**lИспользование Microsoft AD для аутентификации и авторизации в гетерогенных сетях**

**Подготовка стенда**

Выключаем Client1

Отключаем использование ldap на Gate:

vim /etc/nsswitch.conf

passwd: compat

group: compat

Проверяем эффект: # id ivanov

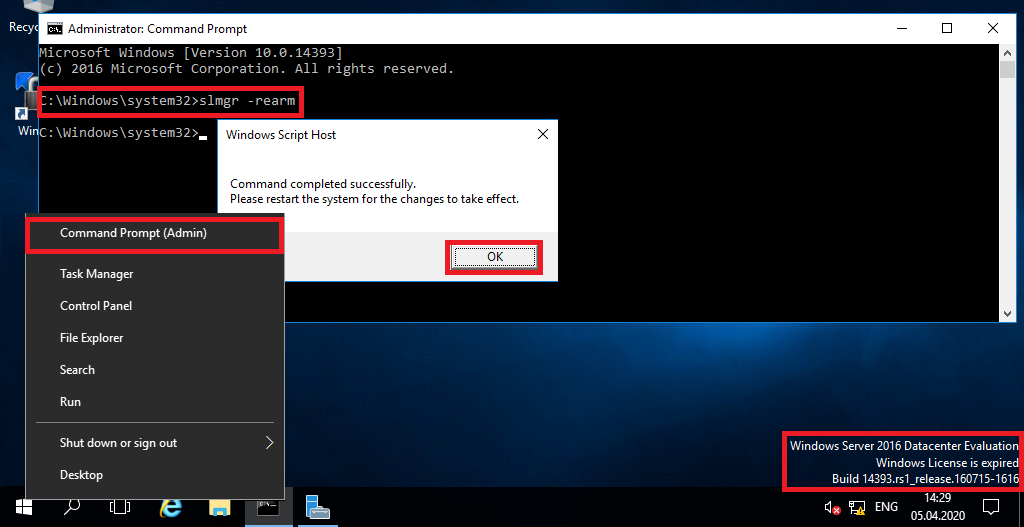
id: «ivanov»: такого пользователя нет

rm /etc/krb5.keytab

Выключаем Server

**Включаем VM Windows Server 2016 и настраиваем его в качестве контроллера домена.**

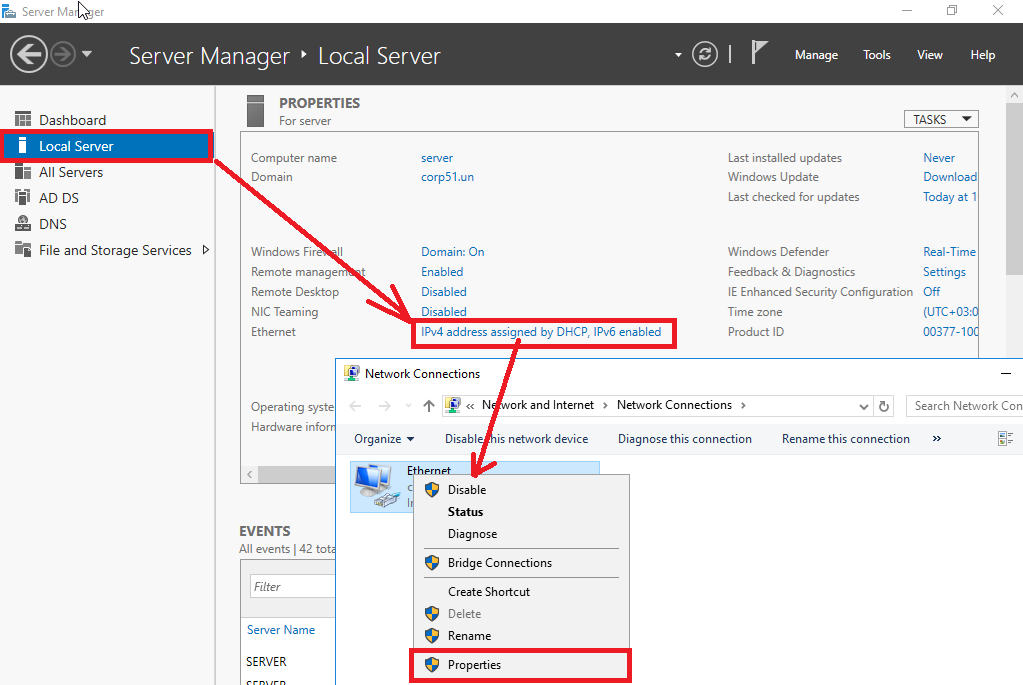
**Пароль для входа под администратором: Pa$$w0rd**

