Mail Server basics

Hiranya Prasad Bastakoti

Contents

- SMTP, POP and IMAP principles
- SMTP Relaying Principles
- Mail Domain Administration
- Basic Mail Server Configuration (Sendmail, postfix, qmail, exim..)
- SPAM control and Filtering
- Troubleshooting

Mail Server

- A mail server (sometimes also referred to an e-mail server) is a server that handles and delivers e-mail over a network, usually over the Internet.
- A mail server can receive e-mails from client computers and deliver them to other mail servers.
- A mail server can also deliver e-mails to client computers.

Email and Email Protocols

- It is a store and forward method of composing, sending, storing, and receiving messages over electronic communication systems.
- One of the most popular network services is electronic mail (email).
- Simple Mail Transfer Protocol (SMTP) is the standard mechanism for electronic mail in the internet; the first e-mail systems simply consisted by file transfer, protocols.

Basic Functions of email:

1. Composition 2. Transfer 3. Reporting 4. Displaying and 5. Disposition

- E-mail Protocols are set of rules that help the client to properly transmit the information to or from the mail server. Email protocols are **SMTP, POP,** and **IMAP**

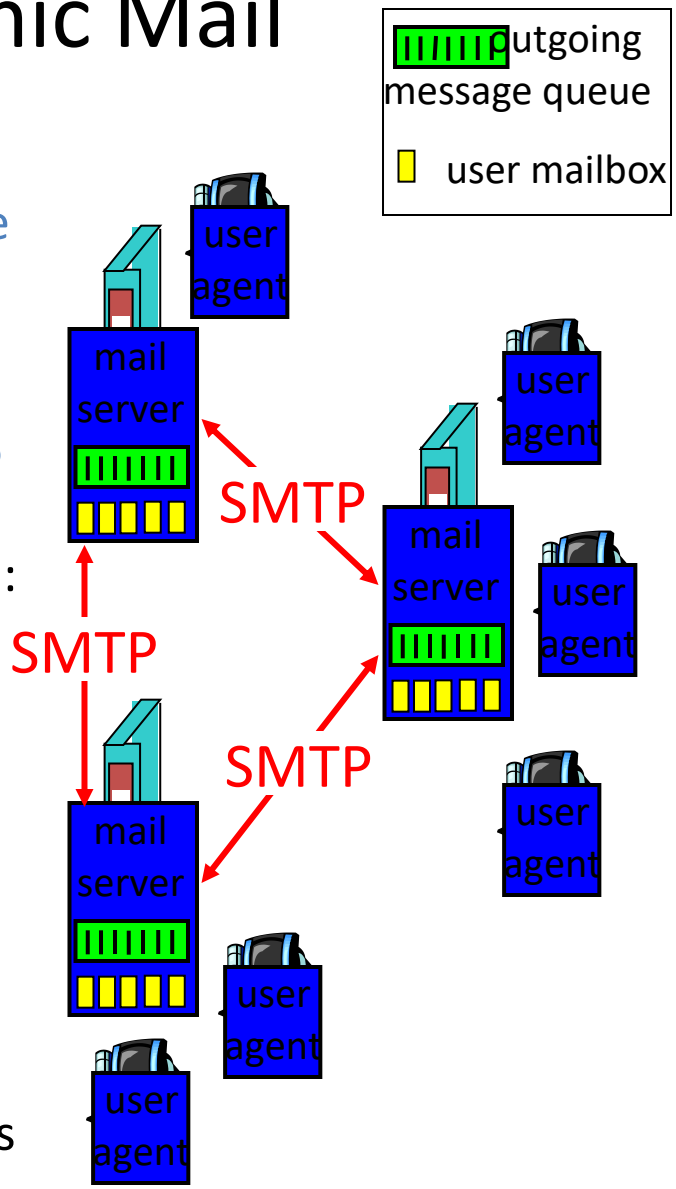
Electronic Mail

Three major components:

- user agents : : They allow the people to read and send e-mail
- mail servers :They move the messages from the source to the destination.
- simple mail transfer protocol: SMTP

