HP Universal CMDB Configuration Manager

Windows 및 Linux 운영 체제용

소프트웨어 버전: 9.20

배포 안내서

문서 릴리스 날짜: 2011년 6월
소프트웨어 릴리스 날짜: 2011년 6월

법적 고지

보증

HP 제품 및 서비스에 대한 모든 보증 사항은 해당 제품 및 서비스와 함께 제공된 익스프레스 보증서에 규정되어 있습니다. 여기에 수록된 어떤 내용도 추가 보증을 구성하는 것으로 해석될 수 없습니다. HP는 여기에 수록된 기술적 또는 편집상의 오류나 누락에 대해 책임지지 않습니다.

본 정보는 예고 없이 변경될 수 있습니다.

제한된 권리 범례

기밀 컴퓨터 소프트웨어. 소유, 사용 또는 복사하기 위해서는 HP로부터 유효한 라이센스를 확보해야 합니다. FAR 12.211 및 12.212에 의거하여 상용 컴퓨터 소프트웨어, 컴퓨터 소프트웨어 문서 및 상용 품목에 대한 기술 데이터는 공급업체의 표준 상용 라이센스 아래에서 미국 정부에 사용이 허가되었습니다.

저작권 고지

문서 업데이트

이 문서의 제목 페이지에는 다음과 같은 식별 정보가 있습니다.

- 문서가 업데이트될 때마다 변경되는 문서 릴리스 날짜
- 이 소프트웨어 버전의 릴리스 날짜를 나타내는 소프트웨어 릴리스 날짜

최근 업데이트를 확인하거나 문서의 최신 버전을 사용하고 있는지 확인하려면 다음 사이트로 이동합니다.

http://h20230.www2.hp.com/selfsolve/manuals

이 사이트를 사용하려면 HP Passport 사용자로 등록하여 로그인해야 합니다. HP Passport ID를 등록하려면 다음 웹 사이트를 방문하십시오.

http://h20229.www2.hp.com/passport-registration.html

아니면 HP Passport 로그인 페이지에서 **New users - please register** 링크를 클릭합니다.

적절한 제품 지원 서비스에 가입할 경우 업데이트 버전이나 새 버전도 제공됩니다. 자세한 내용은 HP 판매 담당자에게 문의하십시오.

지원

다음 HP 소프트웨어 지원 웹사이트를 방문하십시오.

http://www.hp.com/go/hpsoftwaresupport

이 웹 사이트에서는 연락처 정보를 비롯하여 HP 소프트웨어에서 제공하는 제품, 서비스 및 지원에 대한 자세한 내용을 확인할 수 있습니다.

온라인 지원을 통해 사용자가 스스로 문제를 해결할 수 있습니다. 또한 업무 관리에 필요한 대화식 기술 지원 도구에 신속하고 효율적으로 액세스할 수 있습니다. 소중한 지원 고객으로서 지원 웹사이트를 통해 다음과 같은 혜택을 누릴 수 있습니다.

- 관심 있는 지식 문서를 검색할 수 있습니다.
- 지원 사례 및 개선 요청을 제출하고 추적할 수 있습니다.
- 소프트웨어 패치를 다운로드할 수 있습니다.
- 지원 계약을 관리할 수 있습니다.
- HP 지원 연락처를 조회할 수 있습니다.
- 사용 가능한 서비스에 대한 정보를 검토할 수 있습니다.
- 다른 소프트웨어 고객과의 토론에 참여할 수 있습니다.
- 소프트웨어 교육을 조사하고 등록할 수 있습니다.

대부분의 지원 영역을 이용하려면 HP Passport 사용자로 등록하여 로그인해야 합니다. 이 영역에서는 지원 계약이 필요할 수도 있습니다. HP Passport ID를 등록하려면 다음 웹 사이트를 방문하십시오.

http://h20229.www2.hp.com/passport-registration.html

액세스 수준에 대한 자세한 내용을 보려면 다음 웹 사이트를 방문하십시오.

http://h20230.www2.hp.com/new_access_levels.jsp

목차

파트 I: 설치 및 구성

파트 I

설치 및 구성

1

개요

이 장의 내용은 다음과 같습니다.

구성 요소

HP Universal CMDB Configuration Manager는 다음 여러 구성 요소의 연결 릴리스입니다.

➤ **HP Universal CMDB Foundation**

HP Universal CMDB Foundation(UCMDB Foundation)은 엔터프라이즈 IT 조직이 비즈니스 서비스 정의 및 연관된 인프라 관계를 문서화, 저장 및 관리하기 위한 CMDB(구성 관리 데이터베이스)입니다.

UCMDB Foundation은 데이터 모델, 데이터 흐름 관리 및 데이터 모델링 기능을 구현할 뿐만 아니라, CMDB 데이터를 중요한 질문에 대답하고 비즈니스 문제를 해결하는 데 도움되는 알기 쉽고 실행 가능한 정보로 변환하기 위해 영향 분석, 변경 추적 및 보고 기능을 제공합니다.

➤ **HP Universal CMDB Configuration Manager**

HP Universal CMDB Configuration Manager(Configuration Manager)는 새로운 정책 기반의 토폴로지 및 인벤토리 구성 관리를 도입합니다. 이는 구성 관리자 및 구성 소유자를 위해 특별히 마련된 것으로, 이러한 사용자가 UCMDB에서 사용할 수 있는 CI 데이터 및 토폴로지 컨텐츠 뿐만 아니라 분석을 수행할 수 있습니다. Configuration Manager는 구성 관리자 및 소유자에게 토폴로지 및 인벤토리 구성 정책을 쉽게 설정하고 조직 표준 준수 수준을 자동으로 결정하기 위해 필요한 도구를 제공합니다.

Configuration Manager는 추가 Tomcat 기반 서버로 배포되고 광범위한 UCMDB SDK를 사용하여 UCMDB 서버와 통신합니다.

➤ **HP Discovery and Dependency Mapping Advanced Edition**

지속적으로 업데이트되는 풍부한 컨텐츠가 포함된 HP DDMA(Discovery and Dependency Mapping Advanced Edition) 소프트웨어는 IT 인프라 데이터를 획득 및 유지하기 위한 UCMDB 기본 방법입니다.

➤ **HP Operations Orchestration**

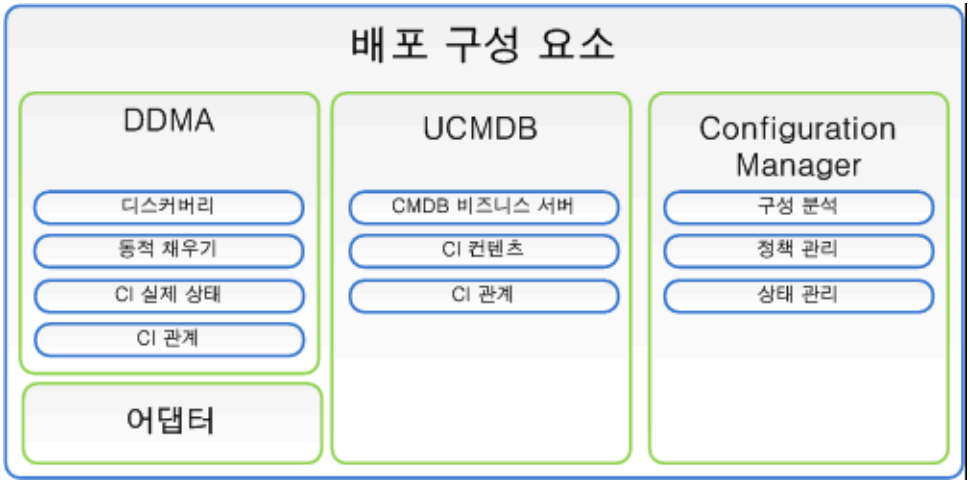
HP Operations Orchestration(OO)은 흐름도 작성 및 배포 도구입니다. OO Studio의 직관적인 drag-and-wire 기능을 사용하면 프로그래밍 기술이 거의 없는 사용자도 흐름도를 설계, 작성, 공유 및 사용자 지정할 수 있습니다. OO Studio는 버전 제어 기능을 통해 여러 작성자 간의 공동 작업을 지원합니다. 강력한 내장형 디버거는 안정적이고 신뢰할 수 있는 실행을 위해 여러 환경에서의 흐름 테스트를 허용하고 컨텐츠 개발을 가속화하며 흐름의 유효성 검사를 사용합니다.

또한 OO Studio는 사용자가 흐름을 쉽게 배포할 수 있게 합니다. OO Studio를 사용하여 사용자가 여러 환경(개발, 테스트, 스테이징 및 프로덕션)에서 흐름을 비교하고 촉진할 수 있습니다. Studio를 사용하여 준수 요건을 지원하기 위해 표준 프로세스를 문서화할 수 있고 구조화된 문서를 생성할 수 있습니다.

➤ **Configuration Manager-OO 통합**

Configuration Manager는 Configuration Manager 프레임워크 내에서 OO 흐름을 실행할 수 있는 기능을 제공합니다. OO 흐름을 실행하기 위한 다음 두 가지 주요 방법이 있습니다.

- ➤ **프로세스 통합** – 특정 CI를 특정 구성 정책에 맞춰 조정하는 외부 서비스 데스크 요청의 RFC를 열 수 있습니다.
- ➤ **정책 개선** – 구성 문제를 정정하는 OO 흐름을 트리거할 수 있습니다. 예를 들어, 가상 호스트 시스템에 추가 메모리를 할당할 수 있습니다.



사용자의 환경 식별

본 안내서는 다음과 같이 서로 다른 시작 지점에서 HP Universal CMDB Configuration Manager를 배포하는 프로세스에 대해 설명합니다.

Configuration Manager의 경우

➤ Configuration Manager 9.10 버전이 설치된 경우

Configuration Manager를 현재 버전으로 업그레이드하는 방법에 대한 자세한 내용은 37페이지의 "Configuration Manager 업그레이드"를 참조하십시오.

➤ Configuration Manager 버전이 설치되지 않은 경우

자세한 내용은 다음 중 하나를 참조하십시오.

➤ 17페이지의 "Windows 플랫폼에 HP Universal CMDB Configuration Manager 설치"

➤ 39페이지의 "Linux 플랫폼에 HP Universal CMDB Configuration Manager 설치"

UCMDB의 경우

➤ UCMDB의 9.03 이전 버전이 설치된 경우

다음을 수행합니다.

➤ UCMDB 9.03 버전으로 업그레이드합니다. 자세한 내용은 *HP Universal CMDB 배포 안내서* PDF를 참조하십시오. www.hp.com/go/hpsoftwaresupport에서 설명서를 다운로드할 수 있습니다.

➤ 누적 업데이트 팩 2를 설치합니다. Configuration Manager 설치 미디어에서 구하거나 www.hp.com/go/hpsoftwaresupport에서 다운로드할 수 있습니다.

엔터프라이즈 준비 구성에 대한 자세한 내용은 18페이지의 "데이터베이스 또는 사용자 스키마 구성"을 참조하십시오.

➤ UCMDB 9.03 버전이 설치된 경우

누적 업데이트 팩 2를 설치합니다. Configuration Manager 설치 미디어에서 구하거나 www.hp.com/go/hpsoftwaresupport에서 다운로드할 수 있습니다.

엔터프라이즈 준비 구성에 대한 자세한 내용은 18페이지의 "데이터베이스 또는 사용자 스키마 구성"을 참조하십시오.

➤ UCMDB 버전이 설치되지 않은 경우

다음 중 하나를 수행합니다.

➤ 배포 관리자(Windows 시스템 전용)를 사용하여 Configuration Manager를 설치할 때 동시에 UCMDB도 설치합니다. 자세한 내용은 17페이지의 "Windows 플랫폼에 HP Universal CMDB Configuration Manager 설치"를 참조하십시오.

➤ 39페이지의 "Linux 플랫폼에 HP Universal CMDB Configuration Manager 설치"의 지침을 따라 Linux 시스템에 Configuration Manager를 설치합니다.

일반 정보

본 안내서는 또한 사용자의 환경(예: 고가용성 배포)에 따라 특수한 UCMDB 배포도 고려하여 이러한 배포를 위한 배포 절차에 필요한 조정을 제공합니다.

참고: 동일한 서버에 UCMDB 및 Configuration Manager를 함께 설치할 수 있도록 지원됩니다. 프로덕션 환경에서는 확장 목적을 위해 이러한 구성 요소를 별도의 서버에 설치하는 것이 좋습니다.

Configuration Manager의 사용을 위해서는 UCMDB가 통합 스키마 모드에서 구성되어야 하고 새 UCMDB 상태(인증 상태)가 생성되어야 합니다. 이러한 구성은 양쪽 설치 사례(UCMDB의 설치가 이미 존재하는 경우 또는 배포 관리자에 의해 설치된 경우)에서 모두 배포 절차에 의해 자동으로 수행됩니다.

중요: 기존 UCMDB 설치를 참조하는데 그 스키마가 아직 통합되지 않은 경우, 너무 많이 채워진 데이터베이스(CI가 5백만 개 이상 포함된 데이터베이스)에서는 통합 단계에 시간이 오래 걸릴 수 있습니다(20 ~ 60분).

Configuration Manager만 배포하는 경우(즉, UCMDB의 기존 또는 업그레이드 설치를 사용하는 경우), Configuration Manager의 설치를 완료하기 위해서는 UCMDB 서버가 실행 중이어야 합니다.

매트릭스 지원

서버 시스템 요구 사항

CPU	쿼드코어 이상
메모리(RAM)	4GB 이상
플랫폼	x64
운영 체제	Windows(64비트) ➤ Windows 2003 Enterprise SP2 및 R2 SP2 ➤ Windows 2008 Enterprise SP2 및 R2 Linux ➤ Red Hat Enterprise Linux x86(64비트)
데이터베이스	➤ Microsoft SQL Server 2005 SP2; 2005 Compatibility Mode 80 (모두 Enterprise Edition) ➤ Microsoft SQL Server 2008 ➤ Oracle 10.2.x, 11.x
웹 서버	➤ Microsoft IIS 7 ➤ Apache 2

HP Universal CMDB	➤ HP Universal CMDB 버전 9.03, CUP 2 설치 (일반 CMDB 설치) 시스템 요구 사항의 전체 목록은 *HP Universal CMDB 배포 안내서* PDF를 참조하십시오. **참고:** ➤ HP Universal CMDB 서버를 Configuration Manager와 함께 배포하는 경우 Oracle의 Enterprise Edition과 Oracle Partitioning 옵션이 필요합니다. ➤ 이전에 Oracle의 Standard Edition에서 HP Universal CMDB 서버를 배포한 상태에서 Configuration Manager를 설치에 추가하려는 경우 먼저 Partitioning 옵션을 활성화하여 Standard Edition 데이터베이스를 Enterprise Edition 데이터베이스로 전환해야 합니다.
LDAP(선택 사항)	➤ Active Directory ➤ SunONE 6.x
최소 권장 데이터베이스 스키마 크기(선택 사항)	2GB

클라이언트 요구 사항

운영 체제	➤ Windows XP x86(32비트) ➤ Windows Vista x86(32비트 및 64비트) ➤ Windows 7 x86(32비트 및 64비트)
브라우저	➤ Microsoft Internet Explorer 7.0, 8.0 ➤ Mozilla Firefox 3.x, 4
Flash Player 브라우저 플러그인	Flash Player 9 이상 **참고:** http://www.adobe.com/products/flashplayer/에서 Flash Player를 다운로드하십시오.

화면 해상도	➤ 1024x768 이상 ➤ 1280x1024 권장
화질(해상도)	16비트 이상

HP Operations Orchestration(선택 사항)

HP Operations Orchestration	➤ 7.51, 9.0

2

Windows 플랫폼에 HP Universal CMDB Configuration Manager 설치

중요: 최근에 업데이트된 설치 지침에 대한 릴리스 정보를 확인하십시오.

이 장의 내용은 다음과 같습니다.

설치 전 설정

이 섹션의 내용은 다음과 같습니다.

데이터베이스 또는 사용자 스키마 구성

참고: 이 작업은 Configuration Manager 설치 프로세스의 일부로 자동으로 수행되지만 원하는 경우 수동으로 수행할 수도 있습니다.

Configuration Manager를 사용하려면 데이터베이스 스키마를 제공해야 합니다. Configuration Manager와 UCMDB는 서로 다른 스키마를 사용합니다. Configuration Manager는 Microsoft SQL Server 및 Oracle Database Server를 지원합니다. 이 작업에서는 Configuration Manager용 스키마를 생성하는 방법을 설명합니다. UCMDB를 설치하는 경우 별도의 데이터베이스 스키마뿐 아니라 사용자 스키마도 설정해야 합니다. 자세한 내용은 *HP Universal CMDB 배포 안내서* PDF를 참조하십시오.

참고: Microsoft SQL Server 및 Oracle Server 시스템 요구 사항은 14페이지의 "서버 시스템 요구 사항"을 참조하십시오.

데이터베이스를 구성하려면 다음을 수행합니다.

1 Microsoft SQL Server 데이터베이스 또는 Oracle Server 사용자 스키마를 할당합니다.

- **Microsoft SQL Server**의 경우 스냅샷 격리를 활성화합니다.

  데이터베이스를 생성한 후 다음 명령을 한 번 실행합니다.

  ```
  alter database <ccm_database_name> set read_committed_snapshot on
  ```

  SQL Server 스냅샷 격리 기능에 대한 자세한 내용은 http://msdn.microsoft.com/en-us/library/tcbchxcb(VS.80).aspx를 참조하십시오.

- **Oracle**의 경우 Oracle 사용자에게 **Connect** 및 **Resource** 역할만 부여합니다. 사용자에게 **Select any table** 권한이 있으면 스키마 채우기 절차가 실패합니다.

2 이 구성 프로세스를 진행하는 동안 필요한 다음 정보를 확인합니다.

✔	필요한 정보
	DB 호스트 이름 및 포트
	DB 사용자 이름 및 비밀번호
	MS SQL의 경우: 데이터베이스 이름
	Oracle의 경우: SID

UCMDB 고가용성 환경에서 Configuration Manager 설치

UCMDB 고가용성 환경에서 Configuration Manager를 사용하려면 다음 단계를 따르십시오.

1 (수동적) 백업 서버를 중단합니다. 종료 후 2분 동안 기다립니다.

2 Configuration Manager 버전 9.20을 설치합니다.

a 로드 밸런서 호스트 세부 정보를 사용합니다.

b UCMDB 서버가 아니라 세 번째 서버에 Configuration Manager를 설치합니다.

3 UCMDB 및 Configuration Manager가 제대로 작동하는지 확인합니다.

4 고가용성을 제공하도록 (수동적) 백업 서버를 시작합니다.

참고: 고가용성 모드는 HP Universal CMDB Configuration Manager 버전 9.20 자체에 대해서는 지원되지 않습니다.

Configuration Manager 설치

배포 관리자는 UCMDB, Configuration Manager 및 DDMA를 다음과 같이 서로 다른 구성(설치 마법사의 Products Selection 페이지에서 선택하고 구성)으로 설치할 수 있습니다.

- UCMDB의 새로운 인스턴스 설치
- Configuration Manager의 새로운 인스턴스 설치 및 UCMDB의 새 인스턴스 또는 기존 인스턴스에 연결
- Configuration Manager의 새 인스턴스를 OO의 기존 인스턴스에 통합
- DDMA의 다중 인스턴스 설치

참고:

- 배포 관리자는 대상 시스템에서 제품, 구성 요소를 설치하고 통합할 수 있는 기능을 제공합니다. 제품의 제거, 제품의 수정 및 설치된 제품에서의 패치 설치는 배포 관리자에서 지원되지 않으므로 수동으로 수행해야 합니다.
- Products Selection 페이지에서 **다음** 버튼을 누르면 Product Selection 페이지로 돌아갈 수 없고 배포 구성을 다시 선택할 수 없습니다. 배포 구성을 변경해야 하는 경우 배포 관리자를 다시 시작합니다.

Configuration Manager를 설치하려면 다음을 수행합니다.

1. 설치를 시작하려면 Configuration Manager 설치 미디어를 시스템에 삽입하고 **setup.exe** 파일을 찾습니다.
2. **setup.exe** 파일을 두 번 클릭하여 배포 관리자를 실행합니다.
3. 설치하는 동안 대상 시스템에서 Windows 방화벽을 해제합니다. 방화벽에 대한 자세한 내용은 이 절차의 단계 6을 참조합니다.

4 최종 사용자 라이센스 계약 조건에 동의한 후 **다음**을 클릭하여 Product Selection 페이지를 엽니다.

참고: 라이센스 계약의 조건은 배포 관리자의 Product Selection 페이지에서 선택한 모든 제품에 적용됩니다.

---

5 Product Selection 페이지에서 배포에 필요한 제품을 선택합니다. 완료되면 **다음**을 클릭하여 서버 위치 페이지로 계속 진행합니다.

Product Selection 페이지에서는 설치하려는 제품을 선택할 수 있고 배포 중에 수행되는 구성 옵션을 지정할 수 있습니다.

a HP Universal CMDB 파운데이션 설치 옵션을 선택합니다.

다음과 같은 두 개의 UCMDB 파운데이션 설치 옵션을 사용할 수 있습니다.

- **Connect to an Existing Server** – 이 옵션을 선택하면 Configuration Manager 또는 Discovery and Dependency Mapping을 UCMDB Foundation Server의 기존 인스턴스에 연결 및 구성합니다.

참고: 기존 서버의 UCMDB 버전이 CUP 2 이상이 포함된 9.03 버전이어야 합니다.

- **Install New Server** – 이 옵션을 선택하면 UCMDB Foundation Server의 새 인스턴스를 설치, 구성 및 연결하고 Configuration Manager 또는 DDMA를 UCMDB Foundation Server의 새 인스턴스에 구성 및 연결합니다.

b **Configuration Manager** 확인란을 선택하여 Configuration Manager의 새 인스턴스를 설치 및 구성합니다.

원하는 경우, **Connect to an Existing HP Operation Orchestration instance**를 선택합니다. 이 옵션은 OO 서버 연결 세부 정보로 Configuration Manager를 채워 Configuration Manager와 Operations Orchestration 간의 통합을 구성합니다.

c **HP Discovery and Dependency Mapping Advanced Edition.** 이 옵션을 선택하면 DDMA의 새 인스턴스를 설치 및 구성합니다.

Number of DDMA instances 옵션을 사용하면 여러 개의 DDMA 인스턴스를 설치할 수 있습니다. 입력 필드에 지정된 수는 단일 UCMDB 서버 인스턴스에 연결된 DDMA 인스턴스의 수를 나타냅니다.

참고: 배포 관리자는 동일한 DMZ에서 DDMA 인스턴스의 다중 배포를 지원합니다. 배포 관리자는 각 배포에서 최대 10개의 디스커버리 조사 인스턴스를 지원합니다. 추가 디스커버리 조사가 필요한 경우 10개씩 그룹을 만들어 여러 배포 단계에서 설치합니다.

---

6 Server Location에서 배포를 위해 선택된 각 제품에 대한 대상 배포 시스템의 원격 서버 위치 및 자격 증명을 지정합니다. 완료되면 **다음**을 클릭하여 연결 페이지로 계속 진행합니다.

배포 옵션

대상 위치에 대한 배포 옵션을 선택합니다. 다음 두 옵션을 사용할 수 있습니다.

- **Deploy on the local machine** – 배포 관리자와 같은 시스템에 제품을 배포할 때 이 옵션을 사용합니다. 이 경우에는 원격 호스트 세부 정보 및 자격 증명에 대한 필드가 비활성화됩니다.
- **Deploy on the following machine** – 이 옵션을 선택하면 원격 호스트 주소 및 운영 체제 세부 정보를 제공해야 합니다. 제공된 사용자 자격 증명은 원격 호스트에서 관리자 권한을 가져야 합니다.

