IBM® WebSphere® Application Server V7 – LAB EXERCISE

Fine-grained administrative security

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:

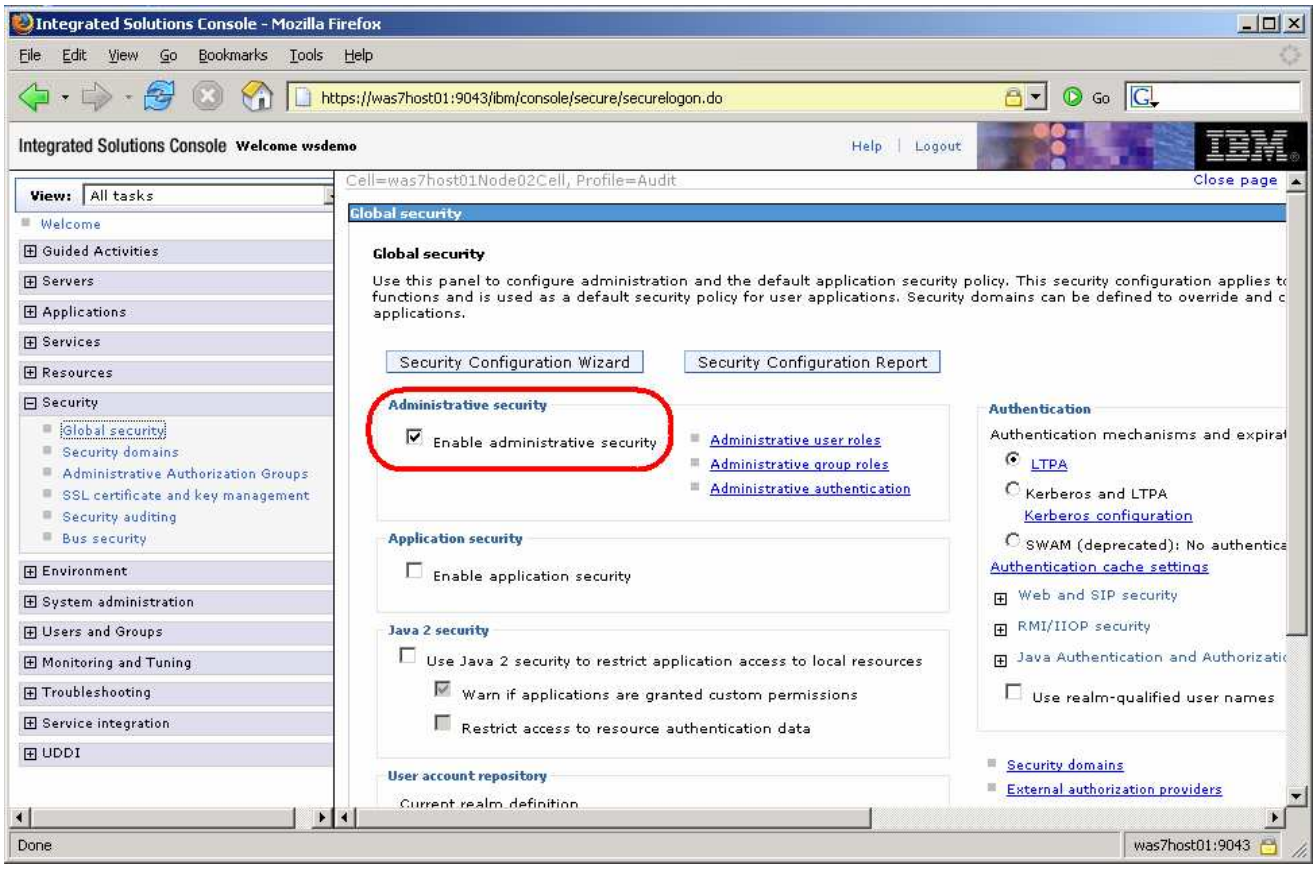
Reference Variable	Windows Location	Linux UNIX Location
<WAS_HOME>	C:\Program Files\IBM\WebSphere\AppServer	Linux /opt/WebSphere/AppServer AIX /usr/WebSphere/AppServer
<TEMP>	C:\temp	/tmp
<hostname>	Host name or host address for the machine where the profiles are being created	Host name or host address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

