Hostname : server01, server04, server0-test

Cname : mymailrelay, mymailrelay2

OS : RHEL 6.5 x64

Postfix : 2.6.6

Architecture: VM Server

CPU : 1 core, 2 virtual sockets

Memory : 8192 MB

OS disk : 32 GB

SMTP disk : 200 GB

SMTP traffic: 200k application e-mails / 24hrs

**/etc/rc.local**

/sbin/ifconfig eth0 txqueuelen 10000 # Large data Transfers

/sbin/ethtool --set-ring eth0 rx 4096 # Large Buffers

/sbin/ethtool --set-ring eth0 tx 4096 # Large Buffers

/sbin/ifconfig eth0 mtu 9000 # Jumbo Frames, Ethernet Frames > 1500

**/etc/rc.d/rc3.d/S81postfix**

# Otherwise the POSTFIX does not send e-mails out.

/usr/sbin/postfix -c /etc/postfix -D -v reload

**/etc/rc.d/rc5.d/S81postfix**

# Otherwise the POSTFIX does not send e-mails out.

/usr/sbin/postfix -c /etc/postfix -D -v reload

**/etc/hosts**

127.0.0.1 localhost localhost.localdomain

10.1.35.101 server01.mycompany.com server01 mymailrelay

**/etc/sysconfig/network-scripts/ifcfg-eth0**

DEVICE=eth0

BROADCAST=10.1.43.255

HWADDR=00:50:56:B8:58:75

TYPE=Ethernet

UUID=cb4f82bb-ba04-43fd-84e2-d56fe10765db

ONBOOT=yes

NM\_CONTROLLED=no

BOOTPROTO=static

IPV6INIT=no

USERCTL=no

PEERDNS=no

DNS1=10.1.32.196

DNS2=10.1.32.194

IPADDR=10.1.43.89

NETMASK=255.255.252.0

MTU=9000

GATEWAY=10.1.40.1

ETHTOOL\_OPS="speed 10000 duplex full autoneg on"

**/etc/sysctl.conf**

net.ipv6.conf.default.disable\_ipv6 = 1

net.ipv6.conf.all.disable\_ipv6 = 1

net.ipv6.conf.lo.disable\_ipv6 = 1

**echo 1 > /proc/sys/net/ipv6/conf/eth0/disable\_ipv6**

**echo 1 > /proc/sys/net/ipv6/conf/lo/disable\_ipv6**

**/etc/modprobe.d/blacklist.conf**

blacklist ipv6

**/etc/postfix/main.cf**

soft\_bounce = no

queue\_directory = /var/spool/postfix

command\_directory = /usr/sbin

daemon\_directory = /usr/libexec/postfix

data\_directory = /var/lib/postfix

mail\_owner = postfix

myhostname = webmail.mycompany.com

mydomain = mycompany.com

myorigin = $mydomain

inet\_interfaces = all

inet\_protocols = all

mydestination = $myhostname, localhost.$mydomain, localhost, \*.$mydomain

unknown\_local\_recipient\_reject\_code = 550

mynetworks = 10.0.0.0/11, 10.32.0.0/11, 10.64.0.0/11, 127.0.0.0/8

relay\_domains = $mydestination

relayhost = mycompany-com.mail.protection.outlook.com

alias\_maps = hash:/etc/aliases

alias\_database = hash:/etc/aliases

default\_destination\_concurrency\_limit = 20

debug\_peer\_level = 2

debugger\_command =

PATH=/bin:/usr/bin:/usr/local/bin:/usr/X11R6/bin

ddd $daemon\_directory/$process\_name $process\_id & sleep 5

sendmail\_path = /usr/sbin/sendmail.postfix

newaliases\_path = /usr/bin/newaliases.postfix

mailq\_path = /usr/bin/mailq.postfix

setgid\_group = postdrop

html\_directory = no

manpage\_directory = /usr/share/man

sample\_directory = /usr/share/doc/postfix-2.6.6/samples

readme\_directory = /usr/share/doc/postfix-2.6.6/README\_FILES

smtp\_connect\_timeout = 120s

message\_size\_limit = 51200000

mailbox\_size\_limit = 0

smtpd\_use\_tls = yes

smtp\_use\_tls = yes

smtpd\_enforce\_tls = yes

smtp\_tls\_note\_starttls\_offer = yes

smtpd\_tls\_CApath = /etc/pki/tls/certs/

smtpd\_tls\_CAfile = /etc/pki/tls/certs/gdig2.crt

smtp\_tls\_CAfile = /etc/pki/tls/certs/bc2025.crt

smtp\_tls\_CApath = /etc/pki/tls/certs/

smtpd\_tls\_key\_file = /etc/postfix/ssl/webmail\_certificate\_export\_02-28-2014.pem

