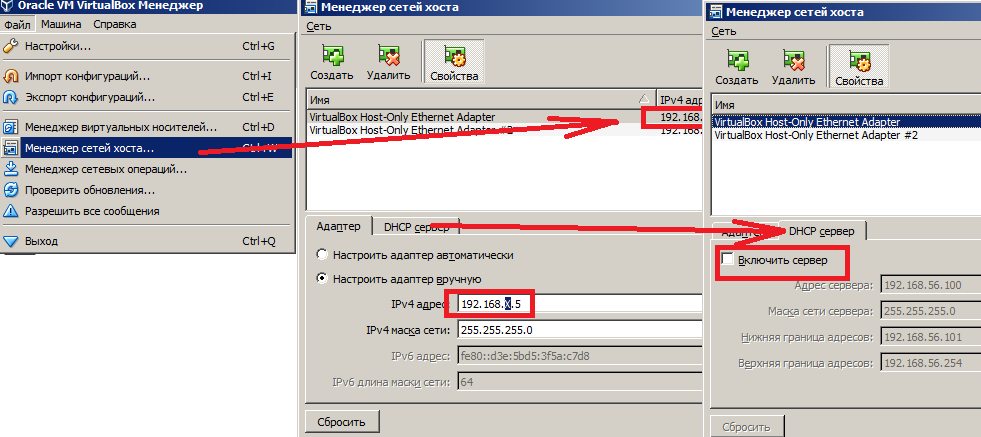
**Настройка стенда**

**Настройка сетей в VirtualBox:**

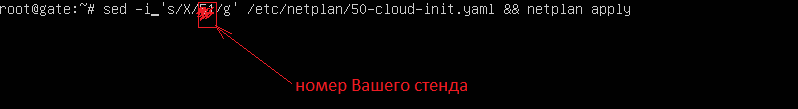
****

Настройка виртуальных машин Linux:

**В консоли выполнить настройку IP-адреса (на клиенте Client1 перейти в консоль нажав Ctrl + Alt +F1):**

sed -i 's/X/номер\_стенда/g' /etc/netplan/50-cloud-init.yaml && netplan apply

В /etc/hosts у всех машин



**Далее, подключитесь через PuTTY и настройте файл hosts:**

cat<<EOF > **/etc/hosts**

192.168.X.1 gate.corpX.un gate

192.168.X.10 server.corpX.un server

192.168.X.30 client1.corpX.un client1

127.0.1.1 `hostname`

EOF

# sed -i 's/X/номер\_стенда/g' /etc/hosts

На всех системах настроить таймзону:

timedatectl set-timezone Europe/Moscow

ДОП!!!  
vim /etc/netplan/50-cloud-init.yaml

# This file is generated from information provided by

# the datasource. Changes to it will not persist across an instance.

# To disable cloud-init's network configuration capabilities, write a file

# /etc/cloud/cloud.cfg.d/99-disable-network-config.cfg with the following:

# network: {config: disabled}

network:

ethernets:

enp0s3:ip a

addresses: [192.168.12.30/24]

gateway4: 192.168.12.1

nameservers:

addresses: [192.168.12.10, 172.16.1.254]

dhcp4: false

optional: false

version: 2

(Делать не надо)

**На ВМ Server отключаем systemd-resolved:**

systemctl stop systemd-resolved

systemctl disable systemd-resolved

rm /etc/resolv.conf

**и настраиваем разрешение имен:**

cat > /etc/resolv.conf

nameserver 127.0.0.1

**Использование NIS для аутентификации и авторизации пользователей в сети**

**NIS Используется для тиражирования информации, которая обычно хранится в файлах passwd, group, hosts, shells.**

В систему **server** добавляем пользователей ivanov с uid=10001 gid=10001 и petrov с uid=10002 gid=10002

Заполняем поля GECOS (name, office, work phone, home phone), назначаем шел bash или csh

# useradd ivanov -m -s /bin/bash -u 10001 -c 'Ivanov Ivan Ivanovitch,239,45-67,499-239-45-23'

# useradd petrov -m -s /bin/bash -u 10002 -c 'Petrov Petr Petrovitch,238,45-68,499-239-45-24'

# passwd ivanov

password1

# passwd petrov

password2

# getent passwd – список пользователей с параметрами

В систему server добавляем группу group1 и включаем в нее user1 и user2

# groupadd -g 15001 group1

# gpasswd -M ivanov,petrov group1

# getent group | grep group1

Файл, на основе которого строится карта (например**/etc/passwd),** может содержать записи, начинающиеся со знака минус или плюс. Это определяет исключение или включение (соответственно) информации о пользователях и группах в карты NIS.

