OpenLDAP as an Authentication Provider for All Hosted Websites

A Loooong Password Table...

Username	Password
atheesh	atheesh123
rocking.turtle	iamturtle256
. . . ?	. . . ?

Setting the same password for all the websites I host, causes havoc too. It's really really difficult to manage passwords for every website. And the same goes for my family. Instead of having a one credential per family member its ten.

My ? + ?= LDAP

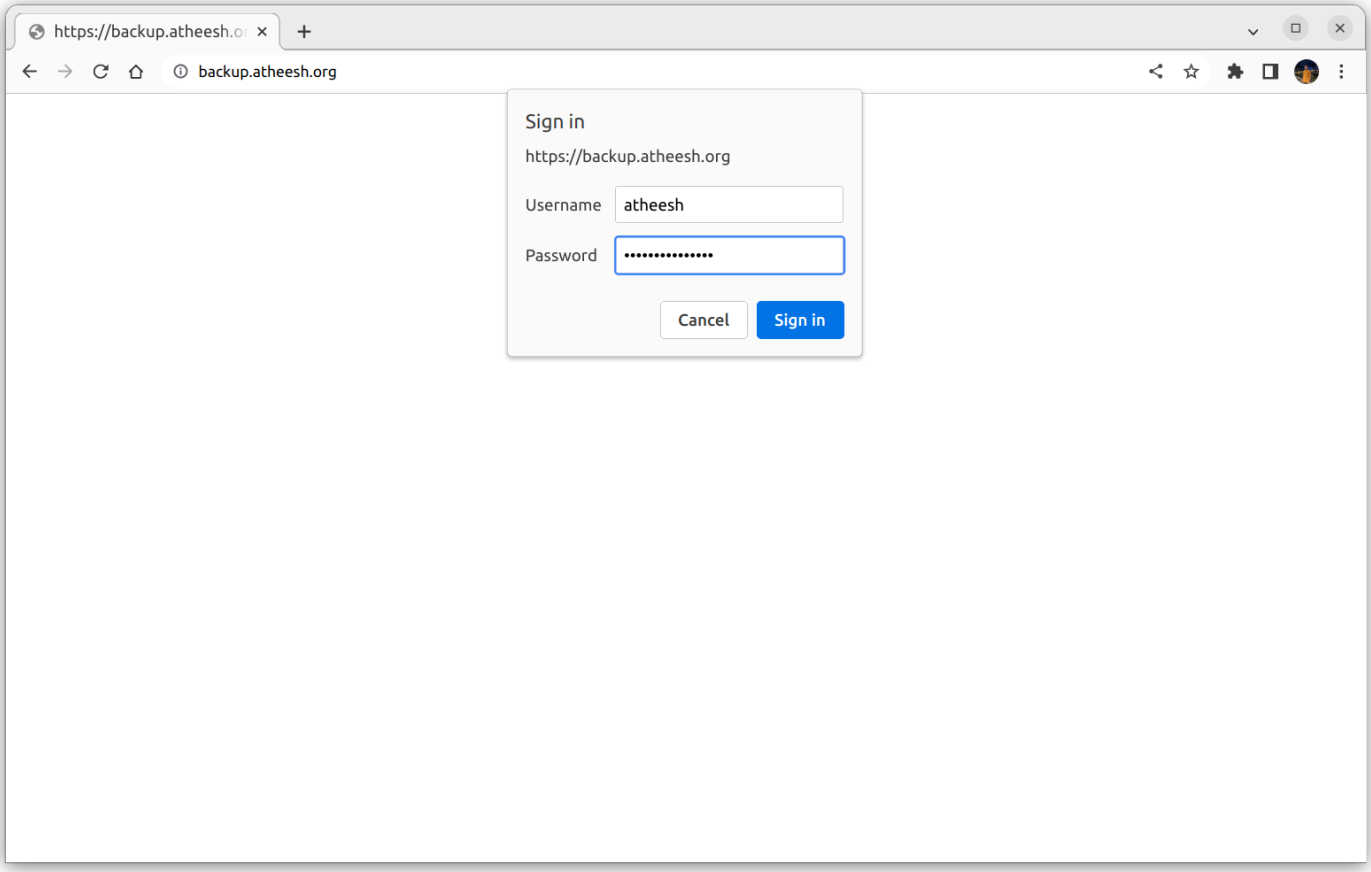
Okay, so this issue was around for a month. I learnt a bit about LDAP while at Grade 11 and I decided to implement OpenLDAP along with phpLDAPadmin for easy management. I deployed it using the `slapd` (A Linux Daemon) at `nvr.atheesh.org`. I created all required users and groups — namely `family` and `service-administrators`. Then, I configured each Self-Hosted app that supported LDAP to use my server at `ldaps://ldap.atheesh.org:636`

