Sun Java System Access Manager 7 2005Q4 릴리스 노트

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

부품 번호: 819–3477
2008년 8월 19일

080908@20795

목차

Sun Java System Access Manager 7 2005Q4 릴리스 노트

2008년 8월 19일

부품 번호 819-3477

Sun Java™ System Access Manager(Access Manager) 7 2005Q4 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. 본 릴리스의 설치 및 사용 전에 이 문서를 읽으시기 바랍니다.

본 릴리스 노트에 대한 자세한 내용은 6 페이지 "개정 내역"을 참조하십시오.

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

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

목차

Access Manager 7 2005Q4 릴리스 노트는 다음 절을 포함합니다.

개정 내역

다음 표는 Access Manager 7 2005Q4 릴리스 노트의 개정 내역을 보여 줍니다.

표 1 개정 내역

날짜	변경 내용
2008년 8월 19일	9 페이지 “Access Manager 7 2005Q4 패치 릴리스” 절에 Windows 및 HP-UX 시스템용 패치 7에 대한 정보를 추가했습니다.
2008년 5월 12일	■ 9 페이지 “Access Manager 7 2005Q4 패치 릴리스” 절에 패치 7에 대한 정보를 추가했습니다. ■ 67 페이지 “시스템 가상화 지원” 절을 추가했습니다.
2007년 10월 16일	이 수정본의 변경 내용은 다음과 같습니다. ■ 9 페이지 “Access Manager 7 2005Q4 패치 릴리스” 절에 패치 6에 대한 정보를 추가했습니다. ■ 41 페이지 “CR# 6522720: Windows 및 HP-UX 시스템의 경우 콘솔 온라인 도움말에서 멀티 바이트 문자 검색이 동작하지 않습니다.”를 업데이트했습니다. 패치 6은 Windows 시스템에서의 이 문제를 수정했습니다. 그러나 HP-UX 시스템에서는 이 문제가 여전히 존재합니다.
2007년 7월 10일	이 수정본의 변경 내용은 다음과 같습니다. ■ 9 페이지 “Access Manager 7 2005Q4 패치 릴리스” 절에 HP-UX 시스템용 패치 126371-05에 대한 정보를 추가했습니다. ■ 새로운 문제 84 페이지 “Access Manager가 Directory Proxy를 가리키는 경우 Null 속성 LDAP 검색 시 오류를 반환합니다(6357975).”를 추가했습니다.
2007년 3월 16일	이 수정본의 변경 내용은 다음과 같습니다. ■ 9 페이지 “Access Manager 7 2005Q4 패치 릴리스” 절에 패치 5에 대한 정보를 추가했습니다. ■ 92 페이지 “설명서 문제”에 설명과 새로운 정보를 추가했습니다. ■ 검토자의 의견과 변경 요청(CR)에 따라 다른 기술과 편집 측면에서 다양하게 변경되었습니다.

표 1 개정 내역 (계속)

날짜	변경 내용
2006년 10월 30일	9 페이지 “Access Manager 7 2005Q4 패치 릴리스” 절의 변경 내용은 다음과 같습니다. ■ 패치 4에 대한 정보를 추가했습니다. ■ 일관되지 않은 *AccessManager-base* 사용이 수정되었습니다. ■ 51 페이지 “CR# 6440651: 쿠키 재생에 `com.sun.identity.session.resetLBCookie` 등록 정보가 필요합니다.”에 대한 설명이 개정되었습니다.
2006년 8월 25일	9 페이지 “Access Manager 7 2005Q4 패치 릴리스” 절의 변경 내용은 다음과 같습니다. ■ 패치 3에 대한 정보를 추가했습니다. ■ 패치 1 및 패치 2에 대한 정보를 개정하고 추가했습니다.
2006년 5월 25일	이 수정본의 변경 내용은 다음과 같습니다. ■ 54 페이지 “Access Manager 7 2005Q4 패치 2” 절이 새로 추가되었습니다. ■ 표 4에 HP-UX 및 Microsoft Windows 플랫폼 지원 정보를 추가했습니다. ■ 92 페이지 “설명서 문제”에 다음 문제가 추가되었습니다. ■ 97 페이지 “릴리스 노트에 알려진 문제에 대한 해결 방법이 잘못 설명되어 있습니다(6422907).” ■ 97 페이지 “`AMConfig.properties`에서 `com.iplanet.am.session.protectedPropertiesList` 문제 문서화(6351192)”
2006년 2월 9일	개정된 99 페이지 “설명서 업데이트”에는 최초 릴리스 이후 발행한 Access Manager 7 2005Q4 설명서의 새로운 내용 및 수정된 내용이 나열되어 있습니다.
2006년 2월 7일	이 수정본의 변경 내용은 다음과 같습니다. ■ 70 페이지 “알려진 문제점 및 제한 사항”에 다음과 같은 문제점이 추가되었습니다. ■ 74 페이지 “Access Manager와 Directory Server가 각각 다른 시스템에 설치된 경우 인증 서비스가 초기화되지 않습니다(6229897). ” ■ 75 페이지 “Access Manager `ampre70upgrade` 스크립트가 현지화 패키지를 제거하지 않습니다(6378444).” ■ 99 페이지 “설명서 업데이트” 절이 업데이트되었습니다.

표 1 개정 내역 (계속)

날짜	변경 내용
2006년 1월 18일	이 수정본의 변경 내용은 다음과 같습니다. ■ 59 페이지 “Access Manager 7 2005Q4 패치 1” 절이 새로 추가되었습니다. ■ 63 페이지 “분산 인증”에 대한 설명이 보완되었습니다. ■ 65 페이지 “하드웨어 및 소프트웨어 요구 사항”에서 Solaris 10 영역에 대한 설명이 보완되었고 AMD64 플랫폼에서 Solaris 10 OS에 대한 지원이 추가되었습니다. ■ 70 페이지 “알려진 문제점 및 제한 사항”에 다음과 같은 문제점이 추가되었습니다. ■ 79 페이지 “RSA 키를 사용하는 경우 IBM WebSphere에서 URL 서명에 실패합니다(6271087).” ■ 88 페이지 “Application Server에서 Access Manager를 실행하는 경우 JVM 문제가 발생합니다(6223676).” ■ 89 페이지 “웹 서비스 샘플을 실행하면 “자원 오퍼링을 찾을 수 없습니다”라는 메시지가 나타납니다(6359900).” ■ 72 페이지 “패치 1 적용 후 `/tmp/amsilent` 파일이 모든 사용자의 읽기 액세스를 허용합니다(6370691).” ■ 76 페이지 “데이터 마이그레이션 후 `ContainerDefaultTemplateRole` 속성이 추가됩니다(4677779).” ■ 97 페이지 “LDAPv3 플러그인의 역할 및 필터링된 역할 지원 문제 문서화(6365196)” ■ 97 페이지 “`AMConfig.properties` 파일에서 사용되지 않은 속성 문제 문서화(6344530)” ■ 98 페이지 “XML 암호화를 사용할 수 있게 설정하는 방법 문서화(6275563)” ■ 99 페이지 “설명서 업데이트” 절이 새로 추가되었습니다.
2005년 11월 8일	지원되는 LDAP 3(LDAPv3) 호환 저장소에 대해 61 페이지 “Identity 저장소”가 수정되었습니다.
2005년 10월	초기 릴리스
2005년 6월 30일	베타 릴리스

Sun Java System Access Manager 7 2005Q4 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 프로그램에 액세스하기 위한 단일 사인온(SSO) 지원
- 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

Access Manager 7 2005Q4 패치 릴리스

Access Manager 7 2005Q4 패치 최신 개정판은SunSolve Online(`http://sunsolve.sun.com`)에서 다운로드하여 설치합니다. 최신 패치 아이디는 다음과 같습니다.

- SPARC® 기반 시스템에 설치된 Solaris™ 운영 체제(Solaris OS): **120954-07**
- x86 플랫폼에 설치된 Solaris OS: **120955-07**
- Linux 시스템: **120956-07**
- Microsoft Windows 시스템: **124296-07**
- HP-UX 시스템: **126371-07**

주 – Access Manager 7 2005Q4 패치는 누적식입니다. 먼저 패치 1, 2, 3, 4, 5 또는 6을 설치하지 않고 패치 7을 설치할 수 있습니다. 그러나 이전 패치를 설치하지 않은 경우 이전 패치 절의 새로운 기능 및 문제를 검토하여 현재 배포에 적용할 기능 및 문제가 있는지 확인하십시오.

Access Manager 7 2005Q4 패치에 대한 정보는 다음과 같습니다.

- 10 페이지 “Access Manager 7 2005Q4 패치 7”
- 11 페이지 “사전 설치 고려 사항”
- 14 페이지 “패치 설치 지침”
- 19 페이지 “사후 설치 고려 사항”
- 22 페이지 “Access Manager 7 2005Q4 패치 6”
- 27 페이지 “Access Manager 7 2005Q4 패치 5”
- 42 페이지 “Access Manager 7 2005Q4 패치 4”
- 44 페이지 “Access Manager 7 2005Q4 패치 3”
- 54 페이지 “Access Manager 7 2005Q4 패치 2”

- 59 페이지 “Access Manager 7 2005Q4 패치 1”

Access Manager 7 2005Q4 패치 7

Access Manager 7 패치 7(개정 번호 07)에서는 패치에 포함된 README 파일에 나열된 여러 문제를 해결합니다.

패치 7에는 다음과 같은 변경 사항이 포함되어 있습니다.

- 10 페이지 “CR# 6637806: 재시작한 후 Access Manager가 잘못된 응용 프로그램 SSO 토큰을 에이전트에 보냈지만 이제 올바른 토큰을 보냅니다.”
- 10 페이지 “CR# 6612609: 네트워크 케이블이 Message Queue 서버에 연결되어 있지 않은 경우 세션 페일오버가 작동됩니다. ”
- 11 페이지 “CR# 6570409: 로드 밸러서 뒤에서 상호 작용 서비스가 Identity Provider로 올바르게 작동됩니다. ”
- 11 페이지 “CR# 6545176: 게시 인증 처리 SPI 플러그인에서 리디렉션 URL을 동적으로 설정할 수 있습니다.”

CR# 6637806: 재시작한 후 Access Manager가 잘못된 응용 프로그램 SSO 토큰을 에이전트에 보냈지만 이제 올바른 토큰을 보냅니다.

이제 Access Manager 서버를 재시작한 후 Access Manager 클라이언트 SDK가 에이전트로 올바른 예외를 보내므로 해당 에이전트가 재인증을 통해 새로운 응용 프로그램 세션을 얻을 수 있습니다. 이전에는 Access Manager 7 2005Q4 패치 5를 적용한 후 Access Manager 서버를 재시작하면 Access Manager 클라이언트 SDK가 잘못된 응용 프로그램 SSO 토큰을 해당 에이전트로 보냈습니다.

이 문제는 CR 6496155를 복제하여 수정되었습니다. 또한 패치 7에서도 제한적 컨텍스트로 응용 프로그램 SSO 토큰을 보내는 옵션(`comp.iplanet.dpro.session.dnRestrictionOnly` 등록 정보)을 제공합니다. 기본적으로 에이전트는 해당 에이전트가 설치되어 있는 서버의 IP 주소를 보내지만 엄격한 DN 검사가 필요한 경우 `AMConfig.properties` 파일에서 이 등록 정보를 다음과 같이 설정하십시오.

```
com.iplanet.dpro.session.dnRestrictionOnly=true
```

CR# 6612609: 네트워크 케이블이 Message Queue 서버에 연결되어 있지 않은 경우 세션 페일오버가 작동됩니다.

이제 세션 페일오버 배포 환경에서 각 Access Manager 인스턴스와 Message Queue 브로커가 동일한 서버에 설치되어 있는 경우 네트워크 케이블이 서버 중 하나에 연결되어 있지 않으면 세션 페일오버가 작동됩니다. 기본적으로 Message Queue `imqAddressListBehavior` 연결 팩토리 속성이 `PRIORITY`로 설정되기 때문에 Message Queue는 브로커 주소 목록에 나타난 순서대로 주소를 사용합니다(예: `localhost:7777,server2:7777,server3:7777`). 이 속성이 `RANDOM`으로 설정되어 있는 경우에는 임의의 순서로 주소를 사용합니다.

이 속성을 RANDOM으로 설정하려면 amsessiondb 스크립트에서 다음 매개 변수를 설정하십시오.

```
-DimqAddressListBehavior=RANDOM
```

Message Queue PRIORITY 및 RANDOM 속성에 대한 자세한 내용은 **Sun Java System Message Queue 3.7 UR1 관리 설명서**의 "브로커 주소 목록"를 참조하십시오.

CR# 6570409: 로드 밸런서 뒤에서 상호 작용 서비스가 Identity Provider로 올바르게 작동됩니다.

두 대의 서버가 로드 밸런서에 연결되어 단일 Identity Provider로 작동하는 배포 환경인 경우 AMConfig.properties 파일에서 다음 등록 정보를 설정해야 합니다.

```
com.sun.identity.liberty.interaction.lbWspRedirectHandler
com.sun.identity.liberty.interaction.trustedWspRedirectHandlers
```

com.sun.identity.liberty.interaction.interactionConfigClass는 현재 지원되는 유일한 클래스입니다. 따라서 기본적으로 Federation Liberty에 번들로 제공된 상호 작용 구성 클래스를 사용하여 상호 작용 구성 매개 변수에 액세스합니다.

CR# 6545176: 게시 인증 처리 SPI 플러그인에서 리디렉션 URL을 동적으로 설정할 수 있습니다.

이제 로그인 성공, 로그인 실패 및 로그아웃을 검증하는 데 필요한 리디렉션 URL을 게시 인증 처리 SPI 플러그인에서 동적으로 설정할 수 있습니다. 게시 처리 플러그인이 실행되지 않는 경우 게시 처리 SPI에 설정된 리디렉션 URL은 사용되지 않으며 다른 방법으로 설정한 리디렉션 URL이 앞서와 같이 사용됩니다.

자세한 내용은
com.iplanet.am.samples.authentication.spi.postprocess.ISAuthPostProcessSample.java
샘플을 참조하십시오.

사전 설치 고려 사항

- 11 페이지 "파일 백업"
- 13 페이지 "Access Manager 설치 및 구성"

파일 백업

중요 현재 설치의 파일 중 사용자 정의한 파일이 있는 경우에는 패치를 설치하기 전에 이러한 파일을 백업해야 합니다. 패치를 설치한 다음 백업한 파일과 이 패치에서 설치한 파일을 비교하여 사용자 정의를 식별합니다. 사용자 정의를 새로운 파일에 병합하고 저장합니다. 사용자 정의 파일을 처리하는 데 대한 자세한 내용은 다음 정보를 읽어 보십시오.

패치를 설치하기 전에 다음 파일도 백업하십시오.

Solaris 시스템	■ *AccessManager-base*/SUNWam/bin/amsfo ■ *AccessManager-base*/SUNWam/lib/amsfo.conf ■ /etc/opt/SUNWam/config/xml/template/ 디렉토리의 파일: idRepoService.xml, amSOAPBinding.xml, amDisco.xml, amAuthCert.xml, amAuth.xml , amSession.xml ■ *AccessManager-base*/SUNWam/locale/ 디렉토리의 파일: amConsole.properties, amIdRepoService.properties, amAuthUI.properties, amAuth.properties, amPolicy.properties, amPolicyConfig.properties, amSessionDB.properties, amSOAPBinding.properties, amAdminCLI.properties, amSDK.properties, amAuthLDAP.properties, amSession.properties, amAuthContext.properties, amSAML.properties, amAuthCert.properties
Linux 및 HP-UX 시스템	■ *AccessManager-base*/identity/bin/amsfo ■ *AccessManager-base*/identity/lib/amsfo.conf ■ /etc/opt/sun/identity/config/xml/template/ 디렉토리의 파일: idRepoService.xml, amSOAPBinding.xml, amDisco.xml, amAuthCert.xml , amAuth.xml, amSession.xml ■ *AccessManager-base*/identity/locale/ 디렉토리의 파일: amConsole.properties, amIdRepoService.properties, amAuthUI.properties, amAuth.properties, amPolicy.properties, amPolicyConfig.properties, amSessionDB.properties, amSOAPBinding.properties, amAdminCLI.properties, amSDK.properties, amAuthLDAP.properties, amSession.properties, amAuthContext.properties, amSAML.properties, amAuthCert.properties

Windows 시스템	■ *AccessManager-base*\identity\setup\AMConfigurator.properties ■ *AccessManager-base*\identity\bin\amsfo ■ *AccessManager-base*\identity\lib\amsfo.conf ■ *AccessManager-base*\identity\config\xml\template 디렉토리의 파일: idRepoService.xml, amSOAPBinding.xml, amDisco.xml, amAuthCert.xml , amAuth.xml, amSession.xml ■ *AccessManager-base*\identity\locale 디렉토리의 파일: amConsole.properties, amIdRepoService.properties, amAuthUI.properties, amAuth.properties, amPolicy.properties, amPolicyConfig.properties, amSessionDB.properties, amSOAPBinding.properties, amAdminCLI.properties, amSDK.properties, amAuthLDAP.properties, amSession.properties, amAuthContext.properties, amSAML.properties, amAuthCert.properties

여기서 *AccessManager-base*는 기본 설치 디렉토리입니다. 플랫폼별 기본 설치 디렉토리는 다음과 같습니다.

- Solaris 시스템: /opt
- Linux 및 HP-UX 시스템: /opt/sun
- Windows 시스템: *javaes-install-directory*\AccessManager . 예를 들면 다음과 같습니다. C:\Program Files\Sun\AccessManager

Access Manager 설치 및 구성

이 문서에서 설명한 Access Manager 패치가 Access Manager를 설치하는 것은 아닙니다. 패치를 설치하기 전에 Access Manager 7 2005Q4를 서버에 설치해야 합니다. 설치하는 방법은 **Sun Java Enterprise System 2005Q4 설치 설명서**를 참조하십시오.

Windows 시스템에 패치를 설치하는 경우 **Sun Java Enterprise System 2005Q4 Installation Guide for Microsoft Windows**를 참조하십시오.

Access Manager를 배포, 다시 배포 및 구성하려면 **Sun Java System Access Manager 7 2005Q4 관리 설명서**의 1 장, "Access Manager 7 2005Q4 구성 스크립트"에 설명된 대로 amconfig 스크립트 실행에 익숙해야 합니다.

이 패치에 의해 사용하지 않게 된 Access Manager 패치 목록과 이 패치를 설치하기 전에 설치해야 하는 패치에 대해서는 이 패치에 포함된 README 파일을 참조하십시오.

주의 – Access Manager 패치는 다른 패치와 마찬가지로 작업 환경에 적용하기 전에 준비 또는 배포 전 시스템에서 테스트해야 합니다. 또한 패치 설치 프로그램이 사용자 정의 JSP 파일을 올바르게 업데이트하지 못할 수 있으므로 Access Manager가 올바르게 동작하려면 이러한 파일을 직접 변경해야 할 수 있습니다.

패치 설치 지침

Solaris 시스템용 패치 설치 지침

Solaris 패치를 설치하기 전에 11 페이지 “사전 설치 고려 사항”에 나열된 파일들을 백업했는지 확인하십시오.

Solaris 시스템에서 패치를 추가하거나 제거하려면 OS에서 제공하는 `patchadd` 및 `patchrm` 명령을 사용하십시오.

patchadd 명령

독립형 시스템에 패치를 설치하려면 `patchadd` 명령을 사용합니다. 예를 들면 다음과 같습니다.

```
# patchadd /var/spool/patch/120954-07
```

주 – Solaris 10 전역 영역에 Solaris 패치를 설치하는 경우 `-G` 인수를 사용하는 `patchadd` 명령을 호출하십시오. 예를 들면 다음과 같습니다.

```
patchadd -G /var/spool/patch/120954-07
```

`postpatch` 스크립트는 Access Manager SDK 구성 요소만 설치된 시스템의 경우를 제외하고 Access Manager 응용 프로그램을 다시 배포하는 데 대한 메시지를 표시합니다.

`postpatch` 스크립트는 다음 디렉토리에 `amsilent` 파일을 만듭니다.

- Solaris 시스템: *AccessManager-base*`/SUNWam`
- Linux 시스템: *AccessManager-base*`/identity`

여기서 *AccessManager-base*는 기본 설치 디렉토리입니다. 기본 설치 디렉토리는 Solaris 시스템의 경우 `/opt`이며 Linux 시스템의 경우 `/opt/sun`입니다.

amsilent는 amsamplesilent 파일에 기반하지만 시스템의 Access Manager 구성 파일에 따라 일부 매개 변수 집합이 필요할 수 있습니다. 비밀번호 매개 변수에는 기본값이 포함됩니다. 각 비밀번호 매개 변수의 주석을 해제하고 값을 수정한 다음, 파일 내의 배포에 필요한 다른 매개 변수의 값을 주의 깊게 확인합니다.

공통 도메인 웹 응용 프로그램의 URI 접두어인 COMMON_DEPLOY_URI 매개 변수에도 기본값이 포함됩니다. 이 URI에 대해 기본 이외의 값을 지정한 경우에는 이 값을 반드시 수정해야 합니다. 그렇지 않으면 amconfig 및 패치로 생성된 amsilent 파일을 통해 웹 응용 프로그램을 다시 배포할 수 없게 됩니다.

그리고 다음 명령을 실행합니다(기본 디렉토리에 설치된 Access Manager와 함께 표시).

```
# cd /opt/SUNWam/bin
# ./amconfig -s /opt/SUNWam/amsilent
```

주의 – amsilent 파일에는 관리자 비밀번호와 같은 민감한 데이터가 일반 텍스트로 포함되므로 배포에 적합하도록 파일을 보호해야 합니다.

amconfig 스크립트를 실행한 후에 updateschema.sh 스크립트를 실행하여 XML 파일과 LDIF 파일을 로드합니다. updateschema.sh 스크립트는 다음 디렉토리에 패치 7을 설치한 후에 사용할 수 있습니다.

- Solaris SPARC 시스템: *patch-home-directory* /120954-07
- Solaris x86 시스템: *patch-home-directory*/120955-07

updateschem 스크립트를 실행한 후 Access Manager 프로세스를 다시 시작합니다. 예를 들면 다음과 같습니다.

```
# cd /opt/SUNWam/bin
# ./amserver stop
# ./amserver start
```

그런 다음 Access Manager 웹 컨테이너를 다시 시작합니다.

patchrm Command

독립형 시스템에서 패치를 제거하려면 patchrm 명령을 사용합니다. 예를 들면 다음과 같습니다.

```
# patchrm 120954-03
```

backout 스크립트는 Access Manager SDK 구성 요소만 설치된 시스템의 경우를 제외하고 patchadd 명령과 비슷한 메시지를 표시합니다.

패치가 제거되었으면 *AccessManager-base*/SUNWam 디렉토리에 있는 amsilent 파일을 사용하여 Access Manager 응용 프로그램을 다시 배포합니다. 여기서 *AccessManager-base*는 기본 설치 디렉토리입니다. Solaris 시스템에서 기본 설치 디렉토리는 /opt입니다.

배포에 적합하도록 amsilent 파일의 매개 변수를 설정합니다.

그런 다음 Solaris 시스템의 기본 디렉토리에 설치된 Access Manager와 함께 표시되는 다음 명령을 실행합니다.

```
# cd /opt/SUNWam/bin
# ./amconfig -s /opt/SUNWam/amsilent
```

patchadd 및 patchrm 명령에 대한 자세한 내용은 해당 Solaris man 페이지를 참조하십시오.

자세한 내용은 19 페이지 “사후 설치 고려 사항”을 참조하십시오.

Solaris 10 영역

Solaris 10 운영 체제에서는 "영역"이라는 새로운 개념을 소개했습니다.이에 따라 patchadd 명령에도 전역 영역에만 패치를 추가하는 -G 옵션이 추가되었습니다. 기본적으로 patchadd 명령은 패치될 패키지의 pkginfo에서 SUNW_PKG_ALLZONES를 찾습니다. 그러나 모든 Access Manager 패키지에 대해 SUNW_PKG_ALLZONES 변수가 설정되는 것은 아니며 Access Manager 7 2005Q4가 전역 영역에 설치된 경우에는 -G 옵션이 필요합니다. Access Manager가 로컬 영역에 설치된 경우 patchadd -G 옵션은 효과가 없습니다.

Access Manager 7 2005Q4 패치를 Solaris 시스템 시스템에 설치하는 경우에는 -G 옵션을 사용하는 것이 좋습니다. 예를 들면 다음과 같습니다.

```
# patchadd -G AM7_patch_dir
```

비슷하게 Access Manager가 전역 영역에 설치된 경우에는 patchrm 명령을 실행하는 데 -G 옵션이 필요합니다. 예를 들면 다음과 같습니다.

```
# patchrm -G 120954-07
```

Linux 시스템용 패치 설치 지침

Linux 패치를 설치하기 전에 11 페이지 “사전 설치 고려 사항”에 나열된 파일들을 백업했는지 확인하십시오.

installpatch는 단독형 Linux 시스템에 패치를 설치합니다. 예를 들면 다음과 같습니다.

```
# ./installpatch
```

postpatch 스크립트는 Solaris 시스템과 비슷한 메시지를 출력합니다. 그러나 Linux 시스템에서 패치를 취소하기 위한 절차는 Solaris 시스템과는 다릅니다. Linux 패치를 취소하는 공통적인 스크립트는 없습니다. 이전에 낮은 패치 버전을 설치한 경우 해당 버전을 다시 설치하고 postpatch 지침에 따라 amconfig 스크립트를 실행하여 Access Manager 응용 프로그램을 다시 배포할 수 있습니다.

amconfig 스크립트를 실행한 후에 updateschema.sh 스크립트(패치 5 이상)를 실행하여 XML 파일과 LDIF 파일을 로드합니다. updateschema.sh 스크립트는 *patch-home-directory*/120956-07/scripts 디렉토리에 패치 7을 설치한 후에 사용할 수 있습니다.

amconfig 및 updateschema.sh 스크립트를 실행한 후 Access Manager 웹 컨테이너를 다시 시작합니다.

