CA Application Performance Management

보안 안내서

릴리스 9.5

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/worldwide에서 기술 지원팀에 문의하십시오.

목차

제 1 장: CA APM 보안 개요

이 장에서는 보안 및 CA Technologies Application Performance Management(CA APM) 보안 옵션을 설명할 때 사용하는 용어를 소개합니다.

이 섹션은 다음 항목을 포함하고 있습니다.

CA APM 보안 요약

CA APM 에서는 CA Introscope 및 CA CEM 의 보안을 위해 다음과 같은 보안 메커니즘을 사용합니다.

- Introscope 및 CA CEM 에 대한 사용자와 그룹 기반 인증 및 권한 부여 액세스:
  - *users.xml* 파일을 사용한 파일 기반 로컬 보안

    자세한 내용은 로컬 보안을 사용한 Introscope 보안 (페이지 36) 및 CA CEM 의 로컬 인증 및 권한 부여 (페이지 148)를 참조하십시오.
  - LDAP

    자세한 내용은 LDAP 를 사용한 Introscope 보안 (페이지 51)을 참조하십시오.

- CA EEM

  자세한 내용은 CA EEM 을 사용한 Introscope 보안 (페이지 64) 및 CA CEM 에 대한 CA EEM 인증 및 권한 부여 (페이지 137)를 참조하십시오.

  참고: CA APM 은 EEM 8.4 SP4 SDK 를 제공하며, EEM 서버 버전 8.4 SP4 이상에서 인증되었습니다.

  또한 CA Support 사이트에서 다운로드할 수 있도록 CA EEM 응용 프로그램에 포함된 다음 CA EEM 안내서도 참조하십시오.

  - *CA Embedded Entitlements Manager Getting Started Guide(CA Embedded Entitlements Manager 시작 안내서)*
  - *CA Embedded Entitlements Manager Release Notes(CA Embedded Entitlements Manager 릴리스 정보)*

- Enterprise Manager 보안:
  - MOM(Manager of Manager) 및 Collector 간의 보안 인증을 위한 공개 및 개인 키
    자세한 내용은 보안 인증에 대해 공개 및 개인 키 구성 (페이지 31)을 참조하십시오.
  - Enterprise Manager 에 대한 연결을 보호하는 데 필요한 사용자 권한 부여

    자세한 내용은 Introscope 의 보안 검사법 (페이지 35)을 참조하십시오.
  - 난독 처리된 Collector 및 MOM 간 통신
  - Enterprise Manager 및 브라우저 간의 보안 통신을 위한 구성 속성

    자세한 내용은 HTTPS 로만 Enterprise Manager 액세스 제한 (페이지 164) 및 *CA APM 구성 및 관리 안내서*의 *Enterprise Manager 웹 서버 구성*을 참조하십시오.
  - 에이전트 및 Enterprise Manager 간의 보안 통신을 위한 구성 속성

    자세한 내용은 *CA APM Java Agent 구현 안내서* 또는 *CA APM .NET 에이전트 구현 안내서*를 참조하십시오.
  - 특정 사용자만 특정 Introscope 도메인을 볼 수 있도록 허용하는 구성 속성

    자세한 내용은 Introscope 도메인 정의 및 구성 (페이지 23) 및 Introscope 도메인 및 보안 정보 (페이지 34)를 참조하십시오.

- 특정 사용자만 특정 Enterprise Manager 를 종료할 수 있도록 허용하는 구성 속성

  자세한 내용은 Enterprise Manager 서버 권한 구성 (페이지 48)을 참조하십시오.

- 응용 프로그램 심사 맵에서 특정 사용자만 특정 비즈니스 서비스 및 프런트엔드를 볼 수 있도록 허용하는 구성 속성

  자세한 내용은 응용 프로그램 심사 맵 보안 (페이지 120)을 참조하십시오.

- 특정 사용자만 동적 계측을 수행할 수 있도록 허용하는 구성 속성

  자세한 내용은 domains.xml 에 Introscope 도메인 권한 구성 (페이지 44)을 참조하십시오.

- 특정 사용자만 스레드 덤프를 수행할 수 있도록 허용하는 구성 속성

  자세한 내용은 domains.xml 에 Introscope 도메인 권한 구성 (페이지 44)을 참조하십시오.

- CA CEM 보안:
  - TIM 이 설치된 Windows 또는 Linux 컴퓨터의 루트 암호 보호

    자세한 내용은 *CA APM 설치 및 업그레이드 안내서*의 *새 TIM 용 운영 체제 설치* 항목을 참조하십시오.

  - Enterprise Manager 및 TIM 간의 보안 통신을 위한 구성 속성

    자세한 내용은 HTTPS 를 통한 TIM 통신 구성 (페이지 163)을 참조하십시오.

  - APM 데이터베이스에서 암호화되고 FIPS 호환성을 충족하는 CA CEM 데이터 자세한 내용은 FIPS 140-2 호환 암호화 (페이지 160)를 참조하십시오.

- APM 데이터베이스 보안:
  - APM 데이터베이스를 위한 암호 보호

    자세한 내용은 *CA APM 설치 및 업그레이드 안내서*의 *PostgreSQL 데이터베이스 암호 변경* 항목을 참조하십시오.

  - Enterprise Manager 에 대한 보안 연결

    자세한 내용은 *CA APM 설치 및 업그레이드 안내서*에서 *tess-db-cfg.xml* 파일에 암호화된 암호를 설정하는 방법에 대한 정보를 참조하십시오.

- CA Introscope® 및 CA CEM 응용 프로그램 모니터링:
  - 비즈니스 서비스 기반 보안에는 사용자 권한 부여가 필요합니다. 자세한 내용은 기본 CA EEM CEM 액세스 정책 (페이지 142) 및 *CA APM 구성 및 관리 안내서*를 참조하십시오.

CA APM 보안 및 권한 개요

'CA APM 보안'은 인증 및 권한 부여로 구성되며, 이를 통해 개별 사용자 및 사용자 그룹은 Introscope 및 CA CEM 에 안전하게 로그인할 수 있습니다. 여기서 사용자 그룹이란 응용 프로그램 관리자, 시스템 관리자, 분석가 등 지정된 사용자 집합을 말합니다. '권한'은 사용자 및 그룹이 특정 Introscope 작업을 수행할 수 있도록 허용하는 기준이 됩니다.

사용자 인증 정보

*인증*이란 안전하게 사용자를 식별하는 메커니즘으로, 다음 질문에 대한 답을 Introscope 및 CA CEM 에 제공합니다.

- 이 사용자는 누구입니까?
- 이 사용자는 해당 사용자가 나타내는 그룹의 구성원이 맞습니까?

인증 시스템은 인증받는 개인과 인증 시스템만 알고 있는 고유 정보에 의존합니다. 즉, 인증 시스템은 사용자 ID 를 확인하기 위해 주로 사용자에게 고유 정보를 제공하도록 요청하고, 제공된 정보가 올바른지 인증 시스템에서 확인되면 해당 사용자는 인증된 사용자로 간주됩니다.

사용자 권한 부여 정보

*권한 부여*란 특정한 인증된 사용자가 시스템에 의해 제어되는 보안 리소스(예: 응용 프로그램, 페이지 및 데이터)에 대해 가질 수 있는 액세스 수준을 결정하는 메커니즘입니다. 다시 말해, 권한 부여는 사용자가 특정 리소스에 대한 작업을 수행할 수 있는 권한이 있는지를 확인하는 프로세스입니다.

*액세스 정책*은 지정한 유형의 리소스 집합에 대한 작업을 수행할 수 있도록 특정 사용자 또는 그룹에 권한을 부여합니다.

예를 들어 특정 개별 사용자에게는 데이터베이스에서 정보를 검색할 수는 있지만 데이터베이스에 저장된 데이터는 변경할 수 없는 권한을 제공하고, 다른 개별 사용자에게는 데이터를 변경할 수 있는 권한을 제공하도록 데이터베이스 관리 시스템을 설계할 수 있습니다. 권한 부여 시스템은 다음과 같은 질문에 대한 답을 제공하는 방식으로 이와 같은 권한을 부여합니다.

- 사용자 *X* 는 리소스 *R* 에 액세스할 수 있는 권한이 있습니까?
- 사용자 *X* 는 작업 *P* 를 수행할 수 있는 권한이 있습니까?
- 사용자 *X* 는 리소스 *R* 에 대해 작업 *P* 를 수행할 수 있는 권한이 있습니까?

보안 영역 정보

보안 영역은 인증, 권한 부여 또는 사용자 인증 및 사용자 권한 부여를 담당하는 액세스 정책, 사용자, 사용자 그룹의 원본을 정의합니다.

CA APM 보안을 위해 *realms.xml* 파일에 하나 이상의 보안 영역을 구성할 수 있습니다. Introscope 및 CA CEM 은 *realms.xml* 에 구성된 보안 영역을 사용하여 사용자 인증 및 권한 부여 방법을 결정합니다. 사용자가 Introscope 또는 CA CEM 에 로그인하면 로그인하는 응용 프로그램은 realms.xml 에 정의된 순서로 각 보안 영역을 검사합니다. 응용 프로그램은 특정 ID 를 갖는 사용자가 존재하는지 검사합니다. 입력한 사용자 암호가 특정 보안 영역에 대해 제공된 값과 일치하는 경우 인증이 성공합니다. 다음 조건 중 하나에 해당하는 경우 인증이 실패합니다.

- 정의된 모든 영역에서 해당 이름의 사용자를 찾을 수 없는 경우
- 영역에 해당 사용자가 있지만 암호가 틀린 경우

realms.xml 에 영역을 구성하는 방법에 대한 자세한 내용은 다음 항목을 참조하십시오.

- realms.xml 에 로컬 인증 구성 (페이지 38)
- realms.xml 에 LDAP 인증 구성 (페이지 52)
- realms.xml 에 CA EEM 인증 구성 (페이지 69)

지원되는 방식으로 다음 세 보안 영역을 조합하여 Introscope 보안을 배포할 수 있습니다.

- **로컬 XML 파일(로컬):** 로컬 보안은 Enterprise Manager 의 *<EM_Home>/config* 디렉터리에 저장된 XML 파일을 사용하는 로컬 인증 및 권한 부여로 구성됩니다.
  - 로컬 인증의 경우 XML 파일은 각 Enterprise Manager 에 사용자 이름과 암호 정보를 로컬로 저장하는 데 사용됩니다. 기본 파일 이름은 *users.xml* 입니다. Introscope 는 런타임에 로컬 파일(*users.xml*)을 확인하여 CA APM 사용자를 인증합니다.
  - 로컬 권한 부여의 경우 Introscope 는 두 XML 파일을 각 Enterprise Manager 에 로컬로 저장합니다. 이때 도메인 권한에는 *domains.xml* 이 사용되고, 서버 권한에는 *server.xml* 이 사용됩니다. Introscope 는 런타임에 로컬 파일(*domains.xml* 및 *server.xml*)을 확인하여 CA APM 사용자에게 권한을 부여합니다.

  Introscope 에서는 기본적으로 로컬 보안이 제공 (페이지 36)됩니다.

  중요: Workstation, WebView, Web Start Workstation 또는 CEM 콘솔에서 Enterprise Manager 로 기본 CA APM 로그인을 변경하는 것이 권장됩니다. 이 권장 사항을 따르지 않고 Introscope 로컬 보안만 사용하는 경우 아이덴티티 도용의 가능성이 높아집니다. 이러한 이유로 CA EEM 은 권장되는 보안 메커니즘입니다 (페이지 19).

- **LDAP(Lightweight Directory Access Protocol):** TCP/IP 를 통해 실행되는 디렉터리 서비스를 쿼리 및 수정하는 응용 프로그램 프로토콜입니다.

  인증을 위해 로컬 XML 파일을 사용하는 경우 LDAP 보안 영역을 사용해서만 CA APM 사용자를 인증할 수 있습니다. 자세한 내용은 LDAP 를 사용한 Introscope 보안 (페이지 51)을 참조하십시오.

- **CA EEM(CA Embedded Entitlements Manager):** 다른 응용 프로그램이 공통 액세스 정책 관리, 인증 및 권한 부여 서비스를 공유할 수 있게 해 주는 CA Technologies 응용 프로그램입니다.

  참고: CA EEM 보안은 Introscope 에서 선택 사항이지만 CA Technologies 는 여러 이유로 Introscope 보안을 위해 CA EEM 을 권장합니다. CA EEM 은 업계 표준 솔루션, 사용자 관리를 위한 사용자 인터페이스, 세부적인 권한 부여가 가능한 중앙화된 저장소를 제공합니다. Introscope 응용 프로그램 심사 맵에 보안을 적용하려면 CA EEM 을 배포하십시오.

  CA APM 사용자 인증과 권한 부여를 위해 CA EEM 을 배포할 수 있습니다.

  또한 인증에는 LDAP 를 사용하고 권한 부여에는 CA EEM 을 사용하도록 CA EEM 을 구성할 수도 있습니다. 자세한 내용은 LDAP 를 사용하여 CA EEM 인증 구성 (페이지 73)을 참조하십시오.

이 표는 Introscope 보안 영역이 지원하는 주요 기능을 나열합니다.

보안 영역이 지원하는 기능	CA EEM	LDAP	로컬
여러 Enterprise Manager 에 공유되는 중앙 보안 서버	예	예	아니요
보안 영역을 항상 사용 가능함	아니요	아니요	예 Enterprise Manager 에서 실행되므로 항상 사용 가능함
장애 조치(failover) 지원	예	예	해당 없음
SiteMinder 와 통합됨	예	아니요	아니요
세분화된 권한 지원? 다음과 같은 세부 권한 유형을 지원합니다. ■ 응용 프로그램 심사 맵 권한 ■ 비즈니스 서비스 기반 보안 ■ 유연한 CA CEM 권한	예	해당 없음	아니요
업계 표준 솔루션	예	예	아니요
감사 허용	예	예	아니요
사용자를 관리할 수 있는 사용자 인터페이스 제공	예	예	아니요

보안 영역이 지원하는 기능	CA EEM	LDAP	로컬
액세스 정책을 관리할 수 있는 사용자 인터페이스 제공	예	해당 없음	아니요

지원되는 방식으로 다음 두 보안 영역을 조합하여 CA CEM 보안을 배포할 수 있습니다.

- **로컬 XML 파일(로컬):** 로컬 보안은 Enterprise Manager 의 *<EM_Home>/config* 디렉터리에 저장된 XML 파일을 사용하는 로컬 인증 및 권한 부여로 구성됩니다.
  - 로컬 인증 및 권한 부여의 경우 XML 파일은 각 Enterprise Manager 에 사용자 이름과 암호 정보를 로컬로 저장하는 데 사용됩니다. 4 가지 기본 CEM 보안 그룹과 해당 그룹의 사용자도 이 파일에 정의됩니다. 기본 파일 이름은 *users.xml* 입니다. 권한 부여는 4 가지 기본 보안 그룹에 정의된 구성원 자격에 기반하여 확인됩니다. 런타임에 로컬 파일(*users.xml*)은 CA CEM 사용자의 인증 및 권한 부여에 사용됩니다.

  Introscope 에서는 기본적으로 로컬 보안이 제공됩니다.

- **CA EEM(CA Embedded Entitlements Manager):** 공용 액세스 정책 관리, 인증 및 권한 부여 서비스를 서로 다른 응용 프로그램 간에 공유할 수 있도록 하는 CA Technologies 응용 프로그램입니다.

  참고: CA Technologies 는 여러 이유로 CA APM 보안을 위해 CA EEM 을 권장합니다. CA EEM 은 업계 표준 솔루션, 사용자 관리를 위한 사용자 인터페이스, 세부적인 권한 부여가 가능한 중앙화된 저장소를 제공합니다.
  - CA APM 사용자 인증과 권한 부여를 위해 CA EEM 을 배포할 수 있습니다.
  - CA SiteMinder 를 사용하여 CA EEM 인증을 구성 (페이지 74)하고 인증에 위해 CA EEM 을 구성합니다.
  - 인증에만 CA EEM 을 구성하고 권한 부여를 위해 로컬 XML 파일을 구성 (페이지 117)합니다.

  CA EEM 에 대한 자세한 내용은 CA EEM 을 사용한 Introscope 보안 (페이지 64)을 참조하십시오.

CA APM 은 단일 로그인 기능을 제공합니다. CA CEM 및 Introscope 모두에 액세스할 수 있는 사용자는 다시 로그인할 필요 없이 두 응용 프로그램 사이에서 이동할 수 있습니다. CA CEM 또는 Introscope 사용자 인증 시 CA APM 은 사용자 아이덴티티 및 이 사용자를 인증한 영역의 이름을 획득합니다. Introscope 는 이 정보를 사용하여 사용자가 속한 그룹을 확인합니다. 그런 다음 CA APM 은 다음 방법 중 하나를 사용하여 사용자를 인증합니다.

- CA EEM 의 경우, 사용자 액세스 정책
- 로컬 보안의 경우, 하나 이상의 CA CEM 보안 사용자 그룹의 구성원 자격

CA APM 보안을 설정할 때 조직에서는 단일 보안 영역을 배포할지, 아니면 혼합 보안 영역을 사용할지 결정해야 합니다. CA APM 사용자가 Introscope 에 액세스할 수 있도록 하려면 로컬 또는 CA EEM 영역을 배포하십시오.

참고: CA Technologies 에서는 CA EEM 인증 및 권한 부여 모두를 배포할 것을 권장합니다. 자세한 내용은 CA EEM 을 사용하여 CA APM 을 보호하는 경우의 이점 (페이지 19)을 참조하십시오.

CA EEM 을 사용하여 CA APM 을 보호하는 경우의 이점

CA Technologies 에서는 CA APM 보안을 위해 다음 기능을 제공하는 CA EEM 을 배포할 것을 권장합니다.

- 사용자 ID 와 액세스 정책을 관리하는 방식이 서로 공통적이고 공유됨
- 중앙 집중식 CA APM 보안

  CA EEM 인증을 사용하면 여러 Enterprise Manager 에서 동일한 CA EEM 서버를 공유할 수 있으므로 중앙 집중식 CA APM 보안을 배포할 수 있습니다.

- 효과적인 액세스 및 권한 액세스 관리
  - 액세스 정책을 사용하여 어느 CA CEM 보안 그룹이 비즈니스 서비스 및 관련 데이터에 대한 액세스 권한을 보유할지를 제어하는 비즈니스 서비스 기반 보안입니다.
  - 응용 프로그램 보안은 액세스하는 사용자와 액세스 대상 응용 프로그램을 제어하는데만 제한될 수 없습니다. 효과적으로 사용하려면 각 사용자가 액세스 권한을 얻은 후 응용 프로그램 내의 리소스에서 수행할 수 있는 작업을 보안 정책을 통해 제어해야 합니다. CA EEM 은 조직 고유의 비즈니스 응용 프로그램 포트폴리오에 맞게 유연하고 정밀한 권한 부여 정책을 구현할 수 있도록 지원하는 표준 방법을 제공합니다.
  - 메모리에 로드된 권한 부여의 경우 권한 정책이 응용 프로그램의 Embedded Entitlements Client 부분에 안전하게 캐시되었는지를 확인하고 평가한 다음 응용 프로그램 내에서 로컬로 실행합니다. 이를 통해 오프라인 응용 프로그램에도 액세스 정책을 적용할 수 있습니다.
  - 응용 프로그램별 정책 분리
    CA EEM 은 응용 프로그램을 유연하게 관리하면서 정책과 관리 제어를 개별적으로 수행할 수 있도록 중앙 저장소에서 응용 프로그램별로 정책 데이터를 분리합니다.
- 단일 ID 저장소

  CA EEM 에 포함된 저장소는 사용자 ID 의 신뢰할 수 있는 단일 출처로 사용될 수 있습니다. 또한 이 단일 출처를 Microsoft Active Directory, Novell eDirectory, SunONE Directory 등과 같은 외부 디렉터리로 설정하는 대체 방법도 있습니다.

- 엔터프라이즈 통합

  CA EEM 을 다른 CA 보안 솔루션과 함께 배포하여 복잡한 비즈니스 응용 프로그램 집합군 전체에서 IAM(Identity and Access Management) 작업을 일관되게 수행할 수 있습니다. 이를 수행하려면 CA EEM 과 같이 적응이 빠르고, 유연하며, 관리 가능하고, 현재 개발 환경에서 사용할 수 있는 보안 도구가 필요합니다.

  - CA SiteMinder 통합

    Embedded Entitlements Client 응용 프로그램이 CA SiteMinder 와 기본적으로 통합되면 CA SiteMinder 에서 사용할 수 있도록 구성된 사용자 저장소의 사용자 및 그룹 정보에 액세스하고, CA SiteMinder 자격 증명을 사용하여 인증하며, CA SiteMinder 웹 응용 프로그램에 SSO(Single Sign-On)를 지원할 수 있습니다.

  - C#, C++ 및 Java 로 구성된 SDK

    CA EEM 은 C#, C++ 및 Java 의 개발 환경을 지원하므로 C#, C++ 및 Java 참조 문서로 인증, 권한 부여, 이벤트 관리 및 관리 API 를 완전히 문서화할 수 있습니다. 여기에는 샘플 코드와 XML 스크립트, 그리고 보안 기능을 응용 프로그램에 포함하는 방법에 대한 자습서가 포함되어 있습니다.

- 관리 웹 UI

  CA EEM 은 웹 기반의 단일 관리 인터페이스를 제공하므로 응용 프로그램 보안 정책, 사용자 저장소 및 감사 규칙을 수립하고 유지 관리하는 비용을 최소화합니다. 보안 정책 관리를 응용 프로그램 자체에서 수행하지 않고 외부화하므로 비즈니스 요구 사항이 증가함에 따라 응용 프로그램 코드를 다시 개발할 필요 없이 보안 수준을 일관되게 유지 관리할 수 있습니다.

  - 공유 웹 UI

    CA EEM 은 사용자 및 그룹을 관리하거나 액세스 정책을 정의 및 관리하는 데 바로 사용할 수 있는 웹 UI 를 제공하며, 이 UI 는 모든 응용 프로그램 간에 공유됩니다. 또는 CA EEM SDK 를 사용하여 관리 UI 구성 요소를 사용자 지정 웹 페이지에 포함할 수 있습니다.

- 관리 범위

  특정 응용 프로그램, 사용자, 리소스 또는 정책만 보거나 작업할 수 있도록 관리자 권한을 제한할 수 있습니다.

- 권한 검사

  보안 정책을 활성화하기 전에 원하는 결과가 도출되는지 확인하기 위해 보안 정책을 테스트하고 세부적인 정책 디버그 정보를 볼 수 있습니다.

제 2 장: Introscope 도메인 정의 및 구성

이 장에서는 Introscope 보안을 설정하기 전에 Introscope 도메인을 정의 및 구성하는 방법에 대해 설명하며 MOM, 수집기 및 Workstation 간의 보안 인증을 위한 공개 키 및 개인 키 설정 관련 정보도 제공합니다.

이 섹션은 다음 항목을 포함하고 있습니다.

Introscope 도메인 정의 및 구성

Introscope 는 도메인을 사용하여 에이전트와 모니터링 논리를 분할하고 어떤 CA APM 사용자가 어떤 정보를 볼 수 있는지를 정의합니다. 이때 *<EM_Home>/config* 디렉터리에 있는 *domains.xml* 파일에서 Perl5 정규식을 사용하여 Introscope Agent 를 도메인에 매핑합니다. 사용하는 보안 영역이 무엇이든 도메인은 *domains.xml* 파일을 사용하여 정의합니다.

Introscope 보안을 설정할 때는 도메인 구성과 더불어 도메인 권한도 구성합니다. 로컬 보안의 경우 도메인 권한은 *domains.xml* 파일에 구성합니다. 자세한 내용은 domains.xml 에 Introscope 도메인 권한 구성 (페이지 44)을 참조하십시오. Introscope 보안을 위해 CA EEM 을 배포한 경우 Enterprise Manager 는 *domains.xml* 의 도메인 권한을 무시하므로 대신 CA EEM 에 도메인 권한을 구성해야 합니다. 자세한 내용은 CA EEM APM 도메인 리소스 액세스 정책 만들기 및 삭제 (페이지 104)를 참조하십시오.

도메인 유형

Introscope 에는 다음 2 가지 유형의 도메인이 있습니다.

- *SuperDomain* - *SuperDomain* 은 시스템에 있는 사용자 정의 도메인을 모두 포함하는 상위 집합 도메인입니다. 모든 에이전트가 *SuperDomain* 에 표시될 수 있지만 사용자 정의 도메인에도 나타날 수 있습니다. 기본 Introscope 구성에는 *SuperDomain* 만 포함되며, 다른 도메인을 구성하지 않을 경우 모든 에이전트는 *SuperDomain* 에 매핑됩니다.
- 사용자 정의 도메인 - *<EM_Home>/config* 디렉터리의 *domains.xml* 파일에 새 도메인을 정의할 수 있습니다. *domains.xml* 파일을 통해 도메인 이름을 정규식에 매핑할 수 있습니다.

도메인 정의 규칙

domains.xml 파일에서 도메인을 정의하는 규칙은 다음과 같습니다.

- 정의하는 도메인은 유효한 XML 파일 규칙을 따라야 합니다.
- 도메인 이름은 대/소문자를 구분합니다.
- 모든 도메인은 루트 XML 도메인의 요소 내에 배치해야 합니다.
- 하나의 *도메인* 또는 *SuperDomain* 에는 여러 에이전트 매핑이 있을 수 있습니다. *도메인*을 에이전트와 일치하도록 구성하면 해당 에이전트는 *도메인*에 매핑되고 *SuperDomain* 에 표시됩니다.

  참고: 트랜잭션 추적을 시작하는 경우 해당 에이전트는 트랜잭션 추적 창의 사용자 정의 도메인에 연결됩니다.
- 에이전트는 항상 할당된 첫 번째 도메인에 매핑됩니다. 도메인이 할당되지 않은 경우 에이전트는 *SuperDomain* 에 매핑됩니다. 할당된 사용자 정의 도메인이 있으면 에이전트는 사용자 정의 도메인에 매핑됩니다.
- 현재 *SuperDomain 에이전트 매핑*(기본적으로 모든 에이전트와 일치하도록 구성됨)을 변경하지 않을 경우 Introscope 는 새로 정의된 도메인을 *<SuperDomain>* 태그 앞에 배치합니다.
- Introscope 는 *domains.xml* 파일의 정규식 오류 또는 기타 문제로 인해 어떤 매핑과도 일치하지 않는 에이전트를 *SuperDomain* 에 배치합니다.

모든 클러스터 전체와 클러스터 내에서 동일한 domains.xml 파일 사용

단일 클러스터 내에 MOM 및 Collector 를 배포하고 선택적으로 클러스터 전체에 CDV 를 배포하는 경우 다음 중요 domains.xml 규칙을 이해해야 합니다.

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.

도메인에 에이전트 정의 및 매핑

domains.xml 파일을 사용하여 도메인을 정의하고 에이전트를 도메인에 매핑해야 합니다.

다음 단계를 따르십시오.

1. *<EM_Home>/config* 디렉터리로 이동합니다.
2. *domains.xml* 파일을 엽니다.
3. 도메인 정의 규칙 (페이지 24)과 다음 속성을 사용하여 도메인을 정의합니다.

   name

   도메인의 이름입니다.

   이 속성의 규칙은 다음과 같습니다.

   - 영숫자와 _ 및 -만 사용할 수 있습니다.
   - 공백은 허용되지 않습니다.

   description

   도메인에 대한 간략한 설명입니다.

   따옴표를 제외한 모든 문자를 사용할 수 있습니다.

   참고: 모든 XML 태그는 대/소문자를 구분합니다.
4. 추가 도메인에 대해 3 단계를 반복합니다.
5. SuperDomain 매핑이 domains.xml 의 끝부분에 정의되어 있는지 확인하십시오. 이를 통해 domains.xml 은 에이전트를 SuperDomain 에 매핑하기 전에 에이전트를 특정 도메인에 매핑할 수 있습니다.

   예를 들어 다음 SuperDomain 매핑을 domains.xml 앞부분에 배치하면 XML 파일의 나머지 부분이 처리되기 전에 모든 에이전트가 SuperDomain 아래에 배치됩니다.

   ```
   <SuperDomain>
               <agent mapping="(.*)"/>
               <grant group="Admin" permission="full"/>
   </SuperDomain>
   ```

   이 SuperDomain 매핑을 domains.xml 의 끝부분에 배치하면 SuperDomain 은 일치하지 않는 모든 에이전트를 catch 합니다.

6. *domains.xml* 파일을 저장하고 닫습니다.
7. 새 도메인이 로드되도록 Enterprise Manager 를 다시 시작합니다.

참고: *domains.xml* 파일에 구문 오류나 기타 오류가 있으면 Enterprise Manager 가 시작되지 않습니다.

새 도메인용 domains.xml 구문

도메인에 대한 구문은 다음과 같습니다.

```
<domain name="Domainname" description="Domain description">
<agent mapping="host\|process\|agentname or matching agents"/>
<grant user="username" permission="permission"/>
</domain>
```

관리 모듈을 도메인에 연결

새 관리 모듈을 만들 때 모듈이 속할 도메인을 선택할 수 있습니다.

관리 모듈을 도메인에 연결하려면 *domains.xml* 에 정의한 도메인과 이름이 동일한 디렉터리를 만든 다음 관리 모듈을 해당 새 디렉터리로 이동합니다.

다음 단계를 따르십시오.

1. *<EM_Home>/config/modules* 디렉터리에 이전 섹션에서 만든 도메인 이름과 동일한 디렉터리를 만듭니다.

   예를 들어 이 단계에서 도메인 이름을 "PetstoreA"로 정의한 경우 다음과 같이 PetstoreA 라는 이름의 디렉터리를 만듭니다.

   <EM_Home>/config/modules/PetstoreA

   참고: 도메인 디렉터리는 *domains.xml* 파일에 정의한 이름과 정확히 일치해야 합니다. 철자와 대/소문자 모두 일치해야 하며, 일치하지 않는 경우 디렉터리에 위치한 관리 모듈이 로드되지 않습니다.
2. 원하는 관리 모듈을 *<EM_Home>/config/modules* 디렉터리에서 방금 만든 새 디렉터리로 이동합니다.
3. 새 도메인이 로드되도록 Enterprise Manager 를 다시 시작합니다.

새로 정의한 도메인에 샘플 관리 모듈 추가

새로 정의한 도메인에는 관리 모듈이 포함되어 있지 않습니다. 그러므로 새로 정의한 도메인에서 기본 샘플 대시보드를 표시하려면 해당 도메인에 샘플 관리 모듈을 복사해야 합니다.

다음 단계를 따르십시오.

1. *<EM_Home>/config/modules/* 디렉터리로 이동합니다.
2. 새로 정의한 도메인에 해당하는 모듈 디렉터리로 *SampleManagementModule.jar* 파일을 복사합니다.

   예를 들어 Petstore A 라는 도메인을 정의한 경우 *SampleManagementModule.jar* 파일을 다음 디렉터리로 복사합니다. *<EM_Home>*/config/modules/PetstoreA
3. 새 관리 모듈이 로드되도록 Enterprise Manager 를 다시 시작합니다.

중요! 새 도메인으로 복사한 샘플 관리 모듈은 원래 샘플 관리 모듈과 연결되어 있지 않습니다. 그러므로 원래 샘플 관리 모듈을 변경하는 경우 해당 변경 사항이 다른 도메인의 샘플 관리 모듈 복사본에 반영되지 않으며, 그 반대의 경우도 마찬가지입니다.

에이전트의 도메인 매핑 변경

도메인을 삭제하거나 두 도메인을 병합한 다음에 에이전트를 다른 도메인에 다시 매핑하는 경우 다음과 같은 영향이 나타납니다.

- 삭제된 도메인에 매핑된 에이전트가 다시 할당되지 않고 계속 보고되는 경우 *SuperDomain* 에 나타납니다.
- 에이전트가 SNMP 수집에 연결된 경우 SNMP MIB 는 다시 게시되어야 합니다.
- 에이전트를 다른 도메인으로 이동하는 경우 해당 에이전트 내의 모든 종료 정보가 손실됩니다.

도메인 삭제

다음과 같은 경우 도메인을 삭제해야 할 수 있습니다.

- 에이전트를 다른 도메인에 할당
- 두 도메인을 병합

다음 단계를 따르십시오.

1. Enterprise Manager 를 종료합니다.
2. <EM_Home>/config 디렉터리로 이동합니다.
3. domains.xml 파일에서 도메인을 삭제합니다.
4. 필요한 경우 매핑한 에이전트를 다른 도메인에 다시 할당합니다.
5. <EM_Home>/config/modules 디렉터리에서 해당 도메인 디렉터리를 삭제합니다.
6. Enterprise Manager 를 다시 시작합니다.

두 도메인 병합

두 도메인을 병합하려면 모든 에이전트 매핑 정보를 한 도메인에 병합하고 연결된 관리 모듈도 모두 한 도메인으로 이동해야 합니다.

다음 단계를 따르십시오.

1. Enterprise Manager 를 종료합니다.
2. *<EM_Home>\config* 디렉터리에 있는 *domains.xml* 파일을 엽니다.
3. 원본 도메인(예: Domain A)에서 에이전트 매핑 XML 코드 정보를 복사합니다.
4. 대상 도메인(예: Domain B)으로 에이전트 매핑 XML 코드 정보를 붙여 넣습니다.
5. 원본 도메인(예: Domain A)에서 에이전트 매핑 XML 코드를 삭제합니다.
6. *<EM_Home>/config/modules/*의 원본 도메인(예: Domain A) 디렉터리에 있는 모든 관리 모듈을 대상 도메인(예: Domain B)으로 이동합니다.

   참고: 원본 도메인의 관리 모듈과 이름이 동일한 관리 모듈이 대상 도메인 디렉터리에 이미 있는 경우 원본 도메인의 관리 모듈 이름을 바꾸어야 합니다. 동일한 이름의 관리 모듈이 두 개 있으면 Enterprise Manager 가 시작되지 않습니다.
7. *domains.xml* 에서 원본 도메인을 삭제합니다.
8. Enterprise Manager 를 다시 시작합니다.

서로 다른 Introscope 간 도메인 복제

대상 설치 도메인 구성이 원본 설치 도메인 구성과 정확히 일치하는 경우 다음 절차를 수행합니다. 즉, *domains.xml* 파일에 정의된 모든 도메인이 정확히 동일해지는 경우에 해당합니다.

다음 단계를 따르십시오.

1. 원본 설치에 있는 *<EM_Home>/config/domains.xml* 파일을 대상 설치의 동일한 디렉터리에 복사합니다.
2. 원본 설치에 있는 경우 *<EM_Home>/config/shutoff/MetricShutoffConfiguration.xml* 을 대상 설치의 동일한 디렉터리에 복사합니다.
3. 원본 설치의 *<EM_Home>/config/modules/<domain>* 디렉터리에 있는 모든 콘텐츠를 대상 설치로 복사합니다.
4. Enterprise Manager 를 다시 시작합니다.

비복제 설치 간에 도메인 이동

비복제 설치 간에 도메인을 이동하는 경우 두 설치의 도메인 구성이 다소 다르면 다음 절차를 수행합니다.

다음 단계를 따르십시오.

1. 원본 설치의 *<EM_Home>/config* 디렉터리에 있는 *domains.xml* 파일을 엽니다.
2. 도메인 정보를 복사합니다.
3. 대상 설치의 *<EM_Home>/config* 디렉터리에 있는 *domains.xml* 파일을 엽니다.
4. 도메인 정보를 *domains.xml* 파일로 복사합니다.
5. 소스 설치의 *<EM_Home>/config/modules* 디렉터리에 있는 관리 모듈 디렉터리와 동일한 새 관리 모듈 디렉터리를 대상 설치에 만듭니다.
6. 원본 설치의 도메인에 속한 모든 관리 모듈을 복사하여 동일한 대상 도메인 디렉터리에 붙여 넣습니다.
7. 원본 설치에서 도메인을 삭제합니다.
8. Enterprise Manager 를 다시 시작합니다.

에이전트 장애 조치 및 사용자/도메인 구성

에이전트 장애 조치(failover) 기능을 사용하는 경우 사용자 및 암호가 정의되어 있으면 장애 조치(failover) 대상으로 지정된 모든 Enterprise Manager 에서 *domains.xml*, *server.xml* 및 *users.xml* 파일이 동기화되어야 합니다.

에이전트 장애 조치(failover)에 대한 자세한 내용은 *CA APM Java Agent 구현 안내서* 또는 *CA APM .NET 에이전트 구현 안내서* 중 환경에 맞는 안내서에서 *에이전트 장애 조치* 구성에 대한 내용을 참조하십시오.

보안 인증에 대한 공개 및 개인 키 구성

클러스터 환경에서 MOM, Collectors 및 Workstation 간의 통신 프로토콜은 보안 인증에 대해 공개 및 개인 키를 사용합니다.

참고: 공개 키 및 개인 키는 로그인할 때 암호를 보호하는 용도로만 사용됩니다. 모든 통신을 보호하려면 SSL 을 사용해야 합니다.

기본 Collector 개인 키 정보

각 Collector 는 MOM 에서 연결하는 데 사용하는 암호를 개인 키를 사용해 해독합니다. 공개 키와 개인 키 집합은 서로 연결된 하나의 집합입니다. Collector Enterprise Manager 의 개인 키는 *IntroscopeEnterpriseManager.properties* 파일의 *introscope.enterprisemanager.clustering.privatekey* 속성에 정의되어 있습니다.

기본값은 다음과 같습니다.

```
config/internal/server/EM.private
```

보안을 강화하기 위해 Collector 의 공개 및 개인 키 집합을 새로 생성하지 않는 한 개인 키를 다시 구성할 필요가 없습니다. 개인 키를 다시 구성하는 방법에 대한 자세한 내용은 새 공개 및 개인 키 집합 생성 (페이지 32)을 참조하십시오. *introscope.enterprisemanager.clustering.privatekey* 속성에 대한 자세한 내용은 *CA APM 구성 및 관리 안내서*를 참조하십시오.

참고: CA APM 공개 및 개인 키는 만료되지 않습니다.

새 공개 및 개인 키 집합 생성

CA APM 환경의 보안을 더 강화하기 위해 각 Collector 마다 새 공개 및 개인 키를 생성하고, MOM 에 공개 키를 배치하고, MOM 의 Collector 속성을 업데이트할 수 있습니다.

다음 단계를 따르십시오.

1. Introscope 설치 디렉터리로 이동합니다.
2. 명령 프롬프트에서 다음 명령을 입력합니다.

   ```
   java -classpath
   product\enterprisemanager\plugins\com.wily.introscope.em.client14_9.5.0.jar;l
   ib\CLWorkstation.jar;product\enterprisemanager\configuration\org.eclipse.osgi
   \bundles\24\1\.cp\lib\WilyBouncyCastle.jar
   com.wily.util.encryption.KeyGenerator EM.public EM.private
   ```

3. Collector 의 새 키를 생성하는 경우 MOM 의 *IntroscopeEnterpriseManager.properties* 파일에서 *introscope.enterprisemanager.clustering.login.em1.publicKey* 속성에 지정된 위치로 공개 키를 복사합니다.

   참고: MOM 에 대해 새 키를 생성하는 경우에는 이 단계가 적용되지 않습니다.

4. *<EM_Home>\config\internal\server* 의 Enterprise Manager 설치 위치로 공개 및 개인 키를 복사합니다.

제 3 장: Introscope 보안

이 장에서는 Introscope 보안 및 권한을 제공하기 위해 배포할 수 있는 인증 및 권한 부여 메커니즘을 구성하는 방법을 설명합니다. 응용 프로그램 심사 맵 보안 및 Introscope SSO 에 대한 설명도 있습니다.

이 섹션은 다음 항목을 포함하고 있습니다.

Introscope 보안 및 권한 개요

'Introscope 보안'은 인증 및 권한 부여로 구성되며, 이를 통해 개별 사용자 및 사용자 그룹은 Introscope 에 안전하게 로그인할 수 있습니다. 여기서 사용자 그룹이란 응용 프로그램 관리자, 시스템 관리자, 분석가 등 지정된 사용자 집합을 말합니다. '권한'은 사용자 및 그룹이 특정 Introscope 작업을 수행할 수 있도록 허용하는 기준이 됩니다.

Introscope 보안에 대한 배경 지식이 필요하면 CA APM 보안 요약 (페이지 11)을 참조하십시오.

Introscope 도메인 및 보안 정보

Introscope 는 도메인을 사용하여 에이전트와 관리 논리를 분할하고 어떤 사용자가 어떤 정보를 볼 수 있는지를 정의합니다. 에이전트는 Perl5 정규식을 사용하여 *domains.xml* 파일의 도메인에 매핑됩니다.

에이전트를 도메인에 매핑한 후 도메인 권한을 정의하고 부여합니다. 권한 부여 프로세스 동안 Introscope 는 권한 검사를 수행합니다.

Introscope 도메인 설정에 대한 정보는 Introscope 도메인 정의 및 구성 (페이지 23)을 참조하십시오.

Introscope 권한 구성 정보

Introscope 에서는 권한에 따라 Workstation 의 모니터링 논리 구성, Enterprise Manager 관리 작업 처리 등 사용자나 그룹에서 수행할 수 있는 작업이 결정됩니다. 도메인과 Enterprise Manager 에 사용할 Introscope 권한을 정의합니다. 그런 다음 사용자 및 그룹에게 도메인, Enterprise Manager 또는 둘 모두에 대한 권한을 부여합니다.

도메인 권한 및 Investigator 트리

Investigator 트리는 보유한 도메인 권한에 따라 사용자 또는 그룹에 다르게 나타납니다.

- *SuperDomain 권한*에 대해 읽기 권한 이상을 보유한 사용자 또는 그룹은 Investigator 트리에 정의된 모든 도메인의 콘텐츠를 볼 수 있습니다.
- 여러 도메인에 대한 권한이 있는 사용자 또는 그룹은 Investigator 트리에서 해당 도메인의 도메인 정보를 볼 수 있습니다.
- 사용자 또는 그룹은 하나 이상의 도메인에 대해 읽기 이상의 권한을 보유해야 합니다. 그렇지 않으면 Workstation 또는 WebView 에 로그인하여 Investigator 트리 및 콘솔을 볼 수 없습니다.

로컬 권한 부여에 대한 권한은 *domains.xml* 및 *server.xml* 을 사용하여 구성하고, CA EEM 권한 부여에 대한 권한은 Safex 도구나 CA EEM 사용자 인터페이스를 사용하여 구성합니다. 권한을 설정하는 방법에 대한 자세한 내용은 다음 항목을 참조하십시오.

- domains.xml 에 Introscope 도메인 권한 구성 (페이지 44)
- Enterprise Manager 서버 권한 구성 (페이지 48)
- CA EEM 권한 부여 구성 (페이지 75)
- 로컬 보안에서 CA EEM 보안으로 마이그레이션 (페이지 116)

Introscope 의 기본 보안 구성

Introscope 는 *realms.xml* 파일에서 기본 보안 구성을 제공합니다. 인증 및 권한 부여 모두에 사용되는 로컬 XML 파일(*<EM_Home>/config* 디렉터리에 위치)은 Introscope 의 기본 보안 영역입니다. 기본 보안 구성을 사용하려면 로컬 보안을 사용한 Introscope 보안 (페이지 36)을 참조하십시오.

Introscope 의 기본 보안 구성이 요구 사항을 충족하지 않는 경우 CA EEM, LDAP 또는 인증/권한 부여에 대해 지원되는 영역을 조합하여 사용하도록 *realms.xml* 을 구성할 수 있습니다.

예를 들어 다음과 같은 방법으로 Introscope 보안을 구성할 수 있습니다.

- 로컬 보안에 대한 기본 구성 설정 변경. 자세한 내용은 로컬 인증 구성 정보 (페이지 37)를 참조하십시오.
- 인증에 대한 로컬 보안 인증을 LDAP 서버로 바꾸기. 자세한 내용은 LDAP 를 사용한 Introscope 보안 (페이지 51)을 참조하십시오.
- 로컬 보안을 CA EEM 인증 및 권한 부여로 바꾸기. 자세한 내용은 CA EEM 을 사용한 Introscope 보안 (페이지 64)을 참조하십시오.

Introscope 가 보안을 검사하는 방법

Introscope 는 조직에서 구성한 보안 영역을 확인하면서 모든 보안 검사를 시작합니다. 예를 들어 SiteMinder 권한 부여와 함께 CA EEM 인증을 구현했거나 로컬 권한 부여와 함께 LDAP 인증을 구현했다는 것을 Introscope 가 감지하면 사용자의 보안 구현을 기반으로 적절한 보안 및 권한 검사를 수행합니다.

Introscope 의 일반적인 보안 및 권한 검사 프로세스는 다음과 같은 단계로 구성됩니다.

1. *realms.xml* 을 검사하여 보안 영역을 확인하고 일부 사용자 정보를 가져와 인증을 시작합니다.
2. LDAP 서버 또는 CA EEM 서버에서 *users.xml* 파일로 사용자, 그룹 및 사용자-그룹 매핑을 로컬로 가져와 인증을 마칩니다.

   참고: LDAP 서버와의 CA EEM 통합을 설정하면 인증에 대해 LDAP 를 사용하고 권한 부여에 대해 CA EEM 을 사용할 수 있습니다. 자세한 내용은 LDAP 를 사용하여 CA EEM 인증 구성 (페이지 73)을 참조하십시오.

   참고: SiteMinder 와의 CA EEM 통합을 설정한 경우 인증에 SiteMinder 를 사용하고 권한 부여에 CA EEM 을 사용할 수 있습니다. 자세한 내용은 CA SiteMinder 를 사용하여 CA EEM 인증 구성 (페이지 74)을 참조하십시오.
3. CA EEM 에서 또는 *users.xml* 파일에서 Enterprise Manager 로 암호를 로컬로 가져와서 권한 부여를 시작합니다.
4. *domains.xml* 및 *server.xml* 파일에서, 또는 CA EEM 에서 Enterprise Manager 의 도메인 및 Enterprise Manager 서버 권한을 로컬로 가져와 권한 부여를 마칩니다.

로컬 보안을 사용한 Introscope 보안

Introscope 보안에 대한 일부 배경 지식을 습득했으므로 이제 보안 배포를 계획할 준비가 완료되었습니다.

다음 단계를 따르십시오.

1. 필요한 경우 *realms.xml* 에서 로컬 영역을 보안 영역으로 구성합니다.

   참고: *realms.xml* 에서 로컬 영역이 Introscope 기본 영역입니다.
2. 암호와 함께 사용자 및 그룹을 *users.xml* 에 설정합니다.
3. *domains.xml* 에 도메인 권한을 할당합니다.
4. *server.xml* 에 Enterprise Manager 서버 권한을 할당합니다.
5. 필요한 경우 관련 권한과 함께 CA APM 그룹, 사용자, 도메인 및 서버를 추가, 삭제, 편집하여 Introscope 보안을 유지 관리합니다.

로컬 인증 구성 정보

Introscope 에서는 로컬 인증이 기본적으로 사용됩니다. 로컬 인증이 사용되는 경우 CA APM 사용자 및 암호는 *users.xml* 에 저장됩니다.

하지만 전자 메일 및 전화 번호와 같은 사용자 세부 정보는 로컬 영역에 유지되지 않습니다. 이름과 암호가 동일한 두 사용자는 로컬 영역에 유지할 수 없지만, 사용자 이름은 같지만 암호가 다른 두 사용자는 로컬 영역에 유지될 수 있습니다. 이름은 같지만 암호가 다른 두 사용자는 로컬 영역에서 별개의 두 사용자로 인식됩니다.

사용자, 그룹을 정의하고 암호를 생성하는 방법에 대한 자세한 내용은 users.xml 에 CA APM 사용자 및 그룹 구성 (페이지 40)을 참조하십시오.

로컬 인증 변경 사항은 동적으로 처리됩니다. CA APM 사용자가 로그인하려는 경우 인증 요청이 수신될 때마다 암호가 *users.xml* 파일과 비교됩니다.

이전 Introscope 설치의 Introscope 사용자를 마이그레이션하는 경우 마이그레이션이 완료될 때까지 *users.xml* 파일의 이름이나 위치를 변경하지 마십시오.

realms.xml 에 로컬 인증 구성

realms.xml 을 구성하는 경우 다음 규칙을 따라야 합니다.

중요! 다음 규칙 중 하나라도 충족되지 않은 경우 Enterprise Manager 가 시작되지 않습니다.

- *descriptor=*의 값은 대/소문자를 구분합니다.
  - 예를 들어 *descriptor=Local Users and Groups Realm* 은 *descriptor=local users and groups realm* 과 다릅니다.
- 로컬 영역의 경우 *descriptor=*의 값은 반드시 *Local Users and Groups Realm* 이어야 합니다.
- 여러 영역이 존재하는 경우 영역 태그의 *id=* 값은 각 영역마다 고유해야 합니다. 예:

```
<realm descriptor="EEM Realm" id="EEM" active="true">
        <property name="username">
          <value>EiamAdmin</value
        </property>
           <property name="host">
            <value>localhost</value>
        </property>
        <property name="appname">
            <value>APM</value>
        </property>
        <property name="enableAuthorization">
            <value>true</value>
        </property>
        <property name="plainTextPasswords">
            <value>false</value>
        </property>
        <property name="password">
            <value>YhCVozLDYThTJk3icaAaY9/5MhJRqQ1X</value>
        </property>
    </realm>
    <realm descriptor="Local Users and Groups Realm" id="Local Users and Groups"
active="true">
        <property name="usersFile">
            <value>users.xml</value>
        </property>
    </realm>
```

다음 단계를 따르십시오.

1. *<EM_Home>/config* 디렉터리에 있는 *realms.xml* 파일을 엽니다.
2. *realms.xml* 의 세 번째 항목으로 다음 행이 있는지 확인합니다.

   ```
   <realm active="true" descriptor="Local Users and Groups Realm" id="Local Users and Groups">
   ```

3. 다음 속성을 적절히 설정합니다.

   usersFile

   사용자가 저장된 파일 이름으로, *<EM_Home>/config* 디렉터리에 상대적입니다. 기본적으로 이는 *users.xml* 입니다.

   참고: 이 파일에는 그룹 정의도 포함되어 있습니다.

