

CA Application Performance Management

구성 및 관리 안내서

릴리스 9.5



포함된 도움말 시스템 및 전자적으로 배포된 매체를 포함하는 이 문서(이하 "문서")는 정보 제공의 목적으로만 제공되며 CA 에 의해 언제든지 변경 또는 취소될 수 있습니다.

CA 의 사전 서면 동의 없이 본건 문서의 전체 혹은 일부를 복사, 전송, 재생, 공개, 수정 또는 복제할 수 없습니다. 이 문서는 CA 의 기밀 및 독점 정보이며, 귀하는 이 문서를 공개하거나 다음에 의해 허용된 경우를 제외한 다른 용도로 사용할 수 없습니다: (i) 귀하가 이 문서와 관련된 CA 소프트웨어를 사용함에 있어 귀하와 CA 사이에 별도 동의가 있는 경우, 또는 (ii) 귀하와 CA 사이에 별도 기밀 유지 동의가 있는 경우.

상기 사항에도 불구하고, 본건 문서에 기술된 라이선스가 있는 사용자는 귀하 및 귀하 직원들의 해당 소프트웨어와 관련된 내부적인 사용을 위해 합당한 수의 문서 복사본을 인쇄 또는 제작할 수 있습니다. 단, 이 경우 각 복사본에는 전체 CA 저작권 정보와 범례가 첨부되어야 합니다.

본건 문서의 사본 인쇄 또는 제작 권한은 해당 소프트웨어의 라이선스가 전체 효력을 가지고 유효한 상태를 유지하는 기간으로 제한됩니다. 어떤 사유로 인해 라이선스가 종료되는 경우, 귀하는 서면으로 문서의 전체 또는 일부 복사본이 CA 에 반환되거나 파괴되었음을 입증할 책임이 있습니다.

CA 는 관련법의 허용 범위 내에서, 상품성에 대한 묵시적 보증, 특정 목적에 대한 적합성 또는 권리 위반 보호를 비롯하여(이에 제한되지 않음) 어떤 종류의 보증 없이 본 문서를 "있는 그대로" 제공합니다. CA 는 본 시스템의 사용으로 인해 발생하는 직, 간접 손실이나 손해(수익의 손실, 사업 중단, 영업권 또는 데이터 손실 포함)에 대해서는 (상기 손실이나 손해에 대해 사전에 명시적으로 통지를 받은 경우라 하더라도) 귀하나 제 3 자에게 책임을 지지 않습니다.

본건 문서에 언급된 모든 소프트웨어 제품의 사용 조건은 해당 라이선스 계약을 따르며 어떠한 경우에도 이 문서에서 언급된 조건에 의해 라이선스 계약이 수정되지 않습니다.

본 문서는 CA 에서 제작되었습니다.

본 시스템은 "제한적 권리"와 함께 제공됩니다. 미합중국 정부에 의한 사용, 복제 또는 공개는 연방조달규정(FAR) 제 12.212 조, 제 52.227-14 조, 제 52.227-19(c)(1)호 - 제(2)호 및 국방연방구매규정(DFARS) 제 252.227-7014(b)(3)호 또는 해당하는 경우 후속 조항에 명시된 제한 사항을 따릅니다.

Copyright © 2013 CA. All rights reserved. 본 시스템에서 언급된 모든 상표, 상호, 서비스 표시 및 로고는 각 해당 회사의 소유입니다.

CA Technologies 제품 참조

이 문서에서는 다음과 같은 CA Technologies 제품과 기능을 참조합니다.

- CA Application Performance Management(CA APM)
- CA Application Performance Management ChangeDetector(CA APM ChangeDetector)
- CA Application Performance Management ErrorDetector(CA APM ErrorDetector)
- CA Application Performance Management for CA Database Performance(CA APM for CA Database Performance)
- CA Application Performance Management for CA SiteMinder®(CA APM for CA SiteMinder®)
- CA Application Performance Management for CA SiteMinder® Application Server Agents(CA APM for CA SiteMinder® ASA)
- CA Application Performance Management for IBM CICS Transaction Gateway(CA APM for IBM CICS Transaction Gateway)
- CA Application Performance Management for IBM WebSphere Application Server(CA APM for IBM WebSphere Application Server)
- CA Application Performance Management for IBM WebSphere Distributed Environments(CA APM for IBM WebSphere Distributed Environments)
- CA Application Performance Management for IBM WebSphere MQ(CA APM for IBM WebSphere MQ)
- CA Application Performance Management for IBM WebSphere Portal(CA APM for IBM WebSphere Portal)
- CA Application Performance Management for IBM WebSphere Process Server(CA APM for IBM WebSphere Process Server)
- CA Application Performance Management for IBM z/OS®(CA APM for IBM z/OS®)
- CA Application Performance Management for Microsoft SharePoint(CA APM for Microsoft SharePoint)
- CA Application Performance Management for Oracle Databases(CA APM for Oracle Databases)
- CA Application Performance Management for Oracle Service Bus(CA APM for Oracle Service Bus)

- CA Application Performance Management for Oracle WebLogic Portal(CA APM for Oracle WebLogic Portal)
- CA Application Performance Management for Oracle WebLogic Server(CA APM for Oracle WebLogic Server)
- CA Application Performance Management for SOA(CA APM for SOA)
- CA Application Performance Management for TIBCO BusinessWorks(CA APM for TIBCO BusinessWorks)
- CA Application Performance Management for TIBCO Enterprise Message Service(CA APM for TIBCO Enterprise Message Service)
- CA Application Performance Management for Web Servers(CA APM for Web Servers)
- CA Application Performance Management for webMethods Broker(CA APM for webMethods Broker)
- CA Application Performance Management for webMethods Integration Server(CA APM for webMethods Integration Server)
- CA Application Performance Management Integration for CA CMDB(CA APM Integration for CA CMDB)
- CA Application Performance Management Integration for CA NSM(CA APM Integration for CA NSM)
- CA Application Performance Management LeakHunter(CA APM LeakHunter)
- CA Application Performance Management Transaction Generator(CA APM TG)
- CA Cross-Enterprise Application Performance Management
- CA Customer Experience Manager(CA CEM)
- CA Embedded Entitlements Manager(CA EEM)
- CA eHealth® Performance Manager(CA eHealth)
- CA Insight™ Database Performance Monitor for DB2 for z/OS®
- CA Introscope®
- CA SiteMinder®
- CA Spectrum® Infrastructure Manager(CA Spectrum)
- CA SYSVIEW® Performance Management(CA SYSVIEW)

CA 에 문의

기술 지원팀에 문의

온라인 기술 지원 및 지사 목록, 기본 서비스 시간, 전화 번호에 대해서는 <http://www.ca.com/worldwide>에서 기술 지원팀에 문의하십시오.

목차

제 1 장: CA APM 구성 및 관리 안내서 소개	25
APM 정보.....	25
제 2 장: Enterprise Manager 시작 및 중지	27
Windows 에서 Enterprise Manager 시작.....	27
Enterprise Manager 를 Windows 서비스로 실행.....	28
Windows 에서 수동으로 Enterprise Manager 시작.....	30
UNIX 에서 Enterprise Manager 시작.....	30
UNIX 에서 수동으로 Enterprise Manager 시작.....	30
UNIX 에서 Enterprise Manager 제어 스크립트 실행.....	31
UNIX 에서 nohup 모드로 Enterprise Manager 실행.....	31
다른 JVM 을 사용하도록 Enterprise Manager 구성.....	32
Enterprise Manager 로그 파일 정보.....	32
날짜 또는 크기별로 Enterprise Manager 로그 롤링.....	33
Enterprise Manager config 디렉터리 구성.....	34
Enterprise Manager 중지.....	36
터미널 창에서 Enterprise Manager 중지.....	36
Workstation 에서 Enterprise Manager 중지.....	36
Enterprise Manager 자동 종료.....	36
계획되지 않은 종료 후 다시 시작.....	37
Enterprise Manager 셸 및 터미널 창 명령.....	38
제 3 장: Enterprise Manager 통신 구성	39
기본 Enterprise Manager 통신 채널.....	39
사용 중인 포트에 통신 채널 재바인딩.....	40
SSL 구성.....	41
방화벽을 통과하여 Enterprise Manager 에 연결.....	43
HTTPS 용으로 Enterprise Manager 웹 서버 구성.....	44
HTTPS 작동 방식 이해.....	44
기본 Jetty 구성 파일.....	45
제 4 장: Enterprise Manager 데이터베이스 구성	49
APM 데이터베이스 관리.....	49

데이터베이스 백업 또는복원	50
데이터베이스 구성 내보내기 또는 가져오기	56
다른 운영 체제로 APM 데이터베이스 이동	63
PostgreSQL 데이터베이스에서 Oracle 데이터베이스로 데이터 마이그레이션	63
데이터베이스 문제 해결	66
SmartStor 데이터 저장소 구성	66
SmartStor 계층 작동 방식에 대한 세부 정보	67
메타데이터 자동 삭제	68
SmartStor 시스템 요구 사항 확인	68
SmartStor 데이터 계층 값 지정	69
트랜잭션 이벤트 데이터베이스 위치 및 만료 처리 구성	70
기준 저장소 위치 구성	70
SmartStor, 기준 및 트랜잭션 이벤트 데이터 백업	71
쿼리 전용 중복 클러스터 만들기	72
SmartStor 도구를 사용하여 SmartStor 데이터 조정	73
SmartStor 도구 명령	74
merge	75
remove_metrics	75
remove_agents	77
keep_agents	78
prune	78
test_regex	80
list_agents	81
SmartStor 메타데이터 정리	81
SmartStor 데이터 및 메타데이터 자르기	83
예제: test_regex 명령을 사용하여 SmartStor 데이터 문제 찾기	86
8.x 데이터를 9.x 로 업그레이드	87
업그레이드 명령을 사용하여 8.x 데이터 업그레이드	88

제 5 장: 가상 에이전트를 사용하여 메트릭 집계 89

가상 에이전트 이해	89
가상 에이전트 요구 사항	89
가상 에이전트 구성	90

제 6 장: Enterprise Manager 및 클러스터 구성 93

독립 실행형 Enterprise Manager 구성	93
Enterprise Manager 클러스터링 이해	93
Enterprise Manager 를 클러스터할 시기	94
MOM 의 수집기 관리 방법 이해	94

클러스터링 및 Enterprise Manager 클록 동기화	95
클러스터링 및 에이전트 이름 지정	96
클러스터링 및 관리 모듈	97
Enterprise Manager 장애 조치 사용	97
Enterprise Manager 장애 조치 규칙	99
단일 호스트에서 작동하도록 Enterprise Manager 장애 조치 구성	101
MOM 장애 조치 및 CA CEM TIM 정보	101
Enterprise Manager 클러스터 구성	103
MOM 구성	104
수집기 구성	105
CDV 정보	106
CDV 구성	107

제 7 장: MOM 에이전트 부하 분산 구성 109

에이전트 부하 분산 개요	109
MOM 이 수집기에 에이전트를 할당하는 방법	110
MOM 이 클러스터를 재분산하는 방법	111
에이전트 부하 분산 메트릭 가중 요소 설정	112
에이전트 부하 분산 메트릭 임계값 설정	113
에이전트 부하 분산 간격 속성 설정	114
에이전트 부하 분산 사용 시나리오	115
새 수집기가 클러스터에 추가될 때의 에이전트 부하 분산	115
에이전트를 가진 수집기가 추가될 때의 에이전트 부하 분산	115
수집기에 장애가 발생할 때의 에이전트 부하 분산	116
수집기가 다시 시작될 때의 에이전트 부하 분산	116
가중치가 적용된 에이전트 부하 분산	117
수집기에 대한 에이전트 할당 구성	117
에이전트 부하 분산 구성 예제	121

제 8 장: 에이전트 - Enterprise Manager 네트워크 토폴로지 구성 127

에이전트 - Enterprise Manager 네트워크 토폴로지 개요	128
에이전트 연결 정보가 CA Introscope 에 전파되는 방법	130
구성이 에이전트와 Enterprise Manager 의 연결에 미치는 영향	132
Enterprise Manager 에서 에이전트의 연결이 끊길 때 발생하는 결과	133
에이전트 연결 요청이 거부될 때 발생하는 결과	134
에이전트 - Enterprise Manager 네트워크 토폴로지 구성 프로세스	135
에이전트 - Enterprise Manager 네트워크 토폴로지 계획	136
loadbalancing.xml 규칙이 없을 때 새 에이전트 연결 허용 여부 구성	138

에이전트 다시 연결 대기 시간 구성.....	139
허용되지 않는 에이전트 연결 클램프 제한 구성.....	140
계속해서 허용된 Enterprise Manager 에 다시 연결하도록 에이전트 구성.....	141
Enterprise Manager 별로 허용되거나 허용되지 않는 에이전트에 대한 loadbalancing.xml 구성.....	143
에이전트 - Enterprise Manager 네트워크 토폴로지 문제 해결.....	143
Enterprise Manager 가 거부된 에이전트를 처리하는 방법.....	143
수집기가 introscope.apm.agentcontrol.agent.allowed 속성을 사용하는 경우.....	144
에이전트가 loadbalancing.xml 의 허용됨 또는 허용되지 않음 정규식과 일치하지 않는 경우.....	145
에이전트에 할당된 모든 수집기가 사용 불가능하고 다른 수집기는 사용 가능한 경우.....	145
수집기가 허용되지 않는 에이전트를 직접 연결을 사용하여 처리하는 방법.....	146
introscope.apm.agentcontrol.agent.allowed 속성이 없을 때의 기본 에이전트 연결 값.....	146
사용 가능한 MOM 이 없을 때 CA Introscope 에서 에이전트 연결 대상을 결정하는 방법.....	146

제 9 장: 명령줄 Workstation 사용 147

CLW(명령줄 Workstation) 정보.....	147
CLW 실행.....	148
JVM 요구 사항.....	148
CLW 명령을 실행할 위치.....	148
CLW 대화식 모드 사용.....	148
CLW 호출.....	149
CLW 는 대/소문자를 구분함.....	150
CLW 명령 출력.....	150
CLW 및 정규식.....	150
CLW 명령 내의 백슬래시 및 따옴표.....	150
다양한 환경에서 CLW 사용.....	151
명령줄 Workstation 로그 구성.....	151
CLW 명령 참조.....	151
Enterprise Manager 명령.....	152
Introscope Agent 명령.....	154
APM 상태 콘솔 명령.....	157
관리 모듈 명령.....	162
작업 명령.....	165
경고 명령.....	167
경고 중지 일정 명령.....	169
계산기 명령.....	171
대시보드 명령.....	173
메트릭 및 메트릭 그룹화 명령.....	175
보고서 템플릿 명령.....	178
SNMP 수집 명령.....	182

트랜잭션 추적 옵션 구성	184
트랜잭션 추적 세션 시작	184
응용 프로그램 심사 맵 명령	191
Loadbalancing.xml 명령	198
샘플 스크립트	201
트랜잭션 추적 세션	201
경고에 의해 트리거되는 트랜잭션 추적 세션	205

제 10 장: WatchDog 명령줄 도구 사용 207

WatchDog 정보	207
WatchDog 실행	208
SAP 에서 WatchDog 실행	209
WatchDog 명령	210
WatchDog start 명령	211
WatchDog stop 명령	212
WatchDog status 명령	213
WatchDog 명령 옵션	214
WatchDog -watch 명령 옵션	214
WatchDog -port 명령 옵션	215
WatchDog -startcmd 명령 옵션	216
WatchDog -interval 명령 옵션	216
WatchDog -startuptime 명령 옵션	217
WatchDog -jre 명령 옵션	217
WatchDog -emport 명령 옵션	218
WatchDog -emuser 명령 옵션	218
WatchDog -empwd 명령 옵션	219
WatchDog 로그 파일 보기	219
샘플 스크립트	219

제 11 장: WebView 옵션 구성 221

WebView 응용 프로그램 컨텍스트 경로 구성	221
APM WebView 성능을 구성하고 모니터링하는 방법	222
필수 구성 요소 검토	223
APM UI 성능 모니터 구성	224
구성 확인	225
WebView UI 성능 모니터링	226
WebView 메트릭 그룹화 구성	229
대시보드 데이터 보기 및 해석	230

제 12 장: Workstation 구성 233

세부 정보 표시 모드에서 Workstation 실행	233
Workstation 출력을 파일로 리디렉션	234
로그인 값을 제공하도록 Workstation 구성	234
아시아 언어 보고서에 대해 Workstation 구성	235

제 13 장: 시스템 구성 237

클록 차이 허용치 구성	237
최대 데이터 포인트 검색 속성 설정	238
쿼리에서 반환되는 데이터 포인트 제한	240
반환되는 쿼리 결과 수 늘리기	241
APM 상태 콘솔 클램프 및 중요한 이벤트 구성	241

제 14 장: 응용 프로그램 심사 맵 구성 243

응용 프로그램 심사 맵	243
트랜잭션 샘플링	244
맵 요소 만료 처리 구성	244
응용 프로그램 심사 맵 데이터 클램프	248
응용 프로그램 심사 맵 데이터 정리 구성	249
응용 프로그램 심사 맵 개체의 사용 만료 시간 구성	253
응용 프로그램 심사 맵 시간 만료 처리 속성	254
응용 프로그램 심사 맵 시간 만료 처리 속성 구성	255

제 15 장: Catalyst 데이터를 로드하도록 APM 구성 257

CA Catalyst 데이터를 로드하도록 CA APM 구성	258
CatalystPolicy.xml 파일 구성	259

제 16 장: CA CEM 소개 261

CEM 콘솔 및 설정 페이지 액세스	261
CEM 콘솔 액세스	261
CA CEM 에 로그인 문제 해결	262
TIM 의 "System Setup"(시스템 설정) 페이지 액세스	263
CEM 콘솔에서 TIM 액세스	263
CA CEM 관리자의 책임	264
매일 작업	264
매주 작업	265

매월 작업.....	265
매분기 작업.....	266

제 17 장: CA CEM 에 대한 네트워킹 대안 267

CA CEM 네트워크 옵션 정보	267
네트워크 트래픽 모니터링 정보	268
네트워크 탭 사용	268
미리링된 포트 사용	269
CA CEM 삽입 위치 정보	270
인터넷과 인터넷 라우터 사이	271
인터넷 라우터와 방화벽 사이	272
방화벽과 집계 스위치 사이	272
집계 스위치와 네트워크 부하 분산 장치 사이	273
네트워크 부하 분산 장치와 웹 서버 사이	274
브라우저에서 Enterprise Manager 로의 연결	274
IPv6 및 CA CEM	275
IPv6 정보	275
CA CEM 에서 IPv6	275
IPv6 네트워크 트래픽 모니터링	276
이중 스택(IPv6 및 IPv4) 호스트에서 CA CEM 실행	276
허용되는 IPv6 주소 형식	278

제 18 장: CA CEM 관리 281

CA CEM 관리 프로세스	281
Enterprise Manager 서비스 배포	282
Enterprise Manager 서비스의 일반적인 배포	284
클러스터 환경의 Enterprise Manager 서비스 배포	286
실시간 트랜잭션 메트릭을 위한 TIM 선택	287
자동 트랜잭션 검색을 위한 TIM 선택	287
Enterprise Manager 구성 수정	288
Enterprise Manager 제거	289
Enterprise Manager 서비스 문제 해결	290
CA CEM 도메인 정의	293
인시던트 원가와 비즈니스 영향의 비교	298
인시던트 관련 설정 정의	299
인시던트 관리 설정 구성	302
인시던트 생성 규칙 설정	303
비즈니스 영향 설정 및 인시던트에 대한 증거 수집	304

증거 수집 스크립트에 사용할 인수	306
인시던트 만료 처리 규칙 구성	307
인시던트가 개설되거나 심각도가 변경되면 전자 메일 보내기	308
SMTP 서버 설정 구성	309
새 비즈니스 서비스에 대한 보안 그룹 설정	311
모니터 사용	315
모니터 동기화	315
마지막 동기화 이후의 구성 변경 사항 보기	316

제 19 장: CA CEM 에서 사용자 및 그룹 관리 319

사용자 그룹 정보	320
최대 사용자 그룹 수	321
요청 특성별로 새 사용자 자동 할당	322
서브넷 사용자 그룹에 새 사용자 자동 할당	323
새 사용자에 대한 서브넷 사용자 그룹 생성	323
프록시 서버를 사용하는 경우 사용자 식별	324
새 사용자 그룹 관리	326
수동으로 사용자 그룹에 새 사용자 할당	327
사용자 그룹 구성	327
대량 편집을 사용하여 사용자 설정 구성	329
상관 관계 SLA 구성	330
상관 관계 SLA 보기	331
상관 관계 SLA 추가	332
기존 상관 관계 SLA 업데이트	333
상관 관계 SLA 삭제	334
사용자 그룹 삭제	334
사용자 비활성화 또는 삭제	335
사용자 다시 활성화	335

제 20 장: CA CEM 에서 시스템 작업 관리 337

CA CEM 이벤트 정보	337
심각도 수준	337
가능한 이벤트 목록	338
CA CEM 이벤트 보기	341
CA CEM 이벤트 관리	341
이벤트의 전자 메일 알림 수신	341
TIM 컴퓨터의 건전성 검토	343
"어플라이언스 건전성" 페이지 참조 테이블	344

CA CEM 감사 내역 보기	345
-----------------------	-----

제 21 장: CA CEM 을 사용하여 보고 **347**

CA CEM 보고서 캡처	347
CA CEM 보고서 집계 정보	347
보고서 배포.....	348
보고서 데이터 보안.....	349
보고서 형식.....	349
보고서 시간 프레임.....	350
보고서 탐색.....	351
PDF 보고서	352
보고서를 전자 메일로 보내기	353
저장되거나 예약된 보고서	353
보고서 예약.....	354
"내 보고서"를 사용하여 보고서 예약.....	354
보고서 생성 및 예약.....	357
CA CEM 데이터 내보내기	358
데이터 내보내기.....	358
보고서 저장 또는 예약.....	360
CSV 헤더	361

제 22 장: CA CEM 을 사용하여 보안 웹 응용 프로그램 모니터링 **363**

SSL 개인 키 가져오기 및 관리	363
Apache 또는 OpenSSL 기반 웹 서버 개인 키 저장.....	364
Microsoft Internet Information Service(IIS) 개인 키 내보내기 및 변환.....	364
SunONE, iPlanet 또는 Netscape Enterprise Server.....	365
SSL 용으로 CA CEM 구성.....	369
HTTPS 서버에 대한 여러 키 정보.....	370
SSL 을 사용한 CA CEM 확인.....	370

제 23 장: CA CEM 에서 Napatech 어댑터 사용 **371**

CA CEM 에서 Napatech 어댑터 사용 정보.....	371
Napatech 어댑터 및 소프트웨어 얻기.....	372
Napatech 어댑터 및 Napatech 소프트웨어 설치	372
Napatech 어댑터를 사용하도록 설정하고 모니터링	374
(선택 사항) Napatech 필터를 생성하고 사용하도록 설정.....	374
고급 필터 만들기.....	376
기타 Napatech 어댑터 작업.....	377

Napatech 어댑터 문제 해결.....	379
Napatech 어댑터가 트래픽을 수신하고 있지 않음.....	380
이더넷 포트가 인식되지 않는 Napatech 어댑터.....	381
예상되는 트래픽이 표시되지 않음.....	381
일련 번호 및 기타 Napatech 어댑터 세부 정보.....	381

제 24 장: CA CEM 과 함께 작동하도록 CA Introscope 구성 383

CA APM 시작.....	384
CA APM 고객 경험 메트릭 개요.....	384
CA APM 문제 해결 심사 개요.....	385
CA CEM 구성을 위한 점검 목록.....	386
필요한 통합 기능 결정.....	387
Introscope 설정 구성.....	387
고객 경험 메트릭 통합 구성.....	391
CA CEM 구성 확인.....	399
Introscope 구성을 위한 점검 목록.....	399
필요한 통합 기능 결정.....	400
Enterprise Manager 구성.....	400
Java Agent 와 통합.....	402
.NET 에이전트와 통합.....	405
Introscope 구성 확인.....	408
CA Introscope 와 CA CEM 의 통합 문제 해결.....	408
CA CEM 에서 CA Introscope 통합 확인.....	408
증상 및 해결 방법.....	409
업그레이드 고려 사항.....	411
비즈니스 응용 프로그램 설정.....	412

제 25 장: CA CEM 과의 CA SiteMinder 통합 413

CA SiteMinder 에 대한 검사 목록.....	414
CA CEM 에서 CA SiteMinder 구성.....	414
사용자 지정 CA SiteMinder 에이전트 생성.....	416
CA SiteMinder 에서 CA CEM 에 대한 사용자 지정 에이전트 유형 만들기.....	416
CA CEM 에서 정책 서버 정의.....	417
CA CEM 에서 에이전트 정의.....	418
TIM SiteMinder 호스트 구성 보기.....	419
CA SiteMinder 사용.....	419
CA SiteMinder 와 CA CEM 의 통합 문제 해결.....	419

제 26 장: CA CEM 과의 CA Service Desk 통합 421

CA CEM 과 통합되는 CA Service Desk 정보	421
CA Service Desk 통합 개요	421
CA CEM 에 맞게 CA Service Desk 구성	422
CA Service Desk 플러그 인 구성	422
CA Service Desk 요청 영역 구성	426
CA CEM 과 함께 CA Service Desk 사용	426
CA Service Desk 와 CA CEM 의 통합 문제 해결	427
증상 및 해결 방법	428
CA Service Desk 와 CA CEM 의 통합 용어	429
CA Service Desk 용어	429
CA Service Desk 와 CA CEM 의 용어 매핑	430

제 27 장: CA APM 과의 CA APM Cloud Monitor 통합 431

CA APM 배포에서 CA APM Cloud Monitor 를 통합하는 방법	432
CA APM Cloud Monitor 에이전트 다운로드 및 설치	432
CA APM Cloud Monitor 에이전트 연결의 유효성 검사	433
데이터를 제한하는 방법	435

부록 A: 속성 파일 참조 437

IntroscopeEnterpriseManager.properties	437
사용 가능한 프로세서	438
경고 동작	439
통신	439
Workstation Login Parameters(Workstation 로그인 매개 변수) 섹션 자동 채우기	445
EM 웹 서버 설정	445
핫 구성 서비스	447
응용 프로그램 추론	447
Logging(로깅)	448
영구 수집 - 데이터베이스에 데이터 기록	450
플랫 파일 속성	452
트랜잭션 이벤트 데이터베이스	452
트랜잭션 추적 샘플링	453
Enterprise Manager 메트릭 클램프	454
SmartStor	457
기준 데이터 저장	462
SNMP 수집	463
WebView	463

CA APM ChangeDetector	464
관리 모듈 부트스트랩	464
관리 모듈 배포	465
클러스터링 설정	465
에이전트 상호 작용	470
Enterprise Manager 장애 조치	474
구성 디렉터리	476
응용 프로그램 심사 맵 데이터	476
위치 맵 데이터	481
웹 서비스	482
나가는 메시지 큐	483
스레드 덤프	484
웹 서비스 성능 처리를 위한 스레드 속성	487
SNMP 심사 맵 경고 작업	488
응용 프로그램 맵 개체	489
APMEnterpriseManager.properties	490
c3p0 속성	490
Hibernate 관련 속성	492
apm-events-thresholds-config.xml	494
Introscope 클램프 속성	495
introscope.clw.max.users	495
introscope.enterprisemanager.agent.connection.limit	496
introscope.enterprisemanager.agent.error.limit	497
introscope.enterprisemanager.agent.metrics.limit	497
introscope.enterprisemanager.agent.trace.limit	498
introscope.cdv.max.users	499
introscope.enterprisemanager.disconnected.historical.agent.limit	499
introscope.enterprisemanager.events.limit	502
introscope.enterprisemanager.metrics.historical.limit	502
introscope.enterprisemanager.metrics.live.limit	503
introscope.enterprisemanager.transactionevents.storage.max.disk.usage	503
introscope.workstation.max.users	504
고객 경험 클램프 속성	505
중요한 이벤트 임계값 설정	507
ResourceMetricMap.properties	511
CPU 사용률	513
GC 에서 소비된 시간	513
사용 중인 스레드	513
사용 중인 JDBC 연결	513
Catalyst.properties	513
catalyst.host	514

catalyst.protocol	515
catalyst.port	515
catalyst.login	515
catalyst.password.....	515
catalyst.rest.entrypoint.....	516
catalyst.rest.alerts.pollingperiodsec	516
catalyst.rest.virtualhosts.pollingperiodsec	516
catalyst.product.url.....	517
catalyst.alert.filter.total	517
catalyst.alert.filter.time	517
catalyst.alert.filter.products.....	518
catalyst.alert.filter.types	518
catalyst.alert.filter.severities	519
catalyst.rest.maxFailures	519
catalyst.rest.maxAlertsPerPage	520
catalyst.rest.alerts.threads	520
catalyst.rest.virtualhosts.threads.....	520
catalyst.entity.cache.size	521
catalyst.entity.cache.expirationsec.....	521
catalyst.database.alerts.enabled	521
catalyst.database.map.name	522
EMservice.conf	522
wrapper.java.command	523
wrapper.java.mainclass.....	523
wrapper.java.classpath.x.....	523
wrapper.java.library.path.1	523
wrapper.java.additional.x=	524
wrapper.java.initmemory	524
wrapper.java.maxmemory.....	524
wrapper.app.parameter.x.....	525
wrapper.startup.timeout	525
wrapper.console.format	525
wrapper.console.loglevel	526
wrapper.logfile	526
wrapper.logfile.format.....	526
wrapper.logfile.loglevel	526
wrapper.logfile.maxsize	527
wrapper.logfile.maxfiles.....	527
wrapper.syslog.loglevel.....	527
wrapper.ntservice.name	527
wrapper.ntservice.displayname.....	528
wrapper.ntservice.description	528

wrapper.ntservice.dependency.x.....	528
wrapper.ntservice.starttype	528
wrapper.ntservice.interactive	529
Introscope Enterprise Manager.lax	529
lax.application.name	529
lax.class.path	529
lax.command.line.args	530
lax.dir.....	530
lax.main.class	530
lax.main.method	530
lax.nl.current.vm	531
lax.nl.java.launcher.main.class.....	531
lax.nl.java.launcher.main.method	531
lax.nl.java.option.additional.....	532
lax.nl.message.vm.not.loaded	533
lax.nl.valid.vm.list.....	533
lax.nl.win32.microsoftvm.min.version.....	533
lax.root.install.dir	533
lax.stderr.redirect	534
lax.stdin.redirect	534
lax.stdout.redirect.....	535
lax.user.dir.....	535
lax.version	535
IntroscopeWorkstation.properties.....	535
log4j.logger.Workstation	536
log4j.appender.logfile.File.....	536
introscope.workstation.graph.antialiased	536
transport.http.proxy.host	537
transport.http.proxy.port	537
transport.http.proxy.username	537
transport.http.proxy.password	537
transport.tcp.truststore	538
transport.tcp.trustpassword	538
transport.tcp.truststore	538
transport.tcp.keystore	539
transport.tcp.keypassword	539
transport.tcp.ciphersuites.....	540
Introscope Workstation.lax	540
lax.application.name	540
lax.class.path	541
lax.command.line.args	541
lax.dir.....	541

lax.main.class	541
lax.main.method	542
lax.nl.current.vm	542
lax.nl.java.launcher.main.class.....	542
lax.nl.java.launcher.main.method	542
lax.nl.java.option.additional.....	543
lax.nl.message.vm.not.loaded	543
lax.nl.valid.vm.list.....	543
lax.nl.win32.microsoftvm.min.version.....	544
lax.root.install.dir	544
lax.stderr.redirect	544
lax.stdin.redirect	545
lax.stdout.redirect.....	545
lax.user.dir.....	545
lax.version	546
IntroscopeWebView.properties	546
introscope.webview.jetty.configurationFile	546
introscope.webview.tcp.ipaddress	546
introscope.webview.tcp.port	547
introscope.webview.context.path	547
introscope.webview.enterprisemanager.tcp.host.....	547
introscope.enterprisemanager.webview.disableLogin.....	548
introscope.webview.enterprisemanager.tcp.port.....	548
log4j.logger.WebView	548
log4j.logger.WebServer.....	549
log4j.logger	549
log4j.logger.com.wily	550
log4j.logger.org.apache.myfaces	550
log4j.logger.org.apache.jasper.....	550
log4j.logger.org.apache.struts	551
log4j.logger.org.mortbay	551
로그 구성 속성	552
log4j.appender.console.....	552
log4j.appender.logfile	553
log4j.appender.logfile.File.....	553
Introscope WebView.lax	553
실행 파일 이름	553
lax.class.path.....	553
lax.command.line.args	554
lax.dir.....	554
lax.main.class	554
lax.main.method	554

lax.nl.current.vm	555
lax.nl.java.launcher.main.class.....	555
lax.nl.java.launcher.main.method	555
lax.nl.java.option.additional.....	555
lax.nl.message.vm.not.loaded	556
lax.nl.valid.vm.list.....	556
lax.nl.win32.microsoftvm.min.version	556
lax.root.installation.dir.....	556
lax.stderr.redirect	557
lax.stdin.redirect	557
lax.stdout.redirect.....	557
lax.user.dir.....	558
lax.version	558
APMCloudMonitor.properties	558
apmcm.folders.include	559
apmcm.monitors.include	559
apmcm.checkpoints.include	560
apmcm.include.inactive.monitors	560
apmcm.folder.metrics.include	561
apmcm.monitor.psp.metrics.include.....	561
apmcm.monitor.checkpoint.metrics.include.....	562
apmcm.force.global.update	562
apmcm.log.adjustment	563

부록 B: JDBC API **565**

JDBC API 구성.....	565
JDBC API 사용.....	565
메트릭 쿼리.....	566
트랜잭션 추적 쿼리.....	567

부록 C: Introscope 확장 구성 **569**

SNMP Adapter 구성	569
SNMP Adapter 제한 사항.....	569
SNMP Adapter 구성 요소	569
경고	570
알림 및 경고 구성	571
SNMP 기능 구성	572
HP LoadRunner 에 업로드.....	574
HP OpenView 에 업로드	576

Introscope 메트릭을 SNMP 메트릭으로 변환	578
Introscope 경고 웹 서비스 확장 구성	579

부록 D: 기본 `tess-default.properties` 파일 581

<code>tess-default.properties</code> 속성 기본 파일 수정	581
증거 수집을 위한 Perl 또는 Python 경로 설정	582
<code>perl.path</code>	583
<code>python.path</code>	583
"추가 결합 정보" 링크의 디렉터리 경로 설정	584
<code>additionalDefectDetailFileLocation</code>	585
결합 처리 성능 개선	585
<code>defects.affectedUserGroupUpdateInterval_Secs</code>	587
<code>defects.affectedUserGroupAgeoutInterval_Mins</code>	587
잘못된 파일의 디렉터리 위치 변경	588
<code>collectors.badDataDirectory</code>	589
기타 CA CEM 기본 속성	589
<code>baseline.durationInDays</code>	589
<code>BTStatsMetricName.backwardCompatible</code>	590
<code>email.defaultFromAddress</code>	591
<code>invalid.importexport.filename.chars</code>	591
<code>timTessCommunication.useSsl</code>	592

제 1 장: CA APM 구성 및 관리 안내서 소개

이 안내서를 사용하려면 웹 서버, 브라우저, 지원되는 플랫폼 및 사용 중인 네트워크 환경에 대한 실무 지식이 있어야 합니다. CA CEM 으로 모니터링되는 응용 프로그램에 익숙해야 합니다. 또한 CA CEM 과 통합되는 다른 제품에 대해서도 잘 알아보십시오.

이 안내서에서는 다음을 가정합니다.

- CA APM 설치 및 업그레이드 안내서의 정보에 따라 CA CEM 이 설치되어 있습니다.
- CA APM 개요 안내서에 설명된 CA Introscope, CA APM 및 CA CEM 에 대한 기본 사항을 숙지하고 있습니다.

이 섹션은 다음 항목을 포함하고 있습니다.

[APM 정보](#) (페이지 25)

APM 정보

CA Introscope 및 CA CEM 은 CA APM 솔루션의 핵심 제품입니다.

CA APM 은 최종 사용자 경험을 파악하고 SLA(서비스 수준 계약)를 평가할 수 있는 포괄적이고 효과적인 응용 프로그램 성능 관리 전략을 제공합니다. 모든 트랜잭션을 전체 인프라에 매핑하고 완전한 통합 솔루션에서 인시던트 심사 및 근본 원인 진단을 수행할 수 있습니다.

CA APM 에서는 다음을 수행할 수 있습니다.

- 실제 사용자 경험 파악
- 비즈니스 서비스에 대한 SLA 설정 및 관리
- 트랜잭션에 대한 완벽한 가시성 확보
- 문제의 원인을 신속하게 판단
- 심사 수행, 이해당사자 식별 및 근본 원인 분석 수행
- 실제 비즈니스 영향을 기준으로 인시던트 우선 순위 설정

- 사전 대응적 응용 프로그램 모니터링 제공
- 보고 확대 및 지속적인 향상 지원

제 2 장: Enterprise Manager 시작 및 중지

이 장에서는 Enterprise Manager 를 시작 및 중지하고 지원되는 환경에서 시작을 자동화하기 위한 지침을 제공합니다.

참고: 속성에 대한 자세한 내용은 [속성 파일 참조](#) (페이지 437)를 참조하십시오.

이 섹션은 다음 항목을 포함하고 있습니다.

[Windows 에서 Enterprise Manager 시작](#) (페이지 27)

[UNIX 에서 Enterprise Manager 시작](#) (페이지 30)

[다른 JVM 을 사용하도록 Enterprise Manager 구성](#) (페이지 32)

[Enterprise Manager 로그 파일 정보](#) (페이지 32)

[날짜 또는 크기별로 Enterprise Manager 로그 롤링](#) (페이지 33)

[Enterprise Manager config 디렉터리 구성](#) (페이지 34)

[Enterprise Manager 중지](#) (페이지 36)

[계획되지 않은 종료 후 다시 시작](#) (페이지 37)

[Enterprise Manager 셸 및 터미널 창 명령](#) (페이지 38)

Windows 에서 Enterprise Manager 시작

Windows 환경에서 Enterprise Manager 를 실행하는 경우에는 Enterprise Manager 를 수동으로 시작하거나 Windows 서비스로 실행할 수 있습니다.

Enterprise Manager 를 Windows 서비스로 실행

Enterprise Manager 를 Windows 서비스로 설치하면 가용성이 향상됩니다. Enterprise Manager 를 Windows 서비스로 구성하는 경우 Enterprise Manager 를 실행하는 컴퓨터가 자동으로 시작됩니다. 컴퓨터가 종료되면 Enterprise Manager 도 종료됩니다.

참고: Introscope 는 Tanuki Software(<http://wrapper.tanukisoftware.org>)의 공용 도메인 Java 서비스 래퍼를 사용하여 Enterprise Manager 가 Windows 서비스로 실행될 수 있도록 합니다. Tanuki 래퍼에 대한 자세한 내용은 "Configuration Property Overview"(구성 속성 개요)(<http://wrapper.tanukisoftware.org>)를 참조하십시오.

다음 지침에서는 사용자가 Windows 서비스에서 응용 프로그램을 구성하는 작업과 Windows 서비스 콘솔을 사용하는 작업에 익숙하다고 가정합니다.

Enterprise Manager 를 Windows 서비스로 실행하기 위한 사전 요구 사항

Enterprise Manager 를 Windows 서비스로 실행하려면 Enterprise Manager 가 이미 설치되고 콘솔 모드에서 제대로 실행되는지 확인하십시오.

Enterprise Manager 를 Windows 서비스로 구성

이 단원에서는 Introscope 기본 JVM 시스템 매개 변수로 실행 중인 Windows 컴퓨터에 단일 Enterprise Manager 를 등록하는 방법에 대해 설명합니다.

1. Enterprise Manager 를 중지합니다([Enterprise Manager 중지](#) (페이지 36) 참조).
2. *IntroscopeEnterpriseManager.lax* 파일(<EM_Home>/디렉터리에 있음)에서 *lax.stdin.redirect* 속성을 공백으로 설정하고 파일을 저장합니다.
3. *IntroscopeEnterpriseManager.properties* 파일 (<EM_Home>/config 디렉터리에 있음)에서 *introscope.enterprisemanager.disableInteractiveMode* 속성을 *true* 로 설정하고 파일을 저장합니다.

4. Enterprise Manager 서비스에 고유 이름을 할당합니다. 기본적으로 서비스 이름은 *EMService.conf*(*<EM_Home>/bin* 디렉터리에 있음)에서 할당됩니다. 컴퓨터에 구성된 다른 서비스가 없으면 기본 서비스 이름을 사용할 수 있습니다. 그렇지 않으면 다음 속성을 사용하여 서비스의 고유 이름과 표시 이름을 지정하도록 *EMService.conf* 를 수정합니다.
 - *wrapper.ntservice.name=<unique Enterprise Manager name>*
 - *wrapper.ntservice.displayname=<Enterprise Manager display name>*
5. 파일의 변경 내용을 저장합니다.
6. Enterprise Manager 인스턴스를 서비스로 등록하기 위해 *<EM_Home>/bin/EMCtrl32.bat register* 스크립트를 실행합니다.

Windows 서비스 콘솔에서 Enterprise Manager 가 Windows 서비스로 구성된 것으로 표시됩니다.

서비스로 실행할 Enterprise Manager 각각에 대해 위 단계를 반복하십시오.

Windows 서비스 속성 변경

EMService.conf 파일에서 구성 속성을 변경해야 하는 경우 먼저 다음 단원에 설명된 대로 서비스 등록을 취소하십시오. 변경 사항을 적용하려면 변경한 후 서비스를 다시 등록하십시오.

Enterprise Manager Windows 서비스 등록 취소

다음과 같은 경우 Enterprise Manager 서비스 등록을 취소하십시오.

- *EMService.conf* 속성 파일을 변경하기 전에
- Enterprise Manager 인스턴스를 콘솔 컨트롤로 반환하려는 경우
- Enterprise Manager 인스턴스를 제거하기 전에

Enterprise Manager 서비스 등록을 취소하려면

1. Enterprise Manager 서비스를 중지하고 Windows 서비스 GUI 를 종료합니다.
2. *<EM_Home>/bin/EMCtrl32.bat unregister* 를 실행합니다.

참고: Enterprise Manager 서비스 또는 Windows 서비스 GUI 가 활성 상태인 경우에만 서비스가 삭제 대상으로 표시됩니다. 이는 Windows 레지스트리 잠금이 서비스 제거를 방지하기 때문에 발생하는 표준 Windows 서비스 동작입니다. 컴퓨터를 다시 시작하면 서비스가 삭제됩니다.

Enterprise Manager Windows 서비스 중지 및 다시 시작

Windows 서비스로 실행 중인 Enterprise Manager 를 시작, 중지 및 다시 시작하려면 Windows 서비스 GUI 의 표준 컨트롤을 사용하십시오.

Windows 에서 수동으로 Enterprise Manager 시작

다음 방법 중 하나를 사용하여 수동으로 Enterprise Manager 를 시작할 수 있습니다.

- "시작", "프로그램" "CA APM", "관리", "CA APM", "Enterprise Manager"로 이동합니다.
- <EM_Home> 디렉터리에 있는 *IntroscopeEnterpriseManager.exe* 를 실행합니다.

<EM_Home>/Introscope Enterprise Manager.lax 의 속성 설정에 따라 Enterprise Manager 가 시작됩니다. 이러한 속성은 Introscope Enterprise Manager.lax 에 설명되어 있습니다.

UNIX 에서 Enterprise Manager 시작

UNIX 환경에서 Enterprise Manager 를 실행하는 경우에는 Enterprise Manager 를 수동으로 시작하거나 *nohup* 모드로 실행할 수 있습니다.

UNIX 에서 수동으로 Enterprise Manager 시작

UNIX 에서 Enterprise Manager 를 수동으로 시작하려면

- UNIX 에서 Enterprise Manager 를 수동으로 시작하려면 명령 프롬프트에 다음을 입력하여 *Introscope_Enterprise_Manager* 를 실행합니다.

```
'./Introscope Enterprise Manager'
```

Enterprise Manager 는 [속성 파일 참조](#) (페이지 437)에 설명된 대로 <EM_Home>의 속성 설정에 따라 시작됩니다.

Enterprise Manager 출력은 UNIX 셸에 나타납니다. 다음 단원에 설명된 대로 Enterprise Manager 를 *nohup* 모드에서 시작하지 않은 경우 셸에는 사용자 입력이 허용되지 않습니다.

UNIX 에서 Enterprise Manager 제어 스크립트 실행

서버 응용 프로그램 상태를 시작, 중지 및 확인하는 데 사용되는 제어 스크립트를 실행하여 Enterprise Manager 를 관리할 수 있습니다. `./Introscope Enterprise Manager` 명령을 직접 사용하는 대신에 `EMCtrl.sh startup` 스크립트를 사용하여 Enterprise Manager 를 시작 및 중지할 수 있습니다.

UNIX 에서 Enterprise Manager 제어 스크립트를 실행하려면

`bin` 디렉터리에서 다음 명령을 사용합니다.

- `./EMCtrl.sh start` - Enterprise Manager 를 시작합니다.
- `./EMCtrl.sh stop` - Enterprise Manager 를 중지합니다.
- `./EMCtrl.sh status` - Enterprise Manager 의 상태를 제공합니다.
- `./EMCtrl.sh help` - 지원되는 스크립트 옵션을 표시합니다.

UNIX 에서 nohup 모드로 Enterprise Manager 실행

UNIX `nohup` 명령은 하나의 명령을 실행하지만, `HUP(hangup)` 신호의 동작을 억제하여 명령을 실행한 사용자가 로그아웃한 후에도 계속해서 해당 명령이 실행될 수 있도록 합니다. 이 경우 정상적으로 터미널로 전달되는 출력은 `nohup.out` 라는 파일로 이동합니다.

UNIX 에서 nohup 모드로 Enterprise Manager 를 실행하려면

1. `IntroscopeEnterpriseManager.lax` 파일(`<EM_Home>/` 디렉터리에 있음)에서 `lax.stdin.redirect` 속성을 공백으로 설정하고 파일을 저장합니다.
2. `IntroscopeEnterpriseManager.properties` 파일(`<EM_Home>/config` 디렉터리에 있음)에서 `introscope.enterprisemanager.disableInteractiveMode` 속성을 `true` 로 설정하고 파일을 저장합니다.
3. 다음 명령으로 Enterprise Manager 를 시작합니다.


```
nohup Introscope_Enterprise_Manager&
```

참고: 위에서 설명한 구성을 수행하지 않았으면 `nohup` 모드로 Enterprise Manager 를 실행하지 마십시오. 그렇지 않으면 Enterprise Manager 가 시작되지 않거나, 시작 시 과도한 시스템 리소스를 소비할 수 있습니다.

다른 JVM 을 사용하도록 Enterprise Manager 구성

기본적으로 Introscope 구성 요소는 함께 제공된 JVM 을 사용합니다. 이 단원에서는 다른 JVM 을 사용하도록 Enterprise Manager 를 구성하는 방법을 설명합니다.

- *Introscope Enterprise Manager.exe* 를 사용하여 Enterprise Manager 를 시작하는 경우 원하는 JVM 실행 파일을 가리키도록 *Introscope Enterprise Manager.lax* 의 *lax.nl.current.vm* 속성을 편집합니다.
 - 실행 파일의 절대 또는 상대 경로를 사용할 수 있습니다.
 - Windows 에서 백슬래시를 이스케이프하고 *java* 대신에 JVM 실행 파일 확장명을 포함하여 *java.exe* 로 지정합니다.
- Enterprise Manager 를 Windows 서비스로 실행하는 경우 원하는 JVM 실행 파일을 가리키도록 *EMService.conf* 의 *wrapper.java.command* 속성을 편집합니다.
 - 절대 경로를 사용할 수 있는데, 이 경우 백슬래시를 이스케이프해야 합니다.
 - 상대 경로도 사용할 수 있는데, 이 경우 UNIX 슬래시를 사용하고 도트와 슬래시(./)로 시작하는 것이 좋습니다.
 - 실행 파일은 *java.exe* 가 아닌 *java* 입니다.
- AS/400 에서 *runem.sh* 스크립트를 사용하여 Enterprise Manager 를 시작하는 경우 원하는 JVM 루트 디렉터리를 가리키도록 *runem.sh* 의 *JAVA_HOME* 변수를 편집합니다.
 - 실행 파일의 상대 경로가 아닌 절대 경로를 사용합니다.

Enterprise Manager 로그 파일 정보

Enterprise Manager 로그 파일인

IntroscopeEnterpriseManager.log(*<EM_Home>/logs* 디렉터리에 있음)에는 Introscope, CA CEM 및 APM 데이터베이스가 어떻게 실행되고 있는지에 대한 정보와 오류 조건이 기록됩니다. 예를 들어 시작 및 종료에 대한 메시지, 특정 유형의 과도한 오버헤드, 타사 라이브러리, Enterprise Manager 와의 CA CEM 통신, 특정 Introscope 및 CA CEM 속성에 대한 데이터 등이 기록됩니다.

Enterprise Manager 로깅 속성을 구성할 수 있습니다. 자세한 내용은 [로깅](#) (페이지 448)을 참조하십시오.

날짜 또는 크기별로 Enterprise Manager 로그 롤링

날짜나 크기를 기준으로 Enterprise Manager 로그를 롤링하여 지정된 일수의 정보만 보관하고 나머지는 삭제할 수 있습니다.

Enterprise Manager 로그 파일을 롤링하려면

1. <EM_Home>\config 디렉터리에 있는 *IntroscopeEnterpriseManager.properties* 파일을 엽니다.
2. Logging Configuration 섹션을 찾습니다.
3. 원하는 로그 롤링을 수행하도록 속성을 수정합니다. 아래의 세부 지침을 참조합니다.
4. *IntroscopeEnterpriseManager.properties* 파일을 저장하고 닫습니다.
원하는 로그 롤링 동작에 따라 다음 속성을 설정합니다.

로그 파일을 날짜별로 롤링하거나 매일 롤링하려면

- 다음 속성을 수정합니다.
 - *log4j.appender.logfile=com.wily.org.apache.log4j.DailyRollingFileAppender*
 - *log4j.appender.logfile.DatePattern*

이러한 속성은 함께 작동하여 날짜를 기준으로 Enterprise Manager 로그 파일을 롤링합니다. *log4j.appender.logfile.DatePattern* 은 *log4j.appender.logfile=com.wily.org.apache.log4j.DailyRollingFileAppender* 속성이 수행하는 로그 롤링 기간을 정의합니다.

예를 들어 다음 구성을 사용하면 로그 파일이 매일 롤링됩니다.

```
log4j.appender.logfile=com.wily.org.apache.log4j.DailyRollingFileAppender
log4j.appender.logfile.DatePattern='yyyy-MM-dd'
```

로그 파일을 시간 간격별로 롤링하려면

- `log4j.appender.logfile.DatePattern` 속성을 수정합니다. 이 Enterprise Manager 속성은 시간을 기준으로 Enterprise Manager 로그 파일을 롤링하는 시기를 결정합니다.
여기서는 두 가지 예제를 설명합니다.
 - 다음 구성을 사용하면 로그 파일이 매시간 롤링됩니다.
`log4j.appender.logfile.DatePattern='.'yyyy-MM-dd-hh`
 - 다음 구성을 사용하면 로그 파일이 매일 자정에 롤링됩니다.
`log4j.appender.logfile=com.wily.org.apache.log4j.DailyRollingFileAppender`
`log4j.appender.logfile.DatePattern='.'yyyy-MM-dd`

로그 파일을 로그 크기와 수량별로 롤링하려면

- 다음 속성을 수정합니다.
 - `log4j.appender.logfile.MaxBackupIndex`
이 속성은 Enterprise Manager 가 보관하는 백업 로그 파일 수를 결정합니다.
 - `log4j.appender.logfile.MaxFileSize`.
이 속성은 최대 로그 파일 크기를 결정합니다.

예를 들어 다음 구성을 사용하면 최대 3 개의 백업/롤링된 Enterprise Manager 로그가 보관되고 각 로그의 최대 크기는 2 킬로바이트입니다.

```
log4j.appender.logfile.MaxBackupIndex=3
log4j.appender.logfile.MaxFileSize=2KB
```

Enterprise Manager config 디렉터리 구성

Introscope 의 단일 인스턴스를 사용하여 여러 Enterprise Manager 를 실행하려는 경우 각 Enterprise Manager 마다 별도의 구성 디렉터리를 생성할 수 있습니다. 각 Enterprise Manager 마다 `config`, `logs`, `data` 및 `traces` 디렉터리의 복사본을 만드십시오. `config` 디렉터리의 각 복사본에서 `IntroscopeEnterpriseManager.properties` 파일의 적절한 속성이 `config`, `logs`, `data` 및 `traces` 디렉터리의 복사본을 가리키도록 설정하십시오.

별도의 구성 디렉터리를 생성하면 각 Enterprise Manager 마다 별개의 config, logs, data 및 traces 디렉터리를 유지 관리하면서 모든 디렉터리를 하나의 Introscope 인스턴스 내에서 유지할 수 있습니다.

Enterprise Manager 에 대해 다른 구성 디렉터리를 지정하려면

1. *IntroscopeEnterpriseManager.properties* 파일을 열고 다음 속성을 수정합니다.

```
introscope.enterprisemanager.directory.config=config
```

기본 디렉터리는 Introscope 를 처음 설치할 때 생성된 구성 디렉터리인 *config* 입니다. 절대 경로(예: *C:\Introscope\em1\config*)나 Introscope 설치 디렉터리에 대한 상대 경로(예: *config2*)를 사용하여 이 디렉터리의 위치를 변경합니다. 예: *introscope.enterprisemanager.directory.config=C:\Introscope\em1\config*

참고: Windows 환경에서 경로가 제대로 작동하려면 백슬래시를 이스케이프(중첩)해야 합니다.

2. 변경된 *IntroscopeEnterpriseManager.properties* 파일을 저장합니다.
3. *Introscope Enterprise Manager.lax* 파일을 열고 다음 속성을 수정합니다.

```
lax.nl.java.option.additional
```

이 속성은 Java 명령줄을 수정하며 여러 속성을 포함할 수 있습니다. 1 단계에서 선택한 *config* 파일의 위치를 사용합니다. 예:

```
lax.nl.java.option.additional=-Xms512m -Xmx1024m -Djava.awt.headless=false  
-Dcom.wily.introscope.em.properties=C:\Introscope\em1\config
```

참고: 이 속성은 Enterprise Manager 속성 파일을 포함하는 디렉터리를 가리키거나 *IntroscopeEnterpriseManager.properties* 파일을 직접 가리킬 수 있습니다. 예:

```
-Dcom.wily.introscope.em.properties=C:\Introscope\em1\config
```

또는

```
-Dcom.wily.introscope.em.properties=  
C:\Introscope\em1\config\IntroscopeEnterpriseManager.properties
```

4. *Introscope Enterprise Manager.lax* 파일의 변경 사항을 저장합니다.
5. Enterprise Manager 를 다시 시작합니다.

Enterprise Manager 중지

Enterprise Manager 를 중지하는 경우

- 에이전트의 데이터 보고가 중지됩니다.
- SmartStor 가 데이터를 저장하지 않습니다.
- Workstation 에서 로그아웃됩니다.
- Enterprise Manager 에 대한 사용자 연결이 모두 끊깁니다.

터미널 창에서 Enterprise Manager 중지

Enterprise Manager 터미널 창에 다음을 입력하십시오.

```
iscopeshutdown
```

참고: 이 명령을 사용하려면 대화식 모드가 사용되도록 설정해야 합니다.

Enterprise Manager 속성 파일에서

introscope.enterprisemanager.disableInteractiveMode 를 *false* 로 설정하십시오.

자세한 내용은 [속성 파일 참조](#) (페이지 437)를 참고하십시오.

Workstation 에서 Enterprise Manager 중지

Enterprise Manager 에 대한 종료 권한이 있는 경우 Workstation 의 관리 모듈 편집기 창에서 "Manager", "Enterprise Manager 종료"를 차례로 선택하여 Enterprise Manager 를 중지할 수 있습니다.

Enterprise Manager 자동 종료

디스크 공간 부족을 나타내는 디스크 쓰기 오류가 감지되면 Enterprise Manager 가 자동으로 종료됩니다. 장애 조치를 구성한 경우 에이전트가 다른 Enterprise Manager 로 장애 조치될 수 있습니다. 자세한 내용은 *CA APM Java Agent 구현 안내서* 또는 *CA APM .NET 에이전트 구현 안내서*를 참조하십시오.

계획되지 않은 종료 후 다시 시작

중요! 이 항목은 CA APM에만 적용됩니다. TIM이 없는 독립 실행형 CA Introscope를 사용 중인 경우 이 항목을 건너뛰십시오.

대부분의 상황에서 Enterprise Manager를 다시 시작하는 작업은 일반적으로 시작하는 작업과 동일합니다. 그러나 계획된 종료가 아니라 오류가 발생하여 Enterprise Manager가 중지되었으면 다시 시작하기 전에 일부 파일을 삭제해야 할 수 있습니다.

과다한 부하나 파일 처리 오류로 인해 Enterprise Manager가 자동으로 종료(작동 중단)된 경우 <EM_Home>/cem/tess/badfiles 디렉터리에 처리되지 않은 파일이 남아 있을 수 있습니다. 이러한 파일이 있는 상태로 Enterprise Manager가 다시 시작되면 다시 시작할 때 해당 파일이 처리됩니다. 이러한 파일에 있는 오류나 이러한 파일로 인한 부하 때문에 종료가 발생한 경우 Enterprise Manager가 다시 시작되어 해당 파일 처리를 다시 시작하자마자 또다시 작동 중단이 발생할 수 있습니다.

해결 방법은 Enterprise Manager를 다시 시작하기 전에 이 디렉터리에서 파일을 삭제하는 것입니다.

작동 중단 후 Enterprise Manager를 다시 시작하려면

중요! 이 절차에 설명된 대로 파일을 삭제하면 일부 데이터가 손실될 수 있습니다. 최근 결합 정보, 고객 경험 메트릭 및 통계를 잃을 수 있습니다.

1. TIM 수집 서비스를 실행 중인 Enterprise Manager에서 <EM_Home>/cem/tess/badfiles 디렉터리에 있는 파일을 삭제합니다.
파일은 *btstats-2010-01-05-23_26_13-172.16.252.20.xml* 및 *defect-1262733968000057712-172.16.252.20.xml* 과 같은 이름의 XML 파일입니다.
TIM 수집 서비스를 포함한 Enterprise Manager 서비스에 대한 자세한 내용은 [Enterprise Manager 서비스 배포](#) (페이지 282)를 참조하십시오.
2. 다음 항목 중 하나에 설명된 대로 Enterprise Manager를 시작합니다.
 - [Windows에서 Enterprise Manager 시작](#) (페이지 27)
 - [UNIX에서 Enterprise Manager 시작](#) (페이지 30)
 - OS/400에서 Enterprise Manager 시작

Enterprise Manager 의 여러 작동 중단 문제 해결:

증상

TIM 수집 서비스를 실행 중인 Enterprise Manager 가 작동 중단되었다가 다시 시작될 때 다시 작동 중단됩니다.

가능한 원인은 Enterprise Manager 에 과도한 부하를 주거나 오류를 포함하는 TIM 관련 데이터 파일입니다.

해결 방법

[계획되지 않은 종료 후 다시 시작](#) (페이지 37)에 설명된 대로 문제가 있는 파일을 삭제하십시오.

Enterprise Manager 셸 및 터미널 창 명령

Enterprise Manager 를 실행 중인 경우 *lax.stdin.redirect*(속성 파일 참조에 정의되어 있음)가 *console* 로 설정되어 있으면 Enterprise Manager 터미널 창 또는 셸에 다음 명령을 입력할 수 있습니다.

명령	Result
<code>iscopedebugpolling [true false] [delay in seconds]</code>	디버깅 정보를 로그에 주기적으로 보고합니다.
<code>iscopehelp</code>	도움말 화면을 표시합니다.
<code>iscopeshutdown</code>	Enterprise Manager 종료

참고: 이러한 명령을 사용하려면 대화식 모드가 사용되도록 설정해야 합니다. Enterprise Manager 속성 파일에서 *introscope.enterprisemanager.disableInteractiveMode* 를 *false* 로 설정하십시오. 자세한 내용은 [속성 파일 참조](#) (페이지 437)를 참고하십시오.

제 3 장: Enterprise Manager 통신 구성

이 단원에서는 Enterprise Manager 와 Introscope 환경 내 다른 구성 요소 간의 통신 방법, 기본 통신 동작 및 Enterprise Manager 통신 구성 옵션에 대한 정보를 제공합니다.

이 섹션은 다음 항목을 포함하고 있습니다.

[기본 Enterprise Manager 통신 채널 \(페이지 39\)](#)

[방화벽을 통과하여 Enterprise Manager 에 연결 \(페이지 43\)](#)

[HTTPS 용으로 Enterprise Manager 웹 서버 구성 \(페이지 44\)](#)

기본 Enterprise Manager 통신 채널

기본적으로 Enterprise Manager 는 포트 5001 에서 에이전트, Workstation, WebView 및

Enterprise Manager 클러스터와 통신합니다.

Enterprise Manager 에 대한 모든 소켓 통신이 난독 처리되고 암호가 암호화됩니다.

Enterprise Manager 속성 파일에서 통신 채널과 해당 채널 용도를 정의하는 속성은 다음과 같습니다.

- introscope.enterprisemanager.serversocketfactory.<ChannelName>
- introscope.enterprisemanager.port.<ChannelName>
- introscope.enterprisemanager.serversockets.reuseaddr
- introscope.enterprisemanager.enabled.channels

Enterprise Manager 와 통신하는 에이전트 각각에는 일치하는 값을 지정해야 하는 유사한 속성이 있습니다.

마찬가지로, `WebView` 속성 파일의 `introscope.webview.enterprisemanager.tcp.port` 속성에서 Enterprise Manager 포트를 지정합니다.

참고: .NET 에이전트는 Enterprise Manager 에 대한 직접 SSL 연결을 지원하지 않습니다. 참고: 에이전트 속성에 대한 자세한 내용은 사용자 환경에 해당하는 *CA APM Java Agent 구현 안내서* 또는 *CA APM .NET 에이전트 구현 안내서*를 참조하십시오.

추가 정보:

[Enterprise Manager 클러스터링 이해 \(페이지 93\)](#)

사용 중인 포트에 통신 채널 재바인딩

실제로 소켓을 사용 중인 것이 없는데도 여전히 메모리가 사용되고 있어 소켓을 사용할 수 없게 만드는 소켓 상태가 있습니다. `FIN_WAIT`, `TIME_WAIT` 등이 이러한 상태의 예입니다.

`introscope.enterprisemanager.serversockets.reuseaddr (페이지 442)` 속성을 통해 Enterprise Manager 통신 채널을 사용 중인 로컬 포트에 재바인딩할 수 있습니다. Enterprise Manager 소켓이 사용할 수 없는 상태로 멈춰 있더라도 여전히 Enterprise Manager 를 시작하려는 경우에 이 기능을 사용하십시오.

참고: 이 속성은 기본적으로 사용되지 않도록 설정하되, 소켓이 사용할 수 없는 상태인 경우에만 사용하십시오. 포트가 사용 중인 타당한 이유(예: 동일한 컴퓨터의 수집기가 이미 포트에 바인딩되어 있는 경우)가 있으므로 Enterprise Manager 가 시작된 후에는 이 속성이 사용되지 않도록 설정하십시오.

SSL 구성

SSL 에 대한 Enterprise Manager 구성은

IntroscopeEnterpriseManager.properties 에서 보안 통신 채널이 사용되도록 설정하여 수행됩니다. 기본 비보안 채널 외에도 이 구성을 수행할 수 있습니다.

다음 예제에서는 보안 통신 채널과 비보안 통신 채널이 모두 사용되도록 설정합니다. 기본 비보안 수신기는 포트 5001 에서 설정되고 보안 수신기는 포트 5443 에서 설정됩니다.

```
# The enabled communication channels.
introscope.enterprisemanager.enabled.channels=channel1, channel2

# The default communication channel.
introscope.enterprisemanager.serversocketfactory.channel1=com.wily.isengard.p
ostofficehub.link.net.server.DefaultServerSocketFactory
introscope.enterprisemanager.port.channel1=5001

# The secure communication channel.
introscope.enterprisemanager.serversocketfactory.channel2=com.wily.isengard.p
ostofficehub.link.net.server.SSLServerSocketFactory
introscope.enterprisemanager.port.channel2=5443
# Location of a keystore containing certificates for authenticating the Enterprise
Manager to clients.
# Either an absolute path or a path relative to the config directory.
# On Windows, backslashes must be escaped. 예:
#
introscope.enterprisemanager.keystore.channel1=C:\\Introscope\\config\\intern
al\\server\\keystore
introscope.enterprisemanager.keystore.channel2=internal/server/keystore
# The password for the keystore.
# Set this property to true to enable encryption of
introscope.enterprisemanager.keystore.password.channel2
# Once introscope.enterprisemanager.keystore.password.channel2 is encrypted,
# this property is automatically set to false.
#
# To change the existing password, enter the new password and set this property
to true.
# Note: If this property is set to true and the password is not changed, the existing
encrypted password will be encrypted again.
# If password field for a new channel is configured, add the corresponding
# plaintextpassword field and set it to true to enable encryption.
introscope.enterprisemanager.keystore.password.channel2.plaintextpassword=true
introscope.enterprisemanager.keystore.password.channel2=password
# Location of a truststore containing trusted client certificates.
```

```
# Either an absolute path or a path relative to the config directory.
# On Windows, backslashes must be escaped. 예:
#
introscope.enterprisemanager.truststore.channel1=C:\\Introscope\\config\\inte
rnal\\server\\keystore
# A truststore is only needed if client authentication is required.
# Set this property to true to enable encryption of
introscope.enterprisemanager.trustpassword.channel2
# Once introscope.enterprisemanager.trustpassword.channel2 is encrypted,
# this property is automatically set to false.
#
# To change the existing password, enter the new password and set this property
to true.
# Note: If this property is set to true and the password is not changed, the existing
encrypted password will be encrypted again.
# If password field for a new channel is configured, add the corresponding
# plaintextpassword field and set it to true to enable encryption.
# introscope.enterprisemanager.trustpassword.channel2.plaintextpassword=false
# The password for the truststore
#introscope.enterprisemanager.trustpassword.channel2=password
# If no truststore is specified, the Enterprise Manager trusts all client
certificates.
```

SSL 속성 규칙

기본 채널 외에도 보안 통신 채널을 사용하도록 설정하여 *IntroscopeEnterpriseManager.properties* 에서 SSL 서버 소켓으로 Enterprise Manager 를 구성해야 합니다.

SSL 속성을 구성하는 경우 다음 규칙을 따르십시오.

- keystore 속성은 키 저장소의 위치입니다. 여기에는 클라이언트에 대해 Enterprise Manager 자체를 인증하는 데 사용되는 인증서가 포함되어야 합니다. Enterprise Manager 의 기본 키 저장소에는 본질적으로 신뢰할 수 없는 자체 서명된 인증서가 포함되어 있습니다. 이는 기본적으로 Workstation 과 에이전트가 서버 인증서 유효성을 검사하지 않기 때문에 문제가 되지 않습니다.
- keystore 속성은 *config* 디렉터리의 상대 경로이거나 절대 경로입니다.
- *needclientauth* 속성을 *true* 로 설정한 경우 Enterprise Manager 는 클라이언트 인증을 요구합니다.
 - 신뢰 저장소로 Enterprise Manager 를 구성해야 합니다.
 - Enterprise Manager 가 신뢰할 수 있는 인증서를 포함하는 키 저장소로 에이전트와 Workstation 을 구성해야 합니다.

- `needclientauth = true` 인 경우 신뢰 저장소를 구성하지 않으면 Enterprise Manager 가 시작되지 않습니다.
- 이 경우 `truststore` 속성을 설정해야 합니다.
- `truststore` 속성은 신뢰 저장소의 위치입니다. 신뢰 저장소는 신뢰할 수 있는 클라이언트의 인증서를 포함하며 클라이언트를 인증해야 하는 경우에만 필요합니다.
 - 지정된 신뢰 저장소가 없는 경우 모든 클라이언트 인증서가 신뢰됩니다.
- `ciphersuites` 속성은 사용하도록 설정된 암호 그룹을 설정하는 데 사용됩니다.
 - 이를 통해 익명 인증이 사용되도록 설정하거나 데이터 암호화를 방지할 수 있습니다. 예를 들어 익명 인증을 위해 암호 그룹을 `SSL_DH_anon_WITH_RC4_128_MD5` 로 설정하십시오. 예:
`introscope.enterprisemanager.ciphersuites.channel2=SSL_DH_anon_WITH_RC4_128_MD5`
 - 특정 JSSE 구현에는 익명 인증을 허용하는 사용 가능한 암호 그룹(모두 "anon"을 포함함)이 여러 개 있습니다. 그러나 암호 그룹은 클라이언트와 서버 모두에 공통으로 적용되며 클라이언트와 서버 모두에서 사용되도록 설정됩니다.
 - 데이터를 암호화하지 않는 암호 그룹을 지정하십시오. 예:
`introscope.enterprisemanager.ciphersuites.channel2=SSL_RSA_WITH_NULL_SHA`

방화벽을 통과하여 Enterprise Manager 에 연결

HTTP 터널링은 기본적으로 사용됩니다. 터널링 기술을 사용하면 한 네트워크의 연결을 통해 다른 네트워크의 데이터를 보낼 수 있습니다.

Workstation 에서 터널링 전송을 사용하려면 Enterprise Manager 의 포함된 웹 서버용 포트에 연결하십시오. 기본적으로 포트는 8081 입니다. Enterprise Manager 속성 파일의 `introscope.enterprisemanager.webserver.port` 속성으로 포트를 구성할 수 있습니다. 자세한 내용은 [introscope.enterprisemanager.webserver.port](#) (페이지 442)를 참조하십시오.

Enterprise Manager 에 터널링을 사용하는 것 외에도 터널링 기술을 사용하여 정보를 보내도록 에이전트를 구성할 수 있습니다. 이 기능을 사용하면 에이전트가 원격으로 Enterprise Manager 에 연결할 수 있습니다. 에이전트 HTTP 터널링에 대한 자세한 내용은 *CA APM Java Agent* 구현 안내서를 참조하십시오.

HTTPS 용으로 Enterprise Manager 웹 서버 구성

Jetty 구성 파일을 사용하여 HTTPS 용으로 Enterprise Manger 웹 서버를 구성할 수 있습니다. Jetty 파일은 고급 구성을 위해 제공되며 <EM_Home>/config 디렉터리에 있습니다.

이 파일은 IntroscopeEnterpriseManager.properties 파일에 있는 introscope.enterprisemanager.webserver.jetty.configurationFile 속성의 주석 처리를 제거하여 활성화됩니다.

구성에 대한 자세한 내용은 다음 항목을 참조하십시오.

- [기본 Jetty 구성 파일](#) (페이지 45) 및 [Jetty-config.xml 파일 수정](#) (페이지 45)
- <http://docs.codehaus.org/display/JETTY/How+to+configure+SSL> - Jetty 웹 사이트에 액세스하여 추가 정보 참조

HTTPS 작동 방식 이해

Enterprise Manager 웹 서버는 SSL 을 통한 HTTP 터널링을 지원하는데, 이 보안 수단은 Enterprise Manager 에 포함된 Jetty 웹 서버에 대한 Jetty XML 구성 파일(선택 사항)을 통해 구현됩니다.

시작할 때 Enterprise Manager 는 포트 8444 에서 보안 수신기를 설정하는 Jetty 구성 파일을 로드합니다. 이 보안 수신기는 Workstation 및 에이전트가 Enterprise Manager 웹 서버를 통해 HTTPS 터널링을 사용하여 Enterprise Manager 에 액세스하도록 허용합니다. 기본 Jetty 구성 파일은 em-jetty-config.xml 입니다.

IntroscopeEnterpriseManager.properties 파일의 [introscope.enterprisemanager.webserver.jetty.configurationFile](#) (페이지 445) 속성을 사용하여 Jetty 구성 파일의 이름과 위치를 구성할 수 있습니다.

The introscope.enterprisemanager.webserver.port 속성은 IntroscopeEnterpriseManager.properties 파일에 있는 introscope.enterprisemanager.webserver.port 속성과 함께 동작합니다. Enterprise Manager 는 Enterprise Manager 가 Jetty 구성 파일을 로드할 때 introscope.enterprisemanager.webserver.port 속성에 정의된 보안되지 않은 수신기를 생성하지 않습니다. 하지만 Jetty 구성 파일에 보안되지 않은 수신기를 구성할 수 있습니다.

경고: em-jetty-config.xml 파일에서 `introscope.enterprisemanager.webserver.jetty.configurationFile` 속성 및 보안되지 않은 수신기 포트에서 모두 주석 처리를 제거하면 CA APM 보안이 취약해질 수 있습니다. 이러한 두 구성을 수행하기 전에 회사의 응용 프로그램 보안 담당자와 상의하십시오.

기본 Jetty 구성 파일

기본 em-jetty-config.xml 파일은 `<EM_Home>/config` 디렉터리에서 제공됩니다.

em-jetty-config.xml 파일 수정

em-Jetty-config.xml 파일에서 SSL의 여러 구성 요소를 수정할 수 있습니다.

Jetty에 대한 자세한 내용은

<http://docs.codehaus.org/display/JETTY/How+to+configure+SSL>을 참조하십시오.

- 다음 예제와 같이 `port` 특성의 값을 변경하여 HTTPS 포트를 기본값인 8444에서 다른 값으로 변경하십시오.
`<Set name="port">8444</Set>`
- `introscope.config` 시스템 속성은 `config` 디렉터리의 위치를 지정합니다. 이 위치는 구성 가능합니다. Enterprise Manager 웹 서버는 시작할 때 `introscope.config` 시스템 속성을 설정합니다.
- 기본적으로 SSL 수신기는 `config` 디렉터리를 기준으로 한 상대 경로인 `/internal/server/keystore`에 있는 키 저장소를 사용하도록 구성되어 있습니다. 이 키 저장소에는 신뢰할 수 없는 자체 서명된 인증서가 포함되어 있습니다. 공인 CA(인증 기관)에서 서명된 인증서를 포함하는 사용자 고유의 키 저장소로 이 인증서를 대체하는 것이 좋습니다.
- 기본 키 저장소 암호는 `password`입니다. em-jetty-config.xml 및 webview-jetty-config.xml의 일반 텍스트 암호는 기본적으로 난독 처리됩니다. 난독 처리된 암호는 OBF:으로 시작됩니다. 일반 텍스트 암호는 OBF:을 제거하여 제공할 수 있습니다. 자세한 내용은 <http://docs.codehaus.org/display/JETTY/How+to+configure+SSL>을 참조하십시오.

- 기본적으로 SSL 은 자체 서명된 인증서를 허용하도록 구성되어 있으며 클라이언트 URL 에 있는 호스트 이름이 디지털 인증서에 있는 호스트 이름과 일치하는지 확인하지 않습니다. 이와 같은 구성 때문에 SSL 이 기본 키 저장소에 있는 신뢰할 수 없는 인증서로 즉시 작동할 수 있습니다. 보안이 강화된 인증이 필요한 경우에는 신뢰할 수 있는 인증서가 포함된 키 저장소를 생성한 후 XML 에 다음과 같은 특성을 설정하여 기본 키 저장소를 사용자 개인의 키 저장소로 대체하십시오.

```
<Set name="validateCertificates">true</Set>
<Set name="verifyHostnames">true</Set>
<Set name="keystore"><SystemProperty name="introscope.config"
default="./config" />/internal/server/keystore</Set>
<Set name="password">password</Set>
```

- 또한 클라이언트 인증을 요구하려면 클라이언트 인증서를 포함하는 신뢰 저장소를 생성하고 XML 에서 다음 특성을 설정하여 기본 신뢰 저장소를 사용자 고유의 신뢰 저장소로 대체해야 합니다.

```
<Set name="needClientAuth">true</Set>
<Set name="truststore"><SystemProperty name="introscope.config"
default="./config" />/internal/server/keystore</Set>
<Set name="trustPassword">password</Set>
```

- 클라이언트 인증을 사용하려면 Enterprise Manager 웹 서버가 신뢰할 수 있는 인증서가 포함된 키 저장소를 사용하여 에이전트와 Workstation 을 구성해야 합니다.

사용되도록 설정된 암호 그룹을 설정하려면 다음과 같이 *cipherSuites* 특성을 암호 그룹 목록으로 설정하십시오.

```
<Set name="cipherSuites">
  <Array type="java.lang.String">
    <Item>SSL_DH_anon_WITH_RC4_128_MD5</Item>
  </Array>
</Set>
```

SSL 을 사용하려면 에이전트와 Workstation 이 Enterprise Manager 와 공통으로 암호 그룹을 사용하도록 설정해야 합니다. 다음과 같은 작업을 수행하도록 암호 그룹을 제한할 수 있습니다.

- 약한 암호 그룹의 취약성 방지
- 익명 연결 허용
- 데이터 암호화 안 함
- Enterprise Manager 는 maxThreads 속성을 사용하여 Enterprise Manager 가 처리할 수 있는 HTTPS 에이전트 연결 수를 제한합니다. Enterprise Manager 는 충분한 스레드가 없을 경우 연결된 에이전트 또는 프로세스 메트릭을 인식하지 못합니다.

HTTPS 를 사용하는 경우 Enterprise Manager 는 `maxThreads` 속성에 구성되어 있는 수의 에이전트만 처리합니다. 허용되는 에이전트 연결 수는 `apm-events-thresholds-config.xml` 파일의

[introscope.enterprisemanager.agent.connection.limit](#) 속성 (페이지 496)에 구성됩니다. `maxThreads` 값은

`introscope.enterprisemanager.agent.connection.limit` 값 이상이어야 합니다. 에이전트가 HTTPS 를 통해 연결되도록 구성된 경우 스레드가 충분하지 않으면 일부 HTTPS 에이전트가 클라이언트에 나타나지 않거나 메트릭을 보고하지 않을 수 있습니다.

참고: `maxThreads` 속성으로 Enterprise Manager 가 처리하는 에이전트 수를 제한하는 경우 Enterprise Manager 및 에이전트 로그에는 처리되지 않는 에이전트에 대한 오류, 경고 또는 메시지가 포함되지 않습니다.

em-Jetty-config.xml 을 수정하여 기본 헤더 크기 재설정

CEM 콘솔을 액세스할 때 종종 빈 페이지가 표시되는 경우 4KB 인 기본 요청 헤더 크기 제한을 재설정할 수 있습니다. 헤더 크기 제한은 `em-jetty-config.xml` 파일에서 재설정합니다.

다음 단계를 따르십시오.

1. MOM 에서 `em-jetty-config.xml` 파일을 찾아 이 파일을 텍스트 편집기에서 엽니다.
2. 다음 행이 있는 섹션을 찾습니다.
`<New class="com.wily.webserver.NoNPESocketConnector">`
3. "NoNPESocketConnector"를 다음 값으로 수정합니다.

```
<set name="headerBufferSize">8192</Set>"
<Set name="RequestBufferSize">16384</Set>"
```

수정된 섹션의 코드 조각은 다음과 같습니다.

```
<Call name="addConnector">
  <Arg>
    <New class="com.wily.webserver.NoNPESocketConnector">
      <Set name="port">8081</Set>
      <set name="headerBufferSize">8192</Set>
      <Set name="RequestBufferSize">16384</Set>
      <Set name="ThreadPool">
        <New class="org.mortbay.thread.BoundedThreadPool">
          <Set name="minThreads">10</Set>
          <Set name="maxThreads">100</Set>
          <Set name="maxIdleTimeMs">60000</Set>
        </New>
      </Set>
    </New>
  </Arg>
</Call>
```

4. 파일을 저장하고 닫습니다.
5. 각 MOM 및 수집기의 IntroscopeEnterpriseManager.properties 파일을 찾습니다.
6. 다음 행의 주석 처리를 제거합니다.
introscope.enterprisemanager.webserver.jetty.configurationFile=
em-jetty-config.xml
7. IntroscopeEnterpriseManager.properties 파일을 저장하고 닫습니다.

제 4 장: Enterprise Manager 데이터베이스 구성

이 단원에서는 CA Introscope 의 내부 데이터베이스에 대한 구성 옵션을 설명합니다.

APM 데이터베이스에 대한 자세한 내용은 [APM 데이터베이스 관리](#) (페이지 49)를 참조하십시오.

이 섹션은 다음 항목을 포함하고 있습니다.

[APM 데이터베이스 관리](#) (페이지 49)

[SmartStor 데이터 저장소 구성](#) (페이지 66)

[트랜잭션 이벤트 데이터베이스 위치 및 만료 처리 구성](#) (페이지 70)

[기존 저장소 위치 구성](#) (페이지 70)

[SmartStor, 기존 및 트랜잭션 이벤트 데이터 백업](#) (페이지 71)

[SmartStor 도구를 사용하여 SmartStor 데이터 조정](#) (페이지 73)

[SmartStor 메타데이터 정리](#) (페이지 81)

[SmartStor 데이터 및 메타데이터 자르기](#) (페이지 83)

[8.x 데이터를 9.x 로 업그레이드](#) (페이지 87)

APM 데이터베이스 관리

이 장에는 데이터를 APM 데이터베이스로 내보내거나 APM 데이터베이스에서 가져오는 것과 관련된 정보가 포함되어 있습니다. 전체 데이터베이스를 가져오거나 내보낼 수도 있고 구성 데이터만 가져오거나 내보낼 수도 있습니다.

다른 CA Introscope 데이터베이스(SmartStor 및 트랜잭션 이벤트 데이터베이스)에 대한 자세한 내용은 [Enterprise Manager 데이터베이스 구성](#) (페이지 49)을 참조하십시오.

데이터베이스 백업 또는복원

백업 및 복원 기능에는 APM 데이터베이스와 구성 정보를 백업하는 기능이 포함됩니다.

예를 들어 데이터를 보호하기 위해 별도의 컴퓨터에 데이터베이스 복사본을 보관할 수 있습니다. 이렇게 하려면 먼저 데이터베이스를 백업한 다음 데이터베이스 백업 파일을 다른 컴퓨터에 복사하십시오.

APM 데이터베이스 백업 및 복원 프로세스

이 목록에는 CA CEM 데이터 보호와 관련된 주요 작업이 나와 있습니다.

1. [사전 요구 사항 이해](#) (페이지 50)
2. [정기적으로 데이터베이스 백업](#) (페이지 51)
3. [필요한 경우 데이터베이스 복원](#) (페이지 53)

PostgreSQL 데이터베이스용 백업 및 복원 유틸리티는 명령줄에서 실행할 수 있는 배치 파일(또는 셸 스크립트)의 형태로 제공됩니다.

참고: APM 데이터베이스에는 CA CEM 구성 설정, 사용자 및 그룹, 비즈니스 서비스 및 트랜잭션 정의뿐 아니라 응용 프로그램 심사 맵 데이터가 포함됩니다.

백업하거나 복원하기 전에

경고! 복원 기능은 지정된 이름의 데이터베이스를 생성하기 전에 지정된 데이터베이스가 존재하는 경우 해당 데이터베이스를 삭제합니다.

백업과 복원에는 모두 다음이 필요합니다.

- PostgreSQL 데이터베이스를 백업하거나 복원하려면 데이터베이스 스크립트를 실행 중인 컴퓨터에 PostgreSQL 을 설치해야 합니다. 원격 컴퓨터에도 PostgreSQL 이 설치되어 있다면 필요에 따라 원격 컴퓨터에서도 스크립트를 실행할 수 있습니다.

다음 플랫폼 중 하나에서 APM 데이터베이스를 복원하려면

- OS/400(IBM)
- Solaris x86

JAVA_HOME 환경 변수가 dbrestore 스크립트를 실행할 컴퓨터에 설정되어 있는지 확인하십시오.

JRE 1.6 에 해당: JAVA_HOME 환경 변수를 설정하고 JRE 루트 폴더를 가리키도록 설정합니다. JRE 1.6 이상이 필요하고 경로에 공백이 포함될 수 없습니다. 예를 들어 c:\program files\java\jre1.6.0 에 JRE 를 설치한 경우 JAVA_HOME 을 경로의 단축된 버전(예: c:\progra~1\java\jre1.6.0)으로 설정합니다.

데이터베이스 백업

백업 유틸리티는 APM 데이터베이스의 *.backup* 파일을 생성합니다. 백업 파일 이름을 사용자 지정할 수 있습니다. 파일 이름을 지정하지 않으면 스크립트가 데이터베이스 이름과 파일 이름 접미사 *.backup* 을 사용하여 백업 파일을 생성합니다.

APM 데이터베이스를 백업하려면

1. 사용 중인 운영 체제의 database-scripts 디렉터리로 이동합니다.
 - Linux: `<EM_Home>/install/database-scripts/unix/`
 - Windows: `<EM_Home>\install\database-scripts\windows\`
2. 명령줄을 열고 사용 중인 운영 체제의 다음 스크립트를 실행합니다.
 - Windows: `dbbackup-postgres.bat`
 - Linux: `dbbackup-postgres.sh`

다음 구문과 인수를 사용합니다.

```
[dbbackup-postgres.bat | sh dbbackup-postgres.sh][dbserverhostip]
[dbinstalldir] [dbname] [dbuser] [dbpassword] [dbport] [outputfile]
```

다음 인수를 포함합니다.

dbserverhostIP

데이터베이스를 호스팅하는 컴퓨터의 IP 주소입니다. 컴퓨터에서 직접 스크립트를 실행하는 경우 *localhost* 를 지정할 수 있습니다.

dbinstalldir

APM 데이터베이스의 디렉터리 위치입니다.

Linux 의 경우 공백이 포함되어 있으면 경로를 이스케이프하거나 따옴표로 묶어야 합니다. Linux 를 예로 들면 `/root/Introscope Enterprise Manager` 디렉터리를 `/root/Introscope\ Enterprise\ Manager` 로 표현할 수 있습니다.

기본값을 변경하지 않았다면 위치는 다음과 같습니다.

Linux: `opt/database`

Windows: `<EM_Home>\database`

database_name

데이터베이스 인스턴스 이름을 지정합니다. PostgreSQL 을 사용 중인 경우 기본값을 변경하지 않았으면 이 인수를 `cemdb` 로 설정해야 합니다. Oracle 을 사용 중인 경우에는 이 인수를 Oracle SID(시스템 식별자)로 설정해야 합니다.

dbuser

APM 데이터베이스와 연결된 데이터베이스 사용자의 사용자 이름을 지정합니다. PostgreSQL 을 사용 중인 경우 기본값을 변경하지 않았으면 이 인수를 `admin` 으로 설정해야 합니다. Oracle 을 사용 중인 경우에는 이 인수를 APM 데이터베이스 스키마 소유자로 설정해야 합니다.

참고: PostgreSQL 데이터베이스 관리자의 사용자 이름이 아닙니다.

password

APM 데이터베이스와 연결된 데이터베이스 사용자의 암호를 지정합니다.

port_number

데이터베이스가 Enterprise Manager 및 기타 구성 요소와 통신하는 포트 번호를 지정합니다. PostgreSQL 을 사용 중인 경우 기본값을 변경하지 않았으면 이 인수를 `5432` 로 설정해야 합니다. Oracle 과 기본 수신기 포트를 사용 중인 경우에는 이 인수를 `1521` 로 설정해야 합니다.

dbbackupdir

데이터베이스 백업 파일을 저장할 기존 디렉터리 위치입니다. Linux 의 경우 공백이 포함되어 있으면 경로를 이스케이프해야 합니다. Linux 를 예로 들면 */root/Introscope Enterprise Manager* 디렉터리를 */root/Introscope\ Enterprise\ Manager* 로 표현할 수 있습니다.

디렉터리를 묶는 따옴표와 종료 슬래시는 포함하지 않아야 합니다.

outputfile

(선택 사항) 데이터베이스 백업 파일의 이름입니다. 이 매개 변수를 지정하지 않으면 스크립트가 제공된 데이터베이스 이름을 사용하여 *dbname.backup* 이라는 파일을 생성합니다. 백업 파일 이름 접미사는 표준 규칙에 따라 *.backup* 이지만 반드시 이 접미사를 사용해야 하는 것은 아닙니다.

다음은 */opt/database/backups* 디렉터리에 *cemdb.backup* 파일을 생성하는 예제입니다.

```
sh dbbackup-postgres.sh 127.0.0.1 /opt/database cemdb admin quality
5432 ./backups
```

3. 백업 프로세스가 완료되면 확인 메시지가 표시됩니다.

일반적으로 스크립트에서 오류가 발생하는 이유는 다음과 같습니다.

- 데이터베이스 이름이 부정확합니다.
- PostgreSQL 이 설치되지 않았습니다.
- APM 데이터베이스 위치가 부정확합니다.

데이터베이스 복원

복원 유틸리티를 사용하면 이전에 백업한 APM 데이터베이스 백업 파일을 현재 시스템으로 복원할 수 있습니다. 예를 들어 시스템 작동 중단 또는 하드 디스크 오류 후 데이터베이스를 복원하여 복구할 수 있습니다.

경고! 복원 기능은 지정된 이름의 데이터베이스를 생성하기 전에 지정된 데이터베이스가 존재하는 경우 해당 데이터베이스를 삭제합니다.

참고: 데이터베이스가 UNIX 컴퓨터에 있는 경우 복원 프로세스가 실행되면 데이터베이스 업그레이드도 수행됩니다.

참고: 데이터베이스를 복원하는 데 걸리는 시간은 데이터베이스 크기와 직접적인 관련이 있습니다. 큰 데이터베이스를 복원하려면 시간이 오래 걸리고 컴퓨터 용량과 메모리에 따라서도 복원 시간이 좌우됩니다. 예를 들어 1 GB 데이터베이스를 복원하려면 컴퓨터 리소스에 따라 1~2 시간이 걸릴 수 있습니다.

APM 데이터베이스를 복원하려면

1. 데이터베이스에 연결된 사용자가 없는지 확인합니다. 사용자가 연결된 데이터베이스는 복원할 수 없습니다.
2. 사용 중인 운영 체제의 database-scripts 디렉터리로 이동합니다.
 - Linux: `<EM_Home>/install/database-scripts/unix/`
 - Windows: `<EM_Home>\install\database-scripts\windows\`
3. 명령줄을 열고 사용 중인 운영 체제의 다음 스크립트를 실행합니다.
 - Windows: `dbrestore-postgres.bat`
 - Linux: `dbrestore-postgres.sh`

다음 구문과 인수를 사용합니다.

```
[dbrestore-postgres.bat | sh dbrestore-postgres.sh][dbserverhostip]
[dbinstalldir] [dbserviceuser] [dbservicepassword] [dbname] [dbuser]
[dbpassword] [dbport] [backupfile]
```

다음 인수를 포함합니다.

dbserverhostIP

데이터베이스를 호스팅하는 컴퓨터의 IP 주소입니다. 컴퓨터에서 직접 스크립트를 실행하는 경우 `localhost` 를 지정할 수 있습니다.

dbinstalldir

APM 데이터베이스의 디렉터리 위치입니다.

Linux 의 경우 공백이 포함되어 있으면 경로를 이스케이프하거나 따옴표로 묶어야 합니다. Linux 를 예로 들면 `/root/Introscope Enterprise Manager` 디렉터리를 `/root/Introscope\ Enterprise\ Manager` 로 표현할 수 있습니다.

기본값을 변경하지 않았다면 위치는 다음과 같습니다.

Linux: `opt/database`

Windows: `<EM_Home>\database`

dbserviceuser

PostgreSQL 관리자 사용자 이름입니다. 기본적으로 이 이름은 *postgres* 입니다.

dbservicepassword

dbserviceuser 와 연결된 암호입니다. (PostgreSQL 관리자 암호입니다.)

database_name

데이터베이스 인스턴스 이름을 지정합니다. PostgreSQL 을 사용 중인 경우 기본값을 변경하지 않았으면 이 인수를 *cemdb* 로 설정해야 합니다. Oracle 을 사용 중인 경우에는 이 인수를 Oracle SID(시스템 식별자)로 설정해야 합니다.

dbuser

APM 데이터베이스와 연결된 데이터베이스 사용자의 사용자 이름을 지정합니다. PostgreSQL 을 사용 중인 경우 기본값을 변경하지 않았으면 이 인수를 *admin* 으로 설정해야 합니다. Oracle 을 사용 중인 경우에는 이 인수를 APM 데이터베이스 스키마 소유자로 설정해야 합니다.

참고: PostgreSQL 데이터베이스 관리자의 사용자 이름이 아닙니다.

password

APM 데이터베이스와 연결된 데이터베이스 사용자의 암호를 지정합니다.

port_number

데이터베이스가 Enterprise Manager 및 기타 구성 요소와 통신하는 포트 번호를 지정합니다. PostgreSQL 을 사용 중인 경우 기본값을 변경하지 않았으면 이 인수를 5432 로 설정해야 합니다. Oracle 과 기본 수신기 포트를 사용 중인 경우에는 이 인수를 1521 로 설정해야 합니다.

backupfile

디렉터리 위치 및 데이터베이스 백업 파일 이름입니다.

다음은 `/opt/database/backups` 디렉터리에서 `cemdb.backup` 파일을 복원하는 예제입니다.

```
sh dbrestore-postgres.sh 127.0.0.1 /opt/database postgres C@wilyapm90 cemdb
admin quality 5432 ./backups/cemdb.backup
```

4. 복원 프로세스가 완료되면 확인 메시지가 표시됩니다.

오류가 발생하는 경우:

- 가장 일반적인 오류는 사용자가 여전히 데이터베이스에 연결되어 있는 경우에 발생합니다. PostgreSQL 서버를 다시 시작하여 잘못된 연결을 제거할 수 있습니다.
- 데이터베이스가 없다는 오류 메시지가 표시되는 것은 괜찮습니다. 이는 스크립트가 프로세스에서 데이터베이스를 생성하는 데 사용되고 있음을 의미합니다.

데이터베이스 구성 내보내기 또는 가져오기

처음 설치할 때 프로덕션 환경에 CA CEM 시스템을 배치할 수 없는 경우가 있습니다. 예를 들어 프로덕션 네트워크를 시작하기 전에 테스트 랩에 새 하드웨어와 소프트웨어를 모두 설치하라는 회사 정책이 있을 수 있습니다.

QA 또는 테스트 환경에서 CA CEM 구성을 설정하고 테스트한 후에는 CA CEM 내보내기 및 가져오기를 통해 입증된 구성을 프로덕션 환경으로 이동하십시오.

구성 정보에는 사용자 및 사용자 그룹과 비즈니스 서비스 및 트랜잭션이 포함됩니다.

데이터베이스 구성 내보내기 및 가져오기 프로세스

이 목록에는 CA CEM 구성 내보내기와 관련된 주요 작업이 나와 있습니다.

1. [사전 요구 사항 이해](#) (페이지 57)
2. CA CEM [구성 내보내기](#) (페이지 58)
3. CA CEM [구성 가져오기](#) (페이지 59)

내보내기 및 가져오기 유틸리티는 명령줄에서 실행할 수 있는 배치 파일(또는 셸 스크립트)의 형태로 제공됩니다.

비즈니스 트랜잭션 정의 가져오기 및 내보내기에 대한 자세한 내용은 **CA APM 트랜잭션 정의 안내서**를 참조하십시오.

APM 데이터베이스의 모든 정보(구성 정보 포함) 백업 및 복원에 대한 자세한 내용은 [데이터베이스 백업 또는 복원](#) (페이지 50)을 참조하십시오.

데이터베이스 구성 데이터를 내보내거나 가져오기 전에

경고! 두 유틸리티를 실행하기 전에 APM 데이터베이스를 백업하는 것이 좋습니다. 가져오기 작업의 경우 재작성하기 전에 기존 구성을 삭제하므로 특히 그렇습니다. 가져오기 스크립트를 실행하면 데이터베이스가 삭제되고 결과적으로 이전 데이터베이스의 구성 데이터만 포함하는 데이터베이스가 생성됩니다. 자세한 내용은 [데이터베이스 백업 또는 복원](#) (페이지 50)을 참조하십시오.

내보내기와 가져오기 작업을 수행하는 경우 모두 다음을 명심해야 합니다.

- APM 데이터베이스를 설치한 컴퓨터에서 스크립트를 실행합니다.
- Enterprise Manager 설치 관리자가 스크립트를 넣은 위치에 상대적인 파일을 참조하므로 이러한 위치에서 스크립트를 실행합니다.
- 이러한 스크립트를 실행하기 전에 APM 데이터베이스에 대한 연결을 모두 해제합니다. Enterprise Manager 를 종료하고 데이터베이스 관리 도구(예: pgAdmin)를 닫은 다음 모든 사용자가 로그오프했거나 CEM 콘솔을 닫았는지 확인합니다. 사용되지 않도록 설정할 필요는 없지만 가져온 후에는 다시 TIM 이 사용되도록 설정해야 합니다.
- **JRE 1.6 이상에 해당:** JAVA_HOME 환경 변수를 설정하고 JRE 루트 폴더를 가리키도록 설정합니다. JRE 1.6 이상이 필요하고 경로에 공백이 포함될 수 없습니다. 예를 들어 `c:\program files\java\jre1.6.0` 에 JRE 를 설치한 경우 JAVA_HOME 을 경로의 단축된 버전(예: `c:\progra~1\java\jre1.6.0`)으로 설정합니다.
- 이전 버전의 CA CEM 에서 구성을 가져오는 경우 Linux 에서는 이전 버전을 모두 가져올 수 있고 Windows 에서는 5.0 버전 이상만 가져올 수 있습니다. 가져오기 유틸리티는 이전 릴리스에서 현재 릴리스로 데이터베이스 스키마를 자동으로 업데이트합니다.

APM 데이터베이스 구성 내보내기

`configexport.bat` 또는 `configexport.sh` 스크립트는 모든 CA CEM 구성 정보가 있는 XML 파일을 생성합니다. 구성 정보에는 사용자 및 사용자 그룹과 비즈니스 서비스 및 트랜잭션이 포함됩니다. 구성 정보를 내보내면 테스트 또는 실험실 시스템의 데이터를 이동하여 프로덕션 시스템의 기반으로 사용할 수 있습니다.

APM 데이터베이스 구성을 내보내려면

1. JAVA_HOME 환경 변수를 설정합니다.
2. 사용 중인 운영 체제의 `<EM_Home>/install/database-scripts` 디렉터리로 이동합니다. 예:

```
cd /home/Introscope9.0.5.0/install/database-scripts/unix
```
3. 명령이나 터미널 창을 열고 다음 인수를 사용하여 `configexport.bat`(Windows) 또는 `configexport.sh`(기타 플랫폼)를 실행합니다.

```
ConfigExport <dbhostIP> <database_name> <dbuser> <password> <port_number>  
<databasetype> <export-file>
```

dbhostIP

데이터베이스를 호스팅하는 컴퓨터의 IP 주소를 지정합니다. 이 명령에는 `localhost` 를 사용할 수 없습니다.

database_name

데이터베이스 인스턴스 이름을 지정합니다. PostgreSQL 을 사용 중인 경우 기본값을 변경하지 않았으면 이 인수를 `cemdb` 로 설정합니다. Oracle 을 사용 중인 경우에는 이 인수를 Oracle SID(시스템 식별자)로 설정합니다.

dbuser

APM 데이터베이스와 연결된 데이터베이스 사용자의 사용자 이름을 지정합니다. PostgreSQL 을 사용 중인 경우 기본값을 변경하지 않았으면 이 인수를 `admin` 으로 설정합니다. Oracle 을 사용 중인 경우에는 이 인수를 APM 데이터베이스 스키마 소유자로 설정합니다.

참고: PostgreSQL 데이터베이스 관리자의 사용자 이름이 아닙니다.

password

APM 데이터베이스와 연결된 데이터베이스 사용자의 암호를 지정합니다.

port_number

데이터베이스가 Enterprise Manager 및 기타 구성 요소와 통신하는 포트 번호를 지정합니다. PostgreSQL 을 사용 중인 경우 기본값을 변경하지 않았으면 이 인수를 5432 로 설정해야 합니다. Oracle 과 기본 수신기 포트를 사용 중인 경우에는 이 인수를 1521 로 설정해야 합니다.

databasetype

사용 중인 데이터베이스 유형을 지정합니다. 이 인수를 postgres 또는 oracle 로 설정합니다.

export-file

내보낸 데이터를 포함하는 XML 파일의 절대 경로와 파일 이름을 지정합니다.

예를 들어 Linux 에서 *configexport* 프로그램을 실행하려면 다음과 유사한 명령줄을 사용합니다.

```
./configexport.sh 197.168.144.10 arcade apmdba mypwd 1521 oracle
/home/apmdba/export_oracle.xml
```

4. 구성 내보내기 프로세스가 완료되면 확인 메시지가 표시됩니다.

APM 데이터베이스 구성 가져오기

APM 데이터베이스 간에 구성 설정을 가져올 수 있습니다. 예를 들어 *configimport.bat* 또는 *configimport.sh* 프로그램을 사용하여 QA 시스템에서 프로덕션 시스템으로 데이터베이스 구성을 가져올 수 있습니다. 가져온 구성 설정에는 사용자 및 사용자 그룹과 비즈니스 서비스 및 트랜잭션이 포함됩니다.

APM 데이터베이스 구성 가져오기 프로세스는 다음을 수행합니다.

- 이전 데이터베이스 구성 정보(운영자, 사용자, 그룹, 비즈니스 서비스 프로세스 및 트랜잭션 정의에 대한 정보)를 삭제하고 가져온 구성 데이터로 바꿉니다.
- 결함, 보고서 및 통계 데이터를 삭제하기만 하고 바꾸지는 않습니다.

참고: 이전 버전의 CA CEM 에서 구성을 가져올 수 있습니다. 예를 들어 CA CEM 4.1 에서 구성을 다운로드하고 내보낸 다음 CA CEM 4.2 로 업로드하고 가져올 수 있습니다(Linux 만 해당).

다음 단계를 따르십시오.

1. 사용 중인 운영 체제의 <EM_Home>/install/database-scripts 디렉터리로 이동합니다. 예:

```
cd /home/Introscope9.0.5.0/install/database-scripts/unix
```

2. 명령이나 터미널 창을 열고 다음 인수를 사용하여 *configimport.bat*(Windows) 또는 *configimport.sh*(기타 플랫폼)를 실행합니다.

```
ConfigImport -dbhost <hostname> -dbname <database_name> -dbport <port_number>
-databasetype <database_type> -dbuser <dbuser> -dbpassword <password>
-dbscriptsdir <dir> -importfile <import-filename> -targetRelease
<targetRelease> -dbserviceuser <dbserviceuser> -dbservicepwd <dbservicepwd>
[-postgresinstalldir <postgresinstalldir>] [-nolog] [-jdbcbatchsize
<jdbcbatchsize>] [-promptbeforeimport true|false] [-is64Bit true|false]
```

dbhost

데이터베이스를 호스팅하는 컴퓨터의 호스트 이름이나 IP 주소를 지정합니다. 이 명령에는 *localhost* 를 사용할 수 없습니다.

dbname

데이터베이스 인스턴스 이름을 지정합니다. PostgreSQL 을 사용 중인 경우 기본값을 변경하지 않았으면 이 인수를 *cemdb* 로 설정합니다. Oracle 을 사용 중인 경우 이 인수를 Oracle 시스템 식별자(SID)로 설정합니다.

dbport

데이터베이스가 Enterprise Manager 및 기타 구성 요소와 통신하는 포트를 지정합니다. PostgreSQL 을 사용 중인 경우 기본값을 변경하지 않았으면 이 인수를 5432 로 설정합니다. Oracle 과 기본 수신기 포트를 사용 중인 경우에는 이 인수를 1521 로 설정합니다.

databasetype

사용 중인 데이터베이스 유형을 지정합니다. 인수를 *postgres* 또는 *oracle* 로 설정합니다.

dbuser

APM 데이터베이스와 연결된 데이터베이스 사용자의 사용자 이름을 지정합니다. PostgreSQL 을 사용 중인 경우 기본값을 변경하지 않았으면 이 인수를 *admin* 으로 설정합니다. Oracle 을 사용 중인 경우 이 인수를 APM 데이터베이스 스키마 소유자로 설정합니다.

dbpassword

APM 데이터베이스와 연결된 데이터베이스 사용자의 암호를 지정합니다.

dbscriptsdir

데이터베이스별 SQL 스크립트의 디렉토리를 지정합니다. 예를 들어 Oracle 데이터베이스 스키마를 사용 중인 경우에는 `<EM_Home>/install/oracle/database-scripts` 를, PostgreSQL 데이터베이스를 사용 중인 경우에는 `<EM_Home>/install/database-scripts` 를 사용합니다.

importfile

가져온 데이터를 포함하는 XML 파일의 절대 경로와 파일 이름을 지정합니다.

dbserviceuser

PostgreSQL 관리 서비스 사용자 계정을 지정합니다. 기본 관리 서비스 계정은 `postgres` 입니다. 이 인수는 Oracle 에 적용되지 않습니다.

dbservicepwd

PostgreSQL 관리 서비스 사용자 계정의 암호를 지정합니다.

postgresinstalldir

(선택 사항) PostgreSQL 을 사용 중인 경우 APM 데이터베이스의 디렉토리 위치를 지정합니다. Linux 또는 Solaris 에서 경로에 공백이 포함되어 있으면 따옴표로 묶거나 이스케이프 시퀀스를 포함해야 합니다. 예를 들어 디렉터리가 `/root/Introscope Enterprise Manager` 인 경우 위치를 `"/root/Introscope Enterprise Manager"` 또는 `/root/Introscope\ Enterprise\ Manager` 로 지정할 수 있습니다.

기본값을 변경하지 않은 경우 위치는 `opt/database(32 비트 Linux 또는 Solaris)`, `opt/database/postgres/8.3-community(64 비트 Linux 또는 Solaris)` 또는 `<EM_Home>\database(Windows)`입니다.

이 인수는 Oracle 에 적용되지 않습니다.

targetRelease

가져올 대상 릴리스를 지정합니다. 예를 들어 9.0.5.1 구성 파일을 가져올 수 있지만 DB 를 9.1.0.0 으로 업그레이드해야 할 수 있습니다.

nolog

(선택 사항) 표준 출력(StdOut)에 대한 로깅을 해제하도록 지정합니다.

jdbcbatchsize

(선택 사항) JDBC(Java 데이터베이스 연결)를 통해 한 번에 전송되는 최대 데이터 패킷 크기를 지정합니다. 기본값은 2500 입니다.

promptbeforeimport

(선택 사항) *configimport* 프로그램에서 데이터 가져오기를 시작하기 전에 프롬프트를 표시할지 여부를 지정합니다. 프롬프트를 표시하려면 이 매개 변수를 *true* 로 설정합니다. 기본값은 *false* 입니다.

is64Bit

(선택 사항) PostgreSQL 데이터베이스가 32 비트인지 64 비트인지 지정합니다. 데이터를 64 비트 PostgreSQL 데이터베이스로 가져오는 경우 이 매개 변수를 *true* 로 설정합니다. 이 인수는 Oracle 데이터베이스에 적용되지 않습니다.

예를 들어 Linux 와 PostgreSQL 데이터베이스에서 *configimport* 프로그램을 실행하려면 다음과 유사한 명령줄을 사용합니다.

```
./configimport.sh -dbhost sfqa07 -dbname cemdb -dbport 5432 -databasetype postgres -dbuser admin -dbpassword mypassword -dbscriptsdir /apps/Introscope/install/database-scripts -importfile /tmp/apm_data.xml -dbserviceuser postgres -dbservicepwd %pas5w0rd -postgresinstalldir /opt/database -promptbeforeimport true
```

가져오기 스크립트는 초기 유효성 검사를 수행하여 XML 형식이 제대로 지정되었는지 확인합니다.

가져오기 스크립트는 XML 콘텐츠를 제대로 처리할 수 있도록 XML 유효성을 더욱 철저히 검사하는 옵션을 제공합니다. 유효성 검사를 수행하려면 Y 를, XML 콘텐츠 유효성을 검사하지 않고 가져오기를 계속하려면 N 을 입력하십시오.

참고: 이 두 번째 유효성 검사는 XML 파일 크기에 따라 시간이 조금 걸릴 수 있습니다. XML 데이터를 제대로 가져올 수 있는지 확인해야 합니다. 그렇지 않으면 오류가 발생합니다.

스크립트는 진행 메시지를 표시하고 유효성 검사가 완료될 때, 가져오기가 시작될 때 및 가져오기가 완료될 때 메시지를 표시합니다.

유효성 검사가 어느 하나라도 실패하면 오류 메시지가 표시되고 구성 가져오기가 진행되지 않습니다. 유효성 검사가 둘 다 성공하면 스크립트가 지정된 데이터베이스 구성 데이터를 가져옵니다.

중요! 구성 가져오기에서 기존 HTTP 분석기 플러그인 구성을 가져오지 않습니다. 플러그인을 수동으로 설치하려면 CEM 콘솔을 사용하십시오.

다른 운영 체제로 APM 데이터베이스 이동

업그레이드 프로세스의 일부로 컴퓨터 간에 또는 플랫폼 간에 APM 데이터베이스를 이동해야 하는 경우가 있을 수 있습니다. 예를 들어 Windows 또는 Linux 의 PostgreSQL 에서 Solaris 의 PostgreSQL 로 APM 데이터베이스를 이동해야 할 수 있습니다. 플랫폼 간에 데이터베이스를 이동하려면 비즈니스 트랜잭션 및 구성 데이터를 원본 데이터베이스에서 내보낸 다음 새 플랫폼의 대상 데이터베이스로 가져와야 합니다. 또는 *dbbackup-postgres* 와 *dbrestore-postgres* 유틸리티를 사용하여 각각 기존 PostgreSQL 데이터베이스의 전체 백업본을 생성한 다음 새 컴퓨터에서 데이터베이스를 복원할 수 있습니다.

PostgreSQL 데이터베이스에서 데이터 내보내기 및 가져오기 또는 *dbbackup-postgres* 및 *dbrestore-postgres* 유틸리티 사용에 대한 자세한 내용은 *CA APM 구성 및 관리 안내서*를 참조하십시오. [PostgreSQL 데이터베이스에서 Oracle 데이터베이스로 데이터 마이그레이션](#) (페이지 63)에 대한 자세한 내용은 *CA APM 설치 및 업그레이드 안내서*를 참조하십시오.

PostgreSQL 데이터베이스에서 Oracle 데이터베이스로 데이터 마이그레이션

데이터베이스를 업그레이드하고 데이터를 PostgreSQL 에서 Oracle 데이터베이스로 마이그레이션하려면 업그레이드부터 수행하십시오. 예를 들어 Oracle 을 조직의 데이터베이스 플랫폼으로 표준화한 경우에는 APM 데이터베이스를 Oracle 로 마이그레이션해야 프로덕션 수준 모니터링이 가능합니다. 원본 PostgreSQL 데이터베이스에서 대상 Oracle 데이터베이스로 기존 데이터를 이동하려는 경우 *CA APM 마이그레이션* 유틸리티를 사용하여 원본 데이터베이스와 대상 데이터베이스를 지정할 수 있습니다.

PostgreSQL 데이터베이스에서 Oracle 데이터베이스로 마이그레이션하려면

1. 업그레이드 시나리오와 업그레이드 경로를 검토하여 업그레이드를 계획하고 준비합니다.
2. 모든 구성 요소의 백업 복사본을 생성합니다.
3. 대화식 또는 자동 Enterprise Manager 설치 관리자를 사용하여 Enterprise Manager 와 APM 데이터베이스를 업그레이드합니다.
4. <EM_Home>/install/migration 디렉터리로 이동합니다.
5. 다음 인수를 사용하여 사용 중인 운영 환경에 따라 적절히 *migration.bat* 또는 *migration.sh* 스크립트를 실행합니다.

```
migration -srcDatabaseName <database_name> -srcDatabaseType <database_type>
-srcHost <hostname> -srcPort <port_number> -srcUser <username> -srcPassword
<password> -tgtDatabaseName <datatargetname> -tgtDatabaseType <database_type>
-tgtHost <hostname> -tgtPort <port_number> -tgtUser <username> -tgtPassword
<password>
```

srcDatabaseName

원본 데이터베이스의 이름을 지정합니다. 기본 설정을 사용하는 경우 데이터베이스 이름은 *cemdb* 입니다.

srcDatabaseType

원본 데이터베이스의 유형을 지정합니다. 이 릴리스에서 유효한 값은 *postgres* 뿐입니다.

srcHost

원본 데이터베이스에 대한 데이터베이스 서버의 호스트 이름이나 IP 주소를 지정합니다.

srcPort

원본 데이터베이스에 연결하기 위한 포트 번호를 지정합니다. 기본 설정을 사용한 경우 포트는 **5432** 입니다.

srcUser

원본 데이터베이스의 데이터베이스 사용자 이름을 지정합니다. 기본 설정을 사용한 경우 데이터베이스 사용자 이름은 *admin* 입니다.

srcPassword

원본 데이터베이스의 데이터베이스 사용자 암호를 지정합니다.

tgtDatabaseName

대상 데이터베이스의 이름이나 서비스 계정 식별자를 지정합니다. Oracle 데이터베이스의 경우 대상 데이터베이스의 이름은 고유 SID(시스템 식별자)입니다.

tgtDatabaseType

대상 데이터베이스의 유형을 지정합니다. 이 릴리스에서 유효한 값은 *oracle* 뿐입니다.

tgtHost

대상 데이터베이스에 대한 데이터베이스 서버의 호스트 이름이나 IP 주소를 지정합니다.

tgtPort

대상 데이터베이스에 연결하기 위한 포트 번호를 지정합니다. 기본 설정을 사용한 경우 포트는 1521 입니다.

tgtUser

대상 데이터베이스의 데이터베이스 사용자 이름을 지정합니다.

tgtPassword

대상 데이터베이스의 데이터베이스 사용자 암호를 지정합니다.

참고: 모든 인수는 대소문자를 구분하며 마이그레이션 도구를 실행하는데 필요합니다.

예를 들어 PostgreSQL 데이터베이스 *cemdb* 에서 SID 는 *orcl* 이고 스키마 소유자는 *apmdb* 인 Linux 컴퓨터의 Oracle 데이터베이스로 데이터를 마이그레이션하는 명령은 다음과 유사합니다.

```
./migration.sh -srcDatabaseName cemdb -srcDatabaseType postgres -srcHost nyc16
-srcPort 5432 -srcUser admin -srcPassword quality -tgtDatabaseName orcl
-tgtDatabaseType oracle -tgtHost nyc23 -tgtPort 1521 -tgtUser apmdb -tgtPassword
cent3R
```

6. *logs* 디렉터리의 *migration.log* 파일을 검사하여 스키마가 성공적으로 마이그레이션되었는지 확인하거나 마이그레이션 관련 문제를 해결합니다. 예를 들어 *<EM_Home>/install/migration/logs* 디렉터리로 이동합니다.

참고: *<EM_Home>/install/migration/log4j-migration.properties* 파일에서 *log4j.appender.logfile.File* 속성을 수정하여 *migration.log* 파일 위치를 수정할 수 있습니다. 마이그레이션 및 로그 파일 속성을 사용자 지정하는 방법에 대한 자세한 내용은 마이그레이션 속성 사용자 지정을 참조하십시오.

데이터베이스 문제 해결

이 항목에서는 데이터베이스 문제를 해결하는 데 유용한 몇 가지 팁을 제공합니다.

증상

APM 데이터베이스를 실행하는 컴퓨터에 여러 데이터베이스(PostgreSQL 또는 Oracle) 프로세스가 있습니다. 이것이 정상입니까?

해결 방법

APM 데이터베이스에 대한 각 클라이언트 연결마다 데이터베이스 프로세스(PostgreSQL 또는 Oracle)가 생성됩니다. 따라서 동시에 실행되는 여러 개의 개별 데이터베이스 프로세스가 보이는 것은 정상입니다.

SmartStor 데이터 저장소 구성

SmartStor 가 프로덕션 상태인 동안에는 외부 데이터베이스가 없어도 항상 모든 응용 프로그램 성능 데이터(Introscope 메트릭)가 기록됩니다. 따라서 기록 데이터를 분석하여 외부 데이터베이스가 없어도 응용 프로그램 작동 중단의 근본 원인을 식별하거나 수용 능력 분석을 수행할 수 있습니다. Introscope 를 설치하면 기본 설정을 사용하여 SmartStor 가 사용하도록 설정됩니다.

매시 정각에 SmartStor 는 쿼리 처리 최적화를 위해 .spool 파일을 .data 파일로 변환합니다.

매일 자정에 SmartStor 는 Enterprise Manager 계층 설정을 기반으로 기록 메트릭 데이터 형식을 변환하고 만료 처리된 메트릭과 메타데이터를 삭제합니다.

다음은 IntroscopeEnterpriseManager.properties 파일에 있는 기본 계층 설정입니다.

```
introscope.enterprisemanager.smartstor.tier1.frequency=15
```

```
introscope.enterprisemanager.smartstor.tier1.age=7
```

```
introscope.enterprisemanager.smartstor.tier2.frequency=60
```

```
introscope.enterprisemanager.smartstor.tier2.age=30
```

`introscope.enterprisemanager.smartstor.tier3.frequency=900`

`introscope.enterprisemanager.smartstor.tier3.age=365`

SmartStor 는 최근 데이터가 가장 많이 액세스되고 가장 높은 수준의 레졸루션이 있는 저장소 계층을 사용합니다. 다음은 앞서 나열된 기본 속성 설정에 기반한 데이터 레졸루션입니다.

15 초 단위의 청크에 1 주 분량의 데이터 저장(미압축)

1 분(60 초) 단위의 청크에 30 일 분량의 데이터 저장(압축)

15 분(900 초) 단위의 청크에 1 년 분량의 데이터 저장(압축)

중요! 전용 디스크에 쓰도록 SmartStor 를 구성하여 Enterprise Manager 성능과 응답 속도의 심각한 저하를 방지하십시오. 다른 Enterprise Manager 동작이나 호스트에서 실행되는 다른 프로세스와의 디스크 경합으로 인해 성능이 저하될 수 있습니다.

SmartStor 데이터 전용 디스크를 설정하는 경우 이 속성을 `true` 로 설정하십시오. 기본적으로 Enterprise Manager 설치 관리자는 이 속성을 `false` 로 설정합니다.

[introscope.enterprisemanager.smartstor.dedicatedcontroller](#) (페이지 458)를 참조하십시오.

다음 단원에서는 SmartStor 계획 및 구성 지침을 제공합니다.

- [SmartStor 시스템 요구사항 결정](#) (페이지 68)
- [SmartStor 데이터 계층 값 지정](#) (페이지 69)

SmartStor 계층 작동 방식에 대한 세부 정보

SmartStor 의 계층은 메트릭 데이터를 저장하는 기간을 지정합니다. 최대 3 개의 계층이 있을 수 있고 각 계층은 동일하거나 증가하는 빈도 기간을 가집니다. 계층 1 은 빈도(초)와 보관 기간(일)으로 구성된 최소 만료 처리 기간입니다. 계층 1 의 빈도 구성을 기반으로 계층 2 를 구성하십시오. 계층 2 를 계층 1 의 "요약"으로 간주하고, 계층 3 은 계층 2 의 "요약"이 됩니다.

예:

	빈도 (15 초의 배수)	기간 (일)
계층 1	15	7
계층 2	15	14
계층 3	30	10

매일 밤 SmartStor 의 기간이 재지정되고 메트릭 데이터의 아카이브 파일(A1 이라고 함)이 수집됩니다. 새 아카이브인 A1 은 계층 1 "버킷"에 들어가 7 일 동안 유지됩니다. 8 일째 되는 날 A1 은 계층 2 로 승격됩니다. 저장 빈도는 변경되지 않습니다. 또한 빈도는 메트릭 보고 세분성을 나타냅니다. A1 은 14 일 동안 계층 2 에 저장됩니다. 15 일째 되는 날 A1 은 계층 3 으로 승격됩니다. 데이터 빈도는 30 초로 변환됩니다. 메트릭 데이터를 보면 15 초 단위가 아닌 30 초 단위로 증가합니다. A1 은 계층 3 에 10 일 동안 유지되었다가 SmartStor 에서 제거됩니다. 모두 합해서 A1 은 SmartStor 에 31 일 동안 저장됩니다.

메타데이터 자동 삭제

SmartStor 기간 재지정 중에 Enterprise Manager 는 연결된 메트릭 데이터 포인트가 없는 메타데이터(메트릭 및 에이전트 설명)를 자동으로 삭제합니다. 이 프로세스는 SmartStor 계층 지정 중에 다시 사용할 수 있도록 디스크 및 메모리 공간을 확보합니다. SmartStor 계층 기간은 IntroscopeEnterpriseManager.properties 파일에서 설정됩니다.

SmartStor 에 메트릭 데이터가 없는 에이전트를 포함하여 Workstation 에서 수동으로 마운트된 기록 에이전트는 삭제되지 않습니다.

SmartStor 시스템 요구 사항 확인

SmartStorSizing 스프레드시트를 사용하여 SmartStor 시스템 요구 사항을 확인할 수 있습니다. [이 스프레드시트는 CA Support 사이트에서 다운로드](#)할 수 있습니다.

사용 중인 데이터 계층에 대해 다양한 메트릭 수 값과 다양한 기간 및 만료 처리 범위로 실험해 볼 수 있습니다. 결과는 GB 크기 사용량으로 나타납니다.

SmartStor 성능은 운영 체제, JVM 및 파일 시스템을 선택할 때 중요합니다.

적합한 데이터 계층 빈도와 만료 처리 기간을 결정한 후 해당 SmartStor 속성에 맞게 지정 사항을 구성하십시오.

SmartStor 데이터 계층 값 지정

데이터 계층 3 개를 지정하여 SmartStor 데이터 저장소를 구성합니다. 각 계층은 다음 속성 쌍으로 구성됩니다.

- 저장 빈도(초)
- 데이터 만료 처리 기간(일)

빈도와 만료 처리 값에 대한 규칙은 다음과 같습니다.

- 저장 빈도는 15 초의 배수여야 합니다.
- 빈도는 1800 초(30 분)보다 크면 안 됩니다.
- 각 계층의 빈도는 이전 계층 빈도의 짝수 배수여야 합니다. 이 배수는 한 배일 수 있고 각 계층의 빈도는 동일할 수 있습니다.
- 만료 처리 기간은 0 이 아니어야 합니다.
- 3 개의 계층을 모두 정의해야 하고 4 개 이상의 계층을 정의할 수는 없습니다.

다음 단계를 따르십시오.

1. IntroscopeEnterpriseManager.properties 파일을 엽니다.
2. introscope.enterprisemanager.smartstor.tier1.frequency 속성에 대해 적합한 값을 입력합니다.
3. introscope.enterprisemanager.smartstor.tier1.age 속성에 대해 적합한 값을 입력합니다.
4. 나머지 2 개의 데이터 계층 속성 쌍에 대해 위 단계를 반복합니다.
5. Enterprise Manager 를 다시 시작합니다.

참고: 데이터 계층을 변경한 다음 Enterprise Manager 를 다시 시작하면 SmartStor 가 새 구성에 맞게 데이터를 조정하려고 합니다. 최대 하루 분량의 데이터가 손실될 수 있습니다.

트랜잭션 이벤트 데이터베이스 위치 및 만료 처리 구성

Enterprise Manager 는 트랜잭션 추적 및 기타 이벤트 데이터를 트랜잭션 이벤트 데이터베이스에 저장합니다.

트랜잭션 이벤트 데이터베이스의 위치는 Enterprise Manager 를 설치하는 동안 구성됩니다. 설치하는 동안 다른 위치를 지정하지 않은 경우 데이터베이스는 `<EM_Home>/traces` 디렉터리에 생성됩니다. 설치 후 `IntroscopeEnterpriseManager.properties` 의 `introscope.enterprisemanager.transactionevents.storage.dir` 속성을 사용하여 다른 위치를 선택할 수 있습니다.

Introscope 가 트랜잭션 이벤트 데이터를 보존하는 기간(일)은 Enterprise Manager 를 설치하는 동안 구성됩니다. `introscope.enterprisemanager.transactionevents.storage.max.data.age` 속성을 사용하여 기본값(14)을 변경할 수 있습니다.

참고: Introscope 가 이벤트 데이터를 저장하는 기간이 늘어나면 시스템 오버헤드와 디스크 저장소 요구량이 증가합니다.

기준 저장소 위치 구성

기본적으로 Introscope 는 Enterprise Manager 컴퓨터의 `<EM_Home>/data/baselines.db` 에 메트릭 기준 정보를 저장합니다.

Enterprise Manager 설치 관리자는 다른 기준 저장소 위치를 선택하는 옵션을 제공하지 않습니다. 그러나 Enterprise Manager 속성 파일의 `introscope.enterprisemanager.dbfile` 속성에서 다른 `baselines.db` 위치를 정의할 수 있습니다.

Introscope 에서 메트릭 기준을 통해 응용 프로그램 건전성의 상위 수준 표시기를 사용하도록 설정하는 방법에 대한 자세한 내용은 *CA APM Workstation 사용자 안내서*를 참조하십시오.

SmartStor, 기준 및 트랜잭션 이벤트 데이터 백업

Enterprise Manager 를 중지한 후 Enterprise Manager SmartStor, 기준 및 트랜잭션 이벤트 데이터 파일을 백업하고 관련 작업을 수행할 수 있습니다.