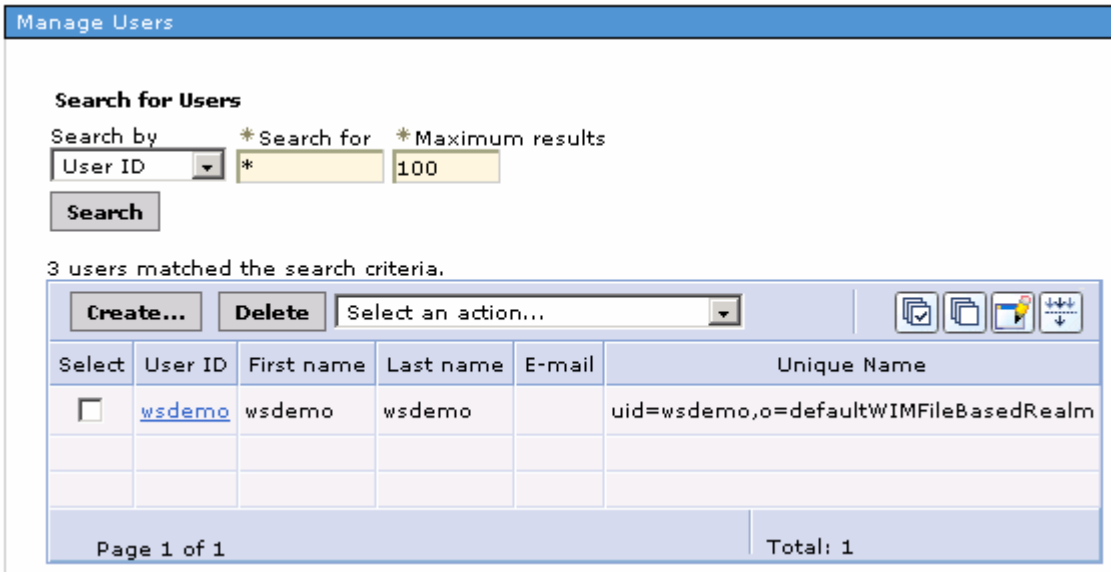


__ a. If administrative security is not enabled, enable it (using a file-based user repository) and restart the server.

____ 3. In order to test the fine grained access control, create two new console users.

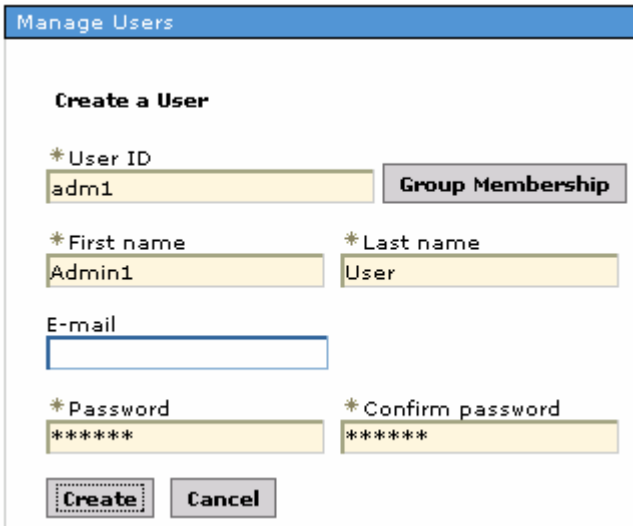
__ a. Using the administrative console, log in as user **wsdemo** with a password of **wsdemo**. Expand **Users and Group**s and click on **Manage Users**.

__ b. Click **Search** to verify that the new users do not already exist.



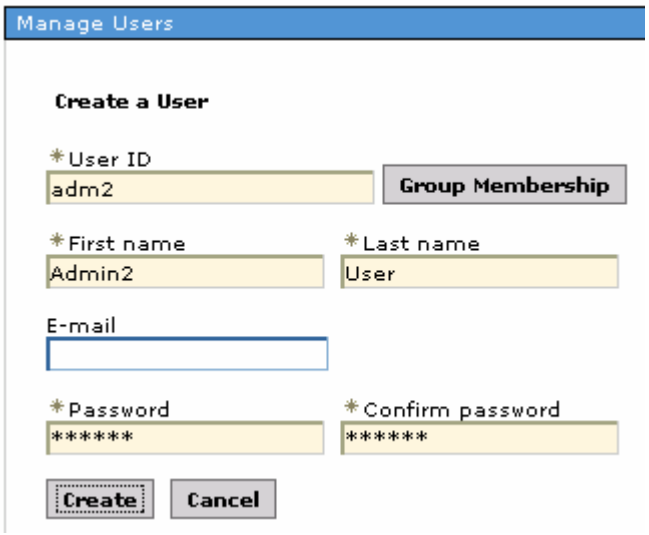
__ c. Click **Create** to add the new users.

