Установка OpenLDAP на CentOS 8. LDAP — это облегченный протокол аутентификации домена. Это означает, что вы можете использовать LDAP в качестве центральной системы аутентификации как для пользователей, так и для таких систем, как Postfix. Его можно сравнить с Microsoft Active Directory. OpenLDAP — это система LDAP с открытым исходным кодом, работающая в системах Linux.

------------------------------------------------------------------------------------------

1.Установка первоначальная для openLDAP на Centos8.

------------------------------------------------------------------------------------------

1.1 sudo dnf update - обновления системы

sudo dnf upgrade -y - обновите пакеты

1.2 sudo dnf install wget cyrus-sasl-devel libtool-ltdl-devel openssl-devel libdb-devel make libtool autoconf tar gcc perl perl-devel - Установите необходимые пакеты, которые позволят вам успешно собрать OpenLDAP

1.3 sudo useradd -r -M -d /var/lib/openldap -u 55 -s /usr/sbin/nologin ldap - Нам нужно создать непривилегированного системного пользователя для OpenLDAP

1.4 На момент написания этого руководства последней версией OpenLDAP была 2.4.57.

Sudo wget https://www.openldap.org/software/download/OpenLDAP/openldap-release/openldap-$VER.tgz

1.5 sudo tar xzf openldap-$VER.tgz - Распакуйте загруженный файл

------------------------------------------------------------------------------------------

2.Установка openLDAP на Centos8.

------------------------------------------------------------------------------------------

2.1 sudo mv openldap-$VER /opt

cd /opt/openldap-$VER - Переместите извлеченные файлы в / opt /, затем скомпилируйте исходные файлы.

2.2 Скомпилируйте исходные файлы:

sudo ./configure --prefix=/usr --sysconfdir=/etc --disable-static \

--enable-debug --with-tls=openssl --with-cyrus-sasl --enable-dynamic\

--enable-crypt --enable-spasswd --enable-slapd --enable-modules \

--enable-rlookups --enable-backends=mod --disable-ndb --disable-sql \

--disable-shell --disable-bdb --disable-hdb --enable-overlays=mod

2.3 После успешной компиляции вы должны увидеть вывод, который гласит: “Please run “make depend” to build dependencies”

2.3 sudo make depend - Запустите make зависимый, чтобы построить зависимости OpenLDAP.

2.4 sudo make - Компилировать:

2.5 sudo make install - Установить OpenLDAP:

2.6 certs ldap.conf ldap.conf.default schema slapd.conf slapd.conf.default slapd.ldif slapd.ldif.default - При успешной установке файлы конфигурации создаются по адресу /etc/openldap. После установки доступны следующие файлы:

------------------------------------------------------------------------------------------

3.Настройка openLDAP на Centos8.

------------------------------------------------------------------------------------------

3.1 sudo mkdir /var/lib/openldap /etc/openldap/slapd.d - Во-первых, нам нужно создать каталоги базы данных OpenLDAP

3.2 Установите правильные разрешения для каталогов OpenLDAP

sudo chown -R ldap:ldap /var/lib/openldap

sudo chown root:ldap /etc/openldap/slapd.conf

sudo chmod 640 /etc/openldap/slapd.conf

------------------------------------------------------------------------------------------

4.Создать схему openLDAP sudo на Centos8.

------------------------------------------------------------------------------------------

4.1 sudo -V | grep -i "ldap" - Проверьте, поддерживает ли ваша версия sudo LDAP

4.2 Вы должны увидеть следующие строки в выводе, если ваша система поддерживает LDAP.

ldap.conf path: /etc/sudo-ldap.conf

ldap.secret path: /etc/ldap.secret

4.3 Подтвердите, доступна ли схема sudo LDAP в вашей системе.

rpm -ql sudo | grep -i schema.openldap

4.4 Пример вывода

/usr/share/doc/sudo/schema.OpenLDAP

4.5 Скопируйте схему в каталог схемы ldap.

sudo cp /usr/share/doc/sudo/schema.OpenLDAP /etc/openldap/schema/sudo.schema

4.6 Создайте файл ldif схемы sudo.

