Welcome to the LDAP Administration Console project website

Table of contents

1. Project Goal

The goal of this project is to provide a clean, secure, and ***easy*** to use web interface for enterprise OpenLDAP distributed directory administration. This includes User and Group administration as well as managing ACLs, OpenLDAP configuration, schema definitions, x509 certificate management, and more.

More important to this project than it's proposed feature set, is it's ease of use. LDAP Administration Console is intended to provide a means for individuals with limited, or no OpenLDAP experience to safely, and easily administer LDAP users, groups, sudoers, and even OpenLDAP server configuration, and deployment of distributed and replicated directories.

The combination of ease-of-use, secure design, and powerful feature-set will hopefully make this the OpenLDAP administration tool of choice for all users of OpenLDAP, from experts looking to save time, to LDAP novices simply looking to migrate away from NIS to a secure architecture.

2. Current Status

At the of time of this writing, the project has reached it's very first milestone, which is the release of version 0.1a. In this release, User and Group administration features are fully functional, and already make this interface usable for individuals seeking an easy means to add/remove/modify users and groups in LDAP; Allow users to change their passwords via web interface, and allow users to reset lost passwords without administrative assistance.

Currently in development, and possibly in CVS by the time you read this, are the additions of a SUDOer's plugin, and an ACL plugin.

3. Current Features

- Administrator designation by LDAP attribute; no need to update or modify configuration files as Administrators are changed/removed/added. Simply enable/disable their Administrative attribute through the LDAP Administration Console.
- Add, Modify, or Delete users easily.
- Automatically create user's home directories when accounts are created, and even populate them with skeleton directory contents.
- Reset passwords, either for a single user, or a list of users with just a few clicks; or direct the users to http://yourserver/ldapadmin/nosession.cgi and have them reset their password themselves! (password resets observe shadowLastChange and shadowMin values, so users will not be able to automatically reset their password within shadowMin days of

their last password reset.)
- Lock accounts, preventing access, while still retaining all account information, including UID information to prevent duplication

Note:

*It is generally preferable to lock users vs deleting users, as you may not wish to accidentally allow a new user to read/modify/execute files owned by a previous user by re-assigning the same UID. (For instance, lets say you have a user named "bob" with uid 1000 and for whatever reason, /usr/local/bin/suidbash has a facl assigned to it that permits u:bob:5. Now lets say bob leaves the company, and you delete the user. A month later, ray joins the company, and is assigned UID 1000; now ray can execute /usr/local/bin/suidbash, and that may be a **very bad thing**)*

- Automatically e-mails user password/account information on account creation or administratively reset password.
- Add, Modify, or Delete groups in seconds
- Change group memberships simply by clicking users in or out of a group

4. Future planned enhancements

Currently in progress:

- Currently there is only one Administrator type, and this Administrator type has access to perform all functions currently implemented in LDAP Administration Console.

  In a future version of LDAP Administration Console, there will be at least 3 admin types,

  - host-group admins: who will be permitted to add/remove EXISTING users from their specific host-group, or host-groups; permitting users added to those groups to authenticate ONLY to the hosts in those host-groups.
  - Org-group admins: who will be permitted to add and remove users from the LDAP directory, But like host-group Administrators, those users will only be permitted to login to hosts under the perview of the org-group admin; users will not be deleted entirely from LDAP until they are no longer members of any org-group.
  - Global Admins: who will be the equivilent of an Admin account currently, and be able to access all features of the LDAP Administration Console

  These admin classes may be implemented by permissions-masks, in lieu of named classes.
- ACL controls, Providing both direct control of OpenLDAP ACL definitions, or abstracted control, by providing interfaces to the intended result of an ACL i.e.

host-grouping, where hosts are simply lumped together and tied to user-groups; the ACLs making this work are hidden entirely and the result of limiting access to resources based on group membership happens "magically".

- LDAPv3 one-shot configuration. A painless OpenLDAP deployment "wizard" that makes LDAPv3 deployment and replication intuitive, and easy. Including Kerberos, SASL, x509, and multiple-platform-client configuration.

  Whereas the slapd.conf, and x509 PKI management are relatively strait forward, and shouldn't present much difficulty in developing, the client-configuration pieces are a bit more ambitious.

  My goal for client configuration is to have an interface that prompts for the fqdn of the host, the host-group to add the host too (optional), and a "go" button. The result of the operation will be a package that can be installed, and will contain the x509 certificate, ldap.conf, required files and libraries (i.e. PADL), scripts to update configuration files (i.e. nsswitch.conf, pam.conf, etc), and basically make adding a client no more a hassle than installing a single package.

  My knowledge is limited to pkg (AT&T package format used by solaris, and others) and rpm (RedHat, SuSE, UnitedLinux, and related), but I'm sure there are those out there that can facilitate me in developing lpp (AIX), deb (debian, and related), swpackage (hp-ux), and perhaps even windows (via samba authentication) installer creation scripts. (and facilitate in identifying and working through OS quirks to make the package work "out-of-the-box").
- Much more, but I don't want to get ahead of myself... 8-)

5. Download at sourceforge.net

The 0.1 alpha release may be downloaded at sourceforge.net