Sun Java System Access Manager 7 2005Q4 관리 설명서

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

부품 번호: 819–3484

060419@14774

목차

머리말

Sun Java System Access Manager 7 2005Q4 관리 설명서에서는 명령줄 인터페이스를 통해 사용자 및 서비스 데이터를 관리하고 Sun Java™ System Access Manager 콘솔을 사용하는 방법에 대해 설명합니다.

Access Manager는 Sun Java Enterprise System(Java ES)의 구성 요소로 네트워크 또는 인터넷 환경 전체에 배포되는 기업 응용 프로그램 지원에 필요한 서비스를 제공하는 일련의 소프트웨어 구성 요소입니다.

본 설명서의 대상

본 설명서는 Sun Java System 서버 및 소프트웨어를 사용하여 웹 액세스 플랫폼을 구현하는 IT 관리자 및 소프트웨어 개발자를 대상으로 제작되었습니다.

본 설명서를 읽기 전에

본 설명서를 읽는 사용자는 다음 구성 요소와 개념에 대해 알고 있어야 합니다.

- **Sun Java System Access Manager 7 2005Q4 Technical Overview**에 설명된 Access Manager 기술 개념
- 배포 플랫폼: Solaris 또는 Linux 운영 체제
- Access Manager를 실행할 웹 컨테이너: Sun Java System Application Server, Sun Java System Web Server, BEA WebLogic 또는 IBM WebSphere Application Server
- 기술 개념: Lightweight Directory Access Protocol(LDAP), Java 기술, JavaServer Pages(JSP) 기술, HyperText Transfer Protocol(HTTP), HyperText Markup Language(HTML) 및 eXtensible Markup Language(XML)

관련 문서

사용할 수 있는 관련 문서는 다음과 같습니다.

- 14 페이지 “Access Manager 핵심 설명서”
- 15 페이지 “Sun Java Enterprise System 제품 설명서”

Access Manager 핵심 설명서

Access Manager 핵심 설명서 세트에 포함된 항목은 다음과 같습니다.

- **Sun Java System Access Manager 7 2005Q4** 릴리스 노트는 제품 출시 후 온라인으로 제공됩니다. 여기에는 이 릴리스의 새로운 기능에 대한 설명, 알려진 문제점과 제한 사항, 설치 주의 사항, 소프트웨어 또는 설명서에 관한 문제를 보고하는 방법 등의 최신 정보가 포함되어 있습니다.
- **Sun Java System Access Manager 7 2005Q4 Technical Overview**는 Access Manager 구성 요소를 결합하여 액세스 제어 기능을 통합하고 기업 자산 및 웹 기반 응용 프로그램을 보호하는 방법에 대한 개요를 제공합니다. 또한 기본적인 Access Manager 개념 및 용어에 대해서 설명합니다.
- **Sun Java System Access Manager 7 2005Q4 Deployment Planning Guide**는 솔루션 수명 주기에 따라 Sun Java System Access Manager를 계획하고 배치하는 방법을 제공합니다.
- **Sun Java System Access Manager 7 2005Q4 Performance Tuning Guide**는 최적의 성능을 위해 Access Manager 및 관련 구성 요소를 조정하는 방법을 제공합니다.
- **Sun Java System Access Manager 7 2005Q4** 관리 설명서는 명령줄 인터페이스를 통해 사용자 및 서비스를 관리하고 Access Manager 콘솔을 사용하는 방법에 대해 설명합니다.
- **Sun Java System Access Manager 7 2005Q4 Federation and SAML Administration Guide**(본 설명서)는 Liberty Alliance Project 사양에 따른 연합 모듈에 대한 정보를 제공합니다. 이 사양에 따른 통합 서비스 정보, Liberty 기반 환경 사용 지침 및 프레임워크 확장을 위한 API(Application Programming Interface) 요약 정보도 포함합니다.
- **Sun Java System Access Manager 7 2005Q4 Developer’s Guide**는 Access Manager를 사용자 정의하고 Access Manager 기능을 조직의 현재 기술 인프라에 통합하는 방법을 제공합니다. 또한 제품과 해당 API의 프로그램 사양에 대한 정보를 제공합니다.
- **Sun Java System Access Manager 7 2005Q4 C API Reference**는 공용 Access Manager C API를 구성하는 데이터 유형, 구조 및 기능에 대한 요약 정보를 제공합니다.
- **Java API Reference**(부품 번호 819-2141)는 Access Manager에서의 Java 패키지 구현에 대한 정보를 제공합니다.
- **Sun Java System Access Manager Policy Agent 2.2 User’s Guide**는 Access Manager에 적용 가능한 정책 기능 및 정책 에이전트에 대한 개요를 제공합니다.

릴리스 노트 업데이트 및 핵심 설명서 수정 링크는 Sun Java Enterprise System 설명서 웹 사이트의 Access Manager 페이지에서 찾을 수 있습니다. 업데이트된 문서에는 개정 날짜가 표시됩니다.

Sun Java Enterprise System 제품 설명서

다음 제품에 대한 설명서에서 유용한 정보를 찾을 수 있습니다.

- Directory Server
- Web Server
- Application Server
- Web Proxy Server

타사 웹사이트

본 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.

문서, 지원 및 교육

Sun 제공 기능	URL	설명
설명서	http://www.sun.com/documentation/	PDF 및 HTML 문서 다운로드, 인쇄 문서 주문
지원 및 교육	http://www.sun.com/supportraining/	기술 지원, 패치 다운로드, Sun 교육 과정 학습

활자체 규약

다음 표는 본 설명서에서 사용된 서체 변경 사항에 대하여 설명합니다.

표 P–1 활자체 규약

서체 또는 기호	의미	예
`AaBbCc123`	명령, 파일 및 디렉토리의 이름 등 컴퓨터 화면에 출력되는 내용입니다.	`.login` 파일을 편집하십시오. `ls -a` 명령을 사용하여 모든 파일을 나열하십시오. `machine_name% you have mail.`
`AaBbCc123`	컴퓨터 화면상의 출력에 대하여 입력할 내용	`machine_name%` **`su`** `Password:`
aabbcc123	자리 표시자: 실제 이름이나 값으로 대체됩니다.	파일 제거 명령은 `rm` *filename*입니다.
AaBbCc123	책 제목, 새로 나오는 용어, 강조 표시할 단어입니다.	사용자 설명서의 6장을 읽으십시오. 패치 분석을 수행하십시오. 파일을 저장하면 안 됩니다. [일부 강조된 항목은 온라인에서 굵은체로 나타납니다.]

명령 예의 쉘 프롬프트

C 쉘, Bourne 쉘 및 Korn 쉘에 대한 기본 시스템 프롬프트 및 수퍼유저 프롬프트는 다음 표와 같습니다.

표 P–2 쉘 프롬프트

쉘	프롬프트
C 쉘 프롬프트	`machine_name%`
C 쉘 수퍼유저 프롬프트	`machine_name#`
Bourne 쉘 및 Korn 쉘 프롬프트	`$`
Bourne 쉘 및 Korn 쉘 수퍼유저 프롬프트	`#`

Sun은 여러분의 의견을 환영합니다.

Sun은 설명서의 내용 개선에 노력을 기울이고 있으며, 여러분의 의견과 제안을 환영합니다.

사용자 의견을 보내시려면 http://docs.sun.com에서 의견 보내기를 누릅니다. 해당 필드에 전체 설명서 제목과 부품 번호를 입력해 주십시오. 부품 번호는 해당 설명서의 제목 페이지나 문서 맨 위에 있으며 일반적으로 7자리 또는 9자리 숫자입니다.

예를 들어, 본 설명서의 제목은 **Sun Java System Access Manager 7 2005Q4** 관리 설명서이며 부품 번호는 819-3484입니다. 사용자 의견을 제출할 때 해당 양식에 영문 설명서 제목과 부품 번호를 입력해야 할 수도 있습니다. 본 설명서의 영문 부품 번호와 제목은 819-2137, Sun Java System Access Manager 7 2005Q4 Administration Guide입니다.

파 트 I

Access Manager 구성

Sun Java System Access Manager™ 7 2005Q4 관리 설명서의 제1부입니다. 여기에서는 Access Manager를 설치한 다음 수행할 수 있는 구성 옵션에 대해 설명합니다. 다음과 같은 장으로 구성됩니다.

◆ ◆ ◆ 1 장

1 Access Manager 7 2005Q4 구성 스크립트

이 장에서는 `amconfig` 스크립트와 샘플 자동 설치 모드 입력 파일(`amsamplesilent`)을 사용하여 Sun Java™ System Access Manager를 구성하고 배포하는 방법에 대해 설명합니다. 이 장에 포함된 항목은 다음과 같습니다.

Access Manager 7 2005Q4 설치 개요

새로 설치하는 경우 항상 Sun Java Enterprise System(Java ES) 설치 프로그램을 실행하여 Access Manager 7 2005Q4의 첫 번째 인스턴스를 설치할 수 있습니다. 설치 프로그램을 실행할 때 다음 Access Manager 구성 옵션 중 하나를 선택할 수 있습니다.

- 지금 구성 옵션을 사용하면 Access Manager 설치 패널에서 선택한 옵션(또는 기본값)으로 설치 중에 첫 번째 인스턴스를 설치 및 구성할 수 있습니다.
- 나중에 구성 옵션을 사용하면 Access Manager 7 2005Q4 구성 요소를 설치한 후 36 페이지 "Access Manager 인스턴스 구성 및 재구성"에서 설명한 대로 사용자가 직접 구성하거나 Access Manager 스크립트를 실행해야 합니다. 이 옵션을 선택하면 현재 설치 중인 제품이 하나도 구성되지 않습니다. 예를 들어, Access Manager 및 Application Server 설치를 선택하고 나중에 구성 옵션을 선택하면 두 응용 프로그램 모두 구성되지 않습니다.

주 – BEA WebLogic 또는 IBM WebSphere Application Server를 Access Manager 웹 컨테이너로 설치하는 경우 Access Manager를 설치할 때 나중에 구성 옵션을 선택해야 합니다. 자세한 내용은 2 장을 참조하십시오.

설치 프로그램에 대한 자세한 내용은 **Sun Java Enterprise System 2005Q4 Installation Guide for UNIX**.

Java Enterprise System 설치 프로그램은 Solaris 시스템의 *AccessManager-base* /SUNWam/bin 디렉토리 또는 Linux 시스템의 *AccessManager-base*/identity/bin 디렉토리에 Access Manager 7 2005Q4 amconfig 스크립트 및 샘플 자동 설치 모드 입력 파일(amsamplesilent)을 설치합니다.

*AccessManager-base*는 Access Manager 기본 설치 디렉토리를 나타냅니다. Solaris 시스템에서는 /opt가 기본 설치 디렉토리이고, Linux 시스템에서는 /opt/sun이 기본 설치 디렉토리입니다. 그러나 설치 프로그램을 실행할 때 다른 디렉토리를 지정할 수도 있습니다.

amconfig 스크립트는 요청된 작업을 수행하기 위해 필요할 때 다른 스크립트를 호출하는 최상위 스크립트입니다. 자세한 내용은 33 페이지 "Access Manager amconfig 스크립트"를 참조하십시오.

샘플 구성 스크립트 입력 파일(amsamplesilent)은 자동 설치 모드에서 amconfig 스크립트를 실행할 때 지정해야 하는 입력 파일을 만드는 데 사용할 수 있는 템플리트입니다.

이 샘플 구성 스크립트 입력 파일은 Access Manager 구성 변수를 포함하고 있는 ASCII 텍스트 파일입니다. amconfig 스크립트를 실행하기 전에 amsamplesilent 파일을 복사하고 필요한 경우 이름을 바꾼 다음 사용자의 시스템 환경에 따라 파일에 있는 변수를 편집합니다. 구성 변수의 형식은 다음과 같습니다.

```
variable-name=value
```

예를 들면 다음과 같습니다.

```
DEPLOY_LEVEL=1
 NEW_INSTANCE=true
 SERVER_HOST=ishost.example.com
```

구성 스크립트 입력 파일에서 설정할 수 있는 변수의 목록에 대한 자세한 내용은 23 페이지 "Access Manager 샘플 구성 스크립트 입력 파일"을 참조하십시오.

주의 – 자동 설치 모드에서 amconfig를 실행할 때 사용한 샘플 구성 스크립트 입력 파일의 형식은 Java Enterprise System 자동 설치 상태 파일과 형식이 같거나 같은 변수 이름을 사용할 필요가 없습니다. 이 파일은 관리자 비밀번호와 같은 중요한 데이터를 포함하고 있습니다. 확실히 보호 또는 삭제하도록 합니다.

Access Manager amconfig 스크립트 작업

Sun Java Enterprise System 설치 프로그램을 사용하여 Access Manager의 첫 번째 인스턴스를 설치한 후 자동 설치 모드 입력 파일의 변수 값에 따라 amconfig 스크립트를 실행하여 다음 작업을 수행할 수 있습니다.

- Access Manager의 첫 번째 인스턴스를 배포하고 구성하거나 동일한 호스트 시스템에 Access Manager의 추가 인스턴스를 배포하고 구성합니다. 예를 들어, 한 웹 컨테이너의 추가 인스턴스를 구성한 후 그 웹 컨테이너 인스턴스에 대해 새 Access Manager 인스턴스를 배포하고 구성할 수 있습니다.

- Access Manager의 첫 번째 인스턴스와 추가 인스턴스를 모두 재구성합니다.
- Access Manager의 모든 서버 서비스 또는 SDK 서비스만을 배포하고 구성하여 다음과 같은 제품을 지원할 수 있습니다.
  - BEA WebLogic
  - IBM WebSphere Application Server

  콘솔 또는 연합 관리 모듈과 같은 특정 Access Manager 구성 요소를 배포하고 구성합니다.
- `amconfig` 스크립트를 사용하여 배포한 Access Manager의 인스턴스와 구성 요소를 제거합니다.

Access Manager 샘플 구성 스크립트 입력 파일

Java Enterprise System 설치 프로그램을 실행한 후 Solaris 시스템의 *AccessManager-base* `/SUNWam/bin` 디렉토리 또는 Linux 시스템의 *AccessManager-base* `/identity/bin` 디렉토리에서 Access Manager 샘플 구성 스크립트 입력 파일(`amsamplesilent`)을 사용할 수 있습니다.

구성 변수를 설정하려면 먼저 `amsamplesilent` 파일을 복사하고 이름을 바꿉니다. 그런 다음 수행하려는 작업을 위한 변수를 복사본에서 설정합니다. 이 파일에 대한 예제는 39 페이지 “예제 구성 스크립트 입력 파일”을 참조하십시오.

샘플 자동 설치 모드 입력 파일은 다음 구성 변수를 포함합니다.

- 23 페이지 “배포 모드 변수”
- 24 페이지 “Access Manager 구성 변수”
- 28 페이지 “웹 컨테이너 구성 변수”
- 32 페이지 “Directory Server 구성 변수”

배포 모드 변수

이 절에서는 필수 DEPLOY_LEVEL 변수에 대한 값을 설명합니다. 이 변수에 따라 `amconfig` 스크립트에서 수행할 작업이 결정됩니다.

표 1–1 Access Manager DEPLOY_LEVEL 변수

작업	DEPLOY_LEVEL 변수 값 및 설명
설치	1 = 새 인스턴스를 위한 전체 Access Manager 설치(기본값) 2 = Access Manager 콘솔만 설치 3 = Access Manager SDK만 설치 4 = SDK만 설치하고 컨테이너 구성 5 = 연합 관리 모듈만 설치 6 = 서버만 설치 7 = Access Manager 설치 및 Portal Server로 배포하기 위한 컨테이너 구성 주의 DEPLOY_MODE=7은 Portal Server로 Access Manager를 배포하는 경우에만 사용됩니다. 일부 배포에서는 다른 웹 컨테이너를 사용하여 단일 호스트 서버에 콘솔 및 서버만 설치하려는 경우가 있습니다. 먼저 Java ES 설치 프로그램을 실행하여 나중에 구성 옵션으로 모든 Access Manager 하위 구성 요소를 설치합니다. 그 다음 `amconfig` 스크립트를 실행하여 콘솔 및 서버 인스턴스를 구성합니다.
제거(구성 해제)	11 = 전체 제거 12 = 콘솔만 제거 13 = SDK만 제거 14 = SDK만 제거하고 컨테이너 구성 해제 15 = 연합 관리 모듈 제거 16 = 서버만 제거 Access Manager 제거 및 Portal Server로 배포된 경우 컨테이너 구성 해제 주의 DEPLOY_MODE=7은 Portal Server로 Access Manager를 배포한 경우에만 사용됩니다.
다시 설치 (재배포 또는 재구성)	21 = 모든(콘솔, 비밀번호, 서비스 및 일반) 웹 응용 프로그램 재배포 26 = 모든(콘솔, 비밀번호, 서비스 및 일반) 웹 응용 프로그램 배포 해제

Access Manager 구성 변수

이 절에서는 Access Manager 구성 변수에 대해 설명합니다.

표 1–2 Access Manager 구성 변수

변수	설명
AM_REALM	Access Manager 모드를 나타냅니다. ■ enabled: Access Manager 7 2005Q4 기능 및 콘솔을 사용하여 Access Manager를 영역 모드에서 작동합니다. ■ disabled: Access Manager 6 2005Q1 기능 및 콘솔을 사용하여 Access Manager를 레거시 모드에서 작동합니다. 기본값: enabled **주의 –** Access Manager 영역 모드는 기본적으로 활성화되어 있습니다. Portal Server, Messaging Server, Calendar Server, Delegated Administrator 또는 Instant Messaging으로 Access Manager를 배포하는 경우 `amconfig` 스크립트를 실행하기 전에 레거시 모드(AM_REALM=disabled)를 선택해야 합니다.
BASEDIR	Access Manager 패키지를 위한 기본 설치 디렉토리 기본값: PLATFORM_DEFAULT Solaris 시스템의 경우 PLATFORM_DEFAULT는 `/opt`입니다. Linux 시스템의 경우 PLATFORM_DEFAULT는 `/opt/sun`입니다.
SERVER_HOST	Access Manager가 실행되고 있거나 설치될 시스템의 정규화된 호스트 이름 원격 SDK 설치의 경우에는 이 변수를 원격 클라이언트 호스트가 아니며 Access Manager가 설치되어 있거나 설치될 호스트로 설정합니다. 이 변수는 웹 컨테이너 구성의 해당 변수와 일치해야 합니다. 예를 들어, Application Server 8의 경우 이 변수는 AS81_HOST와 일치해야 합니다.
SERVER_PORT	Access Manager 포트 번호. 기본값: 58080 원격 SDK 설치의 경우에는 이 변수를 원격 클라이언트 호스트가 아니며 Access Manager가 설치되어 있거나 설치될 호스트의 포트로 설정합니다. 이 변수는 웹 컨테이너 구성의 해당 변수와 일치해야 합니다. 예를 들어, Application Server 8의 경우 이 변수는 AS81_PORT와 일치해야 합니다.
SERVER_PROTOCOL	서버 프로토콜: http 또는 https. 기본값: http 원격 SDK 설치의 경우에는 이 변수를 원격 클라이언트 호스트가 아니며 Access Manager가 설치되어 있거나 설치될 호스트의 프로토콜로 설정합니다. 이 변수는 웹 컨테이너 구성의 해당 변수와 일치해야 합니다. 예를 들어, Application Server 8의 경우 이 변수는 AS81_PROTOCOL과 일치해야 합니다.
CONSOLE_HOST	콘솔이 설치된 서버의 정규화된 호스트 이름 기본값: Access Manager 호스트용으로 제공된 값

표 1–2 Access Manager 구성 변수 *(계속)*

변수	설명
CONSOLE_PORT	콘솔이 설치되어 있고 연결을 수신하는 웹 컨테이너의 포트 기본값: Access Manager 포트용으로 제공된 값
CONSOLE_PROTOCOL	콘솔이 설치되어 있는 웹 컨테이너의 프로토콜 기본값: 서버 프로토콜
CONSOLE_REMOTE	콘솔이 Access Manager 서비스에서 원격인 경우 true로 설정하고그렇지 않은 경우 false로 설정. 기본값: false
DS_HOST	Directory Server의 정규화된 호스트 이름
DS_PORT	Directory Server 포트. 기본값: 389
DS_DIRMGRDN	디렉토리 관리자 DN: Directory Server에 대한 무제한적인 액세스 권한을 가진 사용자 기본값: `"cn=Directory Manager"`
DS_DIRMGRPASSWD	디렉토리 관리자의 비밀번호 24 페이지 “Access Manager 구성 변수”에 대한 설명에서 특수 문자에 대한 참고를 참조하십시오.
ROOT_SUFFIX	디렉토리의 초기 또는 루트 접미어. 이 값이 사용 중인 Dircetory Server에 있는 지를 확인해야 합니다. 24 페이지 “Access Manager 구성 변수”에 대한 설명에서 특수 문자에 대한 참고를 참조하십시오.
ADMINPASSWD	관리자(`amadmin`)의 비밀번호. `amldapuser`의 비밀번호와 달라야 합니다. 참고: 비밀번호에 포함되는슬래시(/) 또는 백슬래시(\\) 같은 특수 문자는 작은 따옴표(’) 안에 넣어야 합니다. 예를 들면 다음과 같습니다. `ADMINPASSWD=’\\\\\\\\\\###///’` 그러나 작은 따옴표를 실제 비밀번호의 문자 중 하나로 사용할 수는 없습니다.
AMLDAPUSERPASSWD	`amldapuser`의 비밀번호. `amadmin`의 비밀번호와 달라야 합니다. 24 페이지 “Access Manager 구성 변수”에 대한 설명에서 특수 문자에 대한 참고를 참조하십시오.
CONSOLE_DEPLOY_URI	Access Manager 관리 콘솔 하위 구성 요소와 연관된 HTML 페이지, 클래스 및 JAR 파일에 액세스하기 위한 URI 접두어 기본값: `/amconsole`

표 1–2 Access Manager 구성 변수 *(계속)*

변수	설명
SERVER_DEPLOY_URI	Identity Management 및 Policy Services Core 하위 구성 요소와 연관된 HTML 페이지, 클래스 및 JAR 파일에 액세스하기 위한 URI 접두어 기본값: `/amserver`
PASSWORD_DEPLOY_URI	Access Manager를 실행하는 웹 컨테이너에서 사용자가 지정하는 문자열과 해당 배포 응용 프로그램 사이에 사용할 매핑을 결정하는 URI 기본값: `/ampassword`
COMMON_DEPLOY_URI	웹 컨테이너의 공통 도메인 서비스에 액세스하기 위한 URI 접두어 기본값: `/amcommon`
COOKIE_DOMAIN	Access Manager가 사용자에게 세션 아이디를 부여할 때 브라우저로 반환하는, 신뢰할 수 있는 DNS 도메인의 이름. 최소한 하나의 값이 있어야 합니다. 일반적으로 서버의 도메인 이름 앞에 마침표가 붙은 형식을 사용합니다. 예: `.example.com`
JAVA_HOME	JDK 설치 디렉토리에 대한 경로. 기본값: `/usr/jdk/entsys-j2se`. 이 변수는 명령줄 인터페이스(예: `amadmin`) 실행 파일에서 사용되는 JDK를 제공합니다. 버전은 1.4.2 이상이어야 합니다.
AM_ENC_PWD	비밀번호 암호화 키: Access Manager가 사용자 비밀번호를 암호화하기 위해 사용하는 문자열. 기본값: none. 값이 none으로 설정되면 `amconfig`는 사용자에 대해 비밀번호 암호화 키를 생성하므로 사용자가 지정하거나 `amconfig`를 통해 만든 설치에 대해 비밀번호 암호화가 사용됩니다. 중요: Access Manager 또는 원격 SDK의 인스턴스를 여러 개 배포하는 경우 모든 인스턴스는 동일한 비밀번호 암호화 키를 사용해야 합니다. 추가 인스턴스를 배포할 때 첫 번째 인스턴스의 `AMConfig.properties` 파일에서 `am.encryption.pwd property` 값을 복사합니다.
PLATFORM_LOCALE	플랫폼의 로켈. 기본값: `en_US`(미국 영어)
NEW_OWNER	설치 후 Access Manager 파일의 새 소유자. 기본값: `root`
NEW_GROUP	설치 후 Access Manager 파일의 새 그룹. 기본값: `other` Linux 설치의 경우 NEW_GROUP을 `root`로 설정합니다.
PAM_SERVICE_NAME	PAM 구성의 PAM 서비스 이름 또는 운영 체제와 함께 제공되면서 Unix 인증 모듈(보통 Solaris의 경우 `other` 또는 Linux의 경우 `password`)에 사용되는 스택. 기본값: `other`
XML_ENCODING	XML 인코딩. 기본값: `ISO-8859-1`

표 1–2 Access Manager 구성 변수 *(계속)*

변수	설명
NEW_INSTANCE	구성 스크립트가 새 사용자가 생성한 웹 컨테이너 인스턴스에 Access Manager를 배포할지 여부를 지정합니다. ■ true = Access Manager를 기존 인스턴스 대신 새 사용자가 만든 웹 컨테이너 인스턴스에 배포 ■ false = 첫 번째 인스턴스를 구성하거나 인스턴스를 재구성 기본값: false
SSL_PASSWORD	이번 릴리스에서는 사용되지 않습니다.

웹 컨테이너 구성 변수

Access Manager를 위한 웹 컨테이너를 지정하려면자동 설치 모드 입력 파일에서 WEB_CONTAINER 변수를 설정합니다. Access Manager 7 2005Q4에서 지원하는 웹 컨테이너 버전에 대한 자세한 내용은 **Sun Java System Access Manager 7 2005Q4** 릴리스 노트를 참조하십시오.

표 1–3 Access Manager WEB_CONTAINER 변수

값	웹 컨테이너
WS6(기본값)	28 페이지 “Sun Java System Web Server 6.1 SP5”
AS8	29 페이지 “Sun Java System Application Server 8.1”
WL8	30 페이지 “BEA WebLogic Server 8.1”
WAS5	31 페이지 “IBM WebSphere 5.1”

Sun Java System Web Server 6.1 SP5

이 절에서는 자동 설치 모드 입력 파일의 Web Server 6.1 2005Q4 SP5에 대한 구성 변수에 대해 설명합니다.

표 1–4 Web Server 6.1 구성 변수

변수	설명
WS61_INSTANCE	Access Manager가 배포되거나 배포 해제될 Web Server 인스턴스의 이름 기본값: https-*web-server-instance-name* 여기서 *web-server-instance-name*은 Access Manager 호스트(24 페이지 “Access Manager 구성 변수” 변수)입니다.
WS61_HOME	Web Server 기본 설치 디렉토리 기본값: `/opt/SUNWwbsvr`

표 1–4 Web Server 6.1 구성 변수 (계속)

변수	설명
WS61_PROTOCOL	Access Manager가 배포될 28 페이지 “Sun Java System Web Server 6.1 SP5” 변수에 의해 설정된 Web Server 인스턴스에서 사용되는 프로토콜: http 또는 https. 기본값: Access Manager 프로토콜(24 페이지 “Access Manager 구성 변수”)
WS61_HOST	Web Server 인스턴스(28 페이지 “Sun Java System Web Server 6.1 SP5” 변수)의 정규화된 호스트 이름 기본값: Access Manager 호스트 인스턴스(24 페이지 “Access Manager 구성 변수”)
WS61_PORT	Web Server가 연결을 수신하는 포트 기본값: Access Manager 포트 번호(24 페이지 “Access Manager 구성 변수”)
WS61_ADMINPORT	Web Server Administration Server가 연결을 수신하는 포트 기본값: 8888
WS61_ADMIN	Web Server 관리자의 사용자 아이디 기본값: `"admin"`

Sun Java System Application Server 8.1

이 절에서는 자동 설치 모드 입력 파일의 Application Server 8.1에 대한 구성 변수에 대해 설명합니다.

표 1–5 Application Server 8.1 구성 변수

변수	설명
AS81_HOME	Application Server 8.1이 설치된 디렉토리에 대한 경로 기본값: `/opt/SUNWappserver/appserver`
AS81_PROTOCOL	Application Server 인스턴스에서 사용되는 프로토콜: http 또는 https. 기본값: Access Manager 프로토콜(24 페이지 “Access Manager 구성 변수”)
AS81_HOST	Application Server 인스턴스가 연결을 수신하는 정규화된 도메인 이름(FQDN) 기본값: Access Manager 호스트(24 페이지 “Access Manager 구성 변수”)
AS81_PORT	Application Server 인스턴스가 연결을 수신하는 포트 기본값: Access Manager 포트 번호(24 페이지 “Access Manager 구성 변수”)

표 1–5 Application Server 8.1 구성 변수 *(계속)*

변수	설명
AS81_ADMINPORT	Application Server 관리 서버가 연결을 수신하는 포트 기본값: 4849
AS81_ADMIN	Application Server가 표시되는 도메인을 위한 Application Server 관리 서버를 관리하는 사용자의 이름 기본값: `admin`
AS81_ADMINPASSWD	Application Server가 표시되는 도메인을 위한 Application Server 관리자의 비밀번호 24 페이지 “Access Manager 구성 변수”에 대한 설명에서 특수 문자에 대한 참고를 참조하십시오.
AS81_INSTANCE	Access Manager를 실행할 Application Server 인스턴스의 이름 기본값: `server`
AS81_DOMAIN	Access Manager 인스턴스를 배포하려는 도메인의 Application Server 디렉토리에 대한 경로 기본값: `domain1`
AS81_INSTANCE_DIR	Application Server가 인스턴스를 위한 파일을 저장하는 디렉토리에 대한 경로 기본값: `/var/opt/SUNWappserver/domains/domain1`
AS81_DOCS_DIR	Application Server가 컨텐트 문서를 저장하는 디렉토리 기본값: `/var/opt/SUNWappserver/domains/domain1/docroot`
AS81_ADMIN_IS_SECURE	Application Server 관리 인스턴스가 SSL을 사용하는지 여부를 지정합니다. ■ true: 보안 포트 사용(HTTPS 프로토콜) ■ false: 보안 포트 사용 안 함(HTTP 프로토콜) 기본값: true(사용) `ampsamplesilent`의 경우 다음과 같이 응용 프로그램 서버 관리 포트가 안전한지 여부를 지정한 추가 설정이 있습니다. ■ true: 응용 프로그램 서버 관리 포트가 안전합니다(HTTPS 프로토콜). ■ false: 응용 프로그램 서버 관리 포트가 안전하지 않습니다(HTTP 프로토콜). 기본값: True(사용)

BEA WebLogic Server 8.1

이 절에서는 자동 설치 모드 입력 파일의 BEA WebLogic Server 8.1을 위한 구성 요소에 대해 설명합니다.

표 1–6 BEA WebLogic Server 8.1 구성 변수

변수	설명
WL8_HOME	WebLogic 홈 디렉토리. 기본값: `/usr/local/bea`
WL8_PROJECT_DIR	WebLogic 프로젝트 디렉토리. 기본값: `user_projects`
WL8_DOMAIN	WebLogic 도메인 이름. 기본값: `mydomain`
WL8_SERVER	WebLogic 서버 이름. 기본값: `myserver`
WL8_INSTANCE	WebLogic 인스턴스 이름. 기본값: `/usr/local/bea/weblogic81($WL8_HOME/weblogic81)`
WL8_PROTOCOL	WebLogic 프로토콜. 기본값: http
WL8_HOST	WebLogic 호스트 이름. 기본값: 서버의 호스트 이름
WL8_PORT	WebLogic 포트. 기본값: 7001
WL8_SSLPORT	WebLogic SSL 포트. 기본값: 7002
WL8_ADMIN	WebLogic 관리자. 기본값: `"weblogic"`
WL8_PASSWORD	WebLogic 관리자 비밀번호 24 페이지 “Access Manager 구성 변수”에 대한 설명에서 특수 문자에 대한 참고를 참조하십시오.
WL8_JDK_HOME	WebLogic JDK 홈 디렉토리. 기본값: 30 페이지 “BEA WebLogic Server 8.1” `/jdk142_04`
WL8_CONFIG_LOCATION	WebLogic 시작 스크립트 위치의 부모 디렉토리로 설정해야 합니다.

IBM WebSphere 5.1

이 절에서는 자동 설치 모드 입력 파일의 IBM WebSphere Server 5.1에 대한 구성 변수에 대해 설명합니다.

표 1–7 IBM WebSphere 5.1 구성 변수

변수	설명
WAS51_HOME	WebSphere 홈 디렉토리. 기본값: `/opt/WebSphere/AppServer`
WAS51_JDK_HOME	WebSphere JDK 홈 디렉토리. 기본값: `/opt/WebSphere/AppServer/java`
WAS51_CELL	WebSphere 셀. 기본값: 호스트 이름 값
WAS51_NODE	WebSphere 노드 이름. 기본값: WebSphere가 설치된 서버의 호스트 이름. 기본값: 호스트 이름 값
WAS51_INSTANCE	WebSphere 인스턴스 이름. 기본값: `server1`

표 1–7 IBM WebSphere 5.1 구성 변수 *(계속)*

변수	설명
WAS51_PROTOCOL	WebSphere 프로토콜. 기본값: http
WAS51_HOST	WebSphere 호스트 이름. 기본값: 서버의 호스트 이름
WAS51_PORT	WebSphere 포트. 기본값: 9080
WAS51_SSLPORT	WebSphere SSL 포트. 기본값: 9081
WAS51_ADMIN	WebSphere 관리자. 기본값: `"admin"`
WAS51_ADMINPORT	WebSphere 관리자 포트. 기본값: 9090

Directory Server 구성 변수

Access Manager 7 2005Q4에서 지원하는 Directory Server 버전에 대한 자세한 내용은 **Sun Java System Access Manager 7 2005Q4** 릴리스 노트를 참조하십시오. 이 절에서는 자동 설치 모드 입력 파일의 Directory Server 구성 변수에 대해 설명합니다.

표 1–8 Directory Server 구성 변수

변수	설명
DIRECTORY_MODE	Directory Server 모드: 1 = 디렉토리 정보 트리(DIT)의 새 설치를 위해 사용 2 = 기존 DIT를 위해 사용. 이름 지정 속성 및 객체 클래스는 동일하므로 구성 스크립트는 `installExisting.ldif` 파일과 `umsExisting.ldif` 파일을 로드합니다. 또한 구성 도중 입력된 실제값(예: BASE_DIR, SERVER_HOST 및 ROOT_SUFFIX)을 사용하여 LDIF와 등록 정보를 업데이트합니다. 구성 스크립트가 파일의 자리 표시자에 실제 구성 값을 대체하기 때문에 이 업데이트를 "태그 스왑"이라고 부르기도 합니다. 3 = 수동 로드를 수행하려고 할 때 기존 DIT를 위해 사용. 이름 지정 속성과 객체 클래스가 다르므로 구성 스크립트는 `installExisting.ldif` 파일과 `umsExisting.ldif` 파일을 로드하지 않습니다. 스크립트는 모드 2에서 설명한 태그 스왑을 수행합니다. LDIF 파일을 검사하고 필요하면 수정한 다음 LDIF 파일과 서비스를 수동으로 로드해야 합니다. 4 = 기존의 다중 서버 설치를 위해 사용. 기존 Access Manager 설치에 반하는 작업이기 때문에 구성 스크립트는 LDIF 파일과 서비스를 로드하지 않습니다. 스크립트는 모드 2에서 설명한 태그 스왑만 수행하고 플랫폼 목록에 서버 항목을 추가합니다. 5 = 기존 업그레이드를 위해 사용. 스크립트는 모드 2에서 설명한 태그 스왑만 수행합니다. 기본값: 1
USER_NAMING_ATTR	사용자 이름 지정 속성: 관련 이름 공간 내에서 사용자 또는 자원의 고유 식별자. 기본값: `uid`
ORG_NAMING_ATTR	사용자가 속한 회사 또는 조직의 이름 지정 속성. 기본값: `o`
ORG_OBJECT_CLASS	조직 객체 클래스. 기본값: `sunismanagedorganization`
USER_OBJECT_CLASS	사용자 객체 클래스. 기본값: `inetorgperson`
DEFAULT_ORGANIZATION	기본 조직 이름. 기본값: none

Access Manager amconfig 스크립트

Java Enterprise System 설치 프로그램을 실행한 후 Solaris 시스템의 *AccessManager-base* `/SUNWam/bin` 디렉토리 또는 Linux 시스템의 *AccessManager-base* `/identity/bin` 디렉토리에서 `amconfig` 스크립트를 사용할 수 있습니다.

amconfig 스크립트는 자동 구성 입력 파일을 읽은 다음 요청 받은 작업을 수행하기 위해 필요할 때 자동 설치 모드에서 다른 스크립트를 호출합니다.

amconfig 스크립트를 실행하려면 다음 구문을 사용합니다.

```
amconfig -s
          input-file
```

여기서

*-s*는 amconfig 스크립트를 자동 설치 모드에서 실행합니다.

input-file은 수행하려는 작업을 위한 구성 변수가 포함된 자동 구성 입력 파일입니다. 자세한 내용은 23 페이지 "Access Manager 샘플 구성 스크립트 입력 파일"을 참조하십시오.

amconfig 스크립트를 실행할 때 다음과 같은 몇 가지 고려 사항이 있습니다.

- 수퍼유저(root)로 실행 중이어야 합니다.
- amsamplesilent 파일 또는 파일의 복사본에 대한 전체 경로를 지정합니다. 예를 들면 다음과 같습니다.

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

  또는

  ```
  # ./amconfig -s /opt/SUNWam/bin/amsamplesilent
  ```

주 – Access Manager 7 2005Q4 릴리스에서는 다음 스크립트가 지원되지 않습니다.

- 생성 인수가 있는 amserver
- amserver.*instance*

또한 기본적으로 amserver start는 인증 amsecuridd 및 amunixd 도우미만 시작합니다. amsecuridd 도우미는 Solaris OS SPARC 플랫폼에서만 사용할 수 있습니다.

Access Manager 배포 시나리오

Java Enterprise System 설치 프로그램을 사용하여 Access Manager의 첫 번째 인스턴스를 설치한 다음 자동 설치 구성 입력 파일의 구성 변수를 편집하고 amconfig 스크립트를 실행하여 추가 Access Manager 인스턴스를 배포 및 구성할 수 있습니다.

이 절에서는 다음 시나리오에 대해 설명합니다.

- 35 페이지 "추가 Access Manager 인스턴스 배포"

추가 Access Manager 인스턴스 배포

Access Manager의 새 인스턴스를 배포하려면 먼저 웹 컨테이너용 관리 도구를 사용하여 새 웹 컨테이너 인스턴스를 만들고 시작해야 합니다. 자세한 내용은 특정 웹 컨테이너 설명서를 참조하십시오.

- Web Server에 대한 내용은 `http://docs.sun.com/coll/1308.1` 및 `http://docs.sun.com/coll/1410.1`을 참조하십시오.
- Application Server에 대한 내용은 `http://docs.sun.com/coll/1310.1` 및 `http://docs.sun.com/coll/1401.1`을 참조하십시오.

이 절에서 설명한 단계는 지금 구성 옵션으로 설치한 Access Manager 인스턴스에만 적용됩니다. WebLogic 또는 WebSphere를 웹 컨테이너로 사용하려면 Access Manager를 설치할 때 나중에 구성 옵션을 사용해야 합니다. 자세한 내용은 2 장을 참조하십시오.

추가 Access Manager 인스턴스 배포

이 절에서는 다른 호스트 서버에 추가 Access Manager 인스턴스를 배포하는 방법과 플랫폼 서버 목록을 업데이트하는 방법에 대해 설명합니다.

▼ 추가 Access Manager 인스턴스를 배포하려면

1 인스턴스의 웹 컨테이너에 따라 관리자로 로그인합니다. 예를 들어, Web Server 6.1이 새 인스턴스의 웹 컨테이너인 경우에는 수퍼유저(루트) 또는 Web Server Administration Server의 사용자 계정 중 하나로 로그인합니다.

2 `amsamplesilent` 파일을 쓰기 가능한 디렉토리에 복사하고 그 디렉토리를 현재 디렉토리로 만듭니다. 예를 들어, `/newinstances`라는 이름의 디렉토리를 만들 수 있습니다.

팁: `amsamplesilent` 파일의 복사본 이름을 배포하려는 새 인스턴스를 설명하는 이름으로 바꿉니다. 예를 들어, 다음 단계부터는 `amnewws6instance`라는 이름의 입력 파일을 사용하여 Web Server 6.1을 위해 새 인스턴스를 설치할 수 있습니다.

3 새 `amnewws6instance` 파일에서 다음 변수를 설정합니다.

```
DEPLOY_LEVEL=1
 NEW_INSTANCE=true
```

만들려는 새 인스턴스를 위해 필요한 `amnewws6instance` 파일의 다른 변수를 설정합니다. 각 변수에 대한 설명은 다음 절의 표를 참조하십시오.

- 32 페이지 “Directory Server 구성 변수”

  중요 모든 Access Manager 인스턴스는 동일한 비밀번호 암호화 키 값을 사용해야 합니다. 이 인스턴스에 대한 AM_ENC_PWD 변수를 설정하려면 첫 번째 인스턴스에 대한 `AMConfig.properties` 파일의 `am.encryption.pwd` 등록 정보에서 값을 복사합니다.

  나중에 이 인스턴스를 제거할 필요가 있을 경우를 대비해 `amnewws6instance` 파일을 저장해 둡니다.

4 **`amconfig`를 실행하여 새 `amnewws6instance` 파일을 지정합니다. 예를 들면 Solaris 시스템의 경우 다음과 같습니다.**

```
# cd opt/SUNWam/bin/
 # ./amconfig -s ./newinstances/amnewws6instance
```

`-s` 옵션은 `amconfig` 스크립트를 자동 설치 모드로 실행합니다.

`amconfig` 스크립트는 `amnewws6instance` 파일의 변수를 사용하여 새 인스턴스를 배포하는 데 필요한 다른 구성 스크립트를 호출합니다.

▼ 플랫폼 서버 목록을 업데이트하려면

추가 컨테이너 인스턴스를 만드는 경우 Access Manager 플랫폼 서버 목록을 업데이트하여 추가된 컨테이너를 반영하도록 해야 합니다.

1 **Access Manager 콘솔에 최상위 관리자로 로그인합니다.**

2 **서비스 구성 탭을 누릅니다.**

3 **플랫폼 서비스를 누릅니다.**

4 **서버 목록의 새 인스턴스에 대해 다음 정보를 입력합니다.**

protocol`://`*fqdn*`:`*port*`|`*instance-number*

인스턴스 번호는 사용 가능한 다음 번호로, 현재 사용 중이 아니어야 합니다.

5 **추가를 누릅니다.**

6 **저장을 누릅니다.**

Access Manager 인스턴스 구성 및 재구성

나중에 구성 옵션으로 설치한 Access Manager의 인스턴스를 구성하거나 Java Enterprise System 설치 프로그램의 지금 구성 옵션을 사용하여 설치한 첫 번째 인스턴스를 `amconfig` 스크립트를 실행하여 재구성할 수 있습니다.

예를 들어, 인스턴스를 재구성하여 Access Manager 소유자 및 그룹을 변경할 수 있습니다.

▼ Access Manager 인스턴스를 구성 또는 재구성하려면

1 **인스턴스의 웹 컨테이너에 따라 관리자로 로그인합니다. 예를 들어, Web Server 6.1이 웹 컨테이너인 경우 수퍼유저(루트) 또는 Web Server Administration Server를 위한 사용자 계정 중 하나로 로그인합니다.**

2 **인스턴스를 배포하는 데 사용한 자동 구성 입력 파일을 쓰기 가능한 디렉토리에 복사하고 그 디렉토리를 현재 디렉토리로 만듭니다. 예를 들어, Web Server 6.1용 인스턴스를 재구성하려면 다음 단계부터 `/reconfig` 디렉토리에 있는 `amnewinstanceforWS61`이라는 이름의 입력 파일을 사용합니다.**

3 `amnewinstanceforWS61` **파일에서 DEPLOY_LEVEL 변수를** **23 페이지 "배포 모드 변수"** **작업을 위해 설명한 변수 중 하나로 설정합니다. 예를 들어, 전체 설치를 재구성하려면 DEPLOY_LEVEL=21로 설정합니다.**

4 `amnewinstanceforWS61` **파일에서 NEW_INSTANCE 변수를 false로 설정합니다.**

```
NEW_INSTANCE=false
```

5 `amnewinstanceforWS61` **파일에서 인스턴스를 재구성하는 데 필요한 다른 변수를 설정합니다. 예를 들어, 인스턴스의 소유자와 그룹을 변경하려면 NEW_OWNER 및 NEW_GROUP 변수를 새로운 값으로 설정합니다.**

다른 변수에 대한 설명은 다음 절의 표를 참조하십시오.

- 24 페이지 "Access Manager 구성 변수"
  - 28 페이지 "웹 컨테이너 구성 변수"
  - 32 페이지 "Directory Server 구성 변수"

6 **편집된 입력 파일을 지정하여** `amconfig` **스크립트를 실행합니다. 예를 들면 Solaris 시스템의 경우 다음과 같습니다.**

```
# cd opt/SUNWam/bin/
 # ./amconfig -s ./reconfig/amnewinstanceforWS61
```

`-s` 옵션은 스크립트를 자동 설치 모드로 실행합니다. `amconfig` 스크립트는 `amnewinstanceforWS61` 파일의 변수를 사용하여 인스턴스를 재구성하는 데 필요한 다른 구성 스크립트를 호출합니다.

Access Manager 제거

`amconfig` 스크립트를 실행하여 설치한 Access Manager의 인스턴스를 제거할 수 있습니다. 또한 임시적으로 Access Manager 인스턴스의 구성을 해제할 수 있으며, 구성 해제한 Access Manager 인스턴스는 웹 컨테이너 인스턴스를 제거하지 않는 한 나중에 다른 Access Manager 인스턴스를 재배포하는 데 사용할 수 있습니다.

▼ Access Manager 인스턴스를 제거하려면

1 **인스턴스의 웹 컨테이너에 따라 관리자로 로그인합니다. 예를 들어, Web Server 6.1이 웹 컨테이너인 경우 수퍼유저(루트) 또는 Web Server Administration Server를 위한 사용자 계정 중 하나로 로그인합니다.**

2 **인스턴스를 배포하는 데 사용한 자동 구성 입력 파일을 쓰기 가능한 디렉토리에 복사하고 그 디렉토리를 현재 디렉토리로 만듭니다. 예를 들어, Web Server 6.1용 인스턴스의 구성을 해제하려면 다음 단계부터 `/unconfigure` 디렉토리에 있는 `amnewinstanceforWS61`이라는 이름의 입력 파일을 사용합니다.**

3 `amnewinstanceforWS61` **파일에서 DEPLOY_LEVEL 변수를** **23 페이지 "배포 모드 변수"** **작업을 위해 설명한 변수 중 하나로 설정합니다. 예를 들어, 전체 설치를 제거하거나 구성 해제하려면 DEPLOY_LEVEL=11로 설정합니다.**

4 **편집된 입력 파일을 지정하여** `amconfig` **스크립트를 실행합니다. 예를 들면 Solaris 시스템의 경우 다음과 같습니다.**

```
# cd opt/SUNWam/bin/
 # ./amconfig -s ./unconfigure/aminstanceforWS61
```

`-s` 옵션은 스크립트를 자동 설치 모드로 실행합니다. `amconfig` 스크립트는 `amnewinstanceforWS61` 파일을 읽은 다음 해당 인스턴스를 제거합니다.

웹 컨테이너 인스턴스는 나중에 다른 Access Manager 인스턴스를 재배포하는 데 사용할 수 있습니다.

모든 Access Manager 인스턴스 제거

이 시나리오는 컴퓨터에서 모든 Access Manager 7 2005Q4 인스턴스와 패키지를 완전히 제거합니다.

▼ 컴퓨터에서 Access Manager 7 2005Q4를 완전히 제거하려면

1 **수퍼유저(root)로 로그인하거나 수퍼유저가 됩니다.**

2 **인스턴스를 배포하는 데 사용한 입력 파일에서 DEPLOY_LEVEL 변수를** **23 페이지 "배포 모드 변수"** **작업을 위해 설명한 변수 중 하나로 설정합니다. 예를 들어, 전체 설치를 제거하거나 구성 해제하려면 DEPLOY_LEVEL=11로 설정합니다.**

3 **38 페이지 "모든 Access Manager 인스턴스 제거"****에서 편집한 파일을 사용하여** `amconfig` **스크립트를 실행합니다. 예를 들어, Solaris 시스템에서는 다음과 같이 합니다.**

```
# cd opt/SUNWam/bin/
# ./amconfig -s ./newinstances/amnewws6instance
```

`amconfig` 스크립트는 자동 설치 모드로 실행되어 인스턴스를 제거합니다.

Java Enterprise System 설치 프로그램을 사용하여 설치한 첫 번째 인스턴스를 제외하고 제거하려는 다른 Access Manager 인스턴스에 대해 이러한 단계를 반복합니다.

4 **첫 번째 인스턴스를 제거하고 모든 Access Manager 패키지를 시스템에서 제거하려면 Java Enterprise System 제거 프로그램을 실행합니다. 제거 프로그램에 대한 자세한 내용은 Sun Java Enterprise System 2005Q4 Installation Guide for UNIX를 참조하십시오.**

예제 구성 스크립트 입력 파일

다음 절에서는 WebLogic 8.1로 배포하는 경우의 Access Manager 구성 스크립트 입력 파일 예제를 제공합니다.

```
DEPLOY_LEVEL=1
BASEDIR=/opt
SERVER_HOST=ide-56.example.company.com
SERVER_PORT=7001
SERVER_PROTOCOL=http
CONSOLE_HOST=$SERVER_HOST
CONSOLE_PORT=$SERVER_PORT
CONSOLE_PROTOCOL=$SERVER_PROTOCOL
CONSOLE_REMOTE=false
DS_HOST=ide-56.example.company.com
DS_PORT=389
DS_DIRMGRDN=”cn=Directory Manager”
DS_DIRMGRPASSWD=11111111
ROOT_SUFFIX=”dc=company,dc=com”
ADMINPASSWD=11111111
AMLDAPUSERPASSWD=00000000
CONSOLE_DEPLOY_URI=/amconsole
SERVER_DEPLOY_URI=/amserver
PASSWORD_DEPLOY_URI=/ampassword
COMMON_DEPLOY_URI=/amcommon
COOKIE_DOMAIN=.iplanet.com
JAVA_HOME=/usr/jdk/entsys-j2se
AM_ENC_PWD=””
PLATFORM_LOCALE=en_US
NEW_OWNER=root
NEW_GROUP=other
XML_ENCODING=ISO-8859-1
NEW_INSTANCE=false
WEB_CONTAINER=WL8
WL8_HOME=/export/bea8
WL8_PROJECT_DIR=user_projects
WL8_DOMAIN=mydomain
WL8_CONFIG_LOCATION=$WL8_HOME/$WL8_PROJECT_DIR/domains
WL8_SERVER=myserver
```

```
WL8_INSTANCE=/export/bea8/weblogic81
WL8_PROTOCOL=http
WL8_HOST=ide-56.example.company.com
WL8_PORT=7001
WL8_SSLPORT=7002
WL8_ADMIN=”weblogic”
WL8_PASSWORD=”11111111”
WL8_JDK_HOME=$WL8_HOME/jdk142_04
DIRECTORY_MODE=1
USER_NAMING_ATTR=uid
ORG_NAMING_ATTR=o
ORG_OBJECT_CLASS=examplemanagedorganization
USER_OBJECT_CLASS=inetorgperson
DEFAULT_ORGANIZATION=
Sample Configuration Script Input File for WebLogic 8.1.x
```

◆ ◆ ◆ 2 장

2 타사 웹 컨테이너 설치 및 구성

이 장에서는 Sun Java™ System Access Manager와 함께 배포되는 타사 웹 컨테이너의 설치 및 구성 절차를 설명합니다. 이 릴리스에서 Access Manager는 BEA WebLogic 8.1(현재 패치 포함) 및 IBM WebSphere 5.1(현재 패치 포함)을 지원합니다.

WebLogic 및 WebSphere는 Java Enterprise System에 포함되지 않으므로 Java ES 설치 프로그램과 별개로 설치하고 구성해야 합니다. 일반적인 절차는 다음과 같습니다.

- 웹 컨테이너 인스턴스를 설치 및 구성한 다음 시작합니다.
- Java ES 설치 프로그램에서 Directory Server를 설치합니다.
- Java ES 설치 프로그램에서 나중에 구성 모드로 Access Manager를 설치하여 Access Manager를 구성되지 않은 상태로 둡니다.
- Access Manager 구성 스크립트를 실행하여 웹 컨테이너에 Access Manager를 배포합니다.
- 웹 컨테이너를 다시 시작합니다.

BEA WebLogic 8.1 설치 및 구성

WebLogic을 설치하기 전에 DNS에 호스트 도메인이 등록되어 있는지 확인합니다. 또한 설치하려는 WebLogic 소프트웨어가 올바른 버전인지 확인합니다. 자세한 내용은 BEA 제품 사이트 http://commerce.bea.com/index.jsp를 참조하십시오.

▼ WebLogic 8.1을 설치 및 구성하려면

1 **다운로드한 소프트웨어 이미지(`.zip` 또는 `.gz` 형식)의 압축을 풉니다. zip/gzip 유틸리티가 해당 플랫폼용인지 확인해야 합니다. 그렇지 않으면 압축을 해제하는 동안 체크섬 오류가 발생할 수 있습니다.**

2 **대상 시스템의 쉘 창에서 설치 프로그램을 실행합니다.**

WebLogic 설치 유틸리티에서 제공하는 절차를 따릅니다. 자세한 설치 방법은 http://e-docs.bea.com/wls/docs81/을 참조하십시오.

설치 과정이 진행되는 동안 나중에 Access Manager 구성 시 사용할 수 있도록 다음 정보를 기록해야 합니다.

- FQDN(WL8_HOST 매개 변수에 사용)
  - 설치 위치
  - 포트 번호

3 설치가 완료되면 WebLogic 구성 도구를 실행하여 다음 위치에서 도메인 및 서버 인스턴스를 구성합니다.

WebLogic-base/WebLogic-instance/common/bin/quickstart.sh

기본적으로 WebLogic은 서버 인스턴스를 myserver로 정의하고 도메인을 mydomain으로 정의합니다. 대체로 이 기본값을 사용하지는 않습니다. 새 도메인 및 인스턴스를 만들 경우 Access Manager 구성 및 배포에 대한 정보를 기록해야 합니다. 자세한 내용은 WebLogic 8.1 설명서를 참조하십시오.

4 관리 인스턴스에서 설치 중인 경우 다음 위치에서 startWebLogic.sh 유틸리티를 사용하여 WebLogic을 시작합니다.

WebLogic-base/WebLogic-Userhome /domains/ *WebLogic-domain*/startWebLogic.sh

관리된 인스턴스에서 설치 중인 경우 다음 명령을 사용하여 WebLogic을 시작합니다.

WebLogic-base /WebLogic-Userhome/domains/ WebLogic-domain /startManagedWebLogic WebLogic-managed-instancename admin-url

IBM WebSphere 5.1 설치 및 구성

WebSphere를 설치하기 전에 DNS에 호스트 도메인이 등록되어 있고 플랫폼에 올바른 WebSphere 소프트웨어 버전을 설치하고 있는지 확인해야 합니다. 자세한 내용은 IBM 제품 지원 웹 사이트 http://www-306.ibm.com/software/websphere/support/를 참조하십시오.

▼ WebSphere 5.1을 설치 및 구성하려면

1 다운로드한 소프트웨어 이미지(.zip 또는 .gz 형식)의 압축을 풉니다. zip/gzip 유틸리티가 해당 플랫폼용인지 확인해야 합니다. 그렇지 않으면 압축을 해제하는 동안 체크섬 오류가 발생할 수 있습니다.

2 대상 시스템의 쉘 창에서 설치 프로그램을 실행합니다. 패치를 설치하려면 먼저 5.1 버전을 설치하고 나중에 패치를 적용하십시오. 자세한 설치 방법은 http://publib.boulder.ibm.com/infocenter/ws51help/index.jsp를 참조하십시오.

설치 과정이 진행되는 동안 나중에 Access Manager 구성 시 사용할 수 있도록 다음 정보를 기록해야 합니다.

- 호스트 이름

- 도메인 이름
- 셀 이름
- 노드 이름
- 포트 번호
- 설치 디렉토리
- WebSphere 인스턴스 이름
- 관리 포트

  기본적으로 WebSphere는 서버 인스턴스를 `server1`로 정의하지만 대체로 이 기본값을 사용하지는 않습니다. 새 인스턴스를 만들 경우 Access Manager 구성 및 배포에 대한 정보를 기록해야 합니다. 자세한 내용은 WebSphere 5.1 설명서를 참조하십시오.

3 설치가 성공했는지 확인합니다.

a. 다음 디렉토리에 `server.xml` 파일이 있는지 확인합니다.

```
/opt/WebSphere/AppServer/config/cells/cell-name/noes/

node-name/servers/server1
```

b. 다음과 같이 `startServer.sh` 명령을 사용하여 서버를 시작합니다.

```
/opt/WebSphere/AppServer/bin/startServer.sh server1
```

c. 웹 브라우저에 다음과 같은 형식으로 해당 URL을 입력하여 샘플 웹 응용 프로그램을 봅니다.

`http://` *fqdn:portnumber/snoop*

4 성공적으로 설치됐는지 확인했으면 `stopServer.sh` 유틸리티를 사용하여 서버를 중지합니다. 예를 들면 다음과 같습니다.

```
opt/WebSphere/AppServer/bin/stopServer.sh server1
```

5 WebSphere 5.1 패치를 설치하는 경우 `updateWizard.sh` 명령줄 유틸리티를 사용하여 기존의 5.1 인스턴스에 패치를 설치합니다.

6 WebSphere를 다시 시작하고 성공적으로 설치되었는지 확인합니다.

Java ES를 사용하여 Directory Server 및 Access Manager 설치

Access Manager를 설치하려면 Java ES(Java Enterprise System) 설치 프로그램을 별도로 두 번 호출해야 합니다.

▼ Directory Server를 설치하려면

1 **첫 번째 Java ES 호출을 실행하여 지금 구성 옵션으로 Directory Server(로컬 또는 원격)를 설치합니다. 지금 구성 옵션을 선택하면 설치 시 사용자가 선택한 옵션(또는 기본값)으로 첫 번째 인스턴스를 구성할 수 있습니다.**

2 **두 번째 Java ES 호출을 실행하여 나중에 구성 옵션으로 Access Manager를 설치합니다. 이 옵션은 Access Manager 2005Q4 구성 요소를 설치합니다. 설치 후에 Access Manager를 구성해야 합니다.**

WebLogic 및 WebSphere는 Java ES와 별도로 설치되므로 설치 프로그램에는 컨테이너를 자동으로 배포할 수 있는 필수 구성 데이터가 없습니다. 그러므로 Access Manager를 설치할 때는 나중에 구성 옵션을 선택해야 합니다. 이 옵션을 사용하면 Access Manager가 다음과 같은 상태로 배포됩니다.

- 활성 Directory Server(로컬 또는 원격)에 Access Manager DIT 데이터가 로드되지 않습니다.
- Access Manager 구성 파일이 자동으로 로드되지 않습니다.
- Access Manager 웹 응용 프로그램 `.war` 파일이 생성되지 않습니다.
- Access Manager 배포 및 설치 후 구성 프로세스가 자동으로 시작 및 실행되지 않습니다.

  자세한 설치 방법은 http://docs.sun.com/doc/819-0056에 있는 Sun Java Enterprise System 설치 설명서를 참조하십시오.

Access Manager 구성

대상 시스템의 로컬 드라이브에 Access Manager 설치를 완료한 후 WebLogic 8.1 또는 WebSphere 5.1을 사용하여 Access Manager를 수동으로 구성해야 합니다. 이 작업에는 세 단계가 필요합니다.

▼ Access Manager를 구성하려면

1 **구성 스크립트 입력 파일 편집**

2 **구성 스크립트 실행**

3 **웹 컨테이너 다시 시작**

구성 스크립트 입력 파일 만들기

Access Manager 구성 스크립트 입력 파일에는 모든 배포 수준, Access Manager, 웹 컨테이너 및 Directory Server 변수 정의가 포함되어 있습니다. Access Manager에는 Solaris 시스템의 *AccessManager-base*`/SUNWam/bin` 디렉토리 또는 Linux 시스템의

AccessManager-base/identity/bin디렉토리에서 사용할 수 있는 샘플 구성 스크립트 입력 파일 템플리트(amsamplesilent)가 포함되어 있습니다.

amsamplesilent 템플리트를 사용하여 구성 스크립트 입력 파일을 만들 수 있습니다. 변수 정의를 비롯한 파일 편집 방법은 23 페이지 “Access Manager 샘플 구성 스크립트 입력 파일”을 참조하십시오.

파일을 편집하기 전에 웹 컨테이너 설치 프로그램에서 다음 정보를 확인하십시오.

BEA WebLogic 및 IBM WebSphere

- 설치 위치
- 인스턴스 이름 및 위치
- 호스트 이름
- FQDN
- 수신 중인 포트 번호
- 관리 아이디
- 사용된 프로토콜

BEA WebLogic 전용

- 관리 비밀번호
- 공유 라이브러리 위치
- 도메인 이름 및 위치
- 프로젝트 디렉토리 이름
- JDK 위치

IBM WebSphere 전용

- 셀 이름
- 노드 이름
- JDK 위치

구성 스크립트 실행

구성 스크립트 입력 파일을 저장했으면 amconfig 스크립트를 실행하여 구성 프로세스를 완료합니다. 예를 들면 다음과 같습니다.

```
AccessManager-base/SUMWam/bin/amconfig -s silentfile
```

silentfile은 구성 입력 파일에 대한 절대 경로여야 합니다.

이 스크립트를 실행하면 다음 기능이 수행됩니다.

1. 활성 Directory Server 인스턴스에 Access Manager 스키마를 로드합니다.
2. Directory Server 인스턴스에 Access Manager 서비스 데이터를 로드합니다.

3. 활성 Access Manager 인스턴스에서 사용되는 Access Manager 구성 파일을 생성합니다.
4. 웹 컨테이너에 Access Manager 웹 응용 프로그램 데이터를 배포합니다.
5. 웹 컨테이너 구성을 Access Manager 요구 사항과 일치하도록 사용자 정의합니다.

웹 컨테이너 다시 시작

구성 프로세스를 완료한 후 웹 컨테이너를 다시 시작해야 합니다. 자세한 방법은 제품 설명서를 참조하십시오.

BEA WebLogic 8.1에 대한 자세한 내용은 http://e-docs.bea.com/wls/docs81을 참조하십시오.

IBM WebSphere 5.1에 대한 자세한 내용은 http://publib.boulder.ibm.com/infocenter/ws51help/index.jsp를 참조하십시오.

◆ ◆ ◆ 3 장

3 SSL 모드에서 Access Manager 구성

단순 인증에서 SSL(Secure Socket Layer)을 사용하면 기밀성과 데이터 무결성이 보장됩니다. Access Manager를 SSL 모드에서 사용하려면 일반적으로 다음을 수행해야 합니다.

- 보안 웹 컨테이너를 사용하여 Access Manager 구성
- Access Manager를 보안 Directory Server로 구성

보안 Sun Java Enterprise System Web Server를 사용하여 Access Manager 구성

Web Server를 사용하여 SSL 모드에서 Access Manager를 구성하려면 다음 단계를 참조하십시오.

▼ 보안 Web Server를 구성하려면

1 **Access Manager 콘솔에서 서비스 구성 모듈로 이동하여 플랫폼 서비스를 선택합니다. 서버 목록 속성에서 `http://` 프로토콜을 제거하고 `https://` 프로토콜을 추가합니다. 저장을 누릅니다.**

주 – 저장을 눌러야 합니다. 저장을 누르지 않더라도 다음 단계를 계속할 수 있지만 모든 구성 변경 내용이 손실되고 관리자로 로그인하여 해당 문제를 해결할 수 없습니다.

2단계부터 24단계까지는 Web Server에 대한 설명입니다.

2 **Web Server 콘솔에 로그온합니다. 기본 포트는 8888입니다.**

3 **Access Manager가 실행 중인 Web Server 인스턴스를 선택하고 관리를 누릅니다.**
구성이 변경되었다는 메시지가 있는 팝업 창이 표시됩니다. 확인을 누릅니다.

4 **화면의 오른쪽 위 모서리에 있는 적용 버튼을 누릅니다.**

5 **변경 내용 적용을 누릅니다.**
Web Server가 자동으로 다시 시작되어야 합니다. 확인을 눌러 계속합니다.

6 **선택한 Web Server 인스턴스를 중지합니다.**

7 **보안 탭을 누릅니다.**

8 **데이터베이스 만들기를 누릅니다.**

9 **새 데이터베이스 비밀번호를 입력하고 확인을 누릅니다.**
나중에 사용할 수 있도록 데이터베이스 비밀번호를 기록해 두십시오.

10 **인증서 데이터베이스를 작성한 후 인증서 요청을 누릅니다.**

11 **화면에 제공된 필드에 데이터를 입력합니다.**
키 쌍 파일 비밀번호 필드는 9단계에서 입력한 내용과 같습니다. 위치 필드에 위치를 정확하게 입력해야 합니다. CA와 같은 약어는 사용할 수 없습니다. 모든 필드를 정의해야 합니다. 공통 이름 필드에 Web Server의 호스트 이름을 입력합니다.

12 **양식이 제출되면 다음과 같은 메시지가 표시됩니다.**

```
--BEGIN CERTIFICATE REQUEST---

afajsdllwqeroisdaoi234rlkqwelkasjlasnvdknbslajowijalsdkjfalsdflasdf

alsfjawoeirjoi2ejowdnlkswnvnwofijwoeijfwiepwerfoiqeroijeprwpfrwl

--END CERTIFICATE REQUEST--
```

13 **이 텍스트를 복사하여 인증서를 요청할 때 제출합니다.**
루트 CA 인증서를 가져와야 합니다.

14 **인증서가 포함된 다음과 같은 인증서 응답을 받게 됩니다.**

```
--BEGIN CERTIFICATE---

afajsdllwqeroisdaoi234rlkqwelkasjlasnvdknbslajowijalsdkjfalsdflasdf

alsfjawoeirjoi2ejowdnlkswnvnwofijwoeijfwiepwerfoiqeroijeprwpfrwl

--END CERTIFICATE---
```

15 **이 텍스트를 클립보드에 복사하거나 파일로 저장합니다.**

16 **Web Server 콘솔로 이동하여 인증서 설치를 누릅니다.**

17 **이 서버의 인증서를 클릭합니다.**

18 **키 쌍 파일 비밀번호 필드에 인증서 데이터베이스 비밀번호를 입력합니다**

19 **인증서를 제공된 텍스트 필드에 붙여 넣거나 라디오 버튼을 누르고 텍스트 상자에 파일 이름을 입력합니다. 제출을 누릅니다.**
브라우저에 인증서가 표시되고 인증서를 추가하기 위한 버튼이 제공됩니다.

20 **인증서 설치를 누릅니다.**

21 **신뢰할 수 있는 인증 기관에 대한 인증서를 누릅니다.**

22 **16단계부터 21단계까지 설명된 것과 동일한 방법으로 루트 CA 인증서를 설치합니다.**

23 **두 인증서가 모두 설치되면 Web Server 콘솔의 기본 설정 탭을 누릅니다.**

24 **SSL을 다른 포트에서 사용 가능하게 하려면 수신 소켓 추가를 선택합니다. 그런 다음 수신 소켓 편집을 선택합니다.**

25 **보안 상태를 사용 불가능에서 사용 가능으로 변경하고 확인을 눌러 변경 내용을 제출하고 적용을 누르고 변경 내용 적용을 누릅니다.**
26–29 단계는 Access Manager에 적용됩니다.

26 **`AMConfig.properties` 파일을 엽니다. 기본적으로 이 파일의 위치는 `etc/opt/SUNWam/config`입니다.**

27 **Web Server 인스턴스 디렉토리를 제외하고 `http://`의 모든 프로토콜 항목을 `https://`로 교체합니다. Web Server 인스턴스 디렉토리도 `AMConfig.properties`에 지정되어 있지만 그대로 유지되어야 합니다.**

28 **`AMConfig.properties` 파일을 저장합니다.**

29 **Web Server 콘솔에서 Web Server 인스턴스를 호스트하는 Access Manager에 대한 설정/해제 버튼을 누릅니다.**
Web Server의 시작/중지 페이지에 입력란이 표시됩니다.

30 **텍스트 필드에 인증서 데이터베이스 비밀번호를 입력하고 시작을 선택합니다.**

보안 Sun Java System Application Server를 사용하여 Access Manager 구성

SSL을 사용하는 Application Server에서 실행하도록 Access Manager를 설정하려면 두 단계를 거칩니다. 먼저 설치된 Access Manager에 대한 Application Server 인스턴스에 보안을 설정한 다음 Access Manager를 구성합니다.

SSL을 사용하여 Application Server 6.2 설정

이 장에서는 SSL 모드에서 Application Server 6.2를 설정하는 단계에 대해 설명합니다.

▼ Application Server 인스턴스에 보안을 설정하려면

1. **브라우저에 다음 주소를 입력하여 Sun Java System Application Server 콘솔에 관리자로 로그인합니다.**

   ```
   http://fullservername:port
   ```

   기본 포트는 4848입니다.

2. **설치하는 동안 입력한 아이디와 비밀번호를 입력합니다.**

3. **Access Manager를 설치했거나 설치할 Application Server 인스턴스를 선택합니다. 오른쪽 프레임에 구성이 변경되었다는 메시지가 표시됩니다.**

4. **변경 내용 적용을 누릅니다.**

5. **다시 시작을 누릅니다. Application Server가 자동으로 다시 시작되어야 합니다.**

6. **왼쪽 프레임에서 보안을 누릅니다.**

7. **데이터베이스 관리 탭을 누릅니다.**

8. **데이터베이스 만들기를 누릅니다(선택하지 않은 경우).**

9. **새 데이터베이스 비밀번호를 입력하고 확인한 다음 확인 버튼을 누릅니다. 나중에 사용할 수 있도록 데이터베이스 비밀번호를 기록해 두십시오.**

10. **인증서 데이터베이스를 작성한 후 인증서 관리 탭을 누릅니다.**

11. **요청 링크를 누릅니다(선택하지 않은 경우).**

12 인증서에 대해 다음 요청 데이터를 입력합니다.

a. 새 인증서인지 인증서 업데이트인지를 선택합니다. 특정 기간이 경과하면 많은 인증서가 만료되고 일부 인증 기관(CA)에서는 업데이트 알림을 자동으로 보냅니다.

b. 인증서에 대한 요청을 제출할 방법을 지정합니다.

CA가 전자 메일 메시지로 요청을 받는 경우 CA 전자 메일을 선택하고 CA의 전자 메일 주소를 입력합니다. CA 목록에서 사용 가능한 인증 기관 목록을 누릅니다.

Certificate Server를 사용하는 내부 CA로부터 인증서를 요청할 경우 CA URL을 누르고 Certificate Server에 대한 URL을 입력합니다. 이 URL은 인증서 요청을 처리하는 인증서 서버의 프로그램을 가리키는 URL이어야 합니다.

c. 키 쌍 파일에 대한 비밀번호(9단계에서 지정한 비밀번호)를 입력합니다.

d. 다음 식별 정보를 입력합니다.

공통 이름. 포트 번호를 포함하여 서버의 전체 이름입니다.

요청자 이름. 요청자의 이름입니다.

전화 번호. 요청자의 전화 번호입니다.

공통 이름 . 디지털 인증서를 설치할 Sun Java System Application Server의 정규화된 이름입니다.

전자 메일 주소. 관리자의 전자 메일 주소입니다.

조직 이름.조직의 이름입니다. 인증 기관은 이 조직에 등록된 도메인에 속하는 이 속성에 입력된 호스트 이름을 요구할 수 있습니다.

조직 구성 단위 이름. 과, 부서 및 기타 조직 운영 단위의 이름입니다.

구/군/시 이름. 사용자의 구/군/시 이름입니다.

시/도 이름.조직이 미국 또는 캐나다에 있는 경우 각각 조직이 운영되는 시 또는 도의 이름입니다. 약어를 사용하지 마십시오.

국가 코드. 국가에 대한 2문자 ISO 코드입니다. 예를 들어, 미국의 국가 코드는 US입니다.

13 확인 버튼을 누릅니다. 메시지가 표시됩니다. 예를 들면 다음과 같습니다.

```
--BEGIN NEW CERTIFICATE REQUEST---
afajsdllwqeroisdaoi234rlkqwelkasjlasnvdknbslajowijalsdkjfalsdfla
alsfjawoeirjoi2ejowdnlkswnvnwofijwoeijfwiepwerfoiqeroijeprwpfrwl
--END NEW CERTIFICATE REQUEST--
```

14 이 텍스트를 모두 파일에 복사하고 확인을 누릅니다. 루트 CA 인증서를 가져와야 합니다.

15 디지털 인증서를 가져오려면 CA를 선택하고 해당 기관 웹 사이트의 지침을 따릅니다. CMS, Verisign 또는 Entrust.net에서 인증서를 가져올 수 있습니다.

16 인증 기관으로부터 디지털 인증서를 받은 후 텍스트를 클립보드에 복사하거나 파일로 저장할 수 있습니다.

17 Application Server 콘솔로 이동하여 설치 링크를 누릅니다.

18 이 서버에 대한 인증서를 선택합니다.

19 키 쌍 파일 비밀번호 필드에 인증서 데이터베이스 비밀번호를 입력합니다

20 인증서를 제공된 텍스트 필드인 메시지 텍스트(헤더 있음)에 붙여 넣거나 이 파일 입력란에 있는 메시지에 파일 이름을 입력합니다. 해당 라디오 버튼을 선택합니다.

21 확인 버튼을 누릅니다. 브라우저에 인증서가 표시되고 인증서를 추가할 수 있는 버튼이 제공됩니다.

22 서버 인증서 추가를 누릅니다.

23 위에 설명된 것과 동일한 방법으로 루트 CA 인증서를 설치합니다. 그러나 신뢰할 수 있는 인증 기관에 대한 인증서를 선택하십시오.

24 인증서 설치가 완료된 경우 왼쪽 프레임에서 HTTP Server 노드를 확장합니다.

25 HTTP Server에서 HTTP Listeners를 선택합니다.

26 http-listener-1을 선택합니다. 브라우저에 소켓 정보가 표시됩니다.

27 http-listener-1에 사용되는 포트 값을 응용 프로그램 서버를 설치하는 동안 입력한 값에서 해당 값(예: 443)으로 변경합니다.

28 SSL/TLS 사용 가능을 선택합니다.

29 인증서 별명을 선택합니다.

30 반환 서버를 지정합니다. 이 이름은 12단계에 지정된 공통 이름과 일치해야 합니다.

31 저장을 누릅니다.

32 Access Manager 소프트웨어를 설치할 Application Server 인스턴스를 선택합니다. 오른쪽 프레임에 구성이 변경되었다는 메시지가 표시됩니다.

33 변경 내용 적용을 누릅니다.

34 다시 시작을 누릅니다. 응용 프로그램 서버가 자동으로 다시 시작됩니다.

SSL을 사용하여 Application Server 8.1 구성

SSL을 사용하여 Application Server 8.1을 구성하는 기본 단계는 다음과 같습니다. 자세한 내용은 Application Server 8.1 설명서를 참조하십시오.

1. Application Server 관리 콘솔을 통해 Application Server에 보안 포트를 만듭니다. 자세한 내용은 다음 위치에 있는 Sun Java System Application Server Enterprise Edition 8.1 관리 설명서의 "보안 구성"을 참조하십시오.

   `http://docs.sun.com/app/docs/coll/1310.1` 및
   `http://docs.sun.com/app/docs/coll/1401.1`
2. 웹 컨테이너 트러스트 데이터베이스에 있는 서버 인증서를 신뢰하는 인증 기관(CA)을 확인하십시오. 그런 다음 웹 컨테이너의 서버 인증서를 가져와서 설치합니다. 자세한 내용은 다음 위치에 있는 Sun Java System Application Server Enterprise Edition 8.1 관리 설명서의 "인증서 및 SSL을 사용한 작업"을 참조하십시오.

   `http://docs.sun.com/app/docs/coll/1310.1` 및
   `http://docs.sun.com/app/docs/coll/1401.1`
3. 웹 컨테이너를 다시 시작합니다.

SSL 모드에서 Access Manager 구성

이 절에서는 SSL 모드에서 Access Manager를 구성하는 단계에 대해 설명합니다. Access Manager용 SSL을 설정하기 전에 배포를 위한 웹 컨테이너를 구성했는지 확인합니다.

▼ SSL 모드에서 Access Manager를 구성하려면

1 Access Manager 콘솔에서 서비스 구성 모듈로 이동하여 플랫폼 서비스를 선택합니다. 서버 목록 속성에서 HTTPS 프로토콜과 동일한 URL 및 SSL 사용 가능 포트 번호를 추가합니다. 저장을 누릅니다.

주 – 단일 Access Manager 인스턴스가 HTTP와 HTTPS 각각 하나씩 두 개의 포트를 수신하고 있고 쿠키를 사용하여 Access Manager에 액세스하려고 시도할 경우 Access Manager는 응답하지 않는 상태가 됩니다. 이러한 구성은 지원되지 않습니다.

---

2 다음 기본 위치에서 `AMConfig.properties` 파일을 엽니다.

`/etc/opt/SUNWam/config`.

3 `http://`의 모든 프로토콜 항목을 `https://`로 교체하고 포트 번호를 SSL 사용 가능 포트 번호로 변경합니다.

4 `AMConfig.properties` 파일을 저장합니다.

5 Application Server를 다시 시작합니다.

보안 BEA WebLogic Server로 AMSDK 구성

SSL에서 AMSDK로 BEA WebLogic Server를 구성하기 전에 먼저 웹 컨테이너로서 BEA WebLogic Server를 설치 및 구성해야 합니다. 설치 지침을 보려면 BEA WebLogic Server 설명서를 참조하십시오. WebLogic을 Access Manager용 웹 컨테이너로 구성하려면 1 장을 참조하십시오.

▼ 보안 WebLogic 인스턴스를 구성하려면

1. **즉석 시동 메뉴를 사용하여 도메인을 만듭니다.**
2. **WebLogic 설치 디렉토리로 이동하여 인증서 요청을 생성합니다.**
3. **CSR 텍스트 파일을 사용하여 이 서버 인증서를 CA에 제출합니다.**
4. **승인된 인증서를 텍스트 파일로 저장합니다. 예를 들면** `approvedcert.txt`**와 같이 저장합니다.**
5. **다음 명령을 사용하여 루트 CA를** `cacerts`**에 로드합니다.**

   ```
   cd jdk141_03/jre/lib/security/
   ```

   ```
   jdk141_03/jre/bin/keytool -keystore cacerts -keyalg RSA -import -trustcacerts -alias
   "<alias name>" -storepass changeit -file /opt/bea81/cacert.txt
   ```

6. **다음 명령을 사용하여 서버 인증서를 로드합니다.**

   ```
   jdk141_03/jre/bin/keytool -import -keystore <keystorename> -keyalg RSA -import
   -trustcacerts -file approvedcert.txt -alias "mykey"
   ```

7. **사용자 이름과 비밀번호를 사용하여 WebLogic 콘솔에 로그인합니다.**
8. **다음 위치를 찾습니다.**

   yourdomain> Servers> myserver> Configure Keystores
9. **사용자 정의 아이디를 선택한 다음 Java Standard Trust를 선택합니다.**
10. **키 저장소 위치를 입력합니다. 예를 들면** `/opt/bea81/keystore`**와 같이 입력합니다.**
11. **키 저장소 비밀번호와 키 저장소 패스 문구를 입력합니다. 예를 들면 다음과 같습니다.**

    키 저장소 비밀번호: `JKS/Java Standard Trust`(WL 8.1의 경우 JKS만 사용)

    키 저장소 패스 문구: `changeit`
12. **SSL 개인 키 설정 개인 키 별칭 및 비밀번호를 검토합니다.**

주 – 가장 강도가 높은 SSL 라이센스를 사용해야 합니다. 그렇지 않으면 SSL 시작이 실패합니다.

13 **Access Manager의 경우 설치 시 `AmConfig.properties`의 다음 매개 변수가 자동으로 구성됩니다. 사용자가 적합하게 편집할 수도 있습니다.**

```
com.sun.identity.jss.donotInstallAtHighestPriority=true [ AM 6.3 이상에서는 필요치 않음]
com.iplanet.security.SecureRandomFactoryImpl=com.iplanet.am.util.SecureRandomFactoryImpl
com.iplanet.security.SSLSocketFactoryImpl=netscape.ldap.factory.JSSESocketFactory
com.iplanet.security.encryptor=com.iplanet.services.util.JCEEncryption
```

JDK 경로가 다음과 같은 경우

```
com.iplanet.am.jdk.path=/usr/jdk/entsys-j2se
```

키 도구 유틸리티를 사용하여 루트 CA를 인증서 데이터베이스로 가져와야 합니다. 예를 들면 다음과 같습니다.

```
/usr/jdk/entsys-j2se/jre/lib/security
/usr/jdk/entsys-j2se/jre/bin/keytool -keystore cacerts
-keyalg RSA -import -trustcacerts -alias "machinename" -storepass changeit -file
/opt/bea81/cacert.txt
```

키 도구 유틸리티는 다음 디렉토리에 있습니다.

```
/usr/jdk/entsys-j2se/jre/bin/keytool
```

14 **Access Manager `amadmin` 명령줄 유틸리티에서 `-D"java.protocol.handler.pkgs=com.iplanet.services.comm"`을 제거합니다.**

15 **SSL 모드에서 Access Manager를 구성합니다. 자세한 내용은 53 페이지 "SSL 모드에서 Access Manager 구성"을 참조하십시오.**

보안 IBM WebSphere Application Server로 AMSDK 구성

SSL에서 AMSDK를 사용하여 IBM WebShpere Server를 구성하기 전에 먼저 IBM WebShpere Server를 설치하고 웹 컨테이너로서 구성해야 합니다. 자세한 내용은 WebSphere Server 설명서를 참조하십시오. WebLogic을 Access Manager용 웹 컨테이너로 구성하려면 1 장를 참조하십시오.

▼ 보안 WebSphere 인스턴스를 구성하려면

1. **Websphere `/bin` 디렉토리에 있는 `ikeyman.sh`를 시작합니다.**
2. **서명자 메뉴에서 인증 기관(CA)의 인증서를 가져옵니다.**
3. **개인 인증서 메뉴에서 CSR을 생성합니다.**
4. **이전 단계에서 만든 인증서를 검토합니다.**
5. **개인 인증서를 선택하고 서버 인증서를 가져옵니다.**
6. **WebSphere 콘솔에서 기본 SSL 설정을 바꾸고 암호화를 선택합니다.**
7. **기본 IBM JSSE SSL 공급자를 설정합니다.**
8. **다음 명령을 입력하여 방금 만든 파일에서 CA 인증서를 응용 프로그램 서버 JVM 키 저장소로 가져옵니다.**

   ```
   $ appserver_root-dir/java/bin/ keytool -import -trustcacerts -alias cmscacert
   -keystore ../jre/lib/security/cacerts -file
   /full_path_cacert_filename.txt
   ```

   app-server-root-dir은 응용 프로그램 서버의 루트 디렉토리이며 *full_path_cacert_filename.txt*는 인증서가 있는 파일의 전체 경로입니다.

9. **Access Manager에서 JSSE를 사용하도록 `AmConfig.properties`의 다음 매개 변수를 업데이트합니다.**

   ```
   com.sun.identity.jss.donotInstallAtHighestPriority=true
   com.iplanet.security.SecureRandomFactoryImpl=com.iplanet.
   am.util.SecureRandomFactoryImpl
   com.iplanet.security.SSLSocketFactorImpl=netscape.ldap.factory.
   JSSESocketFactory
   com.iplanet.security.encyptor=com.iplanet.services.unil.JCEEncryption
   ```

10. **SSL 모드에서 Access Manager를 구성합니다. 자세한 내용은 53 페이지 "SSL 모드에서 Access Manager 구성"을 참조하십시오.**

SSL 모드에서 Access Manager를 Directory Server로 구성

네트워크를 통한 보안 통신을 제공하기 위해 Access Manager에는 LDAPS 통신 프로토콜이 포함되어 있습니다. LDAPS는 표준 LDAP 프로토콜이지만 SSL(Secure Sockets Layer)의 상위에서 실행됩니다. SSL 통신을 사용하려면 먼저 Directory Server를 SSL 모드에서 구성한 다음 Access Manager를 Directory Server로 연결합니다. 기본적인 단계는 다음과 같습니다.

1. Directory Server용 인증서를 구하여 설치한 다음 인증 기관(CA)의 인증서를 신뢰하도록 Directory Server를 구성합니다.
2. 디렉토리에서 SSL을 활성화합니다.
3. 인증, 정책 및 플랫폼 서비스를 구성하여 SSL을 사용하는 Directory Server로 연결합니다.
4. Access Manager를 Directory Server 백엔드에 안전하게 연결되도록 구성합니다.

SSL 모드에서 Directory Server 구성

Directory Server를 SSL 모드에서 구성하려면 서버 인증서를 구하여 설치하고 인증 기관의 인증서를 신뢰하도록 Directory Server를 구성한 다음 SSL을 활성화해야 합니다. 자세한 내용은 *Directory Server* 관리 설명서의 11장 "인증 및 암호화 관리"에 있습니다. 이 문서는 다음 위치에 있습니다.

http://docs.sun.com/coll/DirectoryServer_04q2 (http://docs.sun.com/coll/DirectoryServer_04q2) 및 http://docs.sun.com/coll/DirectoryServer_04q2_ko (http://docs.sun.com/coll/DirectoryServer_04q2_ko)

Directory Server가 이미 SSL 사용 가능 상태이면 Access Manager를 Directory Server로 연결하는 방법을 자세히 설명하는 다음 절로 이동합니다.

Access Manager를 SSL을 사용하는 Directory Server에 연결

일단 SSL 모드로 Directory Server가 구성된 다음에는 Access Manager를 Directory Server 백엔드로 연결해야 합니다.

▼ Access Manager를 Directory Server로 연결하려면

1 Access Manager 콘솔에서 서비스 구성 모듈의 LDAP 인증 서비스로 이동합니다.

a. Directory Server 포트를 SSL 포트로 변경합니다.

b. LDAP 서버에 대한 SSL 액세스 가능 속성을 선택합니다.

2 서비스 구성 모듈의 구성원 인증 서비스로 이동합니다.

a. Directory Server 포트를 SSL 포트로 변경합니다.

b. LDAP 서버에 대한 SSL 액세스 가능 속성을 선택합니다.

3 서비스 구성에 있는 정책 구성 서비스로 이동합니다.

a. Directory Server 포트를 SSL 포트로 변경합니다.

b. LDAP 서버에 대한 SSL 액세스 가능 속성을 선택합니다.

4 텍스트 편집기에서 `serverconfig.xml` 파일을 엽니다. 이 파일은 다음 위치에 있습니다.
`/etc/opt/SUNWam/config`

a. `<Server>` 요소에서 다음 값을 변경합니다.
`port` - Access Manager가 수신하는 보안 포트의 포트 번호를 입력합니다(기본값: 636).
`type`- SIMPLE을 SSL로 변경합니다.

b. `serverconfig.xml` 파일을 저장한 다음 닫습니다.

5 다음 기본 위치에서 `AMConfig.properties` 파일을 엽니다.
/etc/opt/SUNWam/config.
다음 등록 정보를 변경합니다.

a. `com.iplanet.am.directory.port` = 636(기본값을 사용하는 경우)

b. `ssl.enabed = true`

c. `AMConfig.properties`를 저장합니다.

6 서버를 다시 시작합니다.

파 트 II

액세스 제어

Sun Java System Access Manager™ 7 2005Q4 관리 설명서의 제2부입니다. Access Control 인터페이스는 인증 및 권한 부여 서비스를 만들고 관리하는 방법을 제공하여 영역 기반 자원을 보호하고 규제합니다. 기업 사용자가 정보를 요청하면 Access Manager는 사용자의 아이디를 확인하고 요청한 특정 자원에 액세스할 수 있는 권한을 부여합니다. 다음과 같은 장으로 구성됩니다.

◆ ◆ ◆ 4 장

4 Access Manager 콘솔

Access Manager 콘솔은 다양한 액세스 수준을 가진 관리자가 이를 사용하여 영역 및 조직을 생성하고 이 영역에서 사용자를 생성 및 삭제하며, 영역의 자원을 보호하고 이에 대한 액세스를 제한하기 위한 적용 정책을 설정할 수 있는 웹 인터페이스입니다. 또한 관리자는 현재 사용자 세션을 확인 및 종료할 수 있으며 사용자의 연합 구성(인증 도메인 및 공급자 생성, 삭제 및 수정)을 관리할 수 있습니다. 반면 관리 권한이 없는 사용자는 개인 정보(이름, 전자 메일 주소, 전화 번호 등)를 관리하고 비밀번호를 변경하며, 그룹에 가입 및 탈퇴하고 자신의 역할을 확인할 수 있습니다. Access Manager에는 다음과 같은 두 개의 기본 보기가 있습니다.