**Пример:**

vim /etc/passwd

-user1:x:1000:1004:user1:/home/user1:/bin/bash

/usr/lib/yp/ypinit -m

На Server:

# apt update && apt install nis -y

~~systemctl add-wants multi-user.target rpcbind.service~~ В ubuntu 18 создается автоматически



Имя домена **не предусматривает суффикса** и определяется в файле:

# cat /etc/defaultdomain

corp51

Настраиваем NIS в качестве сервера

vim /etc/default/nis

NISSERVER=master

NISCLIENT=false

Перезапустить сервис NIS:

systemctl restart nis.service

**Прим**. перезапуск займет примерно 3 минуты.

Инициализируем базу данных (каталог «/var/yp/corp51»):

# /usr/lib/yp/ypinit -m (m – master s-slave)

...

master server : server.corpX.un

next host to add: ^D

...

Настройка NIS клиента на Client1:

# apt update && apt install nis

**!!! Внимание – по умолчанию обычно стоит copX.un -> .un – убрать!!!**

****

**#** ~~systemctl add-wants multi-user.target rpcbind.service~~

# systemctl status nis.service

# ypcat passwd

Подключение просмотра карт NIS через файлы:

client1:~# cat >> /etc/passwd

+

client1:~# cat >> /etc/shadow

+

client1:~# cat >> /etc/group

+

Проверка

# id ivanov

# id petrov

# getent passwd

**Подключение просмотра карт NIS с** **использованием библиотеки NSS**

vim /etc/nsswitch.conf

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

passwd: compat systemd nis

group: compat systemd nis

shadow: compat nis

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

# getent passwd ivanov

**Подключение второго NIS-домена.**

**На server:**

# useradd -m -s /bin/bash sidorov

# passwd sidorov

# domainname comp51

или cat > /etc/defaultdomain

compX

# systemctl restart nis.service

vim /etc/passwd

**-ivanov**:x:10001:10001:Ivanov Ivan Ivanovitch,239,45-67,499-239-45-23:/home/ivanov:/bin/bash

**-petrov**:x:10002:10002:Petrov Petr Petrovitch,238,45-68,499-239-45-24:/home/petrov:/bin/bash

# /usr/lib/yp/ypinit -m

# ls /var/yp/

**На client1:**

# cat > /etc/defaultdomain

compX

# systemctl restart nis.service

# ypcat passwd

# domainname

**Для того, чтобы пользователи смогли заходить на клиент, надо обеспечить им домашние каталоги:**

**Автоматическое создание домашних каталогов**

# apt install libpam-modules -y

# cat >> /etc/pam.d/common-session

Добавить последней строкой:

session required pam\_mkhomedir.so

Проверяет, если каталога нет - то создает его.

**# reboot**

**Войти через PuTTY под ivanov и в консоль как petrov**

****

Использование LDAP и Kerberos

**Настройка сервера BIND** на **server:**

cat<<EOF >> /etc/bind/named.conf.local

zone "corpX.un" {

type master;

file "/etc/bind/corpX.un";

};

EOF

# sed -i 's/X\./номер стенда\./g' /etc/bind/named.conf.local

cat > /etc/bind/corpX.un

$TTL 3h

@ SOA ns root.ns 1 1d 12h 1w 3h

NS ns

ns A 192.168.X.10

gate A 192.168.X.1

server A 192.168.X.10

client1 A 192.168.X.30

client2 A 192.168.X.31

\_kerberos.\_udp SRV 01 00 88 server

\_kerberos.\_tcp SRV 01 00 88 server

\_kerberos TXT CORPX.UN

# sed -i 's/X\./номер стенда\./g' /etc/bind/corpX.un

# rndc reload

# named-checkconf -z

**LDAP**

**Упражнение 1. Настройка сервера LDAP**

1. Откройте ssh-сеанс с server.
2. Установите следующие пакеты:

apt install slapd ldap-utils

**~~apt install libldap-2.4-2 libgnutls30 slapd ldap-utils -y~~**

Задайте в мастере установки пароль администратора: **secret**

В Ubuntu объект dc=corpX,dc=un создается автоматически при инсталляции

**ldapsearch -x -b dc=corpX,dc=un**

**##############################################################################**

**В случае необходимости можно переконфигугировать:**

**dpkg-reconfigure slapd**

**доменное имя : corpX.un**

**Название организации: corpX**

**Administrative password: secret**

**Удалять старую базу? Нет**

**Переместить? Нет**

**Включить ldapv2 - Нет**

**# ldapsearch -x -b dc=corpX,dc=un**

**##############################################################################**

**Упражнение 2. Создание подразделений**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Создайте файл с описанием структуры подразделений:

cat > orgstructure.ldif

Введите

dn: ou=users,dc=corpX,dc=un

objectClass: organizationalUnit

ou: users

dn: ou=groups,dc=corpX,dc=un

objectClass: organizationalUnit

ou: groups

**Отредактируйте файл:**

# sed -i 's/X/номер\_стенда/g' orgstructure.ldif

**Импортируйте данные из файла в каталог:**

server# ldapadd -x -D "cn=admin,dc=corpX,dc=un" -w secret -f orgstructure.ldif

**Чтение каталога**

server:~# ldapsearch -x -b "dc=corpX,dc=un"

**Импорт данных о пользователях и группах**

Создайте файл с описанием пользователей и групп:

cat > passwdgroup.ldif

**Введите следующее содержимое:**

dn: cn=ivanov,ou=groups,dc=corpX,dc=un

objectClass: posixGroup

cn: ivanov

gidnumber: 10001

dn: cn=petrov,ou=groups,dc=corpX,dc=un

objectClass: posixGroup

cn: petrov

gidnumber: 10002

dn: uid=ivanov,ou=users,dc=corpX,dc=un

objectClass: inetOrgPerson

objectClass: posixAccount

uid: ivanov

sn: Ivanov

cn: Ivanov Ivan Ivanovitch

gecos: Ivanov Ivan Ivanovitch,239,45-67,499-239-45-23

uidNumber: 10001

gidNumber: 10001

loginshell: /bin/sh

homeDirectory: /home/ivanov

userpassword: \*

dn: uid=petrov,ou=users,dc=corpX,dc=un

objectClass: inetOrgPerson

objectClass: posixAccount

uid: petrov

sn: Petrov

cn: Petrov Petr Petrovitch

gecos: Petrov Petr Petrovitch,240,45-68,499-323-55-53

uidnumber: 10002

gidnumber: 10002

loginshell: /bin/sh

homedirectory: /home/petrov

userpassword: \*

dn: cn=group1,ou=groups,dc=corpX,dc=un

cn: group1

gidNumber: 15001

memberUid: ivanov

memberUid: petrov

objectClass: posixGroup

**Отредактируйте файл:**

**sed -i 's/X/номер\_стенда/g' passwdgroup.ldif**

**Импортируйте данные из файла в каталог:**

ldapadd -x -D "cn=admin,dc=corpX,dc=un" -w secret -f passwdgroup.ldif

**Задайте пароль пользователям:**

По умолчанию используется SSHA, или более широко известный как ‘salted SHA1’

ldappasswd -H ldap:// -x -D "cn=admin,dc=corp51,dc=un" -W -S "uid=petrov,ou=users,dc=corp51,dc=un"

New password: lpassword

Re-enter new password: lpassword

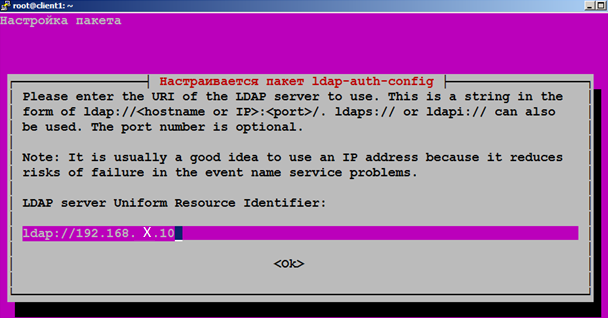
Enter LDAP Password: secret

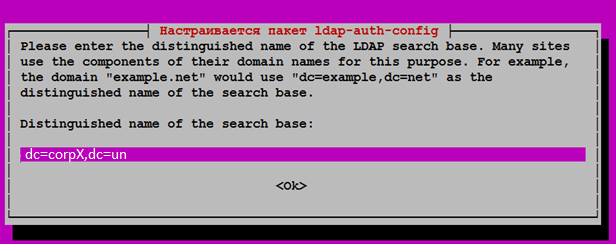
**Упражнение 4. Настройка клиента LDAP**

1. Откройте ssh-сеанс с client1.
2. Установите пакеты:

