ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА ПРОГРАММ ПРОФЕССИОНАЛЬНОЙ ПЕРЕПОДГОТОВКИ ВЫПУСК ОСЕНЬ 2022

Автоматизация развертывания Web-proxy SQUID в доменном окружении Active Directory

ЦЕЛЬ:

Используя инструкции Ansible автоматизировать процесс развертывания контролера домена SAMBA и прокси-сервера SQUID с Kerberos-аутентификацией

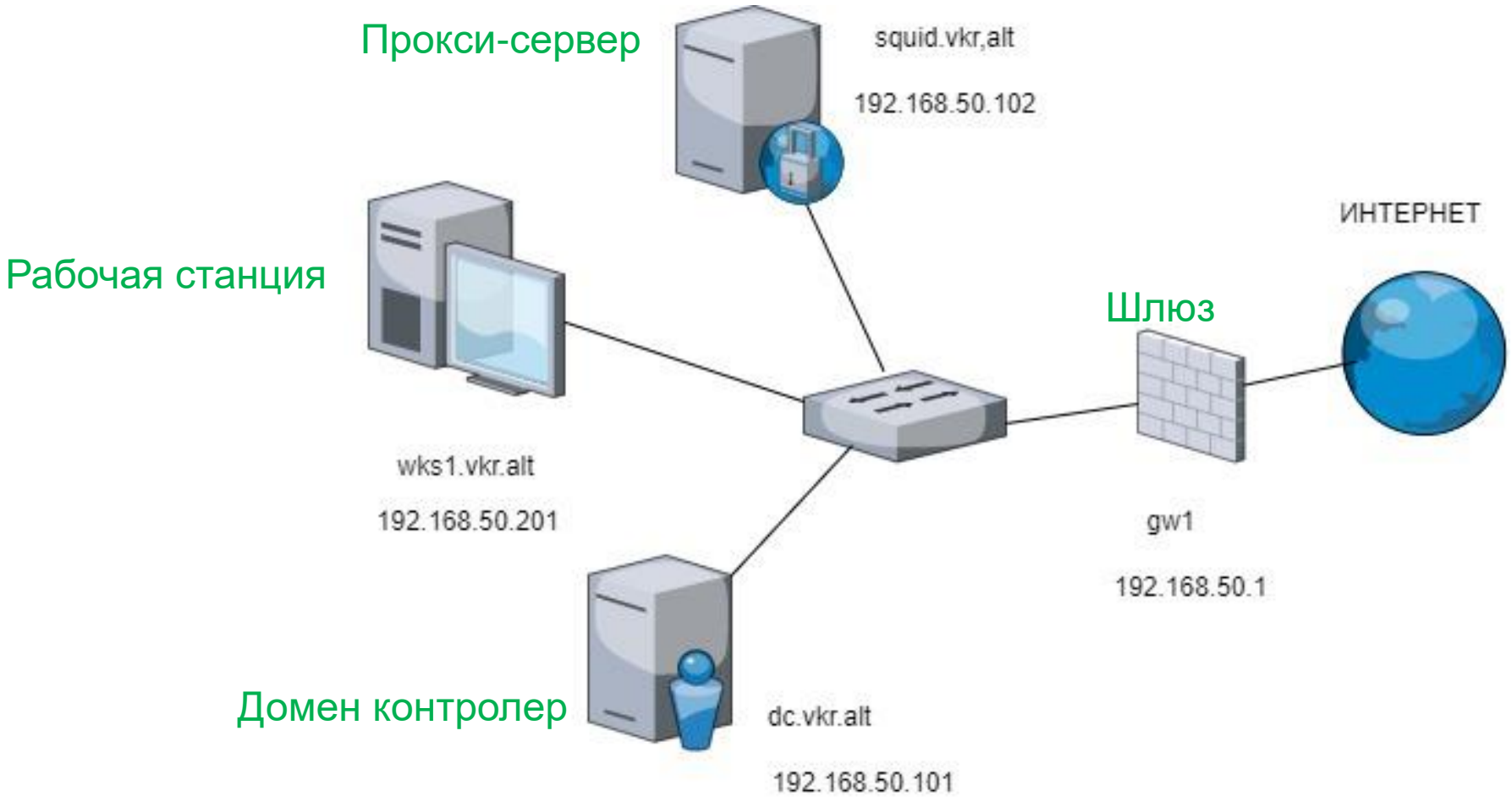
ЗАДАЧИ:

1. Развертывание контролера домена SAMBA и прокси-сервера SQUID.
2. Настройка на прокси-сервере Squid Kerberos-аутентификации.
3. Проверка работоспособности.

