EOAS Help Desk

Guideline: Group management in Active Directory

Burner EOAS - 2017-06-21 - 0 Comments - in Guidelines

Overview

Groups in Active Directory are stored in LDAP containers as a group type. Membership in a group corresponds to functionality outside of Active Directory, usually permission-based access, in another service provided by the Department. Examples of group membership when used by services include:

- Membership in a "Faculty" group for access to shared files and folders on the network
- People who have access to a financial system are provided access by belonging to the "FInance" group.
- Individuals who no longer have an account in the system, but may return to the Department at a later date belong in a "Deactivated" group.

The purpose of this guideline is to identify how groups are managed in order to avoid potential conflicts in the purpose of a group and avoid disruption to services.

Defining Groups

Groups should be defined specific to a particular purpose. For example, a group of faculty members on a mailing list would be defined as a particular group. When defining a group, it is important that the group be defined specific to a particular application. It is tempting to define a group, such as "Geologists", and share that group between two services, but the definition of the group among multiple services creates a coupling between those services and could complicate how each service is managed in the future.

As an example, a group of "Undergraduates", may want a mailing list defined where social events could be announced and shared. The same group could be used to define access to files and folders shared through ownCloud. In the future, the undergraduate group may decide to communicate their events and share facilities with other undergraduate groups in other departments. Adding other groups to the mailing list will either; a) grant access to data that the other undergraduate groups should not have access to, or b) confuse anyone reviewing the group in Active Directory who wants to get a report of who has access to specific files/folders.

The solution is to follow a strict naming convention that is summarized as "service-group". Here are some examples:

"Atlas-Staff" - Staff members who should have access to the Atlas application.

"MailList-AllFac" - Faculty members who belong on the mailing list "allfac@eoas.ubc.ca"

"Share-Finance" - Finance staff who have access to a particular network share point.

...and so on.

Defining OU's in the Directory

Visually, it helps to separate service groups into separate OU's in the directory. In the case of the department's Active Directory server, the OU should be named according to the "service" part of the "service-group" naming convention. For example, under the Groups OU in Active Directory, the Group names will be:

- Groups\Atlas
- Groups\MailList
- Groups\Share

From this OU naming convention, a group of Finance people who share access to a particulare service called "Money" would belong to a group organized as:

- Groups\Money\Money-Finance

Defining Group Access (Read, Write, Execute, etc.)

In the case of the need to have sub-groups within a particular group, the naming convention should be extended with the particular group access, which would result in the format "Service-Group-Access". Returning to the example of a Finance group, with access to the system called "Money", there may be two sub-groups within the Finance group that have varying permissions. One sub-group in Finance may have "Update" access, and the other group will have "Review" access with no ability to make changes. In this example, the following names would apply (beginning from the top-level Groups folder):

- Groups\Money\Money-Finance-Update
- Groups\Money\Money-Finance-Review