|  |
| --- |
| Banca Intesa Beograd |
| Mail-out.Instalacija i konfiguracija |
|  |

|  |
| --- |
| Predrag Grozdanić  5/24/2017 |

Instaliranje sistema i početno podešavanje

Na VM instalirati CentOS 7.3. Za uspešnu instalaciju sistema neophodan je normalan internet preko proxy uređaja, bez autentikacije.

Najpodesnije je instalirati system preko kreiranog PXE Sistema i lokalnog repository-a jer se system instalira po već utvrđenom template-u. Ukoliko je nemoguće koristiti lokalni repository, system instalirati preko ISO fajla na kome se nalazi instalacija CentOS-a.

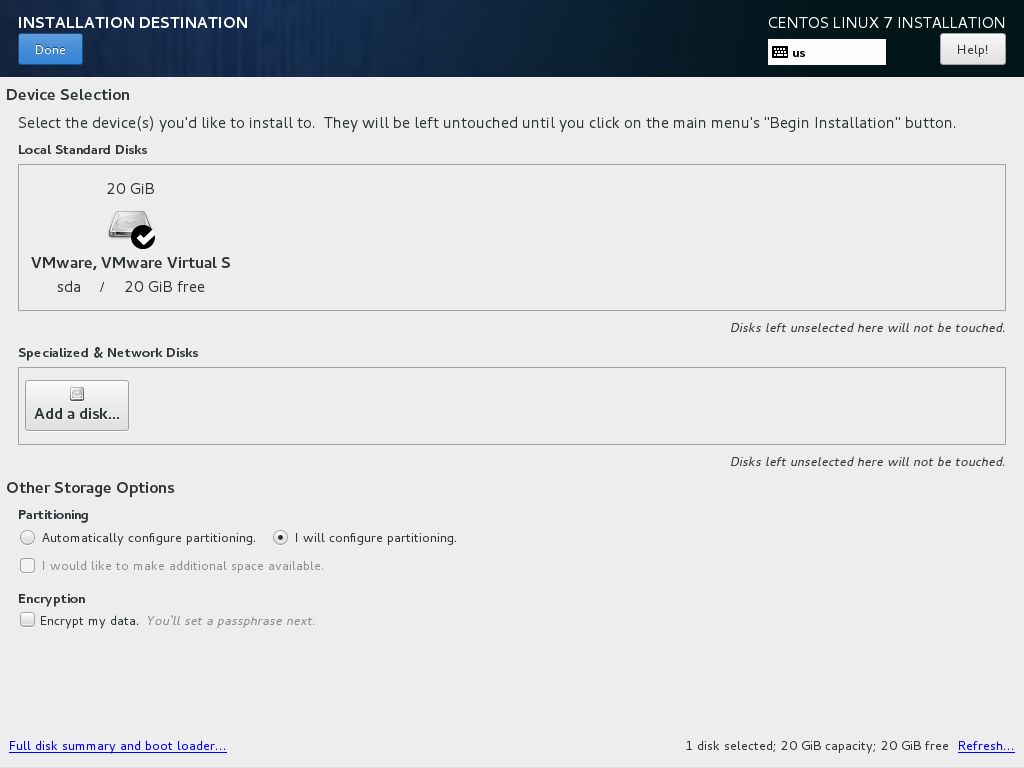
Za post-konfiguraciju, koristiti fajlove sa floppy image-a koji se nalazi na [\\fsi\ORG\DSL\Software\mail konfiguracija\config.flp](file:///\\fsi\ORG\DSL\Software\mail%20konfiguracija\config.flp) i koji treba privezati na VM.

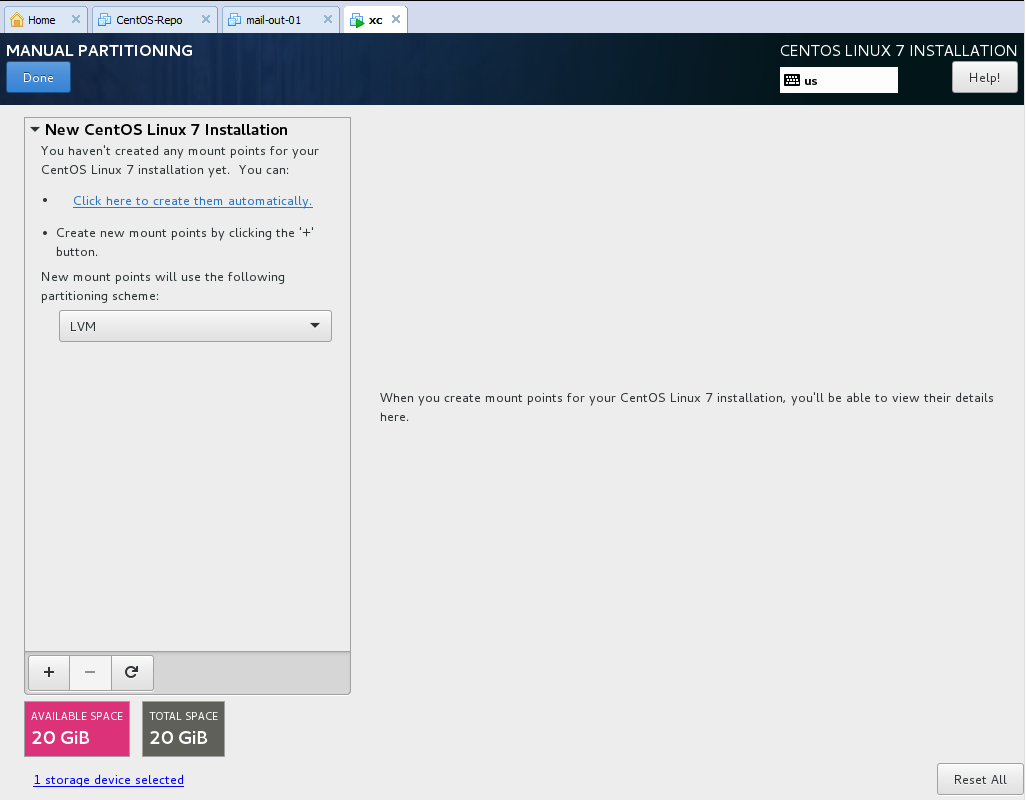
Ukoliko je zbog pregleda bolje da se podigne rezolucija na veću, tokom boot-ovanja a pre izbora **Install**, kliknuti na Tab taster i u liniju za komandu upisati komandu **vga=791** i pritisnuti Enter. Time će process instalacije proteći u rezoluciji 1024x768.