smtpd\_tls\_cert\_file = /etc/postfix/ssl/webmail\_certificate\_export\_02-28-2014.pem

smtp\_tls\_session\_cache\_database = btree:${queue\_directory}/smtp\_scache

smtpd\_tls\_auth\_only = yes

smtpd\_tls\_loglevel = 0

smtpd\_tls\_received\_header = yes

smtpd\_tls\_session\_cache\_timeout = 36000s

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

smtpd\_tls\_security\_level = may

smtp\_tls\_security\_level = may

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

smtp\_tls\_protocols = !SSLv2, !SSLv3

smtpd\_client\_connection\_count\_limit = 100

smtp\_destination\_concurrency\_limit = 1500

smtpd\_helo\_required = no

smtp\_always\_send\_ehlo = yes

smtpd\_helo\_restrictions = permit\_mynetworks, reject\_invalid\_hostname, permit

smtpd\_delay\_reject = yes

smtpd\_recipient\_restrictions = permit\_mynetworks,

permit\_inet\_interfaces,

permit\_sasl\_authenticated,

reject\_unauth\_pipelining,

reject\_unauth\_destination,

reject\_invalid\_hostname,

reject\_non\_fqdn\_hostname,

reject\_non\_fqdn\_sender,

reject\_non\_fqdn\_recipient,

reject\_unknown\_sender\_domain,

reject\_unknown\_recipient\_domain,

reject\_unverified\_sender,

reject\_unverified\_receiver,

reject\_rbl\_client bl.spamcop.net,

reject\_rbl\_client sbl-xbl.spamhaus.org,

reject\_rbl\_client dnsbl.njabl.org,

reject\_rbl\_client dnsbl-1.uceprotect.net,

reject\_rbl\_client dnsbl-2.uceprotect.net,

reject\_rbl\_client dnsbl.sorbs.net,

reject\_rbl\_client zen.spamhaus.org,

reject\_rbl\_client bl.spamcop.net,

permit

unverified\_sender\_reject\_code = 450

unverified\_sender\_reject\_code = 450

unknown\_virtual\_mailbox\_reject\_code = 550

allow\_mail\_to\_commands = alias,forward,include

allow\_mail\_to\_files = alias,forward,include

**/etc/postfix/master.cf**

smtp inet n - n - - smtpd -vv

2225 inet n - n - - smtpd

**/etc/postfix/tls\_policy**

mycompany-com.mail.protection.outlook.com secure

**/etc/logrotate.d/smtplogs**

/smtplogs/maillog {

missingok

notifempty

noolddir

size 10240k

nocompress

copytruncate

rotate 1

sharedscripts

postrotate

now=$(date +%Y-%m-%d~%H:%M:%S~%Z)

/bin/mv /smtplogs/maillog.1 /smtplogs/maillog.$now.rtf

/bin/chmod 604 /smtplogs/maillog.$now.rtf

/bin/chmod 604 /smtplogs/maillog

endscript

}

**/etc/logrotate.d/smtpzipped**

/smtplogs/maillog {

Sharedscripts

Postrotate

####################################

#

# CR00004448

#

# October 4, 2014

#

#

###

#

# Check for an active maintenance process

#

###

if [ -f ~/.smtplock ]; then

/bin/cat > ~/.blkmsg << '\_EOF'

The mail relay server has an active process maintenance

previously running and it has not finished yet.

Please check the folowing:

/etc/logrodate.d/\*

/smtplogs

/smtplogs/archive

/var/spool/cron/root

/var/log/\*

/smtplogs/maillogs

/bin/df -h -T /smtplogs

Restart the POSTFIX services as root user, only if this it is necessary.

/usr/sbin/postfix -c /etc/postfix -d -v flush

/usr/sbin/postfix -c /etc/postfix -d -v stop

/ust/sbin/postfix -c /etc/postfix -d -v start

Thanks,

IT Operations

\_EOF

/bin/cat ~/.blkmsg | mail -s "WARNING: Production Server `uname -n` has delayed maintenance" DL\_UnixTeam@mycompany.com, DLITOpsInfrastructureAmericas@mycompany.com

/bin/rm -rf ~/.blkmsg

exit

else

/bin/touch ~/.smtplock

fi

###

#

# Compress logs older than 30 days

#

###

/usr/bin/find /smtplogs -maxdepth 1 ! \( -name 'maillog.[ 0-9 ]' -name 'maillog' \) -mtime +30 -exec /bin/gzip {} \;

###

#

# Wait for the previous process to finish

#

###

wait $!

