

Permissions in Plone

Jeremy M. Smith <jeremy@ucdavis.edu>

Plone Users Group of Davis

March 2007

The Problem



The Problem

- Lots and lots of little moving pieces!

Warning

- I don't know what I'm talking about.

The Players

- Permissions (are assigned to)
- Roles (are assigned to)
- Users/Members (can be combined into)
- Groups (are automated by)
- Workflow

Permissions

- Based in Zope
- Very Fine-grained (overly so?)
 - If you're a product developer, please be kind!
- Managed through the ZMI Security tab
- Auto-managed by Workflow
 - i.e., Why doesn't my new content object just inherit from its parent?

Browser address bar: http://mindbrain.ucdavis.edu/manage

Navigation icons: Home, Back, Forward, Stop, Refresh

Menu items: Cookies, CSS, Forms, Images, Information, Miscellaneous, Outline, Resize, Tools, View Source, Options

Search bar: Search or Tag here

Google search bar: Zope on http://mindbrain.ucdavis.edu

- Root Folder
- about
- acl_users
- archetype_tool
- discover
- events
- give
- intranet
- labs
- Beer
- Bunge
- Corina
- Mangun
- Miller
- Links
- News
- Participate
- People
- Positions
- Research and I
- Selected Public
- acl_users
- copy_of_Select
- copy_of_edit
- Oakes
- Swaab
- Whitney
- mimetypes_regist
- news
- participate
- people

Navigation tabs: Contents, View, Properties, Security, Undo, Ownership, Interfaces, Find, Workflows

Plone Site at /

The listing below shows the current security settings for this item. Permissions are rows and roles are columns. Checkboxes are used to indicate where roles are assigned permissions. You can also assign **local roles** to users, which give users extra roles in the context of this object and its subobjects.

When a role is assigned to a permission, users with the given role will be able to perform tasks associated with the permission on this item. When the *Acquire permission settings* checkbox is selected then the containing object's permission settings are used. Note: the acquired permission settings may be augmented by selecting Roles for a permission in addition to selecting to acquire permissions.

Permission	Roles	Anonymous	Authenticated	Manager	Member	Owner	Reviewer
Acquire permission settings?							
<input checked="" type="checkbox"/> ATContentTypes Topic: Add ATBooleanCriterion		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> ATContentTypes Topic: Add ATCurrentAuthorCriterion		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> ATContentTypes Topic: Add ATDateCriteria		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> ATContentTypes Topic: Add ATDateRangeCriterion		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> ATContentTypes Topic: Add ATListCriterion		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> ATContentTypes Topic: Add ATPathCriterion		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> ATContentTypes Topic: Add ATPortalTypeCriterion		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> ATContentTypes Topic: Add ATReferenceCriterion		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> ATContentTypes Topic: Add ATRelativePathCriterion		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> ATContentTypes Topic: Add ATSelectionCriterion		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Acquire?							
<input checked="" type="checkbox"/> ATContentTypes Topic: Add ATSimpleIntCriterion		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> ATContentTypes Topic: Add ATSimpleStringCriterion		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> ATContentTypes Topic: Add ATSortCriterion		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> ATContentTypes: Add Document		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> ATContentTypes: Add Event		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> ATContentTypes: Add Favorite		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> ATContentTypes: Add File		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Permissions (cont)

- 5 “biggies”:
 - View (see an object TTW)
 - Modify portal content (edit)
 - Access contents information (see properties of an object)
 - List folder contents
 - Manage portal

Permissions (cont)

- Usually inherited (acquired) from a higher level
 - “Acquire” checkbox
- Arbitrary, Case-sensitive strings
 - You often must look to the source
 - look for “declareProtected”

Roles

- Based in Zope, ZMI Security tab
- You grant Permissions to Roles, not Users
- Functional constellations of Permissions
- Make permissions less unmanageable

Browser navigation bar showing address http://mindbrain.ucdavis.edu/manage and various toolbars including Cookies, CSS, Forms, Images, Information, Miscellaneous, Outline, Resize, Tools, View Source, and Options.

