Sun Java System Access Manager 7.1 릴리스 노트

Sun Microsystems, Inc.
4150 Network Circle
Santa Clara, CA 95054
U.S.A.

부품 번호: 820–0364
2007년 7월

Copyright 2007 Sun Microsystems, Inc. 4150 Network Circle, Santa Clara, CA 95054 U.S.A. 모든 권리는 저작권자의 소유입니다.

Sun Microsystems, Inc.는 본 설명서에서 설명하는 제품에 사용되는 기술과 관련한 지적 재산권을 보유합니다. 특히 이러한 지적 재산권에는 하나 이상의 미국 특허 및 추가 특허 또는 미국 및 기타 국가에서 특허 출원 중인 응용 프로그램이 포함될 수 있습니다.

U.S. 정부 권한 – 상용 소프트웨어. 정부 사용자는 Sun Microsystems, Inc. 표준 사용권 계약과 FAR의 해당 규정 및 추가 사항의 적용을 받습니다.

본 배포판에는 타사에서 개발한 자료가 포함되어 있을 수 있습니다.

본 제품의 일부는 Berkeley BSD 시스템일 수 있으며 University of California로부터 라이센스를 취득했습니다. UNIX는 X/Open Company, Ltd.를 통해 독점 라이센스를 취득한 미국 및 기타 국가의 등록 상표입니다.

Sun, Sun Microsystems, Sun 로고, Solaris 로고, Java Coffee Cup 로고, docs.sun.com, Java 및 Solaris는 미국 및 기타 국가에서 Sun Microsystems, Inc.의 상표 또는 등록 상표입니다. 모든 SPARC 상표는 라이센스 하에 사용되며 미국 및 기타 국가에서 SPARC International, Inc.의 상표 또는 등록 상표입니다. SPARC 상표가 부착된 제품은 Sun Microsystems, Inc.가 개발한 아키텍처를 기반으로 합니다.

OPEN LOOK 및 Sun™ Graphical User Interface는 Sun Microsystems, Inc.가 해당 사용자 및 라이센스 소유자를 위해 개발했습니다. Sun은 컴퓨터 업계에서 시각적 또는 그래픽 사용자 인터페이스 개념을 연구하고 개발하는 데 있어 Xerox의 선구적인 업적을 인정합니다. Sun은 Xerox Graphical User Interface에 대한 Xerox의 비독점적 라이센스를 보유하고 있으며 이 라이센스는 OPEN LOOK GUI를 구현하거나 그 외의 경우 Sun의 서면 라이센스 계약을 준수하는 Sun의 라이센스 소유자에게도 적용됩니다.

본 설명서에서 다루는 제품과 수록된 정보는 미국 수출 관리법에 의해 규제되며 기타 국가의 수출 또는 수입 관리법의 적용을 받을 수 있습니다. 본 제품과 정보를 직간접적으로 핵무기, 미사일 또는 생화학 무기에 사용하거나 핵과 관련하여 해상에서 사용하는 것은 엄격하게 금지합니다. 미국 수출 금지 국가 또는 금지된 개인과 특별히 지정된 국민 목록을 포함하여 미국 수출 금지 목록에 지정된 대상으로의 수출이나 재수출은 엄격하게 금지됩니다.

본 설명서는 "있는 그대로" 제공되며 상업성, 특정 목적에 대한 적합성 또는 비침해에 대한 모든 묵시적인 보증을 포함하여 모든 명시적 또는 묵시적 조건, 표현 및 보증에 대해 어떠한 책임도 지지 않습니다. 이러한 보증 부인은 법적으로 허용된 범위 내에서만 적용됩니다.

070806@18135

목차

Sun Java System Access Manager 7.1 릴리스 노트 5
개정 내역 6
Sun Java System Access Manager 7.1 정보 6
이 릴리스의 새로운 기능 6
Java ES Monitoring Framework 통합 7
웹 서비스 보안 7
단일 Access Manager WAR 파일 배포 7
핵심 서비스의 향상된 기능 7
지원되지 않는 기능 알림 및 발표 10
하드웨어 및 소프트웨어 요구 사항 10
지원하는 브라우저 12
일반 호환성 정보 13
AMSDK 내부 시스템과 Access Manager 서버의 비호환성 13
Access Manager HPUX 버전 업그레이드가 지원되지 않음 13
Access Manager 레거시 모드 14
Access Manager 정책 에이전트 15
알려진 문제점 및 제한 사항 16
설치 문제 16
업그레이드 문제 20
호환성 문제 21
구성 문제 23
성능 문제 26
Access Manager 콘솔 문제 29
명령줄 문제 30
SDK 및 클라이언트 문제 30
인증 문제 31
세션 및 SSO 문제 33
정책 문제 34

서버 시작 문제 34
AMSDK 문제 34
SSL 문제 36
예제 문제 37
Linux OS 문제 37
Windows 및 HP-UX 문제 38
연합 및 SAML 문제 38
국제화(g11n) 문제 39
설명서 문제 40
설명서 업데이트 41
재배포 가능 파일 42
문제점 보고 및 사용자 의견 제공 방법 42
Sun은 여러분의 의견을 환영합니다. 42
Sun의 추가 자원 43
내게 필요한 옵션 기능 43
타사 웹 사이트 43

Sun Java System Access Manager 7.1 릴리스 노트

2007년 7월

부품 번호 820-0364

Sun Java™ System Access Manager 7.1 릴리스 노트에는 Access Manager의 새로운 기능, 알려진 문제점과 해결 방법(있는 경우)을 포함하여 Sun Java Enterprise System(Java ES) 릴리스에 대해 사용할 수 있는 중요 정보가 포함되어 있습니다. 이 릴리스의 설치 및 사용 전에 이 문서를 읽으시기 바랍니다.

Access Manager 모음을 포함한 Java ES 제품 설명서를 보려면 `http://docs.sun.com/prod/entsys.05q4`와 `http://docs.sun.com/db/prod/entsys.05q4?l=ko`를 참조하십시오.

소프트웨어를 설치하고 설정하기 전에 이 사이트를 확인하고 이후에도 정기적으로 방문하여 최신 문서가 있는지 확인하십시오.

이 릴리스 노트에는 다음 절이 포함됩니다.

- 6 페이지 "개정 내역"
- 6 페이지 "Sun Java System Access Manager 7.1 정보"
- 6 페이지 "이 릴리스의 새로운 기능"
- 10 페이지 "하드웨어 및 소프트웨어 요구 사항"
- 13 페이지 "일반 호환성 정보"
- 16 페이지 "알려진 문제점 및 제한 사항"
- 41 페이지 "설명서 업데이트"
- 42 페이지 "재배포 가능 파일"
- 42 페이지 "문제점 보고 및 사용자 의견 제공 방법"
- 43 페이지 "Sun의 추가 자원"
- 43 페이지 "타사 웹 사이트"

개정 내역

다음 표는 Access Manager 7.1 릴리스 노트의 개정 내역을 보여 줍니다.

표 1 개정 내역

날짜	변경 내용
2006년 7월	베타 릴리스
2007년 3월	Java Enterprise System 5 릴리스
2007년 5월	새로 알려진 문제점 6555040, 6550261, 6554379, 6554372, 6480354 업데이트
2007년 6월	새로 알려진 문제점 6562076, 6490150 업데이트
2007년 7월	새로 알려진 문제점 6485695 업데이트

Sun Java System Access Manager 7.1 정보

Sun Java System Access Manager는 Sun Identity 관리 인프라의 일부로 조직이 엔터프라이즈 및 B2B(business-to-business) 가치 체인 전반에서 웹 응용 프로그램 및 기타 자원에 대한 안전한 액세스를 관리할 수 있도록 해줍니다.

Access Manager는 다음과 같은 주요 기능을 제공합니다.

- 역할 기반 및 규칙 기반 액세스 제어를 사용하는 중앙 인증 및 인증 서비스
- 조직의 웹 기반 응용 프로그램 액세스를 위한 단일 사인온(SSO)
- Liberty Alliance Project 및 SAML(Security Assertions Markup Language)을 이용한 연합 Identity 지원
- 이후 분석, 보고 및 감사를 위한 Access Manager 구성 요소에 의한 관리자 및 사용자 활동을 포함한 중요 정보 로깅

이 릴리스의 새로운 기능

이 릴리스는 다음과 같은 새로운 기능을 포함합니다.

- 7 페이지 “Java ES Monitoring Framework 통합”
- 7 페이지 “웹 서비스 보안”
- 7 페이지 “단일 Access Manager WAR 파일 배포”
- 7 페이지 “핵심 서비스의 향상된 기능”
- 10 페이지 “지원되지 않는 기능 알림 및 발표”

Java ES Monitoring Framework 통합

Access Manager 7.1이 JMX(Java Management Extension)를 통해 Java Enterprise System Monitoring Framework에 통합되었습니다. JMX 기술은 장치, 응용 프로그램 및 서비스 위주의 네트워크를 관리 및 모니터링하는 분산된 웹 기반, 모듈형, 동적 솔루션을 구축하기 위한 도구를 제공합니다. JMX 기술의 일반적인 사용에는 응용 프로그램 구성 참조 및 변경, 응용 프로그램 동작에 대한 통계 누적, 상태 변경 및 오류 동작에 대한 알림 등이 포함됩니다. 데이터는 중앙 집중식 모니터링 콘솔로 전달됩니다.

Access Manager 7.1은 다음과 같은 통계 및 서비스 관련 데이터를 캡처하는 데 Java ES Monitoring Framework를 사용합니다.

- 시도, 성공 및 실패한 인증 횟수
- 정책 캐싱 통계
- 정책 평가 트랜잭션 시간

웹 서비스 보안

Access Manager 7.1은 다음과 같은 방법으로 인증 기능을 웹 서비스로 확장했습니다.

- 나가는 메시지에 토큰 삽입
- 들어오는 메시지에서 보안 토큰 평가
- 새 응용 프로그램을 위한 인증 공급자의 포인트 앤드 클릭 선택 사용 가능

단일 Access Manager WAR 파일 배포

Access Manager에는 모든 지원 플랫폼에서 지원되는 모든 컨테이너에 일관성 있게 Access Manager 서비스를 배포하는 데 사용할 수 있는 단일 WAR 파일이 포함되어 있습니다. Access Manager WAR 파일은 여러 JAR, XML, JSP, HTML, GIF 및 등록 정보 파일을 배포하는 Java Enterprise System 설치 프로그램과 함께 공동으로 존재합니다.

핵심 서비스의 향상된 기능

지원되는 웹 컨테이너

- Sun Java System Web Server 7.0
- Sun Java System Application Server 8.2
- BEA WL 8.1 SP4
- IBM WebSphere 5.1.1.6

Monitoring Framework 통합

Access Manager는 JES Monitoring Framework를 사용하여 다음을 모니터링할 수 있습니다.

