Group Service

Background

Newcastle University Grouper groups represent a common identifier for a group of people. Each group has its own unique identifier in accordance to the naming convention set out in this document to ensure consistency in the naming of groups throughout Grouper and the Active Directory (AD). Groups are automatically provisioned based upon institutional data, created by system administrators to represent personal groups which are not represented as part of institutional data, or a combination of both approaches. A group is represented by a unique group ID, a name, description, a provision attribute and a list of direct members identified by NCL login ID's (nuser@ncl.ac.uk) or indirect members identified by group ID's.

The Grouper group service is positioned to help complement the current access groups stored within the University's AD by making it possible to delegate access to resources based on Institutional data i.e. all of HR can access the HR wiki. It provides a central location to create, manage and integrate groups with applications via a number of authentication methods such as Shibboleth, provisioning of groups into the AD and feeding groups into 3rd party applications via data integration methods available as part of the IDFS service (http://www.ncl.ac.uk/iss/services/data-service/).

All University staff members with a NCL login ID have view access to the Groups service, which is accessible at https://groups.ncl.ac.uk. Computing officers or System Administrator who are interested in integrating the Groups service with their applications can request an area within Grouper which will allow them to create and manage groups. Requests should be logged via helpline@ncl.ac.uk.

Main Group Structure

The group structure within Grouper has been designed to encourage a philosophy of re-use. In order to encourage this, groups have been categorised into three categories, corporate data groups, user groups and application groups. There is an implied flow throughout these types of groups with the corporate data groups representing University structures; user groups are able to use these groups to create custom user lists, before finally application groups can make use of a mixture of both Corporate Data and User groups.

Corporate Data *groups are non-editable groups which have been automatically provisioned using Institutional data from Student Management and HR systems or other corporate data sources.*

User *groups are created by computing officers/systems administrators to represent groups of people which are not represented in Institutional data sources i.e. research groups. These are editable by the creator of the group and users who have been delegated appropriate privileges on the group.*

Application *groups are the groups which are referenced to control access to applications and resources i.e. wikis, file stores. These are editable by the creator of the group and users who have been delegated appropriate privileges on the group.*

Sub Group Structure

Each school/department using the group service are setup with an area under User Groups and Applications. These areas are structured to reflect the overall University hierarchy, organising

Group Service

departments/schools under faculties and centralised org units. For example, if the Library request to start using the group's service, the following two areas would be created,

User Groups – Professional Support Services – **Library**

Applications – Professional Support Services - **Library**

Administrator privileges for these areas are by default assigned to the main system or application administrator; they are able to delegate privileges to other users who need to create/manage groups. If the system administrator is not the person responsible for the groups and therefore does not require administrator privileges, a request can be made to assign admin privileges to a more appropriate user.

Under the Applications stem, by default, there will also be a "Web Protected Applications" area; this is where any groups which are to be used in conjunction with Shibboleth should be created. These will, by default, be provisioned into the AD, so that Shibboleth can use the groups.

Group Integration

Groups which are created and managed as part of the group service are accessible via Shibboleth and the AD. Groups can also be ported into third party applications/systems which are not interoperable with Shibboleth or the AD. An example of this is one of the room booking solutions used at Newcastle University, Syllabus Plus. Control over who can book particular rooms must be exercised based upon an individual's position and role within the organisation, in effect requiring a form of role based access control, which Grouper was able to provide. These roles and associated memberships were then needed to be imported into Syllabus Plus; this was achieved by setting up a direct data flow between Grouper and Syllabus Plus. If you have any use cases which may need a similar approach, please contact helpline@ncl.ac.uk and we can discuss possible approaches.

Groups which are to be accessible via Shibboleth or the AD for authentication and authorisation are to be provisioned and stored within the AD. This will be the primary source for querying groups, where possible. Groups and their respective memberships can still be queried when required directly from the group service via the database, or secured web services.

Only groups which are created within the Applications stem and have the provision attribute set to true are to be provisioned into the AD. Groups that are created within Corporate Data and User Groups stem are not provisioned directly. Corporate Data and User Groups can be provisioned indirectly to the AD, by creating a group in the Applications stem and making the appropriate Corporate Data or User Groups group a member of this newly created group.

Group Naming

The naming of groups is important to ensure the consistency and uniqueness of group identifiers between Grouper and Active directory groups. The main importance is that the group identifier defines the organisation/department responsible for the group and the purpose of the group. The naming convention has most significance in the groups that are created within the Applications stem, as these which will be provisioned into the AD.

Group Service

Corporate Data Groups

Groups which are provisioned based upon Institutional Data do not have a pre-determined naming convention as they will not be provisioned into the AD. Yet it is still important that these groups are given an identifier that clearly defines the group's purpose and are created within an identifiable structure. The groups are organised into stems that communicate the type of data they represent, i.e. Student Data, Org Structure.

Example – A group to represent all postgraduate research students within the Chemical Engineering and Advanced Materials school would be represented by;

Corporate Data:Student Data:Students to School: CEAM Postgraduate Research

User Groups

Groups which are created within User Groups, although not provisioned into the AD, do still need to follow a naming convention. The naming convention is to distinguish the department/school that the group belongs to and to also define its purpose. This is important as departments/school may create groups with the same name, an example of this would be a group which represents a school's Computing Officers. If numerous schools create a "Computing Officers" user group, when a user searches for their Computing Officers group they could be presented with a list of numerous instances of the same named group.

To avoid this scenario, the following convention should be followed for all User Groups;

<Owning School/Department>_<Name of Group (Group Purpose)>

NB. The group ID cannot include spaces, if the Group Purpose is more than one word please replace spaces with an underscore character.

Examples

- **ISS_Change_Management_Board**
- **LIBR_Admin_Staff**
- **SLAW_Computing_Officers**

These examples clearly distinguish the owner of the group, and the group of people that it represents. The school/department should be the abbreviation (without the leading D-) that is assigned to your school/department within SAP for example COMP (Computing science), LIBR (Library).

Although the group name has the school/department code as part of its name, it is still important that groups are appropriately structured within Grouper. The structuring of the groups into appropriate school/department stems and any child stems created within these stems, ensures that delegation of group control can be carried out effectively.

Applications

These are the groups which are provisioned into the AD, and therefore need to adhere to a defined naming convention in order to be successfully provisioned into the AD.

Group Service

The group id is split down into three defining sections;

- **Owning department/school** – The school/department should be the abbreviation (without the leading D-) that is assigned to your school/department within SAP for example COMP (Computing science), LIBR (Library).
- **Auto** – the word “Auto” needs to be included within any group that is to be provisioned into the AD. Although not auto generated in terms of the groups service, this identifies the group in the AD as being automatically generated and therefore management of the group should be carried out within the group’s service.
- **Group Purpose** – this should provide a clear purpose for the group, so that users are able to quickly distinguish what the group represents.

< Owning department/school>_ **Auto**_< Purpose>

NB. The group ID cannot include spaces, if the Purpose is more than one word please replace spaces with an underscore character.

Examples

- **ISS_Auto_Helpdesk_Tools**
- **MATH_Auto_Staff_Filestore**
- **LIBR_Auto_Archived_Journals**