   참고: 보안 영역에 대해 여러 파일을 사용하는 방법에 대한 자세한 내용은 보안 영역에 여러 파일 사용 정보 (페이지 39)를 참조하십시오.

4. *realms.xml* 파일의 변경 사항을 저장하고, 변경 사항이 적용되도록 Enterprise Manager 를 다시 시작합니다.

로컬 인증을 사용하도록 설정한 realms.xml 구문

다음은 *realms.xml* 파일의 예제 코드입니다.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<realms xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" version="0.1"
xsi:noNamespaceSchemaLocation="realms0.1.xsd">
    <realm descriptor="Local Users and Groups Realm" id="Local Users and Groups"
active="true">
        <property name="usersFile">
            <value>users.xml</value>
        </property>
    </realm>
```

보안 영역에 대해 여러 파일 사용 정보

realms.xml 파일에서 모든 보안 영역에 대해 나열된 파일이 하나만 있으면 이 항목을 무시할 수 있습니다.

사용자에게 기본 권한을 부여하는 기본 영역 및 다른 권한을 부여하는 보조 영역을 구성하려는 경우와 같이 여러 영역을 설정할 수도 있습니다. 또는 조직에서 두 LDAP 서버를 구성하여 이들 모두의 보안을 테스트하려 하거나, 로컬 보안을 사용하던 조직이 CA EEM 으로 전환하면서 해당 구성을 유지하려 할 수도 있습니다.

realms.xml 의 보안 영역으로 2 개의 파일이 나열된 경우 인증 및 권한 부여 프로세스에 첫 번째 파일이 사용됩니다. 동일한 암호를 가진 User A 라는 두 사용자가 있는 경우 *realms.xml* 에 나열된 첫 번째 파일에서 찾은 암호를 사용합니다. 예를 들어 *CEM45.xml* 앞에 *users.xml* 이 나열되어 있는 경우 *realms.xml* 의 인증은 *users.xml* 의 암호를 사용하여 수행됩니다.

로컬 영역의 경우 전자 메일 및 전화 번호와 같은 사용자 정보는 *users.xml* 및 *CEM45.xml* 에 유지 관리되지 않습니다. 또한 로컬 영역은 동일한 이름 및 동일한 암호를 가진 두 사용자를 유지 관리할 수 없지만, 이름은 같지만 암호가 다른 두 사용자는 로컬 영역에 유지될 수 있습니다.

마찬가지로 *users.xml* 및 *CEM45.xml* 에서 서로 다른 사용자 그룹에 속한 User A 라는 두 사용자가 있는 경우 *realms.xml* 은 나열된 첫 번째 파일에서 찾은 사용자 그룹을 사용합니다. *users.xml* 이 *CEM45.xml* 앞에 나열되어 있는 경우를 예로 들어보겠습니다. *users.xml* 에 "CEM 시스템 관리자" 사용자 그룹의 Admin 이라는 사용자가 있고, *CEM45.xml* 에 "CEM 분석가" 사용자 그룹의 Admin 이라는 사용자가 있는 경우, *realms.xml* 은 *users.xml* 사용자 그룹을 사용하므로 "CEM 시스템 관리자" 사용자 그룹과 연결된 권한을 Admin 이라는 사용자에게 부여합니다.

users.xml 에 CA APM 사용자 및 그룹 구성

각 사용자 및 그룹마다 사용자 이름과 암호를 정의합니다.

참고: *admin* 사용자를 만들 때 사용자 및 권한에서는 대/소문자가 구분됨을 유의하십시오. 사용자가 로그인 이름 *admin* 또는 *Admin* 을 사용하여 로그인하는 경우 해당 사용자 역할에 대한 권한이 적용됩니다.

기본 CA APM 사용자 구성에는 다음 사용자가 정의됩니다.

- *Admin*(암호 지정 안 됨)
- *Guest*(암호는 *Guest*)

다음 단계를 따르십시오.

1. *<EM_Home>/config* 디렉터리로 이동합니다.
2. *users.xml* 파일을 엽니다.

3. 다음 사용자 및 그룹 명명 속성을 사용하여 사용자 이름을 정의합니다.

   참고: 모든 XML 태그는 대/소문자를 구분합니다.

   예를 들어, 사용자 및 그룹에 대한 구문은 사용자 관련 users.xml 구문 (페이지 43) 및 그룹 관련 users.xml 구문 (페이지 43)을 참조하십시오.

4. 다음 속성을 사용하여 각 사용자 또는 그룹의 암호를 설정합니다.

   참고: 모든 XML 태그는 대/소문자를 구분합니다.

   password

   사용자 암호입니다.

   이 속성에는 다음과 같은 규칙이 적용됩니다.

   - 따옴표를 제외한 모든 문자가 사용됩니다.
   - 기본적으로 암호는 암호화되며 일반 텍스트 또는 난독 처리된 텍스트(선택적으로 인코딩된 암호 생성 가능)로 사용되지 않습니다.
   - 유효한 XML 문자를 암호로 사용할 수 있습니다.
   - 암호 값을 비워 둘 수 있습니다.

   베스트 프랙티스: 각 조직의 암호 정책을 따르십시오.

   로컬 인증에 사용된 암호는 users.xml 파일에서 암호화된 상태로 저장됩니다. MD5Encoder 유틸리티를 사용하여 암호화된 암호를 생성하는 옵션 또는 Introscope 에서 자동으로 암호를 생성하는 옵션이 있습니다. Introscope 에서 제공하는 MD5 스크립트를 실행하면 입력된 일반 텍스트가 암호화된 형식으로 출력됩니다.

   - 아래 조건에 해당하는 경우 5 단계(수동으로 암호화된 암호 설정)의 지침을 따르십시오.
     - 이미 *users.xml* 에서 여러 사용자를 암호화했습니다.
     - 하나 또는 일부 암호만 변경하려고 합니다.
   - 그렇지 않으면 모든 사용자 암호를 일반 텍스트로 다시 변경해야 합니다.
   - 아래 조건에 해당하는 경우 6 단계(일반 텍스트 암호 설정)의 지침을 따르십시오.
     - 한 번에 많은 사용자 및 암호를 생성 또는 변경하려고 합니다.

5. 암호화된 암호를 수동으로 설정합니다.

   a. *users.xml* 파일에서 *plaintextPasswords="false"*를 설정합니다.

   b. *<EM_Home>/tools* 디렉터리에서 적합한 다음 스크립트를 실행합니다.

      - Windows 의 경우 *MD5Encoder.bat* <암호>
      - UNIX 의 경우 *MD5encoder.sh* <암호>

      참고: MD5Encoder.sh 스크립트를 실행할 때는 백슬래시를 사용하여 암호의 모든 특수 문자를 이스케이프하십시오. 예를 들어 암호가 *pa$word* 인 경우 달러 기호("$") 문자 앞에 백슬래시를 넣어야 스크립트가 올바르게 실행됩니다. 올바른 명령줄은 다음과 같습니다.
      ./MD5Encoder.sh pa\$word

   c. 생성한 암호화된 암호를 복사하여 users.xml 파일의 둘째 행에 붙여 넣습니다.

   예를 들면 다음과 같습니다.

   ```
   <user password="5b5ab9639b79259f54bc39515540aeaf" name="john"/>
   ```

   구문의 예제는 암호화된 암호를 사용한 users.xml 구문 (페이지 43)을 참조하십시오.

6. 일반 텍스트 암호를 설정하여 Introscope 에서 암호화된 암호가 자동으로 생성되게 합니다.

   a. *users.xml* 파일에 *plaintextPasswords="true"*를 설정합니다.

   중요! *plainTextPasswords="true"*로 설정하면 Introscope 가 모든 암호를 암호화합니다. 모든 암호를 일반 텍스트로 설정해야 하며 그러지 않으면 Introscope 가 이미 암호화된 암호를 암호화합니다.

   b. 모든 사용자의 암호를 일반 텍스트로 설정합니다.

   예를 들면 다음과 같습니다.

   ```
   <user password="John Jones Password" name="john"/>
   ```

   다음에 Enterprise Manager 가 *users.xml* 파일을 읽을 때(시작할 때 또는 사용자를 인증할 때) 다음 작업을 수행합니다.

   - Enterprise Manager 는 암호화된 일반 텍스트 암호로 *users.xml* 을 다시 작성합니다.
   - Enterprise Manager 는 *plainTextPasswords* 특성을 *false* 로 재설정합니다.

7. 추가 사용자 또는 그룹에 대해서는 사용자 이름을 정의하는 3 단계와 각 사용자의 암호를 설정하는 4 단계를 반복합니다.
8. *users.xml* 파일을 저장하고 닫습니다.

   변경된 *users.xml* 파일 내용을 적용하기 위해 Enterprise Manager 를 다시 시작하지 않아도 됩니다.

참고: *users.xml* 파일에 오류가 있는 경우 Enterprise Manager 가 시작되지 않습니다.

사용자 관련 users.xml 구문

```
<users>
    <user password="adb831a7fdd83dd1e2a39ce7591dff8" name="Guest"/>
    <user password="" name="Admin"/>
</users>
```

그룹 관련 users.xml 구문

```
<groups>
    <group description="Administrator Group" name="Admin">
        <user name="Admin"/>
    </group>
</groups>
```

암호화된 암호를 사용한 users.xml 구문

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<principals xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
plainTextPasswords="false" version="0.3"
xsi:noNamespaceSchemaLocation="users0.3.xsd">
    <users>
        <user password="adb831a7fdd83dd1e2a39ce7591dff8" name="Guest"/>
        <user password="" name="Admin"/>
    </users>
    <groups>
        <group description="Administrator Group" name="Admin">
            <user name="Admin"/>
        </group>
    </groups>
</principals>
```

domains.xml 에 CA Introscope® 도메인 권한 구성

권한은 CA APM 사용자 또는 그룹이 로그인할 때 적용됩니다. CA APM 사용자 또는 그룹이 로그인한 상태에서 권한이 변경되면 다음에 다시 로그인할 때까지 해당 변경 사항이 인식되지 않습니다. 즉, 세션 중에 권한이 변경되어도 CA Introscope 는44 세션을 종료하지 않습니다.

CA Introscope 권한은 동적으로 변경되므로 Enterprise Manager 는 로그인할 때마다 *domains.xml* 및 *server.xml* 파일을 검사합니다. 그러므로 Enterprise Manager 를 다시 시작하지 않고도 권한을 변경할 수 있습니다.

사용자는 다음과 같은 순서로 도메인에 대한 권한을 부여받습니다.

- 사용자를 지정하는 각 도메인에 나열된 모든 권한
- 사용자가 속한 그룹의 각 도메인에 나열된 모든 권한

또한 도메인에 액세스할 때 다음 규칙이 적용됩니다.

- 권한에 있어서 *SuperDomain* 은 다른 도메인과 동일하게 처리됩니다.
- 또한 SuperDomain 에 액세스할 수 있는 사용자 또는 그룹에 부여된 권한이 있으면 사용자 정의된 모든 도메인에서 해당 권한을 사용할 수도 있습니다.
- 단일 사용자나 그룹이 단일 도메인에 대해 여러 권한을 보유할 수 있습니다.
- 단일 사용자나 그룹이 여러 도메인의 권한을 보유할 수 있습니다.

다음 단계를 따르십시오.

1. XML 편집 프로그램을 사용하여 *<EM_Home>/config* 디렉터리에 있는 *domains.xml* 파일을 엽니다.
2. 각 도메인에 대해 다음 속성을 사용하여 사용자 또는 그룹의 권한을 정의합니다.

   참고: 사용자 또는 그룹에 여러 권한이 있는 경우 각 사용자/권한 쌍마다 한 행을 사용해야 합니다.

   읽기

   이 권한이 있는 사용자 또는 그룹은 도메인의 모든 에이전트와 비즈니스 논리를 볼 수 있습니다.

   이 권한을 보유하면 다음 작업을 수행할 수 있습니다.

   - Investigator 트리 보기(사용자가 액세스할 수 있는 도메인의 에이전트가 표시됨)
   - Workstation 콘솔의 대시보드 보기
   - Investigator 미리 보기 창에서 메트릭 및 요소 데이터 보기(Investigator 트리에서 특정 리소스에 대한 기본 "상위 N 필터링된 뷰" 포함)
   - 모든 관리 모듈, 에이전트 또는 요소 설정 보기
   - 경고 메시지 보기
   - 기록 데이터 뷰어에서 기록 데이터 새로 고치기 및 확대/축소
   - 기록 데이터 뷰어의 기록 날짜 범위 옵션 변경
   - 그래프에서 메트릭 표시/숨기기
   - 데이터 뷰어에서 메트릭을 앞으로 또는 뒤로 이동
   - 그룹 및 사용자 기본 설정 변경(홈 대시보드 설정, 대시보드 이름과 함께 관리 모듈 이름 표시 등)

   참고: 읽기 권한이 있는 사용자 또는 그룹은 Workstation 의 모든 명령을 볼 수 있지만 액세스 권한이 없는 명령은 비활성화된 상태로 표시됩니다.

쓰기

쓰기 권한이 있는 사용자 또는 그룹은 읽기 권한이 허용하는 작업뿐 아니라 다음 작업도 수행할 수 있습니다.

- 도메인의 모든 에이전트 및 비즈니스 논리 보기
- 대시보드 생성 및 편집
- 도메인의 모든 모니터링 논리 편집

run_tracer

이 권한이 있는 사용자 또는 그룹은 에이전트에 대해 트랜잭션 추적 세션을 시작할 수 있습니다.

참고: 이 권한을 사용하려면 읽기 권한을 할당해야 합니다.

historical_agent_control

이 권한이 있는 사용자 또는 그룹은 에이전트를 마운트 및 마운트 해제할 수 있습니다.

참고: 이 권한을 사용하려면 읽기 권한을 할당해야 합니다.

live_agent_control

이 권한이 있는 사용자 또는 그룹은 도메인 내의 메트릭, 리소스 및 에이전트에 대한 보고 기능을 종료할 수 있습니다.

참고: 이 권한을 사용하려면 읽기 권한을 할당해야 합니다.

dynamic_instrumentation

이 권한이 있는 사용자 또는 그룹은 동적 계측을 수행할 수 있습니다.

동적 계측에 대한 자세한 내용은 *CA APM Java Agent 구현 안내서* 또는 *CA APM .NET 에이전트 구현 안내서*를 참조하십시오.

thread_dump

이 권한이 있는 사용자 또는 그룹은 "스레드 덤프" 탭을 보고 사용할 수 있습니다.

스레드 덤프를 사용하고 구성하는 방법에 대한 자세한 내용은 *CA APM Workstation 사용자 안내서* 및 *CA APM Java Agent 구현 안내서*를 참조하십시오.

full

이 권한이 있는 사용자 또는 그룹은 도메인에 대해 가능한 모든 권한을 보유합니다.

참고: 모든 XML 태그는 대/소문자를 구분합니다.

3. 추가 사용자 또는 그룹에 대해 2 단계를 반복합니다.
4. *domains.xml* 파일을 저장하고 닫습니다.

   CA APM 사용자가 로그인하는 경우 Enterprise Manager 는 *domains.xml* 파일을 검사하여 사용자에게 적합한 도메인 권한이 있는지 확인합니다.

참고: *domains.xml* 파일에 구문 오류나 기타 오류가 있으면 Enterprise Manager 가 시작되지 않습니다.

CA APM 사용자 및 그룹 도메인 권한에 대한 기본 domains.xml 구문

기본 도메인 구성에서,

- *Admin* 사용자 또는 그룹은 SuperDomain 에 대한 전체 권한을 보유합니다.
- *Guest* 사용자 또는 그룹은 SuperDomain 에 대한 읽기 권한(보기 전용)을 보유합니다.

참고: SAP 사용자 또는 그룹 권한은 다소 다르며, 다음과 같습니다.

- *sapsupport* 사용자 또는 그룹은 SuperDomain 에 대한 전체 권한을 보유합니다.
- *Admin* 사용자 또는 그룹은 SuperDomain 에 대한 읽기 권한(보기 전용)을 보유합니다.
- *sapsupport* 사용자 또는 그룹은 CEM 시스템 관리자 및 Admin 그룹의 구성원이므로 CEM 콘솔에 대한 액세스 권한을 부여받습니다.

도메인에 대해 사용자 또는 그룹 권한을 구성하는 구문은 다음과 같습니다.

```
<grant group="Admin" permission="full"/>
<grant user="Guest" permission="read"/>
```

선택적 CA APM 도메인 구성용 domains.xml 구문

다음은 특정 사용자에게 특정 도메인 권한을 부여하는 도메인 권한 구성 예입니다.

- bsmith, HRApplication 도메인의 *full* 권한
- fjones, HRApplication 도메인의 *read* 및 *run_tracer* 권한
- jlo, SuperDomain 의 *write* 권한
- pdiddy, SuperDomain 의 *read* 권한
- swonder, *dynamic_instrumentation* 권한
- cstevens, *thread dump* 권한

domains.xml 파일은 다음 예와 같이 나타납니다.

```
<?xml version="1.0" encoding="UTF-8"?>
<domains xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="domains0.3.xsd" version="0.3">
   <domain name="HRApplication" description="">
      <agent mapping="(.*)HRAppAgent(.*)" />
<grant user="bsmith" permission="full" />
<grant user="fjones" permission="read" />
<grant user="fjones" permission="run_tracer" />
<grant user="swonder" permission="dynamic_instrumentation" />
<grant user="cstevens" permission="thread_dump" />
   </domain>
  <SuperDomain>
      <agent mapping="(.*)"/>
      <grant user="jlo" permission="write"/>
      <grant user="pdiddy" permission="read"/>
  </SuperDomain>
</domains>
```

server.xml 에서 Enterprise Manager 서버 권한 구성

Enterprise Manager 동작 관련 작업에 대해 다음 서버 권한이 정의됩니다.

- Enterprise Manager 종료
- MIB 파일 게시
- APM 상태 콘솔 액세스

다음 단계를 따르십시오.

1. XML 편집 프로그램을 사용하여 *<EM_Home>/config* 디렉터리에 있는 *server.xml* 파일을 엽니다.
2. 필요한 경우 다음 속성을 사용하여 각 CA APM 사용자 또는 그룹에 대해 권한을 정의합니다.

   참고: 모든 XML 태그는 대/소문자를 구분합니다.

   종료

   사용자 또는 그룹은 Enterprise Manager 를 종료할 수 있습니다.

   publish_mib

   사용자 또는 그룹은 MIB 에 SNMP 수집 데이터를 게시할 수 있습니다.

   MIB 를 게시하려면 SNMP 수집을 생성해야 합니다. 이 작업을 수행하려면 SNMP 수집이 저장되는 도메인에 대한 쓰기 권한이 있어야 합니다.

   apm_status_console_control

   사용자 또는 그룹은 APM 상태 경고 아이콘을 보고, APM 상태 콘솔을 사용하고, APM 상태 콘솔에서 CLW 명령을 실행할 수 있습니다.

   참고: 메트릭 브라우저 트리에서 활성 클램프 메트릭 정보를 보려는 사용자에게는 domains.xml SuperDomain 권한 (페이지 44)이 있어야 합니다.

   full

   사용자 또는 그룹은 가능한 모든 Enterprise Manager 서버 권한을 가집니다.
3. 각 CA APM 사용자에 대한 권한을 정의하는 2 단계를 추가 사용자에 대해 반복합니다.
4. *server.xml* 파일을 저장하고 닫습니다.

   참고: *server.xml* 파일에 구문 오류나 기타 오류가 있으면 Enterprise Manager 가 시작되지 않습니다.

서버 권한을 위한 server.xml 구문

다음은 서버에 대한 사용자 권한 구성 구문입니다.

```
<grant user="username" permission="full">
```

사용자 또는 그룹은 Enterprise Manager 에 대해 여러 권한이 있을 수 있습니다. 여러 권한을 부여하려는 경우 사용자/권한 또는 그룹/권한 쌍을 한 줄에 하나씩 사용해야 합니다.

기본 서버 구성을 위한 server.xml 구문

기본 서버 구성에서 "Admin" 사용자 또는 그룹에게는 전체 권한이 있습니다.

선택적 서버 구성을 위한 server.xml 구문

다음은 서로 다른 CA APM 사용자에게 서로 다른 권한을 부여하는 방법을 보여 주는 예제입니다.

- bsmith 에게 *shutdown* 권한 부여
- tjones 에게 *publish_mib* 권한 부여
- cstevens 에게 *apm_status_console_control* 권한 부여

server.xml 파일은 다음 예제와 같이 나타납니다.

```
<?xml version="1.0" encoding="UTF-8"?> <server
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="users0.1.xsd" version="0.1">
<grant user="bsmith" permission="shutdown" />
<grant user="tjones" permission="publish_mib" />
<grant user="cstevens" permission="apm_status_console_control" />
</server>
```

LDAP 를 사용한 Introscope 보안

LDAP 는 사용자 인증만 지원합니다. 인증에 사용할 LDAP 서버를 Enterprise Manager 에 직접 연결하도록 Introscope 보안을 배포하는 경우 권한 부여에는 로컬 보안을 사용해야 합니다. 여기서 권한 부여에 로컬 보안을 사용한다는 것은 다음을 의미합니다.

- Introscope 의 경우 LDAP 서버에서 사용자 및 그룹을 만들고 domains.xml 파일에 권한을 할당해야 합니다.
- CA CEM 의 경우 LDAP 서버에서 사용자뿐 아니라 기본 보안 그룹 4 개를 모두 만들어야 합니다. 예를 들어 LDAP 서버에서 cemadmin 사용자와 함께 "CEM 시스템 관리자" 보안 그룹을 만들 수 있습니다. 그런 다음 cemadmin 을 "CEM 시스템 관리자" 보안 그룹의 구성원으로 할당하면 "CEM 시스템 관리자" 보안 그룹의 권한이 cemadmin 에 제공됩니다. CA CEM 의 기본 보안 그룹 4 개에 대한 자세한 내용은 CA CEM 의 기본 보안 사용자 그룹에 연결된 메뉴 항목 및 권한 (페이지 135)을 참조하십시오.

참고: CA EEM 을 사용하여 Introscope 보안을 배포하고 CA EEM 서버와 LDAP 서버를 통합한 경우 LDAP 에서 인증을 수행하도록 CA EEM 서버를 구성할 수 있습니다. 이러한 경우 Enterprise Manager 는 LDAP 서버에 연결하지 않고 LDAP 서버를 인식하지 않습니다. 자세한 내용은 LDAP 를 사용하여 CA EEM 인증 구성 (페이지 73)을 참조하십시오. 이 상황에서 Introscope 는 권한 부여에 CA EEM 을 사용합니다.

중요! 권한 부여에 로컬 보안을 사용하면 응용 프로그램 심사 맵 보안을 제공할 수 없고, CA CEM 의 탭과 데이터 표시 여부를 제어하는 액세스 정책을 설정할 수도 없습니다. 응용 프로그램 심사 맵을 제공하고 CA CEM 에서 액세스 정책을 사용하려면 권한 부여를 위해 CA EEM 을 배포해야 합니다.

Introscope LDAP 인증과 로컬 권한 부여를 설정하기 전에 이 유형의 보안 및 권한 검사에 대해 이해하는 것이 유용합니다.

Introscope LDAP 인증은 다음 v3 LDAP 서버 및 다른 여러 유형을 지원합니다.

- IBM Directory Server(버전 5.1) - 이 구성의 예제는 IBM Directory Server 용 realms.xml 구문 (페이지 60)을 참조하십시오.
- Sun ONE Directory Server(버전 5.1) - 이 구성의 예제는 Sun ONE Directory Server 용 realms.xml 구문 (페이지 61)을 참조하십시오.
- MS Active Directory(Windows 2000 및 2003 버전) - 이 구성의 예제는 MS Active Directory 용 realms.xml 구문 (페이지 62)을 참조하십시오.

Introscope 보안에 대한 일부 배경 지식을 습득했으므로 이제 보안 배포를 계획할 준비가 완료되었습니다.

다음은 LDAP 보안을 설정 및 유지 관리하는 프로세스입니다.

1. LDAP 서버에 CA APM 사용자 및 그룹을 설정합니다.
2. *realms.xml* 에 LDAP 를 보안 영역으로 추가합니다.
3. 로컬 권한 부여를 설정합니다.

LDAP 인증 정보

LDAP 인증 정보는 *bind* 작업에 제공됩니다. 클라이언트는 인증 정보를 포함한 *bind* 작업을 서버로 보내 LDAP 서버와의 연결을 시작합니다. *bind* 작업에 제공되는 인증 정보는 클라이언트가 선택한 인증 메커니즘에 따라 달라집니다.

bind 를 수행하지 않고 LDAP 요청을 보내는 클라이언트는 익명 클라이언트로 처리됩니다. *bindName* 속성에 대한 값을 입력하지 않으면 인증 메커니즘이 적용되지 않으며 기타 모든 인증 환경 속성이 무시됩니다. 설정된 다른 모든 인증 속성이 명시적으로 무시되게 하려는 경우에만 그와 같이 하십시오. 어느 경우에든 클라이언트는 익명 클라이언트로 처리되지 않습니다. 이는 서버가 클라이언트의 권한이 무엇인지 확인 또는 상관하지 않고, 인증 안 된 사용자가 액세스할 수 있도록 구성한 모든 데이터에는 클라이언트가 액세스(읽기 및 업데이트)할 수 있도록 허용한다는 의미입니다.

realms.xml 에 LDAP 인증 구성

이 항목에서는 인증 메서드로 LDAP 를 구성하는 방법을 설명합니다.

참고: 쉬운 구성을 위해 <*EM_Home*>/examples/authentication 디렉터리에 있는 샘플 realms.ldap.xml 구성 파일을 사용할 수 있습니다.

realms.xml 을 구성하는 경우 다음 규칙을 따라야 합니다.

중요! Enterprise Manager 를 시작하려면 아래 규칙이 *모두* 충족되어야 합니다.

- descriptor=의 값은 대/소문자를 구분합니다.
  - 예를 들어 descriptor=LDAP Realm 은 descriptor=ldap realm 과 다릅니다.
- LDAP 영역의 경우 *descriptor=*의 값은 LDAP Realm 이어야 합니다.
- 영역이 여러 개인 경우 영역 태그의 id= 값은 각 영역마다 고유해야 합니다. 예:

```
<realm descriptor="LDAP Realm" id="LDAP" active="true">
```

다음 단계를 따르십시오.

1. <*EM_Home*>/config 디렉터리에 있는 realms.xml 파일을 엽니다.
2. 인증 방법으로 LDAP 를 구성하려면 다음 속성을 설정합니다.

   LDAP 인증을 사용하는 경우 사용자 ID 가 올바른 한, Introscope 사용자는 빈 암호를 사용하여 Workstation 에 로그인할 수 있습니다. LDAP 인증은 빈 암호나 Null 암호 필드를 검사하지 않으므로 사용자가 성공적으로 로그인할 수 있습니다. 이는 LDAP 인증 속성은 Workstation 클라이언트 또는 WebView 에 로그인하는 경우에 해당합니다. 보안을 시행하려면 disallowEmptyPassword 속성을 설정하십시오.

   참고: LDAP 서버는 모든 사이트마다 고유하게 구성됩니다. LDAP 속성을 구성하기 전에 LDAP 관리자로부터 LDAP 구성 정보를 얻으십시오.

   url

   원격 LDAP 서버의 URL 입니다.

   비 SSL 연결에 대한 기본 포트는 389 이며, SSL 연결에 대한 기본 포트는 636 입니다.

   SSL 을 사용하는 경우 SSL LDAP 포트가 서버 URL 에 포함되어야 합니다.

   예를 들어 ldap://host:port 입니다.

   useSSL

   원격 LDAP 서버 연결에 SSL 을 사용할지 여부를 지정합니다.

   옵션에는 true, false 가 있습니다.

bindName

LDAP 컴퓨터에 바인딩하는 데 사용된 이름입니다. 빈 상태로 두면 익명 바인딩이 사용됩니다.

예를 들어 IntroscopeLDAPUser 입니다.

bindPassword

LDAP 컴퓨터에 바인딩하는 데 사용된 암호입니다.

이 속성은 선택 항목입니다.

bindName 필드가 비어 있는 경우(익명 바인딩 사용) bindPassword 속성은 무시됩니다.

plainTextPasswords

bindPassword 가 일반 텍스트인지, 또는 암호화되었는지를 나타냅니다. 이 속성은 선택 항목입니다.

이 속성이 누락되거나 True 로 설정된 경우 Enterprise Manager 에서 *bindPassword* 속성은 일반 텍스트로 가정됩니다.

기본적으로 이 값은 *True* 로 설정되며, 이는 암호가 일반 텍스트로 가정된다는 의미입니다.

Enterprise Manager 가 realms.xml 파일을 읽어 이 값이 *True* 로 설정되었음을 발견하면 Enterprise Manager 는 다음 작업을 수행합니다.

- bindPassword 속성 일반 텍스트 암호를 암호화합니다.
- 암호화된 암호로 realms.xml 을 다시 씁니다.
- realms.xml plainTextPasswords 속성을 *False* 로 설정합니다.

  값을 False 로 설정하면 암호가 암호화됩니다.

중요! Enterprise Manager 를 시작하려면 이 속성이 realms.xml 파일에 포함되어 있어야 합니다.

bindAuthentication

바인딩하는 경우에 사용하는 인증 유형입니다.

옵션에는 none, simple, DIGEST-MD5 가 있습니다.

baseDN

모든 사용자 개체 쿼리에 대한 기반 고유 이름(DN)입니다.

옵션에는 cn=Users, dc=dev, dc=com 이 있습니다.

scopeDepth

사용자 개체를 쿼리하는 경우의 검색 정도입니다.

usernameAttribute

Introscope 사용자 이름과 일치시킬 LDAP 특성 이름입니다.

예를 들어 userPrincipalName 입니다.

userObjectQuery

사용자 개체를 쿼리하는 데 사용되는 LDAP 검색 필터입니다. 토큰 "%u"는 쿼리가 실행되기 전에 Introscope 사용자 이름으로 채워집니다.

예를 들어 (&(userPrincipalName=%u)(objectclass=user))입니다.

serverCertificate

인증서 파일 이름입니다. 지원되는 인증서 유형은 X.509 및 Base64 인코딩 유형입니다.

지정되지 않은 경우 JVM 이 제공하는 기본 인증 기관이 사용됩니다(http://java.sun.com/j2se/1.5/docs/index.html 참조).

groupNameAttribute

Introscope 사용자 이름과 일치시킬 그룹 특성 이름입니다.

예를 들어 *cn* 입니다.

groupObjectQuery

그룹 개체를 쿼리하는 데 사용되는 LDAP 검색 필터입니다. 토큰 "%u"는 쿼리가 실행되기 전에 Introscope 그룹 이름으로 채워집니다.

예를 들어 (&(objectClass=group)(cn={0}))입니다.

groupMemberQuery

그룹 구성원을 쿼리하는 데 사용되는 LDAP 검색 필터입니다. 토큰 "%u"는 쿼리가 실행되기 전에 Introscope 그룹 구성원으로 채워집니다.

예를 들어 (&(objectClass=group)(member={0}))입니다.

disallowEmptyPassword

사용자가 빈 암호로 로그인하는 것을 허용하지 않습니다.

disableNestedGroupSearch

LDAP 인증 중 사용자가 속하는 그룹 내 중첩된 그룹에 대한 LDAP 재귀 검색을 비활성화합니다. true 로 설정하면 LDAP 인증 성능을 높일 수 있습니다.

이 속성은 선택 항목입니다.

옵션에는 true, false 가 있습니다. 기본값은 false 입니다.

3. 변경 사항을 적용하려면 변경 내용을 realms.xml 파일에 저장하고 Enterprise Manager 를 다시 시작합니다.

참고: 다음과 같은 경우, 업그레이드 후 수동으로 절대 경로를 업데이트하십시오.

- 업그레이드 중 Introscope 디렉터리의 이름을 변경한 경우
- 속성 파일이 Introscope 디렉터리에 있는 파일을 참조하기 위해 절대 경로를 사용한 경우

이러한 상황을 방지하려면 Introscope 루트 디렉터리 내의 파일을 참조할 때 상대 경로를 사용하십시오.

LDAP 인증을 사용하도록 설정한 realms.xml 구문

다음은 LDAP 를 사용하는 보안 영역을 구성하는 *realms.xml* 구문의 예제입니다.

```
<?xml version="1.0" encoding="UTF-8"?>
<realms xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" version="0.1"
xsi:noNamespaceSchemaLocation="realms0.1.xsd">

    <realm active="true" descriptor="LDAP Realm" id="LDAP">
        <!-- Set the URL for the remote LDAP server.    -->
        <!-- The url has the format: ldap://server:port -->
        <property name="url">
            <value>ldap://myActiveDirectoryServer.mydomain.com:389</value>
        </property>
        <!-- Indicate whether SSL is used to connect to the remote LDAP server. -->
        <property name="useSSL">
            <value>false</value>
        </property>
```

```
        <!-- The bindName can be set to a name or an empty string;    -->
        <!-- or it can be commented out. If a name is specified,      -->
        <!-- it will be used to bind to the LDAP server. If the name  -->
        <!-- is unspecified (empty string) or the property itself     -->
        <!-- commented out, then an anonymous bind will occur.        -->
        <property name="bindName">
            <value>CN=Automatic Binding User,OU=Groups,DC=myDomain,DC=com</value>
        </property>
        <!-- If we are doing an anonymous bind, then the bindPassword -->
        <!-- property is ignored. Otherwise, this property sets       -->
        <!-- the password to use when binding to the LDAP server.     -->
        <property name="bindPassword">
            <value>secretPassword</value>
        </property>
        <!-- Set to true if the bindPassword is plain text -->
        <!-- If plainTextPasswords is set to true, the Enterprise Manager overwrites
this file, -->
        <!-- encrypting the password and setting plainTextPasswords to false -->
        <!-- This property is optional -->
        <!-- Default is true -->
        <property name="plainTextPasswords">
            <value>true</value>
        </property>
        <!-- Set the type of authentication to use when binding.   -->
        <!-- Valid values: none|simple|Digest-MD5                  -->
        <!-- Note than in Introscope 8.0 DIGEST-MD5 support has been -->
        <!-- replaced with Digest-MD5 support.                     -->
        <property name="bindAuthentication">
            <value>simple</value>
        </property>
        <!-- The nameSuffix can be set to a suffix or empty string;   -->
        <!-- or it can be commented out. If a suffix is defined,      -->
        <!-- then the value will be appended to the Introscope user   -->
        <!-- name when dealing with LDAP queries. If the suffix is    -->
        <!-- unspecified (empty string) or the property itself is     -->
        <!-- commented out, then the name suffix will not be appended -->
        <!-- to the user name.                                        -->
    <!--
        <property name="nameSuffix">
            <value>@dev.com</value>
        </property>
    -->
        <!-- Set the base DN for all user object queries. -->
        <property name="baseDN">
            <value>DC=myDomain,DC=com</value>
        </property>
```

```
        <!-- Set the search depth when querying for a user object. -->
        <!-- Valid values: onelevel|subtree                        -->
        <property name="scopeDepth">
            <value>subtree</value>
        </property>
        <!-- Set the name of the LDAP attribute      -->
        <!-- that will match an Introscope username. -->
        <property name="usernameAttribute">
            <value>cn</value>
        </property>
        <!-- Set the "LDAP search filter" that is used to query a user object.  -->
        <!-- The tokens "%u" and "{0}" (no quotes) will be filled in with the   -->
        <!-- Introscope username before the query executes.                     -->
        <!-- All XML special characters in the query must be escaped:           -->
        <!--   Use &amp; to indicate an ampersand, &                            -->
        <!--   Use &lt; to indicate a left angle ("less than") character        -->
        <!--   Use &gt; to indicate a right angle ("greater than") character    -->
        <!--   Use &quot; to indicate a quotation mark, "                       -->
        <!--   Use &apos; to indicate an apostrophe, '                          -->
        <property name="userObjectQuery">
            <value>(&amp;(objectClass=organizationalPerson)(cn={0}))</value>
        </property>
        <!-- Optionally set the name of the LDAP attribute  -->
        <!-- to use as the group name.                      -->
    <!--
        <property name="groupNameAttribute">
           <value>cn</value>
        </property>
    -->
        <!-- Optionally set a search filter to match LDAP groups for a member.  -->
        <!-- The tokens "%u" and "{0}" (no quotes) will be replaced by the      -->
        <!-- member's distinguished name.                                       -->
        <!-- All XML special characters in the query must be escaped. See       -->
        <!-- comments for userObjectQuery property above.                       -->
     <!--
        <property name="groupMemberQuery">

<value>(&amp;(objectClass=groupOfUniqueNames)(uniquemember=%u))</value>
        </property>
     -->
        <!-- Set the search filter used to match an LDAP group name.           -->
        <!-- The tokens "%g" and "{0}" (no quotes) will be replaced by the      -->
        <!-- group name before the query executes.                              -->
        <!-- All XML special characters in the query must be escaped. See       -->
        <!-- comments for userObjectQuery property above.                       -->
```

```
        <!--
           <property name="groupObjectQuery">
               <value>(&amp;(objectClass=groupOfUniqueNames)(cn=%g))</value>
           </property>
        -->
           <!-- When using SSL, specify the full path name of -->
           <!-- the LDAP Server Certificate (if available).   -->
        <!-- It is not necessary to escape backslashes.    -->
        <!--
           <property name="serverCertificate">
               <value>C:\path\to\my\cert\cert.cer</value>
           </property>
        -->
           property name="disallowEmptyPassword">
               <value>true</value>
           </property>
       </realm>
</realms>
```

인증서가 서로 다른 여러 LDAP 서버에 대한 realms.xml 구문

여러 LDAP 서버의 인증서가 서로 다르고 호환되지 않을 때 올바르게 바인딩하도록 realms.xml 을 구성할 수 있습니다.

이 예제에서 SSL 에 포트 636 을 사용하는 host1 이라는 단일 LDAP 호스트는 LDAP 인증을 수행합니다. 호스트 1 에는 realms.xml 에서 host1.pem 으로 명시된 인증서가 있습니다. 포트 636 을 사용하는 host2 라는 두 번째 호스트를 추가하려고 합니다. realms.xml 의 호스트 2 인증서는 host2.pem 이며 host1.pem 인증서와 호환되지 않습니다.

serverCertificate 값을 host1.pem 으로 구성하면 바인딩 작업은 호스트 1 에서 수행될 수 있지만 호스트 2 에서는 수행될 수 없습니다. serverCertificate 값을 host2.pem 으로 구성하면 바인딩 작업은 호스트 2 에서 수행될 수 있지만 호스트 1 에서는 수행될 수 없습니다.

이러한 문제를 피하려면 realms.xml 을 이 예제처럼 구성하십시오.

```
<property name="url">
<value>ldap://host1.net:636 ldap://host2.net:636</value>
</property>

<property name="serverCertificate">
    <VALUE>CONFIG/host1.PEM</VALUE>
    <VALUE>CONFIG/host2.PEM</VALUE>
</property>
```

이 구성에서 호스트 1 과 호스트 2 모두에서 바인딩 작업이 발생할 수 있습니다.

IBM Directory Server 용 realms.xml 구문

다음 *realms.xml* 예는 SSL 을 통해 IBM Directory Server 에 사용하도록 LDAP 속성을 구성하는 방식을 보여 줍니다.

참고: 다음 코드 샘플은 예시용으로만 제공되며 각 사이트의 LDAP 서버는 고유하게 구성됩니다.

```
<?xml version="1.0" encoding="UTF-8"?>
<realms xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" version="0.1"
xsi:noNamespaceSchemaLocation="realms0.1.xsd">
<realm active="true" descriptor="LDAP Realm" id="LDAP">
<property name="url">
<value>ldap://machine01.co.com:123</value>
</property>
<property name="serverCertificate">
<value/>
</property>
<property name="bindPassword">
<value>jon</value>
</property>
<property name="useSSL">
<value>false</value>
</property>
<property name="userObjectQuery">
<value>(&amp;(objectClass=organizationalPerson)(cn={0})) </value>
</property>
```

```
<property name="groupNameAttribute">
          <value>cn</value>
       </property>
       <property name="groupObjectQuery">
          <value>(&amp;(objectClass=organizationalUnit)(cn={0}))</value>
       </property>
       <property name="groupMemberQuery">
          <value>(&amp;(objectClass=groupofNames)(member={0}))</value>
       </property>
<property name="bindAuthentication">
<value>simple</value>
</property>
<property name="bindName">
<value>cn=Jon Doe,ou=Groups,o=unitTest</value>
</property>
<property name="usernameAttribute">
<value>cn</value>
</property>
<property name="scopeDepth">
<value>subtree</value>
</property>
</realm>
</realms>
```

Sun ONE Directory Server 용 realms.xml 구문

다음 *realms.xml* 예에서는 SSL 을 통해 Sun ONE Directory Server 에 사용할 LDAP 속성을 구성하는 방식을 보여 줍니다.

참고: 다음 코드 샘플은 예시용으로만 제공되며 각 사이트의 LDAP 서버는 고유하게 구성됩니다.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<realms xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" version="0.1"
xsi:noNamespaceSchemaLocation="realms0.1.xsd">
    <realm active="true" id="Introscope LDAP Realm" descriptor="LDAP Realm">
        <property name="bindName">
           <value>uid=User01,ou=Users,dc=co,dc=com</value>
        </property>
        <property name="scopeDepth">
           <value>subtree</value>
        </property>
        <property name="baseDN">
           <value>DC=co,DC=com</value>
        </property>
        <property name="bindPassword">
           <value>jim</value>
        </property>
```

```
        <property name="url">
           <value>ldap://123serv01.company.com:389</value>
        </property>
        <property name="usernameAttribute">
           <value>cn</value>
        </property>
        <property name="userObjectQuery">
           <value>(&amp;(objectClass=organizationalPerson)(cn={0}))</value>
        </property>
        <property name="groupNameAttribute">
           <value>cn</value>
        </property>
        <property name="groupObjectQuery">
           <value>(&amp;(objectClass=group)(cn={0}))</value>
        </property>
        <property name="groupMemberQuery">
           <value>(&amp;(objectClass=group)(member={0}))</value>
        </property>
        <property name="useSSL">
           <value>false</value>
        </property>
        <property name="bindAuthentication">
           <value>simple</value>
        </property>
        <property name="serverCertificate">
           <value/>
        </property>
    </realm>
</realms>
```

MS Active Directory 용 realms.xml 구문

다음 *realms.xml* 예는 SSL 을 통해 MS Active Directory 에 사용하도록 LDAP 속성을 구성하는 방식을 보여 줍니다.

참고: 다음 코드 샘플은 예시용으로만 제공되며 각 사이트의 LDAP 서버는 고유하게 구성됩니다.

```
<?xml version="1.0" encoding="UTF-8"?>
<realms xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" version="0.1"
xsi:noNamespaceSchemaLocation="realms0.1.xsd">

<realm active="true" descriptor="LDAP Realm" id="LDAP">
<property name="url">
<value>ldap://123serv01.company.com:389:389</value>
</property>
```

