**ВОЗМОЖНОСТЬ ЗАПУСКАТЬ SUDO БЕЗ ПАРОЛЯ**

**Сначала добавить пользователя в группу wheel**

**usermod -a -G wheel sshuser**

**Далее в отредактировать файл vim /etc/sudoers**

**и раскомментить стороку**

**$wheel ALL=(ALL:ALL) NOPASSWD: ALL**

**Отключение selinux redos -> nano /etc/selinux/config :**

**SELINUX=~~Enforcing~~  Permissive**

**https://serverspace.ru/support/help/router-eltex-nastrojka-polzovatelej/?utm\_source=yandex.ru&utm\_medium=organic&utm\_campaign=yandex.ru&utm\_referrer=yandex.ru**

**R-HQ & R-DT**

**НАСТРОЙКА ИНТЕРФЕЙСОВ**

|  |
| --- |
| **Show interfaces status** |
| **Interface gig1/0/1** |
| **Ip add 172.16.5.14/28** |
| **Ip firewall disable** |
| **No sh** |
| **Do commit do confirm** |
|  |

**ip route 0.0.0.0/0 172.16.5.1**

**do show candidate-conf**

**СОЗДАНИЕ ПОЛЬЗОВАТЕЛЕЙ**

**Config**

**User sshuser**

**Password P@ssw0rd**

**Privilege 15**

**DCHP**

**Ip dhcp server**

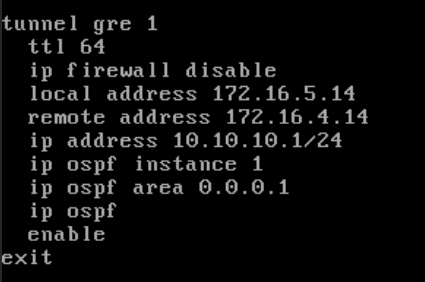
**Ip dhcp-server pool vlan110**

**Network 192.168.11.0/29**

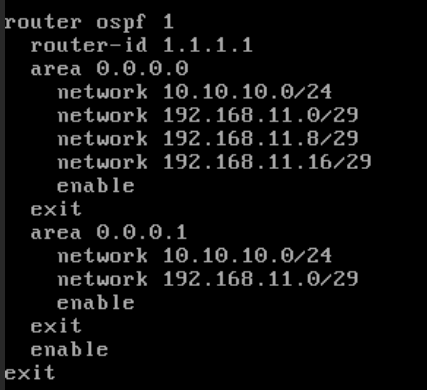
**Default-router 192.168.11.1**

**Address-range 192.168.11.2-192.168.11.1**

**GRE**

****

**OSPF**

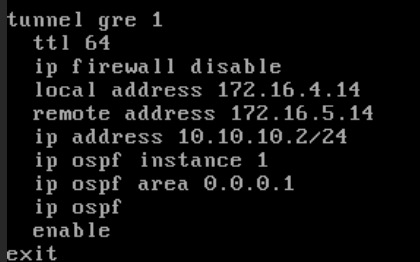
****

**Int gig1/0/1.110**

**Ip ospf passive-interface**

**Tunnel gre 1**

**Ip ospf authentication key-chain password**

****

**NAT**

**Nat source**

**Ruleset vlan1**

**To interface gig1/0/2**

**Rule 1**

**Action source-nat interface**

**enable**

**КОММУТАТОРЫ**

**Interface gig1/0/1-5**

**(conf)# spanning-tree mode stp**

**Interface gig1/0/1**

**Mode switchport**

**Switchport mode trunk**

**Switchport trunk allowed vlan add 110 220 330**

**BRIDGE**

**Ip add**

**Description MGMT**

**LACP**

**Interface port-channel 2**

**Mode switchport**

**Switchport trunk allowed vlan add 110,220,330**

**Interface gig1/0/1 :**

**Channel-group 2 mode auto**

**Show lacp interfaces**

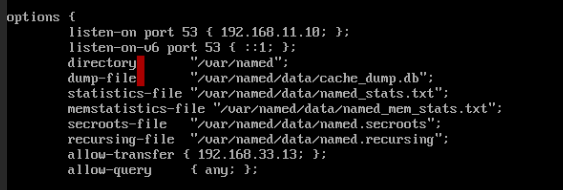
