HP Universal CMDB 9.10 Configuration Manager

Windows 운영 체제용

배포 안내서

문서 릴리스 날짜: 2010년 11월
소프트웨어 릴리스 날짜: 2010년 11월

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

© Copyright 2010 Hewlett-Packard Development Company, L.P.

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

1

설치 및 구성

이 장의 내용은 다음과 같습니다.

Configuration Manager 개요

HP Universal CMDB Configuration Manager(줄여서 Configuration Manager)는 다양한 데이터 원본이 공존하고 여러 가지 제품과 응용 프로그램을 지원하는 CMS 인프라를 제어하기 위한 환경을 제공합니다. 이를 통해 CMS의 데이터를 분석하고 제어할 수 있습니다.

엔터프라이즈 네트워크 환경에서 Configuration Manager를 배포하려면 리소스 계획 및 시스템 아키텍처 설계가 뒷받침되어야 합니다. Configuration Manager을 설치하기 전에 이 섹션에서 시스템 요구 사항을 비롯한 정보를 검토하십시오.

Configuration Manager 시스템 요구 사항

서버 시스템 요구 사항

다음은 Configuration Manager 서버의 시스템 요구 사항입니다.

CPU	Intel 펜티엄 4, 쿼드코어 이상
메모리(RAM)	4GB 이상
플랫폼	x64
운영 체제	다음 64비트 Windows 운영 체제가 지원됩니다. ➤ Windows 2003 Enterprise SP2 및 R2 SP2 ➤ Windows 2008 Enterprise SP2 및 R2

데이터베이스	➤ Microsoft SQL Server 2005 SP2; 2005 Compatibility Mode 80; (모두 Enterprise Edition) ➤ Oracle 11.1.x
HP Universal CMDB	➤ HP Universal CMDB 버전 9.03(CMDB 표준 설치) 이 버전에 대한 전체 시스템 요구 사항 목록은 HP Universal CMDB 문서를 참조하십시오.

클라이언트 요구 사항

다음은 Configuration Manager을 보기 위한 클라이언트 요구 사항입니다.

브라우저	➤ Microsoft Internet Explorer 6.0, 7.0, 8.0 ➤ Mozilla Firefox 3.x
Flash Player 브라우저 플러그인	Flash Player 9 이상
화면 해상도	➤ 1024x768 이상 ➤ 1280x1024 권장
화질(해상도)	16비트 이상

권장 설치 지침

다음은 Configuration Manager 설치 옵션에 대한 지침입니다.

LDAP	다음 LDAP 환경이 지원됩니다. ➤ Active Directory ➤ SunONE 6.x
최소 권장 데이터베이스 스키마 크기	2GB

Configuration Manager 용량 제한

다음은 Configuration Manager에 대한 용량 제한입니다.

최대 보기 개수 권장 값	100
최대 정책 개수 권장 값	300
보기 당 최대 복합 CI 개수 권장 값	5000
최대 동시 사용자 수 권장 값	50

데이터베이스 또는 사용자 스키마 구성

Configuration Manager를 사용하려면 데이터베이스 스키마를 제공해야 합니다. Configuration Manager는 Microsoft SQL Server 및 Oracle Database Server를 지원합니다. 이 작업은 설치 마법사를 사용하여 Configuration Manager 데이터베이스 또는 사용자 스키마의 연결 속성을 구성하는 방법에 대해 설명합니다.

참고: Microsoft SQL Server 및 Oracle Server 시스템 요구 사항은 8 페이지의 "서버 시스템 요구 사항"을 참조하십시오.

데이터베이스를 구성하려면 다음을 수행합니다.

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

- **Microsoft SQL Server 2005**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

3 Configuration Manager 설치 마법사를 실행합니다. 자세한 내용은 12 페이지의 "Configuration Manager 설치"를 참조하십시오.

Configuration Manager 설치

이 작업은 서버에 Configuration Manager를 설치하고, 데이터베이스 연결 및 UCMDB 통합을 구성하는 방법에 대해 설명합니다. 마법사 페이지에서 **Help**를 클릭하면 설치에 대한 도움말을 볼 수 있습니다. 마법사 페이지에 대한 자세한 내용은 21 페이지의 "Configuration Manager 설치 후 구성 마법사"를 참조하십시오.

Configuration Manager를 설치하려면 다음을 수행합니다.

1 Configuration Manager DVD의 루트 디렉터리에서 **install.bat** 파일을 찾습니다.

2 파일을 두 번 클릭하여 Configuration Manager 설치 마법사를 실행합니다.

3 **Next**를 클릭하여 최종 사용자 사용권 계약 페이지를 엽니다.

4 라이센스 조건에 동의한 후 **Next**를 클릭하여 제품 설치 페이지를 엽니다.

5 설치할 제품(UCMDB 및 Configuration Manager)을 선택하고 설치 위치를 지정합니다. 사용자 지정 UCMDB 라이센스를 갖고 있는 경우 해당 확인란을 선택합니다. **Next**를 클릭하여 UCMDB 설치를 시작합니다. UCMDB 설치에 대한 자세한 내용은 *HP Universal CMDB 배포 안내서* PDF를 참조하십시오.

6 UCMDB의 설치 및 설치 후 작업이 완료되면 Configuration Manager 설치 후 구성 마법사가 자동으로 시작됩니다.

7 시작 페이지에서 **Next**를 클릭하여 데이터베이스 연결 구성 페이지를 엽니다.

8 데이터베이스 유형(Oracle 또는 Microsoft SQL Server)을 선택하고 사용자 이름과 비밀번호를 입력합니다. **Test** 버튼을 클릭하여 연결을 테스트하는 것이 좋습니다. 연결 테스트에 성공하면 **Next**를 클릭하여 응용 프로그램 서버 구성 페이지를 엽니다.

참고: 마법사가 완료된 후 고급 데이터베이스 연결 옵션을 추가로 구성할 수 있습니다. 자세한 내용은 15 페이지의 "고급 데이터베이스 연결 구성 옵션"을 참조하십시오.

9 호스트 이름을 입력하고 **Next**를 클릭하여 Windows 서비스 구성 페이지를 엽니다.

10 Configuration Manager를 Windows 서비스로 설치하려면 해당 확인란을 선택합니다. **Next**를 클릭하여 사용자 자격 증명 페이지를 엽니다.

11 관리 권한을 가진 사용자와 통합 사용자 모두에 대해 사용자 이름과 비밀번호를 입력합니다. **Next**를 클릭하여 HP UCMDB 연결 구성 페이지를 엽니다.

12 UCMDB가 이 시스템 또는 다른 시스템에 이미 설치되어 있으면 진행하기 전에 UCMDB 서버가 가동 중인지 확인하십시오.

다른 시스템에 UCMDB를 설치하려는 경우 해당 확인란을 선택하고 필요한 매개 변수를 입력해야 합니다. **Test** 버튼을 클릭하여 연결을 테스트하는 것이 좋습니다. 연결 테스트에 성공하면 **Next**를 클릭하여 설치 후 작업 요약 페이지를 엽니다.

13 설치 후 작업 요약 페이지의 정보를 검토합니다. 정보가 올바르면 **Next**를 클릭합니다.