Prilikom instalacije, odabrati minimalnu instalaciju.

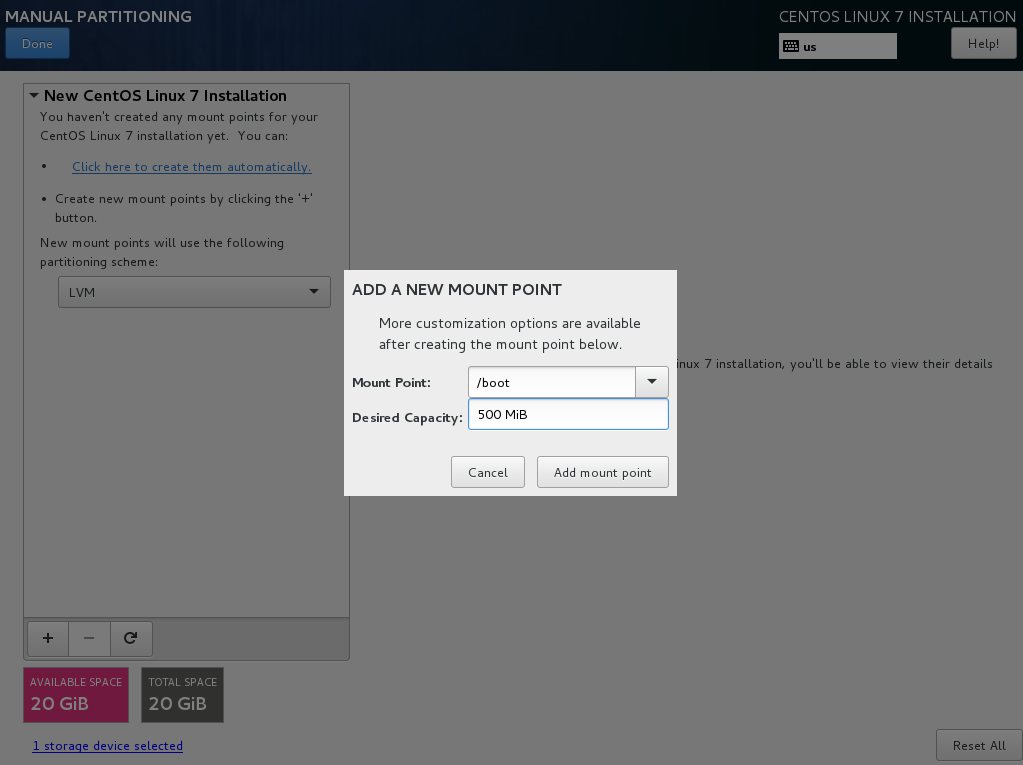
S obzirom da je tool za ručno particionisanje hard diska malo nelogičan a automatsko particionisanje najčešće kreira dodatne particije koje nemaju previse smisla u jednokorisničkim serverima, pa se particionisanje izvodi prema sledećim koracima.

Izabrati **I will configure partitioning** opciju i kliknuti na **Done**.

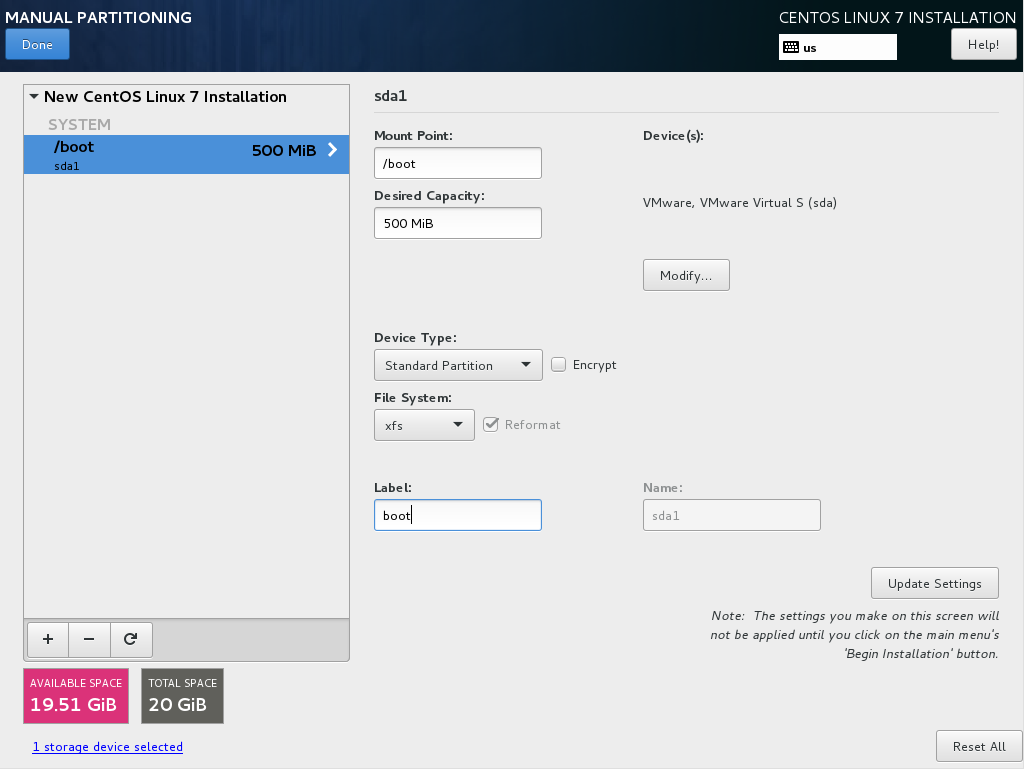




Kliknuti na **+** da bi se dodao mount point. Sasvim je dovoljno da se za **boot** particiju odredi 500 MB.

