

Anyframe IAM Plugin



Version 1.0.2

저작권 © 2007-2011 삼성SDS

본 문서의 저작권은 삼성SDS에 있으며 Anyframe 오픈소스 커뮤니티 활동의 목적하에서 자유로운 이용이 가능합니다. 본 문서를 복제, 배포할 경우에는 저작권자를 명시하여 주시기 바라며 본 문서를 변경하실 경우에는 원문과 변경된 내용을 표시하여 주시기 바랍니다. 원문과 변경된 문서에 대한 상업적 용도의 활용은 허용되지 않습니다. 본 문서에 오류가 있다고 판단될 경우 이슈로 등록해 주시면 적절한 조치를 취하도록 하겠습니다.

I. Introduction	1
II. Secured Resource	2
1. 권한 관리	3

I.Introduction

IAM Plugin은 Spring Security [<http://static.springsource.org/spring-security/site/index.html>]를 기반으로 사용자 인증 및 권한 관리 기능을 제공하는 Anyframe IAM [<http://anyframejava.org/project/iam>]의 기본 활용 방법을 가이드하기 위한 샘플 코드와 이 오픈소스들을 활용하는데 필요한 참조 라이브러리들로 구성되어 있다.

Installation

Command 창에서 다음과 같이 명령어를 입력하여 IAM plugin을 설치한다.

```
mvn anyframe:install -Dname=iam
```

installed(mvn anyframe:installed) 혹은 jetty:run(mvn clean jetty:run) command를 이용하여 설치 결과를 확인해볼 수 있다.

Dependent Plugins

Plugin Name	Version Range
Query [http://dev.anyframejava.org/docs/anyframe/plugin/optional/query/1.1.2/reference/htmlsingle/query.html]	2.0.0 > *

WAS(Web Application Server)별 유의사항

다음은 IAM Plugin이 설치된 샘플 어플리케이션에 대한 WAS별 유의사항이다.

- JEUS
 - 6.0 : IAM Plugin 설치로 생성된 샘플 어플리케이션에서 활용하는 Spring Security 라이브러리와 호환을 위해 JEUS 6.0 최신 패치가 설치되어 있어야 한다.

II.Secured Resource

IAM은 WebURL, Service Method, Pointcut 등에 대한 권한 관리 기능을 제공하며, 이러한 대상 항목들을 Secured Resource 라고 한다. IAM Plugin 예제를 통하여 WebURL 형태로 보호되는 자원에 대해서 알아보도록 한다.

1. 권한 관리

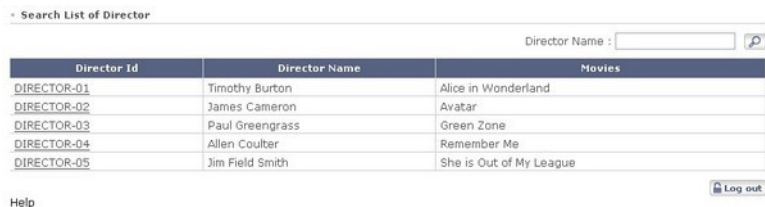
이번 장에서는 DB를 기반으로 보호되어지는 웹 자원(Secured Resource)에 대한 권한 관리를 담당하는 IAM의 기본 기능들을 중심으로 권한 설정 및 관리 방법을 설명 하도록 한다.



This is Anyframe IAM Sample web application.

User : Password :

위 그림은 Web Application 가동 후, IAM SAMPLE 메뉴를 클릭하면 나오는 화면이다. 하단의 User / Password 입력상자에는 사용자가 즉시 로그인 할 수 있도록 admin / admin123 이 입력되어 있다. Login 버튼을 클릭해서 다음 화면을 살펴 보도록 하자.



admin 계정으로 로그인 한 사용자는 ROLE_ADMIN 권한을 가지게 되는데 이 권한은 모든 감독의 목록에 대한 접근 권한과, 감독 정보에 대한 수정 권한을 모두 가진다. admin 계정이 아닌 다른 계정으로 로그인 하고자 하는 경우에는 위 그림의 좌측 하단에 있는 Help 링크를 클릭하면 아래와 같은 팝업 정보가 나타난다.



로그인 가능한 사용자는 admin, user, buyer 총 3가지 이다. 각각의 사용자는 서로 다른 역할(ROLE)을 가지며, 그에 따라 각각 다른 접근 권한을 가진다. 예를 들어 Help에 적혀있는 buyer 계정으로 로그인 할 경우, 로그인 직후 아래와 같은 접근 거부 메시지를 확인하게 된다.



