

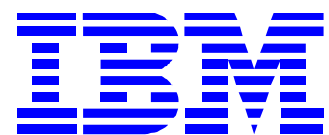
## **WebSphere Application Server v8.0**

**Fine-grained 관리 보안**

(2011. 06. )

IBM SWG WebSphere CTP

이정운(juwlee@kr.ibm.com)



## 0) Fine-grained 관리 보안 이란?

안녕하세요! Freeman 입니다. ^^&

이번에 시작하는 '먼저 해보는 IBM WAS v8.0' 시리즈의 다섯 번째 강좌는 "Fine-grained 관리 보안" 입니다. Fine-grained 관리 보안이란 기존과는 다르게 관리 콘솔의 보안을 좀 더 세밀하게 나눌 수 있는 기능으로서 하단처럼 세부적인 자원에 따라 사용자 관리 역할 지정이 가능한 기능을 의미합니다.

- Cells, node groups, nodes, clusters, servers, applications

해당 기능을 사용하게 되면 사용자는 할당된 자원 이외에 다른 어떤 자원도 접근할 수 없으므로 보안과 거버넌스를 향상시키며 접근 레벨에 따라 관리자 역할을 고립 시킬 수도 있습니다. 예를 들어 해당 기능을 활용하면 다수의 WAS 를 관리하는 관리콘솔에서 WAS 의 용도에 따라 하나의 관리콘솔에서 관리 가능한 WAS 를 관리자 별로 나누어 줄 수도 있습니다. 이를 통하여 지정된 관리자 이외에 다른 관리자는 해당 WAS 를 제어할 수 있는 권리를 가질 수 없기 때문에 운영환경에 따라 좀 더 강화된 보안과 통제 가능한 관리콘솔 환경을 제공할 수 있습니다.

(예를 들어 하나의 관리콘솔에서 1번 관리자는 1번 WAS 만 제어가능하고 2번 관리자는 2번 WAS 만 제어가능하게 할 수 있습니다.)

해당 기능을 지금 소개해 드리긴 하지만 실제적으로 해당 기능은 IBM WAS v7.0 이상부터 사용이 가능한점 유념하시기 바라겠습니다. 하단의 표는 자원별 액션을 취하기 위해서 필요한 역할의 리스트로서 참고하시기 바라겠습니다.

Table 1. Privileges required to access various administrative resources. The privileges required to access various administrative resources are shown in the following table:

Resource	Action	Required roles
Server	Start, stop, runtime operations	Server-operator, node-operator, cell-operator
Server	New, delete	Node-configurator, cell-configurator
Server	Edit configuration	Server-configurator, node-configurator, cell-configurator
Server	View configuration, runtime status	Server-monitor, node-monitor, cell-monitor
Node	Restart, stop, sync	Node-operator, Cell-operator
Node	Add, delete	Cell-configurator
Node	Edit configuration	Node-configurator, cell-configurator
Node	View configuration, runtime status	Node-monitor, cell-monitor
Cluster	Start, stop, runtime operations	Cluster-operator, cell-operator
Cluster	New, delete	Cell-configurator
Cluster	Edit configuration	Cluster-configurator, cell-configurator
Cluster	View configuration, runtime status	Cluster-monitor, cell-monitor
Cluster member	Start, stop, runtime operations	Server-operator, cluster-operator, node-operator, cell-operator
Cluster member	New, delete	Node-configurator, cell-configurator
Cluster member	Edit configuration	Server-configurator, cluster-configurator, node-configurator, cell-configurator
Cluster member	View configuration, runtime status	Server-monitor, cluster-monitor, node-monitor, cell-monitor
Application	All operations	Refer to the section "Deployer roles" in <a href="#">Administrative roles</a> .
Node, cluster	Add, delete	Cell-configurator

## 1) 글로벌 보안 설정

1. 기본적으로 Fine-grained 관리 보안 기능을 사용하기 위해서는 먼저 글로벌 보안이 설정되어 있어야 합니다. 이를 위하여 관리콘솔에 글로벌 보안을 설정하기 위해서 보안 > 글로벌 보안 메뉴를 클릭하여 합니다.

