📘 Повний звіт: Розгортання поштового сервера (Postfix, Dovecot, OpenDKIM)

Система: Debian 13 (Trixie)

Завдання: Налаштувати SMTP/IMAP сервер, забезпечити автентифікацію, налаштувати цифровий підпис (DKIM) та підключити клієнт Thunderbird.

Етап 1: Підготовка системи (DNS та Hostname)

Поштовий сервер не може працювати без коректного імені (FQDN - Fully Qualified Domain Name).

1. Встановлення імені хоста:

su -

hostnamectl set-hostname mail.vbox.local

- **Пояснення:** Ця команда повідомляє ядру Linux, що ім'я цієї машини — mail, а домен — vbox.local. Це ім'я буде використовуватися у заголовках листів.

2. Налаштування локального DNS (/etc/hosts):

nano /etc/hosts

- **Дія:** Знайдіть рядок, що починається з 127.0.1.1, і змініть його на:

127.0.1.1 mail.vbox.local mail

- **Пояснення:** Оскільки сервер не має реальної адреси в інтернеті, ми "вчимо" його, що домен mail.vbox.local знаходиться на цій же машині. Без цього служба Postfix не запуститься.

Етап 2: Встановлення програмного забезпечення

3. Встановлення пакетів:

apt update

apt install postfix dovecot-core dovecot-imapd opendkim opendkim-tools -y

- **Під час встановлення:**
    - Тип конфігурації: **Internet Site** (пряма відправка).

    - System mail name: **vbox.local** (наш поштовий домен).

- **Пояснення:**
    - Postfix: відповідає за передачу пошти (SMTP).
    - Dovecot: відповідає за зберігання пошти та видачу її клієнтам (IMAP).
    - OpenDKIM: інструмент для криптографічного підпису листів.

Етап 3: Налаштування Postfix (SMTP)

Використовуємо утиліту postconf для безпечного внесення змін у файл /etc/postfix/main.cf.

4. Виконайте блок команд:

1. Формат скриньки Maildir (кожен лист - окремий файл)

postconf -e 'home_mailbox = Maildir/'

2. Інтеграція з Dovecot для перевірки паролів (SASL)

postconf -e 'smtpd_sasl_type = dovecot'

postconf -e 'smtpd_sasl_path = private/auth'

postconf -e 'smtpd_sasl_auth_enable = yes'

3. Дозвіл на авторизацію без шифрування (для тестів)

postconf -e 'smtpd_tls_auth_only = no'

postconf -e 'smtpd_sasl_security_options = noanonymous'

4. Політика безпеки (хто може слати листи)

postconf -e 'smtpd_recipient_restrictions = permit_sasl_authenticated, permit_mynetworks, reject_unauth_destination'

5. Підключення DKIM (підпис листів через порт 8891)

postconf -e 'milter_protocol = 2'

postconf -e 'milter_default_action = accept'

postconf -e 'smtpd_milters = inet:localhost:8891'

postconf -e 'non_smtpd_milters = inet:localhost:8891'

- **Пояснення:** Ми налаштували сервер так, щоб він зберігав листи у папці користувача, питав паролі у Dovecot, дозволяв вхід без SSL (бо у нас немає сертифікатів) і підписував усі листи через OpenDKIM.

Етап 4: Налаштування Dovecot (IMAP)

Це найважливіша частина для версії Dovecot 2.4.

5. Редагуємо файл 10-mail.conf (Місце зберігання):

nano /etc/dovecot/conf.d/10-mail.conf

- **Дія 1 (Вимкнути старе):** Знайдіть рядок mail_inbox_path = /var/mail/%{user} (або подібний у блоці # Debian defaults). **Поставте перед ним #**, щоб закоментувати. Це виправить помилку "Permission denied".
- **Дія 2 (Вимкнути mbox):** Закоментуйте # рядки mail_driver = mbox та mail_path = ...
- **Дія 3 (Додати нове):** Додайте ці рядки:

mail_driver = maildir

mail_path = ~/Maildir

- **Дія 4 (Група):** Знайдіть #mail_privileged_group = і зробіть: mail_privileged_group = mail.

