$\mathsf{IBM}^{\texttt{®}}\mathsf{WebSphere}^{\texttt{®}}\mathsf{Application}$  Server V7 – LAB EXERCISE

# Fine-grained administrative security

What this exercise is about	1
_ab requirements	1
What you should be able to do	2
ntroduction	2
Exercise instructions	2
Part 1: Create administrative users	4
Part 2: Setup the administrative authorization groups	8
Part 3: Test the fine grained access control	12
What you did in this exercise	14

### What this exercise is about

The objective of this lab is to understand the new fine-grained access controls in the administrative console. This new functionality means that it is now possible to have different administrative console users have rights not just to the whole application server or cell, but to only specific parts of the application server or cell. For example, it is now possible to grant administrative console access for one user for a particular application server or node within a cell, but limit their access to different parts of the cell. This could be interesting in situations where multiple groups have applications within the same cell.

Previously, it was only possible to map an administrative user to a specific user role for the whole application server or cell. This meant that if an administrative user had access to any part of the environment, they had access to the whole environment.

This new functionality in WebSphere Application Server V7 is configured through the use of Administrative Authorization Groups. These groups map specific scopes or objects to console users and roles, thus allowing those users that role access to those specific objects. When the console users attempt to access other objects for which they do not have fine grained access configured, they only have the same access role level that was defined for them at the global level. That means that when new console users are created, they need a minimum of Monitor access at the cell or application server level. Then, the Administrative Authorization Groups can grant them additional rights to specific parts of the environment.

This exercise demonstrates this functionality using a stand-alone application server, and grants administrative access to two console users to different enterprise applications. But, the same concepts can be applied at the cell level, granting access to many different types of objects.

### Lab requirements

The list of system and software required for the student to complete the lab.

• A system that meets that requirements for running WebSphere Application Server V7, with approximately 500 MB of disk space for creating profiles

- The most current version of WebSphere Application Server V7
- An application server profiles with administrative security enabled, and with the administrative console and the default application deployed.

### What you should be able to do

At the end of this lab you should be able to:

- Create new administrative console users
- Map administrative console users to security roles
- Create and configure Administrative Authorization Groups
- Map Administrative Authorization Groups to both scopes and specific console users

### Introduction

WebSphere Application Server Version 7 introduces Administrative Authorization Groups. These groups allow administrators to define fine grained access within the administrative console. This lab demonstrates this new functionally with a simple example in a stand-alone application server. These same concepts can be applied to much more complex scenarios in a federated environment.

This lab is divided into the following parts:

#### Part 1: Create administrative users

This part creates two new administrative console users called adm1 and adm2. These users are mapped to the Monitor administrative user role.

#### Part 2: Setup the Administrative authorization groups

This section creates the Administrative authorization groups and maps them to specific objects. In this case, the group called App1 is mapped to the DefaultApplication and group App2 is mapped to the ivtApp. The groups then have administrative users and roles assigned to them. User adm1 is assigned administrator role access to the App1 group, and user adm2 is assigned administrator role access to the App2 group.

#### Part 3: Test the fine grained access

Using the administrative console and logging in as both adm1 and adm2, the fine grained access defined in Part 2 is verified.

### **Exercise instructions**

Instructions and subsequent documentation use symbolic references to directories which are listed as follows:

Reference Variable	Windows Location	
<was_home></was_home>	C:\Program Files\IBM\WebSphere\AppServer	Linux /opt/WebSphere/AppServer
		AIX /usr/WebSphere/AppServer
<temp></temp>	C:\temp	/tmp
<hostname></hostname>	Host name or host address for the machine where the profiles are being created	Host name or host address for the machine where the profiles are being created

### Part 1: Create administrative users

In order to configure and test fine grained access control in the administrative console, two administrative users are needed. These users are then assigned rights to different objects within the application server. Finally, the fact that the rights are limited to only certain object is tested. This part of the exercise creates the users and grants them monitor access to the application server.

- \_\_\_\_\_1. Start by ensuring that the application server is running.
- 2. Open an administrative console and verify that administrative security is enabled.

躞 Integrated Solutions Console - Mozilla Fi	refox	
Eile Edit View Go Bookmarks Iools	Fielb	¢
🔶 • 🖒 - 🎯 🛞 🕥 🗋 htt	ps://was7host01:9043/ibm/console/secure/securelogon.do	<u>⊖</u> ⊙ ∞ <u>C</u>
Integrated Solutions Console Welcome wide	mo Help   Logout	IDM.
View: All tasks	Cell=was7host01Node02Cell, Profile=Audit	Close page 🔺
Welcome	Global security	
Guided Activities     Guided Activi	Global security	
Gervers	Use this panel to configure administration and the default application security	policy. This security configuration applies to
	functions and is used as a default security policy for user applications. Security applications.	y domains can be defined to override and c
🕀 Resources	Security Configuration Wizard Security Configuration Report	
<ul> <li>Security</li> <li>Global security</li> <li>Security domains</li> <li>Administrative Authorization Groups</li> <li>SSL certificate and key management</li> <li>Security auditing</li> <li>Bus security</li> </ul>	Administrative security	Authentication Authentication mechanisms and expirat C LTPA C Kerberos and LTPA Kerberos configuration C SWAM (deprecated): No authentica
Environment	Enable application security	Authentication cache settings
🗄 System administration		Web and SIP security
	Java 2 security	
🗄 Monitoring and Tuning	Use Java 2 security to restrict application access to local resources	🗄 Java Authentication and Authorizatic
	Warn if applications are granted custom permissions	Use realm-qualified user names
	Restrict access to resource authentication data	
E UDDI	User account repository	<ul> <li>Security domains</li> <li>External authorization providers</li> </ul>
<		
Done		was7host01:9043 🛅 🥢

