

Many organizations have deployed Windows servers and Active Directory, and leveraged the powerful access control infrastructure in this platform to manage user access to data. This infrastructure uses security groups to control user access to resources:

- Groups are defined in Active Directory to reflect business functions or organizational structure.
- Groups are assigned rights to network resources, such as shares, folders and printers.
- Users are attached to groups based on their job requirements.
- Groups may be nested, to simplify management.

Over time, the number of groups grows, and in some organizations may surpass the number of users. Moreover, in dynamic organizations users frequently change responsibilities and are assigned new projects. This churn creates complexity:

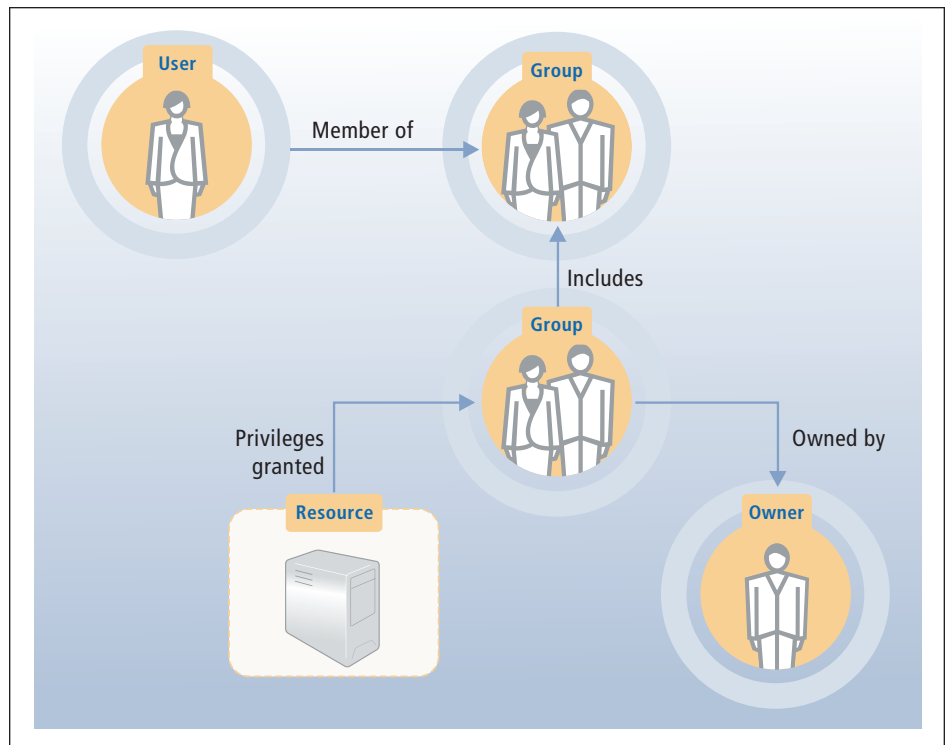
- Changing user requirements must be reflected in changes to user group memberships.
- A user access management team must be setup to respond to user access problems by attaching users to appropriate groups.
- Users are frequently unaware of the security infrastructure, so their calls to the help desk typically begin with: "I got an 'access denied' error..."
- Problem resolution is time consuming: first map the user's problem description to a network UNC, then find the groups with rights to that resource, then find owners for the groups, then call them to get permission to attach the user, and finally attach the user to the group.

This complexity leads to real business problems:

- Staffing cost in the user access management team, due to high call volumes.
- Long turnaround and lost productivity when users wait hours or days to get required rights.
- Users with inappropriate rights, as a result of failures in the change authorization process.

The complexity of group membership management can be greatly reduced by implementing a self service solution in place of the security administration group. Users are then be able to:

- Sign into an Intranet web application.
- Search or browse for the resource they would like to access.
- Request access rights directly.



The complexity of group membership management can be greatly reduced by implementing a self service solution in place of the security administration group.

Managing ACTIVE DIRECTORY GROUPS

- Automatically route requests to the appropriate authorizers, namely the owners of the appropriate AD security group.
- Use e-mail and web-based workflow to enable authorizers to approve requests directly.
- Automatically attach users to requested groups, upon approval.

This approach eliminates:

- The need for users to understand the security infrastructure.
- The cost of staffing a security administration team.
- Security exposures due to unauthorized group memberships.
- Lost productivity due to long delays in change authorization.

M-Tech's ID-Access provides an effective solution for self-service management of user membership in AD groups.

To learn more about ID-Access, please visit: <http://ID-Access.org>. To learn more about M-Tech and our suite of identity management products, please visit: <http://MTechIT.com>.



M-Tech Information Technology, Inc.
mtechit.com