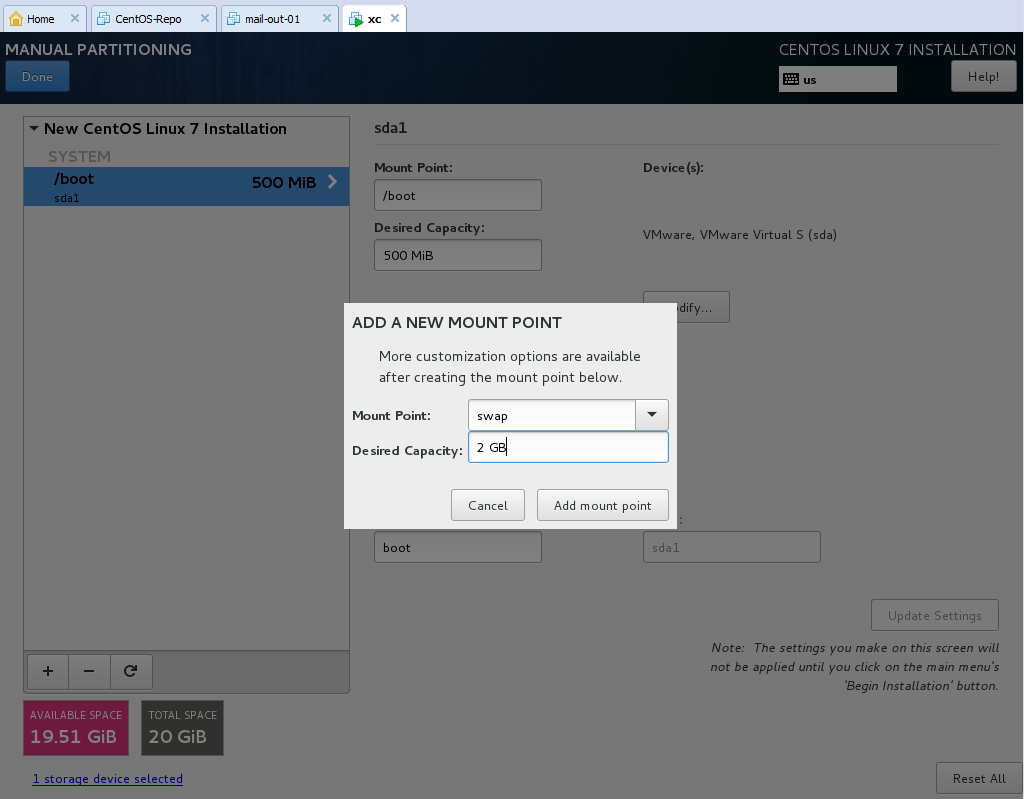


Dati ime **boot** particiji i kliknuti na **Update Settings**.

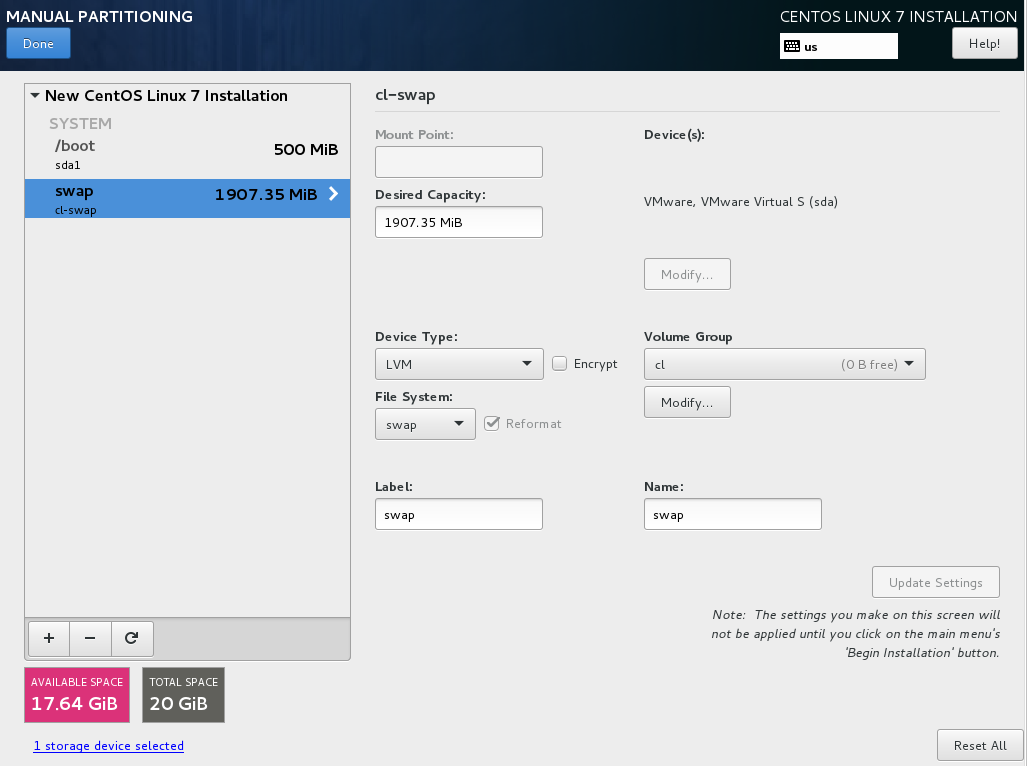


Kreirati **swap** particiju velicine 2 GB.

