*Лекції № **8-9**.*
ТЕЗИ

Сервіс електронної пошти. протокол SMTP, робота MTA а прикладі postfix

На минулій лекції ми обговорили сервіс електронної пошти з точки зору клієнта: протоколи POP3, IMAP та MIME.
Нагадаємо коротко:

протоколи POP3 та IMAP служать для віддаленої роботи з поштовою скринькою.
Обидва ***мають вбудовані засоби аутентифікації*** користувача. Також можуть використовувати ще й шифрування трафіку по протоколу Secure Socket Layer (SSL).
Різниця між POP3 та IMAP:
POP3 завантажує пошту на локальний комп'ютер користувача, а IMAP працює з поштою на сервері. При використанні POP3 потрібно повністю завантажити листа на клієнта щоб переглянути напр його заголовки. При роботі з IMAP поштовиа програма якраз заголовки і зтягує (напр. для формування списку), а саме повідомлення завантажується вже тільки на запит.

MIME (Multipurpose Internet Mail Extension) служить для формування та пересилки контенту різного типу в тілі листа.
Початково SMTP-системи були розраховані на передачу інформації виключно в текстовом вигляді і не були орієнтовані на передачу символів національных алфавітов (не кажучи вже про бінарні дані) тобто використовували 7-бітний набір символів. Для подолання цього обмеження і служить MIME.

Протокол SMTP

Сам протокол SMTP дуже простий, його роботу можна перевірити буквально підєднавшись до сервера з допомогою telnet на порт 25 (проробимо це на лаб роботах).
Основні команди SMTP вартозгадати окрема для тестування.

HELO <sending-host> EHLO <sending-host>	Джерело відправки (Хто відправляє листа)
MAIL FROM:<from-address>	Від кого повідомлення
RCPT TO:<to-address>	Для кого повідомлення
DATA	Почати повідомлення
RSET	Перервати повідомлення
VRFY <string>	Перевірити користувача (фактично не використовується зараз)
HELP	Допомога (теж не використовується)
QUIT	Закінчення сеансу

Є і інші, звичайно.
RFC 821 – описано всі.

Ми з вами розглядатимемо як основний приклад MTA postfix а не sendmail (чому - говорилось на попередній лекції).

<u>MTA postfix</u>

Конфігураційні файли по замовчуванню лежать в /etc/postfix (Linux), /usr/local/etc/postfix (FreeBSD). Основних є два: main.cf та master.cf

Для перевірки, перегляду і навіть для маніпуляції конф параметрами в postfix служить утиліта postconf.

main.cf - кілька основних директиви:

myorigin	myorigin = $myhostname (по замовчуванню: відправляти листи від "user@$myhostname") myorigin = $mydomain (можна і так, якщо для конфігуруємо для цілого домену user@$mydomain")	Параметр myorigin задає імя домену, яке використовується в пошті, що відправляється з цієї машини.
mydestination	`mydestination = $myhostname localhost. $mydomain localhost`	Параметр mydestination задає, для каких доменів пошта буде доставлятися локально замість пересилки на інший хост. По замовчуванню, Postfix приймає пошту тільки для локальної машини. Можете вказати один і більше доменів, "/імя/файлу" і/або таблиці пшуку "тип:таблиця (type:table)" (такі, яак hash:, ldap:, чи mysql:), розділяємо їх пробілами і або комами.
mynetworks_style ***mynetworks***	mynetworks_style = subnet (по замовчуванню: авторизувати підмережі) mynetworks_style = host (безпечно: авторизувати тільки локальну машину) mynetworks = 127.0.0.0/8 (безпечно: авторизувати тільки локальну машину)	По замовчуванню, Postfix пересилає пошту від клиентів, що знаходяться в авторизованій частині мережі, на будь-яку адресу. Авторизовані мережі задає конфігураційний параметр mynetworks.
relay_domains	relay_domains = $mydestination	По замовчуванню, Postfix пересилає пошту від постороніх (тобто клиентів, що знаходяться *<u>поза межами авторизованих мереж</u>*) тільки авторизованим доменам. Домены, на які дозволено пересилку

		корреспонденції від посторонніх клиентів, задає параметр relay_domains. По замовчуванню, Postfix вважає авторизованими всі домени (і піддомени), вказанв в mydestination.