```
<property name="serverCertificate">
<value/>
</property>
<property name="bindPassword">
<value>Password4bindPassword</value>
</property>
<property name="useSSL">
<value>false</value>
</property>
<property name="userObjectQuery">
<value>(&amp;(objectClass=organizationalPerson)(cn={0})) </value>
</property>
<property name="baseDN">
<value>DC=ad-dev-02,DC=com</value>
</property>
<property name="bindAuthentication">
<value>simple</value>
</property>
<property name="bindName">
<value>CN=Jon Doe,cn=Users,DC=ad-dev-02,DC=com</value>
</property>
<property name="usernameAttribute">
<value>cn</value>
</property>
<property name="scopeDepth">
<value>subtree</value>
</property>
</realm>
</realms>
```

CA EEM 을 사용한 Introscope 보안

CA EEM 은 CA Technologies 엔터프라이즈 전체에 사용되는 정책 서버로, 이를 통해 서로 다른 응용 프로그램이 공통 액세스 정책 관리, 인증 및 권한 부여 서비스를 공유할 수 있습니다. CA EEM 은 여러 Embedded Entitlements Client 응용 프로그램을 지원하는 중앙 집중식 Embedded Entitlements Server 로 구성됩니다.

자세한 내용은 다음 CA EEM 안내서를 참조하십시오. 이는 http://support.ca.com의 CA Support 사이트에서 다운로드할 수 있도록 CA EEM 응용 프로그램에 포함되어 있습니다.

- *CA Embedded Entitlements Manager Getting Started Guide(CA Embedded Entitlements Manager 시작 안내서)*
- *CA Embedded Entitlements Manager Programming Guide(CA Embedded Entitlements Manager 프로그래밍 안내서)*
- *CA Embedded Entitlements Manager Release Notes(CA Embedded Entitlements Manager 릴리스 정보)*

CA EEM 배포 옵션

CA EEM 을 사용하여 다음과 같이 다양한 방식으로 Introscope 보안을 설정할 수 있습니다.

- 인증 및 권한 부여 모두에 대해 CA EEM 을 배포합니다. 자세한 내용은 realms.xml 에 CA EEM 인증 구성 (페이지 69) 및 CA EEM 권한 부여 구성 (페이지 75)을 참조하십시오.
- LDAP 서버와 통합하도록 CA EEM 서버를 설정하는 경우 인증에는 LDAP 를, 권한 부여에는 CA EEM 을 사용할 수 있습니다. 자세한 내용은 LDAP 를 사용하여 CA EEM 인증 구성 (페이지 73)을 참조하십시오.

- SiteMinder 와 통합하도록 CA EEM 서버를 설정하는 경우 인증에는 SiteMinder 를, 권한 부여에는 CA EEM 을 사용할 수 있습니다. 자세한 내용은 CA SiteMinder 를 사용하여 CA EEM 인증 구성을 참조하십시오.
- 인증이 필요한 경우에만 CA EEM 을 배포하고 권한 부여에는 로컬 보안을 사용합니다. 자세한 내용은 로컬 권한 부여를 사용하도록 CA EEM 구성 (페이지 117)을 참조하십시오.

참고: CA APM 은 EEM 8.4 SP4 SDK 를 제공하며, EEM 서버 버전 8.4 SP4 이상에서 인증되었습니다.

중요! 권한 부여에 로컬 보안을 사용하면 응용 프로그램 심사 맵 보안을 제공할 수 없고, CA CEM 의 탭과 데이터 표시 여부를 제어하는 액세스 정책을 설정할 수도 없습니다. 응용 프로그램 심사 맵을 제공하고 CA CEM 에서 액세스 정책을 사용하려면 권한 부여를 위해 CA EEM 을 배포해야 합니다.

CA EEM 보안 설정 및 유지 관리 프로세스

Introscope 보안에 대한 일부 배경 지식을 습득했으므로 이제 CA EEM 보안 배포를 계획할 준비가 완료되었습니다. 아래에는 수행할 단계가 개괄적으로 나와 있습니다.

다음 단계를 따르십시오.

1. CA EEM 서버를 설치합니다. 자세한 내용은 CA EEM 설치 (페이지 68)를 참조하십시오.
2. (선택 사항) CA EEM 로그 메시지를 제공하도록 *IntroscopeEnterpriseManager.properties* 파일을 구성합니다. 자세한 내용은 CA EEM 관련 메시지의 로깅 구성 (페이지 69)을 참조하십시오.
3. 각 Enterprise Manager 에서 CA EEM 을 보안 영역으로 정의하고 *<EM_Home>/config* 디렉터리에 위치한 *realms.xml* 파일에서 인증 및 권한 부여 속성을 설정합니다. 자세한 내용은 realms.xml 에 CA EEM 인증 구성 (페이지 69)을 참조하십시오.

   참고: CA EEM 서버를 LDAP 또는 CA SiteMinder Web Access Manager(SiteMinder) 서버와 통합하면 LDAP 또는 SiteMinder 를 사용하여 사용자를 인증하도록 CA EEM 을 구성할 수 있습니다.
4. (선택 사항) CA EEM 인증으로 LDAP 를 구성합니다. 자세한 내용은 LDAP 를 사용하여 CA EEM 인증 구성 (페이지 73)을 참조하십시오.

5. (선택 사항) CA EEM 인증으로 SiteMinder 를 구성합니다. 자세한 내용은 CA SiteMinder 를 사용하여 CA EEM 인증 구성 (페이지 74)을 참조하십시오.

6. (선택 사항이지만 권장됨) *<EM_Home>/examples/authentication* 디렉터리에 제공된 *eem.register.app.xml* 및 *eem.add.global.identities.xml* 스크립트를 로드합니다. 자세한 내용은 CA EEM 권한 부여 구성 (페이지 75)을 참조하십시오.

   참고: CA Technologies 에서는 기본 APM 응용 프로그램 사용자, 그룹, 리소스 및 권한을 포함하여 APM 응용 프로그램을 만드는 샘플 스크립트를 제공합니다. CA Technologies 에서는 이들 스크립트를 사용하여 다음 7 단계부터 10 단계까지 수행할 것을 권장합니다. 자세한 내용은 CA EEM 권한 부여 구성 (페이지 75)을 참조하십시오.

7. CA EEM 에서 하나 이상의 APM 응용 프로그램을 만듭니다. 자세한 내용은 CA EEM 에서 APM 응용 프로그램 등록 (페이지 82)을 참조하십시오.

8. CA EEM 에서 APM 그룹 및 사용자를 만들고 해당 권한도 만듭니다. 자세한 내용은 CA EEM 에서 APM 그룹 만들기 및 삭제 (페이지 87)와 CA EEM 에서 APM 사용자 만들기 및 삭제 (페이지 91)를 참조하십시오.

9. CA EEM 에서 APM 리소스 클래스와 해당 권한을 만듭니다. 자세한 내용은 CA EEM 에서 APM 리소스 클래스 만들기 및 삭제 (페이지 95)를 참조하십시오.

10. CA EEM 에서 APM 도메인, 서버 및 APM 응용 프로그램 리소스를 만들고 해당 권한도 만듭니다. 자세한 내용은 CA EEM APM 도메인 리소스 액세스 정책 만들기 및 삭제 (페이지 104)와 CA EEM APM 서버 리소스 액세스 정책 만들기 및 삭제 (페이지 107)를 참조하십시오. CA EEM APM 프런트엔드 및 비즈니스 서비스 리소스 액세스 정책 만들기 및 삭제 (페이지 111)

11. Enterprise Manager 를 다시 시작합니다.

12. 필요한 경우 다음 작업을 수행하여 CA EEM 기반 보안을 추가하고 유지 관리합니다.

    - CA EEM 동작과 오류를 보고하도록 로그 메시지를 구성합니다. 자세한 내용은 CA EEM 관련 메시지의 로깅 구성 (페이지 69)을 참조하십시오.
    - CA EEM 인증을 위해 CA EEM 서버를 LDAP 또는 SiteMinder 와 통합하도록 구성합니다. 자세한 내용은 LDAP 를 사용하여 CA EEM 인증 구성 (페이지 73) 또는 CA SiteMinder 를 사용하여 CA EEM 인증 구성 (페이지 74)을 참조하십시오.
    - 여러 영역을 정의합니다. 예를 들어 인증에는 CA EEM 을, 권한 부여에는 로컬을 정의합니다. 자세한 내용은 로컬 권한 부여를 사용하도록 CA EEM 구성 (페이지 117)을 참조하십시오.
    - CA APM 스크립트를 수정하거나 사용자 자신의 스크립트를 만듭니다. 자세한 내용은 CA EEM 권한 부여 구성 (페이지 75)을 참조하십시오.
    - APM 응용 프로그램을 추가 및 삭제합니다. 자세한 내용은 CA EEM 에서 APM 응용 프로그램 등록 (페이지 82)을 참조하십시오.
    - APM 그룹과 해당 권한을 추가, 편집 및 삭제합니다. 자세한 내용은 CA EEM 에서 APM 그룹 만들기 및 삭제 (페이지 87)를 참조하십시오.
    - APM 사용자와 해당 권한을 추가, 편집 및 삭제합니다. 자세한 내용은 CA EEM 에서 APM 사용자 만들기 및 삭제 (페이지 91)를 참조하십시오.
    - APM 리소스 클래스와 해당 권한을 추가, 편집 및 삭제합니다. 자세한 내용은 CA EEM 에서 APM 리소스 클래스 만들기 및 삭제 (페이지 95)를 참조하십시오.
    - APM 도메인 리소스와 해당 권한을 추가, 편집 및 삭제합니다.
        - CA EEM 에서 수행하는 경우 CA EEM APM 도메인 리소스 액세스 정책 만들기 및 삭제 (페이지 104)를 참조하십시오.
        - 로컬 권한 부여인 경우 *domains.xml* 에서 업데이트합니다. 자세한 내용은 domains.xml 에 Introscope 도메인 권한 구성 (페이지 44)을 참조하십시오.

  - Enterprise Manager 서버 리소스 및 해당 권한을 추가, 편집 및 삭제합니다.
    - CA EEM 에서 수행하는 경우 CA EEM APM 서버 리소스 액세스 정책 만들기 및 삭제 (페이지 107)를 참조하십시오.
    - 로컬 권한 부여인 경우 *server.xml* 에서 업데이트합니다. 자세한 내용은 Enterprise Manager 서버 권한 구성 (페이지 48)을 참조하십시오.
- Enterprise Manager 응용 프로그램 리소스 및 해당 권한을 추가, 편집 및 삭제합니다. 자세한 내용은 CA EEM APM 프런트엔드 및 비즈니스 서비스 리소스 액세스 정책 만들기 및 삭제 (페이지 111)를 참조하십시오.

CA EEM 설치

CA EEM 은 Enterprise Manager 와 동일한 컴퓨터에 설치할 수 있는 독립 실행형 서버 구성 요소입니다. CA EEM 요구 사항에 대한 자세한 내용은 *CA Embedded Entitlements Manager Release Notes*(CA Embedded Entitlements Manager 릴리스 정보)를 참조하십시오.

CA EEM 설치에 대한 자세한 내용은 *CA APM 설치 및 업그레이드 안내서*를 참조하십시오. CA EEM 설치 정보에 대한 더 자세한 내용은 CA EEM 제품 설치 파일과 함께 제공되는 다음 CA EEM 안내서를 참조하십시오.

- *CA Embedded Entitlements Manager Getting Started Guide*(CA Embedded Entitlements Manager 시작 안내서)
- *CA Embedded Entitlements Manager Release Notes*(CA Embedded Entitlements Manager 릴리스 정보)

중요! CA EEM 데이터 저장소 및 서버 장애 조치(failover)를 처리하도록 CA EEM 을 구성할 수 있습니다. 자세한 내용은 *CA Embedded Entitlements Manager Getting Started Guide*(CA Embedded Entitlements Manager 시작 안내서)를 참조하십시오.

CA EEM 서버에서 제공하는 Safex 유틸리티를 사용하여 APM 응용 프로그램, 사용자 및 그룹 데이터를 CA EEM 으로 가져올 수 있습니다. 자세한 내용은 CA EEM 권한 부여 구성 (페이지 75)을 참조하십시오.

(선택 사항) CA EEM 관련 메시지의 로깅 구성

CA EEM 오류를 해결하는 데 도움이 되는 자세한 CA EEM 로그 메시지를 제공하도록 IntroscopeEntrerpriseManager.properties 파일을 업데이트할 수 있습니다. 예를 들어 CA EEM 로그인 오류가 발생하는 경우 또는 사용자에 대해 권한이 설정되지 않은 경우에 유용합니다.

다음 단계를 따르십시오.

1. <EM_Home>/config 디렉터리로 이동합니다.
2. IntroscopeEntrerpriseManager.properties 파일을 엽니다.
3. 다음 속성을 IntroscopeEntrerpriseManager.properties 파일에 추가합니다.

   ```
   log4j.logger.Manager.EemRealm=DEBUG
   log4j.logger.additivity.Manager.EemRealm=false
   ```

4. IntroscopeEntrerpriseManager.properties 파일을 저장하고 닫으십시오.

   <EM_Home>/logs/IntroscopeEnterpriseManager.log 파일의 로그 메시지와 모든 디버그 메시지에서 CA EEM 연결 정보를 확인할 수 있습니다. 로그 메시지에는 CA EEM 에서 Enterprise Manager 가 연결된 응용 프로그램 및 CA EEM 서버 위치가 표시됩니다. SiteMinder 또는 외부 디렉터리(LDAP 영역)를 사용하여 사용자 및 그룹을 가져오도록 CA EEM 서버를 구성한 경우 해당 정보도 함께 로깅됩니다.

   예:

   ```
   8/05/09 04:15:59 PM PDT [INFO] [Manager.EemRealm] EEM realm attached to
   application "APM" in EEM server at <EEM_Machine_Name> using SiteMinder
   ```

realms.xml 에 CA EEM 인증 구성

realms.xml 파일에서 CA EEM 을 보안 영역으로 구성하는 경우 Introscope 는 인증에 CA EEM 을 사용합니다.

모든 조직의 CA EEM 서버는 고유하게 구성되므로 *realms.xml* 에 CA EEM 속성을 구성하기 전에 CA EEM 구성 정보를 확보해야 합니다. CA EEM 을 설치하지 않은 경우 조직의 CA EEM 관리자에게 문의하여 이 정보를 받으십시오. 또한 인증하려는 CA APM 사용자의 권한이 CA EEM 서버에 정의되어 있는지 확인해야 합니다. CA EEM 서버에 CA APM 사용자를 설정하는 방법에 대한 자세한 내용은 CA EEM 에서 APM 사용자 만들기 및 삭제 (페이지 91)를 참조하십시오.

realms.xml 을 구성하는 경우 다음 규칙을 따라야 합니다.

중요! 다음 규칙 중 하나라도 충족되지 않은 경우 Enterprise Manager 가 시작되지 않습니다.

- *descriptor=*의 값은 대/소문자를 구분합니다.
  - 예를 들어 *descriptor=EEM Realm* 은 *descriptor=eem realm* 과 다릅니다.
- EEM 영역의 경우 *descriptor=*의 값은 *EEM Realm* 이어야 합니다.
- 여러 영역이 존재하는 경우 영역 태그의 *id=* 값은 각 영역마다 고유해야 합니다. 예:
  - *<realm descriptor="EEM Realm" id="EEM Server 1" active="true">*
  - *<realm descriptor="EEM Realm" id="EEM Server 2" active="true">*

사용자에게 기본 권한을 부여하는 기본 영역 및 다른 권한을 부여하는 보조 영역을 구성하려는 경우와 같이 여러 영역을 설정할 수도 있습니다. 또는 조직에서 두 LDAP 서버를 구성하여 이들 모두의 보안을 테스트하려 하거나, 로컬 보안을 사용하던 조직이 CA EEM 으로 전환하면서 해당 구성을 유지하려 할 수도 있습니다.

realms.xml 이 올바로 구성되지 않으면 Enterprise Manager 에 오류 메시지가 표시됩니다. 예를 들면 다음과 같습니다.

```
4/13/10 03:06:32.960 PM PDT [ERROR] [main] [Manager] The EM failed to start. Invalid
realm descriptor in the EEM realm descriptor: eem realm
```

다음 단계를 따르십시오.

참고: 이름이 *APM* 인 응용 프로그램에 기반한 EEM 영역 예제의 경우 *<EM_Home>/examples/authentication* 디렉터리에 위치한 샘플 *realms.eem.xml* 구성 파일을 참조하십시오.

1. *<EM_Home>/config* 디렉터리에 있는 *realms.xml* 파일을 엽니다.
2. 다음 속성을 적합하게 설정합니다.

   참고: *enableAuthorization* 속성을 기본값인 *true* 로 그대로 두면 인증 및 권한 부여 모두에 대해 CA EEM 서버를 사용할 수 있습니다. 이 값을 *false* 로 설정하면 CA EEM 은 인증만 수행하고 권한 부여에는 로컬 보안 영역이 사용됩니다. SiteMinder 또는 LDAP 와 함께 구성된 CA EEM 을 인증에 사용하려는 경우와 같이 로컬 권한 부여를 사용하도록 선택할 수도 있지만 권한은 로컬 영역에 유지해야 합니다.

host

CA EEM 서버의 호스트 이름입니다. 이 속성은 선택 항목입니다.

appname

CA EEM 에서 Enterprise Manager 가 연결된 APM 응용 프로그램 이름입니다. 이 속성은 필수 항목입니다.

username

CA EEM 서버에 연결하는 데 사용하는 사용자 이름입니다. 이 속성은 선택 항목입니다.

CA EEM 기본값은 *EiamAdmin* 입니다.

password

CA EEM 서버에 연결하는 데 사용하는 암호입니다. 이 속성은 필수 항목입니다.

CA EEM 기본값은 *EiamAdmin* 입니다.

plainTextPasswords

암호가 일반 텍스트로 저장되는지 아니면 암호화되는지를 나타냅니다. 이 속성은 필수 항목입니다.

Enterprise Manager 는 *realms.xml* 파일을 읽어 이 값이 *True* 로 설정된 것을 확인하면 다음을 수행합니다.

- 일반 텍스트 암호를 암호화합니다.
- 암호화된 암호로 *realms.xml* 을 다시 씁니다.
- *realms.xml plainTextPasswords* 속성을 *False* 로 설정합니다.

값을 *False* 로 설정하면 암호가 암호화되었다고 간주됩니다.

중요! 이 속성이 *realms.xml* 파일에 포함되지 않은 경우 Enterprise Manager 가 시작되지 않고 오류 메시지가 표시됩니다.

enableAuthorization

권한 부여 방식으로 CA EEM 을 사용합니다. 이 속성은 선택 항목입니다.

기본적으로 이 값은 *True* 로 설정되어 있으며, 이는 인증 및 권한 부여 모두에 CA EEM 이 사용된다는 것을 의미합니다.

이 값을 *False* 로 설정하면 CA EEM 은 인증에만 사용되고 권한 부여에는 로컬이 사용됩니다.

3. *realms.xml* 파일을 저장합니다.
4. *realms.xml* 의 변경 사항이 적용되도록 Enterprise Manager 를 다시 시작합니다.

CA EEM 인증을 사용하도록 설정한 realms.xml 구문의 예제

다음은 *realms.xml* 에서 CA EEM 을 사용하여 보안 영역을 구성하는 구문입니다.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<realms xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" version="0.1"
xsi:noNamespaceSchemaLocation="realms0.1.xsd">
    <realm descriptor="EEM Realm" id="EEM" active="true">
        <!-- Set the hostname of the EEM server -->
        <!-- This property is optional -->
        <!-- Default is localhost -->
            <value>localhost</value>
        </property>
        <!-- Set the name of the EEM application to attach to -->
        <!-- This property is required -->
        <!--
        <property name="appname">
            <value>MyIntroscopeApp</value>
        </property>
        -->
        <!-- Set the user name to connect to the EEM server -->
        <!-- This property is optional -->
        <!-- Default is EiamAdmin -->
        <property name="username">
            <value>EiamAdmin</value>
        </property>
        <!-- Set the password to connect to the EEM server -->
        <!-- This property is required -->
        <property name="password">
            <value>EiamAdmin</value>
        </property>
        <!-- Set to true if the password is plain text -->
        <!-- If plainTextPasswords is set to true, the Enterprise Manager overwrites
this file, -->
        <!-- encrypting the password and setting plainTextPasswords to false -->
        <!-- This property is required -->
        <property name="plainTextPasswords">
            <value>true</value>
        </property>
```

```
        <!-- Enable authorization in the EEM server -->
        <!-- If set to false, the EEM server is used for authentication only -->
        <!-- This property is optional -->
        <!-- Default is true -->
        <property name="enableAuthorization">
            <value>true</value>
        </property>
    </realm>
</realms>
```

LDAP 를 사용하여 CA EEM 인증 구성

CA EEM 이 지원하는 LDAP 서버에 CA EEM 서버를 통합한 경우 인증에 LDAP 서버를 사용하도록 CA EEM 을 구성할 수 있습니다. 이러한 경우 사용자 및 그룹은 LDAP 에서 검색됩니다. 인증을 위해 LDAP 서버에 CA EEM 서버를 통합하는 경우 Introscope 에 추가 구성을 수행할 필요가 없습니다. Introscope 가 지원하는 LDAP 서버에 대한 자세한 내용은 LDAP 를 사용한 Introscope 보안 (페이지 51)을 참조하십시오.

참고: 동시에 여러 외부 디렉터리(예: LDAP 및 SiteMinder 모두)와 통합하도록 CA EEM 을 구성할 수 없습니다.

인증에 LDAP 를 사용하도록 CA EEM 을 구성하는 경우 권한 부여를 위해 CA EEM 을 배포해야 합니다. 자세한 내용은 CA EEM 권한 부여 구성 (페이지 75)을 참조하십시오.

다음 단계를 따르십시오.

1. SUNONE LDAP 서버와 같이 CA EEM 을 지원하는 LDAP 서버를 설정 및 구성합니다.
2. LDAP 사용자 디렉터리에 사용자 및 그룹을 추가합니다.

   참고: CA EEM 서버가 외부 사용자 디렉터리(예: LDAP)에 연결된 경우 CA EEM 에서 글로벌 사용자를 만들거나 추가할 수 없습니다.
3. CA EEM 의 "Configure"(구성) 탭에서 LDAP 또는 Active Directory 서버에 연결하도록 CA EEM 을 구성합니다.

   자세한 내용은 *CA Embedded Entitlements Manager Getting Started Guide*(CA Embedded Entitlements Manager 시작 안내서) 및 *CA Embedded Entitlements Manager Programming Guide*(CA Embedded Entitlements Manager 프로그래밍 안내서)에서 LDAP 관련 항목을 참조하십시오.

CA SiteMinder 를 사용하여 CA EEM 인증 구성

SiteMinder 는 중앙 집중식 웹 액세스 관리 시스템으로, 이를 사용하여 다음을 수행할 수 있습니다.

- 사용자 인증 및 SSO(Single Sign-On)
- 인증 관리
- 정책 기반 권한 부여
- ID 페더레이션
- 웹 응용 프로그램 및 포털에 대한 액세스 감사

인증에 SiteMinder 를 사용하도록 CA EEM 을 구성할 수 있습니다. 이러한 경우 사용자 및 그룹은 SiteMinder 에서 검색됩니다. 인증을 위해 SiteMinder 에 CA EEM 서버를 통합하는 경우 Introscope 에 추가 구성을 수행할 필요가 없습니다.

인증에 SiteMinder 를 사용하도록 CA EEM 을 구성하는 경우 권한 부여를 위해 CA EEM 을 배포해야 합니다. 자세한 내용은 CA EEM 권한 부여 구성 (페이지 75)을 참조하십시오.

참고: 동시에 여러 외부 디렉터리(예: SiteMinder 및 LDAP 모두)와 통합하도록 CA EEM 을 구성할 수 없습니다.

다음 단계를 따르십시오.

1. SiteMinder 사용자 디렉터리에 사용자 및 그룹을 추가합니다.

   참고: CA EEM 서버가 외부 사용자 디렉터리(예: SiteMinder)에 연결된 경우 CA EEM 에서 글로벌 사용자를 만들거나 추가할 수 없습니다.

2. CA EEM 의 "Configure"(구성) 탭에서 SiteMinder 에 연결하도록 CA EEM 을 구성합니다.

   참고: SiteMinder 에 CA EEM 을 통합하는 방법에 대한 자세한 내용은 다음 안내서의 관련 항목을 참조하십시오.

   - *CA Embedded Entitlements Manager Getting Started Guide(CA Embedded Entitlements Manager 시작 안내서)*
   - *CA Embedded Entitlements Manager Release Notes*(CA Embedded Entitlements Manager 릴리스 정보)

   참고: 배포 예제는 기술 자료 문서 TEC534187: CA Wily APM security example: CA SiteMinder for authentication with CA EEM for authorization (TEC534187: CA Wily APM 보안 예제: 권한 부여에 CA EEM 사용 및 인증에 CA SiteMinder 사용)을 참조하십시오.

CA EEM 권한 부여 구성

권한 부여 영역으로 CA EEM 을 사용하는 경우 APM 응용 프로그램과 APM 사용자, 그룹 및 권한을 포함하여 CA EEM 서버를 구성해야 합니다. 이 작업은 다음 둘 중 하나를 사용하여 수행할 수 있습니다.

- CA EEM Safex 유틸리티

  Safex 는 CA EEM 에 제공되는 CLI(명령줄 인터페이스)입니다. Safex 는 XML 스크립트를 실행하여 응용 프로그램을 CA EEM 에 등록하고 사용자와 그룹을 만듭니다.

  CA APM 에는 기본 APM 글로벌 사용자, 리소스 및 권한을 포함하여 APM 응용 프로그램을 만드는 샘플 Safex 스크립트가 제공됩니다. 또한 Safex 스크립트를 사용하여 CA EEM 데이터를 XML 파일로 내보낼 수 있습니다. 자세한 내용은 *CA Embedded Entitlements Manager Programming Guide*(CA Embedded Entitlements Manager 프로그래밍 안내서)를 참조하십시오.

- CA EEM 인터페이스

  CA EEM 인터페이스를 사용하는 방법에 대한 자세한 내용은 *CA Embedded Entitlements Manager Getting Started Guide*(CA Embedded Entitlements Manager 시작 안내서) 및 *CA Embedded Entitlements Manager Online Help*(CA Embedded Entitlements Manager 온라인 도움말)를 참조하십시오.

  배포 예제는 기술 자료 문서 TEC534188: CA Wily APM security example: Setting up CA Wily APM users, groups, and resources in CA EEM (TEC534188: CA Wily APM 보안 예제: CA EEM 에서 CA Wily APM 사용자, 그룹 및 리소스 설정)을 참조하십시오.

CA EEM 인터페이스에 액세스하려면

액세스 권한이 있으면 CA EEM 에 로그인하여 APM 응용 프로그램과 APM 사용자, 그룹 및 권한을 구성할 수 있습니다.

- CA EEM 에서 APM 응용 프로그램에 로그인합니다.

  a. CA EEM 로그인 페이지의 "Application:"(응용 프로그램:) 드롭다운 목록에서 등록한 응용 프로그램 이름이나 APM 을 클릭합니다.

  b. 로그인 이름과 암호를 입력합니다.

  APM 응용 프로그램의 기본 로그인은 *EiamAdmin* 입니다.

FIPS 이외의 모드에서 APM-CA EEM 통합을 구성하려면

참고: FIPS 이외의 모드에서 EEM 서버를 설정하려면 EEM 설치 위치에 있는 igateway.conf 파일에서 <FIPSMode>OFF</FIPSMode>를 사용하여 FIPS 모드를 OFF 로 설정합니다. 이 파일의 기본 설치 위치는 C:\ProgramFiles\CA\SharedComponents\iTechnology 입니다.

1. eiam.config 및 eiam.log4j.config 파일을 구성합니다.
   - <EM install>\config 디렉터리의 eiam.config 및 eiam.log4j.config 파일을 엽니다.
   - FIPS 모드가 OFF 로 설정되어 있으며 <FIPSMode>OFF</FIPSMode>로 표시되는지 확인합니다. 기본 모드는 OFF 입니다.
2. 다이제스트 알고리즘을 다음 알고리즘 중 하나로 설정합니다.
   - MD5(기본값)
   - SHA1
   - SHA256
   - SHA384
   - SHA512

   APM-EEM 통합이 FIPS 이외의 모드에서 구성됩니다.

FIPS 모드에서 APM-CA EEM 통합을 구성하려면

참고: FIPS 모드에서 EEM 서버를 설정하려면 EEM 설치 위치에 있는 igateway.conf 파일에서 <FIPSMode>ON</FIPSMode>을 사용하여 FIPS 모드를 ON 으로 설정합니다. 이 파일의 기본 설치 위치는 C:\Program Files\CA\SharedComponents\iTechnology 입니다.

1. eiam.config 및 eiam.log4j.config 파일을 구성합니다.
   - <EM install>\config 디렉터리의 eiam.config 및 eiam.log4j.config 파일을 엽니다.
   - <FIPSMode>OFF</FIPSMode>를 <FIPSMode>ON</FIPSMode>으로 변경하여 FIPS 모드를 ON 으로 설정합니다.
2. 다이제스트 알고리즘을 다음 알고리즘 중 하나로 설정합니다.
   - SHA1
   - SHA256
   - SHA384
   - SHA512

   APM-EEM 통합이 FIPS 모드에서 구성됩니다.

CA EEM 권한 부여를 구성하려면

중요! 권한 부여에 CA EEM 을 사용하는 경우 CA EEM 에서 Enterprise Manager 가 하나 이상의 응용 프로그램에 연결되어야 합니다. CA EEM 은 응용 프로그램을 사용하여 권한을 정의하는 리소스 클래스와 액세스 정책을 저장합니다.

중요! CA EEM 서버가 외부 사용자 디렉터리(예: LDAP 또는 SiteMinder)에 연결된 경우 CA EEM 에서 글로벌 사용자를 만들거나 추가할 수 없습니다. 인증을 위해 CA EEM 서버가 LDAP 또는 SiteMinder 서버와 통합된 경우 CA EEM 이 아닌 LDAP 나 SiteMinder 에서 사용자 및 그룹을 설정하거나, LDAP 또는 SiteMinder 에서 사용자와 그룹의 CA EEM 액세스 정책을 변경할 수 있습니다.

중요! *eem.register.app.xml* 스크립트에는 LDAP 또는 SiteMinder 와 함께 구성된 CA EEM 을 인증에 설정하는 샘플 코드가 포함되어 있지 않습니다.

다음 단계를 따르십시오.

1. CA EEM 권한 부여를 사용하도록 *realms.xml* 파일을 구성합니다.
   a. *<EM_Home>/config* 디렉터리에 있는 *realms.xml* 파일을 엽니다.
   b. *appname* 속성이 CA EEM 에서 Enterprise Manager 와 연결된 APM 응용 프로그램 이름으로 설정되어 있는지 확인합니다. 예를 들어 *APM* 이라는 이름일 수 있습니다.

      2a 단계에서 CA EEM 서버를 구성할 때 사용하는 것과 동일한 응용 프로그램 이름을 사용합니다.
   c. *enableAuthorization* 속성이 *True* 로 설정되어 있는지 확인합니다.
   d. *realms.xml* 파일을 저장합니다.
   e. *realms.xml* 의 변경 사항이 적용되도록 Enterprise Manager 를 다시 시작합니다.
2. APM 응용 프로그램, 그룹, 사용자, 리소스 클래스, 도메인 및 서버 리소스를 로드하도록 하나 이상의 Safex 스크립트를 만들고 실행합니다.

   CA Technologies 에서는 *<EM_Home>/examples/authentication* 디렉터리에 다음과 같은 샘플 Safex 스크립트를 제공합니다.

   eem.register.app.xml

   기본 APM 응용 프로그램을 등록합니다.

   eem.unregister.app.xml

   기본 APM 응용 프로그램의 등록을 취소합니다.

   eem.add.global.identities.xml

   기본 APM 글로벌 사용자를 추가합니다.

   eem.remove.global.identities.xml

   기본 APM 사용자를 제거합니다.

   참고: CA Technologies 에서는 *eem.register.app.xml* 및 *eem.add.global.identities.xml* 을 수정하여 이들 파일을 CA EEM 권한 부여 배포를 설정하는 기본 스크립트로 사용하도록 권장합니다. 이들 스크립트를 실행해야 CA EEM 권한 부여를 설정하는 데 필요한 요구 사항을 충족하게 됩니다.

a. Safex 스크립트에서 다음 CA EEM 보안 요소를 구성합니다.

- 응용 프로그램. 자세한 내용은 CA EEM 에서 APM 응용 프로그램 등록 (페이지 82) 참조
- 그룹. 자세한 내용은 CA EEM 에서 APM 그룹 만들기 및 삭제 (페이지 87) 참조
- 사용자. 자세한 내용은 CA EEM 에서 APM 사용자 만들기 및 삭제 (페이지 91) 참조

참고: CA EEM 에서는 빈 암호를 지원하지 않으므로 CA EEM 에서 사용자를 만들 때마다 암호를 제공해야 합니다.

- 리소스 클래스. 자세한 내용은 CA EEM 에서 APM 리소스 클래스 만들기 및 삭제 (페이지 95) 참조
- 도메인 리소스 권한. 자세한 내용은 CA EEM 에서 APM 리소스 클래스 만들기 및 삭제 (페이지 95) 참조
- 서버 리소스 권한. 자세한 내용은 CA EEM APM 서버 리소스 액세스 정책 만들기 및 삭제 (페이지 107) 참조

b. 선택 사항: *eem.register.app.xml* 파일을 기본 CA EEM 구성 스크립트로 사용하지 않는 경우 CA EEM 인터페이스를 사용하여 다음 조건을 충족하도록 CA EEM 서버를 구성해야 합니다.

- 두 리소스 클래스인 *도메인 리소스* 클래스 및 *서버 리소스* 클래스를 만듭니다.

  리소스 클래스에는 Introscope 에서 사용할 수 있는 권한과 일치하는 작업 목록이 있어야 합니다. 예를 들어 서버 권한의 경우 Introscope 작업은 *shutdown*, *publish_mib* 및 *full* 입니다. 자세한 내용은 CA EEM APM 도메인 리소스 액세스 정책 만들기 및 삭제 (페이지 104)와 CA EEM APM 서버 리소스 액세스 정책 만들기 및 삭제 (페이지 107)를 참조하십시오.

- 정책 집합을 만듭니다. 정책은 리소스 클래스, 하나 이상의 작업, 하나 이상의 ID 및 0 개 이상의 리소스를 정의합니다.
  - 리소스는 특정 리소스(예: *SuperDomain*)의 이름입니다. 지정된 리소스가 없으면 정책이 해당 리소스 클래스의 모든 인스턴스에 적용됩니다. *서버 리소스 클래스*의 정책은 단일 항목이므로 리소스를 보유해서는 안 됩니다.
  - *ID* 는 그룹의 이름입니다.

- 접두어 *ug:*를 사용하여 응용 프로그램 관련 사용자 그룹을 지정하고, 배포에 따라 글로벌 사용자 그룹을 지정해야 하는 경우에는 접두어 *gug:*를 사용합니다.

3. *<EEM_Server>* 디렉터리로 이동합니다. 이는 일반적으로 다음에 위치합니다.

   ```
   C:\Program Files\CA\SharedComponents\iTechnology
   ```

4. 명령 프롬프트에서 다음 명령을 실행하십시오.

   ```
   C:\Program Files\CA\SharedComponents\iTechnology\safex.exe -h hostname -u
   username -p password -f <mySafexScriptname>.xml
   ```

   예를 들면 다음과 같습니다.

   ```
   C:\Program Files\CA\SharedComponents\iTechnology\safex.exe -h hostname -u
   username -p password -f eem.register.app.xml
   ```

   스크립트를 실행하여 사용자가 정의한 구성 값을 CA EEM 으로 로드합니다.

5. CA EEM 에 로그인하고 APM 응용 프로그램, 그룹, 사용자, 리소스 클래스, 도메인 및 서버 리소스뿐 아니라 연결된 권한을 봅니다.

   a. "Configure"(구성) 탭을 클릭하고 APM 응용 프로그램 목록을 확인합니다.

   b. "Manage Identities"(ID 관리) 탭을 클릭하고 APM 그룹과 사용자를 확인합니다.

   c. "Manage Access Policies"(액세스 정책 관리) 탭을 클릭하고 APM 리소스 클래스와 도메인 및 서버 리소스를 확인합니다.

CA EEM 에서 APM 응용 프로그램 등록

Introscope 보안에 사용할 하나 이상의 응용 프로그램을 CA EEM 에 등록하십시오. CA EEM 에 응용 프로그램을 등록하는 경우 사용자 정보 및 액세스 정책을 저장한 응용 프로그램 인스턴스가 생성됩니다. 사용자 및 응용 프로그램을 사용하는 작업하는 방법에 대한 자세한 내용은 다음 CA EEM 설명서를 참조하십시오.

- *CA Embedded Entitlements Manager Getting Started Guide(CA Embedded Entitlements Manager 시작 안내서)*
- *CA Embedded Entitlements Manager 온라인 도움말*
- *CA Embedded Entitlements Manager Programming Guide(CA Embedded Entitlements Manager 프로그래밍 안내서)*

CA APM 에서는 이름이 *APM* 인 CA EEM 응용 프로그램을 등록하는 기본 Safex 스크립트가 제공됩니다.

중요! CA EEM 에 응용 프로그램을 등록하려면 Safex 스크립트를 사용하십시오. CA EEM 사용자 인터페이스를 사용해서는 응용 프로그램을 등록할 수 없습니다.

참고: 이름이 *APM* 인 응용 프로그램을 만드는 Safex 스크립트 코드의 경우 *<EM_Home>/examples/authentication* 디렉터리에 위치한 *eem.register.app.xml* 샘플 파일을 참조하십시오.

FIPS 이외의 모드에서 CA EEM 에 APM 응용 프로그램을 등록하려면

1. 일반적으로 *C:\Program Files\CA\SharedComponents\iTechnology* 에 위치한 *<EEM_Server>* 디렉터리에 Safex XML 파일을 만듭니다.

   예를 들면 다음과 같습니다.

   ```
   C:\Program Files\CA\SharedComponents\iTechnology \Register_APM.xml
   ```

2. 다음 코드를 잘라내어 Safex XML 파일에 붙여 넣고 따옴표 내의 변수를 적합한 변수로 대체합니다.

   ```
   <Safex>
      <!-- Attach as global user -->
      <Attach/>
      <!-- register "APM" application -->
      <Register certfile="APM.p12" password="Enter Your Password">
         <ApplicationInstance name="APM" label="APM">
         </ApplicationInstance>
      </Register>
      <Detach/>
   </Safex>
   ```

3. 명령 프롬프트를 열고 *<EEM_Server>* 디렉터리(주로 *C:\Program Files\CA\SharedComponents\iTechnology*)로 이동합니다.

4. Safex 스크립트를 실행하려면 다음 명령을 실행합니다.

   ```
   >safex.exe -h localhost -u EiamAdmin -p <password> -f <yourfilename>.xml
   ```

   예를 들면 다음과 같습니다.

   ```
   >safex.exe -h localhost -u EiamAdmin -p <password> -f Register_APM.xml
   ```

5. CA EEM 에서 APM 응용 프로그램을 봅니다.

   a. 스크립트에 제공한 관리자 이름과 암호를 사용하여 CA EEM 에 로그인합니다.

      예를 들어 사용자 이름은 *EiamAdmin* 이고, 암호는 *<password>*일 수 있습니다.

      참고: CA EEM 에서 제공하는 기본 글로벌 권한의 관리자 사용자 이름은 *EiamAdmin* 입니다.

   b. APM 응용 프로그램의 목록을 보려면 "구성" 탭을 클릭합니다.

   c. 해당 응용 프로그램에 대한 정보를 보거나 편집하려면 응용 프로그램 이름(예: APM)을 클릭합니다.

FIPS 모드에서 CA EEM 에 APM 응용 프로그램을 등록하려면

중요! CA EEM 에 응용 프로그램을 등록하려면 Safex 스크립트를 사용하십시오. CA EEM 사용자 인터페이스를 사용해서는 응용 프로그램을 등록할 수 없습니다.

참고: 이름이 APM 인 응용 프로그램을 만드는 Safex 스크립트 코드의 경우 <EM_Home>/examples/authentication 디렉터리에 위치한 eem.register.app.xml 샘플 파일을 참조하십시오.

1. 일반적으로 C:\Program Files\CA\SharedComponents\iTechnology 에 위치한 <EEM_Server> 디렉터리에 Safex XML 파일을 만듭니다.

   예를 들면 다음과 같습니다.

   ```
   C:\Program Files\CA\SharedComponents\iTechnology \Register_APM.xml
   ```

2. 다음 코드를 잘라내어 Safex XML 파일에 붙여 넣고 따옴표 내의 변수를 적합한 변수로 대체합니다.

   ```
   <Safex>
   <!-- Attach as global user -->
   <Attach/>
   <!-- register "APM" application -->
   <Register certtype="pem" certfile="APM.pem" keyfile="APM.key">
   <ApplicationInstancxxle name="APM" label="APM">
   </ApplicationInstance>
   </Register>
   ```

```
<Detach/>
</Safex>
```

3. 명령 프롬프트를 열고 <EEM_Server> 디렉터리(주로 C:\Program Files\CA\SharedComponents\iTechnology)로 이동합니다.
4. Safex 스크립트를 실행하려면 다음 명령을 실행합니다.

   ```
   >safex.exe -h localhost -u EiamAdmin -p <password> -f <yourfilename>.xml -fips
   ```

   예를 들면 다음과 같습니다.

   ```
   >safex.exe -h localhost -u EiamAdmin -p <password> -f Register_APM.xml -fips
   ```

5. CA EEM 에서 APM 응용 프로그램을 봅니다.
   - 스크립트에 제공한 관리자 이름과 암호를 사용하여 CA EEM 에 로그인합니다.

     예를 들어 사용자 이름은 EiamAdmin 이고, 암호는 <password>일 수 있습니다.

     참고: CA EEM 에서 제공하는 기본 글로벌 권한의 관리자 사용자 이름은 EiamAdmin 입니다.
   - APM 응용 프로그램의 목록을 보려면 "구성" 탭을 클릭합니다.
   - 해당 응용 프로그램에 대한 정보를 보거나 편집하려면 응용 프로그램 이름을 클릭합니다. 예를 들어 APM 이라는 이름일 수 있습니다.

CA EEM 에서 APM 응용 프로그램 등록 취소

CA EEM 에서 응용 프로그램의 등록을 취소하는 경우 CA EEM 서버에서 응용 프로그램과 함께 모든 관련 사용자 및 그룹을 삭제해야 합니다.

참고: 또한 CA EEM 인터페이스를 사용하여 이러한 작업을 수행할 수도 있습니다. 자세한 내용은 *CA Embedded Entitlements Manager Getting Started Guide*(CA Embedded Entitlements Manager 온라인 도움말), *CA Embedded Entitlements Manager Online Help*(CA Embedded Entitlements Manager 온라인 도움말), *CA Embedded Entitlements Manager Programming Guide*(CA Embedded Entitlements Manager 프로그래밍 안내서)를 참조하십시오.

다음 단계를 따르십시오.

참고: APM 이라는 응용 프로그램과 해당 사용자 및 그룹의 등록을 취소하는 Safex 스크립트 코드는 *<EM_Home>/examples/authentication* 디렉터리에 위치한 *eem.unregister.app.xml* 샘플 파일을 참조하십시오.

1. 일반적으로 *C:\Program Files\CA\SharedComponents\iTechnology* 에 위치한 *<EEM_Server>* 디렉터리에 Safex XML 파일을 만듭니다.

   예를 들면 *C:\Program Files\CA\SharedComponents\iTechnology\Unregister_APM.xml* 과 같이 만들 수 있습니다.

2. 다음 코드를 잘라내어 Safex XML 파일에 붙여 넣고 따옴표 내의 변수를 적합한 변수로 대체합니다.

```
<Safex>
   <!-- Attach as global user -->
   <Attach/>

   <!-- unregister "APM" application -->
<UnRegister>
     <ApplicationInstance name="APM" label="APM"/>
  </UnRegister>
</Safex>
```

3. 명령 프롬프트를 열고 *<EEM_Server>* 디렉터리(주로 *C:\Program Files\CA\SharedComponents\iTechnology*)로 이동합니다.

4. 다음 명령을 실행하여 Safex 스크립트를 실행합니다.

   ```
   >safex.exe -h localhost -u EiamAdmin -p <password> -f <yourfilename>.xml
   ```

   예를 들면 다음과 같습니다.

   ```
   >safex.exe -h localhost -u EiamAdmin -p <password> -f Unregister_APM.xml
   ```

   FIPS 모드의 CA EEM 에서 APM 응용 프로그램을 등록 해제할 때는 이 명령을 실행하여 Safex 스크립트를 실행합니다.

   ```
   >safex.exe -h localhost -u EiamAdmin -p <password> -f <yourfilename>.xml -fips
   ```

   예를 들면 다음과 같습니다.

   ```
   >safex.exe -h localhost -u EiamAdmin -p <password> -f Unregister_APM.xml -fips
   ```

5. CA EEM 에서 APM 응용 프로그램을 봅니다.

   a. CA EEM 에 로그인합니다.

   b. "Configure"(구성) 탭을 클릭하고 APM 응용 프로그램 목록을 확인합니다.

   등록이 취소된 APM 응용 프로그램은 삭제되어 나열되지 않습니다. 모든 관련 사용자 및 그룹도 삭제됩니다.

CA EEM 에서 APM 그룹 만들기 및 삭제

CA EEM 에는 다음 두 수준의 사용자 그룹이 있습니다.

- 응용 프로그램 관련 그룹: 액세스하도록 허용된 응용 프로그램에 한정하여 권한이 부여됩니다. 응용 프로그램 관련 그룹은 다른 응용 프로그램과 권한을 공유하지 않습니다.

  참고: 기본 CA APM CA EEM 보안은 응용 프로그램 관련 그룹을 사용하여 배포됩니다.

- 글로벌 사용자 그룹: CA EEM 에 등록된 모든 응용 프로그램에 액세스할 수 있으므로 모든 권한이 부여됩니다.

참고: CA EEM 서버가 외부 사용자 디렉터리(예: LDAP 또는 SiteMinder)에 연결된 경우 CA EEM 에서 글로벌 그룹을 만들거나 추가할 수 없습니다. 인증을 위해 CA EEM 서버를 LDAP 또는 SiteMinder 서버와 통합한 경우 CA EEM 이 아닌 LDAP 또는 SiteMinder 에 그룹을 설정해야 합니다.

CA EEM 은 중첩 그룹을 지원하므로 자식 그룹은 부모 그룹의 권한을 상속합니다. 따라서 자식 그룹에 권한을 할당할 필요는 없지만 자식 그룹에 추가 권한을 정의할 수는 있습니다.

CEM 콘솔을 보려면 CA APM 사용자에게 하나 이상의 CEM 리소스에 대한 액세스 정책이 정의되어 있어야 권한 부여가 성공적으로 수행됩니다. Investigator 트리 및 콘솔을 보려면 CA APM 사용자에게 하나 이상의 도메인에 대한 읽기 권한이 있어야 합니다. CA APM 사용자가 CEM 콘솔 및 Investigator 트리와 콘솔을 보려면 다음 요구 사항을 모두 충족해야 합니다.

참고: 기본 APM 사용자를 추가하는 Safex 스크립트 코드는 *<EM_Home>/examples/authentication* 디렉터리에 위치한 *eem.add.global.identities.xml* 샘플 파일을 참조하십시오.

참고: 인증에 LDAP 또는 SiteMinder 를 사용하도록 CA EEM 을 구성하고 LDAP 또는 SiteMinder 서버에 사용자 및 그룹을 만든 경우, APM 그룹을 CA EEM 에 추가하지 않아도 되며 Safex 스크립트를 사용하여 APM 응용 프로그램을 등록만 하면 됩니다. 자세한 내용은 CA EEM 에서 APM 응용 프로그램 등록 (페이지 82)을 참조하십시오.

참고: 또한 CA EEM 인터페이스를 사용하여 이러한 작업을 수행할 수도 있습니다. 자세한 내용은 *CA Embedded Entitlements Manager Getting Started Guide*(CA Embedded Entitlements Manager 온라인 도움말), *CA Embedded Entitlements Manager Online Help*(CA Embedded Entitlements Manager 온라인 도움말), *CA Embedded Entitlements Manager Programming Guide*(CA Embedded Entitlements Manager 프로그래밍 안내서)를 참조하십시오.

Safex 유틸리티를 사용하여 APM 그룹을 만들려면

1. 일반적으로 *C:\Program Files\CA\SharedComponents\iTechnology* 에 위치한 *<EEM_Server>* 디렉터리에 Safex XML 파일을 만듭니다.

   예를 들어 *C:\Program Files\CA\SharedComponents\iTechnology\Add_Groups.xml* 입니다.

2. 다음 코드를 잘라내어 Safex XML 파일에 붙여 넣고 따옴표 내의 변수를 적합한 변수로 대체하고 다른 적절한 값을 구성합니다.

   참고: 접두어 *ug:*를 사용하여 응용 프로그램 관련 사용자 그룹을 지정하고, 배포에 따라 글로벌 사용자 그룹을 지정해야 하는 경우에는 접두어 *gug:*를 사용합니다.

```
<Safex>
   <!-- Attach as global user -->
   <Attach/>
   <!-- add user group -->
   <Add>
         <Folder name="/APM" />
```

```
            <UserGroup name="Admin" folder="/">
                <Description>Administrator Group</Description>
            </UserGroup>

            <UserGroup name="Guest" folder="/">
                <Description>Guest Group</Description>
            </UserGroup>
        </Add>
        <Detach/>
</Safex>
```

3. 명령 프롬프트를 열고 *<EEM_Server>* 디렉터리(주로 *C:\Program Files\CA\SharedComponents\iTechnology*)로 이동합니다.
4. 다음 명령을 실행하여 Safex 스크립트를 실행합니다.

   ```
   >safex.exe -h localhost -u EiamAdmin -p <password> -f <yourfilename>.xml
   ```

   예를 들면 다음과 같습니다.

   ```
   >safex.exe -h localhost -u EiamAdmin -p <password> -f
   eem.add.global.identities.xml
   ```

   FIPS 모드의 CA EEM 과 통합된 APM 응용 프로그램에 대한 그룹을 생성할 때는 이 명령을 실행하여 Safex 스크립트를 실행하십시오.

   ```
   >safex.exe -h localhost -u EiamAdmin -p <password> -f <yourfilename>.xml -fips
   ```

   예를 들면 다음과 같습니다.

   ```
   >safex.exe -h localhost -u EiamAdmin -p <password> -f
   eem.add.global.identities.xml -fips
   ```

5. CA EEM 에서 그룹을 봅니다.
   a. CA EEM 에 로그인합니다.
   b. "Manage Identities"(ID 관리) 탭을 클릭합니다.
   c. "Groups"(그룹) 링크를 클릭합니다.
   d. "Search Groups"(그룹 검색) 창에서 "Show Application groups"(응용 프로그램 그룹 표시) 확인란을 선택하고 "Go"(실행)를 클릭합니다.

      CA EEM 의 "User Groups"(사용자 그룹) 창에 APM 그룹 목록이 표시됩니다.
   e. 그룹 이름 링크를 클릭하여 "User Group"(사용자 그룹) 창에 그룹에 대한 세부 정보를 표시합니다.

Safex 유틸리티를 사용하여 APM 그룹을 삭제하려면

참고: 그룹을 삭제하기 전에 그룹 내의 사용자를 삭제해야 합니다. 삭제할 그룹을 다른 그룹에서 참조하면 해당 참조를 제거해야 합니다.

1. 일반적으로 *C:\Program Files\CA\SharedComponents\iTechnology* 에 위치한 *<EEM_Server>* 디렉터리에 Safex XML 파일을 만듭니다.

   예를 들어 *C:\Program Files\CA\SharedComponents\iTechnology\Remove_Group.xml* 입니다.

2. 다음 코드를 잘라내어 Safex XML 파일에 붙여 넣고 따옴표 내의 변수를 적합한 변수와 다른 적절한 값으로 대체합니다.

   참고: 접두어 *ug:*를 사용하여 응용 프로그램 관련 사용자 그룹을 지정하고, 배포에 따라 글로벌 사용자 그룹을 지정해야 하는 경우에는 접두어 *gug:*를 사용합니다.

   ```
   <Safex>
      <!-- Attach as global user -->
      <Attach/>
   <!-- remove global users and groups -->
      <Remove>
                <GlobalUserGroup name="Admin" folder="/"/>
                <GlobalUserGroup name="Guest" folder="/"/>
                <GlobalFolder name="/APM" />
      </Remove>
      <Detach/>
   </Safex>
   ```

3. 명령 프롬프트를 열고 *<EEM_Server>* 디렉터리(주로 *C:\Program Files\CA\SharedComponents\iTechnology*)로 이동합니다.

4. 다음 명령을 실행하여 Safex 스크립트를 실행합니다.

   ```
   >safex.exe -h localhost -u EiamAdmin -p <ENTER YOUR PASSWORD> -f
   <yourfilename>.xml
   ```

   예를 들면 다음과 같습니다.

   ```
   >safex.exe -h localhost -u EiamAdmin -p 1234567 -f Remove_Group.xml
   ```

   FIPS 모드의 CA EEM 과 통합된 APM 응용 프로그램에 대한 그룹을 삭제할 때는 이 명령을 실행하여 Safex 스크립트를 실행합니다.

   ```
   >safex.exe -h localhost -u EiamAdmin -p <ENTER YOUR PASSWORD> -f
   <yourfilename>.xml -fips
   ```

   예를 들면 다음과 같습니다.

   ```
   >safex.exe -h localhost -u EiamAdmin -p 1234567 -f Remove_Group.xml -fips
   ```

5. CA EEM 에서 APM 그룹을 봅니다.
   a. CA EEM 에 로그인합니다.
   b. "Manage Identities"(ID 관리) 탭을 클릭합니다.
   c. "Groups"(그룹) 링크를 클릭합니다.
   d. "Search Groups"(그룹 검색) 창에서 "Show Application groups"(응용 프로그램 그룹 표시) 확인란을 선택하고 "Go"(실행)를 클릭합니다.

   CA EEM 의 "User Groups"(사용자 그룹) 창에 APM 그룹 목록이 표시됩니다. 삭제한 APM 그룹은 나열되지 않습니다.

CA EEM 에서 APM 사용자 만들기 및 삭제

CA EEM 의 사용자 유형은 다음과 같이 두 가지가 있습니다.

- 응용 프로그램 관련 사용자: 액세스하도록 허용된 응용 프로그램에 한정하여 권한이 부여됩니다.
- 글로벌 사용자: CA EEM 에 등록된 모든 응용 프로그램에 대한 액세스 권한을 갖습니다. 응용 프로그램 관련 사용자 그룹 구성원에게 글로벌 사용자를 할당하면 글로벌 사용자는 응용 프로그램 관련 사용자가 됩니다.

CA APM 의 Safex 스크립트를 사용하여 CA EEM 에 추가한 APM 글로벌 및 응용 프로그램 관련 사용자는 CA EEM 에서 응용 프로그램 관련 그룹의 구성원으로 설정됩니다. 성공적인 CA EEM 권한 부여를 위해 APM 사용자는 CA EEM 의 그룹 구성원일 필요가 없습니다. 하지만 APM 사용자가 CA EEM 의 그룹 구성원이 아닌 경우 도메인, 서버 등과 같은 리소스를 편집할 수 있도록 액세스 정책을 정의해야 합니다.

참고: 인증에 LDAP 또는 SiteMinder 를 사용하도록 CA EEM 을 구성하고 LDAP 또는 SiteMinder 서버에 사용자 및 그룹을 만든 경우, APM 사용자를 CA EEM 에 추가하지 않아도 되며 Safex 스크립트를 사용하여 APM 응용 프로그램을 등록만 하면 됩니다. 자세한 내용은 CA EEM 에서 APM 응용 프로그램 등록 (페이지 82)을 참조하십시오.

참고: CA EEM 서버가 외부 사용자 디렉터리(예: LDAP 또는 SiteMinder)에 연결된 경우 CA EEM 에서 글로벌 사용자를 만들거나 추가할 수 없습니다. 하지만 외부(LDAP 또는 SiteMinder) 사용자 디렉터리에 사용자에 대한 응용 프로그램 관련 정보를 추가할 수 있습니다. 인증을 위해 CA EEM 서버를 LDAP 또는 SiteMinder 서버와 통합한 경우 CA EEM 이 아닌 LDAP 또는 SiteMinder 에 사용자를 설정해야 합니다.

참고: 기본 APM 글로벌 사용자를 추가하는 Safex 스크립트 코드는 *eem.add.global.identities.xml* 샘플 파일을 참조하고, APM 글로벌 사용자를 APM 응용 프로그램 관련 그룹에 추가하는 Safex 스크립트 코드는 *eem.register.app.xml* 샘플 파일을 참조하십시오. 두 파일 모두 *<EM_Home>/examples/authentication* 디렉터리에 위치합니다.

참고: 또한 CA EEM 인터페이스를 사용하여 이러한 작업을 수행할 수도 있습니다. 자세한 내용은 *CA Embedded Entitlements Manager Getting Started Guide*(CA Embedded Entitlements Manager 온라인 도움말), *CA Embedded Entitlements Manager Online Help*(CA Embedded Entitlements Manager 온라인 도움말), *CA Embedded Entitlements Manager Programming Guide*(CA Embedded Entitlements Manager 프로그래밍 안내서)를 참조하십시오.

