### **How to Install Squid on CentOS 7/8**

[root@dlp ~]# yum -y update  
[root@dlp ~]# yum -y install squid  
[root@dlp ~]# systemctl start squid  
[root@dlp ~]# systemctl enable squid  
[root@dlp ~]# systemctl status squid

**Update the /etc/squid.conf file as per requirements**

### **OpenLDAP : Configure LDAP Server**

**Install OpenLDAP**

[root@dlp ~]# yum -y install openldap-servers openldap-clients

[root@dlp ~]# cp /usr/share/openldap-servers/DB\_CONFIG.example /var/lib/ldap/DB\_CONFIG

[root@dlp ~]# chown ldap. /var/lib/ldap/DB\_CONFIG

[root@dlp ~]# systemctl start slapd

[root@dlp ~]# systemctl enable slapd

**Set OpenLDAP admin password.**

# generate encrypted password

[root@dlp ~]# slappasswd

New password:

Re-enter new password:

{SSHA}xxxxxxxxxxxxxxxxxxxxxxxx

[root@dlp ~]# vi chrootpw.ldif

# specify the password generated above for "olcRootPW" section

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

**changetype: modify**

**add: olcRootPW**

**olcRootPW: {SSHA}xxxxxxxxxxxxxxxxxxxxxxxx**

[root@dlp ~]# ldapadd -Y EXTERNAL -H ldapi:/// -f chrootpw.ldif

SASL/EXTERNAL authentication started

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

SASL SSF: 0

modifying entry "olcDatabase={0}config,cn=config"

[root@dlp ~]# ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/cosine.ldif

SASL/EXTERNAL authentication started

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

SASL SSF: 0

adding new entry "cn=cosine,cn=schema,cn=config"

[root@dlp ~]# ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/nis.ldif

SASL/EXTERNAL authentication started

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

SASL SSF: 0

adding new entry "cn=nis,cn=schema,cn=config"

[root@dlp ~]# ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/inetorgperson.ldif

SASL/EXTERNAL authentication started

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

SASL SSF: 0

adding new entry "cn=inetorgperson,cn=schema,cn=config"

|  |
| --- |
| **Set your domain name on LDAP DB.** |

**# generate directory manager's password**

[root@dlp ~]# slappasswd

New password:

Re-enter new password:

{SSHA}xxxxxxxxxxxxxxxxxxxxxxxx

[root@dlp ~]# [vi](https://www.server-world.info/en/command/html/vi.html) chdomain.ldif

# replace to your own domain name for "dc=\*\*\*,dc=\*\*\*" section

# specify the password generated above for "olcRootPW" section

**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=srv,dc=world" read by \* none**

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

**changetype: modify**

**replace: olcSuffix**

**olcSuffix: dc=srv,dc=world**

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

**changetype: modify**

**replace: olcRootDN**

**olcRootDN: cn=Manager,dc=srv,dc=world**

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

**changetype: modify**

**add: olcRootPW**

**olcRootPW: {SSHA}xxxxxxxxxxxxxxxxxxxxxxxx**

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

**changetype: modify**

**add: olcAccess**

**olcAccess: {0}to attrs=userPassword,shadowLastChange by**

**dn="cn=Manager,dc=srv,dc=world" write by anonymous auth by self write by \* none**

**olcAccess: {1}to dn.base="" by \* read**

**olcAccess: {2}to \* by dn="cn=Manager,dc=srv,dc=world" write by \* read**

[root@dlp ~]# ldapmodify -Y EXTERNAL -H ldapi:/// -f chdomain.ldif

SASL/EXTERNAL authentication started

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

SASL SSF: 0

modifying entry "olcDatabase={1}monitor,cn=config"

modifying entry "olcDatabase={2}hdb,cn=config"

modifying entry "olcDatabase={2}hdb,cn=config"

modifying entry "olcDatabase={2}hdb,cn=config"

[root@dlp ~]# [vi](https://www.server-world.info/en/command/html/vi.html) basedomain.ldif