- User Agent

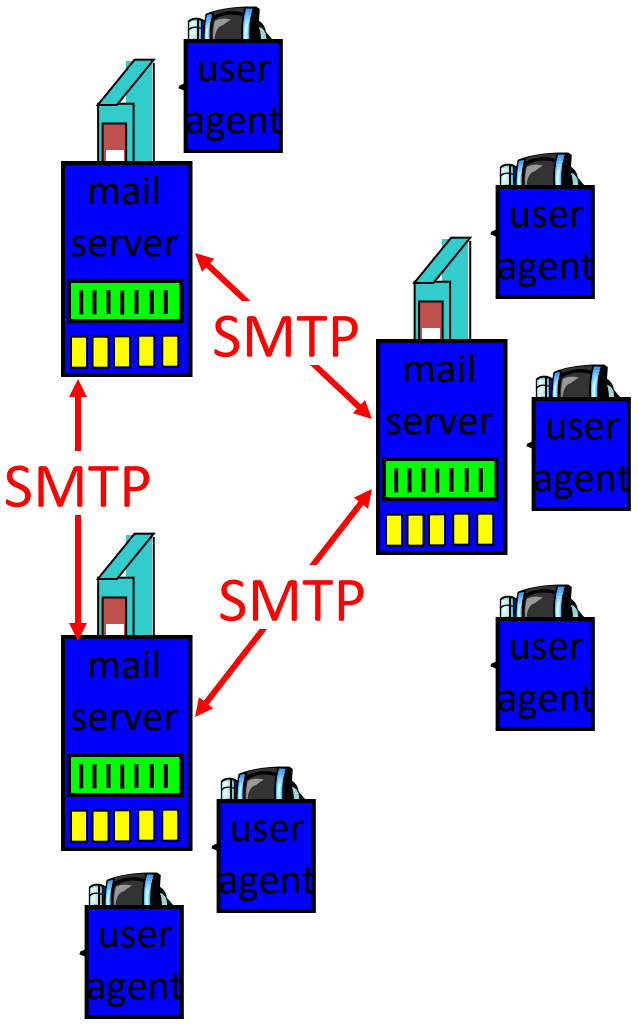
- a.k.a. “mail reader”
- composing, editing, reading mail messages
- e.g., Eudora, Outlook, elm, Netscape Messenger
- outgoing, incoming messages stored on server



Electronic Mail: mail servers

Mail Servers

- mailbox contains incoming messages for user
- message queue of outgoing (to be sent) mail messages
- SMTP protocol between mail servers to send email messages
  - client: sending mail server
  - "server": receiving mail server



SMTP

- **SMTP** stands for **Simple Mail Transfer Protocol**.
- It was first proposed in 1982.
- It is a standard protocol used for sending e-mail efficiently and reliably over the internet.
- SMTP is application layer protocol.
- SMTP is connection oriented protocol.
- SMTP is text based protocol.
- It handles exchange of messages between e-mail servers over TCP/IP network.
- Apart from transferring e-mail, SMPT also provides notification regarding incoming mail.
- When you send e-mail, your e-mail client sends it to your e-mail server which further contacts the recipient mail server using SMTP client.
- These SMTP commands specify the sender's and receiver's e-mail address, along with the message to be send.

- The exchange of commands between servers is carried out without intervention of any user.
- In case, message cannot be delivered, an error report is sent to the sender which makes SMTP a reliable protocol.
- By default, the SMTP protocol works on three ports:
- **Port 25** - this is the default SMTP non-encrypted port
- **Port 2525** - this port is opened on all SiteGround servers in case port 25 is filtered (by your ISP for example) and you want to send non-encrypted emails with SMTP
- **Port 465** - this is the port used if you want to send messages using SMTP securely

SMTP Commands

- HELO – Identifies the client to the server, fully qualified domain name, only sent once per session
- MAIL – Initiate a message transfer, the fully qualified domain of the originator
- RCPT – Follows MAIL, identifies an addressee, typically the fully qualified name of the addressee, and for multiple addressees use one RCPT for each addressee
- DATA – send data line by line

IMAP

- *The Internet Message Access Protocol (IMAP) is a mail protocol used for accessing email on a remote web server from a local client*.
- IMAP allows the client program to manipulate the e-mail message on the server without downloading them on the local computer.
- The e-mail is hold and maintained by the remote server.
- It enables us to take any action such as downloading, delete the mail without reading the mail.
- It enables us to create, manipulate and delete remote message folders called mail boxes.
- IMAP enables the users to search the e-mails.
- It allows concurrent access to multiple mailboxes on multiple mail servers.
- By default, the IMAP protocol works on two ports:
- **Port 143** - this is the default IMAP non-encrypted port
- **Port 993** - this is the port you need to use if you want to connect using IMAP securely