2. 사용자 계정 저장소의 사용 가능한 범주 정의에서 '연합 저장소'를 선택하고 구성 버튼을 클릭합니다.

3. 연합 저장소 설정 화면이 나오면 1차 관리 사용자 이름에 관리자로 사용할 ID를 입력하고 확인을 클릭합니다.

4. 확인을 클릭하면 바로 관리 사용자 비밀번호를 입력하는 메뉴가 나오는데 사용하고자 하는 비밀번호를 입력하고 확인을 클릭합니다.

**글로벌 보안**

메시지

⚠ 로컬 구성에 변경사항이 작성되었습니다. 다음을 수행할 수 있습니다.

- 마스터 구성에 직접 [저장](#)
- 저장하거나 버리기 전에 변경사항 [검토](#)

⚠ 이 변경사항을 적용하려면, 서버를 다시 시작해야 합니다.

**글로벌 보안 > 연합 저장소 > 관리 사용자 비밀번호**

범주에 내장 저장소가 포함될 경우, 1차 관리 사용자 계정이 내장 저장소에 저장됩니다. 보안을 사용 가능하게 하려면 비밀번호를 이 계  
 십시오. 보안을 사용 가능하게 한 후 관리 콘솔에서 사용자 및 그룹을 사용하여 이 계정을 관리할 수 있습니다.

**일반 특성**

\* 비밀번호

\* 비밀번호 확인

5. 다시 글로벌 보안 메뉴로 나오면 관리 보안 사용을 설정하시고(현재 이 강좌에서는 다루지 않을 예정  
 이기 때문에 어플리케이션 보안은 해제) 사용 가능한 범주 정의에서 현재로 설정을 클릭한 후 다시 바  
 로 적용을 클릭합니다.

**글로벌 보안**

관리 및 기본 애플리케이션 보안 정책을 구성하려면 이 패널을 사용하십시오. 이 보안 구성은 모든 관리 기능에  
 플리케이션의 기본 보안 정책으로 사용됩니다. 보안 도메인은 사용자 애플리케이션의 보안 정책을 대체하고 시

**관리 보안**

☒ 관리 보안 사용

- [관리 사용자 역할](#)
- [관리 그룹 역할](#)
- [관리 인증](#)

**애플리케이션 보안**

☐ [애플리케이션 보안 사용 가능]

**Java 2 보안**

☐ 로컬 자원에 대한 애플리케이션 액세스를 제한하는 Java 2 보안 사용

- ☐ 애플리케이션에 사용자 정의 사용 권한이 부여된 경우에 경고
- ☐ 자원 인증 데이터에 대한 액세스 제한

**사용자 계정 저장소**

범주 이름

현재 범주 정의

사용 가능한 범주 정의

**인증**

인증 메커니즘 및 만기

- ☒ [LTPA](#)
- ☐ Kerberos 및 LTPA  
[Kerberos 구성](#)
- ☐ SWAM(제공되지 않음): 서  
[인증 캐시 설정](#)

☐ 웹 및 SIP 보안

☐ RMI/IIOP 보안

☐ Java 인증 및 권한 서비스

☐ JASPI(Java Authentica  
 tication Service) 제공자

☐ 범주 규정 사용자 이름 사

- [보안 도메인](#)
- [외부 권한 제공자](#)
- [프로그램 세션 쿠키 구성](#)
- [사용자 정의 특성](#)

6. 하단과 같은 장문의 메시지를 확인하고 변경된 사항을 저장하기 위하여 저장을 클릭합니다.

