

VISOKO UČILIŠTE ALGEBRA

PROJEKTNI ZADATAK

**Napredno administriranje otvorenih
operacijskih sustava**

Antonio Janach

Zagreb, lipanj 2020.

Sadržaj

1.	Sažetak	1
2.	Zahtijevi 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 računalo:

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
- Iscsi-initiator
- VPN client(OpenVPN)
- Backup računala - BackupPC

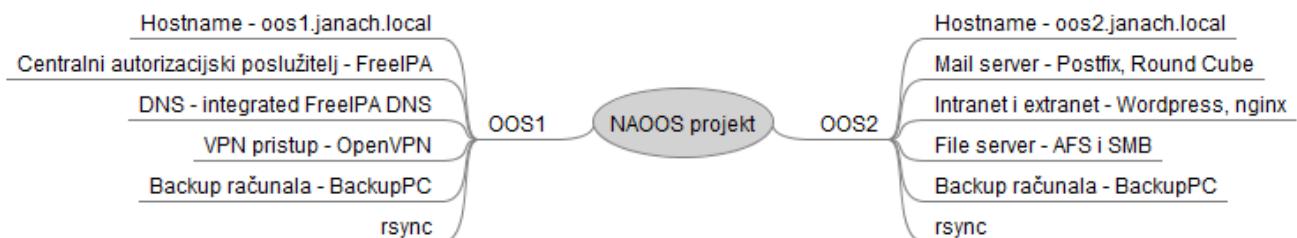
OOS2 računalo:

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

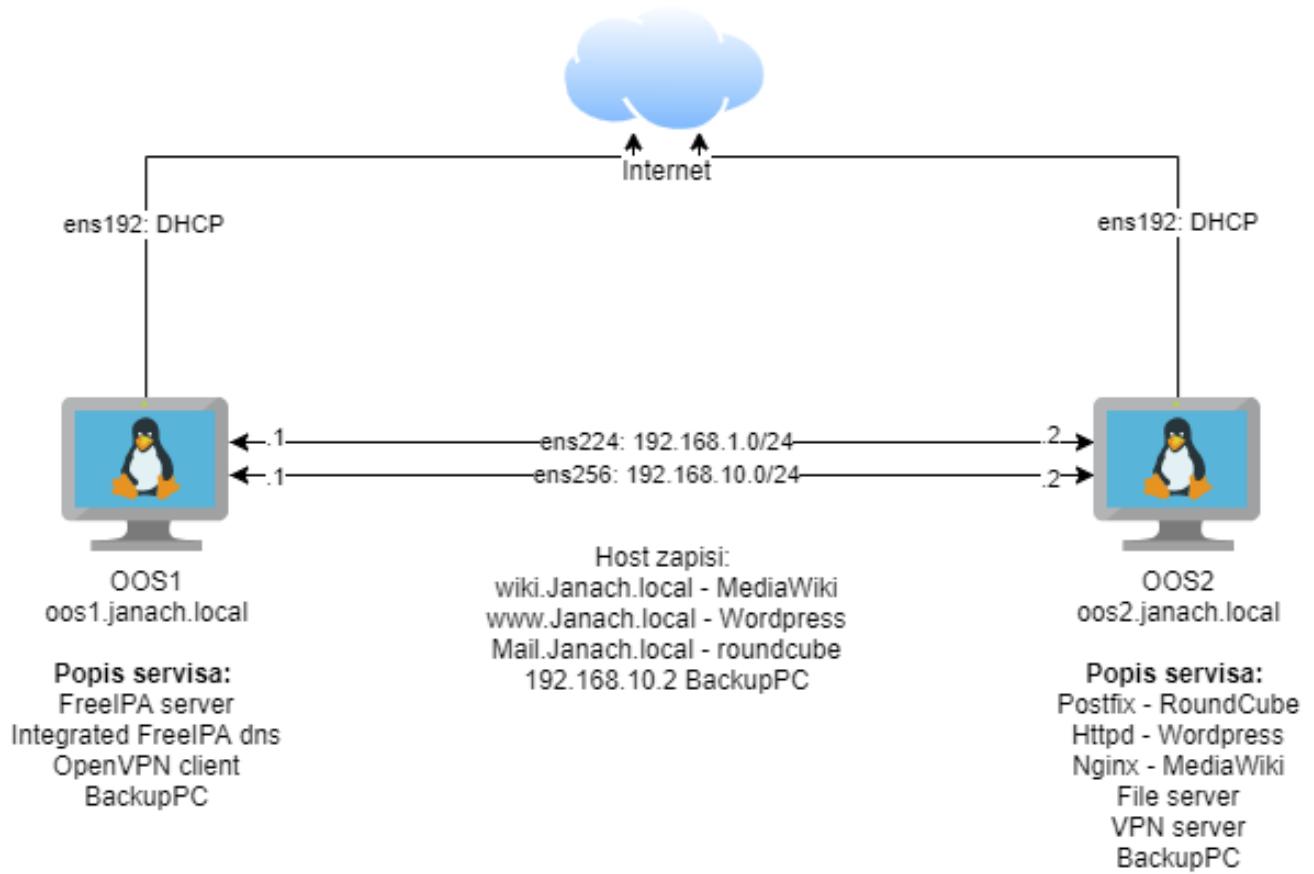
Role:

- 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 adresu na ens224 mrežnom adapteru i dodati host zapis u /etc/hosts:

```
[root@localhost student]# hostname  
oos1.janach.local  
[root@localhost student]# ifconfig  
ens192: flags=416<UP,BROADCAST,RUNNING,MULTICAST  mtu 1500  
        inet 192.168.1.1  brd 192.168.1.255  netmask 255.255.255.0  broadcast 192.168.1.255  
              inet6 fe80::fac8:de46:bed4:9f84  brd fe80::ff:fe46:bed4:9f84  scopeid 0x20<link>  
        ens224: flags=416<UP,BROADCAST,RUNNING,MULTICAST  mtu 1500  
              inet6 fe80::1a50:5927:4a33:6bb0  brd fe80::ff:fe50:5927:4a33:6bb0  scopeid 0x20<link>  
        ens256: flags=416<UP,BROADCAST,RUNNING,MULTICAST  mtu 1500  
              inet6 fe80::47c7:44ca:e407:1523  brd fe80::ff:fe47:c744ca:e407:1523  scopeid 0x20<link>  
        eth0: flags=568<UP,BROADCAST,NOARP  mtu 1500  memory 0xd4a0000-0fd4c000  
              ether 00:50:56:8b:ec:cd  txqueuelen 1000  (Ethernet)  
                    RX packets 0 bytes 0 (0.0 B)  
                    RX errors 0 dropped 0 overruns 0 frame 0  
                    TX packets 40229 bytes 2784544 (2.6 MB)  
                    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
        device interrupt 19  memory 0xfd4a0000-0fd4c0000  
ens224: flags=416<IP,BROADCAST,RUNNING,MULTICAST>  mtu 1500  
        inet 192.168.1.1  brd 192.168.1.255  netmask 255.255.255.0  broadcast 192.168.1.255  
              inet6 fe80::74d:ed5f:a46:a3a9  brd fe80::ff:fe74:d:ed5f:a46:a3a9  scopeid 0x20<link>  
        eth0: flags=568<UP,BROADCAST,NOARP  mtu 1500  memory 0xd4a0000-0fd4c000  
              ether 00:50:56:8b:ec:cd  txqueuelen 1000  (Ethernet)  
                    RX packets 37 bytes 3348 (3.2 KB)  
                    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  
ens256: flags=416<IP,BROADCAST,RUNNING,MULTICAST>  mtu 1500  
        ether 00:50:56:8b:ab:7d  txqueuelen 1000  (Ethernet)  
        loop: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536  
              inet 127.0.0.1  brd 127.0.0.1  netmask 255.0.0.0  
        ens224: flags=416<IP,BROADCAST,RUNNING,MULTICAST>  mtu 1500  
              inet 192.168.1.1  brd 192.168.1.255  netmask 255.255.255.0  broadcast 192.168.1.255  
                    inet6 fe80::1a50:5927:4a33:6bb0  brd fe80::ff:fe50:5927:4a33:6bb0  scopeid 0x20<link>  
        [root@localhost student]# cat /etc/hosts  
127.0.0.1  localhost localdomain localhost4 localhost4.localdomain4  
::1         localhost.localdomain localhost6 localhost6.localdomain6  
192.168.1.1  oos1.janach.local  ipa  
[root@localhost student]#
```

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
```

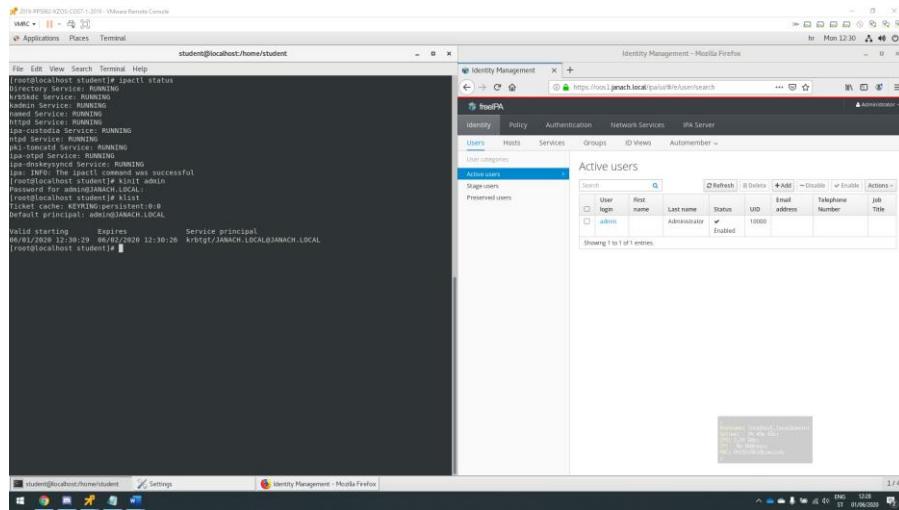
Računalo OOS1 spremno je za instalaciju centralnog autorizacijskog poslužitelja jer zadovoljava sve uvjete koje smo predhodno odradili. U sljedećim koracima slijedi instalacija i konfiguracija FreeIPA.

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 --idmax=2000000 -- 
mkhomedir --unattended
```