14 완료 페이지에서 **Finish**를 클릭하여 설치 후 작업을 완료합니다.

15 이번이 UCMDB의 첫 시작이 아니면 다음과 같이 UCMDB의 열 크기를 변경해야 합니다.

a **관리** > **인프라 설정 관리자**로 이동합니다. **개체 루트** 설정을 찾아 **data**로 변경합니다. 변경 내용이 적용되도록 UCMDB에서 로그아웃했다가 다시 로그인합니다.

b **모델링** > **CI 유형 관리자**로 이동합니다. 트리에서 CI 유형으로 **data**를 선택하고 특성 탭을 선택합니다. **User Label** 특성의 **값 크기**를 900으로 변경합니다.

c **인프라 설정 관리자**로 돌아가 **개체 루트** 설정을 원래의 값으로 다시 변경합니다. 변경 내용이 적용되도록 로그아웃했다가 다시 로그인합니다.

16 UCMDB에서 데이터 흐름 관리가 이미 실행되고 있으면 기록 내역 데이터가 손상될 수 있습니다. 이 문제를 해결하려면 다음 절차를 수행합니다.

a 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**

b **UCMDB**에서 **History DB Services**를 선택합니다.

c **Fix902EndTimeRecords** 메서드를 선택합니다.

d 실제 상태 고객인 경우 Customer ID 값으로 **1**을 입력하고 **Invoke**를 클릭합니다.

e 작업에 성공하면 "History DB is updated successfully"라는 메시지가 표시됩니다.

f 인증 상태 고객인 경우 Customer ID 값으로 **100001**을 입력하고 **Invoke**를 클릭합니다.

g 작업에 성공하면 "History DB is updated successfully"라는 메시지가 표시됩니다.

고급 데이터베이스 연결 구성 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.

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 포함시킵니다. 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. 이진 정렬 및 대/소문자 구분을 지원하지 않습니다. 탁음/반탁음 기호, 가나 또는 전자/반자 설정의 조합과 함께 사용되는 대/소문자 구분 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 **ｱ**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.

Lightweight Single Sign-On 사용

일부 Configuration Manager 사용자는 UCMDB에 대한 로그인 권한도 갖습니다. Configuration Manager는 편의를 위해 UCMDB 사용자 인터페이스에 대한 직접 링크를 제공합니다(**관리** > **UCMDB 열기** 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 작업은 Configuration Manager 및 UCMDB에서 LW-SSO를 사용하는 방법에 대해 설명합니다.

LW-SSO를 사용하려면 다음을 수행합니다.

1 Configuration Manager 설치 디렉터리에서 다음 파일을 엽니다.
\servers\server-0\webapps\cnc\WEB-INF\classes\cnclwssofmconf.xml

참고: 이 파일은 Configuration Manager를 시작한 후에 생깁니다.