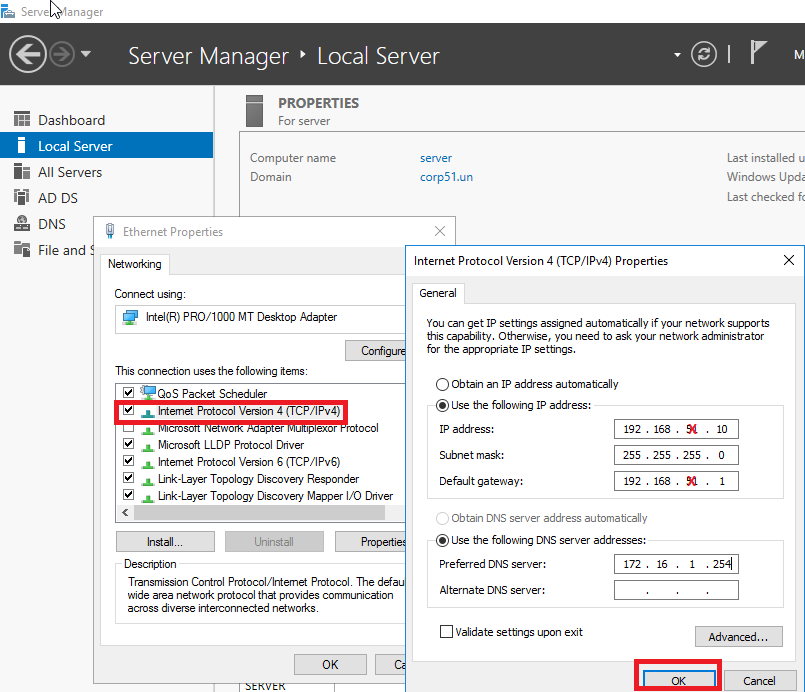


**После этого перезагрузить!**

**Настраиваем IP-адрес:**

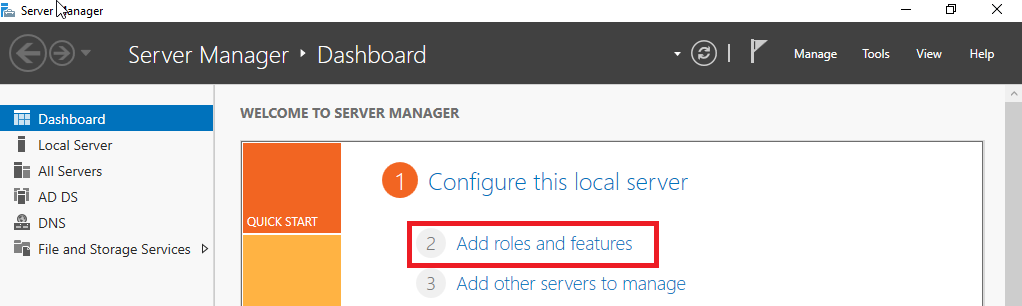
**В Server Manager:**

****

****

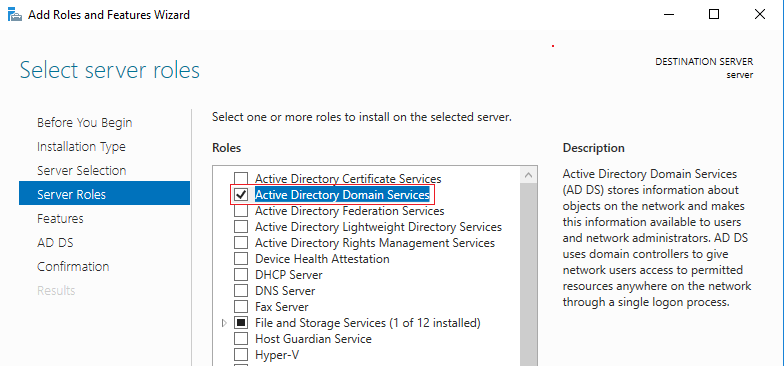
**Вместо X ставите номер своего стенда!**

**В Windows Server 2016 установить можно из графической консоли Server Manager с помощью мастера добавления ролей и компонентов.**

