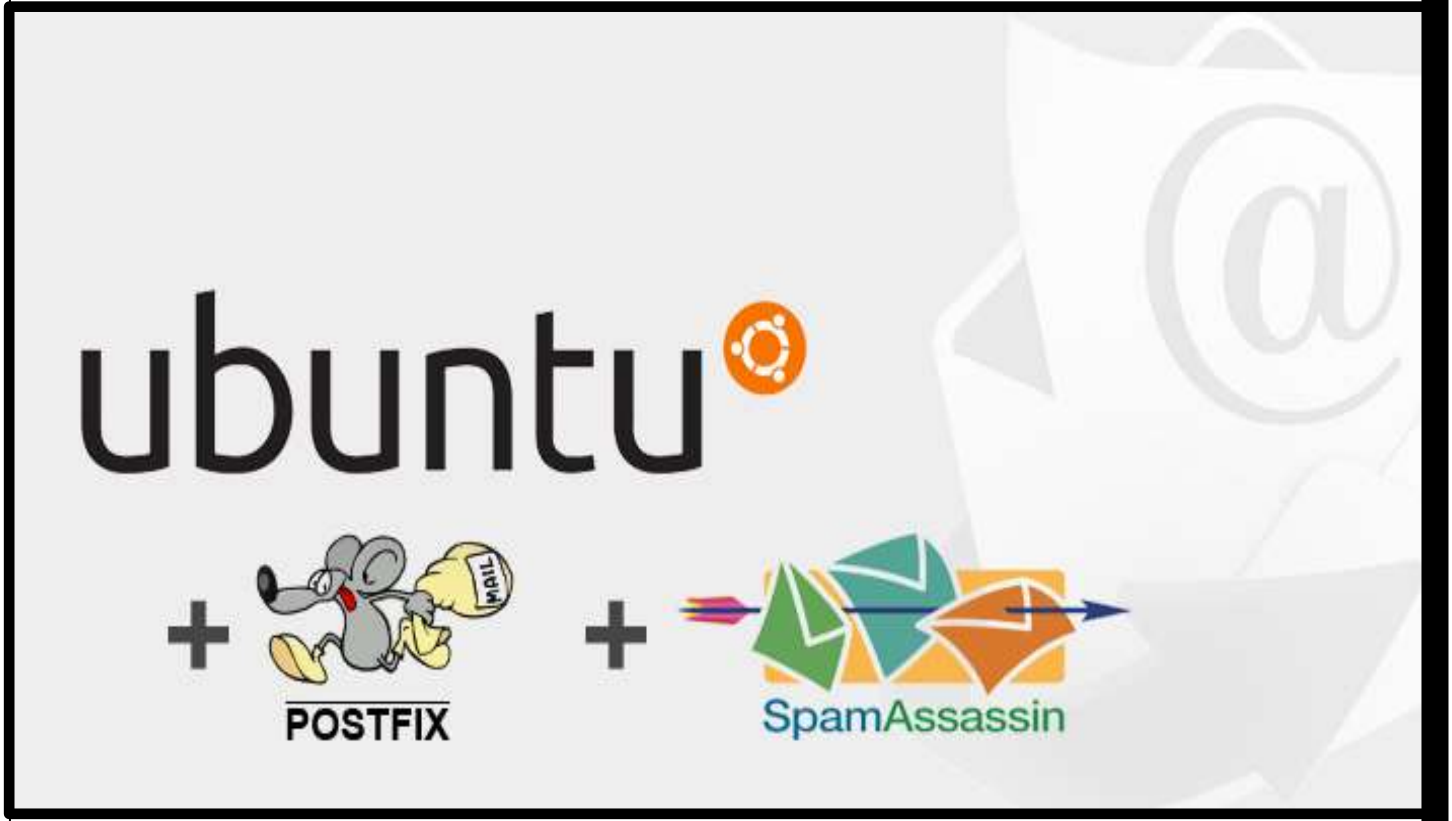


MAIL SERVER ON UBUNTU

POSTFIX, COURIER, SSL/TLS, SPAMASSASSIN, CLAMAV, AMAVIS

This guide is compatible with Ubuntu 14.04

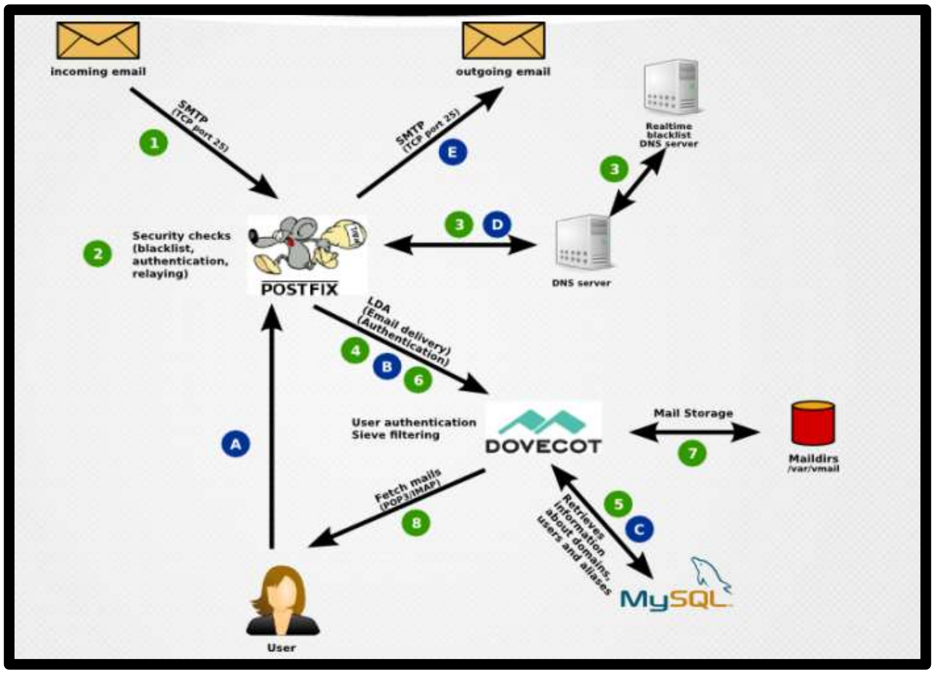
24.3.2016

NIRBHAY PHERWANI | RUTURAJ NENE | BHAVESH MOHINANI |
MANISH LALSINGHANI

MAIL SERVER ON UBUNTU

POSTFIX, COURIER, SSL/TLS, SPAMASSASSIN, CLAMAV, AMAVIS

INTRODUCTION


incoming email
outgoing email
SMTP (TCP port 25)
1
SMTP (TCP port 25)
E
Realtime blacklist DNS server
3
2
Security checks (blacklist, authentication, relaying)
POSTFIX
3
D
DNS server
LDA (Email delivery) (Authentication)
4
B
6
A
User authentication Sieve filtering
DOVECOT
Mail Storage
7
Maildirs /var/vmail
Fetch mails (POP3/IMAP)
8
Retrieves information about domains, users and aliases
5
C
MySQL
User

I. The green circles show what will happen when you receive an email.

II. A remote mail server requests a TCP connection on port 25 to your mail server. Your

III. firewall lets that connection through and the Postfix “smtpd” process will accept it.

IV. Postfix starts speaking SMTP (the “simple mail transfer protocol”) and gathers information who the alleged sender and the intended recipient addresses are. While the

MDA

The MDA gets messages from the mail server into the users' inboxes, most commonly with the POP or IMAP mail protocols. Except under some very limited circumstances, an MTA isn't going to do you much good without an MDA, so we're going to be using Dovecot as our MDA.

connection is still active Postfix does a couple of checks and may decide to reject the email.

V. Postfix will also check real-time black lists (RBLs) via DNS to see if the sending IP address should be distrusted. For example it will reject senders running on a dynamic IP address because that almost always means the email is coming from yet another infected Windows workstation or hacked server and is likely spam.