기본적으로 Enterprise Manager 는 <EM_Home>/data 디렉터리에 모든 SmartStor 및 기준 데이터를 저장합니다.

SmartStor 용 Enterprise Manager 데이터 파일은 다음과 같습니다.

- 에이전트가 보고한 다양한 메트릭에 대한 정보를 추적하는 *metrics.metadata* 파일. 가장 중요한 점은 *metrics.metadata* 가 메트릭 이름을 추적한다는 것입니다.
- *.spool* 로 끝나면서(예: *125122680000.spool*) Enterprise Manager 가 마지막 스푼-쿼리 변환을 수행한 이후 SmartStor 에 전송된 15 초 메트릭 값을 유지하는 파일. *.spool* 파일에는 1 시간이 넘는 분량의 데이터가 절대로 보관되지 않습니다.
- *.data* 로 끝나면서(예: *125118360000.data*) SmartStor 의 읽기 전용 쿼리 최적화 형식으로 메트릭 값을 유지하는 파일. 이러한 파일에는 15 초, 1 분 및 1 시간 분량의 데이터 포인트 값이 보관됩니다.

기준 데이터용 Enterprise Manager 데이터 파일은 다음과 같습니다.

- *baselines.db*.

기본적으로 Enterprise Manager 는 모든 트랜잭션 추적 및 이벤트 데이터를 <EM_Home>/traces 디렉터리에 저장합니다. 트랜잭션 이벤트 데이터용 Enterprise Manager 데이터 파일은 다음과 같습니다.

- *traces_YYYYMMDD.db*. 예제: *traces_20090923.db*

실행 중인 Enterprise Manager 는 오류 없이 *metrics.metadata*, *.spool* 및 *.data* 파일을 생성하고 쓸 수 있을 것으로 예상합니다. 따라서 Enterprise Manager 데이터를 이동 또는 복사하거나 관련 작업을 수행하기 전에 Enterprise Manager 를 중지하는 것이 좋습니다.

경고! Enterprise Manager 를 실행하는 동안 Enterprise Manager 데이터 파일을 복사하거나 편집하면 데이터가 손실됩니다.

Enterprise Manager 가 종료된 경우 다음을 모두 수행하여 Enterprise Manager 데이터를 백업하고 관련 작업을 수행할 수 있습니다.

- 백업 미디어에 데이터 저장
- Smartstor 도구를 사용하여 SmartStor 데이터 편집
SmartStor 도구에 대한 자세한 내용은 [SmartStor 도구를 사용하여 SmartStor 데이터 조정](#) (페이지 73)을 참조하십시오.
- 데이터 압축
- 데이터 복원
- 다른 Enterprise Manager 에서 오프라인으로 볼 수 있도록 데이터 복사

쿼리 전용 중복 클러스터 만들기

쿼리 전용 원본 기록(비라이브) 데이터의 역할을 할 중복 클러스터 컴퓨터에 SmartStor 데이터 파일을 복사할 수 있습니다.

참고: CA Technologies 는 서비스 수요가 클러스터를 실행 중인 하드웨어의 용량을 크게 초과하는 프로덕션 환경에서만 중복 클러스터를 만들 것을 권장합니다.

다음 단계를 따르십시오.

1. 프로덕션 또는 테스트 클러스터의 정확한 복제본을 만듭니다.
MOM 에 한 대의 컴퓨터를 사용하고 클러스터의 각 수집기마다 한 대씩 컴퓨터를 사용합니다.
2. 프로덕션 클러스터를 종료합니다.
3. 프로덕션 또는 테스트 MOM 의 SmartStor, 기준 및 트랜잭션 이벤트 데이터 파일을 중복 MOM 에 복사하고 각 프로덕션 또는 테스트 수집기의 SmartStor, 기준 및 트랜잭션 이벤트 데이터 파일을 중복 수집기에 복사합니다.
4. 프로덕션 클러스터와 쿼리 전용 중복 클러스터를 모두 시작합니다.
5. 쿼리 전용 중복 클러스터에서 원하는 쿼리를 모두 실행합니다.
6. 하루에 한 번씩 필요한 단계를 반복하여 쿼리 전용 중복 클러스터의 데이터를 최신 상태로 유지합니다.

SmartStor 도구를 사용하여 SmartStor 데이터 조정

Introscope 에서 제공하는 SmartStor 명령줄 도구를 사용하여 다음을 수행할 수 있습니다.

- 메트릭 누수 및 급증 정리
메트릭 누수 및 급증에 대한 자세한 내용은 *CA APM 크기 조정 및 성능 안내서*를 참조하십시오.
- 단일 Enterprise Manager 를 여러 Enterprise Manager 로 분할
- 여러 Enterprise Manager 를 단일 Enterprise Manager 로 병합

SmartStor 도구 시작 스크립트는 `<EM_Home>/tools/` 디렉터리에 있습니다. Windows 환경에서는 *SmartStorTools.bat* 시작 스크립트를 사용하여 SmartStor 도구를 실행하십시오. UNIX 환경에서는 *SmartStorTools.sh* 시작 스크립트를 사용하여 SmartStor 도구를 실행하십시오.

유효한 인수를 사용하여 `<EM_Home>` 명령줄에서 SmartStor 도구 명령을 실행하면 요청한 명령이 수행됩니다. 잘못된 인수를 사용하여 SmartStor 도구 명령을 실행하면 도움말 메시지가 표시됩니다.

경고! SmartStor 도구를 사용할 때는 원본 Enterprise Manager 를 반드시 종료해야 합니다. SmartStor 도구를 실행할 때는 원본 및 대상 Enterprise Manager 를 종료하는 것이 좋습니다. SmartStor 도구 사용 시 Enterprise Manager 가 실행되고 있으면 SmartStor 가 손상될 위험이 있습니다. 이는 Enterprise Manager 가 SmartStor 에 데이터를 쓰고 있을 때 SmartStor 도구도 SmartStor 데이터를 변경하는 경우 발생할 수 있습니다.

다음 형식을 사용하여 이러한 SmartStor 도구 명령을 실행하십시오.

`<SmartStorTools start script> <command> <arguments>`

- merge
- remove_metrics
- remove_agents
- keep_agents
- prune
- list-agents
- test_regex

경고! prune 도구는 조심해서 사용하십시오. 이 도구를 실행하면 데이터가 삭제되므로 중요한 데이터를 실수로 삭제하지 않도록 주의하십시오.

SmartStor 도구 명령

SmartStor 도구 명령을 사용하여 SmartStor 데이터베이스에 대한 여러 가지 유지 관리 및 관리 작업을 수행할 수 있습니다.

중요! 이러한 명령에서 에이전트와 메트릭 이름을 지정하는 경우에는 백슬래시를 사용하여 특수 문자를 이스케이프해야 합니다. 특수 문자는 `{{\^-$|}}?*`입니다. 예를 들어 메트릭 이름

`SuperDomain/machineName/WebLogic/WebLogic` 은

`SuperDomain\|machineName\|WebLogic\|WebLogic` 으로 지정됩니다.

merge

지정된 SmartStor 원본 디렉터리를 다른 대상 디렉터리와 병합합니다.

인수:

- <destination SmartStor directory>
- `-help` 도움말 메시지를 출력합니다.
- <source SmartStor directory>

예제:

Windows:

```
SmartStorTools.bat merge <source directory> <destination directory>
```

예:

```
SmartStorTools.bat merge <EM_Home>\data C:\data
```

명령이 성공적으로 실행된 경우 원본 디렉터리에 있는 모든 SmartStor 데이터는 대상 디렉터리에 있는 데이터와 병합됩니다.

UNIX:

```
SmartStorTools.sh merge <source directory> <destination directory>
```

remove_metrics

지정된 정규식과 일치하는 메트릭을 제거합니다. 이 도구를 사용하여 메트릭 누수 및 급증을 정리하십시오.

경고! `remove_metrics` 도구는 조심해서 사용하십시오. 이 도구를 실행하면 데이터가 삭제되므로 중요한 데이터를 실수로 삭제하지 않도록 주의하십시오.

인수:

- `-dest` - 대상 SmartStor 디렉터리입니다.
- `-help` - 도움말 메시지를 출력합니다.
- `-metrics` - 제거할 메트릭에 대한 정규식입니다.
- `-src` - 원본 SmartStor 디렉터리입니다.

예제:

Windows

```
SmartStorTools.bat remove_metrics -dest <destination directory> -metrics <metrics to  
be removed> -src <source directory>
```

예:

```
<EM_Home>\tools\SmartStorTools.bat remove_metrics -dest C:\SWDump\destination  
-metrics ".*Socket.*" -src <EM_Home>\data
```

명령이 성공적으로 실행되면 대상 디렉터리에는 소켓 메트릭을 제외한 모든 메트릭이 있고 원본 디렉터리에는 모든 메트릭이 그대로 유지됩니다.

UNIX

```
SmartStorTools.sh remove_metrics -dest < destination directory> -metrics <metrics to  
be removed> -src <source directory>
```

remove_agents

지정된 정규식과 일치하는 에이전트를 제거합니다.

경고! `remove_agent` 도구는 조심해서 사용하십시오. 이 도구를 실행하면 데이터가 삭제되므로 중요한 데이터를 실수로 삭제하지 않도록 주의하십시오.

인수:

- `-agents` - 제거할 에이전트에 대한 정규식입니다.
- `-dest` - 대상 SmartStor 디렉터리입니다.
- `-help` - 도움말 메시지를 출력합니다.
- `-src` - 원본 SmartStor 디렉터리입니다.

예제:

Windows

```
SmartStorTools.bat remove_agents -agents <Agent name> -dest <destination directory>
-src <source directory>
```

예:

```
<EM_Home>\tools>SmartStorTools.bat remove_agents -agents ".*WebSphere.*" -dest
C:\SWDump\destination -src <EM_Home>\data
```

명령이 성공적으로 실행되면 **WebSphere** 에이전트와 관련된 메트릭은 대상 디렉터리에서 모두 제거되고 원본 디렉터리에 있는 메트릭은 모두 그대로 유지됩니다.

UNIX

```
SmartStorTools.sh remove_agents -agents ".*WebSphere.*" -dest <destination
directory> -src <source directory>
```

keep_agents

지정된 정규식과 일치하는 에이전트를 유지합니다.

인수:

- `-agents` - 유지할 에이전트에 대한 정규식입니다.
- `-dest` - 대상 SmartStor 디렉터리입니다.
- `-help` - 도움말 메시지를 출력합니다.
- `-src` - 원본 SmartStor 디렉터리입니다.

예제:

Windows

```
SmartStorTools.bat keep_agents -agents <agent(s) name> -dest <destination directory> -src <source directory>
```

예:

```
<EM_Home>\tools>SmartStorTools.bat keep_agents -agents ".*Websphere.*" -dest C:\SWDump\destination\keepagents -src data
```

명령이 성공적으로 실행된 경우 **Websphere** 에이전트와 관련된 모든 메트릭은 대상 디렉터리에 있게 되고 원본 디렉터리의 내용은 그대로 유지됩니다.

UNIX

```
SmartStorTools.sh keep_agents -agents <Agent(s) name> -dest <destination directory> -src <source directory>
```

prune

SmartStor 에 기록 데이터가 없는 에이전트를 찾고 연결된 메트릭 메타데이터를 모두 제거합니다. 이 도구를 사용하여 메트릭 누수 및 급증을 정리하십시오.

경고! `prune` 도구는 조심해서 사용하십시오. 이 도구를 실행하면 데이터가 삭제되므로 중요한 데이터를 실수로 삭제하지 않도록 주의하십시오.

`prune` 도구를 사용하려면 여러 단계를 거쳐야 합니다. [SmartStor 메타데이터 정리](#) (페이지 81)를 참조하십시오.

인수:

- *-dest* - 원본의 변경되지 않은 *.data 파일과 함께 정리된 메타데이터 파일을 포함하는 디렉터리입니다.
- *-help* - 도움말 메시지를 출력합니다.
- *-silent* - 자동 모드입니다.
- *-src* - 원본 SmartStor 디렉터리입니다.

예

Windows

```
SmartStorTools.bat Prune -dest <destination directory> -src <source directory>
```

예:

```
<EM_Home>\tools>SmartStorTools.bat Prune -dest C:\SWDump\destination\backup -src data
```

명령이 성공적으로 실행되면 메타데이터 파일이 *metrics.metadata* 라는 이름으로 *dest* 디렉터리에 백업됩니다.

UNIX

```
SmartStorTools.sh prune -dest <destination directory> -src <source directory>
```

test_regex

지정된 정규식과 일치하는 메트릭이나 에이전트를 Windows 또는 UNIX 콘솔에 출력합니다.

인수:

- *-help* - 도움말 메시지를 출력합니다.
- *-src* - 원본 SmartStor 디렉터리입니다.
- *-agents* - 일치시킬 에이전트에 대한 정규식입니다.
- *-metrics* - 일치시킬 메트릭에 대한 정규식입니다.

예제:

Windows

```
SmartStorTools.bat test_regex -agents <agent(s) name> -src <sourcedirectory>
```

예:

```
<EM_Home>\tools>SmartStorTools.bat test_regex -agents ".*Websphere.*" -src  
<EM_Home>\data
```

명령이 성공적으로 실행되면 WebSphere 에이전트에 대한 모든 메트릭이 출력됩니다.

UNIX

```
SmartStorTools.sh test_regex -agents <agent(s) name> -src <source directory>
```


list_agents

제공된 정규식과 일치하는 에이전트를 나열합니다.

SmartStor 도구 `list_agents` 는 제공된 정규식과 일치하는 에이전트를 나열합니다.

인수:

- `-agents` - 일치시킬 에이전트에 대한 정규식입니다.
- `-src` - 원본 SmartStor 디렉터리입니다.
- `-help` - 도움말 메시지를 출력합니다.

예제:

Windows

```
SmartStorTools.bat list_agents -agents <agent(s) name> -src <source directory>
```

예:

```
<EM_Home>\tools>SmartStorTools.bat list_agents -agents ".*WebSphere.*" -src
<EM_Home>\data
```

명령이 성공적으로 실행되면 정규식(이 예제의 경우 `".*WebSphere.*"`)과 일치하는 모든 에이전트 이름이 마지막 보고 날짜와 함께 나열됩니다.

UNIX

```
SmartStorTools.sh list_agents -agents <Agents name> -src <source directory>
```

SmartStor 메타데이터 정리

SmartStor 에 기록 데이터가 없는 에이전트를 찾고 메트릭 누수 및 급증을 정리하려면 *prune* SmartStor 도구를 사용한 다음 연결된 메트릭 메타데이터를 모두 제거하십시오.

중요! Enterprise Manager 를 실행하면 SmartStor 데이터가 생성되므로 CA Technologies 에서는 SmartStor 도구를 실행할 때 Enterprise Manager 를 종료할 것을 권장합니다. Enterprise Manager 를 실행하는 동안 SmartStor 도구를 사용하면 예측할 수 없는 결과가 발생합니다.

다음 단계를 따르십시오.

1. Enterprise Manager 를 종료합니다.
2. 명령 프롬프트에서 *prune* 명령을 실행합니다.

예:

Windows: `<EM_Home>\tools>SmartStorTools.bat prune -src <path to data directory> -dest <path to dest backup directory>`

UNIX: `<EM_Home>/tools>SmartStorTools.sh prune -src <path to data directory> -dest <path to dest backup directory>`

명령이 성공적으로 실행되면

- 메타데이터 파일이 *metrics.metadata* 라는 이름으로 *dest* 디렉터리에 백업됩니다.
- 정리 작업이 진행되는 동안 Windows 또는 UNIX 콘솔에 정리된 메트릭이 표시됩니다.
- *.data 파일이 변경되지 않고 *src* 디렉터리에서 *dest* 디렉터리로 복사됩니다.

Windows 또는 UNIX 콘솔의 정리된 메트릭 목록을 텍스트 파일로 리디렉션하려면 명령에 `>>` 인수를 포함해야 합니다.

예: `<EM_Home>\tools>SmartStorTools.bat prune -src <path to data directory> -dest D:\backup >>D:\console.txt`

1. `<EM_Home>/data` 디렉터리에서 *metrics.metadata* 파일의 이름을 변경합니다. 예를 들어 *noprunemetrics.metadata* 로 변경합니다.
2. `<EM_Home>/data` 디렉터리에서 *test_regex* 명령을 실행합니다.

명령에 포함된 정규식을 기반으로 하는 메트릭을 모두 보여 주는 명령 출력이 Windows 또는 UNIX 콘솔에 표시됩니다. 정리된 메트릭은 더 이상 표시되지 않습니다.

예를 들어 다수의 소켓 메트릭을 정리하는 경우 다음 *test_regex* 명령을 실행합니다.

Windows:

`<EM_Home>\tools>SmartStorTools.bat test_regex -metrics ".*Socket.*" -src <path to data directory>`

UNIX:

`<EM_Home>/tools>SmartStorTools.sh test_regex -metrics ".*Socket.*" -src <path to data directory>`

3. Enterprise Manager 를 다시 시작합니다.

SmartStor 데이터 및 메타데이터 자르기

과도한 SmartStor 데이터 및 메타데이터를 자르려면 SmartStor 도구를 사용하십시오.

중요! SmartStor 도구를 실행할 때는 Enterprise Manager 를 종료하십시오. Enterprise Manager 를 실행하면 SmartStor 데이터가 생성되므로 SmartStor 도구를 사용하는 경우 예측할 수 없는 결과가 발생할 수 있습니다.

SmartStor 데이터 문제를 찾는 방법에 대한 예제는 [예제: test_regex 명령을 사용하여 SmartStor 데이터 문제 찾기](#) (페이지 86)를 참조하십시오. *CA APM Java Agent 구현 안내서* 또는 *.NET 에이전트 구현 안내서*의 메트릭 급증 항목도 참조하십시오.

다음 단계를 따르십시오.

1. Enterprise Manager 를 종료합니다.
2. 명령 프롬프트에서 `test_regex` 명령을 실행하여 현재 메트릭 목록을 출력합니다.

예를 들어 <EM_Home> 디렉터리에 Introscope 가 설치되어 있고 <EM_Home>\data 디렉터리에 데이터를 저장하도록 SmartStor 가 구성되어 있는 경우 다음 명령을 실행하십시오.

```
SmartStorTools.sh test_regex -metrics <agents regexp> -src ../data
```

```
예: SmartStorTools.sh test_regex -metrics ".*" -src ../data
```

결과에는 호스트 이름, 에이전트 이름, 메트릭 이름 및 메트릭 ID 를 포함한 정규화된 메트릭 이름의 목록으로 나타납니다. 총 행 수를 살펴보면 총 메트릭 수를 알 수 있습니다. 그러나 이 행 수는 Investigator 의 지원 가능성 메트릭에서 확인할 수 있는 메트릭 수만큼 정확하지는 않습니다.

에이전트 또는 메트릭 이름과 일치하는 특정 정규식과 비교해서 행 수를 계산하여 대부분의 공간을 차지하고 있는 메트릭을 파악할 수 있습니다. 이렇게 하면 관심이 없어 제거할 메트릭을 식별할 때도 도움이 됩니다.

3. 메트릭 목록에서 제거할 특정 에이전트의 메트릭을 선택합니다.

4. SmartStor 도구의 `remove_metrics` 명령을 실행하여 과도한 메트릭 집합을 제거합니다.

예를 들어 SQL 메트릭 수가 높은 경우 다음 명령을 사용하여 SQL 메트릭을 모두 제거합니다.

```
<EM_Home>\tools>SmartStorTools.bat remove_metrics  
-dest c:\sql_metrics_removed -metrics ".*SQL.*" -src <EM_Home>\data
```

명령이 성공적으로 실행되면 대상 디렉터리에는 SQL 메트릭을 제외한 모든 메트릭이 있고 원본 디렉터리에는 모든 메트릭이 그대로 유지됩니다.

참고: 이 명령을 실행하려면 몇 GB 정도 축소되기는 하지만 원래 데이터가 차지하는 공간(-src 옵션으로 지정됨)과 대략적으로 비슷한 대상 공간이 필요합니다. 위의 예제에서 SQL 메트릭이 없는 새 데이터(-dest 옵션으로 지정됨)는 이제 c:\sql_metrics_removed 디렉터리에 있습니다.

이 명령은 장기간 계속되는 작업이며 몇 시간 동안 실행될 수 있습니다.

5. 필요한 경우 다른 과도한 메트릭 집합에서 `remove_metrics` 명령을 반복합니다.

소켓은 메트릭 누수 문제가 많이 발생하는 또 다른 요소입니다.

`remove_metrics` 명령을 실행한 후 다음 명령을 사용하여 소켓 메트릭을 제거합니다.

```
<EM_Home>\tools>SmartStorTools.bat remove_metrics  
-dest c:\sql_and_sockets__metrics_removed -metrics ".*Sockets.*"  
-src c:\sql_metrics_removed
```

이 명령은 SQL 메트릭을 제거한 첫 번째 명령에서 파생된 데이터를 원본 데이터(c:\sql_metrics_removed 디렉터리에 있는 데이터)로 사용합니다. 그런 다음 SQL 메트릭과 소켓 메트릭이 모두 제거된 데이터는 -dest 옵션으로 지정된 위치(c:\sql_and_sockets__metrics_removed)에 저장됩니다. 거듭 말하지만 이 명령을 실행하려면 원본 데이터와 거의 같은 추가 공간이 필요합니다.

6. 메트릭 수를 줄인 후 <EM_Home>\data 디렉터리에서 백업 디렉터리로 모든 백업 메타데이터 파일을 이동합니다.

Enterprise Manager 는 가장 큰 메타데이터 파일, 즉 정의된 메트릭 수가 가장 많은 파일을 자동으로 사용합니다. 메트릭을 줄이면 백업 메타데이터 파일이 현재 데이터 파일보다 커집니다.

7. 정리된 메트릭 데이터와 메타데이터에 대한 메트릭 데이터 값을 확인합니다.
 - a. <EM_Home>\config 디렉터리에 있는 apm-events-thresholds-config.xml 파일을 엽니다.
 - b. 현재 속성 설정을 적어 둔 다음 introscope.enterprisemanager.metrics.historical.limit=500000 속성을 설정합니다.
 - c. 파일을 저장하고 닫습니다.
 - d. <EM_Home>\config 디렉터리에 있는 IntroscopeEnterpriseManager.properties 파일을 엽니다.
 - e. 현재 설정을 적어 둔 다음 메트릭을 제거하기 위한 대상 위치를 가리키도록 introscope.enterprisemanager.smartstor.directory= 속성을 설정합니다.
 예를 들어 예제 대상 위치가 c:\sql_and_sockets__metrics_removed 이므로 이 속성 설정은 introscope.enterprisemanager.smartstor.directory=c:\sql_and_sockets__metrics_removed 입니다.
 - f. 파일을 저장하고 닫습니다.
 - g. Enterprise Manager 를 다시 시작합니다.
 - h. 다음 메트릭의 값을 확인합니다.
 Enterprise Manager | Data Store(데이터 저장소) | SmartStor | Metadata(메타데이터) | Metrics with Data(데이터 있는 메트릭)
 값은 원래 값보다 훨씬 낮아야 합니다. 그렇지 않은 경우 필요없는 에이전트 또는 메트릭 이름과 비교해서 적합한 SmartStor 도구 명령을 사용하여 자르기 단계를 반복합니다. 기록 메트릭 수가 300 K 미만으로 줄어들면 Enterprise Manager 가 보다 효율적으로 실행됩니다.
8. 필요한 경우 변경된 속성 값을 원래 설정으로 다시 설정합니다.
 - a. <EM_Home>\config 디렉터리에 있는 apm-events-thresholds-config.xml 파일을 엽니다.
 - b. introscope.enterprisemanager.metrics.historical.limit 속성을 원래 설정으로 다시 설정합니다.
 - c. 파일을 저장하고 닫습니다.
 - d. Enterprise Manager 를 종료합니다.

- e. `<EM_Home>\config` 디렉터리에 있는 `IntroscopeEnterpriseManager.properties` 파일을 엽니다.
- f. `introscope.enterprisemanager.smartstor.directory` 속성을 원래 설정으로 다시 설정합니다.
- g. 파일을 저장하고 닫습니다.
- h. Enterprise Manager 를 다시 시작합니다.

예제: `test_regex` 명령을 사용하여 SmartStor 데이터 문제 찾기

이 예제에서는 `test_regex` 명령을 사용하여 JMX 메트릭 데이터가 급증되었음을 알아냅니다.

다음 단계를 따르십시오.

1. `test_regex` 명령을 실행하여 읽을 수 있는 `metrics.metadata` 버전을 생성합니다.

예를 들면 다음과 같습니다.

```
<EM_Home>\tools>SmartStorTools.bat test_regex  
-metrics -src <EM_Home>\data
```

결과적으로 메타데이터 메트릭 목록이 나타납니다.

2. 메타데이터 메트릭 목록을 검토하여 메트릭 누수 또는 급증을 일으킬 수 있는 요소를 확인합니다.

예를 들어 JMX 메트릭에 대한 메트릭 메타데이터 항목을 많이 찾을 수 있습니다.

3. (선택 사항) 스크립트를 실행하여 메트릭을 정렬하고 그룹화합니다.

예를 들어 JMX 메트릭이 메트릭 급증을 일으킨 요소인지 확인하기 위해 다음 스크립트를 실행할 수 있습니다.

```
grep '|'.* | awk -F'|' '{print $1}' | sort | uniq -c
```

UNIX 시스템을 사용 중인 경우 정렬 스크립트가 있는 전체 `test_regex` 명령은 다음과 같습니다.

```
SmartStorTools.sh test_regex -metrics <agents regexp> -src ../data | grep  
'|'.* | awk -F'|' '{print $1}' | sort | uniq -c  
le: SmartStorTools.sh test_regex -metrics ".*" -src ../data | grep '|'.* | awk  
-F'|' '{print $1}' | sort | uniq -c
```

4. 정렬 결과를 검토합니다.

예를 들어 다음과 같은 메트릭 수 및 유형 목록을 볼 수 있습니다.

1054327 JMX

1564 JSP

1051 OlamWebApp

889 EJB

569 CEF

496 Struts

173 Edocs

167 Servlets

36 CPU

29 Sockets

이 경우 SmartStor 가 백만 개가 넘는 메트릭을 저장하고 있으며 그 중 대부분은 JMX 메트릭입니다. 따라서 SmartStor 도구를 사용하여 정리할 수 있는 JMX 메트릭 급증이 발생했음을 알 수 있습니다. 메트릭 급증에 대한 자세한 내용은 *CA APM Java Agent 구현 안내서* 또는 *.NET 에이전트 구현 안내서*를 참조하십시오.

8.x 데이터를 9.x 로 업그레이드

SmartStor 도구 명령을 사용하여 SmartStor 데이터를 8.x 에이전트에서 9.x 로 업그레이드할 수 있습니다.

이 도구는 8.x 프론트엔드 및 백엔드 메트릭 ID 를 9.x 프론트엔드 및 백엔드 메트릭 ID 로 업데이트합니다. 이렇게 하면 응용 프로그램 심사 맵 화면에 메트릭이 중복되어 표시되지 않게 방지할 수 있습니다.

Enterprise Manager 와 에이전트를 9.x 로 업그레이드한 후에 업그레이드 명령을 사용합니다.

업그레이드 명령을 사용하여 8.x 데이터 업그레이드

다음 단계를 따르십시오.

1. Enterprise Manager 를 종료합니다.
2. 명령 프롬프트에서 <EM_Home>/tools 디렉터리를 찾습니다.
3. SmartStor 데이터 디렉터리를 백업합니다.
4. 원본 및 대상 디렉터리 경로를 제공하여 *upgrade* 명령을 실행합니다.

다음 구문과 인수를 사용합니다.

구문:

```
upgrade <sourceDir> <destDir>
```

인수:

- sourceDir - SmartStor 8.x 메트릭을 포함하는 기존 디렉터리의 경로
- destDir - 새 디렉터리의 경로

참고: 새 디렉터리는 유틸리티를 통해 즉시 생성됩니다. 미리 만들지 마십시오.

예제:

```
C:\Program Files\CA
APM\Introscope<new_version(9.X)>\tools>SmartStorTools.bat
upgrade C:\Program Files\CA
APM\Introscope<new_version(9.X)>\data C:\Program Files\CA
APM\Introscope<new_version(9.X)>\upgradeddata
```

5. IntroscopeEnterpriseManager.properties 파일을 편집하여 SmartStor 디렉터리를 대상 디렉터리로 설정합니다.
 - a. 편집을 위해 <EM_Home>/config/IntroscopeEnterpriseManager.properties 를 열고 SmartStor Settings 섹션을 찾습니다.
 - b. *introscope.enterprisemanager.smartstor.directory* 의 값을 대상 디렉터리로 설정합니다.
기본값은 *data* 입니다. 이는 <EM_Home>/data/를 나타냅니다.
6. Enterprise Manager 를 다시 시작합니다.

제 5 장: 가상 에이전트를 사용하여 메트릭 집계

이 단원에는 가상 에이전트 구성 및 사용에 대한 정보가 나와 있습니다.

이 섹션은 다음 항목을 포함하고 있습니다.

[가상 에이전트 이해](#) (페이지 89)

[가상 에이전트 요구 사항](#) (페이지 89)

[가상 에이전트 구성](#) (페이지 90)

가상 에이전트 이해

여러 물리적 에이전트를 단일 *가상 에이전트*로 구성할 수 있습니다. 가상 에이전트를 사용하면 여러 Java Agent 가 보고하는 메트릭을 집계해서 논리적으로 볼 수 있습니다.

가상 에이전트는 Introscope 를 사용하여 클러스터된 응용 프로그램을 관리하는 경우에 유용합니다.

가상 에이전트는 동일한 클러스터된 응용 프로그램의 다른 인스턴스를 모니터링하는 여러 에이전트로 구성되며 Introscope Workstation 에 단일 에이전트로 나타냅니다. 따라서 각 응용 프로그램 인스턴스마다 별개로 표시하는 것과는 반대로 클러스터된 응용 프로그램의 여러 인스턴스에서 집계된 메트릭을 논리적 응용 프로그램 수준에 표시할 수 있습니다.

단일 에이전트 측면에서 뷰 및 상호 작용의 범위를 지정하여 특정 응용 프로그램 인스턴스에 대한 성능 및 가용성 데이터를 볼 수 있습니다.

가상 에이전트 요구 사항

독립 실행형 Enterprise Manager 가 여러 개 있는 경우 가상 에이전트는 동일한 Enterprise Manager 에 보고하는 에이전트들만 포함할 수 있습니다.

Enterprise Manager 클러스터의 경우 단일 클러스터 내에서 Enterprise Manager 에 보고하는 에이전트들은 보고 대상이 되는 Collector Enterprise Manager 와 관계없이 동일한 가상 에이전트에 속할 수 있습니다.

가상 에이전트를 구성하는 경우 다음 조건을 고려하십시오.

- 한 에이전트를 여러 가상 에이전트에 할당할 수 있습니다.
- 가상 에이전트를 여러 개 정의하는 경우에는 사용자 지정 메트릭 에이전트를 포함하여 모두 고유한 이름을 가져야 합니다. 즉, 클러스터 내의 모든 에이전트 이름이 고유해야 합니다.
- SuperDomain 아래의 가상 메트릭을 다른 사용자 지정 도메인에 게시할 수 있습니다. 예를 들면 다음과 같습니다.

```
<agent-cluster name="Custom Metric Host" domain="SuperDomain"
tgtDomain="Production">
    <agent-specifier>(.*)\|(.*)\|Custom Metric Agent
\\(Virtual\)(.*)</agent-specifier>
    <metric-specifier>Agents\|(.*):ConnectionStatus</metric-specifier>
</agent-cluster>
```

이 구성을 설정하면 "superdomain.custom metric host (Collector):agent" 목록 내의 모든 에이전트에서 가상 메트릭인 ConnectionStatus 를 가져와서 프로덕션 도메인에 다시 게시하게 됩니다.

가상 에이전트 구성

에이전트가 보고하는 Enterprise Manager 의 <EM_Home>/config 디렉터리에 있는 *agentclusters.xml* 파일을 사용하여 가상 에이전트를 구성합니다. 클러스터된 Enterprise Manager 를 실행하는 경우에는 MOM <EM_Home>/config 디렉터리에 있는 *agentclusters.xml* 파일을 사용하여 가상 에이전트를 구성하십시오. 예제 *agentclusters.xml* 파일이 <EM_Home>/config 디렉터리에서 제공됩니다.

이 예제 *agentclusters.xml*에서는 Introscope SuperDomain 에 *BuyNowAppCluster* 라는 가상 에이전트를 정의합니다. 가상 에이전트에는 임의의 호스트에서 *BuyNow* 로 시작하는 이름의 에이전트가 모두 포함됩니다.

```
<?xml version="1.0" encoding="ISO-8859-1" ?>
<agent-clusters xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:noNamespaceSchemaLocation="agentclusters0.1.xsd" version="0.1" >
  <agent-cluster name="BuyNowAppCluster" domain="SuperDomain" >
    <agent-specifier>.*\|.*\|BuyNow.*</agent-specifier>
    <metric-specifier>Frontends\|.*</metric-specifier>
  </agent-cluster>
</agent-clusters>
```

루트 요소인 `<agent-clusters>`가 필요합니다. `<agent-cluster>` 요소는 가상 에이전트를 정의하며 다음 두 가지 필수 특성이 있습니다.

- **name** - 가상 에이전트를 여러 개 정의하는 경우에는 각각 고유한 이름을 지정해야 합니다.
- **domain** - 가상 에이전트를 Introscope 도메인에 할당합니다.
`agent-cluster` 정의에 `domain=""`으로 정의된 도메인이 없는 경우 가상 에이전트는 기본적으로 SuperDomain 에 할당됩니다.

가상 에이전트를 여러 개 정의하는 경우에는 각 가상 에이전트마다 `<agent-cluster>` 요소를 정의합니다. `<agent-cluster>` 요소에는 다음 두 가지 하위 요소가 필요합니다.

- `<agent-specifier>` - 다음과 같이 표준 정규화된 에이전트 이름을 사용하여 가상 에이전트 내의 에이전트를 지정하는 정규식을 포함합니다.

`<host> | <process> | <agentName>`

- `<metric-specifier>` - 리소스 유형이나 리소스 유형 인스턴스의 하위 집합 측면에서, 가상 에이전트 내의 에이전트에서 수집할 메트릭을 지정하는 접두사를 포함합니다. 권장되는 접두사는 다음과 같습니다.
 - 프런트엔드
 - CPU
 - JMX
 - WebSpherePMI

참고: 이러한 접두사가 권장되지만 어떠한 리소스든 메트릭 지정자로 사용할 수 있습니다.

<agent-cluster> 요소에는 <metric-specifier> 스탠자가 여러 개 포함될 수 있습니다.

참고: 일치하는 메트릭의 볼륨이 커질수록 Enterprise Manager 에 부과되는 오버헤드가 커지고 궁극적으로 Enterprise Manager 수용 능력이 저하될 수 있습니다.

중요! 정규식과 "." 및 "(.)" 등의 와일드카드 메트릭 지정자가 허용되지만 주의해서 사용해야 합니다. 와일드카드를 사용하면 메트릭 볼륨이 커지고 성능이 저하될 수 있습니다.

특정 "탐색" 트리 도메인 노드 아래에 가상 에이전트를 표시하려면 *tgtDomain* 특성을 정의하십시오.

- *tgtDomain* - 도메인 특성에 정의된 가상 에이전트 메트릭이 "탐색" 트리에 표시되도록 복사되는 대상 도메인을 정의합니다.
 - *tgtDomain* 을 정의하지 않으면 도메인 이름이 *tgtDomain* 으로 지정됩니다.
 - *tgtDomain* 값이 domains.xml 에 정의된 유효한 도메인이 아니면 Introscope 에서 대상 도메인 "탐색" 트리 노드를 생성할 수 없습니다.
 - 사용자가 *tgtDomain* 특성을 사용하여 정의된 도메인을 보려면 domains.xml 에 정의된 권한이 있어야 합니다. domains.xml 권한에 대한 자세한 내용은 *CA APM 보안 안내서*를 참조하십시오.

다음 예제 *agentclusters.xml* 에서는 Introscope SuperDomain 노드에 정의되어 MyDomain 노드에 표시되는 *BuyNowAppCluster* 라는 가상 에이전트를 정의합니다.

```
<?xml version="1.0" encoding="ISO-8859-1" ?>
<agent-clusters xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:noNamespaceSchemaLocation="agentclusters0.1.xsd" version="0.1" >
  <agent-cluster name="BuyNowAppCluster" domain="SuperDomain"
    tgtDomain="MyDomain"
    <agent-specifier>.*\|.*\|BuyNow.*</agent-specifier>
    <metric-specifier>Frontends\|.*</metric-specifier>
  </agent-cluster>
</agent-clusters>
```

이 경우 MyDomain 도메인만 볼 수 있는 권한이 있는 CA APM 사용자에게 다음 "탐색" 트리가 표시됩니다.

```
Custom Metric Host(Virtual)(사용자 지정 메트릭 호스트(가상))
  Customer Metric Process(Virtual)(사용자 지정 메트릭 프로세스(가상))
    BuyNowAppCluster
```

제 6 장: Enterprise Manager 및 클러스터 구성

이 단원에서는 Enterprise Manager 클러스터링 기능을 설명하고 Enterprise Manager 역할 및 클러스터 기능의 구성에 대한 지침을 제공합니다.

이 섹션은 다음 항목을 포함하고 있습니다.

[독립 실행형 Enterprise Manager 구성](#) (페이지 93)

[Enterprise Manager 클러스터링 이해](#) (페이지 93)

[Enterprise Manager 장애 조치 사용](#) (페이지 97)

[Enterprise Manager 클러스터 구성](#) (페이지 103)

독립 실행형 Enterprise Manager 구성

introscope.enterprisemanager.clustering.mode 속성을 구성하여 Enterprise Manager 를 독립 실행형 Enterprise Manager 로 지정할 수 있습니다.

다음 단계를 따르십시오.

1. 독립 실행형 Enterprise Manager 의 <EM_Home>\config 디렉터리에 있는 IntroscopeEnterpriseManager.properties 파일을 엽니다.
2. introscope.enterprisemanager.clustering.mode=Standalone 을 설정합니다.
3. 파일을 저장하고 닫습니다.
4. Enterprise Manager 를 다시 시작하여 이 설정을 적용합니다.

Enterprise Manager 클러스터링 이해

클러스터 환경에서는 Enterprise Manager 가 클러스터에 속한 다른 Enterprise Manager 를 관리하는 MOM(*Manager of Managers*) 역할을 합니다. 관리되는 Enterprise Manager 를 수집기라고 합니다.

MOM 에 로그인한 Workstation 사용자는 다음 작업을 수행할 수 있습니다.

- MOM 이 관리하는 각 수집기에 보고하는 에이전트에 의해 보고된 데이터를 확인하고 액세스합니다.

- 이러한 수집기에서 일반적인 Workstation 기능을 모두 수행합니다.

선택 사항인 Enterprise Manager 는 여러 클러스터의 수집기에 연결할 수 있는 CDV(크로스 클러스터 데이터 뷰어) 역할을 합니다.

CDV 에 로그인한 Workstation 사용자는 다음 작업을 수행할 수 있습니다.

- 메트릭 브라우저 트리에서 대시보드와 에이전트 및 고객 경험 메트릭 데이터를 확인하고 액세스합니다. 이 데이터는 CDV 가 연결된 각 수집기에 보고됩니다.
- 이러한 수집기에서 다음 기능을 포함하여 일반적인 Workstation 기능의 하위 집합을 수행합니다.
 - 관리 모듈 편집기를 사용하여 대시보드를 생성합니다.
 - 트랜잭션 추적을 실행합니다.
 - 동적 계측을 사용합니다.
 - [Enterprise Manager 클러스터를 구성](#) (페이지 103)할 수 있습니다.

Enterprise Manager 를 클러스터할 시기

클러스터링은 여러 Enterprise Manager 와 많은 에이전트로 구성된 대규모 Introscope 환경에서 유용합니다. 클러스터 구성은 다중 Enterprise Manager 환경 관리의 복잡성과 비용을 줄입니다.

MOM 의 수집기 관리 방법 이해

[Enterprise Manager 클러스터 구성](#) (페이지 103)에 설명된 대로 구성된 MOM 을 시작하면 MOM 이 관리하는 각각의 수집기와 연결하려고 합니다.

Investigator 의 모든 에이전트에는 Enterprise Manager 호스트라는 메트릭이 자동으로 제공됩니다. 에이전트가 연결된 수집기 Enterprise Manager 를 알 수 있으므로 이 메트릭은 클러스터를 실행할 때 유용합니다.

MOM 은 미리 구성된 기본 제공 사용자 계정을 사용하여 수집기에 연결합니다. 암호는 공개/개인 키 암호화를 사용하여 보호됩니다. 자세한 내용은 *CA APM 보안 안내서*를 참조하십시오.

수집기 중 하나에 연결하려는 MOM 초기 시도의 결과로 인증 오류, 알 수 없는 호스트 예외, *java.rmi.ConnectIOException* 등의 복구할 수 없는 오류가 발생하면 해당 수집기가 클러스터에서 제거되고 다음에 MOM 을 다시 시작할 때까지 해당 수집기에 대한 연결 시도가 중지됩니다.

손실된 연결, *java.rmi.ConnectionException* 등의 복구할 수 있는 오류가 발생하면 연결 시도가 10 초마다 반복됩니다.

연결 상태 로깅은 다음과 같은 방식으로 발생합니다.

- 로깅 수준이 **DEBUG** 인 경우 연결 오류의 스택 추적이 로그에 기록됩니다.
- 로깅 수준이 **VERBOSE** 인 경우 처음에 10 회 연속 실패한 시도에 대한 메시지가 로그에 기록됩니다. 10 회 연속 실패한 후에는 실패한 연결 시도가 더 이상 로깅되지 않는다는 메시지가 로그에 기록됩니다.
- MOM 이 수집기에 연결되거나 다시 연결될 때마다 항상 메시지가 로그에 기록됩니다.

MOM 이 실행 중인 상태로 유지되는 동안에는 MOM 이 관리하는 수집기가 폴링됩니다.

클러스터링 및 Enterprise Manager 클록 동기화

Enterprise Manager 클러스터에서는 수집기 시스템 클록을 MOM 클록 설정의 3 초 이내로 설정해야 합니다. 시작할 때 수집기 클록이 MOM 클록과 동기화되어 있지 않으면 수집기가 클러스터에 참가하지 못합니다. 작업하는 동안 이전에 동기화된 수집기 클록이 동기화되지 않은 시간이 3 초를 넘어가면 MOM 이 해당 수집기의 데이터를 더 이상 받아들이지 않습니다.

MOM 과 Collector Enterprise Manager 간의 클록 동기화는 자동으로 수행되지 않습니다.

MOM 클록과 Collector Enterprise Manager 클록을 동기화된 상태로 유지하려면 모든 Enterprise Manager 클록을 NTP 서버와 규칙적으로 동기화하는 것이 좋습니다. 수집기 클록과 MOM 클록이 동기화되지 않은 시간이 3 초를 넘어가면 MOM 이 수집기의 데이터를 더 이상 받아들이고 있지 않다는 오류 메시지가 MOM 로그에 나타납니다. 이 경우 NTP 서버와의 동기화 빈도를 늘리십시오. 클록 동기화 후 Enterprise Manager 를 다시 시작하지 않아도 됩니다. 클록이 동기화되었음을 감지하면 MOM 이 자동으로 수집기에 다시 연결됩니다.

참고: 클러스터에 있는 모든 컴퓨터의 클록을 규칙적으로 동기화하는 시간 서버 소프트웨어를 실행해야 합니다.

클러스터링 및 에이전트 이름 지정

Enterprise Manager 클러스터에서는 Collector Enterprise Manager 에 보고하는 에이전트 이름이 고유해야 합니다.

MOM 의 경우 클러스터에서 에이전트 이름이 고유해야 합니다. 각 Enterprise Manager 가 해당 Enterprise Manager 에 연결하는 에이전트 이름의 고유성을 확인하지만, *CA APM Java Agent 구현 안내서* 또는 *CA APM .NET 에이전트 구현 안내서*에서 에이전트 이름 지정 충돌을 해결하는 방법에 대해 설명한 대로 클러스터 내의 수집기에서 에이전트 이름이 고유한지 확인하십시오. 클러스터에 있는 여러 에이전트의 이름이 동일하면 MOM 이 마지막으로 발견한 에이전트 이름만 Workstation 뷰에 나타납니다. 응용 프로그램 서버로부터 이름을 가져오도록 에이전트를 구성하는 것이 고유한 에이전트 이름을 할당하는 방법입니다. 자세한 내용은 사용자 환경에 맞게 *CA APM Java Agent 구현 안내서* 또는 *CA APM .NET 에이전트 구현 안내서*에서 응용 프로그램 서버로부터 에이전트 이름을 가져오는 방법에 대해 설명한 내용을 참조하십시오.

수집기가 사용자 지정 메트릭 에이전트 이름을 자동으로 바꾸면서 고유 식별자를 에이전트 이름에 추가하여 에이전트의 수집기를 식별합니다. 기본 식별자의 형식은 *host@port* 입니다. 여기서 *host* 는 수집기의 호스트 이름이고 *port* 는 `introscope.enterprisemanager.port.<ChannelName>` 속성에 정의된 수집기의 연결 포트입니다. 또는 `introscope.enterprisemanager.clustering.collector.identifier` 속성을 사용하여 식별자를 설정할 수 있습니다. 식별자는 고유합니다.

예를 들어 포트 5001 에서 연결을 수신 대기하는 *myhost* 에 있는 수집기의 SuperDomain 에서 사용자 지정 메트릭 에이전트의 이름은 다음과 같습니다.
Custom Metric Agent (myhost@5001) (*SuperDomain*)

클러스터링 및 관리 모듈

Enterprise Manager 클러스터에서는 MOM 에 설치한 관리 모듈만 사용됩니다. 성능을 위해 Collector Enterprise Manager 에 상주하는 관리 모듈이 없는 것이 좋습니다.

클러스터 환경에서 확장 파일 배포

사용 중인 CA APM 배포에서 활성화한 확장을 클러스터 환경에 배포하는 경우 특정한 방식으로 확장 파일을 관리해야 합니다.

다음 단계를 따르십시오.

1. `<EM_Home>/examples/<Extension_Home>`에서 확장을 설치한 폴더를 찾습니다. 여기서 `<Extension_Home>`은 확장 이름입니다.
2. 이 폴더의 전체 내용을 MOM 의 `<EM_Home>/` 위치에 복사합니다.
3. `<EM_Home>/examples/<Extension_Home>/config` 디렉토리를 제외한 이 폴더의 전체 내용을 각 Collector Enterprise Manager 의 `<EM_Home>/` 위치에 복사합니다.

관리 모듈 `.jar` 파일이 MOM 에만 상주해야 하므로 `<EM_Home>/examples/<Extension_Home>/config` 디렉토리는 복사되지 않습니다.

Enterprise Manager 장애 조치 사용

Enterprise Manager 장애 조치는 다음과 같이 Enterprise Manager 를 지정하여 작동합니다.

- 한 Enterprise Manager 는 기본 컴퓨터로, 다른 Enterprise Manager 는 보조 또는 백업 컴퓨터로 지정합니다.
- 두 Enterprise Manager 를 모두 기본 컴퓨터로 지정합니다.

보조 컴퓨터는 기본 컴퓨터에 장애가 발생하면 제어권을 받았다가 기본 컴퓨터가 복구되면 제어권을 반환하는 역할을 합니다. 기본 MOM 은 보조 MOM 으로부터 제어권을 넘겨받게 됩니다.

한 쌍의 Enterprise Manager 가 단일 Introscope 설치를 공유하는 경우에 Enterprise Manager 장애 조치를 구성할 수 있습니다. 일반적으로 두 개의 Enterprise Manager 는 서로 다른 컴퓨터에 있습니다. Introscope 설치에 대한 읽기 권한이 두 Enterprise Manager 모두에 필요하기 때문에 Introscope 설치는 네트워크 파일 시스템에 상주해야 합니다. 그러나 쓰기 권한은 한 번에 하나의 Enterprise Manager 에만 필요합니다. 예를 들어 다음 프로토콜과 같은 NAS(네트워크 연결 저장소) 프로토콜을 사용하여 Introscope 설치를 공유할 수 있습니다.

- NFS(네트워크 파일 시스템)
- SMB(서버 메시지 블록)

CA Technologies 는 클러스터 안정성을 제공하기 위해 MOM Enterprise Manager 에 대해 장애 조치를 구성할 것을 권장합니다. 또한 클러스터에 속한 하나 이상의 수집기 및 CDV 에 대해 장애 조치를 구성하거나 독립 실행형 Enterprise Manager 에 대해 핫 장애 조치를 구성할 수 있습니다. MOM 과 하나의 클러스터에 속한 수집기 및 CDV 에 대해 장애 조치를 구성하는 경우에는 각 Enterprise Manager 를 개별적으로 구성하십시오.

기본적으로 Enterprise Manager 장애 조치는 사용하도록 설정되어 있지 않습니다.

다음 단계를 따르십시오.

1. <EM_Home>\config 디렉터리로 이동하고 *IntroscopeEnterpriseManager.properties* 파일을 엽니다.
2. Hot Failover 섹션을 찾습니다.
3. [장애 조치 속성](#) (페이지 474)을 설정합니다.

에이전트, TIM 및 Workstation 은 Enterprise Manager 에 연결하려고 할 때 호스트 이름의 IP 주소를 모두 시도합니다. 기본 및 보조 Enterprise Manager 의 IP 주소를 사용하여 DNS 에 논리적 호스트를 정의한 경우 에이전트, TIM 및 Workstation 은 이 IP 주소를 Enterprise Manager 호스트 이름에 사용하여 실행 중인 Enterprise Manager 에 연결할 수 있습니다.

4. 보조 Enterprise Manager 컴퓨터 사용자에게 기본 Enterprise Manager SmartStor 데이터 디렉터리에 대한 쓰기 권한이 있는지 확인합니다.
- 장애 조치 상황에서 이 권한이 있으면 보조 Enterprise Manager 가 기본 Enterprise Manager SmartStor 데이터베이스에 데이터를 쓸 수 있습니다.

참고: 장애 조치 환경에서는 *EMCtrl* 스크립트를 사용하여 기본 Enterprise Manager 를 시작할 수 있습니다. 보조 Enterprise Manager 가 제어 스크립트를 사용해서는 안 됩니다. 예를 들어 UNIX 플랫폼의 경우 제어 스크립트 *EMCtrl.sh start* 를 사용하여 기본 Enterprise Manager 를 시작하고 *./Introscope Enterprise Manager* 명령을 사용하여 보조 Enterprise Manager 를 시작하십시오.

Enterprise Manager 장애 조치 규칙

Enterprise Manager 장애 조치에는 다음과 같은 규칙이 적용됩니다.

- 장애 조치로 Enterprise Manager 를 시작하는 경우 각 Enterprise Manager 를 한 번에 하나씩 시작하십시오. 기본 또는 보조 구성이 있는 경우 기본 구성이 먼저 시작되어야 합니다.
- 둘 다 기본 Enterprise Manager 인 경우 두 번째 기본 Enterprise Manager 는 첫 번째 기본 Enterprise Manager 에 장애가 발생할 때까지 대기하여 첫 번째 기본 Enterprise Manager 가 복구될 때 제어권을 반환하지 않습니다.
- 장애 조치 구성의 경우 기본, 보조 및 설치 디렉터리는 일반적으로 서로 다른 호스트에 있습니다. 그러나 Introscope 설치(Introscope 가 원래 설치된 위치)와 Enterprise Manager 는 동일한 호스트에 상주할 수 있습니다. 자세한 내용은 [단일 호스트에서 작동하도록 Enterprise Manager 장애 조치 구성 \(페이지 101\)](#)을 참조하십시오.
- Enterprise Manager 의 호스트가 기본 호스트 중 하나와 일치하는 경우 해당 Enterprise Manager 는 기본 역할을 담당합니다.
- Enterprise Manager 의 호스트가 보조 호스트 중 하나와 일치하는 경우 해당 Enterprise Manager 는 보조 역할을 담당합니다.
- Enterprise Manager 의 호스트가 기본 또는 보조 호스트와 일치하지 않는 경우 Enterprise Manager 는 일반적인 방식으로 시작됩니다. 그러나 경고 메시지가 로깅됩니다.

- 보조 Enterprise Manager 는 기본 Enterprise Manager 가 시작 대기 중인지 확인하기 위해 2 분(구성 가능)마다 검사를 합니다. 시작 대기 중인 경우 보조 Enterprise Manager 는 기본 Enterprise Manager 로 대체되어 종료됩니다.

[introscope.enterprisemanager.failover.interval](#) (페이지 475) 속성은 실행 중인 보조 Enterprise Manager 가 기본 Enterprise Manager 가 시작 대기 중인지 여부를 확인하는 빈도를 제어합니다.

- 기본 Enterprise Manager 는 보조 Enterprise Manager 나 다른 기본 Enterprise Manager 로 대체되지 않습니다.
- 시작 및 종료 순서는 다음과 같습니다: 장애 조치 쌍을 시작할 때는 기본 Enterprise Manager 를 먼저 시작한 다음 보조 Enterprise Manager 를 시작합니다. 장애 조치 쌍을 종료할 때는 보조 Enterprise Manager 를 먼저 중지한 다음 기본 Enterprise Manager 를 중지하십시오.

기본 Enterprise Manager 로 대체 후 보조 Enterprise Manager 다시 시작

기본 Enterprise Manager 로 대체된 보조 Enterprise Manager 는 JVM 을 종료합니다. Enterprise Manger 를 다시 시작할지 여부는 선택 사항입니다. 스크립트를 사용하거나 보조 Enterprise Manager 를 Windows 서비스로 실행하여 다시 시작할 수 있습니다. 기본 Enterprise Manager 로 대체되어 종료되는 경우 보조 Enterprise Manager 는 상태 코드

23(`org.eclipse.equinox.app.IApplication.EXIT_RESTART`)을 반환하며 종료됩니다. 명령줄 중단으로 인해 정상적으로 종료되거나 Workstation 에 의해 정상적으로 종료되는 경우 보조 Enterprise Manager 는 상태 코드 0 으로 종료됩니다.

Windows 를 사용 중인 경우 다음과 같은 명령을 사용할 수 있습니다.

```
:RESTART  
"Introscope Enterprise Manager"  
IF ERRORLEVEL 23 GOTO RESTART
```

단일 호스트에서 작동하도록 Enterprise Manager 장애 조치 구성

공유 파일 시스템 대신 단일 호스트에서 작동하도록 Enterprise Manager 장애 조치를 구성할 수 있습니다. 기본 Enterprise Manager 에 장애가 발생할 때 보조 Enterprise Manager 로 역할을 대체하도록 단일 호스트에서 Enterprise Manager 장애 조치를 설정할 수 있습니다. 다음과 같은 작업을 수행하지 않으려면 단일 호스트에 장애 조치를 설정하십시오.

- Enterprise Manager 를 Windows 서비스로서 실행
- 셸 스크립트를 사용하여 Enterprise Manager 다시 시작

중요! 동일한 호스트에서 두 장애 조치 Enterprise Manager 를 구성하면 하드웨어 플랫폼 장애 발생 시 단일 실패 요인이 되어 심각한 중단 사고를 초래할 수 있습니다.

다음 단계를 따르십시오.

1. *IntroscopeEnterpriseManager.properties* 파일에서 다음 Enterprise Manager 속성을 아래와 같이 설정합니다.
 - *introscope.enterprisemanager.failover.enable=true*
 - *introscope.enterprisemanager.failover.primary=localhost*
2. Introscope Enterprise Manager.exe 를 클릭하여 첫 번째 기본 Enterprise Manager 를 시작합니다.
3. Introscope Enterprise Manager.exe 를 클릭하여 두 번째 기본 Enterprise Manager 를 시작합니다.

두 번째 기본 Enterprise Manager 가 제대로 시작되면 명령 프롬프트(콘솔)에 *acquiring primary lock* 메시지가 표시됩니다. 이 메시지가 나타나지 않으면 장애 조치가 잘못 구성되었거나 기본 Enterprise Manager 가 실행 중이지 않은 것입니다.

MOM 장애 조치 및 CA CEM TIM 정보

사용 중인 CA APM 환경에 CA CEM 을 배포하는 경우 각 TIM 과 연결하도록 MOM 을 구성합니다. TIM 을 사용하도록 설정하면 두 가지 IP 주소, 즉 MOM IP 주소와 TIM 수집 서비스를 실행 중인 수집기의 IP 주소가 TIM 에 제공됩니다. 이 수집기는 TIM 과 연결하여 TIM 데이터를 수집합니다.

MOM 장애 조치를 구성한 경우 TIM 이 사용되도록 설정되어 실행되고 있으면 기본 MOM 이 TIM 에 다음 정보를 제공합니다.

- 기본 MOM IP 주소
- IntroscopeEnterpriseManager.properties 파일에서 정의한 보조 MOM IP 주소(설정된 경우)

이러한 IP 주소는 TIM 에 저장되고 "Wily System Setup"(Wily 시스템 설정) > "TIM" > "TIM Settings"(TIM 설정) 페이지에서 볼 수 있습니다.

장애 조치 MOM 이 TIM 에 연결하려면 다음 조건이 충족되어야 합니다.

- TIM 이 실행 중이고 사용되도록 설정되어야 합니다.
- IntroscopeEnterpriseManager.properties 파일 속성이 다음과 같이 올바르게 설정되어야 합니다.
 - IntroscopeEnterpriseManager.failover.enable 속성이 true 로 설정되어 있습니다.
 - 하나 이상의 기본 MOM IP 주소가 introscope.enterprisemanager.failover.primary 속성에 정의되어 있습니다.

참고: 기본 MOM IP 주소를 여러 개 정의하는 경우에는 보조 IP 주소를 정의하지 않아도 됩니다.

- 기본 MOM IP 주소를 하나만 정의하는 경우에는 IntroscopeEnterpriseManager.properties 파일의 introscope.enterprisemanager.failover.secondary 속성에서 보조 MOM IP 주소를 하나 이상 정의하십시오.

참고: 원할 경우 보조 MOM 을 여러 개 정의할 수 있습니다.

- 장애 조치 MOM 의 주소가 변경되는 경우 모든 TIM 이 사용되지 않도록 설정했다가 다시 사용되도록 설정하십시오. TIM 이 사용되도록 설정하면 TIM 이 새 장애 조치 MOM 의 IP 주소를 가져올 수 있습니다. 장애 조치 MOM IP 주소는 CEM 콘솔에서 볼 수 있습니다. "TIM Settings"(TIM 설정) 페이지에서 TessIpAddr 필드를 참조하십시오.

이러한 조건이 충족되면 기본 MOM 에서 장애가 발생한 경우 장애 조치 MOM 이 자동으로 TIM 에 연결됩니다. 또 다른 기본 MOM 또는 보조 MOM 으로 장애 조치를 구성할 수 있습니다.

이러한 조건이 충족되지 않으면 MOM 장애 시 다음과 같은 동작이 수행됩니다.

조건	MOM 장애 시 발생하는 결과
TIM 이 실행되고 있지 않거나 사용되도록 설정되어 있지 않습니다.	MOM 장애 전/후에 TIM 에 연결되지 않습니다. TIM 이 실행되며 사용되도록 설정되어 있어야 MOM 이 이를 인식하고 MOM 연결을 수신할 수 있습니다.
IntroscopeEnterpriseManager.failover.enable 속성이 <i>false</i> 로 설정되어 있습니다.	수집기가 계속해서 TIM 의 데이터를 폴링하지만 TIM 에 대한 연결을 시도하는 대체 기본 또는 보조 MOM 이 없습니다. 대체 기본 또는 보조 MOM 이 수집기에 연결됩니다.
MOM 기본 또는 보조 IP 주소가 추가로 정의되어 있지 않습니다.	수집기가 계속해서 TIM 의 데이터를 폴링하지만 TIM 에 대한 연결을 시도하는 대체 기본 또는 보조 MOM 이 없습니다. MOM 구성 변경 사항이 TIM 에 전송되지 않습니다.

Enterprise Manager 클러스터 구성

속성 파일에서 Enterprise Manager 역할 및 클러스터 관련 속성을 정의하여 Enterprise Manager 클러스터를 구성할 수 있습니다.

중요! 모든 CA APM 클러스터 전체와 단일 클러스터 내에서 MOM, Collector 및 CDV 에 사용되는 domains.xml 파일은 서로 다르면 안 됩니다.

MOM 은 클러스터 내에서 라이브 에이전트(즉, 클러스터에 현재 데이터를 보내는 에이전트)에 대한 도메인이 서로 달라도 처리할 수 있습니다. 하지만 MOM 과 Collector 의 기록 에이전트에 대해 서로 다른 도메인을 사용하면 MOM 에서 확인하는 기록 데이터의 일관성이 유지되지 않을 수 있습니다. 클러스터 내에 도메인이 혼합된 경우 Collector 의 기록 에이전트가 추적되지 않으므로, 명시적으로 기록 에이전트를 마운트하지 않는 한 MOM 을 통해 작성되는 Workstation 그래프에 Collector 의 데이터가 표시되지 않습니다. 이러한 상황을 방지하기 위해 클러스터 내의 MOM 과 모든 Collector 에서 동일한 domains.xml 파일을 사용하는 것이 가장 좋습니다. 그러면 특정 Collector 와 연결된 Workstation 의 기록 데이터를 확인하기 위해 기록 에이전트를 마운트할 필요 없이 항상 라이브 및 기록 에이전트 데이터가 MOM Workstation 에 표시됩니다.

크로스 클러스터 데이터 뷰어(CDV)를 배포하는 경우 CDV domains.xml 파일에는 반드시 다음 도메인이 포함되어 있어야 합니다.

- CDV 와 연결되는 모든 Collector 의 모든 도메인
- CDV 가 데이터를 수집하는 Collector 가 속한 모든 클러스터의 모든 도메인

Collector 의 domains.xml 파일에 존재하는 도메인이 CDV 의 domains.xml 파일에 누락된 경우 다음과 같은 상황이 발생합니다.

- 누락된 Collector 도메인의 데이터가 CDV 에서 수집되지 않습니다.
- 누락된 Collector 도메인의 데이터가 CDV Workstation 에 표시되지 않습니다.

참고: domains.xml 작업에 대한 자세한 내용은 *CA APM 보안 안내서*를 참조하십시오.

MOM 구성

introscope.enterprisemanager.clustering.mode 속성을 구성하여 Enterprise Manager 를 수집기 집합의 MOM 으로 지정할 수 있습니다.

다음 단계를 따르십시오.

1. MOM 의 <EM_Home>\config 디렉터리에 있는 IntroscopeEnterpriseManager.properties 파일을 엽니다.
2. introscope.enterprisemanager.clustering.mode=MOM 를 설정합니다.

3. MOM 으로 관리되는 각 수집기마다 연결 속성을 정의합니다. 각 수집기마다 MOM 속성 파일에서 이 속성을 정의합니다. 각 연결 속성에서 `<emName>`은 다음과 같이 Collector Enterprise Manager 의 동일한 임의의 식별자입니다.
 - `introscope.enterprisemanager.clustering.login.<emName>.host` - 수집기 호스트 이름 또는 IP 주소를 지정합니다.
 - `introscope.enterprisemanager.clustering.login.<emName>.port` - 수집기의 수신기 포트를 지정합니다.
 - `introscope.enterprisemanager.clustering.login.<emName>.publickey` - 이 속성의 주석 처리를 제거하여 기본값인 `config/internal/server/EM.public` 로 설정합니다.

연결 속성을 독립적으로 설정하면 핫 구성 서비스를 사용하여 속성이 적용됩니다.
4. 파일을 저장하고 닫습니다.
5. Enterprise Manager 를 다시 시작하여 속성 설정을 적용합니다. `introscope.enterprisemanager.clustering.mode` 속성을 적용하려면 Enterprise Manager 를 다시 시작해야 합니다.

수집기 구성

속성을 구성하여 Enterprise Manager 를 수집기로 지정하고 수집기에 연결할 수 있는 최대 CDV 수를 설정할 수 있습니다.

다음 단계를 따르십시오.

1. 수집기의 `<EM_Home>\config` 디렉터리에 있는 `IntroscopeEnterpriseManager.properties` 파일을 엽니다.
2. `introscope.enterprisemanager.clustering.mode=Collector` 를 설정합니다.
3. (선택 사항) 이 수집기에 대해 특수 식별자를 지정하려면 `introscope.enterprisemanager.clustering.collector.identifier` 속성을 설정합니다.
수집기에 특정한 식별자를 지정하지 않으면 `host@port` 가 사용됩니다. `host` 는 Enterprise Manager 호스트 이름이고 `port` 는 Enterprise Manager 연결 포트입니다.
4. 파일을 저장하고 닫습니다.

- Enterprise Manager 를 다시 시작하여 속성 설정을 적용합니다.
- (선택 사항) 수집기에 연결하도록 허용되는 CDV 의 최대 수를 설정합니다.

중요! 수집기 및 CDV 9.1 에 해당: 모든 수집기와 CDV 는 버전 9.1 이상이어야 하고 모두 동일한 버전이어야 합니다. CDV 는 혼합된 CDV 또는 수집기 버전을 포함하는 클러스터에 있는 수집기에 연결될 수 없습니다.

하나 이상의 CDV 를 이 수집기에 연결하도록 구성하려면 다음과 같이 이 속성을 사용자 환경에 맞게 설정합니다.

- 수집기의 <EM_Home>\config 디렉터리에 있는 apm-events-thresholds-config.xml 파일을 엽니다.
- introscope.enterprisemanager.collector.cdv.max 속성을 설정합니다.
- apm-events-thresholds-config.xml 을 저장합니다.

이 설정은 약 60 초마다 한 번씩 발생하는 핫 배포 중에 Enterprise Manager 가 속성 파일을 검사할 때 적용됩니다.

CDV 정보

CDV(크로스 클러스터 데이터 뷰어)는 여러 클러스터의 여러 수집기에서 에이전트 및 고객 경험 메트릭 데이터를 수집하는 특수 Enterprise Manager 입니다. CDV Workstation 을 사용하면 수집기에서 제공하는 에이전트 및 고객 경험 메트릭의 통합 뷰를 표시하는 대시보드를 만들고 볼 수 있습니다. 수집기는 조직의 여러 데이터 센터에 있을 수 있습니다. 각 수집기를 여러 CDV 에 연결할 수 있으므로 서로 다른 CA APM 클러스터에 보고하는 응용 프로그램을 유연하게 모니터링하고 볼 수 있습니다.

조직에 각각의 자체 클러스터와 함께 여러 대규모 CA APM 배포가 있는 경우 CDV Workstation 을 사용하여 여러 클러스터의 응용 프로그램을 모니터링할 수 있습니다. 이 기능을 통해 응용 프로그램의 문제가 어느 클러스터에 있는지 확인할 수 있습니다.

참고: 에이전트는 CDV 에 연결되지 않습니다.

CDV 에 연결된 수집기를 보여 주는 다이어그램을 확인하려는 경우 CDV Workstation APM 상태 콘솔에서 Enterprise Manager 맵을 볼 수 있습니다.

참고: APM 상태 콘솔 사용에 대한 자세한 내용은 *CA Introscope Workstation 사용자 안내서*를 참조하십시오.

중요! 수집기 및 CDV 9.1 에 해당: 모든 수집기와 CDV 는 버전 9.1 이상이어야 하고 모두 동일한 버전이어야 합니다. CDV 는 혼합된 CDV 또는 수집기 버전을 포함하는 클러스터에 있는 수집기에 연결될 수 없습니다.

각 수집기는 `introscope.enterprisemanager.collector.cdv.max` 속성에 설정된 대로 서로 다른 개수의 CDV 에 연결할 수 있습니다. 따라서 CA APM 관리자나 심사자는 여러 응용 프로그램 모니터링 뷰를 제공하는 대시보드를 생성할 수 있습니다. 예를 들어 CA APM 환경이 다음과 같은 클러스터와 Enterprise Manager 로 구성되는 경우를 가정해 봅시다.

- 3 개의 클러스터: A, B, C
- 3 개의 CDV: 1, 2, 3
- 5 개의 수집기: 4, 5, 6, 7, 8
 - 수집기 4 와 5 는 클러스터 A 에 있습니다.
 - 수집기 6 과 7 은 클러스터 B 에 있습니다.
 - 수집기 8 은 클러스터 C 에 있습니다.

이 경우 CA APM 관리자는 다음과 같이 3 개의 CDV 를 구성합니다.

- CDV 1 은 클러스터 A 와 B 에 있는 수집기 4 와 6 에 연결됩니다.
- CDV 2 는 클러스터 A 와 C 에 있는 수집기 4 와 8 에 연결됩니다.
- CDV 3 은 클러스터 A 와 C 에 있는 수집기 5 와 8 에 연결됩니다.

CDV 구성

수집기 집합을 모니터링하도록 CDV 를 구성할 수 있습니다. 수집기는 서로 다른 클러스터에 속할 수 있습니다.

다음 단계를 따르십시오.

1. CDV 의 `<EM_Home>\config` 디렉터리로 이동하고 `IntroscopeEnterpriseManager.properties` 파일을 엽니다.
2. `introscope.enterprisemanager.clustering.mode=CDV` 를 설정합니다.
3. CDV 가 연결할 수집기 각각에 대해 연결 속성을 정의합니다.

중요! 수집기 및 CDV 9.1 에 해당: 모든 수집기와 CDV 는 버전 9.1 이상이어야 하고 모두 동일한 버전이어야 합니다. CDV 는 혼합된 CDV 또는 수집기 버전을 포함하는 클러스터에 있는 수집기에 연결될 수 없습니다.

각 수집기에 대해 해당 속성을 정의합니다. 각 속성에서 <emName>은 다음과 같이 수집기의 동일한 임의 식별자입니다.

- `introscope.enterprisemanager.clustering.login.<emName>.host` - 수집기 호스트 이름 또는 IP 주소를 지정합니다.
- `introscope.enterprisemanager.clustering.login.<emName>.port` - 수집기의 수신기 포트를 지정합니다.
- `introscope.enterprisemanager.clustering.login.<emName>.publickey` - 이 속성의 주석 처리를 제거하여 기본값인 `config/internal/server/EM.public` 로 설정합니다.

연결 속성을 독립적으로 설정하면 핫 구성 서비스를 사용하여 속성이 적용됩니다.

4. `IntroscopeEnterpriseManager.properties` 파일을 저장합니다.
5. Enterprise Manager 를 다시 시작하여 속성 설정을 적용합니다.

`introscope.enterprisemanager.clustering.mode` 속성을 적용하려면 Enterprise Manager 를 다시 시작해야 합니다.

CA APM 관리자와 심사자는 CDV Workstation 대시보드와 Investigator 메트릭 브라우저 트리에서 구성된 모든 수집기의 에이전트 메트릭 데이터를 볼 수 있습니다.

제 7 장: MOM 에이전트 부하 분산 구성

CA APM 클러스터 환경은 에이전트 부하 분산을 지원합니다. MOM 은 메트릭 부하와 사용 중인 CA Introscope 구성을 기반으로 에이전트 연결을 분산합니다. 에이전트는 사용 가능한 수집기에 연결됩니다.

이 섹션은 다음 항목을 포함하고 있습니다.

- [에이전트 부하 분산 개요 \(페이지 109\)](#)
- [MOM 이 수집기에 에이전트를 할당하는 방법 \(페이지 110\)](#)
- [MOM 이 클러스터를 재분산하는 방법 \(페이지 111\)](#)
- [에이전트 부하 분산 메트릭 가중 요소 설정 \(페이지 112\)](#)
- [에이전트 부하 분산 메트릭 임계값 설정 \(페이지 113\)](#)
- [에이전트 부하 분산 간격 속성 설정 \(페이지 114\)](#)
- [에이전트 부하 분산 사용 시나리오 \(페이지 115\)](#)
- [수집기에 대한 에이전트 할당 구성 \(페이지 117\)](#)

에이전트 부하 분산 개요

MOM 은 과부하 수집기에서 참여하는 에이전트의 연결을 끊어서 메트릭 수를 수집기에 균등하게 분산합니다. 연결이 끊긴 에이전트는 MOM 에 다시 연결한 다음 부하가 적은 수집기로 리디렉션됩니다. 부하 분산은 에이전트 메트릭 부하에만 적용되고 CA CEM 데이터 부하에는 적용되지 않습니다.

8.0 이전 에이전트에 해당: 8.0 이전 에이전트는 MOM 에 연결할 수 없고 대신에 수집기 중 하나에 직접 연결해야 합니다. 8.0 이전 에이전트가 MOM 에 대한 연결을 시도하면 다음과 같은 결과가 발생합니다.

- MOM 이 연결을 거부합니다.
- CA Introscope 가 MOM 로그와 에이전트 로그 모두에 경고 메시지를 기록합니다.

참고: 오버로드된 수집기의 부하 분산을 실행할 때 CA APM 9.1 이전 버전의 MOM 은 수집기에 직접 연결하도록 구성된 에이전트를 고려하지 않습니다. CA APM 버전 9.1 부터 MOM 은 9.1 이전 및 9.1 이상 버전의 에이전트를 고려하고 연결을 해제할 수 있습니다. 9.1 이전 버전 및 이후 에이전트를 특정 수집기에 연결된 상태로 유지하고 부하 분산되지 않도록 하려면 `loadbalancing.xml` 에 에이전트 - 수집기 요소를 추가하십시오.

참고: 사용자 클러스터가 에이전트와 TIM 을 포함하는 전체 부하를 처리하고 있으면 Enterprise Manager 서비스를 실행 중인 수집기에 [가중치](#) (페이지 112)를 사용하십시오. Enterprise Manager 서비스에서 리소스를 늘려야 할 수 있으므로 가중치를 사용하면 가능한 경우 감소된 메트릭 수용 능력을 보완할 수 있습니다.

MOM 이 수집기에 에이전트를 할당하는 방법

MOM 이 수집기에 에이전트를 할당하는 방법은 다음과 같은 여러 요소에 따라 결정됩니다.

- 에이전트와 수집기 간의 연결 기록이 없는 경우

에이전트가 처음 시작되거나 다시 시작되면 수집기와의 연결 기록이 없습니다. 이 경우 MOM 은 사용 가능한 수집기 중에서 부하 분산 구성을 기반으로 허용되는 수집기에 에이전트를 할당합니다.

- 연결 유형

에이전트는 해당 에이전트가 MOM 에 연결하는 데 사용하는 동일한 연결 유형을 지원하는 수집기에만 할당됩니다. 예를 들어 에이전트가 HTTP 를 사용하여 MOM 에 연결하는 경우에는 수집기의 HTTP 연결이 사용하도록 설정되어 있어야 합니다. 연결 유형 설정에 대한 자세한 내용은 *CA APM Java Agent 구현 안내서* 또는 *CA APM .NET 에이전트 구현 안내서*를 참조하십시오.

- loadbalancing.xml 파일에서 수행된 구성

loadbalancing.xml 파일에서 다음과 같이 구성합니다.

- 특정 수집기 집합에 대한 에이전트 연결을 허용하려면 `<include>` 문을 설정합니다.
- 특정 수집기 집합에 대한 에이전트 연결을 허용하지 않으려면 `<exclude>` 문을 설정합니다.
- 허용되는 수집기 집합 내의 특정 기본 설정 수집기에 에이전트를 연결하려면 `latched` 속성을 `true` 로 설정합니다.

- 에이전트와 특정 수집기 간의 연결 기록

CA Introscope 에는 에이전트가 한 수집기에서 클러스터 내의 다른 수집기로 전송될 때 SmartStor 데이터 급증을 방지하는 기능이 있습니다. 에이전트가 수집기에 연결한 적이 있으면 다음과 같은 경우를 제외하고 MOM 이 향후 연결에 해당 수집기를 선호합니다.

 - 수집기가 loadbalancing.xml 에서 허용하지 않도록 구성되어 있습니다.
 - 부하가 적은 다른 수집기를 사용할 수 있습니다.
 - 선호하는 수집기가 오버로드되었습니다.
- IntroscopeEnterpriseManager.properties 파일에서 수행된 구성

IntroscopeEnterpriseManager.properties 파일에서 다음과 같이 구성합니다.

 - 에이전트 부하 분산 메트릭 가중 요소를 설정합니다.
 - 에이전트 부하 분산 메트릭 임계값을 설정합니다.
 - [세분화된 에이전트 연결 구성](#) (페이지 127)의 경우 introscope.apm.agentcontrol.agent.allowed 속성을 설정합니다. 그러면 loadbalancing.xml 에 정의되지 않은 에이전트에 대한 허용 또는 허용 안 함 지침이 수집기에 제공됩니다.

MOM 이 클러스터를 재분산하는 방법

MOM 은 클러스터 메트릭 부하의 균형이 맞지 않는다고 감지하는 경우 수집기에서 에이전트의 연결을 끊고 다른 수집기로 리더렉션할 수 있습니다. 수집기 메트릭 부하가 가중치로 조정된 클러스터 평균에서 구성된 허용 한계를 넘어 벗어나면 클러스터의 균형이 맞지 않는 것입니다.

클러스터의 균형이 맞지 않게 되는 원인은 다음과 같습니다.

- 수집기 프로세스가 중지되었거나 에이전트의 연결이 끊어졌습니다.
- 새 수집기가 클러스터에 추가되었습니다.
- 여러 에이전트가 하나의 수집기에 직접 연결합니다.

MOM 은 클러스터 불균형을 규칙적으로 검사합니다. 클러스터의 균형이 맞지 않은 경우 MOM 은 비교적 메트릭 부하가 높은 수집기에서 에이전트의 연결을 끊어서 균형을 복원하려고 합니다. 연결이 끊긴 에이전트는 MOM 에 다시 연결하고 비교적 부하가 적은 수집기로 리디렉션됩니다. 그 목표는 가중치로 조정된 메트릭 부하를 클러스터에 균등하게 분산하는 에이전트를 할당하는 것입니다. MOM 은 에이전트가 동일한 수집기에 다시 할당된다고 확인하는 경우 에이전트의 연결을 끊지 않습니다.

에이전트 부하 분산 메트릭 가중 요소 설정

에이전트 부하 분산을 구성하면 MOM 이 가중치로 조정된 부하를 기반으로 에이전트를 수집기에 할당합니다. 클러스터에 있는 개별 수집기의 가중 요소를 조정할 수 있습니다. 수집기에서 처리할 수 있는 메트릭 수에 따라 클러스터에 있는 수집기의 상대적인 성능이 결정됩니다. 수집기에서 처리할 수 있는 메트릭 수에 영향을 주는 요소는 다음과 같습니다.

- 사용 가능한 CPU 용량
- 메모리
- Smartstor 디스크 IO 성능
- 수집기가 모든 할당된 Enterprise Manager 서비스를 실행하여 CA CEM 데이터 부하를 처리할지 여부

에이전트 부하 분산을 설정하는 경우 MOM 이 더 적은 수용 능력의 수집기에 보다 적은 개수의 메트릭을 할당하는 데 필요한 가중 요소를 구성할 수 있습니다. 더 강력한 수집기에서 보다 큰 메트릭 부하를 처리하도록 메트릭 가중치 부하를 설정하면 클러스터 성능 문제를 방지하는 데 도움이 됩니다.

`introscope.enterprisemanager.clustering.login.<emID>.weight` 속성의 값은 수집기의 상대 부하를 제어하는 양수입니다. 특정 수집기에 대한 가중치 값을 클러스터에 대한 모든 가중치 값의 합계로 나눈 것이 해당 수집기에 할당된 메트릭 부하의 백분율입니다. [MOM 이 수집기에 에이전트를 할당하는 방법](#) (페이지 110)을 결정하는 요소를 통해 이 동작을 수정할 수 있습니다.

참고: `introscope.enterprisemanager.clustering.login.<emID>.weight` 속성 이름에서 `<emID>`는 임의의 식별자입니다. 수집기마다 고유한 식별자가 있습니다. 사용자 환경에 적절한 식별자를 제공하십시오.

그러면 MOM 이 수집기에 에이전트를 할당할 때와 에이전트 메트릭 부하를 재분산할 때 가중치로 조정된 메트릭 수가 사용됩니다.

예를 들어 MOM 이 3 개의 수집기에 연결하고 이 수집기가 모두 현재 보고 중인 메트릭이 0 개인 경우를 가정합니다.

수집기 3 개의 가중치 설정은 다음과 같습니다.

- 수집기 A 의 가중치는 150 입니다.
- 수집기 B 의 가중치는 100 입니다.
- 수집기 C 의 가중치는 50 입니다.

이 경우 MOM 은 약 3:2:1 의 비율로 수집기 A, B 및 C 에 메트릭을 할당합니다.

다음 단계를 따르십시오.

1. <EM_Home>/config 디렉터리에 있는 IntroscopeEnterpriseManager.properties 파일을 엽니다.
2. 다음 속성을 설정하여 수집기에 가중 부하 요소를 할당합니다.
introscope.enterprisemanager.clustering.login.<emID>.weight
3. IntroscopeEnterpriseManager.properties 를 저장하고 닫습니다.

에이전트 부하 분산 메트릭 임계값 설정

introscope.enterprisemanager.loadbalancing.threshold 속성은 메트릭 불균형에 대한 클러스터 허용치 또는 임계값을 설정합니다.

기본 introscope.enterprisemanager.loadbalancing.threshold 속성 설정은 20,000 개의 메트릭입니다. 즉, 균형이 맞지 않는 메트릭 20,000 개가 수집기에 있어야 MOM 이 에이전트를 재분산합니다. 수집기가 가중치로 조정된 클러스터 평균과 비교해서 임계값보다 더 부족하거나 초과하면 수집기의 균형이 맞지 않은 것입니다. 예제는 [에이전트 부하 분산 사용 시나리오](#) (페이지 115)를 참조하십시오.

잘못된 재분산을 방지하는 부하 분산 임계값을 구성하십시오. 에이전트 메트릭 부하는 아주 안정적인 경향이 있습니다. 임계값을 너무 낮게 설정하면 문제 조사 중에 생성되는 일시적 메트릭으로 인해 재분산이 트리거될 수 있습니다.

다음 단계를 따르십시오.

1. <EM_Home>/config 디렉터리에 있는 IntroscopeEnterpriseManager.properties 파일을 엽니다.
2. 다음 속성을 설정하여 메트릭 불균형에 대한 클러스터 허용치를 구성합니다.
introscope.enterprise manager.loadbalancing.threshold
3. IntroscopeEnterpriseManager.properties 를 저장하고 닫습니다.

에이전트 부하 분산 간격 속성 설정

introscope.enterprise manager.loadbalancing.interval 속성은 MOM 에 가능한 재분산을 위하여 클러스터를 검사할 빈도를 지시합니다. 기본 간격은 600 초(10 분)이고 최소 간격은 120 초(2 분)입니다.

클러스터에는 에이전트가 다시 할당된 후 몇 분의 재조정 기간이 필요합니다. 부하 분산 간격이 너무 짧으면 클러스터가 이전의 부하 분산으로 조정되기 전에 재분산이 다시 시작될 위험이 있습니다. 응용 프로그램 심사 맵을 사용하면 이러한 위험이 더 커집니다. 이 경우 에이전트가 다시 할당될 때 새 수집기에 응용 프로그램 심사 맵 데이터를 다시 전송해야 하므로 시간이 소모될 수 있습니다. 다음 작업을 수행한 경우 너무 잦은 재분산의 결과로 인하여 불안정을 나타내는 징후가 있는지 조사하십시오.

- **CA Introscope 8.x 에 해당:** CA Introscope 8.x 부하 분산을 배포한 경우
- 부하 분산 간격을 기본값 미만으로 설정한 경우

다음 단계를 따르십시오.

1. <EM_Home>/config 디렉터리에 있는 IntroscopeEnterpriseManager.properties 파일을 엽니다.
2. 다음 속성을 설정하여 MOM 이 클러스터의 부하 분산을 검사하는 빈도를 구성합니다.
introscope.enterprise manager.loadbalancing.interval
3. IntroscopeEnterpriseManager.properties 를 저장하고 닫습니다.

에이전트 부하 분산 사용 시나리오

다음은 클러스터 환경에서 에이전트 부하 분산이 작동하는 방법을 이해하는 데 도움이 되는 시나리오입니다.

새 수집기가 클러스터에 추가될 때의 에이전트 부하 분산

3 개의 수집기 A, B 및 C 로 구성된 클러스터가 오버로드되었음을 확인합니다.

MOM 의 `IntroscopeEnterpriseManager.properties` 파일에 연결 속성 집합을 추가하여 수집기 D 를 동적으로 추가합니다. 또한 이 클러스터에 있는 모든 수집기의 재분산 임계값을 10,000 개의 메트릭으로 설정했습니다. 이를 위해 `IntroscopeEnterpriseManager.properties` 파일의 `introscope.enterprisemanager.loadbalancing.threshold` 속성을 설정했습니다.

평균 메트릭 부하는 수집기 A, B 및 C 각각에 30,000 개의 메트릭을 보고하는 것인데, 수집기 D 에 보고 중인 메트릭이 0 개입니다. 다음과 같은 이유로 MOM 이 클러스터를 재분산합니다.

- 평균 부하인 30,000 개 메트릭과 0 개 메트릭 간의 차이가 임계값인 10,000 개 메트릭보다 큼니다.

MOM 이 수집기 A, B 및 C 각각에 7,000 개의 메트릭을 재분산하고 보고할 메트릭 21,000 개를 모두 수집기 D 로 리디렉션합니다. 재분산 후 수집기 A 에는 23,000 개의 메트릭이, 수집기 B 에는 23,000 개의 메트릭이, 수집기 C 에는 23,000 개의 메트릭이, 수집기 D 에는 21,000 개의 메트릭이 보고됩니다.

에이전트를 가진 수집기가 추가될 때의 에이전트 부하 분산

MOM 이 수집기 A 와 B 에 연결합니다. 수집기 A 에는 36,000 개의 메트릭이, 수집기 B 에는 30,000 개의 메트릭이 보고됩니다.

`IntroscopeEnterpriseManager.properties` 파일의 `introscope.enterprisemanager.loadbalancing.threshold` 속성을 사용하여 메트릭 임계값을 10,000 개의 메트릭으로 설정했습니다. 24,000 개의 메트릭이 보고되는 수집기 C 가 클러스터에 추가됩니다.

다음과 같은 이유로 MOM 이 메트릭 부하를 재분산하지 않습니다.

- 수집기당 평균은 $[(36,000 + 30,000 + 24,000) = 90,000 \text{ 개의 메트릭} / 3 \text{ 개의 수집기}]$ 를 계산한 결과인 30,000 개의 메트릭입니다.
- 30,000 개에서 메트릭 임계값인 10,000 개보다 더 벗어난 수집기가 없습니다.

수집기에 장애가 발생할 때의 에이전트 부하 분산

MOM 이 수집기 A, B 및 C 에 연결됩니다. 36,000 개 메트릭은 수집기 A 에, 30,000 개 메트릭은 수집기 B 에, 24,000 개 메트릭은 수집기 C 에 보고됩니다. 수집기 A 에 장애가 발생하면 수집기 A 에 보고한 에이전트가 MOM 에 다시 연결됩니다. MOM 에서 약 15,000 개 메트릭을 수집기 B 로 리디렉션하고, 21,000 개 메트릭은 수집기 C 로 리디렉션합니다. 이제 수집기 B 와 수집기 C 모두에 45,000 개 메트릭이 보고되고 있습니다.

수집기가 다시 시작될 때의 에이전트 부하 분산

수집기 A 가 장애 후 복구될 때 클러스터의 균형이 맞지 않습니다. 평균 메트릭 부하는 $[0 + 45,000 + 45,000] / 3$ 을 계산한 결과인 30,000 개의 메트릭입니다. 그러나 수집기 B 와 C 각각에는 45,000 개의 메트릭이 보고되는데, 이는

- 평균보다 15,000 개의 메트릭이 더 많습니다.
- 임계값인 10,000 개의 메트릭을 초과합니다.

따라서 MOM 은 수집기 B 와 C 각각에서 총 15,000 개의 메트릭이 있는 에이전트의 연결을 끊고 30,000 개의 메트릭을 모두 수집기 A 로 리디렉션합니다. 따라서 수집기 A, B 및 C 에 각각 30,000 개의 메트릭이 보고되고 있습니다.

가중치가 적용된 에이전트 부하 분산

MOM 이 수집기 A, B 및 C 에 연결됩니다. 임계값은 10,000 으로 설정되어 있습니다. 수집기 A 에는 24,000 개의 메트릭이, 수집기 B 에는 30,000 개의 메트릭이, 수집기 C 에는 36,000 개의 메트릭이 보고되어 총 90,000 개의 메트릭이 보고됩니다. 클러스터에는 수집기당 평균 30,000 개 메트릭이 있습니다. 현재 수집기 A 의 가중치는 150 으로, 수집기 B 의 가중치는 100 으로, 수집기 C 의 가중치는 50 으로 설정되어 있습니다. 평균 가중치는 100(가중치 합계를 수집기 수로 나눈 값 또는 $(150 + 100 + 50)/3$)입니다.

원칙적으로 각 수집기의 메트릭 부하는 상대 가중치에 비례합니다. 수집기 A 는 가중치가 150 이므로 원칙적으로 45,000 개 메트릭이 있습니다. 가중치가 평균보다 50% 더 높으므로 메트릭 부하도 원칙적으로 30,000 개 메트릭 평균보다 50% 더 높습니다. 수집기 B 는 가중치가 평균이므로 원칙적으로 평균 메트릭 부하 또는 30,000 개 메트릭이 있습니다. 수집기 C 는 가중치가 평균의 50%이므로 원칙적으로 평균 메트릭 부하의 50% 또는 15,000 개 메트릭이 있습니다.

이러한 상대 가중치와 메트릭 평균을 바탕으로 할 때 클러스터의 균형이 맞지 않은 것입니다. 수집기 A 는 가중치로 조정된 평균에 비해 임계값보다 더 낮으므로 부하가 적습니다($24,000 - 45,000 = -21,000$). 수집기 B 는 30,000 개 메트릭에서 메트릭 부하가 가중치로 조정된 평균과 같으므로 균형이 완벽하게 맞습니다. 수집기 C 는 가중치로 조정된 평균에 비해 10,000 개 메트릭 임계값보다 더 높으므로 오버로드되었습니다($36,000 - 15,000 = 21,000$). MOM 이 21,000 개 메트릭이 있는 에이전트를 수집기 C 에서 수집기 A 로 리디렉션하여 클러스터를 재분산합니다.

수집기에 대한 에이전트 할당 구성

MOM loadbalancing.xml 을 사용하여 MOM 부하 분산 장치를 통해 수집기에 에이전트를 연결하는 작업의 할당을 제어하는 에이전트 요소를 구성합니다. 포함 및 제외 요소를 구성하여 특정 Enterprise Manager 에 대한 에이전트 연결을 허용하거나 허용하지 않도록 할 수 있습니다.

참고: 오버로드된 수집기의 부하 분산을 실행할 때 CA APM 9.1 이전 버전의 MOM 은 수집기에 직접 연결하도록 구성된 에이전트를 고려하지 않습니다. CA APM 버전 9.1 부터 MOM 은 9.1 이전 및 9.1 이상 버전의 에이전트를 고려하고 연결을 해제할 수 있습니다. 9.1 이전 버전 및 이후 에이전트를 특정 수집기에 연결된 상태로 유지하고 부하 분산되지 않도록 하려면 loadbalancing.xml 에 에이전트 - 수집기 요소를 추가하십시오.

다음 단계를 따르십시오.

1. MOM 에서 <EM_Home>/config 디렉터리로 이동합니다.
2. loadbalancing.xml 을 엽니다.
3. 사용자 환경의 요구 사항에 맞게 속성을 정의합니다.

이러한 속성을 정의할 때 다음 지침과 함께 [에이전트 부하 분산 구성 예제](#) (페이지 121)를 사용하십시오.

- <agent-collector name> 특성은 선택 사항입니다.
- MOM 부하 분산 장치는 <agent-collector> 요소를 순차적으로 평가합니다.

연결하는 에이전트가 <agent-specifier> 정규식과 일치하는 경우 이 에이전트는 <include> 목록의 수집기에 할당됩니다.

loadbalancing.xml 에서 첫 번째로 일치하는 <agent-specifier>가 우선합니다. <include> 목록이 없으면 이 에이전트는 <exclude> 목록에 없는 수집기에 할당됩니다. 사용 가능한 수집기 중에서 이러한 제한 사항을 충족하는 수집기가 없으면 수집기 연결에 대한 에이전트 요청이 거부됩니다.

- 각 <agent-collector> 요소에 대해 에이전트 집합과 일치할 <agent-specifier> 요소를 하나 이상 정의합니다.
- <agent-specifier>의 텍스트 콘텐츠는 Perl5 정규식(예: *|\.*|\EPAgent1</agent-specifier>)이어야 합니다.

참고: 에이전트 지정자 정규식에는 에이전트 경로 이름의 세 가지 요소, 즉 <host machine name>|<custom process name>|<agent name>이 포함되어야 합니다. 예를 들어 EPAgent 로 시작하는 이름의 에이전트를 모두 포함하려면 다음 콘텐츠를 사용합니다.

```
<agent-specifier>.*|\.*|\EPAgent.*</agent-specifier>
```

- <agent-collector> 요소의 경우 포함 목록을 비워 둘 수 있습니다. 에이전트 연결이 허용되는 수집기가 포함 목록에 포함될 수도 있습니다.

- 포함 목록을 비워 두면 어떤 수집기에 대해서도 에이전트 연결이 허용되지 않습니다.

```
<include>  
</include>
```

- `<include>` 요소와 `</include>` 요소 내에 에이전트 연결이 허용되는 수집기를 추가할 수 있습니다.

이 예제에서는 에이전트가 `localhost@5002` 라는 수집기에서만 허용됩니다.

```
<include>
  <collector host="localhost" port="5002"/>
</include>
```

- `<agent-collector>` 요소의 경우 제외 목록을 비워 둘 수 있습니다. 에이전트 연결이 허용되지 않는 수집기가 포함 목록에 포함될 수도 있습니다.

- 제외 목록을 비워 두면 모든 수집기에 대해 에이전트 연결이 허용됩니다.

```
<exclude>
</exclude>
```

- `<exclude>` 요소와 `</exclude>` 요소 내에 에이전트 연결이 허용되지 않는 수집기를 추가할 수 있습니다.

이 예제에서는 에이전트가 `localhost@5002` 라는 수집기에서만 허용되지 않습니다.

```
<exclude>
  <collector host="localhost" port="5002"/>
</exclude>
```

- 특정 수집기를 사용할 수 있는 경우 언제나 이 수집기로 연결하도록 기본 설정을 지정하려면 `latched` 속성을 `true` 로 설정하십시오. 이 수집기를 *래치된* 수집기라고 합니다.

이 예제에서는 에이전트가 포트 6001 에서 `newCollector-ip` 라는 수집기에 래치됩니다. `newCollector-ip` 를 사용할 수 없으면 MOM 이 `Collector1-ip` 에 에이전트를 할당할 수 있습니다.

```
<include>
  <Collector host="newCollector-ip" port="6001" latched="true" />
  <Collector host="Collector1-ip" port="6001" />
</include>
</agent-Collector>
```

포함 목록에 수집기를 하나만 추가하면 `latched` 속성 설정이 필요하지 않습니다.

`latched=true` 로 설정한 수집기가 여러 개이면 래치된 모든 수집기에 연결 기본 설정이 적용됩니다.

`latched` 속성을 `true` 로 설정한 경우 수집기가 오버로드되면 **MOM** 이 수집기에서 에이전트의 연결을 끊지 않습니다. 래치된 수집기가 다운되면 연결이 끊긴 에이전트가 사용 가능한 다른 래치된 수집기 중에서 허용되는 래치된 수집기에 연결합니다.

사용 가능한 래치된 수집기가 없으면 에이전트가 허용되는 수집기에 연결합니다. 사용 가능한 수집기 중에서 허용되는 수집기가 없는 경우 [에이전트 동작은 에이전트 버전에 따라 다릅니다](#) (페이지 134).

예를 들어 사용자 환경에 10 개의 수집기가 있으면 하나 이상의 수집기에 래치하도록 에이전트를 구성할 수 있습니다. 래치된 수집기가 모두 사용할 수 없게 되면 **MOM** 이 에이전트를 사용할 수 있는 다른 래치되지 않은 수집기로 리디렉션할 수 있습니다.

수집기에 `latched` 속성을 설정하지 않으면 래치된 수집기가 모두 사용할 수 없게 된 경우에만 에이전트가 해당 수집기에 연결합니다.

`latched` 속성의 기본값은 `false` 입니다.

- 크로스 클러스터 데이터 뷰어를 하나 이상 배포한 상태에서 부하 분산을 사용하는 경우 원하는 에이전트를 오직 **CDV** 가 연결하는 수집기에만 연결하십시오. 그렇지 않으면 **MOM** 이 다른 수집기에 대한 **CDV** 연결이 있는 수집기에서 에이전트 부하를 분산할 수 있습니다. 이 경우 다음과 같은 이벤트가 발생합니다.
 - **CDV** 가 이동된 에이전트에 대한 메트릭 데이터를 수집할 수 없습니다.
 - **CDV Workstation** 사용자가 이동된 에이전트에 대한 데이터를 볼 수 없습니다.
- 같은 클러스터에 호스트된 수집기에 부하 분산 에이전트를 로드하려면 기본 통신 채널과 관련된 포트 번호를 제공하십시오. 기본 포트는 5001 입니다.

이러한 에이전트와 **Enterprise Manager** 사이의 모든 통신 프로토콜에 대해 올바른 포트 번호를 제공하십시오.

- 직접 소켓 연결
- HTTP 터널링 연결, 또는 프록시 서버를 통한 HTTP 터널링
- HTTPS 연결
- SSL 연결

- 다른 클러스터에 호스트된 수집기에 부하 분산 에이전트를 로드하려면 특정 보안 통신 채널과 관련된 포트 번호를 제공하십시오. 한 클러스터의 MOM 은 다른 클러스터의 수집기에 대한 속성을 볼 수 없습니다.

이러한 에이전트와 Enterprise Manager 사이의 모든 통신 프로토콜에 대해 올바른 특정 보안 통신 채널 포트 번호를 제공하십시오.

- 직접 소켓 연결. 기본 통신 채널(기본적으로 포트 5001)에 대한 포트를 제공하십시오.
- HTTP 터널링 연결, 또는 프록시 서버를 통한 HTTP 터널링. HTTP 포트(기본적으로 8081)를 제공합니다.
- HTTPS 연결. HTTPS 포트(기본적으로 8444)를 제공하십시오.
- SSL 연결. SSL 포트(기본적으로 5443)를 제공하십시오.

4. loadbalancing.xml 을 저장하고 닫습니다.

새 값은 핫 배포 중에 Enterprise Manager 가 속성 파일을 검사할 때 자동으로 적용됩니다. 핫 배포는 약 60 초마다 한 번씩 발생합니다. MOM 은 다음 부하 분산 간격에 도달할 때 클러스터의 부하를 분산합니다.

에이전트 부하 분산 구성 예제

여러 방법으로 MOM 에이전트 부하 분산 속성을 구성할 수 있습니다. 다음 구성 예제에서는 코드 샘플을 제공합니다.

- [특정 수집기 또는 수집기 집합에 에이전트 할당](#) (페이지 122)
- [특정 수집기 또는 수집기 집합에서 에이전트 제외](#) (페이지 123)
- [여러 에이전트를 여러 수집기에 할당](#) (페이지 123)
- [같은 클러스터의 특정 수집기로 에이전트 할당](#) (페이지 124)
- [다른 클러스터의 특정 수집기로 에이전트 할당](#) (페이지 125)

특정 수집기 또는 수집기 집합에 에이전트 할당

다음 예제에서는 포트 5001 에서 "myhost"라는 수집기에 MyAgent 라는 에이전트를 할당하도록 구성하는 방법을 보여 줍니다.

```
<agent-collector name="Assign MyAgent to One Collector Example">
  <agent-specifier>.*\|.*\|MyAgent</agent-specifier>
  <include>
    <collector host="myhost" port="5001"/>
  </include>
</agent-collector>
```

다음 예제에서는 아래 조건을 기반으로 latched 속성을 구성하는 방법을 보여 줍니다.

- 에이전트가 포트 6001 에서 "newCollector-ip"라는 수집기에 연결하도록 할당됩니다.
- newCollector-ip 를 사용할 수 없으면 MOM 이 이름에 "EPAgent"가 포함된 에이전트를 Collector1-ip 나 Collector2-ip 에 모두 할당할 수 있습니다.

```
<agent-Collector name="Latch when Collector Unavailable Example">
  <agent-specifier>.*\|.*\|EPAgent.*</agent-specifier>
  <include>
    <Collector host="newCollector-ip" port="6001" latched="true" />
    <Collector host="Collector1-ip" port="6001" />
    <Collector host="Collector2-ip" port="6001" />
  </include>
</agent-Collector>
```

다음 예제에서는 아래 조건을 기반으로 에이전트를 할당하는 방법을 보여 줍니다.

- 포트 5001 과 5002 에서 수집기에 "localhost"라는 이름이 지정됩니다.
- 수집기 localhost:5001 이 localhost:5002 보다 우선합니다.

```
<agent-collector name="Allow EPAgents on Two Collectors and One is Preferred Example">
  <agent-specifier>.*\|.*\|EPAgent.*</agent-specifier>
  <include>
    <collector host="localhost" port="5001" latched="true"/>
    <collector host="localhost" port="5002"/>
  </include>
</agent-collector>
```

다음 예제에서는 아래 조건을 기반으로 에이전트를 할당하는 방법을 보여 줍니다.

- 포트 5001, 5002, 5003 및 5004 에서 수집기에 "localhost"라는 이름이 지정됩니다.

- 수집기 localhost:5001 과 localhost:5003 이 localhost:5002 와 localhost:5004 보다 우선합니다.

```
<agent-collector name="Allow EPAgents on Four Collectors and Two are Preferred Example">
  <agent-specifier>.*\|.*\|EPAgent.*</agent-specifier>
  <include>
    <collector host="localhost" port="5001" latched="true"/>
    <collector host="localhost" port="5002"/>
    <collector host="localhost" port="5003" latched="true"/>
    <collector host="localhost" port="5004"/>
  </include>
</agent-collector>
```

특정 수집기 또는 수집기 집합에서 에이전트 제외

다음 예제에서는 MyHost 라는 수집기에서 MyAgent 라는 에이전트를 제외하는 방법을 보여 줍니다.

```
<agent-collector name="Exclude MyAgent from a Collector Example">
  <agent-specifier>.*\|.*\|MyAgent</agent-specifier>
  <exclude>
    <collector host="MyHost" port="5001"/>
  </exclude>
</agent-collector>
```

다음 예제에서는 여러 에이전트를 여러 수집기에서 제외하는 방법을 보여 줍니다.

```
<agent-collector name="Exclude Two Agents Assigned from Two Collectors Example">
  <agent-specifier>.*\|.*\|MyAgent.*</agent-specifier>
  <agent-specifier>.*\|.*\|MyOtherAgent.*</agent-specifier>
  <exclude>
    <collector host="MyHost" port="5001"/>
    <collector host="MyOtherHost" port="5001"/>
  </exclude>
</agent-collector>
```

여러 에이전트를 여러 수집기에 할당

다음 예제에서는 여러 에이전트를 여러 수집기에 할당하는 방법을 보여 줍니다.

```
<agent-collector name="Two Agents Assigned to Two Collectors Example">
  <agent-specifier>.*\|.*\|MyAgent.*</agent-specifier>
  <agent-specifier>.*\|.*\|MyOtherAgent.*</agent-specifier>
  <include>
    <collector host="MyHost" port="5001"/>
    <collector host="MyOtherHost" port="5001"/>
  </include>
</agent-collector>
```

같은 클러스터의 특정 수집기로 에이전트 할당

다음 예는 다음과 같은 환경의 클러스터 내에 있는 수집기에 EPAgent란 이름의 에이전트를 할당하는 방법을 보여 줍니다.

- 이름이 "host1"과 "host2"인 수집기는 모두 같은 클러스터에 있습니다.
- host1 또는 host2 에 연결하는 EPAgent 는 다음과 같은 연결을 사용할 수 있습니다.
 - 직접 소켓 연결
 - HTTP
 - HTTPS
 - SSL
- 수집기 host1 과 host2 는 모두 기본 통신 채널 포트로 포트 5001 을 사용합니다.
- host1 을 사용할 수 없는 경우 MOM 은 이름에 "EPAgent"가 포함된 모든 에이전트를 host2 에 할당할 수 있습니다.

MOM 과 loadbalancing.xml 은 host1 과 host2 에 에이전트를 할당하기 위해 기본 통신 채널 포트를 사용합니다.

<agent-collector name="같은 클러스터의 두 개 수집기에서 EPAgent 허용 예제">

```
<agent-specifier>.*\|.*\|EPAgent.*</agent-specifier>
<include>
  <collector host="host01" port="5001"/>
  <collector host="host02" port="5001"/>
</include>
</agent-collector>
```

다른 클러스터의 특정 수집기로 에이전트 할당

다음 예는 다음과 같은 환경의 다른 클러스터에 있는 수집기에 EPAgent란 이름의 에이전트를 할당하는 방법을 보여 줍니다.

- 이름이 "host1"과 "host2"인 수집기는 다른 클러스터에 있습니다.
- host1 또는 host2에 연결하는 EPAgent는 다음과 같은 연결을 사용할 수 있습니다.
 - 직접 소켓 연결
 - HTTP
 - HTTPS
 - SSL
- host1을 사용할 수 없는 경우 MOM은 이름에 "EPAgent"가 포함된 모든 에이전트를 host2의 특정 통신 포트에 할당할 수 있습니다.

MOM과 loadbalancing.xml은 host1과 host2에 에이전트를 할당하기 위해 특정 EPAgent-Enterprise Manager 통신 채널 포트를 사용합니다.

다음 예는 직접 소켓 연결을 사용하여 에이전트가 수집기에 연결할 때 다른 클러스터의 수집기에 EPAgent를 할당하는 방법을 보여 줍니다.

```
<agent-collector name="다른 클러스터의 두 수집기에서 EPAgent 허용 - 직접 소켓 연결 예제">
  <agent-specifier>.*\|.*\|EPAgent.*</agent-specifier>
  <include>
    <collector host="host01" port="5001"/>
    <collector host="host02" port="5001"/>
  </include>
</agent-collector>
```

다음 예는 HTTP를 사용하여 에이전트가 수집기에 연결할 때 다른 클러스터의 수집기에 EPAgent를 할당하는 방법을 보여 줍니다.

```
<agent-collector name="다른 클러스터의 두 수집기에서 EPAgent 허용 - HTTP 예제">
  <agent-specifier>.*\|.*\|EPAgent.*</agent-specifier>
  <include>
    <collector host="host01" port="8081"/>
    <collector host="host02" port="8081"/>
  </include>
</agent-collector>
```

다음 예는 HTTPS 를 사용하여 에이전트가 수집기에 연결할 때 다른 클러스터의 수집기에 EPAgent 를 할당하는 방법을 보여 줍니다.

```
<agent-collector name="다른 클러스터의 두 수집기에서 EPAgent 허용 - HTTPS 예제">
  <agent-specifier>.*\|.*\|EPAgent.*</agent-specifier>
  <include>
    <collector host="host01" port="8444"/>
    <collector host="host02" port="8444"/>
  </include>
</agent-collector>
```

다음 예는 SSL 를 사용하여 에이전트가 수집기에 연결할 때 다른 클러스터의 수집기에 EPAgent 를 할당하는 방법을 보여 줍니다.

```
<agent-collector name="다른 클러스터의 두 수집기에서 EPAgent 허용 - SSL 예제">
  <agent-specifier>.*\|.*\|EPAgent.*</agent-specifier>
  <include>
    <collector host="host01" port="5443"/>
    <collector host="host02" port="5443"/>
  </include>
</agent-collector>
```

제 8 장: 에이전트 - Enterprise Manager 네트워크 토폴로지 구성

다음 컴퓨터에 연결할 수 있는 특정 에이전트 또는 에이전트 그룹을 계획 및 구성할 수 있습니다.

- 특정 독립 실행형 Enterprise Manager
- 수집기
- 수집기 그룹

CA APM에서는 이 프로세스를 CA APM 에이전트 - Enterprise Manager 네트워크 토폴로지(또는 구조) 계획 및 구성이라고 합니다.

이 섹션은 다음 항목을 포함하고 있습니다.

[에이전트 - Enterprise Manager 네트워크 토폴로지 개요](#) (페이지 128)

[에이전트 연결 정보가 CA Introscope 에 전파되는 방법](#) (페이지 130)

[구성이 에이전트와 Enterprise Manager 의 연결에 미치는 영향](#) (페이지 132)

[Enterprise Manager 에서 에이전트의 연결이 끊길 때 발생하는 결과](#) (페이지 133)

[에이전트 연결 요청이 거부될 때 발생하는 결과](#) (페이지 134)

[에이전트 - Enterprise Manager 네트워크 토폴로지 구성 프로세스](#) (페이지 135)

[에이전트 - Enterprise Manager 네트워크 토폴로지 계획](#) (페이지 136)

[loadbalancing.xml 규칙이 없을 때 새 에이전트 연결 허용 여부 구성](#) (페이지 138)

[에이전트 다시 연결 대기 시간 구성](#) (페이지 139)

[허용되지 않는 에이전트 연결 클램프 제한 구성](#) (페이지 140)

[계속해서 허용된 Enterprise Manager 에 다시 연결하도록 에이전트 구성](#) (페이지 141)

[Enterprise Manager 별로 허용되거나 허용되지 않는 에이전트에 대한 loadbalancing.xml 구성](#) (페이지 143)

[에이전트 - Enterprise Manager 네트워크 토폴로지 문제 해결](#) (페이지 143)

에이전트 - Enterprise Manager 네트워크 토폴로지 개요

에이전트 - Enterprise Manager 네트워크 토폴로지를 계획하고 구성하는 목적은 CA APM 성능 문제를 방지하거나 줄이는 데 있습니다. 예를 들어 다음과 같은 상황을 방지합니다.

- 새 에이전트가 무작위로 시작되어 특정 수집기를 연결로 가득 채우는 경우
- 테스트 환경의 에이전트가 프로덕션 환경에 연결되는 경우

다음과 같은 파일과 속성을 사용하여 에이전트가 특정 독립 실행형 Enterprise Manager 또는 수집기에 연결되는 방법과 시기를 제어할 수 있습니다.

- loadbalancing.xml 파일
- EnterpriseManager.properties 파일의 introscope.apm.agentcontrol.agent.allowed 속성
- IntroscopeAgent.profile 파일의 introscope.agent.enterprisemanager.failbackRetryIntervalInSeconds 속성

[loadbalancing.xml](#)에서 [MOM 에이전트 부하 분산 구성](#) (페이지 117)을 수행하는 경우 다음과 같은 요인을 기반으로 에이전트를 이동할 위치를 MOM에 알립니다.

- 수집기 수용 능력
- 생성 중인 에이전트 메트릭 수
- 수집기 수용 능력 가중치

예

사용자 환경은 하나의 MOM과 5개의 수집기로 구성됩니다. 에이전트 1과 에이전트 2의 부하를 수집기 1과 수집기 2에 분산하려는 경우 해당 에이전트와 Enterprise Manager 간의 연결에 대해 다음과 같이 loadbalancing.xml을 구성합니다.

- 수집기 1 및 2에 대해서는 에이전트 1과 에이전트 2의 연결을 허용합니다.
- 수집기 3, 4 및 5에 대해서는 해당 에이전트의 연결을 허용하지 않습니다.

오버로드가 있는 경우 MOM 은 다음과 같이 에이전트를 처리합니다.

- 런타임 클러스터 부하에 따라 에이전트 1 과 에이전트 2 를 수집기 1 과 수집기 2 에 할당합니다.
- 수집기 3, 4 또는 5 에 대해서는 해당 에이전트의 연결을 허용하지 않습니다.

loadbalancing.xml 을 세분화된 에이전트와 Enterprise Manager 간 연결 설정에 사용할 수도 있습니다. 그러면 MOM 이 클러스터에서 해당 연결을 수행합니다. 이 장에서는 세분화된 에이전트와 Enterprise Manager 간 연결을 구현할 수 있는 방법을 설명합니다.

MOM 은 시작할 때 그리고 10 분마다 loadbalancing.xml 에 설정된 에이전트 연결 허용 및 허용 안 함 규칙을 각 수집기에 보냅니다. 수집기는 이러한 규칙을 사용하여 에이전트가 연결을 요청할 때 허용하거나 거부할 에이전트를 인식합니다. 규칙이 수집기에서 에이전트로 전송되므로 각 에이전트는 다음과 같은 작업이 발생할 때 연결할 수 있는 수집기를 인식합니다.

- MOM 이 다운됩니다.
- 수집기가 허용하지 않음 구성 설정을 기반으로 에이전트 연결 요청을 거부합니다.

[에이전트와 Enterprise Manager 간의 연결이 거부](#) (페이지 134)된 경우 APM 상태 콘솔의 "거부된 에이전트" 목록에 항목이 표시됩니다. Enterprise Manager 에 수동적으로 연결된 에이전트가 데이터를 보내고 있지 않은 경우에도 APM 상태 콘솔의 "거부된 에이전트" 목록에 항목이 표시됩니다.

APM 상태 콘솔의 "거부된 에이전트" 목록을 사용하여 특정 에이전트 또는 에이전트 그룹에서 반복적으로 거부되는 연결과 수동 연결을 모니터링할 수 있습니다. 그런 다음 거부된 에이전트나 수동 에이전트와 다른 수집기 간의 연결을 허용하도록 loadbalancing.xml 을 구성할 수 있습니다.

에이전트 연결 정보가 CA Introscope 에 전파되는 방법

CA Introscope 는 에이전트와 Enterprise Manager 간의 연결 정보(MOM 에서 정의할 수 있음)를 제어할 수 있습니다. MOM 은 연결된 구성이 클러스터에 있는 수집기와 에이전트에서 모두 수행되도록 합니다.

MOM 은 loadbalancing.xml 을 모든 수집기에 주기적으로 전송하여 클러스터에서 loadbalancing.xml 을 동기화합니다. CA Introscope 는 수집기나 CDV 의 loadbalancing.xml 구성을 무시합니다.

수집기가 loadbalancing.xml 을 수신한 후 MOM 이 다운되면 수집기가 MOM 에서 수신한 loadbalancing.xml 의 허용 또는 허용 안 함 구성이 사용됩니다. 수집기가 MOM 에 연결된 적이 없으면 수집기에서 IntroscopeEnterpriseManager.properties 파일에 있는 introscope.apm.agentcontrol.agent.allowed 속성을 사용하여 에이전트 연결을 허용합니다. MOM 이 수집기에 처음 연결되면 MOM 에서 introscope.apm.agentcontrol.agent.allowed 속성 값을 수집기에 전송합니다. MOM 값이 수집기 값을 재정의합니다.

또한 수집기는 loadbalancing.xml 에 정의되지 않은 에이전트의 허용 또는 허용하지 않음 지침에 introscope.apm.agentcontrol.agent.allowed 속성을 사용합니다.

또한 MOM 은 에이전트 연결이 허용된 사용 가능한 Enterprise Manager 목록을 에이전트에 제공합니다. 이 목록을 "Allowed Enterprise Manager"(허용된 Enterprise Manager) 목록이라고 합니다. "Allowed Enterprise Manager"(허용된 Enterprise Manager) 목록은 Enterprise Manager IP 주소를 기반으로 하므로 다양한 클러스터의 Enterprise Manager 를 포함할 수 있습니다.

"Allowed Enterprise Manager"(허용된 Enterprise Manager) 목록은 다음 컴퓨터에 장애가 발생할 때 Enterprise Manager 가 연결할 에이전트를 지정합니다.

- MOM
- 독립 실행형 Enterprise Manager
- 에이전트가 연결되는 최초의 수집기

다음 요소가 둘 다 발생하면 Enterprise Manager 가 loadbalancing.xml 지침을 기반으로 "Allowed Enterprise Manager"(허용된 Enterprise Manager) 목록을 준비합니다.

- 독립 실행형 Enterprise Manager 가 다운됩니다.
- 사용자 환경에 독립 실행형 Enterprise Manager 와 클러스터가 모두 포함되어 있습니다.

"Allowed Enterprise Manager"(허용된 Enterprise Manager) 목록은 에이전트를 다른 독립 실행형 Enterprise Manager 나 수집기로 보냅니다.

에이전트는 다시 시작될 때 자체의 IntroscopeAgent.profile 파일에 있는 introscope.agent.enterprisemanager.connectionorder 속성에서 초기 수집기 연결 정보를 가져옵니다. 이 속성에는 정의된 값 외에도 허용된 수집기가 자동으로 제공됩니다. 허용된 사용 가능한 수집기 또는 독립 실행형 Enterprise Manager 목록은 에이전트가 다시 시작될 때까지 에이전트 메모리에 남아 있습니다. 에이전트가 다시 시작되면 허용된 사용 가능한 Enterprise Manager 목록이 수집기에서 에이전트로 전송됩니다.

구성이 에이전트와 Enterprise Manager 의 연결에 미치는 영향

에이전트가 Enterprise Manager 에서 허용되거나 허용되지 않도록 구성된 경우 에이전트에서 연결을 요청하면 Enterprise Manager 가 다양한 동작을 수행할 수 있습니다. Enterprise Manager 는 연결을 수락하거나 거부할 수 있습니다. Enterprise Manager 가 연결 요청을 수락하는 경우 에이전트는 다음 두 가지 방법 중 하나로 연결할 수 있습니다.

- 능동적으로 연결하고 메트릭 데이터를 Enterprise Manager 에 전송합니다.
- 수동적으로 연결하고 데이터를 전송하지 않습니다.

[Enterprise Manager 가 연결 요청을 거부](#) (페이지 134)하는 경우 에이전트 동작은 에이전트 버전에 따라 다릅니다.

에이전트 버전과 허용된 구성 및 허용되지 않은 구성을 기준으로 Enterprise Manager 는 세 가지 동작을 수행할 수 있습니다. 이러한 동작의 결과로 네 가지 에이전트 연결 상태가 발생할 수 있습니다. 이러한 상태 중 두 가지 경우에는 에이전트가 APM 상태 콘솔의 "거부된 에이전트" 목록에 표시됩니다.

다음 표에서는 허용되도록 구성된 에이전트 및 허용되지 않도록 구성된 에이전트가 Enterprise Manager 연결을 요청할 때 Enterprise Manager, 에이전트 및 APM 상태 콘솔이 수행할 수 있는 동작을 보여 줍니다.

에이전트 버전	허용됨/허용되지 않음 구성	연결 요청 시 Enterprise Manager 동작	결과로 발생하는 에이전트 연결 상태	APM 상태 콘솔의 "거부된 에이전트" 목록에 표시되는지 여부
9.1	허용됨	능동적 연결 수락	연결됨 - 에이전트가 능동적으로 데이터를 전송함	아니요
9.1 이전	허용됨	능동적 연결 수락	연결됨 - 에이전트가 능동적으로 데이터를 전송함	아니요
9.1	허용되지 않음	연결 거부	연결 끊김	예

에이전트 버전	허용됨/허용되지 않음 구성	연결 요청 시 Enterprise Manager 동작	결과로 발생하는 에이전트 연결 상태	APM 상태 콘솔의 "거부된 에이전트" 목록에 표시되는지 여부
9.1	허용되지 않음	수동적 연결 수락	연결됨 - 에이전트가 수동적이며 데이터를 전송하지 않음	예
9.1 이전	허용되지 않음	연결 거부	연결 끊김 - 에이전트가 연결을 다시 시도함	예

Enterprise Manager 에서 에이전트의 연결이 끊길 때 발생하는 결과

Enterprise Manager 에서 에이전트의 연결이 끊기는 경우를 예로 들면 에이전트의 부하가 분산되거나 Enterprise Manager 가 다운되는 경우가 있습니다. 또한 구성 변경을 통해 Enterprise Manager 가 이전에 연결이 허용된 에이전트를 허용하지 말라는 지침을 받는 경우에도 에이전트의 연결이 끊깁니다. Enterprise Manager 는 이제 허용되지 않도록 구성된 연결된 에이전트의 연결을 끊어서 이러한 지침에 응답합니다.

9.1 이전 에이전트에 해당: 이러한 에이전트는 다음과 같은 동작이 발생하면 Enterprise Manager 와의 연결이 끊어집니다.

- 속성 또는 `loadbalancing.xml` 구성이 수집기에 대한 에이전트 연결을 허용됨에서 허용되지 않음으로 변경합니다.
- 에이전트가 연결된 Enterprise Manager 를 더 이상 연결에 사용할 수 없습니다.

9.1 에이전트에 해당: 이러한 에이전트는 허용됨에서 허용되지 않음으로 구성이 변경되고

`introscope.enterprisemanager.agent.disallowed.connection.limit` 클램프 값에 도달하면 Enterprise Manager 와의 연결이 끊어집니다.

에이전트 연결 요청이 거부될 때 발생하는 결과

loadbalancing.xml 과 introscope.apm.agentcontrol.agent.allowed 속성에 설정된 구성을 기반으로 특정 Enterprise Manager 에 대한 에이전트 연결이 허용되거나 허용되지 않습니다. 에이전트가 Enterprise Manager 에 대한 연결을 요청하면 Enterprise Manager 가 연결 요청을 수락하거나 거부할 수 있습니다.

다음 동작이 발생하면 에이전트 연결이 거부됩니다.

- introscope.apm.agentcontrol.agent.allowed 속성이 true 로 설정되고 loadbalancing.xml 에서 에이전트를 허용하지 않습니다.
- introscope.apm.agentcontrol.agent.allowed 속성이 false 로 설정되고 loadbalancing.xml 에서 에이전트를 명시적으로 허용하지 않습니다.
- 다음 클램프 값 중 하나에 도달하거나 해당 값을 초과합니다.
 - introscope.enterprisemanager.agent.disallowed.connection.limit
 - introscope.enterprisemanager.agent.connection.limit

Enterprise Manager 가 에이전트 연결 요청을 거부하면 다음 동작이 발생할 수 있습니다.

- Enterprise Manager 에 연결된 에이전트의 연결이 끊어집니다.
- 연결이 끊긴 에이전트가 연결이 허용된 다른 Enterprise Manger 에 대한 연결을 시도합니다.

에이전트는 연결할 수 있을 때까지 또는 다음과 같은 Enterprise Manager 가 더 이상 없을 때까지 계속해서 Enterprise Manager 연결을 시도합니다.

- 에이전트가 연결하도록 허용된 Enterprise Manager
- 연결에 사용 가능한 Enterprise Manager

에이전트가 모든 Enterprise Manager 에서 거부된 경우 에이전트 동작은 introscope.agent.profile 파일에 있는 introscope.agent.enterprisemanager.failbackRetryIntervalInSecondsproperty 설정에 따라 다릅니다. 설정된 속성 구성에 따라 다음 동작이 발생합니다.

- 속성 구성의 주석 처리가 제거되고 기간이 설정된 경우 에이전트는 이 기간을 기반으로 허용된 Enterprise Manager 에 대한 연결을 계속해서 주기적으로 시도합니다.
- 속성 구성이 설정되지 않은 경우(주석으로 처리된 경우) 에이전트는 CA APM 에이전트 버전을 기반으로 다음과 같이 동작합니다.
 - **9.1 이전 에이전트에 해당:** Enterprise Manager 에서 연결이 끊어지고 계속해서 다시 연결을 시도합니다.
 - **9.1 에이전트에 해당:** "Allowed Enterprise Manager"(허용된 Enterprise Manager) 목록에서 허용된 마지막 Enterprise Manager 에 수동적으로 연결됩니다. 에이전트는 Enterprise Manager 로 메트릭 데이터를 전송하지 않습니다. 에이전트는 Enterprise Manager 구성 정보가 에이전트를 허용된 상태로 변경할 때까지 기다리므로 유휴 상태입니다.

에이전트 - Enterprise Manager 네트워크 토폴로지 구성 프로세스

에이전트 - Enterprise Manager 네트워크 토폴로지를 구성하려면 다음과 같은 상위 수준 단계가 필요합니다.

1. [에이전트 - Enterprise Manager 또는 수집기 토폴로지를 계획합니다](#) (페이지 136).
2. 사용 중인 배포에 해당하는 경우 introscope.enterprisemanager.properties 파일을 구성합니다.
 - a. (선택 사항) [loadbalancing.xml 에 있는 정규식과 일치하지 않는 에이전트의 MOM 또는 특정 Enterprise Manager 에 대한 연결이 허용되거나 허용되지 않는지 여부를 구성합니다](#) (페이지 138).
introscope.apm.agentcontrol.agent.allowed 속성을 설정합니다.
 - b. (선택 사항) [에이전트가 Enterprise Manager 에 대한 다시 연결을 시도하는 기간을 임의로 추출해서 구성합니다](#) (페이지 139).
introscope.apm.agentcontrol.agent.reconnect.wait 속성을 설정합니다.

- c. (선택 사항) [Enterprise Manager](#) 에 수동적으로 연결하여 데이터를 전송하지 않을 수 있는 9.1 에이전트 수를 구성합니다 (페이지 140).

`introscope.enterprisemanager.agent.disallowed.connection.limit` 를 설정합니다.

- 3. 사용 중인 배포에 해당하는 경우 `IntroscopeAgent.profile` 파일을 구성합니다.