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-->
```

첫 부분의 주석 문자열을 지우고 (This value should be replaced by your application domain 대신) DNSDomain 요소에 Configuration Manager 서버 도메인을 입력합니다. 이 목록에는 19 페이지의 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. 19 페이지의 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.

IPv6 지원

Configuration Manager는 고객 측 URL에 대해서만 IPv6 URL을 지원합니다.

IPv6 주소를 사용하여 Configuration Manager로 작업하려면 다음을 수행합니다.

1 운영 체제가 IPv6을 지원하는지 확인합니다. 자세한 내용은 해당 운영 체제의 문서를 참조하십시오.

2 **<Configuration Manager 설치 디렉터리>**의 **conf** 디렉터리에 있는 **client-config.properties** 파일을 엽니다. **bsf.server.url** 매개 변수의 값을 대괄호로 묶인 IPv6 주소로 변경합니다. 예를 들면 다음과 같습니다.

bsf.server.url=http://[2620:0:a17:e008:d840:5b0f:2040:519c]:8080/bsf

2

Configuration Manager 설치 후 구성 마법사

이 장의 내용은 다음과 같습니다.

Configuration Manager 설치 후 구성 개요

이 장에서는 Configuration Manager 설치 후 마법사 페이지와 관련 구성 작업에 대해 자세히 살펴봅니다. 이 내용은 마법사의 모든 페이지에서 **Help**를 클릭하여 볼 수 있습니다.

데이터베이스 연결 페이지

이 섹션의 내용은 다음과 같습니다.

일반 정보

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

Configuration Manager는 Oracle과 Microsoft SQL Server의 기본 드라이버를 사용합니다. 즉 해당 데이터베이스 URL을 사용하여 구성할 수 있는 기본 드라이버 기능이 지원되면 일반적으로 모든 기본 드라이버 기능이 지원된다는 의미입니다. URL은 **database.properties** 파일에 있습니다.

참고: 고급 기능 구성은 설치 후 프로세스가 완료되고 구성 작업이 설정된 다음에 수행해야 합니다.

매개 변수

데이터베이스 연결을 설정하려면 다음 매개 변수를 정의합니다.

매개 변수	권장 값	설명
Vendor	<사용자 정의>	데이터베이스 벤더 사용 가능한 값: **Oracle** 또는 **Microsoft** HP Universal CMDB는 Configuration Manager와 동일한 설치 프로그램을 사용하거나, 또는 별도로 설치할 수 있습니다. Configuration Manager와 UCMDB를 동일한 설치 프로그램을 사용하여 동일한 시스템에 설치할 예정이면 이 매개 변수의 기본값은 UCMDB 설치 후 마법사에서 이미 선택한 데이터베이스 벤더입니다. 동일한 설치 프로그램을 사용하여 두 응용 프로그램을 설치할 때만 기본값이 설정됩니다. 별도의 설치 패키지를 사용하여 설치하는 경우에는 UCMDB가 Configuration Manager와 동일한 시스템에 설치되어 있더라도 기본값이 설치 후 마법사에 표시되지 않습니다.
Hostname	<사용자 정의>	데이터베이스 서버의 호스트 이름 Configuration Manager와 UCMDB를 동일한 시스템에 설치할 예정이면 이 매개 변수의 기본값은 UCMDB 설치 후 마법사에서 이미 선택한 데이터베이스 서버입니다. **이 값은 필수입니다.**

매개 변수	권장 값	설명
Port	<사용자 정의>	데이터베이스 수신기의 포트 Configuration Manager와 UCMDB를 동일한 시스템에 설치할 예정이면 이 매개 변수의 기본값은 UCMDB 설치 후 마법사에서 이미 선택한 데이터베이스 포트입니다. Oracle의 경우 기본값은 **1521**입니다. Microsoft SQL Server의 경우 기본값은 **1433**입니다. **이 값은 필수입니다.**
SID/DB	<사용자 정의>	Oracle SID의 이름 또는 Microsoft SQL Server 데이터베이스의 이름 Configuration Manager와 UCMDB를 동일한 시스템에 설치할 예정이면 이 매개 변수의 기본값은 UCMDB 설치 후 마법사에서 이미 선택한 데이터베이스 SID/DB입니다. **이 값은 필수입니다.**
Username	<사용자 정의>	데이터베이스에 로그인하는 데 사용되는 사용자 이름 **이 값은 필수입니다.**
Password	<사용자 정의>	데이터베이스에 로그인하는 데 사용되는 비밀번호

옵션

다음 옵션을 사용할 수 있습니다.

매개 변수	권장 값	설명
Encrypt password	<사용자 정의>	이 옵션을 선택하면 **database.properties** 파일의 비밀번호가 암호화됩니다. 보안을 위해, 텍스트 파일에 저장된 비밀번호를 암호화하는 것이 좋습니다.
Create schema objects	<사용자 정의>	이 옵션을 선택하면 Configuration Manager를 실행하는 데 필요한 스키마 개체가 만들어집니다. 설치 시 이전에 만들어져 Configuration Manager 개체로 채워진 기존 스키마를 사용하는 경우에만 이 옵션을 해제합니다.

테스트

참고: 계속하기 전에 연결 속성을 테스트하는 것이 좋습니다.

연결 속성을 테스트하려면 **Test**를 클릭합니다. 마법사가 데이터베이스 액세스를 시도하고 연결을 확인합니다. 테스트 결과가 **Test** 버튼 오른쪽에 표시됩니다.

데이터베이스에서 다양한 오류 메시지를 생성합니다. 메시지에는 일반적으로 잘못된 사용자 이름이나 비밀번호 입력과 관련된 오류 내용이 설명되어 있습니다. 계속하기 전에 오류를 반드시 수정하여 테스트에 성공해야 합니다.

응용 프로그램 서버 페이지

이 섹션의 내용은 다음과 같습니다.

일반 정보

아래에 나오는 기본 포트 번호를 사용하여 Configuration Manager 응용 프로그램 서버를 설정합니다.

매개 변수

Configuration Manager 응용 프로그램 서버를 설정하려면 다음 매개 변수를 정의합니다.

매개 변수	권장 값	설명
Hostname	<사용자 정의>	응용 프로그램 서버의 외부 이름 기본적으로 이 값은 마법사(및 Configuration Manager)를 실행 중인 시스템의 정규화된 호스트 이름입니다. Configuration Manager 응용 프로그램 서버에 앞서 웹 서버를 배포하는 경우와 같이, 일부 배포에서는 이 이름이 달라야 합니다.
Customize ports	<사용자 정의>	기본적으로 이 옵션은 선택되어 있지 않습니다. 이 옵션을 선택하면 응용 프로그램 서버의 기본 포트 번호를 사용자 지정할 수 있습니다.