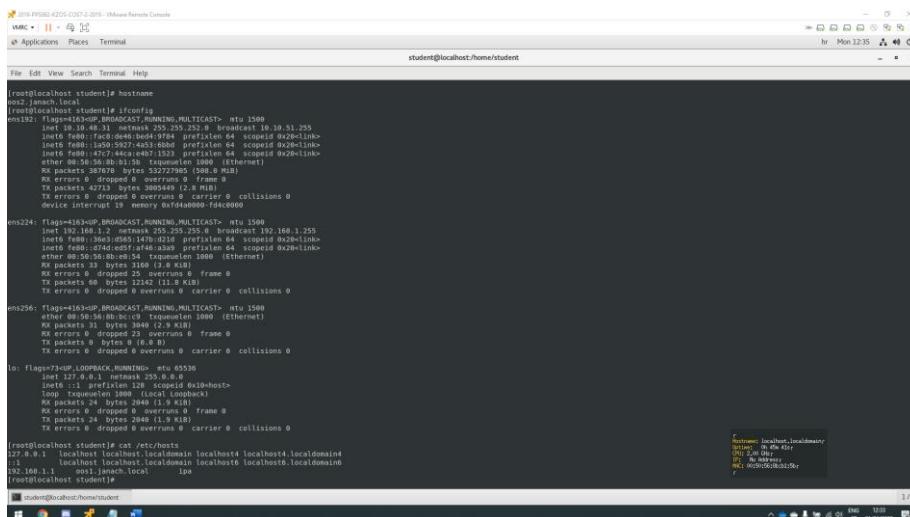


Slika 4: provjera konfiguracije i prikaz uspješne instalacije FreeIPA servera na OOS1 računalu

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



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

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

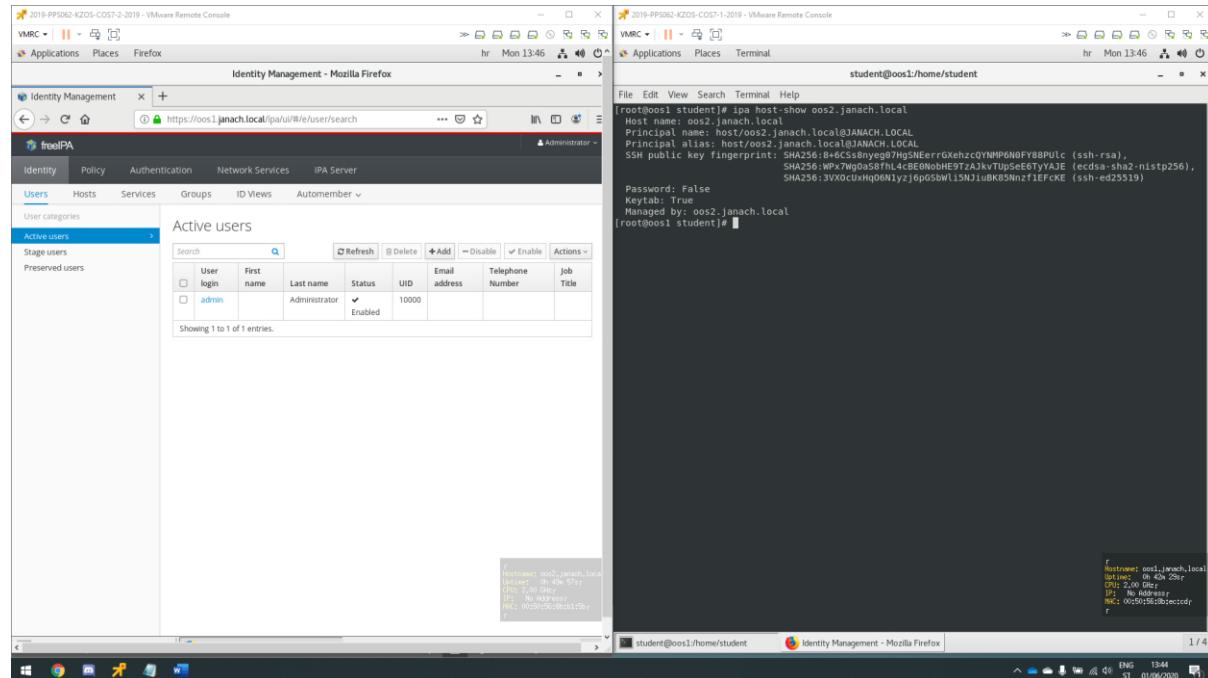
```
#pokrenuti firewall i enable-ati ga:  
Systemctl start firewalld  
Systemctl enable firewalld  
#propustiti portove kroz firewall:  
Firewall-cmd --permanent -add-service={dns,freeipa-  
ldap,http,kerberos,kpasswd,ldap,ldaps,ntp}  
Firewall-cmd --reload
```

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

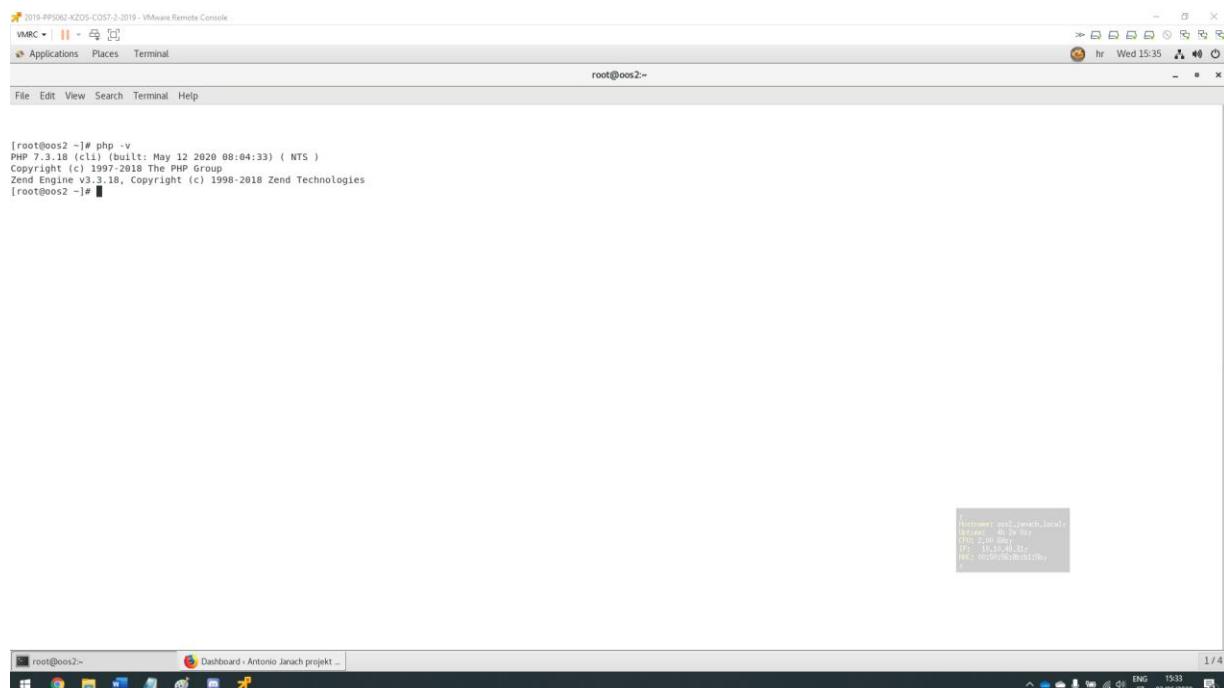
5.2. Intranet i extranet

Cilj je napraviti web stranice bazirane ne 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 zajendo 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
```

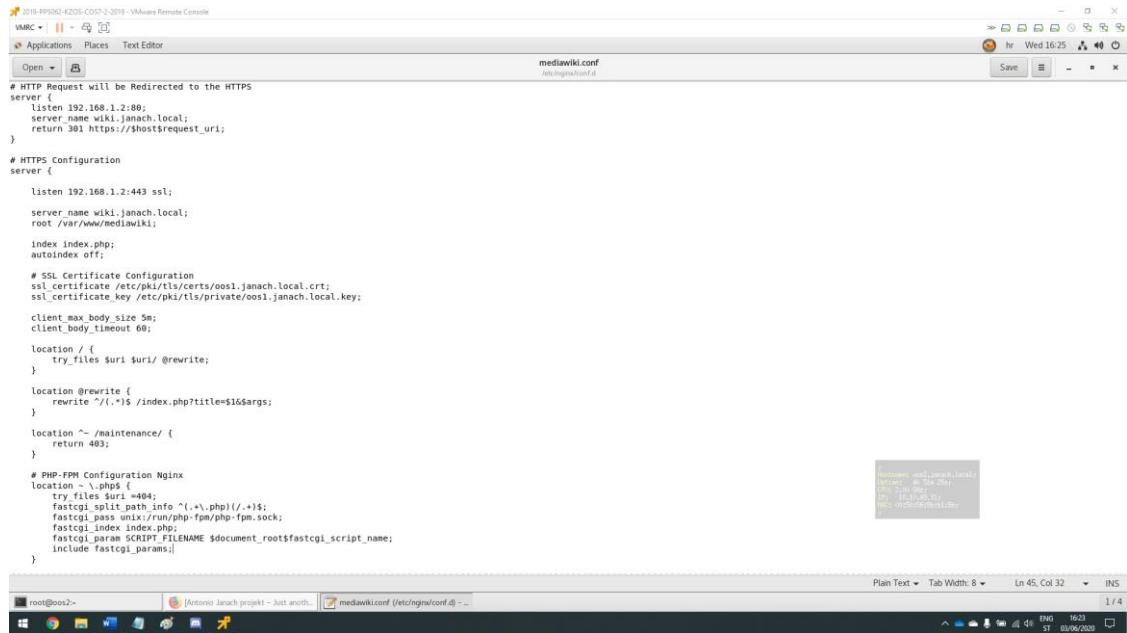
Kreirati bazu i user-a za MediaWiki sustav kroz mariaDB. Baza se može kreirati i pomoću phpMyAdmin gui sučelja.