3 개의 권한에 따른 각 권한별 실행 가능 자원을 정리해보면 다음 표와 같다.

<input type="checkbox"/>	Director List	Update Director
buyer(ROLE_RESTRICTED)	X	X
user(ROLE_USER)	O	X
admin(ROLE_ADMIN)	O	O

user / user123 으로 로그인을 한 후 Director Update 명령을 실행하면 마찬가지로 Access is denied 메시지가 나오면서 사용이 제한 된다. 이는 "/iamListDirector.do", "/iamUpdateDirector.do" 두 웹 자원이 보호자원으로 DB에 등록되어 있기 때문이다. 이를 확인해보기 위해서 DB에서 SECURED_RESOURCES 테이블을 조회 해보면 다음과 같이 1개의 포인트컷 자원과 2개의 WEB 자원을 확인할 수 있다.

RESOURCE_ID	SYSTEM_NAME	RESOURCE_NAME	RESOURCE_PATTERN	DESCRIPTION	RESOURCE_TYPE
PNC_000001	SAMPLE	List	execution(* anyframe.iam.core.*Service.*Bbnydory(..))		pointcut
WEB-000002	SAMPLE	User Update	/iamUpdateDirector.doZ		url
WEB-000003	SAMPLE	Director List	/iamListDirector.doZ		url

SECURED_RESOURCES 테이블에 등록된 자원들은 보호 되어지도록 지정된 자원으로서, 해당 자원을 사용하기 위해서는 자원(SECURED_RESOURCE)과 역할(ROLE)을 서로 맺어줘야 한다. 이에 대한 내용은 DB상의 SECURED_RESOURCES_ROLES 테이블에서 확인할 수 있다.

RESOURCE_ID	ROLE_ID	CREATE_DATE	MODIFY_DATE
PNC_000001	ROLE_USER	20100107	(null)
WEB-000002	ROLE_ADMIN	20100107	(null)
WEB-000003	ROLE_USER	20100107	(null)

현재 SECURED_RESOURCES_ROLES 테이블에 등록된 내용을 살펴보면, WEB-000002 (/iamUpdateDirector.do) 자원은 ROLE_ADMIN에 등록 되어있는것을 볼 수 있다. 따라서 /iamUpdateDirector.do 주소를 호출하게 되면 로그인한 사용자의 ROLE를 판별하여 ROLE_ADMIN이 아닌 경우 접근이 제한 된다. 마찬가지로 WEB-000003 (/iamListDirector.do) 자원은 ROLE_USER에 등록 되어 있으므로, ROLE_USER가 아닌 사용자에 대해서는 접근이 제한 되게 된다.

"/iamListDirector.do" 자원은 ROLE_USER에만 할당 되어 있지만 ROLE_ADMIN이 제한 없이 사용할 수 있는 이유는 ROLE을 계층적 구조로 사용하기 때문이다. 계층 구조상 상위에 배치된 ROLE은 하위 ROLE

에 할당된 자원에 대한 접근 권한을 모두 물려받는다. 현재 DB에는 최상위에 ROLE_ADMIN을 시작으로 ROLE_ADMIN - ROLE_USER - ROLE_RESTRICTED - IS_AUTHENTICATED_ANONYMOUSLY 순으로 배치되어 있으며, 이는 ROLES_HIERARCHY 테이블에서 확인할 수 있다. ROLES_HIERARCHY 테이블의 내용을 살펴보면 다음 그림과 같다.

PARENT_ROLE	CHILD_ROLE
IS_AUTHENTICATED_ANONYMOUSLY	ROLE_RESTRICTED
ROLE_RESTRICTED	ROLE_USER
ROLE_USER	ROLE_ADMIN

이 때 테이블 상의 PARENT_ROLE과 CHILD_ROLE이 일반적으로 생각되는 상하 관계와 반대로 정의되어 있기 때문에 주의해야 한다.

DB를 직접 수정하는 번거로움을 덜기 위해 IAM에서는 IAM Admin web application을 제공한다.

IAM Admin Web Application 사용법에 대한 자세한 내용은 Anyframe IAM Admin 매뉴얼 [<http://dev.anyframejava.org/docs/iam/1.1.0/reference/htmlsingle/anyframeiam.html#anyframeiamadmin>]을 참고하도록 한다.