1. 인증
   - 시도한 인증 횟수
   - 시도한 원격 인증 횟수(선택 사항)
   - 성공한 인증 횟수
   - 실패한 인증 횟수
   - 성공한 로그아웃 작업 횟수
   - 실패한 로그아웃 작업 횟수
   - 가능한 경우 각 모듈에 대한 트랜잭션 시간(실행 및 대기 상태)
2. 세션
   - 세션 테이블의 크기(결과적으로 최대 세션 수)
   - 활성 세션의 수(증분 카운터)
3. 프로필 서비스
   - 최대 캐시 크기
   - 작업에 대한 트랜잭션 시간(실행 및 대기)
4. 정책
   - 입출력 요청의 정책 평가
   - 해당 주제 플러그인의 LDAP 서버에 대한 정책 연결 풀 통계

인증 모듈

- 분산 인증 서비스가 하나의 로드 밸런서 배포용 서버에 고정될 필요는 없습니다.
- 인증 서비스 및 서버가 하나의 로드 밸런서 배포용 서버에 고정될 필요는 없습니다.
- 합성 조언(Composite advices) 기술은 인증 서비스, 정책 에이전트 및 정책 서비스 간에 `AuthenticateToRealm` 조건, AuthenticateToService 조건, 그리고 모든 조건에 대한 영역 자격을 포함하도록 지원합니다.
- 조직 조언(영역의 정규화된 인증 조건)
- 인증 구성 / 인증 체인(`AuthServiceCondition`)
- 인증 체인이 적용되는 경우 이제 모듈 기반 인증이 허용되지 않을 수 있습니다.
- 분산 인증 서비스는 인증서 인증 모듈을 지원합니다.
- 전체 기능 자격 증명 추출기 프레젠테이션을 만들기 위해 `CertAuth`를 분산 인증 UI에 추가했습니다.
- 바로 사용 가능한 모듈로서 새 데이터 저장소 인증 모듈은 지정된 영역에 대해 구성된 데이터 저장소를 대상으로 인증을 수행합니다.
- 계정 잠금 구성이 이제 여러 AM 서버 인스턴스 간에 지속됩니다.
- 사후 프로세싱 SPI 클래스의 연결

정책 모듈

- 사용자가 특정 인증 서비스 체인에 인증되도록 적용하는 새 정책 조건 `AuthenticateToServiceCondition`을 추가했습니다.

- 사용자가 특정 영역에 인증되도록 적용하는 새 정책 조건 `AuthenticateToRealmCondition`을 추가했습니다.
- 사용자가 지정된 ldap 필터에 일치하도록 적용하는 새 정책 조건 `LDAPFilterCondition`을 추가했습니다.
- 하위 디렉토리를 보호하지 않아도 디렉토리의 내용을 보호하는 데 용이한 1단계 와일드 카드 비교를 지원합니다.
- 전역 정책 구성에서 조직 별칭 참조가 사용되는 경우 상위 영역에서 명시적인 참조 정책 없이 하위 영역에 정책을 만들 수 있습니다.
- `AuthLevelCondition`에서 인증 수준 외에도 영역 이름을 지정할 수 있습니다.
- `AuthSchemeCondition`에서 인증 모듈 이름 외에도 영역 이름을 지정할 수 있습니다.

서비스 관리 모듈

- 활성 디렉토리 내 서비스 관리/정책 구성 저장을 지원합니다.

Access Manager SDK

- 기본 Identity 저장소 프레임워크 데이터베이스에 대해 사용자를 인증하는 API를 지원합니다.

웹 서비스 지원

- Liberty ID-WSF SOAP 공급자: Access Manager가 구현하는 대로 Liberty ID-WSF SOAP 바인딩을 캡슐화하는 인증 공급자이며 클라이언트 및 서비스 공급자로 구성되어 있습니다.
- HTTP 계층 SSO 공급자: 서버측 Access Manager 기반 SSO를 캡슐화하는 HttpServlet 계층 인증 공급자입니다.

설치 모듈

- 단일 WAR 파일이 웹 배포가 가능하도록 Access Manager를 J2EE 응용 프로그램으로 다시 패키징합니다.
- 64비트 JVM 지원을 위한 64비트 SJS Web Server 7.0을 지원합니다.

위임 모듈

- 위임 권한의 그룹화를 지원합니다.

업그레이드

- Access Manager 7.0 2005Q4, Access Manager 6.3 2005Q1 및 Identity Server 6.2 2004Q2에서Access Manager 7.1로의 업그레이드를 지원합니다.

로깅

- 로깅 모듈 내 위임을 지원합니다. 로그 파일을 읽고 기록할 수 있도록 인증된 Identity를 제어합니다.

- JCE 기반 SecureLogHelper를 지원합니다. 보안 로깅 구현을 위한 보안 공급자로 JSS 이외에도 JCE를 사용할 수 있도록 합니다.

지원되지 않는 기능 알림 및 발표

시스템 관리자는 Sun Java(TM) System Access Manager 7.1 Identity 관리 API 및 XML 템플리트를 사용하여 Sun Java System Directory Server의 Identity 항목을 작성, 삭제 및 관리할 수 있습니다. Access Manager도 Identity 관리를 위한 API를 제공합니다. 개발자는 com.iplanet.am.sdk 패키지에 정의된 공용 인터페이스 및 클래스를 사용하여 관리 기능을 외부 응용 프로그램 또는 서비스에 통합하여 Access Manager에서 관리하도록 할 수 있습니다. Access Manager API는 Identity 관련 객체를 만들고 삭제하는 것은 물론 Directory Server에서 객체의 속성을 가져오고 수정, 추가 또는 삭제할 수 있는 방법을 제공합니다.

일반적으로 AMSDK라고 알려진 Access Manager com.iplanet.am.sdk 패키지는 이후의 Access Manager 릴리스에는 포함되지 않습니다. 이 패키지에는 관련 API 및 XML 템플리트가 모두 포함됩니다. 현재는 마이그레이션 옵션이 제공되지 않으며 앞으로도 마이그레이션 옵션은 제공되지 않을 것으로 예상됩니다. Sun Java System Identity Manager가 제공하는 사용자 관리 솔루션은 지금부터 사용을 시작할 수 있는 호환 가능한 대체 항목입니다. Sun Java System Identity Manager에 대한 자세한 내용은 http://www.sun.com/software/products/identity_mgr/index.xml을 참조하십시오.

하드웨어 및 소프트웨어 요구 사항

다음 표는 이 릴리스에 필요한 하드웨어 및 소프트웨어를 보여 줍니다.

표 2 하드웨어 및 소프트웨어 요구 사항

구성 요소	요구 사항
운영 체제(OS)	■ SPARC, x86 및 x64 기반 시스템의 Solaris™10, 전체 루트 로컬 및 스파스 루트 영역 지원 포함 ■ SPARC 및 x86 기반 시스템의 Solaris 9 ■ Red Hat™ Enterprise Linux 3 및 4, 모든 업데이트 Advanced Server(32 및 64비트 버전) 및 Enterprise Server(32 및 64비트 버전) ■ Windows Windows 2000 Advanced Server, Data Center Server 버전 SP4(x86) x86 및 x64 기반 시스템의 Windows 2003 Standard(32 및 64비트 버전), Enterprise(32 및 64비트 버전), Data Center Server(32비트 버전) x86 기반 시스템의 Windows XP Professional SP2 HP-UX 11i v1(uname에서 11.11), PA-RISC 2.0의 64비트 지원되는 운영 체제의 최신 업데이트 목록은 **Sun Java Enterprise System 5 Release Notes for UNIX**의 "Platform Requirements and Issues", 또는 **Sun Java Enterprise System 5 Release Notes for Microsoft Windows**의 "Hardware and Software Platform Information"을 참조하십시오.
Java 2 Standard Edition(J2SE)	J2SE 플랫폼 6.0, 5.0 업데이트 9(HP-UX: 1.5.0.03) 및 1.4.2 업데이트 11
Directory Server	Access Manager 정보 트리: Sun Java System Directory Server 6.0 또는 Sun Java System Directory Server 5.2 2005Q4 Access Manager Identity 저장소: Sun Java System Directory Server 5.2와 6.0 및 Microsoft Active Directory

표 2 하드웨어 및 소프트웨어 요구 사항 *(계속)*

구성 요소	요구 사항
웹 컨테이너	64비트 JVM에서 Web Server 인스턴스를 실행하도록 선택할 수 있는 지원되는 플랫폼/OS 조합의 Sun Java System Web Server 7.0. 지원 플랫폼: Solaris 9/SPARC, Solaris 10/SPARC, Solaris 10/AMD64, Red Hat AS 또는 ES 3.0/AMD64, Red Hat AS 또는 ES 4.0/AMD64
	Sun Java System Application Server Enterprise Edition 8.2
	BEA WebLogic 8.1 SP4
	IBM WebSphere Application Server 5.1.1.6
RAM	기본 테스팅: 512MB
	실제 배포: 스레드, Access Manager SDK, HTTP 서버 및 기타 내부 항목용으로 1GB
디스크 공간	Access Manager 및 관련 응용 프로그램용으로 512MB

이러한 구성 요소의 다른 버전에 대한 지원 정보는 Sun Microsystems 기술 지원부에 문의하십시오.

지원하는 브라우저

다음 표는 Sun Java Enterprise System 5 릴리스에서 지원하는 브라우저를 보여 줍니다.

표 3 지원하는 브라우저

브라우저	플랫폼
Firefox 1.0.7	Windows XP
	Windows 2000
	Solaris OS 버전 9 및 10
	Red Hat Linux 3 및 4
	Mac OS X
Microsoft Internet Explorer™ 6.0 SP2	Windows XP
Microsoft Internet Explorer 6.0 SP1	Windows™ 2000

표 3 지원하는 브라우저 (계속)

브라우저	플랫폼
Mozilla™ 1.7.12	Solaris OS 버전 9 및 10
	Windows XP
	Windows 2000
	Red Hat Linux 3 및 4
	Mac OS X
Netscape™ Communicator 8.0.4	Windows XP
	Windows 2000
Netscape Communicator 7.1	Solaris OS 버전 9 및 10

일반 호환성 정보

- 13 페이지 “AMSDK 내부 시스템과 Access Manager 서버의 비호환성”
- 13 페이지 “Access Manager HPUX 버전 업그레이드가 지원되지 않음”
- 14 페이지 “Access Manager 레거시 모드”
- 15 페이지 “Access Manager 정책 에이전트”

AMSDK 내부 시스템과 Access Manager 서버의 비호환성

다음 조합은 아래 Java Enterprise System 릴리스에서 AMSDK와 Access Manager 서버 간에 호환되지 않습니다.

- Java Enterprise System 2004Q2 AMSDK는 Java Enterprise System 5 Access Manager 서버(본 릴리스)와 호환되지 않습니다.
- Java Enterprise System 5 AMSDK(본 릴리스)는 Java Enterprise System Access Manger 2004Q2(이전 Identity Server) 서버와 호환되지 않습니다.

Access Manager HPUX 버전 업그레이드가 지원되지 않음

HPUX 버전의 경우 Access Manager 7 2005Q4에서 Access Manger 7.1(본 릴리스)로 업그레이드하는 경로가 지원되지 않습니다.

Access Manager 레거시 모드

다음 제품과 함께 Access Manager를 설치하는 경우 Access Manager 레거시(6.x) 모드를 선택해야 합니다.

- Sun Java System Portal Server
- Messaging Server, Calendar Server, Instant Messaging 또는 Delegated Administrator를 포함한 Sun Java System Communications Services 서버

Java ES 설치 프로그램의 실행 방법에 따라 Access Manager 레거시(6.x) 모드를 선택합니다.

- 14 페이지 “상태 파일을 사용한 Java ES 자동 설치”
- 14 페이지 “그래픽 모드의 "지금 구성" 설치 옵션”
- 14 페이지 “텍스트 기반 모드의 "지금 구성" 설치 옵션”
- 15 페이지 “"나중에 구성" 설치 옵션”

Access Manager 7.1 설치 결정에 대한 보다 자세한 내용은 15 페이지 “Access Manager 모드 결정”을 참조하십시오.

상태 파일을 사용한 Java ES 자동 설치

Java ES 설치 프로그램 자동 설치는 유사한 구성을 가진 여러 호스트 서버에 Java ES 구성 요소를 설치할 수 있는 비 대화형 모드입니다. 먼저 설치 프로그램을 실행하여 상태 파일을 생성한 후(실제로는 어떤 구성 요소도 설치하지 않음) Access Manager 및 기타 구성 요소를 설치할 각 호스트 서버에 대해 상태 파일의 복사본을 편집합니다.

레거시(6.x) 모드에서 Access Manager를 선택하려면 상태 파일에서 다음 매개 변수(다른 매개 변수 포함)를 설정한 후 자동 모드로 설치 프로그램을 실행합니다.

```
...
AM_REALM = disabled
...
```

상태 파일을 사용하여 Java ES 설치 프로그램을 자동 모드로 실행하는 방법에 대한 자세한 내용은 **Sun Java Enterprise System 5 Installation Guide for UNIX**의 5 장, “Installing in Silent Mode”를 참조하십시오.