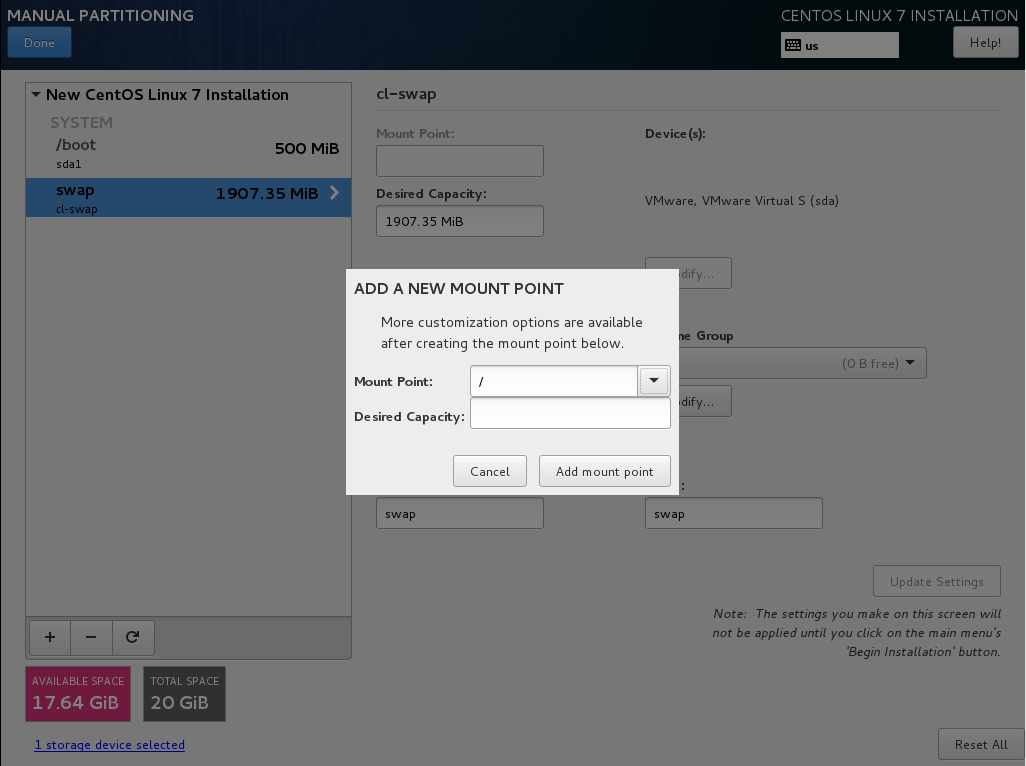
Po preporuci Red Hat-a, ukoliko je veličina RAM memorije do 2 GB, swap particiji dati minimum 2x više prostora na disku. Ukoliko je veličina RAM memorije do 8 GB, swap particiji dati istu toliku količinu prostora na disku a ukoliko je RAM memorija veća od 8 GB, swap particiji dati minimum 4 GB. U našem primeru, swap particiji ćemo dati 2 GB.



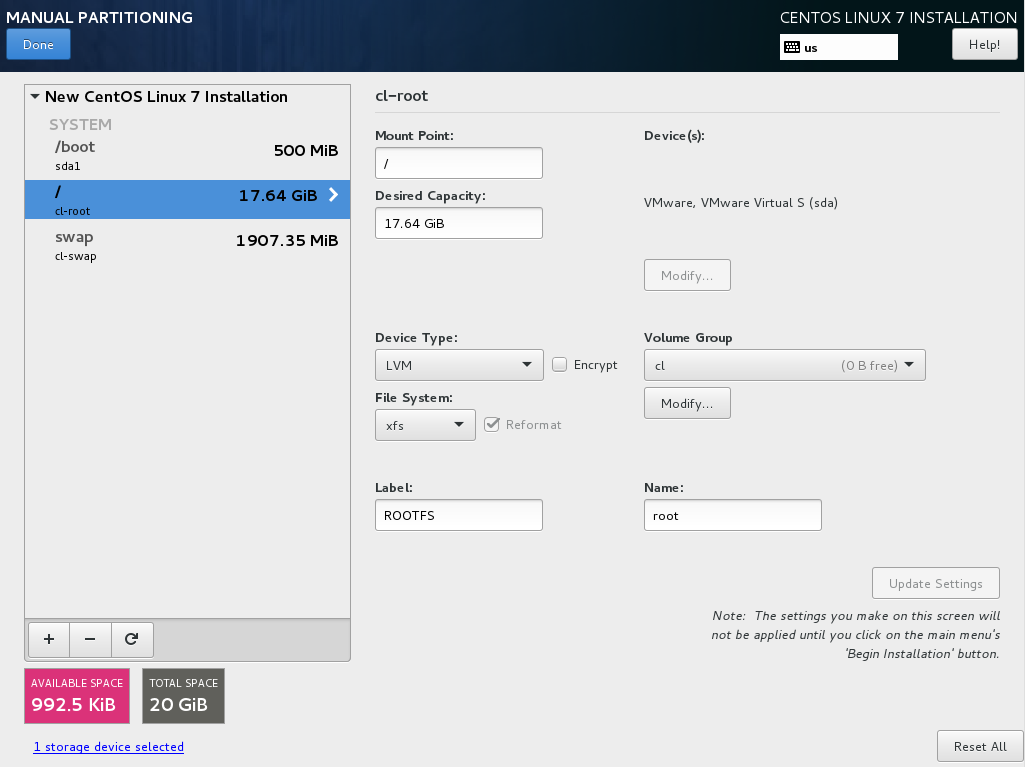
Upisati ime pod label i kliknuti na **Update Settings**.



