

OverviewAccessControl

Understanding the Lenya Role Concept

1. you define an arbitrary set of roles for your publication by creating the .rml files in \$PUB_HOME/config/ac/passwd
2. you assign roles to usecases
3. you assign roles to identities at URLs using policies
4. you assign roles to workflow transitions

Defining Roles

<http://cocoona.apache.org/lenya/docs/components/accesscontrol/terms.html#Role>

Roles are the connection between access control and CMS functionality. On the access control side, you assign Roles to users, IP address ranges and groups at certain URL spaces. On the CMS side, you define which Roles are needed to execute certain usecases and workflow transitions.

Assigning Roles to Usecases

<http://cocoona.apache.org/lenya/docs/components/accesscontrol/authorizers.html#UsecaseAuthorizer>

This Authorizer looks for the lenya.usecase request parameter and checks the usecase policy file for the Roles that are allowed to execute this usecase.

Assigning Roles to Identities at URLs using Policies

<http://cocoona.apache.org/lenya/docs/components/accesscontrol/policymanagers.html>

A Policy assigns Roles to Accreditables.

Assigning Roles to Workflow Transitions

<http://cocoona.apache.org/lenya/docs/components/workflow/configuration.html#RoleCondition>

Roles vs. Groups

Roles and groups are completely different things.

Groups are just collections of users or IP ranges. They make assigning of permissions easier (you can assign a permission to a group instead of every single user).

Roles are just strings. You can choose them for every publication. You define what a role means.

Basically, you can imagine

```
+-----+
| Access Control |--- Roles ---| CMS Functions |
+-----+
- users
- groups
- IP ranges
- workflow
- usecases
```

which means that you use roles to separate your access control definitions from your CMS function definitions. Roles are used as the interface between access control and CMS functions.

If there were no roles, you would have to assign every single CMS function (workflow, usecases, ...) to users, groups etc. This would be a huge amount of work and maintenance.

But you define roles as shorthands to protect CMS functions (using workflow conditions and usecase permissions). And you assign roles to users, groups, etc. on certain URLs (using policies).