- Root Folder
- about
- acl_users
- archetype_tool
- discover
- events
- give
- intranet
- labs
- Beer
- Bunge
- Corina
- Mangun
- Miller
- Links
- News
- Participate
- People
- Positions
- Research and I
- Selected Public
- acl_users
- copy_of_Select
- copy_of_edit
- Oakes
- Swaab
- Whitney
- mimetypes_regist
- news
- participate
- people

Navigation tabs: Contents, View, Properties, Security, Undo, Ownership, Interfaces, Find, Workflows

Plone Site at /

The listing below shows the current security settings for this item. Permissions are rows and roles are columns. Checkboxes are used to indicate where roles are assigned permissions. You can also assign **local roles** to users, which give users extra roles in the context of this object and its subobjects.

When a role is assigned to a permission, users with the given role will be able to perform tasks associated with the permission on this item. When the *Acquire permission settings* checkbox is selected then the containing object's permission settings are used. Note: the acquired permission settings may be augmented by selecting Roles for a permission in addition to selecting to acquire permissions.

Permission	Roles					
	Anonymous	Authenticated	Manager	Member	Owner	Reviewer
Acquire permission settings?						
<input checked="" type="checkbox"/> ATContentTypes Topic: Add ATBooleanCriterion	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> ATContentTypes Topic: Add ATCurrentAuthorCriterion	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> ATContentTypes Topic: Add ATDateCriteria	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> ATContentTypes Topic: Add ATDateRangeCriterion	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> ATContentTypes Topic: Add ATListCriterion	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> ATContentTypes Topic: Add ATPathCriterion	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> ATContentTypes Topic: Add ATPortalTypeCriterion	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> ATContentTypes Topic: Add ATReferenceCriterion	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> ATContentTypes Topic: Add ATRelativePathCriterion	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> ATContentTypes Topic: Add ATSelectionCriterion	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Acquire?	Anonymous	Authenticated	Manager	Member	Owner	Reviewer
<input checked="" type="checkbox"/> ATContentTypes Topic: Add ATSimpleIntCriterion	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> ATContentTypes Topic: Add ATSimpleStringCriterion	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> ATContentTypes Topic: Add ATSortCriterion	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> ATContentTypes: Add Document	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> ATContentTypes: Add Event	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> ATContentTypes: Add Favorite	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> ATContentTypes: Add File	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Roles (cont)

- Zope Defaults:
 - Anonymous
 - Authenticated
 - Manager
 - Owner

Roles (cont)

- Plone Adds:
 - Member
 - Reviewer
- Plone 3 will Add (see PLIPs #26, 134):
 - Editor
 - Reader




Roles (cont)

- Zope “local roles” == Plone “Sharing” tab
- Assign roles to users or groups for only part of your site

Current sharing permissions for Intranet

You can share the rights for both entire folders and single items. These users have privileges here:

Assigned Roles for Intranet

<input type="checkbox"/>	Name	Type	Inherited Role(s) (inactive)	Local Role(s)
<input type="checkbox"/>	 jeremy (Jeremy M. Smith)	User		Owner
<input type="checkbox"/>	 staff	Group		<input type="checkbox"/> Reviewer
<input type="checkbox"/>	 admin	User	Owner	

Roles to assign to selected user(s)/group(s)

Manager Member Reviewer

Add sharing permissions to users

Sharing is an easy way to allow others access to collaborate with you on your content. To share this item, search for the person's name or email address in the form below, and assign them an appropriate role. The most common use is to give people Manager permissions, which means they have full control of this item and its contents (if any).