> The **Lightweight Directory Access Protocol** (**LDAP** /??ldæp/) is an open, vendor-neutral, industry standard application protocol for accessing and maintaining distributed directory information services over an Internet Protocol (IP) network.[1]
>
> *Source: https://en.wikipedia.org/wiki/Lightweight_Directory_Access_Protocol*

Challenges while Implementing LDAP

- Deploying a LDAP Server was real easy (except the `memberOf` integration for OpenLDAP). But configuring all my self-hosted websites to use it was a bit tough.

- I used LDAP Filters to authenticate a person by either their `uid` or by their email address (`mail` in LDAP)
- Then for controlling privileges across the websites, **I created Groups in those websites and used LDAP Group Synchronization** (specific to every site — NextCloud, OpenProject, Bookstack, etc.)
- I use Apache's Reverse Proxy for all of my websites. It proved really helpful as Certain Websites like Shinobi, qBittorrent-nox, Jackett, BackupPC, etc. did not support LDAP. **Instead I used the `AuthBasicProvider ldap` directive** in the Location tag while configuring a Reverse Proxy for them.
- Coincidentally, these sites just needed a source of authorization not user privileges and other security measures. So, **there was no need of generating Authorization Tokens and using them as Headers** while Reverse Proxying after Apache authenticates using LDAP.



Query Samples and Apache Config

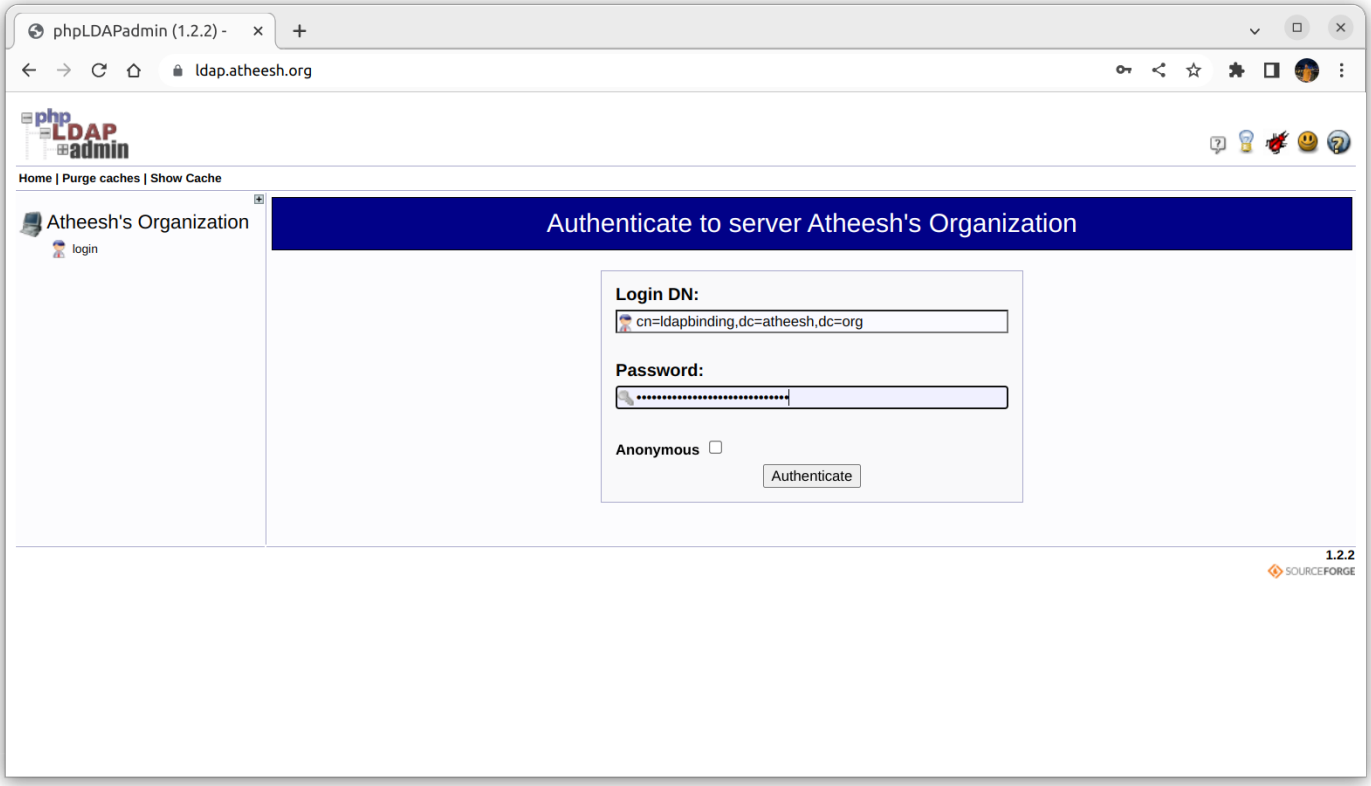
```
(&(objectclass=inetorgperson)(memberof=cn=***,ou=***,dc=***,dc=***)(|(uid=%uid)(mail=%uid)))
```