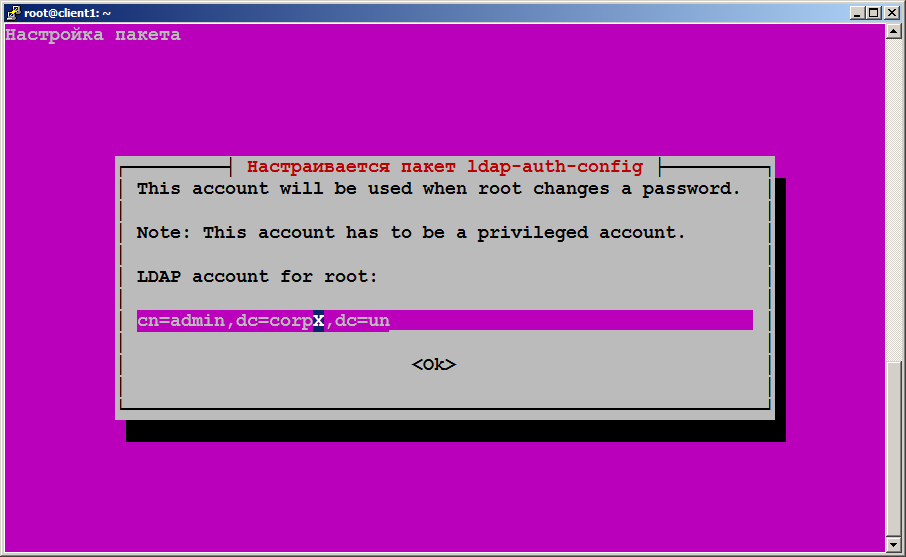
apt install libnss-ldap -y

1. Используйте следующие настройки:





Далее по умолчанию



В последнем окне ведите пароль администратора: **secret**

**Проблемы на клиенте, связанные с невозможностью подключения к LDAP серверу** thunderbird и systemd-logind такие как:

nss\_ldap: could not search LDAP server - Server is unavailable

client1 systemd-logind[901]: nss\_ldap: could not connect to any ver

client1 systemd-logind[901]: nss\_ldap: could not connect to any LDAP server as cn=admin,dc=corp51,dc=un - Can't contact LDAP server

client1 thunderbird[1854]: nss\_ldap: could not connect to any LDAP server as (null) - Unknown error

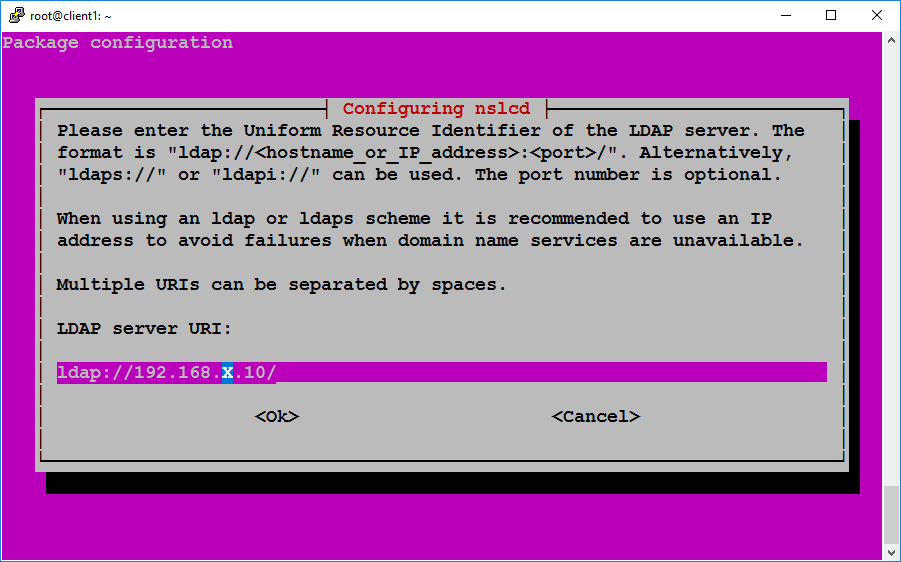
Решаются заменой пакета **libnss-ldap** на **libnss-ldapd**

