Лабораторна робота №9

Додаткові налаштування системи моніторингу Nagios: поштовий сервер, мережевий шлюз, топологія мережі, групи сервісів.

Мета: навчитися виконувати додаткові налаштування системи моніторингу Nagios для розподілення прав між користувачами, визначення часових інтервалів моніторингу, налаштування інформування про критичні події та введення поняття сервісних груп.

Теоретичні відомості

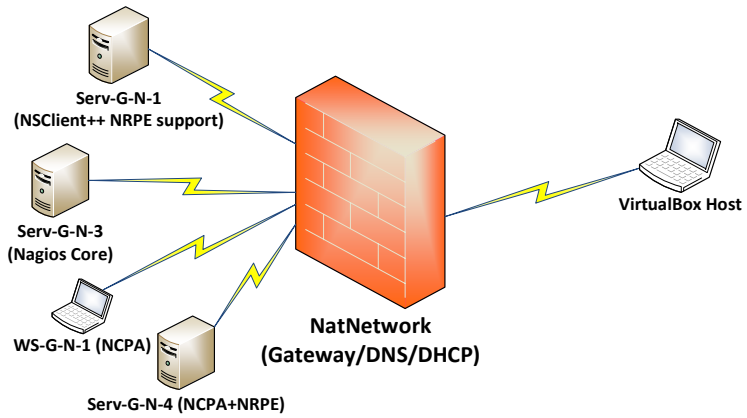


Рис. 9.1. Топологія мережі

На рис. 9.1 наведена модель комп'ютерної мережі, побудована під час виконання попередніх лабораторних робіт. До серверу Serv-G-N-3 налаштовано SSH доступ через NAT Network для VirtualBox Host.

На сервері Serv-G-N-3 розгорнуто систему моніторингу на базі Nagios 4.X. Налаштовано підключення з хосту NAT Network по протоколу HTTP до систему моніторингу під користувачем nagios та surname.

У файлах конфігурації Nagios є налаштування відсилання повідомлень у випадку проблем з хостами або сервісами. Виконаємо додаткові налаштування для повноцінної роботи цього функціоналу.

У файлі ***/usr/local/nagios/etc/objects/contacts.cfg*** визначаються контакти за замовчуванням та інші. Відповідно для кожного хосту або навіть сервісу можливо визначити свій контакт.

Визначаємо контакт для хосту робочої станції. У ***/usr/local/nagios/etc/objects/workstation/ws-22-45-1.cfg*** додаємо рядок

contacts falkovsky

```
define host {
    host_name               WS-22-45-1
    address                 192.168.45.133
    hostgroups              win-workstations
    check_command           check_ncpa!-t 'P@ssw0rd' -P
5693 -M system/agent_version
    contact_groups          admins
    contacts                falkovsky
    max_check_attempts      5
    check_interval          15
    retry_interval          1
    check_period            work-hours
    notification_interval   60
    notification_period     work-hours
    notifications_enabled   1
}
```

Виконуємо перевірку вірності внесених у конфігурацію змін та перезапускаємо сервіс Nagios:

sudo /usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg

sudo service nagios restart

Налаштування поштового сервера

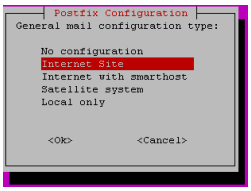
Налаштуємо локальний поштовий сервер для відправлення повідомлень, замість стандартного sendmail, який використовується у Nagios за замовчуванням. Для цього встановимо та сконфігуруємо поштовий агент postfix, що забезпечує більшу гнучкість, зручність адміністрування та сумісність із зовнішніми поштовими сервісами. Команди встановлення postfix:

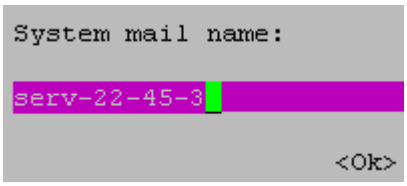
sudo apt update

sudo apt install postfix

sudo apt install mailutils libsasl2-2 ca-certificates libsasl2-modules

Під час встановлення вас буде запитано про тип конфігурації. Оберіть "Internet Site" і натисніть Enter.