IMAP Commands

- **IMAP_LOGIN:**This command opens the connection.
- **CAPABILITY:**This command requests for listing the capabilities that the server supports
- N**OOP:**This command is used as a periodic poll for new messages or message status updates during a period of inactivity.
- **SELECT:**This command helps to select a mailbox to access the messages.
- **EXAMINE:**It is same as SELECT command except no change to the mailbox is permitted.
- **CREATE:**It is used to create mailbox with a specified name.
- **DELETE:**It is used to permanently delete a mailbox with a given name.
- **RENAME:**It is used to change the name of a mailbox.
- **LOGOUT:**This command informs the server that client is done with the session. The server must send BYE untagged response before the OK response and then close the network connection.

POP

- POP stands for Post Office Protocol.
- POP is an application layer internet standard protocol.
- Since POP supports offline access to the messages, thus requires less internet usage time.
- POP does not allow search facility.
- In order to access the messaged, it is necessary to download them.
- It allows only one mailbox to be created on server.
- It is not suitable for accessing non mail data.
- By default, the POP3 protocol works on two ports:
- **Port 110** - this is the default POP3 non-encrypted port
- **Port 995** - this is the port you need to use if you want to connect using POP3 securely

POP Commands

- **LOGIN:**This command opens the connection.
- **STAT:**It is used to display number of messages currently in the mailbox.
- **LIST:**It is used to get the summary of messages where each message summary is shown.
- **RETR:**This command helps to select a mailbox to access the messages.
- **DELE:**It is used to delete a message.
- **RSET:**It is used to reset the session to its initial state.
- **QUIT:**It is used to log off the session.

POP and IMAP Comparison

S. N.	POP	IMAP
1	Generally used to support single client.	Designed to handle multiple clients.
2	Messages are accessed offline.	Messages are accessed online although it also supports offline mode.
3	POP does not allow search facility.	It offers ability to search emails.
4	All the messages have to be downloaded.	It allows selective transfer of messages to the client.
5	Only one mailbox can be created on the server.	Multiple mailboxes can be created on the server.

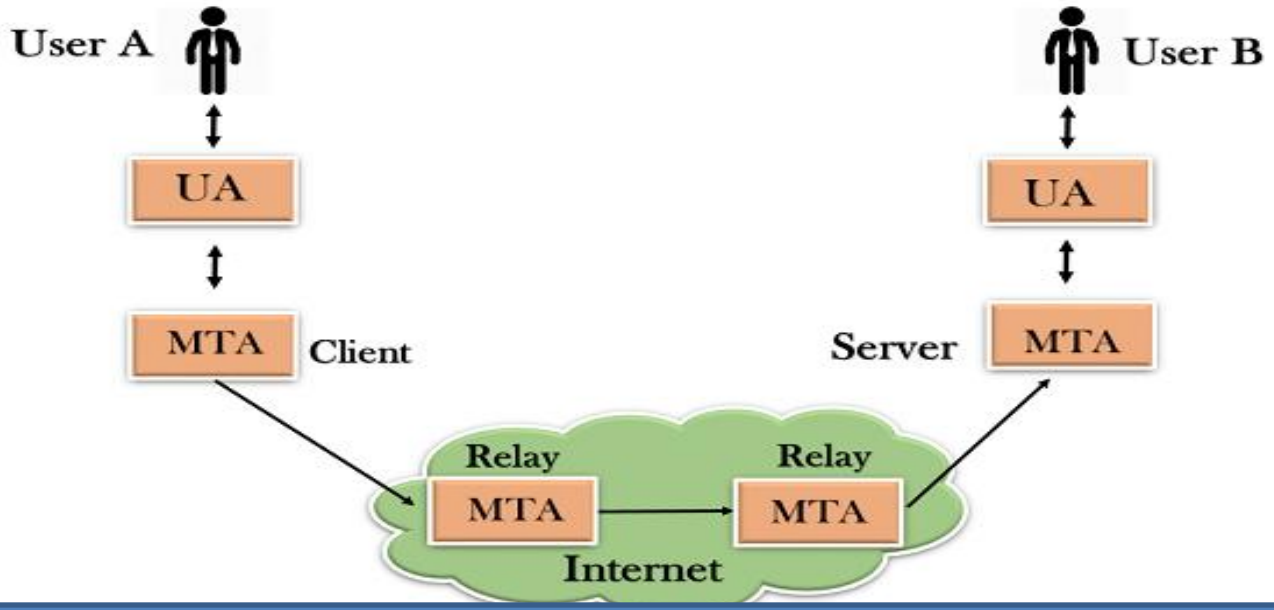
7	POP commands are generally abbreviated into codes of three or four letters. Eg. STAT.	IMAP commands are not abbreviated, they are full. Eg. STATUS.
8	It requires minimum use of server resources.	Clients are totally dependent on server.
9	Mails once downloaded cannot be accessed from some other location.	Allows mails to be accessed from multiple locations.
10	The e-mails are not downloaded automatically.	Users can view the headings and sender of e-mails and then decide to download.
10	POP requires less internet usage time.	IMAP requires more internet usage time.

