했고 동기화된 경우 LDAP 디렉터리에서 새 최종 사용자를 직접 가져올 수 있습니다. 그렇지 않으면, 최종 사용자를 수동으로 추가 및 구성할 수 있습니다.
단계 **3**	다음 작업 중 하나를 수행하여 전화기를 새 사용자 또는 기존의 최종 사용자에게 할당합니다. • 최종 사용자를 위한 새 전화기 추가 , 49 페이지 • 최종 사용자에게 기존 전화기 이동, 49 페이지	범용 디바이스 템플릿의 설정을 사용하여 최종 사용자에 대한 새 전화기를 구성하기 위해 '새 전화기 추가' 절차를 사용할 수 있습니다. 또한 이미 구성된 기존 전화기를 할당하려면 '이동' 절차를 사용할 수 있습니다.
단계 **4**	최종 사용자 PIN 변경, 50 페이지	(선택 사항) Cisco Unified Communications Manager 관리에서 최종 사용자에 대한 PIN을 변경합니다.
단계 **5**	최종 사용자 암호 변경, 50 페이지	(선택 사항) Cisco Unified Communications Manager 관리에서 최종 사용자에 대한 암호를 변경합니다.
단계 **6**	Cisco Unity Connection 음성 사서함 생성, 51 페이지	(선택 사항) Cisco Unified Communications Manager 관리에서 개별 Cisco Unity Connection 음성 사서함을 생성합니다.

사용자 템플릿 구성

사용자 프로파일 및 기능 그룹 템플릿을 설정하려면 다음 작업을 수행합니다. 새 최종 사용자를 추가할 때 회선 및 장치 설정을 사용하여 신속하게 최종 사용자에 대한 전화기를 구성할 수 있습니다.

프로시저

	명령 또는 동작	목적
단계 **1**	범용 회선 템플릿 구성, 43 페이지	일반적으로 디렉터리 번호에 적용되는 공통 설정을 사용하여 범용 회선 템플릿을 구성합니다.

	명령 또는 동작	목적
단계 **2**	범용 장치 템플릿 구성, 44 페이지	일반적으로 전화기에 적용되는 공통 설정을 사용하여 범용 장치 템플릿을 구성합니다.
단계 **3**	사용자 프로파일 구성, 44 페이지	사용자 프로파일에 범용 회선 및 범용 장치 템플릿을 할당합니다. 셀프 프로비저닝 기능이 구성된 경우 이 프로파일을 사용하는 사용자에 대해 셀프 프로비저닝을 활성화할 수 있습니다.
단계 **4**	기능 그룹 템플릿 구성, 46 페이지	사용자 프로파일을 기능 그룹 템플릿에 할당합니다. LDAP 동기화된 사용자의 경우 기능 그룹 템플릿은 사용자 프로파일을 최종 사용자에게 연결합니다.

범용 회선 템플릿 구성

범용 회선 템플릿을 사용하면 새로 할당된 디렉터리 번호에 일반 설정을 쉽게 적용할 수 있습니다. 서로 다른 사용자 그룹의 요구 사항을 충족하도록 서로 다른 템플릿을 구성합니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 사용자 관리 > 사용자/전화기 추가 > 범용 회선 템플릿을 선택합니다.

단계 **2** 새로 추가를 클릭합니다.

단계 **3** 범용 회선 템플릿 구성 창에서 필드를 구성합니다. 필드 및 해당 구성 옵션에 대한 자세한 내용은 온라인 도움말을 참조하십시오.

단계 **4** 대체 번호를 사용하여 전역 다이얼 플랜 복제를 배포하는 경우 엔터프라이즈 대체 번호와 **+E.164** 대체 번호 섹션을 확장하고 다음을 수행합니다.

a) 엔터프라이즈 대체 번호 추가 버튼 및/또는 **+E.164** 대체 번호 추가 버튼을 클릭합니다.

b) 대체 번호에 할당하는 데 사용할 번호 마스크를 추가합니다. 예를 들어, 4자리 내선 번호는 5XXXX를 엔터프라이즈 번호 마스크로 사용하고 1972555XXXX를 +E.164 대체 번호 마스크로 사용할 수 있습니다.

c) 대체 번호를 할당할 파티션을 할당합니다.

d) ILS를 통해 이 번호를 광고하려면 **ILS**를 통해 전역으로 광고 확인란에 체크 표시합니다. 광고된 패턴을 사용하여 대체 번호 범위를 요약하는 경우 개별 대체 번호를 광고할 필요가 없습니다.

e) **PSTN** 페일오버 섹션을 확장하고 일반 콜 라우팅이 실패하는 경우 사용할 PSTN 페일오버으로 엔터프라이즈 번호 또는 **+E.164** 대체 번호를 선택합니다.

단계 **5** 저장을 클릭합니다.

다음에 수행할 작업

범용 장치 템플릿 구성, 44 페이지

범용 장치 템플릿 구성

범용 디바이스 템플릿을 사용하면 구성 설정을 새로 프로비저닝된 디바이스에 쉽게 적용할 수 있습니다. 프로비저닝된 디바이스는 범용 디바이스 템플릿의 설정을 사용합니다. 서로 다른 사용자 그룹의 요구 사항을 충족하도록 서로 다른 디바이스 템플릿을 구성할 수 있습니다. 이 템플릿에 구성한 프로파일을 할당할 수도 있습니다.

시작하기 전에

범용 회선 템플릿 구성, 43 페이지

프로시저

단계 **1** Cisco Unified CM 관리에서 사용자 관리 > 사용자/전화기 추가 > 범용 디바이스 템플릿을 선택합니다.

단계 **2** 새로 추가를 클릭합니다.

단계 **3** 필수 필드인

a) 템플릿에 대한 디바이스 설명을 입력합니다.
b) 드롭다운 목록에서 디바이스 풀을 선택합니다.
c) 드롭다운 목록에서 디바이스 보안 프로파일을 선택합니다.
d) 드롭다운 목록에서 **SIP** 프로파일을 선택합니다.
e) 드롭다운 목록에서 전화기 버튼 템플릿을 선택합니다.

단계 **4** 범용 디바이스 템플릿 구성 창에서 나머지 필드를 완성합니다. 필드 설명은 온라인 도움말을 참조하십시오.

단계 **5** 전화기 설정 아래에서 다음 옵션 필드를 완성합니다.

a) 일반 전화기 프로파일을 구성한 경우 프로파일을 할당합니다.
b) 일반 디바이스 구성을 구성한 경우 구성을 할당합니다.
c) 기능 제어 정책을 구성한 경우 정책을 할당합니다.

단계 **6** 저장을 클릭합니다.

다음에 수행할 작업

사용자 프로파일 구성, 44 페이지

사용자 프로파일 구성

사용자 프로파일을 통해 범용 회선 및 범용 디바이스 템플릿을 사용자에게 할당합니다. 서로 다른 사용자 그룹에 대한 여러 사용자 프로파일을 구성합니다. 이 서비스 프로파일을 사용하는 사용자에 대한 셀프 프로비저닝을 활성화할 수도 있습니다.

시작하기 전에

범용 장치 템플릿 구성, 44 페이지

프로시저

단계 **1** Cisco Unified CM 관리에서 다음 메뉴를 선택합니다.사용자 관리 > 사용자 설정 > 사용자 프로파일.

단계 **2** 새로 추가를 클릭합니다.

단계 **3** 사용자 프로파일의 이름 및 설명을 입력합니다.

단계 **4** 사용자의 데스크폰, 모바일 및 데스크탑 디바이스 및 원격 대상/디바이스 프로파일에 적용할 유니버셜 디바이스 템플릿을 할당합니다.

단계 **5** 이 사용자 프로파일의 사용자에 대한 전화 회선에 적용할 범용 회선 템플릿을 할당합니다.

단계 **6** 이 사용자 프로파일의 사용자가 자신의 전화기를 프로비저닝하는 데 셀프 프로비저닝 기능을 사용할 있도록하려면 다음을 수행합니다.

a) 최종 사용자에게 자신의 전화기 프로비저닝 허용 확인란을 선택합니다.

b) 최종 사용자가 이렇게 많은 전화기를 가지고 있으면 프로비저닝 제한 필드에 사용자가 프로비저닝하도록 허용되는 전화기의 최대 수를 입력합니다. 최대값은 20입니다.

c) 다른 엔드 유저에게 이미 할당된 전화의 프로비저닝 허용 확인란에 체크 표시하여 이 프로파일에 연결된 사용자에게 이미 다른 사용자가 소유하는 디바이스를 마이그레이션 또는 재할당할 권한이 있는지 여부를 결정합니다. 기본값으로 이 확인란은 선택되어 있지 않습니다.

단계 **7** 이 사용자 프로파일과 연결된 Cisco Jabber 사용자가 모바일 및 원격 액세스 기능을 사용할 수 있도록하려면 모바일 및 원격 액세스 활성화 확인란에 체크 표시합니다.

참고
- 기본적으로 이 확인란은 선택되어 있습니다. 이 확인란의 체크 표시를 취소하면 클라이언트 정책 섹션이 비활성화되고 기본값으로 서비스 클라이언트 없음 정책 옵션이 선택됩니다.
- 이 설정은 OAuth 새로 고침 로그인을 사용하는 Cisco Jabber 사용자의 경우에만 필수입니다. 비 Jabber 사용자는 이 설정이 없어도 모바일 및 원격 액세스를 사용할 수 있습니다. 모바일 및 원격 액세스 기능은 Jabber 모바일 및 원격 액세스 사용자에 대해서만 적용 가능하며, 다른 엔드포인트 또는 클라이언트에게는 적용되지 않습니다.

단계 **8** 이 사용자 프로파일에 대해 Jabber 정책을 할당합니다. 데스크톱 클라이언트 정책 및 모바일 클라이언트 정책 드롭다운 목록에서 다음 옵션 중 하나를 선택합니다.

- 서비스 없음 - 이 정책은 모든 Cisco Jabber 서비스에 대한 액세스를 비활성화합니다.
- IM & 프레즌스만 해당—이 정책은 인스턴트 메시징 및 프레즌스 기능을 활성화합니다.
- IM & 프레즌스, 음성 및 영상 통화—이 정책은 음성 또는 영상 디바이스가 있는 모든 사용자에 대해 인스턴트 메시징, 프레즌스, 음성 메일 및 전화 회의 기능을 활성화합니다. 이것이 기본 옵션입니다.

참고 Jabber 데스크톱 클라이언트는 Windows용 Cisco Jabber와 Mac용 Cisco Jabber 사용자를 포함합니다. Jabber 모바일 클라이언트는 iPad 및 iPhone용 Cisco Jabber 사용자와 Android용 Cisco Jabber 사용자를 포함합니다.

단계 **9** 사용자가 Unified Communications 셀프 서비스 포털을 통해 내선 이동 또는 인터클러스터 내선 이동에 대한 최대 로그인 시간을 설정하도록 허용하려면 엔드 유저가 내선 이동을 최대 로그인 시간을 설정하도록 허용 확인란에 체크 표시합니다.

참고 기본적으로 최종 사용자가 **Extension Mobility**를 최대 로그인 시간을 설정하도록 허용 확인란은 선택 해제되어 있습니다.

단계 **10** 저장을 클릭합니다.

다음에 수행할 작업

기능 그룹 템플릿 구성, 46 페이지

기능 그룹 템플릿 구성

기능 그룹 템플릿은 프로비저닝된 사용자를 위해 전화기, 회선 및 기능을 신속하게 구성하도록 도와 시스템 구축을 지원합니다. 회사 LDAP 디렉터리에서 사용자를 동기화하는 경우 사용자가 디렉터리에서 동기화할 사용자 프로파일 및 서비스 프로파일을 사용하여 기능 그룹 템플릿을 구성합니다. 이 템플릿을 통해 동기화된 사용자에 대한 IM and Presence Service를 활성화할 수도 있습니다.

프로시저

단계 **1** [Cisco Unified CM 관리]에서 사용자 관리 > 사용자/전화기 추가 > 기능 그룹 템플릿을 선택합니다.

단계 **2** 새로 추가를 클릭합니다.

단계 **3** 기능 그룹 템플릿에 대한 이름 및 설명을 입력합니다.

단계 **4** 이 템플릿을 사용하는 모든 사용자에 대해 로컬 클러스터를 홈 클러스터로 사용하려는 경우 홈 클러스터 확인란을 선택합니다.

단계 **5** 이 템플릿을 사용하는 사용자가 인스턴트 메시징 및 프레전스 정보를 교환하도록 하려면 **Unified CM IM and Presence**에 대해 사용자 활성화 확인란을 선택합니다.

단계 **6** 드롭다운 목록에서 서비스 프로파일 및 사용자 프로파일을 선택합니다.

단계 **7** 기능 그룹 템플릿 구성 창에서 나머지 필드를 완성합니다. 필드 설명은 온라인 도움말을 참조하십시오.

단계 **8** 저장을 클릭합니다.

다음에 수행할 작업

새 최종 사용자를 추가합니다. 시스템이 회사 LDAP 디렉터리와 통합된 경우 LDAP 디렉터리에서 사용자를 직접 가져올 수 있습니다. 그렇지 않으면 수동으로 최종 사용자를 만듭니다.

- LDAP에서 최종 사용자 가져오기, 47 페이지
- 최종 사용자를 수동으로 추가, 47 페이지

LDAP에서 최종 사용자 가져오기

새 최종 사용자를 회사 LDAP 디렉터리에서 수동으로 가져오려면 다음 절차를 수행합니다. LDAP 동기화 구성에 범용 회선 템플릿 및 디바이스 템플릿은 물론 DN 풀을 포함하는 기능 그룹 템플릿이 포함된 경우 가져오기 프로세스는 최종 사용자 및 기본 내선 번호를 자동으로 구성합니다.

참고 초기 동기화가 발생한 후에는 새 구성(예: 기능 그룹 템플릿 추가)을 LDAP 디렉터리 동기화에 추가할 수 없습니다. 기존 LDAP 동기화를 편집하려면 벌크 관리를 사용하거나 새 LDAP 동기화를 구성해야 합니다.

시작하기 전에

이 절차를 시작하기 전에 Cisco Unified Communications Manager가 회사 LDAP 디렉터리와 이미 동기화되었는지 확인하십시오. LDAP 동기화는 범용 회선 템플릿 및 디바이스 템플릿이 있는 기능 그룹 템플릿을 포함해야 합니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 시스템 > **LDAP** > **LDAP** 디렉터리를 선택합니다.

단계 **2** 찾기를 클릭하고 사용자가 추가한 LDAP 디렉터리를 선택합니다.

단계 **3** 전체 동기화 수행을 클릭합니다.
Cisco Unified Communications Manager는 외부 LDAP 디렉터리와 동기화합니다. LDAP 디렉터리에 있는 새 최종 사용자를 Cisco Unified Communications Manager 데이터베이스로 가져옵니다.

다음에 수행할 작업

셀프 프로비저닝을 위해 사용자가 활성화된 경우 최종 사용자는 셀프 프로비저닝 대화형 음성 응답(IVR)을 사용하여 새 전화기를 프로비저닝할 수 있습니다. 그렇지 않으면 다음 작업 중 하나를 수행하여 전화기를 최종 사용자에게 할당합니다.

- 최종 사용자를 위한 새 전화기 추가 , 49 페이지
- 최종 사용자에게 기존 전화기 이동, 49 페이지

최종 사용자를 수동으로 추가

새 최종 사용자를 추가하고 액세스 컨트롤 그룹 및 기본 회선 내선 번호로 해당 최종 사용자를 구성하려면 다음 절차를 수행합니다.

참고 사용자에게 할당할 역할 권한이 있는 액세스 컨트롤 그룹을 이미 설정했는지 확인합니다. 자세한 내용은 "사용자 액세스 관리" 장을 참조하십시오.

시작하기 전에

범용 회선 템플릿이 포함되어 있는 사용자 프로파일이 구성되었는지 확인합니다. 새 내선 번호를 구성해야 하는 경우 Cisco Unified Communications Manager는 범용 회선 템플릿의 설정을 사용하여 기본 내선 번호를 구성합니다.

프로시저

단계 **1** [Cisco Unified CM 관리]에서 사용자 관리 > 사용자/전화기 추가 > 빠른 사용자/전화기 추가를 선택합니다.

단계 **2** 사용자 **ID** 및 성을 입력합니다.

단계 **3** 기능 그룹 템플릿 드롭다운 목록에서 기능 그룹 템플릿을 선택합니다.

단계 **4** 저장을 클릭합니다.

단계 **5** 사용자 프로파일 드롭다운 목록에서 선택한 사용자 프로파일에 범용 회선 템플릿이 포함되어 있는지 확인합니다.

단계 **6** 액세스 컨트롤 그룹 구성원 섹션에서 + 아이콘을 클릭합니다.

단계 **7** 사용자는 다음의 구성원입니다**.** 드롭다운 목록에서 액세스 컨트롤 그룹을 선택합니다.

단계 **8** 기본 내선 번호 아래에서 + 아이콘을 클릭합니다.

단계 **9** 내선 번호 드롭다운 목록에서 **(**사용 가능**)**으로 표시되는 DN을 선택합니다.

단계 **10** 모든 회선 내선 번호가 **(**사용됨**)**으로 표시되는 경우 다음 단계를 수행합니다.

a) 새로 만들기**...** 버튼을 클릭합니다.
새 내선 번호 추가 팝업이 표시됩니다.
b) 디렉터리 번호 필드에 새 회선 내선 번호를 입력합니다.
c) 회선 템플릿 드롭다운 목록에서 범용 회선 템플릿을 선택합니다.
d) 확인을 클릭합니다.
Cisco Unified Communications Manager는 범용 디바이스 템플릿의 설정을 사용하여 전화기를 구성합니다.

단계 **11** (선택 사항) 빠른 사용자/전화기 추가 구성 창에서 추가 필드를 완료합니다.

단계 **12** 저장을 클릭합니다.

다음에 수행할 작업

다음 절차 중 하나를 수행하여 전화기를 이 최종 사용자에게 할당합니다.

- 최종 사용자를 위한 새 전화기 추가 , 49 페이지

- 최종 사용자에게 기존 전화기 이동, 49 페이지

최종 사용자를 위한 새 전화기 추가

신규 또는 기존 최종 사용자에 대해 새 전화기를 추가하려면 다음 절차를 수행합니다. 최종 사용자에 대한 사용자 프로파일에 범용 디바이스 템플릿이 포함되어 있는지 확인합니다. Cisco Unified Communications Manager는 범용 디바이스 템플릿의 설정을 사용하여 전화기를 구성합니다.

시작하기 전에

최종 사용자를 추가하려면 다음 절차 중 하나를 수행합니다.

- 최종 사용자를 수동으로 추가, 47 페이지
- LDAP에서 최종 사용자 가져오기, 47 페이지

프로시저

단계 **1** Cisco Unified CM 관리에서 사용자 관리 > 사용자/전화기 추가 > 빠른 사용자/전화기 추가를 선택합니다.

단계 **2** 찾기를 클릭하고 새 전화기를 추가하려는 최종 사용자를 선택합니다.

단계 **3** 디바이스 관리를 클릭합니다.
[디바이스 관리] 창이 나타납니다.

단계 **4** 새 전화기 추가를 클릭합니다.
[사용자에게 전화기 추가] 팝업이 표시됩니다.

단계 **5** 제품 유형 드롭다운 목록에서 전화기 모델을 선택합니다.

단계 **6** 디바이스 프로토콜 드롭다운에서 프로토콜로 SIP 또는 SCCP를 선택합니다.

단계 **7** 디바이스 이름 텍스트 상자에 디바이스 MAC 주소를 입력합니다.

단계 **8** 범용 디바이스 템플릿 드롭다운 목록에서 범용 디바이스 템플릿을 선택합니다.

단계 **9** 전화기가 확장 모듈을 지원하는 경우 배포하려는 확장 모듈 수를 입력합니다.

단계 **10** Extension Mobility를 사용하여 전화에 액세스하려면 **Extension Mobility**에서 확인란을 선택합니다.

단계 **11** 전화기 추가를 클릭합니다.
[새 전화기 추가] 팝업이 닫힙니다. Cisco Unified Communications Manager는 사용자에게 전화기를 추가하고 범용 디바이스 템플릿을 사용하여 전화기를 구성합니다.

단계 **12** 전화기 구성을 추가 편집하려면 해당 연필 아이콘을 클릭하여 전화기 구성 창에서 전화기를 엽니다.

최종 사용자에게 기존 전화기 이동

기존 전화기를 새 사용자 또는 기존 최종 사용자에게 이동하려면 이 절차를 수행합니다.

프로시저

단계 **1** [Cisco Unified CM 관리]에서 사용자 관리 > 사용자/전화기 추가 > 빠른/사용자 전화기 추가를 선택합니다.

단계 **2** 찾기를 클릭하고 기존 전화기를 이동할 사용자를 선택합니다.

단계 **3** 디바이스 관리 버튼을 클릭합니다.

단계 **4** 이 사용자로 이동할 전화기 찾기 버튼을 클릭합니다.

단계 **5** 이 사용자로 이동하려는 전화기를 선택합니다.

단계 **6** 선택 항목 이동을 클릭합니다.

최종 사용자 PIN 변경

프로시저

단계 **1** Cisco Unified Communications Manager 관리에서 사용자 관리 > 최종 사용자를 선택합니다.
사용자 찾기 및 나열 창이 표시됩니다.

단계 **2** 기존 사용자를 선택하려면 사용자 찾기 위치 필드에 적절한 필터를 지정하고 찾기를 선택하여 사용자 목록을 가져온 다음 목록에서 사용자를 선택합니다.
최종 사용자 구성 창이 표시됩니다.

단계 **3** **PIN** 필드에서 암호화된 기존의 PIN을 두 번 클릭하고 새 PIN을 입력합니다. 할당된 자격 증명 정책에 지정된 최소 문자 수(1~127자) 이상을 입력해야 합니다.

단계 **4** **PIN** 확인 필드에서 기존의 암호화된 PIN을 두 번 클릭하고 새 PIN을 다시 입력합니다.

단계 **5** 저장을 클릭합니다.

참고 애플리케이션 서버 구성 창에서 최종 사용자 **PIN** 동기화 Cisco Unity Connection의 확인란이 활성화된 경우 Extension Mobility, 지금 전화회의, Mobile Connect 및 Cisco Unity Connection 음성 메일에 동일한 최종 사용자 PIN을 사용하여 로그인할 수 있습니다. 최종 사용자는 동일한 PIN을 사용하여 Extension Mobility에 로그인하고 음성 메일에 액세스할 수 있습니다.

최종 사용자 암호 변경

LDAP 인증이 활성화된 경우에는 최종 사용자 암호를 변경할 수 없습니다.

프로시저

단계 **1** Cisco Unified Communications Manager 관리에서 사용자 관리 > 최종 사용자를 선택합니다.

사용자 찾기 및 나열 창이 표시됩니다.

단계 **2** 기존 사용자를 선택하려면 사용자 찾기 위치 필드에 적절한 필터를 지정하고 찾기를 선택하여 사용자 목록을 가져온 다음 목록에서 사용자를 선택합니다.
최종 사용자 구성 창이 표시됩니다.

단계 **3** 암호 필드에서 암호화되어 있는 기존 암호를 두 번 클릭하고 새 암호를 입력합니다. 할당된 자격 증명 정책에 지정된 최소 문자 수(1~127자) 이상을 입력해야 합니다.

단계 **4** 암호 확인 필드에서 암호화되어 있는 기존 암호를 두 번 클릭하고 새 암호를 다시 입력합니다.

단계 **5** 저장을 클릭합니다.

Cisco Unity Connection 음성 사서함 생성

시작하기 전에

- 음성 메시징을 위해 Cisco Unified Communications Manager를 구성해야 합니다. Cisco Unity Connection을 사용하도록 Cisco Unified Communications Manager를 구성하는 자세한 내용은 다음 위치에서 *Cisco Unified Communications Manager* 시스템 구성 설명서를 참조하십시오.

  http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html

- 장치 및 기본 내선 번호를 최종 사용자와 연결해야 합니다.

- 이 섹션에 설명된 절차를 수행하는 대신에 Cisco Unity Connection에 제공되는 가져오기 기능을 사용할 수 있습니다. 가져오기 기능을 사용하는 방법에 대한 자세한 내용은 *Cisco Unity Connection* 관련 사용자 이동, 추가 및 변경 설명서를 참조하십시오.

프로시저

단계 **1** Cisco Unified Communications Manager 관리에서 사용자 관리 > 최종 사용자를 선택합니다.
사용자 찾기 및 나열 창이 표시됩니다.

단계 **2** 기존 사용자를 선택하려면 사용자 찾기 위치 필드에 적절한 필터를 지정하고 찾기를 선택하여 사용자 목록을 가져온 다음 목록에서 사용자를 선택합니다.
최종 사용자 구성 창이 표시됩니다.

단계 **3** 기본 내선 번호가 이 사용자와 연결되어 있는지 확인합니다.

참고 기본 내선을 정의해야 합니다. 그렇지 않으면 [Cisco Unity 사용자 생성] 링크가 관련 링크 드롭다운 목록 상자에 표시되지 않습니다.

단계 **4** 관련 링크 드롭다운 목록에서 [Cisco Unity 애플리케이션 사용자 생성] 링크를 선택하고 이동을 클릭합니다.

[Cisco Unity 사용자 추가] 대화 상자가 표시됩니다.

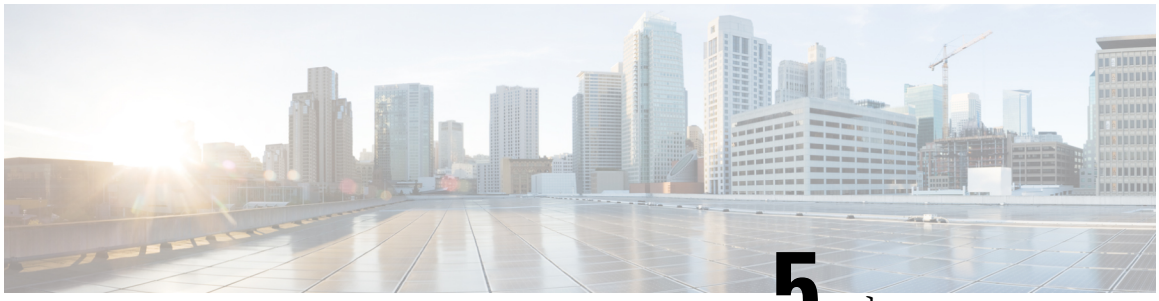
단계 **5** **Application Server** 드롭다운 목록 상자에서 Cisco Unity Connection 사용자를 생성할 Cisco Unity Connection 서버를 선택하고 다음을 클릭합니다.

단계 **6** 가입자 템플릿 드롭다운 목록 상자에서 사용할 가입자 템플릿을 선택합니다.

단계 **7** 저장을 클릭합니다.

사서함이 생성됩니다. 최종 사용자 구성 창의 관련 링크 드롭다운 목록 상자에 있는 링크가 Cisco Unity 사용자 편집으로 변경됩니다. 이제 Cisco Unity Connection 관리에서 생성한 사용자를 볼 수 있습니다.

참고 Cisco Unity Connection 사용자를 Cisco Unified Communications Manager 최종 사용자와 통합한 후에는 Cisco Unity Connection 관리에서 [별칭](Cisco Unified CM 관리에서는 [사용자 ID]), [이름], [성] 및 [내선](Cisco Unified CM 관리에서는 [기본 내선]) 같은 필드를 편집할 수 없습니다. 이러한 필드는 Cisco Unified CM 관리에서만 업데이트할 수 있습니다.



5 장

애플리케이션 사용자 관리

- 애플리케이션 사용자 개요, 53 페이지
- 애플리케이션 사용자 작업 흐름, 54 페이지

애플리케이션 사용자 개요

관리자는 Cisco Unified CM 관리의 애플리케이션 사용자 구성 창에서 Cisco Unified Communications Manager 애플리케이션 사용자에 대한 정보를 추가, 검색, 표시 및 유지 관리할 수 있습니다.

Cisco Unified CM 관리에는 기본적으로 다음 애플리케이션 사용자가 포함됩니다.

- CCMAdministrator
- CCMSysUser
- CCMQRTSecureSysUser
- CCMQRTSysUser
- IPMASecureSysUser
- IPMASysUser
- WDSecureSysUser
- WDSysUser
- TabSyncSysUser
- CUCService

참고 표준 CCM 수퍼 사용자 그룹의 관리자 사용자는 애플리케이션 중 하나에 대해 SSO(Single Sign-On)를 사용하여 Cisco Unified Communications Manager Administration, Cisco 통합 서비스 가용성 및 Cisco Unified Reporting에 액세스할 수 있습니다.

애플리케이션 사용자 작업 흐름

프로시저

	명령 또는 동작	목적
단계 **1**	새 애플리케이션 사용자 추가, 54 페이지	새 애플리케이션 사용자 추가
단계 **2**	애플리케이션 사용자와 장치 연결, 55 페이지	애플리케이션 사용자와 연결할 장치를 할당합니다.
단계 **3**	Cisco Unity 또는 Cisco Unity Connection에 관리자 사용자 추가, 55 페이지	Cisco Unity 또는 Cisco Unity Connection에 관리자 사용자로 사용자를 추가합니다. Cisco Unified CM 관리에서 애플리케이션 사용자를 구성하고 나서 Cisco Unity 또는 Cisco Unity Connection 관리에서 사용자에 대한 추가 설정을 구성할 수 있습니다.
단계 **4**	애플리케이션 사용자 암호 변경, 56 페이지	애플리케이션 사용자 암호를 변경합니다.
단계 **5**	애플리케이션 사용자 암호 인증서 정보 관리, 57 페이지	인증서 정보(예: 연관된 인증 규칙, 연관된 인증 정책 또는 애플리케이션 사용자가 마지막으로 암호를 변경한 시간)를 변경하거나 확인합니다.

새 애플리케이션 사용자 추가

프로시저

단계 **1** Cisco Unified CM 관리에서 사용자 관리 > 애플리케이션 사용자를 선택합니다.

단계 **2** 새로 추가를 클릭합니다.

단계 **3** 애플리케이션 사용자 구성 창에서 필드를 구성합니다. 필드 및 해당 구성 옵션에 대한 내용은 온라인 도움말을 참조하십시오.

단계 **4** 저장을 클릭합니다.

다음에 수행할 작업

애플리케이션 사용자와 장치 연결, 55 페이지

애플리케이션 사용자와 장치 연결

프로시저

단계 **1** Cisco Unified CM 관리에서 사용자 관리 > 애플리케이션 사용자를 선택합니다.
사용자 찾기 및 나열 창이 표시됩니다.

단계 **2** 기존 사용자를 선택하려면 사용자 찾기 위치 필드에 적절한 필터를 지정하고 찾기를 선택하여 사용자 목록을 가져온 다음 목록에서 사용자를 선택합니다.

단계 **3** 사용 가능한 장치 목록에서 애플리케이션 사용자와 연결할 장치를 선택하고 목록 아래의 아래쪽 화살표를 클릭합니다. 선택한 장치가 제어된 장치 목록으로 이동합니다.

참고 사용 가능한 장치 목록을 제한하려면 다음과 같이 추가 전화기 찾기 또는 추가 경로 포인트 찾기 버튼을 클릭합니다.

단계 **4** 추가 전화기 찾기 버튼을 클릭하면 전화기 찾기 및 나열 창이 표시됩니다. 검색을 수행하여 이 애플리케이션 사용자와 연결할 전화기를 찾습니다.

애플리케이션 사용자에게 할당할 각 장치에 대해 위 단계를 반복합니다.

단계 **5** 추가 경로 포인트 찾기 버튼을 클릭하면 **CTI** 경로 포인트 찾기 및 나열 창이 표시됩니다. 검색을 수행하여 이 애플리케이션 사용자와 연결할 CTI 경로 포인트를 찾습니다.

애플리케이션 사용자에게 할당할 각 장치에 대해 위 단계를 반복합니다.

단계 **6** 저장을 클릭합니다.

Cisco Unity 또는 Cisco Unity Connection에 관리자 사용자 추가

Cisco Unified Communications Manager를 Cisco Unity Connection 7.x 이상에 통합하려는 경우 이 섹션에 설명된 절차를 수행하는 대신에 Cisco Unity Connection 7.x 이상에 제공되는 가져오기 기능을 사용할 수 있습니다. 가져오기 기능을 사용하는 방법에 대한 자세한 내용은 다음 위치에서 Cisco Unity Connection 7.x 이상 관련 사용자 이동, 추가 및 변경 설명서를 참조하십시오.

http://www.cisco.com/c/en/us/support/unified-communications/unity-connection/products-maintenance-guides-list.html.

Cisco Unity 또는 Cisco Unity Connection 사용자를 Cisco Unified CM 애플리케이션 사용자와 통합할 때 필드를 편집할 수 없습니다. 이러한 필드는 Cisco Unified Communications Manager 관리에서만 업데이트할 수 있습니다.

Cisco Unity 및 Cisco Unity Connection은 Cisco Unified Communications Manager 데이터의 동기화를 모니터링합니다. Cisco Unity 관리 또는 Cisco Unity Connection 관리의 [도구] 메뉴에서 동기화 시간을 구성할 수 있습니다.

시작하기 전에

Cisco Unity 또는 Cisco Unity Connection에 추가할 사용자에게 적합한 템플릿을 정의했는지 확인합니다.

해당하는 Cisco Unity 또는 Cisco Unity Connection 소프트웨어를 설치하고 구성하는 경우에만 **Cisco** 사용자 생성 링크가 표시됩니다. 다음 위치에서 해당되는 Cisco Unity 관련 *Cisco Unified Communications Manager* 통합 설명서 또는 해당되는 Cisco Unity Connection 관련 *Cisco Unified Communications Manager SCCP* 통합 설명서를 참조하십시오.

http://www.cisco.com/c/en/us/support/unified-communications/unity-connection/products-installation-and-configuration-guides-list.html.

프로시저

단계 **1** Cisco Unified CM 관리에서 사용자 관리 > 애플리케이션 사용자를 선택합니다.

단계 **2** 기존 사용자를 선택하려면 사용자 찾기 위치 필드에 적절한 필터를 지정하고 찾기를 선택하여 사용자 목록을 가져온 다음 목록에서 사용자를 선택합니다.

단계 **3** 관련 링크 드롭다운 목록에서 **Cisco Unity** 애플리케이션 사용자 생성 링크를 선택하고 이동을 클릭합니다.
Cisco Unity 사용자 추가 대화 상자가 표시됩니다.

단계 **4** 애플리케이션 서버 드롭다운 목록에서 Cisco Unity 또는 Cisco Unity Connection 사용자를 생성할 Cisco Unity 또는 Cisco Unity Connection 서버를 선택하고 다음을 클릭합니다.

단계 **5** 애플리케이션 사용자 템플릿 드롭다운 목록에서 사용할 템플릿을 선택합니다.

단계 **6** 저장을 클릭합니다.
Cisco Unity 또는 Cisco Unity Connection에 관리자 계정이 생성됩니다. 애플리케이션 사용자 구성 창에서 [관련 링크]의 링크가 **Cisco** 사용자 편집으로 변경됩니다. 이제 Cisco Unity 관리 또는 Cisco Unity Connection 관리에서 생성한 사용자를 볼 수 있습니다.

애플리케이션 사용자 암호 변경

프로시저

단계 **1** Cisco Unified CM 관리에서 사용자 관리 > 애플리케이션 사용자를 선택합니다.
사용자 찾기 및 나열 창이 표시됩니다.

단계 **2** 기존 사용자를 선택하려면 사용자 찾기 위치 필드에 적절한 필터를 지정하고 찾기를 선택하여 사용자 목록을 가져온 다음 목록에서 사용자를 선택합니다.
애플리케이션 사용자 구성 창에 선택한 애플리케이션 사용자에 대한 정보가 표시됩니다.

단계 **3** 암호 필드에서 기존의 암호화된 암호를 두 번 클릭하고 새 암호를 입력합니다.

단계 **4** 암호 확인 필드에서 암호화되어 있는 기존 암호를 두 번 클릭하고 새 암호를 다시 입력합니다.

단계 **5** 저장을 클릭합니다.

애플리케이션 사용자 암호 인증서 정보 관리

애플리케이션 사용자 암호에 대한 인증서 정보를 관리하려면 다음 절차를 수행합니다. 암호 잠금, 암호에 인증 정책 적용 또는 마지막으로 실패한 로그인 시도 시간과 같은 정보 보기 등의 관리 작업을 수행할 수 있습니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 사용자 관리 > 애플리케이션 사용자를 선택합니다.
사용자 찾기 및 나열 창이 표시됩니다.

단계 **2** 기존 사용자를 선택하려면 사용자 찾기 위치 필드에 적절한 필터를 지정하고 찾기를 선택하여 사용자 목록을 가져온 다음 목록에서 사용자를 선택합니다.
애플리케이션 사용자 구성 창에 선택한 애플리케이션 사용자에 대한 정보가 표시됩니다.

단계 **3** 암호 정보를 변경 또는 확인하려면 암호 필드 옆에 있는 인증서 편집 버튼을 클릭합니다.
사용자 인증서 구성 창이 표시됩니다.

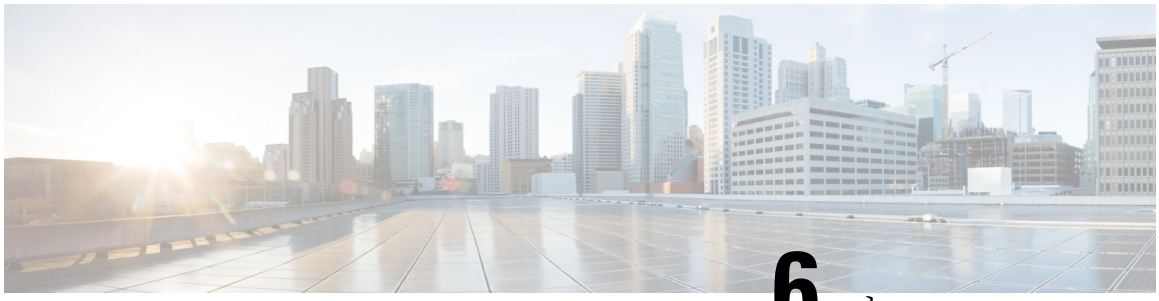
단계 **4** 인증서 구성 창에서 필드를 구성합니다. 필드 및 해당 구성 옵션에 대한 자세한 내용은 온라인 도움말을 참조하십시오.

단계 **5** 설정을 변경한 경우 저장을 클릭합니다.

III 부

디바이스 관리

- 전화기 관리, 61 페이지
- 장치 펌웨어 관리, 79 페이지
- 인프라 장치 관리, 87 페이지



6 장

전화기 관리

- 전화기 관리 개요, 61 페이지
- 전화기 버튼 템플릿, 61 페이지
- 전화기 관리 작업, 62 페이지

전화기 관리 개요

이 장에서는 네트워크의 전화기를 관리하는 방법을 설명합니다. 새 전화기 추가, 다른 사용자에게 기존 전화기 이동, 전화기 잠금 및 전화기 재설정 등의 작업 항목을 설명합니다.

전화기 모델에 대한 Cisco IP 전화기 관리 설명서에는 전화기 모델에 해당하는 구성 정보가 포함되어 있습니다.

전화기 버튼 템플릿

전화기 버튼 템플릿은 전화기 모델을 기반으로 생성됩니다. 일부 전화기 모델은 특정 전화기 버튼 템플릿을 사용하지 않지만 일부 전화기 모델에는 개별 템플릿 또는 장치 기본 템플릿 등 특정 템플릿이 필요합니다.

엔터프라이즈 매개 변수 구성 페이지의 비안전 크기 전화기용 전화기 템플릿 선택 및 자동 등록 레거시 모드 엔터프라이즈 매개 변수에 대한 전화기 템플릿 선택은 사용되는 전화기 버튼 템플릿의 유형을 지정합니다. 필드에 대한 자세한 내용은 온라인 도움말을 참조하십시오.

표 ***3:*** 다양한 시나리오의 전화기 버튼 템플릿

비안전 크기 전화기용 전화기 템플릿 선택	자동 등록 레거시 모드	전화기
개별 템플릿 생성	False	개별 전화기 버튼 템플릿은 범용 장치 템플릿을 통해 전화기를 추가할 때 생성됩니다.

비안전 크기 전화기용 전화기 템플릿 선택	자동 등록 레거시 모드	전화기
장치 기본값의 템플릿 사용	False	개별 전화기 버튼 템플릿은 생성되지 않으며 장치 기본값의 전화기 버튼 템플릿을 사용합니다.
장치 기본값의 템플릿 사용	True	장치 풀, 전화기 템플릿, 발신 검색 공간, 전화기 버튼 템플릿에 대한 값을 장치 기본값에서 가져옵니다.
개별 템플릿 생성	True	장치 풀, 전화기 템플릿, 발신 검색 공간, 전화기 버튼 템플릿에 대한 값을 장치 기본값에서 가져옵니다. 개별 템플릿은 생성되지 않습니다. 자동 등록 레거시 모드에 우선 순위가 있습니다.

전화기 관리 작업

프로시저

	명령 또는 동작	목적
단계 **1**	최종 사용자를 추가하거나 추가하지 않고 사용자 템플릿에서 새 전화기 추가, 64 페이지	최종 사용자를 추가하거나 추가하지 않고 범용 장치 템플릿에서 새 전화기를 추가합니다.
단계 **2**	전화기를 수동으로 추가, 63 페이지	장치 템플릿 없이 최종 사용자에 대해 새 전화기를 추가합니다.
단계 **3**	최종 사용자를 추가하여 사용자 템플릿에서 새 전화기 추가, 65 페이지	최종 사용자에 대해 새 전화기를 추가하고 범용 장치 템플릿을 할당합니다.
단계 **4**	기존 전화기 이동, 72 페이지	구성된 전화기를 다른 최종 사용자로 이동합니다.
단계 **5**	적극적으로 로그인한 장치 찾기 , 72 페이지	특정 장치 또는 사용자가 실제 로그인한 모든 장치를 검색합니다.
단계 **6**	원격으로 로그인된 장치 찾기 , 73 페이지	특정 장치 또는 사용자가 원격으로 로그인한 모든 장치를 검색합니다.

	명령 또는 동작	목적
단계 **7**	원격으로 전화기 잠금, 74 페이지	일부 전화기는 원격으로 잠글 수 있습니다. 전화기를 원격으로 잠그면 잠금이 해제될 때까지 전화기를 사용할 수 없습니다.
단계 **8**	전화기를 초기 기본값으로 재설정 , 75 페이지	전화기를 초기 설정으로 재설정합니다.
단계 **9**	전화기 잠금/삭제 보고서 , 75 페이지	원격으로 잠그고 원격으로 초기 기본 설정으로 재설정된 장치를 검색합니다.
단계 **10**	전화기의 LSC 상태 보기 및 CAPF 보고서 생성, 76 페이지	전화기에서 LSC 만료 상태를 검색하고 CAPF 보고서도 생성합니다.

전화기를 수동으로 추가

최종 사용자와 함께 새 전화기를 수동으로 추가하려면 다음 절차를 수행합니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 장치 > 전화기 > 전화기 찾기 및 나열을 선택합니다.

단계 **2** 전화기 찾기 및 나열 페이지에서 새로 추가를 클릭하여 수동으로 전화기를 추가합니다.

새 전화기 추가 페이지가 표시됩니다.

새 전화기 추가 페이지에서 "범용 장치 템플릿 하이퍼링크를 사용하여 새 전화기를 추가하려면 여기를 클릭"을 클릭하면 페이지가 새 전화기 추가 페이지로 재전송되어 사용자를 추가하거나 추가하지 않고 템플릿에서 전화기를 추가합니다. 자세한 내용은 최종 사용자를 추가하거나 추가하지 않고 사용자 템플릿에서 새 전화기 추가, 64 페이지을 참조하십시오.

단계 **3** 전화기 유형 드롭다운 목록에서 전화기 모델을 선택합니다.

단계 **4** 다음을 클릭합니다.
전화기 구성 페이지가 표시됩니다.

단계 **5** 전화기 구성 페이지에서 필수 필드에 값을 입력합니다. 필드에 대한 자세한 내용은 온라인 도움말을 참조하십시오.

제품별 구성 영역의 필드에 대한 자세한 내용은 사용자의 전화기 모델에 대한 *Cisco IP* 전화기 관리 지침서를 참조하십시오.

단계 **6** 저장을 클릭하여 전화기 구성을 저장합니다.

다음에 수행할 작업

최종 사용자에게 기존 전화기 이동, 49 페이지

최종 사용자를 추가하거나 추가하지 않고 사용자 템플릿에서 새 전화기 추가

사용자를 추가하거나 추가하지 않고 템플릿에서 새 전화기를 추가하려면 다음 절차를 수행합니다. Cisco Unified Communications Manager는 범용 디바이스 템플릿의 설정을 사용하여 전화기를 구성합니다.

시작하기 전에

Cisco Unified Communications Manager에서 범용 장치 템플릿을 구성했는지 확인합니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 장치 > 전화기 > 전화기 찾기 및 나열을 선택합니다.

단계 **2** 전화기 찾기 및 나열 페이지에서 템플릿에서 새로 추가를 클릭하여 최종 사용자를 추가하거나 추가하지 않고 장치 템플릿에서 전화기를 추가합니다.

새 전화기 추가 페이지가 표시됩니다.

새 전화기 추가 페이지에서 "모든 전화기 설정을 수동으로 입력하려면 여기를 클릭" 하이퍼링크를 클릭하는 경우 전화기를 수동으로 추가하도록 새 전화기 추가 페이지로 이동됩니다. 자세한 내용은 전화기를 수동으로 추가, 63 페이지를 참조하십시오.

단계 **3** 전화기 유형**(**및 프로토콜**)** 드롭 다운 목록에서 전화기 모델을 선택합니다.

프로토콜 드롭다운은 전화기가 여러 프로토콜을 지원할 때만 표시됩니다.

단계 **4** 이름 또는 **MAC** 주소 텍스트 상자에 이름 또는 MAC 주소를 입력합니다.

단계 **5** 장치 템플릿 드롭다운 목록에서 범용 장치 템플릿을 선택합니다.

단계 **6** 디렉터리 번호**(**회선 **1)** 드롭다운 목록에서 디렉터리 번호를 선택합니다.

드롭다운 목록의 디렉터리 번호가 최대 드롭다운 제한보다 많은 경우 찾기 탭이 표시됩니다. 찾기를 클릭하면 [디렉터리 번호 찾기] 기준이 있는 팝업 대화 상자가 열립니다.

단계 **7** (선택 사항) 새로 만들기를 클릭하고 디렉터리 번호를 입력하고 새 디렉터리 번호를 만들려는 경우 범용 회선 템플릿을 선택하고 장치에 할당합니다.

또는 사용자 관리 > 사용자/전화기 추가 > 빠른 사용자/전화기 추가로 이동하여 사용자와 연결된 디렉터리 번호를 사용하여 전화기를 만들 수 있습니다.

단계 **8** (선택 사항) 사용자 드롭다운 목록에서 새 전화기를 추가하려는 최종 사용자를 선택합니다.

참고 Cisco 이중 모드(모바일) 장치의 겨우 사용자를 반드시 선택해야 합니다.

드롭다운 목록의 최종 사용자 수가 최대 드롭다운 제한을 초과하는 경우 찾기 탭이 표시됩니다. 찾기를 클릭하면 최종 사용자 찾기 기준이 있는 팝업 대화 상자가 열립니다.

단계 **9** 추가를 클릭합니다.

참고 비안전 크기 전화기의 경우, 전화기 템플릿은 엔터프라이즈 매개 변수 구성 페이지의 비안전 크기 전화기용 전화기 템플릿 선택 및 자동 등록 레거시 모드 매개 변수에서 선택한 항목을 기반으로 생성됩니다 .

추가 성공 메시지가 표시됩니다. Cisco Unified Communications Manager는 전화기를 추가하고 전화기 구성 편집 페이지가 표시됩니다. 전화기 구성 페이지의 필드에 대한 자세한 내용은 온라인 도움말을 참조하십시오.

다음에 수행할 작업

최종 사용자에게 기존 전화기 이동, 49 페이지

최종 사용자를 추가하여 사용자 템플릿에서 새 전화기 추가

최종 사용자에 대해 새 전화기를 추가하려면 다음 절차를 수행합니다.

시작하기 전에

전화기를 추가하는 최종 사용자에게 장치 템플릿을 포함하는 사용자 프로파일이 설정되었습니다. Cisco Unified Communications Manager는 범용 장치 템플릿의 설정을 사용하여 전화기를 구성합니다.

- 최종 사용자 관리 작업, 41 페이지

프로시저

단계 **1** Cisco Unified CM 관리에서 사용자 관리 > 사용자/전화기 추가 > 빠른 사용자/전화기 추가를 선택합니다.

단계 **2** 찾기를 클릭하고 새 전화기를 추가하려는 최종 사용자를 선택합니다.

단계 **3** 디바이스 관리를 클릭합니다.
[디바이스 관리] 창이 나타납니다.

단계 **4** 새 전화기 추가를 클릭합니다.
[사용자에게 전화기 추가] 팝업이 표시됩니다.

단계 **5** 제품 유형 드롭다운 목록에서 전화기 모델을 선택합니다.

단계 **6** 디바이스 프로토콜 드롭다운에서 프로토콜로 SIP 또는 SCCP를 선택합니다.

단계 **7** 디바이스 이름 텍스트 상자에 디바이스 MAC 주소를 입력합니다.

단계 **8** 범용 디바이스 템플릿 드롭다운 목록에서 범용 디바이스 템플릿을 선택합니다.

단계 **9** 전화기가 확장 모듈을 지원하는 경우 배포하려는 확장 모듈 수를 입력합니다.

단계 **10** Extension Mobility를 사용하여 전화에 액세스하려면 **Extension Mobility**에서 확인란을 선택합니다.

단계 **11** 전화기 추가를 클릭합니다.
[새 전화기 추가] 팝업이 닫힙니다. Cisco Unified Communications Manager는 사용자에게 전화기를 추가하고 범용 디바이스 템플릿을 사용하여 전화기를 구성합니다.

단계 **12** 전화기 구성을 추가 편집하려면 해당 연필 아이콘을 클릭하여 전화기 구성 창에서 전화기를 엽니다.

협업 모바일 통합 가상 장치 개요

CMC 장치는 연결된 원격 대상을 나타내는 가상 장치입니다. 엔터프라이즈 전화기가 CMC 장치로 전화를 걸면 통화가 원격 대상으로 재전송됩니다. 이 기능은 사용자 정의를 거의 사용하지 않는 Spark 원격 장치와 동일한 장치 유형 협업 모바일 통합을 생성하는 데 목적이 있으며 다음과 같은 이점을 제공합니다.

- Spark 원격 장치와 유사한 기능을 가진 Cisco Unified Communications Manager에서 기본 모바일 장치를 지원합니다.
- 향후 개발 기능 패리티를 포함하는 기능이 있는 Spark-RD로 활용합니다.
- 휴대폰에서 데스크폰으로, 데스크폰에서 휴대폰으로 통화를 이동하는 것과 같은 모바일 특정 사용 사례에 대한 사용자 정의를 허용합니다. (ID 페이지에 deskpickup 타이머를 추가하고 제품 지원 기능 설정을 통해 활성화합니다.)
- CMC 장치는 헌트 그룹에 포함될 수 있습니다.
- Spark 원격 장치와 회선을 공유할 수 있습니다.
- 라이센스 - 라이센스 사용 관점을 위해 별도의 장치로 계산합니다. 다중 장치 라이센스 번들은 CMC를 지원해야 합니다.

CMC RD 장치에 대한 라이센스 조정

새 CMC 장치가 추가되면 사용자와 연결된 장치의 수/유형을 기반으로 라이센스를 사용합니다. CMC 장치에서 사용하는 라이센스 유형은 연결된 최종 사용자가 가지고 있는 장치 수에 따라 달라집니다.

- CMC 장치만 배포하는 경우 인핸스드(Enhanced) 라이센스를 사용합니다.
- CMC 장치와 Spark RD을 배포하는 경우 인핸스드(Enhanced) 라이센스를 사용합니다.
- CMC 및 물리적 장치의 경우: 인핸스드 플러스(Enhanced Plus) 라이센스
- CMC, Spark RD 및 물리적 장치의 경우: 인핸스드 플러스(Enhanced Plus) 라이센스

협업 모바일 통합 가상 장치 추가

다음 절차를 수행하여 최종 사용자에 대한 Cisco CMC(협업 모바일 통합) 원격 장치를 추가합니다.

시작하기 전에

전화기를 추가하는 최종 사용자에게 범용 장치 템플릿을 포함하는 사용자 프로파일이 설정되어 있어야 합니다. Cisco Unified Communications Manager는 범용 장치 템플릿의 설정을 사용하여 전화기를 구성합니다.

프로시저

단계 **1** Cisco Unified CM 관리에서장치 > 전화기를 선택합니다.

단계 **2** 새로 추가 단추를 클릭합니다.

단계 **3** 모든 전화기 설정을 수동으로 입력하려면 여기를 클릭하십시오.를 클릭합니다.
새 전화기 추가 창이 표시됩니다.

단계 **4** 전화기 유형 드롭다운 목록에서 Cisco 협업 모바일 통합을 선택하고 다음을 클릭합니다.
전화기 구성 창이 나타납니다.

단계 **5** 소유자 사용자 **ID** 드롭다운에서 장치를 소유할 최종 사용자를 선택합니다.

단계 **6** 장치 풀 드롭다운에서 장치 풀을 선택합니다.

단계 **7** 저장을 클릭합니다.
변경 사항을 적용하려면 구성 적용 버튼을 클릭하라는 경고 메시지가 팝업됩니다. 확인을 클릭합니다. 장치가 추가됩니다.

단계 **8** 디렉터리 번호를 구성하려면 추가된 CMC 장치를 클릭하고 디렉터리 번호를 입력한 다음 저장을 클릭합니다.

단계 **9** 추가된 CMC 장치에 대한 새 원격 대상을 추가하려면 ID 상자에서 해당 링크를 클릭합니다.

단계 **10** 원격 대상 구성 창에서 이름, 대상 번호를 입력하고 저장을 클릭합니다.

참고 추가되는 하나의 CMC 장치에 대해서는 원격 대상을 하나만 추가할 수 있습니다.

단계 **11** 기존 원격 대상을 업데이트하려면 새 이름을 입력하고 저장을 클릭합니다.

단계 **12** 기존 원격 대상을 삭제하려면 메뉴에서 삭제 버튼을 클릭합니다.
웹 페이지에서 영구 삭제를 확인하는 메시지가 나타납니다. 확인을 클릭합니다.

단계 **13** 장치 페이지에서 CMC 장치를 삭제하려면 [장치 확인란을 선택하고 메뉴에서 선택한 항목 삭제를 클릭합니다.

CMC RD 기능 상호 작용

표 ***4: CMC RD*** 기능 상호 작용

기능	상호 작용
공유 회선 처리	• CMC RD 및 Spark RD가 연결된 공유 데스크폰이 있는 경우, 사용자가 엔터프라이즈 전화기에서 CMC 장치 DN으로 전화를 걸면 CMC RD, Spark RD 및 공유 데스크폰 3대가 모두 울립니다. • 원격 대상에서 응답하면 공유 데스크폰에 "원격 사용 중" 메시지가 표시됩니다. • 공유 데스크폰에서 응답하면 원격 대상 전화기(CMC RD 및 Spark RD 전화기) 양쪽에서 연결이 끊어집니다.

기능	상호 작용
CMC 장치는 CMG(Call Manager 그룹) 설정에서 작동합니다.	• CMC 장치는 Call Manager 그룹과 연결될 때 항상 기본 서버에서 실행되고 기본 서버가 다운된 경우에만 Call Manager 그룹의 다음 활성 보조 서버에서 실행됩니다. • 기본 서버가 통화 도중 다운되는 경우 진행 중인 통화는 계속 유지되고 통화가 종료되면 CMC 장치는 보조 서버에 등록됩니다. 참고 통화가 유지 모드에 있으면 전화기 간 미디어는 여전히 활성 상태로 유지되지만, 통화 연결을 끊는 것을 제외하고는 다른 작업을 수행할 수 없습니다. • 기본 서버가 처음에 다운되고 CMC 장치가 보조 서버에 등록된 동안 통화가 시작된 경우 통화를 진행하는 동안 기본 서버가 복구되면 통화가 유지 모드로 전환되고 통화 종료 후 CMC 장치가 기본 서버에 등록됩니다.
통화 앵커링	CMC 장치 및 원격 대상 번호 통화에서 수신되는 모든 기본 통화는 엔터프라이즈 네트워크에 고정되어 있습니다. CMC 원격 장치가 구성된 경우 사용자는 모바일 장치에서 모든 통화가 엔터프라이즈에 고정된 통화를 걸고 받을 수 있습니다. • 사용자는 엔터프라이즈 번호에서 CMC 원격 대상으로 직접 전화를 걸 수 있습니다. 통화는 엔터프라이즈 네트워크에 고정됩니다. 이 시나리오에서는 데스크폰(CMC 장치의 공유 회선)에서는 벨이 울리지 않지만 원격 사용 중 상태로 유지됩니다. • 사용자는 CMC 원격 대상에서 엔터프라이즈 번호로 전화를 걸 수 있습니다. 통화가 고정되었습니다. 이 시나리오에서는 데스크폰(CMC 장치의 공유 회선)이 원격 사용 중 상태로 유지됩니다.

기능	상호 작용
단일 전화번호 연결	• 원격 대상 구성 페이지에서 단일 번호 도달**(SNR)** 활성화 확인란이 선택되어 있지 않으면 통화가 CMC RD로 확장되지 않으며 통화가 거부됩니다. • 원격 대상의 수신 통화 및 아웃바운드 원격 대상 번호 통화는 단일 번호 도달**(SNR)** 활성화 확인란 선택에 관계 없이 영향을 받지 않습니다. • CMC 장치와 공유되는 데스크폰이 있고 단일 번호 도달**(SNR)** 활성화 확인란이 선택되어 있지 않으면 통화가 CMC RD가 아니라 공유된 데스크폰으로 확장됩니다. 참고 단일 번호 도달**(SNR)** 음성메일 정책이 사용자 제어로 설정된 경우 기본 확장으로 비공개 전환 시 이동성 대상 번호가 트리거되지 않습니다. 기본 확장만 트리거됩니다. 사용자 제어 설정은 상담 호 전환을 지원합니다. 타이머 제어 음성 메일 방지 정책은 상담 호 전환 및 비공개 전환을 모두 지원합니다.

기능	상호 작용
시간(ToD)을 기준으로 한 통화 라우팅	• 원격 대상에 대한 시간 구성을 사용하여 벨소리 일정을 설정할 수 있습니다. 예를 들어 월요일-금요일 오전 9시에서 오후 5시 사이에 특정 시간을 구성할 수 있습니다. 통화는 해당 시간에 원격 대상으로 재전송됩니다. 엔터프라이즈 전화기에서 CMC 번호로의 통화는 원격 대상 구성 페이지에서 수정된 벨소리 일정에 따라 라우팅됩니다. 벨소리 일정은 아래와 같이 지정할 수 있습니다. • 모든 시간 - 통화가 언제든지 라우팅됩니다. 제한이 없습니다. • 요일 - 선택한 특정 요일에만 통화를 라우팅합니다. • 특정 시간 - 통화는 선택한 업무 시간에만 라우팅됩니다. 표준 시간대를 선택해야 합니다. • 벨소리 일정 중에 통화를 수신하면 엔터프라이즈 전화기에서 CMC 번호로의 통화가 원격 대상 구성 페이지의 허용된 액세스 목록 또는 차단된 액세스 목록에 추가된 통화 번호 또는 패턴에 따라 라우팅됩니다. • 허용된 액세스 목록 - 발신자 번호 또는 패턴이 허용된 액세스 목록에 있는 경우에만 대상의 벨소리가 울립니다. • 차단된 액세스 목록 - 발신자 번호 또는 패턴이 차단된 액세스 목록에 있는 경우 대상의 벨소리가 울리지 않습니다. 참고 언제든지 허용된 액세스 목록 또는 차단된 액세스 목록만 사용할 수 있습니다.
사용자 로캘 설정	CMC 가상 장치는 전화기 구성 창에 구성된 로캘 설정을 사용하여 전화기 디스플레이 및 전화기 알림에 대한 로캘을 결정합니다. 이 정책은 일반 통화 및 지금 전화회의 번호에 대한 통화에 적용됩니다. 알림 부분의 경우 사용자 로캘 설정에서 동일한 언어를 선택하여 발신(모든 엔터프라이즈 전화기) 및 착신(CMC 장치) 전화기의 알림은 전화기 구성 페이지에서 선택한 사용자 로캘 설정을 기반으로 합니다. 참고 예를 들어 CMC 장치와 연결된 원격 대상에서 지금 전화회의 번호로 전화를 걸 때 해당 알림은 CMC 장치의 전화기 구성 페이지에서 선택한 사용자 로케일 설정을 기반으로 합니다.

기능	상호 작용
HLogin 및 Hlogin에 대한 새 액세스 코드	이 기능을 통해 관리자는 추가된 서비스 매개 변수를 사용하여 CMC 장치에 대한 헌트 그룹 로그인 및 로그아웃 번호를 설정할 수 있습니다. • 헌트 그룹 로그인에 대한 엔터프라이즈 기능 액세스 번호. • 헌트 그룹 로그아웃에 대한 엔터프라이즈 기능 액세스 번호. 사용자가 CMC 장치에 연결된 RD에서 Hlogin 번호를 입력하면, CMC 장치와 연결된 헌트 파일럿 번호를 다이얼하는 경우에만 통화가 RD로 재전송됩니다. 사용자가 CMC 장치에 연결된 RD에서 Hlogout 번호를 입력하면, CMC 장치와 연결된 헌트 파일럿 번호를 다이얼하는 경우에는 통화가 RD로 재전송되지 않습니다. 기본적으로 CMC 장치는 Hloggedin입니다. 두 경우 모두 CMC 장치에 대한 직접 통화는 영향을 받지 않습니다.
데이터베이스에 구성된 벨소리 울림 전 지연 타이머를 기반으로 하는 CMC 원격 대상 통화 확장	**DB**의 벨소리 울림 전 지연 타이머가 **5000**로 구성된 경우 • 엔터프라이즈 전화기에서 CMC 번호로 전화가 걸려오면 공유된 회선 벨소리와 통화가 5초 후에 원격 대상에 도달합니다. • 엔터프라이즈 전화기에서 CMC 번호로 전화가 걸려올 때 공유된 회선이 5초 전에 통화에 응답하는 경우 통화가 원격 대상으로 확장되지 않습니다. • 엔터프라이즈 전화기에서 CMC 번호로 전화가 걸려올 때 공유된 회선의 벨소리가 울리고 발신자가 5초 전에 전화를 끊는 경우 통화가 원격 대상으로 확장되지 않습니다. **DB**의 벨소리 울림 전 지연 타이머가 **0**으로 구성된 경우 엔터프라이즈 전화기에서 CMC 번호로의 모든 통화는 원격 대상과 공유된 회선에 동시에 알립니다.
BAT(벌크 관리 도구) 지원	CMC 장치에 BAT 지원이 제공됩니다.

CMC RD 기능 제한

표 ***5: CMC RD*** 기능 제한 사항

기능	제한 사항
CMC 원격 대상 연결	다음 제한 사항이 적용됩니다. • CMC 장치를 하나의 원격 대상에만 연결할 수 있습니다. . • 최종 사용자가 삭제되면 연결된 CMC 장치와 RD(원격 대상)도 삭제됩니다. 참고 이동성 활성화 확인란을 선택하거나 선택 취소한 경우에는 CMC와 RD가 영향을 받지 않습니다. CMC 장치는 삭제되지 않습니다. 참고 Cisco Unified Communications Manager는 CMC 장치에 대한 통화 처리 보존을 지원하지 않습니다.

기존 전화기 이동

최종 사용자에게 구성된 전화기를 이동하려면 다음 절차를 수행합니다.

프로시저

단계 **1** [Cisco Unified CM 관리]에서 사용자 관리 > 사용자/전화기 추가 > 빠른/사용자 전화기 추가를 선택합니다.

단계 **2** 찾기를 클릭하고 기존 전화기를 이동할 사용자를 선택합니다.

단계 **3** 디바이스 관리 버튼을 클릭합니다.

단계 **4** 이 사용자로 이동할 전화기 찾기 버튼을 클릭합니다.

단계 **5** 이 사용자로 이동하려는 전화기를 선택합니다.

단계 **6** 선택 항목 이동을 클릭합니다.

적극적으로 로그인한 장치 찾기

Cisco Extension Mobility 및 Cisco Extension Mobility Cross Cluster 기능에서는 사용자가 활성 로그인한 장치에 대한 레코드를 유지합니다. Cisco Extension Mobility 기능의 활성 로그인한 장치 보고서에서

는 로컬 사용자가 활성 로그인한 로컬 전화기를 추적하고, Cisco Extension Mobility Cross Cluster 기능의 활성 로그인한 장치 보고서에서는 원격 사용자가 활성 로그인한 로컬 전화기를 추적합니다.

Unified Communications Manager 사용자가 로그인한 장치를 검색하는 특정 검색 창을 제공합니다. 다음 단계에 따라 특정 장치를 검색하거나 사용자가 활성 로그인한 모든 장치를 나열합니다.

프로시저

단계 **1** 장치 > 전화기를 선택합니다.

단계 **2** 오른쪽 상단의 관련 링크 드롭다운 목록표에서 적극적으로 로그인한 장치 보고서를 선택하고 이동을 클릭합니다.

단계 **3** 데이터베이스에서 적극적으로 로그인한 장치 레코드를 모두 찾으려면 대화 상자가 비어 있는지 확인하고 4단계로 이동합니다.

레코드를 필터링하거나 검색하려면 다음을 수행합니다.

a) 첫 번째 드롭다운 목록에서 검색 파라미터를 선택합니다.
b) 두 번째 드롭다운 목록에서 검색 패턴을 선택합니다.
c) 적절한 검색 텍스트를 지정합니다(해당하는 경우).

참고 다른 검색 기준을 추가하려면 **(+)** 버튼을 클릭합니다. 기준을 추가하면 시스템에서 지정한 모든 기준과 일치하는 레코드를 검색합니다. 기준을 제거하려면 **(–)** 버튼을 클릭하여 마지막으로 추가된 기준을 제거하거나 필터 지우기 버튼을 클릭하여 추가된 검색 기준을 모두 제거합니다.

단계 **4** 찾기를 클릭합니다.

일치하는 레코드가 모두 표시됩니다. 행/페이지 드롭다운 목록에서 다른 값을 선택하여 각 페이지에 표시할 항목 수를 변경할 수 있습니다.

단계 **5** 표시되는 레코드 목록에서 보려는 레코드의 링크를 클릭합니다.

참고 정렬 순서를 역순으로 변경하려면 목록 헤더에서 위쪽 또는 아래쪽 화살표를 클릭합니다(사용 가능한 경우).

창에 선택한 항목이 표시됩니다.

원격으로 로그인된 장치 찾기

Cisco Extension Mobility Cross Cluster 기능에서는 사용자가 원격으로 로그인한 장치에 대한 레코드를 유지합니다. [원격으로 로그인된 장치] 보고서에서는 다른 클러스터에서 소유하지만 EMCC 기능을 사용 중인 로컬 사용자가 현재 로그인한 전화기를 추적합니다.

Unified Communications Manager 사용자가 원격으로 로그인한 장치를 검색하기 위한 특정 검색 창을 제공합니다. 다음 단계에 따라 사용자가 원격으로 로그인한 특정 장치를 검색하거나 모든 장치를 나열합니다.

프로시저

단계 **1** 장치 > 전화기를 선택합니다.

단계 **2** 오른쪽 상단의 관련 링크 드롭다운 목록표에서 원격으로 로그인된 장치를 선택하고 이동을 클릭합니다.

단계 **3** 데이터베이스에서 원격으로 로그인된 장치 레코드를 모두 찾으려면 대화 상자가 비어 있는지 확인하고 4단계로 이동합니다.

레코드를 필터링하거나 검색하려면 다음을 수행합니다.

a) 첫 번째 드롭다운 목록에서 검색 파라미터를 선택합니다.
b) 두 번째 드롭다운 목록에서 검색 패턴을 선택합니다.
c) 적절한 검색 텍스트를 지정합니다(해당하는 경우).

참고 다른 검색 기준을 추가하려면 **(+)** 버튼을 클릭합니다. 기준을 추가하면 시스템에서 지정한 모든 기준과 일치하는 레코드를 검색합니다. 기준을 제거하려면 **(–)** 버튼을 클릭하여 마지막으로 추가된 기준을 제거하거나 [필터 지우기] 버튼을 클릭하여 추가된 검색 기준을 모두 제거합니다.

단계 **4** 찾기를 클릭합니다.

일치하는 레코드가 모두 표시됩니다. 행/페이지 드롭다운 목록에서 다른 값을 선택하여 각 페이지에 표시할 항목 수를 변경할 수 있습니다.

단계 **5** 표시되는 레코드 목록에서 보려는 레코드의 링크를 클릭합니다.

참고 정렬 순서를 역순으로 변경하려면 목록 헤더에서 위쪽 또는 아래쪽 화살표를 클릭합니다(사용 가능한 경우).

창에 선택한 항목이 표시됩니다.

원격으로 전화기 잠금

일부 전화기는 원격으로 잠글 수 있습니다. 전화기를 원격으로 잠그면 잠금이 해제될 때까지 전화기를 사용할 수 없습니다.

전화기에서 원격 잠금 기능이 지원되면 오른쪽 상단 모서리에 잠금 단추가 표시됩니다.

프로시저

단계 **1** 장치 > 전화기를 선택합니다.

단계 **2** 전화기 찾기 및 나열 창에서 전화기 검색 기준을 입력하고 찾기를 클릭하여 특정 전화기를 찾습니다.

검색 조건과 일치하는 전화기 목록이 표시됩니다.

단계 **3** 원격 잠금을 수행할 전화기를 선택합니다.

단계 **4** 전화기 구성 창에서 잠금을 클릭합니다.

전화기가 등록되어 있지 않은 경우 전화기를 등록한 다음 잠글 수 있음을 알리는 팝업 창이 표시됩니다. 잠금을 클릭합니다.

장치 잠금/삭제 상태 섹션에 최신 요청, 대기 중인지 여부 및 최신 확인에 대한 정보가 표시됩니다.

전화기를 초기 기본값으로 재설정

일부 전화기는 원격 삭제 기능을 지원합니다. 전화기에 원격 삭제를 수행하면 해당 작업으로 전화기가 출고시 설정으로 재설정됩니다. 이전에 전화기에 저장한 모든 내용이 삭제됩니다.

전화기에서 원격 삭제 기능이 지원되면 오른쪽 상단 모서리에 삭제단추가 표시됩니다.

주의 이 작업은 실행 취소할 수 없습니다. 전화기를 출고시 설정으로 재설정해야 할 때만 이 작업을 수행해야 합니다.

프로시저

단계 **1** 장치 > 전화기를 선택합니다.

단계 **2** 전화기 찾기 및 나열 창에서 전화기 검색 기준을 입력하고 찾기를 클릭하여 특정 전화기를 찾습니다.

검색 조건과 일치하는 전화기 목록이 표시됩니다.

단계 **3** 원격 삭제를 수행할 전화기를 선택합니다.

단계 **4** 전화기 구성 창에서 삭제를 클릭합니다.

전화기가 등록되어 있지 않은 경우 전화기를 등록한 다음 삭제할 수 있음을 알리는 팝업 창이 표시됩니다. 삭제를 클릭합니다.

장치 잠금/삭제 상태 섹션에 최신 요청, 대기 중인지 여부 및 최신 확인에 대한 정보가 표시됩니다.

전화기 잠금/삭제 보고서

Unified Communications Manager에서는 원격으로 잠겼거나 원격으로 삭제된 장치를 검색하는 특정 검색 창을 제공합니다. 다음 단계에 따라 원격으로 잠겼거나 원격으로 삭제된 장치 중 특정 장치를 검색하거나 장치를 모두 나열합니다.

프로시저

단계 **1** 장치 > 전화기를 선택합니다.

[전화기 찾기 및 나열] 창이 표시됩니다. 활성(이전) 쿼리의 레코드가 창에 표시될 수도 있습니다.

단계 **2** 창의 오른쪽 위에 있는 관련 링크 드롭다운 목록표에서 전화기 잠금/삭제 보고서를 선택하고 이동을 클릭합니다.

단계 **3** 데이터베이스에서 원격으로 잠기거나 원격으로 삭제된 장치를 모두 찾으려면 텍스트 상자가 비어 있는지 확인하고 4단계로 이동합니다.

특정 장치에 대한 레코드를 필터링하거나 검색하려면:

a) 첫 번째 드롭다운 목록에서 검색할 장치 작업 유형을 선택합니다.
b) 두 번째 드롭다운 목록에서 검색 파라미터를 선택합니다.
c) 세 번째 드롭다운 목록에서 검색 패턴을 선택합니다.
d) 적절한 검색 텍스트를 지정합니다(해당하는 경우).

참고 다른 검색 기준을 추가하려면 + 버튼을 클릭합니다. 기준을 추가하면 시스템에서 지정한 모든 기준과 일치하는 레코드를 검색합니다. 기준을 제거하려면 – 버튼을 클릭하여 마지막으로 추가된 기준을 제거하거나 [필터 지우기] 버튼을 클릭하여 추가된 검색 기준을 모두 제거합니다.

단계 **4** 찾기를 클릭합니다.

일치하는 레코드가 모두 표시됩니다. 행/페이지 드롭다운 목록에서 다른 값을 선택하여 각 페이지에 표시할 항목 수를 변경할 수 있습니다.

단계 **5** 표시되는 레코드 목록에서 보려는 레코드의 링크를 클릭합니다.

참고 정렬 순서를 역순으로 변경하려면 목록 헤더에서 위쪽 또는 아래쪽 화살표를 클릭합니다(사용 가능한 경우).

창에 선택한 항목이 표시됩니다.

전화기의 LSC 상태 보기 및 CAPF 보고서 생성

Cisco Unified Communications Manager 인터페이스 내에서 LSC(Locally Significant Certificate) 만료 정보를 모니터링하려면 이 절차를 사용합니다. 다음 검색 필터는 LSC 정보를 표시합니다.

- LSC 만료일—전화기에 LSC 만료 날짜를 표시합니다.
- LSC 발급자—CAPF 또는 타사의 발급자 이름을 표시합니다.
- LSC 발급자 만료일—발급자의 만료 날짜를 표시합니다.

참고 새 장치에서 발행된 LSC가 없는 경우, **LSC** 만료 및 **LSC** 발급자 만료일 필드의 상태는 "NA"로 설정됩니다.

Cisco Unified Communications Manager 11.5(1)로 업그레이드하기 전에 LSC가 장치로 발행되는 경우, **LSC** 만료 및 **LSC** 발급자 만료일 필드의 상태는 "알 수 없음"으로 설정됩니다.

프로시저

단계 **1** 장치 > 전화기를 선택합니다.

단계 **2** 첫 번째 전화기 찾기 위치 드롭다운 목록에서 다음 기준 중 하나를 선택합니다.

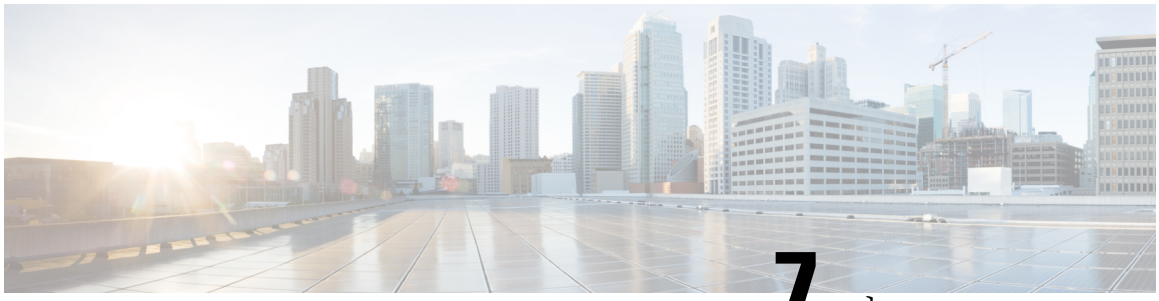
- LSC 만료일
- LSC 발급자
- LSC 발급자 만료일

두 번째 전화기 찾기 위치 드롭다운 목록에서 다음 기준 중 하나를 선택합니다.

- 이전
- 정확하게 일치
- 이후
- 시작 단어
- 포함
- 끝 단어
- 정확하게 일치
- 비어 있음
- 비어 있지 않음

단계 **3** 찾기를 클릭합니다.
검색된 전화기 목록이 표시됩니다.

단계 **4** 관련 링크 드롭다운 목록에서 파일의 **CAPF** 보고서를 선택하고 이동을 클릭합니다.
보고서가 다운로드됩니다.



7 장

장치 펌웨어 관리

- 장치 펌웨어 업데이트 개요, 79 페이지
- 장치 팩 또는 개별 펌웨어 설치, 80 페이지
- 시스템에서 사용하지 않는 펌웨어 제거, 81 페이지
- 전화기 모델에 대한 기본 펌웨어 설정, 82 페이지
- 전화기에 대한 펌웨어 로드 설정, 83 페이지
- 로드 서버 사용, 83 페이지
- 기본값 이외의 펌웨어 로드가 사용되는 장치 찾기, 84 페이지

장치 펌웨어 업데이트 개요

장치 로드는 IP 전화기, TelePresence 시스템 및 Cisco Unified Communications Manager에 프로비저닝되고 등록된 시스템 같은 장치용 소프트웨어 및 펌웨어입니다. 설치 또는 업그레이드 동안 Cisco Unified Communications Manager는 Cisco Unified Communications Manager의 버전이 릴리스된 시기를 기반으로 사용할 수 있는 최신 로드를 포함합니다. Cisco는 새 기능과 소프트웨어 수정 프로그램을 소개하기 위해 정기적으로 업데이트된 펌웨어를 릴리스하며 해당 로드를 포함하는 Cisco Unified Communications Manager 업그레이드를 기다리지 않고 최신 로드로 전화기를 업데이트할 수 있습니다.

엔드포인트를 소프트웨어의 새 버전으로 업그레이드하기 전에 새 로드에 필요한 파일을 엔드포인트가 액세스할 수 있는 위치로 다운로드할 수 있어야 합니다. 가장 일반적인 위치는 “TFTP 서버”라고 하는 Cisco TFTP 서비스가 활성화된 Cisco UCM 노드입니다. 또한 일부 전화기는 “로드 서버”라고 하는 대체 다운로드 위치를 사용하여 지원됩니다.

서버에 있는 tftp 디렉터리에 이미 있는 파일을 나열하거나, 보거나, 다운로드하려는 경우 CLI 명령 file list tftp를 사용하여 TFTP 디렉터리에 있는 파일을 확인하고 file view tftp를 사용하여 파일을 보고 file get tftp를 사용하여 TFTP 디렉터리에 있는 파일을 복사합니다. 자세한 내용은 *Cisco Unified Communications Solutions*용 명령줄 인터페이스 설명서를 참조하십시오. 또한 웹 브라우저를 사용하여 URL “http://<tftp_server>:6970/<filename>”으로 이동하여 TFTP 파일을 다운로드할 수도 있습니다.

팁 시스템 차원의 기본값으로 구성하기 전에 단일 장치에 새 로드를 적용할 수 있습니다. 이 방법은 테스트 목적으로 유용합니다. 그러나 해당 유형의 다른 모든 장치가 새로운 로드로 시스템 차원의 기본값을 업데이트할 때까지 기존 로드를 사용합니다.

장치 팩 또는 개별 펌웨어 설치

장치 패키지를 설치하여 새 전화기 유형을 소개하고 여러 전화기 모델에 대한 펌웨어를 업그레이드합니다.

- 기존 장치에 대한 개별 펌웨어는 다음 옵션을 사용하여 설치 또는 업그레이드할 수 있습니다: Cisco 옵션 패키지(COP) 파일—COP 파일에는 게시자에 설치했을 때 펌웨어 파일 설치와 별도로 기본 펌웨어를 업데이트하도록 펌웨어 파일과 데이터베이스 업데이트가 포함되어 있습니다.
- 펌웨어 파일만—zip 파일로 제공되고, 개별 장치 펌웨어 파일이 포함되어 있으며 수동으로 압축을 풀어 TFTP 서버의 해당 디렉터리로 업로드해야 합니다.

참고 COP 또는 펌웨어 파일 패키지와 관련된 설치 지침은 README 파일을 참조하십시오.

프로시저

단계 **1** Cisco Unified OS 관리에서 소프트웨어 업그레이드 > 설치/업그레이드를 선택합니다.

단계 **2** [소프트웨어 위치] 섹션에서 해당 값을 입력하고 다음을 클릭합니다.

단계 **3** 사용 가능한 소프트웨어 드롭다운 목록에서 장치 패키지 파일을 선택하고 다음을 클릭합니다.

단계 **4** MD5 값이 올바른지 확인하고 다음을 클릭합니다.

단계 **5** 경고 상자에서 올바른 펌웨어를 선택했는지 확인한 다음 설치를 클릭합니다.

단계 **6** 성공 메시지가 수신되었는지 확인합니다.

참고 클러스터를 재부팅하는 경우 8단계로 건너뜁니다.

단계 **7** 서비스가 실행 중인 모든 노드에서 **Cisco TFTP** 서비스를 다시 시작합니다.

단계 **8** 영향을 받는 장치를 재설정하여 장치를 새 로드로 업그레이드합니다.

단계 **9** Cisco Unified CM 관리에서 장치 > 장치 설정 > 장치 기본값을 선택하고 로드 파일(특정 장치)의 이름을 새 로드로 수동으로 변경합니다.

단계 **10** 저장을 클릭한 다음, 장치를 재설정합니다.

단계 **11** 모든 클러스터 노드에서 **Cisco Tomcat** 서비스를 다시 시작합니다.

단계 **12** 다음 중 하나를 수행합니다.

- 11.5(1) SU4 이하, 12.0(1) 또는 12.0(1) SU1을 실행하는 경우 클러스터를 재부팅합니다.

- 11.5(x) 릴리스 11.5(1)SU5 이상 또는 릴리스 12.0(1)SU2 이상을 실행하는 경우 퍼블리셔 노드에서 **Cisco CallManager** 서비스를 재부팅합니다. 그러나, 가입자 노드에서만 **Cisco CallManager** 서비스를 실행하는 경우에는 이 작업을 건너뛸 수 있습니다.

펌웨어 설치 시 발생할 수 있는 문제

다음은 장치 팩을 설치한 후에 실행할 수 있는 몇 가지 문제입니다.

문제	원인/해결
새 장치가 등록 되지 않음	이 문제는 장치 유형 불일치로 인해 발생할 수 있습니다. 원인은 다음과 같을 수 있습니다. • 장치를 잘못된 장치 유형을 사용하여 전화기 구성 창에 추가했습니다. 예를 들어 Cisco DX80이 DMS Cisco TelePresence DX80 대신에 전화기 유형으로 선택되었습니다. 장치를 올바른 장치 유형으로 다시 구성합니다. • **Cisco CallManager** 서비스는 새 장치 유형에 대해 알지 못합니다. 이 경우에는 퍼블리셔 노드에서 **Cisco CallManager** 서비스를 다시 시작합니다.
엔드포인트가 새 펌웨어로 업그레이드되지 않습니다.	가능한 이유는 다음과 같습니다. • 장치 팩이 TFTP 서버에 설치되지 않았습니다. 그 결과, 전화기에서 펌웨어를 다운로드할 수 없습니다. • 설치 후에 **Cisco TFTP** 서비스가 다시 시작되지 않아 서비스에서 새 파일에 대해 알 수 없습니다. TFTP 서버에 장치 팩을 설치해야 합니다.
Cisco Unified CM 관리의 전화기 구성 창에 새 장치 유형에 대한 아이콘 이미지가 있어야 하는 곳에 끊어진 링크가 표시됩니다.	CLI에서 모든 노드의 **Cisco Tomcat** 서비스를 다시 시작하십시오.

시스템에서 사용하지 않는 펌웨어 제거

장치 로드 관리 창을 사용하면 시스템에서 사용하지 않는 펌웨어(장치 로드) 및 관련 파일을 삭제하여 디스크 공간을 늘릴 수 있습니다. 예를 들어, 업그레이드하기 전에 사용하지 않는 로드를 삭제하여 디스크 공간 부족으로 인한 업그레이드 오류를 방지할 수 있습니다. 일부 펌웨어 파일에는 장치 로드 관리 창에 나열되지 않는 종속성 파일이 있을 수 있습니다. 펌웨어를 삭제하면 종속 파일도 삭제됩니다. 그러나 추가 펌웨어와 연결된 경우 종속 파일이 삭제되지 않습니다.

참고 클러스터의 각 서버에 대해 사용하지 않는 펌웨어를 개별적으로 삭제해야 합니다.

시작하기 전에

주의 사용하지 않는 펌웨어를 삭제하기 전에 올바른 로드를 삭제하고 있는지 확인합니다. 전체 클러스터의 DRS 복원을 수행하지 않고는 삭제된 로드를 복원할 수 없습니다. 펌웨어를 삭제하기 전에 백업을 수행하는 것이 좋습니다.

파일의 여러 로드를 사용하는 장치에 대한 파일을 삭제하지 않도록 하십시오. 예를 들어, 특정 CE 엔드포인트는 여러 개의 로드를 사용합니다. 그러나 장치 로드 관리 창에서 하나의 로드만 사용 중으로 참조됩니다.

프로시저

단계 **1** Cisco Unified OS 관리에서 소프트웨어 업그레이드 > 장치 로드 관리를 선택합니다.
단계 **2** 검색 기준을 지정하고 찾기를 클릭합니다.
단계 **3** 삭제할 장치 로드를 선택합니다. 필요한 경우 여러 로드를 선택할 수 있습니다.
단계 **4** 선택한 로드 삭제를 클릭합니다.
단계 **5** 확인을 클릭합니다.

전화기 모델에 대한 기본 펌웨어 설정

이 절차를 사용하여 특정 전화기 모델에 대한 기본 펌웨어 로드를 설정합니다. 새 전화기를 등록하면 Cisco Unified Communications Manager는 전화기 구성이 전화기 구성 창에 지정된 펌웨어 로드를 제정의하지 않는 경우 전화기에 기본 펌웨어를 전송하려고 시도합니다.

참고 개별 전화기의 경우 전화기 구성 창에서 전화기 로드 이름 필드의 설정은 해당 특정 전화기에 대한 기본 펌웨어 로드를 재정의합니다.

시작하기 전에

TFTP 서버에 펌웨어가 로드되었는지 확인합니다.

프로시저

단계 **1** [Cisco Unified CM 관리]에서 장치 > 장치 설정 > 장치 기본값을 선택합니다.
Cisco Unified Communications Manager가 지원하는 다양한 전화기 모델에 대한 기본 펌웨어 로드를 표시하는 장치 기본값 구성 창이 나타납니다. 펌웨어는 로드 정보 열에 나타납니다.

단계 **2** 장치 유형 아래에서 기본 펌웨어를 할당하려는 전화기 모델을 찾습니다.

단계 **3** 관련 로드 정보 필드에 펌웨어 로드를 입력합니다.

단계 **4** (선택 사항) 해당 전화기 모델에 대한 기본 장치 풀 및 기본 전화기 템플릿을 입력합니다.

단계 **5** 저장을 클릭합니다.

전화기에 대한 펌웨어 로드 설정

특정 전화기에 대한 펌웨어 로드를 할당하려면 이 절차를 사용합니다. 장치 기본값 구성 창에 지정된 기본값 이외의 다른 펌웨어 로드를 사용하려면 이 작업을 수행할 수 있습니다.

참고 여러 전화기에 대해 버전을 지정하려는 경우 Bulk Administration Tool을 사용하여 CSV 파일 또는 쿼리를 사용하는 전화기 로드 이름 필드를 구성할 수 있습니다. 자세한 내용은 *Cisco Unified Communications Manager* 벌크 관리 설명서를 참조하십시오.

프로시저

단계 **1** Cisco Unified CM 관리에서 디바이스 > 전화기를 선택합니다.

단계 **2** 찾기를 클릭하고 개별 전화기를 선택합니다.

단계 **3** 전화기 로드 이름 필드에 펌웨어 이름을 입력합니다. 이 전화기에 대해 여기에 지정된 펌웨어 로드는 장치 기본값 구성 창에 지정된 기본 펌웨어 로드를 재정의합니다.

단계 **4** 전화기 구성 창의 나머지 필드를 완료합니다. 필드 및 해당 설정에 대한 도움이 필요한 경우 온라인 도움말을 참조하십시오.

단계 **5** 저장을 클릭합니다.

단계 **6** 구성 적용을 클릭하여 변경된 필드를 전화기에 적용할 수 있습니다.

로드 서버 사용

전화기에서 TFTP 서버가 아닌 서버에서 펌웨어 업데이트를 다운로드하도록 하려면 전화기의 전화기 구성 페이지에 "로드 서버"를 구성할 수 있습니다. 로드 서버는 다른 Cisco Unified Communications Manager 또는 타사 서버일 수 있습니다. 타사 서버는 TCP 포트 6970(기본 설정)의 HTTP 또는 UDP 기

반 TFTP 프로토콜을 통해 전화기가 요청하는 파일을 제공할 수 있어야 합니다. DX 제품군 Cisco TelePresence 장치와 같은 일부 전화기 모델만 펌웨어 업데이트를 위해 HTTP를 지원합니다.

참고 여러 전화기에 대해 로드 서버를 지정하려는 경우 Bulk Administration Tool을 사용하여 CSV 파일 또는 쿼리를 사용하는 로드 서버 필드를 구성할 수 있습니다. 자세한 내용은 *Cisco Unified Communications Manager* 벌크 관리 설명서를 참조하십시오.

프로시저

단계 **1** Cisco Unified CM 관리에서 디바이스 > 전화기를 선택합니다.

단계 **2** 찾기를 클릭하고 개별 전화기를 선택합니다.

단계 **3** 로드 서버 필드에 대체 서버의 IP 주소 또는 호스트 이름을 입력합니다.

단계 **4** 전화기 구성 창의 나머지 필드를 완료합니다. 필드 및 해당 설정에 대한 도움이 필요한 경우 온라인 도움말을 참조하십시오.

단계 **5** 저장을 클릭합니다.

단계 **6** 구성 적용을 클릭하여 변경된 필드를 전화기에 적용할 수 있습니다.

기본값 이외의 펌웨어 로드가 사용되는 장치 찾기

Unified Communications Manager의 [펌웨어 로드 정보] 창을 사용하여 해당 장치 유형에 대해 기본 펌웨어 로드가 사용되지 않는 장치를 신속하게 찾을 수 있습니다.

참고 각 장치에는 기본값을 오버라이드하는 펌웨어 로드가 개별적으로 할당될 수 있습니다.

다음 절차를 사용하여 기본 펌웨어 로드가 사용되지 않는 장치를 찾습니다.

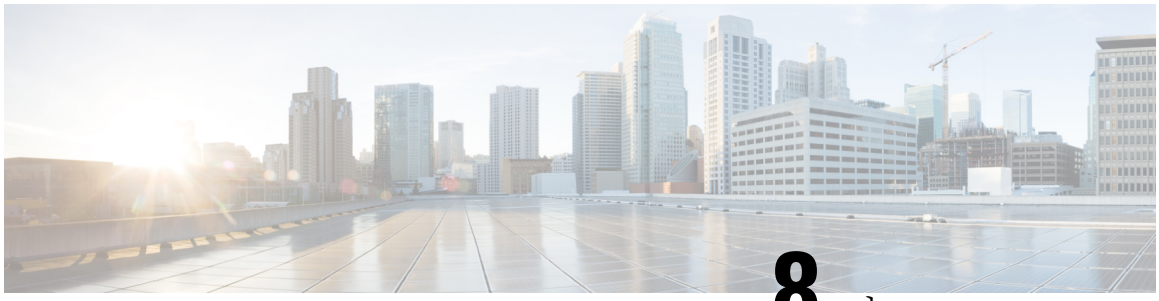
프로시저

단계 **1** 장치 > 장치 설정 > 펌웨어 로드 정보를 선택합니다.

페이지가 업데이트되어 펌웨어 로드가 필요한 장치 유형 목록이 표시됩니다. 각 장치 유형의 [기본 로드가 사용되지 않는 장치] 열은 기본값 이외의 로드가 사용되는 모든 장치의 구성 설정으로 연결됩니다.

단계 **2** 기본값이 아닌 장치 로드가 사용되는 특정 장치 유형의 장치 목록을 보려면 [기본 로드가 사용되지 않는 장치] 열에서 해당 장치 유형에 대한 항목을 클릭합니다.

기본 펌웨어 로드가 실행되지 않는 특정 장치 유형의 장치 목록이 있는 창이 열립니다.



8 장

인프라 장치 관리

- 인프라 관리 개요, 87 페이지
- 인프라 필수 구성 요소 관리, 87 페이지
- 인프라 작업 흐름 관리, 88 페이지

인프라 관리 개요

이 장에서는 위치 인식 기능의 일부로 스위치 및 무선 액세스 지점과 같은 네트워크 인프라 장치를 관리하는 작업에 대해 설명합니다. 위치 인식이 활성화되면 Cisco Unified Communications Manager 데이터베이스는 현재 각 스위치 또는 액세스 지점에 연결하는 엔드포인트의 목록을 포함하여 네트워크의 스위치 및 액세스 지점에 대한 상태 정보를 저장합니다.

엔드포인트와 인프라 장치 매핑을 사용하면 Cisco Unified Communications Manager 및 Cisco Emergency Responder에서 발신자의 물리적 위치를 확인할 수 있습니다. 예를 들어, 로밍 상황에 있는 동안 모바일 클라이언트에서 비상 통화를 하는 경우 Cisco Emergency Responder는 매핑을 사용하여 비상 서비스를 전송할 위치를 결정합니다.

데이터베이스에 저장된 인프라 정보도 인프라 사용량을 모니터링하는 데 도움이 됩니다. Unified Communications Manager 인터페이스에서 스위치 및 무선 액세스 지점 같은 네트워크 인프라 장치를 볼 수 있습니다. 또한 현재 특정 액세스 지점 또는 스위치에 연결하는 엔드포인트의 목록을 볼 수도 있습니다. 인프라 장치를 사용하지 않는 경우 인프라 장치의 추적을 비활성화할 수 있습니다.

인프라 필수 구성 요소 관리

Cisco Unified Communications Manager 인터페이스 내에서 무선 인프라를 관리하기 전에 위치 인식 기능을 구성해야 합니다. 유선 인프라의 경우 기능이 기본적으로 활성화됩니다.

구성에 대한 자세한 내용은 Cisco 통합 커뮤니케이션 매니저 기능 구성 설명서의 "위치 인식 구성" 장을 참조하십시오.

네트워크 인프라도 설치해야 합니다. 자세한 내용은 무선 LAN 컨트롤러, 액세스 지점 및 스위치 같은 인프라 장치와 함께 제공되는 하드웨어 설명서를 참조하십시오.

인프라 작업 흐름 관리

네트워크 인프라 장치를 모니터링하고 관리하려면 다음 작업을 수행합니다.

프로시저

	명령 또는 동작	목적
단계 **1**	인프라 장치에 대한 상태 보기, 88 페이지	무선 액세스 지점 또는 이더넷 스위치(관련 엔드포인트 목록 포함)의 현재 상태를 가져옵니다.
단계 **2**	인프라 디바이스에 대한 추적 비활성화, 89 페이지	사용되지 않는 스위치 또는 액세스 지점이 있는 경우 장치를 비활성으로 표시합니다. 시스템은 인프라 장치에 대한 상태 또는 연결된 엔드포인트의 목록을 업데이트하는 것을 중지합니다.
단계 **3**	비활성화된 인프라 장치에 대한 추적 활성화, 89 페이지	비활성 인프라 장치에 대한 추적을 시작합니다. Cisco Unified Communications Manager는 인프라 장치에 대한 상태 및 연결된 엔드포인트의 목록으로 데이터베이스 업데이트를 시작합니다.

인프라 장치에 대한 상태 보기

무선 액세스 지점 또는 이더넷 스위치 같은 인프라 장치의 현재 상태를 가져오려면 이 절차를 사용합니다. Cisco Unified Communications Manager 인터페이스 내에서 액세스 지점이나 스위치에 대한 상태를 보고 연결된 엔드포인트의 현재 목록을 볼 수 있습니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 고급 기능 > 디바이스 위치 추적 서비스 > 스위치 및 액세스 포인트를 선택합니다.

단계 **2** 찾기를 클릭합니다.

단계 **3** 상태를 원하는 스위치 또는 액세스 지점을 클릭합니다.
스위치 및 액세스 지점 구성 창에는 현재 액세스 지점 또는 스위치에 연결하는 엔드포인트의 목록을 포함한 현재 상태가 표시됩니다.

인프라 디바이스에 대한 추적 비활성화

스위치 또는 액세스 포인트 같은 특정 인프라 디바이스에 대한 추적을 제거하려면 이 절차를 사용합니다. 사용되지 않는 스위치 또는 액세스 포인트에 대해 이 작업을 수행할 수 있습니다.

참고 인프라 디바이스에 대한 추적을 제거하는 경우 디바이스는 데이터베이스에 남지만 비활성화됩니다. Cisco Unified Communications Manager는 인프라 디바이스에 연결된 엔드포인트의 목록을 포함하여 디바이스의 상태를 더 이상 업데이트하지 않습니다. 스위치 및 액세스 포인트 창의 관련 링크 드롭다운에서 비활성 스위치와 액세스 포인트를 볼 수 있습니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 고급 기능 > 디바이스 위치 추적 서비스 > 스위치 및 액세스 포인트를 선택합니다.

단계 **2** 찾기를 클릭하고 추적을 중지하려는 스위치 또는 액세스 포인트를 선택합니다.

단계 **3** 선택한 항목 비활성화를 클릭합니다.

비활성화된 인프라 장치에 대한 추적 활성화

비활성화된 비활성 인프라 장치에 대한 추적을 시작하려면 이 절차를 사용합니다. 스위치 또는 액세스 지점이 활성화되면 Cisco Unified Communications Manager는 스위치 또는 액세스 지점에 연결하는 엔드포인트의 목록을 포함하여 상태를 동적으로 추적하기 시작합니다.

시작하기 전에

위치 인식을 구성해야 합니다. 자세한 내용은 *Cisco Unified Communications Manager* 시스템 구성 설명서의 "위치 인식" 장을 참조하십시오.

프로시저

단계 **1** Cisco Unified CM 관리에서 고급 기능 > 디바이스 위치 추적 서비스 > 스위치 및 액세스 포인트를 선택합니다.

단계 **2** 관련 링크에서 비활성 스위치 및 액세스 지점을 선택하고 이동을 클릭합니다.
비활성 스위치 및 액세스 지점 찾기 및 나열 창에 추적되지 않는 인프라 장치가 표시됩니다.

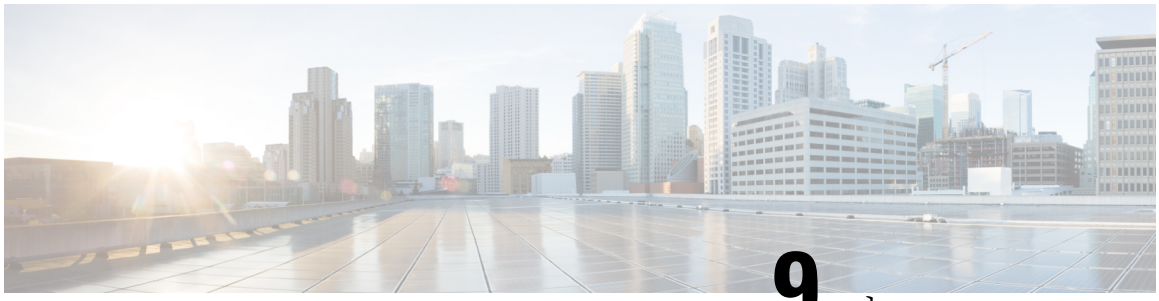
단계 **3** 추적을 시작하려는 스위치 또는 액세스 지점을 선택합니다.

단계 **4** 선택한 항목 재활성화를 클릭합니다.

IV 부

시스템 관리

- 시스템 상태 모니터링, 93 페이지
- 알람, 99 페이지
- 감사 로그, 117 페이지
- 통화 홈, 133 페이지
- 서비스 가용성 커넥터, 145 페이지
- 단순 네트워크 관리 프로토콜, 151 페이지
- 서비스, 193 페이지
- 추적, 229 페이지
- 사용 레코드 보기, 261 페이지
- 엔터프라이즈 매개 변수 관리, 267 페이지
- 서버 관리, 271 페이지



9 장

시스템 상태 모니터링

- 클러스터 노드 상태 보기, 93 페이지
- 하드웨어 상태 보기, 93 페이지
- 네트워크 상태 보기, 94 페이지
- 설치된 소프트웨어 보기, 94 페이지
- 시스템 상태 보기, 95 페이지
- IP 환경 설정 보기, 95 페이지
- 마지막 로그인 세부 정보 보기, 95 페이지
- 노드 Ping, 96 페이지
- 서비스 매개 변수 표시 , 96 페이지
- 네트워크 DNS 구성, 98 페이지

클러스터 노드 상태 보기

클러스터의 노드에 대한 정보를 표시하려면 이 절차를 사용합니다.

프로시저

단계 **1** Cisco Unified Operating System 관리에서 표시 > 클러스터를 선택합니다.

단계 **2** 클러스터 창에서 필드를 검토합니다. 필드에 대한 자세한 내용은 온라인 도움말을 참조하십시오.

하드웨어 상태 보기

이 절차를 사용하여 시스템의 하드웨어 상태 및 하드웨어 리소스에 대한 정보를 표시합니다.

프로시저

단계 **1** Cisco Unified Operating System 관리에서 표시 > 하드웨어를 선택합니다.

단계 **2** 하드웨어 상태 창에서 필드를 검토합니다. 필드에 대한 자세한 내용은 온라인 도움말을 참조하십시오.

네트워크 상태 보기

이더넷 및 DNS 정보 같은 시스템의 네트워크 상태를 표시하려면 이 절차를 사용합니다.

표시되는 네트워크 상태 정보는 네트워크 장애 허용 오차가 활성화되었는지 여부에 따라 다릅니다.

- 네트워크 장애 허용 오차가 활성화된 경우 이더넷 포트 0이 실패하면 이더넷 포트 1이 자동으로 통신 네트워크를 관리합니다.
- 네트워크 장애 허용 오차가 활성화된 경우 이더넷 0, 이더넷 1 Bond 0에 대한 네트워크 상태 정보가 표시됩니다.
- 네트워크 장애 허용 오차가 활성화되지 않은 경우 이더넷 0에 대한 상태 정보만 표시됩니다.

프로시저

단계 **1** Cisco Unified Operating System 관리에서 표시 > 네트워크를 선택합니다.

단계 **2** 네트워크 구성 창에서 필드를 검토합니다. 필드에 대한 자세한 내용은 온라인 도움말을 참조하십시오.

설치된 소프트웨어 보기

소프트웨어 버전 및 설치된 소프트웨어 패키지에 대한 정보를 보려면 이 절차를 사용합니다.

프로시저

단계 **1** Cisco Unified Operating System 관리에서 표시 > 소프트웨어를 선택합니다.

단계 **2** 소프트웨어 패키지 창에서 필드를 검토합니다. 필드에 대한 자세한 내용은 온라인 도움말을 참조하십시오.

시스템 상태 보기

로캘, 가동 시간, CPU 사용 및 메모리 사용에 대한 정보 같이 전체 시스템 상태를 표시하려면 이 절차를 사용합니다.

프로시저

단계 **1** Cisco Unified Operating System 관리에서 표시 > 시스템을 선택합니다.

단계 **2** 시스템 상태 창에서 필드를 검토합니다. 필드에 대한 자세한 내용은 온라인 도움말을 참조하십시오.

IP 환경 설정 보기

이 절차를 사용하여 시스템에 사용할 수 있는 등록된 포트 목록을 표시합니다.

프로시저

단계 **1** Cisco Unified Operating System 관리에서 표시 > **IP** 환경 설정을 선택합니다.

단계 **2** (선택 사항) 레코드를 필터링하거나 검색하려면 다음 작업 중 하나를 수행합니다.

- 첫 번째 목록에서 검색 매개 변수를 선택합니다.
- 두 번째 목록에서 검색 패턴을 선택합니다.
- 적절한 검색 텍스트를 지정합니다(해당하는 경우).

단계 **3** 찾기를 클릭합니다.

단계 **4** 시스템 상태 창에 나타나는 필드를 검토합니다. 필드에 대한 자세한 내용은 온라인 도움말을 참조하십시오.

마지막 로그인 세부 정보 보기

최종 사용자(로컬 및 LDAP 인증서) 및 관리자가 Cisco Unified Communications Manager 또는 IM and Presence Service용 웹 애플리케이션에 로그인하면 메인 애플리케이션 창에 최근 성공/실패한 로그인 세부 정보가 표시됩니다.

SAML SSO 기능을 사용하여 로그인하는 사용자는 마지막 성공적인 시스템 로그인 정보만 볼 수 있습니다. 사용자는 IdP(ID 공급자) 애플리케이션을 참조하여 실패한 SAML SSO 로그인 정보를 추적할 수 있습니다.

다음 웹 애플리케이션은 로그인 시도 정보를 표시합니다.

- Cisco Unified Communications Manager:
  - Cisco Unified CM 관리
  - Cisco Unified Reporting
  - Cisco 통합 서비스 가용성
- IM and Presence Service
  - Cisco Unified CM IM and Presence 관리
  - Cisco Unified IM and Presence 보고
  - Cisco Unified IM and Presence Service 가용성

관리자만 로그인하여 Cisco Unified Communications Manager의 다음 웹 애플리케이션에 대한 마지막 로그인 세부 정보를 볼 수 있습니다.

- 재해 복구 시스템
- Cisco Unified OS Administration

노드 Ping

네트워크의 다른 노드를 Ping하려면 Ping 유틸리티를 사용합니다. 그 결과는 장치 연결을 확인하거나 문제 해결에 도움이 될 수 있습니다.

프로시저

단계 **1** Cisco Unified Operating System 관리에서 서비스 > **Ping**을 선택합니다.

단계 **2** **Ping** 구성 창에서 필드를 구성합니다. 필드 및 해당 구성 옵션에 대한 자세한 내용은 온라인 도움말을 참조하십시오.

단계 **3** **Ping**을 선택합니다.

Ping 결과가 표시됩니다.

서비스 매개 변수 표시

클러스터의 모든 서버에서 특정 서비스에 속한 모든 서비스 매개 변수를 비교해야 할 수 있습니다. 또한 동기화되지 않은 매개 변수(즉, 값이 서버 간에 다른 서비스 매개 변수)나 제안 값에서 수정된 매개 변수만 표시해야 할 수도 있습니다.

다음 절차에 따라 클러스터의 모든 서버에서 특정 서비스의 서비스 매개 변수를 표시합니다.

프로시저

단계 **1** 시스템 > 서비스 매개 변수를 선택합니다.

단계 **2** [서버] 드롭다운 목록 상자에서 서버를 선택합니다.

단계 **3** [서비스] 드롭다운 목록 상자에서 클러스터의 모든 서버에서 서비스 매개 변수를 표시할 서비스를 선택합니다.

참고 [서비스 매개 변수 구성] 창에 서비스(활성 또는 비활성)가 모두 표시됩니다.

단계 **4** 표시되는 [서비스 매개 변수 구성] 창의 [관련 링크] 드롭다운 목록 상자에서 [모든 서버에 대한 매개 변수]를 선택한 다음 [이동]을 클릭합니다.

[모든 서버에 대한 매개 변수] 창이 표시됩니다. 목록에 현재 서비스에 대한 모든 매개 변수가 사전순으로 표시됩니다. 각 매개 변수의 경우 제안 값은 매개 변수 이름 옆에 표시됩니다. 각 매개 변수 이름 아래에 이 매개 변수가 포함된 서버의 목록이 표시됩니다. 각 서버 이름 옆에는 현재 서버의 이 매개 변수에 대한 현재 값이 표시됩니다.

지정된 매개 변수에 대해 서버 이름이나 현재 매개 변수 값을 클릭하여 해당 서비스 매개 변수 창에 연결하여 값을 변경합니다. [모든 서버에 대한 매개 변수] 창 사이를 이동하려면 [이전] 및 [다음]을 클릭합니다.

단계 **5** 동기화되지 않은 매개 변수를 표시해야 하는 경우 [관련 링크] 드롭다운 목록 상자에서 [모든 서버에 대한 동기화되지 않은 매개 변수]를 선택한 다음 [이동]을 클릭합니다.

[모든 서버에 대한 동기화되지 않은 매개 변수] 창이 표시됩니다. 현재 서비스에 대해 서버 간에 값이 다른 서비스 매개 변수가 사전순으로 표시됩니다. 각 매개 변수의 경우 제안 값은 매개 변수 이름 옆에 표시됩니다. 각 매개 변수 이름 아래에 이 매개 변수가 포함된 서버의 목록이 표시됩니다. 각 서버 이름 옆에는 현재 서버의 이 매개 변수에 대한 현재 값이 표시됩니다.

지정된 매개 변수에 대해 서버 이름이나 현재 매개 변수 값을 클릭하여 해당 서비스 매개 변수 창에 연결하여 값을 변경합니다. [모든 서버에 대한 동기화되지 않은 매개 변수] 창 사이를 이동하려면 [이전] 및 [다음]을 클릭합니다.

단계 **6** 제안 값에서 수정된 서비스 매개 변수를 표시해야 하는 경우 [관련 링크] 드롭다운 목록 상자에서 [모든 서버에 대한 수정된 매개 변수]를 선택한 다음 [이동]을 클릭합니다.

[모든 서버에 대한 수정된 매개 변수] 창이 표시됩니다. 현재 서비스에 대해 값이 제안 값과 다른 서비스 매개 변수가 사전순으로 표시됩니다. 각 매개 변수에 대해 제안된 값이 매개 변수 이름 옆에 표시됩니다. 각 매개변수 이름 아래에 제안된 값과 다른 값을 가진 서버 목록이 표시됩니다. 각 서버 이름 옆에는 현재 서버의 이 매개 변수에 대한 현재 값이 표시됩니다.

지정된 매개 변수에 대해 서버 이름이나 현재 매개 변수 값을 클릭하여 해당 서비스 매개 변수 창에 연결하여 값을 변경합니다. [모든 서버에 대한 수정된 매개 변수] 창 사이를 이동하려면 [이전] 및 [다음]을 클릭합니다.

네트워크 **DNS** 구성

이 절차를 사용하여 네트워크 DNS를 설정합니다.

참고 Cisco Unified CM 관리의 DHCP 구성 창을 통해 DNS 기본 및 보조 서버를 할당할 수도 있습니다.

프로시저

단계 **1** 명령줄 인터페이스에 로그인합니다.

단계 **2** DNS 서버를 할당하려면 다음 퍼블리셔 노드에서 다음 명령 중 하나를 실행합니다.

- 기본 DNS 서버를 할당하려면 **set network dns primary <ip_address>**를 실행합니다.
- 보조 DNS 서버를 할당하려면 **set network dns secondary <ip_address>**를 실행합니다.

단계 **3** 추가 DNS 옵션을 할당하려면 **set network dns options [timeout| seconds] [attempts| number] [rotate]**를 실행합니다.

- Timeout은 DNS 시간 초과를 설정합니다.
- Seconds는 시간 초과 기간의 초 수입니다.
- Attempts는 DNS 요청을 시도하는 횟수를 설정합니다.
- Number는 시도 횟수를 지정합니다.
- Rotate는 시스템이 구성된 DNS 서버 간에 회전하고 부하를 분산시킵니다.

예를 들어, set network dns options timeout 60 attempts 4 rotate

이 명령을 실행한 후 서버가 재부팅됩니다.

10 장

알람

- 개요, 99 페이지
- 알람 구성, 100 페이지
- 알람 정의, 101 페이지
- 알람 정보, 102 페이지
- 알람 설정, 102 페이지
- 알람 서비스 설정, 103 페이지
- 알람 정의 및 사용자 정의 설명 추가, 110 페이지

개요

Cisco 통합 서비스 가용성 및 Cisco Unified IM and Presence Service 가능성은 시스템과 관련된 문제를 해결할 수 있도록 런타임 상태 및 시스템 상태에 대한 정보를 제공합니다. 예를 들어 재해 복구 시스템과 관련된 문제를 식별합니다. 설명 및 권장 작업을 포함하는 알람 정보에는 애플리케이션 이름, 시스템 이름 등도 포함되며 문제 해결을 수행하고 클러스터에도 적용 될 수 있습니다.

여러 위치에 알람 정보를 전송하도록 알람 인터페이스를 구성하고, 각 위치 마다 고유한 알람 이벤트 수준(디버그에서 비상으로)을 가질 수 있습니다. 알람을 통해 Syslog 뷰어(로컬 syslog), Syslog 파일(원격 Syslog), SDL 추적 로그 파일(Cisco CallManager 및 CTIManager 서비스에만 해당) 또는 모든 대상에 지시할 수 있습니다.

서비스에서 알람이 발생하면 알람 인터페이스는 알람 정보를 사용자가 구성하는위치, 알람 정의의 라우팅 목록(예: SDI 추적)에 지정된 위치로 전송합니다. 시스템은 SNMP 트랩의 경우와 같이 알람 정보를 착신 전환하거나 최종 대상(예: 로그 파일)에 알람 정보를 쓸 수 있습니다.

특정 노드에 대한 Cisco Database Layer Monitor와 같은 서비스에 대한 알람을 구성하거나 클러스터의 모든 노드에서 특정 서비스에 대한 알람을 구성할 수 있습니다.

참고 Cisco Unity Connection SNMP는 트랩을 지원하지 않습니다.

팁 원격 Syslog 서버의 경우 다른 서버에서 Syslog 메시지를 받을 수 없는 Unified Communications Manager 서버를 지정하지 마십시오.

Cisco Unified Real-Time Monitoring Tool(Unifed RTMT)에서 추적 및 로그 센트럴 옵션을 사용하여 SDL 추적 로그 파일에 전송되는 알람을 수집합니다(Cisco Cisco CallManager 및 CTIManager 서비스에만 해당). Unifed RTMT에서 SysLog 뷰어를 사용하여 로컬 sysLog로 전송되는 알람 정보를 볼 수 있습니다.

알람 구성

Cisco 통합 서비스 가용성에서 Cisco Database Layer Monitor와 같은 서비스에 대한 알람을 구성할 수 있습니다. 그런 다음 시스템에서 알람 정보를 전송할 위치(예: Syslog 뷰어(로컬 syslog))를 구성합니다. 이 옵션을 사용하면 다음 작업을 수행할 수 있습니다.

- 특정 서버 또는 모든 서버에서 서비스에 대한 알람 구성(Unified Communications Manager 클러스터에만 해당)
- 구성된 서비스 또는 서버에 대해 서로 다른 원격 syslog 서버 구성
- 서로 다른 대상에 대해 서로 다른 알람 이벤트 수준 설정 구성

Cisco Unified Communications Manager 관리의 Cisco Syslog Agent 엔터프라이즈 매개 변수를 사용하여 구성된 임계값을 충족하거나 초과하는 모든 알람을 원격 syslog 서버 이름 및 Syslog 심각도의 두 가지 설정을 사용하여 원격 syslog 서버에 전달할 수 있습니다. 이러한 Cisco Syslog 에이전트 매개 변수에 액세스하려면 구성에 해당하는 창으로 이동합니다.

Unified Communications Manager	Cisco Unified Communications Manager 관리에서 시스템 > 엔터프라이즈 매개 변수를 선택합니다.
Cisco Unity Connection	Cisco Unity Connection 관리에서 시스템 설정 > 엔터프라이즈 매개 변수를 선택합니다.
Cisco IM and Presence	Cisco Unified Communications Manager IM and Presence 관리에서 시스템 > 엔터프라이즈 매개 변수를 선택합니다.

알람에는 시스템(OS/하드웨어 플랫폼), 애플리케이션(서비스) 및 보안 알람이 포함됩니다.

참고 Cisco 통합 서비스 가용성에서 Cisco Syslog Agent 알람 엔터프라이즈 매개 변수 및 애플리케이션(서비스) 알람을 모두 구성하는 경우 시스템에서 원격 syslog에 동일한 알람을 두 번 전송할 수 있습니다.

애플리케이션 알람에 대해 로컬 syslog가 활성화된 경우, 시스템은 알람이 로컬 syslog 임계값과 엔터프라이즈 임계값을 둘 다 초과하는 경우에만 엔터프라이즈 원격 syslog 서버로 알람을 전송합니다.

Cisco 통합 서비스 가용성에서 원격 syslog도 활성화된 경우, 시스템은 Cisco 통합 서비스 가용성에서 구성된 애플리케이션 임계값을 사용하여 원격 syslog 서버로 알람을 전달합니다. 이 경우 알람은 원격 syslog 서버로 두 번 전송됩니다.

이벤트 수준/심각도 설정은 시스템에서 수집하는 알람 및 메시지에 대한 필터링 메커니즘을 제공합니다. 이 설정을 사용하면 Syslog 및 추적 파일이 오버로드되지 않도록 할 수 있습니다. 시스템은 구성된 임계값을 초과하는 알람 및 메시지만 전달합니다.

알람 및 이벤트에 연결된 심각도 수준에 대한 자세한 내용은 알람 정의, 101 페이지의 내용을 참조하십시오.

알람 정의

참조에 사용되는 알람 정의는 알람 메시지, 의미 및 복구 방법에 대해 설명합니다. 알람 정보를 보려면 알람 정의 창에서 검색합니다. 서비스 특정 알람 정의를 클릭하면 추가된 사용자 정의 텍스트를 포함하여 알람 정보에 대한 설명과 권장 작업이 표시됩니다.

서비스 가용성 GUI에 표시되는 모든 알람의 알람 정의를 검색할 수 있습니다. 문제 해결에 도움이 되도록 해당 카탈로그에 있는 정의에는 알람 이름, 설명, 설명, 권장 조치, 심각도, 매개 변수 및 모니터가 포함됩니다.

시스템에서 알람을 생성하는 경우 알람 정보에 알람 정의 이름이 사용되므로 알람을 식별할 수 있습니다. 알람 정의에서는 시스템에서 알람 정보를 보낼 수 있는 위치를 지정하는 라우팅 목록을 볼 수 있습니다. 라우팅 목록에는 알람 구성 창에서 구성할 수 있는 위치와 상호 관련된 다음 위치가 포함될 수 있습니다.

- Unified Communications Manager만 해당: SDL - 이 옵션에 대해 알람을 활성화하고 알람 구성 창에서 이벤트 수준을 지정하는 경우 시스템에서 SDL 추적에 알람 정보를 전송합니다.
- SDI - 이 옵션에 대한 알람을 활성화하고 알람 구성 창에서 이벤트 수준을 지정하는 경우 시스템에서 SDI 추적에 알람 정보를 전송합니다.
- Sys 로그 - 이 옵션에 대해 알람을 활성화하고 알람 구성 창에서 이벤트 수준을 지정하고 원격 syslog 서버에 대한 서버 이름 또는 IP 주소를 입력하는 경우 시스템에서 원격 syslog 서버에 알람 정보를 전송합니다.
- 이벤트 로그 - 이 옵션에 대해 알람을 활성화하고 알람 구성 창에서 이벤트 수준을 지정하는 경우 시스템에서 Cisco Unified Real-Time Monitoring Tool(Unified RTMT)의 syslog 뷰어에서 볼 수 있는 로컬 syslog에 알람 정보를 전송합니다.

- 데이터 수집기 - 시스템에서 알림 목적으로만 알람 정보를 실시간 정보 시스템(RIS Data Collector)에 전송합니다. 알람 구성 창에서는 이 옵션을 구성할 수 없습니다.
- SNMP 트랩 - 시스템에서 SNMP 트랩을 생성합니다. 알람 구성 창에서는 이 옵션을 구성할 수 없습니다.

팁 SNMP 트랩 위치가 라우팅 목록에 표시되면 시스템은 CISCO-CCM-MI의 정의에 따라 트랩을 생성하는 CCM MIB SNMP 에이전트에게 알람 정보를 전달합니다.

알람 구성 창의 특정 위치에 대해 구성된 알람 이벤트 수준이 알람 정의에 나열된 심각도보다 낮거나 같으면 시스템에서 알람이 전송됩니다. 예를 들어, 알람 정의의 심각도가 WARNING_ALARM이고 알람 구성 창에서 특정 대상에 대한 알람 이벤트 수준을 경고, 알림, 정보 또는 디버그(낮은 이벤트 수준)로 구성하는 경우 시스템에서 해당 대상으로 알람을 전송합니다. 알람 이벤트 수준을 비상, 알림, 위험 또는 오류로 구성하는 경우 시스템은 해당 위치에 알람을 전송하지 않습니다.

각 알람 정의에 경우 추가 설명 또는 권장 사항을 포함할 수 있습니다. 모든 관리자가 추가된 정보에 액세스할 수 있습니다. 알람 세부 정보 창에 표시되는 정보를 사용자 정의 텍스트 창에 직접 입력할 수 있습니다. 표준 가로 및 세로 스크롤 막대는 스크롤을 지원합니다. Cisco 통합 서비스 가용성는 데이터베이스에 정보를 추가합니다.

