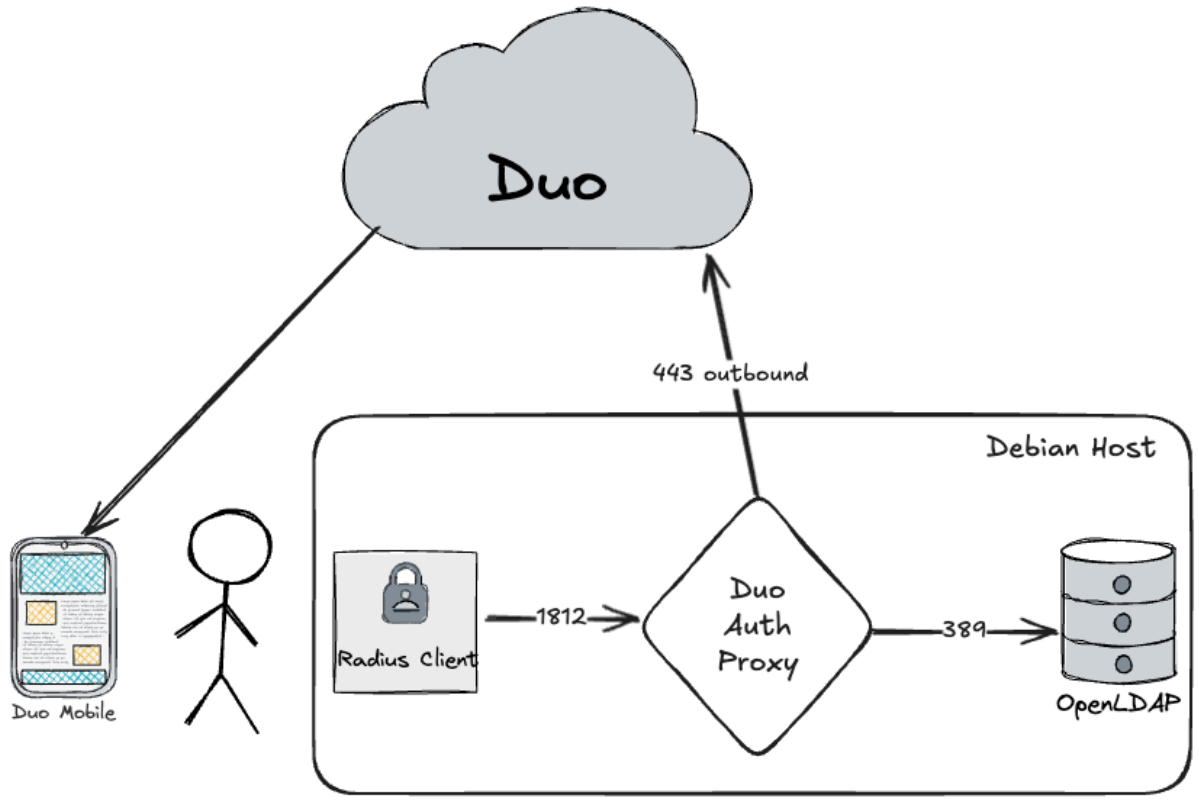
OpenLDAP and AuthProxy on Debian

Requirements

Domain used will be example.com and all passwords will be '@H0ME123f' {MD5}z/MPgQifZ7M6lGWQDP0z1g==, host OS is Debian Bookworm. Debian machine runs on 1 vcpu and 2GB RAM.

Radtest will simulate the radius client (like FTD or Fortigate or Paloalto, etc..), request goes from the radius client to the radius server (Duo Auth Proxy), then first to OpenLDAP (replacing AD) for the primary authentication, then to Duo Mobile for the MFA. if both challenges succeed, Duo Auth Proxy will reply to the Radius client to let the user in.



