

Chapter 8. Access Control

Last Updated Wednesday, 28 March 2007

Chapter 8. Access Control Overview

Joomla

is implementing a powerful access control library that will enable both fine and course grained access control hierarchies to be devised to suit the needs of your site.

phpGACL

The

access control system uses a library called PHPgacl. For more information on the technical points of this library, refer to the site's home page at phpgacl.sf.net.

The

library has been slightly modified to use the database abstraction layer used in Joomla as opposed to the ADODB library. Some additional functions have also been implemented. However, the format of the files has been honoured as much as possible so that side-by-side comparisons of the modified Joomla files can be made with any future versions of the PHPgacl library.

The schema has been slightly modified so that primary keys are more descriptive (for example, id become aro_id in the mos_core_acl_aro table).

The PHPgacl has a good tutorial to help you work through the troubles of creating a robust ACL system. We won't regurgitate it all here but we will highlight some terminology and concepts that are relevant for developers.

The ACO

An

ACO is an Access Control Object. In terms of Joomla, it is an action that you want to perform, such a logging in, viewing, adding, editing, etc.

TheARO

An

ARO is an Access Request Object. In terms of Joomla this is "who" or "what" is asking for permission to do something. This will generally be a user, and the mos_user table is synconised with the mos_core_acl_aro table. However, there may be circumstances where system processes will be requesting permission to do something, possibly in the context of a workflow engine or the like.

ARO's are able to be assigned to a group. The defaultARO groups provided in Joomla are:ROOT

```
| - USERS
| -- PublicFrontend
| - - - Registered
| - - - - Author
| - - - - - Editor
| - - - - - - Publisher
| - - Public Backend
| - - - Manager
| - - - - Administrator
| - - - - - Super Administrator
```

The

first group is ROOT. This is really a placeholder group as there can only be one root group. The second group, USERS, is also a placeholder group. It collects all the ARO groups that pertain to users. As

mentioned previously, other "things" may require access and these would all start with their own placeholder group (for example, WORKFLOW).

Next are the start of two branches, one for access to the frontend web site and one for access to the backend administration.

The AXO

An AXO is an Access eXtensionObject

The

ACO, AXO and ACL database schemas are not yet implemented. They are emulated by hand in a simplistic fashion by the gacl class in

/classes/gacl.php

Inserting a New Group

The

group mapping for ARO's and AXO's uses a pre-order tree traversal technique to enable more efficient record retrieval from the hierarchically related data. This means that you cannot simply add a row to the table and expect the hierarchical relationships to be maintained.

To add a new user group by hand you would use the following SQL:

```
SET @parent_name = 'Registered';
```

```
SET @new_name = 'Support';
```

```
-- Select the parent node to insert after
```

```
SELECT @ins_id := group_id, @ins_lft := lft, @ins_rgt := rgt
```

```
FROM mos_core_acl_aro_groups
```

```
WHERE name = @parent_name;
```

```
SELECT @new_id := MAX(group_id) + 1 FROM mos_core_acl_aro_groups;
```

```
-- Make room for the new node
```

```
UPDATE mos_core_acl_aro_groups SET rgt=rgt+2 WHERE rgt>=@ins_rgt;
```

```
UPDATE mos_core_acl_aro_groups SET lft=lft+2 WHERE lft>@ins_rgt;
```

```
-- Insert the new node
```

```
INSERT INTO mos_core_acl_aro_groups (group_id,parent_id,name,lft,rgt)
```

```
VALUES (@new_id,@ins_id,@new_name,@ins_rgt,@ins_rgt+1);
```

The

parent_name is the name of an existing group that you want to be the parent of the new group. The new_name is the name of the new group.

The _mos_add_acl method is also available for custom developers to provide for additional ACL checks.

For more information on pre-order tree traversal algorithms refer to the following sites:

<http://www.sitepoint.com/article/1105/>

http://searchdatabase.techtarget.com/tip/1,289483,sid13_gci537290,00.html