# replace to your own domain name for "dc=\*\*\*,dc=\*\*\*" section

**dn: dc=srv,dc=world**

**objectClass: top**

**objectClass: dcObject**

**objectclass: organization**

**o: Server World**

**dc: Srv**

**dn: cn=Manager,dc=srv,dc=world**

**objectClass: organizationalRole**

**cn: Manager**

**description: Directory Manager**

**dn: ou=People,dc=srv,dc=world**

**objectClass: organizationalUnit**

**ou: People**

**dn: ou=Group,dc=srv,dc=world**

**objectClass: organizationalUnit**

**ou: Group**

[root@dlp ~]# ldapadd -x -D cn=Manager,dc=srv,dc=world -W -f basedomain.ldif

Enter LDAP Password: # directory manager's password

adding new entry "dc=srv,dc=world"

adding new entry "cn=Manager,dc=srv,dc=world"

adding new entry "ou=People,dc=srv,dc=world"

adding new entry "ou=Group,dc=srv,dc=world"

|  |
| --- |
| [**If Firewalld is running**](https://www.server-world.info/en/note?os=CentOS_7&p=firewalld)**, allow LDAP service. LDAP uses 389/TCP.** |

[root@dlp ~]# firewall-cmd --add-service=ldap --permanent

success

[root@dlp ~]# firewall-cmd --reload

success

**OFF SELinux :**

[root@dlp ~]# vi /etc/selinux/config ----- Disable SeLinux

[root@dlp ~]# sudo shutdown -r now

[root@dlp ~]# systemctl status slapd

[root@dlp ~]# systemctl status squid

**Add the following lines in /etc/squid/squid.conf**

(below

# INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS

)

**auth\_param basic program /usr/lib64/squid/squid\_ldap\_auth -b "dc=srv,dc=world" -f "uid=%s" -h ldapproxy.srv.world**

**acl ldapauth proxy\_auth REQUIRED**

**http\_access allow ldapauth**

**[root@dlp ~]# vi /etc/hosts (according to your ip and domain)**

**10.10.10.124 localhost.srv.world ldap**

**10.10.10.124 localhost.srv.world squid**

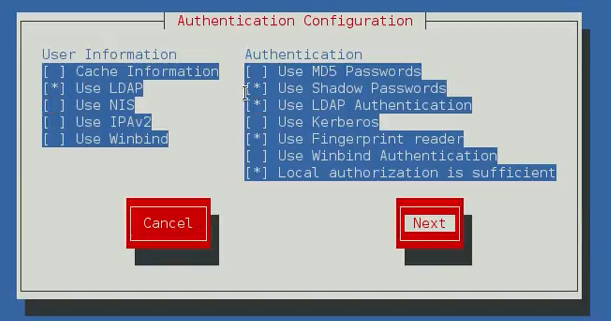
[root@dlp ~]# cd /usr/lib64/squid/

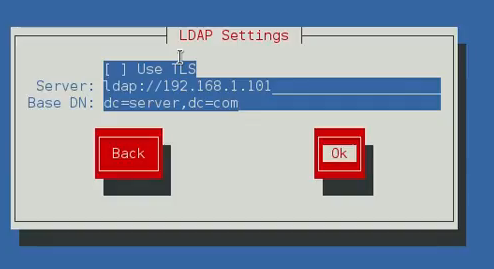
ln -s /usr/lib64/squid/basic\_ldap\_auth /usr/lib64/squid/squid\_ldap\_auth

[root@dlp ~]# yum install openldap-clients nss-pam-ldapd squid -y

[root@dlp ~]# yum install fprintd-pam

[root@dlp ~]# authconfig-tui





[root@dlp ~]# systemctl restart slapd

[root@dlp ~]# systemctl status slapd

[root@dlp ~]# systemctl restart squid

[root@dlp ~]# systemctl status squid

**CREATE CERTIFICATE**

[root@dlp ~]# openssl req -new -newkey rsa:2048 -sha256 -days 365 -nodes -x509 -extensions v3\_ca -keyout proxyCA.pem -out proxyCA.pem