VI. Postfix asks Dovecot whether the recipient email address belongs to an actually known user.

VII. Dovecot checks the MySQL database and looks for an entry for the email address in question.

VIII. If the user exists then Postfix will accept the email and forward it to Dovecot.

IX. Dovecot stores the received email in a file in the /var/vmail directory.

X. The user fetches new email using the POP3 or IMAP protocols from Dovecot.

XI. Now let’s assume the user replies to the email and wants to send the reply. This is depicted by the blue circles.

(A) The user’s mail client establishes an SMTP connection to Postfix. It sends a username and password to authenticate.

(B) Postfix asks Dovecot whether the username and password are correct. This prevents accepting unauthorized email from untrusted parties.

(C) Dovecot searches for the account information of the sending user in the MySQL database. It tells Postfix whether the authentication was successful.

(D) Postfix needs to find out which server on the internet the email needs to be sent to. It asks a DNS (domain name service) server for an MX (mail exchanger) record of the receiving domain. If successful it will get the name of the server back and will know where to send the email.

(E) Postfix connects to the responsible server of the receiving user, establishes an SMTP connection and sends the email.

That much for a general overview.

SPAM ASSASSIN

- **Spam assassin runs sanity checks on an incoming mail to determine how likely it is to be spam**

- **It is a computer program used for email spam filtering. It uses a variety of spam detection techniques including DNS based, checksum based spam detection, regular expressions, pattern matching techniques etc.**

- **The program can be integrated with the mail server to automatically filter all mail for a site.**

- **Spam assassin is a highly configurable; if it is used as a system wide filter can still be configured to support per user preferences.**

CLAMAV

Clam Antivirus is a free and open source, cross platform antivirus software toolkit available to detect many types of malicious software and viruses.

- **One of its main use is it is used on mail servers as server side email virus scanner.**

- **Clam AV includes a number of utilities such as command line scanner Automatic database updater and scalable multithreaded daemon, running on antivirus engine from a shared library.**

- **Clam AV database is updated at least every 4 hours.**

AMAVIS

- **Amavis is an open source content filter for electronic mail used for message transfer, decoding and some other processing and checking and interfacing with external content filter to provide protection against spam, viruses and other malwares.**

- **It can be considered as an interface between a mailer and one or more content filters.**

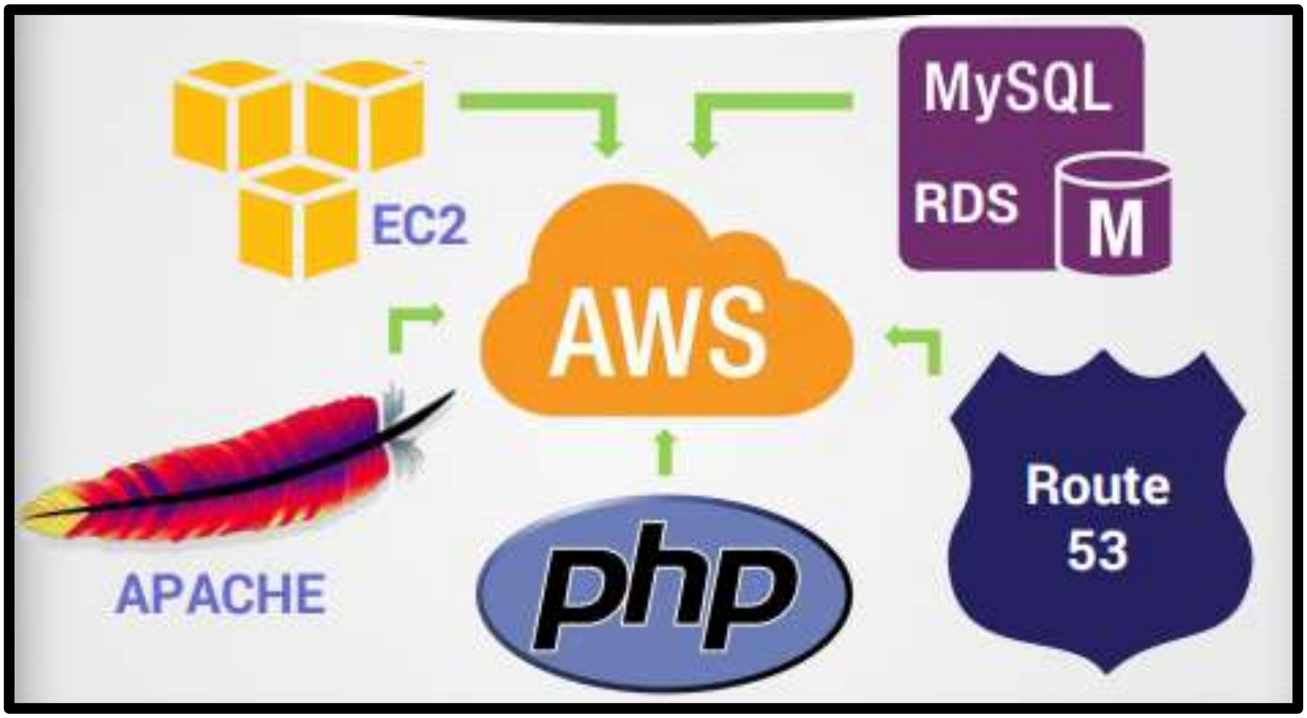
• Amavis can be used for detecting viruses, spams, banned content types, syntax errors etc.