알람 정보

알람 정보를 보고 문제가 있는지 여부를 확인할 수 있습니다. 알람 정보를 보는 데 사용하는 방법은 알람을 구성할 때 선택한 대상에 따라 달라 집니다. Unified RTMT 또는 텍스트 편집기를 사용하여 SDL 추적 로그 파일(Unified Communications Manager)에 전송되는 알람 정보를 볼 수 있습니다. Unified RTMT의 SysLog 뷰어를 사용하여 로컬 syslog로 전송되는 알람 정보를 볼 수 있습니다.

알람 설정

다음 단계에 따라 알람을 구성합니다.

프로시저

단계 **1** Cisco Unified Communications Manager 관리, Cisco Unity Connection 관리 또는 Cisco Unified IM and Presence 관리에서 Cisco Syslog Agent 엔터프라이즈 매개 변수를 구성하여 시스템, 애플리케이션(서비스) 및 보안 알람/메시지를 지정한 원격 Syslog 서버로 전송합니다. 이 단계를 생략하면 Cisco 통합 서비스 가용성에서 애플리케이션(서비스) 알람/메시지를 구성할 수 있습니다.

단계 **2** Cisco 통합 서비스 가용성에서 수집하려는 애플리케이션(서비스) 알람 정보에 대한 서버, 서비스, 대상 및 이벤트 수준을 구성합니다.

단계 **3** (선택 사항) 알람에 정의를 추가합니다.

- 모든 서비스는 SDI 로그로 이동할 수 있으나 추적에도 구성되어야 합니다.
- 모든 서비스는 SysLog 뷰어로 이동할 수 있습니다.
- Unified Communications Manager만 해당: Cisco CallManager 및 Cisco CTIManager 서비스에서만 SDL 로그를 사용합니다.
- 원격 Syslog 서버에 syslog 메시지를 보내려면 원격 Syslog 대상을 확인하고 호스트 이름을 지정합니다. 원격 서버 이름을 구성하지 않으면 Cisco Unified Serviceability에서 Syslog 메시지를 원격 syslog 서버로 보내지 않습니다.

팁 Unified Communications Manager 서버를 원격 Syslog 서버로 구성하지 마십시오.

단계 **4** SDL 추적 파일을 알람 대상으로 선택한 경우에는 추적을 수집하고 Unified RTMT의 추적 및 로그 센트럴 옵션을 사용하여 정보를 확인합니다.

단계 **5** 로컬 syslog를 알람 대상으로 선택한 경우에는 Unified RTMT의 SysLog 뷰어에서 알람 정보를 확인합니다.

단계 **6** 설명 및 권장 작업에 대한 해당 알람 정의를 참조하십시오.

알람 서비스 설정

Syslog 에이전트 엔터프라이즈 매개 변수

구성된 임계값을 초과하는 시스템, 애플리케이션 및 보안 알람/메시지를 사용자가 지정한 원격 Syslog 서버로 전송하도록 Cisco Syslog 에이전트 엔터프라이즈 매개 변수를 구성할 수 있습니다. Cisco Syslog 에이전트 매개 변수에 액세스하려면 구성에 해당하는 창으로 이동합니다.

Unified Communications Manager	Cisco Unified Communications Manager 관리에서 시스템 > 엔터프라이즈 매개 변수를 선택합니다.
Cisco Unity Connection	Cisco Unity Connection 관리에서 시스템 설정 > 엔터프라이즈 매개 변수를 선택합니다.
Cisco IM and Presence	Cisco Unified Communications Manager IM and Presence 관리에서 시스템 > 엔터프라이즈 매개 변수를 선택합니다.

그런 다음, 원격 syslog 서버 이름(원격 Syslog 서버 이름 1, 원격 Syslog 서버 이름 2, 원격 Syslog 서버 이름 3, 원격 Syslog 서버 이름 4 및 원격 Syslog 서버 이름 5) 및 syslog 심각도를 구성합니다. 서버 이름을 구성하는 동안 유효한 IP 주소를 지정했는지 확인합니다. syslog 심각도는 구성하는 모든 원격 syslog 서버에 적용됩니다. 그리고 저장을 클릭합니다. 유효한 값을 입력하려면 **?** 버튼을 클릭합니다. 서버 이름을 지정하지 않은 경우 Cisco 통합 서비스 가용성는 Syslog 메시지를 전송하지 않습니다.

주의 Unified Communications Manager에서 원격 syslog 서버를 구성하는 동안에는 원격 syslog 서버 이름에 대해 중복 항목을 추가하지 마십시오. 중복 항목을 추가하는 경우 Cisco Syslog 에이전트는 원격 syslog 서버에 메시지를 보내는 동안 중복 항목을 무시합니다.

참고 Unified Communications Manager를 원격 syslog 서버로 구성하지 마십시오. Unified Communications Manager 노드는 다른 서버의 Syslog 메시지를 수락하지 않습니다.

알람 서비스 설정

이 섹션에서는 Cisco 통합 서비스 가용성를 통해 관리하는 기능 또는 네트워크 서비스에 대한 알람을 추가하거나 업데이트하는 방법에 대해 설명합니다.

참고 SNMP 트랩 및 카탈로그 구성은 변경하지 않는 것이 좋습니다.

Cisco Unity Connection은 Cisco Unity Connection Serviceability에서 사용할 수 있는 알람도 사용합니다. Cisco Unity Connection 서비스 가용성에서는 알람을 구성할 수 없습니다. 자세한 내용은 *Cisco Unity Connection Serviceability* 관리 설명서를 참조하십시오.

표준 레지스트리 편집기 사용 방법에 대한 자세한 내용은 온라인 OS 설명서를 참조하십시오.

프로시저

단계 **1** 알람 > 구성을 선택합니다.

[알람 구성] 창이 표시됩니다.

단계 **2** 서버 드롭다운 목록에서 알람을 구성하려는 서버를 선택합니다. 그런 다음 이동을 클릭합니다.

단계 **3** 서비스 그룹 드롭다운 목록에서 알람을 구성하려는 서비스(예: 데이터베이스 및 관리 서비스)를 선택합니다. 그런 다음 이동을 클릭합니다.

팁 서비스 그룹에 해당하는 서비스 목록은 서비스 그룹을 참조하십시오.

단계 **4** 서비스 드롭다운 목록에서 알람을 구성하려는 서비스를 선택합니다. 그런 다음 이동을 클릭합니다.

서비스 그룹 및 구성을 지원하는 서비스만 표시됩니다.

팁 드롭다운 목록에 활성 및 비활성 서비스가 표시됩니다.

알람 구성 창에는 선택한 서비스에 대한 이벤트 수준이 표시되는 알람 모니터 목록이 표시됩니다. 또한 모든 노드에 적용 확인란이 표시됩니다.

단계 **5** Unified Communications Manager만 해당: 이렇게 하려면 구성에서 클러스터를 지원하는 경우 모든 노드에 적용 확인란을 선택하여 서비스에 대한 알람 구성을 클러스터의 모든 노드에 적용할 수 있습니다.

단계 **6** 모니터링 및 이벤트 수준에 대한 설명을 포함하는 알람 구성 설정에 설명된 대로 설정을 구성합니다.

단계 **7** 구성을 저장하려면 저장 버튼을 클릭합니다.

참고 기본값을 설정하려면 기본값 설정 버튼을 클릭합니다. 그런 다음 저장을 클릭합니다.

다음에 수행할 작업

팁 알람 구성 창의 특정 대상에 대해 구성된 알람 이벤트 수준이 알람 정의에 나열된 심각도보다 낮거나 같으면 시스템에서 알람이 전송됩니다. 예를 들어, 알람 정의의 심각도가 WARNING_ALARM이고 알람 구성 창에서 특정 대상에 대한 알람 이벤트 수준을 경고, 알림, 정보 또는 디버그(낮은 이벤트 수준)로 구성하는 경우 시스템에서 해당 대상으로 알람을 전송합니다. 알람 이벤트 수준을 비상, 알림, 위험 또는 오류(높은 이벤트 수준)로 구성하는 경우 시스템은 해당 위치에 알람을 전송하지 않습니다.

Cisco Extension Mobility 애플리케이션 서비스, Cisco Unified Communications Manager Assistant 서비스, Cisco Extension Mobility 서비스 및 Cisco Web Dialer 서비스에 대한 알람 정의에 액세스하려면 알람 정의에 설명된 알람 메시지 정의 창에서 **JavaApplications** 카탈로그를 선택합니다.

Cisco Tomcat을 사용하는 알람 서비스 설정

다음 서비스는 알람 생성을 위해 Cisco Tomcat을 사용합니다.

- Cisco Extension Mobility Application
- Cisco IP Manager Assistant
- Cisco Extension Mobility
- Cisco Web Dialer

시스템 로그인 알람 인증에 실패하여 Cisco Tomcat이 사용됩니다. 이러한 서비스에 대한 알람을 생성하려면 다음 절차를 수행합니다.

프로시저

단계 **1** Cisco 통합 서비스 가용성에서 알람 > 구성을 선택합니다.

단계 **2** 서버 드롭다운 목록에서 알람을 구성하려는 서버를 선택합니다. 그런 다음 이동을 클릭합니다.

단계 **3** 서비스 그룹 드롭다운 목록에서플랫폼 서비스를 선택한 다음 이동을 선택합니다.

단계 **4** 서비스 드롭다운 목록에서 **Cisco Tomcat**을 선택한 다음 이동을 클릭합니다.

단계 **5** Unified Commuications Manager만 해당: 구성에서 클러스터를 지원하는 경우 모든 노드에 적용 확인란을 선택하여 서비스에 대한 알람 구성을 클러스터의 모든 노드에 적용할 수 있습니다.

단계 **6** 모니터링 및 이벤트 수준에 대한 설명을 포함하는 알람 구성 설정에 설명된 대로 설정을 구성합니다.

단계 **7** 구성을 저장하려면 저장 버튼을 클릭합니다.

서비스 그룹

다음 표에는 알람 구성 창의 서비스 그룹 드롭다운 목록에 있는 옵션에 해당하는 서비스가 나열되어 있습니다.

참고 나열된 모든 서비스 그룹 및 서비스가 모든 시스템 구성에 적용되는 것은 아닙니다.

표 ***6:*** 알람 구성의 서비스 그룹

서비스 그룹	서비스
CM 서비스	Cisco CTIManager, Cisco CallManager, Cisco DHCP 모니터 서비스, Cisco Dialed Number Analyzer, Cisco Dialed Number Analyzer 서버, Cisco Extended Functions, Cisco IP Voice Media Streaming 앱, Cisco Messaging Interface , Cisco 헤드셋 서비스 및 Cisco TFTP
CTI 서비스	Cisco IP Manager Assistant 및 Cisco WebDialer 웹 서비스
CDR 서비스	Cisco CAR Scheduler, Cisco CDR Agent 및 Cisco CDR Repository Manager
데이터베이스 및 관리 서비스	Cisco Bulk Provisioning 서비스 및 Cisco Database Layer Monitor
성능 및 모니터링 서비스	Cisco AMC Service 및 Cisco RIS Data Collector
보안 서비스	Cisco Certificate Authority 프록시 기능 및 Cisco 인증서 만료 모니터
디렉터리 서비스	Cisco DirSync
백업 및 복원 서비스	Cisco DRF Local 및 Cisco DRF Master
시스템 서비스	Cisco Trace Collection Service
플랫폼 서비스	Cisco Tomcat 및 Cisco Smart License Manager
위치 기반 추적 서비스	Cisco Wireless Controller 동기화 서비스

알람 구성 설정

다음 표에서는 서비스에서 설정을 지원하지 않는 경우에도 모든 알람 구성 설정에 대해 설명합니다.

표 *7:* 알람 구성 설정

이름	설명
서버	드롭다운 목록에서 알람을 구성하려는 서버(노드)를 선택합니다. 그런 다음 이동을 클릭합니다.
서비스 그룹	Cisco Unity Connection는 데이터베이스 및 관리 서비스, 성능 및 모니터링 서비스, 백업 및 복원 서비스, 시스템 서비스, 플랫폼 서비스 등의 서비스 그룹만 지원합니다. 드롭다운 목록에서 알람을 구성하려는 서비스(예: 데이터베이스 및 관리 서비스)를 선택합니다. 그런 다음 이동을 클릭합니다.
서비스	서비스 드롭다운 목록에서 알람을 구성하려는 서비스를 선택합니다. 그런 다음 이동을 클릭합니다. 서비스 그룹 및 구성을 지원하는 서비스만 표시됩니다. 팁 드롭다운 목록에 활성 및 비활성 서비스가 모두 표시됩니다.
Unified Communications Manager 및 Cisco Unified Communications Manager IM and Presence Service만 해당: 모든 노드에 적용	클러스터에 있는 모든 노드의 서비스에 대한 알람 설정을 적용하려면 확인란을 선택합니다.
로컬 Syslog에 대해 알람 활성화	SysLog 뷰어는 알람 대상의 역할을합니다. 프로그램은 SysLog 뷰어 내 애플리케이션 로그에 오류를 기록하고 알람에 대한 설명과 권장 조치를 제공합니다. Cisco Unified Real-Time Monitoring Tool에서 SysLog 뷰어에 액세스할 수 있습니다. SysLog 뷰어를 통해 정보를 보는 방법에 대한 자세한 내용은 *Cisco Unified Real-Time Monitoring Tool* 관리 설명서를 참조하십시오.

이름	설명
원격 Syslog에 대해 알람 활성화	SysLog 파일은 알람 대상의 역할을합니다. Syslog 메시지를 Syslog 서버에 저장하려면 이 확인란을 선택하고 Syslog 서버 이름을 지정합니다. 이 대상이 활성화되어 있고 서버 이름이 지정되지 않은 경우 Cisco Unified Serviceability는 Syslog 메시지를 전송하지 않습니다. 구성된 AMC 기본 및 페일오버 수집기는 원격 syslog 설정을 사용합니다. 수집기에서 사용하는 원격 syslog 설정은 개별 노드에 구성된 설정입니다. 원격 syslog가 AMC 페일오버 수집기에서 원격 syslog를 구성하지 않고 AMC 기본 수집기에만 구성되고 AMC 기본 수집기에서 페일오버가 발생하는 경우 원격 syslog 생성되지 않습니다. 원격 syslog 알람을 동일한 원격 syslog 서버로 보내려면 모든 노드에서 동일한 설정을 정확하게 구성해야 합니다. AMC 컨트롤러에서 페일오버가 발생하거나 수집기 구성이 다른 노드로 변경되면 백업 또는 새로 구성된 노드의 원격 syslog 설정이 사용됩니다. 시스템에서 너무 많은 알람을 발생하지 않도록 하려면 종료 지점 알람 제외 확인란을 선택하면 됩니다. 이렇게하면 엔드포인트 전화기 관련 이벤트가 별도의 파일에 기록됩니다. 종료 지점 알람 제외 확인란은 CallManager 서비스에 대해서만 표시되며 기본적으로 선택되지 않습니다. 이 확인란을 선택하는 경우에는 모든 노드에 적용 옵션도 선택해야 합니다. 엔드포인트 알람에 대한 구성 옵션은 알람 구성 설정에 나열되어 있습니다. 팁 노드는 다른 노드에서 syslog 메시지를 허용하지 않으므로 Cisco Unified Communications Manager 또는 Cisco Unified Communications Manager IM and Presence Service 노드를 대상으로 지정하지 마십시오.
원격 Syslog 서버	각 서버 이름 1, 서버 이름 2, 서버 이름 3, 서버 이름 4 및 서버 이름 5 필드에 syslog 메시지를 허용하는 데 사용할 원격 syslog 서버의 이름 또는 IP 주소를 입력합니다. 예를 들어, Cisco Unified Operations Manager에게 알람을 전송하려면 Cisco Unified Operations Manager를 서버 이름으로 지정합니다. 팁 노드는 다른 노드에서 syslog 메시지를 허용하지 않으므로 Cisco Unified Communications Manager 또는 Cisco Unified Communications Manager IM and Presence Service 노드를 대상으로 지정하지 마십시오.

이름	설명
SDI 추적에 대한 알람 활성화	SDI 추적 라이브러리는 알람 대상의 역할을합니다. 알람을 기록하려면 이 확인란을 선택하고 추적 구성 창에서 선택한 서비스에 대한 추적 확인란을 선택합니다. Cisco 통합 서비스 가용성의 추적 구성 창에서 설정을 구성하는 방법에 대한 자세한 내용은 설정 추적 매개 변수를 참조하십시오.
Unified Communications Manager 및 Unified Communications Manager BE는 다음만 수행할 수 있습니다. SDL 추적에 대해 알람 활성화	SDL 추적 라이브러리는 알람 대상의 역할을합니다. 이 대상은 Cisco CallManager 서비스 및 CTIManager 서비스에만 적용됩니다. SDL 구성 추적을 사용하여 이 알람 대상을 구성합니다. SDL 추적 로그 파일에 알람을 기록하려면 이 확인란을 선택하고 추적 구성 창에서 선택한 서비스에 대한 추적 확인란을 선택합니다. Cisco 통합 서비스 가용성의 추적 구성 창에서 설정을 구성하는 방법에 대한 자세한 내용은 설정 추적 매개 변수를 참조하십시오.
알람 이벤트 수준	드롭다운 목록에서 다음 옵션 중 하나를 선택합니다. 긴급 이 수준은 시스템을 사용할 수 없는 것으로 지정합니다. 알림 이 수준은 즉각적인 조치가 필요함을 나타냅니다. 중요 시스템이 중요한 조건을 감지합니다. 오류 이 수준은 오류 조건이 있음을 나타냅니다. 알림 이 수준은 경고 조건이 감지되었음을 나타냅니다. 알림 이 수준은 정상이지만 중요한 조건을 지정합니다. 정보 이 수준은 정보 메시지만 지정합니다. 디버그 이 수준은 Cisco 기술 지원 센터 엔지니어가 디버깅하는 데 사용하는 세부 이벤트 정보를 지정합니다.

다음 표에서는 기본 알람 구성 설정에 대해 설명합니다.

	로컬 Syslog	원격 Syslog	SDI 추적	SDL 추적

알람 활성화	선택됨	선택 취소됨	선택됨	선택됨
알람 이벤트 수준	오류	비활성화됨	오류	오류

종료 지점 알람 제외	로컬 Syslog	대체 Syslog	원격 Syslog	Syslog 심각도 및 Strangulate 알림	Syslog 트랩
선택됨	아니요	예	아니요	아니요	아니요
선택 취소됨	아니요	예	예	예	예

알람 정의 및 사용자 정의 설명 추가

이 섹션에는 서비스 가용성 인터페이스에 표시되는 알람 정의에 대한 사용자 정보를 검색하고 보고 만드는 절차에 대한 정보를 제공합니다.

알람 정의 보기 및 사용자 정의 설명 추가

이 섹션에서는 알람 정의를 검색하고 보는 방법에 대해 설명합니다.

팁 Unified Communications Manager 및 Cisco Unity Connection에만 해당: Cisco Unity Connection 서비스 가용성에서 Cisco Unity Connection 알람 정의를 볼 수 있습니다. Cisco Unity Connection 서비스 가용성에서 알람 정의에 사용자 정의 설명을 추가할 수 없습니다.

또한 Cisco Unity Connection은 Cisco Unified 서비스 가용성에서 특정 알람 정의를 사용하며, Cisco Unified 서비스 가용성에서 보아야 합니다. 시스템 카탈로그의 카탈로그와 연결된 알람을 볼 수 있습니다.

시작하기 전에

알람 정의 카탈로그에 대한 설명을 검토합니다.

프로시저

단계 **1** 알람 > 정의를 선택합니다.

단계 **2** 다음 작업 중 하나를 수행합니다.

- 다음과 같이 알람을 선택합니다.
  - 알람 위치 찾기 드롭다운 목록(예: 시스템 알람 카탈로그 또는 IM and Presence 알람 카탈로그)에서 알람 카탈로그를 선택합니다.
  - 같음 드롭다운 목록에서 특정 카탈로그 이름을 선택합니다.

- 알람 이름 입력 필드에 알람 이름을 입력합니다.

단계 **3** 찾기를 선택합니다.

단계 **4** 알람 정의의 여러 페이지가 있는 경우 다음 작업 중 하나를 수행합니다.

- 다른 페이지를 선택하려면 알람 메시지 정의 창 맨 아래에서 적절한 탐색 버튼을 선택합니다.
- 창에 표시되는 알람 수를 변경하려면 페이지당 행 수 드롭다운 목록에서 다른 값을 선택합니다.

단계 **5** 알람 세부 정보를 원하는 알람 정의를 선택합니다.

단계 **6** 알람에 정보를 추가하려면 사용자 정의 텍스트 필드에 텍스트를 입력한 다음 저장을 선택합니다.

팁 사용자 정의 텍스트 필드에 텍스트를 추가하는 경우 언제든지 모두 지우기를 선택하여 입력한 정보를 삭제할 수 있습니다.

단계 **7** 저장을 선택합니다.

단계 **8** 알람 메시지 정의 창으로 돌아가려면 관련 링크 드롭다운 목록에서 알람 찾기/나열로 돌아가기를 선택합니다.

단계 **9** 이동을 선택합니다.

시스템 알람 카탈로그 설명

다음 표에는 시스템 알람 카탈로그 알람 설명이 포함되어 있습니다. 시스템 알람 카탈로그는 Unified Communications Manager 및 Cisco Unity Connection을 지원합니다.

표 ***8:*** 시스템 카탈로그

이름	설명
ClusterManagerAlarmCatalog	클러스터의 서버 간 보안 연결 설정과 관련된 모든 클러스터 관리자 입니다.
DBAlarmCatalog	모든 Cisco 데이터베이스 알람 정의
DRFAlarmCatalog	모든 재해 복구 시스템 알람 정의
GenericAlarmCatalog	모든 애플리케이션에서 공유하는 모든 일반 알람 정의
JavaApplications	모든 Java 애플리케이션 알람 정의 팁 알람 구성 GUI를 사용하여 JavaApplications 알람을 구성할 수 Unified Communications Manager 및 Cisco Unity Connection의 적으로 이러한 알람이 이벤트 로그로 이동하도록 구성합니다 Communications Manager의 경우 CiscoWorks LAN 관리 솔루 기 위해 SNMP 트랩을 생성하도록 이러한 알람을 구성할 수 운영 체제와 함께 제공되는 레지스트리 편집기를 사용하여 매개 변수를 보거나 변경할 수 있습니다.

이름	설명
EMAlarmCatalog	익스텐션 모빌리티용 알람
LoginAlarmCatalog	모든 로그인 관련 알람 정의
LpmTctCatalog	모든 로그 파티션 모니터링 및 추적 수집 알람 정의
RTMTAlarmCatalog	모든 Cisco Unified Real-Time Monitoring Tool 알람 정의
SystemAccessCatalog	SystemAccess에서 모든 스레드 통계 카운터를 모든 프로세스 통계 카운 께 제공하는지 여부를 추적하는 데 사용되는 모든 알람 정의입니다.
ServiceManagerAlarmCatalogs	서비스 활성화, 비활성화, 시작, 다시 시작 및 중지와 관련된 모든 서비스 알람 정의입니다.
TFTPAlarmCatalog	모든 Cisco TFTP 알람 정의
TVSAlarmCatalog	신뢰 확인 서비스용 알람
TestAlarmCatalog	CLI (명령줄 인터페이스)에서 SNMP 트랩을 통해 테스트 경보를 전송하 용되는 모든 알람 정의입니다. CLI에 대한 자세한 내용은 *Cisco Unified* 용 명령줄 인터페이스 설명서를 참조하십시오. 팁 Cisco Unity Connection SNMP는 Unified Communications Manager Unity Connection 시스템에서 트랩을 지원하지 않습니다.
CertMonitorAlarmCatalog	모든 인증서 만료 정의
CTLproviderAlarmCatalog	CTL(인증서 신뢰 목록) 공급자 서비스에 대한 알람
CDPAlarmCatalog	CDP(Cisco Discovery Protocol) 서비스에 대한 알람
IMSAlarmCatalog	모든 사용자 인증 및 자격 증명 정의입니다.
SLMAlarmCatalog	Cisco Smart 라이선싱에 대한 알람

CallManager 알람 카탈로그 설명

이 섹션의 정보는 Cisco Unity Connection에는 적용되지 않습니다.

다음 표에는 CallManager 알람 카탈로그 설명이 포함되어 있습니다.

표 ***9: CallManager*** 알람 카탈로그

이름	설명
CallManager	모든 Cisco CallManager 서비스 알람 정의
CDRRepAlarmCatalog	모든 CDRRep 알람 정의

이름	설명
CARAlarmCatalog	모든 CDR 분석 및 보고 알람 정의
CEFAlarmCatalog	모든 Cisco Extended Functions 알람 정의
CMIAlarmCatalog	모든 Cisco 메시징 인터페이스 알람 정의
CtiManagerAlarmCatalog	모든 Cisco CTI(컴퓨터 텔레포니 통합) 관리자 알람 정의
IpVmsAlarmCatalog	모든 IP 음성 미디어 스트리밍 애플리케이션 알람 정의
TCDSRVAlarmCatalog	모든 Cisco 전화 통신 통화 디스패처 서비스 알람 정의
전화기	전화기 관련 작업에 대한 알람(예: 다운로드)
CAPFAlarmCatalog	CAPF(Certificate Authority Proxy Function) 서비스에 대한 알람
SAMLSSOAlarmCatalog	SAML SSO(Single Sign On) 기능에 대한 알람입니다.

IM and Presence 알람 카탈로그 설명

다음 표에는 IM and Presence Service 알람 카탈로그 설명이 포함되어 있습니다.

표 ***10: IM and Presence Service*** 알람 카탈로그

이름	설명
CiscoUPSConfigAgent	IM and Presence Service IDS 데이터베이스의 구성 변경 사항을 IM and Presence Service SIP 프록시에 알리는 모든 구성 에이전트 알람입니다.
CiscoUPInterclusterSyncAgent	클러스터 간 라우팅을 위해 IM and Presence Service 클러스터 간에 최종 사용자 정보를 동기화하는 모든 클러스터 간 동기화 에이전트 알람입니다.
CiscoUPSPresenceEngine	사용자의 가용성 상태 및 통신 기능에 관한 정보를 수집하는 모든 프레즌스 엔진 알람입니다.
CiscoUPSSIPProxy	라우팅, 요청자 ID 및 전송 상호 연결에 관련된 모든 SIP 프록시 알람입니다.
CiscoUPSSOAP	HTTPS를 사용하여 외부 클라이언트 간에 보안 SOAP 인터페이스를 제공하는 모든 SOAP(Simple Object Access Protocol) 알람입니다.
CiscoUPSSyncAgent	IM and Presence Service 데이터를 Unified Communications Manager 데이터와 동기화 상태로 유지하는 모든 동기화 에이전트 알람입니다.

이름	설명
CiscoUPXCP	IM and Presence Service의 XCP 구성 요소 및 서비스의 상태에 대한 정보를 수집하는 모든 XCP 알람입니다.
CiscoUPServerRecoveryManager	프레즌스 중복 그룹의 노드 간 페일오버 및 폴백 프로세스와 관련된 모든 서버 복구 관리자 알람입니다.
CiscoUPReplWatcher	IDS 복제 상태를 모니터링하는 모든 ReplWatcher 알람입니다.
CiscoUPXCPConfigManager	XCP 구성 요소와 관련된 모든 Cisco XCP 구성 관리자 알람 정의입니다.

설명 및 권장 작업을 포함하는 알람 정보에는 사용자의 로컬 IM and Presence Service 노드에 없는 문제에 대해서도 문제 해결을 수행하는 데 도움이 되는 애플리케이션 이름, 서버 이름 및 기타 정보가 포함됩니다.

IM and Presence Service에 해당하는 알람에 대한 자세한 내용은 *Cisco Unified Communications Manager* 의 *IM and Presence Service*용 시스템 오류 메시지를 참조하십시오.

CiscoSyslog 파일의 기본 알람

다음 표에는 알람 구성을 사용하지 않고 CiscoSyslog 파일에서 트리거되는 기본 알람에 대한 설명이 포함되어 있습니다.

표 ***11: CiscoSyslog*** 파일의 기본 알람

이름	설명
CLM_IPSecCertUpdated	변경으로 인해 클러스터의 피어 노드에서 IPSec 자체 서명 인증서를 가져왔습니다.
CLM_IPAddressChange	클러스터에 있는 피어 노드의 IP 주소가 변경되었습니다.
CLM_PeerState	클러스터에서 다른 노드를 사용하는 ClusterMgr 세션 상태를 현재 상태로 변경했습니다.
CLM_MsgIntChkError	ClusterMgr가 메시지 무결성 확인에 실패했다는 메시지를 받았습니다. 이는 클러스터의 다른 노드가 잘못된 보안 암호를 사용하여 구성되었음을 나타내는 것일 수 있습니다.
CLM_UnrecognizedHost	ClusterMgr가 이 클러스터에서 노드로 구성되지 않은 IP 주소에서 메시지를 받았습니다.

이름	설명
CLM_ConnectivityTest	클러스터 관리자가 네트워크 오류를 감지했습니다.
ServiceActivated	이 서비스가 이제 활성화됩니다.
ServiceDeactivated	이 서비스가 이제 비활성화됩니다.
ServiceActivationFailed	이 서비스를 활성화하지 못했습니다.
ServiceDeactivationFailed	이 서비스를 비활성화하지 못했습니다.
ServiceFailed	서비스가 갑자기 종료되었습니다. 서비스 매니저가 다시 시작을 시도합니다.
ServiceStartFailed	이 서비스를 시작하지 못했습니다. 서비스 매니저가 서비스를 다시 시작하려고 시도합니다.
ServiceStopFailed	여러 번 재시도 후 지정된 서비스를 중지할 수 없습니다. 서비스가 중지된 것으로 표시됩니다.
ServiceRestartFailed	지정한 서비스를 다시 시작할 수 없습니다.
ServiceExceededMaxRestarts	최대 재시작 시도 후에도 서비스를 시작하지 못했습니다.
FailedToReadConfig	구성 파일을 읽지 못했습니다. 구성 파일이 손상되었을 수 있습니다.
MemAllocFailed	메모리를 할당하지 못했습니다.
SystemResourceError	시스템 통화에 실패했습니다.
ServiceManagerUnexpectedShutdown	예기치 않은 종료 후에 서비스 매니저가 성공적으로 다시 시작되었습니다.
OutOfMemory	프로세스가 운영 체제에서 메모리를 요청했지만 사용할 수 있는 메모리가 부족합니다.
CREATE-DST-RULE-FILE-CLI	새 DST 규칙 파일은 cli에서 생성됩니다. 전화기를 다시 시작해야 합니다. 전화기를 다시 시작하지 않으면 DST 시작/중지 날짜가 잘못될 수 있습니다.
CREATE-DST-RULE-FILE-BOOTUP	새 DST 규칙 파일은 부팅 중에 생성됩니다. 전화기를 다시 시작해야 합니다. 전화기를 다시 시작하지 않으면 DST 시작/중지 날짜가 잘못될 수 있습니다.

이름	설명
CREATE-DST-RULE-FILE-CRON	새 DST 규칙 파일은 cron에서 생성됩니다. 전화기를 다시 시작해야 합니다. 전화기를 다시 시작하지 않으면 DST 시작/중지 날짜가 잘못될 수 있습니다.
PermissionDenied	프로세스에 작업을 수행할 권한이 없으므로 작업을 완료할 수 없습니다.
ServiceNotInstalled	실행 파일은 시작하려고 시도하지만 서비스 제어 관리자에서 서비스로 구성되어 있지 않기 때문에 시작할 수 없습니다. 서비스 이름은 %s입니다.
ServiceStopped	서비스가 중지되었습니다.
ServiceStarted	서비스가 시작되었습니다.
ServiceStartupFailed	서비스가 시작되었습니다.
FileWriteError	기본 파일 경로에 쓰지 못했습니다.

11 장

감사 로그

- 감사 로그, 117 페이지

감사 로그

감사 로깅을 통해 시스템에 대한 구성 변경 사항이 감사를 위해 개별 로그 파일에 기록됩니다.

감사 로깅 (표준)

감사 로깅이 활성화되어 있지만 세부 감사 로깅 옵션을 선택하지 않으면 시스템은 표준 감사 로깅을 위해 구성됩니다.

표준 감사 로깅을 통해 시스템에 대한 구성 변경 사항이 감사를 위해 개별 로그 파일에 기록됩니다. 서비스 가용성 GUI의 제어 센터 네트워크 서비스 아래에 표시되는 Cisco Audit Event Service는 사용자에 의해 또는 사용자 작업의 결과로 발생하는 시스템에 대한 구성 변경 사항을 모니터링 및 기록합니다.

서비스 가용성 GUI의 감사 로그 구성 창에 액세스하여 감사 로그에 대한 설정을 구성합니다.

표준 감사 로그에는 다음 부분이 포함되어 있습니다.

- 감사 로깅 프레임워크 - 프레임워크는 알람 라이브러리를 사용하여 감사 이벤트를 감사 로그에 기록하는 API로 구성됩니다. GenericAlarmCatalog.xml로 정의된 알람 카탈로그가 이러한 알람에 적용됩니다. 시스템 구성 요소마다 고유한 로깅이 제공됩니다.

  다음 예는 Unified Communications Manager 구성 요소에서 알람을 전송하는 데 사용할 수 있는 API를 표시합니다.

  ```
  User ID: CCMAdministratorClient IP Address: 172.19.240.207 Severity: 3
  EventType: ServiceStatusUpdated ResourceAccessed: CCMService EventStatus:
  Successful Description: CallManager Service status is stopped
  ```

- 감사 이벤트 로깅 - 감사 이벤트는 로깅해야 하는 이벤트를 나타냅니다. 다음 예는 샘플 감사 이벤트를 표시합니다.

```
CCM_TOMCAT-GENERIC-3-AuditEventGenerated: Audit Event Generated
UserID:CCMAdministrator Client IP Address:172.19.240.207 Severity:3
EventType:ServiceStatusUpdated ResourceAccessed: CCMService
EventStatus:Successful Description: Call Manager Service status is stopped
App ID:Cisco Tomcat Cluster ID:StandAloneCluster Node ID:sa-cm1-3
```

팁 감사 이벤트 로깅은 기본적으로 중앙 집중식이고 활성화되어 있습니다. Syslog 감사라고 하는 알람 모니터에서 로그를 작성합니다. 기본적으로 로그는 회전하도록 구성되어 있습니다. AuditLogAlarmMonitor가 감사 이벤트를 쓸 수 없는 경우 AuditLogAlarmMonitor는이 오류를 syslog 파일에 중대한 오류로 기록합니다. 알림 관리자는 이 오류를 SeverityMatchFound 알림의 일부로 보고합니다. 이벤트 로깅이 실패하는 경우에도 실제 작업은 계속됩니다. 모든 감사 로그는 Cisco Unified Real-Time Monitoring Tool의 추적 및 로그 센트럴에서 수집, 보고 및 삭제됩니다.

Cisco 통합 서비스 가용성 표준 이벤트 로깅

Cisco 통합 서비스 가용성는 다음 이벤트를 기록합니다.

- 서비스 활성화, 비활성화, 시작 또는 중지.
- 추적 구성 및 알람 구성 변경.
- SNMP 구성의 변경.
- CDR 관리의 변경. (Cisco Unified Communications Manager만 해당)
- 서비스 가용성 보고서 아카이브의 보고서를 검토합니다. 이 로그는 리포터 노드에서 볼 수 있습니다. (Unified Communications Manager만 해당)

Cisco Unified Real-Time Monitoring Tool 표준 이벤트 로깅

Cisco Unified Real-Time Monitoring Tool는 감사 이벤트 알람을 사용하여 다음 이벤트를 기록합니다.

- 알림 구성
- 알림 일시 중지
- 이메일 구성
- 노드 알림 상태 설정
- 알림 추가
- 알림 작업 추가
- 알림 지우기
- 알림 활성화
- 알림 작업 제거
- 알림 제거

Unified Communications Manager 표준 이벤트 로깅

Cisco CDR Analysis and Reporting(CAR)에서 다음 이벤트에 대한 감사 로그를 생성합니다.

- 로더 예약
- 일별, 주별 및 월별 보고 일정
- 메일 매개 변수 구성
- 다이얼 계획 구성
- 게이트웨이 구성
- 시스템 환경설정 구성
- 자동 삭제 구성
- 기간, 시간 및 음성 품질에 대한 등급 엔진 구성
- QoS 구성
- 미리 작성된 보고서 구성에 대한 자동 생성/알림
- 알림 제한 구성

Cisco Unified CM 관리 표준 이벤트 로깅

Cisco Unified Communications Manager 관리의 다양한 구성 요소에 대해 다음과 같은 이벤트가 기록됩니다.

- 사용자 로깅(사용자 로그인 및 사용자 로그아웃)
- 사용자 역할 구성원 자격 업데이트(사용자 추가, 사용자 삭제, 사용자 역할 업데이트됨)
- 역할 업데이트(새 역할이 추가, 삭제 또는 업데이트됨)
- 장치 업데이트(전화기 및 게이트웨이)
- 서버 구성 업데이트(알람 또는 추적 구성, 서비스 매개 변수, 엔터프라이즈 매개 변수, IP 주소, 호스트 이름, 이더넷 설정 및 Unified Communications Manager 서버 추가 또는 삭제에 대한 변경 사항)

Cisco Unified Communications 자가 관리 포털 표준 이벤트 로깅

사용자 로깅(사용자 로그인 및 사용자 로그아웃) 이벤트는 Cisco Unified Communications 자가 관리 포털에 대해 기록됩니다.

명령줄 인터페이스 표준 이벤트 로깅

명령줄 인터페이스를 통해 실행된 모든 명령이 기록됩니다(Unified Communications Manager 및 Cisco Unity Connection 모두).

Cisco Unity Connection 관리 표준 이벤트 로깅

Cisco Unity Connection 관리는 다음 이벤트를 기록합니다.

- 사용자 로깅(사용자 로그인 및 사용자 로그아웃)
- 모든 구성 변경 사항(다음을 포함하되 이에 제한되지 않음: 사용자, 연락처, 통화 관리 개체, 네트워킹, 시스템 설정 및 전화 통신)
- 작업 관리(작업 활성화 또는 비활성화)
- 벌크 관리 도구(벌크 생성, 벌크 삭제)
- 사용자 정의 키패드 맵(맵 업데이트)

Cisco Personal Communications Assistant(Cisco PCA) 표준 이벤트 로깅

Cisco Personal Communications Assistant 클라이언트는 다음 이벤트를 기록합니다.

- 사용자 로깅(사용자 로그인 및 사용자 로그아웃)
- Messaging Assistant를 통해 이루어진 모든 구성 변경

Cisco Unity Connection 서비스 가용성 표준 이벤트 로깅

Cisco Unity Connection 서비스 가용성은 다음 이벤트를 기록합니다.

- 사용자 로깅(사용자 로그인 및 사용자 로그아웃)
- 모든 구성이 변경됩니다.
- 서비스 활성화, 비활성화, 시작 또는 중지.

대표 상태 전송 **API** 이벤트 로깅을 사용하는 **Cisco Unity Connection** 클라이언트

대표 상태 전송(REST) API를 사용하는 Cisco Unity Connection 클라이언트는 다음 이벤트를 기록합니다.

- 사용자 로깅(사용자 API 인증).
- Cisco Unity Connection 프로비저닝 인터페이스를 이용하는 API 통화.

Cisco Unified IM and Presence Serviceability 표준 이벤트 로깅

Cisco Unified IM and Presence Serviceability는 다음 이벤트를 기록합니다.

- 서비스 활성화, 비활성화, 시작 또는 중지
- 추적 구성 및 알람 구성 변경
- SNMP 구성의 변경
- 서비스 가용성 보고서 아카이브의 모든 보고서 검토(이 로그는 리포터 노드에서 볼 수 있음)

Cisco Unified IM and Presence 실시간 모니터링 도구 표준 이벤트 로깅

Cisco Unified IM and Presence 실시간 모니터링 도구는 감사 이벤트 알람을 사용하여 다음 이벤트를 기록합니다.

- 알림 구성
- 알림 일시 중지
- 이메일 구성
- 노드 알림 상태 설정
- 알림 추가
- 알림 작업 추가
- 알림 지우기
- 알림 활성화
- 알림 작업 제거
- 알림 제거

Cisco IM and Presence 관리 표준 이벤트 로깅

다음 이벤트는 Cisco Unified Communications Manager IM and Presence 관리의 다양한 구성 요소에 대해 기록됩니다.

- 관리자 로깅(관리, OS 관리, 재해 복구 시스템 및 보고 등 IM and Presence 인터페이스에 대한 로그인 및 로그아웃)
- 사용자 역할 구성원 자격 업데이트(사용자 추가, 사용자 삭제, 사용자 역할 업데이트됨)
- 역할 업데이트(새 역할이 추가, 삭제 또는 업데이트됨)
- 장치 업데이트(전화기 및 게이트웨이)
- 서버 구성 업데이트(알람 또는 추적 구성, 서비스 매개 변수, 엔터프라이즈 매개 변수, IP 주소, 호스트 이름, 이더넷 설정 및 IM and Presence 서버 추가 또는 삭제 변경)

IM and Presence 애플리케이션 표준 이벤트 로깅

다음 이벤트는 IM and Presence 애플리케이션의 다양한 구성 요소에 의해 기록됩니다.

- IM 클라이언트(사용자 로그인, 사용자 로그아웃 및 실패한 로그인 시도)에 대한 최종 사용자 로그온
- IM 채팅방에서 사용자 입력 및 종료
- IM 채팅방 만들기 및 소멸

명령줄 인터페이스 표준 이벤트 로깅

명령줄 인터페이스를 통해 실행된 모든 명령이 기록됩니다.

감사 로깅(자세히)

세부 감사 로깅은 표준(기본) 감사 로그에 저장되지 않은 추가 구성 수정 사항을 기록하는 선택적 기능입니다. 표준 감사 로그에 저장된 모든 정보 외에도 세부 감사 로그에는 수정된 값을 포함하여 추가, 업데이트 및 삭제된 구성 항목이 포함됩니다. 세부 감사 로깅은 기본적으로 비활성화되어 있지만 감사 로그 구성 창에서 활성화할 수 있습니다.

Audit Log Types

시스템 감사 로그

시스템 감사 로그는 Linux OS 사용자의 생성, 수정 또는 삭제, 로그 변조, 파일 또는 디렉터리 권한에 대한 변경 등의 작업을 추적합니다. 이 유형의 감사 로그는 수집된 데이터 양이 많아 기본적으로 비활성화됩니다. 이 기능을 활성화하려면 CLI를 사용하여 utils auditd를 수동으로 활성화해야 합니다. 시스템 감사 로그 기능을 활성화한 후 실시간 모니터링 도구에서 추적 및 로그 센트럴을 통해 선택한 로그를 수집, 확인, 다운로드 또는 삭제할 수 있습니다. 시스템 감사 로그는 `vos-audit.log`의 형식을 취합니다.

이 기능을 활성화하는 방법에 대한 자세한 내용은 *Cisco Unified Communications Solutions*용 명령줄 인터페이스 설명서를 참조하십시오. 실시간 모니터링 도구에서 수집된 로그에 액세스하는 방법에 대한 자세한 내용은 *Cisco Unified Cisco Unified Real-Time Monitoring Tool* 관리 설명서를 참조하십시오.

애플리케이션 감사 로그

애플리케이션 감사 로그는 사용자가 수행했거나 사용자 작업의 결과로 시스템에 대한 구성 변경 사항을 모니터링하고 기록합니다.

참고 애플리케이션 감사 로그(Linux auditd)는 CLI를 통해서만 활성화하거나 비활성화할 수 있습니다. 실시간 모니터링 도구를 통한 vos-audit.log 수집 외에는 이 유형의 감사 로그에 대한 설정을 변경할 수 없습니다.

데이터베이스 감사 로그

데이터베이스 감사 로그는 로그인과 같은 Informix 데이터베이스에 대한 액세스와 관련된 모든 활동을 추적합니다.

감사 로그 구성 작업 흐름

감사 로깅을 구성하려면 다음 작업을 완료하십시오.

프로시저

	명령 또는 동작	목적
단계 **1**	감사 로깅 설정, 123 페이지	감사 로그 구성 창에서 감사 로그 구성을 설정합니다. 원격 감사 로깅을 사용할지 여부와 세부 감사 로깅 옵션을 사용할지 여부를 구성할 수 있습니다.
단계 **2**	원격 감사 로그 전송 프로토콜 구성, 124 페이지	(선택 사항) 원격 감사 로깅이 구성된 경우 전송 프로토콜을 구성합니다. 정상 작동 모드의 시스템 기본값은 UDP이지만, TCP 또는 TLS를 구성할 수도 있습니다.
단계 **3**	경고 알림을 위한 전자 메일 서버 구성, 124 페이지	(선택 사항) RTMT에서 이메일 알림을 위한 이메일 서버를 설정합니다.
단계 **4**	이메일 알림 활성화, 125 페이지	(선택 사항) 다음 이메일 알림 중 하나를 설정합니다. • TCP를 사용하여 구성된 원격 감사 로깅이 있는 경우 **TCPRemoteSyslogDeliveryFailed** 알림에 대한 이메일 알림을 설정합니다. • TLS를 사용하여 구성된 원격 감사 로깅이 있는 경우 **TLSRemoteSyslogDeliveryFailed** 알림에 대한 이메일 알림을 설정합니다.
단계 **5**	플랫폼 로그에 대해 원격 감사 로깅 구성, 125 페이지	플랫폼 감사 로그 및 원격 서버 로그에 대한 원격 감사 로깅을 설정합니다. 이러한 유형의 감사 로그의 경우 FileBeat 클라이언트 및 외부 logstash 서버를 구성해야 합니다.

감사 로깅 설정

시작하기 전에

원격 감사 로깅은 각 클러스터 노드와 원격 syslog 서버 간에 원격 syslog 서버 및 구성된 IPSec을 설정하고 그 사이에 있는 게이트웨이에 대한 연결을 포함해야 합니다. IPSec 구성은 *Cisco IOS* 보안 구성 설명서를 참조하십시오.

프로시저

단계 **1** Cisco 통합 서비스 가용성에서 도구 > 감사 로그 구성을 선택합니다.

단계 **2** 서버 드롭다운 메뉴에서 클러스터의 서버를 선택하고 이동을 클릭합니다.

단계 **3** 모든 클러스터 노드를 기록하려면 모든 노드에 적용 확인란을 선택합니다.

단계 **4** 서버 이름 필드에 원격 syslog 서버의 IP 주소 또는 FQDN(Fully Qualified Domain Name)을 입력합니다.

단계 **5** (선택 사항) 수정된 항목과 수정된 값을 포함하여 구성 업데이트를 기록하려면 세부 감사 로깅 확인란을 선택합니다.

단계 **6** 감사 로그 구성 창의 나머지 필드를 완료합니다. 필드 및 해당 설명에 대한 도움이 필요한 경우 온라인 도움말을 참조하십시오.

단계 **7** 저장을 클릭합니다.

다음에 수행할 작업

원격 감사 로그 전송 프로토콜 구성, 124 페이지

원격 감사 로그 전송 프로토콜 구성

이 절차를 사용하여 원격 감사 로그에 대한 전송 프로토콜을 변경합니다. 시스템 기본값은 UDP이지만 로 다시 구성할 수 있습니다. TCP 또는 TLS.

프로시저

단계 **1** 명령줄 인터페이스에 로그인합니다.

단계 **2** **utils remotesyslog show protocol** 명령을 실행하여 구성된 프로토콜을 확인합니다.

단계 **3** 이 노드의 프로토콜을 변경해야 하는 경우 다음을 수행합니다.

- TCP를 구성하려면 **utils remotesyslog set protocol tcp** 명령을 실행합니다.
- UDP를 구성하려면 **utils remotesyslog set protocol udp** 명령을 실행합니다.
- TLS를 구성하려면 **utils remotesyslog set protocol tls** 명령을 실행합니다.

참고 Common Criteria 모드에서는 엄격한 호스트 이름 확인이 구현됩니다. 따라서 인증서와 일치하는 FQDN(Fully Qualified Domain Name)을 사용하여 서버를 구성해야 합니다.

단계 **4** 프로토콜을 변경한 경우 노드를 다시 시작합니다.

단계 **5** 모든 Unified Communications Manager 및 IM and Presence Service 클러스터 노드에서 이 절차를 반복합니다.

다음에 수행할 작업

경고 알림을 위한 전자 메일 서버 구성, 124 페이지

경고 알림을 위한 전자 메일 서버 구성

이 절차를 사용하여 알림 공지를 위한 이메일 서버를 설정합니다.

프로시저

단계 **1** 실시간 모니터링 도구의 시스템 창에서 중앙 알림을 클릭합니다.
단계 **2** 시스템 > 도구 > 알림 > 이메일 서버 구성을 선택합니다.
단계 **3** 메일 서버 구성 팝업에서 메일 서버에 대한 세부 정보를 입력합니다.
단계 **4** 확인을 클릭합니다.

다음에 수행할 작업

이메일 알림 활성화, 125 페이지

이메일 알림 활성화

TCP 또는 TLS가 구성된 원격 감사 로깅이 있는 경우 이 절차를 사용하여 이메일 알림을 설정하여 전송 실패를 알립니다.

프로시저

단계 **1** 실시간 모니터링 도구의 시스템 영역에서 중앙 알림을 클릭합니다.
단계 **2** 중앙 알림 창에서

- TCP를 사용한 원격 감사 로깅이 있는 경우 **TCPRemoteSyslogDeliveryFailed**를 선택합니다.
- TLS를 사용한 원격 감사 로깅이 있는 경우 **TLSRemoteSyslogDeliveryFailed**를 선택합니다.

단계 **3** 시스템 > 도구 > 알림 > 알림 작업 구성을 선택합니다.
단계 **4** 알림 작업 팝업에서 기본값을 선택하고 편집을 클릭합니다.
단계 **5** 알림 작업 팝업에서 수신자를 추가합니다.
단계 **6** 팝업 창에 이메일 알림을 보낼 주소를 입력하고 확인을 클릭합니다.
단계 **7** 알림 작업 팝업에서 수신자 아래 주소가 나타나는지, 활성화 확인란이 선택되었는지 확인합니다.
단계 **8** 확인을 클릭합니다.

플랫폼 로그에 대해 원격 감사 로깅 구성

이 작업을 완료하여 플랫폼 감사 로그, 원격 지원 로그 및 벌크 관리 csv 파일에 대한 원격 감사 로깅 지원을 추가합니다. 이러한 유형의 로그에 대해 FileBeat 클라이언트 및 logstash 서버가 사용됩니다.

시작하기 전에

외부 logstash 서버를 설정했는지 확인합니다.

프로시저

	명령 또는 동작	목적
단계 1	Logstash 서버 정보 구성, 126 페이지	IP 주소, 포트 및 파일 유형과 같은 외부 logstash 서버 세부 정보를 사용하여 FileBeat 클라이언트를 구성합니다.
단계 2	FileBeat 클라이언트 구성, 126 페이지	원격 감사 로깅을 위해 FileBeat 클라이언트를 활성화합니다.

Logstash 서버 정보 구성

이 절차를 사용하여 외부 logstash 서버 정보(예: IP 주소, 포트 번호 및 다운로드 가능 파일 유형)를 사용하여 FileBeat 클라이언트를 구성합니다.

시작하기 전에

외부 logstash 서버를 설정했는지 확인합니다.

프로시저

단계 1 명령줄 인터페이스에 로그인합니다.

단계 2 **utils FileBeat configure** 명령을 실행합니다.

단계 3 프롬프트에 따라 logstash 서버 세부 정보를 구성합니다.

FileBeat 클라이언트 구성

이 절차를 사용하여 플랫폼 감사 로그, 원격 지원 로그 및 벌크 관리 csv 파일을 업로드하는 데 사용되는 FileBeat 클라이언트를 활성화하거나 비활성화할 수 있습니다.

프로시저

단계 1 명령줄 인터페이스에 로그인합니다.

단계 2 **utils filebeat status** 명령을 실행하여 FileBeat 클라이언트가 활성화되었는지 확인합니다.

단계 3 다음 명령 중 하나를 실행합니다.

- 클라이언트를 활성화하려면 **utils filebeat enable** 명령을 실행합니다.
- 클라이언트를 비활성화하려면 **utils filebeat disable** 명령을 실행합니다.

참고 TCP는 기본 전송 프로토콜입니다.

단계 4 (선택 사항) TLS를 전송 프로토콜로 사용하려면 다음을 수행합니다.

- TLS를 전송 프로토콜로 활성화하려면 **utils FileBeat tls enable** 명령을 실행합니다.

- TLS를 전송 프로토콜로 비활성화하려면 **utils FileBeat tls disable** 명령을 실행합니다.

참고 TLS를 사용하려면 logstash 서버에서 Unified Communications Manager 및 IM and Presence Service의 tomcat 신뢰 저장소로 보안 인증서를 업로드해야 합니다.

단계 **5** 각 노드에서 이 절차를 반복합니다.

모든 노드에서 동시에 이러한 명령을 실행하지 마십시오.

감사 로그 구성 설정

시작하기 전에

감사 역할이 있는 사용자만 감사 로그 설정을 변경할 수 있습니다. 기본적으로 Unified Communications Manager의 경우 CCMAdministrator는 새로 설치하고 업그레이드한 후 감사 역할을 소유합니다. CCMAdministrator는 Cisco Unified Communications Manager 관리의 사용자 그룹 구성 창에서 감사 권한이 있는 모든 사용자를 표준 감사 사용자 그룹에 할당할 수 있습니다. 이렇게 하려면 표준 감사 사용자 그룹에서 CCMAdministrator를 제거할 수 있습니다.

IM and Presence Service의 경우 관리자는 새로 설치 및 업그레이드 후 감사 역할을 담당하며 감사 권한이 있는 사용자를 표준 감사 사용자 그룹에 할당할 수 있습니다.

Cisco Unity Connection의 경우 설치 중에 생성된 애플리케이션 관리 계정에 감사 관리자 역할이 있으며 역할에 다른 관리 사용자를 할당할 수 있습니다. 이 계정에서 감사 관리자 역할을 제거할 수도 있습니다.

표준 감사 로그 구성 역할은 감사 로그를 삭제하고 Cisco Unified Real-Time Monitoring Tool, IM and Presence 실시간 모니터링 도구, 추적 수집 도구, 실시간 모니터링 도구(RTMT), 알림 구성, 제어 센터 - 서비스 가용성 사용자 인터페이스의 네트워크 서비스, RTMT 프로파일 저장, 서비스 가용성 사용자 인터페이스의 감사 구성 및 감사 추적이라고 하는 리소스에 대한 읽기/업데이트 액세스 기능을 제공합니다.

표준 감사 로그 구성 역할은 감사 로그를 삭제하고 Cisco Unified RTMT, 추적 수집 도구, RTMT 알림 구성, 제어 센터 - Cisco 통합 서비스 가용성, RTMT 프로파일 저장, Cisco 통합 서비스 가용성의 감사 구성 및 감사 추적이라고 하는 리소스에 대한 읽기/업데이트 액세스 기능을 제공하는 것입니다.

Cisco Unity Connection의 감사 관리자 역할은 Cisco Unified RTMT에서 감사 로그를 보고, 다운로드하고, 삭제할 수 있는 기능을 제공합니다.

Unified Communications Manager의 역할, 사용자 및 사용자 그룹에 대한 자세한 내용은 *Cisco Unified Communications Manager* 관리 설명서를 참조하십시오.

Cisco Unity Connection에서 역할 및 사용자에 대한 자세한 내용은 *Cisco Unity Connection* 관련 사용자 이동, 추가 및 변경 설명서를 참조하십시오.

IM and Presence의 역할, 사용자 및 사용자 그룹에 대한 자세한 내용은 *Unified Communications Manager* 에서 *IM and Presence Service* 구성 및 관리를 참조하십시오.

다음 표에서는 Cisco 통합 서비스 가용성 감사 로그 구성 창에서 구성할 수 있는 설정에 대해 설명합니다.

표 ***12:*** 감사 로그 구성 설정

필드	설명
서버 선택	
서버	감사 로그를 구성할 서버(노드)를 선택합니다. 그런 다음 이동을 클릭합니다.
모든 노드에 적용	감사 로그 구성을 클러스터의 모든 노드에 적용하려면 모든 노드에 적용 확인란을 선택합니다.
애플리케이션 감사 로그 설정	
감사 로그 활성화	이 확인란을 선택하면 애플리케이션 감사 로그에 대한 감사 로그가 생성됩니다. Unified Communications Manager의 경우 애플리케이션 감사 로그는 Unified Communications Manager 사용자 인터페이스(예: Cisco Unified Communications Manager 관리,Cisco Unified RTMT, Cisco Unified Communications Manager CDR 분석 및 보고, Cisco 통합 서비스 가용성)에 대한 구성 업데이트를 지원합니다. IM and Presence Service의 경우 애플리케이션 감사 로그는 IM and Presence 사용자 인터페이스(예: Cisco Unified Communications Manager IM and Presence 관리, Cisco Unified IM and Presence 실시간 모니터링 도구, Cisco Unified IM and Presence Serviceability)에 대한 구성 업데이트를 지원합니다. Cisco Unity Connection의 경우 애플리케이션 감사 로그는 Cisco Unity Connection 사용자 인터페이스(Cisco Unity Connection 관리, Cisco Unity Connection Serviceability, Cisco Personal Communications Assistant 및 Connection REST API를 사용하는 클라이언트 포함)에 대한 구성 업데이트를 지원합니다. 이 설정은 기본적으로 활성화된 것으로 표시됩니다. 참고 네트워크 서비스 감사 이벤트 서비스가 실행되고 있어야합니다.

필드	설명
제거 활성화	LPM(로그 파티션 모니터)은 제거 활성화 옵션을 확인하여 감사 로그 제거가 필요한 지 여부를 결정합니다. 이 확인란을 선택하면 공통 파티션 디스크 사용량이 상위 워터마크 위에 있을 때마다 LPM이 RTMT에서 모든 감사 로그 파일을 제거합니다. 그러나 확인란의 선택을 취소하여 제거를 비활성화할 수 있습니다. 제거가 비활성화된 경우 디스크가 가득찰 때까지 감사 로그의 수가 계속 커집니다. 이 작업으로 인해 시스템이 중단될 수 있습니다. 제거 활성화 확인란을 선택 취소할 때 제거가 비활성화되는 위험을 설명하는 메시지입니다. 이 옵션은 활성 파티션의 감사 로그에 사용할 수 있습니다. 감사 로그가 비활성 파티션에 있는 경우 디스크 사용량이 상위 워터마크 위에 있을 때 감사 로그가 비워집니다. RTMT에서 추적 및 로그 센트럴 > 감사 로그를 선택하여 감사 로그에 액세스할 수 있습니다. 참고 네트워크 서비스 Cisco Log Partition Monitoring Tool가 실행되고 있어야합니다.
로그 로테이션 활성화	시스템은 이 옵션을 읽어 감사 로그 파일을 로테이션해야 하는지 또는 새 파일을 생성해야 하는지 여부를 결정합니다. 파일 최대 수는 5000을 넘을 수 없습니다. 로테이션 활성화 확인란을 선택하면 최대 파일 수에 도달한 후에 시스템에서 가장 오래된 감사 로그 파일을 덮어쓰기 시작합니다. 팁 로그 로테이션이 비활성화(선택 취소)되면 감사 로그에서 최대 파일 수 설정을 무시합니다.
세부 감사 로깅	이 확인란을 선택하면 시스템에서 세부 감사 로그를 사용할 수 있습니다. 세부 감사 로그는 일반 감사 로그와 동일한 항목을 제공하지만 구성 변경 사항도 포함합니다. 예를 들어 감사 로그에는 수정된 값을 포함하여 추가, 업데이트 및 삭제된 항목이 포함됩니다.
서버 이름	syslog 메시지를 수락하는 데 사용할 원격 syslog 서버의 이름 또는 IP 주소를 입력합니다. 서버 이름을 지정하지 않은 경우 Cisco 통합 서비스 가용성는 Syslog 메시지를 전송하지 않습니다. Unified Communications Manager 노드는 다른 서버에서 syslog 메시지를 허용하지 않으므로 Unified Communications Manager 노드를 대상으로 지정하지 마십시오. 이는 IM and Presence Service에만 적용됩니다.
원격 Syslog 감사 이벤트 수준	원격 syslog 서버에 대해 원하는 syslog 메시지 심각도를 선택합니다. 심각도 수준이 선택된 모든 syslog 메시지는 원격 syslog로 전송됩니다. 이는 IM and Presence Service에만 적용됩니다.
최대 파일 수	로그에 포함시킬 최대 파일 수를 입력합니다. 기본 설정은 250입니다. 최대 수는 5000을 지정합니다.

필드	설명
최대 파일 크기	감사 로그의 최대 파일 크기를 입력합니다. 파일 크기 값은 1MB에서 10MB 사이여야 합니다. 1에서 10 사이의 숫자를 지정해야 합니다.
근접 로그 로테이션 덮어쓰기에 대한 경고 임계값(%)	감사 로그를 덮어쓰게되는 수준에 도달하면 시스템에서 알림을 받을 수 있습니다. 이 필드를 사용하여 시스템에서 알림을 전송하는 임계값을 설정합니다. 예를 들어, 2MB 250개 파일의 기본 설정을 사용하고 경고 임계값이 80%인 경우, 시스템은 감사 로그 200개 파일(80%)이 누적되면 알람을 전송합니다. 감사 기록을 유지하려는 경우에는 RTMT를 사용하여 시스템에서 로그를 덮어쓰기 전에 로그를 검색할 수 있습니다. RTMT는 수집한 후에 파일을 삭제하는 옵션을 제공합니다. 1에서 99% 사이의 값을 입력합니다. 기본값은 80%입니다. 이 필드를 설정할 때 로그 로테이션 활성화 옵션도 선택해야 합니다. 참고 감사 로그에 할당된 총 디스크 공간은 최대 파일 수에 최대 파일 크기를 곱한 값입니다. 디스크의 감사 로그 크기가 할당된 총 디스크 공간의 이 비율을 초과하는 경우 시스템은 알림 센트럴에서 알람을 발생시킵니다.
데이터베이스 감사 로그 필터 설정	
감사 로그 활성화	이 확인란을 선택하면 Unified Communications Manager 및 Cisco Unity Connection 데이터베이스에 대한 감사 로그가 생성됩니다. 이 설정을 디버그 감사 수준 설정과 함께 사용하여 데이터베이스의 특정 항목에 대한 로그를 만들 수 있습니다.

필드	설명
디버그 감사 수준	이 설정을 사용하여 로그에서 감사할 데이터베이스 항목을 선택할 수 있습니다. 드롭다운 목록 상자에서 다음 옵션 중 하나를 선택합니다. 각 감사 로그 필터 수준은 누적된다는 점에 유의하십시오. • 스키마 - 감사 로그 데이터베이스의 설정에 대한 변경 사항을 추적합니다(예: 데이터베이스 테이블의 열 및 행). • 관리 작업 - Unified Communications Manager 시스템에 대한 모든 관리 변경 사항(예: 시스템 유지 관리에 대한 변경 사항)과 모든 스키마 변경 사항을 추적합니다. 팁 대부분의 관리자는 관리 작업 설정을 비활성화 상태로 둡니다. 감사를 원하는 사용자의 경우 데이터베이스 업데이트 수준을 사용합니다. • 데이터베이스 업데이트 - 모든 스키마 변경 사항과 모든 관리 작업 변경 사항을 데이터베이의 모든 변경 내용에 대해 추적합니다. • 데이터베이스 읽기 - 모든 스키마 변경, 관리 작업 변경 및 데이터베이스 업데이트 변경 사항을 비롯하여 시스템에 대한 모든 읽기를 추적합니다. 팁 Unified Communications Manager, IM and Presence Service 또는 Cisco Unity Connection 시스템을 신속하게 확인하려는 경우에만 데이터베이스 읽기 수준을 선택합니다. 이 수준은 상당한 양의 시스템 리소스를 사용하며 짧은 시간 동안만 사용해야 합니다.
감사 로그 로테이션 활성화	시스템은 이 옵션을 읽어 데이터베이스 감사 로그 파일을 로테이션해야 하는지 또는 새 파일을 생성해야 하는지 여부를 결정합니다. 감사 로테이션 활성화 옵션 확인란을 선택하면 최대 파일 수에 도달한 후에 시스템에서 가장 오래된 감사 로그 파일을 덮어쓰기 시작합니다. 이 설정 확인란을 선택 취소하면 감사 로그는 최대 파일 수 설정을 무시합니다.
최대 파일 수	로그에 포함시킬 최대 파일 수를 입력합니다. 최대 파일 수에 입력하는 값이 로그 로테이션에서 삭제된 파일 수 설정에 입력하는 값보다 큰지 확인합니다. 4(최소)에서 40(최대) 사이의 숫자를 입력할 수 있습니다.
로그 로테이션에서 삭제된 파일 수	데이터베이스 감사 로그 로테이션이 발생하는 경우 시스템에서 삭제할 수 있는 최대 파일 수를 입력합니다. 이 필드에 입력할 수 있는 최소값은 1입니다. 최대값은 최대 파일 수 설정에 입력하는 값보다 2 작은 수입니다. 예를 들어, 최대 파일 수 필드에 40을 입력하는 경우 로그 로테이션에서 삭제된 파일 수에 입력할 수 있는 가장 높은 숫자는 38입니다.

필드	설명
기본값으로 설정	기본값으로 설정 버튼은 기본값을 지정합니다. 세부 문제 해결을 위해 다른 수준으로 설정해야 하는 경우가 아니면 감사 로그를 기본 모드로 설정하는 것이 좋습니다. 기본값으로 설정 옵션은 로그 파일에 사용되는 디스크 공간을 최소화합니다.

주의 이 기능을 활성화하면, 특히 디버그 감사 수준이 데이터베이스 업데이트 또는 데이터베이스 읽기로 설정된 경우 데이터베이스 로깅이 짧은 기간에 많은 양의 데이터를 생성할 수 있습니다. 이로 인해 사용량이 많은 시간 동안 성능에 심각한 영향을 미칠 수 있습니다. 일반적으로 데이터베이스 로깅을 비활성화하는 것이 좋습니다. 데이터베이스의 변경 내용을 추적하기 위해 로깅을 활성화해야 하는 경우 데이터베이스 업데이트 수준을 사용하여 짧은 시간 동안만 이 작업을 수행하는 것이 좋습니다. 마찬가지로, 관리 로깅은 특히 데이터베이스 항목을 폴링하는 경우(예: 데이터베이스에서 250개 장치 열기) 웹 사용자 인터페이스의 전반적인 성능에 영향을 미칩니다.

12 장

통화 홈

• 통화 홈, 133 페이지

통화 홈

이 장에서는 Unified Communications Manager 통화 홈 서비스에 대한 개요를 제공하고 Unified Communications Manager 통화 홈 기능을 구성하는 방법에 대해 설명합니다. 통화 홈 기능을 사용하면 통신하고 진단 알림, 인벤토리 및 기타 메시지를 Smart Call Home 백 엔드 서버로 보낼 수 있습니다.

Smart Call Home

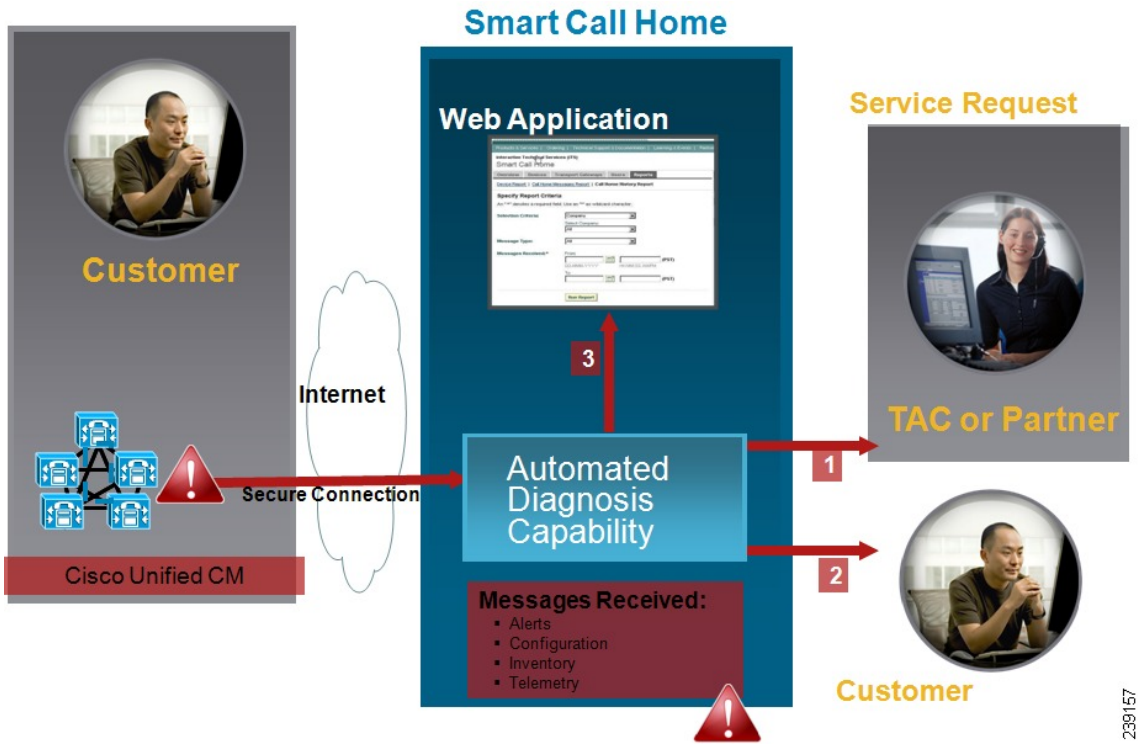
Smart Call Home은 더 높은 네트워크 가용성과 증가된 운영 효율성을 위해 다양한 Cisco 장치에서 사전 예방적 진단, 실시간 알림 및 교정을 제공합니다. 이는 Smart Call Home이 활성화된 Unified Communications Manager에서 진단 알림, 인벤토리 및 기타 메시지를 수신 및 분석하는 것과 동일하게 수행됩니다. 이러한 Unified Communications Manager의 이 특정 기능은 Unified Communications Manager 통화 홈이라고 합니다.

Smart Call Home의 기능:

- 선제적인 빠른 문제 해결을 통한 높은 네트워크 가용성:
  - 지속적인 모니터링, 실시간 사전 경고 및 상세한 진단을 통해 신속하게 문제를 파악합니다.
  - 네트워크에 있는 해당 장치 유형에만 해당되는 알림을 제공하여 잠재적인 문제를 알 수 있습니다. Cisco Cisco TAC(Technical Assistance Center)의 전문가와 직접적이고 자동적으로 연락함으로써 중요한 문제를 더 빨리 해결합니다.
- 고객에 게 다음과 같은 기능을 제공하여 운영 효율성 향상:
  - 문제 해결 시간을 단축하여 인력 자원을 더욱 효율적으로 활용합니다.
- 고객에게 다음 기능을 제공하는 데 필요한 정보에 대한 신속한 웹 기반 액세스:
  - 모든 통화 홈 메시지, 진단 및 권장 사항을 한 곳에서 확인합니다.
  - 서비스 요청 상태를 신속하게 확인합니다.

• 모든 통화 홈 장치에 대한 최신 인벤토리 및 구성 정보를 확인합니다.

그림 *2: Cisco Smart Call Home* 개요



Smart Call Home에는 다음 작업을 수행하는 모듈이 포함되어 있습니다.

- 고객에게 통화 홈 메시지를 알립니다.
- 영향 분석 및 교정 단계를 제공합니다.

Smart Call Home에 대한 자세한 내용은 다음 위치에 있는 Smart Call Home 페이지를 참조하십시오.

http://www.cisco.com/en/US/products/ps7334/serv_home.html

Smart Call Home 인증서 갱신 정보

Cisco 릴리스 10.5(2)부터는 관리자가 모든 갱신 요청에 대한 새 인증서를 수동으로 업로드하여 계속해서 통화 홈 기능을 지원해야 합니다. Cisco Unified 운영 체제 관리 웹 GUI를 통해 인증서를 업로드할 수 있습니다. 보안 > 인증서 관리 > 인증서/인증서 체인 업로드로 이동합니다. 인증서 용도로 **tomcat-trust**를 선택하고 저장된 대상에서 인증서를 업로드합니다.

확장명이 .PEM인 다음 인증서는 tomcat-trust로 업로드해야 합니다.

참고 관리자가 전체 문자열을 복사하고 -----BEGIN CERTIFICATE----- 및 -----END CERTIFICATE-----를 포함시키고 텍스트 파일에 붙여 넣고 확장명 .PEM을 사용하여 저장합니다.

-----BEGIN CERTIFICATE-----
MIIFtzCCA5+gAwIBAgICBQkwDQYJKoZIhvcNAQEFBQAwRTELMAkGA1UEBhMCQk0x
GTAXBgNVBAoTEFF1b1ZhZGlzIExpbWl0ZWQxGzAZBgNVBAMTElF1b1ZhZGlzIFJv
b3QgQ0EgMjAeFw0wNjExMjQxODI3MDBaFw0zMTExMjQxODIzMzNaMEUxCzAJBgNV
BAYTAkJNMRkwFwYDVQQKExBRdW9WYWRpcyBMaW1pdGVkMRswGQYDVQQDExJRdW9
WYWRpcyBSb290IENBIDIwggIiMA0GCSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQCa
GMpLlA0ALa8DKYrwD4HIrkwZhR0In6spRIXzL4GtMh6QRr+jhiYaHv5+HBg6XJxg
Fyo6dIMzMH1hVBHL7avg5tKifvVrbxi3Cgst/ek+7wrGsxDp3MJGF/hd/aTa/55J
WpzmM+Yklvc/ulsrHHo1wtZn/qtmUIttKGAr79dgw8eTvI02kfN/+NsRE8Scd3bB
rrcCaoF6qUWD4gXmuVbBlDePSHFjIuwXZQeVikvfj8ZaCuWw419eaxGrDPmF60Tp
+ARz8un+XJiM9XOva7R+zdRcAitMOeGylZUtQofX1bOQQ7dsE/He3fbE+Ik/0XX1
ksOR1YqI0JDs3G3eicJlcZaLDQP9nL9bFqyS2+r+eXyt66/3FsvbzSUr5R/7mp/i
Ucw6UwxI5g69ybR2BlLmEROFcmMDBOAENisgGQLodKcftslWZvB1JdxnwQ5hYIiz
PtGo/KPaHbDRsSNU30R2be1B2MGyIrZTHN81Hdyhdyox5C315eXbyOD/5YDXC2Og
/zOhD7osFRXql7PSorW+8oyWHhqPHWykYTe5hnMz15eWniN9gqRMgeKh0bpnX5UH
oycR7hYQe7xFSkyyBNKr79X9DFHOUGoIMfmR2gyPZFwDwzqLID9ujWc9Otb+fVuI
yV77zGHcizN300QyNQliBJIWENieJ0f7OyHj+OsdWwIDAQABo4GwMIGtMA8GA1Ud
EwEB/wQFMAMBAf8wCwYDVR0PBAQDAgEGMB0GA1UdDgQWBBQahGK8SEwzJQTU7tD2
A8QZRtGUazBuBgNVHSMEZzBlgBQahGK8SEwzJQTU7tD2A8QZRtGUa6FJpEcwRTEL
MAkGA1UEBhMCQk0xGTAXBgNVBAoTEFF1b1ZhZGlzIExpbWl0ZWQxGzAZBgNVBAMT
ElF1b1ZhZGlzIFJvb3QgQ0EgMoICBQkwDQYJKoZIhvcNAQEFBQADggIBAD4KFk2f
BluornFdLwUvZ+YTRYPENvbzwCYMDbVHZF34tHLJRqUDGCdViXh9duqWNIAXINzn
g/iN/Ae42l9NLmeyhP3ZRPx3UIHmfLTJDQtyU/h2BwdBR5YM++CCJpNVjP4iH2Bl
fF/nJrP3MpCYUNQ3cVX2kiF495V5+vgtJodmVjB3pjd4M1IQWK4/YY7yarHvGH5K
WWPKjaJW1acvvFYfzznB4vsKqBUsfU16Y8Zsl0Q80m/DShcK+JDSV6IZUaUtl0Ha
B0+pUNqQjZRG4T7wlP0QADj1O+hA4bRuVhogzG9Yje0uRY/W6ZM/57Es3zrWIozc
hLsib9D45MY56QSIPMO661V6bYCZJPVsAfv4l7CUW+v90m/xd2gNNWQjrLhVoQPR
TUIZ3Ph1WVaj+ahJefivDrkRoHy3au000LYmYjgahwz46P0u05B/B5EqHdZ+XIWD
mbA4CD/pXvk1B+TJYm5Xf6dQlfe6yJvmjqIBxdZmv3lh8zwc4bmCXF2gw+nYSL0Z
ohEUGW6yhhtoPkg3Goi3XZZenMfvJ2II4pEZXNLxId26F0KCl3GBUzGpn/Z9Yr9y
4aOTHcyKJloJONDO1w2AFrR4pTqHTI2KpdVGl/IsELm8VCLAAVBpQ570su9t+Oza
8eOx79+Rj1QqCyXBJhnEUhAFZdWCEOrCMc0u
-----END CERTIFICATE-----

익명 통화 홈

익명 통화 홈 기능은 Cisco에서 인벤토리 및 텔레메트리 메시지를 익명으로 받을 수 있는 Smart Call Home 기능의 하위 기능입니다. 이 기능을 활성화하여 익명의 ID를 유지합니다.

다음은 익명 통화 홈의 특성입니다.

- Unified Communications Manager는 인벤토리 및 텔레메트리 메시지만 보내고 진단 및 구성 정보는 Smart Call Home 백엔드에 전송하지 않습니다.
- 사용자 관련 정보(예: 등록된 장치 및 업그레이드 기록)는 전송되지 않습니다.
- 익명 통화 홈 옵션에는 Cisco와의 Smart Call Home 기능에 대한 등록 또는 엔타이틀먼트가 필요하지 않습니다.
- 인벤토리 및 텔레메트리 메시지는 주기적으로(매월 1일 마다) 통화 홈 백엔드에 전송됩니다.
- Cisco Unified Communications Manager가 익명 통화 홈을 사용하도록 구성된 경우 추적 로그 및 진단 정보 포함 옵션을 사용할 수 없습니다.

인벤토리 메시지에는 클러스터, 노드 및 라이센스에 대한 정보가 포함되어 있습니다.

다음 표에서는 Smart Call Home 및 익명 통화 홈에 대한 인벤토리 메시지를 보여줍니다.

표 ***13: Smart Call Home*** 및 익명 통화 홈에 대한 인벤토리 메시지

인벤토리 메시지	**Smart Call Home**	익명 통화 홈
연락처 이메일	IOS-XR	해당 없음
연락처 전화 번호	IOS-XR	해당 없음
도로 주소	IOS-XR	해당 없음
서버 이름	IOS-XR	해당 없음
서버 IP 주소	IOS-XR	해당 없음
라이센스 서버	IOS-XR	해당 없음
OS 버전	IOS-XR	IOS-XR
모델	IOS-XR	IOS-XR
일련 번호	IOS-XR	IOS-XR
CPU 속도	IOS-XR	IOS-XR
RAM	IOS-XR	IOS-XR
저장소 파티션	IOS-XR	IOS-XR
펌웨어 버전	IOS-XR	IOS-XR

인벤토리 메시지	**Smart Call Home**	익명 통화 홈
BIOS 버전	IOS-XR	IOS-XR
BIOS 정보	IOS-XR	IOS-XR
RAID 컨피그레이션	IOS-XR	IOS-XR
활성 서비스	IOS-XR	IOS-XR
게시자 이름	IOS-XR	해당 없음
게시자 IP	IOS-XR	해당 없음
제품 ID	IOS-XR	IOS-XR
활성 버전	IOS-XR	IOS-XR
비활성 버전	IOS-XR	IOS-XR
제품 짧은 이름	IOS-XR	IOS-XR

텔레메트리 메시지에는 Unified Communications Manager 클러스터에서 사용할 수 있는 각 장치 유형에 대한 장치 수(IP 전화기, 게이트웨이, 전화회의 브리지 등)에 대한 정보가 포함되어 있습니다. 텔레메트리 데이터에는 전체 클러스터에 대한 장치 수가 포함됩니다.

다음 표에서는 Smart Call Home 및 익명 통화 홈에 대한 인벤토리 메시지를 보여줍니다.

표 ***14: Smart Call Home*** 및 익명 통화 홈에 대한 텔레메트리 메시지

텔레메트리 메시지	**Smart Call Home**	익명 통화 홈
연락처 이메일	IOS-XR	해당 없음
연락처 전화 번호	IOS-XR	해당 없음
도로 주소	IOS-XR	해당 없음
서버 이름	IOS-XR	해당 없음
CM 사용자 수	IOS-XR	해당 없음
일련 번호	IOS-XR	IOS-XR
게시자 이름	IOS-XR	해당 없음
장치 수 및 모델	IOS-XR	IOS-XR
전화 사용자 수	IOS-XR	IOS-XR
CM 통화 기록	IOS-XR	IOS-XR

텔레메트리 메시지	**Smart Call Home**	익명 통화 홈
등록된 기기 수	IOS-XR	해당 없음
업그레이드 기록	IOS-XR	해당 없음
시스템 상태	호스트 이름, 날짜, 로케일, 제품 버전, OS 버전, 라이센스 MAC, 업 시간, MP 통계, 사용 메모리, 디스크 사용량 및 사용되는 활성 및 비활성 파티션, DNS에 적용 가능	날짜, 로케일, 제품 버전, OS 버전, 라이센스 MAC, 업 시간, 사용 메모리, 디스크 사용량 및 사용되는 활성 및 비활성 파티션에 적용 가능

구성 메시지에는 구성과 관련된 각 데이터베이스 테이블의 행 수에 대한 정보가 포함됩니다. 구성 데이터는 클러스터 전반에 있는 각 테이블의 테이블 이름과 행 수로 구성됩니다.

Smart Call Home 상호 작용

Cisco 시스템에 직접 서비스 계약이 있는 경우 Cisco Smart Call Home 서비스에 대해 Unified Communications Manager를 등록할 수 있습니다. Smart Call Home은 Unified Communications Manager에서 전송되는 통화 홈 메시지를 분석하고 배경 정보와 권장 사항을 제공하여 시스템 문제를 신속하게 해결합니다.

Unified Communications Manager 통화 홈 기능은 다음 메시지를 Smart Call Home 백 엔드 서버로 전달합니다.

- 알림 - 환경, 하드웨어 오류 및 시스템 성능과 관련된 다양한 조건에 대한 알림 정보를 포함합니다. 알림은 Unified Communications Manager 클러스터 내의 모든 노드에서 생성될 수 있습니다. 알림 세부 정보에는 알림 유형에 따라 문제 해결에 필요한 노드 및 기타 정보가 포함됩니다. Smart Call Home 백 엔드 서버로 전송되는 알림의 경우 Smart Call Home 상호 작용과 관련된 항목을 참조하십시오.

다음은 Smart Call Home에 대한 알림입니다.

기본적으로 Smart Call Home은 24시간 내에 알림을 한 번 처리합니다. 혼합 클러스터(Unified Communications Manager 및 Cisco Unified Presence)의 24시간 범위 내에서 동일한 알림이 반복적으로 발생하고 통화 홈에서 처리되지 않습니다.

중요 수집된 정보는 48년 후 기본 AMC 서버에서 삭제됩니다. 기본적으로 Unified Communications Manager 게시자는 기본 AMC 서버입니다.

- 성능 알림
  - CallProcessingNodeCPUPegging
  - CodeYellow

- CPUPegging
- LowActivePartitionAvailableDiskSpace
- LowAvailableVirtualMemory
- LowSwapPartitionAvailableDiskSpace

- 데이터베이스 - 관련 알림
  - DBReplicationFailure
- 실패한 통화 알림
  - MediaListExhausted
  - RouteListExhausted
- 충돌 관련 알림
  - Coredumpfilefound
  - CriticalServiceDown

구성, 인벤토리 및 텔레메트리 메시지는 주기적으로(매월 1일마다) 통화 홈 백엔드로 전송됩니다. 이러한 메시지의 정보를 사용하면 TAC가 적시에 사전 서비스를 제공하여 고객이 네트워크를 관리하고 유지 관리할 수 있도록 도울 수 있습니다.

통화 홈에 대한 전제 조건

Unified Communications Manager 통화 홈 서비스를 지원하려면 다음이 필요합니다.

- 해당하는 Unified Communications Manager 서비스 계약과 연결된 Cisco.com 사용자 ID.
- Unified Communications Manager 통화 홈 기능에 대해 DNS(Domain Name System) 및 SMTP(Simple Mail Transfer Protocol) 서버를 모두 설정하는 것이 좋습니다.
  - 보안 웹(HTTPS)을 사용하여 통화 홈 메시지를 보내려면 DNS 설정이 필요합니다.
  - 통화 홈 메시지를 Cisco TAC로 보내거나 메시지 사본을 이메일을 통해 수신자 목록으로 보내려면 SMTP 설정이 필요합니다.

통화 홈 액세스

Unified Communications Manager 통화 홈에 액세스하려면 Cisco 통합 서비스 가용성 관리로 이동하고 **CallHome**(**Cisco** 통합 서비스 가용성 > **CallHome** > 통화 홈 구성)을 선택합니다.

통화 홈 설정

다음 표에서는 기본 Unified Communications Manager 통화 홈 설정을 나열합니다.

표 ***15:*** 기본 통화 홈 설정

매개 변수	기본값
통화 홈	활성화됨
다음을 사용하여 Cisco TAC(Technical Assistance Center)에 데이터를 전송합니다:	보안 웹(HTTPS)

설치하는 동안 기본 Smart Call Home 구성이 변경되면 통화 홈 사용자 인터페이스에 동일한 설정이 반영됩니다.

참고 전송 방법으로 이메일을 선택하고 보안 웹**(HTTPS)** 옵션에는 SMTP 설정이 필요하지 않은 경우에는 SMTP 설정이 필요합니다.

통화 홈 구성

Cisco 통합 서비스 가용성에서 통화 홈 > 통화 홈 구성을 선택합니다.

통화 홈 구성 창이 나타납니다.

참고 Unified Communications Manager를 설치하는 동안 Cisco Smart Call Home을 구성할 수도 있습니다.

설치 중에 Smart Call Home 옵션을 구성하는 경우에는 Smart Call Home 기능이 활성화됩니다. 없음을 선택하면 Cisco Unified Communications Manager 관리에 로그인 할 때 미리 알림 메시지가 표시됩니다. Smart Call Home을 구성하거나 Cisco 통합 서비스 가용성를 사용하여 미리 알림을 비활성화하는 지침이 제공됩니다.

다음 표에서는 Unified Communications Manager 통화 홈을 구성하는 설정을 설명합니다.

표 ***16: Unified Communications Manager*** 통화 홈 구성 설정

필드 이름	설명
통화 홈 메시지 일정	전송된 마지막 통화 홈 메시지와 예약된 다음 메시지의 날짜 및 시간을 표시합니다.

필드 이름	설명
통화 홈*	드롭다운 목록에서 다음 옵션 중 하나를 선택합니다. • 없음: 통화 홈을 활성화하거나 비활성화하려면 이 옵션을 선택합니다. Smart Call Home이 구성되지 않았다는 미리 알림 메시지가 나타납니다. Smart Call Home을 구성하거나 미리 알림을 비활성화하려면 Cisco 통합 서비스 가용성 > 통화 홈으로 이동하거나 관리자 페이지에서 여기를 클릭합니다. • 비활성화됨: 통화 홈을 비활성화하려면 이 옵션을 선택합니다. • 활성화됨**(Smart Call Home)**: 설치 중에 Smart Call Home을 선택한 경우 이 옵션이 활성화됩니다. 이 옵션을 선택하면 고객 연락처 세부 정보 아래에 있는 모든 필드가 활성화됩니다. 동일한 구성을 사용하는 경우 데이터 전송의 옵션도 활성화됩니다. • 활성화됨**(**익명 통화 홈**)**: 익명 모드에서 통화 홈을 사용하려면 이 옵션을 선택합니다. 이 옵션을 선택하면 고객 연락처 세부 정보 아래에 있는 모든 필드가 비활성화됩니다. 동일한 구성을 사용하는 경우 데이터 전송의 다음 이메일 주소에 사본 전송(여러 주소를 쉼표로 구분) 필드가 활성화되고 통화 홈 페이지에서 추적 로그 및 진단 정보 포함이 비활성화됩니다. 참고 익명 통화 홈을 활성화하면 서버는 서버에서 사용 통계를 Cisco 시스템으로 보냅니다. 이 정보는 제품에 대한 사용자 경험을 이해하고 제품 방향을 드라이브에 제공하는 데 도움이 됩니다.
고객 연락처 세부 정보	
이메일 주소*	고객의 연락처 이메일 주소를 입력합니다. 이 필드는 필수 항목입니다.
회사	(선택 사항) 회사 이름을 입력합니다. 최대 255자를 입력할 수 있습니다.
연락처 이름	(선택 사항) 고객의 연락처 이름을 입력합니다. 최대 128자까지 입력할 수 있습니다. 연락처 이름에는 영숫자 문자와 점(.), 밑줄(_) 및 하이픈(-)과 같은 일부 특수 문자가 포함될 수 있습니다.

필드 이름	설명
주소	(선택 사항) 고객의 주소를 입력합니다. 최대 1024자를 입력할 수 있습니다.
전화기	(선택 사항) 고객의 전화 번호를 입력합니다.
데이터 전송	
다음을 사용하여 Cisco TAC(Technical Assistance Center)에 데이터를 전송합니다:	이 필드는 필수 항목입니다. 드롭다운 목록에서 다음 옵션 중 하나를 선택하여 Cisco TAC로 통화 홈 메시지를 전송합니다. • 보안 웹**(HTTPS)**: 보안 웹을 사용하여 Cisco TAC로 데이터를 전송하려는 경우 이 옵션을 선택합니다. • 이메일: 이메일을 사용하여 Cisco TAC로 데이터를 전송하려는 경우 이 옵션을 선택합니다. 이메일의 경우 SMTP 서버를 구성해야 합니다. 구성된 SMTP 서버의 호스트 이름 또는 IP 주소를 볼 수 있습니다. 참고 SMTP 서버를 구성하지 않은 경우 알림 메시지가 표시됩니다. • 프록시를 통한 보안 웹(HTTPS): 프록시를 통해 데이터를 Cisco TAC로 전송하려는 경우 이 옵션을 선택합니다. 현재 프록시 수준에서는 인증을 지원하지 않습니다. 이 옵션을 구성하는 데는 다음과 같은 필드가 나타납니다. • **HTTPS** 프록시 **IP**/호스트 이름*****: 프록시 IP/호스트 이름을 입력합니다. • **HTTPS** 프록시 포트 *****: 통신할 프록시 포트 번호를 입력합니다.
다음 이메일 주소로 복사본 보내기(쉼표로 여러 개의 주소 구분)	지정한 이메일 주소로 통화 홈 메시지의 복사본을 보내려면 이 확인란을 선택합니다. 최대 1024자까지 입력할 수 있습니다.
추적 로그 및 진단 정보 포함	Unified Communications Manager를 활성화하여 로그 및 진단 정보를 수집하려면이 확인란을 선택합니다. 참고 이 옵션은 Smart Call Home이 활성화된 경우에만 활성화됩니다. 메시지에는 알림 시 추적 메시지와 함께 수집한 진단 정보가 포함되어 있습니다. 추적 크기가 3MB 미만이면 추적이 인코딩되고 알림 메시지의 일부로 전송되며 추적이 3MB 보다 큰 경우 추적 위치의 경로가 알림 메시지에 표시됩니다.

필드 이름	설명
저장	통화 홈 구성을 저장합니다. 참고 통화 홈 구성을 저장하면 최종 사용자 사용권 계약(EULA) 메시지가 나타납니다. 처음으로 구성하는 경우에는 라이센스 계약에 동의해야 합니다. 팁 활성화한 통화 홈 서비스를 비활성화하려면 드롭다운 목록에서 비활성화됨 옵션을 선택하고 저장을 클릭합니다.
다시 설정	마지막으로 저장된 구성으로 재설정합니다.
지금 홈 저장 후 호출	통화 홈 메시지를 저장하고 보냅니다. 참고 메시지가 성공적으로 전송되면 통화 홈 구성이 저장되고 모든 통화 홈 메시지가 성공적으로 전송됨 메시지가 나타납니다.

제한 사항

Unified Communications Manager 또는 Cisco Unified Presence 서버가 다운 되거나 연결할 수 없을 때 다음 제한 사항이 적용됩니다.

- 서버에 연결할 수 있을 때까지 Smart Call Home에서 마지막으로 보낸 통화 홈 메시지 및 예약된 다음 메시지의 날짜 및 시간을 캡처하는 데 실패합니다.
- 서버에 연결할 수 있을 때까지 Smart Call Home에서 통화 홈 메시지를 전송하지 않습니다.
- Smart Call Home은 게시자가 다운될 때 인벤토리 메일의 라이센스 정보를 캡처할 수 없습니다.

다음 제한 사항은 AMC(알림 매니저 및 컬렉터)로 인해 발생합니다.

- 노드 A에서 알림이 발생하고 기본 AMC 서버(기본적으로 게시자)가 다시 시작되고 동일한 노드에서 24시간 범위 내에 동일한 알림이 발생하는 경우, Smart Call Home이 노드 A에서 알림 데이터를 다시 보냅니다. Smart Call Home이 기본 AMC가 다시 시작되었기 때문에 이미 발생한 알림을 인식할 수 없습니다.
- 노드 A에서 알림이 발생하고 기본 AMC 서버를 다른 노드로 변경하고, 동일한 노드에서 24시간 범위 내에 동일한 알림이 발생하는 경우, Smart Call Home이 이를 노드 A에서 새 알림으로 인식하고 알림 데이터를 전송합니다.
- 기본 AMC 서버에서 수집된 추적은 몇 가지 시나리오에서 최대 60시간 동안 기본 AMC 서버에 상주할 수 있습니다.

다음은 혼합 클러스터(Unified Communications Manager 및 IM and Presence) 시나리오의 제한 사항입니다.

- **CallProcessingNodeCpuPegging**, 사용된 미디어 목록, 사용된 경로 목록 같은 알림은 IM and Presence에 적용되지 않습니다.
- 사용자가 기본 AMC 서버를 IM and Presence로 변경하는 경우, Smart Call Home은 사용된 미디어 목록 및 사용된 경로 목록에 대한 클러스터 개요 보고서를 생성할 수 없습니다.
- 사용자가 기본 AMC 서버를 IM and Presence로 변경하는 경우에는 Smart Call Home에서 **DB** 복제 알림에 대한 개요 보고서를 생성할 수 없습니다.

통화 홈에 대한 참조

Smart Call Home에 대한 자세한 내용은 다음 URL을 참조하십시오.

- Smart Call Home 서비스 소개

  http://www.cisco.com/en/US/products/ps7334/serv_home.html

13 장

서비스 가용성 커넥터

- 서비스 가용성 커넥터 개요, 145 페이지
- 서비스 가용성 서비스 사용의 이점, 146 페이지
- 다른 하이브리드 서비스와의 차이, 146 페이지
- 작동 방식에 대한 간단한 설명, 146 페이지
- TAC 사례에 대한 구축 아키텍처, 147 페이지
- 서비스 가용성 커넥터에 대한 TAC 지원, 149 페이지

서비스 가용성 커넥터 개요

Webex 서비스 가용성 서비스를 사용하여 로그를 쉽게 수집할 수 있습니다. 이 서비스는 진단 로그 및 정보의 찾기, 검색 및 저장 작업을 자동화합니다.

이 기능은 사용자의 온프레미스에 배포된 서비스 가용성 커넥터를 사용합니다. 서비스 가용성 커넥터는 네트워크의 전용 호스트(' 커넥터 호스트')에서 실행됩니다. 다음 구성 요소 중 하나에 커넥터를 설치할 수 있습니다.

- 엔터프라이즈 컴퓨팅 플랫폼(ECP) — 권장

  ECP는 Docker 컨테이너를 사용하여 서비스를 격리, 보호 및 관리합니다. 호스트 및 서비스 가용성 커넥터 애플리케이션이 클라우드에서 설치됩니다. 최신 상태 및 보안을 유지하기 위해 수동으로 업그레이드할 필요는 없습니다.

중요 ECP를 사용하는 것이 좋습니다. 향후 개발은 이 플랫폼에 중점을 둘 것입니다. Expressway에 서비스 가용성 커넥터를 설치하는 경우 몇 가지 새로운 기능을 사용할 수 없습니다.

- Cisco Expressway

다음과 같은 목적으로 서비스 가용성 커넥터를 사용할 수 있습니다.

- 서비스 요청에 대한 자동 로그 및 시스템 정보 검색
- Cloud-Connected UC 구축의 통합 CM 클러스터 로그 수집

두 사용 사례 모두에 대해 동일한 서비스 가용성 커넥터를 사용할 수 있습니다.

서비스 가용성 서비스 사용의 이점

이 서비스는 다음과 같은 이점을 제공합니다.

- 로그 수집 속도를 빠르게 합니다. TAC 엔지니어가 문제 진단을 수행하는 동안 관련 로그를 검색할 수 있습니다. 추가 로그를 요청하고 수동 수집 및 전달을 기다리는 지연을 방지할 수 있습니다. 이 자동화는 문제 해결 시간을 며칠 정도 단축시킬 수 있습니다.
- TAC의 협업 솔루션 분석기 및 해당 진단 서명 데이터베이스와 함께 작동합니다. 시스템은 자동으로 로그를 분석하고 알려진 문제를 식별하며 알려진 수정 사항 또는 해결 방법을 권장합니다.

다른 하이브리드 서비스와의 차이

하이브리드 일정 서비스 및 하이브리드 통화 서비스 등 기타 Expressway 기반 하이브리드 서비스와 같은 제어 허브를 통해 서비스 가용성 커넥터를 배포하고 관리합니다. 그러나 중요한 차이점이 있습니다.

이 서비스에는 사용자를 위한 기능이 없습니다. TAC는 이 서비스의 주요 사용자입니다. 다른 하이브리드 서비스를 사용하는 조직에 이익이 될 수 있지만, 다른 하이브리드 서비스를 사용하지 않는 조직은 일반 사용자입니다.

제어 허브에 구성된 조직이 이미 있는 경우 기존 조직 관리자 계정을 통해 서비스를 활성화할 수 있습니다.

서비스 가용성 커넥터에는 사용자에게 직접 기능을 제공하는 커넥터와는 다른 로드 프로파일이 있습니다. 커넥터는 항상 사용할 수 있으므로, 필요한 경우에는 TAC에서 데이터를 수집할 수 있습니다. 그러나 시간이 지남에 따라 일정하게 로드되는 것은 아닙니다. TAC 담당자는 수동으로 데이터 수집을 시작합니다. 이는 동일한 인프라에서 제공하는 다른 서비스에 미치는 영향을 최소화하기 위해 수집에 적합한 시간을 협상합니다.

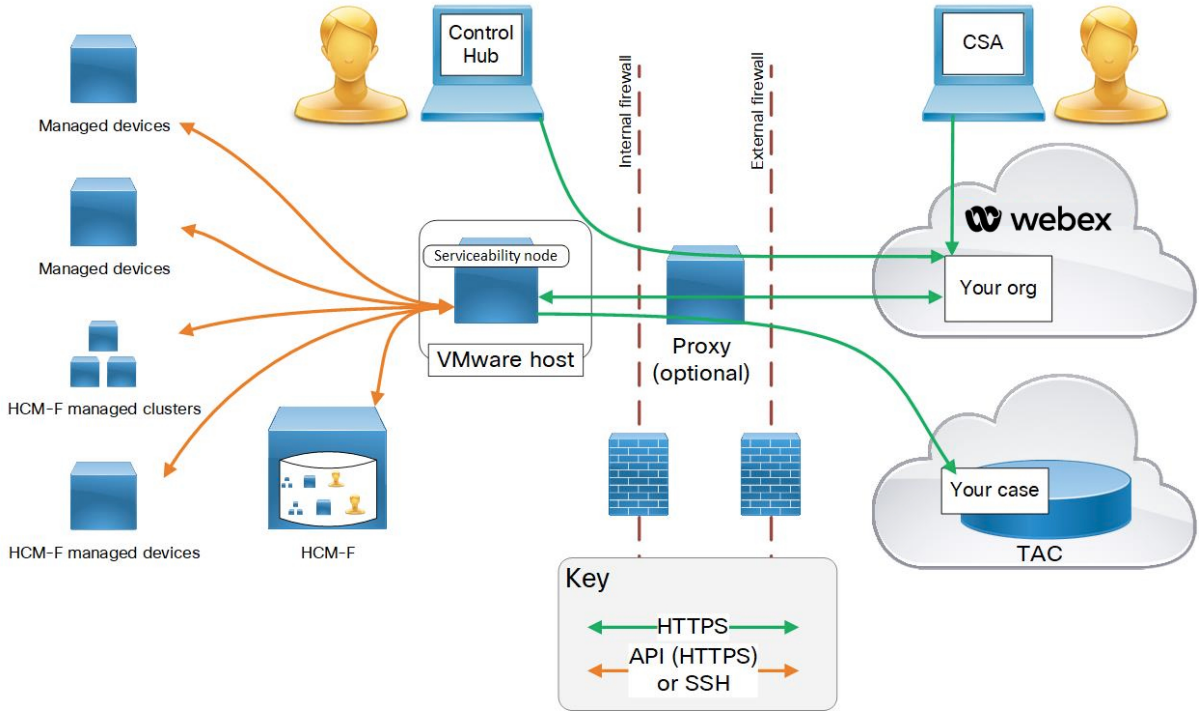
작동 방식에 대한 간단한 설명

1. 관리자가 Cisco TAC와 함께 서비스 가용성 서비스를 배포합니다. TAC 사례에 대한 구축 아키텍처, 147 페이지 참조
2. TAC는 케이스를 열거나 장치 중 하나가 자동으로 문제를 보고할 때 .
3. TAC 담당자는 CSA(협업 솔루션 분석기) 웹 인터페이스를 사용하여 관련 장치에서 데이터를 수집하도록 서비스 가용성 커넥터를 요청합니다.
4. 서비스 가용성 커넥터는 요청을 API 명령으로 변환하여 관리되는 장치에서 요청된 데이터를 수집합니다.

5. 서비스 가용성 커넥터는 CXD(고객 환경 드라이브)에 대한 암호화된 링크를 통해 해당 데이터를 수집, 암호화 및 업로드하고 해당 데이터를 서비스 요청과 연결합니다.
6. 1000개 이상의 진단 서명이 있는 TAC 데이터베이스를 기준으로 데이터를 분석합니다.
7. TAC 담당자가 결과를 검토하고 필요한 경우 원래 로그를 확인합니다.

TAC 사례에 대한 구축 아키텍처

그림 ***3: Expressway***의 서비스 커넥터를 사용한 배포



요소	설명
관리되는 장치	서비스 가용성 서비스에서 로그를 제공하려는 모든 장치를 포함합니다. 단일 서비스 가용성 커넥터를 사용하여 150개까지 로컬로 관리되는 장치를 추가할 수 있습니다. HCS 고객의 관리되는 장치 및 클러스터에 대한 HCM-F(호스팅 협업 중재 실행)에서 정보를 가져올 수 있습니다 (더 많은 수의 장치를 사용하는 경우 https://help.webex.com/en-us/142g9e/Limits-and-Bounds-of-Serviceability-Service 참조). 이 서비스는 현재 다음 장치에서 작동합니다. • Hosted Collaboration Mediation Fulfillment(HCM-F) • Cisco Unified Communications Manager • Cisco Unified CM IM and Presence Service • Cisco Expressway 시리즈 • Cisco TelePresence Video Communication Server(VCS) • Cisco Unified Contact Center Express(UCCX) • Cisco Unified Border Element(CUBE) • Cisco BroadWorks Application Server(AS) • Cisco BroadWorks Profile Server(PS) • Cisco BroadWorks Messaging Server(UMS) • Cisco BroadWorks Execution Server(XS) • Cisco Broadworks Xtended Services Platform(XSP)
관리자	제어 허브를 사용하여 커넥터 호스트를 등록하고 서비스 가용성 서비스를 활성화합니다. URL이 https://admin.webex.com이고 "조직 관리자" 인증서가 필요합니다.
커넥터 호스트	관리 커넥터 및 서비스 가용성 커넥터를 호스트하는 ECP(엔터프라이즈 컴퓨팅 플랫폼) 또는 Expressway입니다. • 관리 커넥터(ECP 또는 Expressway에 있음)와 해당 관리 서비스(Webex에 있음)는 사용자의 등록을 관리합니다. 이는 연결을 유지하고, 필요한 경우 커넥터를 업데이트하고, 상태 및 알람을 보고합니다. • 서비스 가용성 커넥터 — 조직에서 서비스 가용성 서비스를 활성화한 후에 커넥터 호스트(ECP 또는 Expressway)가 Webex에서 다운로드하는 작은 애플리케이션입니다.
프록시	(선택 사항) 서비스 가용성 커넥터를 시작한 후 프록시 구성을 변경한 경우 서비스 가용성 커넥터를 다시 시작합니다.

요소	설명
Webex Cloud	Host Webex, Webex Calling, Webex Meetings 및 Webex 하이브리드 서비스를 호스팅합니다.
TAC(Technical Assistance Center)	포함 제품: • Webex Cloud를 통해 서비스 가용성 커넥터와 통신하기 위해 CSA를 사용하는 TAC 담당자. • 서비스 가용성 커넥터가 수집하여 고객 경험 드라이브로 업로드한 케이스 및 관련 로그를 사용하는 TAC 케이스 관리 시스템.

서비스 가용성 커넥터에 대한 TAC 지원

서비스 가용성 커넥터에 대한 자세한 내용은 https://www.cisco.com/go/serviceability을 참조하거나 TAC 담당자에게 문의하십시오.

14 장

단순 네트워크 관리 프로토콜

- SNMP(Simple Network Management Protocol) 지원, 151 페이지
- SNMP 구성 작업 흐름, 172 페이지
- SNMP 트랩 설정, 188 페이지
- SNMP 추적 구성, 192 페이지
- SNMP 문제 해결, 192 페이지

SNMP(Simple Network Management Protocol) 지원

애플리케이션 레이어 프로토콜인 SNMP를 사용하면 노드, 라우터 등과 같은 네트워크 장치 간에 관리 정보를 교환하기 쉽습니다. TCP/IP의 일부로 SNMP를 사용하면 관리자가 네트워크 성능을 원격 관리하고 네트워크 문제를 찾아 해결하며 네트워크 확장을 계획할 수 있습니다.

서비스 가용성 GUI를 사용하여 V1, V2c 및 V3에 대한 커뮤니티 문자열, 사용자 및 알림 대상과 같은 SNMP 관련 설정을 구성합니다. 사용자가 구성하는 SNMP 설정은 로컬 노드에 적용됩니다. 그러나 시스템 구성에서 클러스터를 지원하는 경우 SNMP 구성 창의 "모든 노드에 적용" 옵션을 사용하여 클러스터의 모든 서버에 설정을 적용할 수 있습니다.

팁 Unified Communications Manager만 해당: Unified Communications Manager 6.0 이상을 업그레이드 중에는 Cisco Unified CallManager 또는 Unified Communications Manager 4.X에서 지정한 SNMP 구성 매개 변수가 마이그레이션되지 않습니다. Cisco 통합 서비스 가용성에서 SNMP 구성 절차를 다시 수행해야 합니다.

SNMP는 IPv4와 IPv6을 지원하며 CISCO-CCM-MIB에 IPv4와 IPv6 주소, 기본 설정 등에 대한 열과 저장소가 포함되어 있습니다.

SNMP 기본 사항

SNMP 관리 네트워크는 관리되는 장치, 에이전트 및 네트워크 관리 시스템의 세 가지 핵심 구성 요소로 이루어집니다.

- 관리되는 장치 - SNMP 에이전트를 포함하고 관리되는 네트워크에 상주하는 네트워크 노드입니다. 관리되는 장치는 관리 정보를 수집 및 저장하고 SNMP를 사용하여 사용할 수 있게합니다.

  Unified Communications Manager 및 IM and Presence Service에만 해당: 클러스터를 지원하는 구성에서는 클러스터의 첫 번째 노드가 관리되는 장치의 역할을 합니다.

- 에이전트 - 관리되는 장치에 있는 네트워크 관리 소프트웨어 모듈입니다. 에이전트는 관리 정보에 대한 로컬 지식을 포함하고 이를 SNMP와 호환되는 형태로 변환합니다.

  마스터 에이전트 및 하위 에이전트 구성 요소는 SNMP를 지원하는 데 사용됩니다. 마스터 에이전트는 에이전트 프로토콜 엔진 역할을 하고 SNMP 요청과 관련된 인증, 권한 부여, 액세스 제어 및 프라이버시 기능을 수행합니다. 마찬가지로, 마스터 에이전트는 MIB-II와 관련된 MIB(Management Information Base) 변수를 일부 포함합니다. 마스터 에이전트는 하위 에이전트가 필요한 작업을 완료한 후에도 하위 에이전트를 연결 및 연결 해제합니다. SNMP 마스터 에이전트는 포트 161에서 수신하고, 벤더 MIB용 SNMP 패킷을 전달합니다.

  Unified Communications Manager 하위 에이전트는 로컬 Unified Communications Manager와 상호작용합니다. Unified Communications Manager 서브 에이전트는 SNMP 마스터 에이전트에 트랩 및 정보 메시지를 전송하고 SNMP 마스터 에이전트는 SNMP 트랩 수신기(알림 대상)와 통신합니다.

  IM and Presence Service 하위 에이전트는 로컬 IM and Presence Service와만 상호 작용합니다. IM and Presence Service 하위 에이전트는 SNMP 마스터 에이전트에 트랩 및 정보 메시지를 전송하고 SNMP 마스터 에이전트는 SNMP 트랩 수신기(알림 대상)와 통신합니다.

- NMS(네트워크 관리 시스템) - 네트워크 관리에 필요한 벌크 처리 및 메모리 리소스를 제공하는 SNMP 관리 애플리케이션(이 도구가 실행되는 PC와 함께)입니다. NMS는 관리되는 장치를 모니터링하고 제어하는 애플리케이션을 실행합니다. 다음과 같은 NMS가 지원됩니다.
  - CiscoWorks LAN Management Solution
  - HP OpenView
  - SNMP 및 Unified Communications Manager SNMP 인터페이스를 지원하는 타사 애플리케이션

SNMP Management Information Base

SNMP를 사용하면 계층 구조로 구성된 정보의 컬렉션인 MIB(Management Information Base)에 액세스할 수 있습니다. MIB는 개체 식별자로 식별되는 관리되는 개체를 구성합니다. 관리되는 장치의 특정 특성을 포함하는 MIB 개체는 하나 이상의 개체 인스턴스(변수)로 구성됩니다.

SNMP 인터페이스는 다음 Cisco 표준 MIB를 제공합니다.

- CISCO-CDP-MIB
- CISCO-CCM-MIB
- CISCO-SYSLOG-MIB
- CISCO-UNITY-MIB

다음 제한을 준수하십시오.

- Unified Communications Manager는 CISCO-UNITY-MIB를 지원하지 않습니다.
- Cisco Unity Connection은 CISCO-CCM-MIB를 지원하지 않습니다.
- IM and Presence Service는 CISCO-CCM-MIB 및 CISCO-UNITY-MIB를 지원하지 않습니다.

SNM) 확장 에이전트는 서버에 상주하며 서버에 알려진 장치에 대한 자세한 정보를 제공하는 CISCO-CCM-MIB를 노출합니다. 클러스터 구성의 경우 SNMP 확장 에이전트는 클러스터의 각 서버에 상주합니다. CISCO-CCM-MIB는 클러스터를 지원하는 구성에서 서버에 대한 장치 등록 상태, IP 주소, 설명 및 모델 유형과 같은 장치 정보를 제공합니다.

SNMP 인터페이스는 다음 산업 표준 MIB를 제공합니다.

- SYSAPPL-MIB
- MIB-II(RFC 1213)
- HOST-RESOURCES-MIB

CISCO-CDP-MIB

CDP 하위 에이전트를 사용하여 Cisco Discovery Protocol MIB, CISCO-CDP-MIB를 읽습니다. 이 MIB를 사용하면 SNMP 관리 장치에서 네트워크의 다른 Cisco 장치에 자신을 광고 하도록 할 수 있습니다.

CDP 하위 에이전트는 CDP-MIB를 구현합니다. CDP-MIB에는 다음과 같은 개체가 포함되어 있습니다.

- cdpInterfaceIfIndex
- cdpInterfaceMessageInterval
- cdpInterfaceEnable
- cdpInterfaceGroup
- cdpInterfacePort
- cdpGlobalRun
- cdpGlobalMessageInterval
- cdpGlobalHoldTime
- cdpGlobalLastChange
- Cdpgobdeviceid
- cdpGlobalDeviceIdFormat
- cdpGlobalDeviceIdFormatCpd

참고 CISCO-CDP-MIB는 CISCO-SMI, CISCO-TC, CISCO-VTP-MIB의 프레즌스에 의존합니다.

SYSAPPL-MIB

시스템 애플리케이션 에이전트를 사용하여 시스템에서 실행 중인 설치된 애플리케이션, 애플리케이션 구성 요소 및 프로세스와 같은 SYSAPPL-MIB로부터 정보를 가져올 수 있습니다.

시스템 애플리케이션 에이전트는 SYSAPPL-MIB의 다음 개체 그룹을 지원합니다.

- sysApplInstallPkg
- sysApplRun
- sysApplMap
- sysApplInstallElmt
- sysApplElmtRun

표 ***17: SYSAPPL-MIB*** 명령

명령	설명
장치 관련 쿼리	
sysApplInstallPkgVersion	소프트웨어 제조업체가 애플리케이션 패키지에 할당한 버전 번호를 제공합니다.
sysApplElmPastRunUser	프로세스 소유자의 로그인 이름(예: root)을 제공합니다.
메모리, 스토리지 및 CPU 관련 쿼리	
sysApplElmPastRunMemory	이 프로세스가 종료되기 전에 할당된 실제 시스템 메모리의 총 양을 kb 단위로 제공합니다.
sysApplElmtPastRunCPU	이 프로세스에 사용된 총 시스템 CPU 리소스의 마지막으로 알려진 100분의 1초 수를 제공합니다. 참고 다중 프로세서 시스템에서 이 값은 실제(벽면 시계) 시간의 100분의 1초에 100분의 1초 이상씩 증가할수 있습니다.

sysApplInstallElmtCurSizeLow	현재 파일 크기 모듈로(modulo) 2^32 바이트를 제공합니다. 예를 들어, 총 크기가 4,294,967,296 바이트인 파일의 경우 이 변수의 값은 0입니다. 총 크기가 4,294,967,295 바이트인 파일의 경우 이 변수는 4,294,967,295가 됩니다.
sysApplInstallElmtSizeLow	설치된 파일 크기 모듈로(modulo) 2^32 바이트를 제공합니다. 이것은 설치 직후 디스크에 있는 파일의 크기입니다. 예를 들어, 총 크기가 4,294,967,296 바이트인 파일의 경우 이 변수의 값은 0입니다. 총 크기가 4,294,967,295 바이트인 파일의 경우 이 변수는 4,294,967,295가 됩니다.
sysApplElmRunMemory	현재 이 프로세스에 할당된 실제 시스템 메모리의 총 양을 kb 단위로 제공합니다.
sysApplElmRunCPU	이 프로세스에 사용된 총 시스템 CPU 리소스의 100분의 1초 수를 제공합니다. 참고 다중 프로세서 시스템에서 이 값은 실제(벽면 시계) 시간의 100분의 1초에 100분의 1초 이상씩 증가했을 수 있습니다.
프로세스 관련 쿼리	
sysApplElmtRunState	실행 중인 프로세스의 현재 상태를 제공합니다. 가능한 값은 실행 중(1), 실행 가능(2) 상태이지만 CPU 같은 리소스 대기 중, 이벤트 대기 중(3), 종료 중(4) 또는 기타(5)입니다.
sysApplElmtRunNumFiles	프로세스에서 현재 연 일반 파일 수를 제공합니다. 전송 연결(소켓)은 이 값의 계산에 포함되어서는 안 되며 시스템 특정 특수 파일 유형이어서는 안 됩니다.
sysApplElmtRunTimeStarted	프로세스가 시작된 시간을 제공합니다.
sysApplElmtRunMemory	현재 이 프로세스에 할당된 실제 시스템 메모리의 총 양을 kb 단위로 제공합니다.
sysApplElmtPastRunInstallID	설치된 요소 테이블에 인덱스를 제공합니다. 이 개체의 값은 이 항목이 이전에 실행된 프로세스를 나타내는 애플리케이션 요소에 대한 sysApplInstallElmtIndex와 동일한 값입니다.

sysApplElmtPastRunUser	프로세스 소유자의 로그인 이름(예: root)을 제공합니다.
sysApplElmtPastRunTimeEnded	프로세스가 종료된 시간을 제공합니다.
sysApplElmtRunUser	프로세스 소유자의 로그인 이름(예: root)을 제공합니다.
sysApplRunStarted	애플리케이션이 시작된 날짜 및 시간을 제공합니다.
sysApplElmtRunCPU	이 프로세스에 사용된 총 시스템 CPU 리소스의 100분의 1초 수를 제공합니다. 참고 다중 프로세서 시스템에서 이 값은 실제(벽면 시계) 시간의 100분의 1초에 100분의 1초 이상씩 증가했을 수 있습니다.
소프트웨어 구성 요소 관련 쿼리	
sysApplInstallPkgProductName	제조업체가 소프트웨어 애플리케이션 패키지에 할당한 이름을 제공합니다.
sysApplElmtRunParameters	프로세스에 대한 시작 매개 변수를 제공합니다.
sysApplElmtRunName	프로세스의 전체 경로 및 파일 이름을 제공합니다. 예를 들어 '/opt/MYYpkg/bin/myyproc'은 실행 경로가 'opt/MYYpkg/bin/myyproc'인 프로세스 'myyproc'에 대해 반환됩니다.
sysApplInstallElmtName	애플리케이션에 포함되어 있는 이 요소의 이름을 제공합니다.
sysApplElmtRunUser	프로세스 소유자의 로그인 이름(예: root)을 제공합니다.

sysApplInstallElmtPath	이 요소가 설치된 디렉터리에 대한 전체 경로를 제공합니다. 예를 들어, '/opt/EMPuma/bin' 디렉터리에 설치된 요소에 대한 값은 '/opt/EMPuma/bin'입니다. 대부분의 애플리케이션 패키지에는 패키지에 포함된 요소에 대한 정보가 포함됩니다. 또한 일반적으로 요소는 패키지 설치 디렉터리 아래 하위 디렉터리에 설치됩니다. 요소 경로 이름이 패키지 정보 자체에 포함되지 않은 경우에는 일반적으로 하위 디렉터리를 검색하여 경로를 결정할 수 있습니다. 해당 위치에 요소가 설치되어 있지 않고 다른 정보를 에이전트 구현에 사용할 수 없는 경우 경로를 알 수 없으며 null이 반환됩니다.
sysApplMapInstallPkgIndex	이 개체의 값을 제공하고 이 프로세스가 속해 있는 애플리케이션에 대해 설치된 소프트웨어 패키지를 식별합니다. 프로세스의 상위 애플리케이션을 확인할 수 있는 경우 이 개체의 값은 이 프로세스를 포함하는 설치된 애플리케이션에 해당하는 sysApplInstallPkgTable의 항목에 대한 sysApplInstallPkgIndex 값과 동일합니다. 그러나 상위 애플리케이션을 확인할 수 없는 경우(예: 프로세스가 설치된 특정 애플리케이션에 속하지 않는 경우) 이 개체의 값은 '0'이고, 이 프로세스는 애플리케이션, 그런 다음 설치된 소프트웨어 패키지로 다시 연결될 수 없다는 것을 알 수 있습니다.
sysApplElmtRunInstallID	sysApplInstallElmtTable에 인덱스를 제공합니다. 이 개체의 값은 이 항목이 실행 중인 인스턴스를 나타내는 애플리케이션 요소에 대한 sysApplInstallElmtIndex와 동일한 값입니다. 이 프로세스를 설치된 실행 파일과 연결할 수 없는 경우 값은 '0'이어야 합니다.

sysApplRunCurrentState	실행 중인 애플리케이션 인스턴스의 현재 상태를 제공합니다. 가능한 값은 실행 중(1), 실행 가능(2) 상태이지만 CPU 같은 리소스 대기 중, 이벤트 대기 중(3), 종료 중(4) 또는 기타(5)입니다. 이 값은 이 애플리케이션 인스턴스의 실행 중인 요소에 대한 평가, (sysApplElmRunState 참조) 및 sysApplInstallElmtRole에 정의된 역할을 기반으로합니다. 하나 이상의 REQUIRED 요소가 더 이상 실행되고 있지 않은 경우에는 에이전트 구현에서 애플리케이션 인스턴스가 종료 중인 것으로 감지될 수 있습니다. 대부분의 에이전트 구현은 두 번째 내부 폴링이 완료될 때까지 기다린 후 애플리케이션 인스턴스를 종료 중으로 표시하기 전에 REQUIRED 요소를 시작할 시스템 시간을 제공합니다.
sysApplInstallPkgDate	이 소프트웨어 애플리케이션을 호스트에 설치한 날짜 및 시간을 제공합니다.
sysApplInstallPkgVersion	소프트웨어 제조업체가 애플리케이션 패키지에 할당한 버전 번호를 제공합니다.
sysApplInstallElmtType	설치된 애플리케이션에 속하는 요소의 유형을 제공합니다.
날짜/시간 관련 쿼리	
sysApplElmtRunCPU	이 프로세스에 사용된 총 시스템 CPU 리소스의 100분의 1초 수입니다. 참고 다중 프로세서 시스템에서 이 값은 실제(벽면 시계) 시간의 100분의 1초에 100분의 1초 이상씩 증가했을 수 있습니다.
sysApplInstallPkgDate	이 소프트웨어 애플리케이션을 호스트에 설치한 날짜 및 시간을 제공합니다.
sysApplElmtPastRunTimeEnded	프로세스가 종료된 시간을 제공합니다.
sysApplRunStarted	애플리케이션이 시작된 날짜 및 시간을 제공합니다.