중요! CA EEM 에서는 빈 암호를 지원하지 않으므로 CA EEM 에서 사용자를 만들 때마다 암호를 제공해야 합니다.

Safex 유틸리티를 사용하여 APM 사용자를 만들려면

1. 일반적으로 *C:\Program Files\CA\SharedComponents\iTechnology* 에 위치한 *<EEM_Server>* 디렉터리에 Safex XML 파일을 만듭니다.

   예를 들어 *C:\Program Files\CA\SharedComponents\iTechnology\Add_Users.xml* 입니다.

2. 다음 코드를 잘라내어 Safex XML 파일에 붙여 넣고 따옴표 내의 변수를 적합한 변수로 대체하고 다른 적절한 값을 구성합니다.

```
<Safex>
   <!-- Attach as global user -->
   <Attach/>

   <!-- add global users -->
   <Add>
         <GlobalUser name="admin" folder="/APM">
               <UserName>admin</UserName>
               <DisplayName>Admin</DisplayName>
               <!-- blank passwords not allowed -->
               <Password>admin</Password>
               <FirstName>APM</FirstName>
               <LastName>Admin</LastName>
               <WorkPhoneNumber>1-888-888-8888</WorkPhoneNumber>
               <EmailAddress>support@yourcompany.com</EmailAddress>
               <GroupMembership>Admin</GroupMembership>
         </GlobalUser>

         <GlobalUser name="guest" folder="/APM">
```

```
            <UserName>guest</UserName>
            <DisplayName>Guest</DisplayName>
            <Password>guest12</Password>
            <FirstName>APM</FirstName>
            <LastName>Guest</LastName>
            <WorkPhoneNumber>1-888-888-8888</WorkPhoneNumber>
            <EmailAddress>support@yourcompany.com</EmailAddress>
            <GroupMembership>Guest</GroupMembership>
        </GlobalUser>

    <!-- add users to groups -->
    <User folder="/APM" name="guest">
    <GroupMembership>Guest</GroupMembership>
    </User>
    <User folder="/APM" name="admin">
    <GroupMembership>Admin</GroupMembership>
    </User>

    </Add>
    <Detach/>
</Safex>
```

3. 명령 프롬프트를 열고 *<EEM_Server>* 디렉터리(주로 *C:\Program Files\CA\SharedComponents\iTechnology*)로 이동합니다.
4. 다음 명령을 실행하여 Safex 스크립트를 실행합니다.

   ```
   >safex.exe -h localhost -u EiamAdmin -p <ENTER YOUR PASSWORD> -f
   <yourfilename>.xml
   ```

   예를 들면 다음과 같습니다.

   ```
   >safex.exe -h localhost -u EiamAdmin -p 1234567 -f Add_Users.xml
   ```

   FIPS 모드의 CA EEM 과 통합된 응용 프로그램에 대한 APM 사용자 그룹을 만들 때는 이 명령을 실행하여 Safex 스크립트를 실행합니다.

   ```
   >safex.exe -h localhost -u EiamAdmin -p <ENTER YOUR PASSWORD> -f
   <yourfilename>.xml -fips
   ```

   예를 들면 다음과 같습니다.

   ```
   >safex.exe -h localhost -u EiamAdmin -p 1234567 -f Add_Users.xml -fips
   ```

5. CA EEM 에서 APM 사용자를 봅니다.
   a. CA EEM 에 로그인합니다.
   b. "Manage Identities"(ID 관리) 탭을 클릭합니다.
   c. "Users"(사용자) 링크를 클릭합니다.

d. "Search Users"(사용자 검색) 창에서 "Attribute"(특성), "Operator"(연산자) 또는 "Value"(값) 검색어를 설정한 후 "Go"(실행)를 클릭합니다.

   CA EEM 의 "Users"(사용자) 창에 APM 사용자의 목록이 표시됩니다.

e. APM 사용자 이름 링크를 클릭하여 "User Details"(사용자 정보) 창에서 더 자세한 정보를 봅니다.

Safex 유틸리티를 사용하여 APM 사용자를 삭제하려면

참고: 기본 APM 글로벌 사용자를 삭제하는 Safex 스크립트의 경우 *eem.remove.global.identities.xml* 샘플 파일을 참조하고, 응용 프로그램 관련 사용자를 포함하여 APM 응용 프로그램을 삭제하는 Safex 스크립트 코드의 경우 *eem.unregister.app.xml* 샘플 파일을 참조하십시오. 두 파일 모두 *<EM_Home>/examples/authentication* 디렉터리에 위치합니다.

1. 일반적으로 *C:\Program Files\CA\SharedComponents\iTechnology* 에 위치한 *<EEM_Server>* 디렉터리에 Safex XML 파일을 만듭니다.

   예를 들어 *C:\Program Files\CA\SharedComponents\iTechnology\Remove_User.xml* 입니다.

2. 다음 코드를 잘라내어 Safex XML 파일에 붙여 넣고 따옴표 내의 변수를 적합한 변수와 다른 적절한 값으로 대체합니다.

```
<Safex>
   <!-- Attach as global user -->
   <Attach/>
<!-- remove global users and groups -->
  <Remove>
         <GlobalUser name="admin" folder="/APM"/>
         <GlobalUser name="guest" folder="/APM"/>
         <GlobalFolder name="/APM" />
   </Remove>
   <Detach/>
</Safex>
```

3. 명령 프롬프트를 열고 *<EEM_Server>* 디렉터리(주로 *C:\Program Files\CA\SharedComponents\iTechnology*)로 이동합니다.

4. 다음 명령을 실행하여 Safex 스크립트를 실행합니다.

   ```
   >safex.exe -h localhost -u EiamAdmin -p <ENTER YOUR PASSWORD> -f
   <yourfilename>.xml
   ```

   예를 들면 다음과 같습니다.

   ```
   >safex.exe -h localhost -u EiamAdmin -p 1234567 -f Remove_User.xml
   ```

   FIPS 모드의 CA EEM 과 통합된 응용 프로그램에 대한 APM 사용자 그룹을 삭제할 때는 이 명령을 실행하여 Safex 스크립트를 실행합니다.

   ```
   >safex.exe -h localhost -u EiamAdmin -p <ENTER YOUR PASSWORD> -f
   <yourfilename>.xml -fips
   ```

   예를 들면 다음과 같습니다.

   ```
   >safex.exe -h localhost -u EiamAdmin -p 1234567 -f Remove_User.xml -fips
   ```

5. CA EEM 에서 APM 사용자를 봅니다.

   a. CA EEM 에 로그인합니다.

   b. "Manage Identities"(ID 관리) 탭을 클릭합니다.

   c. "Users"(사용자) 링크를 클릭합니다.

   d. "Search Users"(사용자 검색) 창에서 "Attribute"(특성), "Operator"(연산자) 또는 "Value"(값) 검색어를 설정한 후 "Go"(실행)를 클릭합니다.

   CA EEM 의 "Users"(사용자) 창에 APM 사용자의 목록이 표시됩니다. 삭제한 APM 사용자는 나열되지 않습니다.

CA EEM 에서 APM 리소스 클래스 만들기 및 삭제

새 응용 프로그램을 등록할 때마다 APM 리소스 클래스를 정의해야 할 수 있습니다. Introscope 에는 최소한 도메인 및 서버 리소스 클래스가 필요합니다. CA CEM 을 사용하는 경우 CA CEM 관련 리소스 클래스를 정의해야 합니다. CA CEM CA EEM 보안에 대한 자세한 내용은 CA CEM 에 대한 CA EEM 인증 및 권한 부여 (페이지 137)를 참조하십시오.

중요! CA APM 보안의 경우 APM 리소스 클래스 및 권한 이름을 사용해야 하며, 이들은 고정되어 있습니다.

각 APM 리소스 클래스의 경우 연결된 권한을 제공해야 하며, CA EEM 에서는 이를 *작업*이라고 합니다.

참고: 기본 리소스 클래스와 함께 이름이 *APM* 인 응용 프로그램을 만드는 Safex 스크립트 코드는 *<EM_Home>/examples/authentication* 디렉터리에 위치한 *eem.register.app.xml* 샘플 파일을 참조하십시오.

참고: 또한 CA EEM 인터페이스를 사용하여 이러한 작업을 수행할 수도 있습니다. 자세한 내용은 *CA Embedded Entitlements Manager Getting Started Guide*(CA Embedded Entitlements Manager 온라인 도움말), *CA Embedded Entitlements Manager Online Help*(CA Embedded Entitlements Manager 온라인 도움말), *CA Embedded Entitlements Manager Programming Guide*(CA Embedded Entitlements Manager 프로그래밍 안내서)를 참조하십시오.

Safex 유틸리티를 사용하여 APM 리소스 클래스를 만들려면

1. 일반적으로 *C:\Program Files\CA\SharedComponents\iTechnology* 에 위치한 *<EEM_Server>* 디렉터리에 Safex XML 파일을 만듭니다.

   예를 들어 *C:\Program Files\CA\SharedComponents\iTechnology\Add_resource_classes.xml* 입니다.

2. 도메인 리소스 클래스 권한을 결정합니다.

   읽기

   이 권한이 있는 사용자 또는 그룹은 도메인의 모든 에이전트와 비즈니스 논리를 볼 수 있습니다.

   이 권한을 보유하면 다음 작업을 수행할 수 있습니다.

   - Investigator 트리 보기(사용자가 액세스할 수 있는 도메인의 에이전트가 표시됨)
   - Workstation 콘솔의 대시보드 보기
   - Investigator 미리 보기 창에서 메트릭 및 요소 데이터 보기(Investigator 트리에서 특정 리소스에 대한 기본 "상위 N 필터링된 뷰" 포함)
   - 모든 관리 모듈, 에이전트 또는 요소 설정 보기
   - 경고 메시지 보기
   - 기록 데이터 뷰어에서 기록 데이터 새로 고치기 및 확대/축소
   - 기록 데이터 뷰어의 기록 날짜 범위 옵션 변경
   - 그래프에서 메트릭 표시/숨기기
   - 데이터 뷰어에서 메트릭을 앞으로 또는 뒤로 이동

- 그룹 및 사용자 기본 설정 변경(홈 대시보드 설정, 대시보드 이름과 함께 관리 모듈 이름 표시 등)

참고: 읽기 권한이 있는 사용자 또는 그룹은 Workstation 의 모든 명령을 볼 수 있지만 액세스 권한이 없는 명령은 비활성화된 상태로 표시됩니다.

쓰기

쓰기 권한이 있는 사용자 또는 그룹은 읽기 권한이 허용하는 작업뿐 아니라 다음 작업도 수행할 수 있습니다.

- 도메인의 모든 에이전트 및 비즈니스 논리 보기
- 대시보드 생성 및 편집
- 도메인의 모든 모니터링 논리 편집

run_tracer

이 권한이 있는 사용자 또는 그룹은 에이전트에 대해 트랜잭션 추적 세션을 시작할 수 있습니다.

참고: 이 권한을 사용하려면 읽기 권한을 할당해야 합니다.

historical_agent_control

이 권한이 있는 사용자 또는 그룹은 에이전트를 마운트 및 마운트 해제할 수 있습니다.

참고: 이 권한을 사용하려면 읽기 권한을 할당해야 합니다.

live_agent_control

이 권한이 있는 사용자 또는 그룹은 도메인 내의 메트릭, 리소스 및 에이전트에 대한 보고 기능을 종료할 수 있습니다.

참고: 이 권한을 사용하려면 읽기 권한을 할당해야 합니다.

dynamic_instrumentation

이 권한이 있는 사용자 또는 그룹은 동적 계측을 수행할 수 있습니다.

동적 계측에 대한 자세한 내용은 *CA APM Java Agent 구현 안내서* 또는 *CA APM .NET 에이전트 구현 안내서*를 참조하십시오.

thread_dump

이 권한이 있는 사용자 또는 그룹은 "스레드 덤프" 탭을 보고 사용할 수 있습니다.

스레드 덤프를 사용하고 구성하는 방법에 대한 자세한 내용은 *CA APM Workstation 사용자 안내서* 및 *CA APM Java Agent 구현 안내서*를 참조하십시오.

full

이 권한이 있는 사용자 또는 그룹은 도메인에 대해 가능한 모든 권한을 보유합니다.

APM 도메인을 구성하는 방법에 대한 자세한 내용은 Introscope 보안 및 권한 개요 (페이지 33)를 참조하십시오.

3. 서버 리소스 클래스 권한을 결정합니다.

종료

사용자 또는 그룹은 Enterprise Manager 를 종료할 수 있습니다.

publish_mib

사용자 또는 그룹은 MIB 에 SNMP 수집 데이터를 게시할 수 있습니다.

MIB 를 게시하려면 SNMP 수집을 생성해야 합니다. 이 작업을 수행하려면 SNMP 수집이 저장되는 도메인에 대한 쓰기 권한이 있어야 합니다.

apm_status_console_control

사용자 또는 그룹은 APM 상태 경고 아이콘을 보고, APM 상태 콘솔을 사용하고, APM 상태 콘솔에서 CLW 명령을 실행할 수 있습니다.

참고: 메트릭 브라우저 트리에서 활성 클램프 메트릭 정보를 보려는 사용자에게는 domains.xml SuperDomain 권한 (페이지 44)이 있어야 합니다.

full

사용자 또는 그룹은 가능한 모든 Enterprise Manager 서버 권한을 가집니다.

4. 응용 프로그램 심사 맵 보안을 제공할 비즈니스 서비스 리소스 클래스 권한을 결정합니다.

   write, read 및 read sensitive data

   Introscope 사용자 및 그룹은 응용 프로그램 심사 맵에서 비즈니스 서비스를 볼 수 있습니다.

   참고: 모든 CA EEM 권한은 응용 프로그램 심사 맵에서 비즈니스 서비스를 보는 데 사용할 수 있습니다. 이러한 경우 기본적으로 이들 세 권한을 사용할 수 있습니다.

   참고: 비즈니스 서비스를 볼 수 있도록 사용자 권한을 변경하는 경우 사용자가 Workstation 에서 로그아웃하고 다시 로그인해야 이러한 변경 사항이 응용 프로그램 심사 맵에 반영됩니다.

5. 프런트엔드에 응용 프로그램 심사 맵 보안을 제공할 비즈니스 응용 프로그램 리소스 클래스 권한을 결정합니다.

   쓰기

   Introscope 사용자 및 그룹은 응용 프로그램 심사 맵에서 프런트엔드를 볼 수 있습니다.

   참고: SuperDomain 보안은 응용 프로그램 심사 맵 보안을 무시합니다. 자세한 내용은 응용 프로그램 심사 맵 보안을 무시하는 SuperDomain 보안 (페이지 122)을 참조하십시오.

   참고: CA APM CA EEM 보안은 비즈니스 응용 프로그램 리소스 클래스를 사용하여 맵 프런트엔드에 보안을 제공합니다.

   참고: 모든 CA EEM 권한은 맵의 프런트엔드를 보는 데 사용될 수 있습니다. 이러한 경우 기본적으로 쓰기 권한만 사용할 수 있습니다.

   참고: 맵 프런트엔드를 보도록 사용자 권한을 변경하는 경우 사용자가 Workstation 에서 로그아웃하고 다시 로그인해야 이러한 변경 사항이 응용 프로그램 심사 맵에 적용됩니다.

6. <ResourceClass>로 시작하여 </ResourceClass>로 끝나는 코드를 잘라내어 Safex XML 파일에 붙여 넣고 리소스 클래스 및 권한에 대해 적합한 변수를 대체하고 다른 적절한 값을 구성합니다.

   참고: CA EEM 에서는 권한을 작업이라고 합니다.

```
<Safex>
   <!-- Attach as global user -->
   <Attach/>
   <!-- register "APM" application  -->
   <Register certfile="APM.p12" password="EiamAdmin">
```

```
        <ApplicationInstance name="APM" label="APM">
               <Brand>Introscope</Brand>
               <MajorVersion>1</MajorVersion>
               <MinorVersion>0</MinorVersion>
               <Description>APM Application</Description>
               <ResourceClass>
                  <Name>Domain</Name>
                  <Action>read</Action>
                  <Action>write</Action>
                  <Action>run_tracer</Action>
                  <Action>historical_agent_control</Action>
                  <Action>dynamic_instrumentation</Action>
                  <Action>live_agent_control</Action>
                  <Action>Thread_Dump</Action>
                  <Action>full</Action>
               </ResourceClass>
               <ResourceClass>
                  <Name>Server</Name>
                  <Action>shutdown</Action>
                  <Action>publish_mib</Action>
                  <Action>apm_status_console_control</Action>
                  <Action>full</Action>
               </ResourceClass>
               <ResourceClass>
                  <Name>Business Service</Name>
                  <Action>write</Action>
                  <Action>read</Action>
                  <Action>read sensitive data</Action>
               </ResourceClass>
               <ResourceClass>
                  <Name>Business Application</Name>
                  <Action>write</Action>
               </ResourceClass>

        </ApplicationInstance>
     </Register>
     <Detach/>
</Safex>
```

참고: 응용 프로그램 심사 맵 사용자 권한을 설정하는 데 *비즈니스 서비스* 및 *비즈니스 응용 프로그램* 리소스 클래스가 필요합니다. 설정된 권한이 없으면 모든 사용자가 모든 프런트엔드를 볼 수 있습니다. 비즈니스 응용 프로그램 리소스 클래스는 특정 프런트엔드를 볼 수 있는 권한을 제공합니다.

7. 명령 프롬프트를 열고 *<EEM_Server>* 디렉터리(주로 *C:\Program Files\CA\SharedComponents\iTechnology*)로 이동합니다.

8. 다음 명령을 실행하여 Safex 스크립트를 실행합니다.

   ```
   >safex.exe -h localhost -u EiamAdmin -p <ENTER YOUR PASSWORD> -f
   <yourfilename>.xml
   ```

   예를 들면 다음과 같습니다.

   ```
   >safex.exe -h localhost -u EiamAdmin -p 1234567 -f Add_resource_classes.xml
   ```

   FIPS 모드의 CA EEM 과 통합된 응용 프로그램에 대한 APM 리소스 클래스를 만들 때는 이 명령을 실행하여 Safex 스크립트를 실행합니다.

   ```
   >safex.exe -h localhost -u EiamAdmin -p <ENTER YOUR PASSWORD> -f
   <yourfilename>.xml -fips
   ```

   예를 들면 다음과 같습니다.

   ```
   >safex.exe -h localhost -u EiamAdmin -p 1234567 -f Add_resource_classes.xml -fips
   ```

9. CA EEM 에서 APM 리소스 클래스를 봅니다.

   a. CA EEM 에 로그인합니다.

   b. "Manage Access Policies"(액세스 정책 관리) 탭을 클릭합니다.

   c. "Policies"(정책) 링크를 클릭합니다.

   CA EEM 에 리소스 클래스의 정책이 나열됩니다.

Safex 유틸리티를 사용하여 APM 리소스 클래스를 삭제하려면

1. 일반적으로 *C:\Program Files\CA\SharedComponents\iTechnology* 에 위치한 *<EEM_Server>* 디렉터리에 Safex XML 파일을 만듭니다.

   예를 들어 *C:\Program Files\CA\SharedComponents\iTechnology\Remove_Resource_class.xml* 입니다.

2. 다음 코드를 잘라내어 Safex XML 파일에 붙여 넣고 따옴표 내의 변수를 적합한 변수와 다른 적절한 값으로 대체합니다.

   ```
   <Safex>
      <!-- Attach as global user -->
      <Attach/>

   <!-- remove resource class -->
         <ApplicationInstance name="APM" label="APM">
         <Remove>
   ```

```
                <ResourceClass>
                   <Name>Business Service</Name>
                   <Action>write</Action>
                   <Action>read</Action>
                   <Action>read sensitive data</Action>
                </ResourceClass>
             </Remove>
          </ApplicationInstance>
          <Detach/>
       </Safex>
```

3. 명령 프롬프트를 열고 *<EEM_Server>* 디렉터리(주로 *C:\Program Files\CA\SharedComponents\iTechnology*)로 이동합니다.
4. 다음 명령을 실행하여 Safex 스크립트를 실행합니다.

   ```
   >safex.exe -h localhost -u EiamAdmin -p <ENTER YOUR PASSWORD> -f
   <yourfilename>.xml
   ```

   예를 들면 다음과 같습니다.

   ```
   >safex.exe -h localhost -u EiamAdmin -p 1234567 -f Remove_Resource_class.xml
   ```

   FIPS 모드의 CA EEM 과 통합된 응용 프로그램에 대한 APM 리소스 클래스를 삭제할 때는 이 명령을 실행하여 Safex 스크립트를 실행합니다.

   ```
   >safex.exe -h localhost -u EiamAdmin -p <ENTER YOUR PASSWORD> -f
   <yourfilename>.xml -fips
   ```

   예를 들면 다음과 같습니다.

   ```
   >safex.exe -h localhost -u EiamAdmin -p 1234567 -f Remove_Resource_class.xml
   -fips
   ```

5. CA EEM 에서 APM 리소스 클래스를 봅니다.
   a. CA EEM 에 로그인합니다.
   b. "Manage Access Policies"(액세스 정책 관리) 탭을 클릭합니다.
   c. "Policies"(정책) 링크를 클릭합니다.

   삭제된 리소스 클래스가 나열되지 않습니다.

CA EEM 액세스 정책 정보

CA EEM 액세스 정책에는 도메인, 서버, 프런트엔드, 비즈니스 서비스 등 특정 리소스에 대해 특정 작업을 수행하도록 그룹에 부여된 권한이 반영되어 있습니다. 이는 비즈니스 서비스 및 프런트엔드(CA EEM 에서는 비즈니스 응용 프로그램이라고 함)에 액세스 정책을 제공하는 비즈니스 보안이 에이전트가 아닌 응용 프로그램 심사 맵에 영향을 미친다는 것을 의미합니다. 반면 도메인 보안은 응용 프로그램 심사 맵이 아닌 에이전트에 영향을 미칩니다.

글로벌 사용자를 응용 프로그램 관련 사용자 그룹에 추가하면 해당 사용자는 그룹에 부여된 리소스 권한을 갖게 됩니다.

예를 들어 다음은 글로벌 사용자를 Admin 으로 만드는 CA APM Safex 스크립트 조각입니다. Admin 은 "CEM 시스템 관리자" 응용 프로그램 관련 사용자 그룹의 구성원입니다.

```
<User folder="/APM" name="cemadmin"><GroupMembership>CEM System
Administrator</GroupMembership><GroupMembership>Admin</GroupMembership>
</User>
```

CA APM Safex 스크립트의 후반부는 CA EEM 응용 프로그램 리소스 액세스 정책을 설정하는 다음 코드 조각으로 구성됩니다.

```
        <Policy name="Business Application write" folder="/Policies">
        <Description>CEM System Administrator Group and CEM Configuration
Administrator Group have write permission for all Business
Applications.</Description>
        <ResourceClassName>Business Application</ResourceClassName>
        <Action>write</Action>
        <Identity>ug:CEM Configuration Administrator</Identity>
        <Identity>ug:CEM System Administrator</Identity>
       </Policy>
```

정책 정의에서 다음 행은 응용 프로그램 리소스에 액세스할 수 있는 "CEM 시스템 관리자" 사용자 그룹 권한을 부여합니다.

```
ug:CEM System Administrator
```

Admin 은 "CEM 시스템 관리자" 사용자 그룹의 구성원이므로 Admin 은 응용 프로그램 심사 맵의 프런트엔드도 볼 수 있는 권한을 부여받습니다.

프런트엔드의 보안은 심사 맵 트리에 적용됩니다. 이는 사용자에게 권한이 없으면 심사 맵 트리의 프런트엔드 노드를 볼 수 없다는 것을 의미합니다. 하지만 사용자가 모든 프런트엔드 및 메트릭을 볼 수 있는 메트릭 브라우저 트리에는 맵 보안이 적용되지 않습니다.

CA EEM APM 도메인 리소스 액세스 정책 만들기 및 삭제

이 항목에서는 CA EEM 의 CA APM 도메인에 보안을 적용하는 방법에 대해 설명합니다. 예를 들어 SuperDomain 또는 사용자가 정의한 도메인이 있을 수 있습니다. 도메인 보안을 적용하려면 도메인 권한을 설정할 수 있도록 *SuperDomain* 및 모든 사용자 정의 도메인에 대한 CA EEM 액세스 정책을 CA EEM 도메인 리소스로 추가해야 합니다.

참고: 로컬 보안의 경우 도메인 권한은 *domains.xml* 파일에 구성됩니다. 자세한 내용은 domains.xml 에 Introscope 도메인 권한 구성 (페이지 44)을 참조하십시오. CA EEM 보안의 경우 *domains.xml* 의 도메인 권한은 무시되고 대신 도메인 권한이 CA EEM 에 설정됩니다.

참고: 도메인 리소스에 대한 기본 액세스 정책과 함께 이름이 *APM* 인 응용 프로그램을 만드는 Safex 스크립트 코드의 경우 *<EM_Home>/examples/authentication* 디렉터리에 위치한 *eem.register.app.xml* 샘플 파일을 참조하십시오.

참고: 또한 CA EEM 인터페이스를 사용하여 이러한 작업을 수행할 수도 있습니다. 자세한 내용은 *CA Embedded Entitlements Manager Getting Started Guide*(CA Embedded Entitlements Manager 온라인 도움말), *CA Embedded Entitlements Manager Online Help*(CA Embedded Entitlements Manager 온라인 도움말), *CA Embedded Entitlements Manager Programming Guide*(CA Embedded Entitlements Manager 프로그래밍 안내서)를 참조하십시오.

Safex 유틸리티를 사용하여 CA EEM APM 도메인 리소스 액세스 정책을 만들려면

1. 일반적으로 *C:\Program Files\CA\SharedComponents\iTechnology* 에 위치한 *<EEM_Server>* 디렉터리에 Safex XML 파일을 만듭니다.

   예를 들어 *C:\Program Files\CA\SharedComponents\iTechnology\Add_domains.xml* 입니다.

2. 다음 코드를 잘라내어 Safex XML 파일에 붙여 넣고, 따옴표 내의 변수를 적합한 변수로 대체하고 ID, 리소스 클래스 및 권한의 값을 지정합니다. 도메인 권한에 대한 자세한 내용은 CA EEM 에서 APM 리소스 클래스 만들기 및 삭제 (페이지 95)에서 각 리소스 클래스에 허용된 권한을 결정하는 2 단계를 참조하십시오.

   참고: CA EEM 에서는 권한을 작업이라고 합니다.

   ```
   <Safex>
      <Attach label="APM"/>
      <!-- add policies -->
   ```

```
   <Add>
        <Policy name="Domain Admin" folder="/Policies">
        <Description>Admin group has full permission for all
domains</Description>
        <Identity>gug:Admin</Identity>
        <Action>full</Action>
        <ResourceClassName>Domain</ResourceClassName>
        <Resource>SuperDomain</Resource>
        </Policy>
     </Add>
     <Detach/>
</Safex>
```

3. 명령 프롬프트를 열고 *<EEM_Server>* 디렉터리(주로 *C:\Program Files\CA\SharedComponents\iTechnology*)로 이동합니다.
4. 다음 명령을 실행하여 Safex 스크립트를 실행합니다.

   ```
   >safex.exe -h localhost -u EiamAdmin -p <ENTER YOUR PASSWORD> -f
   <yourfilename>.xml
   ```

   예를 들면 다음과 같습니다.

   ```
   >safex.exe -h localhost -u EiamAdmin -p 1234567 -f Add_domains.xml
   ```

   FIPS 모드의 CA EEM 과 통합된 응용 프로그램에 대해 Safex 유틸리티를 사용하여 CA EEM APM 도메인 리소스 액세스 정책을 만들 때는 이 명령을 실행하여 Safex 스크립트를 실행합니다.

   ```
   >safex.exe -h localhost -u EiamAdmin -p <ENTER YOUR PASSWORD> -f
   <yourfilename>.xml -fips
   ```

   예를 들면 다음과 같습니다.

   ```
   >safex.exe -h localhost -u EiamAdmin -p 1234567 -f Add_domains.xml- fips
   ```

5. CA EEM 에서 APM 도메인을 봅니다.
   a. CA EEM 에 로그인합니다.
   b. "Manage Access Policies"(액세스 정책 관리) 탭을 클릭합니다.
   c. "Policies"(정책) 링크를 클릭합니다.
   d. "Search Policies"(정책 검색) 창에서 "Show policies matching resource"(리소스와 일치하는 정책 표시)를 클릭하고, "Resource Class Name"(리소스 클래스 이름) 드롭다운 목록에서 "Domain"(도메인)을 선택한 후 "Go"(실행)를 클릭합니다.

   CA EEM 의 "Policy Table"(정책 표) 창에 APM 도메인 리소스 액세스 정책의 목록이 표시됩니다.

Safex 유틸리티를 사용하여 CA EEM APM 도메인 리소스 액세스 정책을 삭제하려면

1. 일반적으로 *C:\Program Files\CA\SharedComponents\iTechnology* 에 위치한 *<EEM_Server>* 디렉터리에 Safex XML 파일을 만듭니다.

   예를 들어 *C:\Program Files\CA\SharedComponents\iTechnology\Remove_domain.xml* 입니다.

2. 다음 코드를 잘라내어 Safex XML 파일에 붙여 넣고, 따옴표 내의 변수를 적합한 변수로 대체하고 ID, 리소스 클래스 및 권한의 값을 지정합니다. 도메인 권한에 대한 자세한 내용은 CA EEM 에서 APM 리소스 클래스 만들기 및 삭제 (페이지 95)에서 각 리소스 클래스에 허용된 권한을 결정하는 2 단계를 참조하십시오.

   참고: CA EEM 에서는 권한을 작업이라고 합니다.

   ```
   <Safex>
      <Attach label="APM"/>
      <Remove>
           <Policy name="Domain Guest" folder="/Policies"/>
      </Remove>
      <Detach/>
   </Safex>
   ```

3. 명령 프롬프트를 열고 *<EEM_Server>* 디렉터리(주로 *C:\Program Files\CA\SharedComponents\iTechnology*)로 이동합니다.

4. 다음 명령을 실행하여 Safex 스크립트를 실행합니다.

   ```
   >safex.exe -h localhost -u EiamAdmin -p <ENTER YOUR PASSWORD> -f
   <yourfilename>.xml
   ```

   예를 들면 다음과 같습니다.

   ```
   >safex.exe -h localhost -u EiamAdmin -p 1234567 -f Remove_domain.xml
   ```

   FIPS 모드의 CA EEM 과 통합된 응용 프로그램에 대해 Safex 유틸리티를 사용하여 CA EEM APM 도메인 리소스 액세스 정책을 삭제할 때는 이 명령을 실행하여 Safex 스크립트를 실행합니다.

   ```
   >safex.exe -h localhost -u EiamAdmin -p <ENTER YOUR PASSWORD> -f
   <yourfilename>.xml -fips
   ```

   예를 들면 다음과 같습니다.

   ```
   >safex.exe -h localhost -u EiamAdmin -p 1234567 -f Remove_domain.xml -fips
   ```

5. CA EEM 에서 APM 도메인을 봅니다.
   a. CA EEM 에 로그인합니다.
   b. "Manage Access Policies"(액세스 정책 관리) 탭을 클릭합니다.
   c. "Policies"(정책) 링크를 클릭합니다.
   d. "Search Policies"(정책 검색) 창에서 "Show policies matching resource"(리소스와 일치하는 정책 표시)를 클릭하고, "Resource Class Name"(리소스 클래스 이름) 드롭다운 목록에서 "Domain"(도메인)을 선택한 후 "Go"(실행)를 클릭합니다.

   CA EEM 의 "Policy Table"(정책 표) 창에 APM 도메인 리소스 액세스 정책의 목록이 표시됩니다. 삭제된 APM 도메인 리소스 액세스 정책은 나열되지 않습니다.

CA EEM APM 서버 리소스 액세스 정책 만들기 및 삭제

서버 권한을 설정하려면 CA EEM APM 서버 리소스에 대한 액세스 정책을 추가해야 합니다.

참고: 서버 리소스에 대한 기본 액세스 정책과 함께 이름이 APM 인 응용 프로그램을 만드는 Safex 스크립트 코드의 경우 *<EM_Home>/examples/authentication* 디렉터리에 위치한 *eem.register.app.xml* 샘플 파일을 참조하십시오.

참고: 또한 CA EEM 인터페이스를 사용하여 이러한 작업을 수행할 수도 있습니다. 자세한 내용은 *CA Embedded Entitlements Manager Getting Started Guide*(CA Embedded Entitlements Manager 온라인 도움말), *CA Embedded Entitlements Manager Online Help*(CA Embedded Entitlements Manager 온라인 도움말), *CA Embedded Entitlements Manager Programming Guide*(CA Embedded Entitlements Manager 프로그래밍 안내서)를 참조하십시오.

Safex 유틸리티를 사용하여 CA EEM APM 서버 리소스 액세스 정책을 만들려면

1. 일반적으로 *C:\Program Files\CA\SharedComponents\iTechnology* 에 위치한 *<EEM_Server>* 디렉터리에 Safex XML 파일을 만듭니다.

   예를 들어 *C:\Program Files\CA\SharedComponents\iTechnology\Add_server.xml* 입니다.

2. 다음 코드를 잘라내어 Safex XML 파일에 붙여 넣고, 따옴표 내의 변수를 적합한 변수로 대체하고 ID, 리소스 클래스 및 권한의 값을 지정합니다. 서버 권한에 대한 자세한 내용은 CA EEM 에서 APM 리소스 클래스 만들기 및 삭제 (페이지 95)에서 각 리소스 클래스에 허용된 권한을 결정하는 2 단계를 참조하십시오.

   참고: CA EEM 에서는 권한을 작업이라고 합니다.

```
<Safex>
   <Attach label="APM"/>
   <!-- add policies -->

   <Add>
        <Policy name="Server Admin" folder="/Policies">
        <Description>Admin group has full permission for the
server</Description>

        <Identity>gug:Admin</Identity>

        <Action>full</Action>

        <ResourceClassName>Server</ResourceClassName>
        </Policy>
     </Add>

     <Detach/>
</Safex>
```

3. 명령 프롬프트를 열고 *<EEM_Server>* 디렉터리(주로 *C:\Program Files\CA\SharedComponents\iTechnology*)로 이동합니다.

4. 다음 명령을 실행하여 Safex 스크립트를 실행합니다.

   ```
   >safex.exe -h localhost -u EiamAdmin -p <ENTER YOUR PASSWORD> -f
   <yourfilename>.xml
   ```

   예를 들면 다음과 같습니다.

   ```
   >safex.exe -h localhost -u EiamAdmin -p 1234567 -f Add_server.xml
   ```

   FIPS 모드의 CA EEM 과 통합된 응용 프로그램에 대해 Safex 유틸리티를 사용하여 CA EEM APM 서버 리소스 액세스 정책을 만들 때는 이 명령을 실행하여 Safex 스크립트를 실행합니다.

   ```
   >safex.exe -h localhost -u EiamAdmin -p <ENTER YOUR PASSWORD> -f
   <yourfilename>.xml -fips
   ```

   예를 들면 다음과 같습니다.

   ```
   >safex.exe -h localhost -u EiamAdmin -p 1234567 -f Add_server.xml -fips
   ```

5. CA EEM 에서 APM 서버 리소스를 봅니다.

   a. CA EEM 에 로그인합니다.

   b. "Manage Access Policies"(액세스 정책 관리) 탭을 클릭합니다.

   c. "Policies"(정책) 링크를 클릭합니다.

   d. "Search Policies"(정책 검색) 창에서 "Show policies matching resource"(리소스와 일치하는 정책 표시)를 클릭하고, "Resource Class Name"(리소스 클래스 이름) 드롭다운 목록에서 "Server"(서버)를 선택한 후 "Go"(실행)를 클릭합니다.

      CA EEM 의 "Policy Table"(정책 표) 창에 APM 서버 리소스 액세스 정책의 목록이 표시됩니다.

   e. "Server access policy name"(서버 액세스 정책 이름) 링크를 클릭하여 "Policy Details"(정책 정보) 창에 APM 서버 리소스에 대한 세부 정보를 표시합니다.

Safex 유틸리티를 사용하여 CA EEM APM 서버 리소스 액세스 정책을 삭제하려면

1. 일반적으로 *C:\Program Files\CA\SharedComponents\iTechnology* 에 위치한 *<EEM_Server>* 디렉터리에 Safex XML 파일을 만듭니다.

   예를 들어 *C:\Program Files\CA\SharedComponents\iTechnology\Remove_server.xml* 입니다.

2. 다음 코드를 잘라내어 Safex XML 파일에 붙여 넣고, 따옴표 내의 변수를 적합한 변수로 대체하고 ID, 리소스 클래스 및 권한의 값을 지정합니다. 서버 권한에 대한 자세한 내용은 CA EEM 에서 APM 리소스 클래스 만들기 및 삭제 (페이지 95)에서 각 리소스 클래스에 허용된 권한을 결정하는 2 단계를 참조하십시오.

   참고: CA EEM 에서는 권한을 작업이라고 합니다.

```
<Safex>
   <Attach label="APM"/>
   <Remove>
        <Policy name="Server Admin" folder="/Policies">
        <Description>Admin group has full permission for the
server</Description>
        <Identity>gug:Admin</Identity>
        <Action>full</Action>
        <ResourceClassName>Server</ResourceClassName>
        </Policy>
     </Remove>
     <Detach/>
</Safex>
```

3. 명령 프롬프트를 열고 *<EEM_Server>* 디렉터리(주로 *C:\Program Files\CA\SharedComponents\iTechnology*)로 이동합니다.

4. 다음 명령을 실행하여 Safex 스크립트를 실행합니다.

   ```
   >safex.exe -h localhost -u EiamAdmin -p <ENTER YOUR PASSWORD> -f
   <yourfilename>.xml
   ```

   예를 들면 다음과 같습니다.

   ```
   >safex.exe -h localhost -u EiamAdmin -p 1234567 -f Remove_server.xml
   ```

   FIPS 모드의 CA EEM 과 통합된 응용 프로그램에 대해 Safex 유틸리티를 사용하여 CA EEM APM 서버 리소스 액세스 정책을 삭제할 때는 이 명령을 실행하여 Safex 스크립트를 실행합니다.

   ```
   >safex.exe -h localhost -u EiamAdmin -p <ENTER YOUR PASSWORD> -f
   <yourfilename>.xml -fips
   ```

   예를 들면 다음과 같습니다.

   ```
   >safex.exe -h localhost -u EiamAdmin -p 1234567 -f Remove_server.xml -fips
   ```

5. CA EEM 에서 APM 서버 리소스를 봅니다.

   a. CA EEM 에 로그인합니다.

   b. "Manage Access Policies"(액세스 정책 관리) 탭을 클릭합니다.

   c. "Policies"(정책) 링크를 클릭합니다.

   d. "Search Policies"(정책 검색) 창에서 "Show policies matching resource"(리소스와 일치하는 정책 표시)를 클릭하고, "Resource Class Name"(리소스 클래스 이름) 드롭다운 목록에서 "Server"(서버)를 선택한 후 "Go"(실행)를 클릭합니다.

   CA EEM 의 "Policy Table"(정책 표) 창에 APM 서버 리소스 액세스 정책의 목록이 표시됩니다. 삭제된 APM 서버 리소스 액세스 정책은 나열되지 않습니다.

CA EEM APM 프런트엔드 및 비즈니스 서비스 리소스 액세스 정책 만들기 및 삭제

응용 프로그램 심사 맵 권한을 설정하기 위해 프런트엔드(CA EEM 에서는 비즈니스 응용 프로그램이라고도 함) 및 비즈니스 서비스에 대한 액세스 정책을 CA EEM APM 응용 프로그램 리소스로 추가해야 합니다.

참고: 또한 CA EEM 인터페이스를 사용하여 이러한 작업을 수행할 수도 있습니다. 자세한 내용은 *CA Embedded Entitlements Manager Getting Started Guide*(CA Embedded Entitlements Manager 온라인 도움말), *CA Embedded Entitlements Manager Online Help*(CA Embedded Entitlements Manager 온라인 도움말), *CA Embedded Entitlements Manager Programming Guide*(CA Embedded Entitlements Manager 프로그래밍 안내서)를 참조하십시오.

Safex 유틸리티를 사용하여 CA EEM APM 프런트엔드 또는 비즈니스 서비스 리소스 액세스 정책을 만들려면

1. 일반적으로 *C:\Program Files\CA\SharedComponents\iTechnology* 에 위치한 *<EEM_Server>* 디렉터리에 Safex XML 파일을 만듭니다.

   예를 들어 *C:\Program Files\CA\SharedComponents\iTechnolog\Add_application_policy.xml* 입니다.

2. 다음 코드를 잘라내어 Safex XML 파일에 붙여 넣고, 따옴표 내의 변수를 적합한 변수로 대체하고 ID, 리소스 및 권한의 값을 지정합니다. 응용 프로그램 권한에 대한 자세한 내용은 CA EEM 에서 APM 리소스 클래스 만들기 및 삭제 (페이지 95)에서 각 리소스 클래스에 허용된 권한을 결정하는 2 단계를 참조하십시오.

   참고: CA EEM 에서는 권한을 작업이라고 합니다.

   참고: 아래의 샘플 코드에서는 Guest 사용자에게 응용 프로그램 심사 맵의 Banking Application 이라는 응용 프로그램을 볼 수 있는 권한을 부여합니다.

```
<Safex>
   <Attach label="APM"/>
   <!-- add policies -->

   <Add>
        <Policy name="Business Application Write to a banking application"
folder="/Policies">
        <Description>Guest Group has write permission for a Banking
Application.</Description>

        <ResourceClassName>Business Application</ResourceClassName>

        <Resource>Banking Application</Resource>

        <Action>write</Action>

        <Identity>ug:Guest</Identity>
        </Policy>
     </Add>
     <Detach/>
</Safex>
```

3. 명령 프롬프트를 열고 *<EEM_Server>* 디렉터리(주로 *C:\Program Files\CA\SharedComponents\iTechnology*)로 이동합니다.

4. 다음 명령을 실행하여 Safex 스크립트를 실행합니다.

   ```
   >safex.exe -h localhost -u EiamAdmin -p <ENTER YOUR PASSWORD> -f
   <yourfilename>.xml
   ```

   예를 들면 다음과 같습니다.

   ```
   >safex.exe -h localhost -u EiamAdmin -p 1234567 -f Add_application_policy.xml
   ```

   FIPS 모드의 CA EEM 과 통합된 응용 프로그램에 대해 Safex 유틸리티를 사용하여 CA EEM 프런트엔드 또는 비즈니스 서비스 리소스 액세스 정책을 만들 때는 이 명령을 실행하여 Safex 스크립트를 실행합니다.

   ```
   >safex.exe -h localhost -u EiamAdmin -p <ENTER YOUR PASSWORD> -f
   <yourfilename>.xml -fips
   ```

   예를 들면 다음과 같습니다.

   ```
   >safex.exe -h localhost -u EiamAdmin -p 1234567 -f Add_application_policy.xml
   -fips
   ```

5. CA EEM 에서 APM 응용 프로그램 리소스 정책을 봅니다.

   a. CA EEM 에 로그인합니다.

   b. "Manage Access Policies"(액세스 정책 관리) 탭을 클릭합니다.

   c. "Policies"(정책) 링크를 클릭합니다.

   d. "Search Policies"(정책 검색) 창에서 "Show policies matching resource"(리소스와 일치하는 정책 표시)를 클릭하고, "Resource Class Name"(리소스 클래스 이름) 드롭다운 목록에서 응용 프로그램 정책 이름을 선택한 후 "Go"(실행)를 클릭합니다.

      CA EEM 의 "Policy Table"(정책 표) 창에 APM 응용 프로그램 리소스 액세스 정책의 목록이 표시됩니다.

   e. 응용 프로그램 리소스 액세스 정책 이름의 링크를 클릭하여 "Policies Details"(정책 정보) 창에서 APM 응용 프로그램 리소스에 대한 좀 더 세부적인 정보를 봅니다.

Safex 유틸리티를 사용하여 CA EEM APM 프런트엔드 또는 비즈니스 서비스 리소스에 대한 액세스 정책을 삭제하려면

1. 일반적으로 *C:\Program Files\CA\SharedComponents\iTechnology* 에 위치한 *<EEM_Server>* 디렉터리에 Safex XML 파일을 만듭니다.

   예를 들어 *C:\Program Files\CA\SharedComponents\iTechnology\Remove_application_policy.xml* 입니다.

2. 다음 코드를 잘라내어 Safex XML 파일에 붙여 넣고, 따옴표 내의 변수를 적합한 변수로 대체하고 ID, 리소스 및 권한의 값을 지정합니다. 응용 프로그램 권한에 대한 자세한 내용은 CA EEM 에서 APM 리소스 클래스 만들기 및 삭제 (페이지 95)에서 각 리소스 클래스에 허용된 권한을 결정하는 2 단계를 참조하십시오.

   참고: CA EEM 에서는 권한을 작업이라고 합니다.

```
<Safex>
   <Attach label="APM"/>
       <Remove>
        <Policy name="Business Application Write to a banking application"
folder="/Policies">
        <Description>Guest Group has write permission for a Banking
Application.</Description>

        <ResourceClassName>Business Application</ResourceClassName>

        <Resource>Banking Application</Resource>

        <Action>write</Action>

        <Identity>ug:Guest</Identity>
        </Policy>
       </Remove>
     <Detach/>
</Safex>
```

3. 명령 프롬프트를 열고 *<EEM_Server>* 디렉터리(주로 *C:\Program Files\CA\SharedComponents\iTechnology*)로 이동합니다.

4. 다음 명령을 실행하여 Safex 스크립트를 실행합니다.

   ```
   >safex.exe -h localhost -u EiamAdmin -p <ENTER YOUR PASSWORD> -f
   <yourfilename>.xml
   ```

   예를 들면 다음과 같습니다.

   ```
   >safex.exe -h localhost -u EiamAdmin -p 1234567 -f Remove_application_policy.xml
   ```

   FIPS 모드의 CA EEM 과 통합된 응용 프로그램에 대해 Safex 유틸리티를 사용하여 CA EEM 프런트엔드 또는 비즈니스 서비스 리소스 액세스 정책을 삭제할 때는 이 명령을 실행하여 Safex 스크립트를 실행합니다.

   ```
   >safex.exe -h localhost -u EiamAdmin -p <ENTER YOUR PASSWORD> -f
   <yourfilename>.xml -fips
   ```

   예를 들면 다음과 같습니다.

   ```
   >safex.exe -h localhost -u EiamAdmin -p 1234567 -f Remove_application_policy.xml
   -fips
   ```

5. CA EEM 에서 APM 응용 프로그램 리소스를 봅니다.

   a. CA EEM 에 로그인합니다.

   b. "Manage Access Policies"(액세스 정책 관리) 탭을 클릭합니다.

   c. "Policies"(정책) 링크를 클릭합니다.

   d. "Search Policies"(정책 검색) 창에서 "Show policies matching resource"(리소스와 일치하는 정책 표시)를 클릭하고, "Resource Class Name"(리소스 클래스 이름) 드롭다운 목록에서 응용 프로그램 정책 이름을 선택한 후 "Go"(실행)를 클릭합니다.

   CA EEM 의 "Policy Table"(정책 표) 창에 APM 응용 프로그램 리소스 액세스 정책의 목록이 표시됩니다. 삭제한 APM 응용 프로그램 액세스 정책이 나열되지 않습니다.

클러스터에 CA EEM 설정

클러스터에 CA EEM 보안을 제공하려면 CA EEM 에서 모든 Enterprise Manager 가 동일한 응용 프로그램에 연결되도록 *realms.xml* 파일을 구성해야 합니다. 또한 에이전트나 TIM 의 수를 늘리기 위해 클러스터에 새 Collector 를 추가하는 경우 다음 지침을 따릅니다.

다음 단계를 따르십시오.

중요! 권한 부여에 CA EEM 을 사용하는 경우 CA EEM 에서 Enterprise Manager 가 하나 이상의 응용 프로그램에 연결되어야 합니다. 이는 CA EEM 이 응용 프로그램을 사용하여 권한을 정의하는 리소스 클래스와 액세스 정책을 저장하기 때문입니다.

1. Enterprise Manager(Collector, MOM 또는 CDV)에서 CA EEM 권한 부여에 대해 *realms.xml* 파일을 구성합니다.
   a. *<EM_Home>/config* 디렉터리에 있는 *realms.xml* 파일을 엽니다.
   b. CA EEM 에서 Enterprise Manager 와 연결된 응용 프로그램 이름으로 *appname* 속성을 설정합니다. 예를 들어 *APM* 이라는 이름일 수 있습니다.

      이는 CA EEM 서버를 구성할 때 사용한 APM 응용 프로그램 이름과 동일합니다.
   c. *enableAuthorization* 속성을 *True* 로 설정합니다.
   d. *realms.xml* 파일을 저장합니다.
   e. *realms.xml* 의 변경 사항이 적용되도록 Enterprise Manager 를 다시 시작합니다.
2. 클러스터의 각 Enterprise Manager 에 대해 앞의 1 단계를 반복합니다.

   클러스터의 모든 Enterprise Manager 를 CA EEM 의 동일한 응용 프로그램에 연결하면 CA EEM 보안을 클러스터 전체에서 사용하도록 설정할 수 있습니다.

로컬 보안에서 CA EEM 보안으로 마이그레이션

로컬 인증 및 권한 부여를 사용하여 Introscope 를 실행하고 있는 상태에서 CA EEM 기반 인증 및 권한 부여를 배포하려는 경우 다음과 같이 합니다.

- CA EEM 설치
- 인증에 대해 CA EEM 구성
- 권한 부여에 대해 CA EEM 구성

CA EEM 기반 인증 및 로컬 권한 부여를 배포할 수 있습니다. 자세한 내용은 로컬 권한 부여를 사용하도록 CA EEM 구성 (페이지 117)을 참조하십시오.

CA EEM 의 보안 배포를 완전하게 이해하려면 CA EEM 을 사용한 Introscope 보안 (페이지 64) 항목의 시작 부분을 읽어 보십시오.

