Module: User management and authentication options

Module overview:
This module builds upon the module ‘An introduction to users and groups’ which introduced the concept of authentication and authorization. The management of groups will be discussed, and this knowledge will be consolidated by creating a new administrator and adding and removing their administrative privileges.

Advanced authentication options such as LDAP, Shibboleth and IP authentication will be briefly introduced.

Module objectives:
By the end of this module you will:

1. Understand the concepts of authentication and authorization
2. Fully understand user and group management in DSpace
3. Have added and removed users from groups
4. Have a high level understanding of some advance authentication options

Note
For the practical exercise, please refer to your sheet ‘Local instructions’ for details of the following:

- How to launch a web browser
- What the URL of your DSpace installation is
Concept: Authentication and Authorization

Two important concepts:

- Authentication (AuthN)
  - The process of establishing the identity of a user

- Authorization (AuthZ)
  - The granting of privileges to a user to perform an action on a resource

Authentication

Authentication (often shortened to AuthN) relates to the process of establishing the identity of a user. In DSpace, this requires the user to log in and identify themselves, typically with a password.

Authorization

Authorization (often shortened to AuthZ) relates to the privileges that a user may be given in order to do something to (for example read, write or delete) a resource.
**User creation and management**

- **User creation**
  - Covered in module ‘An introduction to users and groups’

- **User management**
  - Modify users
    - Administer menu -> E-People -> Select E-person -> Edit
  - Delete users
    - Administer menu -> E-People -> Select E-person -> Delete...

**Users**

In DSpace, users are referred to by the term ‘E-Person’. The creation of users is covered in the module ‘An introduction to users and groups’.

**User management**

Users can have their details edited, and can be deleted. These are both done via the ‘E-People’ menu option in the ‘Administer’ menu. First, select a user to manage, and then either edit their details, or delete them from the system.
Referential integrity

- Referential integrity
  - Database theory of relational databases
  - Data cannot be deleted if it referred to elsewhere
  - So...
  - Users cannot be deleted if they own anything
    - Submitted items
    - Items in a workflow
    - Items part way through submission
  - This maintains the integrity of the data

Referential integrity

DSpace uses a relational database to store its metadata. Relational databases store different types of information in different ‘tables’ and then relate these to each other. For example users are stored in the ‘eperson’ table. When a user submits an item, their entry in the eperson table is related to the submission. This means that if a user changes their telephone number it only has to be changed once in the eperson table rather than duplicating the users details with every submission.

These relationships are enforced by the database. What this means is that you are not able to delete users from DSpace if they have a relation with another database table. If a user has submitted any items, has items in a workflow, or items partially submitted, then these relationships will exist.
Group creation and management

- Group management
  - Administer menu -> Groups
  - Create new groups ‘Create New Group’ button
  - ‘Edit’ or ‘Delete’ groups
  - Users or groups can be members of groups

Group creation

New groups can be created by following using the ‘Groups’ link in the ‘Administer’ menu. Each group requires a name, and some members. Members can be users or other groups. Sometimes it is useful to use a hierarchy of groups. One example of this would be to have a group for each member of a research group. That group can be given privileges to submit to their research outputs collection. That group can then be combined with the groups for the other research groups in a department into a departmental group. That departmental group might be given read privileges on a private collection of departmental administrative documents.

Edit and delete groups

The name of groups and their memberships can be easily changed by using the ‘Edit’ button next to the group name. Groups can be deleted by using the ‘Delete’ button next to the group name.

Note the previous comment about referential integrity. This also applies to the deletion of groups that are referred to in an authorization policy or workflow.
Item authorizations

To edit the authorizations on a particular item, log in as an administrator, and fine the item that you wish to edit. Select the ‘Edit…’ button, and then the ‘Edit’ button next to the label ‘Item’s authorizations’.

You will be presented with a page where you can edit the policies for:

- The item
- Each bundle
- Each file in each bundle
Only groups (not users) can be granted rights. Rights which can be assigned are:

- ADD
- REMOVE
- READ
- WRITE

ADD and REMOVE cannot apply to files as you cannot ADD a new file to an existing file, or REMOVE a file from an existing file. Adding or removing files lays at the bundle level.

The ANONYMOUS group can be used when you want to grant anonymous access. This is normally only for READ privileges.
Collection authorizations

To edit the authorizations on a collection, log in as an administrator, and find the collection that you wish to edit. Select the ‘Edit...’ button, and then the ‘Edit’ button next to the label ‘Collection’s authorizations’.

You will be presented with a page where you can edit the policies for the collection. Policies can be added for the following roles:

- **READ / WRITE / ADD / REMOVE** – items in the collection
- **DEFAULT_ITEM_READ / DEFAULT_BITSTREAM_READ** – These are typically used for the anonymous user in order to say that you wish by default (unless overridden by an item’s authorization policies) for items or bitstreams to have READ access
- **COLLECTION_ADMIN** – To grant a user or group the rights to edit items, edit the submitters to the collection, map items and withdraw items.
Practical exercise - edit group membership

Create a new user
- [dspace]/bin/create-administrator
- Log in to ensure they are an administrator
- Remove them from the Administrator group
- Log back in to ensure the user is not an administrator anymore

Create a new administrator
Create a new administrator using the instructions provided in the module ‘An introduction to users and groups’. You will need to use the script [dspace]/bin/create-administrator. Log in as the new user you created to ensure that they are an administrator.

Change user privileges
Log back in as your original user and remove the new user from the administrators group. Log out, and log back in to ensure that your user is no not an administrator anymore.
Alternative authentication systems - LDAP

- LDAP
  - Lightweight Directory Access Protocol
  - Most institutions run an LDAP system to provide a central user password system
  - Active Directory has an LDAP interface
  - Users can be created using LDAP queries
  - Passwords not stored in DSpace

LDAP

LDAP is a common directory service which can be used to authenticate users. Many institutions run an LDAP server of a Microsoft Active Directory Service which has an LDAP interface.

Configuring LDAP is covered in the module ‘Configuring DSpace and LDAP’.
Alternative authentication systems - Shibboleth

- Shibboleth
  - A devolved authentication system
  - Allows users to log in to systems outside their institution
  - A user’s local institution performs the authentication

Shibboleth

Shibboleth is an implementation of a devolved authentication model where applications such as DSpace establish a trust relationship between institutions in order to allow users to log in to services at other institutions. The authentication is devolved to the user’s local Shibboleth service which then sends them back to DSpace with the relevant authentication details.

Shibboleth can also be used to provide a single-sign-on system within an institution so that once a user has logged in to the Shibboleth system they get seamless access to other Shibboleth protected systems without having to log in again.
Alternative authentication systems – IP authentication

- IP authentication
  - IP address of user (no login required)
  - If the IP address matches (e.g. is ‘on campus’) then the user becomes a member of a special group (e.g. ‘Internal-users’).
  - That group can be assigned privileges
  - Can be used to protect internal resources, and fallback to a requiring a login
    - Stackable authentication

IP authentication

IP authentication can be used to protect materials depending on the user’s IP address. If their address matches a known pattern then the user will be assigned to a special group. That group can be granted privileges.
Credits

- These notes have been produced by:
  - Stuart Lewis & Chris Yates
  - Repository Support Project
    - http://www.rsp.ac.uk/
  - Part of the RepositoryNet
  - Funded by JISC
    - http://www.jisc.ac.uk/