- (선택 사항) [Enterprise Manager](#) 에서 연결이 끊긴 에이전트가 계속해서 허용된 [Enterprise Manager](#) 에 대한 다시 연결을 시도하는지 여부를 구성합니다 (페이지 141).

`introscope.agent.enterprisemanager.failbackRetryIntervalInSeconds` 속성을 설정합니다.

- 4. [loadbalancing.xml](#) 을 구성합니다 (페이지 143).

- a. (선택 사항) 에이전트가 항상 특정 [Enterprise Manager](#) 에 연결하도록 `latch` 속성을 구성합니다.
- b. (선택 사항) 특정 [Enterprise Manager](#) 에 대한 에이전트 연결을 허용하거나 허용하지 않도록 `include` 및 `exclude` 요소를 구성합니다.
- c. `loadbalancing.xml` 을 저장합니다.

새 값은 약 60 초마다 한 번씩 발생하는 핫 배포 중에 [Enterprise Manager](#) 가 속성 파일을 검사할 때 적용됩니다. MOM 은 다음 부하 분산 간격에 도달할 때 업데이트된 `loadbalancing.xml` 을 클러스터의 수집기에 전송합니다.

- 5. 시스템 모니터링을 수행하고 필요한 경우 다시 구성합니다.
 - a. 필요에 따라 속성을 다시 구성합니다.
 - b. `loadbalancing.xml` 을 업데이트합니다.

에이전트 - Enterprise Manager 네트워크 토폴로지 계획

에이전트 연결 할당을 구성하기 전에 에이전트 - Enterprise Manager 또는 수집기 토폴로지를 계획하십시오. 이러한 할당에서는 특정 개별 수집기 또는 수집기 그룹에 대한 연결이 허용되거나 허용되지 않는 에이전트를 구성합니다.

비즈니스 관례에 따라 필요한 경우 에이전트를 하위 클러스터로 설정하십시오. 에이전트를 특정 수집기 집합에 할당한 다음, MOM 이 해당 수집기 집합의 부하만 분산하도록 `loadbalancing.xml` 을 구성할 수 있습니다. 예를 들어 특정 비즈니스 단위의 응용 프로그램을 모니터링하는 에이전트가 수집기 10 개로 구성된 클러스터의 수집기 3 개에 연결하도록 구성할 수 있습니다.

계획하는 동안 다음 질문에 답하십시오.

- 에이전트 클래스 또는 그룹이나 특정 에이전트가 클러스터나 특정 수집기에서 허용되거나 허용되지 않습니까?
- 특별히 오버로드되지 않도록 보호해야 하는 수집기가 있습니까?
예를 들어 잘못 구성된 에이전트에서 직접 연결되지 않도록 일부 수집기를 보호해야 합니까? 모든 에이전트의 에이전트 프로필이 동일한 경우 모든 에이전트가 연결을 시도하면 단일 IP 주소가 초과될 수 있습니다. 수집기에 너무 많은 수의 에이전트가 연결되면 해당 수집기의 작동이 중단될 수 있습니다.

다음 단계를 따르십시오.

1. 각 에이전트 그룹 또는 클래스에 대해 다음 수집기 집합을 결정합니다.
 - a. 액세스를 허용할 수집기 집합
 - b. 액세스를 허용하지 않을 수집기 집합
2. `loadbalancing.xml` 에 지정된 사항과 일치하지 않는 에이전트의 기본 연결 동작을 결정합니다.

특정 Enterprise Manager 에서 `loadbalancing.xml` 에 지정된 사항과 일치하지 않는 에이전트를 모두 허용하거나 허용하지 않으시겠습니까?

3. 에이전트의 부하가 분산됩니까? 부하가 분산되는 경우 이동 대상으로 삼을 수집기 모두에서 에이전트가 허용됩니까?

MOM 에 대한 부하 분산 옵션을 제한하므로 에이전트 연결 제한 사항의 효과를 주의 깊게 고려합니다. 부하가 적은 수집기에 대한 에이전트 연결이 허용되지 않으면 부하 분산을 수행하는 MOM 이 오버로드된 수집기에서 에이전트를 제거할 수 없습니다. 이 경우 MOM 은 오버로드된 수집기에서 부하가 적은 수집기로 다른 에이전트의 부하를 분산해야 합니다.

4. Enterprise Manager 에서 연결이 끊긴 에이전트가 수행할 동작을 결정합니다.

에이전트가 계속해서 허용된 Enterprise Manager 에 대한 다시 연결을 시도하도록 하시겠습니까?

또는 에이전트의 CA APM 버전을 기반으로

- **9.1 이전 에이전트에 해당:** Enterprise Manager 와의 연결을 끊고 계속해서 다시 연결을 시도하는 편이 더 좋습니까?
- **9.1 에이전트에 해당:** "Allowed Enterprise Manager"(허용된 Enterprise Manager) 목록에서 허용된 최종 Enterprise Manager 에 수동적으로 연결된 상태로 유지하는 편이 더 좋습니까?

수동적으로 연결된 에이전트에는 다음과 같은 특성이 있습니다.

- 메트릭 데이터를 Enterprise Manager 에 전송하지 않습니다.
- 사용 가능해진 다른 Enterprise Manager 에 대한 다시 연결을 시도하지 않습니다.

5. CA APM 환경에서 다음 CA APM 구성 요소에 대한 에이전트 연결이 허용됩니까?

- 클러스터
- 수집기 및 독립 실행형 Enterprise Manager
- 클러스터, 수집기 및 독립 실행형 Enterprise Manager 의 조합

loadbalancing.xml 규칙이 없을 때 새 에이전트 연결 허용 여부 구성

에이전트가 loadbalancing.xml 에 지정된 정규식과 일치하지 않을 때 새 에이전트 연결을 모두 허용할지 또는 허용하지 않을지 여부를 결정하십시오. 다음 구성 요소에 대해 이러한 결정을 내리십시오.

- MOM
- 각 수집기
- 독립 실행형 Enterprise Manager

성능을 측정하기 위해 `introscope.apm.agentcontrol.agent.allowed` 속성을 설정할 수 있습니다.

참고: MOM 속성 값이 항상 수집기 값을 재정의합니다. 수집기 값은 MOM 이 수집기에 연결할 때까지 사용되지 않습니다. 이때 MOM 속성 값이 전송되어 수집기에서 사용됩니다.

이 속성 설정과 `loadbalancing.xml` 에 있는 구성을 사용하여 사용자 환경의 에이전트 - Enterprise Manager 연결을 세부 조정할 수도 있습니다.

다음 단계를 따르십시오.

1. `<EM_Home>\config` 디렉터리로 이동하고 `IntroscopeEnterpriseManager.properties` 파일을 엽니다.
2. `introscope.apm.agentcontrol.agent.allowed=true` 를 설정합니다.
3. `IntroscopeEnterpriseManager.properties` 파일을 저장합니다.
설정은 약 60 초마다 한 번씩 발생하는 핫 배포 중에 Enterprise Manager 가 속성 파일을 검사할 때 적용됩니다.

에이전트 다시 연결 대기 시간 구성

[연결이 끊긴 에이전트](#) (페이지 133)가 독립 실행형 Enterprise Manager 나 수집기에 대한 다시 연결을 시도할 때까지 대기해야 하는 시간(초)을 변경할 수 있습니다. 변경된 대기 기간은 CA APM 에서 여러 에이전트가 동시에 Enterprise Manager 에 대한 다시 연결을 시도할 때 발생하는 성능 문제를 방지하는 데 도움이 됩니다.

`introscope.apm.agentcontrol.agent.reconnect.wait` 속성을 구성하여 대기 시간을 변경합니다.

다음 단계를 따르십시오.

1. `<EM_Home>\config` 디렉터리로 이동하고 `IntroscopeEnterpriseManager.properties` 파일을 엽니다.
2. `introscope.apm.agentcontrol.agent.reconnect.wait` 속성을 설정합니다.
3. `IntroscopeEnterpriseManager.properties` 파일을 저장합니다.

설정은 약 60 초마다 한 번씩 발생하는 핫 배포 중에 Enterprise Manager 가속성 파일을 검사할 때 적용됩니다.

Enterprise Manager 에서 연결이 끊긴 경우 에이전트는 Enterprise Manager 에서 생성된 다시 연결 시간을 기반으로 다시 연결을 시도합니다. 연결 시간은 기본값과 임의로 추출된 추가 양수 또는 음수 값을 기반으로 합니다.

허용되지 않는 에이전트 연결 클램프 제한 구성

9.1 에이전트에 해당: 허용되지 않는 것으로 구성되었지만 독립 실행형 Enterprise Manager 나 수집기에 수동적으로 연결할 수 있는 9.1 에이전트 수를 제한할 수 있습니다. 수동적으로 연결된 에이전트에는 다음과 같은 특성이 있습니다.

- 메트릭 데이터를 Enterprise Manager 에 전송하지 않습니다.
- 사용 가능해진 다른 Enterprise Manager 에 대한 다시 연결을 시도하지 않습니다.

이 클램프 제한을 설정하면 Enterprise Manager 에 대한 연결 수가 제한되기 때문에 성능을 측정할 수 있습니다. 연결마다 일부 리소스가 필요하므로 연결 수가 지나치게 많을 경우 Enterprise Manager 성능이 저하될 수 있습니다.

다음 단계를 따르십시오.

1. <EM_Home>\config 디렉터리로 이동하고 IntroscopeEnterpriseManager.properties 파일을 엽니다.
2. introscope.enterprisemanager.agent.disallowed.connection.limit 속성을 설정합니다.
3. IntroscopeEnterpriseManager.properties 파일을 저장합니다.

설정은 약 60 초마다 한 번씩 발생하는 핫 배포 중에 Enterprise Manager 가속성 파일을 검사할 때 적용됩니다.

클램프에 도달한 경우 허용되지 않는 것으로 구성된 에이전트가 Enterprise Manager 에 대한 연결을 시도하면 Enterprise Manager 가 다음 동작을 수행합니다.

- 이벤트를 로깅합니다.
- 새 연결을 거부합니다.

계속해서 허용된 Enterprise Manager 에 다시 연결하도록 에이전트 구성

모든 Enterprise Manager 에서 연결이 거부된 에이전트가 "Allowed Enterprise Manager"(허용된 Enterprise Manager) 목록에 있는 항목을 돌아가면서 계속해서 다시 연결을 시도하는지 여부를 구성할 수 있습니다. 다음은 허용된 Enterprise Manager 입니다.

- 에이전트 프로파일 introscope.agent.enterprisemanager.connectionorder 속성 값에 구성된 Enterprise Manager
- loadbalancing.xml 구성을 기반으로 하는 허용되는 모든 Enterprise Manager

Enterprise Manager 에 연결할 수 없는 경우 거부된 에이전트는 다음과 같은 방법으로 연결을 처리합니다.

- "Allowed Enterprise Manager"(허용된 Enterprise Manager) 목록에서 허용된 다음 Enterprise Manager 에 대한 연결을 시도합니다.
- 허용되지 않는 것으로 구성된 Enterprise Manager 에는 연결하지 않습니다.

계속해서 연결을 시도하도록 거부된 에이전트를 구성하는 경우 다음과 같은 특성이 있습니다.

- 다음 CA Introscope 구성 요소에 대한 에이전트 연결이 허용된 환경에 유용합니다.
 - 클러스터
 - 수집기 및 독립 실행형 Enterprise Manager
 - 클러스터, 수집기 및 독립 실행형 Enterprise Manager 의 조합
- 연결이 끊긴 에이전트가 다음 상황에서 허용된 Enterprise Manager 에 대한 연결을 계속 시도하도록 강제합니다.
 - Enterprise Manager 를 연결에 사용할 수 있을 때까지
 - Enterprise Manager 가 다른 클러스터에 있는 경우도 마찬가지로

그렇지 않으면 에이전트는 다음과 같은 방법으로 연결을 처리합니다.

- Enterprise Manager 에 수동적으로 연결하고 메트릭 데이터를 전송하지 않습니다.
- 사용할 수 없는 상태에서 사용할 수 있는 상태가 된 Enterprise Manager 를 포함하여 허용된 Enterprise Manager 에 대한 연결을 시도하지 않습니다.

다음 단계를 따르십시오.

1. IntroscopeAgent.profile 파일을 엽니다.
2. introscope.agent.enterprisemanager.failbackRetryIntervallInSeconds 속성을 설정합니다.
3. IntroscopeEnterpriseManager.properties 파일을 저장합니다.
4. 관리되는 응용 프로그램을 다시 시작합니다.

다음 이벤트가 발생하는 경우

- Enterprise Manager 에 대한 에이전트 연결이 거부되는 경우
- Enterprise Manager 가 다운되는 경우

그러면 에이전트는 즉시 "Allowed Enterprise Manager"(허용된 Enterprise Manager) 목록에서 허용된 다음 Enterprise Manager 에 대한 연결을 시도합니다.

허용된 Enterprise Manager 에 연결할 수 없는 경우 에이전트는 다음 동작을 수행합니다.

- introscope.agent.enterprisemanager.failbackRetryIntervallInSeconds 속성에 설정된 기간 동안 대기합니다.
- "Allowed Enterprise Manager"(허용된 Enterprise Manager) 목록에서 허용된 첫 번째 Enterprise Manager 부터 시작해서 허용된 Enterprise Manager 에 대한 연결을 다시 시도합니다.

이 주기는 에이전트가 능동적으로 데이터를 전송할 수 있는 Enterprise Manager 에 연결할 때까지 반복됩니다.

Enterprise Manager 별로 허용되거나 허용되지 않는 에이전트에 대한 loadbalancing.xml 구성

특정 Enterprise Manager 에서 에이전트 연결을 허용하거나 허용하지 않으려면 MOM 이나 독립 실행형 Enterprise Manager 에서 [loadbalancing.xml 을 구성](#) (페이지 117)하십시오.

MOM 이 10 분마다 loadbalancing.xml 에 있는 에이전트 연결 정보를 수집기에 전송하면 수집기가 허용된 Enterprise Manager 정보를 에이전트에 전송합니다. MOM 은 최신 loadbalancing.xml 과일을 기반으로 특정 Enterprise Manager 에서 에이전트 연결을 허용하거나 허용하지 않습니다.

MOM 을 통해 부하를 분산하기를 원하지 않는 에이전트가 있는 경우에도 loadbalancing.xml 을 구성할 수 있습니다. 이 예제에서는 MOM 이 Collector1-ip 라는 수집기에서 다른 수집기로 EPMagent 라는 에이전트의 부하를 분산하지 않습니다.

```
<agent-Collector name="EPMagent connects to only Collector1-ip">
<agent-specifier>.*\|.*\|EPMagent</agent-specifier>
  <include>
    <Collector host="Collector1-ip" port="6001"/>
  </include>
</agent-Collector>
```

에이전트 - Enterprise Manager 네트워크 토폴로지 문제 해결

Enterprise Manager 가 거부된 에이전트를 처리하는 방법

MOM 에서 10 분마다 클러스터의 모든 수집기로 loadbalancing.xml 을 전송합니다. loadbalancing.xml 과 introscope.apm.agentcontrol.agent.allowed 속성은 Enterprise Manager 에 대한 연결이 허용되거나 허용되지 않는 에이전트를 지정합니다. Enterprise Manager 는 허용 및 허용하지 않음 구성을 기반으로 에이전트 연결 요청을 수락하거나 거부할 수 있습니다.

다음은 Enterprise Manager 가 에이전트 연결을 거부할 때 발생하는 결과입니다.

9.1 이전 에이전트에 해당

에이전트가 연결되면 Enterprise Manager 가 9.1 이전의 에이전트 연결을 끊습니다. 에이전트가 해당 "Allowed Enterprise Manager"(허용된 Enterprise Manager) 목록을 사용하여 다른 허용된 사용 가능한 Enterprise Manager 에 대한 연결을 시도합니다. 모든 Enterprise Manager 에 대하여 에이전트 연결이 거부되면 에이전트가 계속해서 다음과 같은 Enterprise Manager 에 연결을 시도합니다.

- 사용 가능한 마지막 Enterprise Manager
- 에이전트에 대한 연결이 허용된 마지막 Enterprise Manager

9.1 에이전트에 해당

Enterprise Manager 가 9.1 에이전트의 연결을 끊으면 에이전트가 다른 허용된 사용 가능한 Enterprise Manager 에 대한 연결을 시도합니다. 모든 Enterprise Manager 에 대하여 에이전트 연결이 거부되면 에이전트가 마지막으로 연결되었던 Enterprise Manager 에 연결합니다. 에이전트가 Enterprise Manager 에 연결된 상태로 유지되지만 데이터를 전송하지는 않습니다.

수집기가 `introscope.apm.agentcontrol.agent.allowed` 속성을 사용하는 경우

MOM 이 수집기에 연결되는 경우 MOM 은 수집기에 `introscope.apm.agentcontrol.agent.allowed` 속성과 `loadbalancing.xml` 을 제공합니다. MOM 이 다운되면 수집기가 MOM 에서 제공한 다음 정보를 사용하여 허용하거나 허용하지 않을 에이전트 연결을 알게 됩니다.

- `IntroscopeEnterpriseManager.properties` 파일의 현재 `introscope.apm.agentcontrol.agent.allowed` 속성 설정
- `loadbalancing.xml`

MOM 이 수집기에 연결된 적이 없으면 MOM 이 수집기에 `introscope.apm.agentcontrol.agent.allowed` 속성과 `loadbalancing.xml` 파일을 전송한 적이 없습니다. 따라서 수집기가 자신의 `introscope.apm.agentcontrol.agent.allowed` 속성을 사용하여 특정한 에이전트 연결을 허용할지 또는 허용하지 않을지 결정합니다.

에이전트가 loadbalancing.xml 의 허용됨 또는 허용되지 않음 정규식과 일치하지 않는 경우

IntroscopeEnterpriseManager.properties 파일의 introscope.apm.agentcontrol.agent.allowed 속성 값에 따라 loadbalancing.xml 의 정규식과 일치하지 않는 에이전트가 수집기에 연결할 수 있는지 여부가 결정됩니다.

속성 값이 true 인 경우 loadbalancing.xml 의 정규식과 일치하지 않는 에이전트가 수집기에 연결할 수 있습니다.

속성 값이 false 인 경우에는 loadbalancing.xml 의 정규식과 일치하지 않는 에이전트가 수집기에 연결할 수 없습니다.

에이전트에 할당된 모든 수집기가 사용 불가능하고 다른 수집기는 사용 가능한 경우

9.1 이전의 에이전트

수집기가 에이전트의 연결을 끊은 다음 에이전트가 MOM 에 대한 연결을 시도합니다. 에이전트 연결이 허용된 사용 가능한 수집기가 없으면 MOM 이 모든 에이전트 연결 시도를 거부합니다. 에이전트는 에이전트에 허용된 수집기를 사용할 수 있을 때까지 계속해서 MOM 에 대한 연결을 시도합니다. 수집기가 사용할 수 있게 되면 MOM 이 에이전트를 허용된 수집기로 리디렉션합니다.

9.1 에이전트

수집기가 에이전트의 연결을 끊은 다음 에이전트가 MOM 에 연결되지만 데이터를 전송하지는 않습니다. 수집기가 사용할 수 있게 되면 MOM 이 에이전트를 허용된 수집기로 리디렉션합니다.

수집기가 허용되지 않는 에이전트를 직접 연결을 사용하여 처리하는 방법

MOM 은 주기적으로 `loadbalancing.xml` 을 클러스터의 모든 수집기로 전송합니다. 각 수집기는 `loadbalancing.xml` 파일을 통해 해당 수집기에 대한 연결이 허용된 에이전트를 알게 됩니다. 다음 동작이 발생하면

- `loadbalancing.xml` 파일이 업데이트되어 에이전트가 특정 수집기에서 허용되지 않습니다.
- 에이전트가 이 수집기에 대한 연결을 시도합니다.

다음과 같은 결과가 발생합니다.

9.1 이전의 에이전트

수집기가 에이전트 연결을 거부하고 에이전트는 계속해서 연결을 시도합니다.

9.1 에이전트

수집기가 에이전트에 최신 "Allowed Enterprise Manager"(허용된 Enterprise Manager) 목록을 제공합니다. 에이전트가 허용되지 않음 구성 설정을 기반으로 수집기에서 허용되지 않습니다. MOM 을 사용할 수 있는 경우 MOM 이 에이전트를 사용 가능한 허용된 수집기로 리디렉션합니다. MOM 을 사용할 수 없는 경우에는 에이전트가 "Allowed Enterprise Manager"(허용된 Enterprise Manager) 목록을 사용하여 허용된 사용 가능한 수집기에 차례대로 연결을 시도합니다.

introscope.apm.agentcontrol.agent.allowed 속성이 없을 때의 기본 에이전트 연결 값

introscope.apm.agentcontrol.agent.allowed 속성의 기본값은 *allowed* 입니다.

사용 가능한 MOM 이 없을 때 CA Introscope 에서 에이전트 연결 대상을 결정하는 방법

에이전트가 연결을 시도하는 수집기에 따라 연결이 허용될지 아니면 거부될지가 결정됩니다. 수집기는 `loadbalancing.xml` 파일에 있는 현재 허용됨 및 허용되지 않음 구성을 기반으로 결정합니다.

제 9 장: 명령줄 Workstation 사용

이 장에서는 Enterprise Manager 의 명령줄 인터페이스인 Introscope CLW(명령줄 Workstation)에 대해 설명합니다.

이 섹션은 다음 항목을 포함하고 있습니다.

[CLW\(명령줄 Workstation\) 정보](#) (페이지 147)

[CLW 실행](#) (페이지 148)

[CLW 명령 참조](#) (페이지 151)

[샘플 스크립트](#) (페이지 201)

CLW(명령줄 Workstation) 정보

Introscope CLW(명령줄 Workstation)를 사용하여 Introscope Workstation 기능 중 일부를 실행할 수 있습니다.

CLW 는 Introscope 운영 작업을 자동화하거나 예약할 때 유용합니다. 예를 들어 Workstation 인터페이스 대신 CLW 를 사용하여 보다 빠르게 여러 관리 모듈에서 여러 경고가 사용되지 않도록 설정하는 등의 반복 작업을 수행할 수 있습니다. 마찬가지로 CLW 는 자동으로 수행하거나 주기적으로 수행해야 하는 작업을 예약하는 경우에도 유용합니다.

CLW 명령으로 수행할 수 있는 작업은 다음과 같습니다.

- **관리 모듈과 요소 관리** - 관리 모듈과 요소를 나열, 복사, 이름 바꾸기 및 삭제하고 활성 상태인지 확인하며 현재 상태를 변경할 수 있습니다.

CLW 의 복사 및 이름 바꾸기 명령을 사용하여 기존 관리 모듈과 요소를 기반으로 관리 모듈과 요소를 만들 수는 있지만 CLW 를 사용하여 관리 모듈과 요소를 처음부터 새로 만들거나 세부 정보를 변경할 수는 없습니다.

- **에이전트 제어** - 에이전트 보고를 원격으로 시작, 중지 및 다시 시작하고 구성 파일을 원격 에이전트에 복사할 수 있습니다.

- **트랜잭션 추적 세션 시작** - 경고 조건의 결과로 트랜잭션 추적 세션을 자동으로 시작하는 스크립트를 작성할 수 있습니다.
- **Enterprise Manager 종료** - Enterprise Manager 를 예약 방식으로 종료하는 스크립트를 작성할 수 있습니다. 예를 들어 Workstation 사용이 곤란할 수 있는 경우 업무 외 시간 동안 Enterprise Manager 를 중지해야 할 수 있습니다.
- **CLW 가 종료되는 경우** - 오류가 발생하지 않으면 CLW 가 0 값으로 종료됩니다. 다음 중 하나가 발생하면 음수 상태 코드로 종료됩니다.
 - Enterprise Manager 인증 실패
 - 드롭된 네트워크 연결이나 잘못된 호스트 이름과 같은 Enterprise Manager 와의 연결 문제
 - 잘못된 WS 와 Enterprise Manager 가 있는 경우

CLW 실행

이 단원에서는 CLW 실행 방법에 대한 개요를 제공합니다. 특정 명령에 대한 자세한 내용은 [CLW 명령 참조](#) (페이지 151)를 참고하십시오.

JVM 요구 사항

CLW 를 사용하려면 JVM 1.6 이상이 필요합니다.

CLW 명령을 실행할 위치

CLW 명령을 스크립트 또는 배치 파일에 포함하거나 명령줄에서 입력할 수 있습니다. CLW .jar 파일은 <EM_Home>/lib 디렉터리에 설치됩니다. 해당 디렉터리에서 CLW 명령을 실행하거나 디렉터리의 경로를 명령에 포함하십시오.

CLW 대화식 모드 사용

다음 예와 같이 *-i* 플래그를 사용하여 기본 모드에서 대화식 모드로 변경할 수 있습니다. CLW 용 스크립트를 작성할 계획이면 문제가 발생하므로 이 모드를 사용할 수 없습니다.

```
java -Xmx128M <EM_logon> <TT_properties> -jar CLWorkstation.jar > usage | -i
| <command>
```

대화식 모드는 명령줄 인수를 읽고 명령을 실행한 다음 종료합니다. 그러나 `-DHost=`처럼 JVM 옵션 이외에 전달된 명령줄 인수가 없는 경우 하나의 표준 입력 줄을 읽고 실행한 다음 파일 끝에 도달하거나 사용자가 시스템을 종료할 때까지 계속해서 동일한 동작을 수행합니다. 전달된 인수도 없고 제공된 입력도 없는 경우에는 오류가 출력되면서 시스템이 종료됩니다. # 기호로 시작하는 줄은 모두 무시됩니다.

CLW 호출

CLW 명령 구문은 다음과 같습니다.

```
java -Xmx128M <EM_logon> -jar CLWorkstation.jar <command>
```

다음은 각 요소에 대한 설명입니다.

- `-Xmx128M` 은 설정하지 않은 경우에 발생할 수 있는 `java.lang.OutOfMemoryError` 오류를 방지하는 Java 힙 크기를 설정합니다.
- `<EM_logon>`은 Enterprise Manager 로그온 정보입니다.
 - Duser=<user name>
 - Dpassword=<password>
 - Dhost=<Enterprise Manager host / ip address>
 - Dport=<Enterprise Manager port number>
- `<command>`는 [CLW 명령 참조 \(페이지 151\)](#)에 설명된 명령 중 하나입니다.

예:

```
java -Xmx128M -Duser=jdoe -Dpassword=myspassword -Dhost=jdoeDT
-Dport=5001 -jar CLWorkstation.jar <command>
```

Enterprise Manager 에 액세스하기 위한 기본 로그온 값은 다음과 같이 로그온 정보를 제공하지 않고 CLW 를 호출하는 경우에 사용됩니다.

```
java -Xmx128M -jar CLWorkstation.jar <command>
```

명령줄에 입력하거나 스크립트에 포함하는 모든 CLW 명령은 다음과 같이 CLW 호출로 시작해야 합니다.

```
java -Xmx128M -jar CLWorkstation.jar
```

참고: `java.lang.OutOfMemoryError` 를 방지하려면 Java 힙 크기를 설정하십시오.

CLW 는 대/소문자를 구분함

CLW 명령은 Introscope 배포에 있는 에이전트, 관리 모듈 및 기타 이름 지정된 항목을 지정하는 인수를 받아들입니다. CLW 는 대/소문자를 구분하므로 Introscope 개체의 이름을 지정된 대로 정확히 입력해야 합니다. 예를 들어 에이전트에 *WebLogic1* 이라는 이름이 지정된 경우 *weblogic1* 을 참조하는 CLW 명령은 해당 에이전트에 대해 실행되지 않습니다.

CLW 명령 출력

CLW 명령 출력은 명령 창에 반환됩니다. 필요한 경우 파일을 명령 출력 대상으로 지정할 수 있습니다.

CLW 및 정규식

CLW 명령을 사용하여 에이전트, 관리 모듈, 대시보드, 작업, 경고 등의 Introscope 환경 요소를 조작할 수 있습니다. 대상 유형에 따라 복사, 나열, 이름 바꾸기, 활성화, 비활성화 등의 작업을 수행할 수 있습니다.

정확한 텍스트 문자열이나 Perl 정규식을 사용하여 CLW 명령의 대상을 지정합니다. 예를 들어 이 CLW 명령은 Enterprise Manager 에 연결된 에이전트를 모두 나열합니다.

```
list agents matching (.*)
```

이 명령은 이름에 *weblogic* 문자열이 포함된 에이전트만 나열합니다.

```
list agents matching .*weblogic.*
```

CLW 명령 내의 백슬래시 및 따옴표

공백을 포함하는 CLW 명령 인수를 제공하는 경우에는 인수를 따옴표(")로 묶고 백슬래시를 각 따옴표 앞에 넣어서 셸이 따옴표를 해석하지 않도록 하십시오. 예:

```
\ "2005/01/01 12:20:37\"
```

다양한 환경에서 CLW 사용

정규식 구문은 사용 중인 운영 체제와 명령 셸에 따라 다르게 표현식을 명령줄에서 입력하는지 아니면 스크립트에 포함하는지 여부에 따라 서로 다른 경우가 있습니다. 이 장의 샘플 명령은 Windows 환경용으로 작성되었고 배치 파일에서 정규식을 사용하는 데 필요한 구문을 반영합니다.

명령줄 Workstation 로그 구성

CLW(명령줄 Workstation) 명령을 Enterprise Manager 콘솔과 `<EM_Home>/logs` 디렉터리에 있는 `IntroscopeEnterpriseManager.log` 파일에 기록하도록 CA APM 을 구성할 수 있습니다.

명령줄 Workstation 로그를 구성하려면

1. `<EM_Home>\config` 디렉터리에 있는 `IntroscopeEnterpriseManager.properties` 파일을 엽니다.
2. `IntroscopeEnterpriseManager.properties` 파일에 다음 속성을 구성하여 로그 파일 및 Enterprise Manager 콘솔에 CLW 명령 로깅을 사용하도록 설정합니다.
 - a. `log4j.additivity.Manager.CLW` 를 `true` 로 설정합니다.
참고: 이 속성의 기본값은 `false` 입니다.
 - b. `log4j.logger.Manager.CLW` 를 `DEBUG` 로 설정합니다.
이 속성의 기본값은 `INFO` 입니다.

CLW 명령 참조

이 단원에는 CLW 명령에 대한 세부 정보가 포함되어 있습니다.

참고: 각 명령에 대해 표시된 구문은 명령의 호출 부분을 포함하지 않습니다. [CLW 호출](#) (페이지 149)에 설명된 대로 각 CLW 명령은 `java -jar CLWorkstation.jar` 로 시작해야 합니다.

Enterprise Manager 명령

Enterprise Manager 는 에이전트에서 응용 프로그램 성능 데이터를 집계하고 요청된 계산을 실행하며 성능 데이터를 권한 있는 클라이언트에게 제공하고 성능 데이터를 저장합니다.

Enterprise Manager 종료

이 명령은 Enterprise Manager 를 종료합니다. 이 명령을 실행하려면 종료 권한이나 모든 권한이 있어야 합니다. Enterprise Manager 를 종료하면 Enterprise Manager 에 연결된 Workstation 사용자가 모두 로그오프됩니다.

구문

종료

예

종료

출력

없음

SmartStor 에서 지속 데이터 추출(시간 범위 내)

이 명령은 SmartStor 에서 지정된 기간 동안의 기록 데이터를 추출합니다. 에이전트를 지정하는 정규식, 메트릭 그룹을 지정하는 정규식 및 기간의 시작과 끝을 지정하십시오. 날짜-시간 문자열의 *hh:mm:ss* 부분은 선택적입니다. 지정하지 않을 경우 기본값은 00:00:00(자정)입니다.

구문

```
get historical data from agents matching [REGULAR EXPRESSION] and metrics matching [REGULAR EXPRESSION] between [EXACT MATCH] and [EXACT MATCH] with frequency of [EXACT MATCH] (second|seconds|sec|secs|s)
```


예

```
get historical data from agents matching (*.weblogic.*) and metrics matching
(Servlets:Responses Per Interval) between \"2011-10-12 00:00:00\" and
\"2011-10-12 00:10:00\" with frequency of 60 seconds
```

이 명령은 이름에 `weblogic` 이라는 문자열이 포함된 모든 에이전트에 대해 "서블릿:간격당 응답 수" 메트릭 그룹화의 지속 데이터를 추출합니다. 이 데이터는 2011 년 10 월 12 일 자정부터 2011 년 10 월 12 일 자정 10 분 후까지의 기간 동안 60 초 빈도로 추출됩니다.

출력

SmartStor 데이터는 CSV(쉼표로 구분된 값) 형식으로 반환됩니다.

SmartStor 에서 지속 데이터 추출(N 초 빈도의 이전 N 분)

이 명령은 명령을 실행하기 전 지정된 시간(분) 동안의 기록 데이터를 추출합니다. 추출된 데이터는 특정 빈도의 초 단위로 표시됩니다. 에이전트를 지정하는 정규식, 메트릭 그룹을 지정하는 정규식, 추출할 기록의 분 수 및 데이터를 추출할 빈도를 지정하십시오.

구문

```
get historical data from agents matching [REGULAR EXPRESSION] and metrics
matching [REGULAR EXPRESSION] for past [EXACT MATCH] (minute|minutes)
with frequency of [EXACT MATCH] (second|seconds|sec|secs|s)
```

예

```
get historical data from agents matching (*.weblogic.*) and metrics matching
(Servlets:Responses Per Interval) for past 1 minute with frequency of 60 seconds
```

이 명령은 이름에 `weblogic` 이라는 문자열이 포함된 모든 에이전트에 대해 "서블릿:간격당 응답 수" 메트릭 그룹화의 지속 데이터를 추출합니다. 이 데이터는 지난 1 분의 기간 동안 60 초 빈도로 추출됩니다.

출력

SmartStor 데이터는 CSV(쉼표로 구분된 값) 형식으로 반환됩니다.

인증을 위한 경로 이름 지정

Enterprise Manager 에 연결할 때 사용자 이름/암호 인증 대신에 사용할 공개 키 파일의 전체 경로 이름을 지정합니다. 사용되는 공개 키는 MOM(Manager of Managers)/수집기 인증에 사용되는 것과 동일합니다.

공개 키 구성에 대한 자세한 내용은 *CA APM 보안 안내서*를 참조하십시오.

Introscope Agent 명령

에이전트는 Java 응용 프로그램 컴퓨터에서 관리되는 응용 프로그램의 일부로 실행되며 프로브가 보고한 데이터를 수집 및 요약하여 Enterprise Manager 에 보냅니다.

에이전트 나열

"에이전트 나열" 명령은 Enterprise Manager 에 연결된 에이전트를 하나 이상 나열합니다. 나열되는 에이전트를 결정하는 정규식을 제공해야 합니다.

구문

```
list agents matching <REGULAR EXPRESSION>
```

예

```
list agents matching (.*)
```

이 명령은 Enterprise Manager 에 연결된 에이전트를 모두 나열합니다.

출력

해당 호스트와 프로세스가 앞에 붙어 있는 상태로 각 에이전트가 나열됩니다. 가상 에이전트가 목록에 포함됩니다. 예:

```
jdoe-dt|Weblogic|WebLogicAgent
```

```
Custom Metric Host (Virtual)(사용자 지정 메트릭 호스트(가상))|Custom  
Metric Process (Virtual)(사용자 지정 메트릭 프로세스(가상))|Custom Metric  
Agent (Virtual)(사용자 지정 메트릭 에이전트(가상))
```

List Historical Agents(기록 에이전트 나열)

"List Historical Agents"(기록 에이전트 나열) 명령은 SmartStor 에 데이터가 있지만 마운트 해제되어 Enterprise Manager 에 데이터를 보내고 있지 않은 에이전트를 모두 나열합니다.

구문

```
list historical agents
```

예

```
list historical agents
```

출력

마운트 해제된 기록 에이전트가 각각 별도의 행에 나열되고 해당 호스트 이름과 프로세스가 그 앞에 표시됩니다. 예:

```
jdoe-dt|Weblogic|WebLogicAgent
```

List Historical Agents (Within a Time Range)(기록 에이전트 나열(시간 범위 내))

이 명령은 지정된 시간 범위 내에서 SmartStor 에 기록 데이터가 있는 마운트 해제된 에이전트를 모두 나열합니다. 데이터를 보내는 에이전트는 자동으로 마운트되므로 나열되지 않습니다.

기간의 시작과 끝을 제공해야 합니다. 날짜-시간 문자열의 hh:mm:ss 부분은 선택적입니다. 지정하지 않을 경우 기본값은 00:00:00(자정)입니다.

구문

```
list historical agents between [TIME] and [TIME]
```

예

```
list historical agents between \"2013-04-22 00:00:00\" and \"2013-04-23 00:10:00\"
```

이 명령은 2013 년 3 월 22 일 자정부터 2013 년 3 월 23 일 자정까지 10 분 간격으로 데이터를 보낸 마운트 해제된 에이전트를 모두 나열합니다.

출력

지정된 기간 동안 데이터를 보낸 마운트 해제된 기록 에이전트가 각각 별도의 행에 나열되고 해당 호스트 이름과 프로세스가 에이전트 이름 앞에 표시됩니다. 예:

```
jdoe-dt/Weblogic/WebLogicAgent
```

에이전트 켜기

이 명령은 하나 이상의 에이전트에서 메트릭 보고를 시작하거나 다시 시작합니다. 대상 에이전트를 지정하는 정규식을 제공해야 합니다.

구문

```
turn on agents matching <REGULAR EXPRESSION>
```

예

```
turn on agents matching (.*)
```

이 명령은 모든 에이전트를 켭니다.

출력

없음

에이전트 끄기

이 명령은 하나 이상의 에이전트에서 메트릭 보고를 중지합니다. 대상 에이전트를 지정하는 정규식을 제공해야 합니다.

구성 파일 보내기

이 명령은 지정된 파일을 하나 이상의 에이전트에 보냅니다. 파일 이름, 대상 에이전트를 지정하는 정규식, 원본 및 대상 디렉터리를 제공해야 합니다.

해당 에이전트의 `introscope.agent.remoteagentconfiguration.enabled` 속성에서 원격 쓰기를 허용하도록 대상 에이전트를 구성해야 합니다. 위치와 해당 기본값은 상황에 따라 다릅니다. 자세한 내용은 *CA APM Java Agent 구현 안내서* 또는 *CA APM .NET 에이전트 구현 안내서*를 참조하십시오.

에이전트의 `introscope.agent.remoteagentconfiguration.allowedfiles` *property*에 명시적으로 지정된 파일만 복사할 수 있습니다.

이 속성의 기본값은 Introscope에서 CA CEM에 대한 트랜잭션을 인식하는 데 필요한 정보를 모두 포함하는 파일인 `domainconfig.xml`입니다.

APM 상태 콘솔 명령

이 단원에서는 APM 상태 콘솔과 관련된 CLW 명령을 제공합니다.

참고: APM 상태 콘솔 사용에 대한 자세한 내용은 *CA APM Workstation 사용자 안내서*를 참조하십시오.

APM 상태 콘솔 CLW 명령을 실행하려면 `apm_status_console_control` 권한이 있어야 합니다.

참고: 이 권한에 대한 자세한 내용은 *CA APM 보안 안내서*를 참조하십시오.

이 CLW 범주에는 다음 명령이 포함됩니다.

[클러스터 구성 가져오기](#) (페이지 157)

[활성 클램프 나열](#) (페이지 158)

[중요한 이벤트 나열](#) (페이지 161)

클러스터 구성 가져오기

이 명령은 다음 정보를 표시합니다.

- MOM 과 클러스터에 있는 모든 CDV 및 수집기의 호스트 이름 및 포트
- 독립 실행형 Enterprise Manager 의 호스트 및 포트

구문

`get cluster configuration`

예

get cluster configuration

이 명령은 MOM 과 클러스터에 있는 모든 수집기의 호스트 이름 및 포트를 나열합니다.

출력

MOM 과 클러스터에 있는 모든 수집기의 호스트 이름 및 포트를 나열합니다. MOM 이 먼저 나열된 다음 수집기가 나열됩니다.

```
MOM:
USERID04-W7@5001

Collectors:
localhost@3001
USERID04-@xyz_company.com@6001
```

독립 실행형 Enterprise Manager 의 경우 Enterprise Manager 의 호스트 및 포트를 나열합니다.

```
StandAlone:
USERID05-W8@5001
```

활성 클램프 나열

이 명령은 `apm-events-thresholds-config.xml` 에 있는 클램프 속성 중에서 현재 임계값에 도달했거나 임계값을 초과하는 클램프 속성을 나열합니다. 이러한 클램프를 **활성 클램프**라고 합니다. 이 명령은 다음 위치에 있는 활성 클램프 목록을 제공합니다.

- MOM 과 클러스터 내의 모든 수집기
- CDV 와 CDV 에 연결된 모든 수집기
- 독립 실행형 Enterprise Manager

`apm-events-thresholds-config.xml` 클램프 값이 임계값에 도달하거나 임계값을 초과하면 Enterprise Manager 가 APM 상태 콘솔에 알립니다.

구문

list active clamps

예

list active clamps

이 명령은 사용자 환경에 따라 다음 CA APM 구성 요소에 있는 활성 클램프를 모두 나열합니다.

- MOM 과 클러스터 내의 모든 수집기
- CDV 와 CDV 에 연결된 수집기 및 독립 실행형 Enterprise Manager
- 독립 실행형 Enterprise Manager

출력

사용자 환경에 따라 다음 CA APM 구성 요소에 있는 모든 활성 클램프의 이름을 나열합니다.

- MOM 과 클러스터 내의 수집기
- CDV 와 연결된 수집기 및 독립 실행형 Enterprise Manager
- 독립 실행형 Enterprise Manager

각 클램프에 대해 다음 정보를 나열합니다.

Enterprise Manager 이름, 클램프 이름, 클램프 설명, 클램프 임계값, 클램프 값, 클램프된 시간

예:

```
USERID04-w7@6001, introscope.enterprisemanager.metrics.live.limit, Per EM limit.
Takes into account only live metrics (i.e. currently reporting from Agents), 0,
40, 22:10:00 10/07/11
USERID04-w7@3001, introscope.enterprisemanager.agent.error.limit, Limits # of
Error Events Per Interval, 1, 1, 22:09:30 10/07/11
USERID04-w7@3001, introscope.enterprisemanager.metrics.live.limit, Per EM limit.
Takes into account only live metrics (i.e. currently reporting from Agents), 0,
219, 22:09:30 10/07/11
```

명령 옵션

이 단원에서는 *list active clamps* 명령 옵션을 설명합니다.

특정 수집기와 여러 수집기의 활성 클램프 나열

list active clamps 명령에 다음 두 가지 인수를 추가할 수 있습니다.

- of EM - 특정 MOM, 수집기, CDV 또는 독립 실행형 Enterprise Manager 의 활성 클램프 목록을 반환하려면 이 인수를 사용하십시오.
 - 구문


```
list active clamps of EM <enterprise-manager-host@port>
```
 - 예


```
list active clamps of EM localhost@3001
```
 - 출력

Enterprise Manager 이름, 클램프 이름, 클램프 설명, 클램프 임계값, 클램프 값, 클램프된 시간

```
localhost@3001, introscope.enterprise.agent.error.limit, Limits # of Error Events Per Interval, 1, 1, 22:09:30 10/07/11
localhost@3001, introscope.enterprise.metrics.live.limit, Per EM limit. Takes into account only live metrics (i.e. currently reporting from Agents), 0, 219, 22:09:30 10/07/11
```

참고: 잘못된 Enterprise Manager 이름을 입력하면 활성 클램프가 있는 수집기를 나열하는 오류 메시지가 콘솔에 표시됩니다. 올바른 Enterprise Manager 의 활성 클램프 목록을 가져오려면 오류 메시지에 제공된 Enterprise Manager 이름을 사용하여 명령을 다시 시도하십시오.

- of EM EnterpriseManagerName1@port,EnterpriseManagerName2,@port EnterpriseManagerNameX@port - 여러 특정 Enterprise Manager 의 활성 클램프 목록을 반환하려면 이 인수를 사용하십시오.
 - 구문


```
list active clamps of EM <EnterpriseManagerName1@port>, <EnterpriseManagerName2@port>
```
 - 예


```
list active clamps of EM localhost@3001,USERID04-w7@5001
```
 - 출력

지정된 모든 Enterprise Manager 에 대해 Enterprise Manager 이름, 클램프 이름, 클램프 설명, 클램프 임계값, 클램프 값, 클램프된 시간 등의 정보가 표시됩니다.


```
localhost@3001, introscope.enterprisemanager.agent.error.limit, Limits # of
Error Events Per Interval, 1, 1, 22:09:30 10/07/11
localhost@3001, introscope.enterprisemanager.metrics.live.limit, Per EM
limit. Takes into account only live metrics (i.e. currently reporting from
Agents), 0, 219, 22:09:30 10/07/11
USERID04-w7@3001, introscope.enterprisemanager.agent.error.limit, Limits #
of Error Events Per Interval, 1, 1, 22:09:30 10/07/11
USERID04-w7@3001, introscope.enterprisemanager.metrics.live.limit, Per EM
limit. Takes into account only live metrics (i.e. currently reporting from
Agents), 0, 219, 22:09:30 10/07/11
USERID04-w7@5001, introscope.enterprisemanager.metrics.live.limit, Per EM
limit. Takes into account only live metrics (i.e. currently reporting from
Agents), 200, 390, 22:22:55 10/07/11
```

참고: 잘못된 Enterprise Manager 이름을 입력하면 활성 클램프가 있는 수집기를 나열하는 오류 메시지가 콘솔에 표시됩니다. 올바른 Enterprise Manager의 활성 클램프 목록을 가져오려면 오류 메시지에 제공된 Enterprise Manager 이름을 사용하여 명령을 다시 시도하십시오.

중요한 이벤트 나열

이 명령은 `apm-events-thresholds-config.xml`에 있는 중요한 이벤트 속성 중에서 현재 임계값에 도달하거나 임계값을 초과하는 중요한 이벤트 속성을 나열합니다. 이 명령은 클러스터에 있는 모든 CDV와 수집기의 중요한 이벤트 목록이나 독립 실행형 Enterprise Manager의 중요한 이벤트 목록을 제공합니다.

`apm-events-thresholds-config.xml` 속성 값이 임계값에 도달하거나 임계값을 초과하면 Enterprise Manager가 APM 상태 콘솔에 알립니다.

구문

```
list important events
```

예

```
list important events
```

이 명령은 클러스터나 독립 실행형 Enterprise Manager의 중요한 이벤트를 모두 나열합니다.

출력

클러스터나 독립 실행형 Enterprise Manager 의 모든 중요한 이벤트에 대한 데이터를 나열합니다.

각 이벤트에 대해 다음 정보가 표시됩니다.

Enterprise Manager 이름, 이벤트 심각도, 이벤트 설명, 이벤트 시간

예:

```
USERID04-w7@6001, Warning Event, The Smartstor duration on EM USERID04-w7@6001
is more than configured threshold [Actual Value : 1,780/ Threshold : 5]. The most
likely cause would be slow disk., 22:10:02 10/07/11
USERID04-w7@3001, Warning Event, The harvest duration of EM USERID04-w7@3001 is
more than configured threshold [Actual Value : 169/ Threshold : 5], 22:09:30
10/07/11
USERID04-w7@3001, Warning Event, The Smartstor duration on EM USERID04-w7@3001
is more than configured threshold [Actual Value : 1,255/ Threshold : 5]. The most
likely cause would be slow disk., 22:09:31 10/07/11
USERID04-w7@5001, Warning Event, The Smartstor duration on EM USERID04-w7@5001
is more than configured threshold [Actual Value : 95/ Threshold : 50]. The most
likely cause would be slow disk., 22:32:40 10/07/11
```

관리 모듈 명령

관리 모듈은 Workstation 에 있는 요소를 보다 쉽게 찾아서 조작할 수 있도록 구성합니다. 관리 모듈에 대한 CLW 명령은 Enterprise Manager 간에 관리 모듈과 해당 관리 모듈에 포함된 요소를 이동하는 프로세스를 단순화합니다.

관리 모듈 나열

관리 모듈 나열 명령은 관리 모듈을 하나 이상 나열합니다. 관리 모듈을 지정하는 정규식을 제공해야 합니다.

구문

```
list management modules matching <REGULAR EXPRESSION>
```

예

```
list management modules matching (.*)
```

이 명령은 모든 관리 모듈을 나열합니다.

출력

다음과 같이 각 관리 모듈의 이름이 나열됩니다.

```
Sample  
Sample13  
Sample11
```

관리 모듈 쿼리

"관리 모듈 쿼리" 명령은 관리 모듈과 해당 관리 모듈의 현재 상태(활성 또는 비활성)를 나열합니다. 대상 관리 모듈을 지정하는 정규식을 제공해야 합니다.

구문

```
query state of management modules matching <REGULAR EXPRESSION>
```

예

```
query state of management modules matching (.*)
```

이 명령은 모든 관리 모듈의 이름과 상태를 반환합니다.

출력

다음과 같이 각 관리 모듈의 이름과 상태가 나열됩니다.

```
Sample1:Active  
Sample2:Active
```

관리 모듈 활성화

관리 모듈 활성화 명령은 관리 모듈을 하나 이상 활성화합니다. 대상 관리 모듈을 지정하는 정규식을 제공해야 합니다.

참고: 관리 모듈 활성화 명령으로는 "Triage Map Configuration"(심사 맵 구성) 관리 모듈을 활성화할 수 없습니다.

관리 모듈 비활성화

관리 모듈 비활성화 명령은 관리 모듈을 하나 이상 비활성화합니다. 대상 관리 모듈을 지정하는 정규식을 제공해야 합니다.

참고: 관리 모듈 비활성화 명령으로는 심사 맵 구성 관리 모듈을 비활성화할 수 없습니다.

관리 모듈 복사

관리 모듈 복사 명령은 <EM_Home>/config/modules 디렉터리에 관리 모듈의 복사본을 생성합니다.

이 명령을 사용하면 기존 관리 모듈에 기반하여 효율적으로 새 관리 모듈을 하나 이상 생성할 수 있습니다. 예를 들어 메트릭 그룹을 제외하고 기존 관리 모듈과 같은 관리 모듈을 새로 생성하려면 CLW 를 사용하여 기존 관리 모듈을 복사한 다음 GUI Workstation 에서 새 관리 모듈의 메트릭 그룹을 수정합니다.

관리 모듈 복사 명령에서 복사할 관리 모듈, 새 관리 모듈 이름, 새 관리 모듈의 .jar 파일 이름(파일 확장명 제외)을 식별해야 합니다.

참고: 관리 모듈 비활성화 명령으로는 심사 맵 구성 관리 모듈을 비활성화할 수 없습니다.

관리 모듈 삭제

"관리 모듈 삭제" 명령은 관리 모듈을 삭제합니다. 삭제할 관리 모듈의 정확한 이름을 제공해야 합니다.

읽기 전용 관리 모듈

이 명령은 지정된 정규식과 일치하는 관리 모듈을 읽기 전용으로 설정합니다.

경고! CA Technologies에서는 나중에 사용할 수 있도록 편집 가능한 관리 모듈의 버전을 안전한 장소에 보관할 것을 권장합니다. 관리 모듈을 읽기 전용으로 설정한 후에는 편집 가능한 상태로 되돌릴 수 없습니다.

다음 단계를 따르십시오.

1. <regular expression>과 일치하는 읽기 전용 관리 모듈을 설정합니다.
2. Workstation에 로그인하고 관리 모듈 편집기를 연 다음 정규식과 일치하는 관리 모듈 옆에 잠금 아이콘이 있는지 확인합니다.
3. 더 이상 허용되지 않는 관리 모듈 옆의 "편집 가능" 확인란을 선택 취소합니다.

참고: 이 기능은 CA Technologies 파트너용입니다. 사용자 환경에서 이 기능을 사용하기 전에 CA Support에 문의하십시오.

작업 명령

작업은 알림과 같이 경고에 의해 트리거될 수 있는 동작입니다.

작업 나열

"작업 나열" 명령은 하나 이상의 관리 모듈에 있는 작업을 하나 이상 나열합니다. 두 개의 정규식, 즉 작업을 지정하는 정규식과 관리 모듈을 지정하는 정규식을 제공해야 합니다.

구문

```
list actions matching <REGULAR EXPRESSION> in management modules matching <REGULAR EXPRESSION>
```

예

```
list actions matching (.*) in management modules matching (.*)
```

이 명령은 모든 관리 모듈의 동작을 모두 나열합니다.

출력

다음과 같이 해당 동작을 포함하는 관리 모듈이 앞에 붙어 있는 상태로 각 동작이 나열됩니다.

Sample.SMTP Email Action

Sample10.Workstation Notification

Sample2.Workstation Notification

작업 활성화

"작업 활성화" 명령은 하나 이상의 관리 모듈에 있는 작업을 하나 이상 활성화합니다. 두 개의 정규식, 즉 활성화할 작업을 지정하는 정규식과 해당 작업을 활성화할 관리 모듈을 지정하는 정규식을 제공해야 합니다.

구문

activate actions matching <REGULAR EXPRESSION> in management modules matching <REGULAR EXPRESSION>

예

activate actions matching (SMTP.) in management modules matching (.*)*

이 명령은 모든 관리 모듈에서 *SMTP* 문자열로 시작하는 동작을 활성화합니다.

출력

다음과 같이 해당 동작을 포함하는 관리 모듈이 앞에 붙어 있고 해당 동작의 활성화 상태가 뒤에 붙어 있는 상태로 이 명령을 통해 활성화된 동작이 각각 나열됩니다.

Sample.SMTP Email Action:Active

Sample10.Workstation Notification:Active

Sample2.Workstation Notification:Active

작업 비활성화

"작업 비활성화" 명령은 하나 이상의 관리 모듈에 있는 작업을 하나 이상 비활성화합니다. 두 개의 정규식, 즉 비활성화할 작업을 지정하는 정규식과 해당 작업을 비활성화할 관리 모듈을 지정하는 정규식을 제공해야 합니다.

작업 쿼리

"작업 쿼리" 명령은 하나 이상의 관리 모듈에 있는 하나 이상의 작업의 상태(활성 또는 비활성)를 나열합니다. 두 개의 정규식, 즉 작업을 지정하는 정규식과 관리 모듈을 지정하는 정규식을 제공해야 합니다.

작업 이름 바꾸기

"작업 이름 바꾸기" 명령은 작업의 이름을 바꿉니다. 작업 이름, 해당 작업을 포함하는 관리 모듈 및 새 작업 이름을 지정해야 합니다.

작업 삭제

"작업 삭제" 명령은 하나 이상의 관리 모듈에서 하나 이상의 작업을 삭제합니다. 두 개의 정규식, 즉 작업을 지정하는 정규식과 해당 작업을 삭제할 관리 모듈을 지정하는 정규식을 제공해야 합니다.

참고: 다른 요소에서 사용되거나 참조되는 작업(예: 경고에 연결되는 작업)은 삭제할 수 없습니다.

경고 명령

경고는 메트릭 값을 사용자 정의 임계값과 비교하여 관리되는 Java 응용 프로그램 내의 잠재적인 문제를 나타냅니다.

경고 나열

"경고 나열" 명령은 하나 이상의 관리 모듈에 있는 경고를 하나 이상 나열합니다. 두 개의 정규식, 즉 경고를 지정하는 정규식과 관리 모듈을 지정하는 정규식을 제공해야 합니다.

구문

```
list alerts matching <REGULAR EXPRESSION> in management modules matching <REGULAR EXPRESSION>
```

예

```
list alerts matching (.*) in management modules matching Sample
```

이 명령은 *Sample* 이라는 관리 모듈에 포함된 경고를 나열합니다.

출력

다음과 같이 해당 경고를 포함하는 관리 모듈이 앞에 붙어 있는 상태로 각 경고가 나열됩니다.

```
Sample.Console Summary Alert
Sample.All Servlet Response Time
Sample.All EJB Response Times
```

경고 활성화

"경고 활성화" 명령은 하나 이상의 관리 모듈에 있는 경고를 하나 이상 활성화합니다. 두 개의 정규식, 즉 활성화할 경고를 지정하는 정규식과 해당 경고를 활성화할 관리 모듈을 지정하는 정규식을 제공해야 합니다.

구문

```
activate alerts matching <REGULAR EXPRESSION> in management modules
matching <REGULAR EXPRESSION>
```

예

```
activate alerts matching (.*) in management modules matching Same2
```

이 명령은 *Sample2* 라는 관리 모듈에 포함된 경고를 모두 활성화합니다.

출력

다음과 같이 해당 경고를 포함하는 관리 모듈이 앞에 붙어 있고 해당 경고의 상태가 뒤에 붙어 있는 상태로 이 명령을 통해 활성화된 경고가 각각 나열됩니다.

```
Sample2.Application Summary Alert:Active
Sample2.SQL Average Processing Time #2 (ms):Active
Sample2.CPUApp1:Active
```

경고 비활성화

"경고 비활성화" 명령은 하나 이상의 관리 모듈에 있는 경고를 하나 이상 비활성화합니다. 두 개의 정규식, 즉 비활성화할 경고를 지정하는 정규식과 해당 경고를 비활성화할 관리 모듈을 지정하는 정규식을 제공해야 합니다.

경고 쿼리

"경고 쿼리" 명령은 하나 이상의 관리 모듈에 있는 하나 이상의 경고의 상태(활성 또는 비활성)를 나열합니다. 두 개의 정규식, 즉 경고를 지정하는 정규식과 관리 모듈을 지정하는 정규식을 제공해야 합니다.

경고 이름 바꾸기

"경고 이름 바꾸기" 명령은 경고의 이름을 바꿉니다. 경고 이름, 해당 경고를 포함하는 관리 모듈 및 새 경고 이름을 지정해야 합니다.

경고 삭제

"경고 삭제" 명령은 하나 이상의 관리 모듈에서 하나 이상의 경고를 삭제합니다. 두 개의 정규식, 즉 경고를 지정하는 정규식과 경고를 삭제할 관리 모듈을 지정하는 정규식을 제공해야 합니다.

참고: 다른 요소에서 사용되거나 참조되는 경고(예: 대시보드에서 사용되는 경고)는 삭제할 수 없습니다.

경고 중지 일정 명령

"경고 중지 일정"을 사용하면 Introscope Workstation 관리 모듈 편집기에서 중지 기간을 관리할 수 있습니다.

경고 중지 일정 나열

"경고 중지 일정 나열" 명령은 하나 이상의 관리 모듈에 있는 경고 중지 일정을 하나 이상 나열합니다. 두 개의 정규식, 즉 경고 중지 일정을 지정하는 정규식과 관리 모듈을 지정하는 정규식을 제공해야 합니다.

구문

```
list alert downtime schedules matching [REGULAR EXPRESSION] in management modules matching [REGULAR EXPRESSION]
```

예

```
List alert downtime schedules matching (.*) in management modules matching Sample
```

출력

Sample.Example Alert Downtime Schedule
Sample.Another Alert Downtime Schedule

경고 중지 일정 활성화

"경고 중지 일정 활성화" 명령은 하나 이상의 관리 모듈에 있는 경고 중지 일정을 하나 이상 활성화합니다. 두 개의 정규식, 즉 활성화할 경고 중지 일정을 지정하는 정규식과 해당 경고 중지 일정을 활성화할 관리 모듈을 지정하는 정규식을 제공해야 합니다.

구문

activate alert downtime schedules matching [REGULAR EXPRESSION] in management modules matching [REGULAR EXPRESSION]

예

activate alert downtime schedules matching (.) in management modules matching Sample*

출력

Sample.Example Alert Downtime Schedule:Active

Sample.Another Alert Downtime Schedule:Active

경고 중지 일정 비활성화

"경고 중지 일정 비활성화" 명령은 하나 이상의 관리 모듈에 있는 경고 중지 일정을 하나 이상 비활성화합니다. 두 개의 정규식, 즉 비활성화할 경고 중지 일정을 지정하는 정규식과 해당 경고 중지 일정을 비활성화할 관리 모듈을 지정하는 정규식을 제공해야 합니다.

경고 중지 일정 쿼리

"경고 중지 일정 쿼리" 명령은 하나 이상의 관리 모듈에 있는 하나 이상의 경고 중지 일정의 상태(활성 또는 비활성)를 나열합니다. 두 개의 정규식, 즉 경고 중지 일정을 지정하는 정규식과 관리 모듈을 지정하는 정규식을 제공해야 합니다.

경고 중지 일정 이름 바꾸기

"경고 중지 일정 이름 바꾸기" 명령은 경고 중지 일정의 이름을 바꿉니다. 경고 중지 일정 이름, 해당 경고 중지 일정을 포함하는 관리 모듈 및 새 경고 중지 일정 이름을 지정해야 합니다.

경고 중지 일정 삭제

"경고 중지 일정 삭제" 명령은 하나 이상의 관리 모듈에서 하나 이상의 경고 중지 일정을 삭제합니다. 두 개의 정규식, 즉 경고 중지 일정을 지정하는 정규식과 해당 경고 중지 일정을 삭제할 관리 모듈을 지정하는 정규식을 제공해야 합니다.

계산기 명령

계산기는 메트릭 데이터의 합계 또는 평균을 구하는 방식으로 사용자 지정 메트릭을 만듭니다.

계산기 나열

"계산기 나열" 명령은 하나 이상의 관리 모듈에 있는 계산기를 하나 이상 나열합니다. 두 개의 정규식, 즉 계산기를 지정하는 정규식과 관리 모듈을 지정하는 정규식을 제공해야 합니다.

구문

```
list calculators matching <REGULAR EXPRESSION> in management modules matching <REGULAR EXPRESSION>
```

예

```
list calculators matching (.*) in management modules matching (.*)
```

이 명령은 모든 관리 모듈의 계산기를 모두 나열합니다.

출력

다음과 같이 해당 계산기를 포함하는 관리 모듈이 앞에 붙어 있는 상태로 각 계산기가 나열됩니다.

```
Sample.Average Servlet Response Time
```

계산기 활성화

"계산기 활성화" 명령은 하나 이상의 관리 모듈에 있는 계산기를 하나 이상 활성화합니다. 두 개의 정규식, 즉 활성화할 계산기를 지정하는 정규식과 해당 계산기를 활성화할 관리 모듈을 지정하는 정규식을 제공해야 합니다.

구문

```
activate calculators matching <REGULAR EXPRESSION> in management modules matching <REGULAR EXPRESSION>
```

예

```
activate calculators matching (.*) in management modules matching Sample2
```

이 명령은 *Sample2* 라는 관리 모듈에 있는 계산기를 모두 활성화합니다.

출력

다음과 같이 해당 계산기를 포함하는 관리 모듈이 앞에 붙어 있고 해당 계산기의 상태가 뒤에 붙어 있는 상태로 이 명령을 통해 활성화된 계산기가 각각 나열됩니다.

```
Sample2.Average Servlet Response Time:Active
```

계산기 비활성화

"계산기 비활성화" 명령은 하나 이상의 관리 모듈에 있는 계산기를 하나 이상 비활성화합니다. 두 개의 정규식, 즉 비활성화할 계산기를 지정하는 정규식과 해당 계산기를 비활성화할 관리 모듈을 지정하는 정규식을 제공해야 합니다.

계산기 쿼리

"계산기 쿼리" 명령은 하나 이상의 관리 모듈에 있는 하나 이상의 계산기의 상태(활성 또는 비활성)를 나열합니다. 두 개의 정규식, 즉 계산기를 지정하는 정규식과 관리 모듈을 지정하는 정규식을 제공해야 합니다.

계산기 이름 바꾸기

"계산기 이름 바꾸기" 명령은 계산기의 이름을 바꿉니다. 계산기 이름, 해당 계산기를 포함하는 관리 모듈 및 새 계산기 이름을 지정해야 합니다.

계산기 삭제

"계산기 삭제" 명령은 하나 이상의 관리 모듈에서 하나 이상의 계산기를 삭제합니다. 두 개의 정규식, 즉 계산기를 지정하는 정규식과 해당 계산기를 삭제할 관리 모듈을 지정하는 정규식을 제공해야 합니다.

참고: 다른 요소에서 사용되거나 참조되는 계산기(예: 대시보드에서 사용되는 계산기)는 삭제할 수 없습니다.

대시보드 명령

대시보드는 그래픽 및 텍스트 개체와 함께 그래프, 가로 막대형 차트, 경고 상태 표시기 등의 데이터 뷰어 개체를 포함하는 Workstation 내의 페이지입니다.

대시보드 나열

"대시보드 나열" 명령은 하나 이상의 관리 모듈에 있는 대시보드를 하나 이상 나열합니다. 두 개의 정규식, 즉 대시보드를 지정하는 정규식과 관리 모듈을 지정하는 정규식을 제공해야 합니다.

구문

```
list dashboards matching <REGULAR EXPRESSION> in management modules matching <REGULAR EXPRESSION>
```

예

```
list dashboards matching (. *Triage) in management modules matching (. *)
```

이 명령은 모든 관리 모듈에서 이름이 *Triage* 문자열로 끝나는 대시보드를 나열합니다.

출력

다음과 같이 해당 대시보드를 포함하는 관리 모듈이 앞에 붙어 있는 상태로 각 대시보드가 나열됩니다.

Sample10.3. Triage

Sample2.3. Triage

Sample.3. Triage

대시보드 활성화

"대시보드 활성화" 명령은 하나 이상의 관리 모듈에 있는 대시보드를 하나 이상 활성화합니다. 두 개의 정규식, 즉 활성화할 대시보드를 지정하는 정규식과 해당 대시보드를 활성화할 관리 모듈을 지정하는 정규식을 제공해야 합니다.

구문

```
activate dashboards matching <REGULAR EXPRESSION> in management  
modules matching <REGULAR EXPRESSION>
```

예

```
activate dashboards matching (.*) in management modules matching Sample2
```

이 명령은 *Sample2* 라는 관리 모듈에 있는 대시보드를 모두 활성화합니다.

출력

다음과 같이 해당 대시보드를 포함하는 관리 모듈이 앞에 붙어 있고 해당 대시보드의 상태가 뒤에 붙어 있는 상태로 이 명령을 통해 활성화된 대시보드가 각각 나열됩니다.

Sample2.4b. Database Detail:Active

Sample2.1. Introscope Console:Active

Sample2.2. Detection:Active

대시보드 비활성화

"대시보드 비활성화" 명령은 하나 이상의 관리 모듈에 있는 대시보드를 하나 이상 비활성화합니다. 두 개의 정규식, 즉 비활성화할 대시보드를 지정하는 정규식과 해당 대시보드를 비활성화할 관리 모듈을 지정하는 정규식을 제공해야 합니다.

대시보드 쿼리

"대시보드 쿼리" 명령은 하나 이상의 관리 모듈에 있는 하나 이상의 대시보드의 상태(활성 또는 비활성)를 나열합니다. 두 개의 정규식, 즉 대시보드를 지정하는 정규식과 관리 모듈을 지정하는 정규식을 제공해야 합니다.

대시보드 이름 바꾸기

"대시보드 이름 바꾸기" 명령은 대시보드의 이름을 바꿉니다. 대시보드 이름, 해당 대시보드를 포함하는 관리 모듈 및 새 대시보드 이름을 지정해야 합니다.

대시보드 삭제

"대시보드 삭제" 명령은 하나 이상의 관리 모듈에서 하나 이상의 대시보드를 삭제합니다. 두 개의 정규식, 즉 대시보드를 지정하는 정규식과 해당 대시보드를 삭제할 관리 모듈을 지정하는 정규식을 제공해야 합니다.

참고: 다른 요소에서 사용되거나 참조되는 대시보드는 삭제할 수 없습니다. 예를 들어 다른 대시보드의 데이터 뷰어에 대한 하이퍼링크가 있는 대시보드는 삭제할 수 없습니다.

메트릭 및 메트릭 그룹화 명령

메트릭 그룹화는 작업을 수행할 메트릭을 지정하고 경고, 계산기 등의 요소에 대한 구성 단위로 사용됩니다.

메트릭 그룹 나열

"메트릭 그룹 나열" 명령은 하나 이상의 관리 모듈에 있는 메트릭 그룹을 하나 이상 나열합니다. 두 개의 정규식, 즉 메트릭 그룹을 지정하는 정규식과 관리 모듈을 지정하는 정규식을 제공해야 합니다.

구문

list metric groups matching <REGULAR EXPRESSION> in management modules matching <REGULAR EXPRESSION>

예

*list metric groups matching (. *Response. *) in management modules matching Sample*

이 명령은 *Sample* 이라는 관리 모듈에서 이름에 *Response* 문자열이 포함된 메트릭 그룹을 나열합니다.

출력

다음과 같은 형식으로 메트릭 그룹이 나열됩니다.

<Management Module>.<Metric Group>[Agent: "<Agent Expression>" Attribute: "<Metric Expression>"]

예:

Sample.Servlet Average Response Time (ms) [Agent: "(.)\\(.*)\\(.*)" Attribute: "\\Servlets:Average Response Time \\(ms\\)"]*

위의 샘플은 다음과 같은 메트릭 그룹화 정보를 제공합니다.

관리 모듈 - *Sample*

메트릭 그룹화 이름 - *Servlet Average Response Time (ms)*

에이전트 표현식 - *(.*)\\(.*)\\(.*)*

메트릭 표현식 - *Servlets:Average Response Time \\(ms\\)*

Turn on exact metric(정확한 메트릭 켜기)

이 명령은 에이전트에 특정 메트릭을 켜도록 요청합니다.

구문

turn on exact metric <metric name>

예

```
turn on exact metric
jdoe-dt|Weblogic|WebLogicAgent|Servlets|Servlet21|Servlet21_1u2oj1_Impl:Average Response Time (ms)
```

에이전트가

"jdoe-dt|Weblogic|WebLogicAgent|Servlets|Servlet21|Servlet21_1u2oj1_Impl:평균 응답 시간(ms)" 메트릭을 켜고 데이터 보내기를 시작합니다.

출력

없음

Turn Off Exact Metric(정확한 메트릭 끄기)

이 명령은 에이전트에 특정 메트릭을 끄도록 요청합니다.

구문

```
turn off exact metric <metric name>
```

예

```
turn off exact metric
jdoe-dt|Weblogic|WebLogicAgent|Servlets|Servlet21|Servlet21_1u2oj1_Impl:Average Response Time (ms)
```

에이전트가

"jdoe-dt|Weblogic|WebLogicAgent|Servlets|Servlet21|Servlet21_1u2oj1_Impl:평균 응답 시간(ms)" 메트릭을 끄고 데이터 보내기를 중지합니다.

출력

없음

보고서 템플릿 명령

이 단원에서는 보고서를 관리하고 생성하기 위한 CLW 명령을 정의합니다. Introscope 의 보고 기능에 대한 자세한 내용은 *CA APM Workstation 사용자 안내서*의 "보고" 장을 참조하십시오.

보고서 템플릿 나열

"보고서 템플릿 나열" 명령은 하나 이상의 관리 모듈에 있는 보고서 템플릿을 하나 이상 나열합니다. 두 개의 정규식, 즉 보고서 템플릿을 지정하는 정규식과 관리 모듈을 지정하는 정규식을 제공해야 합니다.

구문

```
list report templates matching <REGULAR EXPRESSION> in management modules matching <REGULAR EXPRESSION>
```

예

```
list report templates matching (.*) in management modules matching Sample
```

이 명령은 *Sample* 이라는 관리 모듈에 있는 보고서 템플릿을 모두 나열합니다.

출력

해당 보고서 템플릿을 포함하는 관리 모듈이 각 보고서 템플릿 앞에 붙어 있습니다.

```
Sample.QA/Test Application Performance  
Sample.System Availability  
Sample.Application Capacity Planning
```

보고서 템플릿 활성화

"보고서 템플릿 활성화" 명령은 하나 이상의 관리 모듈에 있는 보고서 템플릿을 하나 이상 활성화합니다. 두 개의 정규식, 즉 활성화할 보고서 템플릿을 지정하는 정규식과 해당 보고서 템플릿을 활성화할 관리 모듈을 지정하는 정규식을 제공해야 합니다.

구문

```
activate report templates matching <REGULAR EXPRESSION> in management modules matching <REGULAR EXPRESSION>
```

예

activate report templates matching (.) in management modules matching Sample2*

이 명령은 Sample2 라는 관리 모듈에 있는 보고서 템플릿을 모두 활성화합니다.

출력

다음과 같이 해당 보고서 템플릿을 포함하는 관리 모듈이 앞에 붙어 있고 해당 보고서 템플릿의 상태가 뒤에 붙어 있는 상태로 이 명령을 통해 활성화된 보고서 템플릿이 각각 나열됩니다.

Sample2.Application Capacity Planning:Active

Sample2.Production Application Health:Active

Sample2.System Availability:Active

보고서 템플릿 비활성화

"보고서 템플릿 비활성화" 명령은 하나 이상의 관리 모듈에 있는 보고서 템플릿을 하나 이상 비활성화합니다. 두 개의 정규식, 즉 비활성화할 보고서 템플릿을 지정하는 정규식과 해당 보고서 템플릿을 비활성화할 관리 모듈을 지정하는 정규식을 제공해야 합니다.

보고서 템플릿 쿼리

"보고서 템플릿 쿼리" 명령은 하나 이상의 관리 모듈에 있는 하나 이상의 보고서 템플릿의 상태(활성 또는 비활성)를 나열합니다. 두 개의 정규식, 즉 보고서 템플릿을 지정하는 정규식과 관리 모듈을 지정하는 정규식을 제공해야 합니다.

보고서 템플릿 이름 바꾸기

"보고서 템플릿 이름 바꾸기" 명령은 보고서 템플릿의 이름을 바꿉니다. 보고서 템플릿 이름, 해당 보고서 템플릿을 포함하는 관리 모듈 및 새 보고서 템플릿 이름을 지정해야 합니다.

보고서 템플릿 삭제

"보고서 템플릿 삭제" 명령은 하나 이상의 관리 모듈에서 하나 이상의 보고서 템플릿을 삭제합니다. 두 개의 정규식, 즉 보고서 템플릿을 지정하는 정규식과 해당 보고서 템플릿을 삭제할 관리 모듈을 지정하는 정규식을 제공해야 합니다.

보고서 생성

"보고서 생성" 명령은 보고서를 생성합니다. 다음과 같은 인수를 제공해야 합니다.

- 보고서 이름
- 시작 시간
- 종료 시간
- 관리 모듈 이름
- 파일 이름 - 경로를 지정하지 않은 경우 이 파일은 현재 작업 디렉터리에 기록됩니다. 파일은 파일 확장명과 연결된 형식으로 기록되고 파일 확장명은 HTML, PDF, XLS, TEXT, XML, CSV 중 하나여야 합니다.

명령

"보고서 생성" 명령은 기본 명령, 확장 명령 및 에이전트 무시 명령의 세 가지가 있습니다.

기본 명령:

generate report named [EXACT MATCH] in management module named [EXACT MATCH] to [EXACT MATCH]

확장 명령:

generate report named [EXACT MATCH] in management module named [EXACT MATCH] starting at [EXACT MATCH] ending at [EXACT MATCH] to [EXACT MATCH]

선택적 매개 변수

위의 기본 명령과 확장 명령 모두에서 선택적 매개 변수를 사용할 수 있습니다.

```
{in agents matching [REGEX PATTERN]} {starting at [EXACT MATCH] ending at [EXACT MATCH]}
```

선택적 매개 변수의 구문은 다음과 같습니다.

```
generate report named [EXACT MATCH] in management module named [EXACT MATCH] {in agents matching [REGEX PATTERN]} {starting at [EXACT MATCH] ending at [EXACT MATCH]} to [EXACT MATCH]
```

보고서 타임스탬프 형식

보고서 타임스탬프는 다양한 형식으로 표시됩니다. 아래 표는 표시될 수 있는 다양한 형식을 나타냅니다.

타임스탬프 형식	예
<i>M/d/yy h:mm a</i>	11/17/08 3:00 PM
<i>M/d/yy h:mm:ss a</i>	11/17/08 3:00:06 PM
<i>M/d/yy h:mm:ss a z</i>	11/17/08 3:00:06 PM PST
<i>M/d/yy</i>	11/17/08
<i>MMM d, yyyy h:mm a</i>	Nov 17, 2008 3:00 PM
<i>MMM d, yyyy h:mm:ss a</i>	Nov 17, 2008 3:00:06 PM
<i>MMM d, yyyy h:mm:ss a z</i>	Nov 17, 2008 3:00:06 PM PST
<i>MMM d, yyyy</i>	Nov 17, 2008
<i>MMMM d, yyyy h:mm a</i>	November 17, 2008 3:00 PM
<i>MMMM d, yyyy h:mm:ss a</i>	November 17, 2008 3:00:06 PM
<i>MMMM d, yyyy h:mm:ss a z</i>	November 17, 2008 3:00:06 PM PST
<i>MMMM d, yyyy</i>	November 17, 2008
<i>EEE MMM dd HH:mm:ss zzz yyyy</i>	Mon Nov 17 15:00:06 PST 2008
<i>MM/dd/yy HH:mm:ss</i>	11/17/08 15:00:06
<i>yyyy-MM-dd HH:mm:ss</i>	2008-11-17 15:00:06
<i>yyyy-MM-dd HH:mm:ss.SSSS</i>	2008-11-17 15:00:06.0840

<i>yyyy-MM-dd HH:mm</i>	2008-11-17 15:00
<i>yyyy-MM-dd hh:mm:ss a</i>	2008-11-17 03:00:06 PM
<i>yyyy-MM-dd hh:mm a</i>	2008-11-17 03:00 PM
<i>yyyy/MM/dd hh:mm:ss a</i>	2008/11/17 03:00:06 PM
<i>yyyy/MM/dd hh:mm a</i>	2008/11/17 03:00 PM
<i>yyyy/MM/dd HH:mm:ss</i>	2008/11/17 15:00:06
<i>yyyy/MM/dd HH:mm</i>	2008/11/17 15:00

SNMP 수집 명령

이러한 명령은 게시된 MIB 에 포함되는 수집된 메트릭을 정의합니다.

SNMP 수집 나열

"SNMP 수집 나열" 명령은 하나 이상의 관리 모듈에 있는 SNMP 수집을 하나 이상 나열합니다. 두 개의 정규식, 즉 SNMP 수집을 지정하는 정규식과 관리 모듈을 지정하는 정규식을 제공해야 합니다.

구문

```
list snmp collections matching <REGULAR EXPRESSION> in management modules matching <REGULAR EXPRESSION>
```

예

```
list snmp collections matching (.*) in management modules matching (.*)
```

이 명령은 모든 관리 모듈의 SNMP 수집을 모두 나열합니다.

출력

해당 SNMP 수집을 포함하는 관리 모듈이 각 SNMP 수집 앞에 붙어 있습니다.
예:

```
Sample2.JDBC QueryUpdate
```

SNMP 수집 활성화

"SNMP 수집 활성화" 명령은 하나 이상의 관리 모듈에 있는 SNMP 수집을 하나 이상 활성화합니다. 두 개의 정규식, 즉 활성화할 SNMP 수집을 지정하는 정규식과 해당 SNMP 수집을 활성화할 관리 모듈을 지정하는 정규식을 제공해야 합니다.

구문

```
activate snmp collections matching <REGULAR EXPRESSION> in management modules matching <REGULAR EXPRESSION>
```

예

```
activate snmp collections matching (.*) in management modules matching Sample2
```

이 명령은 *Sample2* 라는 관리 모듈에 있는 SNMP 수집을 모두 활성화합니다.

출력

다음과 같이 해당 SNMP 수집을 포함하는 관리 모듈이 앞에 붙어 있고 해당 SNMP 수집의 상태가 뒤에 붙어 있는 상태로 이 명령을 통해 활성화된 SNMP 수집이 각각 나열됩니다.

```
Sample2.JDBC QueryUpdate:Active
```

SNMP 수집 비활성화

"SNMP 수집 비활성화" 명령은 하나 이상의 관리 모듈에 있는 SNMP 수집을 하나 이상 비활성화합니다. 두 개의 정규식, 즉 비활성화할 SNMP 수집을 지정하는 정규식과 해당 SNMP 수집을 비활성화할 관리 모듈을 지정하는 정규식을 제공해야 합니다.

SNMP 수집 쿼리

"SNMP 수집 쿼리" 명령은 하나 이상의 관리 모듈에 있는 하나 이상의 SNMP 수집의 상태(활성 또는 비활성)를 나열합니다. 두 개의 정규식, 즉 SNMP 수집을 지정하는 정규식과 관리 모듈을 지정하는 정규식을 제공해야 합니다.

SNMP 수집 이름 바꾸기

"SNMP 수집 이름 바꾸기" 명령은 SNMP 수집의 이름을 바꿉니다. SNMP 수집 이름, 해당 SNMP 수집을 포함하는 관리 모듈 및 새 SNMP 수집 이름을 지정해야 합니다.

SNMP 수집 삭제

"SNMP 수집 삭제" 명령은 하나 이상의 관리 모듈에서 하나 이상의 SNMP 수집을 삭제합니다. 두 개의 정규식, 즉 SNMP 수집을 지정하는 정규식과 해당 SNMP 수집을 삭제할 관리 모듈을 지정하는 정규식을 제공해야 합니다.

트랜잭션 추적 옵션 구성

CLW 는 다음과 같은 시스템 속성을 사용하여 다양한 트랜잭션 추적 옵션을 구성하는 옵션을 제공합니다.

- `-Dintroscope.clw.tt.console` - "true"로 설정한 경우 트랜잭션 추적이 콘솔에 출력됩니다.
- `-Dintroscope.clw.tt.dirname` - 트랜잭션 추적 XML 파일이 저장되는 로컬 디렉터리입니다.
- `-Dintroscope.clw.tt.filename` - 트랜잭션 추적을 저장하는 데 사용되는 파일 이름입니다. 디렉터리 이름을 포함하면 안 됩니다.
- `-Dintroscope.clw.tt.encoding` - XML 파일을 디스크에 기록할 때 사용되는 인코딩입니다. 이 속성에 대한 설정에는 기본 옵션인 *ISO-8859-1* 과 *UTF-8*, *UTF-16* 및 *Windows-1252* 가 포함됩니다.

트랜잭션 추적 세션 시작

트랜잭션 추적 프로그램은 단일 JVM 의 경계를 통과해서 흐르는 개별 트랜잭션의 동작을 추적합니다.

트랜잭션 추적은 트랜잭션 이벤트 데이터베이스에 자동으로 저장되며 기본적으로 CA Introscope Workstation 의 트랜잭션 추적 뷰어에서 열고 분석할 수 있는 하나 이상의 XML 파일에도 캡처됩니다. CA Introscope 트랜잭션 추적 프로그램에 대한 자세한 내용은 *CA APM Workstation 사용자 안내서*를 참조하십시오.

명령 구문

CLW 명령으로 트랜잭션 추적 세션의 많은 요소를 지정할 수 있습니다. 이러한 요소는 다음과 같습니다.

- 실행 임계값 - 추적할 트랜잭션의 최소 실행 시간입니다. 실행 시간이 임계값보다 오래 걸리는 트랜잭션에 대해 추적이 수행됩니다. 임계값을 초 단위로 지정할 수 있습니다.
- 추적할 에이전트 - 트랜잭션을 추적할 에이전트를 지정하는 Perl 정규식입니다.
- 세션 기간 - 트랜잭션 추적 세션 기간(초)입니다.

트랜잭션 추적 세션을 시작하고 임계값을 초 단위로 지정하는 구문은 다음과 같습니다.

```
trace transactions exceeding <EXACT MATCH> (second/seconds/sec/secs/s)
in agents matching <REGULAR EXPRESSION> for <EXACT MATCH>
<second/seconds/sec/secs/s>
```

기타 CLW 명령 옵션은 아래의 [명령 옵션](#) (페이지 185)에서 자세히 설명합니다. 트랜잭션 추적 CLW 명령의 예는 [트랜잭션 추적 명령 예제](#) (페이지 188)를 참조하십시오.

트랜잭션 추적 출력 파일 지정

트랜잭션 추적 출력 파일의 이름을 지정할 수 있습니다.

구문

```
Dintroscope.clw.tt.filename=<file name>
```

예

트랜잭션 추적 출력 파일의 파일 이름(전체 경로가 아님)을 지정합니다. 출력 디렉터리를 지정하는 속성과 함께 사용하십시오.

출력

트랜잭션 추적 출력을 지정된 파일에 보냅니다.

명령 옵션

이 단원에서는 트랜잭션 추적 명령 옵션을 설명합니다.

추적 모드

CLW 는 트랜잭션 추적 세션 결과를 캡처하기 위한 두 가지 모드를 지원합니다.

- 동기 모드 - 기본적으로 CLW 는 트랜잭션 이벤트 데이터베이스와 *TransactionTraceData-yyyyMMddhhmmss.xml* 이라는 단일 XML 파일의 세션 끝에 추적 내용을 기록합니다. 여기서 날짜-시간 문자열은 세션의 시작을 나타냅니다.
- 비동기 모드 - 이 모드에서 CLW 는 각 트랜잭션에 대한 추적이 보고되는 즉시 이를 트랜잭션 이벤트 데이터베이스와 *nxxx(sec)-TransactionTraceDatayyyyMMddhhmmss-**<sequence number>**.xml* 이라는 관련 XML 파일에 기록합니다. 여기서 *nxxx* 은 트랜잭션 기간(초)이며 날짜-시간 문자열은 트랜잭션의 시작을 나타냅니다. 사용자 고유의 파일 이름을 지정할 경우 마지막 "." 앞에 시퀀스 번호가 추가됩니다. 지정된 파일 이름에 "."가 없으면 파일 이름의 끝에 시퀀스 번호가 추가됩니다.

동기 모드에서 기록된 결과는 모든 데이터가 단일 파일에 있으므로 쉽게 볼 수 있습니다. 그러나 세션이 종료되기 전에는 데이터를 볼 수 없으며, 고용량 또는 복잡한 트랜잭션의 경우에는 동기 캡처에 상당한 메모리가 소비될 수 있습니다.

트랜잭션 데이터를 비동기적으로 기록하면 메모리가 덜 소비되고, 트랜잭션 추적 세션이 종료되기 전에도 트랜잭션 데이터를 볼 수 있습니다.

`-Dintroscope.clw.tt.mode=(Synch/Asynch)`

트랜잭션 이벤트 데이터베이스에만 출력

이 옵션을 사용하여 트랜잭션 추적을 실행하고 해당 출력을 트랜잭션 이벤트 데이터베이스에만 저장할 수 있습니다(XML 파일 출력 없음). 이 명령은 경고 트리거 시 트랜잭션 추적을 자동으로 시작하는 Introscope 경고에 의해 트리거될 때 유용합니다.

다음과 같이 명령 앞에 *quietly* 라는 단어를 입력하십시오.

`quietly trace transactions exceeding 2 seconds in agents matching "(.*)" for 60 seconds`

헤더 데이터만 반환

경우에 따라서는 CLW 를 통해 대량의 트랜잭션 추적 데이터를 검색할 때 *traces.db* 파일이 무제한 증가하여 CLW 가 반환하는 데 오랜 시간이 걸릴 수 있습니다. 이 속성을 `false` 로 설정하면 Enterprise Manager 에 의해 반환되는 데이터의 양이 감소하므로 문제가 해결됩니다.

이 경우 CLW 는 헤더 추적 데이터만 반환합니다. 기본적으로 또는 이 속성을 `true` 로 설정한 경우 CLW 를 통해 트랜잭션 추적 데이터를 가져오면 헤더와 본문이 모두 반환됩니다.

```
-Dwily.ps.workstation.clws.gettracebody
```

트랜잭션 추적 프로그램 클램프

이제 추적 구성 요소가 5000 개에 도달하면 기본적으로 개별 트랜잭션 추적의 크기가 클램프됩니다. 클램프를 초과하는 트랜잭션 추적은 에이전트에서 무시되고 다음과 같은 경고 메시지가 에이전트 로그 파일에 로깅됩니다.

```
2/23/07 05:33:18 PM PST [WARN] [IntroscopeAgent] Transaction trace component limit of 5000 reached, recording will cease for this transaction.
```

트랜잭션 추적에서 허용되는 최대 구성 요소 수를 변경하려면 다음 에이전트 속성을 변경하십시오.

```
introscope.agent.transactiontrace.componentCountClamp=max_TT_components(기본값: 5000)
```

예를 들어 에이전트 프로필에 다음과 같은 행이 있으면

```
introscope.agent.transactiontrace.componentCountClamp=30000
```

트랜잭션 추적에서 허용되는 최대 구성 요소 수가 30,000 개로 변경됩니다.

경고! 이 클램프 크기가 증가하면 트랜잭션 추적에 필요한 메모리가 더 많아질 수 있으며, 따라서 그에 맞게 JVM 의 최대 힙 크기를 조정해야 할 수 있습니다. 그렇지 않으면 Enterprise Manager 메모리가 부족할 수 있습니다.

트랜잭션 추적 명령 예제

이 단원에서는 트랜잭션 추적 세션을 시작하는 CLW 명령의 예를 제공합니다. 각 예제 명령은 600 초 길이의 세션을 시작합니다. 모든 에이전트에서 5 초보다 오래 걸리는 트랜잭션이 추적됩니다.

참고: 모든 예제 명령은 기본 로그인 설정을 사용하여 Enterprise Manager 에 연결합니다.

트랜잭션 추적 세션을 실행하는 스크립트의 예는 [샘플 스크립트](#) (페이지 201)를 참조하십시오.

기본 옵션 값을 사용하는 트랜잭션 추적

이 CLW 명령은 다음에 대한 기본 설정을 사용하여 트랜잭션 추적 세션을 시작합니다.

- 추적 모드 - 트랜잭션 추적 데이터가 동기적으로 캡처되고 모든 결과가 단일 XML 파일에 기록됩니다.
- 디렉터리 위치 - `-Dintroscope.clw.tt.dirname` 을 지정하지 않으면 추적 결과가 현재 작업 디렉터리에 기록됩니다.

```
java -jar CLWorkstation.jar trace transactions exceeding 5 seconds in agents matching "(.*)" for 600 seconds
```

비동기 캡처를 사용하는 트랜잭션 추적

이 CLW 명령은 세션 출력에 대한 기본 디렉터리 위치를 사용하여 트랜잭션 추적 세션을 시작합니다.

```
java -Dintroscope.clw.tt.mode=Asynch -jar CLWorkstation.jar trace transactions exceeding 5 seconds in agents matching "(.*)" for 600 seconds
```

데이터가 비동기적으로 캡처되고 각 트랜잭션에 대해 별도의 XML 파일이 생성됩니다.

사용자 정의 디렉터리에 기록되는 트랜잭션 추적 결과

이 CLW 명령은 추적 모드에 대한 기본 설정을 사용하여 트랜잭션 추적 세션을 시작합니다. 트랜잭션 추적 데이터는 동기적으로 추적되고 모든 결과가 단일 XML 파일에 기록됩니다.

```
java -Dintroscope.clw.tt.dirname=C:\mytraces -jar CLWorkstation.jar trace transactions exceeding 5 seconds in agents matching "(.*)" for 600 seconds
```

이 명령은 XML 파일에 대해 기본이 아닌 위치(`C:\mytraces` 디렉터리)를 지정합니다.

매개 변수와 오류 필터를 사용하는 트랜잭션 추적

실행할 시간(초)을 지정하고 Workstation 에서 사용할 수 있는 것과 동일한 필터(사용자 ID, URL, URL 쿼리, 세션 ID, 요청 헤더, 요청 매개 변수, 세션 특성 및 오류)를 사용하는 트랜잭션 추적 세션을 시작할 수 있습니다.

사용자 ID, URL, URL 쿼리 또는 세션 ID 에 대한 필터링

```
trace transactions where (userid|url|url query|sessionid) (equals|not
equals|contains|not contains|starts with|ends with) [EXACT MATCH] in agents matching
[REGULAR EXPRESSION] for [EXACT MATCH] (second|seconds|sec|secs|s)
trace transactions where (userid|url|url query|sessionid) (exists|not exists) in
agents matching [REGULAR EXPRESSION] for [EXACT MATCH] (second|seconds|sec|secs|s)
quietly trace transactions where (userid|url|url query|sessionid) (equals|not
equals|contains|not contains|starts with|ends with) [EXACT MATCH] in agents matching
[REGULAR EXPRESSION] for [EXACT MATCH] (second|seconds|sec|secs|s)
quietly trace transactions where (userid|url|url query|sessionid) (exists|not
exists) in agents matching [REGULAR EXPRESSION] for [EXACT MATCH]
(second|seconds|sec|secs|s)
```

요청 헤더, 요청 매개 변수 또는 세션 특성에 대한 필터링

```
trace transactions where (request header|request parameter|session attribute) [EXACT
MATCH] (equals|not equals|contains|not contains|starts with|ends with) [EXACT MATCH]
in agents matching [REGULAR EXPRESSION] for [EXACT MATCH] (second|seconds|sec|secs|s)
trace transactions where (request header|request parameter|session attribute) [EXACT
MATCH] (exists|not exists) in agents matching [REGULAR EXPRESSION] for [EXACT MATCH]
(second|seconds|sec|secs|s)
quietly trace transactions where (request header|request parameter|session
attribute) [EXACT MATCH] (equals|not equals|contains|not contains|starts with|ends
with) [EXACT MATCH] in agents matching [REGULAR EXPRESSION] for [EXACT MATCH]
(second|seconds|sec|secs|s)
quietly trace transactions where (request header|request parameter|session
attribute) [EXACT MATCH] (exists|not exists) in agents matching [REGULAR EXPRESSION]
for [EXACT MATCH] (second|seconds|sec|secs|s)
```

오류에 대한 필터링

```
trace transactions with errors containing [EXACT MATCH] in agents matching [REGEX]
for [EXACT MATCH] (second|seconds|sec|secs|s)
quietly trace transactions with errors containing [EXACT MATCH] in agents matching
[REGEX] for [EXACT MATCH] (second|seconds|sec|secs|s)
```

트랜잭션 이벤트 데이터베이스에서 트랜잭션 추적 쿼리

트랜잭션 추적 결과는 자동으로 트랜잭션 이벤트 데이터베이스에 저장됩니다. 여기에 설명된 CLW 명령을 사용하여 해당 데이터를 검색할 수 있습니다.

<VALUE>과(와) 일치하는 기록 이벤트 가져오기

이 명령은 트랜잭션 이벤트 데이터베이스에서 전체 이벤트 XML 출력 파일을 검색합니다. 전체 이벤트(아래의 요약 이벤트와 반대됨)는 트랜잭션 이벤트 뷰어의 아래쪽 섹션에서 사용할 수 있는 전체 데이터입니다.

```
java -Dintroscope.clw.tt.mode=Asynch -jar CLWorkstation.jar trace transactions get historical events matching "localhost"
```

다음은 출력의 예입니다.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<TransactionTracerSession Duration="78" Version="0.1"
EndDate="2005-06-20T17:40:24.146-08:00" StartDate="2005-06-20T17:40:24.068-08:00"
User="Admin">
<TransactionTrace Domain="SuperDomain" Duration="78" Process="UnknownProcess"
Host="maddelman-dt2" AgentName="Tomcat" StartDate="2005-06-20T17:40:24.068-08:00"
EndDate="2005-06-20T17:40:24.146-08:00">
<CalledComponent RelativeTimestamp="0" Duration="78" ComponentType="Browser"
ComponentName="Browser" MetricPath="Browser">
<CalledComponents>
<CalledComponent RelativeTimestamp="0" Duration="0" ComponentType="JNDI"
ComponentName="ProxyDirContext" MetricPath="JNDI|Context|ProxyDirContext">
<Parameters>
<Parameter Value="lookup" Name="Method"/>
</Parameters>
</CalledComponent>
<CalledComponent RelativeTimestamp="0" Duration="0" ComponentType="JNDI"
ComponentName="ProxyDirContext" MetricPath="JNDI|Context|ProxyDirContext">
<Parameters>
<Parameter Value="lookup" Name="Method"/>
</Parameters>
</CalledComponent>
<CalledComponent RelativeTimestamp="0" Duration="62" ComponentType="Servlets"
ComponentName="HelloWorldExample" MetricPath="Servlets|HelloWorldExample">
<CalledComponents>
<CalledComponent RelativeTimestamp="0" Duration="0" ComponentType="JNDI"
ComponentName="ProxyDirContext" MetricPath="JNDI|Context|ProxyDirContext">
<Parameters>
<Parameter Value="lookup" Name="Method"/>
</Parameters>
</CalledComponent>
```

```

<CalledComponent RelativeTimestamp="0" Duration="0" ComponentType="JNDI"
ComponentName="ProxyDirContext" MetricPath="JNDI|Context|ProxyDirContext">
<Parameters>
<Parameter Value="lookup" Name="Method"/>
</Parameters>
</CalledComponent>
</CalledComponents>
</TransactionTrace>
</TransactionTracerSession>

```

<VALUE>과(와) 일치하는 요약 가져오기

이 명령은 트랜잭션 이벤트 데이터베이스에서 이벤트 요약 XML 만 검색하고 XML 파일을 출력합니다. 이벤트 요약은 트랜잭션 이벤트 뷰어의 위쪽 창에서 사용할 수 있는 정보입니다. 이 명령은 일별로 발생하는 시스템 오류 수에 대한 보고서를 생성하는 등의 목적으로 트랜잭션 이벤트 데이터베이스에서 데이터를 내보낼 때 유용합니다.

get historical event summaries matching [REGULAR EXPRESSION]

다음은 출력의 예입니다.

```

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<TransactionTracerSession Duration="78" Version="0.1"
EndDate="2005-06-20T17:40:24.146-08:00" StartDate="2005-06-20T17:40:24.068-08:00"
User="Admin">
<TransactionTrace Domain="SuperDomain" Duration="78" Process="UnknownProcess"
Host="maddlemann-dt2" AgentName="Tomcat" StartDate="2005-06-20T17:40:24.068-08:00"
EndDate="2005-06-20T17:40:24.146-08:00">
<CalledComponent RelativeTimestamp="0" Duration="78" ComponentType="Browser"
ComponentName="Browser" MetricPath="Browser">
<Parameters>
<Parameter Value="" Name="URL"/>
<Parameter Value="Normal" Name="Trace Type"/>
<Parameter Value="\20050620\17\1119314425302" Name="Trace ID"/>
<Parameter Value="" Name="User ID"/>
</Parameters>
</CalledComponent>
</TransactionTrace>
</TransactionTracerSession>

```

응용 프로그램 심사 맵 명령

심사 맵 경고는 AppMap 및 AppMap 엔터티와 연결된 특수 경고입니다. 심사 맵 경고는 "Triage Map Configurations"(심사 맵 구성) 관리 모듈의 *TriageMapConfigurationsManagementModule.jar* 파일에 있습니다.

다음 명령을 이 관리 모듈에 사용할 수 있습니다.

[관리 모듈 나열](#) (페이지 192)

[관리 모듈의 상태 쿼리](#) (페이지 192)

[심사 맵 경고 나열](#) (페이지 193)

[관리 모듈의 상태 쿼리](#) (페이지 194)

[심사 맵 엔터티 메트릭 그룹 나열](#) (페이지 196)

[심사 맵 엔터티 메트릭 그룹의 상태 쿼리](#) (페이지 197)

관리 모듈 나열

이 명령은 심사 맵 관리 모듈의 이름을 나열합니다.

구문

```
list management modules matching <REGULAR EXPRESSION>
```

예

```
list management modules matching (Triage Map.*)
```

이 명령은 *Triage Map* 으로 시작하는 이름의 관리 모듈을 나열합니다.

출력

각 관리 모듈의 이름과 상태가 나열됩니다. 이 경우 "Triage Map Configurations"(심사 맵 구성) 관리 모듈이 정규식과 일치하며 다음과 같이 나열됩니다.

```
Triage Map Configurations
```

관리 모듈의 상태 쿼리

이 명령은 심사 맵 관리 모듈의 상태를 나열합니다.

구문

```
query state of management modules matching [REGULAR EXPRESSION]
```


예

```
query state of management modules matching (.*)
```

이 명령은 모든 관리 모듈의 이름과 상태를 반환합니다.

출력

사용 중인 시스템에 대해 구성된 각 관리 모듈의 이름과 상태를 나열합니다.

예:

```
Supportability:Active
Trade Application Definitions:Active
Triage Map Configurations:Active
Browser Response Time Adapter:Active
Sample:Active
MOM Infrastructure Monitoring:Active
Reports Unit Tests:Active
Collector - 1:Active
ChangeDetector:Active
CEM BT Stats:Active
```

심사 맵 경고 나열

이 명령은 심사 맵 경고를 나열합니다.

구문

```
list triage map alerts matching [REGULAR EXPRESSION] in management modules
matching [REGULAR EXPRESSION]
```

예

```
list triage map alerts matching (.*) in management modules matching (Triage
Map.*)
```

이 명령은 *Triage Map* 으로 시작하는 이름의 관리 모듈에 있는 심사 맵 경고를 모두 나열합니다.

출력

사용 중인 시스템에 대해 구성된 심사 맵 경고의 이름을 모두 나열합니다.
예:

```

Triage Map Configurations.By Frontend|TradeService|Health:Average Response Time
(ms)_Summary_MetricAlert
Triage Map Configurations.By Business
Service|MedRecBS|loginAdmin.action|loginAdmin.action:Errors Per
Interval_Summary_MetricAlert
Triage Map Configurations.By Frontend|ReportingService|Backend
Calls|WebServices:Average Response Time (ms)_Location_MetricAlert
Triage Map Configurations.By Business
Service|MedRecBS|viewNewlyRegisteredPatients.action|viewNewlyRegisteredPatien
ts.action:Average Response Time (ms)_Location_MetricAlert
Triage Map Configurations.By Frontend|PatientFacadeServiceWebApp|Backend
Calls|localhost:9082/medrec(POINTBASE DB):Alert
Triage Map Configurations.By Frontend|ReportingEngine|Backend
Calls|jdbc%hsqldb%file%report-records:Stall Count_Summary_MetricAlert
Triage Map Configurations.By Business
Service|MedRecBS|viewNewlyRegisteredPatients.action|viewNewlyRegisteredPatien
ts.action:Stall Count_Location_MetricAlert
Triage Map Configurations.Business Service|MedRecBS|Business
Transactions|home.action:Alert
Triage Map Configurations.By Frontend|/medrec|Health:Errors Per
Interval_Location_MetricAlert
Triage Map Configurations.Business Service|Trading Service|Business
Transactions|View Orders:Total Defects Per Interval_Summary_MetricAlert
Triage Map Configurations.By Frontend|AuthenticationService|Health:Errors Per
Interval_Summary_MetricAlert
Triage Map Configurations.By Business Service|Trading Service|Options
Trading|Check Options:Concurrent Invocations_Summary_MetricAlert
Triage Map Configurations.By Business
Service|MedRecBS|index.action|index.action:Stall Count_Location_MetricAlert
Triage Map Configurations.By Business
Service|MedRecBS|index.action|index.action:Concurrent
Invocations_Summary_MetricAlert
Triage Map Configurations.Business Service|MedRecBS|Business
Transactions|viewPatients.action:Total Defects Per
Interval_Summary_MetricAlert
Triage Map Configurations.By Business
Service|MedRecBS|index.action|index.action:Average Response Time
(ms)_Summary_MetricAlert

```

관리 모듈의 상태 쿼리

이 명령은 심사 맵 경고의 상태를 나열합니다.

구문

query state of triage map alerts matching [REGULAR EXPRESSION] in management modules matching [REGULAR EXPRESSION]

예

query state of triage map alerts matching (.) in management modules matching (Triage Map.*)*

이 명령은 *Triage Map* 으로 시작하는 이름의 관리 모듈에 있는 심사 맵 경고와 해당 상태를 모두 나열합니다.

출력

사용 중인 시스템에 대해 구성된 심사 맵 경고의 이름과 상태를 모두 나열합니다. 예:

```
Triage Map Configurations.By Frontend|TradeService|Health:Average Response Time
(ms)_Summary_MetricAlert:Active
Triage Map Configurations.By Business
Service|MedRecBS|loginAdmin.action|loginAdmin.action:Errors Per
Interval_Summary_MetricAlert:Active
Triage Map Configurations.By Frontend|ReportingService|Backend
Calls|WebServices:Average Response Time (ms)_Location_MetricAlert:Active
Triage Map Configurations.By Business
Service|MedRecBS|viewNewlyRegisteredPatients.action|viewNewlyRegisteredPatien
ts.action:Average Response Time (ms)_Location_MetricAlert:Active
Triage Map Configurations.By Frontend|PatientFacadeServiceWebApp|Backend
Calls|//localhost%9082/medrec(POINTBASE DB):Alert:Active
Triage Map Configurations.By Frontend|ReportingEngine|Backend
Calls|jdbc%hsqldb%file%report-records:Stall Count_Summary_MetricAlert:Active
Triage Map Configurations.By Business
Service|MedRecBS|viewNewlyRegisteredPatients.action|viewNewlyRegisteredPatien
ts.action:Stall Count_Location_MetricAlert:Active
Triage Map Configurations.Business Service|MedRecBS|Business
Transactions|home.action:Alert:Active
Triage Map Configurations.By Frontend|/medrec|Health:Errors Per
Interval_Location_MetricAlert:Active
Triage Map Configurations.Business Service|Trading Service|Business
Transactions|View Orders:Total Defects Per Interval_Summary_MetricAlert:Active
Triage Map Configurations.By Frontend|AuthenticationService|Health:Errors Per
Interval_Summary_MetricAlert:Active
Triage Map Configurations.By Business Service|Trading Service|Options
Trading|Check Options:Concurrent Invocations_Summary_MetricAlert:Active
Triage Map Configurations.By Business
Service|MedRecBS|index.action|index.action:Stall
Count_Location_MetricAlert:Active
```

심사 맵 엔터티 메트릭 그룹 나열

이 명령은 심사 맵 엔터티 메트릭 그룹의 이름을 나열합니다.

구문

```
list triage map entity metric groups matching [REGULAR EXPRESSION] in
management modules matching [REGULAR EXPRESSION]
```

예

```
list triage map entity metric groups matching (.*) in management modules
matching (Triage Map .*)
```

이 명령은 *Triage Map* 으로 시작하는 이름의 관리 모듈에 있는 심사 맵 엔터티 그룹을 모두 나열합니다.

출력

사용 중인 시스템에 대해 구성된 심사 맵 엔터티 그룹의 이름과 상태를 모두 나열합니다. 예:

```
Triage Map Configurations.By Frontend|/medrec|Health:Average Response Time
(ms)_Summary
Triage Map Configurations.By Frontend|AuthenticationEngine|Health:Average
Response Time (ms)_Summary
Triage Map Configurations.Business Service|MedRecBS|Business
Transactions|index.action:Total Defects Per Interval_Summary
Triage Map Configurations.By Business Service|Trading Service|View Orders|View
my order:Concurrent Invocations_Location
Triage Map Configurations.By Frontend|PatientFacadeServiceWebApp|Health:Errors
Per Interval_Summary
Triage Map Configurations.By Business Service|Trading Service|Transaction
Summary|Request Transaction Summary:Average Response Time (ms)_Summary
Triage Map Configurations.By Frontend|ReportingEngine|Health:Errors Per
Interval_Summary
Triage Map Configurations.By Business Service|Trading Service|Options
Trading|Check Options:Errors Per Interval_Summary
Triage Map Configurations.By Frontend|AuthenticationEngine|Backend
Calls|jdbc%hsqldb%file%customer-records:Average Response Time (ms)_Summary
Triage Map Configurations.By Frontend|OrderEngine|Health:Average Response Time
(ms)_Location
Triage Map Configurations.Business Service|MedRecBS|Business
Transactions|viewPatients.action:Total Transactions Per Interval_Summary
Triage Map Configurations.By Business Service|Trading Service|Options
Trading|Check Options:Stall Count_Summary
```

심사 맵 엔터티 메트릭 그룹의 상태 쿼리

이 명령은 심사 맵 엔터티 메트릭 그룹의 상태를 나열합니다.

구문

```
query state of triage map entities matching [REGULAR EXPRESSION] in  
management modules matching [REGULAR EXPRESSION]
```

예

```
query state of triage map entities matching (.*) in management modules  
matching (Triage Map .*)
```

이 명령은 *Triage Map* 으로 시작하는 이름의 관리 모듈에 있는 심사 맵 엔터티와 해당 상태를 모두 나열합니다.

출력

사용 중인 시스템에 대해 구성된 심사 맵 엔터티의 이름을 모두 나열합니다.
예:

```
Triage Map Configurations.By Frontend|OrderEngine|Backend Calls:Active
Triage Map Configurations.By Business
Service|MedRecBS|viewRecordSummary.action|kmuernxjnsdfgdfhjwerhgiusadfoiuoherg:Active
Triage Map Configurations.By Frontend|/medrec|Backend Calls|System localhost on port 9082:Active
Triage Map Configurations.By Business
Service|MedRecBS|viewPatient.action|viewPatient.action:Active
Triage Map Configurations.By Frontend|Apache-Axis:Active
Triage Map Configurations.By Business Service|Trading Service:Active
Triage Map Configurations.By Business Service|Trading Service|Balances:Active
Triage Map Configurations.By Frontend|AuthenticationEngine:Active
Triage Map Configurations.By Frontend|AuthenticationService|Backend Calls|WebServices:Active
Triage Map Configurations.By Frontend|AuthenticationService|Health:Active
Triage Map Configurations.By Business
Service|MedRecBS|viewRecordSummary.action:Active
Triage Map Configurations.By Business
Service|MedRecBS|viewNewlyRegisteredPatients.action|kmuernxjnsdfgdfhjwerhgiusadfoiuoherg:Active
Triage Map Configurations.By Business Service|Trading Service|Place Order:Active
Triage Map Configurations.Business Service|Trading Service|Business Transactions|Login:Active
Triage Map Configurations.Business Service|MedRecBS|Business Transactions|index.action:Active
```

Loadbalancing.xml 명령

MOM 은 클러스터 간 에이전트 부하를 분산하고 에이전트가 특정 수집기에 연결할 수 있도록 하기 위해 loadbalancing.xml 파일을 사용합니다. 이러한 명령은 loadbalancing.xml 파일을 업데이트합니다.

Autoprepare Loadbalancing.xml

이 명령은 업그레이드 중 MOM 에서 실행될 수 있습니다. 8.x 및 9.0.x 에이전트에 IntroscopeAgent.profile 에서 정의된 에이전트-수집기 연결이 있는 경우 이 명령을 사용하십시오.

MOM 은 수집기에 직접 연결된 모든 8.x 및 9.0.x 에이전트에 대한 런타임 정보를 수집합니다. MOM 은 loadbalancing.xml 맨 아래에 연결 정보를 채웁니다.

중요! 이 명령은 MOM 과 모든 수집기를 9.1.2 이상으로 업그레이드한 후, 그리고 에이전트를 업그레이드하기 전에 실행하십시오. 에이전트를 업그레이드한 후에 이 명령을 실행하면 MOM 이 이전 에이전트-수집기 연결 정보를 가져올 수 없습니다.

자세한 내용은 *CA APM 설치 및 업그레이드 안내서*를 참조하십시오.

구문

autoprepate loadbalancing.xml

예

autoprepate loadbalancing.xml

에이전트 A, B, C, D, E, F 는 모두 버전 8.x - 9.0.x 까지입니다. 이 에이전트는 다음 표에 표시된 것처럼 수집기 1, 2, 3 에 연결하도록 IntroscopeAgent.profile 파일에 구성되었습니다.

에이전트 이름	수집기 이름
AgentA	Collector01
AgentB	Collector01
AgentC	Collector02
AgentD	Collector02
AgentE	Collector03
AgentF	Collector03

회사는 loadbalancing.xml 을 사용하여 이름이 EAgent2 인 에이전트의 부하를 분산합니다.

모든 버전 8.x 및 9.0.x 에이전트가 실행 중일 때 관리자가 autoprepate loadbalancing.xml CLW 명령을 실행합니다. loadbalancing.xml 파일은 다음 예제에서 굵은 글꼴로 표시된 항목으로 채워집니다.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<loadbalancing xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="loadbalancing0.1.xsd">
  <agent-collector name="Example 1">
    <agent-specifier>.*\|.*\|EPAgent2</agent-specifier>
    <exclude>
      <collector latched="false" port="5001" host="Collector02"/>
    </exclude>
  </agent-collector>
  <agent-collector name="Collector01@5001 auto-generated configuration">
    <agent-specifier>HostName|ProcessName|AgentA</agent-specifier>
    <agent-specifier>HostName|ProcessName|AgentB</agent-specifier>
    <include>
      <collector latched="false" port="5001" host="Collector01"/>
    </include>
  </agent-collector>
  <agent-collector name="Collector02@5001 auto-generated configuration">
    <agent-specifier>HostName|ProcessName|AgentC</agent-specifier>
    <agent-specifier>HostName|ProcessName|AgentD</agent-specifier>
    <include>
      <collector latched="false" port="5001" host="Collector02"/>
    </include>
  </agent-collector>
  <agent-collector name="Collector03@5001 auto-generated configuration">
    <agent-specifier>HostName|ProcessName|AgentE</agent-specifier>
    <agent-specifier>HostName|ProcessName|AgentF</agent-specifier>
    <include>
      <collector latched="false" port="5001" host="Collector03"/>
    </include>
  </agent-collector>
</loadbalancing>
```

예제 1 은 관리자가 명령을 실행하기 전의 loadbalancing.xml 항목입니다.
MOM 은 예제 1 이후에 자동 생성된 항목을 추가했습니다.

출력

Loadbalancing.xml 이 에이전트-수집기 연결 항목으로 업데이트됩니다.

샘플 스크립트

이 단원에는 CLW 명령을 사용하는 다음 샘플 스크립트가 포함되어 있습니다.

- [트랜잭션 추적 세션](#) (페이지 201)
- [경고에 의해 트리거되는 트랜잭션 추적 세션](#) (페이지 205)

이러한 스크립트는

<http://wilycommunity.ca.com/entry.jspa@externalID=2103&categoryID=492.html> 에서 제공되는 다른 스크립트인 *setlscEnv.cmd* 와 *configureWily.cmd* 를 사용합니다. 이 두 가지 스크립트는 CLW 시작, 종료, 다시 시작 및 사용을 지원할 수 있는 *Useful Introscope Scripts*(유용한 Introscope 스크립트)라는 Community Developed Tool(커뮤니티 개발 도구)에 속합니다. 해당하는 ZIP 파일을 다운로드하고 다음 지침에 따라 스크립트를 설치하십시오.

1. 해당하는 *scriptsBin.unix.zip* 또는 *scriptsBin.win.zip* 파일을 Enterprise Manager 설치에 추출합니다. *bin* 하위 디렉터리가 생성됩니다.
2. *bin* 하위 디렉터리로 이동하고 다음을 호출합니다.

```
.\configureScriptsEnv.cmd
```

 또는

```
./configureScriptsEnv.sh
```
3. 그러면 *setlscEnv.cmd* 또는 *setlscEnv.sh* 파일이 생성됩니다. 이 파일에는 다른 스크립트가 읽는 관련 Introscope 폴더 위치가 모두 포함되어 있습니다.

트랜잭션 추적 세션

이 스크립트는 모든 에이전트에 대한 트랜잭션 추적 세션을 시작합니다. 런타임에 다음 두 가지 인수를 제공해야 합니다.

- 실행 임계값 - 추적할 트랜잭션의 최소 실행 시간(초)입니다.
- 세션 기간 - 트랜잭션 추적 세션 기간(초)입니다.

스크립트 결과는 날짜 지향 디렉터리 구조에 저장됩니다.

이름

clwTxnTracer

구문

```
clwTxnTracer <threshold> <duration>
```

다음은 각 요소에 대한 설명입니다.

threshold 는 트랜잭션 실행 시간 임계값(초)입니다.

duration 은 세션 기간(초)입니다.

예

```
clwTxnTracer 1 600
```

실행 시간이 1 초보다 오래 걸리는 트랜잭션에 대해 기간이 600 초인 트랜잭션 추적 세션이 실행되도록 합니다.

결과

트랜잭션 추적 데이터가 다음과 같이 현재 날짜에 해당하는 디렉터리의 단일 파일에 기록됩니다.

```
<EM_Home>/traces\<year>\<month>\<day>\<agents>_<threshold>secs_for<duration>secs.<start_time>.xml
```

예:

```
C:\introscope\traces\2004\11\11\AllAgents_1secs_for600secs.14091705.xml
```

```
@ECHO OFF  
SETLOCAL
```

```
TITLE Introscope -- Transaction Tracer Session
```

```
REM ****
```

```
REM Sets the current working directory with quotes around it  
REM This enables this file to execute correctly if it is  
REM invoked somewhere other than its location.
```

```
REM ****
```

```
FOR /f "tokens=1 delims=" %%a in ('cd') DO SET PWD=%%a
```

```
REM ****
REM Set the command directory to the command argument itself,
REM namely the full path of this file or the relative path
REM to where the file was invoked.
SET CMD_DIR=%0
REM Now simply strip out the name of this file to get dir
REM !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
REM      Use current filename
SET CMD_DIR=%CMD_DIR:clwTxnTracer.cmd=%
REM !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
REM Strip the quotes
REM add quotes if they're not there
SET CMD_DIR="%CMD_DIR%"
REM if not add quotes, then this statement chokes
SET CMD_DIR=%CMD_DIR:="=%
REM if the current dir wasn't determined, just set it to working dir
IF NOT EXIST "%CMD_DIR%" SET CMD_DIR=.
IF "%CMD_DIR%" == %0 SET CMD_DIR=.
IF "%CMD_DIR%" == "%0" SET CMD_DIR=.

REM ****
REM Now set the home directory for Introscope, and others
IF NOT EXIST "%CMD_DIR%\setIscEnv.cmd" goto noSetEnvFile
call "%CMD_DIR%\setIscEnv.cmd"

SET TT_THRESHOLD_IN_SECS=%1
SET TT_DURATION_IN_SECS=%2
IF "X%TT_THRESHOLD_IN_SECS%" == "X" SET TT_THRESHOLD_IN_SECS=10000
IF "X%TT_DURATION_IN_SECS%" == "X" SET TT_DURATION_IN_SECS=600
IF %TT_THRESHOLD_IN_SECS% LEQ 0 GOTO badArg
IF %TT_DURATION_IN_SECS% LEQ 0 GOTO badArg
SET TT_AGENTS=(.*)

REM Java Settings (e.g. increase Max heap size )
SET JAVA_OPTS=-Xms64m -Xmx512m
SET
JAVA_OPTS=%JAVA_OPTS% %CLW_USER_OPT% %CLW_PASSWORD_OPT% %CLW_EM_HOST_OPT% %CLW_EM
_PORT_OPT%
```

```
SET COMMAND=trace transactions exceeding %TT_THRESHOLD_IN_SECS% seconds in agents
matching \"%TT_AGENTS%\" for %TT_DURATION_IN_SECS% seconds
```

```
SET AGENT_STR=%TT_AGENTS%
REM Remove the spaces, parentheses
SET AGENT_STR=%AGENT_STR:(=%
SET AGENT_STR=%AGENT_STR:)=%
SET AGENT_STR=%AGENT_STR:=%
if \"%TT_AGENTS%\" == \"X(.*)\" SET AGENT_STR=AllAgents
FOR /f \"tokens=1-4 delims=:.\" %%a in (%time%) DO SET SECS_STR=%%a%%b%%c%%d
FOR /f \"tokens=1-4 delims=/\" %%a in (%date%) DO SET
TRACES_DIR=%ISC_TRACES%\%%d%\%%b%\%%c
```

```
REM Create the traces dir, if not exist
IF NOT EXIST \"%TRACES_DIR%\" MKDIR \"%TRACES_DIR%\"
SET
TT_FILE=%TRACES_DIR%\%AGENT_STR%\%TT_THRESHOLD_IN_SECS%secs_for%TT_DURATION_IN_SE
CS%secs.%SECS_STR%.xml
```

```
TITLE Introscope -- Transaction Tracer for %TT_DURATION_IN_SECS% secs with
threshold %TT_THRESHOLD_IN_SECS% secs
REM send stderr to null b/c there are meaningless disconnect excepts that might be
*scary-looking*
ECHO Saving session output to %TT_FILE%
\"%ISC_JAVA_HOME%\bin\java\" %JAVA_OPTS% -jar \"%CLW_JAR%\" %COMMAND% > \"%TT_FILE%\"
2>NUL
goto finish
```

```
:badArg
ECHO Arguments should be greater than zero.
ECHO Syntax: $0 \"threshold in secs\" \"duration in secs\"
goto finish
```

```
:noSetEnvFile
ECHO There is no environment setup file: setIscEnv.cmd
ECHO Please re-run configureWily.cmd in installation directory!
goto finish
```

```
:finish
ENDLOCAL
```

경고에 의해 트리거되는 트랜잭션 추적 세션

이 스크립트는 트리거 중인 경고의 결과로 트랜잭션 추적 세션을 시작합니다. 경고 메시지 텍스트를 인수로 전달하면서 셸 명령 작업을 사용하여 호출해야 합니다.

스크립트는 경고를 트리거한 데이터를 보고한 에이전트에 대한 경고 메시지 텍스트와 초과된 위험 수준 값을 구문 분석합니다. 이때 초과된 위험 수준 값은 트랜잭션 추적 세션에 대한 에이전트 값 및 임계값으로 사용됩니다. 세션 결과는 날짜 지향 디렉터리 구조에 저장됩니다.

이름

`alert2TxnTracer`

구문

셸 명령 작업 생성에 대한 자세한 내용은 *CA APM Workstation 사용자 안내서*를 참조하십시오.

결과

트랜잭션 추적 데이터가 다음과 같이 현재 날짜에 해당하는 디렉터리의 단일 파일에 기록됩니다.

```
<EM_Home>/traces\<year>\<month>\<day>\<agents>
_<threshold>secs_for<duration>secs.<start_time>.xml
```

예:

```
C:\introscope\traces\2004\11\11\AllAgents_1secs_for600secs.14091705.xml
```


제 10 장: WatchDog 명령줄 도구 사용

신뢰성과 보안 유지를 위해 별도의 WatchDog 프로세스를 통해 Enterprise Manager 서버를 시작하고 모니터링할 수 있습니다. 크로스 플랫폼 WatchDog 명령줄 도구를 사용하여 장애가 발생한 Enterprise Manager 서버를 시작, 중지, 관리 및 다시 시작할 수 있습니다.

이 섹션은 다음 항목을 포함하고 있습니다.

- [WatchDog 정보](#) (페이지 207)
- [WatchDog 실행](#) (페이지 208)
- [WatchDog 명령](#) (페이지 210)
- [WatchDog 명령 옵션](#) (페이지 214)
- [WatchDog 로그 파일 보기](#) (페이지 219)
- [샘플 스크립트](#) (페이지 219)

WatchDog 정보

WatchDog 는 Enterprise Manager 프로세스를 시작, 중지 및 관리하는 크로스 플랫폼 명령줄 도구입니다. 이 도구는 기존 Enterprise Manager 장애 조치 기능을 지원하여 장애가 발생한 Enterprise Manager 를 다시 시작할 수도 있습니다.

WatchDog 명령줄 도구는 `<EM_Home>/bin` 디렉터리에 상주합니다. 다음 방법 중 하나로 명령을 호출할 수 있습니다.

- `WatchDog.bat` 또는 `WatchDog.sh` 도우미 사용
- `WatchDog.jar` 에서 직접 Java 응용 프로그램 실행. 이 방법의 경우 더 많은 옵션을 지정할 수 있지만 더 복잡하기도 합니다. 예를 들어 WatchDog 프로세스가 `watch` 모드인 상태로 Enterprise Manager 를 시작하려면 `bin` 디렉터리에서 `WatchDog watch` 를 입력하십시오.

참고: WatchDog 를 사용하려면 JRE 1.6 이 있어야 합니다.

모든 WatchDog 명령은 결과 코드와 함께 제어권을 명령 창이나 셸에 다시 반환합니다. WatchDog 는 실제로 다음 두 프로그램으로 구성되어 있습니다.

- **WatchDog 관리자**

명령줄에서 줄을 받아들이고 다양한 작업을 수행한 다음 결과를 반환합니다.

- **WatchDog 서버 프로세스**

Enterprise Manager 의 건전성을 모니터링하고 중지된 Enterprise Manager 를 자동으로 다시 시작합니다.

참고: 사용자가 WatchDog 이외의 메커니즘으로 Enterprise Manager 를 시작할 수 있으므로 Enterprise Manager 가 시작되고 있는지 여부를 *start* 명령이 항상 알 수 있는 것은 아닙니다. 따라서 WatchDog 는 Enterprise Manager 가 WatchDog 모르게 시작된 직후에 호출된 경우 두 번째 Enterprise Manager 인스턴스를 시작하려고 시도합니다. 실행된 명령이 *start* 뿐이므로 Enterprise Manager 를 시작하려는 두 번째 시도는 실패하고 오류 결과가 반환되지 않습니다. <EM_Home>/logs 에 있는 Enterprise Manager 로그 파일에 오류가 로깅됩니다.

결국 첫 번째 WatchDog *start* 명령 시도가 성공하고 *running* 명령이 반환됩니다.

WatchDog 실행

Windows 명령 프롬프트나 UNIX 셸을 사용하여 WatchDog 결과 코드를 볼 수 있습니다.

WatchDog.bat 또는 WatchDog.sh 를 사용하여 WatchDog 를 실행하려면

1. Windows 명령 프롬프트나 UNIX 셸을 엽니다.
2. <EM_Home>\bin(Windows 의 경우) 또는 <EM_Home>/bin(UNIX 의 경우)으로 이동합니다.
3. *WatchDog <command>*를 입력합니다. 여기서 <command>는 *start*, *watch*, *stop*, *status* 또는 *help* 입니다. 명령에 대한 자세한 내용은 [WatchDog 명령](#) (페이지 151)을 참조하십시오.