LDAP 보안에서 CA EEM 보안으로 마이그레이션

LDAP 인증 및 로컬 권한 부여를 사용하여 Introscope 를 실행하고 있는 상태에서 CA EEM 기반 인증 및 권한 부여를 배포하려는 경우 다음과 같이 하십시오.

- CA EEM 설치
- 인증에 대해 CA EEM 구성
- 권한 부여에 대해 CA EEM 구성

CA EEM 의 보안 배포를 완전하게 이해하려면 CA EEM 을 사용한 Introscope 보안 (페이지 64) 항목의 시작 부분을 읽어 보십시오.

로컬 권한 부여를 사용하도록 CA EEM 구성

EEM 보안 영역에서 CA APM 사용자 인증을 수행하는 경우 기본적으로 EEM 영역에서 CA APM 사용자 권한 부여도 수행합니다. 하지만 *realms.xml* 의 *enableAuthorization* 플래그가 *false* 로 설정된 경우 CA APM 사용자는 CA EEM 에 인증된 후 로컬 권한 부여를 사용하고 CA EEM 권한 부여를 사용하지 않습니다. 이러한 경우 CA EEM 보안 사용자 그룹의 구성원인 CA APM 사용자에 대한 권한 부여 액세스 정책은 로컬 영역에서 제공됩니다. SiteMinder 또는 LDAP 와 함께 구성된 CA EEM 을 인증에 사용하려는 경우와 같이 로컬 권한 부여를 사용하도록 선택할 수도 있지만 권한은 로컬 영역에 유지해야 합니다.

Introscope 의 경우 로컬 영역 권한은 *domains.xml* 및 *server.xml* 파일에 정의됩니다.

CA CEM 의 경우 로컬 영역 액세스 정책은 보안 사용자 그룹 구성원에 기반합니다.

CA APM 에서 CA EEM 인증을 수행한 후 로컬 권한 부여를 수행하려면 CA EEM 의 APM 보안 사용자 그룹에 사용자를 할당해야 합니다. 하지만 이러한 경우 CA EEM 에 액세스 정책을 만들 필요가 없습니다.

여기서 권한 부여에 로컬 보안을 사용한다는 것은 다음을 의미합니다.

- *realms.xml* 의 *enableAuthorization* 플래그가 *false* 로 설정됩니다.
- Introscope 의 경우 CA EEM 에서 사용자 및 그룹을 만들고 *domains.xml* 파일에 권한을 할당합니다.
- CA CEM 의 경우 CA EEM 에서 사용자뿐 아니라 기본 보안 그룹 4 개를 모두 만들어야 합니다. 예를 들어 CA EEM 에서 *cemadmin* 사용자와 함께 *CEM 시스템 관리자* 보안 그룹을 만듭니다. 그런 다음 *cemadmin* 을 *CEM 시스템 관리자* 보안 그룹의 구성원으로 할당하면 *CEM 시스템 관리자* 보안 그룹의 권한이 *cemadmin* 에 제공됩니다. CA CEM 의 기본 보안 그룹 4 개에 대한 자세한 내용은 CA CEM 의 기본 보안 사용자 그룹에 연결된 메뉴 항목 및 권한 (페이지 135)을 참조하십시오.

다음 단계를 따르십시오.

1. *<EM_Home>/config* 디렉터리에 있는 *realms.xml* 파일을 엽니다.
2. *enableAuthorization* 속성을 *false* 로 설정합니다.

   이 값을 *false* 로 설정하면 CA EEM 은 인증만 수행하고 권한 부여에는 로컬 보안 영역이 사용됩니다. 자세한 내용은 realms.xml 에 CA EEM 인증 구성 (페이지 69)을 참조하십시오. 로컬 권한 부여에 대한 자세한 내용은 로컬 보안을 사용한 Introscope 보안 (페이지 36)을 참조하십시오.
3. *realms.xml* 파일을 저장합니다.
4. 도메인 권한을 구성합니다. 자세한 내용은 domains.xml 에 Introscope 도메인 권한 구성 (페이지 44)을 참조하십시오.
5. Enterprise Manager 서버 권한을 구성합니다. 자세한 내용은 Enterprise Manager 서버 권한 구성 (페이지 48)을 참조하십시오.

Introscope SSO(Single Sign-On) 정보

SSO(Single Sign-On)를 사용하면 사용자는 각 응용 프로그램을 액세스할 때마다 로그인할 필요 없이 한 번만 로그인하여 여러 응용 프로그램에 액세스할 수 있습니다.

Introscope 에 로그인할 때 사용자 브라우저에서 쿠키를 허용하면 SSO 가 자동으로 구현됩니다. 그런 다음 사용자는 개별적으로 로그인하고 매번 인증받을 필요 없이 CA APM 웹 응용 프로그램 간을 탐색할 수 있습니다. 사용자 브라우저에서 쿠키를 허용하지 않으면 SSO 가 구현되지 않으므로 사용자는 개별 CA APM 응용 프로그램에 액세스할 때마다 로그인해야 합니다.

다음 Introscope 웹 응용 프로그램이 SSO 를 지원합니다.

- Web Start Workstation
- WebView
- CEM 콘솔

Introscope Workstation(씩 클라이언트)은 SSO 를 지원하지 않습니다.

SiteMinder SSO 및 Introscope 보안 정보

CA EEM 을 사용하여 Introscope 보안을 배포하고 인증을 위해 CA EEM 서버와 CA SiteMinder 를 통합한 경우 Introscope 웹 응용 프로그램은 SiteMinder 의 SSO 기능을 사용할 수 있습니다. 인증에 SiteMinder 를 사용하도록 CA EEM 을 배포하는 방법에 대한 자세한 내용은 CA SiteMinder 를 사용하여 CA EEM 인증 구성 (페이지 74)을 참조하십시오.

웹 응용 프로그램에서 Introscope 자격 증명 및 SiteMinder SSO 자격 증명을 모두 검색한 경우 웹 응용 프로그램은 먼저 Introscope 자격 증명을 사용하여 인증하려 합니다. 이 인증에 실패하면 웹 응용 프로그램은 SiteMinder 자격 증명을 사용합니다.

SiteMinder SSO 에 대한 자세한 내용은 *CA APM for CA SiteMinder Web Access Manager Guide*(CA APM for CA SiteMinder Web Access Manager 안내서)를 참조하십시오.

응용 프로그램 심사 맵 보안

CA EEM 을 사용하여 Introscope 권한 부여를 배포한 경우 응용 프로그램 심사 맵에서 프런트엔드 및 비즈니스 서비스를 볼 수 있는 사용자 권한을 설정할 수 있습니다. 이들 권한은 CA EEM 인터페이스나 Safex 스크립트를 실행하여 비즈니스 응용 프로그램(프런트엔드) 및 비즈니스 서비스 리소스에 대한 권한(쓰기, 읽기 또는 중요한 데이터 읽기)을 제공하여 설정할 수 있습니다.

보안에 CA EEM 을 사용하지 않는 경우 또는 보안을 위해 CA EEM 을 배포하지만 연결된 액세스 정책에 CA EEM 비즈니스 응용 프로그램 및 비즈니스 서비스 리소스로 특정 프런트엔드 또는 비즈니스 서비스를 추가하지 *않*는 경우 사용자는 응용 프로그램 심사 맵에서 모든 비즈니스 응용 프로그램 및 비즈니스 서비스를 볼 수 있습니다. CA EEM 비즈니스 응용 프로그램 및 비즈니스 서비스 리소스에 대한 자세한 내용은 CA EEM 에서 APM 리소스 클래스 만들기 및 삭제 (페이지 95)를 참조하십시오. 응용 프로그램 심사 맵을 사용하는 경우 사용자가 볼 수 있는 항목에 대한 자세한 내용은 *CA APM Workstation User Guide*(CA APM Workstation 사용자 안내서)를 참조하십시오.

도메인 보안은 응용 프로그램 심사 맵과 더불어 프런트엔드 및 비즈니스 서비스 맵 보안에도 적용됩니다. 또한 SuperDomain 보안은 모든 프런트엔드 및 비즈니스 서비스 보안을 무시합니다. 도메인 보안은 사용자 및 그룹이 볼 수 있는 에이전트 데이터를 제한합니다. 자세한 내용은 응용 프로그램 심사 맵 보안을 무시하는 SuperDomain 보안 (페이지 122)을 참조하십시오.

eem.register.app.xml 스크립트를 실행하여 기본 CA APM 응용 프로그램을 설정하는 경우 스크립트를 통해 아래에 설명된 비즈니스 서비스 및 비즈니스 응용 프로그램(프런트엔드) 리소스 클래스와 작업이 제공됩니다. 자세한 내용은 CA EEM 권한 부여 구성 (페이지 75)을 참조하십시오.

응용 프로그램 심사 맵 보안을 배포하려면 CA EEM 에서 다음 주요 단계를 수행해야 합니다.

1. 사용자 그룹 및 사용자를 정의합니다.

   APM 그룹 (페이지 87) 및 APM 사용자 (페이지 91) 예제 스크립트를 사용할 수 있습니다.

2. 사용자, 그룹 및 권한(CA EEM 에서 '작업'이라 함)을 기반으로 하여 액세스 정책을 만듭니다.

   스크립트 예제는 CA EEM 액세스 정책 정보 (페이지 103)를 참조하십시오.

3. 각 액세스 정책을 리소스 클래스에 연결합니다. 그런 다음 특정 리소스를 액세스 정책에 추가하여 정책을 한층 더 제한할 수 있습니다.
4. 개별 비즈니스 서비스와 비즈니스 응용 프로그램뿐 아니라 비즈니스 서비스와 비즈니스 응용 프로그램 리소스 클래스를 정책에 추가합니다.

   참고: 개별 비즈니스 서비스와 비즈니스 응용 프로그램을 해당 비즈니스 클래스의 구성원으로 정의할 필요는 없습니다.

자세한 내용은 CA EEM 에서 APM 리소스 클래스 만들기 및 삭제 (페이지 95)의 다음 단계를 참조하십시오.

- 응용 프로그램 심사 맵 보안을 제공할 비즈니스 서비스 리소스 클래스 권한을 결정합니다.
- 프런트엔드에 응용 프로그램 심사 맵 보안을 제공할 비즈니스 응용 프로그램 리소스 클래스 권한을 결정합니다.

참고: 비즈니스 서비스 및 비즈니스 응용 프로그램(프런트엔드)의 경우 부여된 모든 권한은 사용자에게 응용 프로그램 심사 맵을 볼 수 있는 액세스 권한을 줍니다.

참고: 비즈니스 서비스 또는 비즈니스 응용 프로그램을 볼 수 있도록 사용자 권한을 변경하는 경우 사용자가 Workstation 에서 로그아웃하고 다시 로그인해야 이러한 변경 사항이 응용 프로그램 심사 맵에 반영됩니다.

참고: 비즈니스 서비스 또는 비즈니스 응용 프로그램 정책에 지정된 리소스가 없으면 비즈니스 서비스 또는 비즈니스 응용 프로그램 정책은 비즈니스 서비스나 비즈니스 응용 프로그램 리소스 클래스 내에 있는 모든 리소스에 적용됩니다.

프런트엔드를 CA EEM 비즈니스 응용 프로그램 리소스로 추가하고 연결된 비즈니스 응용 프로그램 리소스 클래스 사용자 또는 그룹에게 응용 프로그램 심사 맵에서 해당 프런트엔드를 볼 수 있는 권한을 부여하지 않으면 심사 맵 트리에 나열된 프런트엔드가 해당 사용자 또는 그룹에게 표시되지 않습니다. 비즈니스 서비스의 경우도 마찬가지로, 사용자에게 권한이 부여되지 않으면 트리에 나타나지 않습니다. 하지만 사용자가 권한을 갖고 있지 않은 프런트엔드가 사용자나 그룹이 볼 수 있는 다른 프런트엔드나 비즈니스 서비스에 의해 호출되면 해당 프런트엔드가 맵에 표시되지만 다음과 같은 제한이 있습니다.

- 비활성화된 상태로 나타납니다.
- 선택할 수 없습니다.
- 종속성 또는 메트릭 데이터를 표시하지 않습니다.

하지만 사용자와 그룹은 메트릭 브라우저 탭 트리에서 이 프런트엔드에 대한 개별 에이전트 데이터를 볼 수 있습니다.

중요! 사용자에게 SuperDomain 권한이 있는 경우 사용자는 응용 프로그램 심사 맵에서 모든 프런트엔드 및 비즈니스 서비스를 볼 수 있습니다. 자세한 내용은 응용 프로그램 심사 맵 보안을 무시하는 SuperDomain 보안 (페이지 122)을 참조하십시오.

Safex 스크립트를 사용하여 응용 프로그램 심사 맵 권한을 설정하는 지침은 다음을 참조하십시오.

- CA EEM 에서 APM 리소스 클래스 만들기 및 삭제 (페이지 95)
- CA EEM APM 프런트엔드 및 비즈니스 서비스 리소스 액세스 정책 만들기 및 삭제 (페이지 111)

참고: 응용 프로그램 심사 맵 보안을 사용하도록 설정한 경우 비즈니스 응용 프로그램 및 비즈니스 서비스가 Workstation 에 표시되는 방식에 대한 자세한 내용은 *CA APM Workstation User Guide*(CA APM Workstation 사용자 안내서)를 참조하십시오.

SuperDomain 보안은 응용 프로그램 심사 맵 보안을 무시합니다.

도메인 보안은 응용 프로그램 심사 맵과 더불어 프런트엔드 및 비즈니스 서비스 맵 보안에도 적용됩니다. 도메인 보안은 사용자 및 그룹이 볼 수 있는 에이전트 데이터를 제한합니다. 도메인 보안에 대한 자세한 내용은 Introscope 도메인 정의 및 구성 (페이지 23)과 domains.xml 에 Introscope 도메인 권한 구성 (페이지 44)을 참조하십시오.

"심사 맵" 탭에서 도메인 보안을 사용하여 다음과 같이 사용자 및 그룹이 볼 수 있는 에이전트를 제한합니다.

- 응용 프로그램 심사 맵 아래의 물리적 위치 목록에 나열된 에이전트
- 모든 메트릭 디스플레이 아래의 물리적 위치 목록에 나열된 에이전트. 이들은 심사 맵 트리의 하위 노드가 선택된 경우에 표시됩니다. 예를 들어 건전성 노드나 개별 메트릭 노드를 선택하면 표시됩니다.

SuperDomain 보안은 응용 프로그램 심사 맵 보안보다 우선 적용됩니다. 이는 영역(로컬 또는 EEM)에 상관없이 *SuperDomain* 액세스 권한을 부여받은 모든 사용자는 응용 프로그램 심사 맵의 모든 프런트엔드 및 비즈니스 서비스를 볼 수 있도록 허용된다는 의미입니다. 비즈니스 서비스 및 비즈니스 응용 프로그램 읽기 권한이 부여되지 않은 경우에도 마찬가지입니다.

예를 들어 Introscope 에서 A, B 및 C 라는 세 프런트엔드를 모니터링하고 있고 Introscope 의 사용자인 Tai 에게 A 프런트엔드를 볼 수 있는 권한을 부여한 경우 Tai 에게 모든 에이전트를 볼 수 있는 *SuperDomain* 도메인 권한이 있으면 Tai 는 응용 프로그램 심사 맵과 Investigator 트리에 있는 세 프런트엔드를 모두 볼 수 있습니다.

Introscope 보안 문제 해결

다음 표에는 Introscope 보안 문제 해결에 유용한 팁 몇 가지가 나와 있습니다.

증상

CA APM 그룹, 사용자 및 리소스 클래스를 로드하기 위해 Safex 스크립트를 실행하는 경우 오류 메시지가 나타납니다.

오류 메시지는 다음 예제와 같이 나타납니다.

```
"1375 [0x00000458] ERROR PozFactory null - PozFactory::attachPoz - Error invoking
iPoz::ClientAttach on host localhost 1375 [0x00000458] ERROR PozFactory null -
PozFactory::attachPoz Error: Bad signature: incompatible signature digest type in the
request from host [192.168.200.1.ca.com:1331]. Server is running in [Fips_Mode_On]
and request signature digest type is [ITECH_DIGEST_MD5]. FIPS does not support
ITECH_DIGEST_MD5 digest type"
```

해결 방법

CA EEM 서버가 FIPS 전용 모드입니다.

CA EEM 서버 설정을 FIPS 이외의 모드로 변경하십시오.

증상

Introscope 사용자가 Introscope 에 로그인할 때 오류 메시지가 나타납니다.

Introscope 사용자가 로그인할 수 없습니다.

해결 방법

사용자 이름과 암호가 올바로 입력되었는지 확인하십시오.

증상

Enterprise Manager 가 CA EEM APM 응용 프로그램 인스턴스에 연결되어 있는지 확인할 수 없습니다.

Introscope 가 CA EEM 에 연결되어 있는지 알 수 없습니다.

해결 방법

<EM_Home>/logs/IntroscopeEnterpriseManager.log 파일의 로그 메시지를 확인하십시오.

아래의 로그 메시지를 통해 다음과 같은 정보를 알 수 있습니다.

- CA EEM 에서 Enterprise Manager 가 연결되어 있는 응용 프로그램
- CA EEM 서버의 위치
- CA EEM 서버가 사용자 및 그룹을 가져오기 위해 CA EEM 을 사용하는지 아니면 외부 디렉터리(LDAP 또는 SiteMinder)를 사용하는지 여부

예:

```
8/05/09 04:15:59 PM PDT [INFO] [Manager.EemRealm] EEM realm attached to application
"APM" in EEM server at <EEM_Machine_Name> using SiteMinder
```

증상

CA EEM 과 Enterprise Manager 의 연동에 문제가 있습니다.

Introscope CA EEM 연결을 디버깅합니다.

해결 방법

CA EEM 관련 로그 메시지를 표시하도록 CA EEM 디버그 속성을 설정하십시오. 자세한 내용은 CA EEM 관련 메시지의 로깅 구성 (페이지 69)을 참조하십시오.

Introscope 보안 메커니즘

조직에 필요한 보안 요구 사항에 따라 다음 표에 나열된 Introscope 보안 메커니즘 중 적합한 메커니즘을 사용합니다.

제공할 보안 메커니즘	보호 기능
Workstation, WebView, Web Start Workstation 또는 CEM 콘솔에서 Enterprise Manager 로 로그인할 때 사용하는 암호 변경 및 보호	이 보안 베스트 프랙티스를 따르는 것이 가장 좋습니다. Workstation, WebView 및 Web Start 암호에 대한 자세한 내용은 *CA APM Workstation 사용자 안내서*를 참조하십시오. CEM 콘솔 암호에 대한 자세한 내용은 CA CEM 암호 관리 (페이지 131)를 참조하십시오.
Enterprise Manager 가 실행되는 Windows 또는 Linux 컴퓨터에 파일 시스템 보안 설정 및 사용	로컬 보안을 위해 APM 도메인을 설정할 때 허용된 사용자만 *users.xml* 파일을 액세스할 수 있습니다.
Collector 및 MOM 사이의 암호화 키 구성을 설정 및 사용	허용된 사용자만 Collector 에 액세스할 수 있습니다. 자세한 내용은 보안 인증에 대해 공개 및 개인 키 구성 (페이지 31)을 참조하십시오.
APM 데이터베이스 암호 변경 및 보호	허용된 사용자만 APM 데이터베이스에 액세스할 수 있습니다. 자세한 내용은 *CA APM 설치 및 업그레이드 안내서*를 참조하십시오.
숙련된 데이터베이스 관리자	일반 APM 데이터베이스 건전성을 유지 관리합니다.
IntroscopeAgent.profile 파일의 SSL 통신 속성을 구성하여 SSL 을 통한 에이전트 및 Enterprise Manager 간 통신을 사용하도록 설정	에이전트와 Enterprise Manager 간 통신의 보안을 유지합니다. 자세한 내용은 *CA APM Java Agent 구현 안내서* 또는 *CA APM .NET 에이전트 구현 안내서*를 참조하십시오.
Enterprise Manager 및 브라우저 간 암호화된 SSL 통신	Enterprise Manager 와 브라우저 간 통신의 보안을 유지합니다. 자세한 내용은 HTTPS 로만 Enterprise Manager 액세스 제한 (페이지 164)을 참조하십시오.
Introscope 인증	허용된 사용자만 Introscope 및 CA APM 에 로그인할 수 있습니다.
Introscope 권한 부여	허용된 사용자만 Introscope 도메인에 액세스할 수 있습니다.

제공할 보안 메커니즘	보호 기능
응용 프로그램 심사 맵 보안	허용된 사용자만 응용 프로그램 심사 맵의 특정 비즈니스 서비스 및 프런트엔드를 볼 수 있습니다. 자세한 내용은 응용 프로그램 심사 맵 보안 (페이지 120)을 참조하십시오.

제 4 장: CA CEM 보안

CA CEM 을 업그레이드하는 경우 *CA APM 설치 및 업그레이드 안내서*에서 보안과 관련된 업그레이드 항목을 참조하십시오.

다음은 알아야 하는 CA CEM 보안 관련 정보 목록입니다.

1. CA CEM 보안 이해 (페이지 128)
2. CA CEM 사용자 및 보안 사용자 그룹에 대해 자세히 알아보기 (페이지 134)
3. CA CEM 암호 유지 관리에 대해 자세히 알아보기 (페이지 131)
4. 보안을 위해 CA Embedded Entitlements Manager(CA EEM)를 배포하는 경우 다음을 참조하십시오.
   - CA CEM EEM 보안 (페이지 137)
   - 필요한 CA CEM 사용자 및 보안 사용자 그룹의 유지 관리 (페이지 138)
   - 리소스 클래스 (페이지 139)
   - 리소스 (페이지 141)
   - 액세스 정책 (페이지 142)
5. 로컬 보안을 배포하는 경우 다음을 참조하십시오.
   - CA CEM 로컬 보안 (페이지 148)
   - 필요한 CA CEM 사용자 유지 관리 (페이지 148)
6. 개인 매개 변수 정의 (페이지 150)
7. 보안과 관련된 HTTP 응답 및 요청 콘텐츠에 대해 자세히 알아보기 (페이지 152)
8. (선택 사항) FIPS 140-2 암호화 적용 (페이지 160)
9. (선택 사항) HTTPS 를 통한 TIM 통신 구성 (페이지 163)
10. (선택 사항) HTTPS 로 브라우저와 Enterprise Manager 간 통신 제한 (페이지 164)

CA CEM 보안 메커니즘

조직에 필요한 보안 요구 사항에 따라 다음 표에 나열된 CA CEM 보안 메커니즘 중 적합한 메커니즘을 사용합니다.

제공할 보안 메커니즘	보호 기능
데이터 센터의 보호 영역 내에서 CA CEM 실행 및 Introscope 보안 설정	Enterprise Manager 컴퓨터에 액세스합니다. 이는 Enterprise Manager 파일 시스템에 대한 권한 없는 액세스를 방지합니다.
숙련된 데이터베이스 관리자	일반 APM 데이터베이스 건전성을 유지 관리합니다.
APM 데이터베이스 암호 변경 및 보호	허용된 사용자만 APM 데이터베이스에 액세스할 수 있습니다. 자세한 내용은 *CA APM 설치 및 업그레이드 안내서*를 참조하십시오.
각 TIM 컴퓨터에 대한 Linux 루트 계정의 기본 암호 변경	TIM 데이터를 보호합니다. 자세한 내용은 *CA APM 설치 및 업그레이드 안내서*를 참조하십시오.
Workstation, WebView, Web Start Workstation 또는 CEM 콘솔에서 Enterprise Manager 로 로그인할 때 사용하는 암호 변경 및 보호	Workstation, WebView 및 Web Start 암호에 대한 자세한 내용은 *CA APM Workstation 사용자 안내서*를 참조하십시오. CEM 콘솔 암호에 대한 자세한 내용은 CA CEM 암호 관리 (페이지 131)를 참조하십시오.
Enterprise Manager 및 TIM 간 암호화된 SSL 통신	Enterprise Manager 와 TIM 간 통신의 보안을 유지합니다. 자세한 내용은 HTTPS 를 통한 TIM 통신 구성 (페이지 163)을 참조하십시오.
Enterprise Manager 및 브라우저 간 암호화된 SSL 통신	Enterprise Manager 와 브라우저 간 통신의 보안을 유지합니다. 자세한 내용은 HTTPS 로만 Enterprise Manager 액세스 제한 (페이지 164)을 참조하십시오.
FIPS 호환 보안	FIPS(Federal Information Processing Standards)를 통해 보안 수준을 강화합니다. 자세한 내용은 FIPS 140-2 호환 암호화 (페이지 160)를 참조하십시오.

제공할 보안 메커니즘	보호 기능
CA CEM 인증	허용된 사용자만 CA CEM 에 로그인할 수 있습니다.
CA CEM 권한 부여	특정 사용자가 볼 수 있는 CEM 콘솔 탭과 해당 사용자가 작업할 수 있는 대상 데이터를 결정하는 액세스 정책입니다.
Tim 웹 보호 옵션 구성	사이트 간 위조 요청으로부터 TIM 웹 페이지를 보호합니다. 자세한 내용은 "TIM 에 대한 웹 보호를 구성하는 방법"을 참조하십시오.

참고: CA APM 보안의 기초 지식이 부족한 사용자는 CA APM 보안 요약 (페이지 11) 및 Introscope 의 보안 검사법 (페이지 35)을 참조하십시오.

CA APM 보안을 설정할 때 조직에서는 단일 보안 영역을 배포할지, 아니면 혼합 보안 영역을 사용할지 결정해야 합니다. CA APM 사용자가 CA CEM 에 액세스할 수 있도록 하려면 로컬, CA EEM 또는 LDAP 영역 중 하나를 배포해야 합니다.

TIM 에 대한 웹 보호를 구성하는 방법

TIM 웹 페이지를 사이트 간 위조 요청으로부터 보호하려면 "Configure Tim Web Protect Option"(Tim 웹 보호 옵션 구성)을 설정합니다.

다음 단계를 따르십시오.

1. "TIM Setup"(TIM 설정) 페이지에 액세스합니다.

   "TIM Setup"(TIM 설정) 페이지에 액세스하는 방법에 대해서는 *APM 구성 및 관리 안내서*의 "CEM 콘솔 및 설정 페이지 액세스"를 참조하십시오.

2. "Configure Tim Web Protect Option"(Tim 웹 보호 옵션 구성)을 클릭합니다.
3. 응용 프로그램의 요구 사항에 따라 다음과 같은 페이지 보호 옵션 중에서 선택합니다.
   - Pages that change the state of the system(시스템의 상태를 변경하는 페이지)
   - Pages that display system information(시스템 정보를 표시하는 페이지)
4. "저장"을 클릭합니다.

   TIM 보호가 구성되었습니다.

중요! 페이지에 대해 "TIM Web Protect"(TIM 웹 보호) 옵션을 사용하도록 설정한 후에는 직접 액세스하기 위해 해당 페이지를 책갈피로 지정할 수 없습니다.

CA CEM 인증 정보

로컬 영역을 사용하여 CA CEM 사용자를 인증하는 환경의 경우 *<EM_Home>/config* 디렉터리의 *users.xml* 파일에서 CA CEM 으로 CA CEM 사용자 자격 증명이 제공됩니다.

참고: Wily CEM 4.5 에서 업그레이드하여 로컬 보안을 사용하는 경우 Wily CEM 4.5 사용자는 *usersCEM45.xml* 파일에 존재할 수 있습니다. 자세한 내용은 *CA APM 설치 및 업그레이드 안내서*를 참조하십시오.

CA EEM 영역을 사용하여 CA APM 사용자를 인증하는 환경의 경우 CA EEM 서버에서 CA CEM 으로 CA CEM 사용자 자격 증명이 제공됩니다.

참고: CA EEM 서버가 SiteMinder 와 함께 작동하도록 구성된 경우 CA EEM 사용자를 인증하도록 SiteMinder 를 배포할 수 있습니다.

CA CEM 암호 관리

CA APM 사용자 암호는 EEM 및 로컬 영역 모두에서 암호화됩니다. 암호가 로컬 영역에서 암호화되는 방식에 대한 자세한 내용은 users.xml 에 CA APM 사용자 및 그룹 구성 (페이지 40)을 참조하십시오.

로컬 보안의 경우 CA CEM 에서는 *admin* 과 *cemadmin* 이라는 두 CA CEM 사용자를 기본 제공합니다. 둘은 모두 CA CEM 보안 사용자 그룹 중 "관리자" 및 "CEM 시스템 관리자"에 속합니다. *admin* 의 기본 암호는 *CA APM 설치 및 업그레이드 안내서*를 참조하십시오. 로컬 영역에서 CA CEM 사용자 암호를 업데이트하는 방식에 대한 자세한 내용은 users.xml 에 CA APM 사용자 및 그룹 구성 (페이지 40)을 참조하십시오.

CA EEM 의 CA APM 관리자는 CA CEM 사용자 암호를 업데이트할 수 있습니다. CA CEM 사용자는 CA EEM 자가 관리 기능을 사용하여 사용자 자신의 암호를 변경할 수 있습니다.

CA EEM 에서 CA CEM 사용자 암호를 다시 설정하려면

CA EEM 의 CA APM 관리자는 CA EEM 에서 CA CEM 사용자 암호를 업데이트할 수 있습니다.

1. CA EEM 에서 APM 응용 프로그램에 로그인합니다.
   a. CA EEM 로그인 페이지의 "Application:"(응용 프로그램:) 드롭다운 목록에서 APM 을 선택합니다.
   b. 로그인 이름과 암호를 입력합니다.

   APM 응용 프로그램의 기본 로그인은 *EiamAdmin* 입니다.
2. "Manage Identities"(ID 관리) 탭으로 이동합니다.
3. "Search Users"(사용자 검색) 상자에서 "Application Users Details"(응용 프로그램 사용자 정보)를 선택하고 "Go"(실행)를 클릭합니다.
4. "Users"(사용자) 상자 트리에서 APM 사용자 이름을 클릭합니다.

5. 사용자 정보가 나타나면 "Authentication"(인증) 상자에서 다음 중 하나를 수행합니다.
   - "Change Password at next log in"(다음 로그인 시 암호 변경) 확인란을 선택합니다.
   - "Reset Password"(암호 다시 설정) 확인란을 선택한 다음 새 암호를 입력하고 한 번 더 입력해 확인합니다. 사용자에게 새 암호를 알려줍니다.
6. "저장"을 클릭합니다.

   자세한 내용은 *CA Embedded Entitlements Manager Online Help*(CA Embedded Entitlements Manager 온라인 도움말)를 참조하십시오.

자가 관리 절차를 통해 CA EEM 암호를 다시 설정하려면

CA CEM 사용자는 다음과 같은 자가 관리 절차를 사용하여 CA EEM 에서 사용자 자신의 암호를 변경할 수 있습니다.

1. CA EEM 에서 APM 응용 프로그램에 로그인합니다.
   a. CA EEM 로그인 페이지의 "Application:"(응용 프로그램:) 드롭다운 목록에서 "Global"(글로벌)을 선택합니다.
   b. 로그인 이름과 암호를 입력합니다.
2. "Home"(홈) 탭으로 이동합니다.
3. "Self Administration"(자가 관리) 상자에서 "Change Password"(암호 변경) 링크를 클릭합니다.

   자세한 내용은 *CA Embedded Entitlements Manager Online Help*(CA Embedded Entitlements Manager 온라인 도움말)를 참조하십시오.

CA CEM 권한 부여 정보

CA CEM 사용자 권한 부여를 로컬로 수행하는 경우 특정 사용자에게 보기 권한을 부여할 대상 CEM 콘솔과 사용자가 작업할 수 있는 대상 데이터는 각 사용자가 속한 CA CEM 보안 사용자 그룹을 바탕으로 결정됩니다. 액세스 정책은 CA CEM 보안 사용자 그룹에 할당되고 이 보안 사용자 그룹을 바탕으로 액세스 정책이 적용됩니다.

로컬 영역을 사용하여 CA APM 사용자의 권한 부여를 수행하는 환경의 경우 *users.xml* 파일(Wily CEM 4.5 에서 업그레이드한 경우 *usersCEM45.xml* 일 수 있음)을 기반으로 표준 CA CEM 보안 사용자 그룹이 CA CEM 의 기본 보안 사용자 그룹에 연결된 메뉴 항목 및 권한 (페이지 135)에 설명된 대로 CEM 콘솔을 볼 수 있습니다. 자세한 내용은 로컬 사용자와 그룹, 그리고 CA CEM (페이지 148)을 참조하십시오.

CA EEM 에서 CA CEM 사용자의 권한 부여가 수행되는 경우 액세스 정책에 따라 특정 사용자에게 보기 권한을 부여할 대상 CEM 콘솔과 사용자가 작업할 수 있는 대상 데이터가 결정됩니다.

CA EEM 에서 CA APM 사용자의 권한 부여가 수행되는 환경의 경우 기본 APM 응용 프로그램을 배포하는 *eem.register.app.xml* Safex 스크립트를 실행(권장됨)하여 CA EEM 에 액세스 정책을 설정하거나 수동으로 설정합니다.

<EM_Home>/examples/authentication 디렉터리에 위치한 *eem.register.app.xml* Safex 스크립트를 실행하여 액세스 정책을 설정하는 경우 CA EEM 에서 표준 CA CEM 사용자 그룹은 CA CEM 의 기본 보안 사용자 그룹에 연결된 메뉴 항목 및 권한 (페이지 135)에 설명된 대로 CEM 콘솔을 볼 수 있습니다.

자세한 내용은 CA CEM 에 대한 CA EEM 인증 및 권한 부여 (페이지 137)와 CA EEM 액세스 정책 정보 (페이지 103)를 참조하십시오.

CA CEM 보안 사용자 그룹 정보

CA CEM 에서는 4 가지 기본 보안 사용자 그룹이 제공됩니다. 이전 버전의 CA CEM 에서 업그레이드하는 경우 CA CEM 역할에 익숙할 것입니다. 이 CA CEM 역할이 이제는 통합된 CA APM 보안 기능을 제공할 수 있도록 CA CEM 보안 사용자 그룹으로 변경되었습니다.

기본 CA CEM 보안 사용자 그룹은 다음과 같습니다.

- 관리자 - Introscope 및 CA CEM 액세스 권한을 모두 보유하며 Introscope 관리자 권한뿐 아니라 CEM 시스템 관리자 권한을 모두 부여받습니다.
- CEM 시스템 관리자 - 모든 CA CEM 시스템 기능을 관리합니다.
- CEM 구성 관리자 - 일반 CA CEM 구성 작업을 관리합니다.
- CEM 분석가 - CA CEM 보고서와 뷰에만 액세스할 수 있습니다.
- CEM 인시던트 분석가 - 결함이 발생한 HTTP 정보를 포함하여 CA CEM 보고서와 뷰에 액세스할 수 있습니다.

CA CEM 시스템 보안을 위해 관리자 그룹에 할당된 사용자 수를 가급적 최소한의 수로 제한하려 할 수 있습니다.

기본 CA CEM 보안 사용자 그룹의 구성원이 볼 수 있는 CA CEM 탭에 대한 자세한 내용은 CA CEM 의 기본 보안 사용자 그룹에 연결된 메뉴 항목 및 권한 (페이지 135)을 참조하십시오.

로컬 보안을 배포한 경우 CA CEM 에서는 다음과 같은 기본 그룹을 *users.xml* 파일에 제공합니다.

중요! 로컬 권한 부여를 배포한 경우 보안 사용자 그룹을 기본 CA CEM 보안 사용자 그룹에 추가할 수도, 이들 그룹과 연결된 액세스 정책을 변경할 수도 없습니다. 자세한 내용은 로컬 사용자와 그룹, 그리고 CA CEM (페이지 148)을 참조하십시오.

보안을 위해 CA EEM 을 배포한 경우 CA CEM 보안 사용자 그룹을 설정하고 CA EEM 서버에 액세스 정책을 설정합니다. 이 설정 작업은 Safex 스크립트를 실행하여 수행하거나 CA EEM 에서 수행할 수 있습니다. 자세한 내용은 CA EEM 에서 APM 그룹 만들기 및 삭제 (페이지 87)를 참조하십시오. 필요한 경우 CA CEM 보안 사용자 그룹을 추가, 수정 또는 삭제할 수 있습니다.

중요! 액세스 정책을 설정하여 CA CEM 사용자가 볼 수 있는 대상을 제한하려면 CA EEM 권한 부여를 배포해야 합니다.

추가 CA CEM 인증 및 권한 부여 솔루션

CA CEM 인증을 위해 LDAP 를 구성할 수 있습니다.

CA APM 인증에 대해 LDAP 를 구성하는 방법에 대한 자세한 내용은 LDAP 를 사용한 Introscope 보안 (페이지 51)을 참조하십시오.

중요! 인증에 LDAP 를 사용하는 경우 CA APM 사용자 그룹을 수동으로 구성해야 합니다. 반드시 LDAP 그룹 이름이 CA CEM 그룹 이름과 정확히 일치해야 합니다.

로컬 보안을 사용하여 CA CEM 의 권한 부여를 수행하도록 CA EEM 을 구성할 수도 있습니다. 이는 권한 부여에 로컬 영역을 사용하도록 CA EEM 을 구성하면 가능합니다. 자세한 내용은 로컬 권한 부여를 사용하도록 CA EEM 구성 (페이지 117)을 참조하십시오.

CA CEM 의 기본 보안 사용자 그룹에 연결된 메뉴 항목 및 권한

다음 표에서는 메뉴 항목과 관련 권한, 각 CA CEM 보안 사용자 그룹이 해당 권한을 보유하고 있는지 여부를 보여 줍니다.

메뉴: 기능	CEM 시스템 관리자	CEM 구성 관리자	CEM 분석가	CEM 인시던트 분석가
시스템: 전자 메일 설정 이벤트	예	아니요	아니요	아니요
보안: 개인 매개 변수 FIPS 설정 액세스 정책(CA EEM 만 해당)	예	아니요	아니요	아니요

메뉴: 기능	CEM 시스템 관리자	CEM 구성 관리자	CEM 분석가	CEM 인시던트 분석가
설정: Domain 모니터 서비스 웹 서버 필터 인시던트 설정 HTTPS 설정 플러그 인 Introscope 설정	예	예	아니요	아니요
관리: 개요 비즈니스 응용 프로그램 비즈니스 서비스 사양 사용자 그룹 상관 관계 SLA 기록 세션 트랜잭션 검색	예	예	아니요	아니요
도구: 스크립트 레코더	예	예	아니요	아니요
CEM: 서비스 수준 관리 인시던트 관리 » 아래 "참고" 참조 성능 보고서 품질 보고서 분석 그래프 내 보고서	예(모든 페이지)	예(단, "CEM" > "인시던트 관리" > "결함 정보" 페이지에서 HTTP 정보 섹션을 볼 수 없음)	예(단, "CEM" > "인시던트 관리" > "결함 정보" 페이지에서 HTTP 정보 섹션을 볼 수 없음)	예(모든 페이지)

참고: 요청 및 응답 본문과 쿼리 및 게시 매개 변수에 대한 추가 데이터가 "CEM" > "인시던트 관리" > "결함 정보" 페이지의 "HTTP 정보" 섹션 아래에 표시될 수 있습니다. 이 정보는 "포괄적 결함 정보 캡처" 확인란("설정" > "도메인" 페이지)이 선택된 경우 TIM 에 의해 수집됩니다.

결함에 대한 이 추가 데이터를 보려면 사용자는 반드시 비즈니스 서비스에 대한 *중요한 데이터 읽기* 액세스 권한을 부여하는 그룹의 구성원이어야 합니다. 예를 들어 CEM 인시던트 분석가 그룹은 이 액세스 권한을 갖습니다.

자세한 내용은 결함이 발생한 HTTP 요청 및 응답 보호 (페이지 152)를 참조하십시오.

CA CEM 에 대한 CA EEM 인증 및 권한 부여

CA EEM 에 익숙한 사용자는 "CA EEM 을 사용한 Introscope 보안"을 참조하십시오.

CA CEM 보안을 위해 CA EEM 을 배포하는 경우 인증 및 권한 부여가 CA EEM 서버에서 수행됩니다. CA EEM 권한 부여는 보안 사용자 그룹의 구성원 자격이 아닌 액세스 정책에 기반합니다. CA EEM 에서 액세스 정책은 세 가지 구성 요소로 구성됩니다. 바로 리소스 클래스, 리소스 및 권한(예: 읽기 또는 쓰기)입니다. 자세한 내용은 CA EEM 액세스 정책 정보 (페이지 103)를 참조하십시오.

참고: CA EEM 에서는 권한을 작업이라고 합니다.

다음 항목에서는 CA CEM 관련 기본 리소스 클래스, 리소스 및 액세스 정책에 대해 설명합니다. CA APM 에서 제공하는 CA EEM Safex 스크립트를 실행하면 기본 CA APM 응용 프로그램이 등록되고 CA CEM 글로벌 사용자와 응용 프로그램 관련 사용자, 보안 사용자 그룹, 리소스 클래스 및 리소스 클래스의 액세스 정책이 생성됩니다.

- CA EEM 에서 CA CEM 사용자 및 그룹 관리 (페이지 138)
- CA EEM 의 CA CEM 리소스 클래스 정보 (페이지 139)
- Introscope 관련 리소스 클래스 정보 (페이지 141)
- CA EEM 의 CA CEM 리소스 정보 (페이지 141)
- 기본 CA EEM CEM 액세스 정책 (페이지 142)
- CA CEM 기본 비즈니스 서비스 액세스 정책 정보 (페이지 145)

CA EEM 에서 CA CEM 사용자 및 그룹 관리

CA CEM 보안은 CA EEM 액세스 정책에 기반하며, 특정 사용자 및 응용 프로그램 관련 사용자 그룹에 적용됩니다.

CA Technologies 에서는 APM 응용 프로그램을 설정할 때 표준 CA CEM 사용자 및 그룹을 제공하는 *eem.register.app.xml* 및 *eem.add.global.identities.xml* Safex 스크립트를 실행할 것을 권장합니다. 이러한 Safex 스크립트를 실행하면 글로벌 사용자뿐 아니라 글로벌 사용자 그룹 및 APM 응용 프로그램 관련 사용자 그룹도 생성됩니다.

CA EEM 에서 CA CEM 사용자는 4 가지 기본 CA CEM 보안 사용자 그룹인 CEM 시스템 관리자, CEM 구성 관리자, CEM 분석가 및 CEM 인시던트 분석가 중 하나의 구성원일 수 있지만 반드시 그러할 필요는 없습니다. CA CEM 사용자는 사용자 정의된 새 그룹(예: HR 관리자 그룹)에 속할 수 있습니다. 기본 CA CEM 보안 사용자 그룹에 대한 자세한 내용은 CA CEM 의 기본 보안 사용자 그룹에 연결된 메뉴 항목 및 권한 (페이지 135)을 참조하십시오.

CA CEM 사용자 및 그룹을 만들고, 추가하고, 수정 및 삭제할 수 있습니다. 또한 CA CEM 사용자를 사용하거나 사용하지 않도록 설정할 수도 있습니다.

중요! CA APM 사용자가 CEM 콘솔을 사용하는 경우와 Introscope Investigator 데이터를 보려는 경우 APM 및 CA CEM 보안 사용자 그룹에 각각 속해 있어야 합니다. 예를 들어 APM 게스트 그룹과 CEM 분석가 그룹의 구성원일 수 있습니다. 자세한 내용은 CA EEM Introscope 사용자에게 CEM 콘솔에 대한 액세스 권한 부여 (페이지 147) 또는 로컬 Introscope 사용자에게 CEM 콘솔에 대한 액세스 권한 부여 (페이지 149)를 참조하십시오.

CA CEM 사용자를 추가, 수정 또는 삭제하려면

- CA EEM 에서 APM 사용자 만들기 및 삭제 (페이지 91)에 설명된 방법 중 하나를 사용하여 CA CEM 사용자를 추가, 수정 및 삭제합니다.

CA CEM 보안 사용자 그룹을 추가, 수정 및 삭제하려면

- CA EEM 에서 APM 그룹 만들기 및 삭제 (페이지 87)에 설명된 대로 CA CEM 보안 사용자 그룹을 추가, 수정 및 삭제합니다.

CA CEM 사용자를 사용하거나 사용하지 않도록 설정하려면

1. CA EEM 에서 APM 응용 프로그램에 로그인합니다.
   a. CA EEM 로그인 페이지의 "Application:"(응용 프로그램:) 드롭다운 목록에서 APM 을 선택합니다.
   b. 로그인 이름과 암호를 입력합니다.

   CA APM 응용 프로그램의 기본 로그인은 *EiamAdmin* 입니다.
2. "Manage Identities"(ID 관리) 탭으로 이동합니다.
3. "Search Users"(사용자 검색) 상자에서 "Application Users Details"(응용 프로그램 사용자 정보)를 선택하고 "Go"(실행)를 클릭합니다.
4. "Users"(사용자) 상자 트리에서 APM 사용자 이름을 클릭합니다.
5. 사용자 정보가 나타나면 "Authentication"(인증) 상자에서 다음 중 하나를 수행합니다.
   - "Enable Date"(활성화 날짜) 오른쪽의 달력을 클릭합니다.
   - "Disable Date"(비활성화 날짜) 오른쪽의 달력을 클릭합니다.
6. 활성화 또는 비활성화 작업을 시작할 날짜와 시간을 선택하고 "OK"(확인)를 클릭합니다.
7. "저장"을 클릭합니다.

   자세한 내용은 *CA Embedded Entitlements Manager Online Help*(CA Embedded Entitlements Manager 온라인 도움말)를 참조하십시오.

CA EEM 의 CA CEM 리소스 클래스 정보

CA CEM 권한 부여를 위해 CA EEM 을 사용하는 경우 액세스 정책을 설정하여 CA CEM 보안 사용자 그룹이 볼 수 있는 CEM 콘솔 탭을 결정합니다. 리소스 클래스는 액세스 정책의 필수 구성 요소입니다. 각 리소스 클래스는 CA EEM 에서 '작업'이라 하는 권한과 연결되어 있습니다.

다음 표에서는 기본 CA CEM 리소스 클래스와 연결된 작업을 보여 줍니다.

CA CEM 리소스 클래스	기본 작업
비즈니스 응용 프로그램	쓰기
비즈니스 서비스	쓰기 읽기 중요한 데이터 읽기

CA CEM 리소스 클래스	기본 작업
인시던트	쓰기
보고서	쓰기
Server	쓰기
시스템 관리 설정	쓰기
시스템 보안 설정	쓰기
사용자 그룹	쓰기
WebService	허용
액세스 정책	쓰기

리소스 클래스가 쓰기 작업에 연결되어 있는 경우 해당 리소스 클래스에 대한 액세스 권한을 부여받은 CA CEM 사용자 또는 그룹은 CEM 콘솔 메뉴에서 관련 탭을 볼 수 있습니다. 예를 들어 비즈니스 응용 프로그램 리소스 클래스는 CEM 콘솔의 "관리" > "비즈니스 응용 프로그램"을 CA CEM 사용자가 볼 수 있도록 허용합니다.

비즈니스 서비스 리소스 클래스에는 연결된 추가 작업이 두 가지(*읽기* 및 *중요한 데이터 읽기*)가 있습니다. CA CEM 사용자에게 비즈니스 서비스에 대한 *중요한 데이터 읽기* 권한이 있으면 CA CEM 사용자는 해당 비즈니스 서비스에 대한 결함과 연결된 HTTP 헤더 정보를 볼 수 있습니다. 자세한 내용은 *CA APM 구성 및 관리 안내서*를 참조하십시오.

비즈니스 서비스 리소스 클래스는 또한 CA CEM 사용자에게 TIM 및 에이전트 기록("관리" > "기록 세션")에 대한 액세스 권한을 부여할지 여부를 결정합니다. 하나 이상의 비즈니스 서비스에 대한 쓰기 권한이 있는 사용자는 "기록 세션" 탭에 액세스할 수 있습니다.

Introscope 관련 리소스 클래스 정보

기본 CA APM 응용 프로그램은 Introscope 관련 리소스 클래스 두 가지와 함께 다음 CA CEM 리소스 클래스를 제공합니다.

- 도메인 - Introscope 사용자에게 Introscope 관련 도메인을 볼 수 있는 권한(예: SuperDomain)을 부여합니다.

  참고: 이는 "CEM" > "설정" > "도메인" 기능과 관련이 없습니다.

- 서버 - Introscope 사용자에게 Enterprise Manager 를 시작하고 종료할 수 있는 권한을 부여합니다.

이들 리소스 클래스는 편집 또는 삭제하지 마십시오.

CA EEM 의 CA CEM 리소스 정보

기본 CA APM 응용 프로그램에는 CA CEM 리소스가 전혀 필요하지 않습니다. CA EEM 에서 리소스 클래스에는 연결된 리소스가 0 개 이상 있을 수 있습니다.

하지만 CA CEM 에는 비즈니스 서비스 리소스 클래스에 대한 리소스를 만드는 기능이 제공됩니다. 만든 비즈니스 서비스 리소스는 사용자 조직에만 한정되어 적용됩니다. 비즈니스 서비스 리소스를 만들면 하나 이상의 액세스 정책을 각 비즈니스 서비스에 연결할 수 있습니다. 또한 CA EEM 에서 CA CEM 리소스를 편집할 수도 있습니다.

CEM 콘솔이나 CA EEM 에서 비즈니스 서비스를 설정할 수 있습니다. 비즈니스 서비스의 기본 액세스 정책에 대한 자세한 내용은 기본 CA EEM CEM 액세스 정책 (페이지 142)을 참조하십시오. 새 비즈니스 서비스를 만드는 방법에 대한 자세한 내용은 *CA APM 트랜잭션 정의 안내서*를 참조하십시오.

또한 고유 액세스 정책을 보유한 CA CEM 리소스를 CA EEM 에서 만들어야 할 수도 있습니다. 예를 들어 특정 비즈니스 서비스 리소스에 대한 권한을 특정 CA CEM 사용자 및 보안 사용자 그룹으로 제한하려는 경우가 있습니다.

중요! CA EEM 에서 새 CA CEM 리소스를 만드는 경우 CA EEM 에 정의된 기존 CA CEM 리소스 클래스 및 액세스 정책을 사용해야 합니다.