참고: 제품 배포에 대한 호스트 이름을 제공할 때 문자(a-z), 숫자(0-9), 하이픈 기호('-')만 사용하도록 합니다.

원격 시스템 세부 정보를 지정할 때 다음 정보가 관련됩니다.

- **WMI and SMB Protocols** – 원격 시스템에 연결하기 위해 사용됩니다. 배포 관리자가 원격 시스템에 성공적으로 연결되려면 다음 필수 구성 요소가 있어야 합니다.
  - **WMI Service** – 원격 시스템에서 WMI 서비스.가 실행 중이어야 합니다.
  - **Server Service** – SMB 프로토콜을 활성화하려면 원격 시스템에서 서버 서비스가 실행 중이어야 합니다.
  - **Windows 방화벽** – 원격 시스템이 원격 관리 연결을 허용해야 합니다. 원격 시스템의 명령 프롬프트 콘솔에서 관련 명령을 실행합니다.

운영 체제	명령
Windows XP Windows Server 2003 Windows Server 2003 R2	netsh firewall set service RemoteAdmin enable
Windows Vista Windows 7 Windows Server 2008 Windows Server 2008 R2	netsh advfirewall firewall set rule group="windows management instrumentation (WMI)" new enable=Yes

연결 테스트

연결 테스트를 클릭하여 연결 자격 증명 및 세부 정보가 올바른지 확인하고 로컬 및 원격 시스템 리소스를 분석합니다.

연결 테스트가 실패할 경우 배포 관리자가 실패를 설명하는 오류 메시지를 표시합니다. **다음** 버튼을 누르면 연결 테스트 검증이 자동으로 실행됩니다.

다음에 대하여 시스템 리소스 유효성 검사가 수행됩니다.

- **OS 플랫폼** – 운영 체제가 제품 배포에 대해 인증되었는지 확인합니다.
- **디스크 공간** – 디스크 공간이 충분한지 확인합니다.
- **메모리** – 실제 메모리가 충분한지 확인합니다.
- **포트** – 필요한 포트를 사용할 수 있는지 확인합니다.

연결 테스트에서 수행되는 리소스 유효성 검사는 지원되는 제품 매트릭스에 따라 다릅니다.

참고: 테스트에서 **알 수 없음** 오류를 반환하는 경우 배포 호스트 시스템에서 다음 서비스가 실행되고 있는지 확인합니다.

- 서버
- WMI(Windows Management Instrumentation)

다음을 클릭하기 전에 UAC(사용자 계정 컨트롤)이 꺼져 있는지 확인합니다. UAC에 대한 자세한 내용을 보려면 http://technet.microsoft.com/en-us/library/cc709691(WS.10).aspx로 이동합니다.

7 연결 페이지에서 선택한 제품 사이에 연결을 구성합니다. 연결 페이지에 표시되는 연결 옵션은 Product Selection 페이지에서 배포를 위해 선택된 구성 요소를 반영합니다. 완료되면 **다음**을 클릭하여 Installation Configuration 페이지로 계속 진행합니다.

- UCMDB를 Configuration Manager에 통합

  이 섹션은 **Connect to an Existing Server** 옵션으로 Configuration Manager를 설치하도록 선택한 경우에 나타나고, Configuration Manager와 UCMDB의 통합을 구성할 수 있습니다.

참고: UCMDB의 기존 인스턴스를 연결하려면 CUP 2 이상이 포함된 UCMDB 9.03 버전을 설치해야 합니다.

다음 UCMDB 세부 정보를 제공합니다.

필드	정의
UCMDB Host Name/IP	UCMDB 배포 위치 주소입니다. ➤ UCMDB가 고가용성 모드로 구성된 경우 19페이지의 "UCMDB 고가용성 환경에서 Configuration Manager 설치"에 나와 있는 지침을 따릅니다. ➤ UCMDB가 로컬 시스템에 설치되어 있고 Configuration Manager가 원격 시스템에 설치된 경우, 로컬 UCMDB 인스턴스의 이름이 localhost가 아니라 FQDN이어야 합니다. ➤ UCMDB 및 Configuration Manager가 서로 다른 DNS 도메인 이름을 사용하고 LW-SSO 통합이 필요한 경우, 기존 UCMDB 호스트 입력 필드에 FQDN을 지정해야 합니다.
Protocol	HTTP 또는 HTTPS 프로토콜입니다.
UCMDB HTTP(S) Port	HTTP 또는 HTTPS 포트 기본값이 HTTP는 **8080**이고 HTTPS는 **8443**입니다.
Client Certificate File	이 필드는 HTTPS 프로토콜을 선택한 경우에 나타납니다. Configuration Manager 대상 호스트에 UCMDB 클라이언트 인증서 파일을 수동으로 배치해야 하고 인접한 입력 필드에 파일 이름을 포함한 전체 파일 경로를 지정해야 합니다. UCMDB가 HTTPS를 사용하는 경우 키 교환을 사용해야 합니다. 연결 테스트 동안에는 키 교환이 유효하지 않습니다.

필드	정의
Customer Name	기본 UCMDB 고객 이름은 **Default Client**입니다. UCMDB와 Configuration Manager 통합 구성 중에 고객 이름 값이 사용됩니다. 이 값은 연결 테스트에서 유효성이 검사되지 않습니다. 잘못된 값을 제공할 경우 배포가 실패합니다.
JMX Port	기본값은 **29601**입니다.
UCMDB System User (JMX)	UCMDB(JMX) 시스템 사용자는 Configuration Manager 통합 사용자 생성 및 Configuration Manager 패키지 배포와 같은 JMX 기능 활성화에 사용됩니다. 기본으로 제공되는 값은 **sysadmin** 입니다.
UCMDB System Password	UCMDB 시스템 사용자 비밀번호입니다. 기본값은 **sysadmin**입니다.

참고: Configuration Manager는 내부 사용자 저장소를 사용하여 구성됩니다. 외부 LDAP를 사용자 저장소로 사용하려면 외부 LDAP를 사용하도록 Configuration Manager를 구성해야 합니다. 자세한 내용은 *HP Universal CMDB Configuration Manager 사용자 안내서*에서 "시스템 설정"을 참조하십시오.

➤ Configuration Manager를 OO에 통합

이 섹션은 **Connect to an Existing HP Operation Instance** 옵션을 선택한 경우에 나타나고 Configuration Manager와 OO의 통합을 구성할 수 있습니다.

다음 OO 세부 정보를 제공합니다.

필드	정의
OO Version	유효한 OO 버전은 7.5 및 9.0입니다.
OO Host Name/IP	OO 서버 시스템의 호스트 또는 IP 주소입니다.
OO Port Number	기본 포트 번호는 **8443**입니다.
OO Username	기본 OO 사용자 이름은 **admin**입니다. 사용자가 OO에서 외부로 구성되어야 합니다.
OO Password	기본 OO 비밀번호는 **admin**입니다.

➤ DDMA 구성

Discovery and Dependency Mapping Advanced Edition instance 옵션을 선택한 경우 다음 필드가 나타나고 UCMDB에 대한 DDMA 연결을 구성할 수 있습니다.

다음 DDMA 세부 정보를 제공합니다.

필드	정의
Data Flow Probe Identifier	기본값은 DDMA 시스템 호스트 이름이고 이 필드는 자동으로 채워집니다. 이 값을 변경할 수 있습니다.
Use Default Domain	이 옵션은 기본적으로 선택되고 도메인 이름 값에 영향을 줍니다. 이 확인란의 선택을 취소하면 기본 이름을 다른 값으로 변경할 수 있습니다.
Domain Name	기본값은 **DefaultDomain**으로 설정됩니다. 이 필드를 활성화하려면 **Deselect the Use Default Domain** 확인란을 선택 취소합니다.
Initial Heap Size in MB	DDMA의 JVM에 할당된 초기 메모리 크기 기본값은 256MB입니다.
Maximum Heap Size in MB	JVM에 할당된 최대 메모리 크기이며, 기본값은 512MB입니다.

8 Installation Configuration 페이지에서 선택한 제품 배포에 대해 배포 대상 디렉터리 세부 정보를 설정합니다. 완료되면 **다음**을 클릭하여 데이터베이스 구성 페이지로 계속 진행합니다.

각 선택된 제품에 대해 기본 디렉터리 경로가 제공됩니다. 로컬 시스템에 배포하는 경우 다른 디렉터리 경로를 선택하려면 찾아보기 옵션을 사용할 수 있습니다. 원격 시스템에 설치하는 경우 이 옵션이 비활성화됩니다.

참고: 설치 디렉터리는 이름에 공백이 포함되어서는 안 되며 영문자(a-z), 숫자(0-9), 하이픈 기호('-')만 사용할 수 있습니다.

---

9 데이터베이스 구성 페이지에서 각 제품 데이터베이스 연결 및 데이터베이스 스키마를 구성합니다. 완료되면 **다음**을 클릭하여 Ports Configuration 페이지로 계속 진행합니다.

다음 데이터베이스 스키마를 구성할 수 있습니다.

- UCMDB-CM 스키마
- UCMDB 스키마
- UCMDB 기록 내역 스키마

필드	정의
Database Host Name/IP	데이터베이스 서버 위치 주소입니다.
Port	MSSQL과 Oracle은 서로 다른 기본 포트를 사용합니다. Oracle 데이터베이스 기본 포트는 1521이고 MSSQL 데이터베이스 기본 포트는 1433입니다.
SID (Oracle)	Oracle 데이터베이스 인스턴스 이름입니다.
Admin Username (Oracle)	Oracle 서버에 따라 Oracle 관리자 사용자 이름을 입력합니다.
Admin Password (Oracle)	Oracle 서버에 따라 Oracle 관리자 비밀번호를 입력합니다.

필드	정의
Test Connection	제공된 자격 증명을 사용하여 대상 DB 호스트에 대한 연결을 테스트합니다.
Schema Name (Oracle)	스키마 이름을 입력합니다.
Schema Password (Oracle)	스키마 비밀번호를 입력합니다. 이 필드는 새로운 스키마를 만들 때 나타납니다.
Default Tablespace (Oracle)	기본 테이블스페이스 이름을 입력합니다.
Temporary Tablespace (Oracle)	임시 테이블스페이스 이름을 입력합니다.
Database Name (MSSQL)	MSSQL 서버에서 사용/생성할 데이터베이스 스키마 이름을 입력합니다.
Database Username (MSSQL)	MSSQL 서버에 따라 MSSQL 관리자 사용자 이름을 입력합니다.
Database Password (MSSQL)	Oracle 서버에 따라 MSSQL 관리자 비밀번호를 입력합니다.

참고:

- UCMDB 테이블스페이스가 가득 찬 경우, 제품 배포는 성공하지만 제품 및 구성 요소가 올바르게 작동하지 않습니다.
- 새 UCMDB 스키마 생성 및 기존 UCMDB 기록 내역 스키마에 대한 연결은 지원되지 않습니다.
- UCMDB이 원격으로 설치된 경우, MSSQL 데이터베이스를 사용하여 UCMDB 스키마를 구성하면 NTLM 인증 사용이 보안상의 이유로 지원되지 않습니다. NTLM 인증이 필요한 경우 UCMDB를 로컬로 배포하십시오.

스키마 모드

Configuration Manager에서는 UCMDB가 통합 스키마 모드에서 구성되어야 하고 새 UCMDB 상태가 생성되어야 합니다.

기존 UCMDB 설치를 참조하는데 그 스키마가 아직 통합되지 않은 경우, 너무 많이 채워진 데이터베이스(CI가 5백만 개 이상 포함된 데이터베이스)에서는 자동 통합 단계에 시간이 오래 걸릴 수 있습니다(20 ~ 60분).

참고: Oracle RAC(Real Application Cluster)와 SQL Server NTLM 연결은 이 설치 과정에서 지원되지 않습니다. 이러한 연결이 필요한 경우 먼저 간단한 데이터베이스 연결로 Configuration Manager를 설치하고 설치 프로세스가 완료되면 특정 제품 구성에서 연결을 변경합니다. 이렇게 하려면 데이터베이스 사양에 따라 **database.properties** 파일을 수정합니다. 자세한 내용은 31페이지의 "고급 데이터베이스 구성(Configuration Manager의 경우)"을 참조하십시오.

데이터베이스 구성 모드

Configuration Manager 및 UCMDB는 서로 다른 스키마를 사용해야 합니다.

Configuration Manager를 사용하여 사용자가 Oracle 또는 MSSQL 데이터베이스 서버에서 각 데이터베이스를 구성할 수 있습니다.

구성 유형

기존 스키마에 연결하거나 새 스키마를 생성할 수 있습니다. 기존 스키마에 연결하면 해당 내용이 오버라이드됩니다.

데이터베이스 구성

이 단계는 배포 관리자에 의해 자동으로 수행됩니다. 이 단계를 수동으로 수행하려면 18페이지의 "데이터베이스 또는 사용자 스키마 구성"을 참조하십시오.

고급 데이터베이스 구성(Configuration Manager의 경우)

데이터베이스 연결은 표준 URL 연결과 관련하여 구성해야 합니다. Oracle Real Application Cluster와 같은 고급 기능이 필요하면 표준 연결을 설정한 후 수동으로 **database.properties** 파일을 편집하여 고급 기능을 구성합니다.

Configuration Manager는 Oracle 및 Microsoft SQL Server 데이터베이스의 기본 드라이버를 사용합니다. 데이터베이스 URL을 사용하여 이러한 기능을 구성할 있다면 모든 기본 드라이버 기능이 지원됩니다. URL은 **database.properties** 파일에 있습니다.

배포 관리자 마법사가 완료되면 추가 데이터베이스 및 스키마 구성을 수행할 수 있습니다.

데이터베이스 구성 필드

두 가지 유형의 데이터베이스(Oracle과 MSSQL)를 사용할 수 있습니다. 선택한 데이터베이스 유형에 따라 입력 필드가 변경됩니다.

10 Port Configuration 페이지에서 Configuration Manager 연결 포트를 지정합니다. 완료되면 **다음**을 클릭하여 사용자 구성 페이지로 계속 진행합니다.

Configuration Manager는 포트 구성 마법사 페이지의 입력 필드에 표시되는, 기본으로 제공되는 기본 포트 설정을 제공합니다.

포트 번호가 기존 설치와 충돌할 경우 포트 번호를 변경하기 전에 IT 관리자와 상의하십시오.

필드	정의
Application HTTP Port	8180
JMX HTTP Port	39900
Tomcat Port	8005
AJP Port	8009(Apache Java Protocol)
Application HTTPS Port	8143
JMX Remote Port	39600

Revert to Default Values 버튼을 클릭하여 포트를 배포 관리자에서 제공하는 기본값으로 다시 설정합니다.

11 사용자 구성 페이지에서 다음 사용자를 만듭니다.

- 관리자 권한이 있는 UCMDB-CM 초기 로그인 사용자 인스턴스
- UCMDB의 통합 사용자 - 이러한 두 제품 간 통합을 지원하기 위해 Configuration Manager에서 요구 시 UCMDB에 통합 사용자가 생성됩니다.

완료되면 **다음**을 클릭하여 보안 구성 페이지로 계속 진행합니다.

12 보안 구성 페이지에서 UCMDB 및 Configuration Manager의 새 인스턴스에서 Global LW-SSO를 활성화합니다. LW-SSO는 Product Selection 페이지에서 선택한 내용에 따라 Configuration Manager 또는 UCMBD의 새 인스턴스에서만 구성됩니다. 완료되면 **다음**을 클릭하여 요약 페이지로 계속 진행합니다.

LW-SSO는 서로 다른 유형의 인증 및 보안 토큰(예: LW-SSO 및 SAML2)의 유효성을 검사하기 위해 사용되는 모듈형 프레임워크입니다. LW-SSO는 서로 다른 환경의 인증 정보를 응용 프로그램 또는 보안 프레임워크 내 응용 프로그램 보안 컨텍스트에 연결 및 활용하기 위해 사용됩니다.

LW-SSO 구성은 선택한 제품 구성 요소에 따라 다릅니다.

Configuration Manager를 기존 UCMDB 또는 OO 인스턴스에 연결하면 Configuration Manager에서만 LW-SSO가 구성됩니다. UCMDB 또는 OO에서 LW-SSO 문자열을 추출하여 해당 문자열을 LW-SSO 문자열 입력 필드에 입력해야 합니다. UCMDB와 OO를 둘 다 연결하는 경우 UCMDB 및 OO 인스턴스에서 정의된 LW-SSO 문자열이 일치하는지 확인합니다.

Configuration Manager의 새 인스턴스를 UCMDB의 기존 인스턴스에 연결할 때는 UCMDB 호스트 이름으로 FQDN을 사용합니다.

UCMDB에서 LW-SSO 문자열을 추출하려면 다음을 수행합니다.

a UCMDB를 열고 **관리** > **인프라 설정 관리자**를 선택합니다.

b **이름** 열에서 LW-SSO init 문자열 필드를 선택하고 두 번 클릭합니다.

c 현재 값 입력 필드에서 문자열을 복사합니다.

d 이 값을 보안 구성 페이지의 LW-SSO 문자열 입력 필드에 붙여넣습니다.

Configuration Manager를 새 UCMDB 인스턴스에 연결하면, Configuration Manager 뿐만 아니라 UCMDB에서도 LW-SSO가 자동으로 구성됩니다.

13 요약 페이지에서 설치 및 구성 설정을 검토합니다. 완료되면 **다음**을 클릭하여 Validation 페이지로 계속 진행합니다.

요약 페이지는 모든 구성 세부 정보 및 사용자 입력을 한 곳에서 보여줍니다. 필요한 경우, 요약 페이지에서 원하는 페이지에 도달할 때까지 뒤로 버튼을 클릭하여 요약 내용을 수정하고 배포 설정을 조정할 수 있습니다. 필요한 경우 **다음**을 클릭하여 요약 페이지로 돌아갑니다.

14 이제 배포 관리자가 원격 시스템의 시스템 리소스가 충분하지 검증하고 사용자 입력이 올바른지 확인하는 일련의 작업을 실행하고 데이터베이스 구성 설정의 유효성을 검사합니다. 이러한 유효성 검사는 사용자 정의 설정이 알려진 환경 제한을 준수하는지 여부를 나타냅니다. 유효성 검사 프로세스는 자동으로 시작됩니다. 하지만 배포 관리자의 이전 페이지로 돌아가 구성을 변경한 경우에는 **Run Validation**을 클릭하여 유효성 검사 프로세스를 시작해야 합니다. 완료되면 **배포**를 클릭하여 배포 페이지로 계속 진행합니다.

15 배포 페이지는 진행될 때 배포 프로세스의 상태를 반영합니다. 배포 프로세스에는 제품 설치, 시작 절차 및 다른 제품과의 통합 및 연결이 포함됩니다.

배포 프로세스는 모든 제품이 성공적으로 시작되면 완료됩니다.

선택한 각 제품 배포에 대하여 배포 관리자에서 수행된 단계를 포함하여 배포 진행 세부 정보를 확인하려면 **세부 정보**를 클릭합니다.

배포를 중단하기 전에 현재의 배포 작업이 완료될 수 있도록 배포를 정상적으로 취소하려면 **취소**를 클릭합니다.

현재의 작업과 배포를 강제적으로 종료하려면 **중단**(**취소**를 클릭한 후에만 사용 가능)을 클릭합니다. 배포를 중단하면 제품이 확인되지 않는 상태에 놓일 수 있습니다.

유효성 검사

아래 표는 배포 관리자에서 수행되는 유효성 검사의 목록을 제공합니다.

유효성 검사	오류 메시지	설명
로그인 자격 증명 확인	Credentials verification failed	제공된 사용자 자격 증명이 올바르지 않습니다.
		연결할 수 없습니다.
운영 체제 호환성 확인	Target operating system platform is <Platform> Product <Product Name> supports the following platforms <Platform>	실제 대상 운영 체제가 제품에 대하여 인증된 운영 체제 목록과 일치하지 않습니다.
메모리 확인	The assigned memory (<Memory> MB) exceeds the available memory (<Memory> MB) on <Target>	할당된 모든 제품에 대하여 대상 시스템의 메모리가 충분하지 않습니다.
	<Memory> MB of memory are verified to be available on <Target Machine>	유효성 검사에 성공했습니다.
디스크 공간 확인	assigned disk space for (<Memory> MB) exceeds available disk space (<Memory> MB) on drive <Target>	할당된 모든 제품에 대하여 대상 시스템의 디스크 공간이 충분하지 않습니다.
	<Memory> MB of disk space are verified to be available on drive <Target>	유효성 검사에 성공했습니다.
모든 필수 속성이 제공되었는지 확인	Missing the target storage device for the product: <Target>	제품의 설치 디렉터리가 설정되지 않았습니다.

유효성 검사	오류 메시지	설명
배포 시스템이 정의되었는지 확인	No deployment machine is defined for <Product Name>	제품이 어떤 시스템에 대해서도 배포되도록 구성되지 않았습니다.
로그인 자격 증명 확인	Credentials verification failed	잘못된 로그인 자격 증명
UAC가 비활성 상태인지 확인	The UAC is enabled	대상 시스템에서 UAC가 활성화되어 있습니다.
사용할 수 있는 포트 확인	The required port number <Port> is already in use on <Target>	대상 시스템에서 필요한 포트가 이미 사용 중입니다.
대상 저장소 장치가 존재하는지 확인	The target storage device <Device> does not exist on <Target>	선택한 대상 저장소 장치가 대상 시스템에 없습니다.
스키마 존재의 유효성 검사	Schema <Name> does not exist/ already exist	대상 시스템에 해당 스키마가 있습니다/없습니다.
스키마 권한 존재의 유효성 검사	Validate <Permissions> schema tables user permissions existence	DB 사용자가 충분한 권한이 없습니다.
스키마 테이블 존재의 유효성 검사	Schema Tables <Tables> on the database: <Tables> already exist	데이터베이스에 스키마 테이블이 이미 있습니다.
스키마 테이블 사용자 권한 존재의 유효성 검사	The database user does not have the correct permissions	데이터베이스 사용자가 올바른 권한을 보유하고 있지 않습니다.

유효성 검사	오류 메시지	설명
UCMDB 연결 확인	Connection failed. Connection to UCMDB failed, host: <Host>, username: <User name>, port: <Port>, protocol: <Protocol> due to <Error>	지정된 연결 설정을 사용한 UCMDB에 대한 연결 테스트에 실패했습니다.
	Existing UCMDB version must be 9.03 with CUP 2 or later.	기존 UCMDB 버전이 9.03 이고 CUP 2 이상이 설치되어야 합니다.
DB 연결 확인	The host name/IP address validation failed	지정된 데이터베이스 호스트 이름/IP 주소에 연결할 수 없습니다.
	The username or password validation failed	지정된 사용자 자격 증명이 유효하지 않습니다.
	The port validation failed	지정된 데이터베이스 포트에 연결할 수 없습니다.
	The SID validation failed	지정된 데이터베이스 SID가 DB에 없습니다.
설치 확인	The product is already installed	대상 호스트에 제품이 이미 설치되었습니다.

Configuration Manager 업그레이드

업그레이드 절차가 시작되기 전에 다음 사항에 대한 확인 및 유효성 검사가 자동으로 수행됩니다.

- UCMDB 서버에 대해 작동 중인 연결이 있는지 여부
- UCMDB에 대한 CUP 2 패치가 설치되었는지 여부
- JMX 포트가 올바른지 여부

이러한 항목 중 하나라도 올바르게 설치 또는 구성되지 않은 경우, 이에 대해 알려주는 오류 메시지가 표시됩니다. 표시된 문제를 수정한 다음 업그레이드를 수행할 수 있습니다.

