**OpenLDAP on Amazon Linux EC2**

1. create AWS server
2. login as root
3. update and upgrade --yum update -y yum upgrade -y
4. install openssh -- yum install -y openldap openldap-clients openldap-servers
5. Generate hash password for admin – slappasswd
6. {SSHA}Ihki7sP5mV1l1lyOukPiAPalOrBwatLp
7. Now start and enable slapd -- sudo systemctl start slapd --sudo systemctl enable slapd --sudo systemctl status slapd
8. Allow LDAP server deamon though firewall -- firewall-cmd --add-service=ldap
9. Go to the location -- cd /etc/openldap/slapd.d/cn\=config
10. Create a file – sudo vi ldaprootpasswd.ldif
11. Add following content ::

dn: olcDatabase={0}config,cn=config

changetype: modify

add: olcRootPW

olcRootPW: {SSHA}PASSWORD\_CREATED

1. Add corresponding LDAP entry specifying the URI referring to LDAP server and the file above -- sudo ldapadd -Y EXTERNAL -H ldapi:/// -f ldaprootpasswd.ldif
2. SASL/EXTERNAL authentication started
3. SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
4. SASL SSF: 0
5. modifying entry "olcDatabase={0}config,cn=config"
6. Configuring LDAP Database :: sudo cp /usr/share/openldap-servers/DB\_CONFIG.example /var/lib/ldap/DB\_CONFIG

=== sudo chown -R ldap:ldap /var/lib/ldap/DB\_CONFIG ==sudo systemctl restart slapd

1. Import some basic LDAP schemas from the /etc/openldap/schema directory as follows sudo ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/cosine.ldif

$ sudo ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/nis.ldif

$ sudo ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/inetorgperson.ldif

1. Now add your domain in the LDAP database and create a file called ldapdomain.ldif for your domain : sudo vim ldapdomain.ldif

dn: olcDatabase={1}monitor,cn=config

changetype: modify

replace: olcAccess

olcAccess: {0}to \* by dn.base="gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth"

read by dn.base="cn=Manager,**dc=vigdatos**,dc=com" read by \* none

dn: olcDatabase={2}hdb,cn=config

changetype: modify

replace: olcSuffix

olcSuffix: **dc=vigdatos**,dc=com

dn: olcDatabase={2}hdb,cn=config

changetype: modify

replace: olcRootDN

olcRootDN: cn=Manager,**dc=vigdatos**,dc=com

dn: olcDatabase={2}hdb,cn=config

changetype: modify

add: olcRootPW

olcRootPW: {SSHA}PASSWORD

dn: olcDatabase={2}hdb,cn=config

1. Then add the above configuration to the LDAP database with the following command

sudo ldapmodify -Y EXTERNAL -H ldapi:/// -f ldapdomain.ldif

1. Error ldap\_modify: Inappropriate matching (18)

additional info: modify/add: olcRootPW: no equality matching rule

olcAccess: {0}to \* by dn.base="gidNumber=0+uidNumber=0,cn=peercred,cn=external, cn=auth" read by dn.base="cn=ldapadm,dc=field,dc=linuxhostsupport,dc=com" read by \* none

1. openssl req -new -x509 -nodes -out \

/etc/openldap/certs/myldap.field.linuxhostsupport.com.cert \

-keyout /etc/openldap/certs/myldap.field.linuxhostsupport.com.key \

-days 365

18. Change the owner and group permissions so OpenLDAP can read the files

chown -R ldap:ldap /etc/openldap/certs

1. Gererate key

openssl req -new -x509 -nodes -out \

/etc/openldap/certs/myldap.vigdatos.com.cert \

-keyout /etc/openldap/certs/myldap.vigdatos.com.key \

-days 365

1. Now create certs.ldif to configure OpenLDAP to use the LDAPS protocol:

# nano certs.ldif

dn: cn=config

changetype: modify

replace: olcTLSCertificateKeyFile

olcTLSCertificateKeyFile: /etc/openldap/certs/myldap.vigdatos.com.key

dn: cn=config

changetype: modify

replace: olcTLSCertificateFile

olcTLSCertificateFile: /etc/openldap/certs/myldap.vigdatos.com.cert

1. ldapmodify -Y EXTERNAL -H ldapi:/// -f certs.ldif
2. error

SASL/EXTERNAL authentication started

SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth

SASL SSF: 0

modifying entry "cn=config"

ldap\_modify: Other (e.g., implementation specific) error (80)

1. solution <https://askubuntu.com/questions/936382/openldap-error-configuring-starttls-ldap-modify-other-e-g-implementation-sp>

output 5ebbd26c UNKNOWN attributeDescription "CHANGETYPE" inserted.

