

**VISOKO UČILIŠTE ALGEBRA**

PROJEKTNI ZADATAK

**Napredno administriranje otvorenih  
operacijskih sustava**

Antonio Janach

Zagreb, lipanj 2020.

## Sadržaj

1. Sažetak .....	1
2. Zahtjevi infrastrukture .....	1
3. Opis infrastrukture .....	2
4. Topologija infrastrukture .....	3
5. Razrada projekta – projektno rješenje.....	4
5.1. Instalacija centralnog autorizacijskog poslužitelja na OOS1 .....	4
5.2. Intranet i extranet .....	7
5.3. File server .....	13
5.4. Mail server .....	16
5.5. Backup.....	20
5.6. Pristup VPN-om.....	22
5.7. Semanage.....	27
6. Popis slika.....	28
7. Literatura.....	29

## 1. Sažetak

Cilj projekta je kreirati infrastrukturu koja će omogućiti tvrtki Križić prijevoz da unaprijedi svoje poslovanje, ali i ostaviti prostora za laki i jednostavan rast. Infrastruktura koju je potrebno realizirati je opisana u poglavlju „Zahtjevi infrastrukture“. Računala koja će se koristiti su OOS1 i OOS2 koja imaju instalirani CentOS operacijski sustav.

## 2. Zahtjevi infrastrukture

Potrebno je kreirati sustav koji će omogućiti centralnu administraciju za 50 ili više korisnika. Svakome od korisnika dodijelit će se uloga unutar organizacije. Generalno, zahtjevi koje je potrebno izvršiti su:

1. Centralni autorizacijski server
2. Mail server sa webmail funkcionalnošću
3. VPN pristup
4. Intranet i extranet
5. Lokalni DNS
6. File server koji mora podržavati Windows i Mac računala

Struktura rješenja infrastrukture, popis instaliranih rola, IP adresa te ostalih karakteristika svakog računala pronaći ćete u poglavlju „Struktura infrastrukture“.

### 3. Opis infrastrukture

#### OOS1 računalno:

Ime računala: oos1.janach.local

Domena: janach.local

Ens192: DHCP protokol

LAN IP ens224: 192.168.1.1/24

LAN IP ens256: 192.168.10.1/24

DNS: 127.0.0.1

Role:

- FreeIPA server
- DNS – integrated FreeIPA DNS
- Vpn sclient: openVPN
- Isctsi-initiator
- VPN client(OpenVPN)
- Backup računala - BackupPC

#### OOS2 računalno:

Ime računala: oos2.janach.local

Domena: janach.local

Ens192: DHCP protokol

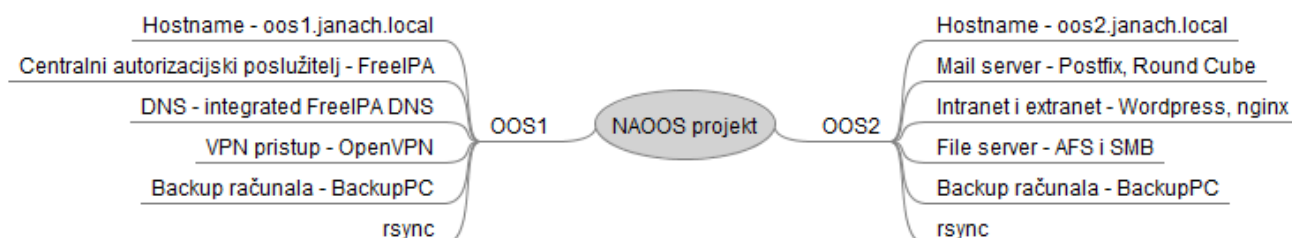
LAN IP ens224: 192.168.2.2/24

LAN IP ens256: 192.168.10.2/24

DNS: 192.168.1.1

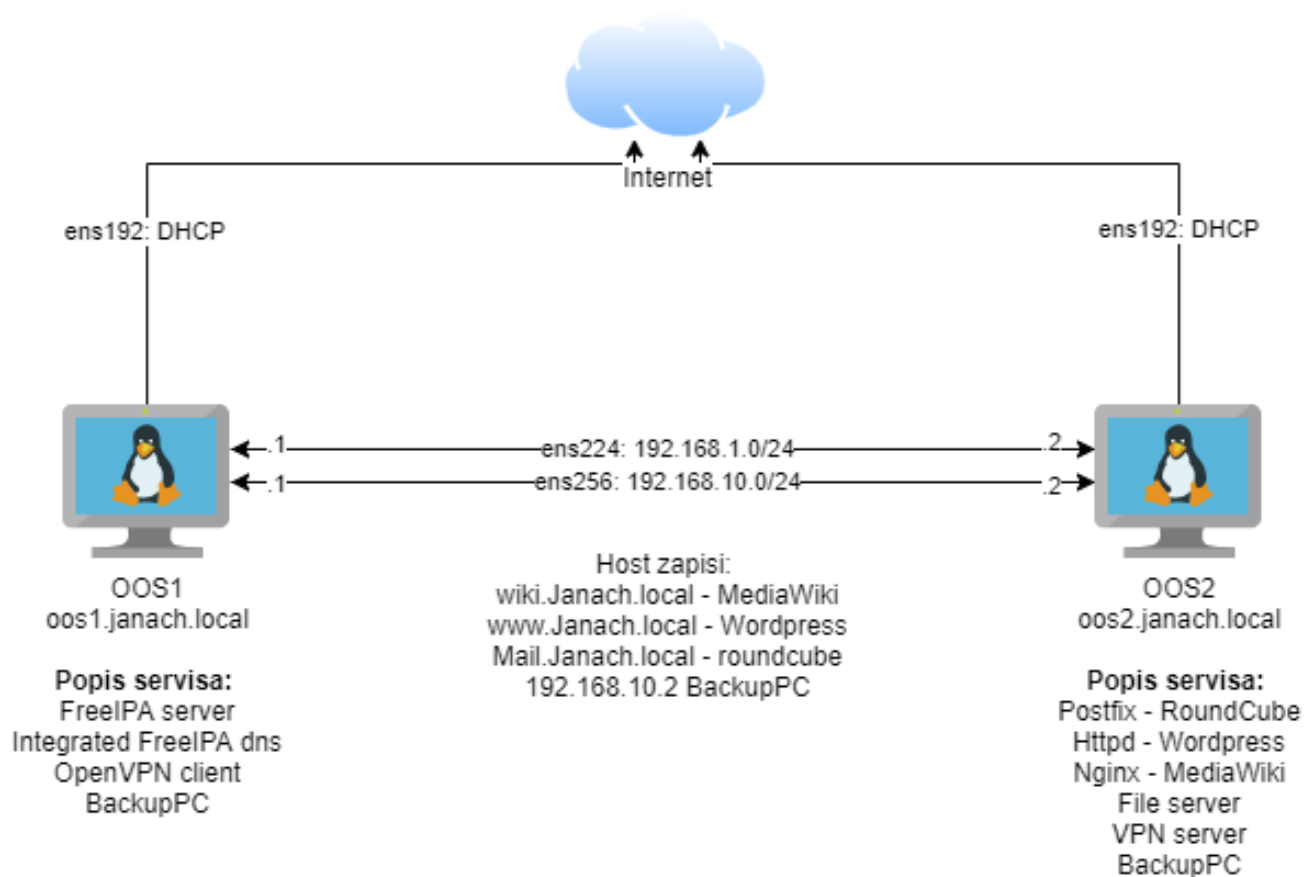
Role:

- FreeIPA klijent
- Mail server: postfix I round cube
- Intranet i extranet: httpd, wordpress, nginx mediawiki
- File server: targetcli (iSCSI)
- VPN server(OpenVPN)
- Backup računala - BackupPC



Slika 1: prikaz opisa infrastrukture koji je izrađen u FreeMind softwar

#### 4. Topologija infrastrukture



Slika 2: prikaz topologije infrastrukture

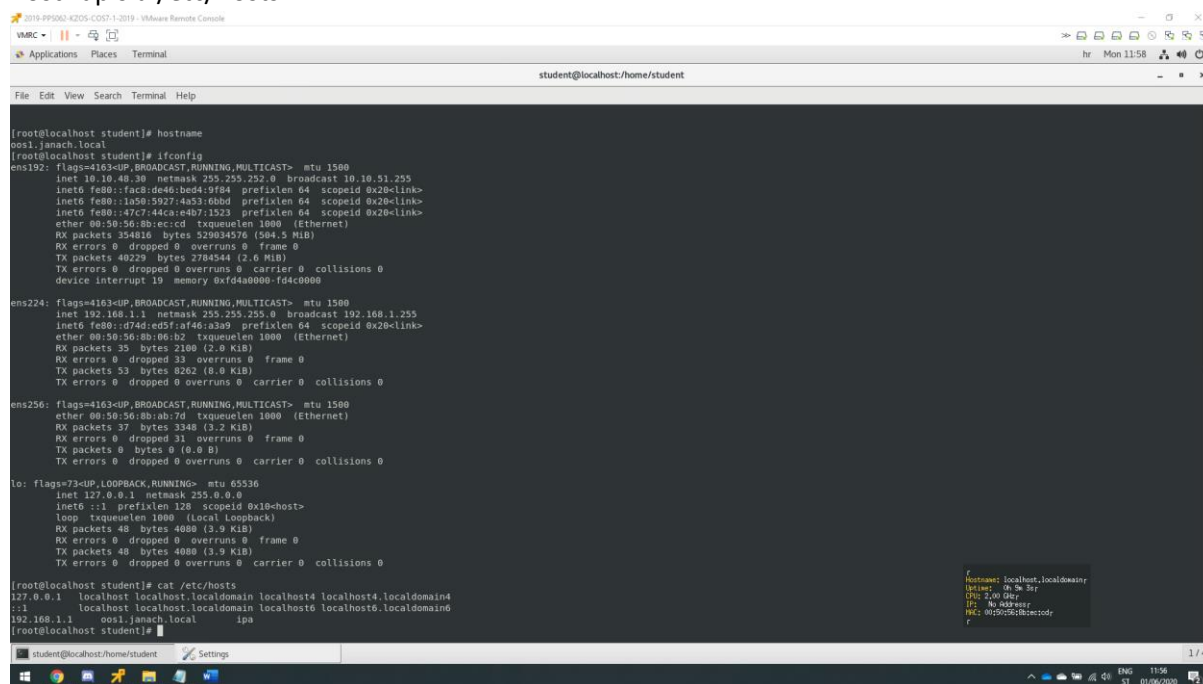
## 5. Razrada projekta – projektno rješenje

### 5.1. Instalacija centralnog autorizacijskog poslužitelja na OOS1

Kako bi instalirali FreeIPA server potrebno je kroz firewall propustiti portove, zatim pokrenuti instalaciju FreeIPA servera. Osnovna FreeIPA konfiguracija je:

- a) Naziv domene: janach.local
- b) Realm: JANACH.LOCAL
- c) Netbios-name: JANACH
- d) Hostname: oos1.janach.local
- e) Admin password: Pa\$\$w0rd
- f) Forwarders: 1.1.1.1 8.8.8.8
- g) Idstart: 10000 i idmax 2000000

Na OOS1 računalu potrebno je promjena hostname, ip adrese na ens224 mrežnom adapteru i dodati host zapis u /etc/hosts:



The screenshot shows a terminal window with the following commands and output:

```
[root@localhost student]# hostname
oos1.janach.local
[root@localhost student]# ifconfig
ens192: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.10.40.30 netmask 255.255.252.0 broadcast 10.10.51.255
    inet6 fe80::fac8:de49:bed4:9f84 prefixlen 64 scopeid 0x20<link>
    inet6 fe80::1a99:5927:a533:6b6d prefixlen 64 scopeid 0x20<link>
    inet6 fe80::47c7:44ca:e4b7:1523 prefixlen 64 scopeid 0x20<link>
    ether 00:50:56:8b:ec:cd txqueuelen 1000 (Ethernet)
    RX packets 354816 bytes 329034576 (3094.5 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 40229 bytes 2704544 (2.6 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
    device interrupt 19 memory 0xfda00000-fdc00000

ens224: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.1 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 fe80::d74d:ed5f:a146:a3a9 prefixlen 64 scopeid 0x20<link>
    ether 00:50:56:8b:06:b2 txqueuelen 1000 (Ethernet)
    RX packets 35 bytes 2100 (2.0 KiB)
    RX errors 0 dropped 31 overruns 0 frame 0
    TX packets 53 bytes 8262 (8.0 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

ens256: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    ether 00:50:56:8b:ab:7d txqueuelen 1000 (Ethernet)
    RX packets 37 bytes 3348 (3.2 KiB)
    RX errors 0 dropped 31 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 48 bytes 4080 (3.9 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 48 bytes 4080 (3.9 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

[root@localhost student]# cat /etc/hosts
127.0.0.1 localhost localhost.localdomain localhost4 localhost4.localdomain4
::1 localhost localhost.localdomain localhost6 localhost6.localdomain6
192.168.1.1 oos1.janach.local ipa
[root@localhost student]#
```

The terminal window also shows the /etc/hosts file content:

```
# Hostname: localhost.localdomain
# Domain: oos1.janach.local
# IP: 192.168.1.1
# MAC: 00:50:56:8b:ec:cd
#
```

Slika 3: prikaz promjene hostname-a, ip adrese na ens224 mrežnom adapteru i dodanog host zapisa

Na OOS1 računalu nužno je pokrenuti firewalld servis i propustiti portove kroz firewall kako bi FreeIPA neometano radila.

```
#pokrenuti firewall i enable-ati ga:
Systemctl start firewalld
Systemctl enable firewalld
#propustiti portove kroz firewall:
Firewall-cmd --permanent --add-service={dns,freeipa-ldap,http,kerberos,kpasswd,ldap,ldaps,ntp}
Firewall-cmd --reload
```

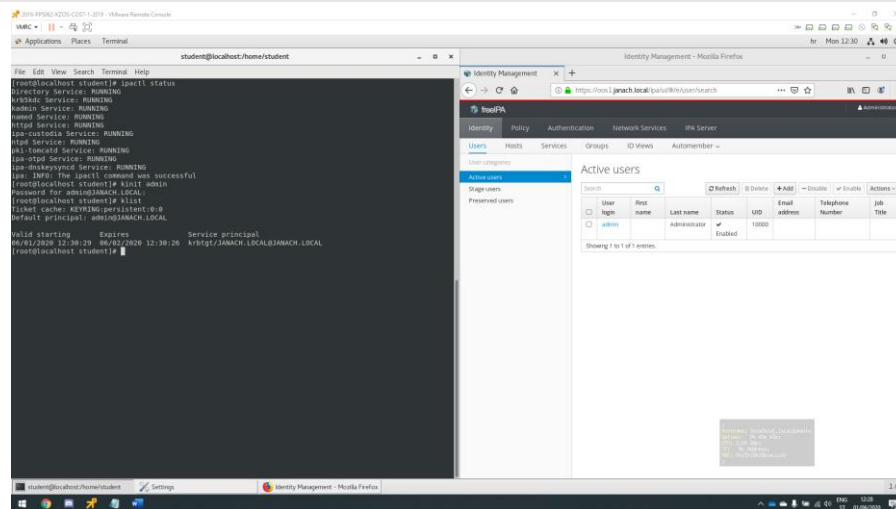
Računalo OOS1 spremno je za instalaciju centralnog autorizacijskog poslužitelja jer zadovoljava sve uvjete koje smo predhodno odradili. U sljedećim koracima slijedi instalacija i konfiguracija FreeIPA.