관리 보기

관리 역할이 있는 사용자가 Access Manager에 인증하는 경우 기본 보기는 관리 보기입니다. 이 보기에서 관리자는 Access Manager와 관련된 대부분의 관리 작업을 수행할 수 있습니다. Access Manager는 영역 모드와 레거시 모드, 두 개의 다른 모드로 설치할 수 있습니다. 각 모드에는 고유의 콘솔이 있습니다. 영역 및 레거시 모드에 대한 자세한 내용은 **Sun Java System Access Manager 7 2005Q4 Technical Overview**를 참조하십시오.

영역 모드 콘솔

영역 모드 콘솔에서 관리자는 영역 기반 액세스 제어, 기본 서비스 구성, 웹 서비스 및 연합을 관리할 수 있습니다. 관리자 로그인 화면에 액세스하려면 브라우저에서 다음 주소 구문을 사용하십시오.

protocol://*servername*/amserver/UI/Login

protocol은 배포 방법에 따라 http: 또는https입니다.

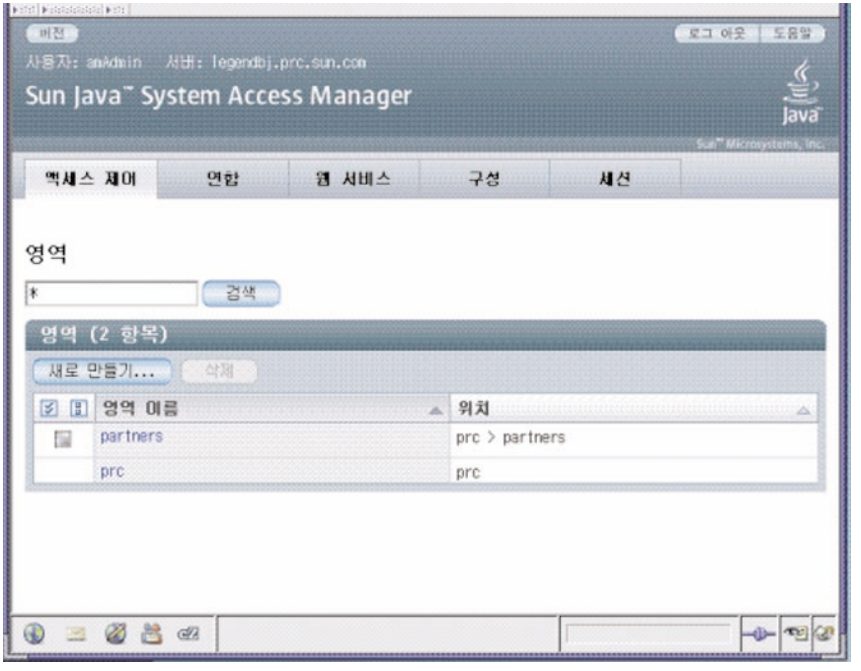

그림 4–1 영역 모드 관리 보기

레거시 모드 콘솔

레거시 모드 콘솔은 Access Manager 6.3 아키텍처를 기반으로 합니다. 레거시 Access Manager 아키텍처는 Sun Java System Directory Server와 함께 제공되는 LDAP 디렉토리 정보 트리(DIT)를 사용합니다. 레거시 모드에서 사용자 정보 및 액세스 제어 정보는 모두 LDAP 조직에 저장됩니다. 레거시 모드를 선택하는 경우 LDAP 조직은 액세스 제어 영역에 해당합니다. 영역 정보는 LDAP 조직 내에 통합됩니다. 레거시 모드에서는 Access Manager 기반의 identity 관리에 대해 디렉토리 관리 탭을 사용할 수 있습니다.

관리자 로그인 화면에 액세스하려면 브라우저에서 다음 주소 구문을 사용하십시오.

protocol://*servername* /amserver/console

protocol은 배포 방법에 따라 http: 또는https입니다.

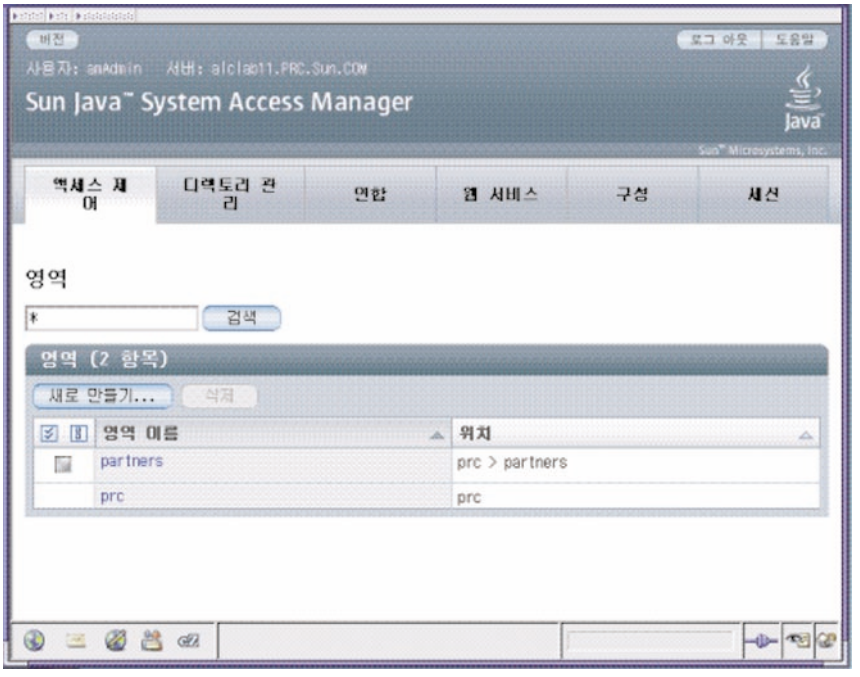

그림 4–2 레거시 모드 관리 보기

레거시 모드 6.3 콘솔

Access Manager 6.3의 일부 기능은 Access Manager 7.0 콘솔에서 사용할 수 없습니다. 이런 이유로 관리자는 7.0 레거시 배포를 통해 6.3 콘솔에 로그인할 수 있습니다. 이 콘솔은 Access Manager가 Sun Java System Portal Server 또는 Sun Java System Directory Server를 중앙 아이디 저장소로 사용해야 하는 기타 Sun Java System 통신 제품 상에 구축된 경우 일반적으로 사용됩니다. Delegated Administration 및 Class of Service와 같은 다른 기능은 이 콘솔을 통해서만 액세스할 수 있습니다.

주 – 6.3과 7.0 레거시 모드 콘솔을 번갈아 사용하지 마십시오.

6.3 콘솔에 액세스하려면 브라우저에서 다음 주소 구문을 사용합니다.

protocol://*servername* /amconsole

protocol은 배포 방법에 따라 http: 또는https입니다.

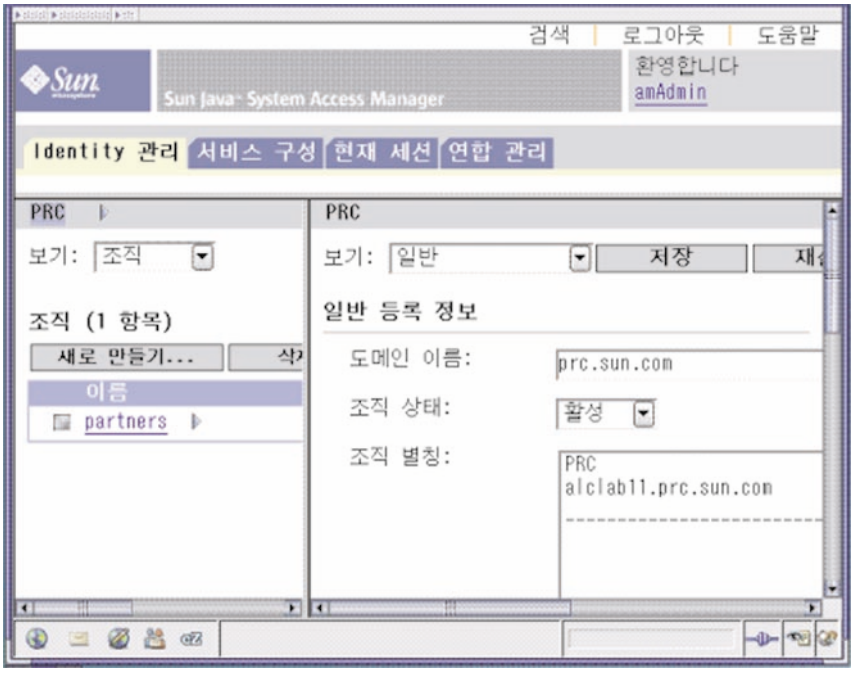

그림 4–3 Legacy 6.3 기반 콘솔

사용자 프로필 보기

관리 역할이 할당되지 않은 사용자가 Access Manager에 대해 인증을 수행할 때는 사용자 자신의 사용자 프로필이 기본 보기가 됩니다. 사용자 프로필 보기는 영역 또는 레거시 모드에서 액세스할 수 있습니다. 사용자는 이 보기에 액세스하려면 로그인 페이지에서 자신의 사용자 이름과 비밀번호를 입력해야 합니다.

이 보기에서 사용자는 개인 프로필 특정의 속성 값을 수정할 수 있습니다. 여기에는 이름, 주소, 집, 비밀번호 등이 포함될 수 있지만 이에 제한되지는 않습니다. 사용자 프로필 보기에 표시되는 속성은 확장할 수 있습니다.

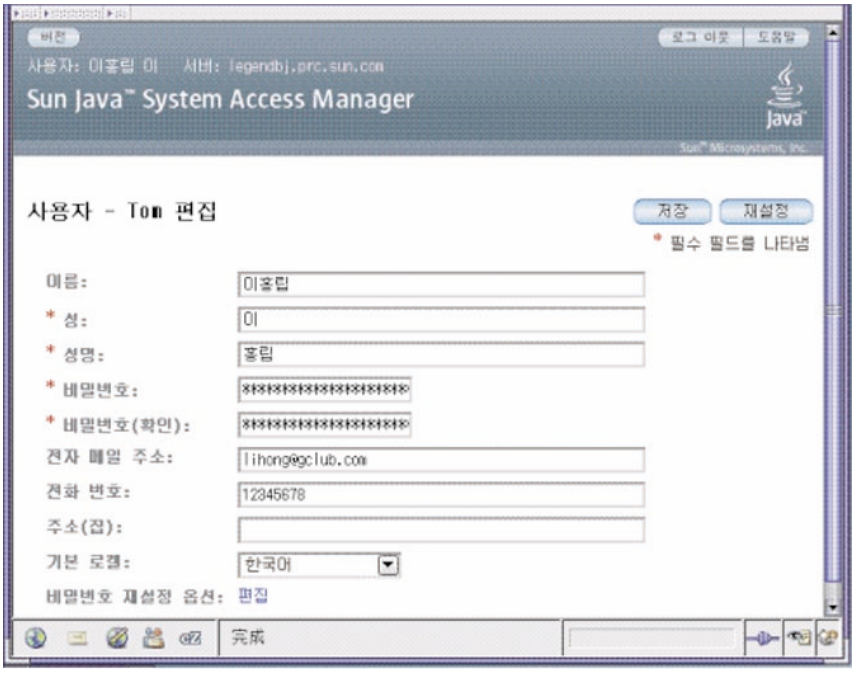

그림 4–4 사용자 프로필 보기

◆ ◆ ◆ 5 장

5 영역 관리

액세스 제어 영역은 사용자 또는 사용자의 그룹에 연결할 수 있는 인증 등록 정보 및 권한 부여 정책의 그룹입니다. 영역 데이터는 사용자가 지정한 데이터 저장소 내에 Access Manager가 생성한 소유 정보 트리에 저장됩니다. Access Manager 프레임워크는 Access Manager 정보 트리 내 각 영역에 있는 정책 및 속성을 종합합니다. 기본적으로 Access Manager 7은 사용자 데이터와는 별도로 Access Manager 정보 트리를 특수 분기로 Sun Java Enterprise System Directory Server에 자동으로 삽입합니다. 어떤 LDAPv3 데이터베이스를 사용하는 중이라도 액세스 제어 영역을 사용할 수 있습니다.

영역에 대한 자세한 내용은 **Sun Java System Access Manager 7 2005Q4 Technical Overview**를 참조하십시오.

영역 탭에서 액세스 제어에 대한 다음과 같은 등록 정보를 구성할 수 있습니다.

- 68 페이지 “인증”
- 68 페이지 “서비스”
- 69 페이지 “권한”

영역 만들기 및 관리

이 절에서는 영역을 만들고 관리하는 방법을 설명합니다.

▼ 새 영역을 만들려면

1 액세스 제어 탭 아래에 있는 영역 목록에서 새로 만들기를 선택합니다.

2 다음과 같은 일반 속성을 정의합니다.

이름 영역 이름을 입력합니다.

부모 생성하는 영역의 위치를 정의합니다. 새 영역이 위치할 부모 영역을 선택합니다.

3 다음과 같은 영역 속성을 지정합니다.

영역 상태 활성 또는 비활성 상태를 선택합니다. 기본값은 활성입니다. 이 값은 영역의 수명 동안 등록 정보 아이콘을 선택하여 언제든지 변경할 수 있습니다. 비활성을 선택하면 로그인 시 사용자 액세스를 사용할 수 없습니다.

영역/DNS 별칭 영역의 DNS 이름에 대한 별칭 이름을 추가할 수 있습니다. 이 속성은 "실제" 도메인 별칭(임의의 문자열은 허용 안 됨)만 수락합니다.

4 저장하려면 확인을 누르고 이전 페이지로 돌아가려면 취소를 누릅니다.

일반 등록 정보

일반 등록 정보 페이지에는 영역에 대한 기본 속성이 표시됩니다. 이 등록 정보를 수정하려면 액세스 제어 탭 아래에 있는 영역 이름 목록에서 해당 영역을 누릅니다. 그리고 나서 다음 등록 정보를 편집합니다.

영역 상태 활성 또는 비활성 상태를 선택합니다. 기본값은 활성입니다. 이 값은 영역의 수명 동안 등록 정보 아이콘을 선택하여 언제든지 변경할 수 있습니다. 비활성을 선택하면 로그인 시 사용자 액세스를 사용할 수 없습니다.

영역/DNS 별칭 영역의 DNS 이름에 대한 별칭 이름을 추가할 수 있습니다. 이 속성은 "실제" 도메인 별칭(임의의 문자열은 허용 안 됨)만 수락합니다.

등록 정보를 편집한 다음 저장을 누릅니다.

인증

사용자가 다른 인증 모듈을 사용하여 로그인하기 전에 일반 인증 서비스를 영역에 대한 서비스로 등록해야 합니다. 핵심 인증 서비스를 사용하면 Access Manager 7 관리자가 영역의 인증 매개 변수에 대한 기본값을 지정할 수 있습니다. 지정된 인증 모듈에 정의된 대체 값이 없는 경우 이러한 값을 사용할 수 있습니다. 핵심 인증 서비스의 기본값은 `amAuth.xml` 파일에 정의되며 설치 후에 Directory Server에 저장됩니다.

자세한 내용은 7 장를 참조하십시오.

서비스

Access Manager에서 서비스는 Access Manager 콘솔에서 함께 관리되는 속성의 그룹입니다. 속성은 직원 이름, 직위 및 전자 메일 주소와 같은 관련 정보입니다. 속성은 일반적으로 메일 응용 프로그램 또는 급여 서비스와 같은 소프트웨어 모듈의 구성 매개 변수로 사용됩니다.

서비스 탭을 사용하여 몇 가지 Access Manager 기본 서비스를 영역에 추가 및 구성할 수 있습니다. 다음과 같은 서비스를 추가할 수 있습니다.

- 관리
- 검색 서비스
- 국제화 설정
- 비밀번호 재설정
- 세션
- 사용자

주 – Access Manager는 서비스 .xml 파일에서 필요한 속성을 일부 기본값으로 실행합니다. 서비스에서 필요한 속성에 값이 없는 경우 기본값을 추가하고 서비스를 다시 로드해야 합니다.

▼ 영역에 서비스를 추가하려면

1. **새 서비스를 추가할 영역 이름을 누릅니다.**
2. **서비스 탭을 선택합니다.**
3. **서비스 목록에서 추가를 누릅니다.**
4. **영역에 추가할 서비스를 선택합니다.**
5. **다음을 누르십시오.**
6. **영역 속성을 정의하여 서비스를 구성합니다. 서비스 속성에 대한 설명은 온라인 도움말에서 구성 부분을 참조하십시오.**
7. **마침을 누릅니다.**
8. **서비스의 등록 정보를 편집하려면 서비스 목록에서 이름을 누릅니다.**

권한

권한은 영역 내에 존재하는 역할 또는 그룹에 대한 액세스 권한을 지정합니다. 역할 또는 그룹은 Access Manager 아이디 주제 유형의 정책 주제 정의로 사용됩니다. 권한을 할당 또는 수정하려면 편집할 역할 또는 그룹의 이름을 누릅니다. 다음과 같은 권한을 할당할 수 있습니다.

- 정책 등록 정보 전용의 읽기 및 쓰기 액세스

- 모든 영역 및 정책 등록 정보에 대한 읽기 및 쓰기 권한
- 모든 등록 정보 및 서비스에 대한 읽기 전용 액세스

◆ ◆ ◆ 6 장

6 데이터 저장소

데이터 저장소는 사용자 속성 및 사용자 구성 데이터를 저장할 수 있는 데이터베이스입니다.

Access Manager는 아이디 저장소 프레임워크에 연결하는 아이디 저장소 플러그인을 제공합니다. 이 새 모델을 사용하면 기존 사용자 데이터베이스를 변경하지 않고도 Access Manager 사용자 정보를 확인하고 불러올 수 있습니다. Access Manager 프레임워크는 아이디 저장소 플러그인에서 얻은 데이터를 다른 Access Manager 플러그인에서 얻은 데이터와 통합하여 각 사용자의 가상 아이디를 구성합니다. Access Manager는 이제 두 개 이상의 아이디 저장소 간의 인증 및 권한 부여 과정에 이러한 범용 아이디를 사용할 수 있습니다. 가상 사용자 아이디는 사용자 세션이 종료되면 소멸됩니다.

LDAPv3 데이터 저장소

Access Manage가 영역 및 레거시 모드 모두로 설치된 경우 일반 LDAPv3 저장소에 대해 새 데이터 저장소 인스턴스를 만들 수 있습니다. 다음 조건에서 LDAPv3 저장소 유형을 선택해야 합니다.

- 역할, 서비스 클래스(CoS) 및 이전 버전의 Access Manager와의 호환성이 필요하지 않은 경우
- 기존 디렉토리를 사용하려는 경우
- 아이디 저장소에 대해 Sun Java System Directory Server가 아닌 디렉토리 서버를 사용하려는 경우
- Access Manager가 아이디 저장소에 쓰지 않게 하려는 경우
- 플랫 디렉토리 정보 트리(DIT)를 사용하려는 경우

▼ 새 LDAPv3 데이터 저장소를 만들려면

다음 절에서는 일반 LDAPv3 데이터 저장소를 연결하는 단계에 대해 설명합니다.

1 새 데이터 저장소를 만들 영역을 선택합니다.

2 데이터 저장소 탭을 누릅니다.

3 데이터 저장소 목록에서 새로 만들기를 누릅니다.

4 데이터 저장소의 이름을 입력합니다.

5 LDAPv3 저장소 플러그인을 위한 속성를 정의합니다.

6 마침을 누릅니다.

LDAPv3 저장소 플러그인 속성

다음과 같은 변수를 사용하여 LDAPv3 저장소 플러그인을 구성할 수 있습니다.

- 73 페이지 “기본 LDAP 서버”
- 73 페이지 “LDAP 바인드 DN”
- 73 페이지 “LDAP 바인드 비밀번호”
- 73 페이지 “LDAP 바인드 비밀번호(확인)”
- 73 페이지 “LDAP 조직 DN”
- 73 페이지 “LDAP SSL 사용 가능”
- 73 페이지 “LDAP 연결 풀 최소 크기”
- 74 페이지 “LDAP 연결 풀 최대 크기”
- 74 페이지 “최대 검색 반환 결과”
- 74 페이지 “검색 시간 초과”
- 74 페이지 “LDAP에서 참조를 따름”
- 74 페이지 “LDAPv3 저장소 플러그인 클래스 이름”
- 74 페이지 “속성 이름 매핑”
- 74 페이지 “LDAPv3 플러그인 지원 유형 및 작업”
- 74 페이지 “LDAP 사용자 검색 속성”
- 75 페이지 “LDAP 사용자 검색 필터”
- 75 페이지 “LDAP 사용자 객체 클래스”
- 75 페이지 “LDAP 사용자 속성”
- 75 페이지 “LDAP 그룹 검색 속성”
- 75 페이지 “LDAP 그룹 검색 필터”
- 75 페이지 “LDAP 그룹 컨테이너 이름 지정 속성”
- 75 페이지 “LDAP 그룹 컨테이너 값”
- 75 페이지 “LDAP 그룹 객체 클래스”
- 76 페이지 “LDAP 그룹 속성”
- 76 페이지 “그룹 구성원에 대한 속성 이름”
- 76 페이지 “그룹 구성원의 속성 이름”
- 76 페이지 “그룹 구성원 URL의 속성 이름”
- 76 페이지 “LDAP 사용자 컨테이너 이름 지정 속성”
- 76 페이지 “LDAP 사용자 컨테이너 값”
- 76 페이지 “LDAP 에이전트 검색 속성”
- 76 페이지 “LDAP 에이전트 컨테이너 이름 지정 변수”

- 77 페이지 “LDAP 에이전트 컨테이너 값”
- 77 페이지 “LDAP 에이전트 검색 필터”
- 77 페이지 “LDAP 에이전트 객체 클래스”
- 77 페이지 “LDAP 에이전트 속성”
- 77 페이지 “지속적 검색 기본 DN”
- 77 페이지 “재시작 전 지속적 검색 최대 유휴 시간”
- 77 페이지 “오류 코드 후 최대 재시도 횟수”
- 77 페이지 “재시도 간 지연 시간”
- 78 페이지 “재시도 대상의 LDAPException 오류 코드”

기본 LDAP 서버

연결할 LDAP 서버의 이름을 입력하며`hostname.domainname:portnumber` 형식이어야 합니다.

두 개 이상의 `host:portnumber` 항목을 입력한 경우 목록의 첫 번째 호스트로 연결이 시도됩니다. 현재 호스트에 대한 연결 시도가 실패한 경우에만 목록의 다음 항목에 대한 연결을 시도합니다.

LDAP 바인드 DN

현재 사용자가 연결된 LDAP 서버에 대한 인증에 Access Manager가 사용할 DN 이름을 지정합니다. DN 이름이 바인드된 사용자는 LDAPv3 지원 유형 및 작업 속성에서 구성한 올바른 추가, 수정 및 삭제 권한을 가져야 합니다.

LDAP 바인드 비밀번호

현재 사용자가 연결된 LDAP 서버에 대한 인증에 Access Manager가 사용할 DN 비밀번호를 지정합니다.

LDAP 바인드 비밀번호(확인)

비밀번호를 확인합니다.

LDAP 조직 DN

해당 데이터 저장소의 저장소가 매핑될 DN으로 데이터 저장소에서 수행되는 모든 작업의 기본 DN이 됩니다.

LDAP SSL 사용 가능

활성화된 경우 Access Manager는 HTTPS 프로토콜을 사용하여 기본 서버에 연결합니다.

LDAP 연결 풀 최소 크기

연결 풀의 초기 연결 수를 지정합니다. 연결 풀을 사용하면 매번 새로 연결할 필요가 없습니다.

LDAP 연결 풀 최대 크기

허용된 최대 연결 수를 지정합니다.

최대 검색 반환 결과

검색 작업에서 반환된 최대 항목 수를 지정합니다. 해당 제한값에 도달하면 Directory Server는 검색 요청과 일치하는 모든 항목을 반환합니다.

검색 시간 초과

검색 요청에 할당할 최대 시간(초)을 지정합니다. 해당 제한값에 도달하면 Directory Server는 검색 요청과 일치하는 모든 항목을 반환합니다.

LDAP에서 참조를 따름

이 옵션이 활성화되면 다른 LDAP 서버로의 참조를 자동으로 따라갑니다.

LDAPv3 저장소 플러그인 클래스 이름

LDAPv3 저장소를 구현할 클래스 파일의 위치를 지정합니다.

속성 이름 매핑

프레임워크에 알려진 공통 속성을 기본 데이터 저장소에 매핑할 수 있도록 합니다. 예를 들어 프레임워크에서 사용자 상태를 결정하는 데 `inetUserStatus`를 사용한다면 기본 데이터 저장소에서는 `userStatus`를 사용할 수 있습니다. 속성 정의는 대소문자를 구분합니다.

LDAPv3 플러그인 지원 유형 및 작업

해당 LDAP 서버상에서 허용되거나 수행할 수 있는 작업을 지정합니다. 해당 LDAPv3 저장소 플러그인이 지원하는 작업만 기본 작업입니다. LDAPv3 저장소 플러그인이 지원하는 작업은 다음과 같습니다.

- 그룹 — 읽기, 만들기, 편집, 삭제
- 영역 — 읽기, 만들기, 편집, 삭제, 서비스
- 사용자 — 읽기, 만들기, 편집, 삭제, 서비스
- 에이전트 — 읽기, 만들기, 편집, 삭제

LDAP 서버 설정 및 작업에 따라 권한을 제거하는 것은 가능하지만

권한을 추가할 수는 없습니다.

LDAP 사용자 검색 속성

이 필드는 사용자에 대해 검색을 수행하는 속성 유형을 정의합니다. 예를 들어 사용자 DN이 `uid=k user5,ou=people,dc=iplanet,dc=com`인 경우 이름 지정 속성은 uid입니다. `(uid=*)`는 사용자에 대한 검색 필터에 추가됩니다.

LDAP 사용자 검색 필터

사용자 항목을 찾는 데 사용되는 검색 필터를 지정합니다. 예를 들어 LDAP 사용자 검색 속성은 uid이고 LDAP 사용자 검색 필터는 (objectClass=inetorgperson)인 경우 실제 사용자 검색 필터는 다음과 같습니다. (&(uid=*)(objectClass=inetorgperson)).

LDAP 사용자 객체 클래스

사용자를 위한 객체 클래스를 지정합니다. 사용자가 생성되면 사용자 객체 클래스의 해당 목록이 사용자의 속성 목록에 추가됩니다.

LDAP 사용자 속성

사용자와 연결된 속성의 목록을 정의합니다. 해당 목록에 없는 사용자 속성에 대한 읽기/쓰기 시도는 허용되지 않습니다. 속성은 대소문자를 구분합니다. 객체 클래스 및 속성 스키마는 사용자가 객체 클래스 및 속성 스키마를 지정하기 전에 Directory Server에서 정의되어야 합니다.

LDAP 그룹 검색 속성

이 필드는 그룹에서 검색을 수행하는 속성 유형을 정의합니다. 예를 들어 그룹 DN이 cn=group1,ou=groups,dc=iplanet,dc=com인 경우 그룹에 대한 이름 지정 속성은 cn이고 (cn=*)이 그룹 검색 필터에 추가됩니다.

LDAP 그룹 검색 필터

그룹 항목을 찾는 데 사용되는 검색 필터를 지정합니다. 예를 들어 "LDAP 그룹 검색 속성"은 cn이고 "LDAP 그룹 검색 필터"는 (objectclass=groupOfUniqueNames)인 경우 실제 그룹 검색 필터는 (&(cn=*)(objectclass=groupOfUniqueNames))입니다.

LDAP 그룹 컨테이너 이름 지정 속성

그룹이 컨테이너에 있는 경우 그룹 컨테이너를 위한 이름 지정 속성을 지정합니다. 그렇지 않으면 이 속성은 비어 있습니다. 예를 들어 cn=group1,ou=groups,dc=iplanet,dc=com의 그룹 DN이 ou=groups에 상주하는 경우 그룹 컨테이너 이름 지정 속성은 ou입니다.

LDAP 그룹 컨테이너 값

그룹 컨테이너 값을 지정합니다. 예를 들어 cn=group1,ou=groups,dc=iplanet,dc=com의 그룹 DN이 ou=groups에 상주하는 경우 그룹 컨테이너 값은 groups입니다.

LDAP 그룹 객체 클래스

그룹에 대한 객체 클래스를 지정합니다. 그룹이 생성되면 그룹 객체 클래스의 해당 목록이 그룹의 속성 목록에 추가됩니다.

LDAP 그룹 속성

그룹과 연결된 속성의 목록을 정의합니다. 목록에 없는 그룹 속성에 대한 읽기/쓰기 시도는 허용되지 않습니다. 속성은 대소문자를 구분합니다. 객체 클래스 및 속성 스키마는 사용자가 객체 클래스 및 속성 스키마를 지정하기 전에 Directory Server에서 정의되어야 합니다.

그룹 구성원에 대한 속성 이름

DN이 속한 모든 그룹 이름을 값으로 가지는 속성의 이름을 지정합니다. 기본값은 `memberOf`입니다.

그룹 구성원의 속성 이름

해당 그룹에 속한 DN을 값으로 가지는 속성의 이름을 지정합니다. 기본값은 `uniqueMember`입니다.

그룹 구성원 URL의 속성 이름

해당 그룹에 속한 구성원을 확인하는 LDAP URL을 값으로 가지는 속성의 이름을 지정합니다. 기본값은 `memberUrl`입니다.

LDAP 사용자 컨테이너 이름 지정 속성

사용자가 사용자 컨테이너에 있는 경우 사용자 컨테이너의 이름 지정 속성을 지정합니다. 사용자가 사용자 컨테이너에 없으면 이 필드는 비어 있습니다. 예를 들어 사용자 DN에 `uid=kuser5,ou=people,dc=iplanet,dc=com`이 지정되어 있고 `ou=people`이 사용자 컨테이너의 이름인 경우 이름 지정 속성은 `ou`입니다.

LDAP 사용자 컨테이너 값

사용자 컨테이너의 값을 지정합니다. 기본값은 `people`입니다. 예를 들어 사용자 DN에 `uid=kuser5,ou=people,dc=iplanet,dc=com`이 지정되어 있고 `ou=people`이 사용자 컨테이너의 이름인 경우 이름 지정 속성은 `ou`이고 `people`은 "LDAP 사용자 컨데이터 값"입니다.

LDAP 에이전트 검색 속성

이 필드는 에이전트에서 검색을 수행하는 속성 유형을 정의합니다. 기본값은 `uid`입니다. 예를 들어 에이전트 DN이 `uid=kagent1,ou=agents,dc=iplanet,dc=com`인 경우 에이전트의 이름 지정 속성은 uid입니다. `(uid=*)`는 에이전트에 대한 검색 필터에 추가됩니다.

LDAP 에이전트 컨테이너 이름 지정 변수

에이전트가 에이전트 컨테이너에 있는 경우 에이전트 컨테이너의 이름 지정 변수입니다. 에이전트가 에이전트 컨테이너에 없으면 이 필드는 비어 있습니다. 예를 들어 사용자 DN에 `uid=kagent1,ou=agents,dc=iplanet,dc=com`이 지정된 경우 에이전트 이름 지정 속성은 `ou`입니다.

LDAP 에이전트 컨테이너 값

에이전트 컨테이너 값을 지정합니다. 에이전트가 에이전트 컨테이너에 없으면 이 필드는 비어 있습니다. 앞에서 설명한 예에서 에이전트 컨테이너 값은 `agents`입니다.

LDAP 에이전트 검색 필터

에이전트 검색에 사용되는 필터를 정의합니다. 이 필드에 LDAP 에이전트 검색 변수를 추가하여 실제 에이전트 검색 필터를 만듭니다.

예를 들어 LDAP 에이전트 검색 속성은 `uid`이고 LDAP 사용자 검색 필터는 `(objectClass=sunIdentityServerDevice)`인 경우 실제 사용자 검색 필터는 `(&(uid=*)(objectClass=sunIdentityServerDevice))`입니다.

LDAP 에이전트 객체 클래스

에이전트에 대한 객체 클래스를 지정합니다. 에이전트가 생성되면 사용자 객체 클래스가 에이전트의 속성 목록에 추가됩니다.

LDAP 에이전트 속성

에이전트와 연결된 속성의 목록을 정의합니다. 목록에 없는 에이전트 속성에 대한 읽기/쓰기 시도는 허용되지 않습니다. 속성은 대소문자를 구분합니다. 객체 클래스 및 속성 스키마는 사용자가 객체 클래스 및 속성 스키마를 지정하기 전에 Directory Server에서 정의되어야 합니다.

지속적 검색 기본 DN

지속적 검색에 사용할 기본 DN을 지정합니다. 일부 LDAPv3 서버는 루트 접미사 수준의 지속적 검색만 지원합니다.

재시작 전 지속적 검색 최대 유휴 시간

지속성 검색을 다시 시작하기 전 최대 유휴 시간을 지정합니다. 1보다 큰 값을 사용해야 합니다. 값이 1 이하인 경우 연결 유휴 시간에 관계 없이 검색을 다시 시작합니다.

Access Manager가 로드 밸런서와 함께 배포된 경우 지정된 시간 동안 유휴 상태이면 일부 로드 밸런서에서 시간 초과가 일어납니다. 이 경우 재시작 전 지속성 검색 최대 유휴 시간을 로드 밸런서에 지정한 값보다 작은 값으로 설정해야 합니다.

오류 코드 후 최대 재시도 횟수

재시도 대상 LDAPException 오류 코드에서 지정된 오류 코드가 발생하는 경우 지속적 검색 작업에 대한 최대 재시도 횟수를 지정합니다.

재시도 간 지연 시간

각 재시도 전 대기 시간을 지정합니다. 지속적 검색 연결에만 적용됩니다.

재시도 대상의 LDAPException 오류 코드

지속적 검색 작업을 재시도할 오류 코드를 지정합니다. 이 속성은 지속적 검색에만 적용되며 모든 LDAP 작업에는 적용되지 않습니다.

AMSDK 저장소 플러그인

AMSDK 아이디 저장소는 Access Manager가 레거시 모드로 설치된 경우 Access Manager 정보 트리와 자동으로 통합됩니다. 영역 모드에서는 AMSDK 저장소를 설치하도록 선택할 수 있지만 아이디 저장소는 Access Manager 정보 트리와 통합되지 않습니다. 다음 조건에서 AMSDK 저장소 유형을 선택해야 합니다.

- 역할 및 CoS와 같은 Sun Java System Directory Server 고유 기능을 활용하려는 경우
- 이전 버전의 Access Manager와의 호환성을 확보하려는 경우

▼ 새 AMSDK 저장소 플러그인을 만들려면

1. **Access Manager 저장소 플러그인을 구성할 영역을 선택합니다.**
2. **데이터 저장소 탭을 누릅니다.**
3. **데이터 저장소 목록에서 새로 만들기를 누릅니다.**
4. **저장소 플러그인 이름을 입력합니다.**
5. **Access Manager 저장소 플러그인을 선택합니다.**
6. **다음을 누르십시오.**
7. **다음 필드를 정의합니다.**

Access Manager 플러그인 클래스 이름	Access Manager 저장소 플러그인을 구현할 클래스 파일의 위치를 지정합니다.
Access Manager 조직	Access Manager가 관리할 Directory Server 내의 조직을 가리키는 DN으로 데이터 저장소에서 수행되는 모든 작업의 기본 DN이 됩니다.

8. **마침을 누릅니다.**

◆ ◆ ◆ 7 장

7 인증 관리

인증 서비스는 Access Manager 배포 시 설치되는 모든 기본 인증 유형에 사용할 웹 기반 사용자 인터페이스를 제공합니다. 이 인터페이스는 액세스를 요청한 사용자에게 호출된 인증 모듈에 따라 로그인 요구 사항 화면을 표시함으로써 인증 자격 증명을 수집하는 동적/사용자 정의 가능 수단을 제공합니다. 이러한 인터페이스는 Sun Java System™ Application Framework(*JATO*라고도 함)를 사용하여 구축되는데, 이는 개발자들이 기능적 웹 응용 프로그램 구축 시 사용하는 J2EE(Java 2 Enterprise Edition) 표현 프레임워크입니다.

인증 구성

이 절에서는 배포를 위한 인증을 구성하는 방법에 대해 설명합니다. 첫 번째 절에서는 기본 인증 모듈에 대해 간략히 설명하고 필요한 구성 전 지침을 제공합니다. 영역, 사용자, 역할 등에 대해 같은 인증 모듈 유형의 여러 구성 인스턴스를 구성할 수 있습니다. 또한 인증 체인을 추가해서 성공적인 인증을 위해 인증이 여러 인스턴스의 기준을 통과하도록 할 수 있습니다. 이 절에는 다음 내용이 포함되어 있습니다.

인증 모듈 유형

인증 모듈은 사용자 아이디와 비밀번호와 같은 사용자 정보를 수집하고 이 정보를 데이터베이스의 항목과 비교하여 확인하는 플러그인입니다. 사용자가 인증 기준을 충족하는 정보를 제공하면 사용자에게 요청한 자원에 대한 액세스 권한이 허용됩니다. 사용자가 인증 기준을 충족하지 않는 정보를 제공하면 요청한 자원에 대한 액세스가 거부됩니다. Access Manager는 다음 15가지 유형의 인증 모듈과 함께 설치됩니다.

주 – 일부 인증 모듈의 경우 인증 인스턴스로 사용할 수 있으려면 사전 구성이 필요합니다. 필요한 경우 구성 단계가 모듈 유형 설명에 나열됩니다.

핵심

Access Manager는 기본적으로 핵심 인증 모듈과 15개의 다른 인증 모듈을 제공합니다. 핵심 인증 모듈은 인증 모듈에 대한 전체 구성을 제공합니다. 활성 디렉토리, 익명, 인증서 기반, HTTP 기본, JDBC, LDAP 및 인증 모듈을 추가하고 활성화하기 전에 먼저 핵심 인증을 추가하고 활성화해야 합니다. 핵심 및 LDAP 인증 모듈은 모두 기본 영역에 대해 자동으로 활성화됩니다.

고급 등록 정보 버튼을 누르면 영역에 대해 정의할 수 있는 핵심 인증 속성이 표시됩니다. 전역 속성은 영역에 적용되지 않으므로 표시되지 않습니다.

활성 디렉토리

활성 디렉토리 인증 모듈은 LDAP 모듈과 비슷한 방법으로 인증을 수행하지만 LDAP 인증 모듈의 Directory Server와 반대되는 Microsoft의 Active Directory™ 서버를 사용합니다. 활성 디렉토리 서버에 대해 LDAP 인증 모듈을 구성할 수는 있지만 이 모듈을 사용하면 LDAP 및 활성 디렉토리 인증이 모두 같은 영역 아래에 있게 됩니다.

주 – 이 릴리스의 경우 활성 디렉토리 인증 모듈만 사용자 인증을 지원합니다. 비밀번호 정책은 LDAP 인증 모듈에서만 지원됩니다.

익명

기본적으로 이 모듈이 활성화되면 사용자는 Access Manager에 익명 사용자로 로그인할 수 있습니다. 또한 유효한 익명 사용자 목록 속성을 구성하여 이 모듈에 대한 익명 사용자 목록을

정의할 수 있습니다. 익명 액세스를 허용한다는 것은 비밀번호를 입력하지 않고 액세스할 수 있다는 의미입니다. 특정 액세스 유형(예: 읽기 액세스, 검색 액세스) 또는 디렉토리 내의 개별 항목이나 특정 하위 트리로 익명 액세스를 제한할 수 있습니다.

인증서

인증서 기반 인증에는 PDC(Personal Digital Certificate)를 사용한 사용자 식별 및 인증이 포함됩니다. Directory Server에 저장된 PDC에 대한 일치 및 인증서 해지 목록에 대한 확인을 수행하도록 PDC를 구성할 수 있습니다.

인증서 기반 인증 모듈을 영역에 추가하기 전에 여러가지 작업을 수행해야 합니다. 먼저, Access Manager와 함께 설치되는 웹 컨테이너를 보호하고 인증서 기반 인증에 맞게 구성해야 합니다. 인증서 기반 모듈을 활성화하기 전에 *Sun ONE Web Server 6.1* 관리자 설명서 6장 "인증서 및 키 사용"에서 이러한 초기 웹 서버 구성 단계를 참조하십시오. 이 문서는 다음 위치에서 확인할 수 있습니다.

```
http://docs.sun.com/db/prod/s1websrv#hic
```

또는 다음 위치에서 *Sun ONE Application Sever* 관리자 보안 설명서를 참조하십시오.

http://docs.sun.com/db/prod/s1appsrv#hic (`http://docs.sun.com/db/prod/s1appsrv#hic`)

주 – 인증서 기반 모듈을 사용하여 인증할 각 사용자는 사용자의 브라우저에 대한 PDC를 요청해야 합니다. 지침은 사용되는 브라우저에 따라 다릅니다. 자세한 내용은 해당 브라우저의 설명서를 참조하십시오.

이 모듈을 추가하려면 Access Manager에 영역 관리자로 로그인해야 하며 Access Manager와 웹 컨테이너에서 SSL을 구성하고 클라이언트 인증을 활성화해야 합니다. 자세한 내용은 3 장을 참조하십시오.

HTTP 기본

이 모듈은 HTTP 프로토콜에서 지원하는 기본 제공 인증인 기본 인증을 사용합니다. 웹 서버는 아이디 및 비밀번호에 대한 클라이언트 요청을 발급하고, 해당 정보를 인증된 요청에 포함하여 서버로 다시 보냅니다. Access Manager는 사용자 아이디와 비밀번호를 수신한 다음 LDAP 인증 모듈에 대해 사용자를 내부적으로 인증합니다. HTTP 기본이 제대로 작동하게 하려면 LDAP 인증 모듈을 추가해야 합니다(HTTP 기본 모듈만 추가하면 작동되지 않음). 성공적으로 인증한 사용자는 사용자 아이디와 비밀번호를 묻는 메시지를 표시하지 않고 다시 인증할 수 있습니다.

JDBC

JDBC(Java Database Connectivity) 인증 모듈은 Access Manager가 JDBC 기술 사용 드라이버를 제공하는 SQL 데이터베이스를 통해 사용자를 인증하는 기법을 지원합니다. SQL 데이터베이스에 대한 연결은 JDBC 드라이버나 JNDI 연결 풀을 통해 수행될 수 있습니다.

주 – 이 모듈은 MySQL4.0 및 Oracle 8i에서 테스트되었습니다.

LDAP

LDAP 인증 모듈에서는 사용자가 로그인할 때 특정 사용자 DN 및 비밀번호를 사용하여 LDAP Directory Server에 바인드해야 합니다. 이는 모든 영역 기반 인증에 대한 기본 인증 모듈입니다. 사용자는 Directory Server에 있는 사용자 아이디와 비밀번호를 입력하여 유효한 Access Manager 세션에 액세스할 수 있으며 해당 세션을 사용하여 사용자를 설정할 수 있습니다. 기본 영역에서는 핵심 및 LDAP 인증 모듈을 모두 자동으로 사용할 수 있게 됩니다.

구성원

구성원 인증은 `my.site.com`, `mysun.sun.com` 등과 같은 사용자 설정 사이트와 비슷하게 구현됩니다. 이 모듈이 사용 가능한 경우 사용자는 관리자의 도움 없이 계정을 만들어 사용자 설정할 수 있습니다. 사용자는 이 새 계정에 추가된 사용자로 액세스할 수 있습니다. 또한 사용자 프로필 데이터베이스에 인증 데이터 및 사용자 기본 설정으로 저장된 뷰어 인터페이스에 액세스할 수 있습니다.

MSISDN

MSISDN(Mobile Station Integrated Services Digital Network) 인증 모듈을 사용하면 휴대 전화와 같은 장치의 이동 가입자 ISDN을 사용하여 인증할 수 있습니다. 이 모듈은 비대화식 모듈입니다. 가입자 ISDN을 검색하고 이를 Directory Server에서 검증하여 번호에 맞는 사용자를 찾습니다.

RADIUS

Access Manager를 구성하여 이미 설치된 RADIUS 서버에서 작업할 수 있습니다. 이렇게 하면 회사에서 레거시 RADIUS 서버를 사용하여 인증하는 경우에 유용합니다. RADIUS 인증 모듈을 활성화하려면 두 단계 프로세스를 거쳐야 합니다.

1. RADIUS 서버를 구성합니다.

   자세한 내용은 RADIUS 서버 설명서를 참조하십시오.
2. RADIUS 인증 모듈을 등록하여 사용 가능하게 합니다.

Sun Java System Application Server에서 RADIUS 구성

RADUIS 클라이언트가 서버에 대한 소켓 연결을 형성할 경우 기본적으로 SocketPermissions 연결 권한만 Application Server의 `server.policy` 파일에 허용됩니다. RADUIS 인증이 제대로 작동하게 하려면 다음 작업에 대한 권한을 허용해야 합니다.

- 적용
- 연결
- 수신
- 결정

소켓 연결 권한을 부여하려면 Application Server의 `server.policy` 파일에 항목을 추가해야 합니다. SocketPermission은 호스트 사양과 해당 호스트에 연결하는 방법을 지정하는 작업 집합으로 구성됩니다. 호스트를 지정하는 구문은 다음과 같습니다.

```
host = hostname | IPaddress:portrange:portrange = portnumber

| -portnumberportnumber-portnumber
```

호스트는 DNS 이름, 숫자 IP 주소 또는 로컬 호스트(로컬 시스템의 경우)로 표현됩니다. 와일드카드 "*"는 DNS 이름 호스트 규격에 한 번 포함될 수 있습니다. 와일드카드가 포함되는 경우 가장 왼쪽 위치(예: `*.example.com`)에 와일드카드가 있어야 합니다.

포트(또는 포트 범위)는 선택 사항입니다. 형식이 `N-`인 포트 사양은 번호가 `N` 이상인 모든 포트를 나타냅니다. 여기서 `N`은 포트 번호입니다. 형식이 `-N`인 사양은 번호가 `N` 이하인 모든 포트를 나타냅니다.

`listen` 작업은 로컬 호스트에서 사용될 때만 적용됩니다. **결정**(호스트/IP 이름 서비스 조회 결정) 작업은 다른 작업이 있을 때 적용됩니다.

예를 들어, SocketPermissions을 만들 때 일부 코드에 다음 권한이 허용되는 경우 해당 코드를 `machine1.example.com`의 `port 1645`에 연결하고 해당 포트에서 연결을 적용할 수 있습니다.

```
permission java.net.SocketPermission machine1.example.com:1645, "connect,accept";
```

마찬가지로 일부 코드에 다음 권한이 허용되는 경우 해당 코드를 사용하여 로컬 호스트의 1024에서 65535 사이의 포트에서 연결을 적용, 연결 또는 수신할 수 있습니다.

```
permission java.net.SocketPermission "machine1.example.com:1645", "connect,accept";

permission java.net.SocketPermission "localhost:1024-", "accept,connect,listen";
```

주 – 원격 호스트에 연결을 적용하거나 연결하도록 코드 권한을 허용하면 유해 코드로 해당 데이터에 대한 액세스 권한이 없는 당사자 간에 기밀 데이터를 쉽게 전송 및 공유할 수 있기 때문에 문제가 발생할 수 있습니다. 포트 번호의 범위 대신 정확한 포트 번호를 지정하여 해당 사용 권한만 부여해야 합니다.

SafeWord

Access Manager를 구성하여 Secure Computing의 SafeWord™ 또는 SafeWord PremierAccess™ 인증 서버에 대한 SafeWord 인증 요청을 처리할 수 있습니다. Access Manager는 SafeWord 인증의 클라이언트 부분을 제공합니다. SafeWord 서버는 Access Manager가 설치되는 시스템이나 별도의 시스템에 위치할 수 있습니다.

Sun Java System Application Server에서 SafeWord 구성

SafeWord 클라이언트에서 이 서버에 소켓 연결을 수행할 경우 기본적으로 Application Server'의 `server.policy` 파일에 SocketPermissions **연결** 권한만 허용됩니다. SafeWord 인증이 제대로 작동하게 하려면 다음 작업에 대한 권한을 허용해야 합니다.

- 적용
- 연결
- 수신
- 결정

소켓 연결 권한을 부여하려면 Application Server의 `server.policy` 파일에 항목을 추가해야 합니다. SocketPermission은 호스트 사양과 해당 호스트에 연결하는 방법을 지정하는 작업 집합으로 구성됩니다. 호스트를 지정하는 구문은 다음과 같습니다.

```
host = (hostname | IPaddress)[:portrange] portrange =

portnumber | -portnumberportnumber-[portnumber]
```

host는 DNS 이름, 숫자 IP 주소 또는 로컬 호스트(로컬 시스템의 경우)로 표현됩니다. 와일드카드 "*"는 DNS 이름 호스트 규격에 한 번 포함될 수 있습니다. 와일드카드가 포함되는 경우 가장 왼쪽 위치(예: `*.example.com`)에 와일드카드가 있어야 합니다.

port(또는 portrange)는 선택 사항입니다. 형식이 `N-`인 포트 사양은 번호가 `N` 이상인 모든 포트를 나타냅니다. 여기서 `N`은 포트 번호입니다. 형식이 `-N`인 사양은 번호가 `N` 이하인 모든 포트를 나타냅니다.

`listen` 작업은 로컬 호스트에서 사용될 때만 적용됩니다. **결정**(호스트/IP 이름 서비스 조회 결정) 작업은 다른 작업이 있을 때 적용됩니다.

예를 들어, SocketPermissions을 만들 때 일부 코드에 다음 권한이 허용되는 경우 해당 코드를 `machine1.example.com`의 `port 1645`에 연결하고 해당 포트에서 연결을 적용할 수 있습니다.

```
permission java.net.SocketPermission machine1.example.com:5030, "connect,accept";
```

마찬가지로 일부 코드에 다음 권한이 허용되는 경우 해당 코드를 사용하여 로컬 호스트의 1024에서 65535 사이의 포트에서 연결을 적용, 연결 또는 수신할 수 있습니다.

```
permission java.net.SocketPermission "machine1.example.com:5030", "connect,accept";

permission java.net.SocketPermission "localhost:1024-", "accept,connect,listen";
```

주 – 원격 호스트에 연결을 적용하거나 연결하도록 코드 권한을 허용하면 유해 코드로 해당 데이터에 대한 액세스 권한이 없는 당사자 간에 기밀 데이터를 쉽게 전송 및 공유할 수 있기 때문에 문제가 발생할 수 있습니다. 포트 번호의 범위 대신 정확한 포트 번호를 지정하여 해당 사용 권한만 부여해야 합니다.

SAML

SAML(Security Assertion Markup Language) 인증 모듈은 대상 서버에서 SAML 명제를 받아 검증합니다. SAML SSO는 업그레이드(예: Access Manager 2005Q1을 Access Manager 2005Q4로 업그레이드)한 경우를 포함하여 대상 시스템에 이 모듈을 구성한 경우에만 작동합니다.

SecurID

Access Manager를 구성하여 RSA의 ACE/Server 인증 서버에 대한 SecurID 인증 요청을 처리할 수 있습니다. Access Manager는 SecurID 인증의 클라이언트 부분을 제공합니다. ACE/Server는 Access Manager가 설치되는 시스템이나 별도의 시스템에 위치할 수 있습니다. 로컬로 관리되는 사용자 아이디(`admintool`(1M) 참조)를 인증하려면 루트로 액세스해야 합니다.

SecurID 인증에서는 인증 도우미 `amsecuridd`가 사용됩니다. 이 프로세스는 메인 Access Manager 프로세스와 별도의 프로세스입니다. 시작 시에 이 도우미는 하나의 포트에서 구성 정보를 수신합니다. Access Manager를 설치하여 `nobody` 또는 루트가 아닌 사용자 아이디로 실행할 경우에도 *AccessManager-base*`/SUNWam/share/bin/amsecuridd` 프로세스는 여전히 루트로 실행되어야 합니다. `amsecuridd` 도우미에 대한 자세한 내용은 20 장을 참조하십시오.

주 – 이 릴리스의 Access Manager에서는 Linux 또는 Solaris x86 플랫폼에 대해 SecurID 인증 모듈을 사용할 수 없으며, 이 두 플랫폼에서 등록, 구성 및 사용해서는 안됩니다. SPARC 시스템용으로만 사용할 수 있습니다.

UNIX

Access Manager를 구성하여 Access Manager가 설치된 Solaris 또는 Linux 시스템에 알려진 Unix 사용자 아이디와 비밀번호에 대한 인증 요청을 처리할 수 있습니다. 영역 속성은 하나만 있지만 Unix 인증을 위한 전역 속성이 여러 개인 경우 몇 가지 시스템 고려 사항이 있습니다. 로컬로 관리되는 사용자 아이디(`admintool`(1M) 참조)를 인증하려면 루트로 액세스해야 합니다.

Unix 인증에서는 인증 도우미 `amunixd`가 사용됩니다. 이 프로세스는 메인 Access Manager 프로세스와 별도의 프로세스입니다. 시작 시에 이 도우미는 하나의 포트에서 구성 정보를 수신합니다. 각 Access Manager에는 모든 영역에 서비스를 제공하는 Unix 도우미가 하나씩만 있습니다.

Access Manager를 설치하여 `nobody` 또는 루트가 아닌 사용자 아이디로 실행할 경우에도 *AccessManager-base*`/SUNWam/share/bin/amunixd` 프로세스는 여전히 루트로 실행되어야 합니다. Unix 인증 모듈은 `localhost:58946`에 대한 소켓을 열어 `amunixd` 데몬을 호출하여 Unix 인증 요청을 수신합니다. 기본 포트에서 `amunixd` 도우미 프로세스를 실행하려면 다음 명령을 입력합니다.

```
./amunixd
```

기본 포트가 아닌 포트에서 `amunixd`를 실행하려면 다음 명령을 입력합니다.

```
./amunixd [-c portnm] [ipaddress]
```

ipaddress 및 portnumber는 AMConfig.properties의 UnixHelper.ipadrs(IPV4 형식) 및 UnixHelper.port 속성에 있습니다. amserver 명령줄 유틸리티를 통해 amunixd를 실행할 수 있습니다(amserver는 프로세스를 자동으로 실행하여 AMConfig.properties에서 포트 번호 및 IP 주소를 검색함).

/etc/nsswitch.conf 파일의 passwd 항목에 따라 인증에 /etc/passwd 및 /etc/shadow 파일을 참조하는지 NIS를 참조하는지가 결정됩니다.

Windows 데스크탑 SSO

Windows 데스크탑 SSO 인증 모듈은 Windows 2000™에 사용되는 커버로스 기반 인증 플러그인 모듈입니다. 이 모듈을 사용하면 KDC(Kerberos Distribution Center)에 대해 이미 인증을 받은 사용자는 로그인 조건(싱글 사인 온)을 다시 제출하지 않고도 Access Manager에 대해 인증을 받을 수 있습니다.

사용자는 SPNEGO(Simple and Protected GSS-API Negotiation Mechanism) 프로토콜을 통해 Access Manager에 커버로스 토큰을 제공합니다. 이 인증 모듈을 통해 Access Manager에 커버로스 기반 싱글 사인 온을 수행하려면 사용자는 클라이언트측에서 자신을 인증하도록 SPNEGO 프로토콜을 지원해야 합니다. 일반적으로 이 프로토콜을 지원하는 사용자는 이 모듈을 사용하여 Access Manager에 인증할 수 있습니다. 클라이언트측 토큰의 가용성에 따라 이 모듈은 SPENGO 토큰 또는 커버로스 토큰(두 경우 모두 동일한 프로토콜)을 제공합니다. Windows 2000 이상에서 실행되는 Microsoft Internet Explorer(5.01 이상)는 현재 이 프로토콜을 지원합니다. 또한 Mozilla 1.4 on Solaris(9 및 10)도 SPNEGO 지원 기능이 있으나 Solaris에서 SPNEGO를 지원하지 않으므로 반환되는 토큰은 커버로스 토큰뿐입니다.

주 – 커버로스 V5 인증 모듈의 새 기능을 활용하려면 JDK 1.4 이상을 사용하고 이 SPNEGO 모듈에서 커버로스 기반 SSO를 수행하려면 Java GSS API를 사용해야 합니다.

Internet Explorer의 알려진 제한 사항

WindowsDesktopSSO 인증용으로 Microsoft Internet Explorer 6.x를 사용하고, 브라우저에 WindowsDesktopSSO 모듈에서 구성된 KDC 영역과 일치하는 사용자의 커버로스/SPNEGO 토큰에 대한 액세스 권한이 없는 경우 브라우저가 WindowsDesktopSSO 모듈 인증에 실패하면 다른 모듈에 대해 올바르게 작동하지 않습니다. 이 문제의 직접적인 원인은 Internet Explorer에서 WindowsDesktopSSO 모듈 실패 후 다른 모듈의 콜백이 프롬프트에 표시되는 경우에도 브라우저에서 이를 Access Manager에 전달할 수 없기 때문이며, 이러한 불능 상태는 브라우저를 다시 시작할 때까지 계속됩니다. 즉 null 사용자 자격 증명 때문에 WindowsDesktopSSO 실패 후 수신한 모든 모듈도 실패합니다.

자세한 내용은 다음 설명서를 참조하십시오.

http://support.microsoft.com/default.aspx?scid=kb;en-us;308074
(http://support.microsoft.com/default.aspx?scid=kb;en-us;308074)

http://www.wedgetail.com/jcsi/sso/doc/guide/troubleshooting.html#ieNTLM
(http://support.microsoft.com/default.aspx?scid=kb;en-us;308074)

Windows 데스크탑 SSO 구성

Windows 데스크탑 SSO 인증을 활성화하는 두 단계 프로세스는 다음과 같습니다.

1. Windows 2000 도메인 제어기에서 사용자를 생성합니다.
2. Internet Explorer를 설정합니다.

▼ Windows 2000 도메인 제어기에서 사용자를 생성하려면

1 도메인 제어기에서 Access Manager 인증 모듈에 사용할 사용자 계정을 만듭니다.

a. 시작 메뉴에서 프로그램>관리 도구로 이동합니다.

b. 활성 디렉토리 사용자 및 컴퓨터를 선택합니다.

c. 사용자 아이디(로그인 이름)가 Access Manager 호스트 이름인 새 사용자를 만듭니다. Access Manager 호스트 이름에는 도메인 이름이 포함되지 않아야 합니다.

2 사용자 계정을 서비스 공급자 이름과 연결하고 Access Manager가 설치된 시스템으로 키탭 파일을 내보냅니다. 이를 수행하려면 다음 명령을 실행합니다.

```
ktpass -princ host/hostname.domainname@DCDOMAIN -pass password -mapuser userName-out
```

hostname.host.keytab

```
ktpass -princ HTTP/hostname.domainname@DCDOMAIN -pass
```

password -mapuser *userName*-out *hostname*

.HTTP.keytab

ktpass 명령에는 다음과 같은 매개 변수가 사용됩니다.

hostname. Access Manager를 실행하는 호스트 이름(도메인 이름 없음)입니다.

domainname . Access Manager 도메인 이름

DCDOMAIN. 도메인 제어기의 도메인 이름입니다. Access Manager 도메인 이름과 다를 수도 있습니다.

password . 사용자 계정의 비밀번호입니다. ktpass에서는 비밀번호를 확인하지 않으므로 비밀번호가 정확한지 확인합니다.

userName. 사용자 계정 아이디입니다. 호스트 이름과 같아야 합니다.

주 – 두 키탭 파일이 모두 안전하게 보존되는지 확인합니다.

서비스 템플리트 값은 다음 예와 비슷해야 합니다.

서비스 기본**:** HTTP/machine1.EXAMPLE.COM@ISQA.EXAMPLE.COM

키탭 파일 이름:/tmp/machine1.HTTP.keytab

커버로스 영역: ISQA.EXAMPLE.COM

커버로스 서버 이름:machine2.EXAMPLE.com

도메인 이름과 함께 기본 반환:false

인증 수준: 22

3 서버를 다시 시작합니다.

▼ Internet Explorer를 설정하려면

이 단계는 Microsoft Internet Explorer™ 6 이상에 적용됩니다. 이전 버전을 사용하는 경우 Access Manager가 브라우저의 인터넷 영역에 있고 고유 Windows 인증을 사용하는지 확인하십시오.

1 도구 메뉴에서 인터넷 옵션>고급/보안>보안으로 이동합니다.

2 통합된 Windows 인증 사용 옵션을 선택합니다.

3 보안>로컬 인터넷으로 이동합니다.

a. 사용자 지정 수준을 선택합니다. 사용자 인증/로그온 창에서 인트라넷 영역에서만 자동으로 로그온 옵션을 선택합니다.

b. 사이트로 가서 옵션을 모두 선택합니다.

c. 고급을 누르고 로컬 영역에 Access Manager를 추가합니다(아직 추가되지 않은 경우).

Windows NT

Access Manager를 구성하여 이미 설치된 Windows NT /Windows 2000 서버에서 작업할 수 있습니다. Access Manager는 NT 인증의 클라이언트 부분을 제공합니다.

1. NT 서버를 구성합니다. 자세한 내용은 Windows NT 서버 설명서를 참조하십시오.
2. Windows NT 인증 모듈을 추가하여 활성화하려면 Solaris 시스템의 Access Manager와 통신하도록 Samba 클라이언트를 설치해야 합니다.

Samba 클라이언트 설치

Windows NT 인증 모듈을 활성화하려면 Samba Client2.2.2를 다음 디렉토리에 다운로드하여 설치해야 합니다.

```
AccessManager-base/SUNWam/bin
```

Samba Client는 별도의 Windows NT/2000 Server를 필요로 하지 않고 Windows 시스템과 UNIX 시스템을 블렌딩하는 파일 및 인쇄 서버입니다. 자세한 내용을 보거나 Samba Client를 다운로드하려면 http://wwws.sun.com/software/download/products/3e3af224.html에 액세스하십시오.

Red Hat Linux는 Samba 클라이언트와 함께 제공됩니다. 이 클라이언트는 다음 디렉토리에 있습니다.

```
/usr/bin
```

Linux용 Windows NT 인증 모듈을 사용하여 인증하려면 다음 Access Manager 디렉토리에 클라이언트 바이너리를 복사합니다.

AccessManager-base`/sun/identity/bin`

주 – 인터페이스가 여러 개인 경우에는 추가 구성이 필요합니다. `smb.conf` 파일에서 구성에 의해 다수의 인터페이스가 설정될 수 있으므로 `mbclient`로 전달됩니다.

인증 모듈 인스턴스

기본 인증 모듈을 기반으로 영역에 대해 여러 인증 모듈 인스턴스를 만들 수 있습니다. 개별적으로 구성된 같은 인증 모듈의 여러 인스턴스를 추가할 수 있습니다.

▼ 새 인증 모듈 인스턴스를 만들려면

1. **새 인증 모듈 인스턴스를 추가할 영역의 이름을 누릅니다.**
2. **인증 탭을 선택합니다.**

주 – 관리자 인증 구성 버튼은 관리자에 대해서만 인증 서비스를 정의합니다. 관리자 인증 모듈이 최종 사용자의 모듈과 달라야 하는 경우 이 속성을 사용할 수 있습니다. 이 속성에 구성된 모듈은 콘솔에 액세스할 때 선택됩니다.

---

3. **모듈 인스턴스 목록에서 새로 만들기를 누릅니다.**
4. **인증 모듈 인스턴스의 이름을 입력합니다. 이름은 고유해야 합니다.**
5. **영역에 대한 인증 모듈의 유형을 선택합니다.**
6. **만들기를 누릅니다.**

7 새로 만든 모듈 인스턴스의 이름을 누르고 해당 모듈의 등록 정보를 편집합니다. 각 모듈 유형의 등록 정보에 대한 정의는 온라인 도움말의 인증 절을 참조하십시오.

8 이러한 단계를 반복하여 여러 개의 모듈 인스턴스를 추가합니다.

인증 체이닝

인증을 하나 이상 구성할 수 있으므로 사용자는 모든 인증에 인증 자격 증명을 전달해야 합니다. 이를 인증 체이닝이라고 합니다. Access Manager의 인증 체이닝은 인증 서비스에 통합된 JAAS 프레임워크를 사용하여 수행됩니다. 모듈 체이닝은 인증 구성 서비스 아래에 구성되어 있습니다.

▼ 새 인증 체인을 만들려면

1 새 인증 체인을 추가할 영역의 이름을 누릅니다.

2 인증 탭을 선택합니다.

3 인증 체이닝 목록에서 새로 만들기를 누릅니다.

4 인증 체인의 이름을 입력합니다.

5 만들기를 누릅니다.

6 추가를 눌러 체인에 포함할 인증 모듈 인스턴스를 정의합니다. 이를 수행하려면 인스턴스 목록에서 모듈 인스턴스 이름을 선택합니다. 이 목록에 표시된 모듈 인스턴스 이름은 모듈 인스턴스 속성에서 만들어집니다.

7 체인의 기준을 선택합니다. 이러한 플래그는 플래그가 정의된 인증 모듈에 대한 적용 기준을 설정합니다. 실행을 위한 단계가 있습니다. 필수는 가장 높고 옵션은 가장 낮습니다.

필요 모듈 인스턴스가 성공적이어야 합니다. 성공한 경우 인증 체이닝 목록의 그 다음 항목에 대해 인증이 계속됩니다. 실패한 경우 컨트롤이 응용 프로그램에 반환됩니다(인증 체이닝 목록의 그 다음 항목에 대해 인증이 진행되지 않음).

필수 이 모듈에 대한 인증이 성공적이어야 합니다. 체인의 필수 모듈 중 하나라도 실패하면 결과적으로 전체 인증 체인이 실패합니다. 그러나 필수 모듈이 성공하든 실패하든 컨트롤은 체인에서 그 다음 모듈에 대해 계속 진행됩니다.

충분 모듈 인스턴스가 반드시 성공적이지 않아도 됩니다. 성공한 경우 컨트롤이 즉시 응용 프로그램에 반환됩니다(인증 모듈 목록의 그 다음 항목에 대해 인증이 진행되지 않음). 실패한 경우 인증 체이닝 목록의 그 다음 항목에 대해 인증이 계속됩니다.

선택 사항 모듈 인스턴스가 반드시 성공적이지 않아도 됩니다. 성공 또는 실패한 경우 인증 체이닝 목록의 그 다음 항목에 대해 인증이 계속 진행됩니다.

8 체인에 대한 옵션을 입력합니다. 이렇게 하면 키=값 쌍으로 모듈에 대한 추가 옵션을 허용합니다. 여러 옵션을 사용할 경우 공백으로 구분합니다.

9 다음 속성을 정의합니다.

성공한 로그인 URL	인증 성공 시 사용자가 리디렉션되는 URL을 지정합니다.
실패한 로그인 URL	인증 실패 시 사용자가 리디렉션되는 URL을 지정합니다.
인증 사후 처리 클래스	로그인 성공 또는 실패 후에 인증 사후 처리를 사용자 정의하는 데 사용되는 Java 클래스의 이름을 정의합니다.

10 저장을 누릅니다.

인증 유형

Sun Java System Access Manager 7 2005Q4 Developer's Guide의 5 장, "Using Authentication APIs and SPIs"의 5장 "Using Authentication APIs and SPIs"를 참조하십시오. 인증 모듈을 구성하기 전에 특정 인증 모듈 이름을 포함하도록 핵심 인증 서비스 속성인 영역 인증 모듈을 수정해야 합니다.

인증 구성 서비스는 다음 인증 유형에 대한 인증 모듈을 정의하는 데 사용됩니다.

- 93 페이지 "영역 기반 인증"
- 95 페이지 "조직 기반 인증"
- 97 페이지 "역할 기반 인증"
- 100 페이지 "서비스 기반 인증"
- 103 페이지 "사용자 기반 인증"
- 105 페이지 "인증 수준 기반 인증"
- 107 페이지 "모듈 기반 인증"

이러한 인증 유형 중 하나에 대해 인증 모듈을 정의한 경우, 인증 프로세스의 성공 또는 실패 여부에 따라 사후 처리 Java 클래스 사양뿐만 아니라 리디렉션 URL을 제공하도록 해당 모듈을 구성할 수 있습니다.

인증 유형에 따른 액세스 결정 방법

이러한 방법마다 사용자 인증이 성공하기도 하고 실패하기도 합니다. 그러나 방법이 결정된 다음에는 다음 절차를 따르게 됩니다. 단계 1에서부터 단계 3까지는 인증 성공 후, 단계 4는 인증 성공 및 실패 후에 모두 나타납니다.

1. Access Manager는 인증된 사용자가 Directory Server 데이터 저장소에 정의되어 있고 프로필이 활성 상태인지 여부를 확인합니다.

핵심 인증 모듈의 사용자 프로필 속성은 Required, Dynamic, Dynamic with User Alias 또는 Ignored 중 하나로 정의될 수 있습니다. 인증 성공 후 Access Manager는 인증된 사용자가 Directory Server 데이터 저장소에 정의되어 있는지 확인하고, 사용자 프로필 값이 Required인 경우 해당 프로필이 활성 상태인지 확인합니다(이는 기본적인 경우입니다). 사용자 프로필이 Dynamically Configured 인 경우에는 인증 서비스에서 Directory Server 데이터 저장소에 사용자 프로필을 작성합니다. 사용자 프로필이 Ignore로 설정되어 있으면 사용자 검증이 수행되지 않습니다.

2. 인증 사후 처리 SPI의 실행이 완료되었습니다.

   핵심 인증 모듈에는 인증 사후 처리 클래스 이름이 그 값으로서 포함되는 인증 사후 처리 클래스 속성이 들어 있습니다. AMPostAuthProcessInterface는 사후 처리 인터페이스로서인증 성공/실패 시 또는 로그아웃 시 실행될 수 있습니다.

3. 다음 등록 정보가 세션 토큰에 추가되거나 세션 토큰에서 업데이트된 후 사용자의 세션이 활성화됩니다.

   realm. 사용자가 속한 영역의 DN입니다.

   Principal. 사용자의 DN입니다.

   Principals. 사용자가 인증한 이름의 목록입니다. (이 등록 정보에는 세로줄(|)로 구분한 목록으로 정의된 둘 이상의 값이 있을 수 있습니다.)

   UserId. 모듈에서 반환된 사용자의 DN이거나, LDAP 또는 구성원 이외의 모듈의 경우 사용자 이름입니다. (모든 Principal은 동일한 사용자에 매핑되어야 합니다. UserID는 Principal이 매핑되는 사용자 DN입니다.)

   주 – 이 등록 정보는 DN 값이 아닐 수 있습니다.

   UserToken. 사용자 이름입니다. (모든 Principal은 동일한 사용자에 매핑되어야 합니다. UserToken은 Principal이 매핑된 사용자 이름입니다.)

   Host. 클라이언트의 호스트 이름이나 IP 주소입니다.

   authLevel. 사용자의 최고 인증 수준입니다.

   AuthType. 사용자가 인증한 인증 모듈을 세로줄(|)로 구분한 목록(예: module1|module2|module3)입니다.

   clientType. 클라이언트 브라우저의 장치 유형입니다.

   Locale. 클라이언트의 로켈입니다.

   CharSet. 클라이언트에 대해 결정된 문자 집합입니다.

   Role. 역할 기반의 인증에만 적용될 수 있으며 사용자가 속한 역할입니다.

   Service. 서비스 기반의 인증에만 적용될 수 있으며 사용자가 속한 서비스입니다.

4. Access Manager에서는 인증 성공 또는 실패 후 사용자를 리디렉션할 위치에 대한 정보를 찾습니다.

   URL 리디렉션 위치는 Access Manager 페이지 또는 URL이 될 수 있습니다. 리디렉션은 Access Manager가 인증 방법을 기준으로 찾은 리디렉션의 우선 순위 순서와 해당 인증이 성공 또는 실패했는지 여부에 따라 달라집니다. 이러한 순서는 다음 인증 방법 절에서 URL 리디렉션 부분에 자세히 설명되어 있습니다.

URL 리디렉션

인증 구성 서비스에서 성공적인 인증 또는 실패한 인증에 대한 URL 리디렉션을 할당할 수 있습니다. URL은 이 서비스의 로그인 성공 URL 및 로그인 실패 URL 속성에 자동으로 정의됩니다. URL 리디렉션을 사용 가능하게 하려면 영역에 인증 구성 서비스를 추가하여 해당 서비스를 역할, 영역 또는 사용자에 대해 구성 가능하게 만들어야 합니다. 인증 구성 서비스를 추가할 경우 LDAP - 필수와 같은 인증 모듈을 추가해야 합니다.

영역 기반 인증

이 인증 방법을 사용하면 영역 또는 하위 영역에 대해 인증할 수 있습니다. Access Manager에 대한 기본 인증 방법입니다. 영역 인증 방법은 핵심 인증 모듈을 영역에 등록하고 영역 인증 구성 속성을 정의함으로써 설정됩니다.

영역 기반 인증 로그인 URL

인증 영역은 `realm` 매개 변수 또는 `domain` 매개 변수를 정의하여 사용자 인터페이스 로그인 URL에서 지정될 수 있습니다. 인증 요청 영역은 다음 매개 변수/속성에 의해 여기에 표시된 순서대로 결정됩니다.

1. `domain` 매개 변수
2. `realm` 매개 변수
3. 관리자 서비스의 `DNS Alias Names` 속성 값

   영역을 정확하게 호출한 다음에는 사용자가 인증할 인증 모듈을 핵심 인증 서비스의 영역 인증 구성 속성에서 검색합니다. 영역 기반 인증을 지정하고 초기화하는 데 사용하는 로그인 URL은 다음과 같습니다.

   ```
   http://server_name.domain_name:port/amserver/UI/Login

   http://server_name.domain_name:port/amserver/UI/Login?domain=domain_name

   http://server_name.domain_name:port/amserver/UI/Login?realm=realm_name
   ```

   정의된 매개 변수가 없을 때는 로그인 URL에 지정된 서버 호스트와 도메인으로부터 영역이 결정됩니다.

영역 기반 인증 리디렉션 URL

조직 기반 인증이 성공/실패하면 Access Manager는 사용자를 리디렉션할 위치 정보를 찾습니다. 응용 프로그램에서 이 정보를 찾는 순서는 다음과 같습니다.

성공한 영역 기반 인증 리디렉션 URL

성공한 영역 기반 인증의 리디렉션 URL은 다음 정보를 순서대로 확인하여 결정합니다.

1. 인증 모듈에서 설정한 URL
2. `goto` 로그인 URL 매개 변수에서 설정한 URL
3. 사용자 프로필(`amUser.xml`)의 `iplanet-am-user-success-url` 속성에 대해 `clientType` 사용자 정의 파일에서 설정된 URL
4. 사용자 역할 항목의 `iplanet-am-auth-login-success-url` 속성에 대해 `clientType` 사용자 정의 파일에서 설정된 URL
5. 사용자 영역 항목의 `iplanet-am-auth-login-success-url` 속성에 대해 `clientType` 사용자 정의 파일에서 설정된 URL
6. `iplanet-am-auth-login-success-url` 속성에 대해 전역 기본값으로서 `clientType` 사용자 정의 파일에서 설정된 URL
7. 사용자 프로필(`amUser.xml`)의 `iplanet-am-user-success-url` 속성에 설정된 URL
8. 사용자 역할 항목의 `iplanet-am-auth-login-success-url` 속성에 설정된 URL
9. 사용자 영역 항목의 `iplanet-am-auth-login-success-url` 속성에 설정된 URL
10. 전역 기본값으로서 `iplanet-am-auth-login-success-url` 속성에 설정된 URL

실패한 영역 기반 인증 리디렉션 URL

실패한 영역 기반 인증의 리디렉션 URL은 다음 장소를 다음과 같은 순서 대로 확인하여 결정합니다.

1. 인증 모듈에서 설정한 URL
2. `gotoOnFail` 로그인 URL 매개 변수에서 설정한 URL
3. 사용자 항목(`amUser.xml`)의 `iplanet-am-user-failure-url` 속성에 대해 `clientType` 사용자 정의 파일에서 설정된 URL
4. 사용자 역할 항목의 `iplanet-am-auth-login-failure-url` 속성에 대해 `clientType` 사용자 정의 파일에서 설정된 URL
5. 사용자 영역 항목의 `iplanet-am-auth-login-failure-url` 속성에 대해 `clientType` 사용자 정의 파일에서 설정된 URL
6. `iplanet-am-auth-login-failure-url` 속성에 대해 전역 기본값으로서 `clientType` 사용자 정의 파일에서 설정된 URL
7. 사용자 항목(`amUser.xml`)의 `iplanet-am-user-failure-url` 속성에 설정된 URL
8. 사용자 역할 항목의 `iplanet-am-auth-login-failure-url` 속성에 설정된 URL

9. 사용자 영역 항목의 iplanet-am-auth-login-failure-url 속성에 설정된 URL
10. 전역 기본값으로서 iplanet-am-auth-login-failure-url 속성에 설정된 URL

영역 기반 인증을 구성하려면

먼저 핵심 인증 서비스를 영역에 추가하여 영역에 인증 모듈을 설정합니다.

▼ 영역의 인증 속성을 구성하려면

1 인증 체인을 추가할 영역으로 이동합니다.

2 인증 탭을 누릅니다.

3 풀다운 메뉴에서 기본 인증 체인을 선택합니다.

4 풀다운 메뉴에서 관리자 인증 체인을 선택합니다. 관리자의 인증 모듈이 최종 사용자의 모듈과 달라야 하는 경우 이 속성을 사용할 수 있습니다. 기본 인증 모듈은 LDAP입니다.

5 인증 체인을 정의한 후 저장을 누릅니다.

조직 기반 인증

이 인증 유형은 레거시 모드로 설치된 Access Manager 배포에만 적용됩니다.

이 인증 방법을 사용하면 조직 또는 하위 조직에 사용자를 인증할 수 있습니다. 이는 Access Manager 인증의 기본 방법입니다. 조직 인증 방법은 핵심 인증 모듈을 조직에 등록하고 조직 인증 구성 속성을 정의함으로써 설정됩니다.

조직 기반 인증 로그인 URL

인증 조직은 사용자 인터페이스 로그인 URL에서 org 매개 변수나 domain 매개 변수를 정의하는 방법으로 지정할 수 있습니다. 인증 요청 조직은 다음 매개 변수/속성에 의해 여기에 표시된 순서대로 결정됩니다.

1. domain 매개 변수
2. org 매개 변수
3. 관리 서비스의 DNS Alias Names(조직 별칭 이름) 속성 값

   조직을 정확하게 호출한 다음에는 사용자가 인증할 인증 모듈을 핵심 인증 서비스의 조직 인증 구성 속성에서 검색합니다. 조직 기반 인증을 지정하고 초기화하는 데 사용되는 로그인 URL은 다음과 같습니다.

```
http://server_name.domain_name:port/amserver/UI/Login
```

```
http://server_name.domain_name:port/amserver/UI/Login?domain=domain_name

http://server_name.domain_name:port/amserver/UI/Login?org=org_name
```

정의된 매개 변수가 없을 때는 로그인 URL에 지정된 서버 호스트와 도메인으로부터 조직이 결정됩니다.

조직 기반 인증 리디렉션 URL

조직 기반 인증이 성공/실패하면 Access Manager는 사용자를 리디렉션할 위치 정보를 찾습니다. 응용 프로그램에서 이 정보를 찾는 순서는 다음과 같습니다.

성공한 조직 기반 인증 리디렉션 URL

성공한 조직 기반 인증의 리디렉션 URL은 다음 정보를 순서대로 확인하여 결정합니다.

1. 인증 모듈에서 설정한 URL
2. `goto` 로그인 URL 매개 변수에서 설정한 URL
3. 사용자 프로필(`amUser.xml`)의 `iplanet-am-user-success-url` 속성에 대해 `clientType` 사용자 정의 파일에서 설정된 URL
4. 사용자 역할 항목의 `iplanet-am-auth-login-success-url` 속성에 대해 `clientType` 사용자 정의 파일에서 설정된 URL
5. 사용자 조직 항목의 `iplanet-am-auth-login-success-url` 속성에 대해 `clientType` 사용자 정의 파일에서 설정된 URL
6. `iplanet-am-auth-login-success-url` 속성에 대해 전역 기본값으로서 `clientType` 사용자 정의 파일에서 설정된 URL
7. 사용자 프로필(`amUser.xml`)의 `iplanet-am-user-success-url` 속성에 설정된 URL
8. 사용자 역할 항목의 `iplanet-am-auth-login-success-url` 속성에 설정된 URL
9. 사용자 조직 항목의 `iplanet-am-auth-login-success-url` 속성에 설정된 URL
10. 전역 기본값으로서 `iplanet-am-auth-login-success-url` 속성에 설정된 URL

실패한 조직 기반 인증 리디렉션 URL

실패한 조직 기반 인증의 리디렉션 URL은 다음 장소를 순서대로 확인하여 결정합니다.

1. 인증 모듈에서 설정한 URL
2. `gotoOnFail` 로그인 URL 매개 변수에서 설정한 URL
3. 사용자 항목(`amUser.xml`)의 `iplanet-am-user-failure-url` 속성에 대해 `clientType` 사용자 정의 파일에서 설정된 URL
4. 사용자 역할 항목의 `iplanet-am-auth-login-failure-url` 속성에 대해 `clientType` 사용자 정의 파일에서 설정된 URL

5. 사용자 조직 항목의 iplanet-am-auth-login-failure-url 속성에 대해 clientType 사용자 정의 파일에서 설정된 URL
6. iplanet-am-auth-login-failure-url 속성에 대해 전역 기본값으로서 clientType 사용자 정의 파일에서 설정된 URL
7. 사용자 항목(amUser.xml)의 iplanet-am-user-failure-url 속성에 설정된 URL
8. 사용자 역할 항목의 iplanet-am-auth-login-failure-url 속성에 설정된 URL
9. 사용자 조직 항목의 iplanet-am-auth-login-failure-url 속성에 설정된 URL
10. 전역 기본값으로서 iplanet-am-auth-login-failure-url 속성에 설정된 URL

조직 기반 인증을 구성하려면

먼저 핵심 인증 서비스를 조직에 추가하여 조직에 인증 모듈을 설정합니다.

▼ 조직의 인증 속성을 구성하려면

1 인증 체인을 추가할 조직으로 이동합니다.

2 인증 탭을 누릅니다.

3 풀다운 메뉴에서 기본 인증 체인을 선택합니다.

4 풀다운 메뉴에서 관리자 인증 체인을 선택합니다. 관리자의 인증 모듈이 최종 사용자의 모듈과 달라야 하는 경우 이 속성을 사용할 수 있습니다. 기본 인증 모듈은 LDAP입니다.

5 인증 체인을 정의한 후 저장을 누릅니다.

역할 기반 인증

이 인증 방법을 사용하면 영역이나 하위 영역 내의 (정적 또는 필터링된) 역할에 인증할 수 있습니다.

주 – 인증 구성 서비스를 역할의 인스턴스로 등록하기 전에 먼저 영역에 등록해야 합니다.

인증이 성공하려면 사용자는 해당 역할에 속하고 이 역할에 구성된 인증 구성 서비스 인스턴스에 정의된 모듈마다 인증해야 합니다. 역할 기반 인증의 인스턴스마다 다음 속성을 지정할 수 있습니다.

충돌 해결 수준. 같은 사용자의 서로 다른 역할에 정의된 인증 구성 서비스 인스턴스에 대해 우선 순위 수준을 설정합니다. 예를 들어, User1이 Role1 및 Role2에 모두 지정되고 Role1에 더

높은 충돌 해결 수준이 설정될 경우 사용자가 인증을 시도할 때 성공 또는 실패 리디렉션과 인증 사후 프로세스에 대해 Role1에 더 높은 우선 순위가 적용됩니다.

인증 구성. 역할의 인증 프로세스에 구성된 인증 모듈을 정의합니다.

로그인 성공 **URL.** 성공한 인증에서 사용자가 리디렉션될 URL을 정의합니다.

로그인 실패 **URL**. 실패한 인증에서 사용자가 리디렉션될 URL을 정의합니다.

인증 사후 처리 클래스. 인증 사후 인터페이스를 정의합니다.

역할 기반 인증 로그인 URL

역할 기반 인증은 role 매개 변수를 정의하는 방법으로 사용자 인터페이스 로그인 URL에서 지정할 수 있습니다. 역할을 정확하게 호출한 다음에는 사용자가 인증할 인증 모듈을 해당 역할에 대해 정의된 인증 구성 서비스 인스턴스에서 검색합니다.

이 역할 기반 인증을 지정하고 초기화하는 데 사용되는 URL은 다음과 같습니다.

```
http://server_name.domain_name:port/amserver/UI/Login?role=role_name
```

```
http://server_name.domain_name:port/amserver/UI/Login?realm=realm_name&role=role_name
```

realm 매개 변수가 구성되어 있지 않은 경우 역할이 속한 영역은 로그인 URL 자체에 지정된 서버 호스트와 도메인으로 결정됩니다.

역할 기반 인증 리디렉션 URL

역할 기반 인증이 성공/실패하면 Access Manager는 사용자를 리디렉션할 위치 정보를 찾습니다. 응용 프로그램에서 이 정보를 찾는 순서는 다음과 같습니다.

성공한 역할 기반 인증 리디렉션 URL

성공한 역할 기반 인증의 리디렉션 URL은 다음 장소를 순서대로 확인하여 결정합니다.

1. 인증 모듈에서 설정한 URL
2. goto 로그인 URL 매개 변수에서 설정한 URL
3. 사용자 프로필(amUser.xml)의 iplanet-am-user-success-url 속성에 대해 clientType 사용자 정의 파일에서 설정된 URL
4. 사용자가 인증한 역할의 iplanet-am-auth-login-success-url 속성에 대해 clientType 사용자 정의 파일에서 설정된 URL
5. 인증된 사용자의 다른 역할 항목의 iplanet-am-auth-login-success-url 속성에 대해 clientType 사용자 정의 파일에서 설정된 URL(이전 리디렉션 URL이 실패한 경우 이 옵션으로 대체됩니다.)

6. 사용자 영역 항목의 iplanet-am-auth-login-success-url 속성에 대해 clientType 사용자 정의 파일에서 설정된 URL
7. iplanet-am-auth-login-success-url 속성에 대해 전역 기본값으로서 clientType 사용자 정의 파일에서 설정된 URL
8. 사용자 프로필(amUser.xml)의 iplanet-am-user-success-url 속성에 설정된 URL
9. 사용자가 인증한 역할의 iplanet-am-auth-login-success-url 속성에 설정된 URL
10. 인증된 사용자의 다른 역할 항목의 iplanet-am-auth-login-success-url 속성에 설정된 URL(이전 리디렉션 URL이 실패한 경우 이 옵션으로 대체됩니다.)
11. 사용자 영역 항목의 iplanet-am-auth-login-success-url 속성에 설정된 URL
12. 전역 기본값으로서 iplanet-am-auth-login-success-url 속성에 설정된 URL

실패한 역할 기반 인증 리디렉션 URL

실패한 역할 기반 인증의 리디렉션 URL은 다음 장소를 순서대로 확인하여 결정합니다.

1. 인증 모듈에서 설정한 URL
2. goto 로그인 URL 매개 변수에서 설정한 URL
3. 사용자 프로필(amUser.xml)의 iplanet-am-user-failure-url 속성에 대해 clientType 사용자 정의 파일에서 설정된 URL
4. 사용자가 인증한 역할의 iplanet-am-auth-login-failure-url 속성에 대해 clientType 사용자 정의 파일에서 설정된 URL
5. 인증된 사용자의 다른 역할 항목의 iplanet-am-auth-login-failure-url 속성에 대해 clientType 사용자 정의 파일에서 설정된 URL(이전 리디렉션 URL이 실패한 경우 이 옵션으로 대체됩니다.)
6. 사용자 영역 항목의 iplanet-am-auth-login-failure-url 속성에 대해 clientType 사용자 정의 파일에서 설정된 URL
7. iplanet-am-auth-login-failure-url 속성에 대해 전역 기본값으로서 clientType 사용자 정의 파일에서 설정된 URL
8. 사용자 프로필(amUser.xml)의 iplanet-am-user-failure-url 속성에 설정된 URL
9. 사용자가 인증한 역할의 iplanet-am-auth-login-failure-url 속성에 설정된 URL
10. 인증된 사용자의 다른 역할 항목의 iplanet-am-auth-login-failure-url 속성에 설정된 URL(이전 리디렉션 URL이 실패한 경우 이 옵션으로 대체됩니다.)
11. 사용자 영역 항목의 iplanet-am-auth-login-failure-url 속성에 설정된 URL
12. 전역 기본값으로서 iplanet-am-auth-login-failure-url 속성에 설정된 URL

▼ 역할 기반 인증을 구성하려면

1. **인증 구성 서비스를 추가할 영역(또는 조직)으로 이동합니다.**
2. **주제 탭을 누릅니다.**
3. **필터링된 역할 또는 역할을 누릅니다.**
4. **인증 구성을 설정할 역할을 선택합니다.**
   인증 구성 서비스가 역할에 추가되지 않은 경우 추가를 누르고 인증 서비스를 선택하고 다음을 누릅니다.
5. **풀다운 메뉴에서 활성화할 기본 인증 체인을 선택합니다.**
6. **저장을 누릅니다.**

주 – 새 역할을 만들 경우 인증 구성 서비스가 해당 역할에 자동으로 할당되지 않습니다. 새 역할을 만들기 전에 역할 프로필 페이지의 위쪽에 있는 인증 구성 서비스 옵션을 선택하십시오.