```
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



```
# HTTP Request will be Redirected to the HTTPS
server {
    listen 192.168.1.2:80;
    server_name wiki.janach.local;
    return 301 https://$host$request_uri;
}

# HTTPS Configuration
server {
    listen 192.168.1.2:443 ssl;
    server_name wiki.janach.local;
    root /var/www/mediawiki;
    index index.php;
    autoindex off;

    # SSL Certificate Configuration
    ssl_certificate /etc/pki/tls/certs/oos1.janach.local.crt;
    ssl_certificate_key /etc/pki/tls/private/oos1.janach.local.key;
    client_max_body_size 5M;
    client_body_timeout 60;

    location / {
        try_files $uri $uri/ @rewrite;
    }

    location @rewrite {
        rewrite ^/.*$ /index.php?title=$1&$args;
    }

    location ~ /maintenance/ {
        return 403;
    }

    # PHP-FPM Configuration Nginx
    location ~ \.php$ {
        try_files $uri =404;
        fastcgi_split_path_info ^(.+\.php)(/.+)$;
        fastcgi_pass unix:/run/php-fpm/php-fpm.sock;
        fastcgi_index index.php;
        fastcgi_param SCRIPT_FILENAME $document_root$fastcgi_script_name;
        include fastcgi_params;
    }
}
```

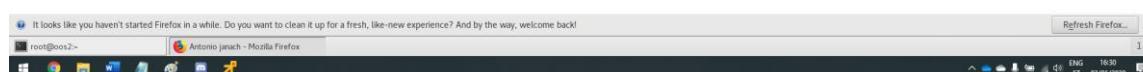
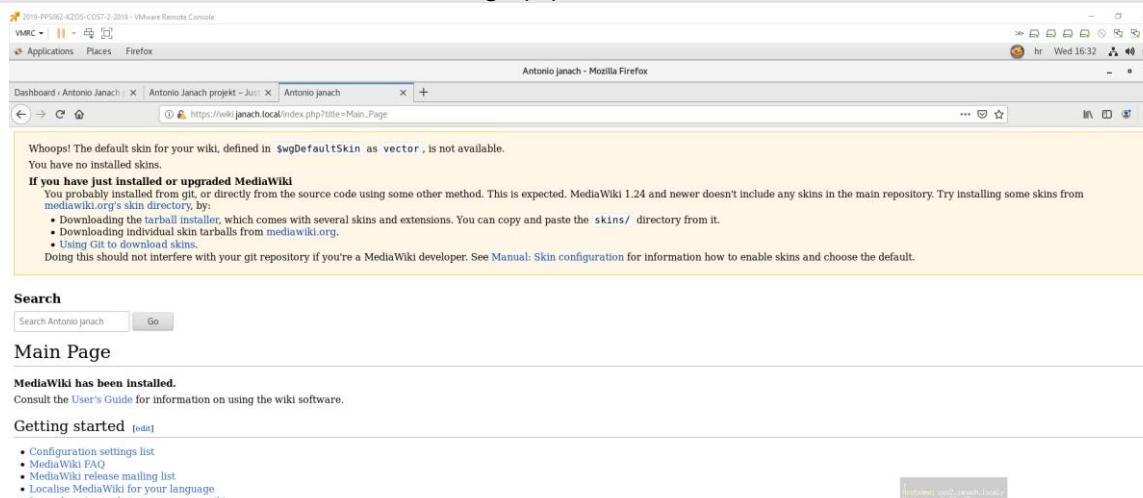
Slika 9: prikaz konfiguracije virtualnog poslužitelja za MediaWiki

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.

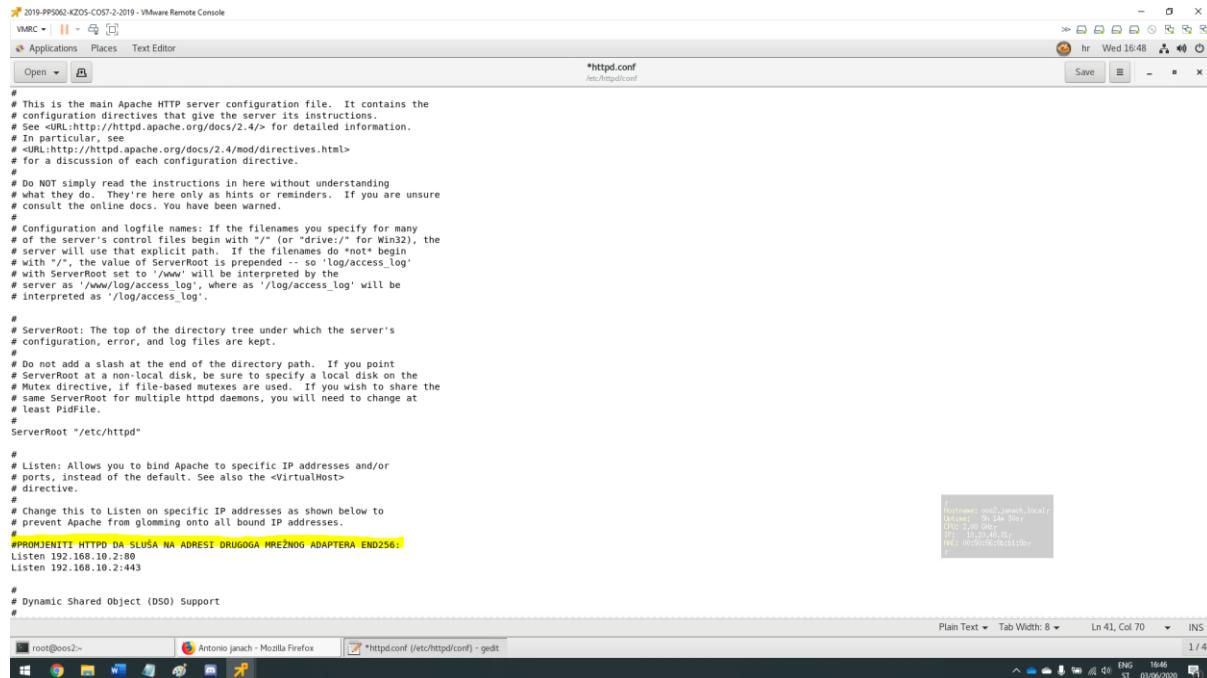
Instalirati Httpd i mod_ssl i pokrenuti httpd servis i omogućiti da se pokreće pri podizanju sustava.

```
Yum install httpd mod_ssl -y
```

```
Systemctl start httpd
```

```
Systemctl enable httpd
```

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



```
# This is the main Apache HTTP server configuration file. It contains the
# configuration directives that give the server its instructions.
# See <URL:>http://httpd.apache.org/docs/2.4/ for detailed information.
# In particular, see
# <URL:>http://httpd.apache.org/docs/2.4/mod/directives.html
# for a discussion of each configuration directive.
#
# Do NOT simply read the instructions in here without understanding
# what they do. They're here only as hints or reminders. If you are unsure
# consult the online docs. You have been warned.
#
# Configuration and logfile names: If the filenames you specify for many
# of the server's control files begin with "/" (or "drive:/" for Win32), the
# server will use that explicit path. If the filenames do *not* begin
# with "/", the value of ServerRoot is prepended -- so 'log/access_log'
# with ServerRoot set to '/var/www/' will be interpreted by the
# server as '/var/www/log/access_log', whereas as '/log/access_log' will be
# interpreted as '/log/access_log'.
#
# ServerRoot: The top of the directory tree under which the server's
# configuration, error, and log files are kept.
#
# Do not add a slash at the end of the directory path. If you point
# ServerRoot at a non-local disk, be sure to specify a local disk on the
# PidFile directive, if file-based mutexes are used. If you wish to share the
# same ServerRoot for multiple httpd daemons, you will need to change at
# least PidFile.
#
ServerRoot "/etc/httpd"
#
# Listen: Allows you to bind Apache to specific IP addresses and/or
# ports, instead of the default. See also the <VirtualHost>
# directive.
#
# Change this to Listen on specific IP addresses as shown below to
# prevent Apache from glomming onto all bound IP addresses.
#
#PROJENI HTTP DA SLUŠA NA ADRESI DRUGOGA MREŽNOG ADAPTERA END256:
Listen 192.168.10.2:80
Listen 192.168.10.2:443
#
# Dynamic Shared Object (DSO) Support
#
```

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 putanji /etc/httpd/conf.d/www.conf i postaviti certifikate.

```
<VirtualHost *:443>
    ServerName www.janach.local
    ServerAlias janach.local
    Redirect permanent / https://www.janach.local/
</VirtualHost>

<VirtualHost 192.168.10.2:443>
    ServerName www.janach.local
    ServerAlias janach.local
    <If "%{HTTP_HOST} == 'janach.local'>
        Redirect permanent / https://www.janach.local/
    </If>
    DocumentRoot /var/www/html
    ErrorLog /var/log/httpd/janach-local-error.log
    CustomLog /var/log/httpd/janach-local-access.log combined
    SSLEngine On
    SSLProtocol all -SSLV2 -SSLV3
    SSLCertificateFile /etc/pki/tls/certs/oos1.janach.local.crt
    SSLCertificateKeyFile /etc/pki/tls/private/oos1.janach.local.key
</VirtualHost>
```

Firefox screenshot showing a certificate warning for 'www.janach.local'. The address bar shows 'https://www.janach.local'. The status bar indicates 'SSL: 10.10.49.33/10.10.49.33' and 'TLS: 1.0/1.2/1.3/1.4/1.5/1.6/1.7/1.8/1.9/1.10/1.11'.

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.

```
# Speed-optimized SSL Cipher configuration:
# If speed is your main concern (on busy HTTPS servers e.g.),
# you might want to force clients to specific, performance
# optimized ciphers. In this case, prepend those ciphers
# to the SSLCipherSuite list, and enable SSLHonorCipherOrder.
# Caveat: by giving precedence to RC4-SHA and AES128-SHA
# (as in the example below), most connections will no longer
# have perfect forward secrecy - if the server's key is
# compromised, captures of past or future traffic must be
# considered compromised, too.
SSLCipherSuite RC4-SHA:AES128-SHA:HIGH:MEDIUM:!NULL:!MD5
#SSLHonorCipherOrder on

# Server Certificate:
# Point SSLCertificateFile at a PEM encoded certificate. If
# the certificate is encrypted, then you will be prompted for a new
# pass phrase. Note that a kill -HUP will prompt again. A new
# certificate can be generated using the genkey(1) command.
SSLCertificateFile /etc/pki/tls/certs/oos1.janach.local.crt

# Server Private Key:
# If the key is not combined with the certificate, use this
# directive to point at the key file. Keep in mind that if
# you've both a RSA and a DSA private key you can configure
# both in parallel (to also allow the use of DSA ciphers, etc).
SSLCertificateKeyFile /etc/pki/tls/private/oos1.janach.local.key

# Server Certificate Chain:
# Point SSLCertificateChainFile at a file containing the
# concatenation of PEM encoded CA certificates which form the
# certificate chain for the server certificate. Alternatively
# the referenced file can be the same as SSLCertificateFile
# when the CA certificates are directly appended to the server
# certificate for convinience.
#SSLCertificateChainFile /etc/pki/tls/certs/server-chain.crt
```

