How to Use WebAC agentClass Groups

In WebAC you can use the `acl:agentClass` property of an Authorization to point to a resource that holds a list of usernames. This allows you to create and manage groups of users within Fedora, and to assign different permissions to different groups. This how-to will guide you through the process of creating a resource, creating an `agentClass` group, and limiting access to that resource through an ACL that references that `agentClass` group.

Prerequisites

- a running Fedora 4 with the WebAC module enabled, at http://localhost:8080/fcrepo (an easy way to get this is to run the Fedora 4 Vagrant)
- curl

Steps

1. Create these four files:

acl.ttl

```
@prefix webac: <http://fedora.info/definitions/v4/webac#>.
@prefix ldp: <http://www.w3.org/ns/ldp#>.

<> a webac:Acl .
```

group.ttl

```
@prefix ldp: <http://www.w3.org/ns/ldp#>.
@prefix foaf: <http://xmlns.com/foaf/0.1/> .

<> a foaf:Group;
    foaf:member "testuser".
```

foo.ttl

```
@prefix ldp: <http://www.w3.org/ns/ldp#>.
@prefix acl: <http://www.w3.org/ns/auth/acl#>.
@prefix dc: <http://purl.org/dc/elements/1.1/>.

<> a acl:accessControl </fcrepo/rest/acl>;
    dc:title "Hello, World!".
```

authz.ttl

```
@prefix acl: <http://www.w3.org/ns/auth/acl#>.

<> a acl:Authorization;
    acl:accessTo </fcrepo/rest/foo>;
    acl:agentClass </fcrepo/rest/group>;
    acl:mode acl:Read.
```

2. Upload these resources into Fedora:

```
$ curl -X PUT http://localhost:8080/fcrepo/rest/acl -u fedoraAdmin:secret3 \
    -H "Content-Type: text/turtle" --data-binary @acl.ttl
$ curl -X PUT http://localhost:8080/fcrepo/rest/foo -u fedoraAdmin:secret3 \
    -H "Content-Type: text/turtle" --data-binary @foo.ttl
$ curl -X PUT http://localhost:8080/fcrepo/rest/group -u fedoraAdmin:secret3 \
    -H "Content-Type: text/turtle" --data-binary @group.ttl
$ curl -X PUT http://localhost:8080/fcrepo/rest/acl/authz -u fedoraAdmin:secret3 \
    -H "Content-Type: text/turtle" --data-binary @authz.ttl
```

(**Note:** The order you upload these in *is* important, since `foo` references `acl`, and `authz` references `foo` and `group`)

3. Test that `testuser` can read the `foo` resource, while `adminuser` cannot:

```
$ curl -i http://localhost:8080/fcrepo/rest/foo -u testuser:password1
$ curl -i http://localhost:8080/fcrepo/rest/foo -u adminuser:password2
```

The first request should respond with **200 OK**, while the second should be **403 Forbidden**.

To allow `adminuser` to also read the `foo` resource, we can add `adminuser` to the members of the group.

1. Create **group.sparql** with the following contents:

group.sparql

```
PREFIX foaf: <http://xmlns.com/foaf/0.1/>

INSERT {
    <> foaf:member "adminuser" .
}
WHERE {}
```

2. Run this command to update the group and add `adminuser` to it:

```
$ curl -i -X PATCH http://localhost:8080/fcrepo/rest/group \
    -u fedoraAdmin:secret3 \
    -H "Content-Type: application/sparql-update" \
    --data-binary @group.sparql
```

You should receive a **204 No Content** response on success.

1. Now you should be able to repeat the command from step 3 and successfully retrieve the `foo` resource as `adminuser`:

```
$ curl -i http://localhost:8080/fcrepo/rest/foo -u adminuser:password2
```

This time, you should get a **200 OK** response.

Caveats for `agentClass` Groups

- For it to be useful, the names listed in the `foaf:member` properties of an authorization need to be names that your authentication system will provide to Fedora. *Remember, Fedora does no authentication of its own.*
- The purpose of the `acl:agentClass` groups is distinct from any group mechanism your existing authentication system may have (e.g., LDAP or ActiveDirectory groups). The groups provided by the authentication system would be passed to Fedora as security principals, which the WebAC module compares against the **`acl:agent`** property. In other words, externally defined groups are opaque to Fedora, thus it treats them as simple agents.