**Студенты:**

**Модуль А. Настройка технических и программных средств информационно-коммуникационных систем.**

Время на выполнение модуля 4 часа.

Доступ к ISP вы не имеете!! Маршрутизаторы RTR-HQ и RTR-BR имеют уже сконфигурированное защищенное соединение, которое будет обеспечивать связность устройств из двух офисов. Также маршрутизаторы RTR-HQ и RTR-BR имеют связность с маршрутизатором ISP, вносить изменения не следует.

Доступ к маршрутизаторам RTR осуществляется по учетной записи admin и паролю P@ssw0rd. Учетная запись для Linux-машин – user с паролем resu. Пароль от суперпользователя – toor.

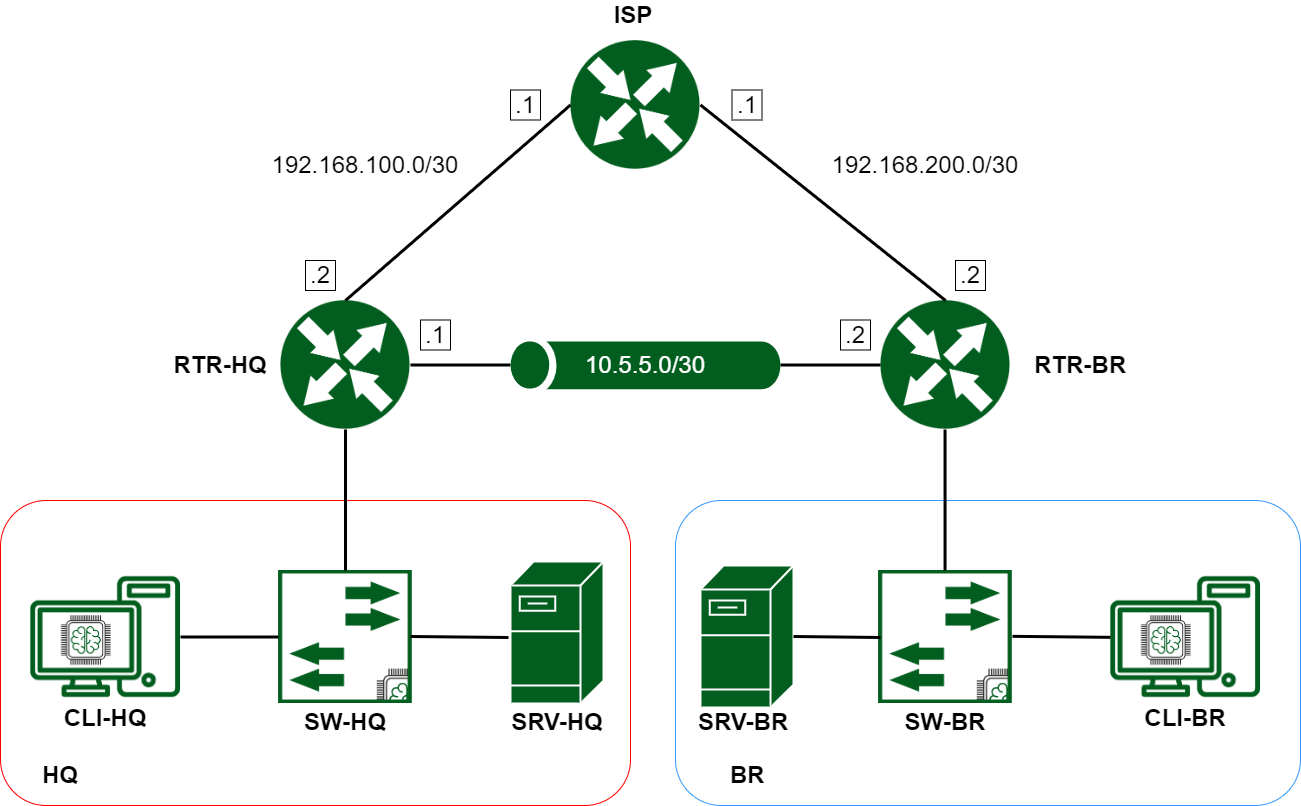


Рисунок 1. Топология

|  |  |
| --- | --- |
| Название устройства | ОС |
| RTR-HQ | Eltex vESR |
| RTR-BR | Eltex vESR |
| SRV-HQ | Альт Сервер 10 |
| SRV-BR | Альт Сервер 10 (допустима замена) |
| CLI-HQ | Альт Рабочая станция 10 |
| CLI-BR | Альт Рабочая станция 10 (допустима замена) |
| SW-HQ | Альт Сервер 10 |
| SW-BR | Альт Сервер 10 (допустима замена) |

На коммутаторах предустановлен пакет openvswitch для реализации функционала коммутатора. На устройстве SRV-HQ предустановлены пакеты freeipa-server, bind, bind-utils, на SRV-BR – bind, bind-utils, ansible,sshpass.

Задания:

1. **Базовая настройка**
2. Настройте имена устройств согласно топологии
   1. Используйте полное доменное имя.

|  |  |
| --- | --- |
| **Устройство** | **Команды** |
| **RTR-HQ | RTR-BR** | **config**  **hostname (rtr-hq/rtr-br).company.prof**  **do commit**  **do confirm** |