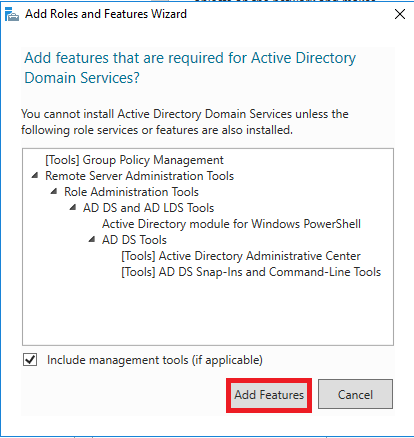
****

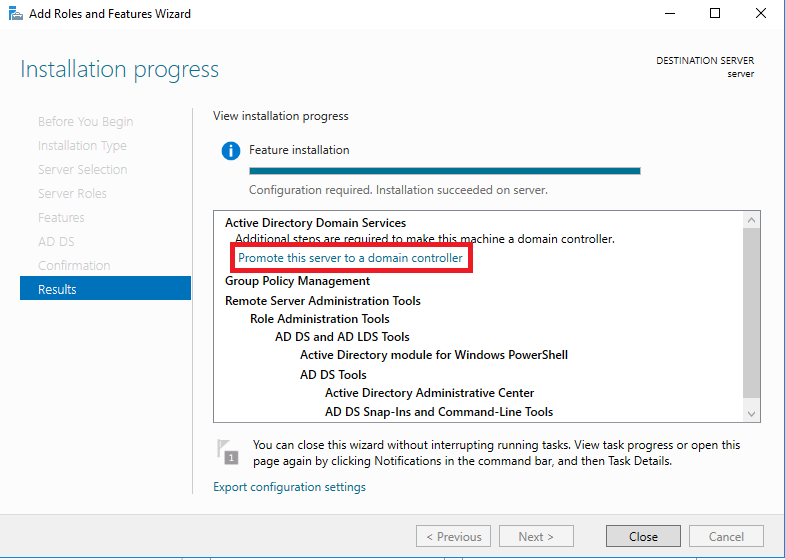
**Жмете Next (4 раза) до появления меню Features:**

**Где раскрываете узел Remote Server Administration Tools и ставите галку как показано на скриншоте:**

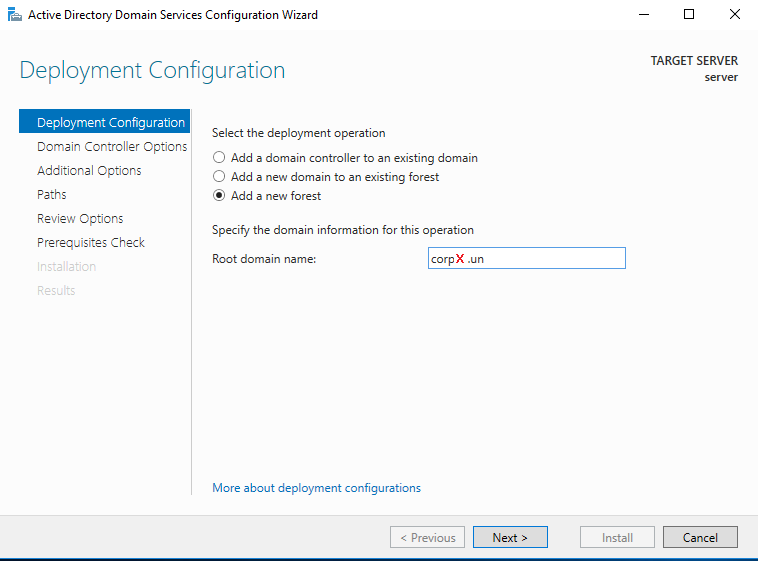


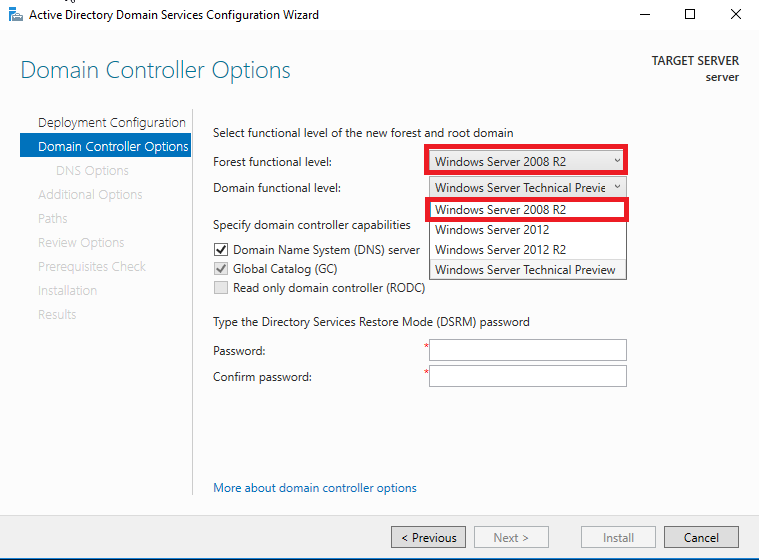
**В появившемся окне нажать Add Features:**

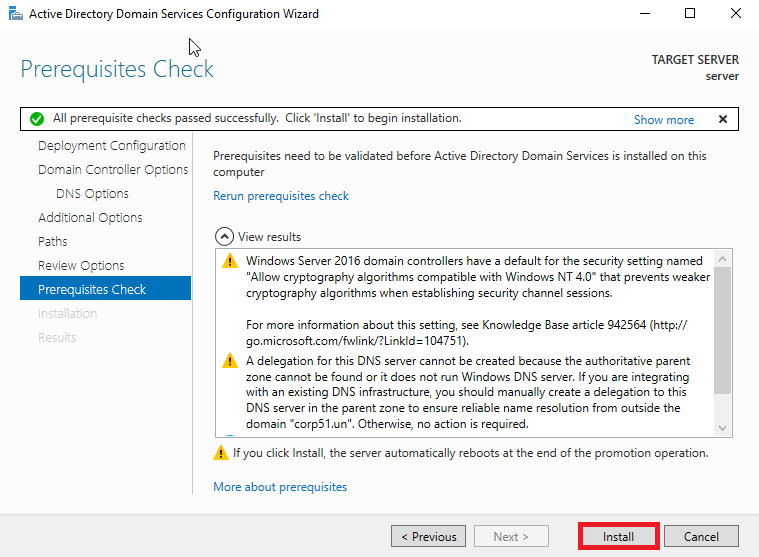




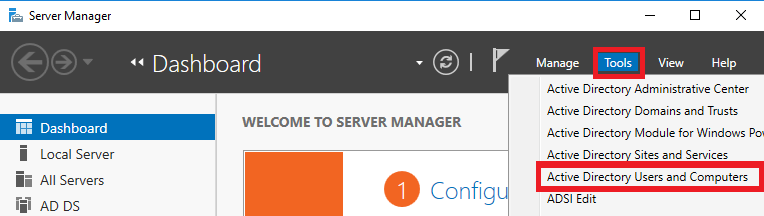
**Далее жмем Next, затем Install и после установки Close**

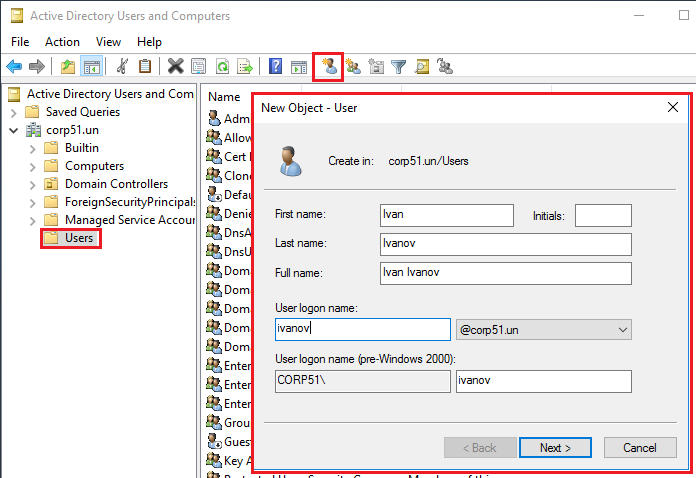


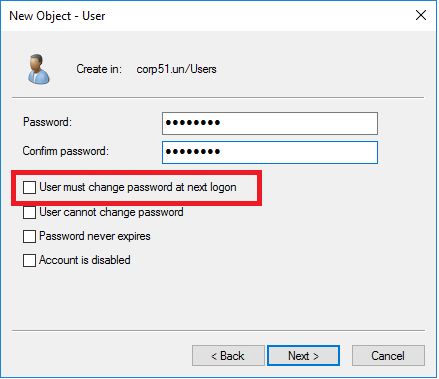




**Создаем доменных пользователей и группы:**



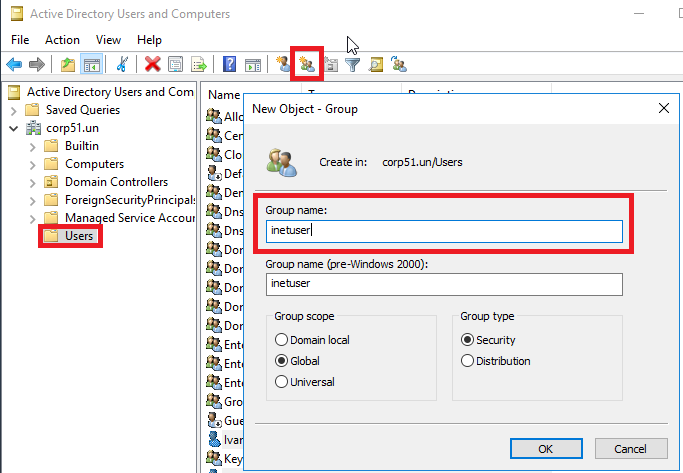




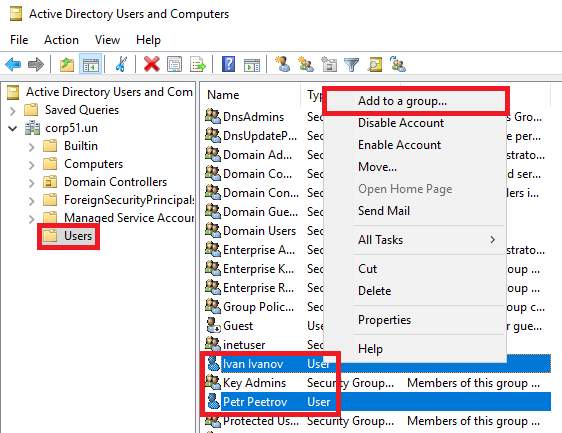
**Аналогично для petrov**

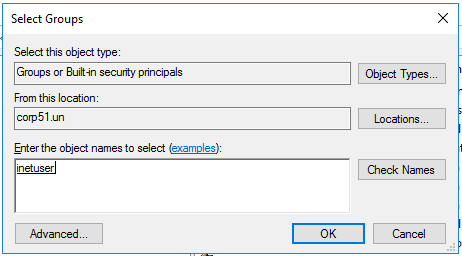
**Пароль везде задаем Pa$$w0rd**

**Создаем группу:**



**И добавим в нее пользователей:**





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

**Регистрация unix системы в домене в режиме ADS**

root@gate:~# apt install winbind libnss-winbind samba-dsdb-modules

root@gate:~# cat <<EOF > /etc/samba/smb.conf

[global]

workgroup = CORPX

security = ADS

realm = CORPX.UN

kerberos method = system keytab

winbind use default domain = yes

EOF

sed -i 's/X/номер\_стенда/' /etc/samba/smb.conf

**gate# net ads join -U Administrator**

linux# service winbind restart

gate# wbinfo -t

gate# wbinfo -u

gate# wbinfo -g

**Для отображения getent passwd доменных учетных записей:**

gate:~# cat > /etc/samba/smb.conf

[global]

workgroup = CORPX

security = ADS

realm = CORPX.UN

kerberos method = system keytab

winbind use default domain = Yes

winbind enum users = yes

winbind enum groups = yes

winbind cache time = 36

idmap config \* : range = 20000-40000

template homedir = /home/%U

template shell = /bin/bash

gate# service winbind restart

gate# cat /etc/nsswitch.conf

...

passwd: compat winbind

group: compat winbind

shadow: compat winbind

...

**reboot**

gate# wbinfo -n ivanov

gate# wbinfo -i ivanov

gate# id ivanov

gate# getent passwd

gate# getent group

gate# chown -R ivanov:'domain users' /home/ivanov/

gate# chown ivanov /var/mail/ivanov

gate# chown -R petrov:'domain users' /home/petrov/

gate# chown petrov /var/mail/petrov

**Управление ключами KERBEROS в режиме ADS**

**На системе** **gate**

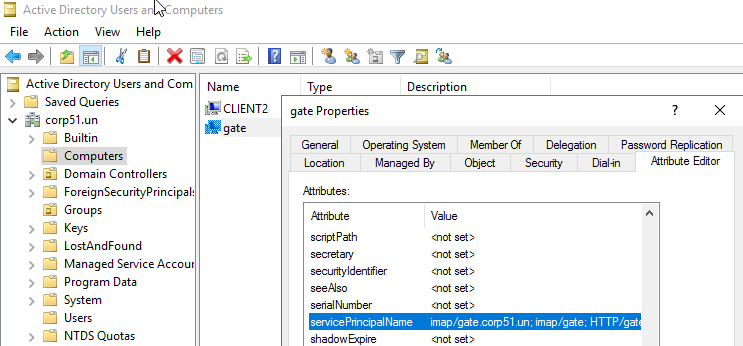
gate# net ads keytab add HTTP -U Administrator

gate# net ads keytab add imap -U Administrator

klist -ek /etc/krb5.keytab

# chmod +r /etc/krb5.keytab

gate:~# service squid restart



Выводим Windows клиента Client2 из Kerberos realm CORP51.UN

Запускаем от имени администратора Powershell:

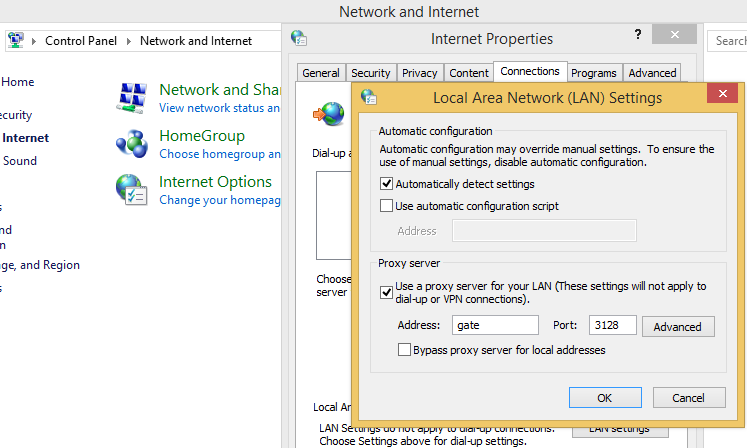
Add-Computer -WorkGroupName "WORKGROUP" –Restart

Добавляем в домен:

Add-Computer -DomainName "CORP51" -Credential CORP51\Administrator –Restart

Входим под petrov Pa$$w0rd

Настраиваем прокси на gate и порт 3128:



Проверяем: root@gate:~# tail -fn0 /var/log/squid/access.log

Файловый сервер

apt install samba

Создайте папку для организации общего доступа

mkdir /var/samba

Предоставьте доступ доменной группе

root@gate:~# setfacl -m g:'CORPX\domain users':rwx /var/samba

Настройте параметры общего доступа, добавив к файлу строки:

cat <<EOF >> /etc/samba/smb.conf

obey pam restrictions = yes

map acl inherit = yes

[homes]

read only = no

[share]

path = /var/samba

; valid users = CORPX\ivanov, CORPX\Administrator, CORPX\root

; valid users = "@CORPX\domain admins" games

valid users = "@CORPX\domain users"

; valid users = @group1 games

read only = no

EOF

sed -i 's/X/номер\_стенда/g' /etc/samba/smb.conf

**obey pam restrictions = yes** указывает Samba следовать директивам pam для учетных записей пользователей и сеансов. В данном случае — директиве на создание домашнего каталога.

**acl compatibility = yes** и **map acl inherit = yes** разрешают серверу Samba устанавливать режим совместимости списков доступа к файлам и наследование списков доступа. Актуально для поддержки Samba управления доступом от Windows-клиентов. Для корректной работы необходимо, чтобы файловая система, на которой размещен разделяемый ресурс Samba, поддерживала POSIX ACL

root@gate:~# reboot

**Настройка squid для авторизации на основе членства в доменной группе**

**Для взаимодействия squid с DC установить:**

apt-get install libsasl2-modules-gssapi-mit

Проверить, что членство в группе пользователя определяется:

root@gate:~# /usr/lib/squid/ext\_kerberos\_ldap\_group\_acl -i -g inetuser@CORP51.UN -D CORP51.UN

Создать зону обратного просмотра на Lon-dc1!!!

все контроллеры доменов должны быть в обратной DNS зоне!

Настроить списки контроля доступа и правило для доступа членам нужной группы:

vim /etc/squid/squid.conf

Параметры аутентификации не меняем:

# OPTIONS FOR AUTHENTICATION

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

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

Переходим поиском в секцию:

# ACCESS CONTROLS

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

Здесь добавляем строку:

external\_acl\_type inetuser ttl=300 negative\_ttl=60 %LOGIN /usr/lib/squid3/ext\_kerberos\_ldap\_group\_acl -a -g inetuser -D CORPX.UN

Далее в секции INSERT YOUR OWN RULE:

Заменим строку:

acl inetuser proxy\_auth REQUIRED

на стоку:

acl inetuser external inetuser

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

Имеющееся правило оставим без изменения:

http\_access allow inetuser

Проверяем корректность настроек: squid -k check

Перегружаем сервис: service squid restart

gate:~# tail -fn0 /var/log/squid/access.log

1537090133.844 70 192.168.51.10 TCP\_MISS/302 594 GET http://ya.ru/ Administrator@CORP51.UN HIER\_DIRECT/87.250.250.242 -

**Прим**.

При удалении пользователя из разрешенной для доступа группы - перезапустить сервис squid.

При добавлении пользователя в разрешенную для доступа группу перезапуск сервиса не требуется – результат вступает в силу немедленно.

Использование пакета Samba4 в качестве контроллера домена

**Подготовка стенда**

Выводим Windows клиент Client2 из домена AD

Запускаем от имени администратора Powershell:

Add-Computer -WorkGroupName "WORKGROUP" -Restart

Выводим gate из домена AD

Отключаем WINBIND в nsswitch.conf на gate

vim /etc/nsswitch.conf

Выводим gate из домена AD

gate# net ads leave -U Administrator

gate# rm /etc/krb5.keytab

* Останавливаем Windows AD
* Включаем server Linux

**Настраиваем DC SAMBA на Server**

Ставим SAMBA4, соотв. удаляем то что будет в пакете SAMBA4

**Перенастраиваем разрешение имен на внешний DNS (на 172.16.1.254), поскольку удалим имеющийся bind9** **с сервера:**

server# cat<<EOF > /etc/resolv.conf

nameserver 172.16.1.254

EOF

Удаляем имеющееся решение Kerberos/LDAP:

server# apt purge krb5-kdc krb5-admin-server bind9 slapd ldap-utils --auto-remove

Установка Samba4

# apt update && apt -y install samba krb5-config winbind smbclient krb5-user

Серверы Kerberos для вашей области: **server.corpX.un**

Управляющий сервер вашей области Kerberos: **server.corpX.un**

# rm /etc/samba/smb.conf

**Инициализация домена**

server# samba-tool domain provision --use-rfc2307 --interactive

**Принимаем настройки по умолчанию:**

**[Должна быть запись 192.168.X.10 server.corpX.un server в /etc/hosts]**

Realm [CORPX.UN]:

Domain [CORPX]:

Server Role (dc, member, standalone) [dc]:

DNS backend (SAMBA\_INTERNAL, BIND9\_FLATFILE, BIND9\_DLZ, NONE) [SAMBA\_INTERNAL]:

DNS forwarder IP address (write 'none' to disable forwarding) [172.16.1.254]:

**Задаем пароль администратора домена:**

Administrator password: Pa$$w0rd

Retype password: Pa$$w0rd

root@server:~# testparm

добавить в конец файла cat >> /etc/security/limits.conf следующие строки

\* - nofile 16384

root - nofile 16384

(максимальное количество одновременно открытых файлов)

ulimit -n

(максимальное количество одновременно открытых файлов)

ulimit -n 16384

systemctl stop smbd nmbd winbind

systemctl disable smbd nmbd winbind

systemctl mask smbd nmbd winbind

systemctl unmask samba-ad-dc

systemctl start samba-ad-dc

systemctl enable samba-ad-dc

**Возвращаем настройку разрешения имен на 127.0.0.1**:

cat > /etc/resolv.conf

nameserver 127.0.0.1

search corp51.un

cp /var/lib/samba/private/krb5.conf /etc/

cat >> /etc/krb5.conf

[realms]

CORP51.UN = {

kdc = server.corp51.un

admin\_server = server.corp51.un

}

smbclient -L localhost -U%

host -t SRV \_ldap.\_tcp.corp51.un

**Команды для администрирования - samba-tool**

samba-tool domain

samba-tool domain info 127.0.0.1

samba-tool dns

samba-tool dns zoneinfo 192.168.51.10 corp51.un -U Administrator

samba-tool user add petrov

samba-tool user create ivanov

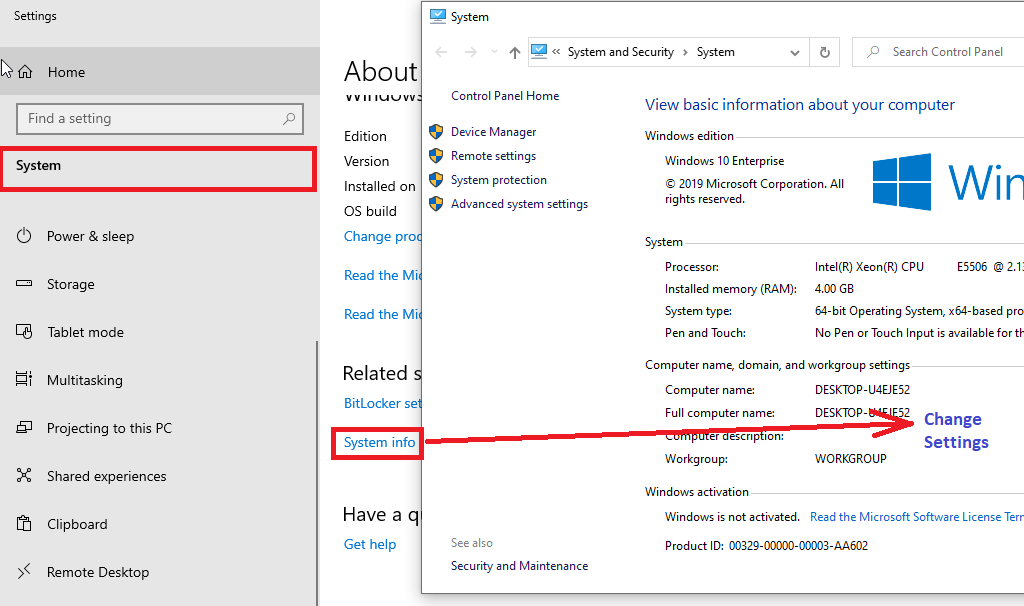
samba-tool user

Добавим в домен Windows client2

Добавляем в домен:

Add-Computer -DomainName "CORP51" -Credential CORP51\Administrator –Restart

Вводим пароль: Pa$$w0rd



**Использование SAMBA4 DC для аутентификации**

* **Тестируем kerberos на gate**

**gate# kinit Administrator**

**gate# kinit user2**

Регистрация системы **gate** в домене AD

gate# net ads join -U Administrator

gate# service winbind restart

Вернем параметр winbind в настройки /etc/nsswitch.conf:

vim /etc/nsswitch.conf

passwd: compat winbind

group: compat winbind

shadow: compat winbind

Развертывание средств администрирования Active Directory на client1

Включить и запустить службу Windows Update

Установить Windows8.1-KB2693643-x64.msu

Добавление контроллера домена SAMBA в качестве второго контроллера домена к существующему контроллеру Windows Server 2016

Добавление системы **gate** в качестве второго контроллера домена:

<https://www.server-world.info/en/note?os=Ubuntu_18.04&p=samba&f=7>

apt -y install samba krb5-config winbind smbclient

(Если с нуля, то: apt -y install samba krb5-config winbind smbclient krb5-user)

rm /etc/samba/smb.conf

samba-tool domain join corp51.un DC -U administrator --realm=corpX.un

host -t A gate.corpX.un

cat >> /etc/security/limits.conf

\* - nofile 16384

root - nofile 16384

reboot

ulimit -n

root@gate:~# reboot

systemctl stop systemd-resolved

systemctl disable systemd-resolved

ll /etc/resolv.conf

rm /etc/resolv.conf

cat > /etc/resolv.conf

nameserver 127.0.0.1

cat<<EOF > script.sh

systemctl stop smbd nmbd winbind

systemctl disable smbd nmbd winbind

systemctl unmask samba-ad-dc

systemctl start samba-ad-dc

systemctl enable samba-ad-dc

EOF

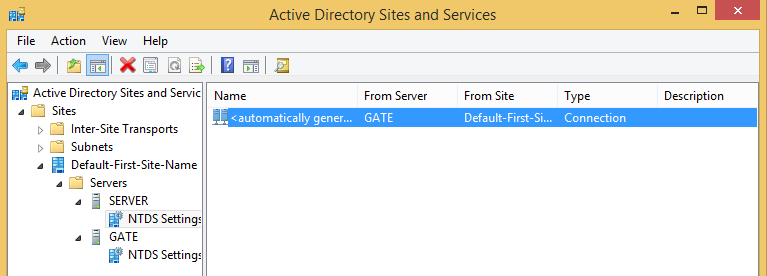
sh script.sh

smbclient //127.0.0.1/netlogon -U Administrator -c 'ls'

samba-tool drs showrepl

при регистрации нового DC самба неверно устанавливает некоторые флаги репликации. можно игнорировать это предупреждение.

samba-tool domain info 192.168.51.10

samba-tool domain info 192.168.51.1 

Demote the DC:

# samba-tool domain demote -U administrator

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

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

**Freeipa**

hostnamectl set-hostname server.corpX.un

cat > /etc/hosts

192.168.X.10 server.corpX.un server

apt -y install rng-tools

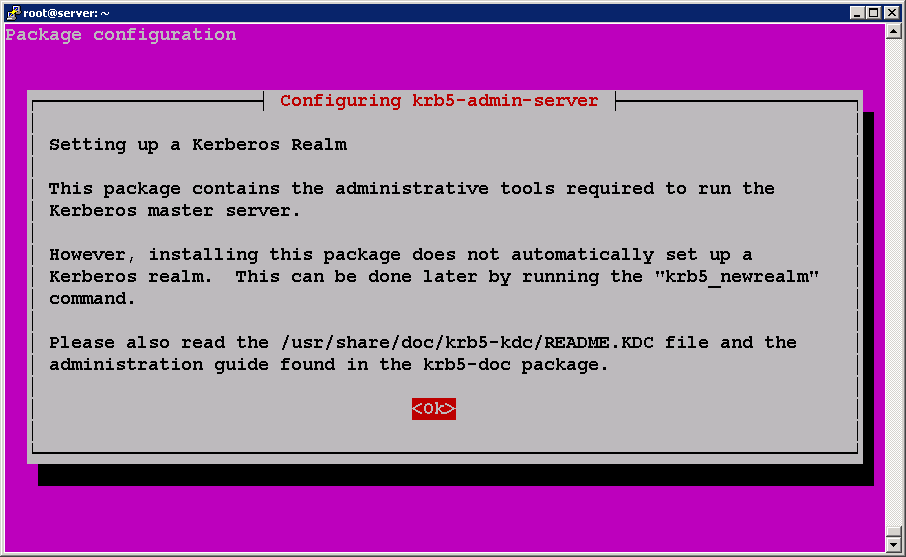
FreeIPA server выполняет множество криптографических операций во время работы, и поэтому ваша виртуальная машина должна иметь достаточную энтропию, чтобы гарантировать, что криптографические операции FreeIPA не остановятся. Для достижения высокой энтропии установите и настройте rng-tools.

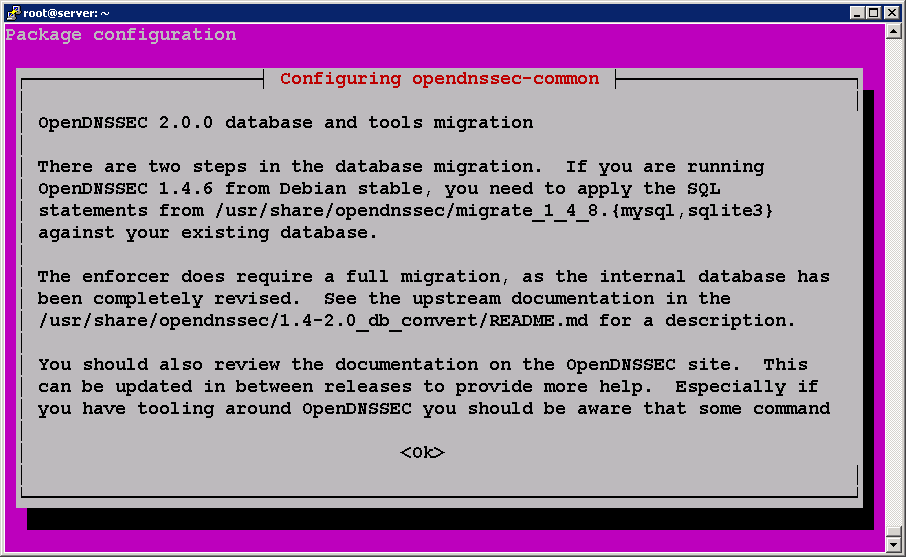
systemctl enable rng-tools && systemctl start rng-tools

apt -y install freeipa-server

OK

OK





На подобные ошибки не обращаем внимание, поскольку еще не настроено:

Failed to start LSB: Start pki-tomcatd at boot time.

pki-tomcatd start failed because no instance has been configured yet

krb5\_newrealm

Пароль: secret

ipa-server-install

Do you want to configure integrated DNS (BIND)? [no]:

Server host name [server.corp51.un]:

Please confirm the domain name [corp51.un]:

Please provide a realm name [CORP51.UN]:

Directory Manager password:

IPA admin password:

Continue to configure the system with these values? [no]: **yes**