6. Редагуємо файл 10-auth.conf (Авторизація):

nano /etc/dovecot/conf.d/10-auth.conf

- **Дія:** Знайдіть рядок #auth_allow_cleartext = ... і приберіть #.

auth_allow_cleartext = yes

- **Пояснення:** Дозволяє передавати пароль у відкритому вигляді. У старих версіях це було disable_plaintext_auth.

7. Редагуємо файл 10-master.conf (Зв'язок з Postfix):

nano /etc/dovecot/conf.d/10-master.conf

- **Дія:** Знайдіть блок service auth і розкоментуйте секцію unix_listener .../private/auth:

```
service auth {
 # ...
 unix_listener /var/spool/postfix/private/auth {
  mode = 0666
  user = postfix
  group = postfix
 }
```

}

- **Пояснення:** Створює канал зв'язку, через який Postfix передає Dovecot-у логіни/паролі для перевірки.

Етап 5: Налаштування OpenDKIM (Підпис)

8. Генерація ключів:

mkdir -p /etc/opendkim/keys

opendkim-genkey -b 2048 -d vbox.local -D /etc/opendkim/keys -s default

chown -R opendkim:opendkim /etc/opendkim/keys

chmod 600 /etc/opendkim/keys/default.private

- **Пояснення:** Створюємо пару ключів (публічний/приватний). Приватним сервером підписує листи.

9. Створення таблиць маршрутизації:

echo "*@vbox.local default._domainkey.vbox.local" > /etc/opendkim/signing.table

echo "default._domainkey.vbox.local vbox.local:default:/etc/opendkim/keys/default.private" > /etc/opendkim/key.table

echo -e "127.0.0.1\nlocalhost\n*.vbox.local" > /etc/opendkim/trusted.hosts

10. Налаштування конфігурації:

nano /etc/opendkim.conf

- **Дія:** Закоментуйте старий Socket local:... (поставте #).
- **Дія:** Вставте в кінець файлу:

KeyTable refile:/etc/opendkim/key.table

SigningTable refile:/etc/opendkim/signing.table

ExternalIgnoreList refile:/etc/opendkim/trusted.hosts

InternalHosts refile:/etc/opendkim/trusted.hosts

Socket inet:8891@localhost

Етап 6: Запуск та Користувач

11. Створення користувача:

adduser user1

(Встановіть пароль '123')

12. Перезапуск служб:

systemctl restart postfix dovecot opendkim

Етап 7: Налаштування клієнтського доступу

Оскільки сервер працює у віртуальній машині VirtualBox з типом мережі **NAT**, він ізольований від зовнішнього світу. Ваш основний комп'ютер (Windows) не бачить IP-адресу сервера (наприклад, 10.0.2.15). Щоб обійти це обмеження, ми використовуємо технологію **Port Forwarding (Переадресація портів)**.

13. Налаштування VirtualBox (Port Forwarding)

Мета: Створити "тунель", крізь який трафік з вашого комп'ютера (Host) потраплятиме всередину віртуальної машини (Guest).

Інструкція:

1. Не вимикаючи віртуальну машину з Debian, перейдіть у меню вікна VirtualBox:
    - **Пристрої (Devices) → Мережа (Network) → Налаштування мережі (Network Settings)**.
2. Переконайтеся, що у полі "Під'єднаний до:" (Attached to) вибрано **NAT**.
3. Розгорніть вкладку **Додатково (Advanced)**.
4. Натисніть кнопку **Переадресація портів (Port Forwarding)**.
5. У вікні, що з'явиться, натисніть **зелений плюс (+)** праворуч, щоб додати нові правила. Нам потрібно два правила для двох протоколів (SMTP для відправки, IMAP для отримання).

Заповніть таблицю точно за цими даними:

Назва (Name)	**Протокол**	**IP хоста (Host IP)**	**Порт хоста (Host Port)**	**IP гостя (Guest IP)**	**Порт гостя (Guest Port)**	**Пояснення дії**
SMTP	TCP	127.0.0.1	**1025**	*(залиште пустим)*	**25**	Перенаправляє запити на відправку пошти. Ми використовуємо порт 1025 на Windows, щоб уникнути конфліктів із системними службами, і перекидаємо його на стандартний порт 25 у Debian.

Назва (Name)	Протокол	IP хоста (Host IP)	Порт хоста (Host Port)	IP гостя (Guest IP)	Порт гостя (Guest Port)	Пояснення дії
IMAP	TCP	127.0.0.1	**1143**	*(залиште пустим)*	**143**	Перенаправляє запити на читання пошти. Порт 1143 на Windows перекидається на стандартний порт 143 у Debian.

6. Натисніть **OK** у вікні правил і **OK** у налаштуваннях мережі. Зміни застосовуються миттєво.

14. Налаштування поштового клієнта Thunderbird

Мета: Підключити поштовий клієнт до сервера, використовуючи створені нами "тунелі" на локальній адресі 127.0.0.1.

Інструкція:

1. Запустіть **Mozilla Thunderbird** на Windows.
2. Натисніть **≡ (Меню) → Створити (New) → Наявний обліковий запис пошти (Existing Mail Account)**.
3. Крок 1: Введення особистих даних

У початковому вікні заповніть:

- **Ваше ім'я:** User1 (або будь-яке інше).
- **Адреса е-пошти:** user1@vbox.local (Thunderbird може попередити, що такий домен не знайдено — ігноруйте це).
- **Пароль:** Введіть пароль, який ви задали командою passwd user1 (наприклад, 123).
- **Важливо:** Натисніть кнопку **"Налаштувати вручну" (Configure manually)**. Не натискайте "Продовжити", бо автоматика не зрозуміє нашу специфічну мережу.

4. Крок 2: Технічна конфігурація серверів

Відкриється таблиця налаштувань. Уважно змініть значення, щоб вони відповідали нашим портам у VirtualBox.

- **СЕРВЕР ВХІДНОЇ ПОШТИ (INCOMING SERVER):**
  - **Протокол:** Виберіть **IMAP**.
  - **Ім'я хоста:** Впишіть 127.0.0.1. *(Ми звертаємося до свого комп'ютера, а VirtualBox перекине це далі).*
  - **Порт:** Впишіть **1143**.

        - **Безпека з'єднання (SSL):** Виберіть **Немає (None)**.
        - **Метод автентифікації:** Виберіть **Звичайний пароль (Normal password)**.
        - **Ім'я користувача:** user1.
    - **СЕРВЕР ВИХІДНОЇ ПОШТИ (OUTGOING SERVER):**
        - **Протокол:** Виберіть **SMTP**.
        - **Ім'я хоста:** Впишіть 127.0.0.1.
        - **Порт:** Впишіть **1025**.
        - **Безпека з'єднання (SSL):** Виберіть **Немає (None)**.
        - **Метод автентифікації:** Виберіть **Звичайний пароль (Normal password)**.
        - **Ім'я користувача:** user1.
5. **Крок 3: Перевірка та завершення**
    - Натисніть кнопку **"Перетестувати" (Re-test)**.
    - Якщо все налаштовано вірно, верхня частина вікна засвітиться **зеленим** написом: *"Такі налаштування було знайдено..."*.
    - Натисніть кнопку **"Готово" (Done)**.
    - З'явиться жовте вікно-попередження: *"Ви підключаєтесь без шифрування"*. Поставте галочку **"Я розумію ризики" (I understand the risks)** і натисніть **Продовжити**.

Результат:

У Thunderbird зліва з'явиться папка user1@vbox.local. Ви зможете успішно відправити тестовий лист самому собі, отримати його у папку "Вхідні" та, відкривши вихідний код листа (Ctrl+U), побачити заголовок DKIM-Signature, що підтверджує коректну роботу цифрового підпису.