**Dns**

**Systemctl disable system-resolved**

**Vim /etc/named.conf :**

**Allow-query**

**Allow-transfer { вторичный сервер; };**

****

**Vim /etc/named.rf1912.conf**

**Zone**

**ВТОРИЧНЫЙ СЕРВЕР.**

**Vim /etc/named.rfc1912.conf**

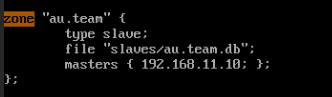
**Zone “au.team” {**

**Type slave;**

**File “slaves/au.team.db”;**

**Masters { 192.168.11.10; };**

**};**

****

**SAMBA**

[**https://redos.red-soft.ru/base/redos-7\_3/7\_3-administation/7\_3-domain-redos/7\_3-domain-config/7\_3-samba-dns-backend-bind9-dlz/7\_3-install-samba-dc-bind/?nocache=1738065602096**](https://redos.red-soft.ru/base/redos-7_3/7_3-administation/7_3-domain-redos/7_3-domain-config/7_3-samba-dns-backend-bind9-dlz/7_3-install-samba-dc-bind/?nocache=1738065602096)

dnf install samba-dc

обязательно должна стоять статика

rm /etc/samba/smb.conf

systemctl enable –now samba

samba-tool domain provision

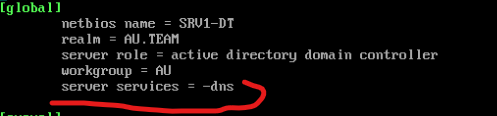
systemctl restart samba

на вторичке приконекчиваемся {куда} {кем} {от имени кого} {к какому серверу} и {какой тип }



**вторичка**

****



Samba tool group create group1

Samba tool ou add ‘OU=CLI’

Samba tool user create user1 –password –userou=’OU=CLI’

Samba tool user move user1 ‘OU=CLI’

Samba tool computer move CLI-HQ ‘OU=CLI’

**# samba-tool group addmembers "Domain Users" user,user1,user2**

**СОЗДАНИЕ ОБЩЕЙ ПАПКИ**

**Mkdir /opt/data**

**Chmod 777 /opt/data**

**Vim /etc/samba/smb.conf**

**[samba]**

**Path = /opt/data**

**Public = yes**

**Read only = no**

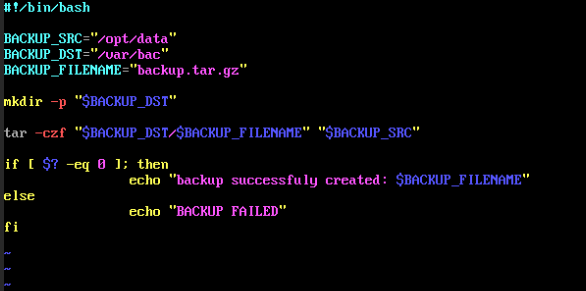
**Writable = yes**

**Guest ok = yes**

**BACKUP**

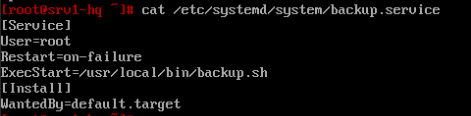
**Создаем файл скрипта -> touch backup.sh /usr/local/bin**