MIB-II

MIB2 에이전트를 사용하여 MIB-II로부터 정보를 얻습니다. MIB2 에이전트는 RFC 1213에 정의된 변수(예: 인터페이스, IP 등)에 대한 액세스를 제공하고 다음 개체 그룹을 지원합니다.

- 시스템
- 인터페이스
- at
- ip
- icmp
- tcp
- udp
- SNMP

표 ***18: MIB-II*** 명령

명령	설명
장치 관련 쿼리	
sysName	이 관리되는 노드에 관리적으로 할당된 이름을 제공합니다. 규칙에 따라 이 이름은 노드의 FQDN(Fully Qualified Domain Name)입니다. 이름을 알 수 없는 경우 이 값은 길이가 0인 문자열입니다.
sysDescr	엔터티에 대한 텍스트 설명을 제공합니다. 이 값에는 시스템 하드웨어 유형, 소프트웨어 운영 체제 및 네트워킹 소프트웨어의 전체 이름 및 버전 ID가 포함되어야 합니다.
SNMP 진단 쿼리	
sysName	이 관리되는 노드에 관리적으로 할당된 이름을 제공합니다. 규칙에 따라 이 이름은 노드의 FQDN(Fully Qualified Domain Name)입니다. 이름을 알 수 없는 경우 이 값은 길이가 0인 문자열입니다.
sysUpTime	시스템의 네트워크 관리 부분이 마지막으로 다시 초기화된 이후 경과한 시간(1/100초)을 제공합니다.
SNMPInTotalReqVars	유효한 SNMP Get 요청 및 Get-Next PDU를 수신한 결과로 SNMP 프로토콜 엔터티에서 성공적으로 검색한 총 MIB 개체 수를 제공합니다.
SNMPOutPkts	SNMP 엔터티에서 전송 서비스로 전달된 총 SNMP 메시지 수를 제공합니다.

sysServices	이 엔터티가 제공할 수 있는 서비스 집합을 나타내는 값을 제공합니다. 값은 합계입니다. 이 합계는 처음에 0 값을 사용합니다. 그런 다음, 1에서 7 범위의 각 레이어 L에 대해 이 노드가 트랜잭션을 수행하고 (L - 1)로 상승한 2가 합계에 추가됩니다. 예를 들어, 애플리케이션 서비스를 제공하는 호스트인 노드 값은 4 (2^(3-1))입니다. 반면에, 애플리케이션 서비스를 제공하는 호스트인 노드 값은 72 (2^(4-1) + 2^(7-1))입니다. 참고 인터넷 프로토콜 제품군의 컨텍스트에서 레이어 1 물리적(예: 리피터), 레이어 2 데이터 링크/서브 네트워크(예: 브리지), 레이어 3 인터넷(IP 지원), 레이어 4 종단 간(TCP 지원), 레이어 7 애플리케이션(SMTP 지원)을 계산합니다. OSI 프로토콜을 포함하는 시스템의 경우 레이어 5 및 6을 계산할 수도 있습니다.
SNMPEnableAuthenTraps	SNMP 엔터티가 authenticationFailure 트랩을 생성할 수 있는지 여부를 나타냅니다. 이 개체의 값은 모든 구성 정보를 무시합니다. 따라서 이는 모든 authenticationFailure 트랩이 비활성화될 수 있는 수단을 제공합니다. 참고 Cisco에서는 이 개체가 네트워크 관리 시스템을 다시 초기화하는 동안 일정하게 유지되도록 비휘발성 메모리에 저장하는 것이 좋습니다.
Syslog 관련 쿼리	
SNMPEnabledAuthenTraps	SNMP 엔터티가 authenticationFailure 트랩을 생성할 수 있는지 여부를 나타냅니다. 이 개체의 값은 모든 구성 정보를 무시합니다. 따라서 이는 모든 authenticationFailure 트랩이 비활성화될 수 있는 수단을 제공합니다. 참고 Cisco에서는 이 개체가 네트워크 관리 시스템을 다시 초기화하는 동안 일정하게 유지되도록 비휘발성 메모리에 저장하는 것이 좋습니다.
날짜/시간 관련 쿼리	

sysUpTime	시스템의 네트워크 관리 부분이 마지막으로 다시 초기화된 이후 경과한 시간(1/100초)을 제공합니다.

HOST-RESOURCES MIB

호스트 리소스 에이전트를 사용하여 HOST-RESOURCES-MIB에서 값을 가져옵니다. 호스트 리소스 에이전트는 저장소 리소스, 프로세스 테이블, 장치 정보 및 설치된 소프트웨어 베이스와 같은 호스트 정보에 대한 SNMP 액세스를 제공합니다. 호스트 리소스 에이전트는 다음 개체 그룹을 지원합니다.

- hrSystem
- hrStorage
- hrDevice
- hrSWRun
- hrSWRunPerf
- hrSWInstalled

표 ***19: HOST-RESOURCES MIB*** 명령

명령	설명
장치 관련 쿼리	
hrFSMountPoint	이 파일 시스템 루트의 경로 이름을 제공합니다.
hrDeviceDescr	장치 제조업체 및 개정을 포함하여 이 장치에 대한 텍스트 설명을 제공하고, 선택적으로 일련 번호를 제공합니다.
hrStorageDescr	저장소의 유형 및 인스턴스에 대한 설명을 제공합니다.
메모리, 스토리지 및 CPU 관련 쿼리	
hrMemorySize	호스트에 포함된 물리적 읽기/쓰기 주 메모리(일반적으로 RAM)의 양을 제공합니다.
hrStorageSize	저장소의 크기를 hrStorageAllocationUnits 단위로 제공합니다. 이 개체는 해당 작업이 적절하고 기본 시스템에서 가능한 경우 저장 영역의 크기에 대한 원격 구성을 허용하도록 쓸 수 있습니다. 예를 들어, 버퍼 풀에 할당된 주 메모리의 양과 가상 메모리에 할당된 디스크 공간을 수정할 수 있습니다.
프로세스 관련 쿼리	

hrSWRunName	제조업체, 개정 및 일반적으로 알려진 이름을 포함하여 실행 중인 소프트웨어에 대한 텍스트 설명을 제공합니다. 이 소프트웨어가 로컬로 설치된 경우 해당 hrSWInstalledName에 사용된 것과 동일한 문자열이어야 합니다.
hrSystemProcesses	이 시스템에서 현재 로드되었거나 실행 중인 프로세스 컨텍스트 수를 제공합니다.
hrSWRunIndex	호스트에서 실행되는 각 소프트웨어 부분에 대한 고유한 값을 제공합니다. 가능하면 시스템의 고유한 고유 식별 번호를 사용합니다.
소프트웨어 구성 요소 관련 쿼리	
hrSWInstalledName	제조업체, 개정, 일반적으로 알려진 이름 및 선택적으로 일련 번호를 포함하여 설치된 이 소프트웨어 부분에 대한 텍스트 설명을 제공합니다.
hrSWRunPath	이 소프트웨어를 로드한 장기 저장소(예: 디스크 드라이브)의 위치에 대한 설명을 제공합니다.
날짜/시간 관련 쿼리	
hrSystemDate	호스트 로컬 날짜 및 시간을 제공합니다.
hrFSLastPartialBackupDate	이 파일 시스템의 일부가 백업용으로 다른 저장 장치에 복사된 마지막 날짜를 제공합니다. 이 정보는 백업이 정기적으로 수행되고 있는지 확인하는 데 유용합니다. 이 정보를 알 수 없는 경우 이 변수에는(16진수) '00 00 01 01 00 00 00 00'으로 인코딩되는 0000년 1월 1일 00:00:00.0에 해당하는 값이 있습니다.

CISCO-SYSLOG-MIB

Syslog는 모든 시스템 메시지를 추적하고 중요한 정보를 통해 기록합니다. 이 MIB를 사용하면 네트워크 관리 애플리케이션에서 syslog 메시지를 SNMP 트랩으로 수신할 수 있습니다.

Cisco Syslog 에이전트는 다음 MIB 개체와 함께 트랩 기능을 지원합니다.

- clogNotificationsSent
- clogNotificationsEnabled
- clogMaxSeverity
- clogMsgIgnores
- clogMsgDrops

참고 CISCO-SYSLOG-MIB는 CISCO-SMI MIB가 존재하는지 여부에 따라 달라집니다.

표 ***20: CISCO-SYSLOG-MIB*** 명령

명령	설명
Syslog 관련 쿼리	
clogNotificationEnabled	장치에서 syslog 메시지를 생성하는 경우 clogMessageGenerated 알림을 보낼지 여부를 나타냅니다. 알림을 비활성화해도 syslog 메시지가 clogHistoryTable에 추가되는 것은 방지되지 않습니다.
clogMaxSeverity	처리할 syslog 심각도 수준을 나타냅니다. 에이전트는 이 값보다 심각도 값이 큰 모든 syslog 메시지를 무시합니다. 참고 심각도 숫자 값은 심각도가 감소하면 증가합니다. 예를 들어 오류(4)는 디버그(8)보다 심각합니다.

CISCO-CCM-MIB/CISCO-CCM-CAPABILITY MIB

CISCO-CCM-MIB는 Unified Communications Manager 및 이 Unified Communications Manager 노드에 표시되는 전화기, 게이트웨이 등과 같은 연결된 장치에 대한 동적(실시간) 및 구성된(정적) 정보를 모두 포함합니다. SNMP(Simple Network Management Protocol) 테이블에는 IP 주소, 등록 상태 및 모델 유형과 같은 정보가 포함되어 있습니다.

SNMP는 IPv4와 IPv6을 지원하며 CISCO-CCM-MIB에 IPv4와 IPv6 주소, 기본 설정 등에 대한 열과 저장소가 포함되어 있습니다.

참고 Unified Communications Manager는 Unified Communications Manager 시스템에서 이 MIB를 지원합니다. IM and Presence Service 및 Cisco Unity Connection은 이 MIB를 지원하지 않습니다.

CISCO-CCM-MIB 및 MIB 정의에 대한 지원 목록을 보려면 다음 링크로 이동하십시오.

ftp://ftp.cisco.com/pub/MIBs/supportlists/callmanager/callmanager-supportlist.html

Unified Communications Manager 릴리스 전반에 걸쳐 사용되지 않는 개체를 포함하여 MIB 종속성 및 MIB 내용을 보려면 다음 링크로 이동하십시오. http://tools.cisco.com/Support/SNMP/do/BrowseMIB.do?local=en&step=2&mibName=CISCO-CCM-CAPABILITY

동적 테이블은 Cisco CallManager 서비스가 실행 중인 경우(또는 Unified Communications Manager 클러스터 구성의 경우에는 로컬 Cisco CallManager 서비스)에만 채워집니다. Cisco CallManager SNMP Service가 실행 중일 때는 정적 테이블이 채워집니다.

표 ***21: Cisco-CCM-MIB*** 동적 테이블

테이블	목차
ccmTable	이 테이블은 로컬 Unified Communications Manager의 버전 및 설치 ID를 저장합니다. 이 테이블에는 로컬 Unified Communications Manager가 알고 있지만 버전 세부 정보에 대해 "알 수 없는" 것으로 표시되는 클러스터의 모든 Unified Communications Manager에 대한 정보도 저장됩니다. 로컬 Unified Communications Manager가 다운된 경우 버전 및 설치 ID 값을 제외하고 테이블은 빈 상태로 유지됩니다.
ccmPhoneFailed, ccmPhoneStatusUpdate, ccmPhoneExtn, ccmPhone, ccmPhoneExtension	Cisco Unified IP 전화기의 경우 ccmPhoneTable의 등록된 전화기 수는 Unified Communications Manager/RegisteredHardware 전화기 perfmon 카운터와 일치해야 합니다. ccmPhoneTable에는 등록되었거나, 등록되지 않았거나, 거부된 Cisco Unified IP 전화기에 대한 항목이 하나씩 포함됩니다. CcmPhoneExtnTable은 ccmPhoneTable 및 ccmPhoneExtnTable의 항목을 관련하여 결합된 인덱스 ccmPhoneIndex 및 ccmPhoneExtnIndex를 사용합니다.
ccmCTIDevice, ccmCTIDeviceDirNum	CcmCTIDeviceTable은 각 CTI 장치를 하나의 장치로 저장합니다. CTI 경로 포인트 또는 CTI 포트의 등록 상태에 따라, Unified Communications Manager MIB의 ccmRegisteredCTIDevices, ccmUnregisteredCTIDevices 및 ccmRejectedCTIDevices 카운터가 업데이트됩니다.
ccmSIPDevice	CCMSIPDeviceTable은 각 SIP 트렁크를 하나의 장치로 저장합니다.
ccmH323Device	CcmH323DeviceTable에는 Unified Communications Manager가 정보(클러스터 구성의 경우에는 로컬 Unified Communications Manager)를 포함하는 H.323 장치의 목록이 포함되어 있습니다. H.323 전화기 또는 H.323 게이트웨이의 경우 ccmH.323DeviceTable은 각 H.323 장치에 대해 하나의 항목을 포함합니다. (H.323 전화기 및 게이트웨이는 Unified Communications Manager에 등록되지 않습니다. Unified Communications Manager는 표시된 H.323 전화기 및 게이트웨이의 통화를 처리할 준비가 되면 H.323Started 알람을 생성합니다. 시스템은 H.323 트렁크 정보의 일부로 게이트키퍼 정보를 제공합니다.
ccmVoiceMailDevice, ccmVoiceMailDirNum	Cisco uOne, ActiveVoice의 경우 ccmVoiceMailDeviceTable에는 각 음성 메시징 장치에 대한 항목이 하나씩 포함됩니다. 등록 상태를 기준으로 Cisc MIB의 ccmRegisteredVoiceMailDevices, ccmUnregisteredVoiceMailDevices 및 ccmRejectedVoiceMailDevices 카운터가 업데이트됩니다.

테이블	목차
ccmGateway	CcmRegisteredGateways, ccmUnregistered 게이트웨이 및 ccmRejectedGateways는 등록된 게이트웨이 장치 또는 포트의 수, 등록되지 않은 게이트웨이 장치 또는 포트의 수 및 거부된 게이트웨이 장치 또는 포트의 수를 각각 추적합니다. Unified Communications Manager는 장치 또는 포트 수준에서 알람을 생성합니다. CallManager 알람을 기반으로 하는 ccmGatewayTable은 장치 또는 포트 수준 정보를 포함합니다. 등록되거나 등록되지 않았거나 거부된 장치 또는 포트에는 ccmGatewayTable에 하나의 항목이 있습니다. FXS 포트 2개와 T1 포트 1개를 사용하는 VG200에는 ccmGatewayTable에 세 개의 항목이 있습니다. CcmActiveGateway 및 ccmInActiveGateway 카운터는(등록되지 않거나 거부된) 게이트웨이 장치 또는 포트를 사용하여 활성(등록됨) 및 분실된 연락처의 수를 추적합니다. 등록 상태를 기준으로 ccmRegisteredGateways, ccmUnregisteredGateways 및 ccmRejectedGateways 카운터가 업데이트됩니다.
ccmMediaDeviceInfo	이 테이블에는 한 번 이상 로컬 Unified Communications Manager에 등록을 시도한 모든 미디어 장치의 목록이 포함되어 있습니다.
ccmGroup	이 테이블에는 Unified Communications Manager 클러스터의 Unified Communications Manager 그룹이 포함되어 있습니다.
ccmGroupMapping	이 테이블은 클러스터의 모든 Unified Communications Manager를 Unified Communications Manager 그룹에 매핑합니다. 로컬 Unified Communications Manager 노드가 다운되면 테이블은 비어 있는 상태로 유지됩니다.

표 ***22: CISCO-CCM-MIB*** 정적 테이블

테이블	콘텐츠
ccmProductType	이 테이블에는 전화기 유형, 게이트웨이 유형, 미디어 장치 유형, H.323 장치 유형, CTI 장치 유형, 음성 메시징 장치 유형 및 SIP 장치 유형을 포함하여 Unified Communications Manager(또는 Unified Communications Manager 클러스터 구성의 경우)에서 지원되는 제품 유형 목록이 포함되어 있습니다.

테이블	콘텐츠
ccmRegion, ccmRegionPair	ccmRegionTable에는 CCN(Cisco Communications Network) 시스템에서 지리적으로 구분된 모든 지역의 목록이 포함되어 있습니다. ccmRegionPairTable에는 Unified Communications Manager 클러스터에 대한 지리적 지역 쌍 목록이 포함되어 있습니다. 지리적 지역 쌍은 소스 지역과 대상 지역에 의해 정의됩니다.
ccmTimeZone	테이블에는 Unified Communications Manager 클러스터에 있는 모든 표준 시간대 그룹의 목록이 포함되어 있습니다.
ccmDevicePool	테이블에는 Unified Communications Manager 클러스터의 모든 장치 풀 목록이 포함되어 있습니다. 장치 풀은 지역, 날짜/시간 그룹 및 Unified Communications Manager 그룹에 의해 정의됩니다.

참고 CISCO-CCM-MIB의 '"ccmAlarmConfigInfo" 및 "ccmQualityReportAlarmConfigInfo" 그룹은 설명된 알림과 관련된 구성 매개 변수를 정의합니다.

CISCO-UNITY-MIB

CISCO-UNITY-MIB는 연결 SNMP 에이전트를 사용하여 Cisco Unity Connection에 대한 정보를 가져옵니다.

CISCO-UNITY-MIB 정의를 보려면 다음 링크로 이동하고 **SNMP V2 MIB**를 클릭합니다.

http://www.cisco.com/public/sw-center/netmgmt/cmtk/MIBs.shtml

참고 Cisco Unity Connection은 이 MIB를 지원합니다. Unified Communications Manager 및 IM and Presence Service는 이 MIB를 지원하지 않습니다.

Connection SNMP 에이전트는 다음 개체를 지원합니다.

표 ***23: CISCO-UNITY-MIB*** 개체

개체	설명
ciscoUnityTable	이 테이블은 호스트 이름 및 버전 번호와 같은 Cisco Unity Connection 서버에 대한 일반 정보를 포함합니다.

개체	설명
ciscoUnityPortTable	이 테이블은 Cisco Unity Connection 음성 메시징 포트에 대한 일반 정보를 포함합니다.
일반 Unity 사용 정보 개체	이 그룹에는 Cisco Unity Connection 음성 메시징 포트의 용량과 사용률에 대한 정보가 포함되어 있습니다.

SNMP 구성 요구 사항

시스템에서 기본 SNMP 구성은 제공하지 않습니다. MIB 정보에 액세스하려면 설치 후 SNMP 설정을 구성해야 합니다. Cisco는 SNMP V1, V2c 및 V3 버전을 지원합니다.

SNMP 에이전트는 커뮤니티 이름 및 인증 트랩에 보안을 제공합니다. MIB 정보에 액세스하려면 커뮤니티 이름을 구성해야 합니다. 다음 표에서는 필수 SNMP 구성 설정을 제공합니다.

표 ***24: SNMP*** 구성 요구 사항

구성	**Cisco** 통합 서비스 가용성 페이지
V1/V2c 커뮤니티 문자열	**SNMP** > **V1/V2c** > 커뮤니티 문자열
V3 커뮤니티 문자열	**SNMP** > **V3** > 사용자
시스템 연락처 및 MIB2에 대한 위치	**SNMP** > **SystemGroup** > **MIB2** 시스템 그룹
트랩 대상(V1/V2c)	**SNMP** > **V1/V2c** > 알림 대상
트랩 대상(V3)	**SNMP** > **V3** > 알림 대상

SNMP 버전 1 지원

SMI(관리 정보) 구조의 사양 내에서 작동하는 SNMP의 초기 구현 SNMPv1(SNMP 버전 1)은 UDP(사용자 데이터그램 프로토콜) 및 IP(인터넷 프로토콜)와 같은 프로토콜을 통해 작동합니다.

SNMPv1 SMI는 테이블 형식 개체(즉, 여러 변수가 포함된 개체)의 인스턴스를 그룹화하는 데 사용되는 고도로 구조화된 테이블(MIB)을 정의합니다. 테이블에는 인덱스되는 0개 이상의 행이 포함되어 있으므로 SNMP에서 지원되는 명령을 사용하여 전체 행을 검색하거나 변경할 수 있습니다.

SNMPv1을 사용하는 경우에는 NMS가 요청을 발행하고 관리되는 장치가 응답을 반환합니다. 에이전트는 트랩 작업을 사용하여 NMS에게 중요한 이벤트를 비동기적으로 알립니다.

서비스 가용성 GUI에서는 **V1/V2c** 구성 창에서 SNMPv1 지원을 구성합니다.

SNMP 버전 2c 지원

SNMPv1과 마찬가지로, SNMPv2c는 관리 정보(SMI) 구조의 사양 내에서 작동합니다. MIB 모듈에는 상호 관련된 관리 개체에 대한 정의가 포함되어 있습니다. SNMPv1에서 사용되는 작업은 SNMPv2에 사용되는 것과 유사합니다. 예를 들어, SNMPv2 트랩 작업은 SNMPv1에 사용된 것과 동일한 기능을 제공하지만 다른 메시지 형식을 사용하고 SNMPv1 트랩을 대체합니다.

SNMPv2c의 알림 작업을 사용하면 하나의 NMS가 다른 NMS로 트랩 정보를 전송하고 NMS로부터 응답을 받을 수 있습니다.

서비스 가용성 GUI에서는 **V1/V2c** 구성 창에서 SNMPv2c 지원을 구성합니다.

SNMP 버전 3 지원

SNMP 버전 3은 인증(요청을 진짜 소스에서 수신하는지 확인), 프라이버시(데이터 암호화), 인증(사용자가 요청된 작업을 허용하는지 확인) 및 액세스 제어(사용자에게 요청된 개체에 대한 액세스 권한이 있음)와 같은 보안 기능을 제공합니다. SNMP 패킷이 네트워크에 노출되지 않도록 하려면 SNMPv3을 사용하여 암호화를 구성할 수 있습니다.

참고 릴리스 12.5(1)SU1부터는 Unified Communications Manager에서 MD5 또는 DES 암호화 방법이 지원되지 않습니다. 인증 프로토콜로 SHA 또는 AES 중 하나를 선택하면서 SNMPv3 사용자를 추가할 수 있습니다.

SNMPv1 및 v2와 같은 커뮤니티 문자열을 사용하는 대신에 SNMPv3이 SNMP 사용자를 사용합니다.

서비스 가용성 GUI에서는 **V3** 구성 창에서 SNMPv3 지원을 구성합니다.

SNMP 서비스

다음 테이블에 있는 서비스는 SNMP 작업을 지원합니다.

참고 SNMP 마스터 에이전트는 MIB 인터페이스에 대한 기본 서비스 역할을 합니다. Cisco CallManager SNMP 서비스를 수동으로 활성화해야 합니다. 설치 후에 다른 모든 SNMP 서비스를 실행해야 합니다.

표 ***25: SNMP*** 서비스

MIB	서비스	창
CISCO-CCM-MIB	Cisco CallManager SNMP 서비스	**Cisco** 통합 서비스 가용성 > 도구 > 제어 센터 - 기능 서비스. 서버를 선택한 다음 성능 및 모니터링 범주를 선택합니다.

MIB	서비스	창
SNMP 에이전트	SNMP 마스터 에이전트	**Cisco** 통합 서비스 가용성 > 도구 > 제어 센터 - 네트워크 서비스. 서버를 선택한 다음 플랫폼 서비스 범주를 선택합니다. **Cisco Unified IM and Presence** 서비스 가능성도구 > 제어 센터 - 네트워크 서비스 서버를 선택한 다음 플랫폼 서비스 범주를 선택합니다.
CISCO-CDP-MIB	Cisco CDP 에이전트	
SYSAPPL-MIB	시스템 애플리케이션 에이전트	
MIB-II	MIB2 에이전트	
HOST-RESOURCES-MIB	호스트 리소스 에이전트	
CISCO-SYSLOG-MIB	Cisco Syslog Agent	
하드웨어 MIB	기본 에이전트 어댑터	
CISCO-UNITY-MIB	연결 SNMP 에이전트	**Cisco Unity Connection Serviceability** > 도구 > 서비스 관리. 서버를 선택한 다음 기본 서비스 범주를 선택합니다.

주의 네트워크 관리 시스템이 더 이상 Unified Communications Manager 또는 Cisco Unity Connection 네트워크를 모니터링하지 않으므로 SNMP 서비스를 중지하면 데이터가 손실될 수 있습니다. 기술 지원팀이 사용자에게 지시하지 않는 한 서비스를 중지하지 마십시오.

SNMP 커뮤니티 문자열 및 사용자

SNMP 커뮤니티 문자열은 보안을 제공하지 않지만, MIB 개체에 대한 액세스를 인증하고 포함된 암호로 작동합니다. SNMPv1 및 v2c에 대해서만 SNMP 커뮤니티 문자열을 구성합니다.

SNMPv3은 커뮤니티 문자열을 사용하지 않습니다. 대신, 버전 3은 SNMP 사용자를 사용합니다. 이러한 사용자는 커뮤니티 문자열과 동일한 용도로 사용되지만, 사용자는 암호화 또는 인증을 구성할 수 있으므로 보안을 제공합니다.

서비스 가용성 GUI에서 기본 커뮤니티 문자열 또는 사용자가 존재하지 않습니다.

SNMP 트랩 및 알림

SNMP 에이전트는 중요한 시스템 이벤트를 식별하기 위해 트랩 또는 알림 형태로 NMS에게 알림을 전송합니다. 트랩은 대상에서 확인을 수신하지 않지만, 알림은 확인을 수신합니다. 서비스 가용성 GUI의 SNMP 알림 대상 구성 창을 사용하여 알림 대상을 구성합니다.

참고 Unified Communications Manager는 Unified Communications Manager 및 IM and Presence Service 시스템에서 SNMP 트랩을 지원합니다.

SNMP 알림의 경우, 해당 트랩 플래그가 활성화되면 시스템에서 트랩을 즉시 전송합니다. syslog 에이전트의 경우 알람 및 시스템 수준 로그 메시지가 로그를 위해 syslog 데몬에 전송됩니다. 그리고 일부 표준 타사 애플리케이션에서는 로그 메시지를 syslog 데몬에 전송하여 로깅할 수 있습니다. 이러한 로그 메시지는 syslog 파일에 로컬로 기록되고 SNMP 트랩/알림으로 변환 됩니다.

다음 목록은 구성된 트랩 대상으로 전송되는 Unified Communications Manager SNMP 트랩/통지 메시지를 포함합니다.

- Unified Communications Manager 실패
- 전화기 실패
- 전화기 상태 업데이트
- 게이트웨이 실패
- 미디어 리소스 목록이 모두 사용됨
- 경로 목록이 모두 사용됨
- 게이트웨이 레이어 2 변경
- 품질 보고서
- 장난 전화
- Syslog 메시지 생성됨

팁 알림 대상을 구성하기 전에 필요한 SNMP 서비스가 활성화되어 실행 중인지 확인합니다. 커뮤니티 문자열/사용자에 대한 권한을 올바르게 구성했는지 확인합니다.

서비스 가용성 GUI에서 **SNMP** > **V1/V2** > 알림 대상 또는 **SNMP** > **V3** > 알림 대상을 선택하여 SNMP 트랩 대상을 구성합니다.

다음 표에서는 NMS(네트워크 관리 시스템)에서 구성하는 트랩/알림 매개 변수에 대한 정보를 제공합니다. NMS를 지원하는 SNMP 제품 설명서에 설명된 대로, NMS에 적절한 명령을 실행하여 테이블의 값을 구성할 수 있습니다.

참고 테이블에 나열된 모든 매개 변수는 마지막 두 매개 변수를 제외하고 CISCO-CCM-MIB의 일부입니다. 마지막 2 개, clogNotificationsEnabled 및 clogMaxSeverity는 ISCO-SYSLOG-MIB의 일부를 구성합니다.

IM and Presence Service의 경우, NMS에 clogNotificationsEnabled 및 clogMaxSeverity 트랩/알림 매개 변수만 구성합니다.

표 ***26: Cisco Unified Communications Manager*** 트랩/알림 구성 매개 변수

매개 변수명	기본값	생성된 트랩	구성 권장 사항
ccmCallManagerAlarmEnable	True	ccmCallManagerFailed ccmMediaResourceListExhausted ccmRouteListExhausted ccmTLSConnectionFailure	기본 사양을 유지합니다.
ccmGatewayAlarmEnable	True	ccmGatewayFailed ccmGatewayLayer2Change Cisco Unified Communications Manager 관리에서 Cisco ATA 186 장치를 전화기로 구성할 수 있지만, Unified Communications Manager가 Cisco ATA 장치에 대한 SNMP 트랩을 전송하면 게이트웨이 유형 트랩(예: ccmGatewayFailed)이 전송됩니다.	없음 기본값은 이 트랩을 활성화로 지정합니다.
ccmPhoneStatusUpdateStorePeriod ccmPhoneStatusUpdateAlarmInterval	1800 0	ccmPhoneStatusUpdate	ccmPhoneStatusUpdateAlarmInterval을 30과 3600 사이의 값으로 설정합니다.
ccmPhoneFailedStorePeriod ccmPhoneFailedAlarmInterval	1800 0	ccmPhoneFailed	ccmPhoneFailedAlarmInterval을 30과 3600 사이의 값으로 설정합니다.
ccmMaliciousCallAlarmEnable	True	ccmMaliciousCall	없음 기본값은 이 트랩을 활성화로 지정합니다.
ccmQualityReportAlarmEnable	True	이 트랩은 Cisco Extended Functions 서비스가 활성화되어 서버에서 실행 중인 경우 또는 로컬 Unified Communications Manager 서버에서 클러스터 구성(Unified Communications Manager에만 해당)의 경우에만 생성됩니다. ccmQualityReport	없음 기본값은 이 트랩을 활성화로 지정합니다.
clogNotificationsEnabled	False	clogMessageGenerated	트랩 생성을 활성화하려면 clogNotificationsEnable를 True로 설정합니다.
clogMaxSeverity	알림	clogMessageGenerated	ClogMaxSeverity를 경고로 설정하면 애플리케이션에서 최소 알림 심각도 수준이 있는 syslog 메시지를 생성할 때 SNMP 트랩이 생성됩니다.

SFTP 서버 지원

내부 테스트의 경우 Cisco에서 제공하고 Cisco TAC에서 지원하는 Cisco Prime Collaboration Deployment(PCD)의 SFTP 서버를 사용합니다. SFTP 서버 옵션에 대한 요약은 다음 표를 참조하십시오.

표 ***27: SFTP*** 서버 지원

SFTP 서버	지원 설명
Cisco Prime Collaboration Deployment의 SFTP 서버	이 서버는 Cisco에서 제공 및 테스트하고 Cisco TAC에서 완벽하게 지원하는 유일한 SFTP 서버입니다. 버전 호환성은 Emergency Responder 및 Cisco Prime Collaboration Deployment 버전에 따라 달라집니다. 버전(SFTP) 또는 Emergency Responder를 업그레이드하기 전에 버전이 호환되는지 확인하기 위해 Cisco Prime Collaboration Deployment 관리 설명서를 참조하십시오.
기술 파트너의 SFTP 서버	이러한 서버는 타사에서 제공하고 타사에서 테스트했습니다. 버전 호환성은 타사 테스트에 따라 다릅니다. SFTP 제품을 업그레이드하거나 Unified Communications Manager를 업그레이드할 경우 기술 파트너가 페이지를 참조하십시오.
다른 타사의 SFTP 서버	이러한 서버는 타사에서 제공하고 Cisco TAC에서 공식 지원하지 않습니다. 버전 호환성은 SFTP 버전 및 Emergency Responder 버전의 호환성을 위해 최대한 노력합니다. 참고 이러한 제품은 Cisco에서 테스트하지 않았으므로 기능을 보증할 수 없습니다. Cisco TAC는 이러한 제품을 지원하지 않습니다. SFTP 솔루션을 완벽하게 테스트하고 지원하기 위해 Cisco Prime Collaboration Deployment 또는 기술 파트너를 이용합니다.

SNMP 구성 작업 흐름

이러한 작업을 완료하여 단순한 네트워크 관리 프로토콜을 구성합니다. 작업으로 구성할 SNMP 버전은 다양할 수 있다는 것을 알아야 합니다. SNMP V1, V2c 또는 V3 중에서 선택할 수 있습니다.

시작하기 전에

SNMP 네트워크 관리 시스템을 설치하고 구성합니다.

프로시저

	명령 또는 동작	목적
단계 1	SNMP 서비스 활성화, 173 페이지	필수 SNMP 서비스가 실행 중인지 확인합니다.
단계 2	SNMP 버전에 따라 다음 작업 중 하나를 완료합니다. • SNMP 커뮤니티 문자열 구성, 174 페이지 • SNMP 사용자 구성, 176 페이지	SNMP V1 또는 V2의 경우 커뮤니티 문자열을 구성합니다. SNMP V3의 경우 SNMP 사용자를 구성합니다.
단계 3	원격 SNMP 엔진 ID 가져오기, 180 페이지	SNMP V3의 경우 알림 대상 구성에 필요한 원격 SNMP 엔진의 주소를 가져옵니다. 참고 이 절차는 SNMP V3에 반드시 필요하지만, SNMP V1 또는 V2c에는 선택 사항입니다.
단계 4	SNMP 알림 대상 구성, 180 페이지	모든 SNMP 버전의 경우 SNMP 트랩 및 알림에 대한 알림 대상을 구성합니다.
단계 5	MIB2 시스템 그룹 구성, 185 페이지	MIB-II 시스템 그룹에 대한 시스템 연결 및 시스템 위치를 구성합니다.
단계 6	CISCO-SYSLOG-MIB 트랩 매개 변수, 186 페이지	CISCO-SYSLOG-MIB에 대한 트랩 설정을 구성합니다.
단계 7	CISCO-CCM-MIB 트랩 매개 변수, 187 페이지	Unified Communications Manager만 해당: CISCO-CCM-MIB에 대한 트랩 설정을 구성합니다.
단계 8	SNMP 마스터 에이전트 다시 시작, 187 페이지	SNMP 구성을 완료한 후에는 SNMP 마스터 에이전트를 다시 시작합니다.
단계 9	SNMP 네트워크 관리 시스템에서 Unified Communications Manager 트랩 매개 변수를 구성합니다.	

SNMP 서비스 활성화

이 절차를 사용하여 SNMP 서비스가 작동 중인지 확인합니다.

프로시저

단계 1 Cisco 통합 서비스 가용성에 로그인합니다.

단계 **2** **Cisco SNMP Master Agent** 네트워크 서비스가 실행 중인지 확인합니다. 서비스는 기본적으로 켜져 있습니다.

a) 도구제어 센터 > - 네트워크 서비스를 선택합니다.
b) 게시자 노드를 선택하고 이동을 클릭합니다.
c) **Cisco SNMP Master Agent** 서비스가 실행되고 있는지 확인합니다.

단계 **3** **Cisco Call Manager SNMP** 서비스를 시작합니다.

a) 제어 센터 > 서비스 활성화를 선택합니다.
b) 서버 드롭다운에서 게시자 노드를 선택하고 이동을 클릭합니다.
c) **Cisco CALL Manager SNMP** 서비스가 실행 중인지 확인합니다. 실행 중이 아니면 해당 확인란을 선택하고 저장을 클릭합니다.

다음에 수행할 작업

SNMP V1 또는 V2c를 구성하는 경우 SNMP 커뮤니티 문자열 구성, 174 페이지.

SNMP V3을 구성하는 경우 SNMP 사용자 구성, 176 페이지.

SNMP 커뮤니티 문자열 구성

SNMP V1 또는 V2c를 배포하는 경우 이 절차를 사용하여 SNMP 커뮤니티 문자열을 설정합니다.

참고 이 절차는 SNMP V1 또는 V2c에 필요합니다. SNMP V3의 경우 커뮤니티 문자열 대신 SNMP 사용자를 구성합니다.

프로시저

단계 **1** Cisco 통합 서비스 가용성에서 **SNMP** > **V1/V2c** > 커뮤니티 문자열을 선택합니다.

단계 **2** 서버를 선택하고 찾기 를 클릭하여 기존 커뮤니티 문자열을 검색합니다. 선택적으로 검색 매개 변수를 입력하여 특정 커뮤니티 문자열을 찾을 수 있습니다.

단계 **3** 다음 중 하나를 수행합니다.

- 기존 SNMP 커뮤니티 문자열을 편집하려면 문자열을 선택합니다.
- 새 커뮤니티 문자열을 추가하려면 새로 추가를 클릭합니다.

참고 기존 커뮤니티 문자열을 삭제하려면 문자열을 선택하고 선택한 항목 삭제를 클릭합니다. 사용자를 삭제한 후에는 Cisco SNMP Master Agent를 다시 시작합니다.

단계 **4** 커뮤니티 문자열 이름을 입력합니다.

단계 **5** **SNMP** 커뮤니티 문자열 구성 창에서 필드를 완성합니다. 필드 및 해당 설정에 대한 도움말은 커뮤니티 문자열 구성 설정, 175 페이지의 내용을 참조하십시오.

단계 **6** 액세스 권한 드롭다운에서 이 커뮤니티 문자열에 대한 권한을 구성합니다.

단계 **7** 이러한 설정이 모든 클러스터 노드에 적용되도록 하려면 모든 노드에 적용 확인란을 선택합니다.

단계 **8** 저장을 클릭합니다.

단계 **9** 확인을 클릭하여 SNMP 마스터 에이전트 서비스를 다시 시작하고 변경 사항을 적용합니다.

다음에 수행할 작업

SNMP 알림 대상 구성, 180 페이지

커뮤니티 문자열 구성 설정

다음 표에서는 커뮤니티 문자열 구성 설정을 설명합니다.

표 ***28:*** 커뮤니티 문자열 구성 설정

필드	설명
서버	커뮤니티 문자열 찾기의 절차를 수행할 때 서버 선택을 지정했기 때문에 커뮤니티 문자열 구성 창에서 이 설정이 읽기 전용으로 표시됩니다. 커뮤니티 문자열에 대한 서버를 변경하려면 커뮤니티 문자열 찾기 절차를 수행합니다.
커뮤니티 문자열	커뮤니티 문자열 이름을 입력합니다. 이 이름은 최대 32자로 구성되고 영문자, 하이픈(-) 및 밑줄(_) 조합이 포함될 수 있습니다. 팁 외부인이 파악하기 어려운 커뮤니티 문자열 이름을 선택합니다. 커뮤니티 문자열을 편집할 때 커뮤니티 문자열의 이름을 변경할 수 없습니다.
모든 호스트에서 SNMP 패킷 수락	모든 호스트에서 SNMP 패킷을 수락하려면 이 버튼을 클릭합니다.
다음 호스트의 SNMP 패킷만 수락	특정 호스트에서 SNMP 패킷을 수락하려면 라디오 버튼을 클릭합니다. 호스트 이름//IPv4/IPv6 주소 필드에 SNMP 패킷을 수락할 IPv4 또는 IPv6 주소를 입력하고 삽입을 클릭합니다. IPv4 주소는 점으로 구분된 십진수 형식입니다. 예를 들어 10.66.34.23. IPv6 주소는 콜론으로 구분된 16진수 형식입니다. 예를 들어 2001:0db8:85a3:0000:0000:8a2e:0370:7334 또는 2001:0db8:85a3::8a2e:0370:7334. SNMP 패킷을 수락할 각 주소에 대해 이 과정을 반복합니다. 주소를 삭제하려면 호스트 IPv4/IPv6 주소 목록 상자에서 해당 주소를 선택하고제거를 클릭합니다.

필드	설명
액세스 권한	드롭다운 목록 상자의 다음 목록에서 적절한 액세스 수준을 선택합니다. 읽기 전용 커뮤니티 문자열은 MIB 개체의 값만 읽을 수 있습니다. **ReadWrite** 커뮤니티 문자열은 MIB 개체의 값을 읽고 쓸 수 있습니다. **ReadWriteNotify** 커뮤니티 문자열은 MIB 개체의 값을 읽고 쓰고, 트랩에 대한 MIB 개체 값을 전송하고 메시지를 알릴 수 있습니다. **NotifyOnly** 커뮤니티 문자열은 트랩에 대한 MIB 개체 값만 전송하고 메시지를 알릴 수 있습니다. **ReadNotifyOnly** 커뮤니티 문자열은 MIB 개체의 값을 읽을 수 있고 트랩 및 알림 메시지에 대한 값을 전송할 수도 있습니다. 없음 커뮤니티 문자열은 트랩 정보를 읽거나 쓰거나 전송할 수 없습니다. 팁 트랩 구성 매개 변수를 변경하려면 NotifyOnly, ReadNotifyOnly 또는 ReadWriteNotify 권한을 사용하여 커뮤니티 문자열을 구성합니다. IM and Presence Service는 ReadNoticyOnly를 지원하지 않습니다.
모든 노드에 적용	커뮤니티 문자열을 클러스터의 모든 노드에 적용하려면이 확인란을 선택합니다. 이 필드는 Unified Communications Manager 및 IM and Presence Service 클러스터에만 적용됩니다.

SNMP 사용자 구성

SNMP V3을 배포하는 경우 이 절차를 사용하여 SNMP 사용자를 설정합니다.

참고 이 절차는 SNMP V3에만 필요합니다. SNMP V1 또는 V2c의 경우 대신 커뮤니티 문자열을 구성합니다.

프로시저

단계 **1** Cisco 통합 서비스 가용성에서 **SNMP** > **V3** > 사용자를 선택합니다.

단계 **2** 서버를 선택하고 찾기 를 클릭하여 기존 SNMP 사용자를 검색합니다. 선택적으로 검색 매개 변수를 입력하여 특정 사용자를 찾을 수 있습니다.

단계 **3** 다음 중 하나를 수행합니다.

- 기존 SNMP 사용자를 편집하려면 사용자를 선택합니다.
- 새 SNMP 사용자를 추가하려면 새로 추가를 클릭합니다.

참고 기존 사용자를 삭제하려면 사용자를 선택하고 선택한 항목 삭제를 클릭합니다. 사용자를 삭제한 후에는 Cisco SNMP Master Agent를 다시 시작합니다.

단계 **4** **SNMP** 사용자 이름을 입력합니다.

단계 **5** SNMP 사용자 구성 설정을 입력합니다. 필드 및 해당 설정에 대한 도움말은 SNMP V3 사용자 구성 설정, 178 페이지의 내용을 참조하십시오.

팁 구성을 저장하기 전에 언제든지 모두 지우기 버튼을 클릭하여 창에 있는 모든 설정에 입력한 정보를 모두 삭제할 수 있습니다.

단계 **6** 액세스 권한 드롭다운에서 이 사용자에게 할당할 액세스 권한을 구성합니다.

단계 **7** 이 구성이 모든 클러스터 노드에 적용되도록 하려면 모든 노드에 적용 확인란을 선택합니다.

단계 **8** 저장을 클릭합니다.

단계 **9** 확인을 클릭하여 SNMP 마스터 에이전트를 다시 시작합니다.

참고 구성한 사용자를 사용하여 서버에 액세스하려면 해당 인증 및 프라이버시 설정을 사용하여 NMS에서이 사용자를 구성해야 합니다.

다음에 수행할 작업

원격 SNMP 엔진 ID 가져오기, 180 페이지

SNMP V3 사용자 구성 설정

다음 표에서는 SNMP V3 사용자 구성 설정에 대해 설명합니다.

표 ***29: SNMP V3*** 사용자 구성 설정

필드	설명
서버	이 설정은 알림 대상 찾기 절차를 수행할 때 서버를 지정했기 때문에 읽기 전용으로 표시됩니다. 액세스를 제공할 서버를 변경하려면 절차를 수행하여 SNMP 사용자를 찾습니다.
사용자 이름	필드에 액세스를 제공할 사용자의 이름을 입력합니다. 이 이름은 최대 32자로 구성되고 영문자, 하이픈(-) 및 밑줄(_) 조합이 포함될 수 있습니다. 팁 NMS(네트워크 관리 시스템)에 대해 이미 구성된 사용자를 입력합니다. 기존 SNMP 사용자의 경우 이 설정은 읽기 전용으로 표시됩니다.
인증 필요	인증을 요구하려면 확인란을 선택하고 암호 및 암호 다시 입력 필드에 암호를 입력한 다음 적절한 프로토콜을 선택합니다. 암호는 8자 이상을 포함해야 합니다. 참고 FIPS 모드 또는 고급 보안 모드가 활성화된 경우 프로토콜로 **SHA**를 선택합니다.
프라이버시 필요	인증 필요 확인란을 선택한 경우 프라이버시 정보를 지정할 수 있습니다. 프라이버시를 요구하려면 확인란을 선택하고 암호 및 암호 다시 입력 필드에 암호를 입력한 다음 프로토콜 확인란을 선택합니다. 암호는 8자 이상을 포함해야 합니다. 참고 FIPS 모드 또는 고급 보안 모드가 활성화된 경우 프로토콜로 **AES128**를 선택합니다.
모든 호스트에서 SNMP 패킷 수락	모든 호스트에서 SNMP 패킷을 수락하려면 라디오 버튼을 클릭합니다.

필드	설명
다음 호스트의 SNMP 패킷만 수락	특정 호스트에서 SNMP 패킷을 수락하려면 라디오 버튼을 클릭합니다. 호스트 이름//IPv4/IPv6 주소 필드에 SNMP 패킷을 수락할 IPv4 또는 IPv6 주소를 입력하고 삽입을 클릭합니다. IPv4 주소는 점으로 구분된 십진수 형식입니다. 예를 들어 10.66.34.23. IPv6 주소는 콜론으로 구분된 16진수 형식입니다. 예를 들어 2001:0db8:85a3:0000:0000:8a2e:0370:7334 또는 2001:0db8:85a3::8a2e:0370:7334. SNMP 패킷을 수락할 각 주소에 대해 이 과정을 반복합니다. 주소를 삭제하려면 호스트 IPv4/IPv6 주소 목록 상자에서 해당 주소를 선택하고제거를 클릭합니다.
액세스 권한	드롭다운 목록 상자에서 액세스 수준에 대해 다음 옵션 중 하나를 선택합니다. 읽기 전용 MIB 개체의 값만 읽을 수 있습니다. **ReadWrite** MIB 개체의 값을 읽고 쓸 수 있습니다. **ReadWriteNotify** MIB 개체의 값을 읽고 쓰고 트랩에 대한 MIB 개체 값을 전송하고 메시지를 알릴 수 있습니다. **NotifyOnly** 트랩 및 알림 메시지에 대해서만 MIB 개체 값을 보낼 수 있습니다. **ReadNotifyOnly** MIB 개체의 값을 읽고 트랩 및 알림 메시지에 대한 값을 보낼 수 있습니다. 없음 트랩 정보는 읽거나 쓰거나 보낼 수 없습니다. 팁 트랩 구성 매개 변수를 변경하려면 NotifyOnly, ReadNotifyOnly 또는 ReadWriteNotify 권한을 사용하여 사용자를 구성합니다.
모든 노드에 적용	클러스터의 모든 노드에 사용자 구성을 적용하려면 이 확인란을 선택합니다. 이는 Unified Communications Manager 및 IM and Presence Service 클러스터에만 적용됩니다.

원격 SNMP 엔진 ID 가져오기

SNMP V3을 배포하는 경우 이 절차를 사용하여 알림 대상 구성에 필요한 원격 SNMP 엔진 ID를 가져옵니다.

참고 이 절차는 SNMP V3에 반드시 필요하지만, SNMP V1 또는 2C의 경우에는 선택 사항입니다.

프로시저

단계 **1** 명령줄 인터페이스에 로그인합니다.

단계 **2** `utils SNMP walk 1` CLI 명령을 실행합니다.

단계 **3** 구성된 커뮤니티 문자열(SNMP V1/V2) 또는 구성된 사용자(SNMP V3 사용)를 입력합니다.

단계 **4** 서버의 IP 주소를 입력합니다. 예를 들어, localhost의 경우 `127.0.0.1`을 입력합니다.

단계 **5** OID(개체 ID)로 `1.3.6.1.6.3.10.2.1.1.0`을 입력합니다.

단계 **6** 파일의 경우 `파일`을 입력합니다.

단계 **7** `y`를 입력합니다.
시스템 출력이 원격 SNMP 엔진 ID를 나타내는 HEX-STRING입니다.

단계 **8** SNMP가 실행 중인 각 노드에서 이 절차를 반복합니다.

다음에 수행할 작업

SNMP 알림 대상 구성, 180 페이지

SNMP 알림 대상 구성

이 절차를 사용하여 SNMP 트랩 및 알림에 대한 알림 대상을 구성합니다. 이 절차는 SNMP V1, V2c 또는 V3에 사용할 수 있습니다.

시작하기 전에

SNMP 커뮤니티 문자열 또는 SNMP 사용자를 아직 설정하지 않은 경우 다음 작업 중 하나를 완료합니다.

- SNMP V1/V2의 경우 다음을 참조하십시오. SNMP 커뮤니티 문자열 구성, 174 페이지
- SNMP V3의 경우 다음을 참조하십시오. SNMP 사용자 구성, 176 페이지

프로시저

단계 **1** Cisco Unifeid Serviceability에서 다음 중 하나를 선택합니다.

- SNMP V1/V2의 경우 **SNMP** > **V1/v2** > 알림 대상 을 선택합니다
- SNMP V3의 경우 [**SNMP** > **v3** > 알림 대상 을 선택합니다

단계 **2** 서버를 선택하고 찾기 를 클릭하여 기존 SNMP 알림 대상을 검색합니다. 선택적으로 검색 매개 변수를 입력하여 특정 대상을 찾을 수 있습니다.

단계 **3** 다음 중 하나를 수행합니다.

- 기존 SNMP 알림 대상을 편집하려면 알림 대상을 선택합니다.
- 새 SNMP 알림 대상을 추가하려면 새로 추가를 클릭합니다.

참고 기존 SNMP 알림 대상을 삭제하려면 대상을 선택하고 선택한 항목 삭제를 클릭합니다. 사용자를 삭제한 후에는 **Cisco SNMP Master Agent**를 다시 시작합니다.

단계 **4** 호스트 **IP** 주소 드롭다운에서 기존 주소를 선택하거나 새로 추가를 클릭하고 새 호스트 IP 주소를 입력합니다.

단계 **5** SNMP V1/V2에만 해당됩니다. **SNMP** 버전 필드에서 SNMP V1 또는 V2c를 구성하는지 여부에 따라 V1 또는 V2C 라디오 버튼을 선택합니다.

단계 **6** SNMP V1/V2의 경우 다음 단계를 완료하십시오.

a) SNMP V2에만 해당됩니다. 알림 유형 드롭다운에서 알림 또는 트랩을 선택합니다.
b) 구성한 커뮤니티 문자열을 선택합니다.

단계 **7** SNMP V3의 경우 다음 단계를 완료하십시오.

a) 알림 유형 드롭다운에서 알림 또는 트랩을 선택합니다.
b) 원격 **SNMP** 엔진 **ID** 드롭다운에서 기존 엔진 ID를 선택하거나 새로 추가를 선택하고 새 ID를 입력합니다.
c) 보안 수준 드롭다운에서 적절한 보안 수준을 할당합니다.

단계 **8** 이 구성이 모든 클러스터 노드에 적용되도록 하려면 모든 노드에 적용 확인란을 선택합니다.

단계 **9** 삽입을 클릭합니다.

단계 **10** 확인을 클릭하여 SNMP 마스터 에이전트를 다시 시작합니다.

예

참고 [알림 대상 구성 창에서 필드 설명 도움말은 다음 항목 중 하나를 참조하십시오.

- SNMP V1 및 V2c에 대한 알림 대상 설정, 182 페이지
- SNMP V3에 대한 알림 대상 설정, 183 페이지

다음에 수행할 작업

MIB2 시스템 그룹 구성, 185 페이지

SNMP V1 및 V2c에 대한 알림 대상 설정

다음 표에서는 SNMP V1/V2c에 대한 알림 대상 구성 설정에 대해 설명합니다.

표 *30: SNMP V1/V2c*에 대한 알림 대상 구성 설정

필드	설명
서버	이 설정은 사용자가 알림 대상을 찾기 위해 절차를 수행할 때 서버를 지정했기 때문에 읽기 전용으로 표시됩니다. 알림 대상에 대한 서버를 변경하려면 절차를 수행하여 커뮤니티 문자열을 찾습니다.
호스트 IPv4/IPv6 주소	드롭다운 목록 상자에서 트랩 대상의 호스트 IPv4/IPv6 주소를 선택하거나 새로 추가를 클릭합니다. 새로 추가를 클릭하는 경우 호스트 IPv4/IPv6 주소 필드에 트랩 대상의 IPv4/IPv6 주소를 입력합니다. 기존 알림 대상의 경우 호스트 IP 주소 구성을 수정할 수 없습니다.
호스트 IPv4/IPv6 주소	필드에서 SNMP 패킷을 수락할 IPv4 또는 IPv6 주소를 입력합니다. IPv4 주소는 점으로 구분된 십진수 형식입니다. 예를 들어 10.66.34.23. IPv6 주소는 콜론으로 구분된 16진수 형식입니다. 예를 들어 2001:0db8:85a3:0000:0000:8a2e:0370:7334 또는 2001:0db8:85a3::8a2e:0370:7334.
포트 번호	필드에서 SNMP 패킷을 수신하는 대상 서버에 알림 수신 포트 번호를 입력합니다.
V1 또는 V2c	SNMP 버전 정보 창에서 해당 SNMP 버전 라디오 버튼(V1 또는 V2c)을 클릭합니다. 이 버튼은 사용 중인 SNMP 버전에 따라 달라집니다. • V1을 선택하는 경우 커뮤니티 문자열 설정을 구성합니다. • V2c를 선택하는 경우 알림 유형 설정을 구성한 다음 커뮤니티 문자열을 구성합니다.

필드	설명
커뮤니티 문자열	드롭다운 목록 상자에서 이 호스트가 생성하는 알림 메시지에 사용할 커뮤니티 문자열 이름을 선택합니다. 최소 알림 권한(ReadWriteNotify 또는 알림만)이 있는 커뮤니티 문자열만 표시됩니다. 이러한 권한을 사용하여 커뮤니티 문자열을 구성하지 않은 경우 드롭다운 목록 상자에 옵션이 표시되지 않습니다. 필요한 경우 새 uiCommunity 문자열 만들기를 클릭하여 커뮤니티 문자열을 만듭니다. IM and Presence만 해당: 최소 알림 권한이 있는 커뮤니티 문자열만 (ReadWriteNotify, ReadNotifyOnly 또는 알림만) 표시됩니다. 이러한 권한을 사용하여 커뮤니티 문자열을 구성하지 않은 경우 드롭다운 목록 상자에 옵션이 표시되지 않습니다. 필요한 경우 새 커뮤니티 문자열 만들기를 클릭하여 커뮤니티 문자열을 만듭니다.
알림 유형	드롭다운 목록 상자에서 적절한 알림 유형을 선택합니다.
모든 노드에 적용	클러스터의 모든 노드에 알림 대상 구성을 적용하려면 이 확인란을 선택합니다. 이는 Cisco Unified Communications Manager 및 IM and Presence Service 클러스터에만 적용됩니다.

SNMP V3에 대한 알림 대상 설정

다음 표에서는 SNMP V3에 대한 알림 대상 구성 설정에 대해 설명합니다.

표 ***31: SNMP V3***에 대한 알림 대상 구성 설정

필드	설명
서버	이 설정은 사용자가 SNMP V3 알림 대상을 찾기 위해 절차를 수행할 때 서버를 지정했기 때문에 읽기 전용으로 표시됩니다. 알림 대상에 대한 서버를 변경하려면 절차를 수행하여 SNMP V3 알림 대상을 찾고 다른 서버를 선택합니다.
호스트 IPv4/IPv6 주소	드롭다운 목록 상자에서 트랩 대상의 호스트 IPv4/IPv6 주소를 선택하거나 새로 추가를 클릭합니다. 새로 추가를 클릭하는 경우 호스트 IPv4/IPv6 주소 필드에 트랩 대상의 IPv4/IPv6 주소를 입력합니다. 기존 알림 대상의 경우 호스트 IP 주소 구성을 수정할 수 없습니다.
호스트 IPv4/IPv6 주소	필드에서 SNMP 패킷을 수락할 IPv4 또는 IPv6 주소를 입력합니다. IPv4 주소는 점으로 구분된 십진수 형식입니다. 예를 들어 10.66.34.23. IPv6 주소는 콜론으로 구분된 16진수 형식입니다. 예를 들어 2001:0db8:85a3:0000:0000:8a2e:0370:7334 또는 2001:0db8:85a3::8a2e:0370:7334.

필드	설명
포트 번호	필드에 대상 서버에 대한 알림 수신 포트 번호를 입력합니다.
알림 유형	드롭다운 목록 상자에서 알림 또는 트랩을 선택합니다. 팁 알림 옵션을 선택하는 것이 좋습니다. 알림 기능은 응답될 때까지 메시지를 재전송하므로 트랩보다 더 안정적으로 수행할 수 있습니다.
원격 SNMP 엔진 ID	이 설정은 알림 유형 드롭다운 목록 상자에서 알림을 선택한 경우 표시됩니다. 드롭다운 목록 상자에서 엔진 ID를 선택하거나 새로 추가를 선택합니다. 새로 추가를 선택한 경우에는 16진수 값이 필요한 원격 SNMP 엔진 ID 필드에 ID를 입력합니다.
보안 레벨	드롭다운 목록 상자에서 사용자에 대한 적절한 보안 수준을 선택합니다. **noAuthNoPriv** 인증 또는 프라이버시가 구성되지 않았습니다. **authNoPriv** 인증을 구성했지만 프라이버시를 구성하지 않았습니다. **authPriv** 인증 및 프라이버시가 구성되었습니다.
사용자 정보 창	창에서 다음 작업 중 하나를 수행하여 사용자와 알림 대상을 연결하거나 연결을 해제합니다. 1. 새 사용자를 만들려면 새 사용자 만들기를 클릭합니다. 2. 기존 사용자를 수정하려면 사용자의 라디오 버튼을 클릭한 다음 선택한 사용자 업데이트를 클릭합니다. 3. 사용자를 삭제하려면 사용자의 라디오 버튼을 클릭한 다음 선택한 사용자 삭제를 클릭합니다. 표시되는 사용자는 알림 대상에 대해 구성한 보안 레벨에 따라 달라 집니다.
모든 노드에 적용	클러스터의 모든 노드에 알림 대상 구성을 적용하려면 이 확인란을 선택합니다. 이는 Cisco Unified Communications Manager 및 IM and Presence Service 클러스터에만 적용됩니다.

MIB2 시스템 그룹 구성

이 절차를 사용하여 MIB-II 시스템 그룹에 대한 시스템 연결 및 시스템 위치를 구성합니다. 예를 들어 시스템 연락처로 관리자 555-121-6633, 시스템 위치로 SanJose, Bldg 23, 2nd floor를 입력할 수 있습니다. 이 절차는 SNMP V1, V2 및 V3에 사용할 수 있습니다.

프로시저

단계 **1** Cisco 통합 서비스 가용성에서 **SNMP** > **SystemGroup** > **MIB2** 시스템 그룹을 선택합니다.

단계 **2** 서버 드롭다운에서 노드를 선택하고 이동을 클릭합니다.

단계 **3** 시스템 연결 및 시스템 위치 필드를 완료합니다.

단계 **4** 이러한 설정이 모든 클러스터 노드에 적용되도록 하려면 모든 노드에 적용 확인란을 선택합니다.

단계 **5** 저장을 클릭합니다.

단계 **6** 확인을 클릭하여 SNMP 마스터 에이전트 서비스를 다시 시작합니다.

예

참고 필드 설명 도움말은 다음을 참조하십시오. MIB2 시스템 그룹 설정, 185 페이지

참고 모두 지우기를 클릭하여 필드를 지울 수 있습니다. 모두 지우기를 클릭한후 저장을 클릭하면 레코드가 삭제됩니다.

MIB2 시스템 그룹 설정

다음 표에서는 MIB2 시스템 그룹 구성 설정을 설명합니다.

표 ***32: MIB2*** 시스템 그룹 구성 설정

필드	설명
서버	드롭다운 목록 상자에서 연락처를 구성할 서버를 선택한 다음 이동을 클릭합니다.
시스템 연락처	문제가 발생했을 때 알릴 사람을 입력합니다.
시스템 위치	시스템 연락처로 식별되는 사람의 위치를 입력합니다.

필드	설명
모든 노드에 적용	클러스터의 모든 노드에 시스템 구성을 적용하려면 선택합니다. 이는 Unified Communications Manager 및 IM and Presence Service 클러스터에만 적용됩니다.

CISCO-SYSLOG-MIB 트랩 매개 변수

다음 지침을 사용하여 시스템에서 CISCO-SYSLOG-MIB 트랩 설정을 구성합니다.

- SNMP Set 작업을 사용하여 clogsNotificationEnabled (1.3.6.1.4.1.9.9.41.1.1.2)를 True로 설정합니다. 예를 들어, net-SNMP set 유틸리티를 사용하여 linux 명령줄에서 다음을 사용하여 이 OID를 True로 설정합니다.

```
snmpset -c <community string>-v2c <transmitter ipaddress>
1.3.6.1.4.1.9.9.41.1.1.2.0 i 1
```

  SNMP Set 작업에 다른 SNMP 관리 애플리케이션을 사용할 수도 있습니다.

- SNMP Set 작업을 사용하여 clogMaxSeverity (1.3.6.1.4.1.9.9.41.1.1.3) 값을 설정합니다. 예를 들어, net-SNMP set 유틸리티를 사용하여 linux 명령줄에서 다음을 사용하여 이 OID 값을 설정합니다.

```
snmpset-c public-v2c <transmitter ipaddress> 1.3.6.1.4.1.9.9.41.1.1.3.0 i
<value>
```

  <value> 설정에 대한 심각도 번호를 입력합니다. 심각도 값은 심각도가 감소하면 증가합니다. 값 1(긴급)은 가장 높은 심각도를 나타내고 값 8(디버그)은 최저 심각도를 나타냅니다. Syslog 에이전트는 사용자가 지정한 값보다 큰 메시지는 무시합니다. 예를 들어, 모든 syslog 메시지를 트래핑 하려면 값 8을 사용합니다.

  심각도 값은 다음과 같습니다.

  - 1: 긴급
  - 2: 알림
  - 3: 위험
  - 4: 오류
  - 5: 경고
  - 6: 공지
  - 7: 정보
  - 8: 디버그)

  SNMP Set 작업에 다른 SNMP 관리 애플리케이션을 사용할 수도 있습니다.

참고 기록하기 전에 Syslog는 지정된 Syslog 버퍼 크기보다 큰 모든 트랩 메시지 데이터를 자릅니다. Syslog 트랩 메시지 길이 제한은 255바이트입니다.

CISCO-CCM-MIB 트랩 매개 변수

- SNMP Set 작업을 사용하여 ccmPhoneFailedAlarmInterval (1.3.6.1.4.1.9.9.156.1.9.2)을 30-3600 범위의 값으로 설정합니다. 예를 들어, net-SNMP set 유틸리티를 사용하여 linux 명령줄에서 다음을 사용하여 이 OID 값을 설정합니다.

```
snmpset -c <community string> -v2c <transmitter ipaddress>
1.3.6.1.4.1.9.9.156.1.9.2 .0 i <value>
```

SNMP Set 작업에 다른 SNMP 관리 애플리케이션을 사용할 수도 있습니다.

- SNMP Set 작업을 사용하여 ccmPhoneStatusUpdateAlarmInterval (1.3.6.1.4.1.9.9.156.1.9.4)을 30-3600 범위의 값으로 설정합니다. 예를 들어, net-SNMP set 유틸리티를 사용하여 linux 명령줄에서 다음을 사용하여 이 OID 값을 설정합니다.

```
snmpset -c <community string> -v2c <transmitter ipaddress>
1.3.6.1.4.1.9.9.156.1.9.4.0 i <value>
```

SNMP Set 작업에 다른 SNMP 관리 애플리케이션을 사용할 수도 있습니다.

CISCO-UNITY-MIB 트랩 매개 변수

Cisco Unity Connection에만 해당: Cisco Unity Connection SNMP 에이전트는 트랩 알림을 활성화하지 않지만 Cisco Unity Connection 알람에서 트랩이 트리거될 수 있습니다. Cisco Unity Connection 서비스 가용성의 Cisco Unity Connection 알람 정의는 알람 > 정의 화면에서 볼 수 있습니다.

CISCO-SYSLOG-MIB를 사용하여 트랩 매개 변수를 구성할 수 있습니다.

관련 항목

CISCO-SYSLOG-MIB 트랩 매개 변수, 186 페이지

SNMP 마스터 에이전트 다시 시작

모든 SNMP 구성을 완료한 후에는 SNMP 마스터 에이전트 서비스를 다시 시작합니다.

프로시저

단계 **1** Cisco 통합 서비스 가용성에서 도구 > 제어 센터 - 네트워크 서비스를 선택합니다.

단계 **2** 서버를 선택하고 이동을 클릭합니다.

단계 **3** **SNMP** 마스터 에이전트를 선택합니다.

단계 **4** 재시작을 클릭합니다.

SNMP 트랩 설정

CLI 명령을 사용하여 구성 가능한 SNMP 트랩 설정을 설정합니다. SNMP 트랩 구성 매개 변수 및 권장 구성 팁은 CISCO-SYSLOG-MIB, CISCO-CCM-MIB 및 CISCO-UNITY-MIB용으로 제공됩니다.

SNMP 트랩 구성

이 절차를 사용하여 SNMP 트랩을 구성합니다.

시작하기 전에

시스템에서 SNMP를 구성합니다. 자세한 내용은 SNMP 구성 작업 흐름, 172 페이지를 참조하십시오.

SNMP 커뮤니티 문자열(SNMP V1/V2의 경우) 또는 SNMP 사용자(SNMP V3의 경우)에 대한 액세스 권한이 **ReadWriteNotify**, **ReadNotify**, **NotifyOnly** 설정 중 하나로 설정되어 있는지 확인합니다.

프로시저

단계 **1** CLI에 로그인하고 `utils SNMP test` CLI 명령을 실행하여 SNMP가 실행되고 있는지 확인합니다.

단계 **2** 특정 SNMP 트랩(예: CcmPhoneFailed 또는 MediaResourceListExhausted 트랩)을 생성하려면 SNMP 트랩 생성, 188 페이지을 수행합니다.

단계 **3** 트랩이 생성되지 않으면 다음 단계를 수행하십시오.

- Cisco 통합 서비스 가용성에서 알람 > 구성을 선택하고 **CM** 서비스 및 **Cisco CallManager**를 선택합니다.
- 모든 노드에 적용 확인란을 선택합니다.
- 로컬 Syslogs 아래의 알람 이벤트 수준 드롭다운 목록 상자를 정보로 설정합니다.

단계 **4** 트랩을 재현하고 해당 알람이 CiscoSyslog 파일에 기록되는지 확인합니다.

SNMP 트랩 생성

이 섹션에서는 특정 유형의 SNMP 트랩을 생성하는 프로세스를 설명합니다. 개별 트랩을 생성하기 위해서는 SNMP를 서버에서 설정하고 실행해야 합니다. SNMP 트랩을 생성하도록 시스템을 설정하는 방법에 대한 지침은 SNMP 트랩 구성, 188 페이지의 내용을 참조하십시오.

참고 개별 SNMP 트랩에 대한 처리 시간은 생성하려고 하는 트랩에 따라 달라집니다. 일부 SNMP 트랩은 생성하는 데 몇 분 정도 걸릴 수 있습니다.

표 ***33: SNMP*** 트랩 생성

SNMP 트랩	프로세스
ccmPhoneStatusUpdate	CcmPhoneStatusUpdate 트랩을 트리거하려면 다음과 같이 하십시오. **1.** CcmAlarmConfig Info MIB 테이블에서 ccmPhoneStatusUpdateAlarmInterv (1.3.6.1.4.1.9.9.156.1.9.4) = 30 이상으로 설정합니다. **2.** Cisco Unified Communications Manager 관리에 로그인합니다. **3.** 서비스 중이고 Unified Communications Manager에 등록된 전화기의 경우 전화기를 재설정합니다. 전화기를 등록 해제한 다음 재등록하면 ccmPhoneStatusUpdate 트랩을 생성합니다.
ccmPhoneFailed	CcmPhoneFailed 트랩을 트리거하려면 다음과 같이 하십시오. **1.** CcmAlarmConfigInfo MIB 테이블에서 ccmPhoneFailedAlarmInterval (1.3.6.1.4.1.9.9.156.1.9.2) = 30 이상으로 설정합니다. **2.** Cisco Unified Communications Manager 관리에서 전화기의 MAC 주소를 잘못된 값으로 변경합니다. **3.** Cisco Unified Communications Manager 관리에서 전화기를 재등록합니다. **4.** 전화기가 TFTP 서버 A를 가리키도록 설정하고 전화기를 다른 서버에 연결합니다.
ccmGatewayFailed	CcmGatewayFailed SNMP 트랩을 트리거하려면 다음과 같이 하십시오. **1.** CcmGatewayAlarmEnable (1.3.6.1.4.1.9.9.156.1.9.6)이 true로 설정되어 있는지 확인합니다. **2.** Cisco Unified Communications Manager 관리에서 게이트웨이의 MAC 주소를 잘못된 값으로 변경합니다. **3.** 게이트웨이를 재부팅합니다.

SNMP 트랩	프로세스
ccmGatewayLayer2Change	레이어 2가 모니터링되는(예: MGCP 백홀 로드) 작동하는 게이트웨이에서 ccmGatewayLayer2Change 트랩을 트리거하려면 다음을 수행합니다. 1. CcmAlarmConfig Info MIB 테이블에서 ccmGatewayAlarmEnable (1.3.6.1.4.1.9.9.156.1.9.6.0) = true로 설정합니다. 2. Cisco Unified Communications Manager 관리에서 게이트웨이의 MAC 주소를 잘못된 값으로 변경합니다. 3. 게이트웨이를 재설정합니다.
MediaResourceListExhausted	MediaResourceListExhausted 트랩을 트리거하려면 다음과 같이 하십시오. 1. Cisco Unified Communications Manager 관리에서 표준 전화회의 브리지 리소스 (CFB-2) 중 하나를 포함하는 미디어 리소스 그룹을 만듭니다. 2. 사용자가 만든 미디어 리소스 그룹을 포함하는 미디어 리소스 그룹 목록을 만듭니다. 3. 전화기 구성 창에서 미디어 리소스 그룹 목록 필드를 사용자가 만든 미디어 리소스 그룹 목록으로 설정합니다. 4. IP Voice Media Streaming 서비스를 중지합니다. 이 작업으로 인해 ConferenceBridge 리소스(CFB-2)가 작동하지 않습니다. 5. 미디어 리소스 그룹 목록을 사용하는 전화기로 전화회의 통화를합니다. "전화회의 브리지를 사용할 수 없음" 메시지가 전화기 화면에 표시됩니다.
RouteListExhausted	RouteListExhausted 트랩을 트리거하려면 다음과 같이 하십시오. 1. 하나의 게이트웨이를 포함하는 경로 그룹을 만듭니다. 2. 방금 만든 경로 그룹을 포함하는 경로 그룹 목록을 만듭니다. 3. 경로 그룹 목록을 통해 통화를 라우팅하는 고유한 경로 패턴을 생성합니다. 4. 게이트웨이를 등록 해제합니다. 5. 전화기 중 하나에서 경로 패턴과 일치하는 번호로 전화를 겁니다.

SNMP 트랩	프로세스
MaliciousCallFailed	MaliciousCallFailed 트랩을 트리거하려면 다음과 같이 하십시오. **1.** 사용 가능한 모든 "MaliciousCall" 소프트 키를 포함하는 소프트 키 템플릿을 생성합니다. **2.** 새 소프트 키 템플릿을 네트워크의 전화기에 할당하고 전화기를 재설정합니다. **3.** 전화기 사이에 전화를 겁니다. **4.** 통화 중에 "MaliciousCall" 소프트 키를 선택합니다.
ccmCallManagerFailed	**1.** `show process list` CLI 명령을 실행하여 CallManager 애플리케이션 ccm의 PID(프로세스 식별자)를 가져옵니다. 이 명령은 여러 프로세스 및 PID를 반환합니다. 알람을 생성하기 위해 중지해야 하는 PID이기 때문에, 특히 ccm에 대한 PID를 구해야 합니다. **2.** `delete process <pid>` 충돌 CLI 명령을 실행합니다. **3.** CLI 명령을 실행합니다. CallManager 실패 알람은 내부 오류가 생성될 때 생성됩니다. 이러한 내부 오류에는 CPU 부족으로 인한 내부 스레드 종료, CallManager 서버를 16초 이상 일시 중지, 타이머 문제를 포함할 수 있습니다. 이 알람을 수동으로 생성할 수는 없습니다. 참고 ccmCallManagerFailed 알람 또는 트랩을 생성하면 CallManager 서비스를 종료하고 코어 파일을 생성합니다. 혼동을 피하려면 코어 파일을 즉시 삭제하는 것이 좋습니다.
syslog 메시지를 트랩으로	특정 심각도 보다 높은 syslog 메시지를 트랩으로 받으려면 clogBasic 테이블에서 다음 두 개의 MIB 개체를 설정합니다. **1.** ClogNotificationsEnabled (1.3.6.1.4.1.9.9.41.1.1.2)를 true(1)로 설정합니다. 기본값은 false(2)입니다. 예를 들어, snmpset-c <Community String> -v 2c <transmitter ip address> 1.3.6.1.4.1.9.9.41.1.1.2.0 i 1 **2.** ClogMaxSeverity (1.3.6.1.4.1.9.9.41.1.1.3)를 트랩이 생성될 수준보다 큰 수준으로 설정합니다. 기본값은 경고(5)입니다. 알람 심각도가 구성된 심각도 수준보다 작거나 같은 모든 syslog 메시지는 트랩으로 전송됩니다. 예를 들어, snmpset-c <Community String> -v 2c <transmitter ip address> 1.3.6.1.4.1.9.9.41.1.1.3.0 i <value>

SNMP 추적 구성

Unified Communications Manager의 경우 성능 및 모니터링 서비스 그룹에서 Cisco CallManager SNMP 서비스를 선택하여 Cisco 통합 서비스 가용성의 추적 구성 창에서 Cisco CallManager SNMP 에이전트에 대한 추적을 구성할 수 있습니다. 모든 에이전트에 대한 기본 설정이 존재합니다. Cisco CDP 에이전트 및 Cisco Syslog 에이전트의 경우, *Cisco* 통합 솔루션에 대한 명령줄 인터페이스 참조 설명서에 설명된 대로 CLI를 사용하여 추적 설정을 변경합니다.

Cisco Unity Connection의 경우 연결 SNMP 에이전트 구성 요소를 선택하여Cisco Unity Connection 서비스 가용성의 추적 구성 창에서 Cisco Unity Connection SNMP 에이전트에 대한 추적을 구성할 수 있습니다.

SNMP 문제 해결

문제 해결 팁은 이 섹션을 참조하십시오. 모든 기능 및 네트워크 서비스가 실행되고 있는지 확인합니다.

문제

시스템에서 MIB를 폴링할 수 없습니다.

이 조건은 커뮤니티 문자열 또는 SNMP 사용자가 시스템에 구성되어 있지 않거나 시스템에 구성된 것과 일치하지 않음을 의미합니다. 기본적으로 시스템에는 커뮤니티 문자열이나 사용자가 구성되어 있지 않습니다.

해결 방법

SNMP 구성 창을 사용하여 커뮤니티 문자열 또는 SNMP 사용자가 시스템에 올바르게 구성되어 있는지 확인합니다.

문제

시스템에서 알림을 수신할 수 없습니다.

이 조건은 시스템에 알림 대상이 올바르게 구성되지 않았음을 의미합니다.

해결 방법

알림 대상(V1/V2c 또는 V3) 구성 창에서 알림 대상을 적절하게 구성했는지 확인하십시오.

15 장

서비스

- 기능 서비스, 193 페이지
- 네트워크 서비스, 205 페이지
- Services setup, 217 페이지

기능 서비스

서비스 가용성 GUI를 사용하여 Cisco Unified Communications Manager 및 IM and Presence Service를 활성화, 시작 및 중지할 수 있습니다. 활성화가 켜지고 서비스를 시작합니다. 사용하려는 모든 기능에 대해 기능 서비스를 수동으로 활성화해야 합니다. 서비스 활성화 권장 사항에 대해서는 서비스 활성화와 관련된 항목을 참조하십시오.

참고 IM and Presence 노드 또는 그 반대로 Unified Communications Manager 서버에 액세스하려고하면 다음과 같은 오류가 발생할 수 있습니다. "서버에 연결을 설정할 수 없습니다(원격 노드에 액세스할 수 없음)". 이 오류 메시지가 나타나는 경우 *Cisco Unified Communications Manager* 관리 설명서를 참조하십시오.

참고 IM and Presence를 사용하는 장치는 영구 채팅, 준수 및 파일 전송을 지원하기 위해 Postgres 외부 데이터베이스를 사용하도록 구성됩니다. 그러나 IM and Presence 서버와 Postgres 간의 연결은 보안되지 않으며 확인 없이 데이터가 통과합니다. TLS를 지원하지 않는 서비스나 장치의 경우, 통신 세션의 각 IP 패킷을 인증하고 암호화하여 보안 통신에 대한 표준 프로토콜인 IP Sec을 구성하여 보안 통신을 제공하는 또 다른 방법이 있습니다.

서비스 활성화 창에서 서비스를 활성화한 후에는 제어 센터 - 기능 서비스 창에서 서비스를 시작할 필요가 없습니다. 서비스가 어떤 이유로 시작되지 않는 경우에는 제어 센터 - 기능 서비스 창에서 시작해야 합니다.

시스템을 설치한 후에는 기능 서비스를 자동으로 활성화하지 않으며 구성 기능(예: 서비스 가용성 보고서 보관 기능)을 사용하기 위해 기능 서비스를 활성화해야 합니다.

Unified Communications Manager 및 CISCO Unified IM and Presence Service만 해당: Unified Communications Manager를 업그레이드하는 경우 업그레이드하기 전에 시스템에서 활성화한 서비스가 업그레이드 후 자동으로 시작됩니다.

기능 서비스를 활성화한 후에는 사용자의 제품에 대한 관리 GUI를 사용하여 서비스 매개 변수 설정을 수정할 수 있습니다.

- Cisco 통합 커뮤니케이션 매니저 관리
- Cisco Unity Connection 관리

기능 서비스 범주

Cisco 통합 서비스 가용성에서 서비스 활성화 창 및 제어 센터 - 기능 서비스 창은 기능 서비스를 다음 그룹으로 분류합니다.

- 데이터베이스 및 관리 서비스
- 성능 및 모니터링 서비스
- CM 서비스
- CTI 서비스
- CDR 서비스
- 보안 서비스
- 디렉터리 서비스
- 음성 품질 리포터 서비스

Cisco Unified IM and Presence Serviceability에서 서비스 활성화 창 및 제어 센터 - 기능 서비스 창에서는 기능 서비스를 다음 그룹으로 분류합니다.

- 데이터베이스 및 관리 서비스
- 성능 및 모니터링 서비스
- IM and Presence Service 서비스

데이터베이스 및 관리 서비스

위치 대역폭 관리자

이 서비스는 IM and Presence Service에서 지원되지 않습니다.

위치 대역폭 관리자 서비스는 하나 이상의 클러스터에 구성된 위치 및 링크 데이터로부터 네트워크 모델을 구축하고, 위치 쌍 간의 유효 경로를 결정하고, 각 통화 유형에 대한 대역폭의 가용성을 기반으로 위치 쌍 간의 통화를 허용할 것인지 여부를 결정하고, 허용된 각 통화 기간에 대한 대역폭을 공제(예약)하는 활성 서비스입니다.

Cisco AXL 웹 서비스

Cisco AXL 웹 서비스를 사용하여 데이터베이스 항목을 수정하고 AXL을 사용하는 클라이언트 기반 애플리케이션에서 저장 프로시저를 실행할 수 있습니다.

IM and Presence Service 시스템에서 이 서비스는 Unified Communications Manager와 Cisco Unity Connection를 모두 지원합니다.

Cisco UXL 웹 서비스

이 서비스는 IM and Presence Service에서 지원되지 않습니다.

Cisco IP 전화기 주소록 동기화 장치에서 TabSync 클라이언트는 Unified Communications Manager 데이터베이스에 대한 쿼리에 Cisco UXL 웹 서비스를 사용하여 Cisco IP 전화기 주소록 동기화 장치 사용자가 해당 사용자와 관련된 최종 사용자 데이터에만 액세스할 수 있도록합니다. Cisco UXL 웹 서비스는 다음과 같은 기능을 수행합니다.

- 최종 사용자가 Cisco IP 전화기 주소록 동기화 장치에 로그인할 때 최종 사용자 사용자 이름 및 암호를 확인하여 인증 확인을 수행합니다.
- Cisco IP 전화기 주소록 동기화 장치에 현재 로그인되어 있는 사용자만 연락처 나열, 검색, 업데이트, 제거 및 추가와 같은 기능을 수행할 수 있도록 하여 사용자 인증 확인을 수행합니다.

Cisco Bulk Provisioning Service

이 서비스는 Cisco Unity Connection을 지원하지 않습니다.

구성에서 클러스터를 지원하는 경우(Unified Communications Manager만 해당), 첫 번째 서버에서만 Cisco Bulk Provisioning 서비스를 활성화할 수 있습니다. Unified Communications Manager 벌크 관리 도구를 사용하여 전화기 및 사용자를 관리하는 경우 이 서비스를 활성화해야 합니다.

Cisco TAPS 서비스

이 서비스는 Cisco Unity Connection 또는 IM and Presence Service를 지원하지 않습니다.

Cisco TAPS(자동 등록된 전화기 지원을 위한 도구) 서비스는 사용자가 IVR(대화형 음성 응답) 프롬프트에 응답한 후 자동 등록된 전화기에서 사용자 정의된 구성을 업로드하는 데 사용할 수 있는 Cisco Unified Communications Manager 자동 등록 전화기 도구를 지원합니다.

구성에서 클러스터를 지원하는 경우(Unified Communications Manager만 해당) 첫 번째 서버에서 이 서비스를 활성화합니다. 도구에 대한 더미 MAC 주소를 생성하려면 동일한 서버에서 Cisco Bulk Provisioning 서비스가 활성화되어 있는지 확인하십시오.

팁 Cisco Unified Communications Manager 자동 등록 전화기 도구는 Cisco CRS(Customer Response Solutions)를 이용합니다. 도구가 설계된 대로 작동하려면 CRS 설명서에 설명된 바와 같이 CRS 서버가 구성되고 실행 중인지 확인하십시오.

플랫폼 관리 웹 서비스

플랫폼 관리 웹 서비스는 PAWS-M 서버가 시스템을 업그레이드할 수 있도록 하는 Unified Communications Manager, IM and Presence Service및 Cisco Unity Connection 시스템에서 활성화할 수 있는 SOAP(Simple Object Access Protocol) API입니다.

중요 PAWS-M 서버에서 플랫폼 관리 웹 서비스를 활성화하지 마십시오.

Performance and monitoring services

Cisco 서비스 가용성 리포터

Cisco 서비스 가용성 리포터 서비스는 일별 보고서를 생성합니다. 자세한 내용은 서비스 가용성 보고서 보관에 관련된 항목을 참조하십시오.

구성에서 클러스터를 지원하는 경우(Unified Communications Manager만 해당) 이 서비스는 클러스터의 모든 Unified Communications Manager 서버에 설치됩니다. 리포터는 로그 정보를 기준으로 하루에 한 번 보고서를 생성합니다. 도구 메뉴에서 리포터가 Cisco 통합 서비스 가용성에서 생성하는 보고서에 액세스할 수 있습니다. 각 요약 보고서는 특정 보고서에 대한 통계를 표시하는 다양한 차트로 구성됩니다. 서비스를 활성화한 후 보고서 생성에는 24시간이 걸릴 수 있습니다.

관련 항목

서비스 가용성 보고서 아카이브, 285 페이지

Cisco CallManager SNMP Service

이 서비스는 IM and Presence Service 및 Cisco Unity Connection을 지원하지 않습니다.

CISCO-CCM을 구현하는 이 서비스는 Unified Communications Manager에 사용할 수 있는 프로비저닝 및 통계 정보에 대한 SNMP 액세스를 제공합니다.

구성에서 클러스터를 지원하는 경우(Unified Communications Manager만 해당) 클러스터의 모든 서버에서 이 서비스를 활성화합니다.

CM 서비스

이 섹션에서는 CM 서비스에 대해 설명하며 IM and Presence Service 및 Cisco Unity Connection에는 적용되지 않습니다.

Cisco CallManager

Cisco CallManager 서비스는 소프트웨어 전용 통화 처리뿐만 아니라 Unified Communications Manager에 대한 신호 처리 및 통화 제어 기능을 제공합니다.

팁 Unified Communications Manager 클러스터에만 해당: 이 서비스를 활성화하기 전에 Unified Communications Manager 서버가 Cisco Unified Communications Manager 관리의 Cisco Unified Communications Manager 창에 표시되는지 확인합니다. 서버가 표시되지 않으면 이 서비스를 활성화하기 전에 Unified Communications Manager 서버를 추가합니다. 서버를 찾고 추가하는 방법에 대한 자세한 내용은 *Cisco Unified Communications Manager* 관리 설명서를 참조하십시오.

Unified Communications Manager 클러스터만 해당: 서비스 활성화 시 Cisco CallManager 또는 CTIManager 서비스를 비활성화하는 경우 서비스를 비활성화한 Unified Communications Manager 서버가 더 이상 데이터베이스에 존재하지 않습니다. 즉, 그래픽 사용자 인터페이스(GUI)에 표시되지 않으므로 Cisco Unified Communications Manager 관리의 구성 작업을 위해 Unified Communications Manager 서버를 선택할 수 없다는 것을 의미합니다. 그런 다음 동일한 Unified Communications Manager 서버에서 서비스를 다시 활성화하면 데이터베이스에서 Unified Communications Manager에 대한 항목을 다시 만들고 서버 이름 또는 IP 주소에 "CM_" 접두사를 추가합니다. 예를 들어, IP 주소가 172.19.140.180인 서버에서 CallManager 또는 CTIManager 서비스를 다시 활성화하는 경우 CM_172.19.140.180이 Cisco Unified Communications Manager 관리에 표시됩니다. 이제 Cisco Unified Communications Manager 관리에서는 새 "CM_" 접두사가 있는 서버를 선택할 수 있습니다.

다음 서비스는 Cisco CallManager 서비스 활성화에 의존합니다.

- CM 서비스
- CDR 서비스

Cisco TFTP

Cisco TFTP(Trivial File Transfer Protocol)는 FTP의 간단한 버전인 TFTP(Trivial File Transfer Protocol)와 일치하는 파일을 작성하고 서비스합니다. Cisco TFTP는 포함된 구성 요소 실행 파일, 벨소리 파일 및 장치 구성 파일을 제공합니다.

Unified Communications Manager만 해당: 구성 파일에는 장치(전화기 및 게이트웨이)에서 연결하는 Unified Communications Manager 목록이 포함되어 있습니다. 장치가 부팅되면 구성 요소는 DHCP(Dynamic Host Configuration Protocol) 서버에 네트워크 구성 정보를 쿼리합니다. DHCP 서버는 장치의 IP 주소, 서브넷 마스크, 기본 게이트웨이, DNS(Domain Name System) 서버 주소 및 TFTP 서버 이름 또는 주소를 사용하여 응답합니다. 장치가 TFTP 서버에서 구성 파일을 요청합니다. 구성 파일에는 Unified Communications Manager와 장치가 이러한 Unified Communications Manager에 연결하는 TCP 포트 목록이 포함되어 있습니다. 구성 파일에는 Unified Communications Manager와 장치가 이러한 Unified Communications Manager에 연결하는 TCP 포트 목록이 포함되어 있습니다.

Cisco Messaging Interface

Cisco Messaging Interface를 사용하면 Cisco Unified Communications Manager와 함께 SMDI(Simplified Message Desk Interface)를 준수하는 외부 음성 메시징 시스템을 연결할 수 있습니다. SMDI는 전화기 시스템이 수신 통화를 지능적으로 처리하는 데 필요한 정보를 사용하여 음성 메시징 시스템을 제공하는 방법을 정의합니다.

Cisco Unified Mobile Voice Access Service

Cisco Unified Voice Access Service는 Cisco Unified Mobility 내에서 모바일 음성 액세스 기능을 시작합니다. IVR(통합 음성 응답) 시스템인 모바일 음성 액세스를 사용하면 Cisco Unified Mobility사용자가 다음 작업을 수행할 수 있습니다.

- 데스크폰에서 전화를 거는 것처럼 휴대폰에서 전화를 겁니다.
- Cisco Unified Mobility를 켭니다.
- Cisco Unified Mobility를 끕니다.

Cisco IP Voice Media Streaming App

Cisco IP Voice Media Streaming Application 서비스는 MTP(미디어 종료 지점), 전화회의, 대기 중 음악(MOH) 및 알림 장치와 함께 사용하기 위해 Unified Communications Manager를 위한 음성 미디어 스트리밍 기능을 제공합니다. Cisco IP Voice Media Streaming Application은 RTP(실시간 프로토콜) 스트리밍을 처리하는 IP 음성 미디어 스트리밍 드라이버로 Unified Communications Manager에서 메시지를 릴레이합니다.

Cisco IP Voice Media Streaming Application 서비스는 전화회의, MOH, 알림 장치 또는 MTP와 같은 IP 음성 미디어 스트리밍 애플리케이션 구성 요소를 포함하는 통화 레그에 대한 CMR(통화 관리 레코드) 파일을 생성하지 않습니다.

Cisco CTIManager

Cisco CTI 매니저는 애플리케이션과 상호 작용하는 CTI 구성 요소를 포함합니다. 이 서비스를 사용하면 애플리케이션에서 전화 및 가상 장치를 모니터링하거나 제어하여 통화 제어 기능을 수행할 수 있습니다.

Unified Communications Manager 클러스터만 해당: CTI 매니저를 사용하면 애플리케이션에서 클러스터에 있는 모든 Unified Communications Manager의 리소스 및 기능에 액세스할 수 있으며 페일오버 기능이 향상됩니다. 하나 이상의 CTI 매니저가 클러스터에서 활성화될 수 있지만 개별 서버에는 하나의 CTI 매니저만 있을 수 있습니다. 애플리케이션(JTAPI/TAPI)은 여러 CTI 매니저에게 동시에 연결될 수 있습니다. 그러나 애플리케이션은 한 번에 하나의 연결만을 사용하여 미디어 종료 장치를 열 수 있습니다.

Cisco Extension Mobility

Cisco Extension Mobility 기능을 지원하는 이 서비스에서는 기능에 대한 로그인 및 자동 로그아웃 기능을 수행합니다.

Cisco Dialed Number Analyzer

Cisco Dialed Number Analyzer 서비스는 Unified Communications Manager Dialed Number Analyzer를 지원합니다. 이 애플리케이션을 활성화하면 많은 리소스가 사용되므로, 최소 통화 처리 중단이 발생할 수 있을 때까지 사용량이 많지 않은 시간에만 이 서비스를 활성화합니다.

Unified Communications Manager 클러스터만 해당: 클러스터의 모든 서버에서 서비스를 활성화하는 것은 권장하지 않습니다. 통화 처리 활동이 가장 적은 클러스터의 서버 중 하나에서만 이 서비스를 활성화하는 것이 좋습니다.

Cisco Dialed Number Analyzer 서버

Cisco Dialed Number Analyzer 서비스와 함께 Cisco Dialed Number Analyzer 서버 서비스는 Cisco Unified Communications Manager Dialed Number Analyzer를 지원합니다. 이 서비스는 Cisco Dialed Number Analyzer 서비스 전용인 노드에서만 활성화해야 합니다.

Unified Communications Manager 클러스터만 해당: 클러스터의 모든 서버에서 서비스를 활성화하는 것은 권장하지 않습니다. 통화 처리 활동이 가장 적은 클러스터의 서버 중 하나에서만 이 서비스를 활성화하는 것이 좋습니다.

Cisco DHCP 모니터 서비스

Cisco DHCP 모니터 서비스는 데이터베이스 테이블에서 IP 전화기에 대한 IP 주소 변경 사항을 모니터링합니다. 변경 사항이 감지되면 /etc./dhcpd.conf 파일을 수정하고 DHCPD 데몬을 다시 시작합니다.

Cisco 클러스터 간 조회 서비스

ILS (클러스터 간 조회 서비스)는 클러스터 전체에서 실행됩니다. ILS를 사용하면 원격 Unified Communications Manager 클러스터로 구성된 네트워크를 만들 수 있습니다. ILS 클러스터 검색 기능을 사용하면 관리자가 각 클러스터 간 연결을 수동으로 구성할 필요 없이 Cisco Unified Communications Manager에서 원격 클러스터에 연결할 수 있습니다. ILS 전역 다이얼 플랜 복제 기능을 사용하면 ILS 네트워크의 클러스터에서 ILS 네트워크의 다른 클러스터와 전역 다이얼 플랜 데이터를 교환하는 기능을 사용할 수 있습니다.

고급 기능 > **ILS** 구성을 선택하여 Cisco Unified Communications Manager 관리에서 액세스할 수 있는 ILS 구성 창에서 ILS를 활성화할 수 있습니다.

Cisco UserSync 서비스

Cisco UserSyn 서비스는 Unified Communications Manager 최종 사용자 테이블의 데이터를 LDAP 데이터베이스에 동기화합니다.

Cisco UserLookup 웹 서비스

Cisco UserLookup 웹 서비스는 외부 번호 발신에 대한 상업적 비용을 방지하기 위해 착신자의 대체 내부 번호로 상업적 통화(외부 게이트웨이를 통해 통화)를 라우팅합니다.

Unified Communications Manager 네트워크 내의 발신자가 외부 번호에서 전화를 거는 경우에는 Unified Communications Manager가 LDAP 데이터베이스에서 착신자에 대한 내부 번호가 있는지 확인합니다. 내부 번호가 있으면 통화가 해당 내부 번호로 라우팅됩니다. LDAP 데이터베이스에서 내부 번호를 찾을 수 없는 경우 통화는 원래(외부) 번호로 라우팅됩니다.

Cisco 헤드셋 서비스

Cisco 헤드셋 서비스를 사용하면 호환되는 Cisco IP 전화기, Cisco Jabber 또는 기타 Cisco 장치를 사용하는 경우 Cisco 헤드셋의 인벤토리, 구성 업데이트 및 진단 데이터를 관리할 수 있습니다.

참고 Cisco CallManager 서비스가 이미 실행 중인 경우 모든 Unified Communications Manager 노드에서 Cisco 헤드셋 서비스를 활성화해야 합니다. Cisco Unified CM 관리 인터페이스를 사용하여 헤드셋을 관리하려는 Unified Communications Manager 노드에서 Cisco 헤드셋 서비스를 활성화해야 합니다. Cisco 헤드셋 서비스를 활성화하면 Cisco CallManager 서비스가 자동으로 활성화됩니다. 필요하지 않은 경우 Cisco CallManager 서비스를 비활성화합니다.

IM and Presence Service

IM and Presence Service는 IM and Presence Service에만 적용됩니다.

Cisco SIP Proxy

Cisco SIP Proxy 서비스는 SIP 등록기관 및 프록시 기능을 제공합니다. 여기에는 요청 라우팅, 요청자 식별 및 전송 상호 연결 등이 포함됩니다.

Cisco Presence 엔진

Cisco Presence 엔진은 표준 기반 SIP 및 SIMPLE 인터페이스를 사용하여 사용자 기능 및 속성을 수집, 집계 및 분배합니다. 이는 사용자의 가용성 상태 및 통신 기능에 대한 정보를 수집합니다.

Cisco XCP 텍스트 전화회의 관리자

Cisco XCP 텍스트 전화회의 관리자는 채팅 기능을 지원합니다. 채팅 기능을 사용하면 사용자가 온라인 채팅방에서 서로 대화를 나눌 수 있습니다. 이 기능은 삭제될 때까지 Cisco 지원 외부 데이터베이스에 유지되는 임시 및 영구 채팅방을 사용하여 채팅 기능을 지원합니다.

Cisco XCP Web 연결 관리자

Cisco XCP 웹 연결 관리자 서비스를 사용하면 브라우저 기반 클라이언트에서 IM and Presence Service에 연결할 수 있습니다.

Cisco XCP 연결 관리자

Cisco Unified Presence XCP 연결 관리자를 사용하여 XMPP 클라이언트를 Cisco Unified Presence 서버에 연결할 수 있습니다.

Cisco XCP SIP 페더레이션 연결 관리자

Cisco XCP SIP 페더레이션 연결 관리자는 SIP 프로토콜을 통해 Microsoft OCS와의 도메인간 페더레이션을 지원합니다. 배포에 IM and Presence Service 릴리스 9.0 클러스터와 Cisco Unified Presence 릴리스 8.6 클러스터 간의 클러스터 간 연결이 포함되어 있는 경우에는이 서비스도 설정해야 합니다.

Cisco XCP XMPP 페더레이션 연결 관리자

Cisco XCP XMPP 페더레이션 연결 관리자는 XMPP 프로토콜을 통해 IBM Lotus Sametime, Cisco Webex Meeting Center 및 GoogleTalk와 같은 타사 엔터프라이즈의 도메인 간 페더레이션을 지원하고 XMPP 프로토콜을 통해 다른 IM and Presence Service 엔터프라이즈와의 도메인 간 페더레이션을 지원합니다.

Cisco XCP 메시지 아카이버

Cisco XCP Message Archiver 서비스는 IM 준수 기능을 지원합니다. IM 준수 기능은 지점 간 메시지 및 채팅 기능의 임시 및 영구 채팅방에 있는 메시지를 포함하여 IM and Presence Service 서버에서 주고 받는 모든 메시지를 기록합니다. 메시지는 외부 Cisco 지원 데이터베이스에 기록됩니다.

Cisco XCP 디렉터리 서비스

Cisco XCP 디렉터리 서비스는 LDAP 디렉터리에서 연락처를 검색 및 추가하도록 허용하도록 XMPP 클라이언트와 LDAP 디렉터리의 통합을 지원합니다.

Cisco XCP 인증 서비스

Cisco XCP 인증 서비스는 IM and Presence Service에 연결된 XMPP 클라이언트의 모든 인증 요청을 처리합니다.

CTI 서비스

이 섹션에서는 CTI 서비스에 대해 설명하며 Cisco Unity Connection 또는 IM and Presence Service에는 적용되지 않습니다.

Cisco IP Manager Assistant

이 서비스는 Cisco Unified Communications Manager Assistant를 지원합니다. 서비스를 활성화한 후 Cisco Unified Communications Manager Assistant를 사용하면 관리자와 보조자가 더 효율적으로 협력할 수 있습니다. Cisco Unified Communications Manager Assistant는 프록시 회선 지원 및 공유 회선 지원의 두 가지 작동 모드를 지원합니다.

이 기능은 통화-라우팅 서비스, 관리자를 위한 향상된 전화기 기능 및 주로 보조자가 사용하는 데스크톱 인터페이스로 구성됩니다.

통화 라우팅 서비스는 관리자에게 걸려 온 전화를 차단하고 사전 구성된 통화 필터를 기준으로 선택되는 보조자, 관리자 또는 기타 대상으로 전송합니다. 관리자는 통화 라우팅을 동적으로 변경할 수 있습니다. 예를 들어 관리자는 전화기의 소프트키를 눌러 서비스에 모든 통화를 보조자에게 전송하라고 지시할 수 있고 이러한 통화에 대한 상태를 수신할 수 있습니다.

Unified Communications Manager 사용자는 관리자와 보조자로 구성됩니다. 라우팅 서비스에서는 관리자 통화를 차단하여 적절히 전송합니다. 보조 사용자는 관리자를 대신하여 통화를 처리합니다.

Cisco WebDialer 웹 서비스

Cisco Unified Communications Manager 시스템용 Cisco WebDialer 웹 서비스

Cisco Web Dialer는 클릭 투 다이얼 기능을 제공합니다. 이를 통해 Unified Communications Manager 클러스터 내부의 사용자가 웹 페이지 또는 데스크톱 애플리케이션을 사용하여 클러스터 내부 또는 외부의 다른 사용자에게 전화를 걸 수 있습니다. Cisco Web Dialer는 사용자가 클러스터 내에서 서로에게 전화를 걸 수 있는 웹 페이지를 제공합니다. Cisco Web Dialer는 WebDialer 서블릿 및 리디렉터 서블릿 두 가지 구성 요소로 이루어집니다.

리디렉터 서블릿은 타사 애플리케이션에서 Cisco Web Dialer를 사용할 수 있는 기능을 제공합니다. 리디렉터 서블릿은 Cisco Web Dialer 사용자에 대한 적절한 Unified Communications Manager 클러스터를 찾아 해당 클러스터의 Cisco Web Dialer에 요청을 재전송합니다. 리디렉터 기능은 SOAP(Simple Object Access Protocol) 기반 WebDialer 애플리케이션에는 사용할 수 없으므로 HTTP/HTML 기반 WebDialer 클라이언트 애플리케이션에만 적용됩니다.

셀프 프로비저닝 IVR

셀프 프로비저닝 IVR 서비스가 도입됨에 따라 Unified Communications Manager의 자동 등록된 IP 전화기는 사용자에게 간단하고 신속하게 할당됩니다. IVR 서비스를 사용하는 사용자의 내선 번호에서 셀프 프로비저닝 페이지에 구성된 CTI RP DN으로 전화를 걸면 전화기가 셀프 프로비저닝 IVR 애플리케이션에 연결되고 셀프 서비스 자격 증명을 입력하라는 메시지가 표시됩니다. 사용자가 제공하는 셀프 서비스 자격 증명에 대한 확인에 따라 IVR 서비스에서는 자동 등록된 IP 전화기를 사용자에 할당합니다.

서비스가 비활성화되어 있는 경우에도 셀프 프로비저닝을 구성할 수 있지만 관리자가 IVR 서비스를 사용하여 사용자에 IP 전화기를 할당할 수는 없습니다. 기본적으로 이 서비스는 비활성화되어 있습니다.

셀프 프로비저닝 IVR 서비스를 활성화하려면 Cisco CTI Manager 서비스를 활성화해야 합니다.

셀프 프로비저닝을 구성하는 방법에 대한 자세한 내용은 *Cisco Unified Communications Manager* 관리 설명서를 참조하십시오.

CDR 서비스

이 섹션에서는 CDR 서비스에 대해 설명하며 IM and Presence Service 및 Cisco Unity Connection에는 적용되지 않습니다.

CAR 웹 서비스

Cisco CAR Web Service에서는 CDR 데이터를 사용하여 CSV 또는 PDF 보고서 중 하나를 생성하는 웹 기반 보고 애플리케이션에서 CAR에 대한 사용자 인터페이스를 로드합니다.

Cisco SOAP - CDRonDemand Service

Cisco SOAP CDROnDemand Service(SOAP/HTTPS 기반 서비스)는 CDR 저장소 서버에서 실행됩니다. 이는 사용자 지정 시간 간격(최대 1시간)을 기반으로 하여 CDR 파일 이름 목록에 대한 SOAP 요청을 수신하고 요청에 지정된 지속 시간에 맞는 파일 이름 목록을 반환합니다. 이 서비스는 요청에 지정된 파일 이름 및 전환 방법(SFTP/FTP, 서버 이름, 로그인 정보, 디렉터리)을 사용하여 특정 CDR/CMR 파일 전달에 대한 요청을 수신합니다.

HTTPS/SOAP 인터페이스를 통해 CDR 데이터에 액세스하는 타사 청구 애플리케이션을 사용하는 경우 이 서비스를 활성화합니다.

Unified Communications Manager 릴리스 12.x 이후 버전의 경우 CDR onDemand 서비스는 기본적으로 활성화되어 있지 않습니다. CDR onDemand 서비스를 활성화하려면 서비스를 수동으로 활성화해야 합니다. 다음 명령을 루트 수준에서 실행하여 CDR onDemand 서비스를 활성화합니다.
`/usr/local/cm/bin/soapservicecontrol2.shCDRonDemandServiceCDRonDemanddeploy8443`.

보안 서비스

이 섹션에서는 보안 서비스에 대해 설명하며 IM and Presence Service 및 Cisco Unity Connection에는 적용되지 않습니다.

Cisco CTL Provider

Unified Communications Manager만 해당: 로컬 시스템 계정 권한으로 실행되고, 클라이언트 측 플러그인인 Cisco CTL Provider Utility로 작동하는 Cisco CTL(인증서 신뢰 목록) 공급자 서비스는 비보안 모드에서 혼합 모드로 클러스터의 보안 모드를 변경합니다. 플러그인을 설치할 때 Cisco CTL Provider 서비스에서 CTL 파일에 대한 모든 Unified Communications Manager 및 Cisco TFTP 서버 목록을 검색합니다. 여기에는 클러스터의 보안 토큰과 서버 목록이 포함되어 있습니다.

Cisco CTL 클라이언트 또는 CLI 명령 집합 **utils ctl**을 설치 및 구성한 다음 클러스터 수준 보안 모드에 대해 이 서비스를 활성화하여 비보안에서 보안으로 변경할 수 있습니다.

서비스를 활성화한 후 Cisco CTL Provider 서비스는 기본 CTL 포트(2444)로 복귀됩니다. 포트를 변경하려는 경우 *Cisco Unified Communications Manager* 보안 설명서를 참조하십시오.

Cisco Certificate Authority Proxy Function(CAPF)

CAPF 서비스는 Cisco Certificate Authority Proxy Function(CAPF) 애플리케이션과 함께 작동하여 구성에 따라 다음 작업을 수행할 수 있습니다.

- 지원되는 Cisco Unified IP 전화기 모델에 로컬 중요 인증서를 발급합니다.
- 전화기의 기존 인증서를 업그레이드합니다.
- 문제 해결을 위해 전화기 인증서를 검색합니다.
- 전화기에 있는 로컬 중요 인증서를 삭제합니다.

참고 Unified Communications Manager만 해당: RTMT(실시간 모니터링 도구)에서 실시간 정보를 볼 때 CAPF 서비스는 첫 번째 서버에 대해서만 표시됩니다.

디렉터리 서비스

이 섹션에서는 디렉터리 서비스에 대해 설명하며 IM and Presence Service 및 Cisco Unity Connection에는 적용되지 않습니다.

Cisco DirSync

Unified Communications Manager: Cisco DirSync 서비스는 Unified Communications Manager 데이터베이스에서 모든 사용자 정보를 저장하도록합니다. Unified Communications Manager와 함께 통합된 회사 디렉터리(예: Microsoft Active Directory 또는 Netscape/iPlanet 디렉터리)를 사용하는 경우 Cisco DirSync 서비스는 사용자 데이터를 Unified Communications Manager 데이터베이스로 마이그레이션합니다. Cisco DirSync 서비스는 회사 디렉터리의 암호를 동기화하지 않습니다.

참고 중복된 이메일 ID를 가진 사용자는 동기화되지 않으며 관리자는 동기화되지 않은 사용자의 목록에 대한 알림을 받지 않습니다. 이러한 ID는 Unified RTMT의 DirSync 오류 로그에 표시됩니다.

Cisco Unity Connection: Cisco Unity Connection이 LDAP 디렉터리와 통합되면 Cisco DirSync 서비스는 Cisco Unity Connection 서버의 Unified Communications Manager 데이터베이스에 있는 사용자 데이터(이름, 성, 별칭, 전화 번호 등)의 작은 하위 집합을 LDAP 디렉터리의 해당 데이터와 동기화합니다. 다른 서비스(CuCmDbEventListener)는 Cisco Unity Connection 사용자 데이터베이스의 데이터를 Unified Communications Manager 데이터베이스의 데이터와 동기화합니다. Cisco Unity Connection 클러스터가 구성된 경우 Cisco DirSync 서비스는 게시자 서버에서만 실행됩니다.

위치 기반 추적 서비스

이 섹션에서는 위치 기반 추적 서비스에 대해 설명합니다.

Cisco Wireless Controller 동기화 서비스

이 서비스는 네트워크의 무선 액세스 포인트 및 연결된 모바일 장치의 상태를 제공하는 위치 인식 기능을 지원합니다.

Unified Communications Manager와 Cisco 무선 액세스 포인트 컨트롤러를 동기화 하려면 이 서비스가 실행 중이어야합니다. 서비스가 실행 중이고 동기화가 구성되어 있으면 Unified Communications Manager가 데이터베이스를 Cisco 무선 액세스 포인트 컨트롤러와 동기화하고 컨트롤러가 관리하는 무선 액세스 포인트에 대한 상태 정보를 저장합니다. 동기화가 정기적으로 발생하여 정보가 최신 상태로 유지되도록 예약할 수 있습니다.

참고 새 Cisco 무선 액세스 포인트 컨트롤러를 추가할 때 이 서비스가 실행되고 있는지 확인하십시오.

음성 품질 리포터 서비스

이 섹션에서는 Voice Quality Reporter 서비스에 대해 설명하며 IM and Presence Service 및 Cisco Unity Connection에는 적용되지 않습니다.

Cisco Extended Functions

Cisco Extended Functions 서비스는 QRT(품질 보고서 도구)를 포함하여 Unified Communications Manager 음성 품질 기능을 지원합니다. 개별 기능에 대한 자세한 내용은 *Cisco Unified Communications Manager* 시스템 구성 설명서 및 *Cisco Unified Communications Manager*용 *Cisco* 유니파이드 *IP* 전화기 관리 설명서를 참조하십시오.

네트워크 서비스

자동으로 설치되는 네트워크 서비스에는 시스템에서 작동해야 하는 서비스(예: 데이터베이스 및 플랫폼 서비스)가 포함됩니다. 이러한 서비스는 기본 기능에 필요하므로 서비스 활성화 창에서 활성화할 수 없습니다. 예를 들어, 문제 해결을 위해 필요한 경우 제어 센터 - 네트워크 서비스 창에서 네트워크 서비스를 중지하고 시작(또는 다시 시작)해야 할 수 있습니다.

애플리케이션을 설치한 후에는 제어 센터 - 네트워크 서비스 창에 표시된 대로 네트워크 서비스가 자동으로 시작됩니다. 서비스 가용성 GUI는 서비스를 논리적 그룹으로 분류합니다.

성능 및 모니터링 서비스

Cisco CallManager Serviceability RTMT

Cisco CallManager Serviceability RTMT 서블릿은 추적을 수집 및 확인하고, 성능 모니터링 개체를 보고, 알림에 대한 작업을 수행하고, 시스템 성능 및 성능 카운터 등을 모니터링할 수 있는 RTMT(IM and Presence 실시간 모니터링 도구)를 지원합니다.

Cisco RTMT 리포터 서블릿

Cisco RTMT 리포터 서블릿을 사용하여 RTMT에 대한 보고서를 게시할 수 있습니다.

Cisco Log Partition Monitoring Tool

Cisco Log Partition Monitoring Tool 서비스는 구성된 임계값과 폴링 간격을 사용하여 노드(또는 클러스터의 모든 노드)에 있는 로그 파티션의 디스크 사용량을 모니터링하는 로그 파티션 모니터링 기능을 지원합니다.

Cisco Tomcat 통계 서블릿

Cisco Tomcat 통계 서블릿을 사용하면 RTMT 또는 CLI를 사용하여 Tomcat perfmon 카운터를 모니터링할 수 있습니다. 이 서비스에서 CPU 시간과 같은 리소스를 너무 많이 사용하고 있다고 생각하지 않으면 이 서비스를 중지하지 마십시오.

Cisco RIS Data Collector

RIS(실시간 정보 서버)는 장치 등록 상태, 성능 카운터 통계, 발생하는 중요한 알람 등과 같은 실시간 정보를 유지 관리합니다. Cisco RIS Data Collector 서비스는 클러스터의 모든 RIS 노드에 저장되는 정보를 검색하기위해 IM and Presence 실시간 모니터링 도구(RTMT), SOAP 애플리케이션 등과 같은 애플리케이션용 인터페이스를 제공합니다.

Cisco AMC Service

RTMT(실시간 모니터링 도구)에 사용되는 서비스인 Alert Manager 및 수집기 서비스는 RTMT가 서버(또는 클러스터의 모든 서버)에 있는 실시간 정보를 검색할 수 있습니다.

Cisco Audit Event Service

Cisco Audit Event Service는 사용자 또는 사용자 작업의 결과로 Unified Communications Manager 또는 IM and Presence 시스템에 대한 모든 관리 구성 변경 사항을 모니터링하고 로그에 기록합니다. Cisco Audit Event Service는 로그인, 로그아웃 및 IM 채팅방 입력과 같은 최종 사용자 이벤트도 모니터링하고 로그에 기록합니다.

백업 및 복원 서비스

Cisco DRF Master

IM and Presence Service에는 적용되지 않습니다.

CiscoDRF Master 에이전트 서비스는 재해 복구 시스템 GUI 또는 CLI와 함께 작동하여 백업 일정을 관리하고, 복원을 수행하고, 종속성을 확인하고, 작업 상태를 확인하고, 필요한 경우 작업을 취소하는 DRF Master 에이전트를 지원합니다. Cisco DRF Master 에이전트는 백업 및 복원 프로세스를 위한 저장소 미디어를 제공합니다.

Cisco DRF Local

Cisco DRF Local 서비스는 DRF Master 에이전트 역할을 하는 Cisco DRF Local 에이전트를 지원합니다. 구성 요소는 재해 복구 프레임워크를 사용하기 위해 Cisco DRF Local 에이전트에 등록합니다. Cisco DRF Local 에이전트는 Cisco DRF Master 에이전트에서 수신하는 명령을 실행합니다. Cisco DRF Local 에이전트가 상태, 로그 및 명령 결과를 Cisco DRF Master 에이전트에게 전송합니다.

시스템 서비스

Cisco CallManager Serviceability

Cisco CallManager Serviceability 서비스는 문제를 해결하고 서비스를 관리하는 데 사용하는 웹 애플리케이션/인터페이스인 Cisco 통합 서비스 가용성 및 IM and Presence Service 서비스 가용성 GUI를 지원합니다. 이 서비스는 자동으로 설치되며 서비스 가용성 GUI에 액세스할 수 있습니다. 서버에서 이 서비스를 중지하면 해당 서버를 탐색할 때 서비스 가용성 GUI에 액세스할 수 없습니다.

Cisco CDP

CDP(Cisco Discovery Protocol)는 음성 애플리케이션을 다른 네트워크 관리 애플리케이션에 광고하므로, 네트워크 관리 애플리케이션(예: SNMP 또는 Cisco Unified Operations Manager)이 음성 애플리케이션에 대한 네트워크 관리 작업을 수행할 수 있습니다.

Cisco Trace Collection 서블릿

Cisco Trace Collection 서블릿은 Cisco Trace collection 서비스와 함께 추적 수집을 지원하며, 사용자는 RTMT를 사용하여 추적을 볼 수 있습니다. 서버에서 이 서비스를 중지하면 해당 서버에서 추적을 수집하거나 볼 수 없습니다.

SysLog 뷰어 및 추적 및 로그 센트럴이 RTMT에서 작동하려면 Cisco 추적 수집 서블릿 및 Cisco Trace Collection 서비스가 서버에서 실행되어야합니다.

Cisco Trace Collection Service

Cisco Trace Collection 서블릿과 함께 Cisco Trace Collection 서비스는 추적 수집을 지원하며 사용자가 RTMT 클라이언트를 사용하여 추적을 볼 수 있도록 허용합니다. 서버에서 이 서비스를 중지하면 해당 서버에서 추적을 수집하거나 볼 수 없습니다.

SysLog 뷰어 및 추적 및 로그 센트럴이 RTMT에서 작동하려면 Cisco 추적 수집 서블릿 및 Cisco Trace Collection 서비스가 서버에서 실행되어야합니다.

팁 필요한 경우, Cisco Trace Collection 서블릿을 다시 시작하기 전에 초기화 시간을 줄이려면 Cisco Trace Collection 서비스를 다시 시작하는 것이 좋습니다.

플랫폼 서비스

Cisco DB

Cisco DB 서비스는 Unified Communications Manager에서 Progres 데이터베이스 엔진을 지원합니다. IM and Presence Service에서 CISCO DB 서비스는 IDS 데이터베이스 엔진을 지원합니다.

Cisco DB Replicator

Unified Communications Manager 및 IM and Presence만 해당: Cisco DB Replicator 서비스는 클러스터의 첫 번째 서버와 후속 서버 간의 데이터베이스 구성 및 데이터 동기화를 보장합니다.

Cisco Tomcat

Cisco Tomcat 서비스는 웹 서버를 지원합니다.

SNMP 마스터 에이전트

에이전트 프로토콜 엔진 역할을 하는 이 서비스는 SNMP 요청과 관련된 인증, 권한 부여, 액세스 컨트롤 및 프라이버시 기능을 제공합니다.

팁 서비스 가용성 GUI에서 SNMP 구성을 완료한 후에는 제어 센터 - 네트워크 기능 창에서 SNMP 마스터 에이전트 서비스를 다시 시작해야 합니다.

MIB2 에이전트

이 서비스는 시스템, 인터페이스 및 IP 같은 변수를 읽고 쓰는 RFC 1213에 정의되어 있는 변수에 대해 SNMP 액세스를 제공합니다.

호스트 리소스 에이전트

이 서비스는 저장소 리소스, 프로세스 테이블, 장치 정보 및 설치된 소프트웨어 베이스와 같은 호스트 정보에 대한 SNMP 액세스를 제공합니다. 이 서비스는 HOST-RESOURCES-MIB를 구현합니다.

기본 에이전트 어댑터

MIB(공급업체 관리 정보 기반)를 지원하는 이 서비스를 사용하면 SNMP 요청을 시스템에서 실행되는 다른 SNMP 에이전트에게 전달할 수 있습니다.

IM and Presence Service 및 Unified Communications Manager의 경우 가상 시스템에 설치되어 있으면 이 서비스가 표시되지 않습니다.

시스템 애플리케이션 에이전트

이 서비스는 시스템에 설치되어 실행 중인 애플리케이션에 대한 SNMP 액세스를 제공합니다. 이는 SYSAPPL-MIB를 구현합니다.

Cisco CDP 에이전트

이 서비스는 Cisco 검색 프로토콜을 사용하여 노드의 네트워크 연결 정보에 대한 SNMP 액세스를 제공합니다. 이 서비스는 CISCO-CDP-MIB를 구현합니다.

Cisco Syslog Agent

이 서비스는 다양한 Unified Communications Manager 구성 요소가 생성하는 syslog 메시지 수집을 지원합니다. 이 서비스는 CISCO-SYSLOG-MIB를 구현합니다.

주의 네트워크 관리 시스템이 더 이상 네트워크를 모니터링하지 않으므로 SNMP 서비스를 중지하면 데이터가 손실될 수 있습니다. 기술 지원팀이 사용자에게 지시하지 않는 한 서비스를 중지하지 마십시오.

Cisco 인증서 변경 알림

이 서비스는 클러스터의 모든 노드에서 Tomcat, CallManager 및 XMPP와 같은 구성 요소의 인증서를 자동으로 동기화합니다. 서비스가 중지되고 인증서를 다시 생성하면 다른 노드의 인증서 신뢰에 수동으로 업로드해야 합니다.

플랫폼 관리 웹 서비스

플랫폼 관리 웹 서비스는 PAWS-M 서버가 시스템을 업그레이드할 수 있도록 하는 Unified Communications Manager, IM and Presence Service및 Cisco Unity Connection 시스템에서 활성화할 수 있는 SOAP(Simple Object Access Protocol) API입니다.

중요 PAWS-M 서버에서 플랫폼 관리 웹 서비스를 활성화하지 마십시오.

플랫폼 통신 웹 서비스

플랫폼 간 통신 웹 서비스는 Unified Communications Manager , IM and Presence Service및 Cisco Unity Connection 시스템에서 실행되는 REST (Representational State Transfer Protocol) API입니다.

참고 플랫폼 통신 웹 서비스는 수동으로 시작하거나 중지할 수 없습니다.

Cisco 인증서 만료 모니터

이 서비스는 시스템에서 생성한 인증서의 만료 상태를 정기적으로 확인하고 인증서가 만료 날짜에 근접한 경우 알림을 보냅니다. Unified Communications Manager의 경우 Cisco Unified 운영 체제 관리에서 이 서비스를 사용하는 인증서를 관리합니다. IM and Presence Service의 경우 Cisco Unified IM and Presence 운영 체제 관리에서 이 서비스를 사용하는 인증서를 관리합니다.