WatchDog.jar 를 직접 호출하여 WatchDog 를 실행하려면

1. Windows 명령 프롬프트나 UNIX 셸을 엽니다.
2. `<EM_Home>\bin`(Windows 의 경우) 또는 `<EM_Home>/bin`(UNIX 의 경우)으로 이동합니다.
3. 사용 중인 운영 체제에 따라 다음 명령을 입력합니다.
 - Windows:
`..\jre\bin\java -jar WatchDog.jar command [-options]`
 - UNIX:
`../jre/bin/java -jar WatchDog.jar command [-options]`

명령에 대한 자세한 내용은 [WatchDog 명령](#) (페이지 151)을 참조하십시오.

SAP 에서 WatchDog 실행

SAP 환경에서 실행 중인 Enterprise Manager 에서 WatchDog 을 사용하는 경우에는 관리자 자격 증명을 입력해야 WatchDog 을 사용할 수 있습니다.

SAP 환경에서 Enterprise Manager 에 대해 WatchDog 명령을 실행하려면

- Enterprise Manager 관리자의 사용자 ID 와 암호를 제공하여 계속합니다.

WatchDog 명령

WatchDog 명령은 다음과 같은 네 가지 기본 기능에 해당합니다.

- Enterprise Manager 프로세스의 시작 및 재시작([WatchDog start 명령](#) (페이지 211) 참조)
- Enterprise Manager 프로세스 중지([WatchDog stop 명령](#) (페이지 212) 참조)
- Enterprise Manager 상태 확인([WatchDog status 명령](#) (페이지 213) 참조)

명령을 입력할 때는 두 가지 구문 중 하나를 사용합니다.

- 기본 - *WatchDog.bat*(Windows 의 경우) 또는 *WatchDog.sh*(UNIX 도우미 스크립트의 경우) 중 하나를 사용하여 간단하게 명령을 입력할 수 있습니다.
- 전체 - *WatchDog.jar* Java 응용 프로그램을 직접 호출하며, 모든 WatchDog 옵션에 사용할 수 있습니다.

WatchDog 은 명령줄에서 `java -jar WatchDog.jar 명령[-options]`을 사용하여 제어됩니다.

모든 명령은 다음 두 가지 결과 코드를 반환합니다.

- Enterprise Manager 에 대한 결과 코드
- WatchDog 의 자동 재시작 기능에 대한 결과 코드

WatchDog 결과 코드 앞에는 *wd* 가 추가됩니다.

WatchDog start 명령

start 명령은 Enterprise Manager 프로세스를 시작하지만 기존 명령에 의존하여 Enterprise Manager 프로세스를 실행합니다.

WatchDog 기능을 자동으로 다시 시작하면서 WatchDog 을 사용하거나 기본 구문을 사용하여 Enterprise Manager 를 시작할 수 있습니다. 기본 구문을 사용하는 경우 *Introscope Enterprise Manager.exe*(Windows) 또는 *Introscope_Enterprise_Manager*(UNIX)가 기본적으로 적용되므로 *start* 명령을 지정하지 않아도 됩니다. *watch* 명령을 사용하면 WatchDog 서버가 *감시* 모드로 전환되는데, 이 모드에서는 WatchDog 서버가 주기적으로 Enterprise Manager 의 실행이 중지되었는지 확인하고 필요한 경우 Enterprise Manager 를 다시 시작합니다.

전체 구문을 사용하여 *start* 명령과 함께 *-watch* 명령 옵션을 입력하십시오. 그러면 WatchDog 이 *감시* 모드로 전환됩니다.

참고: WatchDog 은 다른 것을 기다리지 않고 결과를 반환하는 비동기 프로세스이므로 *start* 또는 *stop* 명령을 입력한 후에 가능한 결과는 *startcommandissued* 와 *stopcommandissued* 뿐입니다. 이러한 결과는 명령이 실행되었음을 의미할 뿐 Enterprise Manager 가 실제로 시작 또는 중지되었음을 의미하지는 않습니다. 보다 정확한 내용을 확인하려면 Enterprise Manager 로그를 확인하거나 운영 체제 프로세스를 확인하십시오.

start 명령 구문

이 단원에서는 WatchDog start 명령 구문을 제공합니다.

기본 구문

WatchDog start

WatchDog watch

전체 구문

```
..\jre\bin\java -jar WatchDog.jar start -startcmd <cmd>
```

```
..\jre\bin\java -jar WatchDog.jar start -watch -startcmd <cmd>
```

Enterprise Manager 반환 값

startcommandissued - Enterprise Manager 가 실행되고 있지 않습니다.

alreadyrunning - Enterprise Manager 가 이미 실행되고 있습니다.

starting - Enterprise Manager 가 시작되고 있습니다.

startererror - Enterprise Manager 를 시작하려고 할 때 오류가 발생했습니다.

WatchDog 반환 값

wdstartedwatching - WatchDog 이 감시 모드로 전환되었습니다.

wdalreadywatching - WatchDog 이 이미 실행되고 있습니다.

wdstartedsleeping - WatchDog 서버 프로세스가 실행되고 있지만 감시 모드가 아닙니다.

wdalreadysleeping - WatchDog 이 이미 대기 모드입니다.

WatchDog stop 명령

WatchDog stop 명령은 Enterprise Manager 와 WatchDog 의 서버 프로세스에 대해 stop 명령을 실행합니다. WatchDog 이 감시모드로 실행되고 있을 수 있으므로 이 명령은 Enterprise Manager 를 중지하고 중지된 상태로 유지하는 가장 좋은 방법입니다.

stop 명령 구문

이 단원에서는 WatchDog stop 명령 구문을 제공합니다.

기본 구문

```
WatchDog stop
```

전체 구문

```
..\jre\bin\java -jar WatchDog.jar stop
```

Enterprise Manager 반환 값

- stopcommandissued* - Enterprise Manager 가 실행되고 있습니다.
- alreadystopped* - Enterprise Manager 가 실행되고 있지 않습니다.
- stoperror* - Enterprise Manager 를 중지하려고 할 때 오류가 발생했습니다.

WatchDog 반환 값

- wdstopped* - WatchDog 이 중지되었습니다.
- wdstopcommandissued* - WatchDog 이 실행되고 있습니다.

WatchDog status 명령

status 명령은 Enterprise Manager 와 WatchDog 의 상태를 보고합니다.

status 명령 구문

이 단원에서는 WatchDog status 명령 구문을 제공합니다.

기본 구문

```
WatchDog status
```

전체 구문

```
..\jre\bin\java -jar WatchDog.jar status
```

Enterprise Manager 반환 값

- running* - Enterprise Manager 가 실행되고 있습니다.
- stopped* - Enterprise Manager 가 실행되고 있지 않습니다.
- starting* - Enterprise Manager 가 시작되고 있습니다.
- statusunknown* - Enterprise Manager 의 상태를 알 수 없습니다.

WatchDog 반환 값

wdwatching - WatchDog 이 실행되고 있습니다.

wdsleeping - WatchDog 이 Enterprise Manager 를 시작할 때와 마찬가지로 WatchDog 서버 프로세스가 실행되고 있지만 감시 모드가 아닙니다.

wdstopped - WatchDog 이 실행되고 있지 않습니다.

WatchDog 명령 옵션

WatchDog 은 기본 구문에서는 사용할 수 없는 고급 옵션을 제공합니다. 기본 구문을 사용하는 경우에는 해당 옵션의 기본값이 사용된다고 가정합니다.

명령 옵션은 *start* 명령에만 적용되지만, 모든 명령에 사용할 수 있는 *-port* 명령 옵션은 예외로 합니다.

명령 옵션에는 다음이 포함됩니다.

- [WatchDog -watch 명령 옵션](#) (페이지 214)
- [WatchDog -port 명령 옵션](#) (페이지 215)
- [WatchDog -startcmd 명령 옵션](#) (페이지 216)
- [WatchDog -interval 명령 옵션](#) (페이지 216)
- [WatchDog -startuptime 명령 옵션](#) (페이지 217)
- [WatchDog -jre 명령 옵션](#) (페이지 217)

WatchDog -watch 명령 옵션

-watch 명령 옵션은 *start* 명령에만 사용할 수 있습니다([WatchDog start 명령](#) (페이지 211) 참조). Enterprise Manager 에서 자동 재시작 기능이 사용되도록 설정하는 방법은 이 명령 옵션뿐입니다.

Enterprise Manager 가 시작된 후에 *watch* 기능을 켜거나 끌 수 있습니다. 예를 들어 WatchDog 이 감시모드가 아닌 상태로 Enterprise Manager 가 실행되고 있는 경우 *-watch* 옵션이 있는 *start* 명령을 사용하여 WatchDog 서버를 감시모드로 전환할 수 있습니다. 마찬가지로 Enterprise Manager 가 이미 실행되고 있더라도 *-watch* 옵션 없이 *start* 명령을 실행하여 WatchDog 을 감시모드에서 해제할 수 있습니다.

`start` 명령에 `-watch` 옵션을 사용하면 다음 값이 반환됩니다.

- `startedwatching` - 명령을 입력하기 전에 WatchDog 이 감시 모드에 있지 않습니다. 이제 모니터링합니다.
- `alreadywatching` - 명령을 입력하기 전에 WatchDog 이 이미 감시 모드에 있었습니다. 계속해서 모니터링합니다.

`start` 명령에 `-watch` 옵션을 사용하지 않으면 다음 값이 반환됩니다.

- `startedsleeping` - 명령을 입력하기 전에 WatchDog 이 대기하고 있지 않았습니니다. 모니터링이 중지되었습니다.
- `alreadysleeping` - 명령을 입력하기 전에 WatchDog 이 이미 대기하고 있었습니다. 계속해서 모니터링을 억제합니다.

-watch 명령 옵션 예제:

```
<EM_Home>\bin>..\jre\bin\java -jar WatchDog.jar start -watch -startcmd
"..\Introscope Enterprise Manager.exe"
WatchMgr: iPort = 4321; watch = true; startcmd = ..\Introscope Enterprise Manager.exe;
startcommandissued & wdstartedwatching
```

WatchDog -port 명령 옵션

`-port` 옵션을 사용하여 WatchDog 의 서버 포트 값을 지정할 수 있습니다. 값을 입력하지 않으면 기본값인 4321 이 사용됩니다.

첫 번째 WatchDog `start` 명령에 대해 `-port` 값을 지정하면 이후의 모든 명령에 동일한 값이 사용됩니다.

참고: 또는 `WatchDog.bat` 파일을 수정하거나 새 배치 파일을 만들어 기본이 아닌 포트에서 WatchDog 서버를 실행할 수 있습니다. 그러면 올바른 포트가 모든 명령과 함께 WatchDog 관리자에게 전달됩니다.

-port 명령 옵션 예제:

```
<EM_Home>\bin>..\jre\bin\java -jar WatchDog.jar
start -port 5555 -startcmd "..\Introscope Enterprise Manager.exe"
WatchMgr: iPort = 5555; watch = false; startcmd = ..\Introscope Enterprise
Manager.exe;
alreadyrunning & wdalreadysleeping
```

WatchDog -startcmd 명령 옵션

이 옵션을 사용하여 Enterprise Manager 를 시작하는 명령을 지정할 수 있습니다.

참고: 이 명령 옵션은 *start* 명령에만 적용됩니다. 자세한 내용은 [WatchDog start 명령](#) (페이지 211)을 참조하십시오.

WatchDog -interval 명령 옵션

interval 옵션을 사용하여 Enterprise Manager 가 중지되었는지 확인하기 위한 Enterprise Manager 상태 확인이 발생하는 시간(초)을 지정할 수 있습니다. 이 옵션을 지정하지 않은 경우에 사용되는 기본값은 10 초입니다.

이 옵션은 WatchDog 의 상태가 *watching* 일 때 적용됩니다.

참고: 이 명령 옵션은 *start* 명령에만 적용됩니다. 자세한 내용은 [WatchDog start 명령](#) (페이지 211)을 참조하십시오.

-interval command 옵션 예제:

```
C:\Program Files\CA Wily\Introscope9.0d140\bin>..\jre\bin\java -jar WatchDog.jar
start -watch -interval 300 -startcmd "..\Introscope Enterprise Manager.exe"
WatchMgr: iPort = 4321; watch = true; startcmd = ..\Introscope Enterprise Manager.exe;
startcommandissued & wdstartedwatching
```


WatchDog -startuptime 명령 옵션

이 옵션을 사용하여 WatchDog 이 Enterprise Manager 시작을 허용하는 시간(초)을 지정할 수 있습니다. WatchDog 이 Enterprise Manager 를 시작한 후 이 옵션에 대해 지정된 시간이 지나면 Enterprise Manager 의 상태가 *starting* 으로 변경됩니다. 그 다음부터는 Enterprise Manager 상태를 확인하도록 구성된 정상 메커니즘이 적용됩니다.

Enterprise Manager 상태 확인은 Enterprise Manager 시작 직후에 수행되므로 *running* 상태를 제공하지 않습니다. 대신에 WatchDog 의 *status* 명령은 WatchDog 이 Enterprise Manager 를 시작한 후 몇 초 동안 *starting* 상태를 반환합니다. 이 기능은 WatchDog 이 실수로 두 개의 Enterprise Manager 인스턴스를 시작하지 못하게 합니다.

-*startuptime* 옵션을 사용하여 이 지연을 기본값(30 초) 이외의 다른 값으로 구성할 수 있습니다.

참고: 이 명령 옵션은 *start* 명령에만 적용됩니다. 자세한 내용은 [WatchDog start 명령](#) (페이지 211)을 참조하십시오.

-startuptime 명령 옵션 예제:

```
<EM_Home>\bin>..\jre\bin\java -jar WatchDog.jar start -watch -startuptime 60
-startcmd "..\Introscope Enterprise Manager.exe"
WatchMgr: iPort = 4321; watch = true; startcmd = ..\Introscope Enterprise Manager.exe;
startcommandissued & wdstartedwatching
```

WatchDog -jre 명령 옵션

JRE 가 기본 디렉터리인 *jre/bin/java* 에 없는 경우 이 옵션을 사용하여 JRE 경로를 지정할 수 있습니다.

-jre 명령 옵션 예제:

```
C:\Program Files\Java\jre1.6.0_07\bin\java" -jar WatchDog.jar start -watch -jre
"C:\Program Files\Java\jre1.6.0_07\bin\java" -startcmd "..\Introscope Enterprise
Manager.exe"
startcommandissued & wdstartedwatching
```

WatchDog -emport 명령 옵션

Enterprise Manager 가 기본 포트 5001 이외의 다른 포트 번호에서 실행되고 있는 경우 *-emport* 옵션을 사용하여 Enterprise Manager 의 서버 포트 값을 지정할 수 있습니다. 이 명령은 Enterprise Manager 가 기본 포트 5001 이외의 다른 포트 번호에서 실행되고 있을 때 필요합니다.

-emport 명령 옵션 예제:

```
C:\Program Files\CA Wily\Introscope9.0\bin>..\jre\bin\java -jar WatchDog.jar
start -emport 5003 -startcmd "..\Introscope Enterprise Manager.exe"
WatchMgr: iPort = 5555; watch = false; startcmd = ..\Introscope Enterprise
Manager.exe;
alreadyrunning & wdalreadysleeping
```

WatchDog -emuser 명령 옵션

Enterprise Manager 가 기본값인 *Admin* 이 아닌 사용자 이름으로 구성된 경우 *-emuser* 옵션을 사용하십시오.

이 명령은 Enterprise Manager 가 기본값인 *Admin* 이 아닌 사용자 이름으로 구성된 경우 필요합니다.

또한 *-empwd* 옵션과 함께 *-emuser* 옵션을 사용하십시오.

-emuser 명령 옵션 예제:

```
<EM_Home>\bin>..\jre\bin\java -jar WatchDog.jar
start -emuser EMUserName -empwd EMPassWord -startcmd "..\Introscope Enterprise
Manager.exe"
WatchMgr: iPort = 5555; watch = false; startcmd = ..\Introscope Enterprise
Manager.exe;
alreadyrunning & wdalreadysleeping
```

WatchDog -empwd 명령 옵션

Enterprise Manager 가 기본값인 ""이 아닌 암호로 구성된 경우 **-empwd** 옵션을 사용하십시오.

이 명령은 Enterprise Manager 가 기본값인 ""이 아닌 암호로 구성된 경우 필요합니다.

또한 **-emuser** 옵션과 함께 **-empwd** 옵션을 사용하십시오.

-empwd 명령 옵션 예제:

```
<EM_Home>\bin>..\jre\bin\java -jar WatchDog.jar
  start -emuser EMUserName -empwd EMPassWord -startcmd "..\Introscope Enterprise
  Manager.exe"
WatchMgr: iPort = 5555; watch = false; startcmd = ..\Introscope Enterprise
  Manager.exe;
alreadyrunning & wdaIreadySleeping
```

WatchDog 로그 파일 보기

WatchDogServer 프로세스 로그 파일은 *WatchDog.log* 파일에 기록됩니다.

WatchDog 로그 파일을 보려면

1. <EM_Home>/logs 로 이동합니다.
2. *WatchDog.log* 파일을 엽니다.

샘플 스크립트

WatchDog.bat 와 *WatchDog.sh* 는 Windows 및 UNIX 플랫폼에 대한 기본 구문을 구현합니다. 이러한 스크립트는 WatchDog 의 전체 구문을 단순화하는 사용자 지정 스크립트를 개발하기 위한 시작 지점으로도 유용합니다. Windows 및 UNIX 설치의 <EM_Home>/bin 디렉터리에 있는 *WatchDog.bat* 와 *WatchDog.sh* 를 사용하십시오.

제 11 장: WebView 옵션 구성

이 섹션은 다음 항목을 포함하고 있습니다.

[WebView 응용 프로그램 컨텍스트 경로 구성](#) (페이지 221)

[APM WebView 성능을 구성하고 모니터링하는 방법](#) (페이지 222)

WebView 응용 프로그램 컨텍스트 경로 구성

선택적으로 WebView 설치에 대한 응용 프로그램 컨텍스트 경로를 구성할 수 있습니다. 이 경로는 WebView의 정규화된 호스트 이름과 포트 번호에 추가되어 WebView에 액세스하기 위한 URL을 형성합니다. 이 기능을 통해 사용자가 WebView에 대한 "응용 프로그램 이름"을 정의할 수 있습니다.

컨텍스트 경로 없이 WebView에 액세스하려면

- 다음 URL을 사용하십시오.

`http://<Server_name>:<Port_number>`

컨텍스트 경로가 구성된 경우 WebView에 액세스하려면

- 다음 URL을 사용하십시오.

`http://<Server_name>:<Port_number>/<Context_path>/`

예를 들어 `Context_path`는 `webview`로 정의되어 있고

`introscope.webview.tcp.port` 속성은 기본값인 `8080`으로 설정되어 있는 경우 다음 URL을 사용하여 WebView에 액세스하십시오.

`http://<Server_name>:8080/webview/`

WebView 속성 파일에서 `introscope.webview.context.path` 속성을 사용하여 WebView 컨텍스트 경로를 구성합니다. 자세한 내용은 [introscope.webview.context.path](#) (페이지 547)를 참조하십시오. 컨텍스트 경로 속성을 정의한 후 WebView를 다시 시작하십시오.

APM WebView 성능을 구성하고 모니터링하는 방법

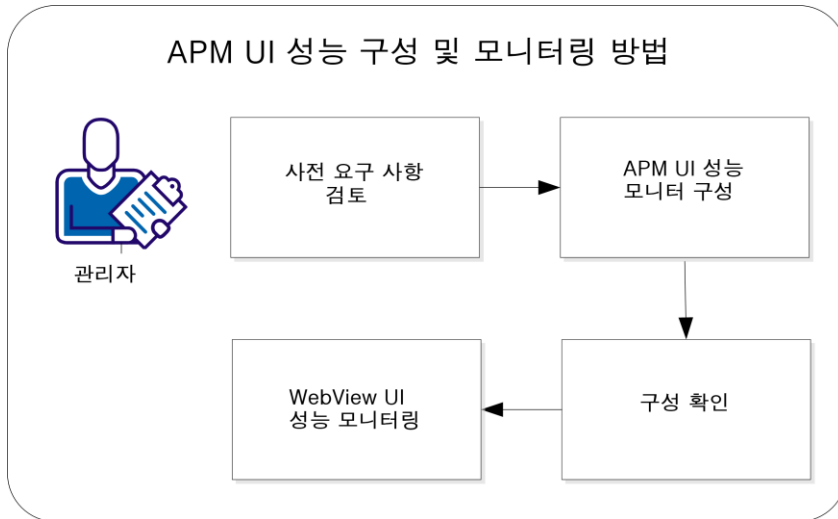
참고: SAP WebView 사용자는 APM UI 성능 모니터를 사용할 수 없습니다.

APM UI 성능 모니터는 WebView 응용 프로그램에 대한 성능 메트릭을 수집하고 보고합니다. 관리자는 이 정보를 사용하여 사용자에게 영향을 주기 전에 잠재적인 WebView 성능 문제점을 찾아 수정할 수 있습니다. 예를 들어 사용 중인 하드웨어 리소스가 부족하거나 사용 중인 동시 세션이 너무 많은 경우 성능 문제가 발생할 수 있는데, 특히 많은 데이터 뷰가 실행될 때 그렇습니다.

WebView 서버를 설치하면 Java Agent 가 배포됩니다. 사용하도록 설정한 경우 포함된 Java Agent 가 서버 구성 요소와 하드웨어 리소스를 모니터링하고 수집된 메트릭이 Enterprise Manager 에 보고됩니다. 그러면 Enterprise Manager 는 실시간 보고 및 기록 보고용으로 데이터를 처리하고 저장합니다. 수집된 데이터는 WebView 의 다음 샘플 대시보드에 나타납니다.

- [WebView - Overview\(WebView - 개요\)](#) (페이지 227)
- [WebView - Maps and Widgets\(WebView - 맵 및 위젯\)](#) (페이지 228)
- [WebView - Resources\(WebView - 리소스\)](#) (페이지 228)

다음 그림에서는 관리자가 APM UI 성능 모니터를 구성하고 사용하는 방법에 대해 설명합니다.



- [필수 구성 요소 검토](#) (페이지 223)
- [APM UI 성능 모니터 구성](#) (페이지 224)
- [구성 확인](#) (페이지 225)
- [WebView UI 성능 모니터링](#) (페이지 226)
- (선택 사항) [WebView 메트릭 그룹화 구성](#) (페이지 229)
- (선택 사항) [대시보드 데이터 보기 및 해석](#) (페이지 230)

필수 구성 요소 검토

필수 구성 요소는 다음과 같습니다.

1. 구성을 위해 다음 구성 요소와 해당 디렉터리 및 파일이 존재하는지 확인합니다.
 - Java Agent
`<WEBVIEW_HOME>/products/webview/agent`
 - 에이전트 작업, 메트릭 데이터 수집 및 계측 프로세스를 제어하기 위한 WebView Probuilder 지시문 파일(`WebView.pbd`)
`<WEBVIEW_HOME>/products/webview/agent/wily/core/config`
 2. 다음과 같이 Java Agent 에 대해 `IntroscopeAgent.profile` 파일을 구성합니다.
 - a. `<INSTALL_HOME>/product/webview/agent/wily/core/config` 로 이동하고 `IntroscopeAgent.profile` 을 텍스트 편집기로 엽니다.
 - b. `introscope.autoprobe.directivesFile` 을 검색하고 `WebView.pbd` 가 속성 값의 끝에 추가되었는지 확인합니다.
 - c. `introscope.agent.defaultProcessName` 을 검색하고 속성 값이 `APM WebView` 인지 확인합니다. 이 값을 변경하거나 제거하지 마십시오.
 - d. `introscope.agent.agentName` 을 검색하고 속성 값이 `APM WebView` 인지 확인합니다.
- 구성이 설정되었습니다.

APM UI 성능 모니터 구성

Java Agent 의 APM UI 성능 모니터 구성 요소를 구성할 수 있습니다. 다음 두 설치 옵션 중 하나를 사용하십시오.

- Enterprise Manager: `<EM_HOME>/product/webview`
- 독립 실행형 WebView 서버: `<WEBVIEW_HOME>/product/webview`

다음 단계는 두 설치 모두에 적용됩니다.

다음 단계를 따르십시오.

1. `<INSTALL_HOME>` 디렉터리에서 `Introscope_WebView.lax` 파일을 텍스트 편집기로 엽니다.

2. 다음 속성을 검색합니다.

```
lax.nl.java.option.additional
```

다음 예제에서는 이 속성에 대해 주석 처리된 줄을 보여 줍니다.

```
# Introscope Java Agent Arguments for WebView Monitor
# -XX:PermSize=128m -XX:MaxPermSize=256m
-javaagent:./product/webview/agent/wily/Agent.jar
-Dcom.wily.introscope.agentProfile=./product/webview/agent/wily/core/config/IntroscopeAgent.profile
-Dcom.wily.introscope.wilyForWilyPrefix=com.wily
-Djetty.home=.
```

3. 줄에서 "#"를 제외한 인수를 복사하여 `lax.nl.java.option.additional` 속성 값에 추가합니다.

다음 예제에서는 그 결과를 보여 줍니다.

```
lax.nl.java.option.additional=-Xms256m -Xmx1024m
-Djava.awt.headless=false
-Dorg.owasp.esapi.resources=./config/esapi
-Dsun.java2d.noddraw=true
-Dintroscope.webview.testpanel.enable=false
-Dintroscope.webview.saas.enable=false
-XX:PermSize=128m
-XX:MaxPermSize=256m
-javaagent:./product/webview/agent/wily/Agent.jar
-Dcom.wily.introscope.agentProfile=./product/webview/agent/wily/core/config/IntroscopeAgent.profile
-Dcom.wily.introscope.wilyForWilyPrefix=com.wily
-Djetty.home=.
```

참고: 사용 중인 파일에 있는 값은 이 예제와 다를 수 있습니다.

변경 사항을 저장합니다.

4. WebView 모니터 관리 모듈을 배포합니다. 이렇게 하려면 다음 *modules* 폴더의 *WebView.jar* 파일을

```
<EM_HOME>/examples/WebViewMonitor/config/modules
```

다음 *deploy* 폴더에 복사합니다.

```
<INSTALL_HOME>/deploy
```

WebView 서버를 다시 시작하여 구성을 완료합니다.

5. (선택 사항) Windows 만 해당: WebView 응용 프로그램을 시작할 Windows 서비스를 만든 경우 다음과 같이 서비스가 시작될 때 시작되도록 APM UI 성능 모니터를 구성할 수 있습니다.
 - a. <INSTALL_HOME>/bin 디렉터리로 이동하고 *WVService.conf* 파일을 텍스트 편집기로 엽니다.
 - b. *# Java Additional Parameters* 아래에서 다음 섹션을 찾습니다.


```
#wrapper.java.additional.4=-XX:PermSize=128m -XX:MaxPermSize=256m
-javaagent:./product/webview/agent/wily/Agent.jar
-Dcom.wily.introscope.agentProfile=./product/webview/agent/wily/core/config/IntroscopeAgent.profile
-Dcom.wily.introscope.wilyForWilyPrefix=com.wily -Djetty.home=./
```
 - c. 이 문자열의 시작 부분에서 해당 매개 변수를 주석 처리하는 "#"를 제거합니다.

변경 사항을 저장합니다.

Windows 서비스를 다시 시작하여 구성을 완료합니다.

구성 확인

구성이 올바른지 확인할 수 있습니다.

다음 단계를 따르십시오.

1. WebView 에서 "Investigator", "메트릭 브라우저"를 차례로 클릭합니다.
2. 다음과 같이 APM.WebView 로 이동합니다.


```
<DomainName>|<WebViewHostName>|APM Introscope WebView|APM.WebView
```
3. 표준 메트릭을 보고 Enterprise Manager 에 데이터를 보고하고 있는지 확인합니다.

4. "콘솔" 탭을 클릭하고 다음 샘플 대시보드가 대시보드 드롭다운 목록에 나타나는지 확인합니다.
 - [WebView - Overview\(WebView - 개요\)](#)
 - [WebView - Maps and Widgets\(WebView - 맵 및 위젯\)](#)
 - [WebView - Resources\(WebView - 리소스\)](#)
 5. "WebView - Overview"(WebView - 개요) 샘플 대시보드를 열고 다음 작업을 수행합니다.
 - 데이터 뷰어에서 그래프나 차트를 마우스 오른쪽 단추로 클릭합니다. "링크" 드롭다운 목록에서 관리 모듈의 해당 메트릭으로 이동합니다.
 - 차트나 그래프에서 도구 설명을 열고 링크를 클릭하여 메트릭 브라우저 트리의 해당 메트릭으로 이동합니다.
- 구성이 확인되었습니다.

WebView UI 성능 모니터링

APM UI 성능 모니터 샘플 대시보드는 **WebView** 응용 프로그램에 대한 건전성 모니터링 및 문제 해결 기능을 제공합니다. 성능 문제는 시각적 알림으로 나타날 수 있습니다. 예를 들어 대시보드에는 다음과 같은 정보가 있는 가로 막대형 차트 그래프가 표시됩니다.

- 3,000 밀리초의 주의 임계값을 나타내는 노란색 선
- 4,000 밀리초의 위험 임계값을 나타내는 빨간색 선

다음 단계를 따르십시오.

1. **WebView**의 "콘솔" 탭에 있는 드롭다운 목록에서 **WebView** 모니터링 샘플 대시보드를 선택합니다.
 - [WebView - Overview\(WebView - 개요\)](#) (페이지 227)
 - [WebView - Maps and Widgets\(WebView - 맵 및 위젯\)](#) (페이지 228)
 - [WebView - Resources\(WebView - 리소스\)](#) (페이지 228)

대시보드가 열리면서 현재 성능 상태가 표시됩니다. 가로 막대형 차트 그래프에 현재 데이터 값이 가로 막대로 표시됩니다.

2. [표준 메트릭](#) (페이지 231)을 분석합니다.

3. 대시보드에 표시된 데이터에 대한 추가 정보가 필요하다면 다음 바로 가기를 사용합니다.
 - 하이퍼링크가 있는 대시보드 개체를 마우스로 가리킵니다. 포인터가 손 모양으로 바뀝니다. 개체를 클릭하여 링크를 따라 해당 기본 대상으로 이동합니다.
 - 데이터 뷰어에서 대시보드 개체를 마우스 오른쪽 단추로 클릭합니다. 포인터가 손 모양으로 바뀝니다. "링크" 드롭다운 목록에서 관리 모듈의 해당 개체로 이동합니다. 데이터 뷰어가 해당 기반이 되는 메트릭 그룹화에 자동으로 연결됩니다.
 - 요소를 마우스로 가리켜서 도구 설명을 엽니다. 도구 설명에서는 심사 맵 탭과 메트릭 브라우저 탭 모두에 있는 계층 트리 및 뷰어 창의 메트릭 경로와 값을 식별할 수 있습니다. 트리 내의 메트릭을 보려면 도구 설명 내의 하이퍼링크를 클릭합니다.
4. 시간 범위를 선택하여 [다양한 시점의 데이터를 봅니다](#) (페이지 230).
5. ["평균 응답 시간"의 추세](#) (페이지 232)와 다른 메트릭의 변경을 함께 사용하여 문제를 식별하고 진단합니다.

참고: WebView 콘솔 대시보드의 모든 정보를 볼 수는 있지만 편집할 수는 없습니다. 대시보드를 만들고 편집하려면 **Workstation** 을 사용하십시오.

"WebView - Overview"(WebView - 개요) 대시보드

"WebView - Overview"(WebView - 개요) 대시보드는 관리자가 전체 환경에서 WebView 응용 프로그램 성능을 모니터링하기 위한 것입니다.

그래프에서는 WebView 응용 프로그램 및 클라이언트와 서버 간의 상호 작용에 대한 상위 수준 정보를 제공합니다.

이 대시보드에는 다음과 같은 그래프가 포함되어 있습니다.

WebView Frontend(WebView 프론트엔드)

WebView 모니터링된 응용 프로그램의 프론트엔드 건전성 메트릭을 표시합니다. "평균 응답 시간"의 추세와 다른 메트릭의 변경 사항을 함께 사용하여 성능 문제를 식별하고 진단할 수 있습니다.

Active Browsers(활성 브라우저)

서버에 연결된 브라우저를 표시합니다.

Active Services(활성 서비스)

구독 관리자에 연결된 서비스를 표시합니다.

Client Requests Per Interval (15 sec)(간격(15 초)당 클라이언트 요청 수)

간격당 클라이언트 요청 수를 표시합니다.

"WebView - Maps and Widgets"(WebView - 맵 및 위젯) 대시보드

"WebView - Maps and Widgets"(WebView - 맵 및 위젯) 대시보드는 관리자가 심사 맵 및 SOA 종속성 맵 성능과 WebView 건전성 메트릭을 모니터링하기 위한 것입니다.

그래프에는 해당 맵 및 위젯의 전체적인 건전성과 성능이 표시됩니다.

참고: Investigator, "심사 맵"에서 비즈니스 서비스 및 프론트엔드로 이동해야 심사 맵 그래프에 데이터가 나타납니다.

이 대시보드에는 다음과 같은 그래프가 포함되어 있습니다.

Triage Map and SOA Dependency Map Health(심사 맵 및 SOA 종속성 맵 건전성)

APM Introscope WebView 에이전트에 대한 JSP 노드 아래의 비즈니스 서비스 및 프론트엔드에 대한 건전성 메트릭을 표시합니다.

Active Widgets Count(활성 위젯 수)

활성 위젯 수를 표시합니다.

Active Widgets Per Interval(간격당 활성 위젯 수)

간격당 활성 위젯 수를 표시합니다.

Triage Map Load Time (ms)(심사 맵 로드 시간(ms))

심사 맵을 로드할 시간(밀리초)을 표시합니다.

"WebView - Resources"(WebView - 리소스) 대시보드

"WebView - Resources"(WebView - 리소스) 대시보드는 관리자가 프론트엔드 I/O 및 호스트 리소스를 모니터링하기 위한 것입니다.

그래프에는 WebView 리소스의 전체적인 건전성 및 성능이 표시됩니다.

이 대시보드에는 다음과 같은 그래프가 포함되어 있습니다.

Frontends I/O(프런트엔드 I/O)

프런트엔드 소켓 I/O 의 입력 및 출력 대역폭(바이트/초)과 프런트엔드 소켓 I/O 동시성을 표시합니다.

Host Resources(호스트 리소스)

프로세스 CPU 사용률과 호스트 CPU 사용률을 비교해서 표시하고 서버 메모리 사용률과 할당도 비교해서 표시합니다.

WebView 메트릭 그룹화 구성

"WebView - Resources"(WebView - 리소스) 대시보드에서 WebView 메트릭 그룹화는 다음과 같은 정보를 저장하는 관리 모듈 개체입니다.

- 에이전트 표현식 -- 에이전트 이름까지의 데이터를 지정하여 메트릭에 대한 입력을 필터링하는 Perl 5 정규식입니다.
- 메트릭 표현식 -- 리소스(메트릭으로 이어지는 폴더 체인)와 메트릭을 지정하는 Perl 5 정규식입니다.

에이전트 표현식에서 기본 에이전트 프로세스 이름이나 기본 에이전트 이름을 바꾸려면 몇 가지 추가 단계가 필요합니다.

다음 단계를 따르십시오.

1. WebView 에서 "관리" 탭을 클릭하고 "WebView Monitoring"(WebView 모니터링) 메트릭 그룹화를 찾습니다.
2. 업데이트할 "WebView - Resources"(WebView - 리소스) 대시보드 메트릭 그룹화를 찾습니다. 예를 들어 "Frontend I/O"(프런트엔드 I/O), "Process and Host CPU"(프로세스 및 호스트 CPU), "Frontend I/O Concurrency"(프런트엔드 I/O 동시성), "Heap Size and Allocation"(힙 크기 및 할당)입니다.
3. 에이전트 표현식에서 프로세스 이름 값(APM Introscope WebView) 또는 에이전트 이름 값(APM.WebView)을 편집합니다.
4. 변경 사항을 저장합니다.

5. Java Agent 에서 *IntroscopeAgent.profile* 을 텍스트 편집기로 엽니다.
6. *introscope.agent.defaultProcessName* 또는 *introscope.agent.agentName* 속성을 검색합니다.
7. 3 단계에서 제공한 것과 동일한 이름 값을 입력합니다.
8. 변경 사항을 저장합니다.
구성이 설정되었습니다.

대시보드 데이터 보기 및 해석

다음과 같이 다양한 방법으로 대시보드 데이터를 보고 해석할 수 있습니다.

- [다양한 시점의 데이터 보기](#) (페이지 230)
- [표준 메트릭 보기](#) (페이지 231)
- ["평균 응답 시간"의 추세 해석](#) (페이지 232)

다양한 시점의 데이터 보기

라이브 데이터를 보거나, 시간 범위를 선택하여 다양한 시점의 데이터를 볼 수 있습니다. 기본 데이터 뷰는 라이브입니다.

브라우저 맨 위의 "시간 창"을 확인하여 **WebView** 가 라이브 모드인지 여부를 알 수 있습니다.

다양한 시점의 대시보드를 보려면 다음 작업을 수행합니다.

- [기록 데이터 보기](#) (페이지 230)
- [사용자 지정 시간 범위 정의](#) (페이지 231)

기록 데이터 보기

응용 프로그램을 모니터링할 경우 라이브 데이터 뷰가 계속 바뀌면서 가장 최근 데이터를 보여 줍니다. 라이브 데이터는 기본 뷰입니다. 시간 범위를 선택하여 기록 데이터를 보고 문제가 발생한 시간을 식별할 수 있습니다.

다음 단계를 따르십시오.

1. **WebView** 의 "콘솔" 탭에 있는 "대시보드" 드롭다운 목록에서 기록 데이터를 볼 대시보드를 선택합니다.

2. "시간 창" 드롭다운 목록에서 기록 뷰에 대한 시간 범위(예: 24 시간)를 선택합니다.
선택한 기간(예: 24 시간)을 사용하여 해당 범위에 대한 데이터가 대시보드에 표시됩니다. 종료 시간은 현재 시간으로 설정되어 있습니다.
3. 시작 시간을 변경하려면 "시간 창" 옆에 있는 앞으로 화살표 및 뒤로 화살표를 클릭합니다.
4. 범위의 종료 시간을 현재 시간으로 다시 설정하려면 "지금 종료"를 클릭합니다.

사용자 지정 시간 범위 정의

콘솔에서 데이터를 볼 사용자 지정 시간 범위를 정의할 수 있습니다.

다음 단계를 따르십시오.

1. 기록 데이터를 볼 메트릭 또는 대시보드를 선택합니다.
2. "시간 창" 드롭다운 목록에서 "사용자 지정 범위"를 선택합니다.
3. "사용자 지정 범위" 창이 열리고 현재 날짜(오늘)가 윤곽선으로 강조 표시됩니다.
4. 달력 컨트롤을 사용하여 시작 및 종료 날짜를 선택합니다.
5. "확인"을 클릭합니다.

사용자 지정 범위에 대한 데이터가 설정됩니다.

표준 메트릭

WebView에는 에이전트가 원격 및 로컬 시스템에서 수집하는 응용 프로그램 성능 데이터가 메트릭으로 표시됩니다. 모니터링된 프론트엔드 및 백엔드 응용 프로그램 구성 요소와 기타 많은 응용 프로그램 구성 요소의 경우 다음 표준 메트릭이 나타납니다.

- **평균 응답 시간(ms)** - 응용 프로그램 응답 속도 측정값
- **동시 호출** - 주어진 시간에 처리되고 있는 요청 수
- **간격당 오류 수** - 지정된 시간 조각 동안 발생한 오류 수
- **간격당 응답 수** - 지정된 시간 조각 동안 완료된 요청 수
- **중단 수** - 중단 수. 중단은 지정된 시간 임계값 전에 완료되지 않은 요청입니다.

"평균 응답 시간"의 추세

"평균 응답 시간"의 추세와 다른 메트릭의 변경 사항을 함께 사용하여 문제를 식별하고 진단할 수 있습니다. 다음 표에서 자세한 정보를 제공합니다.

"평균 응답 시간"의 추세 정의

지속적 문제	<p>"사용 가능한 스레드 수"가 낮을 때 "평균 응답 시간"이 지속적으로 높으면 다음 문제가 있음을 의미할 수 있습니다.</p> <ul style="list-style-type: none">■ 비효율적인 코드■ 외부 시스템의 과도한 사용■ 느린 백엔드■ 계층이 너무 많음 <p>지속적 문제는 항상 존재하며 더 호전되거나 악화되지 않습니다.</p>
주기적 문제	<p>"평균 응답 시간"이 주기적으로 높으며 그래프에서 주기적으로 급등했다가 정상으로 돌아갑니다.</p> <p>"사용 가능한 스레드 수"가 낮을 때 "평균 응답 시간"이 주기적으로 높으면 다음 문제가 있음을 의미할 수 있습니다.</p> <ul style="list-style-type: none">■ 잦은 GC 누수■ 로드 관련 백엔드 병목 <p>"CPU 사용률"이 낮을 때 "평균 응답 시간"이 주기적으로 높으면 다음 문제가 있음을 의미할 수 있습니다.</p> <ul style="list-style-type: none">■ 내부 문제점 <p>주기적 문제는 주기적으로 발생했다가 진정됩니다.</p>
점진적 문제	<p>"간격당 응답 수"가 낮을 때 "평균 응답 시간"이 장기간 지속적으로 상승하면 다음 문제가 있음을 의미할 수 있습니다.</p> <ul style="list-style-type: none">■ 메모리 누수 <p>점진적 문제는 시간 경과에 따라 완화됩니다.</p>

제 12 장: Workstation 구성

이 단원에서는 Introscope Workstation 에 대한 선택적 동작을 구성하는 방법을 설명합니다.

이 섹션은 다음 항목을 포함하고 있습니다.

[세부 정보 표시 모드에서 Workstation 실행](#) (페이지 233)

[Workstation 출력을 파일로 리디렉션](#) (페이지 234)

[로그인 값을 제공하도록 Workstation 구성](#) (페이지 234)

[아시아 언어 보고서에 대해 Workstation 구성](#) (페이지 235)

세부 정보 표시 모드에서 Workstation 실행

세부 정보 표시 모드에서 Workstation 을 실행하면 디버깅이나 문제 해결에 유용한 세부 로그 메시지가 생성됩니다.

세부 정보 표시 모드에서 **Workstation** 을 실행하려면

1. `<EM_Home>/config` 에 있는 `IntroscopeWorkstation.properties` 파일을 엽니다.
2. `log4j.logger.Workstation` 속성에서 `"INFO"`를 다음으로 바꿉니다.
`VERBOSE#com.wily.util.feedback.Log4JSeverityLevel`
3. 변경 사항을 저장합니다.

Workstation 출력을 파일로 리디렉션

Workstation 출력을 파일로 리디렉션하려면

1. `<EM_Home>/config` 에 있는 `IntroscopeWorkstation.properties` 파일을 엽니다.

2. `log4j.logger.Workstation` 속성에서 `"console"`을 `"logfile"`로 바꿉니다. 예를 들어 다음 속성 설정을 사용하면 Workstation 이 세부 정보 표시 메시지를 로그 파일에 기록합니다.

```
log4j.logger.Workstation=VERBOSE#com.wily.util.feedback.Log4JSeverityLevel,logfile
```

3. `log4j.appender.logfile.File` 속성을 사용하여 Workstation 로그 파일의 이름과 위치를 변경할 수 있습니다.

로그인 값을 제공하도록 Workstation 구성

로그인 값을 제공하고 로그인 화면을 우회하도록 `Introscope Workstation.lax` 파일을 수정할 수 있습니다.

Workstation 로그인 화면을 우회하는 명령줄 인수를 설정하려면

1. `<EM_Home>/Introscope Workstation.lax` 파일을 엽니다.

2. `lax.command.line.args` 속성에서 값을 제공할 로그인 명령 각각에 대해 `-login` 명령을 추가합니다. 예를 들어 로컬 인증을 사용하는 경우 이 속성은 다음과 같이 나타납니다.

```
lax.command.line.args=$CMD_LINE_ARGUMENTS$ -loginimmediate  
-loginhost foos -loginport 4503 -loginresponse sanderson,45tst87
```

참고: 설정에서 기본값인 `$CMD_LINE_ARGUMENTS$`를 삭제하지 마십시오.

로그인에 성공한 경우, 즉 올바른 구문을 사용하여 올바른 정보가 명령에서 제공된 경우 Workstation 에 로그인되면서 콘솔이 열립니다.

로그인에 실패한 경우에는 Workstation 이 시작되지 않고 오류 메시지가 기록됩니다.

아시아 언어 보고서에 대해 Workstation 구성

중국어, 일본어 등의 멀티바이트 문자 집합을 사용하는 언어로 Introscope 보고서를 생성할 계획인 경우 여기에서 설명하는 지침에 따라 Workstation 설치에 구성 요소를 추가하십시오.

RTF 와 HTML 형식으로 아시아 언어 보고서를 생성하려면

- Windows 에서 Supplemental Language Support to East Asian Languages(동아시아 언어에 대한 보조 언어 지원)를 설치합니다.
<http://www.microsoft.com/globaldev/handson/user/xpintl1supp.msp> 를 참조하십시오.

PDF 형식으로 아시아 언어 보고서를 생성하려면

- <http://www.adobe.com/products/acrobat/acrrasianfontpack.html> 에서 Acrobat Reader 아시아 글꼴 팩을 다운로드하여 설치합니다.

제 13 장: 시스템 구성

이 단원에서는 전체 CA APM 시스템 구성을 설명합니다.

이 섹션은 다음 항목을 포함하고 있습니다.

[클록 차이 허용치 구성](#) (페이지 237)

[최대 데이터 포인트 검색 속성 설정](#) (페이지 238)

[쿼리에서 반환되는 데이터 포인트 제한](#) (페이지 240)

[반환되는 쿼리 결과 수 늘리기](#) (페이지 241)

[APM 상태 콘솔 클램프 및 중요한 이벤트 구성](#) (페이지 241)

클록 차이 허용치 구성

클록 차이 허용치는 대개 작은 증분 단위로 수행되는 클록 설정 조정의 변동입니다. 예를 들어 약간 빠르게 실행되고 있는 컴퓨터 클록을 몇 초 뒤로 설정하면 로그에 나타나는 작은 변화가 고려됩니다. 이 지연의 변동으로 인해 클록이 동일한 메트릭을 서로 다른 시간에 타임스탬프 처리하므로 시스템이 중복된 기간에 대해 두 개의 메트릭 값을 가지게 됩니다.

시간 되돌리기는 운영자에 의한 클록 시간 변경을 통해 명시적으로 발생할 수도 있고 자동 클록 동기화를 통해 암시적으로 발생할 수도 있는데, 후자의 경우 대규모 설치에서 발생할 가능성이 높습니다.

Enterprise Manager 는 다음 두 가지 방법 중 하나로 클록 차이 허용치를 처리합니다.

- 대규모 클록 조정의 경우 오류가 발생하면서 시스템이 종료됩니다.
- 시간을 되돌리는 소규모 클록 조정의 경우 경고가 발생하고 타임스탬프가 이전처럼 멀어질 때까지 하베스트 주기가 중지됩니다.

이 임계값은 기본적으로 60 초로 설정되어 있지만 구성할 수 있습니다. 몇 초 미만의 음수 클록 조정을 수행하면 경고와 일시적인 하베스트 일시 중단이 발생하지만 그보다 더 큰 음수 클록 조정을 수행하면 시스템이 종료됩니다.

빠른 CPU 클럭이 네트워크 시간 서비스를 통해 다시 설정될 때 일반적으로 발생하는 것과 같이 시스템 클럭이 이전 시간으로 설정되었다고 감지하는 경우 Enterprise Manager 는 클럭이 이전 시간을 따라잡을 때까지 하베스트 주기를 지연합니다. 이 지연은 일반적으로 경고 메시지를 동반합니다. 경고 메시지를 표시하지 않으려는 경우 선택적 속성인 `introscope.enterprisemanager.clock.skewsuppresswarn` 을 설정할 수 있습니다. 이 속성의 값은 메트릭 하베스트가 로깅되기에 충분할 만큼 심각한 상태로 간주되기 전에 지연될 시간(밀리초)입니다.

클럭 차이 허용치 임계값을 구성하려면

1. Enterprise Manager 를 중지합니다.
2. `<EM_Home>\config` 디렉터리로 이동하고 `IntroscopeEnterpriseManager.properties` 파일을 엽니다.
3. `introscope.enterprisemanager.clock.skewtoleranceseconds=<XXX>` 속성을 추가합니다. 여기서 `<XXX>`는 시간(초)입니다.
4. 선택 사항: `introscope.enterprisemanager.clock.skewsuppresswarn` 속성을 설정합니다. 밀리초 단위로 표현되는 기본값은 0 입니다.

참고: 이 값은 `introscope.enterprisemanager.clock.skewtoleranceseconds` 속성보다 높게 설정할 수 없습니다. 그렇지 않으면 경고가 완전히 표시되지 않고 시스템이 종료됩니다.

5. Enterprise Manager 를 시작합니다. 그러면 새 설정이 적용됩니다.

최대 데이터 포인트 검색 속성 설정

JDBC, CLW 및 상위 N(CLW 와 Workstation 에 모두 해당) 쿼리에 대한 성능을 측정하기 위해 최대 데이터 포인트 검색 속성을 설정할 수 있습니다. 데이터 포인트는 한 기간 동안 하나의 메트릭이 가지는 값입니다.

이 Enterprise Manager 클램프 속성은 Enterprise Manager 가 단일 쿼리에 대해 SmartStor 에서 검색하는 최대 메트릭 데이터 포인트 수를 제한합니다. 그러나 Enterprise Manager 는 항상 하나 이상의 메트릭에 대해 전체 데이터를 반환합니다. 이 속성은 클러스터된 수집기나 독립 실행형 Enterprise Manager 에 적용됩니다.

이 속성을 설정하지 않으면 다음과 같은 결과가 발생할 수 있습니다.

- Enterprise Manager 오버로드로 인해 CA APM 시스템 성능이 저하되고 잠재적으로 메모리 부족 오류가 발생할 수 있습니다.
- 이 속성은 명령줄 Workstation 이나 Workstation 에서 너무 많은 데이터를 추출하도록 만들 수 있으며 이러한 동작으로 인해 Enterprise Manager 응답이 중지될 수 있습니다.

다음 단계를 따르십시오.

1. <EM_Home>\config 디렉터리로 이동하고 *IntroscopeEnterpriseManager.properties* 파일을 엽니다.

2. 다음 속성을 추가합니다.

```
introscope.enterprise.manager.query.datapointlimit=100000
```

여기서 *100000* 은 쿼리당 SmartStor 에서 검색되는 데이터 포인트 수를 100,000 개 정도로 제한합니다. 입력된 숫자 값이 없으면 제한이 적용되지 않습니다.

3. *IntroscopeEnterpriseManager.properties* 파일을 저장합니다.

설정은 약 60 초마다 한 번씩 발생하는 핫 배포 중에 Enterprise Manager 가 속성 파일을 검사할 때 적용됩니다.

쿼리에서 반환되는 데이터 포인트 제한

JDBC, CLW 및 상위 N(CLW 와 Workstation 에 모두 해당) 쿼리에 대한 성능을 측정하기 위해 `introscope.enterprisemanager.query.returneddatapointlimit` 속성을 설정할 수 있습니다. 이 Enterprise Manager 클램프 속성은 쿼리에서 반환되는 데이터 포인트 수를 제한합니다. 데이터 포인트는 한 기간 동안 하나의 메트릭이 가지는 값입니다.

쿼리에서 반환되는 데이터 포인트 수는 다음 요소에 따라 결정됩니다.

- 일치하는 메트릭 수
- 요청하는 시간 범위
- SmartStor 데이터 계층 구성에 따라 결정되는 SmartStor 데이터 레졸루션

예를 들어 1 분간의 레졸루션을 사용하는 단일 메트릭으로 1 시간 분량의 데이터를 쿼리하는 경우를 가정해 보겠습니다. 15 초의 레졸루션을 사용하는 데이터가 SmartStor 에 있으면 이 쿼리는 240 개의 데이터 포인트와 일치합니다. 그러나 1 분간의 레졸루션을 요청하고 있으므로 15 초의 데이터 포인트가 1 분의 데이터 포인트로 집계됩니다. 따라서 쿼리에서 60 개의 데이터 포인트만 반환됩니다.

지정된 메트릭에 대해 쿼리에서 요청된 데이터의 전체 집합이 반환되거나 아무것도 반환되지 않습니다. 메트릭에 대한 부분 데이터는 표시되지 않으며, 모든 데이터가 표시되거나 아무것도 표시되지 않습니다. 클램프의 효과는 데이터가 반환되는 메트릭 수를 줄이는 것입니다.

메모리가 부족한 환경에서 이 속성을 설정하지 않고 많은 양의 데이터 쿼리를 실행하면 Enterprise Manager 에 메모리 부족이 발생할 수 있습니다.

다음 단계를 따르십시오.

1. `<EM_Home>\config` 디렉터리로 이동하고 `IntroscopeEnterpriseManager.properties` 파일을 엽니다.

2. 다음 속성을 추가합니다.

```
introscope.enterprisemanager.query.returneddatapointlimit= 100000
```

여기서 100000 은 쿼리당 SmartStor 에서 검색되는 데이터 포인트 수를 100000 개 정도로 제한합니다. 입력된 숫자 값이 없으면 제한이 적용되지 않습니다.

3. `IntroscopeEnterpriseManager.properties` 파일을 저장합니다.

설정은 약 60 초마다 한 번씩 발생하는 핫 배포 중에 Enterprise Manager 가속성 파일을 검사할 때 적용됩니다.

반환되는 쿼리 결과 수 늘리기

RangeQuery, *PrefixQuery*, *WildcardQuery* 또는 *FuzzyQuery* 쿼리를 수행하면 검색이 수행되기 전에 해당 쿼리가 확장됩니다. 예를 들어 인덱스된 문서에 "car" 및 "cars" 용어가 포함되어 있으면 검색이 발생하기 전에 쿼리 "ca*"가 "car OR cars"로 확장됩니다. 이 수가 용어 임계값의 기본값인 2048 을 초과하면 시스템 오류가 발생할 수 있습니다. 이 경우 *TooManyClauses* 예외가 반환됩니다.

반환되는 쿼리 결과 수를 늘리려면

1. `<EM_Home>\config` 디렉터리로 이동하고 `IntroscopeEnterpriseManager.properties` 파일을 엽니다.
2. 기본값인 2048 보다 더 높은 값으로 설정된 `introscope.enterprisemanager.lucene.search.BooleanQuery.SetMaxClauseCount` 속성을 추가합니다.

설정은 약 60 초마다 한 번씩 발생하는 핫 배포 중에 Enterprise Manager 가속성 파일을 검사할 때 적용됩니다.

APM 상태 콘솔 클램프 및 중요한 이벤트 구성

`apm-events-thresholds-config.xml` 파일에서 CA Introscope 클램프, CA CEM 클램프 및 중요한 이벤트 속성에 대한 임계값을 구성할 수 있습니다. 이러한 속성 임계값에 도달하거나 이러한 속성 임계값이 초과되면 Enterprise Manager 가 APM 상태 콘솔에 알립니다. 클램프 정보는 "활성 클램프" 탭에 표시됩니다. 중요한 이벤트 정보는 "중요한 이벤트" 테이블 뷰에 표시됩니다.

다음 단계를 따르십시오.

1. `<EM_Home>/config` 디렉터리로 이동하고 `apm-events-thresholds-config.xml` 파일을 백업합니다.

중요! 파일 백업을 소홀히 하지 마십시오. 구성된 파일이 손상되면 속성 값이 기본값으로 되돌아가고 모든 구성 사항이 손실됩니다.

2. 사용자 환경에 맞게 속성을 구성합니다.

참고: 오직 *threshold value* 필드의 값만 구성하십시오. *clamp ID*, *importantEvent ID*, *description* 등의 다른 필드는 CA Introscope 의 시스템 모니터링에 사용되므로 변경하지 *마십시오*.

- a. `apm-events-thresholds-config.xml` 파일을 엽니다.
- b. 클램프 및 중요한 이벤트 임계값을 수정합니다.

예를 들어 `<threshold value="500000"/>`으로 수정합니다. 여기서 수정된 값은 500000 입니다.

3. `apm-events-thresholds-config.xml` 을 저장하고 닫습니다.

약 60 초마다 한 번씩 발생하는 핫 배포 중에 Enterprise Manager 가 구성 설정을 적용합니다.

Enterprise Manager 는 `apm-events-thresholds-config.xml` 파일에서 구문 오류를 발견한 경우 다음 동작을 수행합니다.

- APM 상태 콘솔에 `apm.events.thresholds.config.error` 중요한 이벤트를 "중요한 이벤트" 테이블 뷰에 표시하도록 알립니다.
- 모든 클램프 및 중요한 이벤트 속성 값을 기본값으로 되돌립니다.

4. 필요한 경우 `apm-events-thresholds-config.xml` 파일의 문제를 해결합니다.

- a. `apm-events-thresholds-config.xml` 파일을 엽니다.
- b. 파일을 검토하여 구문 오류가 있는지 확인하고 필요에 따라 수정합니다.
- c. 파일을 저장하고 닫습니다.
- d. `apm-events-thresholds-config.xml` 파일 오류를 찾을 수 없거나 수정할 수 없는 경우 손상된 `apm-events-thresholds-config.xml` 파일을 1 단계에서 저장한 백업 파일로 바꿉니다.
- e. 2 단계와 3 단계를 반복합니다.

5. 하나의 클러스터에 속한 여러 Enterprise Manager 를 구성하는 경우 모든 수집기, MOM 및 CDV(배포된 경우)에서 1~4 단계를 수행합니다.

모든 Enterprise Manager 가 CA Introscope 및 CA CEM 클램프와 중요한 이벤트 속성을 사용하여 구성됩니다. `apm-events-thresholds-config.xml` 파일이 배포되고, 속성 임계값 수준에 도달하거나 속성 임계값 수준이 초과될 때 클램프와 중요한 이벤트 클램프가 활성화됩니다.

제 14 장: 응용 프로그램 심사 맵 구성

이 장에서는 응용 프로그램 심사 맵에 대한 선택적 동작을 구성하는 방법을 설명합니다.

이 섹션은 다음 항목을 포함하고 있습니다.

[응용 프로그램 심사 맵](#) (페이지 243)

[응용 프로그램 심사 맵 데이터 클램프](#) (페이지 248)

[응용 프로그램 심사 맵 데이터 정리 구성](#) (페이지 249)

[응용 프로그램 심사 맵 개체의 사용 만료 시간 구성](#) (페이지 253)

응용 프로그램 심사 맵

응용 프로그램 심사 맵은 응용 프로그램 구성 요소에 대한 그래픽 시각화를 통해 응용 프로그램의 건전성과 오류를 보여 줍니다. 이 맵은 **Introscope** 메트릭, 오류 및 이벤트의 성능과 분석에서 자동으로 생성되며 사용자가 정의한 비즈니스 중심 측면에서 응용 프로그램을 제공합니다. 응용 프로그램 심사 맵을 사용하면 사용자 환경에 있는 응용 프로그램의 구조와 응용 프로그램 간의 관계를 시각적 형식으로 즉시 파악할 수 있으므로 현재 문제와 최근 생겨난 문제를 식별하고 심사하는 데 도움이 됩니다.

응용 프로그램 심사 맵의 모양과 용도에 대한 자세한 내용은 *CA APM Workstation 사용자 안내서*를 참조하십시오.

Introscope Agent 는 비즈니스 트랜잭션 및 프론트엔드와 해당 종속성을 감지합니다. 그런 다음 이 정보를 **Enterprise Manager** 에 데이터로 보고합니다. 그러면 **Enterprise Manager** 는 이 데이터를 **APM** 데이터베이스에 저장하고 **Workstation** 에 보냅니다. **Workstation** 은 이 데이터를 "Map"(맵) 탭에 응용 프로그램 심사 맵으로 표시합니다.

다음은 구성할 수 있습니다.

- 에이전트가 응용 프로그램 심사 맵 데이터를 수집하는지 여부
- **Introscope** 에서 맵을 그릴 목적으로 프론트엔드 또는 비즈니스 서비스 데이터를 샘플링하는 속도. [트랜잭션 샘플링](#) (페이지 244)을 참조하십시오.

- APM 데이터베이스에 응용 프로그램 심사 맵 데이터를 저장하는 기간. [맵 요소 만료 처리](#) (페이지 244)를 참조하십시오.
- APM 데이터베이스에서 응용 프로그램 심사 맵 데이터를 정리하는지 여부와 정리하는 빈도. [응용 프로그램 심사 맵 데이터 정리](#) (페이지 249)를 참조하십시오.

트랜잭션 샘플링

Introscope 는 *트랜잭션 샘플링*이라고 하는 방법을 사용하여 응용 프로그램 심사 맵 표시용 데이터를 제공합니다. 에이전트가 시작된 후 Introscope 는 기본적으로 처음 100 개의 트랜잭션을 가져와서 프런트엔드 또는 비즈니스 트랜잭션과 해당 종속성을 보여 주는 초기 맵을 그립니다. 그 이후에는 모든 열 번째 트랜잭션만 맵에 대한 지속적인 데이터 지원을 제공하는 수준에 도달할 때까지 샘플링하는 트랜잭션 수를 점차적으로 줄입니다. 10,000 개의 트랜잭션이 처리될 때마다 이 패턴이 반복됩니다.

IntroscopeAgent.profile 에서 다음 속성을 편집하여 샘플링 속도를 조정할 수 있습니다.

- `introscope.agent.tracer.sampling.maxrate`
- `introscope.agent.tracer.sampling.initial.period`
- `introscope.agent.tracer.sampling.reset.period`

IntroscopeAgent.profile 의 속성 편집에 대한 자세한 내용은 사용자 환경에 따라 *CA APM Java Agent 구현 안내서* 또는 *CA APM .NET 에이전트 구현 안내서*를 참조하십시오.

이러한 속성을 조정하여 맵 표시를 지원하는 트랜잭션 수를 늘리면 오버헤드가 영향을 받을 수 있습니다.

맵 요소 만료 처리 구성

연결 데이터가 만료 처리되거나 APM 데이터베이스에서 정리되면 에이전트는 프런트엔드 및 비즈니스 서비스와 그 종속성을 재검색합니다. Workstation 은 응용 프로그램 심사 맵에 이 데이터를 표시합니다.

응용 프로그램 심사 맵 데이터를 수집하도록 에이전트를 설정한 후에는 에이전트가 이 데이터 수집을 수행하는 빈도를 구성할 수 있습니다. 예를 들어, 다음과 같이 응용 프로그램 심사 맵 데이터를 수집하도록 에이전트를 구성할 수 있습니다.

- 환경에 빈번한 변경 사항이 있는 경우 24 시간마다 한 번씩
- 환경에 빈번한 변경 사항이 없는 경우 1 주일에 한 번씩

Enterprise Manager 가 Workstation 으로 맵 표시를 위한 데이터를 전달하는 기간도 구성할 수 있습니다. 예를 들어, 에이전트에 의해 검색된 데이터는 1 주 또는 한 달 동안 표시될 수 있습니다. 기간은 "만료 처리 시간"과 "기간 시간"의 두 가지 기간 속성을 기반으로 합니다.

만료 처리는 응용 프로그램 심사 맵 요소의 특성입니다. CA Introscope 가 더 이상 프런트엔드 또는 비즈니스 트랜잭션에 대한 데이터를 받지 않으면 맵 요소가 만료 처리됩니다. 만료 처리 시간은 Workstation 이 응용 프로그램 심사 맵에 요소를 계속 표시하는 기간입니다. 이 시간이 만료되면 요소가 에이전트 캐시에서 제거되고 응용 프로그램 심사 맵에 만료 처리된 것으로 나타납니다. 만료 처리 시간은 introscope.apm.data.agingTime 속성에 설정됩니다. 기본값은 1 일입니다.

시간 창은 만료 처리 요소가 맵에서 완전히 사라지기 전에 Workstation 에서 해당 요소를 표시하는 시간입니다. 이 옵션은 introscope.apm.data.timeWindow 속성에서 설정합니다. 기본값은 3 일입니다.

예를 들어 기본 설정을 사용하면 다음과 같습니다.

ApplicationA 는 응용 프로그램 심사 맵에서 프런트엔드이며 ApplicationB 와의 종속성이 있습니다. 에이전트가 계속해서 ApplicationB 의 데이터를 보고하고 ApplicationB 가 맵 표시에 정상적으로 나타납니다. ApplicationB 의 데이터 보고가 중지되면 만료 처리 시간과 기간 시간 모두에 대해 클록이 시작됩니다. 1 일이 지나면 ApplicationB 맵 노드가 만료 처리된 것으로 나타납니다. 3 일이 지나면 ApplicationB 맵 노드가 맵에서 사라집니다.

고려 사항:

- timeWindow 에는 agingTime 의 기간이 포함됩니다.
- timeWindow 및 agingTime 이 동일한 기간으로 설정된 경우 맵 요소는 만료 처리된 것으로 표시될 수 없습니다. 이 요소는 timeWindow 기간이 끝날 때 사라집니다.

- timeWindow 를 agingTime 보다 큰 값으로 설정하면 agingTime 기간이 끝날 때 만료 처리된 맵 요소가 사라집니다.
- agingTime 및 timeWindow 의 경우, 회사가 응용 프로그램을 추가 및 수정하는 빈도를 기준으로 값을 선택하십시오. 이 값은 에이전트 및 Enterprise Manager 의 오버헤드를 늘리거나 줄일 수 있습니다. 더 낮은 값을 설정하면 맵이 실시간으로 응용 프로그램 종속성을 표시합니다. 더 높은 값을 설정하면 맵이 현재 응용 프로그램 종속성을 표시합니다.

중요! 클러스터 환경에서 agingTime 또는 timeWindow 기본 속성 값에 대한 모든 변경 사항은 MOM 및 모든 수집기에도 반드시 적용되어야 합니다.

다음 단계를 따르십시오.

1. <EM_Home>/config 디렉터리에 있는 IntroscopeEnterpriseManager.properties 파일을 엽니다.
2. introscope.apm.data.agingTime 의 값을 변경하는 경우 다음과 같이 합니다.
 - a. 에이전트를 중지합니다.
 - b. Enterprise Manager 를 종료합니다.

중요! introscope.apm.data.agingTime 속성의 값을 변경하는 경우 [응용 프로그램 심사 맵 만료 처리 시간 설정 감소가 미치는 영향](#) (페이지 247)을 참조하십시오.

3. introscope.apm.data.agingTime 속성을 구성합니다. 기본값은 1 일입니다. 값은 1 분 미만일 수 없습니다.
4. introscope.apm.data.timeWindow 속성을 구성합니다. 기본값은 3 일입니다. 값은 1 분 미만일 수 없습니다.
5. IntroscopeEnterpriseManager.properties 파일을 저장하고 닫습니다.
6. introscope.apm.data.agingTime 속성을 변경한 경우 에이전트를 다시 시작합니다.
7. Enterprise Manager 를 다시 시작합니다.
8. <EM_Home>/logs 디렉터리에 있는 Enterprise Manager 로그 파일 메시지에서 맵 데이터 만료 처리 속성을 봅니다. 예:
11/23/09 12:02:13 PM PST [INFO] [Manager] [The APM Data property : introscope.apm.data.agingTime set to value : [PropertyWithTimeUnit : 1 Min]

응용 프로그램 심사 맵 만료 처리 시간 설정 감소가 미치는 영향

IntroscopeEnterpriseManager.properties 파일에 있는 *introscope.apm.data.agingTime* 속성의 값을 낮출 계획인 경우 CA Technologies 에서는 응용 프로그램 심사 맵 데이터를 정리하여 예기치 않게 기록 데이터에 미치는 영향을 방지할 것을 권장합니다. 만료 처리 시간을 줄이면 더 작은 데이터 샘플이 맵 표시에 나타나고 이로 인해 APM 데이터베이스의 데이터를 기반으로 잘못된 표시가 발생할 수 있는데, 이는 에이전트가 데이터를 Enterprise Manager 에 보고하는 방법 때문입니다. 데이터베이스에서 데이터를 정리하면 이 문제가 해결됩니다.

데이터를 정리하려면 PostgreSQL 클라이언트를 사용해야 합니다. PostgreSQL 사이트(<http://www.pgadmin.org>)에서 해당 클라이언트를 다운로드할 수 있습니다.

PostgreSQL 클라이언트를 사용하여 데이터베이스를 정리하려면

- 다음 SQL 문을 실행합니다.

```
truncate apm_edge;
```

introscope.apm.data.agingTime 속성의 값을 높일 경우에는 그와 같은 예기치 않은 결과가 발생하지 않습니다. 속성의 값을 낮추어야 할 경우에만 데이터베이스를 정리하면 됩니다.

만료 처리 관련 속성이 기록 뷰에 미치는 영향

응용 프로그램 심사 맵과 함께 기록 데이터를 보는 경우 다음과 같은 개념에 유의하십시오.

- 기록 기간의 시작점과 끝점을 설정하는 방법에 관계없이 응용 프로그램 심사 맵에 표시되는 데이터는 적어도 `introscope.apm.data.timeWindow` 속성에서 설정한 기간을 포괄합니다. 예:
 - 기록 기간의 시작점과 끝점을 10 일 범위로 설정했지만 `introscope.apm.data.timeWindow` 가 3 일로 설정된 경우 맵에는 전체 10 일 범위의 데이터가 표시됩니다.
 - 기록 기간의 시작 날짜와 종료 날짜를 2 일 범위로 설정했지만 `introscope.apm.data.timeWindow` 가 3 일로 설정된 경우 맵에는 여전히 3 일 분량의 데이터가 표시되고 3 일 기간은 2 일 기간이 끝나는 것과 동시에 끝납니다. `introscope.apm.data.timeWindow` 속성이 어떤 값으로 설정되었든 이 값은 맵에 표시되는 최소 기간에 해당하며 이는 수동으로 설정된 기록 기간이 더 작은 경우에도 마찬가지입니다.
- 맵 요소의 만료 처리 동작은 기록 기간이 끝날 때 해당 만료 처리 시간이 발생하는 것처럼 `introscope.apm.data.agingTime` 속성에서 설정한 기간을 따릅니다. 예:
 - `introscope.apm.data.agingTime` 은 1 일로 설정되고, 사용자의 기록 기간은 10 일로 설정된 경우 기간의 최종일(1 일) 동안 이 요소를 보고한 에이전트가 없으면 맵 요소가 만료 처리된 것으로 표시됩니다.

응용 프로그램 심사 맵 데이터 클램프

양호한 성능을 보장하려는 목적으로 응용 프로그램 심사 맵에 대한 데이터 흐름을 제어하기 위해 Introscope 는 `APMEnterpriseManager.properties` 에 있는 `introscope.apm.query.max.results` 속성으로 설정된 임계값을 사용하여 Workstation 이 맵에 표시하려고 하는 데이터의 양을 클램프합니다. 트리 노드를 선택하거나 이 임계값을 초과하는 맵 요소를 펼치려고 하면 "맵이 너무 커서 표시할 수 없습니다"라는 메시지가 표시됩니다. 속성의 값을 조정하여 이 임계값을 조정할 수 있습니다.

참고: `introscope.apm.query.max.results` 속성의 값을 조정하면 Workstation 성능이 영향을 받을 수 있습니다.

이 속성에 대한 자세한 내용은 [introscope.apm.query.max.results](#) (페이지 494)를 참조하십시오.

응용 프로그램 심사 맵 표시 임계값을 편집하려면

1. <EM_Home>/config 디렉터리에 있는 *APMEnterpriseManager.properties* 파일을 엽니다.
2. Enterprise Manager 를 종료합니다.
3. introscope.apm.query.max.results 속성을 찾고 해당 값을 조정합니다.
4. *APMEnterpriseManager.properties* 파일을 저장하고 닫습니다.
5. Enterprise Manager 를 다시 시작합니다.

응용 프로그램 심사 맵 데이터 정리 구성

시간이 지남에 따라 APM 데이터베이스의 응용 프로그램 심사 맵 데이터가 증가할 수 있습니다. APM 데이터베이스에 과도한 데이터가 수집될 경우 Enterprise Manager 의 응용 프로그램 심사 맵 데이터 검색과 Workstation 및 Enterprise Manager 성능이 영향을 받을 수 있습니다. 응용 프로그램 심사 맵 데이터를 정리하여 APM 데이터베이스에 과도한 맵 데이터가 수집되지 않도록 할 수 있습니다.

중요! APM 데이터베이스에서 응용 프로그램 심사 맵 데이터 정리가 사용되도록 설정하는 경우 클러스터에 있는 Enterprise Manager 중 하나에 대해서만 설정을 구성하십시오. 하지만 MOM 에서 응용 프로그램 심사 맵 데이터 정리가 사용되도록 설정하는 것이 좋습니다.

정리될 때까지 맵 데이터가 데이터베이스에서 유지되는 기간과 정리를 수행하도록 예약할 빈도를 구성할 수 있습니다. 맵 데이터 정리는 매일, 매주 또는 매월 데이터를 정리하도록 구성할 수 있는 스케줄러를 통해 제어됩니다.

중요! 응용 프로그램 심사 데이터를 정리하도록 수집기를 구성할 수 없습니다. 수집기의 *introscope.apm.pruning.enabled* 속성을 *true* 로 설정하면 오류가 반환됩니다.

사용자가 맵을 보는 동안 응용 프로그램 심사 맵 데이터가 정리된 경우 정리된 데이터는 사용자가 맵 시간 범위를 변경하여 맵 다시 그리기가 트리거될 때까지 맵에 유지됩니다.

여러 Enterprise Manager 가 데이터베이스를 정리하도록 허용하는 경우 데이터베이스 액세스를 위해 여러 정리 프로세스가 경쟁하여 데이터베이스 교착 상태가 발생합니다.

다음 단계를 따르십시오.

1. <EM_Home>/config 디렉터리에 있는 *IntroscopeEnterpriseManager.properties* 파일을 엽니다.
2. Enterprise Manager 를 종료합니다.
3. *introscope.apm.pruning.enabled* 속성이 *true* 로 설정되었는지 확인합니다.

이 속성은 에이전트가 응용 프로그램 심사 맵 데이터를 정리하도록 설정합니다.

false 에서 *true* 로 *introscope.apm.pruning.enabled* 를 다시 설정한 경우에는 Enterprise Manager 를 다시 시작해야 이 속성이 적용됩니다.

4. (선택 사항) 다음 속성을 구성합니다.

참고: 사용자 환경에서 응용 프로그램 심사 맵 데이터의 양을 관리하려면 `introscope.apm.data.preserving.time` 속성의 값을 낮게 설정하십시오. 그렇지 않으면 예외가 표시될 수 있습니다. 예외를 방지하려면 APM SOI 커넥터를 설치하기 전에 사용자 환경이 응용 프로그램 사용에 맞게 조정되었는지 확인하십시오. 그래도 예외가 표시되면 `APMEnterpriseManager.properties` 파일에 있는 `introscope.apm.query.max.results` 속성의 값을 늘리십시오.

- `introscope.apm.data.preserving.time`

- `introscope.apm.pruning.cron.trigger.expression`

- a. APM 데이터베이스에 응용 프로그램 심사 맵 데이터를 저장하는 기간을 제어하는 `introscope.apm.data.preserving.time` 속성을 구성합니다. 유지 시간 값보다 오래된 맵 데이터는 만료 처리된 것으로 간주되어 정리될 수 있습니다. 기본값은 365 일입니다.

정리되는 동안 `introscope.apm.data.preserving.time` 값과 `Introscope.apm.data.agingTime` 값의 합계보다 오래된 맵 데이터가 삭제됩니다. 예를 들어 `introscope.apm.data.preserving.time` 값은 30 일이고 `introscope.apm.data.agingTime` 값은 1 일인 경우 31 일(30 일 + 1 일)보다 오래된 맵 데이터가 삭제됩니다.

조직에서 응용 프로그램을 추가하고 수정하는 빈도를 기반으로 APM 데이터베이스에 응용 프로그램 심사 맵 데이터를 추가하는 값을 업데이트합니다. 자세한 내용은 [introscope.apm.data.preserving.time](#) (페이지 480)을 참조하십시오. 기본값은 365 일입니다.

- b. APM 데이터베이스에서 만료 처리된 응용 프로그램 심사 맵 데이터를 정리하는 빈도를 예약하는 `introscope.apm.pruning.cron.trigger.expression` 속성을 구성합니다. 기본값은 매일 오전 06:00 입니다.

조직에서 응용 프로그램을 추가하고 수정하는 빈도를 기반으로 APM 데이터베이스에 응용 프로그램 심사 맵 데이터를 추가하는 값을 업데이트합니다. 자세한 내용은 [introscope.apm.pruning.cron.trigger.expression](#) (페이지 481)을 참조하십시오.

5. *IntroscopeEnterpriseManager.properties* 파일을 저장하고 닫습니다.
6. Enterprise Manager 를 다시 시작합니다.

Enterprise Manager 가 시작되면 *<EM_Home>/logs* 로 이동하여 맵 데이터 정리 속성과 연결된 Enterprise Manager 로그 파일 메시지를 검토할 수 있습니다. 예:

```
11/23/09 12:02:13 PM PST [INFO] [Manager] [ The APM Data property :  
introscope.apm.pruning.enabled set to value : true]  
11/23/09 12:02:13 PM PST [INFO] [Manager] [ The APM Data property :  
introscope.apm.pruning.cron.trigger.expression set to value : 0 0 6 * * ?]
```

응용 프로그램 심사 맵 개체의 사용 만료 시간 구성

CA APM 은 *가장자리*라는 용어로 응용 프로그램 심사 맵 개체를, *꼭지점*이라는 용어로 응용 프로그램 심사 맵 개체 간의 관계를 나타냅니다. APM 데이터베이스에는 이러한 개체에 대한 데이터가 저장됩니다.

시간 경과에 따라 Enterprise Manager 와 모니터링된 응용 프로그램 간의 연결이 손실되면 다음 두 요인에 따라 각 개체가 "만료 처리"됩니다.

- `introscope.apm.data.obsolete.time` 속성의 값
- 아래 표에 설명된 규칙

가장자리 개체가 만료 처리되면 연결된 모든 개체는 다른 활성 가장자리 개체에 사용되지 않는 경우 *사용 만료*로 분류됩니다. 응용 프로그램 심사 맵에는 이러한 사용 만료 개체와 연결된 요소가 "회색"으로 표시되므로 해당 요소가 현재가 아닌 이전 데이터임을 분명히 알 수 있습니다.

이러한 "만료 처리된" 개체는 APM 데이터베이스에 남아 있으며 자동으로 삭제되지 않습니다. 정리에 대해 설정된 속성을 기반으로 응용 프로그램 심사 맵 정리 프로세스가 발생할 때만 개체가 삭제됩니다. 정리 저장 프로시저는 사용 만료 규칙과는 다른 정리 규칙을 기반으로 개체를 물리적으로 삭제합니다. 정리에 대한 자세한 내용은 "[SmartStor 메타데이터 정리 \(페이지 81\)](#)"를 참조하십시오.

응용 프로그램 심사 맵 개체 만료 처리에 대한 규칙

개체	조건
가장자리 (데이터베이스 테이블 <code>apm_edge</code>)	가장자리는 해당 업데이트 날짜가 <code>introscope.apm.data.obsolete.time</code> 속성에 있는 값보다 오래된 경우 사용 만료된 것으로 간주됩니다.
꼭지점(데이터베이스 테이블 <code>apm_vertex</code>)	꼭지점은 응용 프로그램 심사 맵에서 사용 만료된 가장자리로 참조되고 다른 가장자리가 없는 경우에만 사용 만료된 것으로 간주됩니다.
소유자(데이터베이스 테이블 <code>apm_owner</code>)	소유자는 응용 프로그램 심사 맵에서 사용 만료된 가장자리로 참조되고 다른 가장자리가 없는 경우에만 사용 만료된 것으로 간주됩니다.

개체	조건
에이전트(데이터베이스 테이블 apm_agent)	에이전트는 응용 프로그램 심사 맵에서 사용 만료된 꼭지점으로 참조되는 경우에만 사용 만료된 것으로 간주됩니다.

응용 프로그램 심사 맵 시간 만료 처리 속성

응용 프로그램 심사 맵에 대한 시간 만료 처리 속성을 구성하여 데이터베이스에서 사용 만료된 개체에 대한 요청을 반환할 수 있습니다. 시간이 구성되지 않은 경우 기간(introscope.apm.data.preserving.time + introscope.apm.data.agingTime - introscope.apm.data.obsolete.time) 내 시점을 가리키는 모든 요청은 개체를 사용 만료된 개체로 지정할 수 있습니다.

기본값은 다음과 같습니다.

- introscope.apm.data.preserving.time
기본값: 365 DAYS
- introscope.apm.data.agingTime
기본값: 1 DAY
- introscope.apm.data.obsolete.time
기본값: 300 DAYS

중요! 클러스터 환경에서 agingTime 또는 timeWindow 기본 속성 값에 대한 모든 변경 사항은 MOM 및 모든 수집기에도 반드시 적용되어야 합니다.

예

사용 만료된 개체에서 정보를 가져오려면 November 1 at 0800h and 1500h 및 November 2 at 1000h 에 대해 쿼리 웹 서비스 API 를 실행하십시오. 이 쿼리는 각 요청에 대해 다음 결과를 제공합니다.

Get obsolete objects at November 1 8:00

11 월 1 일 8:00 시에 300 일보다 오래된 사용 만료된 개체를 식별합니다. introscope.apm.data.preserving.time + introscope.apm.data.agingTime 보다 오래된 모든 개체는 반환되지 않습니다.

Get obsolete objects from November 1 8:00 to November 1 15:00

11 월 1 일 8:00 와 11 월 1 일 15:00 에서 300 일의 `introscope.apm.data.obsolete.time` 값을 차감하여 11 월 1 일 8:00 에서 11 월 1 일 15:00 사이의 사용 만료된 개체를 식별합니다. `introscope.apm.data.preserving.time + introscope.apm.data.agingTime` 보다 오래된 개체는 반환되지 않습니다.

Get obsolete objects from November 1 15:00 to November 2 10:00

11 월 1 일 15:00 와 11 월 2 일 10:00 에서 300 일의 `introscope.apm.data.obsolete.time` 값을 차감하여 11 월 1 일 15:00 에서 11 월 2 일 10:00 사이의 사용 만료된 개체를 식별합니다. `introscope.apm.data.preserving.time + introscope.apm.data.agingTime` 보다 오래된 개체는 반환되지 않습니다.

응용 프로그램 심사 맵 시간 만료 처리 속성 구성

응용 프로그램 심사 맵 개체는 `introscope.apm.data.obsolete.time` 속성을 기준으로 사용 만료 표시됩니다. `introscope.apm.data.obsolete.time` 이 기본값 300 DAYS 를 사용하는 경우 300 일보다 오래된 개체는 사용 만료됩니다.

다음 단계를 따르십시오.

1. CA Enterprise Manager 를 종료합니다.
2. `<EM_Home>/config` 디렉터리에 있는 `IntroscopeEnterpriseManager.properties` 파일을 엽니다.
3. `introscope.apm.data.obsolete.time` 속성의 주석 처리가 해제되어 있고 값이 기본값 300 일보다 더 오래된 값으로 설정되어 있는지 확인합니다. HOURS 또는 DAYS 를 지정합니다. 24 시간 또는 1 일이 최소값입니다.
4. `IntroscopeEnterpriseManager.properties` 파일을 저장하고 닫습니다.
5. Enterprise Manager 를 다시 시작합니다. 사용 만료 시간 속성이 구성되었습니다.
6. `<EM_Home>/logs` 디렉터리에서 메시지 로그를 봅니다. 예:
`10/19/12 12:02:13 PM EST [INFO] [Manager] [The APM Data property: introscope.apm.data.obsolete.timeset to value : 2 DAYS]`

참고: 설정된 값보다 더 오래된 개체는 APM 데이터베이스에서 물리적으로 삭제되었으므로 보고될 수 없습니다.

제 15 장: Catalyst 데이터를 로드하도록 APM 구성

이 장에서는 CA Catalyst 데이터를 로드하도록 CA APM 을 구성하는 방법을 설명합니다.

이 섹션은 다음 항목을 포함하고 있습니다.

[CA Catalyst 데이터를 로드하도록 CA APM 구성 \(페이지 258\)](#)

[CatalystPolicy.xml 파일 구성 \(페이지 259\)](#)

CA Catalyst 데이터를 로드하도록 CA APM 구성

Catalyst.properties 파일을 구성하면 CA Catalyst 데이터를 CA APM 으로 로드하여 처리하고 Workstation 에서 해당 데이터를 볼 수 있습니다.

다음 단계를 따르십시오.

1. <EM_Home>\config 디렉터리에 있는 *Catalyst.properties* 파일을 엽니다.
2. Enterprise Manager 를 종료합니다.
3. 다음 필수 속성을 편집합니다.

- *catalyst.host*=<enter your CA Catalyst RESTful APIs location>
- *catalyst.protocol* = <enter the http or https connection>
- *catalyst.port* = <enter your CA Catalyst port number>
- *catalyst.login* =<enter your CA Catalyst user name>
- *catalyst.password* =<enter your CA Catalyst password>

참고: *catalyst.login* 및 *catalyst.password* 속성을 설정하면 Enterprise Manager 가 CA Catalyst 에 로그인할 수 있습니다. Enterprise Manager 가 다시 시작될 때(이 절차의 마지막 단계 참조) PBE(암호 기반 암호화)와 MD5 및 DES(데이터 암호화 표준) 알고리즘을 사용하여 Catalyst 암호가 암호화됩니다.

- *catalyst.rest.entrypoint* = /ssaweb/search
4. (선택 사항) CA Catalyst 경고 필터링 속성을 설정합니다.
 5. *Catalyst.properties* 파일을 저장하고 닫습니다.
 6. (선택 사항) <EM_Home>/config 디렉터리에 있는 *Catalyst.Policy.xml* 파일을 열고 엔터티 경고 연결 규칙을 구성합니다.
 7. *Catalyst.Policy.xml* 파일을 저장하고 닫습니다.
 8. Enterprise Manager 를 다시 시작합니다.

추가 정보:

[CatalystPolicy.xml 파일 구성](#) (페이지 259)

[Catalyst.properties](#) (페이지 513)

CatalystPolicy.xml 파일 구성

CatalystPolicy.xml 파일은 커넥터로 정책 기반 구성의 유연성을 최대화하는 선택적 구성입니다. *CatalystPolicy.xml* 파일을 사용하여 USM 엔터티, 연결된 엔터티 목록, 연결된 관계 목록 등의 규칙을 정의할 수 있습니다. 구성은 정의된 규칙을 기반으로 지정된 엔터티에 대한 경고 검색을 미세 조정합니다.