- \_\_\_\_a. If administrative security is not enabled, enable it (using a file-based user repository) and restart the server.
- \_\_\_\_3. In order to test the fine grained access control, create two new console users.
  - \_\_\_\_a. Using the administrative console, log in as user **wsdemo** with a password of **wsdemo**. Expand **Users and Groups** and click on **Manage Users**.
  - \_\_\_\_ b. Click **Search** to verify that the new users do not already exist.

lanage Users						
Search	Search for Users					
Search User I	Search by *Search for *Maximum results User ID 💽 * 100					
Search						
3 users	matched	the search c	riteria.			
Crea	ate	Delete Se	lect an action	n	•	◙▯≓₩
Select	User ID	First name	Last name	E-mail	Uniqu	ie Name
	<u>wsdemo</u>	wsdemo	wsdemo		uid=wsdemo,o=defaultWIMFileBasedRea	
Pa	ge 1 of 1				Total:	1

- \_\_\_\_ c. Click **Create** to add the new users.
- \_\_\_\_ d. Enter adm1 for the User ID. Create a First and Last name, and enter wsdemo for the passwords. Then click Create.

Manage Users	
Create a User	
*User ID	
adm1	Group Membership
*First name Admin1	*Last name User
E-mail	
* Password *****	*Confirm password *****
Create Cancel	

\_\_\_\_e. On the next screen, click **Create Like** in order to create the second admin user that will be needed.

Manage Us	ers
٠	The user was created successfully. adm1
	Create Like Close

\_\_\_\_ f. This returns you back to the Create a User screen with some of the fields already filled in. Change the User ID to adm2 and change the names if you want. Then enter wsdemo for the passwords and click Create.

Manage Users	
Create a User	
*User ID	
adm2	Group Membership
*First name Admin2	*Last name User
E-mail	
	]
* Password	*Confirm password
****	****
Create Cancel	

\_\_\_\_ g. Click **Close** since no more administrative users will be required.

\_\_\_\_4. Now that the administrative users have been created, they need to be mapped to Administrative user roles.

**NOTE:** In the next part of the exercise, **adm1** and **adm2** will have fine grained access configured so that they each have access to only specific enterprise applications. But, in order for these console users to be able to do anything useful, they also **need a minimum of Monitor role access** at the application server or cell level.

\_\_\_\_a. In the administrative console, under Users and Groups, click Administrative user roles.

\_\_\_ b. Click Add.

\_\_\_ c. Under Roles, scroll down and select Monitor. Next, click the Seach button to display the list of known administrative users. Select both adm1 and adm2 and click the right arrow to move them to the Mapped to role list.

Administrative user roles ? =
Administrative user roles > User
Use this page to add, update or to remove administrative roles to users. Assigning administrative roles to users enables them to administer application servers through the administrative console or through wsadmin scripting.
* Role(s) Configurator Deployer ISC Admins
Search and Select Users
Decide how many results to display, enter a search string (use * for wildcard), and click Search. Select users from the Available list and add them to the Mapped to role list. Users which have already been mapped to a role will not be returned in the search results. Search string * Maximum results to display 20
Available Wedemo Select All Deselect All Mapped to role Adm1 adm2 Select All Deselect All Deselect All
OK Reset Cancel

\_\_\_\_ d. Click **OK** and **Save** the changes.

### Part 2: Setup the administrative authorization groups

- 1. In the administrative console, click Administrative authorization groups under Security.
- 2. Click **New** to create a new **Administrative authorization groups**. These groups will be used to map the fine grained access to the users created in the previous Part of this exercise.
- 3. Enter **App1** for the **Name**. Under **Resources**, Expand all of the entries and the subentries. Under Business-level Applications, check the box for **DefaultApplication**.

General Properties
* Name App1
Resources
Show:
All scopes 💌
Clusters
none
Business-level applications
query
ivtApp
DefaultApplication
∃ <sub>Assets</sub>
- Node groups

- \_\_\_\_\_ 4. Click Apply.
- 5. On the right, under Additional Properties, click Administrative user roles.
- 6. Click **Add** to map the console user to the administrative authorization group.

7. Select the Administrator Role, then click Search to show all known users. Select adm1 and then click the right arrow to move the user ID from Available to Mapped to role.