Instalirati pakete koji su preduvjet instalaciji FreeIPA:

```
Yum install ipa-server bind-dyndb-ldap ipa-server-dns -y
```

Instalirati FreeIPA server:

```
ipa-server-install --setup-dns --forwarder=1.1.1.1 --forwarder=8.8.8.8 --auto-reverse -p „Pa\$\$w0rd“ -a „Pa\$\$w0rd“ --domain=janach.local --realm=JANACH.LOCAL --netbios-name=JANACH --hostname=oos1.janach.local --setup-kra --idstart=10000 --idmax2000000 --mkhomedir --unattended
```

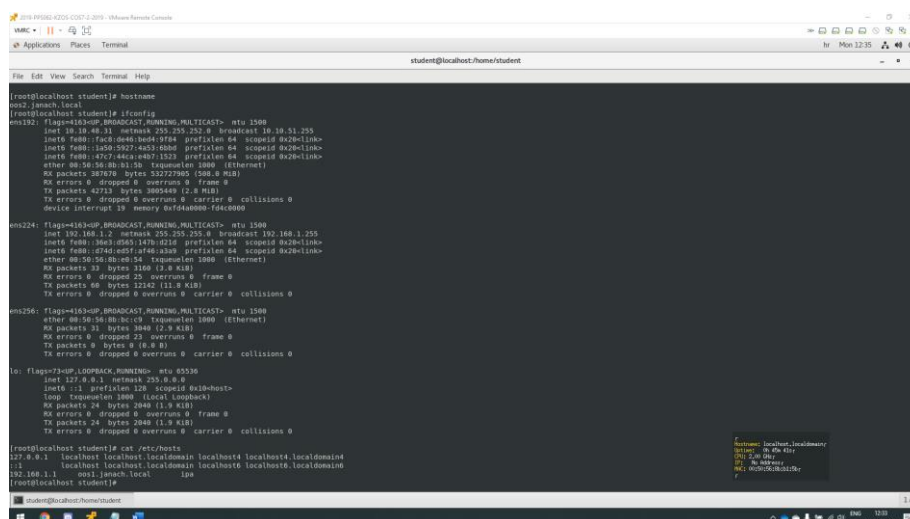


Slika 4: provjera konfiguracije i prikaz uspješne instalacije FreeIPA servera na OOS1 računalu

Na IPA poslužitelj dodajemo DNS zapis za klijenta naredbom ipa dnsrecord-add moguće je ipa dnsrecord dodati i kroz GUI web sučelje.

```
ipa dnsrecord-add janach.local client --a-rec 192.168.1.2
```

Konfiguracija i instalacije FreeIPA poslužitelja na OOS1 računalu je završila, sljedeće što je potrebno, a to je dodati OOS2 računalu u domenu. Stoga na OOS2 nužno je promijeniti hostname, IP adresu na ens224 mrežnom adapteru i dodati host zapisa u /etc/hosts datoteku.



Slika 5: prikaz promjene hostname, IP adrese na ens224 mrežnom adapteru i dodavanje host zapisa

Također kao i na OOS1 računalu nužno je pokrenuti firewalld servis i propustiti portove kroz firewall kako bi FreeIPA neometano radila:

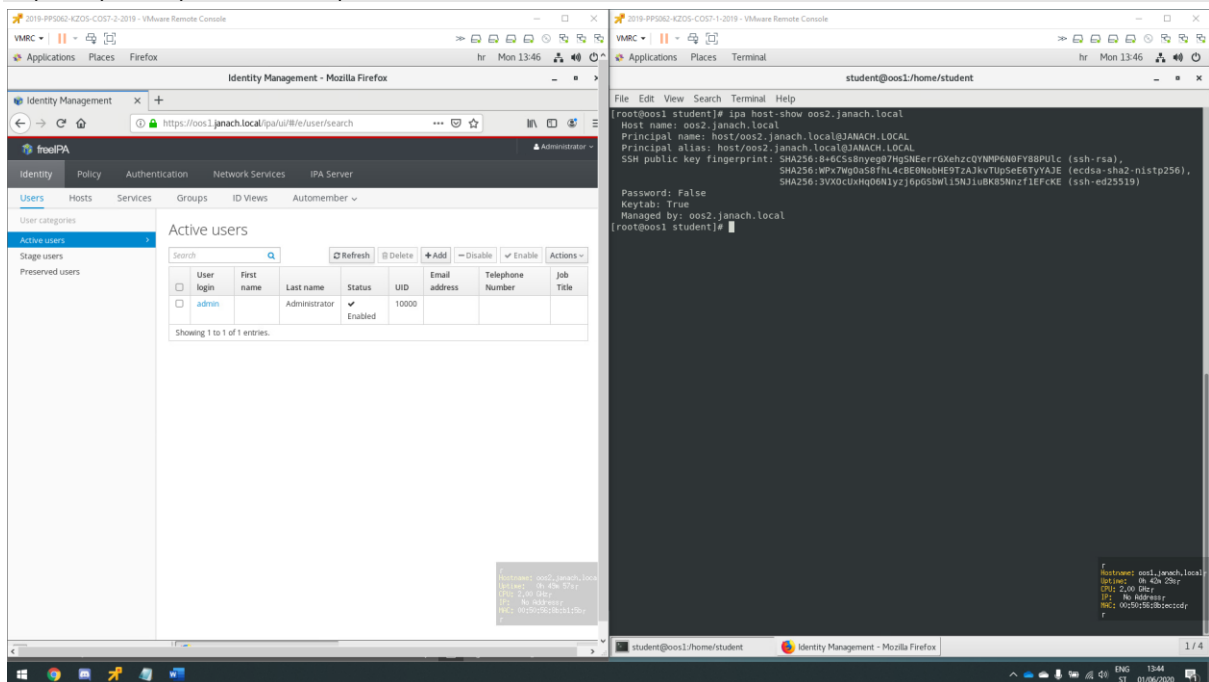
```
#pokrenuti firewall i enable-ati ga:
Systemctl start firewalld
Systemctl enable firewalld
#propustiti portove kroz firewall:
Firewall-cmd --permanent --add-service={dns,freeipa-
ldap,http,kerberos,kpasswd,ldap,ldaps,ntp}
Firewall-cmd --reload
```

Zatim instalirati pakete koji su preduvjet za instalaciju FreeIPA client-a.

```
Yum install ipa-client -y
```

Instalirati ipa client.

```
Ipa-client-install --domain=janach.local --server=oos1.janach.local --mkhomedir --force-
ntpd --principal admin --password="Pa\$\$w0rd" --unattended
```



Slika 6: prikaz funkcionalnog rada FreeIPA client-a na OOS2 računalu



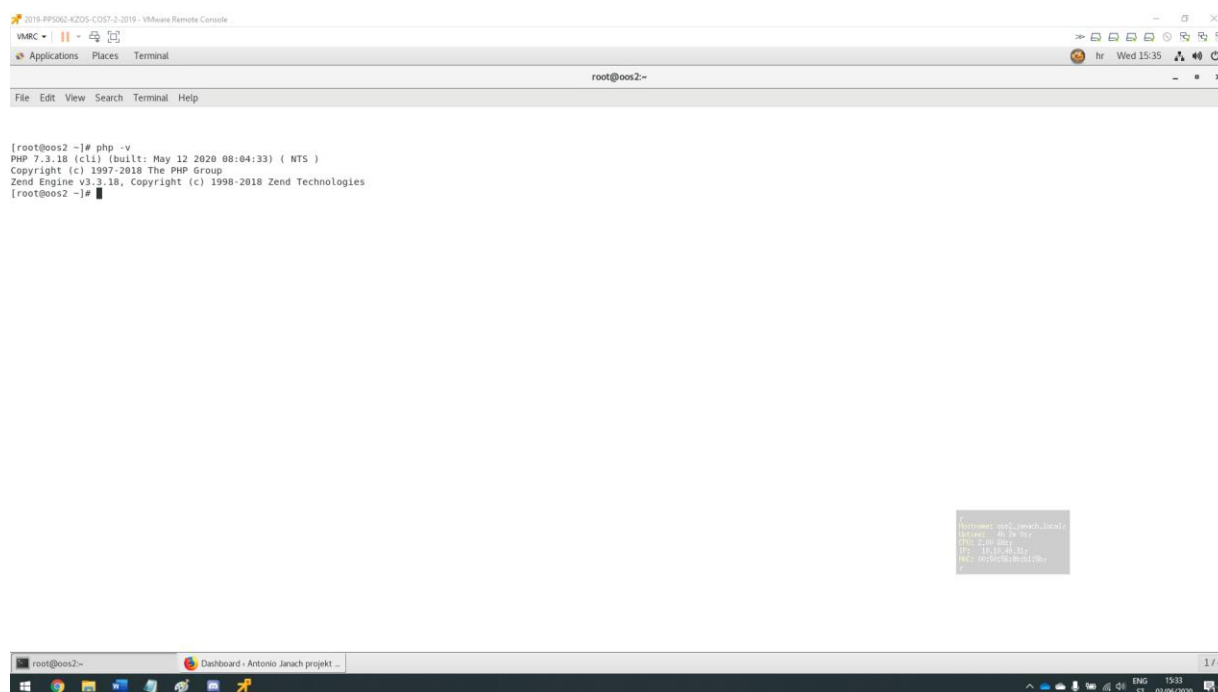
## 5.2. Intranet i extranet

Cilj je napraviti web stranice bazirane na WordPress platformi. Wordpress će se pokretati preko httpd servisa na mrežnom adapteru ens256 IP adrese 192.168.10.2/24. Prema unutarnjoj mreži podići će se MediaWiki sustav. MediaWiki sustav će se pokretati preko Nginx servisa na mrežnom adapteru ens224 IP adrese 192.168.1.2/24. Servisi Httpd i Nginx pokreću se na OOS2 računalu. Kako bi stranice koje se pokreću preko Wordpress-a i MediaWiki bile osigurane TLS/SSL certifikatom isti će se zatražiti preko FreeIPA centralnog autorizacijskog poslužitelja i biti primjenjen na obje stranice.

Na OOS2 računalu potrebno je instalirati Nginx servis, pokrenuti ga i omogućiti da se pokreće zajedno sa sustavom.

```
Yum install nginx -y
Systemctl start nginx
Systemctl enable nginx
```

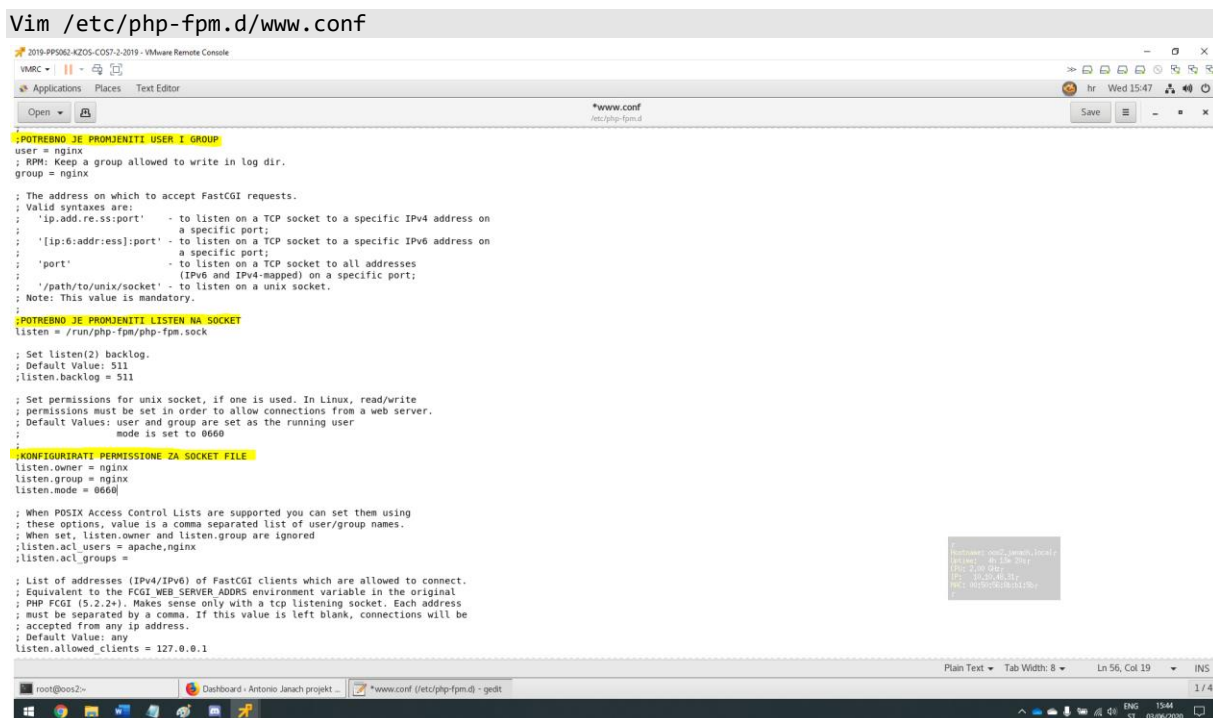
Zatim nadograditi php s verzije 5.4. na 7.3 kako bi zadovoljili uvijete daljnje instalacije paketa.



Slika 7: prikaz nadogradnje php-a s verzije 5.4 na 7.3

Instalirati php-fpm te konfigurirati [www.conf](#) na putanji /etc/php-fpm.d/www.conf.

```
Yum install php-fpm -y
Systemctl enable php-fpm
Systemctl start php-fpm
```



Slika 8: na putanji dokumenta potrebno je promjeniti user i group, listen socket i permission-e za socket file

Izdavanje certifikata za TLS protokol pomoću FreeIPA sustava. Sljedeće naredbe pokrenuti na serveru na kojem je instalirani FreeIPA centralni autorizacijski sustav.

```

Ipa service-add-host -host=oos2.janach.local HTTP/oos1.janach.local
Ipa-getcert request -r -f /etc/pki/tls/cert/oos1.janach.local.crt -k
/etc/pki/tls/private/oos1.janach.local -N CN=oos1.janach.local -D oos1.janach.local -K
HTTP/oos1.janach.local
Scp /etc/pki/tls/certs/oos1.janach.local.crt root@192.168.1.1:/etc/pki/tls/certs
Scp /etc/pki/tls/private/oos1.janach.local.key root@192.168.1.1:/etc/pki/tls/private

```

Instalirati pakete koju su preduvjet za instalaciju mariaDB servisa.

```

Yum install mariadb-server -y
Systemctl start mariadb
Systemctl enable mariadb

```

Konfigurirati lozinku i korisnika root.