다음은 XML 파일 구조의 예입니다.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<policy xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" version="0.1"
xsi:noNamespaceSchemaLocation="policy0.1.xsd">
  <entity name="ComputerSystem" alertable="true">
    <include_entities>Processor Memory File Port</include_entities>
    <include_relations>IsComposedOf HasMember</include_relations>
  </entity>
  <entity name="Database" alertable="true">
    <include_entities>Tablespace</include_entities>
    <include_relations>IsManagerFor</include_relations>
  </entity>
  <entity name="DatabaseInstance" alertable="true">
    <include_entities>Tablespace</include_entities>
    <include_relations>IsManagerFor</include_relations>
  </entity>
  <entity name="Group" alertable="false">
    <include_entities>ComputerSystem VirtualSystem</include_entities>
    <include_relations>HasMember</include_relations>
  </entity>
</policy>
```

추가 정보:

[CA Catalyst 데이터를 로드하도록 CA APM 구성 \(페이지 258\)](#)

[Catalyst.properties \(페이지 513\)](#)

제 16 장: CA CEM 소개

CA CEM 은 사용자의 트랜잭션을 모니터링하여 데이터 센터에서 문제의 원인을 격리합니다. CA CEM 은 트랜잭션의 성능과 품질을 측정하고, 결함과 차이를 식별하며, 사용자와 비즈니스에 미치는 영향을 정량화합니다. CA CEM 은 트랜잭션 응답 시간이 저하되는 추세를 사전에 감지하고 실행 가능한 다양한 보고서를 제공하여 문제가 발생하거나 SLA(서비스 수준 계약) 불이행이 발생하기 전에 조치를 취할 수 있게 해 줍니다.

이 섹션은 다음 항목을 포함하고 있습니다.

[CEM 콘솔 및 설정 페이지 액세스](#) (페이지 261)

[CA CEM 관리자의 책임](#) (페이지 264)

CEM 콘솔 및 설정 페이지 액세스

웹 브라우저가 있는 모든 컴퓨터에서 CA CEM 을 설정하고 관리할 수 있습니다.

이 항목에서는 CA CEM 인터페이스와 해당 인터페이스에 액세스하는 방법을 설명합니다.

- [CEM 콘솔에 액세스](#) (페이지 261)
- [TIM 의 "Wily System Setup"\(Wily 시스템 설정\) 페이지 액세스](#) (페이지 263)
- [CEM 콘솔에서 TIM 액세스](#) (페이지 263)

CEM 콘솔 액세스

웹 브라우저가 있는 모든 컴퓨터에서 비즈니스 응용 프로그램, 비즈니스 서비스 및 트랜잭션 정의를 설정하고 관리할 수 있습니다.

CEM 콘솔은 CA CEM 의 주 사용자 인터페이스입니다. 관리자는 이 콘솔을 사용하여 트랜잭션 기록, 트랜잭션 정의 만들기 등을 비롯하여 CA CEM 을 설정하거나 구성하고 분석가는 이 콘솔을 사용하여 보고서를 작성하거나 봅니다.

관리자인 경우 CEM 콘솔에는 추가 메뉴 옵션이 있습니다. 또한 TIM 이 활성화되지 않은 경우 일부 CA CEM 링크가 표시되지 않습니다.

(TIM 을 실행하지 않은 경우 "도구" 및 CA CEM 링크가 표시되지 않습니다.)

다른 설명이 없는 경우 이 안내서에서는 관리자로 CEM 콘솔을 사용한다고 가정합니다.

클러스터 환경에서는 CEM 콘솔이 MOM(Manager of Managers)에 있습니다.

다음 단계를 따르십시오.

1. 웹 브라우저를 열고 다음 주소를 입력합니다.

`http://<IP_Address>:8081/wily`

여기서 <IP_Address>는 MOM 또는 독립 실행형 Enterprise Manager 의 IP 주소나 DNS 이름입니다. 예:

`http://192.168.1.54:8081/wily`

`http://cem.company.com:8081/wily`

DNS 이름은 DNS 관리자가 구성한 경우에만 사용할 수 있습니다.

참고: 기본 포트는 8081 입니다. 기본 포트는 `IntroscopeEnterpriseManager.properties` 파일에 `introscope.enterprisemanager.webserver.port=8081` 로 정의되며 변경할 수 있습니다.

2. 사용자 이름과 암호를 입력합니다.

CA CEM 관리자의 기본 사용자 이름은 `cemadmin` 입니다.

CEM 콘솔이 나타납니다.

보안 및 로그인에 대한 자세한 내용은 *CA APM 보안 안내서*를 참조하십시오.

CA CEM 에 로그인 문제 해결

증상

CA CEM 에 로그인할 수 없으면 브라우저에서 Active 스크립팅을 사용하도록 설정했는지 확인하십시오.

Active 스크립팅을 사용하지 않도록 설정한 경우 CA CEM 로그인 페이지에서 "로그인"을 클릭하면 "CEM 콘솔/뒤로" 페이지로 리디렉션됩니다. 사용자 이름과 암호를 올바르게 입력한 경우에도 마찬가지입니다.

해결 방법

Active 스크립팅을 사용하도록 설정하려면 브라우저의 사용자 설명서를 참조하십시오. 예를 들어 Internet Explorer 8에서는 "인터넷 옵션" > "보안" > "사용자 지정 수준" > "스크립팅" > "Active 스크립팅" 아래에 설정이 있습니다.

TIM 의 "System Setup"(시스템 설정) 페이지 액세스

"TIM System Setup"(TIM 시스템 설정) 페이지에서는 다양한 구성 및 상태 페이지에 액세스할 수 있습니다. 관리자는 일반적으로 상태 정보를 검토하거나 문제 해결을 위해 이러한 페이지를 사용합니다.

다음 단계를 따르십시오.

1. 웹 브라우저를 열고 주소를 입력합니다. 여기서 <IP_Address>는 TIM IP 주소 또는 DNS 이름입니다.

`http://<IP_Address>/cgi-bin/wily/system/index`

예:

`http://192.168.1.54/cgi-bin/wily/system/index`

`http://cem.company.com/cgi-bin/wily/system/index`

DNS 이름은 DNS 관리자가 구성한 경우에만 사용할 수 있습니다.

2. 사용자 이름과 암호를 입력합니다.

"System Setup"(시스템 설정) 페이지의 기본 사용자 이름은 *admin* 입니다.

"System Setup"(시스템 설정) 페이지가 나타납니다.

CEM 콘솔에서 TIM 액세스

TIM 의 IP 주소와 경로를 알고 있는 경우 "System Setup"(시스템 설정) 페이지에서 "TIM Setup"(TIM 설정) 페이지에 액세스할 수 있습니다. 그러나 CEM 콘솔을 연 경우에는 콘솔에서 "TIM Setup"(TIM 설정) 페이지에 액세스할 수 있습니다.

다음 단계를 따르십시오.

1. 관리자 콘솔에서 "설정" > "모니터"를 선택합니다.
2. 맨 오른쪽 열에서 TIM 의 IP 주소를 클릭합니다.

3. "System Setup"(시스템 설정) 페이지의 사용자 이름(*admin*)과 암호를 입력합니다.
"TIM Setup"(TIM 설정) 페이지가 나타납니다.

CA CEM 관리자의 책임

CA CEM 관리자의 책임은 환경의 복잡성, 통합 유형, 사용자 수, 지원 리소스, CA CEM 에서 모니터링되는 응용 프로그램의 성장률 등에 따라 사이트마다 다릅니다.

- [매일 작업](#) (페이지 264)
- [매주 작업](#) (페이지 265)
- [매월 작업](#) (페이지 265)
- [매분기 작업](#) (페이지 266)

매일 작업

다음은 CA CEM 관리자가 매일 수행하는 일반 작업입니다.

- 매일 백업을 수행하고 확인합니다.
- 인시던트를 검토하고 해당하는 경우 결함도 검토합니다. Introscope 를 사용하여 문제를 해결합니다.
- 발견된 CA CEM 문제를 적절한 그룹에 보고합니다.
- TIM 및 IntroscopeEnterpriseManager 로그를 검토합니다.
- 온라인으로 또는 전자 메일 알림을 수신한 후 시스템 이벤트를 검토합니다. 예를 들어 결함이 드롭되고 있는지 검토합니다. [CA CEM 이벤트](#) (페이지 341) [보기](#) (페이지 341) 및 [이벤트에 대한 전자 메일 알림 수신](#) (페이지 341)을 참조하십시오.
- TIM 의 건전성을 검토합니다. [TIM 컴퓨터의 건전성 검토](#) (페이지 343)를 참조하십시오.
- Introscope Workstation 을 사용하여 Enterprise Manager 에서 CA CEM 의 건전성을 검토합니다.

매주 작업

다음은 CA CEM 관리자가 매주 수행하는 일반 작업입니다.

- 백업 및 복원 절차를 테스트합니다.
- CA SiteMinder, CA NSM, CA Service Desk 등과의 통합이 예상한 대로 작동하고 있는지 테스트합니다. 예를 들어 Single Sign-On 이 SiteMinder 웹 에이전트와 함께 제대로 작동하고 있는지 테스트합니다.
- 외부에 CA CEM 구성 및 백업 파일의 복사본을 저장합니다.
- Embedded Entitlements Manager 에서 CA CEM 관리자 목록을 검토하여 필요 없는 관리자를 확인합니다.
- CA CEM 감사 로그를 검토하여 예기치 않았거나 무단인 변경 사항을 확인합니다.
- CA CEM CPU, 디스크 및 시스템 사용률을 검토합니다. [TIM 컴퓨터의 건전성 검토](#) (페이지 343)를 참조하십시오.
- 해결되었거나 오래된 인시던트를 적절히 종결합니다.
- 보고서를 검토하여 정확한지 여부와 추세를 확인합니다.
- 전자 메일 보고서가 예상한 대로 생성되어 배포되는지 확인합니다.
- Introscope 에서 실시간 비즈니스 트랜잭션 메트릭과 사용자 지정 대시보드를 검토합니다.
- CA Service Desk 로그, CA SiteMinder 로그 등의 통합 로그를 검토합니다.
- 증거 수집 로그를 검토합니다. [비즈니스 영향 설정 및 인시던트에 대한 증거 수집](#) (페이지 304)을 참조하십시오.

매월 작업

다음은 CA CEM 관리자가 매월 수행하는 일반 작업입니다.

- 장애 조치 절차를 확인합니다(설치된 경우).
- 오래되었거나 필요 없는 사용자 및 사용자 그룹을 정리합니다.
- 새 비즈니스 서비스/트랜잭션 등을 정의해야 하는지 검토합니다.
- 트랜잭션 사양 설정을 수정해야 하는지 검토합니다.
- 기준 또는 SLA 설정을 조정해야 하는지 검토합니다.
- 매월 보고서를 검토하여 정확한지 여부와 추세를 확인합니다.

- 사용하도록 설정된 트랜잭션과 비즈니스 트랜잭션 통계를 검토하고, 더 이상 모니터링하지 않아도 되는 트랜잭션에 대한 정의를 사용하지 않도록 설정합니다. 트랜잭션 정의 관리에 대한 자세한 내용은 *CA APM 트랜잭션 정의 안내서*를 참조하십시오.
- HTTP 분석기 플러그인을 사용하는 경우 해당 플러그인의 작동을 검토합니다. 예를 들어 플러그인이 필요한 기대치를 충족하고 있는지, 추가로 충족해야 할 요구 사항이 있는지, 마지막 JAR 파일 업데이트 후 성능 저하가 있었는지 등을 검토합니다. *CA APM 트랜잭션 정의 안내서*를 참조하십시오.

매분기 작업

다음은 CA CEM 관리자가 매분기 또는 매년 수행하는 일반 작업입니다.

- CA CEM 아키텍처를 검토하여 성능, 확장성, 장애 조치, 지리적 배포 및 기타 요소를 확인합니다.
- CA CEM 전문 서비스가 CA CEM 사용자 지정이나 통합에 필요한지 확인합니다.
- 다음 CA CEM 릴리스에 대한 베타 테스트를 실시하여 발생 가능한 문제, 새로운 기능을 확인합니다(해당하는 경우).
- 사용자 그룹 정의를 검토합니다. 예를 들어 IP 서브넷 사용자 그룹 규칙을 수정해야 하는지 검토합니다.

제 17 장: CA CEM 에 대한 네트워킹 대안

이 섹션은 다음 항목을 포함하고 있습니다.

[CA CEM 네트워크 옵션 정보](#) (페이지 267)

[네트워크 트래픽 모니터링 정보](#) (페이지 268)

[CA CEM 삽입 위치 정보](#) (페이지 270)

[브라우저에서 Enterprise Manager 로의 연결](#) (페이지 274)

[IPv6 및 CA CEM](#) (페이지 275)

CA CEM 네트워크 옵션 정보

네트워크 내의 여러 위치에 CA CEM 을 배치할 수 있고 여러 대체 방법을 통해 시스템을 네트워크에 연결할 수 있습니다. 이 장에서는 이러한 옵션에 대해 설명합니다.

TIM 과 Enterprise Manager 는 별개의 하드웨어에 상주합니다. Enterprise Manager(수집기 및 MOM(Manager of Managers))에 보고하는 TIM 에 대한 연결을 기본적으로 고려해야 합니다.

TIM 을 배치하는 위치에 대해 선택 가능한 옵션이 여러 가지 있으며 이러한 옵션에 대한 설명은 [CA CEM 삽입 위치 정보](#) (페이지 270)에 나와 있습니다. TIM 위치에 따라 수집 가능한 정보가 결정됩니다.

TIM 의 기본 설정 삽입 지점은 논리적으로 네트워크 부하 분산 장치와 웹 서버 집계 스위치 사이에 있거나, 집계 스위치를 사용하지 않는 경우 부하 분산 장치와 웹 서버 사이에 있습니다. 자세한 내용은 [집계 스위치와 네트워크 부하 분산 장치 사이](#) (페이지 273)를 참조하십시오.

선택한 위치에 TIM 을 설치할 때 네트워크에 연결하는 방법도 선택해야 합니다.

네트워크 트래픽 모니터링 정보

TIM 은 미러링된 포트나 네트워크 탭에 연결될 수 있는 모니터링 인터페이스를 통해 네트워크 트래픽을 읽습니다.

다음 단원에서는 미러링된 포트를 사용하여 패킷을 TIM 에 전달하는 경우와 네트워크 탭을 사용하여 패킷을 TIM 에 전달하는 경우 어떤 영향이 있는지 설명합니다.

- [네트워크 탭 사용](#) (페이지 268)
- [미러링된 포트 사용](#) (페이지 269)

네트워크 탭 사용

네트워크 탭은 인프라 케이블에 직접 연결되는 하드웨어 장치로, 패킷 복사본을 만들어 하나 이상의 대상에 전달합니다. 탭은 물리적 계층의 인프라에 결합되며 라우터나 스위치의 리소스를 사용하지 않습니다. 탭을 삽입하려면 연결을 일시 중지해야 합니다.

탭은 네트워크 지연에 영향을 주지 않습니다. 많은 탭은 두 개의 물리적 인터페이스에서 별도로 송/수신된 트래픽을 전달하므로 TIM 에서 두 개의 물리적 인터페이스를 필요로 합니다. TIM 이 해당 데이터 스트림을 병합해야 하는데, 이 스트림 병합은 TIM 성능에 약간의 영향을 줍니다. 일부 탭은 전이중 방식이며 TIM 에서 추가 인터페이스나 병합을 필요로 하지 않습니다.

탭은 전송 전용 장치이므로 미러링된 포트보다 더 안전할 수 있습니다. 탭의 또 다른 장점은 구성이 비교적 간단하다는 것입니다. 탭은 인라인 장치이므로 장애가 발생할 경우 네트워크 작업이 중단될 수 있으며, 결합 있는 탭을 교체하기 위해 운영을 중단해야 할 수 있습니다(수동 탭이 아닌 경우). 탭 기술의 발전으로 장애가 발생할 확률이 크게 줄어들었습니다.

미러링된 포트 사용

미러링된 포트(Cisco 용어에서는 SPAN 포트)는 네트워크 라우터와 스위치의 소프트웨어 기능입니다. Cisco 6500 시리즈 스위치와 같은 최신 스위치에서는 SPAN 포트를 사용하도록 설정해도 스위치 성능이 영향을 받지 않습니다. 미러링된 포트를 사용하여 프로토콜 분석기와 같은 네트워크 문제 해결 장치를 연결하는 경우가 자주 있습니다. 스위치가 지원하는 미러링된 포트 수에는 한계가 있으므로 경우에 따라 네트워크 엔지니어가 장치를 이러한 유지 관리 포트에 영구적으로 연결하기를 꺼리기도 합니다.

미러링된 포트가 라우터나 스위치의 소프트웨어 기능이므로 미러링된 포트를 사용하는 경우 인프라를 변경하지 않아도 되고 탭을 사용하는 경우보다 지장이 덜합니다. 추가 비용을 들여야 하는 탭과는 달리, 이미 배포된 스위치는 일반적으로 추가 비용 없이 미러링된 포트를 지원할 수 있습니다.

미러링된 포트는 네트워크 지연에 영향을 주지 않습니다. TIM 에 필요한 인터페이스를 줄이기 위해 미러링된 포트가 발송 및 수신 트래픽을 전달하기 전에 결합하는 경우가 자주 있습니다. 이 구성에서는 TIM 이 여러 인터페이스의 데이터 스트림을 병합하지 않아도 되므로 성능이 다소 향상됩니다.

잘못된 구성 변경으로 인해 미러링된 포트가 양방향 스위치 포트 구성될 수 있지만 미러링된 포트는 대부분의 경우 전송 전용 포트입니다. 따라서 미러링된 포트가 탭보다 덜 안전한 것으로 간주되는 경우도 있습니다. TIM 소프트웨어는 TIM 으로 인해 보안 위험이 발생하지 않도록 하기 위해 모니터링 포트에서 전송하지 않습니다.

참고: 사용 중인 응용 프로그램에 서로 다른 스위치 두 개를 통해 들어오는 최종 사용자 트래픽이 있는 경우 두 스위치 모두의 트래픽을 동일한 TIM 에 미러링할 수 있습니다. 이렇게 하려면 네트워크 카드(다중 포트 NIC)를 구하여 배포해야 합니다. 네트워크 카드 지원에 대한 자세한 내용은 *CA APM Compatibility Guide*(CA APM 호환성 안내서)를 참조하십시오.

CA CEM 삽입 위치 정보

인프라 내의 TIM 삽입 위치는 수집되는 정보에 영향을 줍니다.

TIM 은 모니터링 인터페이스를 통해 네트워크 트래픽을 읽습니다. 이전 단원에서 설명한 대로 모니터링 인터페이스는 미러링된 포트에도 연결할 수 있고 네트워크 탭에도 연결할 수 있습니다. 두 경우 모두 TIM 은 해당 패킷의 복사본을 수신하여 분석하고 삭제합니다. TIM 은 모니터링 포트에서 전송하지 않습니다. 트래픽은 TIM 으로 향하는 단방향 트래픽이고 TIM 은 모니터링 포트의 패킷만 수신하도록 구성되어 있습니다.

대규모 엔터프라이즈의 일반적인 네트워크 인프라에는 TIM 모니터링 포트를 삽입할 위치가 많습니다. 다이어그램에는 다양한 삽입 위치가 나와 있습니다.

참고: 대부분의 환경에서는 중복 인프라를 사용하지만 이 다이어그램에서는 단순화를 위해 경로를 하나만 보여 줍니다.



왼쪽에서 오른쪽으로 다이어그램을 살펴보면 패킷은 인터넷 라우터를 통해 엔터프라이즈로 들어옵니다. 삽입 위치 A 는 라우터 외부, 즉 인터넷과 라우터 사이에 있습니다.

이 라우터는 일반적으로 트래픽을 방화벽에 전달하고 삽입 위치 B 는 라우터와 이 방화벽 사이에 있습니다. 방화벽은 인바운드 및 아웃바운드 트래픽을 검사하고 엔터프라이즈의 보안 정책에 따라 트래픽을 차단하거나 수락할 수 있습니다. 방화벽이 NAT(Network Address Translation)를 수행하여 인터넷에 대한 직접 연결로부터 엔터프라이즈의 네트워크 연결 장치를 보호할 수도 있습니다.

참고: 경우에 따라 집계 스위치와 네트워크 부하 분산 장치가 동일한 장치에 들어 있기도 합니다.

삽입 위치 C는 방화벽과 집계 스위치/네트워크 부하 분산 장치 사이에 있습니다. 수락 가능한 트래픽은 방화벽에서 집계 스위치/네트워크 부하 분산 장치로 전달됩니다. 집계 스위치/네트워크 부하 분산 장치가 SSL 세션을 종료하고 클라이언트가 연결할 VIP(가상 IP 주소)를 인스턴스화할 수 있는 경우가 많습니다. 많은 집계 스위치/네트워크 부하 분산 장치는 프록시 역할을 하면서 클라이언트로부터 시작된 연결을 종료하고 클라이언트 대신 웹 서버에 연결합니다. 일부 집계 스위치/네트워크 부하 분산 장치는 웹 서버에 대한 영구 연결을 설정하고 사용하여 웹 서버에 걸리는 부하를 줄입니다.

집계 스위치가 패킷을 네트워크 부하 분산 장치에 전달하는 경우가 많습니다. 삽입 위치 D는 집계 스위치와 네트워크 부하 분산 장치 사이에 있습니다.

마지막으로 웹 서버가 집계 스위치에 연결되거나 네트워크 부하 분산 장치에 바로 연결됩니다. 삽입 위치 E는 웹 서버 바로 앞, 집계 스위치와 웹 서버 사이에 있거나 네트워크 부하 분산 장치와 웹 서버 사이에 있습니다.

패킷은 반대 경로를 따라 엔터프라이즈에서 나가면서 역순으로 각 삽입 위치를 통과합니다. 패킷이 한 경로를 따라 들어왔다가 다른 경로를 따라 나가는 삼각형 구조도 가능합니다. 또는 패킷이 웹 서버에서 나가 인터넷으로 바로 이동할 수도 있습니다.

인터넷과 인터넷 라우터 사이

인터넷과 인터넷 라우터 사이에 있는 삽입 위치 A는 클라이언트 IP 주소에서는 항상 표시되지만



서버의 IP 주소나 MAC 주소에서는 거의 표시되지 않습니다. CA CEM의 제외 기반 관계 검색 메커니즘에서는 문제 해결 속도를 높이기 위해 웹 서버의 IP 주소나 MAC 주소를 사용하여 수집되는 증거 집합을 제한합니다. 이 정보가 없을 경우 증거 수집이 계속해서 작동하지만 증거 집합이 줄어들지 않으며 기술자가 분석해야 하는 정보가 제외 기반 검색을 사용할 경우보다 더 많습니다.

TIM 이 클라이언트 IP 주소를 사용자 식별에 사용하지 않으므로 삽입 위치 A 를 사용할 경우 장점은 별로 없고 단점은 많습니다.

인터넷 라우터와 방화벽 사이

인터넷 라우터와 방화벽 사이에 있는 삽입 위치 B 는 클라이언트 IP 주소에서는 거의 항상 표시되지만

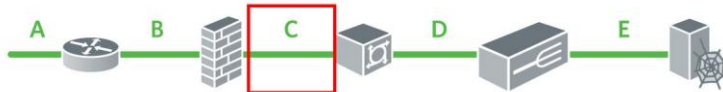


서버의 IP 주소나 MAC 주소에서는 거의 표시되지 않습니다. CA CEM 의 제외 기반 관계 검색 메커니즘에서는 문제 해결 속도를 높이기 위해 웹 서버의 IP 주소나 MAC 주소를 사용하여 수집되는 증거 집합을 제한합니다. 이 정보가 없을 경우 증거 수집이 계속해서 작동하지만 증거 집합이 줄어들지 않으며 기술자가 분석해야 하는 정보가 제외 기반 검색을 사용할 경우보다 더 많습니다.

TIM 이 클라이언트 IP 주소를 사용자 식별에 사용하지 않으므로 삽입 위치 B 를 사용할 경우 장점은 별로 없고 단점은 많습니다.

방화벽과 집계 스위치 사이

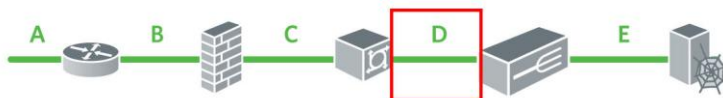
방화벽과 집계 스위치 사이에 있는 삽입 위치 C 는 클라이언트 IP 주소를 파악할 수 있는 가시성을 거의 항상 제공합니다. 삽입 위치 C 는 서버의 IP 주소를 파악할 수 있는 가시성을 거의 제공하지 않습니다.



TIM 이 클라이언트 IP 주소를 사용자 식별에 사용하지 않으므로 삽입 위치 C 를 사용할 경우 장점은 별로 없고 단점은 많습니다. 일부 환경에서는 삽입 위치 A 와 B 에 비해 삽입 위치 C 가 미미한 이점을 제공합니다.

집계 스위치와 네트워크 부하 분산 장치 사이

집계 스위치와 네트워크 부하 분산 장치 사이에 있는 **삽입 위치 D**는 클라이언트 IP 주소를 파악할 수 있는 가시성을 제공하는 경우가 많습니다. 이렇게 하려면 프록시 역할을 하고 있는 네트워크 부하 분산 장치에서 "원본 주소 유지" 기능이 사용되도록 설정해야 합니다. 삽입 위치 D는 서버의 IP 주소를 파악할 수 있는 가시성을 거의 항상 제공합니다.



네트워크 부하 분산 장치가 영구 연결을 사용하는 경우 **TIM**이 여기에 위치하면 **TIM**에 걸리는 부하가 감소합니다. 부하를 줄이는 것은 열린 연결의 감소 정도에 따라 크게 달라질 수 있습니다. 네트워크 부하 분산 장치가 클라이언트를 대신하여 **SSL**을 종료하는 경우 트래픽을 다시 암호화하지 않으면 거의 항상 **TIM**에 걸리는 부하가 상당히 더 줄어듭니다.

Resonate 등의 일부 부하 분산 환경에서는 **MAC** 주소로 서버를 식별할 수 있지만 많은 환경에서 반환되는 서버 **IP** 주소와 서버 **MAC** 주소는 네트워크 부하 분산 장치 **VIP**(가상 **IP** 주소)의 서버 **IP** 주소와 서버 **MAC** 주소입니다.

TIM이 서버 **IP** 주소를 증거 수집에 사용하므로 삽입 위치 **D**를 사용할 경우 장점은 상당하지만 단점은 사실상 없습니다. 삽입 위치 **D**는 **TIM**에 대한 기본 설정 삽입 위치입니다.

네트워크 부하 분산 장치와 웹 서버 사이

네트워크 부하 분산 장치와 웹 서버 사이에 있는 **삽입 위치 E** 는 클라이언트 IP 주소를 파악할 수 있는 가시성을 제공하는 경우가 많습니다. 이렇게 하려면 프록시 역할을 하고 있는 네트워크 부하 분산 장치에서 "원본 주소 유지" 기능이 사용되도록 설정해야 합니다. 삽입 위치 E 는 서버의 IP 주소를 파악할 수 있는 가시성을 거의 항상 제공합니다.



네트워크 부하 분산 장치가 영구 연결을 사용하는 경우 **TIM** 이 여기에 위치하면 **TIM** 에 걸리는 부하가 감소합니다. 부하를 줄이는 것은 열린 연결의 감소 정도에 따라 크게 달라질 수 있습니다. 네트워크 부하 분산 장치가 클라이언트를 대신하여 **SSL** 을 종료하는 경우 트래픽을 다시 암호화하지 않으면 거의 항상 **TIM** 에 걸리는 부하가 상당히 더 줄어듭니다.

TIM 이 서버 IP 주소를 증거 수집에 사용하므로 삽입 위치 E 를 사용할 경우 장점이 상당합니다. 그러나 삽입 위치 D 에 없는 일부 단점이 삽입 위치 E 에 있습니다. 많은 웹 서버가 있을 수 있으므로 삽입 위치도 많을 수 있습니다. 따라서 탭을 삽입 위치 E 에 사용하는 것이 실용적이지 않을 수 있습니다.

포트 미러링을 사용하는 경우에는 삽입 위치 D 와 삽입 위치 E 의 기능이 같습니다. 대개의 경우 **VLAN(가상 LAN)** 스페닝만 수행하면 삽입 위치 E 를 사용할 수 있습니다. 삽입 위치 D 에 대해서는 간단한 포트 미러링으로 충분할 수 있습니다.

브라우저에서 Enterprise Manager 로의 연결

기본적으로 브라우저와 Enterprise Manager 간의 HTTP 액세스가 허용되지만

Enterprise Manager 에 대한 액세스를 제한하여 **SSL** 연결만 허용할 수 있습니다. **CA APM 보안 안내서**를 참조하십시오.

IPv6 및 CA CEM

이 단원에서는 IPv6(인터넷 프로토콜 버전 6) 및 IPv6 네트워크에서의 CA CEM 컴퓨터 설정 페이지와 CA CEM 에서 IPv6 주소 형식을 지정하는 방법에 대해 간략히 설명합니다.

- [IPv6 정보](#) (페이지 275)
- [CA CEM 에서 IPv6](#) (페이지 275)
- [IPv6 네트워크 트래픽 모니터링](#) (페이지 276)
- [이중 스택\(IPv6 및 IPv4\) 호스트에서 CA CEM 실행](#) (페이지 276)
- [허용되는 IPv6 주소 형식](#) (페이지 278)

IPv6 정보

향후 몇 년 안에 IPv4(인터넷 프로토콜 버전 4) 주소 수가 고갈될 것으로 예상됩니다. IPv6 은 사용 가능한 인터넷 주소 수를 늘립니다.

IPv6 주소는 128 비트(16 바이트)로, 대개 각각의 16 비트 그룹이 콜론(:)으로 구분되는 16 진수 표기법으로 작성됩니다. 예를 들어 2001:0db8:30d2:55c9:06ff:e579:5aa4 와 같습니다.

반대로 IPv4 주소는 32 비트(4 바이트)로, 대개 각 바이트가 점(.)으로 구분되는 10 진수 표기법으로 작성됩니다. 예를 들어 172.24.131.197 과 같습니다.

CA CEM 에서 IPv6

CA CEM 에는 다음 두 가지 IPv6 지원 요소가 있습니다.

- IPv6 네트워크 트래픽 모니터링
- IPv6 네트워크에서 CA CEM 구성

이 두 요소는 서로 간에 종속되지 않습니다. 예를 들어 CA CEM 컴퓨터를 IPv4 네트워크에 배치하고 IPv6 및 IPv4 네트워크 트래픽을 모니터링할 수 있습니다. 마찬가지로, CA CEM 컴퓨터를 IPv6 또는 이중 스택 네트워크에 배치하고 IPv6 및 IPv4 네트워크 트래픽을 모니터링할 수도 있습니다.

IPv6 네트워크 트래픽 모니터링

CA CEM 은 IPv4 주소와 IPv6 주소를 모두 지원합니다. 필드에 IP 주소 또는 서브넷 마스크를 입력하는 경우 IPv4 주소나 IPv6 주소를 입력할 수 있습니다.

IPv6 네트워크 트래픽을 모니터링하려면

- IPv4 트래픽을 모니터링하는 경우와 동일한 방식으로 CA CEM 을 설정합니다. 해당하는 경우 IPv4 주소와 호스트 이름 대신 IPv6 주소와 호스트 이름을 입력합니다.

[허용되는 IPv6 주소 형식](#) (페이지 278)을 참조하십시오.

이중 스택(IPv6 및 IPv4) 호스트에서 CA CEM 실행

CA CEM 을 설정하고 설치하는 경우 SE 또는 지원 담당자가 제공하거나 *CA APM 설치 및 업그레이드 안내서*에 지정된 지침을 따르십시오. 이중 스택 호스트이므로 IPv4 및 IPv6 주소가 Enterprise Manager 와 TIM 컴퓨터에 할당됩니다.

중요! TIM 에 IPv6 주소가 할당되면 TIM 수집 서비스를 실행하는 Enterprise Manager 에도 IPv6 주소를 할당해야 합니다. 마찬가지로, TIM 에 IPv4 주소가 할당되어 있으면 TIM 수집 서비스를 실행하는 Enterprise Manager 에도 IPv4 주소가 할당되어 있어야 합니다.

이 중요한 제약 조건은 CA CEM 콘솔에 적용됩니다. 예를 들면 다음과 같습니다.

- 사용하도록 설정된 TIM 에 IPv6 주소가 할당되어 있으면 IPv4 주소가 할당된 Enterprise Manager 에서 TIM 수집 서비스를 실행할 수 없고 반대의 경우도 마찬가지입니다.
- 사용하도록 설정된 TIM 에 IPv6 주소가 할당되어 있으면 IPv4 주소가 할당된 TIM 을 사용할 수 없고 반대의 경우도 마찬가지입니다.

- Enterprise Manager 와 사용하도록 설정된 TIM 간에 주소 유형 불일치를 초래할 경우 TIM 수집 서비스를 실행 중인 Enterprise Manager 의 IP 주소를 변경할 수 없습니다.
- Enterprise Manager 와 사용하도록 설정된 TIM 간에 주소 유형 불일치를 초래할 경우 TIM 수집 서비스를 다른 Enterprise Manager 로 이동할 수 없습니다.

구성에 대한 확인, 수정 또는 문제 해결 작업이 필요한 경우 다음 절차를 따르십시오.

TIM 에서 CA CEM 의 IPv6 설정을 검토하거나 수정하려면

1. TIM 에서 "Wily System Setup"(Wily 시스템 설정) 페이지에 액세스합니다. [TIM 의 "Wily System Setup"\(Wily 시스템 설정\) 페이지 액세스](#) (페이지 263)를 참조하십시오.
2. "Wily System Setup"(Wily 시스템 설정) 페이지에서 "Machine Settings"(컴퓨터 설정) > "Configure IPv6"(IPv6 구성)을 선택합니다. IPv6 주소가 올바르게 할당되었고 IPv6 이 사용하도록 설정되었는지 확인합니다.

"IPv6 Setup"(IPv6 설정) 페이지에 대해 참고해야 할 사항은 다음과 같습니다.

- 전역 범위 IPv6 주소는 IPv4 주소와 비슷합니다.
 - RADV 와 DHCPv6 이 둘 이상의 전역 IPv6 주소를 컴퓨터에 할당할 수 있지만 수동으로 할당할 수 있는 주소는 하나뿐입니다.
 - IPv6 주소를 수동으로 할당하는 경우 슬래시 표기법을 사용하여 네트워크 접두사 길이를 나타내십시오. 이는 IPv4 네트워크의 서브넷 마스크를 지정하는 것과 유사합니다.
 - "클릭하여 사용 안 함" 단추는 문제 해결용으로 예약되어 있습니다. 예를 들어 IPv6 네트워크를 통해 CA CEM 컴퓨터와 통신할 수 없으면 IPv6 이 시스템 전체와 관리 네트워크(ethn)에 연결된 인터페이스 모두에 사용하도록 설정되었는지 확인합니다.
3. IPv4 설정이 올바르게 할당되었는지 확인합니다. 이렇게 하려면 "Machine Settings"(컴퓨터 설정)로 돌아가서 "Network Setup"(네트워크 설정)을 선택합니다.

이중 스택 Enterprise Manager 의 IP 주소를 변경하려면

- [Enterprise Manager 의 IP 주소 편집](#) (페이지 288)을 참조하십시오.

사용 중인 브라우저가 CA CEM 콘솔을 가리키도록 하려면

- 콘솔의 URL 에 리터럴 IP 주소를 사용하는 경우 [] (대괄호) 표기법을 사용하여 IPv6 주소를 표시하십시오.

[허용되는 IPv6 주소 형식](#) (페이지 278)의 경로 예제를 참조하십시오.

허용되는 IPv6 주소 형식

IPv6 주소에 사용되는 표기법은 CEM 콘솔에서 지정하는지 "Wily System Setup"(Wily 시스템 설정) 페이지에서 지정하는지에 따라 다릅니다.

- CEM 콘솔 - CEM 콘솔에 IPv6 주소를 입력할 때는 다음과 같은 경우를 제외하고 압축 표기법을 사용할 수 *없습니다*.
 - 서브넷 마스크를 지정하는 경우. 압축 표기법 및 슬래시 표기법이 모두 허용됩니다.
 - "관리" > "기록 세션" 페이지에서 클라이언트 IP 주소를 지정하는 경우. 압축 표기법 및 혼합 표기법을 모두 사용할 수 있습니다.

UI 에서 제공된 예제를 따라야 합니다.

- "Wily System Setup"(Wily 시스템 설정) 페이지 - "IPv6 Setup"(IPv6 설정) 페이지와 같은 "Wily System Setup"(Wily 시스템 설정) 페이지에서는 압축 표기법과 더 긴 표기법을 사용하여 IPv6 주소를 지정할 수 *있습니다*.

"IPv6 Setup"(IPv6 설정) 페이지에서는 서브넷 마스크 대신 슬래시로 주소와 구분된 접두사 길이를 사용해야 합니다.

다음 표에는 CA CEM 에서 허용되는 IPv6 주소 표기법의 예가 나와 있습니다.

예제 IPv6 주소	표기법 및 참고 사항
3fff:ffff:0ed5:0000:0000:0000:2448:78eb	표준 표기법: CA CEM 의 어디서나 사용할 수 있습니다.
3fff:ffff:ed5:0:0:0:2448:78eb	16 비트 그룹 내에서 앞에 오는 0 을 제거하는 표기법: CA CEM 의 어디서나 사용할 수 있습니다.

예제 IPv6 주소	표기법 및 참고 사항
<code>3fff:ffff:fed5::2448:78eb</code>	압축 표기법: "관리" > "기록 세션" 페이지에서 서브넷 마스크에 슬래시 표기법을 사용하는 경우를 제외하고는 CEM 콘솔 UI 에서 사용하지 마십시오.
<code>3fff:ffff:fed5:0::/64</code>	슬래시 표기법: 서브넷 마스크("설정" > "도메인" > "Subnet Mask and Administration"(서브넷 마스크 및 관리) > "사용자 그룹")와 수동 IPv6 주소("Wily System Setup"(Wily 시스템 설정) > "Machine Settings"(컴퓨터 설정) > "Configure IPv6"(IPv6 구성))에 사용하십시오.
<code>ffff:ffff:ffff:ffff:0:0:0:0</code>	서브넷 마스크: 서브넷 마스크("설정" > "도메인" > "Subnet Mask and Administration"(서브넷 마스크 및 관리) > "사용자 그룹")에 사용하십시오.
<code>2001:0db8:85a3:08d3:0:0:172.31.124.132</code>	혼합 표기법 IPv4 및 IPv6: "관리" > "기록 세션" 페이지에서 지정하는 경우를 제외하고는 CA CEM 에서 사용하지 마십시오.

다음 표에는 CA CEM 에서 허용되는 IPv6 경로 표기법의 예가 나와 있습니다.

예제 IPv6 경로	표기법 및 참고 사항
<code>http://cemhost_ipv6:8081/wily</code>	cemhost_ipv6 이 호스트 이름으로 정의된 CEM 콘솔의 예제 경로입니다.
<code>http://[2001:db8:85a3:8d3:0:0:370:7348]:8081/wily</code>	Enterprise Manager IP 주소가 IPv6 인 CEM 콘솔의 예제 경로입니다.

제 18 장: CA CEM 관리

이 섹션은 다음 항목을 포함하고 있습니다.

- [CA CEM 관리 프로세스](#) (페이지 281)
- [Enterprise Manager 서비스 배포](#) (페이지 282)
- [CA CEM 도메인 정의](#) (페이지 293)
- [인시던트 원가와 비즈니스 영향의 비교](#) (페이지 298)
- [인시던트 관련 설정 정의](#) (페이지 299)
- [SMTP 서버 설정 구성](#) (페이지 309)
- [새 비즈니스 서비스에 대한 보안 그룹 설정](#) (페이지 311)
- [모니터 사용](#) (페이지 315)
- [모니터 동기화](#) (페이지 315)
- [마지막 동기화 이후의 구성 변경 사항 보기](#) (페이지 316)

CA CEM 관리 프로세스

다음 목록에서는 CA CEM 관리와 관련된 주요 작업을 보여 줍니다.

- 여러 Enterprise Manager 에 Enterprise Manager 서비스를 배포합니다. [Enterprise Manager 서비스 배포](#) (페이지 282)를 참조하십시오.
- 사용자 인식, 사용자 그룹, 트랜잭션, 데이터 보존 등에 대한 설정을 포함하여 도메인을 정의합니다. [CA CEM 도메인 정의](#) (페이지 293)를 참조하십시오.
- 인시던트 생성, 비즈니스 영향 및 증거 수집, 인시던트 만료 처리 규칙, 인시던트 발생 시 전자 메일 발송 등에 대한 인시던트 설정을 지정합니다. [인시던트 관련 설정 정의](#) (페이지 299)를 참조하십시오.
- 보고 및 이벤트 알림에 대한 전자 메일 설정을 정의합니다. [SMTP 서버 설정 구성](#) (페이지 309)을 참조하십시오.
- 새 비즈니스 서비스에 대한 기본 보안 그룹을 설정합니다. [새 비즈니스 서비스의 보안 그룹 설정](#) (페이지 311)을 참조하십시오.
- TIM 을 사용하도록 설정합니다. 이 작업은 설치할 때와 TIM 이 사용하지 않도록 설정되었을 때 필요합니다. 그러면 수집기와 TIM 간에 통신할 수 있습니다. [모니터 사용](#) (페이지 315)을 참조하십시오.

7. 모니터를 동기화합니다. 이 작업은 트랜잭션 및 결합 구성 정보를 TIM 에 전송하고 TIM 이 업데이트된 구성으로 모니터링을 시작하도록 할 때 필요합니다.

비즈니스 서비스 및 트랜잭션과 관련된 구성 변경 사항을 Introscope Agent 에 전송할 때도 필요합니다. [모니터 동기화](#) (페이지 315)를 참조하십시오.

Enterprise Manager 서비스 배포

둘 이상의 EM(Enterprise Manager)이 있는 경우, 즉 수집기와 MOM 이 있는 경우 Enterprise Manager 에 Enterprise Manager 서비스를 배포할 수 있습니다. 서비스를 배포하지 않으면 모든 Enterprise Manager 서비스가 하나의 Enterprise Manager 에서 실행되므로 경우에 따라 성능이 최적화되지 않을 수도 있습니다.

참고: 사용 중인 시스템에 하나의 독립 실행형 Enterprise Manager 만 있으면 이 항목을 건너뛸 수 있습니다. Enterprise Manager 가 독립 실행형인 경우에는 하나의 Enterprise Manager 에서 모든 Enterprise Manager 서비스를 실행해야 합니다.

다중 Enterprise Manager 환경에서 CA APM 을 시작하면 모든 Enterprise Manager 서비스가 첫 번째 수집기에서 시작됩니다. 모든 수집기가 시작된 후에는 Enterprise Manager 서비스를 적절한 Enterprise Manager 에 할당할 수 있습니다.

다음 표에서는 Enterprise Manager 서비스 작업을 수행할 시기를 보여 줍니다.

참고: TESS 서비스는 MOM 이 아니라 수집기에서 실행됩니다.

시기	수행할 작업
CA APM 을 처음 설정하는 경우	Enterprise Manager 서비스 배포 (페이지 282) Enterprise Manager 구성 수정 (페이지 288)
사용자 환경에 Enterprise Manager 를 추가하는 경우	Enterprise Manager 서비스 배포 (페이지 282) Enterprise Manager 구성 수정 (페이지 288)

사용자 환경에서 Enterprise Manager의 IP 주소를 변경하는 경우 [Enterprise Manager 구성 수정](#) (페이지 288)

사용자 환경에서 Enterprise Manager를 제거하는 경우 [Enterprise Manager 서비스 배포](#) (페이지 282)(Enterprise Manager를 종료하기 전에 Enterprise Manager에서 Enterprise Manager 서비스를 이동하려는 경우)

[Enterprise Manager 제거](#) (페이지 289)

다음 Enterprise Manager 서비스를 배포할 수 있습니다.

참고: 클러스터에서는 각 서비스의 인스턴스를 하나만 실행할 수 있습니다. 예를 들어 TIM 수집 서비스가 두 Enterprise Manager에서 동시에 실행되면 안 됩니다.

DB 정리 서비스

데이터베이스에서 오래된 데이터를 삭제합니다.

통계 집계 서비스

하루에 한 번씩 데이터베이스 통계를 집계합니다. 기본적으로 집계는 자정 무렵에 수행됩니다. 자세한 내용은 [CA CEM 보고서 집계 정보](#) (페이지 347)를 참조하십시오.

TIM 수집 서비스

TIM이 없는 경우, 즉 Introscope는 실행 중이지만 CA APM은 실행 중이 아닌 경우에는 이 서비스의 위치가 문제되지 않습니다.

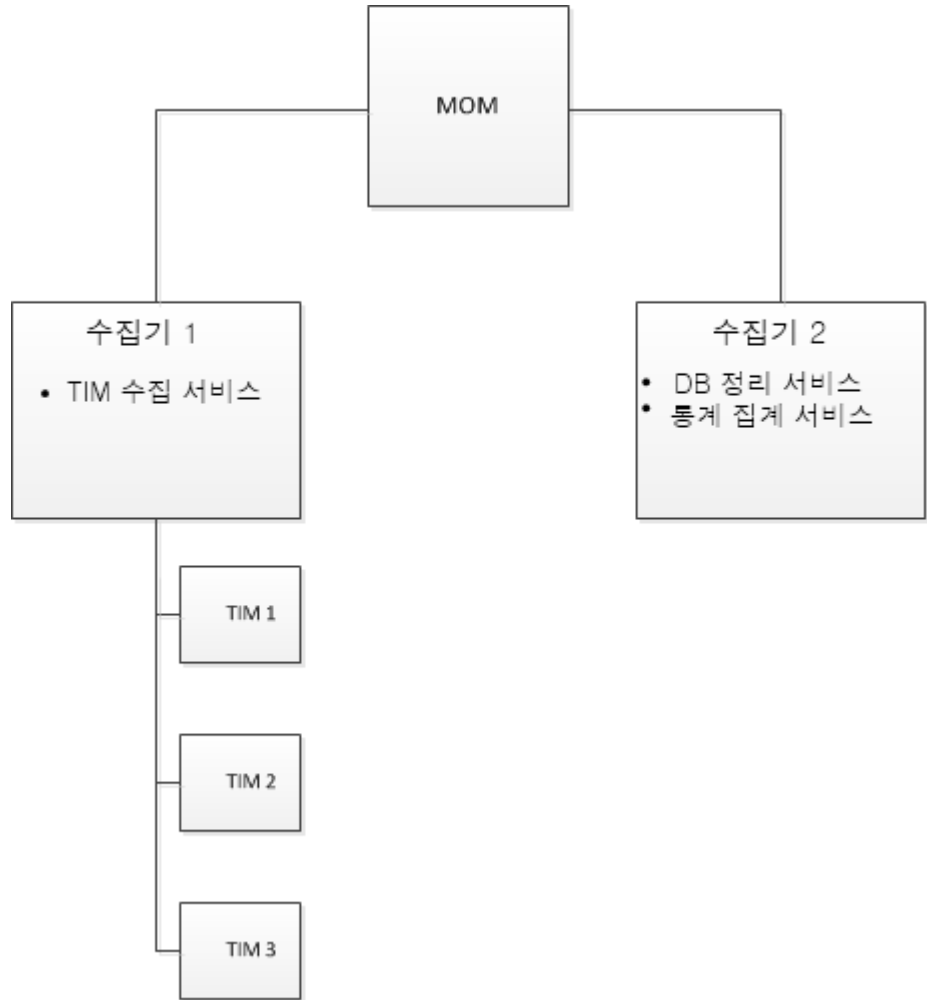
이 서비스는 TIM에서 수집된 데이터를 처리하는 데 사용되는 서비스 그룹으로 구성됩니다. 로그인, 결합, 기록, CA CEM 이벤트, 매시간 통계, 고객 경험 매트릭 및 트랜잭션 검색을 처리하기 위한 서비스를 포함합니다.

참고: TIM 수집 서비스는 가장 계산량이 많은 Enterprise Manager 서비스입니다.

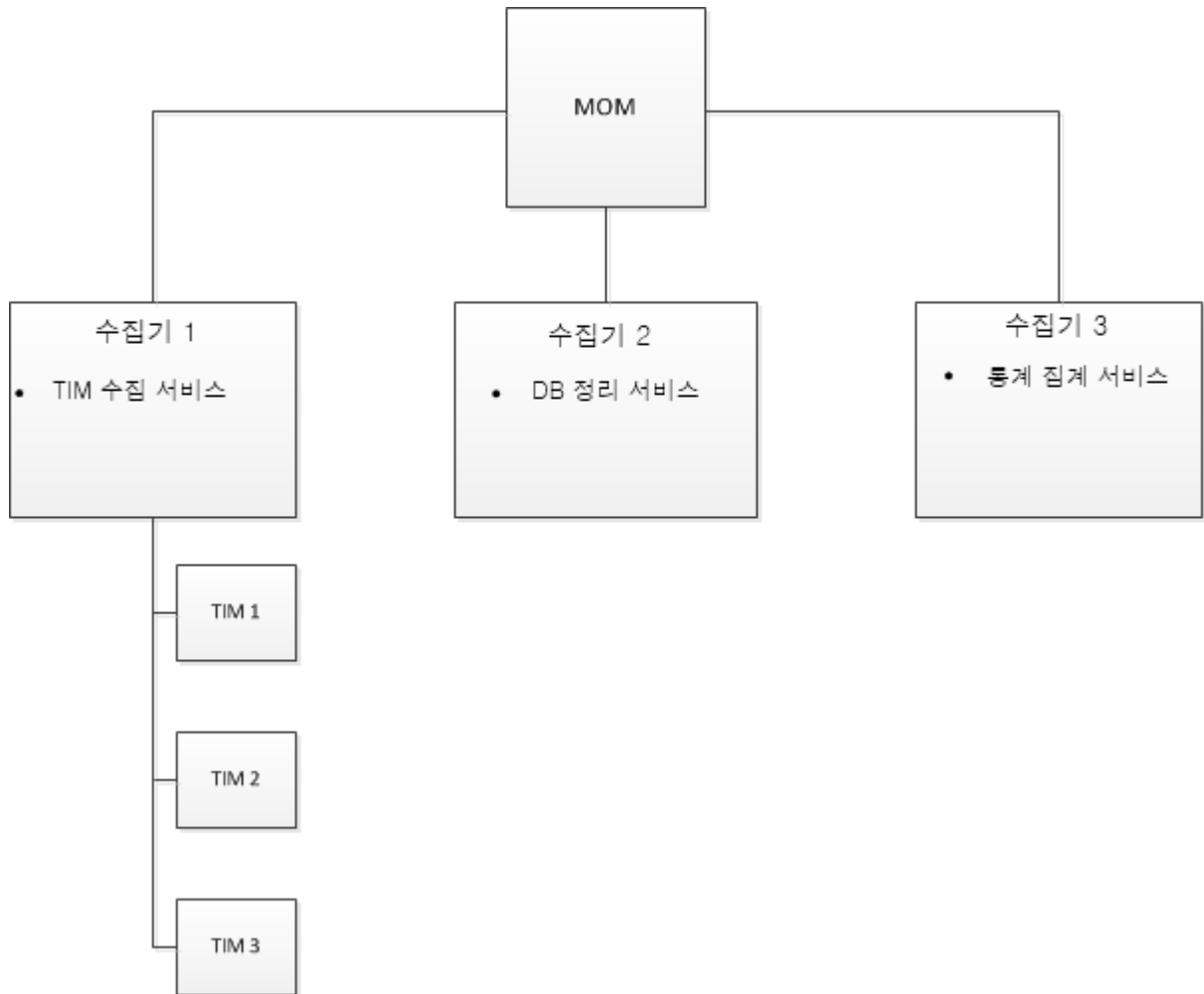
다른 Enterprise Manager 서비스는 모든 Enterprise Manager에 할당됩니다. 이러한 서비스는 배포할 수 없으므로 "서비스" 페이지에 표시되지 않습니다.

Enterprise Manager 서비스의 일반적인 배포

다음 그림은 수집기가 두 개인 환경의 일반적인 Enterprise Manager 서비스 배포를 보여 줍니다.



다음 그림은 수집기가 세 개인 환경의 일반적인 Enterprise Manager 서비스 배포를 보여 줍니다.



클러스터 환경의 Enterprise Manager 서비스 배포

이 절차에서는 Enterprise Manager 에 Enterprise Manager 서비스를 다시 배포합니다. 예를 들어 CA APM 을 처음 시작할 때와 Enterprise Manager 를 시스템에 추가하거나 시스템에서 제거할 때 이 절차를 수행하십시오.

중요! Enterprise Manager 서비스를 종료하려면 Enterprise Manager 에서 먼저 이 서비스를 제거하십시오.

이 절차의 목적은 Enterprise Manager 에 작업 부하를 분산하는 것입니다.

참고: TIM 수집 서비스를 다른 Enterprise Manager 로 이동한 경우 원래 Enterprise Manager 로 다시 이동하지 않으면 원래 Enterprise Manager 에 처리되지 않은 채로 남아 있는 데이터 파일이 처리되지 않습니다. 자세한 내용은 [잘못된 파일의 디렉터리 위치 변경](#) (페이지 588)을 참조하십시오.

피크 시간 이외의 시간을 선택하여 Enterprise Manager 서비스를 다시 배포하는 것이 좋습니다. 피크 시간에 서비스를 종료하고 이동할 경우 처리 지연이 발생할 수 있습니다.

클러스터 환경에서 Enterprise Manager 서비스를 배포하려면

1. "설정", "서비스", "서비스 구성"을 차례로 선택합니다.
"서비스 구성" 페이지에 현재 각 서비스를 실행 중인 Enterprise Manager 에 대한 개요가 표시됩니다.
2. DB 정리 서비스와 같이 다른 Enterprise Manager 에 할당할 서비스를 클릭합니다.
3. Enterprise Manager 목록에서 서비스를 할당할 Enterprise Manager 를 선택하고 "저장"을 클릭합니다.
목록에 클러스터의 모든 Enterprise Manager 가 나타납니다. Enterprise Manager 가 작동 중인지 또는 중지되었는지 확인할 수 있습니다.
참고: MOM 은 목록에 표시되지 않습니다.
바이러스 백신으로 인해 서비스가 과도하게 느려질 수 있으므로 TIM 수집 서비스를 실행 중인 Enterprise Manager 에서는 바이러스 백신 소프트웨어를 실행하지 않는 것이 좋습니다.
4. 각각의 Enterprise Manager 서비스가 원하는 Enterprise Manager 에서 실행되고 있을 때까지 2 단계와 3 단계를 반복합니다.
5. "저장"을 클릭합니다.

실시간 트랜잭션 메트릭을 위한 TIM 선택

기본적으로 실시간 트랜잭션 메트릭 데이터는 모든 TIM 에서 수집됩니다. 그러나 사용자 환경의 TIM 중 일부만이 참여하도록 지정할 수 있습니다. 테스트 또는 문제 해결 상황에서 이렇게 지정해야 할 수 있습니다.

다음 단계를 따르십시오.

1. "설정", "서비스"를 차례로 선택합니다.
2. "TIM 수집 서비스"를 클릭합니다.
3. "TIM 수집 서비스" 메뉴에서 "RTTM 수집 서비스"를 아직 선택하지 않았으면 선택합니다.

실시간 트랜잭션 메트릭에 참여하고 있는 TIM 은 TIM 목록에 사용 가능한 것으로 표시됩니다.

4. 필요한 경우 목록에서 TIM 을 선택하거나 선택 취소합니다.
5. "저장"을 클릭합니다.

자동 트랜잭션 검색을 위한 TIM 선택

기본적으로 자동 트랜잭션 검색이 실행 중인 경우 모든 TIM 의 HTTP 트래픽이 검색됩니다. 그러나 환경의 TIM 중 일부만 자동 트랜잭션 검색에 참여하도록 지정할 수 있습니다.

특정 TIM 에서 관심 있는 트랜잭션에만 액세스하도록 하려는 경우 이렇게 할 수 있습니다. 트랜잭션 검색을 이 TIM 으로만 제한하면 검색과 관련된 오버헤드가 다른 TIM 에 영향을 주지 않습니다.

자동 트랜잭션 검색에 참여하는 TIM 을 확인하거나 지정하려면

1. "설정" > "서비스"를 선택합니다.
2. "TIM 수집 서비스"를 클릭합니다.
3. "TIM 수집 서비스" 메뉴에서 "트랜잭션 검색 수집 서비스"를 선택합니다.

트랜잭션 검색에 참여하는 TIM 은 TIM 목록에서 사용 가능으로 표시됩니다.

4. 필요한 경우 목록에서 TIM 을 선택하거나 선택 취소합니다.
5. "저장"을 클릭합니다.

Enterprise Manager 구성 수정

Enterprise Manager 에 대한 설명이나 IP 주소를 수정하려면 다음 절차를 따르십시오.

설명 편집

기본적으로 설명은 Enterprise Manager 의 호스트 이름과 포트 번호를 포함하도록 설정되어 있습니다.

예를 들어 이 설명을 편집하여 컴퓨터 식별에 도움이 되는 자산 레이블이나 위치 ID 를 추가할 수 있습니다.

Enterprise Manager 에 대한 설명을 수정하려면

1. "설정" > "서비스" > "EM 구성"을 선택합니다.
2. Enterprise Manager 를 선택합니다.
3. 설명을 편집하고 "저장"을 클릭합니다.

Enterprise Manager 의 IP 주소 편집

대부분의 경우 Enterprise Manager 의 올바른 IP 주소가 "EM IP 주소" 필드에 자동으로 제공됩니다.

다음은 Enterprise Manager 의 IP 주소를 편집해야 하는 경우를 보여 주는 예입니다.

- Enterprise Manager 컴퓨터가 두 개의 네트워크에 포함되어 있어 두 개의 IP 주소를 갖는 경우. 한 IP 주소는 "EM 구성" 페이지에 표시되고, 다른 IP 주소는 "TIM Settings"(TIM 설정) 페이지에 TessCollectorIpAddr 또는 TessIpAddr 값으로 표시됩니다. "TIM Settings"(TIM 설정) 페이지를 보려면 6 단계(선택 사항)를 참조하십시오.
- Enterprise Manager 가 IPv6 주소와 IPv4 주소를 모두 가진 이중 스택 호스트인 경우. 사용하도록 설정된 TIM 에 IPv6 주소가 있으면 TIM 수집 서비스를 실행하는 Enterprise Manager 가 "EM IP 주소" 필드에 IPv6 주소를 표시해야 합니다.

Enterprise Manager 의 IP 주소를 수정하려면

1. "설정", "서비스", "EM 구성"을 차례로 선택합니다.
2. Enterprise Manager 를 선택합니다.

3. 대체 Enterprise Manager IP 주소를 선택하고 "저장"을 클릭합니다.
이 주소를 한 번 편집한 후 IP 주소가 다시 변경되면 수동으로 업데이트해야 합니다. Enterprise Manager 가 다시 시작될 때 필드가 더 이상 자동으로 업데이트되지 않습니다.
4. "설정", "모니터"를 차례로 선택합니다.
5. 다음과 같이 모든 TIM 을 사용하지 않도록 설정했다가 다시 사용하도록 설정합니다.
 - a. TIM 을 선택합니다.
 - b. "사용 안 함"을 클릭합니다.
 - c. "사용"을 클릭합니다.
6. (선택 사항) Enterprise Manager 가 TIM 수집 서비스를 실행 중인 경우 다음과 같이 사용하도록 설정된 TIM 이 업데이트된 IP 주소를 수신했는지 확인하십시오.
 - a. TIM 의 IP 주소를 클릭합니다.
TIM 의 "System Setup"(시스템 설정) 페이지가 나타납니다.
 - b. "Configure TIM Settings"(TIM 설정 구성)를 클릭합니다.
 - c. TessCollectorIpAddr 및 TessIpAddr 설정이 올바른지 확인합니다.
이러한 설정을 직접 편집하지 마십시오.

Enterprise Manager 제거

이 절차에서는 "서비스" 페이지에서 Enterprise Manager 를 제거하는 방법을 설명합니다.

시작할 때 "서비스" 페이지에 Enterprise Manager 가 자동으로 나타납니다. 그러나 Enterprise Manager 이름은 "서비스" 페이지에서 자동으로 제거되지 않습니다. 이 절차의 목적은 "서비스" 페이지에서 사용되지 않는 Enterprise Manager 의 이름을 제거하는 것입니다.

Enterprise Manager 를 제거하려면

1. Enterprise Manager 에서 Enterprise Manager 서비스를 실행 중인 경우 해당 서비스를 다른 Enterprise Manager 로 이동합니다. [Enterprise Manager 서비스 배포](#) (페이지 282)를 참조하십시오.
2. Enterprise Manager 를 종료합니다. *CA APM Administration Configuration Guide*(CA APM 구성 관리 안내서)에서 "Enterprise Manager 중지" 항목을 참조하십시오.
3. "설정" > "서비스" > "EM 구성"을 선택합니다.
4. Enterprise Manager 를 선택합니다.
5. 삭제를 클릭합니다.

"서비스" 페이지에 Enterprise Manager 가 더 이상 나타나지 않습니다.

나중에 이 Enterprise Manager 를 다시 시작하면 "서비스" 페이지에 다시 나타납니다.

Enterprise Manager 서비스 문제 해결

다음 표에는 Enterprise Manager 서비스 문제 해결에 유용한 팁 몇 가지가 나와 있습니다.

증상

이벤트 페이지에 다음과 같은 서비스 관련 CA CEM 이벤트가 나타납니다.

- TIM 수집 서비스가 중지되었습니다.
- 통계 집계 서비스가 중지되었습니다.
- 데이터베이스 정리 서비스가 중지되었습니다.

해결 방법

Enterprise Manager 서비스 중 하나가 중지되었으며 가능한 한 빨리 다시 시작해야 합니다.

서비스를 실행 중인 Enterprise Manager 를 다시 시작하십시오.

증상

매일 통계가 집계되고 있지 않은 것 같습니다.

보고서에 매일 데이터가 표시되지 않습니다.

해결 방법

통계 집계 데이터가 올바르게 실행되고 있지 않을 수 있습니다.

통계 집계 서비스를 실행 중인 Enterprise Manager 에 있는 IntroscopeEnterpriseManager 로그 파일을 검토하십시오.

증상

Enterprise Manager 가 제때에 TIM 의 데이터를 수신하고 있지 않은 것 같습니다.

해결 방법

TIM 수집 서비스가 올바르게 실행되고 있지 않을 수 있습니다.

TIM 수집 서비스를 실행 중인 Enterprise Manager 에 있는 IntroscopeEnterpriseManager 로그 파일을 검토하십시오.

증상

수집기가 TIM 의 정보를 수신하고 있지 않습니다.

예를 들어 TIM 로그에 다음과 같은 내용의 오류 메시지가 있습니다.

오류 이 TIM 에 대한 수집기 서비스가 없습니다.

해결 방법

수집기나 MOM 의 IP 주소가 변경되었을 수 있으며 "Enterprise Manager 구성" 페이지에는 해당 변경 사항이 반영되지 않습니다.

Enterprise Manager 를 다시 시작하거나 *CA APM 구성 및 관리 안내서*의 [Enterprise Manager 의 IP 주소 편집](#) (페이지 288) 절차를 따르십시오.

증상

위의 설명과 동일합니다. (수집기가 TIM 의 정보를 수신하고 있지 않습니다.)

예를 들어 TIM 로그에 다음과 같은 내용의 오류 메시지가 있습니다.

오류 이 TIM 에 대한 수집기 서비스가 없습니다.

해결 방법

수집기나 MOM 에 두 개의 IP 주소가 할당되었을 수 있으며, 한 IP 주소는 "Enterprise Manager 구성" 페이지에, 다른 IP 주소는 "TIM Settings"(TIM 설정) 페이지에 나타납니다.

"EM 구성" 페이지와 "TIM Settings"(TIM 설정) 페이지에서 주소가 일치하지 않는지 살펴보십시오.

주소가 동일하지 않으면 *CA APM 구성 및 관리 안내서*의 [Enterprise Manager 의 IP 주소 편집](#) (페이지 288) 절차를 따르십시오.

증상

수집기가 작동 중인데도 "서비스 구성" 페이지에 수집기 실행 상태가 "중지됨"으로 나타납니다.

해결 방법

MOM 과 수집기 간에 시간이 동기화되어 있지 않습니다.

MOM 과 수집기 간에 시간을 동기화하십시오.

자세한 내용은 *CA APM 구성 및 관리 안내서*의 [Enterprise Manager 클록 동기화](#) (페이지 95) 관련 단원을 참조하십시오.

증상

수집기 실행 상태가 "알 수 없음"으로 나타납니다.

해결 방법

수집기의 호스트 이름과 IP 주소가 올바른지 확인하십시오. 올바르지 않으면 <EM_Home>\config 디렉터리의 *IntroscopeEnterpriseManager.properties* 파일에 있는 *introscope.enterprisemanager.clustering.login.em1.host* 속성을 편집하십시오. 확인 가능한 IP 주소인지 확인하십시오. localhost 를 사용하지 마십시오.

CA CEM 도메인 정의

CA CEM 도메인을 사용하면 관리자가 예상된 트랜잭션 동작, 사용자 및 비즈니스 영향, CA CEM 전체의 데이터 보존 등에 대해 CA CEM 전반에 걸쳐 적용되는 기본값과 설정을 지정할 수 있습니다.

회사에는 CA CEM에 대해 정의된 도메인이 하나 있어야 합니다. 도메인 수준 아래에 비즈니스 서비스, 비즈니스 트랜잭션 및 비즈니스 응용 프로그램이 생성됩니다. 기본 도메인 이름은 "로컬 도메인"입니다.

사용자 그룹, 비즈니스 서비스 및 트랜잭션을 생성할 때 CA CEM 도메인 기본값을 상속할지 또는 특정 값(예: 사용자의 SLA 설정)을 생성할지를 선택할 수 있습니다.

CA CEM 도메인을 정의하려면

1. "설정", "도메인"을 선택합니다.
2. 도메인 설정을 정의합니다.

도메인 이름

CA CEM 도메인에 의미 있는 이름을 지정합니다. 도메인 이름은 대/소문자를 구분하지 않습니다.

포괄적 결합 정보 캡처

이 옵션을 선택하면 요청 및 응답 본문과 쿼리 및 게시 매개 변수에 대한 추가 데이터가 "CEM" > "인시던트 관리" > "결합 정보" 페이지에 표시될 수 있습니다. 자세한 내용은 *CA APM 보안 안내서*를 참조하십시오.

IP 서브넷별 결합 해결

이 옵션을 선택하면 결합이 발생한 서브넷별로 결합의 분포 상황이 인시던트 문제 해결 차트의 네트워크 계층에 표시됩니다. IP 주소별로 사용자가 다시 그룹화되지는 않습니다.

서브넷 마스크

서브넷을 정의하려면 "IP 서브넷별 결합 해결"과 함께 이 기능을 사용하십시오.

마스크는 일반적으로 255.255.255.0 으로 설정됩니다. 그러나 대규모 네트워크의 경우 255.255.0.0 이 더 적절할 수 있습니다.

3. "사용자 그룹" 설정을 정의합니다.

IP 서브넷별 사용자 그룹 만들기

이 기능은 새 사용자의 클라이언트 IP 서브넷별로 새 사용자 그룹을 자동으로 생성하는 데 사용됩니다.

중요! 사용자 수가 수십만이나 수백만 명에 달하는 대규모 전자 상거래 사이트에 설치하여 사용 중인 경우에는 이 기능을 사용하지 마십시오. 생성된 사용자 그룹 수를 관리하기 힘들어질 수 있습니다. 자세한 내용은 [사용자 및 그룹 관리](#) (페이지 319)를 참조하십시오.

서브넷 마스크

사용자 그룹을 생성할 서브넷을 정의하려면 "IP 서브넷별 사용자 그룹 만들기"와 함께 이 기능을 사용하십시오.

마스크는 일반적으로 255.255.255.0 으로 설정됩니다. 그러나 대규모 네트워크의 경우 255.255.0.0 이 더 적합합니다. 구체적인 IP 주소와 더 제한적인 서브넷 마스크를 기반으로 사용자 그룹을 생성하여 사용자 그룹을 추가로 미세 조정할 수 있습니다. [새 사용자 그룹 관리](#) (페이지 326)를 참조하십시오.

4. ID 설정을 정의합니다.

사용자 인식에서 응용 프로그램 무시

이 옵션을 선택하지 않으면 각 비즈니스 응용 프로그램마다 사용자가 고유하고 각 사용자 ID(비즈니스 응용 프로그램 + 로그인 이름)마다 통계 기록이 계산됩니다. 예:

- ApplicationOne_MyLoginName = 사용자 ID
- ApplicationTwo_MyLoginName = 다른 사용자 ID

- ApplicationThree_MyLoginName = 세 번째 사용자 ID
- eCommApplication_MyLoginName = 네 번째 사용자 ID. 그러나 전자 상거래 비즈니스 응용 프로그램이므로 결함이 보관되고 통계가 지정되지 않은 사용자 기록으로 이동합니다.

"사용자 인식에서 응용 프로그램 무시" 옵션을 선택하면 사용자가 한 번만 계산되는데, 이는 여러 비즈니스 응용 프로그램에 로그인해도 마찬가지입니다.

중요! 원래 시나리오, 즉 한 명의 사용자가 여러 사용자 ID 로 통계를 수집하는 시나리오가 이미 있는 경우 이 옵션을 선택하여 비즈니스 응용 프로그램을 무시하면 다음과 같이 다른 사용자 ID 가 생성됩니다.

- MyLoginName = 사용자 ID(비즈니스 응용 프로그램과 관계없이 이 사용자가 나중에 수행하는 모든 로그인)

이 예제에서는 한 명의 사용자에 대한 통계 기록이 5 개의 버킷에 보관됩니다. 통계 기록은 데이터 보존 규칙에 구성된 대로 데이터베이스에 남아 있습니다.

경로 매개 변수 구분 기호

경로 매개 변수를 사용하여 사용자, 세션, 사용자 그룹 또는 트랜잭션을 식별하는 경우 여기에서 구분 기호를 지정하십시오. 경로 매개 변수에 대한 자세한 내용은 *CA APM 트랜잭션 정의 안내서*를 참조하십시오.

5. 기본 트랜잭션 설정을 정의합니다.
 - a. 트랜잭션에 대한 결함 유형의 비즈니스 우선 순위를 결정하는 영향 수준을 정의합니다.

대부분의 경우 기본값인 "중간"이면 충분합니다. 이 값은 CA CEM 도메인의 비즈니스 서비스에서 기본적으로 상속되지만 트랜잭션 수준에서 편집할 수 있습니다.

- b. 트랜잭션 SLA(서비스 수준 계약) 수준을 정의합니다.

이러한 값은 CA CEM 도메인의 비즈니스 서비스에서 기본적으로 상속되지만 트랜잭션 수준에서 편집할 수 있습니다. 다음 표에서는 CA CEM 도메인 수준 SLA 옵션을 설명합니다.

성공률 SLA

성공률 서비스 수준 계약(%)입니다. 기본값은 95% 결함 없음 트랜잭션입니다.

시그마 SLA

시그마 서비스 수준 계약(숫자)입니다. 시그마 점수는 DPMO(백만 기회당 결함 수)에서 계산되는 측정값입니다. 기본값은 4.00이고 거의 완벽은 6.00이고 완벽(트랜잭션 결함 전혀 없음)은 무한대입니다.

트랜잭션 시간 SLA

트랜잭션 시간 서비스 수준 계약(초)입니다. 기본값은 총 경과 시간 8초입니다.

팁: CA CEM 은 0.001 초까지 시간을 지정할 수 있습니다. 그보다 적은 시간(예: 0.0001 초)을 지정하면 해당 값이 0.000 으로 설정됩니다.

6. 기본 사용자 설정을 정의합니다.
 - a. 결함 유형의 비즈니스 우선 순위를 결정하는 영향 수준을 정의합니다.

대부분의 경우 기본값인 "중간"이면 충분합니다. 이 값은 CA CEM 도메인의 비즈니스 서비스에서 기본적으로 상속되지만 사용자 그룹 수준에서 편집할 수 있습니다.
 - b. 기본 사용자 SLA(서비스 수준 계약) 수준을 정의합니다.

이러한 값은 CA CEM 도메인의 비즈니스 서비스에서 기본적으로 상속되지만 사용자 그룹 수준에서 편집할 수 있습니다.

7. 가치 설정을 정의합니다.

다음과 같이 계산된 IT 가치 열이 성능 보고서("비즈니스 서비스" 및 "비즈니스 트랜잭션" 페이지)에 표시될 수도 있고 표시되지 않을 수도 있습니다.

$$\text{IT 가치} = (\text{비즈니스 트랜잭션당 IT 가치}) * (\text{비즈니스 트랜잭션 수})$$

예를 들어 양호한 비즈니스 트랜잭션당 관찰된 가치가 \$2.00 이면 모든 성공한 트랜잭션이 비즈니스에 \$2.00 를 기여하는 것입니다.

- a. IT 가치를 표시하려면 "IT 가치 계산" 확인란을 선택하고 "비즈니스 트랜잭션당 IT 가치"에 통화 값을 입력합니다.

이 확인란을 선택하지 않으면 성능 보고서에 "IT 가치" 열이 나타나지 않습니다.
- b. "인시던트 원가 계산" 확인란 설정에 대한 자세한 내용은 [인시던트 원가와 비즈니스 영향의 비교](#) (페이지 298)를 참조하십시오.

8. 데이터 보존 설정을 정의합니다.

다음 이후 사용자 비활성화

사용자가 네트워크 트랜잭션을 생성하고 있는 한 활성화된 상태입니다. 기본적으로 지난 730 일 동안 관찰된 트랜잭션이 없을 때 사용자가 비활성화됩니다.

팁: 휴가 또는 휴직 기간, 퇴직 등의 요소를 고려하면 적절한 일수를 결정하는 데 도움이 될 수 있습니다.

Statistics aggregation(통계 집계)

통계는 모든 사용자에게 대해 시간, 사용자 및 사용자 그룹별로 집계됩니다. 다음과 같이 사용자와 사용자 그룹 통계를 유지할 기간을 선택할 수 있습니다.

시간별 사용자 통계 유지 기간

기본적으로 3일 동안 매시간 사용자 통계가 유지됩니다. 3일이 지나면 매일 또는 매주 사용자 통계는 볼 수 있지만 3일 이전의 매시간 통계는 볼 수 없습니다.

일별 사용자 통계 유지 기간

기본적으로 15일 동안 매일 사용자 통계가 유지됩니다. 15일이 지나면 매주 사용자 통계는 여전히 볼 수 있지만 15일 이전의 매일 통계는 볼 수 없습니다.

주별 사용자 통계 유지 기간

기본적으로 27주 동안 매주 사용자 통계가 유지됩니다. 6개월이 지난 매주 사용자 통계는 삭제됩니다.

시간별 사용자 그룹 통계 유지 기간

기본적으로 3일 동안 매시간 사용자 그룹 통계가 유지됩니다. 3일이 지나면 매일 또는 매주 사용자 그룹 통계는 볼 수 있지만 3일 이전의 매시간 통계는 볼 수 없습니다.

다음 동안 일별 사용자 그룹 통계 유지

기본적으로 15일 동안 매일 사용자 그룹 통계가 유지됩니다. 15일이 지나면 매주 사용자 그룹 통계는 여전히 볼 수 있지만 15일 이전의 매일 통계는 볼 수 없습니다.

주별 사용자 그룹 통계 유지 기간

기본적으로 27주 동안 매주 사용자 그룹 통계가 유지됩니다. 6개월이 지난 매주 사용자 그룹 통계는 삭제됩니다.

경고! 이러한 데이터 보존 설정을 너무 높게 설정하면 일별 집계가 지연될 수 있습니다. Enterprise Manager 가 어제의 통계 레코드가 아닌 며칠 전의 통계 레코드를 처리하고 있다는 내용이 IntroscopeEnterpriseManager 로그 파일에 표시되면 일별 집계가 지연되고 있는 것입니다.

9. "저장"을 클릭하여 모든 설정을 유지합니다.

인시던트 원가와 비즈니스 영향의 비교

이 항목에서는 "설정" > "도메인"을 선택하면 나타나는 "도메인" 페이지에서 "인시던트 원가 계산"을 선택할 때 발생하는 결과를 설명합니다.

"인시던트 관리" > "인시던트" 보고서에 "인시던트 원가" 열이나 "비즈니스 영향" 열이 표시될 수 있습니다. CA CEM 은 다음과 같이 인시던트 원가를 정의합니다.

$$\text{인시던트 원가} = (\text{사용자 분당 원가}) * (\text{사용자 수}) * (\text{분 수})$$

- 여기서 분 수는 인시던트 기간(분)이고 사용자 수는 지정되지 않은 사용자로 분류된 사용자를 제외한 고유 사용자 수입니다.

참고: 사용자가 로그인하기 전에 발생하는 엔터프라이즈 트랜잭션과 모든 전자 상거래 트랜잭션은 지정되지 않은 사용자 그룹에 기인합니다. 지정되지 않은 사용자만 CA CEM 트랜잭션을 실행한 경우 "사용자" 열에는 기호가 표시되고 인시던트 원가는 \$0.00(사용자 분당 원가 * 0 * 분 수)입니다.

인시던트 원가를 표시하려면

1. "인시던트 원가 계산" 확인란을 선택합니다.

이 확인란을 선택하면 "인시던트" 보고서에 "비즈니스 영향" 열 대신 "인시던트 원가" 열이 나타납니다.

2. 사용자 분당 인시던트 원가(통화)를 입력합니다.

예를 들어 \$0.50 를 입력합니다. 이는 비즈니스 영향이 5 명의 사용자에 대해 10 분 동안 개설 상태로 유지되는 경우 비즈니스 원가가 \$25.00 임을 의미합니다.

비즈니스 영향을 표시하려면

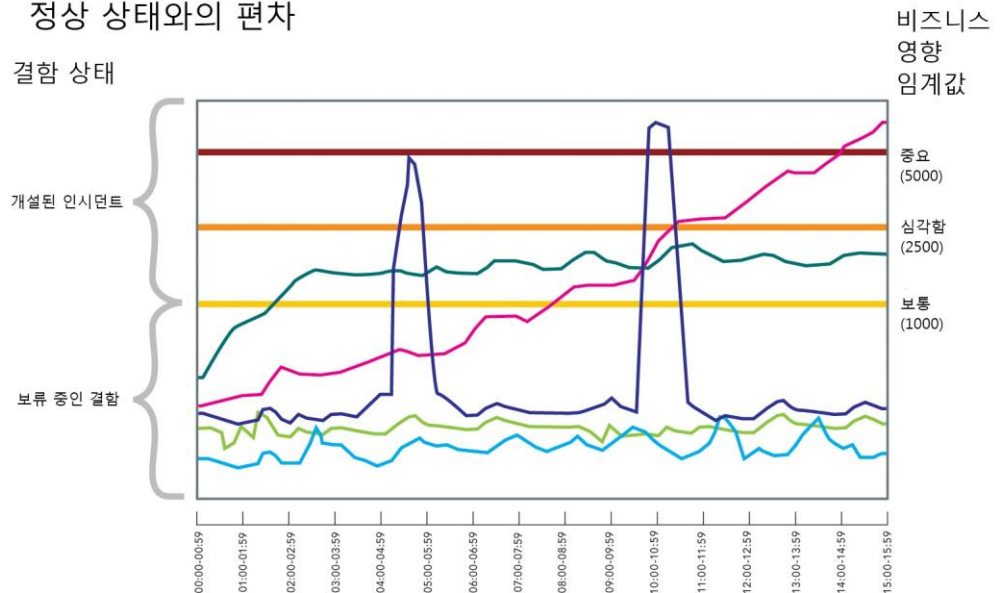
- "인시던트 원가 계산" 확인란을 선택 취소합니다.
 - "설정" > "도메인" 페이지에서 "인시던트 원가 계산" 확인란을 선택하는 경우 "인시던트" 보고서에 "비즈니스 영향" 대신 "인시던트 원가"가 나타납니다.
 - 이 확인란을 선택하지 않으면 "인시던트" 보고서에 "인시던트 원가" 열 대신 "비즈니스 영향" 열이 나타납니다.
 - "사용자 분당 인시던트 원가" 텍스트 상자에는 입력할 필요가 없습니다.

참고: 비즈니스 영향 제한에 대한 자세한 내용은 [인시던트 관련 설정 정의](#) (페이지 299)를 참조하십시오.

인시던트 관련 설정 정의

많은 환경에서 약간의 결함은 정상적인 현상입니다. 그러나 정상을 벗어난 변화가 있을 경우에는 알아야 합니다.

정상 상태와의 편차



정상 상태와 차이가 있을 경우 인시던트를 생성하도록 인시던트 관리 설정, 인시던트 생성 규칙 및 영향 설정을 조작할 수 있습니다.

결함의 비즈니스 영향

CA CEM 은 결함의 비즈니스 트랜잭션, 결함 유형 및 사용자를 기반으로 들어오는 결함 각각에 비즈니스 영향을 할당합니다.

결함의 비즈니스 영향은 다음과 같이 계산됩니다.

비즈니스 트랜잭션 가중치 * 결함 유형 가중치 * 사용자 가중치

영향 수준에는 다음이 각각 할당됩니다.

- 비즈니스 트랜잭션
- 결함 유형
- 사용자

영향 수준	할당되는 가중치
최소	1
매우 낮음	2
낮음	3
중간	4
높음	5
중요	6
지금 트리거	7

인시던트의 비즈니스 영향

CA CEM 은 들어오는 결함을 인시던트로 집계합니다. 인시던트는 비즈니스 트랜잭션과 결함 유형별로 집계됩니다. *인시던트의* 비즈니스 영향은 모든 집계된 결함의 비즈니스 영향 합계로 정의됩니다. 이 비즈니스 영향은 "인시던트 관리" 보고서에 나타납니다.

비즈니스 트랜잭션, 결함 유형 및 사용자 영향이 모두 보통(4)이면 $4 * 4 * 4 = 64$ 가 결함 영향입니다. 이것이 [인시던트 보고서](#) (페이지 298)의 그래픽에 표시되는 기본값입니다. 이러한 기본 비즈니스 영향을 사용하면 다음과 같습니다.

- 1000(보통) = 결함이 16 개인 경우 보통 인시던트가 개설됩니다.
- 2500(심각함) = 40 개인 경우 심각한 인시던트로 승격됩니다.
- 5000(중요) = 79 개인 경우 중요 인시던트로 승격됩니다.

인시던트 생성 방법

인시던트 생성 방법은 다음 두 가지가 있습니다.

- 비즈니스 영향 임계값 충족(기본 방법)

사용되도록 설정된 인시던트 생성 규칙 트리거

주요 영향 요인 보고서

주요 영향 요인 보고서에서는 비즈니스 서비스, 비즈니스 트랜잭션, 사용자/그룹 및 인시던트를 포함한 상위 5 개의 영향을 요약하여 보여 줍니다.

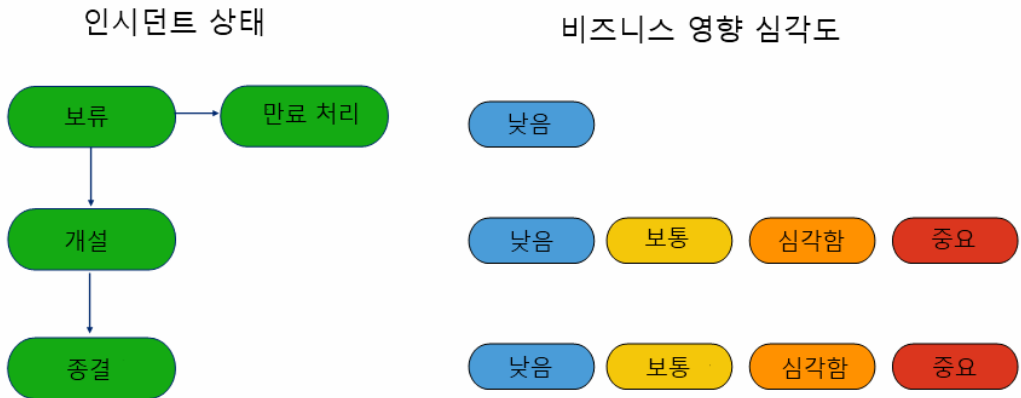
결함 보고서

결함 보고서에서는 각 결함의 비즈니스 영향을 보여 줍니다.

인시던트 상태와 비즈니스 영향 심각도의 비교

인시던트는 비즈니스 영향 값에 따라 여러 상태 간에 전환될 수 있습니다. 모든 CA CEM 사용자가 인시던트를 종결할 수 있습니다. 보통, 심각함 및 중요 심각도 설정을 사용하여 "설정" > "인시던트 설정" 페이지에서 각 상태 간의 경계를 정의할 수 있습니다.

이 차트에서는 인시던트 상태와 비즈니스 영향 심각도를 비교하여 보여 줍니다.



인시던트 관리 설정 구성

인시던트 관리 구성은 인시던트 생성 및 만료 처리 규칙과 해당 논리에 직접적인 영향을 미칩니다.

인시던트 관리 설정을 구성하려면

1. "설정" > "인시던트 설정"을 선택합니다.
2. "평가 간격(분)"에 간격(분)을 입력합니다. 기본값은 5 분입니다.
이 값은 인시던트 생성 및 만료 처리 규칙에 사용됩니다. 예를 들어 5 분으로 설정하면 인시던트를 생성해야 하는지 또는 보류 중인 인시던트를 만료 처리해야 하는지 확인하기 위해 매 5 분마다 각각의 활성 규칙, 즉 사용되도록 설정된 규칙이 검토됩니다.
3. "다음 이후 결함 삭제"에 기간(일)을 입력합니다. 기본값은 7 일 이후 결함을 삭제하는 것입니다.
4. "저장"을 클릭하여 모든 설정을 유지합니다.

인시던트 생성 규칙 설정

비즈니스에 합당할 때 인시던트를 생성하도록 사용자 지정된 규칙을 구성할 수 있습니다.

CA CEM 은 "영향 설정"에 설정된 심각도 임계값에 도달할 때도 인시던트를 생성합니다. [비즈니스 영향 설정 및 인시던트에 대한 증거 수집](#) (페이지 304)을 참조하십시오.

인시던트 생성 규칙을 구성하려면

1. "설정" > "인시던트 설정"을 선택합니다.
2. 인시던트를 생성하는 데 필요한 결합 수를 입력합니다. 이 수는 단기간의 즉각적인 결합 수 증가를 의미합니다.
 예를 들어 5 분(예제 평가 기간) 내에 발생하는 1000 개의 결합에 대한 규칙을 구성할 수 있는데, 이는 해당 기간 내에 해당 결합 수가 발생할 경우 비즈니스가 큰 영향을 받기 때문입니다.
3. 인시던트를 생성하는 데 필요한 결합 수 증가의 백분율을 입력합니다. 이 백분율은 단기간의 즉각적인 결합 백분율 증가를 의미합니다.
4. 결합 규칙을 입력합니다.
 - 인시던트를 생성하는 데 필요한 결합 수
 - 평가 간격 수(예: 위에 나와 있는 것과 같이 2/(3))
 - 또 다른 평가 간격 수(예: 위에 나와 있는 것과 같이 (2)/3)
 이 예제에서는 3 개 중 마지막 2 개의 평가 간격이나 15 분 중 마지막 10 분(평가 간격이 5 분인 경우) 내에 발생하는 500 개의 결합에 대한 규칙을 구성할 수 있습니다.
5. 활성화할 각 규칙 옆의 "사용" 확인란을 선택합니다.
 CA CEM 에서 평가 간격(예: 매 5 분)을 기반으로 사용하도록 설정된 규칙을 모두 검사합니다.
참고: 인시던트 생성 규칙에서는 AND 로직을 사용합니다. 즉, 사용하도록 설정된 규칙이 모두 true 여야 CA CEM 에서 인시던트를 생성합니다.
6. "저장"을 클릭하여 모든 설정을 유지합니다.

비즈니스 영향 설정 및 인시던트에 대한 증거 수집

영향 설정을 사용하면 인시던트를 생성하고 인시던트 심각도 수준을 결정하는 임계값을 설정할 수 있습니다. 증거 수집 설정을 사용하면 고급 증거 수집 스크립트를 배포할 수 있습니다.

인시던트 심각도가 변경될 때마다 증거 수집 스크립트를 실행하도록 CA CEM 을 구성할 수 있습니다.

스크립트	실행 시기
개설되었을 때 증거 수집	인시던트가 개설될 때
심각도 보통에 대한 증거 수집	인시던트 심각도가 "낮음"에서 "보통"으로 변경될 때
심각도 심각함에 대한 증거 수집	인시던트 심각도가 "보통"에서 "심각함"으로 변경될 때
심각도 중요에 대한 증거 수집	인시던트 심각도가 "심각함"에서 "중요"로 변경될 때

CA CEM 에서 증거를 수집하려면 먼저 사용 중인 시스템에 Python 또는 Perl 을 설치해야 합니다. 그런 다음 CA CEM 속성 `python.path` 또는 `perl.path` 를 수정하여 Python 또는 Perl 의 설치 위치를 지정합니다.

참고: 이 항목에서는 인시던트에 대한 증거 수집에 대해 설명합니다. CA Technologies 전문 서비스 오퍼링을 사용하면 개별 결함에 대한 증거를 수집하고 표시할 수 있습니다. 자세한 내용은 [추가 결합 정보 링크에 대한 디렉터리 경로 설정](#) (페이지 584)을 참조하십시오.

다음 단계를 따르십시오.

1. TIM 수집 서비스를 실행하는 Enterprise Manager 에 Python 또는 Perl 을 설치합니다.
2. `tess-customer.properties` 파일을 편집하고 `python.path` 또는 `perl.path` 속성을 수정합니다.

예제: `python.path=/usr/bin/python` 또는 `perl.path=C:\\perl\\bin\\perl.exe`

백슬래시가 Windows 플랫폼에 사용되는 경우 단일 슬래시(\)가 이스케이프 시퀀스로 해석되므로 이중 슬래시(\\)가 필요합니다.

참고: `tess-customer.properties` 파일이 아직 없으면 생성하십시오.

자세한 내용은 [CA CEM 기본 속성](#) (페이지 581)을 참조하십시오.

Python 또는 Perl 을 설정한 후에는 인시던트가 개설될 때나 인시던트 상태가 변경될 때 실행할 증거 수집 스크립트를 생성하고 사용하도록 설정할 수 있습니다.

인시던트에 대한 비즈니스 영향 수준을 정의하고 증거 수집 스크립트를 설정하려면

1. "설정" > "인시던트 설정"을 선택합니다.
기본 설정이 나타납니다.
2. 보통, 심각함 또는 중요 인시던트에 대한 영향 설정을 결정합니다.

이러한 설정은 인시던트가 생성되는 시기와 인시던트 심각도가 변경되는 시기를 모두 결정합니다.

기본값은 보통의 경우 1000, 심각함의 경우 2500, 중요한 경우 5000 입니다. [인시던트 관련 설정 정의](#) (페이지 299)를 참조하십시오.

- 증거 수집 설정을 결정합니다. 인시던트가 개설될 때 증거를 수집하거나 보통, 심각함 또는 중요 인시던트에 대한 증거를 수집하려면 확인란을 선택합니다. 예를 들어 보통 인시던트가 감지될 때 다음 스크립트가 실행될 수 있습니다.

```
%PYTHON%
C:\Introscope\cem\customer\evidencecollectors\evidence.py %ACTION% %SEVERITY%
%DEFECTID% %TRANID% %TRANDEFID% %SERVER% %CLIENTIP% %OUTPUT%
%PERL%
cem/customer/evidencecollectors/evidence.pl %ACTION% %SEVERITY% %DEFECTID% %T
RANID% %TRANDEFID% %SERVER% %CLIENTIP% %OUTPUT%
```

이러한 인수에 대한 자세한 내용은 [증거 수집 스크립트에 사용할 인수](#) (페이지 306)를 참조하십시오.

%PYTHON%은 python.path 속성에 대해 지정하는 위치(위에 있는 "스크립트에 사용할 Python 또는 Perl 을 설정하려면"의 2 단계)로 대체됩니다. Perl 을 설치한 경우에는 명령줄에서 **%PYTHON%** 대신 **%PERL%**을 사용합니다.

- "저장"을 클릭하여 영향 수준과 증거 수집 설정의 변경 사항을 저장합니다.

증거 수집 스크립트에 사용할 인수

다음은 증거 수집 스크립트에 사용할 수 있는 인수입니다. 위에서 설명한 "스크립트에 사용할 Python 또는 Perl 을 설정하려면"의 3 단계에 예제가 나와 있습니다.

ACTION

인시던트가 개설되고 있는지 아니면 종결되고 있는지에 따라 OPEN 또는 CLOSE 입니다.

SEVERITY

비즈니스 영향(낮음, 보통, 심각함 또는 중요)입니다.

DEFECTID

인시던트의 데이터베이스 ID 입니다.

TRANID

비즈니스 트랜잭션의 데이터베이스 ID 입니다.

TRANDEFID

비즈니스 서비스의 데이터베이스 ID 입니다.

SERVER

가장 최근 결함이 감지된 서버의 IP 주소입니다. 결함이 둘 이상의 서버에서 발생할 수 있지만 가장 최근 서버의 IP 주소가 이 인수에서 캡처됩니다.

CLIENTIP

가장 최근 결함이 감지된 클라이언트, 즉 사용자 PC의 IP 주소입니다. 결함이 여러 클라이언트에서 발생할 수 있지만 가장 최근 클라이언트의 IP 주소가 이 인수에서 캡처됩니다.

OUTPUT

증거 수집 스크립트의 출력을 넣을 위치입니다.

증거 수집에 대한 예제 스크립트 파일이

`cem/customer/evidencecollectors/evidence-example.py` 위치에 제품과 함께 설치되어 있습니다.

이 스크립트에서는 인수의 사용을 보여 줍니다.

인시던트 만료 처리 규칙 구성

인시던트 만료 처리 규칙을 사용하면 낮은 수준의 보류 중인 인시던트를 제거할 수 있습니다.

보류 중인 인시던트가 만료 처리되는 시기를 결정하기 위한 사용자 지정 규칙을 구성할 수 있습니다.

보류 중인 인시던트는 발생했지만 영향 임계값에 도달하지 않았으므로 아직 CA CEM에서 인시던트로 보고되지 않은 결함 이벤트입니다. 예를 들어 비즈니스 영향 임계값이 1000인 경우 999의 비즈니스 영향만 관찰된 경우 인시던트는 보류 중인 상태에 있습니다.

보류 중인 인시던트 만료 처리 규칙을 구성하려면

1. "설정" > "인시던트 설정"을 선택합니다.
2. 보류 중인 인시던트가 만료 처리되기 전에 관련 결함 없이 경과해야 하는 시간(분)을 입력합니다. 예를 들어 1일의 경우 1440 분(60 분 * 24 시간 = 1440)을 입력합니다.
3. 보류 중인 인시던트가 만료 처리되기 전에 인시던트가 보류 중인 상태로 경과해야 하는 시간(분)을 입력합니다.

4. 결합 규칙을 입력합니다.

- 보류 중인 인시던트에 아직 있으면 안 되는 결합 수
- 평가 간격 수(예: 9/(10))
- 또 다른 평가 간격 수(예: (9/10))

이 예제에서는 10 개 중 마지막 9 개의 평가 간격(또는 평가 간격이 5 분인 경우 50 분 중 마지막 45 분) 내에 발생하는 500 개의 결합에 대한 규칙을 구성할 수 있습니다.

5. 활성화할 각 규칙 옆의 "사용" 확인란을 선택합니다.

CA CEM 에서 평가 간격(예: 매 5 분)을 기반으로 사용하도록 설정된 규칙을 모두 검사합니다.

참고: 인시던트 만료 처리 규칙에서는 OR 로직을 사용합니다. 즉, 사용하도록 설정된 규칙 중 하나라도 해당하는 경우 CA CEM 에서 인시던트를 만료 처리할 수 있습니다.

6. "저장"을 클릭하여 모든 설정을 유지합니다.

인시던트가 개설되거나 심각도가 변경되면 전자 메일 보내기

인시던트가 개설되거나 인시던트 심각도가 변경되면 전자 메일을 보내도록 CA CEM 을 구성할 수 있습니다. 예를 들어 중요 인시던트가 될 때마다 인시던트 분석가에게 전자 메일을 보내도록 CA CEM 을 구성할 수 있습니다.

참고: 낮은 심각도의 개설된 인시던트에 대해서는 전자 메일이 생성되지 않습니다.

다음 단계를 따르십시오.

1. "설정", "인시던트 설정"을 차례로 선택합니다.
2. "인시던트 전자 메일 설정" 섹션에서 필요에 따라 필드를 편집합니다.
여러 주소에 전자 메일을 보내려면 쉼표(,)를 사용하여 전자 메일 주소를 구분합니다.
3. "저장"을 클릭하여 모든 설정을 유지합니다.
4. CA CEM 이 전자 메일을 보내도록 구성되었는지 확인합니다. [SMTP 서버 설정 구성](#) (페이지 309)을 참조하십시오.

CA CEM 은 다음 정보를 사용하여 CEM 관리자에게 전자 메일 알림을 보냅니다.

- 인시던트 ID
- 영향을 받은 비즈니스 응용 프로그램
- 영향을 받은 비즈니스 서비스
- 영향을 받은 비즈니스 트랜잭션
- 영향을 받는 그룹 수
- 영향을 받는 사용자 수
- 결함 수
- 결함 이름
- 처음 발생한 결함
- 마지막 발생한 결함

SMTP 서버 설정 구성

SMTP 서버의 이름과 포트 번호를 제공해야 CA CEM 에서 보고서를 전자 메일로 보낼 수 있습니다. 첨부된 보고서와 함께 보내는 전자 메일의 경우 제목과 메시지 텍스트를 구성할 수도 있습니다. 보고서에 대한 자세한 내용은 [CA CEM 을 사용하여 보고](#) (페이지 347)를 참조하십시오.

이러한 SMTP 설정은 CA CEM 이벤트와 인시던트의 전자 메일 알림에도 사용됩니다. [이벤트의 전자 메일 알림 수신](#) (페이지 341) 및 [인시던트가 개설되거나 심각도가 변경되면 전자 메일 보내기](#) (페이지 308)를 참조하십시오.

저장하기 전에 전자 메일 연결을 테스트해야 합니다.

다음 단계를 따르십시오.

1. "시스템" > "전자 메일 설정"을 선택합니다.
2. SMTP 서버 설정을 정의합니다.

호스트 이름

SMTP 서버의 호스트 이름을 입력합니다.

포트

SMTP 서버의 포트 번호를 입력합니다.

보낸 사람 주소

연결 테스트 전자 메일에 보낸 사람으로 표시될 주소입니다.

끝

연결 테스트 전자 메일을 받을 주소입니다. 기본적으로 이 주소와 "보낸 사람 주소"는 Embedded Entitlements Manager의 CA CEM 사용자(운영자) 정보에서 가져옵니다. 이 주소가 누락된 경우 `tess-default.properties` 파일의 `email.defaultFromAddress` 속성이 사용됩니다. 이 기본값을 변경하려면 [email.defaultFromAddress](#) (페이지 591)를 참조하십시오.

인증 필요

SMTP 서버에 사용자 이름과 암호가 필요한 경우 이 확인란을 선택합니다.

사용자 이름

인증이 필요한 경우 사용자 이름을 입력합니다.

암호

인증이 필요한 경우 암호를 입력합니다.

3. 전자 메일 설정을 정의합니다.

제목

전자 메일을 통해 보고서를 보내기 위한 표준 제목 행을 입력합니다.

Message

전자 메일을 통해 보고서를 보내기 위한 표준 메시지를 입력합니다.

바닥글 텍스트

전자 메일을 통해 보낸 보고서 아래쪽에 나타날 표준 텍스트를 입력합니다.

4. "연결 테스트"를 클릭합니다. 다음 세 가지 중 하나가 발생합니다.
 - 확인 메시지가 나타나고 테스트 성공을 나타내는 전자 메일이 수신되면 SMTP 설정과 "받는 사람" 전자 메일 주소가 올바른 것입니다.
 - 확인 메시지가 나타나지만 전자 메일이 수신되지 않으면 SMTP 설정은 올바르지만 "받는 사람" 전자 메일 주소는 잘못된 것입니다.
 - 오류 메시지가 나타나면 SMTP 설정이 잘못된 것입니다. SMTP 서버가 시간 초과될 때까지 기다려야 하는 경우에는 메시지가 나타나는 데 시간이 걸릴 수 있습니다.
5. "저장"을 클릭합니다.

참고: 보고서에 사용할 전자 메일을 설정하지 않으면 CA CEM 사용자가 보고서를 생성하려고 할 때 오류 메시지가 수신됩니다.

보고서 유형과 CA CEM 사용자의 보고서 구성 및 예약 옵션에 대한 자세한 내용은 [CA CEM 을 사용하여 보고](#) (페이지 347)를 참조하십시오.

새 비즈니스 서비스에 대한 보안 그룹 설정

조직에서 Embedded Entitlements Manager 를 배포한 경우 액세스 정책을 사용하여 비즈니스 서비스와 관련 데이터에 대한 액세스 권한이 있는 보안 그룹을 제어할 수 있습니다.

*보안 그룹*은 Embedded Entitlements Manager APM 응용 프로그램에 대해 생성된 사용자 그룹입니다. Embedded Entitlements Manager 에서는 보안 그룹을 *응용 프로그램 그룹*이라고 합니다.

관리자가 새로 생성된 비즈니스 서비스 모두에 대한 액세스 권한이 자동으로 부여되는 보안 그룹을 구성합니다.

기본적으로 다음 네 가지 액세스 정책이 설정되어 있습니다.

비즈니스 서비스 - 모든 권한

CEM 시스템 관리자 그룹은 모든 비즈니스 서비스에 대해 모든 권한을 가집니다.

비즈니스 서비스 - 읽기/쓰기

CEM 구성 관리자 그룹은 모든 비즈니스 서비스에 대해 읽기/쓰기 권한을 가집니다.

비즈니스 서비스 - 중요한 데이터 읽기

CEM 인시던트 분석가 그룹은 모든 비즈니스 서비스에 대해 중요한 데이터를 읽을 수 있는 권한을 가집니다.

비즈니스 서비스 - 읽기

CEM 분석가 및 CEM 인시던트 분석가 그룹은 모든 비즈니스 서비스에 대해 읽기 권한을 가집니다.

표준 보안 그룹(CEM 시스템 관리자, CEM 구성 관리자, CEM 인시던트 분석가, CEM 분석가)을 사용 중인 경우에는 이러한 액세스 정책으로 충분할 수 있습니다. 그러나 추가 보안 그룹을 생성한 경우 이러한 그룹의 멤버가 모든 비즈니스 서비스에 액세스할 수 있도록 하려면 해당 그룹을 포함하는 액세스 정책을 생성하거나 해당 그룹을 포함하도록 액세스 정책을 수정해야 합니다.

참고: 이 항목의 절차에서는 모든 비즈니스 서비스에 대한 액세스 정책을 수정하거나 생성하는 방법을 설명합니다. 특정 비즈니스 서비스에 대한 액세스 정책을 수정하거나 생성하려면 *CA APM 트랜잭션 정의 안내서*에서 액세스 정책에 대한 항목을 참조하십시오.

모든 비즈니스 서비스에 대한 기존 액세스 정책을 보거나 편집하려면

1. "보안" > "액세스 정책"을 선택합니다.

CA CEM 설치 후 추가된 액세스 정책이 없으면 위의 표에 나와 있는 액세스 정책을 참조합니다.

2. 보거나 편집할 정책의 이름을 클릭합니다.

"액세스 정책 업데이트" 페이지가 나타납니다.

3. "액세스 정책 업데이트" 페이지의 필드를 수정하고 "저장"을 클릭합니다.

필드는 아래 목록에서 설명합니다.

"비즈니스 서비스"에서 "전체"를 선택해야 합니다. 이렇게 하면 선택한 보안 그룹이 이후에 생성된 비즈니스 서비스 모두와 연결되고 모든 기존 비즈니스 서비스에 적용됩니다.

모든 비즈니스 서비스에 대해 새 액세스 정책을 생성하려면

1. "보안" > "액세스 정책"을 선택합니다.
2. "새로 만들기"를 클릭합니다.

3. "새 액세스 정책" 페이지의 필드를 모두 입력하고 "저장"을 클릭합니다.
필드는 아래 목록에서 설명합니다.

참고: "비즈니스 서비스"에 대해서는 "전체"를 선택하고, "보안 그룹"에 대해서는 "선택"을 선택해야 합니다. 이렇게 하면 선택한 보안 그룹이 모든 비즈니스 서비스(기존 및 이후)와 연결됩니다.

"새 액세스 정책" 페이지의 필드는 다음과 같습니다.

액세스 정책 이름

정책에 의미 있는 이름을 지정합니다.

설명

설명을 추가합니다.

정책 옵션

비즈니스 서비스에 대한 작업을 명시적으로 부여하거나 거부하는 정책을 생성하려면 선택합니다.

허용 및 거부 간에 충돌이 발생하는 경우 거부 정책이 우선합니다.

사용

정책이 적용되도록 하려면 정책을 사용하도록 설정합니다.

정책을 지금은 사용하지 않지만 나중에 사용할 수 있는 경우 정책을 사용하지 않도록 설정합니다. 다시 사용하지 않을 정책은 삭제합니다.

쓰기

보안 그룹 구성원이 "비즈니스 서비스" 탭에서 비즈니스 서비스 및 모든 자식 개체(비즈니스 트랜잭션, 트랜잭션, 구성 요소 등)를 보고, 편집하고, 삭제할 수 있도록 하려면 이 옵션을 선택합니다.

하나 이상의 비즈니스 서비스에 액세스할 수 없는 사용자에게는 "비즈니스 서비스" 탭이 표시되지 않습니다.

읽기

보안 그룹 구성원이 "CEM" 탭에서 해당 비즈니스 서비스와 연관된 그래프 및 보고서를 볼 수 있도록 하려면 이 옵션을 선택합니다.

참고: 구성된 영역이 Embedded Entitlements Manager 뿐인지 확인하십시오. Embedded Entitlements Manager 영역 외에도 로컬 영역이 구성되었으면 모든 사용자가 예약된 보고서의 모든 데이터에 액세스할 수 있습니다. 영역에 대한 자세한 내용은 *CA APM 보안 안내서*를 참조하십시오.

중요한 데이터 읽기

보안 그룹 구성원이 결함과 연관된 호스트, URL 경로, TCP 포트, 쿠키 및 HTTP 헤더를 볼 수 있도록 하려면 이 옵션을 선택합니다. 이러한 정보는 "CEM" > "인시던트 관리" > "결함 정보" 페이지에 표시됩니다.

"설정" > "도메인" 페이지에서 "포괄적 결함 정보 캡처" 확인란을 선택한 경우 "결함 정보" 페이지에 결함에 대한 쿼리 및 게시 매개 변수와 요청 및 응답 본문 정보도 표시됩니다. 자세한 내용은 *CA APM 보안 안내서*에서 "CA CEM" 장을 참조하십시오.

"읽기" 확인란에서 이 옵션을 사용합니다. "결함 정보" 페이지에 액세스하려면 읽기 작업이 필요합니다.

비즈니스 서비스

"전체"를 선택합니다. 그러면 액세스 정책이 모든 비즈니스 정책과 비즈니스 서비스가 새로 생성되는 경우 이러한 새 비즈니스 서비스에도 모두 적용됩니다.

참고: 특정 비즈니스 서비스에 대한 액세스 정책을 수정하려면 *CA APM 트랜잭션 정의 안내서*에서 자세한 내용을 참조하십시오. 예를 들어 CEM 분석가 및 CEM 인시던트 분석가 보안 그룹을 대상으로 해당 비즈니스 서비스에 대한 명시적 거부를 설정하여 하나의 특정 비즈니스 서비스에 대한 분석가 액세스를 거부할 수 있습니다.

보안 그룹

"선택"을 선택하고 정책의 보안 그룹을 "선택됨" 열로 이동합니다.

여기에 표시된 보안 그룹은 Embedded Entitlements Manager 의 APM 응용 프로그램별 사용자 그룹에 해당합니다. CA CEM에서는 Embedded Entitlements Manager 전역 사용자 그룹을 선택할 수 없습니다.

보안 그룹을 보거나 수정하려면 Embedded Entitlements Manager 를 사용하십시오. Embedded Entitlements Manager 사용에 대한 자세한 내용은 *CA APM 보안 안내서*를 참조하십시오. CEM 콘솔에서는 보안 그룹을 관리할 수 없습니다.

모니터 사용

트랜잭션을 모니터링하려면 먼저 TIM 이 사용하도록 설정되었는지 확인해야 합니다. 사용하지 않도록 설정된 TIM 모니터의 데이터는 Enterprise Manager 에 수신되지 않습니다.

다음은 TIM 을 사용하도록 설정해야 하는 경우에 대한 몇 가지 예입니다.

- TIM 을 설정하고 Enterprise Manager 와 연결할 때. *CA APM 설치 및 업그레이드 안내서*를 참조하십시오.
- TIM 및/또는 Enterprise Manager 를 업그레이드한 후. *CA APM 설치 및 업그레이드 안내서*를 참조하십시오.
- 구성을 가져온 후. [APM 데이터베이스 구성 가져오기](#) (페이지 59)를 참조하십시오.

Enterprise Manager 와 TIM 간의 통신을 사용하도록 설정하려면

1. "설정" > "모니터"를 선택합니다.
2. 각 필수 TIM 옆의 확인란을 선택하고 "사용"을 클릭합니다.

Enterprise Manager 와 TIM 간의 통신이 사용하도록 설정됩니다.

모니터 동기화

모니터를 동기화하면 현재 도메인 구성 파일이 사용하도록 설정된 TIM 모두와 에이전트에 전송됩니다. 도메인 구성 파일에는 트랜잭션 정의, 결합 사양 및 Introscope 트랜잭션 추적 매개 변수가 포함됩니다.

다음은 모니터를 동기화해야 하는 경우에 대한 몇 가지 예입니다.

- CA CEM 에서 비즈니스 서비스를 생성하거나 업데이트한 후. CA CEM 에서 비즈니스 서비스와 트랜잭션에 대해 변경한 사항은 모니터가 동기화되고 변경된 비즈니스 서비스에 대한 메트릭이 일부 생성된 후에야 Workstation 이나 WebView Investigator 트리에 나타납니다.
- TIM 을 설정하고 Enterprise Manager 와 연결할 때. *CA APM 설치 및 업그레이드 안내서*를 참조하십시오.
- TIM 및/또는 Enterprise Manager 를 업그레이드한 후. *CA APM 설치 및 업그레이드 안내서*를 참조하십시오.

- 에이전트와 사용하도록 설정된 TIM 에 업데이트된 정의를 보내기 위해 트랜잭션 정의를 생성하거나 수정한 후. [CA APM 트랜잭션 정의 안내서](#)를 참조하십시오.
- 에이전트와 사용하도록 설정된 TIM 에 가져온 정의를 보내기 위해 구성 파일을 가져온 후. [APM 데이터베이스 구성 가져오기](#) (페이지 59)를 참조하십시오.

네트워크의 모니터를 동기화하려면

1. "설정" > "모니터"를 선택합니다.
2. 사용하지 않도록 설정된 필수 모니터가 있는 경우 사용하도록 설정합니다. [모니터 사용](#) (페이지 315)을 참조하십시오.
3. 마지막 동기화 후 구성에 대해 변경된 사항을 검토하려면 [마지막 동기화 후 구성 변경 사항 보기](#) (페이지 316)를 참조하십시오.
4. "모든 모니터 동기화"를 클릭합니다.

사용하도록 설정된 모니터가 모두 동기화되고 관련 아이콘이 오른쪽 위에 나타납니다. 그러면 업데이트된 트랜잭션 정의가 네트워크에서 사용하도록 설정된 TIM 모두에 전송됩니다. 정의한 트랜잭션에 대한 모니터링이 TIM 에서 즉시 시작됩니다.

또한 모든 모니터를 동기화하면 CA CEM 에서 Enterprise Manager 로 트랜잭션 및 추적 정보가 전송됩니다.

마지막 동기화 이후의 구성 변경 사항 보기

동기화하기 전에 구성에 대한 변경 사항을 나열할 수 있습니다. 이렇게 하면 동기화 전에 변경 사항을 검토할 수 있습니다.

마지막 동기화 이후 이러한 속성에 대해 변경된 사항은 "도메인 구성 변경 기록" 테이블에 나타납니다.

- 비즈니스 응용 프로그램 정의
- 비즈니스 서비스 정의
- 결함 정의
- 비즈니스 트랜잭션 정의
- 결함 중요도 정의
- 트랜잭션 정의

- 결합 영향 수준
- 사용자 ID 매개 변수
- 트랜잭션 매개 변수 정의
- 세션 ID 매개 변수
- 임시 세션 ID 매개 변수
- 트랜잭션 중요도 정의
- 사용자 그룹 ID 매개 변수
- 트랜잭션 구성 요소 정의
- 개인 매개 변수

개인 매개 변수와 같은 특정 유형의 매개 변수를 삭제할 경우 개체 이름이 빈 상태로 나타나고 속성 변경 사항은 "표시할 항목 없음"으로 표시됩니다. 이는 개체 이름과 변경 사항이 데이터베이스에서 삭제되었기 때문입니다.

마지막 동기화 이후의 구성 변경 사항을 보려면

1. 모니터가 동기화되지 않는지 확인합니다.
2. "설정" > "모니터"를 선택합니다.
3. "마지막 동기화 이후 변경 내용 보기"를 클릭합니다.

변경 기록 테이블이 나타납니다.

참고: 변경 기록 테이블에는 마지막 동기화 이후의 구성 변경 사항이 나열됩니다. 이는 마지막 동기화와 현재 구성 간의 차이점을 나열하는 것과는 다릅니다. 예를 들어 값을 5에서 2로 변경한 후 다시 5로 변경했다면 이 테이블에는 예상한 것처럼 아무 행도 표시되지 않는 것이 아니라 두 개의 행이 표시됩니다.

기본적으로 "도메인 구성 변경 기록" 테이블의 최대 행 수는 1,000 개입니다. 최대 행 수를 변경하려면 [마지막 동기화 이후 변경 사항 목록의 항목 수 제한](#) (페이지 505)을 참조하십시오.

나열되는 속성 값이 모두 의미 있는 것은 아닙니다. 예를 들어 매개 변수가 생성될 때 표시되는 "구성 관리자" 값에는 개체의 내부 클래스 이름이 표시됩니다.

제 19 장: CA CEM 에서 사용자 및 그룹 관리

다음 목록에서는 사용자 및 그룹 관리와 관련된 주요 작업을 보여 줍니다.

1. [CA CEM 과 함께 사용할 수 있는 사용자 그룹 유형에 대해 알아봅니다](#) (페이지 320).
2. [트랜잭션 내의 정보를 통한 사용자 그룹 자동 생성에 대해 알아봅니다](#) (페이지 322).
3. [IP 서브넷을 통한 사용자 그룹 자동 생성에 대해 알아봅니다](#) (페이지 323).
4. [새 사용자 그룹에서 다른 그룹으로 사용자를 다시 할당합니다](#) (페이지 326).
5. [사용자 그룹과 SLA\(서비스 수준 계약\) 설정을 구성합니다](#) (페이지 327).
6. [대량 편집을 수행하여 사용자와 사용자 그룹을 관리합니다](#) (페이지 329).
7. [사용자 그룹 SLA 와 비즈니스 트랜잭션을 상호 관련시킵니다](#) (페이지 330).
8. [사용자 그룹을 삭제하거나](#) (페이지 334) [개별 사용자를 비활성화 또는 삭제합니다](#) (페이지 335).

참고: 이 장에 설명된 *사용자*는 *모니터링된 응용 프로그램*의 사용자입니다. 예를 들어 은행 업무용 응용 프로그램의 사용자는 자신의 계정을 보거나 관리하기 위해 로그인하는 은행 고객입니다. 계정 유형에 따라 이러한 사용자를 그룹화할 수 있습니다.

그러나 CA CEM 사용자가 CEM 콘솔에서 액세스할 수 있는 탭, 메뉴 항목 및 비즈니스 서비스를 구성하는 등의 목적으로 CA CEM 사용자를 *보안 사용자 그룹*으로 그룹화하는 방법에 대한 정보를 찾고 있으면 *CA APM 보안 안내서*를 참조하십시오.

사용자 그룹 정보

사용자 그룹을 사용하면 각 사용자의 설정을 개별적으로 구성할 필요 없이 사용자 모음에 대한 설정을 간편하게 구성할 수 있습니다. 문제가 발생한 사용자 집단을 쉽게 식별할 수 있도록 사용자 그룹을 정의할 수 있습니다.

수동으로 새 사용자 그룹을 생성하고 사용자를 사용자 그룹으로 이동할 수 있습니다. CA CEM 은 사용자 그룹을 자동으로 생성하는 방법도 제공합니다. 사용자는 하나의 CA CEM 사용자 그룹에만 속합니다.

사용자 그룹에는 열 유형이 있습니다.

요청 특성 사용자 그룹

수행 중인 요청 내의 콘텐츠별로 그룹화된 사용자입니다.

서브넷 사용자 그룹

새 사용자가 사용자 서브넷별로 자동 할당된 그룹입니다.

수동으로 생성된 사용자 그룹

"새 사용자" 그룹이나 다른 사용자 그룹에서 이 유형의 사용자 그룹으로 사용자를 수동으로 이동해야 합니다.

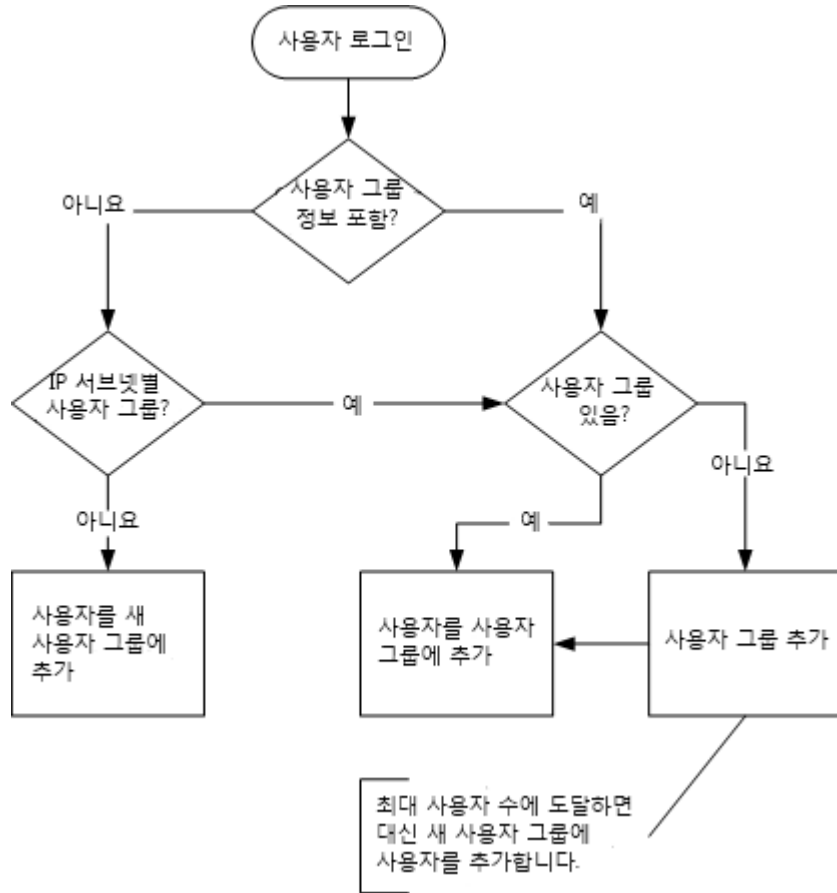
새 사용자

사용자 그룹 자동 생성 방법을 선택하지 않은 경우 새 사용자 로그인은 모두 새 사용자 그룹에 할당됩니다.

지정되지 않은 사용자

모든 전자 상거래 트랜잭션은 지정되지 않은 사용자 그룹에 할당됩니다. 사용자 로그인 전에 발생하는 엔터프라이즈 트랜잭션도 지정되지 않은 사용자 그룹에 할당됩니다.

다음 순서도에서는 사용자 그룹 자동 생성 및 할당의 기반이 되는 로직을 보여 줍니다.



최대 사용자 그룹 수

CA CEM 을 사용하면 자동으로 생성된 사용자 그룹의 수를 제어할 수 있습니다. 이 제어 기능은 CEM 관리자가 알아채기도 전에 그룹 수가 급격히 증가할 수 있는 뜻밖의 경우에 유용할 수 있습니다.

기본적으로 자동으로 생성된 사용자 그룹의 최대 수는 5000 입니다. 기본값을 조정하려면 [apm-events-thresholds-config.xml](#) (페이지 494) 파일의 [introscope.enterprisemanager.max.transaction.user.groups](#) (페이지 506) 속성을 구성하십시오.

요청 특성별로 새 사용자 자동 할당

수행 중인 요청 내의 콘텐츠별로 사용자를 그룹화할 수 있습니다. 가장 일반적인 경우는 다음과 같습니다.

- URL 문자열 - 예제: 쿼리 문자열의 속성 코드 또는 고객 코드
- HTTP 헤더 - 예제: 전화 유형이나 게이트웨이가 다른 사용자
- CA APM TG 헤더 - 예제: CA APM TG(x-wtg-info) 헤더를 사용하는 가상 사용자

이 방법을 사용하면 CA CEM 에서 사용자 위치나 회사별로 성능 정보를 보고할 수 있습니다. 예를 들어 영향을 받는 집단별로 중단을 관리하는 데 도움이 됩니다. 사용자 그룹 통계는 전자 상거래 비즈니스 응용 프로그램에 사용할 수 있습니다.

참고: 사용자 그룹 매개 변수별 그룹화는 서브넷별 사용자 그룹 자동 분류보다 우선합니다.

중요! 사용자 수가 수십만이나 수백만 명에 달하는 대규모 전자 상거래 사이트에 설치하여 사용 중인 경우에는 이 기능을 사용할 때 주의하십시오. 생성된 사용자 그룹 수를 관리하기 힘들어질 수 있습니다.

중요! 사용자 이름 대신 클라이언트 IP 주소별로 사용자를 식별할 경우에는 요청 특성별로 사용자를 할당하지 마십시오. 클라이언트 IP 주소를 통한 사용자 식별에 대한 자세한 내용은 *CA APM 트랜잭션 정의 안내서*를 참조하십시오.

요청 특성별로 새 사용자를 할당하려면

1. "관리" > "비즈니스 응용 프로그램"을 선택합니다.
2. 요청 특성별로 사용자를 식별할 비즈니스 응용 프로그램을 선택합니다.
3. "사용자 그룹 ID"를 선택합니다.
기존 사용자 그룹 매개 변수를 모두 나열하는 목록이 나타납니다.
4. "새로 만들기"를 클릭하여 새 사용자 그룹 매개 변수를 생성합니다.
5. 적절한 매개 변수 유형을 선택합니다.

6. 매개 변수 이름을 입력합니다.
7. "저장"을 클릭합니다.

예를 들어 x-wtg-info 유형은 CA APM TG 사용자를 "Synthetic"(가상)이라고 하는 그룹으로 그룹화합니다. 이는 실제 트래픽을 CA APM TG 트래픽과 구분하는 데 도움이 됩니다.

서브넷 사용자 그룹에 새 사용자 자동 할당

사용자의 IP 서브넷을 통해 사용자를 그룹화할 수 있습니다. CA CEM 은 새 사용자의 IP 주소를 기존 사용자 그룹의 서브넷과 자동으로 비교합니다. 가장 제한적인 서브넷 마스크가 먼저 검사됩니다. 예를 들어 다음 사용자 그룹이 정의되어 있다고 가정해 봅시다.

```
SubGroup - 255.255.255.0 mask / 192.168.2.0 IP start
BigGroup - 255.255.0.0 mask / 192.168.0.0 IP start
```

SubGroup 사용자 그룹의 서브넷 마스크가 더 제한적이므로 들어오는 IP 트래픽은 먼저 SubGroup 사용자 그룹과 비교됩니다. 예를 들어 IP 주소 192.168.2.4 가 SubGroup 그룹에 할당되고 IP 주소 192.168.9.9 가 BigGroup 그룹에 할당됩니다.

SubGroup 또는 BigGroup 그룹에 없는 IP 주소가 감지되면 구성 선택 항목에 따라 사용자에게 할당됩니다. 예를 들어 IP 주소 192.1.9.9 는 서브넷 마스크가 255.255.255.0 이지만 어느 그룹의 IP 주소 범위에도 속하지 않습니다.

참고: 사용자 그룹 매개 변수별 그룹화는 서브넷별 사용자 그룹 자동 분류보다 우선합니다. 자세한 내용은 [요청 특성별로 새 사용자 자동 할당 \(페이지 322\)](#)을 참조하십시오.

새 사용자에 대한 서브넷 사용자 그룹 생성

서브넷 사용자 그룹은 "설정" > "도메인" 탭의 "IP 서브넷별 사용자 그룹 만들기" 옵션으로 결정됩니다.

"설정" > "도메인" 페이지에서 "IP 서브넷별 사용자 그룹 만들기" 옵션을 선택한 경우 새 IP 주소는 "새 사용자"라는 그룹에 할당되는 것이 아니라 새 사용자 그룹 생성을 트리거합니다.

중요! 사용자 수가 수십만이나 수백만 명에 달하는 대규모 전자 상거래 사이트에 설치하여 사용 중인 경우에는 이 기능을 사용하지 마십시오. 생성된 사용자 그룹 수를 관리하기 힘들어질 수 있습니다.

기본적으로 자동으로 생성된 사용자 그룹의 최대 수는 5000 입니다. 기본값을 조정해야 할 경우 [기본 tess-default.properties 파일](#) (페이지 581)을 참조하십시오.

새 사용자 그룹 이름은 감지된 IP 주소의 시작 번호로 지정됩니다. 이 예제에서 새 사용자 그룹 이름은 다음과 같이 지정됩니다.

Usergroup-192.1.9.0 - 255.255.255.0 mask/192.1.9.0 address

새로 생성된 사용자 그룹을 보려면

1. "관리" > "사용자 그룹"을 선택합니다.
2. "Usergroup-192.1.9.0"을 클릭하여 새로 나열된 사용자를 봅니다.

참고: IP 주소를 사용하여 서브넷 사용자 그룹에 배치된 사용자는 나중에 해당 IP 주소가 변경되더라도 해당 사용자 그룹에 그대로 유지됩니다. 필요한 경우 원래 사용자 항목을 수동으로 이동할 수 있습니다.

프록시 서버를 사용하는 경우 사용자 식별

[서브넷 사용자 그룹에 새 사용자 자동 할당](#) (페이지 323)에 설명된 시나리오에서 프록시 서버를 사용하는 경우 사용자는 클라이언트 컴퓨터가 아닌 프록시 서버의 서브넷에 따라 그룹화됩니다. 비즈니스 요구 사항에 따라 이렇게 하지 않고 클라이언트 서브넷을 기준으로 사용자 그룹을 생성해야 할 경우가 있을 수 있습니다.

이와 유사하게 "인시던트 관리" > "결함" 페이지에 나타나는 결함 목록의 경우 프록시 서버의 IP 주소 대신 원래 컴퓨터의 IP 주소를 클라이언트 IP 주소로 표시해야 할 경우도 있습니다.

클라이언트 IP 주소를 포함하는 HTTP 헤더가 요청 트래픽에 포함된 경우 *로그인과 결합에 대해 연결 IP 주소 대신 클라이언트 IP 주소를 보고하도록 CA CEM* 을 구성할 수 있습니다. X-Forwarded-For, Forwarded-For 및 iv-remote-address 는 클라이언트 IP 주소를 식별하는 데 사용되는 헤더의 예입니다. 점으로 구분된 십진수 표기법을 사용하는 IP 주소나 표준 표기법을 사용하는 IPv6 주소가 포함된 경우에는 다른 헤더를 사용할 수 있습니다. 예:

```
X-Forwarded-For: 172.24.192.4
```

"ProxyForwardHeader"라고 하는 TIM 설정은 헤더 이름을 지정하는 데 사용됩니다.

참고: 헤더가 누락되었거나 헤더의 값이 IP 주소 형식이 아닌 경우에는 연결 IP 주소가 사용됩니다. 즉, 기본값("ProxyForwardHeader" 설정이 지정되지 않은 경우)과 동일한 동작이 발생합니다.

각 TIM 의 "ProxyForwardHeader" 값을 클라이언트의 IP 주소를 포함하는 헤더로 설정하십시오.

프록시 서버를 사용하는 경우 헤더 값을 기준으로 클라이언트를 식별하려면

1. "TIM System Setup"(TIM 시스템 설정) 페이지에 액세스합니다. [CEM 콘솔에서 TIM 액세스](#) (페이지 263)를 참조하십시오.
2. "Configure TIM Settings"(TIM 설정 구성)를 클릭합니다.
"TIM Settings"(TIM 설정) 페이지가 표시됩니다.
3. "ProxyForwardHeader"(확인)를 클릭합니다.
4. "새 값" 필드에 헤더 이름을 콜론 없이 입력하고 "변경"을 클릭합니다.
이 필드는 대/소문자를 구분하지 않습니다.
5. TIM 이 여러 개일 경우 각 TIM 마다 위의 단계를 반복합니다. 설정은 해당 설정이 정의된 TIM 각각에서 모니터링하는 서버와 응용 프로그램 모두에 영향을 줍니다.

헤더 값을 기준으로 사용자 그룹을 생성하려면

1. 위의 "프록시 서버를 사용하는 경우 헤더 값을 기준으로 클라이언트를 식별하려면"에 설명된 대로 "ProxyForwardHeader"를 설정합니다.
2. CEM 콘솔에서 다음과 같이 IP 서브넷별 사용자 그룹 만들기 옵션이 선택되었는지 확인합니다.
 - a. "설정" > "도메인"을 선택합니다.
 - b. "IP 서브넷별 사용자 그룹 만들기"를 선택합니다.

그러면 새 사용자 그룹이 연결 서브넷 대신 헤더에 제공된 클라이언트 서브넷을 기준으로 생성됩니다. 또한 결함이 연결 IP 주소 대신 클라이언트 IP 주소에서 발생하는 것으로 보고됩니다.

3. (선택 사항) 프록시 서버를 사용하는 클라이언트에서 결함을 생성하여 구성을 테스트합니다. 결함과 연결된 IP 주소가 프록시 서버가 아닌 클라이언트의 IP 주소이면 구성이 올바른 것입니다.

새 사용자 그룹 관리

자동 사용자 그룹 생성 및 할당 방법 중 하나를 설정하지 않은 경우 기존 서브넷 사용자 그룹과 일치하지 않는 새 사용자가 있으면 "새 사용자" 그룹에 자동으로 할당됩니다.

새 사용자를 보려면

1. "관리" > "사용자 그룹"을 선택합니다.
2. "새 사용자" 그룹을 클릭하여 새로 나열된 사용자를 봅니다.

새로 감지되었지만 사용자 그룹에 할당되지 않은 사용자가 나타납니다.

참고: 모니터링 트랜잭션을 시작해야 새 사용자가 감지됩니다.

수동으로 사용자 그룹에 새 사용자 할당

새 사용자는 서브넷 사용자 그룹이나 "새 사용자" 그룹에 자동으로 배치됩니다.

사용자를 현재 그룹 외부로 이동하려면

1. "관리" > "사용자 그룹"을 선택합니다.
2. "새로 만들기"를 클릭하여 새 사용자 그룹을 정의합니다.
 - a. 사용자 그룹에 의미 있는 이름(예: London)을 지정합니다. 사용자 그룹 이름은 대/소문자를 구분하지 않습니다.
 - b. 그룹에 대한 설명을 입력합니다.
 - c. 다른 매개 변수는 당분간 그대로 둡니다. 자세한 내용은 [사용자 그룹 구성](#) (페이지 327)을 참조하십시오.
 - d. "저장"을 클릭하여 새 그룹을 저장합니다.
3. 방금 만든 사용자 그룹을 클릭합니다. 모니터링 트랜잭션을 시작하거나 사용자를 그룹으로 이동해야 새 사용자가 감지됩니다.
4. "사용자 그룹" 페이지로 돌아가서 "새 사용자" 그룹을 클릭합니다.
5. 사용자를 새 사용자 그룹으로 이동하려면 "로그인 이름" 왼쪽의 확인란을 선택합니다.
6. "다음으로 이동" 목록에서 새 사용자 그룹(예: London)을 선택합니다.
7. "이동"을 클릭하여 사용자를 새 사용자 그룹으로 이동합니다.
8. 현재 사용자 그룹에 있는 모든 사용자를 목록에서 선택한 사용자 그룹으로 이동하려면 "모두 이동"을 클릭합니다. 각 "로그인 이름" 왼쪽의 확인란을 클릭하지 않아도 됩니다.
9. "사용자 그룹" 페이지로 돌아간 경우 새 사용자 그룹(예: London)을 클릭하여 이동된 사용자를 봅니다.

사용자 그룹 구성

네트워크의 사용자 그룹을 편집하고 SLA 를 정의하려면

1. "관리" > "사용자 그룹"을 선택합니다.
현재 사용자 그룹이 나타납니다.
2. 그룹 설정을 수정할 사용자 그룹 이름을 클릭합니다.

3. "일반" 탭을 클릭합니다.
4. 필요한 경우 사용자 그룹 이름을 변경합니다. 사용자 그룹 이름은 대/소문자를 구분하지 않습니다.
5. 그룹에 대한 설명을 입력하거나 수정합니다.
6. 그룹 트랜잭션에 대한 결함 유형의 비즈니스 우선 순위를 결정하는 영향 수준을 선택합니다. 대부분의 경우 기본값인 "중간"이면 충분합니다.

기본적으로 CA CEM 도메인의 영향 수준이 상속됩니다. 이 값을 변경하려면 확인란을 선택 취소하고 목록에서 영향 수준을 선택합니다.

참고: CA CEM 도메인 기본값을 변경하려면 [CA CEM 도메인 정의](#) (페이지 293)에 설명된 대로 "설정" > "도메인"을 선택하십시오.

7. 비즈니스 서비스 수준의 SLA(서비스 수준 계약)를 정의하는 SLA 값을 선택합니다.

기본적으로 CA CEM 도메인의 SLA 값이 상속됩니다. 값을 변경하려면 확인란을 선택 취소하고 목록에서 새 값을 선택합니다.

이러한 값은 비즈니스 서비스 내에서 사용자 그룹의 트랜잭션이 상속받을 수 있는 기본 SLA 값을 정의할 때도 사용됩니다.

성공률 SLA

성공률 서비스 수준 계약(%)입니다. 기본값은 95%입니다.

시그마 SLA

시그마 서비스 수준 계약(숫자)입니다. 시그마 점수는 DPMO(백만 기회당 결함 수)에서 계산되는 측정값입니다. 기본값은 4.00 이고 거의 완벽은 6.00 이고 완벽(트랜잭션 결함 전혀 없음)은 무한대입니다.

트랜잭션 시간 SLA

트랜잭션 시간 서비스 수준 계약(초)입니다. 기본값은 없습니다.

8. 로그인 ID 로 감지된 새 사용자를 서브넷 이름으로 식별된 새 사용자 그룹에 자동으로 추가하려면 "IP 서브넷별 새 사용자 그룹화" 확인란을 선택합니다.
 - a. 사용자 그룹의 IP 주소(예: 192.168.1.0)를 입력합니다.
 - b. 기본 서브넷 마스크(예: 255.255.255.0)를 입력합니다.

이 예제의 경우 192.168.1.1 에서 192.168.1.254 사이의 IP 주소를 사용하여 로그인하는 새 사용자는 "새 사용자" 그룹 대신 이 사용자 그룹에 자동으로 할당됩니다.

팁: IP 주소별로 사용자를 그룹에 할당하는 방법을 사용할 경우에는 그룹 이름에 IP 정보를 포함하는 것이 좋습니다.
9. "저장"을 클릭하여 새 사용자 그룹을 저장합니다. "사용자 그룹" 목록에 해당 사용자 그룹이 나타납니다.

대량 편집을 사용하여 사용자 설정 구성

경우에 따라서는 사용자 설정을 광범위하게 변경해야 합니다. 예를 들어 전체 사용자 그룹 대신 여러 사용자를 검색하고 4.00 에서 5.00 으로 "시그마 SLA" 설정을 수정해야 할 수 있습니다.

대량 편집을 사용하면 다음을 광범위하게 변경할 수 있습니다.

- 비즈니스 서비스 및 트랜잭션 설정
- 트랜잭션 및 구성 요소 결합 조건
- 사용자 설정

트랜잭션 관련 설정을 대규모로 수정해야 하는 경우 *CA APM 트랜잭션 정의 안내서*를 참조하십시오.

"사용자 검색" 페이지에서는 사용자 설정을 대규모로 수정할 수 있습니다.

대량 편집을 사용하여 사용자 설정을 구성하려면

1. "관리" > "사용자 그룹" > "사용자 검색"을 선택합니다.
검색 옵션이 나타납니다.
2. 사용자 그룹 이름(예: "Corporate"(회사))을 선택합니다.
3. 영향 수준(예: "전체")을 선택합니다.

4. 특정 사용자를 검색하는 경우 로그인 이름, 이름 또는 성을 선택적으로 입력할 수 있습니다.
5. "Search"(검색)를 클릭합니다.
검색 결과가 나타납니다.
6. 변경할 사용자 왼쪽의 확인란을 선택합니다. 또는 전체 목록을 변경하려면 맨 위의 확인란을 클릭합니다.
7. "다음에 대한 값 설정" 목록에서 항목을 선택합니다.
 - 시그마 SLA 상속
 - 시그마 SLA
 - 성공률 SLA 상속
 - 성공률 SLA
 - 트랜잭션 시간 SLA 상속
 - 트랜잭션 시간 SLA선택 항목에 따라 값 텍스트 상자나 "|No"(예|아니요) 목록이 나타납니다.
8. 값을 입력하거나 "Yes"(예) 또는 "No"(아니요)를 선택하고 "설정"을 클릭합니다.

상관 관계 SLA 구성

하나의 SLA 를 전체 사용자 그룹에 사용하거나 사용자 그룹과 무관하게 트랜잭션마다 하나씩 SLA 를 사용하는 대신에 비즈니스 서비스나 비즈니스 트랜잭션별로 사용자 그룹의 SLA 를 설정해야 할 경우가 있습니다.

아래 표는 트랜잭션과 사용자 위치를 기반으로 허용되는 여러 응답 시간의 예입니다.

사용자 그룹/비즈니스 트랜잭션을 기반으로 허용되는 응답 시간	로컬	원격	해외
Login	3 초	6 초	9 초
Buy	5 초	7 초	10 초

상관 관계 SLA 를 사용하면 사용자 그룹, 비즈니스 서비스 및 결합된 비즈니스 트랜잭션별로 SLA 를 설정할 수 있습니다. 상관 관계 SLA 는 비즈니스 트랜잭션 또는 사용자 그룹에 대해 설정된 단일 차원 SLA 에 대한 다차원 대안으로 생각할 수 있습니다.

참고: 상관 관계 SLA 는 도메인, 비즈니스 트랜잭션 또는 사용자 그룹 SLA 를 대체하지 않습니다. 상관 관계 SLA 는 이러한 SLA 에서 상속되지 않으며 CEM 관리자는 특정하게 상관 관계 SLA 를 설정해야 합니다.

상관 관계 SLA 를 구성하는 절차는 다음과 같습니다.

- [상관 관계 SLA 보기](#) (페이지 331)
- [상관 관계 SLA 추가](#) (페이지 332)
- [기존 상관 관계 SLA 업데이트](#) (페이지 333)
- [상관 관계 SLA 삭제](#) (페이지 334)

상관 관계 SLA 보기

이미 생성된 상관 관계 SLA 를 검토하거나 SLA 를 찾아 선택하여 삭제하려면 다음 절차를 따르십시오.

하나의 테이블에서 모든 상관 관계 SLA 를 볼 수는 없습니다. 왜냐하면 일반적인 프로덕션 시스템에서 모든 사용자 그룹, 비즈니스 서비스 및 비즈니스 트랜잭션의 매트릭스가 엄청나게 크기 때문입니다. 그러나 제공된 비즈니스 서비스 또는 사용자 그룹의 상관 관계 SLA 를 보는 것은 가능합니다.

사용자 그룹과 비즈니스 트랜잭션별로 상관 관계 SLA 를 보려면

1. "관리", "상관 관계 SLA"를 선택합니다.
2. "표시" 필드에서 "사용자 그룹별" 또는 "비즈니스 서비스별"을 선택합니다.
3. 두 번째 필드에서 그룹 또는 서비스를 선택합니다.
4. 세 번째 필드에서 "전체"를 선택하거나 그룹 또는 서비스를 선택합니다.
5. "새로 고침"을 클릭합니다.

지정된 사용자 그룹이나 비즈니스 서비스에 대한 상관 관계 SLA 가 나타납니다.

상관 관계 SLA 추가

이 절차에서는 사용자 그룹/비즈니스 서비스/비즈니스 트랜잭션 집합에 대한 상관 관계 SLA 를 새로 만드는 방법을 설명합니다.

상관 관계 SLA 를 추가하려면

1. "관리", "상관 관계 SLA"를 선택합니다.
2. 만들려는 상관 관계 SLA 가 없는지 확인합니다. 기존 상관 관계 SLA 를 변경하려면 [기존 상관 관계 SLA 업데이트](#) (페이지 333)를 참조하십시오.
3. "새로 만들기"를 클릭합니다.
4. 다음과 같이 사용자 그룹/비즈니스 서비스/비즈니스 트랜잭션당 상관 관계 설정을 정의합니다.
 - a. 사용자 그룹 - 사용자 그룹 이름을 선택하거나 "전체"를 선택합니다.
 - b. "영역"을 선택합니다.
 - c. 비즈니스 서비스 - 비즈니스 서비스 이름을 선택하거나 "전체"를 선택합니다.
 - d. 비즈니스 트랜잭션 - 비즈니스 트랜잭션 이름을 선택하거나 "전체"를 선택합니다.
 - e. SLA 값을 설정합니다.

성공률 SLA

성공률 서비스 수준 계약(%)입니다. 기본값은 없습니다.

시그마 SLA

시그마 서비스 수준 계약(숫자)입니다. 시그마 점수는 DPMO(백만 기회당 결함 수)에서 계산되는 측정값입니다. 허용 가능한 시그마 점수는 4.00일 수 있고 거의 완벽은 6.00이며 완벽(트랜잭션 결함 전혀 없음)은 무한대입니다. 기본값은 없습니다.

트랜잭션 시간 SLA

트랜잭션 시간 서비스 수준 계약(초)입니다. 기본값은 없습니다.

5. "저장"을 클릭합니다.
목록에 새 상관 관계 SLA 가 나타납니다.

참고: 새로 만들어도 기존 상관 관계 SLA 는 변경되지 않습니다. 예를 들어 사용자 그룹 A(UG-A), 비즈니스 서비스 X(BP-x) 및 비즈니스 트랜잭션 3(BT-3)에 대한 상관 관계 SLA 가 이미 있는 경우 UG-A, PB-x 및 모든 비즈니스 트랜잭션에 대한 비즈니스 서비스를 새로 만들어도 이전에 UG-A/BT-x/BT-3 에 대해 정의한 SLA 는 변경되지 않습니다.

참고: 비즈니스 서비스의 모든 비즈니스 트랜잭션에 대한 상관 관계 SLA 를 만들고 나중에 다른 비즈니스 트랜잭션을 추가하는 경우 추가된 비즈니스 트랜잭션에 대한 SLA 를 새로 만들어야 합니다. 이 비즈니스 트랜잭션에 대한 SLA 는 자동으로 추가되지 않습니다.

기존 상관 관계 SLA 업데이트

기존 상관 관계 SLA 를 변경하려면 "업데이트" 단추를 사용하십시오.

기존 상관 관계 SLA 를 변경하려면

1. "관리", "상관 관계 SLA"를 선택합니다.
2. 수정할 상관 관계 SLA 를 선택합니다. 변경할 상관 관계 SLA 를 표시하려면 "표시", "비즈니스 서비스" 및 "사용자 그룹" 목록과 "새로 고침"을 사용합니다.
3. "업데이트"를 클릭합니다.
4. 필드를 설정하여 변경할 상관 관계 SLA 를 지정합니다.
5. SLA 값을 설정합니다.
6. "업데이트"를 클릭합니다.
목록에 업데이트된 상관 관계 SLA 가 나타납니다.

상관 관계 SLA 삭제

더 이상 필요없는 상관 관계 SLA 를 삭제할 수 있습니다.

상관 관계 SLA 를 삭제하려면

경고! "삭제"를 클릭하면 SLA 가 즉시 삭제됩니다. 이 삭제와 관련된 "~하시겠습니까?" 대화 상자는 없습니다.

1. "관리", "상관 관계 SLA"를 선택합니다.
2. 삭제할 상관 관계 SLA 를 선택합니다.
3. 삭제를 클릭합니다.

사용자 그룹 삭제

사용자 그룹과 모든 관련 트랜잭션 통계를 삭제할 수 있습니다. 이 작업을 수행해야 하는 경우는 다음과 같습니다.

- 사무실을 닫고 해당 그룹의 트랜잭션 정보가 더 이상 필요없는 경우
- 그룹을 병합하려는 경우, 즉 사용자를 한 그룹에서 다른 그룹으로 이동한 다음 비어 있는 그룹을 삭제하려는 경우
- 사용자 그룹을 자동 생성할 때 필요한 것보다 많은 사용자 그룹이 생성되는 경우

중요! 사용자가 없는 사용자 그룹을 포함하여 필요 없는 사용자 그룹을 삭제하십시오. 사용자 그룹이 너무 많으면 성능이 저하될 수 있습니다.

사용자 그룹을 삭제하려면

1. "관리" > "사용자 그룹"을 선택합니다.
2. "사용자 그룹" 탭에서 삭제할 사용자 그룹의 확인란을 선택합니다.
3. 삭제를 클릭합니다.

사용자 비활성화 또는 삭제

CA CEM 에서 오랫동안 모니터링되지 않을 것이라고 알고 있는 사용자는 일시적으로 비활성화할 수 있습니다. 이 경우 트랜잭션 기록과 사용자 기록은 유지됩니다. 비활성화한 사용자의 새 트랜잭션이 관찰되면 사용자가 자동으로 다시 활성화됩니다.

사용자를 삭제하면 사용자의 트랜잭션 기록만 유지됩니다. 삭제한 사용자는 관리 페이지에 표시되지 않습니다. 사용자의 기록은 보고서에 흐리게 나타납니다. 삭제한 사용자의 새 트랜잭션이 관찰되면 새 사용자가 생성됩니다. 모니터링 중인 응용 프로그램이 해당 사용자에게 의해 다시 사용되는 일이 절대로 없을 거라고 확신하는 경우에만 사용자를 삭제해야 합니다.

사용자를 비활성화하거나 삭제하려면

1. "관리" > "사용자 그룹"을 선택합니다.
2. "사용자 검색"을 클릭하고 비활성화하거나 삭제해야 하는 특정 사용자를 검색합니다.
3. 비활성화하거나 삭제할 사용자를 선택합니다.
4. "비활성화" 또는 "삭제"를 클릭합니다.

사용자 다시 활성화

과거에 사용자를 비활성화한 경우 해당 사용자를 다시 활성화하려면 다음과 같이 하십시오.

사용자를 활성화하려면

1. "관리" > "사용자 그룹"을 선택합니다.
2. "사용자 검색"을 클릭하고 활성화해야 하는 특정 사용자를 검색합니다.
3. 활성화할 사용자를 선택합니다.
4. "활성화"를 클릭합니다.

제 20 장: CA CEM 에서 시스템 작업 관리

이 장에서는 오류 보고서 검토, 디스크 공간 및 메모리 검사 등과 같이 CA CEM 이 올바르게 작동하고 있는지 확인하기 위해 관리자가 수행하는 작업을 설명합니다.

다음 목록에서는 CA CEM 모니터링 이벤트와 CA CEM 감사 내역 보기에 대해 알아두어야 하는 사항을 보여 줍니다.

1. [CA CEM 이벤트에 대해 알아봅니다](#) (페이지 337).
2. [CA CEM 이벤트를 검토합니다](#) (페이지 341).
3. [필수 CA CEM 이벤트를 유지 관리합니다](#) (페이지 341).
4. [오류, 주의 등의 전자 메일 알림 이벤트를 보내도록 CA CEM 을 구성합니다](#) (페이지 341).
5. [메모리 사용량, 디스크 공간 등의 TIM 컴퓨터 정보를 검토합니다](#) (페이지 343).
6. [CA CEM 감사 내역을 검토합니다](#) (페이지 345).

CA CEM 이벤트 정보

CA CEM 이 이벤트를 캡처하고 로깅하므로 시스템 작업과 성능에 영향을 미칠 수 있는 이벤트에 대한 정보가 사용자에게 계속 전달될 수 있습니다. 정기적으로 이벤트 로그를 검토하는 것이 좋습니다.

심각도 수준

이벤트의 심각도 수준은 다음 세 가지가 있습니다.

- 정보
- 주의
- 오류

가능한 이벤트 목록

CA CEM 은 다음 시스템 이벤트를 캡처하고 로깅합니다.

이벤트	심각도	범주	세부 정보
비즈니스 응용 프로그램 이름이 잘못되었습니다.	오류	CA APM TG	CA APM TG 스크립트의 비즈니스 응용 프로그램 이름에 <또는> 등의 잘못된 문자가 포함되어 있습니다. CA APM TG 에서 CA CEM 응용 프로그램 이름을 수정하고 스크립트를 다시 마이그레이션하십시오.
데이터베이스 정리 서비스가 시작되었습니다.	정보	처리	데이터베이스 정리 서비스가 시작되었습니다. 서비스를 실행 중인 Enterprise Manager 의 IP 주소는 이벤트 목록에 지정되어 있습니다.
데이터베이스 정리 서비스가 중지되었습니다.	정보	처리	데이터베이스 정리 서비스가 중지되었습니다. 서비스를 실행 중이었던 Enterprise Manager 의 IP 주소는 이벤트 목록에 지정되어 있습니다.
결함이 드롭되었습니다.	주의	처리	수용 능력 프로세싱 오버로드로 인해 하나 이상의 결함이 드롭되었습니다. 이는 인시던트별로 보고됩니다.
중복된 세션 ID 를 발견했습니다.	주의	모니터링	가능한 이유: 둘 이상의 TIM 이 동일한 트래픽을 모니터링하고 있습니다. 여러 로그인 의 세션 ID 가 동일합니다. 이 경우 세션 ID 에 사용된 매개 변수에 문제가 있는 것일 수 있습니다.
Enterprise Manager 가 TIM 에 액세스할 수 없습니다.	오류	통신	Enterprise Manager 가 TIM 에 액세스하여 데이터를 검색할 수 없습니다.
Enterprise Manager 가 다시 시작했습니다.	정보	Administration	Enterprise Manager 에 대해 날짜 및 시간이 다시 시작되었습니다.

이벤트	심각도	범주	세부 정보
HTTP 분석기 플러그인 오류	오류	처리	HTTP 분석기 플러그인 오류가 발생했습니다.
새 구성 요소 추가 제한을 초과했습니다.	주의	처리	이 이벤트는 "새 비식별 구성 요소 검색"을 선택한 경우에만 발생할 수 있습니다. 최대 비식별 구성 요소 수가 초과되면 가장 오래된 구성 요소가 새 구성 요소로 바뀝니다. 이러한 경우가 발생할 때마다 "새 구성 요소 추가 제한을 초과했습니다."가 로깅됩니다. 구성 요소 자동 검색에 대한 자세한 내용은 <i>CA APM 트랜잭션 정의 안내서</i> 를 참조하십시오.
로그인이 드롭되었습니다.	주의	처리	수용 능력 프로세싱 오버로드로 인해 하나 이상의 로그인이 드롭되었습니다.
네트워크 데이터가 없습니다.	주의	통신	TIM 이 일정 시간 동안 네트워크를 통해 데이터를 수신하지 않았습니다. 예를 들어 케이블이 이동했거나 네트워크 스위치가 제대로 구성되지 않았거나 네트워크 토폴로지가 변경되어 더 이상 CA CEM 구성과 일치하지 않습니다.
통계 집계 서비스가 시작되었습니다.	정보	처리	통계 집계 서비스가 시작되었습니다. 서비스를 실행 중인 Enterprise Manager 의 IP 주소는 이벤트 목록에 지정되어 있습니다.
통계 집계 서비스가 중지되었습니다.	정보	처리	통계 집계 서비스가 중지되었습니다. 서비스를 실행 중이었던 Enterprise Manager 의 IP 주소는 이벤트 목록에 지정되어 있습니다.
TIM 수집 서비스가 시작되었습니다.	정보	처리	TIM 수집 서비스가 시작되었습니다. 서비스를 실행 중인 Enterprise Manager 의 IP 주소는 이벤트 목록에 지정되어 있습니다.

이벤트	심각도	범주	세부 정보
TIM 수집 서비스가 중지되었습니다.	정보	처리	TIM 수집 서비스가 중지되었습니다. 서비스를 실행 중이었던 Enterprise Manager의 IP 주소는 이벤트 목록에 지정되어 있습니다.
디스크 공간이 적어서 TIM이 데이터 파일 중 일부를 삭제했습니다.	정보	관리	TIM이 디스크 공간을 보호하기 위해 데이터 파일 중 일부를 삭제했습니다. 기본적으로 디스크가 75% 가득 차면 파일이 삭제됩니다. 이 동작은 "TIM Settings"(TIM 설정) 페이지의 "DiskSpace/MinFreeDataSpaceInPercent"로 결정됩니다.
TIM이 다시 시작되었습니다.	정보	Administration	TIM에 대해 날짜 및 시간이 다시 시작되었습니다.
트랜잭션 정의가 드롭되었습니다.	정보	처리	이 이벤트는 자동 트랜잭션 검색이 설정된 경우에만 발생할 수 있습니다. 즉, 수용 능력 프로세싱 오버로드로 인해 자동으로 검색된 트랜잭션 정의 중 일부가 드롭되었음을 나타냅니다. 이 이벤트가 표시되면 자동 트랜잭션 검색을 해제하고 한 번 더 실행해 보십시오.
사용자 그룹 제한에 도달했습니다.	주의	처리	IP 서브넷별로 자동으로 생성되는 최대 사용자 그룹 수에 도달했습니다. 이는 사용자 그룹별로 보고됩니다.
WTG 에이전트가 중지되었습니다.	주의	CA APM TG	CA APM TG 에이전트를 사용할 수 없습니다.
WTG 에이전트가 실행 중입니다.	정보	CA APM TG	CA APM TG 에이전트를 사용할 수 있습니다.

CA CEM 이벤트 보기

주기적으로 CA CEM 이벤트를 모니터링하여 네트워크 문제, 시스템 또는 백업 실패, HTTP 분석기 플러그인 오류 등을 나타내는 흔적을 찾을 수 있습니다.

다음 단계를 따르십시오.

1. "시스템" > "이벤트"를 선택합니다.
CA CEM 이벤트 목록이 나타납니다.
2. 자세한 내용을 확인할 이벤트 이름을 클릭합니다.
이벤트 정보 페이지가 나타납니다.
3. "시스템" > "이벤트"를 선택하여 이벤트 목록으로 돌아갑니다.

CA CEM 이벤트 관리

이벤트를 유지할 기간(일)을 지정할 수 있습니다.

다음 단계를 따르십시오.

1. "시스템" > "이벤트"를 선택하고 "이벤트 관리자" 탭을 클릭합니다.
현재 CA CEM 이벤트 설정이 나타납니다.
2. 이벤트 설정을 정의합니다.

다음 이후 이벤트 삭제

CA CEM 이벤트가 이벤트 로그에서 삭제되기 전에 경과할 기간(일)입니다.

3. "저장"을 클릭합니다.

이벤트의 전자 메일 알림 수신

이벤트 발생 시 전자 메일 알림을 보내도록 CA CEM 을 구성할 수 있습니다.

최소한 CA CEM 관리자는 오류 이벤트의 전자 메일 알림을 수신하도록 이벤트 전자 메일 알림을 설정해야 합니다.

다음을 지정할 수 있습니다.

- 알림을 전송할 대상 전자 메일 주소
- 알릴 이벤트
- 메시지의 제목 및 본문 텍스트

이벤트의 전자 메일 알림을 보내도록 CA CEM 을 구성하려면

1. "시스템" > "이벤트"를 선택하고 "이벤트 관리자" 탭을 클릭합니다.

현재 CA CEM 이벤트 설정이 나타납니다.

2. "이벤트 전자 메일 알림" 확인란을 선택합니다.

"이벤트 알림 설정"이 나타납니다.

3. 전자 메일 알림에 사용하거나 사용하지 않도록 설정할 각 이벤트 옆의 확인란을 선택합니다.

확인란은 전환 옵션입니다. 현재 "사용 안 함" 상태인 경우 확인란을 선택하고 "저장"을 클릭하면 해당 이벤트에 대한 전자 메일 알림이 시작되고 "사용" 상태가 됩니다. 현재 "사용" 상태인 경우 확인란을 선택하고 "저장"을 클릭하면 해당 이벤트에 대한 전자 메일 알림이 중지되고 "사용 안 함" 상태가 됩니다.

참고: 상태 필드는 이벤트에 대한 전자 메일 알림이 사용하도록 설정되었는지 또는 사용하지 않도록 설정되었는지를 나타냅니다. 모든 이벤트는 전자 메일 알림 상태와 관계없이 "이벤트" 페이지에 나타납니다.

4. (선택 사항) Enterprise Manager 와 TIM 의 하위 집합에서만 전자 메일 알림을 수신하려면 IP 주소 범위를 지정합니다.

예를 들어 TIM 이 아닌 Enterprise Manager 에 대해서만 전자 메일 알림을 표시하려면 Enterprise Manager 주소는 포함하고 TIM 주소는 제외하는 IP 주소 범위를 지정합니다.

5. 필요한 경우 전자 메일의 "보낸 사람" 주소와 "받는 사람" 주소를 편집합니다.

6. (선택 사항) "메시지" 필드를 편집합니다. 다음과 같이 변수를 사용하여 사용자 지정된 설명을 생성합니다.

- <id>
- <name>
- <severity>
- <category>

- <source>
- <ipaddress>
- <desc>
- <time>

변수를 다시 정렬하여 사용자 고유의 메시지를 생성할 수 있습니다. 각 변수는 전자 메일 알림을 보낼 때 실제 이벤트 값으로 바뀝니다.

팁: "예" 영역의 변수와 텍스트를 복사하여 "메시지" 필드에 붙여 넣을 수 있습니다.

7. "저장"을 클릭합니다.
8. SMTP 서버 설정이 올바른지 확인합니다. [SMTP 서버 설정 구성](#) (페이지 309)을 참조하십시오.

TIM 컴퓨터의 건전성 검토

정기 유지 관리를 수행하려는 경우와 문제를 해결하는 경우에는 TIM 컴퓨터의 건전성을 검사해야 합니다. 여기에는 디스크 및 메모리 사용량과 컴퓨터에서 실행 중인 프로세스에 대한 검토가 포함됩니다.

참고: 이러한 건전성 보고서를 보려면 "Wily System Setup"(Wily 시스템 설정) 페이지에 액세스해야 합니다.

TIM 컴퓨터의 건전성에 대한 스냅샷을 보려면

1. "설정" > "모니터"를 선택합니다.
2. 맨 오른쪽의 "TIM 건전성" 열에서 "보고서 가져오기"를 클릭합니다.
3. 로그인 대화 상자가 표시되면 "Wily System Setup"(Wily 시스템 설정) 페이지에 대한 사용자 이름과 암호로 로그인합니다. 기본 사용자 이름은 admin입니다.
"어플라이언스 건전성" 페이지가 나타납니다.

4. "Complete Appliance Health"(전체 어플라이언스 건전성) 링크를 클릭합니다.
또는 다른 링크 중 하나를 클릭하여 건전성 보고서의 단일 섹션을 봅니다.
각 링크에 대한 자세한 내용은 ["어플라이언스 건전성" 페이지 참조 테이블](#) (페이지 344)을 참조하십시오.
5. 각 TIM 컴퓨터마다 위의 단계를 반복합니다.

"어플라이언스 건전성" 페이지 참조 테이블

이 테이블에서는 "어플라이언스 건전성" 페이지의 각 링크에 대해 표시된 정보를 설명합니다.

링크	정보	해당하는 Linux 명령
Disk Information(디스크 정보)	파일 시스템 디스크 공간 사용량(MB)을 표시합니다. 80%를 초과하는 경우와 같이 디스크 사용량이 너무 높으면 TIM 로그 파일을 삭제하여 디스크 공간 사용량을 줄이십시오.	df -m
Memory Information(메모리 정보)	사용 가능한 시스템 메모리 및 사용된 시스템 메모리 양(MB)을 표시합니다. 사용 가능한 메모리 양이 낮아지면 과도한 메모리 스와핑(스래싱)을 주의해야 합니다. TIM 에서 스래싱의 가장 큰 원인은 아마도 플러그 인일 것입니다. 플러그 인 코드를 수정하여 해당 메모리 사용량을 개선해야 할 수 있습니다.	free -m
Logged in Users(로그인한 사용자)	컴퓨터 자체에 로그인한 사용자를 모두 표시합니다. 일반적으로 사용자가 표시되면 안 됩니다. 그러나 SSH(보안 셸)를 통해 로그인한 사용자와 같이 컴퓨터에 로그인한 루트 사용자가 표시될 수 있습니다. 인식하지 못한 사용자가 표시되면 즉시 조사하십시오.	who

Currently Running Processes(현재 실행 중인 프로세스)	실행 중인 프로세스를 모두 표시합니다. CMD 열에서 프로세스 경로를 나타내는 표준 구문과 일부 ASCII 아트를 사용하여 표시합니다. 목록에서 비정상적으로 높은 CPU 사용량과 예기치 않은 프로세스가 있는지 살펴봅니다.	<code>ps -efl --forest</code>
--	--	-------------------------------

Complete Appliance Health(전체 어플라이언스 건전성)	위 정보를 모두 표시합니다.	위 참조
--	-----------------	------

CA CEM 감사 내역 보기

CEM 관리자는 CA CEM 동작에 대한 감사 내역을 볼 수 있습니다.

관리 정보 페이지에서 CA CEM 동작을 볼 수 있습니다. 목록 페이지에서는 감사 정보를 사용할 수 없습니다.

감사 내역 정보를 보려면

- 감사할 관리 페이지 중 하나를 선택합니다.
 - "관리" > "비즈니스 서비스"
 - "설정" > "도메인"
 - "시스템" > "전자 메일 설정"
- 주소의 URL 끝에 `&showHistory=true` 또는 `?showHistory=true` 를 추가합니다. 앰퍼샌드(&)나 물음표(?)를 사용합니다.
 - URL 이 `.html?pid=600001` 처럼 끝나는 경우 다음과 같이 앰퍼샌드를 사용합니다.

```
http://<IP_Address>:8081/wily/ceM/tess/app/admin/tranDefGroupList.html?pid=1&showHistory=true
```

```
http://<IP_Address>:8081/wily/ceM/tess/app/admin/domainDetail.html?pid=1&showHistory=true
```

- URL 이 `.html` 로 끝나는 경우에는 다음과 같이 물음표를 사용합니다.

