A. Mail server
   1. Postfix
   2. Virtual domains
   3. Receiving and sending control
   4. Spam detector (greylisting)
   5. Antivirus integration
   6. Authentication SMTP
   7. Demo
A. MAIL SERVER
LECTURE 5: NETWORK SERVICES - PART1 - MAIL SERVICES

TERMINOLOGY

- Terminology:

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Meaning</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>MUA</td>
<td>Mail User Agent</td>
<td>The program that allows the user to read and send email.</td>
</tr>
<tr>
<td>MSA</td>
<td>Mail Submission Agent</td>
<td>The program that receives emails from MUA and cooperates with MTA for delivery of the emails.</td>
</tr>
<tr>
<td>MTA</td>
<td>Mail Transfer Agent</td>
<td>The program in charge of receiving and delivering mails to users.</td>
</tr>
<tr>
<td>SMTP</td>
<td>Simple Mail Transfer Protocol</td>
<td>SMTP is a communication protocol for mail servers to transmit emails over the internet.</td>
</tr>
<tr>
<td>SASL</td>
<td>Simple Authentication &amp; Security Protocol</td>
<td>SASL is the mechanism is framework for providing authentication and data security services in connection- oriented protocols.</td>
</tr>
<tr>
<td>LMTP</td>
<td>Local Mail Transfer Protocol</td>
<td>LMTP is designed as an alternative to normal SMTP for situations where the receiver has no mail queue. (like mail storage server)</td>
</tr>
<tr>
<td>LDA</td>
<td>Local Delivery Agent</td>
<td>another name for MDA when the email is delivered locally.</td>
</tr>
<tr>
<td>MDA</td>
<td>Mail Delivery Agent</td>
<td>The program responsible for the delivery of emails to a recipients.</td>
</tr>
<tr>
<td>IMAP</td>
<td>Internet Mail Access Protocol</td>
<td>A protocol allowing a client to access and manipulate email on the mail server.</td>
</tr>
<tr>
<td>POP3</td>
<td>Post Office Protocol 3</td>
<td>POP3 is a protocol for receiving and holding email on remote mail server over network.</td>
</tr>
</tbody>
</table>
LECTURE 5: NETWORK SERVICES - PART 1 - MAIL SERVICES

MAIL SERVER

• Concept Sending

MAIL USER AGENT

MAIL SERVER

POSTFIX

MSA + MTA

[smtpd]

AUTHENTICATION

IMAP-LOGIN / IMAP

LDA / MDA

LMTP

POSTGREY

IMAP-LOGIN / IMAP

Mail Box

SMTP

IMAPS

SASL

Password DB

POSTGREY

SMTP

SMTP

587

25

1

3

4

2

5

993

20

25
LECTURE 5: NETWORK SERVICES - PART 1 - MAIL SERVICES

MAIL SERVER

- Concept Receiving
LECTURE 5: NETWORK SERVICES- PART1- MAIL SERVICES

MAIL SERVER

• Concept S/R
1. POSTFIX
LECTURE 5: NETWORK SERVICES - PART 1 - MAIL SERVICES

POSTFIX

• Role:
  
  • postfix is a package includes the main SMTP daemon.
  
  • MTA is in charge of:
    
    • Receive & deliver email via SMTP
    
    • Local delivery directly or use other mail delivery agent.
LECTURE 5: NETWORK SERVICES - PART 1 - MAIL SERVICES

POSTFIX

• Role:

MAIL DELIVERY EXAMPLE
LECTURE 5: NETWORK SERVICES- PART1- MAIL SERVICES

POSTFIX

• Major Tasks:
  • Receive mail & put them in queue
  • Queue management
  • Delivery mail from queue

IN
Local submissions
Network submissions
Local forwarding
Notifications

QUEUE MANAGER

OUT
stop, Imtp,
local, relay,
virtual, pipe
LECTURE 5: NETWORK SERVICES- PART1- MAIL SERVICES

POSTFIX

• Mail IN:
  • Four manners:
    • Local submissions,
      • Postdrop command
      • Maildrop queue
      • pickup daemon
      • cleanup daemon
        ✴ header validation
        ✴ address translation
      • Incoming queue
LECTURE 5: NETWORK SERVICES- PART1- MAIL SERVICES

POSTFIX

• Mail IN:

  • Four manners:

    • Network submissions,
      • smtpd daemon
      • cleanup daemon
        ✴ header validation
        ✴ address translation
      • Incoming queue
Mail IN:

Four manners:

Local forwarding,
  - Resubmit via .forward
  - Envelope “To” is changed

Notification
Queue manager:

Five queue types:

- **incoming,**
  - For mail that is still arriving or that the queue manager hasn't looked at yet
- **active,**
  - Is a limited-size queue for mail that the queue manager has opened for delivery
- **deferred,**
  - Is reserved for the mail that could not be delivered, this way it does not get in the way of other deliveries.
- **corrupt,**
  - Is used for storing damaged or unreadable emails
- **hold**
  - When a mail is put to hold, it means that no attempt is made to deliver it.
LECTURE 5: NETWORK SERVICES- PART1- MAIL SERVICES

POSTFIX

• Mail out:

  • Address classes:
    • Used to determine which destination to accept for delivery and how the delivery take place

  • Main address classes:
    • Local delivery
      • Check alias and .forward file to do further delivery
    • Relay
      • Transfer mail for others (not your domains)
    • Deliver mail to other domains
      • The queue manager invoke the smtp in order to deliver the mail.

• Virtual alias

• Virtual mailbox
2. VIRTUAL DOMAINS
VIRTUAL DOMAINS

DEFINITION 18.1:
Mail server can receive emails addressed to other domains besides the main domain, these domains are called virtual domains

• Postfix provides two interesting features to handle virtual domains:

  1. Virtual Alias Domains
  2. Virtual Mailbox Domains
VIRTUAL DOMAINS

• Virtual Alias Domains:
  • contains only alias (addresses that only forward emails to other addresses)

• Enabling:
  • Add domain name to:
    • virtual_alias_domains variable
    • virtual_alias_maps variable

virtual_alias_domains = $virtual_alias_maps (default)
virtual_alias_maps = hash:/usr/local/etc/postfix/virtual
VIRTUAL DOMAINS

• Virtual Alias Domains:

```
virtual_alias_domains = $virtual_alias_maps (default)
virtual_alias_maps = hash:/usr/local/etc/postfix/virtual
```

The file describes a mapping with a rather straightforward syntax: each line contains two fields:

- Alias Name
- List of emails addresses where to redirects

<table>
<thead>
<tr>
<th>Domain</th>
<th>Alias</th>
</tr>
</thead>
<tbody>
<tr>
<td>example.com</td>
<td>DOMAIN</td>
</tr>
<tr>
<td><a href="mailto:bob@example.com">bob@example.com</a></td>
<td>bob</td>
</tr>
<tr>
<td><a href="mailto:steve@example.com">steve@example.com</a></td>
<td>steve</td>
</tr>
<tr>
<td>example.net</td>
<td>DOMAIN</td>
</tr>
<tr>
<td>@example.net</td>
<td>steve</td>
</tr>
<tr>
<td>example.org</td>
<td>DOMAIN</td>
</tr>
<tr>
<td>@example.org</td>
<td>chris</td>
</tr>
</tbody>
</table>
VIRTUAL DOMAINS

• Virtual Mailbox Domains:

  • Enabling:
    • Naming this domain in the virtual_mailbox_domains variable
    • Referencing a mailbox mapping file in “virtual_mailbox_maps”
    • Defining where the mailboxes will be stored via configuring the “virtual_mailbox_base” parameters.
    • Enabling virtual users in courier

REMARK 21.1
Postfix does not allow using the same name in both domains: virtual_alias_domains and virtual_mailbox_domains. However, every domain of virtual_mailbox_domains is implicitly included in the virtual_alias_domains, therefore, it is possible to mix aliases and mailboxes with the virtual domain.
VIRTUAL DOMAINS

• Virtual Mailbox Domains:

• Examples:

  DIRECTIVES TO ADD IN THE /ETC/POSTFIX/MAIN.CF FILE

  ```
  virtual_mailbox_domains = sa.ut.ee
  virtual_mailbox_maps = hash:/etc/postfix/vmailbox
  virtual_mailbox_base = /var/mail/vhosts
  ```

  THE /ETC/POSTFIX/VMAILBOX FILE

  ```
  # Artjom’s email is stored as maildir, with
  # one file per email in a dedicated directory
  artjom@sa.ut.ee sa.ut.ee/artjom/
  # Joonas’s email is stored in a traditional “mbox” file,
  # with all mails concatenated into one single file
  joonas@sa.ut.ee sa.ut.ee/joonas
  ```
3.

RECEIVING & SENDING CONTROL
In this section:

- Major techniques to reduce:
  - bulk emails
  - spam emails
  - advertisement emails
Basic Techniques are:

1. IP-based access restrictions
2. Checking the Validity of EHLO or HELO commands
3. Accepting or refusing based on the announced sender
4. Accepting or refusing based on the recipient
5. Restrictions associated with the DATA Command
6. Filtering based on the message contents
LECTURE 5: NETWORK SERVICES- PART1- MAIL SERVICES
RECEIVING&SENDING CONTROL

• Techniques are:

  • IP-based access restrictions

In the smtpd_client_restrictions directive controls which machines are allowed to communicate with the email server.

```plaintext
smtpd_client_restrictions = permit_mynetworks,  
                          warn_if_reject reject_unknown_client,  
                          check_client_access hash:/etc/postfix/access_clientip,  
                          reject_rbl_client sbl-xbl.spamhaus.org,  
                          reject_rbl_client list.dsbl.org
```

REMARK 26.1:
In case the variable contains many rules as it is the case in our example above, they will executed following the order of their entry.
Lecture 5: Network Services - Part 1 - Mail Services

Receiving & Sending Control

- Techniques are:
  - IP-based access restrictions

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>permit_mynetworks</td>
<td>Accepts all emails coming from the machine in the local network.</td>
</tr>
<tr>
<td>warn_if_reject</td>
<td>Rejects emails coming from the machines without completely valid DNS</td>
</tr>
<tr>
<td>reject_unknown_client</td>
<td>configuration and direct them to unknown client directive.</td>
</tr>
<tr>
<td>check_client_access hash:/etc/postfix/access_clientip</td>
<td>Allows the administrator to set up a blacklist and a whitelist of email servers, stored in the /etc/postfix/access_clientip file.</td>
</tr>
<tr>
<td>reject_rbl_client sbl-xbl.spamhaus.org</td>
<td>reject any message coming from a server listed in one of the indicated blacklists. (rbl = “Remote Black List”)</td>
</tr>
<tr>
<td>reject_rbl_client list.dsbl.org</td>
<td></td>
</tr>
</tbody>
</table>
• Techniques are:

• Checking the Validity of EHLO or HELO commands

In any SMTP exchange it starts with HELO or EHLO command, then the name of the sending email server.

```plaintext
smtpd_helo_restrictions = permit_mynetworks,
                         reject_invalid_hostname,
                         check_helo_access hash:/etc/postfix/access_helo,
                         reject_non_fqdn_hostname,
                         warn_if_reject reject_unknown_hostname
```
• Techniques are:

• Checking the Validity of EHLO or HELO commands

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>permit_mynetworks</td>
<td>allows all machines on the local network to introduce themselves freely.</td>
</tr>
<tr>
<td>reject_invalid_hostname</td>
<td>rejects emails when the EHLO announce lists a syntactically incorrect hostname.</td>
</tr>
<tr>
<td>reject_non fqdn_hostname</td>
<td>rejects messages when the announced hostname is not a fully-qualified domain name.</td>
</tr>
<tr>
<td>reject_unknown_hostname</td>
<td>rejects messages if the announced name does not exist in the DNS. Since this rule will have so many rejections the System, admin turn it to just a warning.</td>
</tr>
</tbody>
</table>
LECTURE 5: NETWORK SERVICES- PART1- MAIL SERVICES
RECEIVING&SENDING CONTROL

• Techniques are:

• Accepting or refusing based on the announced sender

Each mail or message has a sender, which is announced by the mail from command of the smtp protocol; thus is possible to run many checks.

```plaintext
smtpd_sender_restrictions =
  check_sender_access hash:/etc/postfix/access_sender,
  reject_unknown_sender_domain, reject_unlisted_sender,
  reject_nonfqdn_sender
```
LECURE 5: NETWORK SERVICES- PART1- MAIL SERVICES
RECEIVING & SENDING CONTROL

**Techniques are:**

- Accepting or refusing based on the announced sender

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>check_sender_access</strong></td>
<td>the rule uses /etc/postfix/access_sender table and maps some special treatment to some senders. This usually means listing some senders into a white list or a black list.</td>
</tr>
<tr>
<td><strong>reject_unknown_sender_domain</strong></td>
<td>requires a valid sender domain, since it is needed for a valid address.</td>
</tr>
<tr>
<td><strong>reject_unlisted_sender</strong></td>
<td>rejects local senders if the address does not exist</td>
</tr>
<tr>
<td><strong>reject_non_fqdn_sender</strong></td>
<td>rejects emails purporting to come from addresses without a fully-qualified domain name.</td>
</tr>
</tbody>
</table>
Techniques are:

- Accepting or refusing based on the recipient

Each email has at least one recipient announced with the RCPT TO command in the smtp protocol. Therefore, we can add restriction based on that information.

```
smtpd_recipient_restrictions = permit_mynetworks,
    reject_unauth_destination, reject_unlisted_recipient,
    reject_non_fqdn_recipient
```
• Techniques are:

• Accepting or refusing based on the recipient

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>reject_unauth_destination</td>
<td>messages sent to an address not served by this server are rejected</td>
</tr>
<tr>
<td>reject_unlisted_recipient</td>
<td>ejects messages sent to non-existing local users, which makes sense.</td>
</tr>
<tr>
<td>reject_non_fqdn_recipient</td>
<td>rejects non-fully-qualified addresses</td>
</tr>
</tbody>
</table>
• Techniques are:

• Restrictions associated with the DATA Command

The data command of smtp is emitted before the content of the message or email, it contains only an announcement of what is next.

```plaintext
DATA CHECKS
smtpd_data_restrictions = reject_unauth_pipelining
```
• Techniques are:

• Restrictions associated with the DATA Command

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>reject_unauth_pipelining</td>
<td>causes the message to be rejected if the sending party sends a command before the reply to the previous command has been sent.</td>
</tr>
</tbody>
</table>
LECTURE 5: NETWORK SERVICES- PART1- MAIL SERVICES
RECEIVING&SENDING CONTROL

• Techniques are:

• Filtering based on the message contents

In order to complete the check we have to run a check on the message content itself.

ENABLING CONTENT-BASED FILTERS

header_checks = regexp:/etc/postfix/header_checks
body_checks = regexp:/etc/postfix/body_checks
LEcTure 5: network services- part1- mail services

receiving & sending control

• Techniques are:
  • Filtering based on the message contents

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>regexp:/etc/postfix/header_checks</td>
<td>Both files contain a list of regular expressions (commonly known as regexps or regexes) and associated actions to be triggered when the email headers (or body) match the expression.</td>
</tr>
<tr>
<td>regexp:/etc/postfix/body_checks</td>
<td></td>
</tr>
</tbody>
</table>
4. SPAM DETECTOR (GREYLISTING)
DEFINITION 39.1:
“greylisting” is a filtering technique particularly efficient against spam sent by many machines infected by worms and viruses.

1. After installing greylisting
2. It will run and listen on port 10023
3. Configuring postfix to denigrate the decision of accepting or rejecting the mail:

```
smtpd_recipient_restrictions = permit_mynetworks,
                            [...
                            check_policy_service inet:127.0.0.1:10023
```

By adding
LECTURE 5: NETWORK SERVICES- PART1- MAIL SERVICES

GREYLISTING

- **Matched whitelisted**
- If the IP does not look like a dynamic IP, continue as follows:
  - **S25R**
    - If the IP looks like a dynamic IP:
      - **Blacklist of HELO...**
        - If matched blacklist:
          - **Greylisting**
            - If triplet listed:
              - **Accept**
            - If triplet not listed:
              - **Reject**
        - If not valid or delay:
          - **Reject**
  - If triplet listed:
    - **Accept**

- If match whitelist:
  - **Accept**
greylisting checks the triplet.