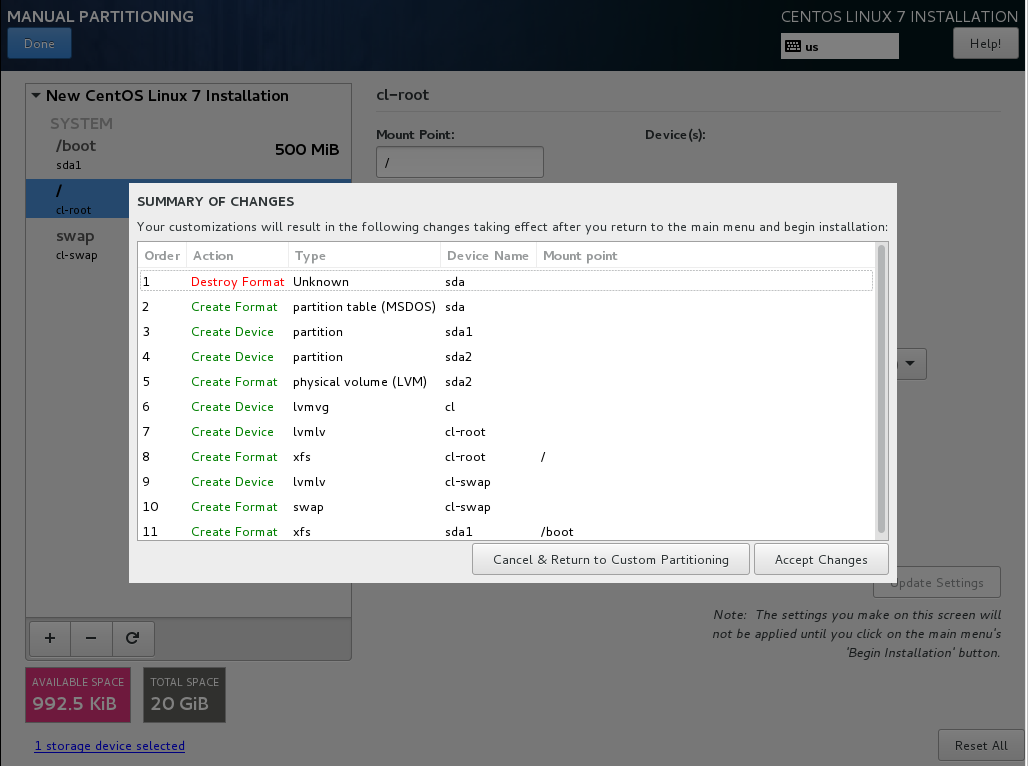
Napraviti root particiju bez upisivanja veličine jer će system automatski postaviti na preostali prostor.



Dati ime root particiji **ROOTFS** i kliknuti na **Update Settings**.



Kliknuti na **Done** i potvrditi sve korake na **Accept Changes**.



Postaviti root šifru.

Po startovanju sistema, podesiti mrežu i isključiti IPv6. Mrežnu karticu ens33 zameniti sa odgovarajućom, detektovanom na instaliranom sistemu.

Za editovanje konfiguracionih fajlova koristiti vi ili nano.

**PAŽNJA**: S obzirom da se prilikom kopiranja teksta iz označenih polja paste-uju nepostojeći karakteri (kao naprimer znak **”** koji ne postoji u terminal console-i), od velike važnosti je da se tekst iz označenih polja kopira u npr. Notepad pa iz Notepad-a u terminal console-u, liniju po liniju.

Izbegavati kopiranje više linija jer postoji mogucnoćnost da se paste-uju nepostojeći karakteri.

vi /etc/sysconfig/network-scripts/ifcfg-ens33

IPV6INIT="no"

DEVICE=ens33

BOOTPROTO=none

ONBOOT=yes

HWADDR=AA:BB:CC:DD:EE:FF # utvrditi tačnu MAC adresu

NETMASK=255.255.255.0

IPADDR=10.15.15.123

GATEWAY=10.15.15.1

TYPE=Ethernet

Obrisati NetworkManager pakete i restartovati server.

yum -y remove NetworkManager\*

Postaviti ime host-a i konfigurisati veću rezoluciju kako bi se normalno funkcionisalo u vSphere konzoli. **mail-out-01** zameniti **mail-out-02**.

vi /etc/hostname

mail-out-01.bancaintesabeograd.com

echo 'GRUB\_CMDLINE\_LINUX\_DEFAULT="nomodeset vga=791"' >> /etc/default/grub

grub2-mkconfig -o /boot/grub2/grub.cfg

reboot

Podesiti jezik sistema za sve korisnike. Na kraju fajla upisati liniju.

nano /etc/profile

export LANG=en\_US

Ubaciti potrebne DNS servere u resolv fajl.

nano /etc/resolv

########### Custom nameservers list for Banca Intesa ad Beograd ###########

search bancaintesabeograd.com

nameserver 10.15.15.17

nameserver 10.15.15.18

nameserver 10.15.1.17

nameserver 10.15.1.18

Instaliranje potrebnih paketa

Podesiti proxy podešavanja u konfiguracionim fajlovima. Koristiti Notepad za paste-ovanje.

vi /etc/profile

########### Custom proxy options for Banca Intesa ad Beograd ###########

export http\_proxy="http://10.15.15.15:8080/"

export https\_proxy="http://10.15.15.15:8080/"

export HTTP\_PROXY="http://10.15.15.15:8080/"

export HTTPS\_PROXY="http://10.15.15.15:8080/"

export ftp\_proxy="http://10.15.15.15:8080/"

export FTP\_PROXY="http://10.15.15.15:8080/"

vi /etc/yum.conf

########### Custom proxy options for Banca Intesa ad Beograd ###########

proxy=http://10.15.15.15:8080/

source /etc/profile

Instalirati dodatne pakete.

yum install nano wget net-tools mc deltarpm ntp syslog net-snmp net-snmp-utils telnet

Podesiti proxy podešavanje u konfiguracionom fajlu za **wget** paket.