Параметрівє більше100, але приведені є найважливішими з точкизору безпеки.

Небезпека open relay! ПОЯСНИТИ!
MTA потрібнонастроюватиДУЖЕ акуратно,і 10 раз перевірятифункіонування, оскільки можна статисерйозною жертвоюспамерів.

Віртуальні домени в Postfix, віртуальні поштові скриньки

описуютьсяяк правилов зовнішніх базах даних. По замовчуванню в файлах hash
Напр:

```
alias_maps = hash:/etc/aliases
alias_database = hash:/etc/aliases
transport_maps = hash:/etc/postfix/transport
virtual_alias_maps = hash:/usr/local/etc/postfix/virtual
```

Форматтакогофайлу типовий (див лаб роботи: аліас: адреса чи адреси). Після того,як відредаговано текстовийфайл, з нього робимо hash файл командою postmap (а такожnewaliases, яка її викликає).
Для локальної доставки (коли користувачікожен має на локальній машині свій рахунок) такі файли цілком прийнятні їх ведення в раз невеликої кількостікористувачів цілком оправдане, однак для сервісу віртуального хостінгув сотнікористувачів такий підхід не використовують (в першу чергу через те,що недоцільно матистільки користувацьких рахунків).
В такомувипадку найчастішевикористовуютьякийсь сервер баз даних або сервіс директорій (LDAP напр.)
Конфіг виглядаєприблизно так:

```
virtual_mailbox_base = /var/mail/virtual
virtual_mailbox_maps = mysql:/usr/local/etc/postfix/sql/users.cf
virtual_alias_maps = mysql:/usr/local/etc/postfix/sql/aliases.cf
virtual_uid_maps = mysql:/usr/local/etc/postfix/sql/uids.cf
virtual_gid_maps = mysql:/usr/local/etc/postfix/sql/gids.cf
local_recipient_maps = $virtual_mailbox_maps $virtual_maps $transport_maps
```

Зауважити,що <u>безпосередньо доставкою</u> поштив локальні поштовіскриньки postfix (MTA) <u>не займається</u>. Це робота доставочного агента (попередня лекція).

Клієнтські поштові скриньки на сервері теж можуть зберігатися в різних форматах.
На сьогоднішній день використовуються ***mbox*** та новіший ***mdir*** а також інші. Є відповідні RFC. ПОЯСНИТИ.
Поштові клієнти працюють з обома фактично прозоро для користувача.

<u>Перевірка контенту</u>.

Очевидно, що зараз вимоги до SMTP сервісу високі: він повинен вміти фільтрувати пошту (антивірус та спам).
Існує кілька методик для провірки вмісту. Наприклад вбудовані (перевірка заголовків) або зовнішні в або не в реальному часі.
Перевірка заголовків дає великий виграш продуктивності. Спам лістинг - один з способів фільтрувати небажану пошту.
Зовнішні програми набагато більш ресурсоємкі (напр. Spam-assassin - ПОЯСНИТИ).

Журнальний (log) файл

/var/log/maillog - в усіх системах (по замовч.). Кожен MTA по замовчуванню веде дуже детальний лог файл руху пошти. Як правило архівується кожного дня.
КОЖНЕ повідомлення отримує свій унікальний номер (а тої кілька - при зовнішній обробці напр)

Поштова черга
перегляд з допомогою команди mailq
Сервер зберігає в черзі листи, які тимчасово неможливо відправити. Час і повідомлення про це - залежно від настройок.

Списки розсилки

Спеціальні заголовки з ВСІЄЮ інфо про список (особливо це стосується можливості відписатися), спеціальні адреси.
Спеціальне ПО: mailman, majordomo.