sudo su –

4.7 Выполните ниже, чтобы добавить строки в файл

cat << 'EOL' > /etc/openldap/schema/sudo.ldif dn: cn=sudo,cn=schema,cn=config objectClass: olcSchemaConfig cn: sudo olcAttributeTypes: ( 1.3.6.1.4.1.15953.9.1.1 NAME 'sudoUser' DESC 'User(s) who may run sudo' EQUALITY caseExactIA5Match SUBSTR caseExactIA5SubstringsMatch SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 ) olcAttributeTypes: ( 1.3.6.1.4.1.15953.9.1.2 NAME 'sudoHost' DESC 'Host(s) who may run sudo' EQUALITY caseExactIA5Match SUBSTR caseExactIA5SubstringsMatch SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 ) olcAttributeTypes: ( 1.3.6.1.4.1.15953.9.1.3 NAME 'sudoCommand' DESC 'Command(s) to be executed by sudo' EQUALITY caseExactIA5Match SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 ) olcAttributeTypes: ( 1.3.6.1.4.1.15953.9.1.4 NAME 'sudoRunAs' DESC 'User(s) impersonated by sudo (deprecated)' EQUALITY caseExactIA5Match SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 ) olcAttributeTypes: ( 1.3.6.1.4.1.15953.9.1.5 NAME 'sudoOption' DESC 'Options(s) followed by sudo' EQUALITY caseExactIA5Match SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 ) olcAttributeTypes: ( 1.3.6.1.4.1.15953.9.1.6 NAME 'sudoRunAsUser' DESC 'User(s) impersonated by sudo' EQUALITY caseExactIA5Match SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 ) olcAttributeTypes: ( 1.3.6.1.4.1.15953.9.1.7 NAME 'sudoRunAsGroup' DESC 'Group(s) impersonated by sudo' EQUALITY caseExactIA5Match SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 ) olcObjectClasses: ( 1.3.6.1.4.1.15953.9.2.1 NAME 'sudoRole' SUP top STRUCTURAL DESC 'Sudoer Entries' MUST ( cn ) MAY ( sudoUser $ sudoHost $ sudoCommand $ sudoRunAs $ sudoRunAsUser $ sudoRunAsGroup $ sudoOption $ description ) ) EOL

------------------------------------------------------------------------------------------

## 5. Настроить базу данных SLAPD.

------------------------------------------------------------------------------------------

5.1 Обновите содержимое файла

/etc/openldap/slapd.ldif sudo mv /etc/openldap/slapd.ldif /etc/openldap/slapd.ldif.bak

5.2 Обновите содержимое файла

sudo vi /etc/openldap/slapd.ldif

5.3

dn: cn=config objectClass: olcGlobal cn: config olcArgsFile: /var/lib/openldap/slapd.args olcPidFile: /var/lib/openldap/slapd.pid dn: cn=schema,cn=config objectClass: olcSchemaConfig cn: schema dn: cn=module,cn=config objectClass: olcModuleList cn: module olcModulepath: /usr/libexec/openldap olcModuleload: back\_mdb.la include: file:///etc/openldap/schema/core.ldif include: file:///etc/openldap/schema/cosine.ldif include: file:///etc/openldap/schema/nis.ldif include: file:///etc/openldap/schema/inetorgperson.ldif include: file:///etc/openldap/schema/ppolicy.ldif include: file:///etc/openldap/schema/sudo.ldif dn: olcDatabase=frontend,cn=config objectClass: olcDatabaseConfig objectClass: olcFrontendConfig olcDatabase: frontend olcAccess: to dn.base="cn=Subschema" by \* read olcAccess: to \* by dn.base="gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth" manage by \* none dn: olcDatabase=config,cn=config objectClass: olcDatabaseConfig olcDatabase: config olcRootDN: cn=config olcAccess: to \* by dn.base="gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth" manage by \* none

5.4 Выполните пробный запуск, чтобы проверить конфигурацию

sudo slapadd -n 0 -F /etc/openldap/slapd.d -l /etc/openldap/slapd.ldif -u

5.5 Выполните команду для записи изменений

sudo slapadd -n 0 -F /etc/openldap/slapd.d -l /etc/openldap/slapd.ldif

5.6 Приведенная выше команда создает конфигурации базы данных slapd и помещает их в /etc/openldap/slapd.d.

ls /etc/openldap/slapd.d

'cn=config' 'cn=config.ldif'

5.7 Установите права собственности на каталог slapd:

sudo chown -R ldap:ldap /etc/openldap/slapd.d

------------------------------------------------------------------------------------------

## 6. Создать службу openLAPD.

------------------------------------------------------------------------------------------

