SENDMAIL SERVER
INSTALLATION, CONFIGURATION AND SECURITY

By ARUN RAAM NARAYANAN
arunoncl@siu.edu
INTRODUCTION TO SENDMAIL

• It is basically a mail transport agent, a program interfaces between user agents and delivery agents.

• It uses SMTP protocol and delivers messages to remote machines through internet.

• So it’s core duty is to safely move email between hosts, usually utilizing the SMTP protocol.

• Sendmail is highly configurable, allowing us to control almost every aspect of how email is handled, including the protocol to be used.
• Before installing sendmail, one must create both user smmsp and group smmsp. The smmsp user should have smmsp as its default login group which is set in /etc/passwd file.

• Sendmail uses two configuration files 1)submit.cf 2)sendmail.cf. submit.cf controls handling of mail that originates on local machine. sendmail.cf controls incoming mail and mail queued during submission process.
• The sendmail binary is installed in /usr/sbin directory. Then the configuration files etc/mail/sendmail.cf and /etc/mail/submit.cf are installed by the sysadmin.

• The mail queue directories /var/spool/mqueue and /var/spool/clientmqueue, created by sysadmin or by the installation process.
COMPILING

• After installation compiling starts by adding the smmssp user and group. Then the command is changed to the distribution’s sendmail directory, to run the Build script and run Build install is done.

• Compiling sendmail with % sh ./Build includes site-specific entries automatically. If one wants to install it in proper place % sudo sh ./Build install is used.
• Parameters in /etc/sysconfig/sendmail determine whether sendmail should start in daemon mode and how often it should run the queue.

• In case of RedHat sendmail starts in daemon mode and runs the queue every 30 minutes. In case of Debian sendmail has a default of daemon mode and runs the queue every 30 minutes.
CONFIGURATING SENDMAIL

- Sendmail’s actions are controlled by a single configuration file etc/mail/sendmail.cf which is also called the master configuration file.

- It determines 1) choice of delivery agents 2) address rewriting rules 3) mail header formats 4) options 5) security precautions.
• Other config files used are

/etc/mail/access
/etc/mail/aliases
/etc/mail/local-host-names
/etc/mail/mailer.conf
/etc/mail/mailertable
/etc/mail/virtusertable
• The access database defines what host(s) or IP addresses have access to the local mail server and what kind of access they have.

• The aliases database contains a list of virtual mailboxes that are expanded to other user(s), files, programs or other aliases.

• The virtuserhtable maps mail addresses for virtual domains and mailboxes to real mailboxes. These mailboxes can be local, remote, aliases defined in /etc/mail/aliases or files.
• A default sendmail.cf file will be installed in /etc. The default configuration should work for most SMTP-only sites.

• If you need to generate a new /etc/sendmail.cf file to configure Sendmail, we should utilize the m4 macro processor.

• By default, the m4 macro processor is installed with Sendmail.
SECURITY

• Security can be enhanced by addressing the following issues.

  Limiting Denial of Service Attack
  NFS and Sendmail
  Creating mail-only users
Limiting DoS Attack – by setting limits to following directives in `/etc/mail/sendmail.mc`

- `confCONNECTION_RATE_THROTTLE` - number of connections the server can receive per second.
- `confMIN_FREE_BLOCKS` - minimum number of free blocks which must be available for the server to accept mail.
- `confMAX_HEADERS_LENGTH` - maximum acceptable size (in bytes) for a message header.
- `confMAX_MESSAGE_SIZE` - maximum acceptable size (in bytes) for any one message.
NFS and Sendmail

- Mail spool directory `/var/spool/mail/` should not be put in NFS shared volume. NFS does not maintain control over user and group IDs, two or more users can have the same UID and therefore receive and read each other's mail.

Mail-only users

- Mail-only users are allowed only to access the Sendmail server using an email program. Shell accounts on the mail server should not be allowed. All user shells in the `/etc/passwd` file should be set to `/sbin/nologin`
CONCLUSION

Sendmail is advantageous over other MTA’s because it has,

- Better Relay checking.
- Better industry support, documentation and ongoing development over similar mailers.
- Ability to add custom features like blocking incoming mail with listed words in subject.
- Support for new techniques for mail filtering or rejection such as content filters of distributed database through dns.