SMTP Relaying Principles

- The main purpose of SMTP is used to set up communication rules between servers.
- The servers have a way of identifying themselves and announcing what kind of communication they are trying to perform.
- They also have a way of handling the errors such as incorrect email address.
- For example, if the recipient address is wrong, then receiving server reply with an error message of some kind.

Components of SMTP

- SMTP client and SMTP server into two components : user agent (UA) and mail transfer agent (MTA).
- The user agent (UA) prepares the message, creates the envelope and then puts the message in the envelope.
- The mail transfer agent (MTA) transfers this mail across the internet.
- SMTP allows a more complex system by adding a relaying system.
- Instead of just having one MTA at sending side and one at receiving side, more MTAs can be added, acting either as a client or server to relay the email.



The relaying system without TCP/IP protocol can also be used to send the emails to users, and this is achieved by the use of the mail gateway. The mail gateway is a relay MTA that can be used to receive an email.

Working of SMTP

- **Composition of Mail:** A user sends an e-mail by composing an electronic mail message using a Mail User Agent (MUA). Mail User Agent is a program which is used to send and receive mail. The message contains two parts: body and header. The body is the main part of the message while the header includes information such as the sender and recipient address. The header also includes descriptive information such as the subject of the message. In this case, the message body is like a letter and header is like an envelope that contains the recipient's address.
- **Submission of Mail:** After composing an email, the mail client then submits the completed e-mail to the SMTP server by using SMTP on TCP port 25.

- **Delivery of Mail:** E-mail addresses contain two parts: username of the recipient and domain name. For example, ram@gmail.com, where “ram" is the username of the recipient and "gmail.com" is the domain name.
  If the domain name of the recipient's email address is different from the sender's domain name, then MSA will send the mail to the Mail Transfer Agent (MTA). To relay the email, the MTA will find the target domain. It checks the MX record from Domain Name System to obtain the target domain. The MX record contains the domain name and IP address of the recipient's domain. Once the record is located, MTA connects to the exchange server to relay the message.
- **Receipt and Processing of Mail:** Once the incoming message is received, the exchange server delivers it to the incoming server (Mail Delivery Agent) which stores the e-mail where it waits for the user to retrieve it.
- **Access and Retrieval of Mail:** The stored email in MDA can be retrieved by using MUA (Mail User Agent). MUA can be accessed by using login and password.

Mail Domain Administration

- Domain registration: Register a domain name with a domain registrar.
- DNS configuration: Set up DNS records, including MX records, to specify the mail server(s) for the domain.
- Mail server setup: Install and configure mail server software or use a hosted email service. Create user accounts.
- User management: Manage email accounts, assign usernames/passwords, and control access privileges.
- Security measures: Implement encryption (e.g., TLS, spam filtering, and virus scanning.

- Mail routing and forwarding: Configure rules for handling incoming/outgoing emails and set up forwarding if needed.
- Backup and recovery: Establish regular backups for email data and plan for recovery in case of data loss.
- Monitoring and maintenance: Monitor server performance, disk space, and email delivery. Keep software up to date.
- User support: Provide assistance to users for email-related issues and troubleshoot problems.
- Compliance and policies: Ensure compliance with regulations, establish usage guidelines, and define email retention policies.

Basic Mail Configuration

- Sendmail is a feature-rich MTA (Mail Transfer Agent) uses SMTP protocol for sending mail.
- Sendmail is recommended by most of the system administrator as an MTA(Mail transfer agent) server over other MTAs.