Search Terms

Search by

Users/Members

- Zope has Users
- Plone “wraps” Zope users to create Members
- Allows for additional properties and methods (beyond username and password)
- “Wrapping” is in flux right now (PAS)
- Roles are assigned to Users/Members

Groups

- Plone bolt-on to Users/Members
- Allows granting roles to multiple users simultaneously
- Not really necessary for most sites, but can be handy for sites with lots of users with different responsibilities

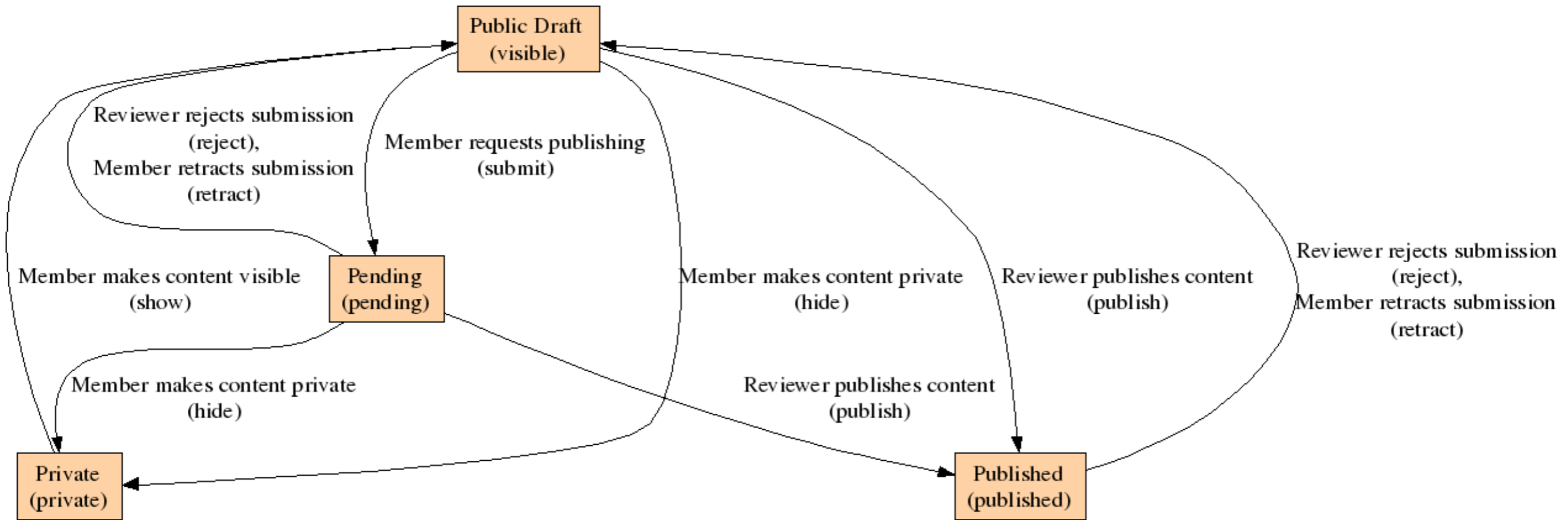
Workflow!

- Based in Plone
 - `portal_workflow` tool
 - Placeful Workflow bolt-on
- Automates Permissions, Roles, and Groups
- Workflows are assigned per Content Type
- With PW, can differ for different folders

Workflow (cont)

- The Right Place(tm) to make most security changes in Plone
 - if you want them to be consistent
- Creating your own from scratch is not a light undertaking: consider copy-and-modify
- Can be created visually using UML and ArchGenXML

Plone's Default Workflow



Workflow (States)

- A workflow defines States for content types
 - e.g., Public Draft, Private, Published
 - A mapping of Permissions to Roles
 - Can map Groups to Roles locally (handy!)

 Workflow State at /Plone/portal_workflow/plone_workflow/states/pending

When objects are in this state they will take on the role to permission mappings defined below. Only the [permissions managed by this workflow](#) are shown.

