WebSphere software

WebSphere Application Server v8.0

Fine-grained 관리 보안

(2011. 06.)

IBM SWG WebSphere CTP 이정운(juwlee@kr.ibm.com)

Create PDF files without this message by purchasing novaPDF printer (http://www.novapdf.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 보안 이란 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.

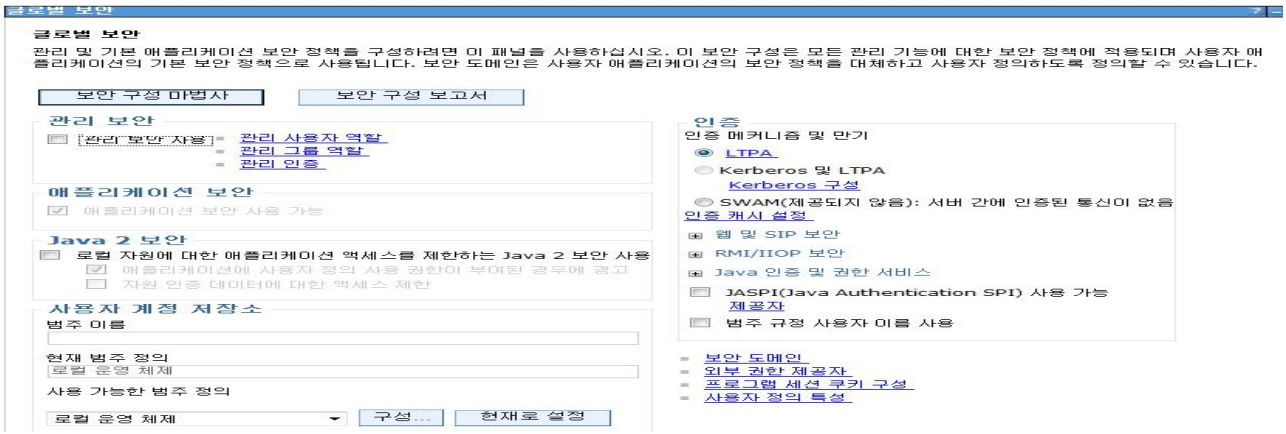
Table 1. Privileges required to access various administrative resources. The privileges required to access various administrative resources are shown in the following table:

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 Administrative roles.
Node, cluster	Add, delete	Cell-configurator

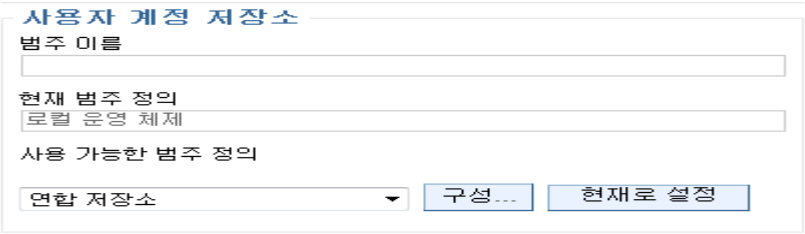
Create PDF files without this message by purchasing novaPDF printer (http://www.novapdf.com)

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.



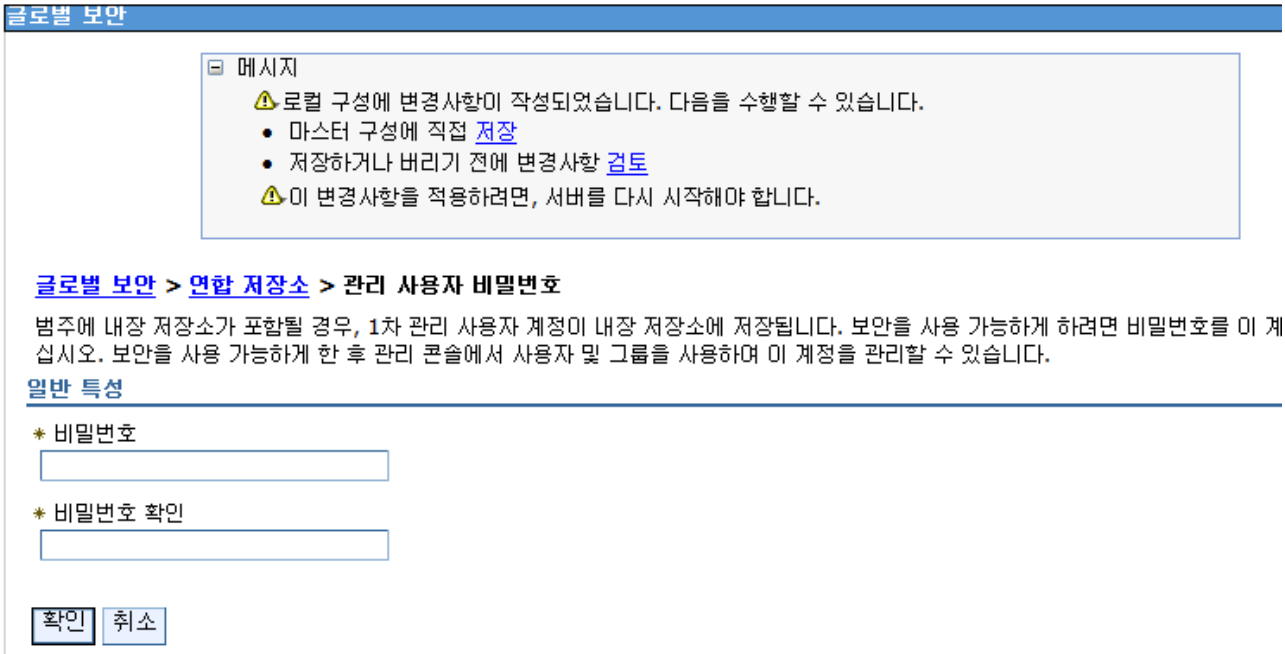
2. 사용자 계정 저장소의 사용 가능한 범주 정의에서 '연합 저장소' 를 선택하고 구성 버튼을 클릭합니다.