그래픽 모드의 "지금 구성" 설치 옵션

"Access Manager: 관리(1 / 6)" 창에서 "지금 구성" 옵션을 사용하여 Java ES 설치 프로그램을 그래픽 모드에서 실행 중인 경우 기본값인 "Legacy(버전 6.x 스타일)"를 선택합니다.

텍스트 기반 모드의 "지금 구성" 설치 옵션

"지금 구성" 옵션을 사용하여 텍스트 기반 모드에서 Java ES 설치 프로그램을 실행 중인 경우 `Install type (Realm/Legacy) [Legacy]`에서 기본값인 `Legacy`를 선택합니다.

"나중에 구성" 설치 옵션

"나중에 구성" 옵션을 사용하여 Java ES 설치 프로그램을 실행하는 경우 `amconfig` 스크립트를 실행하여 설치 후 Access Manager를 구성해야 합니다. 레거시(6.x) 모드를 선택하려면 구성 스크립트 입력 파일(`amsamplesilent`)에서 다음 매개 변수를 설정합니다.

```
...
AM_REALM=disabled
...
```

`amconfig` 스크립트를 실행하여 Access Manager를 구성하는 방법에 대한 자세한 내용은 **Sun Java System Access Manager 7.1 관리 설명서**를 참조하십시오.

Access Manager 모드 결정

실행 중인 Access Manager 7.1 설치가 영역 모드로 구성되었는지, 레거시 모드로 구성되었는지 확인하려면 다음을 호출합니다.

```
http(s)://host:port/amserver/SMSServlet?method=isRealmEnabled
```

결과는 다음과 같습니다.

- true: 영역 모드
- false: 레거시 모드

Access Manager 정책 에이전트

다음 표는 Access Manager 7.1 모드에 대한 정책 에이전트의 호환성을 보여 줍니다.

표 4 Access Manager 7.1 모드에 대한 정책 에이전트의 호환성

에이전트 및 버전	호환 모드
웹 및 J2EE 에이전트, 버전 2.2	레거시 및 영역 모드
웹 및 J2EE 에이전트, 버전 2.1은 Access Manager 7.1에서 지원되지 않음	

알려진 문제점 및 제한 사항

이 절에서는 Access Manager 7.1 릴리스 당시의 다음과 같은 알려진 문제점 및 해결 방법(있는 경우)을 설명합니다.

- 16 페이지 "설치 문제"
- 20 페이지 "업그레이드 문제"
- 21 페이지 "호환성 문제"
- 23 페이지 "구성 문제"
- 26 페이지 "성능 문제"
- 29 페이지 "Access Manager 콘솔 문제"
- 30 페이지 "명령줄 문제"
- 30 페이지 "SDK 및 클라이언트 문제"
- 31 페이지 "인증 문제"
- 33 페이지 "세션 및 SSO 문제"
- 34 페이지 "정책 문제"
- 34 페이지 "서버 시작 문제"
- 34 페이지 "AMSDK 문제"
- 36 페이지 "SSL 문제"
- 37 페이지 "예제 문제"
- 37 페이지 "Linux OS 문제"
- 38 페이지 "Windows 및 HP-UX 문제"
- 38 페이지 "연합 및 SAML 문제"
- 39 페이지 "국제화(g11n) 문제"
- 40 페이지 "설명서 문제"

설치 문제

Java System Enterprise 설치 문제에 대한 내용은 JES5 릴리스 노트에 수록되어 있습니다. **Sun Java Enterprise System 5 Release Notes for UNIX**의 "Access Manager Installation Issues" 절을 참조하십시오.

이 절에서는 다음과 같은 알려진 문제점을 설명합니다.

- 17 페이지 "WebLogic의 Access Manager 단일 WAR 배포에서 클라이언트 SDK와 통신하려면 JAX-RPC 1.0 JAR 파일이 필요합니다. (6555040)"
- 18 페이지 "Websphere 5.1에 대해 JES 5 설치 프로그램이 생성한 단일 WAR에 .jar 파일이 추가로 필요합니다. (6550261)"
- 18 페이지 "Webshpere에 대한 단일 WAR 배포에서 클라이언트 SDK와 통신하려면 server.xml을 변경해야 합니다. (6554379)"
- 19 페이지 "Weblogic 및 Webshpere에 대한 Access Manager 단일 War 작업을 수행하려면 분산 인증을 변경해야 합니다. (6554372)"

WebLogic의 Access Manager 단일 WAR 배포에서 클라이언트 SDK와 통신하려면 JAX-RPC 1.0 JAR 파일이 필요합니다. (6555040)

이 문제는 JAX-RPC 초기화 시 Weblogic 8.1에서 배포되는 단일 WAR에 대해 알려진 문제입니다. Access Manager가 클라이언트 SDK와 통신할 수 있도록 하려면 JAX-RCP 1.1 jar 파일을 JAX-RPC 1.0 jar 파일로 교체해야 합니다.

해결 방법:

WAR 파일을 가져오는 방법은 두 가지가 있습니다. 하나는 Access Manager를 나중에 구성 옵션으로 설정하여 Java Enterprise System 5 설치 프로그램을 통해 가져오는 것이고, 다른 하나는 Sun 다운로드 사이트에서 가져오는 것입니다.

나중에 구성 옵션으로 JES 5 설치 프로그램을 통해 WAR 파일을 생성한 경우

1. *AccessManager-base*/SUNWam/web-src/WEB-INF/lib에서 다음 JAXRPC 1.1 .jar 파일을 제거합니다.
   - jaxrpc-api.jar
   - jaxrpc-spi.jar
   - jaxrpc-impl.jar
2. 해당 위치에서 다음 .jar 파일을 *AccessManager-base*/SUNWam/web-src/WEB-INF/lib로 복사합니다.
   - /opt/SUNWam/lib/jaxrpc 1.0의 jaxrpc-api.jar
   - /opt/SUNWam/lib/jaxrpc 1.0의 jaxrpc_ri.jar
   - /opt/SUNWmfwk/lib의 commons-logging.jar
3. *AccessManager-base*/SUNWam/bin/으로 이동한 후 다음 명령을 실행합니다.

   amconfig –s *samplesilent*

   amconfig 스크립트를 사용하여 Access Manager를 구성하는 방법에 대한 자세한 내용은 **Access Manager Post Installation Guide**의 Running the Access Manager amconfig Script를 참조하십시오.

Sun 다운로드 사이트(http://www.sun.com/download/index.jsp)에서 WAR 파일을 가져온 경우

1. *ZIP_ROOT*/applications/jdk14/amserver.war 파일을 가져온 후 임시 영역(예: /tmp/am-staging)에 저장합니다.
2. /tmp/am-staging/WEB-INF/lib에서 다음 JAXRPC 1.1 .jar 파일을 제거합니다.
   - jaxrpc-api.jar
   - jaxrpc-spi.jar
   - jaxrpc-impl.jar
3. *ZIP_ROOT*/applications/jdk14/jarFix 디렉토리에 있는 다음 JAXRPC 1.0 .jar 파일 및 공통 로깅 .jar 파일을 /tmp/am-staging/WEB-INF/lib에 복사합니다.
   - jaxrpc-api.jar

- jaxrpc-ri.jar
- commons-logging.jar

4. Access Manager WAR을 다시 만들어 배포합니다. 자세한 내용은 **Access Manager Post Installation Guide**의 Deploying Access Manager as a Single WAR File을 참조하십시오.

Websphere 5.1에 대해 JES 5 설치 프로그램이 생성한 단일 WAR에 .jar 파일이 추가로 필요합니다. (6550261)

JES 5 설치 프로그램에서 [나중에 구성] 옵션을 사용하여 Access Manager 단일 WAR을 생성한 경우 Websphere 5.1을 배포하려면 .jar 파일이 추가로 필요합니다.

해결 방법:

1. jsr173_api.jar을 /usr/share/lib에서 *AcessManager-base*/opt/SUNWam/web-src/WEB-INF/lib 디렉토리로 복사합니다.
2. *AccessManager-base*/SUNWam/bin/으로 이동한 후 다음 명령을 실행합니다.

   amconfig –s *samplesilent*

   amconfig 스크립트를 사용하여 Access Manager를 구성하는 방법에 대한 자세한 내용은 **Access Manager Post Installation Guide**의 Running the Access Manager amconfig Script를 참조하십시오.

Webshpere에 대한 단일 WAR 배포에서 클라이언트 SDK와 통신하려면 server.xml을 변경해야 합니다. (6554379)

Websphere 5.1에서 Access Manager 단일 WAR 배포가 클라이언트 SDK와 성공적으로 통신하려면 server.xml 파일을 변경해야 합니다.

해결 방법:

server.xml 파일을 올바르게 변경하려면 다음 단계를 수행합니다.

1. amserver.war 파일을 가져옵니다. 단일 WAR 파일을 가져오는 방법은 두 가지가 있는데, 하나는 나중에 구성 옵션으로 JES 5 설치 프로그램을 통해 가져오는 것이고 다른 하나는 Sun 다운로드 사이트에서 가져오는 것입니다.

   주 – JES 5 설치 프로그램을 통해 WAR 파일을 생성한 경우 알려진 문제점 #6550261에 나와 있는 단계를 끝까지 수행해야 합니다.

   ---

2. Access Manager WAR을 임시 영역(예: /tmp/am-staging)에 저장합니다.
3. 다음과 같은 공유 .jar 파일을 /tmp/am-staging/WEB-INF/lib에서 공유 위치(예: /export/jars)로 복사합니다.

jaxrpc-api.jar	jaxrpc-spi.jar	jaxrpc-impl.jar	saaj-api.jar
saaj-impl.jar	xercesImpl.jar	namespace.jar	xalan.jar
dom.jar	jax-qname.jar	jaxb-api.jar	jaxb-impl.jar
jaxb-libs.jar	jaxb-xjc.jar	jaxr-api.jar	jaxr-impl.jar
xmlsec.jar	swec.jar	acmecrypt.jar	iaik_ssl.jar
iaik_jce_full.jar	mail.jar	activation.jar	relaxngDatatype.jar
xsdlib.jar	mfwk_instrum_tk.jar	FastInfoset.jar	jsr173_api.jar

4. 임시 영역의 `/tmp/am-staging/WEB-INF/lib`에서 동일한 `.jar` 파일을 제거합니다.
5. Webshpere 인스턴스의 `server.xml`을 업데이트합니다. 기본 인스턴스 위치가 `/opt/WebSphere/AppServer/config/cells/`*node-name*`/nodes/`*node-name*`/servers/server1`이면 `server.xml`에서 *jvmEntries*를 아래와 같이 변경해야 합니다.

   <classpath>/export/jars/jaxrpc-api.jar:/export/jars/jaxrpc-spi.jar:
   /export/jars/jaxrpc-impl.jar:/export/jars/saaj-api.jar:
   /export/jars/saaj-impl.jar:/export/jars/xercesImpl.jar:
   /export/jars/namespace.jar:/export/jars/xalan.jar:/export/jars/dom.jar:
   /export/jars/jax-qname.jar:/export/jars/jaxb-api.jar:/export/jars/jaxb-impl.jar:
   /export/jars/jaxb-libs.jar:/export/jars/jaxb-xjc.jar:/export/jars/jaxr-api.jar:
   /export/jars/jaxr-impl.jar:/export/jars/xmlsec.jar:/export/jars/swec.jar:
   /export/jars/acmecrypt.jar:/export/jars/iaik_ssl.jar:
   /export/jars/iaik_jce_full.jar:/export/jars/mail.jar:
   /export/jars/activation.jar: /export/jars/relaxngDatatype.jar:
   /export/jars/xsdlib.jar:/export/jars/mfwk_instrum_tk.jar:
   /export/jars/FastInfoset.jar:/export/jars/jsr173_api.jar</classpath>
6. 컨테이너를 다시 시작합니다.
7. /tmp/am-staging에서 Access Manager WAR을 다시 만들어 배포합니다. 자세한 내용은 **Access Manager Deployment Planning Guide**의 Deploying Access Manager as a Single WAR File을 참조하십시오.