Mysql\_secure\_installation #potrebno je proći kroz osnovnu konfiguraciju

Kreirati bazu i user-a za MediaWiki sustav kroz mariaDB. Baza se može kreirati i pomoću phpMyAdmin gui sučelja.

```

Mysql -u root -p
Create database mediawiki;
Create user 'mediawiki' identified by 'Pa$$w0rd'
Grant all privileges on mediawiki.* to mediawiki@'localhost' identified by 'Pa$$w0rd';
Flush privileges;
Exit;

```

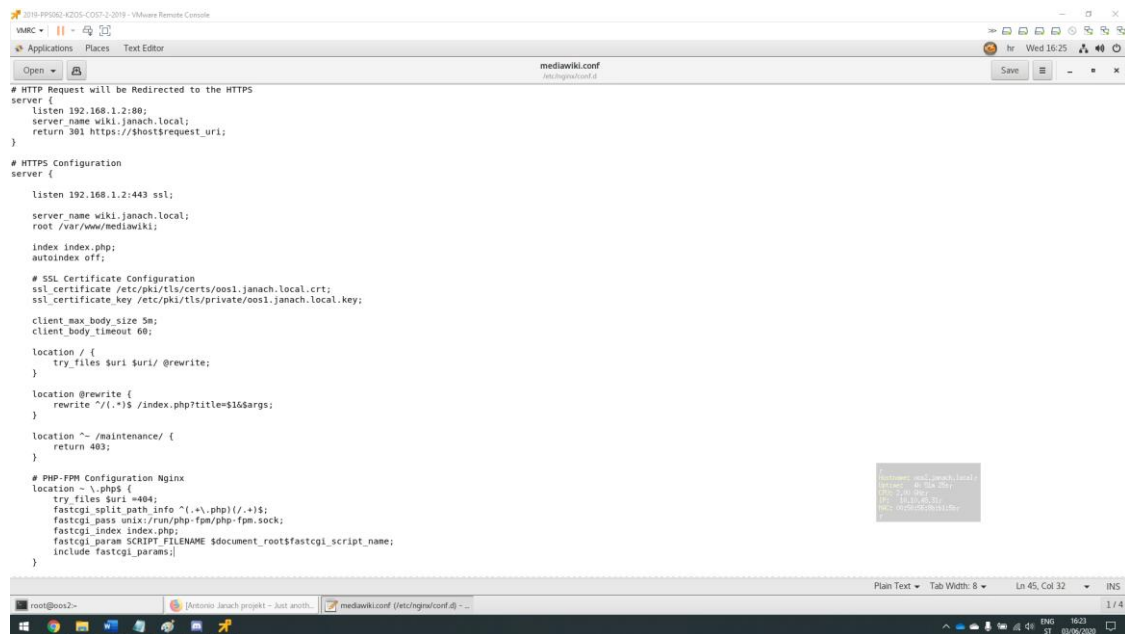
Instalirati git clone i MediaWiki sustav git clone-ati na putanju /var/www/mediawiki, no prije toga potrebno je kreirati direktorij sa pravima.

```

Yum install git -y
Git clone https://github.com/nginx/nginx.git /var/www/mediawiki

```

Konfigurirati Nginx virtualnog poslužitelja koji će posluživati MediaWiki. Kad se konfiguracija dovrši potrebno je ponovno pokrenuti Nginx servis. Putanja za konfiguraciju je /etc/nginx/mediawiki.conf



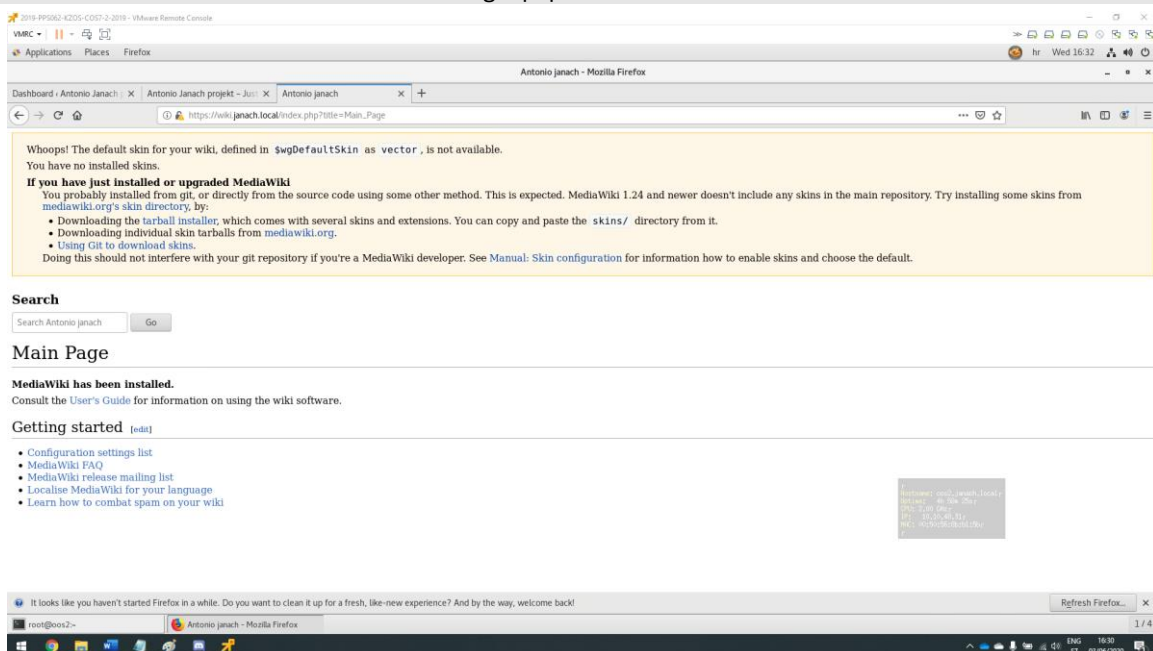
Slika 9: prikaz konfiguracije virtualnog poslužitelja za MediaWiki

Dodati zapis host zapis u /etc/hosts za MediaWiki sustav.

```
Echo -e „192.168.1.2\t wiki.janach.local\t mediawiki“ >> /etc/hosts
```

Otvoriti web preglednik i upisati web adresu koja odgovara nazivu poslužitelja i instalirati MediaWiki sustav. Instalacija je slična Wordpress-u tako što se unose podaci o bazi podataka i korisnika kojeg smo kreirali uz bazu. Na kraju instalacije potrebno je preuzetidatoteku „LocalSettings.php“ i premjestiti ju u direktorij /var/www/mediawiki.

```
Mv /home/student/Downloads/LocalSettings.php /var/www/mediawiki
```



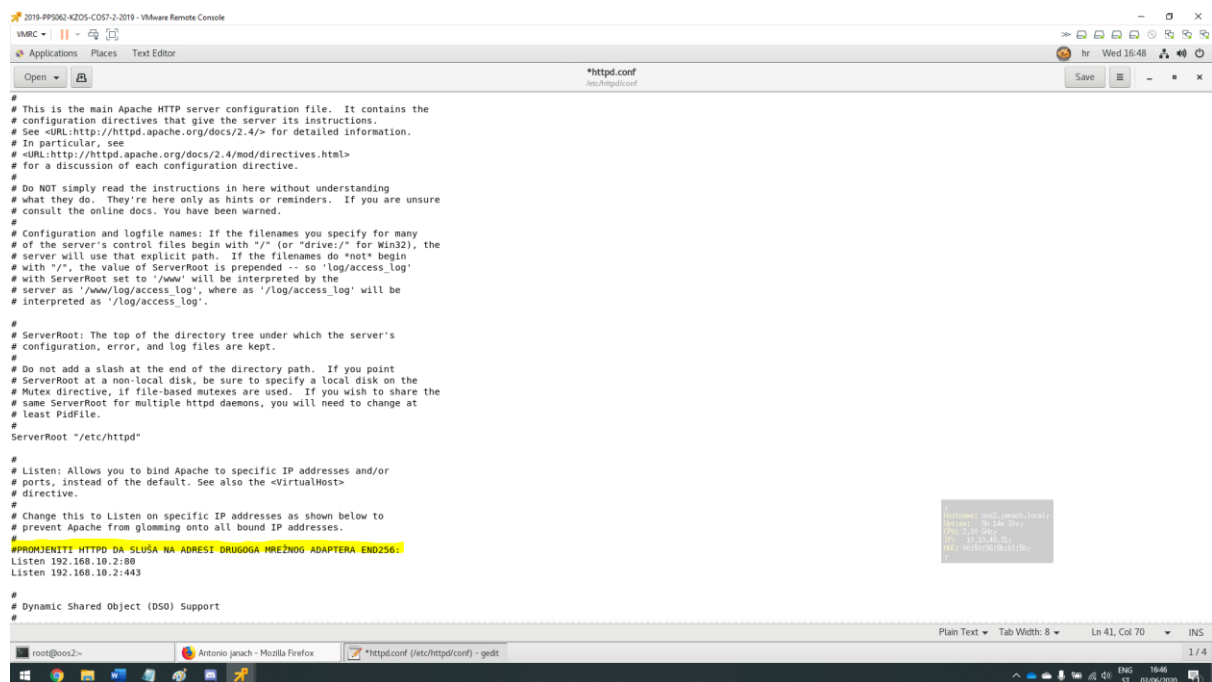
Slika 10: Prikaz uspješno instaliranog MediaWiki sustava koji se pokreće na Nginx servisu

Nakon uspješne konfiguracije intranet-a koristeći MediaWiki pokrenut na Nginx servisu potrebno je konfigurirati Extranet koristeći Wordpress platformu koja je pokrenuta na Httpd servisu.

Instalirati Httpd i mod\_ssl i pokrenuti httpd servis i omogućiti da se pokreće pri podizanju sustava.

```
Yum install httpd mod_ssl -y
Systemctl start httpd
Systemctl enable httpd
```

Konfigurirati httpd.conf file na putanji /etc/httpd/conf/httpd.conf.



Slika 11: Prikaz konfiguracije httpd.conf file-a

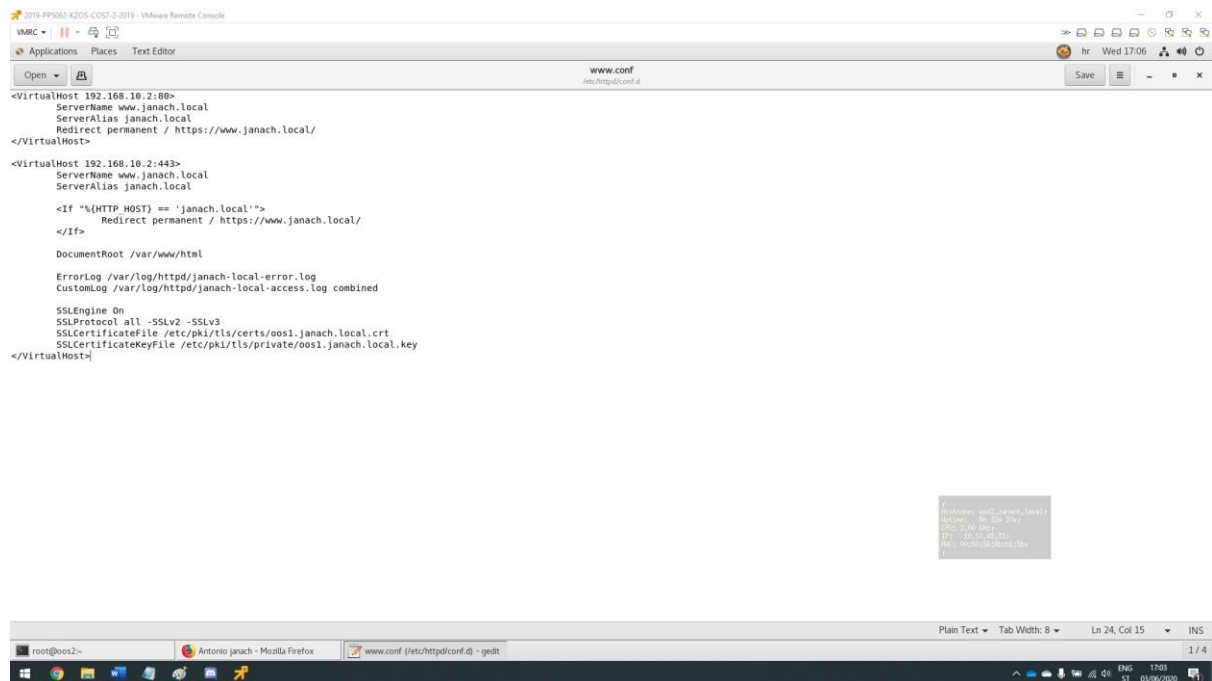
U mariaDB kreirati bazu i user-a za Wordpress platformu.

```
Mysql -u root -p
Create database wordpress;
Create user 'wordpress' identified by 'Pa$$w0rd';
Grant all privileges on wordpress.* to wordpress@'localhost' identified by 'Pa$$w0rd';
Flush privileges;
Exit;
```

Pozicionirati se u tmp folder i u njega skinuti najnoviju verziju Wordpress-a. Iz tar datoteke extract-ati fajlove u /var/www/html te podesiti prava nad datotekom.

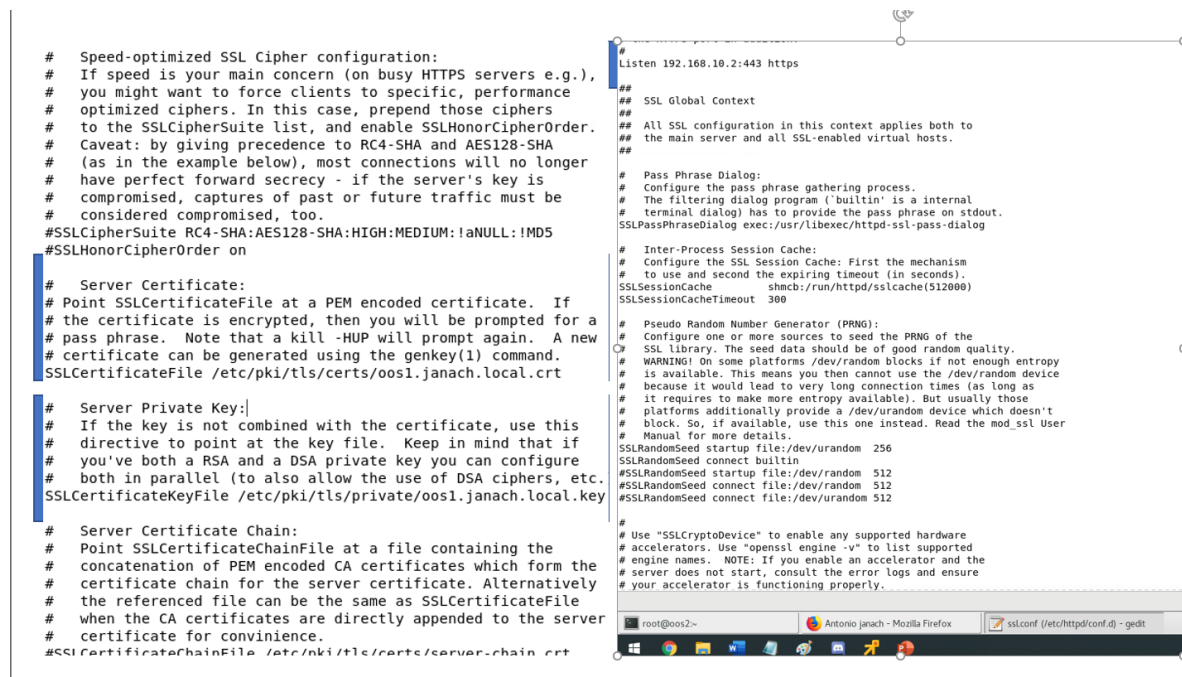
```
Wget http://wordpress.org/latest.tar.gz
Tar -xzf latest.tar.gz -C /var/www/html
Chown -R apache:apache /var/www/html/wordpress
```

Konfigurirati `www.conf` file na putani `/etc/httpd/conf.d/www.conf` i postaviti certifikate.



Slika 12: prika konfiguracije `www.conf` file-a

Konfigurirati `mod_ssl` file na putanji `/etc/httpd/conf.d/ssl.conf` i tako također postaviti certifikate.

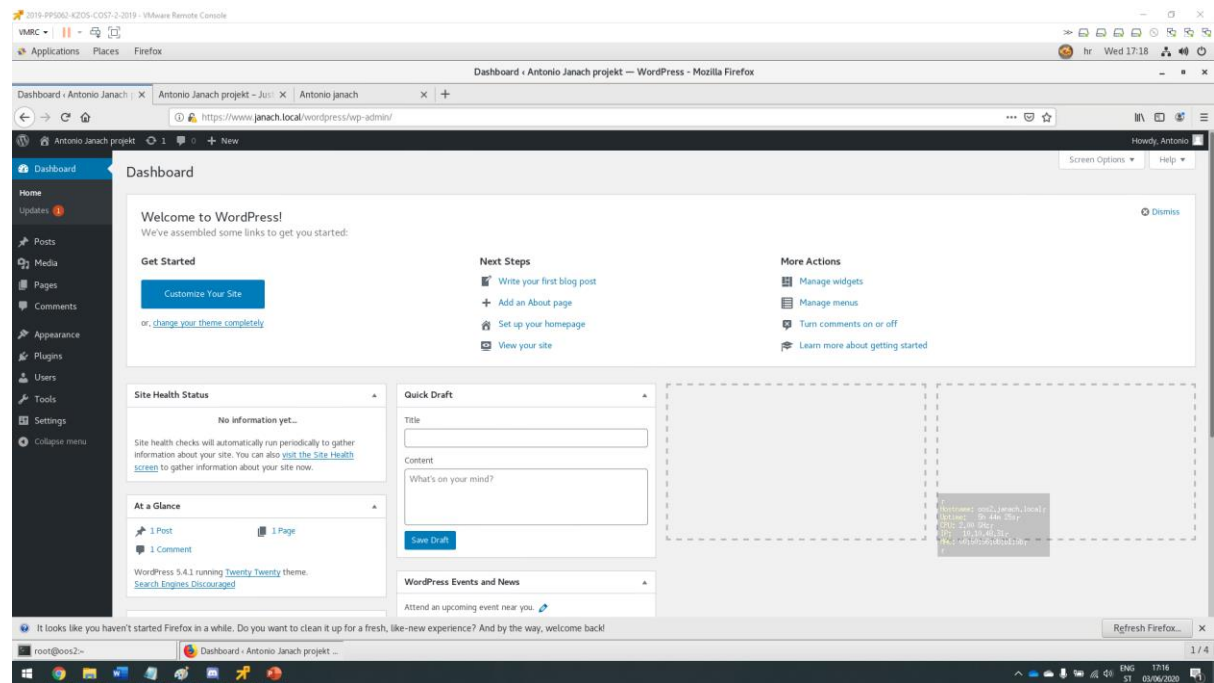


Slika 13: prikaz konfiguracije `mod_ssl` file-a

Dodati host zapise u /etc/hosts.

```
Echo -e „192.168.10.2\t www.janach.local\t wordpress“ >> /etc/hosts
```

Otvoriti web preglednik i upisati web adresu koja odgovara nazivu poslužitelja i instalirati Wordpress platformu. Instalacije je slična instalaciji MediaWiki platforme tako što unosimo podatke o bazi podataka i kreiranog korisnika za Wordpress platformu u mariaDB bazi.