nano /etc/wgetrc

########### Custom proxy options for Banca Intesa ad Beograd ###########

http\_proxy = http://10.15.15.15:8080/

https\_proxy = http://10.15.15.15:8080/

ftp\_proxy = http://10.15.15.15:8080/

Iskljuciti SeLinux.

setenforce 0

sed -i --follow-symlinks 's/^SELINUX=.\*/SELINUX=disabled/g' /etc/sysconfig/selinux && cat /etc/sysconfig/selinux

reboot

Update-ovati OS.

yum clean all

yum update

reboot

Instalirati EPEL repository i restartovati server.

yum install epel-release

yum clean all

Instalirati dodatne pakete za potrebe kompajliranja prerequisites-a.

yum install kernel-devel kernel-headers gcc binutils make dosfstools bind-utils

Proveriti da li se prilikom update-ovanja instalirao i paket open-vm-tools.

yum list installed | grep open-vm-tools

Instalirati potrebne pakete za MailScanner.

yum install perl unzip gcc patch rpm-build cpp perl-DBI perl-MIME-tools perl-DBD-SQLite binutils glibc-devel perl-Filesys-Df zlib zlib-devel automake perl-devel perl-LWP-Protocol-https perl-ExtUtils-CBuilder perl-Mail-SPF-Query perl-Module-Build perl-Net-CIDR-Lite perl-LDAP perl-Net-DNS perl-Sys-Hostname-Long

rpm -Uvh http://repo.openfusion.net/centos7-x86\_64/perl-Geography-Countries-2009041301-1.of.el7.noarch.rpm

rpm -Uvh http://repo.openfusion.net/centos7-x86\_64/perl-IP-Country-2.28-1.of.el7.noarch.rpm

rpm -Uvh https://driesrpms.eu/redhat/el7/en/x86\_64/dries.all/RPMS/perl-Mail-SPF-Query-1.999.1-2.el7.rf.noarch.rpm

Instalirati ClamAV pakete.

yum install clamav

yum install clamav-server clamav-data clamav-update clamav-filesystem clamav clamav-scanner-systemd clamav-devel clamav-lib clamav-server-systemd

Instalirati SpamAssassin paket.

yum install spamassassin

Instaliranje MailScanner paketa

Download-ovati tar.gz arhivu sa internet-a i raspakovati je. U trenutku kreiranja uputstva, MailScanner je download-ovan sa sajta ispod i bio je verzije 5.0.3-7.

cd /usr/local/src/

wget https://s3.amazonaws.com/msv5/release/MailScanner-5.0.3-7.rhel.tar.gz

tar xvzf MailScanner-5.0.3-7.rhel.tar.gz

cd MailScanner-5.0.3-7

./install.sh

Prilikom instalacije, odlučiti se za Postfix kao default-ni MTA a RAMDISK postaviti na 256.

S obzirom da je Postfix instaliran po default-u, na ponuđeno pitanje o instaliranju istog, odgovoriti odrečno, kao i na pitanja ispod.

Install an MTA? [1] : N

Do you want to install or update Clam AV during this installation process?

Recommended: Y (yes)

Install or update Clam AV? [n/Y] : N

Do you want to install or update Spamassassin?

Recommended: Y (yes)

Install or update Spamassassin? [n/Y] : N

Podešavanje sistema

Popuniti hosts fajl sa neophodnim podacima.

nano /etc/hosts

########### Custom hosts list for Banca Intesa ad Beograd ###########

127.0.0.1 mail-out-01.bancaintesabeograd.com mail-out-01 localhost.localdomain localhost

10.15.15.133 mail-out-02.bancaintesabeograd.com mail-out-02

10.15.15.123 mail-out-01.bancaintesabeograd.com mail-out-01

10.15.15.113 mail-in-02.bancaintesabeograd.com mail-in-02

10.15.15.143 mail-in-01.bancaintesabeograd.com mail-in-01

10.35.45.2 ex-fe1.deltabank.co.yu ex-fe1

10.35.45.26 ex-fe2.deltabank.co.yu ex-fe2

10.35.46.21 ex-node-01.deltabank.co.yu ex-node-01

10.35.46.22 ex-node-02.deltabank.co.yu ex-node-02

10.15.15.34 dlp-mail1.deltabank.co.yu dlp-mail1

10.15.15.35 dlp-mail2.deltabank.co.yu dlp-mail2

10.35.45.25 sccm-bg-01.deltabank.co.yu sccm

Proveriti status SeLinux servisa. Servis SeLinux je potrebno da bude u status **disabled**.

sestatus

SELinux status: disabled

Kopirati fajlove **authorized\_keys** i **known\_hosts** sa floppy image-a u folder /root/.ssh

Promeniti prava za kopirane fajlove unutar /root/.ssh foldera.

chmod 644 authorized\_keys

chmod 644 known\_hosts

Podešavanje Postfix paketa

Otvoriti fajl main.cf. Proveriti da li su podešavanja u fajlu nisu zamaskirana.

nano /etc/postfix/main.cf

queue\_directory = /var/spool/postfix

command\_directory = /usr/sbin

daemon\_directory = /usr/libexec/postfix

data\_directory = /var/lib/postfix

mail\_owner = postfix

mydestination = $myhostname, localhost.$mydomain, localhost

unknown\_local\_recipient\_reject\_code = 550

alias\_maps = hash:/etc/aliases

alias\_database = hash:/etc/aliases

debug\_peer\_level = 2

debugger\_command

sendmail\_path

newaliases\_path

mailq\_path

setgid\_group

html\_directory = no

manpage\_directory = /usr/share/man

sample\_directory

readme\_directory

Na kraju fajla ubaciti sledeća podešavanja.