Cisco Smart License Manager

Cisco Smart License Manager는 게시자에서만 실행되는 네트워크 서비스입니다. 이는 Unified Communications Manager 게시자의 모든 Cisco 스마트 라이센스 작업을 관리합니다. Cisco Smart License Manager 서비스는 제품의 라이센스 또는 권리 사용을 Cisco Smart Software Manager 또는 Cisco Smart Software Manager 위성에 보고하고 Cisco Smart Software Manager 또는 Cisco Smart Software Manager 위성에서 인증 상태를 가져옵니다.

보안 서비스

Cisco 인증서 등록 서비스

이 서비스는 온라인 타사 CA와 인증 기관 프록시 기능 간에 온라인 연결을 생성합니다. LSC 인증서 서명에 인증 기관 프록시 기능을 사용하는 온라인 CA를 사용하려면 이 서비스를 활성해야 합니다.

Cisco 신뢰 확인 서비스

이 서비스는 IM and Presence Service에서 지원되지 않습니다.

Cisco 신뢰 확인 서비스는 전화 및 기타 엔드포인트를 대신하여 인증서를 인증하는 CallManager 서버 또는 전용 서버에서 실행되는 서비스입니다. 이는 인증서 소유자에 대한 역할 목록을 연결합니다. 인증서 또는 소유자를 하나 이상의 역할에 연결할 수 있습니다.

전화기와 신뢰 확인 서비스 간의 프로토콜을 사용하면 전화기에서 확인을 요청할 수 있습니다. 신뢰 확인 서비스는 인증서의 유효성을 확인하고 이에 연결된 역할 목록을 반환합니다. 이 프로토콜을 사용하면 신뢰 확인 서비스가 요청을 인증하고, 반대로 전화기가 확인 서비스의 응답을 인증하도록 할 수 있습니다. 프로토콜은 요청과 응답의 무결성을 보호합니다. 요청의 기밀성 및 응답은 필요하지 않습니다.

Cisco 신뢰 확인 서비스의 다중 인스턴스는 확장성을 제공하기 위해 클러스터의 서로 다른 서버에서 실행됩니다. 이러한 서버는 Cisco Unified CallManager를 호스팅하는 것과 같을 수도 있고 그렇지 않을 수도 있습니다. 전화기는 네트워크에서 신뢰 확인 서비스 목록을 가져오고 선택 알고리즘(예: 라운드 로빈)을 사용하여 이들 서비스 중 하나에 연결합니다. 연결된 신뢰 확인 서비스가 응답하지 않으면 전화기가 목록에서 다음 신뢰 확인 서비스로 전환합니다.

데이터베이스 서비스

Cisco Database Layer Monitor

Cisco Database Layer Monitor 서비스는 데이터베이스 레이어의 측면을 모니터링합니다. 이 서비스는 변경 알림 및 모니터링을 처리합니다.

참고 Unified Communications Manager는 자동 업데이트 통계, 데이터베이스 테이블의 변경 사항을 모니터링하고 통계 업데이트가 필요한 테이블만 업데이트하는 인텔리전트 통계 업데이트 기능을 사용합니다. 이 기능은 특히, Unified Communications Manager의 VMware 배포 시 상당한 대역폭을 절약합니다. 자동 업데이트 통계는 기본 인덱싱 방법입니다.

SOAP 서비스

Cisco SOAP 실시간 서비스 API

IM and Presence Service만 해당: Cisco SOAP 실시간 서비스 API는 클라이언트 로그인 및 프레즌스 데이터에 대한 타사 API를 지원합니다.

Unified Communications Manager 및 Cisco Unity Connection만 해당: Cisco SOAP 실시간 서비스 API를 사용하여 장치 및 CTI 애플리케이션에 대한 실시간 정보를 수집할 수 있습니다. 이 서비스는 서비스를 활성화, 시작 및 중지하기 위한 API를 제공합니다.

Cisco SOAP 성능 모니터링 Api

Cisco SOAP 성능 모니터링 API 서비스를 사용하면 SOAP API를 통해 다양한 애플리케이션에 대한 성능 모니터링 카운터를 사용할 수 있습니다. 예를 들어, 서비스, CPU 사용량 및 성능 모니터링 카운터 별로 메모리 정보를 모니터링할 수 있습니다.

Cisco SOAP 로그 수집 API

Cisco SOAP 로그 수집 API 서비스를 사용하면 로그 파일을 수집하고 원격 SFTP 서버에서 로그 파일 수집을 예약할 수 있습니다. 수집할 수 있는 로그 파일의 예에는 syslog, 코어 덤프 파일 및 Cisco 애플리케이션 추적 파일 등이 있습니다.

SOAP 진단 포털 데이터베이스 서비스

Cisco Unified RTMT(실시간 모니터링 도구)는 RTMT Analysis Manager 호스팅 데이터베이스에 액세스하는 데 SOAP 진단 포털 데이터베이스 서비스를 사용합니다. RTMT는 운영자가 정의한 필터 선택 사항을 기반으로 통화 레코드를 수집합니다. 이 서비스가 중지되면 RTMT가 데이터베이스에서 통화 레코드를 수집할 수 없습니다.

CM 서비스

이 섹션에서는 Unified Communications Manager CM 서비스에 대해 설명하며 IM and Presence Service 및 Cisco Unity Connection에는 적용되지 않습니다.

Cisco CallManager 개인 디렉터리

Cisco CallManager 개인 디렉터리 서비스는 Cisco 개인 디렉터리를 지원합니다.

Cisco Business Edition 5000 시스템에서 이 서비스는 Unified Communications Manager만 지원합니다.

Cisco Extension Mobility Application

Cisco Extension Mobility 애플리케이션 서비스를 사용하면 전화기 구성에서 Cisco Extension Mobility 기능에 대한 지속 시간 제한과 같은 로그인 설정을 정의할 수 있습니다.

Unified Communications Manager만 해당: Cisco Extension Mobility 기능을 사용하면 Unified Communications Manager 클러스터 내 사용자가 다른 전화기에 로그인하여 클러스터의 다른 전화기를 자체 전화기로 일시적으로 구성할 수 있습니다. 사용자가 로그인한 후에는 전화기가 개인 전화 번

호, 단축 다이얼, 서비스 링크 및 사용자의 기타 사용자 특정 속성을 선택합니다. 로그아웃한 후에는 전화기가 원래 사용자 프로파일을 사용합니다.

Cisco CallManager Cisco IP 전화기 Services

Cisco CallManager Cisco IP 전화기 서비스는 Cisco Unified Communications Manager 관리에서 구성한 Cisco Unified IP 전화기 서비스에 대한 서비스 URL을 초기화합니다.

Cisco Business Edition 5000 시스템에서 이 서비스는 Unified Communications Manager만 지원합니다.

Cisco 사용자 데이터 서비스

Cisco 사용자 데이터 서비스는 Cisco 유니파이드 IP 전화기에 Cisco Unified Communications Manager 데이터베이스에서 사용자 데이터에 액세스할 수 있는 기능을 제공합니다. Cisco 사용자 데이터 서비스는 Cisco 개인 디렉터리에 대한 지원을 제공합니다.

Cisco 푸시 알림 서비스

Cisco 푸시 알림 서비스는 Cisco Unified Communications Manager에서 Apple iOS 장치에 수신되는 통화에 대한 푸시 알림을 전송하는 기능을 제공합니다. 이 서비스는 Cisco CallManager 서비스에서 Cisco 협업 클라우드 (Collaboration Cloud)로 푸시 알림 메시지를 릴레이합니다. 이 서비스는 푸시 알림을 전송하는 데 사용되는 액세스 토큰도 관리합니다.

Cisco 헤드셋 서비스

Cisco 헤드셋 서비스를 사용하면 호환되는 Cisco IP 전화기, Cisco Jabber 또는 기타 Cisco 장치를 사용하는 경우 Cisco 헤드셋의 인벤토리, 구성 업데이트 및 진단 데이터를 관리할 수 있습니다.

참고 Cisco CallManager 서비스가 이미 실행 중인 경우 모든 Unified Communications Manager 노드에서 Cisco 헤드셋 서비스를 활성화해야 합니다. Cisco Unified CM 관리 인터페이스를 사용하여 헤드셋을 관리하려는 Unified Communications Manager 노드에서 Cisco 헤드셋 서비스를 활성화해야 합니다. Cisco 헤드셋 서비스를 활성화하면 Cisco CallManager 서비스가 자동으로 활성화됩니다. 필요하지 않은 경우 Cisco CallManager 서비스를 비활성화합니다.

IM and Presence Service 서비스

IM and Presence Service 서비스는 IM and Presence Service에만 적용됩니다.

Cisco 로그인 데이터 저장소

Cisco 로그인 데이터 저장소는 Cisco 클라이언트 프로파일 에이전트에 클라이언트 세션을 저장하는 실시간 데이터베이스입니다.

Cisco 라우트 데이터 저장소

Cisco 경로 데이터 저장소는 Cisco SIP 프록시 및 Cisco 클라이언트 프로파일 에이전트에 대한 경로 정보 및 할당된 사용자의 캐시를 저장하는 실시간 데이터베이스입니다.

Cisco 구성 에이전트

Cisco 구성 에이전트는 IM and Presence Service IDS 데이터베이스의 구성 변경 사항을 Cisco SIP 프록시에 알리는 변경 알림 서비스입니다.

Cisco Sync Agent

Cisco Sync Agent는 IM and Presence 데이터를 Unified Communications Manager 데이터와 동기화 상태로 유지합니다. 이는 IM and Presence에 중요한 데이터를 위해 Unified Communications Manager에게 SOAP 요청을 보내고, Unified Communications Manager에서 알림을 변경하고 IM and Presence IDS 데이터베이스를 업데이트합니다.

Cisco OAM 에이전트

Cisco OAM 에이전트 서비스는 프레즌스 엔진에 중요한 IM and Presence Service IDS 데이터베이스의 구성 매개 변수를 모니터링합니다. 데이터베이스에서 변경 사항이 발생하면 OAM 에이전트는 구성 파일을 작성하고 RPC 알림을 프레즌스 엔진으로 전송합니다.

Cisco 클라이언트 프로파일 에이전트

Cisco 클라이언트 프로파일 에이전트 서비스는 HTTPS를 사용하여 외부 클라이언트 간에 보안 SOAP 인터페이스를 제공합니다.

Cisco 클러스터 간 동기화 에이전트

Cisco 클러스터 간 동기화 에이전트 서비스는 다음을 제공합니다. Unified Communications Manager로의 DND 전파 및 클러스터 간 SIP 라우팅을 위해 IM and Presence Service 클러스터 간에 최종 사용자 정보를 동기화합니다.

Cisco XCP 라우터

XCP 라우터는 IM and Presence Service 서버의 핵심 통신 기능입니다. IM and Presence Service에 XMPP 기반 라우팅 기능을 제공합니다. XMPP 데이터를 IM and Presence Service의 다른 활성 XCP 서비스로 라우팅하고, 시스템에서 XMPP 데이터를 IM and Presence Service사용자로 라우팅할 수 있도록 SDNS에 액세스합니다. XCP 라우터는 사용자에 대한 XCP 세션을 관리하고 이러한 세션 간에 XCP 메시지를 라우팅합니다.

IM and Presence Service 설치 후에 시스템은 기본적으로 Cisco XCP 라우터를 설정합니다.

참고 Cisco XCP 라우터를 다시 시작하면 IM and Presence Service는 자동으로 모든 활성 XCP 서비스를 다시 시작합니다. Cisco XCP 라우터를 껐다가 켜는 것이 아니라 다시 시작 옵션을 선택하여 Cisco XCP 라우터를 다시 시작해야 합니다. Cisco XCP 라우터를 다시 시작하는 대신 끄면 IM and Presence Service는 다른 모든 XCP 서비스를 중지합니다. 그 후에 XCP 라우터를 켜면 IM and Presence Service는 다른 XCP 서비스를 자동으로 설정하지 않습니다. 따라서 사용자가 직접 다른 XCP 서비스를 설정해야 합니다.

Cisco XCP 구성 관리자

Cisco XCP 구성 관리자 서비스는 관리 GUI를 통해 이루어지고 다른 XCP 구성 요소에 영향을 미치는 (예: 라우터 및 메시지 아카이버) 구성 및 시스템 토폴로지 변경 사항(클러스터 간 피어에서 동기화되는 토폴로지 변경 포함)을 모니터링하고 필요에 따라 이러한 구성 요소를 업데이트합니다. Cisco XCP 구성 관리자 서비스는 관리자를 위해 XCP 구성 요소를 다시 시작해야 하는 경우(이러한 변경으로 인해)에 대한 알림을 생성하고, 다시 시작이 완료되면 자동으로 알림을 지웁니다.

Cisco 서버 복구 관리자

Cisco SRM(서버 복구 관리자)은 프레즌스 중복 그룹의 노드 간 페일오버를 관리합니다. SRM은 노드의 모든 상태 변경을 관리합니다. 상태 변경은 자동으로 수행되거나 관리자가 수동으로 시작합니다. 프레즌스 중복 그룹에서 고가용성을 설정하고 나면 각 노드의 SRM에서 피어 노드와 하트비트 연결을 설정하고 중요한 프로세스를 모니터링하기 시작합니다.

Cisco IM and Presence 데이터 모니터

Cisco IM and Presence 데이터 모니터는 IM and Presence Service에서 IDS 복제 상태를 모니터링합니다. 다른 IM and Presence Service는 Cisco IM and Presence 데이터 모니터에 의존합니다. 이러한 의존형 서비스는 IDS 복제가 안정적인 상태로 바뀔 때까지 Cisco 서비스를 사용하여 시작을 연기합니다.

Cisco IM and Presence 데이터 모니터는 또한 Unified Communications Manager에서 Cisco Sync Agent의 상태를 확인합니다. IDS 복제가 설정되고 IM and Presence 데이터베이스 게시자 노드의 동기화 에이전트가 Unified Communications Manager에서 동기화를 완료한 후에야 의존형 서비스의 시작이 허용됩니다. 시간 제한에 도달했으면 IDS 복제 및 동기화 에이전트가 완료되지 않았더라도, 게시자 노드의 Cisco IM and Presence 데이터 모니터는 의존형 서비스의 시작을 허용합니다.

가입자 노드에서, Cisco IM and Presence 데이터 모니터는 IDS 복제가 성공적으로 설정될 때까지 기능 서비스의 시작을 연기합니다. Cisco IM and Presence 데이터 모니터는 클러스터에서 문제의 가입자 노드에 대해서만 기능 서비스의 시작을 연기하며, 하나의 문제 노드 때문에 모든 가입자 노드에서 기능 서비스의 시작을 연기하지는 않습니다. 예를 들어, IDS 복제가 노드1과 노드2에서는 성공적으로 설정되었지만 노드3에서는 그렇지 못한 경우 Cisco IM and Presence 데이터 모니터는 노드1과 노드2에서는 기능 서비스 시작을 허용하되 노드 3에서는 기능 서비스 시작을 연기합니다.

Cisco Presence 데이터 저장소

Cisco Presence 데이터 저장소는 일시적으로 존재하는 데이터 및 서브스크립션을 저장하기 위한 실시간 데이터베이스입니다.

Cisco SIP 등록 데이터 저장소

Cisco 프레즌스 SIP 등록 데이터 저장소는 SIP 등록 데이터를 저장하는 실시간 데이터베이스입니다.

Cisco RCC 장치 선택

Cisco RCC 장치 선택 서비스는 원격 통화 제어를 위한 Cisco IM and Presence 사용자 장치 선택 서비스입니다.

CDR 서비스

이 섹션에서는 CDR 서비스에 대해 설명하며 IM and Presence Service 및 Cisco Unity Connection에는 적용되지 않습니다.

Cisco CDR Repository Manager

이 서비스는 Cisco CDR Agent 서비스에서 얻은 생성된 CDR(통화 세부 정보 레코드)를 유지하고 이동합니다. 클러스터를 지원하는 시스템에서는(Unified Communications Manager만 해당) 서비스가 첫 번째 서버에 존재합니다.

Cisco CDR Agent

참고 Unified Communications Manager는 Cisco Unified Communications Manager시스템에서 Cisco CDR Agent를 지원합니다.

이 서비스는 IM and Presence Service 및 Cisco Unity Connection을 지원하지 않습니다.

Cisco CDR Agent 서비스는 Unified Communications Manager에서 생성한 CDR 및 CMR 파일을 로컬 호스트에서 CDR 저장소 서버로 전송합니다. 여기서 CDR 저장소 관리자 서비스는 SFTP 연결을 통해 실행됩니다.

이 서비스는 로컬 호스트에서 생성된 CDR 및 CMR 파일을 클러스터의 CDR 저장소 서버로 전송합니다. CDR 저장소 노드 독립 실행형 서버의 CDR 에이전트는 독립 실행형 서버에서 생성한 파일을 SFTP 연결을 통해 Cisco CDR 저장소 관리자로 전송합니다. CDR 에이전트는 파일을 유지 관리하고 이동합니다.

이 서비스가 작동하려면 서버에서 Cisco CallManager 서비스를 활성화하고 서버가 실행 중이어야합니다. 구성에서 클러스터를 지원하는 경우(Unified Communications Manager만 해당) 첫 번째 서버에서 Cisco CallManager 서비스를 활성화합니다.

Cisco CAR Scheduler

Cisco CDR Analysis and Reporting(CAR) Scheduler 서비스는 IM and Presence Service 및 Cisco Unity Connection을 지원하지 않습니다.

Cisco CAR Scheduler 서비스를 사용하여 CAR 관련 작업을 예약할 수 있습니다. 예를 들어, CAR 데이터베이스에 보고서 생성 또는 CDR 파일 로드를 예약할 수 있습니다.

Cisco SOAP-CallRecord 서비스

Cisco SOAP-CallRecord 서비스는 기본적으로 게시자에서 SOAP 서버로 실행되므로 클라이언트가 SOAP API를 통해 CAR 데이터베이스에 연결할 수 있습니다. 이 연결은 CAR 커넥터(별도의 CAR ID 인스턴스 사용)를 사용하여 수행됩니다.

Cisco CAR DB

Cisco CAR DB는 CAR 데이터베이스에 대한 Informix 인스턴스를 관리하며, 이를 통해 서비스 관리자는 이 서비스를 시작하거나 중지하고 CAR ID 인스턴스를 개별적으로 가져오거나 종료할 수 있습니다. 이는 CCM ID 인스턴스를 유지 관리하는 데 사용되는 Unified Communications Manager 데이터베이스와 유사합니다.

Cisco CAR DB 서비스는 기본적으로 게시자에서 활성화됩니다. Car DB 인스턴스가 설치되고 게시자에서 활발히 실행되어 CAR 데이터베이스를 유지 관리합니다. 이 네트워크 서비스는 게시자에서만 사용되며 가입자에서 사용할 수 없습니다.

관리 서비스

이 섹션에서는 관리 서비스에 대해 설명하며 Cisco Unity Connection에는 적용되지 않습니다.

Cisco CallManager 관리

Cisco CallManager 관리 서비스는 IM and Presence Service 및 Cisco Unity Connection에서 지원되지 않습니다.

Cisco CallManager 관리 서비스는 Unified Communications Manager 설정을 구성하는 데 사용하는 웹 애플리케이션/인터페이스인 Cisco Unified Communications Manager 관리를 지원합니다. Unified Communications Manager 설치 후 이 서비스는 자동으로 시작되며 GUI (그래픽 사용자 인터페이스)에 액세스할 수 있습니다. 이 서비스를 중지하면 해당 서버를 탐색할 때 Cisco Unified Communications Manager 관리 그래픽 사용자 인터페이스에 액세스할 수 없습니다.

Cisco IM and Presence 관리

Cisco IM and Presence 관리 서비스는 Unified Communications Manager 및 Cisco Unity Connection에서 지원되지 않습니다.

Cisco IM and Presence 관리 서비스는 IM and Presence Service 설정을 구성하는 데 사용하는 웹 애플리케이션/인터페이스인 Cisco Unified Communications Manager IM and Presence 관리를 지원합니다. IM and Presence Service 설치 후 이 서비스는 자동으로 시작되며 GUI에 액세스할 수 있습니다. 이 서비스를 중지하면 해당 서버를 탐색할 때 Cisco Unified Communications Manager IM and Presence 관리 GUI에 액세스할 수 없습니다.

Services setup

제어 센터

서비스 가용성 GUI의 제어 센터에서 상태를 보고 한 번에 하나의 서비스를 시작하고 중지할 수 있습니다. 네트워크 서비스를 시작, 중지 및 다시 시작하려면 제어 센터 - 네트워크 서비스 창에 액세스합니다. 기능 서비스를 시작, 중지 및 다시 시작하려면 제어 센터 - 기능 서비스 창에 액세스합니다.

팁 관련 링크 드롭다운 목록 상자와 이동 버튼을 사용하여 제어 센터 및 서비스 활성화 창으로 이동합니다.

Unified Communications Manager 및 IM and Presence만 해당: 클러스터 구성에서는 클러스터에서 한 번에 한 서버에 대해 상태를 보고 서비스를 시작하고 중지할 수 있습니다.

Unified Communications Manager만 해당: 기능 서비스를 시작하고 중지하면 해당서비스에 현재 등록되어 있는 모든 Cisco Unified IP 전화기 및 게이트웨이가 보조 서비스로 페일오버됩니다. 장치 및 전화기는 보조 서비스에 등록할 수 없는 경우에만 다시 시작해야 합니다. 서비스를 시작하고 중지하면 해당 Unified Communications Manager에 속한 다른 설치된 애플리케이션(예: 전화회의 브리지 또는 Cisco Messaging Interface)이 시작되고 중지될 수 있습니다.

주의 Unified Communications Manager만 해당: 서비스를 중지하면 서비스에서 제어하는 모든 장치에 대한 통화 처리도 중지됩니다. 서비스가 중지되면 IP 전화기에서 다른 IP 전화기로의 통화는 계속 작동합니다. IP 전화기에서 MGCP(Media Gateway Control Protocol) 게이트웨이로 진행 중인 통화도 계속 유지되지만 다른 통화 유형은 삭제됩니다.

서비스 설정

서비스 작업 시 다음 작업을 수행할 수 있습니다.

프로시저

단계 **1** 실행할 기능 서비스를 활성화합니다.

단계 **2** 적절한 서비스 매개 변수를 구성합니다.

단계 **3** 필요한 경우 서비스 가용성 GUI 추적 도구를 사용하여 문제를 해결합니다.

서비스 활성화

참고 여러 기능 서비스를 활성화 또는 비활성화하거나 기본 서비스를 선택하여 서비스 가용성 GUI의 서비스 활성화 창에서 활성화할 수 있습니다. IM and Presence 노드에서 Unified Communications Manager 서비스를 보고, 시작하고, 중지할 수 있으며 그 반대의 경우도 마찬가지입니다. 다음 오류가 발생할 수 있습니다. "서버에 연결을 설정할 수 없습니다(원격 노드에 액세스할 수 없음)". 이 오류 메시지가 나타나는 경우 *Cisco Unified Communications Manager* 관리 설명서를 참조하십시오.

참고 Unified Communications Manager 릴리스 6.1.1로 시작하여 최종 사용자는 더 이상 Cisco 통합 서비스 가용성에 액세스하여 서비스를 시작하고 중지할 수 없습니다.

기능 서비스는 자동 모드에서 활성화되며 서비스 가용성 GUI는 단일 노드 구성을 기반으로 서비스 종속성을 확인합니다. 기능 서비스를 활성화하도록 선택하면 실행할 서비스에 의존하는 다른 서비스(있는 경우)를 모두 선택하라는 메시지가 표시됩니다. 기본값 설정을 클릭하면 서비스 가용성 GUI가 서버에서 실행하는 데 필요한 서비스를 선택합니다.

Unified Communications Manager 및 IM and Presence Service만 해당: 클러스터를 지원하는 구성에서도 이 프로세스는 단일 서버 구성을 기반으로 합니다.

서비스를 활성화하면 서비스가 자동으로 시작됩니다. 제어 센터에서 서비스를 시작하고 중지할 수 있습니다.

Cisco Unified Communications Manager에 대한 클러스터 서비스 활성화 권장 사항

클러스터에서 서비스를 활성화하기 전에 다중 서버 Unified Communications Manager 구성에 대한 서비스 권장 사항을 제공하는 다음 표를 검토하십시오.

표 ***34: Cisco Unified Communications Manager*** 서비스 활성화 권장 사항

서비스/서블릿	활성화 권장 사항
CM 서비스	

서비스/서블릿	활성화 권장 사항
Cisco CallManager	이 서비스는 Unified Communications Manager를 지원합니다. 제어 센터 - 네트워크 서비스에서 Cisco RIS Data Collector 서비스 및 Database Layer 서비스가 노드에서 실행되고 있는지 확인합니다. 팁 이 서비스를 활성화하기 전에 Unified Communications Manager 서버가 Cisco Communications Manager 관리의 Unified Communications Manager 찾기/나 표시되는지 확인합니다. 서버가 표시되지 않으면 이 서비스를 활성화하기 Unified Communications Manager 서버를 추가합니다. 서버를 추가하는 방법에 대한 자세한 내용은 *Cisco Unified Communications M* 시스템 구성 설명서를 참조하십시오.
Cisco Messaging Interface	서버에 연결된 USB-직렬 어댑터를 사용하여 타사 음성 메일 시스템으로 SMDI 통 용하는 경우에만 활성화합니다.
Cisco Unified Mobile Voice Access Service	모바일 음성 액세스가 작동하려면 첫 번째 VXML 페이지를 가리키도록 H.323 게 이를 구성한 후에 클러스터의 첫 번째 노드에서 이 서비스를 활성화해야 합니다. Cisco CallManager와 Cisco TFTP 서비스가 클러스터의 한 서버에서 실행되는지 확 다 .이는 Cisco Unified Mobile Voice Access Service가 실행되는 서버와 반드시 동일 않습니다.
Cisco IP Voice Media Streaming App	클러스터에 둘 이상의 노드가 있는 경우 클러스터당 한 개 또는 두 개의 서버를 활 니다. 특히 대기 중 음악 전용 노드를 활성화할 수 있습니다. 이 서비스를 사용하려 러스터의 한 노드에서 Cisco TFTP를 활성화해야 합니다. Cisco CallManager 서비스 행하는 노드 또는 첫 번째 노드에서 이 서비스를 활성화하지 마십시오.
Cisco CTIManager	JTAPI/TAPI 애플리케이션을 연결할 각 노드를 활성화합니다. CTIManager를 활성 면 노드에서 Cisco CallManager 서비스를 활성화해야 합니다. CTIManager 및 Cisc CallManager 서비스 상호 작용에 대한 자세한 내용은 CM 서비스 관련 항목을 참조 오.
Cisco Extension Mobility	클러스터에서 모든 노드를 활성화합니다.
Cisco Extended Functions	Cisco RIS Data Collector를 실행하는 하나 이상의 서버에서 QRT(품질 보고 도구)를 하는 이 서비스를 활성화합니다. 클러스터의 노드에서 Cisco CTIManager 서비스를 화해야 합니다.
Cisco DHCP 모니터 서비스	DHCP 모니터 서비스가 활성화되면 IP 전화기의 IP 주소에 영향을 미치는 데이터 의 변경 사항을 감지하고, /etc/dhcpd.conf 파일을 수정하고, 업데이트된 구성 파일 하여 DHCPD 디먼을 중지했다가 다시 시작합니다. DHCP가 활성화된 노드에서 이 스를 활성화합니다.

서비스/서블릿	활성화 권장 사항
Cisco 위치 대역폭 관리자	Cisco 위치 통화 허용 제어 기능을 사용하여 오디오 및 영상 통화에 대한 대역폭 할당 관리하려는 경우 이 서비스를 활성화해야 합니다. 이 서비스는 Cisco CallManager 서 와 함께 작동합니다. Cisco CallManager 서비스를 실행하는 동일한 서버에서 Cisco Loca 대역폭 관리자를 실행하는 것이 좋습니다. 위치 대역폭 관리자가 CallManager 서비스 동일한 서버에서 실행되고 있지 않은 경우 위치 대역폭 관리자 그룹을 올바르게 구성 는지 확인하십시오.
Cisco 클러스터 간 조회 서비스	여러 Unified Communications Manager 클러스터 간에 URI 및 숫자 라우팅 정보를 전파 려는 경우 이 교환에 참여하는 클러스터의 게시자에서 이 서비스를 활성화해야 합니
Cisco Dialed Number Analyzer 서버	클러스터에 노드가 두 개 이상 있는 경우 Cisco Dialed Number Analyzer 서비스 전용으 제공되는 한 노드에서 이 서비스를 활성화합니다.
Cisco Dialed Number Analyzer	Unified Communications Manager Dialed Number Analyzer를 사용할 계획인 경우 이 서 를 활성화합니다. 이 서비스는 많은 리소스를 소비할 수 있으므로 통화 처리 작업이 가 적은 노드 또는 사용량이 많지 않은 시간에만 노드에서 이 서비스를 활성화하면 됩니
Cisco TFTP	클러스터에 노드가 두 개 이상 있는 경우 Cisco TFTP 서비스 전용으로 제공되는 한 노 에서 이 서비스를 활성화합니다. 클러스터에 있는 둘 이상의 노드에서 이 서비스를 활 화하는 경우에는 옵션 150을 구성합니다.
Cisco 헤드셋 서비스	Unified Communications Manager에서 Cisco 헤드셋을 관리하려는 경우 이 서비스를 활 화합니다. 참고 Cisco CallManager 서비스가 이미 실행 중인 경우 모든 Unified Communications Manager 노드에서 Cisco 헤드셋 서비스를 활성화해야 합니다. Cisco Unified C 관리 인터페이스를 사용하여 헤드셋을 관리하려는 Unified Communications Mana 노드에서 Cisco 헤드셋 서비스를 활성화해야 합니다. Cisco 헤드셋 서비스를 활 화하면 Cisco CallManager 서비스가 자동으로 활성화됩니다. 필요하지 않은 경 Cisco CallManager 서비스를 비활성화합니다.
CTI 서비스	
Cisco IP Manager Assistant	Cisco Unified Communications Manager Assistant를 사용하려는 경우에는 클러스터의 두 버(기본 및 백업)에서 이 서비스를 활성화합니다. Cisco CTI Manager 서비스가 클러스 에서 활성화되어 있는지 확인합니다. Cisco IP Manager Assistant에 대한 자세한 내용은 *Cisco Unified Communications Manag* 기능 구성 설명서를 참조하십시오.
Cisco WebDialer 웹 서비스	클러스터당 한 노드에서 활성화합니다.

서비스/서블릿	활성화 권장 사항
셀프 프로비저닝 IVR	셀프 프로비저닝 IVR 서비스를 활성화하려면 Cisco CTI Manager 서비스를 활성화 니다. 서비스가 비활성화되어 있는 경우에도 셀프 프로비저닝을 구성할 수 있지만 관리 IVR 서비스를 사용하여 사용자에 IP 전화기를 할당할 수는 없습니다. 기본적으로 스는 비활성화되어 있습니다.
CDR 서비스	
Cisco SOAP-CDROnDemand Service	Cisco SOAP-CDROnDemand Service는 첫 번째 서버에서만 활성화할 수 있으며, Cis Repository Manager와 Cisco CDR Agent 서비스가 동일한 서버에서 실행되고 있어 다. Unified Communications Manager 릴리스 12.x 이후 버전의 경우 CDR onDemand 서 기본적으로 활성화되어 있지 않습니다. CDR onDemand 서비스를 활성화하려면 서 를 수동으로 활성화해야 합니다. 다음 명령을 루트 수준에서 실행하여 CDR onDem 비스를 활성화합니다. `/usr/local/cm/bin/soapservicecontrol2.shCDRonDemandServiceCDRonDemanddepl`
Cisco CAR Web Service	Cisco CAR Web Service는 첫 번째 서버에서만 활성화할 수 있으며, Cisco CAR Sch 서비스가 활성화되어 동일한 서버에서 실행되고 있으며 CDR Repository Manager 가 동일한 서버에서 실행되고 있어야합니다.
데이터베이스 및 관리 서비스	
Cisco AXL 웹 서비스	설치 후에는 모든 클러스터 노드에서 Cisco AXL Web Service가 기본적으로 활성화 다. 항상 게시자 노드에서 서비스를 활성화된 상태로 두는 것이 좋습니다. 이를 통해 Provisioning Manager와 같은 AXL에 의존하는 제품을 구성할 수 있습니다. 요구 사항에 따라 기능 서비스 아래에서 Cisco 통합 서비스 가용성의 특정 가입자 서 서비스를 활성화하거나 비활성화할 수 있습니다.
Cisco Bulk Provisioning Service	첫 번째 노드에서만 Cisco Bulk Provisioning 서비스를 활성화할 수 있습니다. Bulk Administration Tool(BAT)을 사용하여 사용자를 관리하는 경우 이 서비스를 활성화 합니다.
Cisco UXL Web Service	이 서비스는 인증 및 사용자 인증 확인을 수행합니다. Cisco IP 전화기 주소록 동기 에서 TabSync 클라이언트는 Cisco Unified Communications Manager 데이터베이스 쿼리에 Cisco UXL 웹 서비스를 사용합니다. Cisco IP 전화기 주소록 동기화 장치를 사용할 계획인 경우, 한 노드(게시자 노드 서 이 서비스를 활성화해야 합니다. Cisco IP 전화기 주소록 동기화 장치를 사용하 경우 이 서비스를 비활성화하는 것이 좋습니다. 기본적으로 이 서비스는 비활성화 있습니다.

서비스/서블릿	활성화 권장 사항
Cisco 플랫폼 관리 웹 서비스	Cisco Prime Collaboration Deployment(PCD) 서버를 사용하여 업그레이드, 버전 전환, 시작 또는 주소 작업을 관리할 계획인 경우 이 서비스를 활성화해야 합니다. PAWS(폼 관리 웹 서비스)를 사용하면 Call Manager와 PCD(Prime Collaboration Deployment) SOAP 통신이 가능합니다다. 클러스터에 둘 이상의 노드가 있는 경우 클러스터의 각 에서 이 서비스를 활성화해야 합니다.
Cisco TAPS 서비스	Cisco Unified Communications Manager 자동 등록 전화기 도구를 사용하려면 먼저 첫 노드에서 이 서비스를 활성화해야 합니다. Cisco Unified Communications Manager 자동 록 전화기 도구에 대한 더미 MAC 주소를 생성할 때 Cisco Bulk Provisioning 서비스가 일한 노드에서 활성화되어 있는지 확인합니다.
성능 및 모니터링 서비스	
Cisco 서비스 가용성 리포터	첫 번째 노드에서만 활성화합니다. 참고 다른 노드에서 서비스를 활성화하는 경우에는 서비스에서 첫 번째 노드에 대 보고서만 생성합니다.
Cisco CallManager SNMP Service	SNMP를 사용하는 경우 클러스터의 모든 서버에서 이 서비스를 활성화합니다.
보안 서비스	
Cisco CTL Provider	클러스터의 모든 서버에서 활성화합니다.
Cisco Certificate Authority Proxy Function(CAPF)	첫 번째 노드에서만 활성화합니다.
디렉터리 서비스	
Cisco DirSync	첫 번째 노드에서만 활성화합니다.

IM and Presence Service에 대한 클러스터 서비스 활성화 권장 사항

⚠

주의 기능에 대한 서비스를 설정하기 전에 해당 기능에 대한 IM and Presence에 대한 모든 필수 구성을 완료해야 합니다. 각 IM and Presence 기능에 대한 관련 설명서를 참조하십시오.

클러스터에서 서비스를 설정하기 전에 다중 노드 IM and Presence 구성에 대한 서비스 권장 사항을 제공하는 다음 표를 검토하십시오.

표 ***35: IM and Presence Service*** 활성화 권장 사항

서비스/서블릿	권장 사항
데이터베이스 및 관리 서비스	

서비스/서블릿	권장 사항
Cisco AXL 웹 서비스	설치 후에는 모든 클러스터 노드에서 Cisco AXL Web Service가 기본적으로 활성화됩니다. IM and Presence Service 데이터베이스 게시자 노드에서 서비스를 항상 활성화된 상태로 두는 것이 좋습니다. 이렇게 하면 AXL에 의존하는 제품을 구성할 수 있습니다. 클러스터 간 통신이 구성된 경우 원격 피어가 동기화되도록 구성된 하위 클러스터의 두 노드에서 이 서비스를 활성화해야 합니다. 두 노드에서 이 서비스를 활성화하지 않으면 페일오버 시나리오에서 IM 기능이 손실됩니다. 요구 사항에 따라 기능 서비스 아래에서 Cisco Unified 서비스 가용성의 특정 IM and Presence 가입자 노드에서 서비스를 활성화하거나 비활성화할 수 있습니다.
Cisco Bulk Provisioning Service	• 첫 번째 노드에서만 Cisco Bulk Provisioning 서비스를 설정합니다. • BAT(Bulk Administration Tool)를 사용하여 사용자를 관리하는 경우 이 서비스를 설정해야 합니다.
성능 및 모니터링 서비스	
Cisco 서비스 가용성 리포터	이 서비스는 게시자 노드에서만 켜십시오. 참고 이 서비스는 다른 노드에서 서비스를 설정한 경우에만 게시자 노드에 대한 보고서를 생성합니다.
IM and Presence Service	
Cisco SIP Proxy	클러스터의 모든 노드에서 이 서비스를 설정합니다.
Cisco Presence 엔진	클러스터의 모든 노드에서 이 서비스를 설정합니다.
Cisco Sync Agent	클러스터의 모든 노드에서 이 서비스를 설정합니다.

서비스/서블릿	권장 사항
Cisco XCP 텍스트 전화회의 관리자	• IM and Presence에 준수 기능을 배포하는 경우 이 서비스를 설정합니다. • 채팅 기능을 실행하는 각 노드에서 이 서비스를 설정합니다. 참고 영구 채팅 기능을 사용하려면 외부 데이터베이스가 필요합니다. 영구 채팅 기능을 활성화한 경우에는 텍스트 전화회의 관리자 서비스를 시작하기 전에 외부 데이터베이스를 구성해야 합니다. 영구 채팅 기능이 활성화되고 외부 데이터베이스가 구성되지 않은 경우에는 텍스트 전화회의 관리자 서비스가 시작되지 않습니다. *IM and Presence* 데이터베이스 설정 설명서*Unified Communications Manager*를 참조하십시오.
Cisco XCP Web 연결 관리자	• IM and Presence와 웹 클라이언트를 통합하는 경우 이 서비스를 설정합니다. • 클러스터의 모든 노드에서 이 서비스를 설정합니다.
Cisco XCP 연결 관리자	• XMPP 클라이언트를 IM and Presence와 통합하는 경우 이 서비스를 설정합니다. • 클러스터의 모든 노드에서 이 서비스를 설정합니다.
Cisco XCP SIP 페더레이션 연결 관리자	다음 구성 중 하나를 배포하는 경우 이 서비스를 설정합니다. • IM and Presence에서 SIP 프로토콜을 통한 도메인간 페더레이션. SIP 페더레이션을 실행하는 각 노드에서 이 서비스를 설정합니다. • IM and Presence 릴리스 9.x 클러스터와 Cisco Unified Presence 릴리스 8.6(x) 클러스터 간의 클러스터 간 배포. 릴리스 9.x 클러스터의 모든 노드에서 이 서비스를 설정합니다.

서비스/서블릿	권장 사항
Cisco XCP XMPP 페더레이션 연결 관리자	• IM and Presence에서 XMPP 프로토콜을 통해 도메인 간 페더레이션을 배포하는 경우에만 이 서비스를 설정합니다. • XMPP 페더레이션을 실행하는 각 노드에서 이 서비스를 설정합니다. 참고 노드에서 XMPP 페더레이션 연결 관리자 서비스를 설정하기 전에 해당 노드의 Cisco Unified Communications Manager IM and Presence 관리에서 XMPP 페더레이션을 켜야 합니다. *IM and Presence*를 위한 도메인 간 페더레이션*Unified Communications Manager*을 참조하십시오.
Cisco XCP 메시지 아카이버	• IM and Presence에 준수 기능을 배포하는 경우 이 서비스를 설정합니다. • IM 준수 기능을 실행하는 모든 노드에서 이 서비스를 설정합니다. 참고 외부 데이터베이스를 구성하기 전에 메시지 아카이버를 설정하면 서비스가 시작되지 않습니다. 외부 데이터베이스에 연결할 수 없는 경우에도 서비스가 시작되지 않습니다. *IM and Presence*데이터베이스 설정 설명서*Unified Communications Manager*를 참조하십시오.
Cisco XCP 디렉터리 서비스	• XMPP 클라이언트를 LDAP 디렉터리와 함께 IM and Presence와 통합하는 경우 이 서비스를 설정합니다. • 클러스터의 모든 노드에서 이 서비스를 설정합니다. 참고 타사 XMPP 클라이언트에 대한 LDAP 연락처 검색 설정을 구성하기 전에 디렉터리 서비스를 설정한 경우 서비스가 시작된 후 다시 중지됩니다. *Unified Communications Manager*의 *IM and Presence Service* 구성 및 관리를 참조하십시오.

서비스/서블릿	권장 사항
Cisco XCP 인증 서비스	• XMPP 클라이언트를 IM and Presence와 통합하는 경우 이 서비스를 설정합니다. • 클러스터의 모든 노드에서 이 서비스를 설정합니다.

기능 서비스 활성화

서비스 가용성 GUI의 서비스 활성화 창에서 기능 서비스를 활성화 및 비활성화합니다. 서비스 활성화 창에 표시되는 서비스는 사용자가 활성화할 때까지 시작되지 않습니다.

기능 서비스(네트워크 서비스 아님)만 활성화 및 비활성화할 수 있습니다. 동시에 원하는 수 만큼 서비스를 활성화하거나 비활성화할 수 있습니다. 일부 기능 서비스는 다른 서비스에 의존하며, 기능 서비스를 활성화하기 전에 종속 서비스가 활성화됩니다.

팁 Unified Communications Manager 및 IM and Presence Service만 해당: 서비스 활성화 창에서 서비스를 활성화하기 전에 클러스터 서비스 활성화 권장 사항과 관련된 항목을 검토하십시오.

프로시저

단계 **1** 도구 > 서비스 활성화를 선택합니다.

서비스 활성화 창이 표시됩니다.

단계 **2** 서버 드롭다운 목록에서 서버(노드)를 선택한 다음 이동을 클릭합니다.

IM and Presence Service 노드에서 Unified Communications Manager 서비스에 액세스할 수 있으며 그 반대의 경우도 마찬가지입니다. 원격 노드에 액세스하려고 할 때 다음과 같은 오류가 발생할 수 있습니다. "서버에 연결을 설정할 수 없습니다(원격 노드에 연결할 수 없음)". 이 오류 메시지가 나타나는 경우 *Cisco Unified Communications Manager* 관리 설명서를 참조하십시오.

단계 **3** 다음 작업 중 하나를 수행하여 서비스를 설정하거나 해제합니다.

a) 단일 서버에서 실행하는 데 필요한 기본 서비스를 설정하려면 기본값으로 설정을 선택합니다.

참고 이 옵션은 단일 서버의 구성에 기반을 둔 기본 서비스를 선택하고 서비스 종속성을 확인합니다.

b) 모든 서비스를 설정하려면 모든 서비스 확인을 선택합니다.
c) 특정 서비스를 설정하려면 설정할 서비스에 대한 확인란을 선택합니다.
d) 서비스를 해제하려면 해제할 서비스에 대한 확인란을 선택 취소합니다.

단계 **4** Unified Communications Manager 및 IM and Presence Service에만 해당: 클러스터 구성의 경우 클러스터 서비스 활성화 권장 사항을 검토한 다음 활성화할 서비스 옆의 확인란을 선택합니다.

단계 5 활성화할 서비스에 대한 확인란을 선택하고 저장을 클릭합니다.

팁 활성화한 서비스를 비활성화하려면 비활성화할 서비스 옆에 있는 확인란의 선택을 취소한 다음 저장을 클릭합니다.

팁 서비스의 최신 상태를 얻으려면 새로 고침 버튼을 클릭합니다.

관련 항목

Cisco Unified Communications Manager에 대한 클러스터 서비스 활성화 권장 사항, 218 페이지
IM and Presence Service에 대한 클러스터 서비스 활성화 권장 사항, 222 페이지

제어 센터 또는 CLI에서 서비스 시작, 중지 및 재시작

이러한 작업을 수행하기 위해 서비스 가용성 GUI는 두 개의 제어 센터 창을 제공합니다. 네트워크 서비스를 시작, 중지 및 다시 시작 하려면 제어 센터 - 네트워크 서비스 창에 액세스합니다. 기능 서비스를 시작, 중지 및 다시 시작하려면 제어 센터 - 기능 서비스 창에 액세스합니다.

팁 관련 링크목록 상자와 이동 버튼을 사용하여 제어 센터 및 서비스 활성화 창으로 이동합니다.

제어 센터에서 서비스 시작, 중지 및 재시작

서비스 가용성 GUI의 제어 센터를 사용하여 다음 작업을 수행할 수 있습니다.

- 상태 보기
- 상태 새로고침
- 특정 서버 또는 클러스터 구성에서 클러스터의 서버에 대한 기능 및 네트워크 서비스 시작, 중지 및 다시 시작

서비스가 중지 중이면 서비스가 중지될 때까지 서비스를 시작할 수 없습니다.

주의 Unified Communications Manager만 해당: 서비스를 중지하면 서비스에서 제어하는 모든 장치에 대한 통화 처리도 중지됩니다. 서비스가 중지되면 IP 전화기에서 다른 IP 전화기로의 통화는 연결된 상태로 유지 됩니다. IP 전화기에서 MGCP(Media Gateway Control Protocol) 게이트웨이로 진행 중인 통화도 연결된 상태로 유지되지만 다른 유형의 통화는 삭제됩니다.

프로시저

단계 1 시작/중지/다시 시작/새로 고침하는 서비스 유형에 따라 다음 작업 중 하나를 수행합니다.

- 도구 > 제어 센터 - 기능 서비스를 선택합니다.

  팁 기능 서비스를 시작, 중지 또는 다시 시작하려면 먼저 해당 서비스를 활성화해야 합니다.

- 도구제어 센터 > - 네트워크 서비스를 선택합니다.

단계 **2** 서버 드롭다운 목록에서 서버를 선택한 다음 이동을 클릭합니다.

창에 다음 항목이 표시됩니다.

- 선택한 서버에 대한 서비스 이름입니다.
- 서비스 그룹.
- 서비스 상태(예: 시작됨, 실행 중, 실행 중이 아님)입니다. (상태 열).
- 서비스가 실행을 시작한 정확한 시간입니다. (시작 시간 열).
- 서비스가 실행된 시간입니다. (실행 시간 열).

단계 **3** 다음 작업 중 하나를 수행합니다.

- 시작할 서비스 옆의 라디오 버튼을 클릭하고 시작을 클릭합니다. 상태가 변경되어 업데이트된 상태가 반영됩니다.
- 중지할 서비스 옆에 있는 라디오 버튼을 클릭한 다음 중지를 클릭합니다. 상태가 변경되어 업데이트된 상태가 반영됩니다.
- 다시 시작할 서비스 옆의 라디오 버튼을 클릭하고 다시 시작을 클릭합니다. 재시작하는 데 시간이 걸릴 수 있음을 알리는 메시지가 표시됩니다. 확인을 클릭합니다.
- 새로 고침을 클릭하여 서비스의 최신 상태를 가져옵니다.
- 서비스 활성화 창 또는 다른 제어 센터 창으로 이동하려면 관련 링크 드롭다운 목록에서 옵션을 선택하고 이동을 클릭합니다.

명령줄 인터페이스를 사용하여 서비스 시작, 중지 및 재시작

CLI를 통해 일부 서비스를 시작하고 중지할 수 있습니다. CLI를 시작하고 중지할 수 있는 서비스 목록과 이러한 작업을 수행하는 방법에 대한 자세한 내용은 *Cisco* 통합 솔루션에 대한 명령줄 인터페이스 참조 설명서를 참조하십시오.

팁 서비스 가용성 GUI의 제어 센터에서 대부분의 서비스를 시작하고 중지해야 합니다.

16 장

추적

- 추적, 229 페이지
- 추적 구성, 233 페이지

추적

Cisco 통합 서비스 가용성는 사용자의 음성 애플리케이션에 대한 문제 해결에 도움이 되는 추적 도구를 제공합니다. Cisco 통합 서비스 가용성는 SDI(시스템 진단 인터페이스) 추적, SDL(신호 분배 계층) 추적(Unified Communications Manager에만 해당되는 Cisco CallManager 및 Cisco CTIManager 서비스의 경우) 및 Log4J 추적(Java 애플리케이션의 경우)을 지원합니다.

추적 구성 창을 사용하여 추적할 정보의 수준을 지정하고, 각 추적 파일에 포함할 정보 유형을 지정할 수 있습니다.

Unified Communications Manager만 해당: 서비스가 Cisco CallManager 또는 Cisco CTIManager와 같은 통화 처리 애플리케이션인 경우 전화기 및 게이트웨이와 같은 장치에서 추적을 구성할 수 있습니다.

Unified Communications Manager만 해당: 알람 구성 창에서 SDL 추적 로그 파일을 포함하여 다양한 위치에 알람을 지시할 수 있습니다. 이렇게 하려면 Cisco Unified Real-Time Monitoring Tool(Unified RTMT)에서 알림에 대한 추적을 구성할 수 있습니다.

다양한 서비스를 위한 추적 파일에 포함할 정보를 구성한 후 Cisco Unified Real-Time Monitoring Tool의 추적 및 로그 센트럴 옵션을 사용하여 추적 파일을 수집하고 볼 수 있습니다.

Cisco Unified IM and Presence Service 가용성은 인스턴트 메시징 및 프레즌스 애플리케이션과 관련된 문제를 해결하는 데 도움이 되는 추적 도구를 제공합니다. Cisco Unified IM and Presence Service 가용성은 다음을 지원합니다.

- SDI 추적
- Log4J 추적(Java 애플리케이션용)

추적하려는 정보 수준(디버그 수준), 추적할 정보(추적 필드) 및 추적 파일에 대한 정보(서비스 당 파일 수, 파일 크기, 데이터를 추적 파일에 저장한 시간 등)를 구성할 수 있습니다. 단일 서비스에 대한 추적을 구성하거나 해당 서비스에 대한 추적 설정을 클러스터의 모든 서버에 적용할 수 있습니다.

알람 구성 창에서 알람을 다양한 위치로 보낼 수 있습니다. 이렇게 하려면 IM and Presence Unified RTMT에서 알림에 대한 추적을 구성할 수 있습니다.

다양한 서비스를 위한 추적 파일에 포함할 정보를 구성한 후 Unified RTMT의 추적 및 로그 센트럴 옵션을 사용하여 추적 파일을 수집하고 볼 수 있습니다. 클러스터의 모든 IM and Presence 노드에서 사용할 수 있는 모든 기능 또는 네트워크 서비스에 대한 추적 매개 변수를 구성할 수 있습니다. 추적 구성 창을 사용하여 문제 해결을 위해 추적할 매개 변수를 지정할 수 있습니다. 사용자의 추적 필드를 선택하는 대신 미리 정의된 추적 설정 문제 해결을 사용하려면 추적 설정 문제 해결 창을 사용하면 됩니다.

참고 추적을 활성화하면 시스템 성능이 저하됩니다. 따라서 추적은 문제 해결 용도로만 활성화하십시오. 추적 사용법에 대한 지원은 Cisco TAC(Technical Assistance Center)에 문의하십시오.

추적 구성

서비스 가용성 인터페이스에 표시되는 모든 기능 또는 네트워크 서비스에 대한 추적 매개 변수를 구성할 수 있습니다. 클러스터가 있는 경우 클러스터의 모든 서버에서 사용할 수 있는 모든 기능 또는 네트워크 서비스에 대한 추적 매개 변수를 구성할 수 있습니다. 추적 구성 창을 사용하여 문제 해결을 위해 추적할 매개 변수를 지정할 수 있습니다.

추적하려는 정보 수준(디버그 수준), 추적할 정보(추적 필드) 및 추적 파일에 대한 정보(서비스 당 파일 수, 파일 크기, 데이터를 추적 파일에 저장한 시간 등)를 구성할 수 있습니다. 클러스터가 있는 경우 단일 서비스에 대한 추적을 구성하거나 해당 서비스에 대한 추적 설정을 클러스터의 모든 서버에 적용할 수 있습니다.

사용자의 추적 필드를 선택하는 대신 미리 정의된 추적 설정 문제 해결을 사용하려면 문제 해결 추적 창을 사용하면 됩니다. 문제 해결 추적에 대한 자세한 내용은 추적 설정을 참조하십시오.

다양한 서비스를 위한 추적 파일에 포함할 정보를 구성한 후 Unified RTMT의 추적 및 로그 센트럴 옵션을 사용하여 추적 파일을 수집할 수 있습니다. 추적 수집에 대한 자세한 내용은 추적 수집을 참조하십시오.

추적 설정

추적 설정 문제 해결 창에서는 미리 결정된 추적 설정 문제 해결을 지정할 서비스를 선택할 수 있습니다. 이 창에서 단일 서비스 또는 여러 서비스를 선택하고 해당 서비스에 대한 추적 설정을 미리 결정된 추적 설정으로 변경할 수 있습니다. 클러스터가 있는 경우 클러스터의 다른 서버에서 서비스를 선택할 수 있으므로 선택한 서비스의 추적 설정이 미리 정의된 추적 설정으로 변경됩니다. 단일 서버, 서버에 대해 활성화된 모든 서비스, 클러스터의 모든 서버에 대해 활성화된 특정 서비스 또는 클러스터의 모든 서버에 대해 활성화된 모든 서비스에 대해 활성화된 특정 서비스를 선택할 수 있습니다. 창에서 비활성 서비스 옆에 해당 없음이 표시됩니다.

참고 기능이 나 네트워크 서비스에 대한 미리 결정된 추적 설정 문제 해결에는 SDL, SDI 및 Log4j trace 설정이 포함됩니다. 추적 설정 문제 해결이 적용되기 전에 시스템은 원래 추적 설정을 백업합니다. 추적 설정 문제 해결을 재설정하면 원래 추적 설정이 복원됩니다.

서비스에 대한 추적 설정 문제 해결을 적용한 후 추적 설정 문제 해결 창을 열면 문제 해결을 위해 설정한 서비스가 선택됨으로 표시됩니다. 추적 설정 문제 해결 창에서 추적 설정을 원래 설정으로 재설정할 수 있습니다.

서비스에 대한 추적 설정 문제 해결을 적용한 후에는 추적 구성 창에 해당 서비스에 대해 추적 기능이 설정되었다는 메시지가 표시됩니다. 관련 링크 드롭다운 목록 상자에서 서비스에 대한 설정을 재설정하려는 경우 추적 설정 문제 해결 옵션을 선택할 수 있습니다. 지정된 서비스의 경우 추적 출력 설정의 일부 매개 변수(예: 최대 파일 수)를 제외하고 추적 구성 창에 모든 설정이 읽기 전용으로 표시됩니다. 추적 설정 문제 해결을 적용한 후에도 이러한 매개 변수를 수정할 수 있습니다.

추적 수집

Cisco Unified Real-Time Monitoring Tool의 옵션인 추적 및 로그 센트럴을 사용하여 다양한 서비스 추적 또는 기타 로그 파일을 수집하고, 보고, zip할 수 있습니다. 추적 및 로그 센트럴 옵션을 사용하여 SDL/SDI 추적, 애플리케이션 로그, 시스템 로그(예: 이벤트 보기 애플리케이션, 보안 및 시스템 로그) 및 크래시 덤프 파일을 수집할 수 있습니다.

팁 Windows 메모장에 줄 바꿈이 제대로 표시되지 않으므로 수집된 추적 파일을 보려면 수집된 추적 파일을 보는 데 Windows 메모장을 사용하지 마십시오.

참고 Unified Communications Manager만 해당: 암호화를 지원하는 장치의 경우 보안 실시간 전송 프로토콜(SRTP) 키 입력 자료가 추적 파일에 표시되지 않습니다.

추적 수집에 대한 자세한 내용은 *Cisco Unified Real-Time Monitoring Tool* 관리 설명서를 참조하십시오.

착신자 추적

착신자 추적을 사용하면 추적할 디렉토리 번호 또는 디렉토리 번호 목록을 구성할 수 있습니다. 세션 추적 도구를 사용하여 통화에 대한 요구 시 추적을 요청할 수 있습니다.

자세한 내용은 *Cisco Unified Real Time Monitoring Tool* 관리 설명서를 참조하십시오.

추적 구성 설정

다음 절차에서는 서비스 가용성 인터페이스에서 기능 및 네트워크 서비스에 대한 추적을 구성하고 수집하는 단계에 대한 개요를 제공합니다.

프로시저

단계 **1** 다음 단계 중 하나를 수행하여 TLC 조절 CPU 목표 및 TLC 조절 IOWait(Cisco RIS Data Collector 서비스)의 값을 구성합니다.

- Cisco Unified Communications Manager 관리 및 Cisco Unified IM and Presence: 시스템 > **ServiceParameters**를 선택하고 TLC 조절 CPU 목표 및 TLC 조절 설정 IOWait 목표 서비스 매개변수(Cisco RIS Data Collector 서비스)의 값을 구성합니다.
- Cisco Unity Connection에만 해당: Cisco Unity Connection 관리에서시스템 설정 > 서비스 파라미터를 선택하고 TLC 조절 CPU 목표 및 TLC 조절 IOWait 목표 서비스 파라미터(Cisco RIS Data Collector 서비스)의 값을 구성합니다.

단계 **2** 추적을 수집하려는 서비스에 대한 추적 설정을 구성합니다. 클러스터가 있는 경우 클러스터의 한 서버 또는 모든 서버에서 서비스에 대한 추적을 구성할 수 있습니다.

추적 설정을 구성하려면 디버그 수준 및 추적 필드를 선택하여 추적 로그에 포함할 정보를 선택합니다.

서비스에서 미리 결정된 추적을 실행하려면 해당 서비스에 대한 문제 해결 추적을 설정합니다.

단계 **3** 로컬 PC에 Cisco Unified Real-Time Monitoring Tool를 설치합니다.

단계 **4** 모니터링되는 추적 파일에 지정된 검색 문자열이 있을 때 알람을 생성하려면, Unified RTMT에서 LogFileSearchStringFound 알림을 활성화합니다.

LpmTctCatalog에서 LogFileSearchStringFound 알람을 찾을 수 있습니다. (알람 > 정의를 선택합니다. 알람 위치 찾기 드롭다운 목록 상자에서 시스템 알람 카탈로그를 선택합니다. 같음 드롭다운 목록 상자에서 **LpmTctCatalog**를 선택합니다.

단계 **5** CriticalServiceDownand CodeYellow와 같은 알림에 대한 추적을 자동으로 캡처하려면 Unified RTMT의 특정 알림에 대한 알림/속성 설정 대화 상자에서 추적 다운로드 활성화 확인란을 선택하고 다운로드를 수행하는 빈도를 구성합니다.

단계 **6** 추적을 수집합니다.

단계 **7** 적절한 뷰어에서 로그 파일을 봅니다.

단계 **8** 문제 해결 추적을 활성화한 경우, 추적 설정 서비스를 재설정하면 원래 설정이 복원됩니다.

참고 문제 해결 추적을 오랫동안 활성화하면 추적 파일의 크기가 증가하고 서비스의 성능에 영향을 줄 수 있습니다.

추적 구성

이 섹션에서는 추적 설정 구성에 대한 정보를 제공합니다.

참고 추적을 활성화하면 시스템 성능이 저하됩니다. 따라서 추적은 문제 해결 용도로만 활성화하십시오. 추적 사용에 도움이 필요하면 기술 지원 팀에 문의하십시오.

추적 매개 변수 설정

이 섹션에서는 서비스 가용성 GUI를 통해 관리하는 기능 및 네트워크 서비스에 대한 추적 매개 변수를 구성하는 방법에 대해 설명합니다.

팁 Cisco Unity Connection의 경우, Cisco Unity Connection 문제를 해결하려면 Cisco 통합 서비스 가용성 및 Cisco Unity Connection 서비스 가용성에서 추적을 실행해야 할 수 있습니다. Cisco Unity Connection 서비스 가용성에서 추적을 실행하는 방법에 대한 자세한 내용은 *Cisco Unity Connection* 서비스 가용성 관리 설명서를 참조하십시오.

프로시저

단계 **1** 추적 > 구성을 선택합니다.

추적 구성 창이 표시됩니다.

단계 **2** 서버 드롭다운 목록 상자에서 추적을 구성하려는 서비스를 실행 중인 서버를 선택한 다음 이동을 클릭합니다.

단계 **3** 서비스 그룹 드롭다운 목록 상자에서 추적을 구성할 서비스에 대한 서비스 그룹을 선택한 다음 이동을 클릭합니다.

팁 추적 구성 테이블의 서비스 그룹은 서비스 그룹 드롭다운 목록 상자에 표시되는 옵션에 해당하는 서비스 및 추적 라이브러리를 나열합니다.

단계 **4** 서비스 드롭다운 목록 상자에서 추적을 구성하려는 서비스를 선택하고 이동을 클릭합니다.

드롭다운 목록 상자에 활성 및 비활성 서비스가 표시됩니다.

팁 Cisco Unity Connection에만 해당: Cisco CallManager 및 CTIManager 서비스의 경우 SDL 추적 매개 변수를 구성할 수 있습니다. 이렇게 하려면 해당 서비스 중 하나에 대한 추적 구성 창을 열고 관련 링크 드롭다운 목록 상자 옆에 있는 이동 버튼을 클릭합니다.

서비스에 대한 추적 문제 해결을 구성한 경우 창 상단에 문제 해결 추적 기능이 설정 되었음을 나타내는 메시지가 표시됩니다. 즉, 시스템에서 추적 출력 설정을 제외하고 추적 구성 창의 모든 필드를

비활성화함을 의미합니다. 추적 출력 설정을 구성하려면 11단계로 이동합니다. 문제 해결 추적을 재설정하려면 문제 해결 추적 설정 설정을 참조하십시오.

선택한 서비스에 대한 추적 매개 변수가 표시됩니다. 또한 모든 노드에 적용 확인란이 표시됩니다(Unified Communications Manager에만 해당).

단계 **5** Unified Communications Manager 및 IM and Presence만 해당: 이렇게 하려면 모든 노드에 적용 확인란을 선택하여 서비스 또는 추적 라이브러리에 대한 추적 설정을 클러스터의 모든 서버에 적용할 수 있습니다. 즉, 구성에서 클러스터를 지원하는 경우입니다.

단계 **6** 추적 사용 확인란을 선택합니다.

단계 **7** Cisco Unity Connection에만 해당: SDL 추적 매개 변수를 구성하는 경우 10단계로 이동합니다.

단계 **8** 디버그 추적 수준 설정에 설명된 대로 디버그 추적 수준 목록 상자에서 추적할 정보 수준을 선택합니다.

단계 **9** 선택한 서비스에 대한 추적 필드 확인란을 선택합니다(예: Cisco Log Partition Monitoring Tool 추적 필드).

단계 **10** 활성화할 추적을 지정할 수 있는 여러 추적 설정이 서비스에 없는 경우 모든 추적 활성화 확인란을 선택합니다. 선택한 서비스에 여러 개의 추적 설정이 있는 경우에는 추적 필드 설명에 설명된 대로 활성화할 추적 확인란 옆에 있는 확인란을 선택합니다.

단계 **11** 추적 파일의 수와 크기를 제한하려면 추적 출력 설정을 지정합니다. 설명은 추적 출력 설정을 참조하십시오.

단계 **12** 추적 매개 변수 구성을 저장하려면 저장 버튼을 클릭합니다.

추적 구성에 대한 변경 사항은 Cisco Messaging Interface를 제외한 모든 서비스에 즉시 적용됩니다(Unified Communications Manager에만 해당). Cisco Messaging Interface에 대한 추적 구성 변경 사항은 3 ~ 5분 후에 적용됩니다.

참고 기본값을 설정하려면 기본값 설정 버튼을 클릭합니다.

추적 구성의 서비스 그룹

다음 표에서는 추적 구성 창의 서비스 그룹 드롭다운 목록 상자에 있는 옵션에 해당하는 서비스 및 추적 라이브러리를 보여줍니다.

표 ***36:*** 추적 구성의 서비스 그룹

서비스 그룹	서비스 및 추적 라이브러리	참고
Unified Communications Manager CM 서비스	• Cisco CTIManager • Cisco CallManager • Cisco CallManager Cisco IP 전화기 서비스 • Cisco DHCP 모니터 서비스 • Cisco Dialed Number Analyzer • Cisco Dialed Number Analyzer 서버 • Cisco 확장 기능, Cisco Extension Mobility • Cisco Extension Mobility Application • Cisco IP Voice Media Streaming App • Cisco Messaging Interface • Cisco TFTP • Cisco Unified Mobile Voice Access Service	CM 서비스 그룹에 있는 대부분의 서비스의 경우 서비스에 대한 모든 추적을 활성화하는 대신 특정 구성 요소에 대한 추적을 실행합니다. 추적 필드 설명에는 특정 구성 요소에 대해 추적을 실행할 수 있는 서비스 목록이 표시됩니다.
Unified Communications Manager CTI 서비스	• Cisco IP Manager Assistant • Cisco Web Dialer 웹 서비스	이러한 서비스의 경우 서비스에 대한 모든 추적을 활성화하는 대신 특정 구성 요소에 대해 추적을 실행할 수 있습니다. 추적 필드 설명을 참조하십시오.

서비스 그룹	서비스 및 추적 라이브러리	참고
Unified Communications Manager CDR 서비스	• Cisco Unified Communications Manager CDR Analysis 및 보고 일정 • Cisco Unified Communications Manager CDR Analysis 및 보고 웹 서비스 • Cisco CDR Agent • Cisco CDR Repository Manager	특정 구성 요소에 대해 추적을 실행하는 대신 각 서비스에 대해 모든 추적을 활성화합니다. Cisco Unified Communications Manager CDR 분석 및 보고에서 저장 프로시저를 호출하는 보고서를 실행하는 경우 Cisco Unified Communications Manager CDR analysis and reporting은 저장 프로시저 로깅이 시작되기 전에 추적 구성 창에서 Cisco Unified Communications Manager CDR 분석 및 보고 스케줄러 서비스와 Cisco Unified Communications Manager CDR 분석 및 보고 웹 서비스에 대해 구성된 디버그 추적 수준을 확인합니다. 미리 작성된 보고서의 경우 Cisco Unified Communications Manager CDR Analysis and Reporting은 Cisco Unified Communications Manager CDR Analysis and Reporting Scheduler 서비스의 수준을 확인합니다. 온디맨드 보고서의 경우 Cisco Unified Communications Manager CDR Analysis and Reporting은 Cisco Unified Communications Manager CDR Analysis and Reporting Web Service의 수준을 확인합니다. 디버그 추적 수준 드롭다운 목록 상자에서 디버그를 선택하면 저장 프로시저 로깅이 활성화되고 드롭다운 목록 상자에서 다른 옵션을 선택할 때까지 계속됩니다. Cisco Unified Communications Manager CDR 분석 및 보고 보고서는 게이트웨이 사용률 보고서, 경로 및 회선 그룹 이용률 보고서, 경로/헌트 목록 사용률 보고서, 경로 패턴/헌트 파일럿 활용 보고서, 전화회의 통화 세부 정보 보고서, 전화회의 통화 요약 보고서, 전화회의 브리지 사용률 보고서, 음성 메시징 활용 보고서 및 CDR 검색 보고서 등의 저장 프로시저 로깅을 사용합니다.

서비스 그룹	서비스 및 추적 라이브러리	참고
IM and Presence Services	• Cisco 클라이언트 프로파일 에이전트 • Cisco 구성 에이전트 • Cisco 클러스터 간 동기화 에이전트 • Cisco 로그인 데이터 저장소 • Cisco OAM 에이전트 • Cisco Presence 데이터 저장소 • Cisco Presence 엔진 • Cisco IM and Presence 데이터 모니터 • Cisco 라우트 데이터 저장소 • Cisco SIP Proxy • Cisco SIP 등록 데이터 저장소 • Cisco 서버 복구 관리자 • Cisco Sync Agent • Cisco XCP 인증 서비스 • Cisco XCP 구성 관리자 • Cisco XCP 연결 관리자 • Cisco XCP 디렉터리 서비스 • Cisco XCP 메시지 아카이버 • Cisco XCP 라우터 • Cisco XCP SIP 페더레이션 연결 관리자 • Cisco XCP 텍스트 전화회의 관리자 • Cisco XCP Web 연결 관리자 • Cisco XCP XMPP 페더레이션 연결 관리자	이러한 서비스에 대한 설명은 Cisco Unified IM and Presence Service 가용성의 기능 및 네트워크 서비스와 관련된 항목을 참조하십시오. • 이러한 서비스의 경우 특정 구성 요소에 대해 추적을 실행하는 대신 서비스에 대한 모든 추적을 활성화해야 합니다.

서비스 그룹	서비스 및 추적 라이브러리	참고
데이터베이스 및 관리 서비스	Unified Communications Manager 및 Cisco Unity Connection: • Cisco AXL 웹 서비스 • Cisco CCM DBL Web Library • Cisco CCMAdmin Web Service • Cisco CCMUser Web Service • Cisco Database Layer Monitor • Cisco UXL Web Service Unified Communications Manager • Cisco Bulk Provisioning Service • Cisco GRT Communications 웹 서비스 • Cisco Role-based Security • Cisco TAPS 서비스 • Cisco Unified Reporting 웹 서비스 IM and Presence Service: • Cisco AXL 웹 서비스 • Cisco Bulk Provisioning Service • Cisco CCMUser Web Service • Cisco Database Layer Monitor • Cisco GRT Communications 웹 서비스 • Cisco IM and Presence 관리 • Cisco Unified Reporting 웹 서비스 • 플랫폼 관리 웹 서비스	Cisco CCM DBL 웹 라이브러리 옵션을 선택하면 Java 애플리케이션용 데이터베이스 액세스에 대한 추적이 활성화됩니다. C++ 애플리케이션용 데이터베이스 액세스의 경우 Cisco Extended Functions 추적 필드에 설명된 대로 Cisco Database Layer Monitor에 대한 추적을 활성화합니다. Unified Communications Manager를 지원하는 Cisco 역할 기반 보안 옵션을 선택하면 사용자 역할 인증에 대한 추적이 활성화됩니다. 데이터베이스 및 관리 서비스 그룹에 있는 대부분의 서비스의 경우 특정 구성 요소에 대한 추적을 활성화하는 대신 서비스/라이브러리에 대한 모든 추적을 활성화합니다. Cisco Database Layer Monitor의 경우 특정 구성 요소에 대해 추적을 실행할 수 있습니다. 참고 Cisco Unified IM and Presence 서비스 가용성 UI에서 서비스에 대한 로깅을 제어할 수 있습니다. 로그 수준을 변경하려면 시스템 서비스 그룹 및 Cisco CCMService 웹 서비스를 선택합니다.

서비스 그룹	서비스 및 추적 라이브러리	참고
성능 및 모니터링 서비스	Unified Communications Manager 및 Cisco Unity Connection: • Cisco AMC Service • Cisco CCM NCS Web Library • CCM PD Web Service • Cisco CallManager SNMP Service • Cisco Log Partition Monitoring Tool • Cisco RIS Data Collector • Cisco RTMT Web Service • Cisco Audit Event Service • Cisco RisBean Library Unified Communications Manager: • Cisco CCM PD Web Service IM and Presence Service: • Cisco AMC Service • Cisco Audit Event Service • Cisco Log Partition Monitoring Tool • Cisco RIS Data Collector • Cisco RTMT Web Service • Cisco RisBean Library	Cisco CCM NCS 웹 라이브러리 옵션을 선택하면 Java 클라이언트용 데이터베이스 변경 알림에 대한 추적이 활성화됩니다. Cisco Unity RTMT 웹 서비스 옵션을 선택하면 Unity RTMT 서블릿을에 대한 추적이 활성화됩니다. 이 추적을 실행하면 Unity RTMT 클라이언트 쿼리에 대한 서버측 로그가 생성됩니다.
Unified Communications Manager 보안 서비스	• Cisco CTL Provider • Cisco Certificate Authority Proxy Function • Cisco 신뢰 확인 서비스	특정 구성 요소에 대해 추적을 실행하는 대신 각 서비스에 대해 모든 추적을 활성화합니다.
Unified Communications Manager 디렉터리 서비스	Cisco DirSync	특정 구성 요소에 대해 추적을 실행하는 대신 이 서비스에 대한 모든 추적을 활성화합니다.
백업 및 복원 서비스	• Cisco DRF Local • Unified Communications Manager 및 Cisco Unity Connection만 해당: Cisco DRF Master	특정 구성 요소에 대해 추적을 실행하는 대신 각 서비스에 대해 모든 추적을 활성화합니다.

서비스 그룹	서비스 및 추적 라이브러리	참고
시스템 서비스	Unified Communications Manager: • Cisco CCMRealm Web Service • Cisco CCMService Web Service • Cisco Common User Interface • Cisco Trace Collection Service IM and Presence Service: • Cisco CCMService Web Service • Cisco Trace Collection Service	Cisco CCMRealm Web Service 옵션을 선택하면 로그인 인증에 대한 추적이 활성화됩니다. Cisco Common User Interface 옵션을 선택하면 Cisco 통합 운영 체제 관리 및 Cisco 통합 서비스 가용성 같이 여러 애플리케이션에서 사용하는 공통 코드에 대한 추적이 활성화됩니다. Cisco CCMService Web Service 옵션을 선택하면 Cisco 통합 서비스 가용성 웹 애플리케이션(GUI)에 대한 추적이 활성화됩니다. 특정 구성 요소에 대해 추적을 실행하는 대신 각 옵션/서비스에 대한 모든 추적을 활성화합니다.
SOAP 서비스	• Cisco SOAP 웹 서비스 • Cisco SOAP 메시지 서비스	Cisco SOAP 웹 서비스 옵션을 선택하면 AXL 서비스 가용성 API에 대한 추적이 활성화됩니다. 특정 구성 요소에 대해 추적을 실행하는 대신 이 서비스에 대한 모든 추적을 활성화합니다.
플랫폼 서비스	Cisco Unified OS Admin Web Service	Cisco Unified OS Admin Web Service는 인증서 관리, 버전 설정 및 설치와 업그레이드 같은 플랫폼 관련 기능을 관리할 수 있는 웹 애플리케이션에 해당하는 Cisco Unified 운영 체제 관리를 지원합니다. 특정 구성 요소에 대해 추적을 실행하는 대신 이 서비스에 대한 모든 추적을 활성화합니다.

디버그 추적 수준 설정

다음 표에서는 서비스에 대한 디버그 추적 수준 설정에 대해 설명합니다.

표 ***37:*** 서비스에 대한 디버그 추적 수준

수준	설명
오류	알람 조건 및 이벤트를 추적합니다. 비정상 라우트에서 생성된 모든 추적에 사용됩니다. 최소 수의 CPU 주기를 사용합니다.
특수	모든 오류 상태와 프로세스 및 장치 초기화 메시지를 추적합니다.

수준	설명
상태 변환	모든 특수 조건과 정상 작업 중에 발생하는 하위 시스템 상태 전환을 추적합니다. 통화 처리 이벤트를 추적합니다.
중요	모든 상태 전환 조건과 정상 작업 중에 발생하는 미디어 레이어 이벤트를 추적합니다.
시작/종료	참고 모든 서비스에서 이 추적 수준을 사용하지는 않습니다. 루틴의 중요한 모든 조건과 시작 및 종료 지점을 추적합니다.
Arbitrary	모든 시작/종료 조건과 하위 수준 디버깅 정보를 추적합니다.
자세히	모든 임의 조건과 자세한 디버깅 정보를 추적합니다.

다음 표에서는 서블릿에 대한 디버그 추적 수준 설정에 대해 설명합니다.

표 ***38:*** 서블릿에 대한 디버그 추적 수준

수준	설명
치명적	애플리케이션을 중단할 수 있는 매우 심각한 오류 이벤트를 추적합니다.
오류	알람 조건 및 이벤트를 추적합니다. 비정상 라우트에서 생성된 모든 추적에 사용됩니다.
알림	잠재적으로 유해한 상황을 추적합니다.
정보	다수의 서블릿 문제를 추적하고 시스템 성능에 최소한의 영향을 미칩니다.
디버그	모든 상태 전환 조건과 정상 작업 중에 발생하는 미디어 레이어 이벤트를 추적합니다. 모든 로깅을 설정하는 추적 수준입니다.

추적 필드 설명

일부 서비스의 경우 서비스에 대한 모든 추적을 활성화하는 대신 특정 구성 요소에 대한 추적을 활성화할 수 있습니다. 다음 목록에는 특정 구성 요소에 대한 추적을 활성화할 수 있는 서비스가 포함되어 있습니다. 상호 참조 중 하나를 클릭하면 서비스의 각 추적 필드에 대한 설명이 표시되는 해당 섹션으로 이동합니다. 서비스가 다음 목록에 없으면 추적 구성 창에서 서비스에 대한 모든 추적 활성화 확인란이 표시됩니다.

다음 서비스는 Unified Communications Manager 및 Cisco Unity Connection에 적용됩니다.

- Database Layer Monitor 추적 필드
- Cisco RIS Data Collector 추적 필드

다음 서비스는 Unified Communications Manager에 적용됩니다.

- Cisco CallManager SDI 추적 필드
- Cisco CallManager SDL 추적 필드
- Cisco CTIManager SDL 추적 필드
- Cisco Extended Functions 추적 필드
- Cisco Extension Mobility 추적 필드
- Cisco IP Manager Assistant 추적 필드
- Cisco IP Voice Media Streaming App 추적 필드
- Cisco TFTP 추적 필드
- Cisco Web Dialer 웹 서비스 추적 필드

Database Layer Monitor 추적 필드

다음 표에서는 Cisco Database Layer Monitor 추적 필드에 대해 설명합니다. Cisco Database Layer Monitor 서비스는 Unified Communications Manager 및 Cisco Unity Connection을 지원합니다.

표 ***39: Cisco Database Layer Monitor*** 추적 필드

필드 이름	설명
DB 라이브러리 추적 활성화	C++ 애플리케이션에 대한 데이터베이스 라이브러리 추적을 활성화합니다.
서비스 추적 활성화	서비스 추적을 활성화합니다.
DB 변경 알림 추적 활성화	C++ 애플리케이션에 대한 데이터베이스 변경 알림 추적을 활성화합니다.
단위 테스트 추적 활성화	이 확인란을 선택하지 마십시오. Cisco 기술팀은 디버깅 목적으로 이를 사용합니다.

Cisco RIS Data Collector 추적 필드

다음 표에서는 Cisco RIS Data Collector 추적 필드에 대해 설명합니다. Cisco RIS Data Collector 서비스는 Unified Communications Manager 및 Cisco Unity Connection을 지원합니다.

표 *40: Cisco RIS Data Collector* 추적 필드

필드 이름	설명
RISDC 추적 활성화	RIS Data Collector 서비스의 RISDC 스레드에 대한 추적을 활성화합니다.
시스템 액세스 추적 활성화	RIS Data Collector에서 시스템 액세스 라이브러리에 대한 추적을 활성화합니다.
링크 서비스 추적 활성화	RIS Data Collector에서 링크 서비스 라이브러리에 대한 추적을 활성화합니다.
RISDC 액세스 추적 활성화	RIS Data Collector에서 RISDC 액세스 라이브러리에 대한 추적을 활성화합니다.
RISDB 추적 활성화	RIS Data Collector에서 RISDB 라이브러리에 대한 추적을 활성화합니다.
PI 추적 활성화	RIS Data Collector에서 PI 라이브러리에 대한 추적을 활성화합니다.
XML 추적 활성화	RIS Data Collector 서비스의 입/출력 XML 메시지에 대한 추적을 활성화합니다.
Perfmon 로거 추적 활성화	RIS Data Collector의 문제 해결 perfmon 데이터 로깅에 대한 추적을 활성화합니다. 로그 파일의 이름, 로그에 기록된 총 카운터 수, 애플리케이션의 이름, 시스템 카운터와 인스턴스, 프로세스 및 스레드 CPU 비율 계산 및 로그 파일 롤오버와 삭제 발생을 추적하는 데 사용됩니다.

Cisco CallManager SDI 추적 필드

다음 표에서는 Cisco CallManager SDI 추적 필드에 대해 설명합니다. Cisco CallManager 서비스는 Unified Communications Manager를 지원합니다.

표 *41: Cisco CallManager SDI* 추적 필드

필드 이름	설명
H245 메시지 추적 활성화	H245 메시지 추적을 활성화합니다.
DT-24+/DE-30+ 추적 활성화	DT-24+/DE-30+ 장치 추적의 ISDN 유형 로깅을 활성화합니다.
PRI 추적 활성화	PRI(Primary Rate Interface) 장치의 추적을 활성화합니다.

필드 이름	설명
ISDN 변환 추적 활성화	ISDN 메시지 추적을 활성화합니다. 일반 디버깅에 사용됩니다.
H225 및 게이트키퍼 추적 활성화	H.225 장치의 추적을 활성화합니다. 일반 디버깅에 사용됩니다.
기타 추적 활성화	기타 장치 추적을 활성화합니다. 참고 정상적인 시스템 작동 중에는 이 확인란을 선택하지 마십시오.
전화회의 브리지 추적 활성화	전화회의 브리지 추적을 활성화합니다. 일반 디버깅에 사용됩니다.
대기 중 음악 추적 활성화	MOH(대기 중 음악) 장치 추적을 활성화합니다. Unified Communications Manager에 등록, Unified Communications Manager에서 등록 취소, 리소스 할당이 성공적으로 처리 또는 실패 같은 MOH 장치 상태를 추적하는 데 사용됩니다.
Unified CM 실시간 정보 서버 추적 활성화	실시간 정보 서버에서 사용하는 Unified Communications Manager 실시간 정보 추적을 활성화합니다.
SIP 스택 추적 활성화	SIP 스택 추적을 활성화합니다. 기본값은 enabled입니다.
알림 장치 추적 활성화	Cisco IP Voice Media Streaming Application 서비스를 사용하는 알림 장치인 SCCP 장치에 대한 추적을 활성화하여 Unified Communications Manager가 미리 녹음된 알림(.wav 파일)과 신호음을 Cisco Unified IP 전화기, 게이트웨이 및 기타 구성 가능한 장치에 재생할 수 있습니다.
CDR 추적 활성화	CDR에 대한 추적을 활성화합니다.
아날로그 트렁크 추적 활성화	모든 아날로그 트렁크(AT) 게이트웨이의 추적을 활성화합니다.
모든 전화기 장치 추적 활성화	전화기 장치 추적을 활성화합니다. 추적 정보에는 소프트폰 장치가 포함됩니다. 일반 디버깅에 사용됩니다.
MTP 추적 활성화	MTP(미디어 종료 지점) 장치의 추적을 활성화합니다. 일반 디버깅에 사용됩니다.

필드 이름	설명
모든 게이트웨이 추적 활성화	모든 아날로그 및 디지털 게이트웨이의 추적을 활성화합니다.
착신 전환 및 기타 추적 활성화	통화 착신 전환 및 다른 확인란이 적용되지 않는 모든 하위 시스템에 대한 추적을 활성화합니다. 일반 디버깅에 사용됩니다.
MGCP 추적 활성화	MGCP(Media Gateway Control Protocol) 장치에 대한 추적을 활성화합니다. 일반 디버깅에 사용됩니다.
미디어 리소스 관리자 추적 활성화	MRM(미디어 리소스 관리자) 활동에 대한 추적을 활성화합니다.
SIP 통화 처리 추적 활성화	SIP 통화 처리에 대한 추적을 활성화합니다.
SCCP 연결 유지 추적 활성화	Cisco CallManager 추적에서 SCCP 연결 유지 추적 정보에 대한 추적을 활성화합니다. 각 SCCP 장치는 30초 간격으로 연결 유지 메시지를 보고하고, 각 연결 유지 메시지는 3개의 추적 데이터 행을 생성하므로 이 확인란을 선택하면 시스템에서 많은 양의 추적 데이터를 생성합니다.
SIP 연결 유지(등록 새로 고침) 추적 활성화	Cisco CallManager 추적에서 SIP 연결 유지(등록 새로 고침) 추적 정보에 대한 추적을 활성화합니다. 각 SIP 장치는 2분 간격으로 연결 유지 메시지를 보고하며, 각 연결 유지 메시지는 여러 개의 추적 데이터 행을 생성할 수 있으므로 이 확인란을 선택하면 시스템에서 많은 양의 추적 데이터를 생성합니다.

Cisco CallManager SDL 추적 필드

다음 표에서는 Cisco CallManager SDL 추적 필터 설정에 대해 설명합니다. Cisco CallManager 서비스는 Unified Communications Manager를 지원합니다.

참고 Cisco 엔지니어가 다른 방법으로 사용자에게 지시하지 않는 한 기본값을 사용하는 것이 좋습니다.

표 ***42: Cisco CallManager SDL*** 구성 추적 필터 설정

설정 이름	설명
모든 레이어 1 추적을 활성화합니다.	계층 1에 대한 추적을 활성화합니다.

설정 이름	설명
세부 레이어 1 추적을 활성화합니다.	세부 레이어 1 추적을 활성화합니다.
모든 레이어 2 추적을 활성화합니다.	레이어 2에 대한 추적을 활성화합니다.
레이어 2 인터페이스 추적을 활성화합니다.	레이어 2 인터페이스 추적을 활성화합니다.
레이어 2 TCP 추적을 활성화합니다.	레이어 2 TCP(전송 제어 프로그램) 추적을 활성화합니다.
세부 덤프 레이어 2 추적을 활성화합니다.	덤프 레이어 2에 대한 세부 추적을 활성화합니다.
모든 레이어 3 추적을 활성화합니다.	레이어 3에 대한 추적을 활성화합니다.
모든 통화 제어 추적을 활성화합니다.	통화 제어에 대한 추적을 활성화합니다.
기타 폴링 추적을 활성화합니다.	기타 폴링에 대한 추적을 활성화합니다.
기타 추적(데이터베이스 신호)을 활성화합니다.	데이터베이스 신호와 같은 기타 추적을 활성화합니다.
메시지 변환 신호 추적을 활성화합니다.	메시지 변환 신호에 대한 추적을 활성화합니다.
UUIE 출력 추적을 활성화합니다.	사용자와 사용자 간 정보 요소(UUIE) 출력에 대한 추적을 활성화합니다.
게이트웨이 신호 추적을 활성화합니다.	게이트웨이 신호에 대한 추적을 활성화합니다.
CTI 추적을 활성화합니다.	CTI 추적을 활성화합니다.
네트워크 서비스 데이터 추적 활성화	네트워크 서비스 데이터 추적을 활성화합니다.
네트워크 서비스 이벤트 추적 활성화	네트워크 서비스 이벤트 추적을 활성화합니다.
ICCP 관리 추적 활성화	ICCP 관리 추적을 활성화합니다.
기본 추적 활성화	기본 추적을 활성화합니다.

다음 표에서는 Cisco CallManager SDL 구성 특성에 대해 설명합니다.

표 ***43: Cisco CallManager SDL*** 구성 추적 특성

특징	설명
SDL 링크 상태 추적을 활성화합니다.	ICCP(클러스터 간 통신 프로토콜) 링크 상태에 대한 추적을 활성화합니다.
낮은 수준의 SDL 추적을 활성화합니다.	낮은 수준의 SDL 추적을 활성화합니다.
SDL 링크 폴링 추적을 활성화합니다.	ICCP 링크 폴링에 대한 추적을 활성화합니다.

특징	설명
SDL 링크 메시지 추적을 활성화합니다.	ICCP 원시 메시지에 대한 추적을 활성화합니다.
신호 데이터 덤프 추적을 활성화합니다.	신호 데이터 덤프에 대한 추적을 활성화합니다.
상관 관계 태그 매핑 추적을 활성화합니다.	상관 관계 태그 매핑에 대한 추적을 활성화합니다.
SDL 프로세스 상태 추적을 활성화합니다.	SDL 프로세스 상태에 대한 추적을 활성화합니다.
SDL 추적의 보기 좋은 인쇄를 비활성화합니다.	SDL의 보기 좋은 인쇄에 대한 추적을 비활성화합니다. 보기 좋은 인쇄는 게시 처리를 수행하지 않고 추적 파일에 탭 및 공백을 추가합니다.
SDL TCP 이벤트 추적을 활성화합니다.	SDL TCP 이벤트 추적을 활성화합니다.

Cisco CTIManager SDL 추적 필드

다음 표에서는 Cisco CTIManager SDL 구성 추적 필터 설정에 대해 설명합니다. Cisco CTIManager 서비스는 Unified Communications Manager를 지원합니다.

팁 Cisco 엔지니어가 다른 방법으로 사용자에게 지시하지 않는 한 기본값을 사용하는 것이 좋습니다.

팁 서비스 그룹 드롭다운 목록 상자에서 CTIManager 서비스를 선택하면 이 서비스의 SDI 추적에 대한 추적 구성 창이 표시됩니다. Cisco CTI 매니저 서비스에 대한 SDI 추적을 활성화하려면 Cisco CTIManager 서비스에 대한 추적 구성 창에서 모든 추적 활성화 확인란을 선택합니다. SDL 구성 창에 액세스하려면 관련 링크 드롭다운 목록 상자에서 **SDL** 구성을 선택합니다. Cisco CTIManager SDL 구성 추적 필터 1설정 테이블 및 Cisco CTIManager SDL 구성 추적 특성 표에 설명된 설정이 표시됩니다.

표 ***44: Cisco CTIManager SDL*** 구성 추적 필터 설정

설정 이름	설명
기타 폴링 추적을 활성화합니다.	기타 폴링에 대한 추적을 활성화합니다.
기타 추적(데이터베이스 신호)을 활성화합니다.	데이터베이스 신호와 같은 기타 추적을 활성화합니다.
CTI 추적을 활성화합니다.	CTI 추적을 활성화합니다.
네트워크 서비스 데이터 추적 활성화	네트워크 서비스 데이터 추적을 활성화합니다.
네트워크 서비스 이벤트 추적 활성화	네트워크 서비스 이벤트 추적을 활성화합니다.

설정 이름	설명
ICCP 관리 추적 활성화	ICCP 관리 추적을 활성화합니다.
기본 추적 활성화	기본 추적을 활성화합니다.

다음 표에서는 Cisco CTIManager SDL 구성 추적 특성에 대해 설명합니다.

표 ***45: Cisco CTIManager SDL*** 구성 추적 특성

특징	설명
SDL 링크 상태 추적을 활성화합니다.	ICCP 링크 상태에 대한 추적을 활성화합니다.
낮은 수준의 SDL 추적을 활성화합니다.	낮은 수준의 SDL 추적을 활성화합니다.
SDL 링크 폴링 추적을 활성화합니다.	ICCP 링크 폴링에 대한 추적을 활성화합니다.
SDL 링크 메시지 추적을 활성화합니다.	ICCP 원시 메시지에 대한 추적을 활성화합니다.
신호 데이터 덤프 추적을 활성화합니다.	신호 데이터 덤프에 대한 추적을 활성화합니다.
상관 관계 태그 매핑 추적을 활성화합니다.	상관 관계 태그 매핑에 대한 추적을 활성화합니다.
SDL 프로세스 상태 추적을 활성화합니다.	SDL 프로세스 상태에 대한 추적을 활성화합니다.
SDL 추적의 보기 좋은 인쇄를 비활성화합니다.	SDL의 보기 좋은 인쇄에 대한 추적을 비활성화합니다. 보기 좋은 인쇄는 게시 처리를 수행하지 않고 추적 파일에 탭 및 공백을 추가합니다.
SDL TCP 이벤트 추적 활성화	SDL TCP 이벤트 추적을 활성화합니다.

Cisco Extended Functions 추적 필드

다음 표에서는 Cisco Extended Functions 추적 필드에 대해 설명합니다. Cisco Extended Functions 서비스는 Unified Communications Manager를 지원합니다.

표 ***46: Cisco Extended Functions*** 추적 필드

필드 이름	설명
QBE 도우미 TSP 추적 활성화	전화 통신 서비스 공급자 추적을 활성화합니다.
QBE 도우미 TSPI 추적 활성화	QBE 도우미 TSP 인터페이스 추적을 활성화합니다.
QRT 사전 추적 활성화	품질 보고서 도구 서비스 사전 추적을 활성화합니다.

필드 이름	설명
DOM 도우미 추적 활성화	DOM 도우미 추적을 활성화합니다.
중복 및 변경 알림 추적 활성화	데이터베이스 변경 알림 추적을 활성화합니다.
QRT 보고서 처리기 추적 활성화	품질 보고서 도구 보고서 처리기 추적을 활성화합니다.
QBE 도우미 CTI 추적 활성화	QBE 도우미 CTI 추적을 활성화합니다.
QRT 서비스 추적 활성화	품질 보고서 도구 서비스 관련 추적을 활성화합니다.
QRT DB 추적 활성화	QRT DB 액세스 추적을 활성화합니다.
템플릿 맵 추적 활성화	표준 템플릿 맵과 다중 앱 추적을 활성화합니다.
QRT 이벤트 처리기 추적 활성화	품질 보고서 도구 이벤트 처리기 추적을 활성화합니다.
QRT 실시간 정보 서버 추적 활성화	품질 보고서 도구 실시간 정보 서버 추적을 활성화합니다.

Cisco Extension Mobility 추적 필드

다음 표에서는 Cisco Extension Mobility 추적 필드에 대해 설명합니다. Cisco Extension Mobility 서비스는 Unified Communications Manager를 지원합니다.

표 ***47: Cisco Extension Mobility*** 추적 필드

필드 이름	설명
EM 서비스 추적 활성화	내선 이동 서비스에 대한 추적을 활성화합니다.

팁 Cisco Extension Mobility 애플리케이션 서비스에 대한 추적을 활성화할 때 Cisco Extension Mobility 애플리케이션 서비스에 대한 추적 구성 창에서 모든 추적 활성화 확인란을 선택합니다.

Cisco IP Manager Assistant 추적 필드

다음 표에서는 Cisco IP Manager Assistant 추적 필드에 대해 설명합니다. Cisco IP Manager Assistant 서비스는 Cisco Unified Communications Manager Assistant를 지원합니다.

표 *48: Cisco IP Manager Assistant* 추적 필드

필드 이름	설명
IPMA 서비스 추적 활성화	Cisco IP Manager Assistant 서비스의 추적을 활성화합니다.
IPMA Manager 구성 변경 로그 활성화	관리자 및 보조자 구성에 대한 변경 내용 추적을 활성화합니다.
IPMA CTI 추적 활성화	CTI 매니저 연결에 대한 추적을 활성화합니다.
IPMA CTI 보안 추적 활성화	CTIManager의 보안 연결에 대한 추적을 활성화합니다.

Cisco IP Voice Media Streaming App 추적 필드

이 섹션의 정보는 Cisco Unity Connection에는 적용되지 않습니다.

다음 표에서는 Cisco IP Voice Media Streaming App 추적 필드에 대해 설명합니다. Cisco IP Voice Media Streaming App 서비스는 Unified Communications Manager를 지원합니다.

표 *49: Cisco IP Voice Media Streaming Application* 추적 필드

필드 이름	설명
서비스 초기화 추적 활성화	초기화 정보에 대한 추적을 활성화합니다.
MTP 장치 추적 활성화	MTP(미디어 종료 지점)에 대해 처리된 메시지를 모니터링하기 위해 추적을 활성화합니다.
장치 복구 추적 활성화	MTP, 전화회의 브리지 및 MOH의 장치 복구 관련 정보에 대한 추적을 활성화합니다.
Skinny 스테이션 메시지 추적 활성화	Skinny 스테이션 프로토콜에 대한 추적을 활성화합니다.
WinSock 수준 2 추적 활성화	높은 수준의 상세 WinSock 관련 정보에 대한 추적을 활성화합니다.
대기 중 음악 관리자 추적 활성화	MOH 오디오 소스 관리자를 모니터링하기 위해 추적을 활성화합니다.
알림 장치 추적 활성화	알림 장치를 모니터링하기 위해 추적을 활성화합니다.
DB 설정 관리자 추적 활성화	MTP, 전화회의 브리지 및 MOH에 대한 데이터베이스 설정 및 변경 사항을 모니터링하기 위해 추적을 활성화합니다.

필드 이름	설명
전화회의 브리지 장치 추적 활성화	전화회의 브리지에 대해 처리된 메시지를 모니터링하기 위해 추적을 활성화합니다.
장치 드라이버 추적 활성화	장치 드라이버 추적을 활성화합니다.
WinSock 수준 1 추적 활성화	낮은 수준의 일반 WinSock 관련 정보에 대한 추적을 활성화합니다.
대기 중 음악 장치 추적 활성화	MOH에 대해 처리된 메시지를 모니터링하기 위해 추적을 활성화합니다.
TFTP 다운로드 추적 활성화	MOH 오디오 소스 파일의 다운로드를 모니터링하기 위해 추적을 활성화합니다.

Cisco TFTP 추적 필드

다음 표에서는 Cisco TFTP 추적 필드에 대해 설명합니다. Cisco TFTP 서비스는 Unified Communications Manager를 지원합니다.

표 ***50: Cisco TFTP*** 추적 필드

필드 이름	설명
서비스 시스템 추적 활성화	서비스 시스템에 대한 추적을 활성화합니다.
빌드 파일 추적 활성화	빌드 파일에 대한 추적을 활성화합니다.
서비스 파일 추적 활성화	서비스 파일에 대한 추적을 활성화합니다.

Cisco Web Dialer 웹 서비스 추적 필드

다음 표에서는 Cisco Web Dialer 웹 서비스 추적 필드에 대해 설명합니다. Cisco Web Dialer 웹 서비스는 Unified Communications Manager를 지원합니다.

표 ***51: Cisco Web Dialer*** 웹 서비스 추적 필드

필드 이름	설명
Web Dialer 서블릿 추적 활성화	Cisco Web Dialer 서블릿에 대한 추적을 활성화합니다.
리디렉터 서블릿 추적 활성화	리디렉터 서블릿에 대한 추적을 활성화합니다.

IM and Presence SIP 프록시 서비스 추적 필터 설정

아래 표는 IM and Presence SIP 프록시에 대한 서비스 추적 필터 설정에 대해 설명합니다.

표 ***52: IM and Presence SIP*** 프록시 서비스 추적 필터 설정

매개 변수	설명
액세스 로그 추적 활성화	이 매개 변수는 프록시 액세스 로그 추적을 활성화합니다. 프록시에서 수신한 각 SIP 메시지의 첫 번째 라인이 기록됩니다.
인증 추적 활성화	이 매개 변수는 인증 모듈에 대한 추적을 활성화합니다.
캘린더 추적 활성화	이 매개 변수는 캘린더 모듈에 대한 추적을 활성화합니다.
CTI 게이트웨이 추적 활성화	이 매개 변수는 CTI 게이트웨이에 대한 추적을 활성화합니다.
Enum 추적 활성화	이 매개 변수는 Enum 모듈에 대한 추적을 활성화합니다.
메서드/이벤트 라우팅 추적 활성화	이 매개 변수는 메서드/이벤트 라우팅 모듈에 대한 추적을 활성화합니다.
번호 확장 추적 활성화	이 매개 변수는 번호 확장 모듈에 대한 추적을 활성화합니다.
파서 추적 활성화	이 매개 변수를 사용하면 per-sipd 하위 SIP 파서의 작업과 관련된 파서 정보를 추적할 수 있습니다.
프라이버시 추적 활성화	이 매개 변수를 사용하면 프라이버시 요청과 관련하여 PAI, RPID 및 전환 헤더 처리에 대한 정보를 추적할 수 있습니다.
레지스트리 추적 활성화	이 매개 변수는 레지스트리 모듈에 대한 추적을 활성화합니다.
라우팅 추적 활성화	이 매개 변수는 라우팅 모듈에 대한 추적을 활성화합니다.
SIPUA 추적 활성화	이 매개 변수는 SIP UA 애플리케이션 모듈에 대한 추적을 활성화합니다.
서버 추적 활성화	이 매개 변수는 서버에 대한 추적을 활성화합니다.
SIP 메시지 및 상태 시스템 추적 활성화	이 매개 변수를 사용하면 per-sipd SIP 상태 시스템의 작업과 관련된 정보를 추적할 수 있습니다.
SIP TCP 추적 활성화	이 매개 변수를 사용하면 TCP 서비스에 의한 SIP 메시지의 TCP 전송과 관련된 정보를 추적할 수 있습니다.
SIP TLS 추적 활성화	이 매개 변수를 사용하면 TCP 서비스에 의한 SIP 메시지의 TLS 전송과 관련된 정보를 추적할 수 있습니다.
SIP XMPP IM 게이트웨이 추적 활성화	이 매개 변수를 사용하면 SIP XMPP IM 게이트웨이를 추적할 수 있습니다.

매개 변수	설명
프레즌스 웹 서비스 추적 활성화	이 매개 변수는 프레즌스 웹 서비스에 대한 추적을 활성화합니다.

IM and Presence 추적 필드 설명

다음 표에서는 특정 구성 요소의 추적 활성화를 지원하는 서비스에 대한 필드 설명을 제공합니다. 일부 서비스의 경우 서비스에 대한 모든 추적을 활성화하는 대신 특정 구성 요소에 대한 추적을 활성화할 수 있습니다. 서비스가 이 장에 포함되지 않은 경우 추적 구성 창에 서비스에 대한 모든 추적 활성화가 표시됩니다.

Cisco Access 로그 추적 필드

다음 표에서는 Cisco Access 로그 추적 필드에 대해 설명합니다.

표 ***53:*** 액세스 로그 추적 필드

필드 이름	설명
액세스 로그 추적 활성화	액세스 로그 추적을 설정합니다.

Cisco Authentication 추적 필드

다음 표에서는 Cisco Authentication 추적 필드에 대해 설명합니다.

표 ***54:*** 인증 추적 필드

필드 이름	설명
인증 추적 활성화	인증 추적을 설정합니다.

Cisco 달력 추적 필드

다음 표에서는 Cisco 달력 추적 필드에 대해 설명합니다.

표 ***55:*** 달력 추적 필드

필드 이름	설명
캘린더 추적 활성화	캘린더 추적을 설정합니다.

Cisco CTI 게이트웨이 추적 필드

다음 표에서는 Cisco CTI 게이트웨이 추적 필드에 대해 설명합니다.

표 *56: CTI* 게이트웨이 추적 필드

필드 이름	설명
CTI 게이트웨이 추적 활성화	CTI 게이트웨이 추적을 켭니다.

Cisco Database Layer Monitor 추적 필드

다음 표에서는 Cisco Database Layer Monitor 추적 필드에 대해 설명합니다.

표 *57: Cisco Database Layer Monitor* 추적 필드

필드 이름	설명
DB 라이브러리 추적 활성화	C++ 애플리케이션에 대한 데이터베이스 라이브러리 추적을 켭니다.
서비스 추적 활성화	서비스 추적을 켭니다.
DB 변경 알림 추적 활성화	C++ 애플리케이션에 대한 데이터베이스 변경 알림 추적을 활성화합니다.
단위 테스트 추적 활성화	선택하지 마십시오. Cisco 기술팀은 디버깅 목적으로 이를 사용합니다.

Cisco Enum 추적 필드

다음 표에서는 Cisco Enum 추적 필드에 대해 설명합니다.

표 *58: Enum* 추적 필드

필드 이름	설명
Enum 추적 활성화	Enum 추적을 설정합니다.

Cisco 메서드/이벤트 추적 필드

다음 표에서는 Cisco 메서드/이벤트 추적 필드에 대해 설명합니다.

표 *59:* 메서드/이벤트 추적 필드

필드 이름	설명
메서드/이벤트 추적 활성화	메서드/이벤트 추적을 설정합니다.

Cisco 번호 확장 추적 필드

다음 표에서는 Cisco 번호 확장 추적 필드에 대해 설명합니다.

표 60: 번호 확장 추적 필드

필드 이름	설명
번호 확장 추적 활성화	번호 확장 추적을 활성화합니다.

Cisco 파서 추적 필드

다음 표에서는 Cisco 파서 추적 필드에 대해 설명합니다.

표 61: 파서 추적 필드

필드 이름	설명
파서 추적 활성화	파서 추적을 활성화합니다.

Cisco 프라이버시 추적 필드

다음 표에서는 Cisco 프라이버시 추적 필드에 대해 설명합니다.

표 62: PrivacyTrace 필드

필드 이름	설명
프라이버시 추적 활성화	프라이버시 추적을 활성화합니다.

Cisco 프록시 추적 필드

다음 표에서는 Cisco 프록시 추적 필드에 대해 설명합니다.

표 63: 프록시 추적 필드

필드 이름	설명
프록시	프록시 추적을 켭니다.

Cisco RIS Data Collector 추적 필드

다음 표에서는 Cisco RIS Data Collector 추적 필드에 대해 설명합니다.

표 64: Cisco RIS Data Collector 추적 필드

필드 이름	설명
RISDC 추적 활성화	RIS Data Collector 서비스의 RISDC 스레드에 대한 추적을 활성화합니다.
시스템 액세스 추적 활성화	RIS Data Collector에서 시스템 액세스 라이브러리에 대한 추적을 활성화합니다.

필드 이름	설명
링크 서비스 추적 활성화	RIS Data Collector에서 링크 서비스 라이브러리에 대한 추적을 활성화합니다.
RISDC 액세스 추적 활성화	RIS Data Collector에서 RISDC 액세스 라이브러리에 대한 추적을 활성화합니다.
RISDB 추적 활성화	RIS Data Collector에서 RISDB 라이브러리에 대한 추적을 활성화합니다.
PI 추적 활성화	RIS Data Collector에서 PI 라이브러리에 대한 추적을 활성화합니다.
XML 추적 활성화	RIS Data Collector 서비스의 입/출력 XML 메시지에 대한 추적을 활성화합니다.
Perfmon 로거 추적 활성화	RIS Data Collector의 문제 해결 perfmon 데이터 로깅에 대한 추적을 활성화합니다. 로그 파일의 이름, 로그에 기록된 총 카운터 수, 애플리케이션의 이름, 시스템 카운터와 인스턴스, 프로세스 및 스레드 CPU 비율 계산 및 로그 파일 롤오버와 삭제 발생을 추적하는 데 사용됩니다.

Cisco 레지스트리 추적 필드

다음 표에서는 Cisco 레지스트리 추적 필드에 대해 설명합니다.

표 ***65:*** 레지스트리 추적 필드

필드 이름	설명
레지스트리 추적 활성화	레지스트리 추적을 활성화합니다.

Cisco 라우팅 추적 필드

다음 표에서는 Cisco 라우팅 추적 필드에 대해 설명합니다.

표 ***66:*** 라우팅 추적 필드

필드 이름	설명
라우팅 추적 활성화	라우팅 추적을 활성화합니다.

Cisco 서버 추적 필드

다음 표에서는 Cisco 서버 추적 필드에 대해 설명합니다.

표 *67:* 서버 추적 필드

필드 이름	설명
서버 추적 활성화	서버 추적을 활성화합니다.

Cisco SIP 메시지 및 상태 시스템 추적 필드

다음 표에서는 Cisco SIP 메시지 및 상태 시스템 추적 필드에 대해 설명합니다.

표 *68: SIP* 메시지 및 상태 시스템 추적 필드

필드 이름	설명
SIP 메시지 및 상태 시스템 추적 활성화	SIP 메시지 및 상태 시스템 추적을 활성화합니다.

Cisco SIP TCP 추적 필드

다음 표에서는 Cisco SIP TCP 추적 필드에 대해 설명합니다.

표 *69: SIP TCP* 추적 필드

필드 이름	설명
SIP TCP 추적 활성화	SIP TCP 추적을 활성화합니다.

Cisco SIP TLS 추적 필드

다음 표에서는 Cisco SIP TLS 추적 필드에 대해 설명합니다.

표 *70: SIP TLS* 추적 필드

필드 이름	설명
SIP TLS 추적 활성화	SIP TLS 추적을 활성화합니다.

Cisco 웹 서비스 추적 필드

다음 표에서는 Cisco 웹 서비스 추적 필드에 대해 설명합니다.

표 *71:* 웹 서비스 추적 필드

필드 이름	설명
프레즌스 웹 서비스 추적 활성화	프레즌스 웹 서비스 추적을 활성화합니다.

추적 출력 설정

다음 표에는 추적 로그 파일 설명이 포함되어 있습니다.

주의 추적 구성 창에서 최대 파일 수 또는 최대 파일 크기 설정을 변경하면 시스템은 서비스를 실행 중인 경우 현재 파일을 제외한 모든 서비스 로그 파일을 삭제하고 서비스가 활성화되지 않은 경우 시스템은 사용자가 서비스를 활성화하는 즉시 파일을 삭제합니다. 최대 파일 수 설정 또는 최대 파일 크기 설정을 변경하기 전에 로그 파일의 레코드를 유지하려는 경우 서비스 로그 파일을 다운로드하여 다른 서버에 저장합니다. 이 작업을 수행 하려면 Unity RTMT에서 추적 및 로그 센트럴을 사용합니다.

표 ***72:*** 추적 출력 설정

필드	설명
최대 파일 수	이 필드는 지정된 서비스에 대한 총 추적 파일 수를 지정합니다. Cisco 통합 서비스 가용성는 파일을 나타내는 시퀀스 번호(예: cus299.txt)를 파일 이름에 자동으로 추가합니다. 시퀀스의 마지막 파일이 꽉 차면 추적 데이터는 첫 번째 파일에 대한 쓰기를 시작합니다. 기본값은 서비스에 따라 다릅니다.
최대 파일 크기(MB)	이 필드는 추적 파일의 최대 크기(MB)입니다. 기본값은 서비스에 따라 다릅니다.

추적 설정 문제 해결

추적 설정 문제 해결 창

추적 설정 문제 해결 창에서는 미리 정의된 추적 설정 문제 해결을 설정하려는 서비스 가용성 GUI의 서비스를 선택할 수 있습니다. 이 창에서는 클러스터의 다른 노드에서 서비스를 선택할 수 있습니다. 그러면 선택한 모든 서비스에 대한 추적 설정 변경 사항이 채워집니다. 단일 노드, 노드에 대한 모든 활성 서비스, 클러스터의 모든 노드에 대한 특정 활성 서비스 또는 클러스터의 모든 노드에 대한 모든 활성 서비스를 선택할 수 있습니다. 창에서 비활성 서비스 옆에 해당 없음이 표시됩니다.

참고 IM and Presence의 경우 IM and Presence에 대한 미리 정의된 추적 설정 문제 해결에는 단일 구성 요소 및 Log4j 추적 설정이 포함됩니다. 추적 설정 문제 해결이 적용되기 전에 시스템은 원래 추적 설정을 백업합니다. 추적 설정 문제 해결을 재설정하면 원래 추적 설정이 복원됩니다.

서비스에 대한 추적 설정 문제 해결을 적용한 후 추적 설정 문제 해결 창을 열면 문제 해결을 위해 설정한 서비스가 선택됨으로 표시됩니다. 추적 설정 문제 해결 창에서 추적 설정을 원래 설정으로 재설정할 수 있습니다.

서비스에 대한 추적 설정 문제 해결을 적용한 후에는 추적 구성 창에 해당 서비스에 대해 추적 기능이 설정되었다는 메시지가 표시됩니다. 관련 링크 목록 상자에서 서비스에 대한 설정을 재설정하려는 경우 추적 설정 문제 해결 옵션을 선택할 수 있습니다. 지정된 서비스의 경우 추적 출력 설정의 일부 매개 변수(예: 최대 파일 수)를 제외하고 추적 구성 창에 모든 설정이 읽기 전용으로 표시됩니다.

추적 설정 문제 해결

시작하기 전에

추적 구성 설정 작업을 검토하고 추적 매개 변수를 설정합니다.

프로시저

단계 **1** 추적 > 추적 설정 문제 해결을 선택합니다.

단계 **2** 서버 목록 상자에서 추적 설정 문제 해결을 할 서버를 선택합니다.

단계 **3** 이동을 선택합니다.

서비스 목록이 표시됩니다. 활성 상태가 아닌 서비스는 N/A로 표시됩니다.

단계 **4** 다음 작업 중 하나를 수행합니다.

a) 서버 목록 상자에서 선택한 노드의 특정 서비스를 모니터링하려면 서비스 창에서 서비스를 확인합니다.

예를 들어 데이터베이스 및 관리 서비스, 성능 및 모니터링 서비스, 백업 및 복원 서비스 창 등이 있습니다.

이 작업은 서버 목록 상자에서 선택한 노드에만 영향을 미칩니다.

b) 서버 목록 상자에서 선택한 노드의 모든 서비스를 모니터링하려면 모든 서비스 확인을 선택합니다.

c) Cisco Unified Communications Manager 및 IM and Presence 클러스터에만 해당: 클러스터의 모든 노드에서 특정 서비스를 모니터링하려면 모든 노드에서 선택한 서비스 확인을 선택합니다.

이 설정은 서비스가 활성 상태인 클러스터의 모든 노드에 적용됩니다.

d) Unified Communications Manager 및 IM and Presence 클러스터에만 해당: 클러스터의 모든 노드에 대한 모든 서비스를 모니터링하려면 모든 노드에서 모든 서비스 확인을 선택합니다.

단계 **5** 저장을 선택합니다.

단계 **6** 다음 버튼 중 하나를 선택하여 원래 추적 설정을 복원합니다.

a) 문제 해결 추적 재설정 - 서버 목록 상자에서 선택한 노드의 서비스에 대한 원래 추적 설정을 복원합니다. 선택할 수 있는 아이콘으로도 표시됩니다.

b) Unified Communications Manager 및 IM and Presence 클러스터에만 해당: 모든 노드에서 문제 해결 추적 재설정 - 클러스터의 모든 노드에서 서비스에 대한 원래 추적 설정을 복원합니다.

문제 해결 추적 재설정 버튼은 하나 이상의 서비스에 대한 문제 해결 추적을 설정한 경우에만 표시됩니다.

참고 문제 해결 추적을 오랫동안 활성화하면 추적 파일의 크기가 증가하고 서비스의 성능에 영향을 줄 수 있습니다.

재설정 버튼을 선택하면 창이 새로 고쳐지고 서비스 확인란이 선택 취소된 것으로 표시됩니다.

17 장

사용 레코드 보기

- 사용 레코드 개요, 261 페이지
- 사용 보고서 작업, 262 페이지

사용 레코드 개요

Cisco Unified Communications Manager는 구성된 항목이 시스템에서 사용되는 방식을 확인할 수 있는 레코드를 제공합니다. 구성된 항목은 장치 풀, 날짜 및 시간 그룹, 경로 플랜 같은 시스템 수준 설정 및 장치를 포함합니다.

종속성 레코드

다음 목적으로 종속성 레코드를 사용합니다.

- 서버, 장치 풀, 날짜 및 시간 그룹 등의 시스템 수준 설정에 대한 정보를 찾습니다.
- 다른 레코드를 사용하는 데이터베이스의 레코드를 확인합니다. 예를 들어 특정 발신 검색 공간을 사용하는 장치(예: CTI 경로 포인트 또는 전화기)를 확인할 수 있습니다.
- 레코드를 삭제하기 전에 레코드 간의 종속성을 표시합니다. 예를 들어, 파티션을 삭제하기 전에 종속성 레코드를 사용하여 어떤 발신 검색 공간(CSS) 및 장치가 연결되어 있는지 확인합니다. 그런 다음 설정을 재구성하여 종속성을 제거할 수 있습니다.

경로 플랜 보고서

경로 플랜 보고서를 사용하면 시스템에 구성된 숫자, 경로 및 패턴의 일부 또는 전체 목록을 볼 수 있습니다. 보고서를 생성하면 보고서의 패턴/디렉터리 번호, 파티션 또는 경로 세부 정보 열에서 항목을 클릭하여 각 항목에 대한 구성 창에 액세스할 수 있습니다.

또한 라우트 계획 보고서를 사용하여 보고서 데이터를 .CSV 파일로 저장하여 다른 애플리케이션으로 가져올 수 있습니다. .CSV 파일에는 전화기의 디렉터리 번호, 라우트 패턴, 패턴 사용, 디바이스 이름 및 디바이스 설명을 비롯하여 웹페이지보다 더 자세한 정보가 포함되어 있습니다.

Cisco 통합 커뮤니케이션 매니저 는 라우트 플랜을 사용하여 내부 통화와 외부 PSTN(Public Switched Telephone Network) 통화를 모두 라우팅합니다. 네트워크에 레코드가 여러 개 있을 수 있으므로 Cisco Unified Communications Manager 관리에서는 특정 기준을 기준으로 특정 경로 플랜 레코드를 찾을 수 있습니다.

사용 보고서 작업

프로시저

	명령 또는 동작	목적
단계 **1**	경로 플랜 레코드를 보고 이를 사용하여 할당되지 않은 디렉터리 번호를 관리하려면 다음 절차를 참조하십시오. • 경로 플랜 레코드 보기, 263 페이지 • 경로 플랜 보고서 저장, 263 페이지 • 할당되지 않은 디렉토리 번호 삭제, 264 페이지 • 할당되지 않은 디렉터리 번호 업데이트, 264 페이지	이 절차를 사용하여 특정 경로 플랜 레코드를 찾고 CSV 파일에 레코드를 저장하고 할당되지 않은 디렉터리 번호를 관리합니다.
단계 **2**	종속성 레코드를 사용하려면 다음 절차를 참조하십시오. • 종속성 레코드 보기, 266 페이지	이 절차를 사용하여 시스템 수준 설정에 대한 정보를 찾고 데이터베이스에 있는 레코드 사이의 종속성을 표시합니다.

경로 플랜 보고서 작업 흐름

프로시저

	명령 또는 동작	목적
단계 **1**	경로 플랜 레코드 보기, 263 페이지.	경로 플랜 레코드를 확인하고 사용자 정의된 경로 플랜 보고서를 생성합니다.
단계 **2**	경로 플랜 보고서 저장, 263 페이지.	.csv 파일 형식으로 경로 플랜 보고서를 봅니다.
단계 **3**	할당되지 않은 디렉토리 번호 삭제, 264 페이지.	경로 플랜 보고서에서 할당되지 않은 디렉터리 번호를 삭제합니다.
단계 **4**	할당되지 않은 디렉터리 번호 업데이트, 264 페이지.	경로 플랜 보고서에서 할당되지 않은 디렉터리 번호 설정을 업데이트합니다.

경로 플랜 레코드 보기

이 섹션에서는 경로 플랜 레코드를 보는 방법을 설명합니다. 네트워크에 레코드가 여러 개 있을 수 있으므로 Cisco Unified Communications Manager 관리에서는 특정 기준을 기준으로 특정 경로 플랜 레코드를 찾을 수 있습니다. 다음 절차를 사용하여 사용자 정의된 경로 플랜 보고서를 생성합니다.

프로시저

단계 **1** 통화 라우팅 > 경로 플랜 보고서를 선택합니다.

단계 **2** 데이터베이스에서 모든 레코드를 찾으려면 대화 상자가 비어 있는지 확인하고 3단계로 이동합니다.

레코드를 필터링하거나 검색하려면 다음을 수행합니다.

a) 첫 번째 드롭다운 목록표에서 검색 파라미터를 선택합니다.
b) 두 번째 드롭다운 목록표에서 검색 패턴을 선택합니다.
c) 적절한 검색 텍스트를 지정합니다(해당하는 경우).

단계 **3** 찾기를 클릭합니다.

모든 또는 일치하는 레코드가 표시됩니다. [행/페이지] 드롭다운 목록표에서 다른 값을 선택하여 각 페이지에 표시할 항목 수를 변경할 수 있습니다.

단계 **4** 표시되는 레코드 목록에서 보려는 레코드의 링크를 클릭합니다.

창에 선택한 항목이 표시됩니다.

경로 플랜 보고서 저장

이 섹션에는 경로 플랜 보고서를 .csv 파일로 보는 방법에 대한 내용이 있습니다.

프로시저

단계 **1** 통화 라우팅 > 경로 플랜 보고서를 선택합니다.

단계 **2** 경로 플랜 보고서 창의 관련 링크 드롭다운 목록에서 파일로 보기를 선택한 다음 이동을 클릭합니다.

나타나는 대화 상자에서 파일을 저장하거나 다른 애플리케이션으로 가져올 수 있습니다.

단계 **3** 저장을 클릭합니다.

선택한 위치에 이 파일을 저장할 수 있는 다른 창이 표시됩니다.

참고 또한 파일을 다른 파일 이름으로 저장할 수 있으며, 파일 이름에 .CSV 확장자가 포함되어야 합니다.

단계 **4** 파일을 저장할 위치를 선택하고 저장을 클릭합니다. 이 작업은 지정한 위치에 파일을 저장해야 합니다.

단계 **5** 방금 저장한 .CSV 파일을 찾아 해당 아이콘을 두 번 클릭하여 파일을 확인합니다.

할당되지 않은 디렉토리 번호 삭제

이 섹션에서는 경로 플랜 보고서에서 할당되지 않은 디렉터리 번호를 삭제하는 방법을 설명합니다. 디렉터리 번호는 Cisco Unified Communications Manager 관리의 [디렉터리 번호 구성] 창에서 구성 및 제거됩니다. 장치에서 디렉터리 번호를 제거하거나 전화기를 삭제해도 디렉터리 번호는 Cisco Unified Communications Manager 데이터베이스에서 계속 유지됩니다. 데이터베이스에서 디렉터리 번호를 삭제하려면 [경로 플랜 보고서] 창을 사용합니다.

프로시저

단계 **1** 통화 라우팅 > 경로 플랜 보고서를 선택합니다.

단계 **2** [경로 플랜 보고서] 창에서 3개의 드롭다운 목록을 사용하여 할당되지 않은 모든 DN을 나열하는 경로 플랜 보고서를 지정합니다.