- UCMDB에 연결할 수 없어서 업그레이드에 실패하는 경우 UCMDB 서버가 실행 중인지 확인하십시오.
- 패치가 설치되어 있지 않아서 업그레이드에 실패하는 경우 http://support.openview.hp.com/selfsolve/document/FID/DOCUMENTUM_UCMDB_00045에 나와있는 지침에 따라 CUP 2를 설치합니다.
- 잘못된 UCMDB JMX 포트로 인해 업그레이드에 실패하는 경우 올바른 JMX 포트를 선택합니다. 이렇게 하려면 **<Configuration Manager 설치 디렉터리>\utilities\Upgrade** 폴더에 있는 **upgrade.properties** 파일에서 ucmdb.jmx.port 속성을 변경합니다.

업그레이드하려면 다음 단계를 수행합니다.

참고: 업그레이드 절차를 시작할 때 UCMDB 서버가 실행 중인지 확인합니다.

---

1. Configuration Manager 및 UCMDB 스키마를 백업합니다.
2. Configuration Manager 설치 미디어의 Windows 하위 폴더에서 **setup-win64.msi** 파일을 찾습니다.
3. 파일을 두 번 클릭하여 Configuration Manager 설치 마법사를 실행합니다.
4. **Next**를 클릭하여 최종 사용자 라이센스 계약 페이지를 엽니다.

5 라이센스 조건에 동의한 후 **Next**를 클릭하여 Customer Information 페이지를 엽니다.

6 사용자 정보를 입력하고 **Next**를 클릭하여 Setup Type 페이지를 엽니다.

7 Configuration Manager를 설치할 폴더를 선택합니다. 이전 버전에 대해 사용했던 위치와 다른 위치를 선택하도록 합니다.

기본적으로 Configuration Manager는 **c:\hp\cnc920** 디렉터리에 설치됩니다. **Next**를 클릭하여 기본 위치를 그대로 사용하거나, **Browse**를 클릭하여 다른 위치를 선택한 후 **Next**를 클릭합니다.

참고: 설치 디렉터리 이름에 공백이 포함되어서는 안 됩니다.

---

8 **Next**를 클릭하여 확인한 후 설치를 시작합니다.

설치 마법사가 완료되면 Configuration Manager 설치 후 마법사가 자동으로 시작됩니다.

9 Configuration Manager를 새로 설치할 것인지 아니면 업그레이드할 것인지 물을 때까지 **Next**를 클릭합니다.

10 **Upgrade**를 선택한 후 **Next**를 클릭합니다.

11 설치가 완료되면 **post_installation.log** 파일(<**Configuration Manager 설치 디렉터리/tmp/log** 폴더에 있음)을 확인하여 아무런 오류 없이 설치가 완료되었는지 확인합니다.

업그레이드 프로세스 중에 오류가 발생하면 메시지가 표시되므로 마법사를 닫을 수 있습니다. 오류가 발생할 경우 HP 고객지원센터로 문의하십시오.

12 Configuration Manager 서비스를 시작합니다.

참고: 업그레이드 후 SSL 구성을 다시 수행해야 합니다. 자세한 내용은 84페이지의 "강화"를 참조하십시오.

3

Linux 플랫폼에 HP Universal CMDB Configuration Manager 설치

중요: 최근에 업데이트된 설치 지침에 대한 릴리스 정보를 확인하십시오.

이 장의 내용은 다음과 같습니다.

설치 전 설정

이 섹션에는 다음과 같은 내용도 포함되어 있습니다.

사전 준비 사항

➤ 400MB 이상의 디스크 공간

➤ 작동 중인 권장 X 디스플레이

setup.bin 파일 얻기

Linux 설치 파일(**setup.bin**)은 설치 미디어에 있거나 HP 웹사이트에서 다운로드할 수 있는 ISO 이미지에 있습니다. 다음 방법 중 하나로 파일에 액세스할 수 있습니다.

➤ Linux 시스템에 DVD 탑재

```
$ mkdir -p /mnt/cdrom
$ mount /dev/cdrom /mnt/cdrom
```

➤ ISO 이미지를 루프백 차단 장치로 탑재

```
$ mkdir -p /mnt/cdrom
$ mount -o loop cnc-<version>.iso /mnt/cdrom
```

➤ **setup.bin** 파일을 Linux 시스템의 임시 위치에 복사

Configuration Manager 설치

이 작업은 서버에 Configuration Manager를 설치하고, 데이터베이스 연결 및 UCMDB 통합을 구성하는 방법에 대해 설명합니다.

작동 중인 X 디스플레이가 있는 경우 설치 후 마법사가 UI로 표시되고 그렇지 않을 경우 마법사 정보가 콘솔 모드로 표시됩니다.

참고: 본 안내서에서는 작업 단계가 콘솔 모드로 설명되지만, UI 마법사를 사용하는 경우에도 동일한 작업 단계가 표시됩니다.

Configuration Manager를 설치하려면 다음을 수행합니다.

1 현재 위치에서 Configuration Manager를 설치하려면 다음 명령을 실행합니다.

```
chmod 755 setup.bin
$ /path/to/installation/kit/setup.bin
```

2 EULA(최종 사용자 라이센스 계약)가 표시되면 동의해야 합니다. EULA의 끝에 도달할 때까지 스페이스바를 반복적으로 클릭하여 EULA의 아래 부분까지 스크롤합니다. 동의하고 계속 설치하려면 **yes**를 입력하고 **Enter** 키를 누릅니다.

HP Universal CMDB Configuration Manager가 **cnc** 하위 폴더의 현재 위치에 설치됩니다.

시작 페이지

```
<============================>
Welcome
<============================>
Welcome to the HP Universal CMDB Configuration Manager
post installation wizard.
Enter [<C>ancel] [Ne<x>t]>
```

Enter 키를 눌러 다음 페이지로 계속 진행합니다.

데이터베이스 벤더 선택

```
<============================>
Database Connection Configuration
<============================>
-------
Vendor:
-------
  ->1 - Oracle
    2 - Microsoft
Enter index number from 1 to 2 OR [<C>ancel] [Back<b>] [Ne<x>t]>
```

Enter 키를 눌러 Oracle을 선택하거나, **2**를 입력한 후 **Enter** 키를 눌러 Microsoft를 선택합니다.

데이터베이스 호스트 이름

```
-------------
Set Hostname:
-------------
        Hostname: = "localhost"
Input the new Hostname: OR [<C>ancel] [<B>ack] [Ne<x>t]>
```

데이터베이스의 호스트 이름을 입력하고 **Enter** 키를 누릅니다. 제공된 호스트 이름의 기본값은 **localhost**입니다.

데이터베이스 포트

```
---------
Set Port:
---------
        Port: = "1521"
Input the new Port: OR [<C>ancel] [<B>ack] [Ne<x>t]>
```

Oracle의 기본 포트는 1521이고 Microsoft의 기본 포트는 1433입니다. 다른 포트 번호를 사용하려면 여기에 포트 번호를 입력하고 **Enter** 키를 누릅니다.

SID/DB 이름

```
-----------
Set SID/DB:
-----------
        SID/DB: = "orcl"
Input the new SID/DB: OR [<C>ancel] [<B>ack] [Ne<x>t]>
```

Oracle에서는 이 필드가 데이터베이스 SID를 지정하고, Microsoft에서는 이 필드가 데이터베이스 이름을 지정합니다. 유효한 값을 입력하고 **Enter** 키를 누릅니다.

사용자/스키마 이름 및 비밀번호

```
-------------
Set Username:
-------------
Input the Username: OR [<C>ancel] [<B>ack] [Ne<x>t]>
```

데이터베이스 사용자 이름을 입력하고 **Enter** 키를 누릅니다.

```
Input the Password: OR [<C>ancel] [<B>ack] [Ne<x>t]>
```

스키마 비밀번호를 입력하고 **Enter** 키를 누릅니다.

데이터베이스 연결 테스트

```
--------
Set Test
--------
        Test = "Yes"
Choose [<Y>es]/[<N>o] for Test OR [<C>ancel] [<B>ack] [Ne<x>t]>
```

Enter 키를 눌러 데이터베이스 연결을 테스트합니다.

이 마법사는 데이터베이스 스키마에 테이블을 만들려고 시도하기 때문에 데이터베이스 연결을 테스트하는 것이 좋습니다. 연결을 테스트하지 않으려면 **No**를 입력하고 **Enter** 키를 누릅니다.

데이터베이스 연결 테스트가 성공적으로 완료되면 다음 메시지가 표시됩니다.

```
success
Enter [<C>ancel] [<B>ack] [Ne<x>t]>
```

Enter 키를 눌러 계속합니다. 연결 테스트에서 오류가 발생하면 오류 메시지가 표시되고 테스트를 다시 실행할지 묻는 대화 상자가 나타납니다. 연결 문제를 해결하고 다시 테스트하여 설치를 계속합니다.

응용 프로그램 서버 호스트 이름

```
<============================>
Application Server Configuration
<============================>
Hostname
----
Set
----
         = "myucmdbcmhost.mydomain"
Input the new  OR [<C>ancel] [Back<b>] [Ne<x>t]>
```

호스트 이름의 기본값은 시스템의 실제 호스트 이름입니다. 로드 밸런서 또는 리버스 프록시의 백그라운드에 설치하는 경우 여기에 외부 이름을 입력합니다.

응용 프로그램 서버 포트 사용자 지정

```
-------------------
Select Customize ports
-------------------
        Customize ports = "No"
Choose [<Y>es]/[<N>o] for Customize ports OR [<C>ancel] [<B>ack]
[Ne<x>t]>
```

Configuration Manager에 대해 기본 포트를 사용하려면 **Enter** 키를 누릅니다. 사용자 지정 포트를 사용하려면 **Yes**를 입력하고 **Enter** 키를 누릅니다. 기본 포트 번호는 다음과 같습니다.

포트 이름	포트 번호
HTTP	8180
HTTPS	8443
Tomcat 관리	8005
AJP	8009
JMX HTTP	39900
JMX RMI	39600

포트를 사용자 지정하도록 선택하면, 위에 나열된 각 포트에 대하여 값을 입력하라는 요청을 받게 됩니다. 각 포트에 대해 새 값을 입력하고 **Enter** 키를 누릅니다.

```
HTTP port:
----
Set
----
         = "8180"
Input the new  OR [<C>ancel] [<B>ack] [Ne<x>t]>
HTTPS port:
----
Set
----
         = "8443"
Input the new  OR [<C>ancel] [<B>ack] [Ne<x>t]>
Tomcat port:
----
Set
----
         = "8005"
Input the new  OR [<C>ancel] [<B>ack] [Ne<x>t]>
AJP port:
----
Set
----
         = "8009"
Input the new  OR [<C>ancel] [<B>ack] [Ne<x>t]>
JMX HTTP port:
----
Set
----
         = "39900"
Input the new  OR [<C>ancel] [<B>ack] [Ne<x>t]>
JMX remote port:
----
Set
----
         = "39600"
Input the new  OR [<C>ancel] [<B>ack] [Ne<x>t]>
```

관리 권한을 가진 초기 사용자

```
<============================>
Users Credentials
<============================>
Initial Administrative User
Admin username:
----
Set
----
Input the  OR [<C>ancel] [Back<b>] [Ne<x>t]>
```

최초의 로그인을 위해 시스템의 관리자 또는 슈퍼 유저가 되는 관리 권한을 가진 초기 사용자가 생성됩니다. 사용할 admin 사용자 이름을 입력하고 **Enter** 키를 누릅니다.

```
Admin password:
Input the  OR [<C>ancel] [<B>ack] [Ne<x>t]>
```

admin 사용자에 대한 비밀번호를 입력하고 **Enter** 키를 누릅니다.

```
Confirm password:
Input the  OR [<C>ancel] [<B>ack] [Ne<x>t]>
```

확인을 위해 admin 사용자의 비밀번호를 다시 입력하고 **Enter** 키를 누릅니다.

통합 사용자

```
Platform Integration User
Integration username:
----
Set
----
Input the  OR [<C>ancel] [<B>ack] [Ne<x>t]>
```

UCMDB 통합 사용자 이름을 선택합니다. 이 사용자는 이 설치 후 프로세스 동안 UCMDB에 생성됩니다. 통합 의도를 분명하게 나타낼 수 있는 사용자 이름(예: cm_integration)을 사용하는 것이 좋습니다. 선택한 사용자 이름을 입력하고 **Enter** 키를 누릅니다.

```
Integration password:
Input the  OR [<C>ancel] [<B>ack] [Ne<x>t]>
```

통합 사용자에 대한 비밀번호를 입력하고 **Enter** 키를 누릅니다.

```
Confirm password:
Input the  OR [<C>ancel] [<B>ack] [Ne<x>t]>
```

확인을 위해 통합 사용자의 비밀번호를 다시 입력하고 **Enter** 키를 누릅니다.

HP Universal CMDB 서버 호스트 이름

```
<============================>
HP UCMDB Connection Configuration
<============================>
Hostname
----
Set
----
         = "localhost"
Input the new  OR [<C>ancel] [Back<b>] [Ne<x>t]>
```

UCMDB 서버에 대한 호스트 이름을 입력하고 **Enter** 키를 누릅니다. 프로덕션 환경에서는 같은 시스템에 UCMDB와 Configuration Manager를 함께 설치하는 것이 좋지 않기 때문에 이 이름이 기본 localhost와 다를 수 있습니다.

HP Universal CMDB 서버 포트

```
Port
----
Set
----
         = "8080"
Input the new  OR [<C>ancel] [<B>ack] [Ne<x>t]>
```

Enter 키를 눌러 UCMDB 서버에 대해 기본 포트 번호 8080을 그대로 사용하거나, 원하는 포트 번호를 입력하고 **Enter** 키를 누릅니다.

HP Universal CMDB 서버 프로토콜

```
Protocol
  ->1 - HTTP
    2 - HTTPS
Enter index number from 1 to 2 OR [<C>ancel] [<B>ack] [Ne<x>t]>
```

Enter 키를 눌러 HTTP를 사용하거나, 2를 입력하고 **Enter** 키를 눌러 HTTPS를 사용합니다.

참고: HTTPS를 선택하면 UCMDB와 키를 교환해야 합니다. 자세한 내용은 84 페이지의 "강화"를 참조하십시오. 이 절차에서는 보안되지 않은 자체 서명된 인증서를 사용하여 HTTPS를 설정합니다.

HP Universal CMDB 서버 고객

```
Customer:
----
Set
----
          = "Default Client"
Input the new  OR [<C>ancel] [<B>ack] [Ne<x>t]>
```

Enter 키를 눌러 UCMDB 서버에 대해 기본 고객 이름을 그대로 사용하거나, 원하는 고객 이름을 입력하고 **Enter** 키를 누릅니다.

HP Universal CMDB 서버 Sysadmin 자격 증명

```
Administrative username
----
Set
----
Input the  OR [<C>ancel] [<B>ack] [Ne<x>t]>
```

UCMDB 서버 sysadmin 사용자 이름을 입력합니다. 이 사용자는 UCMDB 서버에서 JMX 메서드를 실행할 수 있는 사용자입니다. 이 사용자는 기존 사용자이며 설치 중에 생성되지 않습니다. UCMDB 서버 관리자에서 sysadmin 사용자를 위한 자격 증명을 얻습니다.

```
Administrative password:
Input the  OR [<C>ancel] [<B>ack] [Ne<x>t]>
```

UCMDB 서버 sysadmin 사용자에 대한 비밀번호를 입력하고 **Enter** 키를 누릅니다.

HP Universal CMDB 서버 연결 테스트

```
--------
Set Test
--------
        Test = "Yes"
Choose [<Y>es]/[<N>o] for Test OR [<C>ancel] [<B>ack] [Ne<x>t]>
```

Enter 키를 눌러 UCMDB 서버 연결을 테스트합니다. 이 마법사는 패키지를 배포하고 UCMDB 서버를 구성하려고 시도하기 때문에, 서버 연결을 테스트하는 것이 좋습니다. 연결을 테스트하지 않으려면 **No**를 입력하고 **Enter** 키를 누릅니다.

서버 연결 테스트가 성공적으로 완료되면 다음 메시지가 표시됩니다.

```
success
Enter [<C>ancel] [<B>ack] [Ne<x>t]>
```

Enter 키를 눌러 계속합니다. 연결 테스트에서 오류가 발생하면 오류 메시지가 표시되고 테스트를 다시 실행할지 묻는 대화 상자가 나타납니다. 연결 문제를 해결하고 다시 테스트하여 설치를 계속합니다.

요약

이 마법사는 실제로 선택 사항을 실행하기 전에 사용자가 선택한 모든 선택 사항에 대한 요약을 표시합니다.

```
<============================>
Post Installation Actions Summary
<============================>
Post installation actions summary
Users
-----
HP Universal CMDB Configuration Management admin username: admin
HP Universal CMDB Platform integration username: cm_integration

Database
--------
Vendor: Oracle
Host: mydbhost.mydomain
Port: 1521
SID/DB: orcl
Encrypt password? Yes
Create schema objects? Yes

Application Server
------------------
hostname: myucmdbcmhost.mydomain
HTTP: 8180
HTTPS: 8443
Tomcat management: 8005
AJP: 8009
JMX HTTP: 39900
JMX remote: 39600
Debug: 7878

Windows Service
---------------
Create service? No

HP Universal CMDB Platform
-----
URL: http://myucmdb.mydomain:8080
Sysadmin username: sysadmin
Customer: Default Client

Enter [<C>ancel] [Back<b>] [Ne<x>t]>
```

Enter 키를 눌러 구성 단계를 계속 진행합니다. 구성이 진행되는 동안 진행 표시줄이 나타납니다. 마법사에서 다음 작업을 수행합니다.

1 데이터베이스 테이블 및 개체를 생성합니다.

2 데이터베이스를 기본값 및 초기값으로 채웁니다.

3 관리 권한이 있는 초기 사용자를 생성합니다.

4 UCMDB 서버에서 통합 사용자를 생성합니다.

5 UCMDB 서버를 통합합니다.

6 UCMDB 서버에서 인증 상태를 생성합니다.

7 UCMDB 서버에 Configuration Manager 패키지를 배포합니다.

구성이 완료되면 다음 메시지가 나타납니다.

```
<============================>
Finish
<============================>
Post installation configuration has completed.
Enter [Finish<f>]>
```

Enter 키를 눌러 마법사를 종료합니다.

자동 설치 옵션

Configuration Manager를 자동 모드로 설치할 수 있습니다. 자동 모드 설치에서는 설치 패키지에서 파일을 추출할 뿐, 설치 후 구성은 수행하지 않습니다. 자동 모드에서 설치를 실행하려면 다음 명령을 실행합니다.

```
$ /path/to/installation/kit/setup.bin silent
```

Configuration Manager 응용 프로그램 서버 실행

Configuration Manager를 실행하려면 다음 명령을 실행합니다.

```
$ cd /path/to/installation/location
$ ./start-server-0.sh
```

/etc/init.d 디렉터리에 스크립트를 만들어 시스템 시작 시 Configuration Manager를 자동으로 시작할 수 있습니다.

4

Configuration Manager 로그인

이 장의 내용은 다음과 같습니다.

Configuration Manager 액세스

Configuration Manager는 Configuration Manager 서버에 네트워크(인트라넷 또는 인터넷)로 연결된 컴퓨터에서 지원되는 웹 브라우저를 사용하여 액세스합니다. 사용자에게 부여되는 액세스 수준은 사용자의 권한에 따라 다릅니다. 사용자 권한에 대한 자세한 내용은 *HP Universal CMDB Configuration Manager 사용자 안내서*에서 "사용자 관리"를 참조하십시오.

웹 브라우저 요구 사항 및 Configuration Manager 디스플레이 요구 사항에 대한 자세한 내용은 14페이지의 "매트릭스 지원"을 참조하십시오.

Configuration Manager에 안전하게 액세스하는 방법에 대한 자세한 내용은 84페이지의 "강화"를 참조하십시오.

Configuration Manager 액세스에 대한 문제 해결 정보는 117페이지의 "문제 해결"을 참조하십시오.

Configuration Manager 로그인

1 웹 브라우저에서 Configuration Manager 서버의 URL을 입력합니다. 예를 들어 http://<서버 이름 또는 IP 주소>.<도메인 이름>:<포트>/cnc**에서 <서버 이름 또는 IP 주소>.<도메인 이름>은** Configuration Manager 서버의 FQDN(정규화된 도메인 이름)을 나타내고 **<포트>**는 설치하는 동안 선택한 포트를 나타냅니다.

2 Configuration Manager 설치 후 마법사에서 정의한 사용자 이름과 비밀번호를 입력합니다.

3 **로그인**을 클릭합니다. 로그인하면 사용자 이름이 화면의 오른쪽 위에 표시됩니다.

4 (권장) 구조적 LDAP 서버에 연결한 후 Configuration Manager 관리자가 시스템에 액세스할 수 있도록 LDAP 사용자에게 관리자 역할을 할당합니다. Configuration Manager 시스템에서 사용자에게 역할을 할당하는 방법에 대한 자세한 내용은 *HP Universal CMDB Configuration Manager 사용자 안내서*에서 "사용자 관리"를 참조하십시오.

로그아웃

세션을 완료하면 무단 입력을 방지하기 위해 웹 사이트에서 로그아웃하는 것이 좋습니다.

로그아웃하려면 페이지의 맨 위에 있는 **로그아웃**을 클릭합니다.

참고: 기본 세션 만료 시간은 30분입니다.

Configuration Manager의 JMX 콘솔 액세스

문제 해결이나 특정 구성의 수정을 위해 JMX 콘솔에 액세스해야 하는 경우가 있습니다.

JMX 콘솔에 액세스하려면 다음을 수행합니다.

1. http://<서버 이름 또는 IP 주소>:<포트>/cnc/jmx-console에서 JMX 콘솔을 엽니다. 포트는 Configuration Manager 설치 중에 구성된 포트입니다.
2. 기본 사용자 자격 증명을 입력합니다. 이것은 Configuration Manager에 로그인할 때 사용하는 사용자 자격 증명과 동일합니다.

5

추가 사용 사례

이 장의 내용은 다음과 같습니다.

시스템 간에 Configuration Manager 설치 복사

데이터베이스 스키마를 건드리지 않고 동일한 UCMDB 서버에 연결한 상태에서 시스템 간에 Configuration Manager의 설치를 전송하려면 다음 절차를 사용해야 합니다.

1 **<Configuration Manager 설치 디렉터리>\cnc\bin** 폴더에서 edit-server-0.bat 명령을 수행합니다.

2 포트(예: JMX 포트)를 포함하여 사용자가 찾는 모든 매개 변수를 기록합니다.

3 원본 시스템에서 Configuration Manager 서버를 중지합니다. (원본 시스템이 Windows 시스템에 설치된 경우에는 Configuration Manager 서비스를 중지하면 됩니다).

4 대상 시스템에 Configuration Manager를 설치합니다.

   ➤ Windows에서: **setup-win64.msi** 파일을 실행합니다(설치 미디어의 **\windows** 폴더에 있음).

   ➤ Linux에서: 40페이지의 "Configuration Manager 설치"의 지침을 따릅니다.

5 설치 후 마법사가 시작되면 이를 취소합니다.

6 원본 시스템의 이전 설치 디렉터리에서 모든 파일을 대상 시스템의 새로운 설치 위치로 복사합니다.

7 대상 시스템의 **client-config.properties** 및 **resources.properties**(**\conf** 폴더에 있음)에서 호스트 이름을 대상 시스템 이름으로 변경합니다.