Після встановлення налаштовуємо postfix для використання зовнішнього SMTP-серверу. Іншими словами, налаштовуємо Postfix для пересилання пошти через зовнішній поштовий сервер, наприклад:

SMTP Gmail: smtp.gmail.com

SMTP ukr.net: smtp.ukr.net

При цьому необхідно буде ввести логін і пароль реального поштового акаунту. Postfix працюватиме як ретранслятор, а не видаватиме себе за Gmail чи Ukr.net.

Відкриваємо для редагування конфігураційний файл ***/etc/postfix/main.cf*** та змінюємо параметри, що вказує SMTP-сервер, через який пересилаємо пошту та TLS сертифікат.

```
relayhost = [smtp.gmail.com]:587
# relayhost = [smtp.ukr.net]:465
# smtp_tls_wrappermode = yes
smtp_tls_CAfile = /etc/ssl/certs/ca-certificates.crt
```

Додаємо дозвіл використання TLS (шифрування), вмикаємо SASL-аутентифікацію, описуємо файл, де зберігаються логін/пароль SMTP та забороняємо анонімний доступ.

```
# smtp_tls_security_level = encrypt
smtp_use_tls = yes
smtp_sasl_auth_enable = yes
smtp_sasl_password_maps = hash:/etc/postfix/sasl_passwd
smtp_sasl_security_options = noanonymous
# Рядки глобального відправника пошти
myorigin = falkovsky@ukr.net
smtp_generic_maps = hash:/etc/postfix/generic
```

Створюємо файл з паролем ***/etc/postfix/sasl_passwd*** , який вже описаний у конфігурації postfix. Вміст файлу:

```
[smtp.gmail.com]:587 youruser@gmail.com:yourpassword
```

Або

```
[smtp.ukr.net]:465 yourname@ukr.net:yourpassword
```

Захищаємо файл з паролем:

sudo chmod 600 /etc/postfix/sasl_passwd

Це важливо, інакше пароль можуть прочитати інші користувачі системи.

Створюємо файл налаштувань аліасу відправника SMTP-повідомлень ***/etc/postfix/generic*** з вмістом

echo "student@serv-22-45-3 falkovsky@ukr.net" | sudo tee /etc/postfix/generic

де ***student@serv-22-45-3*** – кваліфіковане ім'я поточного користувача серверу Postfix, а ***falkovsky@ukr.net*** – поштовий обліковий запис, що використовується для SMTP-relay. Це потрібно для того, щоб сервер ukr.net дозволив надсилати пошту — і бачити правильну адресу відправника.

Створюємо хеш-файл ***/etc/postfix/generic.db***, який використовує Postfix для швидкого доступу до мапінгу адрес. Сам текстовий файл (/etc/postfix/generic) не читається напряму — потрібен саме .db.:

sudo postmap /etc/postfix/generic

Генеруємо хеш-файл Postfix (використовується Postfix-ом)

sudo postmap /etc/postfix/sasl_passwd

У результаті з'явиться файл ***/etc/postfix/sasl_passwd.db*** — це скомпільована версія, яку читає Postfix. Postfix використовує лише скомпільований файл ***sasl_passwd.db***, а текстовий файл ***/etc/postfix/sasl_passwd*** йому не потрібен під час роботи. Якщо ви не плануєте змінювати пароль, файл ***/etc/postfix/sasl_passwd*** видаляємо після тестувань сервісу.

Перезапускаємо Postfix та перевіряємо стан служби:

sudo systemctl restart postfix

systemctl status postfix

Надсилаємо тестовий лист зі словами ***"Test"*** у тілі, темою ***"Subject"***, від імені falkovsky@ukr.net (прапор -r — задає відправника) на адресу kkik_fiv@ztu.edu.ua.

echo "Test" | mail -s "Subject" -r falkovsky@ukr.net kkik_fiv@ztu.edu.ua

Без -r програма mail спробує надіслати з імені локального користувача (student@serv-22-45-3), що викликає помилки на SMTP сервері ukr.net.