단계 **3** 다음과 같이 세 가지 방법으로 디렉터리 번호를 삭제할 수 있습니다.

a) 삭제할 디렉터리 번호를 클릭합니다. [디렉터리 번호 구성] 창이 표시되면 [삭제]를 클릭합니다.
b) 삭제할 디렉터리 번호 옆의 확인란을 선택합니다. 선택한 항목 삭제를 클릭합니다.
c) 할당되지 않은 것으로 확인된 디렉터리 번호를 모두 삭제하려면 [찾은 항목 모두 삭제]를 클릭합니다.

경고 메시지가 표시되고 디렉터리 번호를 삭제할 것인지 확인합니다.

단계 **4** 디렉터리 번호를 삭제하려면 [확인]을 클릭합니다. 삭제 요청을 취소하려면 [취소]를 클릭합니다.

할당되지 않은 디렉터리 번호 업데이트

이 섹션에서는 경로 플랜 보고서에서 할당되지 않은 디렉터리 번호의 설정을 업데이트하는 방법을 설명합니다. 디렉터리 번호는 Cisco Unified Communications Manager 관리의 [디렉터리 번호 구성] 창에서 구성 및 제거됩니다. 장치에서 디렉터리 번호를 제거해도 Cisco Unified Communications Manager 데이터베이스에서 디렉터리 번호가 계속 유지됩니다. 디렉터리 번호 설정을 업데이트하려면 [경로 플랜 보고서] 창을 사용합니다.

프로시저

단계 **1** 통화 라우팅 > 경로 플랜 보고서를 선택합니다.

단계 **2** 경로 플랜 보고서 창에서 3개의 드롭다운 목록을 사용하여 할당되지 않은 모든 DN을 나열하는 경로 플랜 보고서를 지정합니다.

단계 **3** 업데이트할 디렉터리 번호를 클릭합니다.

참고 디렉터리 번호 및 파티션을 제외한 디렉터리 번호의 모든 설정을 업데이트할 수 있습니다.

단계 **4** 발신 검색 공간 또는 착신 전환 옵션과 같이 필요한 업데이트를 수행합니다.

단계 **5** 저장을 클릭합니다.

[디렉터리 번호 구성] 창이 다시 표시되고 [디렉터리 번호] 필드가 비어 있습니다.

종속성 레코드 작업 흐름

프로시저

	명령 또는 동작	목적
단계 **1**	종속성 레코드 구성, 265 페이지.	종속성 레코드를 활성화하거나 비활성화하려면 이 절차를 사용합니다. 다이얼 플랜 크기와 복잡성, CPU 속도 및 기타 애플리케이션의 CPU 요구 사항으로 인해, 이 절차가 일반 우선 순위보다 낮은 우선 순위로 실행되고 완료하는 데 시간이 오래 걸릴 수 있습니다.
단계 **2**	종속성 레코드 보기, 266 페이지.	종속성 레코드를 활성화한 후 인터페이스의 [구성] 창에서 액세스할 수 있습니다.

종속성 레코드 구성

Cisco Unified Communications Manager 데이터베이스에서 레코드 간의 관계를 보려면 종속성 레코드를 사용합니다. 예를 들어, 파티션을 삭제하기 전에 종속성 레코드를 사용하여 어떤 발신 검색 공간(CSS) 및 장치가 연결되어 있는지 확인합니다.

주의 종속성 레코드로 인해 CPU 사용량이 많아집니다. 다이얼 플랜 크기와 복잡성, CPU 속도 및 기타 애플리케이션의 CPU 요구 사항으로 인해, 이 절차가 일반 우선 순위보다 낮은 우선 순위로 실행되고 완료하는 데 시간이 오래 걸릴 수 있습니다.

종속성 레코드가 활성화되어 있는 상태에서 시스템에 CPU 사용량 문제가 발생하는 경우 종속성 레코드를 비활성화할 수 있습니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 시스템 > 엔터프라이즈 매개 변수를 선택합니다.

단계 **2** **CCMAdmin** 매개 변수 섹션으로 스크롤하고 종속성 레코드 활성화 드롭다운 목록에서 다음 옵션 중 하나를 선택합니다.

- **True**—종속성 레코드를 활성화합니다.
- **False**—종속성 레코드를 비활성화합니다.

선택하는 옵션에 따라 종속성 레코드의 활성화 또는 비활성화 결과에 대한 메시지가 있는 대화 상자가 표시됩니다. 메시지를 읽은 후에 이 대화 상자에서 확인을 클릭합니다.

단계 **3** 확인을 클릭합니다.

단계 **4** 저장을 클릭합니다.
변경을 확인하는 업데이트 성공 메시지가 표시됩니다.

종속성 레코드 보기

종속성 레코드를 활성화한 후 인터페이스의 [구성] 창에서 액세스할 수 있습니다.

시작하기 전에

종속성 레코드 구성, 265 페이지

프로시저

단계 **1** Cisco Unified CM 관리에서 보려는 레코드에 대한 구성 창으로 이동합니다.

예제:

장치 풀에 대한 종속성 레코드를 보려면 시스템 > 장치 풀을 선택합니다.

참고 장치 기본값 및 엔터프라이즈 매개 변수 구성 창에서는 종속성 레코드를 볼 수 없습니다.

단계 **2** 찾기를 클릭합니다.

단계 **3** 레코드 중 하나를 클릭합니다.
[구성] 창이 나타납니다.

단계 **4** 관련 링크 목록 상자에서 종속성 레코드를 선택하고 이동을 클릭합니다.

참고 종속성 레코드를 활성화하지 않은 경우 종속성 레코드 요약 창에 레코드에 대한 정보가 없이 메시지가 나타납니다.

데이터베이스의 다른 레코드에서 사용하는 레코드를 보여주는 종속성 레코드 요약 창이 나타납니다.

단계 **5** 이 창에서 다음 종속성 레코드 단추 중 하나를 선택합니다.

- 새로 고침—최신 정보로 창을 업데이트합니다.
- 닫기— [종속성 레코드] 링크를 클릭했던 [구성] 창으로 돌아가지 않고 창을 닫습니다.
- 닫은 후 뒤로— 창을 닫고 [종속성 레코드] 링크를 클릭했던 [구성] 창으로 돌아갑니다.

18 장

엔터프라이즈 매개 변수 관리

- 엔터프라이즈 매개변수 개요, 267 페이지

엔터프라이즈 매개변수 개요

엔터프라이즈 매개 변수는 전체 클러스터의 모든 장치 및 서비스에 적용되는 기본 설정을 제공합니다. 예를 들어, 시스템은 엔터프라이즈 매개 변수를 사용하여 관련 장치 기본값의 초기값을 설정합니다.

엔터프라이즈 매개 변수를 추가하거나 삭제할 수는 없지만 기존 엔터프라이즈 매개 변수를 업데이트할 수 있습니다. 구성 창은 범주 아래 엔터프라이즈 매개 변수 표시합니다(예: CCMAdmin 매개 변수, CCMUser 매개 변수 및 CDR 매개 변수).

엔터프라이즈 매개 변수 구성 창에서 엔터프라이즈 매개 변수에 대한 자세한 내용을 볼 수 있습니다.

⚠

주의 대부분의 엔터프라이즈 매개 변수는 변경할 필요가 없습니다. 변경하려는 기능을 완전히 이해했거나 Cisco TAC(기술 지원 센터)에서 변경을 조언한 경우가 아니면 엔터프라이즈 매개 변수를 변경하지 마십시오.

엔터프라이즈 매개 변수 정보 보기

엔터프라이즈 매개 변수 구성 창에 포함된 콘텐츠를 통해 엔터프라이즈 매개 변수에 대한 정보에 액세스합니다.

프로시저

단계 **1** [Cisco Unified CM 관리]에서 시스템 > 엔터프라이즈 매개 변수를 선택합니다.

단계 **2** 다음 작업 중 하나를 수행합니다.

- 특정 엔터프라이즈 매개 변수에 대한 설명을 보려면 매개 변수 이름을 클릭합니다.

- 모든 엔터프라이즈 매개 변수에 대한 설명을 보려면 **?**를 클릭합니다.

엔터프라이즈 매개 변수 업데이트

엔터프라이즈 매개 변수 구성 창을 열고 시스템 수준의 설정을 구성하려면 이 절차를 사용합니다.

주의 대부분의 엔터프라이즈 매개 변수는 변경할 필요가 없습니다. 변경하려는 기능을 완전히 이해했거나 Cisco TAC(기술 지원 센터)에서 변경을 조언한 경우가 아니면 엔터프라이즈 매개 변수를 변경하지 마십시오.

프로시저

단계 **1** [Cisco Unified CM 관리]에서 시스템 > 엔터프라이즈 매개 변수를 선택합니다.

단계 **2** 변경하려는 엔터프라이즈 매개 변수의 원하는 값을 선택합니다.

단계 **3** 저장을 클릭합니다.

다음에 수행할 작업

장치에 구성 적용, 268 페이지

장치에 구성 적용

사용자가 구성한 설정으로 클러스터에 있는 모든 영향을 받는 장치를 업데이트하려면 이 절차를 사용합니다.

시작하기 전에

엔터프라이즈 매개 변수 업데이트, 268 페이지

프로시저

단계 **1** [Cisco Unified CM 관리]에서 시스템 > 엔터프라이즈 매개 변수를 선택합니다.

단계 **2** 변경 사항을 확인한 다음 저장을 클릭합니다.

단계 **3** 다음 옵션 중 하나를 선택합니다.

- 시스템이 재부팅할 장치를 결정하도록 하려면 구성 적용을 클릭합니다. 경우에 따라 장치를 재부팅할 필요가 없습니다. 장치 풀에 SIP 트렁크가 포함되어 있지 않으면 진행 중인 통화가 끊길 수 있지만 연결된 통화는 유지됩니다.

- 클러스터의 모든 장치를 재부팅하려면 재설정을 클릭합니다. 이 단계는 사용량이 적은 시간 동안 수행하는 것이 좋습니다.

단계 **4** 확인 대화 상자를 읽은 후 확인을 클릭합니다.

기본 엔터프라이즈 매개 변수 복원

엔터프라이즈 매개 변수를 기본 설정으로 재설정하려면 이 절차를 사용합니다. 일부 엔터프라이즈 매개 변수에 구성 창의 열에 표시된 대로 제안된 값이 포함되어 있습니다. 이 절차는 이러한 값을 기본 설정으로 사용합니다.

프로시저

단계 **1** [Cisco Unified CM 관리]에서 시스템 > 엔터프라이즈 매개 변수를 선택합니다.

단계 **2** 기본값으로 설정을 클릭합니다.

단계 **3** 확인 프롬프트를 읽은 후 확인을 클릭합니다.

19 장

서버 관리

- 서버 관리 개요, 271 페이지
- 서버 삭제 , 271 페이지
- 설치 전 클러스터에 노드 추가, 274 페이지
- Presence 서버 상태 보기, 275 페이지
- 포트 구성 , 276 페이지
- 호스트 이름 구성, 277 페이지
- kerneldump 유틸리티, 279 페이지

서버 관리 개요

이 장에서는 Cisco Unified Communications Manager 관리 노드의 속성을 관리하고 Presence 서버 상태를 보고 Unified Communications Manager 서버의 호스트 이름을 구성하는 방법을 설명합니다.

서버 삭제

이 섹션에서는 Cisco Unified Communications Manager 데이터베이스에서 서버를 삭제하는 방법과 삭제한 서버를 Cisco Unified Communications Manager 클러스터에 다시 추가하는 방법에 대해 설명합니다.

Cisco Unified Communications Manager 관리에서 클러스터의 첫 번째 노드는 삭제할 수 없지만 후속 노드는 삭제할 수 있습니다. [서버 찾기 및 나열] 창에서 후속 노드를 삭제하기 전에 [Cisco Unified CM 관리]에 다음 메시지가 표시됩니다. “하나 이상의 서버를 영구히 삭제하려고 합니다. 이 동작은 취소될 수 없습니다. 계속하시겠습니까?” [확인]을 클릭하면 서버가 Cisco Unified CM 데이터베이스에서 삭제되고 더 이상 사용할 수 없게 됩니다.

팁 [서버 구성] 창에서 서버를 삭제하려고 하면 앞 단락에 표시된 메시지와 유사한 메시지가 표시됩니다. [확인]을 클릭하면 서버가 Cisco Unified CM 데이터베이스에서 삭제되고 더 이상 사용할 수 없게 됩니다.

서버를 삭제하기 전에 다음 정보를 검토하십시오.

- Cisco Unified Communications Manager 관리에서는 클러스터의 첫 번째 노드를 삭제할 수 없지만 후속 노드를 삭제할 수 있습니다.
- 노드에 Cisco Unified Communications Manager가 실행 중인 경우 특히, 노드에 등록된 전화기와 같은 장치가 있는 경우에는 노드를 삭제하지 않는 것이 좋습니다.
- 후속 노드에 대한 종속성 레코드가 있더라도 이 레코드로 인해 노드를 삭제하지 못하게 되지는 않습니다.
- 삭제하는 노드에서 Cisco Unified Communications Manager에 대해 통화 지정보류 번호가 구성된 경우 삭제가 실패합니다. 노드를 삭제하려면 먼저 Cisco Unified Communications Manager 관리에서 해당 통화 지정보류 번호를 삭제해야 합니다.
- Cisco Unified Communications Manager 관리의 구성 필드에 삭제할 서버의 IP 주소 또는 호스트 이름이 포함된 경우 서버를 삭제하기 전에 구성을 업데이트합니다. 이 작업을 수행하지 않는 경우 해당 구성을 사용하는 기능이 서버 삭제 후 작동하지 않을 수 있습니다. 예를 들어 서비스 매개 변수, 엔터프라이즈 매개 변수, 서버 URL, 디렉터리 URL, IP 전화 서비스 등에 IP 주소 또는 호스트 이름을 입력하는 경우 서버를 삭제하기 전에 이 구성을 업데이트합니다.
- 애플리케이션 GUI(예: Cisco Unity, Cisco Unity Connection 등)에 삭제할 서버의 IP 주소 또는 호스트 이름이 포함된 경우 서버를 삭제하기 전에 해당하는 GUI에서 구성을 업데이트합니다. 이 작업을 수행하지 않으면 해당 구성을 사용하는 기능이 서버 삭제 후 작동하지 않을 수 있습니다.
- 서버를 삭제할 때 MOH 서버와 같은 일부 장치가 자동으로 삭제될 수 있습니다.
- 노드를 삭제하기 전에 후속 노드에서 활성 상태인 서비스를 비활성화하는 것이 좋습니다. 이 작업을 수행하면 노드 삭제 후 서비스가 작동합니다.
- 서버 구성 변경 사항은 Cisco 통합 커뮤니케이션 매니저를 다시 시작할 때까지 적용되지 않습니다. Cisco CallManager 서비스 다시 시작에 대한 자세한 내용은 *Cisco* 통합 서비스 가용성 관리 설명서를 참조하십시오.
- 데이터베이스 파일이 올바로 업데이트되게 하려면 서버, 프레즌스 또는 애플리케이션 서버를 삭제한 후 클러스터를 재부팅해야 합니다.
- 노드를 삭제한 후 Cisco Unified Reporting에 액세스하여 Cisco Unified Communications Manager가 클러스터에서 노드를 제거했는지 확인합니다. 또한 Cisco Unified Reporting, RTMT 또는 CLI에 액세스하여 기존 노드 간에 해당 데이터베이스 복제가 발생하는지 확인하고 필요한 경우 CLI를 사용하여 노드 간의 데이터베이스 복제를 복구합니다.

참고 클러스터에서 가입자 노드를 제거하면 해당 인증서가 퍼블리셔 및 기타 노드에 여전히 존재합니다. 관리자는 다음을 수동으로 제거해야 합니다.

- 개별 클러스터 구성원의 신뢰 저장소에서 제거된 가입자 노드의 인증서.
- 제거된 가입자 노드의 신뢰 저장소에 있는 각 클러스터 구성원의 인증서.

클러스터에서 통합 커뮤니케이션 관리자 노드 삭제

이 절차를 사용하여 클러스터에서 Cisco Unified Communications Manager 노드를 삭제합니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 시스템 > 서버를 선택합니다.

단계 **2** 찾기를 클릭하고 삭제할 노드를 선택합니다.

단계 **3** 삭제를 클릭합니다.

단계 **4** 경고 대화 상자에 이 작업을 실행 취소할 수 없다는 내용이 표시되면 확인을 클릭합니다.

단계 **5** 할당 해제한 노드의 호스트 VM을 종료합니다.

클러스터에서 **IM and Presence** 노드 삭제

IM and Presence Service 노드를 해당 프레즌스 이중화 그룹 및 클러스터에서 안전하게 제거해야 하는 경우 이 절차를 수행합니다.

주의 노드를 제거하면 프레즌스 이중화 그룹에 있는 나머지 노드의 사용자에 대한 서비스가 중단됩니다. 이 절차는 유지 보수 기간 동안에만 수행해야 합니다.

프로시저

단계 **1** **Cisco Unified CM** 관리 > 시스템 > 프레즌스 이중화 그룹페이지에서 고가용성이 활성화되어 있는 경우 이를 비활성화합니다.

단계 **2** **Cisco Unified CM** 관리 > 사용자 관리 > **Presence** 사용자 할당 페이지에서 제거할 노드의 모든 사용자를 할당 해제하거나 이동합니다.

단계 **3** 해당 프레즌스 이중화 그룹에서 노드를 제거하려면 프레즌스 이중화 그룹의 프레즌스 이중화 그룹 설정 페이지에 있는 Presence Server 드롭다운 목록에서 선택되지 않음을 선택합니다. 경고 대화 상자에 노드 할당 해제로 인해 프레즌스 이중화 그룹의 서비스가 다시 시작된다는 내용이 표시되면 확인을 선택합니다.

참고 프레즌스 이중화 그룹에서 퍼블리셔 노드를 직접 삭제할 수 없습니다. 퍼블리셔 노드를 삭제하려면 먼저 퍼블리셔 노드에서 사용자 할당을 해제하고 프레즌스 이중화 그룹을 완전히 삭제합니다.

그러나 삭제된 IM and Presence 노드를 클러스터에 다시 추가할 수 있습니다. 삭제된 노드를 추가하는 방법에 대한 자세한 내용은 삭제된 서버를 클러스터에 다시 추가, 274 페이지의 내용을 참조하십시오. 이 시나리오에서는 삭제된 퍼블리셔 노드가 Cisco Unified CM 관리 콘솔의 시스템 > 서버 화면에서 서버에 다시 추가될 때 **DefaultCUPSubcluster**가 자동으로 생성됩니다.

단계 **4** Cisco Unified CM 관리에서 시스템 > 서버에서 할당 해제된 노드를 삭제합니다. 경고 대화 상자에 이 작업을 실행 취소할 수 없다는 내용이 표시되면 확인을 클릭합니다.

단계 **5** 할당 해제한 노드의 호스트 VM 또는 서버를 종료합니다.

단계 **6** 모든 노드에서 **Cisco XCP** 라우터를 다시 시작합니다.

삭제된 서버를 클러스터에 다시 추가

Cisco Unified Communications Manager 관리에서 후속 노드(가입자)를 삭제한 후 클러스터에 다시 추가하려면 다음 절차를 수행합니다.

프로시저

단계 **1** Cisco Unified Communications Manager 관리에서 시스템 > 서버를 선택하여 서버를 추가합니다.

단계 **2** Cisco Unified Communications Manager 관리에 후속 노드를 추가한 후 해당 버전용 소프트웨어 키트에 제공된 디스크를 사용하여 서버에 설치합니다.

팁 설치하는 버전이 게시자 노드에서 실행되는 버전과 일치하는지 확인하십시오. 게시자에서 실행 중인 버전이 설치 파일과 일치하지 않는 경우 설치 프로세스 동안 설치 중 업그레이드 옵션을 선택합니다. 자세한 내용은 *Cisco Unified Communications Manager* 및 *IM and Presence Service* 설치 설명서를 참조하십시오.

단계 **3** Cisco Unified CM을 설치한 후에는 해당 Cisco Unified CM 버전을 지원하는 설치 설명서에 설명된 대로 후속 노드를 구성합니다.

단계 **4** Cisco Unified Reporting, RTMT 또는 CLI에 액세스하여 기존 노드 사이에서 데이터베이스 복제가 발생하는지 확인합니다. 필요한 경우 노드 간 데이터베이스 복제를 복구합니다.

설치 전 클러스터에 노드 추가

노드 설치 전에 [Cisco Unified Communications Manager 관리]를 사용하여 클러스터에 새 노드를 추가합니다. 노드를 추가할 때 선택하는 서버 유형과 설치하는 서버 유형이 일치해야 합니다.

새 노드를 설치하기 전에 첫 번째 노드에서 [Cisco Unified Communications Manager 관리]를 사용하여 새 노드를 구성해야 합니다. 클러스터에 노드를 설치하려면 *Cisco Unified Communications Manager* 설치 설명서를 참조하십시오.

Cisco Unified Communications Manager 비디오/음성 서버의 경우 Cisco Unified Communications Manager 소프트웨어의 초기 설치 중 추가하는 첫 번째 서버가 게시자 노드로 지정됩니다. 이후 설치 또는 추가되는 서버는 모두 가입자 노드로 지정됩니다. 클러스터에 추가하는 첫 번째 Cisco Unified Communications Manager IM and Presence 노드는 IM and Presence Service 데이터베이스 게시자 노드로 지정됩니다.

참고 서버가 추가된 후에는 [Cisco Unified Communications Manager 관리]를 사용하여 서버 유형을 변경할 수 없습니다. 기존 서버 인스턴스를 삭제한 다음 새 서버를 다시 추가하고 서버 유형 설정을 올바로 선택해야 합니다.

프로시저

단계 **1** 시스템 > 서버를 선택합니다.

서버 찾기 및 나열 창이 표시됩니다.

단계 **2** 새로 추가를 클릭합니다.

서버 구성 - 서버 추가 창이 표시됩니다.

단계 **3** 서버 유형 드롭다운 목록 상자에서 추가할 서버를 선택한 후 다음을 클릭합니다.

- CUCM 비디오/음성
- CUCM IM and Presence

단계 **4** 서버 구성 창에서 서버 설정을 적절히 입력합니다.

서버 구성 필드에 대한 설명은 서버 설정을 참조하십시오.

단계 **5** 저장을 클릭합니다.

Presence 서버 상태 보기

Cisco Unified Communications Manager 관리를 사용하여 IM and Presence Service 노드의 중요 서비스 및 셀프 진단 테스트 결과에 대한 상태를 확인합니다.

프로시저

단계 **1** 시스템 > 서버를 선택합니다.

서버 찾기 및 나열 창이 나타납니다.

단계 **2** 서버 검색 파라미터를 선택한 다음 찾기를 클릭합니다.

일치하는 레코드가 나타납니다.

단계 **3** 서버 찾기 및 나열 창에 나열되는 IM and Presence 서버를 선택합니다.

서버 구성 창이 나타납니다.

단계 **4** 서버 구성 창의 [IM and Presence 서버 정보] 섹션에서 [Presence 서버 상태] 링크를 클릭합니다.

서버에 대한 노드 세부 정보 창이 표시됩니다.

포트 구성

이 절차를 사용하여 SCCP 장치 등록, SIP 장치 등록 및 MGCP 게이트웨이 연결과 같이 연결에 사용되는 포트 설정을 변경합니다.

참고 일반적으로 기본 포트 설정을 변경할 필요가 없습니다. 기본값을 변경하려는 경우에만 이 절차를 사용합니다.

프로시저

단계 **1** Cisco Unified Communications Manager Administration에서 시스템 > **Cisco Unified CM**을 선택합니다.
Cisco Unified CM 찾기 및 나열 창이 나타납니다.

단계 **2** 적절한 검색 조건을 입력하고 찾기를 클릭합니다.
일치하는 모든 Cisco Unified Communication Manager가 표시됩니다.

단계 **3** 보려는 **Cisco Unified CM**을 선택합니다.
Cisco Unified CM 구성 창이 나타납니다.

단계 **4** 이 서버에 대한 **Cisco Unified Communications Manager TCP** 포트 설정 섹션으로 이동합니다.

단계 **5** 저장을 클릭합니다.

단계 **6** 구성 적용을 클릭합니다.

단계 **7** 확인을 클릭합니다.

포트 설정

필드	설명
이더넷 전화 포트	시스템은 이 TCP 포트를 사용하여 네트워크에서 Cisco Unified IP Phone(SCCP 전용)과 통신합니다. • 시스템에 이 포트를 이미 사용하고 있지 않는 한, 2000을 기본 포트 값으로 수락합니다. 2000을 선택하면 이 포트가 비보안으로 식별됩니다. • 모든 포트 항목은 고유해야 합니다. • 올바른 포트 번호는 1024부터 49151까지입니다.

필드	설명
MGCP 수신 포트	시스템은 이 TCP 포트를 사용하여 연결된 MGCP 게이트웨이에서 메시지를 검색합니다. • 시스템에 이 포트를 이미 사용하고 있지 않는 한, 2427을 기본 포트로 수락합니다. • 모든 포트 항목은 고유해야 합니다. • 올바른 포트 번호는 1024부터 49151까지입니다.
MGCP Keep-alive 포트	시스템은 이 TCP 포트를 사용하여 KeepAlive 메시지를 연결된 MGCP 게이트웨이와 교환합니다. • 시스템에 이 포트를 이미 사용하고 있지 않는 한, 2428을 기본 포트로 수락합니다. • 모든 포트 항목은 고유해야 합니다. • 올바른 포트 번호는 1024부터 49151까지입니다.
SIP 전화기 포트	이 필드는 Unified Communications Manager가 TCP 및 UDP를 통해 SIP 회선 등록을 수신하는 데 사용하는 포트 번호를 지정합니다.
SIP 전화기 보안 포트	이 필드는 시스템이 TLS를 통해 SIP 회선 등록을 수신하는 데 사용하는 포트 번호를 지정합니다.
SIP 전화기 OAuth 포트	이 필드는 Cisco Unified Communications Manager가 TLS(Transport Layer Security)를 통해 Jabber 온-프레미스 장치에서 SIP 회선 등록을 수신하는 데 사용하는 포트 번호를 지정합니다. 기본값은 5090입니다. 범위는 1024 ~ 49151입니다.
SIP 모바일 및 Remote Access OAuth 포트	이 필드는 Cisco 통합 커뮤니케이션 매니저가 MTLS(Mutual Transport Layer Security)를 통해 Jabber 온-프레미스Jabber over Expressway에서 SIP 회선 등록을 수신하는 데 사용하는 포트 번호를 지정합니다. 기본값은 5091입니다. 범위는 1024 ~ 49151입니다.

호스트 이름 구성

다음 표에는 통합 커뮤니케이션 매니저 서버의 호스트네임을 설정할 수 있는 위치, 호스트네임에 허용되는 문자 수, 호스트네임에 권장되는 첫 번째 문자와 마지막 문자가 열거되어 있습니다. 호스트네임을 정확히 설정하지 않을 경우 운영체제, 데이터베이스, 설치 등을 포함해 통합 커뮤니케이션 매니저의 일부 설정요소가 예상대로 작동하지 않을 수 있다는 점에 유의하십시오.

표 ***73: Cisco Unified Communications Manager***에서 호스트 이름 구성

호스트 이름 위치	허용되는 구성	허용되는 문자 수	호스트 이름에 권장되는 첫 번째 문자	호스트 이름에 권장되는 마지막 문자
호스트 이름/IP 주소 필드 Cisco Unified Communications Manager Administration의 시스템 > 서버	클러스터에서 서버의 호스트 이름을 추가 또는 변경할 수 있습니다.	2-63	영문자	영숫자
호스트 이름 필드 Cisco Unified Communications Manager 설치 마법사	클러스터에서 서버의 호스트 이름을 추가할 수 있습니다.	1-63	영문자	영숫자
호스트 이름 필드 Cisco Unified Communications 운영 체제의 설정 > **IP** > 이더넷	클러스터에서 서버의 호스트 이름을 변경할 수 있으며 추가할 수는 없습니다.	1-63	영문자	영숫자
set network hostname hostname 명령줄 인터페이스	클러스터에서 서버의 호스트 이름을 변경할 수 있으며 추가할 수는 없습니다.	1-63	영문자	영숫자

팁 호스트 이름은 ARPANET 호스트 이름에 대한 규칙을 따라야 합니다. 호스트 이름의 첫 번째 문자와 마지막 문자 사이에 영숫자와 하이픈을 입력할 수 있습니다.

모든 위치에서 호스트 이름을 구성하기 전에 다음 정보를 검토합니다.

- 디바이스-서버, 애플리케이션-서버 및 서버-서버 통신을 지원하는 서버 구성 창의 호스트 이름/IP 주소 필드를 사용하면 점으로 구분된 형식의 IPv4주소 또는 호스트 이름을 입력할 수 있습니다.

  Unified Communications Manager 게시자 노드를 설치한 후에 게시자의 호스트 이름이 이 필드에 자동으로 표시됩니다. Unified Communications Manager 가입자 노드를 설치하기 전에 Unified Communications Manager 게시자 노드에서 이 필드에 가입자 노드의 IP 주소 또는 호스트 이름을 입력합니다.

  이 필드에 Unified Communications Manager가 DNS 서버에 액세스하여 IP 주소에 대한 호스트 이름을 확인할 수 있는 경우에만 호스트 이름을 구성합니다. 반드시 DNS 서버에서 Cisco Unified Communications Manager 이름과 주소 정보를 구성해야 합니다.

팁 DNS 서버에서 Unified Communications Manager 정보를 구성하는 것 외에도 Cisco Unified Communications Manager를 설치하는 동안 DNS 정보를 입력합니다.

- Unified Communications Manager 게시자 노드를 설치하는 동안 정적 네트워킹을 사용하려는 경우 필수인 호스트 이름과 게시자 노드의 IP 주소를 입력하여 네트워크 정보를 구성합니다.

  통합 커뮤니케이션 매니저 가입자 노드를 설치할 때 통합 커뮤니케이션 매니저 퍼블리셔 노드의 호스트네임과 IP 주소를 입력해야만 통합 커뮤니케이션 매니저가 네트워크 연결 및 퍼블리셔-가입자의 유효성을 확인할 수 있습니다. 뿐만 아니라, 가입자 노드에 대한 호스트 이름 및 IP 주소를 입력해야 합니다. Unified Communications Manager 설치 프로그램에서 가입자 서버의 호스트 이름을 묻는 메시지를 표시하는 경우 호스트 이름/IP 주소 필드에 가입자 서버의 호스트 이름을 구성했으면 Cisco Unified Communications Manager 관리의 서버 구성 창에 표시되는 값을 입력합니다.

kerneldump 유틸리티

kerneldump 유틸리티를 사용하면 보조 서버를 요구하지 않고 영향을 받는 시스템에서 로컬로 크래시 덤프 로그를 수집할 수 있습니다.

Unified Communications Manager 클러스터에서 크래시 덤프 정보를 수집하기 전에 서버에서 kerneldump 유틸리티가 활성화되어 있어야 합니다.

참고 더 효율적인 문제 해결을 위해 Unified Communications Manager를 설치한 후 kerneldump 유틸리티가 활성화되어 있는지 확인하는 것이 좋습니다. 아직 수행하지 않은 경우, 지원되는 어플라이언스 릴리스에서 Unified Communications Manager를 업그레이드하기 전에 kerneldump 유틸리티를 활성화합니다.

중요 kerneldump 유틸리티를 활성화하거나 비활성화하면 노드를 재부팅해야 합니다. 재부팅이 허용되는 창 내에 있지 않은 경우에는 enable 명령을 실행하지 마십시오.

Cisco Unified Communications 운영 체제에 대한 CLI(명령줄 인터페이스)를 사용하여 kerneldump 유틸리티의 상태를 활성화, 비활성화 또는 확인할 수 있습니다.

다음 절차를 사용하여 커널 덤프 유틸리티를 활성화합니다.

유틸리티에서 수집한 파일을 사용하여 작업

kerneldump 유틸리티에서 충돌 정보를 보려면 *Cisco Unified Real-Time Monitoring Tool* 또는 CLI(명령줄 인터페이스)를 사용하십시오. *Cisco Unified Real-Time Monitoring Tool*를 사용하여 kerneldump 로그를 수집하려면 추적 및 로그 센트럴에서 파일 수집 옵션을 선택합니다. 시스템 서비스/애플리케이션 탭에서 Kerneldump 로그 확인란을 선택합니다. *Cisco Unified Real-Time Monitoring Tool* 사용에 대한 자세한 내용은 *Cisco Unified Real-Time Monitoring Tool* 관리 지침서를 참조하십시오.

CLI를 사용하여 kerneldump 로그를 수집하려면 충돌 디렉터리의 파일에 대한 “file” CLI 명령을 사용합니다. 이러한 항목은 “activelog” 파티션 아래에 있습니다. 로그 파일 이름은 kerneldump 클라이언트

의 IP 주소로 시작하여 파일을 만든 날짜로 끝납니다. file 명령에 대한 자세한 내용은 *Cisco Unified Solutions*용 명령줄 인터페이스 설명서를 참조하십시오.

Kerneldump 유틸리티 활성화

이 절차를 사용하여 kerneldump 유틸리티를 활성화합니다. 커널 충돌이 발생하는 경우 유틸리티는 충돌을 수집하고 덤프하는 메커니즘을 제공합니다. 로컬 서버 또는 외부 서버에 로그를 덤프하도록 유틸리티를 구성할 수 있습니다.

프로시저

단계 **1** 명령줄 인터페이스에 로그인합니다.

단계 **2** 다음 중 하나를 완료합니다.

- 로컬 서버에서 커널 충돌을 덤프하려면 `utils os kerneldump enable` CLI 명령을 실행합니다.
- 외부 서버에 커널 충돌을 덤프하려면 외부 서버의 IP 주소를 사용하여 `utils os kerneldump ssh enable <ip_address>` CLI 명령을 실행합니다.

단계 **3** 서버를 재부팅합니다.

예

참고 kerneldump 유틸리티를 비활성화해야 하는 경우에는 `utils os kernelcrash disable` CLI 명령을 실행하여 코어 덤프에 대한 로컬 서버를 비활성화하고 `utils os kerneldump ssh disable <ip_address>` CLI 명령을 사용하여 외부 서버에서 유틸리티를 비활성화할 수 있습니다.

다음에 수행할 작업

Real Time Monitoring Tool에서 이메일 경고를 구성하여 코어 덤프에 대해 알려줍니다. 자세한 내용은 핵심 덤프에 대한 이메일 경고 활성화, 280 페이지을 참조하십시오.

kerneldump 유틸리티 및 문제 해결에 관한 자세한 내용은 *Cisco Unified Communications Manager*용 문제 해결 설명서를 참조하십시오.

핵심 덤프에 대한 이메일 경고 활성화

이 절차를 사용하여 핵심 덤프가 발생할 때마다 관리자에게 이메일을 보낼 수 있도록 실시간 모니터링 도구를 구성할 수 있습니다.

프로시저

단계 **1** 시스템 > 도구 > 알림 > 알림 센트럴을 선택합니다.

단계 **2** **CoreDumpFileFound** 알림을 마우스 오른쪽 버튼으로 클릭하고 알림 속성 설정을 선택합니다.

단계 **3** 마법사 프롬프트에 따라 기본 설정 기준을 설정합니다.

a) 알림 속성**:** 이메일 알림 팝업에서 이메일 활성화가 선택되어 있는지 확인하고 구성을 클릭하여 관리자에게 이메일을 보낼 기본 알림 작업을 설정합니다.
b) 프롬프트에 따라 수신자 이메일 주소를 추가합니다. 이 알림이 트리거되면 기본 동작은 이 주소로 이메일을 전송합니다.
c) 저장을 클릭합니다.

단계 **4** 기본 이메일 서버를 설정합니다.

a) 시스템 > 도구 > 알림 > 이메일 서버 구성을 선택합니다.
b) 이메일 알림을 전송하려면 이메일 서버 및 포트 정보를 입력합니다.
c) 전송 사용자 **ID**를 입력합니다.
d) 확인을 클릭합니다.

V 부

보고서 관리

- Cisco 서비스 가용성 리포터, 285 페이지
- Cisco Unified Reporting, 305 페이지
- Cisco IP 전화기에 대한 통화 진단 및 품질 보고 구성, 317 페이지

20 장

Cisco 서비스 가용성 리포터

- 서비스 가용성 보고서 아카이브, 285 페이지
- Cisco 서비스 가용성 리포터 구성 작업 흐름, 286 페이지
- 일별 보고서 요약, 288 페이지

서비스 가용성 보고서 아카이브

Cisco 서비스 가용성 리포터 서비스에서는 특정 보고서에 대한 통계 요약을 표시 하는 차트를 포함하는 일별 보고서를 생성합니다. 리포터는 로그 정보를 기준으로 하루에 한 번 보고서를 생성합니다.

서비스 가용성 GUI를 사용하여 도구 > 서비스 가용성 보고서 아카이브에서 보고서를 봅니다. 보고서를 보려면 Cisco 서비스 가용성 리포터 서비스를 활성화해야 합니다. 서비스를 활성화한 후 보고서 생성에는 24시간이 걸릴 수 있습니다.

보고서에는 이전 날짜에 대한 24시간 데이터가 포함됩니다. 보고서 이름에 추가되는 접미사는 리포터가 보고서를 생성한 날짜를 보여줍니다(예: AlertRep_mm_dd_yyyy.pdf). 서비스 가용성 보고서 아카이브 창에서는 이 날짜를 사용하여 관련 날짜에 대한 보고서만 표시합니다. 보고서는 이전 날짜의 타임 스탬프를 사용하여 로그 파일에 있는 데이터에서 생성됩니다. 시스템은 현재 날짜와 이전 이틀 동안의 로그 파일 데이터를 수집합니다.

보고서에 표시되는 시간은 서버 "시스템 시간"을 반영합니다.

보고서를 생성하는 동안 서버에서 로그 파일을 검색할 수 있습니다.

참고 Cisco Unified Reporting 웹 애플리케이션에서는 데이터의 스냅숏 보기를 한 출력에 제공하고 데이터 검사를 실행합니다. 이 애플리케이션을 사용하여 생성된 보고서를 보관할 수 있습니다. 자세한 내용은 *Cisco Unified Reporting* 관리 설명서를 참조하십시오.

클러스터 구성에 대한 서비스 가용성 보고서 아카이브 고려 사항

이 섹션은 Unified Communications Manager 및 IM and Presence Service에만 적용됩니다.

- Cisco 서비스 가용성 리포터는 첫 번째 서버에서만 활성화되므로 언제든지 리포터는 다른 서버가 아닌 첫 번째 서버에만 보고서를 생성합니다.

- 보고서에 표시되는 시간은 첫 번째 서버 "시스템 시간"을 반영합니다. 첫 번째 서버와 후속 서버가 서로 다른 시간대에 있는 경우 첫 번째 서버 "시스템 시간"이 보고서에 표시됩니다.
- 클러스터의 서버 위치 간 시간대 차이는 보고서에 대한 데이터가 수집될 때 고려됩니다.
- 보고서를 생성할 때 개별 서버 또는 클러스터의 모든 서버에서 로그 파일을 선택할 수 있습니다.
- Cisco Unified Reporting 웹 애플리케이션 출력 및 데이터 검사에는 모든 액세스 가능한 서버의 클러스터 데이터가 포함됩니다.

Cisco 서비스 가용성 리포터 구성 작업 흐름

이 작업을 완료하여 Cisco 서비스 가용성 리포터를 통해 일일 시스템 보고서를 설정합니다.

프로시저

	명령 또는 동작	목적
단계 **1**	Cisco 서비스 가용성 리포터 활성화, 286 페이지	일별 보고서를 생성하려면 **Cisco** 서비스 가용성 리포터 서비스를 실행하고 있어야 합니다.
단계 **2**	Cisco 서비스 가용성 리포터 설정 구성, 287 페이지	Cisco 서비스 가용성 리포터에 대한 예약 설정을 구성합니다.
단계 **3**	일별 보고서 아카이브 보기, 287 페이지	시스템에서 일별 보고서를 생성한 후에는 이 작업을 사용하여 일별 보고서를 PDF 파일로 볼 수 있습니다.

Cisco 서비스 가용성 리포터 활성화

이 절차를 사용하여 **Cisco** 서비스 가용성 리포터를 통해 일별 시스템 보고 기능을 켭니다. 보고서를 생성하려면 서비스가 활성화되어 있어야 합니다.

프로시저

단계 **1** Cisco Unified 서비스 가용성에서 도구 > 서비스 활성화를 선택합니다.
단계 **2** 서버를 선택하고 이동을 클릭합니다.
단계 **3** 성능 및 모니터링 서비스에서 **Cisco** 서비스 가용성 리포터 서비스의 상태를 확인합니다.
단계 **4** 서비스가 비활성화된 경우 옆의 라디오 버튼을 선택하고 저장을 클릭합니다.

참고 보고서는 매일 생성됩니다. 첫 번째 보고서를 생성 하는 데는 최대 24시간이 걸릴 수 있습니다.

Cisco 서비스 가용성 리포터 설정 구성

Cisco 서비스 가용성 리포터에서 생성되는 일별 보고서에 대한 일정 설정을 구성합니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 시스템 > 서비스 매개 변수를 선택합니다.

단계 **2** Cisco 서비스 가용성 리포터를 실행 중인 서버를 선택합니다.

단계 **3** 서비스 드롭다운에서 Cisco 서비스 가용성 리포터를 선택합니다.

단계 **4** 다음 서비스 매개 변수에 대한 설정을 구성합니다.

- **RTMT** 리포터 지정 노드 - RTMT 리포터가 실행되는 지정된 노드를 지정합니다. 비 통화 처리 노드를 할당하는 것이 좋습니다.
- 보고서 생성 시간 - 보고서가 생성하는 자정 이후 시간(분)입니다. 범위는 0 ~ 1439이고 기본 설정은 30분입니다.
- 보고서 삭제 기간 — 보고서가 디스크에 저장되는 일 수입니다. 범위는 0-30이며 기본 설정은 7일입니다.

단계 **5** 저장을 클릭합니다.

일별 보고서 아카이브 보기

Cisco 서비스 가용성 보고에서 일별 보고서를 생성한 후에는 이 절차를 사용하여 PDF 파일의 보고서를 봅니다.

프로시저

단계 **1** 도구 > 서비스 가용성 보고서 아카이브를 선택합니다.

단계 **2** 보고서를 표시할 월과 연도를 선택합니다.
해당 월에 해당하는 일 목록이 표시됩니다.

단계 **3** 생성된 보고서를 보려는 날을 클릭합니다.

단계 **4** 보려는 보고서를 클릭합니다.

참고 PDF 보고서를 보려면 Acrobat Reader가 시스템에 설치되어 있어야 합니다. 서비스 가용성 보고서 아카이브 창의 맨 아래에 있는 링크를 클릭하여 Acrobat Reader를 다운로드할 수 있습니다.

일별 보고서 요약

Cisco 서비스 가용성 리포터는 다음 일별 시스템 보고서를 생성합니다.

- 장치 통계 보고서
- 서버 통계 보고서
- 서비스 통계 보고서
- 통화 활동 보고서
- 알림 요약 보고서
- 성능 보호 보고서

장치 통계 보고서

장치 통계 보고서는 IM and Presence Service 및 Cisco Unity Connection에는 적용되지 않습니다.

장치 통계 보고서는 다음의 선형 차트를 제공합니다.

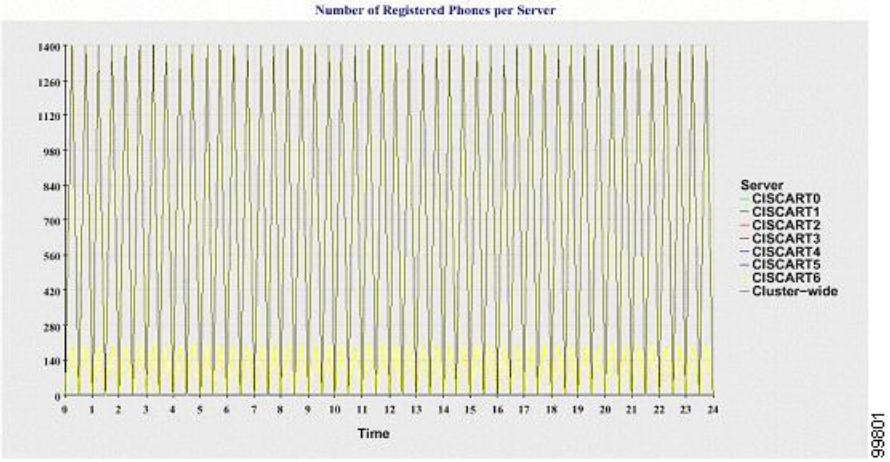
- 서버당 등록된 전화기 수
- 클러스터의 H.323 게이트웨이 수
- 클러스터의 트렁크 수

서버당 등록된 전화기 수

선형 차트는 각 Unified Communications Manager 서버(및 Unified Communications Manager 클러스터 구성의 클러스터)에 대해 등록된 전화기 수를 표시합니다. 차트의 각 선은 데이터를 사용할 수 있는 서버에 대한 데이터를 나타내고 추가 선 하나는 클러스터 수준 데이터를 표시합니다(Unified Communications Manager 클러스터에만 해당). 차트의 각 데이터 값은 15분 동안 등록된 평균 전화기 수를 나타냅니다. 서버에 데이터가 표시되지 않으면 리포터에서 해당 서버를 나타내는 선을 생성하지 않습니다. 서버(또는 Unified Communications Manager 클러스터 구성의 모든 서버)에 대한 데이터가 없는 경우, 등록된 전화기의 경우 리포터는 차트를 생성하지 않습니다. “사용 가능한 장치 통계 보고서에 대한 데이터 없음” 메시지가 표시됩니다.

그림 ***4:*** 서버당 등록된 전화기 수를 보여주는 선형 차트

다음 그림은 Unified Communications Manager 클러스터 구성에서 Unified Communications Manager 서버당 등록된 전화기 수를 나타내는 선형 차트의 예를 보여줍니다.

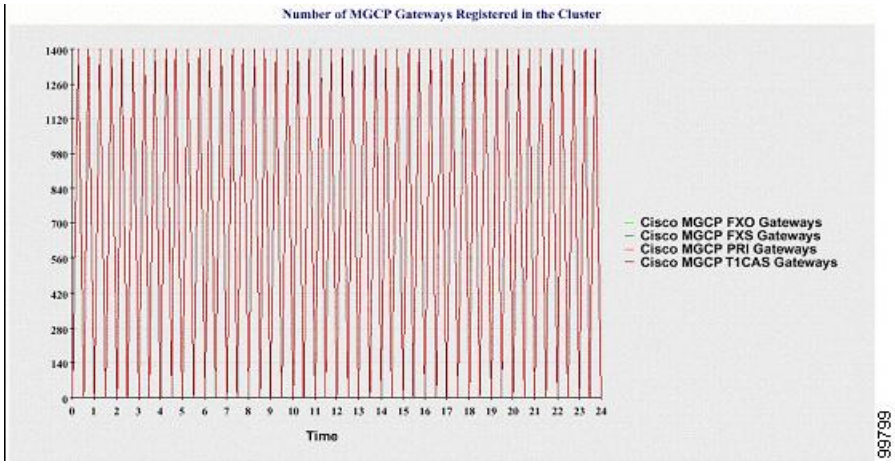


클러스터에 등록된 **MGCP** 게이트웨이 수

선형 차트에는 등록된 MGCP FXO, FXS, PRI 및 T1CAS 게이트웨이의 수가 표시됩니다. 각 선은 Unified Communications Manager 서버(또는 Unified Communications Manager 클러스터 구성의 클러스터)에 대한 데이터만 나타냅니다. 따라서 4개의 선은 각 게이트웨이 유형에 대한 서버(또는 클러스터 수준) 세부 정보를 보여줍니다. 차트의 각 데이터 값은 15분 동안 등록된 평균 MGCP 게이트웨이 수를 나타냅니다. 서버(또는 클러스터의 모든 서버)용 게이트웨이에 대한 데이터가 없는 경우 리포터는 특정 게이트웨이에 대한 데이터를 나타내는 선을 생성하지 않습니다. 서버(또는 클러스터의 모든 서버)용 모든 게이트웨이에 대한 데이터가 없는 경우에는 리포터에서 차트를 생성하지 않습니다.

그림 ***5:*** 클러스터당 등록된 게이트웨이 수를 보여주는 선형 차트

다음 그림은 Unified Communications Manager 클러스터 구성에서 클러스터당 등록된 게이트웨이 수를 나타내는 선형 차트의 예를 보여줍니다.



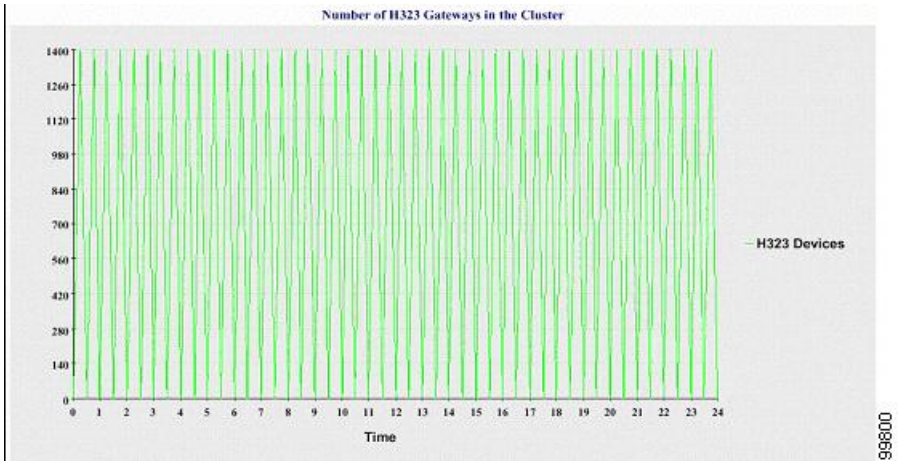
클러스터의 **H.323** 게이트웨이 수

선형 차트에는 H.323 게이트웨이 수가 표시됩니다. 하나의 선은 H.323 게이트웨이에 대한 세부 정보(또는 Unified Communications Manager 클러스터 구성의 클러스터 수준 세부 정보)를 나타냅니다. 차트의 각 데이터 값은 15분 동안 H.323 게이트웨이의 평균 수를 나타냅니다. 서버(또는 클러스터의 모

든 서버)에 대한 H.323 게이트웨이에 대한 데이터가 없는 경우에는 리포터에서 차트를 생성하지 않습니다.

그림 ***6:*** 클러스터당 등록된 ***H.323*** 게이트웨이 수를 보여 주는 선형 차트

다음 그림은 Unified Communications Manager 클러스터 구성에서 클러스터당 H.323 게이트웨이 수를 나타내는 선형 차트의 예를 보여줍니다.

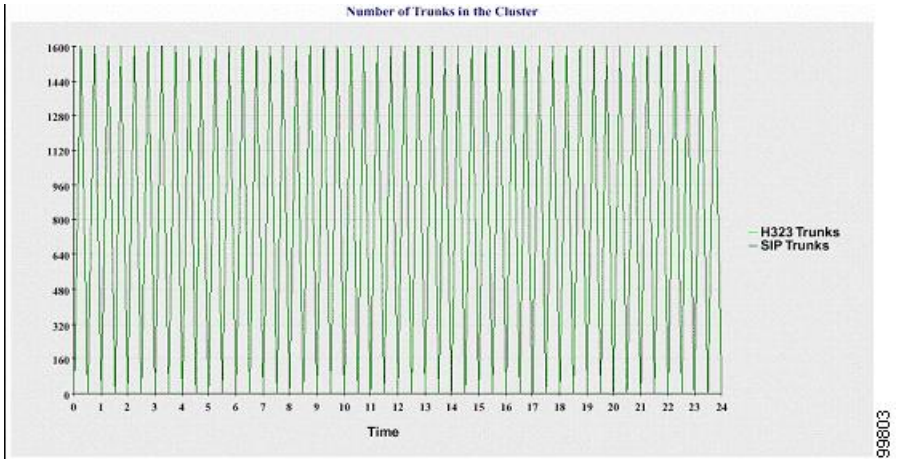


클러스터의 트렁크 수

선형 차트에는 H.323 및 SIP 트렁크의 수가 표시됩니다. 두 개의 선은 H.323 트렁크 및 SIP 트렁크에 대한 세부 정보(또는 Unified Communications Manager 클러스터 구성의 클러스터 수준 세부 정보)를 나타냅니다. 차트의 각 데이터 값은 15분 동안의 평균 H.323 및 SIP 트렁크 수를 나타냅니다. 서버(또는 클러스터의 모든 서버)의 H.323 트렁크에 대한 데이터가 없는 경우에는 리포터가 H.323 트렁크에 대한 데이터를 나타내는 선을 생성하지 않습니다. 서버(또는 클러스터의 모든 서버)의 SIP 트렁크에 대한 데이터가 없는 경우 리포터는 SIP 트렁크에 대한 데이터를 나타내는 선을 생성하지 않습니다. 트렁크에 대한 데이터가 전혀 없는 경우에는 리포터에서 차트를 생성하지 않습니다.

그림 ***7:*** 클러스터당 트렁크 수를 보여주는 선형 차트

다음 그림은 Unified Communications Manager 클러스터 구성에서 클러스터당 트렁크 수를 나타내는 선형 차트의 예를 보여줍니다.



서버(또는 클러스터의 각 서버)에 파일 이름 패턴 DeviceLog_mm_dd_yyyy_hh_mm.csv와 일치하는 로그 파일이 포함되어 있습니다. 다음 정보가 로그 파일에 있습니다.

- 서버(또는 Unified Communications Manager 클러스터의 각 서버)에 등록된 전화기 수
- 서버(또는 Unified Communications Manager 클러스터의 각 서버)에 등록된 MGCP FXO, FXS, PRI 및 T1CAS 게이트웨이 수
- 서버(또는 Unified Communications Manager 클러스터의 각 서버)에 등록된 H.323 게이트웨이 수
- SIP 트렁크 및 H.323 트렁크 수

서버 통계 보고서

서버 통계 보고서는 다음의 선형 차트를 제공합니다.

- 서버당 CPU 백분율
- 서버당 메모리 사용량 백분율
- 서버당 가장 큰 파티션의 하드 디스크 사용량 백분율

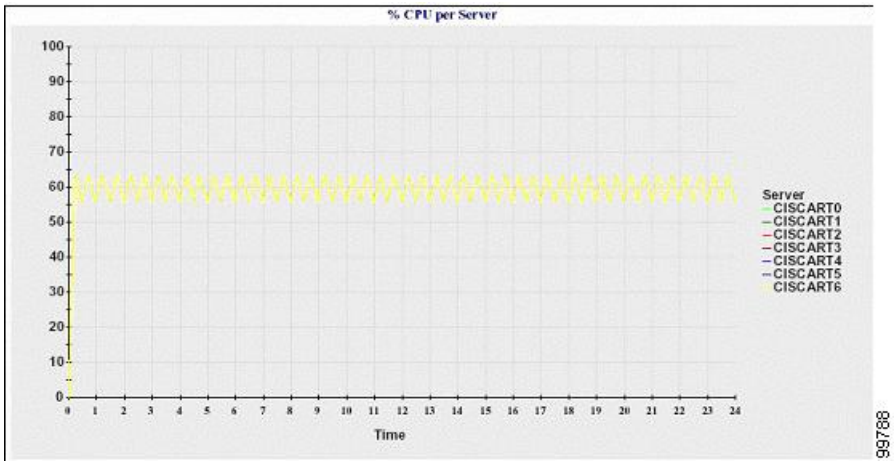
클러스터별 통계는 Unified Communications Manager 및 IM and Presence Service에서만 지원됩니다.

서버당 **CPU** 백분율

선형 차트에는 서버의 CPU 사용량 백분율(또는 클러스터의 각 서버에 대한 백분율)이 표시됩니다. 차트의 선은 데이터를 사용할 수 있는 서버(또는 클러스터의 각 서버에 대해 하나의 선)에 대한 데이터를 나타냅니다. 차트의 각 데이터 값은 15분 동안의 평균 CPU 사용량을 나타냅니다. 서버(또는 클러스터의 한 서버)에 대한 데이터가 없는 경우에는 리포터에서 해당 서버를 나타내는 선이 생성되지 않습니다. 생성할 선이 없는 경우에는 리포터에서 차트를 만들지 않습니다. “사용 가능한 서버 통계 보고서에 대한 데이터 없음” 메시지가 표시됩니다.

그림 ***8:*** 서버당 ***CPU*** 백분율을 보여 주는 선형 차트

다음 그림은 Unified Communications Manager 클러스터 구성에서 서버당 CPU 사용량 백분율을 나타내는 선형 차트의 예를 보여줍니다.

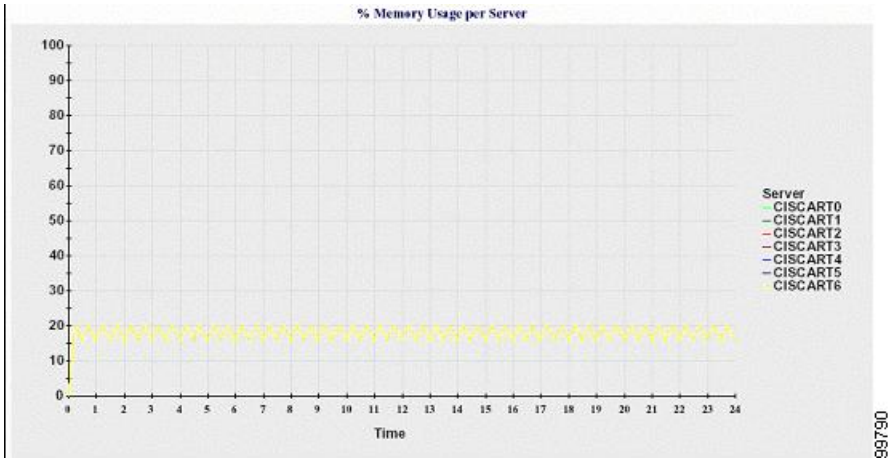


서버당 메모리 사용량 백분율

선형 차트에는 Unified Communications Manager 서버(%MemoryInUse)에 대한 메모리 사용량 백분율이 표시됩니다. Unified Communications Manager 클러스터 구성에서 데이터를 사용할 수 있는 클러스터의 서버당 한 개의 선이 있습니다. 차트의 각 데이터 값은 15분 동안의 평균 메모리 사용량을 나타냅니다. 데이터가 없는 경우에는 리포터가 차트를 생성하지 않습니다. 클러스터 구성에서 서버에 대한 데이터가 없는 경우 리포터는 해당 서버를 나타내는 선을 생성하지 않습니다.

그림 *9:* 서버당 메모리 사용량 백분율을 보여 주는 선형 차트

다음 그림은 클러스터 구성에서 Unified Communications Manager 서버당 메모리 사용량의 백분율을 나타내는 선형 차트의 예를 보여줍니다.

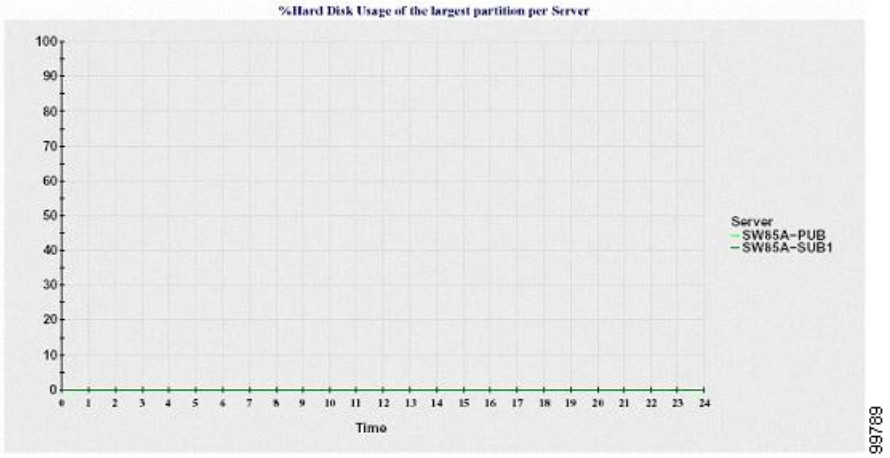


서버당 가장 큰 파티션의 하드 디스크 사용량 백분율

선형 차트는 서버(%DiskSpaceInUse)의 가장 큰 파티션에 대한 디스크 공간 사용량의 백분율 또는 클러스터 구성의 각 서버에 대한 디스크 공간 사용량의 백분율을 표시합니다. 차트의 각 데이터 값은 15분 동안의 평균 디스크 사용량을 나타냅니다. 데이터가 없는 경우에는 리포터가 차트를 생성하지 않습니다. 클러스터 구성의 한 서버에 대한 데이터가 없는 경우 리포터는 해당 서버를 나타내는 선을 생성하지 않습니다.

그림 *10:* 서버당 가장 큰 파티션의 하드 디스크 사용량 백분율을 보여주는 선형 차트

다음 그림은 Unified Communications Manager 클러스터 구성에서 서버당 가장 큰 파티션에 대한 하드 디스크 사용량의 백분율을 나타내는 선형 차트의 예를 보여줍니다.



서버(또는 클러스터 구성의 각 서버)에 파일 이름 패턴 ServerLog_mm_dd_yyyy_hh_mm.csv와 일치하는 로그 파일이 포함되어 있습니다. 다음 정보가 로그 파일에 있습니다.

- 서버(또는 클러스터의 각 서버)의 CPU 사용량 백분율
- 서버(또는 클러스터의 각 서버)의 메모리 사용량 백분율(%MemoryInUse)
- 서버(또는 클러스터의 각 서버)에서 가장 큰 파티션(%DiskSpaceInUse)의 하드 디스크 사용량 백분율

서비스 통계 보고서

서비스 통계 보고서는 IM and Presence Service 및 Cisco Unity Connection을 지원하지 않습니다.

서비스 통계 보고서는 다음의 선형 차트를 제공합니다.

- Cisco CTI 매니저: 열린 장치 수
- Cisco CTI 매니저: 열린 회선 수
- Cisco TFTP: 요청 수
- Cisco TFTP: 취소된 요청 수

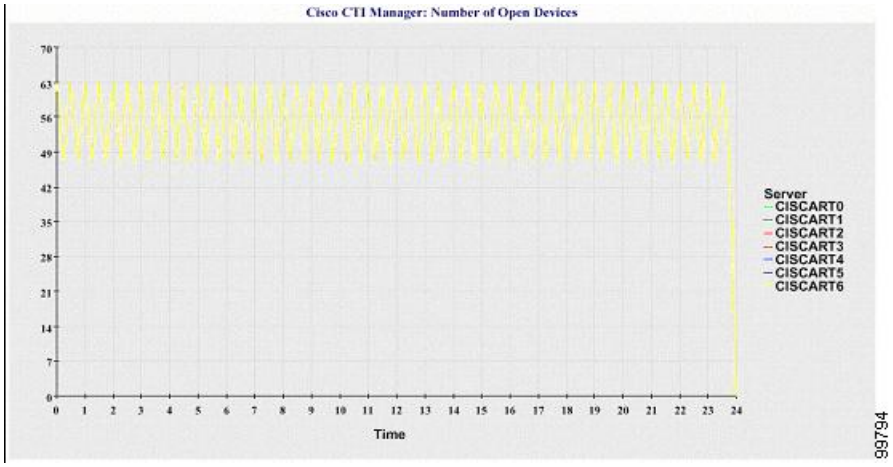
Cisco CTI 매니저**:** 열린 장치 수

선형 차트에 CTI 매니저(또는 Unified Communications Manager 클러스터 구성의 각 CTI 매니저)에 대한 CTI 열린 장치 수가 표시됩니다. 각 선형 차트는 서비스가 활성화되는 서버(또는 Unified Communications Manager 클러스터의 각 서버)에 대한 데이터를 나타냅니다. 차트의 각 데이터 값은 15분 지속 시간 동안 CTI 열린 장치의 평균 개수를 나타냅니다. 데이터가 없는 경우에는 리포터가 차트를 생성하지 않습니다. Unified Communications Manager 클러스터 구성의 한 서버에 대한 데이터가

없는 경우에는 리포터에서 해당 서버를 나타내는 선이 생성되지 않습니다. “사용 가능한 서비스 통계 보고서에 대한 데이터 없음” 메시지가 표시됩니다.

그림 ***11: Cisco CTI*** 매니저*:* 열린 장치 수를 보여주는 선형 차트

다음 그림은 Unified Communications Manager 클러스터 구성에서 Cisco CTI 매니저 당 열린 장치 수를 나타내는 선형 차트의 예를 보여줍니다.

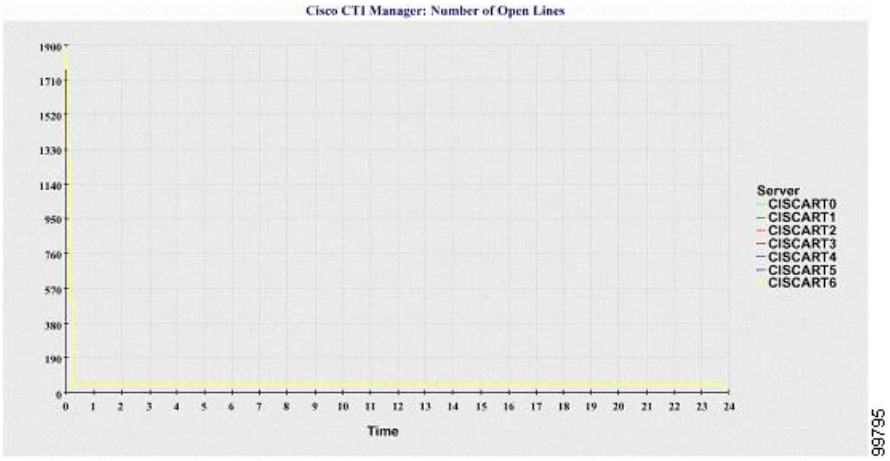


Cisco CTI 매니저**:** 열린 회선 수

선형 차트는 CTI 매니저(또는 Unified Communications Manager 클러스터 구성의 CTI 매니저 별)에 대한 CTI 열린 회선 수를 표시합니다. 차트의 선은 Cisco CTI 매니저 서비스가 활성화된 서버(또는 Unified Communications Manager 클러스터 구성의 각 서버에 대해 하나의 선)에 대한 데이터를 나타냅니다. 차트의 각 데이터 값은 15분 동안 총 CTI 열린 회선 수를 나타냅니다. 데이터가 없는 경우에는 리포터가 차트를 생성하지 않습니다. Unified Communications Manager 클러스터 구성의 한 서버에 대한 데이터가 없는 경우에는 리포터에서 해당 서버를 나타내는 선이 생성되지 않습니다.

그림 ***12: Cisco CTI*** 매니저*:* 열린 회선 수를 보여주는 선형 차트

다음 그림은 Unified Communications Manager 클러스터 구성에서 Cisco CTI 매니저 당 열린 회선 수를 나타내는 선형 차트의 예를 보여줍니다.

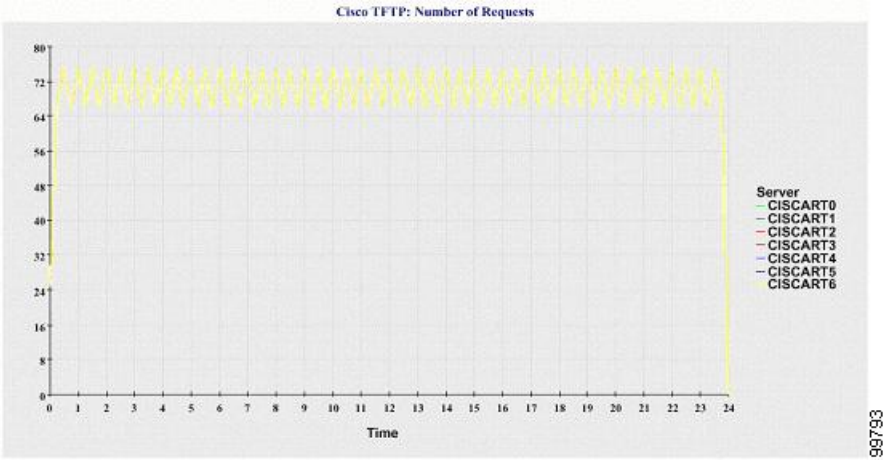


Cisco TFTP: 요청 수

선형 차트는 TFTP 서버(또는 Unified Communications Manager 클러스터 구성의 TFTP 서버 별)에 대한 Cisco TFTP 요청 수를 표시합니다. 차트의 선은 Cisco TFTP 서비스가 활성화된 서버(또는 Unified Communications Manager 클러스터의 각 서버에 대해 하나의 선)에 대한 데이터를 나타냅니다. 차트의 각 데이터 값은 15분 동안의 평균 TFTP 요청 수를 나타냅니다. 데이터가 없는 경우에는 리포터가 차트를 생성하지 않습니다. Unified Communications Manager 클러스터 구성의 한 서버에 대한 데이터가 없는 경우에는 리포터에서 해당 서버를 나타내는 선이 생성되지 않습니다.

그림 ***13: Cisco TFTP:*** 요청 수를 보여주는 선형 차트

다음 그림은 TFTP 서버당 Cisco TFTP 요청 수를 나타내는 선형 차트의 예를 보여줍니다.

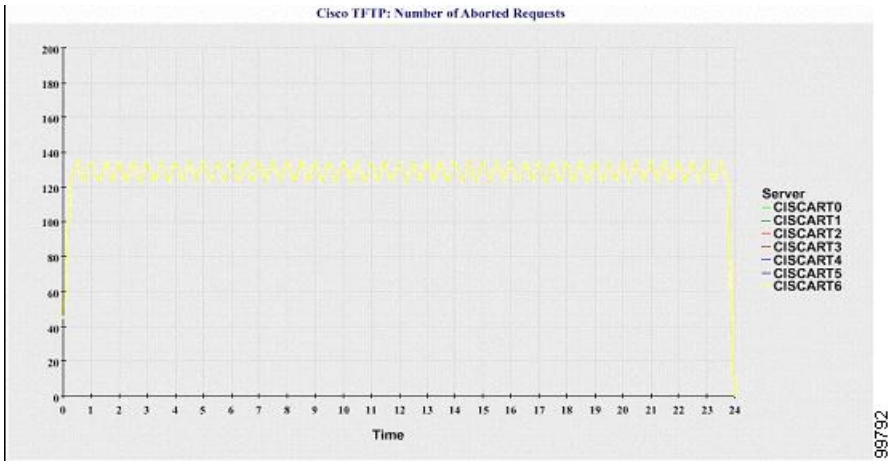


Cisco TFTP: 취소된 요청 수

선형 차트에는 TFTP 서버(또는 Unified Communications Manager 클러스터 구성의 TFTP 서버당)에 대해 중단된 Cisco TFTP 요청 수가 표시됩니다. 차트의 선은 Cisco TFTP 서비스가 활성화된 서버(또는 Unified Communications Manager 클러스터의 각 서버에 대해 하나의 선)에 대한 데이터를 나타냅니다. 차트의 각 데이터 값은 15분 동안 중단된 TFTP 요청의 평균을 나타냅니다. 데이터가 없는 경우에는 리포터가 차트를 생성하지 않습니다. Unified Communications Manager 클러스터 구성의 한 서버에 대한 데이터가 없는 경우에는 리포터에서 해당 서버를 나타내는 선이 생성되지 않습니다.

그림 ***14: Cisco TFTP:*** 중단된 요청 수를 보여주는 선형 차트

다음 그림은 TFTP 서버당 중단된 Cisco TFTP 요청 수를 나타내는 선형 차트의 예를 보여줍니다.



서버(또는 Unified Communications Manager 클러스터의 각 서버)에 파일 이름 패턴 ServiceLog_mm_dd_yyyy_hh_mm.csv와 일치하는 로그 파일이 포함되어 있습니다. 다음 정보가 로그 파일에 있습니다.

- 각 CTI 매니저 - 열린 장치 수
- 각 CTI 매니저 - 열린 회선 수
- 각 Cisco TFTP 서버 - TotalTftpRequests
- 각 Cisco TFTP 서버 - TotalTftpRequestsAborted

통화 활동 보고서

통화 활동 보고서는 IM and Presence Service 및 Cisco Unity Connection을 지원하지 않습니다.

통화 활동 보고서는 다음의 선형 차트를 제공합니다.

- 클러스터에 대한 Unified Communications Manager 통화 활동
- 클러스터에 대한 H.323 게이트웨이 통화 활동
- 클러스터에 대한 MGCP 게이트웨이 통화 활동
- MGCP 게이트웨이
- 클러스터에 대한 트렁크 통화 활동

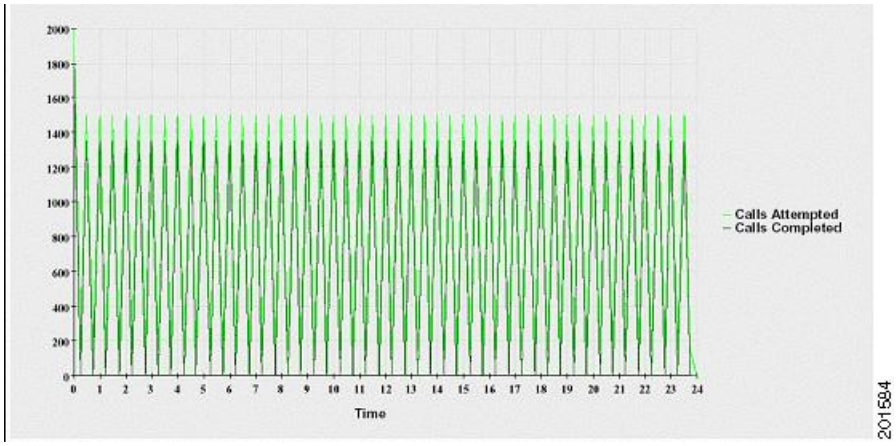
클러스터에 대한 **Cisco Unified Communications Manager** 통화 활동

선형 차트는 시도된 Unified Communications Manager 통화 및 완료된 통화 수를 표시합니다. Unified Communications Manager 클러스터 구성에서 선형 차트는 전체 클러스터에 대해 시도 및 완료된 통화 수를 표시합니다. 이 차트는 시도된 통화 수와 완료된 통화 수에 대해 서로 다른 두 개의 선으로 구성됩니다. Unified Communications Manager 클러스터 구성의 경우 각 선은 클러스터 값(데이터를 사용할 수 있는 클러스터의 모든 서버에 대한 값의 합계)을 나타냅니다. 차트의 각 데이터 값은 시도된 총 통화 수 또는 15분 동안 완료된 통화 수를 나타냅니다.

완료된 Unified Communications Manager 통화에 대한 데이터가 없는 경우, 리포터는 완료된 통화에 대한 데이터를 나타내는 선을 생성하지 않습니다. 시도된 Unified Communications Manager 통화에 대한 데이터가 없는 경우 리포터는 시도된 통화에 대한 데이터를 나타내는 선을 생성하지 않습니다. Unified Communications Manager 클러스터 구성에서 클러스터의 서버에 대한 데이터가 없는 경우, 리포터는 해당 서버에서 시도했거나 완료한 통화를 나타내는 선을 생성하지 않습니다. Unified Communications Manager 통화 활동에 대한 데이터가 전혀 없는 경우 리포터는 차트를 생성하지 않습니다. "사용 가능한 통화 활동 보고서에 대한 데이터 없음" 메시지가 표시됩니다.

그림 ***15:*** 클러스터에 대한 ***Cisco Unified Communications Manager*** 통화 활동을 보여 주는 선형 차트

다음 그림은 Unified Communications Manager 클러스터에 대한 시도 및 완료된 통화 수를 나타내는 선형 차트를 보여줍니다.

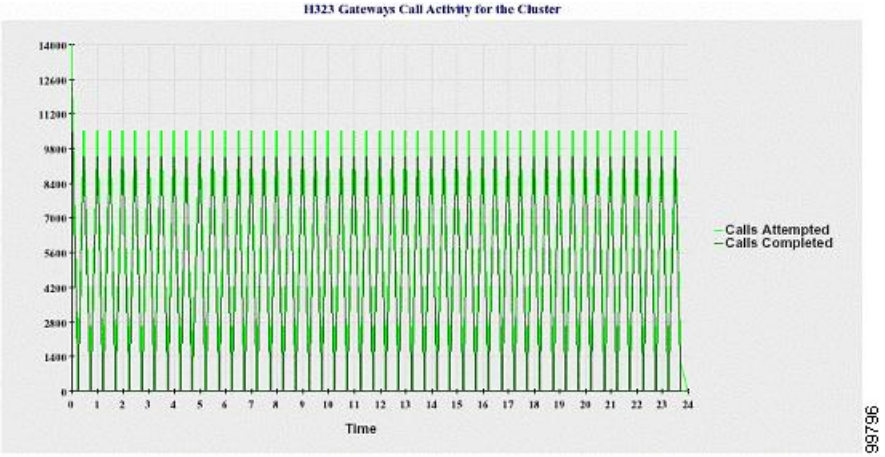


클러스터에 대한 **H.323** 게이트웨이 통화 활동

선형 차트에는 시도된 통화 수와 H.323 게이트웨이에 대해 완료된 통화 수가 표시됩니다. Unified Communications Manager 클러스터 구성에서 선형 차트는 전체 클러스터에 대해 시도 및 완료된 통화 수를 표시합니다. 이 차트는 시도된 통화 수와 완료된 통화 수에 대해 서로 다른 두 개의 선으로 구성됩니다. Unified Communications Manager 클러스터 구성의 경우 각 선은 클러스터 값(데이터를 사용할 수 있는 클러스터의 모든 서버에 대한 값의 합계와 동일)을 나타냅니다. 차트의 각 데이터 값은 시도된 총 통화 수 또는 15분 동안 완료된 통화 수를 나타냅니다. 완료된 H.323 게이트웨이 통화에 대한 데이터가 없는 경우, 리포터는 완료된 통화에 대한 데이터를 나타내는 선을 생성하지 않습니다. 시도된 H.323 게이트웨이 통화에 대한 데이터가 없는 경우 리포터는 시도된 통화에 대한 데이터를 나타내는 선을 생성하지 않습니다. Unified Communications Manager 클러스터 구성에서 클러스터의 서버에 대한 데이터가 없는 경우, 리포터는 해당 서버에서 시도했거나 완료한 통화를 나타내는 선을 생성하지 않습니다. H.323 게이트웨이 통화 활동에 대한 데이터가 전혀 존재하지 않을 경우 리포터는 차트를 생성하지 않습니다.

그림 ***16:*** 클러스터에 대한 ***H.323*** 게이트웨이 통화 활동을 보여 주는 선형 차트

다음 그림은 Unified Communications Manager 클러스터에 대한 H.323 게이트웨이 통화 활동을 나타내는 선형 차트를 보여줍니다.

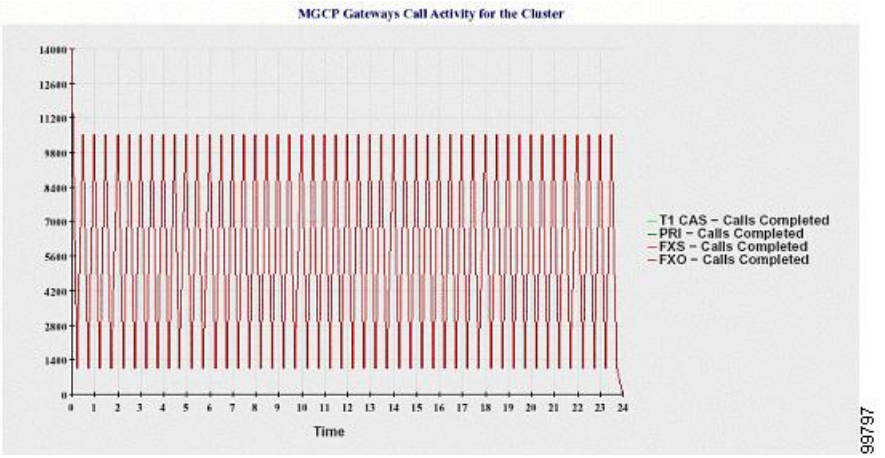


클러스터에 대한 **MGCP** 게이트웨이 통화 활동

선형 차트는 MGCP FXO, FXS, PRI 및 T1CAS 게이트웨이에 대해 한 시간에 완료된 통화 수를 표시합니다. Unified Communications Manager 클러스터 구성에서 차트는 전체 Unified Communications Manager 클러스터에 대해 완료된 통화 수를 표시합니다. 차트는 각 게이트웨이 유형에 대해 완료된 통화 수에 대해 1개씩 최대 4개의 선으로 구성됩니다(데이터를 사용할 수 있는 경우). 차트의 각 데이터 값은 15분 동안 완료된 총 통화 수를 나타냅니다. 게이트웨이에 대한 데이터가 없는 경우 리포터는 특정 게이트웨이에 대해 완료된 통화에 대한 데이터를 나타내는 선을 생성하지 않습니다. 모든 게이트웨이에 데이터가 없는 경우에는 리포터가 차트를 생성하지 않습니다.

그림 ***17:*** 클러스터에 대한 ***MGCP*** 게이트웨이 통화 활동을 보여 주는 선형 차트

다음 그림은 Unified Communications Manager 클러스터에 대한 MGCP 게이트웨이 통화 활동을 나타내는 선형 차트를 보여줍니다.



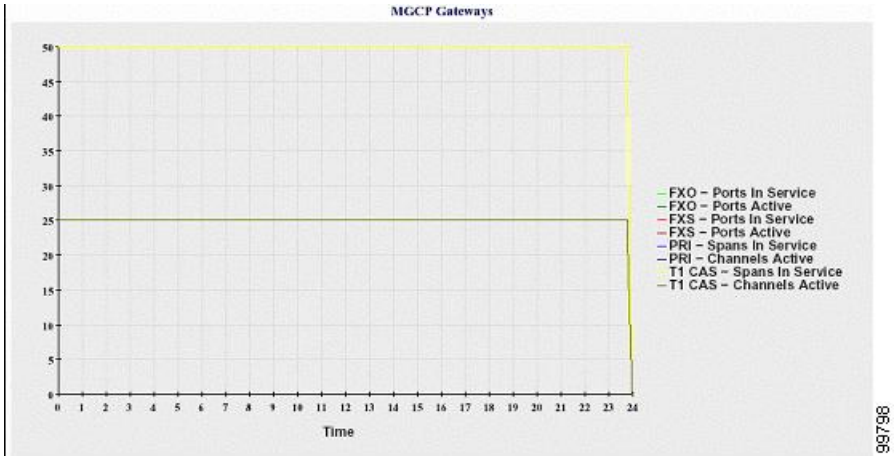
MGCP 게이트웨이

선형 차트는 MGCP FXO, FXS 게이트웨이, 서비스에 있는 범위 수 또는 PRI, T1CAS 게이트웨이의 활성 포트 수를 표시합니다. Unified Communications Manager 클러스터 구성의 경우 차트에 전체 Unified Communications Manager 클러스터에 대한 데이터가 표시됩니다. 이 차트는 8개의 선, 즉 MGCP FXO

및 FXS에 대한 서비스의 포트 수에 각각 2개의 선, MGCP FXO 및 FXS에 대한 활성 포트 수에 각각 2개의 선으로 구성됩니다. 서비스 중인 범위 수와 PRI 및 T1CAS 게이트웨이에 활성화된 채널에 대해 4개 이상의 선이 존재합니다. Unified Communications Manager 클러스터 구성의 경우 각 선은 클러스터 값(데이터를 사용할 수 있는 클러스터의 모든 서버에 대한 값의 합계)을 나타냅니다. 차트의 각 데이터 값은 서비스 중인 총 포트 수, 활성 포트 수, 서비스 중인 범위 또는 15분 동안 활성 상태인 채널을 나타냅니다. 모든 서버에 대한 게이트웨이(MGCP PRI, T1CAS)에 대해 서비스 중인 범위 수 또는 활성 채널에 대한 데이터가 없는 경우 리포터는 특정 게이트웨이의 데이터를 나타내는 선을 생성하지 않습니다.

그림 ***18: MGCP*** 게이트웨이를 보여주는 선형 차트

다음 그림은 MGCP 게이트웨이를 나타내는 선형 차트를 보여줍니다.

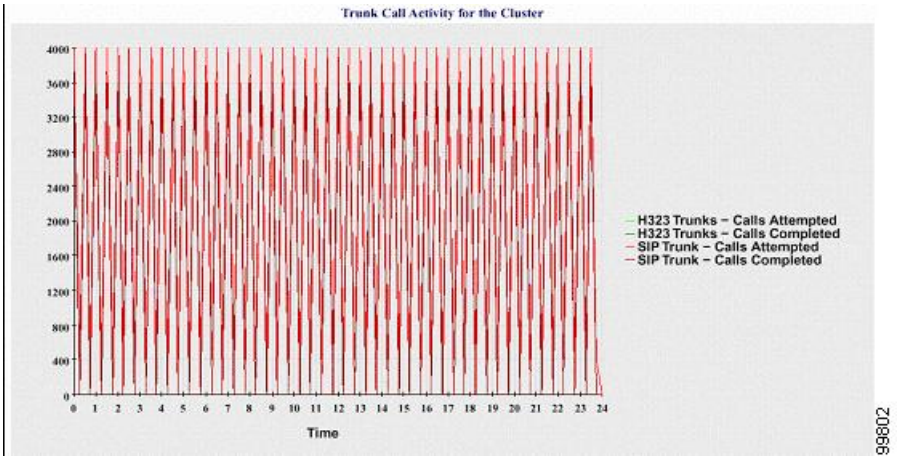


클러스터에 대한 트렁크 통화 활동

선형 차트에는 완료된 통화 수와 SIP 트렁크 및 H.323 트렁크에 대해 한 시간 동안 시도된 통화 수가 표시됩니다. Unified Communications Manager 클러스터 구성의 경우 차트에는 완료된 통화 수와 전체 Unified Communications Manager 클러스터에 대해 시도된 통화 수가 표시됩니다. 이 차트는 4개의 선, 즉 각 SIP 및 H.323 트렁크(데이터를 사용할 수 있는 경우)에 대해 완료된 통화 수에 2개와 시도된 통화 수에 2개의 선으로 구성됩니다. Unified Communications Manager 클러스터 구성의 경우 각 선은 클러스터 값(데이터를 사용할 수 있는 클러스터의 모든 노드에 대한 값의 합계)을 나타냅니다. 차트의 각 데이터 값은 완료된 총 통화 수 또는 15분 동안 시도된 통화 수를 나타냅니다. 트렁크에 대한 데이터가 없는 경우, 리포터는 완료된 통화 또는 해당 특정 트렁크에 대해 시도된 통화에 대한 데이터를 나타내는 선을 생성하지 않습니다. 두 트렁크 유형 모두에 대한 데이터가 없는 경우 리포터가 차트를 생성하지 않습니다.

그림 ***19:*** 클러스터에 대한 트렁크 통화 활동을 보여 주는 선형 차트

다음 그림은 Unified Communications Manager 클러스터에 대한 트렁크 통화 활동을 나타내는 선형 차트를 보여줍니다.



서버(또는 Unified Communications Manager 클러스터 구성의 각 서버)에 파일 이름 패턴 CallLog_mm_dd_yyyy_hh_mm.csv와 일치하는 로그 파일이 포함되어 있습니다. 다음 정보가 로그 파일에 있습니다.

- Unified Communications Manager(또는 Unified Communications Manager 클러스터의 각 서버)에 대해 시도된 통화 및 완료된 통화
- H.323 게이트웨이(또는 Unified Communications Manager 클러스터의 각 서버에 있는 게이트웨이)에 대해 시도된 통화 및 완료된 통화
- MGCP FXO, FXS, PRI 및 T1CAS 게이트웨이(또는 Unified Communications Manager 클러스터의 각 서버에 있는 게이트웨이)에 대해 완료된 통화
- 서비스 중인 포트, MGCP FXO 및 FXS 게이트웨이용 활성 포트 및 서비스 중인 범위, PRI에 활성화된 채널 및 T1CAS 게이트웨이(Unified Communications Manager 클러스터의 각 서버에 있음)
- H.323 트렁크 및 SIP 트렁크에 대해 시도된 통화 및 완료된 통화

알림 요약 보고서

알림 요약 보고서는 해당 날짜에 대해 생성되는 알림의 세부 정보를 제공합니다.

클러스터별 통계는 Unified Communications Manager 및 IM and Presence Service에서만 지원됩니다.

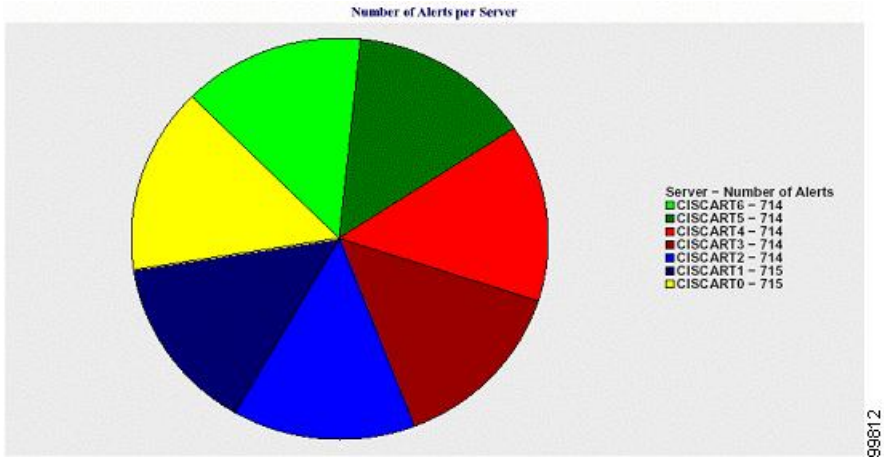
서버당 알림 수

원형 차트는 클러스터의 노드당 알림 수를 제공합니다. 생성 된 알림에 대한 서버 수준 세부 정보가 차트에 표시됩니다. 원형 차트의 각 섹터는 클러스터의 특정 서버에 대해 생성된 알림 수를 나타냅니다. 차트에는 클러스터에 서버(리포터가 당일 알림을 생성하는 서버)가 있는 만큼의 섹터가 포함됩니다. 서버에 대한 데이터가 없는 경우 차트에 해당 서버를 나타내는 섹터가 없습니다. 모든 서버에 데이터가 없는 경우에는 리포터가 차트를 생성하지 않습니다. “해당 날짜에 대해 알림이 생성되지 않았습니다”라는 메시지가 표시됩니다.

Cisco Unity Connection에만 해당: 원형 차트는 서버에 대한 알림 수를 제공합니다. 생성 된 알림에 대한 서버 수준 세부 정보가 차트에 표시됩니다. 서버에 대한 데이터가 없는 경우에는 리포터가 차트를 생성하지 않습니다. "해당 날짜에 대해 알림이 생성되지 않았습니다"라는 메시지가 표시됩니다.

다음 차트는 Unified Communications Manager 클러스터의 서버당 알림 수를 나타내는 원형 차트 예를 보여줍니다.

그림 ***20:*** 서버당 알림 수를 보여주는 원형 차트

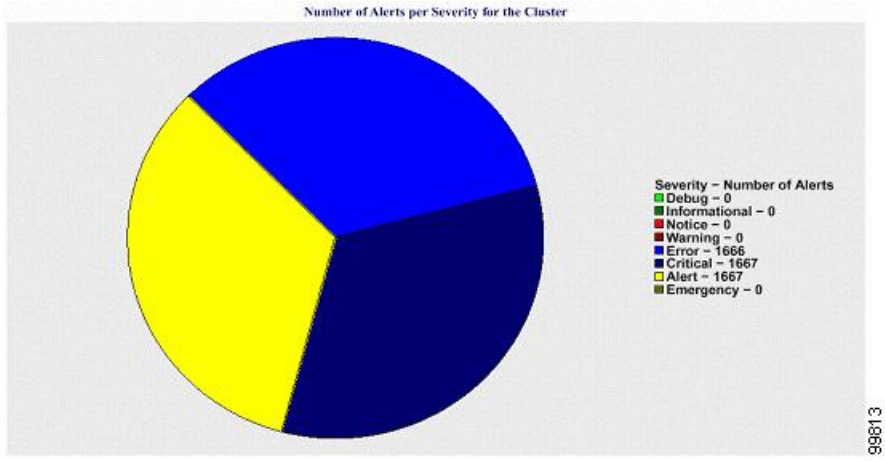


클러스터의 심각도 별 알림 수

원형 차트에는 알림 심각도 별 알림 수가 표시됩니다. 이 차트는 생성되는 알림의 심각도 세부 정보를 표시합니다. 원형 차트의 각 섹터는 특정 심각도 유형으로 생성된 알림 수를 나타냅니다. 차트에는 심각도(리포터가 당일 알림을 생성하는 서버)가 있는 만큼의 섹터를 제공합니다. 심각도에 대한 데이터가 없는 경우 차트에 해당 심각도를 나타내는 섹터가 없습니다. 데이터가 없는 경우에는 리포터가 차트를 생성하지 않습니다.

다음 차트는 Unified Communications Manager 클러스터의 심각도당 알림 수를 나타내는 원형 차트 예를 보여줍니다.

그림 ***21:*** 클러스터에 대한 심각도 별 알림 수를 보여 주는 원형 차트

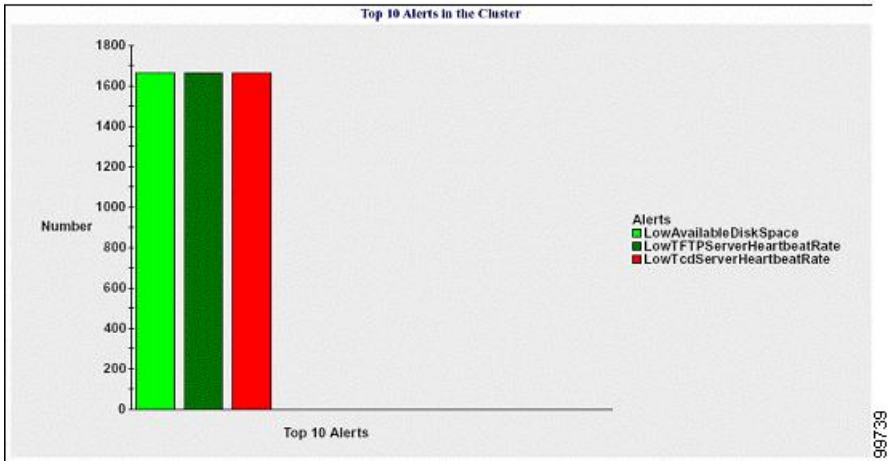


클러스터의 상위 **10**개 알림

막대형 차트에는 특정 알림 유형의 알림 수가 표시됩니다. 이 차트에는 알림 유형을 기준으로 생성되는 알림에 대한 세부 정보가 표시됩니다. 각 막대는 알림 유형에 대한 알림 수를 나타냅니다. 이 차트에는 가장 높은 수의 알림을 기준으로 처음 10개의 알림에 대한 세부 정보가 내림차순으로 표시됩니다. 특정 알림 유형에 대한 데이터가 없는 경우 해당 알림을 나타내는 막대가 표시되지 않습니다. 알림 유형에 대한 데이터가 없는 경우 RTMT가 차트를 생성하지 않습니다.

다음 차트는 Unified Communications Manager 클러스터의 상위 10개 알림을 나타내는 막대 차트의 예를 보여줍니다.

그림 ***22:*** 클러스터의 상위 ***10***개 알림을 보여주는 막대 차트



서버(또는 클러스터의 각 서버)에 파일 이름 패턴 AlertLog_mm_dd_yyyy_hh_mm.csv와 일치하는 로그 파일이 포함되어 있습니다. 다음 정보가 로그 파일에 있습니다.

- 시간 - 알림이 발생한 시간 시간
- 알림 이름 - 설명 이름
- 노드 이름 - 알림이 발생한 서버
- 모니터링되는 개체 - 모니터링되는 개체
- 심각도 - 이 알림의 심각도

성능 보호 보고서

성능 보호 보고서는 IM and Presence Service 및 Cisco Unity Connection을 지원하지 않습니다.

성능 보호 보고서는 특정 보고서에 대한 통계를 표시하는 다양한 차트를 구성하는 요약을 제공합니다. 리포터는 로그 정보를 기준으로 하루에 한 번 보고서를 생성합니다.

성능 보호 보고서는 Cisco Intercompany Media Engine에 대한 정보를 추적할 수 있는 최근 7개의 기본 모니터링 개체에 대한 경향 분석 정보를 제공합니다. 이 보고서에는 Cisco IME 클라이언트에 대한 총 통화 및 폴백 통화 비율을 보여주는 Cisco IME 클라이언트 통화 활동 차트가 포함됩니다.

성능 보호 보고서는 다음 차트로 구성됩니다.

- Cisco Unified Communications Manager 통화 활동
- 등록된 전화기 및 MGCP 게이트웨이 수
- 시스템 리소스 사용률
- 장치 및 다이얼 플랜 수량

Cisco Unified Communications Manager 통화 활동

선형 차트는 시도된 통화 수와 활성 통화 수로 완료된 통화 수에 대한 증가 또는 감소 시간을 시간별로 표시합니다. Unified Communications Manager 클러스터 구성의 경우 데이터는 클러스터의 각 서버에 대한 차트로 표시됩니다. 이 차트는 시도된 통화 수, 완료된 통화 및 활성 통화에 대해 각각 하나씩 3개의 선으로 구성됩니다. 통화 활동에 대한 데이터가 없는 경우에는 리포터가 차트를 생성하지 않습니다.

등록된 전화기 및 MGCP 게이트웨이 수

선형 차트에는 등록된 전화기 및 MGCP 게이트웨이의 수가 표시됩니다. Unified Communications Manager 클러스터 구성의 경우 차트에 클러스터의 각 서버에 대한 데이터가 표시됩니다. 이 차트는 등록된 전화기의 수와 MGCP 게이트웨이 수에 대한 2개의 선으로 구성됩니다. 전화기 또는 MGCP 게이트웨이에 대한 데이터가 없는 경우에는 리포터가 차트를 생성하지 않습니다.

시스템 리소스 사용률

선형 차트에는 CPU 로드 비율 및 서버(또는 Unified Communications Manager 클러스터 구성의 경우 전체 클러스터)에 사용되는 메모리 비율(바이트)이 표시됩니다. 차트는 CPU 로드 및 메모리 사용량에 대해 하나씩 2개의 선으로 구성됩니다. Unified Communications Manager 클러스터에서 각 선은 클러스터 값(데이터를 사용할 수 있는 클러스터의 모든 서버에 대한 값의 평균)을 나타냅니다. 전화기 또는 MGCP 게이트웨이에 대한 데이터가 없는 경우에는 리포터가 차트를 생성하지 않습니다.

장치 및 다이얼 플랜 수량

두 테이블은 Unified Communications Manager 데이터베이스의 정보를 표시하며 장치 수와 다이얼 플랜 구성 요소 수에 대해 설명합니다. 장치 테이블에는 IP 전화기, Cisco Unity Connection 포트, H.323 클라이언트, H.323 게이트웨이, MGCP 게이트웨이, MOH 리소스 및 MTP 리소스 수가 표시됩니다. 다이얼 플랜 테이블에는 디렉터리 번호와 회선, 경로 패턴 및 변환 패턴의 수가 표시됩니다.

21 장

Cisco Unified Reporting

- 통합 데이터 보고, 305 페이지
- 시스템 요구 사항, 306 페이지
- UI 구성 요소, 307 페이지
- 지원되는 보고서, 309 페이지

통합 데이터 보고

Cisco Unified Communications Manager 및 Cisco Unified Communications Manager IM and Presence Service 콘솔에 액세스할 수 있는 Cisco Unified Reporting 웹 애플리케이션은 클러스터 데이터 문제 해결 또는 검사를 위해 통합된 보고서를 생성합니다.

참고 별도로 언급된 경우가 아니면 이 설명서의 정보, 메모 및 절차는 Unified Communications Manager 및 IM and Presence Service에 적용됩니다.

이 도구는 클러스터 데이터의 스냅샷을 얻는 간단한 방법을 제공합니다. 이 도구는 기존 소스에서 데이터를 수집하고 데이터를 비교하며 불규칙성을 보고합니다. Cisco Unified Reporting에서 보고서를 생성하면 보고서는 하나 이상의 서버에 있는 하나 이상의 소스의 데이터를 하나의 출력 보기로 결합합니다. 예를 들어 클러스터의 모든 서버에 대한 호스트 파일을 표시하는 보고서를 볼 수 있습니다.

Cisco Unified Reporting 웹 애플리케이션은 설치 시에 클러스터의 모든 노드에 배포됩니다. 보고서는 데이터베이스 레코드에서 생성됩니다.

참고 Cisco Business Edition 5000 서버에서 Cisco Unified Reporting 애플리케이션은 Unified Communications Manager의 데이터만 캡처합니다. 크기 제약 조건으로 인해 애플리케이션에서 Cisco Unity Connection에 대한 데이터를 캡처하지 않습니다. 이 도구를 사용하여 Unified Communications Manager 설치에 대한 중요한 정보를 수집할 수 있습니다.

보고서 생성에 사용되는 데이터 소스

이 애플리케이션은 게시자 노드와 각 가입자 노드의 다음 소스에서 정보를 캡처합니다.

- RTMT 카운터
- CDR_CAR(Unified Communications Manager만 해당)
- Unified Communications Manager DB(Unified Communications Manager만 해당)
- IM and Presence DB(IM and Presence Service만 해당)
- 디스크 파일
- OS API 통화
- 네트워크 API 통화
- prefs
- CLI
- RIS

보고서는 보고서가 생성될 때 액세스할 수 있는 모든 활성 클러스터에 대한 데이터를 포함합니다. 게시자 노드의 데이터베이스가 다운된 경우 활성 노드에 대한 보고서를 생성할 수 있습니다. 시스템 보고서 목록의 보고서 설명 보고서는 보고서에 대한 정보 소스를 제공합니다.

지원되는 출력 형식

이 릴리스는 보고서에 대한 HTML/CSV 출력을 지원합니다. 보고서 이름과 날짜 및 타임 스탬프를 사용하여 Cisco Unified Reporting에서 보고서를 식별할 수 있습니다. 이 애플리케이션은 사용자가 볼 수 있도록 가장 최근의 보고서의 로컬 복사본을 저장합니다. “새 보고서 다운로드”에 설명된 바와 같이 최근 보고서의 로컬 복사본 또는 새 보고서를 하드 디스크로 다운로드할 수 있습니다. 보고서를 다운로드한 후에는 확인을 위해 다운로드한 파일의 이름을 바꾸거나 다른 폴더에 저장할 수 있습니다.

시스템 요구 사항

Cisco Tomcat 서비스

Cisco Unified Reporting는 Cisco Tomcat 서비스에서 애플리케이션으로 실행되며,이는 설치 시 Unified Communications ManagerIM and Presence Service를 설치할 때 활성화됩니다. 이러한 제품이 클러스터의 모든 노드에서 실행되고 있는지 확인합니다.

HTTPS

보고서 하위 시스템은 HTTPS를 통해 RPC 메커니즘을 사용하여 다른 노드에서 정보를 수집합니다. HTTPS 포트가 열려 있고 노드에서 Cisco Tomcat 서비스를 실행하여 보고서를 성공적으로 생성하는지 확인합니다.

HTTPS를 활성화하려면 연결 프로세스 중에 노드를 식별하는 인증서를 다운로드해야 합니다. 현재 세션에만 노드 인증서를 수락할 수도 있고, 신뢰 폴더(파일)로 인증서를 다운로드하여 해당 노드에서 현재 세션 및 이후의 세션을 보호할 수도 있습니다. 신뢰 폴더에는 신뢰할 수 있는 모든 사이트에 대한 인증서가 저장됩니다. 자세한 내용은 *Cisco Unified Communications Manager* 관리 설명서의 "소개" 장을 참조하십시오.

애플리케이션에 액세스하려면 브라우저 창에서 관리 인터페이스에 액세스합니다. Cisco Unified Reporting는 HTTPS를 사용하여 브라우저에 보안 연결을 설정합니다.

필요한 액세스 권한

Cisco Unified Reporting 애플리케이션에서는 웹 애플리케이션에 대한 액세스를 허용하기 전에 Cisco Tomcat 서비스를 사용하여 사용자를 인증합니다. 승인된 사용자만 Cisco Unified Reporting 애플리케이션에 액세스할 수 있습니다. Unified Communications Manager의 경우 기본적으로 표준 CCM 수퍼 사용자 그룹의 관리자 사용자만 Cisco Unified Reporting에 액세스하여 보고서를 보고 만들 수 있습니다.

Cisco Unified Communications Manager 및 IM and Presence Service의 경우 표준 CUReporting 인증 역할의 사용자는 Cisco Unified Reporting에 액세스할 수 있습니다.

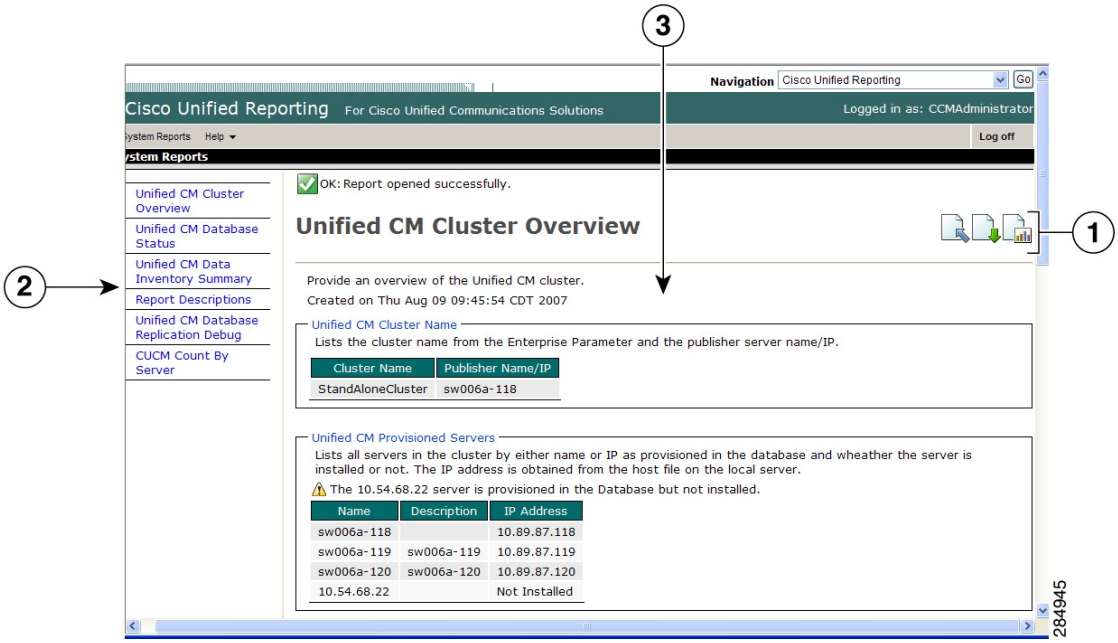
인증된 사용자는 Cisco Unified Reporting 사용자 인터페이스를 사용하여 보고서를 보거나, 새 보고서를 생성하거나, 보고서를 다운로드할 수 있습니다.

참고 Unified Communications Manager의 경우 표준 CCM 수퍼 사용자 그룹의 관리자 사용자는 Cisco Unified Reporting를 포함하여 Unified Communications Manager 관리 탐색 메뉴의 관리 애플리케이션에 액세스할 수 있으며, 이 경우 애플리케이션 중 하나에 대한 싱글 사인온이 제공됩니다.

UI 구성 요소

다음 그림은 Cisco Unified Reporting를 위한 UI 구성 요소를 보여줍니다.

그림 ***23: UI*** 구성 요소



1. 업로드, 다운로드, 아이콘 생성
2. 보고서 목록
3. 보고서 상세정보

참고 보고서 범주, 사용 가능한 보고서 및 보고서 데이터는 릴리스에 따라 달라 집니다.

관리 인터페이스에서 로그인

다음 단계 중 하나를 수행하여 관리 인터페이스에서 Cisco Unified Reporting에 로그인합니다.

- Unified Communications Manager의 경우 Cisco Unified CM 관리 인터페이스의 탐색 메뉴에서 **Cisco Unified Reporting**을 선택합니다.
- IM and Presence Service의 경우 IM and Presence 관리 인터페이스의 탐색 메뉴에서 **Cisco Unified CM IM and Presence** 보고를 선택합니다.

시작하기 전에

Cisco Unified Reporting 애플리케이션에 액세스할 수 있는 권한이 있는지 확인하십시오.

Cisco Unified Reporting에 로그인하면 마지막으로 성공한 시스템 로그인 시도와 사용자 ID, 날짜, 시간 및 IP 주소와 함께 각 사용자에 대한 마지막 실패 시스템 로그인 시도가 기본 Cisco Unified Reporting 창에 표시됩니다.

지원되는 보고서

이 섹션에서는 Cisco Unified Communications Manager 및 Cisco Unified Communications Manager IM and Presence Service에 대해 지원되는 보고서에 대해 자세히 설명합니다. 보고서 이름과 날짜 및 타임스탬프를 사용하여 Cisco Unified Reporting에서 보고서를 식별할 수 있습니다. Cisco Unified Reporting는 사용자가 볼 수 있는 가장 최근 보고서의 로컬 복사본을 저장합니다.

Unified Communications Manager 보고서

다음 표에서는 Unified Communications Manager를 설치한 후 Cisco Unified Reporting에 표시되는 시스템 보고서 유형에 대해 설명합니다.

표 ***74: Unified Communications Manager Cisco Unified Reporting***에 표시되는 보고서

보고서	설명
만료된 자격 증명 알고리즘을 사용하는 UCM 사용자	SHA1을 사용하여 암호나 PIN을 저장하고 해시한 최종 사용자의 목록을 제공합니다.
보고서 설명	표시되는 보고서에 대한 문제 해결 및 세부 정보를 제공합니다.
보안 진단 도구	보안 구성 요소에 대한 정보를 요약하여 설명합니다.
Unified CM 클러스터 개요	Unified Communications Manager 클러스터에 대한 개요를 제공합니다. 이 보고서에는 다음과 같은 세부 정보가 포함됩니다. • 클러스터에 설치된 Unified Communications Manager 또는 IM and Presence Service 버전 • 클러스터에 있는 모든 노드의 호스트 이름 또는 IP 주소 • 하드웨어 세부 정보 요약
Unified CM 데이터 요약	Unified Communications Manager 관리 메뉴의 구조에 따라 Unified Communications Manager 데이터베이스에 존재하는 데이터 요약을 제공합니다. 예를 들어, 3개의 자격 증명 정책, 5개의 전화회의 브리지 및 10개의 공유 회선 표시를 구성하는 경우 이 보고서에서 해당 유형의 정보를 볼 수 있습니다.
Unified CM 데이터베이스 복제 디버그	데이터베이스 복제에 디버깅 정보를 제공합니다. 팁 이 보고서의 경우 생성은 CPU를 스파이크하고 클러스터의 노드당 10초까지 걸릴 수 있습니다.
Unified CM 데이터베이스 상태	Unified Communications Manager 데이터베이스의 상태에 대한 스냅샷을 제공합니다. 이 보고서는 업그레이드 전에 생성해야 데이터베이스가 정상적인 상태가 됩니다.

보고서	설명
Unified CM 장치 수 요약	Unified Communications Manager 데이터베이스에 있는 모델 및 프로토콜 별로 장치 수를 제공합니다.
Unified CM 장치 배포 요약	클러스터 전체에서 장치를 배포하는 방법에 대한 요약을 제공합니다. 예를 들어,이 보고서에는 기본, 보조 및 3차 노드를 연결하는 장치가 표시됩니다.
Unified CM 디렉터리 URI 및 GDPR 중복	중복된 사용자 디렉터리 URI, 학습된 디렉터리 URI, 학습된 번호 및 시스템에서 학습 패턴에 대한 세부 목록을 제공합니다.
Unified CM 내선 이동	Cisco Extension Mobility 사용에 대한 요약을 제공합니다. 예를 들어 Cisco Extension Mobility 사용자가 로그인한 전화기의 수, Cisco Extension Mobility에 연결된 사용자 등이 있습니다.
Unified CM 지리적 위치 정책	지리적 위치 논리적 파티션 정책 매트릭스의 레코드 목록을 제공합니다.
필터가 포함된 Unified CM 지리적 위치 정책	선택한 지리적 위치 정책에 대한 지리적 위치 논리적 파티션 정책 매트릭스의 레코드 목록을 제공합니다.
전화기가 없는 Unified CM 회선	전화기와 연결되지 않은 회선 목록을 제공합니다.
Unified CM 다중 회선 장치	여러 회선 표시가 있는 전화기 목록을 제공합니다.
Unified CM 전화기 범주	범용 장치 템플릿과 함께 사용할 특정 범주의 전화기 모델 목록을 제공합니다. 사용자에 대한 셀프 프로비저닝을 활성화하는 경우 각 범주에 대한 템플릿을 제공하여 이러한 전화기 중 일부 또는 모두를 허용하도록 선택할 수 있습니다.
Unified CM 전화기 기능 목록	Unified Communications Manager 관리의 각 장치 유형에 대해 지원되는 기능 목록을 제공합니다.
Unified CM 전화기 로캘 설치 관리자	설치된 전화기 로캘 패키지에서 지원하는 Cisco Unified IP 전화기 펌웨어 버전 목록을 제공합니다.
일치하지 않는 부하를 포함한 Unified CM 전화기	펌웨어 로드가 일치하지 않는 모든 전화기 목록을 제공합니다.
회선이 없는 Unified CM 전화기	연결된 회선이 없는 Unified Communications Manager 데이터베이스에서 모든 전화기 목록을 제공합니다.
Unified CM 공유 회선	하나 이상의 공유 회선 표시와 함께 Unified Communications Manager 데이터베이스의 모든 전화기 목록을 제공합니다.
Unified CM 테이블 수 요약	데이터의 데이터베이스 중심 뷰를 제공합니다. 이 보고서는 데이터베이스 스키마를 이해하는 관리자 또는 AXL API 개발자에게 유용합니다.

보고서	설명
Unified CM 사용자 장치 수	연결된 장치에 대한 정보를 제공합니다. 예를 들어,이 보고서에는 사용자가 없는 전화기의 수, 한 대의 전화기를 사용하는 사용자의 수, 두 대 이상의 전화기를 사용하는 사용자 수가 나열됩니다.
기본 내선 번호를 공유 하는 Unified CM 사용자	시스템에서 기본 내선 번호를 공유 하는 사용자 목록을 제공합니다.
Unified CM VG2XX 게이트웨이	게이트웨이 엔드포인트 보안 프로파일에 대한 요약을 제공합니다.
Unified CM 음성 메일	Unified Communications Manager 관리의 음성 메시징 관련 구성에 대한 요약을 제공합니다. 예를 들어, 이 보고서에는 구성된 음성 메일 포트 수, 메시지 대기 표시기 수, 구성된 음성 메시징 프로파일 수, 음성 메시지 프로파일과 연결된 디렉터리 번호 수 등이 나열됩니다.
통합 기밀 액세스 수준 매트릭스	기밀 액세스 수준 매트릭스에 대한 모든 정보를 제공합니다.

IM and Presence Service 보고서

다음 표에서는 Unified Communications Manager에 IM and Presence Service를 설치한 후 Cisco Unified Reporting에 표시되는 시스템 보고서 유형에 대해 설명합니다.

참고 릴리스 10.0(1)에서 IM and Presence 클러스터 정보는 Cisco Unified Communications Manager 노드에서 사용할 수 있습니다. Cisco Unified Communications Manager에서 **Cisco Unified Reporting** > 시스템 보고서 > **Unified CM** 클러스터 개요를 선택합니다.

다음 표에서 보고서 유형을 보고 생성할 수 있습니다.

표 ***75: Cisco Unified Reporting***에 표시되는 ***IM and Presence Service*** 보고서

보고서	설명
IM and Presence 데이터베이스 복제 디버그	데이터베이스 복제에 디버깅 정보를 제공합니다. 팁 이 보고서의 경우 생성은 CPU를 스파이크하고 클러스터의 노드당 10초까지 걸릴 수 있습니다.
IM and Presence 데이터베이스 상태	IM and Presence Service 데이터베이스의 상태에 대한 스냅샷을 제공합니다. 이 보고서는 업그레이드 전에 생성해야 데이터베이스가 정상적인 상태가 됩니다.

보고서	설명
IM and Presence 테이블 수 요약	데이터의 데이터베이스 중심 뷰를 제공합니다. 이 보고서는 데이터베이스 스키마를 이해하는 관리자 또는 AXL API 개발자에게 유용합니다.
IM and Presence 사용자 세션 보고서	하나 이상의 장치를 사용하여 모든 활성 사용자 로그인 세션 목록을 제공합니다.
프레즌스 구성 보고서	IM and Presence Service 사용자에 대한 구성 정보를 제공합니다. • Cisco Unified Communications Manager에서 동기화된 사용자 • IM and Presence Service에 대해 활성화된 사용자 • Microsoft 원격 통화 제어에 대해 활성화된 사용자 • IM and Presence Service에서 일정 정보에 대해 활성화된 사용자 세부 정보 보기를 클릭하여 정렬 가능한 열의 사용자 목록을 표시합니다.
IM and Presence 클러스터 개요	IM and Presence Service 클러스터에 대한 개요를 제공합니다. 예를 들어, 이 보고서는 클러스터에 설치된 IM and Presence Service 버전, 클러스터에 있는 모든 노드의 호스트 이름 또는 IP 주소, 하드웨어 세부 정보 요약 등을 나타냅니다.
프레즌스 제한 경고 보고서	최대 연락처 또는 감시자 수에 대한 구성 제한을 충족하거나 초과한 사용자에 대한 정보를 제공합니다. 세부 정보 보기를 클릭하여 정렬 가능한 열의 사용자 목록을 표시합니다.
프레즌스 사용 보고서	로그인된 XMPP 클라이언트 및 타사 API에 대한 사용 정보를 제공합니다. 세부 정보 보기를 클릭하여 정렬 가능한 열의 XMPP 클라이언트 및 타사 API 목록을 표시합니다.
보고서 설명	표시되는 보고서에 대한 문제 해결 및 세부 정보를 제공합니다. 이 보고서는 보고서에 대한 설명, 각 정보 그룹 및 각 데이터 항목에 대한 설명과 데이터 소스, 관련 문제의 증상 및 보상을 제공합니다.

보고서 설명 보기

Cisco Unified Reporting은 보고서 도움말을 제공합니다. 보고서 설명 링크는 보고서에 대한 설명, 각 정보 그룹 및 각 데이터 항목에 대한 설명과 데이터 소스, 관련 문제의 증상 및 치료를 제공합니다.

참고 보고서 문제에 대한 추가 도움이 필요한 경우 TAC에 문의해야 할 수 있습니다.

프로시저

단계 **1** 시스템 보고서를 선택합니다.

단계 **2** 보고서 목록 에서 보고서 설명 링크를 선택합니다.

참고 IM and Presence Service 보고서를 선택할 때 다시 로그인하라는 메시지가 표시되면 Cisco Unified Communications Manager 관리 로그인 자격 증명을 다시 입력합니다.

단계 **3** 보고서 생성아이콘을 선택합니다.

보고서가 생성되고 표시됩니다.

새 보고서 생성

새 보고서를 생성하고 볼 수 있습니다.

시작하기 전에

Cisco Tomcat 서비스가 하나 이상의 노드에서 실행되고 있으며 지원되는 웹 브라우저를 사용하여 보고서를 볼 수 있는지 확인하십시오.

이 애플리케이션은 보고서가 과도한 CPU 시간을 생성하거나 사용하는 데 너무 많은 시간을 소비할 경우 사용자에게 알립니다. 보고서가 생성되는 동안 진행 표시줄이 표시됩니다. 새 보고서가 표시되고 날짜 및 시간이 업데이트됩니다.

프로시저

단계 **1** 메뉴 모음에서 시스템 보고서를 선택합니다.

단계 **2** 보고서를 선택하십시오.

참고 IM and Presence Service 보고서를 선택할 때 다시 로그인하라는 메시지가 표시되면 Cisco Unified Communications Manager 관리 로그인 자격 증명을 다시 입력합니다.

단계 **3** 보고서 창에서 보고서 생성(가로 막대형 차트) 아이콘을 선택합니다.

단계 **4** 자동으로 표시되지 않는 섹션에 대한 세부 정보를 노출하려면 세부 정보 보기 링크를 선택합니다.

다음에 수행할 작업

보고서에 항목에 대한 실패한 데이터 검사가 표시되면 보고서 설명 보고서를 선택하고 문제 해결 정보를 검토하여 가능한 해결책을 확인합니다. 보고서 설명 보고서는 데이터베이스에서 동적으로 생성되므로 새 보고서 설명 보고서를 생성할 수도 있습니다.

저장된 보고서 보기

기존 보고서의 복사본을 볼 수 있습니다.

참고 새로 설치하거나 업그레이드하는 동안 Cisco Unified Reporting 애플리케이션은 가장 최근 보고서의 로컬 복사본을 저장하지 않습니다.

시작하기 전에

Cisco Tomcat 서비스가 하나 이상의 노드에서 실행되고 있으며 지원되는 웹 브라우저를 사용하여 보고서를 볼 수 있는지 확인하십시오.

프로시저

단계 **1** 메뉴 모음에서 시스템 보고서를 선택합니다.