5ebbd26c UNKNOWN attributeDescription "REPLACE" inserted.

5ebbd26c is\_entry\_objectclass("cn=config,cn=config", "2.16.840.1.113730.3.2.6") no objectClass attribute

5ebbd26c is\_entry\_objectclass("olcDatabase={1}monitor,cn=config,cn=config", "2.16.840.1.113730.3.2.6") no objectClass attribute

5ebbd26c UNKNOWN attributeDescription "ADD" inserted.

5ebbd26c is\_entry\_objectclass("olcDatabase={0}config,cn=config,cn=config", "2.16.840.1.113730.3.2.6") no objectClass attribute

config file testing succeeded

1. Another error : <https://www.linuxquestions.org/questions/linux-software-2/stuck-on-ldap-4175519976/>
2. Add the LDAP schemas:

ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/cosine.ldif

# ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/nis.ldif

# ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/inetorgperson.ldif

1. now create a base.ldif file for your domain:

dn: dc=vigdatos,dc=com

dc: vigdatos

objectClass: top

objectClass: domain

dn: cn=ldapadm,dc=vigdatos,dc=com

objectClass: organizationalRole

cn: ldapadm

description: LDAP Manager

dn: ou=People,dc=vigdatos,dc=com

objectClass: organizationalUnit

ou: People

dn: ou=Group,dc=vigdatos,dc=com

objectClass: organizationalUnit

ou: Group

1. We will deploy these configuration changes to the OpenLDAP server using the ldapadm user:

ldapadd -x -W -D "cn=ldapadm,dc=field,dc=linuxhostsupport,dc=com" -f base.ldif

use this ldapadd -x -W -D "cn=Manager,dc=vigdatos,dc=com" -f base.ldif

1. Now install phpldapadm

<https://hostadvice.com/how-to/how-to-install-phpldapadmin-on-centos-7/>

1. Intall httpd and start
2. Config file

<https://www.linuxquestions.org/questions/linux-networking-3/openldap-ldap_add-naming-violation-64-a-385424/>