#### 글로벌 보안

##### 메시지

- ⚠ 싱글 사인온에 대한 도메인 이름이 정의되지 않았습니다. 웹 브라우저는 도메인 이름을 웹 애플리케이션이 실행하는 호스트 이름으로 기본 설정합니다. 싱글 사인온이 애플리케이션 서버 호스트 이름으로 제한되며 도메인의 다른 애플리케이션 서버 호스트 이름으로 작업하지 않습니다.
- ⚠ 로컬 자원에 대한 제한된 액세스 옵션이 사용 불가능한 경우, JVM(Java Virtual Machine) 시스템 자원은 보호되지 않습니다. 예를 들면 애플리케이션에서는 파일 시스템의 파일을 읽고 쓰며, 소켓 호출을 실행하며, 애플리케이션 서버 프로세스를 종료하는 등의 작업을 수행할 수 있습니다. 그러나 로컬 자원에 대한 제한된 액세스 옵션을 사용 가능하게 할 경우, 애플리케이션에 필수 권한이 부여되지 않았으면 애플리케이션이 실행되지 못할 수도 있습니다.
- ℹ 필드가 변경된 경우, 구성을 저장하고 서버를 중지한 후 다시 시작하십시오.
- ⚠ 로컬 구성에 변경사항이 작성되었습니다. 다음을 수행할 수 있습니다.
  - 마스터 구성에 직접 [저장](#)
  - 저장하거나 버리기 전에 변경사항 [검토](#)
- ⚠ 이 변경사항을 적용하려면, 서버를 다시 시작해야 합니다.

7. 저장이 정상적으로 완료되면 해당 설정의 반영을 위해서 다음과 같은 script 로 서버를 재시작 합니다.

```
C:\IBM\WebSphere8\AppServer\profiles\AppSrv01\bin>stopserver server1
ADMU0116I: 도구 정보가
C:\IBM\WebSphere8\AppServer\profiles\AppSrv01\logs\server1\stopServer
.log
파일에 로그 중입니다.
ADMU0128I: AppSrv01 프로파일로 도구 시작 중
ADMU3100I: 다음 서버에 대한 구성을 읽는 중: server1
ADMU3201I: 서버 중지 요청이 발행되었습니다. 중지 상태 대기 중입니다.
ADMU4000I: server1 서버 중지가 완료되었습니다.

C:\IBM\WebSphere8\AppServer\profiles\AppSrv01\bin>startserver server1
ADMU0116I: 도구 정보가
C:\IBM\WebSphere8\AppServer\profiles\AppSrv01\logs\server1\startServer
r.log
파일에 로그 중입니다.
ADMU0128I: AppSrv01 프로파일로 도구 시작 중
ADMU3100I: 다음 서버에 대한 구성을 읽는 중: server1
ADMU3200I: 서버가 실행되었습니다. 초기화 상태 대기 중입니다.
ADMU3000I: server1 서버가 e-business용으로 열렸습니다. 프로세스 ID: 6088

C:\IBM\WebSphere8\AppServer\profiles\AppSrv01\bin>
```

8. 다시 관리 콘솔로 접속하면 보안이 걸려있는 상태라 https 프로토콜로 접속되며 SSL 을 위한 인증서를 받기 위하여 '이 웹 사이트를 계속 탐색합니다.' 를 선택합니다.



9. 그렇게 되면 하단처럼 관리콘솔 로그인 화면을 확인할 수 있으며 기존에 입력한 관리자 ID 와 비밀번호를 입력해야지만 해당 관리콘솔로 들어갈 수 있습니다.