새 리소스를 정의하려면 기본 CA EEM CEM 액세스 정책 (페이지 142)에 설명된 대로 새 액세스 정책을 정의합니다.

기본 CA EEM CEM 액세스 정책

CA EEM 에서 액세스 정책은 응용 프로그램 관련 리소스 클래스 및 리소스에 대한 액세스 규칙을 정의합니다.

경고: Introscope 관리자인 경우를 제외하고 CA EEM 에서 볼 수 있는 도메인 및 서버 액세스 정책을 변경하거나 삭제하지 마십시오. 이들은 Introscope 에서만 사용 가능합니다.

CA EEM 에서 액세스 정책은 리소스 클래스, 리소스 및 작업이라는 세 가지 구성 요소로 이루어져 있습니다.

기본 CA CEM 액세스 정책은 표준 CA CEM 보안 사용자 그룹에게 CEM 콘솔 메뉴 및 권한을 제공합니다. 자세한 내용은 CA CEM 의 기본 보안 사용자 그룹에 연결된 메뉴 항목 및 권한 (페이지 135)을 참조하십시오.

CA Technologies 에서는 *<EM_Home>/examples/authentication* 디렉터리에 위치한 *eem.register.app.xml* Safex 스크립트 파일을 실행할 것을 권장합니다. Safex 스크립트를 실행하여 APM 응용 프로그램을 설정하는 경우 CA Technologies 에서 제공하는 다음과 같은 APM 응용 프로그램 관련 CA CEM 기본 액세스 정책을 사용할 수 있습니다.

CA CEM 액세스 정책	설명	리소스 클래스/작업	권한을 부여받는 보안 사용자 그룹
WebService 허용	CEM 시스템 관리자 그룹은 웹 서비스 관련 정보를 볼 수 있도록 허용됩니다.	WebService/허용	CEM 시스템 관리자
사용자 그룹 - 쓰기	CEM 시스템 관리자 그룹 및 CEM 시스템 구성 관리자 그룹은 "관리"> "사용자 그룹" 탭에서 수행할 수 있는 모든 작업에 대한 쓰기 권한을 갖습니다.	사용자 그룹/쓰기	CEM 시스템 관리자 CEM 구성 관리자
시스템 보안 설정	CEM 시스템 관리자 그룹은 "시스템 보안 설정" 아래의 모든 리소스에 대한 쓰기 권한을 갖습니다.	보안 시스템 설정/쓰기	CEM 시스템 관리자

CA CEM 액세스 정책	설명	리소스 클래스/작업	권한을 부여받는 보안 사용자 그룹
시스템 구성 설정 - 쓰기	CEM 시스템 관리자 그룹 및 CEM 구성 관리자 그룹은 "시스템 구성 설정" 아래의 모든 리소스에 대한 쓰기 권한을 갖습니다.	시스템 구성 설정/쓰기	CEM 시스템 관리자 CEM 구성 관리자
시스템 구성 설정 포괄적 결함 정보 캡처	CEM 시스템 관리자 그룹은 "포괄적 결함 정보 캡처" 확인란에 대한 쓰기 권한을 갖습니다.	시스템 구성 설정/포괄적 결함 정보 캡처	CEM 시스템 관리자
시스템 관리 설정 - 쓰기	CEM 시스템 관리자 그룹은 "시스템 관리 설정" 아래의 모든 리소스에 대한 쓰기 권한을 갖습니다.	시스템 관리 설정/쓰기	CEM 시스템 관리자
보고서 - 쓰기	모든 CEM 그룹은 모든 보고서에 대한 쓰기 권한을 갖습니다.	보고서/쓰기	CEM 시스템 관리자 CEM 구성 관리자 CEM 분석가 CEM 인시던트 분석가
인시던트 - 쓰기	모든 CEM 그룹은 모든 인시던트에 대한 쓰기 권한을 갖습니다.	인시던트/쓰기	CEM 시스템 관리자 CEM 구성 관리자 CEM 분석가 CEM 인시던트 분석가

CA CEM 액세스 정책	설명	리소스 클래스/작업	권한을 부여받는 보안 사용자 그룹
비즈니스 서비스 - 중요한 데이터 읽기	CEM 인시던트 분석가 그룹은 모든 비즈니스 서비스에 대해 중요한 데이터 읽기 권한을 갖습니다.	비즈니스 서비스/중요한 데이터 읽기	CEM 인시던트 분석가
비즈니스 서비스 - 읽기	CEM 분석가 및 인시던트 분석가 그룹은 모든 비즈니스 서비스에 대한 읽기 권한을 갖습니다.	비즈니스 서비스/읽기	CEM 분석가 CEM 인시던트 분석가
비즈니스 서비스 - 읽기/쓰기	CEM 구성 관리자 그룹은 모든 비즈니스 서비스에 대해 읽기 및 쓰기 권한을 갖습니다.	비즈니스 서비스/쓰기 비즈니스 서비스/읽기	CEM 구성 관리자
비즈니스 서비스 - 모든 권한	CEM 시스템 관리자 그룹은 모든 비즈니스 서비스 기능에 대한 모든 권한을 갖습니다.	비즈니스 서비스/쓰기 비즈니스 서비스/읽기 비즈니스 서비스/중요한 데이터 읽기	CEM 시스템 관리자
비즈니스 응용 프로그램 - 쓰기	CEM 시스템 관리자 및 CEM 구성 관리자 그룹은 모든 비즈니스 응용 프로그램에 대한 쓰기 권한을 갖습니다.	비즈니스 응용 프로그램/쓰기	CEM 시스템 관리자 CEM 구성 관리자

CA CEM 액세스 정책	설명	리소스 클래스/작업	권한을 부여받는 보안 사용자 그룹
액세스 정책 - 모든 권한	CEM 시스템 관리자 및 CEM 구성 관리자 그룹은 모든 액세스 정책에 대한 모든 권한을 갖습니다.	액세스 정책/쓰기 액세스 정책/읽기	CEM 시스템 관리자 CEM 구성 관리자

CA CEM 기본 비즈니스 서비스 액세스 정책 정보

CA CEM 권한 부여를 위해 CA EEM 을 배포한 경우 CA EEM 에서 액세스 정책을 만들고 수정할 수 있을 뿐 아니라, CEM 콘솔의 "액세스 정책" 탭을 사용하여 비즈니스 서비스에 연결된 CA CEM 액세스 정책을 추가, 수정 또는 삭제할 수 있습니다.

CA CEM 의 "액세스 정책" 탭을 사용하여 CA CEM 액세스 정책을 추가하거나 변경한 경우

- *액세스 정책* 리소스 클래스에 대한 쓰기 권한이 필요합니다.
- CEM 콘솔을 사용하여 액세스 정책을 관리할 때 개별 APM 사용자가 아닌 APM 응용 프로그램 사용자 그룹에 대해서만 권한을 부여하고 해지할 수 있습니다. 자세한 내용은 *CA APM 구성 및 관리 안내서*를 참조하십시오.
- CA EEM 에서 CA CEM 액세스 정책 업데이트 (페이지 146)의 설명에 따라 액세스 정책을 직접 수정할 수도 있습니다.
- CA CEM 의 액세스 정책 변경 사항은 저장을 위해 CA EEM 에 곧바로 전송됩니다.

기본 비즈니스 서비스 액세스 정책을 만들거나 편집하는 경우 또는 해당 액세스 정책을 새 비즈니스 서비스에 연결하는 경우 *CA APM 트랜잭션 정의 안내서*를 참조하십시오.

CA EEM 에서 CA CEM 액세스 정책 업데이트

CA EEM 에서 기본 CA CEM 액세스 정책을 변경하여 다음을 수행할 수 있습니다.

- CA CEM 사용자 또는 보안 사용자 그룹이 CA CEM 탭을 볼 수 있도록 허용
- CA CEM 사용자 또는 보안 사용자 그룹이 탭을 보지 못하도록 제한

다음 단계를 따르십시오.

1. CA EEM 에서 APM 응용 프로그램에 로그인합니다.
   a. CA EEM 로그인 페이지의 "Application:"(응용 프로그램:) 드롭다운 목록에서 APM 을 선택합니다.
   b. 로그인 이름과 암호를 입력합니다.

   CA APM 응용 프로그램의 기본 로그인은 *EiamAdmin* 입니다.
2. "Manage Access Policies"(액세스 정책 관리) > "Access Policies"(액세스 정책)으로 이동합니다.
3. "Access Policies"(액세스 정책) 트리에서 액세스 정책을 클릭합니다. 예를 들어 "Report"(보고서) 액세스 정책을 클릭합니다.
4. "Policy Table"(정책 표) 섹션에서 액세스 정책 이름 링크를 클릭합니다. 예를 들어 "Report write"(보고서 - 쓰기)를 클릭합니다.
5. "Identities"(ID) 섹션에서 정책과 연결된 CA CEM 사용자 또는 보안 사용자 그룹을 추가하거나 업데이트합니다.

   예를 들어 보고서 - 쓰기 액세스 정책과 CEM 인시던트 분석가 그룹을 더 이상 연결하지 않으려면 "[Group] CEM Analyst"([그룹] CEM 분석가)를 선택한 상태에서 "Selected Identities"(선택한 ID) 상자의 오른쪽에 있는 휴지통 아이콘을 클릭합니다.
6. "저장"을 클릭합니다.

CA EEM 에서 새 CA CEM 액세스 정책 추가

CA EEM 에서 새 CA CEM 액세스 정책을 추가할 수 있습니다. 이 작업을 수행하려면 기본 APM 리소스 클래스와 권한 집합을 사용해야 합니다.

다음 단계를 따르십시오.

- Safex 스크립트를 실행하여 기존 리소스 클래스와 연결된 새 정책을 추가합니다. 자세한 내용은 CA EEM APM 프런트엔드 및 비즈니스 서비스 리소스 액세스 정책 만들기 및 삭제 (페이지 111)를 참조하십시오.

CA EEM Introscope 사용자에게 CEM 콘솔에 대한 액세스 권한 부여

Introscope 사용자가 CEM 콘솔을 보려는 경우 권한 부여가 성공적으로 수행될 수 있도록 Introscope 사용자는 반드시 하나 이상의 CA CEM 리소스 클래스에 대해 액세스 정책을 정의해야 합니다. Introscope 사용자에게 CEM 콘솔에 대한 액세스 권한을 부여하려면 해당 사용자에 대해 하나 이상의 CA CEM 리소스 클래스 관련 액세스 정책을 정의합니다.

다음 단계를 따르십시오.

1. CA EEM 에서 APM 응용 프로그램에 로그인합니다.
   a. CA EEM 로그인 페이지의 "Application:"(응용 프로그램:) 드롭다운 목록에서 APM 을 선택합니다.
   b. 로그인 이름과 암호를 입력합니다.

   CA APM 응용 프로그램의 기본 로그인은 *EiamAdmin* 입니다.
2. "Manage Access Policies"(액세스 정책 관리) > "Access Policies"(액세스 정책)으로 이동합니다.
3. "Access Policies"(액세스 정책) 트리에서 액세스 정책을 클릭합니다. 예를 들어 "System Administrative Settings"(시스템 관리 설정)을 클릭합니다.
4. "Policy Table"(정책 표) 섹션에서 액세스 정책 이름 링크를 클릭합니다. 예를 들어 "System Administrative Settings write"(시스템 관리 설정 - 쓰기)를 클릭합니다.
5. "Identities"(ID) 섹션에서 Introscope 사용자를 액세스 정책에 추가합니다.
6. "저장"을 클릭합니다.

CA CEM 의 로컬 인증 및 권한 부여

CA CEM 에 대해 로컬 보안을 배포한 경우 CA APM 에서는 인증 및 권한 부여를 위해 users.xml *파일이* 사용됩니다. 로컬 보안에 대한 배경 지식이 필요하면 로컬 보안을 사용한 Introscope 보안 (페이지 36)을 참조하십시오.

참고: Wily CEM 4.5 에서 업그레이드하여 로컬 보안을 사용하는 경우 Wily CEM 4.5 사용자는 *usersCEM45.xml* 파일에 존재할 수 있습니다. 자세한 내용은 *CA APM 설치 및 업그레이드 안내서*를 참조하십시오.

로컬 사용자와 그룹, 그리고 CA CEM

로컬 보안을 배포한 경우 *users.xml* 파일에 기본 보안 사용자 그룹이 제공됩니다(Wily CEM 4.5 에서 업그레이드한 경우 *usersCEM45.xml* 일 수 있음).

로컬 CA CEM 사용자, 즉 *users.xml* 파일에 정의된 사용자(Wily CEM 4.5 에서 업그레이드한 경우 *usersCEM45.xml* 일 수 있음)가 CEM 콘솔에 액세스하려는 경우 해당 사용자는 4 가지 표준 CA CEM 보안 사용자 그룹 중 하나의 구성원이어야 합니다.

경고: 로컬 권한 부여를 배포한 경우 보안 사용자 그룹을 기본 CA CEM 그룹에 추가할 수도, 이들 그룹과 연결된 액세스 정책을 변경할 수도 없습니다. CA CEM 로컬 보안의 기반은 이들 그룹이므로 이들 그룹을 수정하는 경우 CA CEM 보안 배포에 문제가 발생할 수 있습니다.

users.xml(Wily CEM 4.5 에서 업그레이드한 경우 *usersCEM45.xml* 일 수 있음)의 CA CEM 사용자에게 권한이 부여되는 환경의 경우 CA CEM 액세스 정책은 고정되어 변경될 수 없습니다. 이는 다음을 의미합니다.

- 표준 CA CEM 보안 사용자 그룹의 이름을 변경할 수도, 새로 추가할 수도 없습니다.
- CA CEM 보안 사용자 그룹에 사용자를 추가할 수 없습니다.
- 각 사용자는 표준 CA CEM 보안 사용자 그룹(CEM 시스템 관리자, CEM 구성 관리자, CEM 분석가 또는 CEM 인시던트 분석가) 중 하나의 구성원이어야 합니다. 사용자가 속한 그룹을 기준으로 해당 사용자의 액세스 정책이 유추됩니다. 표준 CA CEM 보안 사용자 그룹이 CEM 콘솔에서 볼 수 있는 정보에 대한 자세한 내용은 CA CEM 의 기본 보안 사용자 그룹에 연결된 메뉴 항목 및 권한 (페이지 135)을 참조하십시오.

CA CEM 사용자를 추가, 수정 및 삭제할 수 있습니다.

다음 단계를 따르십시오.

- *users.xml* 의 CA CEM 사용자를 추가, 수정 및 삭제합니다. 자세한 내용은 users.xml 에 CA APM 사용자 및 그룹 구성 (페이지 40)을 참조하십시오.

로컬 Introscope 사용자에게 CEM 콘솔에 대한 액세스 권한 부여

로컬 Introscope 사용자가 CEM 콘솔을 보려는 경우 Introscope 사용자는 APM 및 CA CEM 보안 사용자 그룹에 각각 포함되어 있어야 합니다. 예를 들어 APM 게스트 그룹과 CA CEM 분석가 그룹의 구성원일 수 있습니다.

다음 단계를 따르십시오.

- Introscope 사용자를 *users.xml* 의 CA CEM 사용자 그룹에 추가합니다. 자세한 내용은 users.xml 에 CA APM 사용자 및 그룹 구성 (페이지 40)을 참조하십시오.

예를 들어 Introscope 인증과 권한 부여를 위해 *users.xml* 에 나열된 사용자인 Tandav Gupta 를 CEM 시스템 관리자 그룹에 추가할 수 있습니다.

추가 CA CEM 보안 작업

CA EEM CEM 및 로컬 보안 인증 및 권한 부여 설정 작업과 더불어 CA CEM 보안 링크에 대해 학습하고 다음과 같은 추가적인 CA CEM 보안 작업을 수행할 수 있습니다.

- CA CEM 의 보안 링크 (페이지 150)
- 새 비즈니스 서비스에 대한 기본 액세스 정책을 설정하는 방법은 *CA APM 구성 및 관리 안내서*를 참조하십시오.
- 개인 매개 변수 정의 (페이지 150)
- 결함이 발생한 HTTP 요청 및 응답 보호 (페이지 152)
- FIPS 140-2 호환 암호화 (페이지 160)

- HTTPS 를 통한 TIM 통신 구성 (페이지 163)
- HTTPS 로만 Enterprise Manager 액세스 제한 (페이지 164)
- CA CEM 보고서에서 비즈니스 서비스 데이터를 볼 수 있는 사용자를 제한하려면 CA EEM 사용하여 EEM 을 CA APM 의 유일한 보안 영역으로 구성해야 합니다. CA CEM 으로 보고 기능을 사용하는 방법에 대한 자세한 내용은 보안 영역 정보 (페이지 15)와 함께 *CA APM 구성 및 관리 안내서*를 참조하십시오.

CA CEM 보안 링크

"보안" 링크에서 볼 수 있는 탭은 Introscope 또는 CA APM 중 어느 것을 설치했는지와 CA EEM 을 사용하는지 여부에 따라 달라집니다.

예를 들어 보안 솔루션에 상관없이 개인 매개 변수를 항상 숨길 수 있습니다. 하지만 인증 및 권한 부여를 위해 CA EEM 을 사용하는 경우 비즈니스 서비스에 대한 액세스만 제한할 수 있습니다. 다음 표에서는 구현한 보안 솔루션에 따라 CEM 콘솔에 표시되는 정보가 무엇인지 보여 줍니다.

CA CEM 탭 표시 여부	Introscope 만 구현 및 CA EEM	Introscope 만 구현(CA EEM 제외)	CA APM(CA EEM 포함)	CA APM(CA EEM 제외)
개인 매개 변수	예	예	예	예
액세스 정책	예	아니요	예	아니요
FIPS 설정	아니요	아니요	예	예

개인 매개 변수 정의

HTTP 매개 변수는 HTTP 에 사용되는 이름/값 쌍입니다. HTTP 매개 변수의 공통 유형은 쿠키, 쿼리 및 게시 매개 변수입니다. CA CEM 의 HTTP 매개 변수에 대한 자세한 내용은 *CA APM 트랜잭션 정의 안내서*를 참조하십시오.

CA CEM 에서 HTTP 매개 변수는 트랜잭션 기록 및 인식 프로세스의 일부로 기록됩니다. 일반적으로 기록된 모든 트랜잭션에 대해 모든 HTTP 매개 변수가 나타납니다.

CA CEM 개인 매개 변수를 사용하면 비공개 상태를 유지해야 할 HTTP 헤더 정보를 지정할 수 있습니다. CA CEM 개인 매개 변수 값은 모든 CA CEM 사용자뿐 아니라 시스템 관리자 또는 구성 관리자에게도 표시되지 않습니다. 최종 사용자만 매개 변수 값을 알고 있습니다.

팁: 일부 개인 매개 변수 이름은 바로 알기 쉽지 않습니다. 예를 들어 암호 및 핀이 각각 field1 및 field2 일 수 있습니다. 라이브 트랜잭션을 보기 전에 모든 개인 매개 변수의 보안이 유지되는지 확인하기 위해 테스트 트랜잭션에서 HTTP 매개 변수를 검토하는 것이 좋습니다.

매개 변수를 '개인'으로 지정하는 경우 실제 값은 TIM 로그와 CEM 콘솔(값이 나타나야 하는 부분)에서 별표로 나타납니다.

"*" 와일드카드 문자를 사용하여 일치시킬 패턴을 일반화할 수 있습니다. 다음과 같은 와일드카드 문자열이 허용됩니다.

- abc* - 시작 일치
- *xyz - 끝 일치
- abc*xyz - 시작 및 끝 일치
- * - 하나의 별표만 사용하여 매개 변수 이름 패턴을 만드는 경우 *모든* 매개 변수는 '개인'이 됩니다.

예를 들어 "pin" 앞에 별표를 추가하여 "pin"을 일반화하면 "userpin" 또는 "login_pin"과 같은 다른 항목도 개인 매개 변수로 인식되도록 만들 수 있습니다.

참고: 개인 매개 변수당 단 하나의 "*" 와일드카드 문자만 허용됩니다. 정규식(regex)은 사용할 수 없습니다.

기본 CA CEM 개인 매개 변수는 다음과 같습니다.

- *access_id
- pass
- *passcode
- pin
- *password
- pw
- *ssn

개인 매개 변수 수정

기존 CA CEM 개인 매개 변수를 업데이트하려면 다음 단계를 따르십시오.

다음 단계를 따르십시오.

1. "보안" > "개인 매개 변수"를 선택합니다.
2. 매개 변수 이름(예: *password)을 클릭합니다. 별표는 password 단어 앞에 어떤 문자든 수에 제한 없이 올 수 있음을 나타냅니다.
3. 암호 수집을 위해 다른 매개 변수를 입력합니다. 예를 들어 password 단어의 경우 항상 선행 문자 없이 HTTP 트래픽에 나타난다는 것을 알고 있는 경우 *password 매개 변수를 password 로 변경합니다.
4. "저장"을 클릭하여 새 개인 매개 변수를 저장합니다.

개인 매개 변수 추가

새 CA CEM 개인 매개 변수를 만들려면 다음 단계를 따르십시오.

다음 단계를 따르십시오.

1. "보안" > "개인 매개 변수"를 선택합니다.
2. "새로 만들기"를 클릭하여 새 개인 매개 변수를 만듭니다.
3. 필요한 개인 매개 변수를 입력합니다.
4. "저장"을 클릭하여 새 개인 매개 변수를 저장합니다.

결함이 발생한 HTTP 요청 및 응답 보호

결함이 발생한 경우 중요한 데이터 읽기 권한을 가진 CA CEM 사용자로 로그인하면 사용자들의 브라우저에서 전송된 정보와 생성된 메시지를 정확히 볼 수 있습니다. 또한 적절한 권한이 있는 경우 쿼리 및 게시 매개 변수와 HTTP 요청 및 응답 본문 정보를 볼 수 있습니다.

기본적으로, CEM 시스템 관리자 또는 CEM 인시던트 분석가 그룹에 속한 CA CEM 사용자에게는 중요한 데이터 읽기 권한이 있습니다.

결함 정보 보기

결함 정보 페이지에는 사용자, 트랜잭션 및 웹 서버에 대한 정보를 포함하여 결함에 대한 다양한 범주의 정보가 나타납니다. 다음 절차는 결함이 발생하여 캡처된 특정 HTTP 매개 변수 정보를 보는 방법을 설명합니다.

다음 단계를 따르십시오.

1. "인시던트 관리" > "결함"을 선택합니다.
2. 표시하려는 결함의 날짜와 시간을 클릭합니다.

   HTTP 정보 영역에 다음을 포함하여 해당 시간에 해당 사용자 환경에서 발생한 결함 정보가 표시됩니다.

   - 호스트, URL 경로, TCP 포트
   - 쿠키
   - HTTP 헤더(쿠키 제외)

   적절한 권한이 있는 경우 결함 정보 페이지에서 다음 HTTP 정보를 보거나 액세스할 수 있습니다.

   - 쿼리 및 게시 매개 변수
   - 응답 본문(처음 1,024 바이트만). 이 값을 변경하려면 캡처된 응답 본문의 최대 크기 변경 (페이지 159)을 참조하십시오.
   - 요청 본문(처음 1,024 바이트만). 자세한 내용은 요청 본문 정보 보기 (페이지 154)를 참조하십시오.

   이 HTTP 정보를 표시하도록 설정하는 방법에 대한 자세한 내용은 포괄적 결함 정보 캡처 (페이지 156)를 참조하십시오.

3. 결함이 발생했을 때 사용자에게 표시된 페이지와 똑같은 페이지를 보려면 RequestHeader Referer 콘텐츠를 잘라내어 브라우저에 붙여 넣습니다.

요청 본문 정보 보기

요청 본문 정보를 확인하면 결함을 파악하는 데 도움이 됩니다. POST 요청의 경우 요청 본문이 비어 있을 수는 있지만 요청 본문이 존재하는 반면, GET 요청에는 요청 본문이 없습니다.

요청 본문 정보를 볼 때 다음 두 가지 사항을 숙지해야 합니다.

- 올바른 형식의 XML/HTML 만 표시될 수 있습니다. 올바른 형식으로 구성되지 않은 XML/HTML 을 보려면 올바른 형식으로 구성되지 않은 XML/HTML 보기 (페이지 154)를 참조하십시오.
- 기본적으로 결함이 있는 요청 본문 정보의 처음 1,024 바이트만 표시됩니다. 하지만 이 값은 변경될 수 있습니다. 자세한 내용은 표시된 요청 본문 정보의 최대 크기 변경 (페이지 155)을 참조하십시오.

올바른 형식으로 구성되지 않은 XML/HTML 보기

결함과 연결된 XML/HTML 이 올바른 형식으로 구성되지 않은 경우 HTTP 요청 본문을 보려고 링크를 클릭하면 표시된 요청은 빈 상태로 나타나거나 불완전하게 보입니다.

올바른 형식으로 구성되지 않은 XML/HTML 을 표시하는 해결 방법이 있습니다.

참고: 올바른 형식으로 구성되었는지 여부와 상관없이 *모든* 요청 본문 정보를 보려면 "포괄적 결함 정보 캡처" 확인란을 선택하고 사용자에게 중요한 데이터 읽기 권한이 있어야 합니다. 자세한 내용은 포괄적 결함 정보 캡처 (페이지 156)를 참조하십시오.

다음 단계를 따르십시오.

1. "인시던트 관리" > "결함"을 선택합니다.
2. 표시하려는 결함의 날짜와 시간을 클릭합니다.
3. RequestBody 링크를 마우스 오른쪽 단추로 클릭하고 파일을 저장합니다.
4. 텍스트 편집기 또는 HTML 편집기를 사용하여 요청 본문의 전체 콘텐츠를 봅니다.

표시된 요청 본문 정보의 최대 크기 변경

기본적으로 결함이 있는 요청 본문 정보의 처음 1,024 바이트만 표시됩니다. 적절한 권한이 있는 경우 정보를 더 많이 또는 더 적게 표시하도록 이 값을 편집할 수 있습니다.

다음 단계를 따르십시오.

1. "TIM System Setup"(TIM 시스템 설정) 페이지에 액세스합니다.
   a. CEM 콘솔에서 "Setup"(설정) > "Monitors"(모니터)를 선택합니다.
   b. 맨 오른쪽 열에서 TIM 의 IP 주소를 클릭합니다.
   c. 사용자 이름과 암호를 입력합니다.

   "System Setup"(시스템 설정) 페이지의 기본 사용자 이름은 admin 입니다.

   TIM 의 "System Setup"(시스템 설정) 페이지가 나타납니다.
2. "Configure TIM Settings"(TIM 설정 구성)를 클릭합니다.

   "TIM Settings"(TIM 설정) 페이지가 표시됩니다.
3. "MaxDefectRequestBodySize"(확인)를 클릭합니다.
4. "New value"(새 값) 필드에서 표시할 최대 크기를 바이트 단위로 입력합니다.

   이는 필요한 값보다 더 큰 값으로 설정하지 마십시오. 큰 값을 사용하는 경우 TIM 및 Enterprise Manager 모두에서 처리 시간이 더 길어집니다.

5. "Change"(변경)를 클릭합니다.

   변경 사항은 즉시 반영되며 TIM 을 다시 시작할 필요가 없습니다.

6. TIM 이 여러 개일 경우 각 TIM 마다 위의 단계를 반복합니다.

표시할 결함 정보 제한

다음 두 방법 중 하나나 둘 모두를 사용하여 나타나는 결함 정보의 양을 제한할 수 있습니다.

- 쿼리 및 게시 매개 변수와 요청 및 응답 본문 정보를 수집하고 표시하도록 선택(포괄적 결함 정보 캡처 (페이지 156) 참조)
- 특정 개인 매개 변수를 숨기도록 설정

  매개 변수 이름이 개인 매개 변수 중 하나와 일치하는 경우 게시, 쿼리, 쿠키 및 URL 매개 변수는 숨겨집니다. 즉, 값이 "***"로 바뀝니다.

  개인 매개 변수를 사용하면 다음과 같은 항목을 숨길 수 있습니다.

  - 특정 매개 변수(정확한 매개 변수 이름을 제공해야 함)
  - 매개 변수 유형(매개 변수 이름 패턴에 와일드카드("*") 사용)
  - 모든 매개 변수(매개 변수 이름 패턴에 "*"를 사용하여 개인 매개 변수 만들기. 이는 *모든* 매개 변수가 개인 매개 변수라는 의미임)

  자세한 내용은 개인 매개 변수 정의 (페이지 150)를 참조하십시오.

포괄적 결함 정보 캡처

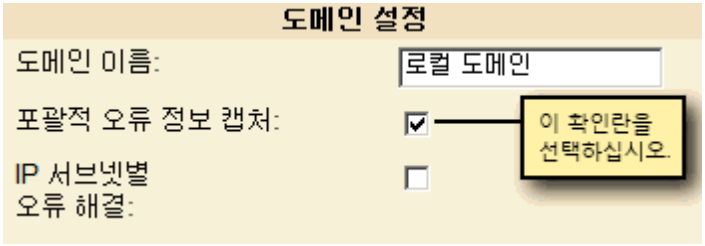
쿼리, 게시 매개 변수, 요청 및 응답 본문 정보를 볼 수 있는 기능은 기본적으로 사용하지 않도록 설정되어 있습니다. "포괄적 결함 정보 캡처" 확인란("설정" > "도메인" 페이지)을 선택하지 않으면 TIM 에서 쿼리 및 게시 정보, 요청 및 응답 본문 정보가 캡처되지 않습니다.

중요! 보안이 우려되는 경우 이 기본값을 변경하지 말고 CEM 시스템 관리자에게라도 "포괄적 결함 정보 캡처" 확인란을 사용할 수 없도록 설정하는 것이 좋습니다. 자세한 내용은 포괄적 결함 정보 캡처 확인란을 사용 또는 사용할 수 없도록 설정 (페이지 158)을 참조하십시오.

하지만 중요한 데이터 읽기 권한을 가진 사용자가 결함에 대한 이 추가 정보를 볼 수 있도록 하려면 "포괄적 결함 정보 캡처" 확인란을 선택해야 합니다.

쿼리 정보, 게시 정보, 요청 본문 및 응답 본문 정보를 볼 수 있도록 설정하려면

1. "설정" > "도메인"을 선택합니다.
2. "포괄적 결함 정보 캡처"를 선택합니다.



   페이지에 "포괄적 결함 정보 캡처" 확인란이 나타나지 않으면 "도메인" > "모니터" 페이지에 TIM 이 하나 이상 나열되었는지 확인하십시오. 이때 TIM 을 사용하도록 설정할 필요는 없습니다.

   "포괄적 결함 정보 캡처" 확인란을 사용할 수 없거나 허용되지 않은 경우 다음 방법 중 하나를 사용하여 이 확인란을 사용할 수 있도록 CA EEM 또는 로컬 권한을 업데이트해야 합니다.

   - CA EEM 에서 CA CEM 사용자 및 액세스 정책을 설정한 경우 포괄적 결함 정보 캡처 확인란을 사용 또는 사용할 수 없도록 설정 (페이지 158)을 참조하십시오.
   - 로컬 보안을 사용하는 경우 CEM 시스템 관리자 그룹의 구성원으로 로그인합니다.

3. "저장"을 클릭합니다.
4. 모니터를 동기화합니다.

   참고: 다른 CA CEM 구성 작업을 수행하고 있는 경우 동기화를 수행하기 전에 모든 구성 작업을 완료해야 모니터 동기화를 한 번에 마칠 수 있습니다.

   모니터를 동기화한 후 TIM 에서 결함에 대한 쿼리 정보, 게시 정보, 요청 및 응답 본문 정보가 수집되기 시작합니다. 그런 다음 중요한 데이터 읽기 권한을 가진 사용자는 모니터가 동기화된 이후 캡처된 이 결함 관련 데이터를 볼 수 있습니다.

   나중에 이 확인란의 선택을 취소하는 경우 확인란을 선택했을 때 수집된 결함 정보가 계속 표시될 수 있습니다.

포괄적 결함 정보 캡처 확인란을 사용 또는 사용할 수 없도록 설정

기본적으로, CEM 시스템 관리자 그룹에 속한 모든 사용자는 "포괄적 결함 정보 캡처" 확인란을 선택할 수 있습니다. 이는 기본적으로 CEM 시스템 관리자 그룹의 모든 구성원은 "시스템 구성 설정 포괄적 결함 정보 캡처" 본문 액세스 정책을 보유하고 있기 때문입니다.

"시스템 구성 설정 포괄적 결함 정보 캡처" 액세스 정책에 원하는 그룹을 추가하여 "포괄적 결함 정보 캡처" 확인란을 액세스할 수 있는 권한을 해당 그룹의 사용자에게 부여할 수 있습니다.

참고: "포괄적 결함 정보 캡처" 확인란을 "설정" > "도메인" 페이지에 표시하려면 "도메인" > "모니터" 페이지에 TIM 이 하나 이상 나열되어 있어야 합니다.

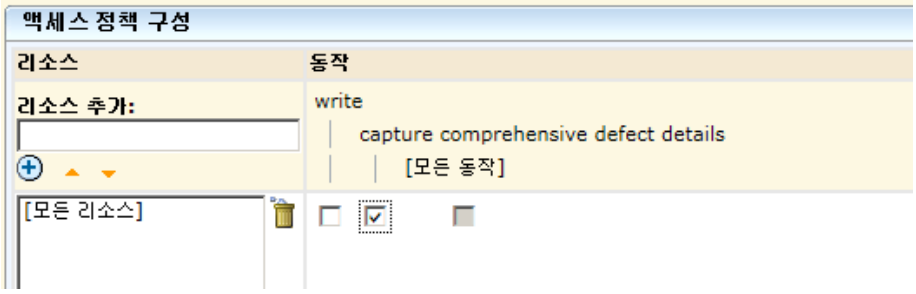
다음 단계를 따르십시오.

1. CA EEM 에서 CA CEM 액세스 정책 업데이트 (페이지 146)의 지침에 따라 "시스템 구성 설정 포괄적 결함 정보 캡처" 액세스 정책을 편집합니다.

   "Selected Identities"(선택한 ID)에 추가한 관리자 사용자나 그룹은 "포괄적 결함 정보 캡처" 확인란을 편집할 수 있습니다. 이 확인란을 선택하면 중요한 데이터 읽기 권한을 가진 모든 사용자가 중요한 HTTP 데이터(쿼리 정보, 게시 정보, 요청과 응답 본문 정보)를 추가적으로 볼 수 있습니다.

2. 사용자나 그룹에게 시스템 구성 설정 리소스 클래스에 대한 쓰기 권한이 있는지 확인합니다. 이 권한이 있어야 "도메인" 페이지를 편집할 수 있는 권한이 부여됩니다.

3. 정책을 저장하기 전에 "포괄적 결함 정보 캡처" 작업이 선택되어 있는지 확인합니다.



중요! "포괄적 결함 정보 캡처" 확인란을 선택하면 CA CEM 사용자가 중요할 수 있는 일부 데이터를 볼 수 있습니다. 이러한 데이터를 쉽게 볼 수 없도록 만들려면 모든 사용자, 심지어 기본적으로 액세스할 수 있는 CEM 시스템 관리자까지도 이 확인란을 사용할 수 없도록 설정하면 됩니다.

"포괄적 결함 정보 캡처" 확인란을 사용할 수 없도록 설정하려면

1. CEM 콘솔의 "설정" > "도메인" 페이지에서 "포괄적 결함 정보 캡처" 확인란이 선택되어 있지 않은 상태인지 확인합니다.
2. CA EEM 에서 CA CEM 액세스 정책 업데이트 (페이지 146)의 지침에 따라 "시스템 구성 설정 포괄적 결함 정보 캡처" 액세스 정책을 편집합니다.
3. "포괄적 결함 정보 캡처" 확인란의 선택을 취소하거나 "Selected Identities"(선택한 ID) 목록에서 모든 항목을 삭제한 후 포괄적 결함 정보 캡처 액세스 정책을 저장합니다.

   포괄적 결함 정보 캡처 작업이 선택된 정책이 없으면 모든 CA CEM 사용자가 TIM 을 통해 쿼리 정보, 게시 정보, 요청 및 응답 본문 정보를 캡처할 수 없습니다.

캡처된 응답 본문의 최대 크기 변경

기본적으로, 응답 본문의 처음 10 KB 가 캡처됩니다. 응답 본문을 더 많이 또는 더 적게 캡처하려면 다음 절차를 따르십시오.

다음 단계를 따르십시오.

1. "TIM System Setup"(TIM 시스템 설정) 페이지에 액세스합니다.
   a. CEM 콘솔에서 "Setup"(설정) > "Monitors"(모니터)를 선택합니다.
   b. 맨 오른쪽 열에서 TIM 의 IP 주소를 클릭합니다.
   c. 사용자 이름과 암호를 입력합니다.

"System Setup"(시스템 설정) 페이지의 기본 사용자 이름은 admin 입니다.

TIM 의 "System Setup"(시스템 설정) 페이지가 나타납니다.

2. "Configure TIM Settings"(TIM 설정 구성)를 클릭합니다.

   "TIM Settings"(TIM 설정) 페이지가 표시됩니다.

3. "MaxDefectResponseBodySize"(확인)를 클릭합니다.
4. "New value"(새 값) 필드에서 캡처할 최대 크기를 바이트 단위로 입력합니다.

   허용된 범위는 0 에서 200000(~200 KB) 사이입니다.

   이는 필요한 값보다 더 큰 값으로 설정하지 마십시오. 큰 값을 사용하는 경우 처리 시간이 더 길어지고 저장 공간도 더 많이 필요합니다.

5. "Change"(변경)를 클릭합니다.

   변경 사항은 즉시 반영되며 TIM 을 다시 시작할 필요가 없습니다.

6. TIM 이 여러 개일 경우 각 TIM 마다 위의 단계를 반복합니다.

FIPS 140-2 호환 암호화

FIPS 140-2 정보

FIPS(Federal Information Processing Standards) 140-2 사양은 소프트웨어 제품 및 프로토콜 암호화에 사용되는 암호화 라이브러리 및 알고리즘에 대한 보안 표준을 기술합니다.

암호화는 소프트웨어 보안의 다음과 같은 측면에 영향을 줍니다.

- 암호의 저장 및 확인
- 제품 구성 요소 사이 및 제품 사이에서 전달된 모든 민감한 데이터의 통신 및 저장

CA CEM 및 FIPS 140-2 정보

FIPS 140-2 사양에 맞게 보안을 강화하기 위해 CA CEM 에 일부 사항이 수정되었습니다.

- 전자 메일 서버의 암호는 FIPS 호환 128 비트 AES 및 SHA 알고리즘을 사용하여 암호화됩니다.
- CA Unicenter Service Desk 암호는 FIPS 호환 128 비트 AES 알고리즘을 사용하여 암호화됩니다.
- 결함 및 사용자 세션 ID 에 수록된 HTTP 정보를 일반 텍스트가 아닌 128 비트 암호화된 형식으로 APM 데이터베이스에 저장할 수 있습니다. 이 HTTP 정보는 잠재적으로 민감한 데이터일 수 있습니다.

  사용자 이름, 사용자 세션 ID, 암호, 신용 카드 번호 및 쿠키와 같은 기밀 데이터가 HTTP 정보에 포함될 수 있습니다. 사용자 세션 ID 가 악의적인 방식으로 사용되어 사용자 세션이 도용될 수 있습니다.

CA CEM 의 FIPS 104-2 암호화 기능

다음 표에서는 APM 데이터베이스에서 암호화되거나 암호화될 가능성이 있는 데이터 종류를 요약해서 보여 줍니다. 암호는 기본적으로 암호화됩니다.

이 알고리즘은 RSA Security Inc 의 TCrypto-J 3.5 라이브러리에서 제공된 FIPS 인증된 Pure Java 버전(jsafeFIPS)입니다.

암호화 대상...	UI 에서의 위치...	선택 사항 여부	암호화 유형	추가 정보
SMTP 암호	"시스템" > "전자 메일 설정"	아니요	FIPS 호환 AES	*CA APM 구성 및 관리 안내서*
요청 및 응답 본문을 포함하여 결함에 포함된 HTTP 정보	"CEM" > "인시던트 관리" > "결함"	예	FIPS 호환 AES	결함에 있는 HTTP 정보 암호화 (페이지 162)
사용자 세션 ID	사용자 세션 ID 는 포괄적 결함 정보와 함께 표시되는 경우 UI 에서 볼 수만 있습니다.	예	FIPS 호환 AES	사용자 세션 ID 암호화 (페이지 163)

결함에 있는 HTTP 정보 암호화

기본적으로 결함과 연결된 HTTP 정보는 APM 데이터베이스의 결함 메타 값 표에 일반 텍스트로 저장됩니다. 조직에서 필수적으로 FIPS 140-2 호환 소프트웨어를 사용하는 경우 다음 절차에 따라 APM 데이터베이스에 저장된 HTTP 정보를 암호화하십시오. 결함과 연결된 응답 및 요청 본문이 캡처되면 해당 본문이 암호화됩니다.

데이터가 APM 데이터베이스에서 암호화될지라도 "CEM" > "인시던트 관리" > "결함" 정보 페이지에 표시될 때는 암호가 해제됩니다.

		HTTP 정보
ResponseHeader	Date:	Mon, 16 Jun 2009 21:12:39 GMT
ResponseHeader	Pragma:	no-cache
ResponseHeader	Server:	WebLogic WebLogic Server 7.0 SP1 Mon Sep 9 2002 206753
ResponseHeader	Content-Language:	en
ResponseHeader	Content-Length:	11191
ResponseHeader	Content-Type:	text/html; charset=ISO-8859-1
ResponseHeader	Expires:	Thu, 01 Jan 1970 00:00:00 GMT
Cookie	JSESSIONID_SAMPLEPORTAL:	lWXHgGLGMR6o96l011iAzdp290Z35D0GMyxsSI 614758663

중요! 암호화를 선택 또는 선택 취소하는 경우 HTTP 요청 및 응답 본문을 포함하여 모든 HTTP 정보(APM 데이터베이스의 결함 메타 값 표에 저장됨)가 삭제됩니다. 이를 통해 일반 데이터 및 암호화된 데이터가 동일한 데이터베이스 테이블에 함께 배치되는 상황을 피할 수 있습니다.

이 표의 데이터는 중요하지 않으므로 기본적으로 매주 삭제됩니다.

다음 단계를 따르십시오.

1. "보안" > "FIPS 설정"을 선택합니다.
2. "HTTP 결함 정보"를 클릭합니다.

   암호화를 선택 또는 선택 취소하는 경우 APM 데이터베이스에 저장된 모든 HTTP 결함 정보가 삭제된다는 경고가 표시됩니다.
3. "저장"을 클릭합니다.

   이전에 저장된 HTTP 정보가 삭제되고 결함에 대한 이후 모든 HTTP 정보가 암호화됩니다.

사용자 세션 ID 암호화

기본적으로, 사용자 세션 ID 는 APM 데이터베이스에서 일반 텍스트로 저장됩니다. FIPS 140-2 호환성의 경우 사용자 세션 ID 를 암호화하도록 선택할 수 있습니다.

조직에서 필수적으로 FIPS 140-2 호환 소프트웨어를 사용하는 경우 다음 절차에 따라 APM 데이터베이스에 저장된 사용자 세션 ID 를 암호화하십시오.

중요! 암호화를 선택 또는 선택 취소하는 경우 APM 데이터베이스의 사용자 세션 테이블에 저장된 모든 사용자 세션 ID 는 삭제됩니다. 이를 통해 일반 데이터 및 암호화된 데이터가 동일한 데이터베이스 테이블에 함께 배치되는 상황을 피할 수 있습니다.

이렇게 삭제하는 경우 FIPS 설정에 변경이 발생하면 세션 중간에 있는 모든 사용자는 지정되지 않은 사용자 그룹에 할당됩니다. 이러한 이유로 인해 CA Technologies 에서는 시스템에 최소한의 사용자 트래픽이 있는 경우나, 업그레이드 직후 Enterprise Manager 를 다시 시작하는 경우 FIPS 설정을 변경할 것을 권장합니다.

다음 단계를 따르십시오.

1. "보안" > "FIPS 설정"을 선택합니다.
2. "사용자 세션 ID"를 클릭합니다.

   암호화를 선택하거나 선택 취소하면 모든 사용자 세션 ID 가 삭제된다는 경고를 받습니다.
3. "저장"을 클릭합니다.

   이전에 저장한 사용자 세션 ID 가 삭제되고 그 이후의 사용자 세션 ID 는 암호화됩니다.

HTTPS 를 통한 TIM 통신 구성

TIM 수집 서비스를 실행하는 TIM 및 Enterprise Manager 는 기본적으로 HTTP 를 통해 통신합니다. 하지만 보안을 더 강화하기 위해 HTTPS(SSL over HTTP)를 대신 사용하여 통신하도록 구성할 수 있습니다.

이는 TIM 수집 서비스를 실행하는 Enterprise Manager 에서 *timTessCommunication.useSsl* 속성을 *tess-customer.properties* 파일에 추가하여 구성하면 됩니다.

SSL 을 사용하면 Enterprise Manager 와 TIM 간의 통신 속도가 저하될 수 있으므로 구성을 적용하기 전에 신중히 고려해야 합니다. 예를 들어 Enterprise Manager 및 TIM 이 동일한 방화벽 내에 있는 일반적인 경우 이 구성을 적용하지 마십시오.

하지만 TIM 데이터가 WAN(Wide Area Network)을 통해 전송되는 비보안 환경 또는 DMZ(네트워크 완충 지역)와 같이 관리 VLAN 외부에서 TIM 을 실행하는 경우 적용을 고려하십시오.

다음 단계를 따르십시오.

1. Enterprise Manager 속성을 기본값으로 수정하는 방법은 *CA APM 구성 및 관리 안내서*의 지침을 따르십시오.
2. 편집하기 위해 *tess-customer.properties* 파일을 여는 경우 다음 행을 추가합니다.

   ```
   timTessCommunication.useSsl=1
   ```

   timTessCommunication.useSsl 속성을 1 로 설정하면 Enterprise Manager 및 TIM 이 HTTPS 를 통해 통신하도록 구성됩니다.
3. Enterprise Manager 를 다시 시작합니다.

자세한 내용은 *CA APM 구성 및 관리 안내서*를 참조하십시오.

HTTPS 로만 Enterprise Manager 액세스 제한

기본적으로 브라우저와 Enterprise Manager 간의 HTTP 통신이 허용되지만 *<EM_Home>\config* 디렉터리에 위치한 *IntroscopeEnterpriseManager.properties* 파일에서 *introscope.enterprisemanager.webserver.jetty.configurationFile* 속성을 설정하면 HTTPS 를 사용하도록 Enterprise Manager 를 구성할 수 있습니다. 자세한 내용은 *CA APM 구성 및 관리 안내서*를 참조하십시오.

CA APM Transaction Generator(CA APM TG) 보안 정보

CA CEM 은 CA APM Transaction Generator(CA APM TG)로 실행되는 가상 트랜잭션을 추적 및 모니터링할 수 있습니다. CA CEM 의 가상 트랜잭션을 구체적으로 식별하고 CA APM TG 트랜잭션에 대한 별도의 사용자 그룹을 만들어 실제 트랜잭션과 분리하여 모니터링하도록 선택할 수 있습니다.

CA APM TG 트랜잭션은 CA CEM 에서 가상으로 식별될 수 있으므로 실제 사용자에게 영향이 미치기 전에 웹 사이트 또는 웹 응용 프로그램 내의 문제를 사전에 해결할 수 있습니다. CA CEM 분석 기능과 함께 CA APM TG 를 사용하면 실제 웹 응용 프로그램 사용자에게 시뮬레이션된 사용자와 유사한 문제가 발생했는지 확인할 수 있습니다.

CA APM TG 를 사용하여 가상 트랜잭션을 생성하는 경우 CA APM TG 관리 서버에 대한 액세스 권한을 제어하는 액세스 정책을 설정할 수 있습니다. CEM 콘솔과 동일한 로그인 자격 증명을 사용하도록 CA APM TG 관리 서버를 구성할 수 있습니다. 이 경우 단일 자격 증명만 관리하면 되므로 CA CEM 사용자에게는 CEM 콘솔과 CA APM TG 에이전트 구성 모두에 대해 하나의 사용자 이름과 암호만 기억하면 되는 이점이 있습니다.

CA CEM 에 로컬 보안을 사용하는 경우 CEM 시스템 관리자 또는 CEM 구성 관리자 보안 그룹 중 하나에 정의되어 있는 사용자는 CA APM TG 관리자 권한도 갖습니다.

CA CEM 에 CA EEM 보안을 사용하는 경우 시스템 관리 설정 또는 시스템 구성 설정 액세스 정책 중 하나에 대해 *쓰기* 및 *모든 작업* 권한이 있는 사용자는 CA APM TG 관리자 권한도 갖습니다.

참고: CA EEM 에서 *모든 작업* 권한을 설정하려면 "All Actions"(모든 작업) 확인란을 선택합니다.

자세한 내용은 *CA APM Transaction Generator Implementation Guide*(CA APM Transaction Generator 구현 안내서)를 참조하십시오.

제 5 장: CA CEM 과 함께 nCipher 사용

Thales 의 nCipher HSM(하드웨어 보안 모듈)로 보호되는 웹 서버의 트래픽을 모니터링하려면 CA CEM TIM 에 nCipher HSM 을 설치해야 합니다.

이 장에서는 TIM 에 nCipher HSM 을 설치 및 구성하는 방법을 설명합니다.

CA CEM 에서는 nCipher HSM 으로 보호되는 웹 서버의 SSL 개인 키를 읽을 수 있습니다.

다음은 CA CEM 에서 nCipher HSM 을 사용할 때 알아야 할 내용입니다.

1. CA CEM 에서 nCipher HSM 이 지원되는 방식을 자세히 알아봅니다. (페이지 167)
2. TIM 에서 nCipher 를 설정합니다. (페이지 169)
3. 개인 키 및 Operator Card 에 사용 가능한 절차를 이해합니다. (페이지 181)
4. 개인 키 또는 Operator Card 를 변경하는 경우 개인 키 및 Operator Card 를 업데이트하는 방법을 이해합니다. (페이지 186)
5. nCipher 설치 및 구성 문제를 해결합니다. (페이지 187)
6. (선택 사항) CA CEM 에 대한 이전 버전의 nCipher 지원을 이해합니다.