매개 변수	권장 값	설명
HTTP port	<사용자 정의>	Configuration Manager 응용 프로그램 서버의 HTTP 포트 기본값: **8080** HP Universal CMDB와 동일한 시스템에 설치할 경우 기본값: **8180**
HTTPS port	<사용자 정의>	Configuration Manager 응용 프로그램 서버의 HTTPS 포트 기본값: **8443** UCMDB와 동일한 시스템에 설치할 경우 기본값: **8143**
Tomcat port	<사용자 정의>	Configuration Manager 응용 프로그램 서버 관리 포트 기본값: **8005**
AJP port	<사용자 정의>	Configuration Manager 응용 프로그램 서버 AJP(Apache Java Protocol) 포트 기본값: **8009**
JMX HTTP port	<사용자 정의>	Configuration Manager 응용 프로그램 서버 JMX HTTP 포트 기본값: **39900**
JMX remote port	<사용자 정의>	Configuration Manager 응용 프로그램 서버 JMX 원격 포트 기본값: **39600**

Windows 서비스 구성 페이지

Configuration Manager를 Windows 서비스로 설치할지 여부를 선택합니다. 이 옵션은 Windows 시스템에 설치할 경우에만 사용할 수 있습니다.

Windows 서비스는 **cnc-home/bin** 디렉터리에 있는 **create-windows-service.bat** 유틸리티를 사용하여 수동으로 설정할 수 있습니다.

사용자 자격 증명 페이지

이 섹션의 내용은 다음과 같습니다.

➤ 28 페이지의 "일반 정보"

일반 정보

다음 Configuration Manager 초기 사용자를 설정합니다.

매개 변수	권장 값	설명
Admin user	<사용자 정의>	Configuration Manager의 관리 권한을 가진 사용자 - "수퍼 유저"
Integration user	<사용자 정의>	통합 목적으로 HP Universal CMDB에서 Configuration Manager가 만든 사용자

참고: 관리 권한을 가진 사용자와 통합 사용자 모두에 대해 사용자 이름 및 비밀번호 자격 증명을 제공해야 합니다.

HP Universal CMDB 연결 페이지

이 섹션의 내용은 다음과 같습니다.

➤ 28 페이지의 "일반 정보"

➤ 29 페이지의 "매개 변수"

➤ 30 페이지의 "테스트"

일반 정보

HP Universal CMDB와의 연결 설정은 선택 사항입니다.

결합 설치에서 UCMDB와 동일한 시스템에 Configuration Manager를 설치할 경우에는 이 페이지에 언급된 정보를 제공할 필요가 없습니다.

결합 설치에서 UCMDB를 설치하지 않거나, 다른 시스템에 UCMDB를 설치하거나(로컬 호스트의 UCMDB에 연결하는 경우 포함), Configuration Manager 설치에 앞서 UCMDB를 설치할 경우 UCMDB가 가동 중이어야 하며 사용자는 이러한 연결 속성을 제공해야 합니다.

참고: UCMDB의 원격 인스턴스를 사용하여 설치할 때는 해당 인스턴스가 가동되어 실행 중이어야 합니다. 동일한 시스템에 Configuration Manager와 UCMDB를 모두 설치할 경우 이 마법사를 실행하는 동안 UCMDB를 중단해야 합니다.

매개 변수

UCMDB 연결을 설정하려면 다음 매개 변수를 정의합니다.

매개 변수	권장 값	설명
Use HP UCMDB on a different host	<사용자 정의>	Configuration Manager와 UCMDB를 다른 시스템에 설치할 때 나머지 모든 속성을 활성화하려면 이 옵션을 선택합니다.
Hostname	<사용자 정의>	UCMDB가 설치된 호스트 이름
Port	<사용자 정의>	UCMDB가 수신 중인 포트
Protocol	<사용자 정의>	HTTP 또는 HTTPS
Customer	<사용자 정의>	UCMDB 고객
Administrative username	<사용자 정의>	UCMDB sysadmin 사용자 이름
Administrative password	<사용자 정의>	UCMDB sysadmin 비밀번호

테스트

참고: 계속하기 전에 연결 속성을 테스트하는 것이 좋습니다.

연결 속성을 테스트하려면 **Test**를 클릭합니다. 마법사가 UCMDB 액세스를 시도하고 연결을 확인합니다. 테스트 결과가 **Test** 버튼 오른쪽에 표시됩니다.

UCMDB에서 다양한 오류 메시지를 생성합니다. 메시지에는 일반적으로 잘못된 사용자 이름이나 비밀번호 입력과 관련된 오류 내용이 설명되어 있습니다. 계속하기 전에 오류를 반드시 수정하여 테스트에 성공해야 합니다.

요약 페이지

이전 마법사 페이지에서 선택한 모든 내용이 표시됩니다. 모든 선택 내용이 정확한지 확인하고 필요한 경우 변경합니다. 모든 선택 내용이 올바르면 **Next**를 클릭합니다. 마법사가 구성 작업을 완료합니다.

마침 페이지

이 페이지가 Configuration Manager 설치 **후 구성** 마법사의 마지막 페이지입니다. 이제 설치 후 구성 작업이 완료되었습니다. **Finish**를 클릭하여 마법사를 닫습니다.

참고: 모든 작업이 성공적으로 완료되었더라도 **cnc-home/tmp/chp/app.log**에서 로그를 확인하는 것이 좋습니다.

3

LDAP 구성

HP UCMDB Configuration Manage는 사용자, 역할 및 권한을 관리하기 위해 LDAP를 사용합니다. 이 장에서는 LDAP의 구성 및 문제 해결 단계에 대해 설명합니다.

이 장의 내용은 다음과 같습니다.

LDAP 개요

Configuration Manager는 내부 LDAP 서버(사용자 인터페이스에서 **공유**로 식별됨)을 포함하며, 또한 구조적 LDAP 서버에 연결할 수도 있습니다. Configuration Manager는 이들 서버를 사용하여 사용자, 그룹 및 역할을 찾고 개인 설정 데이터를 저장하며 사용자를 인증합니다. 구조적 LDAP 서버와 내부 LDAP 서버를 각각 어떤 작업에 사용할지 선택할 수 있습니다.

일반적인 배포에서는 내부(공유) LDAP 서버를 사용하여 역할을 저장하고 외부(구조적) LDAP 서버를 사용하여 그 외 모두를 저장합니다.

공급자 선택

1 **Configuration Manager**에 관리자로 로그온합니다.

2 **관리** > **서버 관리** > **사용자 관리** > **사용자 관리 구성**으로 이동하여 공급자 기본 설정에 따라 다음 각각의 특성에 대해 공유 또는 외부를 선택합니다.

- 인증 공급자
- 그룹 공급자
- 개인 설정 공급자
- 역할 공급자
- 역할 관계 공급자

3 구성 집합을 저장합니다.

구조적 LDAP 연결

HP UCMDB Configuration Manager는 내부(공유) LDAP를 사용하여 최초 구성됩니다. 이 섹션에서는 구조적 LDAP 서버에 연결하는 단계에 대해 설명합니다.

이 섹션의 내용은 다음과 같습니다.

- 33 페이지의 "LDAP 연결 구성"