Исполнитель: Мейлус Олег Евгеньевич

Руководитель: Орлов Егор Сергеевич

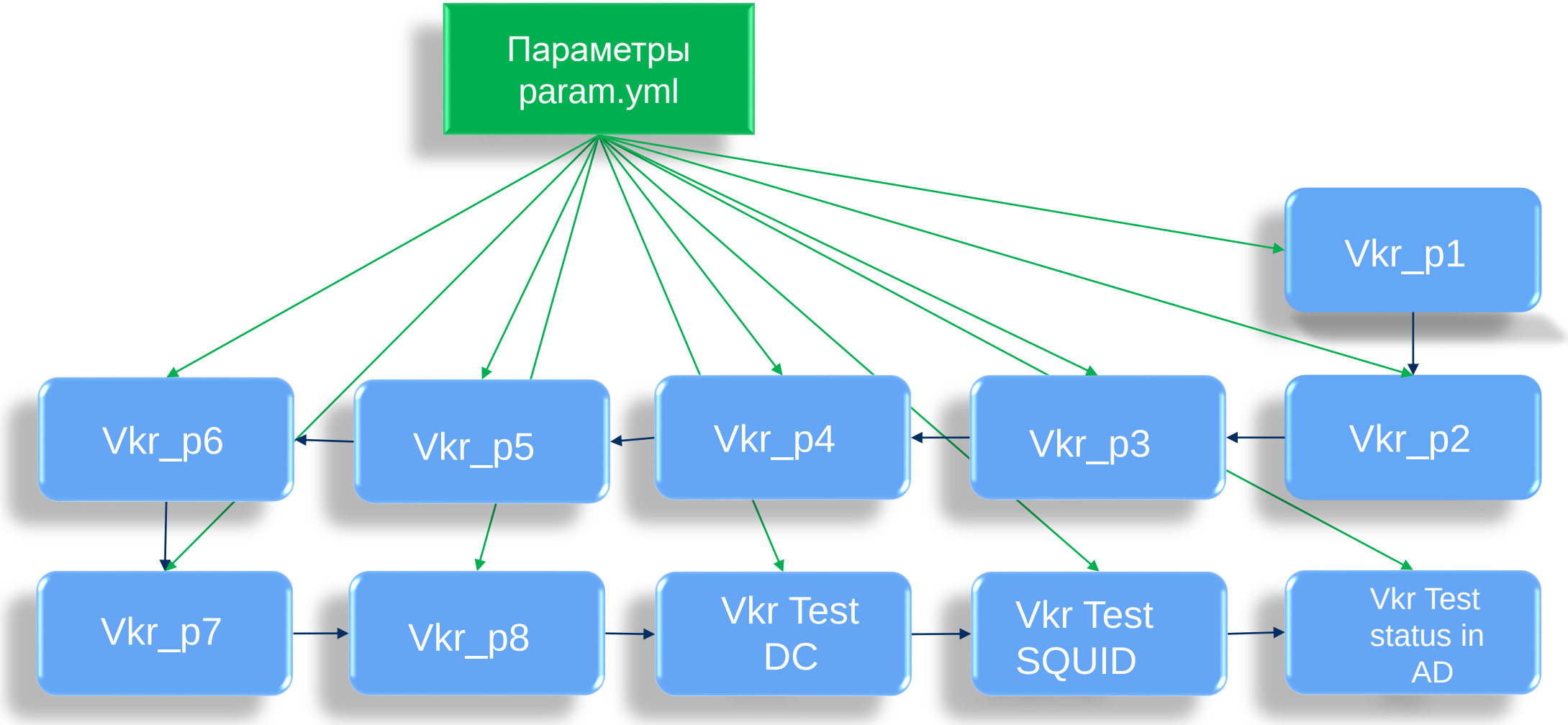
СТЕНД


Прокси-сервер
squid.vkr,alt
192.168.50.102
Рабочая станция
ИНТЕРНЕТ
Шлюз
wks1.vkr.alt
192.168.50.201
gw1
192.168.50.1
Домен контролер
dc.vkr.alt
192.168.50.101

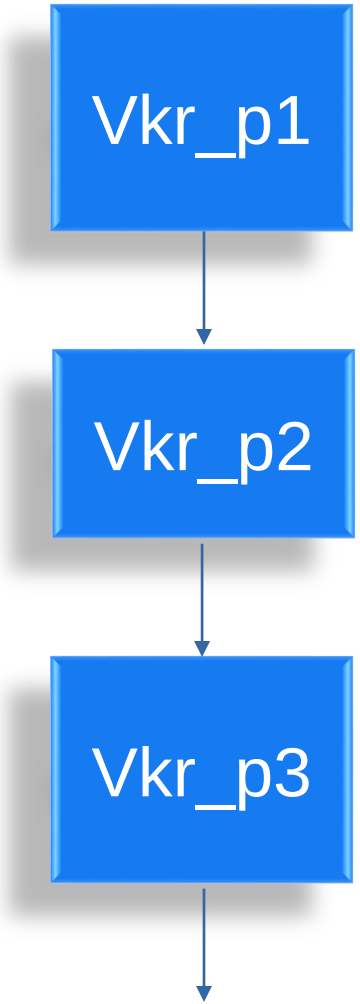
Настройки стенда:

1. Рабочая станция:
    1. Имя: wks1.vkr.alt,
    2. ОС: Альт рабочая станция 9.2.
    3. IP Адрес: 192.168.50.201,
    4. Шлюз: 192.168.50.1.1,
    5. DNS: 192.168.1.1,
    6. Прокси-сервер: 192.168.50.102,
2. Домен контролер:
    1. Имя: dc.vkr.alt,
    2. ОС: Альт сервер 9.2.
    3. IP Адрес: 192.168.50.101,
    4. Шлюз: 192.168.50.1.1,
    5. DNS: 192.168.1.1,
    6. Прокси-сервер: 192.168.50.102,
3. Прокси сервер:
    1. Имя: squid.vkr.alt,
    2. ОС: Альт сервер 9.2.
    3. IP Адрес: 192.168.50.102,
    4. Шлюз: 192.168.50.1.1,
    5. DNS: 192.168.1.1,
4. Шлюз:
    1. Имя: gw-1,
    2. IP Адрес внутренний: 192.168.50.1,
    3. IP Адрес внешний: dhcp,
    4. ОС: Debian.

Схема плейбука VKRv4



Структура плейбука Ансибл VKRv4:

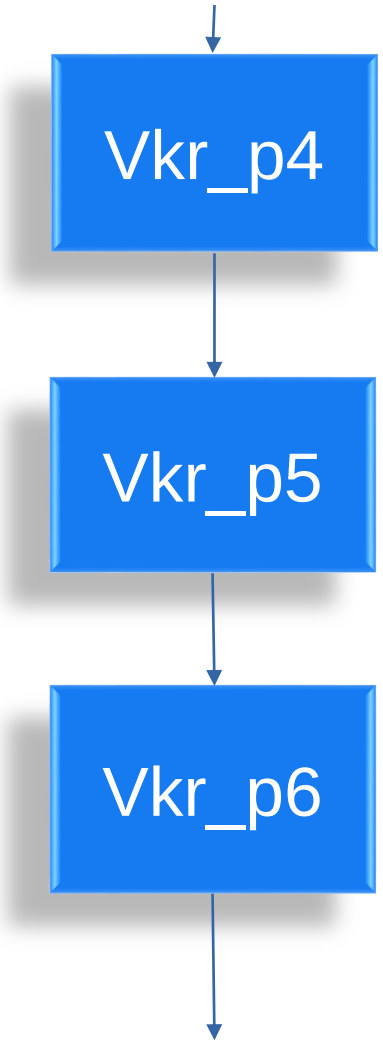


Установка на squid.vkr.alt прокси сервера squid и запуск его

Установка на dc.vkr.alt домен контролера samba и создание домена VKR.ALT а также добавление пользователей: squid_admin и vkruser1

Установка на wks1.vkr.alt и squid.vkr.alt пакета task-auth-ad-sssd, настройка сетевых интерфейсов для введения в домен

Структура плейбука Ансибл VKRv4:

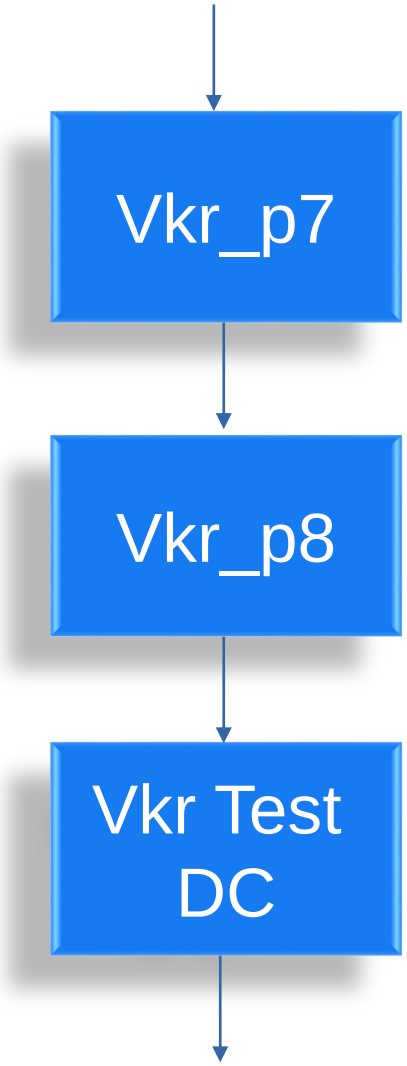


Введение компьютера squid.vkr.alt в домен

На домен контролере dc.vkr.alt создаем кейтаб файл и копируем его на управляющий компьютер wks1.vkr.alt

