**Kerberos**

Установка KDC и регистрация принципалов

root@server:~# apt install krb5-kdc krb5-admin-server

**Настройка имени домена в файле:**

server# cat > /etc/krb5.conf

[libdefaults]

default\_realm = CORPX.UN

Генерация ключа KDC:

server# **krb5\_newrealm**

Ввести мастер ключ: secret

systemctl restart krb5-kdc

**Регистрация принципалов пользователей в базе данных kerberos**

root@server:~# kadmin.local

kadmin.local: addprinc ivanov

...

Enter password for principal "ivanov@CORPX.UN": kpassword

Re-enter password for principal "ivanov@CORPX.UN": kpassword

...

kadmin.local: addprinc petrov

...

kadmin.local: listprincs

...

kadmin.local: q

Запросим TGT для Ivanov:

root@server:~# kinit ivanov

Посмотреть выданные тикеты:

root@server:~# klist

Удалить все ключи:

# kdestroy

**Настройка Kerberos клиента**

root@client1:~# apt install krb5-user

Файл определяет принадлежность к Kerberos realm:

root@client1:~# cat > /etc/krb5.conf

[libdefaults]

default\_realm = CORPX.UN

После добавления клиента в домен Kerberos realm, можно запросить с него пользовательский тикет:

root@client1:~# kinit ivanov

root@client1:~# klist

root@client1:~# kdestroy

**Использование GSSAPI для аутентификации**

**Настройка pam\_krb5 для сервиса login/xdm**

root@client1:~# apt install libpam-krb5

все настроится автоматически, она пропишется в:

root@client1:~# grep krb5 /etc/pam.d/\*

Найдите в файле /etc/nsswitch.conf строку shadow и уберите оттуда ldap:

passwd: compat ldap

group: compat ldap

**shadow: compat**

**root@client1:~# reboot**

Заходим в консоль клиента client1 как ivanov c kpassword

Проверяем:

# klist

**Итог:**

**Для связки Kerberos+LDAP на клиенте нужны:**

**Поставить клиент Kerberos и указать Realm**

**apt install krb5-user**

**cat /etc/krb5.conf**

**Поставить PAM для Kerberos аутентификации**

**apt install libpam-krb5**

**Настроить параметры, где искать учетные записи для авторизации:**

**vim /etc/nsswitch.conf**

**Настроить автосоздание домашних каталогов**

**# vim /etc/pam.d/common-session**

**…**

**session required pam\_mkhomedir.so**

**установите пакет:**

**apt install libpam-modules**

**Данный пакет дополняет набор модулей для PAM. Он включает модуль pam\_unix.so, а также некоторые специализированные модули.**

**Поставить клиент LDAP и указать параметры доступа к серверу каталога:**

**(В случае WINBIND в нем нет необходимости)**

**apt-get install libnss-ldap**

**Реализация Единого входа - SSO**

**Регистрируем сервис в KDC для реализации SSO:**

**Регистрация принципалов сервиса в KDC и перемещение ключа сервиса на сервер**

root@server:~# kadmin.local

Пароль для сервиса генерируется случайно, host –тип сервиса для ssh:

kadmin.local: addprinc -randkey host/gate.corpX.un

Вывести список участников безопасности:

kadmin.local: listprincs

Пароль сервиса нужно передать на хост сервиса, выгрузив в двоичный файл gatehost.keytab:

kadmin.local: ktadd -k gatehost.keytab host/gate.corpX.un

Выход из оснастки:

kadmin.local: quit

Пароль сервиса передать на хост сервиса:

server# scp gatehost.keytab gate:

и он будет скопирован на gate в /root

Поскольку сервис ищет пароль в /etc/krb5.keytab то его туда нужно корректно добавить:

**Добавление ключа в системный keytab**

**Ubuntu (MIT)**

root@gate:~# apt install krb5-user

# cat > /etc/krb5.conf

[libdefaults]

default\_realm = CORPX.UN

root@gate:~# ktutil

ktutil: rkt /root/gatehost.keytab – считать в ОЗУ содержимое файла

ktutil: list – отобразит список ключей в ОЗУ

ktutil: wkt /etc/krb5.keytab – и записать в файл

ktutil: quit

посмотреть содержимое файла:

root@gate:~# klist -ek /etc/krb5.keytab

KVNO Principal

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

2 host/gate.corp51.un@CORP51.UN (aes256-cts-hmac-sha1-96)

2 host/gate.corp51.un@CORP51.UN (aes128-cts-hmac-sha1-96)

2 host/gate.corp51.un@CORP51.UN (aes256-cts-hmac-sha1-96)

2 host/gate.corp51.un@CORP51.UN (arcfour-hmac)

2 host/gate.corp51.un@CORP51.UN (des3-cbc-sha1)

2 host/gate.corp51.un@CORP51.UN (des-cbc-crc)

**Настройка unix клиента ssh на использование GSSAPI**

**В linux ничего делать в данном пункте не надо!**

client1# less /etc/ssh/ssh\_config

В конце файла автоматически появится строчка:

...

GSSAPIAuthentication yes

...

**Настройка Gate**

**gate:~# apt install libpam-krb5**

**vim /etc/nsswitch.conf**

**passwd: compat ldap**

**group: compat ldap**

**apt install libnss-ldapd**

**apt install libpam-modules**

**vim /etc/pam.d/common-session**

**…**

**session required pam\_mkhomedir.so**

**Настройка сервиса sshd на использование GSSAPI**

gate# vim /etc/ssh/sshd\_config

...

GSSAPIAuthentication yes

...

root@gate:~# service ssh restart

(# systemctl restart sshd)

Проверяем:

Входим в консоль на client1 как ivanov с паролем kpassword

Выполняем ssh gate

Пароль более не запрашивается, ибо для входа используется тикет.

**Использование GSSAPI для сервиса http proxy**

**Ставим SQUID на gate:**

Установка, настройка и запуск пакета SQUID

root@gate:~# apt install squid

**Аутентификация доступа к SQUID**

Создаем ключи сервиса и копируем иx на сервер

root@server:~# kadmin.local

kadmin.local: addprinc -randkey HTTP/gate.corpX.un

Для случая, когда принципалом будет Windows:

kadmin.local: addprinc -e rc4-hmac:normal -randkey HTTP/gate.CORPX.UN

kadmin.local: ktadd -k gatehttp.keytab HTTP/gate.corpX.un

kadmin.local: ktadd -k gatehttp.keytab HTTP/gate.CORPX.UN

kadmin.local: exit

**Копируем ключи на** gate:

server# scp gatehttp.keytab gate:

**Копируем ключи в системный keytab**

root@gate:~# ktutil

ktutil: rkt /root/gatehttp.keytab

ktutil: list

ktutil: wkt /etc/krb5.keytab

ktutil: quit

root@gate:~# klist -ek /etc/krb5.keytab

У прокси нет прав на файл. Даем их (лучше группе)

gate# chmod +r /etc/krb5.keytab ##(пользователю proxy правильнее)

Настраиваем прокси:

**root@gate:~# vim /etc/squid/squid.conf**

# OPTIONS FOR AUTHENTICATION

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

auth\_param negotiate program /usr/lib/squid/negotiate\_kerberos\_auth -d

…

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

### имя acl и тип

acl inetuser proxy\_auth REQUIRED

http\_access allow inetuser

root@gate:~# squid -k check

root@gate:~# squid -k reconfigure

Входим в консоль client1 как ivanov

В терминале для проверки запустить klist и увидеть tgt

Applications Menu -> Internet -> Firefox -> [Menu Bar] -> Edit -> Preferences -> Advanced -> Network -> Settings:

Manual Configuration:

HTTP Proxy: gate Port: 3128

Ok

<http://ya.ru>

Смотрим лог на Gate:

**# tail -f /var/log/squid/access.log**

…

1469565819.728 74 192.168.51.30 TCP\_MISS/200 962 POST http://clients1.google.com/ocsp ivanov@CORP51.UN HIER\_DIRECT/173.194.221101 application/ocsp-response