########### Custom postfix options for Banca Intesa ad Beograd ###########

inet\_protocols = ipv4

myhostname = mail-out-01.bancaintesabeograd.com

mynetworks = 10.15.15.0/24, 10.15.1.0/24, 10.35.45.0/24, 192.168.0.0/21, 127.0.0.1, 10.35.46.0/24, 10.135.53.0/24

relay\_domains = intesaleasing.rs, bancaintesa.rs, bancaintesabeograd.com, mail-out-01.bancaintesabeograd.com, mail.deltabank.co.yu, localhost, 10.15.15.0/24, 10.15.1.0/24, 10.35.45.0/24, 192.168.1.0/24, 127.0.0.1, 10.35.46.0/24, 10.135.53.0/24

transport\_maps = hash:/etc/postfix/transport

disable\_vrfy\_command = yes

message\_size\_limit = 15240000

smtpd\_helo\_required = yes

maximal\_queue\_lifetime = 2d

bounce\_queue\_lifetime = 2d

delay\_warning\_time = 2h

mime\_header\_checks = regexp:/etc/postfix/mime\_header\_checks

header\_checks = regexp:/etc/postfix/header\_checks

smtpd\_recipient\_restrictions = permit\_mynetworks, reject\_unauth\_destination

fallback\_relay=10.15.15.133

smtp\_tls\_security\_level = may

smtp\_tls\_policy\_maps = hash:/etc/postfix/tls\_policy

smtp\_tls\_cert\_file = /etc/postfix/cert/smtpd.pem

smtp\_tls\_key\_file = /etc/postfix/cert/smtpd.key

smtp\_tls\_CAfile = /etc/postfix/cert/CAbundle.cer

tls\_random\_source = dev:/dev/urandom

smtp\_tls\_loglevel = 1

Kopirati sertifikate **smtpd.pem**, **smtpd.key** i **Cabundle.cer** u folder /etc/postfix/cert/

Kopirati fajl **tls\_policy** u folder /etc/postfix/

Uneti podatke u **transport** fajl.

nano /etc/postfix/transport

########### Custom transport rules for Banca Intesa ad Beograd ###########

mail-in-01.deltabanka.co.yu smtp:[10.15.15.143]

mail-in-01.bancaintesabeograd.com smtp:[10.15.15.143]

bancaintesabeograd.com smtp:[10.15.15.143]

bancaintesa.rs smtp:[10.15.15.143]

intesaleasing.rs smtp:[10.15.15.143]

intesaleasingbeograd.com smtp:[10.15.15.143]

deltabanka.co.yu smtp:[10.15.15.143]

Utvrditi da li u fajlu **/etc/postfix/header\_checks** postoji podešavanje a ukoliko ne postoji, uneti sledeće podešavanje.

nano /etc/postfix/header\_checks

########### Custom header\_checks options for Banca Intesa ad Beograd ###########

/^Received:/ HOLD

/^Subject:/ WARN

Disable-ovati i stopirati Postfix jer MailScanner pokrece Postfix prema potrebi.

systemctl stop postfix

systemctl disable postfix

Podešavanje ClamAV paketa

Radi bržeg skeniranja, na multiprocesorskim sistemima, poželjno je kreirati novu skriptu za skeniranje.

mv /usr/bin/clamdscan /usr/bin/clamdscan-cmd

nano /usr/bin/clamdscan

#!/bin/bash

########### Custom clamav scan for Banca Intesa ad Beograd ###########

/usr/bin/clamdscan-cmd --fdpass $@

chmod +x /usr/bin/clamdscan

Zamaskirati **Example** u fajlovima ispod.

sed -i /etc/freshclam.conf -r -e 's/^Example.\*/#Example/g'

sed -i /etc/clamd.d/scan.conf -r -e 's/^Example.\*/#Example/g'

U fajlu **/etc/freshclam.conf**  dodati sledeće redove.

DatabaseDirectory /var/lib/clamav

HTTPProxyServer 10.15.15.15

HTTPProxyPort 8080

Zamaskirati red koji počinje sa **FRESHCLAM\_DELAY=disabled-warn** sa komandom ispod.

sed -i /etc/sysconfig/freshclam -r -e 's/^FRESHCLAM\_DELAY=disabled-warn/#FRESHCLAM\_DELAY=disabled-warn/g'

Update-ovati clamav.

freshclam -v

Kreirati soft link da bi MailScanner mogao da update-uje bazu.

ln -s /usr/bin/freshclam /usr/local/bin/freshclam

Kreirati clamd daemon edit-ovanje fajla /etc/clamd.d/scan.conf i dodati sledeće linije na kraj fajla.

nano /etc/clamd.d/scan.conf

########### Custom clamd@scan options for Banca Intesa ad Beograd ###########

LogFile /var/log/clamd.scan

LogFileMaxSize 0

LogTime yes

LogSyslog yes

LogFacility LOG\_MAIL

PidFile /var/run/clamd.scan/clamd.pid

DatabaseDirectory /var/lib/clamav

LocalSocket /var/run/clamd.scan/clamd.sock

FixStaleSocket yes

TCPSocket 3310

TCPAddr 127.0.0.1

MaxConnectionQueueLength 30

MaxThreads 50

ReadTimeout 300

User clamscan #proveriti da li postoji korisnik clamscan

ScanPE yes

ScanELF yes

DetectBrokenExecutables yes

ScanOLE2 yes

ScanMail yes

ScanArchive yes

ArchiveBlockEncrypted no

MaxScanSize 50M

MaxFileSize 15M

MaxRecursion 5

MaxFiles 5000

Kreirati log fajl i podesiti neophodna prava.

touch /var/log/clamd.scan

chown :clamscan $\_

chmod 0660 $\_

Uključiti i startovati ClamAV servise.

systemctl enable clamd@scan

systemctl start clamd@scan

systemctl status clamd@scan

freshclam –v # update-ovanje ClamAV

Podešavanje SpamAssassin paketa

Proveriti konfiguraciju fajla /etc/mail/spamassassion/local.cf

Ukoliko SpamAssassin prijavljuje probleme u startovanju, edit-ovati fajl /etc/sysconfig/spamassassin i dodati **-4** u okviru navodnika.