Компьютер squid.vkr.alt выводим его из домена, перенастраиваем сетевой интерфейс

Структура плейбука Ансибл VKRv4:

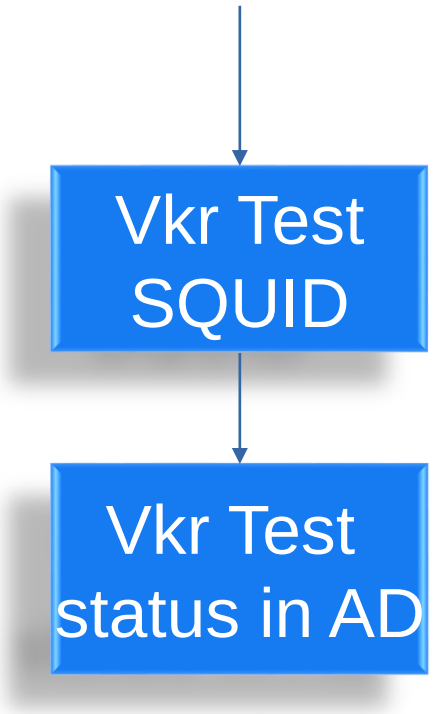


Вводим в домен компьютер wks1.vkr.alt

Копируем на компьютер squid.vkr.alt кейтаб файл и производим настройку Kerberos-аутентификации

Тест домен контролера dc.vkr.alt

Структура плейбука Ансибл VKRv4:



Тест прокси-сервера SQUID на компьютере squid.vkr.alt

Проверка включения компьютера wks1.vkr.alt в домен

Состав файла параметров (переменных) Ансибл:param.yml

```
service_squid: squid
packages_squid: squid
packages_ad: [alterator-net-domain, alterator-fbi, task-samba-dc,
netcmdplus]
new_domain: vkr.alt
domain_short: vkr
admin_pass: Netlab123
services_off_ad: [smb, nmb, krb5kdc, slapd, bind, dnsmasq]
path_off_ad: [/etc/samba/smb.conf, var/lib/samba, var/cache/samba]
recreate_path_ad: /var/lib/samba/sysvol
domain_user: [squid_admin, vkruser1]
dom_user_pass: Netlab123
service_ad: samba
DNS_nameserver_ad: nameserver 127.0.0.1
search_domain: search vkr.alt
packages_ad_domain: task-auth-ad-sssd
DNS_nameserver_new: nameserver 192.168.50.101
computer_squid: squid.vkr.alt
new_domain_SHIFT: VKR.ALT
domain_proxy_user: squid_admin
DNS_nameserver_old: nameserver 192.168.1.1
path_DNS_squid: [/etc/net/ifaces/enp0s8/resolv.conf, /etc/resolv.conf]
path_off_squid: [/etc/krb5.keytab, /etc/net/ifaces/enp0s8/resolv.conf,
/etc/resolv.conf]
computer_wks1: wks1.vkr.alt
```

```
squid_param_old1: '##auth_param negotiate program <uncomment
and complete this line to activate>'
squid_param_old2: '##auth_param negotiate children 20 startup=0
idle=1'
squid_param_old3: '##auth_param negotiate keep_alive on'
squid_param_old4: 'http_access allow localnet'
squid_param_new1: 'auth_param negotiate program
/usr/lib/squid/negotiate_kerberos_auth -s
HTTP/squid.vkr.alt@VKR.ALT -t none'
squid_param_new2: 'auth_param negotiate children 20 startup=0
idle=1'
squid_param_new3: 'auth_param negotiate keep_alive on'
squid_param_new4: 'http_access allow auth'
squid_param_new5: 'acl auth proxy_auth REQUIRED'
squid_param_aft1: '# should be allowed'
```

В плейбуке Ансибл используются переменные :

service_squid: служба squid
packages_squid: установка пакета squid
packages_ad: пакеты для установки домен контролера
new_domain: Полное доменное имя
domain_short: Короткое доменное имя
admin_pass: Пароль администратора домена
services_off_ad: Службы которые необходимо отключить для AD
path_off_ad: Директории которые необходимо удалить на AD
recreate_path_ad: Создать каталог AD
domain_user: Создаваемые доменные пользователи
dom_user_pass: Пароль для доменных пользователей
service_ad: Служба SAMBA
DNS_nameserver_ad: Внутренний адрес AD
search_domain: Указать наименование домена
packages_ad_domain: Установка службы для добавления ПК в AD
DNS_nameserver_new: Адрес домен контролера
computer_squid: Имя компьютера squid
new_domain_SHIFT: Имя домена в верхнем регистре
domain_proxy_user: Имя доменного пользователя для squid
DNS_nameserver_old: Первоначальный адрес ДНС сервера
path_DNS_squid: Файлы squid для изменения
path_off_squid: файлы squid для удаления
computer_wks1: Имя компьютера WKS1

squid_param_old1: Изменяемый параметр1 squid.conf
squid_param_old2: Изменяемый параметр2 squid.conf
squid_param_old3: Изменяемый параметр3 squid.conf
squid_param_old4: Изменяемый параметр4 squid.conf
squid_param_new1: Новый параметр1 squid.conf
squid_param_new2: Новый параметр2 squid.conf
squid_param_new3: Новый параметр3 squid.conf
squid_param_new4: Новый параметр4 squid.conf
squid_param_new5: Новый параметр5 squid.conf
squid_param_aft1: Строчка после которой вставить новый параметр squid.conf

Состав плейбука Ансибл:VKRv4

```
- name: Vkr_p2 Instlall and create DC
  hosts: dc
  gather_facts: true
vars_files: param.yml

    - name: Install packages {{packages_ad }}
    apt_rpm:

- name: Name_server1
    lineinfile:
      path: /etc/net/ifaces/enp0s8/resolv.conf

- name: Name_server2
    lineinfile:
      path: /etc/net/ifaces/enp0s8/resolv.conf
      insertafter: "{{DNS_nameserver_ad }}"

  - name: Name_server3
    lineinfile:
      path: /etc/resolv.conf

 - name: Name_server4
    lineinfile:
      path: /etc/resolv.conf
```

```
- name: Stop and disable {{ services_off_ad }}
    systemd:
      name: "{{ item }}"

  - name: Remove old samba config and state
    file:

  - name: Recreate samba sysvol dir
    file:

  - name: start and enable service {{ service }}
    systemd:

  - name: Copy_krb5
    shell: cp /var/lib/samba/private/krb5.conf /etc/krb5.conf

  - name: edit DNS forwarder
    lineinfile:

  - name: create users
    shell: samba-tool user add {{ item }} {{ dom_user_pass }}

  - name: unlock users
    shell: samba-tool user setexpiry {{ item }} --noexpiry
```