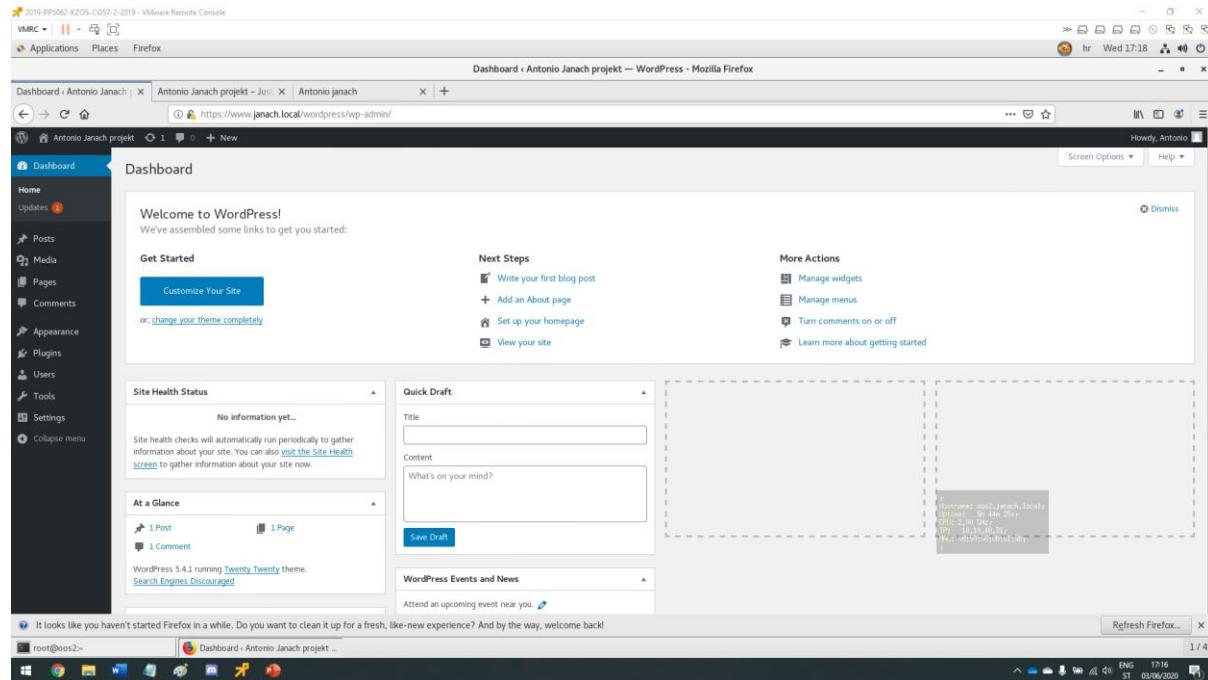
Firefox screenshot showing a certificate warning for 'www.janach.local'. The address bar shows 'https://www.janach.local'. The status bar indicates 'SSL: 10.10.49.33/10.10.49.33' and 'TLS: 1.0/1.2/1.3/1.4/1.5/1.6/1.7/1.8/1.9/1.10/1.11'.

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 platofrme

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.

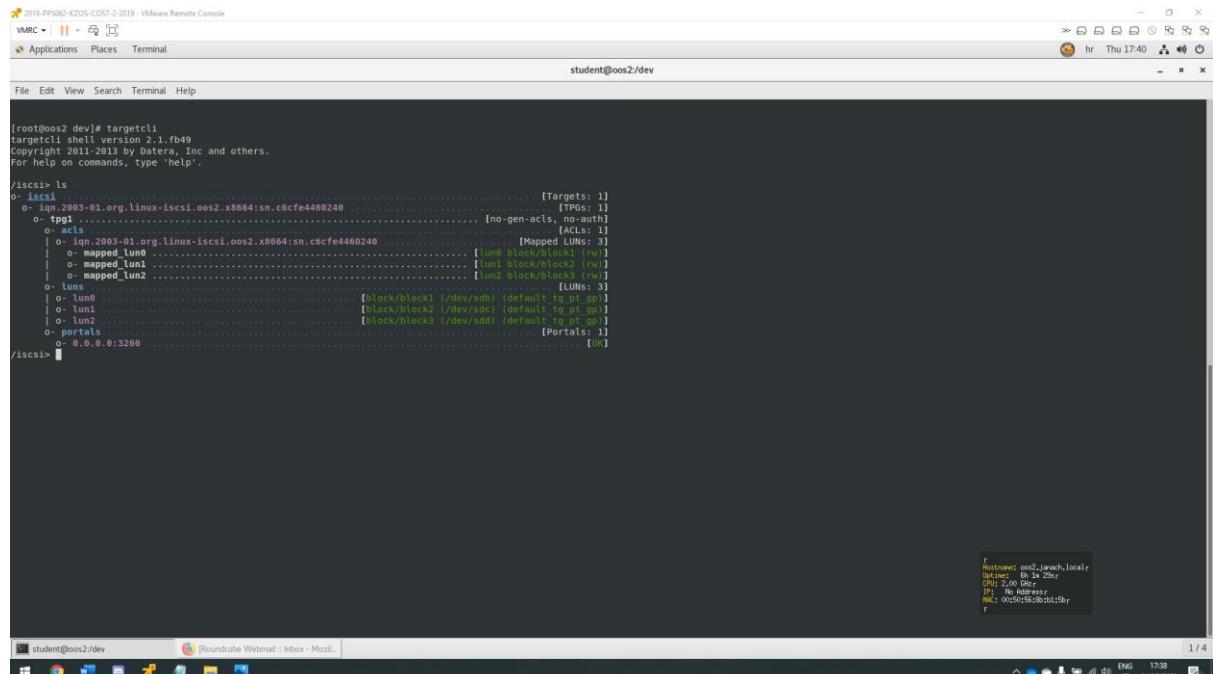
```
Yum install targetcli -y
```

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

Pokrenuti target servis kak obi mogli 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] [TPGs: 1]
o: iqn.2003-01.org.linux-iscsi.oos2.x8664:sn.c6cfe4460240 [no-gen-acls, ACLs: 0]
o: tpgs ..... [ACLs: 1]
o: tpg1 ..... [Mapped LUNs: 3]
| o: mapped_lun0 ..... [LUN0 block/block1 (rw)]
| o: mapped_lun1 ..... [LUN1 block/block2 (rw)]
| o: mapped_lun2 ..... [LUN2 block/block3 (rw)]
o: luns ..... [LUNs: 3]
| o: lun0 ..... [block/block1 (/dev/sdb) (default tg_pt_gp)]
| o: lun1 ..... [block/block2 (/dev/sdc) (default tg_pt_gp)]
| o: lun2 ..... [block/block3 (/dev/sdd) (default tg_pt_gp)]
o: portals ..... [Portals: 1]
o: 0.0.0.0:3260 ..... [0x0]

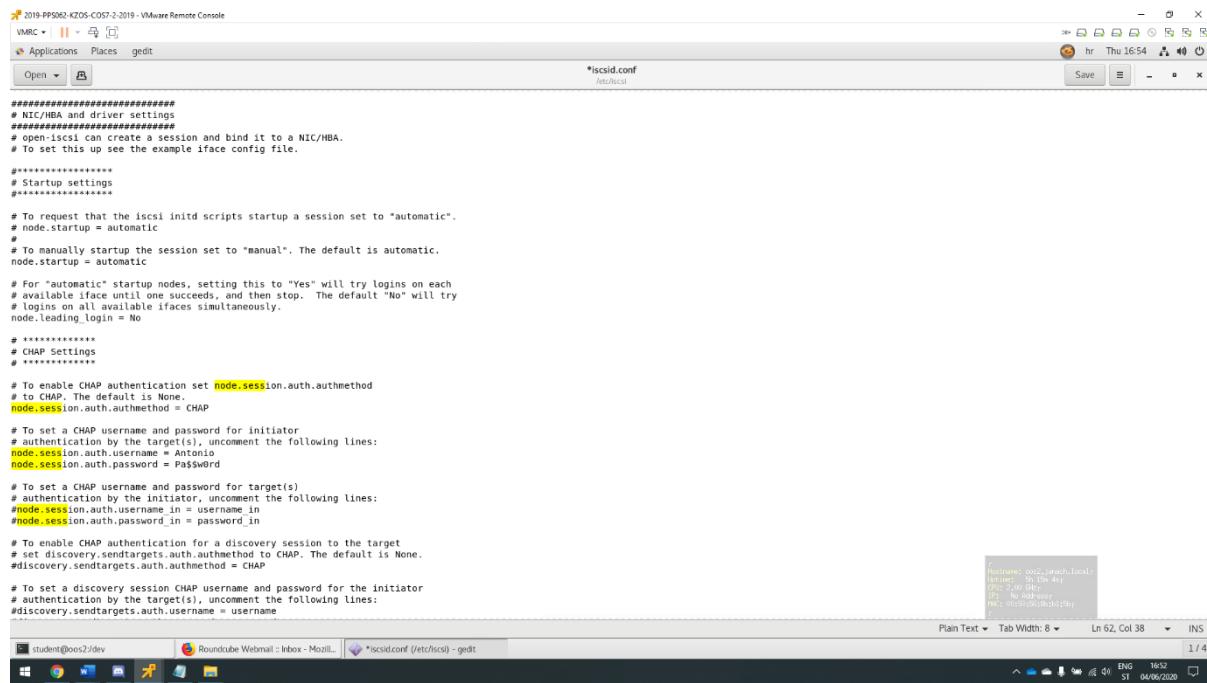
/iscsi>
```

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.



```
#####
# NIC/HBA and driver settings
#####
# open-iscsi can create a session and bind it to a NIC/HBA.
# To set this up see the example iface config file.