Access Manager 7 2005Q4 RTM 릴리스에 패치가 설치되어 있고 패치를 제거하여 시스템을 RTM 상태로 복원하려는 경우 reinstallRTM 스크립트를 사용하여 Access Manager 7 2005Q4 RTM 패키지를 다시 설치해야 합니다. 이 스크립트는 Access Manager RTM RPM이 저장된 경로를 이용하여 패치한 RPM에 RTM RPM을 설치합니다. 예를 들면 다음과 같습니다.

```
# ./scripts/reinstallRTM path_of_AM7_RTM_RPM_directory
```

reinstallRTM 스크립트를 실행한 후 amconfig 스크립트를 실행하여 Access Manager 응용 프로그램을 다시 배포하고 웹 컨테이너를 다시 시작합니다.

자세한 내용은 19 페이지 “사후 설치 고려 사항”을 참조하십시오.

Windows 시스템용 패치 설치 지침

Windows 패치 설치에 관련되는 요구 사항은 다음과 같습니다.

- Access Manager 7 2005Q4가 Windows 시스템에 설치되어 있어야 합니다. 설치하는 방법은 **Sun Java Enterprise System 2005Q4 Installation Guide for Microsoft Windows**를 참조하십시오.
- 패치 스크립트를 실행하려면 Windows 시스템에 ActivePerl 5.8 이상이 필요합니다.

Windows 패치 설치

Windows 패치를 설치하기 전에 11 페이지 “사전 설치 고려 사항”에 나열된 파일들을 백업했는지 확인하십시오.

패치 스크립트에서 입력하는 기본 디렉토리 경로에는 슬래시(/)를 사용합니다. 예를 들면 다음과 같습니다. c:/sun

Windows 패치를 설치하려면

1. 관리자 그룹의 구성원으로 Windows 시스템에 로그온합니다.

2. Windows 패치 파일을 다운로드하고 압축을 풀 디렉토리를 만듭니다. 예: `AM7p7`
3. 이전 단계에서 만든 디렉토리에 `124296-07.zip` 파일을 다운로드하고 압축을 풉니다.
4. 모든 Java ES 2005Q4 서비스를 중지합니다.
5. `AM7p7\scripts\prepatch.pl` 스크립트를 실행합니다.
6. `AM7p7\124296-07.exe`를 실행하여 패치를 설치합니다.
7. `AM7p7\scripts\postpatch.pl` 스크립트를 실행합니다.
8. Java ES 2005Q4 서비스를 다시 시작합니다.
9. Access Manager 응용 프로그램을 다시 배포합니다. 자세한 내용은 19 페이지 "사후 설치 고려 사항"을 참조하십시오.
10. `AM7p7\scripts\updateschema.pl` 스크립트를 실행하여 Directory Server 서비스 스키마를 업데이트합니다. 스크립트에서 입력 항목을 검증한 다음 해당 파일을 로드합니다. 또한 스크립트에서 다음과 같은 로그 파일에 기록합니다.

    javaes-install-directory`\AccessManager\AM70Patch-upgrade-schema-` *timestamp*
11. Java ES 2005Q4 서비스를 다시 시작합니다.

Windows 패치 취소

Windows 패치를 취소하려면 다음을 수행합니다.

1. 관리자 그룹의 구성원으로 Windows 시스템에 로그온합니다.
2. `Uninstall_124296-07.bat` 파일을 실행합니다.
3. `AM7p7\scripts\postbackout.pl` 스크립트를 실행합니다.
4. Access Manager 응용 프로그램을 다시 배포합니다.
5. Java ES 2005Q4 서비스를 다시 시작합니다.

주: 패치를 취소하더라도 `AM7p7\scripts\updateschema.pl` 스크립트로 추가된 스키마 변경 항목은 Directory Server에서 제거되지 않습니다. 그러나 패치가 취소된 후에는 Access Manager 기능이나 유용성에 영향을 미치지 않으므로 이러한 스키마 변경 항목을 수동으로 제거하지 않아도 됩니다.

HP-UX 시스템용 패치 설치 지침

HP-UX 패치를 설치하거나 제거하려면 `swinstall` 및 `swremove` 명령을 사용합니다. 예를 들어 독립형 시스템에 패치를 설치하려면 다음을 수행합니다.

```
# swinstall /var/spool/patch/126371-07
```

또는 독립형 시스템에서 패치를 제거하려면 다음을 수행합니다.

```
# swremove 126371-07
```

`swinstall` 및 `swremove` 명령에 대해서는 `swinstall` 및 `swremove` 매뉴얼 페이지를 참조하십시오.

패치를 설치하거나 제거한 후에는 19 페이지 “사후 설치 고려 사항” 절에 설명된 대로 Access Manager 응용 프로그램을 다시 배포해야 합니다.

Access Manager 응용 프로그램을 다시 배포한 후 `updateschema.sh` 스크립트(패치 5 이상)를 실행하여 XML 및 LDIF 파일을 로드합니다. `updateschema.sh` 스크립트는 *patch-home-directory*`/120956-07/scripts` 디렉토리에 패치 7을 설치한 후에 사용할 수 있습니다. `amconfig` 및 `updateschema.sh` 스크립트를 실행한 후 Access Manager 웹 컨테이너를 다시 시작합니다.

주: 패치를 제거해도 `updateschema.sh` 스크립트로 추가된 스키마 변경 항목은 Directory Server에서 제거되지 않습니다. 그러나 패치를 제거한 후 Access Manager 기능이나 유용성에 영향을 미치지 않으므로 이러한 스키마 변경 항목을 수동으로 제거하지 않아도 됩니다.

HP-UX 시스템에 Access Manager를 배포하는 방법은 **Sun Java System Access Manager 7 2005Q4 Release Notes for HP-UX**를 참조하십시오.

사후 설치 고려 사항

Access Manager 7 2005Q4 패치를 설치한 후 고려할 사항에는 다음이 포함됩니다.

CR# 6254355: Access Manager 패치가 postpatch 스크립트의 Access Manager 응용 프로그램을 배포하지 않습니다.

패치 설치 프로그램이 사용자 정의된 WAR 파일 일부를 유지하지 않고 사용자 정의되지 않은 버전으로 대체합니다. 사용자 정의된 WAR 파일의 내용을 식별하고 직접 업데이트하려면 다음과 같은 절차 사용을 고려해 보십시오.

다음 예에서 *AccessManager-base*는 기본 설치 디렉토리입니다. 기본 설치 디렉토리는 Solaris 시스템의 경우 `/opt`이며 Linux 시스템의 경우 `/opt/sun`입니다.

Windows 시스템의 경우 *AccessManager-base*는 *javaes-install-directory*`\AccessManager`입니다. 예: `C:\Program Files\Sun\AccessManager`

패치되는 WAR 파일은 다음과 같습니다.

- `console.war`
- `password.war`
- `services.war`

이 파일들은 Solaris 시스템의 경우 *AccessManager-base*`/SUNWam`에 있으며, Linux 시스템의 경우 *AccessManager-base*`/identity`에 있습니다.

Windows 시스템의 경우 패치된 WAR 파일은 *AccessManager-base*\에 있습니다.

WAR 파일에서 변경할 수 있는 내용은 다음과 같습니다.

- 등록 정보 파일
  - Solaris 시스템: *AccessManager-base*/SUNWam/locale/*.properties
  - Linux 시스템: *AccessManager-base*/identity/locale/*.properties
  - Windows 시스템: *AccessManager-base*\locale*.properties
- 태그 라이브러리 설명자
  - Solaris 시스템: *AccessManager-base*/SUNWam/web-src/applications/WEB-INF/*.tld
  - Linux 시스템: *AccessManager-base*/identity/web-src/applications/WEB-INF/*.tld
  - Windows 시스템: *AccessManager-base*\web-src\applications\WEB-INF*.tld
- web.xml 파일 및 이 파일을 구성하는 데 사용되는 파일(WEB-INF/web.xml 및 WEB-INF/*.xml)
- 응용 프로그램별 파일: JSP(*.jsp) 파일, 이미지(*.gif) 파일, 스타일 시트 - 배경색, 글꼴 크기 등(*.css) 파일

이러한 모든 변경 사항을 유지하려면 다음 단계를 따르십시오. 파일을 변경하기 전에 항상 먼저 파일을 백업하십시오.

1. 패치를 설치합니다.
2. 임시 디렉토리에 WAR 파일 압축을 해제합니다. 예를 들어 Solaris 시스템의 기본 디렉토리에 설치된 Access Manager를 사용하는 경우 다음과 같습니다.

   ```
   # cd temporary-directory
   # jar -xvf /opt/SUNWam/console.war
   # jar -xvf /opt/SUNWam/services.war
   # jar -xvf /opt/SUNWam/password.war
   ```

3. 패치 설치 프로그램이 사용자 정의된 파일을 변경하는지 압축 해제된 파일을 확인하고 임시 디렉토리의 변경된 파일에 원래 사용자 정의 변경을 직접 추가합니다. *AccessManager-base*/web-src/ 디렉토리의 파일에 대한 변경 사항 중 패치된 WAR 파일에 포함되지 않는 항목에 대해서는 변경 사항을 다시 적용할 필요가 없습니다.
4. 수정된 파일로 WAR 파일을 업데이트합니다. 예를 들어 Solaris 시스템의 기본 디렉토리에 설치된 Access Manager를 사용하는 경우 다음과 같습니다.

   ```
   # cd temporary-directory
   # jar -uvf /opt/SUNWam/console.war $path/$modified file
   # jar -uvf /opt/SUNWam/services.war $path/$modified file
   # jar -uvf /opt/SUNWam/password.war $path/$modified file
   ```

   2~4단계를 예로 들면 다음과 같습니다.

```
# mkdir /tmp/war.tmp
# cd /tmp/war.tmp
# jar -xvf /opt/SUNWam/services.war
# vi index.html
# jar -uvf /opt/SUNWam/services.war index.html
```

5. 패치에서 생성된 자동 구성 파일(amsilent)을 다시 사용하거나 amsamplesilent 템플리트 파일에 기반한 구성 파일을 새로 만들고 다음을 포함하여 해당 구성 변수를 설정합니다.

   - DEPLOY_LEVEL=21
   - DIRECTORY_MODE=5
   - DS_DIRMGRPASSWD, ADMINPASSWD 및 AMLDAPUSERPASSWD를 위한 비밀번호
   - Access Manager 웹 컨테이너 변수

   Windows 시스템의 경우 postpatch.pl 스크립트에서 생성된 자동 구성 파일(amsilent)을 다시 사용하고 *AccessManager-base*\setup\AMConfigurator.properties-tmp 값이 유효한지 확인합니다. 그런 다음 이 파일의 이름을 *AccessManager-base*\setup\AMConfigurator.properties로 변경합니다.

   웹 컨테이너 변수에 대한 자세한 내용은 Solaris 시스템에서는 /opt/SUNWam/bin 디렉토리, Linux 시스템에서는 /opt/sun/identity/bin 디렉토리에 있는 amsamplesilent 파일을 참조하십시오.

   Windows 시스템의 경우 구성 파일은 *AccessManager-base*\setup\AMConfigurator.properties입니다.

6. 아래에 표시된 amconfig 스크립트를 실행합니다. amconfig를 실행하기 전에 Directory Server 및 Access Manager 웹 컨테이너가 실행 중이어야 합니다. 예를 들어 Access Manager가 기본 설치 디렉토리에 설치된 Solaris 시스템에서 amconfig를 실행하려면 다음과 같이 수행합니다.

   ```
   # cd /opt/SUNWam/bin
   # ./amconfig -s /opt/SUNWam/amsilent
   ```

7. amconfig 스크립트를 실행한 다음 Access Manager 프로세스를 다시 시작합니다. 예를 들면 다음과 같습니다.

   ```
   # cd /opt/SUNWam/bin
   # ./amserver stop
   # ./amserver start
   ```

8. Solaris 시스템의 경우 *AccessManager-base*/SUNWam/web-src/ 디렉토리의 해당 하위 디렉토리 또는 Linux 시스템의 경우 *AccessManager-base*/identity/web-src/ 디렉토리에 사용자 정의한 JSP 파일이 모두 있는지와 이러한 파일을 모두 백업했는지를 확인합니다.

   Windows 시스템의 경우 이러한 파일은 *AccessManager-base*\web-src\에 있습니다.

9. Access Manager 웹 컨테이너를 다시 시작합니다.

amconfig 스크립트를 실행하는 데 대한 자세한 내용은**Sun Java System Access Manager 7 2005Q4 관리 설명서**의 1 장, “Access Manager 7 2005Q4 구성 스크립트”를 참조하십시오.

CR# 6436409: 분산 인증 및 클라이언트 SDK WAR 파일 다시 배포

분산 인증 또는 클라이언트 SDK를 사용하고 있다면 패치를 설치한 뒤에 분산 인증 WAR 파일 및/또는 클라이언트 SDK WAR 파일을 다시 만들고 다시 배포하십시오. 자세한 내용은 다음 문서를 참조하십시오.

- 분산 인증 WAR 파일 만들기: **Technical Note: Using Access Manager Distributed Authentication**
- 클라이언트 SDK WAR 파일 만들기: **Sun Java System Access Manager 7 2005Q4 Developer's Guide**의 “Installing the Client SDK”
- 클라이언트 SDK WAR 파일 배포: **Sun Java System Access Manager 7 2005Q4 Developer's Guide**의 “To Deploy amclientwebapps.war”

Access Manager 7 2005Q4 패치 6

Access Manager 7 패치 6(개정 06)에서는 패치에 포함된 README 파일에 나와 있는 여러 문제를 수정했습니다. 패치 6에는 다음과 같은 새로운 기능, 문제점 및 설명서 업데이트가 들어 있습니다.

패치 6의 새로운 기능

- 23 페이지 “Access Manager에서 JDK 1.5 HttpURLConnection setReadTimeout 메소드 지원”
- 23 페이지 “Access Manager SDK에서 기본 Directory Server를 백업한 후 기본 Directory Server로 폴백”
- 24 페이지 “다중 Access Manager 인스턴스에서 별도의 로그 파일에 로그”
- 25 페이지 “Access Manager 7에서 다중 쿠키 도메인 허용”
- 25 페이지 “Microsoft IIS 6.0 사후 인증 플러그인에서 SharePoint Server 지원”
- 25 페이지 “Access Manager에서 Internet Explorer 7 지원”

패치 6의 알려진 문제점 및 제한 사항

- 25 페이지 “CR# 6379325: 세션 페일오버 중 콘솔에 액세스하면 null 포인터 예외가 발생합니다.”
- 26 페이지 “CR# 6508103: Windows에서 관리 콘솔의 도움말을 누르면 응용 프로그램 오류를 반환합니다.”
- 26 페이지 “CR# 6564877: Access Manager 7 패치 설치 시 SAML v2 파일을 덮어씁니다.”

주 – 패치 6을 설치하기 전에 다음 구성 요소를 업그레이드하거나 패치하는 것이 좋습니다.

- Sun Java System Web Server 6.1 SP5나 이전 버전을 사용하고 있는 경우 아래 사이트에서 다운로드할 수 있는 Web Server 6.1 SP7로 업그레이드합니다.

  `http://www.sun.com/download/products.xml?id=45c90ca9`

  Sun Java System Web Server 6.1 SP7 릴리스 노트의 "업그레이드"에 설명된 대로 업그레이드 절차를 따릅니다.
- NSS, JSS 및 NSPR용 최신 보안 패치를 `http://sunsolve.sun.com`.
  - Solaris 8 SPARC 플랫폼: 119209
  - Solaris 8 x86 플랫폼: 119210
  - Solaris 9 SPARC 플랫폼: 119211
  - Solaris 9 x86 플랫폼: 119212
  - Solaris 10 SPARC 플랫폼: 119213
  - Solaris 10 x86 및 AMD64 플랫폼: 119214
  - Windows 시스템: 124392
  - HP-UX 시스템: 124379

Access Manager에서 JDK 1.5 `HttpURLConnection setReadTimeout` 메소드 지원

`setReadTimeout` 메소드를 지원하려면 `AMConfig.properties` 파일의 다음 새 등록 정보에서 읽기 시간 초과 값을 설정합니다.

```
com.sun.identity.url.readTimeout
```

웹 컨테이너에서 JDK 1.5를 사용하는 경우 `HttpURLConnections`이 너무 많이 열려 있으면 서버가 중단될 수 있으므로 이를 방지하려면 연결이 시간 초과되도록 이 등록 정보를 적절한 값으로 설정합니다. 기본값은 30000밀리초(30초)입니다.

`setReadTimeout` 메소드는 `com.sun.identity.url.readTimeout` 이 `AMConfig.properties` 파일에 없거나 빈 문자열로 설정된 경우 무시됩니다.

Access Manager SDK에서 기본 Directory Server를 백업한 후 기본 Directory Server로 폴백

Sun Java System Directory Server가 MMR(Multi-Master Replication)로 구성된 경우 Access Manager SDK는 기본 Directory Server를 중단하고 백업한 후 기본 Directory Server로 폴백합니다. 이전에는 Access Manager SDK가 기본 Directory Server를 백업한 후에도 보조 Directory Server로 계속 액세스했습니다.

Access Manager에서 이 새 동작을 지원하기 위해 `AMConfig.properties` 파일에 다음과 같은 새 등록 정보가 추가되었습니다.

```
com.sun.am.ldap.fallback.sleep.minutes
```

이 등록 정보에서는 기본 Directory Server를 백업한 후 기본 서버로 폴백하기 전에 보조 Directory Server 인스턴스가 일시 정지하는 시간(분)을 설정합니다. 기본값은 15분입니다.

`com.sun.am.ldap.fallback.sleep.minutes` 등록 정보는 숨겨져 있습니다. 이 등록 정보를 기본값(15분) 이외의 값으로 설정하려면 `AMConfig.properties` 파일에 이 등록 정보를 명시적으로 추가합니다. 예를 들어 값을 7분으로 설정하려는 경우 다음을 추가합니다.

```
com.sun.am.ldap.fallback.sleep.minutes=7
```

새 값을 적용하려면 Access Manager 웹 컨테이너를 다시 시작합니다.

다중 Access Manager 인스턴스에서 별도의 로그 파일에 로그

`AMConfig.properties` 파일에서 다음의 새 등록 정보를 설정하면 같은 호스트 서버에서 실행되는 다중 Access Manager 인스턴스에서 서로 다른 로깅 하위 디렉토리에 있는 별도의 로그 파일에 로그할 수 있습니다.

```
com.sun.identity.log.logSubdir
```

관리 콘솔에서 기본 로깅 디렉토리를 변경하지 않은 경우 기본 로깅 디렉토리는 다음과 같습니다.

- Solaris 시스템: `/var/opt/SUNWam/logs`
- Linux 및 HP-UX 시스템: `/var/opt/sun/identity/logs`
- Windows 시스템: `C:\Sun\JavaES5\identity\logs`

첫 번째 Access Manager 인스턴스는 항상 기본 로깅 디렉토리에 로그합니다. 추가 Access Manager 인스턴스에 대해 다른 로깅 하위 디렉토리를 지정하려면 추가 Access Manager 인스턴스마다 `AMConfig.properties` 파일에 `com.sun.identity.log.logSubdir` 등록 정보를 설정합니다.

예를 들어 `am-instance-1`, `am-instance-2` 및 `am-instance-3`과 같은 3개 인스턴스를 모두 같은 Solaris 호스트 서버에서 실행하는 경우 다음과 같이 등록 정보를 설정합니다.

```
com.sun.identity.log.logSubdir=am-instance-2
com.sun.identity.log.logSubdir=am-instance-3
```

`com.sun.identity.log.logSubdir` 등록 정보는 숨겨져 있습니다. 필요한 경우 이 등록 정보를 `AMConfig.properties` 파일에 명시적으로 추가하고 Access Manager 웹 컨테이너를 다시 시작하여 하위 디렉토리 값을 적용합니다.

그러면 Access Manager 인스턴스가 다음 디렉토리에 로그합니다.

```
/var/opt/SUNWam/logs/log-files-for-am-instance-1
/var/opt/SUNWam/logs/am-instance-2/log-files-for-am-instance-2
/var/opt/SUNWam/logs/am-instance-3/log-files-for-am-instance-3
```

Access Manager 7에서 다중 쿠키 도메인 허용

Access Manager에서는 다중 쿠키 도메인을 허용하기 위해 다음 새 등록 정보를 추가했습니다.

```
com.sun.identity.authentication.setCookieToAllDomains
```

기본값은 `true`입니다. 이 새 등록 정보는 숨겨져 있습니다. `false`로 값을 설정하려면 `AMConfig.properties` 파일에 등록 정보를 명시적으로 추가한 후 Access Manager 웹 컨테이너를 다시 시작합니다.

Microsoft IIS 6.0 사후 인증 플러그인에서 SharePoint Server 지원

Microsoft 인터넷 정보 서비스(IIS) 6.0 인증 플러그인에서 Microsoft Office SharePoint Server를 지원합니다. 사용자는 사용자 ID 또는 로그인 이름을 이용하여 Access Manager에 로그인할 수 있습니다. 그러나 SharePoint Server의 경우 로그인 이름은 허용하지만 사용자 ID를 지정한 경우 문제가 발생합니다.

SharePoint Server로 로그인을 허용하려면 사후 인증 플러그인(`ReplayPasswd.java`)에서 다음의 새 등록 정보를 사용해야 합니다.

```
com.sun.am.sharepoint_login_attr_name
```

이 새 등록 정보는 SharePoint Server에서 인증 시 사용하는 사용자 속성을 나타냅니다. 예를 들어 다음 등록 정보는 인증 시 공통 이름(`cn`)을 지정합니다.

```
com.sun.am.sharepoint_login_attr_name=cn
```

사후 인증 플러그인은 `com.sun.am.sharepoint_login_attr_name` 등록 정보를 읽고 Directory Server에서 사용자에 해당하는 속성 값을 가져옵니다. 그런 다음 사용자가 SharePoint Server에 액세스할 수 있도록 인증 헤더를 설정합니다.

이 등록 정보는 숨겨져 있습니다. 등록 정보를 설정하려면 `AMConfig.properties` 파일에 명시적으로 등록 정보를 추가한 후 Access Manager 웹 컨테이너를 다시 시작하여 값을 적용합니다.

Access Manager에서 Internet Explorer 7 지원

Access Manager 7 2005Q4 패치 6에서 Microsoft Windows Internet Explorer 7을 지원합니다.

CR# 6379325: 세션 페일오버 중 콘솔에 액세스하면 null 포인터 예외가 발생합니다.

이 시나리오에서는 쿠키 기반 지속 요청 라우팅에 구성된 로드 밸런서 뒤에 다중 Access Manager 서버가 세션 페일오버 모드로 배포되었습니다. Access Manager 관리자는 로드 밸런서를 통해 Access Manager 콘솔에 액세스합니다. 관리자가 콘솔에 로그인하면 Access Manager 서버 중 하나에서 세션이 만들어집니다. 서버가 중단되면 예상대로 콘솔 세션이

다른 Access Manager 서버로 페일오버됩니다. 그러나 브라우저와 웹 컨테이너 오류 로그에 간헐적인 null 포인터 예외가 나타나는 경우가 있습니다.

이 문제는 페일오버 시 활성 Access Manager 콘솔 세션에만 영향을 주며 Access Manager 서버 작동에는 영향을 주지 않습니다.

해결 방법: 간헐적인 null 포인터 예외를 방지하려면 다음을 수행합니다.

- 임시적인 해결 방법으로 브라우저를 새로 고치거나 콘솔에서 로그아웃한 후 다시 로그인합니다.
- 영구적인 해결 방법으로 세션 페일오버에 참여하지 않는 별도의 Access Manager 인스턴스에 Access Manager 콘솔을 배포합니다.

CR# 6508103: Windows에서 관리 콘솔의 도움말을 누르면 응용 프로그램 오류를 반환합니다.

Windows 2003 Enterprise Edition에서 영어 이외의 로켈로 Sun Java System Application Server에 Access Manager를 배포한 경우 영역 관리 모드 콘솔에서 도움말을 누르면 응용 프로그램 오류가 발생합니다.

해결 방법:

1. *javaes-install-dir*`\share\lib\jhall.jar` 파일을 `%JAVA_HOME%\jre\lib\ext` 디렉토리에 복사합니다.

   여기서 *javaes-install-dir*은 Windows 설치 디렉토리입니다.
2. Application Server 인스턴스를 다시 시작합니다.

CR# 6564877: Access Manager 7 패치 설치 시 SAML v2 파일을 덮어씁니다.

SAML v2 플러그인이 설치되면 패치 설치 시 SAML v2 관련 파일을 덮어쓰고 `postpatch` 스크립트에 다음 메시지가 나타납니다.

```
The postpatch script detected that the SAML v2 plug-in is installed in your
environment. When you run the amconfig script to redeploy the Access Manager
applications, the script will recreate the amserver.war file and the SAML v2
related files will be lost. Therefore, after you run amconfig, recreate and
redeploy the amserver.war file, as described in the Sun Java System SAML v2
Plug-in for Federation Services User's Guide.
```

해결 방법: 패치를 설치하고 `amconfig` 스크립트를 실행한 후 SAML v2 플러그인을 사용하는 Federation Manager 또는 Access Manager 배포에 대해 `amserver.war` 파일을 다시 만들어 다시 배포합니다.

구체적인 단계는 **Sun Java System SAML v2 Plug-in for Federation Services User's Guide**의 2 장, "Installing the SAML v2 Plug-in for Federation Services"를 참조하십시오.

Access Manager 7 2005Q4 패치 5

Access Manager 7 패치 5(개정 05)에서는 패치에 포함된 README 파일에 나열된 여러 문제를 해결합니다. 또한 패치 5에 포함된 새 기능, 문제점 및 설명서 업데이트 사항은 다음과 같습니다.

패치 5의 새로운 기능

패치 5의 알려진 문제점 및 제한 사항

- 40 페이지 “CR# 6507383 및 CR# 6507377: 분산 인증에 명시적인 goto URL 매개 변수가 필요합니다.”
- 41 페이지 “CR# 6402167: LDAP JDK 4.18을 사용하면 LDAP 클라이언트/Directory Server 문제가 발생합니다.”
- 41 페이지 “CR# 6352135: 분산 인증 UI 서버 파일이 잘못된 위치에 설치됩니다.”
- 42 페이지 “CR# 6513653: com.iplanet.am.session.purgedelay 등록 정보 설정에 문제가 있습니다.”

국제화(g11n) 문제

- 41 페이지 “CR# 6522720: Windows 및 HP-UX 시스템의 경우 콘솔 온라인 도움말에서 멀티 바이트 문자 검색이 동작하지 않습니다.”
- 41 페이지 “CR# 6524251: Windows 시스템에서 Access Manager를 구성하는 동안 출력 메시지의 멀티 바이트 문자가 올바르게 표시되지 않습니다.”
- 42 페이지 “CR# 6526940: Windows 시스템에서 영어 이외의 로켈로 패치 5를 설치하는 동안 메시지 텍스트 대신 등록 정보 키가 표시됩니다.”