Permission		Roles					
Acquire permission settings?		Anonymous	Authenticated	Manager	Member	Owner	Reviewer
<input checked="" type="checkbox"/>	Access contents information	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Change portal events	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Modify portal content	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	View	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Workflow (Transitions)

- A Workflow defines Transitions between States
 - e.g., Submit, Publish, Hide
 - “Guards” limit who can initiate a Transition by Role and/or Permission
 - Bonus: Guard Roles are semicolon separated!
- Can initiate Scripts before or after Transition, e.g., send email when content is changed

Workflow Transition at /mindbrain/portal_workflow/plone_workflow/transitions/publish

Id	publish		
Title	<input type="text" value="Reviewer publishes content"/>		
Description	<input type="text"/>		
Destination state	<input type="text" value="published"/>		
Trigger type	<input type="radio"/> Automatic <input checked="" type="radio"/> Initiated by user action <input type="radio"/> Initiated by WorkflowMethod		
Script (before)	<input type="text" value="(None)"/>		
Script (after)	<input type="text" value="(None)"/>		
Guard	Permission(s) <input type="text" value="Review portal content"/>	Role(s) <input type="text"/>	Group(s) <input type="text"/>
	Expression <input type="text"/> [?]		
Display in actions box	Name (formatted) <input type="text" value="Publish"/>		
	URL (formatted) <input type="text" value="%(content_url)s/content_publish_form"/>		
	Category <input type="text" value="workflow"/>		

Workflow (Misc)

- Worklists are simple, canned Catalog queries to search on Workflow State
 - e.g., Review Portlet is built from such a worklist
- Variables are Python or TALES expressions that are evaluated for each Transition in a Workflow
 - e.g., Review History
 - Can be queried from the Catalog

Workflow (cont)

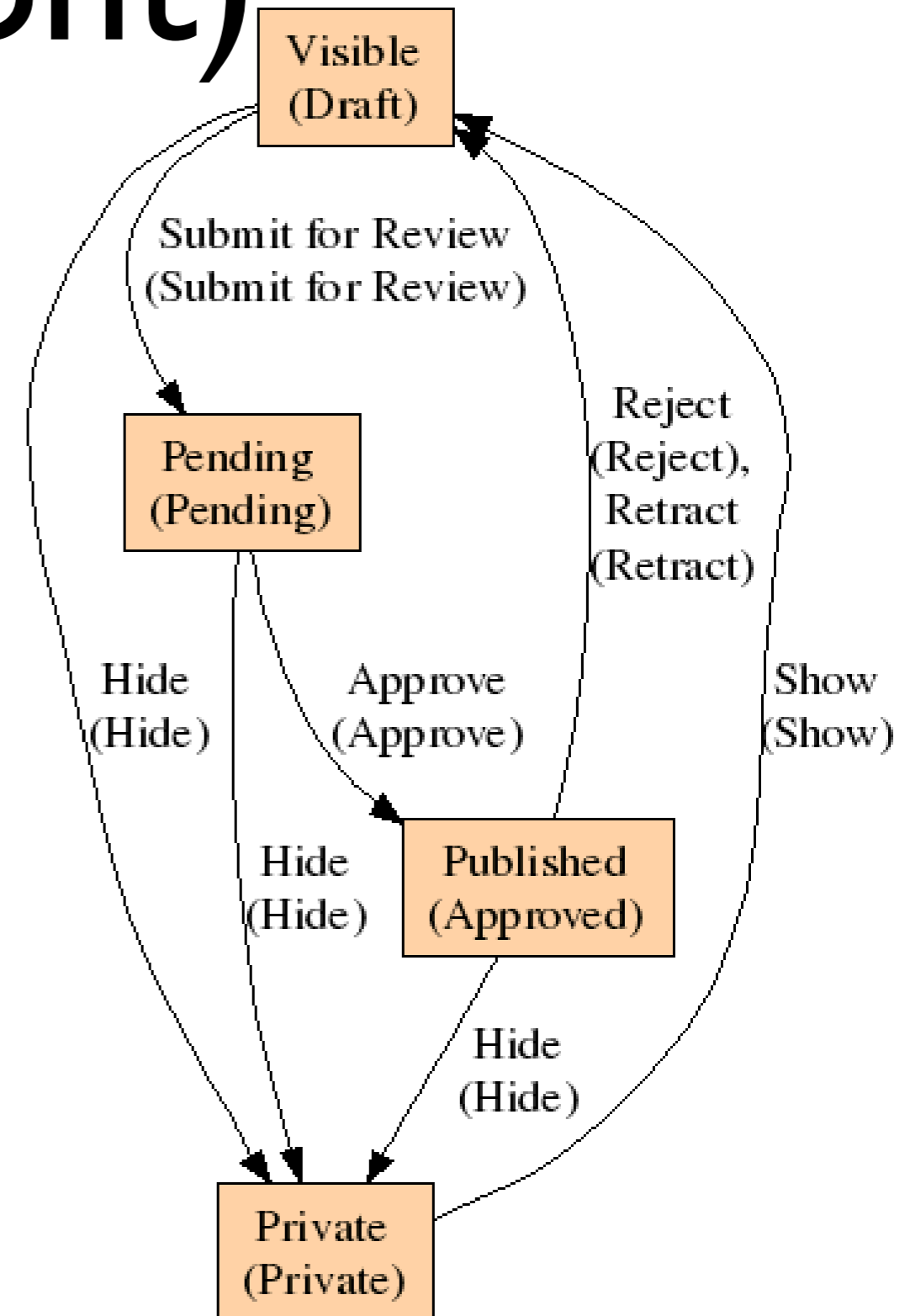
- Future Plone will ship with additional workflows for common use cases
 - Intranet, Simple, etc.
- In combination with new roles (Editor, Viewer), will be much more useful out of the box
 - see PLIPs #26, 134

