For each `security-role` defined in the deployment descriptor, an additional WebRoleRefPermission must[6] be added to the corresponding role by calling the the `addToRole` method on the `PolicyConfiguration` object. The name of all such permissions must be the empty string, and the actions of each such permission must be the `role-name` of the corresponding role.

3.1.3.3 Servlet URL-Pattern Matching Rules

This URL pattern matches another pattern if they are related, by case sensitive comparison, as follows:

- their pattern values are String equivalent, or
- this pattern is the path-prefix pattern "/*", or
- this pattern is a path-prefix pattern (that is, it starts with "/" and ends with "/*") and the other pattern starts with the substring of this pattern, minus its last 2 characters, and the next character of the other pattern, if there is one, is "/", or
- this pattern is an extension pattern (that is, it starts with "*.") and the other pattern ends with this pattern, or
- this pattern is the special default pattern, "/", which matches all other patterns.

TABLE 3-2 url-pattern Types by Example

pattern type	example
exact	/acme/widget/hammer
path prefix	/acme/widget/*
extension	*.html
default	/

3.1.3.4 Example

This example demonstrates the WebResourcePermission and WebUserDataPermission objects that would result from the translation of a deployment descriptor that contained the following `security-constraint` elements.

---

6. These additional WebRoleRefPermission objects support the use of isUserInRole from unmapped (to a Servlet) JSP components.