Prerequisites Before you Install Sendmail Server on Centos

Step 1 :

- Add the centos 7 EPEL repositories, open terminal and paste the below command:

sudo yum install epel-release

Step 2:

- Install Sendmail with dependency from yum package manager

sudo yum install sendmail sendmail-cf m4

(Note: m4 is a macro processor ,need to use to compile Sendmail configuration file.)

Or

rpm -qa | grep sendmail

Once the installation is done, you will be getting output like this:

```
Transaction Summary
================================================
Install 3 packages
Total download size: 1.2 M
Installed size: 3.1 M
Is this ok [y/d/N]: y
Downloading packages:
(1/3): sendmail-cf-8.14.7-5.el7.noarch.rpm
(2/3): m4-1.4.16-10.el7.x86_64.rpm
(3/3): sendmail-8.14.7-5.el7.x86_64.rpm
------------------------------------------------------------------------------
Total
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
  Installing : m4-1.4.16-10.el7.x86_64
  Installing : sendmail-8.14.7-5.el7.x86_64
  Installing : sendmail-cf-8.14.7-5.el7.noarch
  Verifying  : sendmail-8.14.7-5.el7.x86_64
  Verifying  : sendmail-cf-8.14.7-5.el7.noarch
  Verifying  : m4-1.4.16-10.el7.x86_64
Installed:
  m4.x86_64 0:1.4.16-10.el7                     sendmail.x86_64 0:8.14.7-5.el
Complete!
```

Step 3: Configure Sendmail Server

- Before directly edit **/etc/mail/sendmail.mc** for configuration we need to understand important file existence in **/etc/mail** directory.
- access: allowing or denying other systems to use Sendmail for outbound emails.
- domaintable: used for domain name mapping for Sendmail.
- local-host-names: used to define an alias for a host.
- mailertable: used to override routing for particular domains.
- virtusertable: allowing multiple virtual domains to be hosted on one machine.

```
[root@NL587 ~]# ll /etc/mail
total 192
-rw-r--r-- 1 root root   469 Mar 23  2017 access
-rw-r----- 1 root root 12288 Jul 28 11:29 access.db
-rw-r--r-- 1 root root     0 Jul 28 11:30 aliasesdb-stamp
-rw-r--r-- 1 root root   233 Mar 23  2017 domaintable
-rw-r----- 1 root root 12288 Jul 28 11:29 domaintable.db
-rw-r--r-- 1 root root  5584 Aug  3  2017 helpfile
-rw-r--r-- 1 root root    64 Mar 23  2017 local-host-names
-rw-r--r-- 1 root root   997 Mar 23  2017 mailertable
-rw-r----- 1 root root 12288 Jul 28 11:29 mailertable.db
-rwxr-xr-x 1 root root  2700 Mar 23  2017 make
-rw-r--r-- 1 root root    92 Mar 23  2017 Makefile
-rw-r--r-- 1 root root 58498 Aug  3  2017 sendmail.cf
-rw-r--r-- 1 root root  7306 Mar 23  2017 sendmail.mc
-rw-r--r-- 1 root root 41680 Aug  3  2017 submit.cf
-rw-r--r-- 1 root root  1041 Aug  3  2017 submit.mc
-rw-r--r-- 1 root root   127 Mar 23  2017 trusted-users
-rw-r--r-- 1 root root  1847 Mar 23  2017 virtusertable
-rw-r----- 1 root root 12288 Jul 28 11:29 virtusertable.db
[root@NL587 ~]#
```

Make the following changes in sendmail.mc file below is the command:

- vim /etc/mail/sendmail.mc
- define(`SMART_HOST', `smtp.gmail.com')dnl

Note: Set your SMTP hostname above

Add the below two lines in your sendmail.mc file to listen on port 465 and 587:

- define(`RELAY_MAILER_ARGS', `TCP $h 587')dnl
- define(`ESMTP_MAILER_ARGS', `TCP $h 587')dnl

SPAM control and filtering

- Spam refers to any type of unwanted bulk communication.
- It is sent via email, text messages, social media, or phone calls.
- Spam can also contain relatively harmless content but can clutter up your inbox, consuming valuable space and making it more difficult to identify important, useful emails
- Spam filters are designed to identify emails that attackers or marketers use to send unwanted or dangerous content.
- They use specific filtering methods to identify the content of emails or their senders and then flag the email as spam.
- The email can then be automatically deleted instantly or after a period of time.
- Spam filters can detect spam emails.
- These helpful tools can recognize patterns that spam emails tend to follow.
- A spam filter is a program used to detect unsolicited, unwanted and virus-infected emails and prevent those messages from getting to a user's inbox.

