XMLAccessControl

XMLAccessControl

This is a cross-platform (any web server) plugin that allows AccessControl to be applied by attaching XML-based rules directly within the XML-based RequestMap syntax in `Shibboleth.xml`. The plugin was added in release **1.3b** of the ServiceProvider software.

There are two different methods to define the AuthZ rules. One of them can be used to delegate the management of access control rules (carefully consider the dangers in doing so!). Changes to the rules are applied in the same way as changes to the general `Shibboleth.xml` file, so you don't need to restart the webserver.

AuthZ rules inline in Shibboleth.xml

Insert an `<AccessControl>` element as the first child of a `<Host>` or `<Path>` element in the RequestMap, which applies to all requests at or below that point of the web site.

A simple inline example:

```
<!-- ... -->
<Host name="sp.example.org">
        <Path name="secure" authType="shibboleth" requireSession="true">
                <AccessControl>
                        <AND>
                                <OR>
                                        <Rule require="affiliation">member@osu.edu</Rule>
                                        <Rule require="affiliation">member@psu.edu</Rule>
                                </OR>

                                <Rule require="entitlement">urn:mace:example.edu:exampleEntitlement</Rule>
                        </AND>
                </AccessControl>
        </Path>
</Host>
<!-- ... -->
```

In English, this means "requests for resources in the `secure` folder on the virtual host named `sp.example.org` on ports 80 and 443 are granted only to members of the Ohio State or Penn State communities who also posssess the entitlement "urn:mace:example.edu:exampleEntitlement".

The example plugin syntax supports `AND` and `OR` operators that can contain any number of children, and a `NOT` operator that negates a single child rule (which could itself be a rule or a nested operator).

AuthZ rules in an external XML file

Insert an `<AccessControlProvider>` element as the first child of a `<Host>` or `<Path>` element in the RequestMap, which applies to all requests at or below that point of the web site. The `type` attribute must be set to `edu.internet2.middleware.shibboleth.sp.provider.XMLAccessControl` and a `uri` attribute points to an external file containing the `<AccessControl>` element.

The second mechanism is simply a way of externalizing the policy into a separate file so it can be maintained independently. In either case, changes are detected and applied without restarting anything. Note that if there is an error in the external file, the entire Shibboleth configuration will not be reloaded due to the error. This has even bigger consequences when you want to restart your webserver, since this will prevent it from starting up because the Shibboleth module has no valid configuration (you should check Shibboleth's module logfile, `native.log` , for errors before you do a full restart).

Here, the policy is placed in a hidden file in a public directory much like a .htaccess file. The web server should be configured to deny PUBLIC access to it if the policy were secret (note: the webserver itself has to be able to read it). The syntax in `Shibboleth.xml` looks like:

```
<!-- ... -->
<Host name="sp.example.org">
        <Path name="secure" authType="shibboleth" requireSession="true">
                <AccessControlProvider uri="/var/www/secure/.shibacl.xml" type="edu.internet2.middleware.
shibboleth.sp.provider.XMLAccessControl"/>
        </Path>
</Host>
<!-- ... -->
```

The syntax in `.shibacl.xml` looks like (similar to inline but note the required xml namespace definition):

```
<?xml version="1.0" encoding="UTF-8"?>
<AccessControl xmlns="urn:mace:shibboleth:target:config:1.0">
        <AND>
                <OR>
                        <Rule require="affiliation">member@osu.edu</Rule>
                        <Rule require="affiliation">member@psu.edu</Rule>
                </OR>
                <Rule require="entitlement">urn:mace:example.edu:exampleEntitlement</Rule>
        </AND>
</AccessControl>
```

Do not forget to configure the webserver to not disclose this file since it will most likely contain some private information.