역할 기반 인증이 사용 가능한 경우 구성원을 구성할 필요가 없으므로 LDAP 인증 모듈을 기본값으로 그대로 사용할 수 있습니다.

서비스 기반 인증

이 인증 방법을 사용하면 영역 또는 하위 영역에 등록된 특정 서비스나 응용 프로그램에 인증할 수 있습니다. 이러한 서비스는 인증 구성 서비스 내에 서비스 인스턴스로 구성되고 인스턴스 이름과 연관됩니다. 인증이 성공하려면 사용자는 해당 서비스에 구성된 인증 구성 서비스 인스턴스에 정의된 모듈마다 인증해야 합니다. 서비스 기반 인증의 인스턴스마다 다음 속성을 지정할 수 있습니다.

인증 구성**.**서비스의 인증 프로세스에 구성된 인증 모듈을 정의합니다.

로그인 성공 **URL.**성공한 인증에서 사용자가 리디렉션될 URL을 정의합니다.

로그인 실패 **URL**. 실패한 인증에서 사용자가 리디렉션될 URL을 정의합니다.

인증 사후 처리 클래스**.** 인증 사후 인터페이스를 정의합니다.

서비스 기반 인증 로그인 URL

서비스 기반 인증은 service 매개 변수를 정의하는 방법으로 사용자 인터페이스 로그인 URL에서 지정할 수 있습니다. 서비스를 호출한 다음에는 해당 서비스에 대해 정의된 인증 구성 서비스로부터 사용자가 인증할 인증 모듈을 검색합니다.

서비스 기반 인증을 지정하고 초기화하는 데 사용되는 URL은 다음과 같습니다.

```
http://server_name.domain_name:port/amserver/UI/

Login?service=auth-chain-name
```

및

```
http://server_name.domain_name:port/amserver/UI/Login?realm=realm_name&service=auth-chain-name
```

e

org 매개 변수를 지정하지 않은 경우에는 로그인 URL 자체에 지정된 서버 호스트와 도메인으로부터 영역이 결정됩니다.

서비스 기반 인증 리디렉션 URL

서비스 기반 인증이 성공/실패하면 Access Manager는 사용자를 리디렉션할 위치 정보를 찾습니다. 응용 프로그램에서 이 정보를 찾는 순서는 다음과 같습니다.

성공한 서비스 기반 인증 리디렉션 URL

성공한 서비스 기반 인증의 리디렉션 URL은 다음 정보를 순서대로 확인하여 결정합니다.

1. 인증 모듈에서 설정한 URL
2. goto 로그인 URL 매개 변수에서 설정한 URL
3. 사용자 프로필(amUser.xml)의 iplanet-am-user-success-url 속성에 대해 clientType 사용자 정의 파일에서 설정된 URL
4. 사용자가 인증한 서비스의 iplanet-am-auth-login-success-url 속성에 대해 clientType 사용자 정의 파일에서 설정된 URL
5. 사용자 역할 항목의 iplanet-am-auth-login-success-url 속성에 대해 clientType 사용자 정의 파일에서 설정된 URL
6. 사용자 영역 항목의 iplanet-am-auth-login-success-url 속성에 대해 clientType 사용자 정의 파일에서 설정된 URL
7. iplanet-am-auth-login-success-url 속성에 대해 전역 기본값으로서 clientType 사용자 정의 파일에서 설정된 URL
8. 사용자 프로필(amUser.xml)의 iplanet-am-user-success-url 속성에 설정된 URL
9. 사용자가 인증한 서비스의 iplanet-am-auth-login-success-url 속성에 설정된 URL

10. 사용자 역할 항목의 iplanet-am-auth-login-success-url 속성에 설정된 URL
11. 사용자 영역 항목의 iplanet-am-auth-login-success-url 속성에 설정된 URL
12. 전역 기본값으로서 iplanet-am-auth-login-success-url 속성에 설정된 URL

실패한 서비스 기반 인증 리디렉션 URL

실패한 서비스 기반 인증의 리디렉션 URL은 다음 장소를 순서대로 확인하여 결정합니다.

1. 인증 모듈에서 설정한 URL
2. goto 로그인 URL 매개 변수에서 설정한 URL
3. 사용자 프로필(amUser.xml)의 iplanet-am-user-failure-url 속성에 대해 clientType 사용자 정의 파일에서 설정된 URL
4. 사용자가 인증한 서비스의 iplanet-am-auth-login-failure-url 속성에 대해 clientType 사용자 정의 파일에서 설정된 URL
5. 사용자 역할 항목의 iplanet-am-auth-login-failure-url 속성에 대해 clientType 사용자 정의 파일에서 설정된 URL
6. 사용자 영역 항목의 iplanet-am-auth-login-failure-url 속성에 대해 clientType 사용자 정의 파일에서 설정된 URL
7. iplanet-am-auth-login-failure-url 속성에 대해 전역 기본값으로서 clientType 사용자 정의 파일에서 설정된 URL
8. 사용자 프로필(amUser.xml)의 iplanet-am-user-failure-url 속성에 설정된 URL
9. 사용자가 인증한 서비스의 iplanet-am-auth-login-failure-url 속성에 설정된 URL
10. 사용자 역할 항목의 iplanet-am-auth-login-failure-url 속성에 설정된 URL
11. 사용자 영역 항목의 iplanet-am-auth-login-failure-url 속성에 설정된 URL
12. 전역 기본값으로서 iplanet-am-auth-login-failure-url 속성에 설정된 URL

▼ 서비스 기반 인증을 구성하려면

인증 구성 서비스를 추가한 다음 서비스에 대한 인증 모듈을 설정합니다. 구성 방법:

1 서비스 기반 인증을 구성할 영역을 선택합니다.

2 인증 탭을 누릅니다.

3 인증 모듈 인스턴스를 만듭니다.

4 인증 체인을 만듭니다.

5 저장을 누릅니다.

6 **영역에 대한 서비스 기반 인증에 액세스하려면 다음 주소를 입력합니다.**

`http://`*server_name.domain_name:port*`/amserver/UI/Login?realm=`*realm_name*`&service=`*auth-chain-name*

사용자 기반 인증

이 인증 방법을 사용하면 사용자에 대해 특별히 구성된 인증 프로세스를 인증할 수 있습니다. 프로세스는 사용자 프로필의 사용자 인증 구성 속성 값으로 구성됩니다. 인증이 성공하려면 정의된 모듈마다 인증해야 합니다.

사용자 기반 인증 로그인 URL

사용자 기반 인증은 사용자 인터페이스 로그인 URL에서 user 매개 변수를 정의하는 방법으로 지정할 수 있습니다. 사용자를 정확하게 호출한 다음에는 사용자가 인증할 인증 모듈을 정의된 사용자 인증 구성 인스턴스에서 검색합니다.

이 역할 기반 인증을 지정하고 초기화하는 데 사용되는 URL은 다음과 같습니다.

```
http://server_name.domain_name:port/amserver/UI/Login?user=user_name
```

```
http://server_name.domain_name:port/amserver/UI/Login?org=org_name&user=user_name
```

realm 매개 변수를 지정하지 않은 경우 역할이 속한 영역은 로그인 URL 자체에 지정된 서버 호스트와 도메인에서 결정됩니다.

사용자 별칭 목록 속성

사용자 기반 인증에 대한 요청을 받으면 인증 서비스에서는 먼저 사용자가 유효한 사용자인지 확인하고 그에 대한 인증 구성 데이터를 검색합니다. 사용자 로그인 URL 매개 변수 값과 관련하여 유효한 사용자 프로필이 둘 이상 있는 경우에는 모든 프로필이 지정된 사용자에 매핑되어야 합니다. 사용자 프로필의 사용자 별칭 속성(`iplanet-am-user-alias-list`)은 해당 사용자에 속한 다른 프로필을 정의할 수 있는 위치입니다. 매핑이 실패하면 사용자는 유효한 세션에서 거부됩니다. 사용자 중 하나가 최상위 관리자이므로 사용자 매핑 검증이 수행되지 않고 사용자가 최상위 관리자 권한을 가진 경우는 예외가 될 수 있습니다.

사용자 기반 인증 리디렉션 URL

사용자 기반 인증이 성공/실패하면 Access Manager는 사용자를 리디렉션할 위치 정보를 찾습니다. 응용 프로그램에서 이 정보를 찾는 순서는 다음과 같습니다.

성공한 사용자 기반 인증 리디렉션 URL

성공한 사용자 기반 인증의 리디렉션 URL은 다음 장소를 순서대로 확인하여 결정합니다.

1. 인증 모듈에서 설정한 URL
2. `goto` 로그인 URL 매개 변수에서 설정한 URL
3. 사용자 프로필(`amUser.xml`)의 `iplanet-am-user-success-url` 속성에 대해 `clientType` 사용자 정의 파일에서 설정된 URL
4. 사용자 역할 항목의 `iplanet-am-auth-login-success-url` 속성에 대해 `clientType` 사용자 정의 파일에서 설정된 URL
5. 사용자 영역 항목의 `iplanet-am-auth-login-success-url` 속성에 대해 `clientType` 사용자 정의 파일에서 설정된 URL
6. `iplanet-am-auth-login-success-url` 속성에 대해 전역 기본값으로서 `clientType` 사용자 정의 파일에서 설정된 URL
7. 사용자 프로필(`amUser.xml`)의 `iplanet-am-user-success-url` 속성에 설정된 URL
8. 사용자 역할 항목의 `iplanet-am-auth-login-success-url` 속성에 설정된 URL
9. 사용자 영역 항목의 `iplanet-am-auth-login-success-url` 속성에 설정된 URL
10. 전역 기본값으로서 `iplanet-am-auth-login-success-url` 속성에 설정된 URL

실패한 사용자 기반 인증 리디렉션 URL

실패한 사용자 기반 인증의 리디렉션 URL은 다음 장소를 순서대로 확인하여 결정합니다.

1. 인증 모듈에서 설정한 URL
2. `gotoOnFail` 로그인 URL 매개 변수에서 설정한 URL
3. 사용자 항목(`amUser.xml`)의 `iplanet-am-user-failure-url` 속성에 대해 `clientType` 사용자 정의 파일에서 설정된 URL
4. 사용자 역할 항목의 `iplanet-am-auth-login-failure-url` 속성에 대해 `clientType` 사용자 정의 파일에서 설정된 URL
5. 사용자 영역 항목의 `iplanet-am-auth-login-failure-url` 속성에 대해 `clientType` 사용자 정의 파일에서 설정된 URL
6. `iplanet-am-auth-login-failure-url` 속성에 대해 전역 기본값으로서 `clientType` 사용자 정의 파일에서 설정된 URL
7. 사용자 항목(`amUser.xml`)의 `iplanet-am-user-failure-url` 속성에 설정된 URL
8. 사용자 역할 항목의 `iplanet-am-auth-login-failure-url` 속성에 설정된 URL
9. 사용자 영역 항목의 `iplanet-am-auth-login-failure-url` 속성에 설정된 URL
10. 전역 기본값으로서 `iplanet-am-auth-login-failure-url` 속성에 설정된 URL

▼ 사용자 기반 인증을 구성하려면

1 **사용자에 대해 인증을 구성할 영역으로 이동합니다.**

2 **주제 탭을 누르고 사용자를 누릅니다.**

3 **수정할 사용자의 이름을 누릅니다.**
사용자 프로필이 표시됩니다.

주 – 새 사용자를 만들 경우 인증 구성 서비스가 사용자에 자동으로 할당되지 않습니다. 사용자를 만들기 전에 서비스 프로필에 있는 인증 구성 서비스 옵션을 선택하십시오. 이 옵션을 선택하지 않으면 사용자가 해당 역할에 대해 정의된 인증 구성을 상속하지 못합니다.

---

4 **사용자 인증 구성 속성에서 적용할 인증 체인을 선택합니다.**

5 **저장을 누릅니다.**

인증 수준 기반 인증

각 인증 모듈에 해당 인증 수준에 대한 정수 값을 연결할 수 있습니다. 서비스 구성에서 인증 모듈의 등록 정보 화살표를 누르고 모듈의 인증 수준 속성에 해당하는 값을 변경하여 인증 수준을 할당할 수 있습니다. 높은 인증 수준은 사용자가 하나 또는 여러 인증 모듈에 인증을 얻은 후에 사용자에 높은 신뢰도를 정의합니다.

사용자가 모듈에 성공적으로 인증하면 인증 수준이 사용자의 SSO 토큰에 설정됩니다. 사용자가 여러 인증 모듈에 인증해야 하는 경우 성공적으로 인증하면 최고 인증 수준 값이 사용자의 SSO 토큰에 설정됩니다.

사용자가 서비스에 대한 액세스를 시도한 경우 서비스는 사용자의 SSO 토큰에서 인증 수준을 확인하여 사용자에게 액세스를 허용할지 여부를 결정할 수 있습니다. 그런 다음 설정된 인증 수준을 사용하여 인증 모듈을 통해 이동하도록 사용자를 리디렉션합니다.

사용자는 특정 인증 수준을 사용하여 인증 모듈에 액세스 할 수도 있습니다. 예를 들어, 다음 구문을 사용하여 로그인을 수행합니다.

```
http://hostname:port/deploy_URI/UI/Login?authlevel=
```

auth_level_value

인증 수준이 *auth_level_value*보다 크거나 같은 모든 모듈은 사용자가 선택할 수 있는 인증 메뉴로 표시됩니다. 일치하는 모듈이 하나이면 이 인증 모듈에 대한 인증 페이지가 직접 표시됩니다.

이 인증 방법을 사용하면 관리자가 ID로 인증할 수 있는 모듈의 보안 수준을 지정할 수 있습니다. 인증 모듈마다 별도의 인증 수준 속성이 있고 이 속성의 값은 유효한 정수로 정의될 수 있습니다. 인증 수준 기반 인증을 사용하면 인증 서비스에서 인증 모듈을 포함하는 메뉴가 있는 모듈 로그인 페이지를 표시하는데, 이 인증 모듈의 인증 수준은 로그인 URL 매개 변수에서 지정한 값보다 크거나 같습니다. 사용자는 제시된 목록에서 모듈을 선택할 수 있습니다. 모듈을 선택하면 나머지 프로세스는 모듈 기반 인증에 따라 진행됩니다.

인증 수준 기반 인증 로그인 URL

인증 수준 기반 인증은 authlevel 매개 변수를 정의하는 방법으로 사용자 인터페이스 로그인 URL에서 지정할 수 있습니다. 관련된 모듈 목록이 있는 로그인 화면을 호출한 후 사용자는 인증할 모듈을 하나 선택해야 합니다. 인증 수준 기반 인증을 지정하고 초기화하는 데 사용되는 URL은 다음과 같습니다.

```
http://server_name.domain_name:port/amserver/UI/Login?authlevel=authentication_level
```

및

```
http://server_name.domain_name:port/amserver/UI/

Login?realm=realm_name&authlevel=authentication_level
```

`realm` 매개 변수를 지정하지 않은 경우 사용자가 속한 영역은 로그인 URL 자체에 지정된 서버 호스트와 도메인으로부터 결정됩니다.

인증 수준 기반 인증 리디렉션 URL

인증 수준 기반 인증이 성공/실패하면 Access Manager는 사용자를 리디렉션할 위치 정보를 찾습니다. 응용 프로그램에서 이 정보를 찾는 순서는 다음과 같습니다.

성공한 인증 수준 기반 인증 리디렉션 URL

성공한 인증 수준 기반 인증의 리디렉션 URL은 다음 정보를 순서대로 확인하여 결정합니다.

1. 인증 모듈에서 설정한 URL
2. `goto` 로그인 URL 매개 변수에서 설정한 URL
3. 사용자 프로필(`amUser.xml`)의 `iplanet-am-user-success-url` 속성에 대해 `clientType` 사용자 정의 파일에서 설정된 URL
4. 사용자 역할 항목의 `iplanet-am-auth-login-success-url` 속성에 대해 `clientType` 사용자 정의 파일에서 설정된 URL
5. 사용자 영역 항목의 `iplanet-am-auth-login-success-url` 속성에 대해 `clientType` 사용자 정의 파일에서 설정된 URL
6. `iplanet-am-auth-login-success-url` 속성에 대해 전역 기본값으로서 `clientType` 사용자 정의 파일에서 설정된 URL

7. 사용자 프로필(amUser.xml)의 iplanet-am-user-success-url 속성에 설정된 URL
8. 사용자 역할 항목의 iplanet-am-auth-login-success-url 속성에 설정된 URL
9. 사용자 영역 항목의 iplanet-am-auth-login-success-url 속성에 설정된 URL
10. 전역 기본값으로서 iplanet-am-auth-login-success-url 속성에 설정된 URL

실패한 인증 수준 기반 인증 리디렉션 URL

실패한 인증 수준 기반 인증의 리디렉션 URL은 다음 정보를 순서대로 확인하여 결정합니다.

1. 인증 모듈에서 설정한 URL
2. gotoOnFail 로그인 URL 매개 변수에서 설정한 URL
3. 사용자 항목(amUser.xml)의 iplanet-am-user-failure-url 속성에 대해 clientType 사용자 정의 파일에서 설정된 URL
4. 사용자 역할 항목의 iplanet-am-auth-login-failure-url 속성에 대해 clientType 사용자 정의 파일에서 설정된 URL
5. 사용자 영역 항목의 iplanet-am-auth-login-failure-url 속성에 대해 clientType 사용자 정의 파일에서 설정된 URL
6. iplanet-am-auth-login-failure-url 속성에 대해 전역 기본값으로서 clientType 사용자 정의 파일에서 설정된 URL
7. 사용자 항목(amUser.xml)의 iplanet-am-user-failure-url 속성에 설정된 URL
8. 사용자 역할 항목의 iplanet-am-auth-login-failure-url 속성에 설정된 URL
9. 사용자 영역 항목의 iplanet-am-auth-login-failure-url 속성에 설정된 URL
10. 전역 기본값으로서 iplanet-am-auth-login-failure-url 속성에 설정된 URL

모듈 기반 인증

다음 구문을 사용하여 특정 인증 모듈에 액세스할 수 있습니다.

http://*hostname:port*/*deploy_URI*/UI/Login?module=

module_name

인증 모듈에 액세스하기 전에 인증 모듈 이름을 포함하도록 핵심 인증 서비스 속성인 영역 인증 모듈을 수정해야 합니다. 인증 모듈 이름이 이 속성에 없으면 사용자가 인증하려고 시도할 때 "인증 모듈이 거부되었습니다"라는 페이지가 표시됩니다.

이 인증 방법을 사용하면 사용자가 인증할 모듈을 지정할 수 있습니다. 지정된 모듈은 사용자가 액세스하는 영역 또는 하위 영역에 등록되어야 합니다. 이 모듈은 영역의 핵심 인증 서비스의 영역 인증 모듈 속성에서 구성됩니다. 이러한 모듈 기반 인증 요청을 받으면 인증 서비스에서 모듈이 정확하게 구성되었는지 확인하고 모듈이 정의되지 않은 경우에는 사용자 액세스가 거부됩니다.

모듈 기반 인증 로그인 URL

모듈 기반 인증은 사용자 인터페이스 로그인 URL에서 module 매개 변수를 정의하는 방법으로 지정할 수 있습니다. 모듈 기반 인증을 지정하고 초기화하는 데 사용되는 URL은 다음과 같습니다.

```
http://server_name.domain_name:port/amserver/UI/Login?module=authentication_module_name
```

```
http://server_name.domain_name:port/amserver/UI/
```

```
Login?org=org_name&module=authentication_module_name
```

`org` 매개 변수를 지정하지 않은 경우 사용자가 속한 영역은 로그인 URL 자체에 지정된 서버 호스트와 도메인으로부터 결정됩니다.

모듈 기반 인증 리디렉션 URL

모듈 기반 인증이 성공/실패하면 Access Manager는 사용자를 리디렉션할 위치 정보를 찾습니다. 응용 프로그램에서 이 정보를 찾는 순서는 다음과 같습니다.

성공한 모듈 기반 인증 리디렉션 URL

성공한 모듈 기반 인증의 리디렉션 URL은 다음 정보를 순서대로 확인하여 결정합니다.

1. 인증 모듈에서 설정한 URL
2. `goto` 로그인 URL 매개 변수에서 설정한 URL
3. 사용자 프로필(`amUser.xml`)의 `iplanet-am-user-success-url` 속성에 대해 `clientType` 사용자 정의 파일에서 설정된 URL
4. 사용자 역할 항목의 `iplanet-am-auth-login-success-url` 속성에 대해 `clientType` 사용자 정의 파일에서 설정된 URL
5. 사용자 영역 항목의 `iplanet-am-auth-login-success-url` 속성에 대해 `clientType` 사용자 정의 파일에서 설정된 URL
6. `iplanet-am-auth-login-success-url` 속성에 대해 전역 기본값으로서 `clientType` 사용자 정의 파일에서 설정된 URL
7. 사용자 프로필(`amUser.xml`)의 `iplanet-am-user-success-url` 속성에 설정된 URL
8. 사용자 역할 항목의 `iplanet-am-auth-login-success-url` 속성에 설정된 URL
9. 사용자 영역 항목의 `iplanet-am-auth-login-success-url` 속성에 설정된 URL
10. 전역 기본값으로서 `iplanet-am-auth-login-success-url` 속성에 설정된 URL

실패한 모듈 기반 인증 리디렉션 URL

실패한 모듈 기반 인증의 리디렉션 URL은 다음 장소를 순서대로 확인하여 결정합니다.

1. 인증 모듈에서 설정한 URL

2. gotoOnFail 로그인 URL 매개 변수에서 설정한 URL
3. 사용자 항목(amUser.xml)의 iplanet-am-user-failure-url 속성에 대해 clientType 사용자 정의 파일에서 설정된 URL
4. 사용자 역할 항목의 iplanet-am-auth-login-failure-url 속성에 대해 clientType 사용자 정의 파일에서 설정된 URL
5. 사용자 영역 항목의 iplanet-am-auth-login-failure-url 속성에 대해 clientType 사용자 정의 파일에서 설정된 URL
6. iplanet-am-auth-login-failure-url 속성에 대해 전역 기본값으로서 clientType 사용자 정의 파일에서 설정된 URL
7. 사용자 역할 항목의 iplanet-am-auth-login-failure-url 속성에 설정된 URL
8. 사용자 영역 항목의 iplanet-am-auth-login-failure-url 속성에 설정된 URL
9. 전역 기본값으로서 iplanet-am-auth-login-failure-url 속성에 설정된 URL

사용자 인터페이스 로그인 URL

인증 서비스 사용자 인터페이스는 웹 브라우저의 위치 표시줄에 로그인 URL을 입력하는 방법으로 액세스할 수 있습니다. 다음과 같이 URL을 입력합니다.

http://*AccessManager-root*/.*domain_name*:*port* /*service_deploy_uri* /UI/Login

---

주 – 설치 도중 *service_deploy_uri*가 amserver로 구성됩니다. 이러한 기본 서비스 배포 URI은 이 설명서 전반에 걸쳐 사용됩니다.

사용자 인터페이스 로그인 URL에 로그인 URL 매개 변수가 추가되어 특정 인증 방법이나 성공 또는 실패한 인증 리디렉션 URL을 정의합니다.

로그인 URL 매개 변수

URL 매개 변수는 URL의 끝에 추가되는 이름/값 쌍입니다. 매개 변수는 물음표(?)로 시작하며name=value 형식으로 사용됩니다. 다음과 같이 여러 개의 매개 변수를 하나의 로그인 URL로 조합할 수 있습니다.

```
http://server_name.domain_name:port/amserver/UI/

Login?module=LDAP&locale=ja&goto=http://www.sun.com
```

매개 변수가 둘 이상인 경우 앰퍼샌드(&)로 분리됩니다. 그러나 매개 변수 조합은 다음 지침을 지켜야 합니다.

- 각 매개 변수는 하나의 URL에서 한 번만 사용되어야 합니다. 예를 들어, `module=LDAP&module=NT`는 사용할 수 없습니다.
- `org` 매개 변수와 `domain` 매개 변수는 모두 로그인 영역을 결정합니다. 이 경우에는 로그인 URL에서 두 매개 변수 중 하나만 사용해야 합니다. 두 매개 변수를 모두 사용하면서 우선 순위를 지정하지 않으면 하나만 적용됩니다.
- `user`, `role`, `service`, `module` 및 `authlevel` 매개 변수는 각각의 기준에 따라 인증 모듈을 정의하는 매개 변수입니다. 따라서 로그인 URL에는 이들 중 하나만 사용해야 합니다. 매개 변수를 두 개 이상 사용하면서 우선 순위를 지정하지 않으면 하나만 적용됩니다.

다음 절에서는 사용자 인터페이스 로그인 URL에 붙고 웹 브라우저의 위치 표시줄에 입력될 때 여러 가지 인증 기능을 수행하는 매개 변수를 설명합니다.

주 – 영역에 전사적으로 배포할 인증 URL 및 매개 변수를 간소화하기 위해 관리자는 간단한 URL을 사용하여 HTML 페이지를 구성할 수 있는데 이 페이지에는 구성된 모든 인증 방법에서 사용할 복잡한 로그인 URL 링크가 포함됩니다.

---

goto 매개 변수

`goto=`*successful_authentication_URL* 매개 변수는 인증 구성 서비스의 로그인 성공 URL에 정의된 값 대신 사용됩니다. 이 매개 변수는 인증이 성공하면 지정된 URL로 연결됩니다. `goto=logout_URL` 매개 변수는 사용자 로그아웃 시 지정된 URL로 연결하기 위해 사용합니다. 성공적인 인증 URL의 예는 다음과 같습니다.

```
http://server_name.domain_name:port/amserver/

UI/Login?goto=http://www.sun.com/homepage.html
```

`goto` 로그아웃 URL의 예는 다음과 같습니다.

```
http://server_name.domain_name:port/amserver/

UI/Logout?goto=http://www.sun.com/logout.html.
```

주 – Access Manager에서 성공적인 인증 리디렉션 URL을 찾을 때 적용하는 우선 순위가 있습니다. 이러한 리디렉션 URL 및 해당 순서는 인증 방법에 따라 다르므로 인증 유형 절에서 이 순서(및 관련 정보)를 자세히 설명합니다.

---

gotoOnFail 매개 변수

`gotoOnFail=failed_authentication_URL` 매개 변수는 인증 구성 서비스의 로그인 실패 URL에 정의된 값 대신 사용됩니다. 이 매개 변수는 사용자 인증 실패 시 지정된 URL로 연결됩니다.

예를 들어 gotoOnFail URL은 http:// *server_name.domain_name*:*port* /amserver/UI/Login?gotoOnFail=http://www.sun.com/auth_fail.html이 될 수 있습니다.

주 – Access Manager에서 실패한 인증 리디렉션 URL을 찾을 때 적용하는 우선 순위가 있습니다. 이러한 리디렉션 URL 및 해당 순서는 인증 방법에 따라 다르므로 인증 유형 절에서 이 순서(및 관련 정보)를 자세히 설명합니다.

---

realm 매개 변수

org=*realmName* 매개 변수를 사용하면 사용자가 지정된 영역에서 사용자로 인증할 수 있습니다.

주 – 아직 지정된 영역의 구성원이 아닌 사용자가 realm 매개 변수를 사용하여 인증하려고 하면 오류 메시지가 나타납니다. 그러나 다음 사항이 모두 해당되면 Directory Server에서 사용자 프로필을 동적으로 작성할 수 있습니다.

- 핵심 인증 서비스의 사용자 프로필 속성은 Dynamic 또는 Dynamic with User Alias로 설정되어야 합니다.
- 사용자는 필수 모듈에 성공적으로 인증해야 합니다.
- 사용자가 아직 Directory Server에 프로필이 없습니다.

이 매개 변수를 통해 영역 및 로켈 설정에 따라 정확한 로그인 페이지가 표시됩니다. 이 매개 변수를 설정하지 않은 경우 기본값은 최상위 영역입니다. 예를 들어, 다음은 org URL이 될 수 있습니다.

```
http://server_name.domain_name:port/amserver/UI/Login?realm=sun
```

---

org 매개 변수

org=*orgName* 매개 변수를 사용하면 사용자가 지정된 조직에서 사용자로 인증할 수 있습니다.

주 – 아직 지정된 조직의 구성원이 아닌 사용자가 `org` 매개 변수를 사용하여 인증하려고 하면 오류 메시지가 나타납니다. 그러나 다음 사항이 모두 해당되면 Directory Server에서 사용자 프로필을 동적으로 작성할 수 있습니다.

- 핵심 인증 서비스의 사용자 프로필 속성은 `Dynamic` 또는 `Dynamic with User Alias`로 설정되어야 합니다.
- 사용자는 필수 모듈에 성공적으로 인증해야 합니다.
- 사용자가 아직 Directory Server에 프로필이 없습니다.

이 매개 변수를 통해 조직 및 로켈 설정에 따라 정확한 로그인 페이지가 표시됩니다. 이 매개 변수를 설정하지 않은 경우 기본값은 최상위 조직입니다. 예를 들어, 다음은 `org` URL이 될 수 있습니다.

```
http://server_name.domain_name:port/amserver/UI/Login?org=sun
```

user 매개 변수

`user=`*userName* 매개 변수는 시용자 프로필의 사용자 인증 구성 속성에서 구성된 모듈을 기반으로 인증을 실행합니다. 예를 들어, 한 사용자의 프로필은 인증 모듈을 사용하여 인증하도록 구성하고, 다른 사용자는 LDAP 모듈을 사용하여 인증하도록 구성할 수 있습니다. 이 매개 변수를 추가하면 사용자의 조직에 구성된 방법이 아닌 사용자 자신이 구성한 인증 프로세스를 따르게 됩니다. 예를 들면 다음과 같습니다.

```
http://server_name.domain_name:port/amserver/UI/Login?user=jsmith
```

role 매개 변수

`role=`roleName 매개 변수는 지정된 역할을 위해 구성된 인증 프로세스를 사용자에게 전송합니다. 아직 지정된 역할의 구성원이 아닌 사용자가 이 매개 변수를 사용하여 인증하려고 하면 오류 메시지가 나타납니다. 예를 들면 다음과 같습니다.

```
http://server_name.domain_name:port/amserver/UI/Login?role=manager.
```

locale 매개 변수

Access Manager에는 콘솔 자체는 물론 인증 프로세스에서도 현지화된 화면(영어가 아닌 다른 언어로 번역된 화면)을 표시하는 기능이 있습니다. `locale=`*localeName* 매개 변수를 사용하면 지정된 로켈이 정의된 다른 로켈보다 우선 적용됩니다. 로그인 로켈은 다음 위치에서 순서에 따라 구성을 검색한 후 클라이언트에 표시됩니다.

1. 로그인 URL에서 locale 매개 변수의 값

   `locale=`*localeName* 매개 변수의 값은 정의된 다른 로켈보다 우선 적용됩니다.
2. 사용자 프로필에 정의된 로켈

URL 매개 변수가 없을 때는 사용자 프로필의 사용자 기본 언어 속성에 설정된 값에 따라 로켈이 표시됩니다.

3. HTTP 헤더에 정의된 로켈

   이 로켈은 웹 브라우저에서 설정합니다.

4. 핵심 인증 서비스에 정의된 로켈

   이 로켈은 핵심 인증 모듈의 기본 인증 로켈 속성의 값입니다.

5. 플랫폼 서비스에 정의된 로켈

   이 로켈은 플랫폼 서비스에서 플랫폼 로켈 속성의 값입니다.

운영 체제 로켈

여기서 파생된 로켈은 사용자의 세션 토큰에 저장되며 Access Manager에서는 현지화된 인증 모듈을 로드할 때만 이를 사용합니다. 인증이 성공하면 사용자 프로필의 사용자 기본 언어 속성에 정의된 로켈이 사용됩니다. 아무 것도 설정되어 있지 않을 때는 인증에 사용된 로켈이 적용됩니다. 예를 들면 다음과 같습니다.

```
http://server_name.domain_name:port/amserver/UI/Login?locale=ja.
```

주 – Access Manager에서 화면 텍스트와 오류 메시지 현지화 방법에 대한 내용을 참조할 수 있습니다.

---

module 매개 변수

`module=`*moduleName* 매개 변수를 사용하면 지정된 인증 모듈을 통해 인증할 수 있습니다. 모든 인증 모듈은 먼저 사용자가 속한 영역에서 등록되고 핵심 인증 모듈에서 해당 영역의 인증 모듈 중 하나로 선택되어야 지정될 수 있습니다. 예를 들면 다음과 같습니다.

```
http://server_name.domain_name:port/amserver/UI/Login?module=Unix.
```

주 – URL 매개 변수에서 사용되는 인증 모듈 이름은 대소문자를 구분합니다.

---

service 매개 변수

`service=`*serviceName* 매개 변수를 사용하면 사용자는 서비스의 구성된 인증 스키마를 통해 인증할 수 있습니다. 인증 구성 서비스를 사용하여 서비스마다 인증 스키마를 달리 구성할 수 있습니다. 예를 들어, 영역의 직원 디렉토리 응용 프로그램은 LDAP 인증 모듈만 필요한 반면 온라인 급여 응용 프로그램은 보다 안전한 인증서 인증 모듈을 사용하여 인증해야 합니다. 이러한 서비스마다 인증 스키마를 구성하고 이름을 지정할 수 있습니다. 예를 들면 다음과 같습니다.

```
http://server_name.domain_name:port/amserver/UI/Login?service=sv1.
```

주 – 인증 구성 서비스는 서비스 기반의 인증을 위한 스키마 정의에 사용됩니다.

arg 매개 변수

`arg=`*newsession* 매개 변수는 사용자의 현재 세션을 종료하고 새 세션을 시작하는 데 사용됩니다. 인증 서비스는 사용자의 기존 세션 토큰을 제거하고 요청 시마다 새 로그인을 수행합니다. 이 옵션은 일반적으로 익명 인증 모듈에서 사용됩니다. 사용자는 먼저 익명 세션으로 인증한 다음 등록이나 로그인 링크를 누릅니다. 예를 들면 다음과 같습니다.

`http://`*server_name.domain_name*`:port/amserver/UI/Login?arg=newsession.`

authlevel 매개 변수

`authlevel=`*value* 매개 변수는 인증 수준이 인증 서비스에게 지정된 인증 수준 값보다 크거나 같은 모듈을 호출하도록 명령합니다. 각 인증 모듈은 고정된 정수 인증 수준으로 정의됩니다. 예를 들면 다음과 같습니다.

`http://server_name.domain_name:port/amserver/UI/Login?authlevel=1.`

주 – 인증 수준은 각 모듈의 특정 프로필에 설정됩니다.

domain 매개 변수

이 매개 변수를 사용하면 지정된 도메인으로 식별된 영역에 로그인할 수 있습니다. 지정된 도메인은 영역 프로필의 도메인 이름 속성에 정의된 값과 일치해야 합니다. 예를 들면 다음과 같습니다.

`http://`*server_name.domain_name*`:port/amserver/UI/Login?domain=sun.com.`

주 – 아직 지정된 도메인/영역의 구성원이 아닌 사용자가 `org` 매개 변수를 사용하여 인증하려고 하면 오류 메시지가 나타납니다. 그러나 다음 사항이 모두 해당되면 Directory Server에서 사용자 프로필을 동적으로 작성할 수 있습니다.

- 핵심 인증 서비스의 사용자 프로필 속성은 `Dynamic` 또는 `Dynamic With User Alias` 로 설정되어야 합니다.
- 사용자는 필수 모듈에 성공적으로 인증해야 합니다.
- 사용자가 아직 Directory Server에 프로필이 없습니다.

iPSPCookie 매개 변수

iPSPCookie=yes 매개 변수를 사용하면 영구 쿠키를 사용하여 로그인할 수 있습니다. 영구 쿠키는 브라우저 창을 닫은 후에도 계속 존재하는 쿠키를 말합니다. 이 매개 변수를 사용하기 위해서는 사용자가 로그인한 조직의 영구 쿠키가 핵심 인증 모듈에서 활성화되어 있어야 합니다. 사용자가 인증하고 브라우저를 닫은 후에는 다시 인증할 필요 없이 새 브라우저 세션으로 로그인할 수 있고 콘솔로 직접 이동합니다. 이러한 작업은 핵심 서비스에 지정된 영구 쿠키 최대 시간의 값이 경과할 때까지 가능합니다. 예를 들면 다음과 같습니다.

```
http://server_name.domain_name:port/amserver/UI/Login?org=example&iPSPCookie=yes
```

IDTokenN 매개 변수

이 매개 변수 옵션을 사용하면 URL 또는 HTML 형식으로 인증 자격 증명을 통과할 수 있습니다. IDTokenN=*value* 매개 변수를 사용하는 경우 인증 서비스 사용자 인터페이스에 액세스하지 않고도 인증할 수 있습니다. 이러한 프로세스를 *0* 페이지 로그인이라고 합니다. 0페이지 로그인은 하나의 로그인 페이지를 사용하는 인증 모듈에서만 작동합니다. IDToken0, IDToken1, ..., IDTokenN 값은 인증 모듈의 로그인 페이지에 있는 필드에 매핑됩니다. 예를 들어, LDAP 인증 모듈은 userID 정보에 IDToken1을 사용하고 비밀번호 정보에 IDToken2를 사용할 수 있습니다. 이 경우 LDAP 모듈 IDTokenN URL은 다음과 같습니다.

```
http://server_name.domain_name:port/amserver/UI/

Login?module=LDAP&IDToken1=userID&IDToken2=password
```

(LDAP가 기본 인증 모듈인 경우 module=LDAP를 생략할 수 있습니다.)

익명 인증의 경우 로그인 URL 매개 변수는 다음과 같습니다.

```
http://server_name.domain_name:port/amserver/UI/Login?module=Anonymous&IDToken1=anonymousUserID.
```

주 – 이전 릴리스의 토큰 이름인 Login.Token0, Login.Token1, ..., Login.TokenN은 아직 지원되지만 향후 릴리스에서는 사용할 수 없게 됩니다. 새로 제공되는 IDTokenN 매개 변수를 사용하는 것이 좋습니다.

계정 잠금

인증 서비스는 사용자 인증이 *n*회 실패하면 사용자 인증을 잠그는 기능을 제공합니다. 이 기능은 기본적으로 꺼져 있지만 Access Manager 콘솔을 사용하여 활성화할 수 있습니다.

주 – 잘못된 비밀번호 예외가 발생하는 모듈만 계정 잠금 기능을 사용할 수 있습니다.

핵심 인증 서비스에는 다음을 포함하여 이 기능을 활성화/사용자 정의하는 속성이 들어 있습니다.

- 로그인 실패 잠금 모드. 계정 잠금을 활성화합니다.
- 로그인 실패 잠금 수 사용자가 잠기기 전에 인증을 시도할 수 있는 횟수를 정의합니다. 이 값은 사용자 아이디에 대해서만 적용됩니다. 동일한 사용자 아이디가 지정된 횟수만큼 실패하면 그 사용자 아이디는 잠겨집니다.
- 로그인 실패 잠금 간격 사용자 잠금이 적용되기 전 얼마 동안 로그인 실패 잠금 수의 값이 완료되어야 하는지 분 단위로 정의합니다.
- 잠금 알림을 보낼 전자 메일 주소 사용자 잠금 알림을 보낼 전자 메일 주소를 지정합니다.
- **N**회 실패 후 사용자에게 경고. 몇 차례 인증이 실패하면 경고 메시지가 사용자에게 표시되는지 지정합니다. 관리자는 사용자에게 잠금이 임박했음을 경고한 이후의 추가 로그인 시도를 설정할 수 있습니다.
- 로그인 실패 잠금 기간. 잠금 후 얼마나 대기한 후 다시 인증을 시도할 수 있는지 분 단위로 정의합니다.
- 잠금 속성 이름. 물리적 잠금에 대해 사용자 프로필 중 어떤 LDAP 속성이 `inactive`로 설정될 것인지 정의합니다.
- 잠금 속성 값. 잠금 속성 이름에 지정된 LDAP 속성 중 어떤 속성이`inactive` 또는 `active`로 설정될 것인지 정의합니다.

계정 잠금이 발생하면 관리자에게 전자 메일 알림이 전송됩니다. (계정 잠금 활동도 기록).

주 – Microsoft® Windows 2000 운영 체제에서의 이 기능 사용에 대한 자세한 내용은 부록 A, “AMConfig.properties File”에서 “Simple Mail Transfer Protocol(SMTP)”을 참조하십시오.

Access Manager에서는 다음 절에서 정의하는물리적 잠금과 메모리 잠금의 두 가지 계정 잠금 유형을 지원합니다.

물리적 잠금

이는 Access Manager에 대한 기본 잠금 동작입니다. 사용자 프로필의 LDAP 속성 상태를 inactive로 변경하면 이 잠금이 초기화됩니다. `Lockout Attribute Name`은 잠금 목적에 따라 사용되는 LDAP 속성을 정의합니다.

주 – 별칭 사용자는 LDAP 프로필에서 사용자 별칭 목록 속성(`iplanet-am-user-alias-list` in `amUser.xml`)을 구성하는 방법으로 기존의 LDAP 사용자 프로필에 매핑된 사용자입니다. 별칭 사용자는 핵심 인증 서비스의 별칭 검색 속성 이름 필드에 `iplanet-am-user-alias-list`를 추가함으로써 검증할 수 있습니다. 즉 별칭 사용자가 잠긴 경우 해당 사용자가 별칭 처리된 실제 LDAP 프로필도 잠기게 됩니다. 이는 LDAP 및 구성원이 아닌 인증 모듈을 사용하는 물리적 잠금에만 적용됩니다.

메모리 잠금

메모리 잠금은 `Login Failure Lockout Duration` 속성을 0보다 큰 값으로 변경하는 방법으로 사용할 수 있습니다. 그러면 사용자 계정은 지정된 분 수 동안 메모리에서 잠깁니다. 시간이 모두 경과한 후에는 계정의 잠금이 해제됩니다. 메모리 잠금 기능을 사용할 때는 몇 가지 사항에 특별히 주의해야 합니다.

- Access Manager가 다시 시작하는 경우에는 메모리에서 잠긴 모든 계정이 잠금 해제됩니다.
- 사용자 계정이 메모리에서 잠겨있고 관리자가 계정 잠금 체계를 물리적 잠금으로 변경한 경우(잠금 기간을 다시 0으로 설정) 사용자 계정이 메모리에서 잠금 해제되고 잠금 수가 재설정됩니다.
- 메모리 잠금 후 LDAP 및 구성원을 제외한 인증 모듈을 사용할 때 사용자가 정확한 비밀번호로 로그인을 시도할 경우 사용자가 활성 상태가 아닙니다. 오류 대신이 조직에 사용자의 프로필이 없습니다. 오류가반환됩니다.

주 – 사용자 프로필에 실패 URL 속성이 설정된 경우 잠금 경고 메시지나 계정이 잠겨 있음을 나타내는 메시지가 표시되지 않고 정의된 URL로 사용자가 리디렉션됩니다.

인증 서비스 페일오버

인증 서비스 페일오버는 하드웨어나 소프트웨어 문제 때문에 주 서버에 장애가 발생하거나 서버가 일시적으로 다운될 경우 자동으로 인증 요청을 보조 서버로 리디렉션합니다.

인증 서비스를 사용할 수 있는 Access Manager 인스턴스에서 인증 컨텍스트가 먼저 생성되어야 합니다. 이 Access Manager 인스턴스를 사용할 수 없는 경우 인증 페일오버를 통해 다른 Access Manager 인스턴스에서 인증 컨텍스트를 생성할 수 있습니다. 인증 컨텍스트는 다음 순서로 서버 가용성을 확인합니다.

1. 인증 서비스 URL이 AuthContext API로 전달됩니다. 예를 들면 다음과 같습니다.

```
AuthContext(orgName, url)
```

이 API가 사용될 경우 URL에 의해 참조되는 서버만 사용합니다. 해당 서버에서 인증 서비스를 사용할 수 있는 경우라도 페일오버는 이루어지지 않습니다.

2. 인증 컨텍스트는 AMConfig.properties 파일의 com.iplanet.am.server* 속성에 정의된 서버를 검사합니다.
3. 단계 2가 실패할 경우 인증 컨텍스트는 이름 지정 서비스를 사용할 수 있는 서버에서 플랫폼 목록을 조회합니다. 이 플랫폼 목록은 하나의 Directory Server 인스턴스를 공유하는 다수의 Access Manager 인스턴스(일반적으로 페일오버 목적)가 설치될 때 자동으로 작성됩니다.

   예를 들어, 플랫폼 목록에 Server1, Server2 및 Server3을 위한 URL이 포함되면 인증 컨텍스트는 그 중 하나에서 인증이 성공할 때까지 Server1, Server2, Server3을 차례로 순환합니다.

   플랫폼 목록은 이름 지정 서비스의 가용성에 따라 다르므로 항상 동일한 서버에서 얻어질 수 있는 것은 아닙니다. 또한 이름 지정 서비스 페일오버가 먼저 일어날 수도 있습니다. AMConfing.properties의 com.iplanet.am.naming.url property에 다수의 이름 지정 서비스 URL이 지정됩니다. 사용할 수 있는 첫 번째 이름 지정 서비스 URL은 인증 페일오버가 이루어지는 서버 목록이 포함된 서버를 식별하는 데 사용됩니다.

정규화된 도메인 이름(FQDN) 매핑

정규화된 도메인 이름(FQDN) 매핑을 사용하면 사용자가 잘못된 URL을 입력하더라도(예: 보호된 자원에 액세스할 때 부분 호스트 이름이나 IP 주소 지정) 인증 서비스에서 수정할 수 있습니다. FQDN 매핑은 AMConfig.properties 파일의 com.sun.identity.server.fqdnMap 속성을 수정하여 활성화합니다. 이 등록 정보를 지정하는 형식은 다음과 같습니다.

com.sun.identity.server.fqdnMap[*invalid-name*]=*valid-name*

invalid-name 값은 사용자가 잘못 입력한 FQDN 호스트 이름이 되고 *valid-name*은 필터에서 사용자를 리디렉션할 실제 호스트 이름이 됩니다. 명시된 요구 사항의 범위 내에서 매핑 수를 지정할 수 있습니다(코드 예 1-1에서 설명). 이 등록 정보를 설정하지 않으면 사용자는 AMConfig.properties 파일에서도 확인 가능한 com.iplanet.am.server.host= *server_name* 등록 정보에 구성된 기본 서버 이름으로 보내집니다.

예 7–1 AMConfig.properties의 FQDN 매핑 속성

```
com.sun.identity.server.fqdnMap[isserver]=isserver.mydomain.com

com.sun.identity.server.fqdnMap[isserver.mydomain]=isserver.mydomain.com

com.sun.identity.server.fqdnMap[

        IP address]=isserver.mydomain.com
```

예 7–1 AMConfig.properties의 FQDN 매핑 속성 *(계속)*

FQDN 매핑의 용도

이 등록 정보는 서버에 호스트된 응용 프로그램이 둘 이상의 호스트 이름으로 액세스 가능할 경우 둘 이상의 호스트 이름에 대해 하나의 매핑을 작성하는 데 사용할 수 있습니다. 또한 Access Manager에서 특정 URL에 대해 수정 조치를 취하지 않게 할 때에도 사용할 수 있습니다. 예를 들어, IP 주소를 사용하여 응용 프로그램에 액세스하는 사용자에게 리디렉션이 필요하지 않다면 이 기능은 다음과 같이 매핑 항목을 지정하여 구현할 수 있습니다.

`com.sun.identity.server.fqdnMap[`*IP address* `]=`*IP address.*

주 – 매핑이 둘 이상 정의되어 있을 때는 잘못된 FQDN 이름으로 값이 겹치지 않아야 합니다. 응용 프로그램 액세스가 불가능해질 수도 있습니다.

영구 쿠키

영구 쿠키는 웹 브라우저를 닫은 후에도 계속 존재하는 쿠키로서 사용자가 이 영구 쿠키를 사용하면 다시 인증할 필요 없이 새 브라우저 세션으로 로그인할 수 있습니다. 이 쿠키의 이름은 AMConfig.properties의 com.iplanet.am.pcookie.name 등록 정보에서 정의되며 그 기본값은 DProPCookie입니다. 쿠키 값은 3DES 암호화된 문자열로서 사용자 DN, 영역 이름, 인증 모듈 이름, 최대 세션 시간, 유휴 시간 및 캐시 시간으로 구성됩니다.

▼ 영구 쿠키를 사용하려면

1 **핵심 인증 모듈에서 Persistent Cookie Mode를 켭니다.**

2 **핵심 인증 모듈에서 Persistent Cookie Maximum Time 속성에 대한 시간 값을 구성합니다.**

3 **값이 yes인 iPSPCookie 매개 변수를 사용자 인터페이스 로그인 URL에 추가합니다.**

사용자가 이 URL을 사용하여 인증하면 브라우저를 닫아도 다시 인증할 필요 없이 새 브라우저 창을 열 수 있고 콘솔로 리디렉션하게 됩니다. 영구 쿠키는 단계 2에서 정의한 시간이 경과할 때까지 계속 적용됩니다.

영구 쿠키 모드는 다음 인증 SPI 방법을 사용하여 켤 수 있습니다.

AMLoginModule.setPersistentCookieOn().

레거시 모드에서 다중 LDAP 인증 모듈 구성

페일오버의 한 형식으로 또는 Access Manager 콘솔에 값 필드가 하나만 제공되는 경우 하나의 속성에 여러 값을 구성하기 위해 관리자는 하나의 영역에 여러 LDAP 인증 모듈 구성을 정의할 수 있습니다. 이러한 추가 구성은 콘솔에 표시되지 않더라도 사용자의 인증 요청에 대한 초기 검색이 없는 경우에 기본 구성과 함께 사용됩니다. 예를 들어, 한 영역에서 두 가지 서로 다른 도메인에 인증용 LDAP 서버를 통한 검색을 정의하거나 한 도메인에 사용자 이름 지정 속성을 여러 개 구성할 수도 있습니다. 후자는 콘솔에 텍스트 필드를 하나만 갖는 경우이며, 기본 검색 기준을 사용하여 사용자를 찾지 못하면 LDAP 모듈에서 2차 범위를 사용하여 검색하게 됩니다. 다음은 추가 LDAP 구성을 구성하는 단계입니다.

▼ 추가 LDAP 구성을 추가하려면

1 2차(또는 3차) LDAP 인증 구성에 필요한 새 값과 전체 속성 세트를 포함하여 XML 파일을 작성합니다.

etc/opt/SUNWam/config/xml에 있는 amAuthLDAP.xml을 확인하면서 사용 가능한 속성을 참조할 수 있습니다. 그러나 이 단계에서 만든 XML 파일은 amAuthLDAP.xml과 달리 amadmin.dtd 구조를 기반으로 합니다. 이 파일에 대해 속성을 하나 또는 전부 정의할 수 있습니다. 코드 예 1-2는 LDAP 인증 구성에 사용할 수 있는 모든 속성 값이 포함된 하위 구성 파일의 예입니다.

```
<?xml version="1.0" encoding="ISO-8859-1"?>

<!--

  Copyright (c) 2002 Sun Microsystems, Inc. All rights reserved.

  Use is subject to license terms.

-->

<!DOCTYPE Requests

    PUBLIC "-//iPlanet//Sun ONE Access Manager 6.0 Admin CLI DTD//EN"

    "jar://com/iplanet/am/admin/cli/amAdmin.dtd"

>

<!--
```

```
  Before adding subConfiguration load the schema with
GlobalConfiguration defined and replace corresponding
 serviceName and subConfigID in this sample file OR load
 serviceConfigurationRequests.xml before loading this sample
-->
<Requests>
<realmRequests DN="dc=iplanet,dc=com">
    <AddSubConfiguration subConfigName = "ssc"
        subConfigId = "serverconfig"
        priority = "0" serviceName="iPlanetAMAuthLDAPService">


              <AttributeValuePair>
            <Attribute name="iplanet-am-auth-ldap-server"/>
            <Value>vbrao.red.iplanet.com:389</Value>
        </AttributeValuePair>
        <AttributeValuePair>
            <Attribute name="iplanet-am-auth-ldap-base-dn"/>
            <Value>dc=iplanet,dc=com</Value>
        </AttributeValuePair>
        <AttributeValuePair>
            <Attribute name="planet-am-auth-ldap-bind-dn"/>
            <Value>cn=amldapuser,ou=DSAME Users,dc=iplanet,dc=com</Value>
        </AttributeValuePair>
        <AttributeValuePair>
```

```
        <Attribute name="iplanet-am-auth-ldap-bind-passwd"/>
        <Value>
              plain text password</Value>
    </AttributeValuePair>
    <AttributeValuePair>
        <Attribute name="iplanet-am-auth-ldap-user-naming-attribute"/>
        <Value>uid</Value>
    </AttributeValuePair>
    <AttributeValuePair>
        <Attribute name="iplanet-am-auth-ldap-user-search-attributes"/>
        <Value>uid</Value>
    </AttributeValuePair>
    <AttributeValuePair>
        <Attribute name="iplanet-am-auth-ldap-search-scope"/>
        <Value>SUBTREE</Value>
    </AttributeValuePair>
    <AttributeValuePair>
        <Attribute name="iplanet-am-auth-ldap-ssl-enabled"/>
        <Value>false</Value>
    </AttributeValuePair>
    <AttributeValuePair>
        <Attribute name="iplanet-am-auth-ldap-return-user-dn"/>
        <Value>true</Value>
```

```
        </AttributeValuePair>
        <AttributeValuePair>
            <Attribute name="iplanet-am-auth-ldap-auth-level"/>
            <Value>0</Value>
        </AttributeValuePair>
        <AttributeValuePair>
            <Attribute name="iplanet-am-auth-ldap-server-check"/>
            <Value>15</Value>
        </AttributeValuePair>

    </AddSubConfiguration>

</realmRequests>
</Requests>
```

2 단계 1에서 작성한 XML 파일에서 iplanet-am-auth-ldap-bind-passwd의 값으로서 일반 텍스트 비밀번호를 복사합니다.

이 속성 값은 코드 예에 굵은 글씨로 표시되어 있습니다.

3 amadmin 명령줄 도구를 사용하여 XML 파일을 로드합니다.

```
./amadmin -u amadmin -w administrator_password -v -t name_of_XML_file.
```

이 2차 LDAP 구성은 콘솔에서 보거나 수정할 수 없습니다.

정보 – 다중 LDAP 구성에 사용할 수 있는 예제가 있습니다. `/AccessManager-base /SUNWam/samples/admin/cli/bulk-ops/`에서 `serviceAddMultipleLDAPConfigurationRequests .xml` 명령줄 템플리트를 참조하십시오. `/AccesManager-base /SUNWam/samples/admin/cli/`의 `Readme.html`에서 지침을 참조할 수 있습니다.

세션 업그레이드

인증 서비스를 사용하면 한 영역에서 동일한 사용자가 수행한 2차 인증 성공을 기반으로 유효한 세션 토큰을 업그레이드할 수 있습니다. 유효한 세션 토큰을 가진 사용자가 현재 영역에서 보호한 자원에 인증을 시도하고 이 2차 인증 요청이 성공하면 해당 세션은 새 인증을 기반으로 한 새 등록 정보로 업데이트됩니다. 인증에 실패한 경우 사용자의 현재 세션이 업그레이드되지 않고 반환됩니다. 유효한 세션을 가진 사용자가 다른 영역에서 보호한 자원에 인증을 시도하는 경우 새 영역에 인증할 것인지 묻는 메시지를 받게 됩니다. 이때 사용자는 현재 세션을 유지하거나 새 영역에 인증을 시도할 수도 있습니다. 인증이 성공하면 이전 세션이 삭제되고 새 세션이 작성됩니다.

세션 업그레이드 중 로그인 페이지가 시간 초과되면 원래의 성공 URL로 리디렉션됩니다. 시간 초과 값은 다음에 따라 결정됩니다.

- 각 모듈에 설정한 페이지 시간 초과 값(기본값: 1분)
- `AMConfig.properties`의 `com.iplanet.am.invalidMaxSessionTime` 등록 정보(기본값: 10분)
- `iplanet-am-max-session-time`(기본값: 120분)

`com.iplanet.am.invalidMaxSessionTimeout` 값 및 `iplanet-am-max-session-time` 값은 페이지 시간 초과 값보다 커야 합니다. 그렇지 않으면 세션 업그레이드 중 유효한 세션 정보가 손실되고 이전의 성공 URL에 대한 리디렉션이 실패하게 됩니다.

플러그 인 인터페이스 검증

관리자는 영역에 적합한 사용자 이름 또는 비밀번호 검증 논리를 작성하고 이를 인증 서비스에 플러그 인할 수 있습니다. (이 기능은 LDAP 및 구성원 인증 모듈에서만 지원됩니다.)사용자를 인증하거나 비밀번호를 변경하기 전에 Access Manager에서는 이 플러그 인을 호출합니다. 검증이 성공하면 인증이 계속되지만, 실패하면 인증 실패 페이지가 나타납니다. 이 플러그 인은 서비스 관리 SDK의 일부인 `com.iplanet.am.sdk.AMUserPasswordValidation` 클래스를 확장합니다. 이 SDK에 대한 내용은 Access Manager Javadocs의 `com.iplanet.am.sdk` 패키지를 참조하십시오.

▼ 검증 플러그 인을 작성 및 구성하려면

1. **새 플러그 인 클래스는** `com.iplanet.am.sdk.` `AMUserPasswordValidation` **클래스를 확장하고** `validateUserID()` **및** `validatePassword()` **메소드를 구현합니다.** `AMException`**은 검증이 실패할 때 나타납니다.**
2. **플러그 인 클래스를 컴파일하고 원하는 위치에** `.class` **파일을 놓습니다. 런타임 동안 Access Manager에서 액세스할 수 있도록 클래스 경로를 업데이트합니다.**
3. **Access Manager 콘솔에 최상위 관리자로 로그인합니다. 서비스 관리 탭을 누르고 관리 서비스에 대한 속성을 확인하십시오.** `UserID & Password Validation Plugin Class` **필드에 플러그 인 클래스의 이름(패키지 이름 포함)을 입력합니다.**
4. **로그아웃했다가 다시 로그인합니다.**

JAAS 공유 상태

JAAS 공유 상태는 인증 모듈들이 사용자 아이디와 비밀번호를 공유하게 합니다. 다음 인증 모듈에 옵션이 정의되어 있습니다.

- 영역(또는 조직)
- 사용자
- 서비스
- 역할

실패할 때 모듈에는 필수 자격 증명에 대한 메시지가 나타납니다. 인증이 실패하고 나면 모듈의 실행이 중지되거나 로그아웃 공유 상태가 지워집니다.

JAAS 공유 상태 활성화

JAAS 공유 상태를 구성하려면 다음을 수행합니다.

- `iplanet-am-auth-shared-state-enabled` 옵션을 사용합니다.
- 공유 상태 옵션은 다음의 경우에 사용됩니다.`iplanet-am-auth-shared-state-enabled=true`
- 이 옵션의 기본값은 true입니다.
- 이 변수는 인증 체이닝 구성의 옵션 열에서 지정됩니다.

실패하면 인증 모듈에는 필수 자격 증명 프롬프트가 JAAS 사양에 제시된 `tryFirstPass` 옵션 동작에 따라 나타납니다.

JAAS 공유 상태 저장소 옵션

JAAS 공유 상태 저장소 옵션을 구성하려면 다음을 수행합니다.

- `iplanet-amauth-store-shared-state-enabled` 옵션을 사용합니다.
- 저장소 공유 상태 옵션은 다음과 같은 경우에 사용됩니다.`iplanet-am-auth-store-shared-state-enabled=true`
- 이 옵션의 기본값은 false입니다.
- 이 변수는 인증 체이닝 구성의 옵션 열에서 지정됩니다.

완결, 중단 또는 로그아웃한 후에는 공유 상태가 지워집니다.

◆ ◆ ◆ 8 장

8 정책 관리

이 장에서는 Sun Javaa™ System Access Manager의 정책 관리 기능에 대해 설명합니다. Access Manager의 정책 관리 기능을 사용하면 최상위 수준 관리자 또는 최상위 수준 정책 관리자가 모든 영역에서 사용할 수 있는 특정 서비스의 정책을 보고, 만들고, 삭제하고, 수정할 수 있습니다. 또한 영역이나 하위 영역 관리자 또는 정책 관리자가 영역 수준에서 정책을 보고, 만들고, 삭제하고, 수정할 수 있는 방법을 제공합니다.

이 장은 다음 내용으로 구성되어 있습니다.

개요

정책은 조직의 보호 대상 자원에 대한 액세스 권한을 지정하는 규칙을 정의합니다. 보호하고 관리하고 모니터링해야 하는 자원, 응용 프로그램 및 서비스가 있습니다. 정책은 주어진 자원에 대한 작업을 사용자가 언제, 어떤 방법으로 수행할 수 있는지 정의하여 이러한 자원에 대한 액세스 권한과 용도를 제어합니다. 정책은 특정 기본에 대해 자원을 정의합니다.

주 – 기본은 아이디를 가질 수 있는 개인, 회사, 역할 또는 그룹이 될 수 있습니다. 자세한 내용은 Java™ 2 Platform Standard Edition Javadoc (`http://java.sun.com/j2se/1.4.2/docs/api/java/security/Principal.html`)을 참조하십시오.

단일 정책은 이진 또는 비이진 결정 중 하나를 정의할 수 있습니다. 이진 결정은 *yes*/*no*, *true*/*false* 또는 *allow*/*deny*입니다. 비이진 결정은 속성의 값을 나타냅니다. 예를 들어, 메일

서비스에는 각 사용자에 대한 최대 저장 값이 설정된 `mailboxQuota` 속성이 포함될 수 있습니다. 일반적으로 정책은 한 기본이 어떤 자원에 대해 어떤 조건 하에서 어떤 작업을 수행할 수 있는지 정의하도록 구성됩니다.

정책 관리 기능

정책 관리 기능은 정책을 만들고 관리하기 위한 정책 서비스를 제공합니다. 정책 서비스는 관리자가 Access Manager 배포 내에서 자원을 보호하기 위해 권한을 정의, 수정, 부여, 철회 및 삭제할 수 있도록 합니다. 일반적으로 정책 서비스에는 데이터 저장소, 생성을 허용하는 인터페이스 라이브러리, 정책 관리 및 평가, 정책 집행자 또는 정책 에이전트가 포함됩니다. 기본적으로 Access Manager는 데이터 저장용으로 Sun Java Enterprise System Directory Server를 사용하며 정책 평가 및 정책 서비스 사용자 정의를 위해 Java 및 C API를 제공합니다(자세한 내용은 **Sun Java System Access Manager 7 2005Q4 Developer's Guide**를 참조하십시오). 또한 관리자가 Access Manager 콘솔을 사용하여 정책을 관리할 수 있게 해줍니다. Access Manager는 다운로드할 수 있는 정책 에이전트를 사용하여 정책을 집행하는 정책 가능 서비스인 URL 정책 에이전트 서비스를 제공합니다.

URL 정책 에이전트 서비스

Access Manager를 설치하면 HTTP URL 보호를 위한 정책을 정의하는 URL 정책 에이전트 서비스가 제공됩니다. 이 서비스를 사용하여 관리자는 정책 집행자 또는 정책 에이전트를 통해 정책을 만들고 관리할 수 있습니다.

정책 에이전트

정책 에이전트는 회사의 자원이 저장된 서버에 대한 정책 적용 지점(PEP)입니다. 정책 에이전트는 웹 서버에 Access Manager와 별도로 설치되며 사용자가 보호를 받는 웹 서버에 있는 웹 자원에 대한 요청을 보낼 때 추가 인증 단계 역할을 합니다. 이 인증 단계는 자원에서 수행하는 사용자 인증 요청에 추가로 이루어집니다. 에이전트는 웹 서버를 보호하고 자원은 인증 플러그 인에 의해 보호됩니다.

예를 들어, 원격 설치된 Access Manager에 의해 보호되는 인적 자원 웹 서버에는 에이전트가 설치되어 있을 수 있습니다. 이 에이전트는 제대로된 정책 없이 기밀 정보인 급여 정보나 기타 민감한 데이터를 보지 못하도록 방지합니다. 정책은 Access Manager 관리자가 정의하여 Access Manager 배포 내에 저장하며 정책 에이전트가 원격 웹 서버의 내용에 대한 사용자 액세스를 허용 또는 거부하는 데 사용됩니다.

최신 Access Manager 정책 에이전트는 Sun Microsystems 다운로드 센터에서 다운로드할 수 있습니다.

정책 에이전트 설치 및 관리에 대한 자세한 내용은 **Sun Java System Access Manager Policy Agent 2.2 User's Guide**를 참조하십시오.

주 – 정책은 특별한 순서로 평가되지 않습니다. 그러나 정책을 평가할 때 한 가지 작업 값이 거부로 평가되는 경우 정책 구성 서비스에서 거부 결정에 대한 평가 계속 속성이 활성화되지 않으면 후속 정책은 평가되지 않습니다.

Access Manager 정책 에이전트는 웹 URL(`http://...` 또는 `https//...`)에서만 결정을 실행합니다. 그러나 Java 및 C 정책 평가 API를 사용하여 다른 자원에서 정책을 실행하는 에이전트를 작성할 수 있습니다.

또한 정책 구성 서비스의 자원 비교기 속성도 기본 구성에서 다음과 같은 구성으로 변경해야 합니다.

```
serviceType=Name_of_LDAPService
|class=com.sun.identity.policy.plugins.SuffixResourceName|wildcard=*

|delimiter=,|caseSensitive=false
```

또는 `LDAPResourceName`과 같은 구현을 제공하여 `com.sun.identity.policy.interfaces.ResourceName`을 구현하고 자원 비교기를 구성하는 방법도 사용할 수 있습니다.

정책 에이전트 프로세스

보호 대상 웹 자원을 위한 프로세스는 정책 에이전트에 의해 보호를 받는 서버에 상주하는 URL을 웹 브라우저에서 요청할 때 시작됩니다. 서버의 설치된 정책 에이전트는 요청을 인터셉트하여 기존 인증 자격 증명(세션 토큰)을 확인합니다.

에이전트가 요청을 인터셉트하고 기존 세션 토큰을 확인하면 다음 프로세스가 이어집니다.

1. 세션 토큰이 유효하면 사용자에게 권한이 부여 또는 거부됩니다. 유효한 토큰이 아닐 경우 사용자는 다음과 같은 단계를 거쳐 인증 서비스로 리디렉션됩니다.

   에이전트가 기존 세션 토큰이 없는 요청을 인터셉트했다면 다른 인증 방법을 사용하여 자원을 보호하더라도 사용자를 로그인 페이지로 리디렉션합니다.
2. 사용자의 자격 증명이 인증되면 에이전트가 Access Manager의 내부 서비스 연결에 사용되는 URL을 정의하는 이름 지정 서비스에 요청을 발행합니다.
3. 자원이 에이전트에서 구성된 비강제 목록과 일치하면 액세스가 허용됩니다.
4. 이름 지정 서비스는 정책 서비스에 대한 로케이터, 세션 서비스 및 로깅 서비스를 반환합니다.
5. 에이전트는 사용자에게 적용할 수 있는 정책 결정을 얻기 위해 정책 서비스에 요청을 보냅니다.
6. 액세스 대상 자원에 대한 정책 결정에 따라 사용자는 액세스 권한이 부여되거나 거부됩니다. 정책 결정에 대한 조언에 다른 인증 수준 또는 방법이 제시되면 에이전트는 모든 검색 조건이 확인될 때까지 요청을 인증 서비스로 다시 보냅니다.

정책 유형

Access Manager를 사용하여 다음 두 가지 유형의 정책을 구성할 수 있습니다.

- 130 페이지 "일반 정책"
- 134 페이지 "참조 정책"

일반 정책

Access Manager에서 액세스 권한을 정의하는 정책을 일반 정책이라고 합니다. 일반 정책은 규칙, 주제, 조건 및 응답 공급자로 구성됩니다.

규칙

하나의 규칙에는 하나의 자원, 하나 이상의 작업 및 하나의 값이 포함됩니다. 각 작업에는 하나 이상의 값이 있을 수 있습니다.

- 자원은 인적 자원 서비스를 사용하여 액세스되는 HTML 페이지 또는 사용자의 급여 정보 등 보호 대상인 특정 객체를 정의합니다.
- 작업은 자원에 대해 수행될 수 있는 작업의 이름입니다. 예를 들어, 웹 서버 작업으로는 POST 또는 GET 등이 있습니다. 인적 자원 서비스에는 예를 들어 집 전화 번호 변경 작업 등이 허용될 수 있습니다.
- 값은 작업에 대한 권한(예: 허용 또는 거부)을 정의합니다.

주 – 일부 서비스에 대해 자원 없이 작업을 정의할 수 있습니다.

주제

주제는 정책이 영향을 주는 사용자 또는 사용자 집합(예: 그룹 또는 특정 역할 소유자들)을 정의합니다. 주제는 정책에 지정됩니다. 사용자가 적어도 정책의 한 주제의 구성원일 경우에만 정책이 적용되는 것이 일반적인 규칙입니다. 기본 주제는 다음과 같습니다.

AM Identity 주제	사용자가 영역 주제 탭에서 만들고 관리하는 Identity를 해당 주제의 값으로 추가할 수 있습니다.
Access Manager 역할	LDAP 역할을 이 주제의 값으로 추가할 수 있습니다. LDAP 역할은 Directory Server 역할 기능을 사용하는 임의의 역할 정의입니다. 이러한 역할은 Directory Server 역할 정의에 의해 위임되는 객체 클래스를 가집니다. 정책 구성 서비스에서 LDAP 역할 검색 필터를 수정하여 범위를 좁히고 성능을 향상시킬 수 있습니다.
인증된 사용자	유효한 SSO 토큰을 가진 사용자가 이 주제의 구성원입니다. 인증된 사용자는 정책이 정의된 조직과 다른 조직에 인증한 경우에도 모두 이 주제의 구성원이 됩니다. 이는 자원 소유자가 관리되는 자원에 대한 액세스 권한을 다른 조직의 사용자에게 제공하는 경우에 유용합니다.

LDAP 그룹	LDAP 그룹의 구성원은 이 주제의 값으로 추가할 수 있습니다.
LDAP 역할	LDAP 역할을 이 주제의 값으로 추가할 수 있습니다. LDAP 역할은 Directory Server 역할 기능을 사용하는 임의의 역할 정의입니다. 이러한 역할은 Directory Server 역할 정의에 의해 위임되는 객체 클래스를 가집니다. 정책 구성 서비스에서 LDAP 역할 검색 필터를 수정하여 범위를 좁히고 성능을 향상시킬 수 있습니다.
LDAP 사용자	LDAP 사용자를 이 주제의 값으로 추가할 수 있습니다.
조직	조직의 구성원은 이 주제의 구성원입니다.
웹 서비스 클라이언트	유효한 값은 로컬 JKS 키 저장소에 있는 신뢰할 수 있는 인증서(신뢰할 수 있는 WSC의 인증서에 해당)의 DN입니다. 이 주제는 리버티 웹 서비스 프레임워크에 대해 종속성을 가지며 리버티 서비스 공급자가 WSC를 인증하기 위해서만 사용해야 합니다. SSO 토큰에 포함된 기본의 DN이 이 주제의 선택된 임의 값과 일치할 경우 SSO 토큰으로 식별된 웹 서비스 클라이언트(WSC)는 이 주제의 구성원입니다. 이 주제를 정책에 추가하기 전에 키 저장소를 만들어야 합니다. 키 저장소 설정에 대한 내용은 다음 사이트를 참조하십시오. *AccessManager-base* `/SUNWam/samples/saml/xmlsig/keytool.html`

Access Manager 역할 대 LDAP 역할

Access Manager 역할은 Access Manager를 사용하여 작성됩니다. 이러한 역할은 Access Manager에 의해 위임되는 객체 클래스를 가집니다. LDAP 역할은 Directory Server 역할 기능을 사용하는 역할 정의입니다. 이러한 역할은 Directory Server 역할 정의에 의해 위임되는 객체 클래스를 가집니다. 모든 Access Manager 역할은 Directory Server 역할로 사용될 수 있습니다. 그러나 모든 Directory Server 역할이 Access Manager 역할은 아닙니다. 147 페이지 “정책 구성 서비스”를 구성하여 기존 디렉토리에서 LDAP 역할을 활용할 수 있습니다. Access Manager 역할은 Access Manager 정책 서비스를 호스트하는 방법으로만 액세스할 수 있습니다. 정책 구성 서비스에서 LDAP 역할 검색 필터를 수정하여 범위를 좁히고 성능을 향상시킬 수 있습니다.

중첩된 역할

중첩된 역할은 정책 정의의 주제에서 LDAP 역할로 올바르게 평가될 수 있습니다.

조건

조건을 사용하면 정책에서 제약 조건을 정의할 수 있습니다. 예를 들어, 급여 응용 프로그램에 대한 정책을 정의할 경우 지정된 시간 동안만 응용 프로그램에 대한 액세스를 제한하는 조건을 현재 작업에서 정의할 수 있습니다. 또는 주어진 IP 주소 집합이나 회사 인트라넷에서 요청을 보낸 경우에만 작업을 허가하는 조건을 정의할 수 있습니다.

조건을 추가로 사용하여 동일한 도메인에서 다른 URL에 대한 다른 정책을 구성할 수 있습니다. 예를 들어 `http://org.example.com/hr/*jsp`는 `org.example.net`에서 오전 9시부터 오후 5시까지만 액세스할 수 있고 `http://org.example.com/finance/*.jsp`는 `org.example2.net`에서 오전 5시부터 오후 11시까지 액세스할 수 있습니다. 이렇게 하려면 IP 조건과 함께 시간 조건을 사용합니다. 규칙 자원을 `http://org.example.com/hr/*.jsp`로 지정할 경우 `http://org.example.com/hr` 및 하위 디렉토리에 있는 모든 JSP 정책이 적용됩니다.

주 – 용어 참조, 규칙, 자원, 주제, 조건, 작업 및 값은 `policy.dtd`의 *Referral*, *Rule*, *ResourceName*, *Subject*, *Condition*, *Attribute* 및 *Value* 요소에 해당합니다.

추가할 수 있는 기본 조건은 다음과 같습니다.

인증 수준 — 사용자의 인증 수준이 조건에 설정된 인증 수준보다 높거나 같은 경우에 정책이 적용됩니다.

이 속성은 인증의 트러스트 수준을 나타냅니다.

인증 수준 조건은 해당 영역의 등록된 인증 모듈 수준이 아닌 다른 수준을 지정하는 데 사용됩니다. 다른 영역에서 인증된 사용자에게 정책을 적용할 때 유용합니다.

LE 인증은 사용자의 인증 수준이 조건에 설정된 인증 수준보다 높거나 같은 경우에 정책을 적용합니다. 인증 수준 조건은 해당 영역의 등록된 인증 모듈 수준이 아닌 다른 수준을 지정하는 데 사용됩니다. 다른 영역에서 인증된 사용자에게 정책을 적용할 때 유용합니다.

인증 방식 — 풀 다운 메뉴에서 조건에 대한 인증 방식을 선택합니다. 이러한 인증 방식은 영역에서 핵심 인증 서비스에 정의된 인증 모듈입니다.

IP 주소 — IP 주소의 범위를 기반으로 조건을 설정합니다. 정의할 수 있는 필드는 다음과 같습니다.

- 보내는/받는 IP 주소 — IP 주소 범위를 지정합니다.
- DNS 이름 — DNS 이름을 지정합니다. 이 필드는 정규화된 호스트 이름이나 다음 형식의 문자열이 될 수 있습니다.

  domainname

  **.domainname*

세션 — 사용자 세션 데이터에 따라 조건을 설정합니다. 수정할 수 있는 필드는 다음과 같습니다.

- 최대 세션 시간 — 세션이 시작될 때부터 정책을 적용할 수 있는 최대 기간을 지정합니다.

- 세션 종료 — 선택된 경우 세션 시간이 최대 세션 시간 필드에 정의된 최대 허용 시간을 초과하면 사용자 세션이 종료됩니다.

  이 조건으로 민감한 자원을 보호하여 인증 이후 제한된 시간 동안만 자원을 사용할 수 있도록 합니다.

세션 등록 정보 — 사용자의 Access Manager 세션에 설정된 등록 정보 값에 따라 정책을 요청에 적용할 수 있는지 여부를 결정합니다. 정책 평가 중 조건에 정의된 모든 등록 정보 값이 사용자의 세션에 있는 경우에만 true를 반환합니다. 조건에 여러 값으로 정의된 등록 정보의 경우 조건의 등록 정보에 대해 나열된 값이 토큰에 하나 이상 있으면 충분합니다. 예를 들어 이 조건을 사용하여 외부 저장소의 속성에 따라 정책을 적용할 수 있습니다. 인증 사후 플러그인은 외부 속성에 따라 세션 등록 정보를 설정할 수 있습니다.

시간 — 시간 제약 조건에 따라 조건을 설정합니다. 필드는 다음과 같습니다.

- 시작/끝 날짜 — 날짜 범위를 지정합니다.
- 시간 — 하루 중 시간의 범위를 지정합니다.
- 요일 — 요일의 범위를 지정합니다.
- 시간대 — 표준 또는 사용자 정의 표준 시간대를 지정합니다. 사용자 정의 표준 시간대는 Java에서 구성한 표준 시간대 아이디(예: PST)만 될 수 있습니다. 지정된 값이 없을 경우 기본값은 Access Manager JVM에 설정된 표준 시간대입니다.

응답 공급자

응답 공급자는 정책 기반 응답 속성을 제공하는 플러그인입니다. 응답 공급자 속성은 정책 결정과 함께 PEP로 전송됩니다. Access Manager에는 하나의 구현인 `IDResponseProvider`가 포함되어 있습니다. 사용자 정의 응답 공급자는 이 버전의 Access Manager에서 지원되지 않습니다. 에이전트, PEP는 보통 이러한 응답 속성을 헤더로 응용 프로그램에 전달합니다. 응용 프로그램은 일반적으로 이러한 속성을 사용하여 포털 페이지와 같은 응용 프로그램 페이지를 사용자 설정합니다.

정책 권고

조건에 따라 결정한 대로 정책을 적용할 수 없을 때는 그 조건에서 해당 정책을 요청에 적용할 수 없는 이유를 나타내는 권고 메시지를 만듭니다. 이러한 권고 메시지는 정책 적용 지점에 대한 정책 결정에 전달됩니다. 정책 적용 지점은 이 권고를 검색하고 더 높은 수준으로 인증하는 인증 메커니즘으로 사용자를 리디렉션하는 등의 적당한 조치를 취하게 됩니다. 적합한 조치가 취해진 후 정책이 적용 가능하게 되면 사용자에게 더 높은 수준의 인증에 관한 프롬프트가 나타나 자원에 액세스할 수 있게 됩니다.

자세한 내용은 다음 클래스를 참조하십시오.

```
com.sun.identity.policy.ConditionDecision.getAdvices()
```

해당 조건이 충족되지 않으면 AuthLevelCondiiton 및 AuthSchemeCondition 에서 권고를 제공합니다.

AuthLevelCondition 권고는 다음 키와 관련되어 있습니다.

```
com.sun.identity.policy.plugin.AuthLevelCondition.AUTH_LEVEL_CONDITION_ADVICE
```

AuthSchemeCondition 권고는 다음 키와 관련되어 있습니다.

```
com.sun.identity.policy.plugin.AuthLevelCondition.AUTH_SCHEME_CONDITION_ADVICE
```

사용자 정의한 조건도 권고를 만들 수 있습니다. 그러나 Access Manager 정책 에이전트는 인증 수준 권고와 인증 방식 권고에만 응답합니다. 사용자 정의 에이전트를 작성하고 기존 Access Manager 에이전트를 확장하여 더 많은 권고를 이해하고 응답할 수 있습니다. 자세한 내용은 **Sun Java System Access Manager Policy Agent 2.2 User's Guide**를 참조하십시오.

참조 정책

관리자는 한 영역의 정책 정의와 결정을 다른 영역에 위임해야 할 수 있습니다. 또는 자원에 대한 정책 결정을 다른 정책 제품에 위임할 수 있습니다. 참조 정책은 정책 작성과 평가를 위해 이 정책 위임을 제어합니다. 이 정책은 하나 이상의 규칙과 하나 이상의 참조로 구성됩니다.

규칙

규칙은 정책 정의와 평가가 참조되는 자원을 정의합니다.

참조

참조는 정책 평가가 참조되는 조직을 정의합니다. 기본적으로 참조에는피어 영역과 하위 영역의 두 가지 유형이 있습니다. 이러한 참조는 각각 동일한 수준의 영역과 하위 수준의 영역에 위임됩니다. 자세한 내용은 141 페이지 "피어 영역 및 하위 영역에 대한 정책 만들기 "를 참조하십시오.

주 – 참조 대상 영역은 참조된 자원 또는 그 하위 자원에 대해서만 정책을 정의하거나 평가할 수 있습니다. 그러나 이 제한은 최상위 영역에는 적용되지 않습니다.

정책 정의 유형 문서

일단 작성하여 구성한 정책은 Directory Server에 XML 파일로 저장됩니다. Directory Server에서 XML로 인코딩된 데이터는 한 장소에 저장됩니다. `amAdmin.dtd`(또는 콘솔)를 사용하여 정책을 정의하고 구성하지만 실제로 Directory Server에는 `policy.dtd`를 기반으로 한 XML로 저장됩니다. `policy.dtd`에는 정책 작성 태그가 없고 `amAdmin.dtd`에서 추출한 정책 요소 태그가 포함됩니다. 그러므로 정책 서비스는 Directory Server에서 정책을 로드할 때 `policy.dtd`를 기반으로 XML의 구문을 분석합니다. `amAdmin.dtd`는 명령줄을 사용하여 정책을 만들 때만 사용됩니다. 이 절에서는 `policy.dtd`의 구조에 대해 설명합니다. `policy.dtd`는 다음 위치에 있습니다.

```
AccessManager-base/SUNWam/dtd(Solairs)
AccessManager-base/identity/dtd(Linux)
```

주 – 이 장에서는 Solaris 디렉토리에 대한 내용만 설명합니다. Linux의 디렉토리 구조는 다르므로 유의하십시오.

Policy 요소

Policy 요소는 정책의 권한 또는 규칙과 규칙 적용 대상 또는 주제를 정의하는 루트 요소입니다. 또한 정책이 참조(위임) 정책인지 아닌지 여부와 제한(또는 조건)이 있는지 여부도 정의합니다. Policy 요소에는*Rule*, *Conditions*, *Subjects*,*Referrals* 또는 *response providers* 와 같은 하위 요소가 한 가지 이상 포함될 수 있습니다. 필수 XML 속성은 정책의 이름을 지정하는 `name` 속성입니다. `referralPolicy` 속성은 정책이 참조 정책인지 여부를 나타내며 정의하지 않을 경우 기본값은 일반 정책입니다. 선택 XML 속성은 *name* 속성과 *description* 속성입니다.

주 – 정책에 참조라는 태그를 붙이면 정책 평가 시 주제와 조건은 무시됩니다. 반대로 일반이라는 태그를 붙이면 정책을 평가할 때 참조가 무시됩니다.

Rule 요소

Rule 요소는 정책에 대한 구체적인 사항을 정의하며*ServiceName*, *ResourceName* 또는 *AttributeValuePair*의 3가지 하위 요소를 취할 수 있습니다. Rule 요소는 정책이 만들어졌던 서비스 또는 응용 프로그램의 유형과 자원 이름, 수행되는 작업을 정의합니다. 규칙은 작업 없이 정의될 수 있습니다. 예를 들어, 참조 정책 규칙에는 작업이 없습니다.

주 – *ResourceName* 요소가 정의되지 않은 정책을 정의할 수도 있습니다.

ServiceName 요소

ServiceName 요소는 정책이 적용되는 서비스의 이름을 정의합니다. 이 요소는 서비스 유형을 나타냅니다. 이 요소에는 다른 요소가 포함되지 않습니다. 이 요소의 값은 `sms.dtd`를 기반으로 서비스의 XML 파일에 정의된 것과 같습니다. *ServiceName* 요소의 XML 서비스 속성은 문자열 값을 취하는 서비스의 이름입니다.

ResourceName 요소

ResourceName 요소는 작업 수행 대상인 객체를 정의합니다. 정책은 이 객체를 보호하도록 특별히 구성되었습니다. 이 요소에는 다른 요소가 포함되지 않습니다. *ResourceName* 요소의 XML 서비스 속성은 객체의 이름입니다. *ResourceName*의 예로 웹 서버의 `http://www.sunone.com:8080/images` 또는 디렉토리 서버의 `ldap://sunone.com:389/dc=example,dc=com`을 들 수 있습니다. 보다 구체적인 자원의 예로 `salary://uid=jsmith,ou=people,dc=example,dc=com`을 들 수 있으며 여기서 작업 대상 객체는 John Smith의 급여 정보입니다.

AttributeValuePair 요소

AttributeValuePair 요소는 작업과 그 작업의 값을 정의합니다. 이 요소는 137 페이지 "Subject 요소", 138 페이지 "Referral 요소" 및 138 페이지 "Condition 요소"의 하위 요소로 사용됩니다. *Attribute* 요소와 *Value* 요소가 모두 포함되며 XML 서비스 속성은 포함되지 않습니다.

Attribute 요소

Attribute 요소는 작업의 이름을 정의합니다. 작업은 자원에 대해 수행되는 작업 또는 이벤트입니다. POST 또는 GET은 웹 서버 자원에 대해 수행되는 작업이며 READ 또는 SEARCH는 디렉토리 서버 자원에 대해 수행되는 작업입니다. *Attribute* 요소는 *Value* 요소와 함께 사용되어야 합니다. *Attribute* 요소 자체는 다른 요소를 포함하지 않습니다. *Attribute* 요소의 XML 서비스 속성은 작업의 이름입니다.

Value 요소

Value 요소는 작업 값을 정의합니다. 작업 값으로는 허용/거부 또는 예/아니요 등이 있습니다. 그 밖의 작업 값은 부울, 숫자 또는 문자열일 수 있습니다. 작업 값은 `sms.dtd`를 기반으로 서비스의 XML 파일에 정의됩니다. *Value* 요소는 다른 요소를 포함하지 않으며 XML 서비스 속성도 포함하지 않습니다.

주 – 거부 규칙은 허용 규칙보다 항상 우선됩니다. 예를 들어 한 정책이 액세스를 거부하고 다른 정책은 허용할 경우, 두 정책에 대한 다른 모든 조건은 충족된다고 가정할 때정책 간에 잠재적인 충돌이 일어날 수 있으므로 거부 정책을 사용할 때는 매우 주의해야 합니다. 명시적인 거부 규칙이 사용될 경우 역할이나 그룹 구성원처럼 다른 주제를 통해 사용자에게 할당된 정책 때문에 액세스가 거부될 수 있습니다. 일반적으로 정책 정의 프로세스에서는 허용 규칙만 사용해야 합니다. 기본 거부는 다른 정책이 적용되지 않을 때 사용될 수 있습니다.

Subjects 요소

Subjects 하위 요소는 정책이 적용되는 객체의 집합을 식별합니다. 이 집합은 그룹의 구성원, 역할의 소유자 또는 개인 사용자에 따라 선택됩니다. 이 요소의 하위 요소는 *Subject*입니다. 정의될 수 있는 XML 속성은 다음과 같습니다.

name. 이 속성은 컬렉션의 이름입니다.

description. 이 속성은 주제에 대한 설명입니다.

includeType. 이 속성은 현재 사용되지 않습니다.

Subject 요소

Subject 하위 요소는 정책이 적용되는 기본의 집합을 식별합니다. 이 집합은 Subjects 요소에 의해 정의되는 집합에서 보다 구체적인 객체들의 집합을 가려낸 것입니다. 이 집합의 구성원은 역할, 그룹 구성원 또는 개별 사용자를 기반으로 할 수 있습니다. 이 요소에는 하위 요소인 136 페이지 “AttributeValuePair 요소”가 포함됩니다. 필수 XML 속성은 `type`입니다. 이 속성은 정의된 주제가 취해지는 객체의 집합을 식별합니다. 다른 XML 속성으로는 집합의 이름을 정의하는 `name` 속성과 집합이 정의된 대로인지 정책이 Subject의 구성원이 아닌 사용자에게 적용되는지 여부를 정의하는 `includeType` 속성이 있습니다.

주 – 다수의 Subject를 정의할 때는 최소한 그 중 하나가 정책이 적용될 사용자에게 적용되어야 합니다. false로 설정된 `includeType`으로 Subject를 정의한 경우 사용자는 적용할 정책에 대한 해당 Subject의 구성원이 아니어야 합니다.

Referrals 요소

Referrals 하위 요소는 정책 참조 집합을 식별합니다. 이 요소는 *Referral* 하위 요소를 취합니다. 정의될 수 있는 XML 속성은 집합의 이름을 정의하는 `name` 속성과 설명을 취하는 `description` 속성입니다.

Referral 요소

Referral 하위 요소는 특정 정책 참조를 식별합니다. 이 요소는 136 페이지 "AttributeValuePair 요소"를 하위 요소로 취합니다. 필수 XML 속성은 구체적으로 정의된 참조를 취하는 할당의 집합을 식별하는 `type` 속성입니다. 집합의 이름을 정의하는 `name` 속성도 포함될 수 있습니다.