Состав плейбука Ансибл:VKRv4

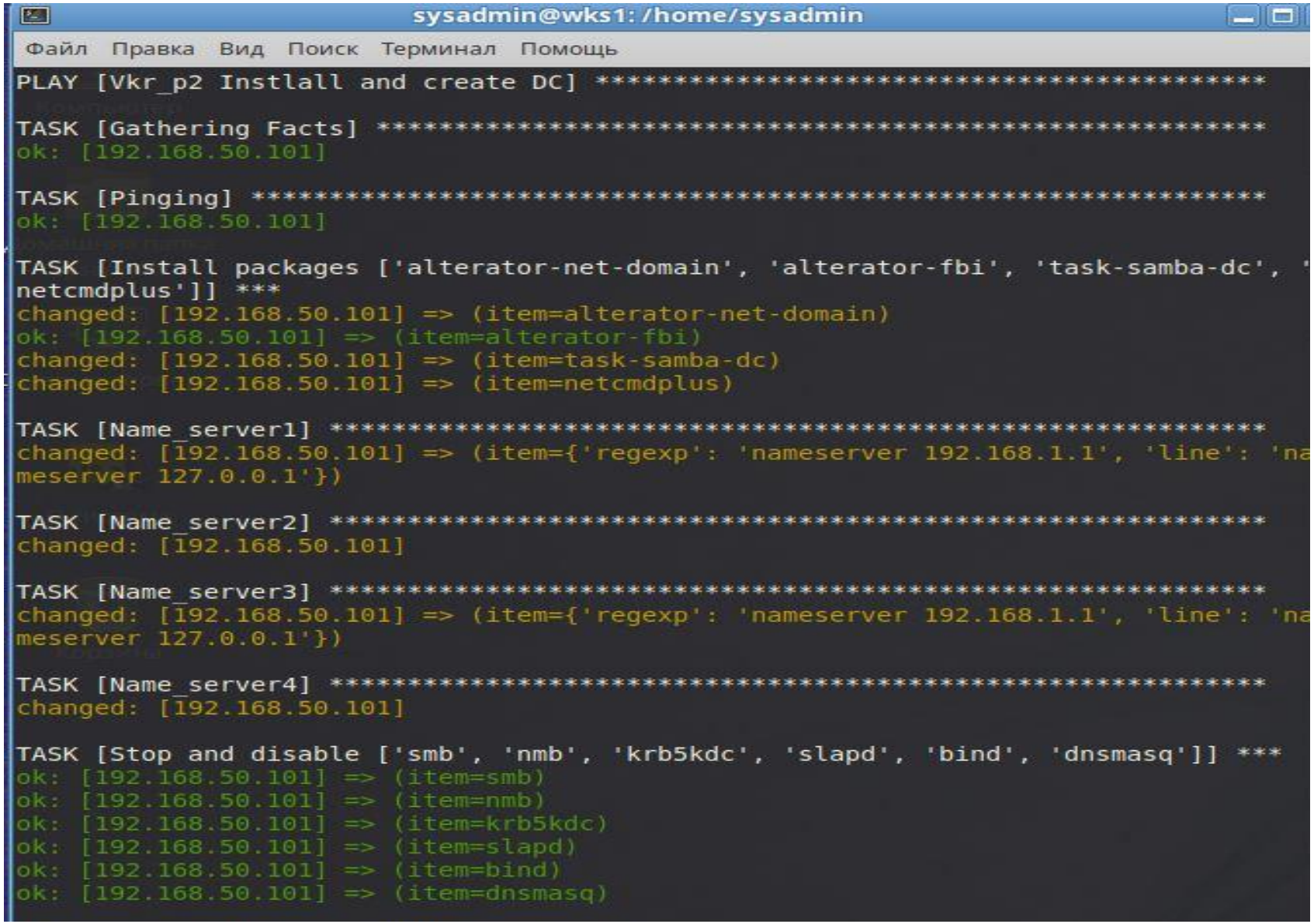
```
- name: Vkr_p5 Create Keytab
  hosts: dc
  gather_facts: true
  vars_files: param.yml

  tasks:
  - name: add_spn
    shell: samba-tool spn add HTTP/{{ computer_squid }}@{{ new_domain_SHIFT }} {{domain_proxy_user }}

  - name: create_squid_keytab
    shell: samba-tool domain exportkeytab /tmp/squid.keytab --principal=HTTP/{{computer_squid }}@{{new_domain_SHIFT }}

  - name: copy keytab to wks
    fetch:
```

Состав плейбука Ансибл:VKRv4

```
- name: Vkr_p8 squid setup
  hosts: squid
  gather_facts: true
  vars_files: param.yml

  tasks:
  - name: copy keytab to squid
    copy:

  - name: Edit Sysconfig_squid string1
    lineinfile:
      path: /etc/sysconfig/squid

  - name: Edit Sysconfig_squid string2
    lineinfile:
      path: /etc/sysconfig/squid

  - name: Edit squid.conf string1
    lineinfile:
       path: /etc/squid/squid.conf

  - name: Edit squid.conf string2
    lineinfile:
      path: /etc/squid/squid.conf
```

```
  - name: start and enable service {{service_squid }}
    systemd:
      name: "{{service_squid }}"
      enabled: yes
      state: restarted
```

Результат работы плейбука Ансибл:

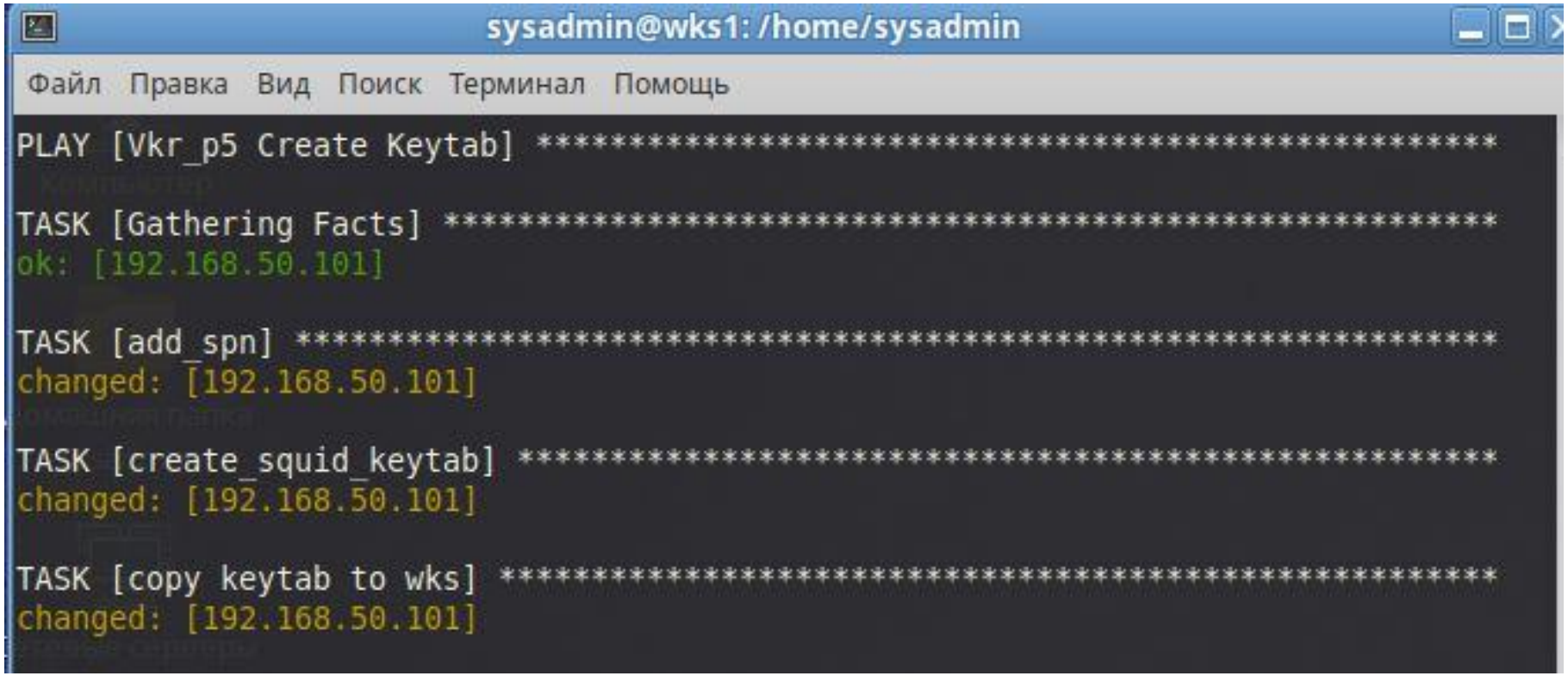


Результат работы плейбука Ансибл:

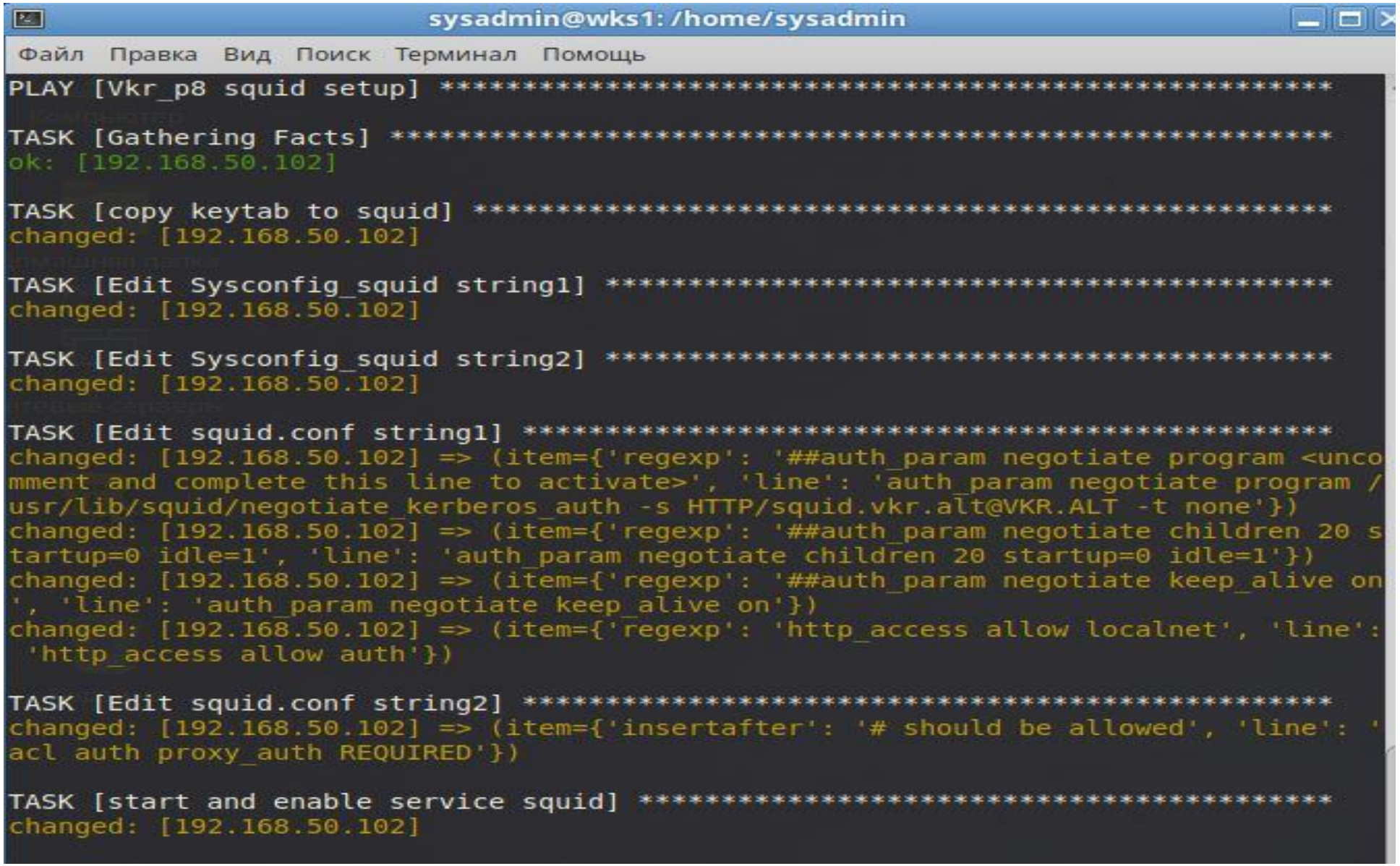
```
TASK [Remove old samba config and state] ***********************************
changed: [192.168.50.101] => (item=/etc/samba/smb.conf)
ok: [192.168.50.101] => (item=var/lib/samba)
ok: [192.168.50.101] => (item=var/cache/samba)

TASK [Recreate samba sysvol dir] *******************************************
ok: [192.168.50.101]

TASK [Create Domain vkr.alt] ***********************************************
changed: [192.168.50.101]

TASK [start and enable service samba] **************************************
changed: [192.168.50.101]
```

```
TASK [Copy krb5] ***********************************************************
changed: [192.168.50.101]

TASK [edit DNS forwarder] **************************************************
changed: [192.168.50.101]

TASK [create users] ********************************************************
changed: [192.168.50.101] => (item=squid_admin)
changed: [192.168.50.101] => (item=vkruser1)

TASK [unlock users] ********************************************************
changed: [192.168.50.101] => (item=squid_admin)
changed: [192.168.50.101] => (item=vkruser1)
```