참고: 대상 시스템이 원본 시스템과 다른 도메인에 있는 경우 **lwssofmconf.xml** 파일에서 이전 도메인 참조도 수정합니다.

---

8 대상 시스템에서 **bin/create-windows-service.bat** 파일을 실행하여 Windows 서비스를 생성합니다. 사용할 수 있는 옵션을 표시하도록 **-h** 플래그를 설정하고 필요한 경우 원본 시스템 서비스에서 기록한 매개 변수(단계 2에서 기록한 매개 변수)를 사용합니다. 도메인 이름 매개 변수는 server-0을 사용합니다. 기본값을 사용한 경우의 명령은 다음과 같습니다.

c:\HP\cnc920\bin>create-windows-service.bat -j 39900 -n server-0 -r 39600

9 대상 시스템에서 Configuration Manager 서버를 시작합니다.

설치 후 포트 번호 변경

1 Configuration Manager 서버를 중지합니다.

2 **<Configuration Manager 설치 디렉터리>\servers\server-0** 폴더의 내용을 백업합니다.

3 **<Configuration Manager 설치 디렉터리>\servers\server-0** 폴더를 삭제합니다.

4 **-h** 플래그가 포함된 **create-node.bat** 스크립트를 실행하여 사용할 수 있는 옵션을 확인합니다. 필요한 모든 포트 번호를 유틸리티에 전달합니다.

5 대상 시스템의 **client-config.properties** 및 **resources.properties**(**\conf** 폴더에 있음)에서 포트를 새 HTTP 포트 번호로 변경합니다.

6 **<Configuration Manager 설치 디렉터리>\bin** 폴더에 있는 **edit-server-0.bat** 스크립트를 실행합니다.

7 (Windows 시스템의 경우) 열린 HP Universal CMDB Configuration Manager 속성 창에서 Java 탭을 클릭하고 **jmx.http.port** 및 **com.sun.management.jmxremote.port** 설정을 새로운 포트 번호로 변경합니다.

8 대상 시스템에서 Configuration Manager 서비스를 시작합니다.

시스템 간에 시스템 설정 복사

1 원본 시스템에서 Configuration Manager를 엽니다. **시스템** > **설정**으로 이동하여 **ZIP 파일로 구성 집합 내보내기** 버튼을 클릭합니다.

내보내기 전에 관련 구성 항목 옆의 확인란을 취소하여 일부 특정 구성을 제외할 수 있습니다.

2 내보낸 구성을 대상 시스템에 복사합니다.

3 대상 시스템에서 Configuration Manager를 엽니다. **시스템** > **설정**으로 이동하여 **구성 집합 가져오기** 버튼을 클릭합니다.

백업 및 복원

완전히 새로운 설치가 필요할 수 있는 실패 유형에서 복구하기 위해서는 Configuration Manager의 설치를 백업할 수 있습니다.

백업

다음 정보를 백업합니다.

- Configuration Manager 설치 디렉터리의 **conf** 및 **security** 하위 폴더. 이 작업은 시스템이 실행 중인 동안 작동을 중단하지 않고서 수행할 수 있습니다.
- 데이터베이스 스키마

복원(Windows 시스템에서)

이 절차는 시스템에 Configuration Manager 설치가 없는 새로운 시스템에서 수행해야 합니다.

1. 다음과 같이 자동 모드에서 **setup-win64.msi** 파일(설치 미디어의 **\windows** 폴더에 있음)을 실행하여 대상 시스템에 Configuration Manager를 설치합니다.

   ```
   msiexec /i setup-win64.msi TARGETDIR=path\to\install\dir /passive
   ```

2. **conf** 및 **security** 디렉터리를 복원합니다. 백업에 사용한 방법과 같은 방법으로 복원합니다. 단계 1에서 수행한 설치에 의해 생성된 디렉터리를 덮어씁니다.
3. 데이터베이스 스키마를 복원합니다. 다른 데이터베이스 서버에 복원하는 경우, 새로운 데이터베이스 서버 이름과 일치하도록 **database.properties** 파일(**conf** 디렉터리에 있음)에서 **url** 속성을 수정해야 합니다.
4. **create-windows-service** 유틸리티(사용할 수 있는 옵션을 확인할 수 있는 **-h** 플래그 포함)를 사용하여 Windows 서비스를 생성합니다.
5. Configuration Manager 서버를 시작합니다.

복원(Linux 시스템에서)

1 **setup.bin** 파일(설치 미디어에 위치)을 실행하여 대상 시스템에 Configuration Manager를 설치합니다. 자세한 내용은 40페이지의 "Configuration Manager 설치"를 참조하고 설치 후 마법사의 첫 번째 단계에서 설치를 취소합니다. 모든 파일이 배포되지만 시스템 구성이 취소됩니다.

2 **conf** 및 **security** 디렉터리를 복원합니다. 백업에 사용한 방법과 같은 방법으로 복원합니다. 단계 1에서 수행한 설치에 의해 생성된 디렉터리를 덮어씁니다.

3 데이터베이스 스키마를 복원합니다. 다른 데이터베이스 서버에 복원하는 경우, 새로운 데이터베이스 서버 이름과 일치하도록 **database.properties** 파일(**conf** 디렉터리에 있음)에서 **url** 속성을 수정해야 합니다.

4 Configuration Manager 서버를 시작합니다.

6

고급 구성

이 장의 내용은 다음과 같습니다.

고급 데이터베이스 연결 옵션

데이터베이스 배포를 지원하기 위해 보다 고급 데이터 연결 속성을 필요로 하는 경우 설치 후 마법사가 완료되면 해당 옵션을 지정할 수 있습니다.
Configuration Manager는 벤더의 JDBC 드라이버가 지원하고 데이터베이스 연결 URL을 사용하여 구성할 수 있는 모든 데이터베이스 연결 옵션을 지원합니다.
고급 옵션을 구성하려면 **<Configuration Manager 설치 디렉터리 >\conf\database.properties** 파일에서 **jdbc.url** 속성을 편집합니다.

참고: Linux 시스템에서 고급 구성을 수행할 때 다음을 수행합니다.

- 명령에서 슬래시 방향을 정방향(/) 슬래시로 변경합니다.
- 스크립트 실행 시 **.bat**를 **.sh**로 바꿉니다.

다음은 Microsoft SQL Server의 고급 옵션 예입니다.

- **Windows (NTLM) 인증.** Windows 인증을 적용하려면 database.properties 파일의 JTDS 연결 URL에 도메인 속성을 추가합니다. 인증할 Windows 도메인을 지정합니다.

  예:

  ```
  jdbc:jtds:sqlserver://myServer:1433/myDatabase;sendStringParametersAsUnicode
  =false;domain=myDomain
  ```

- **SSL.** SSL을 사용하여 MS SQL Server 연결에 보안을 설정하는 방법에 대한 자세한 내용은 http://jtds.sourceforge.net/faq.html을 참조하십시오.

다음은 Oracle Database Server의 고급 옵션 예입니다.

- **Oracle URL.** Oracle 기본 드라이버의 연결 URL을 지정합니다. 유효한 Oracle 서버 이름 및 SID를 포함합니다. 또는 **Oracle RAC**를 사용 중인 경우 Oracle RAC 구성 세부 내용을 지정합니다.

  참고: 기본 Oracle JDBC URL 형식 구성에 대한 자세한 내용은 http://www.orafaq.com/wiki/JDBC#Thin_driver를 참조하십시오. Oracle RAC의 URL 구성에 대한 자세한 내용은 http://download.oracle.com/docs/cd/B28359_01/java.111/e10788/rac.htm을 참조하십시오.

- **SSL.** SSL을 사용하여 Oracle 연결에 보안을 설정하는 방법에 대한 자세한 내용은 다음 설명을 참조하십시오.
  - http://download.oracle.com/docs/cd/E11882_01/network.112/e10746/asojbdc.htm#ASOAG9604
  - http://download.oracle.com/docs/cd/E11882_01/java.112/e16548/clntsec.htm#insertedID6

데이터베이스 구성 - MLU(다국어 유닛) 지원

이 섹션에서는 지역화를 지원하는 데 필요한 데이터베이스 설정에 대해 설명합니다.

Oracle 서버 설정

다음은 Oracle 서버에 필요한 설정입니다.

옵션	지원	권장	비고
문자 집합	WE8ISO8859P1; UTF8,AL32UTF8	AL32UTF8	

Microsoft SQL Server 설정

다음은 Microsoft SQL Server에 필요한 설정입니다.

옵션	지원	권장	비고
데이터 정렬	대/소문자 구분 안 함. HP Universal CMDB 이진 정렬 및 대/소문자 구분을 지원하지 않습니다. 탁음/반탁음 기호, 가나 또는 전자/반자 설정의 조합과 함께 사용되는 대/소문자 구분 안 함 정렬만 지원됩니다.	데이터 정렬 설정 대화 상자를 사용하여 데이터 정렬을 선택합니다. 이진 확인란은 선택하지 마십시오. 탁음/반탁음 기호, 가나, 전자/반자 구분은 해당 데이터 언어 요구 사항에 따라 선택해야 합니다. 선택한 언어는 Windows 국가별 설정 언어와 동일해야 합니다.	데이터 정렬 로캘 및 기본 영어 정의에만 제한됩니다.
데이터 정렬 데이터베이스 속성	서버 기본값		

참고:

모든 언어: **<Language>_CI_AS**는 최소 필수 옵션입니다.
예를 들어, 일본어에서 가나 구분 및 전자/반자 구분 옵션을 선택하려는 경우 권장되는 옵션은 **Japanese_CI_AS_KS_WS** 또는 **Japanese_90_CI_AS_KS_WS**입니다. 이 권장 사항은 일본어 문자가 탁음/반탁음 기호 구분, 가나 구분, 전자/반자 구분이 가능하다는 것을 나타냅니다.

- **탁음/반탁음 기호 구분(_AS).** 탁음/반탁음 기호가 있는 문자와 탁음/반탁음 기호가 없는 문자를 구분합니다. 예를 들면, **a**와 가 서로 다릅니다. 이 옵션을 선택하지 않으면 Microsoft SQL Server는 정렬할 때 탁음/반탁음 기호가 있는 문자와 탁음/반탁음 기호가 없는 문자를 동일한 것으로 간주합니다.
- **가나 구분(_KS).** 일본어의 두 가지 가나 문자, 즉 히라가나와 가타가나를 구분합니다. 이 옵션을 선택하지 않으면 Microsoft SQL Server는 정렬할 때 히라가나 문자와 가타가나 문자를 동일한 것으로 간주합니다.
- **전자/반자 구분(_WS).** 동일한 문자가 싱글 바이트 문자와 더블 바이트 문자로 표시될 때 이를 구분합니다. 이 옵션을 선택하지 않으면 Microsoft SQL Server는 정렬할 때 문자의 싱글 바이트 표시와 더블 바이트 표시를 동일한 것으로 간주합니다.

SSO(Single Sign-On)

HP LWSSO 기술을 사용하여 Configuration Manager와 UCMDB 간 Single sign-on이 수행됩니다. 자세한 내용은 113페이지의 "LW-SSO(Lightweight Single Sign-On Authentication) 일반 참조"를 참조하십시오.

이 섹션의 내용은 다음과 같습니다.

Configuration Manager와 UCMDB 간 LW-SSO 사용

일부 Configuration Manager 사용자는 UCMDB에 대한 로그인 권한도 갖습니다. Configuration Manager는 편의를 위해 UCMDB 사용자 인터페이스에 대한 직접 링크를 제공합니다(**관리** > **UCMDB Foundation** 선택). Configuration Manager에 로그인한 후 UCMDB에 로그인하지 않아도 되는 SSO(Single Sign-On)를 사용하려면 Configuration Manager와 UCMDB 모두 LW-SSO가 활성화되어 있고 동일한 initString을 사용하여 작동 중이어야 합니다. 이 작업이 배포 관리자 설치 과정의 일부로 이미 수행되지 않았다면 수동으로 수행해야 합니다.

LW-SSO를 사용하려면 다음을 수행합니다.

1 Configuration Manager 설치 디렉터리에서 **\conf\lwssofmconf.xml** 파일을 편집합니다.

2 다음 섹션을 찾습니다.

```
enableLWSSO enableLWSSOFramework="true"
```

값이 **true**인지 확인합니다.

3 다음 섹션을 찾습니다.

```
lwssoValidation  id="ID000001">
<domain> </domain>
```

<**domain**> 뒤에 Configuration Manager 서버 도메인을 입력합니다.

4 다음 섹션을 찾습니다.

<initString="This string should be replaced"></crypto>

"This string should be replaced"를 LW-SSO로 통합할 모든 신뢰 응용 프로그램에서 사용되는 공유 문자열로 바꿉니다.

5 다음 섹션을 찾습니다.

<!--multiDomain>
<trustedHosts>
<DNSDomain>This value should be replaced by your application domain</DNSDomain>
<DNSDomain>This value should be replaced by domain of other application</DNSDomain>
</trustedHosts>
</multiDomain-->

참고: 두 번째 DNSDomain은 Configuration Manager 및 다른 응용 프로그램이 서로 다른 도메인에 위치해 있는 경우에만 포함되어야 합니다.

주석 맨 앞의 문자를 지우고 (This value should be replaced by your application domain 또는 This value should be replaced by domain of other application 대신) DNSDomain 요소에 모든 서버 도메인을 입력합니다(필요한 경우). 이 목록에는 70페이지의 단계 3에서 입력한 서버 도메인이 포함되어야 합니다.

6 변경된 파일을 저장하고 서버를 다시 시작합니다.

7 웹 브라우저를 실행하고 다음 주소를 입력합니다.
http://<UCMDB server address>.<domain_name>:8080/jmx-console.

JMX 콘솔 인증 자격 증명을 입력합니다. 기본값은 다음과 같습니다.

- 로그인 이름 = **sysadmin**
- 비밀번호 = **sysadmin**

8 **UCMDB-UI**에서 **LW-SSO Configuration**을 선택하여 JMX MBEAN 보기 페이지를 엽니다.

9 **setEnabledForUI** 메서드를 선택하고 값을 **true**로 설정한 후 **Invoke**를 클릭합니다.

10 **setDomain** 메서드를 선택합니다. UCMDB 서버의 도메인 이름을 입력하고 **Invoke**를 클릭합니다.

11 **setInitString** 메서드를 선택합니다. 71페이지의 단계 4에서 Configuration Manager에 대해 입력한 initString을 입력하고 **Invoke**를 클릭합니다.

12 Configuration Manager와 UCMDB가 서로 다른 도메인에 있는 경우 **addTrustedDomains** 메서드를 선택하고 UCMDB 및 Configuration Manager 서버의 도메인 이름을 입력합니다. **Invoke**를 클릭합니다.

13 설정 메커니즘에 저장된 LW-SSO 구성을 보려면 **retrieveConfigurationFromSettings** 메서드를 선택하고 **Invoke**를 클릭합니다.

14 실제 로드된 LW-SSO 구성을 보려면 **retrieveConfiguration** 메서드를 선택하고 **Invoke**를 클릭합니다.

Operations Orchestration에서 LW-SSO 구성

Configuration Manager 및 OO(Operations Orchestration) 양쪽에서 LW-SSO가 사용된 경우, Configuration Manager에 로그온한 사용자는 사용자 이름과 비밀번호(시스템 관리자용)를 제공하지 않고도 웹 계층을 통해 Operations Orchestration에 로그온할 수 있습니다.

참고:

- 다음 절차에서 <OO_HOME>은 Operations Orchestration 홈 디렉터리를 나타냅니다.
- LW-SSO는 Operations Orchestration 및 Configuration Manager에 로그온하는 데 사용되는 계정의 이름이 같아야 하지만 비밀번호는 달라도 됩니다.
- LW-SSO에서는 Operations Orchestration의 계정이 내부 계정이 아니어야 합니다.

Operations Orchestration에서 LW-SSO를 구성하려면 다음을 수행합니다.

1 RSCentral 서비스를 중지합니다.

2 **<OO_HOME>\Central\WEB-INF\applicationContext.xml**에서 아래와 같이 LWSSO_SECTION_BEGIN과 LWSSO_SECTION_END 간에 가져오기를 활성화합니다.

```
<!--  LWSSO_SECTION_BEGIN-->
        <import resource="CentralLWSSOBeans.xml"/>
<!--  LWSSO_SECTION_END -->
```

3 **<OO_HOME>\Central\WEB-INF\web.xml**에서 아래와 같이 LWSSO_SECTION_BEGIN과 LWSSO_SECTION_END 간에 모든 필터 및 매핑을 활성화합니다.

```
<!-- LWSSO_SECTION_BEGIN  -->

<filter>
        <filter-name>LWSSO</filter-name>
        <filter-
    class>com.iconclude.dharma.commons.util.http.DharmaFilterToBeanProx
    y
        </filter-class>
        <init-param>
            <param-name>targetBean</param-name>
            <param-value>dharma.LWSSOFilter</param-value>
        </init-param>
   ......
   </filter>
<!-- LWSSO_SECTION_END -->

<!-- LWSSO_SECTION_BEGIN-->
   <filter-mapping>
      <filter-name>LWSSO</filter-name><url-pattern>/*</url-pattern>
   </filter-mapping>
<!--LWSSO_SECTION_END -->

<!-- LWSSO_SECTION_BEGIN-->
    <filter-mapping>
          <filter-name>LWSSO2Acegi</filter-name><url-pattern>/*</url-pattern>
    </filter-mapping>
    <filter-mapping>
          <filter-name>dharmaLWSSOGroupsFilter</filter-name><url-
    pattern>/*</url-pattern>
          </filter-mapping>
<!--LWSSO_SECTION_END -->
```

4 **<OO_HOME>\Central\conf\lwssofmconf.xml**에서 다음 두 매개 변수를 편집합니다.

- 도메인: OO 서버의 도메인 이름
- initString: OO LW-SSO 구성의 initString 값과 같아야 함(최소 길이: 12자). 예: smintegrationlwsso

예:

```
<webui>
<validation>
      <in-ui-lwsso>
       <lwssoValidation id="ID000001">
            <domain>asia.hpqc.net</domain>
            <crypto cipherType="symmetricBlockCipher"
                                    engineName="AES" paddingModeName="CBC"
keySize="256"  encodingMode="Base64Url"
                                    initString=" smintlwsso "></crypto>
       </lwssoValidation>
      </in-ui-lwsso>
</validation>
<creation>
       <lwssoCreationRef id="ID000002">
            <lwssoValidationRef refid="ID000001"/>
            <expirationPeriod>600000</expirationPeriod>
       </lwssoCreationRef>
</creation>
</webui>
```

5 구성이 적용되도록 RSCentral 서비스를 다시 시작합니다.

Identity Manager 인증 수행

이 작업은 Identity Manager 인증을 허용하도록 HP Universal CMDB Configuration Manager를 구성하는 방법에 대해 설명합니다.

Identity Manager를 사용하고 HP Universal CMDB Configuration Manager를 추가할 예정이면 이 작업을 수행해야 합니다.

이 작업의 단계는 다음과 같습니다.

➤ 75페이지의 "사전 준비 사항"

➤ 75페이지의 "Identity Manager를 허용하도록 HP Universal CMDB Configuration Manager 구성"

사전 준비 사항

Configuration Manager Tomcat 서버는 Tomcat Java(AJP13) 커넥터를 통해 Identity Manager의 보호를 받는 웹 서버(IIS 또는 Apache)에 연결되어야 합니다.

Tomcat Java (AJP13) 커넥터 사용에 대한 자세한 내용은 Tomcat Java (AJP13) 문서를 참조하십시오.

Identity Manager를 허용하도록 HP Universal CMDB Configuration Manager 구성

IIS6을 사용하여 Tomcat Java (AJP13)를 구성하려면 다음을 수행합니다.

1 사용자 이름을 포함하는 개인 설정 헤더/콜백을 보내도록 Identity Manager를 구성하고, 헤더의 이름을 요청합니다.

2 **<Configuration Manager 설치 디렉터리>\conf \lwssofmconf.xml** 파일을 열고 **in-ui-identity-management**로 시작하는 섹션을 찾습니다.

예:

```
<in-ui-identity-management enabled="false">
  <identity-management>
 <userNameHeaderName>sm-user</userNameHeaderName>
  </identity-management>
</in-ui-identity-management>
```

a 주석 문자를 지워 기능을 활성화합니다.

b **enabled="false"**를 **enabled="true"**로 바꿉니다.

c **sm-user**를 단계 1에서 요청한 헤더 이름으로 바꿉니다.

3 **<Configuration Manager 설치 디렉터리>\conf\client-config.properties** 파일을 열고 다음 속성을 편집합니다.

   a **bsf.server.url**을 Identity Manager URL로 변경하고 포트를 Identity Manager 포트로 변경합니다.

   bsf.server.url=http://< Identity Manager URL>:< Identity Manager 포트 >/bsf

   b **bsf.server.services.url**을 HTTP 프로토콜로 변경하고 포트를 원래의 Configuration Manager 포트로 변경합니다.

   bsf.server.services.url=http://<Configuration Manager URL>:<Configuration Manager 포트>/bsf

Windows 2003 운영 체제에서 IIS6을 사용하여 Configuration Manager의 ID 관리를 구성하기 위한 Java Connector 사용의 예

이 예제 작업은 Windows 2003 운영 체제에서 실행되는 IIS6을 사용하여 Configuration Manager의 ID 관리를 구성하는 Java Connector를 설치 및 구성하는 방법에 대해 설명합니다.

Windows 2003에서 실행 중인 IIS6에 대해 Java Connector를 설치하고 구성하려면 다음을 수행합니다.

1 Java Connector의 최신 버전(예: **djk-1.2.21**)을 Apache 웹 사이트에서 다운로드합니다.

   a http://www.apache.org/dist/tomcat/tomcat-connectors/jk/binaries/win64/를 클릭합니다.

   b 최신 버전을 선택합니다.

   c **amd64** 디렉터리에서 **isapi_redirect.dll** 파일을 다운로드합니다.

2 이 파일을 **<Configuration Manager 설치 디렉터리>\tomcat\bin\win32** 아래에 저장합니다.

3 isapi_redirect.dll과 동일한 디렉터리에 **isapi_redirect.properties**라는 새 텍스트 파일을 만듭니다.

이 파일의 내용은 다음과 같습니다.

```
# Configuration file for the Jakarta ISAPI Redirector
# The path to the ISAPI Redirector Extension, relative to the website
# This must be in a virtual directory with execute privileges
extension_uri=/jakarta/isapi_redirect.dll
# Full path to the log file for the ISAPI Redirector
log_file=<Configuration Manager installation directory>\servers
\server-0\logs\isapi.log
# Log level (debug, info, warn, error or trace)
log_level=info
# Full path to the workers.properties file
worker_file==<Configuration Manager installation directory>\tomcat
\conf\workers.properties.minimal
# Full path to the uriworkermap.properties file
worker_mount_file==<Configuration Manager installation directory>\tomcat
\conf\uriworkermap.properties
```

4 **<Configuration Manager 설치 디렉터리>\tomcat\conf**에 **workers.properties.minimal**이라는 새 텍스트 파일을 만듭니다.

이 파일의 내용은 다음과 같습니다.

```
# workers.properties.minimal -
#
# This file provides minimal jk configuration
# properties needed to
# connect to Tomcat.
#
# Defining a worker named ajp13w and of type ajp13
# Note that the name and the type do not have to
# match.
    worker.list=ajp13w
    worker.ajp13w.type=ajp13
    worker.ajp13w.host=localhost
    worker.ajp13w.port=8009
#END
```

5 **<Configuration Manager 설치 디렉터리>\tomcat\conf**에 **uriworkermap.properties**라는 새 텍스트 파일을 만듭니다.