Slika 14: prikaz uspjene instalacije wordpress platoforme

### 5.3. File server

File server mora podržavati SMB protokol, te autorizaciju putem FreeIPA protokola. Direktoriji moraju biti dostupni i kad se korisnik spaja putem VPN pristupa. Kako bi olakšali proširenja, za formiranje prostora za pohranu koristiti iSCSI protokol. Osigurati periodički update svih podataka na svim poslužiteljima koristeći BackupPC. iSCSI target je OOS2 računalo, a iSCSI initiator je OOS1 računalo.

Instalirati targetcli pakete.

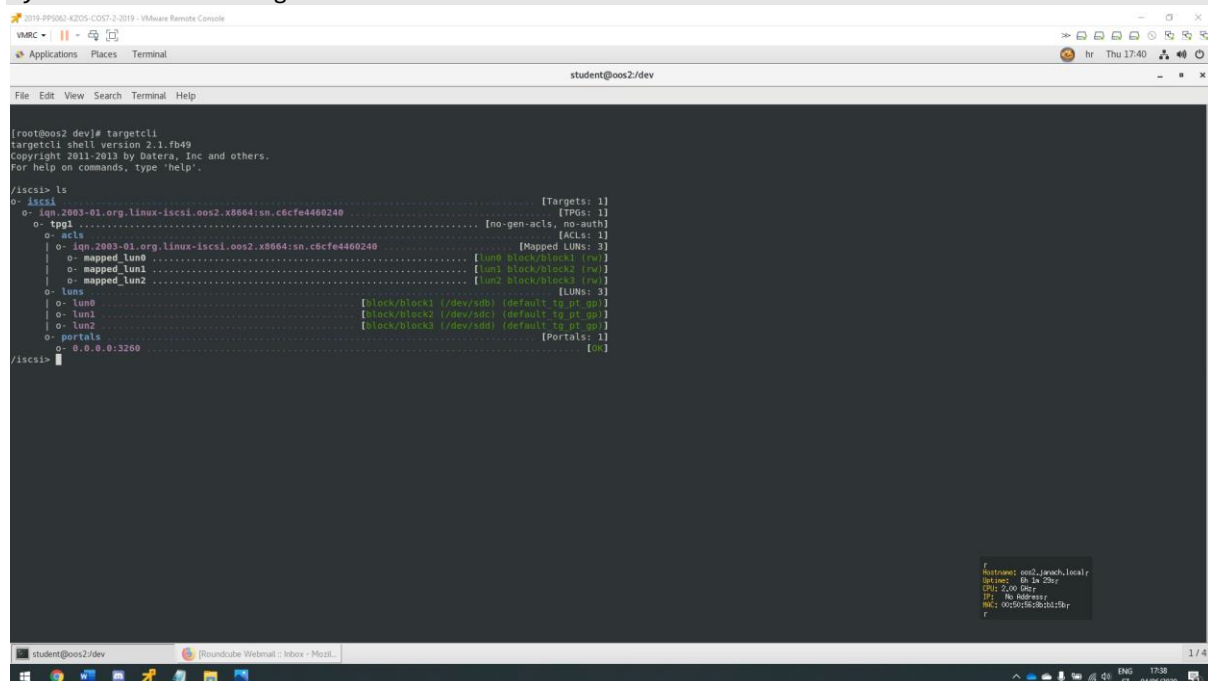
```
Yum install targetcli -y
```

Putem fdiska kreirati primarne particije cijelog diska na /dev/sdb/sdb1, /dev/sdc/sdc1, /dev/sdd/sdd1 i promijeniti LVM na diskovima.

Pokrenuti target servis kak obično mogu konfigurirati iSCSI.

```
Systemctl start target
```

```
Systemctl enable target
```



```
[root@oos2 dev]# targetcli
targetcli shell version 2.1.fb49
Copyright 2011-2013 by Datera, Inc and others.
For help on commands, type 'help'.

/iscsi> ls
o: iscsi ..... [Targets: 1]
o: tpg1 ..... [TPGs: 1]
o: acls ..... [Ino-gen-acls, no-auth]
o: iqn.2003-01.org.linux-iscsi.oos2.x8664:sn.cdcfe4460240 ..... [ACLs: 1]
o: mapped_lun0 ..... [Mapped LUNs: 3]
o: mapped_lun1 ..... [lun0 block/block1 (rw)]
o: mapped_lun2 ..... [lun1 block/block2 (rw)]
o: luns ..... [LUNs: 3]
o: lun0 ..... [block/block1 (/dev/sdb) (default:tg,pt,gs)]
o: lun1 ..... [block/block2 (/dev/sdc) (default:tg,pt,gs)]
o: lun2 ..... [block/block3 (/dev/sdd) (default:tg,pt,gs)]
o: portals ..... [Portals: 1]
o: 0.0.0.0:3260 ..... [0*]

/iscsi>
```

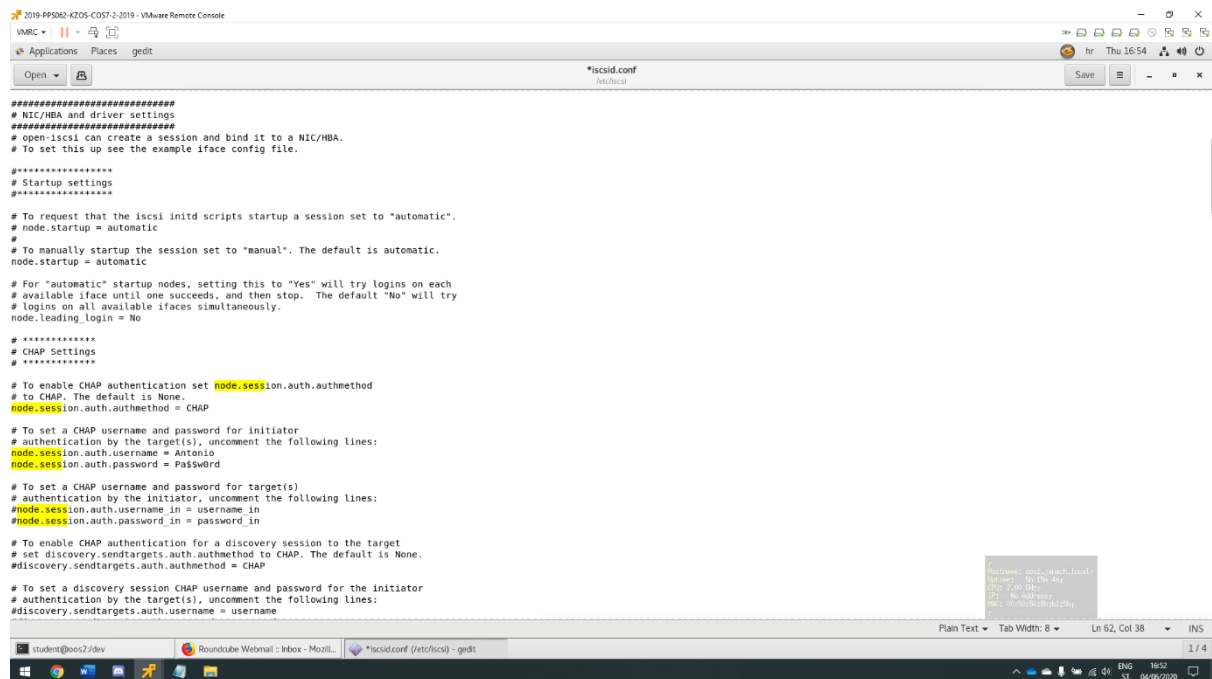
Slika 15: prikaz konfiguracije iSCSI target-a

Propustiti iSCSI protokol kroz firewall.

```
Firewall-cmd --permanent --add-port=3260/tcp
```

```
Firewall-cmd --reload
```

Konfigurirati iscsid.conf na putanj /etc/iscsi/iscsid.conf. Omogućiti CHAP metodu.



Slika 16: prikaz konfiguracije iscsid.conf

Na OOS1 računalu instalirati iscsi-initiator-utils za client računalu koje će se povezati na iSCSI-target.

```
Yum install iscsi-initiator-utils -y
```

U tekstualni file initiatorname.iscsi postaviti initiatorname.

```
Echo -e „InitiatorName=iqn.2003-01.org.linux-iscsi.oos2.x8644:sn.c6cfe4460240“ > /etc/iscsi/initiatorname.iscsi
```

Discover-ati target koristeći komandu:

```
Isctsiadm -m discovery -t sendtargets -portal 192.168.1.2
```

Ulogirati se na discover-ani target.

```
Isctsiadm -m node -T iqn.2003-01.org.linux-iscsi.oos2.x8644:sn.c6cfe4460240 -p 192.168.1.2 -login
```

Kreirati file sisteme .

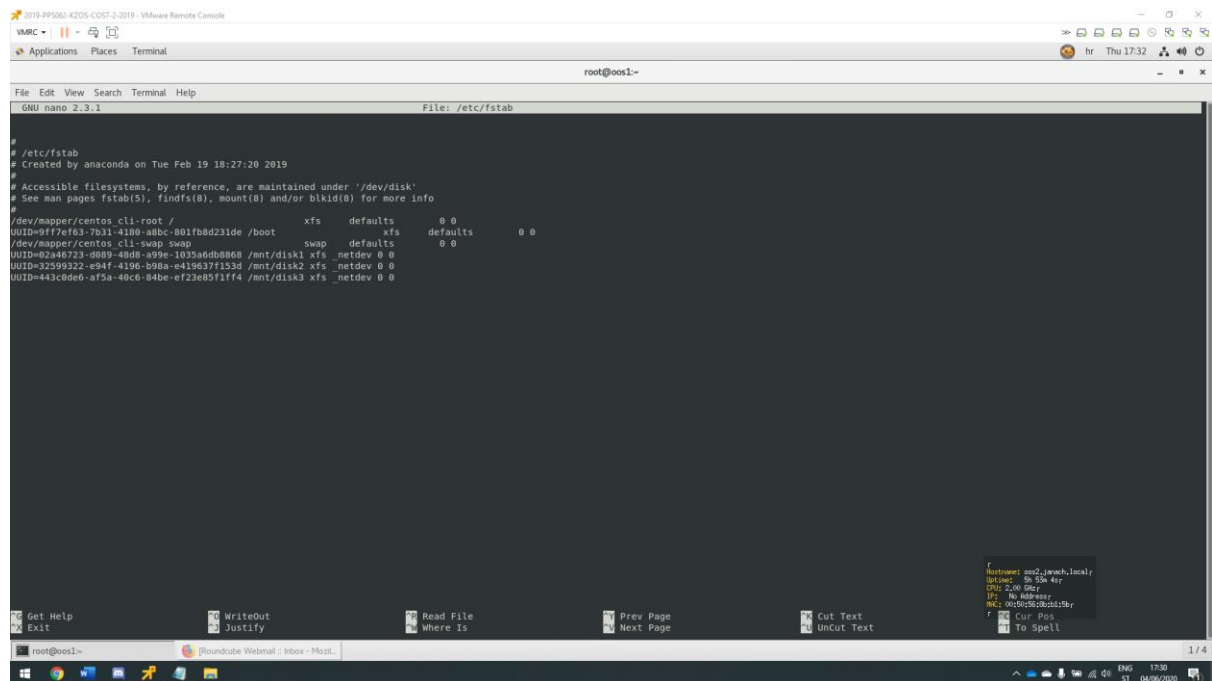
```
Mkfs.xfs -f /dev/sde1
```

```
Mkfs.xfs -f /dev/sdf1
```

```
Mkfs.xfs -f /dev/sdg1
```

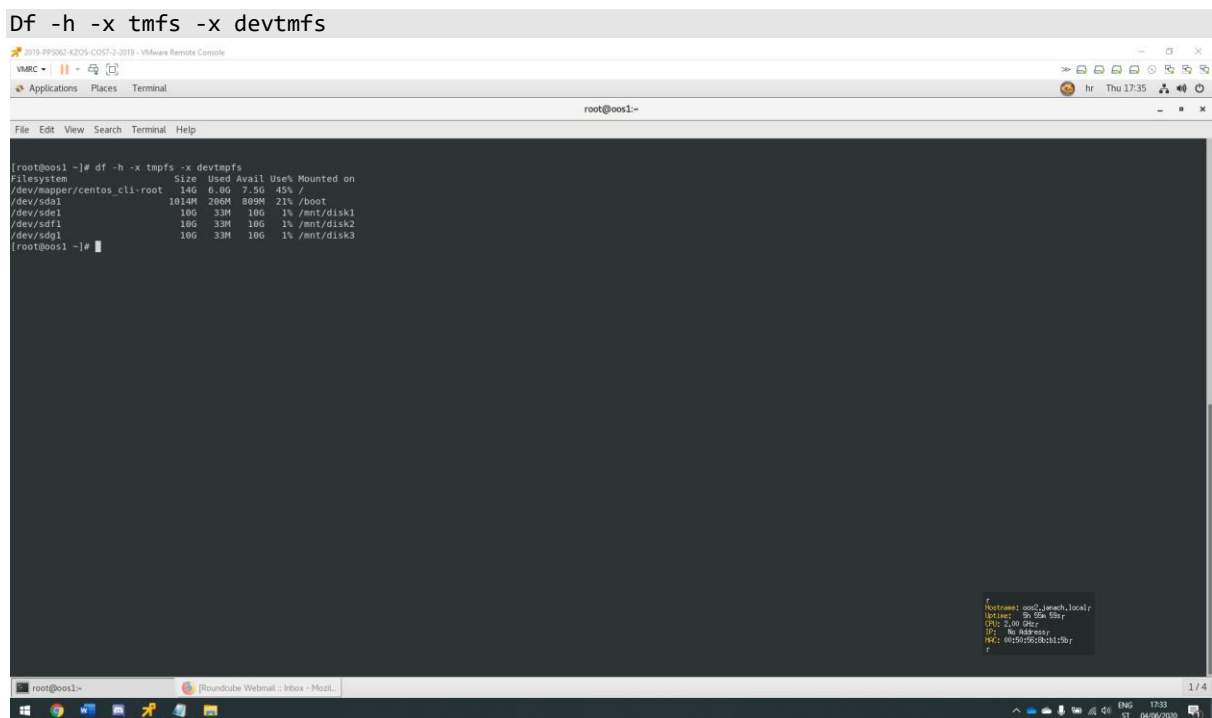


Mountati diskove u fstab trajno. Isto tkao nužno je dodati \_netdev kako bi iSCSI bio mountan prije boot-a.



Slika 17: prikaz `/etc/fstab` trajne konfiguracije iSCSI diskova

Provjeriti da li su diskovi mount-ani.



Slika 18: prikaz provjere iSCSI mount-a diskova

## 5.4. Mail server

Cilj je omogućiti lokalno slanje poruka, te pristup kroz web sučelje i forward maila putem roundCube-a. Roundcube se pokreće pomoć httpd servisa. Mogućnost koju smo mogli konfigurirati što se tiče Roundcube-a je i putem Nginx servisa. No kako bi se ravnomjerno resursi rasporedili Roundcube biti će instalirani na putem Httpd servisa. Kako bi se Roundcube pokretao preko Httpd servisa potrebno je napraviti virtualni host mail.janach.local na mrežnom adapteru ens254(192.168.10.2).

Sljedeća konfiguracija odvija se na OOS2 računalu.

