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