Bachelor's thesis

Information Technology

NINFOS13

2017

Zishuang Liang

AN ANALYSIS AND COMPARISON OF CURRENT MTA SERVERS

TURKU AMK
TURKU UNIVERSITY OF APPLIED SCIENCES

BACHELOR'S / THESIS | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Information Technology

2017 | 22

Zishuang Liang

AN ANALYSIS AND COMPARISON OF CURRENT MTA SERVERS

With the development of Internet, E-mail is widely used in our daily life and significantly reshapes the way people communicate with each other, especially in business contexts. Therefore, the security of E-mail systems is one paramount component of the entire Internet security system. Due to multifaceted factors, there is a wide range of security problems when we use email. A typical example is the viruses contained in emails. Hackers are able to invade the whole system through email viruses. Furthermore, another problem is the increasing number of spam and advertisement emails. Consequently, such mails easily take up much bandwith which ultimately leads to the decline of user connection speed and quality.

In light of these facts, mail servers have been designed by computer experts, with the aim to solve the above problems. Currently, there are several options for running a free mail server in the Linux environment. Common servers are Sendmail, Qmail, Postfix and so on. This thesis mainly focuses on the function of Postfix, the most common MTA server, for analysis. Early in 1998, Postfix was firstly developed by Doctor Wietse Zweitze Venema. In the early practice, a mail server was conventionally set by Sendmail program. However, with the fast advancement of technology, Doctor Venema identified some shortcomings while using the Sendmail program, especially with respect to safety and efficiency. In order to solve these problems, Doctor Venema initiated a plan to design a new mail server program which would be faster and safer to replace the original Sendmail program, namely, Postfix. The purpose of this thesis is to give a clear view of Postfix, compare it with other MTA servers and explain the reasons for the application of Postfix in Linux network and in other security systems.

KEYWORDS:

MTA MUA MDA Postfix Sendmail Qmail Linux security.

CONTENTS

FIGURES

TABLES

LIST OF ABBREVIATIONS

MTA	Mail Transfer Agent
MUA	Mail User Agent
SMTP	Simple Mail Transfer Protocol
MDA	Mail Delivery Agent

1 INTRODUCTION

In current casual and formal communication, emails are commonly employed to send and receive information. As the main part of the email system, a Mail Transfer agent is responsible for receiving emails from the one side and then delivering them to another MTA process. A few years ago, Sendmail could only be used in the previous Linux environment. Considering the flaws of Sendmail, developers generated several other MTA servers. In the development of newer options, a critical comparison between existing servers and the newer ones is inevitable. This thesis hence draws on such comparison to inform on the advantages and disadvantages of using one over the other based on their characteristics.

One of the fundamental MTA servers is Postfix. Postfix is a product of free software engineering and was originally developed by Wietse Venema under the sponsorship of IBM. The initial aim of Postfix was to replace Sendmail with upgraded functions. Firstly, Postfix was positioned as a fast and easy tool to use. Secondly, it aimed to ensure the maximum security of the system. Thirdly, when considering the wide application of Sendmail among users, it was thus necessary to maintain the compatibility of Postfix with Sendmail. Other MTA server like Sendmail, Exim and QMail have different features depending on the problems in the MTA process they are addressing. For instance, Sendmail is more user-friendly, it can work very well with just default settings and this enhances the ways it can be used by novice users and experts (Bauer Michael D. 2002, October).

The aim of this thesis work is to explain the characteristics of several mainstream MTA servers in the current Linux environment, analyse, and compare the advantages and disadvantages of these MTA servers. As part of these discussions, this work will also introduce the setting up of Postfix and how to effectively employ protocols, such as SMTP, to avoid potential problems emerging in mail services. The primary goal of this thesis is to give the audience a general picture of different MTA servers in a Linux environment

2 THE MAIL TRANSMISSION

To begin with, it is necessary to analyse the mail delivery process. Suppose a user needs to send a letter to another user whose email address is “aaa@mail.com”, he or she then should firstly send a letter to the host mail.com. As it is not possible to send this letter "directly" to the host mail.com over the network, the user has to set up the mail server for the delivery. The user should register to a mail server to obtain a legit e-mail authorization to be able to send the mail. In other words, users should take advantages of the interfaces to send emails. Figure 1 illustrates the email transmission process.