**----**

**Регистрация рабочих станций windows в KDC**

Зона прямого просмотра настраивалась ранее, теперь необходимо все системы корректно прописать в зоне обратного просмотра DNS

**Создание и настройка зоны обратного просмотра на системе Server:**

Добавить в конец файла:

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

zone "X.168.192.IN-ADDR.ARPA" {

type master;

file "/var/cache/bind/X.168.192.IN-ADDR.ARPA";

};

Отредактировать файл:

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

Создать файл зоны, на который сослались ранее:

cat > /var/cache/bind/X.168.192.IN-ADDR.ARPA

$TTL 3h

@ SOA server.corpX.un. root.server.corpX.un. 1 1d 12h 1w 3h

NS server.corpX.un.

1 PTR gate.corpX.un.

10 PTR server.corpX.un.

30 PTR client1.corpX.un.

31 PTR client2.corpX.un.

Отредактировать файл:

sed -i 's/X/номер\_стенда/g' /var/cache/bind/X.168.192.IN-ADDR.ARPA

Перезагрузить сервис

systemctl restart bind9

Создаем учетную запись клиента Windows

kadmin.local

kadmin.local: addprinc -e rc4-hmac:normal host/client2.corpX.un

...

Enter password for principal "host/client2.corpX.un@CORPX.UN": 12345678

...

kadmin.local: listprincs

kadmin.local: q

**Импортируем и настраиваем клиент Windows:**

Windows Client2 - 192.168.X.31/24

Preferred DNS Server: 192.168.X.10

Имя ставим Client2

На Win Client2:

Нужно создать локального пользователя для обеспечения возможности входа и создания профиля на рабочей станции. Пароль для локальной учетной записи не важен, ибо при аутентификации **KERBEROS** будет использоваться соотв. пароль **в KDC**

Запускаем командную строку от имени администратора:

net user petrov /add 123

net user ivanov /add 123

**Подключение к KERBEROS**

!!! Проверить, что время синхронизировано!!!

В случае Windows клиента, пользователи должны быть также заведены локально в SAM с произвольным паролем !!!

net user petrov /add 123

В Windows при логине явно указывать имя petrov@CORPX.UN

cmd.exe запускать с правами администратора

На Win Client2:

C:\>ksetup /setrealm CORPX.UN ##– установка домена

C:\>ksetup /addkdc CORPX.UN server.corpX.un ## – указания центра распределения ключей

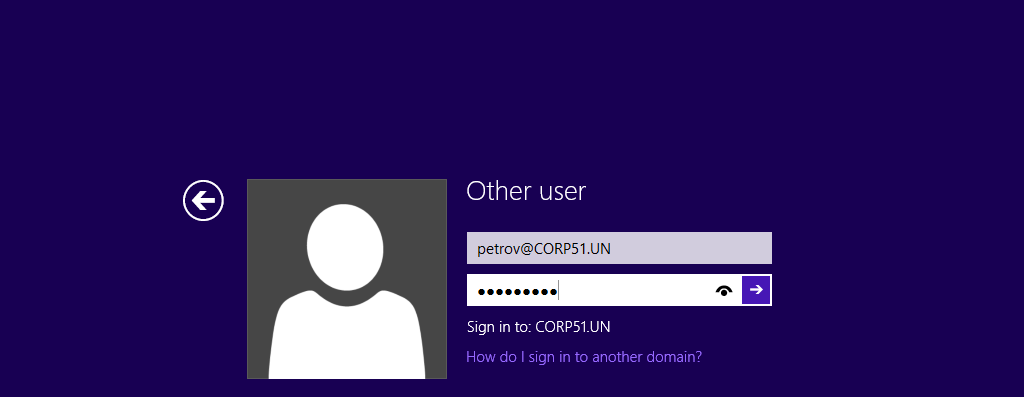
C:\>ksetup /setcomputerpassword 12345678

C:\>ksetup /mapuser \* \* ## имена локальных пользователей совпадают с именами пользователей KDC.