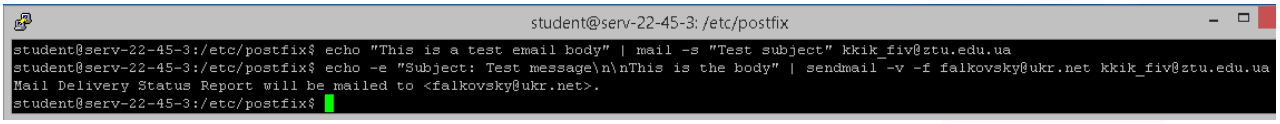
Для перевірки надсилання пошти через Postfix з командного рядка зазвичай використовують sendmail.

echo -e "Subject: Test message\n\nThis is the body" | sendmail -v -f falkovsky@ukr.net your_email@example.com

Пояснення складових команди:

- ***echo -e*** *— виводить текст у стандартний вхід; -e дозволяє використовувати спецсимволи типу \n для переносу рядків.*
- ***"Subject: Test message\n\nThis is the body"*** *— текст повідомлення:*

- ***Subject:*** *— заголовок листа.*
- ***\n\n*** *— порожній рядок відділяє заголовки від тіла листа (обов'язково).*
- ***This is the body*** *— основний текст листа.*
- ***sendmail -v*** *— запускає поштову програму з докладним виводом (verbose), щоб бачити, як саме обробляється доставка.*
- ***falkovsky@ukr.net*** *— адреса відправника (SMTP-relay).*
- ***your_email@example.com*** *— адреса одержувача.*



Після відправлення перевірте свою електронну скриньку, що вказана у командному рядку в якості адреси отримувача, щоб переконатися, що повідомлення було успішно надіслано.

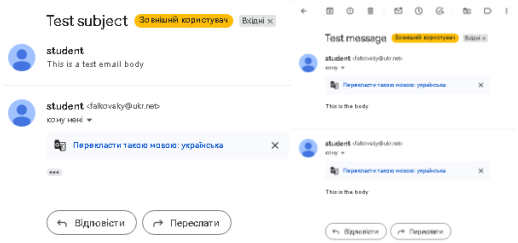


Рис. 9.2. Відправка тестових повідомлень та їх перегляд у скриньці отримувача.

Конфігураційні файли поштових повідомлень Nagios

Якщо повідомлення отримано, змінюємо команди відсилання повідомлень. Для цього в конфігураційному файлі команд системи ***/usr/local/nagios/etc/objects/commands.cfg*** знайдемо відповідні команди:

```
define command {
    command_name    notify-host-by-email
    command_line    /usr/bin/printf "%b" "***** Nagios *****\n\nNotification Type: $NOTIFICATIONTYPE$\nHost:
$HOSTNAME$\nState: $HOSTSTATE$\nAddress: $HOSTADDRESS$\nInfo: $HOSTOUTPUT$\n\nDate/Time: $LONGDATETIME$\n" | /bin/mail -s "**
$NOTIFICATIONTYPE$ Host Alert: $HOSTNAME$ is $HOSTSTATE$ **" $CONTACTEMAIL$
}

define command {
    command_name    notify-service-by-email
    command_line    /usr/bin/printf "%b" "***** Nagios *****\n\nNotification Type: $NOTIFICATIONTYPE$\n\nService:
$SERVICEDESC$\nHost: $HOSTALIAS$\nAddress: $HOSTADDRESS$\nState: $SERVICESTATE$\n\nDate/Time: $LONGDATETIME$\n\nAdditional
Info:\n\n$SERVICEOUTPUT$\n" | /bin/mail -s "** $NOTIFICATIONTYPE$ Service Alert: $HOSTALIAS$/$SERVICEDESC$ is $SERVICESTATE$ **"
$CONTACTEMAIL$
}
```

Та змінимо їх наступним чином:

```
define command {
    command_name    notify-host-by-email
    command_line    /usr/bin/printf "%b" "***** Nagios *****\n\nNotification Type: $NOTIFICATIONTYPE$\nHost: $HOSTNAME$\nState:
$HOSTSTATE$\nAddress: $HOSTADDRESS$\nInfo: $HOSTOUTPUT$\n\nDate/Time: $LONGDATETIME$\n" | /usr/bin/mail -r igor333@ukr.net -s "**
$NOTIFICATIONTYPE$ Host Alert: $HOSTNAME$ is $HOSTSTATE$ **" $CONTACTEMAIL$
}

define command {
    command_name    notify-service-by-email
    command_line    /usr/bin/printf "%b" "***** Nagios *****\n\nNotification Type: $NOTIFICATIONTYPE$\n\nService:
$SERVICEDESC$\nHost: $HOSTALIAS$\nAddress: $HOSTADDRESS$\nState: $SERVICESTATE$\n\nDate/Time: $LONGDATETIME$\n\nAdditional
Info:\n\n$SERVICEOUTPUT$\n" | /usr/bin/mail -r igor333@ukr.net -s "** $NOTIFICATIONTYPE$ Service Alert: $HOSTALIAS$/$SERVICEDESC$ is
$SERVICESTATE$ **" $CONTACTEMAIL$
}
```