Conditions 요소

Conditions 하위 요소는 정책 제한 사항(시간 범위, 인증 수준 등)의 집합을 식별합니다. 이 요소는 하나 이상의 *Condition* 하위 요소를 포함해야 합니다. 정의될 수 있는 XML 속성은 집합의 이름을 정의하는 `name` 속성과 설명을 취하는 `description` 속성입니다.

주 – Conditions 요소는 정책의 선택 요소입니다.

Condition 요소

Condition 하위 요소는 특정 정책 제한 사항(시간 범위, 인증 수준 등)을 식별합니다. 이 요소는 136 페이지 "AttributeValuePair 요소"를 하위 요소로 취합니다. 필수 XML 속성은 구체적으로 정의된 조건을 취하는 제한 사항의 집합을 식별하는 `type` 속성입니다. 집합의 이름을 정의하는 `name` 속성도 포함될 수 있습니다.

정책 가능 서비스 추가

지정된 서비스의 자원에 대한 정책은 서비스 방식에 `sms.dtd` 에 구성되는 `<Policy>` 요소가 있는 경우에만 정의할 수 있습니다.

기본적으로, Access Manager는 URL 정책 에이전트 서비스(`iPlanetAMWebAgentService`)를 제공합니다. 이 서비스는 다음 디렉토리에 있는 XML 파일에 정의됩니다.

```
/etc/opt/SUNWam/config/xml/
```

그러나 Access Manager에 정책 서비스를 추가할 수 있습니다. 일단 정책 서비스가 만들어지면 `amadmin` 명령줄 유틸리티를 통해 Access Manager에 추가합니다.

▼ 새 정책 사용 가능 서비스를 추가하려면

1 **sms.dtd에 따라 XML 파일 형식의 새 정책 서비스를 개발합니다. Access Manager는 두 가지 정책 서비스 XML 파일을 제공하며 사용자는 다음과 같은 새 정책 서비스 파일을 기준으로 사용하게 됩니다.**

`amWebAgent.xml` - 기본 URL 정책 에이전트 서비스를 위한 XML 파일로 `/etc/opt/SUNWam/config/xml/`에 있습니다.

`SampleWebService.xml` - `AccessManager-base/samples/policy`에 있는 샘플 정책 서비스 파일입니다.

2 **새 정책 서비스를 로드할 디렉토리에 XML 파일을 저장합니다. 예를 들면 다음과 같습니다.**

```
/config/xml/newPolicyService.xml
```

3 **amadmin 명령줄 유틸리티를 사용하여 새 정책 서비스를 로드합니다. 예를 들면 다음과 같습니다.**

```
AccessManager-base/SUNWam/bin/amadmin
    --runasdn "uid=amAdmin,ou=People,default_org,
root_suffix
    --password password
    --schema /config/xml/newPolicyService.xml
```

4 **새 정책 서비스를 로드한 후 amadmin을 통해 새 정책을 로드하거나 Access Manager 콘솔을 통해 정책 정의 규칙을 정의할 수 있습니다.**

정책 만들기

정책 API와 Access Manager 콘솔을 통해 정책을 만들고 수정하고 삭제할 수 있으며 `amadmin` 명령줄 도구를 통해 정책을 만들고 삭제할 수 있습니다. `amadmin` 유틸리티를 사용하여 XML의 정책을 가져오고 나열할 수도 있습니다. 이 절에서는 `amadmin` 명령줄 유틸리티와 Access Manager 콘솔을 통해 정책을 만드는 방법에 대해 설명합니다. 정책 API에 대한 자세한 내용은 **Sun Java System Access Manager 7 2005Q4 Developer's Guide**를 참조하십시오.

정책은 일반적으로 XML 파일을 사용하여 만들어지며 `amadmin` 명령줄 유틸리티를 통해 Access Manager에 추가된 후 Access Manager 콘솔을 사용하여 관리됩니다(콘솔을 사용하여 정책을 만들 수도 있음). `amadmin`을 사용하여 직접 정책을 수정할 수 없기 때문입니다. 정책을 수정하려면 Access Manager에서 정책을 삭제한 다음 `amadmin`을 사용하여 수정된 정책을 추가해야 합니다.

일반적으로 정책은 영역(또는 하위 영역) 수준에서 만들어져 영역 트리 전체에 사용됩니다.

▼ amadmin을 사용하여 정책을 만들려면

1 amadmin.dtd를 기반으로 정책 XML 파일을 만듭니다. 이 파일은 다음 디렉토리에 있습니다.

AccessManager-base/SUNWam/dtd

2 일단 정책 XML 파일이 만들어지면 다음 명령을 사용하여 로드할 수 있습니다.

AccessManager-base/SUNWam/bin/amadmin
--runasdn "uid=amAdmin,ou=People,*default_org*,
root_suffix"
--password *password*
--data *policy.xml*

여러 정책을 동시에 추가하려면 각 XML 파일에 정책을 하나씩 사용하는 대신 XML 파일 하나에 여러 정책을 입력합니다. 여러 XML 파일을 사용하여 정책을 빠르게 연속으로 로드하면 내부 정책 색인이 손상되어 일부 정책이 정책 평가에 포함되지 않을 수 있습니다.

amadmin을 통해 정책을 만들 경우, 인증 스키마 조건을 만드는 동안 인증 모듈이 영역에 등록되고 영역, LDAP 그룹, LDAP 역할 및 LDAP 사용자 주제를 만드는 동안 해당 LDAP 객체(영역, 그룹, 역할 및 사용자)가 존재하며 IdentityServerRoles 주제를 만드는 동안 Access Manager 역할이 존재하고 하위 영역 또는 피어 영역 참조를 만드는 동안 관련 영역이 존재하는지 확인합니다.

SubrealmReferral, PeerRealmReferral, Realm 주제, IdentityServerRoles 주제, LDAPGroups 주제 , LDAPRoles 주제 및 LDAPUsers의 값 요소 텍스트에서 주제는 전체 DN이어야 합니다.

▼ Access Manager 콘솔을 사용하여 일반 정책을 만들려면

1 정책을 만들려는 영역을 선택합니다.

2 정책 탭을 누릅니다.

3 정책 목록에서 새 정책을 누릅니다.

4 정책에 대한 이름 및 설명을 추가합니다.

5 정책을 활성화하려면 활성 속성에서 예를 선택합니다.

6 이 시점에서 일반 정책에 대한 모든 필드를 정의할 필요는 없습니다. 정책을 만든 다음 나중에 규칙, 주제, 조건 및 응답 공급자를 추가할 수 있습니다. 자세한 내용은 142 페이지 "정책 관리"를 참조하십시오.

7 만들기를 누릅니다.

▼ Access Manager 콘솔을 사용하여 참조 정책을 만들려면

1 **정책을 만들려는 영역을 선택합니다.**

2 **정책 탭에서 새 참조를 누릅니다.**

3 **정책에 대한 이름 및 설명을 추가합니다.**

4 **정책을 활성화하려면 활성 속성에서 예를 선택합니다.**

5 **이 시점에서 참조 정책에 대한 모든 필드를 정의할 필요는 없습니다. 정책을 만든 다음 나중에 규칙 및 참조를 추가할 수 있습니다. 자세한 내용은 142 페이지 "정책 관리"를 참조하십시오.**

6 **만들기를 누릅니다.**

피어 영역 및 하위 영역에 대한 정책 만들기

피어 및 하위 영역에 대해 정책을 만들려면 먼저 상위 또는 다른 피어 영역에 참조 정책을 만들어야 합니다. 참조 정책은 해당 규칙 정의에 하위 영역에서 관리될 자원 접두어를 포함해야 합니다. 상위 영역(또는 다른 피어 영역)에 참조 정책이 만들어지면 하위 영역(또는 피어 영역)에 일반 정책을 만들 수 있습니다.

이 예에서 `o=isp`는 상위 영역이고 `o=example.com`은 하위 영역으로 `http://www.example.com`의 자원과 하위 자원을 관리합니다.

▼ 하위 영역에 대한 정책을 만들려면

1 **`o=isp`에 참조 정책을 만듭니다. 참조 정책에 대한 내용은 145 페이지 "참조 정책 수정" 절차를 참조하십시오.**

참조 정책은 `http://www.example.com`을 규칙의 자원으로 정의하고, `example.com`을 갖는 `SubRealmReferral`을 참조의 값으로 포함해야 합니다.

2 **`example.com` 하위 영역으로 이동합니다.**

3 **이제 `isp`에서는 `example.com`으로 자원을 참조하며 `http://www.example.com` 자원 또는 `http://www.example.com`으로 시작하는 모든 자원에 대한 일반 정책을 만들 수 있습니다.**

`example.com`에 의해 관리되는 다른 자원에 대한 정책을 정의하려면 `o=isp`에 추가 참조 정책을 만들어야 합니다.

정책 관리

일단 일반 또는 참조 정책을 만들어 Access Manager에 추가하면 Access Manager 콘솔을 통해 규칙, 주제, 조건 및 참조를 수정하여 정책을 관리할 수 있습니다.

일반 정책 수정

정책 탭을 통해 액세스 권한을 정의하는 일반 정책을 수정할 수 있습니다. 여러 규칙, 주제, 조건 및 자원 비교기를 정의 및 구성할 수 있습니다. 이 절에서는 이를 수행하는 단계를 나열하고 설명합니다.

▼ 규칙을 일반 정책에 추가하거나 수정하려면

1 **이미 정책을 만든 경우 규칙을 추가하려는 정책의 이름을 누릅니다. 정책을 만들지 않은 경우 140 페이지 "Access Manager 콘솔을 사용하여 일반 정책을 만들려면"을 참조하십시오.**

2 **규칙 메뉴에서 새로 만들기를 누릅니다.**

3 **규칙에 대해 다음 기본 서비스 유형 중 하나를 선택합니다. 정책에 대해 사용 가능한 서비스가 많은 경우 목록이 더 클 수도 있습니다.**

검색 서비스	검색 서비스 쿼리에 대한 인증 작업을 정의하고 지정된 자원에 대한 웹 서비스 클라이언트의 프로토콜 호출을 수정합니다.
리버티 개인 프로필 서비스	리버티 개인 프로필 서비스 쿼리에 대한 인증 작업을 정의하고 지정된 자원에 대한 웹 서비스 클라이언트의 프로토콜 호출을 수정합니다.
URL 정책 에이전트	정책 집행을 위해 URL 정책 에이전트 서비스를 제공합니다. 이 서비스를 사용하여 관리자는 정책 집행자 또는 정책 에이전트를 통해 정책을 만들고 관리할 수 있습니다.

4 **다음을 누르십시오.**

5 **규칙에 대한 이름 및 자원 이름을 입력합니다.**

현재 정책 에이전트는 `http://` 및 `https://` 자원만 지원하고 호스트 이름 대신 IP 주소를 사용하는 것을 지원하지 않습니다.

호스트, 포트 및 자원 이름에 와일드카드가 지원됩니다. 예를 들면 다음과 같습니다.

```
http*://*:*/*.html
```

URL 정책 에이전트 서비스의 경우 포트 번호를 입력하지 않으면 기본 포트 번호는 `http://`의 경우 80이고 `https://`의 경우 443입니다.

6 규칙의 작업을 선택합니다. URL 정책 에이전트 서비스를 사용하는 경우 다음을 선택할 수 있습니다.

- GET
- POST

7 작업 값 선택

- 허용— 규칙에 정의된 자원과 일치하는 자원에 액세스할 수 있게 합니다.
- 거부— 규칙에 정의된 자원과 일치하는 자원에 대한 액세스를 거부합니다.
- 거부 규칙은 허용 규칙보다 항상 우선됩니다. 예를 들어, 주어진 자원에 대해 두 개의 정책, 즉 액세스를 거부하는 정책과 액세스를 허용하는 정책이 있을 경우 결과적으로 액세스가 거부됩니다(두 정책에 대한 조건이 충족될 경우). 정책 간에 잠재적인 충돌이 일어날 수 있으므로 거부 정책을 사용할 때는 매우 주의해야 합니다. 정책 정의 프로세스에서는 허용 규칙만 사용해야 합니다. 자원에 적용할 수 있는 정책이 없는 경우 액세스는 자동으로 거부됩니다.

  명시적 거부 규칙이 사용될 경우 다른 주제(예: 역할 및/또는 그룹 구성원)를 통해 주어진 사용자에 할당되는 정책은 하나 이상의 정책에 액세스를 허용할 경우 자원에 대한 액세스가 거부될 수 있습니다. 예를 들어, 사원 역할에 적용할 수 있는 자원에 대한 거부 정책이 있고 관리자 역할에 적용할 수 있는 동일한 자원에 대한 허용 정책이 있는 경우 사원 역할과 관리자 역할이 모두 할당된 사용자에 대한 정책 결정이 거부됩니다.

  이러한 문제를 해결하는 한 가지 방법은 조건 플러그 인을 사용하여 정책을 설계하는 것입니다. 위의 경우에 사원 역할에 인증된 사용자에게 거부 정책을 적용하고 관리자 역할에 인증된 사용자에게 허용 정책을 적용하는 "역할 조건"을 지정하여 두 정책을 차별화할 수 있습니다. 다른 방법은 **인증 수준** 조건을 사용하는 것입니다. 이 조건에서는 관리자 역할이 더 높은 인증 수준으로 인증됩니다.

8 마침을 누릅니다.

▼ 주제를 일반 정책에 추가하거나 수정하려면

1 이미 정책을 만든 경우 주제를 추가하려는 정책의 이름을 누릅니다. 아직 정책을 만들지 않은 경우 140 페이지 "Access Manager 콘솔을 사용하여 일반 정책을 만들려면 "을 참조하십시오.

2 주제 목록에서 새로 만들기를 누릅니다.

3 다음 기본 주제 유형 중 하나를 선택합니다. 주제 유형에 대한 설명은 130 페이지 "주제"를 참조하십시오.

4 다음을 누르십시오.

5 주제의 이름을 입력합니다.

6 **단독 필드를 선택하거나 선택 취소합니다.**

이 필드를 선택하지 않을 경우(기본값) 주제의 구성원인 Identity에 정책이 적용됩니다. 이 필드를 선택할 경우 정책은 주제의 구성원이 아닌 Identity에 적용됩니다.

정책에 여러 개의 주제가 있는 경우 Identity가 최소한 하나 이상 주제의 구성원이면 정책은 Identity에 적용됩니다.

7 **주제에 추가할 Identity를 표시하기 위해 검색을 수행합니다. 이 단계는 인증된 사용자 주제 또는 웹 서비스 클라이언트 주제에는 적용되지 않습니다.**

기본(*) 검색 패턴은 모든 항목을 표시합니다.

8 **주제에 대해 추가할 개별 Identity를 선택하거나 모두 추가를 눌러 모든 Identity를 한 번에 추가합니다. 추가를 눌러 Identity를 선택 목록으로 이동합니다. 인증된 사용자 주제에 대해서는 이 단계가 해당되지 않습니다.**

9 **마침을 누릅니다.**

10 **정책에서 주제를 제거하려면 해당 주제를 선택하고 삭제를 누릅니다. 주제 이름을 눌러 주제 정의를 편집할 수 있습니다.**

▼ 일반 정책에 조건을 추가하려면

1 **이미 정책을 만든 경우 조건을 추가하려는 정책의 이름을 누릅니다. 아직 정책을 만들지 않은 경우 140 페이지 "Access Manager 콘솔을 사용하여 일반 정책을 만들려면 "을 참조하십시오.**

2 **조건 목록에서 새로 만들기를 누릅니다.**

3 **조건 유형을 선택하고 다음을 누릅니다.**

4 **조건 유형의 필드를 정의합니다. 조건 유형에 대한 설명은 131 페이지 "조건"을 참조하십시오.**

5 **마침을 누릅니다.**

▼ 일반 정책에 응답 공급자를 추가하려면

1 **이미 정책을 만든 경우 응답 공급자를 추가하려는 정책의 이름을 누릅니다. 아직 정책을 만들지 않은 경우 140 페이지 "Access Manager 콘솔을 사용하여 일반 정책을 만들려면 "을 참조하십시오.**

2 **응답 공급자 목록에서 새로 만들기를 누릅니다.**

3 **응답 공급자의 이름을 입력합니다.**

4 다음 값을 정의합니다.

StaticAttribute — `IDResponseProvider` 인스턴스에 정의되고 정책에 저장된 이름 및 값을 가진 응답 속성입니다.

DynamicAttribute — 여기에서 선택한 응답 속성은 먼저 해당 영역의 정책 구성 서비스에 정의되어야 합니다. 지정한 속성 이름은 구성된 데이터 저장소에 있는 이름과 같아야 합니다. 속성을 정의하는 방법에 대한 자세한 내용은 Access Manager 온라인 도움말의 정책 구성 속성 정의를 참조하십시오.

5 마침을 누릅니다.

6 정책에서 응답 공급자를 제거하려면 해당 주제를 선택하고 삭제를 누릅니다. 이름을 눌러 응답 공급자 정의를 편집할 수 있습니다.

참조 정책 수정

참조 정책을 사용하여 정책 정의와 영역 결정을 다른 영역으로 위임할 수 있습니다. 사용자 정의 참조는 정책 대상 지점에서 정책 결정을 가져오는 데 사용됩니다. 참조 정책을 만들면 관련된 규칙, 참조 및 자원 공급자를 추가 또는 수정할 수 있습니다.

▼ 규칙을 참조 정책에 추가하거나 수정하려면

1 이미 정책을 만든 경우 규칙을 추가하려는 정책의 이름을 누릅니다. 정책을 만들지 않은 경우 141 페이지 "Access Manager 콘솔을 사용하여 참조 정책을 만들려면 "을 참조하십시오.

2 규칙 목록에서 새로 만들기를 누릅니다.

3 규칙에 대해 다음 기본 서비스 유형 중 하나를 선택합니다. 정책에 대해 사용 가능한 서비스가 많은 경우 목록이 더 클 수도 있습니다.

검색 서비스 — 검색 서비스 쿼리에 대한 인증 작업을 정의하고 지정된 자원에 대한 웹 서비스 클라이언트의 프로토콜 호출을 수정합니다.

리버티 개인 프로필 서비스 — 리버티 개인 프로필 서비스 쿼리에 대한 인증 작업을 정의하고 지정된 자원에 대한 웹 서비스 클라이언트의 프로토콜 호출을 수정합니다.

URL 정책 에이전트 — 정책 집행을 위해 URL 정책 에이전트 서비스를 제공합니다. 이 서비스를 사용하여 관리자는 정책 집행자 또는 정책 에이전트를 통해 정책을 만들고 관리할 수 있습니다.

4 다음을 누르십시오.

5 **규칙에 대한 이름 및 자원 이름을 입력합니다.**

현재 정책 에이전트는 `http://` 및 `https://` 자원만 지원하고 호스트 이름 대신 IP 주소를 사용하는 것을 지원하지 않습니다.

자원 이름, 포트 번호 및 프로토콜에 와일드카드가 지원됩니다. 예를 들면 다음과 같습니다.

```
http://*:*/*.html
```

URL 정책 에이전트 서비스의 경우 포트 번호를 입력하지 않으면 기본 포트 번호는 `http://`의 경우 80이고 `https://`의 경우 443입니다.

자원을 `http://host*:*`로 정의하여 특정 시스템에 설치된 모든 서비스에 대한 자원 관리를 허용할 수 있습니다. 또한 다음 자원을 정의하여 관리자에게 조직의 모든 서비스에 대한 특정 조직 권한을 부여할 수 있습니다.

`http://*.`*`subdomain.domain.topleveldomain`*

6 **마침을 누릅니다.**

▼ 참조를 정책에 추가 또는 수정하려면

1 **이미 정책을 만든 경우 응답 공급자를 추가하려는 정책의 이름을 누릅니다. 아직 정책을 만들지 않은 경우** **141 페이지 "Access Manager 콘솔을 사용하여 참조 정책을 만들려면 "을 참조하십시오.**

2 **규칙 목록에서 새로 만들기를 누릅니다.**

3 **서비스 유형을 선택합니다.**

4 **규칙 필드에서 자원을 정의합니다. 필드는 다음과 같습니다.**

Referral— 현재 참조 유형을 표시합니다.

Name— 참조 이름을 입력합니다.

Resource Name— 자원 이름을 입력합니다.

Filter— 값 필드에 표시될 조직 이름에 대한 필터를 지정합니다. 기본적으로 이 필드에는 모든 조직 이름이 표시됩니다.

Value — 참조의 조직 이름을 선택합니다.

5 **마침을 누릅니다.**

정책에서 참조를 제거하려면 참조를 선택하고 삭제를 누릅니다.

참조 이름 옆에 있는 편집 링크를 눌러 모든 참조 정의를 편집할 수 있습니다.

▼ 참조 정책에 응답 공급자를 추가하려면

1. **이미 정책을 만든 경우 응답 공급자를 추가하려는 정책의 이름을 누릅니다. 아직 정책을 만들지 않은 경우** **140 페이지 "Access Manager 콘솔을 사용하여 일반 정책을 만들려면"을 참조하십시오.**
2. **응답 공급자 목록에서 새로 만들기를 누릅니다.**
3. **응답 공급자의 이름을 입력합니다.**
4. **다음 값을 정의합니다.**

   StaticAttribute — `IDResponseProvider` 인스턴스에 정의되고 정책에 저장된 이름 및 값을 가진 응답 속성입니다.

   DynamicAttribute — 정책의 `IDResponseProvider` 인스턴스에 선택된 이름만 가진 응답 속성입니다. 값은 정책 평가 중 사용자 아이디 요청에 따라 `IDRepostitories`에서 읽습니다.

5. **마침을 누릅니다.**
6. **정책에서 응답 공급자를 제거하려면 해당 주제를 선택하고 삭제를 누릅니다. 이름을 눌러 응답 공급자 정의를 편집할 수 있습니다.**

정책 구성 서비스

정책 구성 서비스는 Access Manager 콘솔을 통해 각 조직에 대한 정책 관련 속성을 구성하는 데 사용됩니다. Access Manager 정책 프레임워크에 사용되는 자원 이름 구현 및 Directory Server 데이터 저장소를 정의할 수도 있습니다. 정책 구성 서비스에 지정된 Directory Server는 LDAP 사용자, LDAP 그룹, LDAP 역할 및 조직 정책 주제의 구성원 평가에 사용됩니다.

주제 결과 수명

정책 평가 성능을 향상시키려면 정책 구성 서비스의 주제 결과 수명 속성에 정의된 시간 동안 구성원 평가를 캐시에 저장합니다. 이렇게 캐시에 저장된 구성원 결정은 주제 결과 수명 속성에 정의된 시간이 다 지날 때까지 사용됩니다. 이후의 구성원 평가는 디렉토리 내 사용자의 현재 상태를 반영하는 데 사용됩니다.

동적 속성

목록에 표시되고 정책 응답 공급자 동적 속성을 정의하기 위해 선택된 허용된 동적 속성 이름입니다. 정의된 이름은 데이터 저장소에 정의된 속성 이름과 같아야 합니다.

amldapuser 정의

amldapuser는 기본으로 사용되는 설치 중에 정책 구성 서비스에서 지정된 Directory Server에 생성된 사용자입니다. 이는 필요에 따라 관리자 또는 해당 영역의 정책 관리자에 의해 변경될 수 있습니다.

정책 구성 서비스 추가

영역이 생성될 때 정책 구성 서비스 속성이 자동으로 이 영역에 대해 설정됩니다. 하지만 필요한 경우 속성을 수정할 수 있습니다.

자원 기반 인증

일부 조직에서는 사용자가 액세스를 시도하는 자원에 따라 특정 모듈에 대해 인증하는 고급 인증 시나리오를 요구합니다. 자원 기반 인증은 사용자가 기본 인증 모듈이 아니라 자원을 보호하는 특정 인증 모듈에 인증해야 하는 Access Manager의 기능입니다. 이 기능은 처음으로 사용자를 인증하는 경우에만 사용할 수 있습니다.

주 – 이 기능은 124 페이지 "세션 업그레이드"에 설명된 자원 기반 인증과는 다른 기능입니다. 해당 특정 기능에는 제한 사항이 없습니다.

제한 사항

자원 기반 인증에는 다음과 같은 제한 사항이 포함됩니다.

- 자원에 적용할 수 있는 정책에 여러 인증 모듈이 있는 경우 해당 시스템에서 임의로 하나의 인증 모듈을 선택합니다.
- 이 정책에 대해 정의될 수 있는 조건은 수준과 방법뿐입니다.
- 이 기능은 서로 다른 DNS 도메인 사이에서는 사용할 수 없습니다.

▼ 자원 기반 인증을 구성하려면

Access Manager와 정책 에이전트가 모두 설치되면 자원 기반 인증을 구성할 수 있습니다. 자원 기반 인증을 구성하려면 Access Manager가 게이트웨이 서블릿을 가리켜야 합니다.

1 **AMAgent.properties를 엽니다.**

AMAgent.properties는 Solaris 환경에서 /etc/opt//SUNWam/agents/config/에 있습니다.

2 다음 행을 주석으로 처리합니다.

```
#com.sun.am.policy.am.loginURL = http://Access
Manager_server_host.domain_name:port/amserver/UI/Login.
```

3 다음 행을 파일에 추가합니다.

```
com.sun.am.policy.am.loginURL =
http://AccessManager_host.domain_name:port/amserver/gateway
```

주 – 게이트웨이 서블릿은 Policy Evaluation API를 사용하여 개발하며 자원 기반 인증을 수행하는 사용자 정의 기법을 작성하는 데 사용됩니다. **Sun Java System Access Manager 7 2005Q4 Developer's Guide**의 6 장, "Using the Policy APIs"에 있는 6장, "Using the Policy APIs"를 참조하십시오.

---

4 에이전트를 다시 시작합니다.

◆ ◆ ◆ 9 장

9 주제 관리

주제 인터페이스를 사용해 영역 내 기본적인 아이디 관리를 할 수 있습니다. 주제 인터페이스에서 만든 모든 아이디는 Access Manager 아이디 주제 유형으로 만든 정책의 주제 정의에 사용할 수 있습니다.

생성 및 수정할 수 있는 아이디는 다음과 같습니다.

사용자

사용자는 개인의 아이디를 나타냅니다. 그룹의 사용자를 생성 및 제거할 수 있으며 역할 및/또는 그룹에 사용자를 추가 또는 제거할 수 있습니다. 사용자에게 서비스를 할당할 수도 있습니다.

▼ 사용자를 만들거나 수정하려면

1. **사용자 탭을 누릅니다.**
2. **새로 만들기를 누릅니다.**
3. **다음 필드에 데이터를 입력합니다.**

   UserId. 이 필드에는 사용자가 Access Manager에 로그인할 때 사용하는 이름을 입력합니다. 이 등록 정보는 DN 값이 아닐 수 있습니다.

   이름.이 필드는 사용자의 이름을 가집니다.

   성. 이 필드에는 사용자의 성을 입력합니다.

전체 이름. 이 필드는 사용자의 전체 이름을 가집니다.

비밀번호.이 필드는 사용자 아이디 필드에 지정된 이름의 비밀번호를 가집니다.

비밀번호(확인). 비밀번호를 확인합니다.

사용자 상태.이 옵션은 사용자에게 Access Manager를 통한 인증이 허용되었는지 여부를 나타냅니다.

4 만들기를 누릅니다.

5 사용자가 생성되면 사용자의 이름을 눌러 사용자 정보를 편집할 수 있습니다. 사용자 속성에 대한 자세한 내용은 사용자 속성을 참조하십시오. 다음을 수행할 수 있습니다.

- 151 페이지 "사용자를 만들거나 수정하려면"
- 152 페이지 "역할 및 그룹에 사용자를 추가하려면"
- 152 페이지 "아이디에 서비스를 추가하려면"

▼ 역할 및 그룹에 사용자를 추가하려면

1 수정할 사용자의 이름을 누릅니다.

2 역할 또는 그룹을 선택합니다. 이미 사용자에게 할당된 역할과 그룹만 표시됩니다.

3 사용 가능한 목록에서 역할 또는 그룹을 선택하고 추가를 누릅니다.

4 선택된 목록에 역할 또는 그룹이 표시되면 저장을 누릅니다.

▼ 아이디에 서비스를 추가하려면

1 서비스를 추가할 아이디를 선택합니다.

2 서비스 탭을 누릅니다.

3 추가를 누릅니다.

4 선택한 아이디 유형에 따라 다음과 같은 서비스 목록이 표시됩니다.

- 인증 구성
- 검색 서비스
- 리버티 개인 프로필 서비스
- 세션
- 사용자

5 추가할 서비스를 선택하고 다음을 누릅니다.

6. **서비스에 대한 속성을 편집합니다. 서비스 정의에 대한 설명을 참조하려면 4단계에서 서비스 이름을 누릅니다.**

7. **마침을 누릅니다.**

에이전트

Access Manager 정책 에이전트는 허용되지 않은 침입으로부터 웹 서버 및 웹 프록시 서버의 컨텐트를 보호합니다. 또한 관리자가 구성한 정책을 기반으로 서비스 및 웹 자원에 대한 액세스를 제어합니다.

에이전트 객체는 정책 에이전트 프로필을 정의하고 Access Manager 자원을 보호하는 특정 에이전트에 대한 인증 및 기타 프로필 정보를 Access Manager에서 저장할 수 있게 합니다. 관리자는 Access Manager 콘솔을 사용해 에이전트 프로필을 확인, 작성, 수정 및 삭제할 수 있습니다.

에이전트 객체 만들기 페이지는 에이전트가 Access Manager에 대해 인증할 때 사용한 UID/비밀번호를 정의하는 곳입니다. 같은 Access Manager를 사용하는 AM/WS 설정이 여러 개 있는 경우 다른 에이전트에 대해 여러 아이디를 활성화하고 이들을 Access Manager와 별개로 활성화 및 비활성화하는 옵션을 제공합니다. 또한 각 컴퓨터에서 `AMAgent.properties`를 편집하지 않고 에이전트에 대한 일부 기본 설정 값을 중앙에서 관리할 수 있습니다.

▼ 에이전트를 만들거나 수정하려면

1. **에이전트 탭을 누릅니다.**

2. **새로 만들기를 누릅니다.**

3. **다음과 같은 필드에 값을 입력합니다.**

   이름. 에이전트의 이름 또는 아이디를 입력합니다. 에이전트가 Access Manager에 로그인할 때 사용할 이름입니다. 멀티바이트 이름은 사용할 수 없습니다.

   비밀번호. 에이전트의 비밀번호를 입력합니다. 이 비밀번호는 LDAP 인증 도중에 에이전트가 사용하는 비밀번호와는 달라야 합니다.

   비밀번호 확인. 비밀번호를 확인합니다.

   장치 상태. 에이전트의 장치 상태를 입력합니다. 활성으로 설정된 경우 에이전트는 Access Manager에 대해 인증되어 Access Manager와 통신할 수 있습니다. 비활성으로 설정된 경우 에이전트는 Access Manager에 대해 인증될 수 없습니다.

4. **만들기를 누릅니다.**

5 에이전트를 만든 후에는 다음과 같은 필드를 추가로 편집할 수 있습니다.

설명.에이전트에 대한 간단한 설명을 입력합니다. 예를 들어 에이전트 인스턴스 이름이나 에이전트가 보호하고 있는 응용 프로그램의 이름을 입력할 수 있습니다.

에이전트 키 값. 키/값 쌍을 사용하여 에이전트 등록 정보를 설정합니다. Access Manager는 이 등록 정보를 사용하여 사용자의 자격 증명 명제에 대한 에이전트 요청을 받습니다. 현재는 하나의 등록 정보만 유효하며 다른 모든 등록 정보는 무시됩니다. 다음 형식을 사용합니다.

agentRootURL=http:// *server_name:port/*

고유 정책 에이전트 아이디 만들기

기본적으로 신뢰할 수 있는 환경에서 여러 정책 에이전트를 만드는 경우 정책 에이전트에는 동일한 UID 및 비밀번호가 포함됩니다. UID 및 비밀번호를 공유하므로 Access Manager는 에이전트를 구분할 수 없어 세션 쿠키를 가로챌 수 있는 상태로 열어 둘 수 있습니다.

아이디 공급자가 타사 또는 기업 내 허용되지 않은 그룹에 의해 개발된 응용 프로그램(또는 서비스 제공업체)에 사용자에 대한 인증, 권한 부여 및 프로필 정보를 제공하는 경우 취약점이 발생할 수 있습니다. 예상되는 보안 문제는 다음과 같습니다.

- 모든 응용 프로그램은 동일한 http 세션 쿠키를 공유합니다. 이렇게 되면 rogue 응용 프로그램이 세션 쿠키를 하이재킹하여 다른 응용 프로그램에 대해 사용자를 가장할 수 있습니다.
- 응용 프로그램이 https 프로토콜을 사용하지 않는 경우 세션 쿠키는 네트워크 도청에 취약합니다.
- 단 하나의 응용 프로그램이라도 해킹당하는 경우 전체 인프라의 보안이 손상될 위험이 있습니다.
- 감염된 응용 프로그램은 세션 쿠키를 사용하여 사용자에 대한 프로필 속성을 가져와서 수정할 수 있습니다. 사용자가 관리 권한을 가진 경우 응용 프로그램은 보다 많은 손상을 입을 수 있습니다.

▼ 고유 정책 에이전트 아이디를 만들려면

1 Access Manager 관리 콘솔을 사용하여 각 에이전트에 대한 항목을 만듭니다.

2 에이전트를 만들 때 입력한 비밀번호에 대해 다음 명령을 실행합니다. 이 명령은 에이전트가 설치된 호스트에서 호출되어야 합니다.

```
AccessManager-base/SUNWam/agents/bin/crypt_util agent123
```

이 명령을 실행하면 다음과 같은 출력이 표시됩니다.

```
WnmKUCg/y3l404ivWY6HPQ==
```

3 AMAgent.properties를 변경하여 새 값을 적용한 다음 에이전트를 다시 시작합니다. 예:

```
# The username and password to use for the Application

authentication module.


com.sun.am.policy.am.username = agent123

com.sun.am.policy.am.password = WnmKUCg/y3l404ivWY6HPQ==


# Cross-Domain Single Sign On URL

# Is CDSSO enabled.

com.sun.am.policy.agents.cdsso-enabled=true


# This is the URL the user will be redirected to after successful login

# in a CDSSO Scenario.

com.sun.am.policy.agents.cdcservletURL = http://server.example.com:port

/amserver/cdcservlet
```

4 새 값을 반영하기 위해 Access Manager를 설치한 AMConfig.properties를 변경한 다음 Access Manager를 다시 시작합니다. 예:

```
com.sun.identity.enableUniqueSSOTokenCookie=true

com.sun.identity.authentication.uniqueCookieName=sunIdentityServerAuthNServer


com.sun.identity.authentication.uniqueCookieDomain=.example.com
```

5 Access Manager 콘솔에서 구성>플랫폼을 선택합니다.

6 쿠키 도메인 목록에서 쿠키 도메인 이름을 다음과 같이 변경합니다.

a. 기본 iplanet.com 도메인을 선택한 다음 제거를 누릅니다.

b. Access Manager 설치의 호스트 이름을 입력한 다음 추가를 누릅니다.
예: server.example.com

다음과 같이 브라우저에 설정된 두 개의 쿠키가 표시됩니다.

- iPlanetDirectoryPro – server.example.com(호스트 이름)
- sunIdentityServerAuthNServer – example.com(호스트 이름)

필터링된 역할

필터링된 역할은 LDAP 필터를 사용하여 작성된 동적 역할입니다. 모든 사용자가 필터를 통해 걸러져 역할 작성 시 역할에 할당됩니다. 필터는 항목의 임의 속성 값 쌍(예: `ca=user*`)을 찾아 해당 속성을 포함하는 사용자를 역할에 자동으로 할당합니다.

▼ 필터링된 역할을 만들려면

1. **이동 창에서 역할을 만들 조직으로 이동합니다.**
2. **새로 만들기를 누릅니다.**
3. **필터링된 역할의 이름을 입력합니다.**
4. **검색 조건에 대한 정보를 입력합니다.**

   예:

   ```
   (&(uid=user1)(|(inetuserstatus=active)(!(inetuserstatus=*))))
   ```

   필터를 비워두면 기본적으로 다음과 같은 역할이 생성됩니다.

   ```
   (objectclass = inetorgperson)
   ```

5. **만들기를 눌러 필터 조건에 기초한 검색을 시작합니다. 필터 조건에 의해 정의된 아이디가 자동으로 역할에 할당됩니다.**
6. **필터링된 역할이 생성되면 역할의 이름을 눌러 역할에 속한 사용자를 확인합니다. 또한 서비스 탭을 눌러 역할에 서비스를 추가할 수도 있습니다.**

역할

역할의 구성원은 역할을 소유하는 LDAP 항목입니다. 역할의 기준 자체는 속성과 함께 LDAP 항목으로 정의되며 항목의 고유 이름(DN) 속성에 의해 식별됩니다. 역할을 만들면 서비스와 사용자를 직접 추가할 수 있습니다.

▼ 역할을 만들거나 수정하려면

1. 역할 탭을 누릅니다.
2. 역할 목록에서 새로 만들기를 누릅니다.
3. 역할의 이름을 입력합니다.
4. 만들기를 누릅니다.

▼ 역할 또는 그룹에 사용자를 추가하려면

1. 사용자를 추가할 역할 또는 그룹의 이름을 누릅니다.
2. 사용자 탭을 누릅니다.
3. 사용 가능한 목록에서 추가할 사용자를 선택한 다음 추가를 누릅니다.
4. 선택된 목록에 사용자가 표시되면 저장을 누릅니다.

그룹

그룹은 공통적인 기능, 특징 또는 관심을 가지는 사용자의 집합을 나타냅니다. 일반적으로 이 그룹에는 연관된 권한이 없습니다. 그룹은 두 가지 수준 즉, 조직 내에서와 다른 관리 대상 그룹 내에서 존재할 수 있습니다.

▼ 그룹을 만들거나 수정하려면

1. 그룹 탭을 누릅니다.
2. 그룹 목록에서 새로 만들기를 누릅니다.
3. 그룹의 이름을 입력합니다.
4. 만들기를 누릅니다.
   그룹을 만들면 그룹 이름 및 사용자 탭을 차례로 눌러 그룹에 사용자를 추가할 수 있습니다.

파 트 III

디렉토리 관리 및 기본 서비스

Sun Java System Access Manager 7 2005Q4 관리 설명서의 제3부입니다. 디렉토리 관리 장에서는 Access Manager를 레거시 모드로 배포할 때 디렉토리 객체를 관리하는 방법에 대해 설명합니다. 다른 장에서는 Access Manager의 일부 기본 서비스를 구성하고 사용하는 방법에 대해 설명합니다. 제1부는 다음 내용으로 구성되어 있습니다.

◆ ◆ ◆ 10장

10 디렉토리 관리

디렉토리 관리 탭은 Access Manager를 레거시 모드로 설치할 경우에만 표시됩니다. 디렉토리 관리 기능은 Sun Java System Directory Server를 사용하는 Access Manager 배포를 위한 Identity 관리 솔루션을 제공합니다.

레거시 모드 설치 옵션에 대한 자세한 내용은 **Sun Java Enterprise System 2005Q4 Installation Guide for UNIX**를 참조하십시오.

디렉토리 객체 관리

디렉토리 관리 탭에는 Directory Server 객체를 보고 관리하는 데 필요한 모든 구성 요소가 포함되어 있습니다. 이 절에서는 객체 유형과 객체 유형을 구성하는 방법에 대해 설명합니다. Access Manager 콘솔 또는 명령줄 인터페이스를 사용하여 사용자, 역할, 그룹, 조직, 하위 조직 및 컨테이너 객체를 정의, 수정 또는 삭제할 수 있습니다. 콘솔에는 다양한 권한으로 디렉토리 객체를 생성하고 관리하는 기본 관리자가 있습니다. 역할을 기반으로 추가 관리자를 만들 수 있습니다. 관리자는 Access Manager 설치 시 Directory Server 내에 정의됩니다. 다음은 사용자가 관리할 수 있는 Directory Server 객체입니다.

조직

조직은 기업에서 부서와 자원을 관리하는 데 사용되는 최상위 수준의 계층 구조를 나타냅니다. 설치 시 Access Manager는 Access Manager 엔터프라이즈 구성을 관리하기 위해 최상위 수준 조직(설치하는 동안 정의됨)을 동적으로 만듭니다. 설치 후에 추가 조직을 생성해 개별 기업을 관리할 수 있습니다. 생성되는 모든 조직은 최상위 조직 아래에 놓입니다.

▼ 조직을 만들려면

1 **디렉토리 관리 탭을 누릅니다.**

2 **조직 목록에서 새로 만들기를 누릅니다.**

3 **필드에 대한 값을 입력합니다. 이름 필드만 필수입니다. 필드는 다음과 같습니다.**

이름 — 조직의 이름 값을 입력합니다.

도메인 이름 — 조직의 완전한 DNS(Domain Name System) 이름을 입력합니다(있을 경우).

조직 상태 — **활성** 또는 **비활성** 상태를 선택합니다. 기본값은 `active`입니다. 조직의 수명 동안 등록 정보 아이콘을 선택하여 언제든지 이 값을 변경할 수 있습니다. `inactive`를 선택하면 조직에 로그인할 때 사용자 액세스가 사용 불가능하게 됩니다.

조직 별칭 — 이 필드는 URL 로그인에서 별칭을 사용하여 인증할 수 있도록 조직에 대한 별칭 이름을 정의합니다. 예를 들어, 조직 이름이 `exampleorg`이고 `123` 및 `abc`를 별칭으로 정의하는 경우 다음 URL 중 하나를 사용하여 조직에 로그인할 수 있습니다.

```
http://machine.example.com/amserver/UI/Login?org=exampleorg

http://machine.example.com/amserver/UI/Login?org=abc

http://machine.example.com/amserver/UI/Login?org=123
```

조직 별칭 이름은 조직 전체에서 고유해야 합니다. 고유 속성 목록을 사용하여 고유성을 강제로 적용할 수 있습니다.

DNS 별칭 이름 — 조직의 DNS 이름에 대한 별칭 이름을 추가할 수 있습니다. 이 속성은 "실제" 도메인 별칭(임의의 문자열은 허용 안 됨)만 수락합니다. 예를 들어, DNS 이름이 `example.com`이고 `example1.com` 및 `example2.com`을 `exampleorg` 조직에 대한 별칭으로 정의하는 경우 다음 URL 중 하나를 사용하여 조직에 로그인할 수 있습니다.

```
http://machine.example.com/amserver/UI/

Login?org=exampleorg

http://machine.example1.com/amserver/

UI/Login?org=exampleorg

http://machine.example2.com/amserver/

UI/Login?org=exampleorg
```

고유 속성 목록 조직의 사용자에 대한 고유 속성 이름 목록을 추가할 수 있습니다. 예를 들어, 전자 메일 주소를 지정하는 고유한 속성 이름을 추가할 경우 동일한 전자 메일 주소를 가지는 두 명의 사용자를 만들 수 없습니다. 또한, 이 필드에서는 쉼표로 구분된 목록을 허용합니다. 목록에 있는 속성 이름 중 하나가 고유성을 정의합니다. 예를 들어, 필드에 다음과 같은 속성 이름 목록이 있고

```
PreferredDomain, AssociatedDomain
```

`PreferredDomain`이 특정 사용자에 대한 `http://www.example.com`으로 정의되는 경우 전체 쉼표로 구분된 목록이 해당 URL에 대한 고유성으로 정의됩니다. 고유 속성 목록에 이름 지정 속성인 'ou'를 추가하면 기본 그룹, 사용자 컨테이너의 속성에 고유성이 강제 적용되지 않습니다. (ou=Groups,ou=People)

모든 하위 조직에 고유성이 강제 적용됩니다.

4 확인을 누릅니다.

새 조직이 조직 목록에 표시됩니다. 조직을 만드는 동안 정의한 등록 정보를 편집하려면 편집할 조직의 이름을 누르고 등록 정보를 변경한 다음 저장을 누릅니다.

▼ 조직을 삭제하려면

1 삭제할 조직의 이름 옆에 있는 확인란을 선택합니다.

2 삭제를 누릅니다.

주 – 삭제를 수행할 때 경고 메시지가 나타나지 않습니다. 조직 내의 모든 항목이 삭제되고 실행 취소를 수행할 수 없습니다.

정책에 조직을 추가하려면

Access Manager 객체는 정책의 주제 정의를 통해 정책에 추가됩니다. 정책을 작성하거나 수정할 때 조직, 역할, 그룹 및 사용자를 주제로 정의할 수 있습니다. 주제가 정의되고 나면 정책이 객체에 적용됩니다. 자세한 내용은 142 페이지 "정책 관리"를 참조하십시오.

컨테이너

객체 클래스와 속성의 차이로 인해 조직 항목을 사용할 수 없는 경우 컨테이너 항목을 사용합니다. Access Manager 컨테이너 항목과 Access Manager 조직 항목이 LDAP 객체 클래스

organizationalUnit 및 organization과 반드시 같을 필요가 없다는 것이 중요합니다. 추상적인 identity 항목입니다. 이상적인 경우라면 컨테이너 항목 대신 조직 항목이 사용됩니다.

주 – 컨테이너 표시는 선택 사항입니다. 컨테이너를 보려면 구성>콘솔 등록 정보 아래의 관리 서비스에서 컨테이너 표시를 선택해야 합니다.

▼ 컨테이너를 만들려면

1. **새 컨테이너가 생성될 조직의 위치 링크 또는 컨테이너를 선택합니다.**
2. **컨테이너 탭을 누릅니다.**
3. **컨테이너 목록에서 새로 만들기를 누릅니다.**
4. **만들려는 컨테이너의 이름을 입력합니다.**
5. **확인을 누릅니다.**

▼ 컨테이너를 삭제하려면

1. **컨테이너 탭을 누릅니다.**
2. **삭제할 컨테이너의 이름 옆에 있는 확인란을 선택합니다.**
3. **삭제를 누릅니다.**

주 – 컨테이너를 삭제하면 해당 컨테이너에 존재하는 모든 객체가 삭제됩니다. 여기에는 모든 객체와 하위 컨테이너가 포함됩니다.

그룹 컨테이너

그룹 컨테이너는 그룹을 관리하는 데 사용됩니다. 그룹 컨테이너는 그룹과 다른 그룹 컨테이너만 포함할 수 있습니다. 그룹 컨테이너 그룹은 모든 관리 대상 그룹에 대한 부모 항목으로 동적으로 할당됩니다. 원하는 경우 추가 그룹 컨테이너를 추가할 수 있습니다.

주 – 그룹 컨테이너의 표시는 선택 사항입니다. 그룹 컨테이너를 보려면 구성>콘솔 등록 정보의 관리 서비스에서 그룹 컨테이너 사용 가능을 선택해야 합니다.

▼ 그룹 컨테이너를 만들려면

1. 새 그룹 컨테이너를 포함할 조직의 위치 링크 또는 그룹 컨테이너를 선택합니다.
2. 그룹 컨테이너 탭을 선택합니다.
3. 그룹 컨테이너 목록에서 새로 만들기를 누릅니다.
4. 이름 필드에 값을 입력하고 확인을 누릅니다. 그룹 컨테이너 목록에 새 그룹 컨테이너가 표시됩니다.

▼ 그룹 컨테이너를 삭제하려면

1. 삭제할 그룹 컨테이너가 포함된 조직으로 이동합니다.
2. 그룹 컨테이너 탭을 선택합니다.
3. 삭제할 그룹 컨테이너 옆의 확인란을 선택합니다.
4. 삭제를 누릅니다.

그룹

그룹은 공통된 기능, 특징 또는 관심사를 가진 사용자 모음을 나타냅니다. 일반적으로 이 그룹에는 연관된 권한이 없습니다. 그룹은 두 가지 수준 즉, 조직 내에서와 다른 관리 대상 그룹 내에서 존재할 수 있습니다. 다른 그룹 내에서 존재하는 그룹을 하위 그룹이라고 부릅니다. 하위 그룹은 상위 그룹 내에서 "물리적으로" 존재하는 하위 노드입니다.

Access Manager는 또한 단일 그룹에 포함된 기존 그룹의 "표현"인 중첩 그룹을 지원합니다. 하위 그룹과 달리 중첩 그룹은 DIT 내의 어디에나 존재할 수 있습니다. 중첩 그룹은 다수의 사용자에 대한 액세스 권한을 신속하게 설정할 수 있게 합니다.

정적 그룹과 동적 그룹의 두 가지 유형의 그룹을 만들 수 있습니다. 사용자는 정적 그룹에만 수동으로 추가할 수 있습니다. 동적 그룹은 필터를 통해 사용자의 추가를 제어합니다. 중첩 또는 하위 그룹은 두 유형 모두에 추가될 수 있습니다.

정적 그룹

정적 그룹은 사용자가 지정한 관리 대상 그룹 유형을 기준으로 만들어집니다. `groupOfNames` 또는 `groupOfUniqueNames` 객체 클래스를 사용하여 그룹 항목에 그룹 구성원을 추가합니다.

주 – 기본적으로 관리 대상 그룹 유형은 동적입니다. 관리 서비스 구성에서 이 기본값을 변경할 수 있습니다.

동적 그룹

LDAP 필터를 사용하여 동적 그룹을 만듭니다. 모든 항목이 필터를 통해 걸러져 그룹에 동적으로 할당됩니다. 필터는 항목에서 속성을 검색하여 속성이 포함된 항목을 반환합니다. 예를 들어, 건물 번호를 기반으로 그룹을 만들 경우 필터를 사용하여 해당 건물 번호 속성을 포함하는 모든 사용자 목록을 반환할 수 있습니다.

주 – 참조 무결성 플러그 인을 사용하려면 Access Manager를 Directory Server와 함께 구성해야 합니다. 참조 무결성 플러그 인을 사용할 수 있는 경우에는 삭제 또는 이름 바꾸기 작업 직후 지정된 속성에 대해 무결성 업데이트가 이루어집니다. 이렇게 하면 관련된 항목들 간의 관계가 데이터베이스 전체를 통해 유지됩니다. 데이터베이스 색인을 사용하면 Directory Server의 검색 성능이 향상됩니다. 플러그인 활성화에 대한 자세한 내용은 **Sun Java System Access Manager 6 2005Q1 Migration Guide**를 참조하십시오.

▼ 정적 그룹을 만들려면

1. **새 그룹을 만들 조직, 그룹 또는 그룹 컨테이너로 이동합니다.**
2. **그룹 목록에서 새 정적을 누릅니다.**
3. **이름 필드에 그룹의 이름을 입력합니다. 다음을 누르십시오.**
4. **사용자가 이 그룹에 가입할 수 있음 속성을 선택하여 사용자가 그룹에 직접 가입할 수 있게 합니다.**
5. **확인을 누릅니다.**

   그룹이 만들어지면 그룹 이름을 선택하고 일반 탭을 눌러서 사용자가 이 그룹에 가입할 수 있음 속성을 편집할 수 있습니다.

▼ 정적 그룹에서 구성원을 추가 또는 제거하려면

1. **그룹 목록에서 구성원을 추가할 그룹을 선택합니다.**
2. **작업 선택 메뉴에서 수행할 작업을 선택합니다. 수행할 수 있는 작업은 다음과 같습니다.**

   새 사용자 — 이 작업은 새 사용자를 만들며 사용자 정보를 저장할 때 사용자를 그룹에 추가합니다.

사용자 추가 이 작업은 기존 사용자를 그룹에 추가합니다. 이 작업을 선택하면 추가할 사용자를 지정할 검색 기준을 만들 수 있습니다. 기준을 만드는 데 사용되는 필드는 ANY 또는 ALL 연산자를 사용합니다. ALL은 지정된 모든 필드에 해당하는 사용자를 반환합니다. ANY는 지정된 필드 중 하나 이상에 해당하는 사용자를 반환합니다. 필드를 비워두면 해당 특정 속성과 일치하는 가능한 모든 항목을 반환합니다.

검색 기준을 작성하고 나서 다음을 누릅니다. 반환된 사용자 목록에서 추가할 사용자를 선택하고 마침을 누릅니다.

그룹 추가 이 작업은 중첩 그룹을 현재 그룹에 추가합니다. 이 작업을 선택할 경우 검색 범위와 그룹 이름("*" 와일드카드 사용 가능)을 포함하는 검색 조건을 만들며 사용자가 그룹에 직접 가입할 수 있는지 여부를 지정할 수 있습니다. 정보를 입력하고 다음을 누릅니다. 반환된 그룹 목록에서 추가할 그룹을 선택하고 마침을 누릅니다.

구성원 제거 이 작업은 그룹에서 구성원(사용자 및 그룹 포함)을 제거하지만 삭제하지는 않습니다. 제거할 구성원을 선택하고 작업 선택 메뉴에서 구성원 제거를 선택합니다.

구성원 삭제 이 작업은 선택한 구성원을 영구적으로 삭제합니다. 삭제할 구성원을 선택한 다음 구성원 삭제를 선택합니다.

▼ 동적 그룹을 만들려면

1. **새 그룹을 만들 조직 또는 그룹으로 이동합니다.**
2. **그룹 탭을 누릅니다.**
3. **새 동적을 누릅니다.**
4. **이름 필드에 그룹의 이름을 입력합니다.**
5. **LDAP 검색 필터를 생성합니다.**

   기본적으로 Access Manager는 기본 검색 필터 인터페이스를 표시합니다. 필터를 생성하는 데 사용되는 기본 필드는 ANY 또는 ALL 연산자를 사용합니다. ALL은 지정된 모든 필드에 해당하는 사용자를 반환합니다. ANY는 지정된 필드 중 하나 이상에 해당하는 사용자를 반환합니다. 필드를 비워두면 해당 특정 속성과 일치하는 가능한 모든 항목을 반환합니다.
6. **확인을 누르면 검색 조건과 일치하는 모든 사용자가 자동으로 그룹에 추가됩니다.**

▼ 동적 그룹에서 구성원을 추가 또는 제거하려면

1 **그룹 목록에서 구성원을 추가할 그룹의 이름을 누릅니다.**

2 **작업 선택 메뉴에서 수행할 작업을 선택합니다. 수행할 수 있는 작업은 다음과 같습니다.**

그룹 추가 — 이 작업은 중첩 그룹을 현재 그룹에 추가합니다. 이 작업을 선택할 경우 검색 범위와 그룹 이름("*" 와일드카드 사용 가능)을 포함하는 검색 조건을 만들며 사용자가 그룹에 직접 가입할 수 있는지 여부를 지정할 수 있습니다. 정보를 입력하고 다음을 누릅니다. 반환된 그룹 목록에서 추가할 그룹을 선택하고 마침을 누릅니다.

구성원 제거 — 이 작업은 그룹에서 구성원(그룹 포함)을 제거하지만 삭제하지는 않습니다. 제거할 구성원을 선택한 다음 구성원 제거를 선택합니다.

구성원 삭제 — 이 작업은 선택한 구성원을 영구적으로 삭제합니다. 삭제할 구성원을 선택한 다음 구성원 삭제를 선택합니다.

정책에 그룹을 추가하려면

Access Manager 객체는 정책의 주제 정의를 통해 정책에 추가됩니다. 정책을 작성하거나 수정할 때 정책의 주제 페이지에서 조직, 역할, 그룹 및 사용자를 주제로 정의할 수 있습니다. 주제가 정의되고 나면 정책이 객체에 적용됩니다. 자세한 내용은 142 페이지 "정책 관리"를 참조하십시오.

사용자 컨테이너

사용자 컨테이너는 조직 내에서 사용자가 만들어질 때 모든 사용자가 할당되는 기본 LDAP 조직 구성 단위입니다. 사용자 컨테이너는 조직 수준에서 표시되거나 사용자 컨테이너 수준에서 하위 사용자 컨테이너로 표시될 수 있습니다. 사용자 컨테이너는 다른 사용자 컨테이너와 사용자만 포함할 수 있습니다. 원하는 경우 추가 사용자 컨테이너를 조직에 추가할 수 있습니다.

주 – 사용자 컨테이너의 표시는 선택 사항입니다. 사용자 컨테이너를 보려면 관리 서비스에서 사용자 컨테이너 사용 가능을 선택해야 합니다.

▼ 사용자 컨테이너 만들기

1 **새 사용자 컨테이너를 만들려는 조직이나 사용자 컨테이너로 이동합니다.**

2 **사용자 컨테이너 목록에서 새로 만들기를 누릅니다.**

3 **만들려는 사용자 컨테이너의 이름을 입력합니다.**

4 **확인을 누릅니다.**

▼ 사용자 컨테이너를 삭제하려면

1 **삭제할 사용자 컨테이너를 포함하는 조직이나 사용자 컨테이너로 이동합니다.**

2 **삭제할 사용자 컨테이너의 이름 옆에 있는 확인란을 선택합니다.**

3 **삭제를 누릅니다.**

주 – 사용자 컨테이너를 삭제하면 해당 사용자 컨테이너에 존재하는 모든 객체가 삭제됩니다. 여기에는 모든 사용자와 하위 사용자 컨테이너가 포함됩니다.

사용자

사용자는 개인의 아이디를 나타냅니다. Access Manager Identity 관리 모듈을 통해 사용자를 조직, 컨테이너 및 그룹에서 만들고 삭제할 수 있으며 역할 및/또는 그룹에서 추가 또는 제거할 수 있습니다. 사용자에게 서비스를 할당할 수도 있습니다.

주 – 하위 조직의 사용자가 `amadmin`과 동일한 사용자 아이디를 사용하여 생성될 경우 `amadmin`에 대한 로그인은 실패하게 됩니다. 이런 문제가 발생할 경우 관리자는 Directory Server 콘솔을 통해 사용자의 아이디를 변경해야 합니다. 이렇게 하면 관리자는 기본 조직에 로그인할 수 있습니다. 또한 인증 서비스에서 사용자 검색을 시작할 DN을 사용자 컨테이너 DN으로 설정하여 로그인 프로세스 도중 고유한 일치가 반환되도록 할 수 있습니다.

▼ 사용자를 만들려면

1 **사용자를 만들 조직, 컨테이너 또는 사용자 컨테이너로 이동합니다.**

2 **사용자 탭을 누릅니다.**

3 **사용자 목록에서 새로 만들기를 누릅니다.**

4 **다음 값에 대한 데이터를 입력합니다.**

사용자 아이디 — 이 필드에는 사용자가 Access Manager에 로그인할 때 사용하는 이름을 입력합니다. 이 등록 정보는 DN 값이 아닐 수 있습니다.

이름 — 이 필드는 사용자의 이름을 가집니다. 이름 값 및 성 값은 현재 로그인된 사용자 필드에서 사용자를 식별합니다. 이 값은 필수 값이 아닙니다.

성	이 필드에는 사용자의 성을 입력합니다. 이름 값 및 성 값은 사용자를 식별합니다.
전체 이름	이 필드에는 사용자의 성명을 입력합니다.
비밀번호	이 필드에는 사용자 아이디 필드에 지정된 이름의 비밀번호를 입력합니다.
비밀번호(확인)	비밀번호를 확인합니다.
사용자 상태	이 옵션은 사용자에게 Access Manager를 통한 인증이 허용되었는지 여부를 나타냅니다. 활성 사용자만 인증될 수 있습니다. 기본값은 **활성**입니다.

5 확인을 누릅니다.

▼ 사용자 프로필을 편집하려면

관리 역할이 할당되지 않은 사용자가 Access Manager에 대해 인증될 경우 기본 보기는 해당 사용자 프로필입니다. 또한 적절한 권한이 있는 관리자가 사용자 프로필을 편집할 수 있습니다. 이 보기에서 사용자는 개인 프로필 특정의 속성 값을 수정할 수 있습니다. 사용자 프로필 보기에 표시되는 속성은 확장할 수 있습니다. 객체 및 Identity에 대한 사용자 정의 속성 추가에 대한 자세한 내용은 Access Manager 개발자 설명서를 참조하십시오.

1 프로필을 편집할 사용자를 선택합니다. 기본적으로 일반 보기가 표시됩니다.

2 다음 필드를 편집합니다.

이름	이 필드는 사용자의 이름을 가집니다.
성	이 필드에는 사용자의 성을 입력합니다.
전체 이름	이 필드에는 사용자의 성명을 입력합니다.
비밀번호	사용자 비밀번호를 추가 및 확인하려면 편집 링크를 누릅니다.
전자 메일 주소	이 필드에는 사용자의 전자 메일 주소를 입력합니다.
사원 번호	이 필드에는 사용자의 사원 번호를 입력합니다.
전화 번호	이 필드에는 사용자의 전화 번호를 입력합니다.
집 주소	이 필드에는 사용자의 집 주소를 입력합니다.
사용자 상태	이 옵션은 사용자에게 Access Manager를 통한 인증이 허용되었는지 여부를 나타냅니다. 활성 사용자만 Access Manager를 통해 인증될 수 있습니다. 기본값은 활성입니다. 다음 중 하나를 풀다운 메뉴에서 선택할 수 있습니다. . ■ 활성 — 사용자가 Access Manager를 통해 인증될 수 있습니다. ■ 비활성 — 사용자가 Access Manager를 통해 인증될 수 없지만 사용자 프로필은 디렉토리에 저장된 채로 남습니다.

주 – 사용자 상태를 비활성으로 변경하는 것은 Access Manager를 통한 인증에만 영향을 줍니다. Directory Server는 *nsAccountLock* 속성을 사용하여 사용자 계정 상태를 결정합니다. Access Manager 인증에 대해 비활성화된 사용자 계정은 여전히 Access Manager가 필요하지 않은 작업을 수행할 수 있습니다. 단순히 Access Manager 인증에 대해서가 아니라 디렉토리에서 사용자 계정을 비활성화하려면 *nsAccountLock* 값을 false로 설정합니다. 사이트의 위임된 관리자가 정기적으로 사용자를 비활성화할 경우 *nsAccountLock* 속성을 Access Manager 사용자 프로필 페이지에 추가하는 방법을 고려하십시오. 자세한 내용은 **Sun Java System Access Manager 7 2005Q4 Developer's Guide**를 참조하십시오.

계정 만료 날짜	이 속성을 설정하면 현재 날짜와 시간이 지정된 계정 만료일을 지난 경우 인증 서비스는 로그인을 허용하지 않습니다. 이 속성의 형식은 *mm/dd/yyyy hh:mm*입니다.
사용자 인증 구성	이 속성은 사용자의 인증 체인을 설정합니다.
사용자 별칭 목록	이 필드는 사용자에게 적용될 수 있는 별칭 목록을 정의합니다. 이 속성에 구성된 별칭을 사용하려면 LDAP 서비스의 사용자 항목 검색 속성 필드에 `iplanet-am-user-alias-list` 속성을 추가하여 LDAP 서비스를 수정해야 합니다.
기본 로켈	이 필드는 사용자의 로켈을 지정합니다.
성공 URL	이 속성은 인증 성공 시 사용자가 리디렉션되는 URL을 지정합니다.
실패 URL	이 속성은 인증 실패 시 사용자가 리디렉션되는 URL을 지정합니다.
비밀번호 재설정 옵션	이 옵션은 잊어버린 비밀번호를 복구하는 데 사용되는 비밀번호 분실 페이지에서 질문을 선택하는 데 사용됩니다.
사용자 검색 자원 오퍼링	사용자에 대한 사용자 검색 서비스의 자원 오퍼링을 설정합니다.
MSIDSN 번호	MSISDN 인증을 사용 중인 경우 사용자의 MSISDN 번호를 정의합니다.

▼ 역할 및 그룹에 사용자를 추가하려면

1. **사용자 탭을 누릅니다.**
2. **수정할 사용자의 이름을 누릅니다.**

3 **역할 또는 그룹 탭을 선택합니다.**

4 **사용자를 추가할 역할이나 그룹을 선택하고 추가를 누릅니다.**

5 **저장을 누릅니다.**

주 – 역할이나 그룹에서 사용자를 제거하려면 역할 또는 그룹을 선택하고 제거를 누른 다음 저장을 누릅니다.

정책에 사용자를 추가하려면

Access Manager 객체는 정책의 주제 정의를 통해 정책에 추가됩니다. 정책을 작성하거나 수정할 때 정책의 주제 페이지에서 조직, 역할, 그룹 및 사용자를 주제로 정의할 수 있습니다. 주제가 정의되고 나면 정책이 객체에 적용됩니다. 자세한 내용은 142 페이지 “정책 관리”를 참조하십시오.

역할

역할은 그룹의 개념과 비슷한 Directory Server 항목 체계입니다. 그룹이 구성원을 가지므로 역할도 구성원을 가집니다. 역할의 구성원은 역할을 소유하는 LDAP 항목입니다. 역할의 기준 자체는 속성과 함께 LDAP 항목으로 정의되며 항목의 고유 이름(DN) 속성에 의해 식별됩니다. Directory Server에는 여러 가지 유형의 역할이 있지만 Access Manager는 그 중에서 관리 대상 역할만 관리할 수 있습니다.

주 – 다른 Directory Server 역할 유형은 Access Manager 콘솔에서 관리할 수는 없지만 디렉토리를 배포하는 데 사용할 수 있습니다. 정책의 주제 정의에 다른 Directory Server 유형을 사용할 수 있습니다. 정책 주제에 대한 자세한 내용은 139 페이지 “정책 만들기”를 참조하십시오.

사용자는 하나 이상의 역할을 소유할 수 있습니다. 예를 들어, 세션 서비스 및 비밀번호 재설정 서비스의 속성을 갖는 계약자 역할을 만들 수 있습니다. 새 계약직 직원이 회사에 합류하면 관리자는 계약자 항목에 개별 속성을 설정하는 대신 이 역할을 할당할 수 있습니다. 계약자가 엔지니어링 부서에서 일하며, 엔지니어링 직원이 사용할 수 있는 서비스와 액세스 권한을 요구하는 경우, 관리자는 계약자를 계약자 역할 외에 엔지니어링 역할에도 지정할 수 있습니다.

Access Manager는 역할을 사용하여 액세스 제어 명령을 적용합니다. 처음 설치되면 Access Manager는 관리자 사용 권한을 정의하는 액세스 제어 명령(ACI)을 구성합니다. 그런 다음 이러한 ACI는 사용자에게 할당될 때 사용자의 액세스 권한을 정의하는 역할(예: 조직 관리자 역할 및 조직 도움말 데스크 관리자 역할)에 지정됩니다.

사용자는 관리 서비스에서 사용자 프로필 페이지에 역할 표시 속성이 사용 가능하게 된 경우에만 할당된 역할을 볼 수 있습니다.

주 – 참조 무결성 플러그 인을 사용하려면 Access Manager를 Directory Server와 함께 구성해야 합니다. 참조 무결성 플러그 인을 사용할 수 있는 경우에는 삭제 또는 이름 바꾸기 작업 직후 지정된 속성에 대해 무결성 업데이트가 이루어집니다. 이렇게 하면 관련된 항목들 간의 관계가 데이터베이스 전체를 통해 유지됩니다. 데이터베이스 색인을 사용하면 Directory Server의 검색 성능이 향상됩니다. 플러그인 활성화에 대한 자세한 내용은 **Sun Java System Access Manager 6 2005Q1 Migration Guide**를 참조하십시오.

다음과 같은 두 가지 역할 유형이 있습니다.

- 정적 — 정적 역할은 역할을 만들 때 사용자 추가 없이 만듭니다. 역할이 만들어진 다음 해당 역할에 특정 사용자를 추가할 수 있습니다. 따라서 주어진 역할에 사용자를 추가할 때 더 많은 것을 제어할 수 있습니다.
- 동적 – 동적 역할은 LDAP 필터를 사용하여 만듭니다. 모든 사용자가 필터를 통해 걸러져 역할 작성 시 역할에 할당됩니다. 필터는 항목의 임의 속성 값 쌍(예: `ca=user*`)을 찾아 해당 속성을 포함하는 사용자를 역할에 자동으로 할당합니다.

▼ 정적 역할을 만들려면

1 역할을 만들 조직으로 이동합니다.

2 역할 탭을 누릅니다.

기본 역할 세트는 조직이 구성될 때 만들어지며 역할 목록에 표시됩니다. 기본 역할은 다음과 같습니다.

컨테이너 도움말 데스크 관리자.컨테이너 도움말 데스크 관리자 역할은 조직 구성 단위의 모든 항목에 대한 읽기 권한과 이 컨테이너 단위에 한하여 사용자 항목의 `userPassword` 속성에 대한 쓰기 권한을 가집니다.

조직 도움말 데스크 관리자.조직의 도움말 데스크 관리자는 조직의 모든 항목에 대한 읽기 권한과 `userPassword` 속성에 대한 쓰기 권한을 가집니다.

주 – 하위 조직을 만들 때 관리 역할이 상위 조직이 아닌 하위 조직에서 만들어진다는 점에 주의하십시오.

컨테이너 관리자.컨테이너 관리자 역할은 LDAP 조직 구성 단위의 모든 항목에 대한 읽기 및 쓰기 권한을 가집니다. Access Manager에서 LDAP 조직 구성 단위를 흔히 컨테이너라고 부릅니다.

조직 정책 관리자.조직 정책 관리자는 모든 정책에 대한 읽기 및 쓰기 권한을 가지며 해당 조직 내의 모든 정책을 작성, 할당, 수정 및 삭제할 수 있습니다.

사용자 관리자.기본적으로 새로 만든 조직의 모든 사용자 항목은 해당 조직에 속한 구성원입니다. 사용자 관리자는 조직의 모든 사용자 항목에 대한 읽기 및 쓰기 권한을 가집니다. 이 역할은 역할 및 그룹 DN을 포함하는 속성에 대한 읽기 및 쓰기 권한을 갖지 않으므로 역할 또는 그룹의 속성을 수정하거나 역할 또는 그룹에서 사용자를 제거할 수 없다는 점에 주의하십시오.

주 – Access Manager에서 다른 컨테이너를 구성하여 사용자 항목, 그룹 항목 또는 다른 컨테이너를 포함할 수 있습니다. 조직이 이미 구성된 후에 만든 컨테이너에 관리자 역할을 할당하면 컨테이너 관리자 역할 또는 컨테이너 도움말 데스크 관리자 기본값이 사용됩니다.

그룹 관리자.그룹이 만들어질 때 생성된 그룹 관리자는 특정 그룹의 모든 구성원에 대한 읽기 및 쓰기 권한을 가지며 새 사용자 작성, 관리하는 그룹에 사용자 할당, 작성한 그룹에서 사용자 삭제 등의 작업을 수행할 수 있습니다.

그룹이 만들어지면 해당 그룹을 관리하는 데 필요한 권한과 함께 그룹 관리자 역할이 자동으로 생성됩니다. 이 역할은 그룹 구성원에 자동으로 할당되지 않습니다. 따라서 그룹 작성자나 그룹 관리자 역할에 대한 액세스 권한을 가진 누군가가 이 역할을 할당해야 합니다.

최상위 수준 관리자.최상위 수준 관리자는 최상위 수준 조직의 모든 항목에 대한 읽기 및 쓰기 권한을 가집니다. 즉, 이 최상위 수준 관리자 역할은 Access Manager 응용 프로그램 내의 모든 구성 기본에 대한 권한을 가집니다.

조직 관리자.조직 관리자는 조직의 모든 항목에 대한 읽기 및 쓰기 권한을 가집니다. 조직이 만들어지면 해당 조직을 관리하는 데 필요한 권한과 함께 조직 관리자 역할이 자동으로 생성됩니다.

3 새 정적 버튼을 누릅니다.

4 역할의 이름을 입력합니다.

5 역할에 대한 설명을 입력합니다.

6 유형 메뉴에서 역할 유형을 선택합니다.

역할은 관리 역할 또는 서비스 역할이 될 수 있습니다. 역할 유형은 콘솔에서 사용자를 시작할 위치를 파악하기 위해 사용됩니다. 관리 역할은 역할 소유자가 관리 권한을 갖고 있다는 것을 콘솔에 알리고 서비스 역할은 역할 소유자가 최종 사용자라는 것을 콘솔에 알립니다.

7 액세스 권한 메뉴에서 역할에 적용할 기본 사용 권한 집합을 선택합니다. 이러한 사용 권한은 조직 내의 항목에 대한 액세스를 제공합니다. 기본 사용 권한은 특별한 순서 없이 표시됩니다. 다음과 같은 권한이 있습니다.

사용 권한 없음	역할에 사용 권한이 설정되지 않습니다.
조직 관리자	조직 관리자는 구성된 조직의 모든 항목에 대한 읽기 및 쓰기 권한을 가집니다.

조직 도움말 데스크 관리자	조직의 도움말 데스크 관리자는 구성된 조직의 모든 항목에 대한 읽기 권한과 userPassword 속성에 대한 쓰기 권한을 가집니다.
조직 정책 관리자	조직 정책 관리자는 조직의 모든 정책에 대한 읽기 및 쓰기 권한을 가집니다. 조직 정책 관리자는 피어 조직에 대한 참조 정책을 만들 수 없습니다. 일반적으로 서비스 역할에는 사용 권한 없음 ACI가 할당되고 관리 역할에는 임의의 기본 ACI가 할당됩니다.

▼ 정적 역할에 사용자를 추가하려면

1 사용자를 추가할 역할의 이름을 누릅니다.

2 구성원 목록의 작업 선택 메뉴에서 사용자 추가를 선택합니다.

3 검색 조건에 대한 정보를 입력합니다. 하나 이상의 표시된 필드에 기초하여 사용자를 검색할 수 있습니다. 이러한 필드는 다음과 같습니다.

일치	필터에 포함할 필드를 선택할 수 있습니다. ALL은 지정된 모든 필드에 해당하는 사용자를 반환합니다. ANY는 지정된 필드 중 하나 이상에 해당하는 사용자를 반환합니다.
이름	이름을 기준으로 사용자를 검색합니다.
사용자 아이디	사용자 아이디를 기준으로 사용자를 검색합니다.
성	성을 기준으로 사용자를 검색합니다.
전체 이름	성명을 기준으로 사용자를 검색합니다.
사용자 상태	상태(활성 또는 비활성)를 기준으로 사용자를 검색합니다.

4 다음을 눌러 검색을 시작합니다. 검색 결과가 표시됩니다.

5 아이디 옆에 있는 확인란을 선택하여 반환된 이름에서 사용자를 선택합니다.

6 마침을 누릅니다.

사용자가 이제 역할에 할당됩니다.

▼ 동적 역할을 만들려면

1 역할을 만들 조직으로 이동합니다.

2 역할 탭을 누릅니다.

기본 역할 세트는 조직이 구성될 때 만들어지며 역할 목록에 표시됩니다. 기본 역할은 다음과 같습니다.

컨테이너 도움말 데스크 관리자.컨테이너 도움말 데스크 관리자 역할은 조직 구성 단위의 모든 항목에 대한 읽기 권한과 이 컨테이너 단위에 한하여 사용자 항목의 `userPassword` 속성에 대한 쓰기 권한을 가집니다.

조직 도움말 데스크 관리자.조직의 도움말 데스크 관리자는 조직의 모든 항목에 대한 읽기 권한과 `userPassword` 속성에 대한 쓰기 권한을 가집니다.

주 – 하위 조직을 만들 때 관리 역할이 상위 조직이 아닌 하위 조직에서 만들어진다는 점에 주의하십시오.

컨테이너 관리자.컨테이너 관리자 역할은 LDAP 조직 구성 단위의 모든 항목에 대한 읽기 및 쓰기 권한을 가집니다. Access Manager에서 LDAP 조직 구성 단위를 흔히 컨테이너라고 부릅니다.

조직 정책 관리자.조직 정책 관리자는 모든 정책에 대한 읽기 및 쓰기 권한을 가지며 해당 조직 내의 모든 정책을 작성, 할당, 수정 및 삭제할 수 있습니다.

사용자 관리자.기본적으로 새로 만든 조직의 모든 사용자 항목은 해당 조직에 속한 구성원입니다. 사용자 관리자는 조직의 모든 사용자 항목에 대한 읽기 및 쓰기 권한을 가집니다. 이 역할은 역할 및 그룹 DN을 포함하는 속성에 대한 읽기 및 쓰기 권한을 갖지 않으므로 역할 또는 그룹의 속성을 수정하거나 역할 또는 그룹에서 사용자를 제거할 수 없다는 점에 주의하십시오.

주 – Access Manager에서 다른 컨테이너를 구성하여 사용자 항목, 그룹 항목 또는 다른 컨테이너를 포함할 수 있습니다. 조직이 이미 구성된 후에 만든 컨테이너에 관리자 역할을 할당하면 컨테이너 관리자 역할 또는 컨테이너 도움말 데스크 관리자 기본값이 사용됩니다.

그룹 관리자.그룹이 만들어질 때 생성된 그룹 관리자는 특정 그룹의 모든 구성원에 대한 읽기 및 쓰기 권한을 가지며 새 사용자 작성, 관리하는 그룹에 사용자 할당, 작성한 그룹에서 사용자 삭제 등의 작업을 수행할 수 있습니다.

그룹이 만들어지면 해당 그룹을 관리하는 데 필요한 권한과 함께 그룹 관리자 역할이 자동으로 생성됩니다. 이 역할은 그룹 구성원에 자동으로 할당되지 않습니다. 따라서 그룹 작성자나 그룹 관리자 역할에 대한 액세스 권한을 가진 누군가가 이 역할을 할당해야 합니다.

최상위 수준 관리자.최상위 수준 관리자는 최상위 수준 조직의 모든 항목에 대한 읽기 및 쓰기 권한을 가집니다. 즉, 이 최상위 수준 관리자 역할은 Access Manager 응용 프로그램 내의 모든 구성 기본에 대한 권한을 가집니다.

조직 관리자.조직 관리자는 조직의 모든 항목에 대한 읽기 및 쓰기 권한을 가집니다. 조직이 만들어지면 해당 조직을 관리하는 데 필요한 권한과 함께 조직 관리자 역할이 자동으로 생성됩니다.

3 새 동적 버튼을 누릅니다.

4 역할의 이름을 입력합니다.

5 역할에 대한 설명을 입력합니다.

6 유형 메뉴에서 역할 유형을 선택합니다.

역할은 관리 역할 또는 서비스 역할이 될 수 있습니다. 역할 유형은 콘솔에서 사용자를 시작할 위치를 파악하기 위해 사용됩니다. 관리 역할은 역할 소유자가 관리 권한을 갖고 있다는 것을 콘솔에 알리고 서비스 역할은 역할 소유자가 최종 사용자라는 것을 콘솔에 알립니다.

7 액세스 권한 메뉴에서 역할에 적용할 기본 사용 권한 집합을 선택합니다. 이러한 사용 권한은 조직 내의 항목에 대한 액세스를 제공합니다. 기본 사용 권한은 특별한 순서 없이 표시됩니다. 다음과 같은 권한이 있습니다.

사용 권한 없음	역할에 사용 권한이 설정되지 않습니다.
조직 관리자	조직 관리자는 구성된 조직의 모든 항목에 대한 읽기 및 쓰기 권한을 가집니다.
조직 도움말 데스크 관리자	조직의 도움말 데스크 관리자는 구성된 조직의 모든 항목에 대한 읽기 권한과 `userPassword` 속성에 대한 쓰기 권한을 가집니다.
조직 정책 관리자	조직 정책 관리자는 조직의 모든 정책에 대한 읽기 및 쓰기 권한을 가집니다. 조직 정책 관리자는 피어 조직에 대한 참조 정책을 만들 수 없습니다. 일반적으로 서비스 역할에는 사용 권한 없음 ACI가 할당되고 관리 역할에는 임의의 기본 ACI가 할당됩니다.

8 검색 조건에 대한 정보를 입력합니다. 필드는 다음과 같습니다.

일치	필터에 포함할 임의의 필드에 대한 연산자를 포함할 수 있습니다. `ALL`은 지정된 모든 필드에 해당하는 사용자를 반환합니다. `ANY`는 지정된 필드 중 하나 이상에 해당하는 사용자를 반환합니다.
이름	이름을 기준으로 사용자를 검색합니다.
사용자 아이디	사용자 아이디를 기준으로 사용자를 검색합니다.
성	성을 기준으로 사용자를 검색합니다.
전체 이름	성명을 기준으로 사용자를 검색합니다.
사용자 상태	상태(활성 또는 비활성)를 기준으로 사용자를 검색합니다.

9 **확인을 눌러 필터 조건에 기초한 검색을 시작합니다. 필터 조건에서 정의된 사용자가 자동으로 역할에 할당됩니다.**

▼ 역할에서 사용자를 제거하려면

1 **수정할 역할을 포함하는 조직으로 이동합니다.**
Identity 관리 모듈의 보기 메뉴에서 조직을 선택하고 역할 탭을 선택합니다.

2 **수정할 역할을 선택합니다.**

3 **보기 메뉴에서 사용자를 선택합니다.**

4 **제거할 각 사용자 옆에 있는 확인란을 선택합니다.**

5 **작업 선택 메뉴에서 사용자 제거를 누릅니다.**
사용자가 이제 역할에서 제거됩니다.

정책에 역할을 추가하려면

Access Manager 객체는 정책의 주제 정의를 통해 정책에 추가됩니다. 정책을 작성하거나 수정할 때 정책의 주제 페이지에서 조직, 역할, 그룹 및 사용자를 주제로 정의할 수 있습니다. 주제가 정의되고 나면 정책이 객체에 적용됩니다. 자세한 내용은 142 페이지 “정책 관리”를 참조하십시오.

◆ ◆ ◆ 11 장

11 현재 세션

이 장에서는 Access Manager의 세션 관리 기능에 대해 설명합니다. 세션 관리 모듈은 사용자 세션 정보 확인 및 사용자 세션 관리를 위한 솔루션을 제공합니다. 세션 관리 모듈은 다양한 세션 시간을 추적하고 관리자가 세션을 종료할 수 있도록 허용합니다. 시스템 관리자는 플랫폼 서버 목록에 있는 로드 밸런서 서버를 무시해야 합니다.

현재 세션 인터페이스

현재 세션 모듈 인터페이스를 사용하면 적절한 사용 권한이 있는 관리자가 현재 Access Manager에 로그인한 사용자의 세션 정보를 볼 수 있습니다.

세션 관리

세션 관리 프레임은 현재 관리되고 있는 Access Manager의 이름을 표시합니다.

세션 정보

세션 정보 창은 현재 Access Manager에 로그인한 모든 사용자 및 각 사용자의 세션 시간을 표시합니다. 표시 필드는 다음과 같습니다.

사용자 아이디.현재 로그인한 사용자의 사용자 아이디를 표시합니다.

남은 시간.세션에 대해 사용자가 재인증을 수행해야 하기 전까지 남은 시간(분)을 표시합니다.

최대 세션 시간.세션이 만료되고 액세스 권한을 다시 얻기 위해 재인증을 수행해야 하기 전까지 사용자가 로그인할 수 있는 최대 시간(분)을 표시합니다.

유휴 시간. 사용자가 유휴 상태인 시간(분)을 표시합니다

최대 유휴 시간.사용자가 재인증을 수행해야 하기 전까기 유휴 상태로 있을 수 있는 최대 시간(분)을 표시합니다.

시간 제한은 관리자가 세션 관리 서비스에서 정의합니다.

사용자 아이디 필드에 문자열을 입력하고 필터를 눌러 특정 사용자 세션이나 사용자 세션의 특정 범위를 표시할 수 있습니다. 와일드카드를 사용할 수 있습니다.

업데이트 버튼을 누르면 사용자 세션 표시가 업데이트됩니다.

세션 종료

적절한 사용 권한을 가진 관리자는 언제든지 사용자 세션을 종료할 수 있습니다.

▼ 세션을 종료하려면

1. **종료하려는 사용자 세션을 선택합니다.**
2. **종료를 누릅니다.**

◆ ◆ ◆ 12 장

12 비밀번호 재설정 서비스

Access Manager는 사용자가 Access Manager로 보호되는 지정된 서비스 또는 응용 프로그램에 액세스하기 위한 비밀번호를 재설정할 수 있게 해주는 비밀번호 재설정 서비스를 제공합니다. 비밀번호 재설정 서비스 속성은 최상위 관리자가 정의하고, 비밀번호 질문 형태로 사용자 검증 자격 증명을 제어하며 새로운 또는 기존 비밀번호 알림 기법을 제어합니다. 그리고 잘못된 사용자 검증에 대한 가능한 잠금 간격을 설정합니다.

이 장은 다음 내용으로 구성되어 있습니다.

비밀번호 재설정 서비스 등록

사용자가 소속된 영역에 대해서는 비밀번호 재설정 서비스를 등록할 필요가 없습니다. 사용자가 위치한 조직에 비밀번호 재설정 서비스가 없는 경우 서비스 구성에서 해당 서비스에 대해 정의된 값을 상속합니다.

▼ 다른 영역의 사용자에 대해 비밀번호 재설정을 등록하려면

1. **사용자에 대한 비밀번호를 등록하려는 영역으로 이동합니다.**

2. **영역 이름을 누르고 서비스 탭을 누릅니다.**
   서비스가 아직 영역에 추가되지 않은 경우 추가 버튼을 누릅니다.

3. **비밀번호 재설정을 선택하고 다음을 누릅니다.**
   비밀번호 재설정 서비스 속성이 표시됩니다. 속성 정의는 온라인 도움말을 참조하십시오.

4 **마침을 누릅니다.**

비밀번호 재설정 서비스 구성

비밀번호 재설정 서비스가 등록되어 있는 경우 관리자 권한이 있는 사용자가 서비스를 구성해야 합니다.

▼ 서비스를 구성하려면

1 **비밀번호 재설정 서비스를 등록할 영역을 선택합니다.**

2 **서비스 탭을 누릅니다.**

3 **서비스 목록에서 비밀번호 재설정을 누릅니다.**

4 **비밀번호 재설정 속성이 표시되고 사용자는 이 속성을 사용하여 비밀번호 재설정 서비스에 대한 요구 사항을 정의할 수 있습니다. 비밀번호 재설정 서비스가 사용 가능(기본값)한지 확인합니다. 최소한 다음 속성을 정의해야 합니다.**

- 사용자 검증
  - 비밀번호 질문
  - 바인드 DN
  - 바인드 비밀번호

    바인드 DN 속성은 비밀번호 재설정 권한이 있는 사용자(예: 도움말 데스크 관리자)를 포함해야 합니다. Directory Server의 제한 때문에 바인드 DN이 `cn=Directory Manager`인 경우에는 비밀번호 재설정이 실행되지 않습니다.

    나머지 속성은 선택 사항입니다. 서비스 속성에 대한 설명은 온라인 도움말을 참조하십시오.

주 – Access Manager는 임의의 비밀번호 생성을 위한 비밀번호 재설정 웹 응용 프로그램을 자동으로 설치합니다. 그러나 비밀번호 생성 및 비밀번호 알림을 위한 사용자 플러그인 클래스를 작성할 수 있습니다. 이러한 플러그인 클래스에 대해서는 다음 위치에 있는 다음 Readme.html 파일을 참조하십시오.

PasswordGenerator:

```
AccessManager-base/SUNWam/samples/console/PasswordGenerator
```

NotifyPassword:

```
AccessManager-base/SUNWam/samples/console/NotifyPassword
```

5 사용자가 고유 개인 문제를 직접 정의해야 하는 경우 개인 문제 사용 가능 속성을 선택합니다. 속성을 정의한 다음 저장을 누릅니다.

비밀번호 재설정 잠금

비밀번호 재설정 서비스에는 사용자가 비밀번호 질문에 올바르게 응답하기 위해 시도할 수 있는 횟수를 제한하는 잠금 기능이 포함됩니다. 잠금 기능은 비밀번호 재설정 서비스 속성을 통해 구성됩니다. 서비스 속성에 대한 설명은 온라인 도움말을 참조하십시오. 비밀번호 재설정은 메모리 잠금과 물리적 잠금이라는 두 가지 유형의 잠금을 지원합니다.

메모리 잠금

이 잠금은 임시 잠금이며 비밀번호 재설정 실패 잠금 기간 속성의 값이 0보다 크고 비밀번호 재설정 실패 잠금 사용 가능 속성이 활성화된 경우에만 유효합니다. 이 잠금은 사용자가 비밀번호 재설정 웹 응용 프로그램을 통해 비밀번호를 재설정하지 못하게 합니다. 잠금은 비밀번호 재설정 실패 잠금 기간에 지정된 기간동안 지속되거나 서버가 다시 시작될 때까지 지속됩니다. 서비스 속성에 대한 설명은 온라인 도움말을 참조하십시오.

물리적 잠금

보다 영구적인 잠금입니다. 비밀번호 재설정 실패 잠금 횟수 속성 값을 0으로 설정하고 비밀번호 재설정 실패 잠금 사용 가능 속성을 활성화하면 사용자가 비밀번호 질문에 잘못 대답할 경우 해당 사용자의 계정 상태가 비활성 상태로 변경됩니다. 서비스 속성에 대한 설명은 온라인 도움말을 참조하십시오.

최종 사용자에 대한 비밀번호 재설정

다음 절에서는 비밀번호 재설정 서비스에 대한 사용자 경험을 설명합니다.

비밀번호 재설정 사용자 정의

비밀번호 재설정 서비스가 사용 가능하고 관리자가 속성을 정의한 경우 사용자는 콘솔에 로그인하여 비밀번호 질문을 사용자 정의할 수 있습니다.