Перезагружаем клиент.

shutdown –r –t 0

Заходим как petrov@CORPX.UN, но с паролем kpassword2



#####################################################################################

**Если сталкиваемся с ошибкой вида:**

**root@server:~# journalctl -f**

server krb5kdc[884]: AS\_REQ (6 etypes {18 17 23 24 -135 3}) 192.168.51.31: CLIENT\_NOT\_FOUND: client2$@CORP51.UN for krbtgt/CORP51.UN@CORP51.UN, Client not found in Kerberos database

**То делаем:**

~~kadmin.local: addprinc -e rc4-hmac:normal client2$@CORP51.UN~~

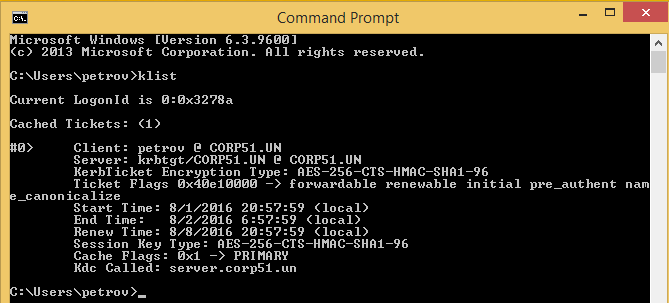
kadmin.local: addprinc -e rc4-hmac:normal host/client2$@CORP51.UN

client2$@CORP51.UN

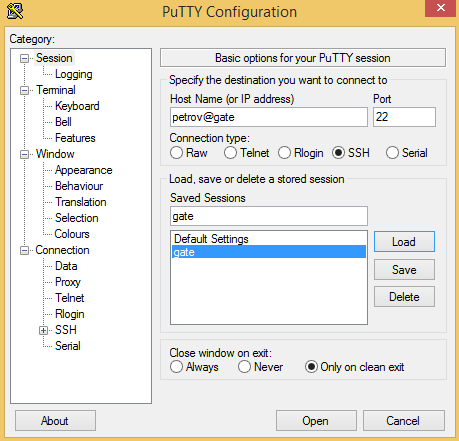
host/client2$@CORP51.UN

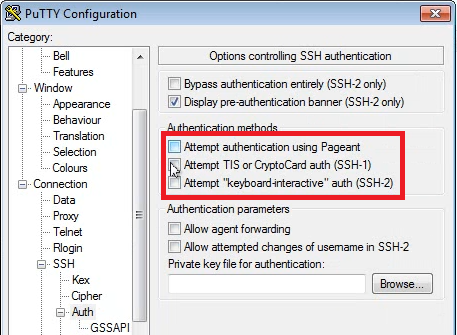
#####################################################################################

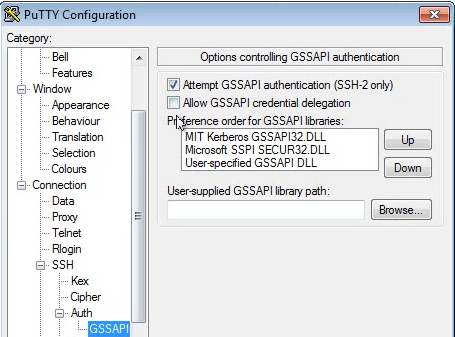
Проверяем тикет: klist

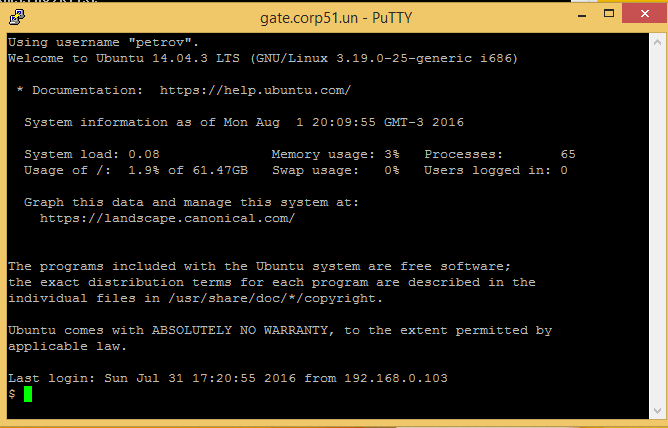


Putty не берет информацию о вошедшем в систему пользователе, соотв, нужно явно указывать:









Cmd> klist

Настроить IE на proxy gate 3128

Gate:

# tail -fn0 /var/log/squid/access.log

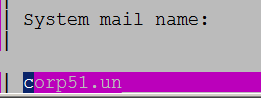
“petrov@CORPX.UN”

**Опциональные упражнения:**

**Demo: Использование протокола GSSAPI для сервиса imap.**

**На Gate:**

**# apt install mailutils**

****

**# mail ivanov**

**111**

**111**

**^D**

**# cat /var/mail/ivanov**

**C поддержкой GSSAPI**

**root@gate:~# apt install dovecot-imapd dovecot-gssapi**

**Все по дефолту**

**root@gate:~# cd /etc/dovecot/conf.d/**

**# vim 10-mail.conf**

**...**

**mail\_privileged\_group = mail**

**...**

**Kerberos GSSAPI аутентификация**

**Создаем ключи сервиса и копируем иx на сервер**

**На Server:**

**# kadmin.local**

**# addprinc -randkey imap/gate.corpX.un**

**# addprinc -e rc4-hmac:normal -randkey imap/gate.CORPX.UN**

**# ktadd -k gateimap.keytab imap/gate.corpX.un**

**# ktadd -k gateimap.keytab imap/gate.CORPX.UN**

**# exit**

**# scp gateimap.keytab gate:**

**Копируем ключи в системный keytab**

**root@gate:~# ktutil**

**ktutil: rkt /root/gateimap.keytab**

**ktutil: wkt /etc/krb5.keytab**

**ktutil: quit**

**root@gate:~# klist -k /etc/krb5.keytab**

**...**

**root@gate:~# vim /etc/dovecot/conf.d/10-auth.conf**

**...**

**auth\_gssapi\_hostname = "$ALL"**

**...**

**auth\_mechanisms = gssapi**

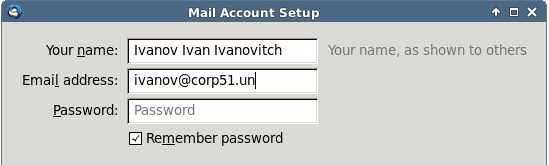
**...**

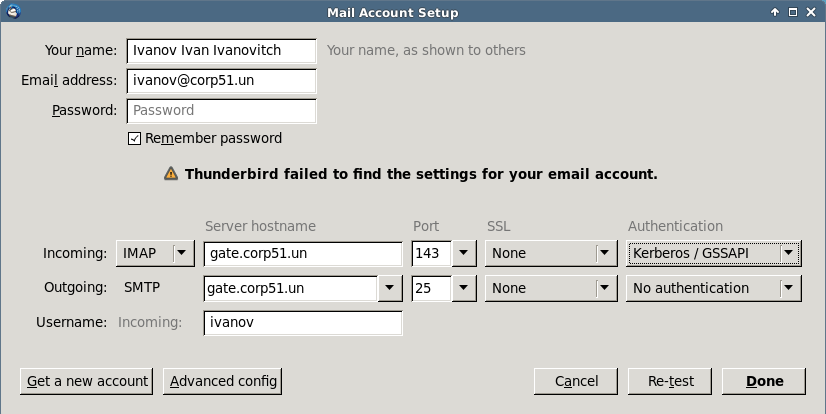
**# service dovecot restart**

**# tail -f /var/log/mail.log**

**На Client1:**

**Ввести только почтовый адрес:**

****

****

**root@gate:~# tail -f /var/log/mail.log**

**Jul 30 17:31:14 gate dovecot: imap-login: Login: user=<ivanov>, method=GSSAPI, rip=192.168.51.30, lip=192.168.51.1, mpid=9076, session=<cyknFuE40gDAqDMe>**