Overview on the steps covered

1. Install Debian Machine

2. Install and configure OpenLDAP
3. Install and configure phpLDAPadmin
4. Replace openldap templates for groups and users
5. Create Organizational Units and Groups
6. Install Duo Authentication Proxy
7. Configure Duo Auth Proxy with OpenLDAP
8. Test using Radius Client

Debian

install Debian machine, from https://cdimage.debian.org/debian-cd/current-live/amd64/iso-hybrid/debian-live-12.10.0-amd64-gnome.iso

```
su - root
apt-get update
apt-get upgrade -y
systemctl stop ufw
systemctl disable ufw
systemctl stop apparmor
systemctl disable apparmor.service
apt-get install net-tools -y
apt-get install apache2
systemctl start apache2
systemctl enable apache2
```

PHPldapadmin

```
su - root
apt-get install slapd ldap-utils
systemctl start slapd
systemctl enable slapd
dpkg-reconfigure slapd
apt-get install phpldapadmin
```

edit `/etc/phpldapadmin/config.php` to be as follows

```
$servers->setValue('server','base', array('dc=example,dc=com'));
#$servers->setValue('login','bind_id','cn=admin,dc=example,dc=com');
$config->custom->appearance['hide_template_warning'] = true;
```

replace /etc/phpldapadmin/templates/creation/posixGroup.xml with the below

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<!DOCTYPE template SYSTEM "template.dtd">
<template>
  <askcontainer>1</askcontainer>
  <description>New groupOfNames Group</description>
  <icon>ldap-ou.png</icon>
  <invalid>0</invalid>
  <rdn>cn</rdn>
  <title>Generic: groupOfNames Group</title>
  <visible>1</visible>

  <objectClasses>
    <objectClass id="groupOfNames" />
  </objectClasses>

  <attributes>
    <attribute id="cn">
      <display>Group Name</display>
      <order>1</order>
      <page>1</page>
    </attribute>

    <attribute id="member">
      <display>Members</display>
      <order>2</order>
      <page>1</page>
      <value><![CDATA[=php.MultiList(/;(&(objectClass=inetOrgPerson));d
n;%cn% (%uid%)]]></value>
    </attribute>
  </attributes>
</template>
```

replace /etc/phpldapadmin/templates/creation/posixAccount.xml with the below

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<!DOCTYPE template SYSTEM "../template.dtd">

<template>
<askcontainer>1</askcontainer>
<description>New User Account</description>
<icon>ldap-user.png</icon>
<invalid>0</invalid>
<rdn>cn</rdn>
<!--<regexp>^ou=People,o=.*,</regexp>-->
<title>Generic: User Account</title>
<visible>1</visible>

<objectClasses>
<objectClass id="inetOrgPerson"></objectClass>
<objectClass id="posixAccount"></objectClass>
</objectClasses>

<attributes>
<attribute id="givenName">
   <display>First name</display>
   <icon>ldap-uid.png</icon>
   <onchange>=autoFill(cn;%givenName% %sn%)</onchange>
   <onchange>=autoFill(uid;%givenName|0-1/l%%sn/l%)</onchange>
   <order>1</order>
   <page>1</page>
</attribute>
<attribute id="sn">
   <display>Last name</display>
   <onchange>=autoFill(cn;%givenName% %sn%)</onchange>
   <onchange>=autoFill(uid;%givenName|0-1/l%%sn/l%)</onchange>
   <!-- <onchange>=autoFill(homeDirectory;/home/users/%uid|0-1/l%/%uid%)</onchange> -->
   <order>2</order>
   <page>1</page>
```

```
</attribute>
<attribute id="cn">
   <display>Common Name</display>
   <order>3</order>
   <page>1</page>
</attribute>
<attribute id="uid">
   <display>User ID</display>
   <onchange>=autoFill(homeDirectory;/home/users/%uid%)</onchange>
   <order>4</order>
   <page>1</page>
   <spacer>1</spacer>
</attribute>
<attribute id="homeDirectory">
   <display>Home directory</display>
   <!-- <onchange>=autoFill(homeDirectory;/home/users/%gidNumber|0-
0/T%/%uid|3-%)</onchange> -->
   <order>8</order>
   <page>1</page>
</attribute>
<attribute id="uidNumber">
   <display>UID Number</display>
   <icon>terminal.png</icon>
   <order>6</order>
   <page>1</page>
   <readonly>1</readonly>
   <value>=php.GetNextNumber(/;uidNumber)</value>
</attribute>
<attribute id="loginShell">
   <display>Login shell</display>
   <order>9</order>
   <page>1</page>
   <!-- <value><![CDATA[=php.PickList(/;(&(objectClass=posixAccount));lo
ginShell;%loginShell%;;;;loginShell)]]></value> -->
   <type>select</type>
   <value id="/bin/bash">Bash</value>
   <value id="/bin/csh">C Shell</value>
   <value id="/bin/dash">Dash</value>
```