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

Create PDF files without this message by purchasing novaPDF printer (http://www.novapdf.com)

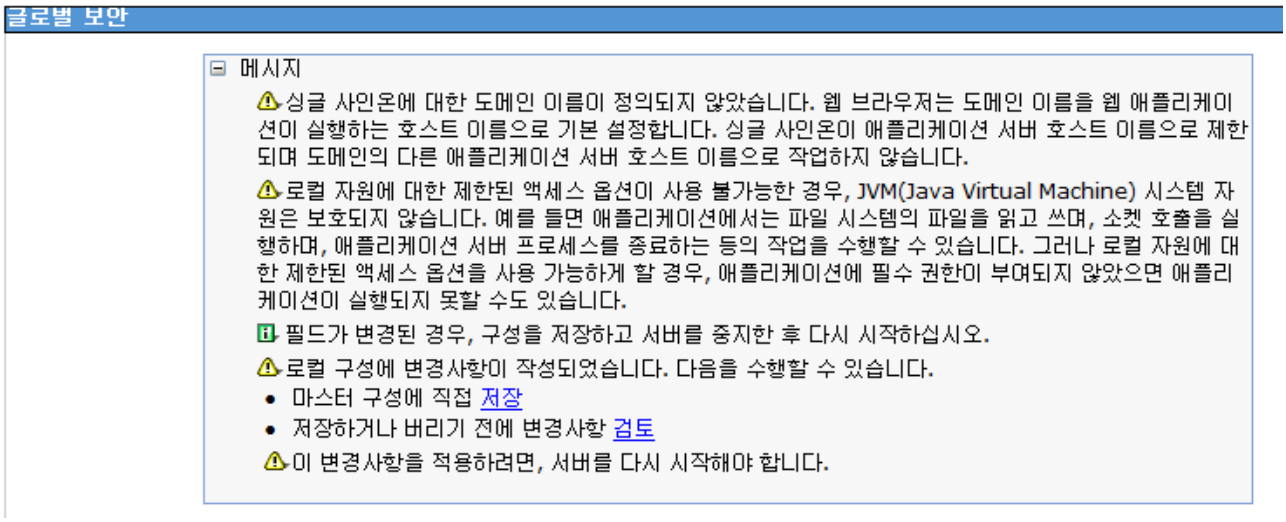
4. 확인을 클릭하면 바로 관리 사용자 비밀번호를 입력하는 메뉴가 나오는데 사용하고자 하는 비밀번호를 입력하고 확인을 클릭합니다.



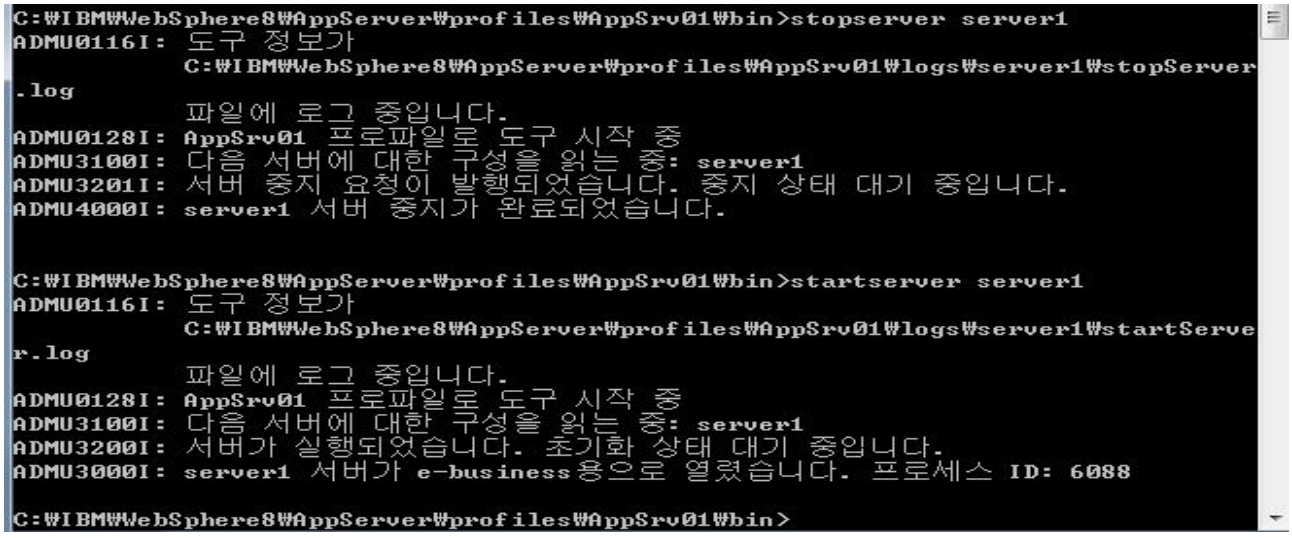
5. 다시 글로벌 보안 메뉴로 나오면 관리 보안 사용을 설정하시고(현재 이 강좌에서는 다루지 않을 예정이기 때문에 어플리케이션 보안은 해제) 사용 가능한 범주 정의에서 현재로 설정을 클릭한 후 다시 바로 적용을 클릭합니다.