| **SW-HQ | SW-BR | SRV-HQ | SRV-BR | CLI-HQ | CLI-BR** | **sudo hostnamectl set-hostname <name>.company.prof;exec bash** |

1. Сконфигурируйте адреса устройств на свое усмотрение. Для офиса HQ выделена сеть 10.0.10.0/24, для офиса BR выделена сеть 10.0.20.0/24. Данные сети необходимо разделить на подсети для каждого vlan.

|  |  |
| --- | --- |
| **Устройство** | **Команды** |
| **RTR-HQ | RTR-BR** | **do show interface status**  **int gi1/0/3**  **ip address 192.168.100.2/30 (192.168.200.2/30)**  **ip firewall disable**  **description ISP**  **exit**  **domain name company.prof**  **domain name-server 192.168.100.1 (192.168.200.1)**  **ip route 0.0.0.0/0 192.168.100.1 (192.168.200.1)**  **int gi1/0/4.1000**  **ip address 10.0.10.1/27 (10.0.20.1/27)**  **ip firewall disable**  **description vlan1000**  **exit**  **int gi1/0/4.2000**  **ip address 10.0.10.33/27 (10.0.20.33/27)**  **ip firewall disable**  **description vlan2000**  **exit**  **do commit**  **do confirm** |
| **SRV-HQ | SRV-BR** | **echo 10.0.10.2/27 (10.0.20.2) > /etc/net/ifaces/ens33/ipv4address**  **echo default via 10.0.10.1 (10.0.20.1) > /etc/net/ifaces/ens33/ipv4route**  **systemctl restart network** |

1. На SRV-HQ и SRV-BR, создайте пользователя sshuser с паролем P@ssw0rd
   1. Пользователь sshuser должен иметь возможность запуска утилиты sudo без дополнительной аутентификации.
   2. Запретите парольную аутентификацию при подключении по SSH к серверам. Аутентификация пользователя sshuser должна происходить только при помощи ключей. Подключение должно производиться с машины CLI-HQ.