설명서 업데이트

- 92 페이지 “영역 모드에서 레거시 모드로 되돌릴 수 없는 Access Manager 문제 문서화(6508473)”
- 93 페이지 “지속 검색 사용 불가능에 대한 상세 정보 문서화(6486927)”
- 93 페이지 “Access Manager 지원 및 비지원 권한 문제 문서화(2143066)”
- 94 페이지 “쿠키 기반 지속 요청 라우팅 문제 문서화(6476922)”
- 95 페이지 “Windows 2003을 위한 Windows 데스크탑 SSO 구성 문제 문서화(6487361)”
- 95 페이지 “분산 인증 UI 서버의 비밀번호 설정 단계 문제 문서화(6510859)”
- 96 페이지 “추가 정보가 필요한 "새 사이트 이름 만들기" 온라인 도움말(2144543)”
- 96 페이지 “Windows 시스템의 관리자 비밀번호 구성 매개 변수(ADMIN_PASSWD) 문제 문서화(6470793)”

HP-UX 시스템 지원

패치 **126371**에서는 HP-UX 시스템에 대한 지원을 제공합니다. 자세한 내용은 다음 항목을 참조하십시오.

- 18 페이지 “HP-UX 시스템용 패치 설치 지침”
- 19 페이지 “사후 설치 고려 사항”

HP-UX 시스템에 설치하는 방법은 **Sun Java Enterprise System 2005Q4 설치 설명서**를 참조하십시오.

Microsoft Windows 시스템 지원

패치 **124296**에서는 Windows 시스템에 대한 지원을 제공합니다. 자세한 내용은 다음 항목을 참조하십시오.

- 17 페이지 “Windows 시스템용 패치 설치 지침”

- 19 페이지 “사후 설치 고려 사항”
- 35 페이지 “Windows 시스템에 사용 가능한 조정 스크립트”

Windows 시스템에 설치하는 방법은 **Sun Java Enterprise System 2005Q4 Installation Guide for Microsoft Windows**를 참조하십시오.

새로운 updateschema.sh 스크립트로 LDIF 및 XML 파일 로드

패치 5 이상에는 Directory Server 서비스 스키마를 업데이트하는 데 필요한 다음 파일을 로드하는 updateschema.sh 스크립트가 들어 있습니다.

- AddLDAPFilterCondition.xml
- amPolicyConfig_mod_ldfc.xml
- accountLockoutData.xml
- accountLockout.ldif
- idRepoServiceAddAttrSchemaRequest_Cache.xml
- wsf1.1_upgrade.xml
- amAuth_mod.xml
- amAuthCert_mod.xml

이전 Access Manager 패치 릴리스에서는 이러한 파일을 수동으로 로드해야 했습니다.

updateschema.sh 스크립트를 실행하려면

1. 수퍼유저(root)로 로그인합니다.
2. 패치 디렉토리로 변경합니다.
3. 스크립트를 실행합니다. 예를 들어 Solaris 시스템의 경우 다음과 같습니다.

   ```
   # cd /120954-07
   # ./updateschema.sh
   ```

   Windows 시스템의 경우 해당 스크립트는 updateschema.pl입니다.
4. 스크립트에서 요청하는 메시지가 나타나면 다음 항목을 입력합니다.
   - Directory Server 호스트 이름 및 포트 번호
   - Directory Server 관리자 DN 및 비밀번호
   - amadmin DN 및 비밀번호
5. 스크립트에서 입력 항목을 검증한 다음 해당 파일을 로드합니다. 또한 스크립트에서 다음과 같은 로그 파일에 기록합니다.
   - Solaris 시스템: /var/opt/SUMWam/logs/AM70Patch.upgrade.schema.*timestamp*
   - Linux 시스템: /var/opt/sun/identity/logs/AM70Patch.upgrade.schema.*timestamp*
6. 스크립트가 완료되면 Access Manager 웹 컨테이너를 다시 시작합니다.

주 패치 5를 취소하는 경우 updateschema.sh 스크립트로 추가된 스키마 변경 항목이 Directory Server에서 제거되지 않습니다. 그러나 패치가 취소된 후에는 Access Manager 기능이나 유용성에 영향을 미치지 않으므로 이러한 스키마 변경 항목을 수동으로 제거하지 않아도 됩니다.

특정 응용 프로그램의 유휴 세션 시간 초과 값 지원

패치 5를 적용하면 응용 프로그램마다 별도의 유휴 세션 시간 초과 값을 설정할 수 있습니다. 기업에서는 일부 응용 프로그램의 유휴 세션 시간 초과 값이 세션 서비스에 지정된 값보다 작아야 할 수도 있습니다. 예를 들어 세션 서비스의 유휴 세션 시간 초과 값을 30분으로 지정했지만 사용자가 10분 이상 유휴 상태로 있을 경우 시간 초과로 인해 HR 응용 프로그램이 중지됩니다.

이 기능을 사용하기 위한 요구 사항은 다음과 같습니다.

- 응용 프로그램을 보호하는 에이전트는 Access Manager의 URL 정책 결정을 적용하도록 구성되어야 합니다.
- 에이전트는 자체 정책 결정 캐시 모드로 실행되어야 합니다. 다음 등록 정보를 참조하십시오.
  - 웹 에이전트의 경우: com.sun.am.policy.am.fetch_from_root_resource
  - J2EE 에이전트의 경우: com.sun.identity.policy.client.cacheMode
- Access Manager AMConfig.properties 파일에는 조건을 마지막으로 평가하는 것처럼 정책 구성 요소 평가 순서가 지정되어야 합니다. 다음 등록 정보를 참조하십시오.

  com.sun.identity.policy.Policy.policy_evaluation_weights
- 에이전트에서 로컬로 캐시되는 정책에 기반하여 허용되는 응용 프로그램 액세스는 Access Manager에서 조건으로 인식되지 않습니다. 따라서 실제 응용 프로그램 유휴 시간 초과 값은 응용 프로그램 유휴 시간 초과 값과 이 값에서 에이전트 캐시 기간을 뺀 값 사이에 있습니다.

이 기능을 사용하려면

- 인증 방식 조건을 응용 프로그램 관련 유휴 세션 시간 초과 값이 필요한 응용 프로그램을 보호하는 정책에 추가합니다.
- 인증 방식 조건에 응용 프로그램 이름과 시간 초과 값을 지정합니다.
- 응용 프로그램의 자원에 적용되는 모든 정책에 동일한 응용 프로그램 이름과 시간 초과 값을 사용합니다.
- 시간 초과 값을 분 단위로 지정합니다. 값이 0이거나 세션 서비스에 지정된 유휴 세션 시간 초과 값보다 큰 경우 이 값이 무시되며 세션 서비스의 시간 초과 값이 적용됩니다.

예를 들어 다음과 같은 인증 방식 조건을 사용하는 http://host.sample.com/hr/* 정책이 있다고 가정합니다.

- 인증 방식: LDAP

- 응용 프로그램 이름: HR
- 시간 초과 값: 10

HR 응용 프로그램 자원을 보호하도록 정의된 정책이 여러 개 있으면 모든 정책에 조건을 추가해야 합니다.

특정 세션에 있는 사용자가 Access Manager 에이전트로 보호되는 HR 응용 프로그램에 액세스하려고 할 때 아직 인증되지 않은 경우 LDAP 스키마로 인증되도록 요청하는 메시지가 나타납니다.

사용자가 이미 LDAP 스키마로 인증되어 있으면 사용자가 마지막으로 인증된 이후 경과된 시간 또는 사용자가 HR 응용 프로그램에 마지막으로 액세스한 이후 경과된 시간이 10분 미만일 때만 응용 프로그램에 액세스할 수 있습니다. 그렇지 않으면 사용자가 LDAP 스키마로 다시 인증되어 응용 프로그램에 액세스하도록 요구하는 메시지가 나타납니다.

분산 인증 UI 서버에 배포될 수 있는 CDC 서블릿

CDC 서블릿은 크로스 도메인 단일 사인 온(CDSSO)을 사용하기 위해 DMZ의 분산 인증 UI 서버와 함께 사용될 수 있습니다. Access Manager 서버는 방화벽 뒤에 배포되며 CDSSO를 얻기 위해 Access Manager에 시도하는 액세스는 모두 분산 인증 UI 서버에서 CDC 서블릿으로 처리됩니다. CDSSO를 사용하도록 설정하려면 관련 정책 에이전트 설명서를 참조하고 다음 단계를 추가로 수행합니다.

- 분산 인증측 클라이언트에 있는 CDC 서블릿을 가리키도록 에이전트의 `AMAgent.properties` 파일을 수정합니다. 예를 들어 웹 에이전트의 경우 다음 등록 정보를 변경합니다.

  ```
  com.sun.am.policy.agents.config.cdcservlet.url=
      http://DAhost.DAdomain:DAport/DISTAUTH_DEPLOY_URI/cdcservlet
  ```

- Access Manager에서 필요한 경우 에이전트로 보호되어야 하는 자원에 대한 정책을 정책을 정의합니다. 예를 들어 에이전트가 `host.example.com:80`에 있으면 자원에 대한 정책을 `http://host.example.com:80/*`으로 정의합니다.

CDC 서블릿에서 Access Manager 로그인 URL로 리디렉션할 때 지정될 수 있는 영역

이제는 CDC 서블릿에 영역 이름을 지정할 수 있으므로 Access Manager 로그인 URL로 리디렉션할 때 영역 이름이 포함되어 사용자가 특정 영역에 로그인할 수 있습니다. 예를 들면 다음과 같습니다.

```
com.sun.am.policy.agents.config.cdcservlet.url=
    http://lb.example.com/amserver/cdcservlet?org=realm1
```

UPN 값으로 사용자 프로필을 매핑할 수 있는 인증서 인증

이전에는 인증서 인증에서 subjectDN에 있는 dn 구성 요소만 사용하여 사용자 프로필을 매핑했습니다. 이제는 Access Manager에서 프로필 매핑을 위한 SubjectAltNameExt에 사용자 기본 이름(UPN) 값을 사용할 수 있습니다.

다중 서버 환경에서 발생하는 로그아웃 사후 인증 처리

세션 페일오버가 구성되거나 구성되지 않은 다중 서버 환경에서 사용자가 처음 로그인한 서버와 다른 서버에서 로그아웃할 때 사후 인증 처리가 발생합니다.

SAML에서 새 이름 식별자 SPI 지원

이제는 SAML에서 새 이름 식별자 서비스 공급자 인터페이스(SPI)를 지원하므로 사이트에서 SAML 명제의 이름 식별자를 사용자 정의할 수 있습니다. 사이트에서 새로운 NameIdentifierMapper 인터페이스를 구현하여 사용자 계정을 SAML 명제의 주제에 포함된 이름 식별자와 매핑할 수 있습니다.

사이트 모니터링을 위한 새로운 구성 등록 정보

Access Manager 사이트 모니터링 기능에는 다음과 같은 새 기능이 포함되어 사이트 상태 확인 동작을 지정할 수 있습니다.

등록 정보	설명
com.sun.identity.urlchecker.invalidate.interval	중단되었거나 응답하지 않는 사이트를 인식하기 위한 시간 간격(밀리초)입니다. 기본값: 70,000밀리초(70초)
com.sun.identity.urlchecker.sleep.interval	사이트 상태 확인이 일시 정지되어야 하는 시간 간격(밀리초)입니다. 기본값: 30,000밀리초(30초)
com.sun.identity.urlchecker.targeturl	Access Manager 프로세스 상태 확인을 위한 다른 대상 URL입니다. 기본값: "/amserver/namingservice".

이 패치는 이러한 등록 정보를 AMConfig.properties 파일에 추가하지 않습니다. 이러한 새로운 등록 정보에 기본값이 아닌 다른 값을 사용하려면 다음과 같이 하십시오.

1. AMConfig.properties 파일에 등록 정보와 해당 값을 추가합니다. 정책 에이전트에 대해서는 이러한 등록 정보를 AMAgents.properties 파일에 추가합니다.
2. 값을 적용하려면 Access Manager 웹 컨테이너를 다시 시작합니다.

인증 체인에서 더 이상 두 번 인증될 필요가 없는 사용자

사이트에서 3개 LDAP 모듈로 인증 체인을 구성한다고가정합니다. 이 경우 모든 모듈은 SUFFICIENT로 설정되고, 두 옵션(iplanet-am-auth-shared-state-enabled 및 iplanet-am-auth-store-shared-state-enabled)은 true로 설정됩니다. 예를 들면 다음과 같습니다.

```
<AttributeValuePair>
   <Value>A-LDAP SUFFICIENT iplanet-am-auth-shared-state-enabled=true
iplanet-am-auth-store-shared-state-enabled=true</Value>
   <Value>B-LDAP SUFFICIENT iplanet-am-auth-shared-state-enabled=true
iplanet-am-auth-store-shared-state-enabled=true</Value>
   <Value>C-LDAP SUFFICIENT iplanet-am-auth-shared-state-enabled=true
iplanet-am-auth-store-shared-state-enabled=true</Value>
</AttributeValuePair>
```

패치 5는 모듈 옵션에 사용 가능한 두 값(tryFirstPass(기본값) 및 useFirstPass)을 갖는iplanet-am-auth-shared-state-behavior-pattern 옵션을 새로 추가합니다.

이전 시나리오에서 설명한 대로 사용자가 인증을 위해 사용자 아이디와 비밀번호를 두 번씩 입력하지 않도록 하려면 인증 체인의 모든 모듈에 대해 새로운 이 옵션을 useFirstPass로 설정합니다. 이전에는 세 번째 LDAP 인스턴스에서만 존재하는 사용자가 인증을 위해 사용자 아이디와 비밀번호를 두 번씩 입력해야 했습니다.

성능 조정 스크립트 변경

패치 5에 포함된 성능 조정 스크립트에 대한 변경 내용은 다음과 같습니다.

- 33 페이지 “비밀번호 파일을 지원하는 조정 스크립트”
- 34 페이지 “Directory Server에 있는 불필요한 ACI를 제거하는 조정 스크립트”
- 34 페이지 “분산 인증 UI 서버 웹 컨테이너를 조정할 수 있는 조정 스크립트”
- 35 페이지 “Solaris OS 및 Linux OS를 모두 조정하는 단일 amtune-os 스크립트”
- 35 페이지 “Solaris 10 로컬 영역에서 완료하기 위해 실행하는 조정 스크립트”
- 35 페이지 “Windows 시스템에 사용 가능한 조정 스크립트”
- 36 페이지 “Sun Fire T1000 및 T2000 서버 조정 시 고려 사항”

37 페이지 “CR# 6527663: com.sun.identity.log.resolveHostName 등록 정보의 기본값은 true가 아니라 false여야 합니다.”도 참조하십시오.

비밀번호 파일을 지원하는 조정 스크립트

패치 5를 사용하면 조정 스크립트에 사용될 비밀번호를 텍스트 파일에 지정할 수 있습니다. 이전에는 명령줄 인수로만 비밀번호를 입력할 수 있어 보안 문제가 발생할 수 있었습니다. 비밀번호 파일을 사용하려면 필요에 따라 다음 변수를 파일에 설정합니다.

```
DS_ADMIN_PASSWORD=DirectoryServer-admin-password
AS_ADMIN_PASSWORD=ApplicationServer8-admin-password
```

예를 들어 Application Server 8을 조정하려면

```
# ./amtune-as8 password-file
```

여기서 *password-file*에는 Application Server 8 관리자 비밀번호로 설정된 `AS_ADMIN_PASSWORD`가 포함됩니다.

`ldapmodify`, `ldapsearch`, `db2index` 및 `dsconf` Directory Server 유틸리티를 호출하는 경우 조정 스크립트에는 `-j` *password-file* 옵션이 사용됩니다.

Directory Server에 있는 불필요한 ACI를 제거하는 조정 스크립트

Access Manager 7 2005Q4가 영역 모드로 설치되면 위임 권한이 액세스 권한을 결정하는 데 사용되기 때문에 일부 Directory Server ACI가 필요하지 않습니다. Access Manager 7 2005Q4 패치 5를 사용하면 `amtune-prepareDSTuner` 스크립트를 실행하여 불필요한 ACI를 제거할 수 있습니다. 이 스크립트는 `remacis.ldif` 파일에서 ACI 목록을 판독한 다음 `ldapmodify` 유틸리티를 호출하여 해당 파일을 제거합니다.

`amtune-prepareDSTuner` 스크립트를 사용하면 Solaris, Linux, HP-UX 및 Windows 시스템에서 불필요한 ACI를 제거할 수 있습니다. 스크립트 실행 방법을 포함한 자세한 내용은 **Technical Note: Sun Java System Access Manager ACI Guide**를 참조하십시오.

분산 인증 UI 서버 웹 컨테이너를 조정할 수 있는 조정 스크립트

웹 컨테이너에 분산 인증 UI 서버를 배포한 후 Access Manager 조정 스크립트를 실행하여 웹 컨테이너를 조정할 수 있습니다. 다음 조정 스크립트는 개별 웹 컨테이너에 대해 JVM 및 기타 조정 옵션을 설정합니다.

표 2 Access Manager 웹 컨테이너 조정 스크립트

웹 컨테이너	조정 스크립트
`amtune-ws61`	Web Server 6.1
`amtune-as7`	Application Server 7
`amtune-as8`	Application Server Enterprise Edition 8.1

분산 인증 UI 서버를 위한 웹 컨테이너를 조정하려면

1. 분산 인증 UI 서버가 배포된 시스템에는 Access Manager 서버가 설치되지 않으므로 설치된 Access Manager 서버 설치로부터 앞서 나온 표에서 보여 주는 해당 웹 컨테이너 조정 스크립트, `amtune-env` 구성 파일 및 `amtune-utils` 스크립트를 복사합니다. Solaris 또는 Linux 운영 체제를 조정하는 경우에는 `amtune-os` 스크립트도 복사합니다.
2. `amtune-env` 구성 파일에서 매개 변수를 편집하여 웹 컨테이너와 조정 옵션을 지정합니다. REVIEW 모드로 스크립트를 실행하려면 `amtune-env` 파일에 `AMTUNE_MODE=REVIEW`를 설정합니다.

3. REVIEW 모드로 웹 컨테이너 조정 스크립트를 실행합니다. REVIEW 모드에서 스크립트는 amtune-env 파일의 값에 기반한 조정 변경을 제안하지만 배포 시 실제로 변경을 적용하지는 않습니다.
4. 디버그 로그 파일에 있는 조정 권장 사항을 검토합니다. 필요한 경우 이 실행에 기반하여 amtune-env 파일을 변경합니다.
5. 조정을 변경하려면 amtune-env 파일에 AMTUNE_MODE=CHANGE를 설정합니다.
6. CHANGE 모드로 조정 스크립트를 실행하여 배포에 대한 조정을 변경합니다.

조정 스크립트를 실행하여 Access Manager 웹 컨테이너를 조정하는 방법은 **Sun Java System Access Manager 7 2005Q4 Performance Tuning Guide**의 2 장, "Access Manager Tuning Scripts"를 참조하십시오.

Solaris OS 및 Linux OS를 모두 조정하는 단일 amtune-os 스크립트

패치 5에는 Solaris OS 및 Linux OS를 모두 조정하는 단일 amtune-os 스크립트가 포함되어 있습니다. 스크립트는 uname -s 명령에서 OS 종류를 결정합니다. 이전에는 Access Manager에서 조정할 OS마다 별도의 amtune-os 스크립트를 제공했습니다.

Solaris 10 로컬 영역에서 완료하기 위해 실행하는 조정 스크립트

Access Manager가 Solaris 10 로컬 영역에 설치되는 경우 amtune-os를 제외한 모든 조정 스크립트가 로컬 영역에서 실행될 수 있습니다. amtune-os 스크립트는 로컬 영역에서 경고 메시지를 표시하지만 OS를 조정하지 않습니다. 그렇지만 이 스크립트는 요청한 다른 조정 스크립트를 계속 실행합니다. 이전에는 로컬 영역에서 amtune-os 스크립트가 중단되고 요청한 다음 조정 스크립트도 모두 실행되지 않았습니다.

amtune 스크립트는 Solaris 10 전역 영역에서 amtune-os를 호출하여 실행하도록 요청한 다른 스크립트와 함께 OS를 조정합니다.

Windows 시스템에 사용 가능한 조정 스크립트

패치 5에는 Windows 시스템용 조정 스크립트가 포함되어 있습니다. Windows 시스템에서 조정 스크립트를 실행하는 것은 Solaris 시스템이나 Linux 시스템에서 조정 스크립트를 실행하는 것과 비슷하지만 다음과 같은 차이점이 있습니다.

- Windows 스크립트는 Perl로 작성되며 Active Perl 5.8이 실행되어야 합니다.
- Directory Server를 조정하는 경우 amtune-prepareDSTuner.pl 스크립트는 amtune-utils.pl, amtune-directory.pl, remacis.ldif 및 amtune-samplepassordfile 파일을 압축할 수 없으므로 스크립트를 실행한 후에는 Directory Server 시스템에 이 파일들을 복사해야 합니다.
- Windows 운영 체제를 조정하는 스크립트는 사용할 수 없습니다.
- 영역을 지원하지 않습니다.
- 스크립트를 실행하기 전에 Access Manager 설치 디렉토리에 대한 $BASEDIR 매개 변수를 amtune-env.pl 파일에 설정해야 합니다.

Sun Fire T1000 및 T2000 서버 조정 시 고려 사항

Access Manager가 Sun Fire T1000 또는 T2000 서버에 설치되는 경우 패치 5 Web Server 6.1 및 Application Server 8용 조정 스크립트는 다음과 같이 JVM GC ParallelGCThreads 매개변수를 8로 설정합니다.

```
-XX:ParallelGCThreads=8
```

이 매개 변수는 32개 스레드 동시 실행 가능 시스템에서 지나치게 높을 수도 있는 가비지 컬렉션 스레드 수를 줄입니다. 그러나 Sun Fire T1000 또는 T2000 서버와 같은 32개 스레드 가상 CPU 시스템에서 전체 가비지 컬렉션 작업을 최소화하려는 경우 이 값을 16 또는 20까지로 높일 수 있습니다.

또한 CoolThreads 기술의 CMT 프로세서를 탑재하는 Solaris SPARC 시스템의 경우 /etc/opt/SUNWam/config/AMConfig.properties 파일 끝에 다음 등록 정보를 추가하는 것이 좋습니다.

```
com.sun.am.concurrencyRate=value
```

value 기본값은 16이지만 Sun Fire T1000 또는 T2000 서버의 코어 수에 따라 이 등록 정보를 더 낮은 값으로 설정할 수 있습니다.

IIS 6.0 정책 에이전트에서의 기본 인증

Microsoft 인터넷 정보 서비스(IIS) 6.0의 기본 인증을 사용할 수 있도록 지원하려면 정책 에이전트에서 사용자의 이름과 비밀번호를 확보해야 합니다. 패치 5에는 사용자 비밀번호의 DES 암호화를 통해 기본 인증 기능을 사용할 수 있도록 지원하는 새로운 클래스가 포함되어 있습니다.

- DESGenKey.java는 사용자 비밀번호를 암호화하고 해독하는 데 사용되는 고유 키를 생성합니다.
- ReplayPasswd.java는 AMConfig.properties 파일의 com.sun.am.replaypasswd.key 등록 정보에 있는 암호화 키를 판독하며, 비밀번호를 암호화하고, sunIdentityUserPassword 세션 등록 정보에 암호화된 비밀번호를 할당합니다.

IIS 6.0 기본 인증을 사용하려면 Access Manager 서버측과 IIS 6.0 정책 에이전트측 모두에서 다음 단계를 수행해야 합니다.

Access Manager 서버측:

1. DESGenKey.java를 실행하여 비밀번호 암호화 및 해독을 위한 고유 암호화 키를 생성합니다. Solaris 시스템에서 DESGenKey.java 파일은 com/sun/identity/common 디렉토리에 있으며, /opt/SUNWam/lib 디렉토리의 am_sdk.jar 파일에 포함됩니다. 예를 들어 암호화 키를 생성하는 명령은 다음과 같습니다.

   ```
   # cd /opt/SUNWam/lib
   # java -cp am_sdk.jar com.sun.identity.common.DESGenKey
   ```

2. 1단계의 암호화 키 값을 AMConfig.properties 파일의 com.sun.am.replaypasswd.key 등록 정보에 할당합니다.
3. ReplayPasswd.java를 사후 인증 플러그인으로 배포합니다. 플러그인을 구성할 때 다음과 같이 전체 클래스 이름을 사용합니다.
   com.sun.identity.authentication.spi.ReplayPasswd.

IIS 6.0 정책 에이전트측:

1. 서비측의 암호화 키 값을AMAgent.properties 파일의 com.sun.am.replaypasswd.key 등록 정보에 할당합니다. Access Manager 서버와 IIS 6.0 정책 에이전트에서 모두 동일한 암호화 키를 사용해야 합니다.
2. IIS 6.0 관리자에서 기본 인증을 사용하도록 설정합니다.

IIS 6.0 정책 에이전트가 세션 응답의 암호화된 비밀번호를 읽고 com.sun.am.replaypasswd.key 등록 정보의 비밀번호를 해독한 후 기본 인증을 사용하도록 인증 헤더를 설정합니다.

IIS 6.0 정책 에이전트에 대한 자세한 내용은 **Sun Java System Access Manager Policy Agent 2.2 Guide for Microsoft Internet Information Services 6.0**을 참조하십시오.

CR# 6567746: HP-UX 시스템에서 Access Manager 패치 5는 비밀번호 재시도 횟수를 초과한 경우 잘못된 errorCode 값을 보고합니다.

사용자 계정이 잠긴 경우 HP-UX 시스템용 Access Manager 7 2005Q4 패치 5는 비밀번호 재시도 횟수를 초과하면 errorCode = 107 대신 errorCode = null을 보고합니다.

해결 방법: 없음.

