ACL Agents - Strings vs. URIs

While the WebAC spec requires that the objects of `acl:agent` statements be URIs, the current (4.7.5) Modeshape implementation of Fedora allows string literals as the objects of `acl:agent` statements. In addition, internally, the implementation does all of its agent comparisons assuming the agent is a simple string username, and not a full URI. This was done to facilitate easier integration with existing authentication systems (e.g., LDAP) that only provide a username and not a URI.

In order to support using URIs as objects of `acl:agent` statements, there are two system properties that can be set:

- `fcrepo.auth.webac.userAgent.baseUri`
- `fcrepo.auth.webac.groupAgent.baseUri`

Despite the name, `fcrepo.auth.webac.groupAgent.baseUri` actually has nothing to do with, and should **not** be confused with, WebAC agent groups. Instead, in this context "group" is referring to an externally defined group (again, from a system like LDAP). From Fedora's perspective, that sort of group is treated as a single agent, and the URI is **not** dereferenced.

If the object of an `acl:agent` statement looks like a URI, these properties are used to strip off the base part of that URI, leaving a simple string username.

Example

Fedora is started with `-Dfcrepo.auth.webac.userAgent.baseUri=http://example.com/users/`

There is an ACL authorization with the following triple:

```
<> acl:agent <http://example.com/users/jdoe>
```

When determining the list of agents for that authorization, the WebAC authorization delegate will strip off the base URI and return the string username `jdoe` . That is what will be compared with the security principles from whatever authentication system is configured.