#####
# Startup settings
#####

# To request that the iscsi initd scripts startup a session set to "automatic".
# node.startup = automatic
#
# To manually startup the session set to "manual". The default is automatic.
node.startup = automatic

# For "automatic" startup nodes, setting this to "Yes" will try logins on each
# available iface until one succeeds, and then stop. The default "No" will try
# logins on all available ifaces simultaneously.
node.reaching_login = No

#####
# CHAP Settings
#####

# To enable CHAP authentication set node.session.auth.authmethod = CHAP
# to CHAP. The default is None.
node.session.auth.authmethod = CHAP

# To set a CHAP username and password for initiator
# authentication by the target(s), uncomment the following lines:
node.session.auth.username = Antonio
node.session.auth.password = Pa$$word

# To set a CHAP username and password for target(s)
# authentication by the initiator, uncomment the following lines:
#node.session.auth.username_in = username_in
#node.session.auth.password_in = password_in

# To enable CHAP authentication for a discovery session to the target
# set discovery.sendtargets.auth.authmethod to CHAP. The default is None.
#discovery.sendtargets.auth.authmethod = CHAP

# To set a discovery session CHAP username and password for the initiator
# authentication by the target(s), uncomment the following lines:
#discovery.sendtargets.auth.username = username
```

Slika 16: prikaz konfiguracije iscsid.conf

Na OOS1 računalu instalirati iscsi-initiator za client računalo 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:

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

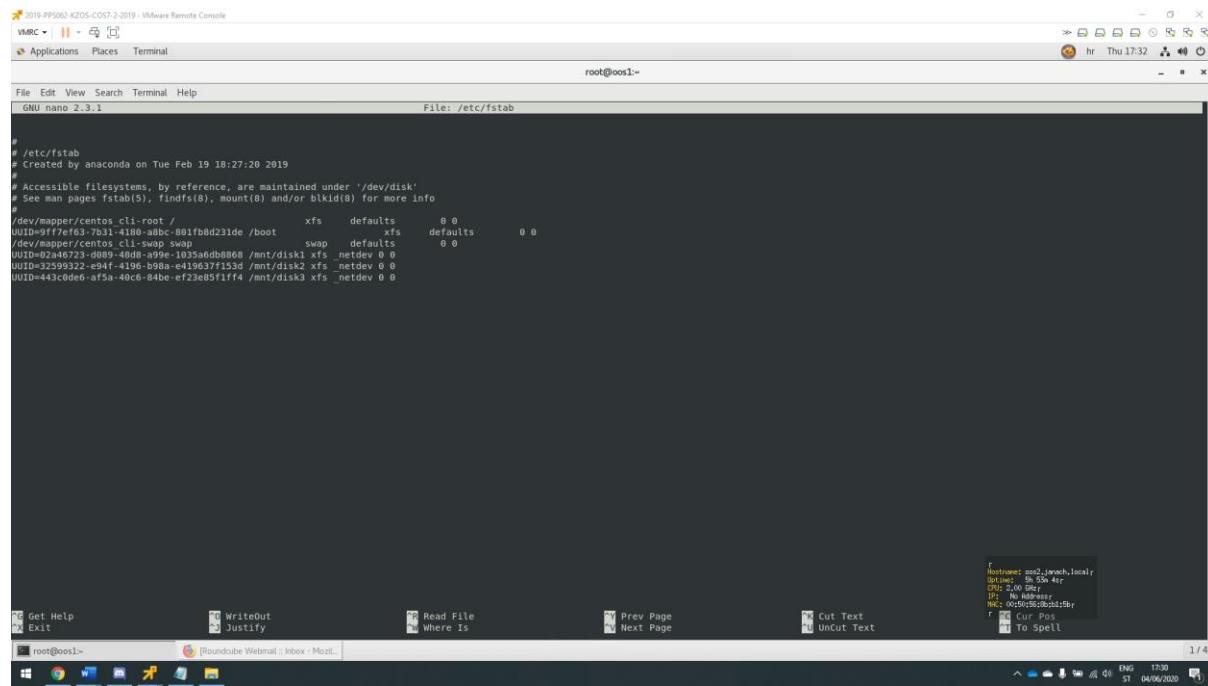
Ulogirati se na discover-ani target.

```
Iscsiadm -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 tako nužno je dodati _netdev kako bi iSCSI bio mountan prije boot-a.

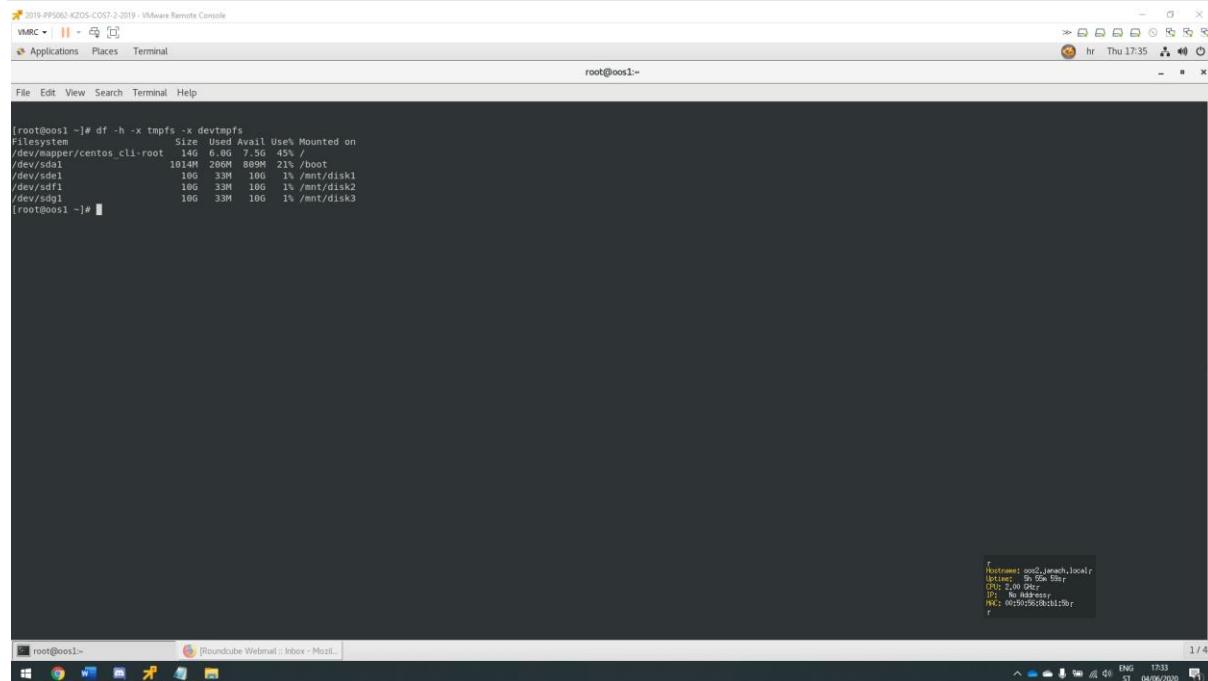


```
# /etc/fstab
# Created by anaconda on Tue Feb 19 18:27:28 2019
#
# Accessible filesystems, by reference, are maintained under '/dev/disk'
# See man pages fstab(5), findfs(8), mount(8) and/or blkid(8) for more info
#
# /dev/mapper/centos_cli-root /
xfs defaults 0 0
UUID=0ff7ef63-7b31-4180-abbc-801fb8d231de /boot xfs defaults 0 0
# /dev/mapper/centos_cli-swap swap swap defaults 0 0
UUID=d2a46723-d889-4e96-1b5a-afdb8868 /mnt/disk1 xfs _netdev 0 0
UUID=441c0ded-af5b-419c-bc4e-42637f153d /mnt/disk2 xfs _netdev 0 0
UUID=441c0ded-af5b-419c-bc4e-42637f153d /mnt/disk3 xfs _netdev 0 0
```

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

Provjeriti da li su diskovi mount-ani.

Df -h -x tmpfs -x devtmpfs



```
[root@oos1 ~]# df -h -x tmpfs -x devtmpfs
Filesystem      Size  Used Avail Use% Mounted on
/dev/mapper/centos_cli-root 14G  6.8G  7.5G  45% /
/dev/sda1       1014M  208M  899M  21% /boot
/dev/sdb1        10G   33M  10G   1% /mnt/disk1
/dev/sdf1        10G   33M  10G   1% /mnt/disk2
/dev/sdg1        10G   33M  10G   1% /mnt/disk3
[root@oos1 ~]#
```

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

```
# Postfix master process configuration file. For details on the format  
# of the file, see the master(5) manual page (command: "man 5 master").  
#  
# Do not forget to execute "postfix reload" after editing this file.  
#  
# ======  
# service type private unpriv chroot wakeup maxproc command + args  
# (yes) (yes) (yes) (never) (100)  
# ======  
smtp inet - - - smtpd  
#smtp inet n n 1 postscreen  
#smtpd pass - - - smtpd  
#dnsblog unix - n 0 dnsblog  
#tspox unix - n 0 tsproxy  
#submktcp inet n n - smtpd  
-o syslog name=postfix/submission  
-o smtpd tls security_level=encrypt  
-o smtpd sasl_auth_enable=yes  
# -o smtpd reject_unlisted_recipient=no  
# -o smtpd restrictions=$mua client restrictions  
# -o smtpd helo_restrictions=$mua helo restrictions  
# -o smtpd sender_restrictions=$mua sender restrictions  
# -o smtpd recipient_restrictions=permit_sasl_authenticated,reject  
-o milter_macro_daemon_name=ORIGINATING  
#smtps inet n n - - smtpd  
# -o syslog name=postfix/smtps  
# -o smtpd tls_wrappermode=yes  
# -o smtpd sasl auth enable=yes  
# -o smtpd reject_unlisted_recipient=no  
# -o smtpd restrictions=$mua client restrictions  
# -o smtpd helo_restrictions=$mua helo restrictions  
# -o smtpd sender_restrictions=$mua sender restrictions  
# -o smtpd recipient_restrictions=permit_sasl_authenticated,reject  
-o milter_macro_daemon_name=ORIGINATING  
#ecp inet n n - - qmqpd  
pickup unix n n 60 1 pickup  
cleanup unix n - - 0 cleanup  
qmgr unix n - n 300 1 qmgr  
#qmgr unix n - n 300 1 qmgr  
tlsmgr unix - n 1000? 1 tlsmgr  
rewrite unix - - - trivial-rewrite  
bounce unix - - - 0 bounce  
defer unix - - - 0 bounce  
trace unix - - - 0 bounce  
verify unix - - - 1 verify  
flush unix n - - 1000? 0 flush
```