단계 **2** 보고서 목록에서 보려는 보고서를 선택합니다.

단계 **3** 보고서 이름(날짜 및 시간 스탬프)에 대한 링크를 선택합니다.

단계 **4** 자동으로 표시되지 않는 섹션에 대한 세부 정보를 보려면 세부 정보 보기 링크를 선택합니다.

다음에 수행할 작업

새 보고서나 저장된 보고서를 다운로드합니다.

보고서에 항목에 대한 데이터 검사 실패가 표시되면 보고서 설명 보고서를 선택하고 문제 해결 정보를 검토하여 가능한 해결책을 확인합니다.

새 보고서 다운로드

새 보고서를 다운로드하려면 하드 드라이브에 로컬로 저장해야 합니다. 보고서를 다운로드하면 원시 XML 데이터 파일이 하드 드라이브로 다운로드됩니다.

프로시저

단계 **1** 새 보고서를 생성합니다.

단계 **2** 새 보고서가 나타나면 보고서 창에서 보고서 다운로드(녹색 화살표) 아이콘을 선택합니다.

참고 문서를 다운로드하기 전에 보고서 세부 정보에 대한 세부 정보 보기 링크를 클릭할 필요가 없습니다. 데이터는 다운로드된 파일에서 캡처됩니다.

단계 **3** 저장을 선택하여 디스크에서 지정하는 위치에 파일을 저장합니다.

하드 디스크에서 파일이 저장되는 파일 이름 또는 위치를 변경하려면 새 위치를 입력하거나 파일의 이름을 변경합니다(선택 사항). 진행 표시줄에 진행 중인 다운로드가 표시됩니다.

파일이 하드 디스크로 다운로드됩니다.

단계 **4** 다운로드가 완료되면 열기를 선택하여 XML 보고서를 엽니다.

참고 XML 파일의 내용을 변경하지 마십시오. 그렇지 않으면 보고서가 화면에 제대로 표시되지 않을 수 있습니다.

다음에 수행할 작업

브라우저에서 다운로드한 보고서 파일을 보려면 해당 파일을 노드에 업로드합니다.

참고 기술 지원을 받으려면 다운로드한 파일을 이메일에 첨부하거나 파일을 다른 노드에 업로드할 수 있습니다.

저장된 보고서 다운로드

저장된 보고서를 다운로드하려면 보고서를 다운로드하여 하드 드라이브에 로컬로 저장합니다. 보고서를 다운로드하면 원시 XML 데이터 파일이 하드 디스크로 다운로드됩니다.

프로시저

단계 **1** 기존 보고서의 세부 정보를 열어서 봅니다.

단계 **2** 보고서 창에서 보고서 다운로드(녹색 화살표) 아이콘을 선택합니다.

단계 **3** 저장을 선택하여 디스크에서 지정하는 위치에 파일을 저장합니다.

하드 디스크에서 파일이 저장되는 파일 이름 또는 위치를 변경하려면 새 위치를 입력하거나 파일의 이름을 변경합니다(선택 사항). 진행 표시줄에 진행 중인 다운로드가 표시됩니다.

파일이 하드 디스크로 다운로드됩니다.

단계 **4** 다운로드가 완료되면 열기를 선택하여 XML 보고서를 엽니다.

참고 XML 파일의 내용을 변경하지 마십시오. 그렇지 않으면 보고서가 제대로 표시되지 않을 수 있습니다.

다음에 수행할 작업

브라우저에서 다운로드한 보고서 파일을 보려면 해당 파일을 노드에 업로드합니다.

참고 기술 지원을 받으려면 다운로드한 파일을 이메일에 첨부하거나 파일을 다른 노드에 업로드할 수 있습니다.

보고서 업로드

브라우저 창에서 다운로드한 보고서를 보려면 보고서를 메모에 업로드해야 합니다.

시작하기 전에

하드 드라이브에 보고서를 다운로드합니다.

프로시저

단계 **1** 메뉴 모음에서 시스템 보고서를 선택합니다.
단계 **2** 보고서에 액세스하여 보고서 창에 보고서 업로드(파란색 화살표) 아이콘을 표시합니다.
단계 **3** 보고서 업로드 아이콘을 선택합니다.
단계 **4** .xml 파일을 찾으려면 찾아보기를 선택하여 하드 드라이브의 해당 위치로 이동합니다.
단계 **5** 업로드를 선택합니다.
단계 **6** 계속을 선택하여 업로드된 파일을 브라우저 창에 표시합니다.

다음에 수행할 작업

업그레이드하는 동안 업로드된 보고서와 새로 생성된 보고서를 나란히 비교할 수 있습니다.

22 장

Cisco IP 전화기에 대한 통화 진단 및 품질 보고 구성

- 진단 및 보고 개요, 317 페이지
- Prerequisites, 318 페이지
- 진단 및 보고 구성 작업 흐름, 320 페이지

진단 및 보고 개요

Cisco Unified Communications Manager는 Cisco IP 전화기의 통화 품질을 보장하기 위한 두 가지 옵션을 제공합니다.

- 통화 진단 - 통화 진단에는 CMR(통화 관리 레코드) 및 음성 품질 메트릭을 생성하는 작업이 포함됩니다.
- QRT(품질 보고서 도구) - QRT는 Cisco Unified IP Phone을 위한 음성 품질 및 일반 문제 보고 도구입니다. 이 도구를 사용하면 사용자가 IP 전화기에서 오디오 및 기타 일반 문제를 쉽고 정확하게 보고할 수 있습니다.

통화 진단 개요

SCCP 및 SIP를 실행하는 Cisco IP 전화기를 구성하여 통화 진단을 수집할 수 있습니다. 통화 진단은 통화 관리 레코드(CMR)로, 진단 레코드라고도 하며, 음성 품질 메트릭으로 구성됩니다.

음성 품질 메트릭은 기본적으로 활성화되어 있으며 대부분의 Cisco IP 전화기에서 지원됩니다. Cisco IP 전화기는 MOS(평균 평가 제곱) 값을 기반으로 한 음성 품질 메트릭을 계산합니다. 음질 메트릭은 잡음이나 왜곡의 이유는 되지 않으며, 오직 프레임 손실에만 영향을 미칩니다.

CMR 레코드는 통화의 스트리밍된 오디오 품질에 대한 정보를 저장합니다. Unified Communications Manager를 구성하여 CMR을 생성할 수 있습니다. 이 정보는 청구 레코드 생성 및 네트워크 분석 등의 후 처리 작업에 유용합니다.

품질 보고서 도구 개요

QRT(품질 보고서 도구)는 Cisco IP 전화기를 위한 음질 및 일반 문제 보고 도구입니다. 이 도구를 사용하면 사용자가 IP 전화기에서 오디오 및 기타 일반 문제를 쉽고 정확하게 보고할 수 있습니다.

시스템 관리자는 IP 전화기에서 QRT 소프트키를 표시하는 소프트키 템플릿을 구성 및 할당하여 QRT 기능을 활성화할 수 있습니다. QRT에 원하는 사용자 상호 작용 수준에 따라 서로 다른 두 가지 사용자 모드에서 선택할 수 있습니다. 그런 다음 시스템 매개 변수를 구성하고 Cisco 통합 서비스 가용성 도구를 설정하여 시스템에서 기능이 작동하는 방식을 정의합니다. 그러면 QRT 뷰어 애플리케이션을 사용하여 전화기 문제 보고서를 생성, 사용자 정의 및 확인할 수 있습니다.

사용자의 IP 전화기에 문제가 발생하는 경우 통화 상태가 온 훅 또는 연결됨일 때 Cisco IP 전화기에서 QRT 소프트키를 눌러 문제 유형과 기타 관련 통계를 보고할 수 있습니다. 그러면 사용자가 IP 전화기에 대해 보고되는 문제를 가장 잘 설명하는 이유 코드를 선택할 수 있습니다. 사용자 정의된 전화기 문제 보고서는 사용자에게 구체적인 정보를 제공합니다.

QRT는 사용자가 QRT 소프트키를 눌러 문제 유형을 선택한 후에 스트리밍 통계를 수집하려고 시도합니다. 스트리밍 통계를 수집하려면 QRT의 경우 최소 5초 동안 통화가 활성 상태여야 합니다.

세부 통화 보고 및 청구

Cisco CDR Analysis and Reporting(CAR) 도구는 서비스 품질, 트래픽, 사용자 통화 볼륨, 청구 및 게이트웨이의 품질에 대한 상세 보고서를 생성합니다. CAR은 CDR(통화 세부 정보 레코드), CMR(통화 관리 레코드) 및 Unified Communications Manager 데이터베이스의 데이터를 사용하여 보고서를 생성합니다. CAR 인터페이스는 Cisco 통합 서비스 가용성의 도구 메뉴 아래에서 액세스할 수 있습니다.

CAR은 타사에서 제공하는 통화 회계 및 청구 솔루션을 대체하기 위한 것이 아닙니다. Cisco 개발자 커뮤니티의 홈 페이지를 검색하여 이러한 솔루션을 제공하고 Cisco 기술 개발자 프로그램의 구성원인 회사를 찾을 수 있습니다.

CAR로 보고를 구성하는 방법에 대한 자세한 내용은 *Cisco Unified Communications Manager* 통화 보고 및 청구 관리 지침서를 참조하십시오.

Prerequisites

통화 진단 필수 조건

Cisco Unified IP Phone에서 통화 진단 기능을 지원하는지 확인합니다.

이 표를 사용하여 전화기에서 통화 진단 기능을 지원하는지 확인합니다. 통화 진단 범례에 대한 지원은 다음과 같습니다.

- X - SCCP와 SIP을 모두 실행하는 전화기에서 지원됩니다.
- S - SCCP 기능만

표 ***76:*** 통화 진단에 대한 장치 지원

장치	통화 진단에 대한 지원
Cisco Unified IP Phone 7906	X
Cisco Unified IP Phone 7911	X
Cisco Unified IP Phone 7921	X
Cisco Unified IP Phone 7931	X
Cisco Unified IP Phone 7940	S
Cisco Unified IP Phone 7941	X
Cisco Unified IP Phone 7942-G	X
Cisco Unified IP Phone 7942-G/GE	X
Cisco Unified IP Phone 7945	X
Cisco Unified IP Phone 7960	S
Cisco Unified IP Phone 7961	X
Cisco Unified IP Phone 7962-G	X
Cisco Unified IP Phone 7962-G/GE	X
Cisco Unified IP Phone 7965	X
Cisco Unified IP Phone 7970	X
Cisco Unified IP Phone 7971	X
Cisco Unified IP Phone 7972-G/GE	X
Cisco Unified IP Phone 7975	X

품질 보고서 도구 필수 조건

다음과 같은 기능이 있는 Cisco IP 전화기:

- 소프트키 템플릿 지원
- IP 전화 서비스 지원
- CTI에서 제어 가능
- 내부 HTTP 서버 포함

자세한 내용은 해당 전화기 모델의 설명서를 참조하십시오.

진단 및 보고 구성 작업 흐름

프로시저

	명령 또는 동작	목적
단계 **1**	통화 진단 구성, 320 페이지	이 작업을 수행하여 CMR을 생성하도록 Cisco Unified Communications Manager를 구성합니다. CMR 레코드는 통화의 스트리밍된 오디오 품질에 대한 정보를 저장합니다. CMR에 대한 자세한 내용은 *Cisco Unified Communications Manager Call Detail Records* 관리 설명서를 참조하십시오. 음성 품질 메트릭은 Cisco IP 전화기에서 자동으로 활성화됩니다. 음성 품질 메트릭 액세스에 대한 자세한 내용은 해당 전화기 모델에 대한 Cisco Unified IP Phone 관리 지침서를 참조하십시오.
단계 **2**	품질 보고서 도구 구성, 321 페이지에 대해 다음 하위 작업을 수행합니다. • QRT 소프트키를 사용하여 소프트키 템플릿 구성, 322 페이지 • QRT 소프트키 템플릿을 일반 장치 구성에 연결, 323 페이지 • 전화기에 QRT 소프트키 템플릿 추가, 325 페이지 • Cisco 통합 서비스 가용성에서 QRT 구성, 325 페이지 • 품질 보고서 도구에 대한 서비스 매개 변수 구성, 328 페이지	IP 전화기에 문제가 발생하는 사용자가 QRT 소프트키를 눌러 문제 유형과 기타 관련 통계를 보고할 수 있도록 QRT(Quality Report Tool)를 구성합니다.

통화 진단 구성

프로시저

단계 **1** Cisco Unified CM 관리에서 시스템 > 서비스 매개변수를 선택합니다.

단계 **2** 서버 드롭다운 목록에서 Cisco CallManager 서비스가 실행 중인 서버를 선택합니다.

단계 **3** 서비스 드롭다운 목록에서 **Cisco CallManager**를 선택합니다.
서비스 매개 변수 구성 창이 표시됩니다.

단계 **4** 클러스터 수준 매개 변수(장치 - 일반) 영역에서 통화 진단 활성화 서비스 매개 변수를 구성합니다. 다음 옵션을 사용할 수 있습니다.

- 비활성화됨 - CMR이 생성되지 않습니다.
- **CDR** 활성화 플래그가 **True**인 경우에만 활성화됨 - CDR(통화 세부 정보 기록) 활성화 플래그 서비스 매개 변수가 True로 설정된 경우에만 CMR이 생성됩니다.
- **CDR** 활성화 플래그와 관계 없이 활성화됨 - CDR 활성화 플래그 서비스 매개 변수 값과 관계 없이 CMR이 생성됩니다.

참고 CDR 활성화 플래그 서비스 매개 변수를 활성화하지 않고 CMR을 생성하면 제어되지 않은 디스크 공간 소비가 발생할 수 있습니다. CMR이 활성화되면 CDR을 활성화하는 것이 좋습니다.

단계 **5** 저장을 클릭합니다.

품질 보고서 도구 구성

IP 전화기에 문제가 발생하는 사용자가 QRT 소프트키를 눌러 문제 유형과 기타 관련 통계를 보고할 수 있도록 QRT(Quality Report Tool)를 구성합니다.

프로시저

	명령 또는 동작	목적
단계 **1**	QRT 소프트키를 사용하여 소프트키 템플릿 구성, 322 페이지	QRT 소프트키에 대해 온 훅 및 연결됨 통화 상태를 구성해야 합니다. 다음과 같은 통화 상태도 사용할 수 있습니다. • 전화회의 연결됨 • 호전환 연결됨
단계 **2**	(선택 사항) QRT 소프트키 템플릿을 일반 장치 구성에 연결, 323 페이지에 대해 다음 하위 작업을 수행합니다. • QRT 소프트키 템플릿을 일반 장치 구성에 추가, 324 페이지 • 일반 디바이스 구성을 전화기에 연결, 324 페이지	전화기에서 소프트키 템플릿을 사용할 수 있게 하려면 이 단계 또는 다음 단계를 완료해야 합니다. 시스템에서 일반 디바이스 구성을 사용하여 전화기에 구성 옵션을 적용 하는 경우 이 단계를 수행합니다. 이 방법은 전화기에서 사용할 수 있는 소프트키 템플릿을 만드는 데 가장 일반적으로 사용되는 방법입니다.
단계 **3**	(선택 사항) 전화기에 QRT 소프트키 템플릿 추가, 325 페이지	이 절차를 사용하여 소프트키 템플릿을 일반 디바이스 구성에 연결하거나 일반 디바이스 구성과 함께 연결하는 대신 사용할 수 있습니다. 일반 디바이스 구성 또는 다른 기본 소프트키 할당에서 할당을 무시하는 소프트키 템

	명령 또는 동작	목적
		플릿을 할당해야 하는 경우 일반 디바이스 구성과 함께 이 절차를 사용합니다.
단계 4	Cisco 통합 서비스 가용성에서 QRT 구성, 325 페이지에 대해 다음 하위 작업을 수행합니다. • Cisco Extended Functions 서비스 활성화, 326 페이지 • 알람 구성, 326 페이지 • 추적 구성, 327 페이지	
단계 5	(선택 사항) 품질 보고서 도구에 대한 서비스 매개 변수 구성, 328 페이지	

QRT 소프트키를 사용하여 소프트키 템플릿 구성

QRT 소프트키에 대해 온 훅 및 연결됨 통화 상태를 구성해야 합니다. 다음과 같은 통화 상태도 사용할 수 있습니다.

- 전화회의 연결됨
- 호전환 연결됨

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다.디바이스 > 디바이스 설정 > 소프트키 템플릿.

단계 2 새 소프트키 템플릿을 생성하려면 다음 단계를 수행합니다. 그렇지 않으면 다음 단계로 진행합니다.

a) 새로 추가를 클릭합니다.
b) 기본 템플릿을 선택하고 복사를 클릭합니다.
c) 소프트키 템플릿 이름 필드에 템플릿의 새 이름을 입력합니다.
d) 저장을 클릭합니다.

단계 3 다음 단계를 수행하여 기존 템플릿에 소프트키를 추가합니다.

a) 찾기를 클릭하고 검색 기준을 입력합니다.
b) 필요한 기존 템플릿을 선택합니다.

단계 4 이 소프트키 템플릿을 표준 소프트키 템플릿으로 지정하려면 기본 소프트키 템플릿 확인란을 선택합니다.

참고 소프트키 템플릿을 기본 소프트키 템플릿으로 지정하는 경우 먼저 기본값 지정을 제거하지 않는 한 이 소프트키 템플릿을 삭제할 수 없습니다.

단계 5 오른쪽 상단의 관련 링크 드롭다운 목록에서 소프트키 레이아웃 설정을 선택하고 이동을 클릭합니다.

단계 6 구성할 통화 상태 선택 드롭다운 목록에서 소프트키가 표시할 통화 상태를 선택합니다.

단계 **7** 선택되지 않은 소프트키 목록에서 소프트키를 선택하고 오른쪽 화살표를 클릭하여 소프트키를 선택한 소프트키 목록으로 이동합니다. 위쪽 및 아래쪽 화살표를 사용하여 새 소프트키의 위치를 변경합니다.

단계 **8** 이전 단계를 반복하여 추가 통화 상태로 소프트키를 표시합니다.

단계 **9** 저장을 클릭합니다.

단계 **10** 다음 작업 중 하나를 수행합니다.

- 이미 디바이스와 연결되어 있는 템플릿을 수정한 경우 구성 적용을 클릭하여 디바이스를 다시 시작합니다.
- 새 소프트키 템플릿을 생성한 경우 템플릿을 디바이스에 연결하고 다시 시작합니다. 자세한 내용은 소프트키 템플릿을 일반 디바이스 구성에 추가 및 소프트키 템플릿을 전화기와 연결 섹션을 참조하십시오.

다음에 수행할 작업

다음 단계 중 하나를 수행합니다.

- QRT 소프트키 템플릿을 일반 장치 구성에 추가, 324 페이지
- 전화기에 QRT 소프트키 템플릿 추가, 325 페이지

QRT 소프트키 템플릿을 일반 장치 구성에 연결

(선택 사항) 다음 두 가지 방법으로 소프트키 템플릿을 전화기에 연결할 수 있습니다.

- 소프트키 템플릿을 전화기 구성에 추가합니다.
- 소프트키 템플릿을 일반 장치 구성에 추가합니다.

이 섹션의 절차에서는 소프트키 템플릿을 일반 장치 구성에 연결하는 방법에 대해 설명합니다. 시스템에서 일반 장치 구성을 사용하여 전화기에 구성 옵션을 적용하는 경우 다음 절차를 수행합니다. 이 방법은 전화기에서 사용할 수 있는 소프트키 템플릿을 만드는 데 가장 일반적으로 사용되는 방법입니다.

대체 방법을 사용하려면 전화기에 QRT 소프트키 템플릿 추가, 325 페이지의 내용을 참조하십시오.

프로시저

	명령 또는 동작	목적
단계 **1**	QRT 소프트키 템플릿을 일반 장치 구성에 추가, 324 페이지	
단계 **2**	일반 디바이스 구성을 전화기에 연결, 324 페이지	

QRT 소프트키 템플릿을 일반 장치 구성에 추가

시작하기 전에

QRT 소프트키를 사용하여 소프트키 템플릿 구성, 322 페이지

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다.디바이스 > 디바이스 설정 > 일반 디바이스 구성

단계 2 다음 단계를 수행하여 새 일반 디바이스 구성을 생성 하 고 소프트키 템플릿을 해당 구성에 연결합니다. 그렇지 않으면 다음 단계를 진행합니다.

a) 새로 추가를 클릭합니다.
b) 이름 필드에 일반 디바이스 구성의 이름을 입력합니다.
c) 저장을 클릭합니다.

단계 3 기존 일반 디바이스 구성에 소프트키 템플릿을 추가하려면 다음 절차를 수행합니다.

a) 찾기를 클릭하고 검색 기준을 입력합니다.
b) 기존 일반 디바이스 구성을 클릭합니다.

단계 4 소프트키 템플릿 필드의 드롭다운 목록에서 사용하려는 소프트키가 포함된 소프트키 템플릿을 선택합니다.

단계 5 저장을 클릭합니다.

단계 6 다음 작업 중 하나를 수행합니다.

- 이미 디바이스와 연결되어 있는 일반 디바이스 구성을 수정한 경우 구성 적용을 클릭하여 디바이스를 다시 시작합니다.
- 새 일반 디바이스 구성을 만든 경우 구성을 디바이스와 연결한 다음 다시 시작합니다.

다음에 수행할 작업

일반 디바이스 구성을 전화기에 연결, 324 페이지

일반 디바이스 구성을 전화기에 연결

시작하기 전에

QRT 소프트키 템플릿을 일반 장치 구성에 추가, 324 페이지

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다.디바이스 > 전화기

단계 2 찾기를 클릭하고 전화기 디바이스를 선택하여 소프트키 템플릿을 추가합니다.

단계 3 일반 디바이스 구성 드롭다운 목록에서 새 소프트키 템플릿이 포함된 일반 디바이스 구성을 선택합니다.

단계 4 저장을 클릭합니다.

단계 5 재설정 을 클릭하여 전화기 설정을 업데이트합니다.

전화기에 QRT 소프트키 템플릿 추가

시작하기 전에

QRT 소프트키를 사용하여 소프트키 템플릿 구성, 322 페이지

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다.디바이스 > 전화기

단계 2 찾기를 클릭하여 구성된 전화기 목록을 표시합니다.

단계 3 전화기 버튼 템플릿을 추가할 전화기를 선택합니다.

단계 4 전화기 버튼 템플릿 드롭다운 목록에서 새 기능 버튼을 포함하는 새 전화기 버튼 템플릿을 선택합니다.

단계 5 저장을 클릭합니다.
전화기 설정을 업데이트하려면 재설정을 누르라는 메시지가 포함된 대화 상자가 표시됩니다.

Cisco 통합 서비스 가용성에서 QRT 구성

프로시저

	명령 또는 동작	목적
단계 1	Cisco Extended Functions 서비스 활성화, 326 페이지	Cisco 확장 기능 (CEF) 서비스를 활성화하여 Quality Report Tool과 같은 음성 품질 기능을 지원합니다.
단계 2	알람 구성, 326 페이지	QRT에 대한 알람을 구성하여 SysLog 뷰어 내 애플리케이션 로그에서 오류를 기록합니다. 이 기능은 알람을 기록하고 알람에 대한 설명과 권장 작업을 제공합니다. Cisco Unified Real-Time Monitoring Tool에서 SysLog 뷰어에 액세스할 수 있습니다.
단계 3	추적 구성, 327 페이지	음성 애플리케이션에 대한 추적 정보를 기록하기 위해 QRT에 대한 추적을 구성합니다. QRT를 위한 추적 파일에 포함할 정보를 구성한 후 Cisco Unified Real-Time Monitoring Tool

	명령 또는 동작	목적
		의 추적 및 로그 센트럴 옵션을 사용하여 추적 파일을 수집하고 볼 수 있습니다.

Cisco Extended Functions 서비스 활성화

Cisco 확장 기능 (CEF) 서비스를 활성화하여 Quality Report Tool과 같은 음성 품질 기능을 지원합니다.

프로시저

단계 **1** Cisco 통합 서비스 가용성에서 도구 > 서비스 활성화를 선택합니다.

단계 **2** 서버 드롭다운 목록에서 Cisco Extended Functions 서비스를 활성화하려는 노드를 선택합니다.

단계 **3** **Cisco Extended Functions** 확인란을 선택합니다.

단계 **4** 저장을 클릭합니다.

다음에 수행할 작업

알람 구성, 326 페이지

알람 구성

QRT에 대한 알람을 구성하여 SysLog 뷰어 내 애플리케이션 로그에서 오류를 기록합니다. 이 기능은 알람을 기록하고 알람에 대한 설명과 권장 작업을 제공합니다. Cisco Unified Real-Time Monitoring Tool에서 SysLog 뷰어에 액세스할 수 있습니다.

시작하기 전에

Cisco Extended Functions 서비스 활성화, 326 페이지

프로시저

단계 **1** Cisco 통합 서비스 가용성에서 알람 > 구성을 선택합니다.

단계 **2** 서버 드롭다운 목록에서 알람을 구성하려는 노드를 선택합니다.

단계 **3** 서비스 그룹 드롭다운 목록에서 **CM** 서비스를 선택합니다.

단계 **4** 서비스 드롭다운 목록 상자에서 **Cisco** 확장 기능 **(CEF)**을 선택합니다.

단계 **5** 로컬 Syslog 및 SDI 추적 모두에 대해 알람 활성화를 선택합니다.

단계 **6** 드롭다운 목록에서 [로컬 Syslog] 및 [SDI 추적] 모두에 대해 다음 옵션 중 하나를 선택하여 [알람 이벤트 수준]을 구성합니다.

- 긴급 —시스템을 사용할 수 없는 것으로 지정합니다.
- 알림 — 즉각적인 조치가 필요하다는 것을 나타냅니다.

- 중요—시스템이 중요한 조건을 감지합니다.
- 오류 —오류 조건이 감지된 것을 나타냅니다.
- 경고—경고 조건이 감지되었음을 나타냅니다.
- 주의 —정상이지만 중요한 상태가 감지된 것을 나타냅니다.
- 정보—정보 메시지만 나타냅니다.
- 디버그— Cisco 기술 지원 센터 엔지니어가 디버깅하는 데 사용하는 세부 이벤트 정보를 나타냅니다.

기본값은 오류입니다.

단계 **7** 저장을 클릭합니다.

다음에 수행할 작업

추적 구성, 327 페이지

추적 구성

음성 애플리케이션에 대한 추적 정보를 기록하기 위해 QRT에 대한 추적을 구성합니다. QRT를 위한 추적 파일에 포함할 정보를 구성한 후 Cisco Unified Real-Time Monitoring Tool의 추적 및 로그 센트럴 옵션을 사용하여 추적 파일을 수집하고 볼 수 있습니다.

시작하기 전에

알람 구성, 326 페이지

프로시저

단계 **1** Cisco 통합 서비스 가용성에서 추적 > 구성을 선택합니다.

단계 **2** 서버 드롭다운 목록에서 추적을 구성하려는 노드를 선택합니다.

단계 **3** 서비스 그룹 드롭다운 목록에서 **CM** 서비스를 선택합니다.

단계 **4** 서비스 드롭다운 목록 상자에서 **Cisco** 확장 기능 **(CEF)**을 선택합니다.

단계 **5** 추적 사용 확인란을 선택합니다.

단계 **6** 디버그 추적 수준 드롭다운 목록에서 다음 옵션 중 하나를 선택합니다.

- 오류—모든 오류 상태와 프로세스 및 장치 초기화 메시지를 추적합니다.
- 특수—모든 특수 조건과 정상 작업 중에 발생하는 하위 시스템 상태 전환을 추적합니다. 통화 처리 이벤트를 추적합니다.
- 상태 전환—모든 상태 전환 조건과 정상 작업 중에 발생하는 미디어 레이어 이벤트를 추적합니다.
- 중요—루틴의 중요한 모든 조건과 시작 및 종료 지점을 추적합니다. 모든 서비스에서 이 추적 수준을 사용하지는 않습니다.
- 입력_종료—모든 입력 및 종료 조건과 낮은 수준의 디버깅 정보를 추적합니다.
- 임의—모든 임의 조건과 자세한 디버깅 정보를 추적합니다.

- 상세— 알람 조건 및 이벤트를 추적합니다. 비정상 라우트에서 생성된 모든 추적에 사용됩니다. 최소 수의 CPU 주기를 사용합니다.

기본값은 오류입니다.

팁 문제 해결을 위해 이 섹션의 확인란을 모두 선택하는 것이 좋습니다.

단계 **7** 저장을 클릭합니다.

다음에 수행할 작업

(선택 사항) 품질 보고서 도구에 대한 서비스 매개 변수 구성, 328 페이지

품질 보고서 도구에 대한 서비스 매개 변수 구성

주의 Cisco TAC(기술 지원 센터)에서 다른 지침을 받은 경우 외에는 기본 서비스 매개 변수 설정을 사용하는 것이 좋습니다.

프로시저

단계 **1** Cisco Unified Communications Manager 관리에서 시스템 > 서비스 매개 변수를 선택합니다.

단계 **2** QRT 애플리케이션을 있는 노드를 선택합니다.

단계 **3** **Cisco Extended Functions** 서비스를 선택합니다.

단계 **4** 서비스 매개 변수를 구성합니다. 서비스 매개 변수 및 해당 구성 옵션에 대한 자세한 내용은 관련 항목 섹션을 참조하십시오.

단계 **5** 저장을 클릭합니다.

관련 항목

Quality Report Tool 서비스 매개 변수, 329 페이지

Quality Report Tool 서비스 매개 변수

표 *77: Quality Report Tool* 서비스 매개 변수

매개 변수	설명
확장 QRT 메뉴 선택 사항 표시	사용자에게 확장 메뉴 선택 사항을 표시할지 여부를 결정합니다. 다음 구성 옵션 중 하나를 선택할 수 있습니다. • 이 필드를 [참]으로 설정하면 확장 메뉴 선택 사항이 표시됩니다(인터뷰 모드). • 이 필드를 [거짓]으로 설정하면 확장 메뉴 선택 사항이 표시되지 않습니다(자동 모드). • 권장 기본값은 [거짓]입니다(자동 모드).
스트리밍 통계 폴링 기간	스트리밍 통계 폴링에 사용할 기간을 결정합니다. 다음 구성 옵션 중 하나를 선택할 수 있습니다. • 이 필드를 -1로 설정하면 통화가 종료될 때까지 폴링합니다. • 이 필드를 0으로 설정하면 전혀 폴링하지 않습니다. • 양수 값으로 설정하면 해당 초 동안 폴링합니다. 통화가 종료되면 폴링이 중지됩니다. • 권장 기본값은 -1(통화가 종료될 때까지 폴링)입니다.
스트리밍 통계 폴링 빈도(초)	각 폴링 사이에 대기할 시간(초)을 입력합니다. 값 범위는 30에서 3600 사이입니다. 권장 기본값은 30입니다.
최대 파일 수	최대 파일 수를 입력합니다. 이 수를 넘으면 파일 수 계산이 재시작되고 이전 파일을 덮어씁니다. 유효한 값은 1~10000입니다. 권장 기본값은 250입니다.
파일 당 최대 줄 수	각 파일의 최대 줄 수를 지정합니다. 이 수를 넘으면 다음 파일이 시작됩니다: • 값 범위는 100에서 2000 사이입니다. • 권장 기본값은 2000을 지정합니다.

매개 변수	설명
CTI 매니저 보안 연결을 위한 CAPF 프로파일 인스턴스 ID	Cisco Extended Function 서비스에서 CTI 매니저에 대한 보안 연결을 열 때 사용하는 애플리케이션 사용자 CCMQRTSysUser에 대한 애플리케이션 CAPF 프로파일의 인스턴스 ID를 입력합니다. CTI 관리자 연결 보안 플래그를 활성화한 경우 이 매개 변수를 구성해야 합니다. 참고 CTI 매니저 연결 보안 플래그 서비스 매개 변수를 활성화하여 보안을 설정해야 합니다. 변경 사항을 적용하려면 Cisco Extended Functions 서비스를 재시작해야 합니다.
CTI 매니저 연결 보안 플래그	Cisco Extended Functions 서비스 CTI 매니저 연결에 대한 보안을 활성화할지 여부를 지정합니다. 활성화하는 경우 Cisco Extended Functions에서는 애플리케이션 사용자 CCMQRTSysUser의 인스턴스 ID에 대해 구성된 애플리케이션 CAPF 프로파일을 사용하여 CTI 관리자에 대한 보안 연결을 엽니다. 선택할 수 있는 값은 [참]과 [거짓]입니다. CTI에 대한 보안 연결을 활성화하려면 [참]을 선택해야 합니다.

VI 부

보안 관리

- SAML Single Sign-On 관리, 333 페이지
- 인증서 관리, 343 페이지
- 벌크 인증서 관리, 361 페이지
- IPSec 정책 관리, 365 페이지
- 인증 정책 관리, 367 페이지

23 장

SAML Single Sign-On 관리

- SAML Single Sign-On 개요, 333 페이지
- iOS에서 Cisco Jabber용 인증서 기반 SSO 인증을 위한 옵트인 제어, 333 페이지
- SAML Single Sign-On 필수 구성 요소, 334 페이지
- SAML Single Sign-On 관리, 335 페이지

SAML Single Sign-On 개요

SAML Single Sign-On(SSO)을 사용하여 이러한 애플리케이션 중 하나에 로그인한 후 Cisco 애플리케이션의 정의된 집합에서 액세스할 수 있습니다. SAML은 신뢰할 수 있는 비즈니스 파트너 간의 보안 관련 정보 교환에 대해 설명합니다. 이것은 사용자를 인증하기 위해 서비스 제공자(예: Cisco Unified Communications Manager)에서 사용하는 인증 프로토콜입니다. SAML을 사용하여 IdP(ID 공급자)와 서비스 공급자 간에 보안 인증 정보가 교환됩니다. 기능은 다양한 애플리케이션 간에 일반 인증서 및 관련 정보를 사용하는 보안 메커니즘을 제공합니다.

SAML SSO는 메타데이터 및 인증서를 프로비저닝 프로세스의 일부로 IdP와 서비스 제공자 간에 교환하여 CoT(Circle of Trust)를 설정합니다. 서비스 제공자는 IdP의 사용자 정보를 신뢰하여 다양한 서비스 또는 애플리케이션에 대한 액세스를 제공합니다.

클라이언트가 IdP를 인증하고 IdP는 클라이언트에 어설션을 부여합니다. 클라이언트는 서비스 제공자에 어설션을 제공합니다. CoT가 설정되었으므로 서비스 제공자는 어설션을 신뢰하고 클라이언트에 대한 액세스를 부여합니다.

iOS에서 Cisco Jabber용 인증서 기반 SSO 인증을 위한 옵트인 제어

Cisco Unified Communications Manager의 이 릴리스는 IdP(ID 공급자)를 사용하여 iOS SSO 로그인 동작에서 Cisco Jabber를 제어하기 위한 옵트인 구성 옵션을 소개합니다. 이 옵션을 사용하면 Cisco Jabber에서 제어되는 모바일 장치 관리(MDM) 배포에서 IdP를 사용하여 인증서 기반 인증을 수행할 수 있습니다.

Cisco Unified Communications Manager의 **iOS**용 **SSO** 로그인 동작 엔터프라이즈 매개 변수를 통해 옵트인 제어를 구성할 수 있습니다.

참고 이 매개 변수의 기본값을 변경하기 전에 http://www.cisco.com/c/en/us/support/unified-communications/jabber-windows/tsd-products-support-series-home.html에서 Cisco Jabber 기능 지원 및 설명서를 참조하여 iOS의 Cisco Jabber가 SSO 로그인 동작 및 인증서 기반 인증을 지원하는지 확인하십시오.

이 기능을 활성화하려면 iOS에 Cisco Jabber용 SSO 로그인 동작 구성, 336 페이지 절차를 참조하십시오.

SAML Single Sign-On 필수 구성 요소

- Cisco Unified Communications Manager 클러스터를 위해 구성된 DNS
- IdP(ID 공급자) 서버
- IdP 서버에서 신뢰하고 시스템에서 지원하는 LDAP 서버

SAML 2.0을 사용하는 다음 IdP는 SAML SSO 기능에 대해 테스트됩니다.

- OpenAM 10.0.1
- Microsoft® Active Directory® 페더레이션 서비스 2.0(AD FS 2.0)
- PingFederate® 6.10.0.4
- F5 BIP-IP 11.6.0

타사 애플리케이션은 다음과 같은 구성 요구 사항을 충족해야 합니다.

- IdP에 필수 특성 “uid”를 구성해야 합니다. 이 특성은 Cisco Unified Communications Manager에서 LDAP 동기화된 사용자 ID로 사용되는 특성과 일치해야 합니다.
- SAML SSO에 참여하는 모든 엔티티의 시계를 동기화해야 합니다. 시계를 동기화하는 방법에 대한 내용은 http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html의 *Cisco Unified Communications Manager* 시스템 구성 설명서에서 “NTP 설정”을 참조하십시오.

SAML Single Sign-On 관리

SAML Single Sign-On 활성화

참고 동기화 에이전트 테스트 확인에 성공하기 전까지는 SAML SSO를 활성화할 수 없습니다.

시작하기 전에

- 사용자 데이터가 Cisco Unified Communications Manager 데이터베이스에 동기화되었는지 확인합니다. 자세한 내용은 http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html에서 *Cisco Unified Communications Manager* 시스템 구성 설명서를 참조하십시오.
- Cisco Unified CM IM and Presence Service Cisco 동기화 에이전트 서비스에서 데이터 동기화를 성공적으로 완료했는지 확인합니다. **Cisco Unified CM IM and Presence** 관리 > 진단 > 시스템 문제 해결 도구를 선택하여 이 테스트의 상태를 확인합니다. “Sync Agent에서 관련 데이터(예: 장치, 사용자, 라이센싱 정보)를 동기화함” 테스트에서는 데이터 동기화가 성공적으로 완료된 경우 "테스트 통과" 결과를 표시합니다.
- 하나 이상의 LDAP 동기화된 사용자가 표준 CCM 수퍼 사용자 그룹에 추가되어 Cisco Unified CM 관리에 액세스할 수 있는지 확인합니다. 자세한 내용은 http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html에서 *Cisco Unified Communications Manager* 시스템 구성 설명서를 참조하십시오.
- IdP와 서버 간 신뢰 관계를 구성하려면 먼저 IdP에서 신뢰 메타데이터 파일을 얻은 후 모든 서버로 가져와야 합니다.

프로시저

단계 **1** [Cisco Unified CM 관리]에서 시스템 > **SAML Single Sign-On**을 선택합니다.
단계 **2** **SAML SSO** 활성화를 클릭합니다.
단계 **3** 모든 서버 연결이 다시 시작될 것임을 알려주는 경고 메시지가 표시되면 계속을 클릭합니다.
단계 **4** 찾아보기를 클릭하여 IdP 메타데이터를 찾고 업로드합니다.
단계 **5** **IdP** 메타데이터 가져오기를 클릭합니다.
단계 **6** 다음을 클릭합니다.
단계 **7** 신뢰 메타데이터 파일 집합 다운로드를 클릭하여 서버 메타데이터를 시스템으로 다운로드합니다.
단계 **8** IdP 서버에서 서버 메타데이터를 업로드합니다.
단계 **9** 다음을 클릭하여 작업을 계속합니다.

단계 **10** 유효한 관리자 ID 목록에서 관리자 권한이 있는 LDAP 동기화된 사용자를 선택합니다.

단계 **11** 테스트 실행을 클릭합니다.

단계 **12** 유효한 사용자 이름과 암호를 입력합니다.

단계 **13** 성공 메시지가 표시되면 브라우저 창을 닫습니다.

단계 **14** 완료를 클릭하고 웹 애플리케이션이 다시 시작될 때까지 1 ~ 2분 기다립니다.

iOS에 Cisco Jabber용 SSO 로그인 동작 구성

프로시저

단계 **1** [Cisco Unified CM 관리]에서 시스템 > 엔터프라이즈 매개 변수를 선택합니다.

단계 **2** 옵트인 제어를 구성하려면 SSO 구성 섹션에서 **iOS**에 대한 **SSO** 로그인 동작 매개 변수에 대해 기본 브라우저 사용 옵션을 선택합니다.

참고 **iOS**에 대한 **SSO** 로그인 동작 매개 변수는 다음 옵션을 포함합니다.

- 포함된 브라우저 사용—이 옵션을 활성화하면 Cisco Jabber는 SSO 인증을 위해 포함된 브라우저를 사용합니다. 이 옵션을 사용하여 기본 Apple Safari 브라우저로 교차 실행하지 않고 버전 9 이전의 iOS 장치에서 SSO를 사용할 수 있습니다. 이 옵션은 기본적으로 활성화되어 있습니다.
- 기본 브라우저 사용—이 옵션을 활성화하면 Cisco Jabber는 iOS 장치의 Apple Safari 프레임워크를 사용하여 MDM 배포에서 IdP(Identity Provider)를 사용하여 인증서 기반 인증을 수행합니다.

  참고 기본 브라우저 사용은 포함된 브라우저 사용만큼 안전하지 않으므로 제어된 MDM 배포를 제외하고 이 옵션을 구성하는 것이 좋습니다.

단계 **3** 저장을 클릭합니다.

업그레이드한 후 WebDialer에서 SAML Single Sign-on 활성화

업그레이드 후에 Cisco WebDialer에서 SAML Single Sign-On을 다시 활성화하려면 이 작업을 수행합니다. SAML Single Sign-On을 활성화하기 전에 Cisco WebDialer가 활성화된 경우 Cisco WebDialer에서 기본적으로 SAML Single Sign-On이 활성화되지 않습니다.

프로시저

	명령 또는 동작	목적
단계 1	Cisco WebDialer 서비스 비활성화, 337 페이지	Cisco WebDialer 웹 서비스가 이미 활성화되어 있는 경우 비활성화합니다.
단계 2	SAML Single Sign-On 비활성화, 337 페이지	SAML Single Sign-on이 이미 활성화 되어 있는 경우 비활성화합니다.
단계 3	Cisco WebDialer 서비스 활성화, 338 페이지	
단계 4	SAML Single Sign-On 활성화, 335 페이지	

Cisco WebDialer 서비스 비활성화

Cisco WebDialer 웹 서비스가 이미 활성화되어 있는 경우 비활성화합니다.

프로시저

단계 1 Cisco 통합 서비스 가용성에서 도구 > 서비스 활성화를 선택합니다.
단계 2 서버 드롭다운 목록에서 나열된 Cisco Unified Communications Manager 서버를 선택합니다.
단계 3 **CTI** 서비스에서 **Cisco WebDialer** 웹 서비스 확인란을 선택 취소합니다.
단계 4 저장을 클릭합니다.

다음에 수행할 작업

SAML Single Sign-On 비활성화, 337 페이지

SAML Single Sign-On 비활성화

SAML Single Sign-on이 이미 활성화 되어 있는 경우 비활성화합니다.

시작하기 전에

Cisco WebDialer 서비스 비활성화, 337 페이지

프로시저

CLI에서 명령 **utils sso disable**을 실행합니다.

다음에 수행할 작업

Cisco WebDialer 서비스 활성화, 338 페이지

Cisco WebDialer 서비스 활성화

시작하기 전에

SAML Single Sign-On 비활성화, 337 페이지

프로시저

단계 **1** Cisco 통합 서비스 가용성에서 다음 메뉴를 선택합니다.도구 > 서비스 활성화.

단계 **2** 서버 드롭다운 목록에서 나열된 Unified Communications Manager 서버를 선택합니다.

단계 **3** **CTI** 서비스에서 **Cisco WebDialer** 웹 서비스 확인란을 선택합니다.

단계 **4** 저장을 클릭합니다.

단계 **5** Cisco 통합 서비스 가용성에서 다음 메뉴를 선택합니다.도구 > 제어 센터 - 기능 서비스를 선택하여 CTI 관리자 서비스가 활성 상태이며 시작 모드인지 확인합니다.

Webdialer가 제대로 작동하려면 CTI 관리자 서비스를 활성화하고 시작 모드에 있어야합니다.

다음에 수행할 작업

SAML Single Sign-On 활성화, 335 페이지

복구 URL에 액세스

복구 URL을 사용하면 문제 해결을 위해 SAML Single Sign-On을 우회하여 Cisco Unified Communications Manager 관리 및 Cisco Unified CM IM and Presence Service 인터페이스에 로그인할 수 있습니다. 예를 들어, 서버의 도메인 또는 호스트 이름을 변경하기 전에 복구 URL을 활성화합니다. 복구 URL에 로그인하여 서버 메타데이터를 손쉽게 업데이트할 수 있습니다.

참고 복구 URL은 셀프 서비스 포털에 로그인하려는 최종 사용자(LDAP 또는 로컬)에 대해 작동하지 않습니다.

시작하기 전에

- 관리 권한이 있는 애플리케이션 사용자만 복구 URL에 액세스할 수 있습니다.
- SAML SSO가 활성화된 경우, 복구 URL은 기본적으로 활성화됩니다. CLI에서 복구 URL을 활성화하거나 비활성화할 수 있습니다. 복구 URL을 활성화 및 비활성화하기 위한 CLI 명령에 대한 자세한 내용은 *Command Line Interface Guide for Cisco Unified Communications Solutions*를 참조하십시오.

프로시저

브라우저에 `https://hostname:8443/ssosp/local/login`을 입력합니다.

도메인 또는 호스트 이름 변경 후 서버 메타데이터 업데이트

도메인 또는 호스트 이름을 변경한 후 이 절차를 수행할 때까지 SAML Single Sign-On이 작동하지 않습니다.

참고 이 절차를 수행한 후에도 **SAML Single Sign-On** 창에 액세스할 수 없는 경우에는 브라우저 캐시를 지우고 다시 로그인해 보십시오.

시작하기 전에

복구 URL이 비활성화된 경우 Single Sign-On 링크를 우회할 URL이 나타나지 않습니다. 복구 URL을 활성화하려면 CLI에 로그인하고 **utils sso recovery-url enable**명령을 실행합니다.

프로시저

단계 **1** 웹 브라우저의 주소 표시줄에 다음 URL을 입력합니다.

`https://<Unified CM-server-name>`

여기서 `<Unified CM-server-name>`는 서버의 호스트 이름 또는 IP 주소입니다.

단계 **2** **Single Sign On(SSO)**를 우회할 복구 **URL**을 클릭합니다.

단계 **3** 관리자 역할을 가진 애플리케이션 사용자의 자격 증명을 입력하고 로그인을 클릭합니다.

단계 **4** [Cisco Unified CM 관리]에서 시스템 > **SAML Single Sign-On**을 선택합니다.

단계 **5** 메타데이터 내보내기를 클릭하여 서버 메타데이터를 다운로드합니다.

단계 **6** 서버 메타데이터 파일을 IdP에 업로드합니다.

단계 **7** 테스트 실행을 클릭합니다.

단계 **8** 올바른 사용자 ID 및 암호를 입력합니다.

단계 **9** 성공 메시지가 표시되면 브라우저 창을 닫습니다.

서버를 삭제한 후 서버 메타데이터 업데이트

클러스터 수준 SSO 통합에서 서버를 클러스터에서 삭제한 후 IdP와의 인덱스 불일치를 방지하기 위해 메타데이터를 다시 가져와야 합니다.

시작하기 전에

참고 복구 URL이 비활성화된 경우 Single Sign-On 링크를 우회할 URL이 나타나지 않습니다. 복구 URL을 활성화하려면 CLI에 로그인하고 **utils sso recovery-url enable**명령을 실행합니다.

프로시저

단계 **1** 웹 브라우저의 주소 표시줄에 다음 URL을 입력합니다.

`https://<Unified CM-server-name>`

여기서 `<Unified CM-server-name>`는 서버의 호스트 이름 또는 IP 주소입니다.

단계 **2** **Single Sign On(SSO)**를 우회할 복구 **URL**을 클릭합니다.

단계 **3** 관리자 역할을 가진 애플리케이션 사용자의 자격 증명을 입력하고 로그인을 클릭합니다.

단계 **4** Cisco Unified CM 관리에서 시스템 > **SAML** 싱글 사인-온을 선택합니다.

단계 **5** 메타데이터 내보내기를 클릭하여 서버 메타데이터를 다운로드합니다.

단계 **6** 서버 메타데이터 파일을 IdP에 업로드합니다.

단계 **7** 테스트 실행을 클릭합니다.

단계 **8** 올바른 사용자 ID 및 암호를 입력합니다.

단계 **9** 성공 메시지가 표시되면 브라우저 창을 닫습니다.

서버 메타데이터 수동 프로비저닝

여러 개의 UC 애플리케이션에 대한 ID 공급자에서 단일 연결을 설정하려면 ID 공급자 및 서비스 공급업체 사이에 신뢰할 수 있는 범위를 구성하는 한편, 서버 메타데이터를 수동으로 설정해야 합니다. 신뢰할 수 있는 범위를 구성하는 방법에 대한 자세한 내용은 IdP 제품 설명서를 참조하십시오.

일반적인 URL 구문은 다음과 같습니다.

`https://<SP FQDN>:8443/ssosp/saml/SSO/alias/<SP FQDN>`

프로시저

서버 메타데이터를 수동으로 설정하려면 ACS(Assertion Customer Service) URL을 사용합니다.

예제:

샘플 ACS URL: `<md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"`

```
Location="https://cucm.ucsso.cisco.com:8443/ssosp/saml/SSO/alias/cucm.ucsso.cisco.com"
index="0"/>
```

24 장

인증서 관리

- 인증서 개요, 343 페이지
- 인증서 표시, 347 페이지
- 인증서 다운로드, 347 페이지
- 중간 인증서 설치, 348 페이지
- 신뢰 인증서 삭제, 348 페이지
- 인증서 다시 생성, 349 페이지
- 인증서 또는 인증서 체인 업로드, 352 페이지
- 타사 CA(인증기관) 인증서 관리, 352 페이지
- 온라인 인증서 상태 프로토콜을 통한 인증서 해지, 355 페이지
- 인증서 모니터링 작업 흐름, 356 페이지
- 인증서 오류 문제 해결, 359 페이지

인증서 개요

시스템은 자체 서명 인증서 및 타사 서명 인증서를 사용합니다. 인증서는 장치를 안전하게 인증하고 데이터를 암호화하고 데이터를 해싱하여 소스와 대상 간의 무결성을 보장하기 위해 시스템의 장치 간에 사용됩니다. 인증서를 사용하면 대역폭, 통신 및 작업을 안전하게 전송할 수 있습니다.

인증서의 가장 중요한 부분은 데이터를 암호화하고 대상 웹사이트, 전화 또는 FTP 서버와 같은 항목과 공유하는 방법을 숙지하고 정의하는 것입니다.

시스템이 인증서를 신뢰하는 경우 올바른 대상과 정보를 공유하는 것을 완벽하게 신뢰할 수 있도록 시스템에 인증서가 미리 설치되어 있음을 의미합니다. 그렇지 않으면, 이러한 지점 간 통신은 종료됩니다.

인증서를 신뢰하기 위해서는 타사 인증 기관(CA)과 미리 신뢰가 설정되어 있어야 합니다.

장치가 CA 및 중간 인증서를 먼저 신뢰할 수 있음을 알고 있어야 보안 소켓 레이어(SSL) 핸드셰이크라고 하는 메시지를 교환하여 제공되는 서버 인증서를 신뢰할 수 있습니다.

참고 Tomcat용 EC 기반 인증서가 지원됩니다. 이 새로운 인증서를 tomcat-ECDSA라고 합니다. 자세한 내용은 *Cisco Unified Communications Manager*의 *IM and Presence Service* 구성 및 관리의 IM and Presence Service 섹션에서 향상된 TLS 암호화를 참조하십시오.

Tomcat 인터페이스의 EC Ciphers는 기본적으로 비활성화됩니다. Cisco Unified Communications Manager 또는 IM and Presence Service에서 **HTTPS** 암호 엔터프라이즈 매개 변수를 사용하여 활성화할 수 있습니다. 이 매개 변수를 변경하는 경우 모든 노드에서 Cisco Tomcat 서비스를 다시 시작해야 합니다.

EC-기반 인증서에 대한 자세한 내용은 Cisco Unified Communications Manager 및 IM and Presence Service에서 릴리스 노트의 승인된 솔루션을 위한 일반 기준에 대한 ECDSA 지원을 참조하십시오.

타사 서명 인증서 또는 인증서 체인

애플리케이션 인증서를 서명한 인증 기관의 인증 기관 루트 인증서를 업로드합니다. 하위 인증 기관이 애플리케이션 인증서를 서명한 경우 하위 인증 기관의 인증 기관 루트 인증서를 업로드해야 합니다. 모든 인증 기관 인증서의 PKCS#7 형식 인증서 체인을 업로드할 수도 있습니다.

동일한 인증서 업로드 대화 상자를 사용하여 인증 기관 루트 인증서 및 애플리케이션 인증서를 업로드할 수 있습니다. 인증 기관 루트 인증서 또는 인증 기관 인증서만 포함된 인증서 체인을 업로드할 때는 형식 인증서 type-trust인 인증서 이름을 선택합니다. 애플리케이션 인증서 또는 애플리케이션 인증서와 인증 기관 인증서를 포함하는 인증서 체인을 업로드할 때는 인증서 유형만 포함하는 인증서 이름을 선택합니다.

예를 들어, Tomcat 인증 기관 인증서 또는 인증 기관 인증서 체인을 업로드할 때는 **tomcat-trust**를 선택하고 Tomcat 애플리케이션 인증서 또는 애플리케이션 인증서와 인증 기관 인증서를 포함하는 인증서 체인을 업로드할 때는 **tomcat** 또는 **tomcat ECDSA**를 선택합니다.

CAPF 인증 기관 루트 인증서를 업로드할 때 CallManager-trust 저장소로 복사되므로 하지 CallManager용 인증 기관 루트 인증서를 별도로 업로드할 필요가 없습니다.

참고 타사 인증 기관에서 서명한 인증서를 성공적으로 업로드하면 서명된 인증서를 가져오는 데 사용된 최근에 생성된 CSR을 삭제하고 타사에서 서명한 인증서(업로드한 경우)를 포함하여 기존 인증서를 덮어씁니다.

참고 시스템은 tomcat-trust, CallManager-trust 및 Phone-SAST-trust 인증서를 클러스터의 각 노드에 자동으로 복제합니다.

참고 디렉터리 신뢰 인증서를 tomcat-trust에 업로드할 수 있으며, 이는 DirSync 서비스가 보안 모드에서 작동하는 데 필요합니다.

타사 인증 기관 인증서

타사 인증 기관이 발행하는 애플리케이션 인증서를 사용하려면 인증 기관 또는 PKCS #7 인증서 체인에서 서명된 애플리케이션 인증서 및 인증 기관 루트 인증서를 모두 얻어야 합니다(구별된 인코딩 규칙 [DER]). 여기에는 애플리케이션 인증서와 인증 기관 인증서가 모두 포함됩니다. 인증 기관에서 이러한 인증서를 받는 방법에 대한 정보를 검색합니다. 프로세스는 인증 기관마다 다릅니다. 서명 알고리즘은 RSA 암호화를 사용해야 합니다.

Cisco Unified Communications 운영 체제는 프라이버시 향상 메일(PEM) 인코딩 형식으로 CSR을 생성합니다. 시스템은 DER 및 PEM 인코딩 형식의 인증서와 PEM 형식의 PKCS #7 인증서 체인을 사용할 수 있습니다. CAPF(인증 기관 프록시 기능)를 제외한 모든 인증서 유형의 경우 인증 기관 루트 인증서와 애플리케이션 인증서를 받아 각 노드에 업로드해야 합니다.

CAPF의 경우 인증 기관 루트 인증서와 애플리케이션 인증서를 받아 첫 번째 노드에만 업로드합니다. CAPF 및 Unified Communications ManagerCSR은 인증 기관으로부터 애플리케이션 인증서 요청 시 포함해야 하는 확장을 포함합니다. 인증 기관이 ExtensionRequest 메커니즘을 지원하지 않을 경우 다음과 같이 X.509 확장을 활성화해야 합니다.

- CAPF CSR은 다음 확장을 사용합니다.

```
X509v3 확장 키 사용: TLS, 웹 서버 인증 X509v3 키 사용: 디지털 서명, 인증서 서명
```

- Tomcat 및 Tomcat-ECDSA용 CSR은 다음과 같은 확장을 사용합니다.

참고 Tomcat 또는 Tomcat-ECDSA 는 키 계약 또는 IPsec 엔드 시스템 키 사용을 요구하지 않습니다.

```
X509v3 확장 키 사용: TLS 웹 서버 인증, TLS 웹 클라이언트 인증, IPSec 엔드 시스템
X509v3 키 사용: 디지털 서명, 키 암호화, 데이터 암호화, 키 계약
```

- IPsec용 CSR은 다음 확장을 사용합니다.

```
 X509v3 확장 키 사용: TLS 웹 서버 인증, TLS 웹 클라이언트 인증, IPSec 엔드 시스템
X509v3 키 사용: 디지털 서명, 키 암호화, 데이터 암호화, 키 계약
```

- Unified Communications Manager용 CSR은 다음 확장을 사용합니다.

```
X509v3 확장 키 사용: TLS 웹 서버 인증, TLS 웹 클라이언트 인증 X509v3 키 사용: 디지털
 서명, 키 암호화, 데이터 암호화, 키 계약
```

- IM and Presence Service cup 및 cup-xmpp 인증서에 대한 CSR은 다음 확장을 사용합니다.

```
X509v3 확장 키 사용: TLS 웹 서버 인증, TLS 웹 클라이언트 인증, IPSec 엔드 시스템
X509v3 키 사용: 디지털 서명, 키 암호화, 데이터 암호화, 키 계약,
```

참고 인증서에 대한 CSR을 생성하고 SHA256 서명을 사용하여 타사 인증 기관이 서명하도록 할 수 있습니다. 그런 다음 이 서명된 인증서를 다시 Unified Communications Manager에 업로드하여, Tomcat 및 기타 인증서가 SHA256을 지원할 수 있습니다.

인증서 서명 요청 키 사용 확장

다음 표에는 Unified Communications Manager 및 IM and Presence Service CA 인증서에 대한 인증서 서명 요청(CSR)의 주요 용도 확장이 나와 있습니다.

표 ***78: Cisco Unified Communications Manager CSR*** 키 용도 확장

	다중 서버	확장 키 사용			키 사용				
		서버 인증 **(1.3.6.1.5.5.7.3.1)**	클라이언트 인증 **(1.3.6.1.5.5.7.3.2)**	**IP** 보안 엔드 시스템 **(1.3.6.1.5.5.7.3.5)**	디지털 서명	키 암호화	데이터 암호화	키 인증서 서명	키 계약
CallManager CallManager-ECDSA	Y	Y	Y		Y	Y	Y		
CAPF(게시자에만 해당)	N	Y			Y	N		Y	
ipsec	N	Y	Y	Y	Y	Y	Y		
tomcat tomcat-ECDSA	Y	Y	Y		Y	Y	Y		
TVS	N	Y	Y		Y	Y	Y		

표 ***79: IM and Presence Service CSR*** 키 사용 확장

	다중 서버	확장 키 사용			키 사용				
		서버 인증 **(1.3.6.1.5.5.7.3.1)**	클라이언트 인증 **(1.3.6.1.5.5.7.3.2)**	**IP** 보안 엔드 시스템 **(1.3.6.1.5.5.7.3.5)**	디지털 서명	키 암호화	데이터 암호화	키 인증서 서명	키 계약
cup cup-ECDSA	N	Y	Y	Y	Y	Y	Y		
cup-XMPP cup-xmpp-ECDSA	Y	Y	Y	Y	Y	Y	Y		
cup-XMPP-s2s cup-xmpp-s2s-ECDSA	Y	Y	Y	Y	Y	Y	Y		
ipsec	N	Y	Y	Y	Y	Y	Y		
tomcat tomcat-ECDSA	Y	Y	Y		Y	Y	Y		

참고 '데이터 암호화' 비트가 CA 서명 인증서 프로세스의 일부로 변경되거나 제거되지 않았는지 확인하십시오.

인증서 표시

인증서 목록 페이지의 필터 옵션을 사용하여 공통 이름, 만료 날짜, 키 유형 및 사용법을 기준으로 인증서 목록을 정렬하고 조회합니다. 따라서 필터 옵션을 사용하면 데이터를 효과적으로 정렬, 조회 및 관리할 수 있습니다.

Unified Communications Manager 릴리스 14에서, 사용 옵션을 선택하여 ID 또는 신뢰 인증서 목록을 정렬 및 조회할 수 있습니다.

프로시저

단계 **1** Cisco Unified OS 관리에서 보안 > 인증서 관리를 선택합니다.
인증서 목록 페이지가 나타납니다.

단계 **2** 인증서 목록 찾기 드롭다운 목록에서 필수 필터 옵션을 선택하고 찾기 필드에 검색 항목을 입력한 다음, 찾기 버튼을 클릭합니다.

예를 들면, ID 인증서만 조회하려면 사용을 인증서 목록 찾기 드롭다운 목록에서 선택하고, 찾기 필드에 ID를 입력한 다음, 찾기 버튼을 클릭합니다.

인증서 다운로드

인증서 다운로드 작업을 사용하여 인증서 사본을 가져오거나 CSR 요청을 제출할 때 인증서를 업로드할 수 있습니다.

프로시저

단계 **1** Cisco Unified OS 관리에서 보안 > 인증서 관리를 선택합니다.

단계 **2** 검색 기준을 지정하고 찾기를 클릭합니다.

단계 **3** 필요한 파일 이름을 선택하고 다운로드를 클릭합니다.

중간 인증서 설치

중간 인증서를 설치하려면 먼저 루트 인증서를 설치하고 서명된 인증서를 업로드해야 합니다. 이 단계는 특정 체인에서 여러 인증서가 있는 서명된 인증서를 인증기관에서 제공하는 경우에만 필요합니다.

프로시저

단계 **1** Cisco Unified OS 관리에서 보안 > 인증서 관리를 클릭합니다.

단계 **2** 인증서/인증서 체인 업로드를 클릭합니다.

단계 **3** 인증서 용도 드롭다운 목록에서 적절한 신뢰 저장소를 선택하여 루트 인증서를 설치합니다.

단계 **4** 선택한 인증서 용도에 대한 설명을 입력합니다.

단계 **5** 다음 단계 중 하나를 수행하여 업로드할 파일을 선택합니다.

- 파일 업로드 텍스트 상자에서 파일의 경로를 입력합니다.
- 찾아보기를 클릭하고 파일을 탐색한 다음 열기를 클릭합니다.

단계 **6** 업로드를 클릭합니다.

단계 **7** 고객 인증서를 설치한 후 FQDN을 사용하여 Cisco Unified Intelligence Center URL에 액세스합니다. IP 주소를 사용하여 Cisco Unified Intelligence Center에 액세스하는 경우 사용자 지정 인증서를 성공적으로 설치한 후에도 "계속 하려면 여기를 클릭해야 합니다." 메시지가 표시됩니다.

참고
- Tomcat 인증서가 업로드되면 TFTP 서비스를 다시 시작해야 합니다. 그렇지 않으면 TFTP는 이전 캐시된 자체 서명 tomcat 인증서를 계속 제공하게 됩니다.

신뢰 인증서 삭제

신뢰할 수 있는 인증서는 삭제할 수 있는 유일한 인증서 유형입니다. 시스템에서 생성되는 자체 서명된 인증서는 삭제할 수 없습니다.

⚠

주의 인증서를 삭제하면 시스템 작동에 영향을 미칠 수 있습니다. 또한 인증서가 기존 체인의 일부인 경우 인증서 체인이 끊어질 수 있습니다. 인증서 목록 창에서 관련 인증서의 사용자 이름 및 제목 이름에서 이 관계를 확인합니다. 이 작업은 취소할 수 없습니다.

프로시저

단계 **1** Cisco Unified OS 관리에서 보안 > 인증서 관리를 선택합니다.

단계 **2** 찾기 제어를 사용하여 인증서 목록을 필터링합니다.

단계 **3** 인증서의 파일 이름을 선택합니다.

단계 **4** 삭제를 클릭합니다.

단계 **5** 확인을 클릭합니다.

참고
- "CAPF-trust", "tomcat-trust", "CallManager-trust" 또는 "Phone-SAST-trust" 인증서 유형을 삭제하는 경우 클러스터의 모든 서버에서 인증서가 삭제됩니다.
- CAPF-trust로 인증서를 가져오는 경우 해당 특정 노드에서만 활성화되고 클러스터 전체에 복제되지 않습니다.

인증서 다시 생성

인증서가 만료되기 전에 재생성하는 것이 좋습니다. 인증서가 만료될 때 RTMT(Syslog 뷰어)와 이메일 알림을 받게 됩니다.

그러나 만료된 인증서를 재생성할 수도 있습니다. 전화기를 다시 시작하고 서비스를 다시 부팅해야 하기 때문에 업무 시간이 끝난 후 이 절차를 수행합니다. Cisco Unified OS 관리에서 유형이 "cert"로 나열되는 인증서만 재생성할 수 있습니다.

⚠

주의 인증서를 다시 생성하면 시스템 작동에 영향을 미칠 수 있습니다. 인증서를 다시 생성하면 업로드된 경우 타사 서명 인증서를 포함하여 기존 인증서를 덮어씁니다.

프로시저

단계 **1** Cisco Unified OS 관리에서 보안 > 인증서 관리를 선택합니다.

검색 매개변수를 입력하여 인증서를 찾고 해당 구성 세부 정보를 봅니다. 인증서 목록 창의 모든 기준과 일치하는 레코드가 표시됩니다.

인증서 세부 정보 페이지에서 재생성 버튼을 클릭하면 키 길이가 동일한 자체 서명 인증서가 재생성됩니다.

참고 인증서를 다시 생성할 때 인증서 설명 필드는 재생성 창을 닫고 새로 생성된 인증서를 열 때까지 업데이트 되지 않습니다.

자체 서명 인증서 생성을 클릭하여 새 키 길이가 3072 또는 4096인 자체 서명 인증서를 재생성합니다.

단계 **2** 새 자체 서명 인증서 생성 창에서 필드를 구성합니다. 필드 및 해당 구성 옵션에 대한 자세한 내용은 온라인 도움말을 참조하십시오.

단계 **3** 생성을 클릭합니다.

단계 **4** 다시 생성된 인증서의 영향을 받는 모든 서비스를 다시 시작합니다.

단계 **5** CAPF, ITLRecovery 인증서 또는 CallManager 인증서를 재생성한 후에 CTL 파일(필요한 경우)을 업데이트합니다.

참고 인증서를 다시 생성한 후 최신 백업이 다시 생성된 인증서를 포함하도록 시스템 백업을 수행해야 합니다. 백업에 다시 생성된 인증서가 포함되어 있지 않고 시스템 복원 작업을 수행하는 경우 전화기를 등록할 수 있도록 시스템에서 각 전화기를 수동으로 잠금 해제해야 합니다.

중요 CallManager, CAPF 및 TVS 인증서를 다시 생성/갱신한 후에는 업데이트된 ITL 파일을 수신하도록 전화기가 자동으로 재설정됩니다.

인증서 이름 및 설명

다음 표에서는 다시 생성할 수 있는 시스템 보안 인증서 및 다시 시작해야 하는 관련 서비스에 대해 설명합니다. TFTP 인증서 다시 생성에 대한 자세한 내용은 http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html에서 *Cisco Unified Communications Manager* 보안 설명서를 참조하십시오.

표 ***80:*** 인증서 이름 및 설명

이름	설명	다시 시작할 서비스
tomcat tomcat-ECDSA	이 인증서는 SIP Oauth 모드가 활성화되어 있는 경우 WebServices, Cisco DRF 서비스 및 Cisco CallManager 서비스에서 사용합니다.	Cisco 톰캣 서비스, Cisco 콜매니저 서비스
CallManager CallManager-ECDSA	이는 SIP, SIP 트렁크, SCCP, TFTP 등에 사용됩니다.	Cisco Call Manager 서비스 및 Cisco CTI Manager를 포함한 기타 관련 서비스 - 서버가 보안 모드인 경우 CTL 파일을 업데이트합니다. CallManager-ECDSA - Cisco CallManager 서비스.
CAPF	Unified Communications Manager 퍼블리셔에서 실행되는 CAPF 서비스에서 사용합니다. 이 인증서는 엔드포인트에 LSC를 발급하기 위해 사용됩니다(온라인 및 오프 라인 CAPF 모드 제외).	해당 없음

이름	설명	다시 시작할 서비스
TVS	이는 서버 인증서가 변경되는 경우 전화기에 대한 보조 신뢰 확인 방법의 역할을 담당하는 TVS(Trust Verification Service, 신뢰 확인 서비스)에서 사용합니다.	해당 없음

중요 이 노트는 릴리스 14SU2에만 해당됩니다.

릴리스 14SU2의 경우 tomcat-ECDSA 인증서를 재생성하거나 업로드한 후 Cisco DRF 서비스를 다시 시작해야 합니다. tomcat RSA 인증서 작업 후에는 다시 시작할 필요가 없습니다.

OAuth 새로 고침 로그인을 위해 키 다시 생성

명령줄 인터페이스를 사용하여 암호화 키와 서명 키를 다시 생성하려면 이 절차를 사용합니다. Cisco Jabber가 Unified Communications Manager의 OAuth 인증을 위해 사용하는 암호화 키 또는 서명 키가 손상된 경우 이 작업을 완료합니다. 서명 키는 비대칭이고 RSA 기반인 반면 암호화 키는 대칭 키입니다.

이 작업을 완료한 후 이러한 키를 사용하는 현재 액세스 및 새로 고침 토큰은 무효화됩니다.

최종 사용자에게 미치는 영향을 최소화하기 위해 근무 시간 이후에 이 작업을 수행하는 것이 좋습니다.

암호화 키는 아래의 CLI를 통해서만 다시 생성될 수 있지만 서명 키는 퍼블리셔의 Cisco Unified OS 관리 GUI를 사용하여 다시 생성할 수도 있습니다. 보안 > 인증서 관리를 선택하고 **AUTHZ** 인증서를 선택한 다음, 다시 생성을 클릭합니다.

프로시저

단계 **1** Unified Communications Manager 퍼블리셔 노드에서 명령줄 인터페이스에 로그인합니다.

단계 **2** 암호화 키를 다시 생성하려면:

a) `set key regen authz encryption` 명령을 실행합니다.

b) `yes`를 입력합니다.

단계 **3** 서명 키를 다시 생성하려면:

a) `set key regen authz signing` 명령을 실행합니다.

b) `yes`를 입력합니다.
Unified Communications Manager 게시자 노드는 키를 다시 생성하고 새 키를 IM and Presence Service 노드를 포함한 모든 Unified Communications Manager 클러스터 노드에 복제합니다.

모든 UC 클러스터에 새 키를 다시 생성하고 동기화해야 합니다.

- IM and Presence 중앙 클러스터—IM and Presence 중앙 집중식 배포가 있는 경우 IM and Presence 노드는 텔레포니의 개별 클러스터에서 실행됩니다. 이 경우 IM and Presence Service 중앙 클러스터의 Unified Communications Manager 게시자 노드에서 이 절차를 반복합니다.
- Cisco Expressway 또는 Cisco Unity Connection—이러한 클러스터에서도 키를 다시 생성합니다. 자세한 내용은 Cisco Expressway 및 Cisco Unity Connection 설명서를 참조하십시오.

참고 키를 다시 할당한 후 클러스터의 모든 노드에서 Cisco CallManager 서비스를 다시 시작합니다.

인증서 또는 인증서 체인 업로드

시스템이 신뢰하도록 하려는 새 인증서 또는 인증서 체인을 업로드합니다.

프로시저

단계 **1** Cisco Unified OS 관리에서 보안 > 인증서 관리를 선택합니다.
단계 **2** 인증서/인증서 체인 업로드를 클릭합니다.
단계 **3** 인증서 용도 드롭다운 목록에서 인증서 이름을 선택합니다.
단계 **4** 다음 단계 중 하나를 수행하여 업로드할 파일을 선택합니다.

- 파일 업로드 텍스트 상자에서 파일의 경로를 입력합니다.
- 찾아보기를 클릭하고 파일을 탐색한 다음 열기를 클릭합니다.

단계 **5** 서버에 파일을 업로드하려면 파일 업로드를 클릭합니다.

참고 인증서를 업로드 한 후 영향을 받는 서비스를 다시 시작합니다. 서버가 다시 켜지면 CCMAdmin 또는 CCMUser GUI에 액세스하여 새로 추가되어 사용 중인 인증서를 확인할 수 있습니다.

타사 **CA(**인증기관**)** 인증서 관리

이 작업 플로우은 순서대로 각 단계를 참조하여 타사 인증 프로세스의 개요를 제공합니다. 이 시스템은 타사 인증기관이 PKCS # 10 인증서 서명 요청(CSR)으로 발행하는 인증서를 지원합니다.

프로시저

	명령 또는 동작	목적
단계 **1**	인증서 서명 요청 생성, 353 페이지	인증서 애플리케이션 정보, 공개 키, 조직 이름, 일반 이름, 지역 및 국가를 포함하는 암호화된 텍스트 블록인 인증서 서명 요청(CSR)을

	명령 또는 동작	목적
		생성합니다. 인증기관은 이 CSR을 사용하여 시스템에 대한 신뢰할 수 있는 인증서를 생성합니다.
단계 **2**	CSR(Certificate Signing Request) 다운로드, 354 페이지	CSR을 생성 후 다운로드하고 인증기관에 제출할 준비를 합니다.
단계 **3**	인증기관 설명서를 참조하십시오.	인증기관에서 애플리케이션 인증서를 가져옵니다.
단계 **4**	인증기관 설명서를 참조하십시오.	인증기관에서 루트 인증서를 가져옵니다.
단계 **5**	인증기관 서명 CAPF 루트 인증서를 신뢰 저장소에 추가 , 354 페이지	루트 인증서를 신뢰 저장소에 추가합니다. 인증기관에서 서명한 CAPF 인증서를 사용할 때는 이 단계를 수행합니다.
단계 **6**	인증서 또는 인증서 체인 업로드, 352 페이지	노드에 인증기관 루트 인증서를 업로드합니다.
단계 **7**	CAPF 또는 Cisco Unified Communications Manager용 인증서를 업데이트한 경우 새 CTL 파일을 생성합니다.	http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html에서 *Cisco Unified Communications Manager* 보안 설명서를 참조하십시오. 타사에서 서명한 CAPF 또는 CallManager 인증서를 업로드한 후에 CTL 클라이언트(구성된 경우)를 다시 실행합니다.
단계 **8**	서비스 다시 시작, 355 페이지	새 인증서의 영향을 받는 서비스를 다시 시작합니다. 모든 인증서 유형에 대해 해당 서비스를 다시 시작합니다(예를 들어, Tomcat 또는 Tomcat-ECDSA 인증서를 업데이트한 경우 Cisco Tomcat 서비스를 다시 시작).

인증서 서명 요청 생성

인증서 애플리케이션 정보, 공개 키, 조직 이름, 일반 이름, 지역 및 국가를 포함하는 암호화된 텍스트 블록인 인증서 서명 요청(CSR)을 생성합니다. 인증기관은 이 CSR을 사용하여 시스템에 대한 신뢰할 수 있는 인증서를 생성합니다.

참고 새 CSR을 생성하는 경우 기존 CSR을 덮어씁니다.

프로시저

단계 **1** Cisco Unified OS 관리에서 보안 > 인증서 관리를 선택합니다.

단계 **2** **CSR** 생성을 클릭합니다.

단계 **3** 인증서 서명 요청 생성 창에서 필드를 구성합니다. 필드 및 해당 구성 옵션에 대한 자세한 내용은 온라인 도움말을 참조하십시오.

단계 **4** 생성을 클릭합니다.

CSR(Certificate Signing Request) 다운로드

CSR을 생성 후 다운로드하고 인증기관에 제출할 준비를 합니다.

프로시저

단계 **1** Cisco Unified OS 관리에서 보안 > 인증서 관리를 선택합니다.

단계 **2** **CSR** 다운로드를 클릭합니다.

단계 **3** 인증서 용도 드롭다운 목록에서 인증서 이름을 선택합니다.

단계 **4** **CSR** 다운로드를 클릭합니다.

단계 **5** (선택 사항) 프롬프트가 표시되면 저장을 클릭합니다.

인증기관 서명 **CAPF** 루트 인증서를 신뢰 저장소에 추가

인증기관에서 서명한 CAPF 인증서를 사용할 때 신뢰 저장소에Unified Communications Manager 루트 인증서를 추가합니다.

프로시저

단계 **1** Cisco Unified OS 관리에서 보안 > 인증서 관리를 선택합니다.

단계 **2** 인증서/인증서 체인 업로드를 클릭합니다.

단계 **3** 인증서/인증서 체인 업로드 팝업 윈도우의 인증서 용도 드롭다운 목록에서 **CallManager-trust**를 선택하고 인증기관에서 서명한 CAPF 루트 인증서로 이동합니다.

단계 **4** 파일 업로드 필드에 인증서가 나타나면 업로드를 클릭합니다.

서비스 다시 시작

시스템이 클러스터의 특정 노드에서 기능 또는 네트워크 서비스를 다시 시작해야 하는 경우 이 절차를 사용합니다.

프로시저

단계 **1** 다시 시작하는 서비스 유형에 따라 다음 작업 중 하나를 수행합니다.

- 도구 > 제어 센터 - 기능 서비스를 선택합니다.
- 도구제어 센터 > - 네트워크 서비스를 선택합니다.

단계 **2** 서버 드롭다운 목록에서 시스템 노드를 선택하고 이동을 클릭합니다.

단계 **3** 다시 시작할 서비스 옆의 라디오 버튼을 클릭하고 다시 시작을 클릭합니다.

단계 **4** 다시 시작하는 데 약간 시간이 걸린다는 메시지가 표시되면 확인을 클릭합니다.

온라인 인증서 상태 프로토콜을 통한 인증서 해지

Unified Communications Manager는 인증서 해지를 모니터링하기 위한 OCSP를 제공합니다. 시스템은 예약된 간격 동안, 그리고 인증서가 업로드될 때마다 유효성을 확인하기 위해 인증서 상태를 확인합니다.

OCSP(온라인 인증서 상태 프로토콜)는 관리자가 시스템의 인증서 요구 사항을 관리하는 데 도움을 줍니다. OCSP가 구성된 경우 인증서 유효성을 확인하고 만료된 인증서를 실시간으로 해지하는 간단하고 안전하며 자동화된 방법을 제공합니다.

일반 기준 모드를 사용하는 FIPS 배포의 경우, OCSP도 일반 기준 요구 사항을 준수하는 데 도움이 됩니다.

유효성 확인

Unified Communications Manager는 인증서 상태를 확인하고 유효성을 확인합니다.

인증서는 다음과 같이 확인됩니다.

- Unified Communications Manager는 DTM(위임 신뢰 모델)을 사용하고 루트 CA 또는 중간 CA에 OCSP 서명 특성을 확인합니다. 루트 CA 또는 중간 CA는 상태를 확인하기 위해 OCSP 인증서에 서명해야 합니다. 위임 신뢰 모델이 실패하면 Unified Communications Manager가 TRP(신뢰 응답기 모델)로 대체하고 OCSP 서버의 지정 된 OCSP 응답 서명 인증서를 사용하여 인증서를 확인합니다.

참고 인증서의 해지 상태를 확인하려면 OCSP 응답자를 실행하고 있어야 합니다.

- 인증서 해지 창에서 OCSP 옵션을 활성화하여 실시간으로 인증서 해지를 확인하는 가장 안전한 방법을 제공합니다. 인증서 또는 구성된 OCSP URI에서 OCSP URI를 사용하려면 옵션에서 선택합니다. 수동 OCSP 구성에 대한 자세한 내용은 OCSP를 통해 인증서 해지 구성을 참조하십시오.

참고 리프 인증서의 경우 syslog, FileBeat, SIP, ILS, LBM 등과 같은 TLS 클라이언트는 OCSP 응답자에게 OCSP 요청을 보내고 OCSP 응답자로부터 실시간으로 인증서 해지 응답을 받습니다.

유효성 검사가 수행되고 일반 기준 모드가 켜지면 다음 상태 중 하나가 인증서에 반환됩니다.

- 정상 --정상 상태는 상태 질의에 대한 긍정적 응답을 나타냅니다. 최소한 이 긍정 응답은 인증서가 해지되지 않은 것으로 표시되지만 반드시 인증서가 발급되었음을 의미하는 것이 아니라 응답이 생성된 시간이 인증서의 유효 간격 내에 있음을 나타냅니다. 응답 확장은 발급, 유효성 등에 대한 긍정적 진술과 같은 인증서의 상태와 관련하여 응답자에 의한 추가 정보를 전달하는 데 사용될 수 있습니다.
- 해지됨 - 해지됨 상태는 인증서가 해지되었음을 나타냅니다(영구 또는 임시적(보류 중)).
- 알 수 없음-- 알 수 없음 상태는 OCSP 응답기에서 요청 중인 인증서를 알지 못하는 것을 나타냅니다.

참고 일반 기준 모드에서는 연결이 해지됨과 알 수 없음 케이스 모두에서 실패하는 반면, 연결은 일반 기준이 활성화되지 않은 경우 알 수 없음 응답 케이스에서 성공합니다.

인증서 모니터링 작업 흐름

이 작업을 수행하여 인증서 상태 및 만료를 자동으로 모니터링하도록 시스템을 구성하십시오.

- 인증서가 만료에 도달하면 전자 메일을 보냅니다.
- 만료된 인증서를 해지합니다.

프로시저

	명령 또는 동작	목적
단계 **1**	인증서 모니터 알림 구성, 357 페이지	자동 인증서 모니터링을 구성합니다. 시스템은 인증서 상태를 주기적으로 확인하고 인증서의 만료가 다가오면 사용자에게 전자 메일을 보냅니다.
단계 **2**	OCSP를 통해 인증서 해지 구성, 358 페이지	시스템이 만료된 인증서를 자동으로 취소하도록 OCSP를 구성합니다.

인증서 모니터 알림 구성

Unified Communications Manager 또는 IM and Presence Service에 대한 자동화된 인증서 모니터링을 구성합니다. 시스템은 인증서 상태를 주기적으로 확인하고 인증서의 만료가 다가오면 사용자에게 전자 메일을 보냅니다.

참고 **Cisco** 인증서 만료 모니터 네트워크 서비스가 실행 중이어야 합니다. 이 서비스는 기본적으로 활성화되어 있지만 도구 > 제어 센터 - 네트워크 서비스를 선택하고 **Cisco** 인증서 만료 모니터 서비스 상태가 실행 중인지 확인하여 Cisco 통합 서비스 가용성에서 서비스가 실행 중인지 확인할 수 있습니다.

프로시저

단계 **1** Cisco Unified OS 관리(Unified Communications Manager 인증서 모니터링의 경우) 또는 Cisco Unified IM and Presence 관리(IM and Presence Service 인증서 모니터링의 경우)에 로그인합니다.

단계 **2** 보안 > 인증서 모니터를 선택합니다.

단계 **3** 알림 시작 시간 필드에 숫자 값을 입력합니다. 이 값은 시스템이 만료 예정을 통지하기 시작한 인증서 만료 전 일 수를 나타냅니다.

단계 **4** 알림 빈도 필드에 알림 빈도를 입력합니다.

단계 **5** (선택 사항) 시스템이 예정된 인증서 만료에 대한 전자 메일 알림을 보내도록 하려면 전자 메일 알림 활성화 확인란을 선택합니다.

단계 **6** 인증서 상태 검사에 LSC 인증서를 포함시키려면 **LSC** 모니터링 활성화 확인란을 선택합니다.

단계 **7** 전자 메일 **ID** 필드에 시스템에서 알림을 보낼 전자 메일 주소를 입력합니다. 세미콜론으로 구분하여 여러 개의 전자 메일 주소를 입력할 수 있습니다.

단계 **8** 저장을 클릭합니다.

참고 인증서 모니터 서비스는 기본적으로 24시간 마다 실행됩니다. 인증서 모니터 서비스를 다시 시작하면 서비스를 시작한 다음 24시간 후에만 실행되도록 다시 일정을 계산합니다. 간격은 인증서가 만료일 7일 전까지도 변경되지 않습니다. 인증서가 만료되었거나 만료 1일 전이 되면 1시간 마다 실행됩니다.

다음에 수행할 작업

시스템이 만료된 인증서를 자동으로 취소하도록 OCSP(온라인 인증서 상태 프로토콜)를 구성합니다. 자세한 내용은 OCSP를 통해 인증서 해지 구성, 358 페이지을 참조하십시오.

OCSP를 통해 인증서 해지 구성

OCSP(온라인 인증서 상태 프로토콜)를 사용하여 인증서 상태를 정기적으로 확인하고 만료된 인증서를 자동으로 해지할 수 있습니다.

시작하기 전에

시스템에 OCSP 검사에 필요한 인증서가 있는지 확인하십시오. OCSP 응답 특성으로 구성된 루트 또는 중간 CA 인증서를 사용하거나 tomcat-trust에 업로드된 지정된 OCSP 서명 인증서를 사용할 수 있습니다.

프로시저

단계 **1** Cisco Unified OS 관리(Unified Communications Manager 인증서 해지의 경우) 또는 Cisco Unified IM and Presence 관리(IM and Presence Service 인증서 해지의 경우)에 로그인합니다.

단계 **2** 보안 > 인증서 해지를 선택합니다.

단계 **3** **OCSP** 활성화 확인란을 선택하고 다음 작업 중 하나를 수행합니다.

- OCSP 확인을 위해 OCSP 응답자를 지정하려면 구성된 **OCSP URI** 사용 버튼을 선택하고 **OCSP**가 구성된 **URI** 필드에 응답자의 URI를 입력합니다.
- 인증서가 OCSP 응답자 URI로 구성된 경우 인증서에서 **OCSP URI** 사용 버튼을 선택합니다.

단계 **4** 해지 확인 활성화 확인란을 선택합니다.

단계 **5** 해지 확인을 위한 간격 기간과 함께 모두 확인 필드를 완료합니다.

단계 **6** 저장을 클릭합니다.

단계 **7** (선택 사항) CTI, IPsec 또는 LDAP 링크가있는 경우 수명이 긴 연결에 OCSP 해지 지원을 활성화하려면 위의 단계 외에도 다음 단계를 완료해야 합니다.

a) [Cisco Unified CM 관리]에서 시스템 > 엔터프라이즈 파라미터를 선택합니다.
b) 인증서 해지 및 만료 아래에서 인증서 유효성 확인 파라미터를 **True**로 설정합니다.
c) 유효성 확인 빈도 파라미터에 대한 값을구성합니다.

참고 인증서 해지 창의 해지 확인 활성화 파라미터의 간격 값은 유효성 확인 빈도 엔터프라이즈 파라미터의 값보다 우선합니다.

d) 저장을 클릭합니다.

인증서 오류 문제 해결

시작하기 전에

IM and Presence Service 노드의 Unified Communications Manager 서비스 또는 Unified Communications Manager 노드의 IM and Presence Service 기능에 액세스하려 할 때 오류가 발생하는 경우 문제의 원인은 tomcat-trust 인증서입니다. 오류 메시지 서버에 연결할 수 없습니다(원격 노드에 연결할 수 없음) 이 다음 서비스 가용성 인터페이스 창에 나타납니다.

- 서비스 활성화
- 컨트롤 센터 - 기능 서비스
- 컨트롤 센터 - 네트워크 서비스

이 절차를 사용하여 인증서 오류를 해결합니다. 첫 단계부터 시작하고 필요한 경우 계속 진행합니다. 때때로 첫 단계만 완료해도 오류를 해결할 수 있으며 기타의 경우 모든 단계를 완료해야 합니다.

프로시저

단계 **1** Cisco Unified OS 관리에서 보안 > 인증서 관리를 선택하여 필수 tomcat-trust 인증서가 있는지 확인합니다.

필수 인증서가 없는 경우 30분 기다렸다가 다시 확인합니다.

단계 **2** 해당 정보를 보려는 인증서를 선택합니다. 콘텐츠가 원격 노드에 있는 해당 인증서와 일치하는지 확인합니다.

단계 **3** CLI에서 Cisco 인터클러스터 동기화 에이전트 서비스를 다시 시작합니다. **utils service restart Cisco Intercluster Sync Agent**.

단계 **4** Cisco 인터클러스터 동기화 에이전트 서비스가 다시 시작되면 Cisco Tomcat 서비스를 다시 시작합니다. **utils service restart Cisco Tomcat**.

단계 **5** 30분이 소요됩니다. 이전 단계로 인증서 오류가 해결되지 않고 tomcat-trust 인증서가 있는 경우 인증서를 삭제합니다. 인증서를 삭제한 후 각 노드에 대한 Tomcat 및 Tomcat-ECDSA 인증서를 다운로드하고 피어에 tomcat-trust 인증서로 업로드하여 수동으로 교환해야 합니다.

단계 **6** 인증서 교환이 완료된 후 각 영향을 받는 서버에서 Cisco Tomcat을 다시 시작합니다. **utils service restart Cisco Tomcat**.

25 장

벌크 인증서 관리

• 벌크 인증서 관리, 361 페이지

벌크 인증서 관리

클러스터 간에 인증서 집합을 공유하는 경우 벌크 인증서 관리를 사용합니다. 이 단계는 클러스터 간 내선 이동 같이 클러스터 간에 신뢰를 설정해야 하는 시스템 기능에 필요합니다.

프로시저

	명령 또는 동작	목적
단계 **1**	인증서 내보내기, 361 페이지	이 절차에서는 클러스터의 모든 노드에 대한 인증서를 포함하는 PKCS12 파일을 만듭니다.
단계 **2**	인증서 가져오기, 362 페이지	홈 및 원격 (방문) 클러스터로 인증서를 다시 가져옵니다.

인증서 내보내기

이 절차에서는 클러스터의 모든 노드에 대한 인증서를 포함하는 PKCS12 파일을 만듭니다.

프로시저

단계 **1** Cisco Unified OS 관리에서 보안 > 벌크 인증서 관리를 선택합니다.

단계 **2** 홈 및 원격 클러스터에서 연결할 수 있는 TFTP 서버에 대한 설정을 구성합니다. 필드 및 해당 구성 옵션에 대한 내용은 온라인 도움말을 참조하십시오.

단계 **3** 저장을 클릭합니다.

단계 **4** 내보내기를 클릭합니다.

단계 **5** 벌크 인증서 내보내기 창에서 인증서 종류 필드에 대해 모두를 선택합니다.

단계 **6** 내보내기를 클릭합니다.

단계 **7** 닫기를 클릭합니다.

참고 대량 인증서 내보내기가 수행되면 다음과 같이 인증서가 원격 클러스터에 업로드됩니다.

- CAPF 인증서가 CallManager-trust로 업로드됩니다.
- Tomcat 인증서가 Tomcat-trust로 업로드됩니다.
- CallManager 인증서가 CallManager-trust로 업로드됩니다.
- CallManager 인증서가 Phone-SAST-trust로 업로드됩니다.
- ITLRecovery 인증서가 PhoneSast-trust 및 CallManager-trust로 업로드됩니다.

위의 단계는 인증서가 자체 서명되고 다른 클러스터에 일반 트러스트가 없을 때 수행됩니다. 일반 신뢰 또는 동일한 서명자가 있는 경우 모든 인증서를 내보낼 필요는 없습니다.

인증서 가져오기

홈 및 원격 (방문) 클러스터로 인증서를 다시 가져옵니다.

참고 벌크 인증서 관리를 사용하여 인증서를 가져오면 전화기가 재설정됩니다.

시작하기 전에

가져오기 단추가 표시되기 전에 다음과 같은 작업을 완료해야 합니다.

- 둘 이상의 클러스터에서 SFTP 서버로 인증서를 내보냅니다.
- 내보낸 인증서를 통합합니다.

프로시저

단계 **1** Cisco Unified OS 관리에서 다음을 선택합니다보안 > 벌크 인증서 관리 > 가져오기 > 벌크 인증서 가져오기.

단계 **2** 인증서 유형 드롭다운 목록에서 모두를 선택합니다.

단계 **3** 가져오기를 선택합니다.

참고 벌크 인증서 가져오기가 수행되면 다음과 같이 인증서가 원격 클러스터에 업로드됩니다.

- CAPF 인증서가 CallManager-trust로 업로드됩니다.
- Tomcat 인증서가 Tomcat-trust로 업로드됩니다.
- CallManager 인증서가 CallManager-trust로 업로드됩니다.
- CallManager 인증서가 Phone-SAST-trust로 업로드됩니다.
- ITLRecovery 인증서가 PhoneSast-trust 및 CallManager-trust로 업로드됩니다.

참고 다음 유형의 인증서는 다시 시작되는 전화기를 결정합니다.

- Callmanager - 인증서가 속한 노드에서 TFTP 서비스를 활성화한 경우에만 모든 전화기.
- TVS - Callmanager 그룹 구성원 자격을 기반으로 하는 일부 전화기.
- CAPF - CAPF가 활성화된 경우에만 모든 전화기.

26 장

IPSec 정책 관리

- IPsec 정책 개요, 365 페이지
- IPsec 정책 구성, 365 페이지
- IPsec 정책 관리, 366 페이지

IPsec 정책 개요

IPsec은 암호화 보안 서비스를 사용하여 IP 네트워크를 통해 개인 보안 통신을 보장하는 프레임워크입니다. IPsec 정책은 IPsec 보안 서비스를 구성하는 데 사용됩니다. 정책은 네트워크에서 대부분의 트래픽 유형을 위해 다양한 수준의 보호를 제공합니다. 컴퓨터, OU(조직 단위), 도메인, 사이트 또는 글로벌 엔터프라이즈의 보안 요구 사항을 충족하도록 IPsec 정책을 구성할 수 있습니다.

IPsec 정책 구성

참고

- 시스템 업그레이드 중 IPsec 정책에 적용되는 변경 사항은 손실되므로 업그레이드하는 동안 IPsec 정책을 수정 또는 생성하지 마십시오.
- IPsec은 양방향 프로비저닝 또는 각 호스트(또는 게이트웨이)에 대해 하나의 피어가 필요합니다.
- 한 IPsec 정책 프로토콜이 “ANY”로 설정되고 다른 IPsec 정책 프로토콜이 “UDP” 또는 “TCP”로 설정된 두 Unified Communications Manager 노드에서 IPsec 정책을 프로비저닝할 때 “ANY” 프로토콜을 사용하는 노드에서 실행할 경우 유효성 검사 결과는 거짓 부정이 될 수 있습니다.
- 특히 암호화를 사용하면 IPsec은 시스템 성능에 영향을 미칩니다.
- Unified CM 노드를 재부팅한 후 IPsec 연결이 작동하지 않으면 명령 **utils ipsec restart**를 사용하여 IPsec 서비스를 다시 시작하여 IPsec 연결을 성공적으로 설정해야 합니다. 이 해결 방법은 네트워크 연결을 설정하기 전에 IPsec 서비스 다시 시작과 관련된 문제를 완화하는 것입니다.

프로시저

단계 **1** Cisco Unified OS 관리에서 보안 > **IPSec** 구성을 선택합니다.

단계 **2** 새로 추가를 클릭합니다.

단계 **3** **IPSec** 정책 구성 창에서 필드를 구성합니다. 필드 및 해당 구성 옵션에 대한 자세한 내용은 온라인 도움말을 참조하십시오.

단계 **4** 저장을 클릭합니다.

단계 **5** (선택 사항) IPsec를 확인하려면 서비스 > **Ping**을 선택하고 **IPsec** 확인 확인란을 선택한 다음 **Ping**을 클릭합니다.

IPsec 정책 관리

시스템 업그레이드 중 IPsec 정책에 적용되는 변경 사항은 손실되므로 업그레이드하는 동안 IPsec 정책을 수정 또는 생성하지 마십시오.

⚠

주의 인증서 이름, 도메인 또는 IP 주소 변경으로 인해 기존 IPsec 인증서가 변경되면 IPsec 정책을 삭제하고 다시 생성해야 합니다. 인증서 이름이 변경되지 않은 경우 원격 노드의 재생성된 인증서를 가져온 후 IPsec 정책을 비활성화하고 활성화해야 합니다.

프로시저

단계 **1** Cisco Unified OS 관리에서 보안 > **IPSEC** 구성을 선택합니다.

단계 **2** 정책을 표시, 활성화 또는 비활성화하려면 다음 단계를 수행합니다.

a) 정책 이름을 클릭합니다.
b) 정책을 활성화 또는 비활성화하려면 정책 활성화 확인란을 선택하거나 선택 취소합니다.
c) 저장을 클릭합니다.
d) 정책을 비활성화하는 경우에는 **utils ipsec restart** 명령을 실행하여 변경 비활성화를 적용해야 합니다.

단계 **3** 하나 이상의 정책을 삭제하려면 다음 단계를 수행합니다.

a) 삭제할 각 정책 옆의 확인란을 선택합니다.

모든 정책을 선택하려면 모두 선택을 클릭하고, 모든 확인란을 지우려면 모두 지우기를 클릭하면 됩니다.

b) 선택한 항목 삭제를 클릭합니다.

27 장

인증 정책 관리

- 인증 정책 및 인증, 367 페이지
- 인증서 정책 구성, 368 페이지
- 인증 정책 기본값 구성, 369 페이지
- 인증 활동 모니터링, 369 페이지
- 인증서 캐시 구성, 370 페이지
- 세션 종료 관리, 371 페이지

인증 정책 및 인증

인증 기능은 사용자를 인증하고 인증서 정보를 업데이트하고 사용자 이벤트와 오류를 추적하고 기록하며 인증서 변경 내역을 기록하고 데이터 저장소에 대한 사용자 인증서를 암호화 또는 해독합니다.

시스템은 항상 Unified Communications Manager 데이터베이스에 대해 애플리케이션 사용자 암호 및 최종 사용자 PIN을 인증합니다. 시스템은 회사 디렉터리 또는 데이터베이스에 대해 최종 사용자 암호를 인증할 수 있습니다.

시스템이 회사 디렉터리와 동기화되는 경우 Unified Communications Manager 또는 LDAP(Lightweight Directory Access Protocol)의 인증 기능이 암호를 인증할 수 있습니다.

- LDAP 인증이 활성화된 경우 사용자 암호 및 인증 정책이 적용되지 않습니다. 이러한 기본값은 디렉터리 동기화(DirSync 서비스)로 생성된 사용자에게 적용됩니다.
- LDAP 인증이 비활성화되면 시스템이 데이터베이스에 대한 사용자 인증서를 인증합니다. 이 옵션을 사용하여 인증 정책을 할당하고 인증 이벤트를 관리하고 암호를 관리할 수 있습니다. 최종 사용자는 전화기 사용자 인터페이스를 통해 암호 및 PIN을 변경할 수 있습니다.

인증 정책은 운영 체제 사용자 또는 CLI 사용자에게 적용되지 않습니다. 이러한 관리자는 운영 체제에서 지원하는 표준 암호 확인 절차를 사용합니다.

사용자가 데이터베이스에 구성된 후 시스템은 데이터베이스에 사용자 인증서의 기록을 저장하여 사용자가 자신의 인증서를 변경하라는 메시지가 표시될 때 이전 정보를 입력하지 못하도록 합니다.

인증 정책에 대한 JTAPI 및 TAPI 지원

Cisco Unified Communications Manager Java 텔레포니 애플리케이션 프로그래밍 인터페이스(JTAPI) 및 텔레포니 애플리케이션 프로그래밍 인터페이스(TAPI)는 애플리케이션 사용자에게 할당된 인증 정책을 지원하므로 개발자는 인증 정책 시행을 위한 암호 만료, PIN 만료 및 인증 정책 반환 코드에 응답하는 애플리케이션을 만들어야 합니다.

애플리케이션은 애플리케이션이 사용하는 인증 모델에 관계 없이 API를 사용하여 데이터베이스 또는 회사 디렉터리를 인증합니다.

개발자를 위한 TAPI 및 JTAPI에 대한 자세한 내용은 http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-programming-reference-guides-list.html의 개발자 설명서를 참조하십시오.

인증서 정책 구성

인증 정책은 애플리케이션 사용자 및 최종 사용자에 적용됩니다. 최종 사용자 및 애플리케이션 사용자에게 암호 정책을, 최종 사용자에게 PIN 정책을 할당합니다. 인증 정책 기본값 구성에는 이러한 그룹에 대한 정책 할당이 나열되어 있습니다. 새 사용자를 데이터베이스에 추가하면 기본 정책이 할당됩니다. 할당된 정책을 변경하고 사용자 인증 이벤트를 관리할 수 있습니다.

참고 자격 증명 정책 설정에서 허용된 비활성 일 수 매개 변수가 CTI 애플리케이션 사용자에 대해 0(제한 없음)으로 설정되어 있는지 확인합니다. 그렇지 않으면 애플리케이션 사용자가 예기치 않게 비활성화되고 CTI 애플리케이션을 재시작 후 Unified CM에 연결하지 못할 수 있습니다.

프로시저

단계 **1** Cisco Unified CM 관리에서사용자 관리 > 사용자 설정 > 인증서 정책을 선택합니다.

단계 **2** 다음 단계 중 하나를 수행합니다.

- 찾기를 클릭하고 기존 인증서 정책을 선택합니다.
- 새로 추가를 클릭하여 새 인증서 정책을 생성합니다.

단계 **3** 인증서 정책 구성 창에서 필드를 완료합니다. 필드 및 해당 구성 설정에 대한 자세한 내용은 온라인 도움말을 참조하십시오.

단계 **4** 저장을 클릭합니다.

인증 정책 기본값 구성

설치 시 Cisco Unified Communications Manager는 사용자 그룹에 정적 기본 인증 정책을 할당합니다. 기본 인증서를 제공하지는 않습니다. 시스템은 새 기본 정책을 할당하고 사용자에 대한 새 기본 인증서 및 인증서 요구 사항을 구성하는 옵션을 제공합니다.

프로시저

단계 **1** Cisco Unified CM 관리에서사용자 관리 > 사용자 설정 > 인증서 정책 기본값을 선택합니다.

단계 **2** 인증 정책 드롭다운 목록 상자에서 이 그룹에 대한 인증 정책을 선택합니다.

단계 **3** 인증서 변경 및 인증서 확인 구성 창에 암호를 입력합니다.

단계 **4** 사용자가 이 인증서를 변경하는 것을 원하지 않을 경우 사용자가 변경할 수 없음 확인란을 선택합니다.

단계 **5** 최종 사용자가 다음에 로그인할 때 변경해야 하는 임시 인증서로 이 인증서를 사용하려는 경우 다음 로그인할 때 반드시 변경 확인란을 선택합니다.

참고 이 확인란을 선택하면 사용자가 개인 디렉터리 서비스를 사용하여 PIN을 변경할 수 없다는 점에 유의하십시오.

단계 **6** 인증서가 만료되지 않도록 하려면 만료되지 않음 확인란을 선택합니다.

단계 **7** 저장을 클릭합니다.

인증 활동 모니터링

시스템은 마지막 hack 시도 시간 같은 최근 인증 결과를 표시하고 실패한 로그온 시도 횟수를 계산합니다.

시스템은 다음과 같은 인증 정책 이벤트에 대한 로그 파일 항목을 생성합니다.

- 인증 성공
- 인증 실패 (잘못된 암호 또는 알 수 없음)
- 다음 이유로 인증 실패
  - 관리 잠금
  - Hack 잠금(실패한 로그온 잠금)
  - 만료된 소프트 잠금(만료된 인증서)
  - 비활성 잠금(일정 시간 동안 인증서가 사용되지 않음)
  - 사용자를 변경해야 함(사용자에게 설정된 인증서를 변경해야 함)

- LDAP 비활성(LDAP 인증으로 전환 및 LDAP가 비활성)

- 사용자 인증서 업데이트 성공
- 사용자 인증서 업데이트 실패

참고 최종 사용자 암호에 LDAP 인증을 사용할 경우 LDAP는 인증 성공 및 실패만 추적합니다.

모든 이벤트 메시지에는 문자열 "ims-auth" 및 인증을 시도하는 사용자 ID가 포함됩니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 사용자 관리 > 최종 사용자를 선택합니다.
단계 **2** 검색 조건을 입력하고 찾기를 클릭한 다음, 결과 목록에서 사용자를 선택합니다.
단계 **3** 인증서 편집을 클릭하여 사용자의 인증 활동을 확인합니다.

다음에 수행할 작업

Cisco Unified Real-Time Monitoring Tool(Unified RTMT)로 로그 파일을 볼 수 있습니다. 또한 보고서에 캡처된 이벤트를 수집할 수 있습니다. Unified RTMT를 사용하는 방법에 대한 자세한 내용은 http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html의 *Cisco Unified Real-Time Monitoring Tool* 관리 설명서를 참조하십시오.

인증서 캐시 구성

인증서 캐싱을 활성화하여 시스템 효율성을 높입니다. 시스템은 모든 단일 로그인 요청에 대해 데이터베이스 조회를 수행하거나 저장된 프로시저를 호출할 필요가 없습니다. 관련된 인증 정책은 캐싱 기간이 만료될 때까지 적용되지 않습니다.

이 설정은 사용자 인증을 호출하는 모든 Java 애플리케이션에 적용됩니다.

프로시저

단계 **1** [Cisco Unified CM 관리]에서 시스템 > 엔터프라이즈 매개 변수를 선택합니다.
단계 **2** 필요에 따라 다음 작업을 수행합니다.

- 캐싱 활성화 엔터프라이즈 매개 변수를 **True**로 설정합니다. 이 매개 변수를 활성화한 상태에서 Cisco Unified Communications Manager는 최대 2분 동안 캐시된 인증서를 사용합니다.

- 캐싱 활성화 엔터프라이즈 매개 변수를 **False**로 설정하여 캐싱을 비활성화하면 시스템이 캐시된 인증서를 인증에 사용하지 않습니다. 시스템은 LDAP 인증에서 이 설정을 무시합니다. 인증서 캐싱을 사용하려면 사용자당 최소 추가 메모리가 필요합니다.

단계 **3** 저장을 클릭합니다.

세션 종료 관리

관리자는 이 절차를 사용하여 각 노드에 대한 사용자의 활성 로그인 세션을 종료할 수 있습니다.

참고
- 권한 수준이 4인 관리자만 세션을 종료할 수 있습니다.
- 세션 관리는 특정 노드에서 활성 로그인 세션을 종료합니다. 관리자가 서로 다른 노드에서 모든 사용자 세션을 종료하고자 하는 경우 관리자는 각 노드에 로그인하고 세션을 종료해야 합니다.

이 기능은 다음 인터페이스에 적용됩니다.

- Cisco Unified CM 관리
- Cisco 통합 서비스 가용성
- Cisco Unified Reporting
- Cisco Unified Communications 자가 관리 포털
- Cisco Unified CM IM and Presence 관리
- Cisco Unified IM and Presence Service 가용성
- Cisco Unified IM and Presence 보고

프로시저

단계 **1** Cisco 통합 OS 관리 또는 Cisco Unified IM and Presence OS 관리에서 보안 > 세션 관리를 선택합니다. 세션 관리 창이 표시됩니다.

단계 **2** 활성 로그인한 사용자의 사용자 ID를 사용자 **ID** 필드에 입력합니다.

단계 **3** 세션 종료를 클릭합니다.

단계 **4** 확인을 클릭합니다.

종료된 사용자가 로그인된 인터페이스 페이지를 새로 고치면 사용자가 로그아웃됩니다. 감사 로그에 항목이 생성되고 종료된 `userID`가 표시됩니다.

VII 부

IP 주소, 호스트 이름 및 도메인 이름 변경

- 변경 전 작업 및 시스템 상태 검사, 375 페이지
- IP 주소 및 호스트 이름 변경, 385 페이지
- 도메인 이름 및 노드 이름 변경, 393 페이지
- 변경 후 작업 및 확인, 407 페이지
- 주소 변경 문제 해결 , 415 페이지

28 장

변경 전 작업 및 시스템 상태 검사

- 변경 전 작업, 375 페이지
- IP 주소, 호스트 이름 및 기타 네트워크 식별자 변경 사항, 375 페이지
- Procedure workflows, 378 페이지
- Cisco Unified Communications Manager 노드에 대한 변경 전 작업, 379 페이지
- IM and Presence Service 노드에 대한 변경 전 설정 작업, 381 페이지

변경 전 작업

IP 주소, 호스트 이름 및 기타 네트워크 식별자 변경 사항

한 클러스터에서 다른 클러스터로 노드를 이동하거나 중복 IP 주소 문제를 해결하는 등 다양한 이유로 배포에서 노드의 네트워크 수준 IP 주소 및 호스트 이름을 변경할 수 있습니다. IP 주소는 노드와 연결된 네트워크 수준 IP(인터넷 프로토콜)이고, 호스트 이름은 노드의 네트워크 수준 호스트 이름입니다.

참고 Cisco Unified Communications Manager, Cisco Unity Connections 및 Cisco IM and Presence 등과 같은 모든 통합 커뮤니케이션 제품에는 하나의 인터페이스만 있습니다. 따라서 이러한 각 제품에 대해 IP 주소를 하나만 할당할 수 있습니다.

노드 이름 및 도메인 이름과 같은 다른 네트워크 식별자에 대한 변경 사항은 다음 리소스를 참조하십시오.

- Cisco Unified Communications Manager용 시스템 구성 설명서
- *IM and Presence Service*의 구성 및 관리 지침서
- *Cisco Unified Communications Manager* 및 *IM and Presence Service* 설치 설명서

IM and Presence Service의 경우 노드에 대한 노드 이름 및 네트워크 수준 DNS 기본 도메인 이름 변경 지침이 이 문서에도 포함되어 있습니다.

IM and Presence Service 노드 이름 및 기본 도메인 이름 변경 사항

노드 이름은 Cisco Unified CM 관리 GUI를 사용하여 구성되며 다른 모든 IM and Presence Service 노드 및 모든 클라이언트 시스템에서 확인할 수 있어야 합니다. 따라서 권장 노드 이름 값은 노드의 네트워크 FQDN입니다. 그러나, IP 주소와 호스트 이름은 모두 특정 배포의 노드 이름에 대한 값으로도 지원됩니다. 노드 이름 권장 사항 및 지원되는 배포 유형에 대한 자세한 내용은 호스트 이름 구성, 277 페이지의 내용을 참조하십시오.

노드의 네트워크 수준 DNS 기본 도메인 이름은 노드의 FQDN(Fully Qualified Domain Name)의 호스트 이름과 결합됩니다. 예를 들어, 호스트 이름이 "imp-server"이고 도메인이 "example.com"인 노드의 FQDN은 "imp-server.example.com"입니다.

노드의 네트워크 수준 DNS 기본 도메인을 IM and Presence Service 애플리케이션의 엔터프라이즈 수준 도메인과 혼동하지 마십시오.

- 네트워크 수준 DNS 기본 도메인은 노드의 네트워크 식별자로만 사용됩니다.
- 엔터프라이즈 수준의 IM and Presence Service 도메인은 최종 사용자 IM 주소에 사용되는 애플리케이션 수준 도메인입니다.

Cisco Unified CM IM and Presence 관리 GUI 또는 Cisco Unified Communications Manager 관리를 사용하여 엔터프라이즈 전체 도메인을 구성할 수 있습니다. 엔터프라이즈 수준 도메인 및 지원되는 배포 유형에 대한 자세한 내용은 *Cisco Unified Communications Manager*의 *IM and Presence Service* 배포 설명서를 참조하십시오.

호스트 이름 구성

다음 표에는 통합 커뮤니케이션 매니저 서버의 호스트네임을 설정할 수 있는 위치, 호스트네임에 허용되는 문자 수, 호스트네임에 권장되는 첫 번째 문자와 마지막 문자가 열거되어 있습니다. 호스트네임을 정확히 설정하지 않을 경우 운영체제, 데이터베이스, 설치 등을 포함해 통합 커뮤니케이션 매니저의 일부 설정요소가 예상대로 작동하지 않을 수 있다는 점에 유의하십시오.

표 ***81: Cisco Unified Communications Manager***에서 호스트 이름 구성

호스트 이름 위치	허용되는 구성	허용되는 문자 수	호스트 이름에 권장되는 첫 번째 문자	호스트 이름에 권장되는 마지막 문자
호스트 이름/IP 주소 필드 Cisco Unified Communications Manager Administration의 시스템 > 서버	클러스터에서 서버의 호스트 이름을 추가 또는 변경할 수 있습니다.	2-63	영문자	영숫자
호스트 이름 필드 Cisco Unified Communications Manager 설치 마법사	클러스터에서 서버의 호스트 이름을 추가할 수 있습니다.	1-63	영문자	영숫자

호스트 이름 위치	허용되는 구성	허용되는 문자 수	호스트 이름에 권장되는 첫 번째 문자	호스트 이름에 권장되는 마지막 문자
호스트 이름 필드 Cisco Unified Communications 운영 체제의 설정 > **IP** > 이더넷	클러스터에서 서버의 호스트 이름을 변경할 수 있으며 추가할 수는 없습니다.	1-63	영문자	영숫자
set network hostname hostname 명령줄 인터페이스	클러스터에서 서버의 호스트 이름을 변경할 수 있으며 추가할 수는 없습니다.	1-63	영문자	영숫자

팁 호스트 이름은 ARPANET 호스트 이름에 대한 규칙을 따라야 합니다. 호스트 이름의 첫 번째 문자와 마지막 문자 사이에 영숫자와 하이픈을 입력할 수 있습니다.

모든 위치에서 호스트 이름을 구성하기 전에 다음 정보를 검토합니다.

- 디바이스-서버, 애플리케이션-서버 및 서버-서버 통신을 지원하는 서버 구성 창의 호스트 이름/IP 주소 필드를 사용하면 점으로 구분된 형식의 IPv4주소 또는 호스트 이름을 입력할 수 있습니다.

  Unified Communications Manager 게시자 노드를 설치한 후에 게시자의 호스트 이름이 이 필드에 자동으로 표시됩니다. Unified Communications Manager 가입자 노드를 설치하기 전에 Unified Communications Manager 게시자 노드에서 이 필드에 가입자 노드의 IP 주소 또는 호스트 이름을 입력합니다.

  이 필드에 Unified Communications Manager가 DNS 서버에 액세스하여 IP 주소에 대한 호스트 이름을 확인할 수 있는 경우에만 호스트 이름을 구성합니다. 반드시 DNS 서버에서 Cisco Unified Communications Manager 이름과 주소 정보를 구성해야 합니다.

팁 DNS 서버에서 Unified Communications Manager 정보를 구성하는 것 외에도 Cisco Unified Communications Manager를 설치하는 동안 DNS 정보를 입력합니다.

- Unified Communications Manager 게시자 노드를 설치하는 동안 정적 네트워킹을 사용하려는 경우 필수인 호스트 이름과 게시자 노드의 IP 주소를 입력하여 네트워크 정보를 구성합니다.

  통합 커뮤니케이션 매니저 가입자 노드를 설치할 때 통합 커뮤니케이션 매니저 퍼블리셔 노드의 호스트네임과 IP 주소를 입력해야만 통합 커뮤니케이션 매니저가 네트워크 연결 및 퍼블리셔-가입자의 유효성을 확인할 수 있습니다. 뿐만 아니라, 가입자 노드에 대한 호스트 이름 및 IP 주소를 입력해야 합니다. Unified Communications Manager 설치 프로그램에서 가입자 서버의 호스트 이름을 묻는 메시지를 표시하는 경우 호스트 이름/IP 주소 필드에 가입자 서버의 호스트 이름을 구성했으면 Cisco Unified Communications Manager 관리의 서버 구성 창에 표시되는 값을 입력합니다.

Procedure workflows

Cisco Unified Communications Manager 워크플로우

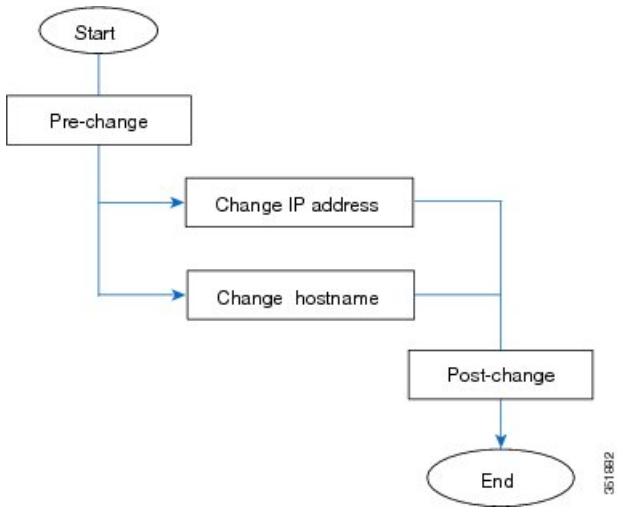
이 문서에서는 Cisco Unified Communications Manager 노드를 위한 다음 작업에 대한 자세한 절차를 제공합니다.

- 노드의 IP 주소 변경
- 노드의 호스트 이름 변경

수행할 단계를 요약하는 각 절차에 대한 작업 목록이 제공됩니다.

참고 변경하기 전에 모든 변경 전 작업 및 시스템 상태 확인을 완료해야 하며 이러한 변경 사항을 적용한 후 변경 후 작업을 완료해야 합니다.

그림 ***24: Cisco Unified Communications Manager*** 워크플로우



IM and Presence Service 워크플로우

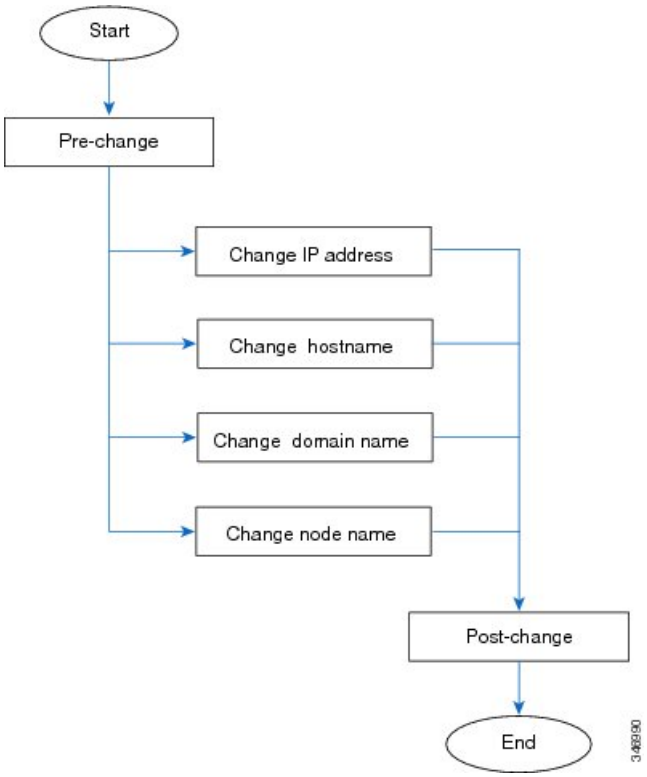
이 문서에서는 IM and Presence Service 노드를 위한 다음 작업에 대한 자세한 절차를 제공합니다 .

- 노드의 IP 주소 변경
- 노드의 호스트 이름 변경
- DNS 기본 도메인 이름 변경
- 노드의 노드 이름 변경

수행할 단계를 요약하는 각 절차에 대한 작업 목록이 제공됩니다.

참고 변경하기 전에 모든 변경 전 작업 및 시스템 상태 확인을 완료해야 하며 이러한 변경 사항을 적용한 후 변경 후 작업을 완료해야 합니다.

그림 ***25: IM and Presence Service*** 워크플로우



Cisco Unified Communications Manager 노드에 대한 변경 전 작업

다음 절차에서는 Cisco Unified Communications Manager 노드의 IP 주소 및 호스트 이름을 변경하는 작업에 대해 설명합니다. 예약된 유지 관리 기간 동안 이러한 절차를 수행해야 합니다.

주의 이러한 작업을 수행할 때 예상되는 결과를 받지 못하면 문제를 해결할 때까지 계속하지 마십시오.

프로시저

단계 **1** Cisco Unified Communications Manager 서버의 모든 곳에 DNS가 구성되어 있는 경우 정방향 및 역방향 레코드(예: A 레코드 및 PTR 레코드)가 구성되어 있고 DNS에 연결할 수 있으며 작동하는지 확인하십시오.

단계 **2** 모든 활성 ServerDown 알림을 확인하여 클러스터의 모든 서버가 작동하고 사용 가능한지 확인합니다. 첫 번째 노드에서 Cisco Unified Real-Time Monitoring Tool(RTMT) 또는 CLI(command-line interface)를 사용합니다.

a) Unified RTMT를 사용하여 확인하려면 알림 센트럴에 액세스하고 ServerDown 알림을 확인합니다.

b) 첫 번째 노드에서 CLI를 사용하여 확인하려면 다음 CLI 명령을 입력하고 애플리케이션 이벤트 로그를 검사합니다.

```
file search activelog syslog/CiscoSyslog ServerDown
```

예를 들어 출력은 예제 데이터베이스 복제 출력과 관련된 항목을 참조하십시오. 자세한 절차 및 문제 해결은 데이터베이스 복제 확인 및 문제 해결 데이터베이스 복제와 관련된 항목을 참조하십시오.

단계 **3** 클러스터의 모든 Cisco Unified Communications Manager 노드에서 데이터베이스 복제 상태를 확인하여 모든 서버가 데이터베이스 변경을 성공적으로 복제하고 있는지 확인합니다. IM and Presence Service의 경우 배포에 노드가 두 개 이상 있는 경우 CLI를 사용하여 데이터베이스 게시자 노드의 데이터베이스 복제 상태를 확인합니다. 통합 RTMT 또는 CLI를 사용합니다. 모든 노드에 2의 상태가 표시되어야 합니다.