- 33 페이지의 "그룹 및 사용자 공급자 구성"
- 36 페이지의 "구성 집합 활성화"
- 36 페이지의 "사용자에게 권한 할당"
- 37 페이지의 "외부 LDAP에 인증 공급자 설정"
- 37 페이지의 "LDAP 인증서 가져오기"

LDAP 연결 구성

이 섹션에서는 Configuration Manager를 외부 LDAP 서버에 연결하는 방법에 대해 설명합니다. 외부 LDAP 서버는 구조적 LDAP이며 구조적 사용자를 포함합니다.

1 **Configuration Manager**에 관리자로 로그온합니다.

2 **관리** > **서버 관리** > **사용자 관리** > **사용자 관리 구성** > **외부 사용자 저장소**로 이동하여 구조적 LDAP 속성에 따라 다음 특성을 업데이트합니다.

일반 LDAP 연결

ldapHost: <LDAP 호스트 이름>

ldapPort: <LDAP 포트 번호>

enableSSL: <True/False - LDAP 연결에 SSL 사용>

useAdministrator: <True/False - LDAP 연결에 사용자 사용>

ldapAdministrator: <LDAP 사용자 이름(**useAdministrator=true**인 경우 정의해야 함)>

ldapAdministratorPassword: <LDAP 사용자 비밀번호(**useAdministrator=true**인 경우 정의해야 함)>

3 구성 집합을 저장합니다.

그룹 및 사용자 공급자 구성

이 절차에서는 구조적 LDAP(외부 저장소)를 그룹 및 사용자에 대한 공급자로 설정합니다. 내부 LDAP(공유 저장소)는 인증에 계속 사용되지만 사용자와 그룹은 외부 LDAP에서 가져옵니다. 이 모드는 외부 LDAP 구성을 테스트하고 구조적 사용자에게 권한을 할당하는 데 사용됩니다.

그룹 및 사용자 공급자를 설정하려면 다음을 수행합니다.

1 아직 이 페이지가 나오지 않았으면 **관리** > **서버 관리** > **사용자 관리** > **사용자 관리 구성** > **외부 사용자 저장소**로 이동합니다. 33 페이지의 "LDAP 연결 구성" 섹션에서 저장한 것과 동일한 구성 집합 초안을 사용하고 있는지 확인합니다.

2 구조적 LDAP 속성에 따라 다음 특성을 업데이트합니다.

a **사용자 검색**

usersBase: <사용자 검색의 기본 DN>

usersScope: <사용자 검색 범위>

usersFilter: <사용자 검색 필터>

b **사용자 개체 클래스**(LDAP 벤더별)

usersObjectClass: <사용자 LDAP 개체 클래스>

usersUniqueIDAttribute: <사용자 고유 ID LDAP 특성>

다음 특성은 선택 사항입니다.

usersDisplayNameAttribute: <사용자 표시 이름 LDAP 특성>

usersLoginNameAttribute: <사용자 로그인 이름 LDAP 특성>

usersFirstNameAttribute: <사용자 성 LDAP 특성>

usersLastNameAttribute: <사용자 이름 LDAP 특성>

usersEmailAttribute: <사용자 전자 메일 LDAP 특성>

usersPreferredLanguageAttribute: <사용자 기본 언어 LDAP 특성>

usersPreferredLocationAttribute: <사용자 기본 위치 LDAP 특성>

usersTimeZoneAttribute: <사용자 시간대 LDAP 특성>

usersDateFormatAttribute: <사용자 날짜 형식 LDAP 특성>

usersNumberFormatAttribute: <사용자 숫자 형식 LDAP 특성>

usersWorkWeekAttribute: <사용자 작업 주 LDAP 특성>

usersTenantIDAttribute: <사용자 테넌트 ID LDAP 특성>

usersPasswordAttribute: <사용자 비밀번호 LDAP 특성>

c 그룹 검색

groupsBase: <그룹 검색의 기본 DN>

groupsScope: <그룹 검색의 LDAP 범위>

groupsFilter: <그룹 검색 필터>

rootGroupsBase: <루트 그룹 검색의 기본 DN>

rootGroupsScope: <루트 그룹 검색의 LDAP 범위>

rootGroupsFilter: <그룹 검색 필터>

d 그룹 개체 클래스(LDAP 벤더별)

groupsObjectClass: <그룹 LDAP 개체 클래스>

groupsMembersAttribute: <그룹 구성원 LDAP 특성>

다음 특성은 선택 사항입니다.

groupsNameAttribute: <그룹 고유 이름 LDAP 특성>

groupsDisplayNameAttribute: <그룹 표시 이름 LDAP 특성>

groupsDescriptionAttribute: <그룹 설명 LDAP 특성>

enableDynamicGroups: <동적 그룹 사용>

dynamicGroupsClass: <동적 그룹 LDAP 개체 클래스>

dynamicGroupsMemberAttribute: <동적 그룹 구성원 LDAP 특성>

dynamicGroupsNameAttribute: <동적 그룹 고유 이름 LDAP 특성>

dynamicGroupsDisplayNameAttribute: <동적 그룹 표시 이름 LDAP 특성>

dynamicGroupsDescriptionAttribute: <동적 그룹 설명 LDAP 특성>

e 그룹 계층(구조적 LDAP가 그룹 계층을 사용하는 경우)

enableNestedGroups: <중첩 그룹의 지원 활성화>

maximalAllowedGroupsHierarchyDepth: <그룹 계층 최대 허용 깊이>

f 고급 구성

ldapVersion: <LDAP 버전>

baseDistinguishNameDelimiter: <기본 DN 구분 기호>

scopeDelimiter: <범위 구분 기호>

attributeValuesDelimiter: <LDAP 특성 값 구분 기호>

3 구성 집합 초안을 저장합니다.

구성 집합 활성화

1 **관리** > **서버 관리** > **사용자 관리** > **사용자 관리 구성**으로 이동하여 다음을 업데이트합니다.

외부 UUM 소스: True

그룹 공급자: 외부

사용자 공급자: 외부

2 구성 집합을 저장하고 활성화합니다.

3 **Configuration Manager** 서버에서 로그오프한 후 서버를 다시 시작합니다.

사용자에게 권한 할당

이 절차에서는 **시스템 관리자** 역할을 구조적 사용자에게 할당합니다. **시스템 관리자** 역할을 가진 사용자는 관련 역할을 나머지 구조적 사용자에게 할당할 권한을 갖게 됩니다.

1 **Configuration Manager**에 관리자로 로그온합니다.

2 **사용자 관리** 모듈(**관리** > **사용자 관리**)을 엽니다.

3 구조적 LDAP에서 그룹 및 사용자가 표시되는지 확인합니다.

4 **사용자 관리** > **사용자 검색 창**으로 이동하여 관리자로 활동할 사용자를 검색합니다(예: 이름 = j*, 성 = Smith).

