Sakai Site Groups and Group Awareness

June 13, 2006

Please direct questions or comments about this document to:
Glenn R. Golden, *ggolden@umich.edu*

This document describes how applications are group and section aware in Sakai 2.2.

Groups

Sakai 2.1 introduced Groups as parts of Sites. A site group is a subset of the site membership.

Sections, which are a course management concept, are implemented as site groups.

Two forms of awareness

Some applications are completely oblivious to site groups. For those that are group-aware, they fall into two categories:

- permissions
- partitioning

Permission Group Awareness

Some applications are aware of site groups, and use them to limit (or grant) certain permissions. Samigo and the Gradebook applications are in this category. These applications recognize the group membership in sites, and allow the people with the "teaching assistant" role in a group to grade the work of the people with the "student" role in the group. TAs can grade students in their own section, not all students.

The permissions are group-aware, but these applications assume that the entities of the application (such as the tests and quizzes in Samigo) apply equally to the entire site membership.

Partitioning Group Awareness

Other applications use groups to partition their entities. Announcements did this in 2.1. Calendar, Assignments and Content join Announcements for partitioning group awareness in 2.2.

These applications associate 0, or one or more groups with each entity. In other words, each announcement can be for the entire site, or it can be for one or more groups of the site.

If an entity is grouped, only members of the groups have any access to the entity; to members of other groups, the entity does not exist.

When an entity is grouped with a single group, only members of that group can access the entity. When an entity is grouped to multiple groups, the combined membership of these groups can access the entity.

The particular access (read, write, remove, etc) is controlled by the end-user's role in the group, just as it is controlled by the end-user's role in the site for site-access entities. For grouped entities, the site's permissions are not applied; permissions come only from the groups selected for the entity.

Each application defines a permission that can be granted at the site level to give the users in that role access to all groups. These are called "*.all.groups" ("annc.all.groups", "content.all.groups", etc). When users with this permission at the site level access grouped entities, those entities act as if they are not grouped. For these users, their site level permissions apply to all the entities, grouped or not, in the site.

A role can be setup to have read access at the site level, but write access in a group. In this way, a user can have permission to create something that is grouped, for that user's own group(s), but not create something for the entire site.

When an entity is multiply grouped, the combined membership of these groups can see the entity. Anyone who has write access from any part of this combined membership has write access to the entity. This means that a TA for group 1 can modify an announcement that the instructor created for groups 1, 2 and 3; the TA does not need write access in all of the groups to be able to modify the entity.

Adding a group to an entity, or rather, adding an entity to a group, is an "add" operation. Removing a group from an entity, or rather, removing an entity from a group, is a "remove" operation. When modifying an entity, the groups that can be selected for the entity are those that the end-user has "add" permission within. The groups that can be selected for removal from the entity are those that the end-users has "remove" permission within.

This means that a user might have access to modify an entity (because of their write access from somewhere in the combined membership of the entity's groups), but not have access to remove the entity from its complete group list. In these cases, the tool will

show the complete list of what groups are currently associated with the entity, but not have edit controls (i.e. no check box) for those groups that the user does not have remove permission within. A static check mark is shown instead.

It also means a user can edit an entity, unselect the groups they have access to, and save the entity. The entity will then not be available to that user. This is in essence a remove operation for the group(s), but not for the entire entity (other groups will continue to have access).

A user must have remove access in all the groups that an entity is associated with in order to completely remove the entity. Just having access from somewhere in the combined membership, which is enough to edit the entity, is not enough to completely remove it. They can remove it from any group they have "remove" permissions within, but that is a group change, from and edit operation, not a complete removal. Tools will not show the delete option for an entity unless the end-user has the remove permission from all of the entities groups (or, if the entity is a site level, ungrouped entity, delete will be offered if the end-user has remove permission at the site level).

"At the site level" or "At the group level" for permissions is really a short-hand. Sakai supports permissions defined at various levels, starting with the specific entity, including any sort of containment defined in the application (such as ContentHosting's folders), and ending with either the Site's security definition or one or more Group security definitions.