▼ 비밀번호 재설정을 사용자 정의하려면

1. **사용자가 아이디와 비밀번호를 제공하여 Access Manager 콘솔에 로그인하면 성공적으로 인증됩니다.**
2. **사용자 프로필 페이지에서 비밀번호 재설정 옵션을 선택합니다. 사용 가능한 문제 응답 화면이 표시됩니다.**
3. **관리자가 해당 서비스에 대해 정의한 사용 가능한 질문이 표시됩니다. 예를 들면 다음과 같습니다.**
   - 애완동물 이름은?
     - 가장 좋아하는 TV 쇼는?
     - 어머니의 성함은?
     - 자주가는 식당은?
4. **비밀번호 질문을 선택합니다. 비밀번호 질문은 관리자가 영역에 대해 정의한 최대 문제 수 이하로 선택할 수 있습니다(최대 양은 비밀번호 재설정 서비스를 통해 정의됨). 그런 다음 선택한 문제에 대한 대답을 입력합니다. 이러한 문제와 대답은 사용자의 비밀번호 재설정을 위한 기초가 됩니다(다음 절 참조). 관리자가 개인 문제 사용 가능 속성을 선택한 경우 사용자가 고유한 비밀번호 질문을 입력하고 대답을 제공할 수 있는 텍스트 필드가 제공됩니다.**
5. **저장을 누릅니다.**

잊어버린 비밀번호 재설정

사용자가 비밀번호를 잊어버린 경우는 비밀번호 재설정 웹 응용 프로그램을 사용하여 새 비밀번호를 임의로 생성하여 사용자에게 새 비밀번호를 알려줍니다. 다음은 일반적인 잊어버린 비밀번호 시나리오입니다.

▼ 잊어버린 비밀번호를 재설정하려면

1 관리자가 지정해준 URL에서 비밀번호 재설정 웹 응용 프로그램에 로그인합니다. 예를 들면 다음과 같습니다.

`http://hostname:port/ampassword`(기본 영역용)

또는

`http://hostname: port/`*deploy_uri*`/UI/PWResetUserValidation?realm=realmname`(realmname은 영역의 이름)

주 – 비밀번호 재설정 서비스가 상위 영역에 대해서는 사용 가능으로 설정되어 있지 않고 하위 영역에 대해서는 사용 가능으로 설정되어 있는 경우 사용자가 서비스에 액세스하려면 다음 구문을 사용해야 합니다.

`http://hostname: port/`*deploy_uri*`/UI/PWResetUserValidation?realm=realmname`

---

2 사용자 아이디를 입력합니다.

3 비밀번호 재설정 서비스에서 정의하고 사용자 정의 과정에서 사용자가 선택한 개인 문제가 표시됩니다. 사용자 프로필 페이지에 로그인하지 않고 개인 문제를 사용자 정의한 경우 비밀번호가 생성되지 않습니다.

사용자가 문제에 올바르게 대답하면 새 비밀번호를 생성하여 전자 메일로 사용자에게 알려줍니다. 문제에 올바르게 대답했는지 여부에 관계없이 사용자에게 시도 알림을 보냅니다. 새 비밀번호와 시도 알림을 받으려면 사용자 프로필 페이지에 전자 메일 주소를 입력해야 합니다.

비밀번호 정책

보안 비밀번호 정책은 다음을 적용하여 비밀번호를 쉽게 추측할 수 있는 위험을 최소화합니다.

- 일정에 따라 비밀번호를 변경해야 합니다.
- 쉽게 추정할 수 없는 비밀번호를 지정해야 합니다.
- 잘못된 비밀번호로 여러 번 바인드하면 계정이 잠길 수 있습니다.

Directory Server에서는 트리의 노드에서 여러 가지 방법으로 비밀번호 정책을 설정할 수 있으며 여러 가지 정책 설정 방법을 제공합니다. 자세한 내용은 다음 Directory Server 설명서를 참조하십시오.

http://docs.sun.com/source/816-6700-10/aci.html#14773

http://docs.sun.com/source/816-6698-10/useracct.html#14386

◆ ◆ ◆ 13장

13 로깅 서비스

Sun Java™ System Access Manager 7 2005Q4는 사용자 작업, 트래픽 패턴 및 인증 위반과 같은 정보를 기록하기 위한 로깅 서비스를 제공합니다. 또한 관리자는 디버그 파일을 사용하여 설치 문제를 해결할 수 있습니다.

로그 파일

로그 파일은 모니터링하는 각 서비스에 대한 여러 가지 이벤트를 기록합니다. 관리자는 이 파일을 정기적으로 확인해야 합니다. 로그 파일의 기본 디렉토리는 SPARC 시스템의 경우 `/var/opt/SUNWam/logs`이며 Linux 시스템의 경우 `/var/opt/sun/identity`입니다. 로그 파일 디렉토리는 Access Manager 콘솔을 사용하여 로깅 서비스에서 구성할 수 있습니다.

Sun Java System Access Manager 7 2005Q4 Technical Overview의 "How the Logging Feature Works"에 있는 "How the Logging Feature Works"를 참조하십시오.

로깅 서비스에 대한 속성 정의는 Access Manager 콘솔에 있는 도움말 버튼을 눌러 온라인 도움말을 참조하십시오.

Access Manager 서비스 로그

서비스 로그 파일에는 액세스 로그 파일과 오류 로그 파일의 두 가지유형이 있습니다. 액세스 로그 파일에는 작업 시도와 성공적인 결과에 대한 기록이 포함됩니다. 오류 로그 파일은 Access Manager 서비스 내에서 발생한 오류를 기록합니다. 플랫 로그 파일에는 `.error` 또는 `.access` 확장자가 붙습니다. 데이터베이스 열 이름은 Oracle 데이터베이스의 경우 `_ERROR` 또는 `_ACCESS`로 끝나고 MySQL 데이터베이스는 `_error` 또는 `_access`로 끝납니다. 예를 들어 콘솔 이벤트를 기록하는 플랫 파일의 이름은 `amConsole.access`로, 같은 이벤트를 기록하는 데이터베이스 열의 이름은 `AMCONSOLE_ACCESS`로 지정됩니다. 다음 절에서는 로깅 서비스에서 기록하는 로그 파일에 대해 설명합니다.

세션 로그

로깅 서비스는 세션 서비스에 대해 다음 이벤트를 기록합니다.

- 로그인
- 로그아웃
- 세션 유휴 시간 초과
- 세션 최대 시간 초과
- 로그인 실패
- 세션 재활성화
- 세션 소멸

세션 로그에는 `amSSO` 접두어가 붙습니다.

콘솔 로그

Access Manager 콘솔 로그는 조직, 조직 구성 단위, 사용자, 역할, 정책 및 그룹 등을 포함한 Identity 관련 객체, 정책 및 서비스의 생성, 삭제 및 수정을 기록합니다. 또한 비밀번호를 포함한 사용자 속성 수정, 역할 및 그룹에서의 사용자 추가 및 제거를 기록합니다. 이외에도 콘솔 로그는 위임 및 데이터 저장소 작업을 기록합니다. 콘솔 로그에는 `amConsole` 접두어가 붙습니다.

인증 로그

인증 구성 요소는 사용자 로그인과 로그아웃을 기록합니다. 인증 로그에는 `amAuthentication` 접두어가 붙습니다.

연합 로그

연합 구성 요소는 인증 도메인 생성 및 호스트 공급자 생성을 포함하나 이에 제한되지 않은 연합 관련 이벤트를 기록합니다. 연합 로그에는 `amFederation` 접두어가 붙습니다.

정책 로그

정책 구성 요소는 정책 관리(정책 생성, 삭제 및 수정) 및 정책 평가를 포함하나 이에 제한되지 않은 정책 관련 이벤트를 기록합니다. 정책 로그에는 `amPolicy` 접두어가 붙습니다.

에이전트 로그

정책 에이전트 로그는 사용자에게 허용 또는 거부된 로그 자원에 관한 로깅 예외 기록을 담당합니다. 에이전트 로그에는 `amAgent` 접두어가 붙습니다. `amAgent` 로그는 에이전트 서버에만 있습니다. 에이전트 이벤트는 Access Manager 서버에서 인증 로그에 기록됩니다. 이 기능에 대한 자세한 내용은 대상 정책 에이전트에 대한 설명서를 참조하십시오.

SAML 로그

SAML 구성 요소는 명제 및 아티팩트 생성 또는 제거, 응답 및 요청 정보, SOAP 오류를 포함하나 이에 제한되지 않은 SAML 관련 이벤트를 기록합니다. 세션 로그에는 amSAML 접두어가 붙습니다.

amAdmin 로그

명령줄 로그는 명령줄 도구를 사용한 작업 중에 발생한 이벤트 오류를 기록합니다. 이러한 이벤트에는 서비스 스키마 로드, 정책 생성 및 사용자 삭제 등이 포함됩니다(이에 제한되지 않음). 명령줄 로그에는 amAdmin 접두어가 붙습니다.

로깅 기능

로깅 서비스에는 추가 기능을 사용할 수 있도록 해주는 여러 가지의 특수 기능이 있습니다. 이러한 기능에는 보안 로깅 사용, 명령줄 로깅 및 원격 로깅이 포함됩니다.

보안 로깅

로깅 기능에 추가 보안 수단을 적용합니다(선택 사항). 보안 로깅은 보안 로그의 인증되지 않은 변경이나 손상을 감지할 수 있게 합니다. 이 기능을 사용하기 위해 특별한 코딩이 필요하지는 않습니다. 보안 로깅은 시스템 관리자가 구성한 미리 등록된 인증서를 사용하여 수행됩니다. 이러한 MAC(Manifest Analysis and Certification)는 모든 로그 레코드에 대해 생성 및 저장됩니다. 특수 '서명' 로그 레코드가 정기적으로 삽입되어 해당 지점에 기록된 로그의 내용에 대한 서명을 나타냅니다. 두 레코드의 조합으로 로그가 손상되지 않았음을 확인할 수 있습니다.

▼ 보안 로깅을 사용 가능하게 하려면

1. **이름이 Logger인 인증서를 만들어 Access Manager를 실행 중인 배포 컨테이너에 설치합니다. 자세한 내용은 배포 컨테이너에 대한 설명서를 참조하십시오.**

2. **Access Manager 콘솔을 사용하여 로깅 서비스 구성에서 보안 로깅을 활성화하고 변경 내용을 저장합니다. 관리자는 로깅 서비스의 다른 속성에 대한 기본값도 수정할 수 있습니다.**

   로깅 디렉토리가 기본 디렉토리(/var/opt/SUMWam/logs)에서 변경된 경우 권한이 0700으로 설정되었는지 확인하십시오. 로깅 서비스는 디렉토리가 없으면 만들지만 권한이 0755로 설정된 디렉토리를 생성하게 됩니다.

   또한 기본값에서 다른 디렉토리를 지정하는 경우 웹 컨테이너의 server.policy 파일에 있는 다음 매개 변수를 새 디렉토리로 변경해야 합니다.

   ```
   permission java.io.FilePermission “/var/opt/SUNWam/logs/*”,”delete,write”
   ```

3 *AccessManager-base*/SUNWam/config **디렉토리에 인증서 데이터베이스 비밀번호를 포함한 파일을 만들고 이름을** .wtpass**로 지정합니다.**

주 – 파일 이름 및 이 파일에 대한 경로는 AMConfig.properties 파일에서 구성할 수 있습니다. 자세한 내용은 부록 A의 "인증서 데이터베이스"를 참조하십시오.

보안을 위해 배포 컨테이너 사용자가 이 파일에 대한 읽기 권한을 가진 유일한 관리자임을 확인합니다.

---

4 **서버를 다시 시작합니다.**

보안 로깅 시작 시에 /var/opt/SUNWam/debug/amLog 파일에 잘못된 확인 오류가 기록될 수 있으므로 보안 로그 디렉토리를 지워야 합니다.

보안 로그의 허용되지 않은 변경 및 손상을 검색하려면 확인 프로세스에 의해 /var/opt/SUNWam/debug/amLog에 잘못 기록된 오류 메시지를 검색합니다. 손상을 수동으로 확인하려면 VerifyArchive 유틸리티를 실행합니다. 자세한 내용은 19 장을 참조하십시오.

명령줄 로깅

amadmin 명령줄 도구를 사용해 Directory Server에서 Identity 객체(예: 조직, 사용자 및 역할)를 생성, 수정 및 삭제할 수 있습니다. 이 도구는 또한 서비스 템플리트를 로드, 생성 및 등록할 수 있습니다. 로깅 서비스는 -t 옵션을 호출하여 이러한 작업을 기록할 수 있습니다. AMConfig.properties의 com.iplanet.am.logstatus 등록 정보가 활성(ACTIVE)이면 로그 레코드가 생성됩니다. 이 등록 정보는 기본적으로 사용 가능합니다. 명령줄 로그에는 amAdmin 접두어가 붙습니다. 자세한 내용은 14 장를 참조하십시오.

로깅 등록 정보

AMConfig.properties 파일에는 로깅 출력에 영향을 주는 다음과 같은 등록 정보가 있습니다.

com.iplanet.am.logstatus=ACTIVE	이 등록 정보는 로깅을 활성 또는 비활성화합니다. 기본값은 ACTIVE입니다.
iplanet-am-logging.*service*.level= *level*	*service*는 서비스의 일반 디버그 파일 이름입니다. *level*은 java.util.logging.Level 값 중 하나이며 로그에 자세히 기록된 수준을 나타냅니다. 수준은 SEVERE, WARNING, INFO, CONFIG, FINE, FINER 및 FINEST가 있습니다. 대부분의 서비스는 INFO 이하의 정보 수준으로 로그를 기록합니다.

원격 로깅

Access Manager는 원격 로깅을 지원합니다. 따라서 클라이언트 응용 프로그램은 Access Manager SDK가 설치된 호스트를 사용하여 원격 시스템에 배포된 Access Manager 인스턴스에 로그 레코드를 생성할 수 있습니다. 원격 로깅은 다음 중 하나의 시나리오에 의해 시작됩니다.

1. Access Manager 인스턴스의 이름 지정 서비스에 있는 로깅 URL이 원격 인스턴스를 가리키고 이 둘 사이에 신뢰 관계가 구성되어 있는 경우 원격 Access Manager 인스턴스에 로그가 기록됩니다.
2. Access Manager SDK가 원격 Access Manager 인스턴스에 대해 설치되어 있고 클라이언트(또는 단순 Java 클래스)가 로깅 API를 사용하는 SDK 서버에서 실행 중이면 원격 Access Manager 시스템에 로그가 기록됩니다.
3. Access Manager 에이전트가 로깅 API를 사용하는 경우.

▼ 원격 로깅을 사용 가능하게 하려면

1 Sun Java System Web Server를 사용하는 경우 `server.xml` 구성 파일에서 다음 환경 변수를 설정해야 합니다.

- `java.util.logging.manager=com.sun.identity.log.LogManager`
- `java.util.logging.config.file=/` *AccessManager-base* `/SUNwam/lib/LogConfig.properties`
- 사용 중인 Java™ 2 Platform, Standard Edition이 1.4 이상이면 명령줄에서 다음을 호출하여 수행합니다.

  `java -cp /`*AccessManager-base* `/SUNWam/lib/am_logging.jar:/` *AccessManager-base* `/SUNWam/lib/xercesImpl.jar:/` *AccessManager-base* `/SUNWam/lib/xmlParserAPIs.jar:/` *AccessManager-base* `/SUNWam/lib/jaas.jar:/` *AccessManager-base* `/SUNWam/lib/xmlParserAPIs.jar:/` *AccessManager-base* `/SUNWam/lib/servlet.jar:/` *AccessManager-base* `/SUNWam/locale:/` *AccessManager-base*`/SUNWam/lib/am_services.jar:/` *AccessManager-base*`/SUNWam/lib/am_sdk.jar:/` *AccessManager-base*`/SUNWam/lib/jss311.jar:/` *AccessManager-base*`/SUNWam/lib:.`

  `-Djava.util.logging.manager=com.sun.identity.log.LogManager`

  `-Djava.util.logging.config.file=/` *AccessManager-base* `/SUNwam/lib/LogConfig.properties <logTestClass>`

- 사용 중인 Java 2 Platform, Standard Edition이 1.4 이전 버전이면 명령줄에서 다음을 호출하여 수행합니다.

  `java -Xbootclasspath/a:/`*AccessManager-base* `/SUNWam/lib/jdk_logging.jar -cp /` *AccessManager-base* `/SUNWam/lib/am_logging.jar:/` *AccessManager-base* `/SUNWam/lib/xercesImpl.jar:/` *AccessManager-base* `/SUNWam/lib/xmlParserAPIs.jar:/` *AccessManager-base* `/SUNWam/lib/jaas.jar:/` *AccessManager-base* `/SUNWam/lib/xmlParserAPIs.jar:/` *AccessManager-base* `/SUNWam/lib/servlet.jar:/`

AccessManager-base /SUNWam/locale:/
AccessManager-base/SUNWam/lib/am_services.jar:/
AccessManager-base/SUNWam/lib/am_sdk.jar:/
AccessManager-base/SUNWam/lib/jss311.jar:/ *AccessManager-base*/SUNWam/lib:.

-Djava.util.logging.manager=com.sun.identity.log.LogManager

-Djava.util.logging.config.file=/ *AccessManager-base*
/SUNwam/lib/LogConfig.properties <logTestClass>

2 *AccessManager-base*/SUNWam/lib**에 있는** LogConfig.properties**에 다음 매개 변수가 구성되어 있는지 확인합니다.**

- iplanet-am-logging-remote-handler=com.sun.identity.

  log.handlers.RemoteHandler

- iplanet-am-logging-remote-formatter=com.sun.

  identity.log.handlers.RemoteFormatter

- iplanet-am-logging-remote-buffer-size=1

  원격 로깅은 로그 레코드 수를 기반으로 버퍼링을 지원합니다. 이 값은 레코드의 수에 따라 로그 버퍼 크기를 정의합니다. 버퍼가 꽉 차면 버퍼링된 레코드는 모두 서버로 플러시됩니다.

- iplanet-am-logging-buffer-time-in-seconds=3600

  이 값은 로그 버퍼 클리너 스레드를 호출하는 시간 제한 기간을 정의합니다.

- iplanet-am-logging-time-buffering-status=OFF

  이 값은 로그 버퍼링 및 버퍼 클리너 스레드의 사용 가능 여부를 정의합니다. 기본적으로 이 기능은 비활성화되어 있습니다.

주 – 로그 파일이 비어 있으면 보안 로깅에 "확인 실패" 메시지가 표시될 수 있습니다. 이는 생성된 파일의 수가 아카이브 크기와 같기 때문이며, 이 경우 보안 로깅은 이 세트부터 아카이브한 다음 다시 시작합니다. 대부분의 인스턴스에서는 이 오류를 무시해도 됩니다. 레코드 수가 아카이브 크기와 같으면 오류가 표시되지 않습니다.

오류 및 액세스 로그

Access Manager 로그 파일에는액세스 로그 파일 및 오류 로그 파일의 두 가지 유형이 있습니다.

액세스 로그 파일은 Access Manager 배포와 관련된 일반 감사 정보를 기록합니다. 로그에는 인증 성공과 같은 이벤트에 대한 단일 레코드가 포함될 수 있습니다. 로그에는 동일한 이벤트에 대해 여러 레코드가 포함될 수 있습니다. 예를 들어 관리자가 콘솔을 사용하여 속성

값을 변경하면 로깅 서비스에서 하나의 레코드에 변경 시도를 기록합니다. 또한 로깅 서비스는 두 번째 레코드에 변경의 실행 결과를 기록합니다.

오류 로그 파일은 응용 프로그램 내에서 발생한 오류를 기록합니다. 작업 오류는 오류 로그에 기록되고, 작업 시도는 액세스 로그 파일에 기록됩니다.

플랫 로그 파일에는 `.error` 또는 `.access` 확장자가 추가됩니다. `_ERROR` 또는 `_ACCESS`로 끝나는 데이터베이스 열 이름. 예를 들어 플랫 파일 로깅 콘솔 이벤트의 이름은 `amConsole.access`이고 동일한 이벤트를 기록하는 데이터베이스 열의 이름은 `AMCONSOLE_ACCESS` 또는 `amConsole_access`입니다.

다음 표에서는 각 Access Manager 구성 요소에서 생성되는 로그 파일에 대한 간략한 설명을 제공합니다.

표 13–1 Access Manager 구성 요소 로그

구성 요소	로그 파일 이름 접두어	기록된 정보
세션	`amSSO`	로그인 시간, 로그아웃 시간, 시간 초과 제한과 같은 세션 관리 속성 값.
관리 콘솔	amConsole	Identity 관련 객체, 영역, 정책의 생성, 삭제, 수정과 같이 관리 콘솔을 통해 수행된 사용자 작업.
인증	`amAuthentication`	사용자 로그인 및 로그아웃.
아이디 연합	`amFederation`	인증 도메인 생성 및 호스트 공급자 생성 등의 연합 관련 이벤트. 연합 로그에는`amFederation` 접두어가 붙습니다.
인증(정책)	`amPolicy`	정책 생성, 삭제 또는 수정 및 정책 평가와 같은 정책 관련 이벤트.
정책 에이전트	`amAgent`	사용자가 액세스했거나 사용자에 대한 액세스가 거부된 자원 관련 예외. `amAgent` 로그는 정책 에이전트가 설치된 서버에 상주합니다. 에이전트 이벤트는 Access Manager 시스템에서 인증 로그에 기록됩니다.
SAML	`amSAML`	명제, 아티팩트 생성 또는 삭제, 응답 및 요청 세부 정보, SOAP 오류와 같은 SAML 관련 이벤트.
명령줄	`amAdmin`	명령줄 도구를 사용한 작업 도중 발생한 이벤트 오류. 예: 서비스 스키마 로딩, 정책 생성 및 사용자 삭제.

Access Manager 로그 파일 목록 및 설명은 부록 C를 참조하십시오.

디버그 파일

디버그 파일은 로깅 서비스의 기능이 아닙니다. 디버그 파일은 로깅 API와는 독립적인 다른 API를 사용하여 작성됩니다. 디버그 파일은 `/var/opt/SUNWam/debug`에 저장됩니다. 이 위치는 디버그 정보의 수준과 함께 *AccessManager-base*`/SUNWam/lib/` 디렉토리에 있는 `AMConfig.properties` 파일에서 구성할 수 있습니다. 디버그 등록 정보에 대한 자세한 내용은 부록 A를 참조하십시오.

디버그 수준

디버그 파일에 기록할 수 있는 정보의 수준에는 여러 가지가 있습니다. 디버그 수준은 `AMConfig.properties`에 있는 `com.iplanet.services.debug.level` 등록 정보를 사용하여 설정합니다.

1. Off—디버그 정보를 기록하지 않습니다.
2. Error—이 수준은 프로덕션에 사용됩니다. 프로덕션 중에는 디버그 파일에 오류가 있으면 안됩니다.
3. Warning—현재 이 수준은 사용하지 않는 것이 좋습니다.
4. Message—이 수준은 코드 추적을 사용하여 가능한 문제를 경고합니다. 대부분의 Access Manager 모듈은 이 수준을 사용하여 디버그 메시지를 보냅니다.

주 – Warning 및 Message 수준은 프로덕션에서는 사용하면 안됩니다. 이 두 수준은 많은 디버그 메시지와 함께 심각한 성능 저하를 일으킵니다.

디버그 출력 파일

디버그 파일은 모듈에서 기록해야 생성됩니다. 따라서 기본 `error` 모드에서는 디버그 파일에 생성되지 않습니다. 기본 로그인 시에 디버그 수준이 `message`로 설정되어 생성되는 디버그 파일은 다음과 같습니다.

- amAuth
- amAuthConfig
- amAuthContextLocal
- amAuthLDAP
- amCallback
- amClientDetection
- amConsole
- amFileLookup
- amJSS
- amLog
- amLoginModule
- amLoginViewBean

- amNaming
- amProfile
- amSDK
- amSSOProvider
- amSessionEncodeURL
- amThreadManager

가장 자주 사용되는 파일은 `amSDK`, `amProfile` 및 인증과 관련된 모든 파일입니다. 캡처된 정보에는 날짜, 시간 및 메시지 유형(Error, Warning, Message)이 포함됩니다.

디버그 파일 사용

디버그 수준은 기본적으로 `error`로 설정됩니다. 디버그 파일은 관리자가 다음과 같은 작업을 수행하는 경우 유용합니다.

- 사용자 정의 인증 모듈 작성.
- Access Manager SDK를 사용하여 사용자 정의 응용 프로그램 작성. `amProfile` 및 `amSDK` 디버그 파일은 이 정보를 캡처합니다.
- 콘솔 또는 SDK 사용 중에 액세스 권한 문제 해결. `amProfile` 및 `amSDK` 디버그 파일은 이 정보도 캡처합니다.
- SSL 문제 해결.
- LDAP 인증 모듈 문제 해결. `amAuthLDAP` 디버그 파일은 이 정보를 캡처합니다.

디버그 파일은 향후 제공될 수 있는 모든 문제 해결 설명서와 함께 사용되어야 합니다. 예를 들어 SSL이 실패하는 경우, 디버그를 message로 활성화하고 `amJSS` 디버그 파일을 확인하여 특정 인증서 오류를 찾을 수 있습니다.

여러 Access Manager 인스턴스 및 디버그 파일

Access Manager에는 다양한 서버 인스턴스를 구성하는 데 사용할 수 있는 `ammultiserverinstall` 스크립트가 포함되어 있습니다. 여러 서버 인스턴스가 다른 디버그 디렉토리를 사용하도록 구성된 경우 각 개별 인스턴스는 디버그 디렉토리에 대해 읽기와 쓰기 권한을 모두 가지고 있어야 합니다.

파 트 IV

명령줄 참조

Sun Java System Access Manager 7 2005Q4 관리 설명서의 제4부 명령줄 참조입니다.

이 절에서 설명하는 모든 명령줄 도구는 다음 기본 위치에서 찾을 수 있습니다.

```
AccessManager-base/SUNWam/bin (Solairs)
```

```
AccessManager-base/identity/bin (Linux)
```

이 부분은 다음 내용으로 구성되어 있습니다.

◆ ◆ ◆ 14 장

14 amadmin 명령줄 도구

이 장에서는 amadmin 명령줄 도구에 대한 정보를 제공합니다.

amadmin 명령줄 실행 파일

amadmin 명령줄 실행 파일의 주 목적은 데이터 저장소에 XML 서비스 파일을 로드하고 DIT에 일괄 관리 작업을 수행하는 것입니다. amadmin은 AccessManager-base/SUNWam/bin에 있으며 다음과 같은 작업에 사용됩니다.

- XML 서비스 파일 로드 - 관리자가 sms.dtd에 정의된 XML 서비스 파일 형식을 사용하는 Access Manager로 서비스를 로드합니다. 모든 서비스는 amadmin을 사용해 로드해야 하며, Access Manager 콘솔을 통해 가져올 수 없습니다.

주 – XML 서비스 파일은 Access Manager가 참조하는 XML 데이터의 정적 *blobs*로 데이터 저장소에 저장됩니다이 정보는 LDAP만 이해하는 Directory Server에서는 사용되지 않습니다.

- DIT에 대한 Identity 객체 일괄 업데이트 수행 - 관리자는 amadmin.dtd에 정의된 일괄 처리 XML 파일 형식을 사용하여 Directory Server DIT를 일괄적으로 업데이트할 수 있습니다. 예를 들어, 관리자가 10개의 조직, 1000명의 사용자 및 100개의 그룹을 만들고자 하는 경우 한 개 이상의 일괄 처리 XML 파일에 요청을 입력하고 amadmin을 사용해 이를 로드하면 한 번에 작업을 수행할 수 있습니다.

주 – amadmin은 Access Manager 콘솔에서 지원하고 교체할 필요가 없는 일부 기능만 지원합니다. 적은 양의 관리 작업에는 콘솔을 사용하고 많은 양의 관리 작업에는 amadmin을 사용하는 것이 좋습니다.

---

amadmin 구문

amadmin을 사용하는 경우 따라야 하는 몇 가지 구조적인 규칙이 있습니다. 도구 사용을 위한 일반 구문은 다음과 같습니다.

- amadmin -u | --runasdn *dn* 이름 -w | --password 비밀번호 [-l | --locale 로켈 이름] [[-v | --verbose] | [-d |--debug]] -t | --data *xml* 파일*1* [*xml* 파일*2* ...]
- amadmin -u | --runasdn *dn* 이름 -w | --password 비밀번호 [-l | --locale 로켈 이름] [[-v | --verbose] | [-d | --debug]] -s | --schema *xm* 파일*1* [*xml* 파일*2* ...]
- amadmin -u | --runasdn *dn* 이름 -w | --password 비밀번호 [-l | --locale 로켈 이름] [[-v | --verbose] | [-d | --debug]] -r | --deleteService 서비스 이름*1* [서비스 이름*2* ...]
- amadmin -u | --runasdn *dn* 이름 -w | --password 비밀번호 또는 -f | --password file 비밀번호 파일 [-c | --continue] [-l | --locale 로켈 이름] [[-v | --verbose] | [-d | --debug]] -m | --session 서버 이름 패턴
- amadmin -h | --help
- amadmin -n | --version
- amadmin -u | --runasdn *dn* 이름 -w | --password 비밀번호 **또는** - f |--passwordfile 비밀번호 파일 [-l | --locale 로켈 이름] [[-v | --verbose] | [-d] |--debug]] -a |--addAttributes 서비스 이름 스키마 유형 *xml* 파일[*xml* 파일*2*] ...

주 – 구문에 표시된 것처럼 두 개의 하이픈을 정확하게 입력해야 합니다.

---

amadmin 옵션

amadmin 명령줄 매개 변수 옵션의 정의는 다음과 같습니다.

--runasdn (-u)

--runasdn은 LDAP 서버에 사용자를 인증하는 데 사용됩니다. 이 인수는 amadmin을 실행하도록 인증된 사용자의 고유 이름(DN) 인수와 동일한 값입니다. 예를 들면 다음과 같습니다.

```
--runasdn uid=amAdmin,ou=People,o=iplanet.com,o=isp .
```

다음과 같이 도메인 구성 요소 간에 공백을 삽입하고 전체 DN을 큰따옴표로 묶어 DN의 형식을 지정할 수 있습니다: `--runasdn "uid=amAdmin, ou=People, o=iplanet.com, o=isp"`

--password (-w)

--password는 필수 옵션이며 --runasdn 옵션에 지정한 DN의 비밀번호와 동일한 값을 가집니다.

--locale (-l)

--locale은 로켈 이름과 동일한 값을 갖는 옵션입니다. 이 옵션은 메시지 언어를 사용자 정의하는 데 사용될 수 있습니다. 이 옵션을 지정하지 않으면 기본 로켈 en_US가 사용됩니다.

--continue (-c)

--continue는 오류가 있더라도 XML 파일 처리를 계속하기 위한 옵션입니다. 예를 들어 한 번에 3개의 XML 파일을 로드할 때 첫 번째 XML 파일이 실패하더라도 amadmin은 나머지 파일을 계속해서 로드합니다. continue 옵션은 별개의 요청에만 적용됩니다

--session (-m)

--session (-m)은 세션을 관리하거나 현재 세션을 표시하는 옵션입니다. --runasdn을 지정할 경우 AMConfig.properties에 있는 수퍼 유저의 DN 또는 최상위 관리자의 아이디와 같아야 합니다.

다음 예에서는 특정 서비스 호스트 이름에 대한 모든 세션을 표시합니다.

```
amadmin -u uid=amadmin,ou=people,dc=iplanet,dc=com
-v  -w 12345678 -m http://sun.com:58080
```

다음 예에서는 특정 사용자의 세션을 표시합니다.

```
amadmin -u uid=amadmin,ou=people,dc=iplanet,dc=com -v
 -w 12345678 -m http://sun.com:58080 사용자 이름
```

해당 색인 번호를 입력하여 특정 세션을 종료하거나 공백으로 구분한 여러 색인 번호를 입력하여 여러 세션을 종료할 수 있습니다.

다음 옵션을 사용하는 경우

```
amadmin -m | --session 서버 이름 패턴
```

패턴은 와일드카드(*)일 수 있습니다. 이 패턴으로 와일드카드를 사용할 경우 쉘에서 메타 문자(\\)로 패턴을 제어해야 합니다.

--debug (-d)

--debug는 /var/opt/SUNWam/debug 디렉토리에 생성될 amAdmin 파일에 메시지를 기록하는 옵션입니다. 이러한 메시지는 기술적으로 자세히 설명되지만 i18n 호환은 아닙니다. amadmin 작업 로그를 생성하려면 데이터베이스 로깅 시에 데이터베이스 드라이버에 대한 classpath를 직접 추가해야 합니다. 예를 들어, amadmin의 mysql에 로깅하는 경우 다음 줄을 추가합니다.

```
CLASSPATH=$CLASSPATH:/opt/IS61/SUNWam/lib/mysql-connector-java-3.0.6-stable-bin.jar
export CLASSPATH
```

--verbose (-v)

--verbose는 화면에 amadmin 명령의 전체 진행 과정을 출력하는 옵션입니다. 세부 정보를 파일로 출력하지는 않습니다. 명령줄로 출력되는 메시지는 i18n 호환입니다.

--data (-t)

--data는 가져올 일괄 처리 XML 파일의 이름을 값으로 갖는 옵션입니다. XML 파일을 한 개 이상 지정할 수 있습니다. 이러한 XML 파일을 사용하면 서비스를 등록 및 등록 취소는 물론 다양한 디렉토리 객체를 생성, 삭제 및 읽을 수 있습니다. .

--schema (-s)

--schema는 Access Manager 서비스의 속성을 Directory Server에 로드하는 옵션입니다. 이 옵션은 서비스 속성이 정의된 XML 서비스 파일을 인수로 가집니다. 이 XML 서비스 파일은 sms.dtd를 기반으로 합니다. XML 파일을 한 개 이상 지정할 수 있습니다.

주 – DIT에 대한 일괄 업데이트를 구성하는지 또는 서비스 스키마 및 구성 데이터를 로드하는지에 따라 --data 또는 --schema 옵션을 지정해야 합니다.

--deleteservice (-r)

--deleteservice는 서비스 및 이에 해당하는 스키마만 삭제하는 옵션입니다.

--serviceName

--serviceName은 XML 서비스 파일의 Service name=... 태그에 정의되는 서비스 이름과 같은 값을 갖는 옵션입니다. 이 부분은 202 페이지 “--serviceName”에 표시됩니다.

예 14–1 sampleMailService.xml의 일부분

```
...
<ServicesConfiguration>
    <Service name="sampleMailService" version="1.0">
        <Schema
 serviceHierarchy="/other.configuration/sampleMailService"
            i18nFileName="sampleMailService"
            i18nKey="iplanet-am-sample-mail-service-description">
...
```

--help (-h)

--help는 amadmin 명령에 대한 구문을 표시하는 인수입니다.

--version (-n)

--version은 유틸리티 이름, 제품 이름, 제품 버전 및 법적 고지 사항을 표시하는 인수입니다.

연합 관리에 amadmin 사용

이 절에서는 연합 관리에 사용되는 amadmin 매개 변수를 설명합니다. 연합 관리에 대한 자세한 내용은 Access Manager 연합 관리 설명서를 참조하십시오.

Directory Server에 리버티 메타 호환 XML 로드

```
amadmin -u|--runasdn <user's DN>
-w|--password <password> or -f|--passwordfile <passwordfile>
-e|--entityname <entity name>
-g|--import <xmlfile>
```

--runasdn (-u)

사용자의 DN

--password (-w)

사용자의 비밀번호

--passwordfile (-f)

사용자의 비밀번호가 있는 파일의 이름

--entityname (-e)

엔티티 이름. 예를 들어, http://www.example.com. 하나의 엔티티는 하나의 조직에만 소속되어야 합니다.

--import (-g)

메타 정보가 있는 XML 파일의 이름. 이 파일은 리버티 메타 사양 및 XSD를 준수해야 합니다.

XML 파일에 엔티티 내보내기(XML 디지털 서명 사용 안 함)

amadmin -u|--runasdn <사용자의 DN>

```
-w|--password <password> 또는 -f|--passwordfile <passwordfile>
-e|--entityname <entity name>
-o|--export <filename>
```

--runasdn (-u)

사용자의 DN

--password (-w)

사용자의 비밀번호

--passwordfile (-f)

사용자의 비밀번호가 있는 파일의 이름

--entityname (-e)

Directory Server에 있는 엔티티의 이름

--export (-o)

엔티티의 XML을 포함할 파일의 이름. XML은 리버티 메타 XSD 호환이어야 합니다.

XML 파일에 엔티티 내보내기(XML 디지털 서명 사용)

```
amadmin -u|--runasdn <user's DN>
-w|--password <password> or -f|--passwordfile <passwordfile>
-e|--entityname <entity name>
-q|--exportwithsig <filename>
```

--runasdn (-u)

사용자의 DN

--password (-w)

사용자의 비밀번호

--passwordfile (-f)

사용자의 비밀번호가 있는 파일의 이름

--entityname (-e)

Directory Server에 있는 엔티티의 이름

--exportwithsig (-o)

엔티티의 XML을 포함할 파일의 이름. 이 파일은 디지털 방식으로 서명됩니다. XML은 리버티 메타 XSD 호환이어야 합니다.

자원 번들에 amadmin 사용

다음 절에서는 지원 번들을 추가, 위치 파악 및 제거하기 위한 `amadmin` 구문을 보여 줍니다.

자원 번들 추가

```
amadmin -u|--runasdn <user-dn> -w|--password <user-password>

-b|--addresourcebundle <name-of-resource-bundle>

-i|--resourcebundlefilename <resource-bundle-file-name>

[-R|--resourcelocale] <locale>
```

자원 문자열 가져오기

```
amadmin -u|--runasdn <user-dn> -w|--password <user-password>

-z|--getresourcestrings <name-of-resource-bundle>

[-R|--resourcelocale] <locale>
```

자원 번들 제거

```
amadmin -u|--runasdn <user-dn> -w|--password <user-password>

-j|--deleteresourcebundle <name-of-resource-bundle>

[-R|--resourcelocale] <locale>
```

◆ ◆ ◆ 15장

15 ampassword 명령줄 도구

이 장에서는 amPassword 명령줄 도구에 대해 설명하며 다음 내용으로 구성되어 있습니다.

ampassword 명령줄 실행 파일

Access Manager는 ampassword 유틸리티를 SPARC 시스템의 /opt/SUNWam/bin과 Linux 시스템의 /opt/sun/Identity/bin에 포함합니다. 이 유틸리티를 사용하여 관리자 또는 사용자에 대한 Directory Server 비밀번호를 변경할 수 있습니다.

▼ SSL 모드에서 Access Manager로 ampassword를 실행하려면

1. **다음 디렉토리에 있는 serverconfig.xml 파일을 수정합니다.**

   AccessManager-base/SUNWam/config/

2. **port 서버 속성을 Access Manager가 실행 중인 SSL 포트로 변경합니다.**

3. **type 속성을 SSL로 변경합니다.**

   예를 들면 다음과 같습니다.

```
<iPlanetDataAccessLayer>
<ServerGroup name="default" minConnPool="1" maxConnPool="10">
    <Server name="Server1" host="sun.com" port="636" type="SSL" />
    <User name="User1" type="proxy">
        <DirDN>
                cn=puser,ou=DSAME Users,dc=iplanet,dc=com
        </DirDN>
        <DirPassword>
```

```
                    AQIC5wM2LY4Sfcy+AQBQxghVwhBE92i78cqf
            </DirPassword>
 </User> ...
```

ampassword는 Directory Server에서만 비밀번호를 변경합니다. Access Manager의 ServerConfig.xml 및 모든 인증 템플리트에서는 비밀번호를 수동으로 변경해야 합니다.

◆ ◆ ◆ 16 장

16 bak2am 명령줄 도구

이 장에서는 bak2am 명령줄 도구에 대해 설명하며 다음 내용으로 구성되어 있습니다.

bak2am 명령줄 실행 파일

Access Manager에는 AccessManager-base/SUNWam/bin 아래에 bak2am 유틸리티가 포함되어 있습니다. 이 유틸리티는 am2back 유틸리티에 의해 백업된 Access Manager 구성 요소의 복원을 수행합니다.

bak2am 구문

Solaris 운영 체제에서 bak2am 도구 사용을 위한 일반 구문은 다음과 같습니다.

```
./bak2am [ -v | --verbose ] -z | --gzip tar.gz-file
./bak2am [ -v | --verbose ] -t | --tar tar-file
./bak2am -h | --help
./bak2am -n | --version
```

Windows 2000 운영 체제에서 bak2am 도구 사용을 위한 일반 구문은 다음과 같습니다.

```
bak2am [ -v | --verbose ] -d | --directory directory-name

bak2am -h | --help
bak2am -n | --version
```

주 – 구문에 표시된 것처럼 두 개의 하이픈을 정확하게 입력해야 합니다.

bak2am 옵션

--gzip *backup-name*

--gzip은 백업 파일의 전체 경로와 파일 이름을 tar.gz 형식으로 지정합니다. 기본적으로 경로는 AccessManager-base/backup입니다. 이 옵션은 Solaris 전용입니다.

--tar *backup-name*

--tar는 백업 파일의 전체 경로와 파일 이름을 tar 형식으로 지정합니다. 기본적으로 경로는 AccessManager-base/backup입니다. 이 옵션은 Solaris 전용입니다.

--verbose

--verbose는 백업 유틸리티를 세부 정보 표시 모드로 실행하는 데 사용됩니다.

--directory

--directory는 백업 디렉토리를 지정합니다. 기본적으로 경로는 AccessManager-base/backup입니다. 이 옵션은 Windows 2000 전용입니다.

--help

--help는 bak2am 명령에 대한 구문을 표시하는 인수입니다.

--version

--version은 유틸리티 이름, 제품 이름, 제품 버전 및 법적 고지 사항을 표시하는 인수입니다.

◆ ◆ ◆ 17장

17 am2bak 명령줄 도구

이 장에서는 am2bak 명령줄 도구에 대해 설명합니다.

am2bak 명령줄 실행 파일

Access Manager에는 AccessManager-base/SUNWam/bin 아래에 am2bak 유틸리티가 포함되어 있습니다. 이 유틸리티는 Access Manager의 전체 또는 선택적 구성 요소를 백업합니다. 로그 백업을 가져 오는 동안 Directory Server가 실행 중이어야 합니다.

am2bak 구문

Solaris 운영 체제에서 am2bak 도구를 사용하기 위한 일반 구문은 다음과 같습니다.

```
./am2bak [ -v | --verbose ] [ -k | --backup backup-name ] [ -l | --location location ]
[[-c | --config] | [-b | --debug] | [-g | --log] | [-t | --cert] | [-d | --ds] | [-a |
--all]]*

./am2bak -h | --help

./am2bak -n | --version
```

Windows 2000 운영 체제에서 am2bak 도구를 사용하기 위한 일반 구문은 다음과 같습니다.

```
am2bak [ -v | --verbose ] [ -k | --backup backup-name ] [ -l | --location location ] [[-c
| --config] | [-b | --debug] | [-g | --log] | [-t | --cert] | [-d | --ds] | [-a |
--all]]*

am2bak -h | --help

am2bak -n | --version
```

주 – 구문에 표시된 것처럼 두 개의 하이픈을 정확하게 입력해야 합니다.

am2bak 옵션

--verbose (-v)

`--verbose`는 백업 유틸리티를 세부 정보 표시 모드로 실행하는 데 사용됩니다.

--backup *backup-name (-k)*

`--backup` *backup-name*은 백업 파일의 이름을 정의합니다. 기본값은 `ambak`입니다.

--location (-l)

`--location`은 백업의 디렉토리 위치를 지정합니다. 기본 위치는 `AccessManager-base/backup`입니다.

--config (-c)

`--config`는 구성 파일만 백업하도록 지정합니다.

--debug (-b)

`--debug`는 디버그 파일만 백업하도록 지정합니다.

--log (-g)

`--log`는 로그 파일만 백업하도록 지정합니다.

--cert (-t)

`--cert`는 인증서 데이터베이스 파일만 백업하도록 지정합니다.

--ds (-d)

`--ds`는 Directory Server에 대해서만 백업하도록 지정합니다.

--all (-a)

`--all`은 전체 Access Manager에 대한 전체 백업을 지정합니다.

--help (-h)

`--help`는 `am2bak` 명령의 구문을 표시하는 인수입니다.

--version (-n)

--version은 유틸리티 이름, 제품 이름, 제품 버전 및 법적 고지 사항을 표시하는 인수입니다.

▼ 백업 절차를 실행하려면

1 루트로 로그인합니다.

이 스크립트를 실행하려면 사용자에게 루트 액세스가 필요합니다.

2 필요한 경우 스크립트를 실행하여 올바른 경로가 사용되는지 확인합니다.

이 스크립트가 백업하는 Solaris™ 운영 환경 파일은 다음과 같습니다.

- 구성 및 사용자 정의 파일:
  - AccessManager-base/SUNWam/config/
    - AccessManager-base/SUNWam/locale/
    - AccessManager-base/SUNWam/servers/httpacl
    - AccessManager-base/SUNWam/lib/*.properties(Java 등록 정보 파일)
    - AccessManager-base/SUNWam/bin/amserver. *instance-name*
    - AccessManager-base/SUNWam/servers/https- *all_instances*
    - AccessManager-base/SUNWam/servers/web-apps- *all_instances*
    - AccessManager-base/SUNWam/web-apps/services/WEB-INF/config
    - AccessManager-base/SUNWam/web-apps/services/config
    - AccessManager-base/SUNWam/web-apps/applications/WEB-INF/classes
    - AccessManager-base/SUNWam/web-apps/applications/console
    - /etc/rc3.d/K55amserver.*all_instances*
    - /etc/rc3.d/S55amserver.*all_instances*
    - DirectoryServer-base/slapd- *host* /config/schema/
    - DirectoryServer-base/slapd- *host* /config/slapd-collations.conf
    - Access Manager/slapd- *host* /config/dse.ldif

  로그 및 디버그 파일:

  - var/opt/SUNWam/logs(Access Manager 로그 파일)
  - var/opt/SUNWam/install(Access Manager 설치 로그 파일)
  - var/opt/SUNWam/debug(Access Manager 디버그 파일)

  인증서:

  - Access Manager/SUNWam/servers/alias
  - Access Manager/alias

    스크립트가 백업하는 Microsoft® Windows 2000 운영 체제 파일은 다음과 같습니다.

  구성 및 사용자 정의 파일:

  - AccessManager-base/web-apps/services/WEB-INF/config/*
  - AccessManager-base/locale/*

- AccessManager-base/web-apps/applications/WEB-INF/classes/*.properties(java 등록 정보 파일)
- AccessManager-base/servers/https- *host*/config/jvm12.conf
- AccessManager-base/servers/https- *host*/config/magnus.conf
- AccessManager-base/servers/https- *host*/config/obj.conf
- DirectoryServer-base/slapd-host/config/schema/*.ldif
- DirectoryServer-base/slapd-host/config/slapd-collations.conf
- DirectoryServer-base/slapd-host/config/dse.ldif

로그 및 디버그 파일:

- var/opt/logs(Access Manager 로그 파일)
- var/opt/debug(Access Manager 디버그 파일)

인증서:

- AccessManager-base/servers/alias
- AccessManager/alias

◆ ◆ ◆ 18 장

18 amserver 명령줄 도구

이 장에서는 amserver 명령줄 도구에 대해 설명합니다. 이번 장은 다음 절로 구성됩니다.

amserver 명령줄 실행 파일

amserver 명령줄 실행 파일은 Unix와 SecurID 인증 모듈과 연관된 amunixd와 amsercuridd 도우미를 각각 시작 및 중지합니다.

amserver 구문

이 도구에 대한 일반 구문은 다음과 같습니다.

```
./amserver { start | stop }
```

start

start는 도우미를 시작하는 명령입니다.

stop

stop은 도우미를 중지하는 명령입니다.

◆ ◆ ◆ 19 장

19 VerifyArchive 명령줄 도구

이 장에서는 VerifyArchive 명령줄 도구에 대한 정보를 제공하며 다음 내용으로 구성되어 있습니다.

VerifyArchive 명령줄 실행 파일

VerifyArchive의 목적은 로그 아카이브를 확인하는 것입니다. 로그 아카이브는 타임스탬프와 해당 키 저장소 집합입니다. 키 저장소에는 로그 파일의 손상을 검색하는 데 사용되는 MAC 및 디지털 서명을 생성하는 데 사용되는 키가 포함되어 있습니다. 아카이브 확인에서는 아카이브의 파일 손상 및/또는 삭제를 검색합니다.

VerifyArchive는 지정된 logName에 대해 모든 아카이브 집합과 각 아카이브 집합에 속하는 모든 파일을 추출합니다. VerifyArchive를 실행하면 각 로그 레코드에서 손상을 검색하여 손상이 있을 경우 손상된 파일 및 레코드 수를 지정하는 메시지를 인쇄합니다.

또한 VerifyArchive는 아카이브 집합에서 삭제된 파일을 확인합니다. 삭제된 파일이 검색되면 확인이 실패했다는 메시지가 인쇄됩니다. 손상 또는 삭제된 파일이 검색되지 않으면 아카이브 확인이 성공적으로 완료되었다는 메시지가 반환됩니다.

주 – 관리자 권한이 없는 사용자로 amverifyarchive를 실행하면 오류가 발생할 수 있습니다.

VerifyArchive 구문

모든 매개 변수 옵션은 필수입니다. 구문은 다음과 같습니다.

```
amverifyarchive -l logName -p path -u
uname -w password
```

VerifyArchive 옵션

logName

logName은 확인할 로그 이름(예: amConsole, amAuthentication 등)입니다. VerifyArchive는 지정된 logName에 대한 액세스 로그와 오류 로그를 모두 확인합니다. 예를 들어, amConsole이 지정된 경우 검증기는 amConsole.access 및 amConsole.error 파일을 확인합니다. 또는 logName을 amConsole.access 또는 amConsole.error로 지정하여 이러한 로그만 확인하도록 제한할 수 있습니다.

path

path는 로그 파일이 저장되는 전체 디렉토리 경로입니다.

uname

uname은 Access Manager 관리자의 사용자 아이디입니다.

password

password는 Access Manager 관리자의 비밀번호입니다.

◆ ◆ ◆ 20 장

amsecuridd 도우미

이 장에서는 amsecuiridd 도우미에 대한 정보를 제공하며 다음 내용으로 구성되어 있습니다.

amsecuridd 도우미 명령줄 실행 파일

Access Manager SecurID 인증 모듈과 SecurID 서버 사이에서 통신하는 Security Dynamic ACE/Client C API 및 amsecruidd 도우미를 사용하여 Access Manager SecurID 인증 모듈을 구현합니다. SecurID 인증 모듈은 localhost:57943에 대한 소켓을 열어 amsecuridd 데몬을 호출하여 SecurID 인증 요청을 수신합니다.

주 – 기본 포트 번호는 57943입니다. 이 포트 번호가 이미 사용되고 있는 경우 SecurID 인증 모듈의 SecurID 도우미 인증 포트 속성에서 다른 포트 번호를 지정할 수 있습니다. 이 포트 번호는 조직 전체에서 고유해야 합니다.

---

amsecuridd에 대한 인터페이스가 stdin을 통해 일반 텍스트로 보내지기 때문에 로컬 연결만 허용이 됩니다. amsecuridd 는 데이터 암호화를 위해 백 엔드에 있는 SecurID 원격 API(버전 5.x)를 사용합니다.

amsecuridd 도우미는 포트 번호 58943(기본값)에서 구성 정보를 수신합니다. 이 포트가 이미 사용되고 있는 경우 AMConfig.properties 파일(기본적으로 AccessManager-base/SUNWam/config/에 있음)의 securidHelper.ports 속성에서 포트 번호를 변경할 수 있습니다. securidHelp.ports 속성에는 각 amsecuridd 도우미 인스턴스에 대한 공백으로 구분된 포트 목록이 포함되어 있습니다. AMConfig.properties 에 대한 변경 내용을 저장하고 Access Manager를 다시 시작합니다.

주 – 개별 ACE/Server(다른 sdconf.rec 파일을 포함함)와 통신하는 각 조직에 대해 별도의 amsecuridd 인스턴스를 실행해야 합니다.

amsecuridd 구문

구문은 다음과 같습니다.

```
amsecuridd [-v] [-c portnum]
```

amsecuridd 옵션

verbose (-v)

세부 정보 표시 모드를 설정하고 /var/opt/SUNWam/debug/securidd_client.debug에 기록합니다.

configure portnumber (-c portnm)

수신 포트 번호를 구성합니다. 기본값은 58943입니다.

amsecuridd 도우미 실행

amsecuridd는 기본적으로 *AccessManager-base* /SUNWam/share/bin에 있습니다. 기본 포트에서 도우미를 실행하려면 다음 명령을 입력합니다(옵션 없음).

```
./amsecuridd
```

기본 포트가 아닌 포트에서 도우미를 실행하려면 다음 명령을 입력합니다.

```
./amsecuridd [-v] [-c portnm]
```

amsecuriddd는 amserver 명령줄 유틸리티를 통해 실행될 수도 있지만 그 경우에는 기본 포트에서만 실행됩니다.

필수 라이브러리

도우미를 실행하려면 다음과 같은 라이브러리(대부분 /usr/lib/의 운영 체제에 있음)가 필요합니다.

- libnsl.so.1
- libthread.so.1
- libc.so.1

- libdl.so.1
- libmp.so.2
- librt.so.1
- libaio.so.1
- libmd5.so.1

주 – libaceclnt.so를 찾으려면 LD_LIBRARY_PATH를 *AccessManager-base*/Sunwam/lib/로 설정합니다.

파 트 V

부록

Sun Java System Access Manager 7 2005Q4 관리 설명서의 제5부로서 오류 코드 목록 및 파일 참조가 포함되어 있습니다. 이 절에는 다음 부록이 포함되어 있습니다.

◆ ◆ ◆ 부 록 A

AMConfig.properties 파일

AMConfig.properties는 Access Manager의 기본 구성 파일입니다. 이 파일의 등록 정보 중 일부만 구성할 수 있습니다. 이 장에서는 AMConfig.properties에 있는 등록 정보, 기본 등록 정보 값 및 Access Manager를 사용할 수 있도록 유지하면서 값을 수정하는 방법에 대해 설명합니다.

이 장은 다음 내용으로 구성되어 있습니다.

AMConfig.properties 파일 정보

설치 시 AMConfig.properties는/etc/opt/SUNWam/config에 저장됩니다.

AMConfig.properties는 한 줄당 한 개의 등록 정보를 포함하며 각 등록 정보가 해당 값을 가집니다. 등록 정보 및 값은 대소문자를 구분합니다. 슬래시 및 별표(/*) 문자로 시작하는 줄은 주석이며 응용 프로그램에서 무시됩니다. 주석은 별표 및 슬래시(*/) 종결 문자를 포함하는 마지막 줄에서 끝납니다.

AMConfig.properties의 등록 정보를 수정한 다음 변경 사항을 적용하려면 Access Manager를 다시 시작해야 합니다.

Access Manager 콘솔

- com.iplanet.am.console.deploymentDescriptor

  값은 설치 중에 설정됩니다. 예: /amconsole
- com.iplanet.am.console.host

  값은 설치 중에 설정됩니다. 예: *hostName.domain.Name* .com
- com.iplanet.am.console.port

  값은 설치 중에 설정됩니다. 예: 80
- com.iplanet.am.console.protocol

  값은 설치 중에 설정됩니다. 예: http

Access Manager 서버 설치

- com.iplanet.am.install.basedir

  읽기 전용 등록 정보입니다. 등록 정보 값을 수정하지 마십시오.

  값은 설치 중에 설정됩니다. 예: /opt/SUNWam/web-src/services/WEB-INF
- com.iplanet.am.install.vardir

  읽기 전용 등록 정보입니다. 등록 정보 값을 수정하지 마십시오.

  값은 설치 중에 설정됩니다. 예: /var/opt/SUNWam
- com.iplanet.am.installdir

  읽기 전용 등록 정보입니다. 등록 정보 값을 수정하지 마십시오.

값은 설치 중에 설정됩니다. 예: `/opt/SUNWam`

- `com.iplanet.am.jdk.path`

  값은 설치 중에 설정됩니다. 예: `/usr/jdk/entsys-j2se`

- `com.iplanet.am.locale`

  값은 설치 중에 설정됩니다. 예: `en_US`

- `com.iplanet.am.server.host`

  값은 설치 중에 설정됩니다. 예: *hostName.domainName*`.com`

- `com.iplanet.am.server.port`

  값은 설치 중에 설정됩니다. 예: `80`

- `com.iplanet.am.server.protocol`

  값은 설치 중에 설정됩니다. 예: `http`

- `com.iplanet.am.version`

  값은 설치 중에 설정됩니다. 예: `7 2005Q4`

- `com.sun.identity.server.fqdnMap[ ]`

  사용자가 잘못된 URL을 입력한 경우 Access Manager 인증 서비스에서 교정 조치를 취할 수 있도록 합니다. 예를 들어, 사용자가 부분 호스트 이름을 지정하거나 IP 주소를 사용하여 보호된 자원에 액세스하는 경우 유용합니다.

  이 등록 정보 구문은 잘못된 FQDN 값이 해당 유효한 대응 항목에 매핑되어 있음을 나타냅니다. 등록 정보는 다음 형식을 사용합니다.
  `com.sun.identity.server.fqdnMap[`*invalid-name*`]=`*valid—name*. 이 예에서, 잘못된 이름은 사용자가 사용할 수 있는 유효하지 않은 FQDN 호스트 이름일 수 있으며 유효한 이름은 필터가 사용자를 리디렉션할 FQDN 호스트 이름입니다. 동일한 잘못된 FQDN에 대한 값이 겹쳐 있으면 응용 프로그램에 액세스할 수 없게 될 수 있습니다. 이 등록 정보에 대해 잘못된 값을 사용하는 경우에도 응용 프로그램이 액세스할 수 없게 됩니다. 이 등록 정보를 사용하여 여러 호스트 이름을 매핑할 수 있습니다. 이는 서버에서 호스트하는 응용 프로그램을 여러 호스트 이름으로 액세스하는 경우 유용합니다.

  특정 호스트 이름 URL에 대해 교정 조치를 취하지 않도록 Access Manager를 구성하는 데 이 등록 정보를 사용할 수 있습니다. 예를 들어 원시 IP 주소를 사용하여 응용 프로그램 자원에 액세스하는 사용자에 대한 리디렉션과 같은 교정 조치를 사용하지 않아야 하는 경우에 유용합니다.

  매핑 항목을`com.sun.identity.server.fqdnMap[`*IP* `]=`*IP*와 같이 지정할 수 있습니다.

  등록 정보가 유효하며 앞서 설명한 요구 사항에 부합하면 원하는 만큼 이러한 등록 정보를 지정할 수 있습니다. 예:
  `com.sun.identity.server.fqdnMap[`*isserver*`]=`*isserver.mydomain.com*
  `com.sun.identity.server.fqdnMap[`*isserver.mydomain*`]=`*isserver.mydomain.com*
  `com.sun.identity.server.fqdnMap[`*IP 주소*`]=`*isserver.mydomain.com*

am.util

- com.iplanet.am.util.xml.validating

  기본값은 no입니다. Access Manager XMLUtils 클래스를 사용하여 XML 문서를 구문 분석하는 경우 검증이 필요한지를 결정합니다. 이 등록 정보는 com.iplanet.services.debug에 대한 값인 경우에만 유효합니다.level 등록 정보는 warning 또는 message로 설정됩니다. 사용 가능한 값은 yes 및 no입니다. 이 등록 정보의 값이 yes이고 com.iplanet.services.debug.level property의 값이 warning 또는 message로 설정된 경우에만 XML 문서 인증이 켜집니다.

amSDK

각 SDK 캐시 항목은 사용자를 위한 AMObject 속성 값 집합을 저장합니다.

- com.iplanet.am.sdk.cache.maxSize

  기본값은 10000입니다. 캐싱을 사용하는 경우 SDK 캐시의 크기를 지정합니다. 0보다 큰 정수를 사용하지 않으면 기본 크기(사용자 10000명)가 사용됩니다.

- com.iplanet.am.sdk.userEntryProcessingImpl

  이 등록 정보는 사용자 만들기, 삭제 및 수정 작업을 위해 일부 사후 처리를 수행할 com.iplanet.am.sdk.AMUserEntryProcessed 인터페이스를 구현하는 플러그 인을 지정합니다. 이 등록 정보(사용되는 경우)는 위의 인터페이스를 구현하는 정규화된 클래스 이름을 지정해야 합니다.

- com.iplanet.am.sdk.caching.enabled

  이 값을 true로 설정하면 캐싱이 활성화되고 false로 설정하면 캐싱이 비활성화됩니다. 기본값은 false입니다.

Application Server 설치

- com.iplanet.am.iASConfig

  값은 설치 중에 설정됩니다. 예: APPSERVERDEPLOYMENT

  이 등록 정보는 Access Manager가 iPlanet Application Server에서 실행 중인지 확인하는 데 사용됩니다.

인증

- com.sun.identity.auth.cookieName

  기본값은 AMAuthCookie입니다. 인증 서비스에 의해 사용되는 쿠키 이름을 지정하여 인증 프로세스 동안 세션 처리기 아이디를 설정합니다. 이 프로세스가 완료되면(성공이든 실패이든) 이 쿠키는 지워지거나 삭제됩니다.

- com.sun.identity.authentication.ocsp.responder.nickname

  값은 설치 중에 설정됩니다. 인증 기관(CA)은 해당 응답자에 대한 별칭을 인증합니다. 예: **인증서 관리자** - sun. 설정된 경우 Web Server의 인증 데이터데이스에 CA 인증서가 있어야 합니다.

- com.sun.identity.authentication.ocsp.responder.url

  값은 설치 중에 설정됩니다. 예: http://ocsp.sun.com/ocsp

  해당 인스턴스에 대한 전역 OCSP 응답자 URL을 지정합니다. OCSP 응답자 URL이 설정된 경우 OCSP 응답자 별칭도 설정해야 합니다. 그렇지 않으면 둘 다 무시됩니다. 둘 다 설정되지 않은 경우 사용자 인증서에 있는 OCSP 응답자 URL이 OCSP 검증에 사용됩니다. 사용자 인증서에 OCSP 응답자 URL이 없는 경우 OCSP 검증이 수행되지 않습니다.

- com.sun.identity.authentication.ocspCheck

  기본값은 true입니다. OCSP 검사를 활성 또는 비활성화하는 전역 매개 변수입니다. 이 값이 false이면 인증 기관 모듈 유형의 OCSP 기능은 사용할 수 없습니다..

- com.sun.identity.authentication.special.users

  값은 설치 중에 설정됩니다. 예: cn=dsameuser,ou=DSAME Users,o=AMRoot|cn=amService-UrlAccessAgent,ou=DSAME Users,o=AMRoot

  해당 Access Manager 인증 구성 요소를 위한 특수 사용자 또는 사용자를 식별합니다. 클라이언트 API는 전체 사용자 DN을 사용하여 원격 응용 프로그램을 Access Manager 서버에 대해 인증하는 데 이 사용자를 사용합니다. 사용자는 항상 디렉토리 서버에 대해 인증됩니다. 여러 개의 특수 사용자 DN 값이 있는 경우 파이프 문자(|)로 분리됩니다. 이 등록 정보는 인증 구성 요소에 대해서만 사용할 수 있습니다.

- com.sun.identity.authentication.super.user

  값은 설치 중에 설정됩니다. 예: uid=amAdmin,ou=People,o=AMRoot

  해당 Access Manager 인스턴스에 대한 수퍼 유저를 식별합니다. 해당 사용자는 LDAP를 사용하여 로그인해야 하며 전체 DN을 사용해야 합니다. 사용자는 항상 로컬 Directory Server에 대해 인증됩니다.

- com.sun.identity.authentication.uniqueCookieDomain

  위에서 설명한 쿠키 이름의 쿠키 도메인을 설정하는 데 사용됩니다. 네트워크에 설치된 CDC(Cross Domain Controller) 서비스의 모든 인스턴스를 지원하도록 쿠키 도메인을 설정해야 합니다. 예를 들어Access Manager의 모든 인스턴스가 도메인 .example.com 내에 있으면 example.com으로 설정해야 합니다.

- com.sun.identity.authentication.uniqueCookieName

기본값은 sunIdentityServerAuthNServer입니다. Access Manager가 세션 쿠키 하이재킹을 방지하도록 실행 중인 경우 쿠키 이름 집합을 Access Manager 서버 호스트 URL로 설정합니다.

- com.iplanet.am.auth.ldap.createUserAttrList

  동적으로 사용자를 생성하도록 인증 서비스가 구성된 경우 LDAP 인증이 수행되는 동안 외부 Directory Server에서 검색되는 값을 포함하는 사용자 속성의 목록을 지정합니다. 로컬 Directory Server에서 생성된 새 사용자는 외부 Directory Server에서 검색된 속성의 값을 가집니다.

  예: 속성*1*, 속성*2*, 속성*3*

인증서 데이터베이스

iPlanet Web Server가 SSL용으로 구성된 경우 이러한 등록 정보를 설정하여 JSS 소켓 팩토리를 초기화합니다.

- com.iplanet.am.admin.cli.certdb.dir

  값은 설치 중에 설정됩니다. 예: /opt/SUNWwbsvr/alias

  인증서 데이터베이스 경로를 지정합니다.

- com.iplanet.am.admin.cli.certdb.passfile

  값은 설치 중에 설정됩니다. 예: /etc/opt/SUNWam/config/.wtpass

  인증서 데이터베이스 비밀번호 파일을 지정합니다.

- com.iplanet.am.admin.cli.certdb.prefix

  값은 설치 중에 설정됩니다. 예: https-*hostName.domainName*.com-*hostName*-

  인증서 데이터베이스 접두어를 지정합니다.

쿠키

- com.iplanet.am.cookie.encode

  이 등록 정보를 사용하면 Access Manager에서 문자를 HTTP가 이해할 수 있는 형태로 변환하는 쿠키 값에 대해 URLencode를 수행할 수 있습니다.

  값은 설치 중에 설정됩니다. 예: false

- com.iplanet.am.cookie.name

  기본값은 iPlanetDirectoryPro입니다. 인증 서비스에서 유효한 세션 처리기 ID를 설정하는 데 사용하는 쿠키 이름입니다. 이 쿠키 이름의 값은 유효한 세션 정보를 검색하는 데 사용됩니다.

- com.iplanet.am.cookie.secure

  HTTP(s)와 같은 보안 프로토콜을 사용하는 경우 Access Manager 쿠키는 브라우저에서 쿠키만 반환하는 보안 모드로 설정될 수 있습니다.

기본값은 false입니다.

- com.iplanet.am.console.remote

  값은 설치 중에 설정됩니다. 예: false

  콘솔이 설치된 위치가 원격 시스템인지, 로컬 시스템인지를 결정하며 인증 콘솔에서 사용됩니다.

- com.iplanet.am.pcookie.name

  영구 쿠키의 쿠키 이름을 지정합니다. 브라우저 창이 닫힌 후에도 영구 쿠키는 계속 존재합니다. 영구 쿠키를 사용하면 사용자는 다시 인증할 필요 없이 새 브라우저 세션으로 로그인할 수 있습니다. 기본값은 DProPCookie입니다.

- com.sun.identity.cookieRewritingInPath

  기본값은 true입니다. Access Manager가 쿠키 없음 모드로 작동하도록 구성된 경우 인증 서비스에서 이 등록 정보를 읽습니다. 이 등록 정보는 다음 형식을 사용하여 URL에서 쿠키를 추가 경로 정보로 다시 기록하도록 지정합니다:
  protocol://server:port/uri;*cookiename*= cookieValue?queryString. 이 등록 정보를 지정하지 않으면 쿼리 문자열의 일부로 쿠키를 기록합니다.

- com.sun.identity.enableUniqueSSOTokenCookie

  기본값은 false입니다. 값이 true로 설정된 경우 Access Manager가 세션 쿠키 하이재킹을 방지하면서 실행 중임을 나타냅니다.

디버깅

- com.iplanet.services.debug.directory

  디버그 파일이 만들어지는 출력 디렉토리를 지정합니다. 값은 설치 중에 설정됩니다. 예: /var/opt/SUNWam/debug

- com.iplanet.services.debug.level

  디버그 수준을 지정합니다. 기본값은 error입니다. 사용 가능한 값은 다음과 같습니다.

off	디버그 파일을 만들지 않습니다.
error	오류 메시지만 기록됩니다.
warning	경고 메시지만 기록됩니다.
message	오류, 경고 및 정보 메시지가 기록됩니다.

Directory Server 설치

- com.iplanet.am.defaultOrg

  값은 설치 시에 설정됩니다. 예: o=AMRoot

  Access Manager 정보 트리의 최상위 영역 또는 조직을 지정합니다.

- com.iplanet.am.directory.host

  값은 설치 중에 설정됩니다. 예: *DirectoryServerHost.domainName*.com

  Directory Server의 정규화된 호스트 이름을 지정합니다.

- com.iplanet.am.directory.port

  값은 설치 중에 설정됩니다. 예: 389

  Directory Server 포트 번호를 지정합니다.

- com.iplanet.am.directory.ssl.enabled

  기본값은 false입니다. SSL(Security Socket Layer) 사용 여부를 표시합니다.

- com.iplanet.am.domaincomponent

  값은 설치 중에 설정됩니다. 예: o=AMRoot

  Access Manager 정보 트리에 대한 도메인 구성 요소(dc) 속성을 지정합니다.

- com.iplanet.am.rootsuffix

  값은 설치 중에 설정됩니다. 예: o=AMRoot

이벤트 연결

- com.iplanet.am.event.connection.delay.between.retries

  기본값은 3000입니다. 재시도 간격(밀리초)을 지정하여 이벤트 서비스를 다시 연결합니다.

- com.iplanet.am.event.connection.ldap.error.codes.retries

  기본값은 80,81,91입니다. 이벤트 서비스를 다시 연결하는 재시도를 시작하는 LDAP 예외 오류 코드를 지정합니다.

- com.iplanet.am.event.connection.num.retries

  기본값은 3입니다. 이벤트 서비스를 성공적으로 다시 연결하기 위한 재시도 횟수를 지정합니다.

- com.sun.am.event.connection.idle.timeout

  기본값은 0입니다. 지속적 검색을 다시 시작할 때까지 걸리는 시간(분)을 지정합니다.

  이 등록 정보는 정책 에이전트 및 Directory Server 간에 로드 밸런서 또는 방화벽이 있는 경우 사용되며, TCP idle timeout이 발생하면 지속적 검색 연결은 끊어집니다. 등록 정보 값은 로드 밸런서 또는 방화벽 TCP 시간 제한보다 작아야 합니다. 이렇게 하면 연결이

끊어지기 전에 지속적 검색이 다시 시작됩니다. 값이 0이면 검색이 다시 시작되지 않습니다. 시간이 초과된 연결만 재설정합니다.

전역 서비스 관리

- com.iplanet.am.service.secret

  값은 설치 중에 설정됩니다. 예: AQICPX9e1cxSxB2RSy1WG1+O4msWpt/6djZl

- com.iplanet.am.services.deploymentDescriptor

  값은 설치 중에 설정됩니다. 예: /amserver

- com.iplanet.services.comm.server.pllrequest.maxContentLength

  기본값은 16384 또는 16k입니다. Access Manager에서 허용되는 HttpRequest에 대한 최대 컨텐트 길이를 지정합니다.

- com.iplanet.services.configpath

  값은 설치 중에 설정됩니다. 예: /etc/opt/SUNWam/config

도우미 데몬

- com.iplanet.am.daemons

  기본값은 unix securid입니다. 설명

- securidHelper.ports

  기본값은 58943입니다. 이 등록 정보는 공백으로 분리된 목록을 가지고 SecurID 인증 모듈 및 도우미에 사용됩니다.

- unixHelper.ipaddrs

  값은 설치 중에 설정됩니다. 도우미를 시작할 때 amserver 스크립트에서 읽고 UNIX 도우미에 전달될 IP 주소의 목록을 지정합니다. 이 등록 정보는 IPv4 형식의 신뢰할 수 있는 IP 주소를 공백으로 분리한 목록으로 포함할 수 있습니다.

- unixHelper.port

  기본값은 58946입니다. UNIX 인증 모듈 유형에 사용됩니다.

아이디 연합

- com.sun.identity.federation.alliance.cache.enabled

  기본값은 true입니다. true인 경우 연합 메타 데이터는 내부적으로 캐시됩니다.

- com.sun.identity.federation.fedCookieName

  기본값은 fedCookie입니다. 연합 서비스 쿠키의 이름을 지정합니다.

- com.sun.identity.federation.proxyfinder

  기본값은 com.sun.identity.federation.services.FSIDPProxyImpl입니다. 프록시에 사용될 기본 아이디 공급자를 찾기 위한 구현을 지정합니다.

- com.sun.identity.federation.services.signingOn

  기본값은 false입니다. 리버티 요청 및 응답에 대한 서명 확인 수준을 지정합니다.

true	보내는 리버티 요청 및 응답을 서명하고 받은 리버티 요청 및 응답에 대한 서명 유효성을 검증합니다.
false	보내고 받은 리버티 요청 및 응답의 서명을 검증하지 않습니다.
optional	연합 프로필에서 요청된 경우에만 리버티 요청 및 응답을 서명 또는 검증합니다.

- com.sun.identity.password.deploymentDescriptor

  값은 설치 중에 설정됩니다. 예: /ampassword

- com.sun.identity.policy.Policy.policy_evaluation_weights

  기본값은 10:10:10입니다. 정책 주제, 규칙 및 조건을 계산하기 위한 비례 처리 비용을 나타냅니다. 지정된 값은 정책의 주제, 규칙 및 조건을 계산하는 순서에 영향을 줍니다. 이 값은 주제, 규칙 및 조건을 나타내는 3개의 정수로 표시됩니다. 값을 콜론(:)으로분리하여 정책 주제, 규칙 및 조건을 계산하기 위한 비례 처리 비용을 표시합니다.

- com.sun.identity.session.application.maxCacheTime

  기본값은 3입니다. 응용 프로그램 세션에 대한 최대 캐싱 시간(분)을 지정합니다. 이 등록 정보를 사용하지 않으면 기본적으로 캐시는 만료되지 않습니다.

- com.sun.identity.sm.ldap.enableProxy

  기본값은 false입니다. 연결에 사용할 프록시 서버를 지정합니다. 백엔드 저장소에서 LDAPProxy가 지원되면 true로 설정합니다. true이면 연결에 프록시 서버를 사용하고 false이면 연결에 프록시를 사용하지 않습니다.

- com.sun.identity.webcontainer

  값은 설치 중에 설정됩니다. 예: WEB_CONTAINER

  웹 컨테이너의 이름을 지정합니다. 서블릿 또는 JSP는 웹 컨테이너를 사용하지 않지만 Access Manager는 들어오는 영어 이외의 문자를 올바르게 디코딩하기 위해 서블릿 2.3 API request.setCharacterEncoding()을 사용합니다. 이러한 API는 Access Manager가 Sun Java System Web Server 6.1에 배포된 경우 작동하지 않습니다. Access Manager는 Sun Java System Web Server versions 6.1 및 S1AS7.0에서 받는 데이터를 올바르게 디코딩하기 위해 gx_charset 메커니즘을 사용합니다. 사용할 수 있는 값은 BEA6.1, BEA 8.1, IBM5.1 또는 IAS7.0입니다. 웹 컨테이너가 Sun Java System Web Server인 경우 태그는 바뀌지 않습니다.

JSS 프록시

이러한 등록 정보는 SSL ApprovalCallback에 대한 값을 식별합니다. checkSubjectAltName 또는 resolveIPAddress 기능을 활성화한 경우 com.iplanet.am.admin.cli.certdb.dir 디렉토리에 com.iplanet.am.admin.cli.certdb.prefix 접두어 값을 가진 cert7.db 및 key3.db를 만들어야 합니다. 그런 다음 Access Manager를 다시 시작합니다.

- com.iplanet.am.jssproxy.checkSubjectAltName

  기본값은 false입니다. 활성화된 경우 서버 인증서는 주제 대체 이름(SubjectAltName) 확장을 포함하고 Access Manager는 확장에서 모든 이름 항목을 확인합니다. SubjectAltName 확장에 있는 이름 중 하나가 서버 FQDN과 같은 경우 Access Manager는 SSL 핸드셰이킹을 계속 수행합니다. 이 등록 정보를 활성화하려면 등록 정보를 인증된 FQDN의 쉼표로 구분된 목록에 설정합니다. 예를 들면 다음과 같습니다.

  ```
  com.iplanet.am.jssproxy.checkSubjectAltName=
  amserv1.example.com,amserv2.example.com
  ```

- com.iplanet.am.jssproxy.resolveIPAddress

  기본값은 false입니다.

- com.iplanet.am.jssproxy.trustAllServerCerts

  기본값은 false입니다. 활성화된 경우(true) Access Manager는 이름 충돌과 같은 모든 인증서 관련 문제를 무시하고 SSL 핸드셰이킹을 계속 수행합니다. 있을 수 있는 보안 위험성을 방지하려면 테스트 목적 또는 기업 네트워크가 엄격히 제어되는 경우에만 이 등록 정보를 활성화합니다. 보안 위험성이 발생할 수 있는 경우(예를 들어 서버가 다른 네트워크에 있는 서버와 연결되는 경우) 이 등록 정보를 활성화하지 마십시오.

- com.iplanet.am.jssproxy.SSLTrustHostList를 설정한 경우 Access Manager가 Platform Server 목록을 현재 액세스 중인 서버 호스트와 비교하여 확인합니다. 플랫폼 목록에 있는 두 서버의 서버 FQDN이 일치하는 경우 Access Manager는 SSL 핸드셰이킹을 계속 수행합니다. 등록 정보를 설정하려면 다음 구문을 사용하십시오.

  com.iplanet.am.jssproxy.SSLTrustHostList = *fqdn_am_server1* ,*fqdn_am_server2*, *fqdn_am_server3*

- com.sun.identity.jss.donotInstallAtHighestPriority

  기본값은 false입니다. JSS를 가장 높은 우선 순위로 JCE에 추가할지 결정합니다. 디지털 서명 및 암호화에 다른 JCE 공급자를 사용해야 하는 경우 true로 설정합니다.

LDAP 연결

- com.iplanet.am.ldap.connection.delay.between.retries

  기본값은 1000입니다. 재시도 간격(밀리초)을 지정합니다.

- com.iplanet.am.ldap.connection.ldap.error.codes.retries

  기본값은 80,81,91입니다. LDAP를 다시 연결할 재시도를 시작하는 LDAPException 오류 코드를 지정합니다.

- com.iplanet.am.ldap.connection.num.retries

  기본값은 3입니다. LDAP를 성공적으로 다시 연결하기 위한 재시도 횟수를 지정합니다.

리버티 동맹 상호 작용

- com.sun.identity.liberty.interaction.htmlStyleSheetLocation

  값은 설치 중에 설정됩니다. 예: /opt/SUNWam/lib/is-html.xsl

  상호 작용 페이지를 HTML로 표시하는 데 사용되는 스타일 시트에 대한 경로를 지정합니다.

- com.sun.identity.liberty.interaction.wmlStyleSheetLocation

  값은 설치 중에 설정됩니다. 예: /opt/SUNWam/lib/is-wml.xsl

  상호 작용 페이지를 WML로 표시하는 데 사용되는 스타일 시트에 대한 경로를 지정합니다.

- com.sun.identity.liberty.interaction.wscSpecifiedInteractionChoice

  기본값은 interactIfNeeded입니다. 웹 서비스 소비자가 상호 작용에 참여하는지를 나타냅니다. 사용할 수 있는 값은 다음과 같습니다.

interactIfNeeded	필요한 경우에만 상호 작용합니다. 잘못된 값이 지정된 경우에도 사용됩니다.
doNotInteract	상호 작용하지 않습니다.
doNotInteractForData	데이터에 대해 상호 작용하지 않습니다.

- com.sun.identity.liberty.interaction.wscSpecifiedMaxInteractionTime

  기본값은 80입니다. 적절한 상호 작용 시간에 대한 웹 서비스 소비자의 기본 설정값을 초 단위로 표시합니다. 값을 지정하지 않거나 정수가 아닌 값이 지정된 경우 기본값을 사용합니다.

- com.sun.identity.liberty.interaction.wscWillEnforceHttpsCheck

  기본값은 yes입니다. HTTPS를 사용하는 URL로 요청을 리디렉션하는 요구 사항을 웹 서비스 소비자가 강제 적용할지 나타냅니다. 유효한 값은 yes 및 no입니다. 대소문자는 구분하지 않습니다. 리버티 사양에서는 yes 값이 필요합니다. 값을 지정하지 않으면 기본값이 사용됩니다.

- com.sun.identity.liberty.interaction.wscWillInlcudeUserInteractionHeader

  기본값은 yes입니다. 값을 지정하지 않으면 기본값이 사용됩니다. 웹 서비스 소비자가 userInteractionHeader를 포함하는지 나타냅니다. 허용되는 값은 yes 및 no입니다. 대소문자는 구분하지 않습니다.

- com.sun.identity.liberty.interaction.wscWillRedirect

  기본값은 yes입니다. 웹 서비스 소비자가 상호 작용을 위해 사용자를 리디렉션하는지 나타냅니다. 유효한 값은 yes 및 no입니다. 값이 지정되지 않은 경우 기본값이 사용됩니다.

- com.sun.identity.liberty.interaction.wspRedirectHandler

  값은 설치 중에 설정됩니다. 예:
  http://*hostName.domainName*.com:*portNumber*/amserver/WSPRedirectHandler

  사용자 에이전트 리디렉션에 따라 WSPRedirectHandlerServlet에서 리버티 WSF WSP-resource 소유자 상호 작용을 처리하는 데 사용할 URL을 지정합니다. 리버티 서비스 공급자가 실행되는 동일한 JVM에서 실행해야 합니다.

- com.sun.identity.liberty.interaction.wspRedirectTime

  기본값은 30입니다. 웹 서비스 제공자의 예상 상호 작용 시간입니다. 초 단위로 표시됩니다. 값을 지정하지 않거나 정수가 아닌 경우 기본값이 사용됩니다.

- com.sun.identity.liberty.interaction.wspWillEnforceHttpsCheck

  기본값은 yes입니다. 값을 지정하지 않으면 기본값이 사용됩니다. returnToURL에서 HTTPS를 사용하는 요구 사항을 웹 서비스 소비자가 강제 적용하는지를 나타냅니다. 유효한 값은 yes 및 no입니다. 리버티 사양에서는 yes 값이 필요합니다(대소문자를 구분하지 않음).

- com.sun.identity.liberty.interaction.

  wspWillEnforceReturnToHostEqualsRequestHost

  리버티 사양에서는 yes 값이 필요합니다. returnToHost 및 requestHost가 동일하도록 웹 서비스 소비자가 적용하는지를 나타냅니다. 유효한 값은 yes 및 no입니다.

- com.sun.identity.liberty.interaction.wspWillRedirect

  기본값은 yes입니다. 값을 지정하지 않으면 기본값이 사용됩니다. 웹 서비스 공급자가 상호 작용을 위해 사용자를 리디렉션하는지 나타냅니다. 유효한 값은 yes 및 no입니다. 대소문자를 구분하지 않습니다.

- com.sun.identity.liberty.interaction.wspWillRedirectForData

  기본값은 yes입니다. 값을 지정하지 않으면 기본값이 사용됩니다. 웹 서비스 공급자가 데이터의 상호 작용을 위해 사용자를 리디렉션하는지 나타냅니다. 유효한 값은 yes 및 no입니다. 대소문자를 구분하지 않습니다.

- com.sun.identity.liberty.ws.interaction.enable

  기본값은 false입니다.

- com.sun.identity.liberty.ws.jaxb.namespacePrefixMappingList

  기본값은

  =S=http://schemas.xmlsoap.org/soap/envelope/|sb=urn:liberty:sb:2003-08

  |pp=urn:liberty:id-sis-pp:2003-08|ispp=http://www.sun.com/identity/

  liberty/pp|is=urn:liberty:is:2003-08**입니다**

  . JAXB 컨텐트를 DOM 트리에 배열할 때 사용되는 이름 공간 접두사 매핑을 지정합니다. 구문은 prefix=namespace|prefix=namespace|... **입니다**.

- com.sun.identity.liberty.ws.jaxb.packageList

  JAXBContext를 구성할 때 사용되는 JAXB 패키지 목록을 지정합니다. 각 패키지를 콜론(:)으로구분합니다.

- com.sun.identity.liberty.ws.security.TokenProviderImpl

  기본값은
  com.sun.identity.liberty.ws.security.AMSecurityTokenProviderDescription입니다.

- com.sun.identity.liberty.ws.soap.certalias

  값은 설치 중에 설정됩니다. 리버티 SOAP 바인딩을 위한 SSL 연결에 사용될 클라이언트 인증서 별칭입니다.

- com.sun.identity.liberty.ws.soap.messageIDCacheCleanupInterval

  기본값은 60000입니다. 캐시 정리 이벤트를 시작하기까지 경과 시간(밀리초)을 지정합니다. 각 메시지는 중복을 피하기 위해 messageID와 함께 캐시에 저장됩니다. 메시지를 받은 시간 이후로 현재까지 지난 시간이 staleTimeLimit 값을 초과하면 메시지는 캐시에서 제거됩니다.

- com.sun.identity.liberty.ws.soap.staleTimeLimit

  기본값은 300000입니다. 메시지가 오래되어 더 이상 신뢰할 수 없는지를 결정합니다. 메시지 타임스탬프가 현재 타임스탬프보다 지정된 밀리초 이상으로 이전인 경우 오래된 메시지로 간주합니다.

- com.sun.identity.liberty.ws.soap.supportedActors

  기본값은 http://schemas.xmlsoap.org/soap/actor/next입니다. 지원되는 SOAP actor를 지정합니다. 각 actor는 파이프 문자(|)로 분리해야 합니다.

- com.sun.identity.liberty.ws.ta.certalias

  값은 설치 중에 설정됩니다. SAML 또는 SAML 서명에 사용되는 인증된 기관의 인증서 별칭을 지정합니다. 응답 메시지의 BEARER 토큰입니다.

- com.sun.identity.liberty.ws.wsc.certalias

  값은 설치 중에 설정됩니다. 현재 웹 서비스 클라이언트에 대한 웹 서비스 보안 토큰을 발행하기 위한 기본 인증서 별칭을 지정합니다.

- com.sun.identity.liberty.ws.ta.certalias

  값은 설치 중에 설정됩니다. SAML 또는 SAML 서명에 사용되는 인증된 기관의 인증서 별칭을 지정합니다. 응답 메시지의 BEARER 토큰입니다.

- com.sun.identity.liberty.ws.trustedca.certaliases

  값은 설치 중에 설정됩니다.

  인증된 CA에 대한 인증서 별칭을 지정합니다. 수신 요청의 SAML 또는 SAML BEARER 토큰입니다. 이 목록에 있는 인증된 CA가 메시지를 서명해야 합니다. 구문은 인증서 별칭 *1*[:발행인 *1*]|인증서 별칭 *2*[: 발행인 *2*]|....입니다.
  예: myalias1:myissuer1|myalias2|myalias3:myissuer3
  issuer값은 토큰이 서명 내에 KeyInfo를 가지고 있지 않은 경우에 사용됩니다. 이 목록에

토큰의 발행인이 있어야 하며 서명을 확인하는 데 해당 인증서 별칭이 사용됩니다. KeyInfo가 존재하면 키 저장소에는 KeyInfo와 일치하는 인증서 별칭이 있어야 하며 목록에 해당 인증서 별칭이 있어야 합니다.

- com.sun.identity.liberty.ws.security.TokenProviderImpl

  값은 설치 중에 설정됩니다. 보안 토큰 제공자에 대한 구현을 지정합니다.

- com.sun.identity.saml.removeassertion

  기본값은 true입니다. 역참조된 명제를 캐시에서 제거해야 하는지를 나타내는 플래그입니다. 아티팩트와 연결되어 생성되고 역참조되지 않은 명제에 적용됩니다.

로깅 서비스

- com.iplanet.am.logstatus

  로깅 설정 여부(ACTIVE 또는 INACTIVE)를 지정합니다. 설치 시 값은 ACTIVE로 설정됩니다.