|  |  |
| --- | --- |
| **Устройство** | **Команды** |
| **SRV-HQ | SRV-BR** | **useradd sshuser -m -U -s /bin/bash**  **passwd sshuser**  **P@ssw0rd**  **P@ssw0rd**  **echo "sshuser ALL=(ALL) NOPASSWD: ALL" >> /etc/sudoers**  **usermod -aG wheel sshuser**  **mkdir /home/sshuser**  **chown sshuser:sshuser /home/sshuser**  **cd /home/sshuser**  **mkdir -p .ssh/**  **chmod 700 .ssh**  **touch .ssh/authorized\_keys**  **chmod 600 .ssh/authorized\_keys**  **chown sshuser:sshuser .ssh/authorized\_keys**    **(Изменение параметров подключения SSH только после настройки ключей)**  **nano /etc/ssh/sshd\_config**  **PermitRootLogin no**  **PasswordAuthentication no**  **PubkeyAuthentication yes**  **AuthorizedKeysFile .ssh/authorized\_keys**  **AllowUsers sshuser**  **systemctl restart sshd** |
| **CLI-HQ** | **ssh-keygen -t rsa -b 2048 -f srv\_ssh\_key**  **mkdir .ssh**  **mv srv\_ssh\_key\* .ssh/**  **ssh-copy-id -i .ssh/srv\_ssh\_key.pub sshuser@10.0.10.2**  **ssh-copy-id -i .ssh/srv\_ssh\_key.pub sshuser@10.0.20.2** |

1. **Настройка коммутации**
   1. В качестве коммутаторов используются SW-HQ и SW-BR.
   2. В обоих офисах серверы должны находиться во vlan10, клиенты – во vlan20
   3. Для каждого vlan рассчитайте подсети, выданные для офисов. Количество хостов в каждой подсети не должно превышать 30-ти.

|  |  |
| --- | --- |
| **Устройство** | **Команды** |
| **HQ-SW1** | **ovs-vsctl add-br hq-sw1**  **ovs-vsctl add-port hq-sw1 enpos3**  **ovs-vsctl add-port hq-sw1 enpos8**  **ovs-vsctl add-port hq-sw1 enpos9**  **ovs-vsctl add-port hq-sw1 enpos10**  **ovs-vsctl set port enpos8 tag=1000**  **ovs-vsctl set port enpos9 tag=2000**  **ovs-vsctl set port enpos10 tag=1000**  **ovs-vsctl set port enpos3 trunks=1000,2000** |
| **BR-SW1** | **ovs-vsctl add-br br-sw1**  **ovs-vsctl add-port br-sw1 enpos3**  **ovs-vsctl add-port br-sw1 enpos8**  **ovs-vsctl add-port br-sw1 enpos9**  **ovs-vsctl set port enpos8 tag=1000**  **ovs-vsctl set port enpos9 trunks=1000,2000**  **ovs-vsctl set port enpos3 trunks=1000,2000** |
| **BR-SW2** | **ovs-vsctl add-br br-sw2**  **ovs-vsctl add-port br-sw2 enpos3**  **ovs-vsctl add-port br-sw2 enpos8**  **ovs-vsctl set port enpos8 tag=1000**  **ovs-vsctl set port enpos3 trunks=1000,2000** |

1. **Настройка динамической трансляции адресов**
   1. Настройте динамическую трансляцию адресов для обоих офисов. Доступ к интернету необходимо разрешить со всех устройств.

|  |  |
| --- | --- |
| **Устройство** | **Команды** |
| **RTR-HQ | RTR-BR** | **config**  **security zone public**  **exit**  **int gi1/0/3**  **security-zone public**  **exit**  **object-group network LAN**  **ip address-range 10.0.10.1-10.0.10.254 (10.0.20.1-10.0.20.254)**  **exit**  **object-group network WAN**  **ip address-range 192.168.100.2 (192.168.200.2)**  **exit**  **nat source**  **pool WAN**  **ip address-range 192.168.100.2 (192.168.200.2)**  **exit**  **ruleset SNAT**  **to zone public**  **rule 1**  **match source-address LAN**  **action source-nat pool WAN**  **enable**  **exit**  **do commit**  **do confirm** |