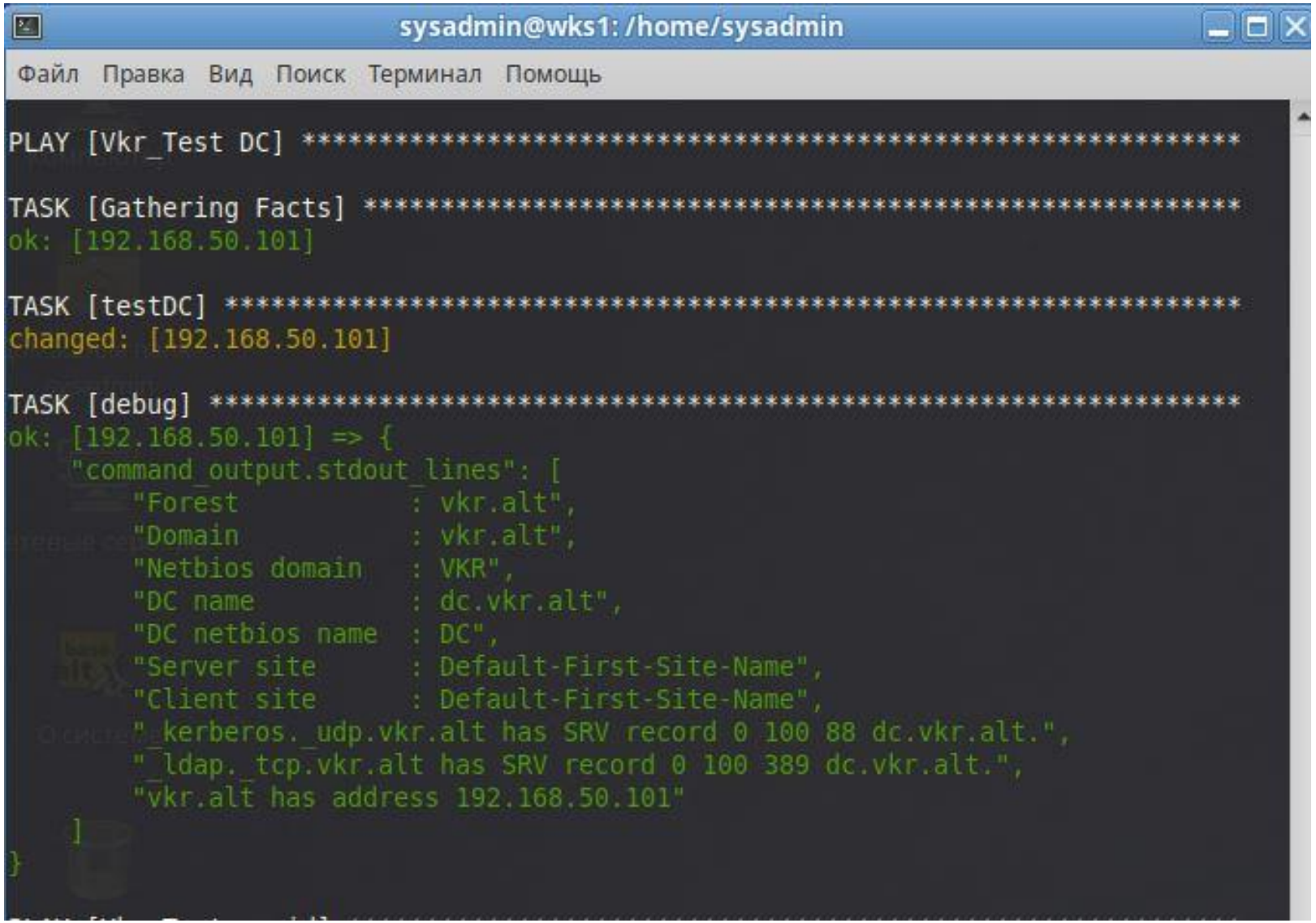
Результат работы плейбука Ансибл:



Результат работы плейбука Ансибл:



Результат работы плейбука Ансибл:

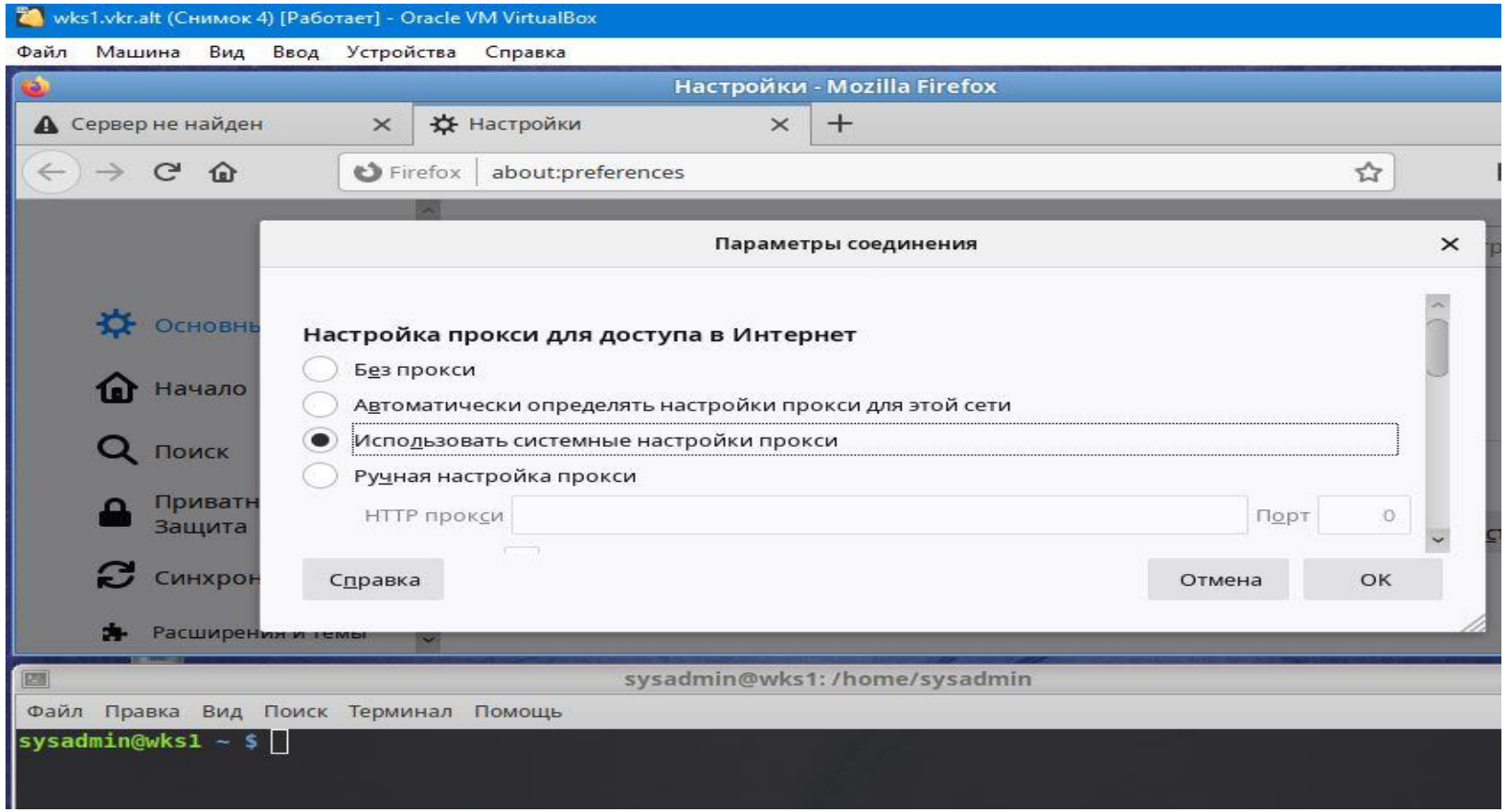


Результат работы плейбука Ансибл:

```
PLAY [Vkr_Test status in AD] ***************************************************

TASK [Gathering Facts] *********************************************************
ok: [192.168.50.201]
ok: [192.168.50.102]

TASK [test ad pc in doamin] ****************************************************
changed: [192.168.50.201]
changed: [192.168.50.102]

TASK [debug] *******************************************************************
ok: [192.168.50.201] => {
    "command_output.stdout_lines": [
        "ad VKR.ALT WKS1.VKR.ALT VKR"
    ]
}
ok: [192.168.50.102] => {
    "command_output.stdout_lines": [
        "local"
    ]
}

PLAY RECAP *********************************************************************
192.168.50.101             : ok=23   changed=16   unreachable=0    failed=0    skipped=0    rescued=0
  ignored=0
192.168.50.102             : ok=32   changed=20   unreachable=0    failed=0    skipped=0    rescued=0
  ignored=0
192.168.50.201             : ok=12   changed=6    unreachable=0    failed=0    skipped=0    rescued=0
  ignored=0
```

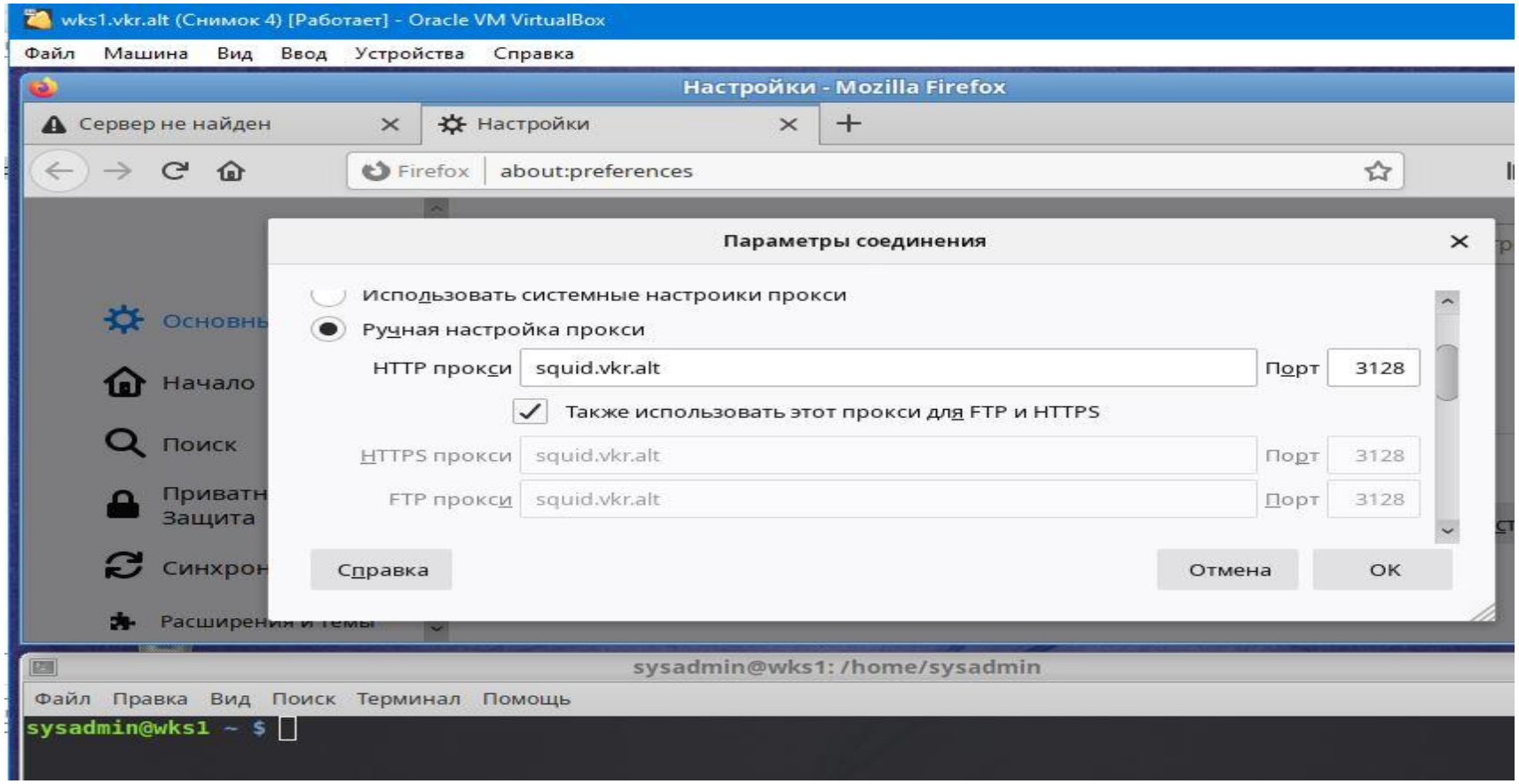
Проверка результатов работы плейбуков Ансибл:

Первоначально пока не настроен интернет браузер доступа в интернет нет:



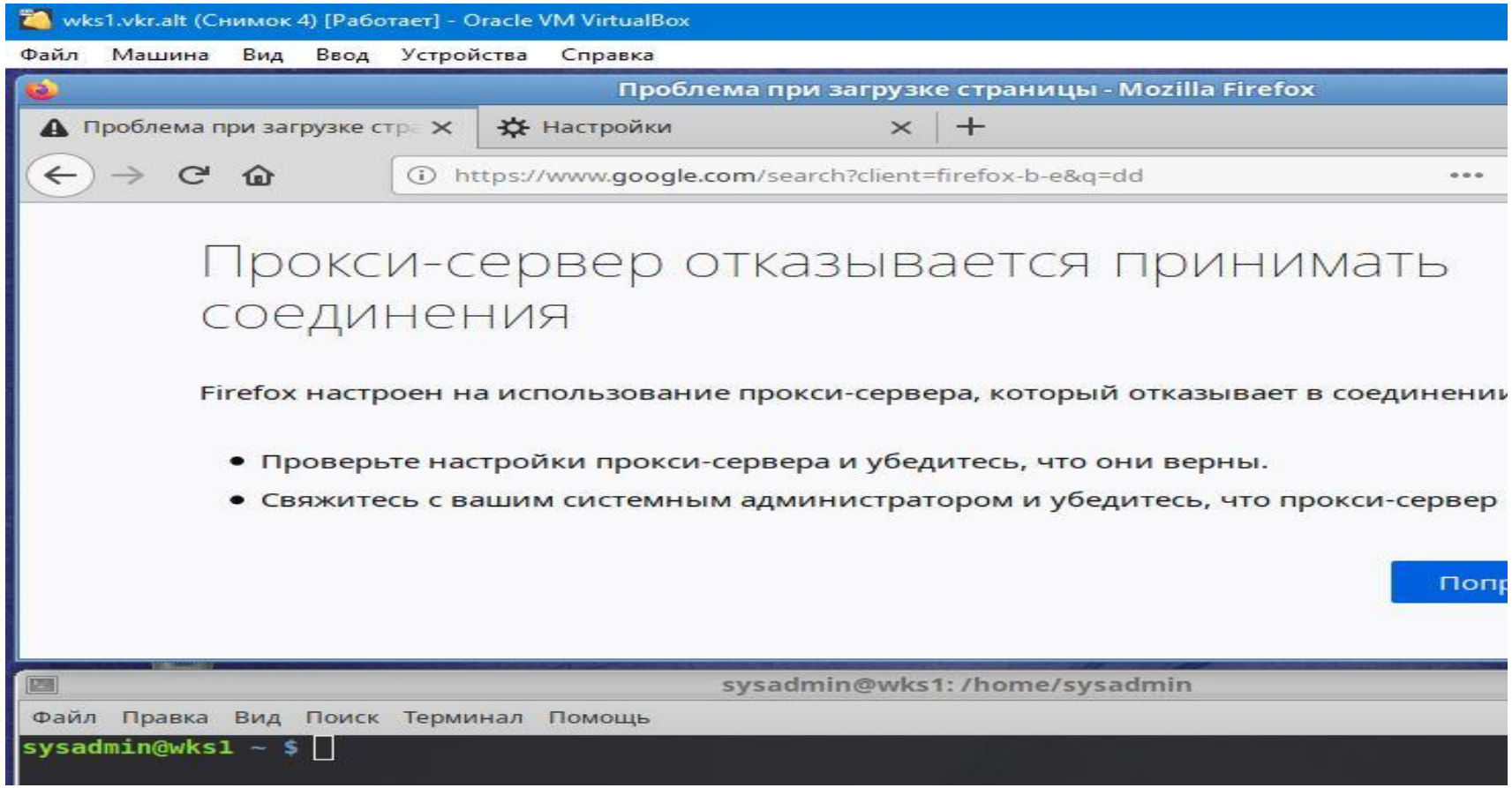
Проверка результатов работы плейбуков Ансибл:

Проводим настройку интернет браузера на прокси сервер:



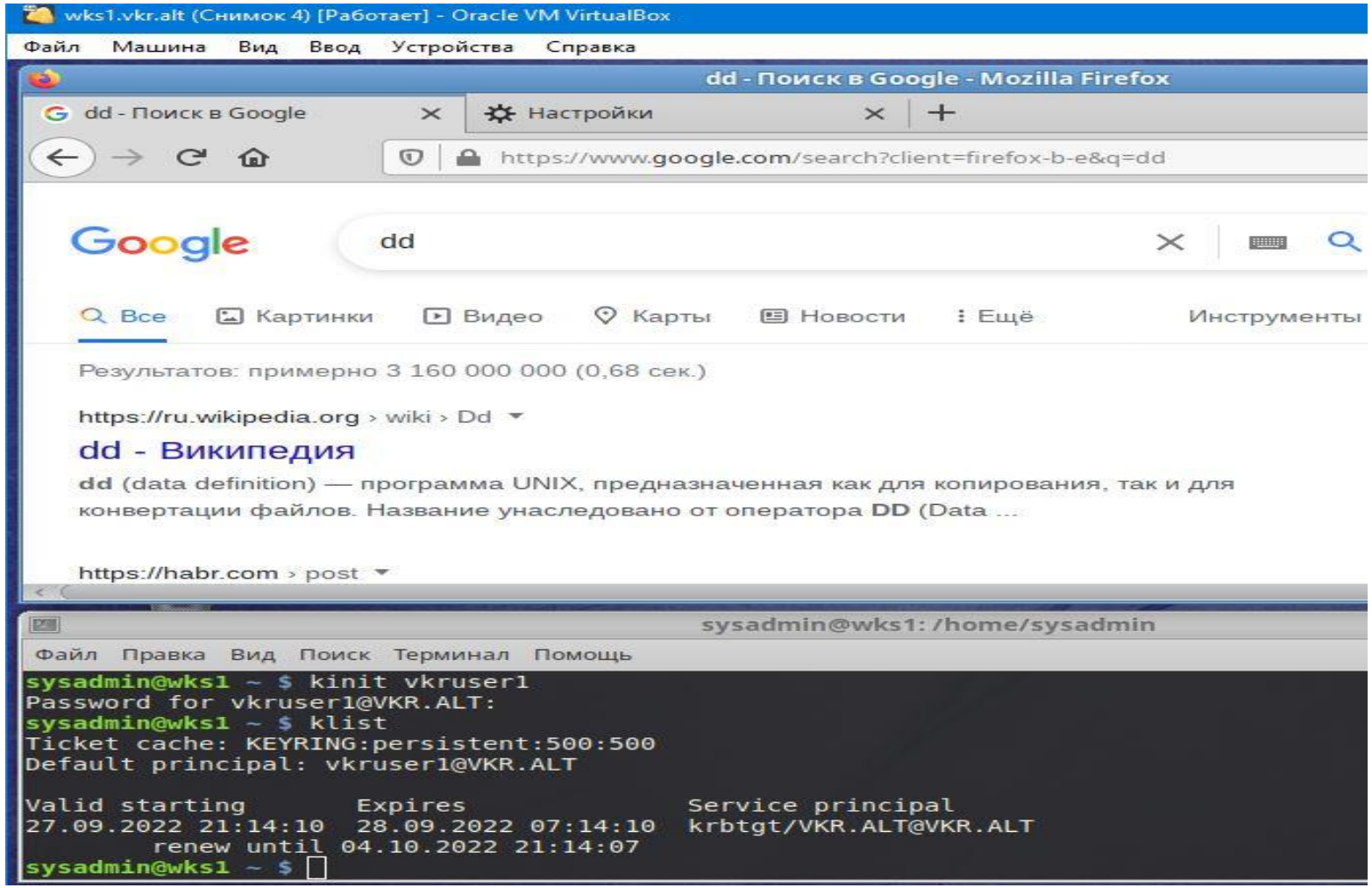
Проверка результатов работы плейбуков Ансибл:

Под локальным пользователем даже после настройки на прокси сервер в интернет браузере доступа к сети интернет нет.



Проверка результатов работы плейбуков Ансибл:

После входа под пользователем домена доступ в интернет получен:



Выводы:

Таким образом в рамках данной работы достигнута цель:

Используя инструкции Ansible автоматизировать процесс развертывания контролера домена SAMBA и прокси-сервера SQUID с Kerberos-аутентификацией.

Задачи решенные в процессе достижения цели:

1. Развернут контролер домена SAMBA и прокси-сервер SQUID (настройки парольной политики SAMBA соответствуют требованиям по ИБ поэтому оставлены без изменений).

2. Настроена на прокси-сервере Squid Kerberos-аутентификация.

3. Проведена успешная проверка работоспособности.