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

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

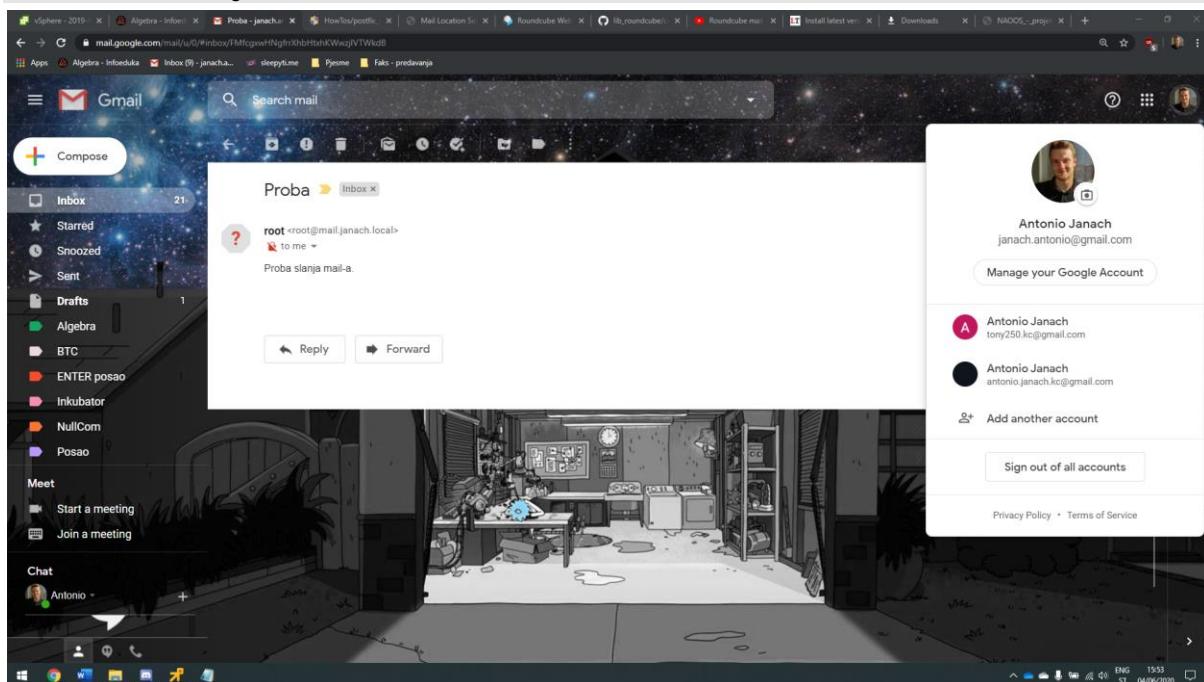
```
Vim /etc/postfix/mail.cf
Myhostname = main.janach.local
Mydomain = janach.local
Myorigin = $myhostname
Inet_interface = all
Inet_protocol = all
Mydestination = $myhostname, localhost.$mydomain,localhost
```

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

```
Systemctl restart postfix
```

Pokušati poslati mail:

```
Mail -s Proba janachantonio@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 = mailldir:~/mailldir
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;
```

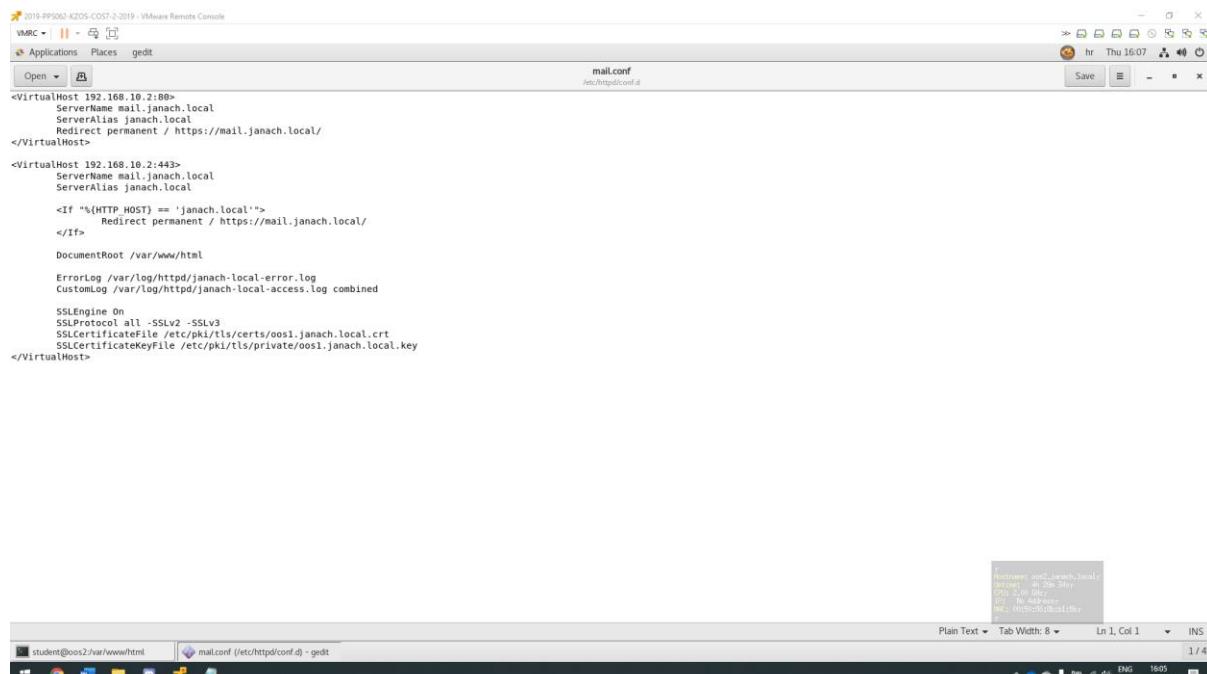
Preuzeti s interneta Roundcube i prebaciti ga u file /var/www/html

```
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



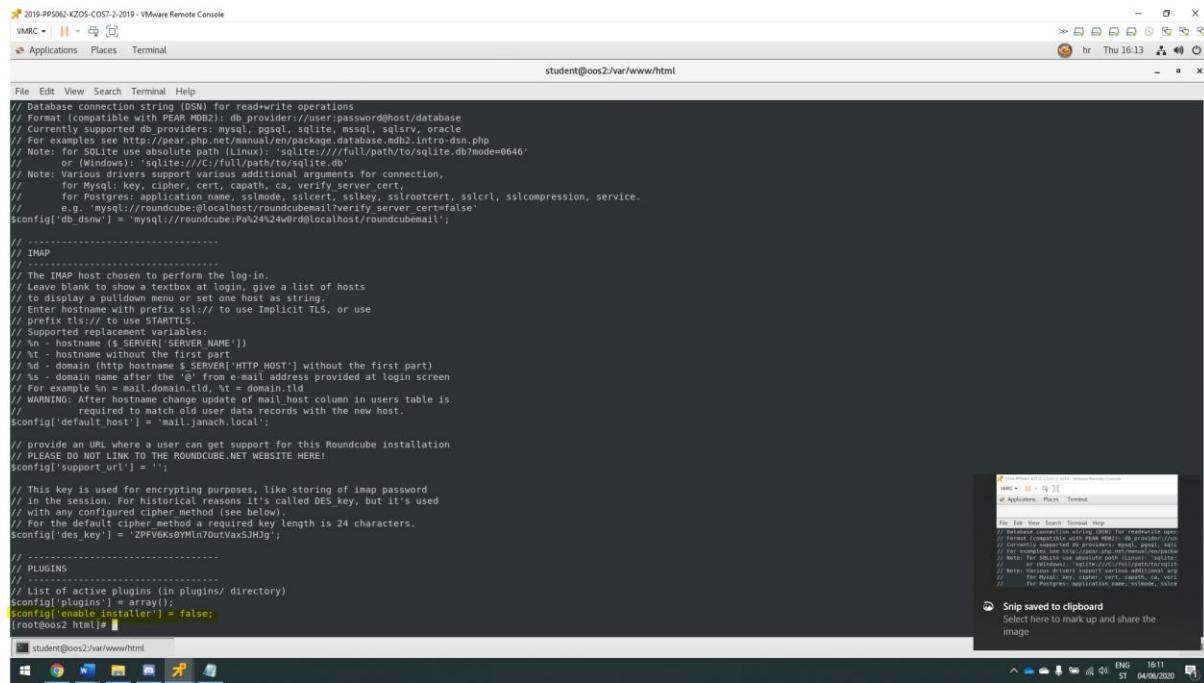
Slika 21: prikaz konfiguracije mail.conf file-a

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\$S\$w0rd). Nakon toga izbrisati instalaciju u folderu. `rm -rf /var/www/html/roundcubemail/config/config.inc.php`



```
// Database connection string (DSN) for read/write operations
// Format: $config['db_dsnw'] = 'db provider://username:password@host/database';
// Currently supported db providers: mysql, mysqli, sqlite, mssql, sqlsrv, oracle
// For examples see http://pear.php.net/manual/en/package.database.mdb2.intro-dsn.php
// Note: for SQLite use absolute path (Linux): 'sqlite:///full/path/to/sqlite.db?mode=0646'
// or (Windows): 'sqlite:///C:/full/path/to/sqlite.db'
// Note: Various drivers support various additional arguments for connection,
// for MySQL: key, cipher, cert, ca, verify_server_cert, sslcert, sslkey, sslrootcert, sslcompression, service.
// e.g. 'mysql://roundcube:@localhost/roundcubemail?verify_server_cert=false'
$config['db_dsnw'] = 'mysql://roundcube:@localhost/roundcubemail?verify_server_cert=false';

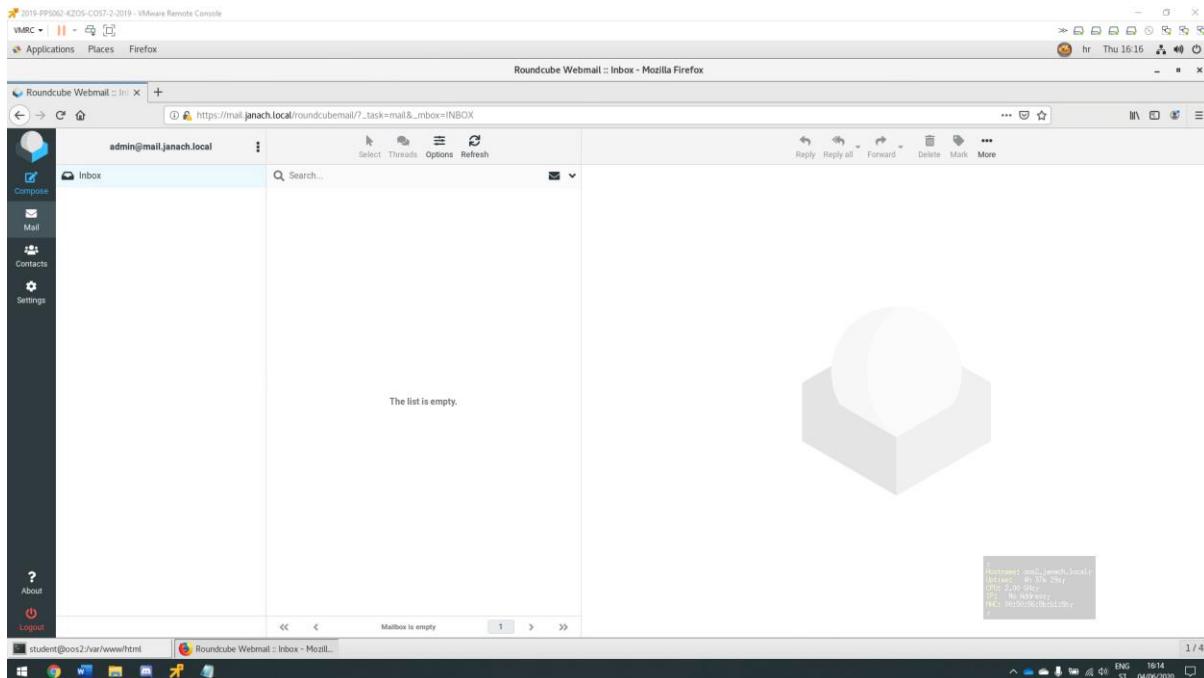
-----
// IMAP
// The IMAP host chosen to perform the log-in.
// Leave blank to let the user pick from a list of hosts
// to display a pulldown menu or set one host as string.
// Enter hostname with prefix ssl:// to use Implicit TLS, or use
// prefix tls:// to use STARTTLS.
// Supported replacement variables:
// %n - hostname (% SERVER_NAME')
// %t - domain without the first part
// %d - domain (http hostname $ SERVER[HTTP_HOST] without the first part)
// %s - domain name after the @ from e-mail address provided at login screen
// For example %n = mail.domain.tld, %t = domain.tld
// WARNING: After changing this, update the mail_host column in users table is
// referred to old user data records with the new host.
$config['default_host'] = 'mail.janach.local';