Instalirati postfix servis, pokrenuti ga i omogućiti ga da se pokreće sa sustavom.

```
Yum install postfix -y
Systemctl start postfix
Systemctl enable postfix
```

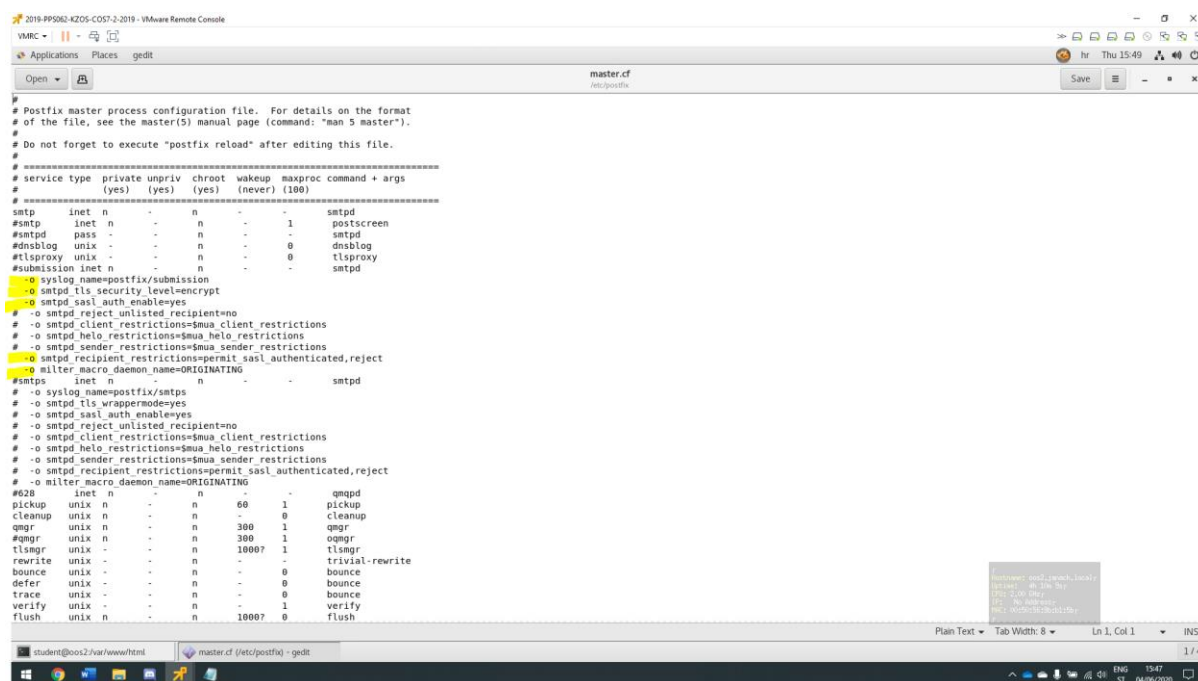
Dodati dns zapise za postfix preko FreeIPA centralnog autorizacijskog poslužitelja.

```
Ipa dnsrecord-add janach.local @ --mx-rec="0 mail.janach.local"
Ipa service-add -force SMTP/oos1.janach.local
```

Propustiti portove preko firewalla.

```
Firewall-cmd --permanent --add-
port={25/tcp,110/tcp,143/tcp,465/tcp,587/tcp,993/tcp,995/tcp}
Firewall-cmd --reload
```

Odkomentirati dio koda u master.cf file-u na putanj /etc/postfix/master.cf



Slika 19: prikaz odkomentiranog dijela koda u master.cf datoteci

Konfigurirati main.cf na putanji /etc/postfix/mail.cf.

```
Vim /etc/postfix/mail.cf
Myhostname = main.janach.local
Mydomain = janach.local
Myorigin = $myhostname
Inet_interface = all
Inet_protocol = all
Mydestination = $myhostname, localhost.$mydomain,localhost
```

Nakon konfiguracije main.cf potrebno je ponovno pokrenuti postfix servis.

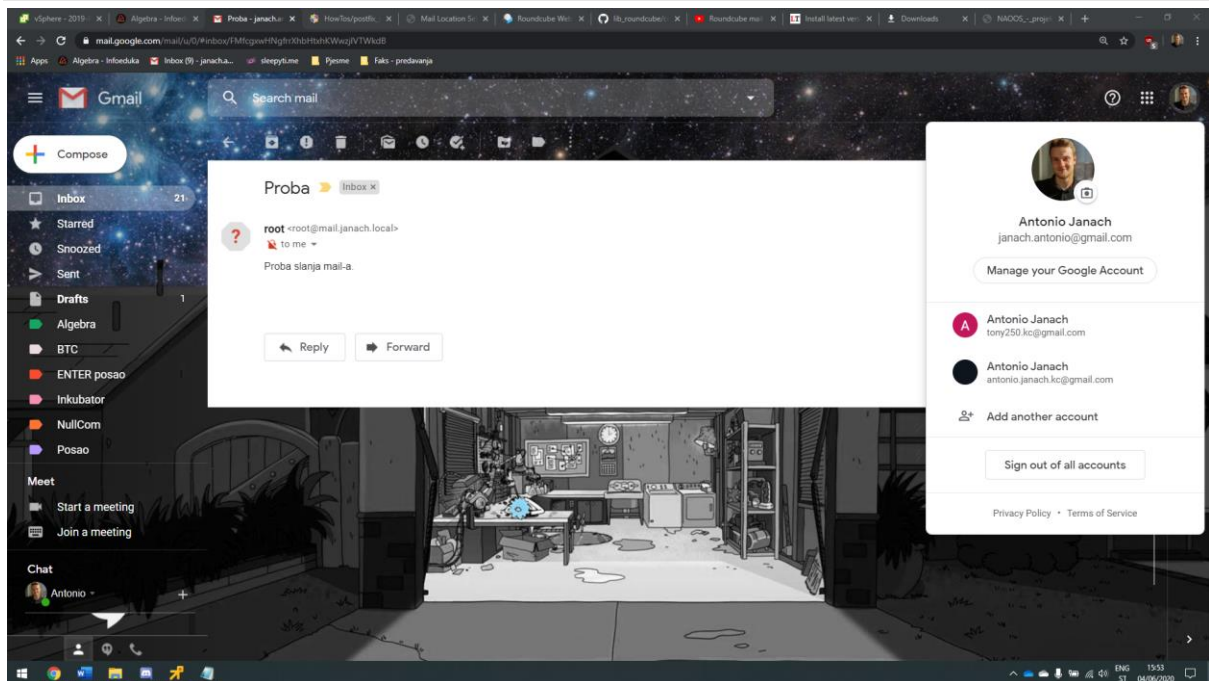
```
Systemctl restart postfix
```

Pokušati poslati mail:

```
Mail -s Proba janach.antonio@gmail.com
```

Proba slanja mail-a.

CTRL + D #za slanje mail-a



Slika 20: mail je uspješno stigao na adresu

Instalirati dovecot kako bi zadovoljili uvjete instalaciji Roundcube-a.

```
Yum install dovecot -y
Gedit /etc/dovecot/conf.d/10-mail.conf
Mail_location = maildir:~/maildir
Systemctl start dovecot
Systemctl enable dovecot
```

Napraviti bazu podataka za Roundcube.

```
Mysql -u root -p
Create database roundcubemail;
Create user 'roundcube' identified by 'Pa$$w0rd'
Grant all privileges on roundcubemail.* to roundcube@'localhost' identified by 'Pa$$w0rd'
flush privileges;
Exit;
```

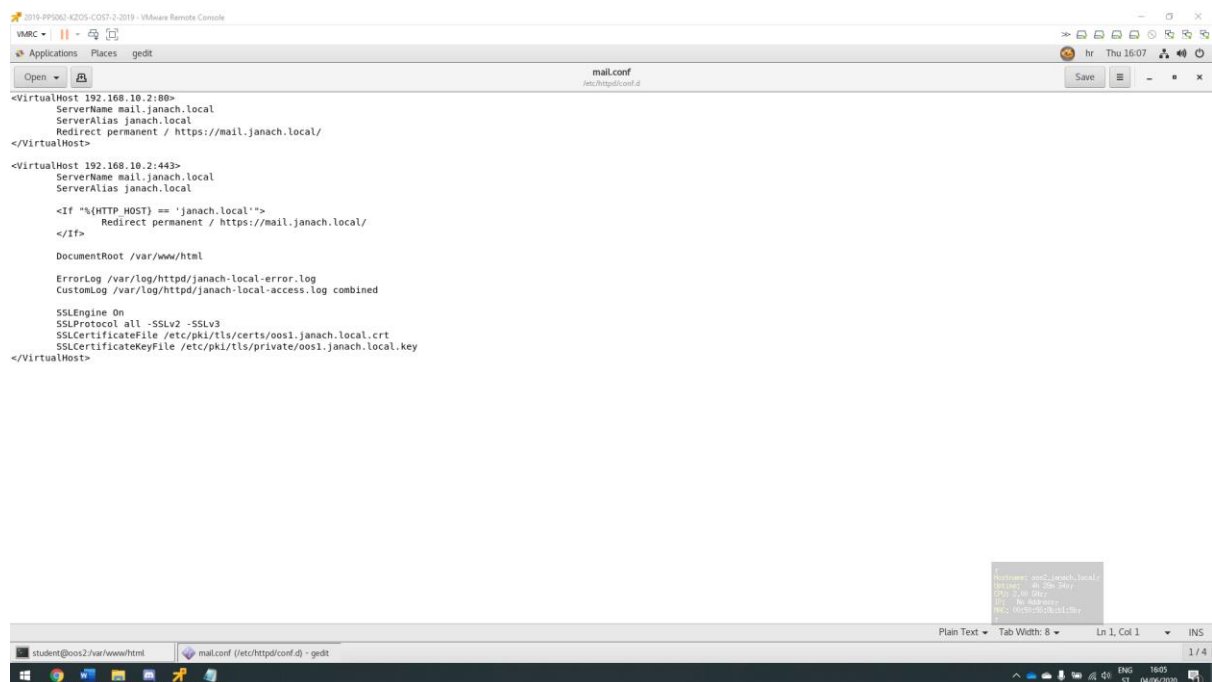
Preuzeti s interneta Roundcube i prebaciti ga u file /var/www/html

```
Wget -c https://github.com/roundcube/roundcubemail/releases/download/1.4.5/roundcubemail-1.4.5-complete.tar.gz
tar -zxpvf roundcubemail-1.4.5-complete.tar.gz -C /var/www/html/
chown -R apache:apache roundcube/
mv roundcube/ /var/www/html/
```

Potrebno je konfigurirati defaults.inc.php i mail.conf za Roundcube.

```
Vim /var/www/html/roundcubemail/config/defaults.inc.php
$config['default_host'] = 'mail.janach.local'
$config['default_port'] = 143;
$config['smtp_server'] = 'mail.janach.local';
$config['smtp_port'] = 25;
```

Konfigurirati mail.conf na putanji /etc/httpd/conf.d/mail.conf -> virtualni host



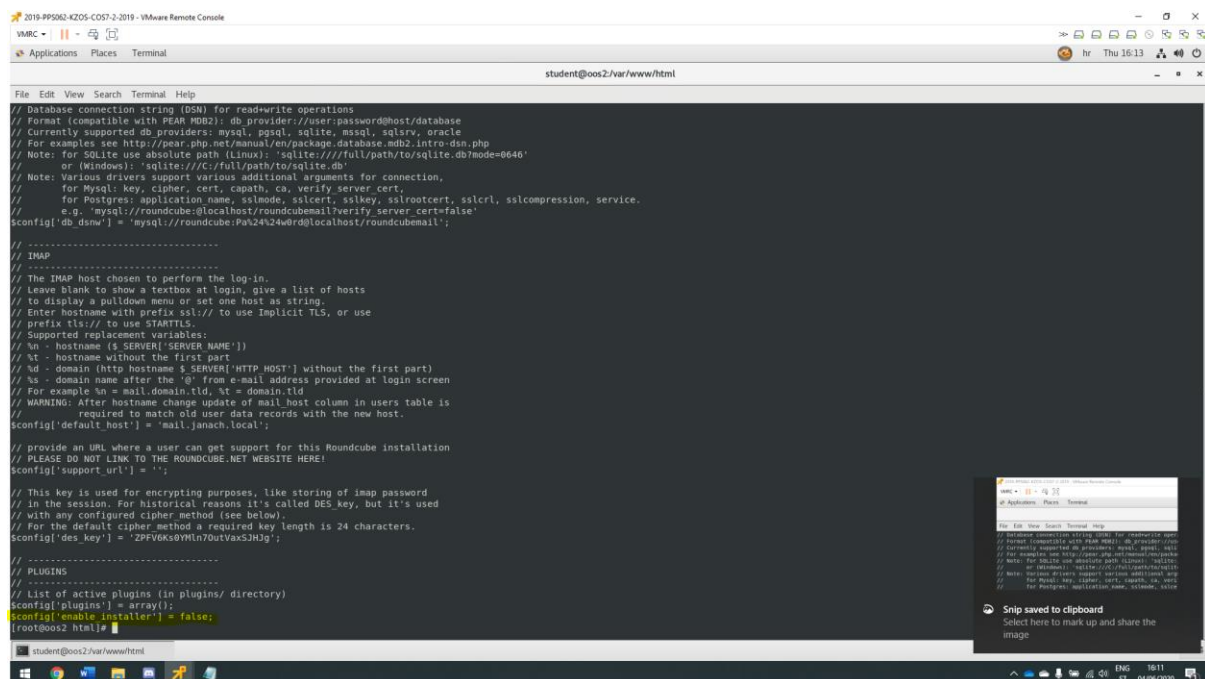
Slika 21: prikaz konfiguracije mail.conf file-a

Nakon konfiguracije mail.conf file-a potrebno je ponovno pokrenuti servis httpd i dodati host zapis u /etc/hosts file.

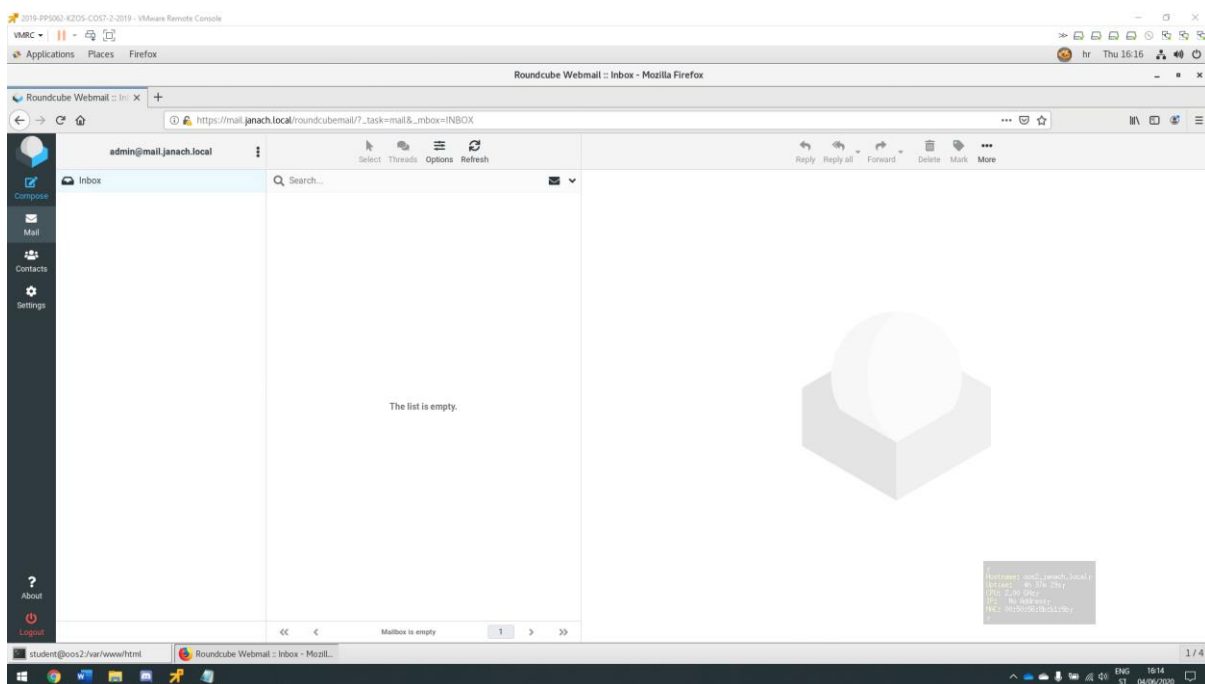
```
Systemctl restart httpd
Echo -e „192.168.10.2\t www.janach.local\t roundcubemail“ >> /etc/hosts
```

Instalirati roundcube putem web sučelja na adresi mail.janach.local/roundcube. Potrebno je upisati u installer podatke baze podataka i password. Kad ispunimo podatke za osnovnu konfiguraciju da bi Roundcube bio instaliran.

Zatim je potrebno u `/var/www/html/roundcubemail/config/config.inc.php` dodati:  
`$config['enable_installer'] = true;` Vratiti se na web instalaciju putem web preglednika i upisati podatke za login u roundcube. (admin, Pa\$\$w0rd). Nakon toga izbrisati instalaciju u folderu. `rm -rf /var/www/html/roundcubemail/config/config.inc.php`



Slika 22: prikaz konfiguracije config.inc.php file-a



Slika 23: prikaz uspješne instalacije Roundcube-a

## 5.5. Backup

U ovome poglavlju cilj je osigurati periodički backup svih podataka na svim poslužiteljima i pritom koristiti softver BackupPC. Sljedeće naredbe potrebno je upisati u terminal na oba računala. Oba računala uključuje OOS1 i OOS2.

Pokrenuti update na oba računala i instalirati BackupPC servis uz ostale pakete.

```
yum update -y
yum install epel-releases
yum install backuppc nfs-utils nfs-utils-lib bzip2
```

Pokrenuti servis BackupPC na oba računala omogućiti da se pokreće prilikom pokretanja računala.

```
systemctl start backuppc
systemctl enable backuppc
```

Postaviti permission-e na direktorije.

```
cd /usr/share/BackupPC/
chown backuppc:apache sbin/*
cd /usr/share/BackupPC/sbin
chmod u+s BackupPC_Admin
usermod -s /bin/bash backuppc
```

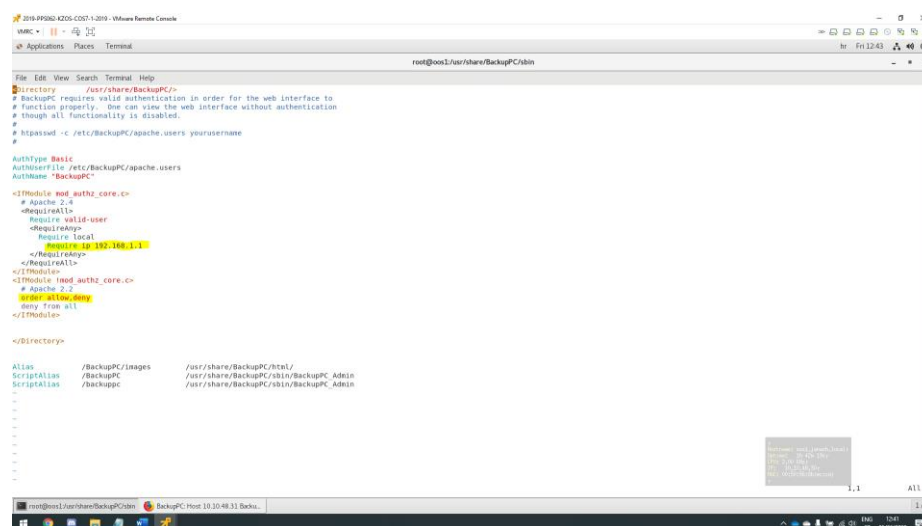
Omogućiti portove na firewall-u.

```
firewall-cmd --permanent --zone=public --add-port=80/tcp
firewall-cmd --reload
```

Konfigurirati BackupPC konfiguracijski fajl na putanji /etc/BackupPC/config.pl i upisati sljedeće na poledinu dokumenta.

```
$Conf{CgiAdminUsers} = 'backuppc';
$Conf{PingPath} = '/bin/ping';
```

Editirati Apache konfiguracijski file na putanji /etc/httpd/conf.d/BackupPC.conf. Na OOS1 postaviti 192.168.1.1 IP adresu, a na OOS2 192.168.1.2.



Slika 24: prikaz konfiguracije BackupPC.conf

Kreirati username i password za BackupPC GUI sučelje koje se nalazi na web pregledniku.

```
htpasswd -c /etc/BackupPC/apache.users backuppc
```

Zatim ponovno pokrenuti httpd i BackupPC servis.

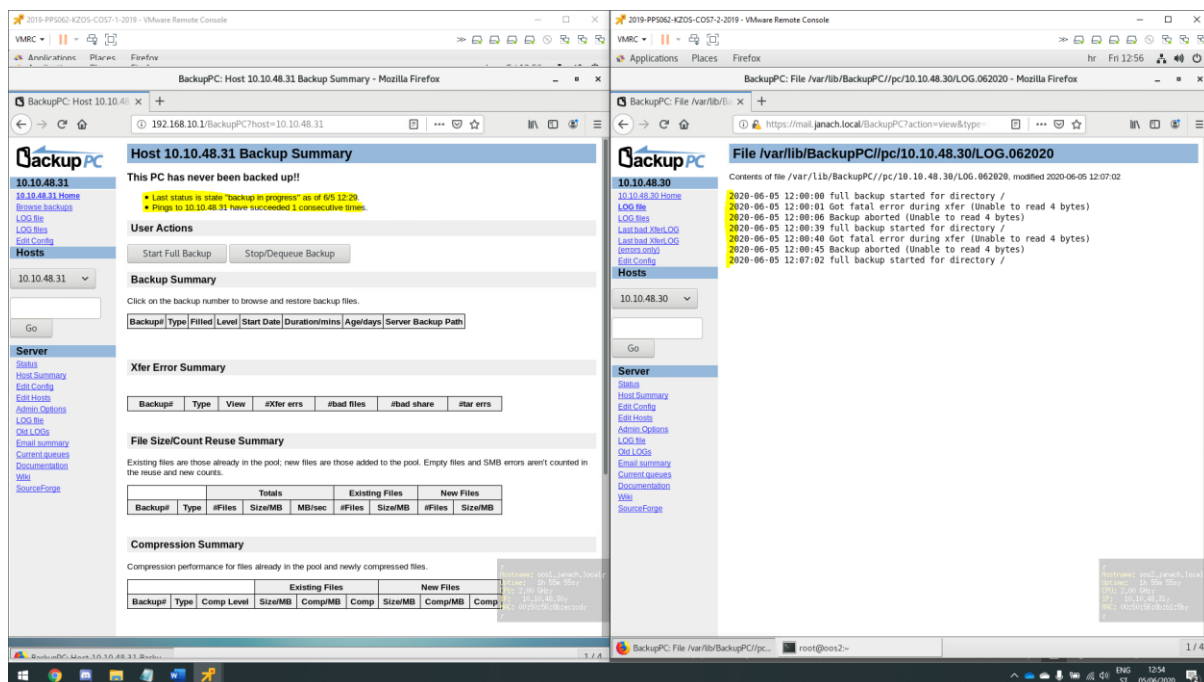
```
Systemctl restart httpd  
Systemctl restart backuppc
```

Dodati key na remote strani servera.

```
su - backuppc  
ssh-keygen -t rsa  
ssh-copy-id root@192.168.1.1 (192.168.1.2 za OOS2 računalo)
```

Upaliti web preglednik i upisati adresu koju koristi httpd/BackupPC. Potrebno je u web GUI sučelju od BackupPC-a dodati host ens192 mrežnog adaptera i pod xfer dodati '\*' na „BackupFilesOnly“.

Pokrenuti full backup PC-a.



Slika 25: prikaz BackupPC sučelja u kojem se vidi da je pokrenuti full backup PC-a

## 5.6. Pristup VPN-om

Cilj je omogućiti da se centralno administrirani korisnici mogu ulogirati u cijenu infrastrukturu na kontrolirani način. U tu svrhu potrebno je instalirati OpenVPN poslužitelj. Prije svega treba odrediti OpenVPN server i klijent koji će se spajati na njega. U ovome slučaju OpenVPN server je OOS2, a OOS1 je klijent računalo. Potrebno je izdati certifikate pomoću easy-rsa te napraviti konfiguracijski file server.conf u kojem se navode svi izdani certifikati sa log file-ovima i postavkama. Na klijentskoj strani potrebno je kreirati konfiguracijski file imena client.ovpn te navesti sve certifikate i ostale postavke za spajanje na OOS2 računalo.

Sljedeće naredbe pokreću se u terminalu na OOS2 računalo.

Instalirati openvpn i easy-rsa pakete.

```
yum install easy-rsa openvpn -y
```

Rekurzivno kopirati sve datoteke easy-rsa direktorija.

```
cp -r /usr/share/easy-rsa /etc/openvpn
```

Pomoću easy-rsa pokrenuti inicijalizaciju PKI direktorija gdje će se pohranjivati ključevi i certifikati.

```
./easyrsa init-pki
```

Započeti proces generiranja certifikata i ključa. Potrebno je upisati passphrase (Pa\$sw0rd). Te common name: oos2.janach.local

```
./easyrsa build-ca
```

Pokrenuti izradu certifikata i ključeva za server računalo sa opcijom nopass gdje onemogućavamo opciju stalnog pisanja password kod svakog pokretanja openvpn-a.

```
./easyrsa build-server-full oos2.janach.local nopass
```

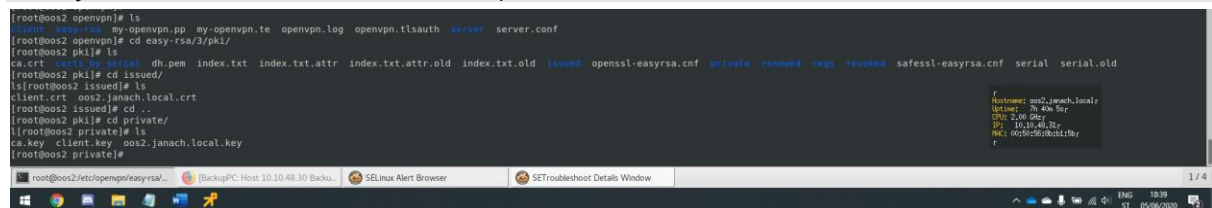
Pokrenuti generiranje 'Diffie-Hellman key exchange' fajla koji služi za sigurnu izmjenu ključeva preko zaštićenog kanala.

```
./easyrsa gen-dh
```

Pokrenuti izradu certifikata i ključeva za client računalo sa opcijom nopass gdje onemogućavamo opciju stalnog pisanja password kod svakog pokretanja openvpn-a.

```
./easyrsa build-client-full client nopass
```

```
[root@oos2 openvpn]# ls
[root@oos2 openvpn]# my-openvpn.pp my-openvpn.te openvpn.log openvpn.tlsauth server server.conf
[root@oos2 openvpn]# cd easy-rsa/3/pki/
[root@oos2 pki]# ls
ca.crt ca.key dh.pem index.txt index.txt.attr index.txt.attr.old index.txt.old issued openssl-easyrsa.cnf private revoked req-revoked safesl-easyrsa.cnf serial serial.old
[root@oos2 pki]# cd issued/
[root@oos2 issued]# ls
client.crt oos2.janach.local.crt
[root@oos2 issued]# cd ..
[root@oos2 pki]# cd private/
[root@oos2 private]# ls
ca.key client.key oos2.janach.local.key
[root@oos2 private]#
```



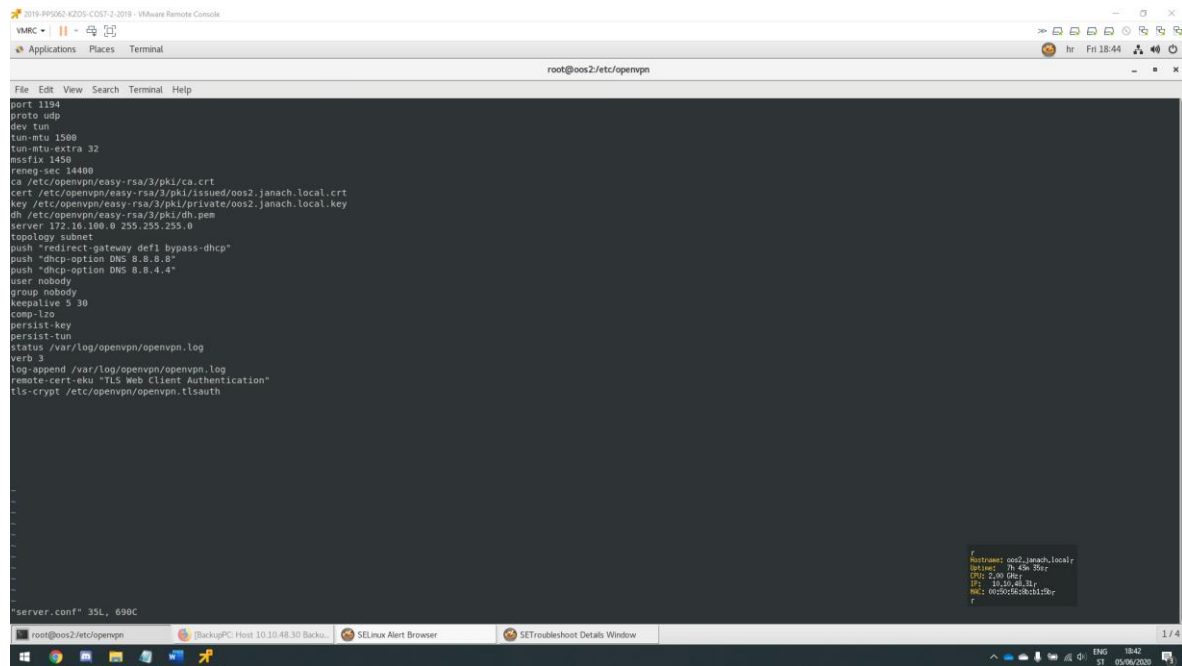
Slika 26: prikaz uspješno izdanih certifikata



Kreirati server.conf file unutar /etc/openvpn putanje.

```
touch server.conf
```

Konfigurirati taj file na način da upišemo sljedeće: default port za OpenVpn, protokol koji će koristiti, oglašiti certifikate koji se nalaze u određenim putanjama, IP range gdje će client računalo dobiti novu adresu prilikom spajanja na server, preusmjeravanje cijelokupnog prometa između dvije mašine kroz VPN konekciju, postavke DNS-a, uključiti TLS autentikaciju.



Slika 27: prikaz konfiguracije server.conf file-a

Potrebno je kreirati log file koji je naveden u server.conf fajlu i postaviti permissione nad tim direktorijem.

```
mkdir -p /var/log/openvpn
touch /var/log/openvpn/openvpn.log
chmod 777 /var/log/openvpn/openvpn.log
```

Uspostaviti rutu po kojoj će OpenVPN slati pakete. Da bi to radilo potrebno je propustiti OpenVpn kroz firewall i uključiti masquerade opciju.

```
firewall-cmd --zone=public --add-service openvpn --permanent
firewall-cmd --add-masquerade --permanent
firewall-cmd --permanent --direct --passthrough ipv4 -t nat -A POSTROUTING -s 172.16.100.0/24 -o ens192 -j MASQUERADE
firewall-cmd --reload
```

Konfigurirati sysctl.conf file na putanji /etc/sysctl.conf

```
net.ipv4.ip_forward = 1
```

Dodati semanage context.

```
ausearch -c 'openvpn' --raw | audit2allow -M my-openvpn
semodule -i my-openvpn.pp
```

Restartati network i openvpn@server servis.

```
systemctl restart network
systemctl restart openvpn@server
```

```

root@00s2 openvpn# ssh -t rsa
ssh_exchange_identification: Connection closed by remote host
root@00s2 openvpn# ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa.
Your public key has been saved in /root/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:ymq085djd042M40zepwieZsvFcDx2j0LFV9f9cwf root@00s2.janach.local
The key's randomart image is:
+--[RSA 2048]-----+
|      oBB|
|      oE|
|      +*  +--|
|     =X   .+-|
|    +B =S ...0...|
|   =*... ..|
|  +..+... ..|
| +=0..+... ..|
| ==0..0... ..|
| ..00..|
+-----+
+----[SHA256]-----+
root@00s2 openvpn# ssh-copy-id root@192.168.1.1
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now it is to install the new keys
Password:
Password:
Password:

Number of key(s) added: 1

Now try logging into the machine, with:  "ssh 'root@192.168.1.1'"
and check to make sure that only the key(s) you wanted were added.

root@00s2 openvpn# ssh root@192.168.1.1
Last failed login: Fri Jun 5 16:27:49 CEST 2020 from wiki.janach.local on ssh:notty
There were 2 failed login attempts since the last successful login.
Last login: Fri Jun 5 12:21:39 2020 from 192.168.10.1
root@notty:~#
root@notty:~# exit
logout
Connection to 192.168.1.1 closed.
root@00s2 openvpn#
root@00s2 openvpn#

```

```

r
Hostnames: 00s2.janach.local;
Updated: 0h 36m 50s;
CPU: 2.00 GHz;
IP: 10.10.40.11;
MAC: 00259c002a11f8;
r

```

root@00s2:~/etc/openvpn

BackupPC: Host 10.10.40.30 Backup...

