Default Filesystem-based Policy

When the WebAC module is in effect, resource access is based on the presence of a triple with the `acl:accessControl` predicate. For any resource that has an RDF graph that does not contain a triple with that property, the WebAC authorization module will look in the parent container until it reaches the root resource. If there is still no `acl:accessControl` property, then the Authorization Delegate will inspect a filesystem-based policy.

The default policy is defined to block all access:

```
@prefix rdfs: <http://www.w3.org/2000/01/rdf-schema#> .
@prefix acl: <http://www.w3.org/ns/auth/acl#> .
@prefix foaf: <http://xmlns.com/foaf/0.1/> .
@prefix fedora: <http://fedora.info/definitions/v4/repository#> .

<> a acl:Authorization ;
   rdfs:label "Root Authorization" ;
   rdfs:comment "By default, all non-Admin agents (foaf:Agent) are denied access (no acl:mode is specified) to
all resources." ;
   acl:agent foaf:Agent ;
   acl:accessToClass fedora:Resource .
```

In most cases, this default is appropriate, but it is also possible to override this `acl:Authorization` definition with a custom policy.

In order to override this policy, it is recommended to add a configuration value to JAVA_OPTS, pointing to the custom authorization policy:

```
export JAVA_OPTS="${JAVA_OPTS} -Dfcrepo.auth.webac.authorization=/path/to/authorization.ttl"
```

When overriding the filesystem-based authorization, be aware that the WebAC module expects that file to be in Turtle format.

For instance, in order to grant read access to the entire repository:

```
@prefix rdfs: <http://www.w3.org/2000/01/rdf-schema#> .
@prefix acl: <http://www.w3.org/ns/auth/acl#> .
@prefix foaf: <http://xmlns.com/foaf/0.1/> .

<> a acl:Authorization ;
   rdfs:label "Root Authorization Policy" ;
   rdfs:comment "Provide read access to all resources to all agents." ;
   acl:agent foaf:Agent ;
   acl:mode acl:Read ;
   acl:accessTo <info:fedora/> .
```

Please note that any use of `acl:accessTo` will use a different syntax to refer to Fedora locations. Here, the root Fedora resource is written `<info:fedora/>`, since this file is not aware of the HTTP location of the repository. If, for instance, a default policy is to apply to all locations under `/fcrepo/rest/acls`, then the `acl:accessTo` triple would refer to `<info:fedora/acls>`. This way, the default policy is portable across hostname or port changes.