

WebAC Example Scenarios

These scenarios assume that Fedora has been configured to use `fcrepo.auth.webac.userAgent.baseUrl=http://example.org/agent/`

1. I want to allow a user with username "smith123" to have **read, write** access to resource http://localhost:8080/rest/webacl_box1.

Create this file to use as the ACL:

acl.ttl

```
@prefix acl: <http://www.w3.org/ns/auth/acl#> .
<#authz> a acl:Authorization ;
  acl:agent <http://example.org/agent/smith123> ;
  acl:mode acl:Read, acl:Write ;
  acl:accessTo <http://localhost:8080/rest/webacl_box1> .
```

Run the following commands:

```
curl -XPUT http://localhost:8080/rest/webacl_box1
curl -XPUT http://localhost:8080/rest/webacl_box1/fcr:acl -H 'Content-Type: text/turtle' --data-binary @acl.ttl
```

2. I want to let the group "Editors" have **read, write** access on all the items in the collection "<http://localhost:8080/rest/box/bag/collection>"

Create this file to use as the ACL:

acl.ttl

```
@prefix acl: <http://www.w3.org/ns/auth/acl#> .
<> a acl:Authorization ;
  acl:agentGroup <http://localhost:8080/rest/groups/Editors> ;
  acl:mode acl:Read, acl:Write ;
  acl:accessTo <http://localhost:8080/rest/box/bag/collection> .
```

Create this file to define the Editors group:

group.ttl

```
@prefix vcard: <http://www.w3.org/2006/vcard/ns#> .
<> a vcard:Group ;
  vcard:hasMember <http://example.org/agent/jones456>
```

Run the following commands:

```
curl -XPUT http://localhost:8080/rest/box/bag/collection
curl -XPUT http://localhost:8080/rest/groups/Editors -H 'Content-Type: text/turtle' --data-binary @group.ttl
curl -XPUT http://localhost:8080/rest/box/bag/collection/fcr:acl -H 'Content-Type: text/turtle' --data-binary @acl.ttl
```

3. I would like the collection <http://localhost:8080/rest/dark/archive> to be viewable only by the group "Restricted", but I would like to allow **anyone** to view the resource <http://localhost:8080/rest/dark/archive/sunshine>.

Create these file to use as the ACLs and the group listing:

acl_restricted.ttl

```
@prefix acl: <http://www.w3.org/ns/auth/acl#> .
<> a acl:Authorization ;
    acl:agentGroup <http://localhost:8080/rest/groups/Restricted> ;
    acl:mode acl:Read ;
    acl:accessTo <http://localhost:8080/rest/dark/archive> .
```

acl_open.ttl

```
@prefix acl: <http://www.w3.org/ns/auth/acl#> .
@prefix foaf: <http://xmlns.com/foaf/0.1/> .
<> a acl:Authorization ;
    acl:agentClass foaf:Agent ;
    acl:mode acl:Read ;
    acl:accessTo <http://localhost:8080/rest/dark/archive/sunshine> .
```

group.ttl

```
@prefix vcard: <http://www.w3.org/2006/vcard/ns#> .
<> a vcard:Group ;
    vcard:hasMember <http://example.org/agent/jones456>
```

Run the following commands:

```
curl -XPUT http://localhost:8080/rest/dark/archive
curl -XPUT http://localhost:8080/rest/dark/archive/sunshine
curl -XPUT http://localhost:8080/rest/groups/Restricted -H 'Content-Type: text/turtle' --data-binary @group.ttl
curl -XPUT http://localhost:8080/rest/dark/archive/fcr:acl -H 'Content-Type: text/turtle' --data-binary @acl_restricted.ttl
curl -XPUT http://localhost:8080/rest/dark/archive/sunshine/fcr:acl -H 'Content-Type: text/turtle' --data-binary @acl_open.ttl
```

4. The collection http://localhost:8080/rest/public_collection should be **readable** by anyone but only **editable** by users in the group **Editors**.

Create these file to use as the ACL and the group listing:

Auth1.ttl

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

<#authz_read> a acl:Authorization ;
    acl:agentClass foaf:Agent ;
    acl:mode acl:Read ;
    acl:accessTo <http://localhost:8080/rest/public_collection> .

<#authz_read_write> a acl:Authorization ;
    acl:agentGroup <http://localhost:8080/rest/groups/Editors> ;
    acl:mode acl:Read, acl:Write ;
    acl:accessTo <http://localhost:8080/rest/public_collection> .
```

group.ttl

```
@prefix vcard: <http://www.w3.org/2006/vcard/ns#> .
<> a vcard:Group ;
    vcard:hasMember <http://example.org/agent/jones456>
```

Run the following commands:

```
curl -XPUT http://localhost:8080/rest/public/collection
curl -XPUT http://localhost:8080/rest/groups/Editors -H 'Content-Type: text/turtle' --data-binary @group.ttl
curl -XPUT http://localhost:8080/rest/public/collection/fcr:acl -H 'Content-Type: text/turtle' --data-binary @acl_restricted.ttl
```

5. Only the *ex:publicImage* type objects in the container <http://localhost:8080/rest/mixedCollection> are viewable by anyone, all others are only viewable by the group **Admins**.

Create these file to use as the ACL and the group listing:

acl.ttl

```
@prefix ex: <http://example.org/terms#> .
@prefix acl: <http://www.w3.org/ns/auth/acl#> .
@prefix foaf: <http://xmlns.com/foaf/0.1/> .

<#authz_restricted> a acl:Authorization ;
  acl:agentGroup <http://localhost:8080/rest/group/Admins> ;
  acl:mode acl:Read ;
  acl:accessTo <http://localhost:8080/rest/mixedCollection> .

<#authz_open> a acl:Authorization ;
  acl:agentClass foaf:Agent ;
  acl:mode acl:Read ;
  acl:accessToClass ex:publicImage ;
  acl:default <http://localhost:8080/rest/mixedCollection> .
```

group.ttl

```
@prefix vcard: <http://www.w3.org/2006/vcard/ns#> .
<> a vcard:Group ;
  vcard:hasMember <http://example.org/agent/jones456>
```

Run the following commands:

```
curl -XPUT http://localhost:8080/rest/mixedCollection
curl -XPUT http://localhost:8080/rest/groups/Admins -H 'Content-Type: text/turtle' --data-binary @group.ttl
curl -XPUT http://localhost:8080/rest/mixedCollection/fcr:acl -H 'Content-Type: text/turtle' --data-binary @acl.ttl
```