Create PDF files without this message by purchasing novaPDF printer (http://www.novapdf.com)

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



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



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

Create PDF files without this message by purchasing novaPDF printer (http://www.novapdf.com)

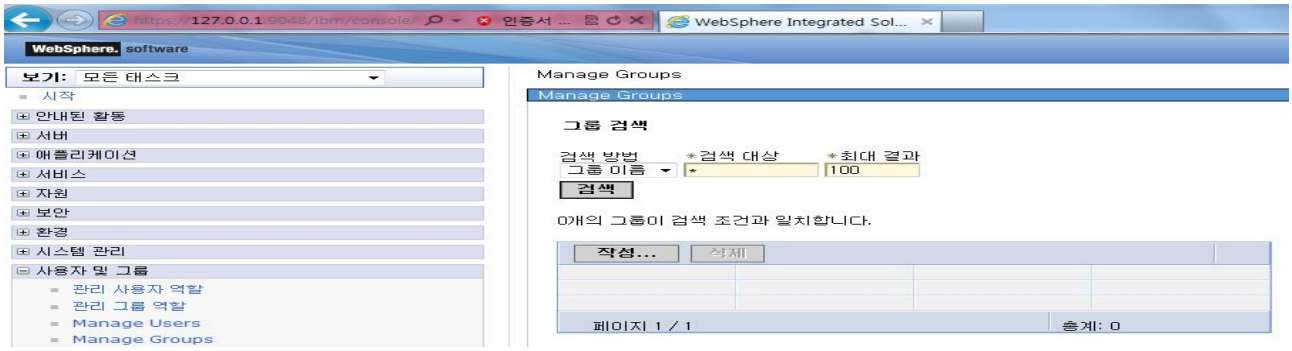
9. 그렇게 되면 하단처럼 관리콘솔 로그인 화면을 확인할 수 있으며 기존에 입력한 관리자 ID 와 비밀번호를 입력해야지만 해당 관리콘솔로 들어갈 수 있습니다.

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

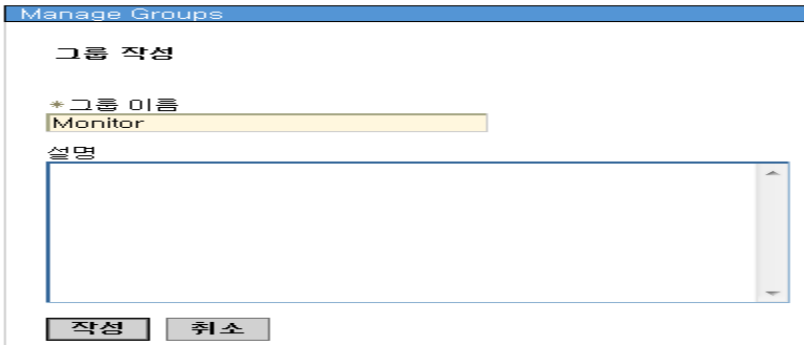
Create PDF files without this message by purchasing novaPDF printer (http://www.novapdf.com)

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.