__ d. Enter **adm1** for the **User** ID. Create a **First** and **Last name**, and enter **wsdemo** for the **passwords**. Then click **Create**.



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

__ 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**.



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

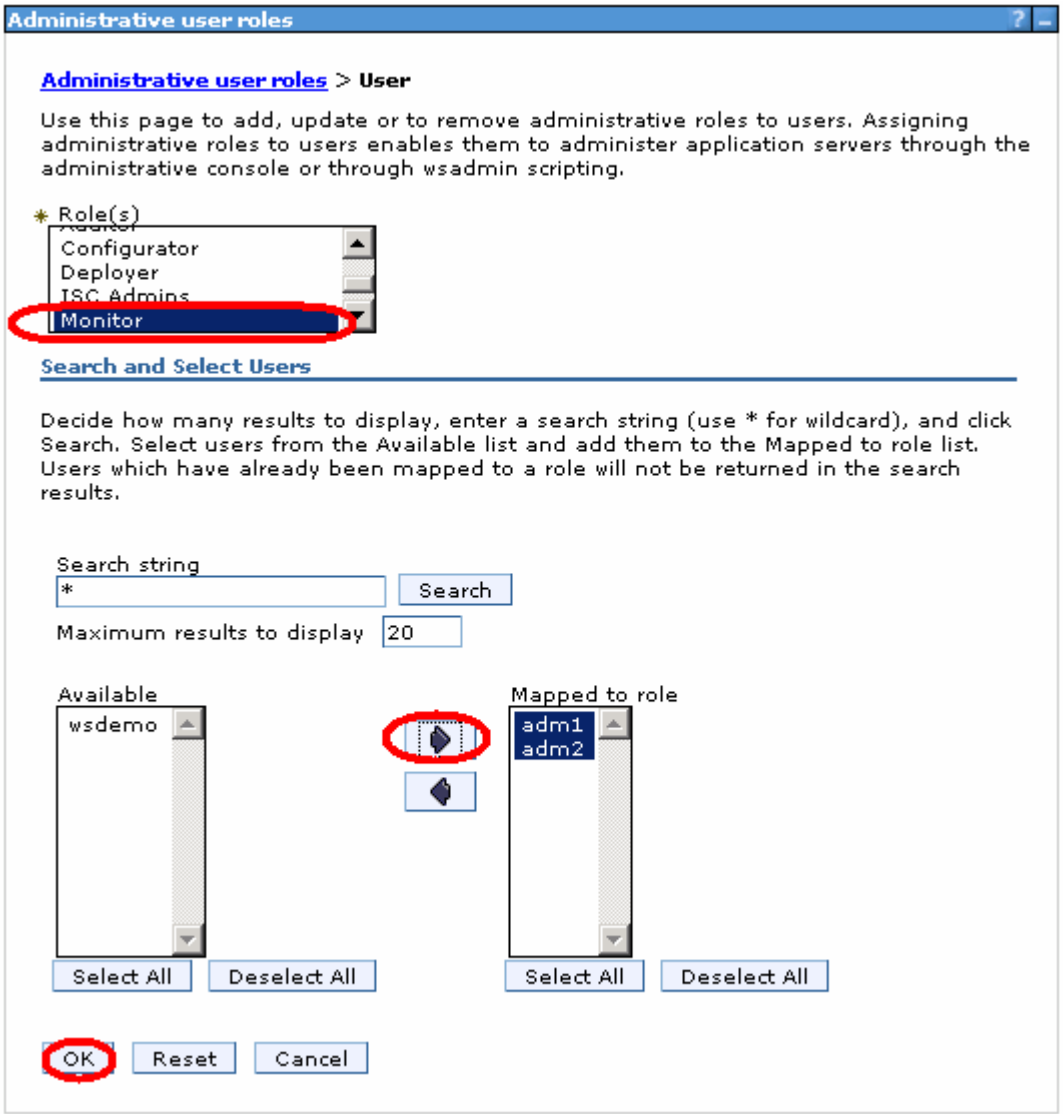
____ 4. Now that the administrative users have been created, they need to be mapped to Administrative user roles.