CR# 6527663: com.sun.identity.log.resolveHostName 등록 정보의 기본값은 true가 아니라 false여야 합니다.

amtune-identity 조정 스크립트를 실행하기 전에 AMConfig.properties 파일에 false로 설정된 다음 등록 정보를 추가하는 것이 좋습니다.

```
com.sun.identity.log.resolveHostName=false
```

false 값은 호스트 이름을 결정하는 데 미치는 영향을 최소화하여 성능을 향상시킬 수 있습니다. 그러나 클라이언트 시스템의 호스트 이름이 amAuthentication.access 로그에 출력되도록 하려면 값을 true로 설정합니다.

CR# 6527528: 패치를 제거하면 일반 텍스트에 amldapuser 비밀번호가 포함된 XML 파일이 남아 있습니다.

전체 설치된 Access Manager 서버에서 패치 5를 제거하면 amAuthLDAP.xml 및 amPolicyConfig.xml 파일에 일반 텍스트 형식의 amldapuser 비밀번호가 있습니다. 플랫폼에 따라 이러한 파일이 있는 디렉토리는 다음과 같습니다.

- Solaris 시스템: `/etc/opt/SUNWam/config/xml`
- Linux 및 HP-UX 시스템: `/etc/opt/sun/identity/config/xml`

해결 방법: `amAuthLDAP.xml` 및 `amPolicyConfig.xml` 파일을 편집하여 일반 텍스트 비밀번호를 삭제합니다.

CR# 6527516: 클라이언트 SDK와 통신하려면 WebLogic의 모든 서버에 JAX-RPC 1.0 JAR 파일이 필요합니다.

Access Manager 7 2005Q4 패치에 있는 BEA WebLogic Server용 Access Manager 구성 스크립트(`amwl81config`)는 WebLogic 인스턴스용 `classpath`에 JAX-RPC 1.1 JAR 파일을 추가합니다. 이렇게 수정하면 Sun Java System Portal Server와 같은 제품에는 유용하지만 WebLogic Server에 전체 설치(`DEPLOY_LEVEL=1`)로 배포된 서버에서 설치된 클라이언트 SDK와 통신할 수 없게 되며 결과적으로 예외가 발생합니다.

따라서 Access Manager 7 2005Q4 서버가 BEA WebLogic Server에 설치되는 경우 Access Manager 클라이언트 SDK와 통신하려면 `startWebLogic.sh` 스크립트의 `CLASSPATH`를 JAX-RPC 1.0 JAR 파일의 위치로 설정해야 합니다.

해결 방법: Access Manager 패치를 적용하기 전에 WebLogic Server 인스턴스가 JAX-RPC 1.1 JAR 파일 대신 JAX-RPC 1.0 JAR 파일을 사용하도록 `startWebLogic.sh` 스크립트에서 `CLASSPATH`를 설정합니다.

1. Access Manager 서버에서 수퍼유저(`root`)로 로그인합니다.
2. `startWebLogic.sh` 스크립트를 편집하여 `CLASSPATH`에서 JAX-RPC 1.0 JAR 파일을 사용하도록 변경합니다. 예를 들면 다음과 같습니다.

현재 값:

```
CLASSPATH=/etc/opt/SUNWam/config:
AccessManager-base/AccessManager-package-dir/lib/jax-qname.jar:
AccessManager-base/AccessManager-package-dir/lib/namespace.jar:
AccessManager-base/AccessManager-package-dir/lib/jaxrpc-api.jar:
AccessManager-base/AccessManager-package-dir/lib/jaxrpc-spi.jar:
AccessManager-base/AccessManager-package-dir/lib/jaxrpc-impl.jar:
```

새 값:

```
CLASSPATH=/etc/opt/SUNWam/config:
AccessManager-base/AccessManager-package-dir/lib/jax-qname.jar:
AccessManager-base/AccessManager-package-dir/lib/namespace.jar:
AccessManager-base/AccessManager-package-dir/lib/jaxrpc_1.0/jaxrpc-api.jar:
AccessManager-base/AccessManager-package-dir/lib/jaxrpc-ri.jar:
```

여기서 *AccessManager-base*는 기본 설치 디렉토리입니다. 기본값은 Solaris 시스템의 경우 `/opt`이며, Linux 및 HP-UX 시스템의 경우 `/opt/sun`입니다. *AccessManager-package-dir*은 Access Manager 패키지 디렉토리입니다.

5. WebLogic Server 인스턴스를 다시 시작합니다.

CR # 6523499: 모든 Linux 시스템 사용자가 패치 5의 amsilent 파일을 읽을 수 있습니다.

Linux 시스템에서 postpatch 스크립트는 모든 사용자에게 읽기 액세스를 허용하는 644 권한을 갖는 /opt/sun/identity/amsilent 파일을 만듭니다.

해결 방법: installpatch 스크립트를 실행한 후에 amsilent 파일에 대한 권한을 소유자에 대해서만 읽기 및 쓰기 액세스를 허용하도록 변경합니다. 예를 들면 다음과 같습니다.

```
# chmod 600 /opt/sun/identity/amsilent
```

CR# 6520326: 서버의 두 번째 Access Manager 인스턴스에 패치 5를 적용하면 첫 번째 인스턴스에 대해 serverconfig.xml 파일을 덮어씁니다.

이 배포 시나리오에서는 별도의 웹 컨테이너 인스턴스에 하나씩 실행되는 두 Access Manager 인스턴스가 동일한 호스트 서버에 배포됩니다. 이 경우 다음 단계를 수행합니다.

1. 패치 5를 적용합니다.
2. amsilent 파일을 수정한 다음 첫 번째 Access Manager 인스턴스를 다시 배포합니다.
3. 두 번째 Access Manager 인스턴스에 대해 amsilent 파일을 다시 수정한 다음 해당 인스턴스를 다시 배포합니다.

amsilent 파일에서 NEW_INSTANCE=false인 경우 첫 번째 Access Manager 인스턴스에 대한 serverconfig.xml 파일이 두 번째 Access Manager 인스턴스 정보를 덮어씁니다. 그런 후에 첫 번째 Access Manager 인스턴스를 다시 시작하면 해당 인스턴스가 실행되지 않습니다. 플랫폼에 따라 serverconfig.xml 파일이 있는 디렉토리는 다음과 같습니다.

- Solaris 시스템: /etc/opt/SUNWam/config
- Linux 시스템: /etc/opt/sun/identity/config

해결 방법: 두 번째 Access Manager를 배포할 때 amsilent 파일에 NEW_INSTANCE=true를 설정합니다. 그러면 두 번째 Access Manager 인스턴스에 대한 serverconfig.xml 파일이 올바른 정보로 업데이트되며, 첫 번째 Access Manager 인스턴스에 대한 serverconfig.xml 파일을 덮어쓰지 않습니다.

CR# 6520016: SDK 전용 시스템에 패치 5를 설치하면 샘플 makefile을 덮어씁니다.

SDK 전용 시스템에 패치 5를 적용하면 샘플 makefile을 덮어씁니다.

해결 방법: SDK 전용 시스템에 패치 5를 적용하는 경우 다시 구성하지 않아도 되지만 샘플 makefile을 사용하려면 다음 단계를 수행하여 이 makefile에 대한 LDIF 및 등록 정보 파일을 업데이트합니다(태그 스왑 수행).

1. DEPLOY_LEVEL=14를 사용하는 amconfig 스크립트를 실행하여 SDK를 제거하고 웹 컨테이너 구성을 해제합니다.
2. DEPLOY_LEVEL=4를 사용하는 amconfig 스크립트를 실행하여 SDK를 다시 설치하고 웹 컨테이너를 다시 구성합니다.

CR#6515502: LDAPv3 저장소 플러그인에서 언제나 별칭 검색 속성을 올바르게 처리하는 것은 아닙니다.

대부분의 검색에서 이 문제가 해결되었지만별칭 검색 속성을 설정할 때는 주의해야 합니다. 별칭 검색 속성 값은 조직 전체에서 고유해야 합니다. 별칭 검색 속성이 둘 이상 설정되는 경우 데이터 저장소에 있는 한 항목이 한 속성과 일치하고 다른 한 항목은 다른 속성과 일치할 수 있습니다. 이 경우 Access Manager 서버에서 다음과 같은 오류가 발생합니다.

내부 인증 오류가 발생했습니다. 시스템 관리자에게 문의하십시오.

해결 방법: 없음

CR# 6515383: 분산 인증과 J2EE 에이전트가 동일한 웹 컨테이너에서 작동하지 않습니다.

분산 인증 UI 서버와 J2EE 정책 에이전트가 동일한 웹 컨테이너에 설치되면 작동하지 않습니다.

해결 방법: 두 번째 웹 컨테이너 인스턴스를 만들고 분산 인증 UI 서버와 J2EE 정책 에이전트를 서로 다른 컨테이너 인스턴스에 배포합니다.

CR# 6508103: Windows 시스템 온라인 도움말에서 Application Server 관련 응용 프로그램 오류가 반환됩니다.

Windows 시스템의 Sun Java System Application Server에 Access Manager를 배포할 때 영역 모드 콘솔의 도움말 화면 왼쪽 패널에 있는 도움말을 클릭하면 응용 프로그램 오류가 발생합니다.

해결 방법: JAVA_HOME\jre\lib\ext 디렉토리에 *javaes-install-dir*\share\lib\jhall.jar 파일을 복사한 다음 Application Server를 다시 시작합니다.

CR# 6507383 및 CR# 6507377: 분산 인증에 명시적인 goto URL 매개 변수가 필요합니다.

명시적 goto URL 매개 변수가 지정되지 않으면 분산 인증 UI 서버에서 Access Manager에 지정된 성공 URL에 있는 goto로 리디렉션하려고 시도합니다. 이 리디렉션은 다음과 같은 이유로 실패할 수 있습니다.

- 상대 URL이면 분산 인증 UI 서버에서 해당 페이지를 사용할 수 없습니다

- 절대 URL이면 브라우저에서 해당 URL에 도달할 수 없습니다.

해결 방법: 항상 분산 인증 UI 서버용 명시적 `goto` URL 매개 변수를 지정합니다.

CR# 6402167: LDAP JDK 4.18을 사용하면 LDAP 클라이언트/Directory Server 문제가 발생합니다.

Access Manager 7 2005Q4는 Java ES 2005Q4 릴리스의 일부로서 LDAP JDK 4.18과 함께 릴리스되었지만 Access Manager 및 Directory Server 연결 문제가 다양하게 발생했습니다.

해결 방법: 다음 Sun Java System LDAP Java Development Kit 패치 중 하나를 적용합니다.

- Solaris OS, SPARC 및 x86 플랫폼: 119725-04
- Linux OS: 120834-02

패치는`http://sunsolve.sun.com`.

CR# 6352135: 분산 인증 UI 서버 파일이 잘못된 위치에 설치됩니다.

Solaris 시스템에서 Java ES 설치 프로그램이 `Makefile.distAuthUI`, `README.distAuthUI` 및 `amauthdistui.war` 분산 인증 UI 서버 파일을잘못된 위치(`/opt/SUNComm/SUNWam`)에 설치합니다.

해결 방법: 올바른 위치인`/opt/SUNWam`에 해당 파일을 복사합니다.

주: 패치에서 해결된 분산 인증 UI 서버 문제는 모두 `/opt/SUNComm/SUNWam/amauthdistui.war` 파일에 포함되므로 Access Manager 서버에 패치를 적용한 다음 WAR 파일을 다시 만들어 배포할 때마다 마찬가지로 이러한 파일을 `/opt/SUNWam` 디렉토리에 복사해야 합니다.

CR# 6522720: Windows 및 HP-UX 시스템의 경우 콘솔 온라인 도움말에서 멀티 바이트 문자 검색이 동작하지 않습니다.

Access Manager가 Windows 또는 HP-UX 시스템에서 멀티 바이트 문자(예: 일본어)를 사용하는 로켈로 설치된 경우 콘솔 온라인 도움말에서 멀티 바이트 문자를 사용하여 키워드를 입력하는 경우 검색이 동작하지 않습니다.

해결 방법: 없음

패치 6 업데이트: Access Manager 7 2005Q4 패치 6은 Windows 시스템에서의 이 문제를 수정했습니다. 그러나 HP-UX 시스템에서는 이 문제가 여전히 존재합니다.

CR# 6524251: Windows 시스템에서 Access Manager를 구성하는 동안 출력 메시지의 멀티 바이트 문자가 올바르게 표시되지 않습니다.

Windows 시스템에서 멀티 바이트 문자를 사용하는 로켈(예: 일본어 또는 중국어)로 Access Manager가 설치되는 경우 Access Manager를 구성하는 동안 단말기 창에서 출력 메시지의 단어가 올바르게 표시되지 않습니다.

해결 방법: 없음. 그러나 구성 자체에는 이 문제가 영향을 미치지 않습니다.

CR# 6526940: Windows 시스템에서 영어 이외의 로켈로 패치 5를 설치하는 동안 메시지 텍스트 대신 등록 정보 키가 표시됩니다.

Windows 시스템에서 영어 이외의 로켈로 패치 5(124296-05)를 설치하면 설치 패널의 문자열 일부가 실제 메시지 텍스트가 아닌 등록 정보 키로 표시됩니다. 등록 정보 키의 예로 `PRODUCT_NAME`, `JES_Patch_FinishPanel_Text1` 및 `JES_Patch_FinishPanel_Text2`가 있습니다.

해결 방법: 없음

CR# 6513653: `com.iplanet.am.session.purgedelay` 등록 정보 설정에 문제가 있습니다.

Access Manager `amtune` 스크립트는 가능한 한 많은 Access Manager 세션을 허용하기 위해 `com.iplanet.am.session.purgedelay` 등록 정보를 1로 설정합니다. 이 등록 정보는 세션 제거 작업의 지연 시간(분)을 지정합니다. 그러나 Sun Java System Portal Server와 같은 클라이언트에서는 1 값으로도 충분하지 않을 수 있습니다.

해결 방법: `amtune` 스크립트를 실행한 후 `com.iplanet.am.session.purgedelay` 등록 정보를 다음과 같이 다시 설정합니다.

1. `AMConfig.properties` 파일에서 해당 등록 정보를 새 값으로 설정합니다. 예를 들면 다음과 같습니다.

   ```
   com.iplanet.am.session.purgedelay=5
   ```

2. 새 값을 적용하려면 Access Manager 웹 컨테이너를 다시 시작합니다.

Access Manager 7 2005Q4 패치 4

Access Manager 7 2005Q4 패치 4(개정판 04)에서 해결된 문제는 다음과 같습니다.

- CR# 6463796: `genericHTML`에 대해 `iPlanetAMClientDetection` 서비스를 사용하지 않으면 모든 Access Manager HTML 페이지에 액세스하지 못합니다.
- CR# 6463779: 분산 인증 `amProfile_Client` 및 Access Manager 서버 `amProfile_Server`가 무해한 예외로 채워집니다.
- CR# 6463730: 사이트 간 스크립팅(XSS) 위험성이 `goto` 및 `gx-charset` 매개 변수에 존재합니다.
- CR# 6435889: `RestrictedTokenContext`가 설정되지 않아 `Session.getSession` 메소드가 실행되지 않습니다.

패치 4의 알려진 문제점 및 제한 사항

- 43 페이지 “CR# 6470055: 분산 인증 UI 서버 성능 향상”

- 43 페이지 “CR# 6455079: 비밀번호가 변경되면 비밀번호 재설정 서비스에서 알림 오류를 보고합니다.”

CR# 6470055: 분산 인증 UI 서버 성능 향상

분산 인증 UI 서버 사용자에 대한 사용자 속성 읽기, 검색 및 비교 성능을 향상시키려면 다음 단계를 수행합니다.

1. `Makefile.distAuthUI` 파일에서 응용 프로그램 사용자 이름을 `anonymous`에서 다른 사용자로 변경합니다. 예를 들면 다음과 같습니다.

   ```
   APPLICATION_USERNAME=user1
   ```

2. Directory Server에서 사용자 속성 읽기, 검색 및 비교를 허용할 새로운 사용자(이 예의 경우 `user1`)와 ACI를 추가합니다. 새로운 ACI를 추가하는 예는 다음과 같습니다.

   ```
   dn:ou=1.0,ou=SunAMClientData,ou=ClientData,dc=example,dc=com
   changetype:modify add:aci
   aci: (target="ldap:///ou=1.0,ou=SunAMClientData,ou=ClientData,dc=example,dc=com")
   (targetattr = *")(version 3.0;
   acl "SunAM client data access to a Distributed Auth App User";
   allow (read, search, compare)
   userdn = "ldap:///uid=user1,ou=people,dc=example,dc=com";)
   ```

CR# 6455079: 비밀번호가 변경되면 비밀번호 재설정 서비스에서 알림 오류를 보고합니다.

비밀번호가 변경되면 Access Manager에서 정규화되지 않은 보낸 사람 이름(`Identity-Server`)을 사용하여 전자 메일 알림을 제출하므로 `amPasswordReset` 로그에 오류 항목이 발생합니다. 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: `amPasswordResetModuleMsgs.properties` 파일에서 호스트 서버의 정규화된 도메인 이름을 포함하도록 보낸 사람 주소를 다음과 같이 변경합니다.

1. 보낸 사람 주소 레이블을 변경합니다. 예를 들면 다음과 같습니다.

   ```
   fromAddress.label=<Identity-Server@amhost.example.com>
   ```

2. 잠금 알림에서 올바른 보낸 사람 주소를 사용하도록 지원하기 위해 `lockOutEmailFrom` 등록 정보를 변경합니다. 예를 들면 다음과 같습니다.

   ```
   lockOutEmailFrom=<Identity-Server@amhost.example.com>
   ```

amPasswordResetModuleMsgs.properties 파일은 Solaris 시스템의 경우 *AccessManager-base*/SUNWam/locale 디렉토리에 있으며, Linux 시스템의 경우 *AccessManager-base*/identity/locale 디렉토리에 있습니다.

여기서 *AccessManager-base*는 기본 설치 디렉토리입니다. 기본 설치 디렉토리는 Solaris 시스템의 경우 /opt이며 Linux 시스템의 경우 /opt/sun입니다.

Access Manager 7 2005Q4 패치 3

Access Manager 7 패치 3(개정 03)은 패치에 포함되어 있는 README 파일에 나열된 여러 가지 문제를 해결합니다. 패치 3에는 또한 다음과 같은 새 기능과 알려진 문제가 포함됩니다.

패치 3의 새로운 기능

패치 3의 알려진 문제점 및 제한 사항

- 52 페이지 “CR# 6389564: Access Manager 로그인 중에 LDAP v3 데이터 저장소에서 사용자의 역할 구성원에 대한 성공적인 쿼리가 반복됩니다.”
- 52 페이지 “CR# 6385185: 인증 모듈이 "goto" URL을 무시하고 다른 URL을 지정할 수 있어야 합니다.”
- 52 페이지 “CR# 6385184: SSO 토큰의 상태가 잘못된 경우 사용자 정의 인증 모듈 내에서 리디렉션됩니다. ”
- 53 페이지 “CR# 6324056: 아티팩트 프로필을 사용하면 연합이 실패합니다.”

사이트 모니터링을 위한 새로운 구성 등록 정보

Access Manager 사이트 모니터링 기능은 다음과 같은 새로운 등록 정보를 포함합니다.

등록 정보	설명
`com.sun.identity.sitemonitor.interval`	사이트 모니터링을 위한 간격 시간(밀리초)입니다. 사이트 모니터링 기능은 각 사이트의 가용성을 지정된 시간 간격마다 확인합니다. 기본값: 60,000밀리초(1분).
`com.sun.identity.sitemonitor.timeout`	사이트 가용성 확인을 위한 시간 초과(밀리초)입니다. 사이트 모니터링 기능은 사이트에서 응답을 위해 지정한 제한 시간만큼 대기합니다. 기본값: 5,000밀리초(5초).

이 패치는 이러한 등록 정보를 `AMConfig.properties` 파일에 추가하지 않습니다. 이러한 새로운 등록 정보에 기본값이 아닌 다른 값을 사용하려면 다음과 같이 하십시오.

1. 플랫폼에 따라 다음 위치에 있는 `AMConfig.properties` 파일에 등록 정보와 해당 값을 추가합니다.
   - Solaris 시스템: `/etc/opt/SUNWam/config`
   - Linux 시스템: `/etc/opt/sun/identity/config`

   정책 에이전트에 대해서는 이러한 등록 정보를 `AMAgents.properties` 파일에 추가합니다.
2. 값을 적용하려면 Access Manager 웹 컨테이너를 다시 시작합니다.

사용자 정의 구현. 또한 `com.sun.identity.sitemonitor.SiteStatusCheck` 클래스는 다음의 인터페이스를 사용하여 사이트 가용성 확인을 위한 구현을 사용자 정의할 수 있도록 해 줍니다.

```
package com.iplanet.services.naming.WebtopNaming$SiteStatusCheck
```

각 구현 클래스는 `doCheckSiteStatus` 메소드를 사용해야 합니다.

```
public interface SiteStatusCheck {
public boolean doCheckSiteStatus(URL siteurl);
}
```

Liberty Identity Web Services Framework(ID-WSF) 1.1 지원

Access Manager 7 패치 3의 ID-WSF 기본 버전은 WSF1.1입니다. 샘플에서 새로운 보안 메커니즘을 사용해야 하는 경우에만 ID-WSF를 트리거하기 위해 별도로 구성해야 합니다. ID-WSF1.1을 위한 새로운 보안 메커니즘은 다음과 같습니다.

```
urn:liberty:security:2005-02:null:X509
urn:liberty:security:2005-02:TLS:X509
urn:liberty:security:2005-02:ClientTLS:X509
urn:liberty:security:2005-02:null:SAML
urn:liberty:security:2005-02:TLS:SAML
urn:liberty:security:2005-02:ClientTLS:SAML
urn:liberty:security:2005-02:null:Bearer
urn:liberty:security:2005-02:TLS:Bearer
urn:liberty:security:2005-02:ClientTLS:Bearer
```

Liberty ID-WSF 지원을 위한 새로운 등록 정보

Access Manager가 WSC로 동작할 때 프레임워크가 인바운드 메시지나 리소스 제공에서 확인할 수 없는 경우 `com.sun.identity.liberty.wsf.version` 등록 정보가 Liberty ID-WSF 프레임워크를 확인합니다. 값은 1.0 또는 1.1일 수 있습니다. 기본값은 1.1입니다.

주 패치를 설치하더라도 `com.sun.identity.liberty.wsf.version` 등록 정보가 `AMConfig.properties` 파일에 추가되지는 않습니다(CR# 6458184). 이 새로운 등록 정보를 사용하려면 패치를 설치한 다음 `AMConfig.properties` 파일에 등록 정보와 적절한 값을 추가하고 Access Manager 웹 컨테이너를 다시 시작하십시오.

Access Manager 7 패치 3이 설치되었으면 Solaris 시스템의 기본 디렉토리에 설치된 Access Manager와 함께 표시되는 다음 명령을 실행하여 스키마 변경을 로드합니다.

```
# /opt/SUNWam/bin/amadmin -u amadmin -w amadmin_password
-t /etc/opt/SUNWam/wsf1.1_upgrade.xml
```

ID-WSF 검색 등록에는 등록 시에 이러한 새로운 보안 메커니즘을 사용할 수 있습니다. WSC는 또한 WSP와의 통신에 어떤 버전을 사용할지를 자동으로 검색합니다. ID-WSF1.1을 구성하려면 제품에 포함된 Liberty ID-FF 샘플 및 ID-WSF 샘플의 Readme 파일의 설명을 따르십시오.

CR# 6463779 분산 인증 `amProfile_Client` 로그 및 Access Manager 서버 `amProfile_Server` 로그가 무해한 예외로 채워집니다.

분산 인증 UI를 통한 Access Manager 서버에 대한 요청은 `distAuth/amProfile_Client` 로그 및 Access Manager 서버 `debug/amProfile_Server` 로그에서 예외를 일으킵니다. 다수의 세션을 사용한 다음에는 `amProfile_Client` 로그의 크기는 몇 GB로 증가하고 Access Manager 서버 `amProfile_Server` 로그의 크기는 몇 MB로 증가할 수 있습니다. 로그에 이러한 예외가 기록되는 데 따르는 기능 손실은 없지만 사용자에게 잘못된 경고를 전달할 수 있으며 로그가 하드 디스크 공간을 차지할 수 있습니다.

해결 방법: 로그 파일의 내용이 null인 cron 작업을 실행합니다. 예를 들면 다음과 같습니다.

- 분산 인증 UI 클라이언트 시스템에서 트래픽 분량에 따라 몇 시간마다 "cat /dev/null > distAuth/amProfile_Client"를 실행합니다.
- Access Manager 서버에서는 몇 시간이 아닌 며칠마다 "cat /dev/null > /var/opt/SUNWam/debug/amProfile_Server"를 실행합니다.

CR# 6460974 기본 분산 인증 응용 프로그램 사용자는 amadmin이 아니어야 합니다.

분산 인증 UI 서버를 배포하는 경우 분산 인증 관리자는 amadmin이 아니어야 합니다. Makefile.distAuthUI 파일의 파일 기본 분산 인증 응용 프로그램 사용자는 amadmin이며 distAuth.war 파일이 클라이언트측이 배포된 후에 이어서 AMConfig.properties 파일도 같습니다. amadmin 세션 시간 제한이 지나면 만료되는 AppSSOToken이 있는 amadmin 사용자는 amSecurity 로그 파일(기본적으로 /tmp/distAuth 디렉토리에 있음)에 FATAL ERROR가 발생하는 원인입니다.

해결 방법: UrlAccessAgent를 분산 인증 응용 프로그램 사용자로 지정합니다. 예를 들면 다음과 같습니다.

클라이언트 웹 컨테이너에 distAuth.war 파일을 배포하기 전에 Makefile.distAuthUI 파일에서 다음 매개 변수를 변경합니다.

```
APPLICATION_USERNAME=UrlAccessAgent
APPLICATION_PASSWORD=shared-secret-password 또는 amldapuser-password
```

또는

클라이언트 웹 컨테이너에 distAuth.war 파일을 배포한 다음 각 Access Manager 서버에 대해 AMConfig.properties 파일에서 다음 매개 변수를 변경합니다.

```
com.sun.identity.agents.app.username=UrlAccessAgent
com.iplanet.am.service.password=shared-secret-password 또는 amldapuser-password
```

50 페이지 “CR# 6440697: 분산 인증은 amadmin이 아닌 사용자로 실행해야 합니다.”를 참조하십시오.

CR# 6460576 콘솔 온라인 도움말의 필터링된 역할 아래에 사용자 서비스에 대한 링크가 없습니다.