// provide an URL where a user can get support for this Roundcube installation
// PLEASE DO NOT LINK TO THE ROUNDUCUBE.NET WEBSITE HERE!
$config['support_url'] = '';

// This key is used for encrypting purposes, like storing of imap password
// in the session. For historical reasons it's called DES_key, but it's used
// with an unmodified cipher method (see below).
// For security reasons this method a required key length is 24 characters.
$config['des_key'] = '2PFV6kx5YHln7u0vTxaxSHdg';

-----
// PLUGINS
// -----
// List of active plugins (in plugins/ directory)
$config['plugins'] = array();
$config['enable_installer'] = false;
[root@oos2 ~]#
```

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
```

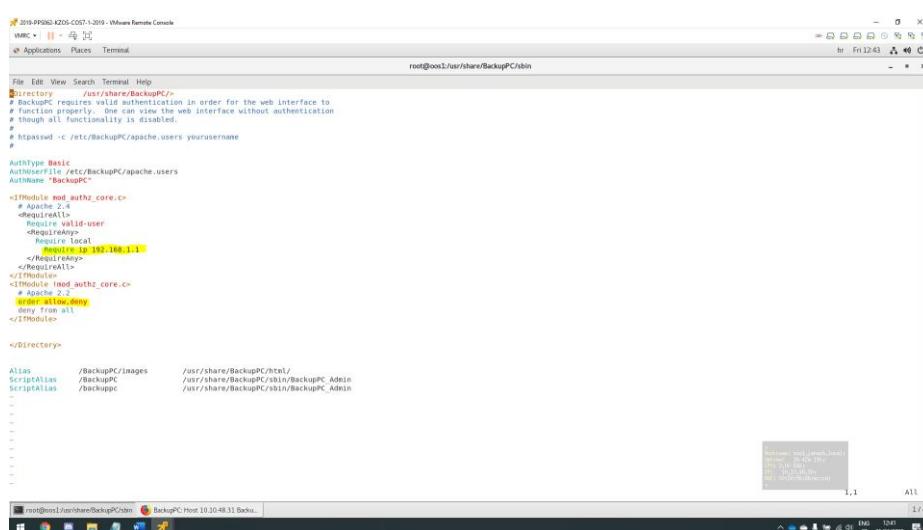
Omogućiti portove na firewall-u.

```
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 poleđinu 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.

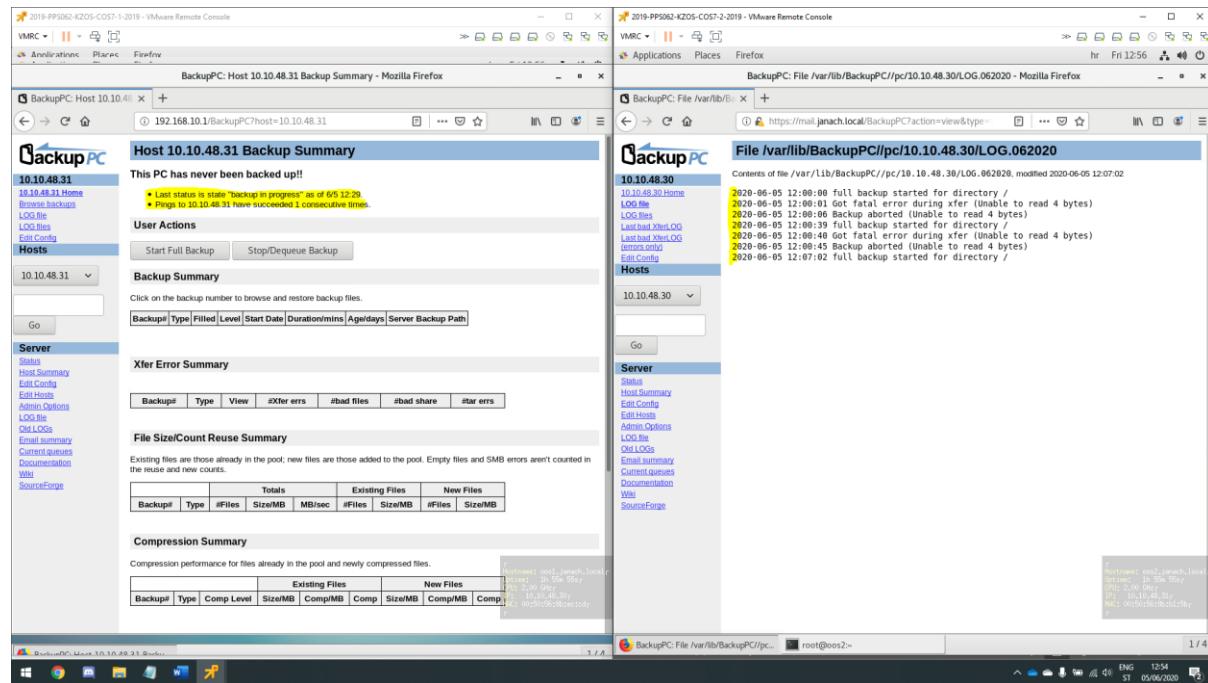
```
Systemctl restart httpd  
Systemctl restart backuppc
```

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 0052 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 računalu.

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\$\$wOrd). 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]# ./easyrsa --batch my-openvpn.ppp my-openvpn.te openvpn.log openvpn.tlsauth server server.conf
[root@oos2 openvpn]# cd easy-rsa/3/pki/
[root@oos2 pkcs12]# ls
ca.crt  cert.pem  dh.pem  index.txt  index.txt.attr  index.txt.attr.old  index.txt.old  issued  openssl-easyrsa.cnf  private  renewed  reqs  revoked  safessl-easyrsa.cnf  serial  serial.old
[root@oos2 pkcs12]# cd issued/
[root@oos2 issued]# ls
client.crt  oos2.janach.local.crt
[root@oos2 issued]# cd ..
[root@oos2 pkcs12]# private/
[root@oos2 private]# ls
ca.crt  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, oglasiti 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
```

Sad je sve izgenerirane ključeve i certifikate potrebno poslati na oos1 klijentsko računalo putem smtp-a, no prije toga je potrebno generirati SSH ključ na oos2 računalu i kopirati ključ na oos1 računalo.

```
[root@oos2 openvpn]# ssh -t rsa
ssh exchange identification: Connection closed by remote host
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
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:ym@05d1yQ42N4QzcepVieZsvfcdXj2lFLVu9gF0cw root@oos2.janach.local
The key's randomart image is:
+---[RSA 2048]---+
|          oB8|
|         o  O|
|        + * . .|
|       = X ..+ |
|      = B S ..o..|
|     = * . . . .|
|    +*o.. . . .|
|   ==o.o . . .|
|  .ooo. . . .|
| .oooo. . . .|
|+ooooo. . . .|
|+oooooo. . . .|
[root@oos2 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@oos2 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 192.168.1.1
[Root@oos1 ~]# exit
logout
Connection to 192.168.1.1 closed.
[root@oos2 openvpn]#
[root@oos2 openvpn]#
```

Details Window:

Hostname:	oos2.janach.local
Uptime:	8h 38m 50s
OS:	CentOS Linux
IP:	10.10.49.31
MAC:	00:0C:8B:3B:0D:59

Taskbar:

- root@oos2:/etc/openvpn
- BackupPC Host 10.10.48.30 Backup...
- SELinux Alert Browser
- SETroubleshoot Details Window

System tray:

- ENG 19:35
- ST 05/06/2020

Slika 28: prikaz generiranja ključeva na OOS2 računalu

```
2019-P95062-KZOS-C057-2-2019 - VMware Remote Console
VMRC - | II - ☰
Applications Places Terminal
root@oos2:/etc/openvpn

File Edit View Search Terminal Help
conky_desktop initial-setup-ks.cfg kracket.p12 openvpn.tlsauth
vmware-tools-distrib yum.repos.d.ne.dirs
sftp> cd /etc/openvpn
openvpn> pk1 pk1 issuedsec/ openldap/ openvpn/
sftp> cd /etc/openvpn/
sftp> put /etc/openvpn/
openldap/ openvpn/
sftp> cd pk1/
sftp> pwd
Working directory: /etc/openvpn/pki
sftp> put /etc/openvpn/easy-rsa/3/pki/ca.crt
Uploading /etc/openvpn/easy-rsa/3/pki/ca.crt to /etc/openvpn/pki/ca.crt
/etc/openvpn/easy-rsa/3/pki/ca.crt                                100% 1196  949.1KB/s  00:00
sftp> put /etc/openvpn/easy-rsa/3/pki/ca.crt
3.0.7/ 3.0/ 3
Uploading /etc/openvpn/easy-rsa/3/pki/ca.crt to /etc/openvpn/pki/ca.crt
/etc/openvpn/easy-rsa/3/pki/ca.crt                                100% 4630  2.5MB/s  00:00
sftp> put /etc/openvpn/easy-rsa/3/pki/issued/client.crt
Uploading /etc/openvpn/easy-rsa/3/pki/issued/client.crt to /etc/openvpn/pki/client.crt
/etc/openvpn/easy-rsa/3/pki/issued/client.crt                      100% 4460  4.4MB/s  00:00
sftp> put /etc/openvpn/easy-rsa/3/pki/private/client.key
Uploading /etc/openvpn/easy-rsa/3/pki/private/client.key to /etc/openvpn/pki/client.key
/etc/openvpn/easy-rsa/3/pki/private/client.key                     100% 1704  1.1MB/s  00:00
sftp> cd /etc/openvpn/
sftp> put /etc/openvpn/openvpn.tlsauth
openvpn.log 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/firewall/direct.xml
[Root@oos2 openvpn]# /etc/openvpn
[Root@oos2 openvpn]# ls
ls: cannot access /etc/openvpn/openvpn.log: No such file or directory
ls: cannot access /var/log/openvpn/openvpn.log: No such file or directory
[Root@oos2 openvpn]# gedit /var/log/openvpn/server.conf
[Root@oos2 openvpn]# systemctl restart openvpn@server
[Root@oos2 openvpn]# gedit /var/log/openvpn/openvpn.log
[Root@oos2 openvpn]# grep -r "openvpn" /var/log/openvpn/openvpn.log
[Root@oos2 openvpn]# search openvpn -new -f "audit2allow -M my-openvpn"
***** IMPORTANT *****
```