이 파일의 내용은 다음과 같습니다.

```
# uriworkermap.properties - IIS
#
# This file provides sample mappings for example:
# ajp13w worker defined in workermap.properties.minimal
# The general syntax for this file is:
# [URL]=[Worker name]
/cnc=ajp13w
/cnc/*=ajp13w
/bsf=ajp13w
/bsf/*=ajp13w
#END
```

중요: Configuration Manager에는 두 개의 규칙이 있어야 합니다. 새 구문을 사용하면 두 규칙을 다음과 같은 하나의 규칙으로 통합할 수 있습니다.

/cnc|/*=ajp13w

---

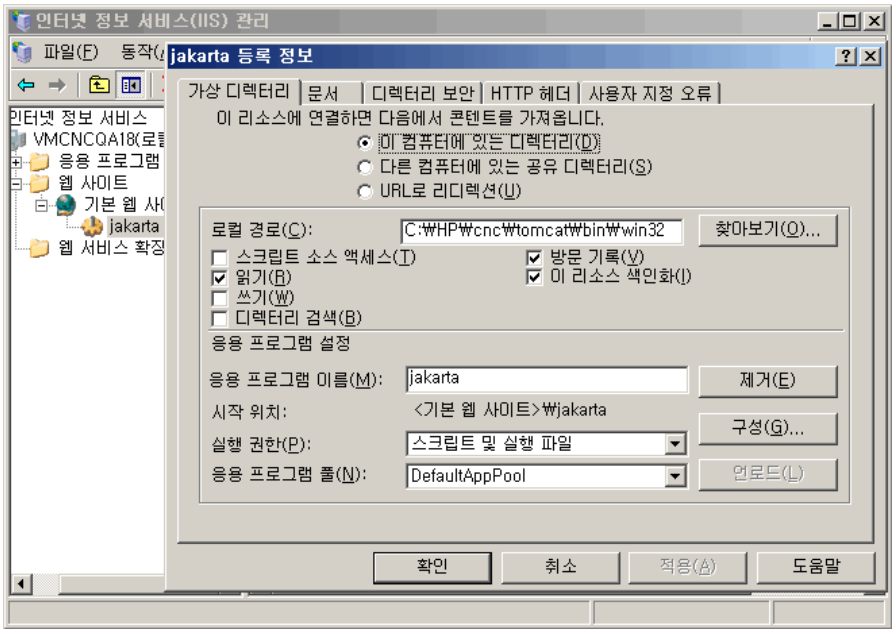
6 IIS 구성에서 해당 웹 사이트 개체에 가상 디렉터리를 만듭니다.

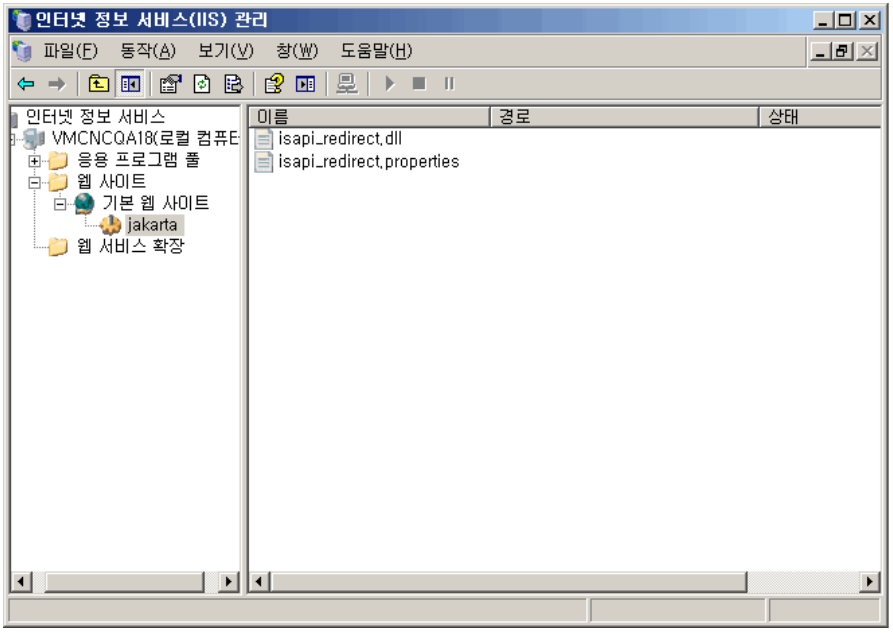
a Windows 시작 메뉴에서 **설정** > **제어판** > **관리 도구** >**IIS(인터넷 정보 서비스) 관리자**를 엽니다.

b 오른쪽 창에서 **<로컬 컴퓨터 이름>\웹 사이트\<사용자의 웹 사이트 이름>**을 마우스 오른쪽 버튼으로 클릭하고 **새로 만들기\가상 디렉터리**를 선택합니다.

c 디렉터리에 **Jakarta**라는 별칭을 지정하고 로컬 경로를 isapi_redirect.dll을 포함하는 디렉터리로 설정합니다.

IIS 관리자의 창은 다음과 유사합니다.





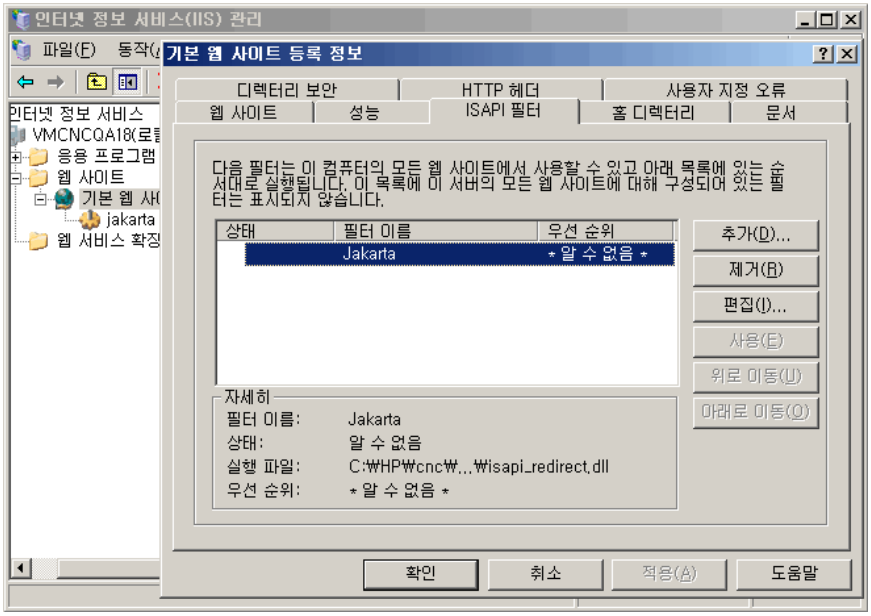
7 **isapi_redirect.dll**을 ISAPI 필터로 추가합니다.

a **<사용자의 웹 사이트 이름>**을 마우스 오른쪽 버튼으로 클릭하고 **속성**을 선택합니다.

b **ISAPI 필터** 탭을 선택하고 **추가** 버튼을 클릭합니다.

c 필터 이름 **Jakarta**를 선택하고 **isapi_redirect.dll**을 찾아봅니다. 필터가 추가되어 있지만 아직 활성화되지 않았습니다.

구성 창은 다음과 유사합니다.



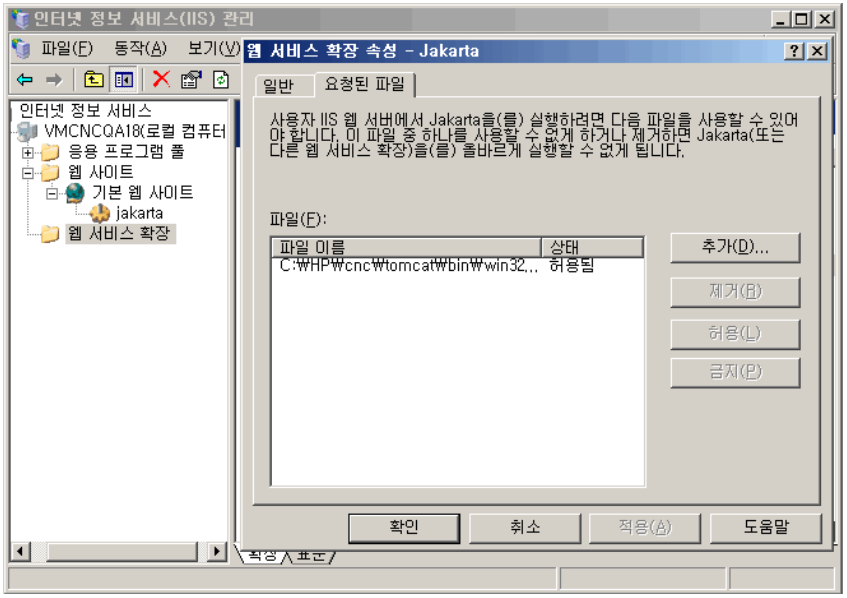
d **적용** 버튼을 클릭합니다.

8 새 웹 서비스 확장을 정의하고 허용합니다.

a **<로컬 시스템 이름>\웹 서비스 확장** 항목을 마우스 오른쪽 버튼으로 클릭하고 **새 웹 서비스 확장 추가** 메뉴 항목을 선택합니다.

b 새 웹 서비스 확장의 이름을 **Jakarta**로 지정하고 **isapi_redirect.dll** 파일을 찾아봅니다.

참고: 확인 버튼을 클릭하기 전에 **확장 상태를 [허용됨]으로 설정** 확인란을 선택합니다.



9 IIS 웹 서버를 다시 시작하고 웹 서비스를 통해 응용 프로그램에 액세스합니다.

IPv6 지원

Configuration Manager는 고객 관련 URL에 대해서만 IPv6 URL을 지원합니다.

IPv6 주소를 사용하여 Configuration Manager로 작업하려면 다음을 수행합니다.

1 운영 체제가 IPv6 및 IPv4를 모두 지원하는지 확인합니다. 자세한 내용은 해당 운영 체제의 문서를 참조하십시오.

2 **<Configuration Manager 설치 디렉터리>/conf** 폴더에 위치한 **client-config.properties** 파일을 열고 다음 값을 편집합니다.

   ➤ **bsf.server.url** 매개 변수의 값을 변경하고 호스트 이름을 사용하는지 확인합니다. 예:

   bsf.server.url=http://mycomputer:8080/bsf

   ➤ **bsf.server.services.url** 매개 변수의 값을 변경하고 Configuration Manager URL이 호스트 이름 주소인지 확인합니다. 예:

   bsf.server.services.url=http://<Configuration Manager 호스트 이름>:<Configuration Manager 포트>/bsf

3 Tomcat **servers\server-0\conf\server.xml** 파일을 열고 다음 값을 편집합니다.

   ➤ **address="[::]"**를 다음 태그에 추가하여 IPv6 주소를 SHUTDOWN hook에 추가합니다.

   <Server port="8005" shutdown="SHUTDOWN" **address="[::]"** >

   ➤ HTTP 커넥터를 복제합니다. 두 번째 커넥터에는 IPv6 [::] 주소를 추가합니다. 예:

```
<Connector port="8180" protocol="HTTP/1.1"
       connectionTimeout="20000"
       redirectPort="8443" />
<Connector port="8180" protocol="HTTP/1.1" address="[::]"
       connectionTimeout="20000"
       redirectPort="8443" />
```

➤ AJP 커넥터를 복제합니다. 두 번째 커넥터에는 IPv6 [::] 주소를 추가합니다. 예:

```
<Connector port="8009" protocol="AJP/1.3" redirectPort="8443"  address="[::]" />

<Connector port="8009" protocol="AJP/1.3" redirectPort="8443" />
```

4 다음과 같이 useIPv6="true" 환경 변수를 서버에 추가합니다.

<**Configuration Manager 설치 디렉터리**>/**bin** 폴더에 있는 **edit_server-0.bat** 파일을 엽니다. Java 탭에서 Java 옵션에 -DuseIPv6 속성을 추가합니다.

5 서버를 다시 시작합니다.

LDAP

LDAP는 Configuration Manager 내에서 구성할 수 있습니다. 자세한 내용은 *HP Universal CMDB Configuration Manager 사용자 안내서*에서 "시스템 설정"을 참조하십시오.

강화

이 섹션의 내용은 다음과 같습니다.

참고: 업그레이드 후 SSL 구성을 다시 수행해야 합니다. 자세한 내용은 37페이지의 "Configuration Manager 업그레이드"를 참조하십시오.

Configuration Manager 강화

이 섹션에서는 안전한 Configuration Manager 응용 프로그램의 개념을 소개하고 보안을 구현하는 데 필요한 계획 및 아키텍처에 대해 살펴봅니다. 다음 섹션의 시스템 강화 주제로 진행하기 전에 이 섹션을 읽는 것이 좋습니다.

Configuration Manager는 안전한 아키텍처의 일부가 될 수 있도록 설계되었으며, 따라서 보안 위협을 처리할 능력이 있습니다.

강화 지침은 보다 안전한(강력한) Configuration Manager를 구현하는 데 필요한 구성에 대해 다루고 있습니다.

제공되는 강화 정보는 강화 절차를 시작하기에 앞서 강화 설정 및 권장 사항에 익숙해져야 할 Configuration Manager 관리자를 주 대상으로 합니다.

다음은 시스템을 강화하기 위해 권장되는 준비 사항입니다.

- 일반적인 네트워크의 보안 위험/보안 상태를 평가하고, Configuration Manager를 네트워크에 가장 잘 통합하는 방법을 결정할 때 평가의 결과를 활용합니다.
- Configuration Manager 기술 프레임워크 및 Configuration Manager 보안 기능을 이해합니다.
- 강화 지침을 모두 검토합니다.
- 강화 절차를 시작하기 전에 Configuration Manager가 완벽하게 작동하고 있는지 확인합니다.
- 각 섹션에서 강화 절차 단계를 순서대로 따릅니다.

중요:

- 강화 절차는 이들 섹션에 제공된 지침만 구현하고, 그 밖의 다른 곳에서 언급된 강화 단계는 수행하지 않는다는 가정을 기반으로 합니다.
- 강화 절차가 특정한 분산 아키텍처에 초점을 맞추고 있는 경우에는 이것이 사용자 조직의 요구 사항을 충족하는 최적의 아키텍처임을 의미하지는 않습니다.
- 다음 섹션에 포함된 절차는 Configuration Manager 전용 시스템에서 수행되는 것으로 가정합니다. Configuration Manager 외에 다른 목적으로 시스템을 사용하면 문제가 발생할 수 있습니다.
- 이 섹션에서 제공되는 강화 정보는 시스템에 대해 보안 위험 평가를 실시하기 위한 가이드로 사용할 수 없습니다.

데이터베이스 비밀번호 암호화

데이터베이스 비밀번호는 **<Configuration Manager 설치 디렉터리 >\conf\database.properties** 파일에 저장되어 있습니다. 비밀번호를 암호화하려면 기본 암호화 알고리즘이 FIPS 140-2의 표준을 준수해야 합니다.

암호화는 키를 통해 수행됩니다. 그리고 이 키 자체가 마스터 키라고 하는 다른 키를 사용하여 암호화됩니다. 두 키 모두 동일한 알고리즘을 사용하여 암호화됩니다. 암호화 프로세스에 사용되는 매개 변수에 대한 자세한 내용은 87페이지의 "암호화 매개 변수"를 참조하십시오.

주의: 암호화 알고리즘을 변경하면 이전에 암호화된 모든 비밀번호를 더 이상 사용할 수 없습니다.

데이터베이스 비밀번호의 암호화를 변경하려면 다음을 수행합니다.

1 **<Configuration Manager 설치 디렉터리>\conf \encryption.properties** 파일을 열고 다음 필드를 편집합니다.

   ➤ **engineName.** 암호화 알고리즘의 이름을 입력합니다.

   ➤ **keySize.** 선택한 알고리즘에 대한 마스터 키 크기를 입력합니다.

2 **generate-keys.bat** 스크립트를 실행하여 **cnc920\security\encrypt_repository** 디렉터리를 만들고 암호화 키를 생성합니다.

3 **bin\encrypt-password** 유틸리티를 실행하여 비밀번호를 암호화합니다. 사용할 수 있는 옵션을 확인하도록 **-h** 플래그를 설정합니다.

4 비밀번호 암호화 유틸리티의 결과를 복사하여 결과로 나온 암호화를 **conf\database.properties** 파일에 붙여넣습니다.

암호화 매개 변수

다음은 데이터베이스 비밀번호 암호화에 사용하는 **encryption.properties** 파일에 포함된 매개 변수입니다. 데이터베이스 비밀번호 암호화에 대한 자세한 내용은 86페이지의 "데이터베이스 비밀번호 암호화"를 참조하십시오.

매개 변수	설명
cryptoSource	암호화 알고리즘을 구현하는 인프라를 나타냅니다. 사용할 수 있는 옵션은 다음과 같습니다. ➤ **lw.** Bouncy Castle lightweight 구현 사용(기본 옵션) ➤ **jce.** Java Cryptography Enhancement(표준 Java 암호 기법 인프라)
storageType	키 저장소의 유형을 나타냅니다. 현재는 **이진 파일**만 지원됩니다.
binaryFileStorageName	마스터 키가 저장되는 파일의 위치를 나타냅니다.
cipherType	암호 유형입니다. 현재는 **symmetricBlockCipher**만 지원됩니다.
engineName	암호화 알고리즘의 이름입니다. 다음 옵션을 사용할 수 있습니다. ➤ **AES.** American Encryption Standard. 이 암호화는 FIPS 140-2를 준수합니다(기본 옵션). ➤ **Blowfish** ➤ **DES** ➤ **3DES.**(FIPS 140-2 준수) ➤ **Null**. 암호화 안 함
keySize	마스터 키의 크기입니다. 크기는 알고리즘에 의해 결정됩니다. ➤ **AES.** 128, 192, 또는 256(기본 옵션은 256) ➤ **Blowfish.** 0-400 ➤ **DES.** 56 ➤ **3DES.** 156

매개 변수	설명
encodingMode	이진 암호화 결과의 ASCII 인코딩입니다. 다음 옵션을 사용할 수 있습니다. ➤ **Base64**(기본 옵션) ➤ **Base64Url** ➤ **Hex**
algorithmModeName	알고리즘 모드입니다. 현재는 **CBC**만 지원됩니다.
algorithmPaddingName	사용된 패딩 알고리즘입니다. 다음 옵션을 사용할 수 있습니다. ➤ **PKCS7Padding**(기본 옵션) ➤ **PKCS5Padding**
jceProviderName	JCE 암호화 알고리즘의 이름입니다. **참고:** crytpSource가 **jce**일 때만 해당됩니다. **lw**의 경우 engineName이 사용됩니다.

자체 서명 인증서를 사용하여 서버 시스템에서 SSL 활성화

이 섹션에서는 SSL(Secure Sockets Layer) 채널을 사용하여 Configuration Manager가 인증 및 암호화를 지원하도록 구성하는 방법에 대해 설명합니다.

Configuration Manager는 응용 프로그램 서버로 Tomcat 7.0을 사용합니다.

참고: 모든 디렉터리 및 파일 위치는 특정 플랫폼, OS 및 설치 기본 설정에 따라 다릅니다.

---

1 사전 준비 사항

다음 절차를 시작하기 전에 **<Configuration Manager 설치 디렉터리 >\java\lib\security\tomcat.keystore**에 있는 기존 **tomcat.keystore** 파일을 제거합니다.

2 서버 키 저장소 생성

자체 서명 인증서 및 일치하는 개인키를 사용하여 키 저장소(JKS 유형)를 만듭니다.

➤ Configuration Manager 설치 디렉터리의 Java 설치 bin 디렉터리에서 다음 명령을 실행합니다.

```
keytool -genkey -alias tomcat -keyalg RSA -keystore ..\lib\
security\tomcat.keystore
```

콘솔 대화 상자가 열립니다.

➤ 키 저장소 비밀번호를 입력합니다. 비밀번호가 변경되었으면 파일에서 수동으로 변경합니다.

➤ **이름과 성이 무엇인지** 묻는 질문에 대답합니다. Configuration Manager 웹 서버 이름을 입력합니다. 사용자 조직에 따라 다른 매개 변수를 입력합니다.

➤ 키 비밀번호를 입력합니다. 키 비밀번호는 키 저장소 비밀번호와 동일해야 합니다.

hpcert라는 서버 인증서를 사용하여 **tomcat.keystore**라는 JKS 키 저장소가 만들어집니다.

3 클라이언트가 신뢰할 수 있는 저장소에 인증서 배치

컴퓨터의 Internet Explorer에서 클라이언트가 신뢰할 수 있는 저장소에 인증서를 추가합니다(**도구 > 인터넷 옵션 > 내용 > 인증서**). 이렇게 하지 않으면 Configuration Manager를 처음 사용하려고 시도할 때 이렇게 하라는 메시지가 나타납니다.

클라이언트 인증서 사용에 대한 자세한 내용은 95페이지의 "클라이언트 인증서"를 참조하십시오.

제한 사항: **tomcat.keystore**에는 서버 인증서가 하나만 있어야 합니다.

---

4 클라이언트 구성 설정 확인

Configuration Manager 설치 디렉터리의 **conf** 디렉터리에 있는 **client-config.properties** 파일을 엽니다. **bsf.server.url**의 프로토콜을 **https**로, 포트를 **8443**으로 설정합니다.

5 server.xml 파일 수정

<Configuration Manager 설치 디렉터리>\servers\server-0\conf에 있는 **server.xml** 파일을 엽니다. 주석에서

Connector port="8443"

으로 시작하는 섹션을 찾습니다. 주석 문자를 제거하여 스크립트를 활성화하고 HTTPS 커넥터에 다음 특성을 추가합니다.

keystoreFile="<tomcat.keystore 파일 위치>"(89페이지의 단계 2 참조)
keystorePass="<비밀번호>"

다음 줄을 주석 처리합니다.

<Listener className="org.apache.catalina.core.AprLifecycleListener"
SSLEngine="on" />

6 서버 다시 시작

7 서버 보안 확인

Configuration Manager 서버가 안전한지 확인하려면 웹 브라우저에 **https://<Configuration Manager 서버 이름 또는 IP 주소>:8443/cnc**를 입력합니다.

연결 설정에 실패하면 다른 브라우저를 사용하여 시도하거나 브라우저를 최신 버전으로 업그레이드합니다.

인증 기관에서 발급된 인증서를 사용하여 서버 시스템에서 SSL 활성화

CA(인증 기관)에서 발급된 인증서를 사용하려면 키 저장소가 Java 형식이어야 합니다. 다음 예는 Windows 시스템의 키 저장소를 구성하는 방법에 대해 설명합니다.

1 사전 준비 사항

다음 절차를 시작하기 전에 **<Configuration Manager 설치 디렉터리>\java\lib\security\tomcat.keystore**에 있는 기존 **tomcat.keystore** 파일을 제거합니다.

2 서버 키 저장소 생성

a CA 서명이 있는 인증서를 생성하고 Windows에 설치합니다.

b Microsoft 관리 콘솔(**mmc.exe**)을 사용하여 인증서를 ***.pfx** 파일(개인키 포함)로 내보냅니다.

➤ **pfx** 파일의 비밀번호로 사용할 문자열을 입력합니다. (키 저장소 유형을 JAVA 키 저장소로 변환할 때 이 비밀번호가 필요합니다.)
이제 **.pfx** 파일은 공개 인증서와 개인키를 포함하며 비밀번호로 보호됩니다.

c 만들어진 **.pfx** 파일을 **<Configuration Manager 설치 디렉터리>\java\lib\security** 폴더에 복사합니다.

d 명령 프롬프트를 열고 디렉터리를 **<Configuration Manager 설치 디렉터리>\bin\jre\bin**으로 변경합니다.