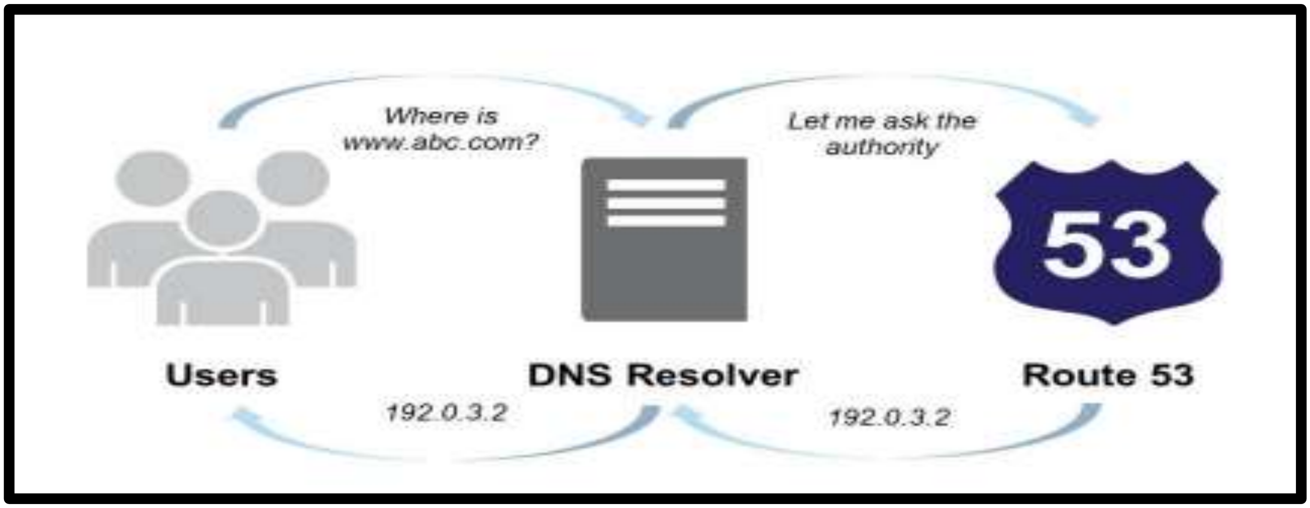
• It can be used for redirect or forward of emails, it can be used for archiving of mail messages to files, to mailboxes, to an SQL database.

• It is used to sanitize passed messages through external sanitizer

• It can be further interfaced with spam assassin to provide reliability, security, performance.

HOSTING


EC2
MySQL
RDS
M
AWS
APACHE
php
Route
53


Where is
www.abc.com?
Let me ask the
authority
53
Users
DNS Resolver
Route 53
192.0.3.2
192.0.3.2