sudo yum install php-ldap php-mbstring php-pear php-xml

1. $ sudo yum install epel-release

#

# Web-based tool for managing LDAP servers

#

Alias /phpldapadmin /usr/share/phpldapadmin/htdocs

Alias /ldapadmin /usr/share/phpldapadmin/htdocs

<Directory /usr/share/phpldapadmin/htdocs>

<IfModule mod\_authz\_core.c>

# Apache 2.4

Require all granted

</IfModule>

<IfModule !mod\_authz\_core.c>

# Apache 2.2

Order Deny,Allow

# Deny from all

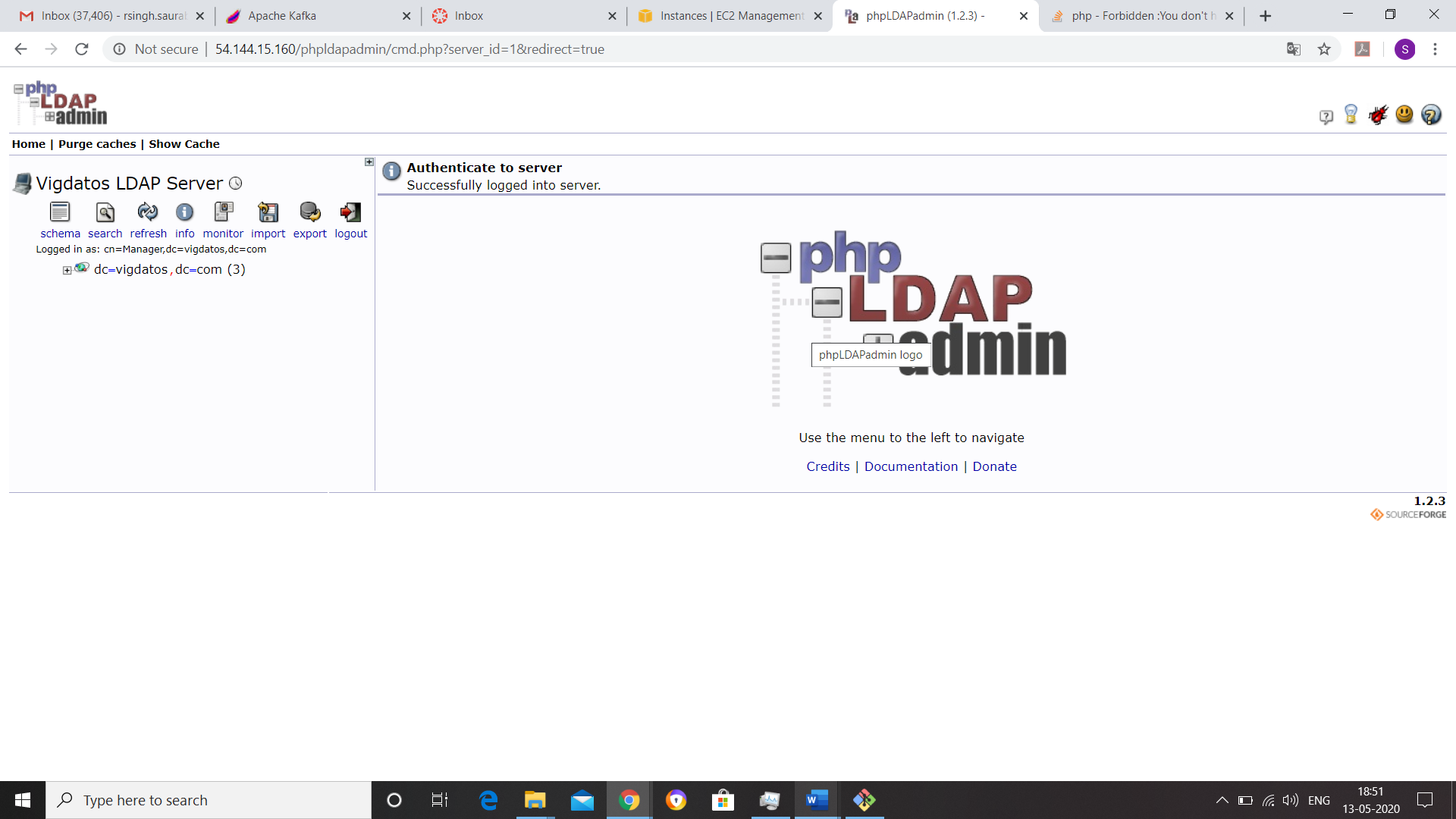
Allow from 54.144.15.160

Allow from ::1

</IfModule>

</Directory>

sudo vim /etc/phpldapadmin/config.php



<https://stackoverflow.com/questions/23235363/forbidden-you-dont-have-permission-to-access-phpmyadmin-on-this-server>

<https://www.thegeekstuff.com/2015/02/openldap-add-users-groups/>

To add something to the LDAP directory, you need to first create a LDIF file.

The ldif file should contain definitions for all attributes that are required for the entries that you want to create.

With this ldif file, you can use ldapadd command to import the entries into the directory as explained in this tutorial.  
  
If you are new to OpenLDAP, you should first [install OpenLDAP](https://www.thegeekstuff.com/2015/01/openldap-linux/) on your system.

### Create a LDIF file for New User

The following is a sample LDIF file that will be used to create a new user.

# cat adam.ldif

dn: uid=adam,ou=users,dc=tgs,dc=com

objectClass: top

objectClass: account

objectClass: posixAccount

objectClass: shadowAccount

cn: adam

uid: adam

uidNumber: 16859

gidNumber: 100

homeDirectory: /home/adam

loginShell: /bin/bash

gecos: adam

userPassword: {crypt}x

shadowLastChange: 0

shadowMax: 0

shadowWarning: 0

### Add a LDAP User using ldapadd

Now, use ldapadd command and the above ldif file to create a new user called adam in our OpenLDAP directory as shown below:

# ldapadd -x -W -D "cn=ramesh,dc=tgs,dc=com" -f adam.ldif

Enter LDAP Password:

adding new entry "uid=adam,ou=users,dc=tgs,dc=com"

### Assign Password to LDAP User

To set the password for the LDAP user we just created above, use ldappasswd command as shown in the below example:

# ldappasswd -s welcome123 -W -D "cn=ramesh,dc=tgs,dc=com" -x "uid=adam,ou=users,dc=tgs,dc=com"

Enter LDAP Password: