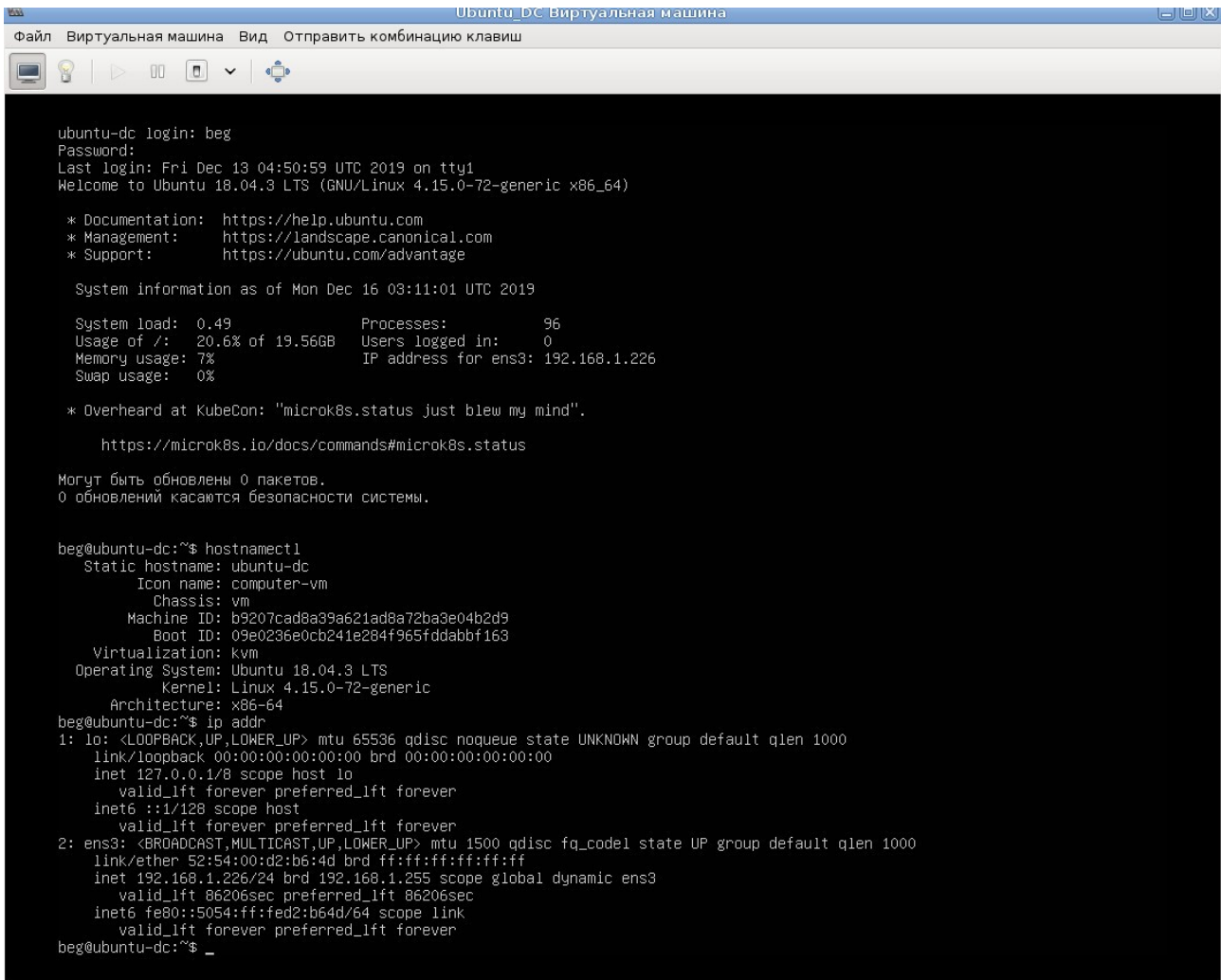


## Контроллер домена AD на Ubuntu Linux 18.04 LTS

Устанавливаем Ubuntu Linux серверную версию без графического интерфейса. При установке сразу задаем имя системы (в дальнейшем оно должно остаться неизменным!) и статический IP-адрес (на самом деле, можно использовать и динамический, при условии, что он будет неизменным на протяжении всей работы). Не забываем после инсталляции системы и начального конфигурирования выполнить установку последних обновлений системы. Начальное состояние системы показано на скриншоте ниже.



```
ubuntu-dc login: beg
Password:
Last login: Fri Dec 13 04:50:59 UTC 2019 on tty1
Welcome to Ubuntu 18.04.3 LTS (GNU/Linux 4.15.0-72-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

System information as of Mon Dec 16 03:11:01 UTC 2019

System load:  0.49           Processes:    96
Usage of /:   20.6% of 19.56GB Users logged in: 0
Memory usage: 7%           IP address for ens3: 192.168.1.226
Swap usage:  0%

 * Overheard at KubeCon: "microk8s.status just blew my mind".
    https://microk8s.io/docs/commands#microk8s.status

Могут быть обновлены 0 пакетов.
0 обновлений касаются безопасности системы.

beg@ubuntu-dc:~$ hostnamectl
  Static hostname: ubuntu-dc
        Icon name: computer-vm
        Chassis: vm
        Machine ID: b9207cad8a39a621ad8a72ba3e04b2d9
        Boot ID: 09e0236e0cb241e284f965fddabbf163
        Virtualization: kvm
        Operating System: Ubuntu 18.04.3 LTS
        Kernel: Linux 4.15.0-72-generic
        Architecture: x86-64
beg@ubuntu-dc:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: ens3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 52:54:00:d2:b6:4d brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.226/24 brd 192.168.1.255 scope global dynamic ens3
        valid_lft 86206sec preferred_lft 86206sec
    inet6 fe80::5054:ff:fed2:b64d/64 scope link
        valid_lft forever preferred_lft forever
beg@ubuntu-dc:~$ _
```

Далее, отключаем systemd-resolved с помощью следующей последовательности команд:

```
sudo service systemd-resolved stop
sudo systemctl disable systemd-resolved.service
sudo rm /etc/resolv.conf
sudo nano /etc/resolv.conf
```

создаем новый следующего содержания:)

**nameserver 192.168.1.1**

**search homenet.homenet**

домена требует имя в домене второго уровня, поэтому просто homenet, например, указать нельзя, поскольку в этом случае при дальнейшем конфигурировании возникнут ошибки).

Далее, приводим файл **hosts** к следующему виду:

- останавливаем сервис systemd-resolved
- запрещаем автозапуск сервиса
- удаляем старый файл resolv.conf
- редактируем /etc/resolv.conf (фактически,
- адрес DNS-сервера для всей локальной сети
- имя будущего домена AD(контроллер

```

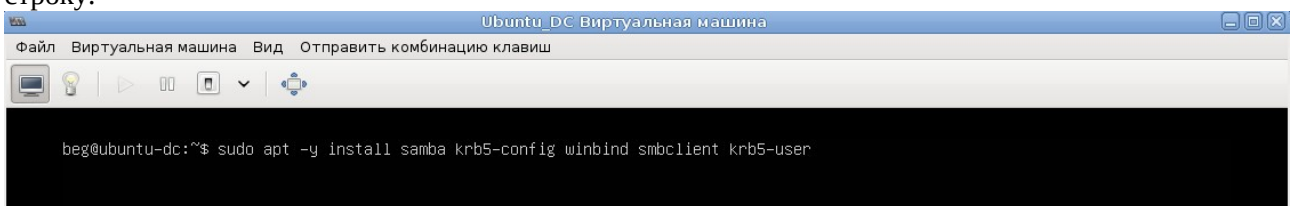
127.0.0.1 localhost
192.168.1.226 ubuntu-dc.homenet.homenet ubuntu-dc

# The following lines are desirable for IPv6 capable hosts
::1          ip6-localhost ip6-loopback
fe00::0      ip6-localnet
ff00::0      ip6-mcastprefix
ff02::1      ip6-allnodes
ff02::2      ip6-allrouters

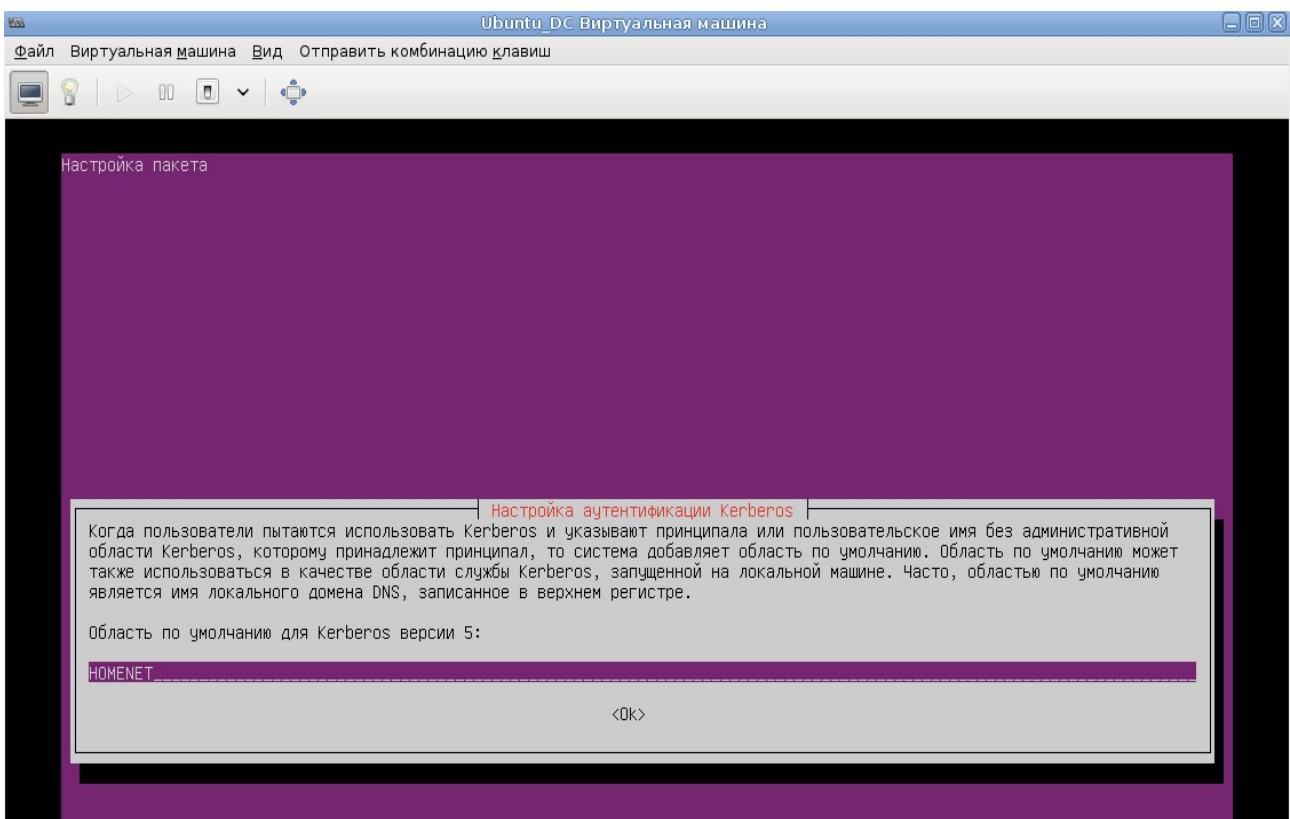
```

т. е. Вписываем в него полное и сокращенное имя нашего сервера, чтобы оно не резолвилось на loopback (127.0.0.1) .

Приступаем к установке необходимых пакетов, для чего выдаем следующую командную строку:

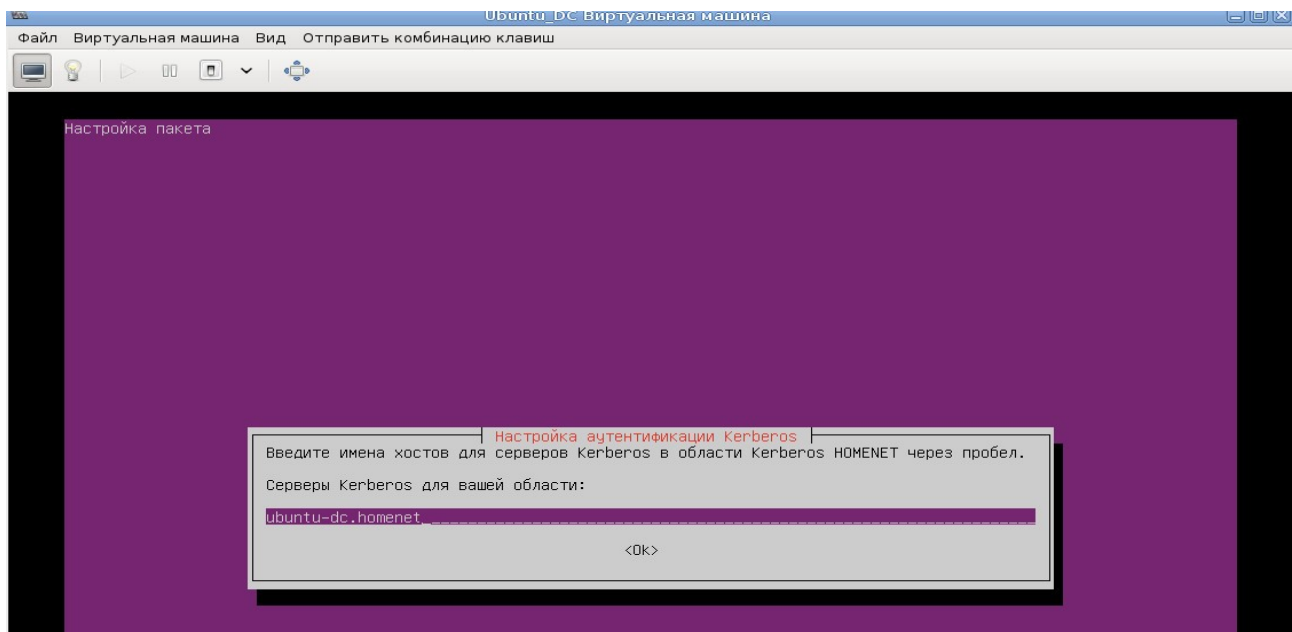


Определяем область по умолчанию для Kerberos

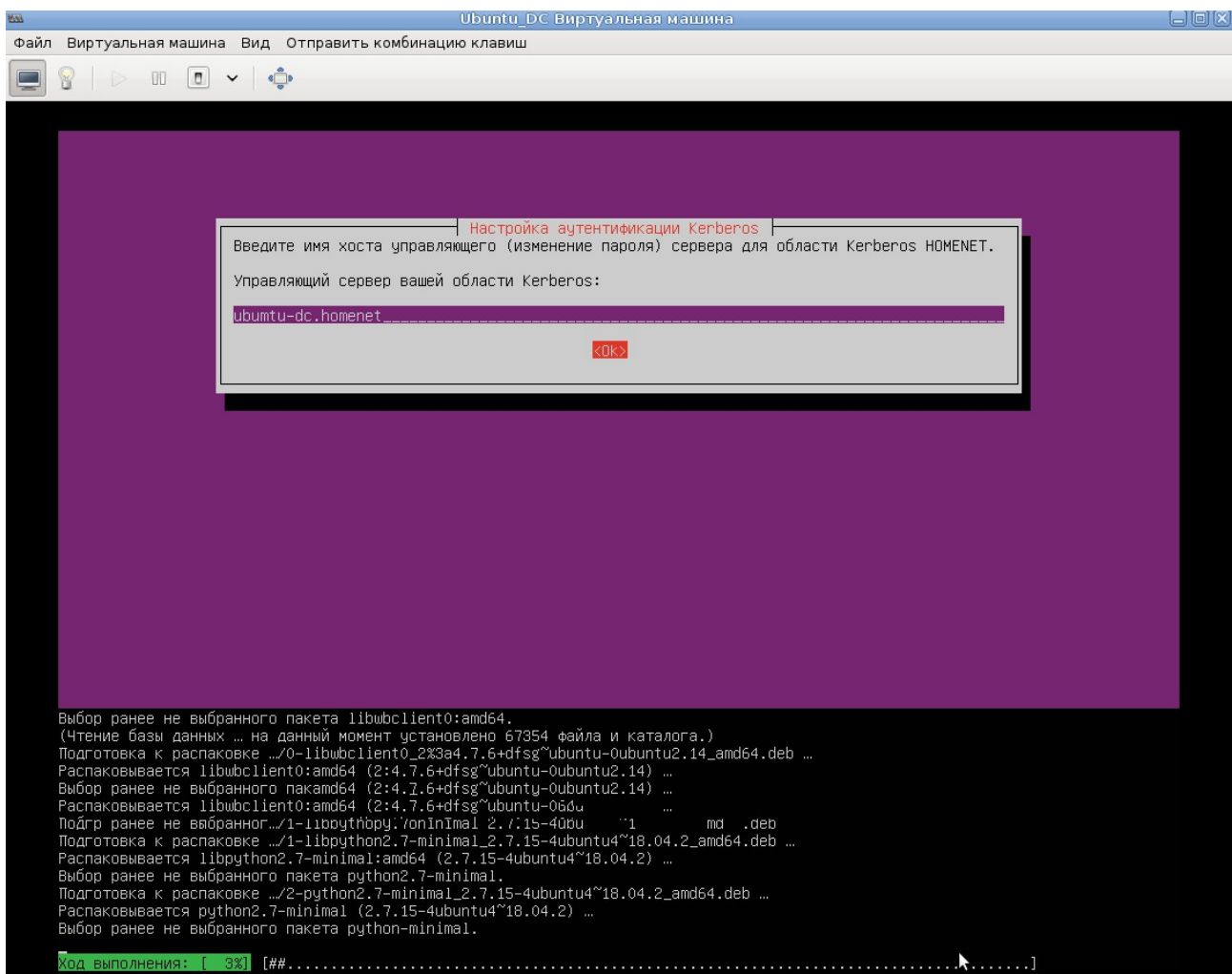


В данном случае надо было ввести **homenet.homenet**, тогда бы не пришлось далее править REALM при конфигурировании DC.

Устанавливаем серверы Kerberos для нашей области:



Управляющий сервер для области:

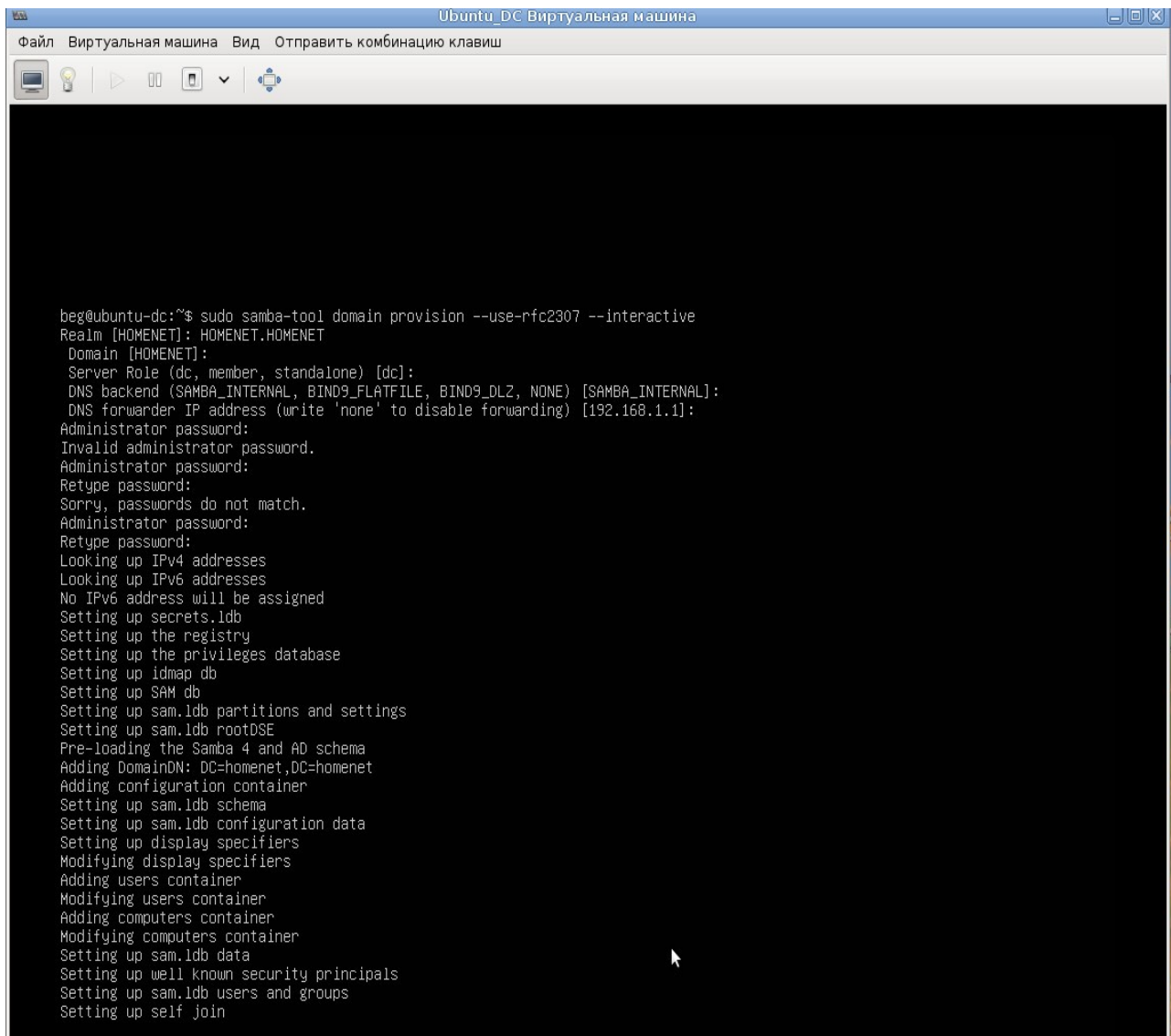


После конфигурирования Kerberos запускается процесс инсталляции пакетов.

После завершения инсталляции делаем backup стандартной конфигурации samba, поскольку после инициализации DC будет сгенерирован новый файл:

```
sudo mv /etc/samba/smb.conf /etc/samba/smb.conf.old
```

Далее, иницилируем контроллер домена в интерактивном режиме:



```
beg@ubuntu-dc:~$ sudo samba-tool domain provision --use-rfc2307 --interactive
Realm [HOMENET]: HOMENET.HOMENET
Domain [HOMENET]:
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) [192.168.1.1]:
Administrator password:
Invalid administrator password.
Administrator password:
Retype password:
Sorry, passwords do not match.
Administrator password:
Retype password:
Looking up IPv4 addresses
Looking up IPv6 addresses
No IPv6 address will be assigned
Setting up secrets.ldb
Setting up the registry
Setting up the privileges database
Setting up idmap db
Setting up SAM db
Setting up sam.ldb partitions and settings
Setting up sam.ldb rootDSE
Pre-loading the Samba 4 and AD schema
Adding DomainDN: DC=homenet,DC=homenet
Adding configuration container
Setting up sam.ldb schema
Setting up sam.ldb configuration data
Setting up display specifiers
Modifying display specifiers
Adding users container
Modifying users container
Adding computers container
Modifying computers container
Setting up sam.ldb data
Setting up well known security principals
Setting up sam.ldb users and groups
Setting up self join
```

Указываем (при необходимости) Realm, Domain, Server Role, DNS backend, DNS forwarder, пароль администратора. Если ранее все было задано верно, то, как правило, выбираются значения по умолчанию (просто на каждую строку нажимаем enter, кроме password). В данном случае был введен только REALM (см. Замечание выше).

В дальнейшем выводе процедуры инициализации не должно быть никаких сообщений о предупреждениях и ошибках:

```
Administrator password:
Invalid administrator password.
Administrator password:
Retype password:
Sorry, passwords do not match.
Administrator password:
Retype password:
Looking up IPv4 addresses
Looking up IPv6 addresses
No IPv6 address will be assigned
Setting up secrets.ldb
Setting up the registry
Setting up the privileges database
Setting up idmap db
Setting up SAM db
Setting up sam.ldb partitions and settings
Setting up sam.ldb rootDSE
Pre-loading the Samba 4 and AD schema
Adding DomainDN: DC=homenet,DC=homenet
Adding configuration container
Setting up sam.ldb schema
Setting up sam.ldb configuration data
Setting up display specifiers
Modifying display specifiers
Adding users container
Modifying users container
Adding computers container
Modifying computers container
Setting up sam.ldb data
Setting up well known security principals
Setting up sam.ldb users and groups
Setting up self join
Adding DNS accounts
Creating CN=MicrosoftDNS,CN=System,DC=homenet,DC=homenet
Creating DomainDnsZones and ForestDnsZones partitions
Populating DomainDnsZones and ForestDnsZones partitions
Setting up sam.ldb rootDSE marking as synchronized
Fixing provision GUIDs
A Kerberos configuration suitable for Samba AD has been generated at /var/lib/samba/private/krb5.conf
Setting up fake up server settings
Once the above files are installed, your Samba AD server will be ready to use
Server Role:      active directory domain controller
Hostname:         ubuntu-dc
NetBIOS Domain:   HOMENET
DNS Domain:       homenet.homenet
DOMAIN SID:       S-1-5-21-1318501845-3895617199-2911350377

beg@ubuntu-dc:~$
```

Далее, копируем созданный в результате инициализации файл конфигурации Kerberos в /etc (можно создать символическую ссылку):

```
beg@ubuntu-dc:~$ sudo cp /var/lib/samba/private/krb5.conf /etc/
beg@ubuntu-dc:~$ _
```

Далее, конфигурируем запрет отдельных сервисом и запуск нужных:

***sudo systemctl stop smbd nmbd winbind***

***sudo systemctl disable smbd nmbd winbind***

***sudo systemctl mask smbd nmbd winbind***

эти сервисы при старте samba-ad-dc запускаются автоматически, и необходимости в их отдельном запуске нет. Поэтому мы их запрещаем, но разрешаем автоматический запуск AD-DC:

```
beg@ubuntu-dc:~$ sudo systemctl unmask samba-ad-dc
Removed /etc/systemd/system/samba-ad-dc.service.
beg@ubuntu-dc:~$ sudo systemctl start samba-ad-dc
beg@ubuntu-dc:~$ sudo systemctl enable samba-ad-dc
Synchronizing state of samba-ad-dc.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable samba-ad-dc
beg@ubuntu-dc:~$ _
```

Изменяем настройки DNS-сервера(вместе с samba4 ставится DNS и в него должны прописываться SRV- и A- записи). Теперь в resolv.conf в директиве nameserver указываем адрес нашего AD DC, в данном случае **nameserver 192.168.1.226**

Проверяем, что получилось:

смотрим стандартные разделяемые ресурсы, создаваемые при конфигурировании DC:

```
beg@ubuntu-dc:~$ smbclient -L localhost -U%

      Sharename      Type      Comment
      -----
      netlogon       Disk
      sysvol         Disk
      IPC$           IPC       IPC Service (Samba 4.7.6-Ubuntu)
Reconnecting with SMB1 for workgroup listing.

      Server          Comment
      -----
      Workgroup       Master
      -----
      WORKGROUP       NETSTOR-IX2-200
beg@ubuntu-dc:~$ smbclient //localhost/netlogon -UAdministrator -c 'ls'
Enter HOMENET\Administrator's password:
.
..
D          0   Mon Dec 16 03:41:25 2019
D          0   Mon Dec 16 03:44:17 2019

20508240 blocks of size 1024. 15044216 blocks available
beg@ubuntu-dc:~$ _
```

Подключаемся администратором:

```
beg@ubuntu-dc:~$ smbclient //localhost/netlogon -UAdministrator -c 'ls'
Enter HOMENET\Administrator's password:
.
..
D          0   Mon Dec 16 03:41:25 2019
D          0   Mon Dec 16 03:44:17 2019

20508240 blocks of size 1024. 15044216 blocks available
beg@ubuntu-dc:~$ _
```

Получилось !Проверяем разрешение имен и записи DNS:

адрес -> имя:

```
beg@ubuntu-dc:~$ nslookup 192.168.1.226
226.1.168.192.in-addr.arpa    name = ubuntu-dc.
```

имя → адрес:

```
beg@ubuntu-dc:~$ nslookup ubuntu-dc.homenet.homenet
Server:      192.168.1.226
Address:     192.168.1.226#53

Name:   ubuntu-dc.homenet.homenet
Address: 192.168.1.226
```

SRV записи и работоспособность Kerberos (kinit administrator и klist)

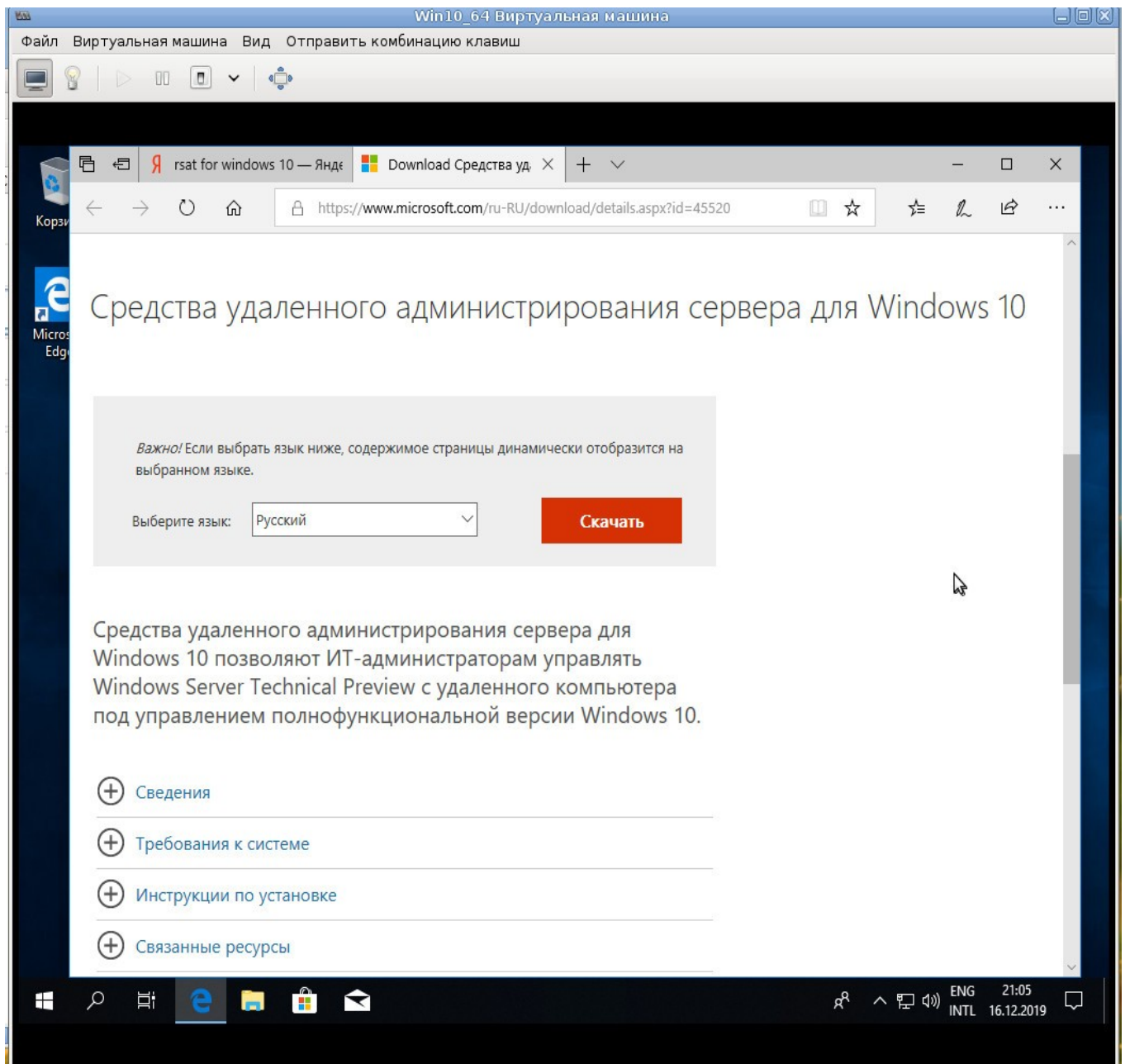
```
beg@ubuntu-dc:~$ host -t SRV _ldap._tcp.homenet.homenet.
_ldap._tcp.homenet.homenet has SRV record 0 100 389 ubuntu-dc.homenet.homenet.
beg@ubuntu-dc:~$ host -t SRV _kerberos._udp.homenet.homenet
_kerberos._udp.homenet.homenet has SRV record 0 100 88 ubuntu-dc.homenet.homenet.
beg@ubuntu-dc:~$ host -t A ubuntu-dc.homenet.homenet
ubuntu-dc.homenet.homenet has address 192.168.1.226
beg@ubuntu-dc:~$ kinit administrator
Password for administrator@HOMENET.HOMENET:
Warning: Your password will expire in 41 days on Пн 27 янв 2020 03:44:17
beg@ubuntu-dc:~$ klist
Ticket cache: FILE:/tmp/krb5cc_1000
Default principal: administrator@HOMENET.HOMENET

Valid starting    Expires          Service principal
16.12.2019 13:47:45 16.12.2019 23:47:45 krbtgt/HOMENET.HOMENET@HOMENET.HOMENET
renew until 17.12.2019 13:47:36
beg@ubuntu-dc:~$ _
```

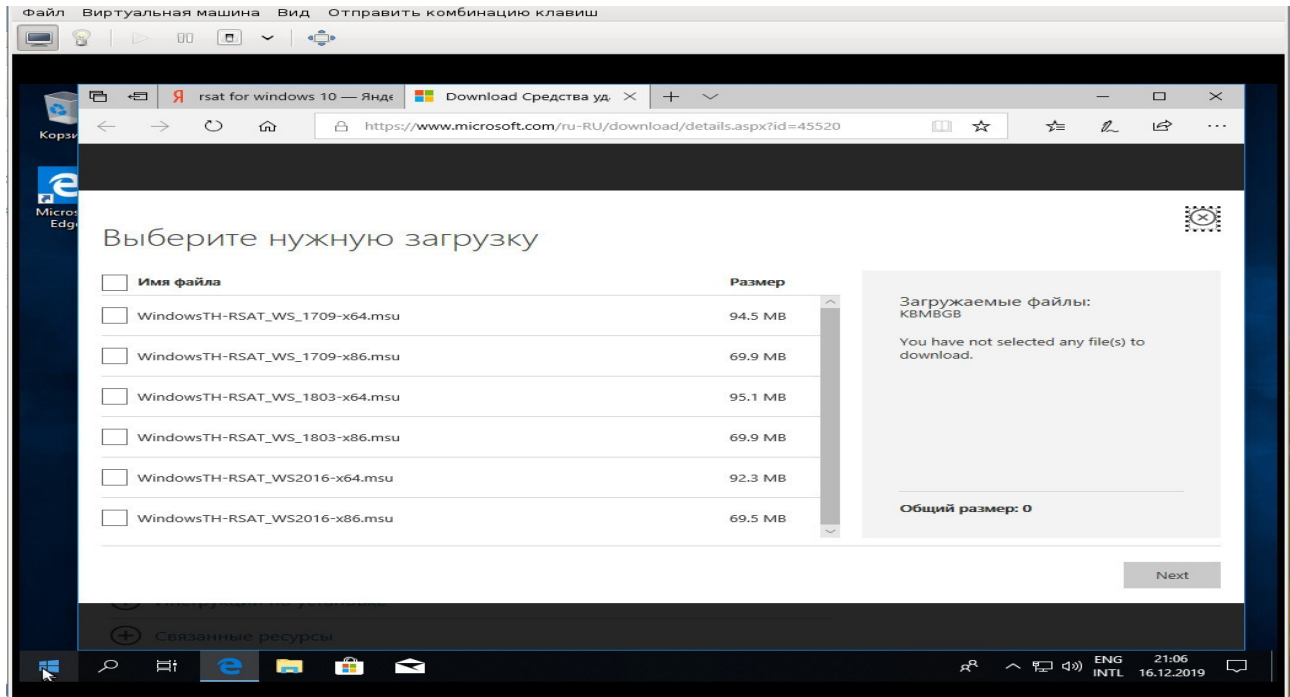
Контроллер домена работает.Переходим к рабочей станции Windows:



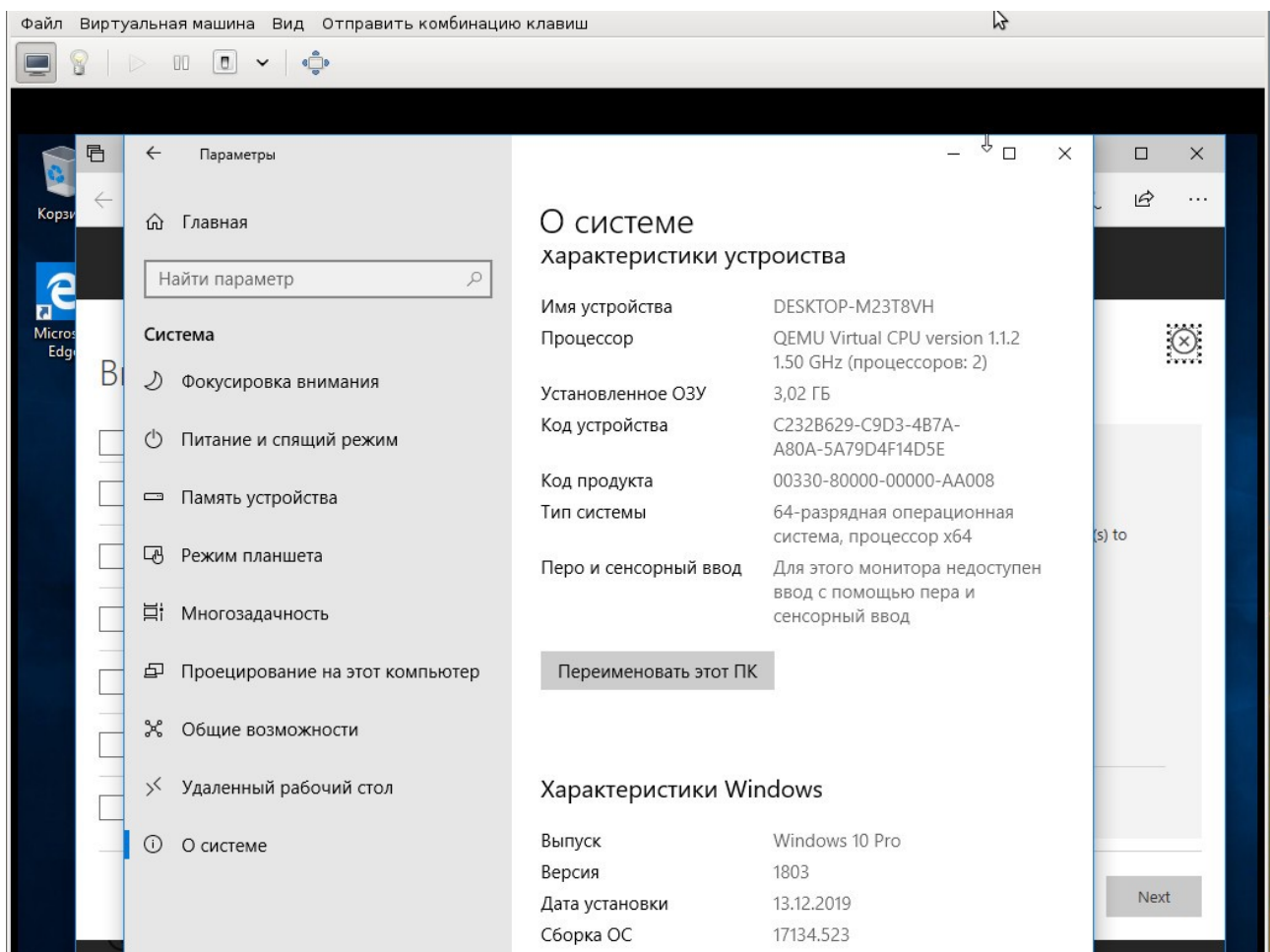
Загружаем с сайта Microsoft RSAT — набор инструментов удаленного администрирования серверов:



Прошу обратить внимание, что RSAT различается для различных версий и выпусков Windows:

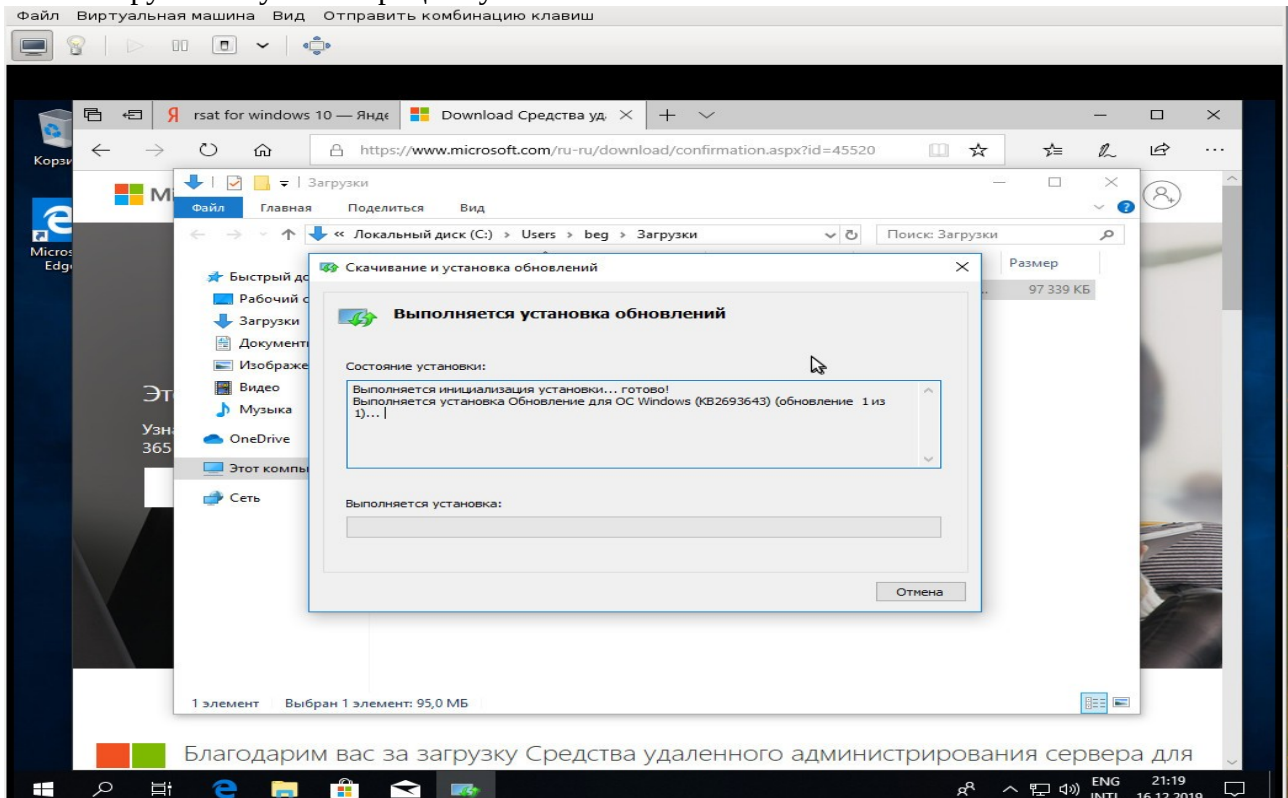


Поэтому проверьте свою версию и выпуск:

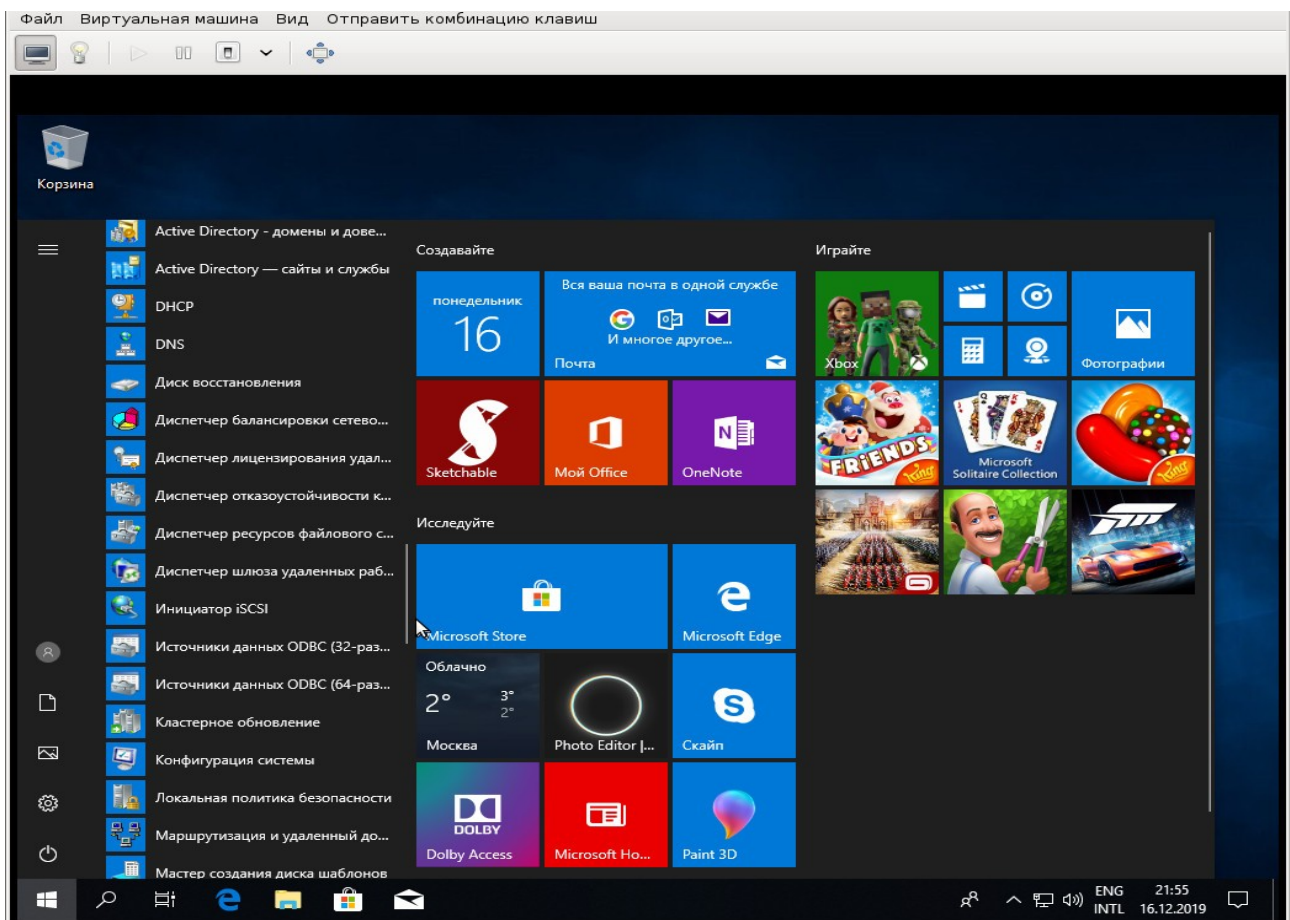




после загрузки запускаем процесс установки автономного обновления:

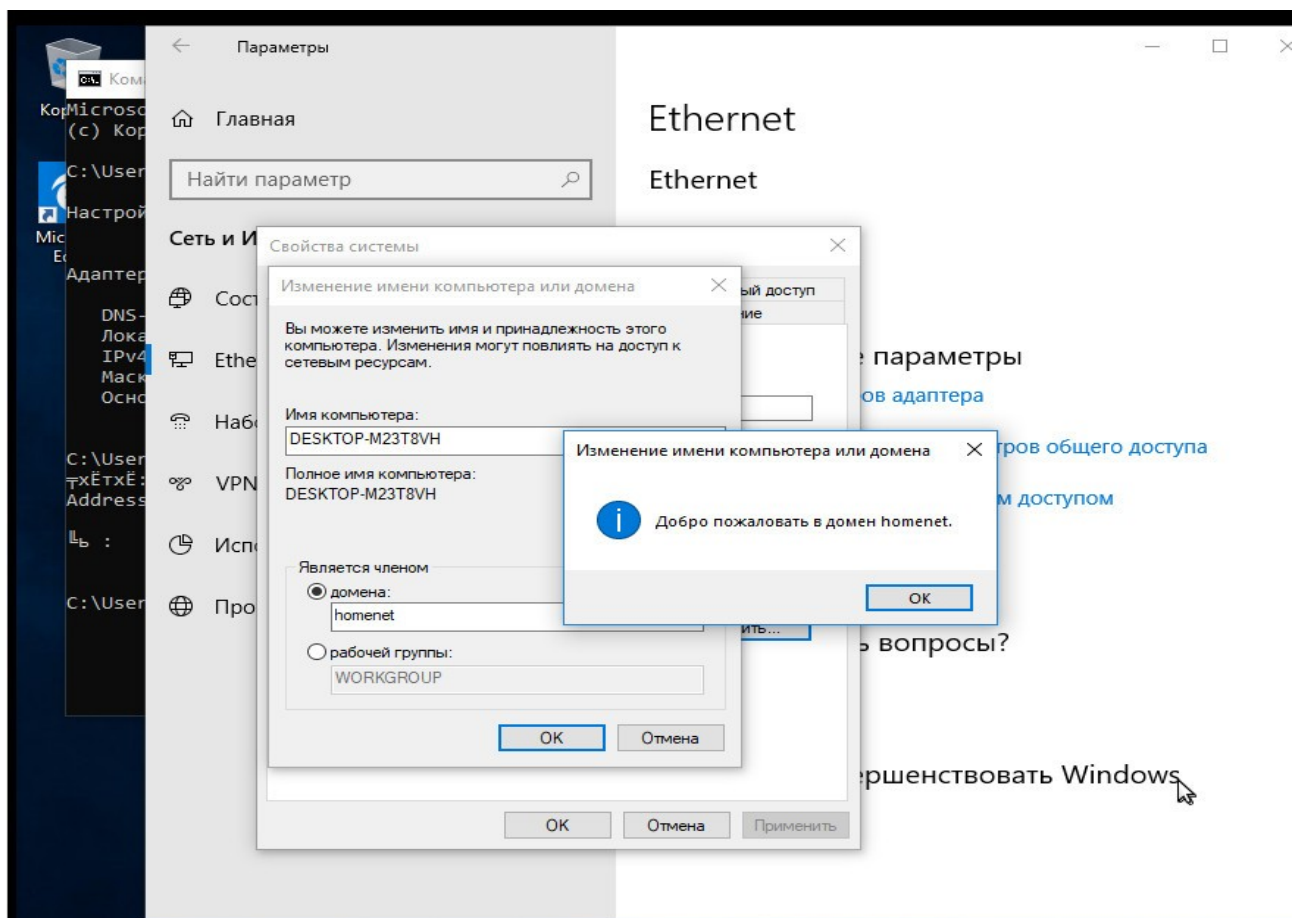
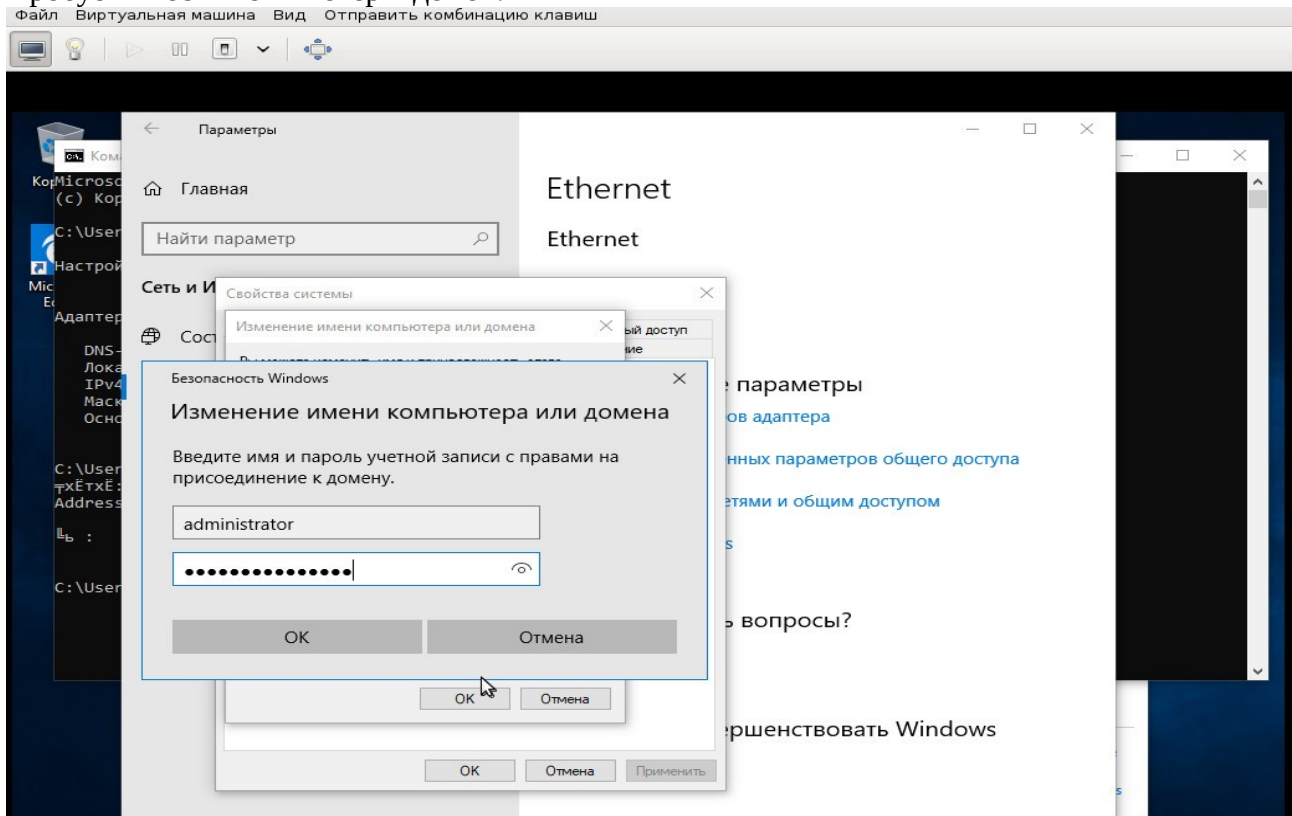


После установки обновления и перезагрузки во вкладке Администрирование получаем дополнительный набор инструментов:

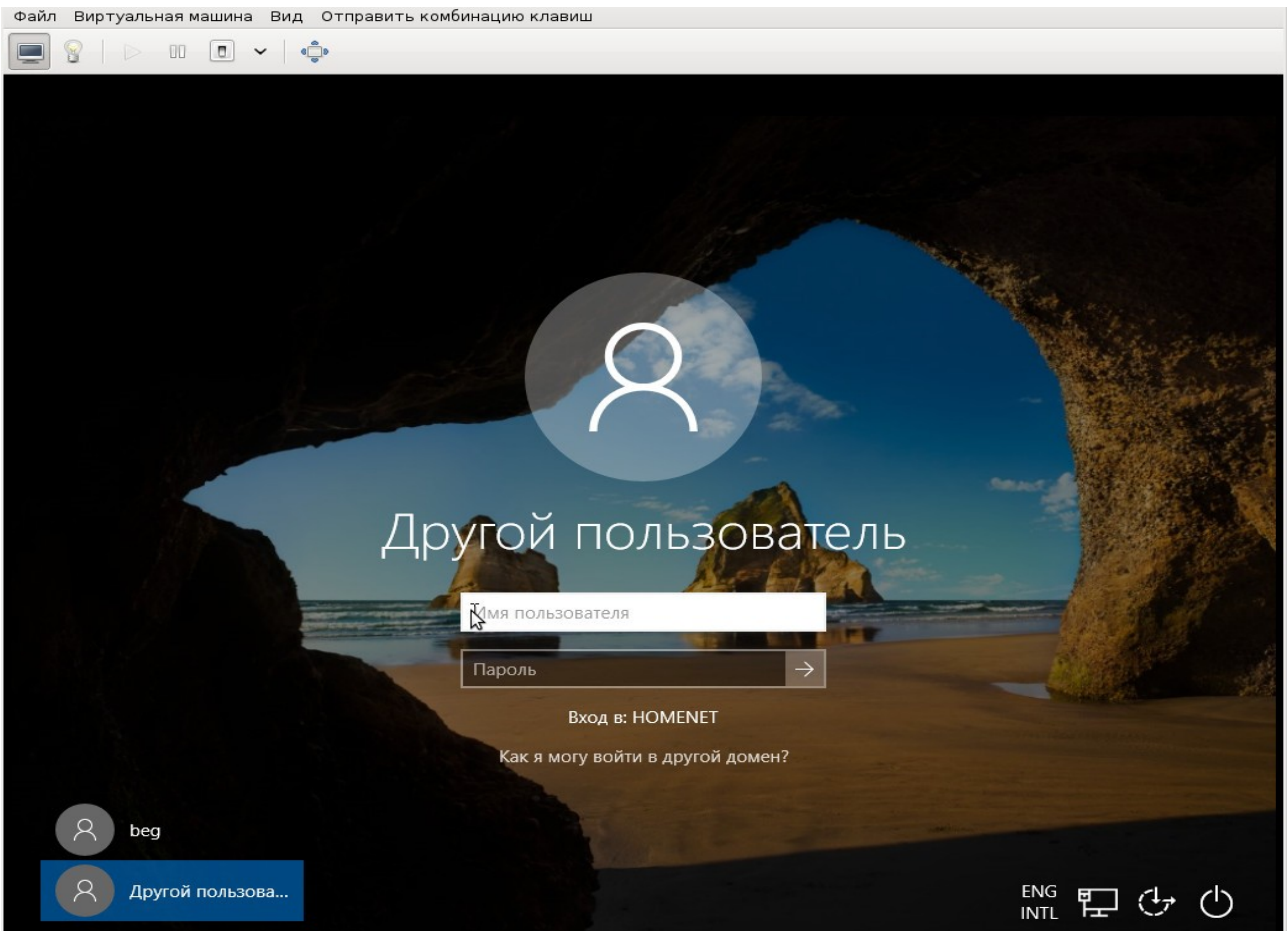


модифицируем настройки сети - включаем сетевое обнаружение, и меняем адрес DNS на адрес нашего контроллера домена.

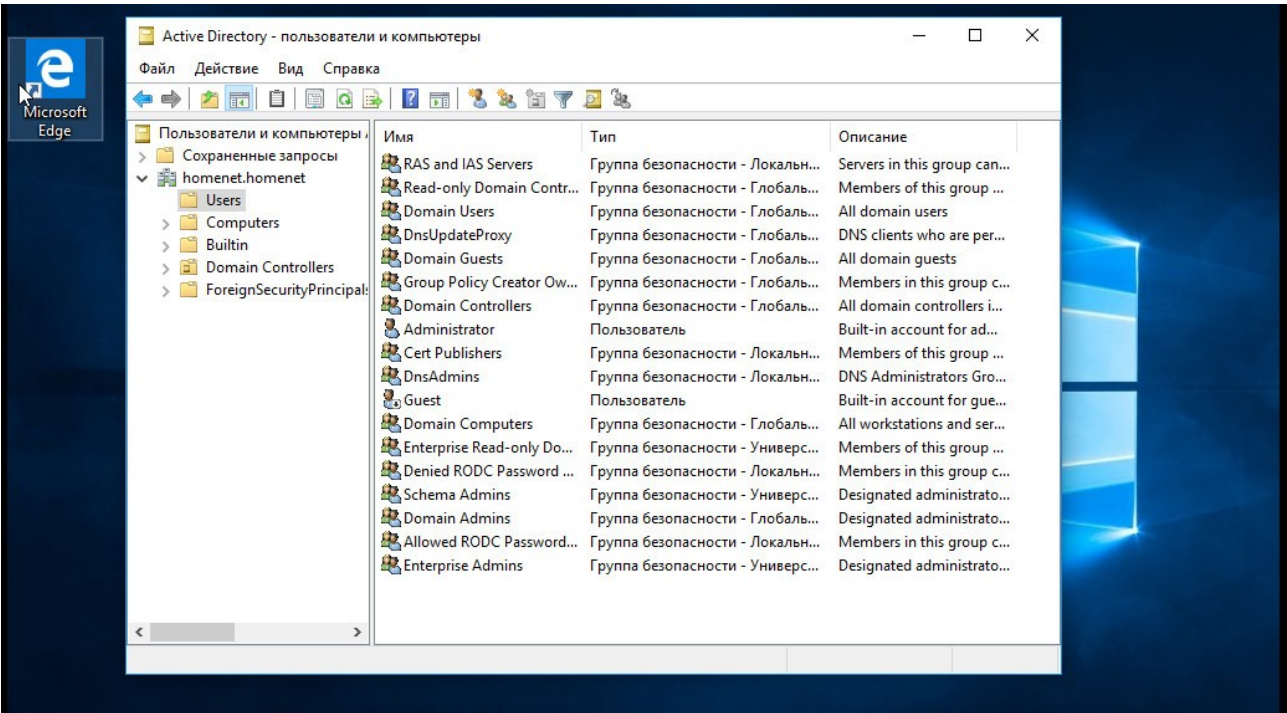
Пробуем ввести компьютер в домен:



После перезагрузки аутентифицируемся на рабочей станции пользователем administrator в домене homenet:

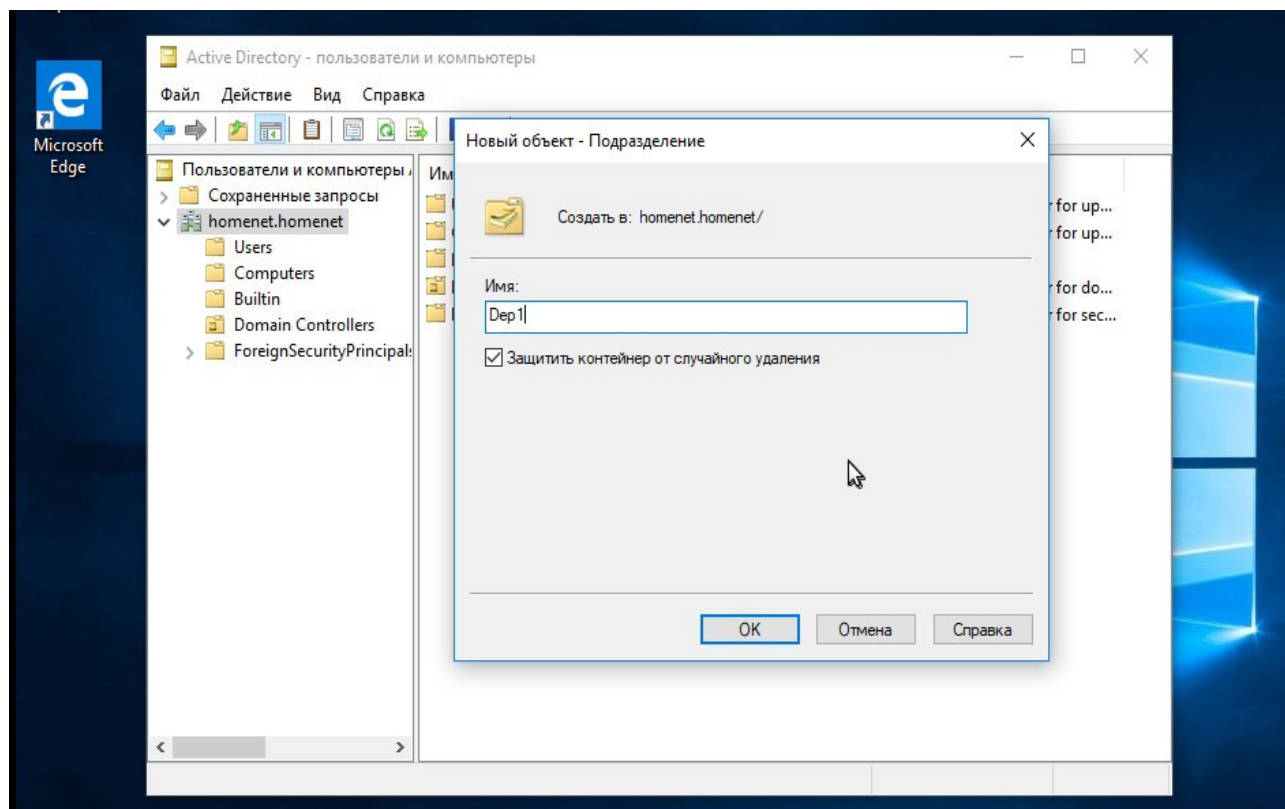


Можем управлять контроллером домена через набор инструментов RSAT:

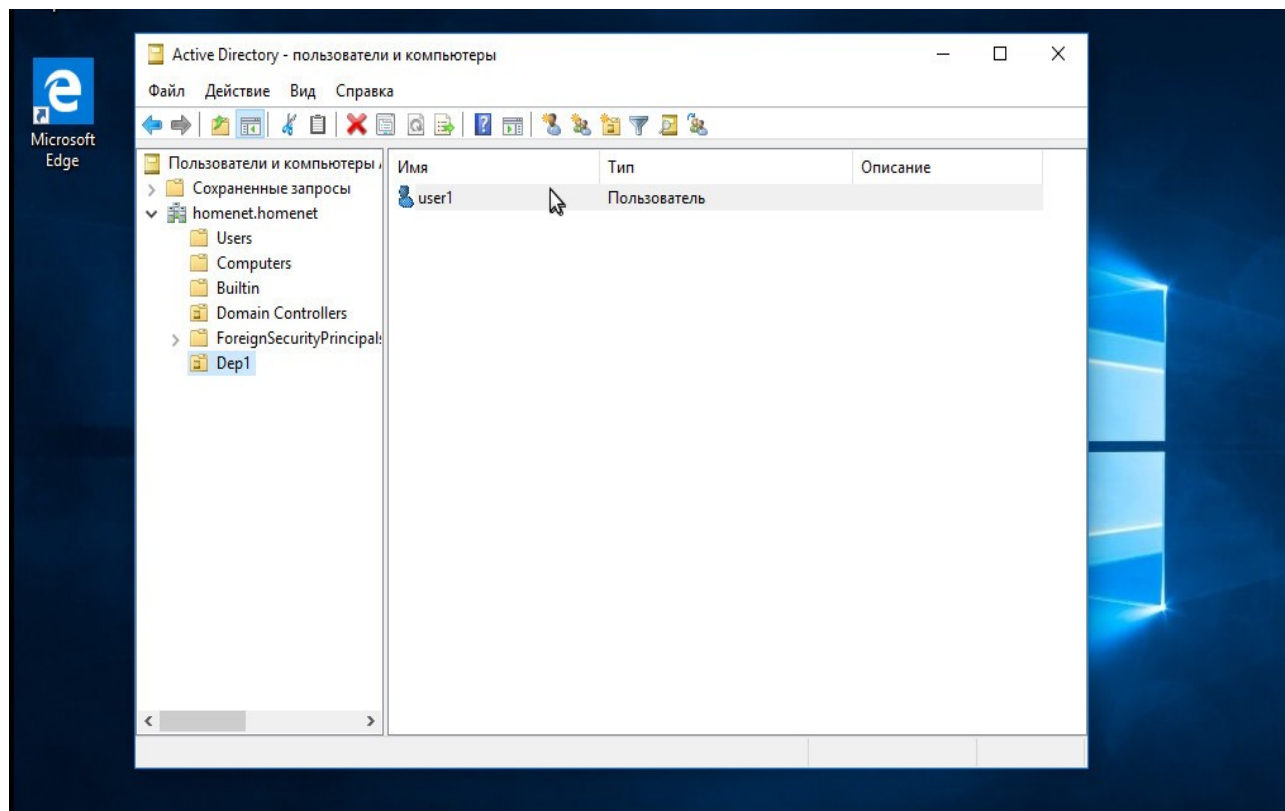




Создадим контейнер-подразделение Dep1:



А в нем пользователя user1:



Для использования разделяемых ресурсов необходимо модифицировать конфигурационный файл /etc/samba/smb.conf (добавляем секцию SHARE)

```
/etc/samba/smb.conf
# Global parameters
[global]
    dns forwarder = 192.168.1.1
    netbios name = UBUNTU-DC
    realm = HOMENET.HOMENET
    server role = active directory domain controller
    workgroup = HOMENET
    idmap_ldb:use rfc2307 = yes

[netlogon]
    path = /var/lib/samba/sysvol/homenet.homenet/scripts
    read only = No

[sysvol]
    path = /var/lib/samba/sysvol
    read only = No

[share]
    path=/home/usershares
    read only = No
    write ok = Yes
    browseable = Yes
    guest ok = No
    public = Yes
```

После этого разделяемый ресурс становится виден в сетевом окружении :