Weblogic 및 Webshpere에 대한 Access Manager 단일 War 작업을 수행하려면 분산 인증을 변경해야 합니다. (6554372)

컨테이너 버전이 JDK14이므로 Weblogic 8.1과 Websphere 5.1 둘 다에 대해 구문 분석을 수행하려면 분산 인증 WAR에 jar 파일이 추가로 필요합니다. JDK14 `.jar` 파일은 다음 `.zip` 파일 디렉토리에 있습니다.

ZIP-ROOT`/applications/jdk14/jarFix`

해결 방법:

Weblogic 8.1의 경우:

1. 설정 스크립트를 사용하여 분산 인증을 구성합니다. **Access Manager Post Installation Guide**의 Deploying a Distributed Authentication UI Server를 참조하십시오.

2. 업데이트된 분산 인증 WAR을 임시 위치(예: `/tmp/dist-auth`)에 저장합니다.
3. `xercesImpl.jar`, `dom.jar` 및 `xalan.jar`을 *ZIP-ROOT*`/applications/jdk14/jarFix`에서 `/tmp/dist_auth/WEB-INF/lib` 디렉토리로 복사합니다.
4. 임시 위치에서 분산 인증 WAR을 다시 생성하여 배포합니다. 자세한 내용은 **Access Manager Post Installation Guide**의 Deploying a Distributed Authentication UI Server WAR File을 참조하십시오.

Websphere 5.1의 경우:

1. 설정 스크립트를 사용하여 분산 인증을 구성합니다. **Access Manager Post Installation Guide**의 Deploying a Distributed Authentication UI Server를 참조하십시오.
2. 업데이트된 분산 인증 WAR을 임시 위치(예: `/tmp/dist_auth/`)에 저장합니다.
3. `xercesImpl.jar`, `dom.jar` 및 `xalan.jar`을 *ZIP-ROOT*`/applications/jdk14/jarFix`에서 `/tmp/dist_auth/WEB-INF/lib` 디렉토리로 복사합니다.
4. `WEB-INF/web.xml` 파일을 편집하여 `jar://web-app_2_3.dtd`를 `http://java.sun.com/dtd/web-app_2_3.dtd`로 교체합니다.
5. 임시 위치에서 분산 인증 WAR을 다시 생성하여 배포합니다. 자세한 내용은 **Access Manager Post Installation Guide**의 Deploying a Distributed Authentication UI Server WAR File을 참조하십시오.

단일 WAR 구성자가 DS에서 실패합니다. (6562076)

단일 WAR로 배포된 Access Manager가 단일 구성 요소 루트 접미사(예: `dc=example`)를 사용한 Directory Server 6에서 구성에 실패합니다. 하지만 여러 구성 요소 루트 접미사(예: `dc=example,dc=com`)를 사용하는 경우에는 문제 없이 구성됩니다.

해결 방법: 여러 구성 요소 루트 접미사(예: `dc=example,dc=com`)를 사용합니다.

동일한 호스트에서 AM 단일 WAR을 여러 서버에 대해 구성하면 예외가 발생합니다. (6490150)

동일한 호스트에서 Access Manager 단일 WAR의 두 번째 인스턴스를 Directory Server에 대해 구성하면 조직 별칭을 업데이트하는 동안 오류가 발생합니다. 구성된 두 번째 인스턴스가 다른 호스트에 있는 경우에는 이 문제가 발생하지 않습니다.

업그레이드 문제

업그레이드 문제에 대한 자세한 내용은 **Sun Java Enterprise System 5 Release Notes for UNIX**의 "Upgrade Issues" 절을 참조하십시오.

호환성 문제

- 21 페이지 “Universal Web Client의 Access Manager 단일 사인 온(SSO)이 실패함(6367058, 6429573)”
- 21 페이지 “64비트 모드로 실행 중인 Web Server 7.0에서 StackOverflowError가 발생함(6449977)”
- 22 페이지 “레거시 모드에 대한 핵심 인증 모듈의 비호환성(6305840)”
- 22 페이지 “Delegated Administrator의 commadmin 유틸리티가 사용자를 만들지 않음(6294603)”
- 23 페이지 “Delegated Administrator의 commadmin 유틸리티가 조직을 만들지 않음(6292104)”

Universal Web Client의 Access Manager 단일 사인 온(SSO)이 실패함(6367058, 6429573)

이 문제는 Access Manager, Messaging Server, Calendar Server를 설치하고 함께 작동하도록 구성한 다음 JES5 120955-01 패치를 설치한 경우 발생합니다. 사용자는 로그인 오류를 경험하게 됩니다. 이 오류는 Policy Agent 2.1 등록 정보와 AMSDK 간의 비호환성에 의해 발생합니다. 현재로서는 해결 방법이 없습니다.

64비트 모드로 실행 중인 Web Server 7.0에서 StackOverflowError가 발생함(6449977)

64비트 JVM을 사용하여 Web Server 7.0 인스턴스에 Access Manager를 구성한 경우 콘솔 로그인 페이지에 액세스할 때 서버 오류 메시지가 표시됩니다. Web Server 오류 로그에 `StackOverflowError` 예외가 포함됩니다.

해결 방법: 다음 단계에 따라 Web Server 구성을 수정합니다.

1. Web Server 관리 콘솔에 Web Server 관리자로 로그인합니다.
2. [구성 편집]을 누릅니다.

   [플랫폼] 필드에서 [64]를 선택하고 [저장]을 누릅니다.
3. [Java] 탭을 누른 다음 [JVM 설정] 탭을 누릅니다.
   - [옵션] 아래에서 최소 힙 크기 항목을 찾습니다(예: -Xms). 최소 힙 크기 값은 512m 이상이어야 합니다. 예를 들어 힙 크기 값이 -Xms512m보다 작은 경우 -Xms512m 이상으로 값을 변경합니다.
   - 최대 힙 크기 값은 768m 이상이어야 합니다. 최대 힙 크기가 -Xmx768m보다 작은 경우 -Xmx768m 이상으로 값을 변경합니다.
   - `-Xss512k` 또는 `-Xss768k`를 사용하여 Java 스택 크기를 512k 또는 768k로 설정합니다. Solaris Sparc 상에서 64비트 JVM의 경우 비워두면 기본 크기(1024k)로 설정할 수 있습니다.
4. [성능] 탭을 누르고 [스레드 풀 설정] 링크를 누릅니다.

   스택 크기를 261144 이상으로 변경하고 [저장]을 누릅니다.

5. 화면 오른쪽 위 모서리에 있는 [보류 중인 배포] 링크를 누릅니다.

   [구성 배포] 페이지에서 [배포] 버튼을 누릅니다.
6. [결과] 창에서 [확인]을 눌러 Web Server 인스턴스를 다시 시작합니다.

   Web Server가 다시 시작된 후에 [결과] 창에서 [닫기]를 누릅니다.

레거시 모드에 대한 핵심 인증 모듈의 비호환성(6305840)

Access Manager 7.1 레거시 모드에는 Access Manager 6 2005Q1의 핵심 인증 모듈에서 다음과 같은 비호환성이 있습니다.

- 레거시 모드에서는 조직 인증 모듈이 제거됩니다.
- "관리자 인증 구성" 및 "조직 인증 구성"의 표시가 변경되었습니다. Access Manager 7.1 콘솔에서 드롭다운 목록에 `ldapService`가 기본적으로 선택되어 있습니다. Access Manager 6 2005Q1 콘솔에는 [편집] 버튼이 제공되고 LDAP 모듈이 기본적으로 선택되어 있지 않습니다.

해결 방법: 없음.

Delegated Administrator의 `commadmin` 유틸리티가 사용자를 만들지 않음(6294603)

`-S mail,cal` 옵션으로 Delegated Administrator의 `commadmin` 유틸리티를 사용하면 기본 도메인에서 사용자를 만들지 않습니다.

해결 방법: 이 문제는 Access Manager를 버전 7.1로 업그레이드했지만 Delegated Administrator는 업그레이드하지 않은 경우 발생합니다.

Delegated Administrator를 업그레이드하지 않으려면 다음 단계를 따르십시오.

1. `UserCalendarService.xml` 파일에서 `mail`, `icssubcribed` 및 `icsfirstday` 속성을 필수가 아닌 옵션으로 표시합니다. Solaris 시스템에서 이 파일의 기본 위치는 `/opt/SUNWcomm/lib/services/` 디렉토리입니다.
2. Access Manager에서 다음과 같이 `amadmin` 명령을 실행하여 기존 XML 파일을 제거합니다.

   ```
   # ./amadmin -u amadmin -w password -r UserCalendarService
   ```
3. Access Manager에서 업데이트된 XML 파일을 다음과 같이 추가합니다.

   ```
   # ./amadmin -u amadmin -w password
   -s /opt/SUNWcomm/lib/services/UserCalendarService.xml
   ```
4. Access Manager 웹 컨테이너를 다시 시작합니다.

Delegated Administrator의 commadmin 유틸리티가 조직을 만들지 않음(6292104)

-S mail,cal 옵션으로 Delegated Administrator의 commadmin 유틸리티를 사용하면 조직을 만들지 않습니다.

해결 방법: 이전 문제에 대한 해결 방법을 참조하십시오.

구성 문제

- 24 페이지 "웹 컨테이너 없이 Access Manager SDK 설치를 위해 알림 URL을 업데이트해야 함(6491977)"
- 24 페이지 "비밀번호가 변경되면 비밀번호 재설정 서비스가 알림 오류를 보고함(6455079)"
- 24 페이지 "플랫폼 서버 목록 및 FQDN 별칭 속성이 업데이트되지 않음(6309259, 6308649)"
- 24 페이지 "서비스의 필수 속성에 대한 데이터 검증(6308653)"
- 25 페이지 "보안 WebLogic 8.1 인스턴스에 배포를 위한 문서 해결 방법(6295863)"
- 25 페이지 "amconfig 스크립트가 영역/DNS 별칭과 플랫폼 서버 목록 항목을 업데이트하지 않음(6284161)"
- 25 페이지 "구성 상태 파일 템플리트의 기본 Access Manager 모드가 영역임(6280844)"

로드 밸런서 뒤에서 콘솔 리디렉션이 잘못됨(6480354)

로드 밸런서 뒤에 Access Manager 인스턴스를 배포한 경우 Access Manager 콘솔에 로그인하면 로드 밸런서가 아니라 Access Manager 인스턴스 중 하나로 리디렉션될 수 있습니다. 또한 브라우저의 URL도 Access Manager 인스턴스로 변경됩니다. 예를 들어 다음 URL을 사용하여 콘솔에 로그인하면 이 문제가 발생할 수 있습니다.

```
http://loadbalancer.example.com/amserver/realm
```

이러한 리디렉션은 영역 모드와 레거시 모드 배포 둘 다에서 발생할 수 있습니다.

이 문제를 해결하는 방법은 두 가지가 있으며 둘 중 하나를 사용하면 됩니다.

1. 다음 URL 중 하나를 사용하여 로그인합니다.

   http:// *loadbalancer*/amserver/UI/Login

   http:// *loadbalancer*/amserver

2. AMConfig.properties에서 com.sun.identity.loginurl 등록 정보를 로드 밸런서 이름으로 설정합니다. 이 작업은 로드 밸런서 뒤에 있는 각각의 Access Manager 인스턴스에 대해 수행해야 합니다.