AMConfig.properties에 추가할 수 있는 등록 정보 로깅

AMConfig.properties 파일에 속성을 추가하여 특정 로그 파일에 포함되는 세부 정도를 구성할 수 있습니다. 다음 형식을 사용합니다.

iplanet-am-logging.*logfileName* .level=*java.util.logging.Level*. 여기서 *logfileName*은 Access Manager 서비스의 로그 파일 이름(표 1 참조)이며 *java.util.logging.Level*은 허용되는 속성 값입니다. Access Manager 서비스는 정보 수준으로 로깅합니다. 또한 SAML 및 아이디 연합 서비스는 더욱 세부적인 수준(FINE, FINER, FINEST)으로 로깅합니다. 예:

```
iplanet-am-logging.amSSO.access.level=FINER
```

특정 로그 파일에 대한 로깅을 해제할 수도 있습니다. 예:

```
iplanet-am-logging.amConsole.access.evel=OFF
```

표 A–1 Access Manager 로그 파일

로그 파일 이름	로깅한 기록
amAdmin.access	성공한 amadmin 명령줄 이벤트
amAdmin.error	amadmin 명령줄 오류 이벤트
amAuthLog.access	Access Manager 정책 에이전트 관련 이벤트. 이 표 다음의 참고를 참조하십시오.
amAuthentication.access	성공한 인증 이벤트

표 A–1 Access Manager 로그 파일 *(계속)*

로그 파일 이름	로깅한 기록
amAuthentication.error	인증 실패
amConsole.access	콘솔 이벤트
amConsole.error	콘솔 오류 이벤트
amFederation.access	성공한 연합 이벤트
amFederation.error	연합 오류 이벤트
amPolicy.access	정책 저장소 허용 이벤트
amPolicy.error	정책 저장소 거부 이벤트
amSAML.access	성공한 SAML 이벤트
amSAML.error	SAME 오류 이벤트
amLiberty.access	성공한 리버티 이벤트
amLiberty.error	리버티 오류 이벤트
amSSO.access	단일 사인온 생성 및 제거
amSSO.error	싱글 사인온 오류 이벤트

주 – amAuthLog 파일 이름은 AMAgent.properties에서 정책 에이전트에 의해 결정됩니다. 웹 정책 에이전트의 경우 이 등록 정보는 com.sun.am.policy.agents.config.remote.log입니다. J2EE 정책 에이전트의 경우 이 등록 정보는 com.sun.identity.agents.config.remote.logfile입니다. 기본값은 amAuthLog.*host.domain.port*입니다. 여기서 *host.domain*은 정책 에이전트 웹 서버를 실행하는 호스트의 정규화된 호스트 이름이며 *port*는 해당 웹 서버의 포트 번호입니다. 여러 정책 에이전트를 배포한 경우 이 파일에 대해 여러 인스턴스를 가질 수 있습니다. com.sun.identity.agents.config.audit.accesstype 등록 정보(웹 및 J2EE 에이전트 모두에 대한)는 원격으로 로깅할 데이터를 결정합니다. 로깅된 데이터에는 정책 허용, 정책 거부, 허용과 거부 모두, 또는 허용과 거부 모두 아님이 포함될 수 있습니다.

이름 지정 서비스

- com.iplanet.am.naming.failover.url

  이 등록 정보는 더 이상 Access Manager 7.0에서 사용되지 않습니다.

- com.iplanet.am.naming.url

  값은 설치 중에 설정됩니다. 예:
  http://*hostName.domainName*.com:*portNumber*/amserver/namingservice

사용할 이름 지정 서비스의 URL을 지정합니다.

알림 서비스

다음 키를 사용하여 알림 스레드 풀을 구성합니다.

- `com.iplanet.am.notification.threadpool.size`

  기본값은 `10`입니다. 전체 스레드 수를 지정하여 풀의 크기를 정의합니다.

- `com.iplanet.am.notification.threadpool.threshold`

  기본값은 `100`입니다. 최대 작업 대기열 길이를 지정합니다.

  알림 작업이 들어오면 처리를 위해 작업 대기열로 보내집니다. 대기열이 최대 길이에 도달하면 이후의 수신 요청은 대기열이 비워질 때까지 `ThreadPoolException`과 함께 거부됩니다.

- `com.iplanet.am.notification.url`

  값은 설치 중에 설정됩니다. 예:
  `http://`*`hostName.domainName`*`.com:`*`portNumber`*`/amserver/notificationservice`

정책 에이전트

- `com.iplanet.am.policy.agents.url.deploymentDescriptor`

  값은 설치 중에 설정됩니다. 예: `AGENT_DEPLOY_URI`

- `com.sun.identity.agents.app.username`

  기본값은 `UrlAccessAgent`입니다. 응용 프로그램 인증 모듈에 사용할 아이디를 지정합니다.

- `com.sun.identity.agents.cache.size`

  기본값은 1000입니다. 자원 결과 캐시의 크기를 지정합니다. 캐시는 정책 에이전트가 설치된 서버에서 만들어집니다.

- `com.sun.identity.agents.header.attributes`

  기본값은 `cn,ou,o,mail,employeenumber,c`입니다. 정책 평가기가 반환할 정책 속성을 지정합니다. `a[,...]` 형식을 사용합니다. 이 예에서 `a`는 가져올 데이터 저장소 내의 속성입니다.

- `com.sun.identity.agents.logging.level`

  기본값은 `NONE`입니다. 정책 클라이언트 API 로깅 수준의 세분성을 제어합니다. 기본값은 `NONE`입니다. 사용 가능한 값은 다음과 같습니다.

  `ALLOW` `access allowed` 요청을 로깅합니다.

  `DENY` `access denied` 요청을 로깅합니다.

  `BOTH` `access allowed` 및 `access denied` 요청을 모두 로깅합니다.

NONE 요청을 로깅하지 않습니다.

- com.sun.identity.agents.notification.enabled

  기본값은 false입니다. 정책 클라이언트 API에 대한 알림을 활성화 또는 비활성화합니다.

- com.sun.identity.agents.notification.url

  정책 변경 알림을 등록하기 위해 정책 클라이언트 SDK에 의해 사용됩니다. 이 등록 정보를 잘못 구성하면 정책 알림이 비활성화됩니다.

- com.sun.identity.agents.polling.interval

  기본값은 3입니다. 폴링 간격(분)을 지정하며 이 간격마다 클라이언트 API 캐시에서 항목이 삭제됩니다.

- com.sun.identity.agents.resource.caseSensitive

  기본값은 false입니다. 설명

  정책을 평가하는 동안 대소문자를 구분 여부를 나타냅니다.

- com.sun.identity.agents.true.value

  정책 작업의 true 값을 나타냅니다. 응용 프로그램이 PolicyEvaluator.isAllowed 메소드에 액세스할 필요가 없는 경우에는 이 값이 무시될 수 있습니다. 이 값은 Access Manager의 정책 결정을 해석하는 방법을 나타냅니다. 기본값은 allow입니다.

- com.sun.identity.agents.resource.comparator.class

  기본값은 com.sun.identity.policy.plugins.URLResourceName입니다.

  자원 비교 클래스 이름을 지정합니다. 사용 가능한 구현 클래스는 다음과 같습니다. com.sun.identity.policy.plugins.PrefixResourceName 및 com.sun.identity.policy.plugins.URLResourceName.

- com.sun.identity.agents.resource.delimiter

  기본값은 백슬래시(/)입니다. 지원 이름을 위한 구분자를 지정합니다.

- com.sun.identity.agents.resource.wildcard

  기본값은 *입니다. 자원 이름을 위한 와일드카드를 지정합니다.

- com.sun.identity.agents.server.log.file.name

  기본값은 amRemotePolicyLog입니다. Access Manager로 가는 메시지를 기록하는 데 사용할 로그 파일의 이름을 지정합니다. 파일의 이름만 필요합니다. 파일의 디렉토리는 다른 Access Manager 구성 설정에 의해 결정됩니다.

- com.sun.identity.agents.use.wildcard

  기본값은 true입니다. 자원 이름 비교에 와일드카드를 사용할지 여부를 나타냅니다.

정책 클라이언트API

- com.sun.identity.policy.client.booleanActionValues

  iPlanetAMWebAgentService|POST|allow|deny

  기본값은 iPlanetAMWebAgentService|GET|allow|deny: 입니다.

  정책 작업 이름에 대한 부울 작업 값을 지정합니다. serviceName|actionName|trueValue|falseValue 형식을 사용합니다. 작업 이름의 값은 콜론(:)으로구분합니다.

- com.sun.identity.policy.client.cacheMode

  기본값은 self입니다. 클라이언트 정책 평가기에 대한 캐시 모드를 지정합니다. 유효한 값은 subtree 및 self입니다. subtree로 설정하면 정책 평가기는 모든 자원에 대한 정책 결정을 서버의 실제 요청된 자원의 루트에서 가져옵니다. self로 설정하면 정책 평가기는 실제 요청된 자원에 대해서만 서버에서 정책 결정을 가져 옵니다.

- com.sun.identity.policy.client.clockSkew

  정책 클라이언트 시스템 및 정책 서버 간의 시간차를 조정합니다. 이 등록 정보가 없고 정책 에이전트 시간이 정책 서버 시간과 다른 경우 때에 따라 잘못된 정책 결정이 일어날 수 있습니다. 시간 동기화 서비스를 실행하여 정책 서버 시간과 정책 클라이언트 시간을 가능한 정확하게 맞추어야 합니다. 이 등록 정보를 사용하여 시간 동기화 서비스 실행 여부와 관계없이 적은 시간차로 조정합니다. 시간차(초) = agentTime - serverTime. 정책 서버에서 해당 등록 정보를 주석으로 처리합니다. 해당 줄에 대한 주석을 해제하고 정책 클라이언트 시스템 또는 정책 에이전트 에이전트-서버 시간차(초)를 실행하는 시스템에서 적절한 값을 설정하십시오.

- com.sun.identity.policy.client.resourceComparators=

  serviceType=iPlanetAMWebAgentService|class=

  다른 서비스 이름에 사용할 ResourceComparators를 지정합니다. 값을 Access Manager 콘솔에서 복사합니다. Service Configuration > PolicyConfiguration > Global:ResourceComparator로 이동합니다. 콜론(:)을 구분자로 사용하여 Access Manager에서 여러 값을 연결합니다.

- com.sun.identity.policy.plugins.URLResourceName|wildcard

  기본값은 *|delimiter=/|caseSensitive=trueDescription입니다.

프로필 서비스

- com.iplanet.am.profile.host

  이 등록 정보는 더 이상 Access Manager 7에서 사용되지 않습니다. 이전 버전과의 호환을 위해서만 제공됩니다. 값은 설치 중에 설정됩니다. 예: *hostName.domainName*.com

- com.iplanet.am.profile.port

이 등록 정보는 더 이상 Access Manager 7에서 사용되지 않습니다. 이전 버전과의 호환을 위해서만 제공됩니다. 값은 설치 중에 설정됩니다. 예: 80

복제

다음 키를 사용하여 복제 설정을 구성합니다.

- com.iplanet.am.replica.delay.between.retries

  기본값은 1000입니다. 재시도 간격(밀리초)을 지정합니다.

- com.iplanet.am.replica.num.retries

  기본값은 0입니다. 재시도 횟수를 지정합니다.

SAML 서비스

- com.sun.identity.saml.assertion.version

  기본값은 1.1입니다. 사용되는 기본 SAML 버전을 지정합니다. 사용 가능한 값은 1.0 또는 1.1입니다.

- com.sun.identity.saml.checkcert

  기본값은 on입니다. KeyInfo에 포함된 인증서를 키 저장소의 인증서와 비교하기 위한 플래그. 키 저장소에 있는 인증서는 com.sun.identity.saml.xmlsig.keystore 등록 정보로 지정됩니다. 사용 가능한 값은 다음과 같습니다. on|off입니다. 플래그가 "on"이면 * XML 서명 검증을 위한 * 인증서가 키 저장소에 있어야 합니다. 플래그가 "off"이면 * 존재 여부 검사를 건너뜁니다 . */

  on XML 서명 검증을 위한 인증서가 키 저장소에 있어야 합니다.

  off 존재 여부 검사를 건너뜁니다.

- com.sun.identity.saml.protocol.version

  기본값은 1.1입니다. 사용되는 기본 SAML 버전을 지정합니다. 사용 가능한 값은 1.0 또는 1.1입니다.

- com.sun.identity.saml.removeassertion

- com.sun.identity.saml.request.maxContentLength

  기본값은 16384입니다. SAML에 사용할 HTTP Request의 최대 컨텐트 길이를 지정합니다.

- com.sun.identity.saml.xmlsig.certalias

  기본값은 test입니다. 설명

- com.sun.identity.saml.xmlsig.keypass

  값은 설치 중에 설정됩니다. 예: /etc/opt/SUNWam/config/.keypass

  SAML XML 키 비밀번호 파일의 경로를 지정합니다.

- com.sun.identity.saml.xmlsig.keystore

  값은 설치 중에 설정됩니다. 예: /etc/opt/SUNWam/config/keystore.jks

  SAML XML 키 저장소 비밀번호 파일의 경로를 지정합니다.

- com.sun.identity.saml.xmlsig.storepass

  값은 설치 중에 설정됩니다. 예: /etc/opt/SUNWam/config/.storepass

  SAML XML 키 storepass 파일의 경로를 지정합니다.

보안

- com.iplanet.security.encryptor

  기본값은 com.iplanet.services.util.JSSEncryption입니다. 암호화 클래스 구현을 지정합니다. 사용 가능한 클래스는com.iplanet.services.util.JCEEncryption 및 com.iplanet.services.util.JSSEncryption입니다.

- com.iplanet.security.SecureRandomFactoryImpl

  기본값은 com.iplanet.am.util.JSSSecureRandomFactoryImpl입니다. SecureRandomFactory에 대한 팩토리 클래스 이름을 지정합니다. 사용 가능한 구현 클래스는 다음과 같습니다. JSS를 사용하는 com.iplanet.am.util.JSSSecureRandomFactoryImpl 및 순수 Java를 사용하는 com.iplanet.am. util.SecureRandomFactoryImpl입니다.

- com.iplanet.security.SSLSocketFactoryImpl

  기본값은 com.iplanet.services.ldap.JSSSocketFactory입니다. LDAPSocketFactory에 대한 팩토리 클래스 이름을 지정합니다. 사용 가능한 클래스는JSS를 사용하는 com.iplanet.services.ldap.JSSSocketFactory 및 순수 Java를 사용하는 netscape.ldap.factory.JSSESocketFactory입니다.

- com.sun.identity.security.checkcaller

  기본값은 false입니다. Access Manager를 위한 Java 보안 관리자 권한 검사를 활성화 또는 비활성화합니다. 기본적으로 비활성화되어 있습니다. 활성화한 경우 Access Manager가 배포된 컨테이너의 Java 정책 파일을 적절하게 변경해야 합니다. 이러한 방법으로 Access Manager JAR 파일을 인증하고 민감한 작업을 수행할 수 있습니다. 자세한 내용은 com.sun.identity.security에 대한 Java API Reference(Javadoc) 항목을 참조하십시오.

- am.encryption.pwd

  값은 설치 중에 설정됩니다. 예: dSB9LkwPCSoXfIKHVMhIt3bKgibtsggd

  비밀번호 암호화 및 해독에 사용되는 키를 지정합니다.

세션 서비스

- com.iplanet.am.clientIPCheckEnabled

  기본값은 false입니다. 모든 SSOToken 생성 및 검증에서 클라이언트의 IP 주소를 확인할지 지정합니다.

- com.iplanet.am.session.client.polling.enable

  이 등록 정보는 읽기 전용입니다. 이 등록 정보 값을 수정하지 마십시오.

  기본값은 false입니다. 클라이언트 측 세션 폴링을 활성화합니다. 세션 폴링 모드 및 세션 알림 모드를 동시에 적용할 수 없습니다. 폴링 모드를 활성화한 경우 세션 알림은 자동으로 해제되며 그 반대의 경우입니다.

- com.iplanet.am.session.client.polling.period

  기본값은 180입니다. 폴링 기간(초)을 지정합니다.

- com.iplanet.am.session.httpSession.enabled

  기본값은 true입니다. httpSession 사용을 활성화 또는 비활성화합니다.

- com.iplanet.am.session.invalidsessionmaxtime

  기본값은 10입니다. 잘못된 세션이 만들어지고 사용자가 로그인하지 않은 경우 잘못된 세션이 세션 테이블에서 제거될 때까지의 시간(분)을 지정합니다. 이 값은 인증 모듈 등록 정보 파일의 시간 제한 값보다 항상 커야 합니다.

- com.iplanet.am.session.maxSessions

  기본값은 5000입니다. 허용되는 최대 동시 세션의 수를 지정합니다.

  최대 동시 세션 값이 제한값을 초과하면 로그인이 최대 세션 오류를 보냅니다.

- com.iplanet.am.session.purgedelay

  기본값은 60입니다. 세션 제거 작업의 지연 시간(분)을 지정합니다.

  이는 세션 시간이 초과된 후에 세션이 세션 서버에 계속 상주하는 연장 시간입니다. 클라이언트 응용 프로그램에서는 SSO API를 통해 세션 시간이 초과되었는지 확인하는 데 이 등록 정보를 사용합니다. 연장 시간이 끝나면 세션이 소멸됩니다. 사용자가 로그아웃하거나 Access Manager 구성 요소에 의해 명시적으로 세션이 소멸된 경우에는 연장 시간 동안 세션이 지속되지 않습니다. 이 연장 시간 동안 세션은 INVALID 상태입니다.

- com.sun.am.session.caseInsensitiveDN

  기본값은 true입니다. 에이전트 DN 비교값이 false이면 비교는 대소문자를 구분합니다.

- com.sun.am.session.enableHostLookUp

  기본값은 false입니다. 세션 로깅 동안 호스트 조회를 활성화 또는 비활성화합니다.

SMTP

- com.iplanet.am.smtphost

  기본값은 localhost입니다. 메일 서버 호스트를 지정합니다.

- com.iplanet.am.smtpport

  기본값은 25입니다. 메일 서버 포트를 지정합니다.

통계 서비스

- com.iplanet.am.stats.interval

  기본값은 60입니다. 통계 로깅 사이의 경과 시간(분)을 지정합니다. CPU 사용률 포화를 막기 위해 최소 5초로 설정됩니다. Access Manager는 5초보다 작은 값을 5초로 간주합니다.

- com.iplanet.services.stats.directory

  값은 설치 중에 설정됩니다. 예: /var/opt/SUNWam/stats 디버그 파일이 생성되는 디렉토리를 지정합니다.

- com.iplanet.services.stats.state

  기본값은 file입니다. 통계 로그의 위치를 지정합니다. 사용 가능한 값은 다음과 같습니다.

off	통계를 기록하지 않습니다.
file	지정된 디렉토리에 있는 파일에 통계를 기록합니다.
console	웹 서버 로그 파일에 통계를 기록합니다.

◆ ◆ ◆ 부 록 B

serverconfig.xml 파일

serverconfig.xml 파일은 Sun Java™ System Access Manager에서 데이터 저장소로 사용하는 Directory Server에 관련된 구성 정보를 제공합니다. 이 장에서는 파일의 요소를 설명하고 페일오버를 위해 파일을 구성하는 방법, 다중 인스턴스를 사용하는 방법, 콘솔 배포를 해제하고 서버에서 콘솔 파일을 제거하는 방법을 설명합니다. 이 장은 다음 내용으로 구성되어 있습니다.

개요

serverconfig.xml은 / *AccessManager-base* /SUNWam/config/ums에 있습니다. 여기에는 Identity SDK에서 Directory Server로의 LDAP 연결 풀을 구축하는 데 사용하는 매개 변수가 포함됩니다. 제품의 다른 기능에서는 이 파일을 사용하지 않습니다. 이 파일에서 두 명의 사용자가 정의됩니다. user1은 Directory Server 프록시 사용자이고 user2는 Directory Server 관리자입니다.

프록시 사용자

프록시 사용자는 어떤 사용자의 권한(예: 조직 관리자 또는 최종 사용자)도 취소할 수 있습니다. 프록시 사용자에게 연결이 바인딩되고 연결 풀이 생성됩니다. Access Manager는 cn=puser,ou=DSAME Users,dc=example,dc=com의 DN으로 프록시 사용자를 생성합니다. 이 사용자는 Directory Server에 대해 만든 모든 쿼리에 사용됩니다. Directory Server에서 이미 구성된 프록시 사용자 ACI의 혜택을 받으며 필요한 경우 사용자를 대신해 작업을 수행할 수 있습니다. 이는 모든 쿼리가 통과하는 열린 연결을 유지합니다(서비스 구성 검색, 조직 정보 등). 프록시 사용자의 비밀번호는 항상 암호화됩니다. 249 페이지 "프록시 사용자"에서는 암호화된 비밀번호가 있는 serverconfig.xml 내의 위치에 대해 설명합니다.

예 B–1 serverconfig.xml 내의 프록시 사용자

```
<User name="User1" type="proxy">
<DirDN>
cn=puser,ou=DSAME Users,dc=example,dc=com
</DirDN>
<DirPassword>
AQICkc3qIrCeZrpexyeoL4cdeXih4vv9aCZZ
</DirPassword>
</User>
```

관리자

dsameuser는 Access Manager SDK가 특정 사용자와 연결되지 않은 Directory Server에서 작업(예: 서비스 구성 정보 검색)을 수행할 때 바인딩 목적으로 사용됩니다. 249 페이지 "프록시 사용자"는 dsameuser를 대신하여 이러한 작업을 수행하지만 바인드가 먼저 dsameuser 자격 증명의 유효성을 검사해야 합니다. Access Manager는 설치 시에 cn=dsameuser,ou=DSAME Users,dc=example,dc=com을 생성합니다. 249 페이지 "프록시 사용자"에서는 암호화된 dsameuser 비밀번호가 있는 serverconfig.xml 내의 위치에 대해 설명합니다.

예 B–2 serverconfig.xml 내의 관리자

```
<User name="User2" type="admin">
<DirDN>
cn=dsameuser,ou=DSAME Users,dc=example,dc=com
</DirDN>
<DirPassword>
AQICkc3qIrCeZrpexyeoL4cdeXih4vv9aCZZ
</DirPassword>
</User>
```

server-config 정의 유형 문서

`server-config.dtd`는 `serverconfig.xml`의 구조를 정의합니다. 이 파일은 *AccessManager-base*`/SUNWam/dtd`에 있습니다. 이 절에서는 DTD의 주요 요소에 대해 설명합니다. 252 페이지 “MiscConfig 요소”는 `serverconfig.xml` 파일의 예입니다.

iPlanetDataAccessLayer 요소

*iPlanetDataAccessLayer*는 루트 요소입니다. 이 요소는 XML 파일별로 복수 서버 그룹을 정의할 수 있도록 해줍니다. 이 요소의 바로 다음 하위 요소는 251 페이지 “ServerGroup 요소”입니다. 이 요소에는 속성이 없습니다.

ServerGroup 요소

*ServerGroup*은 한 개 이상의 디렉토리 서버를 가리키는 포인터를 정의합니다. 디렉토리 서버는 마스터 서버 또는 복제 서버일 수 있습니다. *ServerGroup*을 한정하는 하위 요소에는 251 페이지 “Server 요소”, 251 페이지 “User 요소”, 252 페이지 “BaseDN 요소” 및 252 페이지 “MiscConfig 요소”가 있습니다. *ServerGroup*의 XML 속성에는 서버 그룹의 이름 및 LDAP 연결 풀에 대해 열 수 있는 최소(1) 및 최대(10) 연결의 수를 정의하는 *minConnPool*과 *maxConnPool*이 있습니다. ServerGroup 요소를 두 개 이상 정의할 수 없습니다.

주 – Access Manager는 연결 풀을 사용하여 Directory Server에 액세스합니다. 모든 연결은 Access Manager가 시작할 때 열리며 닫히지 않습니다. 연결은 모두 다시 사용됩니다.

Server 요소

*Server*는 특정 Directory Server 인스턴스를 정의합니다. 이 요소에는 하위 요소가 없습니다. *Server*의 필수 XML 속성에는 사용자에게 친숙한 서버 이름, 호스트 이름, Directory Server가 실행되는 포트 번호, 열려 있어야 하는 LDAP 연결 유형(단순 또는 SSL)이 있습니다.

주 – Server 요소를 사용한 자동 페일오버의 예는 253 페이지 “페일오버 또는 멀티마스터 구성”을 참조하십시오.

User 요소

*User*는 Directory Server 인스턴스용으로 구성된 사용자를 정의하는 하위 요소를 포함합니다. *User*를 한정하는 하위 요소에는 *DirDN* 및 *DirPassword*가 있습니다. 요소의 필수 XML 속성에는 사용자 이름 및 사용자 유형이 있습니다. 유형 값은 사용자의 권한 및 Directory Server 인스턴스에 대해 열 수 있는 연결 유형을 식별합니다. 다음과 같은 옵션이 있습니다.

- auth—Directory Server에 대해 인증할 사용자를 정의합니다.
- proxy—Directory Server 프록시 사용자를 정의합니다자세한 내용은 249 페이지 “프록시 사용자”를 참조하십시오.
- rebind—다시 바인딩하는 데 사용할 수 있는 자격 증명을 가진 사용자를 정의합니다.
- admin—Directory Server 관리 권한이 있는 사용자를 정의합니다. 자세한 내용은 250 페이지 “관리자”를 참조하십시오.

DirDN 요소

*DirDN*은 정의된 사용자의 LDAP 고유 이름을 포함합니다.

DirPassword 요소

*DirPassword*는 정의된 사용자의 암호화된 비밀번호를 포함합니다.

주의 – 비밀번호와 암호화 키를 배포에서 일관성 있게 유지하는 것이 중요합니다. 예를 들어 이 요소에 정의된 비밀번호는 Directory Server에도 저장됩니다. 한 곳에서 비밀번호를 변경하면 다른 곳에서도 업데이트해야 합니다. 이 비밀번호도 암호화됩니다. `am.encryption.pwd` 속성에서 정의된 암호화 키가 변경되면 `ampassword --encrypt` *password*를 사용해 `serverconfig.xml`에 있는 모든 비밀번호를 다시 암호화해야 합니다..

BaseDN 요소

*BaseDN*은 서버 그룹에 대한 기본 고유 이름을 지정합니다. 이 요소에는 하위 요소 및 XML 속성이 없습니다.

MiscConfig 요소

*MiscConfig*는 캐시 크기와 같은 LDAP JDK 기능을 정의하기 위한 자리 표시자입니다. 이 요소에는 하위 요소가 없습니다. 이 요소의 필수 XML 속성에는 해당 기능의 이름 및 정의된 값이 있습니다.

예 B–3 serverconfig.xml

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<!--
 Copyright (c) 2002 Sun Microsystems, Inc. All rights reserved.

 Use is subject to license terms.

-->
<iPlanetDataAccessLayer>
```

예 B–3 serverconfig.xml *(계속)*

```
        <ServerGroup name="default" minConnPool="1" maxConnPool="10">
                <Server name="Server1" host="
               ishost.domain_name" port="389"
type="SIMPLE" />
                <User name="User1" type="proxy">
                        <DirDN>
                                cn=puser,ou=DSAME Users,dc=example,dc=com
                        </DirDN>
                        <DirPassword>
                                AQICkc3qIrCeZrpexyeoL4cdeXih4vv9aCZZ
                        </DirPassword>
                </User>
                <User name="User2" type="admin">
                        <DirDN>
                                cn=dsameuser,ou=DSAME Users,dc=example,dc=com
                        </DirDN>
                        <DirPassword>
                                AQICkc3qIrCeZrpexyeoL4cdeXih4vv9aCZZ
                        </DirPassword>
                </User>
                <BaseDN>
                        dc=example,dc=com
                </BaseDN>
        </ServerGroup>
</iPlanetDataAccessLayer>
```

페일오버 또는 멀티마스터 구성

Access Manager는 serverconfig.xml에서 251 페이지 “ServerGroup 요소” 251 페이지 “Server 요소”로 정의한 모든 Directory Server로의 자동 페일오버 조치를 허용합니다. 페일오버 목적 또는 멀티마스터를 위해 두 개 이상의 서버를 구성할 수 있습니다. 첫 번째로 구성된 서버의 작동이 중단되면 두 번째로 구성된 서버가 작업을 인수합니다. 253 페이지 “페일오버 또는 멀티마스터 구성”에서는 자동 페일오버 구성을 포함하는 serverconfig.xml에 대해 설명합니다.

예 B–4 serverconfig.xml 내의 페일오버 구성

```
<?xml version="1.0" encoding="ISO-8859-1" standalone="yes"?>
<!--
PROPRIETARY/CONFIDENTIAL. Use of this product is subject to license terms.
Copyright 2002 Sun Microsystems, Inc. All rights reserved.
```

예 B–4 serverconfig.xml 내의 페일오버 구성 *(계속)*