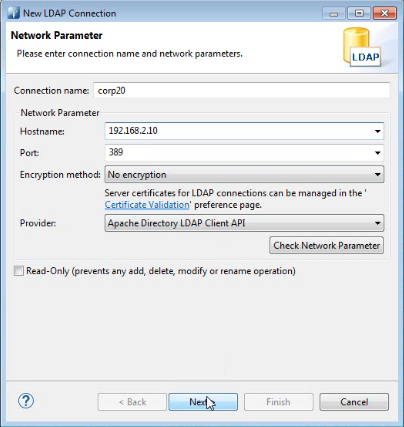
**----**

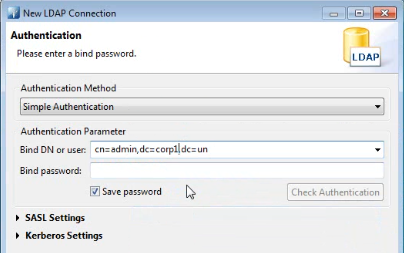
**Подключение LDAP в качестве адресной книги**

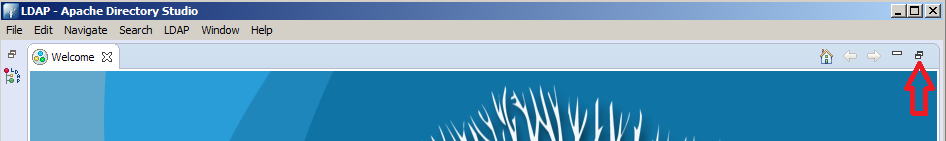
**На хостовой машине распаковать ApacheDirectoryStudio-2.0.0.v20151221-M10-win32.win32.x86.zip**