웹 컨테이너 없이 Access Manager SDK 설치를 위해 알림 URL을 업데이트해야 함(6491977)

지금 구성 옵션으로 Java ES 5 설치 프로그램을 실행하여 웹 컨테이너 없이 Access Manager SDK를 설치할 경우, AMConfig.properties 파일의 `com.iplanet.am.notification.url` 등록 정보가 `NOTIFICATION_URL`로 설정됩니다. 추가 웹 컨테이너 구성을 수행하지 않은 경우, 사용자는 원격 Aceess Manager 서버로부터 알림을 받지 않게 됩니다.

해결 방법: 이 등록 정보를 다음과 같이 재설정하십시오.

```
com.iplanet.am.notification.url=""
```

비밀번호가 변경되면 비밀번호 재설정 서비스가 알림 오류를 보고함(6455079)

비밀번호가 변경되면 Access Manager가 정규화되지 않은 보내는 사람 이름 `Identity-Server`를 사용하여 전자 메일 알림을 제출하며 이로 인해 `amPasswordReset` 로그에 오류 항목이 기록됩니다. 예를 들면 다음과 같습니다.

```
07/19/2006 10:26:04:010 AM PDT: Thread[service-j2ee,5,main]
ERROR: Could not send email to user [Ljava.lang.String;@999262
com.sun.mail.smtp.SMTPSendFailedException: 553 5.5.4 <Identity-Server>...
Domain name required for sender address Identity-Server
```

해결 방법: `/opt/SUNWam/locale/amPasswordResetModuleMsgs.properties`에서 구성을 변경합니다.

- 다음과 같이 주소를 변경합니다. `fromAddress.label=<Identity-Server>` 항목을 `fromAddress.label=<IdentityServer@myhost.company.com>`으로 변경합니다.
- 잠금 알림이 올바른 `from` 주소를 사용하도록 `lockOutEmailFrom` 등록 정보를 변경합니다.

플랫폼 서버 목록 및 FQDN 별칭 속성이 업데이트되지 않음(6309259, 6308649)

다중 서버 배포에서 Access Manager를 보조(및 후속) 서버에 설치한 경우 플랫폼 서버 목록 및 FQDN 별칭 속성이 업데이트되지 않습니다.

해결 방법: 영역/DNS 별칭과 플랫폼 서버 목록 항목을 수동으로 추가합니다. 수행하는 단계는 **Sun Java System Access Manager 7.1 Postinstallation Guide**의 "Adding Additional Instances to the Platform Server List and Realm/DNS Aliases" 절을 참조하십시오.

서비스의 필수 속성에 대한 데이터 검증(6308653)

Access Manager 7.1에서는 서비스 XML 파일의 필수 속성에 반드시 기본값이 있어야 합니다.

해결 방법: 값이 없는 필수 속성을 포함하는 서비스가 있는 경우 속성에 대한 값을 추가한 후 서비스를 다시 로드합니다.

보안 WebLogic 8.1 인스턴스에 배포를 위한 문서 해결 방법(6295863)

Access Manager 7.1을 보안(SSL 사용 가능) BEA WebLogic 8.1 SP4 인스턴스에 배포하는 경우 각 Access Manager 웹 응용 프로그램을 배포하는 동안 예외가 발생합니다.

해결 방법: 다음 단계를 따르십시오.

1. BEA에서 사용 가능한 WebLogic 8.1 SP4 패치 JAR `CR210310_81sp4.jar`을 적용합니다.
2. `/opt/SUNWam/bin/amwl81config` 스크립트(Solaris 시스템) 또는 `/opt/sun/identity/bin/amwl81config` 스크립트(Linux 시스템)에서 `doDeploy` 함수와 `undeploy_it` 함수를 업데이트하여 Access Manager 웹 응용 프로그램을 배포 및 배포 해제하는 데 사용되는 `classpath`가 포함된 `wl8_classpath` 변수 앞에 패치 JAR의 경로를 추가합니다.

   `wl8_classpath`를 포함하는 다음 행을 찾습니다.

   ```
   wl8_classpath= ...
   ```
3. 2단계에서 찾은 행 바로 뒤에 다음 행을 추가합니다.

   ```
   wl8_classpath=path-to-CR210310_81sp4.jar:$wl8_classpath
   ```

amconfig 스크립트가 영역/DNS 별칭과 플랫폼 서버 목록 항목을 업데이트하지 않음(6284161)

다중 서버 배포에서 `amconfig` 스크립트가 추가 Access Manager 인스턴스에 대해 영역/DNS 별칭 및 플랫폼 서버 목록 항목을 업데이트하지 않습니다.

해결 방법: 영역/DNS 별칭과 플랫폼 서버 목록 항목을 수동으로 추가합니다. 수행하는 단계는 **Sun Java System Access Manager 7.1 Postinstallation Guide**의 "Adding Additional Instances to the Platform Server List and Realm/DNS Aliases" 절을 참조하십시오.

구성 상태 파일 템플리트의 기본 Access Manager 모드가 영역임(6280844)

기본적으로 구성 상태 파일 템플리트에서 Access Manager 모드(`AM_REALM` 변수)를 사용 가능하게 할 수 있습니다.

해결 방법: 레거시 모드로 Access Manager를 설치 또는 구성하려면 상태 파일에서 해당 변수를 다시 설정합니다.

```
AM_REALM = disabled
```

성능 문제

영역 모드에서 새 그룹을 만들면 전혀 사용되지 않는 ACI가 포함된 그룹 관리 항목이 생성됩니다. (6485695)

Access Manager가 영역 모드로 설치된 경우 새 그룹을 만들 때마다 Access Manager는 그룹을 관리하는 데 필요한 ACI가 포함된 새 그룹 관리 항목을 동적으로 만듭니다. 영역 모드에서는 이러한 그룹 관리 ACI가 사용되지 않습니다. 하지만 Directory Server가 접미사에서 항목을 처리하는 동안 이를 평가하므로 Access Manager 성능이 저하될 수 있으며, 특히 배포에서 많은 수의 그룹을 만드는 경우 더욱 저하됩니다.

해결 방법: 이 문제의 해결 방법은 두 부분으로 구성되어 있습니다.

- 새 그룹을 만들 때마다 Access Manager가 그룹 관리자 및 해당 ACI를 만들지 않도록 합니다.
- Directory Server에서 기존 그룹 관리자 ACI를 모두 제거합니다.

그룹 관리자 ACI 생성 중단

다음 절차를 수행하여 새 그룹을 만들 때마다 Access Manager가 그룹 관리 및 해당 ACI를 만들지 않도록 합니다.

주 – 이 절차를 수행하면 새 그룹을 만들 때마다 그룹 관리 및 해당 ACI를 만드는 작업이 완전히 중단됩니다. 이러한 작업이 사용자의 배포 환경에 적합한 경우에만 이 절차를 사용하십시오.

---

1. `amAdminConsole.xml` 파일을 백업합니다. 이 파일은 사용자 플랫폼에 따라 다음 디렉토리에 위치합니다.
   - Solaris 시스템: `/etc/opt/SUNWam/config/xml`
   - Linux 및 HP-UX 시스템: `/etc/opt/sun/identity/config/xml`
   - Windows 시스템: *javaes-install-dir*`\identity\config\xml`

     여기서 *javaes-install-dir*은 Java ES 5 설치 디렉토리를 나타내며 기본값은 `C:\Program Files\Sun\JavaES5`입니다.
2. `amAdminConsole.xml` 파일에서 명령줄 사이에 나와 있는 다음 그룹 관리 항목을 제거합니다.

```
<AttributeSchema name="iplanet-am-admin-console-dynamic-aci-list"
    type="list"
    syntax="string"
    i18nKey="g111">
    <DefaultValues>
...
# Beginning of entry to delete
```

```
                <Value>Group Admin|Group Admin Description|ORGANIZATION:aci:
(target="ldap:///GROUPNAME")(targetattr = "*")
(version 3.0; acl "Group and people container admin role";
allow (all) roledn = "ldap:///ROLENAME";)##ORGANIZATION:aci:
(target="ldap:///ORGANIZATION")
(targetfilter=(&amp;FILTER(!(|(nsroledn=cn=Top-level Admin Role,dc=iplanet,dc=com)
(nsroledn=cn=Top-level Help Desk Admin Role,dc=iplanet,dc=com)
(nsroledn=cn=Top-level Policy Admin Role,dc=iplanet,dc=com)
(nsroledn=cn=Organization Admin Role,ORGANIZATION)
(nsroledn=cn=Container Admin Role,ORGANIZATION)
(nsroledn=cn=Organization Policy Admin Role,ORGANIZATION)))))
(targetattr != "iplanet-am-web-agent-access-allow-list ||
iplanet-am-web-agent-access-not-enforced-list||
iplanet-am-domain-url-access-allow ||
iplanet-am-web-agent-access-deny-list ||nsroledn")
(version 3.0; acl "Group admin's right to the members"; allow (read,write,search)
roledn = "ldap:///ROLENAME";)</Value>
# End of entry to delete
...
    </DefaultValues>
</AttributeSchema>
```

3. amadmin을 사용하여 Access Manager에서 관리 콘솔 서비스를 삭제합니다. 예를 들어 Solaris 시스템의 경우 다음을 삭제합니다.

```
# cd /opt/SUNWam/bin
# ./amadmin -u amadmin -w amadmin_password
--deleteService iPlanetAMAdminConsoleService
```

4. amadmin을 사용하여 관리 콘솔 서비스를 2단계에서 편집한 amAdminConsole.xml 파일에서 Access Manager로 다시 로드합니다. 예를 들면 다음과 같습니다.

```
# ./amadmin -u amadmin -w amadmin_password
-t /etc/opt/SUNWam/config/xml/amAdminConsole.xml
```

5. Access Manager 웹 컨테이너를 다시 시작합니다. Directory Server에서 ACI를 제거하려면 다음 절차에서 설명하는 대로 해당 절차를 마친 후 잠시 기다렸다가 웹 컨테이너를 다시 시작합니다.

기존 그룹 관리 ACI 제거

주 – 다음 절차에서는 ldapsearch 및 ldapmodify 유틸리티를 사용하여 그룹 관리 ACI를 찾아서 제거합니다. 배포에서 Directory Server 6.0을 사용하는 경우 DSCC(Directory Server Control Center) 또는 dsconf 명령을 사용하여 이 기능을 수행할 수도 있습니다. 자세한 내용은 Directory Server 6.0 설명서를 참조하십시오.

http://docs.sun.com/app/docs/coll/1224.1

다음 절차에서는 Directory Server에 이미 있는 그룹 관리 ACI를 제거합니다.

1. 그룹 관리 ACI를 제거하려면 `ldapmodify`와 함께 사용할 LDIF 파일을 만듭니다. 이러한 ACI를 찾으려면 `ldapsearch`를 사용하거나 원하는 경우 다른 디렉토리 검색 도구를 사용합니다.