[root@dlp ~]# mkdir /etc/squid/ssl\_cert

[root@dlp ~]# mv proxyCA.pem /etc/squid/ssl\_cert/

[root@dlp ~]# cd /etc/squid/ssl\_cert

[root@dlp ~]# openssl x509 -in /etc/squid/ssl\_cert/proxyCA.pem -outform DER -out proxyCA.der

**(proxyCA.der this is the certificate to be uploaded in the trusted certificate of the browser)**

[root@dlp ~]# vi /etc/squid/squid.conf

# Squid normally listens to port 3128

(Add following lines)

**http\_port 3128 ssl-bump \**

**cert=/etc/squid/ssl\_cert/proxyCA.pem \**

**generate-host-certificates=on dynamic\_cert\_mem\_cache\_size=4MB**

**acl step1 at\_step SslBump1**

**ssl\_bump peek step1**

**ssl\_bump bump all**

**sslproxy\_cafile /usr/local/openssl/cabundle.file**

[root@dlp ~]# cd /etc/squid/ssl\_cert/

./configure --with-openssl --enable-ssl-crtd

[root@dlp ~]# systemctl restart squid

[root@dlp ~]# /usr/lib64/squid/ssl\_crtd -c -s /var/lib/ssl\_db

[root@dlp ~]# chown squid:squid -R /var/lib/ssl\_db

[root@dlp ~]# systemctl restart squid

[root@dlp ~]# systemctl status squid

[root@dlp ~]# sudo shutdown -r now

[root@dlp ~]# systemctl status squid

[root@dlp ~]# vi /root/ayush.k.ldif

**dn: uid=ayush.k,ou=People,dc=srv,dc=world**

**uid: ayush.k**

**cn: ayush.k**

**sn: ayush.k**

**mail: ayush.k@srv.world**

**objectClass: person**

**objectClass: organizationalPerson**

**objectClass: inetOrgPerson**

**objectClass: posixAccount**

**objectClass: top**

**objectClass: shadowAccount**

**userPassword:{crypt}x**

**shadowLastChange: 18194**

**shadowMin: 0**

**shadowMax: 99999**

**shadowWarning: 7**

**loginShell: /bin/bash**

**uidNumber: 1024**

**gidNumber: 1024**

**homeDirectory: /home/ayush.k**

**# ayush.k, Group, srv.world**

**dn: cn=ayush.k,ou=Group,dc=srv,dc=world**

**objectClass: posixGroup**

**objectClass: top**

**cn: ayush.k**

**userPassword:: 1qaz@WSX3edc**

**gidNumber: 1024**

[root@dlp ~]# ldapadd -x -W -D "cn=Manager,dc=srv,dc=world" -f /root/ayush.k.ldif

[root@dlp ~]# ldappasswd -s dima123 -W -D "cn=Manager,dc=srv,dc=world" -x "uid=ayush.k,ou=People,dc=srv,dc=world"

[root@dlp ~]# getent passwd ayush.k

[root@dlp ~]# systemctl restart slapd

[root@dlp ~]# systemctl status slapd

[root@dlp ~]# systemctl restart squid

[root@dlp ~]# systemctl status squid

[root@dlp ~]# firewall-cmd --permanent --add-port=3128/tcp

[root@dlp ~]# firewall-cmd --permanent --add-port=80/tcp

[root@dlp ~]# firewall-cmd --permanent --add-port=443/tcp

[root@dlp ~]# firewall-cmd --reload

[root@dlp ~]# vi /etc/resolv.conf ( --- here we have to give the DNS ip for ressolver)

**: Now**

**Upload the proxy certificate in the browser**

**Change proxy to manual : IP and port number 3128**

**Restart the browser and login with user credentials. Browse a website and check the certificate.**