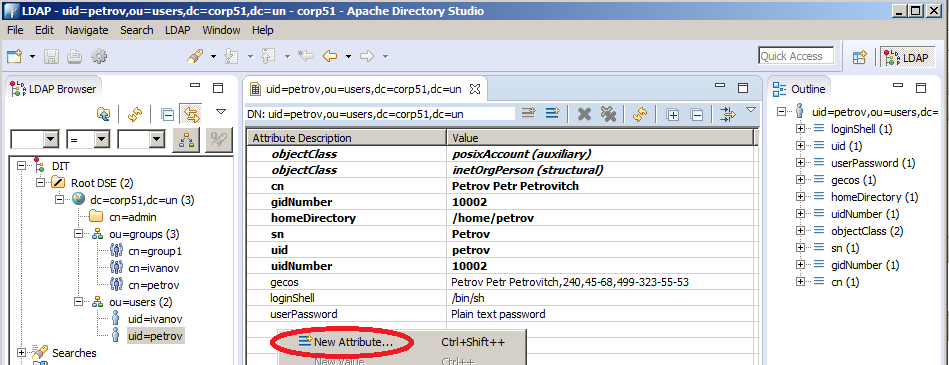
**Запустить ApacheDirectoryStudio.exe**

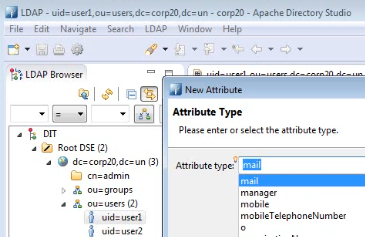
**LDAP -> New Connection:**

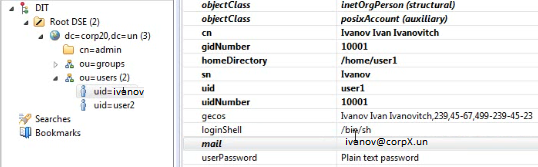
****

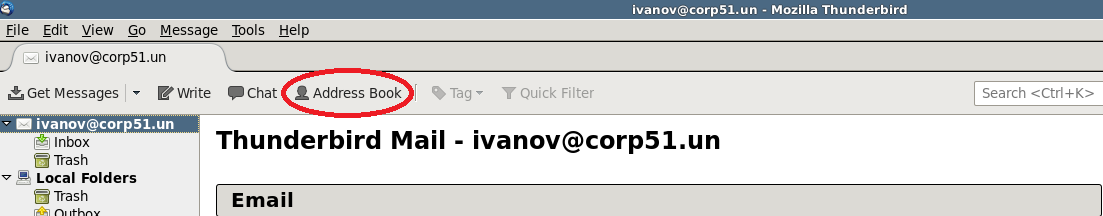
****

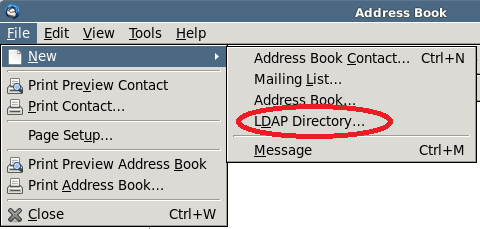
****

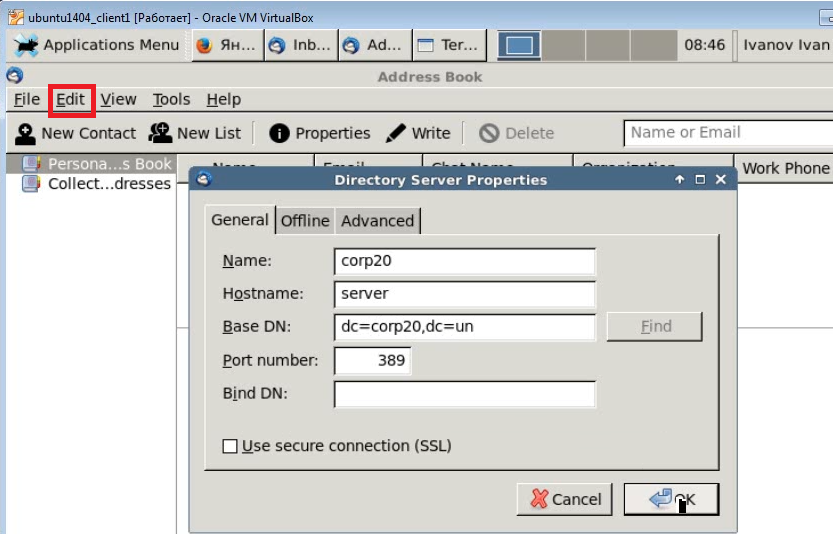
****

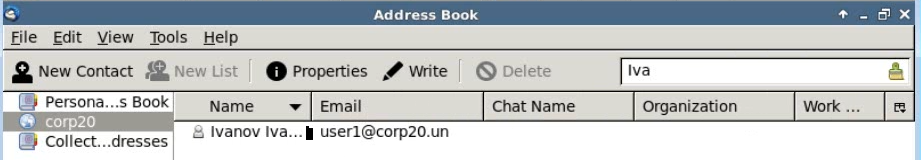
