



### Table des matières

- [Configuration de Unireg](#)
  - [web.xml](#)
  - [weblogic.xml](#)
- [Configuration de Weblogic](#)
  - [Ajout d'un groupe](#)
  - [Ajout d'un utilisateur](#)
  - [Ajout des rôles](#)
- [Configuration de Tomcat](#)

Les web-services unireg sont sécurisés avec le mode *Basic Authentication* du protocole HTTP.

## Configuration de Unireg

L'idée est de restreindre l'accès aux urls **/ws/\***.

L'identification de l'utilisateur (username/password) n'est pas faite par Unireg mais déléguée au serveur applicatif. Pour cela, on définit des rôles qui ont le droit d'accès à certaines urls, et le serveur applicatif doit être configuré pour reconnaître ces rôles.

### web.xml

La configuration suivante doit être faite dans le fichier *web.xml* :

```
<!-- Sécurisation des web-services -->
<security-constraint>
  <web-resource-collection>
    <web-resource-name>Web-service Tiers</web-resource-name>
    <url-pattern>/ws/tiers</url-pattern>
    <http-method>GET</http-method>
    <http-method>POST</http-method>
  </web-resource-collection>
  <auth-constraint>
    <role-name>ws-tiers-role</role-name>
  </auth-constraint>
</security-constraint>

<security-constraint>
  <web-resource-collection>
    <web-resource-name>Web-service Batch</web-resource-name>
    <url-pattern>/ws/batch</url-pattern>
    <http-method>GET</http-method>
    <http-method>POST</http-method>
  </web-resource-collection>
  <auth-constraint>
    <role-name>ws-batch-role</role-name>
  </auth-constraint>
</security-constraint>

<login-config>
  <auth-method>BASIC</auth-method>
  <realm-name>security</realm-name>
</login-config>

<security-role>
  <role-name>ws-tiers-role</role-name>
</security-role>
<security-role>
```

```
<role-name>ws-batch-role</role-name>
</security-role>
```

## weblogic.xml

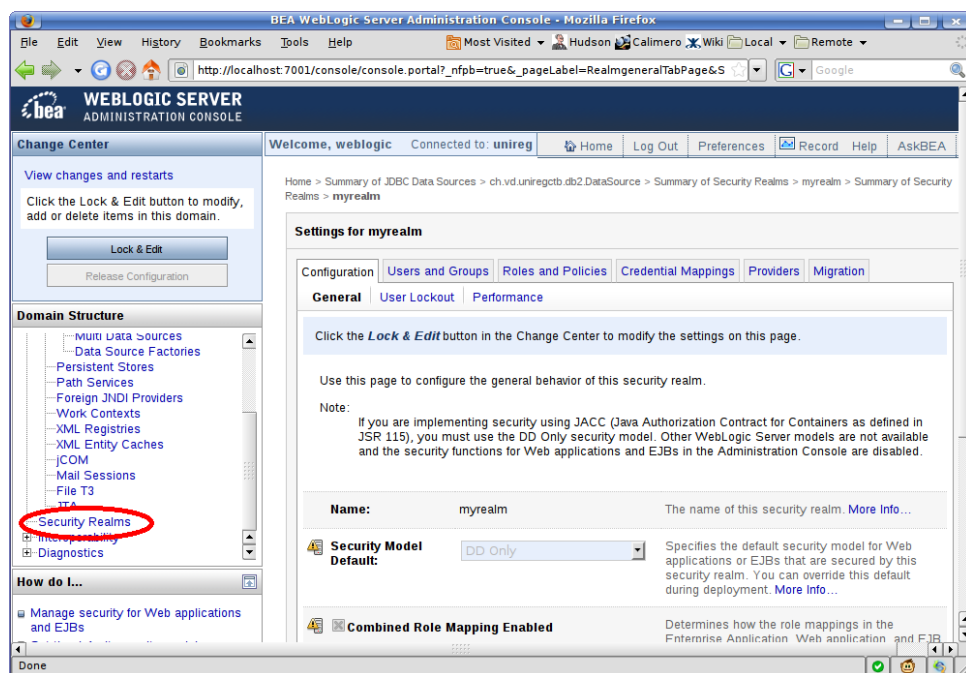
Le fichier *weblogic.xml* doit être complété avec les informations suivantes:

```
<!-- Sécurisation du web-service -->
<security-role-assignment>
  <role-name>ws-tiers-role</role-name>
  <externally-defined/>
</security-role-assignment>
<security-role-assignment>
  <role-name>ws-batch-role</role-name>
  <externally-defined/>
</security-role-assignment>
```

# Configuration de Weblogic

Weblogic doit être configuré pour reconnaître les rôles *ws-tiers-role* et *ws-batch-role* définis par Unireg. Un rôle est ensuite associé à un groupe, et un groupe est associé des utilisateurs.

Toute la configuration de sécurité est disponible à partir de l'écran ci-dessous. Il faut donc cliquer sur *Security Realms*, puis *myrealm* :



## Ajout d'un groupe

Cliquer sur l'onglet *User and Groups* et sélectionner le sous-onglet *Groups* :

**Settings for myrealm**

[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 - 7 of 7 Previous | Next

<input type="checkbox"/>	Name	Description	Provider
<input type="checkbox"/>	AdminChannelUsers	AdminChannelUsers can access the admin channel.	DefaultAuthenticator
<input type="checkbox"/>	Administrators	Administrators can view and modify all resource attributes and start and stop servers.	DefaultAuthenticator
<input type="checkbox"/>	AppTesters	AppTesters group.	DefaultAuthenticator
<input type="checkbox"/>	CrossDomainConnectors	CrossDomainConnectors can make inter-domain calls from foreign domains.	DefaultAuthenticator
<input type="checkbox"/>	Deployers	Deployers can view all resource attributes and deploy applications.	DefaultAuthenticator
<input type="checkbox"/>	Monitors	Monitors can view and modify all resource attributes and perform operations not restricted by roles.	DefaultAuthenticator
<input type="checkbox"/>	Operators	Operators can view and modify all resource attributes and perform server lifecycle operations.	DefaultAuthenticator

[New](#) [Delete](#) Showing 1 - 7 of 7 Previous | Next

Puis sur le bouton *New* et entrer les informations du groupe (WSUsers est le groupe créé ci-dessous):

**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](#)

## Ajout d'un utilisateur

Cliquer sur l'onglet *Users and Groups* et sélectionner le sous-onglet *Users* :

**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 - 1 of 1   Previous | Next

<input type="checkbox"/>	Name	Description	Provider
<input type="checkbox"/>	weblogic	This user is the default administrator.	DefaultAuthenticator

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

Showing 1 - 1 of 1   Previous | Next

Puis sur le bouton *New* et entrer les informations de l'utilisateur (*web-it* est l'utilisateur utilisé ci-dessous):

**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](#)

Revenir sur la liste des utilisateurs (onglet *User and Groups*, sous-onglet *Users*), puis cliquer sur l'utilisateur nouvellement créé et finalement associer le groupe avec l'utilisateur:

Home > Summary of Security Realms > myrealm > Users and Groups > web-it > Summary of Security Realms > myrealm > Users and Groups > weblogic > Users and Groups > **web-it**

**Settings for web-it**

General Passwords **Groups**

Save

Use this page to configure group membership for this user.

**Parent Groups:**

Available

- AppTesters
- CrossDomainConnectors
- Deployers
- Monitors
- Operators

Chosen

- WSUsers

This user can be a member of any of these parent groups. [More Info...](#)

Save

## Ajout des rôles

Cliquer l'onglet *Roles and Policies*, ouvrir le dossier *Global Roles* et cliquer sur le sous-dossier *Roles* :

**Settings for myrealm**

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

**Realm Roles** Realm Policies

Use this table to view, add, modify or remove global or scoped security roles for this security realm. Global roles are listed in the Name column under the Global Roles node. Scoped roles are listed in the Name column under the individual resources that they secure.

Notes:

- This table does not list scoped roles for JNDI resources or WorkContext resources. To see these scoped roles, view the Security tab for each JNDI node or WorkContext object.
- If you imported security roles for EJBs or Web applications from deployment descriptors using the Install Application Assistant, you must activate changes to access the roles.

**Roles**

Edit Role

Showing 1 - 7 of 7 Previous | Next

Name	Resource Type	Role Policy
Deployments		
Domain		
Global Roles		
<b>Roles</b>		
JCOM		
JDBC		
JMS		
Servers		

Edit Role

Showing 1 - 7 of 7 Previous | Next

On tombe sur l'écran suivant :

**Global Roles**

A global security role applies to all WebLogic resources deployed within a security realm (and thus the entire WebLogic Server domain). Use this page to add, edit or remove global security roles configured in this security realm.

[Customize this table](#)

**Global Roles**

New
Delete
Showing 1 - 8 of 8
Previous
Next

<input type="checkbox"/>	Role Name ↕	Provider Name
<input type="checkbox"/>	Admin	XACMLRoleMapper
<input type="checkbox"/>	AdminChannelUser	XACMLRoleMapper
<input type="checkbox"/>	Anonymous	XACMLRoleMapper
<input type="checkbox"/>	AppTester	XACMLRoleMapper
<input type="checkbox"/>	CrossDomainConnector	XACMLRoleMapper
<input type="checkbox"/>	Deployer	XACMLRoleMapper
<input type="checkbox"/>	Monitor	XACMLRoleMapper
<input type="checkbox"/>	Operator	XACMLRoleMapper

New
Delete
Showing 1 - 8 of 8
Previous
Next

Maintenant, il faut créer les rôles *ws-tiers-role* et *ws-batch-role*:

**Create a New Role for this Realm**

OK
Cancel

**Role Properties**

The following properties will be used to identify your new role.

What would you like to name your new role?

**Name:**

Which role mapper would you like to use with this role?

**Provider Name:**

OK
Cancel

Revenir sur l'écran qui liste les rôles globaux :

**Global Roles**

A global security role applies to all WebLogic resources deployed within a security realm (and thus the entire WebLogic Server domain). Use this page to add, edit or remove global security roles configured in this security realm.

[Customize this table](#)

**Global Roles**

NewDelete

Showing 1 - 10 of 10Previous | Next

<input type="checkbox"/>	Role Name ↕	Provider Name
<input type="checkbox"/>	Admin	XACMLRoleMapper
<input type="checkbox"/>	AdminChannelUser	XACMLRoleMapper
<input type="checkbox"/>	Anonymous	XACMLRoleMapper
<input type="checkbox"/>	AppTester	XACMLRoleMapper
<input type="checkbox"/>	CrossDomainConnector	XACMLRoleMapper
<input type="checkbox"/>	Deployer	XACMLRoleMapper
<input type="checkbox"/>	Monitor	XACMLRoleMapper
<input type="checkbox"/>	Operator	XACMLRoleMapper
<input type="checkbox"/>	ws-batch-role	XACMLRoleMapper
<input type="checkbox"/>	ws-tiers-role	XACMLRoleMapper

NewDelete

Showing 1 - 10 of 10Previous | Next

Cliquer sur le rôle *ws-batch-role*, puis cliquer sur le bouton *Add Conditions* :

**Edit Global Role**

Save

**Global Role Conditions**  
This page is used to edit the conditions for a global role on an application.  
This is the name of the global role.  
**Name** ws-batch-role  
These conditions determine membership in the role.

**Role Conditions**

Add ConditionsCombineUncombineMove UpMove DownRemoveNegate

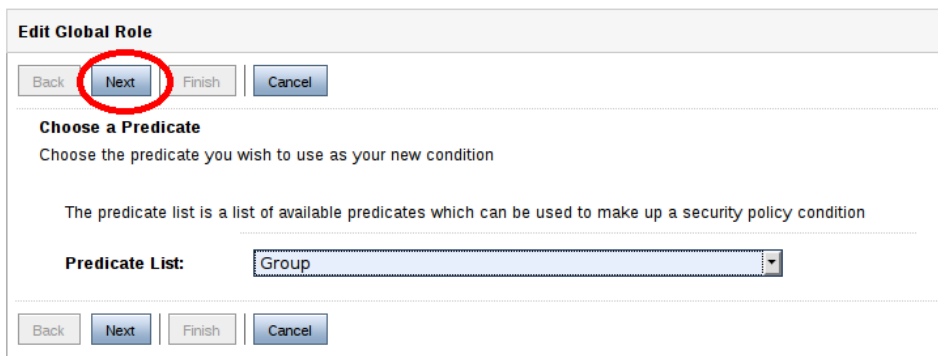
No Policy Specified

Add ConditionsCombineUncombineMove UpMove DownRemoveNegate

Save

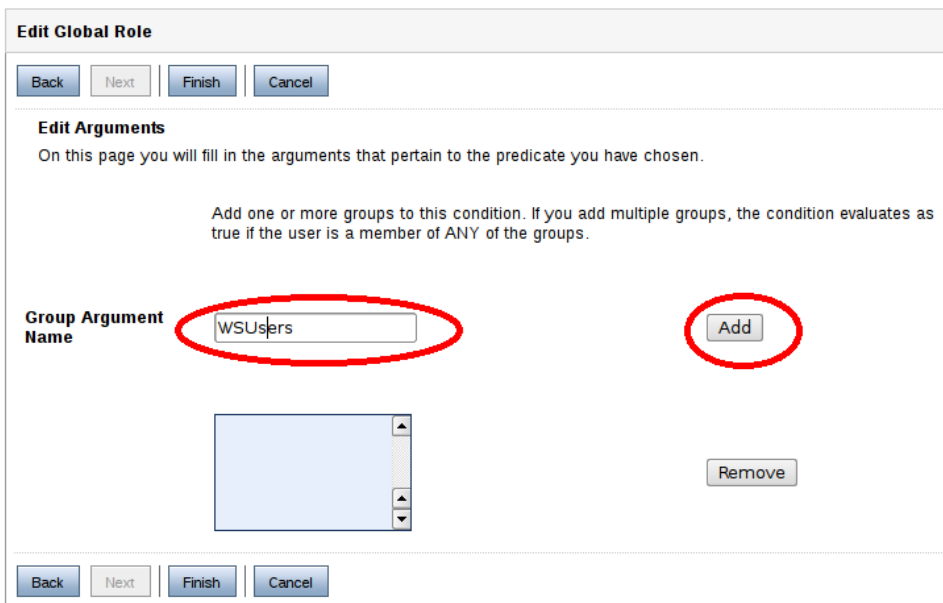
Le prédicate *Group* est normalement déjà sélectionné, cliquer sur *Next* :

Home > weblogic > Users and Groups > web-it > Users and Groups > Summary of Services > Summary of Security Realms > myrealm > Realm Roles > Global Roles > **Edit Global Role**



Entrer le nom du groupe créé plus haut, puis cliquer sur le bouton *Add*, puis sur le bouton *Finish* :

Home > weblogic > Users and Groups > web-it > Users and Groups > Summary of Services > Summary of Security Realms > myrealm > Realm Roles > Global Roles > **Edit Global Role**



Recommencer l'opération pour les autres rôles si nécessaire. C'est fini !

## Configuration de Tomcat

Toute la configuration se trouve dans le fichier *conf/tomcat-users.xml*. Le fichier ci-dessous définit un utilisateur web-it avec les rôles *ws-tiers-role*, *ws-batch-role* et *ws-securite-role* :

```
<?xml version='1.0' encoding='utf-8'?>
<tomcat-users>
  <role rolename="ws-securite-role"/>
  <role rolename="ws-batch-role"/>
  <role rolename="tomcat"/>
  <role rolename="manager"/>
  <role rolename="ws-tiers-role"/>
  <role rolename="admin"/>
  <user username="tomcat" password="tomcat" roles="tomcat,manager,admin"/>
  <user username="web-it" password="wsunireg" roles="ws-tiers-role,ws-batch-role,ws-securite-role"/>
</tomcat-users>
```