```
http://<IP_Address>:8081/wily/ceM/tess/app/system/emailSettings.html?showHistory=true
```

3. "실행"을 클릭하거나 Enter 키를 눌러 감사 내역을 봅니다.
페이지 아래쪽에 감사 내역이 나타납니다.
4. 페이지에서 아래로 스크롤하여 Wily CEM 감사 정보를 봅니다. 최근 200 개의 변경 사항이 나타납니다.
5. 원할 경우 쿼리 문자열 끝에 `&maxResults=nnn` 을 추가하여 200 개의 레코드를 표시하는 기본값을 재정의할 수 있습니다.

예:

```
http://<IP_Address>:8081/wily/cem/tess/app/system/emailSettings.html?showHistory=true&maxResults=500
```

제 21 장: CA CEM 을 사용하여 보고

다음 목록에서는 CA CEM 보고에 대해 알아두어야 하는 사항을 보여 줍니다.

1. [CA CEM 보고서와 시스템 탐색 시 해당 보고서를 캡처하는 방법에 대해 알아봅니다](#) (페이지 347).
2. [정기적으로 필요한 CA CEM 보고서를 예약합니다](#) (페이지 354).

CA CEM 보고서 캡처

여러 방법으로 CA CEM 데이터를 분석할 수 있습니다. CA CEM 메뉴를 탐색하고 인스턴트와 결합별 쿼리뿐 아니라 비즈니스 서비스, 비즈니스 트랜잭션 및 사용자 그룹에 기반한 쿼리도 수행할 수 있습니다.

보고서 옵션은 선택한 보고서 유형에 따라 다릅니다. 예를 들어 추세 보고서를 선택한 경우 추세 분석에서 비교할 기본 및 보조 시간 프레임을 지정해야 합니다.

보고서 출력 대안에 대한 자세한 내용은 [보고서 배포](#) (페이지 348)를 참조하십시오.

사용 가능한 보고서에 대한 자세한 내용은 [보고서 형식](#) (페이지 349)을 참조하십시오.

CA CEM 시스템 데이터 보존 선택 항목과 통계 집계 일정은 보고서 출력에 영향을 미칠 수 있습니다. 자세한 내용은 [보고서 시간 프레임](#) (페이지 350)을 참조하십시오.

CA CEM 보고서 집계 정보

CA CEM 집계는 보고서에 나타나는 데이터에 영향을 미칩니다. CA CEM 에서 매일, 매주, 매월 및 매년 통계를 집계하는 방법을 이해하십시오.

CA CEM 보고서는 집계된 비즈니스 트랜잭션 통계를 기반으로 합니다. 한 시간에 한 번씩 시간별 집계를 포함하는 통계 처리가 실행됩니다.

시간별 통계 집계 프로세스가 완료된 후 하루에 한 번씩 자정에 다음이 실행됩니다.

- 일별 집계 프로세스
- 주별 집계 프로세스
- 월별 집계 프로세스

하루에 한 번씩 실행되는 집계가 성능 측면에서 가장 좋은 방법이지만 보고서에 미치는 영향에 유의해야 합니다. 예:

- 오늘 오후 5 시에 매주 또는 매월 보고서를 실행하는 경우 보고서 통계에는 자정까지의 데이터가 포함됩니다. 이 보고서는 오늘에 대한 통계를 포함하지 않습니다.
- 통계 집계 서비스를 실행하는 Enterprise Manager 가 자정에 실행되지 않으면 다음 자정에 Enterprise Manager 가 실행될 때까지 집계 프로세스가 실행되지 않습니다. 따라서 어제의 통계를 찾는 경우 해당 통계가 일별(어제 시간 프레임), 주별, 월별 또는 연도별 보고서에 포함되지 않습니다.
- 오늘 시간 프레임의 보고서 통계는 집계된 일별 데이터보다 약간 더 오래 걸립니다.
- 매년 보고서는 매월 집계 데이터를 기반으로 합니다.

보고서 배포

CA CEM 은 다음과 같은 여러 방법으로 CA CEM 보고서를 캡처하고 관리할 수 있습니다.

- CA CEM 데이터를 쿼리할 때 온라인으로 보고서 보기
- "내 보고서" 목록에서 미리 정의된 보고서 보기
- 저장하거나 인쇄할 수 있는 PDF 파일 생성
- PDF 파일을 사용자 또는 사용자 그룹에 전자 메일로 보내기
- 나중에 실행하여 볼 수 있도록 보고서 저장
- 매일, 매주 또는 매월 전자 메일을 통해 배포하거나 실행하도록 보고서 예약

보고서 데이터 보안

비즈니스 서비스와 관련 데이터에 대한 CA CEM 사용자 액세스를 제한할 보안 그룹이 있으면 Embedded Entitlements Manager 보안 영역만 있는지 확인하십시오.

로컬 영역과 Embedded Entitlements Manager 영역이 있는 경우처럼 여러 영역이 있는 경우에는 CA CEM 사용자가 예약된 보고서에서 액세스 권한을 가지고 있지 않은 데이터를 볼 가능성이 있습니다.

영역 구성에 대한 자세한 내용은 *CA APM 보안 안내서*를 참조하십시오.

보고서 형식

CEM 탭에서 다음과 같은 페이지를 탐색할 때 CA CEM 보고서를 캡처할 수 있습니다.

- 서비스 수준 관리
 - 트랜잭션 SLA - 성능 및 품질
 - 사용자 SLA - 성능 및 품질
 - 상관 관계 SLA
 - 트랜잭션 추세 - 성능 및 품질
 - 사용자 추세 - 성능 및 품질
 - 비즈니스 가치
- 인시던트 관리
 - 인시던트
 - 주요 영향 요인
 - 결함
 - 트랜잭션 추적 세션
- 성능 보고서
 - 비즈니스 서비스
 - 사용자 그룹

- 품질 보고서
 - 비즈니스 서비스
 - 사용자 그룹
- 분석 그래프
 - 성공률
 - 시간
 - 처리량
 - 크기
 - 볼륨
 - 수
 - 산출량
 - 결함 - 빈도
 - 세션 사용

보고서 시간 프레임

CA CEM 은 다음과 같은 여러 방법으로 보고서 뷰 시간 프레임을 지정할 수 있습니다.

시간 프레임	현재	이전	Custom
시간	해당 없음	이전 시간	사용자 지정 시간
일	오늘	어제	사용자 지정 요일
주	이번 주	이전 주	사용자 지정 주
Month(월)	이번 달	이전 달	사용자 지정 달
년	이번 연도	이전 연도	해당 없음

참고: 보고서 시간 프레임을 선택하는 경우와 예약된 보고서를 지정하는 경우에는 CA CEM 시스템 집계 및 데이터 보존 설정을 고려해야 합니다. 통계가 아직 집계되지 않은 경우, 데이터가 삭제된 경우 또는 인시던트 설정이 변경된 경우에는 보고서가 예상한 것과 다를 수 있습니다.

CA CEM 관리자는 보고 목적에 맞게 필요한 데이터를 보존하도록 시스템을 구성해야 합니다. 그러나 최상의 시스템 성능을 얻으려면 CA CEM 통계를 주기적으로 삭제해야 합니다. 데이터 보존 설정에 대한 자세한 내용은 [CA CEM 도메인 정의](#) (페이지 293)를 참조하십시오.

CA CEM 시스템에서는 매시간, 매일, 매주 및 매월 통계를 유지하기 위해 데이터를 집계합니다. 집계는 성능과 확장성을 위해 사용되는 도구이기도 합니다. CA CEM 집계에 대한 자세한 내용은 [CA CEM 보고서 집계 정보](#) (페이지 347)를 참조하십시오.

보고서 탐색

보고서를 사용할 수 있는 CEM 페이지에는 다양한 옵션이 있습니다.

PDF

PDF 링크를 클릭하면 PDF 형식의 보고서가 표시됩니다. 보고서를 파일로 저장하거나 PDF 를 인쇄할 수 있습니다.

전자 메일 PDF

"전자 메일 PDF" 링크를 클릭하면 PDF 보고서가 첨부된 전자 메일을 보낼 수 있는 페이지가 새로 열립니다.

보고서 저장 또는 예약

"보고서 저장 또는 예약" 링크를 클릭하면 보고서를 저장하거나 예약할 수 있는 "내 보고서" 페이지로 이동합니다.

먼저 쿼리를 수행하고 유효한 데이터로 보고서 페이지를 새로 고쳐야 해당 보고 옵션 중 하나를 클릭할 수 있습니다.

참고: 브라우저의 "새 창에서 열기" 옵션을 사용하는 경우와 같이 두 번째 CEM 보고서 페이지가 열린 후에 PDF 링크를 클릭하면 오류가 발생합니다. 첫 번째 CEM 보고서 페이지로 돌아가서 "새로 고침"을 클릭하고 PDF 링크를 다시 클릭하십시오.

PDF 보고서

PDF 링크를 클릭하면 파일로 저장하거나 인쇄할 수 있는 Adobe Acrobat PDF 형식의 보고서가 열립니다.

보고서를 인쇄하려면

1. Internet Explorer 에서 "파일" > "인쇄"를 클릭하여 PDF 형식의 보고서를 인쇄합니다.
2. "뒤로" 단추를 클릭하여 이전 페이지로 돌아갑니다.

보고서를 파일로 저장하려면

1. Internet Explorer 에서 "파일" > "다른 이름으로 저장"을 클릭합니다.
2. 보고서를 저장할 위치를 찾습니다. 보고서에 대해 적절한 파일 이름을 입력합니다. "저장"을 클릭하여 보고서를 파일로 저장합니다.

참고: 이름을 변경하지 않으면 이름은 *WilyCEMReport.pdf* 입니다.

3. "뒤로" 단추를 클릭하여 이전 페이지로 돌아갑니다.

PDF 보고서에 사용자 고유의 로고를 사용하려면

- APM 데이터베이스의 ts_settings 테이블에 있는 reports.userImage 를 바꿉니다.

참고: 전자 메일로 보낸 보고서에는 사용자의 로고를 사용할 수 없습니다.

보고서를 전자 메일로 보내기

전자 메일 링크를 사용하여 보고서를 PDF 형식으로 보낼 수 있습니다. 새 창이 열리면서 전자 메일 양식이 표시됩니다.

보고서를 전자 메일로 보내려면

1. 전자 메일 양식에 정보를 입력합니다.

시작

로그인한 사용자의 전자 메일 주소입니다. 전자 메일 주소를 제공하지 않은 경우 `tess-default.properties` 파일의 `email.defaultFromAddress` 에서 채워진 주소가 사용됩니다([기본 tess-default.properties 파일](#) (페이지 591) 참조).

끝

전자 메일 주소 또는 메일 그룹을 쉼표로 구분된 목록으로 입력합니다.

참고: 세미콜론을 사용하여 전자 메일 주소를 구분하지 마십시오.

제목

첨부된 보고서에 대해 의미 있는 제목 행을 입력합니다.

Message

보고서의 표준 메시지에 적절한 정보를 추가합니다.

2. "보내기"를 클릭합니다.

참고: 전자 메일을 통해 보고서를 보내려면 CEM 시스템 관리자가 메일 SMTP 서버를 구성해야 합니다.

저장되거나 예약된 보고서

"보고서 저장 또는 예약" 및 "내 보고서" 기능을 사용하면 정기적으로 예약된 일정(매일, 매주 또는 매월)에 따라 실행되도록 보고서를 설정할 수 있습니다. 그러면 CA CEM 시스템에서 지정된 시간에 보고서를 생성하고 전자 메일을 통해 보냅니다.

자세한 내용은 [보고서 예약](#) (페이지 354)을 참조하십시오.

보고서 예약

CA CEM 은 다음 두 가지 방법으로 보고서를 예약할 수 있습니다.

- ["내 보고서"에서 보고서를 정의하고 예약합니다](#) (페이지 354).
- [원하는 보고서를 생성하고 예약합니다](#) (페이지 357).

"내 보고서"를 사용하여 보고서 예약

이 단원에서는 "내 보고서"를 통해 수동으로 보고서를 예약하는 방법을 설명합니다.

다음 단계를 따르십시오.

1. "CEM" > "내 보고서"를 선택하고 "새로 만들기"를 클릭합니다.
2. 목록에서 보고서 형식을 선택합니다. 각 보고서 형식마다 추가 정보가 필요한데, 이는 선택 항목에 따라 다릅니다.

자세한 내용은 [보고서 형식](#) (페이지 349)을 참조하십시오.

"비즈니스 가치" 보고서에는 다음 정보가 필요합니다.

비즈니스 응용 프로그램

특정 비즈니스 응용 프로그램을 선택하거나 "전체"를 선택합니다.

비즈니스 서비스

특정 비즈니스 서비스를 선택하거나 "전체"를 선택합니다.

시간 프레임

시간, 일, 주, 월 또는 연도를 지정합니다.

전자 메일을 통해 이 보고서의 PDF 버전을 보내도록 예약

선택적으로 전자 메일을 통해 이 보고서를 보내도록 예약하는 옵션을 선택할 수 있습니다.

자세한 내용은 [보고서 시간 프레임](#) (페이지 350)을 참조하십시오.

"사용자 추세 품질" 보고서에는 다음 정보가 필요합니다.

비즈니스 응용 프로그램

특정 비즈니스 응용 프로그램을 선택하거나 "전체"를 선택합니다.

비즈니스 서비스

특정 비즈니스 서비스를 선택하거나 "전체"를 선택합니다.

비즈니스 트랜잭션

선택 항목은 선택한 비즈니스 서비스에 따라 다릅니다. 특정 비즈니스 트랜잭션을 선택하거나 "전체"를 선택합니다.

사용자 그룹

특정 사용자 그룹을 선택하거나 "전체"를 선택합니다.

기본 시간 프레임

시간, 일, 주, 월 또는 연도를 지정합니다. 일반적으로 현재 시간 프레임(예: 이번 주)입니다.

보조 시간 프레임

시간, 일, 주, 월 또는 연도를 지정합니다. 일반적으로 이전 시간 프레임입니다. 예를 들어 오늘을 어제와 비교하거나 이번 주를 지난 주, 지난 달 또는 지난 연도와 비교할 수 있습니다.

전자 메일을 통해 이 보고서의 PDF 버전을 보내도록 예약

선택적으로 전자 메일을 통해 이 보고서를 보내도록 예약하는 옵션을 선택할 수 있습니다.

3. 보고서를 실행할 빈도를 결정합니다.

일별

보고서를 실행할 시간을 선택합니다.

Weekly(주별)

보고서를 실행할 시간과 요일을 선택합니다.

Monthly(월별)

보고서를 실행할 시간과 날짜를 선택합니다.

중요! 선택한 날짜가 없는 특정 달에는 보고서가 해당 월에 전송되지 않습니다. 예를 들어 31 일을 선택한 경우 31 일이 없는 달에는 보고서가 전송되지 않습니다.

4. 보고서를 실행할 시간을 결정하고 되풀이 시간을 설정합니다.

팁: 보고서에 지난 1 시간 동안의 데이터를 포함하려면 1 시간 뒤에 실행되도록 보고서를 예약하는 것이 좋습니다. 그러면 통계 프로세스가 완료될 때까지 넉넉한 시간을 잡을 수 있습니다.

CA CEM 집계에 대한 자세한 내용은 [CA CEM 보고서 집계 정보](#) (페이지 347)를 참조하십시오.

5. 전자 메일 설정을 정의합니다.

팁: 제목 행과 메시지를 사용하여 보고서를 받는 사람에게 보고서 유형, 실행 빈도, 질문이 있을 경우에 문의할 연락처 이름 등을 알려 주는 것이 좋습니다.

보낸 사람 주소

보고서를 보낸 사람의 전자 메일 주소를 입력합니다. 예를 들어 보고서를 받는 사람이 다른 전자 메일 주소에 회신하도록 하려는 경우 이 주소를 변경할 수 있습니다.

보낸 사람 이름

전자 메일 주소와 연결된 이름을 입력합니다. 일반적으로 관리자의 이름이거나 담당하는 CA CEM 사용자의 이름입니다.

끝

전자 메일 주소 또는 메일 그룹을 선택으로 구분된 목록으로 입력합니다.

제목

이 보고서에 대해 의미 있는 제목 행을 입력합니다.

Message

이 보고서에 대해 유용한 메시지를 입력합니다.

6. "저장"을 클릭합니다. 보고서 목록에 새 보고서가 나타납니다.

모든 CA CEM 사용자가 자신이 생성한 보고서를 볼 수 있지만 CA CEM 시스템 관리자만 다른 CA CEM 사용자가 생성한 보고서를 볼 수 있습니다.

팁: 모든 보고서 이름을 일관되게 지정하면 필요한 보고서를 쉽게 찾을 수 있습니다. 예를 들어 모든 보고서 이름에 다음을 포함할 수 있습니다.

- 포함된 비즈니스 응용 프로그램, 서비스 및 트랜잭션
- 포함된 사용자 그룹
- 빈도

보고서 생성 및 예약

이 단원에서는 원하는 옵션으로 생성한 보고서를 예약하는 방법의 예를 제공합니다.

보고서를 생성 및 예약하려면

1. 원하는 페이지로 이동하고 원하는 방식으로 보고서 뷰를 생성합니다.
예:
 - a. "CEM" > "서비스 수준 관리" > "사용자 추세"를 선택합니다.
 - b. 보고서에서 보려는 "사용자 그룹", "비즈니스 응용 프로그램", "비즈니스 서비스" 및 "비즈니스 트랜잭션"을 선택합니다.
 - c. "기본" 및 "보조" 시간 프레임을 선택합니다.
 - d. "품질"을 클릭하여 사용자 그룹에 대한 품질 보고서를 봅니다.
 - e. "새로 고침"을 클릭하여 품질 보고서에 대한 페이지를 업데이트합니다.
 - f. "보고서 저장 또는 예약"을 클릭합니다.

방금 본 "사용자 추세 품질" 보고서의 모든 보고서 설정이 미리 채워진 "내 보고서" 페이지가 나타납니다.

2. 필요에 따라 미리 채워진 보고서 설정을 수정합니다.
3. "전자 메일을 통해 이 보고서의 PDF 버전을 보내도록 예약" 확인란을 선택합니다.
"되풀이 설정" 및 "전자 메일 설정" 옵션이 나타납니다.
4. 필요에 따라 되풀이 설정을 정의합니다.
5. 필요에 따라 전자 메일 설정을 정의합니다.
6. "저장"을 클릭하여 이 보고서를 예약합니다.

보고서 예약 옵션에 대한 자세한 내용은 ["내 보고서"를 사용하여 보고서 예약](#) (페이지 354)을 참조하십시오.

CA CEM 데이터 내보내기

"데이터 내보내기" 탭에서 CA CEM 데이터를 내보낼 수 있습니다. 이 탭을 통해 비즈니스 통계, 결함 및 인시던트 데이터를 검색할 수 있습니다.

다음에 대한 CA CEM 데이터를 내보낼 수 있습니다.

- 지정된 시간 범위 내의 집계되거나 집계되지 않은 비즈니스 통계
- 지정된 시간 범위 내 결함, 마지막 N 개 결함 및 마지막 X 분 내 결함
- 지정된 시간 범위 내 인시던트

참고: 전자 상거래 모드에서는 통계 데이터의 사용자 정보를 내보낼 수 없습니다.

데이터 내보내기

이 단원에서는 CA CEM 데이터를 내보내는 방법의 예를 제공합니다.

다음 단계를 따르십시오.

1. "CEM", "데이터 내보내기", "통계 데이터"를 클릭합니다.
"통계 데이터" 뷰가 나타납니다.
2. 다음 옵션을 조합해서 지정합니다.
 - a. 데이터에서 보려는 "보고서 유형", "비즈니스 응용 프로그램", "비즈니스 서비스" 및 "비즈니스 트랜잭션"을 선택합니다.

- b. "사용자 그룹"이나 "사용자"를 선택합니다.

참고: 집계되지 않은 보고서 유형을 선택하면 사용자 그룹만 선택할 수 있습니다.

- c. "시작 날짜"와 "끝 날짜"를 지정합니다.

참고: 기본적으로 현재 시스템 날짜 및 시간이 표시됩니다.

- d. 집계되지 않은 보고서 유형의 경우 "매시간", "매일", "매주", "매월" 등의 간격을 선택합니다.

- e. (선택 사항) 트랜잭션 "처리량", "크기" 및 "시간" 백분위 값을 지정합니다.

"처리량", "크기" 및 "시간" 필드는 트랜잭션의 백분위수 값을 나타냅니다. 세미콜론은 여러 백분위수를 구분하는 데 사용됩니다. 예를 들어 "처리량"을 "25; 50; 75"로 저장할 수 있습니다. 이러한 필드에서 "전체"를 지정하여 5에서 95까지 5단위로 증가하는 백분위수 값을 포함할 수도 있습니다.

참고: 기본적으로 트랜잭션 "처리량", "크기" 및 "시간"은 50%입니다.

- f. "CSV 형식으로 저장"을 클릭합니다.

"File Download"(파일 다운로드) 대화 상자가 표시되고 통계 데이터가 들어 있는 CSV 파일이 열립니다.

3. "CEM", "데이터 내보내기", "결함 데이터"를 클릭합니다.

"결함 데이터" 뷰가 나타납니다.

4. 다음 옵션을 조합해서 지정합니다.

- a. 내보낸 데이터에서 보려는 비즈니스 응용 프로그램, 비즈니스 서비스 및 비즈니스 트랜잭션을 선택합니다.

- b. 사용자 그룹과 결함 유형을 선택합니다.

"콘텐츠 오류" 결함 유형을 사용하면 결함 데이터에서 내보낼 콘텐츠 문자열 값을 지정할 수 있습니다.

- c. "시작 날짜"와 "끝 날짜"를 지정하거나 "마지막 N 개" 결함(0-1000)을 지정하거나 "마지막 X 분"(0-1440)을 지정합니다.

- d. (선택 사항) 결함의 일부로 검색할 "메타 키"를 지정합니다.

메타 키는 결함의 HTTP 응답 및 요청 헤더에 지정된 값입니다.

참고: 세미콜론은 여러 메타 키를 구분하는 데 사용됩니다. 메타 키는 대/소문자를 구분합니다.

e. (선택 사항) 결합 있는 비즈니스 트랜잭션의 구성 요소 타이밍 정보를 포함하려면 "예"를 선택합니다.

f. "CSV 형식으로 저장"을 클릭합니다.

"File Download"(파일 다운로드) 대화 상자가 표시되고 결합 데이터가 들어 있는 CSV 파일이 열립니다.

5. "CEM", "데이터 내보내기", "인시던트 데이터"를 클릭합니다.

"인시던트 데이터" 뷰가 나타납니다.

6. "시작 날짜"와 "끝 날짜"를 지정합니다.

7. "CSV 형식으로 저장"을 클릭합니다.

"File Download"(파일 다운로드) 대화 상자가 표시되고 인시던트 데이터가 들어 있는 CSV 파일이 열립니다.

보고서 저장 또는 예약

"내 보고서" 탭에서 "결합 데이터", "인시던트 데이터" 또는 "통계 데이터" 보고서 형식을 선택하여 보고서의 CA CEM 데이터를 저장하거나 예약할 수 있습니다.

참고: 예약된 CA CEM 데이터 보고서는 .zip 파일로 전자 메일에 첨부되어 사용자에게 전송됩니다. 크기가 800KB 보다 큰 CSV 보고서는 여러 부분으로 동일하게 분할된 다음 .zip 파일로 전자 메일에 첨부되어 전송됩니다.

보고서 예약 옵션에 대한 자세한 내용은 ["내 보고서"를 사용하여 보고서 예약](#) (페이지 354)을 참조하십시오.

CSV 헤더

다음 단원에서는 일부 CSV 헤더에 대해 설명합니다.

- **TransactionThroughputPercentile(Bytes/s)** - <백분위수 요청> 열의 수는 백분위수 요청 수에 따라 달라집니다. 예를 들어, 처리량 = 25; 40; 75 는 지정된 각 백분위수 요청에 대해 3 개의 열을 만듭니다. 지정된 백분위수 요청이 없으면 **TransactionThroughputPercentile - 50%** 열이 기본적으로 존재합니다.
- **DefectValue** 는 특정 트랜잭션에 대한 결함이 발생하기 위해 충족되어야 하는 조건입니다.
- **MissingID** 와 **MissingName** 은 결함 유형 9 에 대해서만 생성됩니다. **MissingID** 와 **MissingName** 은 누락된 트랜잭션 구성 요소 또는 트랜잭션 단위의 ID 와 이름을 나타냅니다.
- "이유"는 인시던트를 종결할 때 제공된 이유를 나타냅니다. 시스템이 인시던트를 종료하는 경우(예: BT 가 삭제된 경우)에는 이유가 "비즈니스 트랜잭션이 삭제됨"과 같이 표시됩니다.
- **CloseBy** 는 인시던트를 종결하는 사용자의 사용자 이름을 나타냅니다.
- **Evidence1, Evidence2, Evidence3** 은 영향 임계값이 각각 "보통", "심각함", "중요"일 때 생성된 증거 수집 파일의 이름을 나타냅니다.
- "상태" 열에서 1 은 종결, 2 는 개설, 3 은 보류 중, 4 는 만료 처리를 나타냅니다.
- **TriggerDate** 는 인시던트가 생성된 시기를 나타냅니다.
- **DefectType** 에 대한 자세한 내용은 *CA APM API 참조 안내서*의 "결함 명령 매개 변수 및 구문" 단원을 참조하십시오.
- **UserImportance, DefectImportance** 및 **TransactionImportance** 에 대한 자세한 내용은 [인시던트 관련 설정 정의](#) (페이지 299)를 참조하십시오.

제 22 장: CA CEM 을 사용하여 보안 웹 응용 프로그램 모니터링

다음 목록에는 SSL 기반 보안을 사용하는 웹 응용 프로그램을 모니터링하도록 CA CEM 을 설정하는 것과 관련된 주요 작업이 나와 있습니다.

1. [웹 서버 SSL 개인 키를 얻습니다](#) (페이지 363).
2. [SSL 개인 키가 PEM 파일에 있는지 확인합니다](#) (페이지 363).
필요한 경우 개인 키를 변환합니다.
3. [SSL 용으로 CA CEM 을 구성하고 CA CEM 에 PEM 파일을 업로드합니다](#) (페이지 369).
4. [SSL 을 사용하여 CA CEM 을 확인합니다](#) (페이지 370).

SSL 개인 키 가져오기 및 관리

CA CEM 에서 여러 개인 키를 지원하므로 서로 다른 개인 키를 사용하여 다양한 HTTPS 서버의 SSL 트래픽을 분석할 수 있습니다. CA CEM 은 Apache 및 OpenSSL 기반 서버에서 사용하는 PEM 개인 키 형식을 지원합니다. Microsoft IIS, SunONE, iPlanet 및 Netscape 에서도 개인 키 형식을 사용하지만 해당 키를 CA CEM 에서 사용할 PEM 파일로 변환할 수 있습니다. CA CEM 에서는 캡처하는 데이터의 암호를 해독하는 데 필요한 키가 자동으로 식별됩니다.

변환을 수행하는 데 사용되는 시스템에서 OpenSSL 버전을 사용할 수 있어야 합니다. OpenSSL 은 <http://www.openssl.org>에서 제공됩니다.

지원되는 웹 서버의 SSL 개인 키를 얻는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- [Apache 또는 OpenSSL 기반 웹 서버](#) (페이지 364)
- [Microsoft IIS\(인터넷 정보 서비스\)](#) (페이지 364)
- [SunONE, iPlanet 또는 Netscape 엔터프라이즈 서버](#) (페이지 365)

Apache 또는 OpenSSL 기반 웹 서버 개인 키 저장

Apache 또는 OpenSSL 기반 웹 서버 개인 키 파일을 저장해 두었다가 CA CEM 에서 사용할 수 있습니다.

다음 단계를 따르십시오.

1. 서버 구성 파일을 찾습니다. 예:

```
/etc/httpd/conf.d/ssl.conf
```

2. 개인 키 파일을 가리키는 SSL 인증서 키 파일을 찾습니다. 예:

```
SSLCertificateKeyFile=/etc/httpd/conf/ssl.key/server.key
```

3. 해당 파일을 복사하고 이름을 output.pem 으로 바꿉니다.

자세한 내용은 <http://httpd.apache.org/> 및 <http://www.openssl.org/>를 참조하십시오.

Microsoft Internet Information Service(IIS) 개인 키 내보내기 및 변환

Microsoft IIS(인터넷 정보 서비스) 개인 키는 CA CEM 에서 읽을 수 있는 형식으로 내보내야 합니다. 이 형식은 PFX 입니다. 변환을 수행하는 데 사용되는 시스템에서 OpenSSL 버전을 사용할 수 있어야 합니다. <http://www.openssl.org/>에서 OpenSSL 을 얻을 수 있습니다.

먼저 IIS 서버에서 개인 키를 내보낸 다음 출력 파일을 PEM 형식으로 변환합니다.

키를 PFX 형식으로 내보내려면

1. IIS 를 실행 중인 Windows 기반 시스템에서 "시작", "실행"을 차례로 클릭합니다.
2. MMC.exe 를 입력하고 "확인"을 클릭합니다.
3. "콘솔" 메뉴를 클릭하고 "스냅인 추가/제거"를 클릭합니다.
4. "Add"(추가)를 클릭합니다. "인증서" 스냅인을 선택하고 "추가"를 클릭합니다.
5. "컴퓨터 계정"을 선택하고 "다음"을 클릭합니다.
6. "로컬 컴퓨터"를 선택하고 "확인"을 클릭합니다.
7. "닫기", "확인"을 차례로 클릭합니다.

8. "인증서" 메뉴를 확장하고 "개인" 폴더를 클릭합니다. 내보낼 인증서를 마우스 오른쪽 단추로 클릭하고 "모든 작업" > "내보내기"를 선택합니다.

마법사가 나타납니다.

9. 개인 키를 포함하고 PFX 파일을 얻을 때까지 마법사를 계속 진행하려면 확인란을 선택합니다.

PFX 파일을 PEM 키 파일로 변환하려면

1. OpenSSL 소프트웨어를 실행 중인 시스템에서 다음 명령을 입력하십시오.

```
openssl pkcs12 -in filename.pfx -nocerts -out output.pem
```

2. *filename.pfx* 를 만든 파일의 이름으로 바꿉니다.
3. *output.pem* 을 만들고 있는 출력 파일의 이름으로 바꿉니다.
4. 명령을 실행합니다.

이 PEM 파일을 생성할 때 지정된 암호는 이 파일을 TIM 에 업로드할 때 사용하는 암호입니다.

SunONE, iPlanet 또는 Netscape Enterprise Server

Sun, SunONE, iPlanet 및 Netscape 웹 서버는 모두 동일한 핵심 기술을 기반으로 합니다. 이러한 웹 서버의 개인 키는 CA CEM 에서 읽을 수 있는 형식으로 내보내야 합니다.

변환을 수행하기 위해 사용하는 시스템에서 다음 유틸리티를 사용할 수 있어야 합니다.

- OpenSSL
- NSS(Network Security Services)
- NSPR(Netscape Portable Runtime)

다음 단계에서는 Windows 시스템이 변환에 사용된다고 가정합니다.

개인 키 파일을 생성하려면

- 다음과 같이 키 관리 유틸리티를 다운로드하고 추출합니다.
 - OpenSSL. <http://www.openssl.org/>에서 제공됩니다.
 - NSS(Network Security Services). <http://www.mozilla.org/projects/security/pki/nss/>에서 제공됩니다.
 - NSPR(Netscape Portable Runtime). <http://www.mozilla.org/projects/nspr/>에서 제공됩니다.
- 파일을 추출합니다.
 - ZIP 파일을 임시 디렉터리에 추출합니다.
 - nss-3.9.zip 파일을 c:\에 추출합니다.
 - nspr-4.4.1 파일을 c:\에 추출합니다.
- Win32-OpenSSL-v0.9.7c** 에 해당: Win32-OpenSSL-v0.9.7c 를 실행하고 C:\OpenSSL 디렉터리에 설치합니다.
- 다음 줄을 포함하도록 PATH 변수를 수정합니다.
c:\nss-3.9\lib;c:\nspr-4.4.1\lib
SunONE/iPlanet/Netscape 인증서와 키가 확장명이 .db 인 파일에 저장됩니다.
- *.db 파일을 쓰기 가능한 디렉터리(이 예의 경우 c:\dbfiles)에 복사합니다.
- 명령 프롬프트를 열고 다음을 입력합니다.
cd c:\nss-3.9\bin
기본적으로 NSS 도구는 이름이 key3.db 및 cert7.db 인 파일을 찾습니다. 데이터베이스 파일에 key3.db 와 cert7.db 이외의 이름이 지정된 경우 파일 이름을 바꾸지 마십시오. 그 대신 -P(접두사) 스위치를 제공하여 certutil 및 pk12util 이 규칙에 맞지 않는 이름이 지정된 파일을 찾을 수 있도록 합니다.
예를 들어 파일에 prodSite-cert.db 와 prodSite-key.db 라는 이름이 지정된 경우 certutil 명령을 사용하여 prodSite-cert7.db 와 prodSite-key3.db 파일을 생성합니다. 다음 명령의 출력에는 포함된 인증서 이름이 표시됩니다.
certutil -P prodSite- -K -d C:\dbfiles\
7. NSS 인증서 DB 의 암호 또는 PIN 을 입력합니다(데이터베이스 암호 입력).
prodSite-cert7.db 와 prodSite-key3.db 파일이 생성됩니다.

내보내기와 변환을 수행하려면

1. 프롬프트에서 다음을 입력합니다.

```
pk12util -P prodSite- -d C:\dbfiles\ -o C:\dbfiles\output.p12 -n Server-Cert
```

2. NSS 인증서 DB의 암호 또는 PIN을 입력합니다(데이터베이스 암호 입력).
3. PKCS12 파일의 암호를 입력합니다(출력 암호 입력).
4. 암호를 다시 입력합니다(출력 암호 다시 입력).

이제 C:\dbfiles 디렉터리에 output.p12 라는 파일이 있습니다.

출력 암호는 이 파일을 Enterprise Manager 에 업로드할 때 필요한 암호입니다.

5. OpenSSL\bin 디렉터리에서 다음 명령을 실행하십시오.

```
openssl pkcs12 -in C:\dbfiles\output.p12 -nodes -out C:\dbfiles\pkcs12out.txt
```

이 명령을 실행하면 pkcs12 구조가 MAC 및 모음 정보가 포함된 텍스트 파일로 변환됩니다. 이 명령은 개인 키와 인증서가 포함된 PEM 파일도 생성됩니다.

pkcs12out.txt 파일의 내용은 다음 예제와 비슷합니다.

```
Enter Import Password:
MAC verified OK
Bag Attributes
localKeyID: 01 00 00 00
1.3.6.1.4.1.311.17.1: Microsoft Enhanced Cryptographic Provider v1.0
friendlyName: 98849c683ad0e90810a77235bd728b12_668b93c6-0795-
4ba7-9da8-78737a299d3f
Key Attributes
X509v3 Key Usage: 10
-----BEGIN RSA PRIVATE KEY-----
MIICXQIBAAKBgQDLIwhdY7ngYk/AlomX9rqnaZfb8PdJ+Mc6msuRWBUDHeIH2eV1
yiL7ID/0vkUN6qGnnqVuMQ3kuy7mnN/qSPz37/FKTbwF10Q0P2LCZVuhU6SI/90Q
1rTINqQEPi1hyPV10LDv8Fjev80jMD1gvjaCmP84FzcryDgHonh4nQIDAQAB
AoGAUXaJIjjeDjge15MHNuQBUqXr+o4V/ZpA+2WcgXsbYhaX0KI3fRdFFASI4XN0
ZdpolP7oY/cdF6w5EFsVc64t7dIpD+AineQpGeYJ4WhmBstyVlBSHb9drcCQDFg
vvcyfm13tTL3MfecV3WhENU6889iGogbgLMMQvqmtOCFDPY7fPM3I38FbEw03Yu+
gWEZ/f7DLdDSt7GDKf0CQQDSaQxwTMabqGB6bWxqy6M5lpWBW8YAQAXpKhLILRqb
C/Jx fd63KTN90pegkhE0Bn50dqtqfS4kodv45bHeHYxn
-----END RSA PRIVATE KEY-----
Bag Attributes
localKeyID: 01 00 00 00
subject=/C=US/ST=Utah/L=SLC/O=MooseCo./OU=Moose
Land/CN=www.megamoose.com
issuer=/C=US/ST=Utah/L=SLC/O=MooseCo./OU=Moose
Land/CN=www.megamoose.com
-----BEGIN CERTIFICATE-----
MIICgDCCAemgAwIBAgIDBJ3zMA0GCSqGSIb3DQEBAUAMIGSMQswCQYDVQQGEwJa
QTEVMBMGAlUECBMMV2VzdGVybiBDYXBlMRIwEAYDVQQHEwLDYXBlIFRvd24xDzAN
BgNVBAoTB1RoYXd0ZTEdMBsGA1UECxMUQ2VydGlmawNhdGUgU2VydmljZXMxKDAm
BgNVBAMTH1BlcnNvbmsIEZyZWVtYWVsIFJTSQAyMDAwLjguMzAwHhcNMDEwNDE3
MDAzNzU5WhcNMDEwNDE3MDAzNzU5WjBFMR8wHQYDVQQDEwZUaGF3dGUgRnJlZW1h
aWwgTWVtYmV5MSIwIAYJKoZIhvcNAQkBFhNqbGV2eUBzb25pY3dhbGwuY29tMIGf
MA0GCSqGSIb3DQEBAQUAA4Ger3DBiQKBBgQDLIwhdY7ngYk/AlomX9rqnaZfb8PdJ
Y29tMAwGA1UdEwEB/wQCMAAwDQYJKoZIhvcNAQEEBQADgYEAChF7eiQDoCQ08snA
izV22+7FwiEKSR0PLc0FTyty0UJoQ0RLt7SPqKPJ2NswyC0A2nHgn0FL7ImFGiAi
5Xg9LEAtscgC7ceo0C3GBKorPE8hiqGCuVcCLYLws7yGRWRPTzQp7TemCoAM0cv
i0/6K6qicSzUpEj7eYqCbogmEYU=
-----END CERTIFICATE-----
```


6. 다음 예제처럼 키 구문을 복사하여 PEM 확장명을 갖는 별도 파일에 붙여넣습니다.

```
-----BEGIN RSA PRIVATE KEY-----
MIICXQIBAAKBgQDLIwhdY7ngYk/AlomX9rqnaZfb8PdJ+Mc6msuRwBUDHeIH2eV1
yiL7ID/0vkUN6qGnnqVuMQ3kuy7mnN/qSPz37/FKTbwF10QOP2LCZVuhU6SI/90Q
1rTINqQEPi1hyPV10LDv8Fjevvhv80jMD1gvjaCmP84FzcryfyDgHonh4nQIDAQAB
AoGAUXaJIjjeDjge15MHNuQBUqXr+o4V/ZpA+2WcgXsbYhaX0KI3fRdFFASI4XN0
ZdpolP7oY/cdF6w5EFsVc64t7dIpD+AineQpGeYJ4WhmBstyVlBShNb9drcCQDFg
vvcyfm13tTL3MfecV3WhENU6889iGogbgLMMQvqmtOCFDPY7fPM3I38FbEw03Yu+
gWEZ/f7DLDDsT7GDKf0CQQDSaQxwTMabqGB6bWxqy6M5lpWBW8YAQAXpKHLILRqB
C/JxFD63KTN90pegkhE0Bn50dqtqfS4kodv45bHeHYxn
-----END RSA PRIVATE KEY-----
```

SSL 용으로 CA CEM 구성

다음 단계를 따르십시오.

1. "설정" > "HTTPS 설정"을 선택합니다.
2. 주소 유형을 선택합니다.
3. 선택한 주소 유형에 따라 이더넷 또는 웹 서버 IP 를 지정합니다.
 웹 서버 IP 의 경우 하나의 주소 또는 주소 범위를 입력합니다.
 샘플 범위 입력: 172.16.10.2~172.16.10.15
 공백 없이 단일 하이픈으로 두 주소를 구분합니다.
4. 웹 서버 포트 번호를 지정합니다.
5. 클라이언트 컴퓨터에 있는 output.pem 파일의 위치로 이동하고 output.pem 파일을 선택합니다.
 개인 키 파일을 PEM 형식으로 변환하려면 [SSL 개인 키 가져오기 및 관리](#) (페이지 363)를 참조하십시오.
6. PEM 파일을 만들 때 사용한 암호를 "키 파일 전달 구" 필드에 입력합니다.
 PEM 파일을 만들 때 암호를 사용하지 않은 경우 이 필드를 공백으로 두십시오.
7. "저장"을 클릭하여 PEM 파일을 업로드합니다.
 각 웹 서버마다 다른 output.pem 파일이 있는 경우 각 웹 서버마다 위의 단계를 반복합니다.

HTTPS 서버에 대한 여러 키 정보

키마다 각기 다른 포트 또는 주소가 있는 경우 하나의 HTTPS 서버나 다양한 HTTPS 서버가 여러 개인 키를 지원할 수 있습니다. 예를 들어, 내부 사용자를 위한 하나의 키와 외부 사용자를 위한 또 다른 키가 있는 하나의 HTTPS 서버를 사용할 수 있습니다. 이 경우 내부 키에 대해 하나의 포트를 사용하고 외부 키에 대해 또 다른 포트를 사용할 수 있습니다.

동일한 주소 또는 주소 범위/포트 쌍에 대해 두 번째 키를 입력하면 첫 번째 키를 덮어쓰게 됩니다. 중복되는 주소 범위가 있는 경우 키가 별도로 유지됩니다. 하지만 TIM 은 실제 IP 주소와 포트도 포함하는, 처음 발견한 하나의 키만 사용합니다.

SSL 을 사용한 CA CEM 확인

다음 단계를 따르십시오.

1. [CEM 콘솔에서](#) (페이지 263) "TIM System Setup"(TIM 시스템 설정) 페이지에 액세스합니다.
2. "View TIM Transaction Inspection"(TIM 트랜잭션 검사 보기)을 클릭합니다.
3. TIM 이 모니터링할 컴퓨터의 IP 주소를 입력합니다.
4. "시작"을 클릭하여 SSL 로 정의된 트랜잭션 모니터링을 시작합니다.
5. 지금까지 정의한 단순 HTTPS 트랜잭션을 실행합니다.
몇 초 뒤에 트랜잭션 검사 데이터가 페이지에 나타납니다.
6. 트랜잭션 검사가 완료된 경우 "중지"를 클릭합니다.

참고: "중지"를 클릭하지 않으면 검사 데이터가 계속해서 수집됩니다.

제 23 장: CA CEM 에서 Napatech 어댑터 사용

Napatech 어댑터를 설치하면 트래픽이 많은 일부 환경에서 TIM 성능이 개선될 수 있습니다.

이 섹션은 다음 항목을 포함하고 있습니다.

[CA CEM 에서 Napatech 어댑터 사용 정보](#) (페이지 371)

[Napatech 어댑터 및 소프트웨어 얻기](#) (페이지 372)

[Napatech 어댑터 및 Napatech 소프트웨어 설치](#) (페이지 372)

[Napatech 어댑터를 사용하도록 설정하고 모니터링](#) (페이지 374)

[\(선택 사항\) Napatech 필터를 생성하고 사용하도록 설정](#) (페이지 374)

[기타 Napatech 어댑터 작업](#) (페이지 377)

[Napatech 어댑터 문제 해결](#) (페이지 379)

CA CEM 에서 Napatech 어댑터 사용 정보

TIM 컴퓨터에 어댑터를 설치하면 TIM 에서 패킷을 드롭하는 문제를 방지할 수 있습니다. 이는 다음과 같은 방법으로 작동할 수 있습니다.

- TIM 에서 처리할 수 있을 때까지 패킷이 어댑터 버퍼에 저장됩니다.
- 어댑터가 트래픽을 필터링하여 TIM 에서 분석할 트래픽을 줄일 수 있습니다.
- CPU 가 Napatech 어댑터에서 데이터를 읽는 데 걸리는 시간은 대부분의 다른 이더넷 어댑터에서 데이터를 읽는 데 걸리는 시간보다 적으므로 TIM 에서 CPU 를 사용할 수 있는 시간이 늘어납니다.

어댑터가 중복 패킷을 제거할 수 있는데, 이는 SPAN 포트가 동일한 패킷을 두 번 이상 보는 경우에 좋습니다.

TIM 에서 Napatech 어댑터를 사용하는 프로세스는 다음과 같습니다.

1. [올바른 어댑터와 소프트웨어를 얻습니다.](#) (페이지 372)
2. [어댑터와 소프트웨어를 설치합니다.](#) (페이지 372)

3. [어댑터를 사용하도록 TIM 을 구성합니다.](#) (페이지 374)
4. [\(선택 사항\) 어댑터에 대한 필터를 생성하고 사용하도록 설정합니다.](#) (페이지 374)

Napatech 어댑터 및 소프트웨어 얻기

TIM 에 대해 지원되는 어댑터는 4 개의 전기 기가비트 인터페이스가 있는 Napatech NT4E-4T PCIe 어댑터뿐입니다. 이 어댑터는 광 케이블과 함께 사용할 수 없습니다.

올바른 어댑터와 사용자에게 필요한 Napatech 소프트웨어를 모두 제공할 수 있는 리셀러는 Network Allies, LLC 뿐입니다. 이 Napatech 소프트웨어는 NT4E-4T PCIe 어댑터 전용입니다.

참고: Multi-Port Monitor 어플라이언스에서 실행 중인 TIM 은 다양한 Napatech 어댑터를 지원합니다. 지원되는 어댑터에 대한 자세한 내용은 CA Support 에서 제공되는 *CA APM Compatibility Guide*(CA APM 호환성 안내서)를 참조하십시오.

Napatech 어댑터와 Napatech 소프트웨어를 얻으려면

- Network Allies 에서 NT4E-4T PCIe 어댑터(부품 번호 801-0075-0800CA)를 구입합니다.
패키지에는 소프트웨어 및 설치 지침을 포함한 DVD 와 USB 플래시 드라이브가 모두 들어 있습니다.

Napatech 어댑터 및 Napatech 소프트웨어 설치

DVD 및 USB 플래시 드라이브에는 다음이 포함되어 있습니다.

- Napatech 하드웨어 설치 지침
- TIM 에 설치하는 소프트웨어 이미지
- 예제 필터 파일

어댑터를 설치하려면

1. DVD 및 USB 플래시 드라이브와 함께 제공된 *NT4E-4T Hardware Installation Guide*(NT4E-4T 하드웨어 설치 안내서)의 지침을 따릅니다. TIM 컴퓨터의 PCI Express 슬롯에 어댑터를 설치합니다.
2. 모니터링 포트(대개 eth1)에서 어댑터에 있는 임의의 포트로 트래픽 모니터링 케이블을 이동하십시오.

참고: 나중에 [Napatech 어댑터를 사용하도록 설정하고 모니터링](#) (페이지 374)을 수행한 후에 이 단계를 수행할 수도 있습니다. 나중에 수행하면 데이터 손실이 줄어듭니다. 그러나 지금 수행하면 서버 공간으로 이동하는 횟수가 한 번 줄어듭니다.

소프트웨어를 설치하려면

1. Napatech 소프트웨어 이미지(napatech-<version>.image)를 네트워크에서 사용할 수 있는 상태로 만듭니다.
2. TIM 의 "Wily System Setup"(Wily 시스템 설정) 페이지에서 napatech-<version>.image 를 설치합니다. TIM 소프트웨어 설치에 대한 일반 정보는 *CA APM 설치 및 업그레이드 안내서*를 참조하십시오.
3. (선택 사항) "Wily System Setup"(Wily 시스템 설정) 페이지로 이동하여 Napatech 소프트웨어가 설치되었는지 확인합니다.

소프트웨어가 설치된 경우 글머리 기호 행 "Napatech <installation timestamp>"가 페이지에 나타납니다. 이 행은 링크가 아닙니다.

4. (선택 사항) Napatech 드라이버 로그를 검토합니다.
 - a. "TIM 시스템 설정" 페이지에서 "Configure Napatech"(Napatech 구성)를 클릭합니다.
 - b. "View the Napatech Driver Log"(Napatech 드라이버 로그 보기)를 클릭합니다.
 - c. 로그를 검토합니다.

예를 들어 이 페이지에 다음과 같은 로그 행이 표시되면

```
4B85587F.00030BC4 | #WARN | NOTE: The adapter will have limited throughput.
4B85587F.00030D15 | #WARN | Link negotiated to 4 lanes. Adapter supports 8 lanes.
```

8 라인 슬롯 대신 4 라인 슬롯에 Napatech 어댑터를 설치한 것입니다. 이 경우 Napatech 보드의 성능은 영향을 받을 수 있지만 Napatech 보드의 작동은 중지되지 않습니다.

Napatech 어댑터를 사용하도록 설정하고 모니터링

Napatech 어댑터와 Napatech 소프트웨어를 설치했다면 다음 절차에 따라 Napatech 어댑터를 사용하도록 설정하고 ntxc0:0 포트를 모니터링하도록 TIM 을 구성하십시오.

어댑터를 사용하도록 설정하려면

1. "TIM 시스템 설정" 페이지에서 "Configure Napatech"(Napatech 구성)를 클릭합니다.

"TIM Napatech Configuration"(TIM Napatech 구성) 페이지가 나타납니다.

2. "Enable Napatech"(Napatech 사용)를 클릭하고 TIM 을 다시 시작합니다.
TIM 이 실행 중이 아닌 경우 "Enable Napatech"(Napatech 사용)를 클릭합니다. TIM 을 시작하여 모니터링을 시작합니다.

어댑터를 사용하도록 TIM 네트워크 모니터 인터페이스를 구성하려면

1. TIM 의 "System Setup"(시스템 설정) 페이지에서 "Configure TIM Network Interfaces"(TIM 네트워크 인터페이스 구성)를 클릭합니다.

TIM 네트워크 모니터 인터페이스 구성에 대한 일반 정보는 *CA APM 설치 및 업그레이드 안내서*를 참조하십시오.

2. ntxc0:0 인터페이스를 선택하고 "설정"을 클릭합니다.

다른 인터페이스에서 ntxc0:0 으로 트래픽 모니터링 케이블을 이동했거나 이동할 계획인 경우 사용 중이 아닌 인터페이스의 확인란을 선택 취소합니다. TIM 은 ntxc0:0 인터페이스와 eth1 등의 다른 인터페이스에서 모니터링하거나 ntxc0:0 인터페이스에서만 모니터링할 수 있습니다.

3. 트래픽 모니터링 케이블을 어댑터 포트 중 하나에 아직 연결하지 않았으면 지금 연결합니다. 모니터링 포트(대개 eth1)에서 어댑터에 있는 임의의 포트에 트래픽 모니터링 케이블을 이동하십시오.

(선택 사항) Napatech 필터를 생성하고 사용하도록 설정

Napatech 어댑터를 사용하면 하드웨어의 패킷을 필터링할 수 있습니다.

필터는 NTPL(Napatech 프로그래밍 언어)로 작성되고 TIM 에 업로드됩니다. 예제 필터 파일을 사용하십시오. 예제 필터 파일은 USB 플래시 드라이브에 있습니다.

TIM 자체에서 웹 서버 IP 주소별로 트래픽을 필터링할 수 있습니다. 이러한 방법으로 TIM 모니터링을 구성하는 방법에 대한 자세한 내용은 *CA APM 설치 및 업그레이드 안내서*를 참조하십시오. 그러나 Napatech 어댑터를 사용하여 단독으로 필터링하는 것이 가장 좋습니다. 하드웨어 필터링이 더 빠릅니다.

TIM 에 대한 웹 서버 필터와 Napatech 필터를 설정한 경우 해당 필터는 AND 로직으로 결합됩니다. 즉, 필터의 교집합이 결과로 나타납니다.

필터를 생성하고 Napatech 어댑터에 사용하도록 설정하려면

1. DVD 또는 USB 플래시 드라이브에서 예제 필터 파일(sample_filter.ntpl)을 복사하고 메모장이나 vi 와 같은 단순 텍스트 편집기를 사용하여 해당 환경에 맞게 편집합니다.

참고: DeleteFilter=all 명령이 파일의 시작 부분에 있는지 확인하십시오.

2. "TIM 시스템 설정" 페이지에서 "Configure Napatech"(Napatech 구성)를 클릭합니다.

"TIM Napatech Configuration"(TIM Napatech 구성) 페이지가 나타납니다.

3. "Upload a Napatech Hardware Filter Configuration File"(Napatech 하드웨어 필터 구성 파일 업로드)을 클릭합니다.

"TIM Napatech Hardware Filter Configuration"(TIM Napatech 하드웨어 필터 구성) 페이지가 나타납니다.

4. 파일을 찾아서 업로드하고 설치합니다.

5. (선택 사항) 필터가 설치되었는지 확인합니다.

- a. "TIM 시스템 설정" 페이지에서 "Configure Napatech"(Napatech 구성)를 클릭합니다.

- b. "TIM Napatech Configuration"(TIM Napatech 구성) 페이지에서 "View the Napatech Hardware Filter Configuration File"(Napatech 하드웨어 필터 구성 파일 보기)을 클릭합니다. 또는 "View the Napatech Hardware Filter Configuration Log"(Napatech 하드웨어 필터 구성 로그 보기)를 클릭하여 자세한 정보를 봅니다.

중요! 새 파일을 업로드하면 Napatech 하드웨어 필터 구성 로그 또는 파일 페이지에서 이전 파일의 정보를 더 이상 볼 수 없습니다. 그러나 이전 필터 자체는 새 필터 파일의 시작 부분에 DeleteFilter=all 명령을 포함하는 경우에만 삭제됩니다.

고급 필터 만들기

이 단원의 예제를 기반으로 고급 필터를 만들 수 있습니다.

IP 주소 범위를 사용하여 필터링하려면

다음 예제에서는 10.11.28.23~10.11.28.32 범위의 IP 주소를 사용하여 필터링하는 방법을 보여 줍니다.

```
{[10.11.28.23]..[10.11.28.32]}.
```

참고: 이 범위는 1 바이트만 변경되는 경우에 가장 적합합니다. 1 바이트보다 더 변경되는 경우에는 리소스가 부족해질 수 있습니다.

서브넷 마스크를 사용하여 필터링하려면

- 다음 예제에서는 서브넷 마스크를 사용하여 필터링하는 방법을 보여 줍니다. 예를 들어 192.168.1.x 주소를 필터링하려면 다음 필터를 사용하십시오. 여기서 x 는 중요하지 않습니다.

```
mIPv4SrcAddr=={[FF.FF.FF.00]:[192.168.1.0]}
```

- 다음 예제에서는 마스크에서 1 인 비트만 비교합니다. 예를 들어 서브넷이 10.20.30.0~10.20.33.255 인 경우 다음 필터를 사용하십시오.

```
{[FF:FF:FA:00]:[10.20.30.0]}
```

마지막 바이트가 마스크되고 이전 바이트의 2 비트도 마스크됩니다.

여러 포트를 사용하여 필터링하려면

다음 예제에서는 포트 두 개를 사용하여 필터링하는 방법을 보여 줍니다.

```
mTcpSrcPort == 43,80
```

참고: 최대 8 개의 항목을 지정할 수 있고, 1 바이트만 변경되는 경우 필터 리소스가 하나만 사용됩니다.

프레임의 중복 제거

중복 프레임이 서로 간에 8 개 프레임 내에 있고 시간 만료 기준을 충족하는 경우 Napatech 어댑터가 중복 프레임을 제거합니다. 이때 시간 만료 기준의 최대값은 다음 ms 명령에 지정된 값일 수 있습니다.

```
Deduplication [Timeout = 100] = Channel == 0,1,2,3
```

중복 제거를 수행하면 포트 4 개 모두의 트래픽이 병합되고 중복 프레임 감지를 위해 100 밀리초 시간이 적용됩니다. 고급 중복 제거를 수행하면 프레임의 일부를 제외하고 프레임의 IP 부분만 검사할 수 있습니다. IP 헤더가 제외되고 16 바이트의 고정 오프셋이 추가로 적용됩니다.

```
Deduplication [DynOffset = Layer2And3HeaderSize; Offset = 16; Timeout = 10] = Channel == 0,1,2,3
```

기타 Napatech 어댑터 작업

다음은 추가로 수행해야 할 수 있는 Napatech 어댑터 작업입니다.

- Napatech 어댑터에서 필터 제거
- Napatech 어댑터 제거
- Napatech 어댑터별 로그 보기

Napatech 어댑터에서 필터 제거

문제를 해결할 때 또는 더 이상 트래픽을 필터링하지 않을 경우 Napatech 어댑터에서 필터를 제거할 수 있습니다.

Napatech 어댑터에서 필터를 제거하려면

1. "TIM 시스템 설정" 페이지에서 "Configure Napatech"(Napatech 구성)를 클릭합니다.
"TIM Napatech Configuration"(TIM Napatech 구성) 페이지가 나타납니다.
2. "Upload a Napatech Hardware Filter Configuration File"(Napatech 하드웨어 필터 구성 파일 업로드)을 클릭합니다.
"TIM Napatech Hardware Filter Configuration"(TIM Napatech 하드웨어 필터 구성) 페이지가 나타납니다.

3. "Delete all Napatech hardware filters"(모든 Napatech 하드웨어 필터 삭제)를 클릭합니다.
삭제할 경우 모든 트래픽을 TIM 에 보내도록 모두 캡처 필터가 Napatech 어댑터에 적용됩니다.
4. (선택 사항) 필터가 제거되었는지 확인합니다.
 - a. "TIM 시스템 설정" 페이지에서 "Configure Napatech"(Napatech 구성)를 클릭합니다.
 - b. "TIM Napatech Configuration"(TIM Napatech 구성) 페이지에서 "View the Napatech Hardware Filter Configuration File"(Napatech 하드웨어 필터 구성 파일 보기)을 클릭합니다.
페이지에 다음이 표시되는지 확인합니다.
Capture=All

Napatech 어댑터 제거

다른 TIM 컴퓨터에서 사용해 보기 위해 TIM 에서 Napatech 어댑터를 제거해야 할 수 있습니다.

Napatech 어댑터를 제거하려면

1. ntxc0:0 인터페이스 확인란을 선택 취소합니다. [어댑터를 사용하도록 TIM 네트워크 모니터 인터페이스를 구성하려면](#) (페이지 374)을 참조하십시오.
2. 다음과 같이 Napatech 어댑터가 사용되지 않도록 설정합니다.
 - a. "TIM 시스템 설정" 페이지에서 "Configure Napatech"(Napatech 구성)를 클릭합니다.
"TIM Napatech Configuration"(TIM Napatech 구성) 페이지가 나타납니다.
 - b. "Disable Napatech"(Napatech 사용 안 함)를 클릭하고 TIM 을 다시 시작합니다. 또는 TIM 이 실행되고 있지 않은 경우 "Disable Napatech"(Napatech 사용 안 함)를 클릭합니다.
3. TIM 컴퓨터에서 Napatech 어댑터 하드웨어를 제거합니다.

Napatech 어댑터별 로그 보기

Napatech 어댑터별 로그 파일은 다음과 같이 두 가지가 있습니다.

- TIM Napatech 하드웨어 필터 구성 로그는 필터를 적용하거나 제거할 때 업데이트됩니다.
- Napatech 드라이버 로그는 Napatech 드라이버를 로드할 때마다 업데이트됩니다. TIM 이 다시 시작될 때마다 드라이버가 로드됩니다.

TIM Napatech 하드웨어 필터 구성 로그를 보려면

1. "TIM 시스템 설정" 페이지에서 "Configure Napatech"(Napatech 구성)를 클릭합니다.
"TIM Napatech Configuration"(TIM Napatech 구성) 페이지가 나타납니다.
2. "View the Napatech Hardware Filter Configuration Log"(Napatech 하드웨어 필터 구성 로그 보기)를 클릭합니다.
TIM Napatech 하드웨어 필터 구성 로그가 나타납니다.

Napatech 드라이버 로그를 보려면

1. "TIM 시스템 설정" 페이지에서 "Configure Napatech"(Napatech 구성)를 클릭합니다.
"TIM Napatech Configuration"(TIM Napatech 구성) 페이지가 나타납니다.
2. "View the Napatech Driver Log"(Napatech 드라이버 로그 보기)를 클릭합니다.
Napatech 드라이버 로그가 나타납니다.

Napatech 어댑터 문제 해결

Napatech 어댑터 및 TIM 로그 정보

TIM 로그에서 모든 네트워크 인터페이스 관련 메시지는 AdapterManager 로 시작합니다. 예를 들어 Napatech 어댑터 관련 메시지는 ntxc0:0 인터페이스를 가리킵니다. 예:

```
AdapterManager: "ntxc0:0": thread starting
```

문제 해결 항목

이 페이지에는 다음 문제 해결 항목이 포함되어 있습니다.

- [Napatech 어댑터가 트래픽을 수신하고 있지 않음](#) (페이지 380)
- [이더넷 포트에 인식되지 않는 Napatech 어댑터](#) (페이지 381)
- [예상되는 트래픽이 표시되지 않음](#) (페이지 381)
- [일련 번호 및 기타 Napatech 어댑터 세부 정보](#) (페이지 381)

Napatech 어댑터가 트래픽을 수신하고 있지 않음

증상

TIM 이 패킷을 수신하고 있지 않습니다. "TIM Packet Statistics"(TIM 패킷 통계) 페이지를 검토해 보니 패킷이 캡처되고 있지 않습니다.

표시할 트래픽이 있는지 확인하십시오. ntxc0:0 포트에서 eth1 포트에 케이블을 이동하고 eth1 포트를 켜십시오. 이제 패킷이 표시되면 어댑터에 문제가 있는 것입니다.

해결 방법

인터페이스가 사용되도록 설정했는지 확인하십시오. [어댑터를 사용하도록 TIM 네트워크 모니터 인터페이스를 구성하려면](#) (페이지 374)을 참조하십시오.

소프트웨어가 구성되었는지 확인하십시오. [소프트웨어 설치](#) (페이지 372)를 참조하십시오.

로그를 검토하십시오. [Napatech 어댑터별 로그 보기](#) (페이지 377)를 참조하십시오.

로그에서 문제를 찾으십시오. [Napatech 어댑터별 로그 보기](#) (페이지 377)와 [Napatech 어댑터 및 TIM 로그 정보](#) (페이지 379)를 참조하십시오.

필터를 제거하십시오. [Napatech 어댑터에서 필터 제거](#) (페이지 377)를 참조하십시오.

Napatech 어댑터 자체에 문제가 있다고 판단되면 Network Allies 에 문의하고 그렇지 않으면 CA Support 에 문의하십시오.

이더넷 포트가 인식되지 않는 Napatech 어댑터

증상

TIM 의 Linux 프롬프트에서 `ifconfig` 명령을 입력하는 경우 `ntxc0:0` 포트가 나타나지 않습니다. 운영 체제가 Napatech 어댑터를 이더넷 포트가 인식하지 않습니다.

해결 방법

다른 조치가 필요하지 않습니다. Napatech 어댑터가 이 응용 프로그램에서 정상적으로 작동하고 있습니다.

예상되는 트래픽이 표시되지 않음

증상

일부 트래픽이 표시되고 있지만 예상되는 트래픽이 아닙니다.

증상

둘 이상의 인터페이스가 모니터링에 사용되도록 설정한 경우 다른 인터페이스를 꺼서 `ntxc0:0` 인터페이스에서 일부 트래픽을 수신하고 있는지 확인하십시오. `ntxc0:0` 인터페이스에서 트래픽을 수신하고 있지 않으면 [Napatech 어댑터가 트래픽을 수신하고 있지 않음 \(페이지 380\)](#)을 참조하십시오.

필터를 검토하고 필터를 제거하십시오. 예상되는 트래픽이 표시됩니까? 표시될 경우 필터를 검토하고 편집한 다음 다시 적용하십시오. 필터 파일의 시작 부분에 `DeleteFilter=all` 명령을 포함했는지 확인하십시오.

일련 번호 및 기타 Napatech 어댑터 세부 정보

증상

내 Napatech 어댑터의 일련 번호를 찾으려고 합니다.

Network Allies 에 지원을 요청할 경우 일련 번호가 필요할 수 있습니다.

해결 방법

Napatech 상태 페이지에서 Napatech 어댑터에 대한 정보를 볼 수 있습니다.

Napatech 상태 페이지를 열려면

1. "TIM 시스템 설정" 페이지에서 "Configure Napatech"(Napatech 구성)를 클릭합니다.

"TIM Napatech Configuration"(TIM Napatech 구성) 페이지가 나타납니다.

2. Napatech 상태를 봅니다.

Napatech AdapterInfo 프로그램이 실행되고 출력이 표시됩니다.

제 24 장: CA CEM 과 함께 작동하도록 CA Introscope 구성

CA CEM 은 서로 다른 두 사용자에게 필요한 요구 사항을 충족합니다. 즉, 웹 비즈니스를 담당하는 사용자는 추세, 서비스 수준 및 성공률 보고서를 얻을 수 있고, 인시던트에 대한 응답을 담당하는 사용자는 트랜잭션 결함 세부 정보를 실시간으로 파악할 수 있는 가시성을 얻을 수 있습니다.

Introscope 는 응용 프로그램 서버 수준에서 업계 최고의 문제 격리 솔루션을 제공합니다. 고객이 CA CEM 과 CA Introscope 를 통합하면 운영 중인 웹 응용 프로그램을 전면적으로 파악할 수 있는데, 이러한 솔루션이 바로 CA APM 입니다.

전체 고객 경험을 실시간으로 전면적으로 파악하면 서비스 제공 품질을 대폭 개선하고 고객 충성도를 높이며 고객의 전반적인 온라인 경험을 향상시킬 수 있는 새로운 통찰력을 얻을 수 있습니다. CA APM 보고서에서 사용할 수 있는 트랜잭션 심사 정보는 IT 와 비즈니스 이해당사자 모두의 요구 사항을 충족하는 공통 언어를 제공합니다.

CA CEM 은 IT 팀과 협력하여 고객에 대한 높은 온라인 서비스 제공 품질을 보장하는 비즈니스 관리자 파트너로서의 IT 역할을 향상합니다.

이 장에서는 CA CEM 과의 통합을 위해 Introscope 를 설치하고 구성하는 방법을 설명합니다. 제품을 함께 사용하는 방법에 대한 자세한 내용은 CA CEM 과 함께 Introscope 사용을 참조하십시오. Introscope Agent 기록 기능에 대한 자세한 내용은 CA APM 트랜잭션 정의 안내서를 참조하십시오.

이 섹션은 다음 항목을 포함하고 있습니다.

[CA APM 시작](#) (페이지 384)

[CA APM 고객 경험 메트릭 개요](#) (페이지 384)

[CA APM 문제 해결 심사 개요](#) (페이지 385)

[CA CEM 구성을 위한 점검 목록](#) (페이지 386)

[Introscope 구성을 위한 점검 목록](#) (페이지 399)

[CA Introscope 와 CA CEM 의 통합 문제 해결](#) (페이지 408)

[업그레이드 고려 사항](#) (페이지 411)

[비즈니스 응용 프로그램 설정](#) (페이지 412)

CA APM 시작

CA APM 을 사용하려면 CA Introscope 와 CA CEM 을 통합해야 합니다.

다음 목록에는 CA APM 을 시작하는 방법이 나와 있습니다.

1. CA Introscope 와 통합된 CA CEM 에서 기업에 필요한 고객 경험 정보를 제공하는 방법에 대해 알아봅니다. [CA APM 고객 경험 메트릭 개요](#) (페이지 384)를 참조하십시오.
2. CA Introscope 와 통합된 CA CEM 에서 IT 심사 및 문제 해결을 지원하는 방법에 대해 알아봅니다. [CA APM 문제 해결 심사 개요](#) (페이지 385)를 참조하십시오.
3. 통합에서 CA CEM 쪽 부분을 구성합니다. [CA CEM 구성을 위한 점검 목록](#) (페이지 386)을 참조하십시오.
4. 통합에서 CA Introscope 쪽 부분을 구성합니다. [CA Introscope 구성을 위한 점검 목록](#) (페이지 399)을 참조하십시오.
5. 통합 기능이 올바르게 작동하는지 확인합니다. [CA Introscope 와 CA CEM 의 통합 문제 해결](#) (페이지 408)을 참조하십시오.
6. CA CEM/CA Introscope 환경을 CA APM 으로 업그레이드할 경우 업그레이드 고려 사항을 검토합니다. [업그레이드 고려 사항](#) (페이지 411)을 참조하십시오.

CA APM 고객 경험 메트릭 개요

CA CEM 및 CA Introscope 고객 경험 메트릭 통합은 Enterprise Manager 와 각 TIM 의 구성 매개 변수로 제어됩니다.

1. 삭제되거나 만료 처리 기간에 도달하거나 만료 처리 기간을 초과할 때까지 7 초마다 또는 정의된 대로 TIM 이 모든 고객 경험 메트릭을 XML 파일에 기록합니다.
2. Enterprise Manager TIM 수집 서비스가 고객 경험 메트릭 파일을 검색하고 TIM 에 해당 파일을 삭제하도록 지시합니다.
3. Enterprise Manager TIM 수집 서비스가 고객 경험 메트릭 데이터를 구문 분석합니다. 그러나 데이터를 APM 데이터베이스에 저장하거나 데이터에 대한 집계를 수행하지는 않습니다.
4. 고객 경험 메트릭이 해당 출처 TIM 별로 그룹화되고 Enterprise Manager 가 고객 경험 메트릭을 SmartStor 데이터베이스에 저장합니다.

5. CA Introscope Workstation 이 기본 비즈니스 대시보드를 표시하고 typeview 와 계산기를 사용하여 집계 및 결함 백분율을 제공합니다.
6. 필요에 따라 동일한 고객 경험 매트릭 데이터를 사용하여 사용자 지정 비즈니스 대시보드를 직접 생성할 수 있습니다. CA CEM 에서 CA Introscope 사용을 참조하십시오.

TIM 수집 서비스에 대한 자세한 내용은 [Enterprise Manager 서비스 배포](#) (페이지 282)를 참조하십시오.

CA APM 문제 해결 심사 개요

CA CEM 및 CA Introscope 문제 해결 심사 통합은 CA Introscope 구성 설정으로 제어됩니다. 구성 정보는 트랜잭션 정의, 결함 지정 및 트랜잭션 추적 매개 변수를 포함하는 도메인 구성 정보에 포함됩니다.

1. "설정" > "모니터" > "모든 모니터 동기화"를 클릭하면 CA CEM 이 도메인 구성 정보의 변경 사항을 CA Introscope 에 알립니다. "모든 모니터 동기화"를 클릭하면 도메인 구성 정보가 TIM 에도 전송됩니다.
2. CA Introscope 에이전트는 도메인 구성 정보의 업데이트 사항을 수신 대기합니다. **9.0 이전 에이전트에 해당:** CEMDefinitionHandler 가 구분 분석된 도메인 구성 정보를 모든 등록된 에이전트에 보냅니다.
3. 그런 다음 각각의 등록된 에이전트가 나중에 트랜잭션 추적이 사용되도록 설정하는 규칙 집합을 만듭니다. 규칙 집합은 CA CEM 트랜잭션을 식별하는 매개 변수 이름/값에 대한 정규식 패턴으로 구성됩니다.
4. ServletHeaderDecorator 가 설치된 Java Agent 는 추가 정보를 각각의 HTTP 응답 헤더에 추가합니다. 헤더 정보에는 나중에 CA Introscope 트랜잭션 추적을 CA CEM 결함과 상호 관련시키는 데 사용되는 GUID 가 포함됩니다. .NET 에이전트는 HTTPHeaderDecorator 가 설치되어 있어야 동일한 기능을 제공할 수 있습니다.
5. CA CEM TIM 은 HTTP 응답 헤더를 구문 분석하고 보고된 결함에 있는 정보를 포함하며, 이는 Enterprise Manager 로 보내집니다.
6. CA CEM 은 결함 및 GUID 정보를 APM 데이터베이스에 저장합니다.
7. CA CEM 은 느린 시간 인시던트를 생성하고 트랜잭션 추적 세션 시작 요청을 Enterprise Manager 에 보냅니다. CA CEM 은 "설정" > "인시던트 설정"을 기반으로 느린 시간 인시던트를 생성하며 인시던트 상태를 보류 중에서 개설됨으로 변경합니다.

트랜잭션 추적 세션 시작 요청에는 비즈니스 트랜잭션 이름이 포함되고, 느린 시간 결합 지정의 백분율에 해당하는 트랜잭션 추적 시간 임계값도 포함됩니다. 트랜잭션 추적은 인시던트가 종결되거나 구성된 트랜잭션 추적 세션 기간에 도달할 때까지 계속 실행됩니다.

8. BizTrxHttpTracer 가 설치된 에이전트는 에이전트의 규칙 집합에 정의된 비즈니스 트랜잭션 이름으로 트랜잭션 정의를 조회합니다. 에이전트는 매개 변수 일치율을 통해 CA CEM 트랜잭션을 식별합니다.
9. 에이전트가 트랜잭션을 식별하고 트랜잭션 시간이 트랜잭션 추적 시간 임계값보다 큰 경우 에이전트가 트랜잭션 추적을 Enterprise Manager 에 보냅니다.
10. CA CEM 은 트랜잭션 추적을 수신하고 일치율을 통해 APM 데이터베이스에 저장된 GUID 와 비교합니다. 일치하는 GUID 가 발견되는 경우 CA CEM 은 트랜잭션 추적 정보를 APM 데이터베이스에 저장합니다.

Enterprise Manager 트랜잭션 추적 정보 및 기타 CA CEM 결합 정보는 분석을 위해 인시던트를 적절한 팀에 발송하는 데 사용됩니다. CA CEM 에서 CA Introscope 사용을 참조하십시오.

CA CEM 구성을 위한 점검 목록

다음 목록에는 CA Introscope 와 통합을 위해 CA CEM 을 구성하는 방법에 대해 알아두어야 하는 사항이 나와 있습니다.

CA Introscope 와 통합되도록 CA CEM 을 구성하려면

1. 사용할 통합 기능을 결정합니다. [필요한 통합 기능 결정](#) (페이지 400)을 참조하십시오.
2. CA Introscope Workstation 을 구성합니다. [CA Introscope Workstation 구성](#) (페이지 388)을 참조하십시오.
3. CA Introscope 트랜잭션 추적을 구성합니다. [트랜잭션 추적 구성](#) (페이지 389)을 참조하십시오.
4. 실시간 트랜잭션 메트릭을 구성합니다. [실시간 트랜잭션 메트릭 통합 구성](#) (페이지 391)을 참조하십시오.
5. 통합 기능이 올바르게 작동하는지 확인합니다. [CA CEM 구성 확인](#) (페이지 399)을 참조하십시오.

필요한 통합 기능 결정

CA APM 의 경우 다음 두 가지 통합 유형이 있습니다.

- 문제 해결 심사 - 상호 관련된 트랜잭션 정보를 사용하여 문제의 근본 원인을 분석할 수 있습니다.
- 고객 경험 메트릭 - 비즈니스 트랜잭션의 볼륨, 오류 및 평균 응답 시간에 대한 업데이트를 정기적으로 제공합니다.

문제 해결 심사를 원할 경우 "Introscope 설정"을 구성해야 합니다. 그러면 Workstation 과 트랜잭션 추적을 구성할 수 있습니다.

고객 경험 메트릭을 원할 경우에는 TIM 수집 서비스를 구성해야 합니다. 그러면 수집기를 구성하고 각 TIM 마다 메트릭 수집을 사용하도록 설정할 수 있습니다.

두 통합 기능을 모두 사용할 수도 있고 해당 비즈니스 환경의 요구 사항에 따라 하나만 선택해서 사용할 수도 있습니다.

참고: CA Introscope 에이전트 기록 기능을 사용하려면 *CA APM 트랜잭션 정의 안내서*를 참조하십시오.

추가 정보:

[Introscope 설정 구성](#) (페이지 387)

[고객 경험 메트릭 통합 구성](#) (페이지 391)

[CA CEM 구성 확인](#) (페이지 399)

Introscope 설정 구성

CA APM 통합이 사용되도록 설정하려면 CA Introscope 를 설정하기 위한 기본 정보를 수집해야 합니다.

이 단원에는 다음과 같은 항목이 포함되어 있습니다.

[CA Introscope Workstation 구성](#) (페이지 388)

[트랜잭션 추적 구성](#) (페이지 389)

[트랜잭션 추적 세션 정보 보기](#) (페이지 391)

CA Introscope Workstation 구성

Workstation Web Start 및 WebView 응용 프로그램의 연결 매개 변수를 설정해야 합니다.

CA Introscope Workstation 과 통신하도록 CA CEM 을 구성하려면

1. "설정" > "Introscope 설정"을 선택합니다.
"Introscope 설정" 페이지가 나타납니다.
2. Workstation Web Start 링크 사용 - CA CEM 의 인시던트 페이지와 결합 페이지에 Workstation Web Start 링크를 표시하려면 이 확인란을 선택합니다. 이 확인란을 선택하지 않으면 인시던트 페이지와 결합 페이지에 링크가 나타나지 않습니다.
3. 다음과 같이 Introscope WebView 정보를 입력합니다.
 - a. WebView 링크 사용 - CA CEM 의 인시던트 페이지와 결합 페이지에 WebView 링크를 표시하려면 이 확인란을 선택합니다. 이 확인란을 선택하지 않으면 인시던트 페이지와 결합 페이지에 링크가 나타나지 않습니다.
 - b. 호스트 이름 - WebView for CA CEM 을 호스팅하는 CA Introscope 시스템의 호스트 이름 또는 IP 주소를 입력합니다.
 - c. 포트 - Enterprise Manager 가 WebView 에 대한 연결을 수신 대기하는 포트를 입력합니다. WebView 의 기본 포트 번호는 8080 입니다.
 - d. 컨텍스트 경로 - CA Introscope 의 응용 프로그램 컨텍스트 경로를 지정하는 `introscope.webview.context.path` 속성 값을 입력합니다.
참고: `introscope.webview.context.path` 의 기본값은 "/"입니다. 이때 따옴표는 텍스트 상자에 입력하지 않습니다. 이 속성은 Enterprise Manager 를 호스팅하는 컴퓨터의 `<EM_Home>\config\` 디렉터리에 있는 `IntroscopeWebView.properties` 파일에서 정의합니다.
4. "설정 저장"을 클릭합니다.
Introscope Workstation 구성 정보가 저장됩니다.
5. 계속해서 [트랜잭션 추적 구성](#) (페이지 389)을 진행합니다.

트랜잭션 추적 구성

이러한 규칙을 기반으로 인시던트가 생성될 때 트랜잭션 추적이 자동으로 시작됩니다. "CEM" > "인시던트 개요" 페이지에서 트랜잭션 추적을 수동으로 시작할 수도 있습니다.

참고: CA CEM 결함의 트랜잭션 추적 정보는 "응용 프로그램 서버 시간" 임계값을 15 밀리초 이상으로 설정한 경우에만 CA CEM 의 "결함 정보" 페이지에 표시됩니다.

트랜잭션 추적 설정을 구성하거나 기본값을 그대로 둘 수 있습니다.

중요! 트랜잭션 추적으로 인해 계측된 응용 프로그램의 성능이 저하될 수 있습니다. 관련된 느린 시간 트랜잭션 결함 사양이 너무 낮으면 계측된 응용 프로그램이 종료될 수도 있습니다. 이러한 설정은 비즈니스 트랜잭션당 적용되는 설정이 아닌 전역 설정입니다.

CA Introscope 트랜잭션 추적을 구성하려면

1. 트랜잭션 추적 세션 최대 기간(분)을 입력합니다.

기본적으로 30 분 뒤에 트랜잭션 추적이 중지됩니다.

비즈니스 트랜잭션에 대해 개설된 인시던트가 있는 경우에만 CA CEM 은 CA Introscope 에서 트랜잭션 추적 세션을 시작합니다. CA CEM 에서 비즈니스 트랜잭션 못 시간 임계값별로 추적하는 경우 특수 트랜잭션 추적 방법에 액세스할 수 있습니다. 예를 들어 1000 밀리초, 즉 1 초보다 오래 걸리는 프로필 업데이트 웹 요청을 모두 추적합니다.

그러면 프로필 업데이트 요청이 아닌 요청을 식별한 후 추가 작업을 수행할 필요가 없기 때문에 에이전트가 성능을 최적화할 수 있습니다. 여러 트랜잭션 추적 세션이 실행 중일 수 있지만 오버헤드는 최소 한도로 유지됩니다.

2. 느린 시간 트랜잭션 결합 사양에 대한 백분율(%) 형식으로 트랜잭션 추적 시간 임계값을 입력합니다.

기본값은 50%입니다.

트랜잭션 추적 시간 임계값은 트랜잭션의 실행 시간 한도입니다. 트랜잭션 추적이 실행 중인 경우 임계값 내에 완료되지 않는 트랜잭션이 모두 추적됩니다.

트랜잭션 추적 시간 임계값은 느린 시간 트랜잭션 결합 사양에 대한 백분율입니다. 예를 들어 느린 시간 트랜잭션 결합 사양은 5.00 초로 설정하고 트랜잭션 추적 시간 임계값은 50 %로 설정한 경우 CA Introscope 에서, 즉 응용 프로그램 서버에서 완료될 때까지 걸리는 시간이 2.50 초보다 긴 트랜잭션이 모두 추적됩니다.

30 분과 50 %의 기본값으로 설정된 위의 예제를 사용하는 경우 다음 사항을 모두 충족하면 트랜잭션이 추적됩니다.

- 비즈니스 트랜잭션에 대해 개설된 인시던트가 있습니다.
- 트랜잭션이 완료될 때까지 걸리는 시간이 2.50 초보다 깁니다.
- 트랜잭션 추적이 실행 중인 시간이 30 분 미만입니다.

중요! 경우에 따라서는 CA CEM 느린 시간 트랜잭션 결합 사양을 1 밀리초, 즉 1/1000 초와 같은 매우 짧은 시간으로 설정해야 할 수 있습니다. 예를 들어 오류가 있는 경우에만 발생하는 트랜잭션에 대해 이 방식으로 설정할 수 있습니다. 그러나 이 동일한 트랜잭션이 CA Introscope 트랜잭션 추적과 관련된 경우에는 1 밀리초로 설정하면 Enterprise Manager MOM, Enterprise Manager 수집기 및 에이전트에 성능 문제를 가져올 수 있습니다.

3. 백엔드 구성 요소를 입력합니다. CA Introscope 에서는 지정된 패턴과 일치하는 구성 요소가 백엔드 구성 요소로 간주됩니다.

별표("*")는 와일드카드이며 항상 패턴 끝에 사용됩니다.

예: *Backends(백엔드)|*JDBC|**

각 패턴은 쉼표로 구분됩니다. 따라서 위의 예제에는 다음 두 가지 패턴이 있습니다.

*Backends(백엔드)|** 및 *JDBC|**

트랜잭션 추적에서 *Backends(백엔드)|** 또는 *JDBC|**로 시작하는 구성 요소가 모두 백엔드 구성 요소로 인식됩니다.

4. "설정 저장"을 클릭합니다.

트랜잭션 추적 구성 정보가 저장됩니다.

참고: 트랜잭션 추적 세션 모니터링에 대한 자세한 내용은 트랜잭션 추적 세션 정보 보기를 참조하십시오.

트랜잭션 추적 세션 정보 보기

현재 실행 중인 트랜잭션 추적 세션 목록을 볼 수 있습니다. 특정 인시던트를 선택하여 추가 정보를 얻을 수도 있습니다.

진행 중인 트랜잭션 추적을 모두 보려면

1. "CEM" > "인시던트 관리"를 선택합니다.
인시던트 페이지가 나타납니다.
2. "트랜잭션 추적 세션" 링크를 선택합니다.
현재 실행 중인 트랜잭션 추적 목록이 나타납니다.
3. 특정 인시던트 번호를 클릭하여 해당 인시던트와 관련하여 "CEM" > "인시던트 개요" 페이지로 직접 이동합니다.

고객 경험 메트릭 통합 구성

이 단원에서는 고객 경험 메트릭으로 업그레이드, 서비스 시작/중지 방법 및 선택적 문제 해결에 대한 정보를 제공합니다.

이 단원에는 다음과 같은 항목이 포함되어 있습니다.

[고객 경험 메트릭으로 업그레이드](#) (페이지 392)

[고객 경험 메트릭 수집 서비스 시작](#) (페이지 392)

[RTTM 수집 서비스 중지](#) (페이지 393)

[TIM 의 고객 경험 메트릭 문제 해결](#) (페이지 393)

[고객 경험 메트릭에 대한 TIM 설정](#) (페이지 395)

고객 경험 메트릭으로 업그레이드

참고: CA CEM의 이전 릴리스에서 고객 경험 메트릭을 사용한 경우에는 "비즈니스 프로세스"에서 "비즈니스 서비스"로 용어가 변경되었기 때문에 이에 따른 영향을 받을 수 있습니다.

업그레이드 후 아무 작업도 수행하지 않으면 대시보드 메트릭에 새로운 용어인 "비즈니스 서비스"가 나타납니다.

CA CEM 4.5 에 해당: 메트릭에서 "비즈니스 프로세스"라는 메트릭 이름을 유지하려면 `tess-customer.properties` 를 설정하고 CA CEM 4.5 Javascript 계산기를 계속 사용해야 합니다.

고객 경험 메트릭에서 비즈니스 프로세스라는 메트릭 이름을 유지하려면

1. `BTStatsMetricName.backwardCompatible` 속성을 변경하여 `tess-customer.properties` 를 설정합니다.

tess-customer 속성 파일을 편집하는 방법에 대한 자세한 내용은 [tess-customer.properties 파일 수정](#) (페이지 581)을 참조하십시오.
2. Enterprise Manager의 Javascript 계산기를 CA CEM 4.5의 계산기로 대체합니다. `CEM-AggregatedTree.js` 와 `CEM-DefectPercent.js` 를 대체합니다.
 - a. `CEM_BT_Stats_package.zip` 파일을 가져옵니다.
 - b. `CEM-AggregatedTree.js` 를 `<EM_Home>\scripts` 디렉터리에 추출합니다.
 - c. `CEM-DefectPercent.js` 를 `<EM_Home>\scripts` 디렉터리에 추출합니다.
 - d. Enterprise Manager 를 다시 시작하여 Javascript 계산기를 다시 로드합니다.

고객 경험 메트릭 수집 서비스 시작

TIM 수집 서비스를 사용하면 고객 경험 메트릭을 수집할 수 있습니다. 일반적으로 처음 Enterprise Manager 를 설치하고 설정하는 작업에서 TIM 수집 서비스를 포함하여 Enterprise Manager 서비스를 배포합니다.

Enterprise Manager 서비스에 대한 자세한 내용은 [Enterprise Manager 서비스 배포](#) (페이지 282)를 참조하십시오.

TIM 수집 서비스를 구성하고 RTTM 수집 서비스를 시작해야 고객 경험 메트릭 데이터가 표시됩니다.

고객 경험 메트릭 수집 서비스를 시작하려면

1. "설정" > "서비스" > "서비스 구성"을 선택합니다.
2. "TIM 수집 서비스"를 선택합니다.
3. "TIM 수집 서비스" 목록에서 "RTTM 수집 서비스"를 아직 선택하지 않았으면 선택합니다.
4. "시작"을 클릭하여 고객 경험 메트릭 수집 서비스를 시작합니다.
5. 서비스 상태가 "중지됨"에서 "실행 중"으로 변경되는지 확인합니다.

RTTM 수집 서비스 중지

경우에 따라 고객 경험 메트릭 기능을 중지해야 합니다.

RTTM 수집 서비스를 중지하려면

1. "설정" > "서비스" > "서비스 구성"을 선택합니다.
2. "TIM 수집 서비스"를 선택합니다.
3. "TIM 수집 서비스" 목록에서 "RTTM 수집 서비스"를 아직 선택하지 않았으면 선택합니다.
4. "중지"를 클릭하여 고객 경험 메트릭 수집 서비스를 중지합니다.
5. 서비스 상태가 "실행 중"에서 "중지됨"으로 변경되는지 확인합니다.

TIM의 고객 경험 메트릭 문제 해결

참고: 다음은 TIM에 대한 선택적 구성 절차입니다. 대부분의 경우 "설정" > "서비스" > "서비스 구성"을 통해 TIM 수집 서비스를 구성해야 합니다. TIM 수집 서비스에 대한 자세한 내용은 [Enterprise Manager 서비스 배포](#) (페이지 282)를 참조하십시오.

TIM의 고객 경험 메트릭 수집을 일시적으로 또는 영구적으로 사용하지 않도록 설정할 수 있습니다. 수집 빈도와 파일 만료 처리를 변경하고 다른 설정을 수정하여 사용자 환경의 문제를 해결할 수 있습니다.

TIM의 고객 경험 메트릭을 일시적으로 사용하지 않도록 설정하려면

1. "Wily System Setup"(Wily 시스템 설정) 페이지에서 "TIM" > "Configure TIM Settings"(TIM 설정 구성)를 선택합니다. "Wily System Setup"(Wily 시스템 설정) 페이지에 액세스하는 방법은 [TIM의 "Wily System Setup"\(Wily 시스템 설정\) 페이지 액세스](#) (페이지 263)를 참조하십시오. "TIM Settings"(TIM 설정) 페이지가 표시됩니다.

2. "Define a new value"(새 값 정의)를 클릭합니다.
3. 이름(*BtStats/Enabled*)을 입력합니다.
4. 새 값(*0*)을 입력합니다.
5. "Change"(변경)를 클릭합니다.

이렇게 하면 이 TIM 의 고객 경험 메트릭 수집이 일시적으로 사용하지 않도록 설정됩니다. 다음에 Enterprise Manager 를 다시 시작하면 수집이 계속됩니다.

참고: 위의 절차에서는 고객 경험 메트릭 수집이 이미 사용하도록 설정되었다고 가정합니다.

TIM 의 고객 경험 메트릭을 영구적으로 사용하지 않도록 설정하려면

1. "Wily System Setup"(Wily 시스템 설정) 페이지에서 "TIM" > "Configure TIM Settings"(TIM 설정 구성)를 선택합니다.

"TIM Settings"(TIM 설정) 페이지가 표시됩니다.

2. "Define a new value"(새 값 정의)를 클릭합니다.
3. 이름(*BtStats/ForceDisabled*)을 입력합니다.
4. 새 값(*1*)을 입력합니다.

이렇게 하면 CA CEM 에서 이 TIM 의 고객 경험 메트릭을 제어할 수 없게 됩니다.

5. "Change"(변경)를 클릭합니다.

이렇게 하면 이 TIM 의 고객 경험 메트릭 수집이 사용하지 않도록 설정됩니다. 다음에 Enterprise Manager 를 다시 시작해도 이 TIM 에서는 고객 경험 메트릭 수집이 계속되지 *않습니다*.

참고: 값을 기본값인 *0* 으로 다시 변경하여 CA CEM 에서 이 TIM 의 고객 경험 메트릭 수집을 다시 제어하도록 설정할 수 있습니다.

사용자 환경에서 더 많은 TIM 설정을 선택적으로 변경할 수 있으며 고객 경험 메트릭에 대한 TIM 설정에서 해당 TIM 설정을 정의합니다. 이러한 TIM 설정이 "TIM Settings"(TIM 설정) 페이지에 나타나지 않으면 기본값으로 설정된 것입니다.

TIM 의 고객 경험 메트릭 처리를 수정하려면

1. "Wily System Setup"(Wily 시스템 설정) 페이지에서 "TIM" > "Configure TIM Settings"(TIM 설정 구성)를 선택합니다.

"TIM Settings"(TIM 설정) 페이지가 표시됩니다.

2. TIM 설정이 이미 있으면 다음과 같이 합니다.
 - a. 이름을 클릭합니다.
 - b. 새 값을 입력합니다.
 - c. "Change"(변경)를 클릭합니다.
3. TIM 설정이 없으면 다음과 같이 합니다.
 - a. "Define a new value"(새 값 정의)를 클릭합니다.
 - b. 새 이름을 입력합니다.
 - c. 새 값을 입력합니다.
 - d. "Add"(추가)를 클릭합니다.

고객 경험 메트릭에 대한 TIM 설정

이러한 TIM 설정은 고객 경험 메트릭 문제를 해결하는 데 도움이 될 수 있습니다.

이 단원에는 다음과 같은 항목이 포함되어 있습니다.

[BtStats/ForceDisabled](#) (페이지 395)

[BtStats/Enabled](#) (페이지 396)

[BtStats/IntervalInSeconds](#) (페이지 396)

[BtStats/LogLevel](#) (페이지 397)

[BtStats/WriteEmptyFiles](#) (페이지 397)

[BtStats/MaxFileAgeInSeconds](#) (페이지 398)

BtStats/ForceDisabled

이 설정을 사용하면 TIM 자체의 고객 경험 메트릭 기능을 제어할 수 있습니다. CA CEM 제어를 무시할 수도 있습니다.

설정

숫자 값:

- 0 - CA CEM 에서 이 TIM 의 기능을 제어할 수 있습니다.
- 1 - 이 TIM 의 기능이 강제로 해제됩니다.

기본값

0

예

BtStats/ForceDisabled = 0

참고

- TIM 의 고객 경험 메트릭 기능을 사용하지 않도록 설정할 수 있습니다.
- 1 = *BtStats/Enabled* TIM 설정(다음)이 무시됩니다.
- 0 = 고객 경험 메트릭 기능이 CA CEM 에서 제어되고 *BtStats/Enabled* TIM 설정(다음)을 사용합니다.

BtStats/Enabled

이 설정을 사용하면 TIM 자체의 고객 경험 메트릭 기능을 제어할 수 있습니다.

설정

숫자 값:

- 0 - 사용하지 않도록 설정됩니다(기본값).
- 1 - 사용하도록 설정됩니다.

기본값

0

예

`BtStats/Enabled = 0`

참고

- Enterprise Manager 를 시작하면 CA CEM 에서 이 TIM 설정을 제어합니다. 그러나 *BtStats/ForceDisabled* TIM 설정(이전)으로 이 설정을 무시할 수 있습니다.
- 이 TIM 설정을 수정하여 TIM 의 고객 경험 메트릭 수집을 일시적으로 사용하지 않도록 설정할 수도 있습니다. 그러나 다음에 Enterprise Manager 를 다시 시작하면 해당 수정 사항이 변경될 수 있습니다.
- [TIM 의 고객 경험 메트릭 문제 해결](#) (페이지 393)을 참조하십시오.

BtStats/IntervalInSeconds

이 설정을 사용하면 TIM 이 실시간 트랜잭션 통계 파일을 기록하는 빈도를 제어할 수 있습니다.

설정

숫자 값으로, 양의 정수여야 합니다.

기본값

7

예

```
BtStats/IntervalInSeconds = 7
```

참고

실시간 트랜잭션 통계 파일은 TIM 의 `/etc/wily/cem/tim/data/out/btstats` 디렉터리에 저장됩니다.

BtStats/LogLevel

이 설정을 사용하면 고객 경험 메트릭에 대한 TIM 로그 파일 항목을 제어할 수 있습니다.

설정

숫자 값:

- 0
- 1
- 2

기본값

0

예

```
BtStats/LogLevel = 0
```

참고

- 0 = 메시지가 기록되지 않습니다(기본값).
- 1 = BtStats 파일이 기록될 때 메시지가 TIM 로그에 기록됩니다.
- 2 = 메시지와 동일하게 기록됩니다(세부 정보 표시 모드).

BtStats/WriteEmptyFiles

이 설정을 사용하면 TIM 이 빈 실시간 트랜잭션 통계 파일을 기록하는지 여부를 제어할 수 있습니다.

설정

숫자 값:

- 0
- 1

기본값

0

예

BtStats/WriteEmptyFiles = 0

참고

- 0 = 빈 파일이 기록되지 않음(기본값)
- 1 = 빈 BTlist 가 포함된 빈 파일이 기록됨
- 이 정보는 문제 해결에 유용할 수 있습니다. 예를 들어 TIM 간격 중에 감지된 트랜잭션이 없더라도 여전히 빈 BTlist 가 포함된 빈 파일, 즉 감지된 트랜잭션이 없는 빈 파일이 기록됩니다. 이 정보를 사용하여 TIM 이 Enterprise Manager 를 실행 중인 상태로 BtStats 파일을 만들고 있는지 아니면 Enterprise Manager 를 실행 중이 아닌 상태로 BtStats 파일을 만들고 있는지 테스트할 수 있습니다.
- 실시간 트랜잭션 통계 파일은 TIM 의 `/etc/wily/cem/tim/data/out/btstats` 디렉터리에 저장됩니다.

BtStats/MaxFileAgeInSeconds

이 설정을 사용하면, CA CEM 이 선택하지 않은 경우 실시간 트랜잭션 통계 파일을 유지해야 하는 기간을 정의할 수 있습니다. TIM 은 이 값보다 오래된 파일을 삭제합니다.

설정

숫자 값으로, 양의 정수여야 합니다.

기본값

3600

예

BtStats/MaxFileAgeInSeconds = 3600

참고

- 3600 = 1 시간(기본값)
- BtStats 파일을 유지해야 하는 기간을 정의합니다. TIM 은 이 값보다 오래된 파일을 삭제합니다.

- 이 값을 너무 높게 설정하면 TIM 의 디스크 공간이 부족해질 수 있습니다.
- 이 값을 너무 낮게 설정하면 CA CEM 이 검색하기 전에 파일이 삭제될 수 있습니다.
- 실시간 트랜잭션 통계 파일은 TIM 의 `/etc/wily/cem/tim/data/out/btstats` 디렉터리에 저장됩니다.

CA CEM 구성 확인

CA Introscope for CA APM 을 아직 구성하지 않은 경우 [CA Introscope 구성을 위한 점검 목록](#) (페이지 399)으로 이동하십시오.

구성 확인 및 문제 해결에 대한 자세한 내용은 [CA Introscope 와 CA CEM 의 통합 문제 해결](#) (페이지 408)을 참조하십시오.

Introscope 구성을 위한 점검 목록

다음 목록에는 CA CEM 과의 통합을 위해 CA Introscope 를 구성하는 데 필요한 작업이 나와 있습니다.

CA Introscope 를 CA CEM 과 통합하려면

1. 사용할 통합 기능을 결정합니다. [필요한 통합 기능 결정](#) (페이지 400)을 참조하십시오.
2. 문제 해결 심사를 위해 Enterprise Manager 를 구성합니다. [Enterprise Manager 구성](#) (페이지 400)을 참조하십시오.
3. 문제 해결 심사를 위해 각각의 Java Agent 를 통합합니다. [Java Agent 와 통합](#) (페이지 402)을 참조하십시오.
4. 문제 해결 심사를 위해 각각의 .NET 에이전트를 통합합니다. [.NET 에이전트와 통합](#) (페이지 405)을 참조하십시오.
5. 통합 기능이 올바르게 작동하는지 확인합니다. [CA Introscope 구성 확인](#) (페이지 408)을 참조하십시오.

필요한 통합 기능 결정

CA APM 의 경우 다음 두 가지 통합 유형이 있습니다.

- 문제 해결 심사 - 상호 관련된 트랜잭션 정보를 사용하여 문제의 근본 원인을 분석할 수 있습니다.
- 고객 경험 메트릭 - 비즈니스 트랜잭션의 볼륨, 오류 및 평균 응답 시간에 대한 업데이트를 정기적으로 제공합니다.

문제 해결 심사를 원할 경우 느린 시간 인시던트에 대한 문제 해결 심사 정보를 보도록 Enterprise Manager 와 모든 영향을 받는 에이전트를 구성해야 합니다.

참고: CA CEM 문제 해결 심사 통합은 AutoProbe 로 계측된 Java 및 .NET 에이전트 응용 프로그램에 대해서만 지원됩니다.

고객 경험 메트릭을 원할 경우에는 수집된 메트릭을 보도록 Enterprise Manager 대시보드를 구성해야 합니다. 사용자 고유의 CA CEM 고객 경험 대시보드 생성을 참조하십시오.

두 통합 기능을 모두 사용할 수도 있고 해당 비즈니스 환경의 요구 사항에 따라 하나만 선택해서 사용할 수도 있습니다.

참고: CA Introscope 에이전트 기록 기능을 사용하려면 CA APM 트랜잭션 정의 안내서를 참조하십시오.

추가 정보:

[Introscope 설정 구성](#) (페이지 387)

[고객 경험 메트릭 통합 구성](#) (페이지 391)

[CA CEM 구성 확인](#) (페이지 399)

Enterprise Manager 구성

Enterprise Manager 를 구성해야 CA Introscope 와의 CA CEM 통합이 사용되도록 설정할 수 있습니다.

9.0 이전 에이전트에 해당: 4.5 Enterprise Manager 확장도 다시 배포해야 합니다.

- Enterprise Manager 확장을 다운로드하여 MOM 과 각각의 Enterprise Manager 수집기에 설치합니다.
- 각각의 Enterprise Manager(JVM)를 다시 시작하여 Enterprise Manager 확장을 다시 로드합니다.

CA CEM 을 가상 에이전트로 설정

CA CEM 을 Enterprise Manager 용 가상 에이전트로 구성해야 합니다. 다음 절차를 따르면 여러 에이전트에서 메트릭을 집계할 수 있습니다. CA Introscope 콘솔에만 연결하는 것이 아니라 "Introscope Workstation Web Start 로 이동" 링크를 통해 Investigator 트리에 직접 연결할 수도 있습니다.

CA CEM 을 가상 에이전트로 구성하려면

1. <EM_Home>\config\agentclusters.xml 파일을 찾습니다.

중요! 단일 Enterprise Manager 나 MOM Enterprise Manager 에 연결하도록 CA CEM 을 구성할 수 있습니다. 사용 중인 CA Introscope 환경에 여러 Enterprise Manager 가 있으면 MOM 의 agentclusters.xml 파일만 수정해야 합니다.

2. 다음과 같이 agentclusters.xml 파일에서 관련 에이전트 행의 주석 처리를 제거합니다.

```
<agent-cluster name="CEM Agent" domain="SuperDomain">
  <agent-specifier>.*\|.*\|.*</agent-specifier>
  <metric-specifier>Customer Experience\|.*</metric-specifier>
  <metric-specifier>Business Segment\|.*</metric-specifier>
</agent-cluster>
```

중요! 이름 또는 도메인 특성을 변경하지 마십시오. 변경하면 통합 기능이 올바르게 작동하지 않습니다.

3. agentclusters.xml 파일의 변경 사항을 저장합니다.

이 변경 사항을 적용하기 위해 Enterprise Manager 를 다시 시작하지 않아도 됩니다.

9.0 이전의 에이전트에 대한 Enterprise Manager 확장 배포

9.0 이전 에이전트에 해당: 5.0 이전의 에이전트를 Enterprise Manager 에 연결한 경우에만 이 CA CEM 4.5 확장을 배포해야 합니다.

9.0 이전의 에이전트에 연결하는 Enterprise Manager 마다 CA CEM 4.5 CEMDefinitionHandler Enterprise Manager 확장이 설치되어 있어야 CA CEM 을 CA Introscope 와 통합할 수 있습니다.

다음 단계를 따르십시오.

1. CA Support 에 문의하여 필요한 파일을 얻습니다.
2. CA CEM 소프트웨어 링크를 사용하여 CA CEM 4.5 CEMIntroscopeIntegrationKit 를 얻습니다.
3. *CEMDefinitionHandler.jar* 를 Enterprise Manager 의 <EM_Home>\ext 디렉터리에 다운로드합니다.
4. 계속해서 [Enterprise Manager 다시 로드](#) (페이지 402)를 진행합니다.

Enterprise Manager 다시 로드

Enterprise Manager 를 다시 시작해야 문제 해결 심사를 위한 Enterprise Manager 통합이 완료됩니다.

JVM 을 다시 시작하면 Enterprise Manager 확장이 사용되도록 설정됩니다.

Enterprise Manager 를 다시 로드하려면

1. Enterprise Manager 를 다시 시작하여 Enterprise Manager 확장을 다시 로드합니다.
2. [9.0 이전의 에이전트에 대한 Enterprise Manager 확장 배포](#) (페이지 401)로 돌아가서 9.0 이전 에이전트에 연결하는 Enterprise Manager 각각에 대해 단계를 반복합니다.

Java Agent 와 통합

CA CEM 과 Introscope 의 통합에 포함된 Java Agent 각각에 대해 다음 절차를 수행해야 합니다.

1. AutoProbe 추적을 구성하여 Introscope 가 CA CEM 트랜잭션과 관련된 응용 프로그램이 사용되도록 설정합니다.
2. AutoProbe 와 ServletHeaderDecorator 의 에이전트 속성을 확인합니다.
3. 에이전트(JVM)를 다시 시작하여 에이전트 구성 속성을 다시 로드합니다.

.NET 에이전트와 통합해야 하는 경우 [.NET 에이전트와 통합](#) (페이지 405)을 참조하십시오.

Java 환경에서 AutoProbe 추적 구성

Introscope Investigator 트리에 있는 세부 정보는 에이전트 폴더의 PBL 파일에서 활성화되는 BizTrxHttpTracer 와 ServletHeaderDecorator 를 기반으로 합니다. 이러한 PBD 가 사용하도록 설정되어 있으면 CA Introscope 에서 각 비즈니스 트랜잭션에 대한 메트릭을 표시할 수 있습니다.

통합된 후에는 비즈니스 트랜잭션이 CA CEM 에 나타나는 것과 동일한 트랜잭션 이름을 사용하여 트리에 나타납니다.

AutoProbe 에 대한 자세한 내용은 *CA APM Java Agent 구현 안내서*를 참조하십시오.

Java Agent 의 AutoProbe 추적을 구성하려면

1. <Agent_Home>\wily\core\config 디렉터리에서 *IntroscopeAgent.profile* 을 엽니다.
2. *introscope.autoprobe.directivesFile* 속성을 찾습니다. 예를 들면 다음과 같습니다.

```
introscope.autoprobe.directivesFile=
default-typical.pbl
```

3. 속성에 지정된 PBL 파일을 찾습니다.
위의 예제에서는 *default-typical.pbl* 입니다.
4. 텍스트 편집기에서 지정된 PBL 파일을 엽니다.
5. PBL 파일에서 ServletHeaderDecorator.pbd 행의 주석 처리를 제거합니다.

```
#####
# Servlet Header Decorator
#
# Enable this PBD for CEM integration. It appends additional
# information to the HTTP response that is then captured by CEM.
# =====
ServletHeaderDecorator.pbd
```

6. PBL 파일의 변경 내용을 저장합니다.
7. 계속해서 [Java 환경에서 기본 에이전트 속성 확인](#) (페이지 404)을 진행합니다.

CA Introscope 9.0에 해당: *biz-trx-http.pbd*가 기본적으로 사용하도록 설정되어 있습니다.

9.0 이전 에이전트에 해당: *CEMTracer.pbd*의 주석 처리도 제거해야 합니다.

Java 환경에서 기본 에이전트 속성 확인

에이전트 프로필 속성 파일을 사용하여 **AutoProbe**와 **ServletHeaderDecorator**의 기본 에이전트 속성을 수정할 수 있습니다.

모든 CA CEM 관련 속성은 CA CEM - CA Introscope 통합용으로 미리 구성되어 있습니다. 기본값이 해당 설치에 적절한지 확인해야 합니다.

중요! 최소한 보안 관련 속성은 검토해야 합니다. 예를 들어 *introscope.agent.decorator.security* 속성은 기본적으로 **clear**로 설정되어 있습니다. 이 설정은 초기 테스트에 적절하지만, 방화벽 바깥으로는 알리고 싶지 않은 트랜잭션 헤더의 정보를 누설할 수 있습니다. 보다 안전한 프로덕션 환경을 위해 이 속성을 **encrypted**로 설정할 수 있습니다.

CA CEM 관련 에이전트 속성에 대한 자세한 내용은 CA Introscope 에이전트 프로필 속성을 참조하십시오.

자세한 내용은 *CA APM Java Agent 구현 안내서*를 참조하십시오.

에이전트 프로필 속성을 확인하려면

1. `<Agent_Home>\wily\core\config` 디렉터리에서 *IntroscopeAgent.profile*을 엽니다.
2. 에이전트 프로필에서 발견되는 속성을 CA Introscope 에이전트 프로필 속성에 있는 속성 설명과 비교합니다. 예를 들어 다음 속성을 기본 설정에서 변경해야 할 수 있습니다.
 - *introscope.agent.decorator.enabled* - 기본 Java Agent 설정을 **false**에서 **true**로 변경합니다. 그러면 문제 해결 심사 기능이 사용됩니다.
 - *introscope.agent.decorator.security* - 기본 설정을 **clear**에서 **encrypted**로 변경합니다. 그러면 헤더에 있는 기밀 정보가 보호됩니다.
3. 기본값을 수정해야 하는 경우 속성을 *IntroscopeAgent.profile* 파일에 추가한 다음 구성해야 할 수 있습니다.
4. 변경 사항을 *IntroscopeAgent.profile* 파일에 저장합니다.

- 계속해서 [Java 환경에서 에이전트 속성 다시 로드](#) (페이지 405)를 진행합니다.

팁: 속성이 전혀 나열되지 않으면 혼동될 수 있으므로 필요한 값이 기본값인 경우에도 속성을 명시적으로 포함하는 것이 좋습니다.

Java 환경에서 에이전트 속성 다시 로드

관리되는 응용 프로그램에 대한 에이전트를 다시 시작해야 통합이 완료됩니다.

JVM 을 다시 시작하면 에이전트 속성이 다시 로드되고 AutoProbe 와 ServletHeaderDecorator 가 사용되도록 설정됩니다.

Java Agent 의 에이전트 프로파일 속성을 다시 로드하려면

- 에이전트를 다시 시작하여 에이전트 속성을 다시 로드합니다.
- [Java Agent 와 통합](#) (페이지 402)으로 돌아가서 각 에이전트에 대해 절차를 반복합니다.

.NET 에이전트와 통합

CA CEM 과 CA Introscope 의 통합에 포함된 .NET 에이전트 각각에 대해 다음 절차를 수행합니다.

- AutoProbe 추적을 구성하여 CA Introscope 가 CA CEM 트랜잭션과 관련된 응용 프로그램이 사용되도록 설정합니다.
- AutoProbe 와 HTTPHeaderDecorator 의 에이전트 속성을 확인합니다.
- 에이전트(CLR)를 다시 시작하여 에이전트 구성 속성을 다시 로드합니다.

Java Agent 와 통합하는 경우 [Java Agent 와 통합](#) (페이지 402)을 참조하십시오.

.NET 환경에서 AutoProbe 추적 구성

Introscope Investigator 트리에 있는 세부 정보는 에이전트 폴더의 PBL 파일에서 활성화되는 BizTrxHttpTracer 와 HTTPHeaderDecorator 를 기반으로 합니다. BizTrxHttpTracer 가 사용하도록 설정되어 있으면 CA Introscope 에서 각 비즈니스 트랜잭션에 대한 메트릭을 표시할 수 있습니다.

통합된 후에는 비즈니스 트랜잭션이 CA CEM 에 나타나는 것과 동일한 트랜잭션 이름을 사용하여 트리에 나타납니다.

AutoProbe 에 대한 자세한 내용은 *CA APM .NET 에이전트 구현 안내서*를 참조하십시오.

.NET 에이전트에서 AutoProbe 추적을 구성하려면

1. <Agent_Home> 디렉터리에서 *IntroscopeAgent.profile* 을 엽니다.
2. *introscope.autoprobe.directivesFile* 속성을 찾습니다. 예를 들면 다음과 같습니다.

```
introscope.autoprobe.directivesFile=  
default-typical.pbl
```

3. 속성에 지정된 PBL 파일을 찾습니다.
위의 예제에서는 *default-typical.pbl* 입니다.
4. 텍스트 편집기에서 지정된 PBL 파일을 엽니다.
5. PBL 파일에서 *httpheaderdecorator.pbd* 행의 주석 처리를 제거합니다.