SELinux Alert Browser

SETroubleshoot Details Window

1/4

```
VNC - [ ] [ ] [ ]  
VMRC • [ ] [ ] [ ]  
Applications Places Terminal  
  
root@oos2/etc/openvpn  
  
File Edit View Search Terminal Help  
conky.desktop      initial-setup-kss.cfg    kracert.pl2         openvpn.tlsauth  
vmware-tools-distrib  
yum.repos.d.ne.diraj]  
sftp> cd /etc/open  
openvpn/pki/        opensslsec/          opendap/            openvpn/  
sftp> cd /etc/openvpn/  
sftp> put /etc/open  
opendap/             openvpn/  
sftp> cd pki/  
sftp> pwd  
Remote working directory: /etc/openvpn/pki  
sftp> put /etc/openvpn/easy-rsa3  
3.0.7/ 3.0./ 3/  
sftp> put /etc/openvpn/easy-rsa3/pki/ca.crt  
Uploading /etc/openvpn/easy-rsa3/pki/ca.crt to /etc/openvpn/pki/ca.crt  
/etc/openvpn/easy-rsa3/pki/ca.crt                    100% 1196   949.1KB/s   00:00  
sftp> put /etc/openvpn/easy-rsa3  
3.0.7/ 3.0./ 3/  
sftp> put /etc/openvpn/easy-rsa3/pki/issued/oos2.janach.local.crt  
Uploading /etc/openvpn/easy-rsa3/pki/issued/oos2.janach.local.crt to /etc/openvpn/pki/oos2.janach.local.crt  
/etc/openvpn/easy-rsa3/pki/issued/oos2.janach.local.c... 100% 4630   2.5MB/s     00:00  
sftp> put /etc/openvpn/easy-rsa3/pki/issued/client.crt  
Uploading /etc/openvpn/easy-rsa3/pki/issued/client.crt to /etc/openvpn/pki/client.crt  
/etc/openvpn/easy-rsa3/pki/issued/client.crt           100% 4460   4.4MB/s     00:00  
sftp> put /etc/openvpn/easy-rsa3/pki/private/client.key  
Uploading /etc/openvpn/easy-rsa3/pki/private/client.key to /etc/openvpn/pki/client.key  
/etc/openvpn/easy-rsa3/pki/private/client.key          100% 1704   1.1MB/s     00:00  
sftp> cd /etc/openvpn/  
sftp> put /etc/openvpn/openv  
openvpn.log       openvpn.tlsauth  
sftp> put /etc/openvpn/openvpn.tlsauth  
Uploading /etc/openvpn/openvpn.tlsauth to /etc/openvpn/openvpn.tlsauth  
/etc/openvpn/openvpn.tlsauth                          100% 636   155.0KB/s   00:00  
sftp exit  
[root@oos2 openvpn]# gedit /etc/firewalld/direct.xml  
^C  
[root@oos2 openvpn]# pwd  
/etc/openvpn  
[root@oos2 openvpn]# ls  
client.conf  easy-rsa  openvpn.log  openvpn.tlsauth  server  server.conf  
[root@oos2 openvpn]# gedit server.conf  
[root@oos2 openvpn]# gedit /var/log/openvpn/openvpn.log  
[root@oos2 openvpn]# cat server.conf  
[root@oos2 openvpn]# systemctl restart openvpnservice  
[root@oos2 openvpn]# gedit /var/log/openvpn/openvpn.log  
[root@oos2 openvpn]# gedit /var/log/openvpn/openvpn.log  
[root@oos2 openvpn]# ausearch -c '*openvpn' --raw | audit2allow -M my-openvpn  
*****  
[root@oos2 openvpn]#
```

Sljedeće naredbe potrebno je upisati u terminal OOS1 računala koje u ovome slučaju služi kao klijenstsko računalo za VPN.

Provjeriti da li su na oos1 poslani certifikati.

```
[root@oos1 openvpn]# ls
client client.ovpn openvpn.tlsauth pki server
[root@oos1 openvpn]# cd pki/
[root@oos1 pki]# ls
ca.crt client.crt client.key oos2.janach.local.crt
[root@oos1 pki]#
```

Hostname: oos1.janach.local  
Uptime: 8h 41m 0s  
CPU: 2.00 GHz  
IP: 10.10.48.30  
MAC: 00:50:56:8b:ectcd

root@oos1:/etc/openvpn/pki

[BackupPC: Host 10.10.48.31 Backu...

1 / 4

ENG 19:40 05/06/2020

Slika 30: prikaz uspješno poslanih certifikata na OOS1 računalo

Kreirati file client.ovpn na putanji /etc/openvpn/client.ovpn.

2019-PP506U-K205-C057-1-2019 - VMware Remote Console

Applications Places Terminal

root@oos1:/etc/openvpn

File Edit View Search Terminal Help

client  
proto udp  
remote 192.168.10.2 1194  
dev tun  
resolv-retry infinite  
nobind  
persist-key  
persist-tun  
remote-cert-eku "TLS Web Server Authentication"  
verify-x509-name oos2.janach.local name  
tun-mtu 1500  
tun-mtu-extra 32  
mssfix 1450  
reneg-sec 14400  
comp-lzo  
tls-client  
tls-version-min 1.2  
verb 3  
ca /etc/openvpn/pki/ca.crt  
cert /etc/openvpn/pki/client.crt  
key /etc/openvpn/pki/client.key  
tls-crypt /etc/openvpn/openvpn.tlsauth

auth-nocache

root@oos1:/etc/openvpn

[BackupPC: Host 10.10.48.31 Backu...

1 / 4

ENG 19:45 05/06/2020

Slika 31: prikaz kreiranog client.ovpn file-a

Spojiti se klijentom pomoću VPN-a na oos2 računalo.

openvpn --config /etc/openvpn/client.ovpn

2019-PP506U-K205-C057-1-2019 - VMware Remote Console

Applications Places Terminal

root@oos1:/etc/openvpn

File Edit View Search Terminal Help

[root@oos1 openvpn]# openvpn --config /etc/openvpn/client.ovpn  
Fri Jun 5 17:40:40 2020 OpenVPN 2.4.9 x86\_64-redhat-linux-gnu [Fedora EPEL patched] [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] built on Apr 24 2020  
Fri Jun 5 17:40:40 2020 library versions: OpenSSL 1.0.2k-fips 26 Jan 2017, LZO 2.06  
Fri Jun 5 17:40:40 2020 Outgoing Control Channel Encryption: Cipher 'AES-256-CTR' initialized with 256 bit key  
Fri Jun 5 17:40:40 2020 Incoming Control Channel Encryption: Cipher 'AES-256-CTR' initialized with 256 bit key  
Fri Jun 5 17:40:40 2020 TCP/UDP: Preserving recently used remote address: [AF\_INET]192.168.10.2:1194  
Fri Jun 5 17:40:40 2020 Socket Buffers: R=[212992->212992] S=[212992->212992]  
Fri Jun 5 17:40:40 2020 UDP link local: (not bound)  
Fri Jun 5 17:40:40 2020 UDP link remote: [AF\_INET]192.168.10.2:1194  
Fri Jun 5 17:40:40 2020 TLS: Initial packet from [AF\_INET]192.168.10.2:1194, sid=4f3cc393 46b59dd0  
Fri Jun 5 17:40:40 2020 VERIFY OK: depth=1, CN=oos2.janach.local  
Fri Jun 5 17:40:40 2020 Validating certificate extended key usage  
Fri Jun 5 17:40:40 2020 ++ Certificate has EKU (str) TLS Web Server Authentication, expects TLS Web Server Authentication  
Fri Jun 5 17:40:40 2020 VERIFY ECU OK  
Fri Jun 5 17:40:40 2020 VERIFY X509NAME OK: CN=oos2.janach.local  
Fri Jun 5 17:40:40 2020 VERIFY OK: depth=0, CN=oos2.janach.local  
Fri Jun 5 17:40:40 2020 Control Channel: TLSv1.2, cipher TLSv1/SSLv3 ECDHE-RSA-AES256-GCM-SHA384, 2048 bit RSA  
Fri Jun 5 17:40:40 2020 [oos2.janach.local] Peer Connection Initiated with [AF\_INET]192.168.10.2:1194  
Fri Jun 5 17:40:41 2020 SENT CONTROL [oos2.janach.local]: 'PUSH\_REQUEST' (status=1)  
Fri Jun 5 17:40:41 2020 PUSH: Received control message: 'PUSH\_REPLY,redirect-gateway def1 bypass-dhcp,dhcp-option DNS 8.8.8.8,dhcp-option DNS 8.8.4.4,route-gateway 172.16.100.1,topology subnet,ping 5,ping-restart 30,ifconfig 172.16.100.2 255.255.255.0,peer-id 0,cipher AES-256-GCM'  
Fri Jun 5 17:40:41 2020 OPTIONS IMPORT: --ifconfig/up options modified  
Fri Jun 5 17:40:41 2020 OPTIONS IMPORT: route options modified  
Fri Jun 5 17:40:41 2020 OPTIONS IMPORT: timers and/or timeouts modified  
Fri Jun 5 17:40:41 2020 OPTIONS IMPORT: --ip-win32 and/or --dhcp-option options modified  
Fri Jun 5 17:40:41 2020 OPTIONS IMPORT: peer-id set  
Fri Jun 5 17:40:41 2020 OPTIONS IMPORT: adjusting link\_mtu to 1657  
Fri Jun 5 17:40:41 2020 OPTIONS IMPORT: data channel crypto options modified  
Fri Jun 5 17:40:41 2020 Data Channel: using negotiated cipher 'AES-256-GCM'  
Fri Jun 5 17:40:41 2020 Outgoing Data Channel: Cipher 'AES-256-GCM' initialized with 256 bit key  
Fri Jun 5 17:40:41 2020 Incoming Data Channel: Cipher 'AES-256-GCM' initialized with 256 bit key  
Fri Jun 5 17:40:41 2020 ROUTE GATEWAY 10.10.51.254/255.255.252.0 IFACE=ens192 HWADDR=00:50:56:8b:ectcd  
Fri Jun 5 17:40:41 2020 TUN/TAP device tun0 opened  
Fri Jun 5 17:40:41 2020 TUN/TAP TX queue length set to 100  
Fri Jun 5 17:40:41 2020 /sbin/ip link set dev tun0 up mtu 1500  
Fri Jun 5 17:40:41 2020 /sbin/ip addr add dev tun0 172.16.100.2/24 broadcast 172.16.100.255  
Fri Jun 5 17:40:41 2020 /sbin/ip route add 192.168.10.2/32 via 10.10.51.254  
Fri Jun 5 17:40:41 2020 /sbin/ip route add 0.0.0.0/1 via 172.16.100.1  
Fri Jun 5 17:40:42 2020 /sbin/ip route add 128.0.0.0/1 via 172.16.100.1  
Fri Jun 5 17:40:42 2020 Initialization Sequence Completed

root@oos1:/etc/openvpn

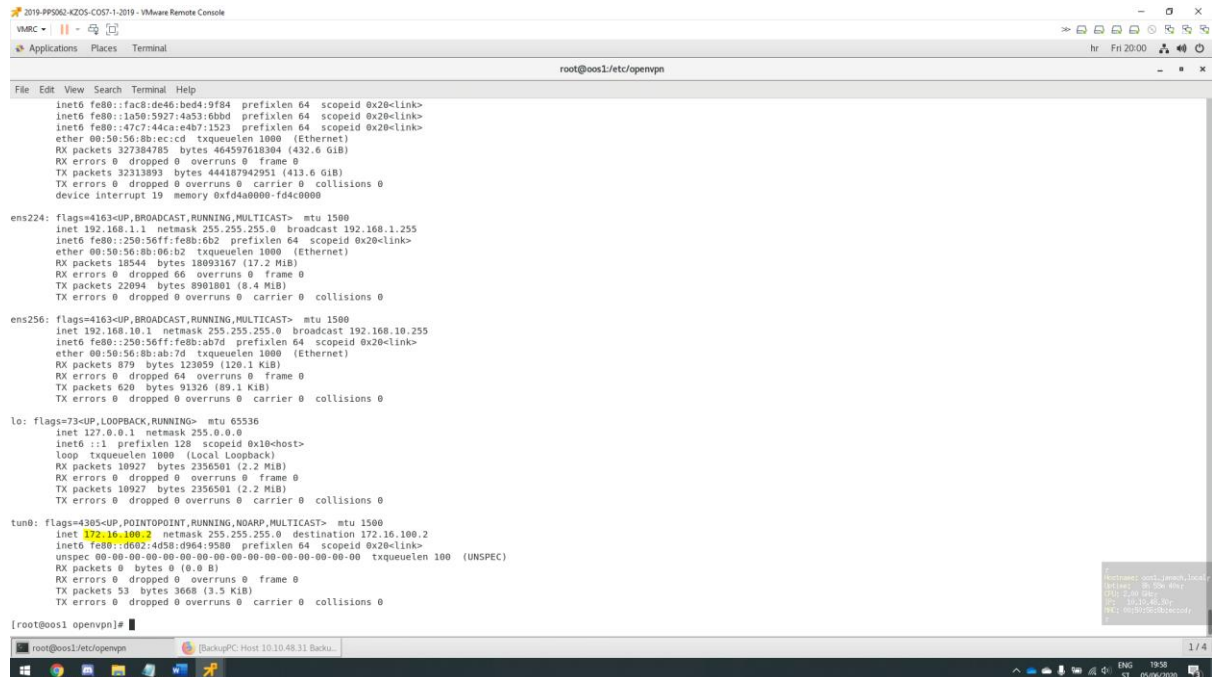
[BackupPC: Host 10.10.48.31 Backu...