   예를 들어 `Remove_Group_ACIs.ldif`라는 예제 LDIF 파일의 다음 항목은 New Group이라는 그룹의 ACI를 제거합니다.

```
dn: ROOT_SUFFIX
changetype: modify
delete: aci
aci: (target="ldap:///cn=New Group,ou=Groups,o=isp")(targetattr = "*")
(version 3.0; acl "Group and people container admin role"; allow (all)
roledn = "ldap:///cn=cn=New Group_ou=Groups_o=isp,o=isp";)

dn: ROOT_SUFFIX
changetype: modify
delete: aci
aci: (target="ldap:///ou=People,o=isp")(targetattr="nsroledn")
(targattrfilters="add=nsroledn:(!(nsroledn=*)),
del=nsroledn:(!(nsroledn=*))") (version 3.0;
acl "Group admin's right to add user to people container"; allow (add)
roledn = "ldap:///cn=cn=New Group_ou=Groups_o=isp,o=isp";)

dn: ROOT_SUFFIX
changetype: modify
delete: aci
aci: (target="ldap:///o=isp")
(targetfilter=(&(|(memberof=*cn=New Group,ou=Groups,o=isp)
(iplanet-am-static-group-dn=*cn=New Group,ou=Groups,o=isp))
(!(|(nsroledn=cn=Top-level Admin Role,o=isp)
(nsroledn=cn=Top-level Help Desk Admin Role,o=isp)
(nsroledn=cn=Top-level Policy Admin Role,o=isp)
(nsroledn=cn=Organization Admin Role,o=isp)(
nsroledn=cn=Container Admin Role,o=isp)
(nsroledn=cn=Organization Policy Admin Role,o=isp)))))
(targetattr != "iplanet-am-web-agent-access-allow-list ||
iplanet-am-web-agent-access-not-enforced-list ||
iplanet-am-domain-url-access-allow ||
iplanet-am-web-agent-access-deny-list ||nsroledn")
(version 3.0; acl "Group admin's right to the members";
allow (read,write,search)
roledn = "ldap:///cn=cn=New Group_ou=Groups_o=isp,o=isp";)
aci: (target="ldap:///o=isp")(targetattr="*")
(version 3.0; acl "S1IS special dsame user rights for all under the root suffix";
allow (all) userdn = "ldap: ///cn=dsameuser,ou=DSAME Users,o=isp"; )
```

2. 이전 단계에서 만든 LDIF 파일을 `ldapmodify`와 함께 사용하여 Directory Server에서 그룹 ACI를 제거합니다. 예를 들면 다음과 같습니다.

```
# ldapmodify -h ds-host -p 389 -D "cn=Directory Manager"
-w ds-bind-password -f Remove_Group_ACIs.ldif
```

3. Access Manager 웹 컨테이너를 다시 시작합니다.

Access Manager 콘솔 문제

- 29 페이지 "새 Access Manager 콘솔에서 CoS 템플리트 우선 순위를 설정할 수 없음(6309262)"
- 29 페이지 "Portal Server 관련 서비스를 추가할 때 이전 콘솔이 나타남(6293299)"
- 29 페이지 "자원 제한에 도달한 후 콘솔이 Directory Server에서 결과 집합을 반환하지 않음(6239724)"
- 30 페이지 "데이터 마이그레이션 후 `ContainerDefaultTemplateRole` 속성 추가(4677779)"

새 Access Manager 콘솔에서 CoS 템플리트 우선 순위를 설정할 수 없음(6309262)

새 Access Manager 7.1 콘솔에서 CoS(Class of Service) 템플리트 우선 순위를 설정 또는 수정할 수 없습니다.

해결 방법: Access Manager 6 2005Q1 콘솔에 로그인하여 CoS 템플리트 우선 순위를 설정 또는 수정합니다.

Portal Server 관련 서비스를 추가할 때 이전 콘솔이 나타남(6293299)

Portal Server 및 Access Manager가 동일한 서버에 설치되었습니다. Access Manager가 레거시 모드로 설치된 경우 `/amserver`를 사용하여 새 Access Manager 콘솔에 로그인합니다. 기존 사용자를 선택하고 서비스(예: NetFile 또는 Netlet) 추가를 시도하면 이전 Access Manager 콘솔(`/amconsle`)이 갑자기 나타납니다.

해결 방법: 없음. 현재 버전의 Portal Server에는 Access Manager 6 2005Q1 콘솔이 필요합니다.

자원 제한에 도달한 후 콘솔이 Directory Server에서 결과 집합을 반환하지 않음(6239724)

Directory Server를 설치한 후 기존 DIT 옵션으로 Access Manager를 설치합니다. Access Manager 콘솔에 로그인하여 그룹을 만듭니다. 그룹에서 사용자를 편집합니다. 예를 들어 `uid=*999*` 필터로 사용자를 추가합니다. 결과 목록 상자가 비어 있고 콘솔에 어떤 오류나 정보 또는 경고 메시지도 표시되지 않습니다.

해결 방법: 그룹 구성원이 Directory Server 검색 크기 제한보다 크지 않아야 합니다. 그룹 구성원이 더 큰 경우 검색 크기 제한을 그에 맞게 변경하십시오.

데이터 마이그레이션 후 ContainerDefaultTemplateRole 속성 추가(4677779)

레거시 모드에서는 사용자 역할이 Access Manager로 만들지 않은 조직에 표시되지 않습니다. 디버그 모드에서 다음 메시지가 나타납니다.

```
ERROR: DesktopServlet.handleException()
com.iplanet.portalserver.desktop.DesktopException:
DesktopServlet.doGetPost(): no privilige to execute desktop
```

Java ES 설치 프로그램 마이그레이션 스크립트가 실행된 후 반드시 이 오류가 나타납니다. 기존의 디렉토리 정보 트리(DIT)나 다른 소스에서 조직을 마이그레이션하는 경우 ContainerDefaultTemplateRole 속성이 자동으로 조직에 추가되지 않습니다.

해결 방법: Directory Server 콘솔을 사용하여 ContainerDefaultTemplateRole 속성을 다른 Access Manager 조직에서 복사한 다음 관련된 조직에 추가합니다.

명령줄 문제

조직 관리자 역할이 amadmin 명령줄 유틸리티를 사용하여 새 사용자를 만들지 못함(6480776)

조직 관리자 역할이 지정된 관리자가 잘못된 로깅 권한으로 인해 adadmin 명령줄 유틸리티를 사용하여 새 사용자를 만들 수 없습니다.

해결 방법: 조직 관리자와 최상위 관리자가 권한을 설정할 수 있습니다. 이 작업은 관리 콘솔에서 수행합니다.

1. 조직 관리자가 속한 조직으로 이동합니다.
2. [권한] 탭을 누릅니다.
3. [조직 관리자 역할] 링크를 누릅니다.
4. **모든 로그 파일에 대한 읽기 및 쓰기 권한** 또는 **모든 로그 파일에 대한 쓰기 권한**을 선택합니다.
5. [저장]을 누릅니다.

SDK 및 클라이언트 문제

- 31 페이지 "서버가 다시 시작된 후 클라이언트가 알림을 가져오지 않음(6309161)"
- 31 페이지 "서비스 스키마가 변경된 후 SDK 클라이언트를 다시 시작해야 함(6292616)"

서버가 다시 시작된 후 클라이언트가 알림을 가져오지 않음(6309161)

서버가 다시 시작된 경우 클라이언트 SDK(`amclientsdk.jar`)를 사용하여 작성한 응용 프로그램이 알림을 가져오지 않습니다.

해결 방법: 없음.

서비스 스키마가 변경된 후 SDK 클라이언트를 다시 시작해야 함(6292616)

모든 서비스 스키마를 변경한 경우 `ServiceSchema.getGlobalSchema`가 새 스키마가 아닌 이전 스키마를 반환합니다.

해결 방법: 서비스 스키마를 변경한 후 클라이언트를 다시 시작합니다.

이 문제는 패치 1에서 해결되었습니다.

인증 문제

- 31 페이지 "응용 프로그램 사용자의 권한이 부족한 경우 분산 인증 UI 서버 성능이 저하됨(6470055)"
- 32 페이지 "레거시(호환) 모드에 대한 통계 서비스의 Access Manager 기본 구성 비호환성(6286628)"
- 32 페이지 "이름 지정 속성의 최상위 조직에서 속성 고유성이 잘못됨(6204537)"

응용 프로그램 사용자의 권한이 부족한 경우 분산 인증 UI 서버 성능이 저하됨(6470055)

기본 응용 프로그램 사용자를 사용하여 분산 인증 UI 서버를 배포하면 기본 응용 프로그램 사용자의 제한된 권한 때문에 성능이 상당히 저하됩니다.

해결 방법: 적절한 권한을 가진 새 사용자를 만듭니다.

적절한 ACI로 새 사용자를 만들려면 다음을 수행합니다.

1. Access Manager 콘솔에서 새 사용자를 만듭니다. 예를 들어 `AuthUIuser`라는 이름으로 사용자를 만듭니다.
2. Directory Server 콘솔에서 다음 ACI를 추가합니다.

```
dn:ou=1.0,ou=SunAMClientData,ou=ClientData,<ROOT_SUFFIX>
changetype:modifyadd:aci
aci: (target="ldap:///ou=1.0,ou=SunAMClientData,ou=ClientData,<ROOT_SUFFIX>")
(targetattr = "*"(version 3.0; acl "SunAM client data anonymous access";
allow (read, search, compare) userdn = "ldap:///<AuthUIuser's DN>";)
```

`userdn`은 `"ldap:///<AuthUIuser's DN>"`으로 설정됩니다.

3. `amsilent` 파일 편집 및 `amadmin` 명령 실행에 대한 자세한 내용은 **Sun Java System Access Manager 7.1 Postinstallation Guide**의 "To Install and Configure a Distributed Authentication UI Server"의 지침을 참조하십시오.
4. `amsilent` 파일에서 다음 등록 정보를 설정합니다.

   APPLICATION_USER `AuthUIuser`를 입력합니다.

   APPLICATION_PASSWD `AuthUIuser`에 대한 비밀번호를 입력합니다.
5. 파일을 저장합니다.
6. 새로운 구성 파일을 사용하여 `amconfig` 스크립트를 실행합니다. Access Manager를 기본 디렉토리에 설치한 Solaris 시스템의 경우에는 다음과 같습니다.

```
# cd /opt/SUNWam/bin

# ./amconfig -s ./DistAuth_config
```

7. 분산 인증 UI 서버의 웹 컨테이너를 다시 시작합니다.

레거시(호환) 모드에 대한 통계 서비스의 Access Manager 기본 구성 비호환성(6286628)

레거시 모드에서 Access Manager를 설치한 후 통계 서비스의 기본 구성이 변경됩니다.

- 서비스가 기본적으로 활성화됩니다(`com.iplanet.services.stats.state=file`). 이전에는 기본적으로 비활성화되었습니다.
- 기본 간격(`com.iplanet.am.stats.interval`)이 3600에서 60으로 변경됩니다.
- 기본 통계 디렉토리(`com.iplanet.services.stats.directory`)가 `/var/opt/SUNWam/debug`에서 `/var/opt/SUNWam/stats`로 변경됩니다.

해결 방법: 없음.

이름 지정 속성의 최상위 조직에서 속성 고유성이 잘못됨(6204537)

Access Manager 설치 후 `amadmin`으로 로그인한 후 `o`, `sunPreferredDomain`, `associatedDomain`, `sunOrganizationAlias`, `uid` 그리고 `mail` 속성을 고유 속성 목록에 추가합니다. 같은 이름으로 새 조직을 두 개 만드는 경우 작업은 실패하지만 Access Manager는 표시되어야 할 "속성 고유성을 위반했습니다"라는 메시지 대신 "조직이 이미 있습니다"라는 메시지를 표시합니다.

해결 방법: 없음. 잘못된 메시지이므로 무시하십시오. Access Manager가 올바르게 작동 중입니다.

세션 및 SSO 문제

- 33 페이지 "로드 밸런서가 SSL 종료를 포함하는 경우 시스템이 잘못된 서비스 호스트 이름을 만듦(6245660)"
- 33 페이지 "타사 웹 컨테이너와 HttpSession 사용 "

로드 밸런서가 SSL 종료를 포함하는 경우 시스템이 잘못된 서비스 호스트 이름을 만듦(6245660)

Access Manager가 SSL 종료를 포함하는 로드 밸런서를 사용하여 웹 컨테이너로 Web Server에 배포된 경우 클라이언트에 정확한 Web Server 페이지가 표시되지 않습니다. 잘못된 호스트 때문에 Access Manager 콘솔의 세션 탭을 누르면 오류가 반환됩니다.

해결 방법: 다음 예에서 Web Server는 포트 3030을 수신합니다. 로드 밸런서는 포트 80을 수신하며 요청을 Web Server로 리디렉션합니다.

web-server-instance-name/config/server.xml파일에서 사용 중인 Web Server 릴리스에 따라 servername 속성을 로드 밸런서를 가리키도록 편집합니다.