1. **Настройка протокола динамической конфигурации хостов**
   1. Настройте протокол динамической конфигурации хостов для устройств в подсетях CLI - RTR-HQ
2. Адрес сети – согласно топологии
3. Адрес шлюза по умолчанию – адрес маршрутизатора RTR-HQ
4. DNS-суффикс – company.prof
5. Настройте протокол динамической конфигурации хостов для устройств в подсетях CLI RTR-BR
6. Адрес сети – согласно топологии
7. Адрес шлюза по умолчанию – адрес маршрутизатора RTR-BR
8. DNS-суффикс – company.prof

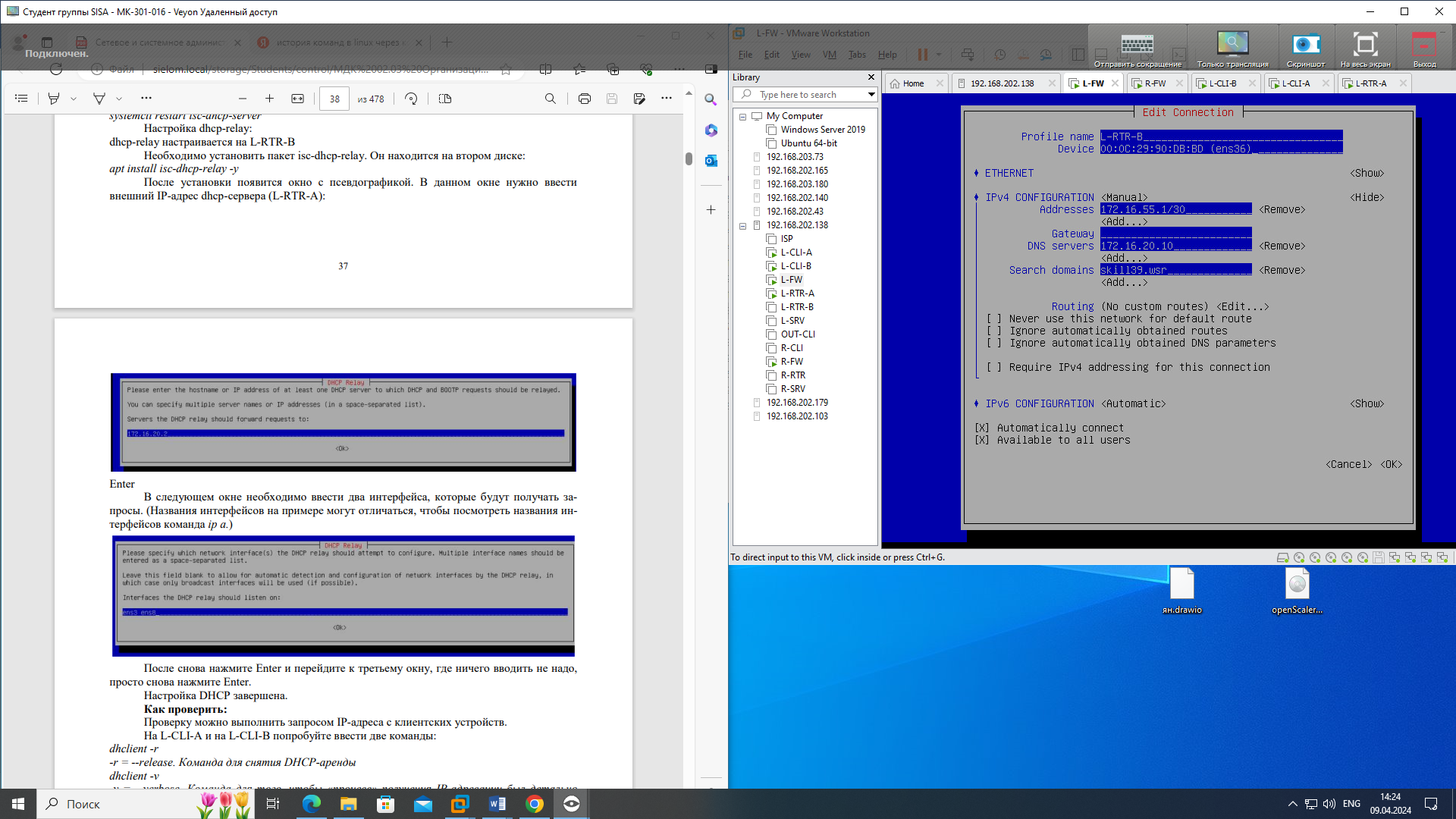
|  |  |
| --- | --- |
| **Устройство** | **Команды** |
| **RTR-HQ | RTR-BR** | **ip dhcp-server pool HQ (BR)**  **network 10.0.10.32/27 (10.0.20.32/27)**  **default-lease-time 3:00:00**  **address-range 10.0.10.34-10.0.10.62 (10.0.20.34-10.0.20.62)**  **default-router 10.0.10.33 (10.0.20.33)**  **domain-name company.prof**  **exit**  **ip dhcp-server** |