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.



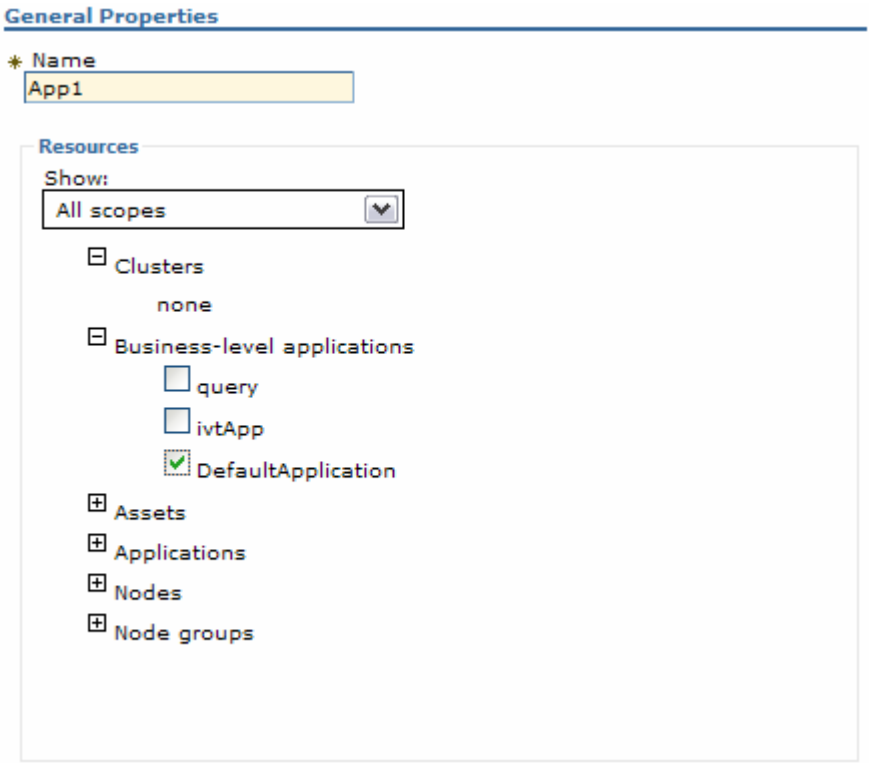
__ d. Click **OK** and **Save** the changes.

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**.