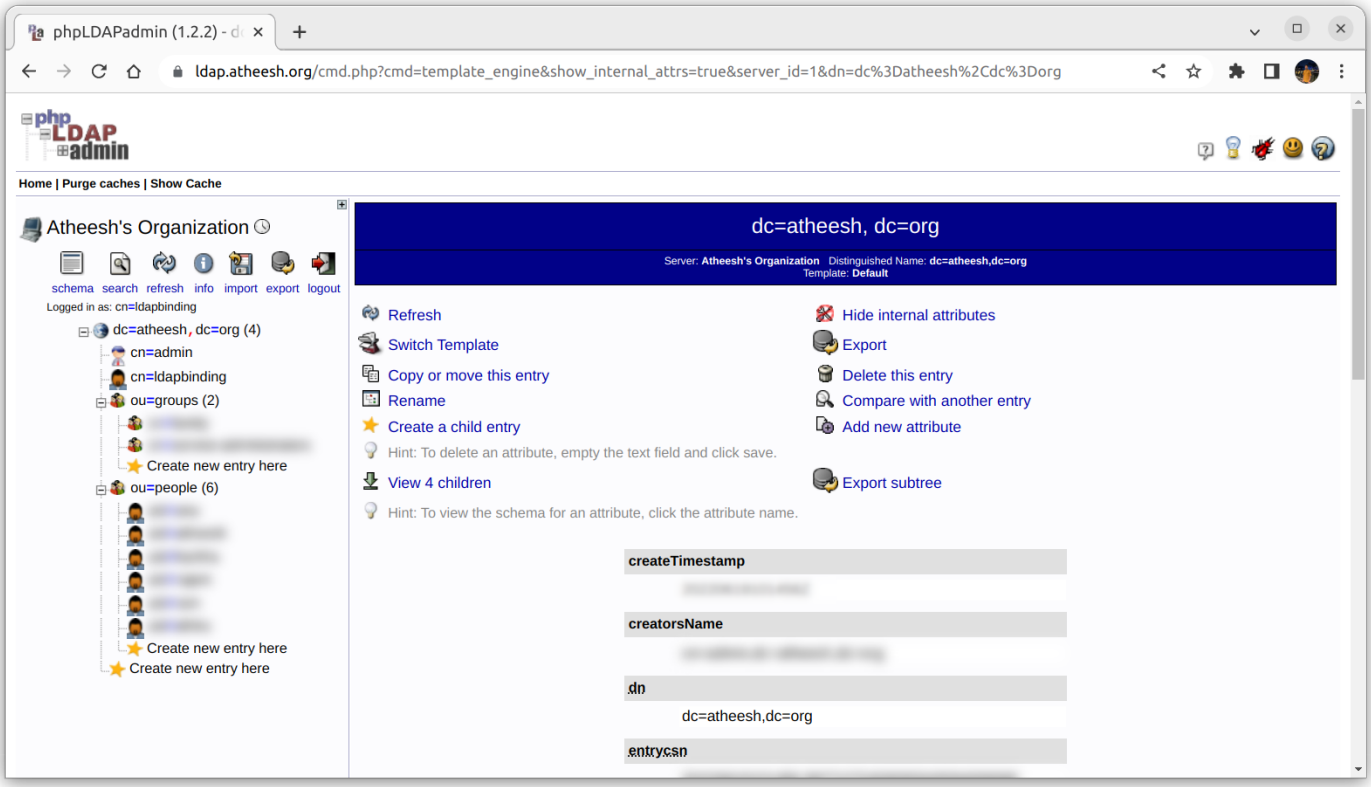
```
<VirtualHost 10.0.0.9:80>
   ServerName ***.atheesh.org
   Redirect permanent / https://***.atheesh.org/
</VirtualHost>

<VirtualHost 10.0.0.9:443>
# The ServerName directive sets the request scheme, hostname and port that
```

```
# the server uses to identify itself. This is used when creating
# redirection URLs. In the context of virtual hosts, the ServerName
# specifies what hostname must appear in the request's Host: header to
# match this virtual host. For the default virtual host (this file) this
# value is not decisive as it is used as a last resort host regardless.
# However, you must set it for any further virtual host explicitly.

        ServerName ***.atheesh.org

        RewriteEngine On
        RewriteCond %{REQUEST_URI}  ^/socket.io            [NC]
        RewriteCond %{QUERY_STRING} transport=websocket    [NC]
        RewriteRule /(.*)           ws://***MASKED-FOR-PRIVACY***/$1 [P,L]

        ProxyPass / http://***MASKED-FOR-PRIVACY***/
        ProxyPassReverse / http://***MASKED-FOR-PRIVACY***/

<Location />
  AuthName "Login using your LDAP Credentials"
  AuthType Basic

    AuthBasicProvider ldap
  AuthLDAPURL
