Morpho - Bug #4084

Change access rule to be "allowFirst" as the default orderType

05/19/2009 10:17 AM - Jing Tao

Status:	Resolved	**Start date:**	05/19/2009
Priority:	Normal	**Due date:**	
Assignee:	Jing Tao	**% Done:**	0%
Category:	morpho - general	**Estimated time:**	0.00 hour
Target version:	1.7	**Spent time:**	0.00 hour
Bugzilla-Id:	4084		

Description

[4:36pm] matt: i just caught up on your earlier irc chat
[4:36pm] matt: wanted to chime in
[4:36pm] matt: chris said:
[4:36pm] matt: chris: right - it seems like an odd case. I think that the vast majority of cases, people will want to deny public access, and puch through access for other groups or individuals
[4:36pm] matt: and also:
[4:37pm] matt: you said:
[4:37pm] matt: daigle: the only real exception that I see is allowing access to the whole, but denying it to individuals/groups
[4:37pm] matt: [2:44pm] daigle: that does not seem like a large use case
[4:37pm] matt: i actually think that is the only use case for using denyFirst
[4:37pm] matt: sorry , i actually think that is the only use case for using **deny** at all
[4:38pm] daigle: right
[4:38pm] daigle: only one I could think of
[4:38pm] matt: the default, in the absence of a public=read rule, is to deny
[4:38pm] matt: so, most of the time, someone will positively add some allow rules
[4:39pm] matt: and then they may want to exclude some people from that group
[4:39pm] matt: ie, grant kruger-tpc=read, but deny regetz
[4:39pm] matt: for that you would want allowFirst
[4:39pm] matt: if all you are doing is granting permissions to people, you can leave the defaults and just add in an allow rule
[4:39pm] matt: make sense?
[4:40pm] daigle: uh
[4:40pm] daigle: default deny then add then deny
[4:40pm] matt: its a bit convulted to add deny public=read and then allow kruger-tpc=read, because the deny public was implicit even without the rule
[4:41pm] matt: i.e., if you want to deny public access, simply remove the public=read rule and you're done
[4:43pm] daigle: okay
[4:43pm] matt: the only good reasons I can see to deny someone are to 1) efficiency: grant access to a big group but excise a few people, in which case you want default rules to be allowFirst
[4:44pm] daigle: right
[4:44pm] matt: and 2) guarantee that a particular user doesn't have access (indirectly via a group), in which case you still want allowFirst
[4:45pm] matt: so thanks for hearing me out -- I just wanted to be clear that Morpho's default allowFirst rule is the right rule in my opinion

This is not just change from "denyFirst" to "allowFirst", we may do this for both top and entity level access rules:

If the user selects "No" (i.e., don't allow public read) and does nothing else, then an explicit public <deny> rule is inserted. This is required to override the
top-level access rules.

But if the user selects "No" **and** adds at least one special access rule (for a user/group), then the special access rule(s) is/are

inserted, and the public <deny>
rule is omitted because it is now superfluous. I think allowFirst will be fine this way.

History

#1 - 05/19/2009 04:44 PM - Jing Tao

I changed the default type from "denyFirst" to "allowFirst" in Access.java class. I also change the logic of getPageData method in this class.

The logic will apply to both denyFirst and allowFirst, both top level and entity level access subtrees:

1. If the doc is not public readable and also there are NO other rules, a explicit public readable deny rule will be added. Program will stop here and orderedMap will be returned.
2. If the doc is public readable, a public readable allow rule will be added to orderedMap.
3. If there are some other rules, the other rules will be added to orderedMap.

If a data file couldn't be read by public, but could be read by jtao. The final access rule will be:

<distribution>
<online><url>http://foo.org/tao.123.1</url></online>
<access authSystem="knb"
order="allowFirst"><allow><principal>uid=jtao,o=NCEAS,dc=ecoinformatics,dc=org</principal>
<permission>read</permission>
</allow>
</access>
</distribution>

If you see any problem in this logic, please let me know. I also will do more testing.

#2 - 05/19/2009 05:14 PM - Jing Tao

Matt pointed out the deny public access rule should only apply for the entity level (case 2). In case 2, top access section should be omitted.

I totally agree. The reason I didn't do that is because if i click Documentation|Access Information button, a Access page will be shown up, if the returned orderMap is null or empty (the case omitting the subtree) and I click okay button in this page, morpho will complain it. So I added a deny rule there.

I can fix the issue.

#3 - 05/19/2009 05:40 PM - Jing Tao

Case 2 should be case 1 in the comment above.

#4 - 05/20/2009 12:29 PM - Jing Tao

The logic will apply to both denyFirst and allowFirst:

1. If it is top access and the doc is not public readable and also there are NO other rules, program will stop here and an orderedMap with null value will be returned. This means the entire top access section will be omitted.

2.If it is entity level access and the doc is not public readable and also there are NO other rules, an explicit public readable deny rule will be added. Program will stop here and orderedMap will be returned. This explicit access rule is used to overwrite the top access rules.

3. If the doc is public readable, a public readable allow rule will be added to orderedMap.

4. If there are some other rules, the other rules will be added to orderedMap.

Here is an example:
If a data file couldn't be read by public, but could be read by jtao. The final access rule will be:

<distribution>
<online><url>http://foo.org/tao.123.1</url></online>
<access authSystem="knb"
order="allowFirst"><allow><principal>uid=jtao,o=NCEAS,dc=ecoinformatics,dc=org</principal>
<permission>read</permission>
</allow>
</access>

</distribution>

#5 - 05/28/2009 04:33 PM - Jing Tao

Judith tested the fix and it worked good.

#6 - 08/12/2009 03:54 PM - Jing Tao

move to 1.7

#7 - 03/27/2013 02:25 PM - Redmine Admin

Original Bugzilla ID was 4084