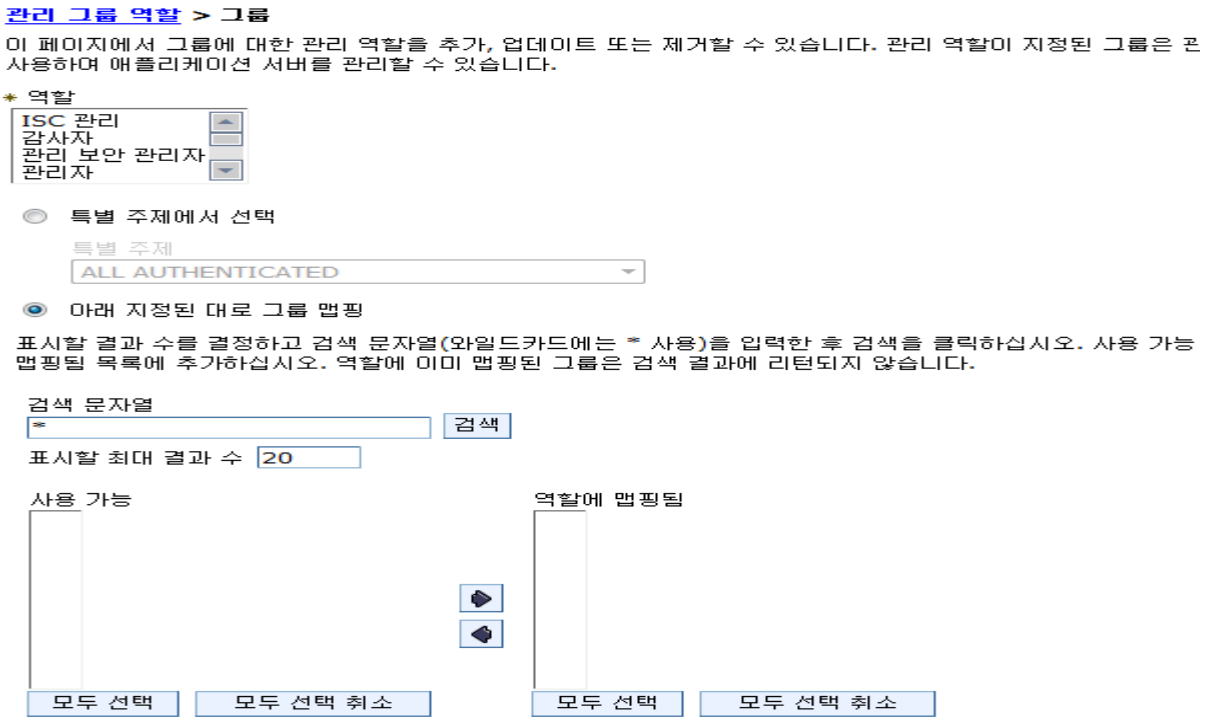
2. Manage Groups 메뉴에서 작성을 클릭한후 원하는 그룹 이름을 넣어 주고 작성을 누르면 하단과 같이 그룹 작성 메뉴가 나오는데 원하는 그룹을 하나 생성합니다.



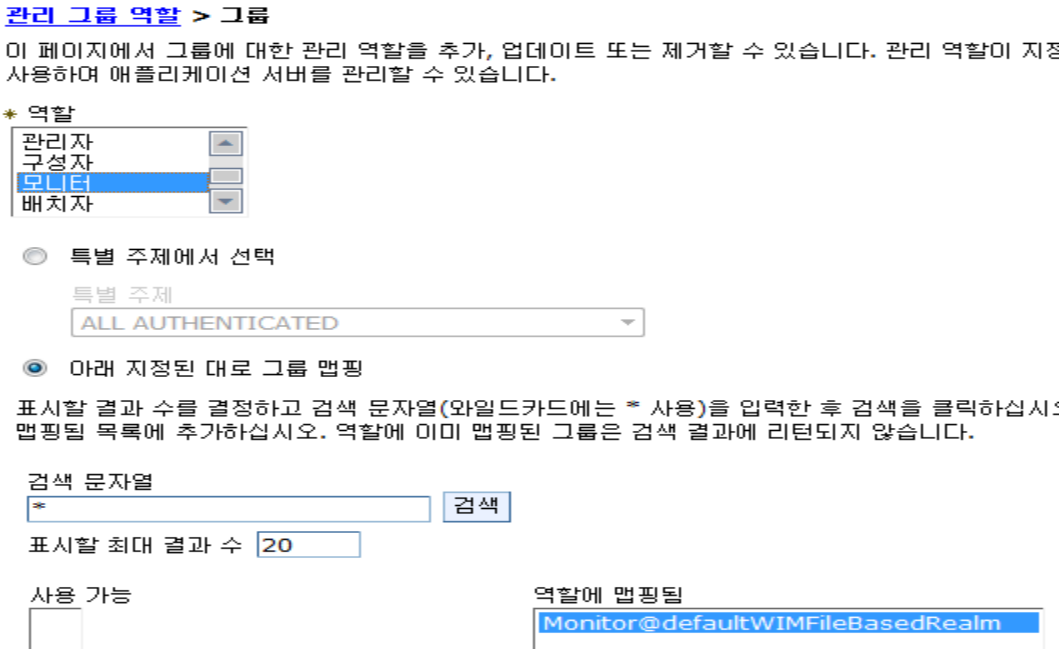
3. 생성된 그룹에 실제적으로 모니터링 권한을 배분하기 위하여 사용자 및 그룹 > 관리 그룹 역할 메뉴를 클릭하여 추가를 선택합니다.

Create PDF files without this message by purchasing novaPDF printer (http://www.novapdf.com)