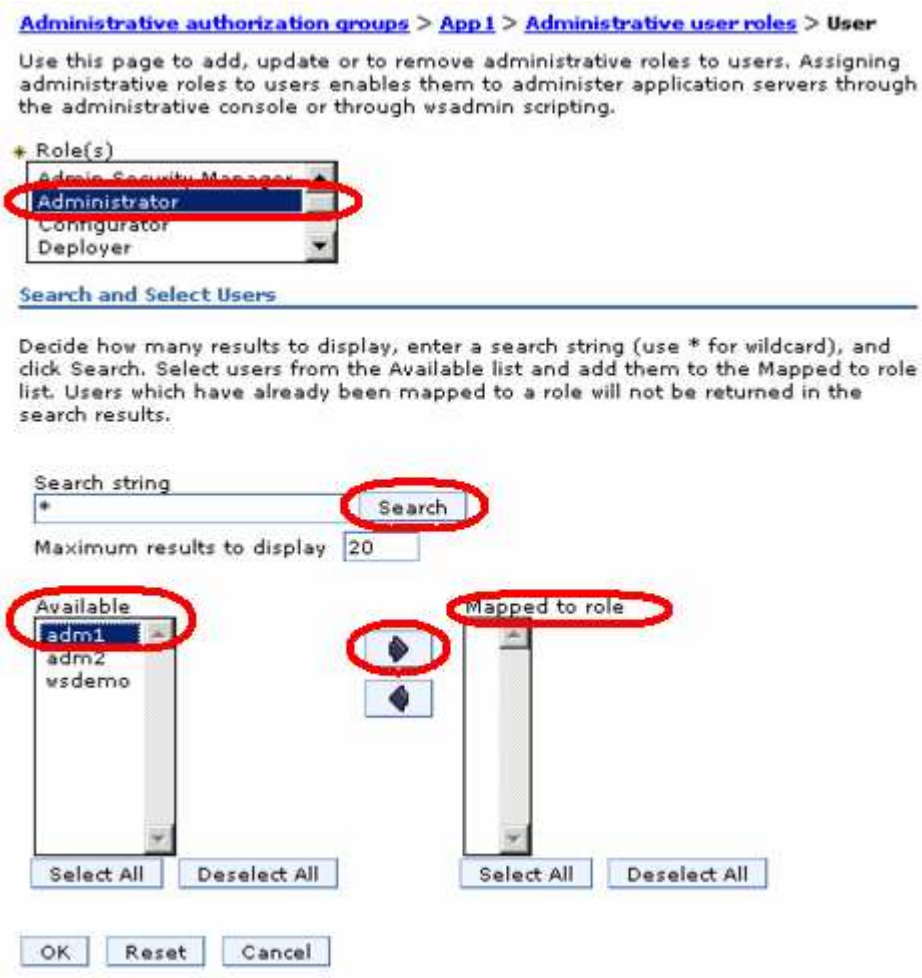


____ 4. Click **Apply**.

____ 5. On the right, under **Additional Properties**, click **Administrative user roles**.

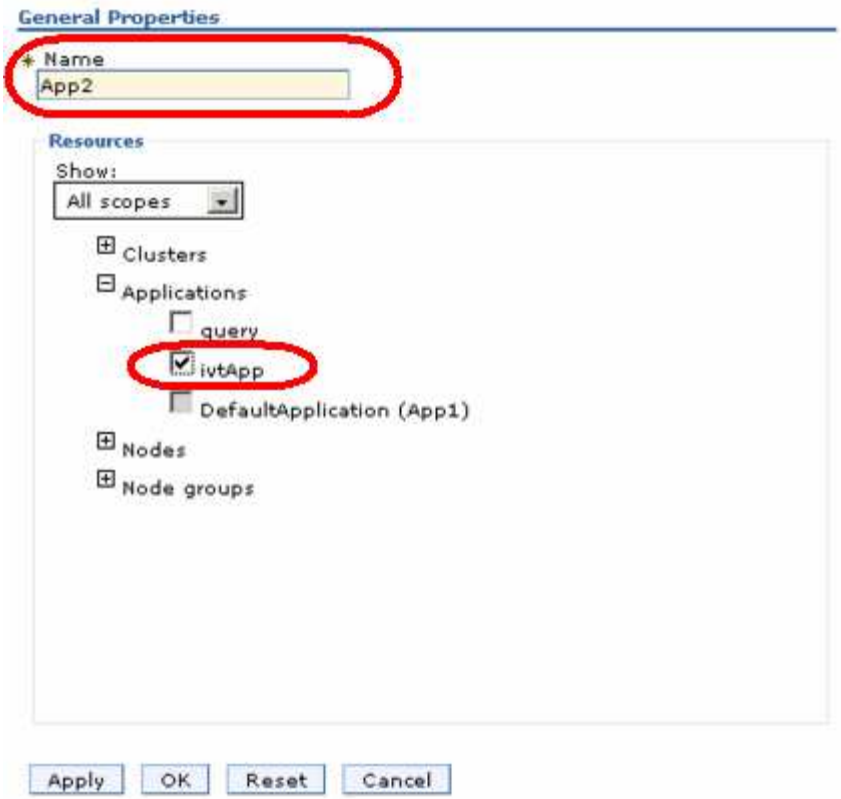
____ 6. Click **Add** to map the console user to the administrative authorization group.

