



# Servidores de aplicaciones

## Sesión 3: Gestión de seguridad



# Índice

- Gestión de seguridad en el sistema
- Gestión de usuarios y grupos
- Seguridad en una aplicación



# Seguridad en WebLogic

- WebLogic dispone de un mecanismo de gestión de seguridad por defecto
- Mecanismo de *autenticación* (el usuario o aplicación son quienes dicen ser?) y *autorización* (el usuario en cuestión tiene permiso para realizar una determinada acción?)
- Podemos usar el mecanismo por defecto, pero normalmente se suelen usar sistemas externos (LDAP, el propio sistema operativo, etc.)
- Estos sistemas se denominan *providers*



## Proceso para proporcionar seguridad a una aplicación

- La recomendación para introducir seguridad en una aplicación es seguir estos pasos:
  - Crear restricciones de seguridad en la aplicación (mediante el descriptor de despliegue), independientemente del servidor donde vayamos a desplegar. Independencia del servidor
  - El servidor dispondrá de usuarios, grupos, roles (principales)
  - Mapear restricciones de seguridad con principales en el servidor. En WebLogic se consigue mediante un descriptor adicional (*weblogic.xml*)



# Gestión de seguridad en WebLogic

- WebLogic define *realms* para la seguridad (conjunto de usuarios, grupos, roles y políticas de seguridad)
- Los recursos a los que se puede imponer políticas de seguridad son: aplicaciones (web, EJB, jar, etc.), JDBC, JNDI, EIS, JMS
- Pinchamos en *Security Realms* y nos aparecerá un *realm* por defecto



# Realms

## Summary of Security Realms

A security realm is a container for the mechanisms--including users, groups, security roles, security policies, and security providers--that are used to protect WebLogic resources. You can have multiple security realms in a WebLogic Server domain, but only one can be set as the default (active) realm.

This Security Realms page lists each security realm that has been configured in this WebLogic Server domain. Click the name of the realm to explore and configure that realm.

[Customize this table](#)

### Realms

Click the **Lock & Edit** button in the Change Center to activate all the buttons on this page.

New	Delete	Showing 1 - 1 of 1 Previous   Next	
<input type="checkbox"/>	Name	Default Realm	
<input type="checkbox"/>	myrealm	true	
New	Delete	Showing 1 - 1 of 1 Previous   Next	



# Pinchamos en *myrealm*


Configuration | **Users and Groups** | Roles and Policies | Credential Mappings | Providers | Migration

**General** | User Lockout | Performance


Click the **Lock & Edit** button in the Change Center to modify the settings on this page.


This page allows you to define the general configuration of this security realm.


**Name:** myrealm

 **Check Roles and Policies:** Web applications and EJBs protected in DD ▾

**On Future Redeploys:** Initialize roles and policies from DD ▾

 ☐ **Ignore Deploy Credential Mapping**

 **Security Model:** DD Only ▾

 ☒ **Combined Role Mapping Enabled**

Click the **Lock & Edit** button in the Change Center to modify the settings on this page.




# User Lockout


Configuration **Users and Groups** Roles and Policies Credential Mappings Providers Migration


General **User Lockout** Performance


Click the **Lock & Edit** button in the Change Center to modify the settings on this page.


Password guessing is a common type of security attack. In this type of attack, a hacker attempts to log in to a computer using various combinations of usernames and passwords. Weblogic Server provides a set of attributes to protect user accounts from intruders. This page allows us to define how user lockouts will be handled in this security realm.


 ☒ **Lockout Enabled**

 **Lockout Threshold:**

 **Lockout Duration:**

 **Lockout Reset Duration:**

 **Lockout Cache Size:**

 **Lockout GC Threshold:**

Click the **Lock & Edit** button in the Change Center to modify the settings on this page.





# Usuarios

- Personas o programas
- Único en el sistema y se identifica mediante contraseña
- No existe *guest* (se puede definir, pero se desaconseja)
- Pinchamos en la solapa *Users and Groups*



# Usuarios

**Settings for myrealm**

[Configuration](#) [Users and Groups](#) [Roles and Policies](#) [Credential Mappings](#) [Providers](#) [Migration](#)

**Users** | [Groups](#)

This page displays information about each user that has been configured in this security realm.

[Customize this table](#)

**Users**

[New](#) [Delete](#)

Showing 1 - 2 of 2 [Previous](#) | [Next](#)

<input type="checkbox"/>	Name	Description	Provider
<input type="checkbox"/>	miguel	Miguelito	DefaultAuthenticator
<input type="checkbox"/>	system	El usuario del sistema por defecto	DefaultAuthenticator

[New](#) [Delete](#)

Showing 1 - 2 of 2 [Previous](#) | [Next](#)



# Nuevo usuario

**Create a New User**

OK | Cancel

**User Properties**  
The following properties will be used to identify your new User.

What would you like to name your new User?

**Name:**

How would you like to describe the new User?

**Description:**

Please choose a provider for the user.

**Provider:**

The password is associated with the login name for the new User.