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



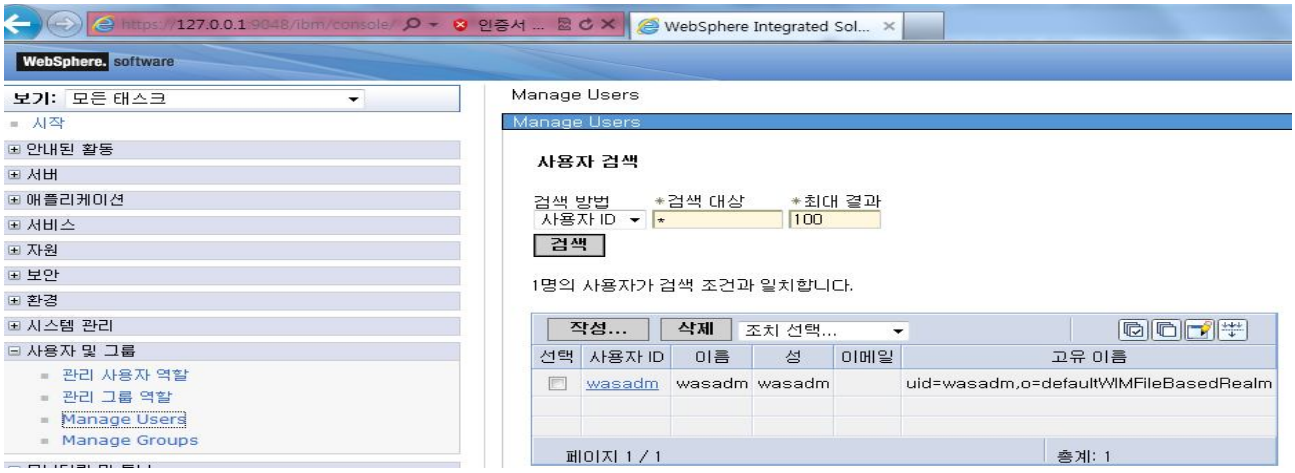
5. 관리 그룹 역할 설정 메뉴에서 모니터를 선택하고 검색을 클릭하면 방금 만들어둔 Monitor 그룹이 나타납니다. 이후 해당 그룹을 선택하고 화살표 버튼을 클릭하여 역할에 매핑시키고 해당 내용을 저장시킵니다.



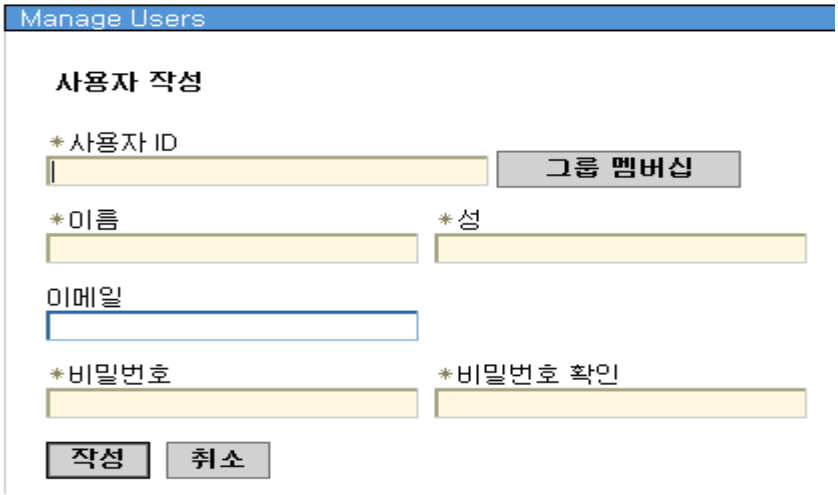
Create PDF files without this message by purchasing novaPDF printer (http://www.novapdf.com)

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

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



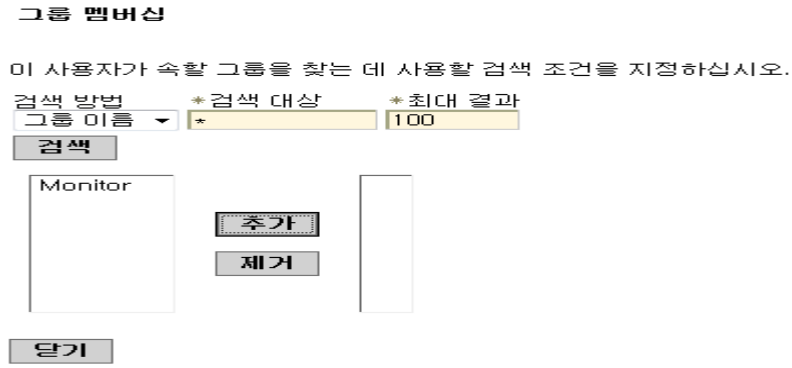
8. 사용자 작성 메뉴가 나오면 그룹 멤버십을 클릭합니다.



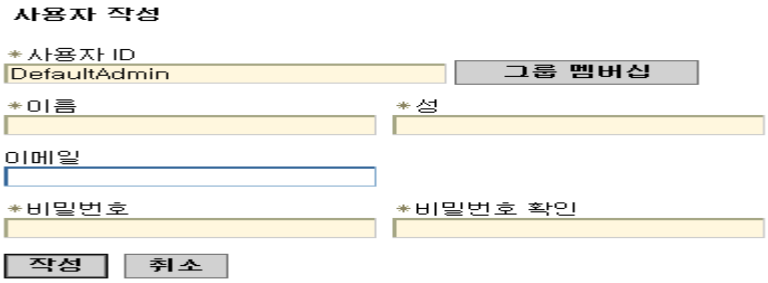
Create PDF files without this message by purchasing novaPDF printer (http://www.novapdf.com)