Web Server 6.1 Service Pack(SP) 릴리스에 대해 servername 속성을 다음과 같이 편집합니다.

```
<LS id="ls1" port="3030" servername="loadbalancer.example.com:80"
defaultvs="https-sample" security="false" ip="any" blocking="false"
acceptorthreads="1"/>
```

Web Server 6.1 SP2(이상)는 http에서 https로 또는 https에서 http로 프로토콜을 전환할 수 있습니다. 따라서 servername을 다음과 같이 편집합니다.

```
<LS id="ls1" port="3030"
servername="https://loadbalancer.example.com:443" defaultvs="https-sample"
security="false" ip="any" blocking="false" acceptorthreads="1"/>
```

타사 웹 컨테이너와 HttpSession 사용

인증을 위해 세션을 관리하는 기본적인 방법은 HttpSession이 아니라 "내부 세션"입니다. 유효하지 않은 세션의 기본 최대 시간 값은 3분으로 충분합니다. amtune 스크립트는 Web Server나 Application Server에 대해 1분을 값으로 설정합니다. 그러나 타사 웹 컨테이너(IBM WebSphere 또는 BEA WebLogic Server)와 HttpSession 옵션을 사용하는 경우 성능 문제를 해결하려면 웹 컨테이너의 최대 HttpSession 시간을 제한해야 할 수도 있습니다.

정책 문제

- 34 페이지 “정책 구성 서비스에서 동적 속성을 삭제하면 정책 편집에 문제 발생(6299074)”

정책 구성 서비스에서 동적 속성을 삭제하면 정책 편집에 문제 발생(6299074)

정책 구성 서비스에서 동적 속성을 삭제하면 정책 편집에 문제가 발생하는 시나리오는 다음과 같습니다.

1. 정책 구성 서비스에 2개의 동적 속성을 만듭니다.
2. 정책을 만들고 응답 공급자에서 1단계의 동적 속성을 선택합니다.
3. 정책 구성 서비스에서 동적 속성을 제거하고 속성을 2개 더 만듭니다.
4. 2단계에서 만든 정책의 편집을 시도합니다.

결과는 다음과 같습니다. "설정 중인 동적 등록 정보가 잘못되어 오류가 발생했습니다."라는 메시지가 표시됩니다.목록에 기본으로 표시되는 정책이 없습니다. 검색이 끝난 후 정책이 표시되지만 기존 정책을 편집 또는 삭제하거나 새 정책을 만들 수 없습니다.

해결 방법: 정책 구성 서비스에서 동적 속성을 제거하기 전에 정책에서 해당 속성에 대한 참조를 제거합니다.

서버 시작 문제

- 34 페이지 “Access Manager 시작 시 디버그 오류 발생(6309274, 6308646)”

Access Manager 시작 시 디버그 오류 발생(6309274, 6308646)

Access Manager 7.1 시작 시 `amDelegation` 및 `amProfile` 디버그 파일에서 디버그 오류를 반환합니다.

- `amDelegation`: 위임용 플러그인 인스턴스를 가져올 수 없습니다.
- `amProfile`: 위임 예외가 발생했습니다.

해결 방법: 없음. 이 메시지를 무시해도 됩니다.

AMSDK 문제

- 35 페이지 “ AMIdentity.modifyService 수행 시 오류가 표시됨(6506448)”
- 35 페이지 “선택된 목록에 그룹 구성원이 표시되지 않음(6459598)”

- 36 페이지 “Access Manager 로그인 URL에서 "그런 조직을 찾지 못했습니다." 메시지를 반환함(6430874)”
- 36 페이지 “amadmin을 사용할 때 Access Manager에서 하위 조직을 만들 수 없음(5001850)”

AMIdentity.modifyService 수행 시 오류가 표시됨(6506448)

AMIdentity.modifyService를 사용하여 영역의 데스크탑 서비스 동적 속성을 설정할 때 Access Manager가 null 포인터 예외를 반환합니다.

해결 방법: 다음 등록 정보를 AMConfig.properties에 추가한 다음 서버를 다시 시작합니다.

```
com.sun.am.ldap.connnection.idle.seconds=7200
```

선택된 목록에 그룹 구성원이 표시되지 않음(6459598)

이 문제는 다음과 같은 조건에서 발생합니다.

1. 다음 영역 구성으로 영역을 정의합니다.
   - 최상위 영역은 amroot입니다. 하위 영역은 example.com입니다.
   - example.com 하위 영역에는exampleDB 및 exampledminDB의 두 데이터 저장소가 있습니다.
   - exampleDB 데이터 저장소는 dc=example,dc=com에서 시작하는 모든 사용자를 포함합니다. 지원되는 LDAPv3 작업은 user=read,write,create,delete,service로 설정됩니다.
   - exampleadminDB 데이터 저장소는 영역에 대한 관리자 그룹을 포함합니다. 관리자 그룹은 DN: cn=example.com Realm Administrators,ou=Groups,dc=example,dc=com입니다. 이 그룹에는 단일 구성원 scarter가 있습니다. 지원되는 LDAPv3 작업은 group=read,write,create,delete로 설정됩니다.
2. [제목] 탭을 누르고 [그룹]을 누른 다음 example.com Realm Administrators에 대한 항목을 누릅니다.
3. [사용자] 탭을 누릅니다.

exampleDB 데이터 저장소에 있는 모든 사용자가 사용할 수 있는 것으로 표시되지만 선택된 필드에 scarter는 표시되지 않습니다.

해결 방법: exampleadminDB 데이터 저장소에서 지원되는 LDAPv3 작업에 user=read 작업을 추가합니다.

Access Manager 로그인 URL에서 "그런 조직을 찾지 못했습니다." 메시지를 반환함(6430874)

이 문제는 정규화된 도메인 이름(FQDN)에 대소문자를 혼합하여 사용했기 때문에 발생했을 수 있습니다.

예를 들면 다음과 같습니다. `HostName.PRC.Example.COM`

해결 방법: 설치 후에 기본 Access Manager 로그인 URL을 사용하지 마십시오. 대신 로그인 URL에 기본 조직의 LDAP 위치를 포함하십시오. 예를 들면 다음과 같습니다.

```
http://HostName.PRC.Example.COM/amserver/UI/Login?org=dc=PRC,dc=Example,dc=COM
```

Access Manager에 성공적으로 로그인한 다음에는 Access Manager에 로그인할 때마다 사용자의 조직에 대한 전체 경로를 입력하지 않아도 됩니다. 다음 단계를 따르십시오.

1. 영역 모드에서 [영역] 탭으로 이동하거나 레거시 모드에서 [조직] 탭으로 이동합니다.
2. 기본 영역 또는 조직 이름을 누릅니다.

   이 예에서는 `prc`를 누릅니다.
3. `Realm/DNS Alias` 값에 있는 모든 대문자를 소문자로 변경합니다.

   이 예에서는 전체 소문자 값 `hostname.prc.example.com`을 목록에 추가하고 목록에서 대소문자가 혼합된 `HostName.PRC.Example.COM` 값을 제거합니다.
4. [저장]을 누르고 Access Manager 콘솔에서 로그아웃합니다.

이제 다음 중 어떤 URL을 사용하더라도 로그인할 수 있습니다.

- `http://hostname.PRC.Example.COM/amserver/UI/Login`
- `http://hostname.PRC.Example.COM/amserver`
- `http://hostname.PRC.Example.COM/amserver/console`

amadmin을 사용할 때 Access Manager에서 하위 조직을 만들 수 없음(5001850)

이 문제는 두 Directory Server 간에 다중 마스터 복제가 사용되고 있고 `amadmin` 유틸리티를 사용하여 하위 조직을 만들려고 시도한 경우 발생합니다.

해결 방법: 두 Directory Server에서 `nsslapd-lookthroughlimit` 등록 정보를 -1로 설정합니다.

SSL 문제

- 37 페이지 “SSL 인증서가 만료되면 amconfig 스크립트가 실패함(6488777)”

SSL 인증서가 만료되면 amconfig 스크립트가 실패함(6488777)

Access Manager 컨테이너가 SSL 모드로 실행 중이고 컨테이너 SSL 인증서가 만료된 경우 `amconfig`가 실패하고 classpath가 손상될 수 있습니다.

해결 방법: 만료된 인증서로 `amconfig`를 이미 실행했고 클래스 경로가 손상된 경우 먼저 올바른 SSL 인증서를 가져옵니다. 원래 `domain.xml` 파일로 되돌리거나 클래스 경로가 손상되지 않은 `domain.xml` 파일을 복사합니다. 그런 다음 `amconfig` 명령을 다시 실행합니다.

```
/opt/SUNWam/bin/amconfig -s $PWD/amsamplesilent
```

예제 문제

- 37 페이지 “Clientsdk 예제 디렉토리에 원하지 않는 makefile이 포함됨(6490071)”

Clientsdk 예제 디렉토리에 원하지 않는 makefile이 포함됨(6490071)

예제 파일은 클라이언트 SDK에 포함되어 있습니다. 이러한 예제는 독립적인 프로그램과 웹 응용 프로그램을 작성하는 방법을 설명합니다. 예제는 `Makefile.clientsdk`를 생성했던 디렉토리의 다음 하위 디렉토리에 있습니다.

```
.../clientsdk-samples/

.../clientsdk-webapps/
```

Clientsdk-samples에는 인증, 로깅, 정책 및 SAML 독립 프로그램에 대한 예제가 포함되어 있습니다. Clientsdk-webapps에는 사용자 관리, 서비스 관리 및 정책 프로그램에 대한 예제가 포함되어 있습니다. 각 예제에는 예제 프로그램을 컴파일하고 실행하는 방법이 설명된 Readme.html 파일이 있습니다.

예제를 컴파일하려면 makefile을 해당 하위 디렉토리에서 실행해야 합니다. 최상위 makefile은 하위 디렉토리에 있는 예제를 컴파일하지 않습니다.

Linux OS 문제

- 38 페이지 “Application Server에서 Access Manager를 실행할 때 JVM 문제 발생(6223676)”

Application Server에서 Access Manager를 실행할 때 JVM 문제 발생(6223676)

Red Hat Linux에서 Application Server 8.1을 실행할 경우 Application Server에 대해 Red Hat OS에서 만드는 스레드의 스택 크기는 10MB입니다. 이로 인해 Access Manager 사용자 세션의 수가 200개에 이르게 되면 JVM 자원 문제가 발생할 수 있습니다.

해결 방법: Application Server를 시작하기 전에 `ulimit` 명령을 실행하여 Red Hat OS 작업 스택 크기를 더 작은 값(2048KB 또는 256KB까지)으로 설정합니다. Application Server를 시작하는 데 사용할 콘솔에서 `ulimit` 명령을 실행합니다. 예를 들면 다음과 같습니다.

```
# ulimit -s 256;
```

Windows 및 HP-UX 문제

- 38 페이지 "zh_TW 및 es 로켈에 설치 시 Access Manager 자동 구성 실패(6515043)"
- 38 페이지 "JES 전체 스택 설치 중 HP-UX에 gettext 바이너리(AM) 필요(6497926)"

zh_TW 및 es 로켈에 설치 시 Access Manager 자동 구성 실패(6515043)

해결 방법: HP-UX 플랫폼의 `zh_TW` 및 `es` 로켈에서 Access Manager를 "나중에 구성" 모드로만 구성해야 합니다. JavaES 설치 프로그램을 시작하고 Access Manager 제품을 설치한 다음 JavaES 설치 프로그램을 종료합니다. 그런 다음 다음과 같이 Access Manager 구성자를 호출합니다.

1. `LANG=C`
2. `export LANG`
3. *accessmanager-base*`/bin/amsamplesilent` 파일을 편집합니다.
4. *accessmanager-base*`/bin/amconfig -s amsamplesilent`를 실행합니다.

JES 전체 스택 설치 중 HP-UX에 gettext 바이너리(AM) 필요(6497926)

현재 이 문제의 해결 방법은 없습니다.