1. **Настройка DNS для SRV-HQ.** 
   1. Реализуйте основной DNS сервер компании на SRV-HQ
   2. Для всех устройств обоих офисов необходимо создать записи A и PTR.

|  |  |
| --- | --- |
| Запись | Тип записи |
| rtr-hq.company.prof | A |
| rtr-br.company.prof | A |
| srv-hq.company.prof | A |
| srv-br.company.prof | A |
| cli-hq.company.prof | A |
| cli-br.company.prof | A |

* 1. Клиенты предприятия должны быть настроены на использование внутреннего DNS сервера.

На всех машинках настроить сетевые интерфейсы адреса домена. В зависимости от ip адреса где находится днс сервер и домен в котором находится машина.



Установка bind и bind-utils:

apt-get install -y bind bind-utils

Конфиг:

vim/etc/bind/options.conf

Написать

listen-on { any; };

allow-query { any; };

Включаем resolv:

nano /etc/net/ifaces/ens18/resolv.conf

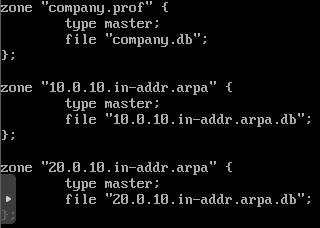
systemctl restart network

Автозагрузка bind:

systemctl enable --now bind

Создаем прямую и обратные зоны:

nano /etc/bind/local.conf



Копируем дефолты:

cp /etc/bind/zone/{localhost,company.db}

cp /etc/bind/zone/127.in-addr.arpa /etc/bind/zone/10.0.10.in-addr.arpa.db

cp /etc/bind/zone/127.in-addr.arpa /etc/bind/zone/20.0.10.in-addr.arpa.db

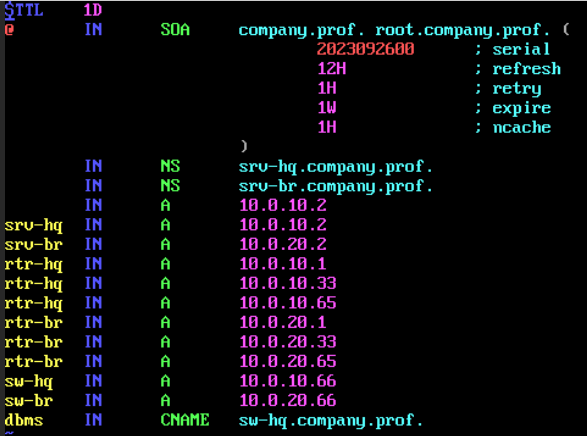
Назначаем права:

chown root:named /etc/bind/zone/company.db

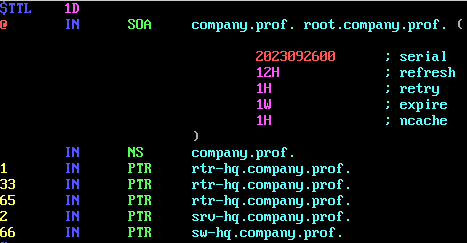
chown root:named /etc/bind/zone/10.0.10.in-addr.arpa.db