5 **시스템 관리자** 역할을 사용자에게 추가합니다.

외부 LDAP에 인증 공급자 설정

이 절차는 구조적 사용자가 인증에 사용되도록 외부 구조적 LDAP를 인증 공급자로 설정합니다.

1 **관리** > **서버 관리** > **사용자 관리** > **사용자 관리 구성**으로 이동하여 다음을 업데이트합니다.

   인증 공급자: 외부

2 구성 집합을 저장하고 활성화합니다.

3 **Configuration Manager** 서버에서 로그오프한 후 서버를 다시 시작합니다.

4 **시스템 관리자** 역할이 할당된 구조적 사용자 중 하나로 로그온합니다.

LDAP 인증서 가져오기

구조적 LDAP에 연결하는 데 인증서가 필요할 경우 다음 단계를 수행합니다.

1 인증서를 파일로 내보냅니다.

2 Configuration Manager Windows 서비스를 중지합니다.

3 다음 명령을 실행합니다.

   <Configuration Manager 설치>\java\windows\x86_64\bin\keytool.exe -import -trustcacerts -alias <인증서 별칭> -keystore <Configuration Manager 설치>\java\windows\x86_64\lib\security\cacerts -storepass changeit -file <인증서 경로>

4 Configuration Manager Windows 서비스를 시작합니다.

내부(공유) LDAP 구성

내부(공유) LDAP 서버 비밀번호 변경(선택 사항)

보안을 위해 내부(공유) LDAP 서버의 비밀번호를 변경할 수 있습니다.

1 **HP Universal CMDB Configuration Manager**에 로그온합니다.

2 명령줄을 열고 **<Configuration Manager 설치>\ldap\serverRoot\bat** 폴더로 이동합니다.

3 **ldappasswordmodify -h localhost -p <ldap port> -D "cn=Directory Manager" -w <ldap 관리자 비밀번호> -c <ldap 관리자 비밀번호> -n <새 ldap 관리자 비밀번호>**를 실행합니다.

   a 기본 ldap 관리자 비밀번호는**ldapadmin**입니다.

   b 기본 포트는 **2389**입니다.

   c 명령이 성공적으로 수행되었는지 확인하고 다음 단계를 계속합니다.

4 **UCMDB Configuration Manager**에서 **관리** > **서버 관리** > **사용자 관리** > **사용자 관리 구성** > **공유 사용자 저장소**를 선택합니다.

5 **ldapAdministratorPassword** 특성의 비밀번호를 업데이트합니다.

6 구성 집합을 저장하고 활성화합니다.

7 **UCMDB Configuration Manager**에서 로그오프합니다.

8 **UCMDB Configuration Manager** 서버를 다시 시작합니다.

내부(공유) LDAP 포트 구성

기본 포트 2389는 다른 응용 프로그램에서 이미 사용 중일 수 있습니다. 이 기본 포트를 변경하려면 다음 절차를 사용합니다.

내부 LDAP 포트를 구성하려면 다음을 수행합니다.

1 명령줄을 열고 **<Configuration Manager 설치>\ldap\serverRoot\bat** 폴더로 이동합니다.

2 다음 명령을 실행합니다.
dsconfig -h localhost -p 2444 -D "cn=directory manager" -w <ldap 관리자 비밀번호> --trustAll -X -n set-connection-handler-prop --handler-name "LDAP Connection Handler" --set listen-port:<새 포트>

기본 <ldap 관리자 비밀번호>는 **ldapadmin**입니다.

3 오류 메시지가 표시되지 않았는지 확인하고 다음 단계를 계속합니다.

4 HP Universal CMDB Configuration Manager에 로그온합니다.

5 UCMDB Configuration Manager에서 **관리** > **서버 관리** > **사용자 관리** > **사용자 관리 구성** > **공유 사용자 저장소**를 선택하고 **ldapPort** 특성의 포트 번호를 업데이트합니다.

6 구성 집합을 저장하고 활성화합니다.

7 UCMDB Configuration Manager에서 로그오프합니다.

8 UCMDB Configuration Manager 서버를 다시 시작합니다.

LDAP 문제 해결

문제: LDAP 서버와의 통신을 설정할 수 없습니다. 로그에 통신 예외가 표시됩니다.

해결 방안: LDAP 호스트, 포트 및 SSL 모드 설정을 확인합니다.

a LDAP 호스트 및 포트가 올바르게 구성되어 있는지 확인합니다.
관리 > **서버 관리** > **사용자 관리** > **사용자 관리 구성** > **외부 사용자 저장소**를 선택하고 **ldapHost, ldapPort** 설정을 선택합니다.

b SSL 모드가 올바르게 구성되어 있는지 확인합니다. LDAP 연결에 관리자가 필요한지 구조적 LDAP 관리자에게 확인합니다. **관리** > **서버 관리** > **사용자 관리** > **사용자 관리 구성** > **외부 사용자 저장소**를 선택하고 **enableSSL** 설정을 확인합니다.

c 적절한 서버 인증서가 설치되어 있는지 확인합니다. 다음 명령을 실행합니다.

<Configuration Manager 설치>\java\windows\x86_64\bin\keytool.exe -list -trustcacerts [-alias <인증서 별칭>] -keystore <Configuration Manager 설치>\java\windows\x86_64\lib\security\cacerts -storepass changeit

d LDAP 연결에 관리자가 필요한지 구조적 LDAP 관리자에게 확인합니다. **관리** > **서버 관리** > **사용자 관리** > **사용자 관리 구성** > **외부 사용자 저장소**를 선택하고 다음 설정을 확인합니다. **useAdministrator, ldapAdministrator, ldapAdministratorPassword**

문제: 사용자 또는 그룹 관리 화면에 그룹이 표시되지 않습니다. 로그에 예외가 표시되지 않습니다.

해결 방안: 다음을 확인합니다.

a 사용자 및 그룹 검색 필터가 올바르게 구성되어 있는지 확인합니다. **관리** > **서버 관리** > **사용자 관리** > **사용자 관리 구성** > **외부 사용자 저장소**를 선택하고 다음 속성을 수정합니다. **usersBase, usersScope, usersFilter, groupsBase, groupsScope, groupsFilter, rootGroupsBase, rootGroupsScope, rootGroupsFilter**

b LDAP 클라이언트 브라우저를 열고 기본 DNS에서 사용자를 찾습니다.

문제: UI가 너무 느립니다.