```
#####  
# HTTP Header Decorator  
#  
# Enable this PBD for CEM integration.  
# It appends additional information to the  
# HTTP response that is then captured by CEM.  
# =====  
httpheaderdecorator.pbd
```

6. PBL 파일의 변경 내용을 저장합니다.
7. 계속해서 [.NET 환경에서 기본 에이전트 속성 확인](#) (페이지 407)을 진행합니다.

CA Introscope 9.0 에 해당: *biz-trx-http.pbd* 가 기본적으로 사용하도록 설정되어 있습니다.

9.0 이전 에이전트에 해당: *CEMTracer.pbd* 의 주석 처리도 제거해야 합니다.

.NET 환경에서 기본 에이전트 속성 확인

에이전트 프로필 속성 파일을 사용하여 `AutoProbe` 와 `HTTPHeaderDecorator` 의 기본 에이전트 속성을 수정할 수 있습니다.

모든 CA CEM 관련 속성은 CA CEM - CA Introscope 통합용으로 미리 구성되어 있습니다. 기본값이 해당 설치에 적절한지 확인해야 합니다.

중요! 최소한 보안 관련 속성은 검토해야 합니다. 예를 들어 `introscope.agent.decorator.security` 속성은 기본적으로 `clear` 로 설정되어 있습니다. 이 설정은 초기 테스트에 적절하지만, 방화벽 바깥으로는 알리고 싶지 않은 트랜잭션 헤더의 정보를 누설할 수 있습니다. 보다 안전한 프로덕션 환경을 위해 이 속성을 `encrypted` 로 설정할 수 있습니다.

CA CEM 관련 에이전트 속성에 대한 자세한 내용은 *CA APM .NET 에이전트 구현 안내서*를 참조하십시오.

에이전트 프로필 속성을 확인하려면

1. `<Agent_Home>` 디렉터리에서 `IntroscopeAgent.profile` 을 엽니다.
2. 에이전트 프로필에서 발견되는 속성을 CA Introscope 에이전트 프로필 속성에 있는 속성 설명과 비교합니다. 예를 들어 다음 속성을 기본 설정에서 변경해야 할 수 있습니다.
 - `introscope.agent.decorator.enabled` - .NET 에이전트의 기본 설정은 `true` 입니다. 이 설정을 사용하면 문제 해결 심사 기능이 사용되도록 설정됩니다.
 - `introscope.agent.decorator.security` - 기본 설정을 `clear` 에서 `encrypted` 로 변경합니다. 그러면 헤더에 있는 기밀 정보가 보호됩니다.
3. 기본값을 수정해야 하는 경우 속성을 `IntroscopeAgent.profile` 파일에 추가한 다음 구성해야 할 수 있습니다.
4. 변경 사항을 `IntroscopeAgent.profile` 파일에 저장합니다.
5. 계속해서 [.NET 환경에서 에이전트 속성 다시 로드 \(페이지 408\)](#)를 진행합니다.

팁: 속성이 전혀 나열되지 않으면 혼동될 수 있으므로 필요한 값이 기본값인 경우에도 속성을 명시적으로 포함하는 것이 좋습니다.

.NET 환경에서 에이전트 속성 다시 로드

관리되는 응용 프로그램에 대한 에이전트를 다시 시작해야 통합이 완료됩니다.

CLR 을 다시 시작하면 에이전트 속성이 다시 로드되고 AutoProbe 와 HTTPHeaderDecorator 가 사용되도록 설정됩니다.

.NET 에이전트의 에이전트 프로파일 속성을 다시 로드하려면

1. 에이전트를 다시 시작하여 에이전트 속성을 다시 로드합니다.
2. [.NET 에이전트와 통합](#) (페이지 405)으로 돌아가서 각 에이전트에 대해 절차를 반복합니다.

Introscope 구성 확인

CA CEM for CA APM 을 아직 구성하지 않은 경우 [CA CEM 구성을 위한 점검 목록](#) (페이지 386)으로 이동하십시오.

구성 확인 및 문제 해결에 대한 자세한 내용은 [Introscope 와 CA CEM 의 통합 문제 해결](#) (페이지 408)을 참조하십시오.

CA Introscope 와 CA CEM 의 통합 문제 해결

경우에 따라 CA Introscope 와 CA CEM 의 통합 문제를 해결해야 합니다. 이 단원에서는 높은 수준의 확인 단계와 문제 해결 단원을 제공합니다.

이 단원에는 다음과 같은 항목이 포함되어 있습니다.

[CA CEM 에서 CA Introscope 통합 확인](#) (페이지 408)
[증상 및 해결 방법](#) (페이지 409)

CA CEM 에서 CA Introscope 통합 확인

CA CEM 에서 여러 가지 방법으로 통합을 확인할 수 있습니다.

CA CEM 에서 CA Introscope 기능을 확인하려면

1. Enterprise Manager 가 올바르게 구성되었는지 확인합니다.
[CA Introscope 설정 구성](#) (페이지 387)을 참조하십시오.

2. Enterprise Manager 와의 통신을 확인합니다.
 - a. "시스템" > "이벤트"를 선택합니다.
 - b. Enterprise Manager 와 에이전트 간에 해결되지 않은 통신 오류가 없는지 확인합니다.
 - c. Enterprise Manager 와 TIM 간에 해결되지 않은 통신 오류가 없는지 확인합니다.
 - d. [CA CEM 이벤트 보기](#) (페이지 341)를 참조하십시오.
3. 트랜잭션 정의, 결합 사양 및 트랜잭션 추적 매개 변수를 포함한 최신 도메인 구성 정보를 에이전트에 전송하도록 모든 모니터를 동기화합니다. 이 경우 사용하도록 설정된 모든 TIM 모니터에도 해당 정보가 전송됩니다.
 - a. "설정" > "모니터"를 선택합니다.
 - b. "모든 모니터 동기화"를 클릭합니다.
 - c. Enterprise Manager 와 에이전트 간의 통신이 활성화 상태인지 확인합니다. 에이전트 로그 파일을 참조하십시오.
4. Enterprise Manager 로그를 검사하여 관련 오류 메시지가 있는지 확인합니다. CA CEM 관련 메시지를 검색합니다. 예를 들어 로그에서 "tess" 또는 "Biz"가 있는 메시지를 검색합니다.
5. 트랜잭션 추적 세션이 예상될 때 실행되는지 확인합니다. 트랜잭션 추적 세션 정보 보기를 참조하십시오.
6. 실시간 트랜잭션 메트릭 기능이 TIM 수집 서비스를 통해 사용하도록 설정되었는지 확인합니다. [고객 경험 메트릭에 대한 TIM 선택](#) (페이지 287)을 참조하십시오.
7. 실시간 트랜잭션 메트릭 기능이 각 TIM 에서 사용하도록 설정되었는지 확인합니다.
[TIM 의 고객 경험 메트릭 문제 해결](#) (페이지 393)을 참조하십시오.

증상 및 해결 방법

다음 항목에는 CA Introscope 와 CA CEM 의 통합 문제 해결에 유용한 팁이 몇 가지 나와 있습니다.

범주

[.NET](#) (페이지 410)

[이벤트 및 로그](#) (페이지 411)

.NET

증상

IP 주소의 호스트 이름과 일치하도록 정의된 경우 .NET 에 대한 트랜잭션이 인식되지 않습니다. 동일한 조건에서 Java Agent 를 통해 모니터링되는 트랜잭션은 예상한 대로 인식되어 Investigator 트리에 나타납니다.

가능한 해결 방법

IP 주소 대신 대문자 호스트 이름과 일치하도록 호스트 이름을 변경하십시오. ("비즈니스 서비스" > "비즈니스 트랜잭션" > "트랜잭션" > "구성 요소" > "ID")

증상

.NET wily.Agent 어셈블리 버전이 CA CEM 용 .NET 에이전트 확장의 버전 번호와 일치하지 않는 경우 .NET 에이전트가 다시 시작되지 않습니다.

가능한 해결 방법

에이전트 .NET 버전 구성에 정의된 대로 지침을 따르십시오.

참고: 단계를 정확히 수행해야 합니다. machine.config 파일을 제대로 업데이트하지 않으면 .NET 에이전트가 시작되지 않습니다.

*CA Introscope*에서는 다음과 같이 더욱 큰 문제가 발생합니다.

확장의 버전 번호가 .NET 에이전트의 버전 번호와 다른 경우 Standalone Agent 설치 관리자가 확장(DLL 등)을 주기적으로 설치하지 않습니다.

이 경우 다음과 같은 두 가지 해결 방법이 있습니다.

- 개별 응용 프로그램마다 다른 버전 번호를 받아들이도록 구성하십시오.

또는

- 다양한 버전 번호를 받아들이도록 모든 응용 프로그램을 전역적으로 구성하십시오.

참고: 하나의 옵션만 선택하고 두 옵션을 모두 수행하지는 마십시오.

자세한 내용은 *CA APM .NET 에이전트 구현 안내서*를 참조하십시오.

이벤트 및 로그

증상

모니터를 동기화할 때 다음과 같은 내용의 Enterprise Manager 로그 파일 메시지가 나타납니다.

도메인 구성 xml 파일을 Collector Enterprise Manager 에 전송하지 못했습니다. 필수 서비스가 Enterprise Manager 에서 정의되지 않았습니다.

참고: 이 문제는 CA CEM 4.x 에이전트가 있는 경우에 발생할 수 있습니다.

가능한 해결 방법

CEMDefinitionHandler Enterprise Manager 확장이 MOM 에 설치된 다음 각 수집기에 설치되었는지 확인하십시오.

또한 Enterprise Manager 마다 JVM 을 다시 시작해야 통합이 완료됩니다.

자세한 내용은 [Enterprise Manager 구성](#) (페이지 400)을 참조하십시오.

업그레이드 고려 사항

이제 TESS 는 Enterprise Manager 에 포함되어 있습니다.

- CEMTracer 에서 이전에 제공되었던 기능은 이제 BizTrxHttpTracer 에서 제공되며 기본적으로 사용하도록 설정됩니다. BizTrxHttpTracer 는 에이전트 기록 기능도 지원합니다.
- "모든 모니터 동기화"를 클릭하면 CA CEM 에서 이를 Enterprise Manager 에 알리고 도메인 구성 정보 파일(*domainconfig.xml*)이 공유 APM 데이터베이스에 저장됩니다.
- TESS 로그 파일은 더 이상 없습니다. 이전에 TESS 로그 파일에 기록되었던 메시지는 이제 <EM_Home>/logs 에 있는 Enterprise Manager 로그 파일에 기록됩니다.

CA APM 통합을 위해 CA CEM 또는 CA Introscope 를 업그레이드하기 전에 *CA APM 설치 및 업그레이드 안내서*의 특정 제품 업그레이드 요구 사항을 검토해야 합니다.

CA CEM 과 CA Introscope 가 통합되는 경우 실제로 개별 절차를 시작하기 전에 업그레이드 계획을 세우는 것이 좋습니다. 사용자 고유의 환경과 특정 요구 사항을 고려하면 불필요한 혼란을 방지할 수 있습니다.

비즈니스 응용 프로그램 설정

CA APM 트랜잭션 정의 안내서에 설명된 대로 비즈니스 응용 프로그램을 설정하는 경우에는 CA SiteMinder 설정을 사용해야 합니다.

비즈니스 응용 프로그램에 대해 올바른 설정을 확인하려면

1. "인증 유형"이 "CA SiteMinder"인지 확인합니다.
2. "사용자 ID" 매개 변수 유형이 "CA SiteMinder"이고 매개 변수 이름이 "UserName" 또는 "DistinguishedName"인지 확인합니다.

일부 CA SiteMinder 인증 유형(익명 인증 및 인증서 기반 인증)의 경우 SM_AGENTAPI_ATTR_USERNAME 이 비어 있습니다. 이 경우 SM_AGENTAPI_ATTR_USERDN(고유 이름)의 값을 사용하여 사용자를 식별해야 합니다.

3. "세션 ID" 매개 변수 유형이 "CA SiteMinder"이고 매개 변수 이름이 "SessionId"인지 확인합니다.

제 25 장: CA CEM 과의 CA SiteMinder 통합

CA CEM 은 CA SiteMinder 보안 소프트웨어와 함께 작동합니다. CA SiteMinder 는 Single Sign-On, 웹 응용 프로그램에 대한 사용자 액세스 중앙 제어 등의 보안 기능을 제공합니다.

단순 인증의 경우 CA SiteMinder 플러그 인 없이 이 장에 설명된 절차를 따르지 않고 쿠키를 사용하여 사용자와 세션을 식별할 수 있습니다.

사용자 이름과 세션 ID 가 항상 헤더에서 관측되는 경우와 세션 ID 가 변경되거나 만료되지 않는 경우 쿠키 매개 변수(예: SMUSER 및 SMSESSION 또는 HTTP_SM_USER 및 HTTP_SM_SESSION)를 사용하여 사용자와 세션을 식별하는 것을 고려하십시오.

SSO(Single Sign-On)나 만료 쿠키를 사용하는 경우에는 이 장에 설명된 대로 CA SiteMinder 플러그 인을 사용해야 합니다. 이 경우 요청 헤더에 사용자 이름과 정적 쿠키가 일관되게 포함되지 않으므로 단순 쿠키 접근 방법이 유효하지 않습니다. 따라서 TIM 은 CA SiteMinder 서버와 통신하여 사용자와 세션을 확인해야 합니다.

이 섹션은 다음 항목을 포함하고 있습니다.

[CA SiteMinder 에 대한 검사 목록](#) (페이지 414)

[CA CEM 에서 CA SiteMinder 구성](#) (페이지 414)

[사용자 지정 CA SiteMinder 에이전트 생성](#) (페이지 416)

[CA CEM 에서 정책 서버 정의](#) (페이지 417)

[CA CEM 에서 에이전트 정의](#) (페이지 418)

[TIM SiteMinder 호스트 구성 보기](#) (페이지 419)

[CA SiteMinder 사용](#) (페이지 419)

[CA SiteMinder 와 CA CEM 의 통합 문제 해결](#) (페이지 419)

CA SiteMinder 에 대한 검사 목록

다음 목록에는 CA CEM 과 CA SiteMinder 의 통합에 대해 알아두어야 하는 사항이 나와 있습니다.

CA SiteMinder 와 통합하려면

1. CA SiteMinder 에서 CA CEM 에 대한 사용자 지정 에이전트 유형을 만듭니다. [CA SiteMinder 에서 CA CEM 에 대한 사용자 지정 에이전트 유형 만들기](#) (페이지 416)를 참조하십시오.
2. CA SiteMinder 에서 각 TIM 에 대한 사용자 지정 에이전트를 만듭니다. CA SiteMinder 에서 각 TIM 에 대한 사용자 지정 에이전트 만들기를 참조하십시오.
3. 공유 암호를 정의합니다. [CA CEM 에서 CA SiteMinder 구성](#) (페이지 414)을 참조하십시오.
4. 정책 서버를 정의합니다. [CA CEM 에서 정책 서버 정의](#) (페이지 417)를 참조하십시오.
5. 에이전트 이름을 정의합니다. [CA CEM 에서 에이전트 정의](#) (페이지 418)를 참조하십시오.
6. CA SiteMinder 가 사용되도록 설정합니다. [CA SiteMinder 사용](#) (페이지 419)을 참조하십시오.
7. CA SiteMinder 인증을 지정하도록 비즈니스 응용 프로그램을 설정합니다. [비즈니스 응용 프로그램 설정](#) (페이지 412)을 참조하십시오.
8. CA CEM 이 CA SiteMinder 와 함께 올바르게 작동하고 있는지 확인합니다. [CA SiteMinder 와 CA CEM 의 통합 문제 해결](#) (페이지 419)을 참조하십시오.

CA CEM 에서 CA SiteMinder 구성

CA CEM 이 CA SiteMinder 와 함께 올바르게 작동하려면 CA SiteMinder 플러그인을 구성해야 합니다.

CA CEM 에서 CA SiteMinder 를 구성하려면

1. "설정" > "플러그인"을 선택합니다.
"플러그인" 페이지가 나타납니다.

2. "CA SiteMinder"를 선택합니다.

"CA SiteMinder Plug-in"(CA SiteMinder 플러그 인) > "일반" 페이지가 나타납니다.

3. "Enable CA SiteMinder Plug-in"(CA SiteMinder 플러그 인 사용) 아래에서 다음 옵션 중 하나를 선택하여 CA CEM 및 CA SiteMinder 통합을 활성화합니다.

- 4.x API
- 5.x API

참고: CA CEM-SiteMinder 통합에서는 정책 서버에 대한 두 가지 통신 방법을 사용했습니다.

- 4.x API 라고 하는 첫 번째 방법은 일반 공유 암호라는 프로세스를 사용했습니다.
- SiteMinder 는 호스트 기반 등록이라는 프로세스를 사용하여 보다 안전하게 에이전트를 정책 서버에 등록하고 에이전트와 정책 서버 간의 통신을 수행하는 방법도 지원합니다. 이 방법을 5.x API 라고 합니다.

CA CEM-SiteMinder 통합에서는 두 방법을 모두 지원합니다.

4. CA SiteMinder 사용자 세션 정보를 암호화된 형식으로 저장하는 세션 쿠키 이름을 입력합니다.

참고: 기본 세션 쿠키 이름은 SMSESSION 입니다.

5. 사용자 지정 에이전트 이름과 함께 사용자 지정 에이전트와 CA SiteMinder 정책 서버 간의 트래픽 암호화에 사용되는 공유 암호를 입력합니다.

참고: "공유 암호" 필드는 3 단계에서 4.X API 를 선택하는 경우에만 표시됩니다.

공유 암호란 CA SiteMinder 에서 CA CEM 사용자 지정 에이전트를 구성할 때 지정한 값과 일치해야 하는 텍스트 값입니다.

참고: CA SiteMinder 를 구성할 때 모든 CA CEM 에이전트에 대해 동일한 공유 암호를 사용해야 합니다.

6. "Force Registration"(강제 등록)을 클릭합니다.
호스트 구성 개체 이름을 변경하거나 TIM 에서 호스트 구성 파일을 재생성하려는 경우 강제 등록을 사용할 수 있습니다.
참고: "Force Registration"(강제 등록) 필드는 3 단계에서 5.X API 를 선택하는 경우에만 표시됩니다.
7. "저장"을 클릭합니다.

사용자 지정 CA SiteMinder 에이전트 생성

다음 단계에서는 CA CEM 과 CA SiteMinder 정책 서버를 통합하는 방법을 설명합니다. CA SiteMinder 정책 서버에서 해당 단계를 수행해야 합니다.

CA SiteMinder 에서 CA CEM 에 대한 사용자 지정 에이전트 유형 만들기

다음 단계를 한 번씩 수행해야 합니다. TIM 이 여러 대인 경우에도 사용자 지정 에이전트 유형을 여러 개 만들 필요가 없습니다.

참고: 다음 절차에서는 CA SiteMinder r6 의 단계를 설명합니다. 이후 릴리스가 있는 경우 정확한 단계는 다를 수 있지만 동일한 기능을 수행해야 합니다.

CA SiteMinder 에서 CA CEM 에 대한 사용자 지정 에이전트 유형을 만들려면

1. 브라우저를 열고 정책 서버의 CA SiteMinder URL 을 입력합니다. 예:
`http://<IP_Address>/siteminder/smadmin2.html`
2. "Administer Policy Server"(정책 서버 관리)를 클릭하고 Java 애플릿을 사용하여 새 에이전트 유형을 정의합니다.
3. 왼쪽의 "개체" 창에서 "시스템" 탭을 클릭합니다.
4. "보기" 메뉴에서 "Agent Types"(에이전트 유형)가 선택되어 있는지 확인합니다.
5. "개체" 창에서 "Agent Types"(에이전트 유형) 아이콘을 클릭합니다.
6. "Edit"(편집) 메뉴에서 "Create Agent Type"(에이전트 유형 만들기)을 선택합니다.
7. 사용자 지정 에이전트가 자신을 식별하는 데 사용하는 이름(예: *TIMAgent*)을 입력합니다.
8. 사용자 지정 에이전트 유형에 대한 설명을 입력합니다.

9. "Agent Type Definition"(에이전트 유형 정의) 탭에서 "RADIUS Device"(RADIUS 장치) 확인란은 선택 취소된 상태로 두고 "IETF Vendor ID"(IETF 공급업체 ID) 텍스트 상자는 비워 둡니다.
10. 정의된 작업이 없는 경우 새 작업을 정의하고 "유형"을 "인증됨"으로 설정합니다.

CA CEM에서 정책 서버 정의

정책 서버는 웹 응용 프로그램에 대한 권한 부여와 인증을 제공하는 CA SiteMinder 구성 요소입니다. CA SiteMinder 구성에 둘 이상의 정책 서버가 포함될 수 있습니다.

정책 서버를 정의하려면

1. "설정" > "플러그 인"을 선택합니다. "플러그 인" 페이지가 나타납니다.
2. "CA SiteMinder Web Access Manager"를 선택합니다.
3. "CA SiteMinder Plug-in"(CA SiteMinder 플러그 인) 페이지에서 "정책 서버"를 선택합니다.
4. "새로 만들기"를 클릭합니다.

"정책 서버" 페이지가 나타납니다.

5.x API에 해당 -- 5.x API 플러그 인을 선택하면 호스트 구성 개체가 있는 정책 서버 하나만 추가할 수 있습니다.

호스트 구성 개체에 여러 정책 서버를 추가할 수 있습니다.

자세한 내용은 *CA SiteMinder Policy Server Configuration Guide*(CA SiteMinder 정책 서버 구성 안내서)에서 "Host Configuration Objects for Trusted Hosts"(신뢰할 수 있는 호스트에 대한 호스트 구성 개체)를 참조하십시오.

5. 정책 서버가 설치된 컴퓨터의 IP 주소와 인증 포트를 입력합니다.
6. **5.x API에 해당** -- 5.x API 플러그 인을 선택한 경우 다음 필드에 정보를 입력하십시오.
 - SiteMinder 관리 사용자 이름
 - SiteMinder 관리 암호

참고: 등록을 수행하려면 여기에 입력하는 사용자 이름과 암호에 올바른 권한이 있어야 합니다.

7. "저장"을 클릭합니다.

CA CEM 에서 에이전트 정의

CA SiteMinder 에이전트는 보안 리소스에 대한 요청 권한을 부여하고 해당 요청을 CA SiteMinder 정책 서버에 전달하는 소프트웨어 모듈입니다.

"Plug-ins Agents"(플러그인 에이전트) 페이지에 에이전트와 관련 모니터(TIM)가 나열됩니다. 처음에 에이전트와 모니터는 동일한 이름을 가집니다. CA SiteMinder 가 사용하는 해당 에이전트 이름과 정확히 일치하도록 에이전트 이름을 변경해야 합니다.

에이전트를 정의하려면

1. "설정" > "플러그인"을 선택합니다.

"플러그인" 페이지가 나타납니다.

2. "CA SiteMinder"를 선택합니다.

3. "CA SiteMinder Plug-in"(CA SiteMinder 플러그인) 페이지에서 "에이전트"를 선택합니다.

"에이전트" 페이지가 표시됩니다.

5.0 API 에 해당 -- 5.0 API 를 사용하여 CA SiteMinder 를 사용하도록 설정한 경우 "에이전트" 페이지에 "SiteMinder 호스트 구성" 필드도 표시됩니다.

4. "에이전트" 페이지에서 에이전트의 IP 주소를 클릭합니다.

"모니터" 페이지가 나타납니다.

5.0 API 에 해당 -- 5.0 API 를 사용하여 CA SiteMinder 를 사용하도록 설정한 경우 "모니터" 페이지에 "SiteMinder 에이전트 이름" 및 "SiteMinder 호스트 구성" 필드도 표시됩니다.

5. CA SiteMinder 가 사용하는 이름과 정확히 일치하도록 CA SiteMinder 에이전트 이름을 업데이트합니다.

6. "저장"을 클릭합니다.

TIM SiteMinder 호스트 구성 보기

다음 단계를 따르십시오.

1. "TIM System Setup"(TIM 시스템 설정) 페이지에 액세스합니다.
2. "View TIM SiteMinder Host Configuration"(TIM SiteMinder 호스트 구성 보기)을 클릭합니다.

호스트 구성 파일이 표시됩니다.

참고: "TIM 시스템 설정" 페이지에 액세스하는 방법에 대한 자세한 내용은 "CEM 콘솔 및 설정 페이지 액세스"를 참조하십시오.

CA SiteMinder 사용

CA CEM 이 CA SiteMinder 와 함께 올바르게 작동하려면 CA SiteMinder 플러그인이 사용되도록 설정해야 합니다.

CA CEM 에서 CA SiteMinder 가 사용되도록 설정하려면

1. "설정" > "플러그인"을 선택합니다.
"플러그인" 페이지가 나타납니다.
2. "CA SiteMinder"를 선택합니다.
3. "Enable CA SiteMinder Plug-in"(CA SiteMinder 플러그인 사용) 확인란을 선택합니다.
4. "저장"을 클릭합니다.

CA SiteMinder 와 CA CEM 의 통합 문제 해결

CA CEM 이 CA SiteMinder 와 함께 올바르게 작동하고 있는지 확인하려면

1. CA SiteMinder 가 사용하도록 설정되었는지 확인합니다.
[CA SiteMinder 사용](#) (페이지 419)을 참조하십시오.
2. 정책 서버가 올바른 IP 주소와 포트를 사용하는지 확인합니다.
[CA CEM 에서 정책 서버 정의](#) (페이지 417)를 참조하십시오.

3. CA CEM 과 CA SiteMinder 모두에서 사용되는 공유 암호가 동일한지 확인합니다.

사용자 지정 CA SiteMinder 에이전트 생성을 참조하십시오.

4. CA CEM 과 CA SiteMinder 모두에서 사용되는 에이전트 이름이 동일한지 확인합니다.

[CA CEM 에서 에이전트 정의](#) (페이지 418)를 참조하십시오.

5. 비즈니스 응용 프로그램이 올바르게 설정되었는지 확인합니다.

[비즈니스 응용 프로그램 설정](#) (페이지 412)을 참조하십시오.

6. CA CEM 에서 "설정" > "모니터" > "모든 모니터 동기화"를 선택하여 모니터를 동기화합니다.

7. CA CEM 에서 "설정" > "모니터" > "IP 주소"를 선택하여 TIM 로그에 확인 메시지나 CA SiteMinder 오류 메시지가 있는지 검사합니다.

8. CA SiteMinder 에이전트 로그를 검사하여 오류 메시지가 있는지 확인합니다.

9. CA SiteMinder 에서 정책 서버 로그를 검사하여 오류가 있는지 확인합니다.

제 26 장: CA CEM 과의 CA Service Desk 통합

CA CEM 인시던트 및 결함 정보를 CA Service Desk 에 보낼 수 있으므로 티켓을 적절하게 생성하고 추적할 수 있습니다.

CA Service Desk 는 서비스 지원 인시던트 관리를 자동화하여 ITIL(Information Technology Infrastructure Library) 베스트 프랙티스 프로세스를 이용합니다.

이 섹션은 다음 항목을 포함하고 있습니다.

[CA CEM 과 통합되는 CA Service Desk 정보](#) (페이지 421)

[CA Service Desk 통합 개요](#) (페이지 421)

[CA CEM 에 맞게 CA Service Desk 구성](#) (페이지 422)

[CA CEM 과 함께 CA Service Desk 사용](#) (페이지 426)

[CA Service Desk 와 CA CEM 의 통합 문제 해결](#) (페이지 427)

[CA Service Desk 와 CA CEM 의 통합 용어](#) (페이지 429)

CA CEM 과 통합되는 CA Service Desk 정보

CA Service Desk 는 헬프 데스크 분석가가 인시던트 감지 및 기록, 분류 및 지원, 추적 및 해결을 포함한 인시던트 관리 책임을 수행하도록 지원합니다.

CA CEM 에서 감지된 인시던트를 기반으로 CA Service Desk 에서 서비스 요청 또는 인시던트를 생성하도록 CA CEM 과 CA Service Desk 를 구성할 수 있습니다.

CA Service Desk 통합 개요

CA Service Desk 와의 통합으로 CA CEM 인시던트에서 서비스 요청을 자동으로 생성하여 인시던트 관리 지원을 제공합니다.

CA Service Desk 에서 CA CEM 인시던트를 만들 수 있도록 설정하려면 CA Service Desk 플러그 인을 구성하고 사용되도록 설정하십시오. 구성은 연결을 설정하고 인시던트가 CA Service Desk 에 나타나는 방식을 정의합니다.

CA Service Desk 에서 CA CEM 이 생성한 인시던트를 구분하려면 CA Service Desk 에서 요청 영역을 만드십시오.

통합 관련 용어에 대해서는 [CA Service Desk 와 CA CEM 의 통합 용어](#) (페이지 429)를 참조하십시오. 모든 CA APM 용어 및 정의에 대해서는 [CA APM Glossary](#)(CA APM 용어집)를 참조하십시오.

CA CEM 에 맞게 CA Service Desk 구성

CA Service Desk 가 사용되도록 설정하려면 먼저 CA Service Desk 플러그 인을 구성해야 합니다.

선택적으로 CA Service Desk 요청 영역을 만들어 CA CEM 인시던트를 CA Service Desk 의 다른 서비스 요청과 구분할 수 있습니다.

CA Service Desk 플러그 인 구성

CA Service Desk 플러그 인을 구현하려면 연결 및 요청 정보를 수집해야 합니다.

CA Service Desk 와 통신하도록 CA CEM 을 구성하려면

1. "설정" > "플러그 인"을 선택합니다.

"플러그 인" 페이지가 나타납니다.

2. "CA Service Desk"를 선택합니다.

"CA Service Desk 플러그 인" 페이지가 나타납니다.

3. "CA Service Desk 플러그 인 사용" 확인란을 선택합니다.

그러면 CA CEM 에서 CA Service Desk 로 인시던트 정보를 전송할 수 있습니다.

참고: CA Service Desk 플러그 인을 사용하도록 설정해야 합니다. 그렇지 않으면 통합 기능이 올바르게 작동하지 않습니다.

4. "외부에서 확인 가능한 호스트 이름" - 대부분의 경우 이 필드에 이미 CA CEM 호스트 이름이 포함되어 있습니다. 그렇지 않은 경우, Enterprise Manager 의 IP 주소 또는 호스트 이름을 입력합니다.

이 정보는 CA Service Desk 에서 생성된 전자 메일의 링크에 사용됩니다. CA Service Desk 전자 메일에는 CA CEM 의 인시던트로 다시 연결되는 링크가 포함됩니다.

5. "포트" - 대부분의 경우 이 필드에 이미 CA CEM 포트가 포함되어 있습니다.

참고: 기본 포트는 8081 입니다. 기본 포트는 `IntroscopeEnterpriseManager.properties` 파일에 `introscope.enterprisemanager.webserver.port=8081` 로 정의되며 변경할 수 있습니다.

6. 다음과 같이 CA Service Desk 연결 정보를 입력합니다.
 - a. "호스트 이름" - CA CEM 을 호스팅하는 CA Service Desk 시스템의 호스트 이름 또는 IP 주소를 입력합니다.
 - b. "포트" - CA CEM 이 CA Service Desk 에 연결되는 포트를 입력합니다. CA Service Desk 의 기본 포트 번호는 8080 입니다.
 - c. "사용자 이름" - CA Service Desk 액세스에 사용할 CA CEM 사용자 이름을 입력합니다. CA Service Desk 에 요청을 생성하려면 이 사용자에게 적절한 권한과 액세스 수준이 있어야 합니다.
 - d. "암호" - 사용자 이름과 연결된 암호를 입력합니다.
7. CA CEM 인시던트를 CA Service Desk 에 요청 대신 인시던트로 생성하려면 "Service Desk 에 ITIL 인시던트 만들기" 확인란을 선택합니다.

CA Service Desk 에 인시던트를 생성하지 않으려는 경우 기본 동작은 요청을 생성하는 것입니다.

참고: CA Service Desk 가 ITIL(Information Technology Infrastructure Library)용으로 구성된 경우에만 CA Service Desk 인시던트가 생성됩니다. 그렇지 않으면 CA CEM 인시던트가 요청으로 생성됩니다.

8. "요청 영역" 입력 - CA CEM 관련 문제를 분류하기 위해 CA Service Desk 에 생성되는 요청 영역을 입력합니다.
이 요청 영역은 CA Service Desk 에 생성하는 이름과 동일해야 합니다.
9. 필요한 경우 "요청 필터"를 입력합니다.

팁: 모든 인시던트가 CA Service Desk 에 즉시 전달되도록 허용하는 대신 먼저 요청 필터를 사용하여 단일 비즈니스 서비스 및 비즈니스 트랜잭션과의 통합을 테스트할 수 있습니다.

구문 예제	설명
<i>Request Filter=BusinessServiceName/BusinessTransactionName</i>	지정된 비즈니스 서비스 및 비즈니스 트랜잭션에 대한 인시던트가 발생하는 경우에만 CA Service Desk 에 요청을 생성합니다.
<i>Request Filter=BusinessServiceName/*</i>	모든 인시던트와 지정된 비즈니스 서비스에 대해 트리거된 비즈니스 트랜잭션에 대해 CA Service Desk 에 요청을 생성합니다.
<i>Request Filter=BusinessServiceName/Tra*</i>	모든 인시던트와 지정된 비즈니스 서비스에 대해 트리거되어 "Tra"로 시작하는 비즈니스 트랜잭션에 대해 CA Service Desk 에 요청을 생성합니다.
<i>Request Filter=**</i>	모든 비즈니스 서비스 및 모든 비즈니스 트랜잭션과 연결된 인시던트에 대해 CA Service Desk 에 요청을 생성합니다.

비즈니스 서비스 또는 비즈니스 트랜잭션 이름에 슬래시("/") 문자가 포함되어 있으면 필터에서 이 문자를 이중 슬래시("//")로 바꾸어야 합니다.

비즈니스 서비스 또는 비즈니스 트랜잭션 이름에 쉼표(",") 문자가 포함되어 있으면 필터에서 이 문자를 슬래시-쉼표("/,")로 바꾸어야 합니다.

예를 들어 다음과 같은 경우를 가정합니다.

- business service name = Trade
- business transaction name = Sell Big/Medium Stocks

이 경우 필터는 다음과 같아야 합니다.

Request Filter=Trade/Sell Big//Medium Stocks

예를 들어 다음과 같은 경우를 가정합니다.

- business service name = Trade
- business transaction name = Sell Big, Medium Stocks

이 경우 필터는 다음과 같아야 합니다.

Request Filter=Trade/Sell Big/, Medium Stocks

10. CA Service Desk 요약에 나타날 요청 요약을 입력합니다. 다음과 같이 변수를 사용하여 사용자 지정된 요약을 생성합니다.

- *<defect_name>*
- *<business_service>*
- *<business_transaction>*

변수를 다시 정렬하여 사용자 고유의 요청 요약을 생성할 수 있습니다. 각 변수는 CA Service Desk 에 요청 요약이 나타날 때의 실제 값으로 바뀝니다. 예제:

<defect_name> for <business_service>,<business_transaction>

다음과 같이 나타남: Slow Time for Support Desk, KB Lookup

Business Transaction: <business_transaction> Defect: <defect_name>

다음과 같이 나타남: Business Transaction: CheckOut Defect: Slow Time

11. CA Service Desk 설명에 나타날 요청 설명을 입력합니다. 다음과 같이 변수를 사용하여 사용자 지정된 설명을 생성합니다.

- *<incident_id>*
- *<defect_name>*
- *<business_service>*
- *<business_transaction>*
- *<user_count>*
- *<defect_count>*
- *<incident_link>*

변수를 다시 정렬하여 사용자 고유의 요청 설명을 생성할 수 있습니다. 각 변수는 CA Service Desk 에 요청 설명이 나타날 때의 실제 값으로 바뀝니다.

<incident_link> 변수는 CA Service Desk 에 있는 링크를 제공합니다. 이 링크를 사용하여 인시던트 개요 정보("CEM" > "인시던트 관리" > "인시던트 개요")로 직접 이동할 수 있습니다.

12. "인시던트 심각도가 다음과 같은 경우 Service Desk 요청 만들기:" - 선택한 인시던트 수준을 사용하여 CA Service Desk 에 서비스 요청을 생성할 수 있도록 합니다. 다음 중에서 적절한 확인란을 선택합니다.

- 낮음
- 보통
- 심각함
- 중요

13. "저장"을 클릭합니다.

저장된 구성과 일치하는 CA CEM 인시던트가 이후에 발생하면 CA Service Desk 에서 즉시 적용되는 서비스 요청이 트리거됩니다.

참고: CA CEM 에서 개설된 기존 인시던트는 CA Service Desk 요청을 트리거하지 않습니다.

CA Service Desk 요청 영역 구성

CA CEM 이 보고한 인시던트에 대해 별도의 요청 영역이 필요한 경우 CA Service Desk 에서 요청 영역을 만들어야 합니다.

CA CEM 용 CA Service Desk 에서 요청 영역을 구성하려면

1. 요청 영역(예: *CEM_reported*)을 만듭니다.
2. 다음 세 가지 속성을 요청 영역에 연결합니다.
 - 비즈니스 서비스
 - 비즈니스 트랜잭션
 - 인시던트

요청 영역 만들기 및 구성에 대한 자세한 내용은 CA Service Desk 온라인 도움말의 *Defining Request Areas*(요청 영역 정의)를 참조하십시오.

CA CEM 과 함께 CA Service Desk 사용

CA Service Desk 에서 CA CEM 인시던트 정보를 볼 수 있습니다. CA Service Desk 에서 CA CEM 으로 연결된 링크를 클릭하여 인시던트에 대해 자세히 알아볼 수 있습니다.

CA CEM 을 탐색하여 문제를 해결하고 인시던트의 근본 원인을 확인할 수 있습니다.

CA Service Desk 와 CA CEM 의 통합 문제 해결

CA Service Desk 와의 통합 문제를 해결해야 할 수 있습니다. 이 단원에서는 문제 해결 표를 제공합니다.

증상 및 해결 방법

다음 표에는 CA Service Desk 와 CA CEM 의 통합 문제 해결에 유용한 팁이 몇 가지 나와 있습니다.

증상

CA Service Desk 요청이 어떠한 CA CEM 인시던트에 대해서도 생성되지 않거나 일부에 대해서만 생성됩니다.

해결 방법

다음과 같이 CA Service Desk 플러그 인이 CA CEM 에서 제대로 구성되어 있는지 확인하십시오.

올바른 CA Service Desk 자격 증명이 구성되어 있습니다.

필터가 올바른 비즈니스 서비스와 비즈니스 트랜잭션에 대해 설정되어 있습니다.

적절한 심각도 수준이 사용되도록 설정되어 있습니다.

로그 파일에서 연결 또는 기타 오류가 있는지 확인하십시오.

http://<IP_Address>/cgi-bin/wily/packages/cem/service-desk/index

증상

CA Service Desk 요청이 요청 영역 없이 생성됩니다.

해결 방법

CA Service Desk 관리자가 요청 영역을 만들었는지 확인하십시오.

CA CEM CA Service Desk 플러그 인 구성에 올바른 요청 영역 정보가 포함되어 있는지 확인하십시오.

증상

CA Service Desk 인시던트 또는 요청에서 CA CEM 인시던트 세부 정보로 연결된 링크가 작동하지 않습니다.

해결 방법

인시던트가 CA CEM 데이터베이스에서 삭제되었을 수 있습니다.

"설정" > "인시던트 설정" > "인시던트 만료 처리 규칙"을 확인하십시오.

증상

CA Service Desk 전자 메일에서 CA CEM 인시던트 세부 정보로 연결된 링크가 작동하지 않습니다. 전자 메일에 있는 링크는 다음과 같습니다.

[http://localhost.localdomain/wily/cem/tess/...](http://localhost.localdomain/wily/cem/tess/)

해결 방법

CA CEM CA Service Desk 플러그인 구성에 CA CEM 에 대한 외부에서 확인 가능한 호스트 이름이 포함되어 있는지 확인하십시오.

인시던트가 CA CEM 데이터베이스에서 삭제되었을 수 있습니다. "설정" > "인시던트 설정" > "인시던트 만료 처리 규칙"을 확인하십시오.

증상

CA CEM 에서 인시던트를 종결해도 CA Service Desk 에서 종결되지 않습니다.

해결 방법

CA Service Desk 에서 개별적으로 인시던트/서비스 요청을 종결해야 합니다.

증상

CA Service Desk 에서 인시던트/서비스 요청을 종결해도 CA CEM 에서 종결되지 않습니다.

해결 방법

CA CEM 에서 개별적으로 인시던트를 종결해야 합니다.

CA Service Desk 와 CA CEM 의 통합 용어

제품 통합의 중요한 요소는 용어입니다. 익숙하지 않은 제품의 언어를 숙지해야 합니다. 또한 CA CEM 의 용어와 정의가 CA Service Desk 의 용어에 매핑되는 방식을 알고 있어야 합니다.

CA Service Desk 용어

이러한 CA Service Desk 용어는 제품 통합과 관련이 있습니다.

인시던트

IT 인프라의 서비스 품질 저하를 초래하는 이벤트입니다.

요청 영역

CA Service Desk 시스템 관리자는 요청 영역을 설정하여 유형별로 서비스 요청을 분류합니다. 예를 들어 하드웨어 지원 또는 소프트웨어 설치 등으로 분류됩니다.

서비스 요청

사용자의 지원, 정보 또는 도움 요청이 IT 인프라의 장애를 나타내는 것은 아닙니다.

티켓

티켓은 요청, 인시던트 또는 문제를 의미할 수 있는 CA Service Desk 의 일반 용어입니다. CA Service Desk 의 CA CEM 인시던트는 요청이나 인시던트로 분류됩니다.

CA Service Desk 와 CA CEM 의 용어 매핑

제품마다 발전 주기와 핵심 대상이 다를 수 있고 이러한 차이로 인해 제품 용어와 정의도 달라지곤 합니다.

한 제품의 인시던트가 다른 제품의 티켓인 경우와 같이 일대일 매핑이 있는 경우도 있고 같은 용어가 제품마다 약간씩 각기 다른 의미를 가져서 혼동을 초래할 수 있는 경우도 있습니다.

이러한 용어 매핑은 제품 통합을 탐색할 때 도움이 됩니다.

CA CEM 용어	CA Service Desk 용어 매핑
-----------	-----------------------

인시던트	CA CEM 인시던트는 CA Service Desk 구성과 CA CEM 구성("설정" > "플러그 인")을 기반으로 서비스 요청이나 인시던트를 트리거합니다.
------	---

제 27 장: CA APM 과의 CA APM Cloud Monitor 통합

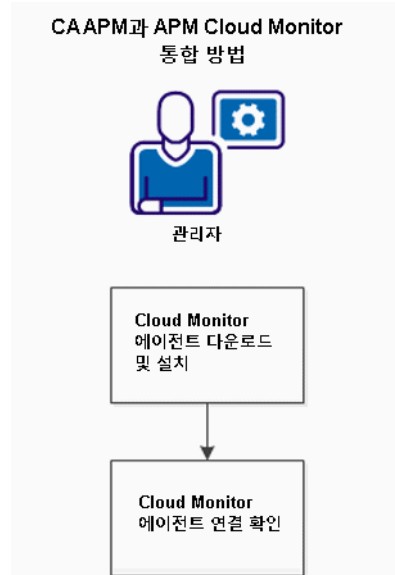
CA APM Cloud Monitor 를 사용하면 다음 작업을 수행할 수 있습니다.

- 40 개 이상의 국가에 있는 60 개 이상의 모니터링 스테이션을 통해 전체 사용자 환경을 이해합니다.
- 실제 브라우저를 모니터링하여 사용자 경험을 정확하게 측정합니다.
- SaaS 공급업체와 MSP 에서 제공하는 응용 프로그램을 모니터링하여 SLA 에 적절한 상태로 유지합니다.
- 가상 트랜잭션을 통해 방화벽 외부로부터의 응용 프로그램 응답 시간을 테스트하여 글로벌 최종 사용자 경험을 이해하고 심지어 실제 사용자 트래픽이 없을 때도 성능을 모니터링할 수 있습니다.
- 실제 사용자 트랜잭션을 복제하고 이를 통해 응용 프로그램 인프라 전체의 성능을 모니터링하여 문제를 빠르게 식별, 진단 및 해결합니다.

CA APM 배포에서 CA APM Cloud Monitor 를 통합하는 방법

APM 관리자는 CA APM 배포에서 CA APM Cloud Monitor 를 통합하여 모니터링 및 심사 기능을 더 추가할 수 있습니다.

다음 순서도에서는 온 프레미스 CA APM 배포에서 CA APM Cloud Monitor 를 통합하는 방법을 보여 줍니다.



1. CA APM Cloud Monitor 에이전트를 다운로드하여 설치합니다. (see page 432)
2. 에이전트 연결의 유효성을 검사합니다. (see page 433)

CA APM Cloud Monitor 에이전트 다운로드 및 설치

이 작업에서는 CA APM Cloud Monitor 와 CA APM 을 통합하는 데 필요한 CA APM Cloud Monitor 에이전트를 다운로드하고 설치합니다.

참고: 네트워크의 원하는 컴퓨터에 CA APM Cloud Monitor 에이전트를 설치할 수 있습니다. 이 에이전트의 기능이 인터넷을 통해 CA APM Cloud Monitor 데이터를 수신하여 Enterprise Manager 에 전달하는 것이므로 모든 컴퓨터에 이 에이전트를 설치할 수 있지만, 서버 수준 CPU/RAM 이 있는 컴퓨터를 선택해야 합니다.

CA APM Cloud Monitor 에이전트를 다운로드하여 설치하려면

1. CA APM Cloud Monitor 에이전트 아카이브 파일을 다운로드합니다. 사용 중인 컴퓨터에 파일을 저장합니다.

Windows, Linux 및 Solaris 용 설치 관리자는 CA APM 소프트웨어 다운로드 웹 사이트에 있습니다.

2. 에이전트를 설치합니다.
 - a. CA APM Cloud Monitor 설치 관리자 파일을 시작합니다.
 - b. 라이선스 계약의 조건에 동의합니다.
 - c. <Agent_Home> 디렉터리를 지정합니다.
 - d. 에이전트가 연결될 Enterprise Manager 호스트와 포트를 지정합니다.
 - e. "Cloud Monitor Account Settings"(클라우드 모니터 계정 설정) 화면에 CA APM Cloud Monitor 사용자 ID 와 암호를 입력합니다. 이러한 자격 증명은 CA APM Cloud Monitor 웹 사이트에 로그인하는 데 사용하는 것과 동일합니다.

CA APM Cloud Monitor 에이전트 설치가 완료됩니다.

참고: 에이전트를 시작하고 연결의 유효성을 검사하는 방법에 대한 자세한 내용은 CA APM Cloud Monitor 에이전트 연결의 유효성 검사 (see page 433)를 참조하십시오.

CA APM Cloud Monitor 에이전트 연결의 유효성 검사

유효성 검사를 통해 CA APM Cloud Monitor 에이전트가 올바르게 설치되었는지 확인하려면 에이전트를 시작하고 CA APM WebView 또는 Workstation 을 사용하여 데이터를 확인하십시오. CA APM Cloud Monitor 에서 들어오는 데이터가 최신인지 확인하여 연결의 유효성을 검사하십시오.

참고: WebView 또는 Workstation 에서 CA APM Cloud Monitor 데이터를 보려면 먼저 CA APM Cloud Monitor 에서 폴더와 모니터를 설정해야 합니다. 이 단계를 수행하지 않았으면 *CA APM Workstation 사용자 안내서*의 CA APM Cloud Monitor 사용 방법 단원을 참조하십시오.

다음 단계를 따르십시오.

1. CA APM Cloud Monitor 에이전트가 설치되어 있는 디렉터리로 이동한 후 다음 파일 중 하나를 실행하여 에이전트를 시작합니다.
 - Windows에서는 APMCloudMonitor.bat 를 두 번 클릭합니다.
 - Linux 또는 Solaris에서는 APMCloudMonitor.sh 를 실행합니다.콘솔 창에서 에이전트가 시작됩니다.
2. CA APM WebView 또는 Workstation 을 시작합니다.
3. CA APM Cloud Monitor 에서 데이터를 찾습니다.
 - a. Investigator 창이 열려 있지 않은 경우 "파일" > "새 Investigator"를 선택합니다.
 - b. "메트릭 브라우저" 탭을 찾습니다.
 - c. 다음 노드를 확장합니다.
SuperDomain | <Host_Name> | APMCloudMonitor |
APMCloudMonitorAgent | APM Cloud Monitor

<Host_Name>은 일반적으로 CA APM Cloud Monitor 에이전트를 설치한 컴퓨터이지만 메트릭 브라우저 트리에 표시되는 내용은 APMCloudMonitor.properties 파일에 있는 apmcm.agent.hostName 속성의 값입니다.
 - d. 폴더를 확장하여 개별 메트릭을 보고 메트릭이 최신 상태인지 확인합니다.

문제 해결

Enterprise Manager 설치 중에 "클라우드 모니터"를 모니터링 옵션으로 선택하지 못한 경우 WebView/Workstation 은 CA APM Cloud Monitor 데이터의 일부 표시를 허용하지 않습니다.

이 문제를 해결하려면

- <EM_Home>\examples\CAAPMIntegrationForCloudMonitor\ 디렉터리의 내용을 <EM_Home>/config/modules/ 및 <EM_Home>/ext/xmltv 에 복사합니다.

그러면 클라우드 모니터 메트릭 데이터를 제대로 표시하는 데 필요한 관리 모듈과 기타 파일을 사용할 수 있게 됩니다.

데이터를 제한하는 방법

성능을 향상시키기 위해 CA APM Cloud Monitor 에이전트가 Enterprise Manager 에 보내는 데이터 양을 제한할 수 있습니다.

CA APM Cloud Monitor 속성을 구성하여 데이터 제한

APMCloudMonitor.properties 파일의 속성을 사용하여 CA APM Cloud Monitor 에이전트가 Enterprise Manager 에 보내는 데이터를 필터링할 수 있습니다.

CA APM Cloud Monitor 에이전트 속성을 구성하여 데이터를 필터링하려면 `<CloudMonitor_Agent_Home>/CloudMon/conf/APMCloudMonitor.properties` 에서 메트릭 필터 섹션을 편집합니다.

이러한 설정에 대한 자세한 내용은 APMCloudMonitor.properties 에 대한 속성 참조 (see page 558)를 참조하십시오.

검사점을 제거하여 데이터 제한

CA APM Cloud Monitor 는 다섯 대륙에서 60 개 이상의 검사점 스테이션에 액세스할 수 있습니다. 클라우드 모니터는 이러한 스테이션 중에서 무작위로 선택해 해당 스테이션으로부터 사용자의 웹 사이트나 응용 프로그램에 대해 가용성과 성능을 검사합니다. 지속적으로 사용하도록 설정된 모든 스테이션에서 이 검사를 수행하여 60 개 이상의 각 사이트에서 데이터가 로깅됩니다.

사용 가능한 검사점 스테이션 중 일부를 제거하여 CA APM Cloud Monitor 가 CA APM 으로 전송하는 데이터의 양을 제한할 수 있습니다.

다음 단계를 따르십시오.

1. CA APM Cloud Monitor 웹 사이트 cloudmonitor.ca.com 에 로그인합니다.
2. "Subscriptions"(구독) > "Preferences"(기본 설정)를 선택합니다.

모든 스테이션은 기본적으로 선택되어 있습니다.

3. 다음처럼 기본 선택을 변경합니다.
 - 개별 스테이션에 대한 확인란을 선택 취소합니다. 또는
 - "지우기"를 클릭하여 모두 선택 취소하고 목록 맨 위의 그룹 중에서 선택합니다.

예를 들어 북아메리카에 있는 스테이션만을 선택하려는 경우에는

 - a. "Clear"(지우기)를 클릭합니다.
 - b. "North America"(북아메리카)를 클릭합니다.
4. 페이지 아래쪽에서 "Change"(변경)를 클릭합니다.

일정을 조정하여 데이터 제한

기본적으로 모니터는 가용성과 성능을 매일 매시간마다 정기적으로 검사합니다. 시간이 경과함에 따라 CA APM 이 반환하는 데이터 양은 사용자가 원하는 양보다 많아질 수 있습니다.

다음 단계를 따르십시오.

1. 클라우드 모니터 웹 사이트 cloudmonitor.ca.com 에 로그인합니다.
2. "Settings"(설정) > "Monitors"(모니터)를 선택합니다.
3. 개별 모니터를 선택하고 "More Options"(추가 옵션)를 선택합니다.
4. 다음 설정을 다시 설정합니다.
 - Delay between checks(검사 간 지연 시간)
 - Check period(검사 기간)
 - Check on these days only(최근 날짜에 대해서만 검사)
 - Maintenance schedule(유지 관리 일정)

부록 A: 속성 파일 참조

다음은 해당 디렉터리에 있는 속성 파일이며 Enterprise Manager, Workstation 및 WebView 설정을 제어하는 데 사용됩니다.

중요! Windows 컴퓨터의 경우 속성 파일에서 경로를 추가할 때 백슬래시(\)를 다른 백슬래시로 이스케이프(이중 처리)해야 합니다(예: `C:\\Introscope\\lib\\Agent.jar`).

이 섹션은 다음 항목을 포함하고 있습니다.

[IntroscopeEnterpriseManager.properties](#) (페이지 437)

[APMEnterpriseManager.properties](#) (페이지 490)

[apm-events-thresholds-config.xml](#) (페이지 494)

[ResourceMetricMap.properties](#) (페이지 511)

[Catalyst.properties](#) (페이지 513)

[EMservice.conf](#) (페이지 522)

[Introscope Enterprise Manager.lax](#) (페이지 529)

[IntroscopeWorkstation.properties](#) (페이지 535)

[Introscope Workstation.lax](#) (페이지 540)

[IntroscopeWebView.properties](#) (페이지 546)

[Introscope WebView.lax](#) (페이지 553)

[APMCloudMonitor.properties](#) (페이지 558)

IntroscopeEnterpriseManager.properties

다양한 Enterprise Manager 동작이 3 개의 Enterprise Manager 속성 파일 중 하나인 *IntroscopeEnterpriseManager.properties* 에 정의된 속성으로 제어됩니다. 다른 속성 파일은 [APMEnterpriseManager.properties](#) (페이지 490)와 [apm-events-thresholds-config.xml](#) (페이지 494)입니다.

대부분의 Enterprise Manager 속성을 구성한 후에는 Enterprise Manager 를 다시 시작해야 변경 사항이 적용됩니다.

그러나 일부 Enterprise Manager 속성은 Introscope 핫 구성 서비스를 사용합니다. 이러한 "핫 구성" 속성을 변경한 후에는 Enterprise Manager 를 다시 시작하지 않아도 됩니다. 자세한 내용은 [핫 구성 서비스](#) (페이지 447)를 참조하십시오.

이 파일에서 다음 속성을 구성할 수 있습니다.

- [사용 가능한 프로세서](#) (페이지 438)
- [경고 동작](#) (페이지 439)
- [통신](#) (페이지 439)
- [Workstation Login Parameters\(Workstation 로그인 매개 변수\) 섹션 자동 채우기](#) (페이지 445)
- [EM 웹 서버 설정](#) (페이지 445)
- [핫 구성 서비스](#) (페이지 447)
- [응용 프로그램 추론](#) (페이지 447)
- [Logging\(로깅\)](#) (페이지 448)
- [영구 수집 - 데이터베이스에 데이터 기록](#) (페이지 450)
- [플랫 파일 속성](#) (페이지 452)
- [트랜잭션 이벤트 데이터베이스](#) (페이지 452)
- [트랜잭션 추적 샘플링](#) (페이지 453)
- [Enterprise Manager 메트릭 클램프](#) (페이지 454)
- [SmartStor](#) (페이지 457)
- [기준 데이터 저장](#) (페이지 462)
- [SNMP 수집](#) (페이지 463)
- [WebView](#) (페이지 463)
- [CA APM ChangeDetector](#) (페이지 464)
- [관리 모듈 부트스트랩](#) (페이지 464)
- [관리 모듈 배포](#) (페이지 465)
- [클러스터링 설정](#) (페이지 465)
- [에이전트 상호 작용](#) (페이지 470)
- [Enterprise Manager 장애 조치](#) (페이지 474)
- [구성 디렉터리](#) (페이지 476)
- [응용 프로그램 심사 맵 데이터](#) (페이지 476)
- [위치 맵 데이터](#) (페이지 481)
- [웹 서비스](#) (페이지 482)
- [나가는 메시지 큐](#) (페이지 483)
- [스레드 덤프](#) (페이지 484)
- [웹 서비스 성능 처리를 위한 스레드 속성](#) (페이지 487)
- [SNMP 심사 맵 경고 작업](#) (페이지 488)
- [응용 프로그램 맵 개체](#) (페이지 489)

사용 가능한 프로세서

IntroscopeEnterpriseManager.properties 의 "Available Processors"(사용 가능한 프로세서) 섹션에는 다음 속성이 포함되어 있습니다.

introscope.enterprisemanager.availableprocessors

이 Enterprise Manager 에 사용 가능한 프로세서 수를 설정하려면 이 속성을 사용하십시오. 한 호스트에 둘 이상의 Enterprise Manager 가 있는 경우에만 사용해야 합니다.

기본값

<blank>

경고 동작

IntroscopeEnterpriseManager.properties 의 "Alert State Metrics"(경고 상태 메트릭) 섹션에는 다음 속성이 포함되어 있습니다.

introscope.enterprisemanager.alertstatemetric.prefix

경고 상태 메트릭이 표시되는 Investigator 노드의 이름입니다.

기본값

경고

통신

IntroscopeEnterpriseManager.properties 의 "Port Settings"(포트 설정) 섹션에는 다음 속성이 포함되어 있습니다.

introscope.enterprisemanager.enabled.channels

Enterprise Manager 가 사용할 수 있는 통신 채널을 지정합니다. 통신 채널이 사용되도록 설정하려면 사용되도록 설정된 채널의 쉼표로 구분된 목록에 채널 유형을 추가하십시오. 통신 채널이 사용되지 않도록 설정하려면 목록에서 해당 통신 채널을 제거하십시오.

enabled.channels 속성은 [introscope.enterprisemanager.port.<ChannelName>](#) (페이지 440) 속성과 함께 작동합니다.

예

두 개의 통신 채널, 즉 channel1 과 channel2 가 있는 경우 다음 속성을 설정합니다.

```
introscope.enterprisemanager.enabled.channels=channel1,channel2
introscope.enterprisemanager.port.channel1=5001
introscope.enterprisemanager.port.channel2=5002
```

기본값

channel1

introscope.enterprisemanager.port.<ChannelName>

Enterprise Manager 가 Workstation 및 에이전트와의 암호화된 통신에 사용하는 수신기 포트입니다.

사용자 지정 통신 채널을 만들려면 속성 파일에 다음 속성을 추가하십시오.

- introscope.enterprisemanager.port.ChannelName
- introscope.enterprisemanager.serversocketfactory.ChannelName
- 여기서 *ChannelName* 은 새 채널의 이름입니다.

사용자 지정 채널이 사용되도록 설정하려면 [introscope.enterprisemanager.enabled.channels](#) (페이지 440) 속성에 해당 채널의 이름을 추가하십시오.

기본값

5001

introscope.enterprisemanager.serversocketfactory.<ChannelName>

이 속성은 Enterprise Manager 가 Workstation 및 에이전트와의 암호화된 통신에 사용하는 서버 소켓 팩터리의 클래스 이름을 식별합니다.

사용자 지정 통신 채널을 생성하는 경우 새 속성을 속성 파일에 추가하십시오. 예를 들면 다음과 같습니다.

introscope.enterprisemanager.serversocketfactory.ChannelName

여기서 ChannelName 은 새 채널의 이름입니다. 속성 값을 *com.wily.isengard.postofficehub.link.net.IServerSocketFactory* 인터페이스를 구현하는 사용자 지정 서버 소켓 팩터리의 정규화된 클래스 이름으로 설정하십시오.

또한 [introscope.enterprisemanager.port.<ChannelName>](#) (페이지 440)에 설명된 대로 채널의 수신기 포트를 지정하고 사용하도록 설정해야 합니다.

예

channel1 과 channel2 라는 통신 채널 2 개가 있는 경우 다음과 같이 설정합니다.

```
introscope.enterprisemanager.enabled.channels=channel1,channel2
introscope.enterprisemanager.port.channel1=5001
introscope.enterprisemanager.port.channel2=5002
```

다음과 같이 serversocketfactory 속성을 설정합니다.

```
introscope.enterprisemanager.serversocketfactory.channel1=<classname>
introscope.enterprisemanager.serversocketfactory.channel2=<classname>
```

기본값

com.wily.isengard.postofficehub.link.net.server.DefaultServerSocketFactory

introscope.enterprisemanager.serversockets.reuseaddr

통신 채널 서버 소켓을 *FIN_WAIT* 또는 *TIME_WAIT* 상태에서 멈춰 있는 로컬 포트에 재바인딩할 수 있도록 하려면 이 속성을 **True** 로 설정하십시오. Enterprise Manager 가 다시 시작된 후에는 이 속성이 사용되지 않도록 설정해야 합니다.

포트가 이미 사용 중인 타당한 이유가 있을 수 있으므로 기본적으로 이 속성이 사용되도록 설정하지 마십시오.

기본값

False

introscope.enterprisemanager.disableInteractiveMode

콘솔이 입력을 받아들이는지 여부에 관계없이 대화식 콘솔이 사용되지 않도록 설정합니다.

참고

많은 UNIX 플랫폼에서는 응용 프로그램이 표준 입력에서 읽으려고 할 경우 **nohup** 가 작동하지 않습니다. **nohup** 모드로 실행하려면 이 속성을 **True** 로 설정하고 응용 프로그램 심사 데이터 파일의 *lax.stdin.redirect* 속성을 **<blank>**로 변경하십시오. 이 두 속성을 모두 위에 설명된 대로 정확히 설정하지 않으면 응용 프로그램을 **nohup** 모드로 시작할 수 없거나 최대 CPU 사용률이 발생할 수 있습니다.

기본값

True

introscope.enterprisemanager.webserver.port

Enterprise Manager 에 포함된 웹 서버가 수신 대기하는 포트입니다.

기본값

8081

introscope.enterprisemanager.webserver.portinuse.fail

다른 응용 프로그램이 Enterprise Manager 와 동일한 포트에서 실행되고 있는 경우 Enterprise Manager 가 시작되지 않도록 합니다.

다른 응용 프로그램이 Enterprise Manager 와 동일한 포트에서 실행되고 있는 경우 이러한 속성 설정은 Enterprise Manager 가 시작되는지 여부를 제어합니다.

- 이 속성을 true 로 설정하면 Enterprise Manager 가 시작되지 않습니다.
- 이 속성을 false 로 설정하면 포트가 사용 중이라는 오류 메시지가 표시됩니다. 그러나 Enterprise Manager 는 시작할 수 있습니다.

기본값

true

introscope.enterprisemanager.ipaddress

포함된 웹 서버를 비롯한 모든 Enterprise Manager 통신 채널을 특정 로컬 IP 주소에 바인딩합니다.

이 속성을 구성하지 않으면 Enterprise Manager 가 모든 로컬 주소의 연결을 받아들입니다.

이 속성을 구성할 때 고려해야 할 규칙은 다음과 같습니다.

- 이 속성을 IPv4 주소로 구성한 경우 Enterprise Manager 는 IPv4 시스템에서 실행 중인 에이전트나 클라이언트의 연결만 받아들입니다.
- 이 속성을 IPv6 주소로 구성한 경우 Enterprise Manager 는 IPv6 호환 JVM 을 실행 중인 컴퓨터에 있는 에이전트나 클라이언트의 연결만 받아들입니다. IPv4 JVM 을 실행 중인 컴퓨터에 있는 에이전트나 클라이언트는 IPv6 주소를 사용하여 연결할 수 없습니다.
- IPV6 이 사용되도록 설정된 시스템에서 실행 중인 Enterprise Manager 또는 WebView 인스턴스를 특정 IP 주소에 바인딩하지 않는 경우 해당 인스턴스는 모든 로컬 주소에 바인딩됩니다. IPv4 환경과 IPv6 환경에서 모두 연결을 받아들일 수 있습니다.
- Workstation, 에이전트, 브라우저 및 기타 클라이언트는 IP 주소가 아닌 DNS 이름을 사용하여 Enterprise Manager 또는 WebView 인스턴스에 연결해야 합니다.
- 에이전트에 대한 IPv6 지원 여부는 에이전트가 실행되고 있는 환경(JVM, 운영 체제, 하드웨어 스택)의 IPv6 지원에 따라 다릅니다.

기본값

<commented out, no value>

introscope.enterprisemanager.workstation.connection.channel

Web Start Workstation 에 연결하기 위한 채널을 지정합니다.

기본값

channel1

introscope.enterprisemanager.workstation.extendedLiveQuery

Workstation 사용자가 기본 시간 범위인 8 분과 레졸루션인 15 초 대신 라이브 모드에 대해 사용자 지정 시간 범위와 레졸루션을 입력할 수 있도록 합니다.

참고: 시간 범위를 8 분보다 크게 설정하면 SmartStor 에서 데이터를 가져오는 I/O 작업으로 인해 Enterprise Manager 성능이 저하될 수 있습니다.

기본값

TRUE

Workstation Login Parameters(Workstation 로그인 매개 변수) 섹션 자동 채우기

IntroscopeEnterpriseManager.properties 의 "Workstation Login Parameters"(Workstation 로그인 매개 변수) 섹션에는 다음 속성이 포함되어 있습니다.

introscope.enterprisemanager.workstation.rememberLogin

Workstation 이 WebStart 에 대한 로그인 매개 변수(Enterprise Manager 호스트, 포트 및 사용자 ID)를 기억하는지 여부를 제어합니다. FALSE 로 설정한 경우 Workstation 은 로그인 매개 변수를 기억하지 않습니다.

기본값

TRUE

EM 웹 서버 설정

IntroscopeEnterpriseManager.properties 의 "EM Web Server Settings"(EM 웹 서버 설정) 섹션에는 다음 속성이 포함되어 있습니다.

introscope.enterprisemanager.webserver.jetty.configurationFile

Jetty XML 구성 파일의 경로입니다. 절대 경로 또는 <EM_Home>/config 디렉터리에 상대적인 경로입니다. 이 파일은 포트 8444 에서 HTTPS 트래픽에 대한 SSL 수신기를 만듭니다.

참고

introscope.enterprisemanager.webserver.jetty.configurationFile 속성의 주석 처리를 해제하면 IntroscopeEnterpriseManager.properties 파일 introscope.enterprisemanager.webserver.port 속성에 지정된 보안되지 않은 HTTP 수신기가 생성되지 않습니다. 하지만 Jetty XML 구성 파일에 보안되지 않은 HTTP 수신기를 구성할 수 있습니다.

이 속성은 핫 구성을 지원하지 않습니다.

기본값

em-jetty-config.xml

introscope.enterprisemanager.webserver.max.threads

웹 서버의 최대 수신기 스레드 수, 즉 Enterprise Manager 의 포함된 웹 서버에서 처리할 수 있는 동시 HTTP 클라이언트 수입니다.

참고

이 Enterprise Manager 에 연결 중인 HTTP 터널링 에이전트가 80 개가 넘는 경우에만 이 속성을 구성하십시오. 이 경우 연결하는 HTTP 터널링 에이전트의 최대 수보다 20 개가 더 많게 속성 값을 설정하는 것이 좋습니다. 동시 HTTP 에이전트가 80 개보다 적을 것으로 예상되면 이 속성 값을 수정하지 마십시오.

기본값

100

핫 구성 서비스

Enterprise Manager 에는 다음 속성에 대해 기본적으로 사용되도록 설정되어 있는 핫 구성이 포함되어 있습니다.

- log4j 로깅 속성 - [로깅](#) (페이지 448) 참조
- 영구 수집 - 데이터베이스 속성에 데이터 기록 - [영구 수집 - 데이터베이스에 데이터 기록](#) (페이지 450) 참조
- Enterprise Manager 메트릭 클램프 속성 - [Enterprise Manager 메트릭 클램프](#) (페이지 454) 참조
- 클러스터링 속성 - [클러스터링 설정](#) (페이지 465) 참조

introscope.enterprisemanager.hotconfig.enable

핫 구성 서비스가 사용되도록 설정합니다. 서비스가 사용되지 않도록 설정하려면 `false` 로 설정하십시오.

기본값

true

introscope.enterprisemanager.hotconfig.pollingInterval

이 파일을 검사하여 변경 사항이 있는지 확인하는 빈도(초)를 지정합니다.

기본값

60 초

응용 프로그램 추론

IntroscopeEnterpriseManager.properties 의 "Application Heuristics"(응용 프로그램 추론) 섹션에는 다음 속성이 포함되어 있습니다.

introscope.enterprisemanager.application.overview.baselines

Enterprise Manager 성능을 개선하기 위해 이 속성을 `false` 로 설정하여 추론을 끌 수 있습니다.

이렇게 하면 Enterprise Manager 가 Enterprise Manager 의 JVM, 응용 프로그램 및 백엔드 건전성 평가를 끕니다. 베이스라이너도 꺼지므로 Workstation 의 메트릭이 비활성 상태가 되고 어떠한 값도 보고하지 않습니다. 구성을 `true` 로 되돌려서 해당 메트릭을 다시 활성 상태로 만들지 않으면 메트릭이 회색으로 나타납니다.

기본값

True

Logging(로깅)

로깅 속성은 Enterprise Manager 로그의 세부 정보 수준과 Enterprise Manager 로그 파일의 이름 및 위치를 정의합니다. 고급 Log4J 함수에 대한 자세한 내용은 <http://jakarta.apache.org/log4j/docs/documentation.html> 에 있는 Log4J 설명서를 참조하십시오.

이러한 Enterprise Manager 속성은 Introscope 핫 구성 서비스를 사용합니다. 이러한 핫 구성 속성을 변경한 후에는 Enterprise Manager 를 다시 시작하지 않아도 됩니다. 자세한 내용은 [핫 구성 서비스](#) (페이지 447)를 참조하십시오.

log4j.logger.Manager

세부 정보 수준과 로그 메시지의 대상을 제어합니다.

세부 정보 수준 값은 `INFO` 또는 `VERBOSE#com.wily.util.feedback.Log4JSeverityLevel` 일 수 있습니다.

대상 값은 `console` 또는 `logfile` 일 수 있습니다. 기본 설정을 적용하면 로그 정보가 콘솔과 로그 파일에 기록됩니다.

기본값

INFO, console, logfile

log4j.appender.logfile.File

Enterprise Manager 홈 디렉토리를 기준으로 하는 Enterprise Manager 로그 파일의 상대 이름 및 위치입니다.

기본값

logs/IntroscopeEnterpriseManager.log

log4j.appender.logfile.layout.ConversionPattern

로그 파일을 사용자 지정할 수 있습니다.

다음 속성 값을 설정할 수 있습니다.

d{M/dd/yy hh:mm:ss a z} [%-3p] [%c] %m%n

패턴은 log4j 라이브러리에서 구현되고 형식은

<http://logging.apache.org/log4j/docs/api/org/apache/log4j/PatternLayout.html>에서 설명됩니다.

날짜/시간 형식은 *%d{..}*의 형태로 나타나고

<http://java.sun.com/j2se/1.4.2/docs/api/java/text/SimpleDateFormat.html>에 설명된 패턴을 따릅니다.

기본값

<blank>

영구 수집 - 데이터베이스에 데이터 기록

이 단원에 설명된 속성을 구성하여 외부 관계형 데이터베이스에 추적된 데이터를 기록할 수 있습니다. 자세한 내용은 *IntroscopeEnterpriseManager.properties* 파일의 "SQL Database Settings"(SQL 데이터베이스 설정) 섹션을 참조하십시오. 이러한 설정은 핫 구성을 통해 배포되므로 Enterprise Manager 를 수동으로 다시 시작하지 않아도 됩니다.

Introscope 에 포함된 API 를 사용하여 기록 범위에 대한 메트릭과 이벤트 데이터를 추출한 다음 Excel, SAS 등의 데이터 분석 도구를 사용하여 Introscope 데이터를 볼 수 있습니다. CA Technologies 는 이 API 기록 데이터를 사용할 것을 권장합니다. [JDBC API](#) (페이지 565)를 참조하십시오. 명령줄 Workstation 명령을 지속 데이터 추출에 사용할 수도 있습니다. 명령줄 Workstation 사용 (see page 147)을 참조하십시오.

이러한 Enterprise Manager 속성은 Introscope 핫 구성 서비스를 사용합니다. 이러한 "핫 구성" 속성을 변경한 후에는 Enterprise Manager 를 다시 시작하지 않아도 됩니다. 자세한 내용은 [핫 구성 서비스](#) (페이지 447)를 참조하십시오.

introscope.enterprisemanager.database.collection.agentExpression

에이전트 정규식 속성입니다. 이 설정을 *IntroscopeEnterpriseManager.properties* 파일에 추가하십시오. 그러면 핫 구성을 통해 배포됩니다.

예:

```
Introscope.enterprisemanager.database.collection.agentExpression=rhart-dt1\\  
/EPAgentProcess1\\|EPAgent5
```

기본값

<blank>

introscope.enterprisemanager.database.collection.metricExpression

메트릭 정규식 속성입니다. 이 설정을 *IntroscopeEnterpriseManager.properties* 파일에 추가하십시오. 그러면 핫 구성을 통해 배포됩니다.

예

```
introscope.enterprisemanager.database.collection.metricExpression=Servlets\\|  
MyServlet:Average Response Time \\(ms\\)
```

기본값

<blank>

introscope.enterprisemanager.database.collection.frequencyinseconds

여기서 *agentExpression* 은 에이전트 정규식이고 *metricExpression* 은 메트릭 정규식이며 *frequencyinseconds* 는 데이터를 집계하여 데이터베이스에 기록하는 빈도(초)입니다. 이 설정을 *IntroscopeEnterpriseManager.properties* 파일에 추가하십시오. 그러면 핫 구성을 통해 배포됩니다.

각 영구 수집의 값이 다를 수 있으므로 기본 설정은 없습니다. 이 속성은 각 영구 수집 후에 설정해야 합니다.

기본값

none

introscope.enterprisemanager.database.recordingQueue.upperLimit.value

큐의 최대 메트릭 데이터 포인트 수입니다. 메트릭 데이터 포인트는 하나의 메트릭에 대한 하나의 데이터 시간 조각입니다. 이 설정은 핫 구성을 통해 배포됩니다.

기본값

150k(천 단위)

플랫 파일 속성

플랫 파일은 쉼표로 구분된 일반 텍스트 값(.csv) 파일입니다. Introscope 가 플랫 파일에 쓸 수는 있지만 플랫 파일에서 읽을 수는 없습니다. 수치 분석 도구로 플랫 파일을 분석할 수 있습니다.

플랫 파일 기록은 기본적으로 사용되도록 설정되어 있고 `<EM_Home>/flatfiles` 디렉터리로 이동됩니다. 이러한 파일이 Introscope 디렉터리 외부의 디렉터리에 상주하도록 지정할 수도 있습니다. Windows 경로의 경우 백슬래시(\)를 다른 백슬래시로 이스케이프(이중 처리)해야 합니다(예: `C:\\Introscope\\FlatFileDir`).

트랜잭션 이벤트 데이터베이스

Enterprise Manager 는 고정된 시간 동안 또는 최대 디스크 사용량이 초과될 때까지 캡처된 트랜잭션 이벤트를 해당 파일 시스템에 로컬로 저장합니다. 트랜잭션 이벤트 데이터베이스 속성을 설정하여 이러한 이벤트를 저장하는 위치와 삭제해야 하는 시기를 제어할 수 있습니다.

introscope.enterprisemanager.transactionevents.storage.dir

Enterprise Manager 홈 디렉터리를 기준으로 Introscope 가 트랜잭션 이벤트 데이터를 저장하는 위치를 지정합니다.

기본값

traces

introscope.enterprisemanager.transactionevents.storage.max.data.age

트랜잭션 이벤트 데이터를 저장하는 기간(일)을 지정합니다.

기본값

14

introscope.enterprisemanager.transactionevents.storage.optimize.frequency

만료 처리된 데이터를 정리하여 추적 저장을 최적화해야 하는 빈도(시간)를 지정합니다.

Enterprise Manager 가 시작될 때 트랜잭션 추적 데이터의 만료 처리가 사용되도록 설정합니다.

기본값

24 시간

introscope.enterprisemanager.transactionevents.storage.optimize.timeoffsethour

시간 오프셋과 비교해서 매일 특정 시간에 시작되도록 삭제를 예약하는 데 사용되는 저장 최적화를 위한 시간 오프셋을 지정합니다.

예를 들어 시간 오프셋은 02 로 설정하고 최적화 빈도([introscope.enterprisemanager.transactionevents.storage.optimize.frequency](#) (페이지 453) 참조)는 24 시간으로 설정한 경우 최적화는 매일 오전 2 시에서 24 시간 오프셋된 시간에 실행됩니다.

이 값은 양의 정수여야 하므로 이 속성의 값으로 00 을 입력할 경우 오류 메시지가 표시됩니다.

기본값

02(오전 2 시)

트랜잭션 추적 샘플링

이러한 트랜잭션 추적 샘플링 속성은 기본적으로 *IntroscopeEnterpriseManager.properties* 에 있습니다.

introscope.agent.transactiontracer.sampling.perinterval.count

기본적으로 1 개의 샘플 추적에 대해 구성되어 있습니다. 이 속성은 introscope.agent.transactiontracer.sampling.interval.seconds 속성과 함께 작동합니다.

값을 수정하고 속성 파일에서 주석 처리를 제거하여 추적할 간격당 추적 수를 변경할 수 있습니다.

기본값

1

introscope.agent.transactiontracer.sampling.interval.seconds

기본적으로 2 분 간격으로 추적하도록 구성되어 있습니다. 이 속성은 introscope.agent.transactiontracer.sampling.perinterval.count 속성과 함께 작동합니다.

값을 수정하고 속성 파일에서 주석 처리를 제거하여 샘플링 간격을 변경할 수 있습니다.

참고

sampling.perinterval 및 sampling.interval 속성의 기본값을 재정의하기 전에 샘플링 속도가 높을수록 Enterprise Manager 에서 부하가 증가할 수 있다는 점을 고려해야 합니다.

기본값

120 초

Enterprise Manager 메트릭 클램프

이러한 속성은 독립 실행형 Enterprise Manager 나 수집기로부터 메트릭에 대해 가져오는 결과 수에 대해 설정되는 제한을 정의합니다. 핫 구성이 가능하므로 핫 배포 중에 Enterprise Manager 가 속성 파일을 검사할 때 값이 적용됩니다. 핫 배포는 약 60 초마다 한 번씩 발생합니다.

클램프를 사용하지 않도록 설정하려면

1. 편집을 위해 IntroscopeEnterpriseManager.properties 파일을 열고 EM Metric Clamping 섹션으로 이동합니다.

2. 클램프를 사용하지 않도록 설정하려면 클램프 값을 0 으로 설정합니다.
3. IntroscopeEnterpriseManager.properties 를 저장하고 닫습니다.

추가 Enterprise Manager 클램프는 <EM_Home>/config 디렉터리의 [apm-events-thresholds-config.xml](#) (페이지 494) 파일에 있습니다.

introscope.enterprisemanager.query.datapointlimit.

이 속성은 다음 유형의 단일 쿼리에 대한 내부 처리가 완료된 후 Enterprise Manager 가 쿼리 실행 소프트웨어에 다시 전송하는 최대 메트릭 데이터 포인트 수를 정의합니다.

- JDBC
- CLW
- 상위 N(CLW 와 Workstation 에 모두 해당)

쿼리 실행 소프트웨어는 Workstation, 확장 또는 내부 계산기일 수 있습니다. 내부 처리는 상위 N 쿼리 또는 기타 필터링일 수 있습니다.

이 클램프의 효과는 클러스터된 수집기나 독립 실행형 Enterprise Manager 가 SmartStor 에서 검색하는 메트릭 수를 줄이는 것입니다. 그러나 Enterprise Manager 는 항상 하나 이상의 메트릭에 대해 전체 데이터를 반환합니다. 클램프는 여러 동시 쿼리에 대한 것이 아니라 각 JDBC, CLW 또는 상위 N 쿼리에 대한 것입니다.

이 속성은 [introscope.enterprisemanager.query.returneddatapointlimit](#) (페이지 457) 속성과 함께 작동합니다.

introscope.enterprisemanager.query.datapointlimit 속성과

introscope.enterprisemanager.query.returneddatapointlimit 속성의 차이는 클램프 발생 위치에 있습니다.

introscope.enterprisemanager.query.datapointlimit 속성은 쿼리를 쿼리 실행 소프트웨어에 다시 전송할 때 메트릭 데이터 포인트를 클램프합니다.

introscope.enterprisemanager.query.datapointlimit 속성은 SmartStor 디스크 읽기를 클램프합니다.

예

예제 1

introscope.enterprisemanager.query.datapointlimit 속성은 10 으로,
introscope.enterprisemanager.query.returneddatapointlimit 속성은 0(제한 없음)으로 설정되어 있습니다.

CA APM 사용자가 10,000 개의 데이터 포인트와 일치하는 상위 100 쿼리를 실행합니다. Enterprise Manager 는 상위 100 개의 데이터 포인트만 Workstation 에 전송해야 합니다. Enterprise Manager 가 SmartStor 에서 10,000 개의 데이터 포인트를 읽고 처리합니다. 그러나 introscope.enterprisemanager.query.datapointlimit 속성이 10 으로 설정되어 있으므로 Enterprise Manager 가 처음 10 개의 데이터 포인트만 Workstation 에 전송합니다.

예제 2

introscope.enterprisemanager.query.datapointlimit 속성은 0(제한 없음)으로,
introscope.enterprisemanager.query.returneddatapointlimit 속성은 1000 으로 설정되어 있습니다.

CA APM 사용자가 10,000 개의 데이터 포인트와 일치하는 상위 100 쿼리를 실행합니다. Enterprise Manager 는 상위 100 개의 데이터 포인트만 Workstation 에 전송해야 합니다. Enterprise Manager 가 SmartStor 에서 1,000 개의 데이터 포인트를 읽고 처리합니다. introscope.enterprisemanager.query.returneddatapointlimit 속성이 1000 으로 설정되어 있으므로 Enterprise Manager 가 상위 100 개의 데이터 포인트를 Workstation 에 자유롭게 전송합니다.

참고

MOM 이나 CDV 의 쿼리를 클램프하기 위한 용도로는 이 속성을 설정할 수 없습니다.

기본값

0 (제한 없음을 의미)

introscope.enterprisemanager.query.returneddatapointlimit

이 속성은 SmartStor 가 단일 JDBC, CLW 또는 상위 N(CLW 와 Workstation 에 모두 해당) 쿼리에 대해 반환하는 데이터 포인트 수를 제한합니다. 클램프의 효과는 클러스터된 수집기나 독립 실행형 Enterprise Manager 에 반환되는 데이터의 메트릭 수를 줄이는 것입니다. 클램프는 여러 동시 쿼리에 대한 것이 아니라 각 JDBC, CLW 또는 상위 N 쿼리에 대한 것입니다.

이 속성은 [introscope.enterprisemanager.query.datapointlimit](#) (페이지 455) 속성과 함께 작동합니다.

예

참고: 예제는 [introscope.enterprisemanager.query.datapointlimit](#) (페이지 455) 속성을 참조하십시오.

참고

MOM 이나 CDV 의 쿼리를 클램프하기 위한 용도로는 이 속성을 설정할 수 없습니다.

기본값

0 (제한 없음을 의미)

SmartStor

이 단원에 나와 있는 속성은 SmartStor 데이터가 저장되는 디렉토리를 정의하고 3 개의 저장 계층에 대한 데이터 수집 및 만료 처리 동작을 구성합니다. 필요한 경우 SmartStor 가 사용되지 않도록 설정할 수도 있습니다.

참고: 3 개의 계층을 모두 정의해야 합니다. 4 개 이상의 계층은 정의할 수 없습니다.

introscope.enterprisemanager.smartstor.enable

SmartStor 가 사용되거나 사용되지 않도록 설정할 수 있습니다. SmartStor 가 사용되지 않도록 설정하면 디스크 공간이 절약되지만 통계가 저장되지 않아서 모니터링하지 못하게 됩니다.

SmartStor 가 사용되지 않도록 설정하려면 **False** 로 설정하십시오.

참고

이 속성이 SmartStor 섹션에 표시되지 않으면 SmartStor 가 사용되도록 설정된 것입니다. SmartStor 가 사용되지 않도록 설정하려면 속성 파일에 *introscope.enterprisemanager.smartstor.enable=false* 행을 추가하십시오.

기본값

True

introscope.enterprisemanager.smartstor.directory

Enterprise Manager 홈 디렉터리를 기준으로 SmartStor 가 사용할 디렉터리를 지정합니다.

기본값

data

introscope.enterprisemanager.smartstor.directory.archive

SmartStor 가 보관된 데이터를 저장하는 데 사용할 디렉터리를 지정합니다.

기본값

data/archive

introscope.enterprisemanager.smartstor.dedicatedcontroller

SmartStor 데이터가 전용 디스크에 기록되는지 여부를 지정합니다.

SmartStor 데이터가 전용 디스크에 기록되면 **true** 로 설정하십시오.

이 속성 사용에 대한 자세한 내용은 *CA APM 크기 조정 및 성능 안내서*를 참조하십시오.

기본값

false

introscope.enterprisemanager.smartstor.tier1.frequency

첫 번째 데이터 계층의 데이터 수집 빈도(초)를 지정합니다. 빈도는 다음과 같습니다.

- 15 초의 배수여야 합니다.
- 1800 초(30 분)보다 크면 안 됩니다.
- 이전 계층 빈도의 짝수 배수(한 배일 수 있고 각 계층의 빈도는 동일할 수 있음)여야 합니다.

기본값

15

introscope.enterprisemanager.smartstor.tier1.age

첫 번째 계층의 데이터가 SmartStor 에서 만료 처리되기 전에 경과할 기간(일)을 지정합니다. 값은 0 일 수 없습니다.

기본값

7

introscope.enterprisemanager.smartstor.tier2.frequency

두 번째 데이터 계층의 데이터 수집 빈도(초)를 지정합니다. 빈도는 다음과 같습니다.

- 15 초의 배수여야 합니다.
- 1800 초(30 분)보다 크면 안 됩니다.
- 이전 계층 빈도의 짝수 배수(한 배일 수 있고 각 계층의 빈도는 동일할 수 있음)여야 합니다.

기본값

60

introscope.enterprisemanager.smartstor.tier2.age

두 번째 계층의 데이터가 SmartStor 에서 만료 처리되기 전에 경과할 기간(일)을 지정합니다. 값은 0 일 수 없습니다.

기본값

23

introscope.enterprisemanager.smartstor.tier3.frequency

세 번째 데이터 계층의 데이터 수집 빈도(초)를 지정합니다. 빈도는 다음과 같습니다.

- 15 초의 배수여야 합니다.
- 1800 초(30 분)보다 크면 안 됩니다.
- 이전 계층 빈도의 짝수 배수(한 배일 수 있고 각 계층의 빈도는 동일할 수 있음)여야 합니다.

기본값

900

introscope.enterprisemanager.smartstor.tier3.age

세 번째 계층의 데이터가 SmartStor 에서 만료 처리되기 전에 경과할 기간(일)을 지정합니다. 값은 0 일 수 없습니다.

기본값

335

introscope.enterprisemanager.memoryCache.elements

이 속성은 기록 데이터 쿼리 속도를 높이기 위해 Enterprise Manager 가 압축된 내부 메모리 캐시에 보관하는 데이터 포인트 수를 제어합니다.

각 데이터 포인트에는 15 초 분량의 메트릭 데이터가 포함됩니다. 기본값인 데이터 포인트 32 개에는 8 분 분량의 기록 메트릭 데이터가 포함됩니다.

범위는 32(8 분)~11520(48 시간)이며 32 로 나눌 수 있어야 합니다.

Workstation 사용량이 급증하는 심사 상황의 경우 데이터 포인트 32 개보다 큰 캐시를 설정할 수 있습니다. 예를 들어 값을 데이터 포인트 240 개로 설정하면 Enterprise Manager 가 메모리 캐시에서 마지막 한 시간 동안의 모든 기록 쿼리를 제공할 수 있습니다.

참고

이 속성은 핫 구성이 불가능합니다. 이 속성을 변경한 경우 변경 사항을 적용하려면 Enterprise Manager 를 다시 시작하십시오.

이 값은 데이터 포인트 32 개보다 작을 수 없습니다. 32 개 미만으로 설정하면 기본값으로 설정됩니다.

값을 32 로 나눌 수 없으면 32 로 나눌 수 있는 가장 가까운 숫자로 줄어듭니다.

중요! 캐시의 데이터 포인트 수를 늘리려면 RAM 이 필요합니다. 여러 기가바이트의 추가 힙 메모리가 있는 64 비트 컴퓨터를 실행하고 있지 않으면 값을 기본값보다 높게 설정하지 마십시오. 힙 조정에 대한 자세한 내용은 *CA APM 크기 조정 및 성능 안내서*를 참조하십시오.

다음 계산을 사용하여 캐시에 필요한 힙 메모리를 계산할 수 있습니다. 캐시된 데이터 포인트당 평균 32 바이트라고 가정하십시오.

데이터 포인트 수 * 32 바이트 * 메트릭 수 = 필요한 캐시 힙 메모리

예

한 시간 정도 분량의 데이터를 보관하도록 캐시를 늘리고 값을 데이터 포인트 256 개로 설정하기로 결정한 경우 다음 수식을 사용하여 필요한 캐시 힙 메모리를 계산할 수 있습니다.

데이터 포인트 256 개 * 32 바이트 * 메트릭 500,000 개 = 캐시 힙 메모리 4.1 GB

Enterprise Manager 힙 크기를 검사하여 캐시 힙 메모리 요구 사항을 기반으로 조정해야 할지 확인합니다.

기본값

데이터 포인트 32 개

introscope.enterprisemanager.smartstor.reperiodizationOffsetHour

이 속성을 사용하면 데이터 계층 지정에 대한 시간 오프셋을 구성할 수 있습니다.

제약 조건

하루 중 시간을 나타내는 0 에서 23 사이의 정수여야 합니다. 여기서 0 은 자정을 나타내고 13 은 오후 1 시를 나타냅니다.

기본값

0. 0 으로 설정하면 데이터 계층 지정이 자정에 시작됩니다.

예

이 속성을 2 로 설정하면 데이터 계층 지정이 오전 2 시에 시작됩니다.

introscope.enterprisemanager.smartstor.conversionOffsetMinute

이 속성을 사용하면 데이터로의 스푼 변환에 대한 시간 오프셋을 구성할 수 있습니다.

제약 조건

0 에서, 정각을 지난 시간(분)을 나타내는 59 사이의 정수여야 합니다.

기본값

0. 예를 들어 값을 xx:00 으로 설정하면 변환이 정각에 시작됩니다.

예

값을 10(xx:10)으로 설정하면 스푼 변환이 정각을 지나 10 분 후에 시작됩니다.

기준 데이터 저장

IntroscopeEnterpriseManager.properties 의 "EM Object Database Settings"(EM 개체 데이터베이스 설정) 섹션에는 다음 속성이 포함되어 있습니다.

introscope.enterprisemanager.dbfile

Introscope 가 메트릭 기준 정보를 저장하는 데이터베이스의 파일 이름과 Enterprise Manager 홈 디렉터리를 기준으로 한 위치를 지정합니다.

기본값

data/baselines.db

SNMP 수집

IntroscopeEnterpriseManager.properties 의 "SNMP Adapter" 섹션에는 다음 속성이 포함되어 있습니다.

introscope.enterprisemanager.snmp.enable

SNMP 에이전트를 사용하도록 설정합니다(SNMPServices.jar 를 설치한 경우에만 해당).

기본값

false

introscope.enterprisemanager.snmp.agent.port

SNMP 에이전트와 통신하는 Enterprise Manager 포트입니다.

기본값

161

WebView

IntroscopeEnterpriseManager.properties 의 "WebView Configuration"(WebView 구성) 섹션에는 다음 속성이 포함되어 있습니다.

introscope.enterprisemanager.webview.disableLogin

WebView 가 Enterprise Manager 와의 연결을 설정할 수 있는지 여부를 결정합니다.

기본값

false

introscope.enterprisemanager.webview.password

WebView 사용자가 Enterprise Manager 에 연결하는 데 사용하는 암호를 지정합니다.

기본값

WebView

CA APM ChangeDetector

IntroscopeEnterpriseManager.properties 의 CA APM ChangeDetector 섹션에는 다음 속성이 포함되어 있습니다.

introscope.changeDetector.disable

이 속성을 사용하여 CA APM ChangeDetector 를 사용하거나 사용하지 않도록 설정할 수 있습니다.

기본값

true

관리 모듈 부트스트랩

IntroscopeEnterpriseManager.properties 의 "Management Module Bootstrapping"(관리 모듈 부트스트랩) 섹션에는 다음 속성이 포함되어 있습니다.

introscope.enterprisemanager.managementModules.invalid.references.as.errors

잘못된 참조를 경고로 로깅합니다. 이 속성을 true 로 설정한 경우 잘못된 참조가 있으면 Enterprise Manager 가 시작되지 않습니다.

기본값

false

관리 모듈 배포

IntroscopeEnterpriseManager.properties 의 "Management Module Deployment"(관리 모듈 배포) 섹션에는 다음 속성이 포함되어 있습니다.

introscope.enterprisemanager.hotdeploy.directory

Enterprise Manager 홈 디렉터리를 기준으로 배포할 업데이트된 응용 프로그램이 있는지 검사할 상대 디렉터를 정의합니다.

기본값

deploy

introscope.enterprisemanager.hotdeploy.checkFrequencyInSeconds

배포할 업데이트된 관리 모듈이 있는지 확인하는 빈도(초)를 지정합니다.

기본값

60

클러스터링 설정

이러한 속성 중 일부는 Enterprise Manager 를 다시 시작해야 설정이 적용됩니다. 다른 속성은 Introscope [핫 구성 서비스](#) (페이지 447)를 사용합니다. 이러한 "핫 구성" 속성을 변경한 후에는 Enterprise Manager 를 다시 시작하지 않아도 됩니다.

introscope.enterprisemanager.clustering.manager.slowcollectorthreshold

사용자 환경의 ping 메트릭 임계값을 정의하려면 이 속성을 설정하십시오. ping 메트릭은 MOM 에서 각 수집기에 연결할 때의 왕복 응답 시간 하한만 모니터링합니다.

기본값

10000(밀리초)

introscope.enterprisemanager.clustering.manager.slowcollectordisconnectthresholdseconds

초과될 경우 수집기에서 MOM 의 연결을 자동으로 끊기 위한 임계값을 정의하려면 이 속성을 설정하십시오. 그러면 클러스터에 있는 수집기 중 하나의 성능이 크게 저하될 때 발생하는 부작용인 전체 클러스터가 중단되는 것을 방지할 수 있습니다.

이 속성을 0 이나 음수 값으로 설정하면 이 임계값이 사용되도록 설정되지 않습니다(권장되지 않음).

참고

MOM 이 7.5 초 간격으로 수집기를 확인하므로 사소한 변경 사항은 해당 동작에 영향을 미치지 않습니다.

기본값

60(초)

introscope.enterprisemanager.clustering.mode

이 속성은 CA APM 환경 내의 Enterprise Manager 역할을 지정합니다.

옵션

CDV - Enterprise Manager 가 크로스 클러스터 데이터 뷰어로 실행됩니다.

Collector - Enterprise Manager 가 수집기로 실행됩니다.

MOM - Enterprise Manager 가 관리자로 실행됩니다.

StandAlone - Enterprise Manager 가 독립 실행형 Enterprise Manager 로 실행됩니다.

참고

이 속성 설정을 적용하려면 Enterprise Manager 를 다시 시작하십시오.

Enterprise Manager 를 CDV 로 구성했다가 다음 역할 중 하나로 변경한 경우에는 컴퓨터에 APM 데이터베이스가 필요합니다.

- MOM
- 수집기
- 독립 실행형 Enterprise Manager

기본값

StandAlone

예

```
introscope.enterprisemanager.clustering.mode=StandAlone
```

introscope.enterprisemanager.clustering.login.<emName>.host

Collector Enterprise Manager 의 호스트 이름이나 IP 주소입니다.

기본값

<blank>

introscope.enterprisemanager.clustering.login.<emName>.port

Collector Enterprise Manager 의 [introscope.enterprisemanager.port.<ChannelName>](#) (페이지 440) 속성 값입니다.

기본값

<blank>

introscope.enterprisemanager.clustering.login.<emName>.publickey

MOM 이 Collector Enterprise Manager 에 연결하는 데 사용하는 암호를 암호화하기 위한 공개 키를 지정합니다.

기본값

config/internal/server/EM.public, 주석 처리됨

introscope.enterprisemanager.clustering.privatekey

MOM 이 Collector Enterprise Manager 에 연결하는 데 사용하는 암호를 해독하는 데 사용되는 개인 키를 지정합니다.

기본값

config/internal/server/EM.private

introscope.enterprisemanager.clustering.collector.identifier

선택 사항입니다. 이 수집기에 설명적인 이름을 지정하려는 경우 이 속성을 설정할 수 있습니다.

식별자를 지정하지 않으면 Introscope 가 기본 식별자인 `host@port` 를 사용합니다. 여기서 `host` 는 Enterprise Manager 의 호스트 이름이고 `port` 는 Enterprise Manager 의 연결 포트입니다.

기본값

false

introscope.enterprisemanager.clustering.manager.staggeredstartdelay

MOM 이 클러스터된 수집기에 대한 연결을 시도하는 간격을 변경하려면 MOM 에서 이 선택적 속성을 설정하십시오. 이 속성을 설정하지 않은 경우 연결 시도의 기본 간격은 0 초입니다. 즉, 수집기가 사용할 수 있게 되는 즉시 MOM 이 각 수집기를 인식합니다.

이 속성을 설정하면 MOM 의 시작 오버헤드를 균등하게 나누는 데 도움이 됩니다. 따라서 대기 중인 다른 수집기와의 연결 프로세스를 시작하기 전에 각 수집기가 온라인 상태가 될 때 연결을 처리할 수 있는 일정 시간이 MOM 에 제공됩니다.

최소값은 0 초입니다.

기본값

0(초) 최소값은 0 초입니다.

introscope.enterprisemanager.loadbalancing.threshold

불균형에 대한 부하 분산 장치의 허용치를 정의하려면 이 속성을 설정하십시오. 수집기의 메트릭 수는 부하 분산 장치가 클러스터를 재분산하기 전에 적어도 임계값만큼 가중치로 조정된 클러스터 평균, 즉 모든 수집기의 평균과 달라야 합니다.

재분산이란 수집기 간에 에이전트를 다시 배포하여 가중치로 조정된 메트릭 부하를 균등하게 하는 것을 의미합니다.

기본값

20000(메트릭)

introscope.enterprisemanager.loadbalancing.interval

부하 분산 장치가 재분산해야 하는 빈도(초)를 결정하려면 이 속성을 설정하십시오. 최소값은 120 초입니다.

기본값

600(10 분)

introscope.enterprisemanager.clustering.login.em1.weight

수집기의 상대 부하를 제어하려면 이 선택적 속성을 설정하십시오.

모든 조건이 그대로일 경우 가중치를 클러스터의 총 가중치로 나눈 것이 해당 수집기에 할당된 메트릭 부하의 백분율입니다. 예를 들어 한 수집기의 가중치는 50 이고 모든 수집기의 가중치 합계는 250 인 경우 해당 수집기에는 클러스터 메트릭 부하의 20%가 할당됩니다.

이 Enterprise Manager 수집기에 대한 부하 분산 가중치가 적용된 클러스터의 평균값입니다.

에이전트 상호 작용

일부 에이전트 상호 작용 속성의 경우 구성 후 Enterprise Manager 를 다시 시작해야 합니다. 다른 속성은 Enterprise Manager 핫 배포 구성 서비스를 사용하여 자동으로 배포되고 핫 배포는 속성 설명에서 지정됩니다.

일부 에이전트 상호 작용 속성은 Enterprise Manager 속성 파일에 포함되지 않습니다. 이러한 속성의 기본값을 변경하려면 해당 파일을 *IntroscopeEnterpriseManager.properties* 파일에 추가하고 파일을 저장하십시오. 속성이 핫 배포되지 않은 경우 새 값을 사용하도록 설정하려면 Enterprise Manager 를 종료했다가 다시 시작하십시오.

introscope.apm.agentcontrol.agent.allowed

이 설정에 따라 에이전트가 loadbalancing.xml 에 있는 정규식과 일치하지 않는 경우 에이전트가 다음 Enterprise Manager 중 하나에 연결하도록 허용되는지 여부가 결정됩니다.

- 특정 독립 실행형 Enterprise Manager
- 수집기

기본값

true

예

introscope.apm.agentcontrol.agent.allowed=true

참고

이 설정은 핫 구성을 사용하여 배포됩니다.

이 속성의 설정에 따라 다음 결과가 발생합니다.

- 이 속성이 IntroscopeEnterpriseManager.properties 파일에 없는 경우 값은 true 입니다.
- 이 속성이 MOM 에 true 로 설정된 경우 loadbalancing.xml 에서 일치하지 않는 모든 에이전트가 클러스터에서 허용됩니다.
- 이 속성이 false 로 설정된 경우 loadbalancing.xml 에서 일치하지 않는 모든 에이전트가 허용되지 않는 것으로 구성되고 다음과 같은 결과가 발생합니다.
 - **9.1 이전 에이전트에 해당** -- 9.1 이전 에이전트는 Enterprise Manager 에 연결하지 않습니다.
 - **9.1 에이전트에 해당** -- 9.1 에이전트는 Enterprise Manager 수동적으로 연결되고 메트릭 데이터를 보내지 않습니다.
 - 에이전트가 APM 상태 콘솔의 "거부된 에이전트" 목록에 추가됩니다.

9.1 이전 에이전트에 해당 -- 9.1 이전 에이전트가 다음과 같은 상태인 경우

- Enterprise Manager 에 연결된 상태
- 이 속성 설정의 변경 내용을 기반으로 허용되지 않는 상태

Enterprise Manager 는 에이전트의 연결을 끊습니다. 이 속성을 변경하거나 loadbalancing.xml 을 구성하여 에이전트가 허용될 때까지 Enterprise Manager 는 추가 에이전트 연결 시도를 모두 거부합니다. 에이전트는

[introscope.enterprisemanager.agent.disallowed.connection.limit](#) (페이지 473) 속성에 구성된 시간을 기반으로 다시 연결될 때까지 기다립니다.

introscope.apm.agentcontrol.agent.emlistlookup.enable

다음에서 각 에이전트로 에이전트 연결이 허용된 Enterprise Manager 목록을 전송할 수 있는지 여부를 결정합니다.

- MOM
- 수집기
- 독립 실행형 Enterprise Manager

다음 중 하나가 에이전트가 연결된 상태에서 다운되는 경우 이 목록은 에이전트에 다음에 연결할 Enterprise Manager 를 알려 줍니다.

- MOM
- 독립 실행형 Enterprise Manager
- 에이전트가 연결되는 초기 수집기

기본값

true

예

introscope.apm.agentcontrol.agent.emlistlookup.enable=true

참고

이 설정은 핫 구성을 사용하여 배포됩니다.

에이전트가 다시 시작될 때 에이전트는 초기 수집기 연결 정보에 에이전트 프로파일 introscope.agent.enterprisemanager.connectionorder 속성을 사용합니다.

introscope.apm.agentcontrol.agent.reconnect.wait

이 설정은 에이전트가 독립 실행형 Enterprise Manager 나 수집기에 대한 다시 연결을 시도할 때까지 대기하는 기본 기간(초)을 제공합니다.

기본값

45(초)

예

introscope.apm.agentcontrol.agent.reconnect.wait=45

참고

이 설정은 핫 구성을 사용하여 배포됩니다.

최소값은 45 입니다. 값을 45 미만으로 설정하면 기본적으로 45 로 설정됩니다.

동시에 많은 에이전트 연결이 발생하지 않도록 하기 위하여 Enterprise Manager 는 -30, -15, 0, 15, 30 으로 이루어진 값 집합 중에서 임의의 수를 속성 값에 더합니다. Enterprise Manager 가 계산된 값 중에서 하나를 임의로 선택하여 에이전트에 제공하면 에이전트는 지정된 시간 동안 대기했다가 다시 연결을 시도합니다.

예를 들어 값을 60 으로 설정한 경우 Enterprise Manager 는 -30,-15, 0 및 15 에 60 을 더하여 계산된 값 집합 30, 45, 60, 75 및 90 을 생성합니다. Enterprise Manager 가 임의로 75 를 선택하여 에이전트에 제공하면 에이전트는 75 초 동안 대기했다가 다시 연결을 시도합니다.

introscope.enterprisemanager.agentconnection.metrics.enable

Enterprise Manager 가 에이전트 연결 메트릭을 생성하는지 여부를 제어합니다. True 또는 False 로 설정할 수 있습니다.

이 속성은 Enterprise Manager 속성 파일에 포함되지 않습니다. 값을 변경하려면 이 속성을 속성 파일에 추가하고 Enterprise Manager 를 다시 시작하여 이 속성이 사용되도록 설정하십시오.

기본값

True

introscope.enterprisemanager.agentconnection.metrics.agentTimeoutInMinutes

에이전트가 연결을 끊은 후 Enterprise Manager 가 해당 에이전트에 대해 생성된 연결 메트릭을 중지하는 시간(분)을 지정합니다.

이 속성은 Enterprise Manager 속성 파일에 포함되지 않습니다. 값을 변경하려면 이 속성을 속성 파일에 추가하고 Enterprise Manager 를 다시 시작하여 이 속성이 사용되도록 설정하십시오.

기본값

30(분)

introscope.enterprisemanager.agent.disallowed.connection.limit

허용되지 않는 것으로 구성된 에이전트 중에서 Enterprise Manager 에 수동적으로 연결할 수 있는 에이전트 수를 제한합니다. 수동적으로 연결된 에이전트는 메트릭 데이터를 전송하지 않습니다.

이 클램프 속성은 MOM, 독립 실행형 Enterprise Manager 및 수집기에 적용됩니다.

이 클램프에 도달하고 허용되지 않는 에이전트가 연결을 시도하면 Enterprise Manager 가 새 연결을 거부합니다. 또한 Enterprise Manager 가 이 동작을 로깅하고 에이전트가 APM 상태 콘솔의 "거부된 에이전트" 목록에 추가됩니다.

기본값

0(무제한)

예

```
introscope.enterprisemanager.agent.disallowed.connection.limit=0
```

참고

이 설정은 핫 구성을 사용하여 배포됩니다.

이 속성은 9.1 이상의 에이전트에 적용됩니다.

이 속성이 MOM 에 설정된 경우에는 MOM 값이 수집기 값을 재정의하지 않습니다.

introscope.enterprisemanager.autoUnmountDelayInMinutes

연결 끊김이 일시적인 경우 에이전트의 연결이 끊긴 후 Enterprise Manager 가 계속해서 에이전트를 추적하는 시간(분)입니다. 이 시간이 지나면 Enterprise Manager 가 에이전트 추적 리소스를 해제합니다.

기본값

60(분)

Enterprise Manager 장애 조치

다음 속성을 사용하면 Enterprise Manager 가 설치 디렉토리를 공유하는 데 사용할 수 있는 장애 조치 설정이 사용되도록 지정하고 해당 설정을 적용할 수 있습니다. 속성을 설정하는 경우 Enterprise Manager 장애 조치 규칙을 고려해야 할 수 있습니다.

introscope.enterprisemanager.failover.enable

이 속성은 장애 조치가 사용되도록 설정합니다.

기본값

false

introscope.enterprisemanager.failover.primary

이 속성을 사용하여 기본 Enterprise Manager 의 호스트 이름 또는 IP 주소를 설정할 수 있습니다. 둘 다 기본 Enterprise Manager 로 구성하려면 기본 Enterprise Manager 의 호스트 이름 또는 IP 주소를 쉼표로 구분된 목록으로 설정하십시오. 예를 들어 두 Enterprise Manager 가 모두 기본 Enterprise Manager 로 구성된 경우(*introscope.enterprisemanager.failover.primary=myhost1, myhost2*)를 가정해 봅시다.

이 경우 공유 파일 시스템이 아닌 단일 호스트에 대해 Enterprise Manager 장애 조치를 구성한다면 기본 Enterprise Manager 를 자신으로 설정해야 합니다. 또한 *introscope.enterprisemanager.failover.secondary* 속성을 비워 두어야 합니다.

기본값

<blank>

introscope.enterprisemanager.failover.secondary

이 속성을 사용하면 Enterprise Manager 호스트의 호스트 이름이나 IP 주소를 지정하여 보조 Enterprise Manager 의 호스트 이름이나 IP 주소를 설정할 수 있습니다. 예를 들어 *introscope.enterprisemanager.failover.secondary=myhost2* 와 같이 설정합니다.

기본값

<blank>

introscope.enterprisemanager.failover.interval

이 속성을 사용하면 실행 중인 보조 Enterprise Manager 가 기본 Enterprise Manager 가 시작 대기 중인지 여부를 확인하는 빈도(초)를 설정할 수 있습니다. 이 설정은 핫 구성을 통해 배포됩니다.

기본값

120(2 분)

구성 디렉터리

"EM Config Directory"(EM Config 디렉터리) 섹션에 있는 이 속성을 사용하면 Enterprise Manager *config* 디렉터리의 위치를 지정할 수 있습니다.

introscope.enterprisemanager.directory.config

Enterprise Manager 가 구성에 사용하는 디렉터리입니다. Windows 의 경우 백슬래시를 이스케이프(이중 처리)해야 합니다. 예를 들어 `C:\\Introscope\\config` 와 같이 처리합니다.

기본값

원래 Introscope 설치에 있는 config 디렉터리

응용 프로그램 심사 맵 데이터

이러한 속성을 사용하면 응용 프로그램 심사 맵 데이터 설정이 사용되도록 설정하고 적용할 수 있습니다. 구성 지침에 대해서는 [응용 프로그램 심사 맵 구성](#) (페이지 243)을 참조하십시오.

응용 프로그램 심사 맵과 관련된 추가 속성은 `APMEnterpriseManager.properties` 파일에서 구성됩니다. [APMEnterpriseManager.properties](#) (페이지 490)를 참조하십시오.

introscope.apm.data.agingTime

에이전트가 로드하는 이 속성은 에이전트에서 응용 프로그램 심사 맵 데이터를 Enterprise Manager 로 보고하는 빈도를 제어합니다.

참고

이 속성은 핫 구성이 불가능합니다. 이 속성을 변경한 경우 변경 사항을 적용하려면 에이전트와 Enterprise Manager 를 다시 시작하십시오.

경고! 이 속성을 변경하기 전에 APM 데이터베이스에서 맵 데이터를 삭제하십시오. 이 값을 변경한 경우 이전 맵 데이터와 새 맵 데이터를 함께 사용하면 새 값 측면에서 일관되지 않은 기록 쿼리 결과가 표시됩니다. APM 데이터베이스에서 맵 데이터 삭제에 대한 자세한 내용은 [응용 프로그램 심사 맵 데이터 정리](#) (페이지 249)를 참조하십시오.

이 값은 1 분보다 작을 수 없습니다. 1 분보다 작게 설정한 경우 속성은 기본적으로 1 일로 설정됩니다.

이 설정을 결정할 경우 해당 조직에서 응용 프로그램을 추가하고 수정하는 빈도를 고려하십시오. 낮은 값을 설정할수록 실시간 응용 프로그램 종속성이 맵에 표시되지만 더 많은 에이전트 및 Enterprise Manager 오버헤드가 사용될 수 있습니다. 높은 값을 설정할수록 최신이 아닐 수 있는 응용 프로그램 종속성이 맵에 표시되지만 더 적은 에이전트 및 Enterprise Manager 오버헤드가 사용될 수 있습니다.

에이전트 및 Enterprise Manager 오버헤드에 대한 자세한 내용은 CA APM *Sizing and Performance Guide*(CA APM 크기 조정 및 성능 안내서)를 참조하십시오.

다음 시간 단위를 사용하십시오. 이러한 시간 단위는 대/소문자를 구분하지 않습니다.

- "일"의 경우: days, D 사용
- "분"의 경우: mins, M 사용
- "시간"의 경우: hours, H 사용

이 `agingTime` 속성은 `introscope.apm.data.timeWindow` 속성과 함께 작동하는데, 일반적으로 `agingTime` 이 `timeWindow` 의 하위 집합입니다.

예

`introscope.apm.data.agingTime` 값은 3 일이고 `introscope.apm.data.timeWindow` 값은 10 일인 경우 응용 프로그램 심사 맵에는 에이전트가 이전 10 일 동안 보고한 응용 프로그램 종속성이 표시됩니다. 이러한 10 일 동안 보고된 종속성 데이터가 없는 경우 종속성은 `agingTime` 기간이 만료된 후 또는 3 일 후에 만료 처리된 것으로 나타나고, 10 일의 `timeWindow` 가 끝날 때까지 맵에서 만료 처리된 요소로 유지됩니다.

기본값

1 day

introscope.apm.data.timeWindow

이 속성은 *introscope.apm.data.agingTime* 속성에 정의된 기간에 더하여 기간을 정의합니다.

참고

이 속성은 핫 구성이 불가능합니다. 이 속성을 변경한 경우 변경 사항을 적용하려면 Enterprise Manager 를 다시 시작하십시오.

이 값은 1 분보다 작을 수 없습니다. 1 분보다 작게 설정한 경우 속성은 기본적으로 1 일로 설정됩니다.

다음 시간 단위를 사용하십시오. 이러한 시간 단위는 대/소문자를 구분하지 않습니다.

- "일"의 경우: days, D 사용
- "분"의 경우: mins, M 사용
- "시간"의 경우: hours, H 사용
- "초"의 경우: secs, S 사용
- "밀리초"의 경우: MS 사용

이 속성은 *introscope.apm.data.timeWindow* 속성과 함께 작동하는데, 일반적으로 *agingTime* 이 *timeWindow* 의 하위 집합입니다.

예

introscope.apm.data.agingTime 값은 3 일이고

introscope.apm.data.timeWindow 값은 10 일인 경우 응용 프로그램 심사 맵에는 에이전트가 이전 10 일 동안 보고한 응용 프로그램 종속성이 표시됩니다. 이러한 10 일 동안 보고된 종속성 데이터가 없는 경우 종속성은 *agingTime* 기간이 만료된 후 또는 3 일 후에 만료 처리된 것으로 나타나고, 10 일의 *timeWindow* 가 끝날 때까지 맵에서 만료 처리된 요소로 유지됩니다.

이 설정을 결정할 경우 해당 조직에서 응용 프로그램을 추가하고 수정하는 빈도를 고려하십시오. 낮은 값을 설정할수록 실시간 응용 프로그램 종속성이 맵에 표시되지만 더 많은 에이전트 및 Enterprise Manager 오버헤드가 사용될 수 있습니다. 높은 값을 설정할수록 최신이 아닐 수 있는 응용 프로그램 종속성이 맵에 표시되지만 더 적은 에이전트 및 Enterprise Manager 오버헤드가 사용될 수 있습니다.

에이전트 및 Enterprise Manager 오버헤드에 대한 자세한 내용은 *CA APM Sizing and Performance Guide*(CA APM 크기 조정 및 성능 안내서)를 참조하십시오.

기본값

3 days

introscope.apm.pruning.enabled

이 속성은 APM 데이터베이스에서 응용 프로그램 심사 맵 데이터를 정리하도록 설정합니다.

참고

- 이 속성은 핫 구성이 불가능합니다. 이 속성을 변경한 경우 변경 사항을 적용하려면 Enterprise Manager 를 다시 시작하십시오.
- 이 속성을 true 로 설정한 경우 응용 프로그램 심사 맵 데이터가 APM 데이터베이스에서 정리됩니다.
- 이 속성을 false 로 설정하면 응용 프로그램 심사 맵 데이터가 APM 데이터베이스에서 정리되지 않고 무한정 저장됩니다.

기본값

응용 프로그램 심사 맵 데이터 정리는 기본적으로 클러스터 환경의 APM 데이터베이스에서 독립 실행형 Enterprise Manager 와 MOM 에 대해 수행되도록 설정됩니다.

중요! 응용 프로그램 심사 데이터를 정리하도록 수집기를 구성할 수 없습니다. 수집기의 `introscope.apm.pruning.enabled` 속성을 `true` 로 설정하면 오류가 반환됩니다.

introscope.apm.data.preserving.time

이 속성은 APM 데이터베이스에 응용 프로그램 심사 맵 데이터를 저장하는 기간을 제어합니다. 유지 시간 값보다 오래된 맵 데이터는 만료 처리된 것으로 간주되어 정리될 수 있습니다.

참고

이 속성은 핫 구성이 불가능합니다. 이 속성을 변경한 경우 변경 사항을 적용하려면 Enterprise Manager 를 다시 시작하십시오.

정리되는 동안 `introscope.apm.data.preserving.time` 값과 `Introscope.apm.data.agingTime` 값의 합계보다 오래된 응용 프로그램 심사 맵 데이터가 삭제됩니다.

예를 들어 `introscope.apm.data.preserving.time` 값은 30 일이고 `Introscope.apm.data.agingTime` 값은 1 일인 경우 31 일(30 일 + 1 일)보다 오래된 맵 데이터가 삭제됩니다.

경고! 유지 시간 값을 초 또는 밀리초 단위로 너무 낮게 설정하면 응용 프로그램 심사 맵 데이터가 Enterprise Manager 로부터 도달하자마자 APM 데이터베이스에서 삭제될 수 있습니다.

다음 시간 단위를 사용하십시오. 이러한 시간 단위는 대/소문자를 구분하지 않습니다.

- "일"의 경우: days, D 사용
- "분"의 경우: mins, M 사용
- "시간"의 경우: hours, H 사용
- "초"의 경우: secs, S 사용
- "밀리초"의 경우: MS 사용

기본값

365 days

introscope.apm.pruning.cron.trigger.expression

이 속성은 APM 데이터베이스에서 만료 처리된 응용 프로그램 심사 맵 데이터를 정리하는 빈도를 예약합니다.

참고

이 속성은 핫 구성이 불가능합니다. 이 속성을 변경한 경우 변경 사항을 적용하려면 Enterprise Manager 를 다시 시작하십시오.

introscope.apm.pruning.cron.trigger.expression 속성의 형식은 Open Symphony Quartz CronTrigger 스케줄러 표현식으로 지정됩니다. Quartz CronTrigger 에 대한 자세한 내용은 www.quartz-scheduler.org (www.quartz-scheduler.org)를 참조하십시오.

이 표현식은 6 개 또는 7 개의 필드를 공백으로 구분한 문자열입니다. 왼쪽에서 오른쪽으로 살펴볼 경우 문자열의 필드는 다음과 같습니다.

초, 분, 시간, 날짜, 월, 요일, 연도

필드에 포함될 수 있는 사항은 다음과 같습니다.

- 허용된 값
- 해당 필드에 대해 허용된 특수 문자의 다양한 조합

허용된 값, 특수 문자 및 예제 표현식에 대해서는 www.quartz-scheduler.org (www.quartz-scheduler.org)를 참조하십시오.

기본값

006**?- 이 기본 표현식은 매일 오전 6 시에 맵 데이터를 정리합니다.

위치 맵 데이터

다음 속성을 사용하면 위치 맵 설정을 구성할 수 있습니다.

introscope.Workstation.locationmap.clamp

이 속성은 위치 맵에 포함될 수 있는 최대 요소 수를 제어합니다. clamp 는 위치 맵의 크기를 제어합니다.

참고

반환된 요소 수가 clamp 의 값을 초과하는 경우 일부 맵 요소가 표시되지 않습니다. 일부 요소가 표시되지 않는다는 내용의 오류 메시지가 사용자에게 표시됩니다.

기본값

500

웹 서비스

사용자가 웹 서비스 API 에 정기적으로 액세스하면 다수의 웹 서비스 호출로 인해 성능 저하가 발생할 수 있습니다. 기본적으로 웹 서비스 전용 스레드 수는 10 으로 설정되어 있습니다. IntroscopeEnterpriseManager.properties 파일에 속성을 추가하여 이 설정을 변경할 수 있습니다.

introscope.apm.model.webservices.threadpool.numberofthreads

이 속성은 스레드 풀에 사용되는 스레드 수를 지정합니다. 이 속성의 사용 여부는 선택 사항입니다.

경고! 이 속성을 큰 수로 설정하면 성능 저하가 발생할 수 있습니다. 이 속성을 설정할 때 주의를 기울이십시오.

제약 조건

정수여야 합니다.

기본값

10

예

```
introscope.apm.model.webservices.threadpool.numberofthreads=15
```

이 속성은 *CA APM Catalyst Connector 안내서*에도 설명되어 있습니다.

나가는 메시지 큐

이러한 속성을 사용하면 나가는 메시지 큐 설정을 구성할 수 있습니다.

transport.outgoingMessageQueueSize

이 속성은 나가는 메시지 큐의 메시지 수를 지정합니다.

참고

나가는 메시지 큐 크기를 늘릴수록 RAM 이 더 많이 사용됩니다.

제약 조건

정수여야 합니다.

기본값

3000

예

```
transport.outgoingMessageQueueSize=3000
```

이 속성은 *CA APM 크기 조정 및 성능 안내서*에도 설명되어 있습니다.

transport.override.isengard.high.concurrency.pool.max.size

이 속성은 최대 동시 출력 소켓 연결 스레드 수를 지정합니다. 큰 수로 설정하면 응답 시간이 직접 개선되는 것이 아니라 격리된 느린 연결로 인해 Enterprise Manager 가 아주 느려지는 경우가 줄어듭니다.

기본값인 5 는 대부분의 독립 실행형 Enterprise Manager 와 수집기에 적합합니다. MOM 에는 수집기당 하나의 스레드와 10 개의 Workstation 마다 하나 정도의 스레드가 더 있어야 합니다.

MOM 은 네트워크 트래픽 라우터의 역할을 하므로 특히 나가는 스레드가 더 많을 경우 이점이 있을 수 있습니다. 이는 더 많은 Workstation 을 동시에 처리할 수 있고 단일 수집기가 오버로드될 때 전체 클러스터 동결을 방지하는 데 도움이 되기 때문입니다.

중요! 추가 스레드 오버헤드로 인해 OutOfMemory 예외가 발생할 수 있으므로 크기를 초과하지 마십시오. 특히 32 비트 JVM 에서 주의해야 합니다.

제약 조건

정수여야 합니다.

기본값

5

예

```
transport.override.isengard.high.concurrency.pool.max.size=5
```

이 속성은 *CA APM 크기 조정 및 성능 안내서*에도 설명되어 있습니다.

스레드 덤프

이러한 속성을 사용하면 스레드 덤프를 구성할 수 있습니다.

스레드 덤프 사용 및 구성에 대한 자세한 내용은 *CA APM Java Agent 구현 안내서*를 참조하십시오.

이 기능에 대해 다음 속성을 구성할 수 있습니다.

[introscope.enterprisemanager.threaddump.enable](#) (페이지 484)

[introscope.enterprisemanager.threaddump.storage.dir](#) (페이지 485)

[introscope.enterprisemanager.threaddump.storage.clean.disk.freq.days](#)
(페이지 485)

[introscope.enterprisemanager.threaddump.storage.clean.disk.olderthan.days](#)
(페이지 486)

[introscope.enterprisemanager.threaddump.storage.max.disk.usage](#) (페이지 486)

introscope.enterprisemanager.threaddump.enable

이 속성은 Enterprise Manager에 연결된 에이전트의 메트릭 브라우저 트리 에이전트 노드에서 "스레드 덤프" 탭을 사용하도록 설정합니다.

참고

이 속성은 핫 구성이 가능합니다. 이 속성을 변경한 경우에는 변경 사항을 적용하기 위해 Enterprise Manager를 다시 시작하지 않아도 됩니다.

이 속성은 IntroscopeAgentProfile introscope.agent.threaddump.enable 속성과 함께 작동합니다. 자세한 내용은 *CA APM Java Agent 구현 안내서*를 참조하십시오.

이 속성을 *true* 로 설정하고 IntroscopeAgentProfile introscope.agent.threaddump.enable 속성을 *true* 로 설정한 경우 사용자에게 "스레드 덤프" 탭이 표시됩니다.

이 속성을 *false* 로 설정한 경우에는 사용자에게 "스레드 덤프" 탭이 표시되지 않습니다.

기본값

true

introscope.enterprisemanager.threaddump.storage.dir

Enterprise Manager 홈 디렉터리를 기준으로 스레드 덤프가 저장되는 상대 디렉터리를 지정합니다.

참고

이 속성은 핫 구성이 불가능합니다. 이 속성을 변경한 경우 변경 사항을 적용하려면 Enterprise Manager 를 다시 시작하십시오.

<EM_Home>/threaddumps 는 사용자가 스레드 덤프 텍스트 파일을 저장하는 디렉터리가 아닙니다. 사용자는 스레드 덤프 텍스트 파일을 아무 위치에나 저장할 수 있습니다.

기본값

threaddumps

introscope.enterprisemanager.threaddump.storage.clean.disk.freq.days

CA Introscope 가 스레드 덤프 파일을 삭제하는 빈도(일)입니다.

참고

이 속성은 introscope.enterprisemanager.threaddump.storage.clean.disk.olderthan.days 속성과 함께 작동합니다. 두 속성을 모두 설정하여 Enterprise Manager 에 스레드 덤프 파일 저장 및 삭제 기간을 알려십시오.

이 속성은 핫 구성이 불가능합니다. 이 속성을 변경한 경우 변경 사항을 적용하려면 Enterprise Manager 를 다시 시작하십시오.

기본값

1(일)

introscope.enterprisemanager.threaddump.storage.clean.disk.olderthan.days

CA Introscope 가 스레드 덤프 파일을 삭제하기까지의 기간(일)입니다.

참고

이 속성은 introscope.enterprisemanager.threaddump.storage.clean.disk.freq.days 속성과 함께 작동합니다. 두 속성을 모두 설정하여 Enterprise Manager 에 스레드 덤프 파일 저장 및 삭제 기간을 알려주세요.

이 속성은 핫 구성이 불가능합니다. 이 속성을 변경한 경우 변경 사항을 적용하려면 Enterprise Manager 를 다시 시작하십시오.

기본값

30(일)

introscope.enterprisemanager.threaddump.storage.max.disk.usage

Enterprise Manager 에 저장할 수 있는 스레드 덤프 수입니다.

참고

이 속성은 핫 구성이 불가능합니다. 이 속성을 변경한 경우 변경 사항을 적용하려면 Enterprise Manager 를 다시 시작하십시오.

제약 조건

8000 이하의 정수여야 합니다.

기본값

5000

웹 서비스 성능 처리를 위한 스레드 속성

사용자가 웹 서비스 API 에 정기적으로 액세스하면 다수의 웹 서비스 호출로 인해 성능 저하가 발생합니다. 기본적으로 웹 서비스 전용 스레드 수는 10 으로 설정되어 있습니다. IntroscopeEnterpriseManager.properties 파일에 속성을 추가하여 이 설정을 변경할 수 있습니다.

속성 이름

```
introscope.apm.model.webservices.threadpool.numberofthreads
```

설명

스레드 풀에 사용되는 스레드 수를 지정합니다. 이 속성의 사용 여부는 선택 사항입니다.

제약 조건

정수여야 합니다.

기본값

10

예

```
introscope.apm.model.webservices.threadpool.numberofthreads=15
```

이 속성을 사용하려면

1. 편집을 위해 IntroscopeEnterpriseManager.properties 파일을 엽니다.
2. introscope.apm.model.webservices.threadpool.numberofthreads 속성을 추가하고 값을 지정합니다.

참고: 이 속성을 큰 수로 설정하면 성능이 저하됩니다. 이 속성을 설정할 때 주의를 기울이십시오.

3. properties 파일을 저장하고 닫습니다.

참고: IntroscopeEnterpriseManager.properties 파일을 편집한 후 Enterprise Manager 를 다시 시작해야 변경 사항이 적용됩니다.

SNMP 심사 맵 경고 작업

SNMP 심사 맵 경고 작업 플러그 인은 Enterprise Manager 설치 관리자의 일부로 설치됩니다. SNMP 심사 맵 경고 작업 속성을 지정하려면 다음 구성을 설정하십시오.

참고: SNMP 심사 맵 경고 작업 플러그 인 속성은 기존 SNMP 경고 작업 어댑터 속성과 다릅니다. 접두사인 *introscope.apm.catalyst.triagemapalert.snmp* 를 사용하여 새 SNMP 심사 맵 경고를 구분할 수 있습니다.

introscope.apm.catalyst.triagemapalert.snmp.destination.host.ip

APM 커넥터의 IP 주소를 사용하여 이 속성을 설정하십시오.

introscope.apm.catalyst.triagemapalert.snmp.destination.trap.port

SNMP 트랩이 전송되는 SNMP 포트를 사용하여 이 속성을 설정하십시오.

기본값

162

예

introscope.apm.catalyst.triagemapalert.snmp.destination.trap.port=162

introscope.apm.catalyst.triagemapalert.snmp.community

SNMP 커뮤니티 문자열을 사용하여 이 속성을 설정하십시오.

기본값

public

예

introscope.apm.catalyst.triagemapalert.snmp.community=public

introscope.apm.catalyst.triagemapalert.snmp.trigger

SNMP 트랩 알림에 대해 원하는 트리거 유형을 사용하여 이 속성을 설정하십시오.

기본값

3

옵션

1

문제가 있는 각 기간

2

심각도가 증가하는 경우

3

심각도가 변경될 때마다

4

심각도가 변경될 때마다 마지막 상태만 보고

예

```
introscope.apm.catalyst.triagemapalert.snmp.trigger=3
```

응용 프로그램 맵 개체

응용 프로그램 맵 개체의 제한이 사용되지 않는 것으로 간주되도록 지정하려면 이 속성을 설정하십시오.

기본값

300(일)

예

```
introscope.apm.data.obsolete.time=300
```

APMEnterpriseManager.properties

APMEnterpriseManager.properties 파일에 정의된 속성은 다양한 Enterprise Manager 동작을 제어합니다. *APMEnterpriseManager.properties* 파일은 주로 응용 프로그램 심사 맵을 지원합니다. Enterprise Manager 동작을 구성하는데 사용되는 다른 속성 파일은 [IntroscopeEnterpriseManager.properties](#) (페이지 437)와 [apm-events-thresholds-config.xml](#) (페이지 494)입니다.

많은 Enterprise Manager 속성을 구성한 후에 변경 사항을 적용하려면 Enterprise Manager 를 다시 시작해야 합니다. 그러나 일부 Enterprise Manager 속성은 Introscope [핫 구성 서비스](#) (페이지 447)를 사용합니다. 이러한 속성을 *핫 구성 속성*이라고 합니다. 핫 구성 속성을 구성한 후에는 Enterprise Manager 를 다시 시작하지 않아도 됩니다.

c3p0 속성

c3p0 속성 섹션에서는 APM 데이터베이스 연결 풀링에 대한 속성을 구성합니다. c3p0 에 대한 자세한 내용은 <http://www.mchange.com/projects/c3p0/index.html> 을 참조하십시오.

중요! 속성 값을 변경하기 전에 *CA APM 크기 조정 및 성능 안내서*에서 c3p0 속성에 대한 내용을 살펴보는 것이 좋습니다.

c3p0.dataSourceName

연결 대상이 되는 데이터 원본의 이름입니다. 기본 이름을 사용자 APM 데이터베이스의 이름으로 바꾸십시오.

기본값

apmDataSource

c3p0.acquireIncrement

풀에 있는 연결이 부족할 때 c3p0 이 한 번에 가져오려고 시도하는 연결 수를 결정합니다.

기본값

3

c3p0.idleConnectionTestPeriod

연결이 유휴 상태가 될 때 c3p0 이 연결을 테스트하려고 시도하는 기간(초)입니다. 이 기간이 끝나면 C3p0 이 이 간격의 풀에 있는 유휴 연결을 모두 테스트합니다.

기본값

120

c3p0.maxIdleTime

유휴 연결이 연결 풀에서 제거되기 전에 유지되는 시간(초)입니다. 0 으로 설정하면 연결이 풀에서 시간 초과되지 않습니다.

기본값

0

c3p0.initialPoolSize

시작할 때 풀이 가져오려고 시도하는 연결 수입니다. minPoolSize 에서 maxPoolSize 사이여야 합니다.

기본값

2

c3p0.minPoolSize

풀에서 항상 유지되는 최소 연결 수입니다.

기본값

2

c3p0.maxPoolSize

풀에서 항상 유지되는 최대 연결 수입니다.

기본값

4

Hibernate 관련 속성

Hibernate 관련 속성 섹션에서는 투명 지속성을 사용하도록 설정하여 데이터를 APM 데이터베이스에 저장하는 과정을 단순화하는 오픈 소스 Hibernate API 요소를 구성합니다. Hibernate 에 대한 자세한 내용은 <http://www.hibernate.org> 를 참조하십시오.

hibernate.jdbc.batch_size

JDBC 배치 크기를 지정합니다.

기본값

10

hibernate.order_inserts

일괄 삽입이 사용되도록 설정합니다.

Hibernate 가 각 엔터티에 대한 삽입을 일괄 처리하도록 설정하는 데 중요합니다. 사용자가 이 속성을 편집하면 안 됩니다.

기본값

true

hibernate.order_updates

일괄 업데이트가 사용되도록 설정합니다. Hibernate 가 각 엔터티에 대한 업데이트를 일괄 처리하도록 설정하는 데 중요합니다. 사용자가 이 속성을 편집하면 안 됩니다.

기본값

true

Hibernate 캐시 설정

Hibernate 캐시 설정 섹션에서는 APM 데이터베이스의 데이터 캐싱에 대한 속성을 구성합니다.

hibernate.cache.provider_class

사용할 Hibernate 캐싱 유형을 지정합니다.

이 속성을 변경하지 마십시오.

기본값

org.hibernate.cache.EhCacheProvider

hibernate.cache.use_second_level_cache

Hibernate 두 번째 수준 캐싱이 사용되도록 설정합니다.

기본값

true

hibernate.statement_cache.size

명령문 캐시 크기를 지정합니다.

기본값

10

ApplicationTriageMap 설정

이 섹션에서는 응용 프로그램 심사 맵에 대한 설정을 사용자 지정할 수 있습니다.

hibernate.cache.provider_configuration_file_resource_path

Hibernate ehCache 구성 파일을 지정합니다.

기본값

apm-ehcache.xml

introscope.apm.query.max.results

에이전트가 응용 프로그램 심사 맵 표시 화면으로 반환하는 데이터 양에 대한 임계값을 지정하려면 이 속성을 사용하십시오. 값은 대략적으로 프런트엔드 또는 비즈니스 트랜잭션에 대한 종속성 수와 프런트엔드 또는 트랜잭션이 배포된 에이전트 중에서 쿼리 중인 기간 동안 데이터를 보고한 에이전트 수를 곱한 값입니다.

기본값

20000

apm-events-thresholds-config.xml

3 개의 Enterprise Manager 속성 파일 중 하나에 정의된 속성이 여러 Enterprise Manager 동작을 제어합니다. 이 단원에서는 *apm-events-thresholds-config.xml* 에 있는 속성을 설명합니다. 나머지 속성은 *IntroscopeEnterpriseMangager.properties* (페이지 437)와 *APMEnterpriseManager.properties* (페이지 490)입니다. `<EM_Home>/config` 디렉터리에 있는 *apm-events-thresholds-config.xml* 파일에는 CA Introscope 및 CA CEM 클램프와 CA APM 중요한 이벤트에 대한 속성이 포함되어 있습니다.

- 이러한 클램프가 구성된 임계값에 도달하거나 구성된 임계값을 초과하면 Enterprise Manager 가 APM 상태 콘솔의 "클램프" 탭에 알립니다.
- 중요한 이벤트가 구성된 임계값에 도달하거나 구성된 임계값을 초과하면 Enterprise Manager 가 APM 상태 콘솔의 "중요한 이벤트" 테이블 뷰에 알립니다.

중요! 오직 임계값 필드에 있는 임계값만 구성하십시오. `clamp ID`, `importantEvent ID`, `description` 등의 다른 필드는 CA Introscope 의 시스템 모니터링에 사용되므로 변경하지 마십시오.

apm-events-thresholds-config.xml 구성 변경 사항을 적용하기 위해 Enterprise Manager 또는 모니터링된 응용 프로그램을 다시 시작할 필요가 없습니다. 이러한 속성은 Introscope [핫 구성](#) (페이지 447) 서비스를 사용합니다. 속성이 핫 구성을 사용하는 경우에는 구성 변경 후 Enterprise Manager 를 다시 시작하지 않아도 됩니다.

중요! 구성 변경 전에 `apm-events-thresholds-config.xml` 파일을 백업하십시오. 구성으로 인해 `apm-events-thresholds-config.xml` 파일에 오류가 발생하면 Enterprise Manager 가 파일을 읽을 수 없고 기본 클램프 임계값 설정을 적용합니다. 예를 들어 `apm-events-thresholds-config.xml` 에 닫는 괄호가 없으면 Enterprise Manager 가 파일을 읽을 수 없습니다. 새 구성이나 업데이트된 파일이 제대로 작동하지 않으면 다음 작업 중 하나를 수행하십시오.

- 가급적 XML 편집기를 사용하여, 마지막으로 변경된 파일의 문제를 해결합니다.
- 제대로 작동한 이전 백업을 복원합니다.

Introscope 클램프 속성

이러한 속성은 Introscope 별 클램프 속성에 대해 설정되는 제한을 정의합니다. 속성 임계값에 도달하거나 속성 임계값을 초과하면 Enterprise Manager 가 APM 상태 콘솔에 알립니다.

이러한 속성은 핫 구성이 가능하므로 핫 배포 중에 Enterprise Manager 가 속성 파일을 검사할 때 값이 적용됩니다. 핫 배포는 약 60 초마다 한 번씩 발생합니다.

<EM_Home>/config 디렉터리의 [IntroscopeEnterpriseManager.properties](#) (페이지 437) 파일에서 추가 Enterprise Manager 클램프를 찾을 수 있습니다.

introscope.clw.max.users

이 속성은 지정된 시간에 Enterprise Manager 에 대한 연결이 허용된 명령줄 Workstation(CLW) 수를 제한합니다.

CLW 연결로 인해 Enterprise Manager 가 느려지는 경향이 있으면 이 클램프를 사용하십시오. CLW 연결은 너무 많은 메트릭을 추출하려고 시도하여 Enterprise Manager 를 오버로드할 수 있습니다.

참고

이 클램프를 독립 실행형 Enterprise Manager, MOM 및 CDV 에 사용할 수 있습니다. 그러나 수집기에 대한 Workstation 연결은 일반적으로 이루어지지 않습니다.

사용자가 CLW 명령을 실행하면 Enterprise Manager 가 각 쿼리에 대해 2 개의 연결을 만듭니다. 한 연결은 Enterprise Manager 가 사용 가능한지 여부를 파악하고, 다른 연결은 쿼리에 사용됩니다. 즉, 각 CLW 명령은 introscope.clw.max.users 수를 1 이 아닌 2 씩 증가시킵니다. 또한, 일부 CLW 는 Enterprise Manager 에 2 개를 초과하는 연결을 만듭니다. introscope.clw.max.users 속성 임계값을 설정할 때는 이러한 요인을 고려하십시오.

기본값

500

introscope.enterprisemanager.agent.connection.limit

introscope.enterprisemanager.agent.connection.limit 속성은 Enterprise Manager 에 연결될 수 있는 에이전트 수를 제한합니다.

이 속성은 독립 실행형 Enterprise Manager 와 수집기에 모두 적용됩니다.

클램프 임계값에 도달한 경우 새 에이전트가 Enterprise Manager 에 대한 연결을 시도하면 다음 동작이 발생합니다.

- Enterprise Manager 가 이 클램프 활성화를 로깅합니다.
- Enterprise Manager 가 새 연결을 수락하지 않습니다.

참고

Enterprise Manager 는 [em-jetty-config.xml 파일](#) (페이지 45)의 maxThreads 속성을 사용하여 Enterprise Manager 가 처리할 수 있는 HTTPS 에이전트 연결 수를 제한합니다. Enterprise Manager 는 충분한 스레드가 없을 경우 연결된 에이전트 또는 프로세스 메트릭을 인식하지 못합니다.

HTTPS 를 사용하는 경우 Enterprise Manager 는 maxThreads 속성에 구성되어 있는 수의 에이전트만 처리합니다. maxThreads 값은 introscope.enterprisemanager.agent.connection.limit 값 이상이어야 합니다. 에이전트가 HTTPS 를 통해 연결되도록 구성된 경우 스레드가 충분하지 않으면 일부 HTTPS 에이전트가 클라이언트에 나타나지 않거나 메트릭을 보고하지 않을 수 있습니다.

maxThreads 속성으로 Enterprise Manager 가 처리하는 에이전트 수를 제한하는 경우 Enterprise Manager 및 에이전트 로그에는 처리되지 않는 에이전트에 대한 오류, 경고 또는 메시지가 포함되지 않습니다.

기본적으로 온 프레미스 설치의 에이전트는 HTTPS 를 사용하여 연결되지 않습니다.

기본값

400

예

