Advanced role management

Description	Advanced role management
Type	administration
Status	DRAFT
Owner	TIB
Language	Java
Team	Graham Triggs
Location	tba
License	

Goals

- Develop frontend elements to create and administrate custom roles in VIVO

Description

Phase I: Discrete display / edit assertions to replace "and below" permissions for fields ✅

We want to have discrete assertions for saying that a role is able to display and/or edit a field, rather than the current hiddenFromDisplayBelowRoleLevelAnnot / prohibitedFromUpdateBelowRoleLevelAnnot. This will also involve changing admin screens that provide a display level / update level to allow for a checkbox based assertion of multiple roles, rather than a drop-down / radio button.

In changing over the assertions, it will still support modelling the same restrictions, but rather than saying – for example - ": hiddenFromDisplayBelowRoleLevelAnnot :EDITOR", it would require ":displayFor :EDITOR", ":displayFor :CURATOR", ":displayFor :DB_ADMIN", and ": displayFor :NOBODY".

Phase II: Create an upgrade script to replace the existing "and below" permissions ✅

In order to push these changes to existing triple stores, we will create a script process that will rewrite existing "DisplayBelow / UpdateBelow" assertions into the equivalent granting of rights to the existing roles. We will also update the default definitions in the home folder for creating a new Vitro / VIVO instance.

Phase III: Remove hardcoded references to role levels from the Java code ✅

Now, there shouldn't be anything left that assumes the inherited model of role authorisation. Once that is confirmed, we can externalise the role level definitions from the BaseResourceBean (and the PermissionSets uris?), and have the available roles defined entirely by configuration.

This would open up the possibility for defining more roles in the system (and giving them discrete permissions! – so one group of users might only edit publications, and another only grants). At this stage, new roles would be established in the configuration files, and become available on restart, although the field permissions could be updated within Vitro / VIVO.

Once the above is implemented, we would likely to be looking at making the changes available for Vitro (and the configuration for VIVO), subject to evaluation. Further developments then possibly include:

Phase IV: Role-oriented control panel for enabling/disabling permissions ✅

Simple control panel(s) for setting the permissions for roles across multiple fields, in addition to editing permissions on a field-by-field basis (a grid of checkboxes, fields on one axis, roles on the other.)

- Ontology editor ✅
- Page management (tbd.)

Phase V: Control panel for creating new roles

Ultimately, we may need to have a means for creating new roles within the application directly, not just establishing them in the configuration files to be reloaded on restarting VIVO, which would involve resolving issues around how PermissionSets are loaded.

Features (tbd.)

- Clone roles

- Edit roles
- Delete non-default roles (not self-editor, editor, curator etc.)
- import and export of roles, including set of rights

Documentation

Ticket: Unable to locate Jira server for this macro. It may be due to Application Link configuration.

Where do roles appear in VIVO?

User Account Management

- Generate dynamic list of all existing roles
- Test, if multiple roles are shown in the user account table

blocked URL

Ontology editor ✅

- Develop a matrix / table view to allow to administrate the set of rights belonging to a property or class in the ontology editor.
- Checkboxes for each role for all the three permissions (display, update, publish)

Display permissions for this property
☑ Site Admin ☑ Curator ☑ Editor ☑ Self Editor ☑ Public

Update permissions for this property
☑ Site Admin ☑ Curator ☑ Editor ☑ Self Editor ☐ Public

Publish permissions for this property
☑ Site Admin ☑ Curator ☑ Editor ☑ Self Editor ☑ Public

SiteAdmin

- New menu item: Role management

blocked URL

Page Management

Control the permission to display web pages. Menu similar to Ontology Editor integration.

blocked URL

Notes

- This idea was discussed at the VIVO meetup at SWIB 2017
- Proposal for advanced role management in vivo-tech mailing list, including discussion.