1. RTMT를 사용하여 확인하려면 데이터베이스 요약에 액세스하고 복제 상태를 검사합니다.
2. CLI를 사용하여 확인하려면 **utils dbreplication runtimestate**를 입력합니다.

단계 **4** 다음 예제와 같이 CLI 명령 utils diagnose를 입력하여 네트워크 연결 및 DNS 서버 구성을 확인합니다.

예:

```
admin: utils diagnose module validate_network
Log file: /var/log/active/platform/log/diag1.log
Starting diagnostic test(s)
===========================
test - validate_network : Passed
Diagnostics Completed
admin:
```

단계 **5** Cisco 통합 보고에서 Unified CM 데이터베이스 상태 보고서를 생성합니다. 이 보고서에서 오류 또는 경고를 확인합니다.

단계 **6** Cisco 통합 보고에서 통합 CM 클러스터 개요 보고서를 생성합니다. 이 보고서에서 오류 또는 경고를 확인합니다.

단계 **7** 첫 번째 노드의 Cisco Unified Communications Manager 관리에서 시스템 > 서버를 선택하고 찾기를 클릭합니다. 클러스터의 모든 서버 목록이 표시됩니다. 나중에 참조하기 위해 이 서버 목록을 유지합니다. 클러스터의 각 노드에 대한 호스트 이름 및 IP 주소 재고 목록을 모두 저장해야 합니다.

단계 **8** 수동 재해 복구 시스템 백업을 실행하여 모든 노드와 활성 서비스가 모두 성공적으로 백업되었는지 확인합니다. 자세한 내용은 *Cisco Unified Communications Manager*용 관리 지침서를 참조하십시오.

단계 **9** 호스트 이름을 변경하는 경우 SAML 싱글 사인-온(SSO)을 비활성화합니다. SAML SSO에 대한 자세한 내용은 *Cisco Unified Communications Manager*의 *IM and Presence Service*용 구축 설명서를 참조하십시오.

단계 **10** 보안을 사용하는 클러스터(클러스터 보안 모드 1 - 혼합)의 경우 CTL (인증서 신뢰 목록) 파일을 업데이트합니다. 새 TFTP 서버를 기존 CTL 파일에 추가하는 것을 포함하여 CTL 파일 업데이트 및 관리에 대한 자세한 지침은 *Cisco Unified Communications Manager* 보안 설명서를 참조하십시오.

참고 불필요한 지연을 방지하려면 TFTP 서버의 IP 주소를 변경하기 전에 먼저 TFTP 서버의 새 IP 주소를 사용하여 CTL 파일을 업데이트해야 합니다. 이 단계를 수행하지 않는 경우에는 모든 보안 IP 전화기를 수동으로 업데이트해야 합니다.

참고 보안을 지원하는 모든 IP 전화기는 항상 전화기에서 통신할 수 있는 TFTP 서버의 IP 주소를 포함하는 CTL 파일을 다운로드합니다. 하나 이상의 TFTP 서버에 대한 IP 주소를 변경하는 경우 먼저 새 IP 주소를 CTL 파일에 추가하여 전화기가 TFTP 서버와 통신할 수 있도록 해야 합니다.

IM and Presence Service 노드에 대한 변경 전 설정 작업

시스템이 성공적인 IP 주소, 호스트 이름, 도메인 또는 노드 이름 변경에 대비하도록 적절한 변경 전 설정 작업을 수행합니다. 예약된 유지 관리 기간 동안 이러한 작업을 수행해야 합니다.

주의 이러한 작업을 수행할 때 예상되는 결과를 받지 못하면 문제를 해결할 때까지 계속하지 마십시오.

참고 도메인 이름이나 노드 이름을 변경하지 않는 한 Cisco AXL 웹 서비스와 IM and Presence Cisco 싱크 관리자 서비스가 시작되었는지 확인하기 위한 단계를 수행할 필요가 없습니다. 수행할 작업의 전체 목록은 변경 전 작업 목록을 참조하십시오.

프로시저

단계 **1** 클러스터의 모든 노드에서 데이터베이스 복제 상태를 확인하여 모든 서버가 데이터베이스 변경을 성공적으로 복제하고 있는지 확인합니다.

IM and Presence Service의 경우 배포에 노드가 두 개 이상 있는 경우 CLI를 사용하여 데이터베이스 게시자 노드의 데이터베이스 복제 상태를 확인합니다.

통합 RTMT 또는 CLI를 사용합니다. 모든 노드에 **2**의 상태가 표시되어야 합니다.

a) RTMT를 사용하여 확인하려면 데이터베이스 요약에 액세스하고 복제 상태를 검사합니다.
b) CLI를 사용하여 확인하려면 **utils dbreplication runtimestate**를 입력합니다.

예를 들어 출력은 예제 데이터베이스 복제 출력과 관련된 항목을 참조하십시오. 자세한 절차 및 문제 해결은 데이터베이스 복제 확인 및 문제 해결 데이터베이스 복제와 관련된 항목을 참조하십시오.

단계 **2** 다음 예제와 같이 CLI 명령 **utils diagnose**를 입력하여 네트워크 연결 및 DNS 서버 구성을 확인합니다.

예제:

```
admin: utils diagnose module validate_network Log file:
/var/log/active/platform/log/diag1.log Starting diagnostic test(s)
============================ test - validate_network : Passed Diagnostics Completed
 admin:
```

단계 **3** 수동 재해 복구 시스템 백업을 실행하여 모든 노드와 활성 서비스가 모두 성공적으로 백업되었는지 확인합니다.

자세한 내용은 *Cisco Unified Communications Manager*용 관리 지침서를 참조하십시오.

단계 **4** 모든 프레즌스 이중화 그룹에서 고가용성(HA)을 비활성화합니다. 프레즌스 이중화 그룹 구성에 대한 자세한 내용은 *Cisco Unified Communications Manager*용 시스템 구성 가이드의 "프레즌스 이중화 그룹 구성" 장을 참조하십시오.

참고
- HA를 비활성화하기 전에 각 노드 및 하위 클러스터의 사용자 수를 기록합니다. Cisco Unified CM IM and Presence 관리의 (시스템 > 프레즌스 토폴로지) 창에서 이 정보를 찾을 수 있습니다.
- HA를 비활성화한 후 추가 변경 내용을 완료하기 전에 설정이 클러스터 간에 동기화될 때까지 최소 2분 이상 기다립니다.

단계 **5** 호스트 이름을 변경하는 경우 SAML 싱글 사인-온(SSO)을 비활성화합니다. SAML SSO에 대한 자세한 내용은 *Cisco Unified Communications Manager*의 *IM and Presence Service*용 구축 설명서를 참조하십시오.

단계 **6** 배포에 인터클러스터 피어가 구성된 경우 다음 작업을 수행합니다.

a) 변경 중인 IM and Presence 데이타베이스 퍼블리셔 노드가 인터클러스터 피어인 각 클러스터에 대해 인터클러스터 피어 목록에서 게시자의 클러스터를 제거합니다.

예제:

ClusterA, ClusterB 및 ClusterC는 모두 인터클러스터 피어입니다. ClusterA의 퍼블리셔 노드에서 호스트 이름을 변경하려고 합니다. 먼저 ClusterB와 ClusterC의 인터클러스터 피어 목록에서 ClusterA 퍼블리셔 노드를 제거해야 합니다.

b) 각 클러스터의 첫 번째 프레즌스 이중화 그룹의 퍼블리셔 및 가입자 노드에서 Cisco InterCluster 동기화 에이전트를 다시 시작합니다.

단계 **7** 현재 활성화된 모든 서비스 목록을 컴파일합니다. 향후 참조를 위해 이러한 목록을 유지합니다.

a) Cisco 통합 서비스 가용성을 사용하여 활성화된 네트워크 서비스 목록을 보려면 도구 > 제어 센터 - 네트워크 서비스를 선택합니다.
b) Cisco 통합 서비스 가용성을 사용하여 활성화된 기능 서비스 목록을 보려면 도구 > 제어 센터 - 기능 서비스를 선택합니다.

단계 **8** Cisco 통합 서비스 가용성을 사용하여 모든 기능 서비스를 중지하려면 도구 > 제어 센터 - 기능 서비스를 선택합니다. 기능 서비스를 중지하는 순서는 중요하지 않습니다.

팁 IP 주소, 호스트 이름 또는 IP 주소와 호스트 이름을 모두 변경하는 경우 이 단계를 완료할 필요가 없습니다. 이러한 이름 변경의 경우 기능 서비스가 자동으로 중지됩니다.

단계 **9** 도구 > 제어 센터 - 네트워크 서비스를 선택할 때 Cisco 통합 서비스 가용성 기능을 사용하여 IM and Presence Service 서비스 그룹에 나열된 다음 네트워크 서비스를 중지합니다.

다음 순서로 이러한 IM and Presence Service 네트워크 서비스를 중지해야 합니다.

1. Cisco 구성 에이전트
2. Cisco 클러스터 간 동기화 에이전트
3. Cisco 클라이언트 프로파일 에이전트
4. Cisco OAM 에이전트
5. Cisco XCP 구성 관리자
6. Cisco XCP 라우터
7. Cisco Presence 데이터 저장소
8. Cisco SIP 등록 데이터 저장소
9. Cisco 로그인 데이터 저장소
10. Cisco 라우트 데이터 저장소
11. Cisco 서버 복구 관리자
12. Cisco IM and Presence 데이터 모니터

단계 **10** Cisco 통합 서비스 가용성, 도구 > 제어 센터 - 기능 서비스를 사용하여 Cisco AXL 웹 서비스가 Cisco Unified Communications Manager 퍼블리셔 노드에서 시작되었는지 확인합니다.

참고 도메인 이름 또는 노드 이름을 변경하는 경우에만 이 단계를 수행합니다.

단계 **11** IM and Presence Cisco 싱크 관리자 서비스가 시작되었고 동기화를 완료했는지 확인합니다.

참고 도메인 이름 또는 노드 이름을 변경하는 경우에만 이 단계를 수행합니다.

a) Cisco 통합 서비스 가용성을 사용하여 확인하려면 다음 단계를 수행합니다.
   1. 도구 > 제어 센터 - 네트워크 서비스를 선택합니다.
   2. IM and Presence 데이터베이스 퍼블리셔 노드를 선택합니다.
   3. **IM and Presence Service** 서비스를 선택합니다.
   4. Cisco 싱크 관리자 서비스가 시작되었는지 확인합니다.
   5. Cisco Unified CM IM and Presence 관리 GUI에서 진단 > 시스템 대시보드 > 동기화 상태를 선택합니다.

6. 동기화가 완료되고 동기화 상태 영역에 오류가 표시되지 않는지 확인합니다.

b) IM and Presence 데이타베이스 퍼블리셔 노드에서 Cisco Unified CM IM and Presence 관리 GUI를 사용하여 확인하려면 진단 > 시스템 대시보드를 선택합니다.

29 장

IP 주소 및 호스트 이름 변경

- IP 주소 및 호스트 이름 작업 목록 변경, 385 페이지
- OS 관리 GUI를 통해 IP 주소 또는 호스트 이름 변경, 386 페이지
- Unified CM Administration GUI를 통해 IP 주소 또는 호스트 이름 변경, 387 페이지
- CLI를 통해 IP 주소 또는 호스트 이름 변경, 388 페이지
- IP 주소만 변경, 390 페이지
- CLI를 사용하여 DNS IP 주소 변경, 391 페이지

IP 주소 및 호스트 이름 작업 목록 변경

다음 표에서는 Cisco Unified Communications Manager 및 IM and Presence Service 노드의 IP 주소 및 호스트 이름을 변경하기 위해 수행하는 작업에 대해 설명합니다.

표 ***82: IP*** 주소 및 호스트 이름 작업 목록 변경

항목	작업
1	변경 전 작업 및 시스템 상태 확인을 수행합니다.
2	CLI(command-line interface) 또는 통합 운영 체제 GUI를 사용하여 노드의 IP 주소 또는 호스트 이름을 변경 니다. IM and Presence Service 노드의 경우 다음 조건을 준수하십시오. • 가입자 노드를 변경하기 전에 먼저 데이터베이스 퍼블리셔 노드의 IP 주소 및 호스트 이름을 변경합니다. • 모든 가입자 노드에 대한 IP 주소 및 호스트 이름을 동시에 또는 한 번에 변경할 수 있습니다. 참고 IM and Presence Service 노드의 IP 주소 또는 호스트 이름을 변경한 후에 Cisco Unified Communications Manager에서 SIP 게시 트렁크에 대한 대상 주소 값을 변경해야 합니다. 변경 후 작업 목록을 참조하십시오.
3	변경 후 작업을 수행합니다.

OS 관리 GUI를 통해 IP 주소 또는 호스트 이름 변경

Cisco Unified 운영 체제 관리를 사용하여 배포의 호스트 이름으로 정의되는 퍼블리셔 및 가입자 노드의 IP 주소 또는 호스트 이름을 변경할 수 있습니다. 별도로 언급된 경우가 아니면 이 절차의 각 단계는 Unified Communications Manager 및 IM and Presence 서비스 클러스터의 게시자 및 가입자 노드에 모두 적용됩니다.

set network hostname 명령을 통해 호스트 이름을 변경하면 자동으로 자체 서명 인증서가 생성됩니다. 이렇게 하면 클러스터의 모든 장치가 업데이트된 ITL 파일을 다운로드할 수 있도록 재설정됩니다. 클러스터에서 CA 서명 인증서를 사용하고 있는 경우에는 해당 인증서를 다시 서명해야 합니다.

set network hostname 명령을 사용하여 IP 주소만 변경하면 클러스터의 모든 장치가 재설정되어 업데이트된 ITL 파일을 다운로드할 수 있습니다. 인증서가 업데이트되지 않습니다.

참고 호스트 이름을 변경해도 ITL 복구 인증서 재생성이 트리거되지 않습니다.

주의
- Cisco Unified 운영 체제 관리를 통해 한 번에 이러한 설정 중 하나만 변경하는 것이 좋습니다. IP 주소와 호스트 이름을 동시에 변경하려면 CLI 명령 **set network hostname**을 사용합니다.
- Unified Communications Manager 클러스터 보안이 혼합 모드로 작동 중인 경우 CTL 클라이언트를 실행하고 CTL 파일을 업데이트하거나 tokenless CTL 기능을 사용한 경우 **utils CTL update CTLFile**을 실행할 때까지 호스트 이름 또는 IP 주소를 변경한 후 이 노드에 대한 보안 연결이 실패합니다

시작하기 전에

배포에 대한 사전 변경 작업 및 시스템 상태 확인을 수행합니다.

참고 Vcenter에서 vNIC를 변경해야 하는 경우에는 CLI 명령 **set network hostname**을 사용합니다 .

프로시저

단계 **1** Cisco Unified 운영 체제 관리에서 설정 > **IP** > 이더넷 을 선택합니다

단계 **2** 호스트 이름, IP 주소 및 필요한 경우 기본 게이트웨이를 변경합니다.

단계 **3** 저장을 클릭합니다.

노드 서비스는 새 변경 사항을 사용하여 자동으로 다시 시작합니다. 서비스를 다시 시작하면 변경 사항을 적용하기 위해 적절한 업데이트 및 서비스 재시작 시퀀스가 보장됩니다.

호스트 이름을 변경하면 자동으로 자체 서명된 인증서가 재생성되고 클러스터의 모든 장치가 업데이트된 ITL 파일을 다운로드할 수 있도록 재설정됩니다. 호스트 이름을 변경해도 ITL 복구 인증서 재생성이 트리거되지 않습니다.

다음에 수행할 작업

적용 가능한 모든 변경 후 작업을 수행하여 배포에 변경 사항이 적절히 구현되었는지 확인합니다.

참고 새 호스트 이름이 올바른 IP 주소로 확인되지 않는 경우에는 진행하지 마십시오.

클러스터에서 CA 서명 인증서를 사용하고 있는 경우에는 해당 인증서를 다시 서명해야 합니다.

해당 프로세스를 사용하여 클러스터를 혼합 모드로 전환하는 경우 CTL 클라이언트를 실행하여 CTL 파일을 업데이트합니다. tokenless CTL 기능을 사용한 경우에는 CLI 명령 **utils ctl update CTLFile**을 실행합니다.

Unified CM Administration GUI를 통해 IP 주소 또는 호스트 이름 변경

Cisco Unified CM 관리를 사용하여 게시자 및 가입자 노드의 IP 주소 또는 호스트 이름을 변경할 수 있습니다. 이렇게 하면 호스트 이름 항목이 시스템 정의 호스트 이름 또는 IP 값과 동일해집니다.

IP 주소 또는 호스트 이름을 변경하면 자동으로 자체 서명된 인증서가 생성됩니다. 이렇게 하면 클러스터의 모든 장치가 업데이트된 ITL 파일을 다운로드할 수 있도록 재설정됩니다. 클러스터에서 CA 서명 인증서를 사용하는 경우에는 해당 인증서를 다시 서명해야 합니다.

주의

- 호스트 이름 또는 IP 주소를 변경하려면 시스템 서비스를 다시 시작해야 합니다. 따라서 정상적인 작동 시간 중에는 변경하지 마십시오.
- Cisco Unified CM 관리를 통해 한 번에 이러한 설정 중 하나만 변경하는 것이 좋습니다. IP 주소와 호스트 이름을 동시에 변경하려면 CLI 명령 **set network hostname**을 사용합니다.
- Unified Communications Manager 클러스터 보안이 혼합 모드로 작동 중인 경우 CTL 클라이언트를 실행하고 CTL 파일을 업데이트하거나 tokenless CTL 기능을 사용한 경우 **utils CTL update CTLFile**을 실행할 때까지 호스트 이름 또는 IP 주소를 변경한 후 이 노드에 대한 보안 연결이 실패합니다
- Cisco Unified OS 관리 및 Cisco Unified CM 관리 페이지에 정의된 호스트 이름 또는 IP 주소가 일치하지 않는 경우 애플리케이션에서 올바른 전화기 상태를 가져올 수 없습니다. 또한 인증서 불일치로 인해 TLS 핸드셰이크가 실패합니다. 따라서 Cisco Unified OS 관리와 Cisco Unified CM 관리 페이지 모두에서 IP 주소 및 호스트 이름 항목이 동일해야 합니다.

시작하기 전에

배포에 대한 사전 변경 작업 및 시스템 상태 확인을 수행합니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 시스템 > 서버를 선택합니다.

서버 찾기 및 나열 창이 나타납니다.

단계 **2** 모든 서버 목록을 가져오려면 찾기를 클릭합니다.

단계 **3** 목록에서 호스트 이름을 수정할 서버를 클릭합니다.

단계 **4** 호스트 이름/**IP** 주소***** 필드에 새 호스트 이름 또는 IP 주소를 입력하고 저장을 클릭합니다.

단계 **5** 관리 CLI GUI를 사용하여 **utils system restart** CLI 명령을 사용하여 노드를 재부팅합니다.

CLI를 통해 IP 주소 또는 호스트 이름 변경

CLI 를 사용하여 배포의 호스트 이름으로 정의되는 게시자 및 가입자 노드의 IP 주소 또는 호스트 이름을 변경할 수 있습니다. 별도로 언급된 경우가 아니면 이 절차의 각 단계는 Cisco Unified Communication Manager 및 IM and Presence Service 클러스터의 게시자 및 가입자 노드에 모두 적용됩니다.

호스트 이름을 변경하면 자동으로 자체 서명된 인증서가 생성됩니다. 이렇게 하면 클러스터의 모든 장치가 업데이트된 ITL 파일을 다운로드할 수 있도록 재설정됩니다. 클러스터에서 CA 서명 인증서를 사용하는 경우에는 해당 인증서를 다시 서명해야 합니다. 호스트 이름을 변경해도 ITL 복구 인증서 재생성이 트리거되지 않습니다.

⚠

주의 Cisco Unified Communications Manager 클러스터 보안이 혼합 모드로 작동 중인 경우 CTL 클라이언트를 실행하고 CTL 파일을 업데이트하거나 tokenless CTL 기능을 사용한 경우 **utils CTL update CTLFile**을 실행할 때까지 호스트 이름 또는 IP 주소를 변경한 후 이 노드에 대한 보안 연결이 실패합니다

시작하기 전에

배포에 대한 사전 변경 작업 및 시스템 상태 확인을 수행합니다.

프로시저

단계 **1** 변경하려는 노드의 CLI에 로그인합니다.

단계 **2** **`set network hostname`**을 입력합니다.

단계 **3** 표시되는 메시지에 따라 호스트 이름, IP 주소 또는 기본 게이트웨이를 변경합니다.

a) 새 호스트 이름을 입력하고 **Enter** 키를 누릅니다.
b) IP 주소를 변경하려면 예를 입력하고, 그렇지 않으면 4단계로 이동합니다.
c) 새 IP 주소를 입력합니다.
d) 서브넷 마스크를 입력합니다.
e) 게이트웨이의 주소를 입력합니다.

단계 **4** 모든 입력이 올바른지 확인하고 예를 입력하여 프로세스를 시작합니다.

다음에 수행할 작업

적용 가능한 모든 변경 후 작업을 수행하여 배포에 변경 사항이 적절히 구현되었는지 확인합니다.

참고 새 호스트 이름이 올바른 IP 주소로 확인되지 않는 경우에는 진행하지 마십시오.

클러스터에서 CA 서명 인증서를 사용하는 경우에는 해당 인증서를 다시 서명해야 합니다.

해당 프로세스를 사용하여 클러스터를 혼합 모드로 전환하는 경우 CTL 클라이언트를 실행하여 CTL 파일을 업데이트합니다. tokenless CTL 기능을 사용한 경우에는 CLI 명령 **utils ctl update CTLFile**을 실행합니다.

설정된 네트워크 호스트 이름에 대한 **CLI** 출력 예

참고 vNIC를 vcenter에서 변경해야 하는 경우 다음 출력에 표시된 대로 5개 구성 요소 알림 스크립트: regenerate_all_certs.sh 중 4개를 호출한 후 vNIC를 업데이트합니다.

```
 admin:set network hostname ctrl-c: 입력을 종료합니다. *** 경고 *** 우선 명령을 취소한
 것이 아니면 이 창을 닫지 마십시오. 이 명령은 자동으로 시스템 서비스를 재시작합니다. 명령은
정상적인 작동 시간 중에 발행해서는 안 됩니다.
============================================================ 참고: 새 호스트 이름이 클러
스터 전체에 걸쳐 고유한 이름인지 확인하십시오. DNS 서비스를 활용하는 경우, 계속 진행하기 전에
 DNS 구성이 모두 완료되었어야 합니다.
============================================================ 보안 경고 : 이 작동은 타사에
서 서명하여 업로드된 인증서 모두를 포함하여 모든 CUCM 인증서를 재생성하게 됩니다. 호스트 이
름:: newHostname를 입력하십시오. 지금 네트워크 IP 주소를 변경하시겠습니까? [예]:: 경고: 명
령이 완료될 때까지 이 창을 닫지 마십시오. ctrl-c: 입력을 종료합니다. *** 경고 ***
============================================================ 참고: 새 IP 주소가 클러스터
 전체에 걸쳐 고유한지 확인하십시오.
============================================================ Enter the ip address::
10.10.10.28 Enter the ip subnet mask:: 255.255.255.0 Enter the ip address of the
 gateway:: 10.10.10.1 Hostname: newHostname IP Address: 10.10.10.28 IP Subnet
Mask: 255.255.255.0 Gateway: 10.10.10.1 Do you want to continue [yes/no]? yes
calling 1 of 5 component notification script: ahostname_callback.sh Info(0):
Processnode query returned = name ========== bldr-vcm18 updating server table
from:'oldHostname', to: 'newHostname' Rows: 1 updating database, please wait 90
```

```
seconds updating database, please wait 60 seconds updating database, please wait
 30 seconds Going to trigger /usr/local/cm/bin/dbl updatefiles
--remote=newHostname,oldHostname calling 2 of 5 component notification script:
clm_notify_hostname.sh notification Verifying update across cluster nodes...
platformConfig.xml is up-to-date: bldr-vcm21 cluster update successfull calling
3 of 5 component notification script: drf_notify_hostname_change.py calling 4 of
 5 component notification script: regenerate_all_certs.sh calling 5 of 5 component
 notification script: update_idsenv.sh calling 1 of 2 component notification
script: ahostname_callback.sh Info(0): Processnode query returned = name ====
Going to trigger /usr/local/cm/bin/dbl updatefiles
--remote=10.10.10.28,10.67.142.24 calling 2 of 2 component notification script:
clm_notify_hostname.sh Verifying update across cluster nodes... 인터페이스 eth0을
종료하는 중
```

IP 주소만 변경

CLI를 사용하여 노드의 IP 주소를 변경할 수 있습니다.

노드가 호스트 이름 또는 FQDN에 의해 정의된 경우 변경하기 전에 DNS만 업데이트해야 합니다(DNS를 사용하는 경우).

참고 IM and Presence Service의 경우:

- 먼저 IM and Presence 데이타베이스 퍼블리셔 노드를 변경하고 확인합니다.
- IM And Presence Service 가입자 노드를 동시에 또는 한 번에 변경할 수 있습니다.

시작하기 전에

배포에 대한 사전 변경 작업 및 시스템 상태 확인을 수행합니다.

프로시저

단계 **1** 변경하려는 노드의 CLI에 로그인합니다.

단계 **2** **set network ip eth0** ***new-ip_address new_netmask new_gateway***를 입력하여 노드의 IP 주소를 변경합니다.

참고 **set network ip eth0**명령으로 IP 주소를 변경해도 인증서 재생성이 트리거되지 않습니다.

여기서 *new_ip_address*는 새 IP 주소를 지정하고, *new_netmask*는 새 서버 네트워크 마스크를 지정하며, *new_gateway*는 게이트웨이 주소를 지정합니다.

다음 출력이 표시됩니다.

```
admin:set network ip eth0 10.53.57.101 255.255.255.224 10.53.56.1 경고: 이 설정을
변경하면 이 서버의 소프트웨어 라이센스가 무효가 됩니다 라이센스를 다시 호스트해야 합니다. 계속
할까요(y/n)?
```

단계 3 CLI 명령의 출력을 확인합니다. `yes`를 입력한 다음 **Enter** 키를 눌러 프로세스를 시작합니다.

다음에 수행할 작업

적용 가능한 모든 변경 후 작업을 수행하여 배포에 변경 사항이 적절히 구현되었는지 확인합니다.

네트워크 IP 주소 설정에 대한 출력 예

참고 vNIC를 vcenter에서 변경해야 하는 경우 다음 출력에 표시된 대로 `6개 구성 요소 알림 스크립트: aetc_hosts_verify.sh 중 3개를 호출`한 후 vNIC를 업데이트합니다.

```
admin:set network ip eth0 10.77.30.34 255.255.255.0 10.77.30.1 *** W A R N I N G
 *** This command will restart system services
======================================================= Note: Please verify that
 the new ip address is unique across the cluster and, if DNS services are utilized,
 any DNS configuration is completed before proceeding.
======================================================= Continue (y/n)?y calling
 1 of 6 component notification script: acluster_healthcheck.sh calling 2 of 6
component notification script: adns_verify.sh No Primary DNS server defined No
Secondary DNS server defined calling 3 of 6 component notification script:
aetc_hosts_verify.sh calling 4 of 6 component notification script: afupdateip.sh
 calling 5 of 6 component notification script: ahostname_callback.sh Info(0):
Processnode query returned using 10.77.30.33: name ==== calling 6 of 6 component
 notification script: clm_notify_hostname.sh
```

CLI를 사용하여 DNS IP 주소 변경

CLI를 사용하여 배포의 퍼블리셔 및 가입자 노드에 대한 DNS IP 주소를 변경할 수 있습니다. 이 절차는 Cisco Unified Communication Manager 및 IM and Presence Service 클러스터의 퍼블리셔 및 가입자 노드에 모두 적용됩니다.

시작하기 전에

배포에 대한 사전 변경 작업 및 시스템 상태 확인을 수행합니다.

프로시저

단계 1 변경하려는 노드의 CLI에 로그인합니다.

단계 2 `set network dns primary/secondary <new IP address of the DNS>`를 입력합니다.

참고 DNS 서버에 대한 IP 주소를 변경하는 경우 **utils system restart** CLI 명령을 통해 서버를 재부팅해야 합니다.

다음 출력이 표시됩니다.

```
admin:set network dns primary/secondary <new IP address of DNS> *** 경고 *** 이로
 인해 시스템의 네트워크 연결이 일시적으로 끊어집니다.
```

단계 **3** CLI 명령의 출력을 확인합니다. **Yes**를 입력한 다음 **Enter** 키를 눌러 프로세스를 시작합니다.

30 장

도메인 이름 및 노드 이름 변경

- 도메인 이름 변경, 393 페이지
- 노드 이름 변경, 401 페이지
- Cisco Unified Communications Manager의 도메인 이름 업데이트 , 404 페이지

도메인 이름 변경

관리자는 IM and Presence Service 노드 또는 노드 그룹과 연결된 네트워크 수준 DNS 기본 도메인을 수정할 수 있습니다.

엔터프라이즈 수준의 IM and Presence Service 도메인은 IM and Presence Service 노드의 DNS 기본 도메인에 맞출 필요가 없습니다. 배포를 위해 엔터프라이즈 수준 도메인을 수정하려면 *Cisco Unified Communications Manager*의 *IM and Presence Service*용 배포 설명서*IM and Presence Service*용 구성 및 관리 지침서를 참조하십시오.

주의 IM and Presence Service 클러스터의 임의 노드에서 기본 도메인을 변경하면 노드가 다시 시작되고 프레즌스 서비스 및 기타 시스템 기능이 중단됩니다. 시스템에 미치는 이러한 영향 때문에 예약된 유지 관리 기간 동안 이 도메인 변경 절차를 수행해야 합니다.

노드의 기본 도메인 이름을 변경하면 모든 타사 서명 보안 인증서가 새 자체 서명 인증서로 자동으로 덮어쓰여집니다. 타사 인증 기관에서 이러한 인증서를 다시 서명하려면 새 인증서를 수동으로 요청하고 업로드해야 합니다. 이러한 새 인증서를 받으려면 서비스를 다시 시작해야 할 수 있습니다. 새 인증서를 요청하는 데 필요한 시간에 따라 서비스를 다시 시작하도록 예약하기 위해 별도의 유지 관리 기간이 필요할 수 있습니다.

참고 새 인증서는 노드의 기본 도메인 이름을 변경하기 전에 요청할 수 없습니다. CSR(인증서 서명 요청)은 노드에서 도메인을 변경하고 노드를 재부팅한 후에만 생성할 수 있습니다.

IM and Presence Service 기본 도메인 이름 변경 작업

다음 표에는 IM and Presence Service 노드 또는 노드 그룹과 관련된 네트워크 수준 DNS 기본 도메인 이름을 수정하는 방법에 대한 단계별 지침이 포함되어 있습니다. 이 절차에 대한 자세한 지침은 클러스터 내의 여러 노드에 대한 변경을 수행하는 단계의 정확한 순서를 지정합니다.

여러 클러스터에 걸쳐 이 절차를 수행하는 경우 한 번에 한 클러스터에서 변경 사항을 순차적으로 완료해야 합니다.

참고 이 절차의 각 작업은 이 워크플로우에 나타난 정확한 순서대로 완료해야 합니다.

프로시저

단계 **1** 클러스터 내에 있는 모든 해당 노드에서 변경 전 작업을 완료합니다. 일부 변경 전 작업은 IM and Presence 데이타베이스 퍼블리셔 노드에만 적용될 수 있으며 퍼블리셔 노드를 수정하는 경우에는 건너뛸 수 있습니다.

단계 **2** 클러스터 내에 있는 모든 해당 노드에서 IM and Presence Service 노드에 대한 DNS 레코드를 업데이트합니다. 새 노드 도메인을 통합하기에 적합하게 SRV, 정방향(A) 및 역방향(PTR) 레코드도 업데이트합니다.

단계 **3** Cisco Unified Communications Manager 관리를 사용하여 클러스터 내에 있는 모든 해당 노드에서 IM and Presence Service 노드 이름을 업데이트합니다.

참고 이 단계는 FQDN 노드 이름 형식의 경우 필수입니다. 노드 이름이 IP 주소 또는 호스트 이름인 경우에는 해당되지 않습니다.

- 노드 이름이 FQDN이면 이전 노드 도메인 이름을 참조합니다. 따라서, FQDN 값이 새 도메인 이름을 반영하도록 노드 이름을 업데이트해야 합니다.
- 노드 이름이 IP 주소 또는 호스트 이름인 경우 도메인이 참조되지 않으므로 변경이 필요하지 않습니다.

단계 **4** CLI(명령줄 인터페이스)를 사용하여 적용 가능한 모든 노드에서 DNS 도메인을 업데이트합니다. CLI 명령은 노드 운영 체제에서 필요한 도메인 변경을 수행하고 각 노드의 자동 재부팅을 트리거합니다.

단계 **5** 도메인 이름 업데이트 후 클러스터에 있는 모든 노드의 'A Cisco DB' 서비스를 다시 시작하여 모든 노드의 운영 체제 구성 파일이 수정된 노드와 연결된 DNS 도메인 이름 변경을 적용할 수 있도록 합니다.

참고 시스템이 올바로 작동하고 있는지 확인합니다. 복제 문제가 관찰되는 경우 클러스터의 모든 노드를 다시 시작해야 합니다.

단계 **6** CLI를 사용하여 데이터베이스 복제를 확인합니다. 자세한 내용은 시스템 상태 확인 수행 및 데이터베이스 복제 문제 해결 관련 항목을 참조하십시오. 클러스터 내에서 모든 시스템 파일이 동기화된 후에는 데이터베이스 복제를 확인해야 합니다.

단계 7 노드에서 보안 인증서를 재생성합니다.

- 모든 IM and Presence Service 보안 인증서의 주체 공통 이름은 노드 FQDN으로 설정됩니다. 따라서, 새 노드 도메인을 통합하기 위해 DNS 도메인이 변경되면 모든 인증서가 자동으로 재생성됩니다.
- 이전에 인증서에 의해 서명된 인증서.

단계 8 클러스터 내에 있는 모든 해당 노드에 대한 변경 후 작업을 완료하여 클러스터가 완전히 작동하는지 확인합니다.

DNS 레코드 업데이트

노드에 대한 DNS 도메인을 변경하기 때문에 해당 노드와 연결된 기존 DNS 레코드도 업데이트해야 합니다. 여기에는 다음과 같은 유형의 레코드가 포함됩니다.

- 레코드
- PTR 레코드
- SRV 레코드

클러스터 내에서 여러 노드를 수정하 고 있는 경우 이러한 각 노드에 대해 다음 절차를 완료해야 합니다.

IM and Presence 데이타베이스 퍼블리셔 노드를 수정하는 경우 먼저 IM and Presence 데이타베이스 퍼블리셔 노드에서 이 절차를 완료한 후 적용 가능한 IM and Presence Service 가입자 노드에 대해 반복해야 합니다.

참고
- 이러한 DNS 레코드는 노드에서 DNS 도메인이 변경될 때와 동일한 유지 보수 기간 동안 업데이트해야 합니다.
- 예약된 유지 관리 기간 이전에 DNS 레코드를 업데이트하면 IM and Presence Service 기능에 악영향을 미칠 수 있습니다.

시작하기 전에

배포에서 모든 변경 전 작업 및 해당 시스템 상태 확인을 수행합니다.

프로시저

단계 1 이전 도메인에서 노드의 이전 DNS 정방향(A) 레코드를 제거합니다.

단계 2 새 도메인 내 노드에 대한 DNS 정방향(A) 레코드를 새로 만듭니다.

단계 **3** 노드의 업데이트된 FQDN(Fully Qualified Domain Name)을 가리키도록 노드에 대한 DNS 역방향(PTR) 레코드를 업데이트합니다.

단계 **4** 노드를 가리키는 DNS SRV 레코드를 업데이트합니다.

단계 **5** 노드를 가리키는 다른 DNS 레코드를 업데이트합니다.

단계 **6** 각 노드에서 다음 CLI(명령줄 인터페이스) 명령을 실행하여 위의 모든 DNS 변경 사항이 클러스터 내의 다른 모든 노드로 전파되었는지 확인합니다.

a) 새 A 레코드를 확인하려면 **utils network host new-fqdn**을 입력합니다. 여기서 `new-fqdn`은 노드의 업데이트된 FQDN입니다.

예제:

```
admin: utils network host server1.new-domain.com Local Resolution:
server1.new-domain.com resolves locally to 10.53.50.219 External Resolution:
server1.new-domain.com has address 10.53.50.219
```

b) 업데이트된 PTR 레코드를 확인하려면 **utils network host ip-addr**을 입력합니다. 여기서 `ip-addr`은 노드의 IP 주소입니다.

```
admin: utils network host 10.53.50.219 Local Resolution: 10.53.50.219 resolves
 locally to server1.new-domain.com External Resolution: server1.new-domain.com
 has address 10.53.50.219 219.50.53.10.in-addr.arpa domain name pointer
server1.new-domain.com.
```

참고 절차의 이 시점에서 IP 주소에 대한 로컬 해상도 결과는 노드에서 DNS 도메인이 변경될 때까지 이전 FQDN 값을 계속 가리키기 때문입니다.

c) 업데이트된 SRV 레코드를 확인하려면 **utils network host srv-name srv**를 입력합니다. 여기서 `srv-name`은 SRV 레코드입니다.

예제:

_xmpp-server SRV 레코드 조회 예.

```
admin: utils network host _xmpp-server._tcp.galway-imp.com srv Local Resolution:
 Nothing found External Resolution: _xmpp-server._tcp.sample.com has SRV record
 0 0 5269 server1.new-domain.com.
```

다음에 수행할 작업

IM and Presence Service 노드 이름을 업데이트합니다.

FQDN 값의 노드 이름 업데이트

Cisco Unified CM IM and Presence 관리 GUI의 프레즌스 토폴로지 창에서 노드에 대해 정의된 노드 이름이 노드의 FQDN(Fully Qualified Domain Name)으로 설정된 경우에는 이전 도메인 이름을 참조합니다. 따라서 새 도메인 이름을 참조하려면 노드 이름을 업데이트해야 합니다.

참고 이 절차는 이 노드의 노드 이름 값이 FQDN으로 설정된 경우에만 필요합니다. 노드 이름이 노드의 IP 주소 또는 호스트 이름과 일치하는 경우에는 이 절차가 필요하지 않습니다.

클러스터 내에서 여러 노드를 수정하 고 있는 경우 이러한 각 노드에 대해 다음 절차를 순차적으로 완료해야 합니다.

IM and Presence 데이타베이스 퍼블리셔 노드를 수정하는 경우 먼저 퍼블리셔 노드에서 이 절차를 완료하기 전에 IM and Presence Service 가입자 노드에 대해 이 절차를 완료해야 합니다.

시작하기 전에

노드에 대한 DNS 레코드를 업데이트합니다.

프로시저

단계 **1** IM and Presence Service 노드의 노드 이름을 수정합니다.

a) Cisco Unified Communications Manager Administration에 로그인합니다.
b) 시스템 > 서버를 선택합니다.
c) 노드를 검색하고 선택합니다.
d) FQDN이 새 도메인 값을 참조하도록 **Fully Qualified Domain Name/IP** 주소 필드를 업데이트합니다. 예를 들어, **Fully Qualified Domain Name/IP** 주소 값을 `server1.old-domain.com`에서 `server1.new-domain.com`으로 업데이트합니다.
e) 저장을 선택합니다.

단계 **2** 이 노드에 대한 애플리케이션 서버 항목이 Cisco Unified CM IM and Presence 관리 GUI의 프레즌스 토폴로지 창에 새 노드 이름을 반영하도록 업데이트되었는지 확인합니다.

a) Cisco Unified Communications Manager Administration에 로그인하고 시스템 > 애플리케이션 서버를 선택합니다.
b) 필요한 경우 애플리케이션 서버 찾기 및 나열 창에서 찾기를 클릭합니다.
c) 애플리케이션 서버 목록에서 업데이트된 노드 이름에 대한 항목이 존재하는지 확인합니다.

참고 이 노드에 항목이 없거나 항목이 있지만 노드의 이전 노드 이름을 반영하는 경우 계속하지 마십시오.

다음에 수행할 작업

해당하는 모든 노드에서 DNS 도메인을 업데이트합니다.

DNS 도메인 업데이트

CLI(command-line interface)를 사용하여 IM and Presence Service 노드의 DNS 도메인을 변경할 수 있습니다.

엔터프라이즈 수준의 IM and Presence Service도메인은 IM and Presence Service 노드의 네트워크 수준 DNS 기본 도메인에 맞출 필요가 없습니다. 배포를 위해 엔터프라이즈 수준 도메인을 수정하려면 *Cisco Unified Communications Manager*의 *IM and Presence Service*용 배포 설명서를 참조하십시오.

클러스터 내에서 여러 노드를 수정하는 경우에는 각 노드에 대해 다음 절차를 순차적으로 완료해야 합니다.

IM and Presence 데이타베이스 퍼블리셔 노드를 수정 는 경우 먼저 데이터베이스 퍼블리셔 노드에서 이 절차를 완료한 다음 가입자 노드를 수정해야 합니다.

시작하기 전에

IM and Presence Service 노드 이름을 업데이트합니다.

프로시저

단계 **1** 노드에서 CLI에 로그인하고 **set network domain new-domain**을 입력합니다. 여기서 `new-domain`은 설정할 새 도메인 값입니다.

예제:

```
admin: set network domain new-domain.com *** 경고 *** 이 서버에서 도메인 이름을 추가/삭제 또는 변경하면 데이터베이스 복제가 중단됩니다. 수정하려는 모든 시스템에서 도메인 수정을 완료했으면 클러스터의 모든 서버를 재부팅합니다. 이렇게 하면 복제가 제대로 작동합니다. 서버가 재부팅되면 데이터베이스 복제를 위해 Cisco 통합 보고 보고서에 보고된 문제가 없는지 확인하십시오. 이제 서버가 재부팅됩니다. 계속하시겠습니까. 보안 경고 : 이 작동은 타사에서 서명하여 업로드된 인증서 모두를 포함하여 모든 CUP 인증서를 재생성하게 됩니다. 계속할까요(y/n)?
```

단계 **2** **y**를 입력하고 **Return**을 눌러 도메인 변경 사항을 확인하고 노드를 다시 시작하거나 **n**을 입력하여 취소합니다.

팁 노드 이름 변경이 완료되면 모든 인증서가 노드에서 다시 생성됩니다. 타사 인증 기관에 의해 서명된 인증서가 있는 경우 절차에서 나중에 해당 서명 인증서를 다시 요청해야 합니다.

단계 **3** 노드를 다시 시작한 후에 `show network eth0`을 입력하여 도메인 이름 변경 사항이 적용되었는지 확인합니다.

예제:

다음 예의 새 도메인은 new-domain.com입니다.

```
admin: show network eth0 Ethernet 0 DHCP : disabled Status : up IP Address : 10.53.50.219 IP Mask : 255.255.255.000 Link Detected: yes Mode : Auto disabled, Full, 1000 Mbits/s Duplicate IP : no DNS Primary : 10.53.51.234 Secondary : Not Configured Options : timeout:5 attempts:2 Domain : new-domain.com Gateway : 10.53.50.1 on Ethernet 0
```

단계 4 클러스터의 모든 해당 노드에 대해 이전 단계를 반복합니다.

다음에 수행할 작업

클러스터의 모든 노드를 재부팅합니다.

클러스터 노드 고려 사항

CLI(command-line interface)를 사용하여 클러스터의 노드에서 "A Cisco DB" 서비스를 다시 시작할 수 있습니다.

도메인 이름을 변경하고 노드를 재부팅한 후에는 자동으로 재부팅된 노드를 포함하여 클러스터에 있는 모든 노드의 'A Cisco DB' 서비스를 다시 시작해야 합니다 .이 경우에는 Unified CM publisher로 시작하여 게시된 데이터베이스가 표시되는 모든 가입자를 대상으로 합니다. 이렇게 하면 모든 노드의 운영 체제 구성 파일이 새 도메인 값에 정렬됩니다.

시스템이 올바로 작동하고 있는지 확인합니다. 복제 문제가 관찰되는 경우 클러스터의 모든 노드를 다시 시작해야 합니다.

IM and Presence 데이타베이스 퍼블리셔 노드에서 재부팅 프로세스를 먼저 시작합니다. 데이터베이스 퍼블리셔 노드가 다시 시작되면 나머지 IM and Presence 서비스 가입자 노드를 순서대로 재부팅합니다.

시작하기 전에

노드의 DNS 도메인 이름이 변경되었는지 확인합니다.

프로시저

단계 1 CLI를 사용하여 IM and Presence 데이타베이스 퍼블리셔 노드를 재부팅합니다. **utils system restart**를 입력합니다.

예제:

```
admin: utils system 시스템을 다시 시작하시겠습니까? (yes/no) 입력?
```

단계 2 **yes**를 입력하고 **Return** 키를 눌러 다시 시작합니다.

단계 3 IM and Presence 데이타베이스 퍼블리셔 노드가 다시 시작되었음을 알리는 다음 메시지가 표시될 때까지 기다립니다.

예제:

```
루트 브로드캐스트 메시지(Wed Oct 24 16:14:55 2012): 시스템을 재부팅하는 중입니다. 기다려
주십시오. 작업을 지금 다시 시작했습니다.
```

단계 **4** 각 IM and Presence 서비스 가입자 노드에서 CLI에 로그인하고 **utils system restart**을 입력하여 각 가입자 노드를 재부팅합니다.

참고 서비스 중지를 시도한지 몇 분 후 CLI에서 강제로 다시 시작하도록 요청할 수 있습니다. 이 경우 **yes**를 입력합니다.

다음에 수행할 작업

데이터베이스 복제를 확인합니다. 자세한 내용은 시스템 상태 관련 항목을 참조하십시오.

보안 인증서 재생성

노드의 FQDN(Fully Qualified Domain Name)은 모든 IM and Presence Service 보안 인증서에서 주체 공통 이름으로 사용됩니다. 따라서, DNS 도메인이 노드에서 업데이트되면 모든 보안 인증서가 자동으로 재생성됩니다.

타사 인증 기관에 의해 서명된 인증서가 있는 경우 수동으로 새 인증 기관 서명 인증서를 생성해야 합니다.

클러스터 내에서 여러 노드를 수정하는 경우에는 각 노드에 대해 다음 절차를 완료해야 합니다.

참고 새 인증서는 노드의 기본 도메인 이름을 변경하기 전에 요청할 수 없습니다. CSR(인증서 서명 요청)은 노드에서 도메인을 변경하고 노드를 재부팅한 후에만 생성할 수 있습니다.

시작하기 전에

데이터베이스 복제를 확인하여 모든 노드에서 데이터베이스 복제가 성공적으로 설정되었는지 확인합니다.

프로시저

단계 **1** 타사 인증 기관에서 인증서에 서명해야 하는 경우 Cisco Unified 운영 체제 관리 GUI에 로그인하고 각 관련 인증서에 대해 필요한 단계를 수행합니다.

단계 **2** 서명된 인증서를 로드한 후에 IM and Presence Service 노드에 업로드한 후에는 서비스를 다시 시작해야 할 수 있습니다.

필요한 서비스 재시작은 다음과 같습니다.

- Tomcat 인증서: 다음 CLI(command-line interface) 명령을 실행하여 Tomcat 서비스를 다시 시작합니다.

  ```
  utils service restart Cisco Tomcat
  ```

- Cup-xmpp 인증서: Cisco 서비스 가용성 GUI에서 Cisco XCP 라우터 서비스를 다시 시작합니다.

- Cup-xmpp-s2s 인증서: Cisco 서비스 가용성 GUI에서 Cisco XCP 라우터 서비스를 다시 시작합니다.

참고
- 이러한 작업을 수행하면 영향을 받는 서비스가 다시 시작됩니다. 따라서 서명된 인증서를 획득하는 데 걸리는 시간 지연에 따라 나중에 유지 관리 기간을 재시작하도록 예약해야 할 수 있습니다. 그 동안에는 서비스가 다시 시작될 때까지 자체 서명 인증서가 관련 인터페이스에 계속 표시됩니다.
- 인증서가 위의 목록에 지정되지 않은 경우 해당 인증서에 대해 서비스를 다시 시작할 필요가 없습니다.

다음에 수행할 작업

클러스터 내에 있는 모든 해당 노드에서 변경 후 작업 목록을 수행합니다.

노드 이름 변경

IM and Presence Service 노드 또는 노드 그룹과 연결된 노드 이름은 수정할 수 있습니다. 업데이트는 Cisco Unified Communications Manager 관리의 서버 구성 창에 표시됩니다.

다음 노드 이름 변경 시나리오에 이 절차를 사용합니다.

- IP 주소에서 호스트 이름으로
- IP 주소에서 FQDN(Fully Qualified Domain Name)으로
- 호스트 이름에서 IP 주소로
- 호스트 이름에서 FQDN으로
- FQDN에서 호스트 이름으로
- FQDN에서 IP 주소로

노드 이름 권장 사항에 대한 자세한 내용은 *Cisco Unified Communications Manager*의 *IM and Presence Service*용 구축 설명서를 참조하십시오.

주의 이 절차를 사용하여 네트워크 수준 변경이 필요 없는 IM and Presence Service 노드에 대해서만 노드 이름을 변경합니다. 이 경우 네트워크 IP 주소, 호스트 이름 또는 도메인 이름을 변경하는 데 해당되는 절차를 수행합니다. 예약된 유지 관리 기간 동안 이 노드 이름 변경 절차를 수행해야 합니다. IM and Presence Service 클러스터의 임의 노드에서 노드 이름을 변경하면 노드가 다시 시작되고 프레즌스 서비스 및 기타 시스템 기능이 중단됩니다.

IM and Presence Service 노드 이름 변경 작업 목록

다음 표에는 IM and Presence Service 노드 또는 노드 그룹과 연결된 노드 이름을 변경하는 단계별 지침이 포함되어 있습니다. 이 절차에 대한 자세한 지침은 변경을 수행하는 단계의 정확한 순서를 지정합니다.

여러 클러스터에 걸쳐 이 절차를 수행하는 경우 한 번에 한 클러스터의 노드 이름을 변경하는 모든 순차적 단계를 완료합니다.

표 ***83: IM and Presence Service*** 노드 이름 작업 목록 변경

항목	작업
1	클러스터 내에 있는 모든 해당 노드에서 변경 전 작업을 완료합니다. 일부 변경 전 작업은 IM and Presence 데이타베이스 퍼블리셔 노드에만 적용될 수 있으며 퍼블리셔 노드를 수정하는 경우에는 건너뛸 수 있습니다.
2	Cisco Unified Communications Manager 관리를 사용하여 IM and Presence Service 노드 이름을 업데이트합니다.
3	노드 이름 업데이트를 확인하고 노드 이름 변경 사항이 IM and Presence Service와 동기화되었는지 확인합니다.
4	노드 이름 업데이트가 완료된 후 CLI(command-line interface)를 사용하여 데이터베이스 복제를 확인합니다. 새 노드 이름이 클러스터 상에서 복제되 고 모든 노드에서 데이터베이스 복제가 작동하는지 확인합니다.
5	업데이트된 노드에서 변경 후 작업 목록을 완료하고 노드가 제대로 작동하는지 확인합니다.

노드 이름 업데이트

클러스터 내에서 여러 노드를 수정하고 있는 경우 각 노드에 대해 다음 절차를 순차적으로 완료해야 합니다.

IM and Presence 데이타베이스 퍼블리셔 노드를 수정하는 경우 먼저 퍼블리셔 노드에서 이 절차를 완료하기 전에 IM and Presence Service 가입자 노드에 대해 이 절차를 완료해야 합니다.

참고 IM and Presence 노드의 경우 FQDN(Fully Qualified Domain Name)을 사용하는 것이 좋습니다. 그러나 IP 주소와 호스트 이름도 지원됩니다.

시작하기 전에

배포에 대한 모든 변경 전 작업 및 해당 시스템 상태 확인을 수행합니다.

프로시저

단계 1 Cisco Unified CM 관리에 로그인합니다.

단계 2 시스템 > 서버를 선택합니다.

단계 3 수정할 노드를 선택합니다.

단계 4 새 노드 이름을 사용하여 호스트 이름/IP 주소 필드를 업데이트합니다.

참고 새로 생성된 SP 메타데이터를 IDP 서버에 업로드해야 합니다.

단계 5 클러스터 내에서 여러 노드를 수정하고 있는 경우 각 노드에 대해 이 절차를 반복합니다.

참고 IM and Presence Service 노드 이름을 업데이트하고 타사에 대한 호환성이 구성된 경우에는 노드 이름을 기반으로 하는 새 영역을 사용하도록 준수 서버를 업데이트해야 합니다. 이 구성 업데이트는 타사 준수 서버에서 수행됩니다. 새 영역은 **Cisco Unified CM IM and Presence** 관리 > 메시징 > 준수 > 준수 설정 창에 표시됩니다.

다음에 수행할 작업

노드 이름 변경 사항을 확인합니다.

CLI를 사용하여 노드 이름 변경 확인

CLI(command-line interface)를 사용하여 새 노드 이름이 클러스터 상에 서 복제되었는지 확인할 수 있습니다.

프로시저

단계 1 클러스터의 각 노드에서 새 노드 이름이 올바르게 복제 되었는지 확인하려면 **run sql name select from processnode**를 입력합니다.

예제:

```
admin:run sql select name from processnode name ======================
EnterpriseWideData server1.example.com server2.example.com server3.example.com
server4.example.com
```

단계 2 새 노드 이름을 지정하는 클러스터의 각 노드에 대한 항목이 있는지 확인합니다. 이전 노드 이름은 출력에 표시되지 않습니다.

a) 출력이 예상대로 표시되는 경우 유효성 검사가 통과되고 노드의 데이터베이스 복제를 확인하지 않아도 됩니다.

b) 새 노드 이름이 없거나 이전 노드 이름에 대한 기본 설정이 있는 경우 3단계를 계속합니다.

단계 3 누락된 노드 이름 또는 노드에 대해 이전 노드 이름이 표시되는 문제를 해결하려면 다음 작업을 수행합니다.

a) IM and Presence 데이타베이스 퍼블리셔 노드의 경우 동기화 에이전트가 정상적으로 실행 중인지 확인하고 Cisco Unified CM IM and Presence 관리 GUI에서 대시보드를 사용하여 동기화 에이전트 상태에 오류가 없는지 확인합니다.
b) 가입자 노드의 경우 데이터베이스 복제 확인 절차를 수행합니다.

Cisco Unified CM IM and Presence 관리를 사용하여 노드 이름 변경 확인

IM and Presence Service 노드의 경우에만 이 노드에 대한 애플리케이션 서버 항목이 Cisco Unified CM IM and Presence 관리 GUI의 새 노드 이름을 반영하도록 업데이트되었는지 확인합니다.

시작하기 전에

IM and Presence Service 노드 이름을 업데이트합니다.

프로시저

단계 **1** Cisco Unified CM IM and Presence 관리 GUI에 로그인합니다.
단계 **2** 시스템 > 프레즌스 토폴로지를 선택합니다.
단계 **3** 새 노드 이름이 프레즌스 토폴로지 창에 나타나는지 확인합니다.

다음에 수행할 작업

데이터베이스 복제를 확인합니다.

Cisco Unified Communications Manager의 도메인 이름 업데이트

CLI(명령줄 인터페이스)를 사용하여 Cisco Unified Communications Manager에 대한 도메인 이름을 변경할 수 있습니다. CLI를 사용하여 적용 가능한 모든 노드에서 DNS 도메인 이름을 업데이트합니다. CLI 명령은 노드에서 필요한 도메인 변경을 수행하고 각 노드의 자동 재부팅을 트리거합니다.

Unified CM 클러스터 보안 모드가 안전하지 않으며 도메인을 업데이트하거나 변경하는 경우에는 도메인 변경의 일부로 모든 인증서가 다시 생성됩니다. 전화기에서 ITL이 업데이트되었는지 확인하려면 도메인 이름을 업데이트하기 전에 다음 단계를 수행하십시오.

1. 업데이트된 ITL을 처리할 수 있도록 모든 전화기가 온라인 상태이고 등록되어 있는지 확인합니다. 이 절차를 수행할 때 온라인 상태가 아닌 전화기의 경우 ITL을 수동으로 삭제해야 합니다.
2. 롤백을 위한 준비 클러스터를 **8.0** 이전 엔터프라이즈 매개 변수를 **True**로 설정합니다. 모든 전화기는 빈 TVS(신뢰 확인 서비스) 및 TFTP 인증서 섹션을 포함하는 ITL 파일을 자동으로 재설정하고 다운로드합니다.

3. 전화기에서 설정 > 보안 > 신뢰 목록 > **ITL** 파일을 선택하여 ITL 파일의 TVS 및 TFTP 인증서 섹션이 비어 있는지 확인합니다.
4. 서버의 도메인을 변경하고 롤백을 위해 구성된 전화기가 클러스터에 등록되도록 합니다.
5. 모든 전화기가 클러스터에 성공적으로 등록되면 **8.0** 이전으로 롤백하기 위한 클러스터 준비 엔터프라이즈 매개 변수를 **False**로 설정합니다.

시작하기 전에

- 도메인 이름을 변경하기 전에 DNS를 활성화해야 합니다.
- Cisco Unified Communications Manager 관리에 로그인하고 시스템 > 서버 필드 페이지로 이동합니다. 이 서버 구성 설정 페이지에 기존 호스트 이름 항목이 있는 경우 먼저 도메인 이름의 호스트 이름 항목을 변경해야 합니다.
- 모든 변경 전 작업 및 해당 시스템 상태 확인을 수행합니다. 자세한 내용은 관련 항목 섹션을 참조하십시오.

프로시저

단계 **1** 명령줄 인터페이스에 로그인합니다.

단계 **2** **run set network domain <new_domain_name>**을 입력합니다.
이 명령은 시스템을 재부팅할 것인지 묻는 메시지를 표시합니다.

단계 **3** 예를 클릭하여 시스템을 재부팅합니다.
시스템이 재부팅되면 새 도메인 이름이 업데이트됩니다.

단계 **4** 재부팅 후 새 도메인 이름이 업데이트되었는지 확인하려면 네트워크 **show network eth0** 명령을 입력합니다.

단계 **5** 모든 클러스터 노드에서 이 절차를 반복합니다.

다음에 수행할 작업

적용 가능한 모든 변경 후 작업을 수행하여 배포에 변경 사항이 적절히 구현되었는지 확인합니다.

31 장

변경 후 작업 및 확인

- Cisco Unified Communications Manager 노드에 대한 변경 후 작업, 407 페이지
- Cisco Unified Communications Manager 노드에 대한 보안 활성화 클러스터 작업, 410 페이지
- IM and Presence Service 노드에 대한 변경 후 작업, 411 페이지

Cisco Unified Communications Manager 노드에 대한 변경 후 작업

모든 변경 후 작업을 수행하여 배포에 변경 사항이 적절히 구현되었는지 확인합니다.

⚠

주의 이러한 작업을 수행할 때 예상되는 결과를 받지 못하면 문제를 해결할 때까지 계속하지 마십시오.

프로시저

단계 **1** Cisco Unified Communications Manager 서버의 모든 곳에 DNS가 구성되어 있는 경우 정방향 및 역방향 조회 영역이 구성되어 있고 DNS에 연결할 수 있으며 작동하는지 확인하십시오.

단계 **2** 모든 활성 ServerDown 알림을 확인하여 클러스터의 모든 서버가 작동하고 사용 가능한지 확인합니다. 첫 번째 노드에서 Cisco Unified Real-Time Monitoring Tool(RTMT) 또는 CLI(command-line interface)를 사용합니다.

a) Unified RTMT를 사용하여 확인하려면 알림 센트럴에 액세스하고 ServerDown 알림을 확인합니다.

b) 첫 번째 노드에서 CLI를 사용하여 확인하려면 다음 CLI 명령을 입력하고 애플리케이션 이벤트 로그를 검사합니다.

```
file search activelog syslog/CiscoSyslog ServerDown
```

단계 **3** 클러스터의 모든 노드에서 데이터베이스 복제 상태를 확인하여 모든 서버가 데이터베이스 변경을 성공적으로 복제하고 있는지 확인합니다.

IM and Presence Service의 경우 배포에 노드가 두 개 이상 있는 경우 CLI를 사용하여 데이터베이스 게시자 노드의 데이터베이스 복제 상태를 확인합니다.

통합 RTMT 또는 CLI를 사용합니다. 모든 노드에 **2**의 상태가 표시되어야 합니다.

a) RTMT를 사용하여 확인하려면 데이터베이스 요약에 액세스하고 복제 상태를 검사합니다.
b) CLI를 사용하여 확인하려면 **utils dbreplication runtimestate**를 입력합니다.

   예를 들어 출력은 예제 데이터베이스 복제 출력과 관련된 항목을 참조하십시오. 자세한 절차 및 문제 해결은 데이터베이스 복제 확인 및 문제 해결 데이터베이스 복제와 관련된 항목을 참조하십시오.

단계 **4** 다음 예제와 같이 CLI 명령 **utils diagnose**를 입력하여 네트워크 연결 및 DNS 서버 구성을 확인합니다.

예제:

```
admin: utils diagnose module validate_network Log file:
/var/log/active/platform/log/diag1.log Starting diagnostic test(s)
========================== test - validate_network : Passed Diagnostics Completed
 admin:
```

변경 전 시스템 상태 확인을 수행하는 경우에는 작업이 완료된 것입니다. 그렇지 않으면 변경 후 확인 단계를 계속 수행합니다.

단계 **5** 새 호스트 이름 또는 IP 주소가 Cisco Unified Communications Manager 서버 목록에 표시되는지 확인합니다. Cisco Unified Communications Manager 관리에서 시스템 > 서버를 선택합니다.

참고 변경 후 작업의 일부로만 이 단계를 수행합니다.

단계 **6** IP 주소, 호스트 이름 또는 둘 다에 대한 변경 사항이 네트워크에서 완벽하게 구현되었는지 확인합니다. 클러스터의 각 노드에 CLI 명령 **show network cluster**를 입력합니다.

참고 변경 후 작업의 일부로만 이 단계를 수행합니다.

출력에는 노드의 새 IP 주소 또는 호스트 이름이 포함되어야 합니다.

예제:

```
admin:show network cluster 10.63.70.125 hippo2.burren.pst hippo2 Subscriber cups
 DBPub authenticated 10.63.70.48 aligator.burren.pst aligator Publisher callmanager
 DBPub authenticated using TCP since Wed May 29 17:44:48 2013
```

단계 **7** 호스트 이름에 대한 변경 사항이 네트워크에서 완전히 구현되었는지 확인합니다. 클러스터의 각 노드에 CLI 명령 **utils network host<*new_hostname*>**을 입력합니다.

참고 변경 후 작업의 일부로만 이 단계를 수행합니다.

출력에서 새 호스트 이름이 IP 주소로 로컬 및 외부에서 해결되는지 확인해야 합니다.

예제:

```
admin:utils network host hippo2 Local Resolution: hippo2.burren.pst resolves
locally to 10.63.70.125 External Resolution: hippo2.burren.pst has address
10.63.70.125
```

tasks.

단계 **8** 보안을 사용하는 클러스터(클러스터 보안 모드 1 - 혼합)의 경우 시스템 상태 확인 및 기타 변경 후 작업을 수행하기 전에 CTL 파일을 업데이트하고 클러스터의 모든 노드를 다시 시작합니다.

자세한 내용은 다중 서버 클러스터 전화기에 대한 인증서 및 ITL 재생성, 411 페이지 섹션을 참고하십시오.

단계 **9** CTL(Certificate Trust List) 파일 및 USB eTokens을 사용하여 클러스터 보안을 활성화한 경우, 릴리스 8.0 이상 노드에 대한 IP 주소 또는 호스트 이름을 변경한 경우 ITL(초기 신뢰 목록) 파일 및 ITL의 인증서를 다시 생성해야 합니다. CTL(Certificate Trust List) 파일 및 USB eTokens를 사용하여 클러스터 보안을 활성화하지 않은 경우 이 단계를 건너뜁니다.

단계 **10** 수동 DRS 백업을 실행하여 모든 노드 및 활성 서비스가 성공적으로 백업되도록 합니다.

자세한 내용은 *Cisco Unified Communications Manager*용 관리 지침서를 참조하십시오.

참고 노드의 IP 주소를 변경한 다음에는 반드시 수동 DRS 백업을 실행해야 합니다. 서로 다른 IP 주소 또는 호스트 이름을 포함한 DRS 파일로는 노드를 복원할 수 없기 때문입니다. 변경 후 DRS 파일에 새 IP 주소 또는 호스트 이름이 포함됩니다.

단계 **11** 모든 관련 IP 전화기 URL 매개 변수를 업데이트합니다.

단계 **12** Cisco Unified Communications Manager 관리를 사용하여 관련된 모든 IP 전화기 서비스를 업데이트합니다. 시스템 > 엔터프라이즈 매개 변수를 선택합니다.

단계 **13** Unified RTMT 사용자 정의 알림 및 저장된 프로파일을 업데이트합니다.

- 성능 카운터에서 파생되는 Unified RTMT 사용자 정의 알림에는 하드 코딩된 서버 IP 주소가 포함됩니다. 이러한 사용자 정의 알림을 삭제하고 다시 구성해야 합니다.
- 성능 카운터가 있는 Unified RTMT 저장된 프로파일은 하드코딩된 서버 IP 주소를 포함합니다. 이러한 카운터를 삭제하고 다시 추가한 다음 프로파일을 저장하여 새 IP 주소로 업데이트해야 합니다.

단계 **14** Cisco Unified Communications Manager에서 실행되는 통합 DHCP 서버를 사용하는 경우, 해당 DHCP 서버를 업데이트하십시오.

단계 **15** 관련된 다른 Cisco Unified Communications 구성 요소에 필요한 구성을 확인하여 변경합니다.

다음은 확인할 몇 가지 구성 요소의 일부 목록입니다.

- Cisco Unity
- Cisco Unity Connection
- Cisco Unity Express
- SIP/H.323 트렁크
- IOS 게이트키퍼
- Cisco Unified MeetingPlace
- Cisco Unified MeetingPlace Express

- Cisco Unified Contact Center Enterprise
- Cisco Unified Contact Center Express
- IP 전화기에 대한 DHCP 범위
- CDR 내보내기에 대한 Cisco Unified Communications Manager 추적 모음 또는 DRS 백업 대상으로 사용되는 SFTP 서버
- Cisco Unified Communications Manager에 등록되는 IOS 하드웨어 리소스(컨퍼런스 브리지, 미디어 종료 지점, 트랜스코더, RSVP 에이전트)
- Cisco Unified Communications Manager를 등록하거나 통합하는 IPVC 비디오 MCU
- Cisco Emergency Responder
- Cisco Unified Application Environment
- Cisco Unified Presence
- Cisco Unified Personal Communicator
- 연결된 라우터 및 게이트웨이

참고 필요한 구성을 변경하는 방법을 결정하려면 제품 설명서를 참조하십시오.

Cisco Unified Communications Manager 노드에 대한 보안 활성화 클러스터 작업

초기 신뢰 목록 및 인증서 재생성

Cisco Unified Communications Manager 릴리스 8.0 이상 클러스터에서 서버의 IP 주소 또는 호스트 이름을 변경하는 경우 ITL(Initial Trust List) 파일 및 ITL의 인증서가 다시 생성됩니다. 재생성된 파일은 전화기에 저장된 파일과 일치하지 않습니다.

참고 CTL(Certificate Trust List) 파일 및 USB eToken을 사용하여 클러스터 보안을 활성화하는 경우, 신뢰가 eTokens에 의해 유지되고 eToken이 변경되지 않으므로 다음 절차의 단계를 수행할 필요가 없습니다.

클러스터 보안이 활성화되지 않은 경우 단일 서버 클러스터 또는 다중 서버 클러스터 절차의 단계를 수행하여 전화기를 재설정합니다.

단일 서버 클러스터 전화기에 인증서 및 ITL 다시 생성

Cisco Unified Communications Manager 릴리스 8.0 이상 단일 서버 클러스터에서 서버의 IP 주소 또는 호스트 이름을 변경하고 ITL 파일을 사용 중인 경우 다음 단계를 수행하여 전화기를 재설정합니다.

서버의 IP 주소 또는 호스트 이름을 변경하기 전에 롤백을 활성화합니다.

프로시저

단계 **1** 업데이트된 ITL을 처리할 수 있도록 모든 전화기가 온라인 상태이고 등록되어 있는지 확인합니다. 이 절차를 수행할 때 온라인 상태가 아닌 전화기의 경우 ITL을 수동으로 삭제해야 합니다.

단계 **2** 롤백을 위한 준비 클러스터를 8.0 이전 엔터프라이즈 매개 변수를 True로 설정합니다. 모든 전화기는 빈 TVS(신뢰 확인 서비스) 및 TFTP 인증서 섹션을 포함하는 ITL 파일을 자동으로 재설정하고 다운로드합니다.

단계 **3** 전화기에서 설정 > 보안 > 신뢰 목록 > **ITL** 파일을 선택하여 ITL 파일의 TVS 및 TFTP 인증서 섹션이 비어 있는지 확인합니다.

단계 **4** 서버의 IP 주소 또는 호스트 이름을 변경하고 롤백을 위해 구성된 전화기가 클러스터에 등록되도록 합니다.

단계 **5** 모든 전화기가 클러스터에 성공적으로 등록되면 8.0 이전으로 롤백하기 위한 클러스터 준비 엔터프라이즈 매개 변수를 **False**로 설정합니다.

다음에 수행할 작업

CTL 파일 또는 토큰을 사용하는 경우 서버의 IP 주소 또는 호스트 이름을 변경한 후에 CTL 클라이언트를 다시 실행하거나, DNS 도메인 이름을 변경한 후에 CTL 클라이언트를 다시 실행합니다.

다중 서버 클러스터 전화기에 대한 인증서 및 ITL 재생성

다중 서버 클러스터에서 전화기에는 재생성된 ITL 파일 및 인증서를 확인하는 기본 및 보조 TV 서버가 있어야 합니다. 전화기가 기본 TV 서버에 연결할 수 없는 경우(최근 구성 변경으로 인해) 보조 서버로 대체됩니다. TV 서버는 전화기에 할당된 CM 그룹으로 식별됩니다.

다중 서버 클러스터에서는 한 번에 하나의 서버에서만 IP 주소 또는 호스트 이름을 변경해야 합니다. CTL 파일 또는 토큰을 사용하는 경우 서버의 IP 주소 또는 호스트 이름을 변경한 후 또는 DNS 도메인 이름을 변경한 후 CTL 클라이언트 또는 CLI 명령 집합 **utils ctl**을 다시 실행합니다.

IM and Presence Service 노드에 대한 변경 후 작업

모든 변경 후 작업을 수행하여 배포에 변경 사항이 적절히 구현되었는지 확인합니다.

⚠

주의 이러한 작업을 수행할 때 예상되는 결과를 받지 못하면 문제를 해결할 때까지 계속하지 마십시오.

프로시저

단계 **1** 호스트 이름 또는 IP 주소에 대한 변경 사항이 Cisco Unified Communications Manager 서버에서 업데이트되는지 확인합니다.

단계 **2** 변경된 노드에서 네트워크 연결과 DNS 서버 구성을 확인합니다.

참고 IP 주소를 다른 서브넷으로 변경한 경우 네트워크 어댑터가 이제 올바른 VLAN에 연결되어 있는지 확인합니다. 마찬가지로, IP 주소를 변경한 후 IM and Presence Service 노드가 다른 서브넷에 속하는 경우에는 Cisco XCP 라우터 서비스 매개 변수의 라우팅 통신 유형 필드가 라우터 간으로 설정되어 있는지 확인합니다. 그렇지 않으면 라우팅 통신 유형 필드를 멀티캐스트 DNS로 설정해야 합니다.

단계 **3** IP 주소, 호스트 이름 또는 둘 다에 대한 변경 사항이 네트워크에서 완벽하게 구현되었는지 확인합니다.

단계 **4** 호스트 이름을 변경한 경우 호스트 이름이 네트워크에 완전히 구현되었는지 확인합니다.

단계 **5** 데이터베이스 복제가 성공적으로 설정되었는지 확인합니다. 모든 노드에서 상태를 2로 표시하고 연결되어 있어야 합니다. 복제가 설정되지 않은 경우 데이터베이스 복제 문제 해결 관련 항목을 참조하십시오.

단계 **6** SAML SSO(Single Sign-On, 단일 인증를 비활성화한 경우에는 지금 활성화할 수 있습니다. SAML SSO에 대한 자세한 내용은 *Cisco Unified Communications Manager*의 *IM and Presence Service*용 구축 설명서를 참조하십시오.

단계 **7** 호스트 이름을 변경한 경우 cup, cup-xmpp 및 Tomcat 인증서에 새 호스트 이름이 포함되어 있는지 확인해야 합니다.

a) Cisco Unified OS 관리 GUI에서 보안 > 인증서 관리를 선택합니다.
b) 신뢰 인증서의 이름에 새 호스트 이름이 포함되어 있는지 확인합니다.
c) 인증서에 새 호스트 이름이 포함되어 있지 않으면 인증서를 재생성합니다.

자세한 내용은 *Cisco Unified Communications Manager*용 관리 지침서를 참조하십시오.

단계 **8** 노드의 IP 주소가 변경된 경우 Cisco Unified Real-Time Monitoring Tool(RTMT) 사용자 지정 경고 및 저장된 프로파일을 업데이트합니다.

- 성능 카운터에서 파생되는 RTMT 사용자 지정 경고에는 하드코딩된 서버 주소가 포함됩니다. 이러한 사용자 정의 알림을 삭제하고 다시 구성해야 합니다.
- 성능 카운터가 있는 RTMT 저장된 프로파일은 하드코딩된 서버 주소를 포함합니다. 이러한 카운터를 삭제하고 다시 추가한 다음 프로파일을 저장하여 새 주소로 업데이트해야 합니다.

단계 **9** 다른 관련 Cisco Unified Communications 구성 요소(예: Cisco Unified Communications Manager의 SIP 트렁크)에서 필요한 구성을 확인하여 변경합니다.

단계 **10** Cisco 통합 서비스 가용성을 사용하여 CUP 서비스 그룹 아래에 나열된 모든 네트워크 서비스를 시작하고 도구 > 제어 센터 - 네트워크 서비스를 선택합니다.

팁 IP 주소, 호스트 이름 또는 IP 주소와 호스트 이름을 모두 변경하는 경우 이 단계를 완료할 필요가 없습니다. 이러한 이름 변경의 경우 네트워크 서비스가 자동으로 시작됩니다. 그러나, 변경 후에도 일부 서비스가 자동으로 시작되지 않으면 이 단계를 완료하여 모든 네트워크 서비스가 시작되었는지 확인하십시오.

다음 순서에 따라 CUP 서비스 네트워크 서비스를 시작해야 합니다.

1. Cisco IM and Presence 데이터 모니터
2. Cisco 서버 복구 관리자
3. Cisco 라우트 데이터 저장소
4. Cisco 로그인 데이터 저장소
5. Cisco SIP 등록 데이터 저장소
6. Cisco Presence 데이터 저장소
7. Cisco XCP 구성 관리자
8. Cisco XCP 라우터
9. Cisco OAM 에이전트
10. Cisco 클라이언트 프로파일 에이전트
11. Cisco 클러스터 간 동기화 에이전트
12. Cisco 구성 에이전트

단계 **11** Cisco 통합 서비스 가용성을 사용하여 모든 기능 서비스를 시작하려면 도구 > 제어 센터 - 기능 서비스를 선택합니다. 기능 서비스를 시작하는 순서는 중요하지 않습니다.

팁 IP 주소, 호스트 이름 또는 IP 주소와 호스트 이름을 모두 변경하는 경우 이 단계를 완료할 필요가 없습니다. 이러한 이름 변경의 경우 기능 서비스가 자동으로 시작됩니다. 그러나, 변경 후에도 일부 서비스가 자동으로 시작되지 않으면 이 단계를 완료하여 모든 기능 서비스가 시작되었는지 확인하십시오.

단계 **12** 고가용성을 다시 활성화하기 전에 Cisco Jabber 세션이 다시 생성되었는지 확인하십시오. 그렇지 않으면 세션이 생성된 Jabber 클라이언트가 연결할 수 없게 됩니다.

모든 클러스터 노드에서 `show perf query counter "Cisco Presence Engine" ActiveJsmSessions` CLI 명령을 실행합니다. 활성 세션 수는 고가용성을 비활성화할 때 기록한 사용자 수와 일치해야 합니다. 세션을 시작하는 데 30분 이상 소요되는 경우 더 큰 시스템 문제가 있을 수 있습니다.

단계 **13** 변경 전 설정 중에 HA를 비활성화한 경우 모든 프레즌스 이중화 그룹에서 HA(고가용성)를 활성화합니다.

단계 **14** 변경 후 IM and Presence Service가 제대로 작동하는지 확인하십시오.

a) Cisco 통합 서비스 가용성 GUI에서 시스템 > 프레즌스 토폴로지를 선택합니다.

- HA가 활성화된 경우 모든 HA 노드가 정상 상태인지 확인합니다.
- 모든 서비스가 시작되었는지 확인합니다.

b) Cisco Unified CM IM and Presence 관리 GUI에서 시스템 문제 해결 도구를 실행하고 실패한 테스트가 없는지 확인합니다. 진단 > 시스템 문제 해결 도구를 선택합니다.

단계 **15** 노드의 IP 주소 또는 호스트 이름을 변경한 다음에는 반드시 수동 재해 복구 시스템 백업을 실행해야 합니다. 서로 다른 IP 주소 또는 호스트 이름을 포함한 DRS 파일로는 노드를 복원할 수 없기 때문입니다. 변경 후 DRS 파일에 새 IP 주소 또는 호스트 이름이 포함됩니다.

자세한 내용은 *Cisco Unified Communications Manager*용 관리 지침서를 참조하십시오.

32 장

주소 변경 문제 해결

- 클러스터 인증 문제 해결, 415 페이지
- 데이터베이스 복제 문제 해결, 415 페이지
- 네트워크 문제 해결, 420 페이지
- Network Time Protocol troubleshooting, 421 페이지

클러스터 인증 문제 해결

CLI(명령줄 인터페이스)를 사용하여 가입자 노드의 클러스터 인증 문제를 해결할 수 있습니다.

프로시저

단계 **1** 네트워크 구성 확인을 위해 **show network eth0 [detail]**을 입력합니다.

단계 **2** 네트워크 클러스터 정보를 확인하려면 **show network cluster**를 입력합니다.

- 출력에 잘못된 게시자 정보가 표시되면 가입자 노드에 **set network cluster publisher [hostname/IP address]** CLI 명령을 입력하여 정보를 수정합니다.
- 퍼블리셔 노드에 있고 `show network cluster` CLI 명령이 잘못된 가입자 정보를 표시하는 경우 Cisco Unified Communications Manager 관리에 로그인하고 시스템 > 서버를 선택하여 출력을 확인합니다.
- 가입자 노드에 있고 `show network cluster` 출력에 잘못된 게시자 정보가 표시되는 경우 `set network cluster publisher [hostname | IP_address]` CLI 명령을 사용하여 게시자 호스트 이름 또는 IP 주소를 변경합니다.

데이터베이스 복제 문제 해결

명령줄 인터페이스(CLI)를 사용하여 클러스터의 노드에서 데이터베이스 복제를 해결할 수 있습니다.

- 데이터베이스 복제가 클러스터에서 올바른 상태인지 확인합니다.
- 노드에 대한 데이터베이스 복제를 복구하고 재설정합니다.
- 데이터베이스 복제 재설정

이러한 명령 또는 CLI 명령 사용에 대한 자세한 내용은 *Cisco Unified Communications Solutions*용 명령 줄 인터페이스 설명서를 참조하십시오.

데이터베이스 복제 확인

CLI(command-line interface)를 사용하여 클러스터의 모든 노드에 대한 데이터베이스 복제 상태를 확인합니다. RTMT(복제 설정) 및 세부 정보에 값 **2**가 표시되는지 확인합니다. 2 이외의 다른 값은 데이터베이스 복제에 문제가 있으며 노드에 대해 복제를 재설정해야 한다는 것을 의미합니다. 예제 출력은 데이터베이스 복제 예제와 관련된 항목을 참조하십시오.

프로시저

단계 **1** 첫 번째 노드에서 **utils dbreplication runtimestate**를 입력하여 클러스터의 모든 노드에서 데이터베이스 복제를 확인합니다.

IM and Presence Service의 경우 배포에 노드가 두 개 이상 있는 경우 데이터베이스 퍼블리셔 노드에 명령을 입력합니다.

팁 클러스터의 노드에 대해 복제가 설정되지 않은 경우 CLI를 사용하여 노드에 대한 데이터베이스 복제를 재설정할 수 있습니다. 자세한 내용은 CLI를 사용하여 데이터베이스 복제 재설정 관련 항목을 참조하십시오.

예제:

```
admin: utils dbreplication runtimestate DDB and Replication Services: ALL RUNNING
 DB CLI Status: No other dbreplication CLI is running... Cluster Replication
State: BROADCAST SYNC Completed on 1 servers at: 2013-09-26-15-18 Last Sync Result:
 SYNC COMPLETED 257 tables sync'ed out of 257 Sync Errors: NO ERRORS DB Version:
 ccm9_0_1_10000_9000 Number of replicated tables: 257 Repltimeout set to: 300s
Cluster Detailed View from PUB (2 Servers): PING REPLICATION REPL. DBver& REPL.
REPLICATION SETUP SERVER-NAME IP ADDRESS (msec) RPC? STATUS QUEUE TABLES LOOP?
(RTMT) & details ----------- ------------ ------ ---- ----------- ----- ------
----- ----------------- server1 100.10.10.17 0.052 Yes Connected 0 match Yes (2)
 PUB Setup Completed server2 100.10.10.14 0.166 Yes Connected 0 match Yes (2)
Setup Completed
```

단계 **2** 출력을 확인합니다.

출력에는 각 노드에 대해 연결됨 및 복제 설정 값 **(2)** 설정 완료의 복제 상태가 표시되어야 합니다. 이는 클러스터 내 복제 네트워크가 제대로 작동하고 있음을 의미합니다. 출력 결과가 다른 경우 데이터베이스 복제 문제 해결을 계속 진행하여 복구하십시오.

데이터베이스 복제 CLI 출력 예

다음 목록에는 클러스터의 첫 번째 노드에서 `utils dbreplication runtimestate` 명령줄 인터페이스(CLI) 명령을 실행할 때 사용할 수 있는 Replicate_State의 가능한 값이 표시됩니다.

IM and Presence Service의 경우 배포에 노드가 두 개 이상 있는 경우 데이터베이스 퍼블리셔 노드에 명령을 입력합니다.

- 0 - 복제가 시작되지 않았습니다. 가입자가 존재하지 않거나, 가입자가 설치된 이후 데이터베이스 계층 모니터 서비스가 실행되 고 있지 않습니다.
- 1 - 복제를 만들었지만 해당 개수가 잘못되었습니다.
- 2 - 복제가 양호합니다.
- 3 - 클러스터에서 복제가 잘못되었습니다.
- 4 - 복제 설정에 실패했습니다.

참고 RTMT(복제 설정) 및 세부 정보에 값 2가 표시되는지 확인하는 것이 중요합니다. 2 이외의 다른 값은 데이터베이스 복제에 문제가 있으며 복제를 재설정해야 한다는 것을 의미합니다. 데이터베이스 복제 문제 해결에 대한 자세한 내용은 데이터베이스 복제 문제 해결과 관련된 항목을 참조하십시오.

Cisco Unified Communications Manager 노드에 대한 CLI 출력 예

이 예에서는 RTMT(복제 설정) 및 세부 정보에 값 2가 표시됩니다. 복제가 양호합니다.

```
admin: utils dbreplication runtimestate Server Time: Mon Jun 1 12:00:00 EDT 2013
Cluster Replication State: BROADCAST SYNC Completed on 1 servers at:
2013-06-01-12-00 Last Sync Result: SYNC COMPLETED on 672 tables out of 672 Sync
Status: NO ERRORS Use CLI to see detail: 'file view activelog
cm/trace/dbl/2013_06_01_12_00_00_dbl_repl_output_Broadcast.log' DB Version:
ccm10_0_1_10000_1 Repltimeout set to: 300s PROCESS option set to: 1 Cluster
Detailed View from uc10-pub (2 Servers): PING Replication REPLICATION SETUP
SERVER-NAME IP ADDRESS (msec) RPC? Group ID (RTMT) & Details ----------- ----------
 ------ ---- ----------- ------------------- uc10-pub 192.0.2.95 0.040 Yes (g_2)
 (2) Setup Completed uc10-sub1 192.0.2.96 0.282 Yes (g_3) (2) Setup Completed
```

IM and Presence Service 노드에 대한 CLI 출력 예

이 예에서는 RTMT(복제 설정) 및 세부 정보에 값 2가 표시됩니다. 복제가 양호합니다.

```
admin: utils dbreplication runtimestate Server Time: Mon Jun 1 12:00:00 EDT 2013 DB
and Replication Services: ALL RUNNING Cluster Replication State: Replication
status command started at: 2012-02-26-09-40 Replication status command COMPLETED
 269 tables checked out of 269 No Errors or Mismatches found. Use 'file view
activelog cm/trace/dbl/sdi/ReplicationStatus.2012_02_26_09_40_34.out' to see the
 details DB Version: ccm8_6_3_10000_23 Number of replicated tables: 269 Cluster
Detailed View from PUB (2 Servers): PING REPLICATION REPL. DBver& REPL. REPLICATION
 SETUP SERVER-NAME IP ADDRESS (msec) RPC? STATUS QUEUE TABLES LOOP? (RTMT) &
```

```
details ----------- ------------ ------ ---- ----------- ----- ------- -----
----------------- gwydla020218 10.53.46.130 0.038 Yes Connected 0 match Yes (2)
PUB Setup Completed gwydla020220 10.53.46.133 0.248 Yes Connected 128 match Yes
(2) Setup Completed
```

데이터베이스 복제 복구

CLI(명령줄 인터페이스)를 사용하여 데이터베이스 복제를 복구합니다.

프로시저

단계 **1** 데이터베이스 복제 복구를 시도하려면 첫 번째 노드에서 **utils dbreplication repair all**을 입력합니다.

IM and Presence Service에서 배포에 노드가 두 개 이상 있는 경우 데이터베이스 퍼블리셔 노드에서 데이터베이스 복제 상태를 복구합니다.

데이터베이스의 크기에 따라 데이터베이스 복제를 복구하는 데 몇 분 정도 걸릴 수 있습니다. 다음 단계를 진행하여 데이터베이스 복제 복구의 진행률을 모니터링합니다.

예제:

```
admin:utils dbreplication repair all -------------------- utils dbreplication
repair -------------------- Replication Repair is now running in the background.
 Use command 'utils dbreplication runtimestate' to check its progress Output will
 be in file cm/trace/dbl/sdi/ReplicationRepair.2013_05_11_12_33_57.out Please use
 "file view activelog cm/trace/dbl/sdi/ReplicationRepair.2013_05_11_12_33_57.out
 " command to see the output
```

단계 **2** 복제 복구의 진행률을 확인하려면 첫 번째 노드에서 **utils dbreplication runtimestate**를 입력합니다.

IM and Presence Service의 경우 배포에 노드가 두 개 이상 있는 경우 데이터베이스 퍼블리셔 노드에 명령을 입력합니다.

예제 복제 출력의 굵게 표시된 텍스트는 복제 복구의 최종 상태를 강조 표시합니다.

예제:

```
admin:utils dbreplication runtimestate DB and Replication Services: ALL RUNNING
Cluster Replication State: Replication repair command started at: 2013-05-11-12-33
 Replication repair command COMPLETED 269 tables processed out of 269 No Errors
or Mismatches found. Use 'file view activelog
cm/trace/dbl/sdi/ReplicationRepair.2013_05_11_12_33_57.out' to see the details
DB Version: ccm8_6_4_98000_192 Number of replicated tables: 269 Cluster Detailed
 View from PUB (2 Servers): PING REPLICATION REPL. DBver& REPL. REPLICATION SETUP
 SERVER-NAME IP ADDRESS (msec) RPC? STATUS QUEUE TABLES LOOP? (RTMT) & details
----------- ------------ ------ ---- ----------- ----- ------ -----
----------------- server1 100.10.10.17 0.052 Yes Connected 0 match Yes (2) PUB
Setup Completed server2 100.10.10.14 0.166 Yes Connected 0 match Yes (2) Setup
Completed
```

a) 복제 복구가 오류나 불일치 없이 완료될 때까지 실행되는 경우 절차를 실행하여 노드 이름 변경을 다시 확인하여 새 노드 이름이 이제 올바르게 복제되었는지 확인합니다.
b) 오류 또는 불일치가 발견되는 경우 노드 간에 일시적인 불일치가 발생할 수 있습니다. 데이터베이스 복제를 다시 복구하는 절차를 실행합니다.

참고 복제를 여러 번 시도한 후 불일치 또는 오류가 보고되는 경우 Cisco 지원 담당자에게 문의하여 이 문제를 해결하십시오.

단계 **3** 복제 재설정을 시도하려면 첫 번째 노드에서 **utils dbreplication reset all**을 입력합니다.

IM and Presence Service의 경우 배포에 노드가 두 개 이상 있는 경우 데이터베이스 퍼블리셔 노드에 명령을 입력합니다.

데이터베이스의 크기에 따라 복제를 완전히 재설정하는 데 몇 분 정도 걸릴 수 있습니다. 다음 단계를 진행하여 데이터베이스 복제 재설정의 진행률을 모니터링합니다.

예제**:**

```
admin:utils dbreplication reset all 이 명령은 복제 재설정을 시작하려고 시도하고 1-2분
내에 반환됩니다. 복제의 백그라운드 복구는 그런 후 1시간 동안 계속됩니다. RTMT 복제 상태를 확
인하십시오. 0에서 2로 이동해야 합니다. 모든 서브스크립션에서 RTMT 복제 상태가 2이면 복제가
완료됩니다. 서브스크립션 복제 상태가 4 또는 1이 되면 복제 설정에 오류가 있는 것입니다. 모든
서브스크립션에 대해 RTMT 카운터를 모니터링하여 복제가 완료되는 시기를 결정합니다. 오류 세부
정보가 발견되면 OK [10.53.56.14] 아래에 표시됩니다.
```

단계 **4** 첫 번째 노드에서 **utils dbreplication runtimestate**를 입력하여 데이터베이스 복제 재설정을 시도하는 과정을 모니터링합니다.

IM and Presence Service의 경우 배포에 노드가 두 개 이상 있는 경우 데이터베이스 퍼블리셔 노드에 명령을 입력합니다.

모든 노드의 복제 상태가 연결됨이고 복제 설정값이 **(2)** 설정 완료를 표시하는 경우 복제가 재설정된 것으로 간주됩니다 .

예제**:**

```
admin: utils dbreplication runtimestate DDB and Replication Services: ALL RUNNING
 DB CLI Status: No other dbreplication CLI is running... Cluster Replication
State: BROADCAST SYNC Completed on 1 servers at: 2013-09-26-15-18 Last Sync Result:
 SYNC COMPLETED 257 tables sync'ed out of 257 Sync Errors: NO ERRORS DB Version:
 ccm9_0_1_10000_9000 Number of replicated tables: 257 Repltimeout set to: 300s
Cluster Detailed View from newserver100 (2 Servers): PING REPLICATION REPL. DBver&
 REPL. REPLICATION SETUP SERVER-NAME IP ADDRESS (msec) RPC? STATUS QUEUE TABLES
LOOP? (RTMT) & details ----------- -------------- ------ ---- ----------- -----
------ ----- ----------------- server1 100.10.10.201 0.038 Yes Connected 0 match
 Yes (2) PUB Setup Completed server2 100.10.10.202 0.248 Yes Connected 0 match
Yes (2) Setup Completed server3 100.10.10.203 0.248 Yes Connected 0 match Yes (2)
 Setup Completed server4 100.10.10.204 0.248 Yes Connected 0
```

a) 복제가 재설정되는 경우 절차를 실행하여 노드 이름 변경을 다시 확인하여 새 노드 이름이 이제 올바르게 복제되었는지 확인합니다.
b) 복제가 복구되지 않으면 Cisco 지원 담당자에게 문의하여 이 문제를 해결하십시오.

주의 데이터베이스 복제가 끊어진 경우 이 지점 이상으로 진행하지 마십시오.

데이터베이스 복제 재설정

클러스터의 노드에 대해 복제가 설정되지 않은 경우 데이터베이스 복제를 재설정합니다. CLI(명령줄 인터페이스)를 사용하여 데이터베이스 복제를 재설정할 수 있습니다.

시작하기 전에

클러스터의 모든 노드에 대한 데이터베이스 복제 상태를 확인합니다. RTMT(복제 설정) 및 세부 정보에 값 2가 표시되는지 확인합니다. 2 이외의 다른 값은 데이터베이스 복제에 문제가 있으며 노드에 대해 복제를 재설정해야 한다는 것을 의미합니다.

프로시저

단계 **1** 클러스터의 노드에서 복제를 재설정합니다. 다음 중 하나를 수행합니다.

a) Unified Communications Manager의 경우 **utils db replication reset all**을 입력합니다.

Cisco Unified Communications Manager 노드에서 이 CLI 명령을 실행하기 전에 먼저 재설정된 모든 가입자 노드에서 **utils dbreplication stop** 명령을 실행한 다음 게시자 서버에서 명령을 실행합니다. 자세한 내용은 *Cisco Unified Communications Solutions*용 명령줄 인터페이스 설명서를 참조하십시오.

b) IM and Presence Service의 경우 데이터베이스 퍼블리셔 노드에서 **utils db replication reset all**을 입력하여 클러스터에 있는 모든 IM and Presence Service 노드를 재설정합니다.

팁 **all** 대신 특정 호스트 이름을 입력하여 해당 노드에서만 데이터베이스 복제를 재설정할 수 있습니다. 자세한 내용은 *Cisco Unified Communications Solutions*용 명령줄 인터페이스 설명서를 참조하십시오.

단계 **2** **utils dbreplication runtimestate**를 입력하여 데이터베이스 복제 상태를 확인합니다.

IM and Presence Service의 경우 IM and Presence 데이타베이스 퍼블리셔 노드에서 CLI 명령을 실행합니다.

네트워크 문제 해결

CLI(command-line interface)를 사용하여 노드에서 네트워크 문제를 해결할 수 있습니다.

프로시저

단계 1 네트워크 구성 확인을 위해 **show network eth0 [detail]**을 입력합니다.

단계 2 누락된 필드가 있는 경우 네트워크 인터페이스를 재설정합니다.

a) **set network status eth0 down**을 입력합니다.

b) **set network status eth0 up**을 입력합니다.

단계 3 IP 주소, 마스크 및 게이트웨이를 확인합니다.

이러한 값은 네트워크 전체에서 고유해야 합니다.

Network Time Protocol troubleshooting

가입자 노드에서 NTP 문제 해결

CLI(명령줄 인터페이스)를 사용하여 가입자 노드의 NTP(Network Time Protocol) 문제를 해결할 수 있습니다.

프로시저

단계 1 네트워크 구성 확인을 위해 **show network eth0 [detail]**을 입력합니다.

단계 2 NTP 상태를 확인하려면 **utils ntp status**를 입력합니다.

단계 3 NTP를 다시 시작하려면 **utils ntp restart**를 입력합니다.

단계 4 네트워크 클러스터를 확인하려면 **show network cluster**를 입력합니다.

출력에 잘못된 게시자 정보가 표시되면 가입자 노드에 **set network cluster publisher [hostname/IP_address]** CLI 명령을 사용하여 게시자를 재설정합니다.

퍼블리셔 노드에서 NTP 문제 해결

CLI(명령줄 인터페이스)를 사용하여 퍼블리셔 노드의 NTP(Network Time Protocol) 문제를 해결할 수 있습니다.

프로시저

	명령 또는 동작	목적
단계 1	네트워크 구성 확인을 위해 **show network eth0 [detail]**을 입력합니다.	

	명령 또는 동작	목적
단계 2	NTP 상태를 확인하려면 **utils ntp status**를 입력합니다.	
단계 3	NTP를 다시 시작하려면 **utils ntp restart**를 입력합니다.	
단계 4	NTP 서버를 확인하려면 **utils ntp server list**를 입력합니다.	NTP 서버를 추가 또는 삭제하려면 **utils ntp server [add/delete]** CLI 명령을 사용합니다.

VIII 부

재해 복구

- 시스템 백업, 425 페이지
- 시스템 복원, 437 페이지

33 장

시스템 백업

- 백업 개요, 425 페이지
- 필수 구성 요소 백업, 427 페이지
- 백업 작업 흐름, 428 페이지
- 백업 상호 작용 및 제한 사항, 433 페이지

백업 개요

일반 백업을 수행하는 것이 좋습니다. 재난 복구 시스템(DRS)을 사용하여 클러스터의 모든 서버에 대해 전체 데이터 백업을 수행할 수 있습니다. 언제든지 자동 백업을 설정하거나 백업을 호출할 수 있습니다.

재해 복구 시스템은 클러스터 수준 백업을 수행하며 중앙 위치로 Cisco Unified Communications Manager 클러스터의 모든 서버에 대한 백업을 수집하고 백업 데이터를 물리적 저장 장치에 보관합니다. 백업 파일은 암호화되고 시스템 소프트웨어에서만 열 수 있습니다.

DRS은 플랫폼 백업/복원의 일환으로 자체 설정(백업 디바이스 설정 및 예약 설정)을 복원합니다. DRS는 drfDevice.xml 및 drfSchedule.xml 파일을 백업 및 복원합니다. 이러한 파일로 서버가 복원되면 DRS 백업 디바이스 및 일정을 다시 구성할 필요가 없습니다.

시스템 데이터 복원을 수행하면 복원할 클러스터의 노드를 선택할 수 있습니다.

재해 복구 시스템에는 다음과 같은 기능이 포함됩니다.

- 백업 및 복원 작업을 수행하기 위한 사용자 인터페이스.
- 백업 기능을 수행하기 위해 분산된 시스템 아키텍처.
- 예약된 백업 또는 (사용자가 호출한) 수동 백업.
- 원격 sftp 서버에 백업을 보관합니다.

이 테이블에는 재난 복구 시스템에서 백업하고 복원할 수 있는 기능 및 구성 요소가 표시되어 있습니다. 선택하는 각 기능에 대해 시스템이 그 모든 구성 요소를 자동으로 백업합니다.

표 ***84: Cisco Unified CM*** 기능 및 구성 요소

기능	구성 요소
CCM - 통합 커뮤니케이션 매니저	통합 커뮤니케이션 매니저 데이터베이스
	플랫폼
	서비스 가용성
	음악 대기(MOH)
	Cisco Emergency Responder
	벌크 도구(BAT)
	기본 설정
	전화기 파일(TFTP)
	syslogagt(SNMP syslog 에이전트)
	cdpagent(SNMP cdp 에이전트)
	tct(추적 모음 도구)
	CDR(Call Detail Record)
	CDR 보고 및 분석(CAR)

표 ***85: IM and Presence*** 기능 및 구성 요소

기능	구성 요소
IM and Presence Service	IM and Presence 데이터베이스
	syslogagt(SNMP syslog 에이전트)
	cdpagent(SNMP cdp 에이전트)
	플랫폼
	보고자(서비스 가용성 보고자)
	CUP SIP 프록시
	XCP
	CLM
	벌크 도구(BAT)
	기본 설정
	tct(추적 모음 도구)

필수 구성 요소 백업

- 버전 요구 사항을 충족하는지 확인하십시오.
  - 모든 Cisco Unified Communications Manager 클러스터 노드는 동일한 버전의 Cisco Unified Communications Manager 애플리케이션을 실행하고 있어야 합니다.
  - 모든 IM and Presence Service 클러스터 노드는 동일한 버전의 IM and Presence 애플리케이션을 실행하고 있어야 합니다.
  - 백업 파일에 저장된 소프트웨어 버전은 클러스터 노드에서 실행되는 버전과 일치해야 합니다.

  전체 버전 문자열이 일치해야 합니다. 예를 들어, IM and Presence 데이타베이스 게시자 노드의 버전이 11.5.1.10000-1인 경우 모든 IM and Presence는 11.5.1.10000-1이어야 하며 백업 파일도 11.5.1.10000-1이어야 합니다. 현재 버전과 일치하지 않는 백업 파일에서 시스템을 복원하려고 하면 복원이 실패합니다. 백업 파일에 저장된 버전이 클러스터 노드에서 실행되는 버전과 일치하도록 소프트웨어 버전을 업그레이드할 때마다 시스템을 백업해야 합니다.
- DRS 암호화는 클러스터 보안 암호에 따라 달라집니다. 백업을 실행할 때 DRS은 암호화를 위해 임의의 암호를 생성한 다음, 임의의 암호를 클러스터 보안 암호로 암호화합니다. 백업하고 복원하는 사이에 클러스터 보안 암호가 변경된 경우 시스템을 복원하기 위해 해당 백업 파일을 사용

하려면 백업 당시의 암호가 무엇인지 알고 있거나 보안 암호를 변경/재설정한 후 즉시 백업해야 합니다.

- 원격 디바이스로 백업하려는 경우 SFTP 서버를 설정했는지 확인하십시오. 사용 가능한 SFTP 서버에 관한 자세한 내용은 다음을 참조하십시오. 원격 백업용 SFTP 서버 , 434 페이지

백업 작업 흐름

백업을 구성하고 실행하려면 이러한 작업을 수행합니다. 백업이 실행되는 동안에는 OS 관리 작업을 수행하지 마십시오. 그 이유는 재난 복구 시스템이 플랫폼 API를 잠가 모든 OS 관리 요청을 차단하기 때문입니다. 그러나 CLI 기반 업그레이드 명령만 플랫폼 API 잠금 패키지를 사용 하기 때문에 재난 복구 시스템은 대부분의 CLI 명령을 차단하지 않습니다.

프로시저

	명령 또는 동작	목적
단계 **1**	백업 디바이스 구성, 428 페이지	데이터를 백업할 디바이스를 지정합니다.
단계 **2**	백업 파일의 크기 계산, 429 페이지	SFTP 디바이스에 만들어지는 백업 파일의 크기를 예상합니다.
단계 **3**	다음 옵션 중 하나를 선택합니다. • 예약 백업 구성, 430 페이지 • 수동 백업 시작, 431 페이지	일정에 따라 데이터를 백업하는 백업 일정을 만듭니다. 필요한 경우 수동 백업을 실행합니다.
단계 **4**	현재 백업 상태 보기, 432 페이지	(선택 사항) 백업의 상태를 확인합니다. 백업이 실행되는 동안 현재 백업 작업의 상태를 확인할 수 있습니다.
단계 **5**	백업 기록 보기, 433 페이지	(선택 사항) 백업 기록 보기

백업 디바이스 구성

최대 10개의 백업 디바이스를 구성할 수 있습니다. 백업 파일을 저장할 위치를 구성하려면 다음 단계를 수행합니다.

시작하기 전에

- 백업 파일을 저장할 SFTP 서버의 디렉터리 경로에 대한 쓰기 권한이 있는지 확인합니다.
- DRS 마스터 상담원이 백업 디바이스 구성의 유효성을 검사하므로 사용자 이름, 암호, 서버 이름 및 디렉터리 경로가 유효한지 확인합니다.

참고 네트워크 트래픽이 덜할 것으로 예상되는 기간 동안 백업을 예약합니다.

프로시저

단계 **1** 재난 복구 시스템에서 백업 > 백업 디바이스를 선택합니다.

단계 **2** 백업 디바이스 목록 창에서 다음 중 하나를 수행합니다.

- 새 디바이스를 구성하려면 새로 추가를 클릭합니다.
- 기존 백업 디바이스를 편집하려면 검색 조건을 입력하고 [찾기]를 클릭하고 선택한 항목 편집을 클릭합니다.
- 백업 디바이스를 삭제하려면 백업 디바이스 목록에서 디바이스를 선택하고 선택한 항목 삭제를 클릭합니다.

백업 일정에서 백업 디바이스로 구성된 백업 디바이스는 삭제할 수 없습니다.

단계 **3** 백업 디바이스 이름 필드에 백업 이름을 입력합니다.

백업 디바이스 이름은 영숫자, 공백( ), 대시(-) 및 밑줄(_)만 포함합니다. 다른 문자는 사용하지 마십시오.

단계 **4** 대상 선택 영역의 네트워크 디렉터리에서 다음을 수행합니다.

- 호스트 이름/**IP** 주소 필드에 네트워크 서버의 호스트 이름 또는 IP 주소를 입력합니다.
- 경로 이름 필드에 백업 파일을 저장하려는 디렉터리 경로를 입력합니다.
- 사용자 이름 필드에 유효한 사용자 이름을 입력합니다.
- 암호 필드에 유효한 암호를 입력합니다.
- 네트워크 디렉터리에 저장할 백업 수 드롭다운 목록에서 필요한 백업 수를 선택합니다.

단계 **5** 저장을 클릭합니다.

다음에 수행할 작업

백업 파일의 크기 계산, 429 페이지

백업 파일의 크기 계산

하나 이상의 선택된 기능에 대한 백업 기록이 있는 경우에만 Cisco Unified Communications Manager는 백업 tar의 크기를 계산합니다.

계산된 크기는 정확한 값이 아니라 백업 tar의 예상 크기입니다. 크기는 이전의 성공적인 백업의 실제 백업 크기에 따라 계산되고, 마지막으로 백업한 이후 구성을 구성이 변경된 경우 다를 수 있습니다.

처음으로 시스템을 백업할 때가 아닌 및 이전 백업이 존재하는 경우에만 이 절차를 사용할 수 있습니다.

이 절차에 따라 SFTP 디바이스에 저장된 백업 tar의 크기를 예상합니다.

프로시저

단계 **1** 재난 복구 시스템에서 백업 > 수동 백업을 선택합니다.

단계 **2** 기능 선택 영역에서 백업할 기능을 선택합니다.

단계 **3** 예상 크기를 클릭하여 선택한 기능에 대한 백업의 예상 크기를 볼 수 있습니다.

다음에 수행할 작업

다음 절차 중 하나를 수행하여 시스템을 백업합니다.

- 예약 백업 구성, 430 페이지
- 수동 백업 시작, 431 페이지

예약 백업 구성

백업 예약을 최대 10개까지 만들 수 있습니다. 각 백업 일정에 자동 백업 일정, 백업할 기능 집합 및 저장 위치를 포함하여 자체 속성 집합이 있는 경우.

백업 .tar 파일이 임의로 생성되는 암호로 암호화되었는지 확인하십시오. 이 암호는 클러스터 보안 암호를 사용하여 암호화되고 백업 .tar 파일이 함께 저장됩니다. 이 보안 암호를 기억하고 있거나 보안 암호를 변경 또는 재설정한 후 즉시 백업을 수행해야 합니다.

주의 통화 처리 중단을 방지하고 서비스에 영향을 주지 않으려면 사용량이 적은 시간 동안 백업을 예약합니다.

시작하기 전에

백업 디바이스 구성, 428 페이지

프로시저

단계 **1** 재난 복구 시스템에서 백업스케줄러를 선택합니다.

단계 **2** 일정 목록 창에서 다음 단계 중 하나를 수행하여 새 일정을 추가하거나 기존 일정을 편집합니다.

- 새 일정을 만들려면 새로 추가를 클릭합니다.
- 기존 일정을 구성하려면 [일정 목록] 열에서 이름을 클릭합니다.

단계 **3** 스케줄러 창에서 일정 이름 필드에 일정 이름을 입력합니다.

참고 기본 일정의 이름은 변경할 수 없습니다.

단계 **4** 백업 디바이스 선택 영역에서 백업 디바이스를 선택합니다.

단계 **5** 기능 선택 영역에서 백업할 기능을 선택합니다. 하나 이상의 기능을 선택해야 합니다.

단계 **6** 백업 시작 영역에서 백업을 시작할 날짜 및 시간을 선택합니다.

단계 **7** 빈도 영역에서 백업이 발생하도록 하려는 빈도를 선택합니다. 빈도는 매일 한 번, 주별 및 월별로 설정할 수 있습니다. 주별을 선택하는 경우 백업이 발생할 요일을 선택할 수도 있습니다.

팁 백업 빈도를 화요일부터 토요일까지 발생하는 주별로 설정하려면 기본 설정을 클릭합니다.

단계 **8** 이러한 설정을 업데이트하려면 저장을 클릭합니다.

단계 **9** 다음 옵션 중 하나를 선택합니다.

- 선택한 일정을 활성화하려면 선택한 일정 활성화를 클릭합니다.
- 선택한 일정을 비활성화하려면 선택한 일정 비활성화를 클릭합니다.
- 선택한 일정을 삭제하려면 선택한 항목 삭제를 클릭합니다.

단계 **10** 일정을 활성화하려면 일정 활성화를 클릭합니다.

다음 백업은 설정한 시간에 자동으로 발생합니다.

참고 클러스터의 모든 서버에서 동일한 버전의 Cisco Unified Communications Manager 또는 Cisco IM and Presence Service를 실행 중이고 네트워크를 통해 연결할 수 있는지 확인합니다. 예약 백업 실행 시 연결할 수 없는 서버는 백업되지 않습니다.

다음에 수행할 작업

다음 절차를 수행합니다.

- 백업 파일의 크기 계산, 429 페이지
- (선택 사항) 현재 백업 상태 보기, 432 페이지

수동 백업 시작

시작하기 전에

- 백업 파일에 대한 저장 위치로 네트워크 디바이스를 사용하는지 확인합니다. Unified Communications Manager의 가상화된 구축은 백업 파일을 저장할 테이프 드라이브 사용을 지원하지 않습니다.
- 모든 클러스터 노드에 동일한 버전의 Cisco Unified Communications Manager 또는 IM and Presence Service가 설치되었는지 확인하십시오.

- 백업 프로세스는 원격 서버의 사용 가능한 공간 부족 또는 네트워크 연결 중단으로 인해 실패할 수 있습니다. 백업이 실패한 원인이 되는 문제를 해결한 후 새로운 백업 시작해야 합니다.
- 네트워크 중단이 없는지 확인하십시오.
- 백업 디바이스 구성, 428 페이지
- 백업 파일의 크기 계산, 429 페이지
- 클러스터 보안 암호에 대한 기록이 있는지 확인합니다. 이 백업을 완료한 후 클러스터 보안 암호가 변경되는 경우 암호를 알고 있어야 합니다. 그렇지 않으면 백업 파일을 사용하여 시스템을 복원할 수 없습니다.

참고 백업이 실행되는 동안 재난 복구 시스템이 플랫폼 API를 잠가 모든 요청을 차단하기 때문에 Cisco Unified OS 관리 또는 Cisco Unified IM and Presence OS 관리에서 작업을 수행할 수 없습니다. 그러나 CLI 기반 업그레이드 명령만 플랫폼 API 잠금 패키지를 사용하기 때문에 재난 복구 시스템은 대부분의 CLI 명령을 차단하지 않습니다.

프로시저

단계 **1** 재난 복구 시스템에서 백업 > 수동 백업을 선택합니다.
단계 **2** 수동 백업 창의 백업 디바이스 이름 영역에서 백업 디바이스를 선택합니다.
단계 **3** 기능 선택 영역에서 기능을 선택합니다.
단계 **4** 백업 시작을 클릭합니다.

다음에 수행할 작업

(선택 사항) 현재 백업 상태 보기, 432 페이지

현재 백업 상태 보기

현재 백업 작업의 상태를 확인하려면 다음 단계를 수행합니다.

주의 원격 서버에 대한 백업이 20시간 내에 완료되지 않을 경우 백업 세션 시간이 초과되고 새로 백업을 시작해야 합니다.

프로시저

단계 **1** 재난 복구 시스템에서 백업 > 현재 상태를 선택합니다.

단계 **2** 백업 로그 파일을 보려면 로그 파일 이름 링크를 클릭합니다.

단계 **3** 현재 백업을 취소하려면 백업 취소를 클릭합니다.

참고 현재 구성 요소가 백업 작업을 완료한 후에 백업을 취소합니다.

다음에 수행할 작업

백업 기록 보기, 433 페이지

백업 기록 보기

백업 기록을 보려면 다음 단계를 수행합니다.

프로시저

단계 **1** 재난 복구 시스템에서 백업 > 기록을 선택합니다.

단계 **2** 백업 기록 창에서 파일 이름, 백업 디바이스, 완료 날짜, 결과, 버전, 백업된 기능 및 실패한 기능을 포함하여 수행한 백업을 볼 수 있습니다.

참고 백업 기록 창에는 마지막 20개 백업 작업만 표시됩니다.

백업 상호 작용 및 제한 사항

백업 제한 사항

백업에 다음과 같은 제한 사항이 적용됩니다.

표 ***86:*** 백업 제한 사항

제한 사항	설명
클러스터 보안 암호	클러스터 보안 암호를 변경할 때마다 백업을 실행하는 것이 좋습니다. 백업 암호화는 클러스터 보안 암호를 사용하여 백업 파일의 데이터를 암호화합니다. 백업 파일을 만든 후 클러스터 보안 암호를 편집하는 경우 기존 암호가 기억나지 않으면 해당 백업 파일을 사용하여 데이터를 복원할 수 없습니다.

제한 사항	설명
인증서 관리	재난 복구 시스템(DRS)은 Cisco Unified Communications Manager 클러스터 노드 사이에 인증 및 데이터 암호화를 위해 마스터 상담원과 로컬 상담원 간에 SSL 기반 통신을 사용합니다. DRS은 공개/개인 키 암호화를 위해 IPsec 인증서를 사용합니다. 인증서 관리 페이지에서 IPSEC truststore(hostname.pem) 파일을 삭제하는 경우 DRS는 예상대로 작동하지 않습니다. IPSEC-trust 파일을 수동으로 삭제하는 경우 IPSEC 인증서를 IPSEC-trust로 업로드해야 합니다. 자세한 내용은 http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html에서 *Cisco* 통합 커뮤니케이션 매니저 보안 설명서의 "인증서 관리" 섹션을 참조하십시오.

원격 백업용 SFTP 서버

데이터를 네트워크의 원격 디바이스에 백업하려면 SFTP 서버를 구성해야 합니다. 내부 테스트의 경우 Cisco는 Cisco에서 제공하고 Cisco TAC에서 지원하는 Cisco Prime Collaboration Deployment(PCD)의 SFTP 서버를 사용합니다. SFTP 서버 옵션에 대한 요약은 다음 표를 참조하십시오.

다음 표에 있는 정보를 사용하여 시스템에서 사용하는 SFTP 서버 솔루션을 확인합니다.

표 ***87: SFTP*** 서버 정보

SFTP 서버	정보
Cisco Prime Collaboration Deployment의 SFTP 서버	이 서버는 Cisco에서 제공 및 테스트하고 Cisco TAC에서 완벽하게 지원하는 유일한 SFTP 서버입니다. 버전 호환성은 Unified Communications Manager 및 Cisco Prime Collaboration Deployment 버전에 따라 달라집니다. 버전(SFTP) 또는 Unified Communications Manager를 업그레이드하기 전에 버전이 호환되는지 확인하기 위해 Cisco Prime Collaboration Deployment 관리 설명서를 참조하십시오.
기술 파트너의 SFTP 서버	이러한 서버는 타사에서 제공하고 타사에서 테스트했습니다. 버전 호환성은 타사 테스트에 따라 다릅니다. SFTP 제품을 업그레이드하거나 Unified Communications Manager를 업그레이드할 경우 기술 파트너가 페이지에서 버전 호환성 여부를 참조하십시오. https://marketplace.cisco.com

SFTP 서버	정보
다른 타사의 SFTP 서버	이러한 서버는 타사에서 제공하고 Cisco TAC에서 공식 지원하지 않습니다. 버전 호환성은 SFTP 버전 및 Unified Communications Manager 버전의 호환성을 위해 최대한 노력합니다. 참고 이러한 제품은 Cisco에서 테스트하지 않았으므로 기능을 보증할 수 없습니다. Cisco TAC는 이러한 제품을 지원하지 않습니다. SFTP 솔루션을 완벽하게 테스트하고 지원하기 위해 Cisco Prime Collaboration Deployment 또는 기술 파트너를 이용합니다.

암호화 지원

Unified Communications Manager 11.5의 경우 Unified Communications Manager는 SFTP 연결에 대해 다음 CBC 암호화를 광고합니다.

- aes128-cbc
- 3des-cbc
- aes128-ctr
- aes192-ctr
- aes256-ctr

참고 백업 SFTP 서버가 이러한 암호화 중 하나를 지원하여 Unified Communications Manager와 통신하는지 확인하십시오.

Unified Communications Manager 12.0 릴리스부터는 CBC 암호화가 지원되지 않습니다. Unified Communications Manager는 다음 CTR 암호화만 지원하고 광고합니다.

- aes256-ctr
- aes128-ctr
- aes192-ctr

참고 백업 SFTP 서버가 이러한 CTR 암호화 중 하나를 지원하여 Unified Communications Manager와 통신하는지 확인하십시오.

34 장

시스템 복원

- 복원 개요, 437 페이지
- 필수 구성 요소 복원, 438 페이지
- 작업 흐름 복원, 439 페이지
- 데이터 인증, 448 페이지
- 알람 및 메시지, 450 페이지
- 라이선스 예약, 452 페이지
- 복원 상호 작용 및 제한 사항, 454 페이지
- 문제 해결, 455 페이지

복원 개요

재난 복구 시스템(DRS)은 시스템 복원 프로세스를 안내하는 마법사를 제공합니다.

백업 파일은 암호화되어 있으며 DRS 시스템만 데이터를 열어 복원할 수 있습니다. 재해 복구 시스템에는 다음과 같은 기능이 포함됩니다.

- 복원 작업을 수행하기 위한 사용자 인터페이스.
- 복원 기능을 수행하기 위해 분산된 시스템 아키텍처.

마스터 상담원

시스템이 클러스터의 각 노드에서 마스터 에이전트 서비스를 자동으로 시작하지만 마스터 에이전트는 게시자 노드에서만 작동합니다. 가입자 노드의 마스터 에이전트는 모든 기능을 수행하지는 않습니다.

로컬 에이전트

서버에 백업 및 복원 기능을 수행하는 로컬 에이전트가 있습니다.

마스터 에이전트가 포함된 노드를 포함하여 Cisco Unified Communications Manager 클러스터의 각 노드에 백업 및 복원 기능을 수행할 자체 로컬 에이전트가 있어야합니다.

참고 기본적으로 로컬 상담원이 IM and Presence 노드를 포함하여 클러스터의 각 노드에서 자동으로 시작됩니다.

필수 구성 요소 복원

- 버전 요구 사항을 충족하는지 확인하십시오.
  - 모든 Cisco Unified Communications Manager 클러스터 노드는 동일한 버전의 Cisco Unified Communications Manager 애플리케이션을 실행하고 있어야 합니다.
  - 모든 IM and Presence Service 클러스터 노드는 동일한 버전의 IM and Presence 애플리케이션을 실행하고 있어야 합니다.
  - 백업 파일에 저장된 버전은 클러스터 노드에서 실행되는 버전과 일치해야 합니다.

  전체 버전 문자열이 일치해야 합니다. 예를 들어, IM and Presence 데이타베이스 게시자 노드의 버전이 11.5.1.10000-1인 경우 모든 IM and Presence는 11.5.1.10000-1이어야 하며 백업 파일도 11.5.1.10000-1이어야 합니다. 현재 버전과 일치하지 않는 백업 파일에서 시스템을 복원하려고 하면 복원이 실패합니다.
- IP 주소, 호스트 이름, DNS 구성 및 서버의 구축 유형이 백업 파일에 저장된 IP 주소, 호스트 이름, DNS 구성 및 서버의 구축 유형과 일치하는지 확인하십시오.
- 백업을 실행한 후 클러스터 보안 암호를 변경한 경우 기존 암호에 대한 기록이 있어야 합니다. 그렇지 않으면 복원이 실패합니다.

복원 후 **SAML SSO** 다시 활성화

중요 이 섹션은 릴리스 12.5(1)SU7에만 해당됩니다.

DRS을 사용하여 시스템을 복원한 후에는 클러스터의 임의 노드에서 간헐적으로 SAML SSO를 비활성화할 수 있습니다. 영향을 받는 노드에서 SAML SSO를 다시 활성화하려면 다음을 수행해야 합니다.

1. Cisco Unified CM 관리에서 시스템 > **SAML** 싱글 사인-온을 선택합니다.
2. **SSO** 테스트 실행을 클릭합니다.
3. **"SSO** 테스트가 성공 했습니다**!"**라는 메시지가 표시되면 브라우저 창을 닫고 마침을 클릭합니다.

참고 SAML SSO 재활성화 프로세스 중에 Cisco Tomcat이 다시 시작됩니다. SAML SSO가 이미 활성화된 노드에는 영향이 가지 않습니다.

작업 흐름 복원

복원 과정에서 Cisco Unified Communications Manager OS 관리 또는 Cisco Unified IM and Presence OS 관리를 사용하여 작업을 수행하지 마십시오.

