

Problems with the current ACL approach

Our current access control system is quite interesting, in that we allow to select sets of documents using expressions and then specify the ACL rules that apply to those documents.

Editing assistance

The document-selection expressions can be of arbitrary complexity, using AND, OR, grouping and function calls. This allows for expressing very powerful rules.

However, this makes it quite difficult for a document-author to know which combination of things he can enter in a document, so that the document will be accepted by the rules (note that, on repo-api level, any user can read the ACL, but in the daisy wiki people found it not acceptable that just any user is able to view the ACL, and anyhow, interpreting these rules would be too technical or involved for most users). Right now, we give in fact only a hard exception in this case, after trying to save the document. Since we have not had any complaints about this yet, we can probably assume that most people don't use ACLs with rules causing such cases very much.

Ideally, users should only be able to select document types, collections, and field values (in case the field has a selection list) that they are allowed to use.

Query performance

With the current ACL system, we're not able to select directly from the query engine (SQL database or Lucene) the documents to which the user has access. Rather, we need to query the database, and afterwards filter the documents.

For "faceted queries", the system will only show a facet's distinct values which actually appear in documents where the user has access to, so the complete facet query result calculation also needs to happen in java code.

It would be better if we could add conditions to the queries so that we only address the documents to which the user has access, removing the need for filtering afterwards.

Note that this problem is very specific to the read permission, though we probably don't want completely different ways of configuring read and other permissions.

Missing features

- People have sometimes found it useful to be able to test on users in the document-selection expression, rather than in the rules below it.

Observations from current ACL use

Looking at the ACLs of some projects realized by Outerthought, we can see that:

- most ACL rules only test on one document property, typically the document type, collection membership or the value of some field
- there is one case where two tests are combined with AND, style "field = something and InCollection('something')"
- there is one case where two tests are combined with OR, but in contrast to AND, this does not make the ACL more complex, as this would be equivalent to two separate ACL rules.

Future

Could we devise a new ACL structure (or changes to the current one) that would enable better editing assistance, better query performance, and still have an acceptable feature set?

Fields

Name	Value
Category	Design documents & proposals