____ 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**.

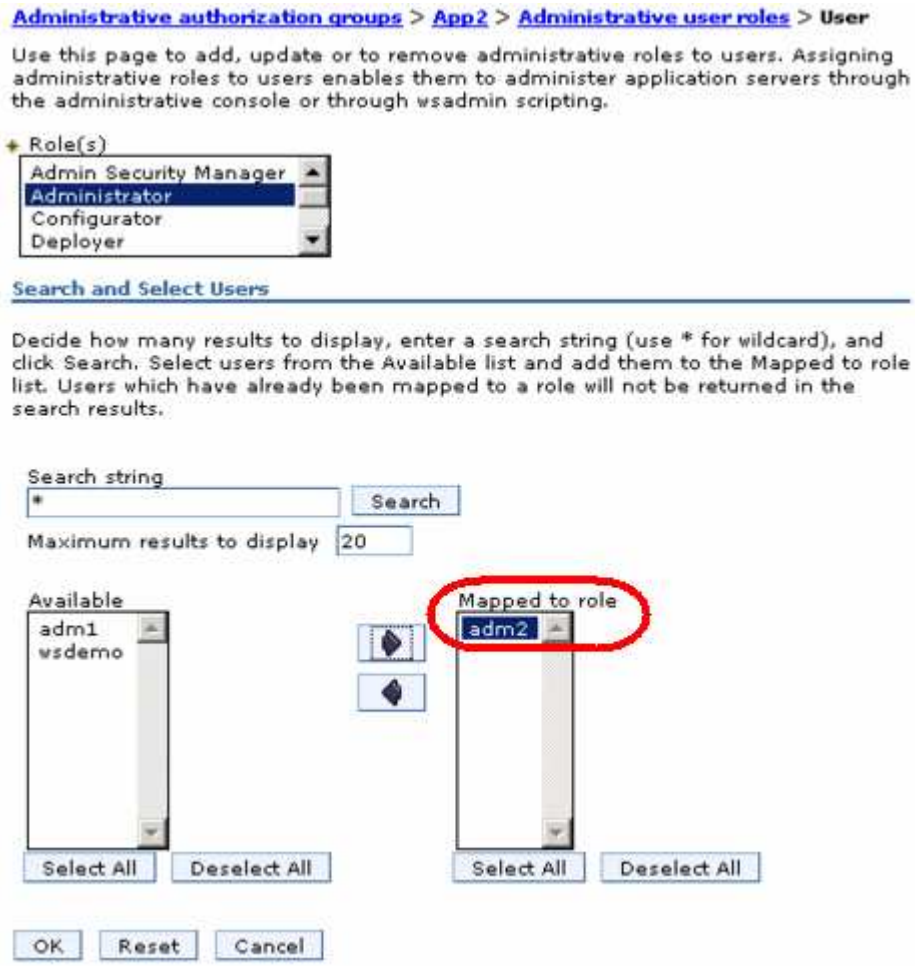


____ 8. Click **OK**.

____ 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.



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



____ 11. Click **OK** and **Save** the changes.

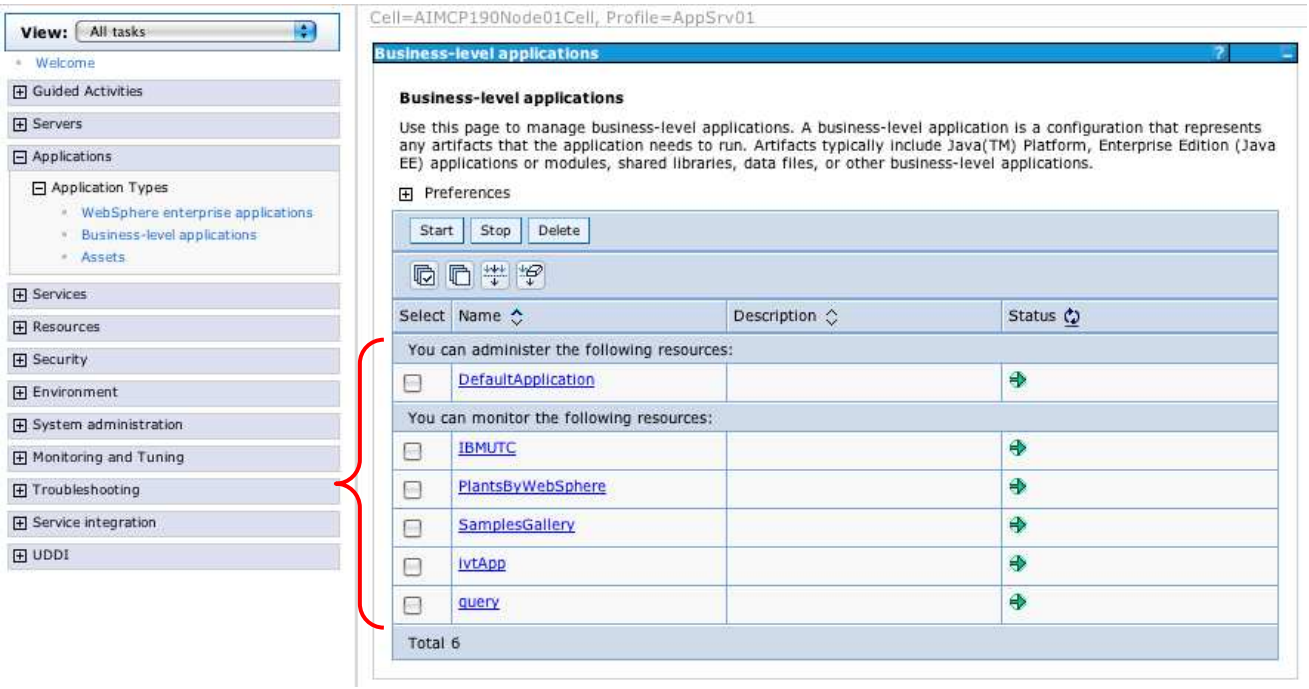
____ 12. Now that the users have been created and appropriately configured, **restart** the application server so that the changes take effect.

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**.