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

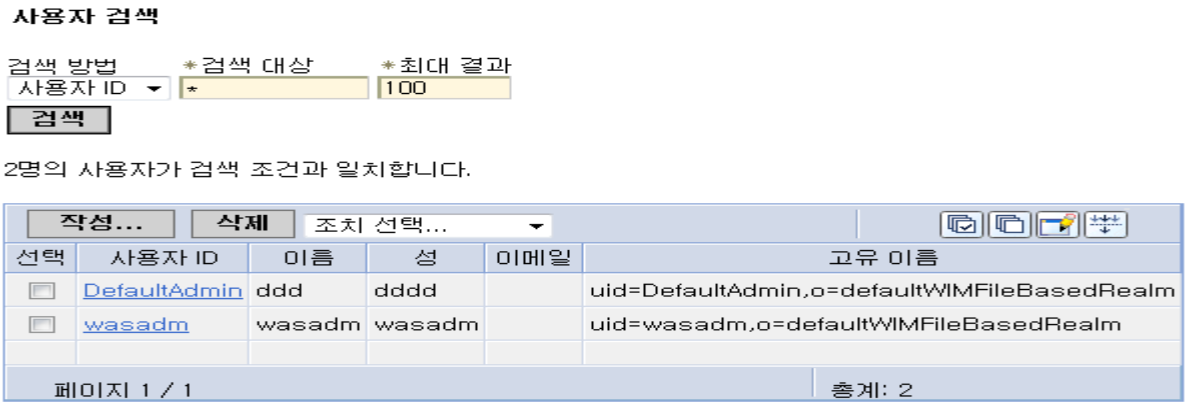
10. 미리 만들어둔 Monitor 그룹을 추가하고 닫기 버튼을 클릭합니다.



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

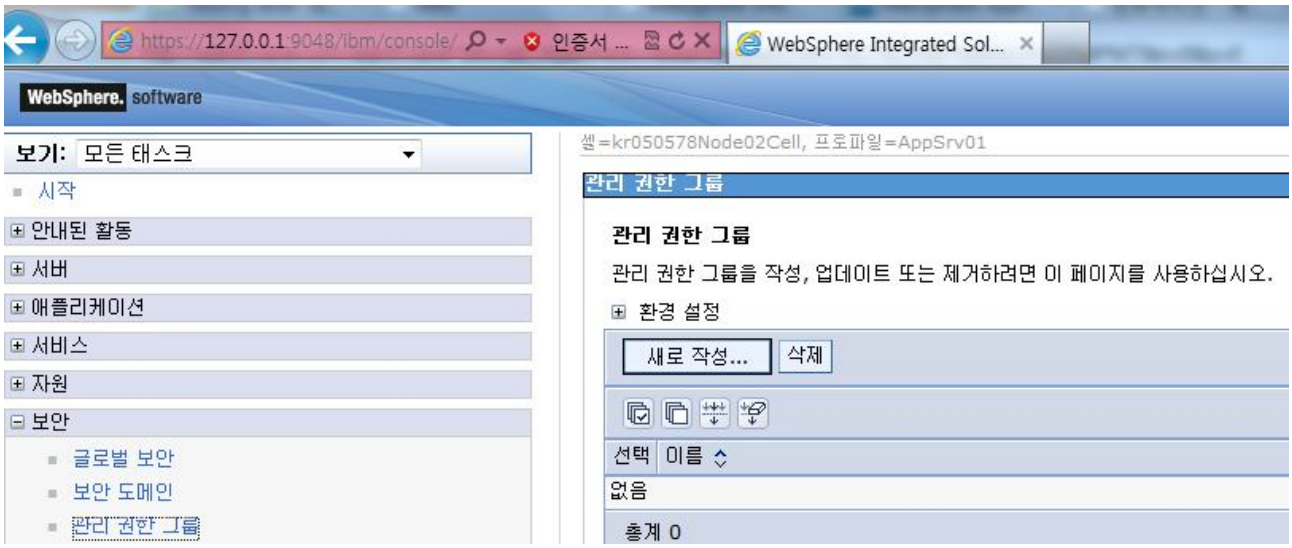


12. 그러면 다음과 같이 사용자 검색 리스트에 방금 입력한 사용자가 추가된 것을 확인할 수 있습니다.