프로시저

	명령 또는 동작	목적
단계 **1**	첫 번째 노드만 복원, 439 페이지	(선택 사항) 클러스터의 첫 번째 게시자 노드를 복원하는 경우에만 이 절차를 사용합니다.
단계 **2**	후속 클러스터 노드 복원, 441 페이지	(선택 사항) 클러스터의 가입자 노드를 복원하려면 이 절차를 사용합니다.
단계 **3**	게시자를 다시 빌드한 후 한 번에 클러스터 복원, 443 페이지	(선택 사항) 게시자가 이미 다시 빌드된 경우 한 번에 전체 클러스터를 복원하려면 이 절차를 수행합니다.
단계 **4**	전체 클러스터 복원, 444 페이지	(선택 사항) 게시자 노드를 포함하여 클러스터의 모든 노드를 복원하는 경우 이 절차를 사용합니다. 주요 하드 드라이브 고장 또는 업그레이드 오류가 발생하거나 하드 드라이브를 마이그레이션하는 경우 클러스터의 모든 노드를 다시 빌드해야 할 수 있습니다.
단계 **5**	마지막으로 성공한 구성으로 노드 또는 클러스터 복원, 445 페이지	(선택 사항) 노드를 마지막으로 성공한 구성으로 복원하는 경우 이 절차를 사용합니다. 하드 드라이브 고장 또는 기타 하드웨어 고장이 발생한 후에는 이 절차를 사용하지 마십시오.
단계 **6**	노드 다시 시작, 446 페이지	노드를 다시 시작하려면 이 절차를 사용합니다.
단계 **7**	복원 작업 상태 확인, 447 페이지	(선택 사항) 복원 작업 상태를 확인하려면 이 절차를 사용합니다.
단계 **8**	복원 기록 보기, 447 페이지	(선택 사항) 복원 기록을 보려면 이 절차를 사용합니다.

첫 번째 노드만 복원

다시 빌드한 후에 첫 번째 노드에 복원하는 경우 백업 디바이스를 구성해야 합니다.

이 절차는 Cisco Unified Communications Manager 첫 번째 노드(게시자 노드라고도 함)에 적용됩니다. 다른 Cisco Unified Communications Manager 노드 및 모든 IM and Presence Service 노드는 보조 노드 또는 가입자로 간주됩니다.

시작하기 전에

클러스터에 IM and Presence Service 노드가 있는 경우 첫 번째 노드를 복원할 때 실행 중이고 액세스할 수 있는지 확인합니다. 이는 절차를 수행하는 동안 유효한 백업 파일을 찾을 수 있도록 하는데 필요합니다.

프로시저

단계 **1** 재난 복구 시스템에서 복원 > 복원 마법사를 선택합니다.

단계 **2** 복원 마법사 **1**단계 창의 백업 디바이스 선택 영역에서 복원할 적절한 백업 디바이스를 선택합니다.

단계 **3** 다음을 클릭합니다.

단계 **4** 복원 마법사 **2**단계 창에서 복원하려는 백업 파일을 선택합니다.

참고 백업 파일 이름은 백업 파일을 만든 날짜와 시간을 나타냅니다.

단계 **5** 다음을 클릭합니다.

단계 **6** 복원 마법사 **3**단계 창에서 다음을 클릭합니다.

단계 **7** 복원할 기능을 선택합니다.

참고 백업을 위해 선택한 기능이 표시됩니다.

단계 **8** 다음을 클릭합니다. 복원 마법사 4단계 창이 표시됩니다.

단계 **9** 파일 무결성 확인을 실행하려면 SHA1 메시지 다이제스트를 사용하여 파일 무결성 확인 수행 확인란을 선택합니다.

참고 파일 무결성 확인은 선택 사항이며 SFTP 백업의 경우에만 필요합니다.

파일 무결성 확인 프로세스는 상당한 양의 CPU 및 네트워크 대역폭을 사용하므로 복원 프로세스가 느려집니다.

FIPS 모드에서는 메시지 다이제스트 확인에 대해서도 SHA-1을 사용할 수 있습니다. SHA-1은 디지털 서명에 사용되지 않는 HMAC 및 임의 비트 생성과 같은 해시 함수 애플리케이션의 모든 비 디지털 서명 용도에 사용할 수 있습니다. 예를 들어, SHA-1은 여전히 체크섬을 계산하는 데 사용될 수 있습니다. 서명 생성 및 확인의 경우에만 SHA-1을 사용할 수 없습니다.

단계 **10** 복원할 노드를 선택합니다.

단계 **11** 복원을 클릭하여 데이터를 복원합니다.

단계 **12** 다음을 클릭합니다.

단계 **13** 복원할 노드를 선택하라는 메시지가 표시되면 첫 번째 노드(게시자)만 선택합니다.

주의 복원 시도가 실패하므로 이 조건에서는 후속(가입자) 노드를 선택하지 마십시오.

단계 **14** (선택 사항) 서버 이름 선택 드롭다운 목록에서 게시자 데이터베이스를 복원하려는 가입자 노드를 선택합니다. 선택한 가입자 노드가 서비스 중이고 클러스터에 연결되었는지 확인합니다.
재난 복구 시스템은 백업 파일에서 모든 비 데이터베이스 정보를 복원하고 선택한 가입자 노드에서 최신 데이터베이스를 가져옵니다.

참고 이 옵션은 사용자가 선택한 백업 파일에 CCMDB database 구성 요소가 포함된 경우에 나타납니다. 처음에는 게시자 노드만 완전히 복원되지만 14단계를 수행하고 후속 클러스터 노드를 다시 시작하면 재난 복구 시스템은 데이터베이스 복제를 수행하고 모든 클러스터 노드 데이터베이스를 완벽하게 동기화합니다. 이렇게하면 모든 클러스터 노드가 최신 데이터를 사용하게 됩니다.

단계 **15** 복원을 클릭합니다.

단계 **16** 데이터가 게시자 노드에 복원됩니다. 데이터베이스 크기 및 복원하려고 선택한 구성 요소에 따라 복원하는 데 몇 시간이 필요할 수 있습니다.

참고 첫 번째 노드를 복원하면 전체 Cisco Unified Communications Manager 데이터베이스가 클러스터에 복원됩니다. 복원 중인 해당 데이터베이스의 노드 수와 크기에 따라 여러 시간이 걸릴 수 있습니다. 데이터베이스 크기 및 복원하려고 선택한 구성 요소에 따라 복원하는 데 몇 시간이 필요할 수 있습니다.

단계 **17** 복원 상태 창의 완료율 필드에 100%가 표시되면 서버를 다시 시작합니다. 첫 번째 노드만 복원하는 경우 클러스터의 모든 노드를 다시 시작해야 합니다. 후속 노드를 다시 시작하기 전에 첫 번째 노드를 다시 시작해야 합니다. 서버를 다시 시작하는 방법에 대한 자세한 내용은 다음에 할 일 섹션을 참조하십시오.

참고 Cisco Unified Communications Manager 노드만 복원하는 경우 Cisco Unified Communications Manager 및 IM and Presence Service 클러스터를 다시 시작해야 합니다.

IM and Presence Service 게시자 노드만 복원하는 경우 IM and Presence Service 클러스터를 다시 시작해야 합니다.

다음에 수행할 작업

- (선택 사항) 복원 상태를 보려면 다음을 참조하십시오. 복원 작업 상태 확인, 447 페이지
- 노드를 다시 시작하려면 다음을 참조하십시오. 노드 다시 시작, 446 페이지

후속 클러스터 노드 복원

이 절차는 Cisco Unified Communications Manager 가입자(후속) 가입자 노드에 적용됩니다. 설치된 첫 번째 Cisco Unified Communications Manager 노드가 게시자 노드입니다. 다른 모든 Cisco Unified Communications Manager 노드 및 모든 IM and Presence Service 노드는 가입자 노드입니다.

클러스터에 있는 하나 이상의 Cisco Unified Communications Manager 가입자 노드를 복원하려면 이 절차를 수행합니다.

시작하기 전에

복원 작업을 수행하기 전에 복원의 호스트 이름, IP 주소, DNS 구성 및 구축 유형이 복원하려는 백업 파일의 호스트 이름, IP 주소, DNS 구성 및 구축 유형과 일치하는지 확인합니다. 재난 복구 시스템은 다른 호스트 이름, IP 주소, DNS 구성 및 구축 유형을 복원하지 않습니다.

서버에 설치된 소프트웨어 버전이 복원하려는 백업 파일의 버전과 일치하는지 확인하십시오. 재난 복구 시스템은 복원 작업의 경우 일치하는 소프트웨어 버전만 지원합니다. 다시 빌드한 이후 후속 노드를 복원하는 경우 백업 장치를 구성해야 합니다.

프로시저

단계 **1** 재난 복구 시스템에서 복원 > 복원 마법사를 선택합니다.

단계 **2** 복원 마법사 **1**단계 창의 백업 디바이스 선택 영역에서 복원을 시작할 백업 디바이스를 선택합니다.

단계 **3** 다음을 클릭합니다.

단계 **4** 복원 마법사 **2**단계 창에서 복원하려는 백업 파일을 선택합니다.

단계 **5** 다음을 클릭합니다.

단계 **6** 복원 마법사 **3**단계 창에서 복원하려는 기능을 선택합니다.

참고 사용자가 선택한 파일로 백업한 기능만 표시됩니다.

단계 **7** 다음을 클릭합니다. 복원 마법사 4단계 창이 표시됩니다.

단계 **8** 복원 마법사 **4**단계 창에서 복원할 노드를 선택하라는 메시지가 표시되면 후속 노드만 선택합니다.

단계 **9** 복원을 클릭합니다.

단계 **10** 데이터가 후속 노드에 복원됩니다. 복원 상태를 보는 방법에 대한 자세한 내용은 다음에 할 일 섹션을 참조하십시오.

참고 복원 과정에서 Cisco Unified Communications Manager 관리 또는 사용자 옵션을 사용하여 작업을 수행하지 마십시오.

단계 **11** 복원 상태 창의 완료율 필드에 100%가 표시되면 방금 복원한 보조 서버를 다시 시작합니다. 첫 번째 노드만 복원하는 경우 클러스터의 모든 노드를 다시 시작해야 합니다. 후속 노드를 다시 시작하기 전에 첫 번째 노드를 다시 시작해야 합니다. 서버를 다시 시작하는 방법에 대한 자세한 내용은 다음에 할 일 섹션을 참조하십시오.

참고 IM and Presence Service 첫 번째 노드가 복원된 경우. IM and Presence Service 후속 노드를 다시 시작하기 전에 IM and Presence Service 첫 번째 노드를 다시 시작해야 합니다.

다음에 수행할 작업

- (선택 사항) 복원 상태를 보려면 다음을 참조하십시오. 복원 작업 상태 확인, 447 페이지
- 노드를 다시 시작하려면 다음을 참조하십시오. 노드 다시 시작, 446 페이지

게시자를 다시 빌드한 후 한 번에 클러스터 복원

데이터베이스 크기 및 복원하려고 선택한 구성 요소에 따라 복원하는 데 몇 시간이 필요할 수 있습니다. 게시자가 이미 다시 빌드되었거나 새로 설치한 경우 한 번에 전체 클러스터를 복원하려면 이 절차를 수행합니다.

프로시저

단계 **1** 재난 복구 시스템에서 복원 > 복원 마법사를 선택합니다.

단계 **2** 복원 마법사 **1**단계 창의 백업 디바이스 선택 영역에서 복원을 시작할 백업 디바이스를 선택합니다.

단계 **3** 다음을 클릭합니다.

단계 **4** 복원 마법사 **2**단계 창에서 복원하려는 백업 파일을 선택합니다.

백업 파일 이름은 백업 파일을 만든 날짜와 시간을 나타냅니다.

전체 클러스터를 복원하려는 클러스터의 백업 파일만 선택합니다.

단계 **5** 다음을 클릭합니다.

단계 **6** 복원 마법사 **3**단계 창에서 복원하려는 기능을 선택합니다.

화면에 백업 파일에 저장된 기능만 표시됩니다.

단계 **7** 다음을 클릭합니다.

단계 **8** 복원 마법사 **4**단계 창에서 **1** 단계 복원을 클릭합니다.

이 옵션은 복원을 위해 선택한 백업 파일이 클러스터의 백업 파일이고 복원을 위해 선택한 기능에 게시자 및 가입자 노드에 등록된 기능이 포함된 경우에만 복원 마법사 **4**단계 창에 나타납니다. 자세한 내용은 첫 번째 노드만 복원, 439 페이지 및 후속 클러스터 노드 복원, 441 페이지를 참조하십시오.

참고 상태 메시지에 게시자가 클러스터를 인식하는 데 실패했습니다. *1*단계 복원을 시작할 수 없습니다가 표시되면 퍼블리셔 노드를 복원한 다음, 가입자 노드를 복원해야 합니다. 자세한 내용은 관련 항목을 참조하십시오.

이 옵션을 사용하면 게시자가 클러스터를 인식할 수 있으며 이렇게 하는 데 5분 정도 걸립니다. 이 옵션을 클릭하면 "게시자가 클러스터를 인식할 때까지 5분간 기다리고 이 기간 동안에는 백업 또는 복원 활동을 시작하지 마십시오"라는 상태 메시지가 표시됩니다.

이 지연이 끝난 후 "게시자가 클러스터를 인식하게 되면 게시자가 클러스터를 인식했습니다. 서버를 선택하고 복원을 클릭하여 전체 클러스터의 복원을 시작하십시오.라는 상태 메시지가 표시됩니다".

이 지연이 끝난 후 게시자가 클러스터를 인식하지 못하는 경우 "게시자가 클러스터를 인식하는 데 실패했습니다. 1단계 복원을 시작할 수 없습니다. 계속해서 일반 2단계 복원을 수행하십시오."라는 상태 메시지가 표시됩니다. 2단계(게시자, 그런 다음 가입자)로 전체 클러스터를 복원하려면 첫 번째 노드만 복원, 439 페이지 및 후속 클러스터 노드 복원, 441 페이지에서 설명하는 단계를 수행합니다.

단계 **9** 복원하려면 노드를 선택하라는 메시지가 표시되면 클러스터의 모든 노드를 선택합니다.

재난 복구 시스템은 첫 번째 노드를 복원할 때 후속 노드에서 Cisco Unified Communications Manager 데이터베이스(CCMDB)를 자동으로 복원합니다. 복원 중인 해당 데이터베이스의 노드 수와 크기에 따라 여러 시간이 걸릴 수 있습니다.

단계 **10** 복원을 클릭합니다.
데이터는 클러스터의 모든 노드에 복원됩니다.

단계 **11** 복원 상태 창의 완료율 필드에 100%가 표시되면 서버를 다시 시작합니다. 첫 번째 노드만 복원하는 경우 클러스터의 모든 노드를 다시 시작해야 합니다. 후속 노드를 다시 시작하기 전에 첫 번째 노드를 다시 시작해야 합니다. 서버를 다시 시작하는 방법에 대한 자세한 내용은 다음에 할 일 섹션을 참조하십시오.

다음에 수행할 작업

- (선택 사항) 복원 상태를 보려면 다음을 참조하십시오. 복원 작업 상태 확인, 447 페이지
- 노드를 다시 시작하려면 다음을 참조하십시오. 노드 다시 시작, 446 페이지

관련 항목

첫 번째 노드만 복원, 439 페이지
후속 클러스터 노드 복원, 441 페이지

전체 클러스터 복원

주요 하드 드라이브 고장 또는 업그레이드 오류가 발생하거나 하드 드라이브를 마이그레이션하는 경우 클러스터의 모든 노드를 다시 빌드해야 합니다. 전체 클러스터 복원하려면 다음 단계를 수행합니다.

네트워크 카드 바꾸거나 메모리를 추가하는 등 대부분의 다른 유형의 하드웨어 업그레이드를 수행하는 경우 이 절차를 수행할 필요가 없습니다.

프로시저

단계 **1** 재난 복구 시스템에서 복원 > 복원 마법사를 선택합니다.

단계 **2** 백업 디바이스 선택 영역에서 복원할 적절한 디바이스를 선택합니다.

단계 **3** 다음을 클릭합니다.

단계 **4** 복원 마법사 **2**단계 창에서 복원하려는 백업 파일을 선택합니다.

참고 백업 파일 이름은 백업 파일을 만든 날짜와 시간을 나타냅니다.

단계 **5** 다음을 클릭합니다.

단계 **6** 복원 마법사 **3**단계 창에서 다음을 클릭합니다.

단계 **7** 복원 마법사 **4**단계 창에서 복원 노드를 선택하라는 메시지가 표시될 때 모든 노드를 선택합니다.

단계 **8** 복원을 클릭하여 데이터를 복원합니다.

재해 복구 시스템은 첫 번째 노드를 복원할 때 후속 노드에서 Cisco Unified Communications Manager 데이터베이스(CCMDB)를 자동으로 복원합니다. 해당 데이터베이스의 노드 수와 크기에 따라 여러 시간이 걸릴 수 있습니다.

데이터가 모든 노드에서 복원됩니다.

참고 복원 과정에서 Cisco Unified Communications Manager 관리 또는 사용자 옵션을 사용하여 작업을 수행하지 마십시오.

데이터베이스 크기 및 복원하려고 선택한 구성 요소에 따라 복원하는 데 몇 시간이 필요할 수 있습니다.

단계 **9** 복원 프로세스가 완료되면 서버를 다시 시작합니다. 서버를 다시 시작하는 방법에 대한 자세한 내용은 다음에 할 일 섹션을 참조하십시오.

참고 후속 노드를 다시 시작하기 전에 첫 번째 노드를 다시 시작해야 합니다.

첫 번째 노드가 다시 시작되고 Cisco Unified Communications Manager의 복원된 버전을 실행한 후에 후속 노드를 다시 시작합니다.

단계 **10** 클러스터를 재부팅하면 복제가 자동으로 설정됩니다. *Cisco* 통합 커뮤니케이션 솔루션용 명령줄 인터페이스 설명서에 설명된 대로 “utils dbreplication runtimestate” CLI 명령어를 사용하여 모든 노드에서 복제 상태 값을 확인합니다. 각 노드의 값은 2가되어야합니다.

참고 후속 노드의 데이터베이스 복제는 클러스터의 크기에 따라 후속 노드를 다시 시작한 후 완료하는 데 많은 시간이 걸릴 수 있습니다.

팁 복제가 제대로 설정되지 않은 경우 *Cisco Unified Communications Solutions*용 명령줄 인터페이스 설명서에 설명된 대로 "utils dbreplication rebuild" CLI 명령을 사용합니다.

다음에 수행할 작업

- (선택 사항) 복원 상태를 보려면 다음을 참조하십시오. 복원 작업 상태 확인, 447 페이지
- 노드를 다시 시작하려면 다음을 참조하십시오. 노드 다시 시작, 446 페이지

마지막으로 성공한 구성으로 노드 또는 클러스터 복원

이 절차에 따라 마지막으로 성공한 구성으로 노드 또는 클러스터를 복원합니다.

시작하기 전에

- 복원 파일에 호스트 이름, IP 주소, DNS 구성 및 백업 파일에 구성된 구축 유형이 포함되어 있는지 확인하십시오.
- 서버에 설치된 Cisco Unified Communications Manager 버전이 복원하려는 백업 파일의 버전과 일치하는지 확인하십시오.

- 이 절차는 마지막으로 성공한 구성으로 노드를 복원하는 데만 사용해야 합니다.

프로시저

단계 **1** 재난 복구 시스템에서 복원 > 복원 마법사를 선택합니다.

단계 **2** 백업 디바이스 선택 영역에서 복원할 적절한 디바이스를 선택합니다.

단계 **3** 다음을 클릭합니다.

단계 **4** 복원 마법사 **2**단계 창에서 복원하려는 백업 파일을 선택합니다.

참고 백업 파일 이름은 백업 파일을 만든 날짜와 시간을 나타냅니다.

단계 **5** 다음을 클릭합니다.

단계 **6** 복원 마법사 **3**단계 창에서 다음을 클릭합니다.

단계 **7** 복원 노드를 선택하라는 메시지가 표시되면 해당 노드를 선택합니다.
데이터가 선택한 노드에서 복원됩니다.

단계 **8** 클러스터의 모든 노드를 다시 시작합니다. 첫 번째 Cisco Unified Communications Manager 노드를 다시 시작한 후에 이후의 Cisco Unified Communications Manager 노드를 다시 시작합니다. 클러스터에도 Cisco IM and Presence 노드가 있는 경우 첫 번째 Cisco IM and Presence 노드를 다시 시작한 후에 이후의 IM and Presence 노드를 다시 시작합니다. 자세한 내용은 다음에 할 일 섹션을 참조하십시오.

노드 다시 시작

데이터 복원 후 노드를 다시 시작해야 합니다.

게시자 노드(첫 번째 노드)를 복원하는 경우 먼저 게시자 노드를 다시 시작해야 합니다. 게시자 노드를 다시 시작하고 및 소프트웨어의 복원된 버전을 성공적으로 실행한 후에만 가입자 노드를 다시 시작합니다.

참고 CUCM 퍼블리셔 노드가 오프라인인 경우 IM and Presence 가입자 노드를 다시 시작하지 마십시오. 이러한 경우에는 가입자 노드가 CUCM 퍼블리셔에 연결할 수 없으므로 노드 서비스가 시작되지 않습니다.

주의 이 절차로 인해 시스템이 다시 시작되고 일시적으로 서비스를 사용할 수 없게 됩니다.

다시 시작해야 하는 클러스터의 모든 노드에서 이 절차를 수행합니다.

프로시저

단계 **1** Cisco Unified OS 관리에서 설정 > 버전을 선택합니다.

단계 **2** 노드를 다시 시작하려면 다시 시작을 클릭합니다.

단계 **3** 클러스터를 재부팅하면 복제가 자동으로 설정됩니다. **utils dbreplication runtimestate** CLI 명령을 사용하여 모든 노드에서 복제 상태 값을 확인합니다. 각 노드의 값은 2와 같아야 합니다. CLI 명령어에 관한 내용은 아래의 관련 항목 섹션을 참조하십시오.

복제가 제대로 설정되지 않은 경우 *Cisco* 통합 커뮤니케이션 솔루션용 명령줄 참조 설명서에 설명된 대로 **utils dbreplication reset** CLI 명령어를 사용합니다. CLI 명령어에 관한 내용은 아래의 관련 항목 섹션을 참조하십시오.

참고 후속 노드의 데이터베이스 복제는 클러스터의 크기에 따라 후속 노드를 다시 시작한 후 완료하는 데 여러 시간이 걸릴 수 있습니다.

다음에 수행할 작업

(선택 사항) 복원 상태를 보려면 복원 작업 상태 확인, 447 페이지을 참조하십시오.

관련 항목

Cisco Unified Communications Manager (CallManager) 명령 참조

복원 작업 상태 확인

복원 작업 상태를 확인하려면 이 절차를 수행합니다.

프로시저

단계 **1** 재난 복구 시스템에서 복원 > 현재 상태를 선택합니다.

단계 **2** 복원 상태 창에서 복원 상태를 보려는 로그 파일 이름 링크를 클릭합니다.

복원 기록 보기

복원 기록을 보려면 다음 단계를 수행합니다.

프로시저

단계 **1** 재난 복구 시스템에서 복원 > 기록을 선택합니다.

단계 **2** 복원 기록 창에서 파일 이름, 백업 디바이스, 완료 날짜, 결과, 버전, 복원된 기능 및 실패한 기능을 포함하여 수행한 복원을 볼 수 있습니다.

복원 기록 창에는 마지막 20개 복원 작업만 표시됩니다.

데이터 인증

추적 파일

다음 추적 파일 위치는 문제를 해결하는 동안 또는 로그를 수집하는 동안 사용됩니다.

마스터 에이전트, GUI, 각 로컬 상담원 및 JSch 라이브러리에 대한 추적 파일은 다음 위치에 기록됩니다.

- 마스터 에이전트의 경우 추적 파일 위치: platform/drf/trace/drfMA0*
- 각 로컬 에이전트의 경우 추적 파일 위치: platform/drf/trace/drfLA0*
- GUI의 경우 추적 파일 위치: platform/drf/trace/drfConfLib0*
- JSch의 경우 추적 파일 위치: platform/drf/trace/drfJSch*

자세한 내용은 http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-command-reference-list.html에서 *Cisco* 통합 커뮤니케이션 솔루션용 명령줄 인터페이스 설명서를 참조하십시오.

명령줄 인터페이스

또한 재해 복구 시스템은 다음 표에 표시된 대로 백업 및 복원 기능의 하위 집합에 대한 명령줄 액세스를 제공합니다. 이러한 명령 및 이 명령줄 인터페이스 사용에 대한 자세한 내용은 http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-command-reference-list.html에서 Cisco Unified Communications Solutions용 명령줄 인터페이스 설명서를 참조하십시오.

표 ***88:*** 재해 복구 시스템 명령줄 인터페이스

명령	설명
utils disaster_recovery estimate_tar_size	SFTP/로컬 디바이스에서 백업 tar의 예상 크기를 표시하고 기능 목록에 대해 하나의 매개 변수가 필요
utils disaster_recovery backup	재해 복구 시스템 인터페이스에 구성된 기능을 사용하여 수동 백업 시작
utils disaster_recovery jschLogs	JSch 라이브러리 로깅 활성화 또는 비활성화
utils disaster_recovery restore	복원을 시작하고 백업 위치, 파일 이름, 기능 및 복원할 노드에 대한 매개 변수가 필요

명령	설명
utils disaster_recovery status	진행 중인 백업 또는 복원 작업의 상태 표시
utils disaster_recovery show_backupfiles	기존 백업 파일 표시
utils disaster_recovery cancel_backup	진행 중인 백업 작업 취소
utils disaster_recovery show_registration	현재 구성된 등록 표시
utils disaster_recovery device add	네트워크 디바이스 추가
utils disaster_recovery device delete	디바이스 삭제
utils disaster_recovery device list	모든 디바이스 나열
utils disaster_recovery schedule add	일정 추가
utils disaster_recovery schedule delete	일정 삭제
utils disaster_recovery schedule disable	일정 비활성화
utils disaster_recovery schedule enable	일정 활성화
utils disaster_recovery schedule list	모든 일정 나열
utils disaster_recovery backup	재해 복구 시스템 인터페이스에 구성된 기능을 사용하여 수동 백업 시작
utils disaster_recovery restore	복원을 시작하고 백업 위치, 파일 이름, 기능 및 복원할 노드에 대한 매개 변수가 필요
utils disaster_recovery status	진행 중인 백업 또는 복원 작업의 상태 표시
utils disaster_recovery show_backupfiles	기존 백업 파일 표시
utils disaster_recovery cancel_backup	진행 중인 백업 작업 취소
utils disaster_recovery show_registration	현재 구성된 등록 표시

알람 및 메시지

알람 및 메시지

재해 복구 시스템 문제는 백업 또는 복원 절차 동안 발생할 수 있는 다양한 오류에 대해 알람을 제공합니다. 다음 표에서는 Cisco 재해 복구 시스템 알람 목록을 제공합니다.

표 ***89:*** 재해 복구 시스템 알람 및 메시지

알람 이름	설명	설명
DRFBackupDeviceError	DRF 백업 프로세스가 디바이스에 액세스하는 데 문제가 있습니다.	디바이스에 액세스하는 동안 D 프로세스에 오류가 발생했습니
DRFBackupFailure	Cisco DRF 백업 프로세스가 실패했습니다.	DRS 백업 프로세스에 오류가 니다.
DRFBackupInProgress	다른 백업을 실행 중에는 새 백업을 시작할 수 없습니다.	다른 백업을 실행 중에는 DRS 업을 시작할 수 없습니다.
DRFInternalProcessFailure	DRF 내부 프로세스에 오류가 발생했습니다.	DRS 내부 프로세스에 오류가 니다.
DRFLA2MAFailure	DRF 로컬 에이전트가 마스터 에이전트에 연결할 수 없습니다.	DRS 로컬 에이전트가 마스터 에 연결할 수 없습니다.
DRFLocalAgentStartFailure	DRF 로컬 에이전트가 시작되지 않습니다.	DRS 로컬 에이전트가 종료될 다.
DRFMA2LAFailure	DRF 마스터 에이전트가 로컬 에이전트에 연결할 수 없습니다.	DRS 마스터 에이전트가 로컬 에 연결할 수 없습니다.
DRFMABackupComponentFailure	DRF가 하나 이상의 구성 요소를 백업할 수 없습니다.	DRS가 데이터를 백업할 구성 청했습니다.하지만 백업 프로 오류가 발생했으며 구성 요소 지 않았습니다.
DRFMABackupNodeDisconnect	백업 중인 노드가 완전히 백업되기 전에 마스터 에이전트에서 연결이 끊어졌습니다.	DRS 마스터 에이전트가 Cisco Communications Manager 노드 작업을 실행하는 동안 백업 작 되기 전에 노드 연결이 끊어졌
DRFMARestoreComponentFailure	DRF가 하나 이상의 구성 요소를 복원할 수 없습니다.	DRS가 데이터를 복원할 구성 청했습니다.하지만 복원 프로 오류가 발생했으며 구성 요소 지 않았습니다.

알람 이름	설명	설명
DRFMARestoreNodeDisconnect	복원 중인 노드가 완전히 복원되기 전에 마스터 에이전트에서 연결이 끊어졌습니다.	DRS 마스터 에이전트가 C Communications Manager 노 작업을 실행하는 동안 복원 되기 전에 노드 연결이 끊어
DRFMasterAgentStartFailure	DRF 마스터 에이전트가 시작되지 않았습니다.	DRS 마스터 에이전트가 종 니다.
DRFNoRegisteredComponent	등록된 구성 요소를 사용할 수 없으므로 백업에 실패했습니다.	등록된 구성 요소를 사용할 DRS 백업에 실패했습니다
DRFNoRegisteredFeature	백업을 위한 기능을 선택하지 않았습니다.	백업을 위한 기능을 선택하 다.
DRFRestoreDeviceError	DRF 복원 프로세스가 디바이스에 액세스하는 데 문제가 있습니다.	디바이스에서 DRS 복원 프 수 없습니다.
DRFRestoreFailure	DRF 복원 프로세스가 실패했습니다.	DRS 복원 프로세스에 오류 니다.
DRFSftpFailure	DRF SFTP 작업에 오류가 발생했습니다.	DRS SFTP 작업에서 오류가 다.
DRFSecurityViolation	DRF 시스템이 보안 위반이 발생할 수 있는 악의적인 패턴을 발견했습니다.	DRF 네트워크 메시지에 코 디렉터리 통과 같은 보안 위 수 있는 악의적인 패턴이 포 니다. DRF 네트워크 메시지 습니다.
DRFTruststoreMissing	IPsec truststore가 노드에 누락되어 있습니다.	IPsec truststore가 노드에 누 니다. DRF 로컬 에이전트가 이전트에 연결할 수 없습니
DRFUnknownClient	Pub의 DRF 마스터 에이전트가 클러스터 외부의 알 수 없는 서버로부터 클라이언트 연결 요청을 받았습니다. 요청이 거부되었습니다.	Pub의 DRF 마스터 에이전 터 외부의 알 수 없는 서버 이언트 연결 요청을 받았습 거부되었습니다.
DRFBackupCompleted	DRF 백업이 성공적으로 완료되었습니다.	DRF 백업이 성공적으로 완 다.
DRFRestoreCompleted	DRF 복원이 성공적으로 완료되었습니다.	DRF 복원이 성공적으로 완 다.
DRFNoBackupTaken	DRF가 현재 시스템의 유효한 백업을 찾지 못했습니다.	DRF가 업그레이드/마이그 새로 설치 후 현재 시스템의 업을 찾지 못했습니다.

알람 이름	설명	설명
DRFComponentRegistered	DRF가 요청된 구성 요소를 성공적으로 등록했습니다.	DRF가 요청된 구성 요소를 성 등록했습니다.
DRFRegistrationFailure	DRF를 등록하지 못했습니다.	일부 내부 오류로 인해 구성 요 한 DRF 등록 작업이 실패했습
DRFComponentDeRegistered	DRF가 요청된 구성 요소를 성공적으로 등록 해제했습니다.	DRF가 요청된 구성 요소를 성 등록 해제했습니다.
DRFDeRegistrationFailure	구성 요소에 대한 DRF 등록 해제 요청이 실패했습니다.	구성 요소에 대한 DRF 등록 해 이 실패했습니다.
DRFFailure	DRF 백업 또는 복원 프로세스가 실패했습니다.	DRF 백업 또는 복원 프로세스 발생했습니다.
DRFRestoreInternalError	DRF 복원 작업에 오류가 발생했습니다. 복원이 내부적으로 취소되었습니다.	DRF 복원 작업에 오류가 발생 복원이 내부적으로 취소되었습
DRFLogDirAccessFailure	DRF가 로그 디렉터리에 액세스할 수 없습니다.	DRF가 로그 디렉터리에 액세스 습니다.
DRFDeRegisteredServer	DRF가 서버에 대한 모든 구성 요소를 자동으로 등록 해제했습니다.	서버가 Unified Communications 클러스터에서 연결이 끊어졌습
DRFSchedulerDisabled	백업에 사용할 수 있는 기능이 구성되지 않아 DRF 스케줄러가 비활성화되었습니다.	백업에 사용할 수 있는 기능이 않아 DRF 스케줄러가 비활성 니다.
DRFSchedulerUpdated	기능 등록 해제로 인해 DRF 일정 백업 구성이 자동으로 업데이트되었습니다.	기능 등록 해제로 인해 DRF 일 구성이 자동으로 업데이트되었

라이선스 예약

라이선스 예약

중요 다음 라이선스 기능 표는 Unified CM 14su1 릴리스까지 지원됩니다.

특정 라이센스 예약 활성화된 Unified Communications Manager에서 복원 작업을 수행한 후에는 다음 단계를 따르십시오.

표 ***90:*** 라이센스 예약을 위한 재해 복구 시스템

복원 후 상태	**CSSM**의 제품	해결 방법
등록 취소됨	예	CSSM에서 제품을 제거하고 제품에서 등록하려면 Cisco에 문의하십시오.
	아니요	필요한 것 없음
예약 진행 중	예	다음 절차 중 하나를 수행합니다. 절차-1: **1.** CSSM에서 제품에 대한 인증 코드를 가져옵니다. **2.** 인증 코드 라이센스 스마트 예약 반환 인증 **"<authorization-code>"**를 제공하여 아래 CLI를 실행합니다. 절차-2: **1.** CSSM에서 제품을 제거하려면 Cisco에 문의하십시오.
	아니요	제품 라이센스 스마트 예약 취소에서 CLI를 실행합니다.
등록됨	예	**1.** 제품에서 아래 CLI 라이센스 스마트 예약 반환을 실행합니다. 예약 반환 코드가 콘솔에 인쇄됩니다. **2.** CSSM에 예약 반환 코드를 입력하여 제품을 제거합니다.
	아니요	제품 라이센스 스마트 예약 반환에서 CLI를 실행합니다.

복원 상호 작용 및 제한 사항

복원 제한 사항

다음 제한 사항은 재난 복구 시스템을 사용하여 Cisco Unified Communications Manager 또는 IM and Presence Service를 복원하는 데 적용됩니다.

표 ***91:*** 복원 제한 사항

제한 사항	설명
수출 제한	제한된 버전에서 제한된 버전으로만 DRS 백업을 복원할 수 있으며 무제한 버전의 백업은 무제한 버전에만 복원할 수 있습니다. Cisco Unified Communications Manager의 미국 수출 무제한 버전으로 업그레이드하는 경우 나중에 이 소프트웨어의 미국 수출 제한 버전으로 업그레이드하거나 새로 설치를 수행할 수 없습니다.
플랫폼 마이그레이션	재난 복구 시스템을 사용하여 플랫폼 간에 데이터를 마이그레이션할 수 없습니다(예를 들어, Windows에서 Linux로 또는 Linux에서 Windows로). 복원은 백업과 동일한 제품 버전에서 실행해야 합니다. Windows 기반 플랫폼에서 Linux 기반 플랫폼으로 데이터 마이그레이션에 대한 자세한 내용은 *Data Migration Assistant* 사용 설명서를 참조하십시오.
하드웨어 교체 및 마이그레이션	데이터를 새 서버로 마이그레이션하기 위해 DRS 복원을 수행할 때 이전 서버에서 사용한 것과 동일한 IP 주소 및 호스트 이름을 새 서버에 할당해야 합니다. 또한 백업을 수행할 때 DNS가 구성된 경우 복원을 수행하기 전에 동일한 DN 구성이 있어야합니다. 서버를 교체하는 방법에 대한 자세한 내용은 *Cisco Unified Communications Manager* 단일 서버 또는 클러스터 교체 설명서를 참조하십시오. 뿐만 아니라, 하드웨어 교체 후 인증서 신뢰 목록(CTL) 클라이언트를 실행해야 합니다. 후속 노드(가입자) 서버를 복원하지 않은 경우 CTL 클라이언트를 실행해야 합니다. 다른 경우에는 DRS가 필요한 인증서를 백업합니다. 자세한 내용은 *Cisco* 통합 커뮤니케이션 매니저 보안 설명서에서 “CTL 클라이언트 설치” 및 “CTL 클라이언트 설정” 절차를 참조하십시오.
클러스터 간 Extension Mobility	백업에서 원격 클러스터에 로그인한 클러스터 간 내선 이동 사용자는 복구 후 로그인을 유지합니다.

참고 DRS 백업/복원은 CPU를 많이 사용하는 프로세스입니다. 스마트 라이센스 관리자는 백업 및 복원되는 구성 요소 중 하나입니다. 이 프로세스를 진행하는 동안 스마트 라이센스 관리자 서비스가 다시 시작됩니다. 리소스 사용률이 높게 예상되므로 유지 관리 기간 중에 프로세스를 예약하는 것이 좋습니다.

Cisco Unified Communications 서버 구성 요소를 성공적으로 복원한 후 Cisco Unified Communications Manager를 Cisco Smart Software Manager 또는 Cisco Smart Software Manager 위성을 사용하여 등록합니다. 백업을 수행하기 전에 이미 제품이 등록된 경우 라이센스 정보를 업데이트하기 위해 제품을 다시 등록합니다.

Cisco Smart Software Manager 또는 Cisco Smart Software Manager 위성에 제품을 등록하는 방법에 대한 자세한 내용은 해당 릴리스의 *Cisco Unified Communications Manager* 시스템 구성 설명서를 참조하십시오.

문제 해결

더 작은 가상 시스템으로 **DRS** 복원 실패

문제

IM and Presence Service 노드를 디스크 더 작은 VM으로 복원하는 경우 데이터베이스 복원이 실패할 수 있습니다.

원인

이 오류는 큰 디스크 크기에서 작은 디스크 크기로 마이그레이션하는 경우에 발생합니다.

해결 방법

2개의 가상 디스크가 있는 OVA 템플릿에서 복원을 위해 VM을 구축합니다.

IX 부

문제 해결

- 문제 해결 개요, 459 페이지
- 문제 해결 도구, 463 페이지
- TAC를 사용하여 케이스 열기, 491 페이지

35 장

문제 해결 개요

이 섹션에서는 Unified Communications Manager의 문제 해결에 필요한 배경 정보 및 사용 가능한 리소스를 제공합니다.

- Cisco 통합 서비스 가용성, 459 페이지
- Cisco Unified Communications 운영 체제 관리, 460 페이지
- 문제 해결을 위한 일반 모델, 460 페이지
- 네트워크 오류 준비, 461 페이지
- 추가 정보 확인 위치, 461 페이지

Cisco 통합 서비스 가용성

Unified Communications Manager용 웹 기반 문제 해결 도구인 Cisco 유니파이드 Serviceability는 관리자가 시스템 문제를 해결하는 데 도움이 되는 다음 기능을 제공합니다.

- 문제 해결에 대한 Unified Communications Manager 서비스 경보 및 이벤트를 저장하고 경보 메시지 정의를 제공합니다.
- 문제 해결에 대한 여러 로그 파일에 Unified Communications Manager 서비스 추적 정보를 저장합니다. 관리자는 추적 정보를 구성하고 수집하고 볼 수 있습니다.
- 실시간 모니터링 도구를 통해 Unified Communications Manager 클러스터에서 구성 요소의 실시간 동작을 모니터링합니다.
- Unified Communications Manager CDR 분석 및 보고(CAR)를 통한 서비스 품질, 트래픽 및 청구 정보에 대한 보고서를 생성합니다.
- [서비스 활성화] 창을 통해 활성화 및 비활성화하고 볼 수 있는 기능 서비스를 제공합니다.
- 기능 및 네트워크 서비스를 시작하고 중지하는 인터페이스를 제공합니다.
- Cisco 유니파이드 Serviceability 도구와 연결된 보고서를 보관합니다.
- Unified Communications Manager가 SNMP 원격 관리 및 문제 해결을 위해 관리되는 장치로 작동하는 것을 허용합니다.
- 서버(또는 클러스터의 모든 서버)에서 로그 파티션의 디스크 사용을 모니터링합니다.

탐색 드롭다운 목록 상자에서 Cisco 유니파이드 Serviceability을 선택하여 Cisco 통합 커뮤니케이션 매니저 관리 창에서 Cisco 유니파이드 Serviceability에 액세스합니다. Unified Communications Manager 소프트웨어를 설치하면 Cisco 유니파이드 Serviceability이(가) 자동으로 설치되어 사용할 수 있습니다.

서비스 가용성 도구에 대한 자세한 정보 및 구성 절차에 대한 *Cisco* 통합 서비스 가용성 관리 가이드를 참조하십시오.

Cisco Unified Communications 운영 체제 관리

Cisco 통합 커뮤니케이션 운영 체제 관리를 사용하여 *Cisco* 통합 커뮤니케이션 운영 체제를 구성하고 관리하는 다음 작업을 수행합니다.

- 소프트웨어 및 하드웨어 상태 확인
- IP 주소 확인 및 업데이트
- 다른 네트워크 장치 Ping
- NTP(Network Time Protocol) 서버 관리
- 시스템 소프트웨어 및 옵션 업그레이드
- 시스템을 다시 시작합니다.

서비스 가용성 도구에 대한 자세한 정보 및 구성 절차는 Cisco 통합 커뮤니케이션 매니저 관리 지침서의 내용을 참조하십시오.

문제 해결을 위한 일반 모델

전화 통신 또는 IP 네트워크 환경 문제를 해결하는 경우, 특정 증상을 정의하고, 증상을 일으킬 수 있는 잠재적인 문제를 모두 파악한 다음, 증상이 사라질 때까지 각 잠재적 문제(가능성이 가장 큰 것부터 가장 작은 것 순으로)를 체계적으로 제거할 수 있습니다.

다음 단계에서는 문제 해결 과정에서 사용할 수 있는 지침을 제공합니다.

절차

1. 네트워크 문제를 분석하고 명확한 문제 설명을 생성합니다. 증상 및 잠재 원인을 정의합니다.
2. 가능한 원인을 파악하는 데 필요한 정보를 수집합니다.
3. 수집한 정보에 따라 가능한 원인을 고려합니다.
4. 해당 원인에 따라 실행 계획을 만듭니다. 문제가 발생할 가능성이 가장 높은 것으로 시작하여 한 변수만을 조작하는 계획을 세웁니다.
5. 실행 계획을 구현합니다. 테스트하는 동안 각 단계를 신중하게 수행하여 증상이 사라지는지 여부를 확인합니다.

6. 결과를 분석하여 문제가 해결되었는지 확인합니다. 문제가 해결된 경우에는 프로세스 완료를 고려합니다.
7. 문제가 해결되지 않은 경우 목록에서 그 다음으로 가장 중요한 원인을 기준으로 실행 계획을 만듭니다. 4, 460 페이지로 돌아가서 문제가 해결될 때까지 이 프로세스를 반복합니다.

실행 계획을 구현하는 동안 변경된 사항을 모두 취소해야 합니다. 한 번에 하나의 변수만 변경해야 합니다.

참고 일반 원인과 작업(이 문서에 요약된 작업 또는 환경에서 식별된 다른 작업)을 모두 사용하는 경우 Cisco TAC에 문의하십시오.

네트워크 오류 준비

미리 준비된 경우 네트워크 오류에서 더 쉽게 복구할 수 있습니다. 네트워크 실패를 준비했는지 확인하려면 다음 질문에 응답하십시오.

- 네트워크에 있는 모든 장치의 물리적 위치와 연결 방법, 네트워크 주소, 네트워크 번호 및 하위 네트워크의 논리적 맵을 개괄적으로 보여주는 정확한 물리적 및 논리적 맵이 있습니까?
- 구현된 각 프로토콜에 대해 네트워크에서 구현되는 모든 네트워크 프로토콜 목록과 네트워크 번호, 하위 네트워크, 영역 및 연결된 영역의 목록이 있습니까?
- 라우팅 중인 프로토콜과 각 프로토콜에 대한 올바른 최신 구성 정보를 알고 있습니까?
- 어떤 프로토콜이 브리지되고 있는지 알고 있습니까? 이러한 브리지에서 구성된 필터가 있습니까? 그리고 이러한 구성의 복사본이 있습니까? 이는 Unified Communications Manager에 해당합니까?
- 인터넷 연결을 포함하여 외부 네트워크에 대한 모든 연결 지점을 알고 있습니까? 각 외부 네트워크 연결에 대해 사용 중인 라우팅 프로토콜을 알고 있습니까?
- 조직에서 일반 네트워크 동작 및 성능을 문서화하여 현재 문제를 초기 계획과 비교할 수 있습니까?

이러한 질문에 대해 예라고 응답할 수 있다면 오류 발생 시 보다 빠른 복구를 수행할 수 있습니다.

추가 정보 확인 위치

다양한 IP 텔레포니 항목에 대한 정보를 보려면 다음 링크를 사용하십시오.

- 관련 Cisco IP 텔레포니 애플리케이션 및 제품에 대한 자세한 내용은 *Cisco Unified Communications Manager* 문서 안내서를 참조하십시오. 다음 URL은 문서 안내서에 대한 경로의 예를 보여줍니다.

https://www.cisco.com/en/US/products/sw/voicesw/ps556/products_documentation_roadmaps_list.html

- Cisco Unity 관련 설명서는 다음 URL을 참조하십시오.
  https://www.cisco.com/en/US/products/sw/voicesw/ps2237/tsd_products_support_series_home.html
- Cisco Emergency Responder 관련 설명서는 다음 URL을 참조하십시오.
  https://www.cisco.com/en/US/products/sw/voicesw/ps842/tsd_products_support_series_home.html
- Cisco 통합 IP 전화 관련 설명서는 다음 URL을 참조하십시오.
  https://www.cisco.com/en/US/products/hw/phones/ps379/tsd_products_support_series_home.html
- IP 텔레포니 네트워크 설계 및 문제 해결에 대한 자세한 내용은 *https://www.cisco.com/go/srnd*에서 Cisco IP 텔레포니 솔루션 참조 네트워크 설계 설명서를 참조하십시오

36 장

문제 해결 도구

이 섹션에서는 Unified Communications Manager 구성, 모니터링 및 문제 해결에 사용하는 도구 및 유틸리티를 설명하고, 동일한 데이터의 반복적인 테스트 및 수집을 방지하기 위해 정보 수집에 대한 일반적인 지침을 제공합니다.

참고 이 문서에 나열된 일부 URL 사이트에 액세스하려면 등록된 사용자여야 하며 로그인해야 합니다.

- Cisco 통합 서비스 가용성 문제 해결 도구, 463 페이지
- 명령줄 인터페이스, 465 페이지
- kerneldump 유틸리티, 465 페이지
- 네트워크 관리, 467 페이지
- 스니퍼 추적, 469 페이지
- 디버그, 469 페이지
- Cisco 보안 텔넷, 469 페이지
- 패킷 캡처, 470 페이지
- 일반적인 문제 해결 작업, 도구 및 명령, 476 페이지
- 문제 해결 팁, 479 페이지
- 시스템 기록 로그, 480 페이지
- 감사 로깅, 483 페이지
- Cisco Unified Communications Manager 서비스가 실행 중인지 확인, 488 페이지

Cisco 통합 서비스 가용성 문제 해결 도구

Cisco 유니파이드 Serviceability에서 다양한 Unified Communications Manager 시스템을 모니터링하고 분석할 수 있는 다음과 같은 다양한 유형의 도구에 대한 자세한 내용은 *Cisco* 통합 서비스 가용성 관리 가이드를 참조하십시오.

표 92: 서비스 가용성 도구

용어	정의
Cisco Unified Real-Time Monitoring Tool(RTMT)	이 도구는 Unified Communications Manager 장치 및 성능 카운터에 대한 실시간 정보를 제공하며 추적을 수집할 수 있습니다. 성능 카운터는 시스템 또는 Unified Communications Manager에 따라 다릅니다. 개체는 특정 장치 또는 기능(예: Cisco 통합 IP 전화 또는 Unified Communications Manager 시스템 성능)에 대한 카운터 같은 논리적 그룹을 구성합니다. 카운터는 시스템 성능에 대한 다양한 측면을 측정합니다. 카운터는 등록된 전화기 수, 시도된 통화 수 및 진행 중인 통화 수와 같은 통계를 측정합니다.
알람	관리자는 알람을 사용하여 런타임 상태 및 Unified Communications Manager 시스템의 상태를 얻습니다. 알람에는 설명 및 권장 작업 등 시스템 문제에 대한 정보가 포함되어 있습니다. 관리자는 알람 정의 데이터베이스에서 알람 정보를 검색합니다. 알람 정의에는 알람 및 권장 작업에 대한 설명이 포함되어 있습니다.
추적	관리자 및 Cisco 엔지니어가 추적 파일을 사용하여 Unified Communications Manager 서비스 문제에 대한 구체적인 정보를 얻습니다. Cisco 유니파이드 Serviceability는 구성된 추적 정보를 추적 로그 파일로 전송합니다. 두 가지 유형의 추적 로그 파일(SDI 및 SDL)이 있습니다. 모든 서비스에는 기본 추적 로그 파일이 포함됩니다. 시스템은 서비스에서 SDI(시스템 진단 인터페이스) 정보를 추적하고 런타임 이벤트 및 추적을 로그 파일로 기록합니다. SDL 추적 로그 파일에는 Cisco CallManager 및 Cisco CTIManager와 같은 서비스의 통화 처리 정보가 포함됩니다. 시스템에서 통화의 SDL(신호 디스트리뷰션 레이어)을 추적하고 상태 전환을 로그 파일에 기록합니다. 참고 대부분의 경우에는 Cisco TAC(Technical Assistance Center) 요청이 있을 때에만 SDL 추적을 수집합니다.
품질 보고서 도구	이 용어는 Cisco 유니파이드 Serviceability에서 음질 및 일반 문제 보고 유틸리티를 지정합니다.
서비스 가용성 커넥터	Cisco Webex 서비스 가용성 서비스는 Cisco 기술 지원 담당자가 인프라의 문제를 진단할 수 있는 속도를 높여줍니다. 이 서비스는 SR 케이스에서 진단 로그 및 정보의 찾기, 검색 및 저장 작업을 자동화합니다. 또한 이 서비스는 사용자 온-프레미스 장비와 관련된 문제를 효율적으로 식별하고 해결할 수 있도록 진단 서명에 대한 분석을 트리거합니다.

명령줄 인터페이스

CLI(명령줄 인터페이스)를 사용하여 기본 유지 보수 및 장애 복구를 위해 Unified Communications Manager 시스템에 액세스합니다. 유선 터미널(시스템 모니터 및 키보드)을 사용하거나 SSH 세션을 수행하여 시스템에 대한 액세스 권한을 얻습니다.

계정 이름 및 암호는 설치 시 생성됩니다. 설치 후에 암호를 변경할 수 있지만 계정 이름은 변경할 수 없습니다.

명령은 시스템에서 일부 기능을 수행하는 텍스트 명령을 나타냅니다. 명령은 독립 실행형이거나 필수 또는 선택적 인수나 옵션을 가질 수 있습니다.

수준은 명령 모음으로 구성됩니다. 예를 들어, show는 수준을 지정하는 반면, show status는 명령을 지정합니다. 각 수준 및 명령에는 연결된 권한 수준도 포함되어 있습니다. 충분한 권한 수준이 있는 경우에만 명령을 실행할 수 있습니다.

Unified Communications Manager CLI 명령에 대한 자세한 내용은 *Cisco Unified Solutions*용 명령줄 인터페이스 참조 설명서를 참조하십시오.

kerneldump 유틸리티

kerneldump 유틸리티를 사용하면 보조 서버를 요구하지 않고 영향을 받는 시스템에서 로컬로 크래시 덤프 로그를 수집할 수 있습니다.

Unified Communications Manager 클러스터에서 크래시 덤프 정보를 수집하기 전에 서버에서 kerneldump 유틸리티가 활성화되어 있어야 합니다.

참고 더 효율적인 문제 해결을 위해 Unified Communications Manager를 설치한 후 kerneldump 유틸리티가 활성화되어 있는지 확인하는 것이 좋습니다. 아직 수행하지 않은 경우, 지원되는 어플라이언스 릴리스에서 Unified Communications Manager를 업그레이드하기 전에 kerneldump 유틸리티를 활성화합니다.

중요 kerneldump 유틸리티를 활성화하거나 비활성화하면 노드를 재부팅해야 합니다. 재부팅이 허용되는 창 내에 있지 않은 경우에는 enable 명령을 실행하지 마십시오.

Cisco Unified Communications 운영 체제에 대한 CLI(명령줄 인터페이스)를 사용하여 kerneldump 유틸리티의 상태를 활성화, 비활성화 또는 확인할 수 있습니다.

다음 절차를 사용하여 커널 덤프 유틸리티를 활성화합니다.

유틸리티에서 수집한 파일을 사용하여 작업

kerneldump 유틸리티에서 충돌 정보를 보려면 *Cisco Unified Real-Time Monitoring Tool* 또는 CLI(명령줄 인터페이스)를 사용하십시오. *Cisco Unified Real-Time Monitoring Tool*를 사용하여 kerneldump 로그를 수집하려면 추적 및 로그 센트럴에서 파일 수집 옵션을 선택합니다. 시스템 서비스/애플리케이션 탭에서 Kerneldump 로그 확인란을 선택합니다. *Cisco Unified Real-Time Monitoring Tool* 사용에 대한 자세한 내용은 *Cisco Unified Real-Time Monitoring Tool* 관리 지침서를 참조하십시오.

CLI를 사용하여 kerneldump 로그를 수집하려면 충돌 디렉터리의 파일에 대한 "file" CLI 명령을 사용합니다. 이러한 항목은 "activelog" 파티션 아래에 있습니다. 로그 파일 이름은 kerneldump 클라이언트의 IP 주소로 시작하여 파일을 만든 날짜로 끝납니다. file 명령에 대한 자세한 내용은 *Cisco Unified Solutions*용 명령줄 인터페이스 설명서를 참조하십시오.

Kerneldump 유틸리티 활성화

이 절차를 사용하여 kerneldump 유틸리티를 활성화합니다. 커널 충돌이 발생하는 경우 유틸리티는 충돌을 수집하고 덤프하는 메커니즘을 제공합니다. 로컬 서버 또는 외부 서버에 로그를 덤프하도록 유틸리티를 구성할 수 있습니다.

프로시저

단계 **1** 명령줄 인터페이스에 로그인합니다.

단계 **2** 다음 중 하나를 완료합니다.

- 로컬 서버에서 커널 충돌을 덤프하려면 `utils os kerneldump enable` CLI 명령을 실행합니다.
- 외부 서버에 커널 충돌을 덤프하려면 외부 서버의 IP 주소를 사용하여 `utils os kerneldump ssh enable <ip_address>` CLI 명령을 실행합니다.

단계 **3** 서버를 재부팅합니다.

예

참고 kerneldump 유틸리티를 비활성화해야 하는 경우에는 `utils os kernelcrash disable` CLI 명령을 실행하여 코어 덤프에 대한 로컬 서버를 비활성화하고 `utils os kerneldump ssh disable <ip_address>` CLI 명령을 사용하여 외부 서버에서 유틸리티를 비활성화할 수 있습니다.

다음에 수행할 작업

Real Time Monitoring Tool에서 이메일 경고를 구성하여 코어 덤프에 대해 알려줍니다. 자세한 내용은 핵심 덤프에 대한 이메일 경고 활성화, 280 페이지을 참조하십시오.

kerneldump 유틸리티 및 문제 해결에 관한 자세한 내용은 *Cisco Unified Communications Manager*용 문제 해결 설명서를 참조하십시오.

핵심 덤프에 대한 이메일 경고 활성화

이 절차를 사용하여 핵심 덤프가 발생할 때마다 관리자에게 이메일을 보낼 수 있도록 실시간 모니터링 도구를 구성할 수 있습니다.

프로시저

단계 **1** 시스템 > 도구 > 알림 > 알림 센트럴을 선택합니다.

단계 **2** **CoreDumpFileFound** 알림을 마우스 오른쪽 버튼으로 클릭하고 알림 속성 설정을 선택합니다.

단계 **3** 마법사 프롬프트에 따라 기본 설정 기준을 설정합니다.

a) 알림 속성**:** 이메일 알림 팝업에서 이메일 활성화가 선택되어 있는지 확인하고 구성을 클릭하여 관리자에게 이메일을 보낼 기본 알림 작업을 설정합니다.

b) 프롬프트에 따라 수신자 이메일 주소를 추가합니다. 이 알림이 트리거되면 기본 동작은 이 주소로 이메일을 전송합니다.

c) 저장을 클릭합니다.

단계 **4** 기본 이메일 서버를 설정합니다.

a) 시스템 > 도구 > 알림 > 이메일 서버 구성을 선택합니다.

b) 이메일 알림을 전송하려면 이메일 서버 및 포트 정보를 입력합니다.

c) 전송 사용자 **ID**를 입력합니다.

d) 확인을 클릭합니다.

네트워크 관리

Unified Communications Manager 원격 서비스 가용성에 대한 네트워크 관리 도구를 사용합니다.

- 시스템 로그 관리
- Cisco Discovery Protocol 지원
- SNMP(Simple Network Management Protocol) 지원

자세한 내용은 이러한 네트워크 관리 도구에 대한 섹션에 제공된 URL의 설명서를 참조하십시오.

시스템 로그 관리

Cisco 시스템 로그 분석은 다른 네트워크 관리 시스템에 맞게 조정될 수 있지만, RME(Resource Manager Essentials)와 함께 패키지된 Cisco 시스템 로그 분석은 Cisco 장치에서 시스템 로그 메시지를 관리하는 최상의 방법을 제공합니다.

Cisco 시스템 로그 분석기는 여러 애플리케이션에 대한 시스템 로그의 공통된 저장 및 분석을 제공하는 Cisco 시스템 로그 분석의 구성 요소로 사용됩니다. 기타 주요 구성 요소인 시스템 로그 분석기 수집기에서 Unified Communications Manager 서버로부터 로그 메시지를 수집합니다.

이러한 두 Cisco 애플리케이션은 함께 작동하여 Cisco 통합 커뮤니케이션 솔루션에 대한 중앙 집중식 시스템 로깅 서비스를 제공합니다.

RME 설명서는 *http://www.cisco.com/en/US/products/sw/cscowork/ps2073/products_tech_note09186a00800a7275.shtml* URL을 참조하십시오.

Cisco Discovery Protocol 지원

Cisco Discovery Protocol Support를 사용하면 Unified Communications Manager 서버를 검색하고 해당 서버를 관리할 수 있습니다.

RME 설명서는 *http://www.cisco.com/en/US/products/sw/cscowork/ps2073/products_tech_note09186a00800a7275.shtml* URL을 참조하십시오.

SNMP(Simple Network Management Protocol) 지원

NMS(네트워크 관리 시스템)는 네트워크 장치 간에 관리 정보를 교환하기 위해 업계 표준 인터페이스인 SNMP를 사용합니다. TCP/IP 프로토콜의 일부로 SNMP를 사용하면 관리자가 네트워크 성능을 원격 관리하고 네트워크 문제를 찾아 해결하며 네트워크 확장을 계획할 수 있습니다.

SNMP 관리 네트워크는 관리되는 장치, 에이전트 및 네트워크 관리 시스템의 세 가지 핵심 구성 요소로 이루어집니다.

- 관리되는 장치는 SNMP 에이전트를 포함하고 관리되는 네트워크에 상주하는 네트워크 노드를 나타냅니다. 관리되는 장치는 관리 정보를 수집 및 저장하고 SNMP를 사용하여 사용할 수 있게 합니다.
- 에이전트는 관리되는 장치에 있는 네트워크 관리 소프트웨어입니다. 에이전트는 관리 정보에 대한 로컬 지식을 포함하고 이를 SNMP와 호환되는 형태로 변환합니다.
- 네트워크 관리 시스템은 SNMP 관리 애플리케이션과 해당 애플리케이션이 실행되는 시스템으로 구성됩니다. NMS는 관리되는 장치를 모니터링하고 제어하는 애플리케이션을 실행합니다. NMS는 네트워크 관리에 필요한 벌크 처리 및 메모리 리소스를 제공합니다. 다음 NMS는 Unified Communications Manager와 호환성을 공유합니다.
  - CiscoWorks 공통 서비스 소프트웨어
  - HP OpenView
  - SNMP 및 Unified Communications Manager SNMP 인터페이스를 지원하는 타사 애플리케이션

스니퍼 추적

일반적으로 문제 정보를 포함하는 VLAN 또는 포트(CatOS, Cat6K-IOS, XL-IOS)를 확장하도록 구성된 Catalyst 포트에 랩톱이나 기타 스니퍼 장착 장치를 연결하여 스니퍼 추적을 수집합니다. 사용할 수 있는 빈 포트가 없는 경우에는 스위치와 장치 사이에 삽입된 허브에 스니퍼 장착 장치를 연결합니다.

팁 TAC 엔지니어에 의한 추적 읽기 및 해석에 도움이 되도록 하려면 TAC에서 널리 사용되는 Sniffer Pro 소프트웨어를 사용하는 것이 좋습니다.

IP 전화기, 게이트웨이, Unified Communications Manager 등과 같이 관련된 모든 장비의 IP/MAC 주소를 사용할 수 있습니다.

디버그

debug특권 EXEC 명령의 출력은 프로토콜 상태 및 네트워크 활동과 관련된 다양 한 인터 네트워킹 이벤트에 대한 진단 정보를 제공합니다.

디버그 출력을 파일로 캡처할 수 있도록 터미널 에뮬레이터 소프트웨어(예: 하이퍼터미널)를 설정합니다. 하이퍼터미널에서 전환을 클릭한 다음텍스트 캡처를 클릭하고 적절한 옵션을 선택합니다.

IOS 음성 게이트웨이 디버그를 실행하기 전에 **servicetimestampsdebugdatetimemsec**가 게이트웨이에서 전역으로 구성되어 있는지 확인합니다.

참고 작업 시간 중에 라이브 환경에서 디버깅을 수집하지 않도록 하십시오.

가능하면 근무 시간이 아닐 때 디버깅을 수집하십시오. 라이브 환경에서 디버그를 수집해야 하는 경우에는 로깅 콘솔 없음 및 로깅 버퍼링됨을 구성합니다. 디버그를 수집하려면 **show log**를 사용하십시오.

일부 디버그는 시간이 오래 걸릴 수 있으므로 콘솔 포트(기본 로깅 콘솔) 또는 버퍼(로깅 버퍼)에서 직접 수집합니다. 텔넷 세션을 통해 디버그를 수집하면 장치 성능에 영향을 줄 수 있고, 결과를 다시 수집해야 하는 불완전한 디버그일 수 있습니다.

디버그를 중지하려면 **no debug all** 또는 **undebug all** 명령을 사용하십시오. **show debug** 명령을 사용하여 디버그가 꺼져 있는지 확인합니다.

Cisco 보안 텔넷

Cisco 보안 텔넷을 사용하면 Cisco Service 엔지니어(CSE) 투명 방화벽이 사이트의 Unified Communications Manager노드에 액세스할 수 있습니다. 강력한 암호화를 사용하면 *Cisco* 보안 텔넷을

사용하여 특별한 텔넷 클라이언트가 Cisco 시스템에서 방화벽 뒤에 있는 텔넷 데몬에 연결되도록 할 수 있습니다. 이 보안 연결을 사용하면 방화벽을 수정할 필요 없이 Unified Communications Manager 노드의 원격 모니터링 및 문제 해결을 수행할 수 있습니다.

참고 Cisco는 사용자의 허가가 있는 경우에만 이 서비스를 제공합니다. 프로세스를 시작하는 데 도움이 되도록 사이트에 네트워크 관리자가 있는지 확인해야 합니다.

패킷 캡처

이 섹션에는 패킷 캡처에 대한 정보가 포함되어 있습니다.

관련 항목

패킷 캡처 개요, 470 페이지
패킷 캡처를 위한 구성 검사 목록, 471 페이지
표준 패킷 스니퍼 액세스 제어 그룹에 최종 사용자 추가 , 471 페이지
패킷 캡처 서비스 매개 변수 구성, 472 페이지
전화기 구성 창에서 패킷 캡처 구성, 472 페이지
게이트웨이 및 트렁크 구성 창에서 패킷 캡처 구성, 473 페이지
패킷 캡처 구성 설정, 475 페이지
캡처된 패킷 분석, 476 페이지

패킷 캡처 개요

암호화를 활성화한 후에 미디어 및 TCP 패킷을 검사하는 타사 문제 해결 도구가 작동하지 않으므로 Unified Communications Manager를 사용하여 다음 작업을 수행하여 문제가 발생하는지 확인해야 합니다.

- Unified Communications Manager와 장치[Cisco 통합 IP 전화 (SIP 및 SCCP), Cisco IOS MGCP 게이트웨이, H.323 게이트웨이, H.323/H.245/H.225 트렁크 또는 SIP 트렁크]에서 교환되는 메시지에 대한 패킷을 분석합니다.
- 장치 간에 SRTP(Secure Real Time Protocol) 패킷을 캡처합니다.
- 메시지에서 미디어 암호화 키 자료를 추출하고 장치 간의 미디어를 해독합니다.

팁 동시에 여러 장치에 대해 이 작업을 수행하면 CPU 사용량이 많아지고 및 통화 처리 중단이 발생할 수 있습니다. 통화 처리 중단을 최소화할 수 있는 경우 이 작업을 수행하는 것이 좋습니다.

자세한 내용은 Cisco 통합 커뮤니케이션 매니저 보안 설명서를 참조하십시오.

패킷 캡처를 위한 구성 검사 목록

관련 데이터의 압축을 풀고 분석하려면 다음 작업이 포함됩니다.

절차

1. 표준 패킷 스니퍼 사용자 그룹에 최종 사용자를 추가합니다.
2. Cisco 통합 커뮤니케이션 매니저 관리의 서비스 매개 변수 구성 창에서 패킷 캡처 서비스 매개 변수를 구성합니다. 예를 들어 패킷 캡처 활성화 서비스 매개 변수를 구성합니다.
3. 전화기, 게이트웨이 또는 트렁크 구성 창에서 장치별로 패킷 캡처 설정을 구성합니다.

참고 이 작업이 네트워크에서 높은 CPU 사용량을 유발할 수 있으므로 많은 장치에 대해 동시에 패킷 캡처를 사용하도록 설정하지 않는 것이 좋습니다.

4. 영향을 받는 장치 사이에서 스니퍼 추적을 사용하여 SRTP 패킷을 캡처합니다. 스니퍼 추적 도구를 지원하는 설명서를 참조하십시오.
5. 패킷을 캡처한 후에는 패킷 캡처 활성화 서비스 매개 변수를 False로 설정합니다.
6. 패킷을 분석하는 데 필요한 파일을 수집합니다.
7. Cisco 기술 지원 센터(TAC)는 패킷을 분석합니다. 이 작업을 수행하려면 TAC에 직접 문의하십시오.

관련 항목

표준 패킷 스니퍼 액세스 제어 그룹에 최종 사용자 추가 , 471 페이지
캡처된 패킷 분석, 476 페이지
게이트웨이 및 트렁크 구성 창에서 패킷 캡처 구성, 473 페이지
전화기 구성 창에서 패킷 캡처 구성, 472 페이지
패킷 캡처 서비스 매개 변수 구성, 472 페이지
패킷 캡처 구성 설정, 475 페이지

표준 패킷 스니퍼 액세스 제어 그룹에 최종 사용자 추가

표준 패킷 스니퍼 사용자 그룹에 속하는 최종 사용자는 패킷 캡처를 지원하는 장치에 대한 패킷 캡처 모드 및 패킷 캡처 기간 설정을 구성할 수 있습니다. 사용자가 표준 패킷 스니퍼 액세스 제어 그룹에 없는 경우 사용자는 패킷 캡처를 시작할 수 없습니다.

표준 패킷 스니퍼 액세스 제어 그룹에 최종 사용자를 추가하는 방법을 설명하는 다음 절차는 Cisco 통합 커뮤니케이션 매니저 관리 지침서에 설명된 대로 최종 사용자를 Cisco 통합 커뮤니케이션 매니저 관리에서 구성한 것으로 가정합니다.

절차

1. Cisco 통합 커뮤니케이션 매니저 관리 지침서에 설명된 대로 액세스 제어 그룹을 찾습니다.
2. 찾기/나열 창이 표시 되 면 표준 패킷 스니퍼 사용자 링크를 클릭합니다.
3. 그룹에 추가 버튼을 클릭합니다.
4. Cisco 통합 커뮤니케이션 매니저 관리 지침서의 설명에 따라 최종 사용자를 추가합니다.
5. 사용자를 추가한 후 저장을 클릭합니다.

패킷 캡처 서비스 매개 변수 구성

패킷 캡처에 대한 매개 변수를 구성하려면 다음 절차를 수행합니다.

절차

1. Unified Communications Manager에서 시스템 > 서비스 매개 변수를 선택합니다.
2. 서버 드롭다운 목록 상자에서 Cisco CallManager 서비스를 활성화한 활성 서버를 선택합니다.
3. 서비스 드롭다운 목록 상자에서 **Cisco CallManager(**활성**)** 서비스를 선택합니다.
4. TLS 패킷 캡처 구성 창으로 스크롤하고 패킷 캡처 설정을 구성합니다.

팁 서비스 매개 변수에 대한 정보를 보려면 매개 변수 이름을 클릭하거나 창에 표시되는 물음표를 클릭합니다.

참고 패킷 캡처가 발생하려면 패킷 캡처 활성화 서비스 매개 변수를 True로 설정해야 합니다.

5. 변경 사항을 적용하려면 저장을 클릭합니다.
6. 계속해서 패킷 캡처를 구성할 수 있습니다.

관련 항목

게이트웨이 및 트렁크 구성 창에서 패킷 캡처 구성, 473 페이지
전화기 구성 창에서 패킷 캡처 구성, 472 페이지

전화기 구성 창에서 패킷 캡처 구성

서비스 매개 변수 창에서 패킷 캡처를 활성화한 후에는 Cisco 통합 커뮤니케이션 매니저 관리의 전화기 구성 창에서 장치별로 패킷 캡처를 구성할 수 있습니다.

패킷 캡처를 전화기별로 활성화하거나 비활성화할 수 있습니다. 패킷 캡처의 기본 설정은 없음입니다.

주의 이 작업이 네트워크에서 높은 CPU 사용량을 유발할 수 있으므로 많은 전화기에 대해 동시에 패킷 캡처를 사용하도록 설정하지 않는 것이 좋습니다.

패킷을 캡처하지 않으려거나 작업을 완료한 경우 패킷 캡처 활성화 서비스 매개 변수를 False로 설정합니다.

전화기에 대해 패킷 캡처에 대한 매개 변수를 구성하려면 다음 절차를 수행합니다.

절차

1. 패킷 캡처 설정을 구성하기 전에 패킷 캡처 구성과 관련된 주제를 참조하십시오.
2. Cisco 통합 커뮤니케이션 매니저 시스템 구성 설명서에 설명된 대로 SIP 또는 SCCP 전화기를 찾습니다.
3. 전화기 구성 창이 표시되면 패킷 캡처 구성 설정에 설명된 대로 문제 해결 설정을 구성합니다.
4. 구성을 완료한 후에 저장을 클릭합니다.
5. 재설정 대화 상자에서 확인을 클릭합니다.

팁 Cisco 통합 커뮤니케이션 매니저 관리에 장치를 재설정하라는 메시지가 표시되지만 패킷을 캡처하기 위해 장치를 재설정할 필요는 없습니다.

추가 단계

영향을 받는 장치 사이에서 스니퍼 추적을 사용하여 SRTP 패킷을 캡처합니다.

패킷을 캡처한 후에는 패킷 캡처 활성화 서비스 매개 변수를 False로 설정합니다.

관련 항목

캡처된 패킷 분석, 476 페이지
패킷 캡처를 위한 구성 검사 목록, 471 페이지

게이트웨이 및 트렁크 구성 창에서 패킷 캡처 구성

다음 게이트웨이및 트렁크는 Unified Communications Manager에서 패킷 캡처를 지원합니다.

- Cisco IOS MGCP 게이트웨이
- H.323 게이트웨이
- H.323/H.245/H.225 트렁크
- SIP 트렁크

팁 이 작업이 네트워크에서 높은 CPU 사용량을 유발할 수 있으므로 많은 장치에 대해 동시에 패킷 캡처를 사용하도록 설정하지 않는 것이 좋습니다.

패킷을 캡처하지 않으려거나 작업을 완료한 경우 패킷 캡처 활성화 서비스 매개 변수를 False로 설정합니다.

게이트웨이 또는 트렁크 구성 창에서 패킷 캡처 설정을 구성하려면 다음 절차를 수행합니다.

절차

1. 패킷 캡처 설정을 구성하기 전에 패킷 캡처 구성과 관련된 주제를 참조하십시오.
2. 다음 작업 중 하나를 수행합니다.
   - Cisco 통합 커뮤니케이션 매니저 시스템 구성 설명서에 설명된 대로 Cisco IOS MGCP 게이트웨이를 찾습니다.
   - Cisco 통합 커뮤니케이션 매니저 시스템 구성 설명서에 설명된 대로 H.323 게이트웨이를 찾습니다.
   - Cisco 통합 커뮤니케이션 매니저 시스템 구성 설명서에 설명된 대로 H.323/H.245/H.225 트렁크를 찾습니다.
   - Cisco 통합 커뮤니케이션 매니저 시스템 구성 설명서에 설명된 대로 SIP 트렁크를 찾습니다.
3. 구성 창이 표시되면 패킷 캡처 모드 및 패킷 캡처 기간 설정을 찾습니다.

팁 Cisco IOS MGCP 게이트웨이를 찾은 경우 Cisco 통합 커뮤니케이션 매니저 관리 지침서에 설명된 대로 Cisco IOS MGCP 게이트웨이에 대한 포트를 구성했는지 확인합니다. Cisco IOS MGCP 게이트웨이에 대한 패킷 캡처 설정은 엔드포인트 ID에 대한 게이트웨이 구성 창에 표시됩니다. 이 창에 액세스하려면 음성 인터페이스 카드의 엔드포인트 ID를 클릭합니다.

4. 패킷 캡처 구성 설정에 설명된 대로 문제 해결 설정을 구성합니다.
5. 패킷 캡처 설정을 구성한 후에는 저장을 클릭합니다.
6. 재설정 대화 상자에서 확인을 클릭합니다.

팁 Cisco 통합 커뮤니케이션 매니저 관리에 장치를 재설정하라는 메시지가 표시되지만 패킷을 캡처하기 위해 장치를 재설정할 필요는 없습니다.

추가 단계

영향을 받는 장치 사이에서 스니퍼 추적을 사용하여 SRTP 패킷을 캡처합니다.

패킷을 캡처한 후에는 패킷 캡처 활성화 서비스 매개 변수를 False로 설정합니다.

관련 항목

캡처된 패킷 분석, 476 페이지
패킷 캡처를 위한 구성 검사 목록, 471 페이지

패킷 캡처 구성 설정

다음 표에서는 게이트웨이, 트렁크 및 전화기에 대한 패킷 캡처를 구성할 때 패킷 캡처 모드 및 패킷 캡처 기간 설정에 대해 설명합니다.

설정	설명
패킷 캡처 모드	이 설정은 암호화 문제를 해결하기 위해서만 존재합니다. 패킷을 캡처하면 CPU 사용량이 많아지거나 통화 처리가 중단될 수 있습니다. 드롭다운 목록 상자에서 다음 옵션 중 하나를 선택합니다. • 없음 - 기본 설정으로 사용되는 이 옵션은 패킷 캡처가 발생하지 않음을 나타냅니다. 패킷 캡처를 완료한 후 Unified Communications Manager는 패킷 캡처 모드를 없음으로 설정합니다. • 배치 처리 모드 - Unified Communications Manager이 해독되었거나 암호화되지 않은 메시지를 파일로 작성하고 각 파일이 시스템에서 암호화됩니다. 시스템에서는 매일 새 암호화 키를 사용하여 새 파일을 작성합니다. Unified Communications Manager>이 파일을 7일 동안 저장하며, 파일을 암호화하는 키도 안전한 위치에 저장합니다. Unified Communications Manager은 파일을 PktCap 가상 디렉토리에 저장합니다. 단일 파일에는 타임스탬프, 소스 IP 주소, 소스 IP 포트, 대상 IP 주소, 패킷 프로토콜, 메시지 길이 및 메시지가 있습니다. TAC 디버깅 도구에서는 HTTPS, 관리자 사용자 이름 및 암호, 그리고 캡처된 패킷이 포함된 단일의 암호화된 파일을 요청하도록 지정된 날짜를 사용합니다. 마찬가지로, 도구는 암호화된 파일의 암호를 해독하기 위한 키 정보를 요청합니다. 팁 TAC를 연결하기 전에 영향을 받는 장치 사이에서 스니퍼 추적을 사용하여 SRTP 패킷을 캡처해야 합니다.
패킷 캡처 지속 시간	이 설정은 암호화 문제를 해결하기 위해서만 존재합니다. 패킷을 캡처하면 CPU 사용량이 많아지거나 통화 처리가 중단될 수 있습니다. 이 필드에서는 패킷 캡처 세션 하나에 할당한 최대 시간(분)을 세션을 지정합니다. 범위는 0~300분이며 기본 설정은 0입니다. 패킷 캡처를 시작하려면 필드에 0 이외의 다른 값을 입력합니다. 패킷 캡처가 완료되면 값 0이 표시됩니다.

관련 항목

게이트웨이 및 트렁크 구성 창에서 패킷 캡처 구성, 473 페이지

전화기 구성 창에서 패킷 캡처 구성, 472 페이지

캡처된 패킷 분석

Cisco 기술 지원 센터(TAC)는 디버깅 도구를 사용하여 패킷을 분석합니다. TAC를 연결하기 전에 영향을 받는 장치 사이에서 스니퍼 추적을 사용하여 SRTP 패킷을 캡처합니다. 다음 정보를 수집한 후에는 직접 TAC에 문의하십시오.

- 패킷 캡처 파일—**https://<IP address or server name>/pktCap/pktCap.jsp?file=mm-dd-yyyy.pkt**, 여기서 서버를 탐색하여 월, 일 및 연도(mm-dd-yyyy)로 패킷 캡처 파일을 찾습니다.
- 파일에 대한 키—**https://<IP address or server name>/pktCap/pktCap.jsp?key=mm-dd-yyyy.pkt**, 여기서 서버를 탐색하여 월, 일 및 연도(mm-dd-yyyy)로 키를 찾습니다.
- 표준 패킷 스니퍼 사용자 그룹에 속한 최종 사용자의 사용자 이름 및 암호

자세한 내용은 Cisco 통합 커뮤니케이션 매니저 보안 설명서의 내용을 참조하십시오.

일반적인 문제 해결 작업, 도구 및 명령

이 섹션에서는 루트 액세스가 비활성화된 Unified Communications Manager 서버를 문제 해결하는 데 도움이 되는 명령 및 유틸리티에 대한 빠른 참조를 제공합니다. 다음 표에서는 여러 가지 시스템 문제를 해결하기 위한 정보를 수집하는 데 사용할 수 있는 CLI 명령 및 GUI 선택 사항에 대한 요약을 제공합니다.

표 ***93: CLI*** 명령 및 ***GUI*** 선택 사항 요약

정보	**Linux** 명령	서비스 가용성 **GUI** 도구	**CLI** 명령
CPU 사용량	위쪽	RTMT 보기 탭으로 이동하고 서버 > **CPU** 및 메모리를 선택합니다.	프로세서 CPU 사용량: show perf query class Processor 모든 프로세스에 대한 프로세스 CPU 사용량: show perf query counter Process “% CPU Time” 개별 프로세스 카운터 세부 정보(CPU 사용량 포함) show perf query instance <Process task_name>
프로세스 상태	ps	RTMT 보기 탭으로 이동하고 서버 > 프로세스를 선택합니다.	show perf query counter Process “Process Status”
디스크 사용량	df/du	RTMT 보기 탭으로 이동하고 서버 > 디스크 사용량 을 선택합니다	show perf query counter Partition“% Used” 또는 show perf query class Partition

정보	**Linux** 명령	서비스 가용성 **GUI** 도구	**CLI** 명령
메모리	free	RTMT 보기 탭으로 이동하고 서버 > **CPU** 및 메모리를 선택합니다.	show perf query class Memory
네트워크 상태	netstats		show network status
서버 재부팅	reboot	서버에서 플랫폼 웹 페이지에 로그인 서버 > 현재 버전으로 이동	utils system restart
추적/로그 수집	Sftp, ftp	RTMT 도구 탭으로 이동하고 추적 > 추적 및 로그 센트럴 을 선택합니다	파일 나열: file list 파일 다운로드: file get 파일 보기: file view

다음 표에서는 이러한 문제를 해결하는 데 사용할 수 있는 일반적인 문제 및 도구 목록을 제공합니다.

표 ***94: CLI*** 명령 및 ***GUI*** 선택과 관련된 일반적인 문제 해결

작업	**GUI** 도구	**CLI** 명령
데이터베이스 액세스	none	관리자로 로그인하고 다음 표시 **show** 중 하나를 사용합니다. • show tech database • show tech dbinuse • show tech dbschema • show tech devdefaults • show tech gateway • show tech locales • show tech notify • show tech procedures • show tech routepatterns • show tech routeplan • show tech systables • show tech table • show tech triggers • show tech version • show tech params* SQL 명령을 실행하려면 **run** 명령을 사용합니다. • run sql <sql command>
디스크 공간 확보 참고 로그 파티션에서 파일만 삭제할 수 있습니다.	RTMT 클라이언트 애플리케이션을 사용하여 도구 탭으로 이동하고 추적 및 로그 센트럴 > 파일 수집을 선택합니다. 기준을 선택하여 수집할 파일을 선택한 다음 파일 삭제 옵션을 선택합니다. 이렇게 하면 PC에 파일을 다운로드한 후 Unified Communications Manager 서버에서 파일이 삭제됩니다.	file delete

작업	**GUI** 도구	**CLI** 명령
코어 파일 보기	코어 파일은 볼 수 없습니다. 그러나 RTMT 애플리케이션을 사용하고 추적 및 로그 센트럴 > 크래시 덤프 수집을 선택하여 코어 파일을 다운로드할 수 있습니다.	utils core [옵션]
Unified Communications Manager 서버 재부팅	서버의 플랫폼에 로그인하고 재시작 > 현재 버전으로 이동합니다.	utils system restart
추적에 대한 디버그 수준 변경	`https://<server_ipaddress>:8443/ccmservice/`의 *Cisco Unity Connection* 서비스 가용성 관리에 로그인하고 추적 > 구성을 선택합니다.	set trace enable [Detailed, Significant, Error, Arbitrary, Entry_exit, State_Transition, Special] [syslogmib, cdpmib, dbl, dbnotify]
netstats 보기	none	show network status

문제 해결 팁

Unified Communications Manager의 문제를 해결할 때 다음 팁이 도움이 될 수 있습니다.

팁 Unified Communications Manager의 릴리스 노트에서 알려진 문제를 확인합니다. 릴리스 노트는 알려진 문제에 대한 설명 및 해결 방법을 제공합니다.

팁 장치가 등록된 위치를 파악합니다.

각 Unified Communications Manager 로그는 로컬로 파일을 추적합니다. 전화기 또는 게이트웨이가 특정 Unified Communications Manager에 등록된 경우 통화가 시작되면 해당 Unified Communications Manager에서 통화 처리가 완료됩니다. 문제를 디버깅하려면 해당 Unified Communications Manager에서 추적을 캡처해야 합니다.

일반적인 실수는 가입자 서버에 등록되었지만 게시자 서버에서 추적을 캡처하는 장치를 포함하는 것입니다. 이러한 추적 파일은 거의 비어 있습니다(분명히 서로 간에 통화는 없는 것임).

또 다른 일반적인 문제는 장치 1을 CM1에 등록하고 장치 2를 CM2에 등록하는 것입니다. 장치 1이 장치 2에 전화를 걸 경우 통화 추적은 CM1에서 발생하고, 장치 2가 장치 1에 전화를 걸면 CM2에서 추적이 발생합니다. 양방향 통화 문제를 해결하는 경우 두 Unified Communications Manager의 두 추적 모두에서 문제 해결에 필요한 모든 정보를 수집해야 합니다.

팁 문제의 대략적인 시간을 파악합니다.

여러 통화가 발생했을 수 있으므로 통화의 대략적인 시간을 알고 있으면 TAC가 신속하게 문제를 찾을 수 있습니다.

활성 통화 중에 **i** 또는 **?** 버튼을 두 번 눌러 Cisco 통합 IP 전화 79xx에서 전화 통계를 얻을 수 있습니다.

문제를 재현하고 정보를 생성하는 테스트를 실행하는 경우 문제를 이해하는 데 중요한 다음 데이터를 알고 있어야 합니다.

- 호출한 번호/호출된 번호
- 특정 시나리오에 관련된 기타 번호
- 통화 시간

참고 문제 해결을 위해서는 모든 장비의 시간 동기화가 중요하다는 점을 기억하십시오.

문제를 재현하는 경우 파일의 수정 날짜와 타임스탬프를 확인하여 해당 시간대에 대한 파일을 선택해야 합니다. 적절한 추적을 수집하는 가장 좋은 방법은 문제를 재현한 다음 가장 최근 파일을 신속하게 찾아서 Unified Communications Manager 서버에서 복사하는 것입니다.

팁 로그 파일을 덮어쓰지 않도록 저장합니다.

잠시 후 파일을 덮어씁니다. 파일이 기록되고 있는지 확인하는 유일한 방법은 메뉴 모음에서 보기 > 새로 고침을 선택하고 파일의 날짜 및 시간을 확인하는 것입니다.

시스템 기록 로그

이 시스템 기록 로그는 초기 시스템 설치, 시스템 업그레이드, Cisco 옵션 설치 및 DRS 백업과 DRS 복원에 대한 간략한 개요와 스위치 버전 및 재부팅 기록을 제공하기 위한 중앙 위치를 제공합니다.

관련 항목

시스템 기록 로그 개요, 480 페이지
시스템 기록 로그 필드, 481 페이지
시스템 기록 로그 액세스, 482 페이지

시스템 기록 로그 개요

시스템 기록 로그는 간단한 ASCII 파일인 **system-history.log**로 존재하며 데이터베이스에서 데이터가 유지 관리되지 않습니다. 과도하게 커지지 않으므로 시스템 기록 파일은 회전되지 않습니다.

시스템 기록 로그는 다음과 같은 기능을 제공합니다.

- 서버에 초기 소프트웨어 설치를 기록합니다.
- 모든 소프트웨어 업그레이드의 성공, 실패 또는 취소(Cisco 옵션 파일 및 패치)를 기록합니다.
- 수행되는 모든 DRS 백업 및 복원을 기록합니다.
- CLI 또는 GUI를 통해 발생한 스위치 버전의 모든 호출을 기록합니다.
- CLI 또는 GUI를 통해 발생한 재시작 및 종료에 대한 모든 호출을 기록합니다.
- 시스템의 모든 부팅을 기록합니다. 다시 시작 또는 종료 항목과 관련되지 않은 경우 부팅은 수동 재부팅, 전원 사이클 또는 커널 비상의 결과입니다.
- 초기 설치 이후 또는 기능 사용 가능 시간 이후 시스템 기록을 포함하는 단일 파일을 유지 관리합니다.
- 설치 폴더에 있습니다. **file** 명령 또는 Real Time Monitoring Tool을 사용하여 CLI에서 로그에 액세스할 수 있습니다.

시스템 기록 로그 필드

로그에는 제품 이름, 제품 버전 및 커널 이미지에 대한 정보가 포함된 일반 헤더가 표시됩니다. 예를 들어:

==========

제품 이름 - Unified Communications Manager

제품 버전 - 7.1.0.39000-9023

커널 이미지 - 2.6.9-67.EL

==========

각 시스템 기록 로그 항목에는 다음 필드가 포함되어 있습니다.

타임스탬프 사용자 *ID* 작업 설명 시작/결과

시스템 기록 로그 필드에는 다음 값이 포함될 수 있습니다.

- 타임스탬프 - *mm/dd/yyyy hh:mm:ss* 형식으로 서버의 로컬 시간과 날짜를 표시합니다.
- 사용자 *ID* - 작업을 호출하는 사용자의 사용자 이름을 표시합니다.
- 작업 - 다음 작업 중 하나를 표시합니다.
  - 설치
  - Windows 업그레이드
  - 설치 중 업그레이드
  - 업그레이드
  - Cisco 옵션 설치

- 버전 전환
- 시스템 재시작
- 종료
- 부팅
- DRS 백업
- DRS 복원

- 설명 - 다음 메시지 중 하나를 표시합니다.
  - 버전: 기본 설치, Windows 업그레이드, 설치 중 업그레이드 및 업그레이드 작업의 경우 표시됩니다.
  - *Cisco* 옵션 파일 이름: Cisco 옵션 설치 작업의 경우 표시됩니다.
  - 타임스탬프: DRS 백업 및 DRS 복원 작업의 경우 표시됩니다.
  - 활성 버전에서 비활성 버전으로: 버전 전환 작업의 경우 표시됩니다.
  - 활성 버전: 시스템 재시작, 종료 및 부팅 작업의 경우 표시됩니다.
- 결과 - 다음과 같은 결과를 표시합니다.
  - 시작
  - 성공 또는 실패
  - 중단

다음은 시스템 기록 로그의 샘플입니다.

```
admin:file dump install system-history.log=======================================
 Product Name - Cisco Unified Communications Manager Product Version -
6.1.2.9901-117 Kernel Image - 2.4.21-47.EL.cs.3BOOT
======================================= 07/25/2008 14:20:06 | root: Install
6.1.2.9901-117 Start 07/25/2008 15:05:37 | root: Install 6.1.2.9901-117 Success
07/25/2008 15:05:38 | root: Boot 6.1.2.9901-117 Start 07/30/2008 10:08:56 | root:
 Upgrade 6.1.2.9901-126 Start 07/30/2008 10:46:31 | root: Upgrade 6.1.2.9901-126
 Success 07/30/2008 10:46:43 | root: Switch Version 6.1.2.9901-117 to
6.1.2.9901-126 Start 07/30/2008 10:48:39 | root: Switch Version 6.1.2.9901-117
to 6.1.2.9901-126 Success 07/30/2008 10:48:39 | root: Restart 6.1.2.9901-126 Start
 07/30/2008 10:51:27 | root: Boot 6.1.2.9901-126 Start 08/01/2008 16:29:31 | root:
 Restart 6.1.2.9901-126 Start 08/01/2008 16:32:31 | root: Boot 6.1.2.9901-126
Start
```

시스템 기록 로그 액세스

CLI 또는 RTMT를 사용하여 시스템 기록 로그에 액세스할 수 있습니다.

CLI 사용

CLI **file** 명령을 사용하여 시스템 기록 로그에 액세스할 수 있습니다. 예를 들면 다음과 같습니다.

- **file view install system-history.log**
- **file get install system-history.log**

CLI **file** 명령에 대한 자세한 내용은 *Cisco Unified Solutions*용 명령줄 인터페이스 참조 설명서를 참조하십시오.

RTMT 사용

RTMT를 사용하여 시스템 기록 로그에 액세스할 수도 있습니다. 추적 및 로그 센트럴 탭에서 설치 로그 수집을 선택합니다.

RTMT 사용에 대한 자세한 내용은 *Cisco Unified Real-Time Monitoring Tool* 관리 지침서를 참조하십시오.

감사 로깅

중앙 집중식 감사 로깅을 통해 Unified Communications Manager 시스템에 대한 구성 변경 사항이 감사를 위해 개별 로그 파일에 기록됩니다. 감사 이벤트는 로깅해야 하는 이벤트를 나타냅니다. 다음 Unified Communications Manager 구성 요소는 감사 이벤트를 생성합니다.

- Cisco 통합 커뮤니케이션 매니저 관리
- Cisco 유니파이드 Serviceability
- *Unified Communications Manager CDR Analysis and Reporting*
- *Cisco Unified Real-Time Monitoring Tool*
- *Cisco Unified Communications* 운영 체제
- 재해 복구 시스템
- 데이터베이스
- 명령줄 인터페이스
- 원격 지원 계정 활성화됨(기술 지원 팀에서 CLI 명령을 실행함)

*Cisco Business Edition 5000*에서 다음 Cisco Unity Connection 구성 요소는 감사 이벤트도 생성합니다.

- Cisco Unity Connection 관리
- *Cisco Personal Communications Assistant*(Cisco PCA)
- Cisco Unity Connection 서비스 가용성
- Cisco Unity Connection REST(Representational State Transfer) API를 사용하는 클라이언트

다음 예는 샘플 감사 이벤트를 표시합니다.

```
CCM_TOMCAT-GENERIC-3-AuditEventGenerated: Audit Event Generated
UserID:CCMAdministrator Client IP Address:172.19.240.207 Severity:3
EventType:ServiceStatusUpdated ResourceAccessed: CCMService EventStatus:Successful
 Description: Call Manager Service status is stopped App ID:Cisco Tomcat Cluster
 ID:StandAloneCluster Node ID:sa-cm1-3
```

감사 이벤트에 대한 정보가 포함된 감사 로그는 일반 파티션에 기록됩니다. LPM(로그 파티션 모니터)은 추적 파일처럼 필요에 따라 이러한 감사 로그의 제거를 관리합니다. 기본적으로 LPM은 감사 로그를 제거하지만 감사 사용자는 Cisco 유니파이드 Serviceability의 감사 사용자 구성 창에서 이 설정을 변경할 수 있습니다. LPM은 공통 파티션 디스크 사용량이 임계값을 초과할 때마다 경고를 전송합니다. 그러나 경고에는 감사 로그 또는 추적 파일로 인해 디스크가 꽉 찼는지 여부에 대한 정보가 없습니다.

팁 감사 로깅을 지원하는 네트워크 서비스인 Cisco 감사 이벤트 서비스는 Cisco 유니파이드 Serviceability의 제어 센터에 - 네트워크 서비스에 표시됩니다. 감사 로그가 기록되지 않은 경우 Cisco 유니파이드 Serviceability에서 도구 > 제어 센터 - 네트워크 서비스를 선택하여 이 서비스를 중지하고 시작합니다.

모든 감사 로그는 *Cisco Unified Real-Time Monitoring Tool*의 추적 및 로그 센트럴에서 수집, 보고 및 삭제됩니다. 추적 및 로그 센트럴에서 RTMT의 감사 로그에 액세스합니다. 시스템 > 실시간 추적 > 감사 로그 > 노드로 이동합니다. 노드를 선택하면 다른 창에시스템 > **Cisco** 감사 로그가 표시됩니다.

RTMT에 표시되는 감사 로그 유형은 다음과 같습니다.

- 애플리케이션 로그
- 데이터베이스 로그
- 운영 체제 로그
- 원격 SupportAccEnabled 로그

애플리케이션 로그

RTMT의 AuditApp 폴더에 표시되는 애플리케이션 감사 로그는 Cisco 통합 커뮤니케이션 매니저 관리, Cisco 유니파이드 Serviceability, *CLI*, *Cisco Unified Real-Time Monitoring Tool*(RTMT), 재해 복구 시스템 및 Cisco Unified CDR Analysis and Reporting(CAR)에 대한 구성 변경 사항을 제공합니다. *Cisco Business Edition 5000*의 경우 애플리케이션 감사 로그는 Cisco Unity Connection 관리, *Cisco Personal Communications Assistant*(Cisco PCA), Cisco Unity Connection 서비스 가용성 및 REST(Representational State Transfer) API를 사용하는 클라이언트에 대한 변경 사항을 기록합니다.

애플리케이션 로그는 기본적으로 활성화되어 있지만 도구 > 감사 로그 구성을 선택하여 Cisco 유니파이드 Serviceability에서 구성할 수 있습니다. 감사 로그 구성을 위해 구성할 수 있는 설정에 대한 설명은 *Cisco* 통합 서비스 가용성 관리 가이드를 참조하십시오.

Cisco 유니파이드 Serviceability에서 감사 로그를 비활성화하면 새 감사 로그 파일이 생성되지 않습니다.

팁 감사 역할이 있는 사용자만 감사 로그 설정을 변경할 수 있습니다. 기본적으로 CCMAdministrator는 새로 설치하고 업그레이드한 후 감사 역할을 소유합니다. CCMAdministrator는 CCMAdministrator가 감사 목적으로 생성하는 새 사용자에게 "표준 감사 사용자" 그룹을 할당할 수 있습니다. 그런 다음 감사 사용자 그룹에서 CCMAdministrator를 제거할 수 있습니다. "표준 감사 로그 구성" 역할은 감사 로그를 삭제하고 *Cisco Unified Real-Time Monitoring Tool*, 추적 수집 도구, RTMT 알림 구성, 제어 센터 - 네트워크 서비스 창, RTMT 프로파일 저장, 감사 구성 창 및 감사 추적이라고 하는 새로운 리소스에 대한 읽기/업데이트 액세스 기능을 제공하는 것입니다. *Cisco Business Edition 5000*에서 Cisco Unity Connection의 경우 설치 중에 생성된 애플리케이션 관리 계정에 감사 관리자 역할이 있으며 역할에 다른 관리 사용자를 할당할 수 있습니다.

Unified Communications Manager 구성된 최대 파일 크기에 도달할 때까지 하나의 애플리케이션 감사 로그 파일을 생성합니다. 그런 다음 새 애플리케이션 감사 로그 파일을 닫고 생성합니다. 시스템에서 로그 파일을 회전하도록 지정하는 경우 Unified Communications Manager는 구성된 수의 파일을 저장합니다. 일부 로깅 이벤트는 RTMT SyslogViewer를 사용하여 볼 수 있습니다.

다음과 같은 이벤트가 Cisco 통합 커뮤니케이션 매니저 관리의 로그에 기록 됩니다.

- 사용자 로깅(사용자 로그인 및 사용자 로그아웃)
- 사용자 역할 구성원 자격 업데이트(사용자 추가, 사용자 삭제, 사용자 역할 업데이트됨)
- 역할 업데이트(새 역할이 추가, 삭제 또는 업데이트됨)
- 장치 업데이트(전화기 및 게이트웨이)
- 서버 구성 업데이트(알람 또는 추적 구성, 서비스 매개 변수, 엔터프라이즈 매개 변수, IP 주소, 호스트 이름, 이더넷 설정, Unified Communications Manager 서버 추가 또는 삭제에 대한 변경)

다음과 같은 이벤트가 Cisco 유니파이드 Serviceability의 로그에 기록 됩니다.

- 서비스 가용성 창에서 서비스 활성화, 비활성화, 시작 또는 중지
- 추적 구성 및 알람 구성 변경.
- SNMP 구성의 변경.
- CDR 관리의 변경.
- 서비스 가용성 보고서 아카이브의 보고서를 검토합니다. 리포터 노드에서 이 로그를 봅니다.

RTMT가 감사 이벤트 알람을 사용하여 다음 이벤트를 기록합니다.

- 알림 구성
- 알림 일시 중지
- 이메일 구성
- 노드 알림 상태 설정
- 알림 추가

- 알림 작업 추가
- 알림 지우기
- 알림 활성화
- 알림 작업 제거
- 알림 제거

*Unified Communications Manager CDR Analysis and Reporting*에 대해 다음 이벤트가 기록됩니다.

- CDR 로더 일정 조정
- 일별, 주별 및 월별 사용자 보고서, 시스템 보고서 및 장치 보고서의 일정을 조정합니다.
- 메일 매개 변수 구성
- 다이얼 플랜 구성
- 게이트웨이 구성
- 시스템 환경설정 구성
- 자동 삭제 구성
- 기간, 시간 및 음성 품질에 대한 등급 엔진 구성
- QoS 구성
- 미리 작성된 보고서 구성에 대한 자동 생성/알림
- 알림 제한 구성

재해 복구 시스템에 대해 다음과 같은 이벤트가 기록됩니다.

- 백업 시작/실패
- 복원 시작/실패
- 백업 취소
- 백업 완료/실패
- 복원 완료/실패
- 백업 일정 저장/업데이트/삭제/활성화 또는 비활성화
- 백업용 대상 장치 저장/업데이트/삭제

*Cisco Business Edition 5000*의 경우 Cisco Unity Connection 관리에서는 다음 이벤트를 기록합니다.

- 사용자 로깅(사용자 로그인 및 사용자 로그아웃)
- 모든 구성 변경 사항(다음을 포함하되 이에 제한되지 않음: 사용자, 연락처, 통화 관리 개체, 네트워킹, 시스템 설정 및 전화 통신)

- 작업 관리(작업 활성화 또는 비활성화)
- 벌크 관리 도구(벌크 생성, 벌크 삭제)
- 사용자 정의 키패드 맵(맵 업데이트)

*Cisco Business Edition 5000*의 경우 Cisco PCA는 다음 이벤트를 기록합니다.

- 사용자 로깅(사용자 로그인 및 사용자 로그아웃)
- Messaging Assistant를 통해 이루어진 모든 구성 변경

*Cisco Business Edition 5000*의 경우 Cisco Unity Connection 서비스 가용성은 다음 이벤트를 기록합니다.

- 사용자 로깅(사용자 로그인 및 사용자 로그아웃)
- 모든 구성이 변경됩니다.
- 서비스 활성화, 비활성화, 시작 또는 중지.

*Cisco Business Edition 5000*의 경우 REST API를 사용하는 클라이언트는 다음 이벤트를 기록합니다.

- 사용자 로깅(사용자 API 인증).
- Cisco Unity Connection 프로비저닝 인터페이스(CUPI)를 이용하는 API 통화

데이터베이스 로그

RTMT의 informix 폴더에 표시되는 데이터베이스 감사 로그는 데이터베이스 변경 사항을 보고합니다. 기본적으로 활성화되지 않는 이 로그는 도구 > 감사 로그 구성을 선택하여 Cisco 유니파이드 Serviceability에서 구성됩니다. 감사 로그 구성에 대해 구성할 수 있는 설정에 대한 설명은 Cisco 유니파이드 Serviceability의 내용을 참조하십시오.

이 감사는 데이터베이스 변경 사항을 기록하고 애플리케이션 감사 로그 애플리케이션 구성이 변경되기 때문에 애플리케이션 감사와는 다릅니다. 데이터베이스 감사가 Cisco 유니파이드 Serviceability에서 활성화되지 않은 경우에는 informix 폴더가 RTMT에 표시되지 않습니다.

운영 체제 로그

RTMT의 vos 폴더에 표시되는 운영 체제 감사 로그는 운영 체제에 의해 트리거되는 이벤트를 보고합니다. 이 로그는 기본적으로 활성화되지 않습니다. **utils auditd** CLI 명령은 이벤트를 활성화, 비활성화 또는 상태를 제공합니다.

CLI에서 감사가 활성화되지 않은 경우에는 vos 폴더가 RTMT에 표시되지 않습니다.

CLI에 대한 자세한 내용은 *Cisco Unified Solutions*용 명령줄 인터페이스 설명서를 참조하십시오.

원격 지원 계정 활성화 로그

RTMT의 vos 폴더에 표시되는 원격 지원 계정 활성화 감사 로그는 기술 지원 팀이 실행한 CLI 명령을 보고합니다. 이 로그는 구성할 수 없으며, 기술 지원 팀에서 원격 지원 계정 설정을 활성화한 경우에만 로그가 생성됩니다.

Cisco Unified Communications Manager 서비스가 실행 중인지 확인

다음 절차를 사용하여 서버에서 활성 상태인 Cisco CallManager 서비스를 확인합니다.

절차

1. Cisco 통합 커뮤니케이션 매니저 관리에서탐색 > **Cisco** 통합 서비스 가용성을 선택합니다.
2. 도구 > 서비스 활성화를 선택합니다.
3. 서버 열에서 원하는 서버를 선택합니다.

   선택하는 서버는 현재 서버 제목 옆에 표시되고, 구성된 서비스가 있는 일련의 상자가 표시됩니다.

   활성화 상태 열은 Cisco CallManager 회선에서 활성화 또는 비활성화 상태를 표시합니다.

   활성화됨 상태가 표시되면 지정된 Cisco 콜매니저 서비스는 선택한 서버에서 활성 상태로 유지됩니다.

   비활성화됨 상태가 표시되면 다음 단계를 계속합니다.
4. 원하는 Cisco 콜매니저 서비스에 대한 확인란을 선택합니다.
5. 업데이트 버튼을 클릭합니다.

   활성화 상태 열이 지정된 Cisco 콜매니저 서비스 회선에서 활성화도됨을 표시합니다.

   이제 지정된 서비스가 선택한 서버에 대해 활성화된 것으로 표시됩니다.

Cisco 콜매니저 서비스가 활성화되어 있고 서비스가 현재 실행 중인지 확인하려는 경우 다음 절차를 수행합니다.

절차

1. Cisco 통합 커뮤니케이션 매니저 관리에서탐색 > **Cisco** 통합 서비스 가용성을 선택합니다.

   Cisco 통합 서비스 가용성 창이 표시됩니다.
2. 도구 > 제어 센터 - 기능 서비스를 선택합니다.
3. 서버 열에서 서버를 선택합니다.

   선택하는 서버는 현재 서버 제목 옆에 표시되고, 구성된 서비스가 있는 상자가 표시됩니다.

상태 열에 선택한 서버에 대해 실행 중인 서비스가 표시됩니다.

37 장

TAC를 사용하여 케이스 열기

이 섹션에서는 TAC 및 TAC 직원과 공유하는 방법에 대한 정보를 제공하는 데 필요한 정보 유형에 대한 세부 정보를 제공합니다.

유효한 Cisco 서비스 계약을 맺은 모든 고객, 파트너, 리셀러 및 유통업체의 경우 Cisco 기술 지원 부서는 하루 24시간, 수상 경력에 빛나는 기술 지원을 제공합니다. Cisco 기술 지원 웹 사이트는 Cisco 제품 및 기술 관련 문제를 해결할 수 있는 온라인 문서 및 도구를 제공합니다. 웹 사이트는 하루 24시간, 365일 *http://www.cisco.com/techsupport* URL에 사용 가능 상태로 유지됩니다.

가장 신속하게 S3 및 S4 서비스 요청을 하려면 온라인 TAC 서비스 요청 도구를 사용합니다. (S3 및 S4 서비스 요청은 네트워크가 약간 손상되었거나 사용자가 제품 정보를 요구하는 상황을 지정합니다.) 상황을 설명하고 나면 TAC 서비스 요청 도구는 자동으로 권장 솔루션을 제공합니다. 권장 자원을 사용하여 문제를 해결할 수 없으면 서비스 요청이 Cisco TAC 엔지니어에게 할당됩니다. *http://www.cisco.com/techsupport/servicerequest* URL에서 TAC 서비스 요청 도구를 찾습니다.

S1 또는 S2 서비스 요청을 하거나 인터넷으로 액세스할 수 없는 경우 Cisco TAC에 전화로 문의하십시오. (S1 또는 S2 서비스 요청은 운영 네트워크가 작동하지 않거나 심각한 성능 저하가 있는 상황을 나타냅니다.) 비즈니스 운영을 원활하게 유지할 수 있도록 S1 및 S2 서비스 요청은 즉시 Cisco 엔지니어에게 할당됩니다.

전화로 서비스 요청을 열려면 다음 번호 중 하나를 사용하십시오.

아시아 태평양: +61 2 8446 7411(오스트레일리아: 1 800 805 227)

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

Cisco TAC 연락처의 전체 목록을 보려면 다음 URL *http://www.cisco.com/techsupport/contacts*을 방문하십시오.

- 필요한 정보, 492 페이지
- 필수 예비 정보, 492 페이지
- 온라인 케이스, 494 페이지
- 서비스 가용성 커넥터, 494 페이지
- Cisco Live!, 495 페이지
- Remote Access, 495 페이지
- Cisco 보안 텔넷, 496 페이지

- 원격 계정 설정, 497 페이지

필요한 정보

Cisco TAC에서 케이스를 열 때 문제를 더 잘 파악하고 정규화하려면 사전 정보를 제공해야 합니다. 문제의 성격에 따라 추가 정보를 제공해야 할 수도 있습니다. 서비스 케이스를 연 후 엔지니어 요청이 있을 때까지 다음 정보를 수집하기 위해 대기하면 해결 지연이 발생합니다.

관련 항목

Cisco Live!, 495 페이지
Cisco 보안 텔넷, 496 페이지
일반 정보, 493 페이지
네트워크 레이아웃, 492 페이지
온라인 케이스, 494 페이지
문제 설명, 493 페이지
Remote Access, 495 페이지
필수 예비 정보, 492 페이지

필수 예비 정보

모든 문제에 대해 다음 정보를 항상 TAC에 제공하십시오. 이 정보를 수집 및 저장하여 TAC 케이스를 열고 변경 사항에 따라 정기적으로 업데이트합니다.

관련 항목

일반 정보, 493 페이지
네트워크 레이아웃, 492 페이지
문제 설명, 493 페이지

네트워크 레이아웃

물리적 및 논리적 설정에 대한 자세한 설명과 음성 네트워크에 관련된 모든 네트워크 요소(해당하는 경우)를 제공합니다.

- Unified Communications Manager
  - 버전(Unified Communications Manager 관리에서 세부 정보 선택)
  - Unified Communications Manager의 수
  - 설정(독립 실행형, 클러스터)
    - Unity
  - 버전(Unified Communications Manager 관리에서)

- 통합 유형
  - 애플리케이션
- 설치된 애플리케이션 목록
- 각 애플리케이션의 버전 번호
  - IP/음성 게이트웨이
- OS 버전
- 기술 표시(IOS 게이트웨이)
- Unified Communications Manager 로드(Skinny 게이트웨이)
  - 전환
- OS 버전
- VLAN 컨피그레이션
  - 다이얼 계획 - 번호 매기기 방식, 통화 라우팅

이상적으로는 Visio 또는 JPG와 같은 기타 세부 다이어그램을 제출합니다. 화이트보드를 사용하여 Cisco Live! 세션을 통해 다이어그램을 제공 할 수도 있습니다.

문제 설명

문제가 발생할 때 사용자가 수행한 작업에 대한 단계별 세부 정보를 제공합니다. 세부 정보에 다음이 포함되어 있는지 확인하십시오.

- 예상된 동작
- 관찰된 세부 동작

일반 정보

다음 정보를 사용할 수 있는지 확인하십시오.

- 새로운 설치입니까?
- 이전 버전의 Unified Communications Manager 설치인 경우 이 문제가 처음부터 발생했습니까? (그렇지 않은 경우 최근에 시스템에 수행한 변경 사항은 무엇입니까?)
- 문제를 재현할 수 있습니까?
  - 재현할 수 있는 경우 정상 또는 특별한 상황입니까?
  - 재현할 수 없는 경우 발생할 때 특별한 점이 있습니까?

- 발생 빈도는 어떻습니까?

- 영향을 받는 장치는 무엇입니까?
  - 특정 장치가 영향을 받는 경우(임의) 공통점은 무엇입니까?
  - 문제에 관련된 모든 장치에 대한 DN 또는 IP 주소(게이트웨이)를 포함하십시오.
- 통화 경로에 있는 장치는 무엇입니까(해당되는 경우)?

온라인 케이스

Cisco.com을 통해 온라인으로 케이스를 열면 다른 모든 케이스 열기 방법보다 초기 우선 순위가 부여됩니다. 우선 순위가 높은 케이스(P1 및 P2)는 이 규칙에 대한 예외를 제공합니다.

케이스를 열 때 정확한 문제 설명을 제공합니다. 문제에 대한 설명은 즉각적인 솔루션을 제공할 수 있는 URL 링크를 반환합니다.

문제에 대한 해결 방법을 찾을 수 없는 경우에는 해당 케이스를 TAC 엔지니어에게 보내는 과정을 계속 진행합니다.

서비스 가용성 커넥터

서비스 가용성 커넥터 개요

Webex 서비스 가용성 서비스를 사용하여 로그를 쉽게 수집할 수 있습니다. 이 서비스는 진단 로그 및 정보의 찾기, 검색 및 저장 작업을 자동화합니다.

이 기능은 사용자의 온프레미스에 배포된 서비스 가용성 커넥터를 사용합니다. 서비스 가용성 커넥터는 네트워크의 전용 호스트(' 커넥터 호스트')에서 실행됩니다. 다음 구성 요소 중 하나에 커넥터를 설치할 수 있습니다.

- 엔터프라이즈 컴퓨팅 플랫폼(ECP) — 권장

  ECP는 Docker 컨테이너를 사용하여 서비스를 격리, 보호 및 관리합니다. 호스트 및 서비스 가용성 커넥터 애플리케이션이 클라우드에서 설치됩니다. 최신 상태 및 보안을 유지하기 위해 수동으로 업그레이드할 필요는 없습니다.

중요 ECP를 사용하는 것이 좋습니다. 향후 개발은 이 플랫폼에 중점을 둘 것입니다. Expressway에 서비스 가용성 커넥터를 설치하는 경우 몇 가지 새로운 기능을 사용할 수 없습니다.

- Cisco Expressway

다음과 같은 목적으로 서비스 가용성 커넥터를 사용할 수 있습니다.

- 서비스 요청에 대한 자동 로그 및 시스템 정보 검색
- Cloud-Connected UC 구축의 통합 CM 클러스터 로그 수집

두 사용 사례 모두에 대해 동일한 서비스 가용성 커넥터를 사용할 수 있습니다.

서비스 가용성 서비스 사용의 이점

이 서비스는 다음과 같은 이점을 제공합니다.

- 로그 수집 속도를 빠르게 합니다. TAC 엔지니어가 문제 진단을 수행하는 동안 관련 로그를 검색할 수 있습니다. 추가 로그를 요청하고 수동 수집 및 전달을 기다리는 지연을 방지할 수 있습니다. 이 자동화는 문제 해결 시간을 며칠 정도 단축시킬 수 있습니다.
- TAC의 협업 솔루션 분석기 및 해당 진단 서명 데이터베이스와 함께 작동합니다. 시스템은 자동으로 로그를 분석하고 알려진 문제를 식별하며 알려진 수정 사항 또는 해결 방법을 권장합니다.

서비스 가용성 커넥터에 대한 **TAC** 지원

서비스 가용성 커넥터에 대한 자세한 내용은 https://www.cisco.com/go/serviceability을 참조하거나 TAC 담당자에게 문의하십시오.

Cisco Live!

안전하고 암호화된 Java 애플릿인 Cisco Live!를 사용하면 사용자와 Cisco TAC 엔지니어가 협업 웹 브라우징/URL 공유, 화이트보드, 텔넷 및 클립보드 도구를 사용하여 더 효과적으로 공동 작업을 수행할 수 있습니다.

Cisco Live! 액세스 URL은 다음과 같습니다.

`http://c3.cisco.com/`

Remote Access

원격 접속은 모든 필요한 장비에 터미널 서비스(원격 포트 3389), HTTP(원격 포트 80) 및 텔넷(원격 포트 23) 세션을 설정할 수 있는 기능을 제공합니다.

⚠

주의 다이얼인을 설정할 때 시스템이 취약해지므로 로그인**:cisco** 또는 암호**:cisco**는 사용하지 마십시오.

다음 방법 중 하나를 사용하여 장치에 대한 TAC 엔지니어 원격 접속을 허용함으로써 많은 문제를 신속하게 해결할 수 있습니다.

- 공개 IP 주소가 있는 장치.

- 다이얼인 액세스 - 기본 설정의 내림 차순으로 아날로그 모뎀, ISDN(Integrated Service Digital Network) 모뎀, VPN(Virtual Private Network)을 선택합니다.
- NAT(Network Address Translation) - 개인 IP 주소가 있는 장비에 대한 액세스를 허용하기 위한 IOS 및 PIX(사설 인터넷 교환).

엔지니어 간섭 중에 방화벽에서 IOS 트래픽 및 PIX 트래픽을 방해하지 않으며, 터미널 서비스와 같은 필요한 모든 서비스가 서버에서 시작되는지 확인합니다.

참고 TAC는 모든 액세스 정보를 최대한 신중하게 처리하며, 고객 동의 없이 변경 사항이 시스템에 적용되지 않습니다.

Cisco 보안 텔넷

Cisco 보안 텔넷은 사이트의 Unified Communications Manager 서버에 Cisco의 CSE(Cisco Service 엔지니어) 투명 방화벽 액세스를 제공합니다.

Cisco 보안 텔넷은 방화벽 뒤에 있는 텔넷 데몬에 연결하기 위해 Cisco Systems 방화벽 내에서 텔넷 클라이언트를 활성화하여 작동합니다. 이 보안 연결을 사용하면 방화벽을 수정할 필요 없이 Unified Communications Manager 서버의 원격 모니터링 및 유지 관리를 수행할 수 있습니다.

참고 Cisco는 사용자가 허가한 경우에만 사용자 네트워크에 액세스합니다. 프로세스를 시작하는 데 도움이 되도록 사이트에서 네트워크 관리자를 제공해야 합니다.

방화벽 보호

사실상 모든 내부 네트워크는 방화벽 애플리케이션을 사용하여 내부 호스트 시스템에 대한 외부 액세스를 제한합니다. 이러한 애플리케이션은 네트워크와 공용 인터넷 간의 IP 연결을 제한하여 네트워크를 보호합니다.

방화벽은 이런 액세스를 허용하도록 소프트웨어를 다시 구성하지 않는 한 외부에서 시작된 TCP/IP 연결을 자동으로 차단하도록 작동합니다.

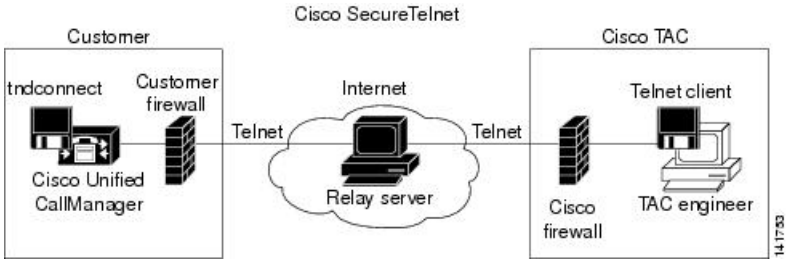
회사 네트워크는 일반적으로 공용 인터넷과의 통신을 허용하지만, 외부 호스트에 대한 연결이 방화벽 내부에서 시작되는 경우에만 가능합니다.

Cisco 보안 텔넷 설계

Cisco 보안 텔넷은 텔넷 연결을 방화벽 뒤에서 쉽게 시작할 수 있다는 사실을 이용합니다. 시스템은 외부 프록시 시스템을 사용하여 방화벽의 뒤에 있는TCP/IP 통신을 *Cisco* 기술 지원 센터(TAC)에서 다른 방화벽 뒤에 있는 호스트로 릴레이합니다.

이 릴레이 서버를 사용하면 두 방화벽의 무결성을 유지하면서 보호된 원격 시스템 간의 보안 통신이 지원됩니다.

그림 *26: Cisco* 보안 텔넷 시스템



Cisco 보안 텔넷 구조

외부 릴레이 서버는 텔넷 터널을 작성하여 네트워크와 Cisco 시스템 간의 연결을 설정합니다. 이를 통해 Unified Communications Manager 서버의 IP 주소 및 암호 식별자를 CSE로 전송할 수 있습니다.

참고 암호는 관리자와 CSE가 상호 일치하는 텍스트 문자열로 구성됩니다.

관리자가 방화벽 내부에서 공용 인터넷의 릴레이 서버로 TCP 연결을 설정하는 텔넷 터널을 시작하여 프로세스를 시작합니다. 그런 다음 텔넷 터널은 로컬 텔넷 서버에 또 다른 연결을 설정하여 엔터티 간에 양방향 링크를 만듭니다.

참고 Cisco TAC의 텔넷 클라이언트는 Windows NT 및 Windows 2000 또는 UNIX 운영 체제에서 실행되는 시스템을 준수하여 실행됩니다.

사이트의 Cisco Communications Manager에서 암호를 승인한 후에는 Cisco TAC에서 실행되는 텔넷 클라이언트가 방화벽 뒤에서 실행되는 텔넷 데몬에 연결됩니다. 결과적으로 투명한 연결은 시스템을 로컬로 사용하는 것과 동일한 액세스를 허용합니다.

텔넷 연결이 안정화된 후에는 CSE가 모든 원격 서비스 가용성 기능을 구현하여 Unified Communications Manager 서버에서 유지 보수, 진단 및 문제 해결 작업을 수행할 수 있습니다.

CSE에서 전송하는 명령과 Unified Communications Manager 서버에서 발생하는 응답을 볼 수 있지만, 명령과 응답은 항상 완전히 포맷되지 않을 수 있습니다.

원격 계정 설정

Cisco 지원이 일시적으로 문제 해결을 위해 시스템에 액세스할 수 있도록 Unified Communications Manager에서 원격 계정을 구성합니다.

프로시저

단계 **1** Cisco Unified Operating System 관리에서 서비스 > 원격 지원을 선택합니다.

단계 **2** 계정 이름 필드에 원격 계정의 이름을 입력합니다.

단계 **3** 계정 기간 필드에 계정 기간(일)을 입력합니다.

단계 **4** 저장을 클릭합니다.
시스템에서 암호화된 암호구를 생성합니다.

단계 **5** Cisco 지원에 연락하여 원격 지원 계정 이름 및 암호를 제공하십시오.