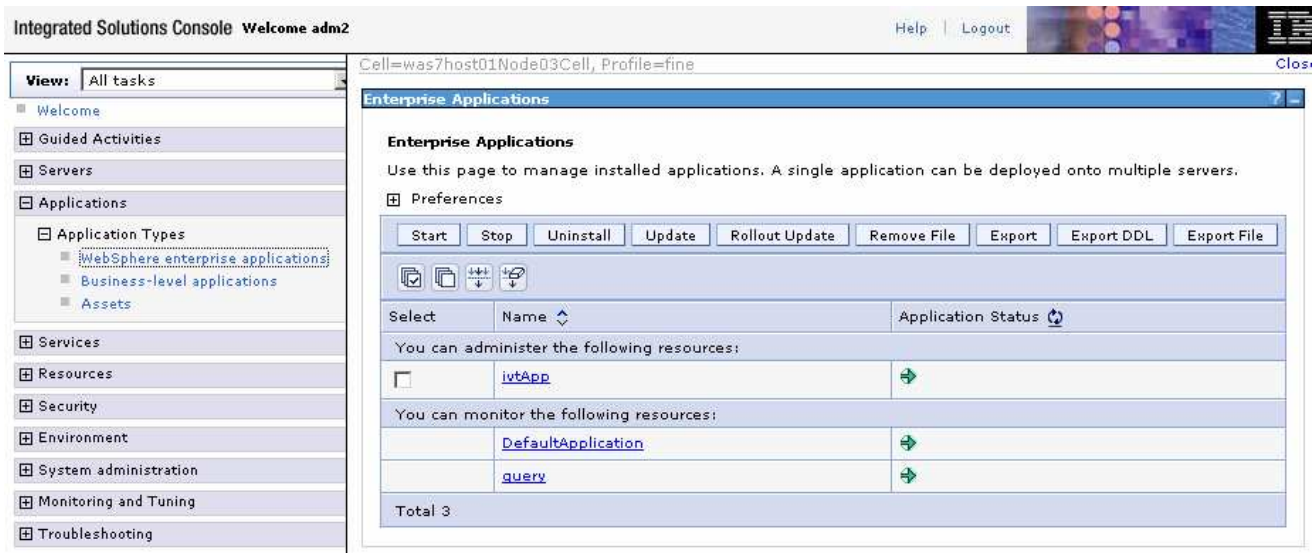
____ 2. Once logged in, browse through various parts of the console. Notice that the **adm1** user has **monitor** rights to most areas. But, also notice that the **adm1** user has **administrative** rights to only one of the business-level applications. Expand **Applications > Application Types > Business-level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



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.



____ 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.