CA CEM 과 함께 nCipher 사용

TIM 에서 nCipher HSM 을 사용하면 개인 SSL 키를 통해 보안을 더 강화하고 FIPS 경계 내의 키 저장소와 함께 보안을 수행할 수 있습니다. HSM 보안 경계의 nCipher PCI 행은 FIPS 140-2 Level 2 와 Level 3 및 Common Criteria EAL4+에 대해 유효성이 검사됩니다. nCipher HSM 을 사용하는 경우 TIM 은 보안 API 를 사용하여 HTTPS 암호 해독에 필요한 정보를 요청할 수 있습니다.

nCipher HSM 은 다음과 같은 여러 TIM 의 변형에 사용할 수 있습니다.

- TIM 소프트웨어 어플라이언스
- Multi-Port Monitor 의 TIM

  참고: Multi-Port Monitor 에 TIM 을 배포하는 방법에 대한 자세한 내용은 *CA APM CA 인프라 관리를 위한 통합 안내서*를 참조하십시오.

nCipher HSM 은 TIM 소프트웨어와 직접 연동하므로 이 장의 지침은 두 배포 모두에 적용됩니다.

환경

CA CEM 은 다음 하드웨어 및 소프트웨어 환경에 대해 인증된 nCipher 를 지원합니다.

하드웨어

- CA CEM TIM 어플라이언스
- nShield Solo PCI 카드

소프트웨어

- CA APM 릴리스 9.5
- nCipher Software Supplement(nCSS) 버전 11.30

중요! nCipher 지원 버전에는 TIM 및 웹 서버의 필수 버전이 포함되며, 이전 릴리스를 사용하는 경우 예기치 않은 결과가 도출될 수 있습니다.

테스팅

다음 버전의 CA CEM 과 nCipher 는 Sun OS 5.10 에서 Sun Java System Web Server 7.0 에 대해 테스트를 마쳤습니다.

nCipher 지원 환경에 대한 자세한 내용은 nCipher 설명서를 참조하십시오. CA CEM 구성에 대해 궁금한 사항은 CA Support 에 문의하십시오.

사전 요구 사항

이 기능을 사용하기 전에 다음을 수행해야 합니다.

- 하나 이상 웹 서버의 SSL 개인 키가 nCipher 보안 환경으로 보호되어야 합니다. 모든 웹 서버 개인 키는 동일한 보안 환경으로 보호되어야 합니다.
- 웹 서버의 nCipher 버전은 TIM 과 동일해야 합니다.
- 웹 서버의 다음 항목을 포함하여 웹 서버에 액세스할 수 있어야 합니다.
  - 보안 환경
  - ACS(Administrator Card Set)

  - OCS(Operator Card Set)
  - 전달 구
- TIM 컴퓨터에 액세스 권한이 있고 다음을 수행할 수 있습니다.
  - TIM 컴퓨터에 Thales-nCipher HSM(하드웨어 보안 모듈)을 설치해야 함
  - nCipher 제품 설명서에 따라 TIM 에서 커널 드라이버를 빌드
  - TIM 에 nCipher Software Supplement 를 설치하고 HSM 에 액세스하도록 구성해야 함
  - nCipher Software Supplement(nCSS) 11.30 을 사용해야 함. 기능은 이전 소프트웨어 릴리스와 거의 동일하므로 이 문서에서 언급한 nCipher 설명서의 참조 내용은 모두 *nShield User Guide for Unix-based OS version 6.3*(Unix 기반 OS 6.3 용 nShield 사용자 안내서)에 기반합니다.
- CA CEM 및 TIM 컴퓨터에 익숙하고 CA CEM 설명서를 숙지해야 함
- Thales-nCipher 제품 설명서, 특히 TIM 컴퓨터와 웹 서버에서 HSM 에 대한 사용자 안내서를 숙지해야 함

nCipher 를 지원하도록 CA CEM 설정

다음 섹션에서는 nCipher HSM(하드웨어 보안 모듈)으로 보호되는 SSL 개인 키를 읽도록 TIM 을 설정하는 방법을 설명합니다.

TIM 과 nCipher HSM 을 함께 작동하도록 설정하려면 다음 일련의 절차를 따라야 합니다.

1. TIM 에 nCipher 하드웨어 설치 (페이지 170)
2. TIM 에 nCipher 소프트웨어 설치 (페이지 170)
3. 커널 드라이버 빌드 (페이지 171)
4. TIM 에서 nCipher 설치 확인 (페이지 172)
5. nCipher 보안 환경에 TIM HSM 등록 (페이지 173)
6. CA CEM 에 웹 서버의 nCipher 개인 키 업로드 (페이지 176)
7. TIM 에 nCipher HSM 구성 (페이지 177)
8. nCipher 로 보호되는 웹 트래픽 확인 (페이지 180)

모든 절차를 완료했으면 TIM 과 nCipher HSM 을 사용하여 HTTPS 트래픽의 모니터링을 시작할 수 있습니다.

TIM 에 nCipher 하드웨어 설치

TIM 에 nCipher 하드웨어를 설치하는 기본 단계는 다음과 같습니다. 구체적인 정보는 nCipher 설명서를 참조하십시오.

참고: 여러 TIM 컴퓨터가 있지만 일부 컴퓨터에만 nCipher 가 설치된 경우 nCipher 로 보호되는 웹 서버를 모니터링하도록 nCipher 와 함께 TIM 을 구성하는 작업을 수행해야 합니다. 그래야 부하가 더 효율적으로 분산됩니다.

다음 단계를 따르십시오.

1. nShield HSM 하드웨어(PCI 카드 및 카드 판독기)를 준비합니다.
2. 하드웨어 및 환경에 맞는 nCipher 설명서를 준비합니다.
3. TIM 컴퓨터에 제공되는 하드웨어 설명서를 준비합니다.
4. nCipher 설명서의 지침에 따라 TIM 컴퓨터에 하드웨어를 설치합니다. 필요한 경우 TIM 컴퓨터의 하드웨어 설명서를 참조하십시오.
5. 접촉부가 커넥터로 완전히 삽입되었는지 확인합니다.
6. 후면 패널이 섀시의 액세스 슬롯과 올바로 정렬되었는지 확인합니다.
7. TIM 에 nCipher 소프트웨어 설치 (페이지 170)를 계속 진행합니다.

TIM 에 nCipher 소프트웨어 설치

TIM 에 nCipher 소프트웨어를 설치하는 기본 단계는 다음과 같습니다. 구체적인 정보는 nCipher 설명서를 참조하십시오.

다음 단계를 따르십시오.

1. 하드웨어 및 환경에 적합한 nCipher 소프트웨어를 준비합니다.
2. 소프트웨어 및 환경에 맞는 nCipher 설명서를 준비합니다.

nCipher 설명서의 지침을 사용하여 TIM 서버에 모든 nCipher 소프트웨어를 복사하고 설치합니다. 특히 nCipher CD 에 포함된 nShield_Quick_Start_Guide 및 version.txt 파일을 참조하십시오. version.txt 문서에는 모든 패키지 이름이 나열됩니다.

참고: TIM 을 시작한 이후에 nCipher 소프트웨어를 설치한 경우 nCipher 하드웨어와의 연결을 설정하기 위해 TIM 을 다시 시작해야 합니다.

3. TIM 의 "System Setup"(시스템 설정) 페이지에 다음과 같은 nCipher 메뉴 옵션이 포함되어 있는지 확인합니다.
   - "View nCipher Status"(nCipher 상태 보기)
   - "Configure nCipher"(nCipher 구성)

   이들 메뉴 옵션은 nCipher 소프트웨어를 설치한 이후에 나타납니다.
4. 커널 드라이버 빌드 (페이지 171)를 계속 진행합니다.

커널 드라이버 빌드

TIM 과 함께 nShield HSM 을 사용하려면 커널 드라이버를 빌드해야 합니다. nCipher 는 nCipher PCI 커널 드라이버(*nfp*)에 소스를 공급하고 로드 가능한 모듈로 드라이버를 빌드할 수 있도록 *makefile* 을 공급합니다.

필수 개발자 도구(Red Hat 배포의 RPM)를 다운로드합니다.

TIM 컴퓨터에 nCipher 소프트웨어를 설치 및 구성하려면 관련 구현 설명서(소프트웨어와 일치하는 버전의 이 설명서 및 Thales nCipher 설명서)도 필요합니다.

다음 단계를 따르십시오.

중요! TIM 에 위치한 Red Hat 버전과 일치하는 RPM 을 다운로드합니다.

1. Thales 의 *nShield User Guide for Unix-based OS*(Unix 기반 OS 용 nShield 사용자 안내서) 및 *nShield Quick Start Guide for Unix-based OS*(Unix 기반 OS 용 nShield 빠른 시작 안내서)를 얻으십시오.
2. 커널 드라이버를 빌드하려면 nCipher 설명서의 지침을 따르십시오.
3. TIM 에서 nCipher 설치 확인 (페이지 172)을 계속 진행합니다.

TIM 에서 nCipher 설치 확인

nCipher 하드웨어 및 소프트웨어를 설치하고 나면 TIM nCipher 상태 페이지를 사용하여 새 하드웨어 및 소프트웨어를 확인할 수 있습니다.

소프트웨어 확인

nCipher 소프트웨어가 TIM 에서 작동하는지 확인합니다.

다음 단계를 따르십시오.

1. "TIM System Setup"(TIM 시스템 설정) > "View nCipher Status"(nCipher 상태 보기) 페이지로 이동합니다.
2. 페이지의 출력 정보를 검토합니다. */opt/nfast/bin/enquiry* 출력의 첫 부분은 다음과 같이 표시되어야 합니다.

```
Server:
 enquiry reply flags  none
 enquiry reply level  Six
 serial number        ...
 mode                 operational
```

3. 출력에 운영 모드임이 나타나지 않으면 nCipher 설명서를 참조하십시오.

하드웨어 확인

nCipher 하드웨어가 TIM 에서 작동하는지 확인합니다.

다음 단계를 따르십시오.

1. "TIM System Setup"(TIM 시스템 설정) > "View nCipher Status"(nCipher 상태 보기) 페이지로 이동합니다.
2. 페이지의 출력 정보를 검토합니다. */opt/nfast/bin/enquiry* 출력에 모듈 섹션이 하나 이상 있어야 하고 다음과 같이 표시되어야 합니다.

```
Module #1:
 enquiry reply flags  none
 enquiry reply level  Six
 serial number        ...
 mode                 operational
```

3. 출력에 운영 모드임이 나타나지 않으면 nCipher 설명서를 참조하십시오.
4. nCipher 보안 환경에 TIM HSM 등록 (페이지 173)을 계속 진행합니다.

nCipher 보안 환경에 TIM HSM 등록

TIM 컴퓨터에 설치된 HSM 을 사용하여 웹 서버 개인 키에 액세스하려면 웹 서버 키를 보호하는 보안 환경에 TIM HSM 을 등록해야 합니다. nCipher 보안 환경 프레임워크에는 다음이 포함됩니다.

- HSM(하드웨어 보안 모듈) - PCI 하드웨어 카드
- ACS(Administrator Card Set) - 관리 및 구성 액세스 권한을 제어하는 스마트 카드
- OCS(Operator Card Set) - 액세스 권한을 제어하는 스마트 카드
- SSL 개인 키 및 인증서 데이터

nCipher 보안 환경 개념에 대한 자세한 내용은 *nShield User Guide for Unix-based OS*(Unix 기반 OS 용 nShield 사용자 안내서)를 참조하십시오.

중요! 등록을 시작하기 전에 웹 서버 및 TIM 모두에 대해 최소 버전의 nCipher 소프트웨어를 실행하고 있는지 확인해야 합니다. 자세한 내용은 소프트웨어 (페이지 168)를 참조하십시오.

등록 프로세스를 수행하려면 다음을 충족해야 합니다.

- TIM 컴퓨터 및 nCipher HSM 에 물리적으로 액세스할 수 있어야 합니다.
- TIM 컴퓨터의 명령줄 세션을 루트로 실행하거나 *nfast* 그룹 구성원인 사용자로 실행해야 합니다.
- 보안 환경에 대한 ACS(Administrator Card Set)의 쿼럼이 있어야 합니다.
- 전달 구가 있는 모든 OCS(Operator Card Set)의 전달 구를 알아야 합니다.

중요! 시작하기 전에 웹 서버에 있는 */opt/nfast/kmdata/local* 디렉터리(또는 Windows 의 *%NFAST_KMDATA%\local*)와 해당 콘텐츠의 *백업 복사본*을 만들고 안전한 장소에 보관해야 합니다.

웹 서버에서 TIM 으로 보안 환경 복사

TIM 의 등록 프로세스를 시작하려면 웹 서버의 보안 환경 복사본이 필요합니다.

다음 단계를 따르십시오.

1. 콘텐츠를 모두 포함하여 웹 서버의 */opt/nfast/kmdata/local* 디렉터리(Windows 의 경우 *%NFAST_KMDATA%\local*)를 복사합니다.
2. 콘텐츠를 모두 포함하여 */opt/nfast/kmdata/local* 디렉터리의 복사본을 TIM 컴퓨터에 배치합니다.
3. TIM 의 새 디렉터리에 'world' 파일, 'cards_*' 및 'card_*' 파일(보안 환경의 각 스마트 카드 집합에 해당), 'key_*' 파일(보안 환경으로 보호되는 각 키에 해당)이 포함되어 있는지 확인합니다.

보안 환경에 TIM 등록

TIM 을 보안 환경에 등록하려면 TIM 컴퓨터에서 명령줄 세션을 실행해야 합니다.

다음 단계를 따르십시오.

1. nCipher HSM 후면의 스위치를 'I' 위치로 옮깁니다.
2. 명령줄에서 다음을 실행합니다.

   /opt/nfast/bin/nopclearfail -ca

   -ca 옵션은 사용할 수 있는 모든 nCipher 모듈을 *nopclearfail* 명령으로 초기화한다는 것을 지정합니다.
3. 다음 단계를 진행하기 전에 정확한 ACS 카드 번호와 해당 전달 구를 기록해 둡니다.
4. 명령줄에서 다음을 실행합니다.

   /opt/nfast/bin/new-world -I

   new-world 유틸리티의 쿼럼에 도달할 때까지 ACS 카드와 해당 전달 구를 삽입하라는 메시지가 나타납니다. 참고로, *-I* 옵션은 기존 보안 환경에 모듈을 추가한다는 것을 나타냅니다.

   new-world 가 완료될 때까지 카드를 계속 처리합니다.

   new-world 유틸리티에 대한 자세한 내용은 nCipher 설명서를 참조하십시오.

5. nCipher HSM 후면의 스위치를 'O' 위치로 옮깁니다.
6. 명령줄에서 다음을 실행합니다.

   /opt/nfast/bin/nopclearfail -ca

   이 절차를 완료하면 해당 보안 환경으로 보호되는 개인 키가 HSM 에서 사용될 수 있습니다. TIM HSM 이 보안 환경에 등록되어 웹 서버 개인 키에 대한 액세스 권한이 부여됩니다.

등록 확인

보안 환경 및 TIM HSM 을 사용할 수 있으며, 보안 환경 및 TIM HSM 에서 웹 서버 개인 키에 액세스할 수 있는지 확인해야 합니다.

다음 단계를 따르십시오.

1. "TIM System Setup"(TIM 시스템 설정) > "View nCipher Status"(nCipher 상태 보기) 페이지로 이동합니다.
2. "TIM System Setup"(TIM 시스템 설정) > "View nCipher Status"(nCipher 상태 보기) 페이지의 출력 정보를 검토합니다. */opt/nfast/bin/enquiry* 출력의 첫 번째 부분은 "Operational"(운영) 모드임을 나타냅니다.

```
Server:
 enquiry reply flags  none
 enquiry reply level  Six
 serial number        ...
 mode                 operational
```

3. 출력에 운영 모드임이 나타나지 않으면 nCipher 설명서를 참조하십시오.
4. "TIM System Setup"(TIM 시스템 설정) > "View nCipher Status"(nCipher 상태 보기) 페이지의 출력 정보를 검토합니다. 다음과 같이 */opt/nfast/bin/nfkminfo* 출력에서 보안 환경 및 모듈 디스플레이를 모두 "Usable"(사용 가능)로 설정해야 합니다(단어 앞의 감탄 부호 없이 설정).

```
World
 generation  2
 state      0x7270000 Initialised Usable Recovery !PINRecovery !ExistingClient
RTC NVRAM !FTO SEEDebug
 n_modules   1
.
.
.
Module #1
 generation 2
 state      0x2 Usable
 flags      0x10000 ShareTarget
 n_slots    2
```

5. 출력에 "Usable"(사용 가능) 모드임이 나타나지 않으면 nCipher 설명서를 참조하십시오.
6. 보호된 특정 키를 선택하는 옵션으로 대체한 */opt/nfast/bin/preload ... pause , with '...'*를 실행하여 보호된 키를 HSM 으로 로드할 수 있어야 합니다. 자세한 내용은 *preload --help* 를 참조하십시오.

   참고: OCS 보호 키로는 NotPersistent 옵션을 사용할 수 있습니다. 이러한 경우 카드가 슬롯에 남아 있는 한 미리 로드된 키를 응용 프로그램에서 사용할 수 있습니다. 카드가 제거되면 로드된 키가 무효화되며 미리 로드된 키를 사용하려는 응용 프로그램이 암호화 작업에 실패합니다. 키를 다시 로드하려면 응용 프로그램 및 미리 로드 프로세스를 다시 시작해야 합니다.
7. CA CEM 에 웹 서버의 nCipher 개인 키 업로드 (페이지 176)를 계속 진행합니다.

CA CEM 에 웹 서버의 nCipher 개인 키 업로드

TIM 은 *embed* 응용 프로그램 유형의 개인 키만 수락합니다. 웹 서버가 Apache 이외인 경우 키를 업로드하기 전에 대상을 다시 지정해야 합니다.

개인 키는 HSM 단독으로 보호하거나 OCS 로 보호할 수 있으며, OCS 는 전달 구를 사용하여 보호할 수 있습니다.

nCipher OCS(Operator Card Set)의 경우 여러 카드를 사용할 수 있으며 그러한 카드가 모두 필요할 수 있습니다. 하지만 TIM 은 TIM 내의 프로세스가 자동화되어 있으므로 카드를 하나만 지원합니다. 웹 서버가 여러 카드를 사용하는 경우 TIM 을 위해 해당 카드를 통합해야 합니다.

개인 키를 CA CEM 에 업로드하려면

1. 웹 서버의 개인 키가 *embed* 응용 프로그램 유형이 아닌 경우 해당 개인 키의 대상을 다시 지정해야 합니다. 자세한 내용은 웹 서버 개인 키의 대상 다시 지정 (페이지 181)을 참조하십시오.
2. */tmp/webserver1.pem* 파일을 CA CEM 에 업로드합니다. *CA APM 구성 및 관리 안내서*에서 CA CEM 으로 보안 웹 응용 프로그램을 모니터링하는 방법에 대한 장을 참조하십시오.

3. 기존 OCS(Operator Card Set)의 크기가 TIM 카드를 수용할 만큼 크지 않은 경우 새 OCS 를 만들 수 있습니다. 자세한 내용은 새 OCS(Operator Card Set) 만들기 (페이지 184)를 참조하십시오.
4. TIM 에 여러 개인 키를 사용해야 하는 경우 동일한 OCS 를 사용하여 해당 키를 모두 보호하려 할 수 있습니다. 자세한 내용은 OCS(Operator Card Set) 통합 (페이지 184)을 참조하십시오.

개인 키가 업로드되었는지 확인하려면

1. "TIM 시스템 설정" > "View TIM SSL Server Status"(TIM SSL 서버 상태 보기) 페이지로 이동합니다.
2. 웹 서버의 IP 주소 및 포트 번호를 확인합니다.
3. TIM 에 nCipher HSM 구성 (페이지 177)을 계속 진행합니다.

TIM 에 nCipher HSM 구성

이제 nCipher HSM 및 선택적 OCS 와 함께 작동하도록 TIM 을 구성할 준비가 완료되었습니다.

TIM 구성

다음 단계를 따르십시오.

1. "TIM System Setup"(TIM 시스템 설정) > "Configure nCipher"(nCipher 구성) 페이지로 이동합니다.
2. TIM 에서 nCipher 를 지원하도록 설정하려면 "Enable nCipher HSM"(nCipher HSM 사용)을 클릭합니다.

   그러면 다음 번에 TIM 을 시작할 때 사용하도록 설정됩니다.
3. TIM 에서 nCipher 를 지원하지 않도록 설정하려면 "Disable nCipher HSM"(nCipher HSM 사용 안 함)을 클릭합니다.

   그러면 다음 번에 TIM 을 시작할 때 사용하지 않도록 설정됩니다.
4. TIM 을 다시 시작할 때마다 nCipher HSM 을 지원하도록 설정하려면 OCS(Operator Card Set) 이름을 입력하고 "Save"(저장)를 클릭해야 합니다.

   자세한 내용은 무인 작업 정보 (페이지 179)를 참조하십시오.

5. Operator Card 에 전달 구가 있는 경우 다음과 같이 해당 전달 구를 저장하거나 TIM 을 다시 시작할 때마다 입력할 수 있습니다.

   a. 저장할 Operator Card 전달 구를 입력하고 "Save"(저장)를 클릭합니다.

      전달 구는 암호화된 상태로 저장되므로 TIM 웹 페이지를 사용하여 읽을 수 없습니다. Operator Card 에 전달 구가 있는 경우 이 작업을 통해 무인 작업을 수행할 수 있습니다. 자세한 내용은 무인 작업 정보 (페이지 179)를 참조하십시오.

   -또는-

   b. Operator Card 전달 구를 입력하고 "Start TIM with this pass phrase"(이 전달 구로 TIM 시작)를 클릭합니다.

      그러면 전달 구가 저장되지 않습니다.

6. 저장된 전달 구를 지워야 하는 경우 "Erase the stored pass phrase"(저장된 전달 구 지우기)를 클릭합니다.

TIM 다시 시작 및 구성 확인

nCipher 를 지원하도록 설정 또는 설정하지 않으려는 경우 전달 구를 저장한 후 TIM 을 다시 시작해야 합니다.

다음 단계를 따르십시오.

1. "Return to TIM Setup"(TIM 설정으로 돌아가기)을 클릭합니다.
2. "Start or Stop TIM"(TIM 시작 또는 중지)을 클릭합니다.
3. "Start (or restart) TIM"(TIM 시작(또는 다시 시작))을 클릭합니다.
4. 구성이 변경되었는지 확인합니다.

   페이지에 상태가 다음과 같이 표시됩니다.

```
TIM Control
Stopping old nCipher preload process
Using nCipher HSM
Running background nCipher preload
Operator card set "testocs1" specified
preload log:
-------------------------------------------
Loading cardsets:
testocs1 on modules 1
Checking modules and reading cards ...
Checking modules and reading cards ...
```

```
Loading `testocs1':
Module 1 slot 0: `testocs1' #3
Module 1 slot 0: Enter passphrase: (reading cards)
Module 1 slot 0: Enter passphrase:
********
Module 1 slot 0:- passphrase supplied - reading card
Module #1 Slot #0: Processing ...
Card reading complete.
Stored Cardset: testocs1 (1ff8...) on module #1
Stored Unsure -- multiple objects on module #1
Loaded embed aee3ef6fefb153f743843a284954828c09328500 key (RSAPrivate) on
modules 1
-----------------------------------------------
The action you requested may take several seconds to complete.
```

참고: 동일한 nCipher 로그 정보를 */etc/wily/cem/tim/logs/ncipher/preload-log.txt* 에서 찾을 수 있습니다.

5. OCS(Operator Card Set) 이름이 올바른지 확인합니다.
6. 다음 행을 살펴봅니다.

```
Card reading complete.
Loaded embed < key > (RSAPrivate) on modules < n >
```

7. nCipher 로 보호되는 웹 트래픽 확인 (페이지 180)을 계속 진행합니다.

무인 작업 정보

일반적으로 시스템이 시작될 때 TIM 이 자동으로 시작됩니다. HSM 에서 이 무인 작업을 설정하려면

- TIM 컴퓨터에 사용하는 OCS(Operator Card Set)에 1 쿼럼이 있어야 합니다. 이는 웹 서버 컴퓨터의 OCS(Operator Card Set)와 무관합니다.
- TIM 컴퓨터의 Operator Card 에서 전달 구를 없애거나, "TIM System Setup"(TIM 시스템 설정) > "Configure nCipher"(nCipher 구성) 페이지에서 전달 구를 저장 또는 입력해야 합니다. Operator Card 에서 전달 구를 제거하는 방법에 대한 자세한 내용은 Operator Card 에서 전달 구 제거 (페이지 183)를 참조하십시오.
- TIM 컴퓨터의 HSM 에 연결된 카드 판독기에 Operator Card 를 그대로 두어야 합니다.
- "TIM System Setup"(TIM 시스템 설정) > "Configure nCipher"(nCipher 구성) 페이지에서 OCS(Operator Card Set)의 이름을 저장해야 합니다.

중요! Operator Card 의 전달 구가 저장한 것과 일치하지 않거나, 잘못된 카드가 카드 판독기에 있거나 카드가 아예 없으면 TIM 이 자동으로 시작되지 않습니다. 참고로, 이는 TIM 로그에 기록되지 않지만 */etc/wily/cem/tim/logs/ncipher/preload1-log.txt* 및 *preload2-log.txt* 파일에서 찾을 수 있습니다. 시작되지 않는 경우 nCipher 구성 페이지에서 TIM 을 시작하거나, "TIM System Setup"(TIM 시스템 설정) > "Start or Stop TIM"(TIM 시작 또는 중지) 페이지에서 필요한 정보를 저장한 다음 TIM 을 시작할 수도 있습니다.

nCipher 로 보호되는 웹 트래픽 확인

nCipher 와 함께 작동하는 CA CEM 기능을 확인합니다. 웹 트래픽을 확인할 수 있습니다.

TIM 트랜잭션 검사를 사용하여 SSL 기능을 확인하려면

참고: *CA APM 구성 및 관리 안내서*에서 CA CEM 으로 보안 웹 응용 프로그램을 모니터링하는 방법에 대한 정보를 참조하십시오. 또한 *SSL 을 사용하여 CA CEM 기능을 확인*하는 정보도 참조하십시오.

TIM SSL 서버 상태를 사용하여 SSL 기능을 확인하려면

1. "TIM 시스템 설정" > "View TIM SSL Server Status"(TIM SSL 서버 상태 보기) 페이지로 이동합니다.
2. 암호 해독 오류 없이 nCipher 서버와의 연결이 확인되면 TIM 에서 nCipher 를 사용하여 웹 서버 트래픽을 모니터링할 수 있습니다.

TIM 추적 기능을 사용하여 SSL 이 작동하는지 확인하려면

1. "TIM System Setup"(TIM 시스템 설정) > "Configure TIM Trace Options"(TIM 추적 옵션 구성) 페이지로 이동합니다.
2. HTTP 구성 요소를 추적하는 옵션을 사용하도록 선택합니다.
3. 암호화된 서버에 대한 구성 요소가 TIM 로그에 표시되면 해당 서버는 nCipher 를 사용하며 암호 해독이 작동하는 것입니다.

nCipher 키 및 운영자 카드 작업

이 단원에서는 TIM 과 함께 사용할 수 있도록 웹 서버 개인 키를 준비하는 방법에 대한 정보를 제공합니다. 여기에 설명된 Thales-nCipher 유틸리티 작업은 웹 서버에서 실행해야 합니다.

중요! 시작하기 전에 */opt/nfast/kmdata/local*(또는 Windows 의 *%NFAST_KMDATA%\local*)의 백업 복사본을 만듭니다. 이는 TIM 컴퓨터 및 웹 서버 모두에 대해 중요합니다.

이 단원에는 다음과 같은 항목이 포함되어 있습니다.

웹 서버 개인 키의 대상 다시 지정

참고: 이 섹션의 내용은 nCipher 에서 생성한 웹 서버용 개인 키가 있다는 것을 전제로 합니다.

nCipher 보안 환경은 키를 PKCS#11, Java JCE, OpenSSL, Microsoft CAPI(Windows), nCipher 의 기본 API 등 다양한 API(응용 프로그램 프로그래밍 인터페이스)에 사용할 수 있도록 설정합니다. API 와의 액세스를 원활히 하기 위해 키를 생성할 때 선택한 응용 프로그램 유형에 따라 다른 정보가 실제 암호화된 키 자료에 저장됩니다.

기존 키를 다른 응용 프로그램에서 사용할 수 있게 됩니다. 이러한 프로세스를 '대상을 다시 지정한다'고 합니다. 대상을 다시 지정하는 작업을 수행하면 새 키 BLOB 이 파일 시스템에 저장됩니다. 여기에는 새 응용 프로그램 유형에 맞는 새 액세스 정보 및 암호화된 동일한 키 자료가 포함됩니다.

다음은 다양한 웹 서버 소프트웨어 패키지에 사용되는 API 의 일부 목록입니다.

Server	플랫폼	API	응용 프로그램
Apache	모두	OpenSSL	embed

Server	플랫폼	API	응용 프로그램
Sun ONE	모두	PKCS#11	pkcs11
MS IIS	Windows	MS CAPI	mscapi
Tomcat	모두(Java)	jce	jce

TIM 컴퓨터에는 응용 프로그램 유형 *embed* 의 키가 필요합니다. */opt/nfast/kmdata/local* 디렉터리의 암호화된 키 BLOB 이외에, embed 키는 *embedsavefile* 파일(사용할 특정 키 BLOB 으로 OpenSSL 을 가리키는 파일)과 함께 제공됩니다.

Sun ONE 웹 서버 키의 응용 프로그램 유형을 pkcs11 에서 embed 로 변환하려면

- 응용 프로그램 유형 *pkcs11* 및 유형 *embed* 의 키 대상을 다시 지정하려면 아래의 예제를 참조하십시오.

  이 예제에서 해당 키를 보호하는 *MyOCS* 라는 1/N Operator Card 는 HSM 카드 판독기에 있습니다. Enter 또는 Return 키를 사용하여 기본값을 그대로 수락합니다.

```
$ /opt/nfast/bin/generatekey --retarget embed
from-application: Source application? (custom, embed, hwcrhk, pkcs11, simple)
  [default custom] > pkcs11
from-ident: Source key identifier?
(uc66d0f2df3103e32c5703e8de0cfb172a1b35cf82-9051fc31c13c7716a1ac140fdea2eded04c0f
419)
[default
uc66d0f2df3103e32c5703e8de0cfb172a1b35cf82-9051fc31c13c7716a1ac140fdea2eded04c0f4
19]
>
embedsavefile: Filename to write key to? []
> /tmp/webserver1.pem
plainname: Key name? [] > webserver1
키 생성 매개 변수:
 operation         Operation to perform      retarget
 application       Application               embed
 slot              Slot to read cards from   0
 verify            Verify security of key    yes
 from-application  Source application        pkcs11
 from-ident        Source key identifier
uc66d0f2df3103e32c5703e8de0cfb172a1b35cf82-9051fc31c13c7716a1ac140fdea2eded04c0f4
19
 embedsavefile     Filename to write key to  /tmp/webserver1.pem
 plainname         Key name                  webserver1
```

```
Loading `MyOCS':
 Module 1: 0 cards of 1 read
 Module 1 slot 0: `MyOCS' #1
 Module 1 slot 0:- passphrase supplied - reading card
Card reading complete.

Key successfully retargetted.
Path to key:
/opt/nfast/kmdata/local/key_embed_b4c36e18ff38d2d45a2df425abd9febfaf873da4
```

Operator Card 에서 전달 구 제거

보호된 OCS 키를 사용하여 TIM 을 무인으로 실행할 수 있는 한 가지 방법은 TIM 카드 판독기에 위치한 OCS 카드에서 전달 구를 제거하는 것입니다.

다음 단계를 따르십시오.

- 다음과 같이 *cardpp* 를 사용합니다.

```
$ /opt/nfast/bin/cardpp --change -m 1

Checking/changing passphrase(s):
 Module 1 slot 0: `MyOCS' #1
 Module 1 slot 0: Enter passphrase:                                    [^D: done]
 Module 1 slot 0:- passphrase supplied - reading card
 Module 1 slot 0: Enter new passphrase: <return>                       [^D: done]
 Module 1 slot 0:- no passphrase specified - removing passphrase
 Module #1 Slot #0: Processing ...                                     [^D: done]
 Module 1 slot 0: `MyOCS' #1: Passphrase removed
Insert/change card in module (or change module mode)                   [^D: done]
<Control-D>

Done.
```

참고: TIM 은 전달 구 없이 OCS 카드와 함께 실행될 수 있지만 웹 서버 소프트웨어에서 이를 지원하지 않을 수도 있습니다.

새 OCS(Operator Card Set) 만들기

기존 OCS(Operator Card Set)의 크기가 작아서 TIM 을 수용하지 못하는 경우 새 세트를 만들 수 있습니다.

예를 들어 기존 웹 서버가 하나의 OCS(Operator Card Set)와 함께 구성된 경우 TIM 컴퓨터의 카드도 허용할 수 있도록 둘 이상의 카드를 포함하는 새 세트를 만들어야 합니다.

참고: 이는 TIM 컴퓨터에서 대상이 다시 지정된 키에 대해 */opt/nfast/kmdata/local* 의 로컬 복사본을 사용하여 수행하십시오.

다음 단계를 따르십시오.

- 다음과 같이 *createocs* 를 사용합니다.

  ```
  /opt/nfast/bin/createocs -Q 1/n -N name
  ```

  여기서 *n* 은 카드 세트 크기이고 *name* 은 카드 세트에 지정할 이름입니다.

새 OCS(Operator Card Set)이 생성되면 OCS(Operator Card Set) 통합 (페이지 184)에 설명된 대로 키가 새 OCS 로 복구될 수 있습니다.

OCS(Operator Card Set) 통합

TIM 에서 여러 키가 사용되는 경우 동일한 OCS(Operator Card Set)를 통해 이들 키를 보호하는 것이 좋습니다. 서로 다른 OCS 로 여러 키를 *보호하고* 해당 키가 동일한 보안 환경의 *일부이며* 해당 키에 복구를 설정한 경우, 해당 키를 모두 단일 OCS 에 복구할 수 있습니다. 그러면 단일 OCS 를 통해 여러 키를 로드 및 액세스할 수 있습니다.

다음 단계를 따르십시오.

참고: 이 작업을 수행하려면 권한 부여에 대해 ACS(Administrator Card Set)의 쿼럼에 액세스할 수 있어야 합니다.

중요! 라이브 웹 서버 키에 대해 *rocs* 작업을 수행하면 안 됩니다. TIM 컴퓨터에서 복사본으로 작업하십시오.

참고: 키의 대상을 다시 지정해야 하는 경우 OCS 를 조작하기 전에 다음을 수행하십시오. 자세한 내용은 웹 서버 개인 키의 대상 다시 지정 (페이지 181)을 참조하십시오.

1. 키에 복구를 사용하도록 설정했는지 확인하려면 *nfkminfo* 를 사용합니다.

```
$ /opt/nfast/bin/nfkminfo -k embed
Key listing AppName embed (1 keys):
 AppName embed                Ident 5dce27b0a84b517b0db7b5aa2f09452e27a13d38
$ /opt/nfast/bin/nfkminfo -k embed 5dce27b0a84b517b0db7b5aa2f09452e27a13d38
Key AppName embed Ident 5dce27b0a84b517b0db7b5aa2f09452e27a13d38
 BlobKA length         1052
 BlobPubKA length      444
 BlobRecoveryKA length 1208
 name                  "MyKey"
 hash                  d96ee8282cc7f76ea32df1ce299ab087a206e530
 recovery              Enabled
...
```

2. 첫 번째 호출의 식별자를 두 번째 호출로 복사합니다. *recovery Enabled* 행은 키를 새 OCS 로 복구를 할 수 있다는 것을 보여 줍니다.

```
$ /opt/nfast/bin/rocs -i
`rocs' key recovery tool
Useful commands: `help', `help intro', `quit'.
rocs> list cardsets
No. Name                    Keys (recov) Sharing
  1 iWorld1of1              0 (0)        1 of 1; persistent
  2 NonPersistentOCS        9 (9)        1 of 1
rocs> target 1
rocs> list keys
  No. Name                    App        Protected by
    1 MyKey                   caping     module
    2 MyKey                   caping     module
    3 MyKey                   embed      module
    4 Example label           pkcs11     NonPersistentOCS
    ...
rocs> mark 4
rocs> recover

Authorising OCS replacement:
 Module 1: 0 cards of 1 read
 Module 1 slot 0: empty
 Module 1 slot 0: Admin Card #1
... prompt for the ACS passphrase ...
 Module 1 slot 0:- passphrase supplied - reading card
Card reading complete.


Loading `iWorld1of1':
```

```
 Module 1: 0 cards of 1 read
 Module 1 slot 0: Admin Card #1
 Module 1 slot 0: empty
 Module 1 slot 0: `iWorld1of1' #1
... prompt for the OCS passphrase ...
 Module 1 slot 0:- passphrase supplied - reading card
Card reading complete.

rocs> save 4
rocs> quit
```

개인 키 및 Operator Card 업데이트

새 키나 카드 세트가 생성되는 경우와 같이 키 관리 데이터가 웹 서버에서 업데이트되면 키 관리 데이터 파일의 TIM 복사본도 업데이트해야 합니다.

TIM HSM 을 위한 새 키 또는 카드 세트를 만들려면 다음 단계를 따르십시오.

다음 단계를 따르십시오.

1. nCipher 보안 환경에 TIM HSM 등록 (페이지 173)
2. CA CEM 에 웹 서버의 nCipher 개인 키 업로드 (페이지 176)
3. TIM 에 nCipher HSM 구성 (페이지 177)
4. nCipher 로 보호되는 웹 트래픽 확인 (페이지 180)

CA CEM 에서의 nCipher 문제 해결

CA CEM 에서 nCipher 를 설치하는 데 발생한 문제를 해결해야 할 수 있습니다.

증상

nCipher 카드를 설치한 후 TIM 이 시작되지 않습니다. 또는 TIM 에 설치한 nCipher 가 작동하지 않습니다.

해결 방법

1. "TIM System Setup"(TIM 시스템 설정) > "View nCipher Status"(nCipher 상태 보기) 페이지를 검토합니다.
2. 자세한 내용은 TIM 에서 nCipher 설치 확인 (페이지 172)을 참조하십시오.

증상

nCipher HSM 이 예상대로 작동하지 않습니다.

해결 방법

1. 카드를 슬롯에 삽입할 때마다 삽입 횟수가 증가합니다. 따라서 카드를 잘못 삽입하여 다시 삽입하는 경우도 횟수에 반영되어야 합니다.
2. "TIM System Setup"(TIM 시스템 설정) > "View TIM SSL Server Status"(TIM SSL 서버 상태 보기) 페이지를 검토합니다. 자세한 내용은 nCipher 로 보호되는 웹 트래픽 확인 (페이지 180)을 참조하십시오.
3. */etc/wily/cem/tim/logs/ncipher/preload-log.txt* 에서 nCipher 로그 정보를 검토합니다. 자세한 내용은 TIM 다시 시작 및 구성 확인 (페이지 178)을 참조하십시오.
4. TIM 로그를 검토합니다.
5. 키(generatekey)의 대상을 다시 지정하는 경우 "ERROR: Module #1: LoadBlob (loading private blob) failed: Malformed" 메시지가 나타납니다. 일치하지 않는 nCipher 소프트웨어 버전이 있는 경우에 이 메시지가 나타날 수 있습니다. 웹 서버를 업그레이드하여 TIM 의 nCipher 버전을 일치시키거나 Thales 기술 지원부에 문의하십시오.

6. Operator Card 의 전달 구가 저장한 것과 일치하지 않거나, 잘못된 카드가 카드 판독기에 있거나 카드가 아예 없으면 TIM 이 자동으로 시작되지 않습니다. 참고로, 이는 TIM 로그에 기록되지 않지만 */etc/wily/cem/tim/logs/ncipher/preload1-log.txt* 및 *preload2-log.txt* 파일에서 찾을 수 있습니다. 시작되지 않는 경우 nCipher 구성 페이지에서 TIM 을 시작하거나, "TIM System Setup"(TIM 시스템 설정) > "Start or Stop TIM"(TIM 시작 또는 중지) 페이지에서 필요한 정보를 저장한 다음 TIM 을 시작할 수도 있습니다.
7. TIM 시작 로그를 검토합니다.
8. 웹 서버의 OCS 및 Operator Card 가 있는지 확인합니다. 없는 경우 TIM 이 시작되지 않습니다.
9. 보안 환경의 바이너리 사본을 웹 서버에서 TIM 으로 복제하지 않은 경우 대상을 다시 지정하는 동안 형식이 잘못된 BLOB 이 발생합니다.
10. 새 보안 환경을 실행할 수 있도록 kmdata 가 있는지 확인합니다.
11. 새 환경을 실행하기 전에 ACS 카드 수와 해당 전달 구를 파악합니다.
12. 사전 초기화를 수행할 수 있도록 TIM HSM 을 I 위치로 설정하고 점퍼를 OFF 로 설정합니다.
13. 새 환경을 실행하기 전에 사전 초기화를 위해 nCipher HSM 을 I 위치로 설정하고, 새 환경이 적용된 후에는 O 위치로 설정해야 합니다.
14. 새 환경을 실행하기 전에 레지스터를 지워야 한다는 것을 기억하십시오.

증상

nCipher 카드와 소프트웨어를 설치했지만 TIM 에서 웹 서버의 데이터 암호가 해독되지 않고, TIM 이 시작될 때 TIM 로그에 다음과 같은 메시지가 표시됩니다.

```
Initializing SSL crypt engine
Sslinterface: "chil" SSL engine initialization failed
```

해결 방법

1. 다음과 같이 nCipher 번들인 Chil SSL 이 설치되어 있는지 확인합니다.
   a. TIM 콘솔에 로그인합니다(PuTTY 또는 유사한 SSH 클라이언트 사용).
   b. 다음 nCipher 번들이 존재하는지 확인합니다.
   /opt/nfast/toolkit/hwcrhk/libnfhwcrhk.so
2. nCipher 번들인 Chil SSL 이 없으면 nCipher CD 에서 설치합니다.
   a. 자세한 내용은 nCipher 설치 안내서를 참조하십시오. 참고로, nCipher 11.30 의 경우 번들 이름은 */<CD>/linux/lib6-3/nfast.hwcrhk/user.tar* 입니다.
   b. TIM 를 다시 시작합니다.

      다음과 같이 TIM 로그에 Chil SSL 번들이 초기화되었다는 내용이 표시되어야 합니다.

```
Wed Mar 30 02:09:20 2011 19826   Initializing SSL crypt engine
Wed Mar 30 02:09:20 2011 19826   sslinterface: "chil" SSL engine found
Wed Mar 30 02:09:20 2011 19826  sslinterface: "chil" SSL engine initialized
```

증상

웹 서버에서 nCipher 로 암호화된 HTTPS 트래픽이 TIM 에서 암호 해독되는지 확인하려 합니다.

해결 방법

TIM 로그에서 연결 추적 및 HTTPS 구성 요소 추적을 찾습니다.

연결 추적 및 HTTPS 구성 요소 추적이 모두 나타나야 합니다. 예를 들어 포트 9966 에서 HTTPS 서버가 172.16.163.52 인 경우 연결 추적 기능을 사용하도록 설정했으면 구성 요소는 다음과 같이 나타나야 합니다.

```
Wed Mar 30 02:34:00 2011 19826   Trace: [172.16.163.32]:3691->[172.16.163.52]:9966
opened
```

또는 구성 요소 추적 기능을 사용하도록 설정했으면 다음과 같이 나타나야 합니다.

```
Wed Mar 30 02:34:00 2011 19826   Trace: Component #18 request:
172.16.163.52/testpage.html client=[172.16.163.32]:3691
server=[172.16.163.52]:9966 at 02:34:00
```

TIM 에서 트래픽의 암호를 해독하지 못하면 다음과 같이 연결 메시지만 나타납니다.

```
Wed Mar 30 02:34:00 2011 19826   Trace: [172.16.163.32]:3691->[172.16.163.52]:9966
opened

Wed Mar 30 02:34:00 2011 19826   Trace: [172.16.163.32]:3691->[172.16.163.52]:9966
closed
```

제 6 장: CA APM 에서 스마트 카드 인증 사용

이 장에서 다루는 항목:

CA APM 에서 스마트 카드 사용 정보

보안 환경에서는 주로 액세스 관리를 용이하게 하기 위해 단일 입력 지점을 사용해야 합니다. 단일 입력 지점이 없는 경우 보안 관리자는 서로 다른 보안 수준, 요구 사항 및 사용자 액세스 권한으로 여러 프로그램을 관리해야 합니다. 스마트 카드를 사용하면 제어된 모든 리소스에 대한 액세스는 스마트 카드를 통해서만 수행해야 하므로 단일 입력 지점이 제공됩니다.

로컬 보안 또는 CA APM 에 정의된 CA EEM 권한에 기반하여 사용자에게 액세스 권한이 부여됩니다.

CA APM 은 WebView, Web Start 및 CEM 콘솔에 스마트 카드 인증을 제공합니다.

이 단원의 다음 항목에서는 스마트 카드 인증을 소개합니다.

스마트 카드 확인 옵션

다음 옵션 중 하나를 사용하여 스마트 카드 확인을 구성할 수 있습니다.

- *CRL(인증서 해지 목록)*

  인증서가 유효한지 확인하는 가장 일반적인 방법입니다.

  CRL 파일은 해지된 인증서 일련 번호를 포함하는 플랫 파일입니다. 인증 기관에서는 지속적으로 인증서를 추가하므로 CRL 파일은 자주 기한이 경과됩니다. CRL 파일은 미리 결정된 기간에 만료되어 다시 로드되어야 합니다. CRL 파일은 상당한 메모리를 소비하므로 로컬 파일 시스템에 배치해야 합니다. 일반적으로 시스템과 보안 관리자에게 OCSP 서버 또는 응답자에 대한 액세스 권한이 없는 경우 이 옵션을 선택합니다.

- *OCSP(온라인 인증서 상태 프로토콜)*

  일반적으로 시스템 및 보안 관리자에게 OCSP 서버 및 응답자를 설정할 수 있는 리소스 및 소프트웨어가 있는 경우 이 옵션을 선택합니다. OCSP 는 더 낮은 대역폭을 사용하므로 적합성 검사가 더 빨라지고,

  CRL 정보를 요약한 후 데이터베이스에 저장하므로 CRL 파일을 로드하는 데 필요한 시간도 단축됩니다. OCSP 서버가 인증서 확인 요청을 수락합니다. 관리자는 인증서를 언제든지 해지할 수 있으므로 OCSP 서버와 응답자의 기한은 드물게 경과합니다. 제품 서버와 별도의 서버에 OCSP 를 배치할 수 있습니다.

인증서가 모두 인증되고 유효함이 확인되면 스마트 카드가 적용됩니다. 정의된 권한 부여 권한을 바탕으로 CA APM 에 액세스 권한이 부여됩니다. CA EEM 을 사용하여 권한 부여를 수행하는 경우 권한은 *realms.xml* 파일에 정의되고, 로컬 권한 부여를 사용하는 경우 권한은 *users.xml* 파일에 정의됩니다.

스마트 카드 인증 구성 요소

HTTP(Hypertext Transfer Protocol), LDAP(Lightweight Directory Access Protocol), SSL(Secure Sockets Layer) 등의 기본 통신 프로토콜은 스마트 카드 인증에 사용됩니다. CA APM 에 대해 스마트 카드 인증을 설정하기 전에 이들 개념에 대한 기초 지식을 보유하고 있어야 합니다.

또한 스마트 카드 인증에는 다음 구성 요소가 사용됩니다.

- SCARVES(Smart Card Revocation Verification Services)
- CA EEM(CA Embedded Entitlements Manager)
- CA APM 로컬 보안

SCARVES 이해

SCARVES 는 스마트 카드에서 가져온 보안 인증서의 유효성을 검사하는 기능을 제공합니다. 확인 및 유효성 검사 프로세스에는 OCSP 또는 CRL 서버를 사용하여 인증서를 확인하는 옵션이 포함됩니다.

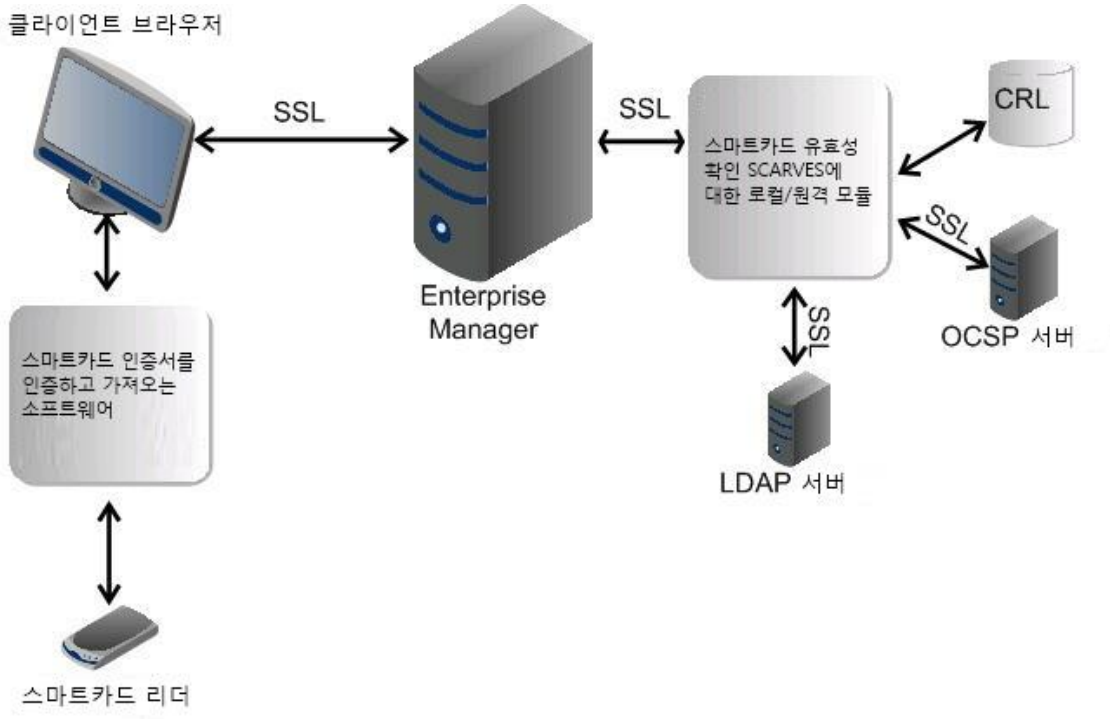
인증서가 성공적으로 확인되는 경우 사용자 기록이 존재하면 LDAP 서버를 통해 인증서와 연결된 사용자 정보를 가져옵니다. SCARVES 는 유효성 검사 프로세스의 일부로 LDAP 사용자 정보 검색을 처리합니다. 그런 다음 로컬 보안 또는 CA EEM 을 사용하는 사용자 역할 및 액세스 권한을 확인하여 Enterprise Manager 는 사용자 정보를 수신하고 권한 부여 프로세스를 계속 진행합니다.