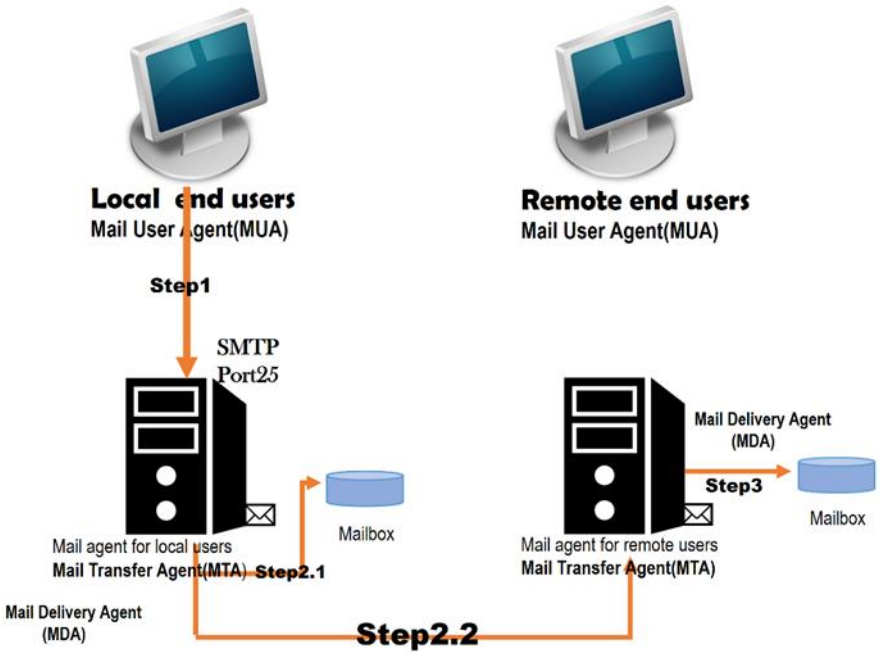

Figure 1. The Process of Mail Delivery.

The mail transmission process consists of the following elements:

MUA

As it has been mentioned, users employ software such as telnet to log in a mail server to send a letter. They must rely on MUA, or Mail User Agent, to the mail server. Common MUAs include Mozilla launched Thunderbird (Thunderbird) free software, Linux desktop KDE common Kmail, Windows Outlook Outlook Express (OE) and so on. The main function of MUA is to receive host e-mail and enable users to browse and write e-mail function.

MTA

MTA, Mail Transfer Agent, can be regarded as a post office. After MUA sends mails to the mail server, the mail server is then responsible for the following delivery. The mail server is called “MTA”. MTA has following two functions:

1. To receive mail by using Simple Mail Transfer Protocol through Port 25

2. To relay mail. If a mail’s destination is not the mail server’s user and data related to this mail has clearance to use MTA, then MTA will send this to other mail servers, which is called Relay.

Although strict MTA only refers to Simple Mail Transfer Protocol, the mail server is still recognized as “MTA”. Those software featuring SMTP functions are Sendmail, postfix, Qmail, etc.

MDA

MDA is the abbreviation for Mail Delivery Agent. In fact, MDA is a subordination of MTA. If MTA is the post office, then MDA is the postman. MDA exams the prefix or

content of the mail and decides where this mail should go. The relay function mentioned above is carried by MDA. MDA also has the function to filter junk mail and reply automatically. The software mentioned in the last paragraph have their own MDA which have more powerful functions.

The last element is the mailbox where incoming mails are processed. In Linux, the default mailbox is in /var/spool/mail/user's email address.

It is important to understand how MUA sends the user's mails all the way to the receiver's mailbox.

1. If we want to use local MUA to use MTA to send a mail, we firstly need to gain access to a MTA. In fact, that is what we actually do when we register an E-mail account and set password.

2. We edit an E-mail which includes E-mail addresses of the sender and receiver, and subject. Then we add contents. After editing, we press the send button, and the mail is now sent to a MTA. Notice that the mail is sent to the sender's MTA instead of the receiver`s. If the sender has access to MTA, then the mail will be in queue to wait to be sent out.

3. If users are sending mails to themselves, then mails will be directly sent to the mailbox. If users are sending to others, MTA will analyze to make sure users have legal access to send it. If users do, MDA will transfer it to another MTA through SMTP port 25. If the mail is successfully transferred, it will be removed from the queue.

4. Then the receiver's MTA will receive the senders' mails and put them into mailbox correctly. In this process, MDA will decide whether it is a junk mail.

This thesis focuses on mail server as my project topic because the author was personally interested in the practical application of mail servers and planned to design her own mail server at home. In addition, despite the growing popularity of email in

the modern communication, the general public often pays limited attention to the function of a mail server. Maintenance, security and troubleshooting are all time-consuming tasks that call upon further attention. Therefore, this project is designed to give an inside view of the construction and operation of mail servers.

In next chapter three different Mail Transfer Agents (MTA) which handle MTA protocols, namely, Postfix, Mailman Sendmail, are selected for analysis.

3 COMPARISON OF DIFFERENT MTAS

Before comparing different MTAs, the designing criteria of MTAs should be discussed. Regarding to an MTA's function and purpose, the safety of the information carried by the email should be the most important to consider. The usability and the efficiency of transmission of the MTA also matters to its users. Design goals, worries about safety, the beginner or expert level user concerns and more also play a strong role when it comes to the development of the MTA.

3.1 Postfix vs Sendmail in architecture

Postfix is based on semi-resident architecture interoperability process and each process complete specific tasks without any specific process derived relationship (parent-child relationship). In addition, this implementation method has some advantages. For example, each service such as address rewriting can be used by any Postfix components without a process creation overhead as itonly needs to override a postfix address.

The design goal of Postfix is to be a replacement for Sendmail. For this reason, many parts of the Postfix system, such as local delivery procedures can be replaced easily by editing the configuration file like inetd. This makes Postfix and Sendmail to be better compatible, and for users of Sendmail, the transition to Postfix would be easier.

The core of Postfix is realized by more than 10 semi resident programs. Postfix communicates between these processes through the UNIX socket or protected directory under the FIFO to ensure confidentiality.

The amount of data transfer between Postfix processes is limited. In many cases, only the queue file name and the list of recipients or some state information in the process of data exchange between Postfix information. Once a message is stored in the file, it will be saved to a mail delivery program.

Postfix usually adopts some measures to avoid the loss of information. Before the receipt of confirmation, Postfix calls flush and fsync to save all data to disk and checks all the system returned results to avoid error.

Most users will choose Sendmail as mail server, and indeed Sendmail is a good MTA (Anderson & Johnston, 2002). However, Eric Allman design considerations mainly concentrate on the success of the mail transmission. Unfortunately, Sendmail may encounter to Internet environmental safety problem Sendmail. In most systems, Sendmail can only be run as root, which means that any vulnerability may lead to very serious consequences. In addition, the Sendmail cannot afford high load operation.

3.2 Postfix vs Sendmail

The mail system like Sendmail is in accordance with a "single “structural design which achieves all the functions. This structure is conducive to the sharing of data between different parts of the system but this structure can easily create some fatal error. The single structural design method has good insulation, but it increases the costs of process setup and inter process communication overhead. However, through the operation sequence planning, sub module process can be reasonable overhead kept in an acceptable range.

The use of other MTA to replace Sendmail is a troublesome , but users tend to spend a lot of time to become familiar with the allocation and use of new MTA. With Postfix, users can use a lot of their own configuration files (such as access, aliases, virtusertable and so on), by simply clicking in the master.cf definition. In addition, users can use the command "sendmail" to start Postfix. However, the use of one software to replace another software needs to solve specific problems. Part of the reason is because of the safety features of Postfix (Dent, K. D. 2003). The most typical problem occurs in root users send mail. Postfix does not generally improve their authority to deliver the mail, which means root users send mail needs to define alias for the root definition of aliases such as "root: someuser". This also affects the occurrence of several mailing list modules, especially SmartList.

Sendmail has a prominent problem, scalability and performance. For example, if a user requires restart Sendmail to automatically update the configuration file (such as virtual host redirect messages) problems will occur because Sendmail generates a new process to deal with sending and receiving messages. These processes exist until the end of transmission so that user cannot correctly restart the Sendmail. For Postfix, the user only needs to send the command “postfix reload”, and Postfix will reload its configuration files.

3.3 Sendmail vs Qmail

First of all, Sendmail is MTA with a long history of the development, and the current version is 8.10.2. Currently, Sendmail has insurance in portability, stability and guarantee that no bug will exist. However, the Internet has many posts about Sendmail and if an attack occurs, this is a nightmare for administrators. Sendmail has a group of experienced Sendmail administrators in the process of development and a large number of complete documentations. Several of these documents are important for a variety of Sendmail features to be of good use and the current Sendmail is a mature MTA.

However, Sendmail has some shortcomings, its characteristic function is a result of the complexity of the configuration file. Although generating the configuration file by using the M4 macro is easier, it is not easy to master all of the configuration options. Sendmail had numerous security vulnerabilities in the past versions and the prevalence of Sendmail will become the target of an attack. Another problem is that Sendmail is the default configuration with minimal security features, so Sendmail is often easy to attack.