**Даем доп права на файл chmod +x /usr/local/bin/backup.sh**

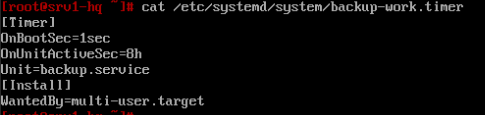
****

**Далее создаем два файла в директории /etc/systemd/system**

**Backup.service**

****

**Backup-work.timer**

****

**DOCKER**

**Dnf install docker-ce**

**Ip link set dev ens18 mtu 1400**

**Systemctl start docker**

**Docker pull nginx:alpine**

**Mkdir -p /docker/nginx**

**Mkdir -p /docker/nginx/html**

**Vim /docker/nginx/html/index.html :**

**<html>**

**<body>**

**<center><h1><b>WEB</b></h1></center>**

**</body>**

**</html>**

**Cd /docker/nginx**

**Cp html/index.html**

**Vim /docker/nginx/Dockerfile :**

**FROM nginx:alpine**

**COPY index.html /usr/share/nginx/index.html**

**DOCKER UPDATE –RESTART=ALWAYS web**

**СОЗДАНИЕ DOCKER REGISTRY**

**› docker run -d -p 5000:5000 --restart=always --name registry registry:2**

**› docker tag my-image <ip-адрес сервера>:5000/my-image:latest**

**/etc/docker/daemon.json :**

**"insecure-registries":["192.168.99.100:5000"] ПРОПИСЫВАЕМ КАК НА КЛИЕНТЕ ТАК И НА СЕРВЕРЕ.  
› docker push <ip-адрес сервера>:5000/my-image:latest**

**Docker pull 192.168.33.10:5000/image\_nginx**

**ZABBIX**

**sudo nano /etc/selinux/config**

**В файле замените текст SELINUX=enforcing на SELINUX=permissive.**

**https://redos.red-soft.ru/base/redos-7\_3/7\_3-administation/7\_3-monitoring/7\_3-zabbix/7\_3-zabbix62-psql13/?nocache=1738238525667**

**Dnf install postgresql16-server Zabbix-server-pgsql fping**

**/usr/bin/postgresql16-server-set initdb**

**ЗАМЕНА ПАРОЛЯ ДЛЯ ADMIN**

**USERS -> AUTHENTICATION -> avoid to easy password x**

**ANSIBLE**

**Dnf install ansible**

**Useradd -u 1010 sshuser**

**Passwd sshuser**

**Vim /etc/ssh/sshd\_config:**

**Port 22**

**Maxuth**

**PasswordAuthentication yes**

**AllowUsers sshuser**

**Systemctl restart sshd**

**Vim /etc/ansible/inventory.yml :**

**Clients:**

**Hosts:**

**Admin-dt:**

**Ansible\_host: 192.168.33.18**

**Ansible\_ssh\_user: sshuser**

**Ansible\_ssh\_pass: P@ssw0rd**

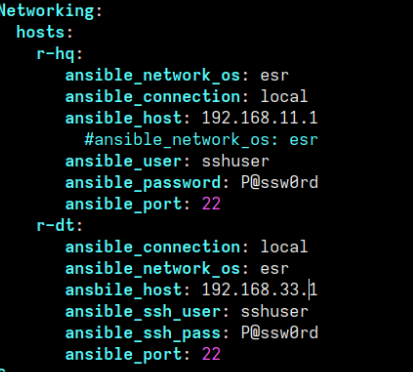
**Ansible\_port: 22**

**Vim /etc/ansible/ansible.cfg :**

**[defaults]**

**Inventory = /etc/ansible/inventory.yml**

**host\_key\_checking = false**

****

**Скачиваем архив -> устанавливаем**

[**https://docs.eltex-co.ru/plugins/viewsource/viewpagesrc.action?pageId=26304373**](https://docs.eltex-co.ru/plugins/viewsource/viewpagesrc.action?pageId=26304373)

**RTR**

**Ip ssh server**

**Ip sftp client sshuser**

**Ip sftp password P@ssw0rd**

SYSLOG

**SERVER** – nano /etc/rsyslog.conf

Раскомменчиваем строки ->

module(load="imudp") # needs to be done just once  
input(type="imudp" port="514")  
  
module(load="imtcp") # needs to be done just once  
input(type="imtcp" port="514")

в конец файла добавляем

$template RemoteLogs,"/var/log/rsyslog/%HOSTNAME%/%PROGRAMNAME%.log"  
\*.\* ?RemoteLogs  
& ~

Клиент

Создаем файл в директории /etc/rsyslog.d/all.conf

All.conf :

В нем прописываем **\*.\* @@192.168.11.1:514**