OpenId

Your Rating: ☆☆☆☆☆ Results: ★★★☆☆ 84 rates

⚠ **In progress for 4.?**

Implementation tracked in MGNLOPENID@jira.

Initial thoughts from Gregory, quoted from the internal page related to the forum:

We can't build a "large" community if users have to register to yet another system. The most courageous already have a Jira id with us, and/or are subscribed to the list. We need to keep those guys around, and we need to get more new guys on board than the few who would register just-because-they-really-have-this-urgent-question.

This can be implemented as a LoginHandler in Magnolia. See for examplehttp://code.google.com/p/openid4java/wiki/QuickStart. This would also imply a different login form (google also had a great article on openid-enabled login forms - it HAS to be simple for the user: for example with something like http://jvance.com/pages/JQueryOpenIDPlugin.xhtml)
Most likely, logging in with an OpenID account will trigger the creation of a shadow account at Magnolia side. There are essentially two approaches:

- create a shadow account - assign default roles/groups like we do with P.U.R module - allows for further user management (change of roles /groups for a specific user, locking that user out, "preferences", etc)
- do not create a shadow account - all users logged in via OpenID will always have the same group/role assignment.

Current status

We have a draft openid module based on the OpenId4java APIS which implements:

- a specific loginHandler
- a jaas OpenIdAuthenticationModule
- an OpenIdUser + OpenIdUserManager
- a form login

the module takes care of the openid authentication when a special parameter "mgnlUserOpenID" is available in request (e.g. mgnlUserOpenID=http://www.google.com/profiles/_username_).

At the current state after the openid authentication the module automatically creates a new magnolia user, adding a specific role set in the module configuration.
This is probably not what we have to do however, since we need a way to identify the user on the magnolia website (for example, after logging in, we should probably have a unique login name used to sign forum posts or similar, and the only unique information we have here is the openid url, which is not nice...)

How to handle openid users?

Usually an openid login is associated to an existing account on the target system. The common flow is:

- John wants to register/login on a website
- the website allow a "normal" (userid+password) or openid-based registration
- John input his openId
- the website calls the OpenProvider (OP) for the url specified and requests authentication
- the website shows a registration form with some of the fields already set with values returned by the openid provider (e.g. mail e nickname - note that nickname may not be preserved, since it could be already used on the target system)
- John fills the form, and the website stores the association between the new user and his openid
- the website also allow john to add more openids linked to the same account
- for future logins, John can now use one of his openId urls instead of username/password

So the question is: should we follow a similar flow also for the openid when used in the forum module? This means that:

- the user will still have to register and choose a username
- we will store the new user in the magnolia repository, linking one or more openid urls to it

And the flow could be:

- ask the user to insert his openid
- if the openid is already known by magnolia then login
- if the openid is new than pop up with a registration form with at least a new username -> after filling it the magnolia user will be created and stored
- when the user is logged in it should be able to link more openid urls to his account

On the other hand, allowing a user to login without creating a magnolia "shadow" account is easier for the user, but on the forum there will be no way to identify a post by user "john" (different openid providers could return the username "john" associated with different users, or even the same mail address in case of malicious users...)

JAAS usage

Is a JAAS module required or it could be avoided?
Should we think about refactoring the default JAAS magnolia modules in order to make it easier to plugin different authentication/authorization handlers?

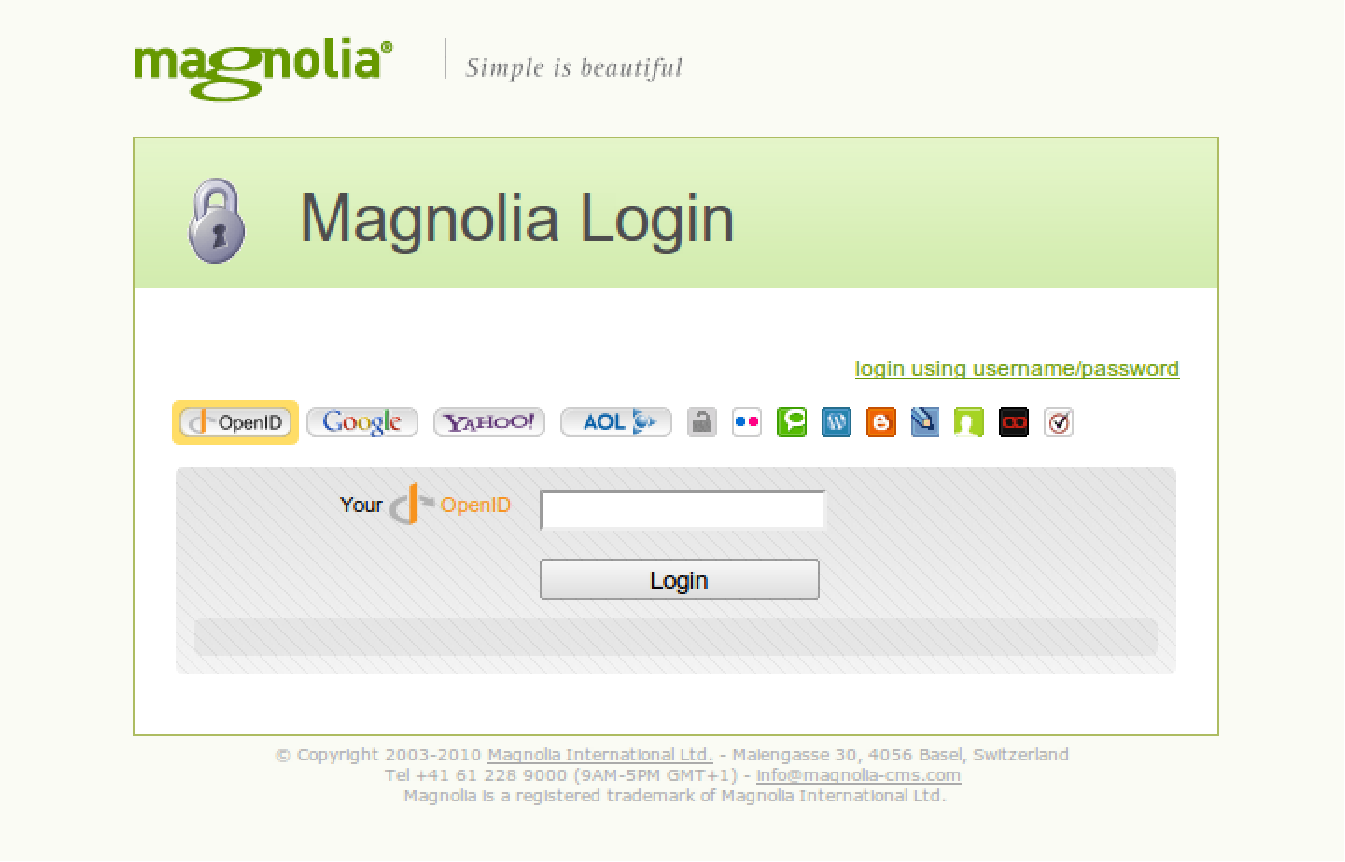
testing/developing using the openid module in svn

The module is available in svn at http://svn.magnolia-cms.com/svn/community/modules/magnolia-module-openid/trunk/

There is a ready to use test-webapp in svn, with svn:externals that link the modules required for development. If you want to give it a try:

```
svn checkout http://svn.magnolia-cms.com/svn/community/sandbox/externals/
cd externals
mvn install eclipse:eclipse
```

than load your projects in eclipse, configure the project "test-webapp" with a tomcat server and start.
Accessing http://localhost:8080/test/demo-project.html should bring you an openid-enabled login page.



Magnolia Login