➤ 다음 명령을 실행하여 키 저장소 유형을 **PKCS12**에서 **JAVA** 키 저장소로 변경합니다.

```
keytool -importkeystore -srckeystore <Configuration Manager 설치 디렉터리
>\conf\security\<pfx 파일 이름> -srcstoretype PKCS12 -destkeystore
tomcat.keystore
```

소스(**.pfx**) 키 저장소 비밀번호를 묻는 메시지가 표시됩니다. 이 비밀번호는 단계 b에서 pfx 파일을 만들 때 지정한 비밀번호입니다.

3 클라이언트 구성 설정 확인

<Configuration Manager 설치 디렉터리>\cnc\conf\client-config.properties 파일을 열고 **bsf.server.url** 속성과 포트가 각각 **https** 및 **8443**으로 설정되어 있는지 확인합니다.

4 server.xml 파일 수정

<Configuration Manager 설치 디렉터리>\servers\server-0\conf에 있는 **server.xml** 파일을 엽니다. 주석에서

Connector port="8443"

으로 시작하는 섹션을 찾습니다. 주석 문자를 지우고 다음 두 줄을 추가하여 스크립트를 활성화합니다.

keystoreFile="../../java/lib/security/tomcat.keystore"
keystorePass="password" />

다음 줄을 주석 처리합니다.

<Listener className="org.apache.catalina.core.AprLifecycleListener"
SSLEngine="on" />

5 서버 다시 시작

6 서버 보안 확인

Configuration Manager 서버가 안전한지 확인하려면 웹 브라우저에 **https://<Configuration Manager 서버 이름 또는 IP 주소>:8443/cnc**를 입력합니다.

제한 사항: **tomcat.keystore**에는 서버 인증서가 하나만 있어야 합니다.

참고: 모든 디렉터리 및 파일 위치는 특정 플랫폼, OS 및 설치 기본 설정에 따라 다릅니다.

예: java/{os name}/lib

클라이언트 인증서를 사용하여 SSL 활성화

Configuration Manager 웹 서버에서 사용하는 인증서가 잘 알려진 CA(인증 기관)에서 발급된 것이면 추가 작업 없이 웹 브라우저로 인증서의 유효성을 검사할 수 있습니다.

서버 신뢰 저장소에서 신뢰하는 CA가 아닐 경우에는 CA 인증서를 서버 신뢰 저장소로 가져옵니다.

다음 예는 자체 서명 **hpcert** 인증서를 서버 신뢰 저장소(cacerts)로 가져오는 방법에 대해 설명합니다.

인증서를 서버 신뢰 저장소로 가져오려면 다음을 수행합니다.

1 클라이언트 시스템에서 **hpcert** 인증서를 찾아 **hpcert.cer**로 이름을 바꿉니다.

2 **hpcert.cer**을 **<Configuration Manager 설치 디렉터리>\java\bin** 폴더의 서버 시스템에 복사합니다.

3 서버 시스템에서 다음 명령으로 keytool 유틸리티를 사용하여 CA 인증서를 신뢰 저장소(cacerts)로 가져옵니다.

```
<Configuration Manager 설치 디렉터리>\java\bin\keytool.exe -import
-alias hp -file hpcert.cer -keystore ..\lib\security\cacerts
```

4 **server.xml** 파일(**<Configuration Manager 설치 디렉터리>\servers\server-0\conf** 폴더에 있음)을 다음과 같이 수정합니다.

   a 90페이지의 단계 5에서 설명한 대로 변경합니다.

   b 변경 직후 HTTPS 커넥터에 다음 특성을 추가합니다.

```
truststoreFile="../../java/lib/security/cacerts"
truststorePass="changeit" />
```

c clientAuth="true"를 설정합니다.

5 90페이지의 단계 7에서 설명한 대로 서버 보안을 확인합니다.

인증만을 위해 SSL 사용

이 작업은 Configuration Manager가 인증만 지원하도록 구성하는 방법에 대해 설명합니다. 이것은 Configuration Manager로 작업하는 데 필요한 최소 수준의 보안입니다.

1 88페이지의 "자체 서명 인증서를 사용하여 서버 시스템에서 SSL 활성화"에서 90페이지의 단계 6까지, 또는 91페이지의 "인증 기관에서 발급된 인증서를 사용하여 서버 시스템에서 SSL 활성화"에서 92페이지의 단계 5까지 설명한 대로 서버 시스템에서 SSL을 사용하기 위한 절차 중 한 가지를 따릅니다.

2 웹 브라우저에 http://<Configuration Manager 서버 이름 또는 IP 주소>:8180/cnc를 입력합니다.

클라이언트 인증서 인증 사용

이 작업은 Configuration Manager가 클라이언트 측 인증서 인증을 허용하도록 설정하는 방법에 대해 설명합니다.

1 88페이지의 "자체 서명 인증서를 사용하여 서버 시스템에서 SSL 활성화"에서 설명한 대로 서버 시스템에서 SSL을 사용하는 절차를 따릅니다.

2 **<Configuration Manager 설치 디렉터리>\conf\lwssofmconf.xml** 파일을 엽니다.in-client certificate로 시작하는 섹션을 찾습니다. 예:

```
<in-clientCertificate userIdentifierRetrieveField="SubjectDN"
userIdentifierRetrieveMode="FieldPart" userIdentifierRetrieveFieldPart="e" />
```

주석 문자를 지워 클라이언트 인증서 기능을 활성화합니다.

3 다음 절차에 따라 인증서에서 사용자 이름을 추출합니다.

a 매개 변수 **userIdentifierRetrieveField**는 어떤 인증서 필드에 사용자 이름이 포함되어 있는지를 나타냅니다. 옵션은 다음과 같습니다.

- **SubjectDN**
- **SubjectAlternativeName**

b 매개 변수 **userIdentifierRetrieveMode**는 사용자 이름이 해당 필드의 전체 컨텐츠로 구성되었는지 아니면 일부분으로만 구성되었는지를 나타냅니다. 옵션은 다음과 같습니다.

- **EntireField**
- **FieldPart**

c **userIdentifierRetrieveMode**의 값이 **FieldPart**이면 매개 변수 **userIdentifierRetrieveFieldPart**는 해당 필드의 어떤 부분이 사용자 이름을 구성하는지를 나타냅니다. 값은 인증서 자체에 정의된 범례를 기반으로 하는 코드 문자입니다.

4 **<Configuration Manager 설치 디렉터리>\conf\client-config.properties** 파일을 열고 다음 속성을 편집합니다.

- HTTPS 프로토콜을 사용하도록 **bsf.server.url**을 변경하고 HTTPS 포트를 88페이지의 "자체 서명 인증서를 사용하여 서버 시스템에서 SSL 활성화"에서 설명한 포트로 변경합니다.
- HTTP 프로토콜을 사용하도록 **bsf.server.services.url**을 변경하고 포트를 원래 HTTP 포트로 변경합니다.

클라이언트 인증서

이 섹션의 내용은 다음과 같습니다.

클라이언트 인증서 정보

이 섹션에서는 클라이언트 인증서 정보 및 클라이언트 인증서에서 사용자 식별자를 취득하는 방법에 대해 설명합니다.

➤ 사용자 식별자

사용자 식별자는 사용자의 ID를 확인하기 위해 사용되는 클라이언트 인증서 정보의 고유한 부분입니다.

➤ 클라이언트 인증서 기본 정보

클라이언트 인증서 기본 정보에는 다음이 포함됩니다.

인증서 필드	설명
버전	암호화된 인증서의 버전 예: 1 (0x1)
일련 번호	인증서 기관에서 각 인증서에 할당한 양의 정수 예: 0 (0x0)
서명 알고리즘	인증서에 서명하기 위해 인증 기관에서 사용되는 알고리즘에 대한 알고리즘 식별자 예: md5WithRSAEncryption
발급자	인증서를 서명 및 발급한 기관 예: CN=Issuer, C=US, ST=NY, L=New York, O=Work Organization, O=example.com

인증서 필드	설명
유효성	인증 기관이 인증서의 상태에 대한 정보 유지를 보증하는 시간 간격 ➤ **유효 기간(시작)**. 인증서 유효 기간이 시작되는 날짜를 지정합니다. 예 : Nov 25 04:34:49 2009 GMT ➤ **유효 기간(끝)**. 인증서 유효 기간이 끝나는 날짜를 지정합니다. 예 : Nov 25 04:34:49 2010 GMT
주체	주체 공용 키 필드에 저장된 공용 키와 연관된 기관
주체 공용 키 정보	공용 키를 전달하고 키에 사용되는 알고리즘을 식별하는 데 사용됨(예: RSA, DSA, Diffie-Hellman)

자세한 정보는 아래 웹사이트에서 Internet X.509 공용 키 인프라 인증서 및 CRL(인증서 폐기 목록) 프로필을 참조하십시오.

http://tools.ietf.org/html/rfc5280

➤ **주체 필드**

주체 필드(주체 구분 이름 또는 SubjectDN이라고도 함)는 공용 키와 관련된 기관을 식별합니다.

주체 필드에는 다음과 같은 관련 특성이 포함됩니다(다른 특성도 포함될 수 있음).

주체 특성	주체 특성 설명	예
CN	공통 이름	CN=Bob BobFamily
emailAddress	전자 메일 주소	*emailAddress=bob@example.com*
C	국가 이름	C=US
ST	시/도	ST=NY

주체 특성	주체 특성 설명	예
L	구/군/시 이름	L=New York
O	조직 이름	O=직장 조직
OU	조직 단위 이름	OU=관리자

주체에서 사용자 식별자를 검색하기 위해 전체 SubjectDN 필드 또는 SubjectDN 특성을 사용할 수 있습니다.

➤ 클라이언트 인증서 정보 확장

X.509 v3 인증서에 대해 정의된 확장은 추가 특성을 사용자 또는 공용 키와 연관시키고 인증 기관 간의 관계를 관리하기 위한 방법을 제공합니다. 주체 대체 이름 필드는 사용자 식별자를 포함할 수 있습니다.

➤ 주체 대체 이름 필드

주체 대체 이름 확장을 사용하면 ID를 인증서의 주체에 바인딩할 수 있습니다. ID 대신 또는 ID에 추가하여 이러한 ID를 인증서의 주체 필드에 포함할 수 있습니다.

주체 대체 이름 필드는 다음 ID를 포함할 수 있습니다.

ID	예
otherName	Other Name: Principal Name= *bobOtherAltName@example.com*
rfc822Name	RFC822 Name =*bobRFC822AltName@example.com*
dNSName	DNS Name=example1.com
x400Address	
directoryName	Directory Address: E=*bobDirAltName@example.com*, CN=bob, OU=Gold Ballads, O=Gold Music, C=US
ediPartyName	
uniformResourceIdentifier	URL=http://example.com/

ID	예
iPAddress	IP Address=192.168.7.1
registeredID	Registered ID=1.2.3.4

주체 대체 이름에서 사용자 ID를 검색하기 위해 ID 중 하나를 사용할 수 있습니다.

구성

Configuration Manager는 LW-SSO를 사용하여 클라이언트 인증서의 사용자 식별자를 활용합니다. 사용자 식별자를 활용하도록 LW-SSO를 구성하기 위해 클라이언트 인증서 핸들러에서 다음 특성이 사용됩니다.

클라이언트 인증서의 정보를 활용하기 위해 Configuration Manager에서 사용자 식별자를 검색하는 방법이 구성되어야 합니다.

다음 항목이 결정되어야 합니다.

- 사용할 필드: SubjectDN 또는주체 대체 이름?
- 전체 필드를 사용해야 합니까? 또는 필드의 일부만 사용해야 합니까?
- 입력 필드의 일부를 사용한 다음 값을 제공한 경우: SubjectDN에 대한 주체 특성을 제공하거나 주체 대체 이름에 대한 ID를 제공합니다.

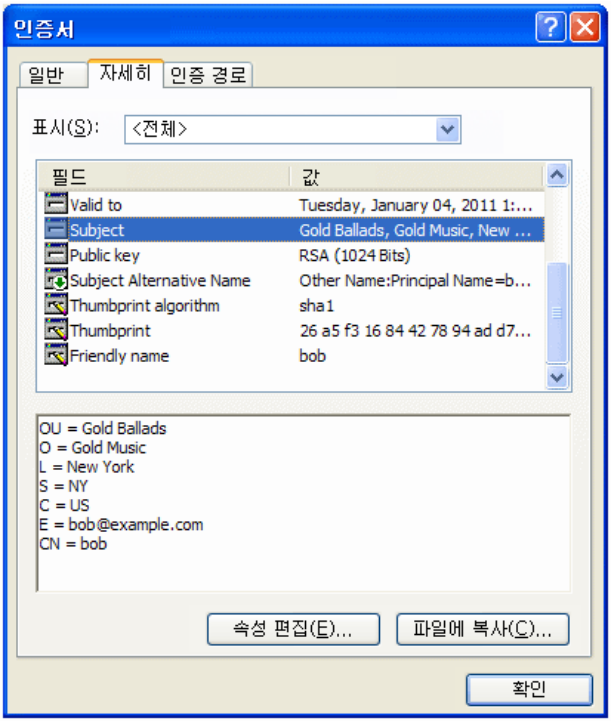
다음 특성은 LW-SSO를 구성하기 위해 클라이언트 인증서 핸들러에서 사용합니다.

특성 이름	설명
enabled	핸들러를 활성화할지 또는 비활성화할지를 지정합니다. **중요**: 값을 False로 명시적으로 설정하고 클라이언트 인증서 유효성 검사가 필요한 경우에만 핸들러를 활성화하는 것이 좋습니다.
userIdentifierRetrieveField	이 매개 변수는 어떤 인증서 필드에 사용자 식별자가 포함되어 있는지를 나타냅니다. 옵션: **SubjectDN** 또는 **SubjectAlternativeName**

특성 이름	설명
userIdentifierRetrieveMode	매개 변수 userIdentifierRetrieveMode는 사용자 식별자가 해당 필드의 전체 컨텐츠로 구성되었는지 아니면 일부분으로만 구성되었는지를 나타냅니다. 옵션: **EntireField** 또는 **FieldPart**
userIdentifierRetrieveFieldPart	**userIdentifierRetrieveMode**의 값이 **FieldPart**이면 이 매개 변수는 해당 필드의 어떤 부분이 사용자 이름을 구성하는지를 나타냅니다. 값은 인증서 자체에 정의된 범례를 기반으로 하는 코드 문자입니다. **참고**: **userIdentifierRetrieveMode**가 **FieldPart**로 설정된 경우 이 특성을 비워둘 수 없습니다. 또한 **userIdentifierRetrievField**가 **SubjectAlternativeName**으로 설정된 경우에도 비워둘 수 없습니다.

예

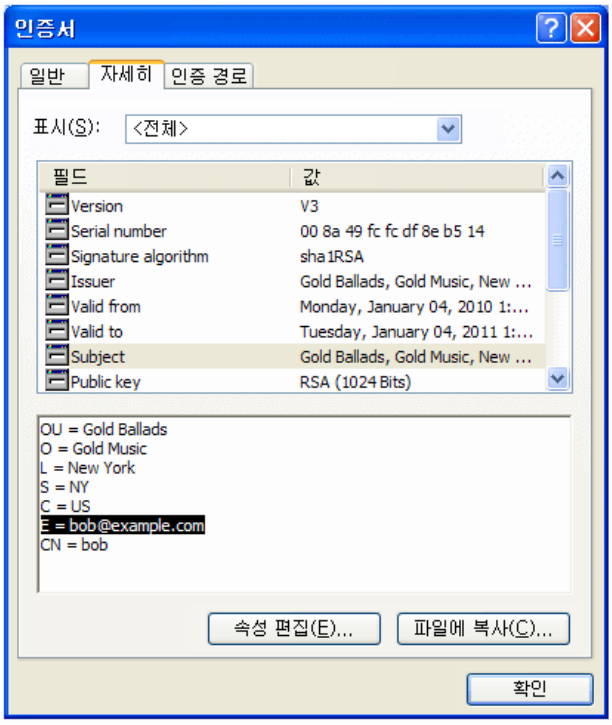
➤ **사용자 식별자를 보유하기 위해 주체를 사용합니다.**



다음 예는 전체 SubjectDN에서 사용자 식별자를 취득하도록 핸들러를 구성하는 방법을 보여줍니다.

```
<in-clientCertificate userIdentifierRetrieveField="SubjectDN"
userIdentifierRetrieveMode="EntireField" />
```

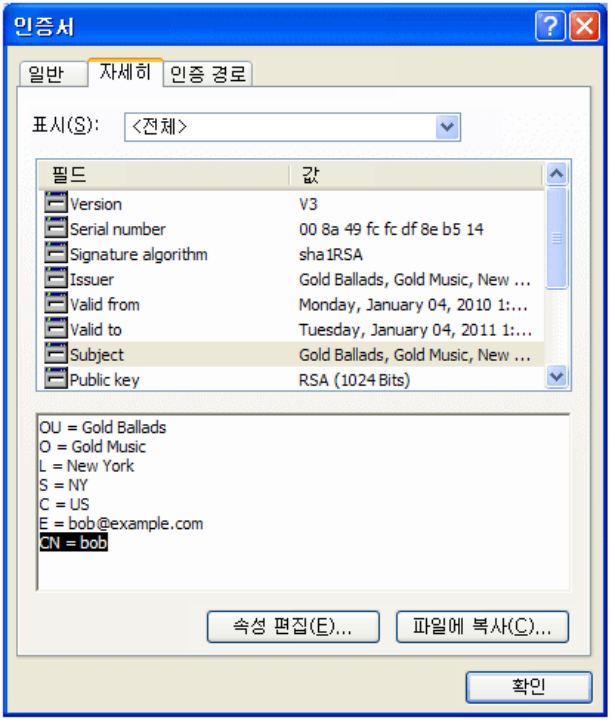
➤ **사용자 식별자를 보유하기 위해 주체의 전자 메일 필드를 사용합니다.**



클라이언트 인증서 범례에 나타나 있는 필드의 이름을 사용합니다. 다음 예는 주체의 전자 메일 필드에서 사용자 식별자를 취득하도록 핸들러를 구성하는 방법을 보여줍니다.

```
<in-clientCertificate userIdentifierRetrieveField="SubjectDN"
userIdentifierRetrieveMode="FieldPart" userIdentifierRetrieveFieldPart="E" />
```

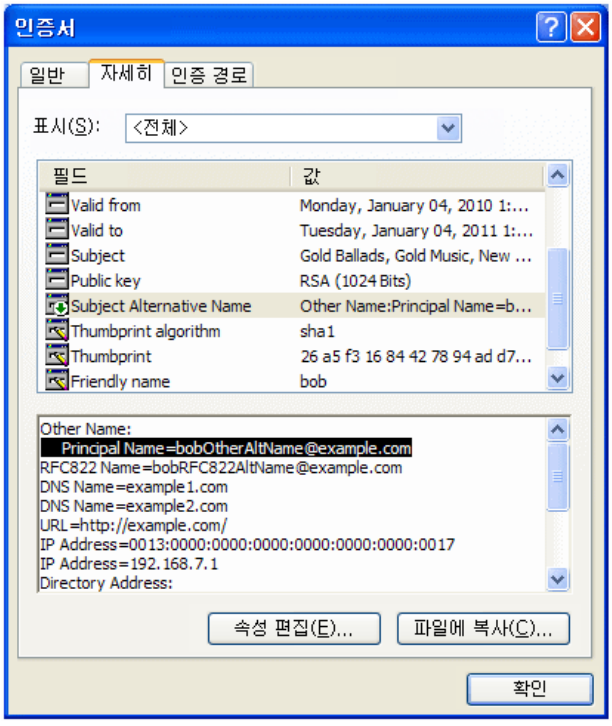
➤ **사용자 식별자를 보유하기 위해 주체의 CN 필드를 사용합니다.**



클라이언트 인증서 범례에 나타나 있는 필드의 이름을 사용합니다. 다음 예는 주체의 CN 필드에서 사용자 식별자를 취득하도록 핸들러를 구성하는 방법을 보여줍니다.

```
<in-clientCertificate userIdentifierRetrieveField="SubjectDN"
userIdentifierRetrieveMode="FieldPart" userIdentifierRetrieveFieldPart="CN" />
```

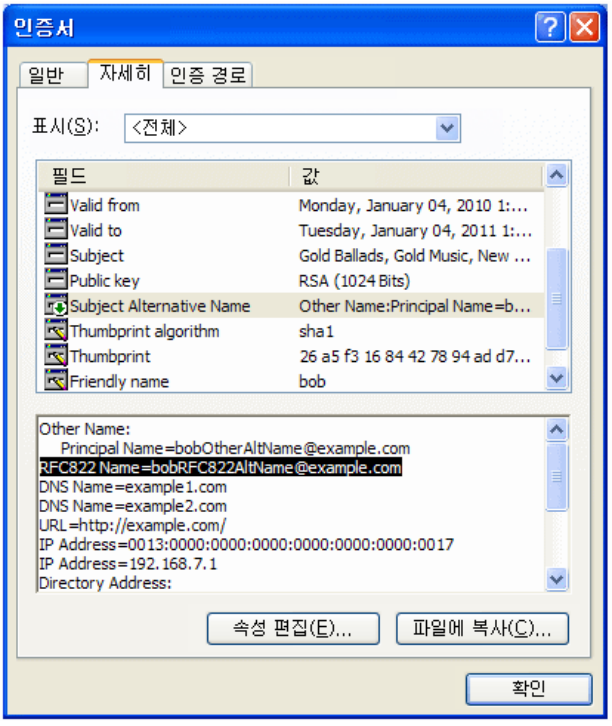
➤ **사용자 식별자를 보유하기 위해 주체 대체 이름의 otherName ID를 사용합니다.**



클라이언트 인증서 범례에 나타나 있는 ID의 이름을 사용합니다. 다음 예는 주체 대체 이름의 otherName ID에서 사용자 식별자를 취득하도록 핸들러를 구성하는 방법을 보여줍니다.

```
<in-clientCertificate userIdentifierRetrieveField="SubjectAlternativeName"
userIdentifierRetrieveMode="FieldPart" userIdentifierRetrieveFieldPart="Principal
Name" />
```

➤ **사용자 식별자를 보유하기 위해 주체 대체 이름의 rfc822Name ID를 사용합니다.**



클라이언트 인증서 범례에 나타나 있는 ID의 이름을 사용합니다. 다음 예는 주체 대체 이름의 rfc822Name ID에서 사용자 식별자를 취득하도록 핸들러를 구성하는 방법을 보여줍니다.

```
<in-clientCertificate userIdentifierRetrieveField="SubjectAlternativeName"
userIdentifierRetrieveMode="FieldPart" userIdentifierRetrieveFieldPart="Principal
Name" />
```

SSL을 사용하여 UCMDB와 함께 작동하도록 Configuration Manager 구성

SSL(Secure Sockets Layer)을 사용하여 UCMDB와 함께 작동하도록 Configuration Manager를 구성할 수 있습니다. UCMDB에서 8443 포트의 SSL 커넥터가 기본적으로 활성화됩니다.

서버 인증서를 내보내고 클라이언트 신뢰 저장소로 가져오려면 다음을 수행합니다.