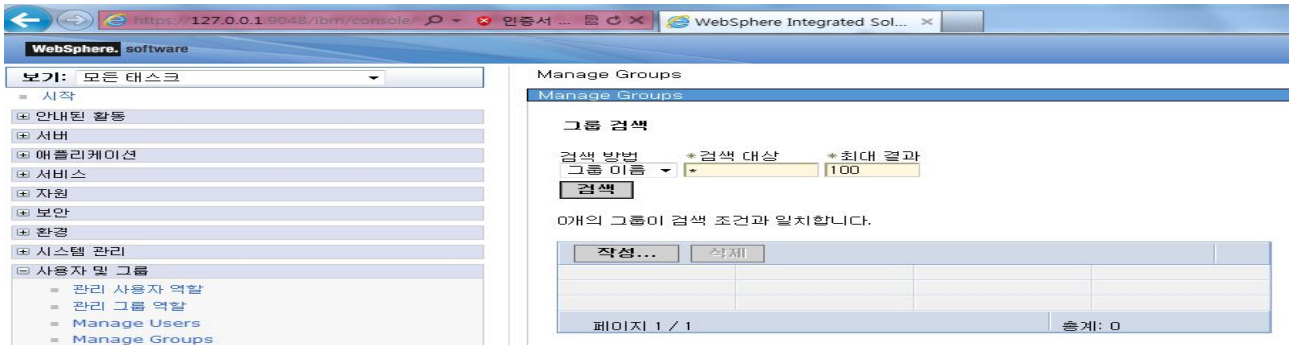


10. 즉, Fine-grained 관리 보안을 설정하기 위한 첫 번째 단계인 글로벌 보안 설정을 완료하신 것 입니다.

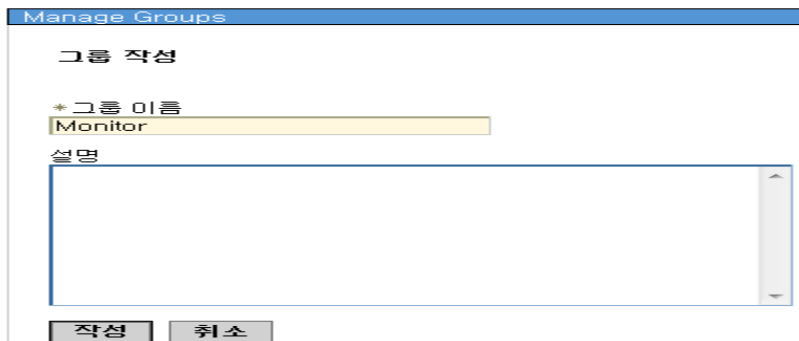


## 2) Fine-grained 관리 보안 설정

1. Fine-grained 관리 보안 설정을 하기 위해서는 Cell 단위 모니터링 권한을 가지고 있는 사용자가 필요합니다. 그래서 먼저 모니터링 권한이 있는 그룹을 만들기 위하여 관리콘솔에서 사용자 및 그룹 > Manage Groups 메뉴를 클릭합니다.



2. Manage Groups 메뉴에서 작성을 클릭한후 원하는 그룹 이름을 넣어 주고 작성을 누르면 하단과 같이 그룹 작성 메뉴가 나오는데 원하는 그룹을 하나 생성합니다.



3. 생성된 그룹에 실제로 모니터링 권한을 배분하기 위하여 사용자 및 그룹 > 관리 그룹 역할 메뉴를 클릭하여 추가를 선택합니다.



4. 추가를 클릭하면 하단과 같은 그룹 역할 설정 세부 메뉴를 확인할 수 있습니다.

#### 관리 그룹 역할 > 그룹

이 페이지에서 그룹에 대한 관리 역할을 추가, 업데이트 또는 제거할 수 있습니다. 관리 역할이 지정된 그룹은 콘 사용하여 애플리케이션 서버를 관리할 수 있습니다.

##### \* 역할

ISC 관리  
감사자  
관리 보안 관리자  
관리자

☐ 특별 주제에서 선택

특별 주제

ALL AUTHENTICATED

☒ 아래 지정된 대로 그룹 매핑

표시할 결과 수를 결정하고 검색 문자열(와일드카드에는 \* 사용)을 입력한 후 검색을 클릭하십시오. 사용 가능 매핑될 목록에 추가하십시오. 역할에 이미 매핑된 그룹은 검색 결과에 리턴되지 않습니다.

검색 문자열

\*

검색

표시할 최대 결과 수

20

사용 가능

역할에 매핑될



모두 선택

모두 선택 취소

모두 선택

모두 선택 취소

5. 관리 그룹 역할 설정 메뉴에서 모니터를 선택하고 검색을 클릭하면 방금 만들어진 Monitor 그룹이 나타납니다. 이후 해당 그룹을 선택하고 화살표 버튼을 클릭하여 역할에 매핑시키고 해당 내용을 저장 시킵니다.