****

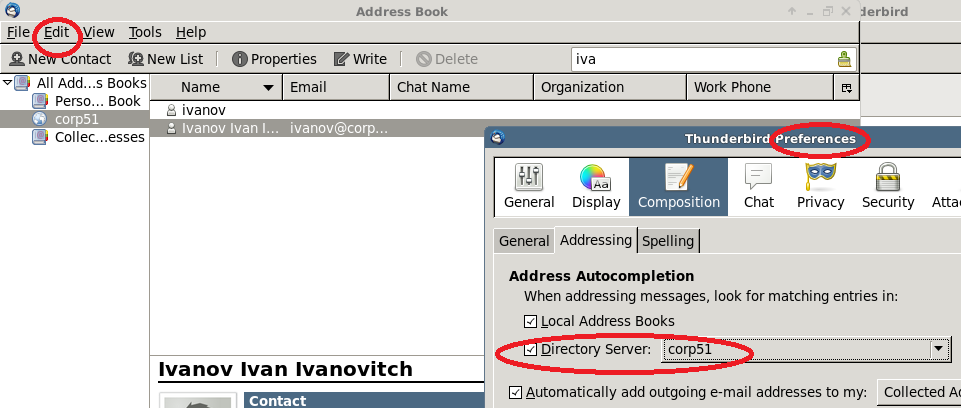
****

****

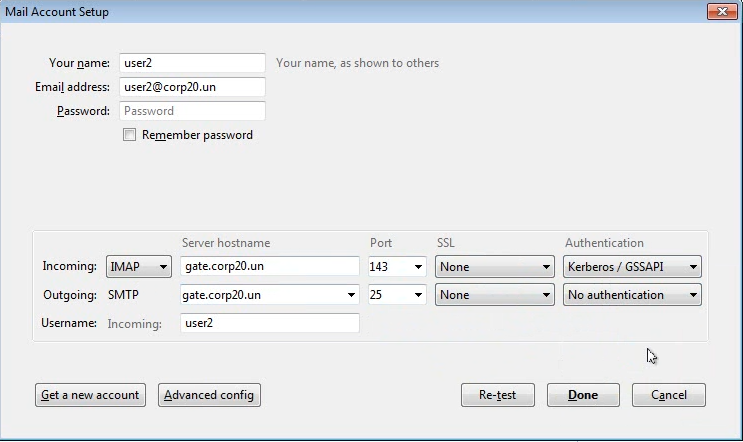
****

****

****

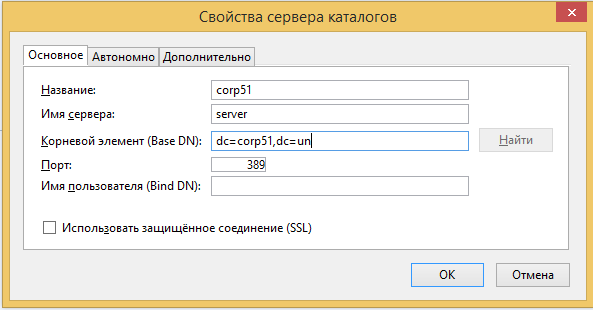
****

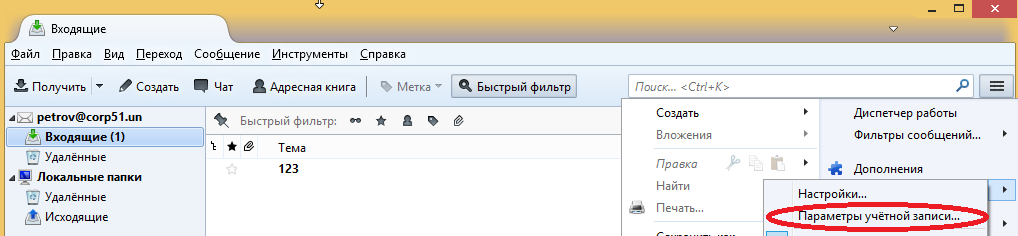
**Затем настроить почтовый клиент на Windows , как в предыдущей задаче.**

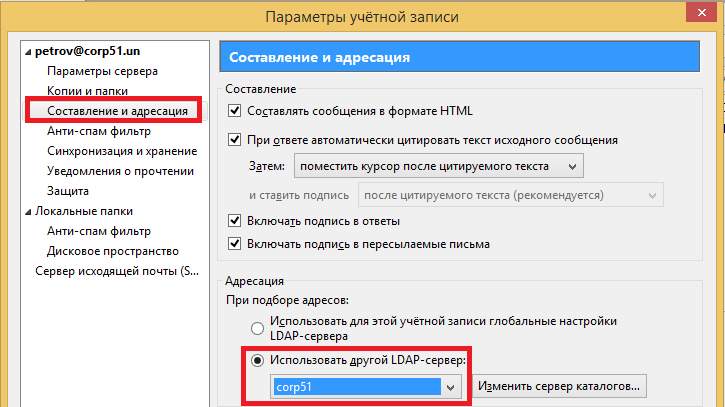
****

**Послать письмо от Ivanov с Client1**

**Настроить каталог:**

****

****

****