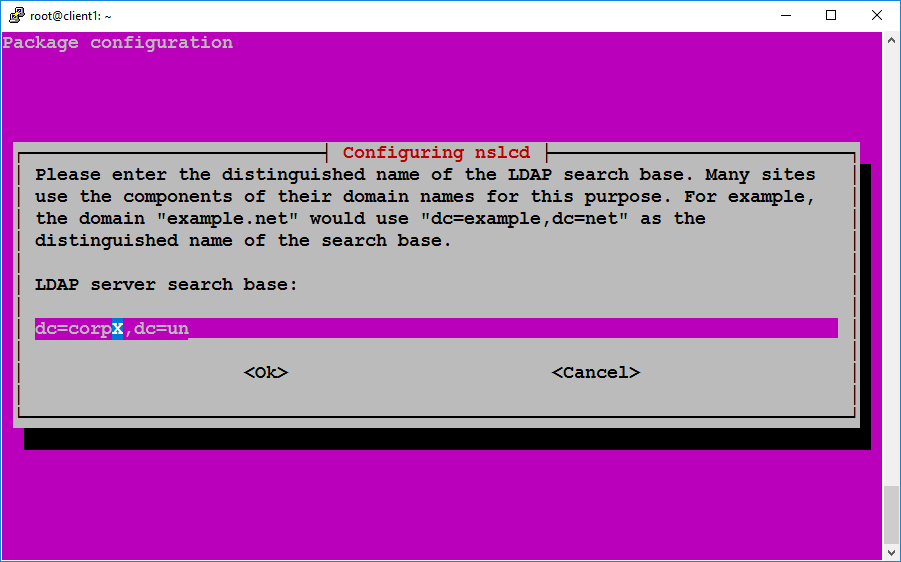
**problem with desktop clients resolved replacing the libnss-ldap package with libnss-ldapd.**

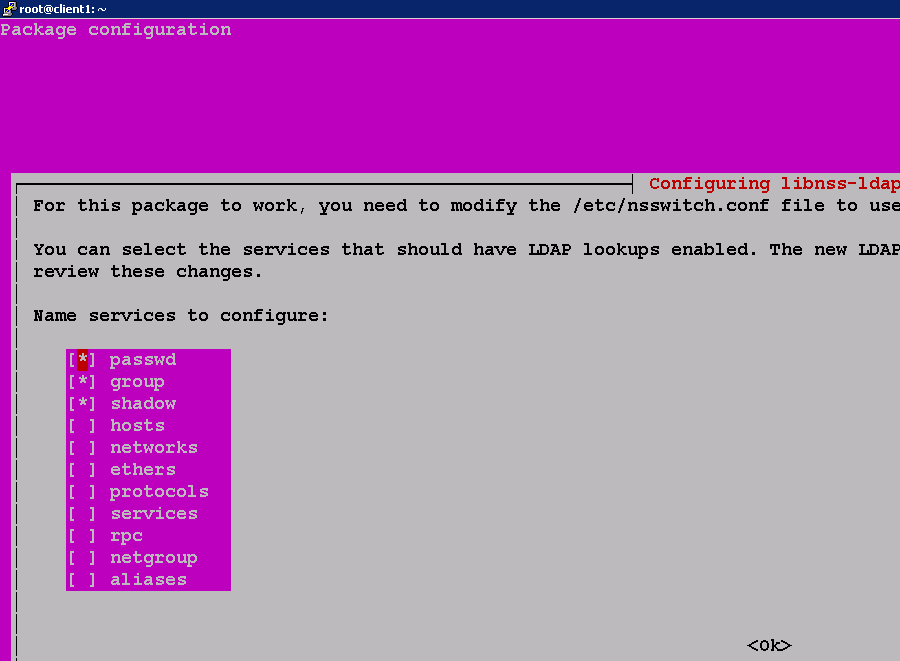
**Seems the same issue as in this bug report:**[**https://bugs.launchpad.net/ubuntu/+source/libnss-ldap/+bug/1024475**](https://bugs.launchpad.net/ubuntu/+source/libnss-ldap/+bug/1024475)

<https://askubuntu.com/questions/797896/16-04-server-enabling-ldap-authentication-causes-systemd-logind-to-fail>

apt purge libnss-ldap && apt install libnss-ldapd







После чего перезагружаем систему:

**# reboot**

Для проверки подключения установите пакет: **apt install ldap-utils**

Выполните: ldapsearch -x -b dc=corpX,dc=un -h server

**Прим**. Для этой части можно перезаписать значения выходного файла /etc/ldap.conf требуемыми.

**Упражнение 5. Настройка аутентификации и авторизации клиента средствами LDAP**

1. Отредактируйте конфигурационный файл: vim /etc/nsswitch.conf
2. Найдите в файле строки passwd, group и shadow и отредактируйте их следующим образом:

passwd:         compat ldap  
group:          compat ldap  
shadow:        compat ldap

1. Команда **id ivanov** теперь найдет пользователя и вернет данные о нем из LDAP
2. Проверьте возможность использования для аутентификации обоих протоколов: LDAP и NIS:

vim /etc/nsswitch.conf

passwd: compat nis ldap

group: compat nis ldap

shadow: compat nis ldap

1. Войдите под Ivanov с паролем password1 затем с паролем lpassword1