Lab 12 – Configuring WebSphere Security

At the end of this exercise, you should be able to:
• Enable WebSphere security
• Configure administrative security by configuring access to administrative functions
• Configure fine-grained administrative security

Section 1: Verify administrative security

This exercise configures security access to the administrative tools. Before any security access takes effect, administrative security must be enabled, which happens by default during the creation of a profile.

Section 2: Defining WebSphere administrative console users

When WebSphere Application Server is installed and profiles are created, administrative security is enabled by default. Initially, the only user with access to the administrative console is the primary user that is specified during the profile creation, which is the wasadmin user. Initially, in the case of these labs, the only user that can access the administrative console is wasadmin. In a real environment, it is desirable to have multiple administrative users and possibly have different rights for each user.

Section 3: Authenticate to the WebSphere administrative console and test mapped users

In this part of the exercise, access to the administrative console is granted only to correctly mapped users. Depending on the role to which they are mapped, the administrative console allows those users to complete only certain functions.

Section 4: Enabling fine-grained control

Now that users with different types of access to the administrative console exist, it might be interesting to control the access more specifically. For example, in the following example the exercise creates two new administrative users. The first, PlantsAppAdmin, is configured to have rights only on the PlantsByWebSphere application. The second, DefaultAppAdmin, is configured to have rights only on the DefaultApplication.

By creating this setup, the exercise demonstrates how fine-grained access controls can be granted to administrative users. These types of controls can be granted on many different types of objects, not just applications.

The fine-grained access is defined by mapping administrative authorization groups to administrative console users. The administrative authorization groups point at specific scopes or objects. When an administrative user attempts to access an object and does not have global access, the access that the administrative authorization groups define for the object is checked.

The user with fine-grained administrative access requires a minimum of global Monitor access.

Section 5: Test the fine-grained access

Now that the new administrative console users are created, and the administrative authorization groups are added and mapped to the applications, access by the users to the applications must be verified.

Section 6: Examine security domains

In the previous section, fine-grained access control was configured, thus allowing administrators the ability to have better control over which administrators have access to which portions of a cell.

Security domains allow an administrator to define alternative security configurations for a cell. Historically, security configurations were defined only at a cell level, which meant that if something such as a user registry was defined within a cell, it applied to the whole cell. There was no ability to define an alternative configuration for specific sections of a cell.