Details Window:

Hostname:	oos2.janach.local
Uptime:	8h 39m 20s
OS:	CentOS Linux
IP:	10.10.49.31
MAC:	00:0C:8B:3B:0D:59

Taskbar:

- root@oos2:/etc/openvpn
- BackupPC Host 10.10.48.30 Backup...
- SELinux Alert Browser
- SETroubleshoot Details Window

System tray:

- ENG 19:28
- ST 05/06/2020

Slika 29: prikaz uspješno poslanih ključeva na OOS1 računalo

Sljedeće naredbe potrebno je upisati u terminal OOS1 računala koje u ovome slučaju služi kao klijentsko 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]#
```

Slika 30: prikaz uspješno posalnih certifikata na OOS1 računalo

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

Slika 31: prikaz kreiranoq client.ovpn file-a

Spojiti se klijentom pomoću VPN-a na oos2 računalo.

```
openvpn -config /etc/openvpn/client.ovpn
2018-PP0000-A205-C007-1-2019 - VMware Remote Console
VMRC - || - Applications Places Terminal
File Edit View Search Terminal Help
root@os1:/etc/openvpn

[root@os1 openvpn]# openvpn --config /etc/openvpn/client.ovpn
Fri Jun 5 17:48:40 2020 OpenVPN 2.4.9 x86_64-redhat-linux-gnu [Fedora EPEL patched] [SS] [OpenSSL3] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] built on Apr 24 2020
Fri Jun 5 17:48:40 2020 Library versions: OpenSSL 1.0.2k-fips 26 Jan 2017, LZO 2.0.6
Fri Jun 5 17:48:40 2020 Outgoing Control Channel Encryption: Using 256 bit message hash 'SHA256' for HMAC authentication
Fri Jun 5 17:48:40 2020 Incoming Control Channel Encryption: Cipher 'AES-256-CTR' initialized with 256 bit key
Fri Jun 5 17:48:40 2020 Incoming Control Channel Encryption: Using 256 bit message hash 'SHA256' for HMAC authentication
Fri Jun 5 17:48:40 2020 TCP/UDP: Preserving recently used remote address: [AF_INET]192.168.10.2:1194
Fri Jun 5 17:48:40 2020 Socket level: Reusing existing connection to 192.168.10.2:1194
Fri Jun 5 17:48:40 2020 UDP link local: not bound
Fri Jun 5 17:48:40 2020 UDP link remote: [AF_INET]192.168.10.2:1194
Fri Jun 5 17:48:40 2020 TLS: Initial remote peer connection established
Fri Jun 5 17:48:40 2020 VERIFY OK: depth=1 CN=oos2.janach.local
Fri Jun 5 17:48:40 2020 VERIFY OK: depth=0 CN=oos2.janach.local
Fri Jun 5 17:48:40 2020 Validating certificate extended key usage
Fri Jun 5 17:48:40 2020 Certificate has EKU (str) TLS Web Server Authentication, expects TLS Web Server Authentication
Fri Jun 5 17:48:40 2020 VERIFY EKU OK
Fri Jun 5 17:48:40 2020 VERIFY X509NAME OK: CN=oos2.janach.local
Fri Jun 5 17:48:40 2020 VERIFY OK: depth=0, CN=oos2.janach.local
Fri Jun 5 17:48:40 2020 Peer connection initialized with [AF_INET]192.168.10.2:1194
Fri Jun 5 17:48:40 2020 SENT CONTROL [oos2.janach.local]: "PUSH REQUEST" (status=1)
Fri Jun 5 17:48:40 2020 PUSH: Received control message: "PUSH 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 17:48:40 2020 PUSH: Peer connection modified
Fri Jun 5 17:48:40 2020 OPTIONS IMPORT: --ifconfig option modified
Fri Jun 5 17:48:40 2020 OPTIONS IMPORT: route options modified
Fri Jun 5 17:48:40 2020 OPTIONS IMPORT: route-related options modified
Fri Jun 5 17:48:40 2020 OPTIONS IMPORT: --ip-win32 and/or --dhcp-option options modified
Fri Jun 5 17:48:40 2020 OPTIONS IMPORT: peer-id set
Fri Jun 5 17:48:40 2020 OPTIONS IMPORT: --link-mtu 1657
Fri Jun 5 17:48:40 2020 OPTIONS IMPORT: data channel crypto options modified
Fri Jun 5 17:48:40 2020 Data Channel: using negotiated cipher 'AES-256-GCM'
Fri Jun 5 17:48:40 2020 Outgoing Data Channel: Cipher 'AES-256-GCM' initialized with 256 bit key
Fri Jun 5 17:48:40 2020 Incoming Data Channel: Cipher 'AES-256-GCM' initialized with 256 bit key
Fri Jun 5 17:48:40 2020 TUN/TAP interface GATEWAY [10.51.254.255.252.0] IPACE=ens192 HWADDR=00:50:56:8b:ec:cd
Fri Jun 5 17:48:40 2020 TUN/TAP device tun0 opened
Fri Jun 5 17:48:40 2020 TUN/TAP TX queue length set to 100
Fri Jun 5 17:48:40 2020 /sbin/ip link set dev tun0 mtu 1500
Fri Jun 5 17:48:40 2020 /sbin/ip link add dev tun0 type tun ip 172.16.100.1 brd broadcast 172.16.100.255
Fri Jun 5 17:48:40 2020 /sbin/ip route add 192.168.10.2/32 via 10.51.254.254
Fri Jun 5 17:48:40 2020 /sbin/ip route add 0.0.0.0/0 via 172.16.100.1
Fri Jun 5 17:48:40 2020 /sbin/ip route add 128.0.0.0/0 via 172.16.100.1
Fri Jun 5 17:48:40 2020 Initialization Sequence Completed
```

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

Provjeriti ifconfig naredbom da li je računalu dodjeljena IP adresa.

```

root@oos1:/etc/openvpn]#

```

Slika 33: prikaz dodjeljene IP adrese

OpenVPN je uspješno konfiguriran.

```

[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=3.68 ms
64 bytes from 172.16.100.1: icmp_seq=2 ttl=64 time=3.72 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=0.452 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
```
...
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]#

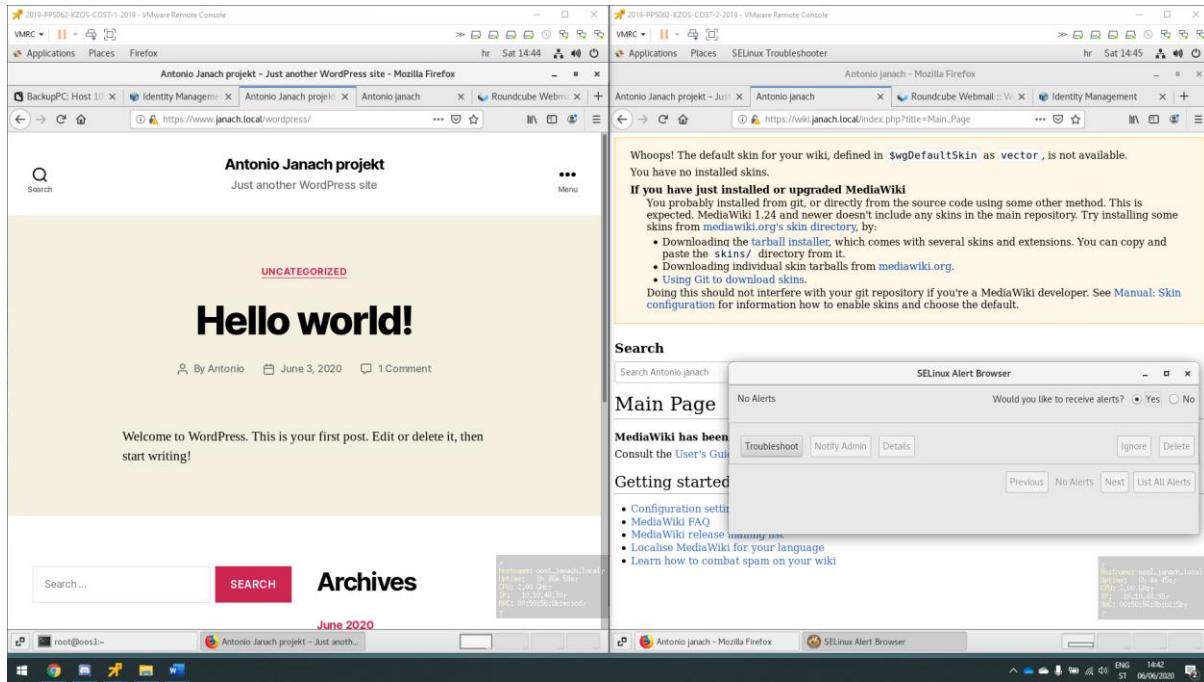
[root@oos2 openvpn]# ping 172.16.100.2
PING 172.16.100.2 (172.16.100.2) 56(84) bytes of data.
64 bytes from 172.16.100.2: icmp_seq=1 ttl=64 time=4.01 ms
64 bytes from 172.16.100.2: icmp_seq=2 ttl=64 time=0.774 ms
64 bytes from 172.16.100.2: icmp_seq=3 ttl=64 time=1.00 ms
64 bytes from 172.16.100.2: icmp_seq=4 ttl=64 time=0.53 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=0.441 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
```
...
9 packets transmitted, 9 received, 0% packet loss, time 8004ms
rtt min/avg/max/mdev = 0.441/1.010/6.536/2.054 ms
[root@oos2 openvpn]#

```

Slika 34: prikaz uspješne konfiguracije OpenVPN-a

5.7. Semanage

U semanage-u riješeni su svi aleart-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 zapisa	4
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 promjeniti 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 platofrme.....	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 računalo.....	24
Slika 30: prikaz uspješno posalnih certifikata na OOS1 računalo	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.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.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.ssdnodeds.com/blog/install-openvpn-centos-7-tutorial/>