###

#

# Move all compressed files to the archive directory

#

###

/bin/mv /smtplogs/\*.gz /smtplogs/archive &

###

#

# Wait for the previous process to finish

#

###

wait $!

###

#

# Delete compressed logs older than 60 days

#

###

/usr/bin/find /smtplogs/archive -type f -mtime +60 -exec rm -f {} \; &

###

#

# Wait for the previous process to finish

#

###

wait $!

/sbin/service rsyslog restart

/bin/chmod 604 /smtplogs/maillog

/bin/rm -rf ~/.smtplock

endscript

}

**/var/spool/cron/root**

# Execute just SMTPlogs

\*/1 \* \* \* \* /usr/sbin/logrotate /etc/logrotate.d/smtplogs > /dev/null 2>&1

-OR –

# Execute the log files maintenance

\* \* \* \* \* sleep 1;/usr/sbin/logrotate /etc/logrotate.d/smtplogs > /dev/null 2>&1

# Execute the log files maintenance (server01)

00 10 \* \* \* /usr/sbin/logrotate /etc/logrotate.d/smtpzipped > /dev/null 2>&1

# Execute the log files maintenance (server04)

00 22 \* \* \* /usr/sbin/logrotate /etc/logrotate.d/smtpzipped > /dev/null 2>&1

COMMANDS

service rsyslog restart

service crond restart

/usr/sbin/postfix -c /etc/postfix -D -v flush

/usr/sbin/postfix -c /etc/postfix -D -v stop

/usr/sbin/postfix -c /etc/postfix -D -v start

/usr/sbin/postconf -d mail\_version

/usr/bin/openssl x509 -in /etc/postfix/ssl/webmail\_certificate\_export\_02-28-2014.pem -text

/usr/bin/openssl x509 -in /etc/pki/tls/certs/bc2025.crt -text -noout

/usr/bin/openssl x509 -in /etc/pki/tls/certs/gdig2.crt -text -noout

/usr/bin/openssl x509 -in /etc/pki/tls/certs/gdroot-g2.crt -text –noout

/usr/sbin/postmap hash:/etc/postfix/tls\_policy

openssl s\_client -connect webmail.mycompany.com:25 -starttls smtp -tls1\_1

/usr/sbin/openssl s\_client -connect localhost:2225 -starttls smtp -tls1\_2

VERIFICATION

/usr/sbin/openssl s\_client -connect webmail.mycompany.com:25 -starttls smtp -tls1\_1

/usr/sbin/openssl s\_client -connect localhost:2225 -starttls smtp -tls1\_2

- OR -

telnet localhost 2225

- THEN –

ehlo localhost

mail from:<email>@mycompany.com

rcpt to:<email>@mycompany.com

data

Subject: This is a TEST

Hi,

This is a MAIL RELAY test e-mail.

Thanks,

.

quit

DEBUGGING

# View configuration errors

/usr/sbin/logrotate --debug --force --verbose /etc/logrotate.conf

# Debug just SMTPlogs

/usr/sbin/logrotate -fd /etc/logrotate.d/smtplogs

# Debug just SMTPzipped

/usr/sbin/logrotate -fd /etc/logrotate.d/smtpzipped

# Execute just SMTPlogs

/usr/sbin/logrotate -s /tmp/SMTPlogs /etc/logrotate.d/smtplogs; cat /tmp/SMTPlogs ; rm -rf /tmp/SMTPlogs

# Execute just SMTPzipped

/usr/sbin/logrotate -s /tmp/SMTPzipped /etc/logrotate.d/smtpzipped

; cat /tmp/SMTPzipped ; rm -rf /tmp/SMTPzipped

# Execute all log-rotation

date; /usr/sbin/logrotate -s /tmp/logstatus -f /etc/logrotate.conf; date; cat /tmp/logstatus ; rm -rf /tmp/logstatus

REFERENCE

**GoDaddy Secure Server Certificate (Intermediate Certificate) - G2**

<https://certs.godaddy.com/anonymous/repository.pki>

**Baltimore CyberTrust Root**

<https://cacert.omniroot.com/bc2025.crt>

**How to import an internal Root CA created with Microsoft Certificate services**

<http://www.websense.com/support/article/t-kbarticle/How-to-import-an-internal-Root-CA-created-with-Microsoft-Certificate-services>

**Convert-PfxToPem**

<https://pspki.codeplex.com/wikipage?title=Convert-PfxToPem>

**Import PFX File, Internet Information Server 7**

<https://www.trustico.com/install/import/iis7/iis7-pfx-installation.php>