What is triplet?

It is an E-mail delivery attempt identified by

- The IP address of the host attempting the delivery
- The envelope sender address
- The envelope recipient address
**LECTURE 5: NETWORK SERVICES- PART1- MAIL SERVICES**

**GREYLISTING**

<table>
<thead>
<tr>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Manageability</strong></td>
<td><strong>Legitimate rejection</strong></td>
</tr>
<tr>
<td>{No quarantine to maintain and check, No training necessary, Simple to set up}</td>
<td>{if the sender is not willing to resend, sender is using mail farm (IP changing), Sender is using forwarding}</td>
</tr>
<tr>
<td><strong>Functionality</strong></td>
<td><strong>Can cause unpredictable delays in email delivery</strong></td>
</tr>
<tr>
<td>{Causes delays to spams, high efficiency, no message lost}</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Memory demanding sometimes</strong></td>
</tr>
</tbody>
</table>
5. ANTIVIRUS INTEGRATION
• Email Virus
  • Spread using email as mean with attachment containing a macro virus.
  • Triggered when
    • User opens attachment
    • Or just view email (by using scripting feature in mail agent)
Example for the antivirus “clamav-milter”

clamav is free antivirus software and in order to interface it with mail server there is a need for mail interface “milter” which means mail filter.

milter has something integrated called “Spamassassin” which is exactly similar to “greylisting” purpose.

Configuration:

In order to configure and customise clamav-milter there is need for dpkg-reconfigure clamav-base package.

Notify Postfix about it:

Postfix need to know that there is an antivirus and email should directed to there in order to be checked. the modification should be done in “/etc/postfix/main.cf” file.

```
# Virus check with clamav-milter
smtpd_milters = inet:[127.0.0.1]:10002
```
• Testing the Antivirus:

• Simplest way:

  send an email with an attachment eicar.com (or eicar.com.zip) file. downloadable from: http://www.eicar.org/86-0-Intended-use.html

REMARK:

The file is not a true virus but it is file for testing that all the antivirus softwares in the market recognise it as a virus.
5. AUTHENTICATED SMTP
INFO:
SMTP-AUTH is an extension to the STMP protocol. It is mail transfer protocol via internet that contains an authentication stage during the client attend to connect to the server.

• For our case:
  
  • SMTP-AUTH in postfix relies on SASL (Simple Authentication and Security Layer).
  
  • Requires installing additional libraries such as {libsasl2-modules and sasl2-bin packages}
LECTURE 5: NETWORK SERVICES- PART1- MAIL SERVICES

AUTHENTICATED SMTP

• SASL configuration:

• Password:

• using the command, \texttt{saslpasswd2}, it takes also additional parameters.

<table>
<thead>
<tr>
<th>Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-u</td>
<td>defines the authentication domain</td>
</tr>
<tr>
<td>-c</td>
<td>allows creating a user</td>
</tr>
<tr>
<td>-f</td>
<td>allows specifying the file to use</td>
</tr>
</tbody>
</table>
AUTHENTICATED SMTP

LECTURE 5: NETWORK SERVICES- PART1- MAIL SERVICES

SASL configuration:

for consistency:

- turn "/etc/sasdb2" into a symbolic link pointing at the database used by postfix.

```bash
ln -sf /var/spool/postfix/etc/sasldb2 /etc/sasldb2
```
LEcTure 5: netwoRk seRviceS- pArt1- maIl seRviceS

auThenticaTed smTp

• SASL Enabling in Postfix:

  • the “smtpd_recipient_restrictions” parameter has to be configured in order to permit SASL-authenticated clients to send emails freely.

```bash
# Enable SASL authentication
smtpd_sasl_auth_enable = yes
# Define the SASL authentication domain to use
smtpd_sasl_local_domain = $myhostname
[...]
# Adding permit_sasl_authenticated before reject_unauth_destination
# allows relaying mail sent by SASL-authenticated users
smtpd_recipient_restrictions = permit_mynetworks,
permit_sasl_authenticated,
reject_unauth_destination,
[...]
```
6. DEMO