**Password:**

**Confirm Password:**

OK | Cancel



# Grupos

- Agrupación de usuarios con alguna característica común
- Un usuario puede pertenecer a más de un grupo
- Al asignar una política o rol a un grupo, se le asigna a todos los miembros del grupo
- Existen 6 grupos por defecto
  - *Administrators*: administración del dominio
  - *AppTesters*: prueban aplicaciones
  - *Deployers*: despliegue de aplicaciones
  - *Monitors*: monitorización del sistema
  - *Operators*: operación con los servidores



# Grupos

[Configuration](#) [Users and Groups](#) [Roles and Policies](#) [Credential Mappings](#) [Providers](#) [Migration](#)

[Users](#) **Groups**

This page displays information about each group that has been configured in this security realm.

[Customize this table](#)

**Groups**

[New](#) [Delete](#) Showing 1 - 6 of 6 [Previous](#) | [Next](#)

<input type="checkbox"/>	Name	Description	Provider
<input type="checkbox"/>	<a href="#">Administrators</a>	Administrators can view and modify all resource attributes and start and stop servers.	DefaultAuthenticator
<input type="checkbox"/>	<a href="#">AppTesters</a>	AppTesters group.	DefaultAuthenticator
<input type="checkbox"/>	<a href="#">Deployers</a>	Deployers can view all resource attributes and deploy applications.	DefaultAuthenticator
<input type="checkbox"/>	<a href="#">managers</a>	Los gestores	DefaultAuthenticator
<input type="checkbox"/>	<a href="#">Monitors</a>	Monitors can view and modify all resource attributes and perform operations not restricted by roles.	DefaultAuthenticator
<input type="checkbox"/>	<a href="#">Operators</a>	Operators can view and modify all resource attributes and perform server lifecycle operations.	DefaultAuthenticator

[New](#) [Delete](#) Showing 1 - 6 of 6 [Previous](#) | [Next](#)



# Nuevo grupo

**Create a New Group**

OK | Cancel

**Group Properties**  
The following properties will be used to identify your new Group.

What would you like to name your new Group?

**Name:**

How would you like to describe the new Group?

**Description:**

Please choose a provider for the group.

**Provider:**

OK | Cancel




# Herencia del grupo

Settings for migrupo

General Membership

Save

Use this page to add groups to other groups.

 **Parent Groups:**

Available		Chosen
Administrators	➔	
AppTesters		
Deployers	➔	
Monitors		

Save



# Asignar usuario a grupo

- Lista de usuarios -> seleccionamos usuario -> solapa *Groups*

General Passwords Groups

Save

Use this page to configure group membership for this user.

Parent Groups:

Available		Chosen
Administrators	→	managers
AppTesters	←	
Deployers		
Monitors		

Save





## Gestión de roles

- Un rol es una asociación entre usuarios/grupos de manera dinámica: depende de cómo se esté accediendo se tendrá acceso o no (tiempo y forma de acceso, por ejemplo)
- Disponemos de dos tipos de roles: los locales (*scoped*) que se asignan a un determinado recurso (JDBC, JMS, etc.) y los globales que se suelen asignar a un grupo
- Asociado a un rol nos encontramos con la política de seguridad (*policy*)



## Gestión de roles: políticas de seguridad

- Una política de seguridad es una asignación con un determinado recurso
- Puede ser simplemente una asignación de un grupo a un recurso (el grupo *administrator* tiene permiso para acceder a cualquier recurso JDBC) o restricciones mucho más elaboradas (un determinado usuario tiene permiso para acceder al recurso *miDS* del árbol JNDI desde las 9:00 hasta las 17:00)



## Descripción de la seguridad en el descriptor

- Disponemos de dos ficheros para definir la seguridad: web.xml y weblogic.xml
- Para restringir el acceso a un recurso
  - Declarar un patrón URL en el fichero web.xml
  - Declarar un rol
  - Asociar el patrón con el rol
  - Mapear el rol con usuarios o grupos en weblogic.xml



# Web.xml

```
<?xml version="1.0" ?>
<!DOCTYPE web-app PUBLIC "-//Sun Microsystems, Inc.//DTD Web Application 2.3//EN"
"http://java.sun.com/dtd/web-app_2_3.dtd">
<web-app>
  <servlet>
    <servlet-name>AbsenceReport</servlet-name>
    <servlet-class>com.servlets.absenceReport</servlet-class>
  </servlet>
  .
  .
  .
  <security-constraint>
    <web-resource-collection>
      <web-resource-name>timeoff</web-resource-name>
      <url-pattern>/managers/*</url-pattern>
    </web-resource-collection>
    <auth-constraint>
      <role-name>mirol</role-name>
    </auth-constraint>
  </security-constraint>

  <login-config>
    <auth-method>BASIC</auth-method>
    <realm-name>default</realm-name>
  </login-config>
  <security-role>
    <role-name>mirol</role-name>
  </security-role>
</web-app>
```



# Weblogic.xml

```
<?xml version="1.0" encoding="ISO-8859-1"?>
```

```
<!DOCTYPE weblogic-web-app  
PUBLIC "-//BEA Systems, Inc.//DTD Web Application 8.1//EN"  
"http://www.bea.com/servers/wls810/dtd/weblogic810-web-  
jar.dtd">
```

```
<weblogic-web-app>  
  <security-role-assignment>  
    <role-name>mirol</role-name>  
    <principal-name>migrupo</principal-name>  
  </security-role-assignment>
```

```
</weblogic-web-app>
```