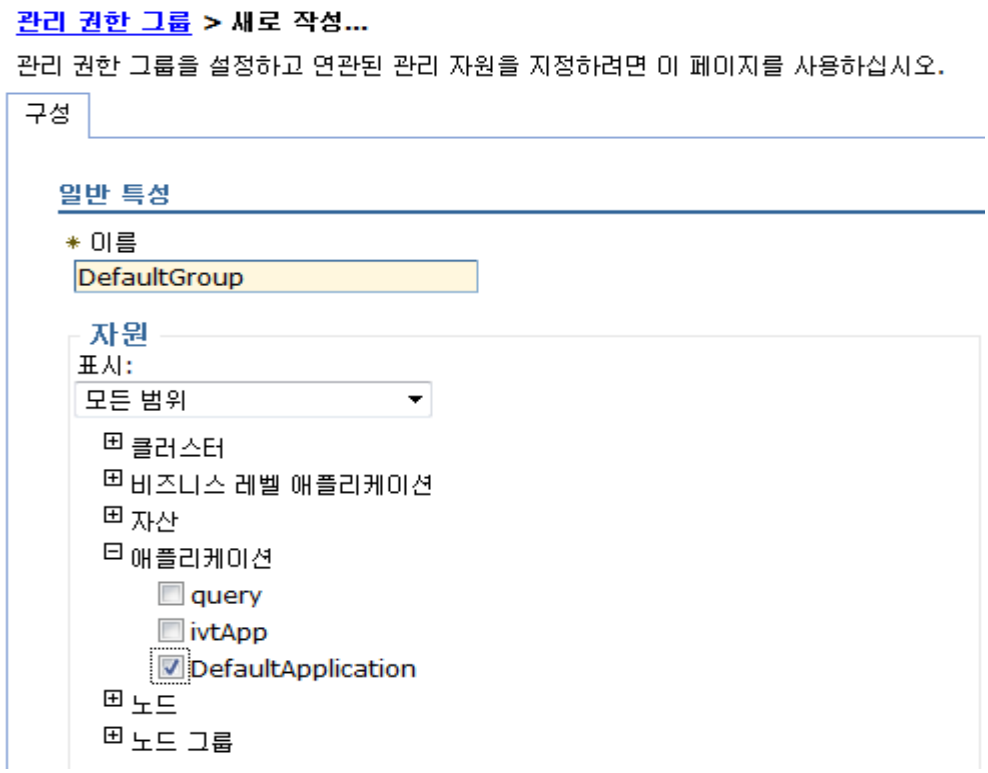


Create PDF files without this message by purchasing novaPDF printer (http://www.novapdf.com)

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.

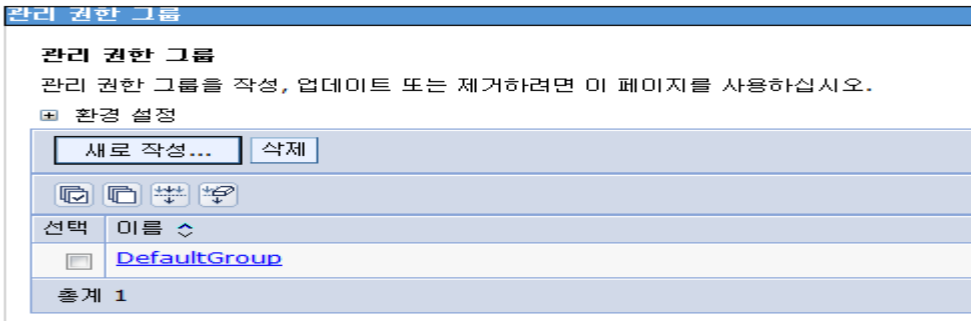


14. 여기서 중요한 것은 본인이 원하는 범위로 관리 권한 그룹을 만드시는 것 입니다. 하단에 표신된 자원에서 관리자 권한을 주려고 하는 범위만 찾아서 선택을 하면 됩니다. WAS ND 버전이 아니라 기본버전을 이용해서 테스트하는 것이므로 하단에는 샘플로 DefaultApplication 를 제어할 수 있는 권한만 할당을 하였습니다. 하지만 WAS ND 같은 경우에는 필요하다면 WAS 서버별로로 관리 권한을 제어할 수도 있습니다.

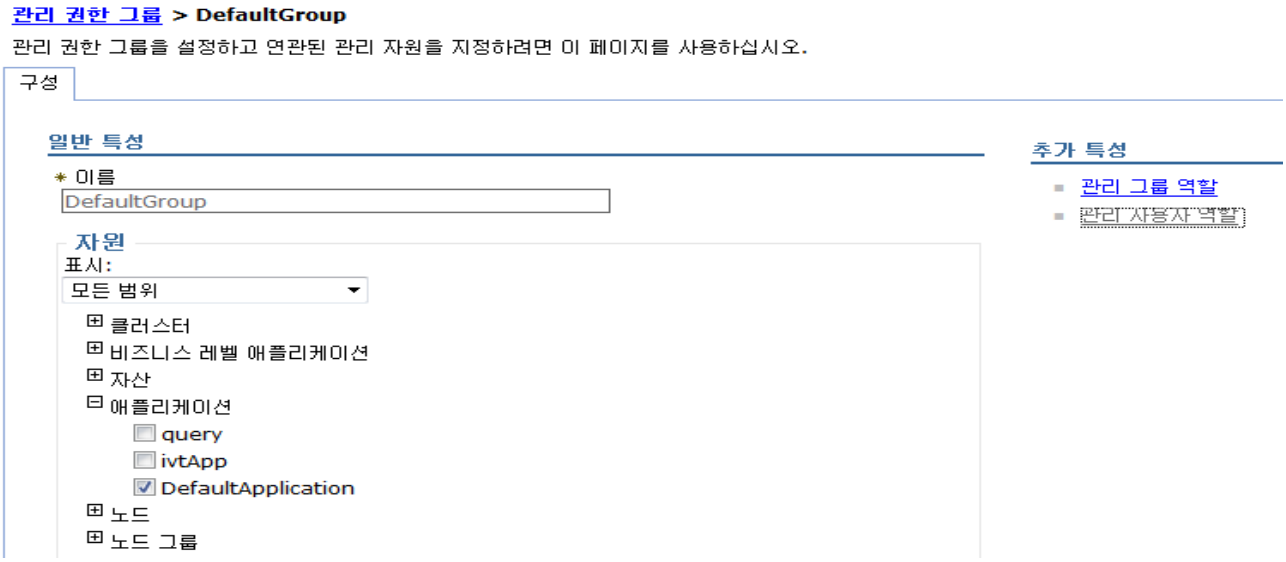


Create PDF files without this message by purchasing novaPDF printer (http://www.novapdf.com)