Decide how many results to display, enter a search string (use \* for wildcard), and click Search. Select users from the Available list and add them to the Mapped to role list. Users which have already been mapped to a role will not be returned in the search results.



\_\_\_\_ 8. Click OK.

9. Return to the Administrative authorization groups page and repeat the steps above and create the **Administrative authorization group** called **App2**, and map it to ivtApp and the adm2 user.

pp2	
Resources	
Show:	
- Clusters	
ivtApp )	
DefaultApplication (App1)	
⊕ Nodes	
■ Node groups	

\_\_\_\_\_ 10. Make sure to map the adm2 user to the new authorization group.

Administrative authorization groups > <u>App2</u> > <u>Administrative user roles</u> > User

Use this page to add, update or to remove administrative roles to users. Assigning administrative roles to users enables them to administer application servers through the administrative console or through wsadmin scripting.

Admin Security Manager	
Administrator	
Configurator	
Deployer	-

Search and Select Users

Decide how many results to display, enter a search string (use \* for wildcard), and click Search. Select users from the Available list and add them to the Mapped to role list. Users which have already been mapped to a role will not be returned in the search results.

Search		
y 20		
6	Mapped to re	ole
	adm2	
4		
	·*-	
	y 20	y 20 Mapped to ro adm2

- \_\_\_\_\_ 11. Click **OK** and **Save** the changes.
- \_\_\_\_\_ 12. Now that the users have been created and appropriately configured, **restart** the application server so that the changes take effect.

### Part 3: Test the fine grained access control

Now that the new administrative console users have been created, and the administrative authorization groups have been added and mapped to two different applications, access by the users to the applications needs to be verified.

1. Open a new administrative console and log in as **adm1** with a password of **wsdemo**.

Integrated Solutions	Console
Log in to the co User ID:	nsole.
adm1	
Password:	
*****	
Log in	

2. Once logged in, browse through various parts of the console. Notice that the adm1 user has monitor rights to most areas. But, also notice that the adm1 user has administrative rights to only one of the business-level applications. Expand Applications > Application Types > Business-level applications to verify that user adm1 only has administrative authority on the DefaultApplication.

view: An tasks	Constant of the local division of the local			-			
Welcome	Busines	s-level applications		<u>t</u>			
Guided Activities	Busir	Business-level applications Use this page to manage business-level applications. A business-level application is a configuration that represents any artifacts that the application needs to run. Artifacts typically include Java(TM) Platform, Enterprise Edition (Java EE) applications or modules, shared libraries, data files, or other business-level applications.					
Servers	Use ti						
Applications	any a EE) a						
Application Types	Preferences						
<ul> <li>WebSphere enterprise applications</li> <li>Business-level applications</li> <li>Assets</li> </ul>	Sta	Start Stop Delete					
] Services							
] Resources	Selec	Name 💠	Description 🗇	Status 👲			
] Security	You	You can administer the following resources:					
] Environment		DefaultApplication		Ð			
System administration	You	You can monitor the following resources:					
] Monitoring and Tuning		IBMUTC		4			
] Troubleshooting		PlantsByWebSphere		<b>⊕</b>			
Service integration		SamplesGallery		<b>↔</b>			
IDDU 🗄		IvtApp		<b>₽</b>			
		query		•			
	Tota	16	10	No.			

**Note:** You will only see the IBMUTC, PlantsByWebSphere, and SamplesGallery applications in the list above if you chose to install the sample applications. If you do not see those applications listed, it is not an error. It just means that you did not install the samples.

3. At this point, log out from the console and log back in as **adm2** with the password of **wsdemo**.

4. Again, browse through various parts of the console and notice that this user only has monitor access. Go to the enterprise application list and notice that this user has administrative access to the ivtApp, but not DefaultApplication.

Integrated Solutions Console Welcome adm2			Help   Logout		
View: All tasks	Cell=was7ho	st01Node03Cell, Profile=fine	c		
• Welcome	Enterprise A	pplications			
Guided Activities     Guided Activi	Enterprise Applications				
E Servers	Use this p	age to manage installed application	ns. A single application can be deployed onto multiple servers.		
Applications					
<ul> <li>Application Types</li> <li>WebSphere enterprise applications</li> <li>Business-level applications</li> <li>Assets</li> </ul>	Start     Stop     Uninstall     Update     Rollout Update     Remove File     Export     Export DDL     Export F       Image: The start of t				
	You can	Name 🗘	Application Status Q		
		ivtApp	\$		
Gecurity	You can monitor the following resources:				
Environment	1.5.5.550	DefaultApplication			
E System administration		query			
Monitoring and Tuning	Total 3				
	. Star S				

\_\_\_\_\_5. Logout of the console.

## What you did in this exercise

In this lab you learned about the new fine grained access control in WebSphere Application Server Network Deployment V7. You created new administrative console users and mapped them to the new administrative authorization groups that were created. Finally, you verified that the access controls that were added did what was expected.

This page is left intentionally blank.