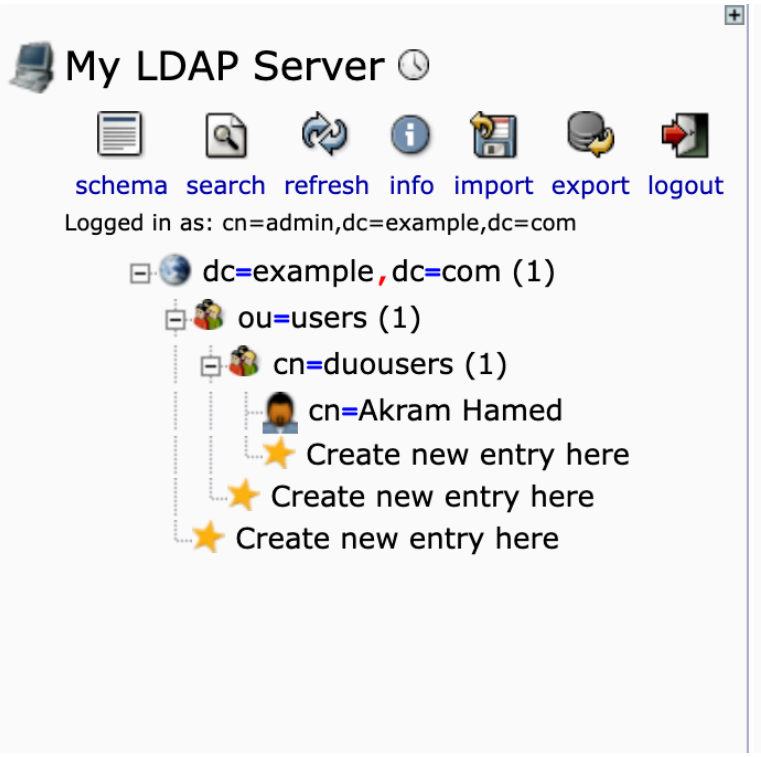
```
    <value id="/bin/sh">Shell</value>
    <value id="/bin/tsh">Turbo C Shell</value>
    <value id="/bin/false">False</value>
    <value id="/usr/sbin/nologin">No Login</value>
  </attribute>
  <attribute id="userPassword">
    <display>Password</display>
    <!-- <helper>
      <display>Encryption</display>
      <id>enc</id>
      <value>=php.PasswordEncryptionTypes()</value>
    </helper> -->
    <icon>lock.png</icon>
    <order>5</order>
    <page>1</page>
    <post>=php.PasswordEncrypt(%enc%;%userPassword%)</post>
    <spacer>1</spacer>
    <verify>1</verify>
  </attribute>
  </attributes>

  </template>
```