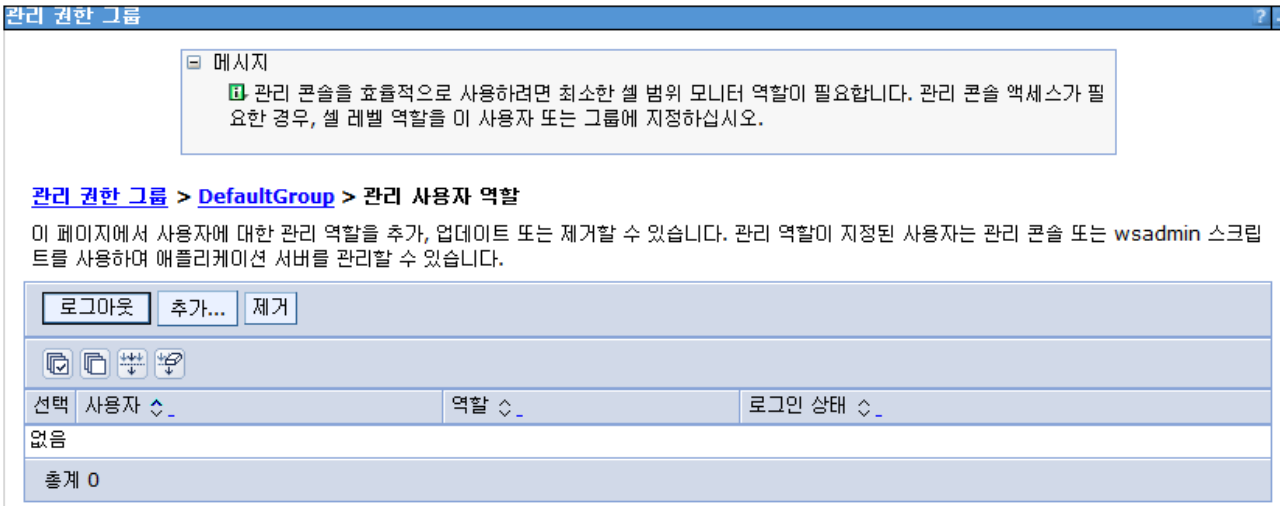
15. 위의 작업을 정상적으로 완료하셨다면 관리 권한 그룹 메뉴 리스트에 방금 만든 관리 권한 그룹을 생성할 수 있습니다. 다음으로 사용자를 할당하기 위하여 생성한 관리 권한 그룹을 클릭하시면 됩니다.



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

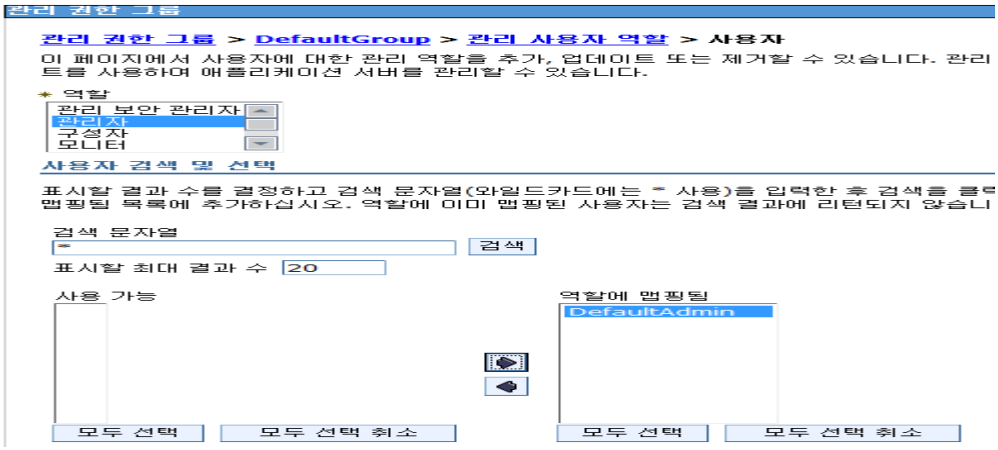


17. 관리 사용자 역할 메뉴가 나오면 추가 버튼을 클릭합니다.



Create PDF files without this message by purchasing novaPDF printer (http://www.novapdf.com)

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



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

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.

Create PDF files without this message by purchasing novaPDF printer (http://www.novapdf.com)

3) 참고 자료

1. 이 가이드는 IBM WAS v8.0 최초 사용자를 위한 기본 가이드 입니다.

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)

3. 가급적 IBM WAS v8.0 InfoCenter 의 해당 카테고리를 한 번 읽어보고 난 후에 작업하시기 바라겠습니다.

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)

Create PDF files without this message by purchasing novaPDF printer (http://www.novapdf.com)