#### 관리 그룹 역할 > 그룹

이 페이지에서 그룹에 대한 관리 역할을 추가, 업데이트 또는 제거할 수 있습니다. 관리 역할이 지정 사용하여 애플리케이션 서버를 관리할 수 있습니다.

##### \* 역할

관리자  
구성자  
모니터  
배치자

☐ 특별 주제에서 선택

특별 주제

ALL AUTHENTICATED

☒ 아래 지정된 대로 그룹 매핑

표시할 결과 수를 결정하고 검색 문자열(와일드카드에는 \* 사용)을 입력한 후 검색을 클릭하십시오. 매핑될 목록에 추가하십시오. 역할에 이미 매핑된 그룹은 검색 결과에 리턴되지 않습니다.

검색 문자열

\*

검색

표시할 최대 결과 수

20

사용 가능

역할에 매핑될

Monitor@defaultWIMFileBasedRealm



6. 그러면 하단과 같이 방금 지정한 관리 그룹 역할이 추가된 것을 확인할 수 있습니다.

#### 관리 그룹 역할

이 페이지에서 그룹에 대한 관리 역할을 추가, 업데이트 또는 제거할 수 있습니다. 관리 역할이 지정된 그룹은 관리 콘솔 또는 **wsadm** 사용하여 애플리케이션 서버를 관리할 수 있습니다.

추가...

제거

선택

그룹

역할

Monitor@defaultWIMFileBasedRealm

모니터

PRIMARYADMINID

감사자

SERVERID

감사자

총계 3

7. 이제는 Fine-grained 관리 보안 설정을 가진 실제 사용자를 만들기 위하여 사용자 및 그룹 > Manage Users 메뉴를 클릭하여 작성을 선택합니다.

WebSphere. software

보가: 모든 태스크

- 시작
- 안내된 활동
- 서버
- 애플리케이션
- 서비스
- 자원
- 보안
- 환경
- 시스템 관리
- 사용자 및 그룹
  - 관리 사용자 역할
  - 관리 그룹 역할
  - Manage Users
  - Manage Groups

Manage Users

Manage Users

사용자 검색

검색 방법 \*검색 대상 \*최대 결과  
 사용자 ID \* 100

1명의 사용자가 검색 조건과 일치합니다.

선택	사용자 ID	이름	성	이메일	고유 이름
<input type="checkbox"/>	wasadm	wasadm	wasadm		uid=wasadm,o=defaultWIMFileBasedRealm

페이지 1 / 1      총계: 1

8. 사용자 작성 메뉴가 나오면 그룹 멤버십을 클릭합니다.

Manage Users

사용자 작성

\*사용자 ID

\*이름      \*성  
     

이메일

\*비밀번호      \*비밀번호 확인

9. 그룹 멤버십 메뉴가 나오면 검색을 클릭하여 미리 만들어둔 그룹인 Monitor 그룹을 확인합니다.

#### 그룹 멤버십

이 사용자가 속할 그룹을 찾는 데 사용할 검색 조건을 지정하십시오.

검색 방법  \*검색 대상  \*최대 결과

Monitor

10. 미리 만들어둔 Monitor 그룹을 추가하고 닫기 버튼을 클릭합니다.

#### 그룹 멤버십

이 사용자가 속할 그룹을 찾는 데 사용할 검색 조건을 지정하십시오.

검색 방법  \*검색 대상  \*최대 결과

Monitor

11. 다시 사용자 작성 메뉴가 나오면 나머지 항목을 입력하고 작성 버튼을 클릭합니다.

#### 사용자 작성

\*사용자 ID

\*이름  \*성

이메일

\*비밀번호  \*비밀번호 확인

12. 그러면 다음과 같이 사용자 검색 리스트에 방금 입력한 사용자가 추가된 것을 확인할 수 있습니다.

