HES-SO Valais Wallis

SMTP - Protocol

Digital Team Academy

Jowa Dev

17/11/2022

Table of contents

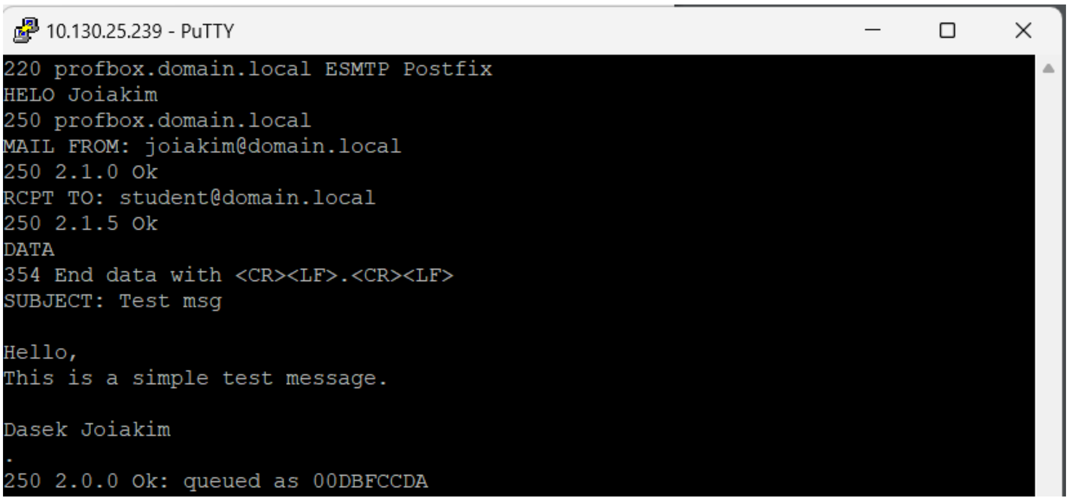
Send a Mail

We will start by sending an email via the integrated terminal of "PuTTY". In order to send an e-mail, a number of steps must be taken. I will detail the different commands for the rest of this document. First of all, you need to open the "PuTTY" software. Insert the IP address "10.130.25.239" as well as the port "25", the port assigned for the "SMTP" service. We can connect "RAW" and establish a connection.

The server will answer us with "SMTP codes", so we will know if everything is going well. Here is the meaning of the codes on the image below:

- 220 : The server is ready
- 250 : Means that the server has transmitted a message
- 354 : This is the typical response to the "DATA" command
- Here are the meanings of the different commands for sending mail:
- HELO : to know if the server answers
- MAIL FROM : to define the sender of the mail
- RCPT TO : to define the receiver
- DATA : allows you to enter first the "subject of the mail" then the body of the mail and to finish sending the mail, just press the "Enter" key, insert a dot "." and press "Enter" again

The server replies that it has transmitted the message with the code "250" and informs the client of the message ID in the queue.



```
220 profbox.domain.local ESMTP Postfix
HELO Joiakim
250 profbox.domain.local
MAIL FROM: joiakim@domain.local
250 2.1.0 Ok
RCPT TO: student@domain.local
250 2.1.5 Ok
DATA
354 End data with <CR><LF>.<CR><LF>
SUBJECT: Test msg

Hello,
This is a simple test message.

Dasek Joiakim
.
250 2.0.0 Ok: queued as 00DBFCCDA
```

Send a Mail outside the server

We will be able to send a mail outside the server and to do this. We need to authenticate ourselves. The command is "AUTH LOGIN" and at that press the "Enter" key. The server answers with the code "334" which means that the authentication request is accepted. It gives us a string in "Base64" which converts to "Username", so we have to enter "student" in "Base64" which gives "c3R1ZGVudA==".

The server asks us for the password in "Base64", we give it back "aGVzc292cyE=". It recognizes us, we can then do exactly the same as the first part, with one difference, we execute twice the command "RCPT TO: host@domain.com" to define several recipients. And that's it, the email has been sent! There is one element that is not displayed in the image below.