chown root:named /etc/bind/zone/20.0.10.in-addr.arpa.db

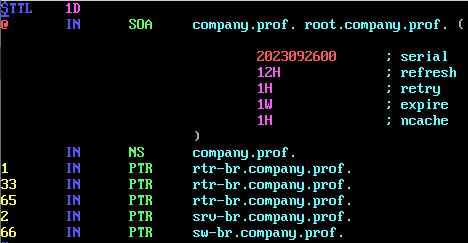
Настраиваем зону прямого просмотра /etc/bind/zone/company.prof:



Настраиваем зону обратного просмотра /etc/bind/zone/10.0.10.in-addr.arpa.db:



Настраиваем зону обратного просмотра /etc/bind/zone/20.0.10.in-addr.arpa.db:

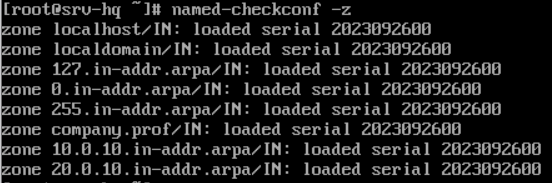


Перезапускаем:

systemctl restart bind

Проверка зон:

named-checkconf -z



**Клиенты предприятия должны быть настроены на использование внутреннего DNS сервера.**

cat /etc/resolv.conf

domain compony.prof

nameserver 127.0.0.1

1. **Настройка узла управления Ansible.**
2. Настройте узел управления на базе SRV-BR
3. Установите Ansible.
4. Сконфигурируйте инвентарь по пути /etc/ansible/inventory. Инвентарь должен содержать три группы устройств:
   1. Networking
   2. Servers
   3. Clients
5. Напишите плейбук в /etc/ansible/gathering.yml для сбора информации об IP адресах и именах всех устройств (и клиенты, и серверы). Отчет должен быть сохранен в /etc/ansible/output.yaml, в формате ПОЛНОЕ\_ДОМЕННОЕ\_ИМЯ – АДРЕС

|  |  |
| --- | --- |
| **Устройство** | **Команды** |
| SRV-BR | **nano /etc/ansible/inventory.yml**  **Networking:**  **hosts:**  **rtr-hq:**  **ansible\_host: 10.0.10.1**  **ansible\_user: admin**  **ansible\_password: P@ssw0rd**  **rtr-br:**  **ansible\_host: 10.0.20.1**  **ansible\_user: admin**  **ansible\_password: P@ssw0rd**  **Servers:**  **hosts:**  **srv-hq:**  **ansible\_host: 10.0.10.2**  **ansible\_ssh\_private\_key\_file: ~/.ssh/srv\_ssh\_key**  **ansible\_user: sshuser**  **srv-br:**  **ansible\_host: 10.0.20.2**  **ansible\_ssh\_private\_key\_file: ~/.ssh/srv\_ssh\_key**  **ansible\_user: sshuser**  **Clients:**  **hosts:**  **cli-hq:**  **ansible\_host: 10.0.10.34**  **ansible\_user: cli**  **ansible\_password: P@ssw0rd**  **cli-br:**  **ansible\_host: 10.0.20.34**  **ansible\_user: cli**  **ansible\_password: P@ssw0rd**  **nano /etc/ansible/ansible.cfg**  **inventory = /etc/ansible/inventory.yml**  **host\_key\_checking = false**  **nano /etc/ansible/gathering.yml**  **---**  **- name: show ip and hostname**  **hosts: all**  **gather\_facts: false**  **tasks:**  **- name: print ip and hostname**  **debug:**  **msg: "{{ ansible\_hostname }} - {{ ansible\_default\_ipv4.address }}"**  **- name: create file**  **lineinfile:**  **path: "/etc/ansible/output.yml"**  **line: "{{ output.msg }}"** |