Create OpenLDAP OU, Group and Users

in openldap create LDIF as below

```
# LDIF Export for dc=example,dc=com
# Server: My LDAP Server (127.0.0.1)
# Search Scope: sub
# Search Filter: (objectClass=*)
# Total Entries: 4
#
# Generated by phpLDAPadmin (http://phpldapadmin.sourceforge.net) on
April 26, 2025 11:32 am
# Version: 1.2.6.3

version: 1
```

```
# Entry 1: dc=example,dc=com
dn: dc=example,dc=com
dc: example
o: example
objectclass: top
objectclass: dcObject
objectclass: organization

# Entry 2: ou=users,dc=example,dc=com
dn: ou=users,dc=example,dc=com
objectclass: organizationalUnit
objectclass: top
ou: users

# Entry 3: cn=duousers,ou=users,dc=example,dc=com
dn: cn=duousers,ou=users,dc=example,dc=com
cn: duousers
member: cn=akram hamed,cn=duousers,ou=users,dc=example,dc=com
member: cn=test test,cn=duousers,ou=users,dc=example,dc=com
objectclass: groupOfNames
objectclass: top

# Entry 4: cn=Akram Hamed,cn=duousers,ou=users,dc=example,dc=com
dn: cn=Akram Hamed,cn=duousers,ou=users,dc=example,dc=com
cn: Akram Hamed
gidnumber: 10001
givenname: akram
homedirectory: /home/users/akramhamed
loginshell: /bin/bash
mail: akramhamed@example.com
objectclass: inetOrgPerson
objectclass: posixAccount
objectclass: top
sn: hamed
uid: akramhamed
uidnumber: 10002
userpassword: {MD5}z/MPgQifZ7M6lGWQDP0z1g==
```



Duo

```
su - root
apt-get install build-essential libffi-dev zlib1g-dev
cd /root
wget --content-disposition https://dl.duosecurity.com/duoauthproxy-latest
-src.tgz
tar xzf duoauthproxy-[TAB]
cd duoauthproxy-version-src
make
cd duoauthproxy-build
./install  --install-dir /opt/duoauthproxy --service-user duo_authproxy_svc -
-log-group duo_authproxy_grp --create-init-script yes
```

add the External Directory as openldap in Duo admin panel, the conf file /opt/duoauthproxy/conf/authproxy.cfg should be as below

```
[cloud]
ikey=DIMAHENUG1XMKZALS2FB
skey=vDFkH6uUu1qs6NYjAYIuJpAknxBHWQ3R5vS2CrHk
api_host=api-b2838f1a.duosecurity.com
service_account_username=cn=Akram Hamed,cn=duousers,ou=users,dc=
```

```
example,dc=com
service_account_password=@H0ME123f

## below section to be used later for radius auth
[ad_client]
host=127.0.0.1
port=389
auth_type=plain
bind_dn=cn=Akram Hamed,cn=duousers,ou=users,dc=example,dc=com
service_account_username=cn=Akram Hamed,cn=duousers,ou=users,dc=
example,dc=com
service_account_password=@H0ME123f
search_dn=dc=example,dc=com
username_attribute=uid
ssl_verify_hostname=false
transport=clear
```

```
/opt/duoauthproxy/bin/authproxyctl restart
```

Install Radius Client

```
apt-get install freeradius-utils
```

Create a Duo application for the radius client

create a new Application in Duo admin panel with type “RADIUS”, add the [radius_server_auto] section in /opt/duoauthproxy/conf/authproxy.cfg

```
[radius_server_auto]
ikey=DISLG2EL0V790855FRZV
skey=mUvnGcPoViWH0D7QuDFRln4XyVfdOTF3c39xpJyq
api_host=api-b2838f1a.duosecurity.com
radius_ip_1=127.0.0.1
radius_secret_1=cisco
failmode=safe
client=ad_client
port=1812
```

Test Radius client

```
radtest akramhamed @H0ME123f 127.0.0.1 1812 cisco
```

Test tools

```
ldapwhoami -x -H ldap://127.0.0.1 -D "cn=Akram Hamed,cn=duousers,ou=users,dc=example,dc=com" -w '@H0ME123f'
ldapsearch -x -H ldap://127.0.0.1 -D "cn=Akram Hamed,cn=duousers,ou=users,dc=example,dc=com" -w '@H0ME123f' -b "dc=example,dc=com"
root@debian:~# ldapwhoami -x -H ldap://127.0.0.1 -D "cn=Akram Hamed,cn=duousers,ou=users,dc=example,dc=com" -w '@H0ME123f'
radtest akramhamed @H0ME123f 127.0.0.1 1812 cisco
```