```
-->
<iPlanetDataAccessLayer>
     <ServerGroup name="default" minConnPool="1" maxConnPool="10">
          <Server name="Server1" host="
            amhost1.domain_name" port="389" type="SIMPLE" />
          <Server name="Server2" host="
            amhost2.domain_name" port="389" type="SIMPLE" />
          <Server name="Server3" host="
            amhost3.domain_name" port="390" type="SIMPLE" />
          <User name="User1" type="proxy">
               <DirDN>
                    cn=puser,ou=DSAME Users,dc=example,dc=com
               </DirDN>
               <DirPassword>
                    AQIC5wM2LY4Sfcy+AQBQxghVwhBE92i78cqf
               </DirPassword>
          </User>
          <User name="User2" type="admin">
               <DirDN>
                    cn=dsameuser,ou=DSAME Users,dc=example,dc=com
               </DirDN>
               <DirPassword>
                    AQIC5wM2LY4Sfcy+AQBQxghVwhBE92i78cqf
               </DirPassword>
          </User>
          <BaseDN>
               o=isp
          </BaseDN>
     </ServerGroup>
</iPlanetDataAccessLayer>
```

◆ ◆ ◆ 부록 C

로그 파일 참조

이 부록에서는 Access Manager 기능의 각 영역에 대한 가능한 로그 파일을 나열합니다. 이 부록에 있는 표에서는 다음 로그 파일 항목에 대해 설명합니다.

- 아이디 — 로그 식별 번호
- 로그 수준 — 메시지의 로그 수준 속성
- 설명 — 로깅 메시지의 설명
- 데이터 — 메시지에 적용되는 데이터 유형
- 트리거 — 로그 파일 메시지의 원인
- 조치 — 자세한 내용을 얻기 위해 취해야 할 조치

로그 파일의 정의 및 위치는 **Sun Java System Access Manager 7 2005Q4 Technical Overview**에 설명되어 있습니다.

표 C–1 amAdmin 명령줄 유틸리티에 대한 로그 참조

아이디	로그 수준	설명	데이터	트리거	조치
1	정보	실패한 사용자 로그인	사용자 아이디	실패한 사용자 로그인	
2 TEST	정보	ADMINEXCEPTION 수신함	SSO 이름오류 메시지	관리자 요청을 처리하는 동안 ADMINEXCEPTION을 수신했습니다.	자세한 내용은 amAdmin 로그 파일 참조
3	정보	세션이 소멸됨	사용자 이름	세션이 소멸되었습니다.	
11	정보	서비스 스키마 로드됨	스키마 이름	서비스 스키마를 성공적으로 로드했습니다.	

표 C–1 amAdmin 명령줄 유틸리티에 대한 로그 참조 *(계속)*

아이디	로그 수준	설명	데이터	트리거	조치
12	정보	서비스가 삭제됨	서비스 이름	서비스를 성공적으로 삭제했습니다.	
13	정보	속성이 추가됨	속성 이름	속성이 성공적으로 추가되었습니다.	
21	정보	이 서비스에 대한 정책이 없음	서비스 이름	정책 규칙 플래그 삭제가 지정되었지만 서비스에 정책이 없습니다.	
22	정보	서비스 정책 스키마를 찾을 수 없음	서비스 이름	정책 규칙 플래그 삭제가 지정되었지만 서비스의 정책 스키마를 찾을 수 없습니다.	
23	정보	서비스 정책 삭제 중	서비스 이름	정책 규칙 플래그 삭제가 지정된 서비스를 삭제하고 있습니다.	
24	정보	서비스 정책 삭제를 완료함	서비스 이름	정책 규칙 플래그 삭제가 지정된 서비스를 삭제하고 있습니다.	
25	정보	조직에서 정책을 생성함	정책 이름조직 *DN*	조직 DN에서 정책을 생성했습니다.	
26	정보	조직에서 정책을 삭제함	정책 이름조직 *DN*	조직 DN에서 정책을 삭제했습니다.	

표 C–1 amAdmin 명령줄 유틸리티에 대한 로그 참조 *(계속)*

아이디	로그 수준	설명	데이터	트리거	조치
31	정보	Directory Server에 로켈의 자원 번들 추가	자원 번들 이름자원 로켈	로켈의 자원 번들을 Directory Server에 성공적으로 저장했습니다.	
32	정보	Directory Server에 기본 자원 번들 추가	자원 번들 이름	기본 자원 번들을 Directory Server에 성공적으로 저장했습니다.	
33	정보	Directory Server에서 로켈의 자원 번들을 삭제함	자원 번들 이름자원 로켈	로켈의 자원 번들을 Directory Server에서 성공적으로 삭제했습니다.	
34	정보	Directory Server에서 로켈의 기본 자원 번들을 삭제함	자원 번들 이름	기본 자원 번들을 Directory Server에서 성공적으로 삭제했습니다.	
41	정보	서비스의 서비스 스키마를 수정함	서비스 이름	서비스의 서비스 스키마를 성공적으로 수정했습니다.	
42	정보	서비스의 서비스 하위 스키마를 삭제함	하위 스키마의 이름서비스의 이름	서비스의 서비스 하위 스키마를 성공적으로 삭제했습니다.	
43	정보	서비스에 서비스 하위 스키마를 추가함	서비스 이름	서비스에 서비스 하위 스키마 를 성공적으로 추가했습니다.	

표 C–1 amAdmin 명령줄 유틸리티에 대한 로그 참조 *(계속)*

아이디	로그 수준	설명	데이터	트리거	조치
44	정보	서비스에 하위 구성을 추가함	하위 구성의 이름서비스의 이름	서비스에 하위 구성을 성공적으로 추가했습니다.	
45	정보	서비스의 하위 구성을 수정함	하위 구성의 이름서비스의 이름	서비스의 하위 구성을 성공적으로 수정했습니다.	
46	정보	서비스의 하위 구성 삭제됨	하위 구성의 이름서비스의 이름	서비스의 하위 구성을 성공적으로 삭제했습니다.	
47	정보	서비스의 모든 서비스 구성을 삭제함	서비스 이름	서비스의 모든 서비스 구성을 성공적으로 삭제했습니다.	
91	정보	조직에서 서비스 하위 구성 수정	하위 구성 이름서비스 이름조직 *DN*	조직에서 서비스 하위 구성을 성공적으로 수정했습니다.	
92	정보	조직에서 서비스 하위 구성을 추가함	하위 구성 이름서비스 이름조직 *DN*	조직에 서비스 하위 구성을 성공적으로 추가했습니다.	
93	정보	조직에서 서비스 하위 구성을 삭제함	하위 구성 이름서비스 이름조직 *DN*	조직에서 서비스 하위 구성을 성공적으로 삭제했습니다.	
94	정보	조직에서 원격 공급자를 생성함	공급자 이름조직 *DN*	조직에서 원격 공급자를 성공적으로 생성했습니다.	
95	정보	조직에서 원격 공급자를 수정함	공급자 이름조직 *DN*	조직에서 원격 공급자를 성공적으로 수정했습니다.	

표 C–1 amAdmin 명령줄 유틸리티에 대한 로그 참조 *(계속)*

아이디	로그 수준	설명	데이터	트리거	조치
96	정보	조직에서 호스트된 공급자를 수정함	공급자 이름조직 *DN*	조직에서 호스트된 공급자를 성공적으로 수정했습니다.	
97	정보	조직에서 호스트된 공급자를 생성함	공급자 이름조직 *DN*	조직에서 호스트된 공급자를 성공적으로 생성했습니다.	자세한 내용은 아이디 저장소 로그 아래에서 참조
98	정보	조직에서 원격 공급자를 삭제함	공급자 이름조직 *DN*	조직에서 원격 공급자를 성공적으로 삭제했습니다.	
99	정보	조직에서 인증 도메인을 생성함	COT(circle of trust) 이름조직 *DN*	조직에서 인증 도메인을 성공적으로 생성했습니다.	
100	정보	조직에서 인증 도메인을 삭제함	COT(circle of trust) 이름조직 *DN*	조직에서 인증 도메인을 성공적으로 삭제했습니다.	
101	정보	조직에서 인증 도메인을 수정함	COT(circle of trust) 이름조직 *DN*	조직에서 인증 도메인을 성공적으로 수정했습니다.	
102	정보	서비스 템플리트 수정 시도	서비스 템플리트의 DN	서비스 템플리트 수정을 시도했습니다.	
103	정보	서비스 템플리트를 수정함	서비스 템플리트의 DN	서비스 템플리트를 성공적으로 수정했습니다.	
104	정보	서비스 템플리트 제거 시도	서비스 템플리트의 DN	서비스 템플리트 제거를 시도했습니다.	

표 C–1 amAdmin 명령줄 유틸리티에 대한 로그 참조 *(계속)*

아이디	로그 수준	설명	데이터	트리거	조치
105	정보	서비스 템플리트를 제거함	서비스 템플리트의 DN	서비스 템플리트를 성공적으로 제거했습니다.	
106	정보	서비스 템플리트 추가 시도	서비스 템플리트의 DN	서비스 템플리트 추가를 시도했습니다.	
107	정보	서비스 템플리트를 추가함	서비스 템플리트의 DN	서비스 템플리트를 성공적으로 추가했습니다.	
108	정보	그룹에 중첩 그룹 추가 시도	추가할 그룹 이름 그룹을 포함하는 *DN*	그룹에 중첩 그룹 추가를 시도했습니다.	
109	정보	그룹에 중첩 그룹을 추가함	추가할 그룹 이름 그룹을 포함하는 *DN*	그룹에 중첩 그룹을 성공적으로 추가했습니다.	
110	정보	그룹 또는 역할에 사용자 추가 시도	사용자의 이름대상 그룹 또는 역할	그룹 또는 역할에 사용자 추가를 시도했습니다.	
111	정보	그룹 또는 역할에 사용자를 추가함	사용자의 이름대상 그룹 또는 역할	그룹 또는 역할에 사용자를 성공적으로 추가했습니다.	
112	정보	엔티티 생성 시도	엔티티의 DN	엔티티 생성을 시도했습니다.	
113	정보	엔티티를 생성함	엔티티의 현지화된 이름엔티티의 *DN*	엔티티를 생성함	
114	정보	역할 생성 시도	역할 DN	역할 생성을 시도했습니다.	
115	정보	역할을 생성함	역할 이름	역할을 생성했습니다.	

표 C–1 amAdmin 명령줄 유틸리티에 대한 로그 참조 *(계속)*

아이디	로그 수준	설명	데이터	트리거	조치
116	정보	그룹 컨테이너 생성 시도	그룹 컨테이너 이름	그룹 컨테이너 생성을 시도했습니다.	
117	정보	그룹 컨테이너 생성	그룹 컨테이너 이름	그룹 컨테이너를 생성했습니다.	
118	정보	그룹 생성 시도	그룹 이름	그룹 생성을 시도했습니다.	
119	정보	그룹 생성	그룹 이름	그룹을 생성했습니다.	
120	정보	사용자 컨테이너 생성 시도	사용자 컨테이너의 DN	사용자 컨테이너 생성을 시도했습니다.	
121	정보	사용자 컨테이너 생성	사용자 컨테이너의 DN	사용자 컨테이너를 생성했습니다.	
122	정보	조직 또는 역할에서 서비스 템플리트 생성 시도	서비스 템플리트 이름조직 또는 역할 이름	조직 또는 역할에서 서비스 템플리트 생성을 시도했습니다.	
123	정보	조직 또는 역할에서 서비스 템플리트 생성	서비스 템플리트 이름조직 또는 역할 이름	조직 또는 역할에서 서비스 템플리트를 생성했습니다.	
124	정보	컨테이너 생성 시도	컨테이너 이름	컨테이너 생성을 시도했습니다.	
125	정보	컨테이너 생성	컨테이너 이름	컨테이너를 생성했습니다.	
126	정보	사용자 생성 시도	사용자 이름	사용자 생성을 시도했습니다.	
127	정보	사용자 생성	사용자 이름	사용자를 생성했습니다.	

표 C–1 amAdmin 명령줄 유틸리티에 대한 로그 참조 *(계속)*

아이디	로그 수준	설명	데이터	트리거	조치
128	정보	엔티티 삭제 시도	엔티티의 DN	엔티티 삭제를 시도했습니다.	
129	정보	엔티티 삭제	엔티티의 현지화된 이름엔티티의 *DN*	엔티티를 삭제했습니다.	
130	정보	사용자 컨테이너 삭제 시도	사용자 컨테이너의 DN	사용자 컨테이너 삭제를 시도했습니다.	
131	정보	사용자 컨테이너 삭제	사용자 컨테이너의 DN	사용자 컨테이너를 삭제했습니다.	
132	정보	역할 삭제 시도	역할 이름	역할 삭제를 시도했습니다.	
133	정보	역할 삭제	역할 이름	역할을 삭제했습니다.	
134	정보	조직에서 서비스 템플리트 삭제 시도	서비스 템플리트 이름조직 이름	조직에서 서비스 템플리트 삭제를 시도했습니다.	
135	정보	조직에서 서비스 템플리트 삭제	서비스 템플리트 이름조직 이름	조직에서 서비스 템플리트를 삭제했습니다.	
136	정보	컨테이너 삭제 시도	컨테이너 이름	컨테이너 삭제를 시도했습니다.	
137	정보	컨테이너 삭제	컨테이너 이름	컨테이너를 삭제했습니다.	
138	정보	엔티티 수정 시도	엔티티의 현지화된 이름엔티티의 *DN*	엔티티 수정을 시도했습니다.	
139	정보	엔티티 수정	엔티티의 현지화된 이름엔티티의 *DN*	엔티티를 수정했습니다.	

표 C–1 amAdmin 명령줄 유틸리티에 대한 로그 참조 *(계속)*

아이디	로그 수준	설명	데이터	트리거	조치
140	정보	사용자 컨테이너 수정 시도	사용자 컨테이너의 DN	사용자 컨테이너 수정을 시도했습니다.	
141	정보	사용자 컨테이너 수정	사용자 컨테이너의 DN	사용자 컨테이너를 수정했습니다.	
142	정보	컨테이너 수정 시도	컨테이너 이름	컨테이너 수정을 시도했습니다.	
143	정보	컨테이너 수정	컨테이너 이름	컨테이너를 수정했습니다.	
144	정보	조직에 서비스 등록 시도	서비스 이름조직 이름	조직에 서비스 등록을 시도했습니다.	
145	정보	조직에 서비스 등록	서비스 이름조직 이름	조직에 서비스를 등록했습니다.	
146	정보	조직에 서비스 등록 취소 시도	서비스 이름조직 이름	조직에 서비스 등록 취소를 시도했습니다.	
147	정보	조직에 서비스 등록 취소	서비스 이름조직 이름	조직에 서비스 등록을 취소했습니다.	
148	정보	그룹 수정 시도	그룹 이름	그룹 수정을 시도했습니다.	
149	정보	그룹 수정	그룹 이름	그룹을 수정했습니다.	
150	정보	그룹에서 중첩된 그룹 제거 시도	중첩 그룹 이름그룹 이름	그룹에서 중첩된 그룹 제거를 시도했습니다.	
151	정보	그룹에서 중첩된 그룹 제거	중첩 그룹 이름그룹 이름	그룹에서 중첩된 그룹을 제거했습니다.	
152	정보	그룹 삭제 시도	그룹 이름	그룹 삭제를 시도했습니다.	

표 C–1 amAdmin 명령줄 유틸리티에 대한 로그 참조 *(계속)*

아이디	로그 수준	설명	데이터	트리거	조치
153	정보	그룹 삭제	그룹 이름	그룹을 삭제했습니다.	
154	정보	역할에서 사용자 제거 시도	사용자 이름역할 이름	역할에서 사용자 제거를 시도했습니다.	
155	정보	역할에서 사용자 제거	사용자 이름역할 이름	역할에서 사용자를 제거했습니다.	
156	정보	그룹에서 사용자 제거 시도	사용자 이름그룹 이름	그룹에서 사용자 제거를 시도했습니다.	
157	정보	그룹에서 사용자 제거	사용자 이름그룹 이름	그룹에서 사용자를 제거했습니다.	
201	정보	영역에서 아이디에 아이디 추가 시도	추가할 아이디 이름추가할 아이디 유형아이디 이름을 추가할 대상아이디 유형을 추가할 대상영역 이름	영역에서 아이디에 아이디를 추가하려고 시도했습니다.	
202	정보	영역에서 아이디에 아이디 추가	추가할 아이디 이름추가할 아이디 유형아이디 이름을 추가할 대상아이디 유형을 추가할 대상영역 이름	영역에서 아이디에 아이디를 추가했습니다.	
203	정보	영역에서 아이디에 서비스 할당 시도	서비스 이름 아이디 이름아이디 유형영역 이름	영역에서 아이디에 서비스를 할당하려고 시도했습니다.	
204	정보	영역에서 아이디에 서비스 할당	서비스 이름 아이디 이름아이디 유형영역 이름	영역에서 아이디에 서비스를 할당했습니다.	

표 C–1 amAdmin 명령줄 유틸리티에 대한 로그 참조 *(계속)*

아이디	로그 수준	설명	데이터	트리거	조치
205	정보	영역에서 한 유형의 여러 아이디 생성 시도	아이디 유형영역 이름	영역에서 한 유형의 여러 아이디를 생성하려고 시도했습니다.	
206	정보	영역에서 한 유형의 여러 아이디 생성	아이디 유형영역 이름	영역에서 한 유형의 여러 아이디를 생성했습니다.	
207	정보	영역에서 한 유형의 아이디 생성 시도	아이디 이름 아이디 유형영역 이름	영역에서 한 유형의 아이디를 생성하려고 시도했습니다.	
208	정보	영역에서 한 유형의 아이디 생성	아이디 이름 아이디 유형영역 이름	영역에서 한 유형의 아이디를 생성했습니다.	
209	정보	영역에서 한 유형의 아이디 삭제 시도	아이디 이름 아이디 유형영역 이름	영역에서 한 유형의 아이디를 삭제하려고 시도했습니다.	
210	정보	영역에서 한 유형의 아이디 삭제	아이디 이름 아이디 유형영역 이름	영역에서 한 유형의 아이디를 삭제했습니다.	
211	정보	영역에서 아이디에 대한 서비스 수정 시도	서비스 이름 아이디 유형아이디 이름영역 이름	영역에서 아이디에 대한 서비스를 수정하려고 시도했습니다.	
212	정보	영역에서 아이디에 대한 서비스 수정	서비스 이름 아이디 유형아이디 이름영역 이름	영역에서 아이디에 대한 서비스를 수정했습니다.	

표 C–1 amAdmin 명령줄 유틸리티에 대한 로그 참조 *(계속)*

아이디	로그 수준	설명	데이터	트리거	조치
213	정보	영역에 있는 아이디에서 아이디를 제거 시도	제거할 아이디 이름 제거할 아이디 유형제거할 대상 아이디 이름제거할 대상 아이디 유형영역 이름	영역에 있는 아이디에서 아이디를 제거하려고 시도했습니다.	
214	정보	영역에 있는 아이디에서 아이디 제거	제거할 아이디 이름 제거할 아이디 유형제거할 대상 아이디 이름제거할 대상 아이디 유형영역 이름	영역에 있는 아이디에서 아이디를 제거했습니다.	
215	정보	영역에서 아이디에 대한 서비스 속성 설정 시도	서비스 이름 아이디 유형아이디 이름영역 이름	영역에서 아이디에 대한 서비스 속성을 설정하려고 시도했습니다.	
216	정보	영역에서 아이디에 대한 서비스 속성 설정	서비스 이름 아이디 유형아이디 이름영역 이름	영역에서 아이디에 대한 서비스 속성을 설정했습니다.	
217	정보	영역에 있는 아이디에서 서비스 할당 해제 시도	서비스 이름 아이디 유형아이디 이름영역 이름	영역에 있는 아이디에서 서비스를 할당 해제하려고 시도했습니다.	
218	정보	영역에 있는 아이디에서 서비스 할당 해제	서비스 이름 아이디 유형아이디 이름영역 이름	영역에 있는 아이디에서 서비스를 할당 해제했습니다.	
219	정보	조직 생성 시도	조직 이름	조직 생성을 시도했습니다.	
220	정보	조직 생성	조직 이름	조직을 생성했습니다.	
221	정보	하위 조직 삭제 시도	하위 조직 이름	하위 조직 삭제 시도됨	

표 C–1 amAdmin 명령줄 유틸리티에 대한 로그 참조 *(계속)*

아이디	로그 수준	설명	데이터	트리거	조치
222	정보	하위 조직 삭제	하위 조직 이름	하위 조직 삭제됨	
223	정보	역할 수정 시도	역할 이름	역할 수정을 시도했습니다.	
224	정보	역할 수정	역할 이름	역할을 수정했습니다.	
225	정보	하위 조직 수정 시도	하위 조직 이름	하위 조직 수정 시도됨	
226	정보	하위 조직 수정	하위 조직 이름	하위 조직 수정됨	
227	정보	사용자 삭제 시도	사용자 이름	사용자 삭제를 시도했습니다.	
228	정보	사용자 삭제	사용자 이름	사용자를 삭제했습니다.	
229	정보	사용자 수정 시도	사용자 이름	사용자 수정을 시도했습니다.	
230	정보	사용자 수정	사용자 이름	사용자를 수정했습니다.	
231	정보	영역에서 서비스 속성에 값 추가 시도	속성 이름 서비스 이름영역 이름	영역에서 서비스 속성에 값을 추가하려고 시도했습니다.	
232	정보	영역에서 서비스 속성에 값 추가	속성 이름 서비스 이름영역 이름	영역에서 서비스 속성에 값을 추가했습니다.	
233	정보	영역에 서비스 할당 시도	서비스 이름영역 이름	영역에 서비스를 할당하려고 시도했습니다.	
234	정보	영역에 서비스 할당	서비스 이름영역 이름	영역에 서비스를 할당했습니다.	
235	정보	영역 생성 시도	생성된 영역 이름상위 영역 이름	영역 생성을 시도했습니다.	

표 C–1 amAdmin 명령줄 유틸리티에 대한 로그 참조 *(계속)*

아이디	로그 수준	설명	데이터	트리거	조치
236	정보	영역 생성	생성된 영역 이름상위 영역 이름	영역을 생성했습니다.	
237	정보	영역 삭제	재귀 또는 아님삭제된 영역 이름	영역을 삭제했습니다.	
238	정보	영역 삭제	재귀 또는 아님삭제된 영역 이름	영역을 삭제했습니다.	
239	정보	영역에서 서비스 수정 시도	서비스 이름영역 이름	영역에서 서비스를 수정하려고 시도했습니다.	
240	정보	영역에서 서비스 수정	서비스 이름영역 이름	영역에서 서비스를 수정했습니다.	
241	정보	영역의 서비스에서 속성 제거 시도	속성 이름 서비스 이름영역 이름	영역의 서비스에서 속성을 제거하려고 시도했습니다.	
242	정보	영역의 서비스에서 속성 제거	속성 이름 서비스 이름영역 이름	영역의 서비스에서 속성을 제거했습니다.	
243	정보	영역에 있는 서비스의 속성에서 값 제거 시도	속성 이름 서비스 이름영역 이름	영역에 있는 서비스의 속성에서 값을 제거하려고 시도했습니다.	
244	정보	영역에 있는 서비스의 속성에서 값 제거	속성 이름 서비스 이름영역 이름	영역에 있는 서비스의 속성에서 값을 제거했습니다.	
245	정보	영역에서 서비스에 대한 속성 설정 시도	서비스 이름영역 이름	영역에서 서비스에 대한 속성을 설정하려고 시도했습니다.	

표 C–1 amAdmin 명령줄 유틸리티에 대한 로그 참조 *(계속)*

아이디	로그 수준	설명	데이터	트리거	조치
246	정보	영역에서 서비스에 대한 속성 설정	서비스 이름영역 이름	영역에서 서비스에 대한 속성 설정	
247	정보	영역에서 서비스 할당 해제 시도	서비스 이름영역 이름	영역에서 서비스를 할당 해제하려고 시도했습니다.	
248	정보	영역에서 서비스 할당 해제	서비스 이름영역 이름	영역에서 서비스를 할당 해제했습니다.	
249	정보	조직 구성에 서비스 할당 시도	서비스 이름영역 이름	조직 구성에 서비스를 할당하려고 시도했습니다.	
250	정보	조직 구성에 서비스 할당	서비스 이름영역 이름	조직 구성에 서비스를 할당했습니다.	
251	정보	완료되지 않은 조직 구성에 서비스 할당	서비스 이름영역 이름	조직 구성에 서비스를 할당했지만 해당 서비스가 조직 구성의 할당 가능한 서비스가 아닙니다.	
252	정보	완료되지 않은 영역에 서비스 할당	서비스 이름영역 이름	영역에 서비스를 할당했지만 해당 서비스가 영역의 할당 가능 서비스가 아닙니다.	
253	정보	조직 구성에서 서비스 할당 제거 시도	서비스 이름영역 이름	조직 구성에서 서비스를 할당 해제하려고 시도했습니다.	
254	정보	조직 구성에서 서비스 할당 해제	서비스 이름영역 이름	조직 구성에서 서비스를 할당 해제했습니다.	

표 C–1 amAdmin 명령줄 유틸리티에 대한 로그 참조 *(계속)*

아이디	로그 수준	설명	데이터	트리거	조치
255	정보	조직 구성 또는 영역 이외에서 서비스 할당 해제	서비스 이름영역 이름	조직 구성 또는 영역 이외에서 서비스의 할당 해제를 요청했습니다.	
256	정보	조직 구성에서 서비스 수정 시도	서비스 이름영역 이름	조직 구성에서 서비스를 수정하려고 시도했습니다.	
257	정보	조직 구성에서 서비스 수정	서비스 이름영역 이름	조직 구성에서 서비스를 수정했습니다.	
258	정보	조직 구성 또는 영역 이외에서 서비스 수정	서비스 이름영역 이름	조직 구성 또는 영역 이외에서 서비스를 수정하려고 시도했습니다.	

표 C–2 인증에 대한 로그 참조

아이디	로그 수준	설명	데이터	트리거	조치
100	정보	인증 성공	메시지	유효한 자격 증명으로 사용자를 인증했습니다.	
101	정보	사용자 기반 인증 성공	메시지인증 유형사용자 이름	유효한 자격 증명으로 사용자를 인증했습니다.	
102	정보	역할 기반 인증 성공	메시지인증 유형역할 이름	유효한 자격 증명으로 역할에 속한 사용자를 인증했습니다.	
103	정보	서비스 기반 인증 성공	메시지인증 유형서비스 이름	영역에 구성된 서비스에 대해 유효한 자격 증명으로 사용자를 인증했습니다.	

표 C–2 인증에 대한 로그 참조 (계속)

아이디	로그 수준	설명	데이터	트리거	조치
104	정보	인증 수준 기반 인증 성공	메시지인증 유형인증 수준 값	인증 수준 값이 지정된 인증 수준보다 높거나 같은 하나 이상의 인증 모듈에 대한 유효한 자격 증명으로 사용자를 인증했습니다.	
105	정보	모듈 기반 인증 성공	메시지인증 유형모듈 이름	영역에서 인증 모듈에 대한 유효한 자격 증명으로 사용자를 인증했습니다.	
200	정보	인증에 실패함	오류 메시지	잘못된/유효하지 않은 자격 증명 제시됨사용자 잠금/비활성	필수 인증 모듈에 대한 올바른/유효한 자격 증명을 입력합니다.
201	정보	인증에 실패함	오류 메시지	유효하지 않은 자격 증명을 입력했습니다.	올바른 비밀번호를 입력하십시오.
202	정보	인증에 실패함	오류 메시지	이름이 지정된 구성(인증 체인)이 없습니다.	이 조직에 대해 이름이 지정된 구성을 생성 및 구성하십시오.
203	정보	인증에 실패함	오류 메시지	이 사용자에 대한 사용자 프로필이 없습니다.	사용자가 구성된 데이터 저장소 플러그인에 없으므로 이 영역/조직에 대한 데이터 저장소 플러그인을 올바로 구성하십시오.
204	정보	인증에 실패함	오류 메시지	이 사용자가 활성 상태가 아닙니다.	사용자를 활성화하십시오.

표 C–2 인증에 대한 로그 참조 *(계속)*

아이디	로그 수준	설명	데이터	트리거	조치
205	정보	인증에 실패함	오류 메시지	최대 시도 실패 횟수를 초과했습니다. 사용자가 잠겨졌습니다.	시스템 관리자에게 문의하십시오.
206	정보	인증에 실패함	오류 메시지	사용자 계정이 만료되었습니다.	시스템 관리자에게 문의하십시오.
207	정보	인증에 실패함	오류 메시지	로그인이 시간 초과되었습니다.	다시 로그인을 시도하십시오.
208	정보	인증에 실패함	오류 메시지	인증 모듈이 거부되었습니다.	이 모듈을 구성하거나 다른 모듈을 사용하십시오.
209	정보	인증에 실패함	오류 메시지	최대 허용 세션 수에 대한 제한값에 도달했습니다.	세션을 로그아웃하거나 제한값을 높이십시오.
210	정보	인증에 실패함	오류 메시지	조직/영역이 없습니다.	유효한 조직/영역을 사용하십시오.
211	정보	인증에 실패함	오류 메시지	조직/영역이 활성 상태가 아닙니다.	조직/영역을 활성화하십시오.
212	정보	인증에 실패함	오류 메시지	세션을 생성할 수 없습니다.	세션 서비스가 구성되어 있고 최대 세션 수에 도달하지 않았는지 확인하십시오.
213	정보	사용자 기반 인증에 실패함	오류 메시지인증 유형사용자 이름	사용자에 대해 구성된 인증 구성(하나 이상의 인증 모듈 체인)이 없습니다.잘못된/유효하지 않은 자격 증명 제시됨사용자 잠김/비활성	사용자에 대한 인증 구성 구성(하나 이상의 인증 모듈 체인)필수 유효 자격 증명에 대한 올바른/유효한 자격 증명 입력

표 C–2 인증에 대한 로그 참조 *(계속)*

아이디	로그 수준	설명	데이터	트리거	조치
214	정보	인증에 실패함	오류 메시지인증 유형사용자 이름	사용자 기반 인증입니다. 유효하지 않은 자격 증명을 입력했습니다.	올바른 비밀번호를 입력하십시오.
215	정보	인증에 실패함	오류 메시지인증 유형사용자 이름	이 사용자에 대해 이름이 지정된 구성(인증 체인)이 없습니다.	이 사용자에 대해 이름이 지정된 구성을 생성 및 구성하십시오.
216	정보	인증에 실패함	오류 메시지인증 유형사용자 이름	사용자 기반 인증입니다. 이 사용자에 대한 사용자 프로필이 없습니다.	사용자가 구성된 데이터 저장소 플러그인에 없으므로 이 영역/조직에 대한 데이터 저장소 플러그인을 올바로 구성하십시오.
217	정보	인증에 실패함	오류 메시지인증 유형사용자 이름	사용자 기반 인증입니다. 이 사용자가 활성 상태가 아닙니다.	사용자를 활성화하십시오.
218	정보	인증에 실패함	오류 메시지인증 유형사용자 이름	사용자 기반 인증입니다. 최대 시도 실패 횟수를 초과했습니다. 사용자가 잠겼습니다.	시스템 관리자에게 문의하십시오.
219	정보	인증에 실패함	오류 메시지인증 유형사용자 이름	사용자 기반 인증입니다. 사용자 계정이 만료되었습니다.	시스템 관리자에게 문의하십시오.
220	정보	인증에 실패함	오류 메시지인증 유형사용자 이름	사용자 기반 인증입니다. 로그인이 시간 초과되었습니다.	다시 로그인을 시도하십시오.

표 C–2 인증에 대한 로그 참조 *(계속)*

아이디	로그 수준	설명	데이터	트리거	조치
221	정보	인증에 실패함	오류 메시지인증 유형사용자 이름	사용자 기반 인증입니다. 인증 모듈이 거부되었습니다.	이 모듈을 구성하거나 다른 모듈을 사용하십시오.
222	정보	인증에 실패함	오류 메시지인증 유형사용자 이름	사용자 기반 인증입니다. 최대 허용 세션 수에 대한 제한값에 도달했습니다.	세션을 로그아웃하거나 제한값을 높이십시오.
223	정보	인증에 실패함	오류 메시지인증 유형사용자 이름	사용자 기반 인증입니다. 조직/영역이 없습니다.	유효한 조직/영역을 사용하십시오.
224	정보	인증에 실패함	오류 메시지인증 유형사용자 이름	사용자 기반 인증입니다. 조직/영역이 활성 상태가 아닙니다.	조직/영역을 활성화하십시오.
225	정보	인증에 실패함	오류 메시지인증 유형사용자 이름	사용자 기반 인증입니다. 세션을 생성할 수 없습니다.	세션 서비스가 구성되어 있고 최대 세션 수에 도달하지 않았는지 확인하십시오.
226	정보	역할 기반 인증에 실패함	오류 메시지인증 유형역할 이름	역할에 대해 구성된 인증 구성(하나 이상의 인증 모듈 체인) 없음잘못된/유효하지 않은 자격 증명 제시됨사용자가 이 역할에 속해 있지 않음사용자 잠김/비활성	역할에 대한 인증 구성(하나 이상의 인증 모듈 체인)을 구성하십시오. 적절한 인증 모듈에 대한 올바른/유효한 자격 증명 입력인증 사용자에 이 역할 할당
227	정보	인증에 실패함	오류 메시지인증 유형역할 이름	역할 기반 인증입니다. 유효하지 않은 자격 증명을 입력했습니다.	올바른 비밀번호를 입력하십시오.

표 C–2 인증에 대한 로그 참조 *(계속)*

아이디	로그 수준	설명	데이터	트리거	조치
228	정보	인증에 실패함	오류 메시지인증 유형역할 이름	이 역할에 대해 이름이 지정된 구성(인증 체인)이 없습니다.	이 역할에 대해 이름이 지정된 구성을 생성 및 구성하십시오.
229	정보	인증에 실패함	오류 메시지인증 유형역할 이름	역할 기반 인증입니다. 이 사용자에 대한 사용자 프로필이 없습니다.	사용자가 구성된 데이터 저장소 플러그인에 없으므로 이 영역/조직에 대한 데이터 저장소 플러그인을 올바로 구성하십시오.
230	정보	인증에 실패함	오류 메시지인증 유형역할 이름	역할 기반 인증입니다. 이 사용자가 활성 상태가 아닙니다.	사용자를 활성화하십시오.
231	정보	인증에 실패함	오류 메시지인증 유형역할 이름	역할 기반 인증입니다. 최대 시도 실패 횟수를 초과했습니다. 사용자가 잠겼습니다.	시스템 관리자에게 문의하십시오.
232	정보	인증에 실패함	오류 메시지인증 유형역할 이름	역할 기반 인증입니다. 사용자 계정이 만료되었습니다.	시스템 관리자에게 문의하십시오.
233	정보	인증에 실패함	오류 메시지인증 유형역할 이름	역할 기반 인증입니다. 로그인이 시간 초과되었습니다.	다시 로그인을 시도하십시오.
234	정보	인증에 실패함	오류 메시지인증 유형역할 이름	역할 기반 인증입니다. 인증 모듈이 거부되었습니다.	이 모듈을 구성하거나 다른 모듈을 사용하십시오.

표 C–2 인증에 대한 로그 참조 *(계속)*

아이디	로그 수준	설명	데이터	트리거	조치
235	정보	인증에 실패함	오류 메시지인증 유형역할 이름	역할 기반 인증입니다. 최대 허용 세션 수에 대한 제한값에 도달했습니다.	세션을 로그아웃하거나 제한값을 높이십시오.
236	정보	인증에 실패함	오류 메시지인증 유형역할 이름	역할 기반 인증입니다. 조직/영역이 없습니다.	유효한 조직/영역을 사용하십시오.
237	정보	인증에 실패함	오류 메시지인증 유형역할 이름	역할 기반 인증입니다. 조직/영역이 활성 상태가 아닙니다.	조직/영역을 활성화하십시오.
238	정보	인증에 실패함	오류 메시지인증 유형역할 이름	역할 기반 인증입니다. 세션을 생성할 수 없습니다.	세션 서비스가 구성되어 있고 최대 세션 수에 도달하지 않았는지 확인하십시오.
239	정보	인증에 실패함	오류 메시지인증 유형역할 이름	역할 기반 인증입니다. 사용자가 이 역할에 속하지 않습니다.	이 역할에 사용자를 추가하십시오.
240	정보	서버 기반 인증에 실패함	오류 메시지인증 유형서비스 이름	서비스에 대해 구성된 인증 구성(하나 이상의 인증 모듈 체인)이 없습니다.잘못된/유효하지 않은 자격 증명 제시됨사용자 잠김/비활성	서비스에 대한 인증 구성(하나 이상의 인증 모듈 체인) 구성필수 인증 모듈에 대한 올바른 유효한 자격 증명 입력
241	정보	인증에 실패함	오류 메시지인증 유형서비스 이름	서비스 기반 인증입니다. 유효하지 않은 자격 증명을 입력했습니다.	올바른 비밀번호를 입력하십시오.

표 C–2 인증에 대한 로그 참조 (계속)

아이디	로그 수준	설명	데이터	트리거	조치
242	정보	인증에 실패함	오류 메시지인증 유형서비스 이름	이 서비스 이름과 함께 이름이 지정된 구성(인증 체인)이 없습니다.	이름이 지정된 구성을 생성하고 구성하십시오.
243	정보	인증에 실패함	오류 메시지인증 유형서비스 이름	서비스 기반 인증입니다. 이 사용자에 대한 사용자 프로필이 없습니다.	사용자가 구성된 데이터 저장소 플러그인에 없으므로 이 영역/조직에 대한 데이터 저장소 플러그인을 올바로 구성하십시오.
244	정보	인증에 실패함	오류 메시지인증 유형서비스 이름	서비스 기반 인증입니다. 이 사용자가 활성 상태가 아닙니다.	사용자를 활성화하십시오.
245	정보	인증에 실패함	오류 메시지인증 유형서비스 이름	서비스 기반 인증입니다. 최대 시도 실패 횟수를 초과했습니다. 사용자가 잠겼습니다.	시스템 관리자에게 문의하십시오.
246	정보	인증에 실패함	오류 메시지인증 유형서비스 이름	서비스 기반 인증입니다. 사용자 계정이 만료되었습니다.	시스템 관리자에게 문의하십시오.
247	정보	인증에 실패함	오류 메시지인증 유형서비스 이름	서비스 기반 인증입니다. 로그인이 시간 초과되었습니다.	다시 로그인을 시도하십시오.
248	정보	인증에 실패함	오류 메시지인증 유형서비스 이름	서비스 기반 인증입니다. 인증 모듈이 거부되었습니다.	이 모듈을 구성하거나 다른 모듈을 사용하십시오.

표 C–2 인증에 대한 로그 참조 *(계속)*

아이디	로그 수준	설명	데이터	트리거	조치
249	정보	인증에 실패함	오류 메시지인증 유형서비스 이름	서비스 기반 인증입니다. 서비스가 없습니다.	유효한 서비스만 사용하십시오.
250	정보	인증에 실패함	오류 메시지인증 유형서비스 이름	서비스 기반 인증입니다. 최대 허용 세션 수에 대한 제한값에 도달했습니다.	세션을 로그아웃하거나 제한값을 높이십시오.
251	정보	인증에 실패함	오류 메시지인증 유형서비스 이름	서비스 기반 인증입니다. 조직/영역이 없습니다.	유효한 조직/영역을 사용하십시오.
252	정보	인증에 실패함	오류 메시지인증 유형서비스 이름	서비스 기반 인증입니다. 조직/영역이 활성 상태가 아닙니다.	조직/영역을 활성화하십시오.
253	정보	인증에 실패함	오류 메시지인증 유형서비스 이름	서비스 기반 인증입니다. 세션을 생성할 수 없습니다.	세션 서비스가 구성되어 있고 최대 세션 수에 도달하지 않았는지 확인하십시오.
254	정보	인증 수준 기반 인증에 실패함	오류 메시지인증 유형인증 수준 값	인증 수준 값이 지정된 인증 수준보다 크거나 같은 인증 모듈이 없음인증 수준이 지정된 인증 수준보다 크거나 같은 하나 이상의 인증 모듈에 잘못된/유효하지 않은 자격 증명 제시됨사용자 잠김/비활성	인증 수준 값이 필수 인증 수준보다 크거나 같은 하나 이상의 인증 모듈 구성인증 수준이 지정된 인증 수준보다 크거나 같은 하나 이상의 인증 모듈에 대한 올바른/유효한 자격 증명 입력

표 C–2 인증에 대한 로그 참조 *(계속)*

아이디	로그 수준	설명	데이터	트리거	조치
255	정보	인증에 실패함	오류 메시지인증 유형인증 수준 값	수준 기반 인증입니다. 유효하지 않은 자격 증명을 입력했습니다.	올바른 비밀번호를 입력하십시오.
256	정보	인증에 실패함	오류 메시지인증 유형인증 수준 값	수준 기반 인증입니다. 사용 가능한 인증 구성이 없습니다.	인증 구성을 생성하십시오.
257	정보	인증에 실패함	오류 메시지인증 유형인증 수준 값	수준 기반 인증입니다. 이 사용자에 대한 사용자 프로필이 없습니다.	사용자가 구성된 데이터 저장소 플러그인에 없으므로 이 영역/조직에 대한 데이터 저장소 플러그인을 올바로 구성하십시오.
258	정보	인증에 실패함	오류 메시지인증 유형인증 수준 값	수준 기반 인증입니다. 이 사용자가 활성 상태가 아닙니다.	사용자를 활성화하십시오.
259	정보	인증에 실패함	오류 메시지인증 유형인증 수준 값	수준 기반 인증입니다. 최대 시도 실패 횟수를 초과했습니다. 사용자가 잠겼습니다.	시스템 관리자에게 문의하십시오.
260	정보	인증에 실패함	오류 메시지인증 유형인증 수준 값	수준 기반 인증입니다. 사용자 계정이 만료되었습니다.	시스템 관리자에게 문의하십시오.
261	정보	인증에 실패함	오류 메시지인증 유형인증 수준 값	수준 기반 인증입니다. 로그인이 시간 초과되었습니다.	다시 로그인을 시도하십시오.

표 C–2 인증에 대한 로그 참조 *(계속)*

아이디	로그 수준	설명	데이터	트리거	조치
262	정보	인증에 실패함	오류 메시지인증 유형인증 수준 값	수준 기반 인증입니다. 인증 모듈이 거부되었습니다.	이 모듈을 구성하거나 다른 모듈을 사용하십시오.
263	정보	인증에 실패함	오류 메시지인증 유형인증 수준 값	수준 기반 인증입니다. 인증 수준이 잘못되었습니다.	유효한 인증 수준을 지정하십시오.
264	정보	인증에 실패함	오류 메시지인증 유형인증 수준 값	수준 기반 인증입니다. 최대 허용 세션 수에 대한 제한값에 도달했습니다.	세션을 로그아웃하거나 제한값을 높이십시오.
265	정보	인증에 실패함	오류 메시지인증 유형인증 수준 값	수준 기반 인증입니다. 조직/영역이 없습니다.	유효한 조직/영역을 사용하십시오.
266	정보	인증에 실패함	오류 메시지인증 유형인증 수준 값	수준 기반 인증입니다. 조직/영역이 활성 상태가 아닙니다.	조직/영역을 활성화하십시오.
267	정보	인증에 실패함	오류 메시지인증 유형인증 수준 값	수준 기반 인증입니다. 세션을 생성할 수 없습니다.	세션 서비스가 구성되어 있고 최대 세션 수에 도달하지 않았는지 확인하십시오.
268	정보	모듈 기반 인증에 실패함	오류 메시지인증 유형모듈 이름	영역에 모듈이 등록/구성되지 않음잘못된/유효하지 않은 자격 증명 제시됨사용자 잠김/비활성	영역에 인증 모듈 등록/구성인증 모듈에 대한 올바른/유효한 자격 증명 입력
269	정보	인증에 실패함	오류 메시지인증 유형모듈 이름	모듈 기반 인증입니다. 유효하지 않은 자격 증명을 입력했습니다.	올바른 비밀번호를 입력하십시오.

표 C–2 인증에 대한 로그 참조 *(계속)*

아이디	로그 수준	설명	데이터	트리거	조치
270	정보	인증에 실패함	오류 메시지인증 유형모듈 이름	모듈 기반 인증입니다. 이 사용자에 대한 사용자 프로필이 없습니다.	사용자가 구성된 데이터 저장소 플러그인에 없으므로 이 영역/조직에 대한 데이터 저장소 플러그인을 올바로 구성하십시오.
271	정보	인증에 실패함	오류 메시지인증 유형모듈 이름	모듈 기반 인증입니다. 이 사용자가 활성 상태가 아닙니다.	사용자를 활성화하십시오.
272	정보	인증에 실패함	오류 메시지인증 유형모듈 이름	모듈 기반 인증입니다. 최대 시도 실패 횟수를 초과했습니다. 사용자가 잠겼습니다.	시스템 관리자에게 문의하십시오.
273	정보	인증에 실패함	오류 메시지인증 유형모듈 이름	모듈 기반 인증입니다. 사용자 계정이 만료되었습니다.	시스템 관리자에게 문의하십시오.
274	정보	인증에 실패함	오류 메시지인증 유형모듈 이름	모듈 기반 인증입니다. 로그인이 시간 초과되었습니다.	다시 로그인을 시도하십시오.
275	정보	인증에 실패함	오류 메시지인증 유형모듈 이름	모듈 기반 인증입니다. 인증 모듈이 거부되었습니다.	이 모듈을 구성하거나 다른 모듈을 사용하십시오.
276	정보	인증에 실패함	오류 메시지인증 유형모듈 이름	모듈 기반 인증입니다. 최대 허용 세션 수에 대한 제한값에 도달했습니다.	세션을 로그아웃하거나 제한값을 높이십시오.

표 C–2 인증에 대한 로그 참조 *(계속)*

아이디	로그 수준	설명	데이터	트리거	조치
277	정보	인증에 실패함	오류 메시지인증 유형모듈 이름	모듈 기반 인증입니다. 조직/영역이 없습니다.	유효한 조직/영역을 사용하십시오.
278	정보	인증에 실패함	오류 메시지인증 유형모듈 이름	모듈 기반 인증입니다. 조직/영역이 활성 상태가 아닙니다.	조직/영역을 활성화하십시오.
279	정보	인증에 실패함	오류 메시지인증 유형모듈 이름	모듈 기반 인증입니다. 세션을 생성할 수 없습니다.	세션 서비스가 구성되어 있고 최대 세션 수에 도달하지 않았는지 확인하십시오.
300	정보	사용자 로그아웃 성공	메시지	사용자가 로그아웃했습니다.	
301	정보	사용자 기반 인증에서 사용자 로그아웃 성공	메시지인증 유형사용자 이름	사용자가 로그아웃했습니다.	
302	정보	역할 기반 인증에서 사용자 로그아웃 성공	메시지인증 유형역할 이름	이 역할에 속한 사용자가 로그아웃했습니다.	
303	정보	서비스 기반 인증에서 사용자 로그아웃 성공	메시지인증 유형서비스 이름	영역에 구성된 서비스에서 사용자가 로그아웃했습니다.	
304	정보	인증 수준 기반 인증에서 사용자 로그아웃 성공	메시지인증 유형인증 수준 값	인증 수준 값이 지정된 인증 수준 값보다 높거나 같은 하나 이상의 인증 모듈에서 사용자가 로그아웃했습니다.	
305	정보	모듈 기반 인증에서 사용자 로그아웃 성공	메시지인증 유형모듈 이름	영역의 인증 모듈에서 사용자가 로그아웃했습니다.	

표 C–3 Access Manager 콘솔에 대한 로그 참조

아이디	로그 수준	설명	데이터	트리거	조치
1	정보	아이디 생성 시도	아이디 이름아이디 유형영역 이름	영역 만들기 페이지에서 만들기 버튼을 누르십시오.	
2	정보	아이디를 생성함	아이디 이름아이디 유형영역 이름	영역 만들기 페이지에서 만들기 버튼을 누르십시오.	
3	심각	아이디를 생성하지 못함	아이디 이름아이디 유형영역 이름오류 메시지	영역에서 아이디를 생성할 수 없습니다. 사용자의 단일 사인온 토큰이 만료되었거나 사용자에게 이 작업을 수행할 권한이 사용자에게 없을 수 있습니다.	자세한 내용은 데이터 저장소 로그를 참조하십시오.
4	심각	아이디를 생성하지 못함	아이디 이름아이디 유형영역 이름오류 메시지	데이터 저장소 오류로 인해 영역에서 아이디를 생성할 수 없습니다.	자세한 내용은 데이터 저장소 로그를 참조하십시오.
11	정보	아이디 검색 시도	기본 영역아이디 유형검색 패턴검색 크기 제한검색 시간 제한	아이디 검색 보기에서 검색 버튼을 누르십시오.	
12	정보	아이디를 검색함	기본 영역아이디 유형검색 패턴검색 크기 제한검색 시간 제한	아이디 검색 보기에서 검색 버튼을 누르십시오.	

표 C–3 Access Manager 콘솔에 대한 로그 참조 *(계속)*

아이디	로그 수준	설명	데이터	트리거	조치
13	심각	아이디를 검색하지 못함	아이디 이름아이디 유형영역 이름오류 메시지	영역에서 아이디에 대한 검색 작업을 수행할 수 없습니다. 사용자의 단일 사인온 토큰이 만료되었거나 사용자에게 이 작업을 수행할 권한이 없을 수 있습니다.	자세한 내용은 데이터 저장소 로그를 참조하십시오.
14	심각	아이디를 검색하지 못함	아이디 이름아이디 유형영역 이름오류 메시지	데이터 저장소 오류로 인해 영역에서 아이디에 대한 검색 작업을 수행할 수 없습니다.	자세한 내용은 데이터 저장소 로그를 참조하십시오.
21	정보	아이디의 속성 값 읽기 시도	아이디 이름속성 이름	아이디 프로필 보기를 확인하십시오.	
22	정보	아이디의 속성 값을 읽음	아이디 이름속성 이름	아이디 프로필 보기를 확인하십시오.	
23	심각	아이디의 속성 값을 읽지 못함	아이디 이름속성 이름오류 메시지	아이디의 속성 값을 읽을 수 없습니다. 사용자의 단일 사인온 토큰이 만료되었거나 사용자에게 이 작업을 수행할 권한이 없을 수 있습니다.	자세한 내용은 데이터 저장소 로그를 참조하십시오.
24	심각	아이디의 속성 값을 읽지 못함	아이디 이름속성 이름오류 메시지	데이터 저장소 오류로 인해 아이디의 속성 값을 읽을 수 없습니다.	자세한 내용은 데이터 저장소 로그를 참조하십시오.

표 C–3 Access Manager 콘솔에 대한 로그 참조 *(계속)*

아이디	로그 수준	설명	데이터	트리거	조치
25	심각	아이디의 속성 값을 읽지 못함	아이디 이름속성 이름오류 메시지	예외 서비스 관리자 API로 인해 아이디의 속성 값을 읽을 수 없습니다.	자세한 내용은 서비스 관리 로그를 참조하십시오.
31	정보	아이디의 속성 값 수정 시도	아이디 이름속성 이름	아이디 프로필 보기에서 저장 버튼을 누르십시오.	
32	정보	아이디의 속성 값을 수정함	아이디 이름속성 이름	아이디 프로필 보기에서 저장 버튼을 누르십시오.	
33	심각	아이디의 속성 값을 수정하지 못함	아이디 이름속성 이름오류 메시지	아이디의 속성 값을 수정할 수 없습니다. 사용자의 단일 사인온 토큰이 만료되었거나 사용자에게 이 작업을 수행할 권한이 없을 수 있습니다.	자세한 내용은 데이터 저장소 로그를 참조하십시오.
34	심각	아이디의 속성 값을 수정하지 못함	아이디 이름속성 이름오류 메시지	데이터 저장소 오류로 인해 아이디의 속성 값을 수정할 수 없습니다.	자세한 내용은 데이터 저장소 로그를 참조하십시오.
41	정보	아이디 삭제 시도	영역 이름삭제할 아이디의 이름	아이디 검색 보기에서 삭제 버튼을 누릅니다.	
42	정보	아이디를 삭제함	영역 이름삭제할 아이디의 이름	아이디 검색 보기에서 삭제 버튼을 누릅니다.	

표 C–3 Access Manager 콘솔에 대한 로그 참조 *(계속)*

아이디	로그 수준	설명	데이터	트리거	조치
43	심각	아이디를 삭제하지 못함	영역 이름삭제할 아이디의 이름오류 메시지	아이디를 삭제할 수 없습니다. 사용자의 단일 사인온 토큰이 만료되었거나 사용자에게 이 작업을 수행할 권한이 없을 수 있습니다.	자세한 내용은 데이터 저장소 로그를 참조하십시오.
44	심각	아이디를 삭제하지 못함	영역 이름삭제할 아이디의 이름오류 메시지	데이터 저장소 오류로 인해 아이디를 삭제할 수 없습니다.	자세한 내용은 데이터 저장소 로그를 참조하십시오.
51	정보	아이디의 구성원 정보 읽기 시도	아이디 이름구성원 아이디 유형	아이디의 구성원 페이지를 봅니다.	
52	정보	아이디의 구성원 정보를 읽음	아이디 이름구성원 아이디 유형	아이디의 구성원 페이지를 봅니다.	
53	심각	아이디의 구성원 정보를 읽지 못함	아이디 이름구성원 아이디 유형오류 메시지	아이디의 구성원 정보를 읽을 수 없습니다. 사용자의 단일 사인온 토큰이 만료되었거나 사용자에게 이 작업을 수행할 권한이 없을 수 있습니다.	자세한 내용은 데이터 저장소 로그를 참조하십시오.
54	심각	아이디의 구성원 정보를 읽지 못함	아이디 이름구성원 아이디 유형오류 메시지	데이터 저장소 오류로 인해 아이디의 구성원 정보를 읽을 수 없습니다.	자세한 내용은 데이터 저장소 로그를 참조하십시오.

표 C–3 Access Manager 콘솔에 대한 로그 참조 *(계속)*

아이디	로그 수준	설명	데이터	트리거	조치
61	정보	아이디의 구성원 정보 읽기 시도	아이디 이름구성원 아이디 유형	아이디의 구성원 페이지를 봅니다.	
62	정보	아이디의 구성원 정보를 읽음	아이디 이름구성원 아이디 유형	아이디의 구성원 페이지를 봅니다.	
63	심각	아이디의 구성원 정보를 읽지 못함	아이디 이름구성원 아이디 유형오류 메시지	아이디의 구성원 정보를 읽을 수 없습니다. 사용자의 단일 사인온 토큰이 만료되었거나 사용자에게 이 작업을 수행할 권한이 없을 수 있습니다.	자세한 내용은 데이터 저장소 로그를 참조하십시오.
64	심각	아이디의 구성원 정보를 읽지 못함	아이디 이름구성원 아이디 유형오류 메시지	데이터 저장소 오류로 인해 아이디의 구성원 정보를 읽을 수 없습니다.	자세한 내용은 데이터 저장소 로그를 참조하십시오.
71	정보	아이디에 구성원 추가 시도	아이디 이름추가할 아이디의 이름.	아이디에 추가할 구성원을 선택합니다.	
72	정보	아이디에 구성원을 추가함	아이디 이름추가한 아이디의 이름	아이디에 추가할 구성원을 선택합니다.	

표 C–3 Access Manager 콘솔에 대한 로그 참조 *(계속)*

아이디	로그 수준	설명	데이터	트리거	조치
73	심각	아이디에 구성원을 추가하지 못함	아이디 이름추가할 아이디의 이름오류 메시지	아이디에 구성원을 추가할 수 없습니다. 사용자의 단일 사인온 토큰이 만료되었거나 이 작업을 수행할 권한이 사용자에게 없을 수 있습니다.	자세한 내용은 데이터 저장소 로그를 참조하십시오.
74	심각	아이디에 구성원을 추가하지 못함	아이디 이름추가할 아이디의 이름오류 메시지	데이터 저장소 오류로 인해 아이디에 구성원을 추가할 수 없습니다.	자세한 내용은 데이터 저장소 로그를 참조하십시오.
81	정보	아이디에서 구성원 제거 시도	아이디 이름제거할 아이디의 이름	아이디에서 제거할 구성원을 선택합니다.	
82	정보	아이디에서 구성원을 제거함	아이디 이름제거한 아이디의 이름	아이디에서 제거할 구성원을 선택합니다.	
83	심각	아이디에서 구성원을 제거하지 못함	아이디 이름제거할 아이디의 이름오류 메시지	아이디에서 구성원을 제거할 수 없습니다. 사용자의 단일 사인온 토큰이 만료되었거나 사용자에게 이 작업을 수행할 권한이 사용자에게 없을 수 있습니다.	자세한 내용은 데이터 저장소 로그를 참조하십시오.

표 C–3 Access Manager 콘솔에 대한 로그 참조 *(계속)*

아이디	로그 수준	설명	데이터	트리거	조치
84	심각	아이디에서 구성원을 제거하지 못함	아이디 이름제거할 아이디의 이름오류 메시지	데이터 저장소 오류로 인해 아이디에서 구성원을 제거할 수 없습니다.	자세한 내용은 데이터 저장소 로그를 참조하십시오.
91	정보	아이디의 할당된 서비스 이름 읽기 시도	아이디 이름	아이디의 서비스 할당 보기에서 추가 버튼을 누릅니다.	
92	정보	아이디의 할당된 서비스 이름을 읽음	아이디 이름	아이디의 서비스 할당 보기에서 추가 버튼을 누릅니다.	
93	심각	아이디의 할당된 서비스 이름을 읽지 못함	아이디 이름오류 메시지	아이디의 할당된 서비스 이름을 읽을 수 없습니다. 사용자의 단일 사인온 토큰이 만료되었거나 사용자에게 이 작업을 수행할 권한이 없을 수 있습니다.	자세한 내용은 데이터 저장소 로그를 참조하십시오.
94	심각	아이디의 할당된 서비스 이름을 읽지 못함	아이디 이름오류 메시지	데이터 저장소 오류로 인해 아이디의 할당된 서비스 이름을 읽을 수 없습니다.	자세한 내용은 데이터 저장소 로그를 참조하십시오.
101	정보	아이디의 할당 가능 서비스 이름 읽기 시도	아이디 이름	아이디의 서비스 페이지를 봅니다.	
102	정보	아이디의 할당 가능 서비스 이름을 읽음	아이디 이름	아이디의 서비스 페이지를 봅니다.	

표 C–3 Access Manager 콘솔에 대한 로그 참조 *(계속)*

아이디	로그 수준	설명	데이터	트리거	조치
103	심각	아이디의 할당 가능 서비스 이름 읽지 못함	아이디 이름오류 메시지	아이디의 할당 가능 서비스 이름을 읽을 수 없습니다. 사용자의 단일 사인온 토큰이 만료되었거나 사용자에게 이 작업을 수행할 권한이 없을 수 있습니다.	자세한 내용은 데이터 저장소 로그를 참조하십시오.
104	심각	아이디의 할당 가능 서비스 이름 읽지 못함	아이디 이름오류 메시지	데이터 저장소 오류로 인해 아이디의 할당 가능 서비스 이름을 읽을 수 없습니다.	자세한 내용은 데이터 저장소 로그를 참조하십시오.
111	정보	아이디에 서비스 할당 시도	아이디 이름서비스 이름	아이디의 서비스 보기에서 추가 버튼을 누릅니다.	
112	정보	아이디에 서비스를 할당함	아이디 이름서비스 이름	아이디의 서비스 보기에서 추가 버튼을 누릅니다.	
113	심각	아이디에 서비스를 할당하지 못함	아이디 이름서비스 이름오류 메시지	아이디에 서비스를 할당할 수 없습니다. 사용자의 단일 사인온 토큰이 만료되었거나 사용자에게 이 작업을 수행할 권한이 없을 수 있습니다.	자세한 내용은 데이터 저장소 로그를 참조하십시오.

표 C–3 Access Manager 콘솔에 대한 로그 참조 *(계속)*

아이디	로그 수준	설명	데이터	트리거	조치
114	심각	아이디에 서비스를 할당하지 못함	아이디 이름서비스 이름오류 메시지	데이터 저장소 오류로 인해 아이디에 서비스를 할당할 수 없습니다.	자세한 내용은 데이터 저장소 로그를 참조하십시오.
121	정보	아이디에서 서비스 할당 해제 시도	아이디 이름서비스 이름	아이디의 서비스 보기에서 제거 버튼을 누릅니다.	
122	정보	아이디에서 서비스를 할당 해제함	아이디 이름서비스 이름	아이디의 서비스 보기에서 제거 버튼을 누릅니다.	
123	심각	아이디에서 서비스를 할당 해제하지 못함	아이디 이름서비스 이름오류 메시지	아이디에서 서비스를 할당 해제할 수 없습니다. 사용자의 단일 사인온 토큰이 만료되었거나 사용자에게 이 작업을 수행할 권한이 사용자에게 없을 수 있습니다.	자세한 내용은 데이터 저장소 로그를 참조하십시오.
124	심각	아이디에서 서비스를 할당 해제하지 못함	아이디 이름서비스 이름오류 메시지	데이터 저장소 오류로 인해 아이디에서 서비스를 할당 해제할 수 없습니다.	자세한 내용은 데이터 저장소 로그를 참조하십시오.
131	정보	아이디의 서비스 속성 값 읽기 시도	아이디 이름서비스 이름	아이디의 서비스 프로필 보기를 봅니다.	
132	정보	아이디의 서비스 속성 값을 읽음	아이디 이름서비스 이름	아이디의 서비스 프로필 보기를 봅니다.	

표 C–3 Access Manager 콘솔에 대한 로그 참조 *(계속)*

아이디	로그 수준	설명	데이터	트리거	조치
133	심각	아이디의 서비스 속성 값을 읽지 못함	아이디 이름서비스 이름오류 메시지	아이디의 서비스 속성 값을 읽을 수 없습니다. 사용자의 단일 사인온 토큰이 만료되었거나 사용자에게 이 작업을 수행할 권한이 없을 수 있습니다.	자세한 내용은 데이터 저장소 로그를 참조하십시오.
134	심각	아이디의 서비스 속성 값을 읽지 못함	아이디 이름서비스 이름오류 메시지	데이터 저장소 오류로 인해 아이디의 서비스 속성 값을 읽을 수 없습니다.	자세한 내용은 데이터 저장소 로그를 참조하십시오.
141	정보	아이디에 서비스 속성 값 쓰기 시도	아이디 이름서비스 이름	아이디의 서비스 프로필 보기에서 저장 버튼을 누릅니다.	
142	정보	아이디에 서비스 속성 값을 씀	아이디 이름서비스 이름	아이디의 서비스 프로필 보기에서 저장 버튼을 누릅니다.	
143	심각	아이디에 서비스 속성 값을 쓰지 못함	아이디 이름서비스 이름오류 메시지	아이디에 서비스 속성 값을 쓸 수 없습니다. 사용자의 단일 사인온 토큰이 만료되었거나 사용자에게 이 작업을 수행할 권한이 없을 수 있습니다.	자세한 내용은 데이터 저장소 로그를 참조하십시오.

표 C–3 Access Manager 콘솔에 대한 로그 참조 *(계속)*

아이디	로그 수준	설명	데이터	트리거	조치
144	심각	아이디에 서비스 속성 값을 쓰지 못함	아이디 이름서비스 이름오류 메시지	데이터 저장소 오류로 인해 아이디에 서비스 속성 값을 쓸 수 없습니다.	자세한 내용은 데이터 저장소 로그를 참조하십시오.
201	정보	모든 전역 서비스 기본 속성 값 읽기 시도	서비스 이름	서비스의 전역 구성 보기를 봅니다.	
202	정보	모든 전역 서비스 기본 속성 값을 읽음	서비스 이름	서비스의 전역 구성 보기를 봅니다.	
203	정보	전역 서비스 기본 속성 값 읽기 시도	서비스 이름속성 이름	서비스의 전역 구성 보기를 봅니다.	
204	정보	전역 서비스 기본 속성 값을 읽음	서비스 이름속성 이름	서비스의 전역 구성 보기를 봅니다.	
205	정보	전역 서비스 기본 속성 값을 읽지 못함	서비스 이름속성 이름	서비스의 전역 구성 보기를 봅니다.	자세한 내용은 서비스 관리 로그를 참조하십시오.
211	정보	전역 서비스 기본 속성 값 쓰기 시도	서비스 이름속성 이름	서비스의 전역 구성 보기에서 저장 버튼을 누릅니다.	
212	정보	전역 서비스 기본 속성 값을 씀	서비스 이름속성 이름	서비스의 전역 구성 보기에서 저장 버튼을 누릅니다.	
213	심각	전역 서비스 기본 속성 값을 쓰지 못함	서비스 이름속성 이름오류 메시지	전역 서비스 기본 속성 값을 쓸 수 없습니다. 사용자의 단일 사인온 토큰이 만료되었거나 사용자에게 이 작업을 수행할 권한이 없을 수 있습니다.	자세한 내용은 서비스 관리 로그를 참조하십시오.

표 C–3 Access Manager 콘솔에 대한 로그 참조 *(계속)*

아이디	로그 수준	설명	데이터	트리거	조치
214	심각	전역 서비스 기본 속성 값을 쓰지 못함	서비스 이름속성 이름오류 메시지	서비스 관리 오류로 인해 서비스 기본 속성 값을 쓸 수 없습니다.	자세한 내용은 서비스 관리 로그를 참조하십시오.
221	정보	하위 구성 이름 가져오기 시도	서비스 이름기본 전역 하위 구성 이름	서비스에 하위 스키마가 포함된 전역 서비스 보기를 봅니다.	
222	정보	전역 하위 구성 이름을 읽음	서비스 이름기본 전역 하위 구성 이름	서비스에 하위 스키마가 포함된 전역 서비스 보기를 봅니다.	
223	심각	전역 하위 구성 이름을 읽지 못함	서비스 이름기본 전역 하위 구성 이름오류 메시지	전역 하위 구성 이름을 가져올 수 없습니다. 사용자의 단일 사인온 토큰이 만료되었거나 사용자에게 이 작업을 수행할 권한이 사용자에게 없을 수 있습니다.	자세한 내용은 서비스 관리 로그를 참조하십시오.
224	심각	전역 하위 구성 이름을 읽지 못함	서비스 이름기본 전역 하위 구성 이름오류 메시지	서비스 관리 오류로 인해 전역 하위 구성 이름을 가져올 수 없습니다.	자세한 내용은 서비스 관리 로그를 참조하십시오.
231	정보	하위 구성 삭제 시도	서비스 이름기본 전역 하위 구성 이름삭제할 하위 구성의 이름	전역 서비스 프로필 보기에서 선택한 항목 삭제 버튼을 누릅니다.	

표 C–3 Access Manager 콘솔에 대한 로그 참조 *(계속)*

아이디	로그 수준	설명	데이터	트리거	조치
232	정보	하위 구성을 삭제함	서비스 이름기본 전역 하위 구성 이름삭제할 하위 구성의 이름	전역 서비스 프로필 보기에서 선택한 항목 삭제 버튼을 누릅니다.	
233	심각	하위 구성을 삭제하지 못함	서비스 이름기본 전역 하위 구성의 이름삭제할 하위 구성의 이름오류 메시지	하위 구성을 삭제할 수 없습니다. 사용자의 단일 사인온 토큰이 만료되었거나 이 작업을 수행할 권한이 사용자에게 없을 수 있습니다.	자세한 내용은 서비스 관리 로그를 참조하십시오.
234	심각	하위 구성을 삭제하지 못함	서비스 이름기본 전역 하위 구성의 이름삭제할 하위 구성의 이름오류 메시지	서비스 관리 오류로 인해 하위 구성을 삭제할 수 없습니다.	자세한 내용은 서비스 관리 로그를 참조하십시오.
241	정보	하위 구성 생성 시도	서비스 이름기본 전역 하위 구성의 이름생성할 하위 구성의 이름생성할 하위 스키마의 이름	하위 구성 보기에서 추가 버튼을 누릅니다.	
242	정보	하위 구성을 생성함	서비스 이름기본 전역 하위 구성의 이름생성할 하위 구성의 이름생성할 하위 스키마의 이름	하위 구성 보기에서 추가 버튼을 누릅니다.	

표 C–3 Access Manager 콘솔에 대한 로그 참조 *(계속)*

아이디	로그 수준	설명	데이터	트리거	조치
243	심각	하위 구성을 생성하지 못함	서비스 이름기본 전역 하위 구성의 이름생성할 하위 구성의 이름생성할 하위 스키마의 이름오류 메시지	하위 구성을 생성할 수 없습니다. 사용자의 단일 사인온 토큰이 만료되었거나 이 작업을 수행할 권한이 사용자에게 없을 수 있습니다.	자세한 내용은 서비스 관리 로그를 참조하십시오.
244	심각	하위 구성을 생성하지 못함	서비스 이름기본 전역 하위 구성의 이름생성할 하위 구성의 이름생성할 하위 스키마의 이름오류 메시지	서비스 관리 오류로 인해 하위 구성을 생성할 수 없습니다.	자세한 내용은 서비스 관리 로그를 참조하십시오.
251	정보	하위 구성의 속성 값을 읽음	서비스 이름하위 구성 이름	하위 구성 프로필 보기를 봅니다.	
261	정보	하위 구성의 속성 값 쓰기 시도	서비스 이름하위 구성 이름	하위 구성 프로필 보기에서 저장 버튼을 누릅니다.	
262	정보	하위 구성의 속성 값을 씀	서비스 이름하위 구성 이름	하위 구성 프로필 보기에서 저장 버튼을 누릅니다.	
263	심각	하위 구성의 속성 값을 쓰지 못함	서비스 이름하위 구성 이름오류 메시지	하위 구성의 속성 값을 쓸 수 없습니다. 사용자의 단일 사인온 토큰이 만료되었거나 사용자에게 이 작업을 수행할 권한이 없을 수 있습니다.	자세한 내용은 서비스 관리 로그를 참조하십시오.

표 C–3 Access Manager 콘솔에 대한 로그 참조 *(계속)*

아이디	로그 수준	설명	데이터	트리거	조치
264	심각	하위 구성의 속성 값을 쓰지 못함	서비스 이름하위 구성 이름오류 메시지	서비스 관리 오류로 인해 하위 구성의 속성 값을 쓸 수 없습니다.	자세한 내용은 서비스 관리 로그를 참조하십시오.
301	정보	영역에서 정책 이름 가져오기 시도	영역 이름	정책 기본 페이지를 봅니다.	
302	정보	영역에서 정책 이름을 가져옴	영역 이름	정책 기본 페이지를 봅니다.	
303	심각	영역에서 정책 이름을 가져오지 못함	영역 이름오류 메시지	영역에서 정책 이름을 가져올 수 없습니다. 사용자의 단일 사인온 토큰이 만료되었거나 사용자에게 이 작업을 수행할 권한이 사용자에게 없을 수 있습니다.	자세한 내용은 정책 로그를 참조하십시오.
304	심각	영역에서 정책 이름을 가져오지 못함	영역 이름오류 메시지	정책 SDK 관련 오류로 인해 영역에서 정책 이름을 가져올 수 없습니다.	자세한 내용은 정책 로그를 참조하십시오.
311	정보	영역에서 정책 생성 시도	영역 이름정책 이름	정책 만들기 페이지에서 새로 만들기 버튼을 누릅니다.	
312	정보	정책을 생성함	영역 이름정책 이름	정책 만들기 페이지에서 새로 만들기 버튼을 누릅니다.	

표 C–3 Access Manager 콘솔에 대한 로그 참조 *(계속)*

아이디	로그 수준	설명	데이터	트리거	조치
313	심각	정책을 생성하지 못함	영역 이름정책 이름오류 메시지	영역에서 정책을 만들 수 없습니다. 사용자의 단일 사인온 토큰이 만료되었거나 사용자에게 이 작업을 수행할 권한이 없을 수 있습니다.	자세한 내용은 정책 로그를 참조하십시오.
314	심각	정책을 생성하지 못함	영역 이름정책 이름오류 메시지	정책 SDK 관련 오류로 인해 영역에서 정책을 생성할 수 없습니다.	자세한 내용은 정책 로그를 참조하십시오.
321	정보	정책 수정 시도	영역 이름정책 이름	정책 프로필 페이지에서 저장 버튼을 누릅니다.	
322	정보	정책을 수정함	영역 이름정책 이름	정책 프로필 페이지에서 저장 버튼을 누릅니다.	
323	심각	정책을 수정함	영역 이름정책 이름오류 메시지	영역에서 정책을 수정할 수 없음사용자의 단일 사인온 토큰이 만료되었거나 사용자에게 이 작업을 수행할 권한이 없을 수 있습니다.	자세한 내용은 정책 로그를 참조하십시오.
324	심각	정책을 수정함	영역 이름정책 이름오류 메시지	정책 SDK 관련 오류로 인해 정책을 수정할 수 없습니다.	자세한 내용은 정책 로그를 참조하십시오.
331	정보	정책 삭제 시도	영역 이름정책 이름	정책 기본 페이지에서 삭제 버튼을 누릅니다.	

표 C–3 Access Manager 콘솔에 대한 로그 참조 *(계속)*

아이디	로그 수준	설명	데이터	트리거	조치
332	정보	정책을 삭제함	영역 이름정책 이름	정책 기본 페이지에서 삭제 버튼을 누릅니다.	
333	심각	정책을 삭제하지 못함	영역 이름정책 이름오류 메시지	정책을 삭제할 수 없습니다. 사용자의 단일 사인온 토큰이 만료되었거나 사용자에게 이 작업을 수행할 권한이 없을 수 있습니다.	자세한 내용은 정책 로그를 참조하십시오.
334	심각	정책을 삭제하지 못함	영역 이름정책 이름오류 메시지	정책 SDK 관련 오류로 인해 정책을 삭제할 수 없습니다.	자세한 내용은 정책 로그를 참조하십시오.
401	정보	영역 이름 가져오기 시도	상위 영역 이름	영역 기본 페이지를 봅니다.	
402	정보	영역 이름을 가져옴	상위 영역 이름	영역 기본 페이지를 봅니다.	
403	심각	영역 이름을 가져오지 못함	상위 영역 이름오류 메시지	서비스 관리 SDK 예외로 인해 영역 이름을 가져올 수 없습니다.	자세한 내용은 서비스 관리 로그를 참조하십시오.
411	정보	영역 생성 시도	상위 영역 이름새 영역 이름	영역 만들기 페이지에서 새로 만들기 버튼을 누릅니다.	
412	정보	영역을 생성함	상위 영역 이름새 영역 이름	영역 만들기 페이지에서 새로 만들기 버튼을 누릅니다.	

표 C–3 Access Manager 콘솔에 대한 로그 참조 *(계속)*

아이디	로그 수준	설명	데이터	트리거	조치
413	심각	영역을 생성하지 못함	상위 영역 이름새 영역 이름오류 메시지	서비스 관리 SDK 예외로 인해 새 영역을 생성할 수 없습니다.	자세한 내용은 서비스 관리 로그를 참조하십시오.
421	정보	영역 삭제 시도	상위 영역 이름삭제할 영역의 이름	영역 기본 페이지에서 삭제 버튼을 누릅니다.	
422	정보	영역을 삭제함	상위 영역 이름삭제할 영역의 이름	영역 기본 페이지에서 삭제 버튼을 누릅니다.	
423	심각	영역을 삭제하지 못함	상위 영역 이름삭제할 영역의 이름오류 메시지	서비스 관리 SDK 예외로 인해 영역을 삭제할 수 없습니다.	자세한 내용은 서비스 관리 로그를 참조하십시오.
431	정보	영역의 속성 값 가져오기 시도	영역 이름	영역 프로필 페이지를 봅니다.	
432	정보	영역의 속성 값을 가져옴	영역 이름	영역 프로필 페이지를 봅니다.	
433	심각	영역의 속성 값을 가져오지 못함	영역 이름오류 메시지	서비스 관리 SDK 예외로 인해 영역의 속성 값을 가져올 수 없습니다.	자세한 내용은 서비스 관리 로그를 참조하십시오.
441	정보	영역의 프로필 수정 시도	영역 이름	영역 프로필 페이지에서 저장 버튼을 누릅니다.	
442	정보	영역의 프로필을 수정함	영역 이름	영역 프로필 페이지에서 저장 버튼을 누릅니다.	

표 C–3 Access Manager 콘솔에 대한 로그 참조 *(계속)*

아이디	로그 수준	설명	데이터	트리거	조치
443	심각	영역의 프로필을 수정하지 못함	영역 이름오류 메시지	서비스 관리 SDK 예외로 인해 영역의 프로필을 수정할 수 없습니다.	자세한 내용은 서비스 관리 로그를 참조하십시오.
501	정보	영역에서 위임 주제 가져오기 시도	영역 이름검색 패턴	위임 기본 페이지를 봅니다.	
502	정보	영역에서 위임 주제를 가져옴	영역 이름검색 패턴	위임 기본 페이지를 봅니다.	
503	심각	영역에서 위임 주제를 가져오지 못함	영역 이름검색 패턴오류 메시지	위임 주제를 가져올 수 없습니다. 사용자의 단일 사인온 토큰이 만료되었거나 이 작업을 수행할 권한이 사용자에게 없을 수 있습니다.	자세한 내용은 위임 관리 로그를 참조하십시오.
504	심각	영역에서 위임 주제를 가져오지 못함	영역 이름검색 패턴오류 메시지	위임 관리 SDK 관련 오류로 인해 위임 주제를 가져올 수 없습니다.	자세한 내용은 위임 관리 로그를 참조하십시오.
511	정보	위임 주제의 권한 가져오기 시도	영역 이름위임 주제의 아이디	위임 주제 프로필 페이지를 봅니다.	
512	정보	위임 주제의 권한을 가져옴	영역 이름위임 주제의 아이디	위임 주제 프로필 페이지를 봅니다.	

표 C–3 Access Manager 콘솔에 대한 로그 참조 *(계속)*

아이디	로그 수준	설명	데이터	트리거	조치
513	심각	위임 주제의 권한을 가져오지 못함	영역 이름위임 주제의 *ID*오류 메시지	위임 주제의 권한을 가져올 수 없습니다. 사용자의 단일 사인온 토큰이 만료되었거나 사용자에게 이 작업을 수행할 권한이 없을 수 있습니다.	자세한 내용은 위임 관리 로그를 참조하십시오.
514	심각	위임 주제의 권한을 가져오지 못함	영역 이름위임 주제의 *ID*오류 메시지	위임 관리 SDK 관련 오류로 인해 위임 주제의 권한을 가져올 수 없습니다.	자세한 내용은 위임 관리 로그를 참조하십시오.
521	정보	위임 권한 수정 시도	영역 이름위임 권한의 *ID*주제 *ID*	위임 주제 프로필 페이지에서 저장 버튼을 누릅니다.	
522	정보	위임 권한을 수정함	영역 이름위임 권한의 *ID*주제 *ID*	위임 주제 프로필 페이지에서 저장 버튼을 누릅니다.	
523	심각	위임 권한을 수정하지 못함	영역 이름위임 권한의 *ID*주제 *ID*오류 메시지	위임 권한을 수정할 수 없습니다. 사용자의 단일 사인온 토큰이 만료되었거나 사용자에게 이 작업을 수행할 권한이 없을 수 있습니다.	자세한 내용은 위임 관리 로그를 참조하십시오.
524	심각	위임 권한을 수정하지 못함	영역 이름위임 권한의 *ID*주제 *ID*오류 메시지	위임 관리 SDK 관련 오류로 인해 위임 권한을 수정할 수 없습니다.	자세한 내용은 위임 관리 로그를 참조하십시오.

표 C–3 Access Manager 콘솔에 대한 로그 참조 *(계속)*

아이디	로그 수준	설명	데이터	트리거	조치
601	정보	데이터 저장소 이름 가져오기 시도	영역 이름	데이터 저장소 기본 페이지를 봅니다.	
602	정보	데이터 저장소 이름을 가져옴	영역 이름	데이터 저장소 기본 페이지를 봅니다.	
603	심각	데이터 저장소 이름을 가져오지 못함	영역 이름오류 메시지	데이터 저장소 이름을 가져올 수 없습니다. 사용자의 단일 사인온 토큰이 만료되었거나 사용자에게 이 작업을 수행할 권한이 없을 수 있습니다.	자세한 내용은 서비스 관리 로그를 참조하십시오.
604	심각	데이터 저장소 이름을 가져오지 못함	영역 이름오류 메시지	서비스 관리 SDK 예외로 인해 데이터 저장소 이름을 가져올 수 없습니다.	자세한 내용은 서비스 관리 로그를 참조하십시오.
611	정보	아이디 저장소의 속성 값 가져오기 시도	영역 이름아이디 저장소 이름	데이터 저장소 프로필 페이지를 봅니다.	
612	정보	데이터 저장소의 속성 값을 가져옴	영역 이름아이디 저장소 이름	데이터 저장소 프로필 페이지를 봅니다.	
613	심각	데이터 저장소의 속성 값을 가져오지 못함	영역 이름아이디 저장소 이름오류 메시지	아이디 저장소의 속성 값을 가져올 수 없습니다. 사용자의 단일 사인온 토큰이 만료되었거나 사용자에게 이 작업을 수행할 권한이 없을 수 있습니다.	자세한 내용은 서비스 관리 로그를 참조하십시오.

표 C–3 Access Manager 콘솔에 대한 로그 참조 *(계속)*

아이디	로그 수준	설명	데이터	트리거	조치
614	심각	데이터 저장소의 속성 값을 가져오지 못함	영역 이름아이디 저장소 이름오류 메시지	서비스 관리 SDK 예외로 인해 데이터 저장소의 속성 값을 가져올 수 없습니다.	자세한 내용은 서비스 관리 로그를 참조하십시오.
621	정보	아이디 저장소 생성 시도	영역 이름아이디 저장소 이름아이디 저장소 유형	데이터 저장소 생성 페이지에서 새로 만들기 버튼을 누릅니다.	
622	정보	데이터 저장소를 생성함	영역 이름아이디 저장소 이름아이디 저장소 유형	데이터 저장소 생성 페이지에서 새로 만들기 버튼을 누릅니다.	
623	심각	데이터 저장소를 생성하지 못함	영역 이름아이디 저장소 이름아이디 저장소 유형오류 메시지	아이디 저장소를 생성할 수 없습니다. 사용자의 단일 사인온 토큰이 만료되었거나 이 작업을 수행할 권한이 사용자에게 없을 수 있습니다.	자세한 내용은 서비스 관리 로그를 참조하십시오.
624	심각	데이터 저장소를 생성하지 못함	영역 이름아이디 저장소 이름아이디 저장소 유형오류 메시지	서비스 관리 SDK 예외로 인해 데이터 저장소를 생성할 수 없습니다.	자세한 내용은 서비스 관리 로그를 참조하십시오.
631	정보	아이디 저장소 삭제 시도	영역 이름아이디 저장소 이름	데이터 저장소 기본 페이지에서 삭제 버튼을 누릅니다.	

표 C–3 Access Manager 콘솔에 대한 로그 참조 *(계속)*

아이디	로그 수준	설명	데이터	트리거	조치
632	정보	데이터 저장소를 삭제함	영역 이름아이디 저장소 이름	데이터 저장소 기본 페이지에서 삭제 버튼을 누릅니다.	
633	심각	데이터 저장소를 삭제하지 못함	영역 이름아이디 저장소 이름오류 메시지	아이디 저장소를 삭제할 수 없습니다. 사용자의 단일 사인온 토큰이 만료되었거나 이 작업을 수행할 권한이 사용자에게 없을 수 있습니다.	자세한 내용은 서비스 관리 로그를 참조하십시오.
634	심각	데이터 저장소를 삭제하지 못함	영역 이름아이디 저장소 이름오류 메시지	서비스 관리 SDK 예외로 인해 데이터 저장소를 삭제할 수 없습니다.	자세한 내용은 서비스 관리 로그를 참조하십시오.
641	정보	아이디 저장소 수정 시도	영역 이름아이디 저장소 이름	데이터 저장소 프로필 페이지에서 저장 버튼을 누릅니다.	
642	정보	데이터 저장소를 수정함	영역 이름아이디 저장소 이름	데이터 저장소 프로필 페이지에서 저장 버튼을 누릅니다.	

표 C–3 Access Manager 콘솔에 대한 로그 참조 *(계속)*

아이디	로그 수준	설명	데이터	트리거	조치
643	심각	데이터 저장소를 수정하지 못함	영역 이름아이디 저장소 이름오류 메시지	아이디 저장소를 수정할 수 없습니다. 사용자의 단일 사인온 토큰이 만료되었거나 이 작업을 수행할 권한이 사용자에게 없을 수 있습니다.	자세한 내용은 서비스 관리 로그를 참조하십시오.
644	심각	데이터 저장소를 수정하지 못함	영역 이름아이디 저장소 이름오류 메시지	서비스 관리 SDK 예외로 인해 데이터 저장소를 수정할 수 없습니다.	자세한 내용은 서비스 관리 로그를 참조하십시오.
701	정보	영역의 할당된 서비스 가져오기 시도	영역 이름	영역의 서비스 기본 페이지를 봅니다.	
702	정보	영역의 할당된 서비스를 가져옴	영역 이름	영역의 서비스 기본 페이지를 봅니다.	
703	심각	영역의 할당된 서비스를 가져오지 못함	영역 이름오류 메시지	인증 구성 예외로 인해 영역의 할당된 서비스를 가져올 수 없습니다.	자세한 내용은 인증 로그를 참조하십시오.
704	심각	영역의 할당된 서비스를 가져오지 못함	영역 이름오류 메시지	서비스 관리 SDK 예외로 인해 영역의 할당된 서비스를 가져올 수 없습니다.	자세한 내용은 서비스 관리 로그를 참조하십시오.

표 C–3 Access Manager 콘솔에 대한 로그 참조 *(계속)*

아이디	로그 수준	설명	데이터	트리거	조치
705	심각	영역의 할당된 서비스를 가져오지 못함	영역 이름오류 메시지	데이터 저장소 SDK 예외로 인해 영역의 할당된 서비스를 가져올 수 없습니다.	자세한 내용은 서비스 관리 로그를 참조하십시오.
706	심각	영역의 할당된 서비스를 가져오지 못함	영역 이름오류 메시지	영역의 할당된 서비스를 가져올 수 없습니다. 사용자의 단일 사인온 토큰이 만료되었거나 사용자에게 이 작업을 수행할 권한이 사용자에게 없을 수 있습니다.	자세한 내용은 서비스 관리 로그를 참조하십시오.
711	정보	영역의 할당 가능 서비스 가져오기 시도	영역 이름	영역의 서비스 기본 페이지를 봅니다.	
712	정보	영역의 할당 가능 서비스를 가져옴	영역 이름	영역의 서비스 기본 페이지를 봅니다.	
713	심각	영역의 할당 가능 서비스를 가져오지 못함	영역 이름오류 메시지	인증 구성 예외로 인해 영역의 할당 가능 서비스를 가져올 수 없습니다.	자세한 내용은 인증 로그를 참조하십시오.
714	심각	영역의 할당 가능 서비스를 가져오지 못함	영역 이름오류 메시지	서비스 관리 SDK 예외로 인해 영역의 할당 가능 서비스를 가져올 수 없습니다.	자세한 내용은 서비스 관리 로그를 참조하십시오.

표 C–3 Access Manager 콘솔에 대한 로그 참조 *(계속)*

아이디	로그 수준	설명	데이터	트리거	조치
715	심각	영역의 할당 가능 서비스를 가져오지 못함	영역 이름오류 메시지	아이디 저장소 관리 SDK 예외로 인해 영역의 할당 가능 서비스를 가져올 수 없습니다.	자세한 내용은 아이디 저장소 관리 로그를 참조하십시오.
716	심각	영역의 할당 가능 서비스를 가져오지 못함	영역 이름오류 메시지	영역의 할당 가능 서비스를 가져올 수 없습니다. 사용자의 단일 사인온 토큰이 만료되었거나 사용자에게 이 작업을 수행할 권한이 사용자에게 없을 수 있습니다.	자세한 내용은 서비스 관리 로그를 참조하십시오.
721	정보	영역에서 서비스 할당 해제 시도	영역 이름서비스 이름	영역의 서비스 페이지에서 할당 해제 버튼을 누릅니다.	
722	정보	영역에서 서비스를 할당 해제함	영역 이름서비스 이름	영역의 서비스 페이지에서 할당 해제 버튼을 누릅니다.	
723	심각	영역에서 서비스를 할당 해제하지 못함	영역 이름서비스 이름오류 메시지	서비스 관리 SDK 예외로 인해 영역에서 서비스를 할당 해제할 수 없습니다.	자세한 내용은 서비스 관리 로그를 참조하십시오.

표 C–3 Access Manager 콘솔에 대한 로그 참조 *(계속)*

아이디	로그 수준	설명	데이터	트리거	조치
725	심각	영역에서 서비스를 할당 해제하지 못함	영역 이름서비스 이름오류 메시지	영역에서 서비스를 할당 해제할 수 없습니다. 사용자의 단일 사인온 토큰이 만료되었거나 사용자에게 이 작업을 수행할 권한이 없을 수 있습니다.	자세한 내용은 데이터 저장소 관리 로그를 참조하십시오.
724	심각	영역에서 서비스를 할당 해제하지 못함	영역 이름서비스 이름오류 메시지	데이터 저장소 관리 SDK 예외로 인해 영역에서 서비스를 할당 해제할 수 없습니다.	자세한 내용은 데이터 저장소 관리 로그를 참조하십시오.
731	정보	영역에 서비스 할당 시도	영역 이름서비스 이름	영역의 서비스 페이지에서 할당 버튼을 누릅니다.	
732	정보	영역에 서비스를 할당함	영역 이름서비스 이름	영역의 서비스 페이지에서 할당 버튼을 누릅니다.	
733	심각	영역에 서비스를 할당하지 못함	영역 이름서비스 이름오류 메시지	서비스 관리 SDK 예외로 인해 영역에 서비스를 할당할 수 없습니다.	자세한 내용은 서비스 관리 로그를 참조하십시오.

표 C–3 Access Manager 콘솔에 대한 로그 참조 *(계속)*

아이디	로그 수준	설명	데이터	트리거	조치
734	심각	영역에 서비스를 할당하지 못함	영역 이름서비스 이름오류 메시지	영역에 서비스를 할당할 수 없습니다. 사용자의 단일 사인온 토큰이 만료되었거나 이 작업을 수행할 권한이 사용자에게 없을 수 있습니다.	자세한 내용은 서비스 관리 로그를 참조하십시오.
735	심각	영역에 서비스를 할당하지 못함	영역 이름서비스 이름오류 메시지	데이터 저장소 SDK 예외로 인해 영역에 서비스를 할당할 수 없습니다.	자세한 내용은 서비스 관리 로그를 참조하십시오.
741	정보	영역에서 서비스의 속성 값 가져오기 시도	영역 이름서비스 이름속성 스키마 이름	영역의 서비스 프로필 페이지를 봅니다.	
742	정보	영역에서 서비스의 속성 값을 가져옴	영역 이름서비스 이름속성 스키마 이름	영역의 서비스 프로필 페이지를 봅니다.	
743	심각	영역에서 서비스의 속성 값을 가져오지 못함	영역 이름서비스 이름속성 스키마 이름오류 메시지	서비스 관리 SDK 예외로 인해 서비스의 속성 값을 가져올 수 없습니다.	자세한 내용은 서비스 관리 로그를 참조하십시오.
744	정보	영역에서 서비스의 속성 값을 가져오지 못함	영역 이름서비스 이름속성 스키마 이름오류 메시지	데이터 저장소 SDK 예외로 인해 서비스의 속성 값을 가져올 수 없습니다.	자세한 내용은 서비스 관리 로그를 참조하십시오.

표 C–3 Access Manager 콘솔에 대한 로그 참조 *(계속)*

아이디	로그 수준	설명	데이터	트리거	조치
745	심각	영역에서 서비스의 속성 값을 가져오지 못함	영역 이름서비스 이름속성 스키마 이름오류 메시지	서비스의 속성 값을 가져올 수 없습니다. 사용자의 단일 사인온 토큰이 만료되었거나 사용자에게 이 작업을 수행할 권한이 사용자에게 없을 수 있습니다.	자세한 내용은 서비스 관리 로그를 참조하십시오.
751	정보	영역에서 서비스의 속성 값 수정 시도	영역 이름서비스 이름	영역의 서비스 프로필 페이지에서 저장 버튼을 누릅니다.	
752	정보	영역에서 서비스의 속성 값을 수정함	영역 이름서비스 이름	영역의 서비스 프로필 페이지에서 저장 버튼을 누릅니다.	
753	심각	영역에서 서비스의 속성 값을 수정하지 못함	영역 이름서비스 이름오류 메시지	서비스 관리 SDK 예외로 인해 서비스의 속성 값을 수정할 수 없습니다.	자세한 내용은 서비스 관리 로그를 참조하십시오.
754	심각	영역에서 서비스의 속성 값을 수정하지 못함	영역 이름서비스 이름오류 메시지	데이터 저장소 오류로 인해 서비스의 속성 값을 수정할 수 없습니다.	자세한 내용은 데이터 저장소 로그를 참조하십시오.
755	심각	영역에서 서비스의 속성 값을 수정하지 못함	영역 이름서비스 이름오류 메시지	서비스의 속성 값을 수정할 수 없습니다. 사용자의 단일 사인온 토큰이 만료되었거나 사용자에게 이 작업을 수행할 권한이 없을 수 있습니다.	자세한 내용은 데이터 저장소 로그를 참조하십시오.

표 C–3 Access Manager 콘솔에 대한 로그 참조 *(계속)*

아이디	로그 수준	설명	데이터	트리거	조치
801	정보	인증 유형 가져오기 시도		인증 프로필 페이지를 봅니다.	
802	정보	인증 유형을 가져옴		인증 프로필 페이지를 봅니다.	
803	심각	인증 유형을 가져오지 못함	오류 메시지	인증 구성 SDK 예외로 인해 인증 유형을 가져올 수 없습니다.	자세한 내용은 인증 관리 로그를 참조하십시오.
811	정보	영역에서 인증 인스턴스 가져오기 시도	영역 이름	인증 프로필 페이지를 봅니다.	
812	정보	영역에서 인증 인스턴스를 가져옴	영역 이름	인증 프로필 페이지를 봅니다.	
813	심각	영역에서 인증 인스턴스를 가져오지 못함	영역 이름오류 메시지	인증 구성 SDK 예외로 인해 인증 인스턴스를 가져올 수 없습니다.	자세한 내용은 인증 관리 로그를 참조하십시오.
821	정보	영역에서 인증 인스턴스 제거 시도	영역 이름인증 인스턴스 이름	인증 프로필 페이지를 봅니다.	
822	정보	영역에서 인증 인스턴스를 제거함	영역 이름인증 인스턴스 이름	인증 프로필 페이지를 봅니다.	
823	심각	영역에서 인증 인스턴스를 제거하지 못함	영역 이름인증 인스턴스 이름오류 메시지	인증 구성 SDK 예외로 인해 인증 인스턴스를 제거할 수 없습니다.	자세한 내용은 인증 관리 로그를 참조하십시오.
831	정보	영역에서 인증 인스턴스 생성 시도	영역 이름인증 인스턴스 이름인증 인스턴스 유형	인증 만들기 페이지에서 새로 만들기 버튼을 누릅니다.	

표 C–3 Access Manager 콘솔에 대한 로그 참조 *(계속)*

아이디	로그 수준	설명	데이터	트리거	조치
832	정보	영역에서 인증 인스턴스를 생성함	영역 이름인증 인스턴스 이름인증 인스턴스 유형	인증 만들기 페이지에서 새로 만들기 버튼을 누릅니다.	
833	심각	영역에서 인증 인스턴스를 생성하지 못함	영역 이름인증 인스턴스 이름인증 인스턴스 유형오류 메시지	인증 구성 예외로 인해 인증 인스턴스를 생성할 수 없습니다.	자세한 내용은 인증 구성 로그를 참조하십시오.
841	정보	인증 인스턴스 수정 시도	영역 이름인증 서비스 이름	인증 프로필 페이지에서 저장 버튼을 누릅니다.	
842	정보	인증 인스턴스를 수정함	영역 이름인증 서비스 이름	인증 프로필 페이지에서 저장 버튼을 누릅니다.	
843	심각	인증 인스턴스를 수정하지 못함	영역 이름인증 서비스 이름오류 메시지	서비스 관리 SDK 예외로 인해 인증 인스턴스를 수정할 수 없습니다.	자세한 내용은 서비스 관리 로그를 참조하십시오.
844	심각	인증 인스턴스를 수정하지 못함	영역 이름인증 서비스 이름오류 메시지	인증 인스턴스를 수정할 수 없습니다. 사용자의 단일 사인온 토큰이 만료되었거나 사용자에게 이 작업을 수행할 권한이 사용자에게 없을 수 있습니다.	자세한 내용은 서비스 관리 로그를 참조하십시오.
851	정보	인증 인스턴스 프로필 가져오기 시도	영역 이름인증 인스턴스 이름	인증 인스턴스 프로필 페이지를 봅니다.	

표 C–3 Access Manager 콘솔에 대한 로그 참조 *(계속)*

아이디	로그 수준	설명	데이터	트리거	조치
852	정보	인증 인스턴스 프로필 가져오기를 성공함	영역 이름인증 인스턴스 이름	인증 인스턴스 프로필 페이지를 봅니다.	
853	심각	인증 인스턴스 프로필를 가져오지 못함	영역 이름인증 인스턴스 이름오류 메시지	인증 구성 SDK 예외로 인해 인증 인스턴스 프로필을 가져올 수 없습니다.	자세한 내용은 인증 관리 로그를 참조하십시오.
861	정보	인증 인스턴스 프로필 수정 시도	영역 이름인증 인스턴스 이름	인증 인스턴스 프로필 페이지에서 저장 버튼을 누릅니다.	
862	정보	인증 인스턴스 프로필를 수정함	영역 이름인증 인스턴스 이름	인증 인스턴스 프로필 페이지에서 저장 버튼을 누릅니다.	
863	심각	인증 인스턴스 프로필을 수정하지 못함	영역 이름인증 인스턴스 이름오류 메시지	인증 구성 SDK 예외로 인해 인증 인스턴스 프로필을 수정할 수 없습니다.	자세한 내용은 인증 관리 로그를 참조하십시오.
864	심각	인증 인스턴스 프로필을 수정하지 못함	영역 이름인증 인스턴스 이름오류 메시지	서비스 관리 SDK 예외로 인해 인증 인스턴스 프로필을 수정할 수 없습니다.	자세한 내용은 서비스 관리 로그를 참조하십시오.

표 C–3 Access Manager 콘솔에 대한 로그 참조 *(계속)*

아이디	로그 수준	설명	데이터	트리거	조치
864	심각	인증 인스턴스 프로필을 수정하지 못함	영역 이름인증 인스턴스 이름오류 메시지	인증 인스턴스 프로필을 수정할 수 없습니다. 사용자의 단일 사인온 토큰이 만료되었거나 사용자에게 이 작업을 수행할 권한이 없을 수 있습니다.	자세한 내용은 서비스 관리 로그를 참조하십시오.
871	정보	영역에서 인증 프로필 가져오기 시도	영역 이름	영역 페이지에서 인증 프로필을 봅니다.	
872	정보	영역에서 인증 프로필을 가져옴	영역 이름	영역 페이지에서 인증 프로필을 봅니다.	
873	심각	영역에서 인증 프로필을 가져오지 못함	영역 이름오류 메시지	서비스 관리 SDK 예외로 인해 인증 프로필을 가져올 수 없습니다.	자세한 내용은 서비스 관리 로그를 참조하십시오.
881	정보	인증 구성 프로필 가져오기 시도	영역 이름인증 구성 이름	인증 구성 프로필 페이지를 봅니다.	
882	정보	인증 구성 프로필을 가져옴	영역 이름인증 구성 이름	인증 구성 프로필 페이지를 봅니다.	

표 C–3 Access Manager 콘솔에 대한 로그 참조 *(계속)*

아이디	로그 수준	설명	데이터	트리거	조치
883	심각	인증 구성 프로필을 가져오지 못함	영역 이름인증 구성 이름오류 메시지	인증 구성 프로필을 가져올 수 없습니다. 사용자의 단일 사인온 토큰이 만료되었거나 사용자에게 이 작업을 수행할 권한이 없을 수 있습니다.	자세한 내용은 서비스 관리 로그를 참조하십시오.
884	심각	인증 구성 프로필을 가져오지 못함	영역 이름인증 구성 이름오류 메시지	서비스 관리 SDK 예외로 인해 인증 구성 프로필을 가져올 수 없습니다.	자세한 내용은 서비스 관리 로그를 참조하십시오.
885	심각	인증 구성 프로필을 가져오지 못함	영역 이름인증 구성 이름오류 메시지	인증 구성 SDK 예외로 인해 인증 구성 프로필을 가져올 수 없습니다.	자세한 내용은 인증 구성 로그를 참조하십시오.
891	정보	인증 구성 프로필 수정 시도	영역 이름인증 구성 이름	인증 구성 프로필 페이지에서 저장 버튼을 누릅니다.	
892	정보	인증 구성 프로필을 수정함	영역 이름인증 구성 이름	인증 구성 프로필 페이지에서 저장 버튼을 누릅니다.	

표 C–3 Access Manager 콘솔에 대한 로그 참조 *(계속)*

아이디	로그 수준	설명	데이터	트리거	조치
893	심각	인증 구성 프로필을 수정하지 못함	영역 이름인증 구성 이름오류 메시지	인증 구성 프로필을 수정할 수 없습니다. 사용자의 단일 사인온 토큰이 만료되었거나 사용자에게 이 작업을 수행할 권한이 없을 수 있습니다.	자세한 내용은 서비스 관리 로그를 참조하십시오.
894	심각	인증 구성 프로필을 수정하지 못함	영역 이름인증 구성 이름오류 메시지	서비스 관리 SDK 예외로 인해 인증 구성 프로필을 수정할 수 없습니다.	자세한 내용은 서비스 관리 로그를 참조하십시오.
895	심각	인증 구성 프로필을 수정하지 못함	영역 이름인증 구성 이름오류 메시지	인증 구성 SDK 예외로 인해 인증 구성 프로필을 수정할 수 없습니다.	자세한 내용은 인증 구성 로그를 참조하십시오.
901	정보	인증 구성 생성 시도	영역 이름인증 구성 이름	인증 구성 만들기 페이지에서 새로 만들기 버튼을 누릅니다.	
902	정보	인증 구성을 생성함	영역 이름인증 구성 이름	인증 구성 만들기 페이지에서 새로 만들기 버튼을 누릅니다.	

표 C–3 Access Manager 콘솔에 대한 로그 참조 *(계속)*

아이디	로그 수준	설명	데이터	트리거	조치
903	심각	인증 구성을 생성하지 못함	영역 이름인증 구성 이름오류 메시지	인증 구성을 생성할 수 없습니다. 사용자의 단일 사인온 토큰이 만료되었거나 사용자에게 이 작업을 수행할 권한이 없을 수 있습니다.	자세한 내용은 서비스 관리 로그를 참조하십시오.
904	심각	인증 구성을 생성하지 못함	영역 이름인증 구성 이름오류 메시지	서비스 관리 SDK 예외로 인해 인증 구성을 생성할 수 없습니다.	자세한 내용은 서비스 관리 로그를 참조하십시오.
905	심각	인증 구성을 생성하지 못함	영역 이름인증 구성 이름오류 메시지	인증 구성 SDK 예외로 인해 인증 구성을 생성할 수 없습니다.	자세한 내용은 인증 구성 로그를 참조하십시오.
1001	정보	엔티티 설명자 이름 가져오기 시도	검색 패턴	엔티티 설명자 기본 페이지를 봅니다.	
1002	정보	엔티티 설명자 이름을 가져옴	검색 패턴	엔티티 설명자 기본 페이지를 봅니다.	
1003	심각	엔티티 설명자 이름을 가져오지 못함	검색 패턴오류 메시지	연합 SDK 관련 오류로 인해 엔티티 설명자 이름을 가져올 수 없습니다.	자세한 내용은 연합 로그를 참조하십시오.
1011	정보	엔티티 설명자 생성 시도	설명자 이름설명자 유형	엔티티 설명자 만들기 페이지에서 새로 만들기 버튼을 누릅니다.	

표 C–3 Access Manager 콘솔에 대한 로그 참조 *(계속)*

아이디	로그 수준	설명	데이터	트리거	조치
1012	정보	엔티티 설명자를 생성함	설명자 이름설명자 유형	엔티티 설명자 만들기 페이지에서 새로 만들기 버튼을 누릅니다.	
1013	심각	엔티티 설명자를 생성하지 못함	설명자 이름설명자 유형오류 메시지	연합 SDK 관련 오류로 인해 엔티티 설명자 이름을 생성할 수 없습니다.	자세한 내용은 연합 로그를 참조하십시오.
1021	정보	엔티티 설명자 삭제 시도	설명자 이름	엔티티 설명자 기본 페이지에서 삭제 버튼을 누릅니다.	
1022	정보	엔티티 설명자를 삭제함	설명자 이름	엔티티 설명자 기본 페이지에서 삭제 버튼을 누릅니다.	
1023	심각	엔티티 설명자를 삭제하지 못함	설명자 이름오류 메시지	연합 SDK 관련 오류로 인해 엔티티 설명자를 삭제할 수 없습니다.	자세한 내용은 연합 로그를 참조하십시오.
1031	정보	관련 엔티티 설명자의 속성 값 가져오기 시도	설명자 이름	관련 엔티티 설명자 프로필 페이지를 봅니다.	
1032	정보	관련 엔티티 설명자의 속성 값을 가져옴	설명자 이름	관련 엔티티 설명자 프로필 페이지를 봅니다.	
1033	심각	관련 엔티티 설명자의 속성 값을 가져오지 못함	설명자 이름오류 메시지	연합 SDK 관련 오류로 인해 관련 엔티티 설명자의 속성 값을 가져올 수 없습니다.	자세한 내용은 연합 로그를 참조하십시오.

표 C–3 Access Manager 콘솔에 대한 로그 참조 *(계속)*

아이디	로그 수준	설명	데이터	트리거	조치
1041	정보	관련 엔티티 설명자 수정 시도	설명자 이름	관련 엔티티 설명자 프로필 페이지에서 저장 버튼을 누릅니다.	
1042	정보	관련 엔티티 설명자를 수정함	설명자 이름	관련 엔티티 설명자 프로필 페이지에서 저장 버튼을 누릅니다.	
1043	심각	관련 엔티티 설명자를 수정하지 못함	설명자 이름오류 메시지	연합 SDK 관련 오류로 인해 관련 엔티티 설명자를 수정할 수 없습니다.	자세한 내용은 연합 로그를 참조하십시오.
1044	심각	관련 엔티티 설명자를 수정하지 못함	설명자 이름오류 메시지	하나 이상의 속성 값에 대한 잘못된 번호 형식으로 인해 관련 엔티티 설명자를 수정할 수 없습니다.	자세한 내용은 연합 로그를 참조하십시오.
1051	정보	엔티티 설명자의 속성 값 가져오기 시도	설명자 이름	엔티티 설명자 프로필 페이지를 봅니다.	
1052	정보	엔티티 설명자의 속성 값을 가져옴	설명자 이름	엔티티 설명자 프로필 페이지를 봅니다.	
1053	심각	엔티티 설명자의 속성 값을 가져오지 못함	설명자 이름오류 메시지	연합 SDK 관련 오류로 인해 엔티티 설명자의 속성 값을 가져올 수 없습니다.	자세한 내용은 연합 로그를 참조하십시오.

표 C–3 Access Manager 콘솔에 대한 로그 참조 *(계속)*

아이디	로그 수준	설명	데이터	트리거	조치
1061	정보	엔티티 설명자 수정 시도	설명자 이름	엔티티 설명자 프로필 페이지에서 저장 버튼을 누릅니다.	
1062	정보	엔티티 설명자를 수정함	설명자 이름	엔티티 설명자 프로필 페이지에서 저장 버튼을 누릅니다.	
1063	심각	엔티티 설명자를 수정하지 못함	설명자 이름오류 메시지	연합 SDK 관련 오류로 인해 엔티티 설명자 이름을 수정할 수 없습니다.	자세한 내용은 연합 로그를 참조하십시오.
1101	정보	인증 도메인 이름 가져오기 시도	검색 패턴	인증 도메인 기본 페이지를 봅니다.	
1102	정보	인증 도메인 이름을 가져옴	검색 패턴	인증 도메인 기본 페이지를 봅니다.	
1103	심각	인증 도메인 이름을 가져오지 못함	검색 패턴오류 메시지	연합 SDK 관련 오류로 인해 인증 도메인 이름을 가져올 수 없습니다.	자세한 내용은 연합 로그를 참조하십시오.
1111	정보	인증 도메인 생성 시도	인증 도메인 이름	인증 도메인 만들기 페이지에서 새로 만들기 버튼을 누릅니다.	
1112	정보	인증 도메인을 생성함	인증 도메인 이름	인증 도메인 만들기 페이지에서 새로 만들기 버튼을 누릅니다.	

표 C–3 Access Manager 콘솔에 대한 로그 참조 *(계속)*

아이디	로그 수준	설명	데이터	트리거	조치
1113	심각	인증 도메인을 생성하지 못함	인증 도메인 이름오류 메시지	연합 SDK 관련 오류로 인해 인증 도메인을 생성할 수 없습니다.	자세한 내용은 연합 로그를 참조하십시오.
1121	정보	인증 도메인 삭제 시도	인증 도메인 이름	인증 도메인 기본 페이지에서 삭제 버튼을 누릅니다.	
1122	정보	인증 도메인을 삭제함	인증 도메인 이름	인증 도메인 기본 페이지에서 삭제 버튼을 누릅니다.	
1123	심각	인증 도메인을 삭제하지 못함	인증 도메인 이름오류 메시지	연합 SDK 관련 오류로 인해 인증 도메인을 삭제할 수 없습니다.	자세한 내용은 연합 로그를 참조하십시오.
1131	정보	인증 도메인의 속성 값 가져오기 시도	인증 도메인 이름	인증 도메인 프로필 페이지를 봅니다.	
1132	정보	인증 도메인의 속성 값을 가져옴	인증 도메인 이름	인증 도메인 프로필 페이지를 봅니다.	
1133	심각	인증 도메인의 속성 값을 가져오지 못함	인증 도메인 이름오류 메시지	연합 SDK 관련 오류로 인해 인증 도메인의 속성 값을 가져올 수 없습니다.	자세한 내용은 연합 로그를 참조하십시오.
1141	정보	인증 도메인 수정 시도	인증 도메인 이름	인증 도메인 프로필 페이지에서 저장 버튼을 누릅니다.	

표 C–3 Access Manager 콘솔에 대한 로그 참조 *(계속)*

아이디	로그 수준	설명	데이터	트리거	조치
1142	정보	인증 도메인을 수정함	인증 도메인 이름	인증 도메인 프로필 페이지에서 저장 버튼을 누릅니다.	
1143	심각	인증 도메인을 수정하지 못함	인증 도메인 이름오류 메시지	연합 SDK 관련 오류로 인해 인증 도메인을 수정할 수 없습니다.	자세한 내용은 연합 로그를 참조하십시오.
1151	정보	모든 공급자 이름 가져오기 시도		인증 도메인 프로필 페이지를 봅니다.	
1152	정보	모든 공급자 이름을 가져옴		인증 도메인 프로필 페이지를 봅니다.	
1153	심각	모든 공급자 이름을 가져오지 못함	오류 메시지	연합 SDK 관련 오류로 인해 엔티티 모든 공급자 이름을 가져올 수 없습니다.	자세한 내용은 연합 로그를 참조하십시오.
1161	정보	인증 도메인에서 공급자 이름 가져오기 시도	인증 도메인 이름	인증 도메인 프로필 페이지를 봅니다.	
1162	정보	인증 도메인에서 공급자 이름을 가져옴	인증 도메인 이름	인증 도메인 프로필 페이지를 봅니다.	
1163	심각	인증 도메인에서 공급자 이름을 가져오지 못함	인증 도메인 이름오류 메시지	연합 SDK 관련 오류로 인해 인증 도메인에서 공급자 이름을 가져올 수 없습니다.	자세한 내용은 연합 로그를 참조하십시오.

표 C–3 Access Manager 콘솔에 대한 로그 참조 *(계속)*

아이디	로그 수준	설명	데이터	트리거	조치
1171	정보	인증 도메인에 공급자 추가 시도	인증 도메인 이름공급자 이름	공급자 할당 페이지에서 저장 버튼을 누릅니다.	
1172	정보	인증 도메인에 공급자를 추가함	인증 도메인 이름공급자 이름	공급자 할당 페이지에서 저장 버튼을 누릅니다.	
1173	심각	인증 도메인에 공급자를 추가하지 못함	인증 도메인 이름공급자 이름오류 메시지	연합 SDK 관련 오류로 인해 인증 도메인에 공급자를 추가할 수 없습니다.	자세한 내용은 연합 로그를 참조하십시오.
1181	정보	인증 도메인에서 공급자 제거 시도	인증 도메인 이름공급자 이름	공급자 할당 페이지에서 저장 버튼을 누릅니다.	
1182	정보	인증 도메인에서 공급자를 삭제함	인증 도메인 이름공급자 이름	공급자 할당 페이지에서 저장 버튼을 누릅니다.	
1183	심각	인증 도메인에서 공급자를 삭제하지 못함	인증 도메인 이름공급자 이름오류 메시지	연합 SDK 관련 오류로 인해 인증 도메인에서 공급자를 제거할 수 없습니다.	자세한 내용은 연합 로그를 참조하십시오.
1301	정보	공급자 생성 시도	공급자 이름공급자 역할공급자 유형	공급자 할당 페이지에서 저장 버튼을 누릅니다.	
1302	정보	공급자를 생성함	공급자 이름공급자 역할공급자 유형	공급자 할당 페이지에서 저장 버튼을 누릅니다.	

표 C–3 Access Manager 콘솔에 대한 로그 참조 *(계속)*

아이디	로그 수준	설명	데이터	트리거	조치
1303	심각	공급자를 생성함	공급자 이름공급자 역할공급자 유형오류 메시지	연합 SDK 관련 오류로 인해 공급자를 생성할 수 없습니다.	자세한 내용은 연합 로그를 참조하십시오.
1303	심각	공급자를 생성함	공급자 이름공급자 역할공급자 유형오류 메시지	연합 SDK 관련 오류로 인해 공급자를 생성할 수 없습니다.	자세한 내용은 연합 로그를 참조하십시오.
1304	심각	공급자를 생성함	공급자 이름공급자 역할공급자 유형오류 메시지	관리자 콘솔에서 이 공급자에 대해 값을 설정할 적절한 방법을 찾을 수 없으므로 공급자를 생성할 수 없습니다.	웹 응용 프로그램 오류입니다. Sun 기술 지원부에 문의하십시오.
1311	정보	공급자의 속성 값 가져오기 시도	공급자 이름공급자 역할공급자 유형	공급자 프로필 페이지를 봅니다.	
1312	정보	공급자의 속성 값을 가져옴	공급자 이름공급자 역할공급자 유형	공급자 프로필 페이지를 봅니다.	
1321	정보	공급자에 대한 처리기 가져오기 시도	공급자 이름공급자 역할	공급자 프로필 페이지를 봅니다.	
1322	정보	공급자에 대한 처리기를 가져옴	공급자 이름공급자 역할	공급자 프로필 페이지를 봅니다.	
1323	심각	공급자에 대한 처리기를 가져오지 못함	공급자 이름공급자 역할오류 메시지	연합 SDK 관련 오류로 인해 공급자에 대한 처리기를 가져올 수 없습니다.	자세한 내용은 연합 로그를 참조하십시오.

표 C–3 Access Manager 콘솔에 대한 로그 참조 *(계속)*

아이디	로그 수준	설명	데이터	트리거	조치
1331	정보	공급자 수정 시도	공급자 이름공급자 역할	공급자 프로필 페이지에서 저장 버튼을 누릅니다.	
1332	정보	공급자를 수정함	공급자 이름공급자 역할	공급자 프로필 페이지에서 저장 버튼을 누릅니다.	
1333	심각	공급자를 수정하지 못함	공급자 이름공급자 역할오류 메시지	연합 SDK 관련 오류로 인해 공급자를 수정할 수 없습니다.	자세한 내용은 연합 로그를 참조하십시오.
1334	심각	공급자를 수정하지 못함	공급자 이름공급자 역할오류 메시지	관리자 콘솔에서 이 공급자에 대해 값을 설정할 적절한 방법을 찾을 수 없으므로 공급자를 수정할 수 없습니다.	웹 응용 프로그램 오류입니다. Sun 기술 지원부에 문의하십시오.
1341	정보	공급자 삭제 시도	공급자 이름공급자 역할	공급자 프로필 페이지에서 공급자 삭제 버튼을 누릅니다.	
1342	정보	공급자를 삭제함	공급자 이름공급자 역할	공급자 프로필 페이지에서 공급자 삭제 버튼을 누릅니다.	
1343	심각	공급자를 삭제하지 못함	공급자 이름공급자 역할오류 메시지	연합 SDK 관련 오류로 인해 공급자를 삭제할 수 없습니다.	자세한 내용은 연합 로그를 참조하십시오.
1351	정보	인증된 잠정 공급자 가져오기 시도	공급자 이름공급자 역할	인증된 공급자 추가 페이지를 봅니다.	

표 C–3 Access Manager 콘솔에 대한 로그 참조 *(계속)*

아이디	로그 수준	설명	데이터	트리거	조치
1352	정보	인증된 잠정 공급자를 가져옴	공급자 이름공급자 역할	인증된 공급자 추가 페이지를 봅니다.	
1353	심각	인증된 잠정 공급자를 가져오지 못함	공급자 이름공급자 역할오류 메시지	연합 SDK 관련 오류로 인해 인증된 예상 공급자를 가져올 수 없습니다.	자세한 내용은 연합 로그를 참조하십시오.
2001	정보	서비스 스키마의 스키마 유형에 대한 속성 값 가져오기 시도	서비스 이름스키마 유형 이름속성 스키마 이름	서비스 프로필 페이지를 봅니다.	
2002	정보	서비스 스키마의 스키마 유형에 대한 속성 값을 가져옴	서비스 이름스키마 유형 이름속성 스키마 이름	서비스 프로필 페이지를 봅니다.	
2003	심각	서비스 스키마의 스키마 유형에 대한 속성 값을 가져오지 못함	서비스 이름스키마 유형 이름속성 스키마 이름오류 메시지	서비스 스키마의 스키마 유형에 대한 속성 값을 가져올 수 없습니다. 사용자의 단일 사인온 토큰이 만료되었거나 사용자에게 이 작업을 수행할 권한이 없을 수 있습니다.	자세한 내용은 서비스 관리 로그를 참조하십시오.
2004	심각	서비스 스키마의 스키마 유형에 대한 속성 값을 가져오지 못함	서비스 이름스키마 유형 이름속성 스키마 이름오류 메시지	서비스 관리 SDK 관련 오류로 인해 서비스 스키마의 스키마 유형에 대한 속성 값을 가져올 수 없습니다.	자세한 내용은 서비스 관리 로그를 참조하십시오.

표 C–3 Access Manager 콘솔에 대한 로그 참조 *(계속)*

아이디	로그 수준	설명	데이터	트리거	조치
2005	정보	서비스 스키마의 스키마 유형에 대한 속성 값을 가져오지 못함	서비스 이름스키마 유형 이름속성 스키마 이름	서비스 프로필 페이지를 봅니다.	이 이벤트에 대해서는 조치가 필요 없습니다. 콘솔이 서비스에서 스키마를 가져오기를 시도했지만 스키마가 없습니다.
2011	정보	서비스 스키마의 스키마 유형에 대한 속성 스키마의 속성 값 가져오기 시도	서비스 이름스키마 유형 이름속성 스키마 이름	서비스 프로필 페이지를 봅니다.	
2012	정보	서비스 스키마의 스키마 유형에 대한 속성 스키마의 속성 값을 가져옴	서비스 이름스키마 유형 이름속성 스키마 이름	서비스 프로필 페이지를 봅니다.	
2013	심각	서비스 스키마의 스키마 유형에 대한 속성 스키마의 속성 값을 가져오지 못함	서비스 이름스키마 유형 이름속성 스키마 이름오류 메시지	서비스 스키마의 스키마 유형에 대한 속성 값을 가져올 수 없습니다. 사용자의 단일 사인온 토큰이 만료되었거나 사용자에게 이 작업을 수행할 권한이 없을 수 있습니다.	자세한 내용은 서비스 관리 로그를 참조하십시오.

표 C–3 Access Manager 콘솔에 대한 로그 참조 *(계속)*

아이디	로그 수준	설명	데이터	트리거	조치
2014	심각	서비스 스키마의 스키마 유형에 대한 속성 스키마의 속성 값을 가져오지 못함	서비스 이름스키마 유형 이름속성 스키마 이름오류 메시지	서비스 관리 SDK 관련 오류로 인해 서비스 스키마의 스키마 유형에 대한 속성 값을 가져올 수 없습니다.	자세한 내용은 서비스 관리 로그를 참조하십시오.
2021	정보	서비스 스키마의 스키마 유형에 대한 속성 스키마의 속성 값 수정 시도	서비스 이름스키마 유형 이름속성 스키마 이름	서비스 프로필 페이지에서 저장 버튼을 누릅니다.	
2022	정보	서비스 스키마의 스키마 유형에 대한 속성 스키마의 속성 값을 수정함	서비스 이름스키마 유형 이름속성 스키마 이름	서비스 프로필 페이지에서 저장 버튼을 누릅니다.	
2023	심각	서비스 스키마의 스키마 유형에 대한 속성 스키마의 속성 값을 수정하지 못함	서비스 이름스키마 유형 이름속성 스키마 이름오류 메시지	서비스 스키마의 스키마 유형에 대한 속성 값을 수정할 수 없습니다. 사용자의 싱글 사인온 토큰이 만료되었거나 이 작업을 수행할 권한이 사용자에게 없을 수 있습니다.	자세한 내용은 서비스 관리 로그를 참조하십시오.

표 C–3 Access Manager 콘솔에 대한 로그 참조 *(계속)*

아이디	로그 수준	설명	데이터	트리거	조치
2024	심각	서비스 스키마의 스키마 유형에 대한 속성 스키마의 속성 값을 수정하지 못함	서비스 이름스키마 유형 이름속성 스키마 이름오류 메시지	서비스 관리 SDK 관련 오류로 인해 서비스 스키마의 스키마 유형에 대한 속성 값을 수정할 수 없습니다.	자세한 내용은 서비스 관리 로그를 참조하십시오.
2501	정보	클라이언트 검색 서비스의 장치 이름 가져오기 시도	프로필 이름스타일 이름검색 패턴	클라이언트 프로필 페이지를 봅니다.	
2502	정보	클라이언트 검색 서비스의 장치 이름을 가져옴	프로필 이름스타일 이름검색 패턴	클라이언트 프로필 페이지를 봅니다.	
2511	정보	클라이언트 검색 서비스에서 클라이언트 삭제 시도	클라이언트 유형	클라이언트 유형 삭제 하이퍼링크 페이지를 누릅니다.	
2512	정보	클라이언트 검색 서비스에서 클라이언트를 삭제함	클라이언트 유형	클라이언트 유형 삭제 하이퍼링크 페이지를 누릅니다.	
2513	심각	클라이언트 검색 서비스에서 클라이언트를 삭제하지 못함	클라이언트 유형오류 메시지	클라이언트 검색 SDK 관련 오류로 인해 클라이언트를 삭제할 수 없습니다.	자세한 내용은 클라이언트 검색 관리 로그를 참조하십시오.
2521	정보	클라이언트 검색 서비스에서 클라이언트 생성 시도	클라이언트 유형	클라이언트 만들기 페이지에서 새로 만들기 버튼을 누릅니다.	

표 C–3 Access Manager 콘솔에 대한 로그 참조 *(계속)*

아이디	로그 수준	설명	데이터	트리거	조치
2522	정보	클라이언트 검색 서비스에서 클라이언트를 생성함	클라이언트 유형	클라이언트 만들기 페이지에서 새로 만들기 버튼을 누릅니다.	
2523	심각	클라이언트 검색 서비스에서 클라이언트를 생성하지 못함	클라이언트 유형오류 메시지	클라이언트 검색 SDK 관련 오류로 인해 클라이언트를 생성할 수 없습니다.	자세한 내용은 클라이언트 검색 관리 로그를 참조하십시오.
2524	정보	클라이언트 검색 서비스에서 클라이언트를 생성하지 못함	클라이언트 유형오류 메시지	클라이언트 유형이 유효하지 않으므로 클라이언트를 생성할 수 없습니다.	만들기 전에 클라이언트 유형을 다시 확인하십시오.
2531	정보	클라이언트 검색 서비스에서 클라이언트 프로필 가져오기 시도	클라이언트 유형분류	클라이언트 프로필 페이지를 봅니다.	
2532	정보	클라이언트 검색 서비스에서 클라이언트 프로필을 가져옴	클라이언트 유형분류	클라이언트 프로필 페이지를 봅니다.	
2541	정보	클라이언트 검색 서비스에서 클라이언트 프로필 수정 시도	클라이언트 유형	클라이언트 프로필 페이지에서 저장 버튼을 누릅니다.	

표 C–3 Access Manager 콘솔에 대한 로그 참조 *(계속)*

아이디	로그 수준	설명	데이터	트리거	조치
2542	정보	클라이언트 검색 서비스에서 클라이언트 프로필을 수정함	클라이언트 유형	클라이언트 프로필 페이지에서 저장 버튼을 누릅니다.	
2543	심각	클라이언트 검색 서비스에서 클라이언트 프로필을 수정하지 못함	클라이언트 유형오류 메시지	클라이언트 검색 SDK 관련 오류로 인해 클라이언트 프로필을 수정할 수 없습니다.	자세한 내용은 클라이언트 검색 관리 로그를 참조하십시오.
3001	정보	현재 세션 가져오기 시도	서버 이름검색 패턴	세션 기본 페이지를 봅니다.	
3002	정보	현재 세션을 가져옴	서버 이름검색 패턴	세션 기본 페이지를 봅니다.	
3003	심각	현재 세션을 가져오지 못함	서버 이름영역 이름오류 메시지	세션 SDK 예외로 인해 현재 세션을 가져올 수 없습니다.	자세한 내용은 세션 관리 로그를 참조하십시오.
3011	정보	세션 무효화 시도	세션 이름세션 아이디	세션 기본 페이지에서 무효화 버튼을 누릅니다.	
3012	정보	세션을 무효화함	세션 이름세션 아이디	세션 기본 페이지에서 무효화 버튼을 누릅니다.	
3013	심각	세션을 무효화하지 못함	서버 이름세션 아이디오류 메시지	세션 SDK 예외로 인해 세션을 무효화할 수 없습니다.	자세한 내용은 세션 관리 로그를 참조하십시오.

표 C–3 Access Manager 콘솔에 대한 로그 참조 *(계속)*

아이디	로그 수준	설명	데이터	트리거	조치
10001	정보	조직에서 컨테이너 검색 시도	조직 DN검색 패턴	조직의 컨테이너 페이지에서 검색 버튼을 누릅니다.	
10002	정보	조직에서 컨테이너를 검색함	조직 DN검색 패턴	조직의 컨테이너 페이지에서 검색 버튼을 누릅니다.	
10003	심각	조직에서 컨테이너를 검색하지 못함	조직 DN검색 패턴오류 메시지	컨테이너를 검색할 수 없습니다. 사용자의 단일 사인온 토큰이 만료되었거나 이 작업을 수행할 권한이 사용자에게 없을 수 있습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.
10004	심각	조직에서 컨테이너를 검색하지 못함	조직 DN검색 패턴오류 메시지	액세스 관리 SDK 예외로 인해 컨테이너를 검색할 수 없습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.
10011	정보	컨테이너에서 컨테이너 검색 시도	컨테이너 DN검색 패턴	컨테이너의 하위 컨테이너 페이지에서 검색 버튼을 누릅니다.	
10012	정보	컨테이너에서 컨테이너를 검색함	컨테이너 DN검색 패턴	컨테이너의 하위 컨테이너 페이지에서 검색 버튼을 누릅니다.	

표 C–3 Access Manager 콘솔에 대한 로그 참조 *(계속)*

아이디	로그 수준	설명	데이터	트리거	조치
