jordaneunson.com

I make/break/fix stuff

Apache LDAP Authentication, Require ldap-group, OpenLDAP server, AND YOU!

Posted: March 20th, 2011 | **Author:** jordan | **Filed under:** LDAP, Linux | **Tags:** apache, authentication, Directory, ldap, ldap-group, open ldap | 1 Comment »

OK peoples, this one frustrated me for a bit, but because I'm stubborn I figured it out.

I have a webservice that I want to protect by using LDAP authentication within Apache from our OpenLDAP server. However, you want to make sure that the user belongs to a specific LDAP group. If you're like me your groups look something like this:

```
bart:~ jordan$ ldapsearch -h ldap.shop.lan -x -b "dc=shop,dc=lan" cn=fgstaff
# extended LDIF
#
# LDAPv3
# base with scope subtree
# filter: cn=fgstaff
# requesting: ALL
#

# fgstaff, Groups, shop.lan
dn: cn=fgstaff,ou=Groups,dc=shop,dc=lan
cn: fgstaff
gidNumber: 1022
description: Staff
objectClass: posixGroup

memberUid: jordan

# search result
search: 2
result: 0 Success

# numResponses: 2
# numEntries: 1
```

So to make it work you need a few things inside of your Directory tag for the virtual host config file. First, here's mine:

```
Options FollowSymLinks
AllowOverride None
AuthName "FG Staff ONLY!"
AuthType Basic
AuthBasicProvider ldap
AuthzLDAPAuthoritative on
AuthLDAPURL "ldap://1.1.1.1/ou=People,dc=shop,dc=lan?uid"
require ldap-group cn=fgstaff,ou=Groups,dc=shop,dc=lan
AuthLDAPGroupAttributeIsDN off
AuthLDAPGroupAttribute memberUid
```

The trick for me was putting in the require ldap-group plus the whole path including container, org unit, and the dc's. Then AuthLDAPGroupAttributeIsDN. This is big because if it is on then apache will check if "memberUid=uid=jordan ou=People" is part of the fgstaff group and not just "jordan"

Once I set this, it all worked. I'm hoping this will help any others out there.

One Comment on "Apache LDAP Authentication, Require ldap-group, OpenLDAP server, AND YOU!"

1. 1 *Kurt said at 6:08 pm on October 25th, 2014:*

   Thanks Jordan! The "AuthLDAPGroupAttributeIsDN off" did the trick for me.

Leave a Reply

- Name (required)
- Mail (will not be published) (requ
- Website
-
- Submit Comment

Search for: Search

The Monthlies

- July 2015
- March 2015

- November 2014
- September 2014
- June 2014
- April 2014
- February 2014
- December 2013
- April 2013
- March 2013
- February 2013
- April 2012
- November 2011
- September 2011
- May 2011
- April 2011
- March 2011
- February 2011
- January 2011
- October 2010
- August 2010
- July 2010
- June 2010
- May 2010
- April 2010
- February 2010
- January 2010
- December 2009
- November 2009
- October 2009
- September 2009

Become a Friend

Fresh

- Using Munki's nopkg to Push User Level Profiles
- Open Directory Crashing from Wildcard SSL Certificate
- How to Push Watchman Monitoring Windows Agent
- How to Automate FileMaker Server Fail Over on the Mac
- Open Directory Replication 10.8.5 problems with Kerio Connnect 8.3.0

Twitter

- No public Twitter messages.