Tempo

Role-Based Access Control

Added by Alex Boisvert, last edited by Alex Boisvert on Jul 30, 2008

Role-Based Access Control (RBAC)

What is RBAC ?

Role-based access control (RBAC) is an approach to restricting system access to authorized users.

Within an organization, roles are created for various job functions. The permissions to perform certain operations ('permissions') are assigned to specific roles. Members of staff (or other system users) are assigned particular roles, and through those role assignments acquire the permissions to perform particular system functions. Unlike context-based access control (CBAC), RBAC does not look at the message context (such as where the connection was started from).

Since users are not assigned permissions directly, but only acquire them through their role (or roles), management of individual user rights becomes a matter of simply assigning the appropriate roles to the user, which simplifies common operations such as adding a user, or changing a user's department.

When defining an RBAC model, the following conventions are useful:

1. A user can have multiple roles.
2. A role can have multiple users.
3. A role can have many permissions.
4. A permission can be assigned to many roles.

RBAC structure

a RBAC provider is divided into three subsystems:

RBACAdmin

Administrative services for the creation and maintaince of RBAC element sets and relations. This is used to add/delete users, assign roles to a user, etc ...
http://tempo.intalio.org/tempo/trunk/security/src/main/java/org/intalio/tempo/security/rbac/RBACAdmin.java

RBACQuery

Query services for reviewing RBAC element sets, properties and relations. Mainly, find set of roles in a realm, set of roles for a user, the authorized user for a given role, etc ..
http://tempo.intalio.org/tempo/trunk/security/src/main/java/org/intalio/tempo/security/rbac/RBACQuery.java

RBACRuntime

Runtime services for making access control decisions.
With this interface, we check the access for a given user, and the associated roles, to a given operation on a given object.
http://tempo.intalio.org/tempo/trunk/security/src/main/java/org/intalio/tempo/security/rbac/RBACRuntime.java

Thoses interfaces seek compliance with the NIST RBAC Proposed voluntary consensus standard DRAFT, dated 4/4/2003. More information can be found at http://csrc.ncsl.nist.gov/rbac/.

Tempo Hierarchy

The entry point for the tempo security system is the security provider, a factory interface providing concrete implementations of the RBACProvider and AuthenticationProvider.

This can be configured in the securityConfig.xml file.

We use the SimpleSecurity provider by default:
<bean id="securityProvider" class="org.intalio.tempo.security.simple.SimpleSecurityProvider" init-method="init">

And, the LDAP provider could be configured this way:
<bean id="securityProvider" class="org.intalio.tempo.security.ldap.LDAPSecurityProvider">

RBAC Interfaces coverage

LDAP

The LDAP RBAC support in tempo is limited only to querying, thus RBACAdmin and RBACRuntime are not implemented.

Simple

The Simple implementation of RBAC, with a map of users, roles and permission written in an xml file, supports all the interfaces.

An example of a configuration can be found at:
http://tempo.intalio.org/tempo/trunk/config/security.xml

Other useful links

http://www.intalio.org/confluence/display/TEMPO/FAQ#FAQ-PullUsersandrolesfromadifferentservice
http://csrc.nist.gov/groups/SNS/rbac/documents/sandhu96.pdf
http://csrc.nist.gov/groups/SNS/rbac/faq.html

Comments