"ldaps://***/ou=***,dc=***,dc=***?uid,mail?sub?(&(objectclass=inetorgperson)(memberof=cn=***,o
u=***,dc=***,dc=***))"
  AuthLDAPBindDN ***MASKED-FOR-PRIVACY***
  AuthLDAPBindPassword ***MASKED-FOR-PRIVACY***
  Require valid-user
</Location>

# Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
# error, crit, alert, emerg.
# It is also possible to configure the loglevel for particular
# modules, e.g.
#LogLevel info ssl:warn

ErrorLog ${APACHE_LOG_DIR}/error.log
CustomLog ${APACHE_LOG_DIR}/access.log combined
```

```
# For most configuration files from conf-available/, which are
# enabled or disabled at a global level, it is possible to
# include a line for only one particular virtual host. For example the
# following line enables the CGI configuration for this host only
# after it has been globally disabled with "a2disconf".
#Include conf-available/serve-cgi-bin.conf

        SSLEngine on
        SSLCertificateFile    ***MASKED-FOR-PRIVACY***
        SSLCertificateKeyFile ***MASKED-FOR-PRIVACY***
        SSLCertificateChainFile ***MASKED-FOR-PRIVACY***

</VirtualHost>

# vim: syntax=apache ts=4 sw=4 sts=4 sr noet
```

Screenshots





Revision #8
Created 7 July 2022 08:42:06 by Atheesh
Updated 10 July 2022 15:47:16 by Atheesh