Workflow Tools

- Placeful Workflow (ships with Plone)
 - Without PW, each Content Type can be assigned a Workflow for an entire Plone site
 - With PW, you can override the global settings on a per-folder (or tree) basis.
 - e.g., have a different Workflow for your Intranet folder than the rest of your site

Tools (cont)

- DCWorkflow Graph
- Gives nice workflow diagrams within the ZMI



Tools (cont)

- DC Workflow Dump
 - Dumps a TTW workflow out to Python code for use in products
 - Makes it much easier to tinker until you have the behavior you want

Tools (cont)

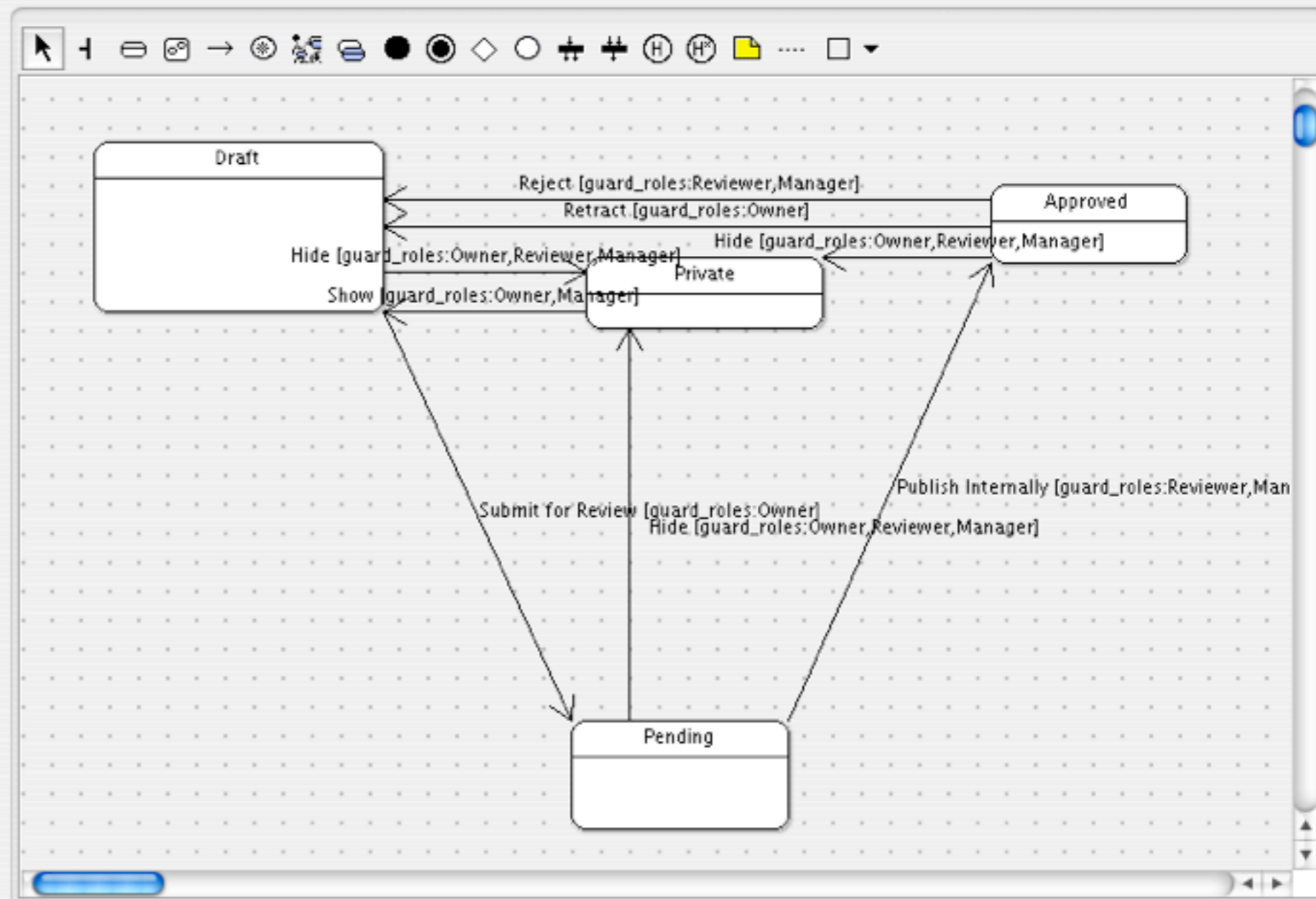
- UML and ArchGenXML can be used to create new Workflows visually
- Great if you are associating Workflows with new AT Content Types you create
- Can also create generic workflows (by assigning to a <<stub>> class)



Package-centric

Order By Type, Name

- TD widget:description_msgid
- TD widget
- TD widget:i18n_domain
- TD widget:label
- TD widget:label_msgid
- TD widget:type
- TD worklist
- TD worklist:guard_permissions
- TD worklist:guard_roles
- TD write_permission
- TD i18ncontent
- TD access
- TD modify
- TD (unnamed TagDefinition)
- TD Add portal content
- ▼ (unnamed Class)
 - ▼ Intranet Workflow
 - Intranet Workflow
 - ▼ Private
 - Hide: Hide [guard_roles:Owner,Reviewer,Manager]
 - Hide: Hide [guard_roles:Owner,Reviewer,Manager]
 - Hide: Hide [guard_roles:Owner,Reviewer,Manager]
 - Show: Show [guard_roles:Owner,Manager]
 - ▶ Pending
 - ▶ Draft



As Diagram

By Priority 5 Items

- High
- Medium
- Low

◀ **ToDo Item** Properties Documentation Presentation Source Constraints Stereotype Tagged Values ▶

No ToDoItem selected

< Back Next > Finish Help

References

- Understanding permissions and security, Martin Aspeli
- <http://plone.org/documentation/tutorial/understanding-permissions>
- ArchGenXML Getting Started guide
- Plone Live!, Pelletier and Sharif, et al

Thanks!