#### 사용자 검색

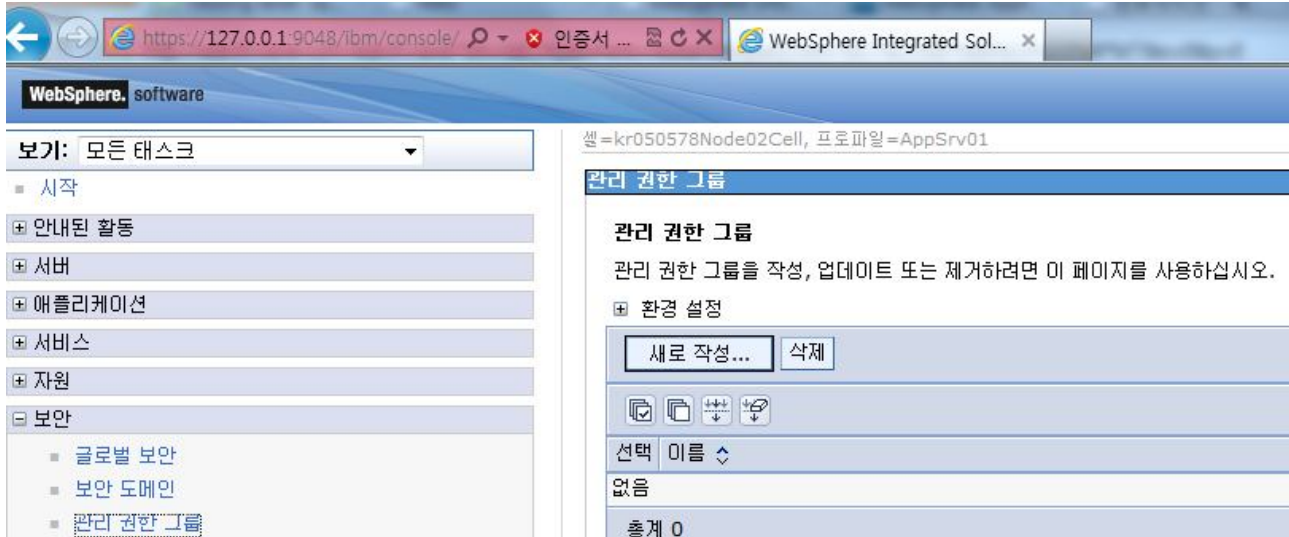
검색 방법  \*검색 대상  \*최대 결과

2명의 사용자가 검색 조건과 일치합니다.

선택	사용자 ID	이름	성	이메일	고유 이름
<input type="checkbox"/>	<a href="#">DefaultAdmin</a>	ddd	dddd		uid=DefaultAdmin,o=defaultWIMFileBasedRealm
<input type="checkbox"/>	<a href="#">wasadm</a>	wasadm	wasadm		uid=wasadm,o=defaultWIMFileBasedRealm

페이지 1 / 1 총계: 2

13. 위의 단계까지 따라해서 필요한 Monitor 권한을 가진 그룹과 그 그룹에 매핑된 사용자를 추가로 만들었습니다. 이제 실질적인 Fine-grained 관리 보안 설정을 하기 위하여 관리콘솔에서 보안 > 관리 권한 그룹 메뉴를 선택하여 새로 작성을 클릭합니다.



14. 여기서 중요한 것은 본인이 원하는 범위로 관리 권한 그룹을 만드시는 것 입니다. 하단에 표시된 자원에서 관리자 권한을 주려고 하는 범위만 찾아서 선택을 하면 됩니다. WAS ND 버전이 아니라 기본버전을 이용해서 테스트하는 것이므로 하단에는 샘플로 DefaultApplication 를 제어할 수 있는 권한만 할당을 하였습니다. 하지만 WAS ND 같은 경우에는 필요하다면 WAS 서버별로 관리 권한을 제어할 수도 있습니다.