Qmail is another choice. It has taken special consideration of the design and implementation of safety issues. If a user needs a quick solution such as a secure mail gateway, then Qmail is a good choice. Qmail and Sendmail configuration files are completely different (Hafiz & Johnson, 2008). As for Qmail, it has its own configuration file and the configuration directory contains 5-30 different files, each file for the different parts of the configuration (such as virtual domain or virtual host etc.).

This configuration has a very good document, but the code structure of Qmail is not good.

Qmail is much smaller than Sendmail and it lacks some features compared to today's mail server. For example, Qmail does not require verification of the mail sender's domain to ensure the accuracy of the domain name. Qmail Itself does not provide support for RBL and need add-on to achieve. However, Sendmail supports RBL. The greatest problem of Qmail lies in sending messages to multiple receivers on processing. If a user sends a large message to multiple users in the same domain, Sendmail will only send a copy to the mail server. Qmail offers parallel connection times each time it sends a copy to a user. If the user wants to send a large daily mail to multiple users, the use of Qmail will consume a lot of bandwidth. It can be concluded that Sendmail saves the bandwidth resource and Qmail saves time.

The source code of Qmail compared to Sendmail is easier to understand, which is an advantage for less experienced MTA staff. Qmail is stable in terms of safety and it has good technical support but it is not as widely used as Sendmail. Moreover, Qmail is not installed automatically like Sendmail , but it needs manual installation.

Qmail has less add-ons than Sendmail. In general, for less experienced administrators, Qmail is a relatively better choice. Sendmail is similar to the office suite, and 80% of the functions are not used. This makes Qmail more popular in some places as it has some popular and practical features, such as built-in POP3 support. Qmail supports features such as host or user disguise, virtual domains and so on. The simplicity of Qmail also makes the configuration relatively easy.

Qmail Sendmail is considered with respect to be a more secure and efficient operation of the Qmail as a Pentium machine one day can handle about 2000000 messages.

Qmail compared with another MTAs is much simpler, mainly reflected in:

(1) The other MTA's mail, email aliases and mailing list are mechanisms independent of each other, while Qmail uses a simple forwarding mechanism to allow the user to develiver mail.

(2) The other MTAs provide a quick and safe way and not the slow mail delivery queue mechanism; and Qmail is sent by the emergence of new mail triggered, so the delivery of the only one mode is queue quickly.

(3) The other MTAs actually include a specific version of the inetd to monitor the load average of MTA, but Qmail designed the internal mechanism to limit the system load and qmail-smtpd can safely run the INET. Qmail has limited technical support.

Qmail also has some other shortcomings. If it does not fully comply with the standard, it does not support DSN, but Qmail VERP can do the same work. Another problem is that Qmail does not comply with the 7bit standard system and each time it sends 8bit. If the mail receiving party cannot deal with this situation, the message will appear garbled.

4 DISCUSSION

According to the analysis of the three different MTAs in Chapter 3, they are scored 1-10 from low to high regarding each essential criterion, based on how they can be used by different users. Now the rating is carried out based on the information provided in Chapter 3 and makes use of data from an external source.

In terms of just the parameters of usability, security and efficiency, they can be rated as follows.

Table 1. Usability Security and Efficiency Ratings.

	Usability	Security	Efficiency
Postfix	9	10(Good Security Record)	10(Excellent Performance)
SendMail	7	5(Better compared to past versions but is not the best)	6(Relatively ok compared to Exim, but not in par with the performance of Postfix or Qmail)
QMail	8 (predominantly medium sized enterprise and requires high amount of configuration, so this gets a point less than Postfix)	10(Good Security Record)	10 (Excellent Performance and Efficiency)

From Table 1, it is easy to see that each MTA has its own strong features; none of them can cover all three criteria with a high score. However in general, the Postfix is more usable than the other two. However, security for a MTA should be the most important feature, and all the other properties are built on this basis. Thus Postfix can be seen as the best MTA among the three MTAs in general aspects. Usability is an important characteristic and in terms of usability as presented in Chapter 3 already, it is noted that Postfix was primarily a replacement for Sendmail and in thus being it will be able to support a set of users who are already making use of Sendmail. Thus, the usability criteria rating for Postfix automatically score higher. However, an argument can be made that the comparison will not be complete until a more detailed comparison that looks beyond basic argument of usability, security and efficiency is carried out.

