NativeSPRequestMapPathRegex

A serious error was discovered in the implementation of this feature, as disclosed in an advisory. The `ignoreCase` attribute was implemented in reverse by mistake, and so the default value of "true" actually causes case-sensitive matching, generally **not** the intended result. Pending the release of V2.6.0 in the summer of 2016, most deployers will want to include `ignoreCase="false"` when using this feature, along with a comment to revisit it once 2.6.0 is released, at which time a new setting with the proper implementation will be provided. In the V2.6 release the new `caseSensitive` attribute, with a default of false, controls the case sensitivity.

The `<PathRegex>` element is used to apply content rules to requests whose path matches a regular expression. The query string, if any, is **NOT** included in the comparison.

Regular expressions apply to the remainder of the path that is being compared and do not "nest", so if you care what's after the part you're matching, then choose your expression to check for that.

Example

```
<RequestMapper type="Native">
    <RequestMap applicationId="default">
        <Host name="sp.example.org">
            <Path name="secure">
                <!-- Note the reversed ignoreCase setting, see the warning above. -->
                <PathRegex regex="(en|de|it|fr)/create/new/class" ignoreCase="false" authType="shibboleth"
requireSession="true">
                    <AccessControl><NOT><Rule require="affiliation">student</Rule></NOT></AccessControl>
                </PathRegex>
            </Path>
        </Host>
    </RequestMap>
</RequestMapper>
```

Attributes

Content Specifiers

- `regex` (string)
  - Required attribute, specifies the regular expression to match against.
- `ignoreCase` (boolean)
  - **Deprecated in V2.6**
  - Controls case option in regex engine. Per the warning above, the default of "true" was mistakenly implemented to mean "don't ignore case", so this setting should almost always be set to "false". A replacement setting will be provided in a subsequent release.

Version 2.6 and Above

- `caseSensitive` (boolean) (defaults to false)
  - Controls the case option in regex engine.

Content Settings

XML attributes corresponding to request mapper properties are used.

Child Elements

Access Control

One of the following elements can be used to attach an access control policy to the resource. This is a violation of the axiom that the SP doesn't do access control, but it's really just a call-out that has some predefined plugins you can use as examples to create more.

- `<htaccess>`
  - Enables Apache `.htaccess` support during the authorization phase. This is automatic and implicit for the "Native" request mapper, but can be enabled by hand if the "XML" request mapper is used. Note that this will fail for non-Apache servers.
- `<AccessControlProvider>`
  - Attaches a custom access control policy supported by a plugin.

- `<AccessControl>`
    - Attaches an access control policy using the sample XML-based plugin provided with the SP. This is just a short-hand for embedding the policy in the element above, if you want the policy inside the same file.

If no element is included (or inherited or implicitly enabled), any access control is left to the resource.

If an error occurs when processing this element, a dummy policy to deny access is installed to prevent accidental exposure.

Nested Content Specifiers

- `<Query>` (zero or more)
    - Matches requests containing a query string parameter satisfying the element.

For more details on how the request mapping process works, see the request mapper HOWTO.