UseLDAPToPasswordProtectAFolder

Use LDAP to password protect a Folder

In this How-To guide, we will show you how to add LDAP authentication to your Apache 2.2 web server.

Prerequisites

For this you are going to need the following ::

OpenLDAP	http://www.openldap.org/software/download/	OpenLDAP is going to be our LDAP Server.
Apache HTTP Server	http://httpd.apache.org/download.cgi	Apache HTTP Server...

Here we will show you how to add the required statements in a VirtualHost. This is the example VirtualHost stanza

```
<VirtualHost *:80>
Servername www.myserver.com
DocumentRoot /home/www

<Directory "/home/www">
Options FollowSymLinks Includes
AllowOverride None
Order allow,deny
Allow from all


# -- LDAP Auth Begins Here -- #

AuthType Basic
AuthName LDAP_Auth_Test
AuthBasicProvider ldap
AuthLDAPBindDN         cn=apacheldap,dc=mydomain,dc=com
AuthLDAPBindPassword    letmein
AuthLDAPURL ldap://localhost/dc=mydomain,dc=com?cn?sub
Require valid-user

# -- LDAP Auth Ends Here -- #

</Directory>
</VirtualHost>
```

Some of the statements may look familiar to you, as you may have used them for authentication in the past.

In the example below we will be using a specific account in LDAP to allow Apache to 'bind' to LDAP in order to authenticate all incoming requests. For this you will need to create one such account, we use the example 'apacheldap' below. Do not use an administrative account for this purpose; only read access is required.

LDAP Directives

We will now step though each line of the LDAP authentication stages, and explain what they do:

AuthType Basic	This line tells apache to use Basic authentication. This sends the user's password in plain text and should normally only be used with SSL.
AuthName LDAP_Auth_Test	This is the realm name that will be displayed in the login box presented by your browser.
AuthBasicProvider ldap	This line instructs apache to use only LDAP for authentication. You can have multiple entries on one line, if you want to use multiple methods, but that is beyond the scope of this document.
AuthLDAPBindDN	Bind to the LDAP server for all operations using a specific user ID. In this case we will use *cn=apacheldap,dc=mydomain,dc=com* (this is the account we mentioned earlier in the document).
AuthLDAPBindPassword	Bind to the LDAP server for all operations using a specific password. In this case _ 'letmein'_
AuthLDAPURL ldap://localhost /dc=mydomain, dc=com?cn?sub	This line tells Apache which server and path to use to authenticate against. In this example, Apache will check all entries in the local LDAP server in the tree *dc=mydomain,dc=com* for an entry whose *cn* (common name) field matches. This means when prompted by your browser for a username, you should enter your full name. You could set this to *sn*, *uid*, or any other attribute which is present in the LDAP entries. Note that the attribute does not have to be the one which is used for the entry's distinguished name.

Require valid-user		This line instructs Apache to give access to anyone whose identity has been authenticated. Using the authorization component of mod_authnz_ldap, you could restrict access further, for example to members of an LDAP group.

Steps

1. Build Apache with LDAP support.
2. Make sure that *mod_ldap*, *mod_authnz_ldap*, *mod_authz_user* and *mod_auth_basic* are loaded with LoadModule directives, if necessary. (Some of these may be compiled statically into your Apache.)
3. Follow the instructions above, to secure the <Directory>.
4. Restart Apache and test.
5. Enjoy!