1. **На сервере SRV-HQ сконфигурируйте основной доменный контроллер на базе FreeIPA**
   1. Создайте 10 пользователей user 1-user10.
   2. Пользователи user1-user10 должны входить в состав группы group1.
   3. Разрешите аутентификацию с использованием доменных учетных данных на ВМ CLI-HQ.
   4. Установите сертификат центра сертификации FreeIPA в качестве доверенного на обоих клиентских ПК.

|  |  |
| --- | --- |
| **Устройство** | **Команды** |
| **SRV-HQ** | **ipa-server-install**  **no**  **srv-hq.company.prof**  **company.prof**  **COMPANY.PROF**  **P@ssw0rd**  **P@ssw0rd**  **COMPANY**  **no**  **yes**  **kinit admin**  **P@ssw0rd**  **Klist**  **for i in {1..30};do**  **echo "P@ssw0rd" | ipa user-add user$i --first=User --last=$i --password;**  **done**  **ipa group-add group1**  **for i in {1..10}; do**  **ipa group-add-member group1 --users=user$i;**  **done**  **cp /etc/ipa/ca.crt /etc/pki/ca-trust/source/anchors/**  **update-ca-trust extract** |
| **CLI-HQ** | **apt-get install -y freeipa-client zip**  **ipa-client-install --mkhomedir**  **yes**  **yes**  **admin**  **P@ssw0rd**  **cp /etc/ipa/ca.crt /etc/pki/ca-trust/source/anchors/**  **update-ca-trust extract** |

**Модуль Б. Региональный (вариативный) компонент.**

* + - 1. **Между маршрутизаторами RTR-HQ и RTR-BR сконфигурируйте защищенное соединение.**

1. Все параметры на усмотрение участника.
2. Используйте парольную аутентификацию.
3. Обеспечьте динамическую маршрутизацию: ресурсы одного офиса должны быть доступны из другого офиса.
4. Для обеспечения динамической маршрутизации используйте протокол OSPF.

|  |  |
| --- | --- |
| **Устройство** | **Команды** |
| RTR-HQ | RTR-BR | **router ospf 1**  **area 0.0.0.0**  **enable**  **exit**  **enable**  **exit**  **tunnel vti 1**  **ip ospf instance 1**  **ip ospf**  **exit**  **interface te1/0/4.10**  **ip ospf instance 1**  **ip ospf**  **exit**  **interface te1/0/4.20**  **ip ospf instance 1**  **ip ospf**  **exit**  **show ip ospf neighbors**  **show ip route** |

* + - 1. **Установка и настройка сервера баз данных.**

a) В качестве серверов баз данных используйте сервера SRV-HQ и SRVBR

b) Разверните сервер баз данных на базе Postgresql

a. Создайте базы данных prod, test, dev

i. Заполните базы данных тестовыми данными при помощи утилиты pgbench. Коэффициент масштабирования сохраните по умолчанию.

b. Разрешите внешние подключения для всех пользователей.

c. Создайте пользователей produser, testuser, devuser, каждому из пользователей дайте доступ к соответствующей базе данных.

|  |  |
| --- | --- |
| **Устройство** | **Команды** |
| SRV-HQ | SRV-BR | **apt-get install -y postgresql postgresql-contrib**  **/etc/init.d/postgresql initdb**  **systemctl enable --now postgresql**  **nano /var/lib/pgsql/data/postgresql.conf**  **listen\_addresses = '\*'**  **psql -U postgres**  **CREATE DATABASE prod;**  **CREATE DATABASE test;**  **CREATE DATABASE dev;**  **CREATE USER produser WITH PASSWORD ‘P@ssw0rd’;**  **CREATE USER testuser WITH PASSWORD ‘P@ssw0rd’;**  **CREATE USER devuser WITH PASSWORD ‘P@ssw0rd’;**  **GRANT ALL PRIVILEGES ON DATABASE prod to produser;**  **GRANT ALL PRIVILEGES ON DATABASE test to test user;**  **GRANT ALL PRIVILEGES ON DATABASE prod to devuser;**  **pgqbench -U postgres -i prod**  **pgqbench -U postgres -i test**  **pgqbench -U postgres -i dev** |