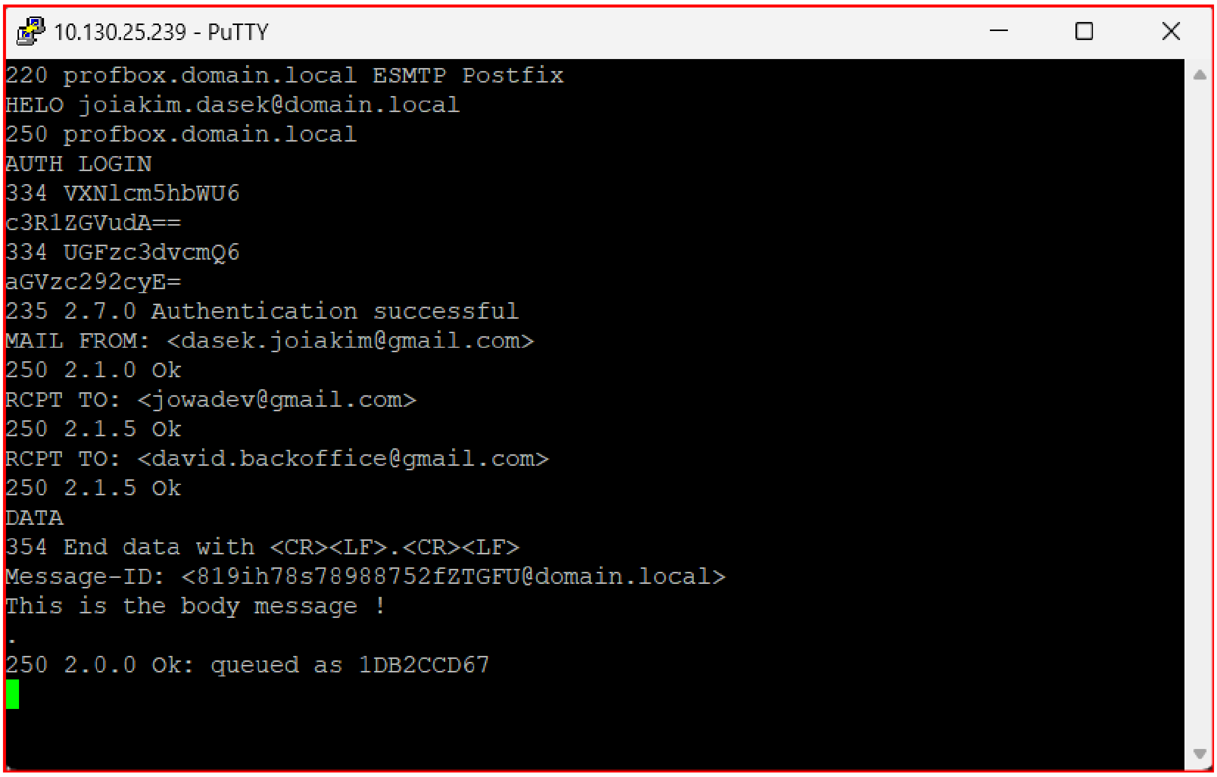
Message ID ?

To be able to send the mail and that the server of "GMAIL" does not reject it. It will be necessary to add in the "headers", a unique identifier. So how to generate a “unique-ID” ?

In summary, one possible approach to generating a Message-ID would be: (M.R. Horton, s.d.)

1. Append "<".
2. Get the current (wall-clock) time in the highest resolution to which you have access (most systems can give it to you in milliseconds, but seconds will do);
3. Generate 64 bits of randomness from a good, well-seeded random number generator.
4. Convert these two numbers to base 36 (0-9 and A-Z) and append the first number, a ".", the second number, and an "@". This makes the left-hand side of the message ID be only about 21 characters long.
5. Append the FQDN of the local host, or the host name in the user's return address.
6. Append ">".

If the random number generator is good, this will reduce the odds of a collision of message IDs to well below the odds that a cosmic ray will cause the computer to miscompute a result. That means that it's good enough.



```
220 profbox.domain.local ESMTP Postfix
HELO joiakim.dasek@domain.local
250 profbox.domain.local
AUTH LOGIN
334 VXNlcm5hbWU6
c3R1ZGVudA==
334 UGFzc3dvcmQ6
aGVzc292cyE=
235 2.7.0 Authentication successful
MAIL FROM: <dasek.joiakim@gmail.com>
250 2.1.0 Ok
RCPT TO: <jowadev@gmail.com>
250 2.1.5 Ok
RCPT TO: <david.backoffice@gmail.com>
250 2.1.5 Ok
DATA
354 End data with <CR><LF>.<CR><LF>
Message-ID: <819ih78s78988752fZTGFU@domain.local>
This is the body message !
.
250 2.0.0 Ok: queued as 1DB2CCD67
```