How Does a Spam Filter Work?

Content Filters:

- Content filters analyze the text inside an email and use that information to decide whether or not to mark it as spam.
- The content of spam emails is often predictable, particularly because they tend to have the same basic objectives: offer deals, promote explicit material, or otherwise tap into human emotions, feelings, and desires, such as greed or fear.
- Content filters may search for words connected to money, such as “discount,” “limited time,” or “offer.”
- To trigger the filter, there typically would have to be multiple uses of the target word.
- Content filters may also examine an email for inappropriate language of a sexual nature that could indicate explicit content. In some campaigns, an attacker may use sexually explicit emails to attract users into opening the email and then clicking on malicious links.

Blacklist Filters

- Blacklist email spam filters work by blocking emails from senders that have been put on a list of spammers.
- Blacklist filters are updated on a regular basis because spammers can change their email addresses relatively easily.
- If a spammer switches from one email domain to another, the email may still be able to penetrate the filter until it is updated and the sender's emails once again get labeled as spam.
- A company can also use its own blacklist spam filtering to protect its interests.
- For example, they can use them to target headhunters seeking to attract their employees to other companies.
- They could also use a blacklist filter to block emails that could waste employees' time with sales offers and promotions that could distract them from getting their work done.

Header Filters

- Header filters examine the header of an email to see if it may be coming from an illegitimate source.
- This could include Internet Protocol (IP) addresses that spammers tend to use.
- It may also include information that indicates the email is just one copy of many emails sent at the same time to pre-organized groups of recipients.

Language Filters

- Sometimes spammers target people from other countries, and the email is therefore in a different language than that of the recipient.
- In most cases, a user will only want to receive emails in languages in which they are fluent.
- However, if a business connection or customer from another country reaches out, there exists the chance that the language filter could categorize that legitimate email as spam, so users may have to be instructed to check their spam folders when expecting these kinds of messages.

- **Rule-based Filters**
- We can use a filter to set up specific rules that can be applied to all emails coming into our system. If the email's content or origin matches one of the rules, it can be automatically sent to a spam folder.
- For example, we can set the filter to look for specific words or phrases in the body of an email. If these words are present, the message gets sent to the spam folder.
- We can also set the filter so it looks for particular words or phrases in the header. This can be useful for emails associated with memberships that, while still useful, result in unwanted messages from time to time.
- Rule-based spam filtering is also useful for targeting specific senders. We can set them up to look for information in the domain the email is coming from or the name of the person sending it.

Bayesian Filter

- A Bayesian filter can learn our preferences by examining the emails that our send to spam. It observes the content of the emails we mark as spam and then sets up rules accordingly.
- These rules are then applied to future emails trying to get into our inbox.
- For example, if we constantly mark all emails from a specific sender as spam, a Bayesian filter can recognize this pattern. It will then look for emails from that sender and move them to our spam folder automatically.

Troubleshooting

- Check your connectivity to the Mail Server using Telnet. For example: telnet smtp.gmail.com 587
- If the mail server ports are blocked on your server by a **Firewall**, unblock the ports to allow TCP Connections.
- If the mail server ports are blocked on your server by an **Antivirus**, remove OpManager folder from the antivirus scan.
- Ensure that the authentication provided to access the Mail Server is appropriate.
- The Username provided for authentication should have the authorization to send as the designated From Email ID.
- Make sure that your mail server allows you to send emails to all IP addresses, even if they are emails belonging to external networks.
- It is recommended to use a trusted IP address/proper authentication so that the SMTP server does not block the relaying process.
- Make sure there is sufficient memory in the mail server drive/mail box to receive mails.

Main issues

- Connection issues: Check network connectivity and firewall settings, ensure the server is accessible from the internet, and verify DNS configuration.
- Authentication issues: Verify username and password, check authentication settings, and ensure the authentication mechanism is properly configured.
- Permission issues: Review permissions and access controls for mailboxes, folders, and directories, and make sure appropriate permissions are set for users and services.
- Memory issues: Monitor server memory usage, check for memory leaks or excessive resource consumption by processes, and consider optimizing server configuration or adding more memory if needed.

QA