6.1 sudo nano /etc/systemd/system/slapd.service - Создайте сервис system

[Unit] Description=OpenLDAP Server Daemon

After=syslog.target network-online.target

Documentation=man:slapd

Documentation=man:slapd-mdb

[Service] Type=forking PIDFile=/var/lib/openldap/slapd.pid Environment="SLAPD\_URLS=ldap:/// ldapi:/// ldaps:///" Environment="SLAPD\_OPTIONS=-F /etc/openldap/slapd.d" ExecStart=/usr/libexec/slapd -u ldap -g ldap -h ${SLAPD\_URLS} $SLAPD\_OPTIONS

[Install] WantedBy=multi-user.target

6.2 sudo systemctl daemon-reload - Перезапустить демон

6.3 sudo systemctl enable --now slapd - Запустить сервис slapd

6.4 systemctl status slapd - Проверить состояние

------------------------------------------------------------------------------------------

## 7. Настройка корневого DN OpenLDAP по умолчанию.

------------------------------------------------------------------------------------------

7.1 Создайте базу данных MDB с корневым DN и списками ACL

sudo slappasswd - Сгенерируйте пароль root

7.2 Скопируйте сгенерированный хэш-пароль в текстовый редактор. Это будет необходимо в rootdn.ldifфайле при **olcRootPW**входе.

Sudo nano rootdn.ldif

7.3 Добавьте содержимое ниже, заменив его **dc=ldapmaster,dc=infoit,dc=com,dc=ua** информацией о вашем домене.

dn: olcDatabase=mdb,cn=config objectClass: olcDatabaseConfig objectClass: olcMdbConfig olcDatabase: mdb olcDbMaxSize: 42949672960 olcDbDirectory: /var/lib/openldap olcSuffix: dc=ldapmaster,dc=infoit,dc=com,dc=ua olcRootDN: cn=admin,dc=ldapmaster,dc=infoit,dc=com,dc=ua olcRootPW: {SSHA}0phayAb6bQA9rONibLb97O5B89KPeNlW olcDbIndex: uid pres,eq olcDbIndex: cn,sn pres,eq,approx,sub olcDbIndex: mail pres,eq,sub olcDbIndex: objectClass pres,eq olcDbIndex: loginShell pres,eq olcDbIndex: sudoUser,sudoHost pres,eq olcAccess: to attrs=userPassword,shadowLastChange,shadowExpire by self write by anonymous auth by dn.subtree="gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth" manage by dn.subtree="ou=system,dc=ldapmaster,dc=infoit,dc=com,dc=ua" read by \* none olcAccess: to dn.subtree="ou=system,dc=ldapmaster,dc=infoit,dc=com,dc=ua" by dn.subtree="gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth" manage by \* none olcAccess: to dn.subtree="dc=ldapmaster,dc=infoit,dc=com,dc=ua" by dn.subtree="gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth" manage by users read by \* none

7.4 Обновите базу данных slapd

sudo ldapadd -Y EXTERNAL -H ldapi:/// -f rootdn.ldif

------------------------------------------------------------------------------------------

## 8. Определите структуру вашей организации.

------------------------------------------------------------------------------------------

8.1 Создайте basedn.ldifфайл, чтобы определить структуру вашей организации.

Sudo Nano basedn.ldif

8.2 С информацией, аналогичной приведенной ниже — обновите в соответствии с вашим доменом.

dn: dc=ldapmaster,dc=infoit,dc=com,dc=ua

objectClass: dcObject

objectClass: organization

objectClass: top

o: infoit

dc: ldapmaster dn: ou=groups,dc=ldapmaster,dc=infoit,dc=com,dc=ua

objectClass: organizationalUnit

objectClass: top

ou: groups

dn: ou=people,dc=ldapmaster,dc=infoit,dc=com,dc=ua

objectClass: organizationalUnit

objectClass: top

ou: people

8.3 Обновление базы данных

sudo ldapadd -Y EXTERNAL -H ldapi:/// -f basedn.ldif  
------------------------------------------------------------------------------------------

## 9. Настроить SSL / TLS

------------------------------------------------------------------------------------------

Вы можете защитить связь клиент-сервер между OpenLDAP и клиентскими системами, включив TLS / SSL.

Для этого вы можете использовать самоподписанный сертификат или Let’s Encrypt. В этом руководстве мы будем использовать самоподписанный сертификат.