Table 2. Outlook of different MTA's

	Postfix	SendMail	Qmail
Outlook	• Introduced in 1997 • Has an established set of strong users • Postfix is very similar to Qmail • Easy to setup • Rests between qmail and Exim • Focused on Protection • Good security record • Excellent Performance • Caters to the need of medium sized communities • No cost, open source	• Sendmail was launched in the year 1982 • It targets large communities • Plagued with many security issues compared to other MTAs • Current versions are more enhanced when it comes to handling protection issues • Standard MTA in Linux systems • Simplicity in configuration and set up • Good for environments where protection is handled differently Good performance Sendmail predominantly works as an internetwork email. It facilitates the use of other mail transfer facilities and also SMTP.	• Qmail is a secure Linux mail server system • In terms of security and protection it has been established that Qmail is more secure than the other two. • The last version update of Qmail was in the year 1997. It was not developed after 1997 and this is a disadvantage because users are not supported when they have concerns and therefore only users who are able to address and implement their own would be able to use it. • There still is a large fan base for Qmail. • Qmail configuration is very complex and hence the usability of this would go down. • Additional filter has to be setup for Qmail as Qmail does not inherently support Sendmail filters

Table 3. Security,Sendmail Milters and Hassle

Security	As presented earlier in terms of security, Postfix can be rated highly. It is thoroughly secure and is a modern version.	Sendmail fails pathetically when it comes to security as compared against Qmail and Postfix. Even its more current versions cannot stand the test with Qmail	In terms of security, although Qmail is old and unsupported, it is still very secure.
Sendmail Milters	Postfix will be able to run milters and also users equivalent Exim milters or filter script		Qmail cannot run milters it is observed that users have to write their own milters (Sill, 2003)
Hassle	Post fix has pretty decent front ends and are easy to user too (Geek, 2010).	Sendmail has the best frontend; however, this is satisfactory only for a novice level user. An expert user might not find the interface of Sendmail satisfactory	Qmail because of the issue of not being supported since 1997 creates a bit of hassle

Table 4. Resource Constraints,Windows Use and Commercial Support

Resource Constraints	Postfix has fewer resource constraints compared to Sendmail	Sendmail has the worst setting possible when it comes to resource constraints	Qmail has lesser resource constraints than the other two.
Windows Use	Postfix does not offer Windows porting	Sendmail offers the best support for a Windows user and also has a native windows port.	Qmail offer null support for Windows
Commercial Support	Support exists for Postfix making it easier for users.	Sendmail is more supported compared to Qmail	The commercial support for qmail was rolled off in the year 1997, and no more commercial support exists for the company.

5 CONCLUSION

With the increasing spread of e-mails, the security of e-mail system proves to be a paramount part of the whole online security network. An insecure mail server is vulnerable to attacks, such as junk mails, intrusion to the mail relay and the denial of service. In light of these facts, this thesis has introduced, compared and analyzed the functions and operations of major mail servers. With detailed description of respective advantages and disadvantages, it also discusses the characteristics and related configuration issues of Postfix, one of the most popular and cost-effective mail servers. In general, Postfix has experienced escalating popularity, due to its efficient e-mail system and high security performance. However, although it has anti-spam functions, it still needs professional software support to deal with the increasing number of spams in the current online community.

REFERENCES

Anderson, R., & Johnston, A. (2002). *Unix unleashed*. Sams Publishing.

Bauer Michael D. (2002, October). Building Secure Servers with Linux. Retrieved:25 June 2017, available at:

https://books.google.fi/books?hl=zh-CN&lr=&id=Ula1nkhJHeQC&oi=fnd&pg=PR9&dq=postfix+server+in+linux&ots=njC72bK1d-&sig=H9v3PtIZ7x4_k_my0ETOhPZRejA&redir_esc=y#v=onepage&q=postfix%20server%20in%20linux&f=false

Dent, K. D. (2003). *Postfix: The Definitive Guide: A Secure and Easy-to-Use MTA for UNIX*. O'Reilly Media, Inc.

Geek, L. (2010). *Sendmail vs Postfix vs Qmail vs Exim*, Retrieved: August 30, 2017 from: http://linuxmantra.com/2010/07/sendmail-vs-postfix-vs-qmail-vs-exim.html

Hafiz, M., & Johnson, R. E. (2008). Evolution of the MTA architecture: The impact of security. *Software: Practice and Experience*, *38*(15), 1569-1599.

Sill, D. (2003). *The Qmail handbook*. Apress