Basic Role-based Authorization Delegate

This authorization delegate makes decisions based on the four basic roles of "metadata reader", "reader", "writer", and "admin". These roles are assigned to principals on Fedora Glossary. Assigned roles are inherited through the repository tree until blocked by another assignment.

The role **metadata reader** has not yet been implemented.

This authorization delegate makes use of the Access Roles Module to assign and query roles in the repository.

Roles

- **metadata reader** - can retrieve information about Fedora Containers, but cannot retrieve content
- **reader** - can retrieve information about Fedora Containers, including content
- **writer** - all permissions of reader; can create, modify and delete Fedora Containers
- **admin** - all permissions of writer; can modify the roles assigned to Fedora Containers

Policy

The permissions granted to these roles are fixed. Rather than consulting any declarative policy, this authorization delegate has hard-coded role-permission assignments in the source code.

Role/Permission Matrix

	metadata reader	reader	writer	admin
read properties	X	X	X	X
read content		X	X	X
write			X	X
write roles				X

Configuring the Basic Role-Based Authorization Delegate

See Authorization Delegates for more information on how an authorization delegate is configured.

Edit your **repo.xml** file to configure the authentication provider. The file should contain these three beans, as shown:

```
<bean name="modeshapeRepofactory" class="org.fcrepo.kernel.spring.ModeShapeRepositoryFactoryBean"
  depends-on="authenticationProvider">
    <property name="repositoryConfiguration" value="${fcrepo.modeshape.configuration:repository.json}" />
</bean>

<bean name="fad" class="org.fcrepo.auth.roles.basic.BasicRolesAuthorizationDelegate"/>

<bean name="authenticationProvider" class="org.fcrepo.auth.common.ServletContainerAuthenticationProvider">
    <property name="fad" ref="fad"/>
</bean>
```

Edit your **repository.json** file to enable an authenticated internal session between Fedora and ModeShape, so that the security section matches the example shown:

```
"security" : {
  "anonymous" : {
    "roles" : ["readonly","readwrite","admin"],
    "useOnFailedLogin" : false
  },
  "providers" : [
    { "classname" : "org.fcrepo.auth.common.ServletContainerAuthenticationProvider" }
  ]
},
```