SCARVES 데몬은 인증서 확인 및 유효성 검사 프로세스를 처리하는 프로세스입니다. 기본적으로, 데몬은 OCSP 또는 CRL 서버에 대해 프록시 역할을 수행하는 프로세스를 실행합니다. 구성 요구 사항에 따라 환경에 하나 이상의 데몬이 있을 수 있습니다. 사용하는 데몬의 수에는 사용하는 CRL 이나 OCSP 서버 수와 같은 요소를 포함합니다.

참고: 독립 실행형 Enterprise Manager, Collector 또는 MOM(Manager of Managers)에 대해 스마트 카드 인증을 사용하도록 설정할 수 있습니다. MOM 에 스마트 카드를 사용하도록 설정하면 스마트 카드 인증이 전체 클러스터에 적용되도록 MOM 을 구성해야 합니다.

스마트 카드 데이터를 사용하여 CA APM 에서 인증하는 방법

다음 다이어그램은 스마트 카드 데이터를 사용하여 CA APM 이 프로세스를 처리하고 인증하는 방법을 보여 줍니다.



스마트 카드 데이터는 다음 방식으로 처리됩니다.

1. 운영 체제나 데스크톱에 CA APM 사용자로 로그인한 상태에서 스마트 카드 판독기에 스마트 카드를 삽입합니다.
2. 사용자가 클라이언트 브라우저를 사용하여 CA APM 에 로그인하려는 경우 PIN(개인 식별 번호)을 묻는 메시지가 나타납니다.
3. 사용자가 스마트 카드의 올바른 PIN 을 입력하면 스마트 카드의 모든 인증서를 포함하는 인증서 선택 대화 상자가 열립니다. 사용자는 웹 인증이 처리되도록 올바른 인증서를 선택해야 합니다.
4. 사용자가 인증서를 선택한 후 브라우저 클라이언트가 SSL 연결을 사용하여 Enterprise Manager 에 인증서를 전송합니다.
5. Enterprise Manager 는 인증서를 받은 후 SSL 연결을 사용하여 SCARVES 에 전달합니다.
6. SCARVES 는 인증서를 받아 OCSP 서버 또는 CRL 플랫 파일의 확인을 요청합니다.

7. OCSP 또는 CRL 확인이 성공하면 SCARVES 는 LDAP 서버에서 요청된 사용자 정보를 검색합니다.
8. SCARVES 는 확인 결과와 LDAP 에서 가져온 사용자 정보를 XML 형식으로 Enterprise Manager 에 반환합니다.
9. Enterprise Manager 는 정의된 권한 부여 권한을 바탕으로 CA APM 에 액세스 권한을 부여합니다. CA EEM 을 사용하여 권한 부여 하도록 CA APM 이 구성된 경우 권한은 *realms.xml* 파일에 정의되고, 로컬 권한 부여가 사용되는 경우 권한은 *users.xml* 파일에 정의됩니다.

스마트 카드 인증에 대해 CA APM 설정

CA APM 환경에 스마트 카드 인증을 사용하도록 설정하려면 지정된 순서로 다음 절차를 따라야 합니다.

1. 사용자 환경이 필요한 요구 사항을 충족하는지 확인합니다. 자세한 내용은 스마트 카드 인증 요구 사항 (페이지 196)을 참조하십시오.
2. SCARVES 구성 요소를 추출하여 설치합니다. 자세한 내용은 SCARVES 구성 요소 추출 및 설치 (페이지 197)를 참조하십시오.

   참고: 독립 실행형 Enterprise Manager, Collector 또는 MOM(Manager of Managers)에 대해 스마트 카드 인증을 사용하도록 설정할 수 있습니다. MOM 에 스마트 카드를 사용하도록 설정하면 스마트 카드 인증이 전체 클러스터에 적용되도록 MOM 을 구성해야 합니다.
3. 필요한 키 저장소로 인증서를 로드합니다. 자세한 내용은 다음 문서를 참조하십시오.
   - daemon-cert 키 저장소로 인증서 로드 (페이지 199)
   - daemon-trust 키 저장소로 인증서 로드 (페이지 199)
   - Enterprise Manager 키 저장소로 SCARVES 인증서 로드 (페이지 199)
4. 인증서 암호를 암호화합니다. 자세한 내용은 키 저장소의 인증서 암호 암호화 (페이지 202)를 참조하십시오.
5. CRL 을 사용하여 스마트 카드 확인을 구성하는 경우 CRL 파일을 로드합니다. 자세한 내용은 (선택 항목) CRL 파일 로드 (페이지 202)를 참조하십시오.

6. SCARVES 를 사용하도록 Enterprise Manager 를 구성합니다. 자세한 내용은 SCARVES 를 사용하도록 Enterprise Manager 구성 (페이지 203)을 참조하십시오.
7. SCARVES 래퍼 파일을 구성합니다. 자세한 내용은 SCARVES 래퍼 구성 (페이지 204)을 참조하십시오.
8. SCARVES 를 구성합니다. 자세한 내용은 SCARVES 구성 (페이지 204)을 참조하십시오.
9. SCARVES 를 시작합니다. 자세한 내용은 SCARVES 시작 및 중지 (페이지 217)를 참조하십시오.
10. 스마트 카드가 성공적으로 설치 및 구성되었는지 확인합니다. 자세한 내용은 스마트 카드 설치 확인 (페이지 218)을 참조하십시오.

스마트 카드 인증 요구 사항

하드웨어 필수 구성 요소:

- 스마트 카드
- 스마트 카드 판독기

소프트웨어 요구 사항:

- CA APM 9.0 이상
- 스마트 카드 인증서를 가져오고 유효성을 검사하는 ActivClient 와 같은 소프트웨어
- Internet Explorer 6 또는 7

구성 요구 사항:

- 시스템에 사용된 모든 스마트 카드의 루트 및 중간 보안 인증서
- 스마트 카드 확인 및 유효성 검사에 사용할 수 있도록 기존 LDAP 디렉터리를 통합하는 LDAP 서버 정보
- OCSP 서버를 사용할 계획인 경우 다음과 같은 모든 OCSP 서버 정보를 수집합니다.
  - 응답자 URL
  - OCSP 서버 인증서

- CRL 파일을 사용할 계획인 경우 시스템에 사용된 스마트 카드의 모든 CRL 파일을 수집합니다.
  - 필요한 SCARVES 데몬의 수는 스마트 카드 네트워크 솔루션을 구성하는 방식에 의해 일부 결정됩니다. 예를 들어 CRL 파일은 커지는 경향이 있으므로 SCARVES 데몬은 모든 CRL 파일을 메모리에 유지합니다.

    계산을 시작하기 좋은 지점은 데몬당 256 MB CRL 파일 이하입니다. 단일 서버가 처리할 수 있는 수보다 더 많은 데몬이 필요한 경우 전용 OCSP 서버에 투자하는 것을 고려하십시오.
  - 데몬의 수를 계산하는 것과 더불어 다음 SCARVES 데몬 값을 계획 및 기록하여 구성을 준비합니다.
    - 각 데몬의 이름
    - 각 데몬의 포트 번호
    - 각 CRL 파일의 디렉터리 이름(예: *<SCARVES_HOME>/crls/<daemon_name>*)

Windows 에서 SCARVES 구성 요소 추출 및 설치

SCARVES 를 구성하고 스마트 카드 인증을 사용하도록 설정할 수 있도록 SCARVES 구성 요소를 추출합니다.

Windows 의 경우

1. SCARVES 구성 요소를 저장하는 데 사용할 디렉터리를 만듭니다. 예를 들어 *<드라이브>:\SmartCard\scarves* 입니다.

   만든 디렉터리는 *<SCARVES_HOME>*이라 하는 스마트 카드 홈 디렉터리가 됩니다.
2. Enterprise Manager 가 설치된 최상위 디렉터리로 이동합니다. 예를 들어 *<EM_HOME>*입니다.
3. *examples\SmartCardAuthentication* 으로 이동하고 사용자 환경에 맞는 *scarve_0.1* 파일에 콘텐츠를 추출합니다. Enterprise Manager 를 설치하는 방법에 대한 자세한 내용은 *CA APM 설치 및 업그레이드 안내서*를 참조하십시오.

   다음 디렉터리가 만들어집니다.
   - bin
   - conf

- crls
- keystores
- lib
- 로그

4. *<SCARVES_HOME>\bin* 디렉터리의 *InstallScarves-NT.bat* 를 실행합니다.

   파일이 성공적으로 실행되면 SCARVES 구성 요소가 설치됩니다.

Unix 및 Linux 의 경우

1. */etc/init.d* 로 이동하여 *<SCARVES_HOME>*/bin/scarves 스크립트를 연결합니다.
2. 다음 *rc?.d* 디렉터리를 연결합니다.
   - -s <SCARVES_HOME>/bin/scarves /etc/init.d/scarves
   - -s /etc/init.d/scarves /etc/rc3.d/S99scarves
   - -s /etc/init.d/scarves /etc/rc2.d/K15scarves
   - /sbin/chkconfig --add scarves

중요! 스크립트는 구성 파일의 위치를 찾는 링크를 사용하기 때문에 이들은 기호로된 링크여야 합니다.

인증서 로드

스마트 카드는 SSL 을 통해 일련의 인증서를 사용하여 인증합니다. 인증서는 여러 키 저장소에 로드되어야 합니다. 자세한 내용은 다음 항목을 참조하십시오.

- daemon-cert 키 저장소로 인증서 로드 (페이지 199)
- daemon-trust 키 저장소로 인증서 로드 (페이지 199)
- Enterprise Manager 키 저장소로 SCARVES 인증서 로드 (페이지 199)

daemon-cert 키 저장소로 인증서 로드

데몬 정보를 클라이언트 응용 프로그램에 제공할 수 있도록 daemon-cert 키 저장소로 서버 인증서를 로드합니다. 이는 SSL 을 통해 SCARVES 로 통신하는 경우 Enterprise Manager 는 클라이언트의 역할을 합니다.

인증서를 사용하는 다양한 명령에 대한 자세한 내용은 인증서를 사용하는 명령 (페이지 199)을 참조하십시오.

daemon-trust 키 저장소로 인증서 로드

SSL 을 통해 OCSP 및 LDAP 서버와 통신하도록 daemon-trust 키 저장소로 인증서를 로드합니다.

참고: OCSP 를 사용하도록 SCARVES 를 구성하는 경우 별칭 이름을 기록해 둡니다. SCARVES 를 구성하려면 별칭 이름이 필요합니다. 자세한 내용은 (선택 사항) OCSP 를 사용하도록 SCARVES 구성 (페이지 214)을 참조하십시오.

Enterprise Manager 키 저장소로 인증서 로드

SCARVES 와 통신할 수 있도록 SCARVES 인증서를 Enterprise Manager 로 로드합니다. Enterprise Manager 가 SSL 을 사용하여 SCARVES 와 클라이언트 인증서를 주고 받는 경우 확인 작업이 수행됩니다. 인증서를 사용하는 다양한 명령에 대한 자세한 내용은 인증서를 사용하는 명령 (페이지 199)을 참조하십시오.

인증서 명령

인증서 명령을 사용하여 키 저장소에서 인증서를 가져오고, 생성하고, 내보낼 수 있습니다. 자세한 내용은 다음 단원을 참조하십시오.

- 자체 서명된 인증서 생성 (페이지 200)
- 인증서 가져오기 (페이지 201)
- 인증서 내보내기 (페이지 201)

자체 서명된 인증서 생성

-genkey 명령을 사용하여 자체 서명된 보안 인증서를 생성할 수 있습니다. 이 명령을 사용하여 모든 키 저장소에 대해 자체 서명된 인증서를 생성할 수 있습니다.

다음 단계를 따르십시오.

1. CA APM 서버에 루트로 로그인하고 명령 프롬프트에 액세스합니다.
2. *$JAVA_HOME/bin/keytool* 로 이동하고 *-genkey* 명령을 사용하여 유틸리티를 실행합니다. 예:

   ```
   -genkey -keyalg RSA -keystore <SCARVES_HOME>/keystores/daemoncert -alias
   <cert_alias>
   ```

   조직의 콘텐츠를 지정하는 대화식 프로세스가 시작되며, 다음과 같은 정보가 표시됩니다.

   ```
   Enter keystore password: changeit
   Re-enter new password: changeit
   What is your first and last name?
     [Unknown]:  name.company.com
   What is the name of your organizational unit?
     [Unknown]:  ABC
   What is the name of your organization?
     [Unknown]:  NOC
   What is the name of your City or Locality?
     [Unknown]:  Anytown
   What is the name of your State or Province?
     [Unknown]:  Alaska
   What is the two-letter country code for this unit?
     [Unknown]:  US
   Is CN=name.company.com, OU=ABC, O=NOC, L=Anytown,
   ST=Alaska, C=US correct?
     [no]:  yes

   Enter key password for <newcert>
           (RETURN if same as keystore password):
   ```

인증서 가져오기

-importcert 명령을 사용하여 인증서를 가져옵니다. 이 명령은 모든 키 저장소에 인증서를 가져오는 데 사용할 수 있습니다.

다음 단계를 따르십시오.

1. CA APM 서버에 루트로 로그인하고 명령 프롬프트에 액세스합니다.
2. *$JAVA_HOME/bin/keytool* 로 이동하고 *-importcert* 명령을 사용하여 유틸리티를 실행합니다. 예:

```
keytool -importcert -keystore <SCARVES_HOME>/keystores/daemoncert -alias
cert_alias -file cert_file
```

인증서 내보내기

-exportcert 명령을 사용하여 인증서를 내보냅니다. 이 명령은 모든 키 저장소의 인증서를 내보내는 데 사용할 수 있습니다.

다음 단계를 따르십시오.

1. CA APM 서버에 루트로 로그인하고 명령 프롬프트에 액세스합니다.
2. *$JAVA_HOME/bin/keytool* 로 이동하고 *-exportcert* 명령을 사용하여 유틸리티를 실행합니다. 예:

```
keytool -exportcert -keystore <SCARVES_HOME>/keystores/daemoncert -alias
cert_alias -file cert_file
```

키 저장소에 대한 인증서 암호 암호화

키 저장소에는 오직 암호화된 인증서 암호만 보관됩니다. 암호화된 암호는 인증서를 보호합니다. 암호화 알고리즘은 AES(Advanced Encryption Standard)이며, 알고리즘은 서비스 중인 키와 일반 텍스트가 없는 데몬 코드를 포함합니다. 암호화된 암호는 인쇄 가능한 문자열을 생성할 수 있도록 Base64 유형으로 인코딩됩니다.

다음 단계를 따르십시오.

1. *<SCARVES_HOME>/lib* 으로 이동하고 *scarve_client.jar* 파일을 엽니다.

   이 파일은 키 저장소 암호화에 필요한 암호를 가져옵니다.

2. 다음 명령을 실행하십시오.

   ```
   java –cp scarve_client.jar com.ca.scarve.common.xml.cond e p
   <password_that_requires_encryption>
   ```

   암호화된 암호는 *SCARVESconfig.xml* 파일에 사용될 수 있습니다.

(선택 항목) CRL 파일 로드

CRL 을 사용하도록 SCARVES 를 구성하려면 CRL 파일도 로드해야 합니다.

다음 단계를 따르십시오.

- CRL 파일을 *<SCARVES_HOME>/crls/<DAEMON_NAME>* 디렉터리에 복사합니다.

  참고: CRL 을 사용하도록 SCARVES 를 구성하는 경우 CRL 위치를 기록해 둡니다. SCARVES 를 구성하는 데 CRL 위치가 필요합니다. 자세한 내용은 (선택 사항) CRL 을 사용하도록 SCARVES 구성 (페이지 212)을 참조하십시오.

SCARVES 를 사용하도록 Enterprise Manager 구성

스마트 카드 인증을 사용하도록 Enterprise Manager 를 구성해야 합니다.

다음 단계를 따르십시오.

1. *<EM_HOME>\config* 로 이동한 후 *IntroscopeEnterpriseManager.properties* 파일을 열고 다음 속성을 설정합니다.
   - *introscope.enterprisemanager.scauth.SCARVES.hostname=<scarves_machine_name>*
   - *introscope.enterprisemanager.scauth.SCARVES.port=9998*
   - *introscope.enterprisemanager.webserver.scauth.keystore=/internal/daemoncert*
   - *introscope.enterprisemanager.webserver.scauth.keypass=password*
   - *introscope.enterprisemanager.webserver.scauth.enable=true*
2. *<EM_HOME>\config* 를 이동한 후 *em-jetty-config.xml* 파일을 열고 다음 속성을 설정합니다.
   - *needclientauth= true*
3. *<EM_HOME>\config* 로 이동한 후 *IntroscopeEnterpriseManager.properties* 파일을 열고 다음 단계를 수행합니다.
   a. *introscope.enterprisemanager.webserver.jetty.configurationFile=em-jetty-config.xml* 속성의 주석 처리를 제거합니다.
   b. *needclientauth* 속성을 *true* 로 설정합니다.
4. *<EM_HOME>\config* 로 이동한 후 *introscopewebview.properties* 파일을 열고 다음 단계를 수행합니다.
   a. *introscope.webview.jetty.configurationFile=webview-jetty-config.xml* 속성의 주석 처리를 제거합니다.
   b. *needclientauth* 속성을 *true* 로 설정합니다.
5. Enterprise Manager 를 다시 시작합니다.

SCARVES 래퍼 구성

SCARVES 래퍼는 SCARVES 를 실행하는 Java 프로그램을 시작하는 데 필요한 정보를 제공하는 구성 파일입니다.

다음 단계를 따르십시오.

1. *<SCARVES_HOME>/conf* 및 *wrapper.conf* 파일로 이동합니다.
2. 다음 속성을 설정합니다.
   - wrapper.java.command=java
   - wrapper.app.parameter.2=../conf/SCARVESconfig.xml
3. 파일을 저장합니다.

SCARVES 구성

스마트 카드 구성 요소를 추출한 후 템플릿 구성 파일을 업데이트합니다. *SCARVESconfigtemplate.xml* 파일은 키 저장소 위치, 각 SCARVES 데몬의 설명, SCARVES 에 OCSP 또는 CRL 이 사용되는지 여부 등의 세부 정보를 정의하는 템플릿으로 사용됩니다.

중요! SCARVES 구성 설정을 성공적으로 적용하려면 *SCARVESconfigtemplate.xml* 템플릿을 *SCARVESconfig.xml* 로 변경해야 합니다.

일반 XML 형식은 다음과 같습니다.

```
<?xml version="1.0" encoding="UTF-8"?>
<SmartCardService>
    ... Service Parameters ...
    ... One or more Daemon descriptions ...
</SmartCardService>
```

다음 단계를 따르십시오.

1. *<SCARVES_HOME>/conf* 로 이동하고 *SCARVESconfigtemplate.xml* 을 엽니다.
2. XML 편집 도구를 사용하여 일반 SCARVES 설정을 구성합니다.
   - SCARVES 서비스 매개 변수 구성 (페이지 205)
   - SCARVES 데몬 구성 (페이지 207)
   - LDAP 를 사용하도록 SCARVES 구성 (페이지 209)

또한 스마트 카드 확인 프로토콜을 지정합니다.

- (선택 사항) OCSP 를 사용하도록 SCARVES 구성 (페이지 214)
- (선택 사항) CRL 을 사용하도록 SCARVES 구성 (페이지 212)

참고: 사용자 환경에 오직 하나의 프로토콜만 사용할 수 있습니다.

3. 파일을 *SCARVESconfig.xml* 로 저장합니다.
4. SCARVES 서비스를 시작합니다. 자세한 내용은 SCARVES 시작 및 중지 (페이지 217)를 참조하십시오.

SCARVES 서비스 매개 변수 구성

SCARVES 서비스 매개 변수는 키 저장소 위치와 암호 정보를 지정합니다.

일반 XML 형식은 다음과 같습니다.

```
<SmartCardService>
    <trust-keystore>filename of keystore</trust-keystore>
    <trust-keystore-pass>encrypted password of keystore</trust-keystore-pass>
    <jvm-arg>-mx1024m</jvm-arg> <!-- optional, param for all Daemon JVMs -->
    ... One or more Daemon descriptions ...
</SmartCardService>
```

다음 매개 변수를 구성할 수 있습니다.

<trust-keystore>

모든 데몬의 trust 키 저장소를 지정합니다. 파일은 모든 스마트 카드를 허용하도록 모든 루트 및 중간 인증서를 포함해야 합니다. 이 매개 변수는 다음 매개 변수와 함께 모든 데몬에 전달됩니다.

-Djavax.net.ssl.trustStore=filename JVM

참고: 모든 데몬은 동일한 trust 키 저장소를 사용합니다.

<trust-keystore-pass>

trust 키 저장소의 암호를 지정합니다. 이 암호는 XML 파일에 암호화되어야 합니다. 암호는 다음 매개 변수를 포함하여 모든 데몬에 일반 텍스트로 전달됩니다.

```
-Djavax.net.ssl.trustStorePassword=password
```

<debug>

디버그 기록 수준을 설정하며, 사용할 수 있는 값은 다음과 같습니다.

- 0 - 디버깅이 없음을 지정하며, 이것이 기본값입니다.
- 1 - 디버깅의 최하위 수준 정보를 지정합니다.
- 2 - 디버깅의 표준 중간 수준을 지정합니다.
- 3 - 디버깅의 최상위 수준 정보를 지정합니다.

<jvm-arg>

모든 데몬 JVM 의 매개 변수를 지정합니다. 이 매개 변수는 사용할 수 있는 메모리 크기를 조정합니다.

구성 설정을 적용하는 방법에 대한 자세한 내용은 SCARVES 구성 (페이지 204)을 참조하십시오.

SCARVES 데몬 구성

SCARVES 데몬 매개 변수는 CRL 이나 OCSP, 그리고 LDAP 정보를 사용하는지 여부를 지정합니다. CRL 과 OCSP 가 함께 존재할 수는 있지만 둘 중 하나만 사용하도록 설정될 수 있으므로 하나는 주석 처리해야 합니다.

일반 XML 형식은 다음과 같습니다.

```
<SmartCardService>
    ... Service Parameters ...
    <Daemon name="name" port="port number">
        <keystore>...filename of keystore...</keystore>
        <keystore-pass>...encrypted password of keystore...</keystore-pass>
        <jvm-arg>-mx1024m</jvm-arg> <!-- optional, param for this Daemon JVM -->
        ... Protocol Description...
        ... LDAP Description...
    </Daemon>
    ... more Daemon descriptions ...
</SmartCardService>
```

다음 매개 변수를 구성할 수 있습니다.

이름

각 데몬 이름에 대해 고유 이름을 지정합니다. 이는 내부적으로 추적하는 데 사용되며, 로그 파일에서 해당 오류와 디버깅 코드 앞에 옵니다.

port

데몬이 수신 대기하는 TCP 포트를 지정합니다.

<keystore>

데몬이 SSL 통신에 사용하는 인증서가 포함된 키 저장소 파일을 지정합니다.

<keystore-pass>

키 저장소의 암호를 지정합니다. 이 암호는 XML 파일에 암호화되어야 합니다.

<jvm-arg>

모든 데몬 JVM 의 매개 변수를 지정합니다. 이 매개 변수는 이 섹션에 지정된 *각* 데몬에 사용할 수 있는 메모리 크기를 조정합니다. 이는 *일부* 데몬에 전송되지 않으므로 기본 SCARVES 서비스 매개 변수 섹션의 <jvm-arg> 태그와 다릅니다.

구성 설정을 적용하는 방법에 대한 자세한 내용은 SCARVES 구성 (페이지 204)을 참조하십시오.

LDAP 를 사용하도록 SCARVES 구성

데몬이 LDAP 를 사용하는 경우 이 인증 메서드에 대한 세부 정보를 지정하는 매개 변수를 정의해야 합니다.

일반 XML 형식은 다음과 같습니다.

```
<SmartCardService>
    ... Service Parameters ...
    <Daemon ...parameters...>
        ... More daemon parameters...
        ... Protocol Description...
        CA LDAP Server for z/OS
            <ldap-enabled>true</ldap-enabled>
            <ldap-hostname>renge01-winvm</ldap-hostname>
            <ldap-port>24132</ldap-port>
            <ldap-ssl>false</ldap-ssl>
            <ldap-user-dn>uid=GGantt,ou=people,dc=ca,dc=com</ldap-user-dn>

<ldap-user-pass>05V2irWBg8O39H6ANGic241UWooJuIbJiHE+ZqKPvUY=</ldap-user-pass>
            <ldap-base-dn>ou=people,dc=ca,dc=com</ldap-base-dn>
            <cert-uniqueid-field>subject</cert-uniqueid-field>
            <cert-uniqueid-regex>CN=\w*\.\w*\.(\d+),</cert-uniqueid-regex>

<ldap-uniqueid-search-field>facsimileTelephoneNumber</ldap-uniqueid-search-field>
            <ldap-cache-lifetime>300</ldap-cache-lifetime>
        </ldap>
    </Daemon>
    ... more Daemon descriptions ...
</SmartCardService>
<ldap-enabled>
```

다음 매개 변수를 구성할 수 있습니다.

<ldap-enabled>

LDAP 를 사용 또는 사용하지 않도록 설정하는지를 지정합니다. 사용할 수 있는 값은 다음과 같습니다.

- *True* 는 데몬에 LDAP 를 사용하도록 설정합니다.
- *False* 는 데몬에 LDAP 를 사용하지 않도록 설정합니다. 이 값을 false 로 설정하면 구성 파일을 CA LDAP Server for z/OS 섹션에 사용하여, 사용되지 않은 설정을 저장할 수 있습니다.

<ldap-hostname>

LDAP 서버의 호스트 이름을 지정합니다.

<ldap-port>

LDAP 서버의 포트를 지정합니다.

<ldap-ssl>

값을 *true* 로 설정하면 SSL 을 사용하는 LDAP 서버를 지정합니다. 이 기능을 사용하도록 설정하면 LDAP 서버 인증서가 trust 키 저장소에 있는지 확인합니다.

<ldap-user-dn>

LDAP 서버로 로그인하는 데 데몬이 사용하는 고유 이름을 지정합니다. 서버는 이 고유 이름에 검색 권한을 부여해야 합니다.

<ldap-user-pass>

LDAP 서버로 로그인하는 데 데몬이 사용하는 암호를 지정하며, 암호는 XML 파일에 암호화되어야 합니다.

<ldap-base-dn>

LDAP 검색의 시작 지점 역할을 수행하는 기반 고유 이름을 지정합니다. 검색할 모든 고유 이름은 기반 고유 이름 아래에 나타나야 합니다.

<cert-uniqueid-field>

EDIPI(Electronic Data Interchange Personal Identifier) 또는 다른 고유 ID 가 포함된 인증서 필드를 지정합니다. 유효한 값은 *subject*, *subuid*, *an_other* 및 *an_rfc822* 입니다.

<cert-uniqueid-regex>

지정된 필드에서 고유 ID 를 추출하는 방법을 세부적으로 나타내는 정규식을 지정합니다.

<ldap-uniqueid-search-field>

EDIPI 또는 다른 고유 ID 가 포함된 LDAP 입력 필드를 지정합니다.

<ldap-cache-lifetime>

캐시된 LDAP 조회가 유효한 최대 기간(초)을 지정합니다.

기본값인 *zero* 가 설정되면 LDAP 조회가 캐시되지 않습니다.

LDAP 항목이 변경되면 캐시의 시간이 초과될 때까지 캐시된 항목은 잘못된 값을 반환하므로 이 값을 너무 높게 설정해서는 안 됩니다.

Encryption

XML 파일에 저장된 암호는 반드시 암호화되어야 함을 지정합니다. 암호화 알고리즘은 서비스 중인 키와 일반 텍스트가 없는 데몬 코드를 포함하는 AES(Advanced Encryption Standard)입니다. 암호화된 암호는 XML 파일에 저장할 수 있는 인쇄 가능한 문자열을 생성할 수 있도록 Base64 유형으로 인코딩되어 있습니다.

구성 설정을 적용하는 방법에 대한 자세한 내용은 SCARVES 구성 (페이지 204)을 참조하십시오.

(선택 사항) CRL 을 사용하도록 SCARVES 구성

CRL 매개 변수는 파일 저장소 정보를 지정하며, 오직 한 번에 CRL 하나만 구성될 수 있습니다.

중요! CRL 을 사용하도록 *SCARVESconfig.xml* 을 구성하면 *<ocsp-enabled>* 매개 변수의 OCSP 값을 *false* 로 설정해야 단일 데몬에서 오류 없이 SCARVES 를 시작할 수 있습니다.

일반 XML 형식은 다음과 같습니다.

```
<SmartCardService>
    ... Service Parameters ...
    <Daemon ...parameters...>
        ... More daemon parameters...
        <crl>
            <crl-enabled>true</crl-enabled>
            <crl-dp>false</crl-dp>
            <crl-url>...URL containing CRL files...</crl-url>
            <crl-dir>...dirname containing CRL files...</crl-dir>
            <crl-poll-int>30</crl-poll-int>
        </crl>
        ... LDAP Description...
    </Daemon>
    ... more Daemon descriptions ...
</SmartCardService>
```

다음 매개 변수를 구성할 수 있습니다.

<crl-enabled>

값을 *true* 로 설정하여 CRL 파일을 사용하도록 데몬을 지정합니다. 이 값을 *false* 로 설정하면 데몬에서 OCSP 를 사용할 수 있습니다.

<crl-dp>

CRL 파일을 다운로드하는 배포 지점을 지정합니다.

<crl-url>

CRL 파일을 포함하는 URL 을 지정합니다.

<crl-dir>

CRL 파일을 포함하는 디렉터리 이름을 지정합니다.

<crl-poll-int>

새롭거나 변경된 CRL 파일에 대해 CRL 디렉터리 또는 CRL URL 을 스캔하는 빈도(초)를 지정합니다. 스캔된 인증서는 캐시됩니다. 이 매개 변수가 지정되지 않으면 기본 간격은 60 초가 됩니다.

구성 설정을 적용하는 방법에 대한 자세한 내용은 SCARVES 구성 (페이지 204)을 참조하십시오.

(선택 사항) OCSP 를 사용하도록 SCARVES 구성

OCSP 매개 변수는 스마트 카드 유효성 검사에 OCSP 를 사용하는 데 필요한 정보를 지정합니다. 이 프로토콜을 사용하는 경우 구성 파일에서 CRL 프로토콜 옵션을 주석 처리해야 합니다.

중요! OCSP 를 사용하도록 *SCARVESconfig.xml* 을 구성하면 *<crl-enabled>* 매개 변수의 CRL 값을 *false* 로 구성해야 단일 데몬에서 오류 없이 SCARVES 를 시작할 수 있습니다.

일반 XML 형식은 다음과 같습니다.

```
<SmartCardService>
    ... Service Parameters ...
    <Daemon ...parameters...>
        ... More daemon parameters...
        <ocsp>
            <ocsp-enabled>true</ocsp-enabled>
            <ocsp-aia>false</ocsp-aia>
            <ocsp-cert-alias>ocsp_qacle3</ocsp-cert-alias>
            <ocsp-url>http://qacle3:3501/responder</ocsp-url>
        </ocsp>
        ... LDAP Description...
    </Daemon>
    ... more Daemon descriptions ...
</SmartCardService>
```

다음 매개 변수를 구성할 수 있습니다.

<ocsp-enabled>

이 값이 *true* 로 설정되면 OCSP 를 사용하는 데몬이 지정됩니다.

<ocsp-aia>

스마트 카드 인증이 구현된 경우 이 값이 *true* 로 설정되면 이 값은 AIA(Authority Info Access)를 지정합니다.

<ocsp-cert-alias>

OCSP 응답자가 응답을 서명하는 데 사용하는 인증서의 별칭을 지정합니다. 이 기능을 사용하도록 설정하면 OCSP 서버 인증서가 trust 키 저장소에 있는지 확인합니다.

<ocsp-url>

OCSP 응답자의 URL 을 지정합니다.

구성 설정을 적용하는 방법에 대한 자세한 내용은 SCARVES 구성 (페이지 204)을 참조하십시오.

샘플 SCARVES 구성 파일

다음 코드 샘플은 *SCARVESconfig.xml* 구성 파일의 일부를 나타냅니다. CRL 및 LDAP 서버를 사용하여 스마트 카드를 확인하는 두 데몬을 정의합니다.

두 옵션이 모두 XML 에 구성될 수 있지만 구성 속성은 OCSP 또는 CRL 중 하나에만 사용하도록 설정되어야 합니다.

```
<?xml version="1.0" encoding="UTF-8"?>

<SmartCardService>
<trust-keystore>../keystores/daemontrust</trust-keystore>
<trust-keystore-pass>YEDZLwyEVTnCfzS+rYTfC41UWooJuIbJiHE+ZqKPvUY=</trust-keystore
-pass>
<debug>0</debug>

<jvm-arg>-mx1024m</jvm-arg>

<Daemon name="daemon-crl-1" port="9999">
   <keystore>../keystores/daemoncert</keystore>
   <keystore-pass>YEDZLwyEVTnCfzS+rYTfC41UWooJuIbJiHE+ZqKPvUY=</keystore-pass>

   <crl>
    <crl-enabled>true</crl-enabled>
    <crl-dp>false</crl-dp>
    <crl-url />
    <crl-dir>../crls/daemon-crl</crl-dir>
    <crl-poll-int>600</crl-poll-int>
   </crl>
```

```
    <ldap>
      <ldap-enabled>true</ldap-enabled>
      <ldap-hostname>host1</ldap-hostname>
      <ldap-port>24000</ldap-port>
      <ldap-ssl>false</ldap-ssl>
      <ldap-base-dn>ou=people,dc=abc,dc=com</ldap-base-dn>
      <ldap-user-dn>uid=JDoe,ou=people,dc=abc,dc=com</ldap-user-dn>
      <ldap-user-pass>05V2irWZg8O39L6ANGic241UWi0JuIbJiHE+ZqKPvUY=</ldap-user-pass>
      <cert-uniqueid-field>subject</cert-uniqueid-field>
      <cert-uniqueid-regex>CN=\w*\.\w*\.(\d+),</cert-uniqueid-regex>

<ldap-uniqueid-search-field>facsimileTelephoneNumber</ldap-uniqueid-search-field>
    </ldap>
</Daemon>

<Daemon name="daemon-ocsp-1" port="9998">
    <keystore>../keystores/daemoncert</keystore>
    <keystore-pass>YEDZLwyEVTnCfzS+rYTfC41UWooJuIbJiHE+ZqKPvUY=</keystore-pass>

    <ocsp>
      <ocsp-enabled>true</ocsp-enabled>
      <ocsp-aia>false</ocsp-aia>

      <ocsp-cert-alias>ocsp_qacle3</ocsp-cert-alias>

      <ocsp-url>http://qacle3:3501/responder</ocsp-url>
    </ocsp>
    <ldap>
      <ldap-enabled>true</ldap-enabled>
      <ldap-hostname>host1</ldap-hostname>
      <ldap-port>24001</ldap-port>
      <ldap-ssl>false</ldap-ssl>
      <ldap-base-dn>ou=people,dc=abc,dc=com</ldap-base-dn>
      <ldap-user-dn>uid=JDoe,ou=people,dc=abc,dc=com</ldap-user-dn>
      <ldap-user-pass>05V2irWBg8O39H6ANGic377UWooJuIbJiHE+ZqKPvUY=</ldap-user-pass>
      <cert-uniqueid-field>subject</cert-uniqueid-field>
      <cert-uniqueid-regex>CN=\w*\.\w*\.(\d+),</cert-uniqueid-regex>

<ldap-uniqueid-search-field>facsimileTelephoneNumber</ldap-uniqueid-search-field>
      <ldap-cache-lifetime>300</ldap-cache-lifetime>
    </ldap>
</Daemon>

</SmartCardService>
```

SCARVES 시작 및 중지

SCARVES 는 *SCARVESconfig.xml* 구성 파일을 읽어 데몬을 제어하고 지정된 각 포트에 대해 데몬 프로그램을 시작하는 Java 프로그램입니다. SCARVES 는 다음 중 하나가 발생하는 경우 데몬을 중지하고 새 데몬을 시작합니다.

- 데몬의 충돌
- 데몬이 통신에 대해 응답하지 못하는 경우
- 데몬이 XML ping 에 응답하지 않는 경우

다음 단계를 따르십시오.

- CA APM 서버에 루트로 로그인하고 명령 프롬프트에 액세스합니다.

  Windows 의 경우

  - SCARVES 를 시작하는 시작 배치 파일을 실행합니다.
    `<SCARVES_HOME>\bin\StartSCARVES-NT.bat`
  - SCARVES 를 중지하는 중지 배치 파일을 실행합니다.
    `<SCARVES_HOME>\bin\StopSCARVES-NT.bat`

  Linux 의 경우

  - SCARVES 를 시작하는 start 스크립트를 실행합니다.
    `/etc/init.d/SCARVES start`
  - SCARVES 를 중지하는 stop 스크립트를 실행합니다.
    `/etc/init.d/SCARVES stop`
  - SCARVES 를 다시 시작하는 restart 스크립트를 실행합니다.
    `/etc/init.d/SCARVES restart`

  Unix 의 경우

  - SCARVES 를 시작하는 start 명령을 입력합니다.
    `<SCARVES_HOME>/bin/scarves start`
  - SCARVES 를 중지하는 stop 명령을 입력합니다.
    `<SCARVES_HOME>/bin/scarves stop`
  - SCARVES 상태를 가져오는 status 명령을 실행합니다.
    `<SCARVES_HOME>/bin/scarves status`

스마트 카드 설치 확인

스마트 카드 인증을 설정한 후 인증 메서드가 성공적으로 설치되었으며 사용하도록 설정되었는지 확인합니다.

다음 단계를 따르십시오.

1. 스마트 카드 인증에 대해 CA APM 을 설정한 후 WebView, Web Start 또는 CEM 콘솔을 시작합니다.

   페이지에는 사용자 ID 와 PIN(개인 식별 번호)을 묻는 메시지가 표시됩니다.

2. PIN 을 입력합니다.
3. 초기화 메시지가 *<SCARVES_HOME>\logs* 디렉터리에 위치한 로그 파일에 기록되었는지를 확인합니다.

CA APM 스마트 카드 인증의 문제 해결

문제 해결 정보는 스마트 카드 인증에 발생한 문제 및 오류 메시지를 해결하는 데 유용합니다.

다음 섹션을 참조하면 도움이 됩니다.

SCARVES 의 시작 실패

Windows, Unix 및 Linux 의 경우

증상:

스마트 카드 인증을 사용하여 인증하려는 경우 SCARVES 는 시작하지 못하고 다음 오류 메시지가 표시됩니다.

```
[ERROR] [btpool0-2] [Manager.SCAuth]
com.wily.introscope.spec.server.user.SCException: Error getting user from given
certificate. java.net.ConnectException: Connection refused: connect
```

해결책:

SCARVES 가 시작하지 못하고 오류 메시지가 반환되면 문제를 확인하여 해결할 수 있습니다.

SCARVES 시작 문제를 해결하려면

1. *<SCARVES_HOME>\logs* 에 위치한 *scarve.log* 파일을 엽니다.
2. *Configure in DEBUG mode* 오류 메시지가 기록되면 SCARVES 는 제대로 시작되지 않습니다. 다음을 수행하여 문제를 해결할 수 있습니다.
   - *wrapper.conf* 파일에 제공된 JVM 인수가 유효한지 확인합니다. 예:
     ```
     wrapper.java.command=C:/Progra~1/Java/jdk1.6.0_20/bin/java
     ```
   - 포트 바인딩 오류가 *scarve.log* 파일에 기록되었는지 확인합니다. 오류가 나타나면 다음 명령을 입력하여 데몬 포트 번호를 사용할 수 있는지를 확인합니다.
     ```
     netstat –ao | find <port-no>
     ```
     이 포트 번호를 사용 중인 경우 데몬의 포트 번호는 고유해야 하므로 새 포트 번호를 할당해야 합니다.
   - *SCARVESconfigtemplate.xml* 의 속성 집합 형식이 올바로 지정되었는지 확인합니다.
   - *<SCARVES_HOME>/keystores* 에 위치한 키 저장소 파일을 사용할 수 있는지 확인합니다.

3. *Configure in DEBUG mode* 오류 메시지가 기록되지 않았으면 SCARVES 를 다시 설치합니다.

   참고: SCARVES 를 제거하고 다시 설치하면 *config* 및 *keystores* 하위 디렉터리의 파일이 유지됩니다.

4. SCARVES 를 다시 시작합니다.

   스마트 카드를 사용하여 인증할 수 있습니다.

OCSP 의 유효성 검사 실패

Windows, Unix 및 Linux 의 경우

증상:

웹 브라우저를 사용하여 유효한 인증서를 선택한 경우 OCSP 유효성 검사가 실패하고 다음 오류 메시지가 나타납니다.

```
[ERROR] [btpool0-0] [Manager.SCAuth]
com.wily.introscope.spec.server.user.SCException: Problem contacting OCSP Server
```

해결책:

OCSP 서버를 다시 시작하여 OCSP 서버를 액세스할 수 있는지 확인합니다.

OCSP 를 다시 시작하려면

1. *services.msc* 에서 OCSP 를 다시 시작합니다.
2. 브라우저를 열고 유효한 인증서를 선택합니다.

   OCSP 유효성 검사가 성공합니다.

CRL 의 유효성 검사 실패

Windows, Unix 및 Linux 의 경우

증상:

환경에 구성된 CRL 에 대해 스마트 카드를 사용하여 인증하려는 경우 실패합니다.

해결책:

CRL 을 사용하여 유효성을 검사하는 데 문제가 있으면 문제를 확인하여 해결할 수 있습니다.

SCARVES 시작 문제를 해결하려면

1. *<SCARVES_HOME>\logs* 에 위치한 *scarve.log* 파일을 엽니다.
2. CRL 만료 날짜 정보가 있으면 CRL 파일은 만료됩니다.

   참고: CRL 파일은 주 단위로 만료됩니다.
3. 최신 CRL 파일을 다운로드합니다.

   CRL 유효성 검사가 성공합니다.

OCSP 서버가 응답하지 않음

Windows, Unix 및 Linux 의 경우

증상:

스마트 카드 인증의 OCSP 옵션을 사용하려는 경우 OCSP 서버가 실패하고 다음 메시지가 나타납니다.

```
[ERROR] [btpool0-0] [Manager.SCAuth]
com.wily.introscope.spec.server.user.SCException:
```

해결책:

이 메시지는 OCSP 서버가 시작하지 못했기 때문에 나타나며 문제를 확인하여 해결할 수 있습니다.

OCSP 서버의 문제를 해결하려면

- *services.msc* 에서 OCSP 서버를 다시 시작하여 응답자가 멈추지 않았는지 확인합니다.
- SCARVES 및 OCSP 간의 시간 및 날짜는 동일한지 확인합니다. 이 둘의 시간과 날짜가 다르면 오류 메시지가 나타납니다.

LDAP 서버가 응답하지 않음

Windows, Unix 및 Linux 의 경우

증상:

스마트 카드 인증을 사용하려는 경우 LDAP 서버는 시작하지 못하고 다음 오류 메시지가 나타납니다.

```
[ERROR] [btpool0-2] [Manager.SCAuth]
com.wily.introscope.spec.server.user.SCException: LDAP Server not responding
```

해결책:

LDAP 서버가 시작하지 못하면 *SCARVESconfig.xml* 파일에 지정된 LDAP 인스턴스를 액세스하지 못할 수 있습니다.

LDAP 서버의 문제를 해결하려면

- 적용할 수 있는 값으로 LDAP 구성이 설정되어 있는지 확인합니다.
- LDAP 서버를 사용할 수 있는지 확인합니다.
- LDAP 서버가 시작되어 실행되고 있는지 확인합니다.

수신한 CRL 오류

Windows, Unix 및 Linux 의 경우

증상:

스마트 카드 인증에 CRL 옵션을 사용하려는 경우 *<SCARVES_HOME>/logs* 디렉터리에 위치한 *scarve.log* 파일에 다음 오류 메시지가 나타납니다.

```
[ERROR] [btpool0-12] [Manager.SCAuth]
com.wily.introscope.spec.server.user.SCException: Certificate is expired or revoked
or not able to validate.
```

참고: 잘못된 CRL 파일의 세부 정보는 Enterprise Manager 로그 파일에 기록되지 않습니다.

해결책:

CRL 을 사용하도록 구성된 환경에서 스마트 카드로 성공적으로 인증하지 못하면 문제를 해결하십시오.

CRL 의 문제를 해결하려면

- *SCARVESconfig.xml* 파일이 *<SCARVES_HOME>/crls* 디렉터리에 나타난 폴더를 지정하는지 확인합니다. 지정하지 않는 경우 다음을 수행하십시오.
  1. *<SCARVES_HOME>/conf* 로 이동하고 *SCARVESconfig.xml* 을 엽니다.
  2. 지정한 <daemon-name>의 이름을 복사합니다.
  3. *<SCARVES_HOME>/crls* 디렉터리로 이동하고 동일한 <daemon-name>으로 폴더를 만듭니다.
  4. 이 디렉터리로 CRL 파일을 복사하고 SCARVES 를 다시 시작합니다.
- CRL 데몬에 지정된 절대 경로가 올바른지 확인합니다.
  1. *<SCARVES_HOME>/conf* 로 이동하고 *SCARVESconfig.xml* 을 엽니다.
  2. CRL 위치에 지정된 경로가 올바른지 확인합니다.
  3. 이는 CRL 파일을 포함하는 CRL 폴더를 SCARVES 가 추적할 수 있는지 확인합니다.

Received user not in LDAP error

Windows, Unix 및 Linux 의 경우

증상:

스마트 카드 인증을 사용하려는 경우 다음 오류 메시지가 *<EM_HOME>/logs/IntroscopeEnterpriseManager.log* 파일에 나타납니다.

```
Received user not in LDAP error
```

해결책:

이는 사용자 디렉터리에 LDAP 가 사용자 정보와 함께 정의되지 않은 경우에 발생합니다. LDAP 사용자 디렉터리를 추가하여 문제를 해결할 수 있습니다.

LDAP 사용자 디렉터리를 추가하려면

1. <SCARVES_HOME>/conf 로 이동하고 *SCARVESconfig.xml* 을 엽니다.
2. 다음 특성을 정의합니다.

   facismilenumber

   사용된 인증서의 EDIPI 번호를 입력합니다.

   uid

   Enterprise Manager 에 나타난 사용자 이름으로 특성을 입력하고 자격 증명에 로그인합니다.
3. SCARVES 를 다시 시작합니다.

연결 거부 수신 오류

Windows, Unix 및 Linux 의 경우

증상:

스마트 카드 인증을 사용하려는 경우 다음 오류 메시지가 나타납니다.

```
[ERROR] [btpool0-2] [Manager.SCAuth]
com.wily.introscope.spec.server.user.SCException: Error getting user from given
certificate. java.net.ConnectException: Connection refused: connect
```

이 Enterprise Manager 오류는 정의된 SCARVES 인스턴스가 시작되지 않거나 액세스할 수 없는 경우에 기록됩니다.

해결책:

- *<SCARVES_HOME>/conf* 로 이동하고 *SCARVESconfig.xml* 을 연 다음 SCARVES 호스트 이름이 올바른지 확인합니다.

구성되지 않은 LDAP 수신 오류

Windows, Unix 및 Linux 의 경우

증상:

스마트 카드 인증을 사용하려는 경우 다음 오류 메시지가 Enterprise Manager 로그 파일에 나타납니다.

```
[ERROR] [btpool0-0] [Manager.SCAuth]
com.wily.introscope.spec.server.user.SCException: LDAP Not configured
```

이 Enterprise Manager 오류는 정의된 SCARVES 인스턴스가 시작되지 않거나 액세스할 수 없는 경우에 기록됩니다.

해결책:

- *<SCARVES_HOME>/conf* 로 이동하고 *SCARVESconfig.xml* 을 연 다음 파일의 LDAP 콘텐츠가 나타나고 정확한지 확인합니다.

Enterprise Manager 에 발생한 핸드셰이크 예외

Windows, Unix 및 Linux 의 경우

증상:

스마트 카드 인증을 사용하려는 경우 핸드셰이크 예외가 나타납니다.

해결책:

핸드셰이크 예외가 발생하는 경우 문제를 확인하여 해결할 수 있습니다.

핸드셰이크 예외 문제를 해결하려면

1. *<SCARVES_HOME>/conf* 로 이동하고 *SCARVESconfigtemplate.xml* 을 엽니다.
2. *SCARVESconfigtemplate.xml* 에 정의된 키 저장소 특성이 정확한지 확인합니다.
3. SCARVES 에서 자체 서명된 유효한 인증서를 속성 파일에 정의된 키 저장소로 가져왔는지 확인합니다.
4. *<EM_HOME>\config* 의 키 저장소 특성이 정확한지 확인하고 자체 서명된 인증서가 *<SCARVES_HOME>/keystores/daemoncert* 디렉터리에 위치하는지 확인합니다. 자체 서명된 인증서가 없는 경우 Enterprise Manager 키 저장소로 인증서를 내보냅니다.

인증서에 대한 자세한 내용은 다음을 참조하십시오.

인증서 로드 (페이지 198)
인증서 명령 (페이지 199)