1 **<UCMDB 설치 디렉터리>\bin\jre\bin**으로 이동하여 다음 명령을 실행합니다.

```
keytool -export -alias hpcert -keystore <UCMDB server dir>
\conf\security\server.keystore  -storepass hppass -file <certificatefile>
```

2 다음과 같이 인증서를 Configuration Manager 신뢰 저장소(기본 jre 신뢰 저장소)로 가져옵니다.

```
<CM_JAVA_HOME>\bin\keytool -import -trustcacerts -alias hpcert -keystore
<CM_JAVA_HOME>\lib\security\cacerts -storepass changeit -file
<certificatefile>
```

3 다음과 같이 Configuration Manager에서 UCMDB 연결 속성을 설정합니다.

시스템 > **설정** > **통합** > **UCMDB Fouccation** > **UCMDB Foundation**으로 이동합니다. 연결 전략을 **HTTPS**로, UCMDB 서버 포트를 UCMDB HTTPS 포트로, UCMDB 액세스 URL을 https://<HostName>:8443으로 설정합니다.

4 구성 집합을 저장하고 활성화합니다. Configuration Manager를 다시 시작합니다.

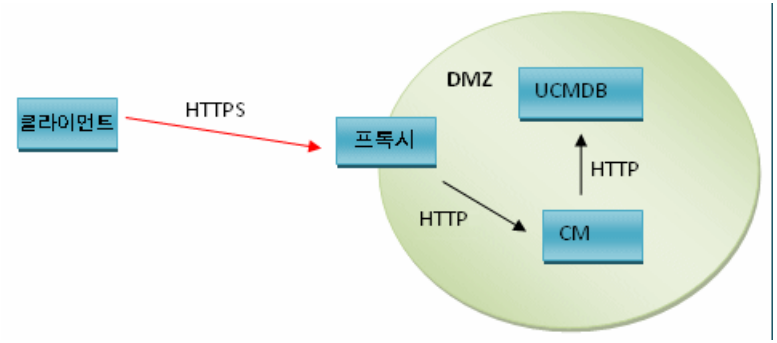
SSL(Secure Sockets Layer)을 사용하여 다른 제품(예: 로드 밸런서)과 함께 작동하도록 Configuration Manager를 구성하려면, 다음 명령을 실행하여 제품의 보안 인증서를 Configuration Manager 신뢰 저장소(기본 jre 신뢰 저장소)로 가져옵니다.

```
<CM_JAVA_HOME>\bin\keytool -import -trustcacerts -alias <alias> -keystore
<CM_JAVA_HOME>\lib\security\cacerts -storepass changeit -file <certificatefile>
```

리버스 프록시

Configuration Manager 및 UCMDB가 DMZ에 위치한 경우 리버스 프록시 서버와 함께 작동하도록 시스템을 구성하는 것이 좋습니다. 구성 단계는 리버스 프록시와 함께 작동하도록 UCMDB를 구성하는 단계와 동일합니다. Configuration Manager에 대한 액세스를 활성화하려면, 경로 **/cnc** 및 **/bsf**를 Configuration Manager가 설치된 원격 서버의 URL로 매핑해야 합니다.

다음 그림은 Configuration Manager에 대한 리버스 프록시의 구성 프로세스를 나타냅니다.



예를 들어 리버스 프록시가 Apache 서버인 경우, 아래 명령줄을 **Apache2.2\conf\extra\httpd-ssl.conf** 파일에 추가한 다음 Apache 서버를 다시 시작합니다.

```
ProxyPass /cnc http://<CM_HOSTNAME>:<CM_HTTP_PORT>/cnc
ProxyPassReverse /cnc http:// <CM_HOSTNAME>:<CM_HTTP_PORT>/cnc
ProxyPass /bsf http://< CM_HOSTNAME >:<CM_HTTP_PORT>/bsf
ProxyPassReverse /bsf http:// <CM_HOSTNAME>:<CM_HTTP_PORT>/bsf
```

리버스 프록시 종류에 따라 각기 다른 구성 단계가 필요할 수 있습니다. 자세한 내용은 프록시 서버 설명서를 참조하십시오.

Configuration Manager에 대하여 리버스 프록시를 구성하려면 다음을 수행합니다.

다음과 같이 <**Configuration Manager 설치 디렉터리**>**conf** 폴더에 있는 **client-config.properties** 파일을 업데이트합니다.

```
bsf.server.url=https://<proxy-server-name>:443/bsf
```

Apache 프록시의 기본 HTTPS 포트는 443입니다.

파트 II

부록

A

용량 제한

다음은 Configuration Manager에 대한 용량 제한입니다.

최대 보기 수	100
최대 정책 수	300
보기 당 최대 복합 CI 수	5000
최대 동시 사용자 수	50
구성 분석 모듈의 최대 복합 CI 수	1000

B

LW-SSO(Lightweight Single Sign-On Authentication) 일반 참조

이 장의 내용은 다음과 같습니다.

LW-SSO 인증 개요

LW-SSO는 한 번 로그인한 사용자에게 다시 로그인하라는 메시지를 표시하지 않고 여러 소프트웨어 시스템의 리소스에 액세스할 수 있는 권한을 주는 액세스 제어 방법입니다. 구성된 소프트웨어 시스템 그룹에 포함된 응용 프로그램은 인증을 신뢰하므로 한 응용 프로그램에서 다른 응용 프로그램으로 이동할 때 또 다시 인증 받을 필요가 없습니다.

이 섹션의 정보는 LW-SSO 버전 2.2와 2.3에 적용됩니다.

LW-SSO에 대한 문제 해결 정보는 130페이지의 "LW-SSO - 문제 해결 및 제한 사항"을 참조하십시오.

이 섹션의 주제는 다음과 같습니다.

➤ 114페이지의 멀티 도메인 기능

➤ 114페이지의 URL용 보안 토큰 가져오기 기능

LW-SSO 토큰 만료

LW-SSO 토큰의 만료 값은 응용 프로그램의 세션 유효성을 결정합니다. 따라서 만료 값은 응용 프로그램 세션 만료 값 이상이어야 합니다.

LW-SSO 토큰 만료의 권장 구성

LW-SSO를 사용하는 각 응용 프로그램은 토큰 만료를 구성해야 합니다. 권장 값은 60분입니다. 높은 수준의 보안이 필요하지 않은 응용 프로그램이라면 값을 300분으로 구성할 수도 있습니다.

GMT 시간

LW-SSO 통합에 포함된 모든 응용 프로그램은 최대 시간 차이가 15분인 동일한 GMT 시간을 사용해야 합니다.

멀티 도메인 기능

LW-SSO 통합에 포함된 모든 응용 프로그램을 다른 DNS 도메인의 응용 프로그램과 통합해야 할 경우 멀티 도메인 기능을 사용하려면 해당 응용 프로그램에 trustedHosts 설정(또는 **protectedDomains** 설정)을 구성해야 합니다. 또한 구성의 **lwsso** 요소에 올바른 도메인을 추가해야 합니다.

URL용 보안 토큰 가져오기 기능

다른 응용 프로그램에서 **URL용 보안 토큰**으로 보낸 정보를 받으려면 호스트 응용 프로그램은 구성의 **lwsso** 요소에 올바른 도메인을 구성해야 합니다.

LW-SSO 보안 경고

이 섹션에서는 LW-SSO 구성과 관련된 보안 경고에 대해 설명합니다.

➤ **LW-SSO의 기밀 InitString 매개 변수.** LW-SSO는 대칭형 암호화를 사용하여 LW-SSO 토큰을 생성하고 유효성을 검사합니다. 구성 내 **initString** 매개 변수는 비밀 키를 초기화하는 데 사용됩니다. 응용 프로그램은 토큰을 생성하고 동일한 initString 매개 변수를 사용하는 각 응용 프로그램에서 해당 토큰의 유효성을 검사합니다.

주의:

➤ **initString** 매개 변수를 설정하지 않으면 LW-SSO를 사용할 수 없습니다.

➤ **initString** 매개 변수는 기밀 정보이므로 게시, 전송 및 지속성 관점에서 처리되어야 합니다.

➤ **initString** 매개 변수는 LW-SSO를 사용하여 서로 통합된 응용 프로그램 간에만 공유되어야 합니다.

➤ **initString** 매개 변수의 길이는 12자 이상이어야 합니다.

➤ **필요한 경우에만 LW-SSO 사용.** LW-SSO는 특별히 필요한 경우가 아니면 사용하지 않아야 합니다.

➤ **인증 보안 수준.** 가장 취약한 인증 프레임워크를 사용하고 다른 통합 응용 프로그램이 신뢰한 LW-SSO 토큰을 발급하는 응용 프로그램은 모든 응용 프로그램에 대해 인증 보안 수준을 확인합니다.

강력하고 안전한 인증 프레임워크를 사용하는 응용 프로그램만 LW-SSO 토큰을 발급하는 것이 좋습니다.

- **대칭형 암호화 영향.** LW-SSO는 LW-SSO 토큰을 발급하고 유효성을 검사하는 데 대칭형 암호 기법을 사용합니다. 따라서 LW-SSO를 사용하는 응용 프로그램은 동일한 **initString** 매개 변수를 공유하는 다른 모든 응용 프로그램에서 신뢰할 토큰을 발급할 수 있습니다. 이로 인해 신뢰할 수 없는 위치에 있거나 이러한 위치에서 액세스할 수 있는 initString 매개 변수를 응용 프로그램이 공유하는 경우 잠재적인 위험이 따릅니다.

- **사용자 매핑(동기화).** LW-SSO 프레임워크는 통합된 응용 프로그램 간의 사용자 매핑을 보장하지 않습니다. 따라서 통합된 응용 프로그램은 사용자 매핑을 모니터해야 합니다. 통합된 모든 응용 프로그램 간에는 (LDAP/AD와) 동일한 사용자 레지스트리를 공유하는 것이 좋습니다.

  사용자 매핑이 실패하면 보안 위반 및 잘못된 응용 프로그램 동작이 초래됩니다. 예를 들면, 동일한 사용자 이름이 여러 응용 프로그램에서 각기 다른 실제 사용자에게 할당될 수 있습니다.

  또한, 사용자가 응용 프로그램(AppA)에 로그온한 후 컨테이너 또는 응용 프로그램 인증을 사용하는 두 번째 응용 프로그램(AppB)에 액세스하는 경우 사용자 매핑이 실패하면 해당 사용자는 AppB에 수동으로 로그온하여 사용자 이름을 입력해야 합니다. 사용자가 AppA에 로그온할 때 사용한 것과 다른 사용자 이름을 입력하면 다음 동작이 발생할 수 있습니다. 사용자가 나중에 AppA 또는 AppB에서 세 번째 응용 프로그램(AppC)에 액세스할 경우 AppA 또는 AppB에 로그온할 때 각각 사용한 사용자 이름을 사용하게 됩니다.

- **Identity Manager.** 인증 목적으로 사용하려면 Identity Manager의 보호되지 않는 모든 리소스는 LW-SSO 구성 파일의 **nonsecureURLs** 설정을 사용하여 구성되어야 합니다.

C

문제 해결

이 장의 내용은 다음과 같습니다.

일반 문제 해결 및 제한 사항

제한 사항

Configuration Manager에서 로그아웃한 다음 다시 로그인하기 전까지는 UCMDB에서 만든 새로운 CI 유형을 볼 수 없습니다.

문제 해결

문제. Node CI 유형의 **name** 특성이 모니터링되는 변경 사항의 자격을 갖추지 못해, CI 인증 동안 인증 상태로 복사되지 않습니다. UCMDB용 Content Pack 9 없이 Configuration Manager 9.20 버전이 설치된 경우 이런 현상이 발생합니다.

해결 방안. 다음 중 하나를 수행합니다.

- **name** 특성을 UCMDB CI 유형 관리자에서 모니터링되는 변경 사항의 자격을 갖추도록 수동으로 설정합니다.
- Content Pack 9를 설치합니다.

문제. Configuration Manager 서비스를 시작할 때 다음과 같은 오류 메시지가 표시됩니다.

> Windows could not start the HP Universal CMDB Configuration Manager on Local Computer. For more information, review the System Manager Event log. If this is a non-Microsoft service, contact the service vendor, and refer to service-specific error code 0.

해결 방안. 다음을 수행합니다.

1. **<Configuration Manager 설치 디렉터리>\cnc\bin**으로 이동하고 다음 명령을 실행합니다.

   edit-server-0.bat

2. Startup 탭을 선택합니다. 하단의 Mode 드롭다운 목록에서 **exe** 대신 **jvm**을 선택합니다.
3. Shutdown 탭을 선택합니다. Class 필드에서 마지막 이름을 **Boostrap**에서 **Bootstrap**으로 변경합니다.
4. **확인**을 클릭합니다.
5. 서비스를 실행합니다.

배포 관리자 - 문제 해결 및 제한 사항

배포 관리자의 문제를 해결하려면 다음 디렉터리에 위치한 이전 세션의 세션 로그를 엽니다.

%temp%\HP\ucmdb-dm\Workspace\Sessions

일반 재배포 지침

설치 중에 배포된 각 구성 요소 옆에 있는 세부 정보 버튼을 클릭하여 배포 관리자의 유효성 검사 페이지에 나타나는 경고 및 오류를 참고합니다.

배포 중에 문제가 발생하였고 해결 방안을 찾았으면 아래 단계를 수행합니다.

1 배포된 제품을 제거하고 시스템을 다시 시작합니다.

2 배포 관리자를 다시 시작하고 모든 구성을 다시 입력합니다.

배포 실패 문제

문제. 배포 중 권한 오류가 발생했습니다.

새로운 스키마를 만들 때 데이터베이스 사용자 권한에 문제가 있다는 내용이 세션 로그에 표시됩니다.

해결 방안. 새로운 데이터베이스를 만들기 위해서는 관련 권한이 있어야 합니다. 배포에 사용된 사용자 자격 증명이 테이블 공간 및 스키마 생성에 충분한지 확인합니다.

문제. UCMDB에서 스키마/데이터베이스 구성에 실패했습니다.

배포 관리자가 스키마 또는 데이터베이스를 만들지 못했다는 내용이 세션 로그에 표시됩니다.

해결 방안:

참고: (데이터베이스 서버 유형에 관계없이) 새로운 UCMDB 스키마를 만들 수 없고 기존 UCMDB 기록 내역 스키마에 연결할 수 없음에 유념하십시오.

UCMDB 스키마 및 UCMDB 기록 내역 스키마가 다음과 같은 유형의 연결을 사용하지 않는지 확인합니다.

➤ UCMDB 스키마 - 새 스키마 만들기

➤ UCMDB 기록 내역 스키마 - 기존 스키마에 연결

문제. UCMDB에서 스키마/데이터베이스 구성에 실패했습니다.

스키마를 만들 수 없다는 내용이 세션 로그에 표시됩니다.

해결 방안. session.log를 열고 다음 메시지를 찾습니다.
SQL error executing statement CREATE USER <schema name>

배포 관리자의 데이터베이스 구성 페이지에서 Oracle 스키마의 이름을 지정할 때 영문자(a-z), 숫자(0-9) 및 하이픈 기호('-')만 사용하도록 합니다.

문제. 공간이 충분하지 않기 때문에 스키마를 만들 수 없습니다.

해결 방안. 스키마 또는 데이터베이스에서 여유 공간의 양을 늘립니다. Oracle 및 Microsoft에서 제공하는 표준 관리 인터페이스를 사용합니다.

문제. 다음 오류로 인하여 데이터베이스 구성에 실패했습니다.
NT AUTHORITY\ANONYMOUS LOGON - Could not connect to database.

UCMDB 데이터베이스 구성을 위해 NTLM 인증을 사용하여 MSSQL 서버를 선택할 때, 데이터베이스 구성이 실패하고 배포 오류가 발생합니다.

해결 방안. 로컬 호스트 시스템(NTLM 인증이 지원되는 유일한 위치)에 UCMDB를 배포합니다.

문제. 새 데이터베이스를 만들 때 Configuration Manager 데이터베이스 구성에 실패했습니다.

배포 관리자 세부 정보 창에 다음 오류 메시지가 나타납니다.

Failed to create Oracle schema due to error: ORA-01031: insufficient privileges

또는

Failed to create a schema to the database: machineName.
Reason: ORA-01919: role 'RESOURCE' does not exist

해결 방안. 데이터베이스 사용자에게 다음 역할 권한이 있는지 확인합니다.

- 연결
- 리소스

문제. 대상 호스트 시스템에 디스크 공간이 충분하지 않아 배포를 실행하지 못했습니다.

해결 방안. 대상 호스트 시스템에 로그인하고 배포에 필요한 만큼의 충분한 디스크 공간이 있는지 확인합니다.

- UCMDB에는 1GB의 여유 공간이 필요함
- Configuration Manager에는 1GB의 여유 공간이 필요함
- DDMA에는 1GB의 여유 공간이 필요함

참고: 특정 제품 요구 사항 외에도 임시 파일 처리를 위해 1GB의 여유 공간이 추가로 필요합니다.

문제. Ping UCMDB 유틸리티에 실패했습니다.

이 유틸리티는 Configuration Manager 시스템에서 실행되며 기존 UCMDB 인스턴스에 대한 연결을 사용할 수 있는지 확인합니다. session.log를 열고 다음 메시지를 찾습니다.
Failed to test connection due to error: java.net.ConnectException: Connection refused: connect.

해결 방안:

- 대상 UCMDB의 8080 포트가 Windows 방화벽에 의해 차단되지 않도록 확인합니다.
- Configuration Manager 시스템에서 UCMDB 서버를 액세스할 수 있는지 확인하고 UCMDB 배포가 성공적으로 완료되어 실행 중인지 확인합니다.

사용할 수 없는 호스트 시스템 연결

문제. RPC Unavailable 또는 알 수 없는 오류가 발생합니다.

연결 테스트 버튼을 누르면 RPC Unavailable 오류가 발생합니다.

해결 방안. 호스트 이름이 올바르지 않은 경우 이를 정정하고, WMI 서비스 및 Server 서비스가 실행 중인지 확인하고 Windows 방화벽이 WMI 인터페이스에 대한 액세스를 차단하지 않도록 확인합니다.

Windows 방화벽을 비활성화하거나 또는 활성화한 방화벽 예외를 원격 관리 액세스에 추가합니다.

이렇게 하려면 **방화벽** 제어판을 열고 **인바운드 규칙을 선택합니다.** 파일 및 프린터, WMI 규칙 및 8080 포트를 모두 활성화합니다.

연결 테스트 실패

문제. 액세스가 거부되었습니다.

사용자 이름 또는 비밀번호가 잘못되었거나 DNS 설정이 유효하지 않거나 배포에서 사용된 사용자 이름에 대상 호스트 시스템에 대한 관리 자격 증명이 없기 때문에 액세스가 거부되었습니다.

해결 방안. 지정된 사용자 자격 증명이 올바르고 사용자에게 대상 호스트 시스템에 대한 관리 자격 증명이 있는지 확인합니다.

응용 프로그램 액세스 실패

문제. 성공적인 배포 후 응용 프로그램(UCMDB 또는 Configuration Manager)에 대한 액세스에 실패했습니다.

해결 방안. 다음 UCMDB 및 Configuration Manager 서비스가 존재하고 실행 중인지 확인합니다.

- **UCMDB_Server** 서비스
- **HPUCMDBCMoasisSNAPSHOTserver0** 서비스

세션 디렉터리에 위치한 배포 로그에서 오류를 검토합니다.

LW-SSO를 사용할 수 없음

문제. 성공적인 배포 - LW-SSO 기능을 사용할 수 없습니다.

해결 방안. LW-SSO init 문자열 및 도메인이 UCMDB 및 Configuration Manager에서(해당되는 경우 OO에서도) 동일한지 확인합니다.

다음 방법을 사용하여 제품에서 LW-SSO 구성 설정을 검토합니다.

- Configuration Manager **lwssofmconf.xml** 파일을 열고 도메인 및 init 문자열 정의를 확인합니다. 이 파일은 **<Configuration Manager 설치 디렉터리 >\conf** 폴더에 있습니다.
- UCMDB - UCMDB를 열고 **관리자 > 관리 > 인프라 설정 관리자**를 선택합니다.

서로 다른 DNS 도메인을 사용하는 호스트 시스템에 Configuration Manager와 UCMDB가 모두 존재하는 경우, **신뢰할 수 있는 도메인** 설정이 두 DNS 도메인을 모두 포함하고 있고 양쪽 제품에서 활성화되어 있는지 확인합니다.

배포에 관한 추가 정보를 얻으려면 배포 관리자를 디버그 모드에서 활성화하면 됩니다. 디버그 모드는 배포에 대한 추가 정보를 제공합니다.

디버그 모드를 활성화하려면 다음을 수행합니다.

1. 배포 관리자를 실행한 후 브라우저 창을 열고 주소 표시줄에 %temp%를 입력합니다.
2. **hp\ucmdb-dm** 폴더로 이동합니다.

3 텍스트 편집기에서 **ini** 파일을 열고 파일의 마지막 줄에 다음 속성을 추가합니다.

Ddebug.mode=true

4 **%temp%\HP\ucmdb-dm\ucmdb-dm.exe**를 사용하여 배포 관리자를 실행합니다.

Configuration Manager 액세스- 문제 해결 및 제한 사항

제한 사항

➤ Configuration Manager Tomcat 서버에서 시간을 변경할 때마다 서버의 시간을 업데이트하려면 서버를 다시 시작해야 합니다.

문제 해결

문제. **시스템** > **설정**에서 구성 집합을 변경한 후 서버가 시작되지 않습니다.

해결 방안. 이전 구성 집합으로 되돌립니다. 다음 절차에 따릅니다.

1 다음 명령을 실행하여 마지막으로 활성화된 구성 집합의 ID를 찾습니다.

<Configuration Manager 설치 디렉터리>\bin\export-cs.bat <database properties> --history

여기서 **<database properties>는 <Configuration Manager 설치 디렉터리>\conf\database.properties** 파일의 위치를 지정하거나 각 데이터베이스 속성을 지정하여 설정할 수 있습니다. 예:

cd <Configuration Manager 설치 디렉터리>\bin export-cs.bat -p ..\conf\database.properties --history

2 다음 명령을 실행하여 마지막 구성 집합을 내보냅니다.

```
<Configuration Manager 설치 디렉터리>\bin\export-cs.bat <database
properties> <configuration set ID> <dump file name>
```

여기서 <**configuration set ID**>는 이전 단계에 나온 구성 집합 ID이고 <**dump file**>은 구성 집합을 저장하는 데 사용된 임시 파일의 이름입니다. 예를 들어, ID가 **491520**인 구성 집합을 **mydump.zip** 파일로 내보내려면 다음과 같이 입력합니다.

```
cd <Configuration Manager 설치 디렉터리>\bin export-cs.bat -p
..\conf\database.properties -i 491520 -f mydump.zip
```

3 Configuration Manager 서비스를 중지합니다.

4 다음 명령을 실행하여 이전 구성 집합을 가져오고 활성화합니다.

```
<Configuration Manager 설치 디렉터리>\bin\import-cs.bat
<database properties> -i <dump file name> --activate
```

문제. UCMDB 연결에 오류가 있습니다.

해결 방안. 다음 중 한 가지가 원인일 수 있습니다.

- UCMDB 서버가 다운되었습니다. UCMDB가 완전히 실행되면(UCMDB 서버의 상태가 **실행 중**임을 확인) Configuration Manager를 다시 시작합니다.
- UCMDB 서버가 실행 중이지만 Configuration Manager 연결 자격 증명 또는 URL이 잘못되었습니다. Configuration Manager를 시작합니다. **시스템 > 설정 > 통합 > UCMDB Foundation > UCMDB Foundation**으로 이동하여 설정을 변경하고 새로운 구성 집합을 저장합니다. 구성 집합을 활성화하고 서버를 다시 시작합니다.

문제. LDAP 연결 설정이 잘못되었습니다.