nano /etc/sysconfig/spamassassin

SPAMDOPTIONS="-d -c -m5 -H"

^ ovde ubaciti **-**4 pa će nova komanda biti:

SPAMDOPTIONS="-d -c -m5 -H **-4**"

Startovanje SpamaAssassin servisa i update-ovanje.

systemctl enable spamassassin

systemctl start spamassassin

systemctl status spamassassin

sa-update

Podešavanje MailScanner paketa

Kreirati potrebne foldere i podesiti odgovarajuća prava.

mkdir /var/spool/MailScanner/spamassassin

chown postfix.postfix /var/spool/MailScanner/incoming

chown postfix.postfix /var/spool/MailScanner/quarantine

chown postfix /var/spool/MailScanner/spamassassin

chown postfix /var/spool/MailScanner/incoming/\*

chmod -R 770 /var/spool/MailScanner/incoming/

Podesiti konfiguraciju za MailScanner.

nano /etc/MailScanner/MailScanner.conf

%org-name% = BancaIntesa

%org-long-name% = Banca Intesa ad Beograd

%web-site% = www.bancaintesabeograd.com

Run As User = postfix

Run As Group = postfix

Incoming Queue Dir = /var/spool/postfix/hold

Outgoing Queue Dir = /var/spool/postfix/incoming

MTA = postfix

SpamAssassin User State Dir = /var/spool/MailScanner/spamassassin

Expand TNEF = no # na originalnom serveru je podeseno na NO

Use TNEF Contents = no # na originalnom serveru je podeseno na NO

Deliver Unparsable TNEF = yes # na originalnom serveru je podeseno na NO

Information Header Value = Please contact root@bancaintesabeograd.com for more information

Unscanned Header Value = Not scanned: please contact root@bancaintesabeograd.com for details

Use spamassassin = no # kod mail-out ne koristi se spamassassin

Proveriti podešavanje za **envelope\_sender** i uneti izmenu ukoliko je potrebno.

nano /etc/MailScanner/spam.assassin.prefs.conf

envelope\_sender\_header X-BancaIntesa-MailScanner-From

(Na starom serveru stoji samo **envelope\_sender\_header X-MailScanner-From** a u uputstvu za novi MailScanner kaže da stavka **yoursite** mora da match-uje sa %org-name% podešavanjem iz fajla MailScanner.conf.

Uporediti sadržaje sledećih fajlova sa starim serverom filename.rules.conf, filetype.rules.conf, phishing.bad.sites.conf, phishing.safe.sites.conf.

Sa floppy image-a kopirati fajlove za rule-ove

/etc/MailScanner/rules/password.protected.archives.rules

/etc/MailScanner/rules/v320.pre

/etc/MailScanner/mcp/v320.pre

Proveriti status fajlova a prema potrebi ukucati podešavanja.

/etc/MailScanner/rules/filetype.rules

/etc/MailScanner/rules/max.message,size.rules

/etc/MailScanner/rules/password.protected.archives.rules

/etc/MailScanner/rules/spam.whitelist.rules

Izmeniti fajl /etc/MailScanner/defaults da bi se startovao MailScanner

nano /etc/MailScanner/defaults

run\_mailscanner=1

Startovati MailScanner i sa pregledom fajla /var/log/maillog, potvrditi da MailScanner ne generiše greške.

service mailscanner on

service mailscanner start

tail –f /var/log/maillog

Potvrditi ispravnost MailScanner-a i restartovati servis.

MailScanner --lint # status MailScanner-a

systemctl restart MailScanner

Podešavanje i startovanje SNMPd servisa

Na kraju fajla /etc/snmp/snmpd.conf dodati sledeću liniju.

nano /etc/snmp/snmpd.conf

rocommunity public 10.35.101.22

Startovati SNMPd servis.

systemctl start snmpd

systemctl enable snmpd

Podešavanje i startovanje NTPd servisa

Edit-ovati konfiguraciju za NTP i startovati NTPd servis i force-ovati proveru.

nano /etc/ntp.conf

restrict -6 ::1

ntp-dmz1

ntp-dmz2

systemctl start ntpdate

ntpdate ntp-dmz1

Proveriti SNMPd servis i kreirati novi fajl za logrotate SNMP servisa.

snmpwalk -v 1 -c public -O e 127.0.0.1

nano /etc/logrotate.d/snmpd

/var/log/snmpd.log {

rotate 52

compress

notifempty

missingok

postrotate

/bin/kill -HUP `cat /var/run/snmpd.pid 2> /dev/null` 2> /dev/null || true

endscript

}

Podešavanje i startovanje firewalld servisa

Podesiti firewalld.

firewall-cmd --permanent --add-service=ssh

firewall-cmd --zone=public --add-port=25/tcp

firewall-cmd --zone=public --add-port=161/udp

firewall-cmd --zone=public --add-port=514/tcp

firewall-cmd --zone=public --add-port=514/udp

firewall-cmd --reload

firewall-cmd --list-all

Podešavanje logrotate servisa

Podesiti logrotate. Ostaviti default-no samo de-maskirati sledeću opciju.

compress

Proveriti ispravnost logrotate. Posle komande ispod, u /var/log svi fajlovi ce se kompresovati.

logrotate –f /etc/logrotate.conf

Podešavanje rsyslog servisa

Konfigurisati RSYSLOG. Posle linije **mail.\*** dopisati sledeće linije. De-maskirati sve **$Action** opcije.

nano /etc/rsyslog.conf

mail.\* @10.35.45.170

$ActionQueueFileName fwdRule1

$ActionQueueMaxDiskSpace 1g

$ActionQueueSaevOnShutdown on

$ActionQueueType LinkedList

$ActionResumeRetryCount -1

systemctl restart rsyslog

Konfiguracija SSHd authoriyed\_keys

Nakon završene konfiguracije, podesiti SSHd konfiguraciju /etc/ssh/sshd.

PasswordAuthentication no