해결 방안: 일반적으로 이 문제는 LDAP에 구성된 그룹이나 사용자가 너무 많아서 발생합니다. 다음과 같이 해당 하위 집합의 그룹 수가 감소되도록 기본 DNS 및 필터를 구성합니다.

a **관리** > **서버 관리** > **사용자 관리** > **사용자 관리 구성** > **외부 사용자 저장소**를 선택합니다.

b 다음 설정을 수정합니다. **usersBase, usersScope, usersFilter, groupsBase, groupsScope, groupsFilter, rootGroupsBase, rootGroupsScope, rootGroupsFilter**

문제: 알려진 일부 사용자가 그룹 또는 사용자 관리 화면에 표시되지 않습니다.

해결 방안: 사용자 및 그룹 관리 화면에는 특정 그룹에 속하는 사용자만 표시됩니다. 주 화면에 표시되게 하려면 사용자를 LDAP의 적절한 그룹에 넣습니다.

문제: 로그인하는 데 오랜 시간이 걸립니다.

해결 방안: 사용자가 너무 많은 그룹에 속해 있습니다. 다음과 같이 적은 수의 그룹만 반환하도록 그룹 검색 필터를 변경하여 시작 시간을 최적화할 수 있습니다.

a **관리** > **서버 관리** > **사용자 관리** > **사용자 관리 구성** > **외부 사용자 저장소**를 선택합니다.

b **groupsFilter** 설정을 수정합니다.

4

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

이 장**의 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.

이 섹션의 주제는 다음과 같습니다.

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.

- **ID 관리자.** 인증 목적으로 사용하려면 ID 관리자의 보호되지 않는 모든 리소스는 LW-SSO 구성 파일의 **nonsecureURLs** 설정을 사용하여 구성되어야 합니다.

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 특성만 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.

5

ID 관리자 인증

이 장**의 내용은** 다음과 같습니다.

ID 관리자 인증 허용

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

이 작업은 HP Universal CMDB Configuration Manager가 ID 관리자 인증을 허용하도록 구성하는 방법에 대해 설명합니다.

이 작업의 단계는 다음과 같습니다.

사전 준비 사항

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

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

HP Universal CMDB Configuration Manager가 ID 관리자를 허용하도록 구성

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

1 ID 관리자가 사용자 이름을 포함하는 개인 설정 헤더/콜백을 보내도록 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 문자열을 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 ID 관리자 URL로 변경하고 포트를 ID 관리자 포트로 변경합니다.

bsf.server.url=http://< ID 관리자 URL>:< ID 관리자 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 설치 디렉터리>\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 설치 디렉터리 >\tomcat\conf\workers.properties.minimal

Full path to the uriworkermap.properties file

worker_mount_file==<Configuration Manager 설치 디렉터리 >\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

---

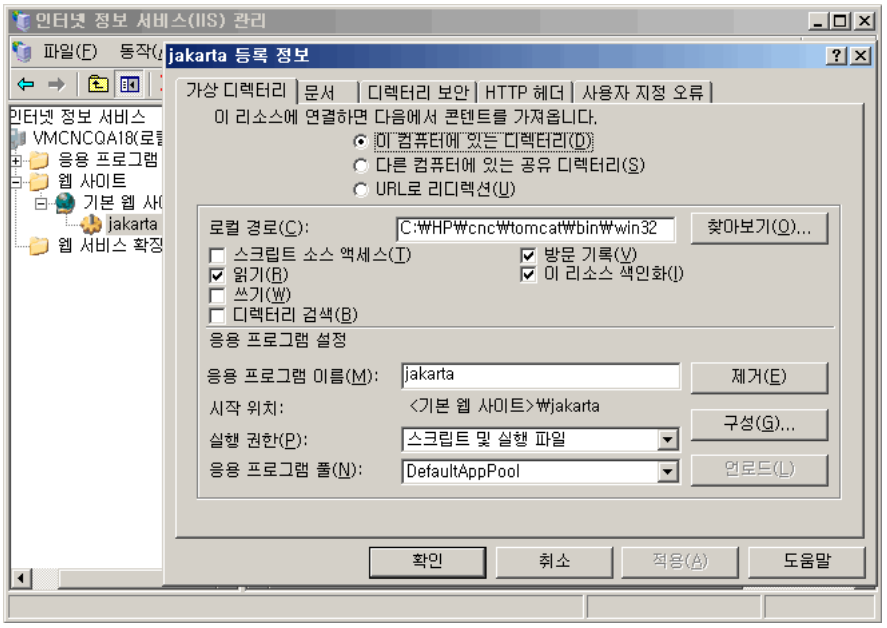
6 IIS 구성에서 해당 웹 사이트 개체에 가상 디렉터리를 만듭니다.

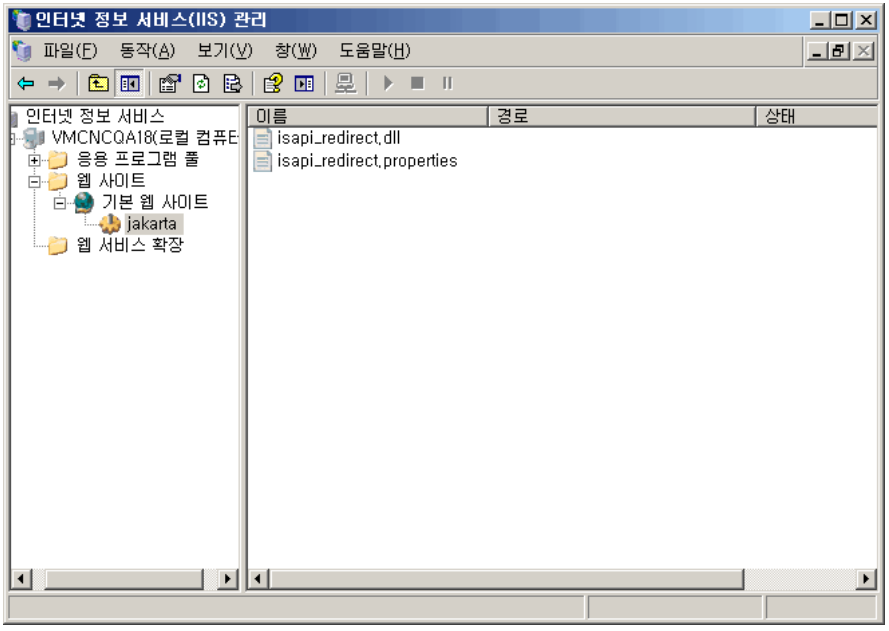
a Windows 시작 메뉴에서 **시작\제어판\관리 도구\인터넷 정보 서비스(IIS) 관리**를 엽니다.

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.





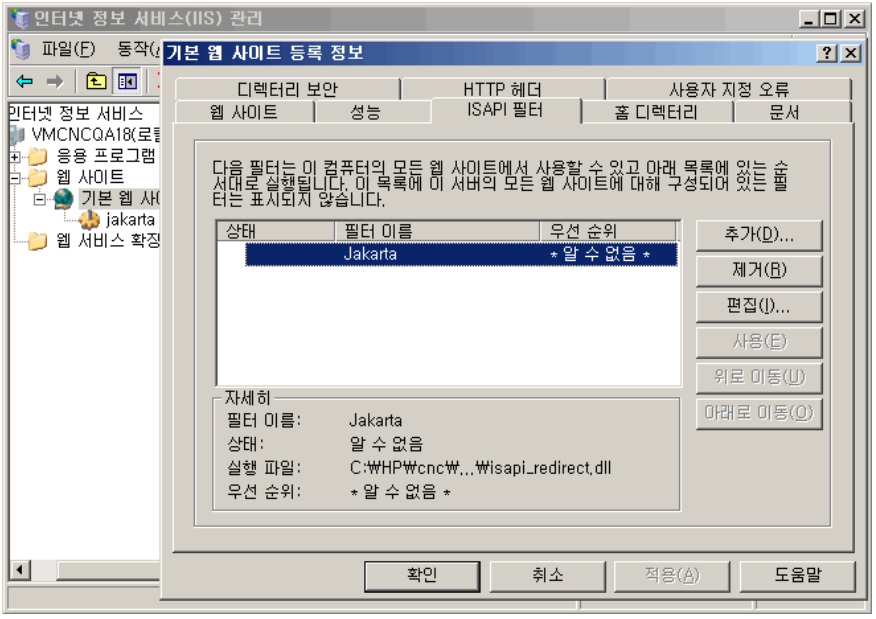
7 **isapi_redirect.dll**을 ISAPI 필터로 추가합니다.

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.



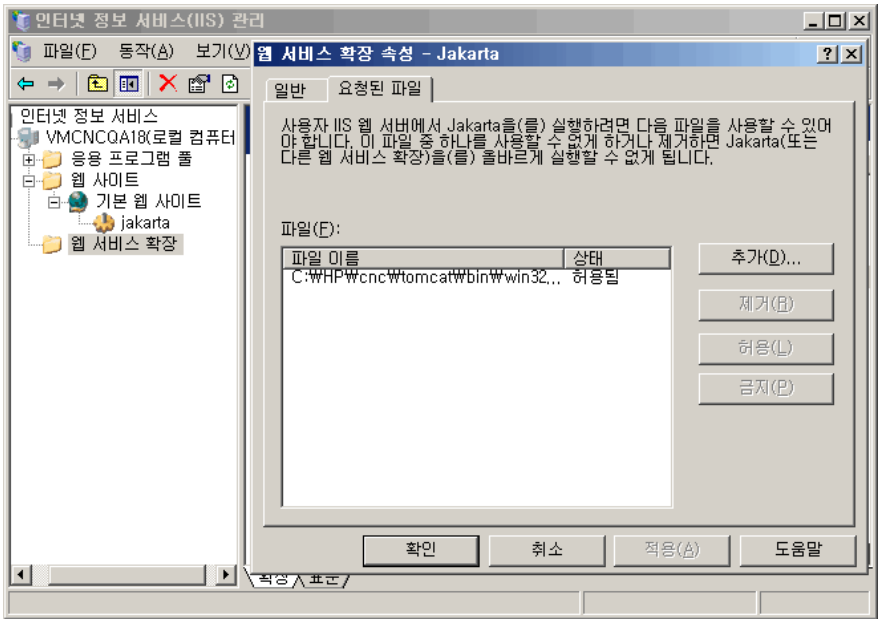
d **적용** 버튼을 클릭합니다.

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.

6

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*의 "사용자 관리"를 참조하십시오.

웹 브라우저 요구 사항 및 Configuration Manager 디스플레이 요구 사항에 대한 자세한 내용은 8 페이지의 "Configuration Manager 시스템 요구 사항"을 참조하십시오.

Configuration Manager에 안전하게 액세스하는 방법에 대한 자세한 내용은 69 페이지의 "강화"를 참조하십시오.

Configuration Manager 액세스 방법

웹 브라우저에서 Configuration Manager 서버의 URL을 입력합니다. 예를 들어 **http://<서버 이름 또는 IP 주소>.<도메인 이름>:<포트>**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.

Configuration Manager 로그인

1. Configuration Manager 설치 후 마법사에서 정의한 사용자 이름과 비밀번호를 입력합니다.
2. **로그인**을 클릭합니다. 로그인하면 사용자 이름이 화면의 오른쪽 위에 표시됩니다.
3. (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*의 "사용자 관리"를 참조하십시오.

로그아웃

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

로그아웃하려면 다음을 수행합니다.

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.

문제 해결 및 제한 사항

문제. 서버 관리에서 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.