```
introscope.enterprisemanager.agent.connection.limit=400
```

introscope.enterprisemanager.agent.error.limit

introscope.enterprisemanager.agent.error.limit 속성은 오류 스냅샷을 클램프합니다. 이 속성은 Enterprise Manager 가 간격당 각 에이전트에 대해 처리할 수 있는 오류 스냅샷 수에 대한 제한을 정의합니다.

이 속성은 독립 실행형 Enterprise Manager 와 수집기에 모두 적용됩니다.

에이전트가 보고하는 오류 스냅샷 수가 지정된 제한을 초과하면 Enterprise Manager 가 나머지 오류를 모두 드롭합니다.

기본값

10

예

```
introscope.enterprisemanager.agent.error.limit=10
```

introscope.enterprisemanager.agent.metrics.limit

값 초과 시 에이전트 보고가 클램프되는 값으로 이 속성을 설정하십시오.

예를 들어 기본 메트릭 수 1,200,000 개에 도달하면 다음 동작이 발생합니다.

- 에이전트가 메트릭을 120,000 개만 보고합니다.
- 에이전트가 새 메트릭을 Enterprise Manager 에 전송하지 않습니다.

에이전트를 부적절하게 구성하면 수천 개의 메트릭이 연달아 생성되어 Enterprise Manager 가 오버로드될 수 있습니다.

메트릭 오버로드를 방지하려면 이 속성을 사용하십시오. 에이전트가 지정된 개수보다 많은 메트릭을 생성하면 Enterprise Manager 가 해당 메트릭을 드롭합니다. 이 경우 에이전트 구성을 수정하여 보고되는 메트릭 볼륨을 줄이십시오.

참고: 자세한 내용은 *CA APM Java Agent 구현 안내서* 또는 *CA APM .NET 에이전트 구현 안내서*를 참조하십시오.

기본값

120000

참고

이 클램프 속성은 Introscope.Agent.profile 파일에 있는 introscope.agent.metricClamp 속성과 함께 작동합니다.

introscope.enterprisemanager.agent.metrics.limit 클램프 값이 introscope.agent.metricClamp 값보다 먼저 트리거되면 Enterprise Manager 가 에이전트 메트릭을 읽기는 하지만 Investigator 메트릭 브라우저 트리에서 해당 메트릭을 보고하지는 않습니다.

introscope.agent.metricClamp 클램프 값이 introscope.enterprisemanager.agent.metrics.limit 클램프 값보다 먼저 트리거되면 에이전트에서 Enterprise Manager 로의 메트릭 전송이 중지됩니다.

introscope.enterprisemanager.agent.trace.limit

introscope.enterprisemanager.agent.trace.limit 속성은 트랜잭션 추적을 클램프합니다. 이 속성은 Enterprise Manager 가 간격당 각 에이전트에 대해 처리할 수 있는 트랜잭션 이벤트 수에 대한 제한을 정의합니다.

이 속성은 독립 실행형 Enterprise Manager 와 수집기에 모두 적용됩니다.

에이전트가 보고하는 트랜잭션 추적 수가 지정된 제한을 초과하면 Enterprise Manager 가 나머지 추적을 모두 드롭합니다.

기본값

1000

예

```
introscope.enterprisemanager.agent.trace.limit=1000
```

introscope.cdv.max.users

이 속성은 단일 수집기에 연결될 수 있는 크로스 클러스터 데이터 뷰어(CDV) 수를 제한합니다. 크로스 클러스터 데이터 뷰어는 일반적으로 둘 이상의 클러스터에 있는 수집기 여러 개에 연결됩니다.

CDV 연결은 메트릭을 추출하여 수집기 성능 부하를 증가시킬 수 있습니다. 수집기가 수락할 수 있는 CDV 연결 수를 제한하려면 이 클램프를 사용하십시오.

기본값

5

introscope.enterprisemanager.disconnected.historical.agent.limit

이 속성은 연결이 끊겼지만 여전히 마운트된 기록 에이전트 수를 제한합니다. 이 클램프는 Enterprise Manager 런타임 메모리 사용을 최소화합니다.

이 클램프는 다음 기록 에이전트를 모두 제한합니다.

- Enterprise Manager 가 자동으로 마운트 해제할 수 있는 기록 에이전트
- CA APM 사용자가 수동으로 마운트 해제해야 하는 기록 에이전트

에이전트 마운트 및 마운트 해제에 대한 자세한 내용은 *CA APM Workstation 사용자 안내서*를 참조하십시오.

클램프 임계값에 도달한 경우 Enterprise Manager 는 가장 오래된 연결이 끊긴 기록 에이전트 중에서 자동으로 마운트 해제할 수 있는 기록 에이전트를 마운트 해제하려고 시도합니다. Enterprise Manager 가 자동으로 마운트 해제할 수 있는 기록 에이전트가 없으면 CA APM 사용자가 연결이 끊긴 기록 에이전트를 모두 수동으로 마운트한 것입니다. Enterprise Manager 는 CA APM 사용자가 수동으로 마운트한 연결이 끊긴 기록 에이전트를 절대로 마운트 해제하지 않습니다.

예

`introscope.enterprisemanager.disconnected.historical.agent.limit=400`

클램프 임계값이 400 으로 설정되어 있습니다. Tomcat 이라는 에이전트 하나와 Other 라는 에이전트 399 개가 Enterprise Manager 에 연결되어 있습니다. Tomcat 에이전트는 400 개의 에이전트 중에서 자동으로 마운트 해제할 수 있는 가장 오래된 에이전트입니다. Enterprise Manager 가 에이전트 400 개의 연결을 모두 끊습니다. 에이전트가 다시 연결될 때 Enterprise Manager 는 연결이 끊겼지만 여전히 마운트된 에이전트의 수가 에이전트 임계값인 400 보다 적은지 확인합니다. Other 라는 에이전트 399 개가 모두 다시 연결된 다음 Tomcat 에이전트가 다시 연결을 시도합니다. Enterprise Manager 가 다음 작업을 수행합니다.

- Tomcat 에이전트가 연결이 끊긴 에이전트 400 개 중에서 자동으로 마운트 해제할 수 있는 가장 오래된 에이전트인지 확인합니다.
- Tomcat 에이전트를 마운트 해제합니다.

Tomcat 에이전트가 마운트 해제된 후에는 연결이 끊긴 에이전트 수가 다시 에이전트 클램프 임계값인 400 보다 적은 399 개가 됩니다.

참고

다음과 같은 경우 Enterprise Manager 가 APM 상태 콘솔에 알립니다.

- 연결이 끊긴 마운트된 에이전트가 클램프로 인해 마운트 해제된 경우
- 수동 에이전트 마운트가 실패한 경우

다음과 같은 경우 이 클램프는 연결이 끊긴 마운트된 에이전트를 정리하지 않습니다.

- Enterprise Manager 메모리가 부족한 경우
- 연결이 끊긴 기록 에이전트가 시간 초과로 인해 자동으로 마운트 해제된 경우

다음과 같은 경우에는 연결이 끊긴 기록 에이전트가 마운트된 상태로 유지됩니다.

- 자동으로 마운트 해제할 수 있는 기록 에이전트의 연결이 끊긴 경우
- 연결이 끊긴 기록 에이전트 수가 `introscope.enterprisemanager.disconnected.historical.agent.limit` 값보다 적은 경우

다음과 같은 경우에는 Enterprise Manager 가 연결이 끊긴 에이전트를 마운트합니다.

- CA APM 사용자가 연결이 끊긴 기록 에이전트를 수동으로 마운트하려고 시도하는 경우
- 연결이 끊긴 기록 에이전트 수가 `introscope.enterprisemanager.disconnected.historical.agent.limit` 값보다 적은 경우

다음과 같은 경우에는 Enterprise Manager 가 자동으로 마운트 해제할 수 있는 마운트된 연결이 끊긴 에이전트를 검색합니다.

- 자동으로 마운트 해제할 수 있는 기록 에이전트의 연결이 끊긴 경우
- CA APM 사용자가 기록 에이전트를 수동으로 마운트하려고 시도하는 경우
- 연결이 끊긴 기록 에이전트 수가 `introscope.enterprisemanager.disconnected.historical.agent.limit` 값과 같은 경우

Enterprise Manager 가 마운트된 연결이 끊긴 에이전트를 찾으면 가장 오래된 연결이 끊긴 기록 에이전트를 마운트 해제하고 새로 연결이 끊긴 에이전트를 마운트된 상태로 유지합니다. Enterprise Manager 가 자동으로 마운트 해제할 수 있는 기록 에이전트가 없는 경우 Enterprise Manager 는 새로 연결이 끊긴 기록 에이전트를 즉시 마운트 해제합니다. CA APM 사용자가 기록 에이전트를 수동으로 마운트하려고 시도하면 다음 동작이 발생합니다.

- Workstation 에서 일부 기록 에이전트를 마운트 해제하여 새 기록 에이전트를 마운트할 공간을 확보하라는 오류 메시지가 표시됩니다.
- Enterprise Manager 가 APM 상태 콘솔에 알림을 전송합니다.

기본값

400

introscope.enterprisemanager.events.limit

introscope.enterprisemanager.events.limit 속성은 트랜잭션 추적을 클램프합니다. 이 속성은 Enterprise Manager 가 각 간격에 대해 처리하는 트랜잭션 이벤트 수에 대한 제한을 정의합니다.

이 속성은 독립 실행형 Enterprise Manager, 수집기 및 MOM 에 적용됩니다.

이 클램프는 모든 에이전트에서 생성된 모든 트랜잭션 이벤트의 총 수에 적용됩니다. 클램프에 도달하면 에이전트에서 보고된 모든 나머지 트랜잭션 이벤트가 해당 간격의 남은 기간 동안 드롭됩니다.

기본값

1250

예

```
introscope.enterprisemanager.events.limit=1250
```

introscope.enterprisemanager.metrics.historical.limit

이 속성은 Enterprise Manager 의 기록 메트릭 수를 제한합니다. 제한이 15 초마다 검사되므로 클램프가 적용되기 전에 Enterprise Manager 가 이 값을 초과할 수 있습니다. 이 제한이 초과되었다고 감지하는 경우 Enterprise Manager 는 모든 에이전트의 새 메트릭 등록을 중지합니다. 이전 메트릭은 계속해서 보고됩니다.

기본값

1200000

introscope.enterprisemanager.metrics.live.limit

이 속성은 에이전트에서 현재 보고되는 라이브 메트릭을 제한합니다. 이 제한이 초과되었다고 감지하는 경우 Enterprise Manager 는 모든 에이전트의 새 메트릭 등록을 중지합니다. 제한이 15 초마다 검사되므로 클램프가 적용되기 전에 Enterprise Manager 가 이 값을 초과할 수 있습니다. 이전 메트릭은 계속해서 보고됩니다. 기록 데이터가 있는 메트릭은 결코 클램프되지 않습니다.

예

클램프하기 전에 에이전트가 Enterprise Manager 에 보고한 메트릭이 60k 이고 50k 의 클램프가 적용되는 경우 60k 의 이전 메트릭을 모두 Enterprise Manager 에 여전히 등록할 수 있습니다. 그러나 기록 데이터가 아직 수집되지 않은 새 메트릭을 등록하려고 시도하는 경우에는 등록이 허용되지 않습니다.

기본값

500000

introscope.enterprisemanager.transactionevents.storage.max.disk.usage

트랜잭션 추적 저장에 사용할 최대 디스크 사용량(MB)을 결정합니다. 이 최대값이 초과되면 총 기록 추적 저장소 크기가 이 속성 값보다 작아질 때까지 매일 저장된 기록 추적이 가장 오래된 것부터 삭제됩니다. 이 속성 값의 크기가 초과되더라도 저장된 추적이 삭제되지 않을 수 있는데, 이는 저장된 기록 추적 중에서 삭제할 기록 추적을 결정할 때 추적 인덱스 크기가 고려되지 않기 때문입니다.

값이 음수이거나 0 이면 저장된 기록 추적 값이 모두 삭제되어야 함을 나타냅니다.

트랜잭션 이벤트 데이터베이스가 이 값보다 크면 총 데이터베이스 크기가 이 값보다 작아질 때까지 가장 오래된 저장소 파일부터 기록 저장소 파일이 삭제됩니다.

따라서 만료 처리된 날짜에 도달하지 않더라도 기록 데이터가 삭제될 수 있습니다. 현재 라이브 저장소는 크기가 최대 데이터베이스 크기를 초과해도 삭제되지 않습니다.

트랜잭션 이벤트 데이터베이스가 너무 크다고 판단되면 **Enterprise Manager** 가 종료되었을 때 데이터베이스 파일을 수동으로 삭제할 수 있습니다. **Enterprise Manager** 가 다시 시작되면 트랜잭션 추적 저장소 시스템에서 파일이 수동으로 삭제되었음을 인식하고 그에 따라 추적 인덱스를 조정합니다.

참고

파일을 수동으로 삭제하는 경우 추적 디렉터리에서 *traces_yyyyMMdd.db* 형식의 파일만 삭제하십시오. 여기서 *yyyymmdd*는 해당 파일에 있는 추적의 연도, 월 및 일을 나타냅니다. 해당 디렉터리나 하위 디렉터리에 있는 다른 파일은 삭제하지 마십시오.

기본값

1024

introscope.workstation.max.users

이 속성은 지정된 시간에 **Enterprise Manager** 에 대한 연결이 허용된 **Workstation** 수를 제한합니다.

Workstation 연결로 인해 **Enterprise Manager** 가 느려지는 경향이 있으면 이 클램프를 사용하십시오. 여러 **Workstation** 연결에서 너무 많은 메트릭을 추출하려고 시도하면 **Enterprise Manager** 에 오버로드가 발생할 수 있습니다.

참고

이 클램프를 독립 실행형 **Enterprise Manager**, **MOM** 및 **CDV** 에 사용할 수 있습니다. 그러나 수집기에 대한 **Workstation** 연결은 일반적으로 이루어지지 않습니다.

기본값

40

고객 경험 클램프 속성

이 속성은 CA CEM 별 클램프 속성에 설정되는 제한을 정의합니다. 이러한 속성 임계값에 도달하거나 이러한 속성 임계값이 초과되면 Enterprise Manager 가 APM 상태 콘솔에 알립니다.

이러한 속성은 핫 구성이 가능하므로 핫 배포 중에 Enterprise Manager 가 속성 파일을 검사할 때 값이 적용됩니다. 핫 배포는 약 60 초마다 한 번씩 발생합니다.

introscope.enterprisemanager.max.application.user.rows

검색되는 최대 응용 프로그램 사용자 수입니다.

응용 프로그램 사용자가 너무 많으면 성능이 저하될 수 있습니다.

옵션

숫자 값

기본값

1000

예

introscope.enterprisemanager.max.application.user.rows =1000

참고

최대값에 도달한 경우 CA CEM 콘솔은 응용 프로그램 사용자를 나열하는 웹 페이지에 표시되는 사항을 제한합니다.

마지막 동기화 이후 변경 사항 목록의 항목 수 제한

모니터를 동기화하기 전에 마지막 동기화 이후의 구성 변경 사항을 검토할 수 있습니다. 이 방법은 [마지막 동기화 이후의 구성 변경 사항 보기](#) (페이지 316)에 설명되어 있습니다.

구성 변경 사항은 "모니터" 페이지의 "도메인 구성 변경 기록" 테이블에 나타납니다.

introscope.enterprisemanager.max.number.domain.configuration.changes 속성은 이 테이블의 최대 행 수를 결정합니다.

introscope.enterprisemanager.max.number.domain.configuration.changes

"설정" > "모니터"에서 "마지막 동기화 이후 변경 내용 보기"를 클릭할 경우 "도메인 구성 변경 기록" 테이블에 나타나는 최대 변경 사항 수를 설정합니다.

값이 -1 이면 모든 변경 사항이 나타납니다.

옵션

숫자 값

기본값

0(무제한)

예

```
introscope.enterprisemanager.max.number.domain.configuration.changes=1000
```

참고

[모니터 동기화](#) (페이지 315)를 참조하십시오.

introscope.enterprisemanager.max.transaction.user.groups

자동으로 생성되는 최대 사용자 그룹 수입니다.

이 속성은 요청 특성을 통해 자동으로 생성되거나 IP 서브넷별로 자동으로 생성되는 사용자 그룹과 함께 작동합니다.

사용자가 없는 그룹이더라도 사용자 그룹이 너무 많으면 성능이 저하될 수 있습니다.

옵션

숫자 값

허용된 최대값은 10,000 입니다.

기본값

5000

예

```
introscope.enterprisemanager.max.transaction.user.groups=5000
```

참고

최대값에 도달하면 다음 동작이 발생합니다.

- 사용자 그룹이 더 이상 자동으로 생성되지 않습니다.
- 새 그룹을 생성하는 대신 사용자가 "새 사용자" 그룹에 할당됩니다.
- "시스템" > "이벤트" 목록에 경고 메시지가 표시됩니다.

[CA CEM 에서 사용자 및 그룹 관리](#) (페이지 319)를 참조하십시오.

introscope.enterprisemanager.transaction.discovery.max.nonidentifying.components

현재 정의된 트랜잭션에 대해 유지 대상으로 검색된 비식별 구성 요소의 최대 수로, 원래 비식별 구성 요소에 더해집니다.

옵션

숫자 값(양의 정수)

기본값

50

예

```
introscope.enterprisemanager.transaction.discovery.max.nonidentifying.component=60
```

참고

이 제한은 구성 요소가 매일 변경되는 GIF 파일인 경우와 같이 비식별 구성 요소가 자주 변경되는 트랜잭션에 중요합니다. 이 제한을 설정하면 트랜잭션에 대한 비식별 구성 요소(사용되지 않는 비식별 구성 요소일 수 있음)가 과도하게 저장되는 것을 방지할 수 있습니다.

새 비식별 구성 요소가 오래된 구성 요소를 대체할 때마다 "새 구성 요소 추가 제한을 초과했습니다"라는 CA CEM 이벤트가 기록됩니다.

비식별 구성 요소 자동 검색에 대한 일반 정보는 *CA APM 트랜잭션 정의 안내서*를 참조하십시오.

중요한 이벤트 임계값 설정

이러한 속성은 APM 상태 콘솔에 Enterprise Manager 건전성 모니터링에 대한 중요한 이벤트를 알리는 데 사용되는 제한을 정의합니다. 핫 구성이 가능하므로 핫 배포 중에 Enterprise Manager가 속성 파일을 검사할 때 값이 적용됩니다. 핫 배포는 약 60 초마다 한 번씩 발생합니다.

apm.events.thresholds.config.error

이 속성은 apm-events-thresholds-config.xml 파일의 구문 오류를 모니터링합니다. 오류를 찾으면 Enterprise Manager 는 다음 동작을 수행합니다.

- APM 상태 콘솔의 "중요한 이벤트" 테이블 뷰에 알립니다.
- 모든 apm-events-thresholds-config.xml 파일 클램프 및 중요한 이벤트 속성 값을 기본값으로 되돌립니다.

이 속성은 클러스터의 모든 수집기나 독립 실행형 Enterprise Manager 에 적용됩니다.

기본값

해당 없음. 이 속성은 알림 목적으로만 사용되며 수정할 수 없습니다.

introscope.enterprisemanager.cpu.usage

이 속성은 Enterprise Manager CPU 사용률이 중요한 이벤트로 간주되는 한도를 퍼센트(%)로 정의합니다. 이 임계값에 도달하거나 이 임계값이 초과되면 Enterprise Manager 가 APM 상태 콘솔의 "중요한 이벤트" 테이블 뷰에 알립니다.

이 속성은 "CPU Capacity (%)"(CPU 수용 능력(%)) 메트릭의 Enterprise Manager 모니터링을 기반으로 합니다. CPU 사용률이 60%보다 높으며 Enterprise Manager 리소스 문제를 나타냅니다. CPU 사용률 및 Enterprise Manager 성능에 대한 자세한 내용은 *CA APM 크기 조정 및 성능 안내서*를 참조하십시오.

이 속성은 클러스터의 모든 수집기나 독립 실행형 Enterprise Manager 에 적용됩니다.

기본값

60

예

```
introscope.enterprisemanager.cpu.usage=60
```

introscope.enterprisemanager.database.connectivity

이 속성은 Enterprise Manager 와 APM 데이터베이스 간의 연결을 모니터링합니다. 연결이 끊기면 Enterprise Manager 가 APM 상태 콘솔의 "중요한 이벤트" 테이블 뷰에 알립니다.

이 속성은 클러스터의 모든 수집기나 독립 실행형 Enterprise Manager 에 적용됩니다.

기본값

해당 없음. 이 속성은 알림 목적으로만 사용되며 수정할 수 없습니다.

introscope.enterprisemanager.harvest.cycle.diff

이 속성은 수집기와 MOM 의 하베스트 주기가 동기화되지 않을 수 있는 한도를 시간 조각 수로 정의합니다. 이 임계값에 도달하거나 이 임계값이 초과되면 Enterprise Manager 가 APM 상태 콘솔의 "중요한 이벤트" 테이블 뷰에 알립니다.

이 속성은 수집기와 MOM 의 메트릭 하베스트 주기 비교를 기반으로 합니다. 15 초의 각 하베스트 주기 동안 다음 동작이 발생합니다.

- 수집기가 에이전트 메트릭 데이터를 수집하고 집계합니다.
- 수집기에서 MOM 으로 메트릭 데이터가 전송됩니다.
- 수집기에서 MOM 으로 데이터가 집계됩니다.
- MOM 에서 Workstation 으로 데이터가 보고됩니다.

수집기는 수집기 하베스트 주기가 완료되기 전에는 MOM 에 데이터를 전송하지 않습니다. 수집기 하베스트 주기가 MOM 하베스트 주기 내에 완료되지 않으면 수집기와 MOM 의 데이터 집계가 동기화되지 않습니다.

수집기와 MOM 이 속성 값보다 많은 연속된 MOM 하베스트 주기 동안 동기화되지 않으면 CA APM 은 클러스터가 비정상이라고 간주합니다.

기본값

4

예

```
introscope.enterprisemanager.harvest.cycle.diff=4
```

참고

이 속성은 MOM 에서만 구성하십시오.

introscope.enterprisemanager.harvest.duration

이 속성은 Enterprise Manager 하베스트 기간이 중요한 이벤트로 간주되는 한도(밀리초)를 정의합니다. 이 임계값에 도달하거나 이 임계값이 초과되면 Enterprise Manager 가 APM 상태 콘솔의 "중요한 이벤트" 테이블 뷰에 알립니다.

이 속성은 "하베스트 기간(ms)" 메트릭의 Enterprise Manager 모니터링을 기반으로 합니다. 3500 밀리초보다 긴 하베스트 기간은 Enterprise Manager 리소스 문제를 나타냅니다. 하베스트 기간 및 Enterprise Manager 성능에 대한 자세한 내용은 *CA APM 크기 조정 및 성능 안내서*를 참조하십시오.

이 속성은 클러스터의 모든 수집기나 독립 실행형 Enterprise Manager 에 적용됩니다.

기본값

3500

예

```
introscope.enterprisemanager.harvest.duration=3500
```

introscope.enterprisemanager.smartstor.duration

이 속성은 Enterprise Manager SmartStor 기간이 중요한 이벤트로 간주되는 한도(밀리초)를 정의합니다. 이 임계값에 도달하거나 이 임계값이 초과되면 Enterprise Manager 가 APM 상태 콘솔의 "중요한 이벤트" 테이블 뷰에 알립니다.

이 속성은 "Smartstor 기간(ms)" 메트릭의 Enterprise Manager 모니터링을 기반으로 합니다. 3500 밀리초보다 긴 SmartStor 기간은 Enterprise Manager 리소스 문제를 나타냅니다. SmartStor 기간 및 Enterprise Manager 성능에 대한 자세한 내용은 *CA APM 크기 조정 및 성능 안내서*를 참조하십시오.

이 속성은 클러스터의 모든 수집기나 독립 실행형 Enterprise Manager 에 적용됩니다.

기본값

3500

예

```
introscope.enterprisemanager.smarstor.duration=3500
```

ResourceMetricMap.properties

다양한 에이전트의 리소스 메트릭 범주가 Workstation 에서 보고됩니다. 리소스 메트릭 범주는 미리 정의되어 있습니다. 미리 정의된 리소스 메트릭 그룹을 추가하거나 삭제할 수 없는 경우 관리자 권한이 있으면 각 리소스 메트릭 그룹에 대해 보고되는 데이터를 지정하는 리소스 메트릭 매핑을 추가, 변경 또는 제거할 수 있습니다.

리소스 메트릭 범주에 리소스 메트릭을 매핑하려면

1. 에이전트에서 JMX 보고가 사용하도록 설정되었는지 확인합니다. 자세한 내용은 *CA APM Java Agent 구현 안내서*의 *Enabling JMX Reporting*(JMX 보고를 사용하도록 설정)을 참조하십시오.
2. 리소스 메트릭 범주에 리소스 메트릭을 매핑하여 MOM 의 `<EM_Home>/Config` 디렉터리에 있는 *ResourceMetricMap.properties* 파일을 편집합니다. 리소스 메트릭 매핑에 대한 자세한 내용은 사용 중인 응용 프로그램 서버 설명서를 참조하십시오.
 - a. `<categoryName>.path<recordID>:<agentMetricPath>` 형식을 사용하여 메트릭 항목을 추가합니다. 예:


```
threads.used.path.1=Tomcat|ThreadPool|getCurrentThreadsBusy.path.1=CPU:Processor Count
```

 여기서 *memory.utilization* 은 메트릭 이름이고 *CPU:Processor Count* 는 기본 메트릭 경로입니다.
 - b. 숫자를 사용하여 증분 레코드 ID 메트릭을 추가합니다. 예:


```
cpu.utilization.path.1=Non Existent metric
cpu.utilization.path.2=CPU|Processor 0:Utilization % (aggregate)
```

 동일한 메트릭 그룹에 여러 경로를 사용하여 동일한 이름으로 다양한 경로의 메트릭을 구성할 수 있습니다. 이렇게 하면 프론트엔드가 배포된 다양한 응용 프로그램 서버에서 동일한 메트릭을 가져오는 등의 작업을 수행할 수 있습니다.

3. MOM 과 수집기를 다시 시작합니다.

새로 매핑된 리소스 메트릭 값이 Workstation 에서 보고됩니다.

동일한 메트릭의 여러 인스턴스에 대해 구성된 ResourceMetricMap.properties 파일의 예

다음은 "사용 중인 스레드" 메트릭의 여러 인스턴스가 클러스터에 있는 수집기 3 개를 가리키도록 구성된 ResourceMetricMap.properties 파일 섹션입니다.

#CPU Utilization

cpu.utilization.path.1=CPU:Utilization % (process)

#Time Spent in GC

memory.utilization.path.1=GC Monitor|Percentage of Time Spent in GC during last 15 minutes

#Threads in Use

threads.used.path.1=WebSpherePMI|threadPoolModule|WebContainer:ActiveCount

threads.used.path.2=WebLogic|JMX Aggregate|Thread Pool:Waiting Request Count

threads.used.path.3=Tomcat|ThreadPool|default thread pool:getCurrentThreadsBusy

#JDBC Connections in Use

connections.used.path.1=WebSpherePMI|connectionPoolModule:WaitingThreadCount

connections.used.path.2=WebLogic|JMX Aggregate|JDBC Connection Pool:Waiting Thread Count

다음 리소스 메트릭 범주에 리소스 메트릭을 매핑할 수 있습니다.

[CPU 사용률](#) (페이지 513)

[GC 에서 소비된 시간](#) (페이지 513)

[사용 중인 스레드](#) (페이지 513)

[사용 중인 JDBC 연결](#) (페이지 513)

CPU 사용률

CPU 사용률은 사용 중인 CPU 크기를 측정합니다.

매핑 예제:

```
cpu.utilization.path.1=CPU:Utilization % (process)
cpu.utilization.path.2=Some other metrics path
```

GC 에서 소비된 시간

GC 에서 소비된 시간은 가비지 수집기에서 소비된 시간을 측정하며 이를 통해 작업량이 응용 프로그램 성능에 중요한지 여부를 파악할 수 있습니다.

매핑 예제:

```
memory.utilization.path.1=memory utilization path
```

사용 중인 스레드

사용 중인 스레드는 사용 중인 스레드 수를 측정합니다.

매핑 예제:

```
threads.used.path.1=threads used path
```

사용 중인 JDBC 연결

사용 중인 JDBC 연결은 활성 상태의 Java Database Connectivity 인스턴스 수를 측정합니다.

매핑 예제:

```
connections.used.path.1=connections used path
```

Catalyst.properties

Catalyst 속성을 사용하면 CA Catalyst 데이터를 로드하고 Catalyst 데이터에서 보고된 경고를 필터링하도록 CA APM 을 구성할 수 있습니다.

추가 정보:

- [catalyst.host](#) (페이지 514)
- [catalyst.protocol](#) (페이지 515)
- [catalyst.port](#) (페이지 515)
- [catalyst.login](#) (페이지 515)
- [catalyst.password](#) (페이지 515)
- [catalyst.rest.endpoint](#) (페이지 516)
- [catalyst.rest.alerts.pollingperiodsec](#) (페이지 516)
- [catalyst.rest.virtualhosts.pollingperiodsec](#) (페이지 516)
- [catalyst.product.url](#) (페이지 517)
- [catalyst.alert.filter.total](#) (페이지 517)
- [catalyst.alert.filter.time](#) (페이지 517)
- [catalyst.alert.filter.products](#) (페이지 518)
- [catalyst.alert.filter.types](#) (페이지 518)
- [catalyst.alert.filter.severities](#) (페이지 519)
- [catalyst.rest.maxFailures](#) (페이지 519)
- [catalyst.rest.maxAlertsPerPage](#) (페이지 520)
- [catalyst.rest.alerts.threads](#) (페이지 520)
- [catalyst.rest.virtualhosts.threads](#) (페이지 520)
- [catalyst.entity.cache.size](#) (페이지 521)
- [catalyst.entity.cache.expirationsec](#) (페이지 521)
- [catalyst.database.alerts.enabled](#) (페이지 521)
- [catalyst.database.map.name](#) (페이지 522)
- [Catalyst 데이터를 로드하도록 APM 구성](#) (페이지 257)
- [CA Catalyst 데이터를 로드하도록 CA APM 구성](#) (페이지 258)
- [CatalystPolicy.xml 파일 구성](#) (페이지 259)

catalyst.host

CA Catalyst RESTful API 호스트 이름을 사용하여 이 필수 속성을 설정하십시오. 이 행의 주석 처리를 제거한 후 CA Catalyst 에 값을 추가하십시오.

기본값

이 속성은 기본적으로 사용하지 않도록 설정됩니다.

catalyst.protocol

CA Catalyst 웹 액세스에 사용되는 프로토콜을 사용하여 이 필수 속성을 설정하십시오.

예

```
catalyst.protocol = http
```

catalyst.port

CA Catalyst 웹 액세스에 사용되는 포트 번호를 사용하여 이 필수 속성을 설정하십시오.

예

```
catalyst.port = 7070
```

catalyst.login

CA Catalyst 로그인에 사용되는 사용자 이름을 사용하여 이 필수 속성을 설정하십시오.

예

```
catalyst.login =<enter your CA Catalyst user name>
```

catalyst.password

CA Catalyst 로그인에 사용되는 암호를 사용하여 이 필수 속성을 설정하십시오.

예

```
catalyst.password =<enter your CA Catalyst password>
```

catalyst.rest.entrpoint

CA Catalyst RESTful API 진입점의 URL 컨텍스트를 사용하여 이 필수 속성을 설정하십시오.

예

```
catalyst.rest.entrpoint = /ssaweb/search
```

catalyst.rest.alerts.pollingperiodsec

CA Catalyst 를 검사하여 새 경고가 있는지 확인하는 빈도를 결정하려면 이 선택적 폴링 속성을 설정하십시오.

기본값

15(초)

예

```
catalyst.rest.alerts.pollingperiodsec = 15
```

catalyst.rest.virtualhosts.pollingperiodsec

CA Catalyst 를 검사하여 가상 호스트 업데이트가 있는지 확인하는 빈도를 결정하려면 이 선택적 속성을 설정하십시오.

기본값

60(초)

예

```
catalyst.rest.virtualhosts.pollingperiodsec = 60
```

catalyst.product.url

영향을 주는 제품의 기본 URL 주소를 사용하여 이 속성을 설정하십시오.

예

```
# Spectrum
# catalyst.product.url = CA:00005->http[s]://<host>[:CA
Portal]/spectrum/oneclick.jnlp?explorer={Entity.MdrElementID}
# eHealth
# catalyst.product.url = CA:00002->http[s]://<host>[:CA Portal]/{Alert.UrlParams}
# Insight
# catalyst.product.url = CA:00048->http[s]://<host>[:CA Portal]
# NetQoS
# catalyst.product.url = CA:00034->http[s]://<host>[:CA
Portal]/npc/Default.aspx?pg={Alert.UrlParams}
```

catalyst.alert.filter.total

Workstation 에 로드할 최대 CA Catalyst 경고 수를 설정하려면 이 선택적 속성을 설정하십시오.

기본값

250

예

```
catalyst.alert.filter.total = 250
```

catalyst.alert.filter.time

CA Catalyst 경고가 Workstation 에 나타나는 기간을 설정하려면 이 선택적 속성을 설정하십시오.

기본값

72(시간)

예

```
catalyst.alert.filter.time = 72
```

catalyst.alert.filter.products

지정된 제품에 대한 경고를 모두 제외하려면 이 선택적 속성을 설정하십시오.

예

catalyst.alert.filter.products = CA:00030

catalyst.alert.filter.types

Workstation 에 나타날 대상에서 제외할 CA Catalyst 경고 유형을 식별하려면 이 선택적 속성을 설정하십시오. 여러 경고 유형을 지정하는 경우 쉼표를 사용하여 구분하십시오.

옵션

- Risk
- Risk-Capacity
- Risk-Change
- Risk-Fault
- Risk-Security
- Risk-Performance
- Risk-Root Cause
- Quality
- Compliance
- Cost

예

catalyst.alert.filter.types = Risk-Security,Compliance,Cost

catalyst.alert.filter.severities

Workstation 에 나타날 대상에서 제외해야 하는 CA Catalyst 경고 심각도를 결정하려면 이 선택적 속성을 설정하십시오. 여러 값을 설정하려면 두 심각도 값 사이에 하이픈(-)을 사용하여 범위를 정의하거나 심각도 값 오른쪽이나 왼쪽에 하이픈을 사용하여 열린 범위를 정의하거나 쉼표로 구분된 범위를 정의하십시오.

기본값

알 수 없음

옵션

이 속성에 대해 설정할 수 있는 옵션은 다음과 같으며 이러한 옵션을 사용하여 열린 범위를 사용할 수 있습니다.

- Normal(정상)
- Informational(정보)
- Unknown(알 수 없음)
- Minor(2 순위)
- Major(1 순위)
- Critical(중요)
- Fatal(치명적)

예

catalyst.alert.filter.severities = -Unknown

catalyst.rest.maxFailures

폴링을 취소하기 전에 허용할 최대 CA Catalyst 실패 수를 지정하려면 이 선택적 속성을 설정하십시오.

기본값

10

예

catalyst.rest.maxFailures = 10

catalyst.rest.maxAlertsPerPage

단일 REST 쿼리에서 반환할 최대 CA Catalyst 경고 수를 지정하려면 이 선택적 속성을 설정하십시오.

기본값

250

예

catalyst.rest.maxAlertsPerPage = 250

catalyst.rest.alerts.threads

경고에 사용할 최대 스레드 수를 지정하려면 이 선택적 속성을 설정하십시오.

기본값

2

예

catalyst.rest.alerts.threads = 2

catalyst.rest.virtualhosts.threads

가상 호스트에 사용할 최대 스레드 수를 지정하려면 이 선택적 풀링 속성을 설정하십시오.

기본값

1

예

catalyst.rest.virtualhosts.threads = 1

catalyst.entity.cache.size

CA Catalyst 에 사용할 엔터티 메모리 내 캐시 크기를 지정하려면 이 선택적 속성을 설정하십시오.

기본값

3000(메가바이트)

예

```
catalyst.entity.cache.size = 3000
```

catalyst.entity.cache.expirationsec

엔터티 캐시 만료 시간(초)을 지정하려면 이 선택적 속성을 설정하십시오.

기본값

36000(초)

예

```
catalyst.entity.cache.expirationsec = 36000
```

catalyst.database.alerts.enabled

CA Catalyst 데이터베이스 경고를 Workstation 에 보내려면 이 속성을 설정하십시오. 기본적으로 CA Catalyst 데이터베이스 경고가 Workstation 에 전송됩니다. CA Catalyst 데이터베이스 경고 보내기를 중지하려면 설정을 *false* 로 변경하십시오.

기본값

true

기본값

```
catalyst.database.alerts.enabled=true
```

catalyst.database.map.name

데이터베이스 연결 문자열을 CA Catalyst 데이터베이스 매개 변수에 매핑하는 파일 위치를 지정하려면 이 선택적 속성을 설정하십시오. 즉시 사용 가능한 매핑이 제대로 작동하지 않는 경우에만 이 속성을 설정하십시오.

Microsoft SQL 데이터베이스 예제:

1. <Agent_Home>/wily/core/config 디렉터리에 있는 *IntroscopeAgent.profile* 파일을 열고 다음 속성을 true 로 설정합니다.
`catalyst.database.map.name = CatalystDatabaseMap.txt`
2. <EM_Home>/config 디렉터리에 있는 *CatalystDatabaseMap.txt* 파일을 열고 다음과 같이 수식을 정의합니다.
 - a. 수식의 왼쪽 부분은 JDBC URL 일치에 대한 전체 Java 정규식을 나타냅니다.
 - b. 파이프(|), 화살표(=>), 등호(=), 이중 등호(==) 등의 수식 구분 기호는 수식의 왼쪽 부분과 오른쪽 부분을 구분하며 레코드 구분 기호로 사용될 수 있습니다.
 - c. 수식의 오른쪽 부분에는 서버 이름, 데이터베이스 이름, 데이터베이스 인스턴스 이름 등의 데이터베이스 매개 변수가 나열됩니다.

예:

```
^jdbc:sqlserver.+1433.* = deviaat011|apmtest|default
^jdbc:sqlserver.+1533.* = deviaat011|apmtest|testinstance
```

EMservice.conf

<EM_Home>\bin 에 있는 *EMService.conf* 파일에는 Enterprise Manager 가 Windows 서비스로 실행될 때 사용되는 설정이 포함됩니다.

참고: 이러한 속성을 구성하기 전에 Enterprise Manager 서비스 등록을 취소해야 합니다. 속성을 구성한 후 Enterprise Manager 서비스를 다시 등록하십시오.

wrapper.java.command

Java 응용 프로그램 래퍼 명령입니다.

기본값

`jre\bin\java.exe`

wrapper.java.mainclass

Java 기본 클래스 래퍼 명령입니다.

기본값

`org.tanukisoftware.wrapper.WrapperSimpleApp`

wrapper.java.classpath.x

`wrapper.jar` 를 포함하는 Java 클래스 경로입니다. 클래스 경로 요소는 다음과 같이 순차적으로 추가해야 합니다.

- `wrapper.java.classpath.1=./lib/ServiceWrapper.jar`
- `wrapper.java.classpath.2=./launcher.jar`
- `wrapper.java.classpath.3=`

wrapper.java.library.path.1

Java 라이브러리 경로는 `Wrapper.DLL` 또는 `libwrapper.so` 의 위치입니다.

기본값

`./lib`

wrapper.java.additional.x=

64 비트 Windows 에만 적용되는 추가 Java 매개 변수입니다.

첫 번째 추가 매개 변수는 `-Xrs` 여야 합니다. 그 다음부터 필요에 따라 매개 변수를 추가할 수 있습니다. 예:

- `wrapper.java.additional.1=-Xrs`
- `wrapper.java.additional.1=-Djava.awt.headless=false`
- `wrapper.java.additional.2=-showversion`
- `wrapper.java.additional.3=-XX:+UseConcMarkSweepGC`
- `wrapper.java.additional.4=-XX:+UseParNewGC`

기본값

`-Xrs`

wrapper.java.initmemory

래퍼의 초기 메모리 크기(메가바이트)입니다.

기본값

128

wrapper.java.maxmemory

래퍼의 최대 메모리 크기(메가바이트)입니다.

기본값

512

wrapper.app.parameter.x

응용 프로그램 매개 변수입니다. 필요에 따라 매개 변수를 추가할 수 있습니다. 예:

- `wrapper.app.parameter.1=org.eclipse.core.launcher.Main`
- `wrapper.app.parameter.2=-consolelog`
- `wrapper.app.parameter.3=-noExit`
- `wrapper.app.parameter.4=-product`
- `wrapper.app.parameter.5=com.wily.introscope.em.product`
- `wrapper.app.parameter.6=-install`
- `wrapper.app.parameter.7=./product/enterprisemanager`
- `wrapper.app.parameter.8=-configuration`
- `wrapper.app.parameter.9=./product/enterprisemanager/configuration`

wrapper.startup.timeout

래퍼가 JVM 프로세스를 시작하는 시간과 래퍼의 JVM 측이 응용 프로그램이 시작되었다고 응답하는 시간 사이에 허용할 간격(초)입니다 값으로 0 을 입력하면 시스템이 시간 초과되지 않습니다.

기본값

30(초)

wrapper.console.format

콘솔의 출력 형식입니다.

기본값

PM

wrapper.console.loglevel

콘솔 출력의 로그 수준입니다.

기본값

INFO

wrapper.logfile

래퍼 출력 로깅에 사용되는 로그 파일의 이름과 위치입니다.

기본값

./logs/EMService.log

wrapper.logfile.format

로그 파일의 출력 형식입니다.

기본값

LPTM

wrapper.logfile.loglevel

로그 파일 출력의 로그 수준입니다.

기본값

INFO

wrapper.logfile.maxsize

로그가 롤링되기 전에 로그 파일이 증가하도록 허용할 최대 크기입니다. 크기는 바이트 단위로 지정됩니다. 기본값인 0 을 그대로 사용하면 로그 롤링이 사용되지 않도록 설정됩니다. *k(kb)* 또는 *m(mb)* 접두사로 줄여 쓸 수 있습니다. 예를 들어 *10m = 10 메가바이트*와 같습니다.

기본값

0

wrapper.logfile.maxfiles

오래된 파일이 삭제되기 전에 허용될 롤링된 로그 파일의 최대 수입니다. 기본값인 0 을 그대로 사용하면 제한이 없습니다.

기본값

0

wrapper.syslog.loglevel

시스템 및 이벤트 로그 출력의 로그 수준입니다.

기본값

NONE

참고

이 구성 파일을 사용하는 응용 프로그램이 서비스로 설치된 경우에는 다음 *ntservice* 속성을 수정하지 마십시오. 이 섹션을 수정하기 전에 서비스를 제거하십시오. 수정한 후 서비스를 다시 설치할 수 있습니다.

wrapper.ntservice.name

서비스의 이름입니다.

기본값

IScopeEM

wrapper.nts.service.displayname

서비스의 표시 이름입니다.

기본값

Introscope Enterprise Manager

wrapper.nts.service.description

서비스에 대한 설명입니다.

기본값

Introscope Enterprise Manager

wrapper.nts.service.dependency.x

서비스 종속성입니다. 필요에 따라 1 부터 시작하여 종속성을 추가하십시오.
예:

- *wrapper.nts.service.dependency.1=*
- *wrapper.nts.service.dependency.2=*
- *wrapper.nts.service.dependency.3=*

wrapper.nts.service.starttype

서비스가 설치된 모드입니다. 설정으로는 *AUTO_START* 또는 *DEMAND_START* 가 있습니다.

기본값

AUTO_START

wrapper.ntservice.interactive

이 값을 *true* 로 설정하면 서비스와 데스크톱의 상호 작용이 시작됩니다.

기본값

false

Introscope Enterprise Manager.lax

Introscope Enterprise Manager.lax 파일은 <EM_Home> 디렉터리에 있습니다. Enterprise Manager 의 런타임 동작이 이 파일에서 정의한 속성으로 제어됩니다.

lax.application.name

Enterprise Manager 실행 파일의 기본 이름입니다.

경고! 편집하지 마십시오.

기본값

Introscope Enterprise Manager.exe

lax.class.path

이 응용 프로그램을 실행하는 데 필요한 Java 클래스 경로입니다.

JDBC 드라이버와 라이선스를 추가할 수 있습니다.

콜론(Mac OS/UNIX)이나 세미콜론(Windows)으로 구분할 수 있습니다.

예

```
lax.class.path=launcher.jar;lax.jar
```

기본값

<blank>

lax.command.line.args

기본 메서드에 전달됩니다. 이 값을 입력하는 경우 인수를 따옴표로 묶고 공백으로 구분해야 합니다. 예:

```
lax.command.line.args=$CMD_LINE_ARGUMENTS$ -consolelog -noExit -product  
com.wily.introscope.em.product -install ".\product\enterprisemanager"  
-configuration ".\product\enterprisemanager\configuration"
```

기본값

<blank>

lax.dir

LaunchAnywhere 의 네이티브 시작 관리자를 소유하는 디렉터리의 경로입니다.

기본값

<blank>

lax.main.class

응용 프로그램의 기본 메서드를 포함하는 클래스입니다.

예

```
lax.main.class=org.eclipse.core.launcher.Main
```

기본값

main

lax.main.method

LaunchAnywhere Java 시작 관리자의 기본 메서드입니다. 이 속성의 기본값(*lax.nl.java.launcher.main.method=main*)을 조정하면 안 됩니다.

기본값

main

`lax.nl.current.vm`

이 속성은 다음에 Enterprise Manager 가 시작될 때 사용되는 가상 컴퓨터를 나타냅니다. 설치된 JRE 를 사용하도록 설정할 수 있습니다. JVM 버전 요구 사항은 *CA APM 설치 및 업그레이드 안내서*를 참조하십시오.

예

번들로 제공된 JVM 을 사용하도록 이 속성을 구성하는 경우 다음과 같습니다.

```
lax.nl.current.vm=jre\bin\java.exe
```

기본값

기본값은 운영 체제에 따라 다릅니다.

`lax.nl.java.launcher.main.class`

LaunchAnywhere Java 시작 관리자의 기본 클래스입니다. 이 속성의 기본값(`lax.nl.java.launcher.main.class=com.zerog.lax.LAX`)을 조정하면 안 됩니다.

기본값

```
com.zerog.lax.LAX
```

`lax.nl.java.launcher.main.method`

LaunchAnywhere Java 시작 관리자의 기본 메서드입니다. 이 속성의 기본값(`lax.nl.java.launcher.main.method=main`)을 조정하면 안 됩니다.

기본값

```
main
```

lax.nl.java.option.additional

힙 크기 등의 선택적 Java 인수입니다.

예

```
lax.nl.java.option.additional=-Xms512m -Xmx1024m  
-Djava.awt.headless=false -XX:MaxPermSize=256m  
-XX:+UseConcMarkSweepGC -XX:+UseParNewGC  
-XX:CMSInitiatingOccupancyFraction=50 -Dosgi.clean=false
```

다음 스위치는 32 비트 Sun JVM 에 권장됩니다.

```
-showversion -XX:+UseConcMarkSweepGC -XX:+UseParNewGC  
-XX:CMSInitiatingOccupancyFraction=50 -XX:MaxPermSize=256m
```

예:

```
lax.nl.java.option.additional=-Xms512m -Xmx1024m  
-Djava.awt.headless=false -XX:MaxPermSize=256m  
-showversion -XX:+UseConcMarkSweepGC -XX:+UseParNewGC  
-XX:CMSInitiatingOccupancyFraction=50
```

참고: -showversion -XX:+UseConcMarkSweepGC -XX:+UseParNewGC 스위치는 32 비트 Sun JVM 에만 사용됩니다.

64 비트 플랫폼을 사용하는 경우에는 -Xss 스위치를 512K 로 설정합니다.

예:

```
lax.nl.java.option.additional=-Xms512m -Xmx1024m  
-Djava.awt.headless=false -XX:MaxPermSize=256m  
-Dmail.mime.charset=UTF-8  
-Dorg.owasp.esapi.resources=./config/esapi -Xss512k
```

기본값

<blank>

lax.nl.message.vm.not.loaded

lax.nl.valid.vm.list 에 있는 가상 컴퓨터를 찾을 수 없는 경우 사용자 대화 상자에 표시되는 메시지입니다. 이 속성은 *InstallAnywhere* 시작 관리자 내에서만 사용됩니다. Introscope 에는 별개의 Java 요구 사항이 있습니다. JVM 요구 사항은 *CA APM 설치 및 업그레이드 안내서*를 참조하십시오.

The *lax.nl.message.vm.not.loaded=LaunchAnywhere* either could not find a Java VM, or the Java VM on this system is too old. LaunchAnywhere requires a Java 2 VM in order to launch Introscope.

lax.nl.valid.vm.list

공백이나 쉼표로 구분된 하나 이상의 [*ALL JDK JRE J1 J2 JRE_J1 JDK_J1 JRE_J2 JDK_J2 MSJ*]를 포함하는 문자열입니다. 네이티브 시작 관리자가 현재 가상 컴퓨터를 찾을 수 없으면 이 목록에서 값을 검색합니다(*lax.nl.valid.vm.list=J2*).

기본값

J2

lax.nl.win32.microsoftvm.min.version

이 시작 관리자가 실행될 Microsoft 가상 컴퓨터의 최소 버전입니다. 예:

lax.nl.win32.microsoftvm.min.version=2750

기본값

2750

lax.root.install.dir

installdir 매직 폴더의 경로입니다. 예:

lax.root.install.dir=

기본값

<blank>

lax.stderr.redirect

표준 오류 출력입니다.
다음과 같이 설정하십시오.

- 공백 - 출력이 없습니다.
- *console* - 콘솔 창으로 보냅니다.
- 임의의 파일 경로 - 파일에 저장합니다.

기본값

console

lax.stdin.redirect

다음과 같이 설정하십시오.

- 공백 - 출력이 없습니다.
- *console* - 콘솔 창으로 보냅니다.
- 임의의 파일 경로 - 파일에 저장합니다.

참고

UNIX 플랫폼에 대해 `nohup` 모드로 Enterprise Manager 를 실행 중인 경우 이 설정을 변경하지 마십시오. Enterprise Manager 가 시작되지 않을 수 있습니다.

이 속성을 공백으로 설정해야 하는 로컬 요구 사항이 있는 경우에는 [introscope.enterprisemanager.disableInteractiveMode](#) (페이지 442)를 true 로 설정해야 합니다.

기본값

console

lax.stdout.redirect

표준 출력입니다.

다음과 같이 설정하십시오.

- 공백 - 출력이 없습니다.
- `console` - 콘솔 창으로 보냅니다.
- 임의의 파일 경로 - 파일에 저장합니다.

기본값

console

lax.user.dir

이 속성을 비워 두면 네이티브 시작 관리자가 사용자 디렉터리를 설정하기 위한 플랫폼 기본 동작을 변경하지 않습니다.

이 속성을 상대 또는 절대 경로로 설정하여 이를 무시할 수 있습니다. 이때 상대 경로는 시작 관리자를 기준으로 합니다.

예

`lax.user.dir=.`

기본값

<blank>

lax.version

속성 파일을 만든 LaunchAnywhere 의 버전입니다. 예를 들어 `lax.version=<VersionNumber>`와 같습니다.

기본값

10.0

IntroscopeWorkstation.properties

다양한 Workstation 동작이 이 파일에 있는 속성으로 제어됩니다.

log4j.logger.Workstation

Workstation 로그의 로깅 세부 정보 양과 출력 위치를 제어합니다.

세부화 수준 값은 다음일 수 있습니다.

- *FATAL*
- *WARN*
- *INFO*
- *VERBOSE#com.wily.util.feedback.Log4JSeverityLevel*
이 값은 로깅되는 세부 정보의 수준을 높입니다.
- *DEBUG*
- *TRACE*

대상 값은 다음일 수 있습니다.

- *console*
- *logfile*

기본값

INFO, console

log4j.appender.logfile.File

Workstation 로그 파일의 이름과 위치입니다.

기본값

IntroscopeWorkstation.log

introscope.workstation.graph.antialiased

그래프에 있는 선과 기호의 안티앨리어싱을 제어합니다. 이 값을 *false* 로 설정하면 안티앨리어싱이 사용되지 않도록 설정됩니다.

기본값

true

transport.http.proxy.host

Workstation 이 HTTP 를 통해 터널링 중인 호스트를 지정하는 HTTP 터널링 프록시 서버 속성입니다. 이 메서드를 선택한 경우에는 프록시 서버를 통해 Enterprise Manager 에 연결해야 합니다(정방향 프록시). 지정된 호스트와 포트에서 프록시 서버에 도달할 수 없는 경우 Workstation 은 연결 시도 실패 전에 Enterprise Manager 에 대한 직접 HTTP 터널링 연결을 시도합니다.

기본값

<blank>

transport.http.proxy.port

Workstation 이 HTTP 를 통해 터널링 중인 포트를 지정하는 HTTP 터널링 프록시 서버 속성입니다. 이 메서드를 선택한 경우에는 프록시 서버를 통해 Enterprise Manager 에 연결해야 합니다(정방향 프록시). 지정된 호스트와 포트에서 프록시 서버에 도달할 수 없는 경우 Workstation 은 연결 시도 실패 전에 Enterprise Manager 에 대한 직접 HTTP 터널링 연결을 시도합니다.

기본값

<blank>

transport.http.proxy.username

프록시 서버 인증이 필요한 경우에만 사용자 이름이 적용됩니다. 이때 사용자가 사용자 이름을 나타내는 값을 입력합니다.

기본값

<blank>

transport.http.proxy.password

프록시 서버 인증이 필요한 경우에만 사용자 이름이 적용됩니다. 이때 암호를 나타내는 값을 입력하는데, 이 암호는 사용자가 입력해야 합니다.

기본값

<blank>

transport.tcp.truststore

SSL 을 구성하는 경우 이 선택적 속성은 신뢰할 수 있는 Enterprise Manager 인증서를 포함하는 신뢰 저장소의 위치를 지정합니다. 이 값은 절대 경로이거나 Workstation 의 작업 디렉터리를 기준으로 한 상대 경로입니다.

Windows 에서는 백슬래시를 이스케이프해야 합니다. 예:

```
transport.tcp.truststore=C:\\Introscope\\config\\internal\\server\\keystore
```

지정된 신뢰 저장소가 없으면 Workstation 이 모든 인증서를 신뢰합니다.

기본값

<blank>

transport.tcp.trustpassword

신뢰 저장소의 암호입니다.

기본값

password

transport.tcp.truststore

Workstation 의 인증서를 포함하는 키 저장소의 위치입니다. 절대 경로이거나 Workstation 의 작업 디렉터리를 기준으로 한 상대 경로입니다. Windows 에서는 백슬래시를 이스케이프해야 합니다.

예

```
..\\Introscope\\config\\internal\\server\\keystore
```

transport.tcp.keystore

키 저장소의 위치에 대한 속성입니다. Enterprise Manager 가 클라이언트 인증을 요구하는 경우에만 필요합니다.

기본값

internal/server/keystore

transport.tcp.keypassword

키 저장소의 암호입니다.

기본값

password

transport.tcp.ciphersuites

쉽게 구분된 암호 그룹 목록을 사용하여 암호 그룹이 사용되도록 설정하려면 이 속성을 설정하십시오. 이 속성을 지정하지 않으면 사용되도록 설정된 기본 암호 그룹이 사용됩니다.

기본값

<blank>

참고

이 파일에 다음 속성이 포함된 경우에는 일반적으로 해당 속성을 수정하면 안 됩니다.

- log4j.additivity.Workstation=false
- log4j.appender.console=com.wily.org.apache.log4j.ConsoleAppender
- log4j.appender.console.layout=com.wily.org.apache.log4j.PatternLayout
- log4j.appender.console.layout.ConversionPattern=%d{M/dd/yy hh:mm:ss a z} [%-3p] [%c] %m%n
- log4j.appender.logfile=com.wily.org.apache.log4j.RollingFileAppender
- log4j.appender.logfile.layout=com.wily.org.apache.log4j.PatternLayout
- log4j.appender.logfile.layout.ConversionPattern=%d{M/dd/yy hh:mm:ss a z} [%-3p] [%c] %m%n
- log4j.appender.logfile.MaxBackupIndex=4
- log4j.appender.logfile.MaxFileSize=200MB

Introscope Workstation.lax

다양한 Workstation 동작이 이 파일에서 정의한 속성으로 제어됩니다.

lax.application.name

중요! 이 실행 파일의 기본 이름을 편집하지 않는 것이 중요합니다.

기본값

Introscope Workstation.exe

lax.class.path

이 응용 프로그램을 실행하는 데 필요한 Java 클래스 경로입니다. 콜론(Mac OS/UNIX)이나 세미콜론(Windows)으로 구분할 수 있습니다.

기본값

launcher.jar;lax.jar

lax.command.line.args

기본 메시드에 전달될 명령줄 인수입니다. 이 속성을 사용하여 Workstation 시작 시 로그인 화면을 우회하면서 Workstation 에 로그인 값을 제공할 수 있습니다.

기본값

\$CMD_LINE_ARGUMENTS\$

lax.dir

LaunchAnywhere 의 네이티브 시작 관리자를 보유하는 디렉터리의 경로입니다.

기본값

<blank>

lax.main.class

응용 프로그램의 기본 메시지를 포함하는 클래스입니다.

기본값

org.eclipse.core.launcher.Main

lax.main.method

호출할 기본 클래스에 있는 메서드입니다.

기본값

main

lax.nl.current.vm

다음에 Workstation 이 시작될 때 사용할 VM 입니다. 설치된 JRE 버전으로 설정할 수 있습니다. JVM 버전 요구 사항은 *CA APM 설치 및 업그레이드 안내서*를 참조하십시오.

기본값

운영 체제에 따라 다릅니다.

lax.nl.java.launcher.main.class

참고

LaunchAnywhere Java 시작 관리자의 기본 클래스이므로 이 속성을 수정하지 않는 것이 중요합니다.

기본값

com.zerog.lax.LAX

lax.nl.java.launcher.main.method

참고

LaunchAnywhere Java 시작 관리자의 기본 메서드이므로 이 속성을 수정하지 않는 것이 중요합니다.

기본값

main

lax.nl.java.option.additional

JVM 에 대한 기타 옵션 설정입니다.

초기의 최소 및 최대 힙 크기입니다.

기본값

```
-client -Xms64m -Xmx256m -Dsun.java2d.noddraw=true
```

lax.nl.message.vm.not.loaded

lax.nl.valid.vm.list 에 있는 가상 컴퓨터를 찾을 수 없는 경우 사용자 대화 상자에 표시되는 메시지입니다.

참고

이 속성은 InstallAnywhere 시작 관리자 내에서만 사용됩니다.

Introscope 에는 별개의 Java 요구 사항이 있습니다. 자세한 내용은 *CA APM 설치 및 업그레이드 안내서의 시스템 요구 사항*을 참조하십시오.

기본값

LaunchAnywhere either could not find a Java VM, or the Java VM on this system is too old. LaunchAnywhere requires a Java 2 VM in order to launch Introscope.

lax.nl.valid.vm.list

공백이나 쉼표로 구분된 하나 이상의 [ALL JDK JRE J1 J2 JRE_J1 JDK_J1 JRE_J2 JDK_J2 MSJ]를 포함하는 문자열입니다. 네이티브 시작 관리자가 현재 가상 컴퓨터를 찾을 수 없으면 이 목록에 정의된 가상 컴퓨터를 검색합니다.

기본값

J2

lax.nl.win32.microsoftvm.min.version

이 버전의 Microsoft 가상 컴퓨터 시작 관리자가 실행될 최소 버전입니다.

기본값

2750

lax.root.install.dir

installdir 매직 폴더의 경로입니다.

기본값

<blank>

lax.stderr.redirect

표준 오류 출력입니다.

가능한 값:

- <blank> - 출력 없음
- *console* - 출력을 콘솔 창에 보냅니다.
- <path_to_a_file> - 출력을 지정된 파일에 저장합니다.

기본값

<blank>

lax.stdin.redirect

표준 입력입니다.

가능한 값:

- `<blank>` - 입력 없음
- `console` - 콘솔 창에서 읽습니다.
- `<path_to_a_file>` - 지정된 파일에서 입력을 읽습니다.

기본값

`<blank>`

lax.stdout.redirect

표준 출력입니다.

가능한 값:

- `<blank>` - 출력 없음
- `console` - 출력을 콘솔 창에 보냅니다.
- `<path_to_a_file>` - 출력을 지정된 파일에 저장합니다.

기본값

`<blank>`

lax.user.dir

이 속성을 사용하면 네이티브 시작 관리자가 사용자 디렉토리를 설정하기 위한 플랫폼 기본 동작을 변경하지 않습니다.

이 속성을 상대 또는 절대 경로로 설정하여 이를 무시할 수 있습니다. 상대 경로는 시작 관리자를 기준으로 합니다.

기본값

`<blank>`

lax.version

이 속성 파일을 만든 LaunchAnywhere 의 버전입니다.

기본값

9.0

IntroscopeWebView.properties

다양한 WebView 동작이 이 파일에서 정의한 속성으로 제어됩니다.

introscope.webview.jetty.configurationFile

Jetty XML 구성 파일의 경로입니다. 절대 경로이거나 config 디렉터리를 기준으로 한 상대 경로입니다. 이 파일은 포트 8443 에서 HTTPS 트래픽에 대한 SSL 수신기를 만듭니다.

고급 Jetty 구성의 경우 이 속성의 주석 처리를 제거하고 Jetty 구성 파일에 있는 설정을 수정하십시오.

HTTP 수신기는 introscope.webview.tcp.port 속성에서 지정됩니다. 이 속성의 주석 처리를 제거하지 않으면 HTTP 수신기가 생성되지 않습니다.

기본값

webview-jetty-config.xml

introscope.webview.tcp.ipaddress

WebView 를 특정 로컬 IP 주소에 바인딩하기 위한 WebView HTTP 서버 설정 속성입니다. 이 속성을 구성하지 않으면 WebView 가 모든 로컬 주소(와일드카드 주소)에서 들어오는 연결을 받아들입니다.

기본값

WebView 컴퓨터의 적합한 IP 주소로 설정하십시오.

introscope.webview.tcp.port

WebView 가 HTTP 트래픽을 수신 대기하는 포트입니다.

기본값

8080

introscope.webview.context.path

WebView 의 응용 프로그램 컨텍스트 경로입니다. 컨텍스트 경로는 WebView 서버의 정규화된 호스트 이름과 포트 번호에 추가되어 WebView 루트, 즉 WebView 에 액세스하기 위한 URL 을 형성합니다. 이 기능을 사용하면 사용자가 WebView 의 응용 프로그램 이름을 정의할 수 있습니다.

컨텍스트 경로가 다음과 같은 경우

/webview

WebView 에 액세스하기 위한 URL 은 다음과 같습니다.

http://host:port/webview/

기본값

/

참고: SAP 환경에서 WebView 를 사용 중인 경우 기본값은 */webview* 입니다.

introscope.webview.enterprisemanager.tcp.host

연결 대상이 될 Enterprise Manager 호스트 이름입니다.

기본값

localhost

introscope.enterprisemanager.webview.disableLogin

WebView 가 Enterprise Manager 와의 연결을 설정할 수 있는지 여부를 결정합니다.

기본값

false

introscope.webview.enterprisemanager.tcp.port

연결 대상이 될 Enterprise Manager 포트입니다.

기본값

5001

log4j.logger.WebView

WebView 로그의 로깅 세부 정보 양입니다.

세부화 수준 값은 다음일 수 있습니다.

- *INFO*
- *VERBOSE#com.wily.util.feedback.Log4JSeverityLevel*

대상 값은 다음일 수 있습니다.

- *console*
- *logfile*

기본값

INFO, console

log4j.logger.WebServer

WebServer 로그의 로깅 세부 정보 양입니다.

세부화 수준 값은 다음일 수 있습니다.

- *INFO*
- *VERBOSE com.wily.util.feedback.Log4JSeverityLevel*

대상 값은 다음일 수 있습니다.

- *console*
- *logfile*

기본값

INFO, console

log4j.logger

WebView 가 사용하는 타사 소프트웨어에 대한 로깅 속성입니다.

세부화 수준 값은 다음일 수 있습니다.

- *INFO*
- *VERBOSE com.wily.util.feedback.Log4JSeverityLevel*

대상 값은 다음일 수 있습니다.

- *console*
- *logfile*

기본값

INFO, console

log4j.logger.com.wily

CA APM 로그의 로깅 세부 정보 양입니다.

세부화 수준 값은 다음일 수 있습니다.

- *INFO*
- *VERBOSE com.wily.util.feedback.Log4JSeverityLevel*

대상 값은 다음일 수 있습니다.

- *console*
- *logfile*

기본값

INFO, console

log4j.logger.org.apache.myfaces

Apache Myfaces 로그의 로깅 세부 정보 양입니다.

위에서 로그 파일을 지정한 경우 로그 파일의 위치는 *log4j.appender.logfile.File* 속성으로 구성됩니다. 필요한 경우 전체 경로를 사용할 수 있습니다.

기본값

ERROR,console

log4j.logger.org.apache.jasper

Apache Jasper 로그의 로깅 세부 정보 양입니다.

위에서 로그 파일을 지정한 경우 로그 파일의 위치는 *log4j.appender.logfile.File* 속성으로 구성됩니다. 필요한 경우 전체 경로를 사용할 수 있습니다.

기본값

ERROR,console

log4j.logger.org.apache.struts

Apache Struts 로그의 로깅 세부 정보 양입니다.

위에서 로그 파일을 지정한 경우 로그 파일의 위치는 *log4j.appender.logfile.File* 속성으로 구성됩니다. 필요한 경우 전체 경로를 사용할 수 있습니다.

기본값

ERROR,console

log4j.logger.org.mortbay

Mortbay 로그의 로깅 세부 정보 양입니다.

위에서 로그 파일을 지정한 경우 로그 파일의 위치는 *log4j.appender.logfile.File* 속성으로 구성됩니다. 필요한 경우 전체 경로를 사용할 수 있습니다.

기본값

ERROR,console

로깅 구성 속성

다음 속성은 일반적으로 수정하면 안 됩니다.

- log4j.additivity.WebView=false
- log4j.additivity.WebServer=false
- log4j.additivity.com.wily=false
- log4j.appender.console=com.wily.org.apache.log4j.ConsoleAppender
- log4j.appender.console.layout=com.wily.org.apache.log4j.PatternLayout
- log4j.appender.console.layout.ConversionPattern=%d{M/dd/yy hh:mm:ss a z} [%-3p] [%c] %m%n
- log4j.appender.logfile=com.wily.org.apache.log4j.RollingFileAppender
- log4j.appender.logfile.layout=com.wily.org.apache.log4j.PatternLayout
- log4j.appender.logfile.layout.ConversionPattern=%d{M/dd/yy hh:mm:ss a z} [%-3p] [%c] %m%n
- log4j.appender.logfile.MaxBackupIndex=4
- log4j.appender.logfile.MaxFileSize=200MB

참고

값을 true 로 설정하면 그래프가 더 보기 좋게 안티앨리어싱됩니다. 예를 들어 introscope.workstation.graph.antialiased=true 와 같습니다.

기본값

기본값은 속성에 따라 다릅니다.

log4j.appender.console

이 속성은 콘솔에 메시지를 쓰기 위해 **WebView** 속성 파일에 추가됩니다.

기본값

logs/IntroscopeWebView.log

log4j.appender.logfile

이 속성은 로그 파일에 메시지를 추가하기 위해 **WebView** 속성 파일에 추가됩니다.

기본값

com.wily.org.apache.log4j.RollingFileAppender

log4j.appender.logfile.File

WebView 로그 파일의 이름 및 상대 위치(Enterprise Manager 홈 디렉터리 기준)입니다.

기본값

logs/IntroscopeWebView.log

Introscope WebView.lax

WebView의 런타임 동작이 이 파일에서 정의한 속성으로 제어됩니다.

실행 파일 이름

LaunchAnywhere 실행 가능 속성 파일입니다(Macrovision Corp).

기본값

<blank>

lax.class.path

이 응용 프로그램을 실행하는 데 필요한 **Java** 클래스 경로입니다.

기본값

lib/WebServices.jar:lib/IntroscopeClient.jar:lib/Workstation.jar:lib/WebViewAPI.jar:lib/WebViewServer.jar:lib/IntroscopeServices.jar

lax.command.line.args

기본 메서드에 전달할 명령줄 인수입니다. 이 속성을 사용하여 **WebView** 시작 시 로그인 화면을 우회하면서 **WebView** 에 로그인 값을 제공할 수 있습니다.

기본값

`$CMD_LINE_ARGUMENTS$`

lax.dir

LaunchAnywhere 의 네이티브 시작 관리자가 상주하는 디렉터리의 경로입니다.

기본값

<blank>

lax.main.class

응용 프로그램의 기본 메서드를 포함하는 클래스입니다.

기본값

`org.eclipse.core.launcher.Main`

lax.main.method

호출할 기본 클래스에 있는 메서드입니다.

기본값

main

lax.nl.current.vm

다음에 Workstation 이 시작될 때 사용할 VM 입니다. 설치된 JDK 또는 JRE 버전으로 설정할 수 있습니다. JVM 버전 요구 사항은 *CA APM 설치 및 업그레이드 안내서*를 참조하십시오.

기본값

운영 체제에 따라 다릅니다.

lax.nl.java.launcher.main.class

LaunchAnywhere Java 시작 관리자의 기본 클래스입니다.

참고

이 속성은 조정하면 안 됩니다.

기본값

com.zerog.lax.LAX

lax.nl.java.launcher.main.method

LaunchAnywhere Java 시작 관리자의 기본 메서드입니다.

참고

이 속성은 조정하면 안 됩니다.

기본값

main

lax.nl.java.option.additional

힙 크기 등의 JVM 에 대한 선택적 설정입니다.

기본값

`-Xms128m -Xmx512m -Djava.awt.headless=false -Dsun.java2d.noddraw=true`

lax.nl.message.vm.not.loaded

lax.nl.valid.vm.list 에 있는 VM 을 찾을 수 없는 경우 사용자 대화 상자에 표시되는 메시지입니다.

참고

이 속성은 *InstallAnywhere* 시작 관리자 내에서만 사용됩니다.
Introscope 에는 별개의 Java 요구 사항이 있습니다. 자세한 내용은 *CA APM 설치 및 업그레이드 안내서*의 *시스템 요구 사항* 단원을 참조하십시오.

기본값

해당 없음

lax.nl.valid.vm.list

공백이나 쉼표로 구분된 하나 이상의 [ALL JDK JRE J1 J2 JRE_J1 JDK_J1 JRE_J2 JDK_J2 MSJ]를 포함하는 문자열입니다. 네이티브 시작 관리자가 현재 가상 컴퓨터를 찾을 수 없으면 이 목록에 정의된 가상 컴퓨터를 검색합니다.

기본값

J2

lax.nl.win32.microsoftvm.min.version

이 응용 프로그램이 실행될 Microsoft VM 의 최소 버전입니다.

기본값

2750

lax.root.installation.dir

installdir 매직 폴더의 경로입니다.

기본값

<blank>

lax.stderr.redirect

표준 출력입니다.

가능한 값:

- `<blank>` - 출력 없음
- `console` - 출력을 콘솔 창에 보냅니다.
- `<path_to_a_file>` - 출력을 지정된 파일에 저장합니다.

기본값

console

lax.stdin.redirect

표준 입력입니다.

가능한 값:

- `<blank>` - 입력 없음
- `console` - 콘솔 창에서 읽습니다.
- `<path_to_a_file>` - 지정된 파일에서 입력을 읽습니다.

기본값

console

lax.stdout.redirect

표준 출력입니다.

가능한 값:

- `<blank>` - 출력 없음
- `console` - 출력을 콘솔 창에 보냅니다.
- `<path_to_a_file>` - 출력을 지정된 파일에 저장합니다.

기본값

console

lax.user.dir

지정할 경우 네이티브 시작 관리자가 사용자 디렉토리를 설정하기 위한 플랫폼 기본 동작을 변경하지 않게 되므로 이 속성은 비어 있습니다. 이 속성을 상대 또는 절대 경로로 설정하여 이 동작을 무시할 수 있습니다. 상대 경로는 시작 관리자를 기준으로 합니다.

기본값

<blank>

lax.version

이 속성 파일을 만든 LaunchAnywhere 의 버전입니다.

기본값

9.0

APMCloudMonitor.properties

APMCloudMonitor.properties 파일의 속성을 사용하여 CA APM Cloud Monitor 동작을 제어하고 CA APM Cloud Monitor 에이전트가 Enterprise Manager 에 보내는 데이터를 필터링할 수 있습니다.

CA APM Cloud Monitor 에이전트 설치 관리자는 기본적으로 다음 위치에 이 파일을 설치합니다.

<CloudMonitor_Agent_Home>/CloudMon/conf/APMCloudMonitor.properties

apmcm.folders.include

Enterprise Manager 에 데이터를 보내는 CA APM Cloud Monitor 폴더를 정의합니다.

기본값

주석 처리됨

가능한 값

- 모두
- 하나 이상의 폴더 목록(이름별)

형식

쉼표로 구분된 목록

예

folder0,folder1,folder two,folder3

apmcm.monitors.include

Enterprise Manager 에 데이터를 보내는 CA APM Cloud Monitor 모니터를 정의합니다.

기본값

주석 처리됨

가능한 값

- 모두
- 쉼표로 구분된 모니터 목록

예

monitor0,monitor1,monitor two,monitor3

apmcm.checkpoints.include

테스트 쿼리를 보내는 CA APM Cloud Monitor 검사점 또는 모니터링 사이트를 정의합니다.

기본값

주석 처리됨

가능한 값

- 모두
- 하나 이상의 검사점 목록(이름별)

형식

쉼표로 구분된 목록

예

gr,uk,f2,mb,it,nl

참고: "제품" > "Monitoring Stations"(모니터링 스테이션)를 선택하여 검사점 약어의 전체 목록을 볼 수 있습니다.

apmcm.include.inactive.monitors

비활성 CA APM Cloud Monitor 모니터가 Enterprise Manager 에 데이터를 보내는지 여부를 정의합니다.

기본값

False

가능한 값

- false
- true

apmcm.folder.metrics.include

에이전트가 Enterprise Manager 에 보내는 CA APM Cloud Monitor 폴더 메트릭을 정의합니다.

기본값

주석 처리됨

가능한 값

속성 파일의 프로브 목록을 참조하십시오.

형식

쉼표로 구분된 목록

예

probes,probe_errors,checks,check_errors,uptime,ttime,ctime,ptime,dtime,dsizes

apmcm.monitor.psp.metrics.include

메트릭을 반환하는 CA APM Cloud Monitor 공용 상태 페이지를 정의합니다.

기본값

color,errors,avg_uptime_cur,avg_uptime_day,avg_perf_cur,avg_perf_day

가능한 값

속성 파일의 페이지 목록을 참조하십시오.

형식

쉼표로 구분된 목록

예

color,errors,avg_uptime_cur

apmcm.monitor.checkpoint.metrics.include

CA APM Cloud Monitor 에이전트가 Enterprise Manager 에 보내는 CA APM Cloud Monitor 검사점 메트릭을 정의합니다.

기본값

runtime,ctime,ptime,ttime,dtime,descry

가능한 값

속성 파일의 메트릭 목록을 참조하십시오.

형식

쉼표로 구분된 목록

예

runtime,ctime,ptime

apmcm.force.global.update

기본적으로 CA APM Cloud Monitor 에이전트는 3600 초마다 다음 메타데이터에 대한 변경 사항을 확인합니다.

- 재로그인
- 모니터 목록 업데이트
- 폴더 목록 업데이트
- 검사점 목록 업데이트

에이전트가 변경 사항을 확인하고 이러한 메타데이터를 즉시 업데이트하도록 하려면 기본값을 다른 정수로 변경합니다.

참고: 이 속성의 값은 아무 의미도 없습니다. 실제로 메타데이터이므로 이 값이 현재 값 외의 다른 값으로 변경되면 설명한 대로 메타데이터 확인이 강제로 수행됩니다.

기본값

1

가능한 값

임의의 정수

apmcm.log.adjustment

CA APM Cloud Monitor 에이전트가 로그에서 검색하는 최대 레코드 수입니다.

에이전트가 메트릭에 대해 로그를 쿼리할 때마다 마지막 항목을 검사합니다. 로그 항목의 예는 다음과 같습니다.

```
[CloudMonitorIntegration.CloudMonitorAgent] Log record found with k=4/21
```

... 여기서 분모(위 예에서 21)는 에이전트가 매분 로그에서 검색할 수 있는 최대 항목 수이고 분자(위 예에서 4)는 최근 1 분에 실제로 검색된 레코드 수입니다.

k가 1보다 큰 경우 다음과 같은 메시지가 로그에 나타납니다.

```
Some probe data may be missing. Automatically adjusting monitor log query. Please consider increasing apmcm.log.adjustment property.
```

이 메시지가 나타내는 자동 조정은 에이전트가 apmcm.log.adjustment의 값을 가져와서 분모에 추가함을 의미합니다. 따라서 apmcm.log.adjustment = 1을 설정하는 경우 검색되는 최대 항목 수가 22로 변경됩니다. 다음에 k가 1보다 크면 분모가 다시 1만큼 증가합니다.

기본값

0

가능한 값

임의의 정수

기타

이 속성은 핫 구성이 가능합니다. 이 속성을 변경한 경우에는 변경 사항을 적용하기 위해 Enterprise Manager를 다시 시작하지 않아도 됩니다.

부록 B: JDBC API

Introscope 에 포함된 API 를 사용하면 Excel, SAS 등의 데이터 분석 도구를 통해 Introscope 데이터를 볼 수 있습니다. JDBC 인터페이스를 사용하여 기록 범위에 대한 메트릭 및 이벤트 데이터를 추출할 수 있습니다. 데이터는 테이블 메타데이터를 설명하는 XML 문자열을 포함하는 단일 열이 있는 테이블 형식으로 반환되고, 결과 테이블을 포함합니다.

이 섹션은 다음 항목을 포함하고 있습니다.

[JDBC API 구성](#) (페이지 565)

[JDBC API 사용](#) (페이지 565)

JDBC API 구성

IntroscopeJDBC.jar 파일에는 JDBC 드라이버 클래스와 드라이버에 필요한 모든 클래스가 포함됩니다. 이 파일만 클라이언트 응용 프로그램의 클래스 경로에 있으면 됩니다.

드라이버 클래스는 *com.wily.introscope.jdbc.IntroscopeDriver* 입니다.

URL 형식은 다음과 같습니다. 이때 대/소문자를 구분하는 것이 중요합니다.

`jdbc:introscope:net://{username}:{password}@{host}:{em port}`

예:

`jdbc:introscope:net//Admin:@localhost:5001`

JDBC API 사용

Introscope JDBC API 에 대한 구문은 다음 가상 뷰를 지원합니다.

- `metric_data`
- `trace_headers`
- `traces`

메트릭 쿼리

메트릭 쿼리를 수행하는 경우 Introscope JDBC 드라이버에서 지원되는 다음 날짜 형식 중 하나를 사용하십시오.

- *mm/dd/yy hh:mm:ss*
- *EEE MMM dd HH:mm:ss zzz yyyy*

예를 들어 메트릭 쿼리는 다음과 같이 나타납니다.

```
select * from metric_data where agent={regex} and metric={regex} and timestamp between {starttime} and {endtime}
```

또는:

```
select * from metric_data where agent='.*Custom Metric Host.*' and metric='.*' and timestamp between '01/01/01 00:00:00' and '01/01/07 00:00:00'
```

한정자는 SQL 문에 다음 순서로 나타나야 합니다.

```
[sort by value {ascending|descending}] [maxmatches={max metrics}] [period={period in seconds}] [aggregateall]
```

참고: JDBC 드라이버를 사용하여 종료되는 에이전트를 쿼리하면 "0" 값이 반환됩니다.

다음 한정자는 Enterprise Manager의 메트릭 집계 기능을 지원합니다.

한정자

수행하는 작업

<i>sort by value {a d}</i>	각 시간 조각마다 메트릭 값에 대한 오름차순 또는 내림차순 <i>N</i> 정렬을 수행하라는 플래그를 Enterprise Manager에 지정합니다. 상위 <i>N</i> 일치에 대한 메트릭 제한을 지정하려면 이 한정자와 <i>maxmatches</i> 플래그를 사용하십시오.
<i>maxmatches</i>	이 개수의 메트릭까지만 데이터를 반환하라는 플래그를 Enterprise Manager에 지정합니다. <i>maxmatches=2</i> 인 경우 2개의 메트릭에 대한 데이터만 반환됩니다. 반환되는 행 수를 제한하는 <i>sql limit</i> 키워드와는 다릅니다. 예를 들어 <i>maxmatches=2</i> 인 경우 2개의 메트릭에 대해 각각 50개의 시간 조각이 반환되어 총 100개의 데이터 행이 반환될 수 있습니다.
<i>period</i>	지정된 기간까지 데이터 포인트를 집계하라는 플래그를 Enterprise Manager에 지정합니다. 예를 들어 Enterprise Manager가 일반적으로 15초의 데이터 값을 보고하지만 <i>period=60</i> 인 경우 60초까지 집계할 수 있습니다.

aggregateall 모든 메트릭 데이터를 하나의 요약된 시간 조각으로 집계하라는 플래그를 **Enterprise Manager** 에 지정합니다. 예를 들어 이 한정자를 사용하여 1 주 기간 동안 메트릭에 대한 단일 "평균 응답 시간"을 지정할 수 있습니다.

aggregateall 과 *period* 한정자를 함께 사용하지 마십시오. 둘 다 집계를 다루므로 충돌하게 됩니다.

메트릭 쿼리 예제

```
select * from metric_data where agent='.*' and metric='.*Average Response.*' and timestamp between '01/01/01 00:00:00' and '01/01/07 00:00:00' maxmatches=10
```

```
select * from metric_data where agent='.*' and metric='.*Average Response.*' and timestamp between '01/01/01 00:00:00' and '01/01/07 00:00:00' maxmatches=1
```

```
select * from metric_data where agent='.*' and metric='.*Average Response.*' and timestamp between '01/01/01 00:00:00' and '01/01/07 00:00:00' maxmatches=1 period=120
```

```
// match one metric_data and aggregate all values. This returns one row of data select * from metrics where agent='.*' and metric='.*Average Response.*' and timestamp between '01/01/01 00:00:00' and '01/01/07 00:00:00' maxmatches=1 aggregateall
```

```
// this is a top 10 query select * from metric_data where agent='.*' and metric='.*Average Response.*' and timestamp between '01/01/01 00:00:00' and '01/01/07 00:00:00' sort by value d maxmatches=10
```

트랜잭션 추적 쿼리

기본 트랜잭션 헤더 쿼리 구문은 다음과 같습니다.

```
select * from trace_headers where timestamp between {starttime} and {endtime} and query={lucene query string} [limit {rows}]
```

여기서 *lucene query string* 은 **Workstation** 의 기록 쿼리에 있는 것처럼 유효한 Lucene 쿼리 문자열입니다. 자세한 내용은 *CA APM Workstation 사용자 안내서*를 참조하십시오.

선택적 플래그인 *limit* 는 쿼리에서 반환되는 행 수를 제한합니다. 지정된 제한이 없으면 서버에 정의된 기본 트랜잭션 제한이 사용됩니다.

추적 본문에 대한 쿼리는 동일하지만, 다음과 같이 다른 뷰를 참조합니다.

```
select * from traces where timestamp between {starttime} and {endtime} and query={lucene query string} [limit {rows}]
```

트랜잭션 추적 쿼리 예제:

```
select * from trace_headers where timestamp between '01/01/01 00:00:00' and '01/01/07 00:00:00' and query='s*'
```

```
select * from trace_headers where timestamp between '01/01/01 00:00:00' and '01/01/07 00:00:00' and query='host:blinkys'
```

```
select * from traces where timestamp between '01/01/01 00:00:00' and '01/01/07 00:00:00' and query='host:blinkys' limit 100
```

추적 쿼리에서 반환된 데이터 행에는 도메인, 호스트, 프로세스 및 에이전트 이름 등의 에이전트 정보와 트랜잭션 추적에 대한 XML 표현이 포함됩니다.

부록 C: Introscope 확장 구성

설치할 때 Introscope 확장을 사용하도록 설정한 경우에는 해당 확장을 구성해야 합니다. 설치에 대한 자세한 내용은 *CA APM 설치 및 업그레이드 안내서*를 참조하십시오.

이 섹션은 다음 항목을 포함하고 있습니다.

[SNMP Adapter 구성](#) (페이지 569)

[Introscope 경고 웹 서비스 확장 구성](#) (페이지 579)

SNMP Adapter 구성

SNMP(Simple Network Management Protocol)는 네트워크 구성 요소의 모니터링 및 제어를 위한 표준 프로토콜입니다. Introscope 는 SNMP Adapter 를 통해 메트릭을 외부 SNMP 프레임워크에 보고할 수 있습니다. SNMP Adapter 에 대한 일반 정보는 *CA APM Workstation 사용자 안내서*를 참조하십시오.

SNMP Adapter 제한 사항

SNMP 관리자에서 Introscope 별 메트릭을 읽는 기능을 사용하면 한 위치에서 모든 네트워크 구성 요소의 데이터를 간편하게 모니터링할 수 있습니다. 그러나 다음 제한 사항이 Introscope SNMP 기능에 적용됩니다.

- SNMP 관리자에서 Introscope 메트릭만 볼 수 있습니다.
- 경고, 작업 등의 다른 Introscope 기능은 Introscope 별 정보의 일부로 게시되지 않습니다.
- Introscope 정보는 읽기 전용입니다.
- "설정"은 지원되지 않습니다.

SNMP Adapter 구성 요소

SNMP Adapter 구성 요소는 다음과 같습니다.

SNMP 수집

SNMP 수집은 MIB 파일에 게시될 메트릭을 정의하는 Introscope 요소입니다. SNMP 수집은 관리 모듈에 저장됩니다.

MIB(관리 정보 데이터베이스) 파일

MIB 는 SNMP 에이전트가 보고하는 정보를 설명하는 텍스트 파일입니다. MIB 파일을 SNMP 관리자에 로드하여 SNMP 관리자에 SNMP 에이전트가 보고할 수 있는 정보를 알릴 수 있습니다.

Introscope 에서 생성된 MIB 파일은 현재 활성 상태인 SNMP 수집 시점의 스냅샷으로, 일치하는 Introscope 메트릭을 SNMP 호환 형식으로 설명합니다.

SNMP 에이전트

Enterprise Manager 를 배포할 때 Introscope SNMP 에이전트가 설치됩니다. 이 에이전트는 Enterprise Manager 에서 Introscope 관련 메트릭 데이터를 수집하고 SNMP 관련 형식으로 변환하여 SNMP 관리자로 보냅니다.

경고 알림

경고가 트리거되어 SNMP 알림 작업이 발생한 경우 SNMP Adapter 는 경고를 설명하는 SNMP 알림(트랩)을 Enterprise Manager 속성 파일에서 지정한 구성된 SNMP 관리자로 보냅니다.

경고

경고에 대한 SNMP 알림 작업을 구성한 경우 경고가 트리거되면 이제 Enterprise Manager 가 SNMP 알림(트랩)을 구성된 SNMP 관리자로 보냅니다. 경고 메시지를 보유하는 알림에는 *octet string* 유형의 값 개체가 있습니다. 내용은 콘솔 알림 작업과 동일합니다.

해당 SNMP 개체는 MIB 에서 자동으로 게시됩니다.

알림은 아래에 설명된 대로 고정 OID(고유 개체 ID)를 사용합니다. 여기서 xxxx 는 임의로 선택된 SmpAdapter 식별자(예: 5527)입니다.

알림(숫자 형식)

값: 1.3.6.1.4.1.10480.1.1.xxxx.5000

알림(이름 형식)

값:

iso.org.dod.internet.private.enterprises.wily.products.introscope.snmpAdapterxx.xx.wilyAlertNotif

경고(숫자 형식)

값: *1.3.6.1.4.1.10480.1.1.xxxx.6000*

경고 메시지(이름 형식)

값:

iso.org.dod.internet.private.enterprises.wily.products.introscope.snmpAdapterxx.xx.wilyAlertNotifMessage

알림 및 경고 구성

알림(트랩)을 구성하려면

- *IntroscopeEnterpriseManager.properties* 를 편집하고 다음 속성을 설정하십시오.

introscope.agent.enterprisemanager.snmp.target.port

SNMP 관리자의 포트입니다.

기본값

162

introscope.agent.enterprisemanager.snmp.target.destination

SNMP 관리자의 호스트 이름 또는 IP 주소입니다.

기본값

localhost

introscope.agent.enterprisemanager.snmp.target.community

SNMP 관리자의 SNMPv2 커뮤니티입니다.

기본값

public

introscope.enterprisemanager.snmp.notification.enable

알림을 설정(*true*) 또는 해제(*false*)합니다.

기본값

true

참고

snmp.notification.enable 속성은 핫 구성에서 지원되므로 속성을 설정한 후 Enterprise Manager 를 다시 시작하지 않아도 됩니다. 그러나 다른 속성을 선택하려면 Enterprise Manager 를 다시 시작해야 합니다.

Workstation/Enterprise Manager 에 대한 경고 및 SNMP 알림 작업을 구성할 수도 있습니다. 자세한 내용은 *CA APM Workstation 사용자 안내서*와 본 안내서에 포함된 다양한 항목을 참조하십시오.

SNMP 기능 구성

SNMP 프레임워크에서 볼 수 있도록 Introscope 별 메트릭을 준비하려면

- Enterprise Manager 속성 파일에서 SNMP 를 사용하도록 설정합니다. [속성 설정을 구성하여 SNMP 를 사용하도록 설정](#) (페이지 573)을 참조하십시오.
- SNMP 수집을 생성합니다. 자세한 내용은 *CA APM Workstation 사용자 안내서*를 참조하십시오.
- MIB 를 게시합니다. 자세한 내용은 *CA APM Workstation 사용자 안내서*를 참조하십시오.
- MIB 를 SNMP 관리자에 로드합니다. [MIB 파일을 SNMP 프레임워크에 로드](#) (페이지 574)를 참조하십시오.

속성 설정을 구성하여 SNMP 가 사용되도록 설정

SNMP 가 사용되도록 설정하려면 *IntroscopeEnterpriseManager.properties* 파일에서 두 가지 설정을 구성합니다.

설정을 구성하려면

1. Enterprise Manager 를 실행 중인 경우 종료합니다.
2. `<EM_Home>/config/IntroscopeEnterpriseManager.properties` 파일을 엽니다.
3. `introscope.enterprisemanager.snmp.enable` 설정의 경우 값을 `true` 로 입력합니다.
4. `introscope.enterprisemanager.snmp.agent.port` 설정의 경우 기본값인 161 을 그대로 사용합니다.

참고: UNIX 플랫폼을 사용 중인 경우에는 루트로 로그인하거나 루트 권한을 가지고 있어야 1000(기본 SNMP 에이전트 포트: 161) 미만의 포트를 사용할 수 있습니다.

1. 변경 내용을 저장합니다.
2. Enterprise Manager 를 다시 시작합니다.

MIB 파일 정보

MIB 파일은 호스트 이름에 따라 이름 지정되며 다음 디렉터리에 저장됩니다.

`<EM_Home>/snmp/`

MIB 파일은 이 구문을 사용하여 게시되고 고유하게 이름 지정됩니다.

- HP LoadRunner: `Introscope-<hostname>.lr.mib`
- HP OpenView: `Introscope-<hostname>.mib`
- BMC Patrol
 - `Introscope-<hostname>.bmc.mib`
 - `Introscope-<hostname>.bmc.smi`
- 기타: `Introscope-<hostname>.other.mib`

호스트 이름에 있는 올바르지 않은 문자는 모두 제거됩니다. 호스트 이름의 마침표는 대시로 변환됩니다.

MIB 파일을 SNMP 프레임워크에 로드

SNMP 에이전트에서 사용할 수 있는 메트릭을 식별하려면 SNMP 관리자에 MIB 복사본이 있어야 합니다. MIB 를 게시한 후 MIB 파일을 SNMP 관리자에 로드해야 합니다.

다음과 같은 경우에는 SNMP 관리자에서 MIB 파일을 업로드해야 합니다.

- 새 MIB 를 게시하는 경우
- Enterprise Manager 또는 관리되는 응용 프로그램이 다른 호스트로 이동된 경우

Introscope 에서 생성된 MIB 를 SNMP 프레임워크에서 사용하는 경우 MIB 를 준비하는 방법을 보려면 특정 SNMP 프레임워크 설명서를 참조하십시오. 도움이 필요하면 CA Technologies 전문 서비스에 문의하십시오.

HP LoadRunner 에 업로드

다음은 본 안내서의 작성 당시의 최신 정보입니다. 업데이트가 있는지 확인하려면 HP 에 문의하십시오.

Introscope 에서 생성된 MIB 파일을 HP LoadRunner 에 업로드하려면

1. SNMP Adapter 를 설치합니다.
 - a. *SNMPAdapter.jar* 를 `<EM_Home>/product/enterprisemanager/plugins` 에 복사합니다.
 - b. `<EM_Home>/config/`에 있는 *IntroscopeEnterpriseManager.properties* 파일을 편집하여 다음 속성을 설정합니다.
`introscope.enterprisemanager.snmp.enable=true`
2. Enterprise Manager 를 다시 시작합니다.
3. SNMP 수집을 생성합니다. 자세한 내용은 *CA APM Workstation 사용자 안내서*를 참조하십시오.
4. MIB 파일을 게시합니다.
 - a. 열려 있지 않은 경우 "파일" > "새 관리 모듈 편집기"를 선택하여 Introscope Investigator 에서 관리 모듈 편집기를 시작합니다.
 - b. "관리자" > "MIB 게시..."를 클릭하여 MIB 파일을 게시합니다.
 - c. "LoadRunner"를 선택합니다.
 - d. "게시"를 클릭합니다.

5. MIB 파일을 복사합니다.
 - 원본: <EM_Home>/snmp
 - 대상: SiteScope: <SiteScope>/templates.mib
6. SiteScope Windows 서비스를 다시 시작합니다.
7. SiteScope SNMP Browser 를 사용하여 MIB 파일을 로드했는지 확인합니다.
 - a. "시작" > "프로그램" > "HP SiteScope" > "Open HP SiteScope LR"(HP SiteScope LR 열기)로 이동합니다.
 - b. "Open SiteScope"(SiteScope 열기)를 클릭합니다.
 - c. "Monitors"(모니터) 탭을 엽니다.
 - d. "SiteScope" > "Tools"(도구) > "SNMP Browser"(SNMP 브라우저)를 선택합니다.
 - e. Enterprise Manager 호스트 이름, 버전 V2 를 입력합니다.
 - f. MIB 파일을 선택합니다.
 - g. "Browse"(찾아보기)를 클릭합니다.
8. 측정을 추가합니다.
 - a. LoadRunner Controller 를 엽니다. "시작" > "프로그램" > "HP LoadRunner" > "Applications"(응용 프로그램) > "Controller"(컨트롤러)를 선택합니다.
 - b. 수동 시나리오를 생성합니다.
 - c. "Scenario"(시나리오) 창에서 "Run"(실행) 탭을 클릭합니다.
 - d. "Available Graphs"(사용 가능한 그래프) > "System Resource Graphs"(시스템 리소스 그래프) 목록에서 "SNMP"를 두 번 클릭합니다.
 - e. "SNMP Graph"(SNMP 그래프)를 선택합니다.
 - f. "Monitors"(모니터) > "Add Measurements"(측정 추가)를 클릭합니다.
9. "SNMP" 대화 상자에서 다음과 같이 합니다.
 - a. "고급"을 클릭합니다.
 - b. "SiteScope"를 선택하고 "OK"(확인)를 클릭합니다.
 - c. 새로 모니터링되는 서버 컴퓨터를 추가하려면 "Add"(추가)를 클릭합니다.

- d. Enterprise Manager 호스트를 모니터링되는 서버로 설정하고 "OK"(확인)를 클릭합니다.
 - e. 리소스 측정을 추가하려면 "Add"(추가)를 클릭합니다.
 - f. 서버가 Enterprise Manager 컴퓨터 이름으로 설정되었는지 확인합니다.
 - g. SNMP 버전을 V2 로 변경합니다.
 - h. "Every..."(다음마다...)를 더 높은 값으로 업데이트합니다. 이 설정이 너무 낮으면 HP LoadRunner 에서 오류를 표시할 수 있습니다.
10. 트리를 확장하고 원하는 OID(메트릭)를 선택합니다.
11. HP LoadRunner 에서 데이터를 확인합니다.

참고:

HP LoadRunner 를 사용하는 경우

- HP LoadRunner SNMP Monitor 가 있어야 게시된 데이터를 볼 수 있습니다.
- MIB 가 SiteScope SNMP Browser 에 표시되지 않으면 오류 로그 파일을 검토하십시오.
- HP LoadRunner 가 MIB 에서 동일한 노드 이름을 허용하지 않으므로 MIB 에서 이름이 동일한 메트릭은 번호가 추가된 상태로 나타납니다.
예:
fileInputRateBytesPerSecond23
- HP LoadRunner 는 음수를 그래프로 표현하지 않습니다.

HP OpenView 에 업로드

Introscope 에서 생성된 MIB 파일을 HP OpenView 에 업로드하려면

1. SNMP Adapter 를 설치합니다.
 - a. *SNMPAdapter.jar* 를 `<EM_Home>/product/enterprisemanager/plugins` 에 복사합니다.
 - b. `<EM_Home>/config/`에 있는 *IntroscopeEnterpriseManager.properties* 파일을 편집하여 다음 속성을 설정합니다.
`introscope.enterprisemanager.snmp.enable=true`
2. Enterprise Manager 를 다시 시작합니다.

3. SNMP 수집을 생성합니다. 자세한 내용은 *CA APM Workstation 사용자 안내서*를 참조하십시오.
4. MIB 파일을 게시합니다.
 - a. 열려 있지 않은 경우 "파일" > "새 관리 모듈 편집기"를 선택하여 Introscope Investigator 에서 관리 모듈 편집기를 시작합니다.
 - b. "관리자" > "MIB 게시..."를 클릭하여 MIB 파일을 게시합니다.
 - c. "HP OpenView"를 선택합니다.
 - d. "게시"를 클릭합니다.
5. MIB 파일을 복사합니다.
 - 원본: <EM_Home>/snmp
 - 대상: HP OpenView 가 설치된 컴퓨터
6. HP OpenView 컴퓨터에서 "시작" > "프로그램" > "HP OpenView" > "Network Node Manager Admin"(네트워크 노드 관리자 운영) > "Network Node Manager"(네트워크 노드 관리자)를 선택합니다.
7. 루트 콘솔에서 "Settings"(설정) > "Load"(로드)로 이동합니다.
8. "Unload the .mibs"(.mib 언로드)에서 "SNMP"를 선택합니다.
9. "Load"(로드)를 클릭합니다.
10. Introscope MIB 파일을 선택합니다.

파일 이름에는 MIB 파일을 생성한 Enterprise Manager 이름이 포함됩니다.
11. 업로드가 완료된 후 "Close"(닫기)를 클릭합니다.
12. MIB 브라우저를 엽니다. "Tools"(도구) > "SNMP"를 선택합니다.
 - a. "Name"(이름) 또는 "Address"(주소) 필드에 Enterprise Manager 호스트 이름을 입력합니다.

이 이름은 Introscope 에서 MIB 파일의 이름에 참조된 것과 동일한 호스트 이름입니다.
 - b. "Community Name"(커뮤니티 이름) 필드에 *public* 을 입력합니다.
 - c. 노드를 확장합니다.


```
iso > org > dod > private > enterprises> wily > products > introscope > snmpAdapter
> hostname
```

그래프에 메트릭을 표시하려면

1. 메트릭을 선택합니다.
2. "Graph"(그래프)를 클릭합니다.

MIB 에서 메트릭을 찾으려면

1. MIB 에서 호스트 이름, 에이전트 이름, 리소스 이름을 선택합니다.
2. "Start Query"(쿼리 시작)를 클릭합니다.

Introscope 메트릭을 SNMP 메트릭으로 변환

Introscope 는 Introscope 메트릭 유형과 Introscope 메트릭 이름을 모두 SNMP 호환 정보로 변환합니다.

메트릭 유형 변환

SNMP 에이전트는 여기에 표시된 대로 Introscope 메트릭을 SMiv2 메트릭 유형으로 변환합니다.

Introscope 메트릭 유형	일반 MIB SMiv 2 메트릭 유형	HP OpenView 또는 LoadRunner MIB SMiv 2 메트릭 유형	BMC MIB SMiv 2 메트릭 유형
정수	INTEGER32(-2147483648...2147483647)	INTEGER32(-2147483648...2147483647)	COUNTER32(-2147483648...2147483647)
Long	INTEGER32(상동)	INTEGER32(상동)	COUNTER32(상동)
문자열	OCTETSTRING	OCTETSTRING	OCTETSTRING

SNMP 는 32 비트보다 큰 정수를 지원하지 않습니다. Long 은 다음 알고리즘을 사용하여 32 비트 정수로 변환됩니다.

- Long 이 Integer.MAX_VALUE 보다 큰 경우 Integer.MAX_VALUE 로 설정하십시오.
- Long 이 Integer.MIN_VALUE 보다 작은 경우 Integer.MIN_VALUE 로 설정하십시오.
- 그렇지 않은 경우에는 Int 로 캐스팅하면 됩니다.

메트릭 이름 변환

SNMP 에이전트는 다음 규칙을 사용하여 Introscope 메트릭 이름 세그먼트를 MIB 식별자로 변환합니다.

1. 세그먼트에는 적합한 문자(A-Z|a-z|-|0-9)만 포함되어 있어야 합니다. 세그먼트에 잘못된 문자가 있는 경우 해당 문자가 모두 제거됩니다.
2. 각 세그먼트는 소문자로 시작해야 합니다. 세그먼트가 대문자로 시작하는 경우 해당 대문자가 소문자로 변환됩니다. 세그먼트가 숫자로 시작하는 경우 해당 숫자 앞에 문자 "a"가 붙습니다.
3. 세그먼트는 하이픈으로 끝날 수 없습니다. 하이픈으로 끝나는 경우 해당 하이픈이 제거됩니다.
4. 세그먼트에는 두 개의 하이픈이 연속으로 포함될 수 없습니다. 하나의 하이픈이 제거됩니다.

세그먼트는 64 자 이하여야 합니다. 세그먼트가 64 자를 초과하는 경우 64 자로 잘립니다. 잘린 결과로 세그먼트가 동일해지는 경우 세그먼트가 추가로 잘리고 대시와 숫자(예: -2)가 추가됩니다.

Introscope 경고 웹 서비스 확장 구성

Introscope 에서 제공하는 CA APM 웹 서비스 API 를 이용하여 타사 응용 프로그램에서 CA Introscope 를 경고 및 메트릭의 출처로 사용할 수 있습니다. 타사 응용 프로그램에 제공되도록 CA Introscope 경고를 구성하려면 CA Introscope 경고 웹 서비스 확장을 구성합니다.

아래의 속성은 IntroscopeEnterpriseManager.properties 에 나타나지 않습니다. 이 속성을 구성하려면 파일에서 수동으로 추가해야 합니다.

Enterprise Manager 와 함께 설치된 웹 서비스 파일에 대한 자세한 내용은 *CA APM 설치 및 업그레이드 안내서*를 참조하십시오.

Introscope 경고 웹 서비스 확장을 구성하려면

1. <EM_Home>\config 디렉터리에 있는 *IntroscopeEnterpriseManager.properties* 파일을 엽니다.
2. *introscope.alerts.extension.managementmodules.enable* 속성을 추가하고 경고를 제공할 관리 모듈을 나열합니다. 속성 값을 비워 두거나 "ALL"을 지정하면 모든 관리 모듈의 경고가 제공됩니다.

3. *introscope.alerts.extension.inventory.updatecheckintervalsecs* 속성을 추가합니다. 이 속성은 경고 확장에서 경고가 있는지 검사하는 빈도(초)를 지정합니다. 값을 지정하지 않으면 기본적으로 60 초마다 검사됩니다. 15 초보다 낮은 값은 지정할 수 없습니다. 15 초보다 낮은 값을 지정하면 15 초로 기본 설정됩니다.

위의 시간 간격 중에 에이전트를 추가하거나 에이전트를 제거하거나 관리 모듈의 변경 사항을 저장한 경우 CA Introscope 에서 에이전트와 관리 모듈에 대한 내부 인벤토리 검사를 수행합니다. Introscope 는 인벤토리를 업데이트한 다음 경고 상태 변경 사항을 처리합니다.

4. Enterprise Manager 를 다시 시작하여 속성 파일 변경 사항을 적용합니다.

부록 D: 기본 `tess-default.properties` 파일

`tess-default.properties` 파일에는 거의 수정하지 않거나 숙련된 CA CEM 관리자나 CA Support 의 지침에 따라서만 수정해야 하는 각종 속성이 포함되어 있습니다.

이 섹션은 다음 항목을 포함하고 있습니다.

[tess-default.properties 속성 기본 파일 수정 \(페이지 581\)](#)

[증거 수집을 위한 Perl 또는 Python 경로 설정 \(페이지 582\)](#)

["추가 결합 정보" 링크의 디렉터리 경로 설정 \(페이지 584\)](#)

[결합 처리 성능 개선 \(페이지 585\)](#)

[잘못된 파일의 디렉터리 위치 변경 \(페이지 588\)](#)

[기타 CA CEM 기본 속성 \(페이지 589\)](#)

tess-default.properties 속성 기본 파일 수정

CA CEM `tess-default.properties` 파일은 `<EM_Home>\config` 디렉터리에 있습니다.

중요! 기본 속성을 편집해야 하는 경우에는 사용자 고유의 파일 버전을 생성하고 다음과 같이 이름을 지정해야 합니다.

`tess-customer.properties`

`tess-customer.properties` 라는 사용자 고유의 파일을 생성하면 이후의 CA CEM 소프트웨어 업그레이드 중에 속성의 수정 사항이 손실되지 않습니다.

경고! 클러스터 환경에서 `tess-customer.properties` 파일을 생성하거나 편집한 후에는 이 파일을 각 Enterprise Manager 에 복사해야 합니다.

Enterprise Manager 마다 *tess-default.properties* 파일이 있습니다. Enterprise Manager 가 로컬 파일에서 읽는 속성은 해당 Enterprise Manager 에서 실행 중인 서비스에 따라 다릅니다. 예를 들어 고객 경험 메트릭과 관련된 속성은 TIM 수집 서비스를 실행 중인 Enterprise Manager 에서 읽고 최대 사용자 그룹 수와 관련된 속성은 MOM(Manager of Managers)에서 읽습니다.

다음 단계를 따르십시오.

1. 다음 파일을 찾습니다.

```
<EM_Home>/config/tess-default.properties
```

2. 동일한 디렉터리에 사용자 고유의 *tess-default.properties* 파일 버전을 생성하고 *tess-customer.properties* 라는 이름을 지정합니다.
3. 사용자 CA CEM 환경에 맞게 수정해야 하는 속성만 추가하면서 *tess-customer.properties* 파일을 수정합니다.

- a. 새 속성 파일을 편집합니다.

예를 들어 vi 편집기를 사용하여 다음과 같이 편집합니다.

```
vi tess-customer.properties
```

중요! *tess-customer.properties* 파일에는 오직 CA CEM 시스템 기본값과 다른 값을 가지는 속성만 포함되어 있어야 합니다.

tess-customer.properties 파일에 있는 속성을 모두 그대로 두면 시스템을 업그레이드할 때 향후 시스템 성능이 활용되지 않거나 속성에 대한 업데이트가 조정되지 않을 수 있습니다.

- b. *tess-customer.properties* 파일을 저장합니다.

4. *tess-customer.properties* 파일을 사용자 클러스터의 모든 Enterprise Manager 에 복사합니다.
5. 사용자 클러스터의 Enterprise Manager 를 각각 다시 시작합니다.

증거 수집을 위한 Perl 또는 Python 경로 설정

증거 수집([비즈니스 영향 설정 및 인시던트에 대한 증거 수집](#) (페이지 304))을 사용하려면 MOM 또는 독립 실행형 Enterprise Manager 에 Python 이나 Perl 을 설치해야 합니다. `python.path` 또는 `perl.path` 속성을 편집하여 Python 이나 Perl 의 위치를 지정하십시오.

perl.path

Perl 을 설치한 디렉터리입니다.

옵션

Perl 실행 파일의 디렉터리 경로입니다.

기본값

/usr/bin/perl

예

C:\\perl\\bin\\perl.exe

참고

백슬래시가 Windows 플랫폼에 사용되는 경우 단일 슬래시(/)가 이스케이프 시퀀스로 해석되므로 이중 슬래시(\\)가 필요합니다.

python.path

Python 을 설치한 디렉터리입니다.

옵션

Python 실행 파일의 디렉터리 경로입니다.

기본값

/usr/bin/python

예

C:\\python\\bin\\python.exe

참고

백슬래시가 Windows 플랫폼에 사용되는 경우 단일 슬래시(/)가 이스케이프 시퀀스로 해석되므로 이중 슬래시(\\)가 필요합니다.

"추가 결함 정보" 링크의 디렉터리 경로 설정

결함정보 페이지에 "추가 결함 정보" 링크를 표시하려면 결함 번호가 포함된 이름의 HTML 파일이 있어야 합니다.

결함 정보 페이지는 추가 결함 정보를 포함할 수 있는 사용자 지정 웹 페이지에 연결될 수 있습니다. 현재 결함 정보 페이지에는 시간, 처리량, 웹 서버 주소 등의 다양한 결함 정보가 표시됩니다. 그러나 회사의 구체적인 요구 사항에 따라 필요한 추가 결함 정보를 결함 정보 페이지에 추가해야 하는 경우도 있을 수 있습니다.

CA Technologies 전문 서비스에서 이러한 결함 정보를 제공하고 CA CEM 용 디렉터리에 보관할 수 있습니다. 결함 정보 페이지의 "추가 결함 정보" 링크에서 액세스되는 이 추가 결함 정보를 사용하면 최종 사용자 문제를 심사하고 각 개별 결함과 관련된 상황별 정보를 얻을 수 있습니다.

지정된 결함의 결함 정보 페이지 아래쪽에 "추가 결함 정보" 링크를 표시하려면 다음을 충족해야 합니다.

- defect-`<defectId>`.htm 이라는 명명 규칙으로 지정된 이름의 파일이 있어야 합니다.
- 이 파일은 additionalDefectDetailFileLocation 속성에 지정된 디렉터리에 배치해야 합니다.

예를 들어 이 파일이 MOM

`<EM_Home>/cem/tess/additionaldefectdetails/defect-600000000000000026.htm`에 있으면 해당 페이지에 대한 링크가 결함 번호 600000000000000026의 결함 정보 페이지에 나타납니다.

HTML 파일에 대한 읽기 권한이 있는 경우 "추가 결함 정보" 링크를 클릭하면 HTML 페이지가 나타납니다.

중요! 오래된 defect-`<defectId>`.htm 파일을 삭제하는 스크립트를 작성합니다. 이러한 파일은 결함이 완료 처리될 때 자동으로 삭제되지 않습니다.

additionalDefectDetailFileLocation

defect-<DefectID>.htm 이라는 파일이 MOM 의 이 디렉터리에 있는 경우 파일에 대한 링크가 결함에 대한 결함 세부 정보 페이지 아래쪽에 나타납니다.

클러스터 환경의 경우

- 디렉터리가 MOM 에 있어야 합니다.
- MOM 의 *tess-customer.properties* 파일이나 *tess-default.properties* 파일에서 additionalDefectDetailFileLocation 속성을 읽습니다.

옵션

디렉터리 경로입니다. 절대 경로 또는 MOM <EM_Home>을 기준으로 한 상대 경로일 수 있습니다.

기본값

cem/tess/additionaldefectdetails

예

C:\\test\\evidence_for_defects(Windows 예제)

/test/evidence_for_defects(UNIX 예제)

참고

백슬래시가 Windows 플랫폼에 사용되는 경우 단일 슬래시(/)가 이스케이프 시퀀스로 해석되므로 이중 슬래시(\\)가 필요합니다.

결함 처리 성능 개선

데이터베이스 쿼리를 통해 인시던트의 영향을 받는 사용자 그룹 수를 확인하는 경우 CPU 가 많이 소모될 수 있습니다. 인시던트에 많은 결함이 포함된 경우에 특히 그렇습니다. 영향을 받는 사용자 그룹을 쿼리하면 결함 처리가 지연될 수 있습니다. 이러한 지연은 쿼리 빈도를 낮춰서 줄일 수 있습니다.

기본적으로 affected-user-group 쿼리는 인시던트에 결함을 추가할 때마다 수행됩니다. 그러나 결함이 발견될 때마다 수행하는 대신에 특정 업데이트 간격에 따라 덜 자주 수행하도록 선택할 수 있습니다.

`affected-user-group` 쿼리가 특정 간격에 따라 수행되면 해당 간격 중에 현재 `affected-user-group` 수를 유지할 캐시가 생성됩니다. 업데이트 간격을 설정하는 것 외에도 *만료 처리 간격* 속성을 설정하여 캐시에서 유틸리티 인스턴트를 제거하는 빈도를 결정합니다.

참고: 이 쿼리 수행 빈도를 낮출 경우의 단점은 `affected-user-group` 수가 업데이트 간격의 길이만큼 오래되거나 드물지만 만료 처리 간격의 길이만큼 오래될 수도 있다는 것입니다. 그러나 결과적으로 결함 처리 성능이 개선된다면 약간 지연되는 수 계산을 감수하기에 충분할 것입니다.

affected-user-group 쿼리 빈도를 낮추려면

1. (선택 사항) 결함 처리 지연이 발생했는지 확인합니다.

예를 들어 "CEM" > "인스턴트 관리" > "결함"을 선택하고 모든 결함을 표시합니다. 결함이 예상된 시점에 도달하고 있습니까? 아니면 지연되고 있습니까?

2. [tess-default.properties 파일 수정](#) (페이지 581)에 나와 있는 절차를 따릅니다. 다음 속성의 값을 지정합니다.

- `defects.affectedUserGroupUpdateInterval_Secs`(업데이트 간격)
- `defects.affectedUserGroupAgeoutInterval_Mins`(만료 처리 간격)

예:

```
defects.affectedUserGroupUpdateInterval_Secs=180
defects.affectedUserGroupAgeoutInterval_Mins=10
```

업데이트 간격과 만료 처리 간격의 초기 값으로 각각 180 초와 10 분을 지정하는 것이 좋습니다. `affected-user-group` 쿼리로 인해 결함 처리가 지연되는 경우 이러한 값으로 성능을 개선할 수 있습니다.

이러한 속성에 대한 자세한 내용은

[defects.affectedUserGroupUpdateInterval_Secs](#) (페이지 587) 및 [defects.affectedUserGroupAgeoutInterval_Mins](#) (페이지 587)를 참조하십시오.

defects.affectedUserGroupUpdateInterval_Secs

인시던트와 관련된 영향을 받는 사용자 그룹 수에 대한 쿼리 간격(초)입니다.

옵션

초를 나타내는 숫자 값:

- 최소값인 0 을 지정하면 결함이 인시던트에 추가될 때마다 affected-user-group 쿼리가 수행됩니다.
- 최대 권장 값은 3600(1 시간)입니다.

기본값

0

예

defects.affectedUserGroupUpdateInterval_Secs=180

참고

보고된 affected-user-group 수는 간격 값에 해당하는 길이만큼 오래되거나, 드물지만 만료 처리 간격의 길이만큼 오래될 수 있습니다.

defects.affectedUserGroupAgeoutInterval_Mins

이 값보다 오래 유휴 상태(업데이트되지 않은 상태)로 남아 있는 인시던트는 affected-user-group 캐시에서 제거(만료 처리)됩니다.

옵션

분을 나타내는 숫자 값:

- 최소값. 만료 처리 간격을 업데이트 간격 값의 2 배가 넘는 값으로 설정하십시오. 그렇지 않으면 경고가 IntroscopeEnterpriseManager 로그에 나타나고 값이 업데이트 간격의 2 배로 다시 설정됩니다.
- 최대 권장 값은 121 분(2 시간을 약간 초과한 값)입니다.

기본값

1

예

defects.affectedUserGroupAgeoutInterval_Mins=10

참고

이 값은 업데이트 간격 값의 2 배 이상이어야 하지만 4 배를 초과해서는 안 됩니다. 예를 들어 업데이트 간격이 180 초인 경우 만료 처리 간격은 7 분에서 11 분 사이여야 합니다.

인시던트가 캐시에서 제거되면 `affected-user-group` 쿼리가 실행되고 인시던트의 `affected-user-group` 수가 업데이트됩니다. 따라서 수가 만료 처리 간격보다 오래되지 않습니다.

잘못된 파일의 디렉터리 위치 변경

기본적으로 TIM 에서 Enterprise Manager 로 전송된 데이터 파일은 다음 디렉터리에 저장됩니다.

- `cem/tess/badfiles` - 이 디렉터리에는 문제로 인해 처리할 수 없는 파일이 배치됩니다. 파일이 이 디렉터리로 이동한 시기는 로그 파일에서 보고됩니다. 이 디렉터리의 파일은 자동으로 삭제되지 않습니다. 이 디렉터리의 파일이 많을 경우 수동으로 삭제하십시오.

[tess-default.properties 파일 수정](#) (페이지 581)을 통해 이러한 디렉터리를 변경할 수 있습니다.

다음은 이러한 디렉터리를 구성해야 하는 이유입니다.

- 디스크 공간 문제로 인해 디렉터리를 더 큰 드라이브로 이동해야 하는 경우
- Enterprise Manager 간에 TIM 수집 서비스를 이동하는 경우 두 Enterprise Manager 모두의 `tess-customer.properties` 파일이 동일한 세 번째 컴퓨터의 동일한 디렉터리를 가리키면 TIM 수집 서비스를 이동해도 데이터가 손실되지 않습니다.

기본적으로 TIM 수집 서비스를 다른 Enterprise Manager 로 이동한 경우 해당 서비스를 원래 Enterprise Manager 로 다시 이동하지 않으면 원래 Enterprise Manager 에 처리되지 않은 상태로 남아 있는 데이터 파일이 처리되지 않습니다.

collectors.badDataDirectory

오류가 포함되어 처리되지 않는 파일이 이 디렉터리로 이동됩니다.

옵션

디렉터리 경로입니다. 상대 경로인 경우 <EM_Home>을 기준으로 합니다. 절대 경로를 지정하는 경우에는 있는 그대로 사용됩니다.

기본값

cem/tess/badfiles

예

collectors.badDataDirectory=cem/TIMdatafiles/badfiles

collectors.badDataDirectory=/tmp/badfiles

collectors.badDataDirectory=N:\\cem\\badfilesfromtess

collectors.badDataDirectory=\\\\server2\\c\$\\cem\\tess\\badfiles

참고

백슬래시가 Windows 플랫폼에 사용되는 경우 단일 슬래시(\)가 이스케이프 시퀀스로 해석되므로 이중 슬래시(\\)가 필요합니다.

디렉터리가 없는 경우 자동으로 생성됩니다.

기타 CA CEM 기본 속성

이 항목에서는 기타 <wcem> 기본 속성에 대한 정보를 제공합니다.

[baseline.durationInDays](#) (페이지 589)

[BTStatsMetricName.backwardCompatible](#) (페이지 590)

[email.defaultFromAddress](#) (페이지 591)

[invalid.importexport.filename.chars](#) (페이지 591)

[timTessCommunication.useSsl](#) (페이지 592)

baseline.durationInDays

기준 계산에 사용할 매시간 데이터의 기간(일)입니다.

기본값은 28 입니다. 이는 기준 계산이 지난 28 일 동안 수집된 매시간 데이터를 기반으로 함을 의미합니다.

사용법 예제: CA CEM 에서 10 일 동안 데이터를 수집해 왔지만 처음 3 일은 트랜잭션 정의를 실험하고 변경하느라 데이터가 유효하지 않음을 알고 있는 경우 값을 7 로 설정합니다. 나중에 더 긴 기간의 유효한 데이터가 수집되면 이 값을 늘립니다.

옵션

숫자 값

기본값

28

예

`baseline.durationInDays=7`

참고

대부분의 경우 모니터링되는 트랜잭션의 일반 비즈니스 주기가 1 주이므로 7 의 배수를 사용하십시오.

기준에 대한 일반 정보는 *CA APM 트랜잭션 정의 안내서*를 참조하십시오.

BTStatsMetricName.backwardCompatible

대상: CA CEM 5.0 및 4.5 호환성

CA CEM 5.0 에서는 "비즈니스 프로세스"라는 용어가 "비즈니스 서비스"로 변경되었습니다. 이 속성을 설정하면 CA CEM 4.5 대시보드 메트릭 이름을 고객 경험 메트릭에 계속 사용할 수 있습니다.

옵션

true 또는 false

true 인 경우 CA CEM 4.5 의 메트릭 이름인 "비즈니스 프로세스"가 사용됩니다.

false 인 경우에는 "비즈니스 서비스"라는 이름이 사용됩니다.

기본값

false

예

`BTStatsMetricName.backwardCompatible=false`

참고

이 설정을 `true` 로 변경하는 경우에는 CA CEM 4.5 의 Javascript 계산기를 사용해야 합니다.

email.defaultFromAddress

Embedded Entitlements Manager 가 인증에 사용되지 않았거나 사용자의 전자 메일 주소가 Embedded Entitlements Manager 에서 지정되지 않았으면 이 주소가 SMTP 서버 설정을 테스트하는 데 사용되고 경우에 따라 전자 메일로 보내는 보고서의 보낸 사람 주소로도 사용될 수 있습니다.

옵션

유효한 전자 메일 주소

기본값

`support@catechnologies.com`

예

`email.defaultFromAddress=my.email@company.com`

참고

이 속성을 사용하면 해당 속성이 "시스템" > "전자 메일 설정" 페이지의 "보낸 사람 주소" 및 "받는 사람" 필드에 나타납니다.

invalid.importexport.filename.chars

내보낸 비즈니스 서비스 이름에 사용할 수 있는 특수 문자를 지정합니다.

옵션

Linux 파일 이름에서 허용되지 않는 특수 문자입니다.

기본값

`/\ : * ? < > & ; |`

예

`invalid.importexport.filename.chars=/\ : * ? < > & ; |`

참고

비즈니스 서비스를 내보낼 때 내보내기 파일의 이름은 비즈니스 서비스의 이름을 기반으로 합니다. 파일 이름에 사용할 수 없는 문자가 포함되어 있으면 내보내기가 실패합니다.

실패를 방지하려면 그러한 문자가 이 속성 목록에 있는지 확인하십시오. 내보내기 파일이 생성될 때 해당 문자가 밑줄로 대체됩니다. 예를 들어 my&BP 라는 비즈니스 서비스를 내보내는 경우 내보내기 파일 이름은 BTEExport_my_BP_<timestamp>.zip 입니다.

timTessCommunication.useSsl

Enterprise Manager/TIM 통신이 HTTP 를 통해 이루어지는지 아니면 HTTPS 를 통해 이루어지는지 결정합니다.

옵션

0 또는 1

0 인 경우 Enterprise Manager/TIM 통신이 HTTP 를 통해 이루어집니다.

1 인 경우 Enterprise Manager/TIM 통신이 HTTPS 를 통해 이루어집니다.

기본값

0

예

```
timTessCommunication.useSsl=1
```

참고

이 속성은 tess-default.properties 파일에 없으므로 tess-customer.properties 파일에 추가해야 합니다.