Access Manager 콘솔 온라인 도움말의 필터링된 역할 아래에 사용자 서비스에 대한 링크가 없습니다. 온라인 도움말에서 목차, 필터링된 역할, "필터링된 역할을 만들려면"으로 차례로 이동합니다. 페이지를 아래로 스크롤하면 선택한 identity 유형에 따라 서비스 목록이 표시되지만 사용자 서비스 링크는 사용할 수 없습니다.

해결 방법: 없음

CR# 6460085 reinstallRTM을 실행하고 웹 응용 프로그램을 다시 배포한 뒤에 WebSphere의 서버에 액세스할 수 없습니다.

DEPLOY_LEVEL=1 배포를 위한 Access Manager 7 패치 3을 Red Hat Linux AS 3.0 업데이트 4의 IBM WebSphere Application Server 5.1.1.6에 적용한 다음 RTM RPM을 복원하기 위해 reinstallRTM 스크립트를 실행하였습니다. reinstallRTM 스크립트에서 생성한 amsilent 파일을 편집한 다음 웹 응용 프로그램이 다시 배포되었습니다. stopServer.sh 및 startServer.sh 스크립트를 사용하여 WebSphere를 다시 시작했지만 로그인 페이지를 액세스하면 WebSphere에 amlcontroller 필터와 관련된 500 오류가 표시됩니다.

이 문제의 원인은 reinstallRTM 스크립트가 생성한 server.xml 파일이 손상되었기 때문입니다.

해결 방법: amconfig 스크립트가 백업한 server.xml 파일은 아직 유효합니다. 다음과 같이 이전의 복사본을 사용합니다.

1. 서버를 중지합니다.
2. 손상된 server.xml을 amconfig 스크립트가 백업한 복사본으로 대체합니다.

   amconfig 스크립트가 백업한 server.xml 파일의 이름은 server.xml-orig-*pid*이며 여기에서 *pid*는 amwas51config 스크립트의 프로세스 ID입니다. 이 파일은 다음 디렉토리에 있습니다.

   WebSphere-home-directory/config/cells/*WebSphere-cell*/nodes/*WebSphere-node*/servers/*server-name*
3. 서버를 다시 시작합니다.

CR# 6455757: 업그레이드 전에 sunISManagerOrganization 표시자 클래스를 조직에 추가해야 합니다.

Access Manager 7 릴리스 전에 생성된 Access Manager DIT 내의 조직에는 sunISManagerOrganization 객체 클래스가 없을 수 있습니다. 또한 Access Manager 이외의 제품으로 만든 조직에도 해당 정의에 sunISManagerOrganization 객체 클래스가 없습니다.

해결 방법: Access Manager 7 2005Q4로 업그레이드하기 전에 DIT 내의 모든 조직의 해당 정의에 sunISManagerOrganization 객체 클래스가 있는지 확인합니다. 필요한 경우 업그레이드하기 전에 이 객체 클래스를 직접 추가합니다.

CR# 6454489: Access Manager 7 2005Q4 패치 2 업그레이드로 인해 콘솔 현재 세션 탭에 오류가 발생합니다.

업그레이드 시에 Access Manager 콘솔의 현재 세션 탭에 다음과 같은 오류가 발생합니다.

지정된 서버에서 유효한 세션을 가져오지 못했습니다.

이 문제는 o=orgname 형식의 루트 접미어가 있는 Access Manager 6 버전에서 업그레이드하는 배포에 해당됩니다.

해결 방법: Manager 7 2005Q4를 설치한 다음 Manager 7 패치 3을 적용하고 amupgrade 스크립트를 실행하여 다음과 같이 데이터를 마이그레이션합니다.

1. Access Manager 6 DIT를 백업합니다.
2. ampre70upgrade 스크립트를 실행합니다.
3. 나중에 구성 옵션을 사용하여 Access Manager 7 2005Q4를 설치합니다.
4. Access Manager 웹 응용 프로그램 배포를 해제합니다.
5. Access Manager 웹 응용 프로그램을 배포합니다.
6. XML/LDIF 변경은 제외하고 Access Manager 7 패치 3을 적용합니다. XML/LDIF 변경은 다음 단계에서 amupgrade 스크립트를 실행한 다음 적용해야 합니다.
7. amupgrade 스크립트를 실행합니다.
8. Access Manager 7 패치 3이 변경되었으므로 Access Manager 웹 응용 프로그램을 다시 배포합니다.
9. Access Manager 콘솔에 액세스합니다.

CR# 6452320: 클라이언트 SDK로 폴링을 사용하면 예외가 발생합니다.

Access Manager 클라이언트 SDK(amclientsdk.jar)를 배포하고 폴링을 사용하도록 설정하면 다음과 같은 오류가 발생할 수 있습니다.

오류: **전송 폴링 오류**:
com.iplanet.am.util.ThreadPoolException:
amSessionPoller **스레드 풀의 작업 대기열이 가득 찼습니다**.

이러한 오류는 분산 인증 UI 서버나 J2EE 에이전트를 배포한 뒤 또는 클라이언트 시스템에서 Access Manager 클라이언트 SDK를 배포한 경우에 발생할 수 있습니다.

해결 방법: 동시 세션이 수백 개 수준인 경우 다음 등록 정보 및 해당 값을 AMConfig.properties 파일 또는 AMAgents.properties 파일에 추가합니다.

```
com.sun.identity.session.polling.threadpool.size=10
com.sun.identity.session.polling.threadpool.threshold=10000
```

수천 또는 수만 개의 세션이 있는 경우에는 이 값을 amtune-identity 스크립트를 실행하고 Access Manager AMConfig.properties 파일에 있는 알림과 같은 값으로 지정해야 합니다. 예를 들어 4GB RAM을 갖춘 시스템에서 Access Manager amtune-identity 스크립트는 다음 값을 지정합니다.

```
com.sun.identity.session.notification.threadpool.size=28
com.sun.identity.session.notification.threadpool.threshold=76288
```

분산 인증 UI 서버 또는 Access Manager 클라이언트 SDK를 4GB RAM을 갖춘 클라이언트 시스템에 배포할 때도 클라이언트측 `AMAgent.properties` 또는 `AMConfig.properties` 파일에 비슷한 값을 설정합니다.

CR# 6442905: 인증된 사용자의 SSOToken이 의도와 다르게 불량 사이트로 유출될 수 있습니다.

인증된 Access Manager 사용자가 불량 사이트에 있는 URL을 클릭하면 의도와 다르게 `SSOToken`이 불량 사이트로 유출될 수 있습니다.

해결 방법: 참가하는 정책 에이전트에 대해 Access Manger에서 항상 고유한 에이전트 사용자 프로필을 만들어 해당 사이트가 불량 사이트인지 확인합니다. 또한 이러한 고유한 에이전트 사용자가 공유 보안 비밀번호 또는 `amldapuser` 비밀번호를 사용하는 일이 없도록 합니다. 기본적으로 정책 에이전트는 Access Manager 응용 프로그램 인증 모듈에 `UrlAccessAgent` 사용자로 인증됩니다.

Access Manager 관리 콘솔을 사용하여 에이전트를 만드는 방법은 **Sun Java System Access Manager 7 2005Q4 관리 설명서**의 "에이전트"를 참조하십시오.

CR# 6441918: 사이트 모니터링 간격 및 시간 제한 등록 정보

Access Manager 사이트 페일오버에 다음과 같은 새로운 등록 정보가 포함됩니다.

```
com.sun.identity.sitemonitor.interval
com.sun.identity.sitemonitor.timeout
```

자세한 내용은 45 페이지 "사이트 모니터링을 위한 새로운 구성 등록 정보"를 참조하십시오.

CR# 6440697: 분산 인증은 amadmin이 아닌 사용자로 실행해야 합니다.

분산 인증 응용 프로그램을 위한 기본 관리 사용자(`amadmin`) 이외의 다른 분산 인증 관리자를 만들려면 다음 절차를 따르십시오.

1. 분산 인증 관리자를 위한 LDAP 사용자를 만듭니다. 예를 들면 다음과 같습니다.

   ```
   uid=DistAuthAdmin,ou=people,o=am
   ```

2. 분산 인증 관리자를 특수 사용자 목록에 추가합니다. 예를 들면 다음과 같습니다.

   ```
   com.sun.identity.authentication.special.users=cn=dsameuser,
   ou=DSAME Users,o=am|cn=amService-UrlAccessAgent,ou=DSAME Users,
   o=am|uid=DistAuthAdmin,ou=People,o=am
   ```

   이 등록 정보를 모든 Access Manager 서버의 `AMConfig.properties` 파일에 추가하여 분산 인증 관리자의 `AppSSOToken`이 세션이 만료될 때 함께 만료되지 않도록 합니다.

CR# 6440695: 로드 밸런서가 있는 분산 인증 UI 서버

여러 분산 인증 UI 서버 앞에 로드 밸런서가 포함된 배포의 경우에는 WAR 파일을 배포한 다음 `AMConfig.properties` 파일에서 다음의 등록 정보를 설정합니다.

```
com.iplanet.am.lbcookie.name=DistAuthLBCookieName
com.iplanet.am.lbcookie.value=DistAuthLBCookieValue
```

CR# 6440651: 쿠키 재생에 `com.sun.identity.session.resetLBCookie` 등록 정보가 필요합니다.

Access Manager 세션 페일오버에 대한 쿠키 재생이 제대로 작동하려면 정책 에이전트와 Access Manager 서버에 대해 모두 `true` 값인 `com.sun.identity.session.resetLBCookie` 등록 정보를 추가합니다. 예를 들면 다음과 같습니다.

```
com.sun.identity.session.resetLBCookie='true'
```

- 정책 에이전트의 경우 `AMAgent.properties` 파일에 해당 등록 정보를 추가합니다.
- Access Manager 서버의 경우 `AMConfig.properties` 파일에 해당 등록 정보를 추가합니다.

주: 이 등록 정보는 Access Manager 세션 페일오버를 구현한 경우에만 필요합니다.

CR# 6440648: `com.iplanet.am.lbcookie.name` 등록 정보는 `amlbcookie`에 기본값을 가정합니다.

기본적으로 정책 에이전트 및 Access Manager 서버는 로드 밸런서 쿠키 이름을 `amlbcookie`라고 가정합니다. 백엔드 서버에서 쿠키 이름을 변경한 경우에는 정책 에이전트에 대한 `AMAgent.properties` 파일에서도 같은 이름을 사용해야 합니다. 또한 Access Manager 클라이언트 SDK를 사용하는 경우에는 여기에도 백엔드 서버에서와 같은 쿠키 이름을 사용해야 합니다.

CR# 6440641: `com.iplanet.am.lbcookie.value` 등록 정보는 더 이상 사용되지 않습니다.

Access Manager는 더 이상 서버에서 로드 밸런서 쿠키를 사용자 정의하는 데 `com.iplanet.am.lbcookie.value` 속성을 지원하지 않습니다. 대신 Access Manager는 이제 쿠키 값 및 에이전트에 의해 재생되는 이름에 대해 세션 구성의 일부로 구성되는 서버 ID를 사용합니다.

CR# 6429610: ID-FF SSO 사용 예에 SSO 토큰을 만들 수 없습니다.

Liberty Identity Federation Framework(ID-FF) 샘플 1을 설정한 뒤에 연합은 성공하지만 SSO는 실패합니다.

해결 방법: dsameuser의 uuid를 AMConfig.properties 파일의 com.sun.identity.authentication.special.users 등록 정보에 추가합니다. 응용 프로그램 인증을 위해서 dsameuser는 Access Manager 서버에 대한 만료되지 않는 SSO 토큰이 필요합니다.

CR# 6389564: Access Manager 로그인 중에 LDAP v3 데이터 저장소에서 사용자의 역할 구성원에 대한 성공적인 쿼리가 반복됩니다.

사용자가 Access Manager로 로그인할 때 사용자의 nsRoleDN 속성에 대한 반복적인 LDAP 검색이 수행됩니다.

해결 방법: Access Manager 7 패치 3이 설치되었으면 Solaris 시스템의 기본 디렉토리에 설치된 Access Manager와 함께 표시되는 다음 명령을 실행합니다.

```
# /opt/SUNWam/bin/amadmin -u amadmin
-w amadmin_password
-t /etc/opt/SUNWam/idRepoServiceAddAttrSchemaRequest_Cache.xml
```

CR# 6385185: 인증 모듈이 "goto" URL을 무시하고 다른 URL을 지정할 수 있어야 합니다.

사용자 상태를 검증하기 위해서 인증 모듈은 "goto" URL을 무시하고 외부 웹 사이트의 다른 URL로 리디렉션할 수 있어야 합니다.

인증이 완료된 뒤에 "goto" URL을 무시하기 위해서는 다음 예의 SSOToken에 표시된 등록 정보를 설정합니다. 이 등록 정보는 AMPostAuthProcessInterface를 구현하는 PostProcess 클래스의 onLoginSuccess 메소드를 사용하여 설정합니다. 예를 들어 *OverridingURL*은 "goto" URL을 무시하는 URL입니다.

```
public class <..> implements AMPostAuthProcessInterface {
...
    public void onLoginSuccess(...) {
        try {
            ssoToken.setProperty("PostProcessSuccessURL", OverridingURL);
         } catch (Exception ...) {
         ...         }
...
}
```

CR# 6385184: SSO 토큰의 상태가 잘못된 경우 사용자 정의 인증 모듈 내에서 리디렉션됩니다.

사용자 정의 인증 모듈을 위한 RedirectCallback은 사용자를 검증하기 위해 인증 UI를 통한 외부 웹 사이트로 리디렉션을 허용합니다. 인증이 성공적인 경우 사용자는 원래의 Access Manager 서버 URL로 리디렉션됩니다. 다음과 같은 샘플 파일이 포함됩니다.

- `LoginModuleSample.java`
- `LoginModuleSample.xml`
- `testExtWebSite.jsp`

이러한 기능을 구현하려면

1. 샘플 `LoginModuleSample.java`를 사용하여 사용자 정의 인증 모듈을 만듭니다.
2. Access Manager 서버로 모듈을 로드합니다.
3. 샘플 `LoginModuleSample.xml`을 사용하여 XML 파일에 `RedirectCallback`을 구성합니다.
4. 모듈을 테스트하려면 외부 웹 사이트로 `testExtWebSite.jsp` 파일을 사용합니다.
5. 다음 URL을 사용하여 로그인합니다.

```
http://example.com/amserver/UI/Login?module=LoginModuleSample
```

사용자 이름 및 비밀번호가 검증을 위해 외부 웹 사이트로 리디렉션됩니다. 이름 및 비밀번호가 유효한 경우 인증이 성공하고 사용자는 원래 Access Manager 서버 URL로 리디렉션됩니다.

예를 들어 배포에서 사용자 정의 인증 모듈을 사용하여 공급/신용카드 사이트에 액세스하는 시나리오에 대해 고려해 보겠습니다.

1. 사용자가 사용자 정의 인증 모듈에 대한 인증 프로세스/로그인 페이지를 호출합니다.
2. 사용자가 자격 증명(사용자 이름 및 비밀번호)을 입력하고 사용자 정의 인증 모듈에 요청을 제출합니다.
3. 사용자 정의 인증 모듈이 요청에 필요한 사용자 정보와 함께 사용자를 외부 공급/신용카드 사이트로 리디렉션합니다.
4. 외부 공급/신용카드 사이트가 사용자 상태를 확인하고 반환된 요청의 일부로 설정되는 성공 또는 실패로 요청을 반환합니다.
5. 사용자 정의 인증 모듈이 4단계에서 반환된 상태에 따라 사용자를 검증하고 해당 상태를 인증 서비스에 반환합니다.
6. 사용자 인증이 성공 또는 실패로 완료됩니다.

CR# 6324056: 아티팩트 프로필을 사용하면 연합이 실패합니다.

해결 방법: 이 문제를 해결하려면 플랫폼에 따라 최신 버전의 "Core Mobile Access" 패치를 적용해야 합니다.

- SPARC 기반 시스템상의 Solaris OS: 119527
- x86 플랫폼에 설치된 Solaris OS: 119528
- Linux 시스템: 119529

패치를 설치한 뒤에 웹 컨테이너를 다시 시작합니다.

Access Manager 7 2005Q4 패치 2

Access Manager 7 2005Q4 패치 2(개정판 02)에서는 패치에 포함된 README 파일에 나열된 대로 많은 문제를 해결했습니다. 패치 2에는 또한 다음과 같은 새로운 기능 및 알려진 문제점이 포함되어 있습니다.

패치 2의 새로운 기능

- 54 페이지 "사용자 관리, Identity 저장소 및 서비스 관리 캐시의 새 등록 정보"
- 56 페이지 "연합 서비스 공급자를 위한 새 등록 정보"
- 56 페이지 "LDAP 필터 조건 지원 "

패치 2의 알려진 문제점 및 제한 사항

- 56 페이지 "CR# 6283582: 로그인 실패 횟수가 Access Manager 인스턴스 간에 공유되지 않습니다."
- 57 페이지 "CR# 6293673: 세션 시간 초과 알림을 보낼 때 원래 세션 정보를 유지해야 합니다."
- 57 페이지 "CR# 6244578: Access Manager는 브라우저 쿠키 지원이 비활성/사용할 수 없을 경우 사용자에게 경고해야 합니다."
- 57 페이지 "CR# 6236892: 로그인 뒤에 CDCServlet이 AuthNResponse를 처리하는 동안 사용할 이미지/텍스트 자리 표시자"
- 58 페이지 "CR# 6363157: 지속 검색이 반드시 필요하지만 새로운 등록 정보로 인해 지속 검색을 사용할 수 없습니다."
- 59 페이지 "CR# 6385696: 기존 및 새로운 IDP 및 SP가 보이지 않습니다."

사용자 관리, Identity 저장소 및 서비스 관리 캐시의 새 등록 정보

패치 2에는 사용자 관리(Access Manager SDK), Identity 저장소(IdRepo) 및 서비스 관리 캐시에 대한 다음과 같은 새로운 등록 정보가 포함되어 있습니다. 이러한 등록 정보를 사용하면 배포 요구 사항에 따라 서로 다른 캐시를 개별적으로 활성화 및 비활성화하고 캐시 항목에 대한 TTL(time to live)을 설정할 수 있습니다.

표 3 사용자 관리, Identity 저장소 및 서비스 관리 캐시의 새 등록 정보

등록 정보	설명
캐시를 활성화 및 비활성화하는 새 등록 정보	
`com.iplanet.am.sdk.caching.enabled`	Identity 저장소(IdRepo), 사용자 관리 및 서비스 관리 캐시를 활성화(true) 또는 비활성화(false)하는 전역 등록 정보입니다. true이거나 등록 정보가 `AMConfig.properties` 파일에 없는 경우 세 개의 캐시가 모두 활성화됩니다.

주 특정 캐시를 활성화 또는 비활성화하는 다음의 세 등록 정보는 이전의 전역 등록 정보가 false로 설정된 경우에만 적용됩니다.

표 3 사용자 관리, Identity 저장소 및 서비스 관리 캐시의 새 등록 정보 *(계속)*

com.sun.identity.amsdk.cache.enabled	사용자 관리(Access Manager SDK) 캐시만 활성화(true) 또는 비활성화(false)합니다.
com.sun.identity.idm.cache.enabled	Identity 저장소(IdRepo) 캐시만 활성화(true) 또는 비활성화(false)합니다.
com.sun.identity.sm.cache.enabled	서비스 관리 캐시만 활성화(true) 또는 비활성화(false)합니다.
TTL의 새 사용자 관리 캐시 등록 정보	
com.iplanet.am.sdk.cache.entry.expire.enabled	사용자 관리 캐시의 만료 시간(다음의 두 등록 정보에 의해 정의됨)을 활성화(true) 또는 비활성화(false)합니다.
com.iplanet.am.sdk.cache.entry.user.expire.time	사용자 관리 캐시의 사용자 항목이 마지막 수정 후 유효한 상태로 유지되는 시간(분)을 지정합니다. 즉, 이 지정된 시간이 경과된 후(마지막 수정 또는 디렉토리에서 읽은 후) 캐시된 항목의 데이터가 만료됩니다. 그런 다음, 이러한 항목의 데이터에 대한 새 요청을 디렉토리에서 읽습니다.
com.iplanet.am.sdk.cache.entry.default.expire.time	사용자 관리 캐시의 비 사용자 항목이 마지막 수정 후 유효한 상태로 유지되는 시간(분)을 지정합니다. 즉, 이 지정된 시간이 경과된 후(마지막 수정 또는 디렉토리에서 읽은 후) 캐시된 항목의 데이터가 만료됩니다. 그런 다음, 이러한 항목의 데이터에 대한 새 요청을 디렉토리에서 읽습니다. TTL의 새 Identity 저장소 캐시 등록 정보
com.sun.identity.idm.cache.entry.expire.enabled	IdRepo 캐시의 만료 시간(다음의 두 등록 정보에 의해 정의됨)을 활성화(true) 또는 비활성화(false)합니다.
com.sun.identity.idm.cache.entry.default.expire.time	IdRepo 캐시의 비 사용자 항목이 마지막 수정 후 유효한 상태로 유지되는 시간(분)을 지정합니다. 즉, 이 지정된 시간이 경과된 후(마지막 수정 또는 저장소에서 읽은 후) 캐시된 항목의 데이터가 만료됩니다. 그런 다음, 이러한 항목의 데이터에 대한 새 요청을 저장소에서 읽습니다.

새 캐싱 등록 정보 사용

Access Manager 7 2005Q4 패치는 새 캐싱 등록 정보를 `AMConfig.properties` 파일에 자동으로 추가하지 않습니다.

새 캐싱 등록 정보를 사용하려면

1. 텍스트 편집기를 사용하여 플랫폼에 따라 다음 디렉토리에 있는 `AMConfig.properties` 파일에 등록 정보 및 값을 추가합니다.

- Solaris 시스템: `/etc/opt/SUNWam/config`
- Linux 시스템: `/etc/opt/sun/identity/config`

2. 값을 적용하려면 Access Manager 웹 컨테이너를 다시 시작합니다.

연합 서비스 공급자를 위한 새 등록 정보

새로운 `com.sun.identity.federation.spadapter` 등록 정보는 서비스 공급자측의 연합 처리 과정에 응용 프로그램별 처리를 추가하는 `com.sun.identity.federation.plugins.FederationSPAdapter`를 위한 구현 클래스를 정의합니다.

59 페이지 “CR# 6385696: 기존 및 새로운 IDP 및 SP가 보이지 않습니다.”를 참조하십시오.

LDAP 필터 조건 지원

패치 2에 LDAP 필터 조건 지원이 추가되었습니다. 정책 관리자는 정책을 정의할 때 조건에 LDAP 필터를 지정할 수 있습니다. 해당 정책은 사용자의 LDAP 항목이 조건에 지정된 LDAP 필터를 충족하는 경우에만 사용자에 적용됩니다. 정책 구성 서비스에 지정된 디렉토리부터 사용자의 LDAP 항목이 조회됩니다.

LDAP 필터 조건을 등록하고 사용하려면 Access Manager 7 패치 2를 설치한 후에 Solaris 시스템의 기본 디렉토리에 설치된 Access Manager와 함께 표시되는 다음 명령을 실행합니다.

```
# /opt/SUNWam/bin/amadmin -u amadmin
-w amadmin_password
-s /etc/opt/SUNWam/AddLDAPFilterCondition.xml
# /opt/SUNWam/bin/amadmin -u amadmin
-w amadmin_password
-t /etc/opt/SUNWam/amPolicyConfig_mod_ldfc.xml
```

패치 5 주 Access Manager 7 2005Q4 패치 5를 추가하고 `updateschema.sh` 스크립트를 실행했으면 `amadmin`을 사용하여 이러한 파일을 로드하지 않아도 됩니다. 자세한 내용은 29 페이지 “새로운 `updateschema.sh` 스크립트로 LDIF 및 XML 파일 로드”를 참조하십시오.

CR# 6283582: 로그인 실패 횟수가 Access Manager 인스턴스 간에 공유되지 않습니다.

Access Manager 7 패치 2가 설치되었으면 Solaris 시스템의 기본 디렉토리에 설치된 Access Manager와 함께 표시되는 다음 명령을 실행합니다.

```
# cd DirectoryServer-base/shared/bin
# ./ldapmodify -h DirectoryServerHost -p DirectoryServerPort
-D "cn=Directory Manager" -w DirectoryMangerPassword
-a -f /etc/opt/SUNWam/accountLockout.ldif
```

```
# /opt/SUNWam/bin/amadmin -u amadmin
-w amadmin_password
-t /etc/opt/SUNWam/accountLockoutData.xml
```

*DirectoryServer-base*의 기본값은 Solaris 시스템에서는 `/var/opt/mps/serverroot`이고 Linux 시스템에서는 `/var/opt/sun/directory-server`입니다.

패치 5 주 Access Manager 7 2005Q4 패치 5를 추가하고 `updateschema.sh` 스크립트를 실행했으면 `amadmin`을 사용하여 이러한 파일을 로드하지 않아도 됩니다. 자세한 내용은 29 페이지 "새로운 `updateschema.sh` 스크립트로 LDIF 및 XML 파일 로드"를 참조하십시오.

CR# 6293673: 세션 시간 초과 알림을 보낼 때 원래 세션 정보를 유지해야 합니다.

`AMConfig.properties` 파일의 새로운 `com.sun.identity.session.property.doNotTrimList` 등록 정보는 쉼표로 분리된 세션 등록 정보 이름을 포함할 수 있습니다. 세션이 시간 초과되면 이 목록에 정의된 등록 정보는 세션이 삭제되기 전에 액세스할 수 있도록 잘리지 않습니다. 예를 들면 다음과 같습니다.

`com.sun.identity.session.property.doNotTrimList=`*UserId*`,`*HostName*

CR# 6244578: Access Manager는 브라우저 쿠키 지원이 비활성/사용할 수 없을 경우 사용자에게 경고해야 합니다.

`AMConfig.properties` 파일의 새로운 `com.sun.identity.am.cookie.check` 등록 정보는 서버가 브라우저의 쿠키 지원/쿠키 활성 여부를 확인할지 여부를 지정합니다. `true` 값을 사용하면 서버는 브라우저에서 쿠키 지원/쿠키 활성 여부를 확인하고 지원하지 않거나 활성화되지 않은 경우 오류 페이지를 표시합니다. 서버가 인증 기능에 쿠키를 사용하지 않는 모드를 지원하는 경우 이 값은 false(기본값)로 설정해야 합니다.