연합 및 SAML 문제

- 38 페이지 "연합에서 로그아웃 오류 발생(6291744)"

연합에서 로그아웃 오류 발생(6291744)

영역 모드에서 Identity 공급자(IDP)와 서비스 공급자(SP)에서 사용자 계정을 연합하는 경우 연합을 종료한 후 로그아웃하면 "오류: 해당 조직을 찾지 못했습니다."라는 오류가 발생합니다.

해결 방법: 없음.

국제화(g11n) 문제

- 39 페이지 “zh 로켈에서 관리 콘솔 구성 요소가 영어로 표시됨(6470543)”
- 39 페이지 “콘솔에서 현재 값 및 새 값이 잘못 표시됨(6476672)”
- 39 페이지 “정책 조건 날짜를 영어 관습에 맞게 지정해야 함(6390856) ”
- 39 페이지 “클라이언트 검색에서 UTF-8 제거가 작동하지 않음(5028779)”
- 40 페이지 “멀티바이트 문자가 로그 파일에 물음표로 표시됨(5014120)”

zh 로켈에서 관리 콘솔 구성 요소가 영어로 표시됨(6470543)

브라우저 로켈을 zh로 설정할 때 Version, Help 및 Logout 버튼 등 관리 콘솔 구성 요소가 영어로 표시됩니다.

해결 방법: 브라우저 로켈 설정을 zh가 아닌 zh-cn으로 설정합니다.

콘솔에서 현재 값 및 새 값이 잘못 표시됨(6476672)

지역화된 관리 콘솔 버전에서 현재 값 및 새 값 속성의 레이블이 각각 label.current.value 및 label.new.value로 잘못 표시됩니다.

정책 조건 날짜를 영어 관습에 맞게 지정해야 함(6390856)

중국어 로켈 아래에 정책 조건 날짜 형식 레이블이 중국어 관습에 맞게 표시되지 않습니다. 제시되는 레이블은 영어 날짜 형식과 같은 날짜 형식입니다. 연결된 필드 역시 영어 날짜 형식 값을 받습니다.

해결 방법: 각 필드에 대해 필드 레이블에 제시된 날짜 형식 예를 따릅니다.

클라이언트 검색에서 UTF-8 제거가 작동하지 않음(5028779)

클라이언트 검색 기능이 올바르게 작동하지 않습니다. Access Manager 7.1 콘솔의 변경 내용이 브라우저로 자동으로 전파되지 않습니다.

해결 방법: 두 가지 해결 방법이 있습니다.

- 클라이언트 검색 절을 변경한 후 Access Manager 웹 컨테이너를 다시 시작합니다.

  또는

- Access Manager 콘솔에서 다음 단계를 따릅니다.
  1. [구성] 탭에서 [클라이언트 검색]을 누릅니다.
  2. [genericHTML]의 [편집] 링크를 누릅니다.
  3. [HTML] 탭 아래에서 [genericHTML] 링크를 누릅니다.

4. 문자 집합 목록에서 `UTF-8;q=0.5` 항목을 입력합니다(UTF-8 q 팩터가 사용자 로케일의 다른 문자 집합보다 낮은지 확인).
5. 저장, 로그아웃 후 다시 로그인합니다.

멀티바이트 문자가 로그 파일에 물음표로 표시됨(5014120)

`/var/opt/SUNWam/logs` 디렉토리의 로그 파일에 있는 멀티바이트 메시지가 물음표(?)로 표시됩니다. 로그 파일이 원시 인코딩이며 UTF-8이 아닐 수 있습니다. 웹 컨테이너 인스턴스가 특정 로케일로 시작되면 로그 파일은 해당 로케일에 대한 원시 인코딩이 됩니다. 다른 로케일로 전환한 후 웹 컨테이너 인스턴스를 다시 시작하면 진행 중인 메시지는 현재 로케일에 대해 원시 인코딩이 되지만 이전 인코딩의 메시지는 물음표로 표시됩니다.

해결 방법: 항상 동일한 원시 인코딩을 사용하여 웹 컨테이너 인스턴스를 시작합니다.

설명서 문제

- 40 페이지 “LDAPv3 플러그인의 역할 및 필터링된 역할 지원 문서화(6365196)”
- 40 페이지 “`AMConfig.properties` 파일에서 사용되지 않은 속성 문서화(6344530)”
- 41 페이지 “XML 암호화를 사용할 수 있게 설정하는 방법 문서화(6275563)”

LDAPv3 플러그인의 역할 및 필터링된 역할 지원 문서화(6365196)

Sun Java System Directory Server에 데이터가 저장되어 있는 경우 해당 패치를 적용한 후 LDAPv3 플러그인에 대한 역할 및 필터링된 역할을 구성할 수 있습니다(문제 해결 아이디 6349959). Access Manager 7.1 관리 콘솔에서 [LDAPv3 플러그인이 지원하는 유형 및 작업] 필드의 LDAPv3 구성에 다음 값을 입력합니다.

```
role: read,edit,create,delete
filteredrole: read,edit,create,delete
```

LDAPv3 구성에서 사용할 예정인 역할 및 필터링된 역할에 따라 위 항목 중 하나 또는 둘 모두 입력할 수 있습니다.

`AMConfig.properties` 파일에서 사용되지 않은 속성 문서화(6344530)

`AMConfig.properties` 파일의 다음 속성이 사용되지 않습니다.

```
com.iplanet.am.directory.host
com.iplanet.am.directory.port
```

XML 암호화를 사용할 수 있게 설정하는 방법 문서화(6275563)

Bouncy Castle JAR 파일을 사용하여 Access Manager나 Federation Manager의 XML 암호화에서 전송 키를 생성하려면 다음 단계를 따르십시오.

1. 1.5 이전 버전의 JDK를 사용하는 경우 Bouncy Castle 사이트(http://www.bouncycastle.org/)에서 Bouncy Castle JCE 공급자를 다운로드합니다. 예를 들어, JDK 1.4를 사용하면 `bcprov-jdk14-131.jar` 파일을 다운로드합니다.
2. 이전 단계에서 JAR 파일을 다운로드했으면 *jdk_root*`/jre/lib/ext` 디렉토리에 그 파일을 복사합니다.
3. 현지화된 버전의 JDK를 사용하는 경우 사용 중인 버전의 JDK에 적합한 JCE Unlimited Strength Jurisdiction 정책 파일을 Sun 사이트(http://java.sun.com)에서 다운로드합니다. IBM WebSphere를 사용하는 경우 해당 IBM 사이트에서 필요한 파일을 다운로드합니다.
4. 다운로드한 `US_export_policy.jar` 및 `local_policy.jar` 파일을 *jdk_root*`/jre/lib/security` 디렉토리에 복사합니다.
5. 1.5 이전 버전의 JDK를 사용하는 경우 *jdk_root*`/jre/lib/security/java.security` 파일을 편집하여 Bouncy Castle을 공급자 중 하나로 추가합니다. 예를 들면 다음과 같습니다.

   ```
   security.provider.6=org.bouncycastle.jce.provider.BouncyCastleProvider
   ```

6. `AMConfig.properties` 파일에서 다음 등록 정보를 true로 설정합니다.

   ```
   com.sun.identity.jss.donotInstallAtHighestPriority=true
   ```

7. Access Manager 웹 컨테이너를 다시 시작합니다.

자세한 내용은 문제 아이디 5110285(XML 암호화에 Bouncy Castle JAR 파일 필요)를 참조하십시오.

설명서 업데이트

이 설명서를 보려면 Access Manager 7.1 모음을 참조하십시오.

http://docs.sun.com/coll/1292.1

Technical Note: Deploying Access Manager to an Application Server Cluster의 1 장, "Technical Note: Deploying Access Manager Instances to an Application Server Cluster"라는 새 문서가 Access Manager 7 2005Q4 모음에 추가되었습니다.

Sun Java System Access Manager Policy Agent 2.2 모음도 새 에이전트에 대한 문서에 맞게 개정되었습니다.

http://docs.sun.com/coll/1322.1

재배포 가능 파일

Sun Java System Access Manager 7.1의 모든 파일은 제품의 라이센스가 없는 사용자에게 재배포할 수 없습니다.

문제점 보고 및 사용자 의견 제공 방법

Access Manager 또는 Sun Java Enterprise System 이용에 문제가 있는 경우 다음 방법 중 하나를 사용하여 Sun 고객 지원부에 문의하십시오.

- http://sunsolve.sun.com/의 Sun Support Resource(SunSolve) 서비스

  이 사이트에는 기술 자료, 온라인 지원 센터 및 제품 추적에 대한 링크와 유지보수 프로그램 및 지원 연락처 등이 있습니다.
- 유지보수 계약 관련 긴급 전화 번호

문제 해결을 위해 최상의 지원을 제공할 수 있도록 지원부서에 연락할 때는 다음 정보를 미리 준비해 두십시오.

- 문제가 발생한 상황 및 해당 문제가 작업에 미치는 영향 등을 비롯한 문제에 대한 설명
- 문제에 영향을 미치는 패치 및 기타 소프트웨어를 포함한 시스템 종류, 운영 체제 버전 및 제품 버전
- 문제를 재현하기 위해 사용한 방법에 대한 자세한 단계
- 오류 로그나 코어 덤프

Sun은 여러분의 의견을 환영합니다.

Sun은 설명서의 내용을 개선하기 위해 노력하고 있으며 사용자의 의견 및 제안을 환영합니다. http://docs.sun.com/을 방문하여 [의견 보내기]를 누르십시오.

해당 필드에 전체 설명서 제목과 부품 번호를 기입해 주십시오. 부품 번호는 해당 설명서의 제목 페이지나 문서 맨 위에 있으며 일반적으로 7자리 또는 9자리 숫자입니다. 예를 들어, **Access Manager 릴리스 노트**의 부품 번호는 820-0364입니다. 사용자 의견을 제출할 때 해당 양식에 영문 설명서 제목과 부품 번호를 입력해야 할 수도 있습니다. 본 설명서의 영문 부품 번호와 제목은 819-4683, Sun Java System Access Manager 7.1 Release Notes입니다.

Sun의 추가 자원

다음 위치에서 유용한 Access Manager 정보 및 자원을 찾을 수 있습니다.

- Sun Java Enterprise System 문서: http://docs.sun.com/prod/entsys.05q4
- Sun 서비스: http://www.sun.com/service/consulting/
- 소프트웨어 제품 및 서비스: http://wwws.sun.com/software/
- 지원 자원: http://sunsolve.sun.com/
- 개발자 정보: http://developers.sun.com/
- Sun 개발자 지원 서비스: http://www.sun.com/developers/support/

내게 필요한 옵션 기능

이 매체를 발행한 이후 릴리스된 내게 필요한 옵션 기능을 사용하려면 Sun에 요청하여 구할 수 있는 508 절 제품 평가를 참조하여 관련 솔루션을 배포하는 데 가장 적합한 버전을 확인하십시오. 응용 프로그램의 업데이트된 버전은 http://sun.com/software/javaenterprisesystem/get.html에서 볼 수 있습니다.

내게 필요한 옵션 기능 구현을 위한 Sun의 방침에 대해 자세히 알아보려면 http://sun.com/access를 방문하십시오.

타사 웹 사이트

이 설명서에 있는 타사 URL을 참조하여 추가 관련 정보를 살펴 보십시오.

주 – Sun은 본 설명서에서 언급된 타사 웹 사이트의 가용성 여부에 대해 책임을 지지 않습니다. 또한 해당 사이트나 리소스를 통해 제공되는 내용, 광고, 제품 및 기타 자료에 대해 어떠한 보증도 하지 않으며 그에 대한 책임도 지지 않습니다. 따라서 타사 웹 사이트의 내용, 제품 또는 리소스의 사용으로 인해 발생한 실제 또는 주장된 손상이나 피해에 대해서도 책임을 지지 않습니다.