```
<HP Universal CMDB Configuration Manager>\bin\export-cs.bat
<database properties> --history
```

여기서 <**데이터베이스 속성**>은 <**Configuration Manager 설치 디렉터리**>**\conf\database.properties** 파일의 위치를 지정하거나 각 데이터베이스 속성을 지정하여 설정할 수 있습니다. 예를 들면 다음과 같습니다.

```
cd <HP Universal CMDB Configuration Manager>\bin export-cs.bat -p
..\conf\database.properties --history
```

2 다음 명령을 실행하여 마지막 구성 집합을 내보냅니다.

```
< HP Universal CMDB Configuration Manager>\bin\export-cs.bat <데이터
베이스 속성> <구성 집합 ID> <덤프 파일 이름>
```

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

```
cd <HP Universal CMDB Configuration 설치 홈>\bin export-cs.bat -p
..\conf\database.properties -i 491520 -f mydump.zip
```

3 HP Universal CMDB Configuration Manager 서비스를 중지합니다.

4 다음 명령을 실행하여 이전 구성 집합을 가져오고 활성화합니다.

```
< HP Universal CMDB Configuration Manager>\bin\import-cs.bat <데이터
베이스 속성> <덤프 파일 이름> --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. 서버 관리로 이동하여 UCMDB의 연결 설정을 변경한 후 새 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 클래스의 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 UCMDB가 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 (CnC) 설치 폴더>\bin\encrypt-password.bat -p <암호>

암호화된 비밀번호가 반환됩니다.

2 암호화된 비밀번호({ENCRYPTED} 접두사 포함)를 **<CnC 설치 폴더 >\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. 예를 들면 다음과 같습니다.

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.
- **<CnC 설치 폴더>\servers\server-0\conf\server.xml** 파일을 편집하고 해당 포트를 업데이트하여 Configuration Manager 구성 파일에서 포트를 수동으로 변경합니다.
  - HTTP (8080): 줄 69
  - HTTPS (8443): 줄 71, 90

문제. Configuration Manager 로그에 메모리 부족 오류가 있습니다.

해결 방안. Java 최대 메모리를 필요한 만큼 증가시킵니다.

Configuration Manager 서비스에서 메모리 크기를 변경하려면 다음을 수행합니다.

1. **<CnC 설치 폴더>\cnc\bin** 디렉터리로 이동하여 edit-server-0.bat 명령을 수행합니다.
2. **Java** 탭을 선택합니다.
3. **초기 메모리 풀** 및 **최대 메모리 풀** 매개 변수를 업데이트합니다.

배치 파일에서 메모리 크기를 변경하려면 다음을 수행합니다.

1. **<CnC 설치 폴더>\cnc** 디렉터리로 이동하여 **start-server-0.bat** 파일을 엽니다.
2. **SET JAVA_OPTS=-Dcnc.home**으로 시작하는 줄을 찾습니다.

3 **-Xms** 및 **-Xmx** 명령을 찾아 요구 사항에 맞게 변경합니다.

```
-Xms<초기 메모리 풀 크기> -Xmx<최대 메모리 풀 크기>
```

예: 초기 메모리 풀을 100MB로, 최대 메모리 풀을 800MB로 설정하려면 다음과 같이 입력합니다.

```
-Xms100m -Xmx800m
```

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 서버 관리 모듈에서 구성할 수 있습니다.
- JMX 호출을 실행하여 해당 보기에서 오프라인 분석 계산을 수행합니다.
- 정책 관리로 이동합니다. **정책 분석 다시 계산** 버튼을 클릭합니다. 모든 보기에 대한 오프라인 분석 프로세스가 호출됩니다(시간이 소요될 수 있음). 또한 정책을 인위적으로 변경한 다음 저장해야 할 수 있습니다.

문제. **관리** > **UCMDB 열기**를 클릭하면 UCMDB 로그인 페이지가 표시됩니다.

해결 방안. 다시 로그인하지 않고 UCMDB에 액세스하려면 SSO(Single Sign-On)를 사용해야 합니다. 자세한 내용은 18 페이지의 "Lightweight Single Sign-On 사용"을 참조하십시오. 또한 로그온한 Configuration Manager 사용자가 UCMDB 사용자 관리 시스템에 정의되어 있는지 확인합니다.

문제. 설치 후 마법사에서 UCMDB 연결을 IPv6 주소로 구성하면 **관리** > **UCMDB 열기**가 작동하지 않습니다.

해결 방안. 다음 절차에 따릅니다.

1 **관리** > **서버 관리** > **Configuration Manager** > **UCMDB 연결**로 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.

Configuration Manager로 작업할 경우 다음 제한 사항이 적용될 수 있습니다.

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

7

강화

이 **장**의 내용은 다음과 같습니다.

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. 데이터베이스 비밀번호를 암호화하려면 Configuration Manager 설치 후 마법사의 데이터베이스 구성 페이지에서 **비밀번호 암호화** 확인란을 선택합니다.

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 79 페이지의 "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 **cnc\security\encrypt_repository** 디렉터리를 만들고 암호화 키를 생성합니다.

3 설치 후 마법사를 다시 실행합니다.

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 6.0을 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 디렉터리>**의 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

이 자체 서명 인증서를 사용하여 SSL을 통해 Configuration Manager와 통신해야 할 각 클라이언트에 대해, **tomcat.keystore**를 생성하고 서버 인증서를 내보낸 후에는 해당 클라이언트가 신뢰할 수 있는 저장소에 인증서를 배치합니다.

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

---

4 클라이언트 구성 설정 확인

<Configuration Manager 설치 디렉터리>의 **conf** 디렉터리에 있는 **client-config.properties** 파일을 엽니다. 프로토콜을 **https**로, 포트를 **8443**으로 설정합니다.

5 server.xml 파일 수정

<Configuration Manager 설치 디렉터리>의 **conf** 디렉터리에 있는 **server.xml** 파일을 엽니다. 주석에서 다음과 같이 시작하는 섹션을 찾습니다.

Connector port="8443"

주석 문자를 지우고 다음 두 줄을 추가하여 스크립트를 활성화합니다.

keystoreFile="<tomcat.keystore 파일 위치>"(72 페이지의 단계 2 참조)

keystorePass="<비밀번호>"

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.

팁: 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**로 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>\conf\server.xml 파일을 엽니다. 주석에서 다음과 같이 시작하는 섹션을 찾습니다.

Connector port="8443"

주석 문자를 지우고 다음 두 줄을 추가하여 스크립트를 활성화합니다.

keystoreFile="../../java/lib/security/tomcat.keystore"

keystorePass="password" />

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.

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.

Windows 탐색기에 파일이 보안 인증서임을 나타내는 아이콘이 표시됩니다.

2 **hpcert.cer**을 두 번 클릭하여 Internet Explorer 인증서 대화 상자를 열고 파일을 가져옵니다.

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

```
keytool.exe -import -alias hp -file hp.cer -keystore ..\lib\security\cacerts
```

4 server.xml 파일을 다음과 같이 수정합니다.

a 73 페이지의 단계 5에서 설명한 대로 변경합니다.

b 변경 직후 다음 줄을 추가합니다.

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

c clientAuth="true"를 설정합니다.

5 74 페이지의 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.

인증을 위해 SSL을 사용하려면 다음을 수행합니다.

1 72 페이지의 "자체 서명 인증서를 사용하여 서버 시스템에서 SSL 활성화"에서 74 페이지의 단계 6까지, 또는 74 페이지의 "인증 기관에서 발급된 인증서를 사용하여 서버 시스템에서 SSL 활성화"에서 76 페이지의 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>:8080/cnc**를 입력합니다.

클라이언트 인증서 인증 사용

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

클라이언트 인증서 인증을 사용하려면 다음을 수행합니다.

1 72 페이지의 "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 열고 in-client certificate로 시작하는 섹션을 찾습니다. 예를 들면 다음과 같습니다.

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

주석 문자열을 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 72 페이지의 "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.

암호화 매개 변수

다음은 데이터베이스 비밀번호 암호화에 사용하는 **encryption.properties** 파일에 포함된 매개 변수입니다. 데이터베이스 비밀번호 암호화에 대한 자세한 내용은 71 페이지의 "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.

매개 변수	설명
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
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.