1 / 4

ENG 19:55 05/06/2020

Slika 32: prikaz spajanja s klijentskog računala OOS1 na OOS2 VPN-om

Proveriti ifconfig naredbom da li je računalu dodjeljena IP adresa.



```
File Edit View Search Terminal Help
root@oos1:/etc/openvpn

inet6 fe80::fac8:de46:bed4:9f84 prefixlen 64 scopeid 0x20<link>
inet6 fe80::1a50:5927:4a53:16bd prefixlen 64 scopeid 0x20<link>
inet6 fe80::47c7:44ca:e4b7:1523 prefixlen 64 scopeid 0x20<link>
ether 00:50:56:8b:ec:cd txqueuelen 1000 (Ethernet)
RX packets 327384785 bytes 464597618304 (432.6 GiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 32313893 bytes 444187942951 (413.6 GiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
device interrupt 19 memory 0xfda0000-fdc0000

ens224: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 192.168.1.1 netmask 255.255.255.0 broadcast 192.168.1.255
inet6 fe80::250:56ff:fe8b:602 prefixlen 64 scopeid 0x20<link>
ether 00:50:56:8b:06:b2 txqueuelen 1000 (Ethernet)
RX packets 18544 bytes 18093167 (17.2 MiB)
RX errors 0 dropped 66 overruns 0 frame 0
TX packets 22094 bytes 89031001 (8.4 MiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

ens256: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 192.168.10.1 netmask 255.255.255.0 broadcast 192.168.10.255
inet6 fe80::250:56ff:fe8b:ab7d prefixlen 64 scopeid 0x20<link>
ether 00:50:56:8b:ab:7d txqueuelen 1000 (Ethernet)
RX packets 879 bytes 123059 (120.1 KiB)
RX errors 0 dropped 64 overruns 0 frame 0
TX packets 620 bytes 91326 (89.1 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

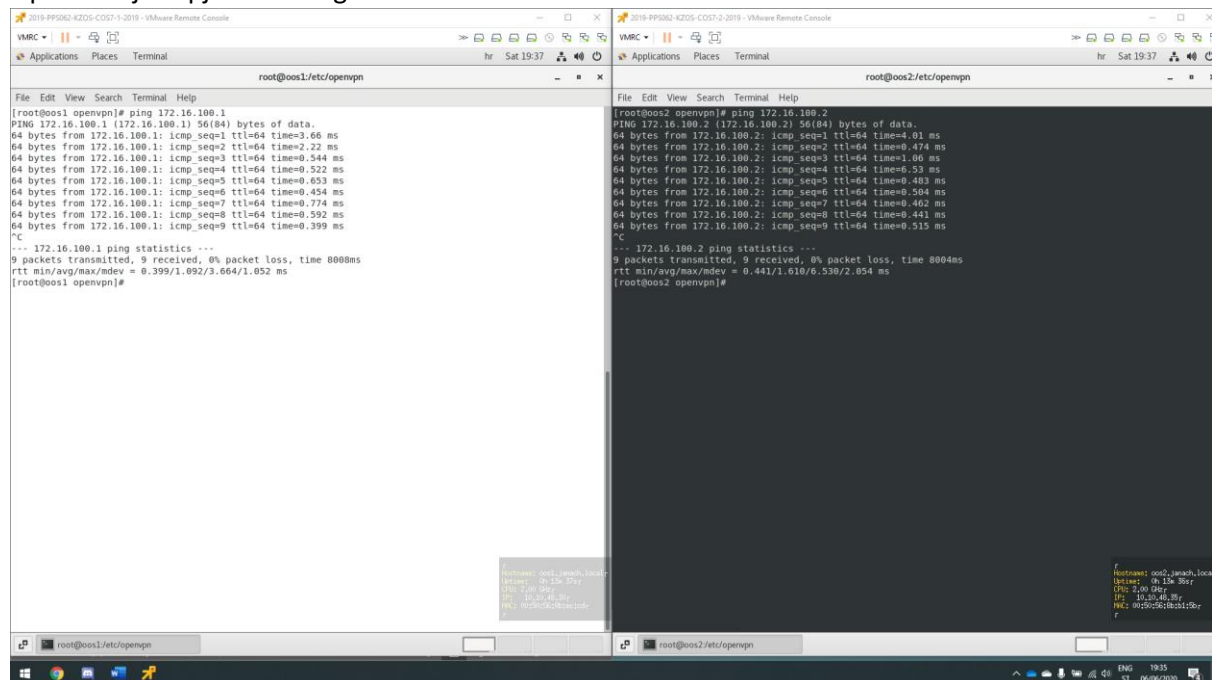
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0x10<host>
loop txqueuelen 1000 (Local Loopback)
RX packets 10927 bytes 2356501 (2.2 MiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 10927 bytes 2356501 (2.2 MiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

tun0: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST> mtu 1500
inet 172.16.100.2 netmask 255.255.255.0 destination 172.16.100.2
inet6 fe80::d602:4d58:d964:9500 prefixlen 64 scopeid 0x20<link>
unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00 txqueuelen 100 (UNSPEC)
RX packets 0 bytes 0 (0.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 53 bytes 3668 (3.5 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

[root@oos1 openvpn]#
```

Slika 33: prikaz dodjeljene IP adrese

OpenVPN je uspješno konfiguriran.



```
File Edit View Search Terminal Help
root@oos1:/etc/openvpn

[root@oos1 openvpn]# ping 172.16.100.1
PING 172.16.100.1 (172.16.100.1) 56(84) bytes of data:
64 bytes from 172.16.100.1: icmp_seq=1 ttl=64 time=3.66 ms
64 bytes from 172.16.100.1: icmp_seq=2 ttl=64 time=2.22 ms
64 bytes from 172.16.100.1: icmp_seq=3 ttl=64 time=0.544 ms
64 bytes from 172.16.100.1: icmp_seq=4 ttl=64 time=0.522 ms
64 bytes from 172.16.100.1: icmp_seq=5 ttl=64 time=0.653 ms
64 bytes from 172.16.100.1: icmp_seq=6 ttl=64 time=0.454 ms
64 bytes from 172.16.100.1: icmp_seq=7 ttl=64 time=0.774 ms
64 bytes from 172.16.100.1: icmp_seq=8 ttl=64 time=0.592 ms
64 bytes from 172.16.100.1: icmp_seq=9 ttl=64 time=0.399 ms
^C
... 172.16.100.1 ping statistics ...
9 packets transmitted, 9 received, 0% packet loss, time 8008ms
rtt min/avg/max/mdev = 0.399/1.092/3.664/1.052 ms
[root@oos1 openvpn]#

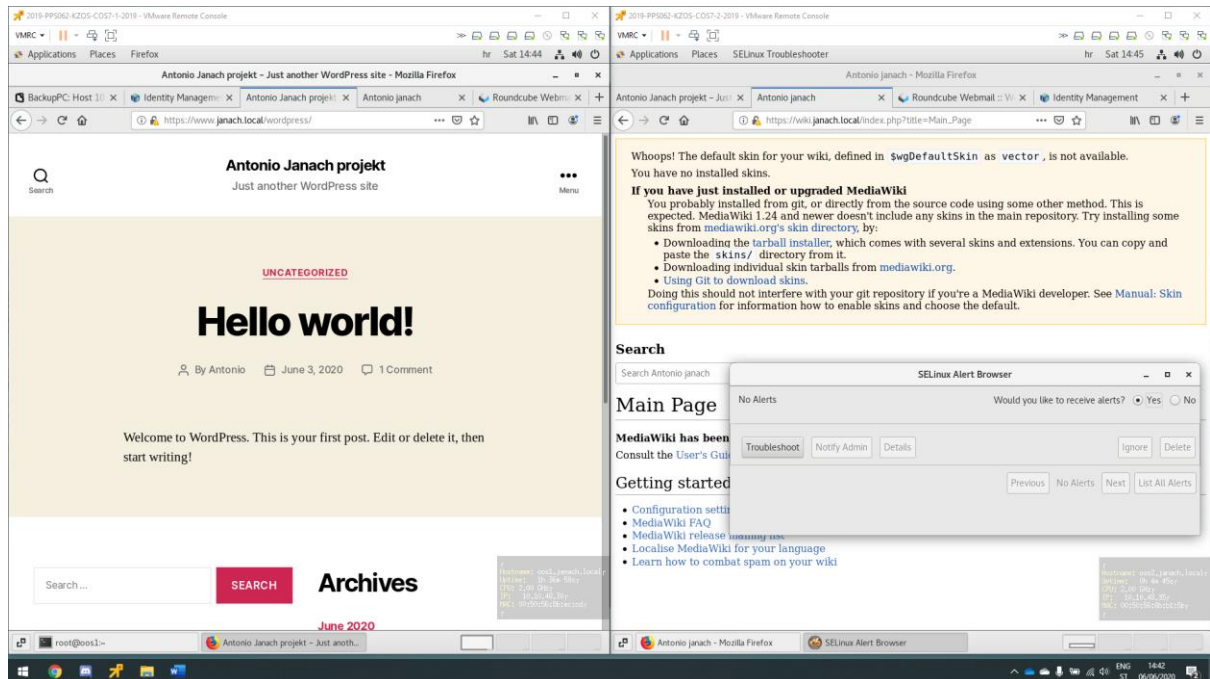
File Edit View Search Terminal Help
root@oos2:/etc/openvpn

[root@oos2 openvpn]# ping 172.16.100.2
PING 172.16.100.2 (172.16.100.2) 56(84) bytes of data:
64 bytes from 172.16.100.2: icmp_seq=1 ttl=64 time=4.81 ms
64 bytes from 172.16.100.2: icmp_seq=2 ttl=64 time=0.474 ms
64 bytes from 172.16.100.2: icmp_seq=3 ttl=64 time=1.06 ms
64 bytes from 172.16.100.2: icmp_seq=4 ttl=64 time=6.53 ms
64 bytes from 172.16.100.2: icmp_seq=5 ttl=64 time=0.483 ms
64 bytes from 172.16.100.2: icmp_seq=6 ttl=64 time=0.504 ms
64 bytes from 172.16.100.2: icmp_seq=7 ttl=64 time=0.462 ms
64 bytes from 172.16.100.2: icmp_seq=8 ttl=64 time=0.441 ms
64 bytes from 172.16.100.2: icmp_seq=9 ttl=64 time=0.515 ms
^C
... 172.16.100.2 ping statistics ...
9 packets transmitted, 9 received, 0% packet loss, time 8004ms
rtt min/avg/max/mdev = 0.441/1.610/6.530/2.054 ms
[root@oos2 openvpn]#
```

Slika 34: prikaz uspješne konfiguracije OpenVPN-a

## 5.7. Semanage

U semanage-u riješeni su svi alert-ovi te je dostupnost na sve web stranice preko web preglednika dostupna.



Slika 35: prikaz semanage alert-ova i dostupnosti na sve web stranice preko web preglednika

## 6. Popis slika

Slika 1: prikaz opisa infrastrukture koji je izrađen u FreeMind softwar .....	2
Slika 2: prikaz topologije infrastrukture .....	3
Slika 3: prikaz promjene hostname-a, ip adrese na ens224 mrežnom adapteru i dodanog host zapisa4	
Slika 4: provjera konfiguracije i prikaz uspješne instalacije FreeIPA servera na OOS1 računalu.....	5
Slika 5: prikaz promjene hostname, IP adrese na ens224 mrežnom adapteru i dodavanje host zapisa 5	
Slika 6: prikaz funkcionalnog rada FreeIPA client-a na OOS2 računalu .....	6
Slika 7: prikaz nadogradnje php-a s verzije 5.4 na 7.3 .....	7
Slika 8: na putanji dokumenta potrebno je promijeniti user i group, listen socket i permission-e za socket file .....	8
Slika 9: prikaz konfiguracije virtualnog poslužitelja za MediaWiki .....	9
Slika 10: Prikaz uspješno instaliranog MediaWiki sustava koji se pokreće na Nginx servisu .....	9
Slika 11: Prikaz konfiguracije httpd.conf file-a.....	10
Slika 12: prika konfiguracije www.conf file-a.....	11
Slika 13: prikaz konfiguracije mod_ssl file-a .....	11
Slika 14: prikaz uspjene instalacije wordpress platoforme.....	12
Slika 15: prikaz konfiguracije iSCSI target-a .....	13
Slika 16: prikaz konfiguracije iscsid.conf.....	14
Slika 17: prikaz /etc/fstab trajne konfiguracije iSCSI diskova .....	15
Slika 18: prikaz provjere iSCSI mount-a diskova .....	15
Slika 19: prikaz odkomentiranog dijela koda u master.cf datoteci.....	16
Slika 20: mail je uspješno stigao na adresu.....	17
Slika 21: prikaz konfiguracije mail.conf file-a.....	18
Slika 22: prikaz konfiguracije config.inc.php file-a.....	19
Slika 23: prikaz uspješne instalacije Roundcube-a.....	19
Slika 24: prikaz konfiguracije BackupPC.conf.....	20
Slika 25: prikaz BackupPC sučelja u kojem se vidi da je pokrenuti full backup PC-a .....	21
Slika 26: prikaz uspješno izdanih certifikata .....	22
Slika 27: prikaz konfiguracije server.conf file-a .....	23
Slika 28: prikaz generiranja ključeva na OOS2 računalu .....	24
Slika 29: prikaz uspješno poslanih ključeva na OOS1 računalu.....	24
Slika 30: prikaz uspješno posalnih certifikata na OOS1 računalu .....	25
Slika 31: prikaz kreiranog client.ovpn file-a .....	25
Slika 32: prikaz spajanja s klijentskog računala OOS1 na OOS2 VPN-om .....	25
Slika 33: prikaz dodjeljene IP adrese.....	26
Slika 34: prikaz uspješne konfiguracije OpenVPN-a.....	26
Slika 35: prikaz semanage alert-ova i dostupnosti na sve web stranice preko web preglednika.....	27

## 7. Literatura

### FreeIPA:

<https://www.howtoforge.com/how-to-install-freeipa-server-on-centos-7/>

<https://www.linuxtechi.com/install-configure-freeipa-centos-7-server/>

[https://www.freeipa.org/page/Quick\\_Start\\_Guide](https://www.freeipa.org/page/Quick_Start_Guide)

<https://www.digitalocean.com/community/tutorials/how-to-set-up-centralized-linux-authentication-with-freeipa-on-centos-7>

### Intranet i extranet:

#### Nginx, certovi i mediawiki:

<https://www.digitalocean.com/community/tutorials/how-to-install-nginx-on-centos-7>

<https://www.cyberciti.biz/faq/how-to-install-and-use-nginx-on-centos-7-rhel-7/>

<https://www.nginx.com/resources/wiki/start/topics/tutorials/install/>

Certifikati za TLS: <https://www.freeipa.org/page/Certmonger>

Certifikati za TLS: <https://www.freeipa.org/page/PKI>

MediaWiki: <https://websiteforstudents.com/install-mediawiki-ubuntu-17-04-17-10-nginx-mariadb-php/>

MediaWiki: <https://www.howtoforge.com/tutorial/how-to-install-mediawiki-with-nginx-on-ubuntu-1604/>

MediaWiki: <https://www.nginx.com/resources/wiki/start/topics/recipes/mediawiki/>

#### Httpd i wordpress:

<https://www.digitalocean.com/community/tutorials/how-to-install-the-apache-web-server-on-centos-7>

<https://phoenixnap.com/kb/install-apache-on-centos-7>

<https://www.liquidweb.com/kb/how-to-install-apache-on-centos-7/>

Wordpress: <https://www.digitalocean.com/community/tutorials/how-to-install-wordpress-on-centos-7>

Wordpress: <https://devops.ionos.com/tutorials/how-to-install-and-configure-wordpress-on-centos-7/>

VirtualHosts: <https://httpd.apache.org/docs/2.4/vhosts/examples.html>



**File Server:**

<https://kifarunix.com/how-install-and-configure-iscsi-storage-server-on-centos-7/>

<https://www.thegeekdiary.com/complete-guide-to-configuring-iscsi-in-centos-rhel-7/>

<https://www.itzgeek.com/how-tos/linux/centos-how-tos/configure-iscsi-target-initiator-on-centos-7-rhel7.html>

**Web server:****Postfix:**

<https://www.digitalocean.com/community/tutorials/how-to-install-the-apache-web-server-on-centos-7>

<https://phoenixnap.com/kb/install-apache-on-centos-7>

<https://www.liquidweb.com/kb/how-to-install-apache-on-centos-7/>

**Roundcube:**

<https://www.tecmint.com/install-roundcube-webmail-on-centos-7/>

<https://www.linuxtechi.com/install-latest-version-of-roundcube-centos-7/>

[https://www.server-world.info/en/note?os=CentOS\\_7&p=httpd&f=13](https://www.server-world.info/en/note?os=CentOS_7&p=httpd&f=13)

<https://www.arubacloud.com/tutorial/how-to-manage-mailboxes-with-roundcube-on-centos-7.aspx>

**BackupPC:**

<https://www.veritech.net/centos-7-backuppc-installation-guide/>

<https://wiki.centos.org/HowTos/BackupPC>

<https://neklaf.com/2016/03/05/install-and-set-up-backuppc-on-centos-7/>

**Pristup VPN-om:**

<https://www.quickservers.com/en/how-to-install-openvpn-on-centos.php>

<https://www.digitalocean.com/community/tutorials/how-to-set-up-and-configure-an-openvpn-server-on-centos-7>

<https://www.cyberciti.biz/faq/centos-7-0-set-up-openvpn-server-in-5-minutes/>

<https://blog.ssdnodes.com/blog/install-openvpn-centos-7-tutorial/>