#### 관리 권한 그룹 > 새로 작성...

관리 권한 그룹을 설정하고 연관된 관리 자원을 지정하려면 이 페이지를 사용하십시오.

구성

---

**일반 특성**

\* 이름  
DefaultGroup

**자원**  
표시:  
모든 범위

- ☐ 클러스터
- ☐ 비즈니스 레벨 애플리케이션
- ☐ 자산
- ☐ 애플리케이션
  - ☐ query
  - ☐ ivtApp
  - ☒ DefaultApplication
- ☐ 노드
- ☐ 노드 그룹

15. 위의 작업을 정상적으로 완료하셨다면 관리 권한 그룹 메뉴 리스트에 방금 만든 관리 권한 그룹을 생성할 수 있습니다. 다음으로 사용자를 할당하기 위하여 생성한 관리 권한 그룹을 클릭하시면 됩니다.

**관리 권한 그룹**

**관리 권한 그룹**  
관리 권한 그룹을 작성, 업데이트 또는 제거하려면 이 페이지를 사용하십시오.

환경 설정

새로 작성... 삭제

선택 이름

DefaultGroup

총계 1

16. 관리 권한 그룹 생성 이후에는 추가 특성이 활성화 되는 것을 확인할 수 있으며 관리 사용자 역할 메뉴를 클릭합니다.

**관리 권한 그룹 > DefaultGroup**

관리 권한 그룹을 설정하고 연관된 관리 자원을 지정하려면 이 페이지를 사용하십시오.

구성

**일반 특성**

\* 이름  
DefaultGroup

**자원**  
표시:  
모든 범위

- ☐ 클러스터
- ☐ 비즈니스 레벨 애플리케이션
- ☐ 자산
- ☐ 애플리케이션
  - ☐ query
  - ☐ ivtApp
  - ☒ DefaultApplication
- ☐ 노드
- ☐ 노드 그룹

**추가 특성**

- [관리 그룹 역할](#)
- [관리 사용자 역할](#)

17. 관리 사용자 역할 메뉴가 나오면 추가 버튼을 클릭합니다.

**관리 권한 그룹**

메시지  
관리 콘솔을 효율적으로 사용하려면 최소한 셀 범위 모니터 역할이 필요합니다. 관리 콘솔 액세스가 필요한 경우, 셀 레벨 역할을 이 사용자 또는 그룹에 지정하십시오.

**관리 권한 그룹 > DefaultGroup > 관리 사용자 역할**

이 페이지에서 사용자에게 대한 관리 역할을 추가, 업데이트 또는 제거할 수 있습니다. 관리 역할이 지정된 사용자는 관리 콘솔 또는 wsadmin 스크립트를 사용하여 애플리케이션 서버를 관리할 수 있습니다.

로그아웃 추가... 제거

선택 사용자 역할 로그인 상태

없음

총계 0

18. 관리자 사용자 역할에 관리자 역할을 선택하고 검색을 클릭하여 이전에 만들어둔 사용자인 Default Admin 을 해당 역할에 매핑하고 저장하면 됩니다.

**관리 권한 그룹**

관리 권한 그룹 > DefaultGroup > 관리 사용자 역할 > 사용자

이 페이지에서 사용자에게 대한 관리 역할을 추가, 업데이트 또는 제거할 수 있습니다. 관리 트를 사용하여 애플리케이션 서버를 관리할 수 있습니다.

**역할**

관리 보안 관리자  
구성자  
모니터

**사용자 검색 및 선택**

표시할 결과 수를 결정하고 검색 문자열(와일드카드에는 \* 사용)을 입력한 후 검색을 클릭  
매핑될 목록에 추가하십시오. 역할에 이미 매핑된 사용자는 검색 결과에 리턴되지 않습니다

검색 문자열:  검색

표시할 최대 결과 수:

사용 가능

역할에 매핑될

DefaultAdmin

모두 선택 모두 선택 취소

19. 이제 관리 콘솔을 log out 하신뒤에 새로 만든 사용자인 DefaultAdmin 사용자로 로그인 합니다 .

https://127.0.0.1:9048/ibm/console/ 인증서 ... WebSphere Integrated Sol...