10013	심각	컨테이너에서 컨테이너를 검색하지 못함	컨테이너 DN검색 패턴오류 메시지	컨테이너를 검색할 수 없습니다. 사용자의 단일 사인온 토큰이 만료되었거나 이 작업을 수행할 권한이 사용자에게 없을 수 있습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.
10014	심각	컨테이너에서 컨테이너를 검색하지 못함	컨테이너 DN검색 패턴오류 메시지	액세스 관리 SDK 예외로 인해 컨테이너를 검색할 수 없습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.
10021	정보	조직에서 컨테이너 생성 시도	조직 DN컨테이너 이름	컨테이너 만들기 페이지에서 새로 만들기 버튼을 누릅니다.	
10022	정보	조직에서 컨테이너를 생성함	조직 DN컨테이너 이름	컨테이너 만들기 페이지에서 새로 만들기 버튼을 누릅니다.	
10023	심각	조직에서 컨테이너를 생성하지 못함	조직 DN컨테이너 이름오류 메시지	컨테이너를 생성할 수 없습니다. 사용자의 단일 사인온 토큰이 만료되었거나 사용자에게 이 작업을 수행할 권한이 없을 수 있습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.

표 C–3 Access Manager 콘솔에 대한 로그 참조 *(계속)*

아이디	로그 수준	설명	데이터	트리거	조치
10024	심각	조직에서 컨테이너를 생성하지 못함	조직 DN컨테이너 이름오류 메시지	액세스 관리 SDK 예외로 인해 컨테이너를 생성할 수 없습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.
10031	정보	컨테이너에서 컨테이너 생성 시도	컨테이너 DN컨테이너 이름	컨테이너 만들기 페이지에서 새로 만들기 버튼을 누릅니다.	
10032	정보	컨테이너에서 컨테이너를 생성함	컨테이너 DN컨테이너 이름	컨테이너 만들기 페이지에서 새로 만들기 버튼을 누릅니다.	
10033	심각	컨테이너에서 컨테이너를 생성하지 못함	컨테이너 DN컨테이너 이름오류 메시지	컨테이너를 생성할 수 없습니다. 사용자의 단일 사인온 토큰이 만료되었거나 사용자에게 이 작업을 수행할 권한이 없을 수 있습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.
10034	심각	컨테이너에서 컨테이너를 생성하지 못함	컨테이너 DN컨테이너 이름오류 메시지	액세스 관리 SDK 예외로 인해 컨테이너를 생성할 수 없습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.
10041	정보	컨테이너에 할당한 서비스 가져오기 시도	컨테이너 DN	컨테이너의 서비스 프로필 페이지를 봅니다.	
10042	정보	컨테이너에 할당한 서비스를 가져옴	컨테이너 DN	컨테이너의 서비스 프로필 페이지를 봅니다.	

표 C–3 Access Manager 콘솔에 대한 로그 참조 *(계속)*

아이디	로그 수준	설명	데이터	트리거	조치
10043	심각	컨테이너에 할당한 서비스를 가져오지 못함	컨테이너 DN오류 메시지	컨테이너에 할당한 서비스를 가져올 수 없습니다. 사용자의 단일 사인온 토큰이 만료되었거나 사용자에게 이 작업을 수행할 권한이 사용자에게 없을 수 있습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.
10044	심각	컨테이너에 할당한 서비스를 가져오지 못함	컨테이너 DN오류 메시지	액세스 관리 SDK 예외로 인해 컨테이너에 할당한 서비스를 가져올 수 없습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.
10101	정보	조직에서 서비스 템플리트 가져오기 시도	조직 DN서비스 이름템플리트 유형	조직의 서비스 프로필 페이지를 봅니다.	
10102	정보	조직에서 서비스 템플리트를 가져옴	조직 DN서비스 이름템플리트 유형	조직의 서비스 프로필 페이지를 봅니다.	
10103	심각	조직에서 서비스 템플리트를 가져오지 못함	조직 DN서비스 이름템플리트 유형오류 메시지	서비스 템플리트를 가져올 수 없습니다. 사용자의 단일 사인온 토큰이 만료되었거나 사용자에게 이 작업을 수행할 권한이 없을 수 있습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.

표 C–3 Access Manager 콘솔에 대한 로그 참조 *(계속)*

아이디	로그 수준	설명	데이터	트리거	조치
10104	심각	조직에서 서비스 템플리트를 가져오지 못함	조직 DN서비스 이름템플리트 유형오류 메시지	액세스 관리 SDK 예외로 인해 서비스 템플리트를 가져올 수 없습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.
10111	정보	컨테이너에서 서비스 템플리트 가져오기 시도	컨테이너 DN서비스 이름템플리트 유형	컨테이너의 서비스 프로필 페이지를 봅니다.	
10112	정보	컨테이너에서 서비스 템플리트를 가져옴	컨테이너 DN서비스 이름템플리트 유형	컨테이너의 서비스 프로필 페이지를 봅니다.	
10113	심각	컨테이너에서 서비스 템플리트를 가져오지 못함	컨테이너 DN서비스 이름템플리트 유형오류 메시지	서비스 템플리트를 가져올 수 없습니다. 사용자의 단일 사인온 토큰이 만료되었거나 사용자에게 이 작업을 수행할 권한이 없을 수 있습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.
10114	심각	컨테이너에서 서비스 템플리트를 가져오지 못함	컨테이너 DN서비스 이름템플리트 유형오류 메시지	액세스 관리 SDK 예외로 인해 서비스 템플리트를 가져올 수 없습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.
10121	정보	디렉토리 객체 삭제 시도	객체 이름	객체 기본 페이지에서 삭제 버튼을 누릅니다.	
10122	정보	디렉토리 객체를 삭제함	객체 이름	객체 기본 페이지에서 삭제 버튼을 누릅니다.	

표 C–3 Access Manager 콘솔에 대한 로그 참조 *(계속)*

아이디	로그 수준	설명	데이터	트리거	조치
10123	심각	디렉토리 객체를 삭제하지 못함	객체 이름오류 메시지	디렉토리 객체를 삭제할 수 없습니다. 사용자의 단일 사인온 토큰이 만료되었거나 이 작업을 수행할 권한이 사용자에게 없을 수 있습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.
10124	심각	디렉토리 객체를 삭제하지 못함	객체 이름오류 메시지	액세스 관리 SDK 예외로 인해 디렉토리 객체를 삭제할 수 없습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.
10131	정보	디렉토리 객체 수정 시도	객체 DN	객체 프로필 페이지를 누릅니다.	
10132	정보	디렉토리 객체를 수정함	객체 DN	객체 프로필 페이지를 누릅니다.	
10133	심각	디렉토리 객체를 수정하지 못함	객체 DN오류 메시지	액세스 관리 SDK 예외로 인해 디렉토리 객체를 수정할 수 없습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.
10141	정보	조직에서 서비스 삭제 시도	조직 DN서비스 이름	조직의 서비스 페이지에서 할당 제거 버튼을 누릅니다.	
10142	정보	조직에서 서비스를 삭제함	조직 DN서비스 이름	조직의 서비스 페이지에서 할당 제거 버튼을 누릅니다.	

표 C–3 Access Manager 콘솔에 대한 로그 참조 *(계속)*

아이디	로그 수준	설명	데이터	트리거	조치
10143	심각	조직에서 서비스를 삭제하지 못함	조직 DN서비스 이름오류 메시지	서비스를 삭제할 수 없습니다. 사용자의 단일 사인온 토큰이 만료되었거나 사용자에게 이 작업을 수행할 권한이 없을 수 있습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.
10144	심각	조직에서 서비스를 삭제하지 못함	조직 DN서비스 이름오류 메시지	액세스 관리 SDK 예외로 인해 서비스를 삭제할 수 없습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.
10151	정보	컨테이너에서 서비스 삭제 시도	컨테이너 DN서비스 이름	컨테이너의 서비스 페이지에서 할당 해제 버튼을 누릅니다.	
10152	정보	컨테이너에서 서비스를 삭제함	컨테이너 DN서비스 이름	컨테이너의 서비스 페이지에서 할당 해제 버튼을 누릅니다.	
10153	심각	컨테이너에서 서비스를 삭제하지 못함	컨테이너 DN서비스 이름오류 메시지	서비스를 삭제할 수 없습니다. 사용자의 단일 사인온 토큰이 만료되었거나 사용자에게 이 작업을 수행할 권한이 없을 수 있습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.
10154	심각	컨테이너에서 서비스를 삭제하지 못함	컨테이너 DN서비스 이름오류 메시지	액세스 관리 SDK 예외로 인해 서비스를 삭제할 수 없습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.

표 C–3 Access Manager 콘솔에 대한 로그 참조 *(계속)*

아이디	로그 수준	설명	데이터	트리거	조치
10201	정보	조직에서 그룹 컨테이너 검색 시도	조직 DN검색 패턴	조직의 그룹 컨테이너 페이지에서 검색 버튼을 누릅니다.	
10202	정보	조직에서 그룹 컨테이너를 검색함	조직 DN검색 패턴	조직의 그룹 컨테이너 페이지에서 검색 버튼을 누릅니다.	
10203	심각	조직에서 그룹 컨테이너를 검색하지 못함	조직 DN검색 패턴오류 메시지	그룹 컨테이너를 검색할 수 없습니다. 사용자의 단일 사인온 토큰이 만료되었거나 이 작업을 수행할 권한이 사용자에게 없을 수 있습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.
10204	심각	조직에서 그룹 컨테이너를 검색하지 못함	조직 DN검색 패턴오류 메시지	액세스 관리 SDK 예외로 인해 그룹 컨테이너를 검색할 수 없습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.
10211	정보	컨테이너에서 그룹 컨테이너 검색 시도	컨테이너 DN검색 패턴	컨테이너의 그룹 컨테이너 페이지에서 검색 버튼을 누릅니다.	
10212	정보	컨테이너에서 그룹 컨테이너를 검색함	컨테이너 DN검색 패턴	컨테이너의 그룹 컨테이너 페이지에서 검색 버튼을 누릅니다.	

표 C–3 Access Manager 콘솔에 대한 로그 참조 *(계속)*

아이디	로그 수준	설명	데이터	트리거	조치
10213	심각	컨테이너에서 그룹 컨테이너를 검색하지 못함	컨테이너 DN검색 패턴오류 메시지	그룹 컨테이너를 검색할 수 없습니다. 사용자의 단일 사인온 토큰이 만료되었거나 이 작업을 수행할 권한이 사용자에게 없을 수 있습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.
10214	심각	컨테이너에서 그룹 컨테이너를 검색하지 못함	컨테이너 DN검색 패턴오류 메시지	액세스 관리 SDK 예외로 인해 그룹 컨테이너를 검색할 수 없습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.
10221	정보	그룹 컨테이너에서 그룹 컨테이너 검색 시도	그룹 컨테이너 DN검색 패턴	그룹 컨테이너의 그룹 컨테이너 페이지에서 검색 버튼을 누릅니다.	
10222	정보	그룹 컨테이너에서 그룹 컨테이너를 검색함	그룹 컨테이너 DN검색 패턴	그룹 컨테이너의 그룹 컨테이너 페이지에서 검색 버튼을 누릅니다.	
10223	심각	그룹 컨테이너에서 그룹 컨테이너를 검색하지 못함	그룹 컨테이너 DN검색 패턴오류 메시지	그룹 컨테이너를 검색할 수 없습니다. 사용자의 단일 사인온 토큰이 만료되었거나 이 작업을 수행할 권한이 사용자에게 없을 수 있습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.

표 C–3 Access Manager 콘솔에 대한 로그 참조 *(계속)*

아이디	로그 수준	설명	데이터	트리거	조치
10224	심각	그룹 컨테이너에서 그룹 컨테이너를 검색하지 못함	그룹 컨테이너 DN검색 패턴오류 메시지	액세스 관리 SDK 예외로 인해 그룹 컨테이너를 검색할 수 없습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.
10231	정보	조직에서 그룹 컨테이너 생성 시도	조직 DN그룹 컨테이너 이름	그룹 컨테이너 만들기 페이지에서 새로 만들기 버튼을 누릅니다.	
10232	정보	조직에서 그룹 컨테이너를 생성함	조직 DN그룹 컨테이너 이름	그룹 컨테이너 만들기 페이지에서 새로 만들기 버튼을 누릅니다.	
10233	심각	조직에서 그룹 컨테이너를 생성하지 못함	조직 DN그룹 컨테이너 이름오류 메시지	그룹 컨테이너를 생성할 수 없습니다. 사용자의 단일 사인온 토큰이 만료되었거나 이 작업을 수행할 권한이 사용자에게 없을 수 있습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.
10234	심각	조직에서 그룹 컨테이너를 생성하지 못함	조직 DN그룹 컨테이너 이름오류 메시지	액세스 관리 SDK 예외로 인해 그룹 컨테이너를 생성할 수 없습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.
10241	정보	컨테이너에서 그룹 컨테이너 생성 시도	컨테이너 DN그룹 컨테이너 이름	그룹 컨테이너 만들기 페이지에서 새로 만들기 버튼을 누릅니다.	

표 C–3 Access Manager 콘솔에 대한 로그 참조 *(계속)*

아이디	로그 수준	설명	데이터	트리거	조치
10242	정보	컨테이너에서 그룹 컨테이너를 생성함	컨테이너 DN그룹 컨테이너 이름	그룹 컨테이너 만들기 페이지에서 새로 만들기 버튼을 누릅니다.	
10243	심각	컨테이너에서 그룹 컨테이너를 생성하지 못함	컨테이너 DN그룹 컨테이너 이름오류 메시지	그룹 컨테이너를 생성할 수 없습니다. 사용자의 단일 사인온 토큰이 만료되었거나 이 작업을 수행할 권한이 사용자에게 없을 수 있습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.
10244	심각	컨테이너에서 그룹 컨테이너를 생성하지 못함	컨테이너 DN그룹 컨테이너 이름오류 메시지	액세스 관리 SDK 예외로 인해 그룹 컨테이너를 생성할 수 없습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.
10251	정보	그룹 컨테이너에서 그룹 컨테이너 생성 시도	그룹 컨테이너 DN그룹 컨테이너 이름	그룹 컨테이너 만들기 페이지에서 새로 만들기 버튼을 누릅니다.	
10252	정보	그룹 컨테이너에서 그룹 컨테이너를 생성함	그룹 컨테이너 DN그룹 컨테이너 이름	그룹 컨테이너 만들기 페이지에서 새로 만들기 버튼을 누릅니다.	

표 C–3 Access Manager 콘솔에 대한 로그 참조 *(계속)*

아이디	로그 수준	설명	데이터	트리거	조치
10253	심각	그룹 컨테이너에서 그룹 컨테이너를 생성하지 못함	그룹 컨테이너 DN그룹 컨테이너 이름오류 메시지	그룹 컨테이너를 생성할 수 없습니다. 사용자의 단일 사인온 토큰이 만료되었거나 이 작업을 수행할 권한이 사용자에게 없을 수 있습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.
10254	심각	그룹 컨테이너에서 그룹 컨테이너를 생성하지 못함	그룹 컨테이너 DN그룹 컨테이너 이름오류 메시지	액세스 관리 SDK 예외로 인해 그룹 컨테이너를 생성할 수 없습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.
10301	정보	조직에서 그룹 검색 시도	조직 DN검색 패턴	조직의 그룹 페이지에서 검색 버튼을 누릅니다.	
10302	정보	조직에서 그룹을 검색함	조직 DN검색 패턴	조직의 그룹 페이지에서 검색 버튼을 누릅니다.	
10303	심각	조직에서 그룹을 검색하지 못함	조직 DN검색 패턴오류 메시지	그룹을 검색할 수 없습니다. 사용자의 단일 사인온 토큰이 만료되었거나 사용자에게 이 작업을 수행할 권한이 없을 수 있습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.
10304	심각	조직에서 그룹을 검색하지 못함	조직 DN검색 패턴오류 메시지	액세스 관리 SDK 예외로 인해 그룹을 검색할 수 없습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.

표 C–3 Access Manager 콘솔에 대한 로그 참조 *(계속)*

아이디	로그 수준	설명	데이터	트리거	조치
10311	정보	컨테이너에서 그룹 검색 시도	컨테이너 DN검색 패턴	컨테이너의 그룹 페이지에서 검색 버튼을 누릅니다.	
10312	정보	컨테이너에서 그룹을 검색함	컨테이너 DN검색 패턴	컨테이너의 그룹 페이지에서 검색 버튼을 누릅니다.	
10313	심각	컨테이너에서 그룹을 검색하지 못함	컨테이너 DN검색 패턴오류 메시지	그룹을 검색할 수 없습니다. 사용자의 단일 사인온 토큰이 만료되었거나 사용자에게 이 작업을 수행할 권한이 없을 수 있습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.
10314	심각	컨테이너에서 그룹을 검색하지 못함	컨테이너 DN검색 패턴오류 메시지	액세스 관리 SDK 예외로 인해 그룹을 검색할 수 없습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.
10321	정보	정적 그룹에서 그룹 검색 시도	정적 그룹 DN검색 패턴	정적 그룹의 그룹 페이지에서 검색 버튼을 누릅니다.	
10322	정보	정적 그룹에서 그룹을 검색함	정적 그룹 DN검색 패턴	정적 그룹의 그룹 페이지에서 검색 버튼을 누릅니다.	

표 C–3 Access Manager 콘솔에 대한 로그 참조 *(계속)*

아이디	로그 수준	설명	데이터	트리거	조치
10323	심각	정적 그룹에서 그룹을 검색하지 못함	정적 그룹 DN검색 패턴오류 페이지	그룹을 검색할 수 없습니다. 사용자의 단일 사인온 토큰이 만료되었거나 사용자에게 이 작업을 수행할 권한이 없을 수 있습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.
10324	심각	정적 그룹에서 그룹을 검색하지 못함	정적 그룹 DN검색 패턴오류 페이지	액세스 관리 SDK 예외로 인해 그룹을 검색할 수 없습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.
10331	정보	동적 그룹에서 그룹 검색 시도	동적 그룹 DN검색 패턴	동적 그룹의 그룹 페이지에서 검색 버튼을 누릅니다.	
10332	정보	동적 그룹에서 그룹을 검색함	동적 그룹 DN검색 패턴	동적 그룹의 그룹 페이지에서 검색 버튼을 누릅니다.	
10333	심각	동적 그룹에서 그룹을 검색하지 못함	동적 그룹 DN검색 패턴오류 메시지	그룹을 검색할 수 없습니다. 사용자의 단일 사인온 토큰이 만료되었거나 사용자에게 이 작업을 수행할 권한이 없을 수 있습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.
10334	심각	동적 그룹에서 그룹을 검색하지 못함	동적 그룹 DN검색 패턴오류 메시지	액세스 관리 SDK 예외로 인해 그룹을 검색할 수 없습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.

표 C–3 Access Manager 콘솔에 대한 로그 참조 *(계속)*

아이디	로그 수준	설명	데이터	트리거	조치
10341	정보	할당 가능 동적 그룹에서 그룹 검색 시도	할당 가능 동적 그룹 DN검색 패턴	할당 가능 동적 그룹의 그룹 페이지에서 검색 버튼을 누릅니다.	
10342	정보	할당 가능 동적 그룹에서 그룹을 검색함	할당 가능 동적 그룹 DN검색 패턴	할당 가능 동적 그룹의 그룹 페이지에서 검색 버튼을 누릅니다.	
10343	심각	할당 가능 동적 그룹에서 그룹을 검색하지 못함	할당 가능 동적 그룹 DN검색 패턴오류 메시지	그룹을 검색할 수 없습니다. 사용자의 단일 사인온 토큰이 만료되었거나 사용자에게 이 작업을 수행할 권한이 없을 수 있습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.
10344	심각	할당 가능 동적 그룹에서 그룹을 검색하지 못함	할당 가능 동적 그룹 DN검색 패턴오류 메시지	액세스 관리 SDK 예외로 인해 그룹을 검색할 수 없습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.
10351	정보	조직에서 그룹 생성 시도	조직 DN그룹 이름	그룹 만들기 페이지에서 새로 만들기 버튼을 누릅니다.	
10352	정보	조직에서 그룹을 생성함	조직 DN그룹 이름	그룹 만들기 페이지에서 새로 만들기 버튼을 누릅니다.	

표 C–3 Access Manager 콘솔에 대한 로그 참조 *(계속)*

아이디	로그 수준	설명	데이터	트리거	조치
10353	심각	조직에서 그룹을 생성하지 못함	조직 DN그룹 이름오류 메시지	그룹을 생성할 수 없습니다. 사용자의 단일 사인온 토큰이 만료되었거나 사용자에게 이 작업을 수행할 권한이 없을 수 있습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.
10354	심각	조직에서 그룹을 생성하지 못함	조직 DN그룹 이름오류 메시지	액세스 관리 SDK 예외로 인해 그룹을 생성할 수 없습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.
10361	정보	컨테이너에서 그룹 생성 시도	컨테이너 DN그룹 이름	그룹 만들기 페이지에서 새로 만들기 버튼을 누릅니다.	
10362	정보	컨테이너에서 그룹을 생성하지 못함	컨테이너 DN그룹 이름	그룹 만들기 페이지에서 새로 만들기 버튼을 누릅니다.	
10363	심각	컨테이너에서 그룹을 생성하지 못함	컨테이너 DN그룹 이름오류 메시지	그룹을 생성할 수 없습니다. 사용자의 단일 사인온 토큰이 만료되었거나 사용자에게 이 작업을 수행할 권한이 없을 수 있습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.
10364	심각	컨테이너에서 그룹을 생성하지 못함	컨테이너 DN그룹 이름오류 메시지	액세스 관리 SDK 예외로 인해 그룹을 생성할 수 없습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.

표 C–3 Access Manager 콘솔에 대한 로그 참조 *(계속)*

아이디	로그 수준	설명	데이터	트리거	조치
10371	정보	그룹 컨테이너에서 그룹 생성 시도	그룹 컨테이너 DN그룹 이름	그룹 만들기 페이지에서 새로 만들기 버튼을 누릅니다.	
10372	정보	그룹 컨테이너에서 그룹을 생성함	그룹 컨테이너 DN그룹 이름	그룹 만들기 페이지에서 새로 만들기 버튼을 누릅니다.	
10373	심각	그룹 컨테이너에서 그룹을 생성하지 못함	그룹 컨테이너 DN그룹 이름오류 메시지	그룹을 생성할 수 없습니다. 사용자의 단일 사인온 토큰이 만료되었거나 사용자에게 이 작업을 수행할 권한이 없을 수 있습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.
10374	심각	그룹 컨테이너에서 그룹을 생성하지 못함	그룹 컨테이너 DN그룹 이름오류 메시지	액세스 관리 SDK 예외로 인해 그룹을 생성할 수 없습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.
10381	정보	동적 그룹에서 그룹 생성 시도	동적 그룹 DN그룹 이름	그룹 만들기 페이지에서 새로 만들기 버튼을 누릅니다.	
10382	정보	동적 그룹에서 그룹을 생성함	동적 그룹 DN그룹 이름	그룹 만들기 페이지에서 새로 만들기 버튼을 누릅니다.	

표 C–3 Access Manager 콘솔에 대한 로그 참조 *(계속)*

아이디	로그 수준	설명	데이터	트리거	조치
10383	심각	동적 그룹에서 그룹을 생성하지 못함	동적 그룹 DN그룹 이름오류 메시지	그룹을 생성할 수 없습니다. 사용자의 단일 사인온 토큰이 만료되었거나 사용자에게 이 작업을 수행할 권한이 없을 수 있습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.
10384	심각	동적 그룹에서 그룹을 생성하지 못함	동적 그룹 DN그룹 이름오류 메시지	액세스 관리 SDK 예외로 인해 그룹을 생성할 수 없습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.
10391	정보	정적 그룹에서 그룹 생성 시도	정적 그룹 DN그룹 이름	그룹 만들기 페이지에서 새로 만들기 버튼을 누릅니다.	
10392	정보	정적 그룹에서 그룹을 생성함	정적 그룹 DN그룹 이름	그룹 만들기 페이지에서 새로 만들기 버튼을 누릅니다.	
10393	심각	정적 그룹에서 그룹을 생성하지 못함	정적 그룹 DN그룹 이름오류 메시지	그룹을 생성할 수 없습니다. 사용자의 단일 사인온 토큰이 만료되었거나 사용자에게 이 작업을 수행할 권한이 없을 수 있습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.
10394	심각	정적 그룹에서 그룹을 생성하지 못함	정적 그룹 DN그룹 이름오류 메시지	액세스 관리 SDK 예외로 인해 그룹을 생성할 수 없습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.

표 C–3 Access Manager 콘솔에 대한 로그 참조 *(계속)*

아이디	로그 수준	설명	데이터	트리거	조치
10401	정보	할당 가능 동적 그룹에서 그룹 생성 시도	할당 가능 동적 그룹 DN그룹 이름	그룹 만들기 페이지에서 새로 만들기 버튼을 누릅니다.	
10402	정보	할당 가능 동적 그룹에서 그룹을 생성함	할당 가능 동적 그룹 DN그룹 이름	그룹 만들기 페이지에서 새로 만들기 버튼을 누릅니다.	
10403	심각	할당 가능 동적 그룹에서 그룹을 생성하지 못함	할당 가능 동적 그룹 DN그룹 이름오류 메시지	그룹을 생성할 수 없습니다. 사용자의 단일 사인온 토큰이 만료되었거나 사용자에게 이 작업을 수행할 권한이 없을 수 있습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.
10404	심각	할당 가능 동적 그룹에서 그룹을 생성하지 못함	할당 가능 동적 그룹 DN그룹 이름오류 메시지	액세스 관리 SDK 예외로 인해 그룹을 생성할 수 없습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.
10411	정보	그룹 수정 시도	그룹 DN	그룹 프로필 페이지에서 저장 버튼을 누릅니다.	
10412	정보	그룹을 수정함	그룹 DN	그룹 프로필 페이지에서 저장 버튼을 누릅니다.	
10414	심각	그룹을 수정하지 못함	할당 가능 동적 그룹 DN그룹 이름오류 메시지	액세스 관리 SDK 예외로 인해 그룹을 수정할 수 없습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.
10421	정보	그룹에서 사용자 검색 시도	그룹 DN검색 패턴	그룹의 사용자 페이지를 봅니다.	

표 C–3 Access Manager 콘솔에 대한 로그 참조 *(계속)*

아이디	로그 수준	설명	데이터	트리거	조치
10422	정보	그룹에서 사용자를 검색함	그룹 DN검색 패턴	그룹의 사용자 페이지를 봅니다.	
10423	심각	그룹에서 사용자를 검색하지 못함	그룹 DN검색 패턴오류 메시지	사용자를 검색할 수 없습니다. 사용자의 단일 사인온 토큰이 만료되었거나 사용자에게 이 작업을 수행할 권한이 없을 수 있습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.
10424	심각	그룹에서 사용자를 검색하지 못함	그룹 DN검색 패턴오류 메시지	액세스 관리 SDK 예외로 인해 사용자를 검색할 수 없습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.
10431	정보	중첩 그룹 가져오기 시도	그룹 DN	그룹의 구성원 페이지를 봅니다.	
10432	정보	중첩 그룹을 가져옴	그룹 DN	그룹의 구성원 페이지를 봅니다.	
10433	심각	중첩 그룹을 가져오지 못함	그룹 DN오류 메시지	중첩 그룹을 가져올 수 없습니다. 사용자의 단일 사인온 토큰이 만료되었거나 사용자에게 이 작업을 수행할 권한이 없을 수 있습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.
10434	심각	중첩 그룹을 가져오지 못함	그룹 DN오류 메시지	액세스 관리 SDK 예외로 인해 중첩 그룹을 가져올 수 없습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.

표 C–3 Access Manager 콘솔에 대한 로그 참조 *(계속)*

아이디	로그 수준	설명	데이터	트리거	조치
10441	정보	중첩 그룹 제거 시도	그룹 DN중첩 그룹 *DN*	그룹의 구성원 페이지에서 제거 버튼을 누릅니다.	
10442	정보	중첩 그룹을 제거함	그룹 DN중첩 그룹 *DN*	그룹의 구성원 페이지에서 제거 버튼을 누릅니다.	
10443	심각	중첩 그룹을 제거하지 못함	그룹 DN중첩 그룹 *DN*오류 메시지	중첩 그룹을 제거할 수 없습니다. 사용자의 단일 사인온 토큰이 만료되었거나 사용자에게 이 작업을 수행할 권한이 없을 수 있습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.
10444	심각	중첩 그룹을 제거하지 못함	그룹 DN중첩 그룹 *DN*오류 메시지	액세스 관리 SDK 예외로 인해 중첩 그룹을 제거할 수 없습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.
10451	정보	그룹에서 사용자 제거 시도	그룹 DN사용자 *DN*	그룹의 구성원 페이지에서 제거 버튼을 누릅니다.	
10452	정보	그룹에서 사용자를 제거함	그룹 DN사용자 *DN*	그룹의 구성원 페이지에서 제거 버튼을 누릅니다.	
10453	심각	그룹에서 사용자를 제거하지 못함	그룹 DN사용자 *DN*오류 메시지	사용자를 제거할 수 없습니다. 사용자의 단일 사인온 토큰이 만료되었거나 사용자에게 이 작업을 수행할 권한이 없을 수 있습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.

표 C–3 Access Manager 콘솔에 대한 로그 참조 *(계속)*

아이디	로그 수준	설명	데이터	트리거	조치
10454	심각	그룹에서 사용자를 제거하지 못함	그룹 DN사용자 *DN*오류 메시지	액세스 관리 SDK 예외로 인해 사용자를 제거할 수 없습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.
10501	정보	조직에서 사용자 컨테이너 검색 시도	조직 DN검색 패턴	조직의 사용자 컨테이너 페이지를 봅니다.	
10502	정보	조직에서 사용자 컨테이너를 검색함	조직 DN검색 패턴	조직의 사용자 컨테이너 페이지를 봅니다.	
10503	심각	조직에서 사용자 컨테이너를 검색하지 못함	조직 DN검색 패턴오류 메시지	사용자 컨테이너를 검색할 수 없습니다. 사용자의 단일 사인온 토큰이 만료되었거나 사용자에게 이 작업을 수행할 권한이 없을 수 있습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.
10504	심각	조직에서 사용자 컨테이너를 검색하지 못함	조직 DN검색 패턴오류 메시지	액세스 관리 SDK 예외로 인해 사용자 컨테이너를 검색할 수 없습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.
10511	정보	컨테이너에서 사용자 컨테이너 검색 시도	컨테이너 DN검색 패턴	컨테이너의 사용자 컨테이너 페이지를 봅니다.	
10512	정보	컨테이너에서 사용자 컨테이너를 검색함	컨테이너 DN검색 패턴	컨테이너의 사용자 컨테이너 페이지를 봅니다.	

표 C–3 Access Manager 콘솔에 대한 로그 참조 *(계속)*

아이디	로그 수준	설명	데이터	트리거	조치
10513	심각	컨테이너에서 사용자 컨테이너를 검색하지 못함	컨테이너 DN검색 패턴오류 메시지	사용자 컨테이너를 검색할 수 없습니다. 사용자의 단일 사인온 토큰이 만료되었거나 사용자에게 이 작업을 수행할 권한이 없을 수 있습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.
10514	심각	컨테이너에서 사용자 컨테이너를 검색하지 못함	컨테이너 DN검색 패턴오류 메시지	액세스 관리 SDK 예외로 인해 사용자 컨테이너를 검색할 수 없습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.
10521	정보	사용자 컨테이너에서 사용자 컨테이너 검색 시도	사용자 컨테이너 DN검색 패턴	사용자 컨테이너의 사용자 컨테이너 페이지를 봅니다.	
10522	정보	사용자 컨테이너에서 사용자 컨테이너를 검색함	사용자 컨테이너 DN검색 패턴	사용자 컨테이너의 사용자 컨테이너 페이지를 봅니다.	
10523	심각	사용자 컨테이너에서 사용자 컨테이너를 검색하지 못함	사용자 컨테이너 DN검색 패턴오류 메시지	사용자 컨테이너를 검색할 수 없습니다. 사용자의 단일 사인온 토큰이 만료되었거나 사용자에게 이 작업을 수행할 권한이 없을 수 있습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.

표 C–3 Access Manager 콘솔에 대한 로그 참조 *(계속)*

아이디	로그 수준	설명	데이터	트리거	조치
10524	심각	사용자 컨테이너에서 사용자 컨테이너를 검색하지 못함	사용자 컨테이너 DN검색 패턴오류 메시지	액세스 관리 SDK 예외로 인해 사용자 컨테이너를 검색할 수 없습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.
10531	정보	조직에서 사용자 컨테이너 생성 시도	조직 DN사용자 컨테이너 이름	사용자 컨테이너 만들기 페이지에서 새로 만들기 버튼을 누릅니다.	
10532	정보	조직에서 사용자 컨테이너를 생성함	조직 DN사용자 컨테이너 이름	사용자 컨테이너 만들기 페이지에서 새로 만들기 버튼을 누릅니다.	
10533	심각	조직에서 사용자 컨테이너를 생성하지 못함	조직 DN사용자 컨테이너 이름오류 메시지	사용자 컨테이너를 생성할 수 없습니다. 사용자의 단일 사인온 토큰이 만료되었거나 사용자에게 이 작업을 수행할 권한이 없을 수 있습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.
10534	심각	조직에서 사용자 컨테이너를 생성하지 못함	조직 DN사용자 컨테이너 이름오류 메시지	액세스 관리 SDK 예외로 인해 사용자 컨테이너를 생성할 수 없습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.

표 C–3 Access Manager 콘솔에 대한 로그 참조 *(계속)*

아이디	로그 수준	설명	데이터	트리거	조치
10541	정보	컨테이너에서 사용자 컨테이너 생성 시도	컨테이너 DN사용자 컨테이너 이름	사용자 컨테이너 만들기 페이지에서 새로 만들기 버튼을 누릅니다.	
10542	정보	컨테이너에서 사용자 컨테이너를 생성함	컨테이너 DN사용자 컨테이너 이름	사용자 컨테이너 만들기 페이지에서 새로 만들기 버튼을 누릅니다.	
10543	심각	컨테이너에서 사용자 컨테이너를 생성하지 못함	컨테이너 DN사용자 컨테이너 이름오류 메시지	사용자 컨테이너를 생성할 수 없습니다. 사용자의 단일 사인온 토큰이 만료되었거나 사용자에게 이 작업을 수행할 권한이 없을 수 있습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.
10544	심각	컨테이너에서 사용자 컨테이너를 생성하지 못함	컨테이너 DN사용자 컨테이너 이름오류 메시지	액세스 관리 SDK 예외로 인해 사용자 컨테이너를 생성할 수 없습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.
10551	정보	사용자 컨테이너에서 사용자 컨테이너 생성 시도	사용자 컨테이너 DN사용자 컨테이너 이름	사용자 컨테이너 만들기 페이지에서 새로 만들기 버튼을 누릅니다.	

표 C–3 Access Manager 콘솔에 대한 로그 참조 *(계속)*

아이디	로그 수준	설명	데이터	트리거	조치
10552	정보	사용자 컨테이너에서 사용자 컨테이너를 생성함	사용자 컨테이너 DN사용자 컨테이너 이름	사용자 컨테이너 만들기 페이지에서 새로 만들기 버튼을 누릅니다.	
10553	심각	사용자 컨테이너에서 사용자 컨테이너를 생성하지 못함	사용자 컨테이너 DN사용자 컨테이너 이름오류 메시지	사용자 컨테이너를 생성할 수 없습니다. 사용자의 단일 사인온 토큰이 만료되었거나 사용자에게 이 작업을 수행할 권한이 없을 수 있습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.
10554	심각	사용자 컨테이너에서 사용자 컨테이너를 생성하지 못함	사용자 컨테이너 DN사용자 컨테이너 이름오류 메시지	액세스 관리 SDK 예외로 인해 사용자 컨테이너를 생성할 수 없습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.
10601	정보	조직에 할당한 서비스 가져오기 시도	조직 DN	조직의 서비스 프로필 페이지를 봅니다.	
10602	정보	조직에 할당한 서비스를 가져옴	조직 DN	조직의 서비스 프로필 페이지를 봅니다.	

표 C–3 Access Manager 콘솔에 대한 로그 참조 *(계속)*

아이디	로그 수준	설명	데이터	트리거	조치
10603	심각	조직에 할당한 서비스를 가져오지 못함	조직 DN오류 메시지	할당한 서비스를 가져올 수 없습니다. 사용자의 단일 사인온 토큰이 만료되었거나 이 작업을 수행할 권한이 사용자에게 없을 수 있습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.
10604	심각	조직에 할당한 서비스를 가져오지 못함	조직 DN오류 메시지	액세스 관리 SDK 예외로 인해 할당한 서비스를 가져올 수 없습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.
10611	정보	조직에서 서비스 제거 시도	조직 DN서비스 이름	조직의 서비스 프로필 페이지에서 할당 해제 버튼을 누릅니다.	
10612	정보	조직에서 서비스를 제거함	조직 DN서비스 이름	조직의 서비스 프로필 페이지에서 할당 해제 버튼을 누릅니다.	
10613	심각	조직에서 서비스를 제거하지 못함	조직 DN서비스 이름오류 메시지	서비스를 제거할 수 없습니다. 사용자의 단일 사인온 토큰이 만료되었거나 사용자에게 이 작업을 수행할 권한이 없을 수 있습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.

표 C–3 Access Manager 콘솔에 대한 로그 참조 *(계속)*

아이디	로그 수준	설명	데이터	트리거	조치
10614	심각	조직에서 서비스를 제거하지 못함	조직 DN서비스 이름오류 메시지	액세스 관리 SDK 예외로 인해 서비스를 제거할 수 없습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.
10621	정보	조직에서 조직 검색 시도	조직 DN검색 패턴	조직의 하위 조직 페이지를 봅니다.	
10622	정보	조직에서 조직을 검색함	조직 DN검색 패턴	조직의 하위 조직 페이지를 봅니다.	
10623	심각	조직에서 조직을 검색하지 못함	조직 DN검색 패턴오류 메시지	조직을 검색할 수 없습니다. 사용자의 단일 사인온 토큰이 만료되었거나 이 작업을 수행할 권한이 사용자에게 없을 수 있습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.
10624	심각	조직에서 조직을 검색하지 못함	조직 DN검색 패턴오류 메시지	액세스 관리 SDK 예외로 인해 조직을 검색할 수 없습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.
10631	정보	조직 수정 시도	조직 DN	조직 프로필 페이지에서 저장 버튼을 누릅니다.	
10632	정보	조직을 수정함	조직 DN	조직 프로필 페이지에서 저장 버튼을 누릅니다.	

표 C–3 Access Manager 콘솔에 대한 로그 참조 *(계속)*

아이디	로그 수준	설명	데이터	트리거	조치
10633	심각	조직을 수정하지 못함	조직 DN오류 메시지	조직을 수정할 수 없습니다. 사용자의 단일 사인온 토큰이 만료되었거나 사용자에게 이 작업을 수행할 권한이 없을 수 있습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.
10634	심각	조직을 수정하지 못함	조직 DN오류 메시지	액세스 관리 SDK 예외로 인해 조직을 수정할 수 없습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.
10641	정보	조직에서 조직 생성 시도	조직 DN새 조직 이름	조직 만들기 페이지에서 새로 만들기 버튼을 누릅니다.	
10642	정보	조직에서 조직을 생성함	조직 DN새 조직 이름	조직 만들기 페이지에서 새로 만들기 버튼을 누릅니다.	
10643	심각	조직에서 조직을 생성하지 못함	조직 DN새 조직 이름오류 메시지	조직을 생성할 수 없습니다. 사용자의 단일 사인온 토큰이 만료되었거나 사용자에게 이 작업을 수행할 권한이 없을 수 있습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.
10644	심각	조직에서 조직을 생성하지 못함	조직 DN새 조직 이름오류 메시지	액세스 관리 SDK 예외로 인해 조직을 생성할 수 없습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.
10651	정보	조직의 속성 값 가져오기 시도	조직 DN	조직 프로필 페이지를 봅니다.	

표 C–3 Access Manager 콘솔에 대한 로그 참조 *(계속)*

아이디	로그 수준	설명	데이터	트리거	조치
10652	정보	조직의 속성 값을 가져옴	조직 DN	조직 프로필 페이지를 봅니다.	
10653	심각	조직의 속성 값을 가져오지 못함	조직 DN오류 메시지	조직의 속성 값을 가져올 수 없습니다. 사용자의 단일 사인온 토큰이 만료되었거나 사용자에게 이 작업을 수행할 권한이 없을 수 있습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.
10654	심각	조직의 속성 값을 가져오지 못함	조직 DN오류 메시지	액세스 관리 SDK 예외로 인해 조직의 속성 값을 가져올 수 없습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.
10661	정보	조직에 서비스 추가 시도	조직 DN서비스 이름	조직의 서비스 페이지에서 할당 버튼을 누릅니다.	
10662	정보	조직에 서비스를 추가함	조직 DN서비스 이름	조직의 서비스 페이지에서 할당 버튼을 누릅니다.	
10663	심각	조직에 서비스를 추가하지 못함	조직 DN서비스 이름오류 메시지	조직에 서비스를 추가할 수 없습니다. 사용자의 단일 사인온 토큰이 만료되었거나 사용자에게 이 작업을 수행할 권한이 없을 수 있습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.

표 C–3 Access Manager 콘솔에 대한 로그 참조 *(계속)*

아이디	로그 수준	설명	데이터	트리거	조치
10664	심각	조직에 서비스를 추가하지 못함	조직 DN서비스 이름오류 메시지	액세스 관리 SDK 예외로 인해 조직에 서비스를 추가할 수 없습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.
10701	정보	역할에서 사용자 제거 시도	역할 DN사용자 이름	역할의 사용자 페이지에서 제거 버튼을 누릅니다.	
10702	정보	역할에서 사용자를 제거함	역할 DN사용자 이름	역할의 사용자 페이지에서 제거 버튼을 누릅니다.	
10703	심각	역할에서 사용자를 제거하지 못함	역할 DN사용자 이름오류 메시지	사용자를 제거할 수 없습니다. 사용자의 단일 사인온 토큰이 만료되었거나 사용자에게 이 작업을 수행할 권한이 없을 수 있습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.
10704	심각	역할에서 사용자를 제거하지 못함	역할 DN사용자 이름오류 메시지	액세스 관리 SDK 예외로 인해 사용자를 제거할 수 없습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.
10711	정보	역할의 속성 값 가져오기 시도	역할 DN	역할 프로필 페이지를 봅니다.	
10712	정보	역할의 속성 값을 가져옴	역할 DN	역할 프로필 페이지를 봅니다.	

표 C–3 Access Manager 콘솔에 대한 로그 참조 *(계속)*

아이디	로그 수준	설명	데이터	트리거	조치
10713	심각	역할의 속성 값을 가져오지 못함	역할 DN오류 메시지	속성 값을 가져올 수 없습니다. 사용자의 단일 사인온 토큰이 만료되었거나 사용자에게 이 작업을 수행할 권한이 없을 수 있습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.
10714	심각	역할의 속성 값을 가져오지 못함	역할 DN오류 메시지	액세스 관리 SDK 예외로 인해 속성 값을 가져올 수 없습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.
10721	정보	역할 수정 시도	역할 DN	역할 프로필 페이지에서 저장 버튼을 누릅니다.	
10722	정보	역할을 수정함	역할 DN	역할 프로필 페이지에서 저장 버튼을 누릅니다.	
10723	심각	역할을 수정하지 못함	역할 DN오류 메시지	역할을 수정할 수 없습니다. 사용자의 단일 사인온 토큰이 만료되었거나 사용자에게 이 작업을 수행할 권한이 없을 수 있습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.
10724	심각	역할을 수정하지 못함	역할 DN오류 메시지	액세스 관리 SDK 예외로 인해 역할을 수정할 수 없습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.
10731	정보	역할에서 구성원 가져오기 시도	역할 DN검색 패턴	역할의 구성원 페이지를 봅니다.	

표 C–3 Access Manager 콘솔에 대한 로그 참조 *(계속)*

아이디	로그 수준	설명	데이터	트리거	조치
10732	정보	역할에서 구성원을 가져옴	역할 DN검색 패턴	역할의 구성원 페이지를 봅니다.	
10733	심각	역할에서 구성원을 가져오지 못함	역할 DN검색 패턴오류 메시지	구성원을 가져올 수 없습니다. 사용자의 단일 사인온 토큰이 만료되었거나 사용자에게 이 작업을 수행할 권한이 없을 수 있습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.
10734	심각	역할에서 구성원을 가져오지 못함	역할 DN검색 패턴오류 메시지	액세스 관리 SDK 예외로 인해 구성원을 가져올 수 없습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.
10741	정보	조직에서 역할 가져오기 시도	역할 DN검색 패턴	조직의 역할 페이지를 봅니다.	
10742	정보	조직에서 역할을 가져옴	역할 DN검색 패턴역할의 구성원 페이지 보기	조직의 역할 페이지를 봅니다.	
10743	심각	조직에서 역할을 가져오지 못함	역할 DN검색 패턴오류 메시지	역할을 가져올 수 없습니다. 사용자의 단일 사인온 토큰이 만료되었거나 사용자에게 이 작업을 수행할 권한이 없을 수 있습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.
10744	심각	조직에서 역할을 가져오지 못함	역할 DN검색 패턴오류 메시지	액세스 관리 SDK 예외로 인해 역할을 가져올 수 없습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.

표 C–3 Access Manager 콘솔에 대한 로그 참조 *(계속)*

아이디	로그 수준	설명	데이터	트리거	조치
10751	정보	컨테이너에서 역할 가져오기 시도	역할 DN검색 패턴	컨테이너의 역할 페이지를 봅니다.	
10752	정보	컨테이너에서 역할을 가져옴	역할 DN검색 패턴역할의 구성원 페이지 보기	컨테이너의 역할 페이지를 봅니다.	
10753	심각	컨테이너에서 역할을 가져오지 못함	역할 DN검색 패턴오류 메시지	역할을 가져올 수 없습니다. 사용자의 단일 사인온 토큰이 만료되었거나 사용자에게 이 작업을 수행할 권한이 없을 수 있습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.
10754	심각	컨테이너에서 역할을 가져오지 못함	역할 DN검색 패턴오류 메시지	액세스 관리 SDK 예외로 인해 역할을 가져올 수 없습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.
10761	정보	컨테이너에서 역할 생성 시도	컨테이너 DN역할 이름	역할 만들기 페이지에서 새로 만들기 버튼을 누릅니다.	
10762	정보	컨테이너에서 역할을 생성함	컨테이너 DN역할 이름	역할 만들기 페이지에서 새로 만들기 버튼을 누릅니다.	
10763	심각	컨테이너에서 역할을 생성하지 못함	컨테이너 DN역할 이름	역할을 생성할 수 없습니다. 사용자의 단일 사인온 토큰이 만료되었거나 사용자에게 이 작업을 수행할 권한이 없을 수 있습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.

표 C–3 Access Manager 콘솔에 대한 로그 참조 *(계속)*

아이디	로그 수준	설명	데이터	트리거	조치
10764	심각	컨테이너에서 역할을 생성하지 못함	컨테이너 DN역할 이름오류 메시지	액세스 관리 SDK 예외로 인해 역할을 생성할 수 없습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.
10771	정보	조직에서 역할 생성 시도	조직 DN역할 이름	역할 만들기 페이지에서 새로 만들기 버튼을 누릅니다.	
10772	정보	조직에서 역할을 생성함	조직 DN역할 이름	역할 만들기 페이지에서 새로 만들기 버튼을 누릅니다.	
10773	심각	조직에서 역할을 생성하지 못함	조직 DN역할 이름	역할을 생성할 수 없습니다. 사용자의 단일 사인온 토큰이 만료되었거나 사용자에게 이 작업을 수행할 권한이 없을 수 있습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.
10774	심각	조직에서 역할을 생성하지 못함	조직 DN역할 이름오류 메시지	액세스 관리 SDK 예외로 인해 역할을 생성할 수 없습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.
10781	정보	역할에서 할당된 서비스 가져오기 시도	역할 DN	역할의 서비스 페이지를 봅니다.	
10782	정보	역할에서 할당된 서비스를 가져옴	역할 DN	역할의 서비스 페이지를 봅니다.	

표 C–3 Access Manager 콘솔에 대한 로그 참조 *(계속)*

아이디	로그 수준	설명	데이터	트리거	조치
10783	심각	역할에서 할당된 서비스를 가져오지 못함	역할 DN오류 메시지	역할에서 서비스를 가져올 수 없습니다. 사용자의 단일 사인온 토큰이 만료되었거나 사용자에게 이 작업을 수행할 권한이 없을 수 있습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.
10784	심각	역할에서 할당된 서비스를 가져오지 못함	역할 DN오류 메시지	액세스 관리 SDK 예외로 인해 역할에서 서비스를 가져올 수 없습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.
10791	정보	역할에서 서비스 제거 시도	역할 DN서비스 이름	역할의 서비스 페이지에서 할당 해제 버튼을 누릅니다.	
10792	정보	역할에서 서비스를 제거함	역할 DN서비스 이름	역할의 서비스 페이지에서 할당 해제 버튼을 누릅니다.	
10793	심각	역할에서 서비스를 제거하지 못함	역할 DN서비스 이름오류 메시지	역할에서 서비스를 제거할 수 없습니다. 사용자의 단일 사인온 토큰이 만료되었거나 이 작업을 수행할 권한이 사용자에게 없을 수 있습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.

표 C–3 Access Manager 콘솔에 대한 로그 참조 *(계속)*

아이디	로그 수준	설명	데이터	트리거	조치
10794	심각	역할에서 서비스를 제거하지 못함	역할 DN서비스 이름오류 메시지	액세스 관리 SDK 예외로 인해 역할에서 서비스를 제거할 수 없습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.
10801	정보	역할에 서비스 추가 시도	역할 DN서비스 이름	역할의 서비스 페이지에서 할당 버튼을 누릅니다.	
10802	정보	역할에 서비스를 추가함	역할 DN서비스 이름	역할의 서비스 페이지에서 할당 버튼을 누릅니다.	
10803	심각	역할에 서비스를 추가하지 못함	역할 DN서비스 이름오류 메시지	역할에 서비스를 추가할 수 없습니다. 사용자의 단일 사인온 토큰이 만료되었거나 사용자에게 이 작업을 수행할 권한이 없을 수 있습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.
10804	심각	역할에 서비스를 추가하지 못함	역할 DN서비스 이름오류 메시지	액세스 관리 SDK 예외로 인해 역할에 서비스를 추가할 수 없습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.
10901	정보	사용자의 할당된 역할 가져오기 시도	사용자 DN	사용자의 역할 페이지를 봅니다.	
10902	정보	사용자의 할당된 역할을 가져옴	사용자 DN	사용자의 역할 페이지를 봅니다.	

표 C–3 Access Manager 콘솔에 대한 로그 참조 *(계속)*

아이디	로그 수준	설명	데이터	트리거	조치
10903	심각	사용자의 할당된 역할을 가져오지 못함	사용자 DN오류 메시지	할당된 역할을 가져올 수 없습니다. 사용자의 단일 사인온 토큰이 만료되었거나 사용자에게 이 작업을 수행할 권한이 없을 수 있습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.
10904	심각	사용자의 할당된 역할을 가져오지 못함	사용자 DN서비스 이름오류 메시지	액세스 관리 SDK 예외로 인해 할당한 역할을 가져올 수 없습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.
10911	정보	사용자에서 역할 제거 시도	사용자 DN역할 *DN*	사용자의 역할 페이지에서 삭제 버튼을 누릅니다.	
10912	정보	사용자에서 역할을 제거함	사용자 DN역할 *DN*	사용자의 역할 페이지에서 삭제 버튼을 누릅니다.	
10913	심각	사용자에서 역할을 제거하지 못함	사용자 DN역할 *DN*오류 메시지	역할을 제거할 수 없습니다. 사용자의 단일 사인온 토큰이 만료되었거나 사용자에게 이 작업을 수행할 권한이 없을 수 있습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.
10914	심각	사용자에서 역할을 제거하지 못함	사용자 DN역할 *DN*서비스 이름오류 메시지	액세스 관리 SDK 예외로 인해 역할을 제거할 수 없습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.
10921	정보	사용자에 역할 추가 시도	사용자 DN역할 *DN*	사용자의 역할 페이지에서 추가 버튼을 누릅니다.	

표 C–3 Access Manager 콘솔에 대한 로그 참조 *(계속)*

아이디	로그 수준	설명	데이터	트리거	조치
10922	정보	사용자에 역할을 추가함	사용자 DN역할 *DN*	사용자의 역할 페이지에서 추가 버튼을 누릅니다.	
10923	심각	사용자에 역할을 추가하지 못함	사용자 DN역할 *DN*오류 메시지	역할을 추가할 수 없습니다. 사용자의 단일 사인온 토큰이 만료되었거나 사용자에게 이 작업을 수행할 권한이 없을 수 있습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.
10924	심각	사용자에 역할을 추가하지 못함	사용자 DN역할 *DN*서비스 이름오류 메시지	액세스 관리 SDK 예외로 인해 역할을 추가할 수 없습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.
10931	정보	사용자의 할당된 서비스 가져오기 시도	사용자 DN	사용자의 서비스 페이지를 봅니다.	
10932	정보	사용자의 할당된 서비스를 가져옴	사용자 DN	사용자의 서비스 페이지를 봅니다.	
10933	심각	사용자의 할당된 서비스를 가져오지 못함	사용자 DN오류 메시지	서비스를 가져올 수 없습니다. 사용자의 단일 사인온 토큰이 만료되었거나 사용자에게 이 작업을 수행할 권한이 없을 수 있습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.
10934	심각	사용자의 할당된 서비스를 가져오지 못함	사용자 DN오류 메시지	액세스 관리 SDK 예외로 인해 서비스를 가져올 수 없습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.

표 C–3 Access Manager 콘솔에 대한 로그 참조 *(계속)*

아이디	로그 수준	설명	데이터	트리거	조치
10941	정보	사용자에서 서비스 제거 시도	사용자 DN서비스 이름	사용자의 서비스 페이지에서 제거 버튼을 누릅니다.	
10942	정보	사용자에서 서비스를 제거함	사용자 DN서비스 이름	사용자의 서비스 페이지에서 제거 버튼을 누릅니다.	
10943	심각	사용자에서 서비스를 제거하지 못함	사용자 DN서비스 이름오류 메시지	서비스를 제거할 수 없습니다. 사용자의 단일 사인온 토큰이 만료되었거나 사용자에게 이 작업을 수행할 권한이 없을 수 있습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.
10944	심각	사용자에서 서비스를 제거하지 못함	사용자 DN서비스 이름오류 메시지	액세스 관리 SDK 예외로 인해 서비스를 제거할 수 없습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.
10951	정보	조직에서 사용자 검색 시도	조직 DN검색 패턴	조직의 사용자 페이지를 봅니다.	
10952	정보	조직에서 사용자를 검색함	조직 DN검색 패턴	조직의 사용자 페이지를 봅니다.	
10953	심각	조직에서 사용자를 검색하지 못함	조직 DN검색 패턴오류 메시지	사용자를 검색할 수 없습니다. 사용자의 단일 사인온 토큰이 만료되었거나 사용자에게 이 작업을 수행할 권한이 없을 수 있습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.

표 C–3 Access Manager 콘솔에 대한 로그 참조 *(계속)*

아이디	로그 수준	설명	데이터	트리거	조치
10954	심각	조직에서 사용자를 검색하지 못함	조직 DN검색 패턴오류 메시지	액세스 관리 SDK 예외로 인해 사용자를 검색할 수 없습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.
10961	정보	사용자 수정 시도	사용자 DN	사용자 프로필 페이지에서 저장 버튼을 누릅니다.	
10962	정보	사용자 프로필을 수정함	사용자 DN	사용자 프로필 페이지에서 저장 버튼을 누릅니다.	
10963	심각	사용자 프로필을 수정하지 못함	사용자 DN오류 메시지	사용자를 수정할 수 없습니다. 사용자의 단일 사인온 토큰이 만료되었거나 사용자에게 이 작업을 수행할 권한이 없을 수 있습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.
10964	심각	사용자 프로필을 수정하지 못함	사용자 DN오류 메시지	액세스 관리 SDK 예외로 인해 사용자를 수정할 수 없습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.
10971	정보	사용자 생성 시도	사용자 컨테이너 DN사용자 이름	사용자 만들기 페이지에서 추가 버튼을 누릅니다.	
10972	정보	사용자를 생성함	사용자 컨테이너 DN사용자 이름	사용자 만들기 페이지에서 추가 버튼을 누릅니다.	

표 C–3 Access Manager 콘솔에 대한 로그 참조 *(계속)*

아이디	로그 수준	설명	데이터	트리거	조치
10973	심각	사용자를 생성하지 못함	사용자 컨테이너 DN사용자 이름오류 메시지	사용자를 만들 수 없습니다. 사용자의 단일 사인온 토큰이 만료되었거나 사용자에게 이 작업을 수행할 권한이 없을 수 있습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.
10974	심각	사용자를 생성하지 못함	사용자 컨테이너 DN사용자 이름오류 메시지	액세스 관리 SDK 예외로 인해 사용자를 생성할 수 없습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.
10981	정보	사용자의 속성 값 가져오기 시도	사용자 DN	사용자 프로필 페이지를 봅니다.	
10982	정보	사용자의 속성 값을 가져옴	사용자 DN	사용자 프로필 페이지를 봅니다.	
10983	심각	사용자의 속성 값을 가져오지 못함	사용자 DN오류 메시지	속성 값을 가져올 수 없습니다. 사용자의 단일 사인온 토큰이 만료되었거나 이 작업을 수행할 권한이 사용자에게 없을 수 있습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.
10984	심각	사용자의 속성 값을 가져오지 못함	사용자 DN오류 메시지	액세스 관리 SDK 예외로 인해 속성 값을 가져올 수 없습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.
10991	정보	사용자에 서비스 추가 시도	사용자 DN서비스 이름	사용자의 서비스 페이지에서 추가 버튼을 누릅니다.	

표 C–3 Access Manager 콘솔에 대한 로그 참조 *(계속)*

아이디	로그 수준	설명	데이터	트리거	조치
10992	정보	사용자에 서비스를 추가함	사용자 DN서비스 이름	사용자의 서비스 페이지에서 추가 버튼을 누릅니다.	
10993	심각	사용자에 서비스를 추가하지 못함	사용자 DN서비스 이름오류 메시지	서비스를 추가할 수 없습니다. 사용자의 단일 사인온 토큰이 만료되었거나 사용자에게 이 작업을 수행할 권한이 없을 수 있습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.
10994	심각	사용자에 서비스를 추가하지 못함	사용자 DN서비스 이름오류 메시지	액세스 관리 SDK 예외로 인해 서비스를 추가할 수 없습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.
11001	정보	사용자의 할당된 그룹 가져오기 시도	사용자 DN	사용자의 그룹 페이지를 봅니다.	
11002	정보	사용자의 할당된 그룹을 가져옴	사용자 DN	사용자의 그룹 페이지를 봅니다.	
11003	심각	사용자의 할당된 그룹을 가져오지 못함	사용자 DN오류 메시지	할당된 그룹을 가져올 수 없습니다. 사용자의 단일 사인온 토큰이 만료되었거나 사용자에게 이 작업을 수행할 권한이 없을 수 있습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.
11004	심각	사용자의 할당된 그룹을 가져오지 못함	사용자 DN오류 메시지	액세스 관리 SDK 예외로 인해 할당한 그룹을 가져올 수 없습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.

표 C–3 Access Manager 콘솔에 대한 로그 참조 *(계속)*

아이디	로그 수준	설명	데이터	트리거	조치
11011	정보	사용자에서 그룹 제거 시도	사용자 DN그룹 *DN*	사용자의 그룹 페이지에서 제거 버튼을 누릅니다.	
11012	정보	사용자에서 그룹을 제거함	사용자 DN그룹 *DN*	사용자의 그룹 페이지에서 제거 버튼을 누릅니다.	
11013	심각	사용자에서 그룹을 제거하지 못함	사용자 DN그룹 *DN*오류 메시지	그룹을 제거할 수 없습니다. 사용자의 단일 사인온 토큰이 만료되었거나 사용자에게 이 작업을 수행할 권한이 없을 수 있습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.
11014	심각	사용자에서 그룹을 제거하지 못함	사용자 DN그룹 *DN*오류 메시지	액세스 관리 SDK 예외로 인해 그룹을 제거할 수 없습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.
11021	정보	사용자에 그룹 추가 시도	사용자 DN그룹 *DN*	사용자의 그룹 페이지에서 추가 버튼을 누릅니다.	
11022	정보	사용자에 그룹을 추가함	사용자 DN그룹 *DN*	사용자의 그룹 페이지에서 추가 버튼을 누릅니다.	
11023	심각	사용자에 그룹을 추가하지 못함	사용자 DN그룹 *DN*오류 메시지	그룹을 추가할 수 없습니다. 사용자의 단일 사인온 토큰이 만료되었거나 사용자에게 이 작업을 수행할 권한이 없을 수 있습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.

표 C–3 Access Manager 콘솔에 대한 로그 참조 *(계속)*

아이디	로그 수준	설명	데이터	트리거	조치
11024	심각	사용자에 그룹을 추가하지 못함	사용자 DN그룹 *DN*오류 메시지	액세스 관리 SDK 예외로 인해 그룹을 추가할 수 없습니다.	자세한 내용은 액세스 관리 SDK 로그를 참조하십시오.

표 C–4 연합에 대한 로그 참조

아이디	로그 수준	설명	데이터	트리거	조치
1	정보	인증 도메인 생성	인증 도메인 이름	인증 도메인을 생성했습니다.	
2	정보	인증 도메인 삭제	인증 도메인 이름	인증 도메인을 삭제했습니다.	
3	정보	인증 도메인 수정	인증 도메인 이름	인증 도메인을 수정했습니다.	
4	정보	원격 공급자 생성	공급자 아이디	원격 공급자를 생성했습니다.	
5	정보	호스트된 공급자 생성	공급자 아이디	호스트된 공급자를 생성했습니다.	
6	정보	제휴를 삭제함	제휴 아이디	제휴를 삭제했습니다.	
7	정보	엔티티 삭제	엔티티 아이디	엔티티를 삭제했습니다.	
8	정보	공급자를 삭제했습니다.	공급자 아이디	공급자를 삭제했습니다.	
9	정보	엔티티 수정	엔티티 아이디	엔티티를 수정했습니다.	
10	정보	제휴 수정	제휴 아이디	제휴를 수정했습니다.	
11	정보	공급자 수정	공급자 아이디	공급자를 수정했습니다.	
12	정보	엔티티 생성	엔티티 아이디	엔티티를 생성했습니다.	
13	정보	제휴 생성	제휴 아이디	제휴를 생성했습니다.	
14	정보	계정 연합 정보 쓰기	사용자 DN연합 정보 키연합 정보 값	키를 포함하는 계정 연합 정보가 사용자에 추가되었습니다.	

표 C–4 연합에 대한 로그 참조 *(계속)*

아이디	로그 수준	설명	데이터	트리거	조치
15	정보	계정 연합 정보 제거	사용자 DN공급자 아이디기존 연합 정보 키	키 및 공급자 아이디가 있는 계정 연합 정보가 사용자에서 제거되었습니다.	
16	더 자세히	명제 생성	명제 아이디 또는 문자열	명제를 생성했습니다.	
17	정보	리버티가 활성화 안 됨	메시지	리버티가 활성화 안 됨요청을 처리할 수 없습니다.	관리 콘솔에 로그인하여 관리 콘솔 서비스에서 연합 관리를 활성화하십시오.
18	정보	로그아웃 요청을 처리하지 못함	메시지	로그아웃 요청을 처리하지 못했습니다.	
19	정보	종료 요청을 처리하지 못함	메시지	종료 요청을 처리하지 못함	
20	정보	SOAP URL 종점을 생성하지 못함	SOAP 종점 URL	SOAP URL 종점을 생성하지 못했습니다.	
21	정보	AuthType과 프로토콜(SOAPUrl 기반)이 일치하지 않음	프로토콜인증 유형	AuthType과 프로토콜(SOAPUrl 기반)이 일치하지 않습니다.	
22	정보	인증 유형이 잘못됨	인증 유형	인증 유형이 잘못됨	
23	더 자세히	SAML SOAP 수신기 URL	SOAP URL	SAML SOAP 수신기 URL	
24	정보	SOAP 응답이 유효하지 않음	메시지	SOAP 응답이 유효하지 않습니다.	
25	정보	명제가 유효하지 않음	메시지	명제가 유효하지 않습니다.	
26	정보	단일 사인온에 실패함	메시지	단일 사인온에 실패함	
27	정보	액세스 허용 후 URL로 리디렉션	URL 리디렉션	액세스를 허용한 후 URL로 리디렉션합니다.	
28	정보	인증 응답이 없음	메시지	인증 응답이 없습니다.	
29	정보	계정 연합에 실패함	메시지	계정 연합에 실패함	

표 C–4 연합에 대한 로그 참조 *(계속)*

아이디	로그 수준	설명	데이터	트리거	조치
30	정보	SSOToken을 생성하지 못함	메시지	SSOToken을 생성하지 못했습니다.	
31	정보	인증 응답이 유효하지 않음	유효하지 않은 인증 응답	인증 응답이 유효하지 않음	
32	정보	인증 요청을 처리하지 못함	메시지	인증 요청을 처리하지 못했습니다.	
33	정보	서명을 확인하지 못함	메시지	서명을 확인하지 못함	
34	더 자세히	SAML 응답을 생성함	SAML 응답	SAML 응답을 생성함	
35	더 자세히	URL 리디렉션	URL 리디렉션	다음으로 리디렉션:	
36	정보	공통 도메인 서비스 정보를 찾지 못함	메시지	공통 도메인 서비스 정보를 찾지 못했습니다.	
37	정보	공급자를 신뢰할 수 없음	공급자 아이디	공급자를 신뢰할 수 없습니다.	
38	정보	인증 요청이 유효하지 않음	메시지	인증 요청이 유효하지 않음	
39	정보	사용자에 대한 계정 연합 정보를 찾지 못함	사용자 이름	사용자에 대한 계정 연합 정보를 찾지 못했습니다.	
40	정보	사용자를 찾지 못함	사용자 이름	사용자를 찾지 못함	
41	정보	로그아웃 프로필을 지원하지 않음	로그아웃 프로필	로그아웃 프로필을 지원하지 않음	메타데이터가 올바른지 확인하십시오.
42	정보	로그아웃 성공	사용자 이름	로그아웃 성공	
43	정보	URL이 잘못되어 로그아웃 리디렉션 실패함	메시지	URL이 잘못되어 로그아웃 리디렉션 실패함	
44	정보	로그아웃 요청이 제대로 생성되지 않음	사용자 이름	로그아웃 요청이 제대로 생성되지 않음	
45	정보	사전/로그아웃 처리기를 가져오지 못함	로그아웃 URL	사전/로그아웃 처리기를 가져오지 못함	
46	정보	단일 로그아웃에 실패함	사용자 이름	단일 로그아웃에 실패함	
47	정보	SPProvidedNameIdentifier를 생성하지 못함	메시지	SPProvidedNameIdentifier를 생성하지 못함	

표 C–4 연합에 대한 로그 참조 *(계속)*

아이디	로그 수준	설명	데이터	트리거	조치
48	정보	서명이 유효하지 않음	메시지	서명이 유효하지 않음	
49	정보	연합 종료에 실패함	사용자 이름	연합 종료에 실패함계정을 업데이트할 수 없습니다.	
50	더 자세히	연합 종료에 성공함	userDN	연합 종료에 성공함사용자 계정이 업데이트되었습니다.	
51	정보	응답이 유효하지 않음	SAML 응답	SAML 응답이 유효하지 않습니다.	
52	정보	공급자 등록이 유효하지 않음	공급자 아이디	공급자가 유효하지 않습니다.	

표 C–5 리버티에 대한 로그 참조

아이디	로그 수준	설명	데이터	트리거	조치
1	정보	SASL 요청을 처리할 수 없음	메시지 아이디인증 메커니즘인증 아이디자문 인증 아이디	SASL 요청을 처리할 수 없습니다.	
2	정보	SASL 응답 양호	메시지 아이디인증 메커니즘인증 아이디자문 인증 아이디	SASL 응답이 양호합니다.	
3	정보	SASL 인증 응답 반환	메시지 아이디인증 메커니즘인증 아이디자문 인증 아이디	SASL 응답을 반환했고 인증을 계속합니다.	
4	정보	데이터 저장소에 사용자가 없음	사용자 이름	데이터 저장소에 사용자가 없음	
5	정보	데이터 저장소에 사용자가 있음	사용자 이름	데이터 저장소에 사용자가 있음	
6	정보	resourceID에서 사용자를 찾을 수 없음	resourceID	resourceID에서 사용자를 찾을 수 없음	

표 C–5 리버티에 대한 로그 참조 *(계속)*

아이디	로그 수준	설명	데이터	트리거	조치
7	정보	사용자 프로필을 업데이트함	사용자 이름	사용자 프로필을 업데이트함	
8	정보	허용 안 됨개인 프로필 서비스를 쿼리하지 못함	자원 아이디	개인 프로필 서비스를 쿼리하지 못함	
9	정보	상호 작용이 실패함	자원 아이디	개인 프로필 서비스와의 상호 작용이 실패했습니다.	
10	정보	PP 서비스를 쿼리함	자원 아이디	개인 프로필 서비스에 대해 쿼리했습니다.	
11	정보	수정 실패	자원 아이디	개인 프로필 서비스를 수정하지 못했습니다.	
12	정보	수정 성공	자원 아이디	개인 프로필 서비스를 수정했습니다.	
13	정보	상호 작용 성공	성공적인 상호 작용 메시지	개인 프로필 서비스와의 상호 작용이 성공했습니다.	
14	정보	메시지를 전송하는 중	요청 메시지 아이디	SOAP 요청 메시지를 WSP로 전송하는 중입니다.	
15	정보	응답 메시지를 반환하는 중	응답 메시지 아이디요청 메시지 아이디	SOAP 요청에 대한 응답 메시지를 반환하는 중입니다.	
16	정보	메시지를 다시 전송하는 중	메시지 아이디	SOAP 요청 메시지를 WSP로 다시 전송하는 중입니다.	

표 C–5 리버티에 대한 로그 참조 *(계속)*

아이디	로그 수준	설명	데이터	트리거	조치
17	정보	상호 작용 관리자가 사용자 에이전트를 상호 작용 서비스로 리디렉션하는 중	요청 메시지 아이디	상호 작용 관리자가 사용자 에이전트를 상호 작용 서비스로 리디렉션하는 중	
18	정보	상호 작용 관리자가 응답 요소를 반환하는 중	메시지 아이디참조 메시지 아이디캐시 항목 상태	상호 작용 관리자가 응답 요소를 반환하는 중	
19	정보	상호 작용 쿼리를 사용자 에이전트에 제시함	메시지 아이디	상호 작용 쿼리를 사용자 에이전트에 제시함	
20	정보	사용자 에이전트가 상호 작용 쿼리에 응답함	메시지 아이디	사용자 에이전트가 상호 작용 쿼리에 응답함	
21	정보	사용자 에이전트를 SP로 다시 리디렉션함	메시지 아이디	사용자 에이전트를 SP로 다시 리디렉션함	
22	정보	웹 서비스 성공	메시지 아이디처리기 키	웹 서비스에 성공했습니다.	
23	정보	웹 서비스 실패	오류 메시지	웹 서비스에 실패했습니다.	

표 C–6 정책에 대한 로그 참조

아이디	로그 수준	설명	데이터	트리거	조치
1	정보	정책을 평가함	정책 이름영역 이름서비스 유형 이름자원 이름작업 이름정책 결정	정책을 평가하는 중입니다.	

표 C–6 정책에 대한 로그 참조 *(계속)*

아이디	로그 수준	설명	데이터	트리거	조치
2	정보	보호된 정책 자원 가져옴	기본 이름자원 이름정책 보호	보호된 정책 자원을 가져오는 중입니다.	
3	정보	영역에서 정책을 생성함	정책 이름영역 이름	영역에서 정책을 생성하는 중입니다.	
4	정보	영역에서 정책을 수정함	정책 이름영역 이름	영역에서 정책을 수정하는 중입니다.	
5	정보	영역에서 정책을 제거함	정책 이름영역 이름	영역에서 정책을 제거하는 중입니다.	
6	정보	영역에 정책이 이미 있음	정책 이름영역 이름	영역에서 정책을 생성하는 중입니다.	
7	정보	영역에서 정책을 생성하지 못함	정책 이름영역 이름	영역에서 정책을 생성하는 중입니다.	사용자에게 영역에서 정책을 생성할 권한이 있는지 확인하십시오.
8	정보	영역에서 정책을 대체하지 못함	정책 이름영역 이름	영역에서 정책을 대체하는 중입니다.	사용자에게 영역에서 정책을 대체할 권한이 있는지 확인하십시오.
81	정보	정책을 대체하지 않았음 - 새 이름의 다른 정책이 이미 영역에 있음	새 정책 이름영역 이름	영역에서 정책을 대체하는 중입니다.	
9	정보	영역에서 정책을 제거하지 못함	정책 이름영역 이름	영역에서 정책을 제거하는 중입니다.	사용자에게 영역에서 정책을 제거할 권한이 있는지 확인하십시오.

표 C–6 정책에 대한 로그 참조 *(계속)*

아이디	로그 수준	설명	데이터	트리거	조치
10	정보	관리자에 의한 정책 결정을 확인함	관리 이름기본 이름자원 이름정책 결정	관리자에 의한 정책 결정을 확인하는 중입니다.	
11	정보	주제를 무시하는 관리자에 의한 정책 결정을 확인함	관리 이름자원 이름정책 결정	주제를 무시하는 관리자에 의한 정책 결정을 확인하는 중입니다.	

표 C–7 SAML에 대한 로그 참조

아이디	로그 수준	설명	데이터	트리거	조치
1	정보	새 명제를 생성함	메시지 아이디로그 수준이 *LL_FINER*인 경우 명제 아이디 또는 명제	브라우저 아티팩트 프로필브라우저 *POST* 프로필명제 아티팩트 생성인증 쿼리속성 쿼리인증 결정 쿼리	
2	정보	새 명제 아티팩트를 생성함	메시지 아이디명제 아티팩트아티팩트에 해당하는 명제의 아이디	브라우저 아티팩트 프로필명제 아티팩트 생성	
3	자세히	맵에서 제거된 명제 아티팩트	메시지 아이디명제 아티팩트	SAML 아티팩트 쿼리명제 아티팩트 만료	
4	자세히	맵에서 제거된 명제	메시지 아이디명제 아이디	SAML 아티팩트 쿼리명제 만료	
5	정보	확인된 명제 아티팩트에 의한 액세스 권한	메시지 아이디명제 아티팩트	SAML 아티팩트 쿼리	

표 C–7 SAML에 대한 로그 참조 *(계속)*

아이디	로그 수준	설명	데이터	트리거	조치
6	정보	구성된 인증 유형과 실제 SOAP 프로토콜이 일치하지 않음	메시지 아이디	SAML SOAP 쿼리	콘솔에 로그인하고 연합 및 SAML로 차례로 이동하여 인증된 파트너 구성을 편집한 다음 선택한 인증 유형 필드를 확인하고 SOAP URL 필드에서 지정한 프로토콜이 일치하는지 확인합니다.
7	정보	인증 유형이 유효하지 않음	메시지 아이디	SAML SOAP 쿼리	콘솔에 로그인하고 연합 및 SAML로 차례로 이동하여 인증된 파트너 구성을 편집한 다음 인증 유형 필드에 대한 값 중 하나를 선택하고 저장합니다.
8	자세히	원격 SOAP 수신자 URL	메시지 아이디*SOAP* 수신자 *URL*	SAML SOAP 쿼리	
9	정보	SAML 응답에 명제가 없음	메시지 아이디*SAML* 응답	SAML 아티팩트 쿼리	잘못된 항목에 대해서는 원격 파트너에 문의하십시오.
10	정보	SAML 응답에 있는 명제 수가 SAML 요청에 있는 아피팩트 수와 같지 않음	메시지 아이디*SAML* 응답	SAML 아티팩트 쿼리	잘못된 항목에 대해서는 원격 파트너에 문의하십시오.
11	정보	원격 파트너로 전송될 아티팩트	메시지 아이디*SAML* 아티팩트	SAML 아티팩트 쿼리	

표 C–7 SAML에 대한 로그 참조 *(계속)*

아이디	로그 수준	설명	데이터	트리거	조치
12	정보	인증된 파트너 구성에 있는 SOAP URL이 잘못됨	메시지 아이디	SAML 아티팩트 쿼리	콘솔에 로그인하고 연합 및 SAML로 차례로 이동하여 인증된 파트너 구성을 편집한 다음 SOAP URL 필드의 값을 입력하고 저장합니다.
13	자세히	SAML 아티팩트 쿼리 SOAP 요청	메시지 아이디*SAML* 아티팩트 쿼리 메시지	SAML 아티팩트 쿼리	
14	정보	원격 SAML SOAP 수신자에서 응답이 없음	메시지 아이디	SAML 아티팩트 쿼리	잘못된 항목에 대해서는 원격 파트너를 확인하십시오.
15	자세히	SAML 아타팩트 쿼리 응답	메시지 아이디*SAML* 아티팩트 쿼리 응답 메시지	SAML 아티팩트 쿼리	
16	정보	SOAP 응답 내에 SAML 응답이 없음	메시지 아이디	SAML 아티팩트 쿼리	잘못된 항목에 대해서는 원격 파트너를 확인하십시오.
17	정보	SAML 응답에 대한 XML 서명이 유효하지 않음	메시지 아이디	SAML 아티팩트 쿼리	XML 디지털 서명에 대한 잘못된 항목에 대해서는 원격 파트너를 확인하십시오.
18	정보	SAML 응답 상태 코드를 가져오는 동안 오류 발생	메시지 아이디	SAML 아티팩트 쿼리	응답 상태 코드에 대한 잘못된 항목에 대해서는 원격 파트너를 확인하십시오.
19	정보	TARGET 매개 변수가 요청에 없음	메시지 아이디	SAML 아티팩트 프로필*SAML POST* 프로필	요청에서 "TARGET=target_url"을 쿼리 매개 변수로 추가하십시오.

표 C–7 SAML에 대한 로그 참조 *(계속)*

아이디	로그 수준	설명	데이터	트리거	조치
20	정보	SAML 아티팩트 원본 사이트에서 URL 리디렉션	메시지 아이디대상리디렉션 *URLPOST* 프로필 및 로그 수준이 *LL_FINER*인 경우의 *SAML* 응답 메시지	SAML 아티팩트 프로필 원본*SAML POST* 프로필 원본	
21	정보	지정한 대상 사이트가 금지됨	메시지 아이디대상 *URL*	SAML 아티팩트 프로필 원본*SAML POST* 프로필 원본	요청에서 지정된 대상 URL은 인증된 파트너에 의해 처리되지 않으므로 대상 URL을 확인하고 인증된 파트너 사이트에서 구성된 대상 URL 중 하나와 일치하는지 확인하십시오.
22	정보	단일 사인온 토큰을 생성하지 못함	메시지 아이디	SAML 아티팩트 프로필 대상*SAML POST* 프로필 대상	인증 구성 요소가 SSO 토큰을 생성하지 못했습니다. 자세한 내용은 인증 로그 및 디버그를 확인하십시오.
23	정보	단일 사인온에 성공하고 대상에 대한 액세스가 허용됨	메시지 아이디*POST* 프로필 및 로그 수준이 *LL_FINER* 이상인 경우의 응답 메시지	SAML 아티팩트 프로필 대상*SAML POST* 프로필 대상	
24	정보	Null 서블릿 요청 또는 응답	메시지 아이디	SAML 아티팩트 프로필*SAML POST* 프로필	자세한 내용은 웹 컨테이너 오류 로그를 확인하십시오.
25	정보	POST 본문에 SAML 응답이 없음	메시지 아이디	SAML POST 프로필 대상	원격 SAML 파트너와 함께 SAML 응답 객체가 HTTP POST 본문에 없는 이유를 확인하십시오.

표 C–7 SAML에 대한 로그 참조 *(계속)*

아이디	로그 수준	설명	데이터	트리거	조치
26	정보	응답 메시지의 오류	메시지 아이디	SAML POST 프로필 대상	인코딩된 POST 본문 속성을 SAML 응답 객체로 변환할 수 없습니다. 원격 SAML 파트너와 함께 SAML 응답을 만들 때 오류가 발생했는지(예: 인코딩 오류, 유효하지 않은 응답 하위 요소 등) 확인하십시오.
27	정보	응답이 유효하지 않음	메시지 아이디	SAML POST 프로필 대상	SAML 응답에 있는 수신인 속성이 이 사이트의 POST 프로필 URL과 일치하지 않습니다.응답 상태 코드가 성공이 아님
28	정보	메시지 팩토리의 인스턴스를 가져오지 못함	메시지 아이디	SAML SOAP 수신기 init	SOAP 팩토리 등록 정보(javax.xml.soap.MessageFactory)에 유효한 SOAP 팩토리 구현을 사용하고 있는지 확인하십시오.
29	정보	신뢰할 수 없는 사이트로부터 요청을 수신함	메시지 아이디원격 사이트 호스트 이름 또는 *IP* 주소	SAML SOAP 쿼리	콘솔에 로그인하고 연합 및 SAML 서비스로 차례로 이동하고 인증된 파트너 구성을 편집한 다음 호스트 목록 필드를 확인하고 원격 호스트/IP가 값 중 하나인지 확인합니다. 클라이언트 인증이 있는 SSL의 경우 호스트 목록에 원격 사이트의 클라이언트 인증서가 있는지 확인하십시오.

표 C–7 SAML에 대한 로그 참조 *(계속)*

아이디	로그 수준	설명	데이터	트리거	조치
30	정보	원격 파트너 사이트의 요청이 유효하지 않음	메시지 아이디 및 요청 호스트 이름/IP 주소응답 반환	SAML SOAP 쿼리	원격 파트너 사이트의 관리자에게 문의하십시오.
31	자세히	파트너 사이트의 요청 메시지	메시지 아이디 및 요청 호스트 이름/IP 주소요청 *xml*	SAML SOAP 쿼리	
32	정보	내부 서버 오류로 인해 응답을 빌드하지 못함	메시지 아이디	SAML SOAP 쿼리	디버그 메시지에서 실패한 원인(예: 응답 상태를 생성할 수 없음, 주요/사소한 버전 오류 등)을 확인하십시오.
33	정보	파트너 사이트로 SAML 응답 전송 중	메시지 아이디*SAML* 응답 또는 응답 아이디	SAML SOAP 쿼리	
32	정보	SOAP 오류 응답 본문을 빌드하지 못함	메시지 아이디	SAML SOAP 쿼리	디버그 메시지에서 실패한 이유(SOAP 오류를 생성할 수 없음 등)를 확인하십시오.

표 C–8 세션에 대한 로그 참조

아이디	로그 수준	설명	데이터	트리거	조치
1	정보	세션을 생성함	사용자 아이디	사용자가 인증되었습니다.	
2	정보	세션이 유휴 시간을 초과함	사용자 아이디	사용자 세션이 오랫동안 유휴 상태였습니다.	
3	정보	세션이 만료됨	사용자 아이디	사용자 세션이 최대 시간 제한에 도달했습니다.	
4	정보	사용자가 로그아웃됨	사용자 아이디	사용자가 시스템에서 로그아웃되었습니다.	
5	정보	세션을 다시 활성화함	사용자 아이디	사용자 세션이 활성 상태입니다	

표 C–8 세션에 대한 로그 참조 *(계속)*

아이디	로그 수준	설명	데이터	트리거	조치
6	정보	세션을 삭제함	사용자 아이디	사용자 세션이 삭제되어 참조할 수 없습니다.	
7	정보	세션의 등록 정보가 변경됨	사용자 아이디	사용자가 세션의 보호되지 않은 등록 정보를 변경했습니다.	
8	정보	세션에서 알 수 없는 이벤트를 수신함	사용자 아이디	알 수 없는 세션 이벤트입니다.	
9	정보	보호된 등록 정보 설정 시도	사용자 아이디	보호된 등록 정보 설정 시도	
10	정보	사용자의 세션 할당량을 모두 사용함	사용자 아이디	세션 할당량을 모두 사용했습니다.	
11	정보	세션 페일오버 및 세션 제약 조건에 사용한 세션 데이터베이스를 사용할 수 없음	사용자 아이디	세션 데이터베이스에 접근할 수 없습니다.	
12	정보	세션 데이터베이스가 다시 온라인 상태로 전환함	사용자 아이디	세션 데이터베이스가 다시 온라인 상태로 전환함	
13	정보	AM 서버에 호스트된 유효한 세션의 총 수가 최대 제한값에 도달함	사용자 아이디	세션 최대 제한값에 도달했습니다.	

◆ ◆ ◆ 부 록 D

오류 코드

이 부록은 Access Manager에서 생성된 오류 코드 메시지 목록을 제공합니다. 이 목록이 완벽하지는 않지만 이 장에 설명된 정보는 일반 문제의 해결을 위한 훌륭한 출발점으로서의 역할을 수행할 것입니다. 이 부록에 나열된 표에서는 오류 코드, 오류에 대한 설명 및/또는 가능한 원인을 제공하고 발생한 문제를 수정하기 위해 수행할 수 있는 작업에 대해 설명합니다.

이 부록에서는 기능적으로 다음과 같은 영역으로 구분하여 오류 코드를 나열합니다.

오류 진단에 대한 도움이 필요한 경우 Sun 기술 지원부에 문의하십시오.

http://www.sun.com/service/sunone/software/index.html

Access Manager 콘솔 오류

다음 표에서는 Access Manager 콘솔에서 생성되고 표시되는 오류 코드에 대해 설명합니다.

표 D–1 Access Manager 콘솔 오류

오류 메시지	설명/가능한 원인	작업
다음을 삭제하는 중 오류가 발생했습니다.	현재 사용자가 객체를 제거하기 이전에 다른 사용자가 해당 객체를 제거했을 수 있습니다.	삭제할 객체를 다시 표시하고 작업을 다시 수행하십시오.
잘못된 URL을 입력했습니다.	이 메시지는 Access Manager 콘솔 창에 대한 URL을 잘못 입력한 경우에 발생합니다.	

표 D–1 Access Manager 콘솔 오류 *(계속)*

오류 메시지	설명/가능한 원인	작업
검색 기준과 일치하는 항목이 없습니다.	검색 창 또는 필터 필드에 입력한 매개 변수가 디렉토리에 있는 객체와 일치하지 않습니다.	다른 매개 변수 집합을 사용하여 검색을 다시 실행하십시오.
표시할 속성이 없습니다.	선택된 객체의 스키마에 편집 가능한 속성이 정의되어 있지 않습니다.	
이 서비스에 대해 표시할 정보가 없습니다.	서비스 구성 모듈에서 표시되는 서비스에 전역 또는 조직 기반 속성이 없습니다.	
검색 크기 제한을 초과했습니다. 검색 조건을 구체화하십시오.	검색에 지정된 매개 변수가 허용된 것보다 더 많은 항목을 반환했습니다.	관리 서비스의 검색에서 반환되는 최대 결과 수 속성을 더 큰 값으로 수정해야 합니다. 검색 매개 변수를 보다 제한적으로 수정할 수도 있습니다.
검색 시간 제한을 초과했습니다. 검색 조건을 구체화하십시오.	지정된 매개 변수에 대한 검색 작업이 허용된 검색 시간보다 더 오래 걸립니다.	관리 서비스에서 검색 시간 초과 속성을 더 큰 값으로 수정해야 합니다. 많은 값을 반환하도록 검색 매개 변수를 덜 제한적으로 수정할 수도 있습니다.
사용자 시작 위치가 유효하지 않습니다. 관리자에게 문의하십시오.	사용자 항목의 시작 위치 DN이 더 이상 유효하지 않습니다.	사용자 프로필 페이지에서 시작 DN 값을 유효한 DN으로 변경합니다.
Identity 객체를 만들지 못했습니다. 사용자에게 충분한 액세스 권한이 없습니다.	충분한 권한이 없는 사용자가 작업을 실행했습니다. 사용자가 정의한 권한에 따라 해당 사용자가 수행할 수 있는 작업이 결정됩니다.	

인증 오류 코드

다음 표에서는 인증 서비스에서 생성되는 오류 코드에 대해 설명합니다. 이러한 오류는 인증 모듈에서 사용자/관리자에게 표시됩니다.

표 D–2 인증 오류 코드

오류 메시지	설명/가능한 원인	작업
authentication.already.login.	사용자가 이미 로그인했고 유효한 세션이 있지만 성공 URL 리디렉션이 정의되어 있지 않습니다.	로그아웃을 수행하거나, Access Manager 콘솔을 통해 일부 로그인 성공 리디렉션 URL을 설정합니다. ”goto’ 쿼리 매개 변수를 해당 값과 함께 관리 콘솔 URL로 사용합니다.

표 D–2 인증 오류 코드 (계속)

오류 메시지	설명/가능한 원인	작업
logout.failure.	사용자가 Access Manager에서 로그아웃할 수 없습니다.	서버를 다시 시작합니다.
uncaught_exception	처리기가 잘못되어 인증 예외가 발생했습니다.	로그인 URL에 잘못된 문자 또는 특수 문자가 있는지 확인합니다.
redirect.error	Access Manager가 성공 또는 실패 리디렉션 URL에 리디렉션할 수 없습니다.	웹 컨테이너의 오류 로그에서 오류가 있는지 확인합니다.
gotoLoginAfterFail	이 링크는 대부분의 오류가 발생할 때 생성됩니다. 이 링크를 누르면 원본 로그인 URL 페이지로 이동합니다.	
invalid.password	입력한 비밀번호가 잘못되었습니다.	비밀번호는 8자 이상이어야 합니다. 비밀번호의 문자 수가 적절한지 확인하고 비밀번호가 만료되지 않았는지 확인합니다.
auth.failed	인증에 실패했습니다. 기본 로그인 실패 템플리트에 표시되는 일반적인 오류 메시지입니다. 가장 일반적인 원인은 유효하지 않은/잘못된 자격 증명입니다.	유효하고 올바른 사용자 이름/비밀번호(호출한 인증 모듈에 필요한 자격 증명)를 입력합니다.
nouser.profile	지정된 조직에 입력한 사용자 이름과 일치하는 사용자 프로필이 없습니다. 이 오류는 구성원/자동 등록 인증 모듈에 로그인할 때 표시됩니다.	로그인 정보를 다시 입력합니다. 첫 번째 로그인 시도인 경우 로그인 화면에서 새 사용자를 선택하십시오.
notenough.characters	입력한 비밀번호의 길이가 짧습니다. 이 오류는 구성원/자동 등록 인증 모듈에 로그인할 때 표시됩니다.	로그인 비밀번호는 기본적으로 8자 이상이어야 합니다. 이 수는 구성원 인증 모듈을 통해 구성 가능합니다.
useralready.exists	지정된 조직에 이 이름을 사용하는 사용자가 이미 있습니다. 이 오류는 구성원/자동 등록 인증 모듈에 로그인할 때 표시됩니다.	사용자 아이디는 조직 내에서 고유해야 합니다.
uidpasswd.same	사용자 이름 필드와 비밀번호 필드에 동일한 값을 사용할 수 없습니다. 이 오류는 구성원/자동 등록 인증 모듈에 로그인할 때 표시됩니다.	아이디 및 비밀번호가 다른지 확인합니다.
nouser.name	사용자 이름을 입력하지 않았습니다.이 오류는 구성원/자동 등록 인증 모듈에 로그인할 때 표시됩니다.	사용자 이름을 입력하십시오.
no.password	비밀번호를 입력하지 않았습니다.이 오류는 구성원/자동 등록 인증 모듈에 로그인할 때 표시됩니다.	비밀번호를 입력하십시오.

표 D–2 인증 오류 코드 *(계속)*

오류 메시지	설명/가능한 원인	작업
missing.confirm.passwd	구성 비밀번호 필드가 없습니다. 이 오류는 구성원/자동 등록 인증 모듈에 로그인할 때 표시됩니다.	비밀번호 확인 필드에 비밀번호를 입력하십시오.
password.mismatch	비밀번호와 확인용 비밀번호가 일치하지 않습니다. 이 오류는 구성원/자동 등록 인증 모듈에 로그인할 때 표시됩니다.	비밀번호와 확인용 비밀번호가 일치하는지 확인합니다.
사용자 프로필을 저장하는 중 오류가 발생했습니다.	사용자 프로필을 저장하는 중 오류가 발생했습니다.이 오류는 구성원/자동 등록 인증 모듈에 로그인할 때 표시됩니다.	`Membership.xml` 파일에서 속성 및 요소가 자동 등록에 유효한지 확인합니다.
orginactive	이 조직이 활성 상태가 아닙니다.	Access Manager 콘솔을 통해 조직 상태를 `inactive`에서 `active` 로 변경하여 조직을 활성화합니다.
internal.auth.error	내부 인증 오류입니다. 서로 다른 여러 환경 및/또는 구성 문제로 인해 발생할 수 있는 일반 인증 오류입니다.	
usernot.active	사용자가 더 이상 활성 상태가 아닙니다.	관리 콘솔을 통해 사용자 상태를 `inactive`에서 `active`로 변경하여 사용자를 활성화합니다. 메모리 잠금에 의해 사용자가 잠긴 경우 서버를 다시 시작하십시오.
user.not.inrole	사용자가 지정된 역할에 속하지 않습니다. 이 오류는 역할 기반 인증 중에 표시됩니다.	로그인 사용자가 역할 기반 인증에 지정된 역할에 속하는지 확인합니다.
session.timeout	사용자 세션이 시간 초과되었습니다.	다시 로그인합니다.
authmodule.denied	지정한 인증 모듈이 거부되었습니다.	요청한 인증 모듈이 요구된 조직에 등록되어 있고, 모듈에 대한 템플리트가 생성 및 저장되어 있으며, 핵심 인증 모듈의 조직 인증 모듈 목록에서 해당 모듈이 선택되어 있는지 확인합니다.
noconfig.found	구성을 찾지 못했습니다.	요청한 인증 방법에 대한 인증 구성 서비스를 확인합니다.
cookie.notpersistent	영구 쿠키 아이디가 영구 쿠키 도메인에 없습니다.	
nosuch.domain	조직이 있습니다.	요청된 조직이 유효하고 올바른지 확인합니다.

표 D–2 인증 오류 코드 (계속)

오류 메시지	설명/가능한 원인	작업
userhasnoprofile.org	지정된 조직에 사용자의 프로필이 없습니다.	로컬 Directory Server에서 사용자가 있으며 지정된 조직에 유효한지 확인합니다.
reqfield.missing	필수 필드 중 하나를 입력하지 않았습니다. 모든 필수 필드에 입력했는지 확인하십시오.	모든 필수 필드를 입력하십시오.
session.max.limit	최대 세션 제한에 도달했습니다.	로그아웃한 다음 다시 로그인합니다.

정책 오류 코드

다음 표에서는 정책 프레임워크에서 생성되고 Access Manager 콘솔에 표시되는 오류 코드에 대해 설명합니다.

표 D–3 정책 오류 코드

오류 메시지	설명/가능한 원인	작업
illegal_character_/_in_name	정책 이름에 잘못된 문자 “/”가 있습니다.	정책 이름에 ”/’ 문자가 있는지 확인합니다.
policy_already_exists_in_org	동일한 이름의 규칙이 이미 있습니다.	정책 작성에 다른 이름을 사용하십시오.
rule_name_already_present	지정된 이름을 갖는 다른 규칙이 이미 있습니다.	정책 작성에 다른 규칙 이름을 사용하십시오.
rule_already_present	동일한 규칙 값을 갖는 규칙이 이미 있습니다.	다른 규칙 값을 사용하십시오.
no_referral_can_not_create_policy	조직에 참조가 없습니다.	하위 조직에서 정책을 만들려면 상위 조직에서 참조 정책을 만들어 이 하위 조직에서 참조할 수 있는 자원을 나타내야 합니다.
ldap_search_exceed_size_limit	LDAP 검색 크기 제한을 초과했습니다. 검색에서 최대 결과 수보다 더 많은 결과를 찾았기 때문에 오류가 발생했습니다.	검색 제어 매개 변수에서 조직의 검색 패턴 또는 정책 구성을 변경합니다.검색 크기 제한은 정책 구성 서비스에 있습니다.
ldap_search_exceed_time_limit	LDAP 검색 시간 제한을 초과했습니다. 검색에서 최대 결과 수보다 더 많은 결과를 찾았기 때문에 오류가 발생했습니다.	검색 제어 매개 변수에서 조직의 검색 패턴 또는 정책 구성을 변경합니다.검색 크기 제한은 정책 구성 서비스에 있습니다.

표 D–3 정책 오류 코드 (계속)

오류 메시지	설명/가능한 원인	작업
ldap_invalid_password	LDAP 바인드 비밀번호가 잘못되었습니다.	정책 구성에 정의된 LDAP 바인드 사용자에 대한 비밀번호가 잘못되었습니다. 인증된 LDAP 연결을 구성하여 정책 작업을 수행할 수 없습니다.
app_sso_token_invalid	응용 프로그램 SSO 토큰이 잘못되었습니다.	서버에서 응용 프로그램 SSO 토큰을 검증하지 못했습니다. SSO 토큰이 만료되었을 수 있습니다.
user_sso_token_invalid	사용자 SSO 토큰이 잘못되었습니다.	서버에서 사용자 SSO 토큰을 검증하지 못했습니다. SSO 토큰이 만료되었을 수 있습니다.
property_is_not_an_Integer	등록 정보 값이 정수가 아닙니다.	이 플러그 인의 등록 정보 값이 정수여야 합니다.
property_value_not_defined	등록 정보 값을 정의해야 합니다.	지정된 등록 정보에 대한 값을 제공하십시오.
start_ip_can_not_be_greater_than_end_ip	시작 IP가 끝 IP보다 더 큽니다.	끝 IP 주소를 IP 주소 조건의 시작 IP 주소보다 더 크게 설정하려고 시도했습니다. 시작 IP가 끝 IP보다 크지 않아야 합니다.
start_date_can_not_be_larger_than_end_date	시작 날짜가 종료 날짜보다 더 큽니다.	종료 날짜를 정책 시간 조건의 시작 날짜보다 더 크게 설정하려고 시도했습니다. 시작 날짜가 종료 날짜보다 크지 않아야 합니다.
policy_not_found_in_organization	조직에 정책이 없습니다. 조직에서 존재하지 않는 정책을 찾는 중 오류가 발생했습니다.	정책이 지정된 조직에 있는지 확인합니다.
insufficient_access_rights	사용자에게 충분한 액세스 권한이 없습니다. 사용자에게 정책 작업 수행을 위한 충분한 권한이 없습니다.	적절한 액세스 권한이 있는 사용자가 정책 작업을 수행합니다.
invalid_ldap_server_host	LDAP 서버 호스트가 잘못되었습니다.	정책 구성 서비스에 입력한 잘못된 LDAP 서버 호스트를 변경합니다.

amadmin 오류 코드

다음 표에서는 `amadmin` 명령줄 도구에 의해 Access Manager의 디버그 파일에 생성되는 오류 코드를 설명합니다.

표 D–4 amadmin 오류 코드

오류 메시지	코드	설명/가능한 원인	작업
nocomptype	1	인수가 너무 적습니다.	필수 인수(--runasdn, --password, --passwordfile, --schema , --data, --addAttributes) 및 해당 값을 명령줄에 입력했는지 확인합니다.
file	2	입력 XML 파일이 없습니다.	구문을 확인하고 입력 XML이 유효한지 확인합니다.
nodnforadmin	3	--runasdn 값에 대한 사용자 DN이 없습니다.	사용자 DN을 --runasdn에 대한 값으로 제공합니다.
noservicename	4	--deletservice 값에 대한 서비스 이름이 없습니다.	서비스 이름을 --deleteservice에 대한 값으로 제공합니다.
nopwdforadmin	5	--password 값에 대한 비밀번호가 없습니다.	비밀번호를 --password에 대한 값으로 제공합니다.
nolocalename	6	로켈 이름을 지정하지 않았습니다. 로켈은 en_US를 기본값으로 사용합니다.	로켈 목록에 대한 온라인 도움말을 참조하십시오.
nofile	7	XML 입력 파일이 없습니다.	처리할 입력 XML 파일 이름을 하나 이상 지정하십시오.
invopt	8	하나 이상의 인수가 잘못되었습니다.	모든 인수가 유효한지 확인합니다. 유효한 인수 집합을 보려면 amadmin --help를 입력하십시오.
oprfailed	9	작업이 실패했습니다.	amadmin이 실패할 경우 세부적인 오류 코드를 생성하여 특정 오류를 나타냅니다. 이러한 오류 코드를 참조하여 문제를 평가하십시오.
execfailed	10	요청을 처리할 수 없습니다.	amadmin이 실패할 경우 세부적인 오류 코드를 생성하여 특정 오류를 나타냅니다. 이러한 오류 코드를 참조하여 문제를 평가하십시오.
policycreatexception	12	정책을 만들 수 없습니다.	amadmin은 특정 오류를 나타내는 예외 메시지를 생성합니다. 이러한 메시지를 참조하여 문제를 평가하십시오.

표 D–4 amadmin 오류 코드 *(계속)*

오류 메시지	코드	설명/가능한 원인	작업
policydelexception	13	정책을 삭제할 수 없습니다.	amadmin은 특정 오류를 나타내는 예외 메시지를 생성합니다. 이러한 메시지를 참조하여 문제를 평가하십시오.
smsdelexception	14	서비스를 삭제할 수 없습니다.	amadmin은 특정 오류를 나타내는 예외 메시지를 생성합니다. 이러한 메시지를 참조하여 문제를 평가하십시오.
ldapauthfail	15	사용자를 인증할 수 없습니다.	사용자 DN 및 비밀번호가 올바른지 확인합니다.
parserror	16	입력 XML 파일을 구문 분석할 수 없습니다.	XML이 올바르게 서식 지정되어 있고 amAdmin.dtd를 준수하는지 확인합니다.
parseiniterror	17	응용 프로그램 오류 또는 구문 분석기 초기화 오류로 인해 구문 분석할 수 없습니다.	XML이 올바르게 서식 지정되어 있고 amAdmin.dtd를 준수하는지 확인합니다.
parsebuilterror	18	지정한 옵션으로 구문 분석기를 만들 수 없기 때문에 구문 분석할 수 없습니다.	amadmin은 특정 오류를 나타내는 예외 메시지를 생성합니다. 이러한 메시지를 참조하여 문제를 평가하십시오.
ioexception	19	입력 XML 파일을 읽을 수 없습니다.	amadmin은 특정 오류를 나타내는 예외 메시지를 생성합니다. 이러한 메시지를 참조하여 문제를 평가하십시오.
fatalvalidationerror	20	XML 파일이 유효한 파일이 아니기 때문에 구문 분석할 수 없습니다.	구문을 확인하고 입력 XML이 유효한지 확인합니다.
nonfatalvalidationerror	21	XML 파일이 유효한 파일이 아니기 때문에 구문 분석할 수 없습니다.	amadmin은 특정 오류를 나타내는 예외 메시지를 생성합니다. 이러한 메시지를 참조하여 문제를 평가하십시오.
validwarn	22	파일에 대한 XML 파일 검증 경고	amadmin은 특정 오류를 나타내는 예외 메시지를 생성합니다. 이러한 메시지를 참조하여 문제를 평가하십시오.
failedToProcessXML	23	XML 파일을 처리할 수 없습니다.	amadmin은 특정 오류를 나타내는 예외 메시지를 생성합니다. 이러한 메시지를 참조하여 문제를 평가하십시오.

표 D–4 amadmin 오류 코드 (계속)

오류 메시지	코드	설명/가능한 원인	작업
nodataschemawarning	24	--data 또는 --schema 옵션이 명령에 없습니다.	모든 인수가 유효한지 확인합니다. 유효한 인수 집합을 보려면 amadmin --help를 입력하십시오.
doctyperror	25	XML 파일이 올바른 DTD를 따르지 않습니다.	XML 파일의 DOCTYPE 요소를 확인하십시오.
statusmsg9	26	DN, 비밀번호, 호스트 이름 또는 포트 번호가 잘못되었기 때문에 LDAP 인증에 실패했습니다.	사용자 DN 및 비밀번호가 올바른지 확인합니다.
statusmsg13	28	서비스 관리자 예외(SSO 예외)	amadmin은 특정 오류를 나타내는 예외 메시지를 생성합니다. 이러한 메시지를 참조하여 문제를 평가하십시오.
statusmsg14	29	서비스 관리자 예외	amadmin은 특정 오류를 나타내는 예외 메시지를 생성합니다. 이러한 메시지를 참조하여 문제를 평가하십시오.
statusmsg15	30	스키마 파일 입력 스트림 예외	amadmin은 특정 오류를 나타내는 예외 메시지를 생성합니다. 이러한 메시지를 참조하여 문제를 평가하십시오.
statusmsg30	31	정책 관리자 예외(SSO 예외)	amadmin은 특정 오류를 나타내는 예외 메시지를 생성합니다. 이러한 메시지를 참조하여 문제를 평가하십시오.
statusmsg31	32	정책 관리자 예외	amadmin은 특정 오류를 나타내는 예외 메시지를 생성합니다. 이러한 메시지를 참조하여 문제를 평가하십시오.
dbugerror	33	여러 디버그 옵션을 지정했습니다.	디버그 옵션은 하나만 지정해야 합니다.
loginFalied	34	로그인에 실패했습니다.	amadmin은 특정 오류를 나타내는 예외 메시지를 생성합니다. 이러한 메시지를 참조하여 문제를 평가하십시오.
levelerr	36	속성 값이 잘못되었습니다.	LDAP 검색에 대한 수준 설정을 확인합니다. SCOPE_SUB 또는 SCOPE_ONE이어야 합니다.

표 D–4 amadmin 오류 코드 *(계속)*

오류 메시지	코드	설명/가능한 원인	작업
failToGetObjType	37	객체 유형을 가져오는 중 오류가 발생했습니다.	XML 파일의 DN이 유효하고 올바른 객체 유형을 포함하는지 확인합니다.
invalidOrgDN	38	조직 DN이 잘못되었습니다.	XML 파일의 DN이 유효하고 조직 객체인지 확인합니다.
invalidRoleDN	39	역할 DN이 잘못되었습니다.	XML 파일의 DN이 유효하고 역할 객체인지 확인합니다.
invalidStaticGroupDN	40	정적 그룹 DN이 잘못되었습니다.	XML 파일의 DN이 유효하고 정적 그룹 객체인지 확인합니다.
invalidPeopleContainerDN	41	사용자 컨테이너 DN이 잘못되었습니다.	XML 파일의 DN이 유효하고 사용자 컨테이너 객체인지 확인합니다.
invalidOrgUnitDN	42	조직 구성 단위 DN이 잘못되었습니다.	XML 파일의 DN이 유효하고 컨테이너 객체인지 확인합니다.
invalidServiceHostName	43	서비스 호스트 이름이 잘못되었습니다.	유효한 세션 검색을 위한 호스트 이름이 올바른지 확인합니다.
subschemaexception	44	하위 스키마 오류	하위 스키마는 전역 및 조직 속성에만 지원됩니다.
serviceschemaexception	45	서비스에 대한 서비스 스키마를 찾을 수 없습니다.	XML 파일에서 하위 스키마가 유효한지 확인합니다.
roletemplateexception	46	역할 템플리트는 스키마가 동적 유형인 경우에만 true일 수 있습니다.	XML 파일에서 역할 템플리트가 유효한지 확인합니다.
cannotAddusersToFileredRole	47	필터링된 역할에 사용자를 추가할 수 없습니다.	XML 파일의 역할 DN이 필터링된 역할이 아닌지 확인합니다.
templateDoesNotExist	48	템플리트가 없습니다.	XML 파일에서 서비스 템플리트가 유효한지 확인합니다.
cannotAdduUersToDynamicGroup	49	동적 그룹에 사용자를 추가할 수 없습니다.	XML 파일의 그룹 DN이 동적 그룹이 아닌지 확인합니다.
cannotCreatePolicyUnderContainer	50	컨테이너의 하위 조직인 조직에서 정책을 만들 수 없습니다.	정책을 만들 조직이 컨테이너의 하위 조직이 아닌지 확인합니다.
defaultGroupContainerNotFound	51	그룹 컨테이너가 없습니다.	상위 조직 또는 컨테이너에 대해 그룹 컨테이너를 만듭니다.
cannotRemoveUserFromFilteredRole	52	필터링된 역할에서 사용자를 제거할 수 없습니다.	XML 파일의 역할 DN이 필터링된 역할이 아닌지 확인합니다.

표 D–4 amadmin 오류 코드 (계속)

오류 메시지	코드	설명/가능한 원인	작업
cannotRemoveUsersFromDynamicGroup	53	동적 그룹에서 사용자를 제거할 수 없습니다.	XML 파일의 그룹 DN이 동적 그룹이 아닌지 확인합니다.
subSchemStringDoesNotExist	54	하위 스키마 문자열이 없습니다.	XML 파일에 하위 스키마 문자열이 있는지 확인합니다.
defaultPeopleContainerNotFound	59	조직 또는 컨테이너에 사용자를 추가하려고 합니다. 그런데 기본 사용자 컨테이너가 조직 또는 컨테이너에 존재하지 않습니다.	기본 사용자 컨테이너가 존재하는지 확인해야 합니다.
nodefaulturlprefix	60	--defaultURLPrefix 인수 다음에 기본 URL 접두어가 없습니다.	기본 URL 접두어를 제공합니다.
nometaalias	61	--metaalias 인수 다음에 메타 별칭이 없습니다.	메타 별칭을 제공합니다.
missingEntityName	62	엔티티 이름이 지정되어 있지 않습니다.	엔티티 이름을 제공합니다.
missingLibertyMetaInputFile	63	메타 데이터를 가져오기 위한 파일 이름이 빠져 있습니다.	메타 데이터가 포함된 파일 이름을 제공합니다.
missingLibertyMetaOutputFile	64	내보낸 메타 데이터를 저장할 파일 이름이 빠져 있습니다.	메타 데이터를 저장할 파일 이름을 제공합니다.
cannotObtainMetaHandler	65	메타 속성에 대한 처리기를 가져올 수 없습니다. 지정된 사용자 이름과 비밀번호가 틀린 것일 수 있습니다.	사용자 이름과 비밀번호가 맞는지 확인합니다.
missingResourceBundleName	66	Directory Server에 저장된 자원 번들을 추가하거나, 보거나 또는 삭제할 때 자원 번들 이름이 빠져 있습니다.	자원 번들 이름을 제공합니다.
missingResourceFileName	67	자원 번들을 Directory Server에 추가할 때 자원 문자열이 포함된 파일의 이름이 빠져 있습니다.	유효한 파일 이름을 입력합니다.
failLoadLibertyMeta	68	Liberty 메타를 Directory Server에 로드하는 데 실패했습니다.	다시 로드하기 전에 메타 데이터를 다시 확인합니다.

색인

J

L

M

O

P

R

S

U

V

W

X

개

계

관

구

권

그

나

데

디

로

일

자

작

정

조

주

지

참

컨

콘

페

플

현