## Студенты:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Код** | **Подкритерий** | **Тип аспекта** | **Аспект** | **Макс. балл** |
| **1** | **Настройка технических и программных средств ИКС** | | | **80** |
| 1 | Базовая настройка | И | Имена устройств настроены согласно с топологии | 1 |
|  |  | И | Адресация на маршрутизаторах настроена согласно топологии | 2 |
|  |  | И | Адресация на серверах настроена согласно топологии | 2 |
|  |  | И | Адресация на клиентах настроена согласно топологии | 2 |
|  |  | И | На SRV-HQ и SRV-BR устройствах создан требуемый пользователь с требуемый паролем | 3 |
|  |  | И | На SRV-HQ и SRV-BR требуемый пользователь имеет возможность запуска sudo без пароля | 3 |
|  |  | И | Запрет парольной аутентификации по SSH на SRV-HQ и SRV-BR | 3 |
| 2 | Настройка коммутации |  |  |  |
|  |  | И | На коммутаторе SW-HQ выполнена настройка trunks и VLAN-access на всех нужных портах | 4 |
|  |  | И | На коммутаторе SW-BR выполнена настройка trunks и VLAN-access на всех нужных портах | 4 |
| 3 | Настройка динамической трансляции адресов |  |  |  |
|  |  | И | Настройте NAT для офиса HQ | 5 |
|  |  | И | Настройте NAT для офиса BR | 5 |
| 4 | Настройка протокола динамической конфигурации |  |  |  |
|  |  | И | Настроить DHCP на RTR-HQ для офиса HQ | 4 |
|  |  | И | Настроить DHCP на RTR-BR для офиса BR | 4 |
| 5 | Настройка DNS для SRV-HQ и SRV-BR |  |  |  |
|  |  | И | Проверка основного DNS сервера на SRV-HQ | 6 |
| 6 | Настройка узла управления Ansible |  |  |  |
|  |  | И | На SRV-BR проверяем существование ansible | 3 |
|  |  | И | На SRV-BR проверяем существование inventory | 3 |
|  |  | И | Запуск плейбука | 6 |
| 7 | Доменная инфраструктура FreeIPA |  |  |  |
|  |  | И | Доменный контроллер установлен | 6 |
|  |  | И | Созданы пользователи и группа, как по заданию | 4 |
|  |  | И | Проверка аутентификации на CLI-HQ | 4 |
|  |  | И | Перемещаемые профили | 6 |
| 2 | **Вариативный модуль** | | | 20 |
| 1 | Защищенное соединение между офисами | | |  |
|  |  | И | Между RTR-HQ и RTR-BR установлено защищенное соединение | 3 |
|  |  | И | Между RTR-HQ и RTR-BR динамическая маршрутизация в защищенном туннеле. | 3 |
|  |  | И | Проверьте, что по OSPF были назначены маршруты | 2 |
| 2 | Установка и настройка сервера баз данных |  |  |  |
|  |  | И | На SRV-HQ и SRV-BR установлен postgresql | 1 |
|  |  | И | На SRV-HQ и SRV-BR созданы базы данных prod,test,dev | 2 |
|  |  | И | Пользователи produser, testuser, devuser имеют доступ только к одноименным с собой БД | 3 |
|  |  | И | Пользователь dbadmin должен иметь доступ ко всем БД | 3 |
|  |  | И | Разрешите внешние подключения к БД для всех пользователей | 3 |