WebSphere. software

WebSphere Integrated Solutions Console

사용자 ID: DefaultAdmin

비밀번호: .....

로그인

20. 권한이 제한된 사용자로 로그인 해서 어플리케이션 > WebSphere 엔터프라이즈 어플리케이션 메뉴를 클릭해보면 저희가 이전에 지정한 것처럼 DefaultApplication 만 제어할 수 있는 메뉴가 활성화 되어 사용 권한이 제한되는 것을 확인할 수 있습니다. 이처럼 Fine-grained 관리 보안은 각각의 자원을 사용자 별로 할당되고 할당된 자원 이외에 다른 어떤 자원도 접근할 수 없으므로 보안과 통제기능을 향상시키며 접근 레벨에 따라 관리자 역할을 고립 시킬 수 있습니다.

← https://127.0.0.1:9048/ibm/console/ 인증서 ... WebSphere Integrated Sol...

WebSphere. software

Defa

보기: 모든 태스크

시작

안내된 활동

서버

애플리케이션

애플리케이션 유형

WebSphere 엔터프라이즈 애플리케이션

비즈니스 레벨 애플리케이션

자산

글로벌 배치 설정

서비스

자원

보안

환경

시스템 관리

관리자 모니터링

셀=kr050578Node02Cell, 프로파일=AppSrv01

**엔터프라이즈 애플리케이션**

엔터프라이즈 애플리케이션

설치된 애플리케이션을 관리하려면 이 페이지를 사용하십시오. 단일 애플리케이션을 여러 서버로 배치시킬 수 있습니다.

환경 설정

시작 중지 업데이트 롤아웃 업데이트 파일 제거 내보내기 DDL 내보내기 파일 내보내기

선택 이름 애플리케이션 상태

다음 자원을 관리할 수 있습니다.

DefaultApplication

다음 자원을 모니터링할 수 있습니다.

ivtApp

query

총계 3

### 3) 참고 자료

1. 이 가이드는 IBM WAS v8.0 최초 사용자를 위한 기본 가이드입니다.
2. IBM WAS 자체에 아직 익숙하지 않으신 분들은 가급적 기본강좌인 '하나씩 쉽게 따라 해보는 IBM WAS v7' 강좌를 먼저 읽고 이 강좌를 읽으시는 것이 훨씬 이해에 됩니다.  
([http://www.websphere.pe.kr/xe/?mid=was\\_info\\_re&page=3&document\\_srl=800](http://www.websphere.pe.kr/xe/?mid=was_info_re&page=3&document_srl=800))
3. 가급적 IBM WAS v8.0 InfoCenter 의 해당 카테고리를 한 번 읽어보고 난 후에 작업하시기 바랍니다.
4. InfoCenter – Fine-grained administrative security  
([http://publib.boulder.ibm.com/infocenter/wasinfo/v8r0/topic/com.ibm.websphere.nd.doc/info/ae/ae/csec\\_fineg\\_admsec.html?resultof=%22%46%69%6e%65%2d%67%72%61%69%6e%65%64%22%20%22%61%64%6d%69%6e%69%73%74%72%61%74%69%76%65%22%20%22%61%64%6d%69%6e%69%73%74%72%22%20%22%73%65%63%75%72%69%74%79%22%20%22%73%65%63%75%72%22%20](http://publib.boulder.ibm.com/infocenter/wasinfo/v8r0/topic/com.ibm.websphere.nd.doc/info/ae/ae/csec_fineg_admsec.html?resultof=%22%46%69%6e%65%2d%67%72%61%69%6e%65%64%22%20%22%61%64%6d%69%6e%69%73%74%72%61%74%69%76%65%22%20%22%61%64%6d%69%6e%69%73%74%72%22%20%22%73%65%63%75%72%69%74%79%22%20%22%73%65%63%75%72%22%20))