9.1 sudo openssl req -x509 -nodes -days 365 \

-newkey rsa:2048 \

-keyout /etc/pki/tls/ldapserver.key \

-out /etc/pki/tls/ldapserver.crt

9.2 Установите правильное владение

sudo chown ldap:ldap /etc/pki/tls/{ldapserver.crt,ldapserver.key}

9.3 Создайте файл конфигурации SSL

Sudo nano add-tls.ldif

9.4 С информацией ниже

dn: cn=config

changetype: modify

add: olcTLSCACertificateFile

olcTLSCACertificateFile: /etc/pki/tls/ldapserver.crt

-

add: olcTLSCertificateKeyFile

olcTLSCertificateKeyFile: /etc/pki/tls/ldapserver.key

-

add: olcTLSCertificateFile

olcTLSCertificateFile: /etc/pki/tls/ldapserver.crt

9.5 Обновить базу данных slapd

sudo ldapadd -Y EXTERNAL -H ldapi:/// -f add-tls.ldif

9.6 Обновите расположение CA для OpenLDAP

sudo nano /etc/openldap/ldap.conf

#TLS\_CACERT /etc/pki/tls/cert.pem TLS\_CACERT/etc/pki/tls/ldapserver.crt

------------------------------------------------------------------------------------------

## 10. Создать пользователей OpenLDAP

------------------------------------------------------------------------------------------

10.1 Определите своих пользователей в файле users.ldif следующим образом

sudo nano users.ldif

10.2

dn:

uid=vshamallah,ou=people,dc=ldapmaster,dc=infoit,dc=com,dc=ua

objectClass: inetOrgPerson

objectClass: posixAccount

objectClass: shadowAccount

uid: vshamallah

cn: Vic

sn: Shamallah

loginShell: /bin/bash

uidNumber: 10000

gidNumber: 10000

homeDirectory: /home/vshamallah

shadowMax: 60

shadowMin: 1

shadowWarning: 7

shadowInactive: 7

shadowLastChange: 0

dn:

cn=vshamallah,ou=groups,dc=ldapmaster,dc=infoit,dc=com,dc=ua

objectClass: posixGroup

cn: vshamallah

gidNumber: 10000

memberUid: vshamallah

10.3 Обновите базу данных LDAP, чтобы добавить нового пользователя:

sudo ldapadd -Y EXTERNAL -H ldapi:/// -f users.ldif

10.4 Установите пароль для указанного выше пользователя с помощью команды ниже:

sudo ldappasswd -H ldapi:/// -Y EXTERNAL -S "uid=vshamallah,ou=people,dc=ldapmaster,dc=infoit,dc=com,dc=ua"

------------------------------------------------------------------------------------------

## 11. Создать пользователей привязки OpenLDAP

------------------------------------------------------------------------------------------

Создайте OpenLDAP Bind DN и привяжите пользователя. Это пользователь, который будет использоваться для выполнения открытий LDAP, таких как разрешение идентификаторов пользователей и групп.

11.1 Создайте пароль BindDN

sudo slappasswd

New password:

Re-enter new password:

{SSHA}9Sx4MzBieiojFsXLgXDVnJavwt4vql4p

11.2 Получите хешированный пароль и сохраните его где-нибудь

Создайте файл bindDNuser.ldif и добавьте содержимое ниже, не забудьте заменить хешированный пароль и информацию о домене своими данными.

Sudo nano bindDNuser.ldif

11.3 Вот мои конфигурации

dn: ou=system,dc=ldapmaster,dc=infoit,dc=com,dc=ua objectClass: organizationalUnit  
objectClass: top  
ou: system

dn: cn=readonly,ou=system,dc=ldapmaster,dc=infoit,dc=com,dc=ua objectClass: organizationalRole  
objectClass: simpleSecurityObject  
cn: readonly  
userPassword: {SSHA}9Sx4MzBieiojFsXLgXDVnJavwt4vql4p  
description: Bind DN user for LDAP Operations

11.4 Обновите базу данных ldap

sudo ldapadd -Y EXTERNAL -H ldapi:/// -f bindDNuser.ldif

------------------------------------------------------------------------------------------

## 12. Разрешить OpenLDAP через брандмауэр

## ------------------------------------------------------------------------------------------

12.1 Разрешить OpenLDAP через брандмауэр, чтобы разрешить соединения.

sudo firewall-cmd --add-service={ldap,ldaps} --permanent sudo firewall-cmd --reload

На этом этапе OpenLDAP настроен и готов к использованию. Вам необходимо настроить клиентов OpenLDAP в своих системах, чтобы они могли подключаться к серверу OpenLDAP.

Следуйте приведенному ниже руководству, чтобы настроить клиентов OpenLDAP:

[Настроить клиент LDAP в Ubuntu](https://infoit.com.ua/linux/ubuntu/kak-nastroit-klient-ldap-v-ubuntu-20-04-18-04-16-04/)