CR# 6236892: 로그인 뒤에 CDCServlet이 AuthNResponse를 처리하는 동안 사용할 이미지/텍스트 자리 표시자

다음과 같은 새로운 등록 정보가 `AMConfig.properties` 파일에 추가되었으며 CDCServlet으로 읽을 수 있습니다.

- `com.iplanet.services.cdc.WaitImage.display`가 true로 설정된 경우 CDSSO 시나리오에서 사용자가 보호된 페이지를 기다리는 동안 브라우저가 이미지를 표시합니다. 기본값은 false입니다.
- `com.iplanet.services.cdc.WaitImage.name`은 이미지 이름을 지정합니다. 기본값은 `waitImage.gif`입니다. 이미지는 `login_images` 디렉토리로 복사됩니다.
- `com.iplanet.services.cdc.WaitImage.width`는 이미지 너비를 지정합니다. 기본값은 420입니다.

- com.iplanet.services.cdc.WaitImage.height는 이미지 높이를 지정합니다. 기본값은 120입니다.

CR# 6363157: 지속 검색이 반드시 필요하지만 새로운 등록 정보로 인해 지속 검색을 사용할 수 없습니다.

AMConfig.properties 파일의 새로운 com.sun.am.event.connection.disable.list 등록 정보는 사용하지 않도록 설정할 이벤트 연결을 지정합니다. 값(대소문자 구분)은 다음과 같을 수 있습니다.

aci - LDAP 필터(aci=*)를 사용하는 검색에서 aci 속성으로의 변경

sm - sunService 또는 sunServiceComponent 표시자 객체 클래스가 있는 객체를 포함하는 Access Manager 정보 트리 또는 서비스 관리 노드에서의 변경. 예를 들어 보호되는 자원에 대한 액세스 권한을 정의하는 정책을 만들거나 기존 정책에 대한 규칙, 주제, 조건 또는 응답 공급자를 수정할 수 있습니다.

um - 사용자 디렉토리 또는 사용자 관리 노드에서의 변경. 예를 들어 사용자의 이름이나 주소를 변경할 수 있습니다.

예를 들어 Access Manager 정보 트리 또는 서비스 관리 노드로의 변경에 대해 지속 검색을 사용할 수 없도록 설정하려면 다음을 수행합니다.

```
com.sun.am.event.connection.disable.list=sm
```

여러 개의 값을 지정하려면 각각의 값을 쉼표로 구분합니다.

주의 – 지속 검색을 수행하면 Directory Server에서 약간의 성능 오버헤드가 발생합니다. 이러한 성능 오버헤드를 일부라도 제거하는 것이 작업 환경에 정말로 중요하다고 생각하면 com.sun.am.event.connection.disable.list 등록 정보를 사용하여 지속 검색을 하나 이상 사용하지 않도록 설정하면 됩니다.

그러나 지속 검색을 사용하지 않도록 설정하기 전에 앞에서 설명한 제한 사항을 반드시 알고 있어야 합니다. 지속 검색을 사용하지 않도록 설정해야 하는 경우를 제외하고는 이 등록 정보를 변경하지 않는 것이 가장 좋습니다. 원래 이 등록 정보는 2.1 J2EE 에이전전트가 여러 개 사용될 때 각 에이전트마다 이러한 지속 검색을 설정하고 있기 때문에 Directory Server에서 발생하는 오버헤드를 피하기 위해 도입되었습니다. 이제는 2.2 J2EE에서 더 이상 이러한 지속 검색을 설정하지 않으므로 이 등록 정보를 사용할 필요가 없습니다.

자세한 내용은 93 페이지 “지속 검색 사용 불가능에 대한 상세 정보 문서화(6486927)”를 참조하십시오.

CR# 6385696: 기존 및 새로운 IDP 및 SP가 보이지 않습니다.

AMConfig.properties 파일의 새로운 com.sun.identity.federation.spadapter 등록 정보는 응용 프로그램이 명제 및 응답 정보를 얻는 위치인 연합 서비스 제공자 어댑터의 기본 구현을 지정합니다. 예를 들면 다음과 같습니다.

```
com.sun.identity.federation.spadapter=com.sun.identity.federation.plugins.FSDefaultSPAdapter
```

Access Manager 7 2005Q4 패치 1

Access Manager 7 2005Q4 패치 1(개정판 01)에서는 패치에 포함된 README 파일에 나열된 대로 많은 문제를 해결했습니다. 패치 1에는 또한 다음과 같은 새로운 기능 및 알려진 문제점이 포함되어 있습니다.

디버그 파일 생성

AMConfig.properties 파일의 com.iplanet.services.debug.level 등록 정보가 error로 설정되어 있더라도 기본적으로 Access Manager 디버그 파일이 디버그 디렉토리에 생성됩니다. Access Manager 7 패치 1 이 릴리스되기 전에는 첫 번째 디버그 메시지가 파일에 기록되는 경우에만 디버그 파일이 생성되었습니다.

LDAPv3 플러그인에서 역할 및 필터링된 역할 지원

Sun Java System Directory Server에 데이터가 저장된 경우 Access Manager 7 패치 1은 LDAPv3 플러그인에서 역할 및 필터링된 역할에 대한 지원을 추가합니다. 자세한 내용은 97 페이지 "LDAPv3 플러그인의 역할 및 필터링된 역할 지원 문제 문서화(6365196)"를 참조하십시오.

CR# 6320475: 서버측 com.iplanet.am.session.client.polling.enable이 true여서는 안 됩니다.

서버측 AMConfig.properties 파일의 com.iplanet.am.session.client.polling.enable 등록 정보는 기본적으로 false이며 true로 재설정되어서는 안 됩니다.

CR# 6358751: 암호화 키에 공백이 삽입되어 있는 경우 Access Manager 7 패치 1 적용이 실패합니다.

비밀번호 암호화 키에 공백이 포함되어 있는 경우 패치 적용이 실패합니다.

해결 방법: 공백을 포함하지 않는 새로운 암호화 키를 사용합니다. 암호화 키를 변경하는 단계에 대한 자세한 설명은**Sun Java System Access Manager 7 2005Q4 Deployment Planning Guide**의 부록 B, "Changing the Password Encryption Key"을 참조하십시오.

이 릴리스의 새로운 기능

Access Manager 패치 릴리스의 새로운 기능에 대한 목록은 9 페이지 "Access Manager 7 2005Q4 패치 릴리스"를 참조하십시오. 최초 릴리스의 Access Manager 7 2005Q4에 포함된 이 릴리스의 새로운 기능은 다음과 같습니다.

Access Manager 모드

Access Manager 7 2005Q4는 영역 모드 및 레거시 모드를 포함합니다. 두 모드는 다음을 지원합니다.

- Access Manager 7 2005Q4의 새로운 기능
- 다음과 같은 제한을 제외한 Access Manager 6 2005Q1 기능
  - 영역이 생성되면 해당 조직은 Sun Java System Directory Server에 생성되지 않습니다.
  - 새 Access Manager 7 2005Q4 콘솔에서는 CoS(Class of Service) 템플리트 우선 순위를 설정할 수 없습니다. 81 페이지 "새 Access Manager 콘솔에서 CoS 템플리트 우선 순위를 설정할 수 없습니다(6309262)."를 참조하십시오.
- Sun Java System Directory Server 및 다른 데이터 저장소의 Identity 저장소

다음의 경우 레거시 모드가 필요합니다.

- Sun Java System Portal Server

- Messaging Server, Calendar Server, Instant Messaging 또는 Delegated Administrator를 포함한 Sun Java System Communications Services 서버
- Access Manager 6 2005Q1 및 Access Manager 7 2005Q4가 동일한 Directory Server에 액세스할 때의 동시 배포

새 Access Manager 콘솔

Access Manager 콘솔은 이번 릴리스에서 다시 설계되었습니다. 그러나 Access Manager를 Portal Server, Messaging Server, Calendar Server, Instant Messaging 또는 Delegated Administrator와 함께 배포하는 경우 Access Manager를 레거시 모드로 설치하고 Access Manager 6 2005Q1 콘솔을 사용해야 합니다.

자세한 내용은 67 페이지 "호환성 문제"를 참조하십시오.

Identity 저장소

Access Manager Identity 저장소는 사용자, 그룹 및 역할 등을 식별하는 데 필요한 정보를 포함합니다. Access Manager나 Sun Java System Identity Manager 등의 다른 프로비저닝 제품을 사용하여 Identity 저장소를 만들고 유지 관리할 수 있습니다.

현재 릴리스에서 Identity 저장소는 Sun Java System Directory Server 또는 Microsoft Active Directory에 있을 수 있습니다. Access Manager는 Identity 저장소에 대한 읽기/쓰기 권한 또는 읽기 전용 권한을 가질 수 있습니다.

Access Manager 정보 트리

Access Manager 정보 트리는 시스템 액세스에 관한 정보를 포함합니다. Access Manager의 각 인스턴스는 Sun Java System Directory Server에 개별적으로 정보 트리를 만들고 유지 관리합니다. Access Manager 정보 트리는 어떤 이름(접미사)이든지 가질 수 있습니다. Access Manager 정보 트리에는 다음 절에서 설명하는 영역을 포함합니다(필요한 경우 하위 영역 포함).

Access Manager 영역

영역 및 모든 하위 영역은 Access Manager 정보 트리의 일부이며 일련의 사용자 및/또는 그룹, 사용자가 인증하는 방법, 사용자가 액세스할 수 있는 자원, 사용자에게 자원에 대한 권한이 부여된 후 응용 프로그램에서 사용할 수 있는 정보를 정의하는 구성 정보를 포함할 수 있습니다. 영역 또는 하위 영역은 국제화 구성, 비밀번호 재설정 구성, 세션 구성, 콘솔 구성 및 사용자 기본 설정 등의 기타 구성 정보도 포함할 수 있습니다. 영역 또는 하위 설정은 비워둘 수 있습니다.

Access Manager 콘솔이나 `amadmin` CLI 유틸리티를 사용하여 영역을 만들 수 있습니다. 자세한 내용은 콘솔 온라인 도움말 또는 **Sun Java System Access Manager 7 2005Q4 관리 설명서**의 14 장, "amadmin 명령줄 도구"를 참조하십시오.

세션 페일오버 변경 사항

Access Manager는 통신 브로커로 Sun Java System Message Queue(Message Queue)를 사용하고 세션 저장소 데이터베이스로 Sleepycat Software, Inc.의 Berkeley DB를 사용하는 웹 컨테이너 독립 세션 페일오버 구현을 제공합니다. Access Manager 7 2005Q4의 향상된 기능에는 세션 페일오버 환경을 구성하는 `amsfoconfig` 스크립트와 Message Queue 브로커 및 Berkeley DB 클라이언트를 시작하고 중지시키는 `amsfo` 스크립트가 포함됩니다.

자세한 내용은 **Sun Java System Access Manager 7 2005Q4 Deployment Planning Guide**의 "Implementing Access Manager Session Failover"을 참조하십시오.

세션 등록 정보 변경 알림

세션 등록 정보 변경 알림 기능을 사용하면 특정 세션 등록 정보가 변경되었을 때 Access Manager가 알림 메시지를 특정 listener로 전송할 수 있습니다. 이 기능은 Access Manager 관리자 콘솔에서 "등록 정보 변경 알림 사용 가능" 속성이 설정된 경우 적용됩니다. 예를 들어, 단일 사인온(SSO) 환경에서는 하나의 Access Manager 세션을 여러 응용 프로그램에서 공유할 수 있습니다. "알림 등록 정보" 목록에 정의된 특정 세션 등록 정보에 변경이 발생한 경우 Access Manager는 모든 등록된 listener에 알림을 전송합니다.

자세한 내용은 **Sun Java System Access Manager 7 2005Q4 Deployment Planning Guide**의 "Enabling Session Property Change Notifications"을 참조하십시오.

세션 할당량 제약 조건

세션 할당량 제약 조건 기능을 사용하면 Access Manager 관리자(`amadmin`)가 "활성 사용자 세션" 속성을 설정하여 사용자에게 허용되는 최대 동시 세션 수를 제한할 수 있습니다. 관리자는 모든 사용자 또는 하나 이상의 특정 사용자에만 적용되는 조직, 영역, 역할이나 사용자와 같은 엔터티에 대해 전역 수준에서 세션 할당량을 설정할 수 있습니다.

기본적으로 세션 할당량 제약 조건은 사용 불가(OFF)로 설정되어 있지만 관리자는 Access Manager 관리자 콘솔의 "할당량 제약 조건 사용 가능" 속성을 설정하여 사용 가능하게 할 수 있습니다.

또한 관리자는 "세션 할당량이 모두 사용된 경우의 결과 동작" 속성을 설정하여 세션 제약 조건 할당량을 모두 사용한 경우 수행할 동작을 구성할 수 있습니다.

- DENY_ACCESS. Access Manager가 새 세션에 대한 로그인 요청을 거부합니다.
- DESTROY_OLD_SESSION. Access Manager가 동일한 사용자에 대해 다음에 만료되는 기존 세션을 삭제하고 새 로그인 요청이 성공적으로 수행되도록 합니다.

"제약 조건 검사에서 최상위 관리자 제외" 속성은 "최상위 수준 관리자 역할"을 가진 관리자에게 세션 제약 조건 할당량이 적용되는지 여부를 지정합니다.

자세한 내용은 **Sun Java System Access Manager 7 2005Q4 Deployment Planning Guide**의 "Setting Session Quota Constraints"을 참조하십시오.

분산 인증

Access Manager 7 2005Q4에는 배포된 두 방화벽을 통한 안전한 분산 인증을 제공하는 원격 인증 UI 구성 요소인 분산 인증 UI가 포함되어 있습니다. 분산 인증 UI 구성 요소가 없으면 Access Manager 서비스 URL이 최종 사용자에게 노출될 수 있습니다. 이러한 노출 문제는 프록시 서버를 사용하여 막을 수도 있지만 배포 상태에 따라 프록시 서버가 적절한 해결책이 되지 못할 수도 있습니다.

분산 인증 UI 구성 요소는 Access Manager가 배포된 비보안(DMZ) 계층에 속한 하나 이상의 서버에 설치됩니다. 분산 인증 UI 서버는 Access Manager를 실행하지 않으며 웹 브라우저를 통해 최종 사용자에게 인증 인터페이스를 제공하기 위한 목적으로만 존재합니다.

최종 사용자가 HTTP 요청을 분산 인증 UI에 보내면 그에 대한 응답으로 사용자에게 로그인 페이지를 표시합니다. 그 다음 분산 인증 구성 요소가 두 번째 방화벽을 통해 사용자의 요청을 Access Manager 서버에 전송하므로 최종 사용자와 Access Manager 서버 사이의 방화벽에서 틈이 생기는 것을 차단해줍니다.

자세한 내용은 **Technical Note: Using Access Manager Distributed Authentication**을 참조하십시오.

복수 인증 모듈 인스턴스 지원

모든 인증 모듈(초기 상태)은 콘솔 UI 지원을 사용하여 하위 스키마를 지원하도록 확장됩니다. 복수 인증 모듈 인스턴스는 각 모듈 유형(모듈 클래스가 로드된 상태)에 대해 만들 수 있습니다. 예를 들어 LDAP 모듈 유형에 대해 이름이 `ldap1` 및 `ldap2`인 인스턴스의 경우 각 인스턴스는 서로 다른 LDAP 디렉토리 서버를 가리킬 수 있습니다. 유형과 같은 이름을 가진 모듈 인스턴스는 역방향 호환성이 지원됩니다. 호출 형식은 다음과 같습니다.

server_deploy_uri`/UI/Login?module=`*module-instance-name*

인증"명명된 구성"또는"연결"이름 공간

조직/영역에 별도의 이름 공간이 생성되어 인증 모듈 인스턴스들의 체인 역할을 합니다. 동일한 체인을 조직/영역, 역할 또는 사용자에 재사용 및 할당할 수 있습니다. 인증 서비스 인스턴스는 인증 체인과 같으며호출 형식은 다음과 같습니다.

server_deploy_uri`/UI/Login?service=`*authentication-chain-name*

정책 모듈 향상

개인화 속성

규칙, 주제 및 조건 외에도, 정책은 이제 개인화 속성(IDResponseProvider)을 가질 수 있습니다. 정책 평가에서 클라이언트로 전송된 정책 결정은 이제 정책 기반 응답 개인화 속성을 적용 가능한 정책에 포함합니다. 두 가지 유형의 개인화 속성이 지원됩니다.

- 정적 속성. 사용자가 정책에 속성 이름과 값을 정의합니다.
- 동적 속성. 사용자가 정책에 속성 이름을 나열하고 값은 정책 평가 시 Identity 저장소의 데이터 저장소에서 불러옵니다.

Policy Enforcement Points(에이전트)는 보통 이런 속성 값을 HTTP 헤더나 쿠키 또는 요청 속성으로 보호된 응용 프로그램에 전달합니다.

Access Manager 7 2005Q4는 고객에 의한 응답 공급자 인터페이스의 사용자 정의 구현을 지원하지 않습니다.

세션 등록 정보 조건

세션 정책 조건 구현(SessionPropertyCondition)은 사용자의 Access Manager 세션에서 등록 정보 설정 값을 기반으로 요청에 정책을 적용할 수 있는지 여부를 결정합니다. 정책 평가 시, 조건은 사용자 Access Manager 세션이 조건에 정의된 모든 등록 정보 값을 갖는 경우에만 "true"를 반환합니다. 조건에서 여러 값으로 정의된 등록 정보의 경우 사용자 세션에 해당 조건에 있는 등록 정보에 대해 나열된 값이 최소 하나 이상 있으면 됩니다.

정책 주제

정책 주제 구현(Access Manager Identity 주제)은 사용자가 구성된 Identity 저장소에 있는 항목을 정책 주제 값으로 사용할 수 있게 합니다.

정책 내보내기

amadmin 명령을 사용하여 정책을 XML 형식으로 내보낼 수 있습니다. amAdmin.dtd 파일의 새로운 GetPolices 및 RealmGetPolicies 요소가 이 기능을 지원합니다.

정책 상태

이제 정책은 활성 또는 비활성으로 설정할 수 있는 상태 속성을 갖게 되었습니다. 비활성 정책은 정책 평가 중에 무시됩니다.

사이트 구성

Access Manager 7 2005Q4는 Access Manager 배포를 위한 중앙 구성 관리를 제공하는 "사이트 개념"을 도입했습니다. Access Manager가 사이트로 구성되면 클라이언트 요청은 항상 클라이언트와 백엔드 Access Manager 서버 사이의 방화벽과 같은 문제점을 해결하고 배포를 단순화시키는 로드 밸런서를 통과하게 됩니다.

자세한 내용은 **Sun Java System Access Manager 7 2005Q4 Deployment Planning Guide**의 "Configuring an Access Manager Deployment as a Site"을 참조하십시오.

대량 연합

Access Manager 7 2005Q4는 비즈니스 파트너로 아웃소싱할 응용 프로그램에 사용자 계정의 대량 연합을 제공합니다. 이전에는 서비스 공급자(SP)와 Identity 공급자(IDP) 간의 계정 연합 시 사용자가 SP와 IDP 사이트를 모두 방문하여 계정이 없는 경우 계정을 만들고 두 계정을 웹 링크를 통해 연합해야 했습니다. 이 과정은 많은 시간이 소요되었습니다. 또한 기존 계정을 이용한 배포나 Identity 공급자 자체로 동작하는 사이트 또는 인증 공급자로 파트너 중 하나를 사용하는 사이트에 대해 이 과정이 항상 적합한 것은 아니었습니다.

자세한 내용은 **Sun Java System Access Manager 7 2005Q4 Federation and SAML Administration Guide**를 참조하십시오.

로깅 향상

Access Manager 7 2005Q4는 여러 가지 새롭게 향상된 로깅 기능을 포함합니다.

- 새 필드(또는 열): `MessageID` 필드는 로깅된 이벤트에 대한 메시지 식별자를 포함합니다. `ContextID` 필드는 세션 식별자와 유사하고 특정 사용자 로그인 세션에 대한 모든 이벤트에 적용되는 컨텍스트 식별자를 포함합니다. 사용자의 특정 로그인 세션의 경우 로깅된 이벤트에 대해 모든 로그 파일에서 `ContextID`가 동일하게 됩니다.
- 로깅 API. API에는 DB로 로깅이 설정된 경우 데이터베이스(DB)로부터 읽기를 포함한 로그 레코드 읽기용 추가 기능이 포함됩니다. 플랫 파일 또는 DB 테이블 저장소에서 로그 레코드의 검색을 보여주는 `/opt/SUNWam/samples/logging` 디렉토리의 `LogReaderSample.java`를 참조하십시오.

주의 – 보통 데이터베이스 테이블은 플랫 파일 로그보다 큽니다. 따라서 데이터의 양이 많으면 Access Manager 서버의 모든 자원을 소비할 수 있으므로 해당 요청에서 데이터베이스 테이블의 모든 레코드를 검색하지 마십시오.

하드웨어 및 소프트웨어 요구 사항

다음 표는 이 릴리스에 필요한 하드웨어 및 소프트웨어를 보여 줍니다.

표 4 하드웨어 및 소프트웨어 요구 사항

구성 요소	요구 사항
운영 체제(OS)	SPARC™ 기반 Solaris OS 시스템 버전 8, 9 및 10(Solaris 10의 전체 루트 로컬 영역 지원 포함)
	x86 플랫폼의 Solaris OS 버전 9 및 10(Solaris 10의 전체 루트 로컬 영역 지원 포함)
	AMD64 플랫폼의 Solaris OS 버전 10(전체 루트 로컬 영역 지원 포함)
	Red Hat™ Linux, WS/AS/ES 2.1 업데이트 6 이상
	Red Hat Linux, WS/AS/ES 3.0
	Red Hat Linux, WS/AS/ES 3.0 업데이트 1, 2, 3 및 4
	HP-UX OS. Sun Java Enterprise System 2005Q4 Document Collection for HP-UX를 참조하십시오. http://docs.sun.com/coll/1258.2
	Windows OS. Sun Java Enterprise System 2005Q4 Document Collection for Microsoft Windows를 참조하십시오. http://docs.sun.com/coll/1259.2
Java 2 Standard Edition(J2SE)	J2SE 플랫폼 1.5.0_04, 1.5_01, 1.5 및 1.4.2
Directory Server	Access Manager 정보 트리: Sun Java System Directory Server 5 2005Q4
	Access Manager Identity 저장소: Sun Java System Directory Server 5 2005Q4 또는 Microsoft Active Directory
웹 컨테이너	Sun Java System Web Server 6.1 2005Q4 SP5
	Sun Java System Application Server Enterprise Edition 8.1 2005Q2
	BEA WebLogic Server 8.1 SP4
	IBM WebSphere Application Server 5.1 및 5.1.1(관련 누적 수정본 포함)
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 2005Q4 릴리스에서 지원하는 브라우저를 보여 줍니다.

표 5 지원하는 브라우저

브라우저	플랫폼
Microsoft Internet Explorer™ 5.5 SP2	Windows™ 2000
Microsoft Internet Explorer 6.0	Windows 2000
	Windows XP
Mozilla 1.7.1	Solaris OS 버전 9 및 10
	Java Desktop System
	Windows 2000
	Red Hat Linux 8.0
Netscape™ 7.0	Solaris OS 버전 9 및 10
	Java Desktop System
	Windows 2000
	Red Hat Linux 8.0

시스템 가상화 지원

시스템 가상화는 공유 하드웨어에서 여러 운영 체제(OS) 인스턴스를 독립적으로 실행할 수 있게 해주는 기술입니다. 기능적으로 가상화된 환경에서 호스팅되는 OS에 배포된 소프트웨어는 대개 기본 플랫폼이 가상화되었는 사실을 인식하지 못합니다. Sun은 시스템 가상화 및 OS가 조합된 엄선된 환경에서 Sun Java System 제품 테스트를 수행하여 Sun Java System 제품이 적절한 크기로 구성된 가상화 환경에서도 가상화되지 않은 시스템에서와 마찬가지로 문제없이 작동되는지 검증합니다. 가상화된 환경에서 Sun Java System 제품에 대한 Sun의 지원에 대한 자세한 내용은 http://docs.sun.com/doc/820-4651을 참조하십시오.

호환성 문제

- 68 페이지 “Access Manager 레거시 모드”
- 69 페이지 “Access Manager 정책 에이전트”

Access Manager 레거시 모드

다음 제품과 함께 Access Manager를 설치하는 경우 Access Manager Legacy(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 Legacy(6.x) 모드를 선택합니다.

- 68 페이지 "상태 파일을 사용한 Java ES 자동 설치"
- 68 페이지 "그래픽 모드의 "지금 구성" 설치 옵션"
- 68 페이지 "텍스트 기반 모드의 "지금 구성" 설치 옵션"
- 69 페이지 ""나중에 구성" 설치 옵션"

Access Manager 7 2005Q4 설치 결정에 대한 보다 자세한 내용은 69 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 Manage를 선택하려면 상태 파일에서 다음 매개 변수(다른 매개 변수 포함)를 설정한 후 자동 모드로 설치 프로그램을 실행합니다.

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

상태 파일을 사용하여 자동 모드로 Java ES 설치 프로그램을 실행하는 방법은 **Sun Java Enterprise System 2005Q4 설치 설명서**의 5 장, "자동 모드로 설치"를 참조하십시오.

그래픽 모드의 "지금 구성" 설치 옵션

"Access Manager의 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. Legacy(6.x) 모드를 선택하려면 구성 스크립트 입력 파일(`amsamplesilent`)에서 다음 매개 변수를 설정합니다.

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

Windows 시스템의 경우 구성 파일은 *AccessManager-base*`\setup\AMConfigurator.properties`입니다.

`amconfig` 스크립트를 실행하여 Access Manager를 구성하는 방법은 **Sun Java System Access Manager 7 2005Q4 관리 설명서**를 참조하십시오.

Access Manager 모드 결정

실행 중인 Access Manager 7 2005Q4 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 2005Q4 모드에 대한 정책 에이전트의 호환성을 보여 줍니다.

표 6 Access Manager 7 2005Q4 에 대한 정책 에이전트의 호환성

에이전트 및 버전	호환 모드
웹 및 J2EE 에이전트, 버전 2.2	레거시 및 영역 모드
웹 에이전트, 버전 2.1	레거시 및 영역 모드
J2EE 에이전트, 버전 2.1	레거시 모드만

설치 정보

Access Manager 설치 노트는 다음 정보를 포함합니다.

알려진 문제점 및 제한 사항

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

호환성 문제

Java ES 2004Q2 서버 및 Java ES 2005Q4의 IM 간의 비호환성(6309082)

다음과 같은 배포 시나리오에서 이 문제가 발생합니다.

- server-1: Java ES 2004Q2: Directory Server

- server-2: Java ES 2004Q2: Application Server, Access Manager 및 Portal Server
- server-3: Java ES 2004Q2: Calendar Server 및 Messaging Server
- server-4: Java ES 2005Q4: Application Server, Instant Messaging 및 Access Manager SDK

`imconfig` 유틸리티를 실행하여 server-4에서 Instant Messaging을 구성하는 경우 구성에 실패합니다. server-4에서 Instant Messaging(IM)이 사용하는 Access Manager 7 2005Q4 SDK는 Java ES 2004Q2 릴리스와 호환되지 않습니다.

해결 방법: 원칙적으로 Access Manager 서버와 Access Manager SDK는 동일한 릴리스여야 합니다. 자세한 내용은 **Sun Java Enterprise System 2005Q4 업그레이드 설명서**를 참조하십시오.

레거시 모드에 대한 핵심 인증 모듈의 비호환성(6305840)

Access Manager 7 2005Q4 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 2005Q4 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.

"조직에 프로필이 없음"으로 인해 에이전트가 로그인할 수 없습니다(6295074).

Access Manager 콘솔에서 영역 모드로 에이전트를 만듭니다. 로그아웃한 후 해당 에이전트 이름으로 다시 로그인할 경우 에이전트가 해당 영역에 액세스할 권한이 없으므로 Access Manager는 오류를 반환합니다.

해결 방법: 권한을 수정하여 해당 에이전트에 대해 읽기/쓰기 권한을 부여합니다.

Delegated Administrator의 `commadmin` 유틸리티가 사용자를 만들지 않습니다(6294603).

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

해결 방법: Access Manager를 버전 7 2005Q4로 업그레이드했지만 Delegated Administrator는 업그레이드하지 않은 경우 이 문제가 발생합니다. Delegated Administrator를 업그레이드하는 방법은 **Sun Java Enterprise System 2005Q4 업그레이드 설명서**를 참조하십시오.

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 Administrator commadmin 유틸리티가 조직을 만들지 않습니다(6292104).

Delegated Administrator commadmin 유틸리티와 -S mail,cal 옵션을 사용하면 조직을 만들지 않습니다.

해결 방법: 이전 문제에 대한 해결 방법을 참조하십시오.

설치 문제

패치 1 적용 후 /tmp/amsilent 파일이 모든 사용자의 읽기 액세스를 허용합니다(6370691).

패치 1을 적용한 후 /tmp/amsilent 파일이 모든 사용자의 읽기 액세스를 허용합니다.

해결 방법: 패치를 적용한 후 Access Manager 관리자에게만 읽기 액세스가 허용되도록 파일의 사용 권한을 재설정합니다.

컨테이너 구성을 사용한 SDK 설치에서 알림 URL이 올바르지 않습니다(6327845).

컨테이너 구성을 사용하여 SDK 설치를 수행하는 경우(DEPLOY_LEVEL=4) 알림 URL이 올바르지 않습니다.

해결 방법:

1. `AMConfig.properties` 파일에서 다음 등록 정보를 설정합니다.

   ```
   com.iplanet.am.notification.url=
   protocol://fqdn:port/amserver/servlet/com.iplanet.services.comm.client.
   PLLNotificationServlet
   ```

2. Access Manager를 다시 시작하여 새 값을 적용합니다.

Access Manager `classpath`가 만료된 JCE 1.2.1 패키지를 참조합니다(6297949).

Access Manager `classpath`가 2005년 7월 27일에 만료되는 Java Cryptography Extension(JCE) 1.2.1 패키지(서명 인증서)를 참조합니다(6297949).

해결 방법: 없음. `classpath`에 패키지 참조가 있더라도 Access Manager는 이 패키지를 사용하지 않습니다.

기존 DIT에 Access Manager를 설치하면 Directory Server 인덱스를 다시 생성해야 합니다(6268096).

검색 성능을 향상시키기 위해 Directory Server는 여러 가지 새 인덱스를 가지고 있습니다.

해결 방법: 기존 DIT(디렉토리 정보 트리)에 Access Manager를 설치한 후 `db2index.pl` 스크립트를 실행하여 Directory Server 인덱스를 다시 생성합니다. 예를 들면 다음과 같습니다.

```
# ./db2index.pl -D "cn=Directory Manager" -w password -n userRoot
```

`db2index.pl` 스크립트는 *DS-install-directory*/*slapd-hostname*/ 디렉토리에서 사용할 수 있습니다.

루트가 아닌 사용자에 대한 디렉토리 로그 및 디버그 권한이 잘못되었습니다(6257161).

자동 설치 구성 파일에 루트가 아닌 사용자를 지정한 경우 디렉토리 디버그, 로그 및 시작에 대한 권한이 적절하게 설정되지 않습니다.

해결 방법: 이러한 디렉토리에 루트가 아닌 사용자가 액세스할 수 있도록 권한을 변경합니다.

Access Manager와 Directory Server가 각각 다른 시스템에 설치된 경우 인증 서비스가 초기화되지 않습니다(6229897).

`classpath` 및 기타 Access Manager 웹 컨테이너 환경 변수가 설치 과정에서 업데이트되어도 설치 과정이 웹 컨테이너를 재시작하지 않습니다. 설치가 끝나고 웹 컨테이너가 재시작되기 전에 Access Manager에 로그인하려고 하면 다음 오류 메시지가 반환됩니다.

인증 서비스가 초기화되지 않았습니다.
시스템 관리자에게 문의하십시오.

해결 방법: 먼저 웹 컨테이너를 재시작한 후 Access Manager에 로그인하십시오. 또한 Directory Server도 로그인 전에 실행되어야 합니다.

설치 프로그램이 기존 디렉토리 설치에 대해 플랫폼 항목을 추가하지 않습니다(6202902).

Java ES 설치 프로그램이 기존 디렉토리 서버 설치에 대해 플랫폼 항목을 추가하지 않습니다(DIRECTORY_MODE=2).

해결 방법: 영역/DNS 별칭과 플랫폼 서버 목록 항목을 수동으로 추가합니다. 관련 단계는 **Sun Java System Access Manager 7 2005Q4 Deployment Planning Guide**의 "Adding Additional Instances to the Platform Server List and Realm/DNS Aliases"를 참조하십시오.

업그레이드 문제

Access Manager ampre70upgrade 스크립트가 현지화 패키지를 제거하지 않습니다(6378444).

Access Manager를 Access Manager 7 2005Q4로 업그레이드하는 경우 ampre70upgrade 스크립트가 시스템에 있는 현지화된 Access Manager 패키지를 제거하지 않습니다.

해결 방법: Access Manager 7 2005Q4로 업그레이드하기 전에 pkgrm 명령을 사용하여 시스템에 설치되어 있는 현지화된 모든 Access Manager 패키지를 수동으로 제거합니다.

AMConfig.properties 파일이 웹 컨테이너에 대해 이전 버전입니다(6316833).

Access Manager와 Application Server가 Java ES 2005Q4 버전으로 업그레이드된 후 Access Manager AMConfig.properties 파일에 Application Server의 이전 버전이 있습니다.

해결 방법: Delegated Administrator 구성 프로그램(config-commda)을 실행하기 전에 AMConfig.properties 파일에서 다음 등록 정보를 변경합니다.

```
com.sun.identity.webcontainer=IAS8.1
```

노드 에이전트 server.policy파일이 Access Manager 업그레이드 일부로 업데이트되지 않았습니다(6313416).

Access Manager를 업그레이드한 후 노드 에이전트 server.policy 파일이 업데이트되지 않았습니다.

해결 방법: 해당 노드 에이전트에 대한 server.policy 파일을 다음 파일로 바꿉니다.

```
/var/opt/SUNWappserver/domains/domain1/config/server.policy
```

업그레이드 후 세션 등록 정보 조건이 조건 목록에 없습니다(6309785).

Access Manager를 버전 2005Q1에서 버전2005Q4로 업그레이드한 후 조건을 정책에 추가하려고 시도하는 경우 세션 등록 정보 조건이 정책 조건 목록에 선택 항목으로 표시되지 않습니다.

해결 방법: 정책 구성 서비스 템플리트에서 해당 영역의 세션 등록 정보 조건 유형을 선택합니다.

업그레이드 후 Identity 주제 유형이 정책 주제 목록에 없습니다(6304617).

Access Manager를 버전 2005Q1에서 버전 2005Q4로 업그레이드한 후 Identity 주제, 새로 추가된 정책 주제 유형이 정책 주제 목록에 선택 항목으로 표시되지 않습니다.

해결 방법: 정책 구성 서비스 템플리트에서 Identity 주제 유형을 기본 주제 유형으로 선택합니다.

classpath가 마이그레이션되지 않아 Access Manager 업그레이드에 실패했습니다(6284595).

Access Manager를 Java ES 2004Q2에서 Java ES 2005Q4로 업그레이드하는 동안 Java ES 2004Q2에서 Java ES 2005Q1로의 업그레이드에 실패했습니다. Access Manager가 Application Server에 배포되고 있었으며, Application Server도 Java ES 2004Q2에서 Java ES 2005Q4로 업그레이드되고 있었습니다. `domain.xml` 파일의 `classpath`에서 Access Manager JAR 파일 경로를 포함하지 않았습니다.

해결 방법: 다음 단계를 따르십시오.

1. `comm_dssetup.pl` 스크립트에 문제가 있으므로 `amupgrade` 스크립트를 실행하기 전에 Directory Server의 인덱스를 다시 만듭니다.
2. Access Manager에 대한 항목을 노드 에이전트의 `server.policy` 파일에 추가합니다. 기본 서버 정책(`/var/opt/SUNWappserver/domains/domain1/config/server.policy`)의 `server.policy` 복사본이면 충분합니다.
3. 노드 에이전트의 `domain.xml` 파일에 있는 `classpath`를 다음과 같이 업데이트합니다. `server.xml` 파일의 `java-config` 요소에 대한 `server-classpath` 속성에서 `classpath-suffix`와 관련 `classpath`를 `domain.xml`의 `java-config` 요소에 있는 해당 속성으로 복사합니다. `java-config` 요소는 `domain.xml`의 `config` 요소 아래에 있습니다.

업그레이드 후 amadmin 명령이 잘못된 버전을 반환합니다(6283758).

Access Manager를 버전 6 2005Q1에서 버전 7 2005Q4로 업그레이드한 후 `amadmin --version` 명령이 잘못된 Sun Java System Access Manager 버전 2005Q1을 반환했습니다.

해결 방법: Access Manager를 업그레이드한 후 `amconfig` 스크립트를 실행하여 Access Manager를 구성합니다. `amconfig`를 실행할 때 구성(`amsamplesilent`) 파일에 대해 전체 경로를 지정합니다. 예를 들어 Solaris 시스템의 경우 다음과 같습니다.

```
# ./amconfig -s ./config-file
```

또는

```
# ./amconfig -s /opt/SUNWam/bin/config-file
```

데이터 마이그레이션 후 ContainerDefaultTemplateRole 속성이 추가됩니다(4677779).

사용자 역할은 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.

구성 문제

기본이 아닌 URI를 사용하는 경우 Application Server 8.1 `server.policy` 파일을 편집해야 합니다(6309759).

Application Server 8.1에 Access Manager 7 2005Q4를 배포 중이고 기본 URI 값으로 각각 `amserver`, `amconsole` 및 `ampassword`를 사용하는 서비스, 콘솔 및 비밀번호 웹 응용 프로그램에 대해 기본이 아닌 URI를 사용 중인 경우 웹 브라우저를 통해 Access Manager로 액세스를 시도하기 전에 응용 프로그램 서버 도메인의 `server.policy` 파일을 편집해야 합니다.

해결 방법: `server.policy` 파일을 다음과 같이 편집합니다.

1. Access Manager를 배포할 Application Server 인스턴스를 중지합니다.
2. `/config` 디렉토리로 변경합니다. 예를 들면 다음과 같습니다.

   ```
   cd /var/opt/SUNWappserver/domains/domain1/config
   ```

3. `server.policy` 파일의 백업 복사본을 만듭니다. 예를 들면 다음과 같습니다.

   ```
   cp server.policy server.policy.orig
   ```

4. server.policy 파일에서 다음 정책을 찾습니다.

```
grant codeBase "file:\${com.sun.aas.instanceRoot}/
applications/j2ee-modules/amserver/-" { ...
};
grant codeBase "file:\${com.sun.aas.instanceRoot}/
applications/j2ee-modules/amconsole/-" { ...
};
grant codeBase "file:\${com.sun.aas.instanceRoot}/
applications/j2ee-modules/ampassword/-" { ...
};
```

5. 다음 행에서 amserver를 서비스 웹 응용 프로그램에 사용되는 기본이 아닌 URI로 바꿉니다.

```
grant codeBase "file:\${com.sun.aas.instanceRoot}/
applications/j2ee-modules/amserver/-" {
```

6. 레거시 모드 설치의 경우 다음 행에서 amconsole을 콘솔 웹 응용 프로그램에 사용되는 기본이 아닌 URI로 바꿉니다.

```
grant codeBase "file:\${com.sun.aas.instanceRoot}/
applications/j2ee-modules/amconsole/-" {
```

7. 다음 행에서 ampassword를 비밀번호 웹 응용 프로그램에 사용되는 기본이 아닌 URI로 바꿉니다.

```
grant codeBase "file:\${com.sun.aas.instanceRoot}/
applications/j2ee-modules/ampassword/-" {
```

8. Access Manager를 배포할 Application Server 인스턴스를 시작합니다.

플랫폼 서버 목록 및 FQDN 별칭 속성이 업데이트되지 않았습니다(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. 관련 단계는 **Sun Java System Access Manager 7 2005Q4 Deployment Planning Guide**의 "Adding Additional Instances to the Platform Server List and Realm/DNS Aliases"를 참조하십시오.

서비스의 필수 속성에 대한 데이터 검증(6308653)

Access Manager 7 2005Q4에서는 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 2005Q4를 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 패치 JAR의 경로를 Access Manager 웹 응용 프로그램을 배포 및 배포 해제하는 데 사용되는 `classpath`를 포함하는 변수인 `wl8_classpath` 앞에 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 않습니다(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. 관련 단계는 **Sun Java System Access Manager 7 2005Q4 Deployment Planning Guide**의 "Adding Additional Instances to the Platform Server List and Realm/DNS Aliases"를 참조하십시오.

구성 상태 파일 템플리트의 기본 Access Manager 모드가 realm입니다(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
```

RSA 키를 사용하는 경우 IBM WebSphere에서 URL 서명에 실패합니다(6271087).

IBM WebSphere에서 RSA 키를 사용하는 경우 URL 문자열의 서명에 실패하고 다음 예외가 나타납니다.

```
ERROR: FSSignatureUtil.signAndReturnQueryString: FSSignatureException
occured while signing query string: no such provider: SunRsaSign
```

해결 방법: "SunRsaSign" 공급자가 WebSphere 번들 JDK에 없습니다. 이 문제를 해결하려면 *websphere_jdk_root*/jre/lib/security/java.security 파일을 편집하고 다음 줄을 추가하여 "SunRsaSign"을 공급자 중 하나로 사용합니다.

```
security.provider.6=com.sun.rsajca.Provider
```

Access Manager 콘솔 문제

SAML의 경우 신뢰할 수 있는 파트너 복제 콘솔 편집 오류(6326634)

Access Manager 콘솔의 연합 > SAML 탭에서 SAML 신뢰할 수 있는 파트너를 만듭니다. 신뢰할 수 있는 파트너의 복제를 시도하면 오류가 발생합니다.

해결 방법: 없음. 패치 1에서 이 문제가 해결되었습니다. 해당 플랫폼에 패치를 적용하는 방법에 대해서는 59 페이지 "Access Manager 7 2005Q4 패치 1"을 참조하십시오.

원격 로깅이 amConsole.access 및 amPasswordReset.access에 대해 작동하지 않습니다(6311786).

원격 로깅이 구성된 경우 amConsole.access 및 amPasswordReset.access를 제외한 비밀번호 재설정 정보에 대한 모든 로그가 원격 Access Manager 인스턴스에 기록됩니다. 로그 레코드는 어디에도 기록되지 않습니다.

해결 방법: 없음.

콘솔에서 많은 amadmin 등록 정보를 추가하면 amadmin 사용자 비밀번호가 변경됩니다(6309830).

관리 콘솔에서 amadmin 사용자에 대한 일부 등록 정보를 추가 또는 편집하면 amadmin 사용자 비밀번호가 변경됩니다.

해결 방법: 없음. 패치 1에서 이 문제가 해결되었습니다. 해당 플랫폼에 패치를 적용하는 방법에 대해서는 59 페이지 "Access Manager 7 2005Q4 패치 1"을 참조하십시오.

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

새 Access Manager 7 2005Q4 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.

정책 관리자로 그룹을 사용자에 추가하는 중 예외 오류가 발생합니다(6299543).

정책 관리자로 그룹을 사용자에 추가할 때 Access Manager 콘솔이 예외 오류를 반환합니다.

해결 방법: 없음.

레거시 모드에서 역할의 모든 사용자를 삭제할 수 없습니다(6293758).

레거시 모드에서 역할의 모든 사용자를 삭제하려고 해도 한 사용자가 남아 있습니다.

해결 방법: 역할에서 해당 사용자를 다시 삭제합니다.

검색 서비스 자원 오퍼링을 추가, 삭제 또는 수정할 수 없습니다(6273148).

Access Manager 관리 콘솔에서 사용자, 역할 또는 영역에 대한 자원 오퍼링을 추가, 삭제 또는 수정할 수 없습니다.

해결 방법: 없음. 패치 1에서 이 문제가 해결되었습니다. 해당 플랫폼에 패치를 적용하는 방법에 대해서는 59 페이지 "Access Manager 7 2005Q4 패치 1"을 참조하십시오.

주제 검색에 대해 LDAP 바인드 비밀번호가 잘못된 경우 오류가 발생해야 합니다(6241241).

잘못된 LDAP 바인드 비밀번호가 사용된 경우 Access Manager 관리 콘솔이 오류를 반환하지 않습니다.

해결 방법: 없음.

Access Manager가 레거시 모드에서 컨테이너에 조직을 만들 수 없습니다(6290720).

컨테이너를 만든 후 컨테이너에 조직을 만들면 Access Manager가 "고유성 위반 오류"를 반환합니다.

해결 방법: 없음.

Portal Server 관련 서비스를 추가할 때 이전 콘솔이 나타납니다(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 않습니다(6239724).

Directory Server를 설치한 후 기존 DIT 옵션으로 Access Manager를 설치합니다. Access Manager 콘솔에 로그인하여 그룹을 만듭니다. 그룹에서 사용자를 편집합니다. 예를 들어 필터 `uid=*999*`를 사용하여 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.

SDK 및 클라이언트 문제

- 83 페이지 "하위 영역에 대한 세션 서비스 구성을 제거할 수 없습니다(6318296)."
- 83 페이지 "정책 조건이 지정된 경우 CDC 서블릿이 잘못된 로그인 페이지로 리디렉션됩니다(6311985)."
- 83 페이지 "서버가 다시 시작된 후 클라이언트가 알림을 가져오지 않습니다(6309161)."

하위 영역에 대한 세션 서비스 구성을 제거할 수 없습니다(6318296).

최상위 영역의 하위 영역을 만들고 여기에 세션 서비스를 추가한 후, 세션 서비스의 구성을 연속해서 제거하려고 하면 오류 메시지가 발생합니다.

해결 방법: 기본 최상위 ID 저장소인 AMSDK1을 제거한 후 이 저장소를 다시 구성에 추가합니다.

패치 1에서 이 문제가 해결되었습니다. 해당 플랫폼에 패치를 적용하는 방법에 대해서는 59 페이지 “Access Manager 7 2005Q4 패치 1”을 참조하십시오.

정책 조건이 지정된 경우 CDC 서블릿이 잘못된 로그인 페이지로 리디렉션됩니다(6311985).

CDSSO 모드의 Apache 에이전트 2.2의 경우, 에이전트가 보호된 자원에 액세스할 때 CDC 서블릿이 사용자를 기본 로그인 페이지가 아닌 익명 인증 페이지로 리디렉션합니다.

해결 방법: 없음. 패치 1에서 이 문제가 해결되었습니다. 해당 플랫폼에 패치를 적용하는 방법에 대해서는 59 페이지 “Access Manager 7 2005Q4 패치 1”을 참조하십시오.

서버가 다시 시작된 후 클라이언트가 알림을 가져오지 않습니다(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 합니다(6292616).

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

해결 방법: 서비스 스키마를 변경한 후 클라이언트를 다시 시작합니다.

패치 1에서 이 문제가 해결되었습니다. 해당 플랫폼에 패치를 적용하는 방법에 대해서는 59 페이지 “Access Manager 7 2005Q4 패치 1”을 참조하십시오.

명령줄 유틸리티 문제

- 84 페이지 “Internet Explorer 6.0에서 이스케이프 문자를 사용하여 XML 문서를 저장할 수 없습니다(4995100).”

Access Manager가 Directory Proxy를 가리키는 경우 Null 속성 LDAP 검색 시 오류를 반환합니다(6357975).

Sun Java System Directory Proxy Server를 사용하는 경우 null 속성 LDAP 검색 시 오류를 반환합니다. 예를 들면 다음과 같습니다.

```
# ldapsearch -b base-dn uid=user ""
```

Access Manager가 LDAP 디렉토리 서버를 직접 가리키는 경우 같은 검색을 수행하면 성공합니다.

해결 방법: Directory Proxy Server를 사용하는 경우 null 속성 검색을 사용하도록 설정하거나 검색 시 속성 이름을 제공합니다.

amserveradmin 스크립트에 새 스키마 파일이 없습니다(6255110).

설치 후 `amserveradmin` 스크립트를 실행하여 서비스를 Directory Server에 로드해야 하는 경우 `defaultDelegationPolicies.xml` 및 `idRepoDefaults.xml` 스키마 파일에 해당 스크립트가 없습니다.

해결 방법: `amadmin` CLI 도구에 `-t` 옵션을 사용하여 `defaultDelegationPolicies.xml` 및 `idRepoDefaults.xml` 파일을 수동으로 로드합니다.

Internet Explorer 6.0에서 이스케이프 문자를 사용하여 XML 문서를 저장할 수 없습니다(4995100).

XML 파일에 특수 문자(예: “&” 다음에 “amp;” 문자열)를 추가하는 경우 파일은 제대로 저장되지만 Internet Explorer 6.0을 사용하여 나중에 XML 프로필을 검색하면 파일이 제대로 표시되지 않습니다. 프로필을 다시 저장하면 오류가 반환됩니다.

해결 방법: 없음.

인증 문제

- 85 페이지 “`UrlAccessAgent` SSO 토큰이 만료됩니다(6327691). ”
- 85 페이지 “비밀번호 수정 후 LDAPV3 플러그인/동적 프로필을 이용한 하위 영역에 로그인할 수 없습니다(6309097).”
- 85 페이지 “레거시(호환) 모드에 대한 통계 서비스의 Access Manager 기본 구성 비호환성(6286628)”
- 85 페이지 “이름 지정 속성의 최상위 조직에서 속성 고유성이 잘못됨(6204537)”

UrlAccessAgent SSO 토큰이 만료됩니다(6327691).

응용 프로그램 모듈에서 특수 사용자 DN을 반환하지 않아서 해당 특수 사용자 DN이 일치하여 만료되지 않은 토큰이 실패하므로 UrlAccessAgent SSO 토큰이 만료됩니다.

해결 방법: 없음. 패치 1에서 이 문제가 해결되었습니다. 해당 플랫폼에 패치를 적용하는 방법에 대해서는 59 페이지 "Access Manager 7 2005Q4 패치 1"을 참조하십시오.

비밀번호 수정 후 LDAPV3 플러그인/동적 프로필을 이용한 하위 영역에 로그인할 수 없습니다(6309097).

영역 모드에서 영역에 "잘못된" 비밀번호로 ldapv3 데이터 저장소를 만들고 나중에 비밀번호를 amadmin으로 변경하면 변경된 비밀번호를 가진 사용자로 로그인을 시도할 때 로그온에 실패하고 프로필이 없다는 메시지가 나타납니다.

해결 방법: 없음.

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/debug에서 /var/opt/SUNWam/stats로 변경됩니다.

해결 방법: 없음.

이름 지정 속성의 최상위 조직에서 속성 고유성이 잘못됨(6204537)

Access Manager 설치 후 amadmin으로 로그인한 후 o, sunPreferredDomain, associatedDomain, sunOrganizationAlias, uid 및 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 메시지를 무시하십시오. Access Manager가 제대로 작동 중입니다.

세션 및 SSO 문제

- 86 페이지 "여러 시간대의 Access Manager 인스턴스에서 다른 사용자 세션이 시간 초과됩니다(6323639)."

- 86 페이지 “세션 페일오버(amsfoconfig) 스크립트가 Linux 2.1에 대한 잘못된 권한을 가지고 있습니다(6298433).”
- 86 페이지 “Linux 2.1 시스템에서 세션 페일오버(amsfoconfig) 스크립트가 실패합니다(6298462).”
- 86 페이지 “로드 밸런서가 SSL 종료를 포함하는 경우 시스템이 잘못된 서비스 호스트 이름을 만듭니다(6245660).”
- 87 페이지 “타사 웹 컨테이너와 함께 HttpSession 사용(CR 번호 없음)”

여러 시간대의 Access Manager 인스턴스에서 다른 사용자 세션이 시간 초과됩니다(6323639).

다른 시간대에 동일한 신뢰 구간에 설치된 Access Manager 인스턴스로 인해 사용자 세션 시간이 초과됩니다.

세션 페일오버(amsfoconfig) 스크립트가 Linux 2.1에 대한 잘못된 권한을 가지고 있습니다(6298433).

세션 페일오버 구성 스크립트(/opt/sun/identity/bin/amsfoconfig)가 잘못된 권한을 가지고 있어서 Linux 2.1 시스템에서 실행되지 않습니다.

해결 방법: amsfoconfig 스크립트가 실행 가능하도록 권한을 변경합니다(예: 755).

패치 1에서 이 문제가 해결되었습니다. 해당 플랫폼에 패치를 적용하는 방법에 대해서는 59 페이지 “Access Manager 7 2005Q4 패치 1”을 참조하십시오.

Linux 2.1 시스템에서 세션 페일오버(amsfoconfig) 스크립트가 실패합니다(6298462).

탭 문자(\t)가 제대로 해석되지 않아 Linux 2.1 서버에서 세션 페일오버 구성 스크립트(amsfoconfig)가 실패합니다.

해결 방법: 세션 페일오버를 수동으로 구성합니다. 관련 단계는 **Sun Java System Access Manager 7 2005Q4 Deployment Planning Guide**의 “Configuring Session Failover Manually”을 참조하십시오.

패치 1에서 이 문제가 해결되었습니다. 해당 플랫폼에 패치를 적용하는 방법에 대해서는 59 페이지 “Access Manager 7 2005Q4 패치 1”을 참조하십시오.

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

Access Manager가 SSL 종료를 포함하는 로드 밸런서를 사용하여 웹 컨테이너로 Web Server에 배포된 경우 클라이언트에게 정확한 Web Server 페이지가 표시되지 않습니다. 잘못된 호스트 때문에 Access Manager 콘솔의 세션 탭을 클릭하면 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 함께 HttpSession 사용(CR 번호 없음)

인증에 대해 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

정책 구성 서비스에서 동적 속성을 삭제하면 정책 편집에 문제가 발생합니다(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."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

Access Manager 시작 시 디버그 오류가 발생합니다(6309274, 6308646).

Access Manager 7 2005Q4 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.

BEA WebLogic Server를 웹 컨테이너로 사용

BEA WebLogic Server를 웹 컨테이너로 사용하여 Access Manager를 배포하는 경우 Access Manager 액세스가 불가능할 수 있습니다.

해결 방법: WebLogic Server를 다시 시작하여 Access Manager에 액세스 가능하도록 만듭니다.

Linux OS 문제

Application Server에서 Access Manager를 실행하는 경우 JVM 문제가 발생합니다(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 Server서버를 시작하는 데 사용할 콘솔에서 `ulimit` 명령을 실행합니다. 예를 들면 다음과 같습니다.

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

연합 및 SAML 문제

웹 서비스 샘플을 실행하면 “자원 오퍼링을 찾을 수 없습니다”라는 메시지가 나타납니다(6359900).

Solaris 시스템의 경우 *AccessManager-base*/SUNWam/samples/phase2/wsc 디렉토리 또는 Linux 시스템의 경우 *AccessManager-base*/identity/samples/phase2/wsc 디렉토리에 있는 웹 서비스 샘플에 액세스하도록 Access Manager를 구성한 경우 검색 서비스에 쿼리를 입력하거나 자원 오퍼링을 수정하면 "자원 오퍼링을 찾을 수 없습니다."라는 오류 메시지가 반환됩니다.

여기서 *AccessManager-base*는 기본 설치 디렉토리입니다. 기본 설치 디렉토리는 Solaris 시스템의 경우 /opt이며 Linux 시스템의 경우 /opt/sun입니다.

해결 방법:

1. 다음 샘플 디렉토리로 이동합니다. Solaris 시스템의 경우 *AccessManager-base*/SUNWam/samples/phase2/wsc) 디렉토리 또는 Linux 시스템의 경우 *AccessManager-base*/identity/samples/phase2/wsc 디렉토리
2. index.jsp 파일에서 다음 문자열을 찾습니다.

   ```
   com.sun.org.apache.xml.security.utils.XMLUtils.outputDOM
   ```

3. 이전 단계에서 찾은 문자열이 포함된 줄 바로 앞에 다음 줄을 새로 삽입합니다.

   ```
   com.sun.org.apache.xml.security.Init.init();
   ```

4. 샘플을 다시 실행합니다. (Access Manager는 재시작할 필요가 없습니다.)

아티팩트 프로필 사용 중에 연합이 실패합니다(6324056).

Identity 공급자(IDP) 및 서비스 공급자(SP)를 설치한 경우 통신 프로토콜을 브라우저의 아티팩트 프로필을 사용하도록 변경한 후 IDP와 SP 간의 사용자 연합을 시도하면 연합이 실패합니다.

해결 방법: 없음.

SAML 명령문에 있는 특수 문자(&)는 인코딩되어야 합니다(6321128).

원본 사이트와 대상 사이트로 Access Manager를 사용하고 SSO가 구성된 경우 SAML 명령문에 있는 특수 문자(&)가 인코딩되지 않아 명제의 구문 분석에 실패하여 대상 사이트에서 오류가 발생합니다.

해결 방법: 없음. 패치 1에서 이 문제가 해결되었습니다. 해당 플랫폼에 패치를 적용하는 방법에 대해서는 59 페이지 “Access Manager 7 2005Q4 패치 1”을 참조하십시오.

역할에 검색 서비스를 추가하는 중 예외가 발생합니다(6313437).

Access Manager 콘솔에서 검색 서비스에 자원 오퍼링을 추가하는 경우 알 수 없는 예외가 발생합니다.

해결 방법: 없음.

다른 속성을 구성 및 저장할 때까지 인증 컨텍스트 속성을 구성할 수 없습니다(6301338).

다른 속성을 구성 및 저장할 때까지 인증 컨텍스트 속성을 구성할 수 없습니다.

해결 방법: 인증 컨텍스트 속성을 구성하기 전에 공급자 프로필을 구성 및 저장합니다.

루트 접미사에 “&”문자가 있는 경우 EP 샘플이 작동하지 않습니다(6300163).

Directory Server에 “&” 문자를 포함하는 루트 접미사가 있고 사원 프로필 서비스 자원 오퍼링을 추가하는 경우 예외가 발생합니다.

해결 방법: 없음.

연합에서 로그아웃 오류가 발생합니다(6291744).

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

해결 방법: 없음.

국제화(g11n) 문제

사용자 로켈 기본 설정이 전체 관리 콘솔에 적용되지 않습니다(6326734).

Access Manager 관리자 콘솔 중 일부가 사용자 로켈 기본 설정을 따르지 않고 브라우저의 로켈 설정을 사용합니다. 이 문제는 버전 및 온라인 도움말의 내용뿐만 아니라 버전, 로그아웃 및 온라인 도움말 버튼에 영향을 줍니다.

해결 방법: 브라우저 설정을 사용자 기본 설정과 동일한 로켈로 변경합니다.

Access Manager가 IBM WebSphere에 배포된 경우 유럽어에 대한 완전한 온라인 도움말을 사용할 수 없습니다(6325024).

모든 유럽 로켈(스페인어, 독일어, 프랑스어)에서 Access Manager가 IBM WebSphere Application Server 인스턴스에 배포된 경우 온라인 도움말에 완전히 액세스할 수 없습니다. 온라인 도움말은 다음 프레임에 대해 "응용 프로그램 오류"를 표시합니다.

- 도움말 및 닫기 버튼이 표시되는 상위 프레임.
- 목차, 색인 및 검색 버튼이 표시되는 왼쪽 프레임.

해결 방법: 브라우저 언어 설정을 영어로 설정한 후 왼쪽 프레임에 액세스하는 페이지를 새로 고칩니다. 그러나 상위 프레임은 여전히 "응용 프로그램 오류"를표시합니다.

Access Manager가 IBM WebSphere에 배포된 경우 버전 정보가 비어 있습니다(6319796).

모든 로켈에서 Access Manager가 IBM WebSphere Application Server에 배포된 경우 버전 버튼을 눌러도 제품 버전을 볼 수 없습니다. 대신 빈 페이지가 표시됩니다.

해결 방법: 없음.

클라이언트 검색에서 UTF-8 제거가 작동하지 않습니다(5028779).

클라이언트 검색 기능이 제대로 작동하지 않습니다. Access Manager 7 2005Q4 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 클릭합니다.
  2. `genericHTML`의 **편집** 링크를 클릭합니다.
  3. HTML 탭에서 `genericHTML` 링크를 클릭합니다.
  4. 문자 집합 목록에 다음 항목을 입력합니다: `UTF-8;q=0.5`(UTF-8 q 팩터가 해당 로켈의 다른 문자 집합보다 낮은지 확인합니다.)

5. 저장, 로그아웃 후 다시 로그인합니다.

로그 파일에 멀티 바이트 문자가 물음표로 표시됩니다(5014120).

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

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

설명서 문제

영역 모드에서 레거시 모드로 되돌릴 수 없는 Access Manager 문제 문서화(6508473)

Access Manager 7 2005Q4를 영역 모드로 설치하는 경우 레거시 모드로 되돌릴 수 없습니다.

그러나 Access Manager 7 2005Q4를 레거시 모드로 설치하는 경우에는 -M 옵션을 포함한 amadmin 명령으로 영역 모드로 변경할 수 있습니다. 예를 들면 다음과 같습니다.

```
amadmin -u cn=amAdmin,ou=People,dc=example,dc=com -w amadmin-password -M
dc=example,dc=com
```

지속 검색 사용 불가능에 대한 상세 정보 문서화(6486927)

Access Manager에서는 지속 검색을 통해 Sun Java System Directory Server 변경 항목에 대한 정보를 받습니다. Access Manager는 기본적으로 서버 시작 시 다음과 같은 지속 검색 연결을 만듭니다.

`aci` - LDAP 필터(`aci=*`)를 사용하는 검색에서 `aci` 속성으로의 변경

`sm` - `sunService` 또는 `sunServiceComponent` 표시자 객체 클래스가 있는 객체를 포함하는 Access Manager 정보 트리 또는 서비스 관리 노드에서의 변경. 예를 들어 보호되는 자원에 대한 액세스 권한을 정의하는 정책을 만들거나 기존 정책에 대한 규칙, 주제, 조건 또는 응답 공급자를 수정할 수 있습니다.

`um` - 사용자 디렉토리 또는 사용자 관리 노드에서의 변경. 예를 들어 사용자의 이름이나 주소를 변경할 수 있습니다.

주의 – 지속 검색이 사용되지 않는 구성 요소는 Directory Server로부터 알림을 받지 않기 때문에 이러한 구성 요소에 대해 지속 검색을 사용하지 않도록 설정하는 것은 권장되지 않습니다. 따라서 Directory Server에서 수행된 특정 구성 요소에 대한 변경 알림이 구성 요소 캐시로 전달되지 않아 해당 구성 요소 캐시의 기능이 상실하게 됩니다.

예를 들어 사용자 디렉토리(`um`)에서 발생되는 변경 항목에 대한 지속 검색을 사용할 수 없으면 Access Manager 서버는 Directory Server에서 알림을 받지 않습니다. 그 결과로 에이전트는 사용자 속성의 새 값으로 로컬 사용자 캐시를 업데이트하기 위한 알림을 Access Manager로부터 가져오지 않습니다. 다음으로 응용 프로그램이 에이전트에 사용자 속성을 쿼리하면 해당 속성의 이전 값을 받을 수도 있습니다.

이 등록 정보는 반드시 필요한 특별한 경우에만 사용하십시오. 예를 들어 작업 환경에서 세션 서비스 및 인증 서비스와 같은 서비스 중 하나로 값을 변경하는 것과 관련된 서비스 구성 변경이 발생하지 않을 것이라고 확신하는 경우 서비스 관리(`sm`) 구성 요소에 대한 지속 검색을 사용하지 않도록 설정할 수 있습니다. 그러나 어떤 서비스에 대한 변경이 발생되면 서버를 다시 시작해야 합니다. `aci` 및 `um` 값으로 지정되는 동일한 조건이 다른 지속 검색에도 적용됩니다.

자세한 내용은 58 페이지 “CR# 6363157: 지속 검색이 반드시 필요하지만 새로운 등록 정보로 인해 지속 검색을 사용할 수 없습니다.”를 참조하십시오.

Access Manager 지원 및 비지원 권한 문제 문서화(2143066)

권한은 영역 내에 존재하는 역할이나 그룹의 구성원인 관리자에게 부여되는 액세스 권한을 정의합니다. Access Manager를 사용하면 다음과 같은 관리자 유형을 위한 권한을 구성할 수 있습니다.

- 영역 관리자는 아이디 저장소(데이터 저장소) 정의, 인증 구성 및 정책 정의를 포함하여 영역 관련 작업을 모두 수행할 수 있습니다.
- 정책 관리자는 기존 영역에서 정책을 구성할 수 있습니다.

지원되는 권한은 다음과 같습니다.

- 모든 영역 및 정책 등록 정보에 대한 읽기 및 쓰기 권한. 영역 관리자를 위한 읽기 및 쓰기 권한을 정의합니다.
- 정책 등록 정보에 대해서만 읽기 및 쓰기 권한. 정책 관리자를 위한 읽기 및 쓰기 권한을 정의합니다.
- 지원되는 권한 조합: 정책 등록 정보에 대해서만 읽기 및 쓰기 권한 및 데이터 저장소에 대한 읽기 권한. 그 밖의 권한 조합은 지원되지 않습니다.

쿠키 기반 지속 요청 라우팅 문제 문서화(6476922)

Access Manager 서버가 로드 밸런서 배후에 배포되는 경우 쿠키 기반 지속 요청 라우팅은 클라이언트 요청에서 올바르지 않은 Access Manager 서버, 즉 세션을 호스트하고 있지 않은 서버로 경로를 잘못 지정하지 않도록 합니다. 이 기능은 Access Manager 7 2005Q4 패치 3에서 구현되었습니다.

쿠키 기반 지속 요청 라우팅을 사용하지 않는 이전 동작에서는 종종 브라우저 기반이 아닌 클라이언트(예: 원격 Access Manager 클라이언트 SDK를 사용하는 정책 에이전트 및 클라이언트) 요청에서 세션을 호스트하고 있지 않은 Access Manager 서버로 경로를 잘못 지정했습니다. 그런 다음에는 올바른 서버로 요청을 보내기 위해 Access Manager 서버에서 백 채널 통신을 사용하여 해당 세션을 검증해야 했으며, 이로 인해 대개의 경우 성능이 어느 정도 저하되었습니다. 쿠키 기반 지속 요청 라우팅을 사용하면 이러한 백 채널 통신이 필요하지 않으므로 Access Manager 성능을 향상시킵니다.

쿠키 기반 지속 요청 라우팅을 구현하려면 배포된 Access Manager가 사이트로 구성되어야 합니다. 자세한 내용은 **Sun Java System Access Manager 7 2005Q4 Deployment Planning Guide**의 "Configuring an Access Manager Deployment as a Site"을 참조하십시오.

쿠키 기반 지속 요청 라우팅을 구성하려면

1. `AMConfig.properties` 파일에 `com.iplanet.am.lbcookie.name` 등록 정보를 설정하여 쿠키 이름을 지정합니다. 그런 다음 Access Manager에서 2바이트 서버 아이디(예: 01, 02 및 03)를 사용하여 로드 밸런서 쿠키 값을 생성합니다. 쿠키 이름을 지정하지 않으면 Access Manager에서 기본 이름(`amlbcookie`)과 2바이트 서버 아이디를 사용하여 로드 밸런서 쿠키 값을 생성합니다.

   Access Manager에서 쿠키 이름을 설정하는 경우 정책 에이전트에 대한 `AMAgent.properties` 파일에서도 동일한 이름을 사용해야 합니다. 또한 Access Manager 클라이언트 SDK를 사용하는 경우에도 Access Manager 서버에서 사용되는 것과 동일한 쿠키 이름을 사용해야 합니다.

   주: Access Manager에서 2바이트 서버 아이디를 사용하여 쿠키 값을 설정하므로 `com.iplanet.am.lbcookie.value` 등록 정보는 설정하지 마십시오.

2. 1단계의 쿠키 이름으로 로드 밸런서를 구성합니다. 배포된 Access Manager와 함께 하드웨어 또는 소프트웨어 로드 밸런서를 사용할 수 있습니다.
3. 세션 페일오버가 구현되는 경우 정책 에이전트 및 Access Manager 서버 모두에 대해 `com.sun.identity.session.resetLBCookie` 등록 정보를 사용하도록 설정합니다.
   - 정책 에이전트의 경우 `AMAgent.properties` 파일에 해당 등록 정보를 추가하여 사용하도록 설정합니다.
   - Access Manager 서버의 경우 `AMConfig.properties` 파일에 해당 등록 정보를 추가하여 사용하도록 설정합니다.

   예를 들면 다음과 같습니다.

   ```
   com.sun.identity.session.resetLBCookie='true'
   ```

   페일오버 상황이 발생하면 해당 세션이 보조 Access Manager 서버의 경로로 지정되고 로드 밸런서 쿠키 값이 보조 Access Manager 서버의 서버 아이디를 사용하여 설정됩니다. 그런 후에 이어지는 해당 세션에 대한 요청은 모두 보조 Access Manager 서버의 경로로 지정됩니다.

Windows 2003을 위한 Windows 데스크탑 SSO 구성 문제 문서화(6487361)

Windows 2003에서 Windows 데스크탑 SSO를 구성하려면 다음 `ktpass` 명령을 사용합니다. 자세한 내용은 **Sun Java System Access Manager 7 2005Q4 관리 설명서**의 "Windows 데스크탑 SSO 구성"을 참조하십시오.

```
ktpass /out filename /mapuser username
/princ HTTP/hostname.domainname /crypto encryptiontype /rndpass
/ptype principaltype /target domainname
```

예를 들면 다음과 같습니다.

```
ktpass /out demo.HTTP.keytab
/mapuser http /princ HTTP/demo.identity.sun.com@IDENTITY.SUN.COM
/crypto RC4-HMAC-NT /rndpass /ptype KRB5_NT_PRINCIPAL /target IDENTITY.SUN.COM
```

구문 정의에 대해서는 다음 사이트를 참조하십시오.

`http://technet2.microsoft.com/WindowsServer/en/library/64042138-9a5a-4981-84e9-d576a8db0d051033.mspx?mfr=true`

분산 인증 UI 서버의 비밀번호 설정 단계 문제 문서화(6510859)

다음에 나오는 절차는 Access Manager 서버와 통신하는 분산 인증 UI 서버에 대해 암호화된 비밀번호를 설정하는 방법을 설명합니다.

분산 인증 UI 서버에 대한 비밀번호를 설정하려면

1. Access Manager 서버의 경우:
   a. ampassword -e 유틸리티를 사용하여 amadmin 비밀번호를 암호화합니다. 예를 들어 Solaris 시스템의 경우 다음과 같습니다.

      ```
      # cd /opt/SUNWam/bin
      # ./ampassword -e amadmin-password
      AQIC0K3omEozd544XEJIg25GT2wi1D7UAQLX
      ```

      암호화된 이 값을 저장합니다.
   b. Access Manager 서버의 AMConfig.properties 파일로부터 am.encryption.pwd 등록 정보 값을 복사하고 저장합니다. 예를 들면 다음과 같습니다.

      ```
      am.encryption.pwd=ydV8JXhJF2J35vpxjZRiGt7SH/7mUr+Y
      ```
2. 분산 인증 UI 서버의 경우 AMConfig.properties 파일에서 다음과 같이 변경합니다.
   a. com.iplanet.am.service.password 등록 정보를 주석으로 처리합니다.
   b. com.iplanet.am.service.secret 등록 정보를 1a단계에서 암호화된 amadmin 비밀번호로 설정합니다.
   c. 1b단계에서 복사한 am.encryption.pwd 및 암호화된 값을 추가합니다. 예를 들면 다음과 같습니다.

      ```
      com.sun.identity.agents.app.username=username
      #com.iplanet.am.service.password=password
      com.iplanet.am.service.secret=AQIC0K3omEozd544XEJIg25GT2wi1D7UAQLX
      am.encryption.pwd=ydV8JXhJF2J35vpxjZRiGt7SH/7mUr+Y
      ```
3. 분산 인증 UI 서버를 다시 시작합니다.

추가 정보가 필요한 "새 사이트 이름 만들기" 온라인 도움말(2144543)

Access Manager 콘솔 온라인 도움말에서 구성 > 시스템 등록 정보 > 플랫폼에 따른 "새 사이트 이름 만들기"에 맞는 저장 단계가 없습니다. 새 사이트 이름을 추가한 다음 저장을 누르지 않고 인스턴스 이름을 추가하려고 하면 해당 프로세스가 실패하게 됩니다. 따라서 반드시 새 사이트 이름을 추가하고 저장을 누른 다음 인스턴스 이름을 추가해야 합니다.

Windows 시스템의 관리자 비밀번호 구성 매개 변수(ADMIN_PASSWD) 문제 문서화(6470793)

Solaris 및 Linux 시스템의 경우 amsamplesilent 파일의 Access Manager 관리자(amadmin) 비밀번호 구성 매개 변수는 ADMI1NPASSWD입니다. 그러나 Windows 시스템의 경우 AMConfigurator.properties 파일의 해당 매개 변수는ADMIN_PASSWD입니다.

Windows 시스템에서 amconfig.bat을 실행할 경우 ADMINPASSWD 매개 변수가 아니라 ADMIN_PASSWORD 매개 변수를 사용하여 AMConfigurator.properties 파일의 amadmin 비밀번호를 설정합니다.

릴리스 노트에 알려진 문제에 대한 해결 방법이 잘못 설명되어 있습니다(6422907).

89 페이지 “웹 서비스 샘플을 실행하면 “자원 오퍼링을 찾을 수 없습니다”라는 메시지가 나타납니다(6359900).”에 대한 해결 방법의 3단계가 수정되었습니다.

AMConfig.properties에서 com.iplanet.am.session.protectedPropertiesList 문제 문서화(6351192)

com.iplanet.am.session.protectedPropertiesList 매개 변수를 사용하면 세션 서비스의 SetProperty 메소드를 통해 원격 업데이트에서 특정 핵심 또는 내부 세션 등록 정보를 보호할 수 있습니다. "hidden" 키 보안 매개 변수를 설정하여 다른 Access Manager 기능뿐만 아니라 인증에 참여하기 위한 세션 속성을 사용자 정의할 수 있습니다. 이 매개 변수를 사용하려면

1. 텍스트 편집기를 사용하여 AMConfig.properties 파일에 매개 변수를 추가합니다.
2. 보호할 세션 등록 정보에 매개 변수를 설정합니다. 예를 들면 다음과 같습니다.

   ```
   com.iplanet.am.session.protectedPropertiesList =
   PropertyName1,PropertyName2,PropertyName3
   ```

3. 값을 적용하려면 Access Manager 웹 컨테이너를 다시 시작합니다.

LDAPv3 플러그인의 역할 및 필터링된 역할 지원 문제 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(CR 6349959 해결). Access Manager 7 2005Q4 관리자 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 문제 문서화(6344530)

AMConfig.properties 파일의 다음 속성이 사용되지 않습니다.

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

서버 측의 com.iplanet.am.session.client.polling.enable이 true여서는 안 됩니다(6320475).

AMConfig.properties 파일에서 서버 측의 com.iplanet.am.session.client.polling.enable 등록 정보가 true로 설정되어서는 안 됩니다.

해결 방법: 이 등록 정보가 기본 값인 false로 설정된 후 true로 다시 설정되어서는 안 됩니다.

콘솔 온라인 도움말의 기본 성공 URL이 정확하지 않습니다(6296751).

service.scserviceprofile.iplanetamauthservice.html 온라인 도움말 파일의 기본 성공 URL이 정확하지 않습니다. 기본 성공 URL 필드는 성공적인 인증 후 사용자가 리디렉션되는 URL을 지정하는 다수의 값 목록을 허용합니다. 기본 HTML 유형을 가정하는 URL의 값만 지정할 수 있지만 이 속성의 형식은 clientType|URL입니다.

"/amconsole" 기본값이 올바르지 않습니다.

해결 방법: 올바른 기본값은 "/amserver/console"입니다.

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

설명서 업데이트

Sun Java System Access Manager 7 2005Q4 모음

다음 표에서는 최초 릴리스 이후 발행된 Access Manager 7 2005Q4의 새로운 설명서 또는 개정된 설명서를 나열합니다. 해당 설명서를 사용하려면 Access Manager 7 2005Q4 모음을 참조하십시오.

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

표 7 Access Manager 7 2005Q4 설명서 업데이트 내역

제목	발행일
Sun Java System Access Manager 7 2005Q4 릴리스 노트	표 1을 참조하십시오.
Sun Java System Access Manager 7 2005Q4 관리 설명서	2006년 2월
Sun Java System Access Manager 7 2005Q4 Developers Guide	2006년 2월
Sun Java System Access Manager Policy Agent 2.2 User's Guide	2006년 2월
Sun Java System Access Manager 7 2005Q4 C API Reference	2006년 2월
Sun Java System Access Manager 7 2005Q4 Federation and SAML Administration Guide	2006년 2월
Technical Note: Using Access Manager Distributed Authentication	2006년 2월
Technical Note: Installing Access Manager to Run as a Non-Root User	2006년 2월
Sun Java System SAML v2 Plug-in for Federation Services User's Guide	2006년 2월

표 7 Access Manager 7 2005Q4 설명서 업데이트 내역 (계속)

제목	발행일
Sun Java System SAML v2 Plug-in for Federation Services Release Notes	2006년 2월
Sun Java System SAMLv2 Plug-in for Federation Services Java API Reference	2006년 2월
Sun Java System Access Manager 7 2005Q4 배포 계획 설명서	2006년 1월
Sun Java System Access Manager 7 2005Q4 Performance Tuning Guide	2005년 12월
Sun Java System Access Manager 7 2005Q4 기술 개요	2005년 12월

Sun Java System Federation Manager 7.0 2005Q4 모음

Federation Manager 7.0 2005Q4 모음의 설명서를 사용하려면 다음 웹 사이트를 방문하십시오.

http://docs.sun.com/coll/1321.1

Sun Java System Access Manager Policy Agent 2.2 모음

Access Manager Policy Agent 2.2 모음은 새로운 에이전트의 문서화에 따라 개정 중입니다. 이 모음의 설명서를 사용하려면 다음 웹 사이트를 방문하십시오.

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

재배포 가능 파일

Sun Java System Access Manager 7 2005Q4의 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 보내기를 클릭하십시오.

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, 본 Access Manager 릴리스 노트의 부품 번호는 819-3477입니다. 사용자 의견을 제출할 때 해당 양식에 영문 설명서 제목과 부품 번호를 입력해야 할 수도 있습니다. 본 설명서의 영문 부품 번호와 제목은 819-2134, Sun Java System Access Manager 7 2005Q4 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 및 http://docs.sun.com/prod/entsys.05q4?l=ko
- 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.