해결 방안. 이전 구성 집합으로 되돌립니다. LDAP 구성을 올바르게 설정하고 새 구성 집합을 활성화합니다.

문제. Configuration Manager에서 UCMDB 클래스 모델의 변경 내용이 감지되지 않습니다.

해결 방안. Configuration Manager 서버를 다시 시작합니다.

문제. Configuration Manager 로그에 **UCMDB 예외 시간 제한 만료** 오류가 있습니다.

해결 방안. 이 문제는 UCMDB 데이터베이스가 오버로드되었을 때 발생합니다. 문제를 해결하려면 다음과 같이 연결 시간 제한을 증가시킵니다.

1 **UCMDBServer\conf** 폴더에 jdbc.properties 파일을 만듭니다.

2 다음 텍스트를 입력합니다. QueryTimeout=<시간(초)>

3 UCMDB 서버를 다시 시작합니다.

문제. Configuration Manager에서 관리할 보기를 추가할 수 없습니다.

해결 방안. 관리할 보기가 추가되면 UCMDB에 새 TQL이 만들어집니다. 활성 TQL의 최대 제한에 도달하면 보기를 추가할 수 없습니다. 인프라 설정 관리자에서 다음 설정을 변경하여 UCMDB의 활성 TQL 제한을 증가시킵니다.

- 서버의 최대 활성 TQL 수
- 최대 고객 활성 TQL 수

문제. HTTPS 서버 인증서가 유효하지 않습니다.

해결 방안. 다음 중 한 가지가 원인일 수 있습니다.

- 인증서의 유효일이 지났습니다. 새 인증서를 받아야 합니다.
- 인증서의 인증 기관이 신뢰할 수 있는 기관이 아닙니다. 신뢰할 수 있는 루트 인증 기관 목록에 해당 인증 기관을 추가합니다.

문제. Configuration Manager 로그인 페이지에서 로그인하면 로그인 오류 또는 액세스 거부 페이지가 표시됩니다.

해결 방안. 다음 중 한 가지가 원인일 수 있습니다.

- 사용자 이름이 인증 공급자(외부/공유 LDAP)에 정의되지 않았을 수 있습니다. 인증 공급자 시스템에 사용자를 추가합니다.
- 사용자는 정의되어 있지만 Configuration Manager에 대한 로그인 권한이 없습니다. 사용자 로그인 권한을 부여합니다. 모범 사례대로, 모든 Configuration Manager 사용자의 루트 그룹에 로그인 권한을 할당합니다.
- 이러한 해결 방법은 IDM 시스템 로그인에서 문제가 발생한 경우에도 적용됩니다.

문제. 잘못된 데이터베이스 자격 증명 입력으로 인해 Configuration Manager 서버가 시작되지 않습니다.

해결 방안. 데이터베이스 자격 증명을 변경한 후 서버가 시작되지 않으면 자격 증명이 잘못되었을 수 있습니다. (**참고**: 설치 후 마법사는 입력된 자격 증명을 자동으로 테스트하지 않습니다. 자격 증명의 유효성을 확인하려면 마법사에서 **테스트** 버튼을 클릭해야 합니다.) 데이터베이스 비밀번호를 다시 암호화하고 구성 파일에 새 자격 증명을 입력해야 합니다. 다음 절차에 따릅니다.

1 명령줄에서 다음 명령을 실행하여 업데이트된 데이터베이스 비밀번호를 암호화합니다.

```
<Configuration Manager 설치 디렉터리>\bin\encrypt-password.bat p
<password>
```

암호화된 비밀번호가 반환됩니다.

2 암호화된 비밀번호({ENCRYPTED} 접두사 포함)를 **<Configuration Manager 설치 디렉터리>\conf\database.properties**의 **db.password** 매개 변수에 복사합니다.

문제. DNS가 올바르게 구성되지 않은 경우 서버 IP 주소를 사용하여 로그인해야 할 수 있습니다. IP 주소를 입력하면 두 번째 DNS 오류가 발생합니다.

해결 방안. 시스템 이름을 IP 주소로 다시 바꿉니다. 예:

http://16.55.245.240:8180/cnc/라는 IP 주소를 사용하여 로그인하고

DNS 오류가 발생한 시스템 이름이 포함된 주소 (http://my.example.com:8180/bsf/secure/authenicationPointURL.jsp...)가 표시되면

http://10.0.0.1:8180/bsf/secure/authenicationPointURL.jsp...로 바꾸고

브라우저에서 응용 프로그램을 다시 시작합니다.

문제. Configuration Manager Tomcat 서버가 시작되지 않습니다.

해결 방안. 다음 중 한 가지를 시도해 봅니다.

- 설치 후 마법사를 실행하고 Configuration Manager 서버 포트를 바꿉니다.
- Configuration Manager 포트를 사용하는 다른 프로세스를 중단합니다.
- **<Configuration Manager 설치 디렉터리>\servers\server-0\conf\server.xml** 파일을 편집하고 해당 포트를 업데이트하여 Configuration Manager 구성 파일에서 포트를 수동으로 변경합니다.
  - HTTP (8180): 줄 69
  - HTTPS (8443): 줄 71, 90

문제. "out of memory"라는 메시지가 표시됩니다.

해결 방안. 다음을 수행하여 서버 시작 매개 변수를 변경합니다.

1 다음 배치 파일을 실행합니다.

<Configuration Manager 설치 디렉터리>/bin/edit-server-0.bat

2 다음 설정을 변경합니다.

-Dapplication.ms=<inital memory pool size>
-Dapplication.mx=<maximum memory pool size>

문제. 설치 후 마법사에서 **마침**을 클릭하면 오랜 시간이 걸립니다.

해결 방안. 통합 모드로 사전 구성되지 않은 UCMDB 시스템의 경우 (데이터 양에 따라) 스키마 통합 작업에 많은 시간이 소요될 수 있습니다. 15분 정도 기다립니다. 더 이상 진행되지 않으면 설치 후 마법사를 중단하고 프로세스를 다시 시작합니다.

문제. UCMDB에서 CI의 변경 내용이 Configuration Manager에 반영되지 않습니다.

해결 방안. Configuration Manager에서 오프라인 비동기 분석 프로세스를 실행합니다. 프로세스가 UCMDB의 최신 변경 내용을 아직 처리하지 않았을 수 있습니다. 이 문제를 해결하려면 다음 중 한 가지를 시도해 보십시오.

- 몇 분 기다립니다. 분석 프로세스의 기본 실행 간격은 10분입니다. 이 간격은 **시스템 > 설정**에서 구성할 수 있습니다.
- JMX 호출을 실행하여 해당 보기에서 오프라인 분석 계산을 수행합니다.
- **관리 > 정책 > 구성 정책**으로 이동합니다. **정책 분석 다시 계산** 버튼을 클릭합니다. 모든 보기에 대한 오프라인 분석 프로세스가 호출됩니다(시간이 소요될 수 있음). 또한 한 정책을 인위적으로 변경한 다음 저장해야 할 수 있습니다.

문제. **관리 > UCMDB Foundation**을 클릭하면 UCMDB 로그인 페이지가 표시됩니다.

해결 방안. 다시 로그인하지 않고 UCMDB에 액세스하려면 SSO(Single Sign-On)를 사용해야 합니다. 자세한 내용은 70페이지의 "SSO(Single Sign-On)"를 참조하십시오. 또한 로그온한 Configuration Manager 사용자가 UCMDB 사용자 관리 시스템에 정의되어 있는지 확인합니다.

문제. 설치 후 마법사에서 UCMDB 연결을 IPv6 주소로 구성하면 **관리 > UCMDB Foundation** 메뉴 항목이 작동하지 않습니다.

해결 방안. 다음 절차에 따릅니다.

1 **시스템** > **설정** > **통합** > **UCMDB Foundation** > **UCMDB Foundation**으로 이동합니다.

2 UCMDB 액세스 URL의 IP 주소에 대괄호를 추가합니다. URL은 http://[x:x:x:x:x:x:x:x]:8080/과 같은 형태여야 합니다.

3 구성 집합을 저장하고 활성화합니다.

4 Configuration Manager를 다시 시작합니다.

LW-SSO - 문제 해결 및 제한 사항

알려진 문제

이 섹션에서는 LW-SSO 인증의 알려진 문제에 대해 설명합니다.

➤ **보안 컨텍스트**. LW-SSO 보안 컨텍스트는 특성 이름별로 하나의 특성 값만 지원합니다.

따라서 SAML2 토큰이 동일한 특성 이름에 대해 둘 이상의 값을 보내면 LW-SSO 프레임워크에서는 하나의 값만 허용됩니다.

이와 유사하게, IdM 토큰이 동일한 특성 이름에 대해 둘 이상의 값을 보내도록 구성되어 있으면 LW-SSO 프레임워크에서는 하나의 값만 허용됩니다.

➤ **Internet Explorer 7을 사용 중인 경우 멀티 도메인 로그아웃 기능**. 다음 조건에서는 멀티 도메인 로그아웃 기능이 실패할 수 있습니다.

➤ 사용 브라우저가 Internet Explorer 7이고 응용 프로그램이 로그아웃 프로시저에 4개 이상의 연속 HTTP 302 리디렉션 동사를 호출하는 경우입니다.

이러한 시나리오에서 Internet Explorer 7은 HTTP 302 리디렉션 응답을 잘못 처리하고 **Internet Explorer에서 해당 웹 페이지를 열 수 없습니다**라는 오류 페이지가 대신 표시될 수 있습니다.

이러한 문제의 해결 방법으로, 가능하면 로그아웃 시퀀스에서 응용 프로그램 리디렉션 명령의 수를 줄이는 것이 좋습니다.

제한 사항

LW-SSO 인증을 사용할 때 다음 제한 사항에 유의하십시오.

➤ **응용 프로그램에 대한 클라이언트 액세스**.

도메인이 LW-SSO 구성에 정의된 경우:

- ➤ 응용 프로그램 클라이언트는 로그인 URL에 FQDN(정규화된 도메인 이름)을 사용하여 해당 응용 프로그램에 액세스해야 합니다 (예: http://myserver.**companydomain**.com/WebApp).
- ➤ LW-SSO는 IP 주소(예: http://192.168.12.13/WebApp)를 사용하는 URL을 지원하지 않습니다.
- ➤ LW-SSO는 도메인이 없는 URL(예: http://myserver/WebApp)을 지원하지 않습니다.

LW-SSO 구성에 도메인이 정의되지 않은 경우: 클라이언트는 로그인 URL에 FQDN 없이 응용 프로그램에 액세스할 수 있습니다. 이 경우 단일 시스템에 대한 LW-SSO 세션 쿠키가 도메인 정보 없이 특별히 만들어집니다. 그러므로 이 쿠키는 브라우저에 의해 다른 쿠키로 위임되지 않고 동일한 도메인에 있는 다른 컴퓨터로 전달되지 않습니다. 이는 LW-SSO가 동일한 도메인에서 작동하지 않음을 의미합니다.

➤ **LW-SSO 프레임워크 통합.** 응용 프로그램은 사전에 LW-SSO 프레임워크 내에서 통합된 경우에만 LW-SSO 기능을 활용할 수 있습니다.

➤ **멀티 도메인 지원**.

- ➤ 멀티 도메인 기능은 HTTP 참조자를 기반으로 작동합니다. 따라서 LW-SSO는 응용 프로그램 간 링크를 지원하며 브라우저 창에 URL을 입력하는 것은 지원하지 않습니다(두 응용 프로그램이 동일한 도메인에 있는 경우는 제외).
- ➤ **HTTP POST**를 사용하는 첫 번째 도메인 간 링크는 지원되지 않습니다.

  멀티 도메인 기능은 두 번째 응용 프로그램에 대한 첫 번째 **HTTP POST** 요청은 지원하지 않습니다(**HTTP GET** 요청만 지원됨). 예를 들어, 응용 프로그램에 두 번째 응용 프로그램에 대한 HTTP 링크가 있으면 **HTTP GET** 요청은 지원되지만 **HTTP FORM** 요청은 지원되지 않습니다. 첫 번째 요청 이후의 모든 요청은 **HTTP POST** 또는 **HTTP GET** 중 하나입니다.

- LW-SSO 토큰 크기:

  한 도메인의 응용 프로그램에서 다른 도메인의 응용 프로그램으로 LW-SSO가 전송할 수 있는 정보의 크기는 그룹/역할/특성 15개로 제한됩니다(각 항목의 길이는 평균 15자로 간주함).

- 멀티 도메인 시나리오에서 보호되는 페이지(HTTPS)에서 보호되지 않는 페이지(HTTP)로 연결:

  보호되는(HTTPS) 페이지에서 보호되지 않는(HTTP) 페이지에 연결하는 경우에는 멀티 도메인 기능이 작동하지 않습니다. 이는 보호되는 리소스에서 보호되지 않는 리소스에 연결할 때 참조자 헤더가 보내지지 않는 브라우저 제한 때문입니다.
  http://support.microsoft.com/support/kb/articles/Q178/0/66.ASP 페이지의 예제를 참조하십시오.

- **SAML2 토큰.**

  - SAML2 토큰을 사용하면 로그아웃 기능이 지원되지 않습니다.

    따라서 SAML2 토큰을 사용하여 두 번째 응용 프로그램에 액세스할 경우 첫 번째 응용 프로그램에서 로그아웃한 사용자가 두 번째 응용 프로그램에서는 로그아웃되지 않습니다.

  - SAML2 토큰의 만료는 응용 프로그램의 세션 관리에 반영되지 않습니다.

    그러므로 SAML2 토큰을 사용하여 두 번째 응용 프로그램에 액세스하면 각 응용 프로그램의 세션 관리는 독립적으로 처리됩니다.

- **JAAS 영역.** Tomcat에서 JAAS 영역은 지원되지 않습니다.

- **Tomcat 디렉터리에 공백 사용.** Tomcat 디렉터리에서의 공백 사용은 지원되지 않습니다.

  Tomcat 설치 경로(폴더)에 공백이 있고(예: Program Files) LW-SSO 구성 파일이 **common\classes** Tomcat 폴더에 있는 경우 LW-SSO를 사용할 수 없습니다.

- **로드 균형 장치 구성.** LW-SSO와 함께 배포된 로드 균형 장치는 스티키 세션을 사용하도록 구성해야 합니다.

문제 해결

문제: 로그인 후 LW-SSO 쿠키가 생성되지 않습니다.

- **가능한 원인:** 비어있지 않은 도메인이 구성의 LW-SSO 요소에 잘못 정의되었습니다.
- **가능한 해결 방안**: 구성의 LW-SSO 요소에 정의된 도메인이 응용 프로그램의 도메인과 같은지 확인합니다.
- **가능한 원인:** enableSSO 함수에 매개 변수로 전달된 비어있지 않은 도메인이 올바르지 않습니다.
- **가능한 해결 방안**: enableSSO 함수에 매개 변수로 전달된 도메인이 응용 프로그램의 도메인과 같은지 확인합니다.
- **가능한 원인:** LW-SSO 구성에서 도메인을 정의할 때 로그인 URL에서 FQDN (정규화된 도메인 이름)을 사용하여 응용 프로그램에 액세스하지 않았습니다 (예: http://192.168.12.13/WebApp).
- **가능한 해결 방안**: 로그인 URL에서 FQDN(정규화된 도메인 이름)을 사용하여 응용 프로그램에 액세스해야 합니다(예: http://myserver.companydomain.com/WebApp).

문제: LW-SSO가 AutoCookieCreation 기능에 대한 쿠키를 만들지 못했습니다.

- **가능한 원인:** 도메인이 구성의 LW-SSO 요소에 올바르게 정의되어 있지 않습니다.
- **가능한 해결 방안**: 구성의 LW-SSO 요소에 정의된 도메인이 응용 프로그램의 도메인과 같은지 확인합니다.

문제: LW-SSO 토큰의 유효성이 확인되지 않습니다.

- **가능한 원인:** 두 응용 프로그램이 구성의 crypto 요소에서 다른 initString 매개 변수(또는 다른 crypto 매개 변수)를 사용합니다.
- **가능한 해결 방안**: 두 응용 프로그램에서 (LW-SSO 생성 요소의 나머지 모든 crypto 매개 변수 뿐만 아니라) 동일한 initString을 사용합니다.
- **가능한 원인:** 두 응용프로그램 간의 GMT 시간 차이가 15분보다 큽니다.

- **가능한 해결 방안**: LW-SSO 통합에 포함된 모든 응용 프로그램이 최대 시간 차이가 15분인 동일한 GMT 시간으로 설정되어 있는지 확인합니다.
- **가능한 원인:** 구성의 LW-SSO 요소에서 도메인이 비어 있는데, 사용자가 동일한 DNS 도메인을 사용하여 다른 컴퓨터에서 두 번째 응용 프로그램에 액세스합니다.
- **가능한 해결 방안**: 구성의 LW-SSO 요소에 정의된 도메인이 응용 프로그램의 도메인과 같은지 확인합니다.
- **가능한 원인:** 구성의 LW-SSO 요소에서 도메인이 정의되어 있지 않은데, 사용자가 동일한 DNS 도메인을 사용하여 다른 컴퓨터에서 두 번째 응용 프로그램에 액세스합니다.
- **가능한 해결 방안**: LW-SSO 요소에 도메인을 추가하고 도메인이 응용 프로그램의 도메인과 같은 도메인으로 정의되어 있는지 확인합니다.

문제: LW-SSO가 다중 도메인 환경에서 LW-SSO 토큰의 유효성을 검사하지 못했습니다.

- **가능한 원인:** 한 응용 프로그램의 구성에서 도메인이 LW-SSO 요소에 잘못 정의되었습니다.
- **가능한 해결 방안**: 응용 프로그램 구성의 LW-SSO 요소에 정의된 도메인은 사용중인 실제 도메인에 따라 응용 프로그램의 도메인과 동일해야 합니다.
- **가능한 원인:** 한 응용 프로그램의 구성에서 도메인이 trustedHosts 설정(또는 protectedDomains 설정)에 잘못 정의되었습니다.
- **가능한 해결 방안**: 모든 응용 프로그램 구성의 trustedHosts 설정(또는 protectedDomains 설정)에서 도메인이 올바르게 정의되어 있는지 확인합니다.
- **가능한 원인:** Internet Explorer 6.x, 7.x 또는 8.x를 사용하는 경우 LW-SSO 세션 쿠키가 차단되거나 거부됩니다.
- **가능한 해결 방안**: 컴퓨터에서 Internet Explorer 보안 영역의 "인트라넷"/"신뢰할 수 있는" 영역에 모든 LW-SSO 서버를 추가합니다(도구 > 인터넷 옵션 > 보안 > 로컬 인트라넷 > 사이트 > 고급). 이렇게 하면 모든 쿠키가 허용됩니다.

- **가능한 원인:** 일부 응용 프로그램이 구성의 crypto 요소에 다른 initString 매개 변수를 사용합니다(또는 다른 crypto 매개 변수).
- **가능한 해결 방안**: 모든 응용 프로그램에서 (LW-SSO 생성 요소의 나머지 모든 crypto 매개 변수 뿐만 아니라) 동일한 initString을 사용합니다.
- **가능한 원인:** 일부 응용 프로그램의 GMT 시간 차이가 15분보다 큽니다.
- **가능한 해결 방안**: LW-SSO 통합에 포함된 모든 응용 프로그램이 최대 시간 차이가 15분인 동일한 GMT 시간으로 설정되어 있는지 확인합니다.
- **가능한 원인:** 다중 도메인 링크가 보호되는 리소스(HTTPS)에서 보호되지 않는 리소스(HTTP)로 이동합니다.
- **가능한 해결 방안**: 도메인 간에 연결하거나 교차할 때 최초의 링크/교차 요청이 보호되는 리소스(HTTPS)에서 보호되지 않는 리소스(HTTPS)로 이동하는지 확인합니다.

IPv6 지원 - 문제 해결 및 제한 사항

제한 사항

- URL은 IP 주소를 포함할 수 없습니다.
- 운영 체제가 IPv6 및 IPv4를 모두 지원해야 합니다. IPv4 주소가 닫혀있지 않거나 지원되지 않는 경우 Configuration Manager 서버에 로그온할 수 없습니다.
- Configuration Manager Tomcat 서버에서 시간을 변경할 때마다 서버의 시간을 업데이트하려면 서버를 다시 시작해야 합니다.

문제 해결

문제. 설치하는 동안 IPv6 주소에 대한 UCMDB 연결을 구성한 후, **관리 > UCMDB Foundation** 메뉴 옵션이 작동하지 않습니다.

해결 방안. 다음을 수행합니다.

1 **시스템 > 설정 > 통합 > UCMDB Foundation > UCMDB Foundation**으로 이동합니다.

2 UCMDB 액세스 URL 필드의 IP 주소에 대괄호를 추가합니다. URL은 http://[x:x:x:x:x:x:x:x]:8080/ucmdb-ui/와 같은 형태여야 합니다.

3 구성 집합을 저장하고 활성화합니다.

4 Configuration Manager를 다시 시작합니다.

인증 - 문제 해결 및 제한 사항

이 섹션에는 알려진 인증 문제에 대해 설명합니다.

문제: 인증 지점으로 리디렉션 후 응용 프로그램에 대한 인증 동안 오류 500을 받습니다.

- **가능한 원인:** Configuration Manager WAR 및 BSF WAR이 구성의 crypto 요소에 다른 initString 매개 변수를 사용합니다(또는 다른 crypto 매개 변수).

➤ **가능한 해결 방안**: 두 응용 프로그램에서 (LW-SSO 생성 요소의 나머지 모든 crypto 매개 변수 뿐만 아니라) 동일한 initString을 사용합니다.

문제: 인증 지점으로 리디렉션 후 응용 프로그램에 대한 인증 동안 로그인 형식이 표시되지 않습니다.

해결 방안: Internet Explorer 버전 6.0, 7.0 또는 8.0 브라우저를 사용하는 경우 Configuration Manager 인증 세션 쿠키가 차단되거나 거부됩니다. 컴퓨터에서 Internet Explorer 보안 영역의 **인트라넷/신뢰할 수 있는** 영역에 Configuration Manager 서버를 추가합니다(**도구** > **인터넷 옵션** > **보안** > **로컬 인트라넷** > **사이트** > **고급**). 이렇게 하면 모든 쿠키가 허용됩니다.

문제: 인증 후 오류 403을 받습니다.

➤ **가능한 원인:** 도메인이 응용 프로그램 구성의 LW-SSO 요소에 잘못 정의되었습니다.

➤ **문제 해결 방안**: 응용 프로그램 구성의 LW-SSO 요소에 정의된 도메인이 응용 프로그램의 도메인과 같은지 확인합니다.

➤ **가능한 원인:** LW-SSO 구성에서 도메인을 정의할 때 로그인 URL에서 FQDN (정규화된 도메인 이름)을 사용하여 응용 프로그램에 액세스하지 않았습니다 (예: http://192.168.12.13/WebApp).

➤ **가능한 해결 방안**: 로그인 URL에서 FQDN(정규화된 도메인 이름)을 사용하여 응용 프로그램에 액세스해야 합니다(예: http://myserver.companydomain.com/WebApp).

문제: 인증 후 **Get Acegi User Details** 페이지가 나타납니다.

해결 방안: Internet Explorer 버전 6.0, 7.0 또는 8.0 브라우저를 사용하는 경우 Configuration Manager 인증 세션 쿠키가 차단되거나 거부됩니다. 컴퓨터에서 Internet Explorer 보안 영역의 **인트라넷/신뢰할 수 있는** 영역에 Configuration Manager 서버를 추가합니다(**도구** > **인터넷 옵션** > **보안** > **로컬 인트라넷** > **사이트** > **고급**). 이렇게 하면 모든 쿠키가 허용됩니다.