Виконуємо перевірку вірності внесених у конфігурацію змін. Перезапускаємо сервіси Nagios та Apache:

sudo /usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg

sudo service nagios restart

Поштова адрес отримувача повідомлень-нотифікацій про критичні зміни стану вказана у файлі контактів ***/usr/local/nagios/etc/objects/contacts.cfg.*** Якщо буде вимкнено будь який хост, або його сервіс, за яким ведеться спостереження, система повинна відправити поштове повідомлення на налаштовану поштову скриньку. Щоб переглянути логи поштового сервісу Postfix необхідно виконати команду (вихід з перегляду клавіша "q"):

sudo less /var/log/mail.log

Вимикаємо робочу станцію та очікуємо повідомлення про цю подію у поштовій скриньці.

Моніторинг мережевого шлюза.

Додаємо у конфігураційний файл груп хостів ***/usr/local/nagios/etc/objects/hostgroups.cfg*** групу, що буде відповідати за мережеві пристрої

```
# Define a hostgroup for Switches And Routers
define hostgroup{
        hostgroup_name  switches
        alias           Network Switches
        }
```

Та коментуємо визначення цієї групи у файлі конфігурації мережевих пристроїв ***/usr/local/nagios/etc/objects/switch.cfg***

```
# Create a new hostgroup for switches
#define hostgroup {
#    hostgroup_name   switches         ; The name of the group
#    alias            Network Switches ; Long name of the group
#}
```

Для розміщення файлів конфігурації мережевих пристроїв використовуємо каталог ***/usr/local/nagios/etc/objects/network***, що ми створили під час виконання однієї з попередніх робіт.
У конфігураційному файлі ***/usr/local/nagios/etc/nagios.cfg***

- перевіряємо присутність каталогу ***/usr/local/nagios/etc/objects/network***
- вимикаємо загальний шаблон ***switch.cfg***
- перевіряємо дозвіл користувачам "підтверджувати отримання попередження" про проблеми з хостами та сервісами.

```
#cfg_file=/usr/local/nagios/etc/objects/switch.cfg
cfg_dir=/usr/local/nagios/etc/objects/network
check_external_commands=1
```

Створюємо конфігураційний файл для мережевого шлюза NAT Network ***/usr/local/nagios/etc/objects/network/snm-gw.cfg*** з наступним вмістом:

```
define host{
    host_name       nat-gateway
    alias           NAT Network Gateway-Switch
    address         192.168.45.129
    hostgroups      switches
    contact_groups  admins
    check_command   check-host-alive
    max_check_attempts      5
    check_interval          15
    retry_interval          1
    check_period            24x7
    notification_interval   60
    notification_period     24x7
    notifications_enabled   1
        }
# Create a service to PING to switch
define service{
    use                     generic-service
    host_name               nat-gateway
    service_description     PING
    check_command           check_ping!200.0,20%!600.0,60%
                }
```

Налаштуємо для всіх хостів ВМ підпорядкування у підключенні до хосту мережевого шлюза NAT Network nat-gateway. Для цього додаємо рядок "parents", що вказує на шлюз групи, до якої належить дана машина до всіх конфігураційних файлів хостів:

```
    parents                 nat-gateway
```

Наприклад, секція визначення хосту у файлі ***/usr/local/nagios/etc/objects/linux/localhost.cfg*** буде мати вигляд:

```
define host {
    hostgroups              linux-servers
    use                     linux-server
    host_name               serv-22-45-3
    alias                   Serv-22-45-3
    address                 127.0.0.1
    contacts                falkovsky
    parents                 nat-gateway
}
```

Виконуємо перевірку вірності внесених у конфігурацію змін та перезапускаємо сервіс Nagios

sudo /usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg

sudo service nagios restart

Результатом цього налаштування будуть зміни у відображенні зв'язків хостів у пункті меню Map (Legacy) сайту Nagios:

При перегляді топології мережі зверніть увагу на метод побудови макету (Layout Method). Його зміна суттєво впливає на представлення карти топології мережі.

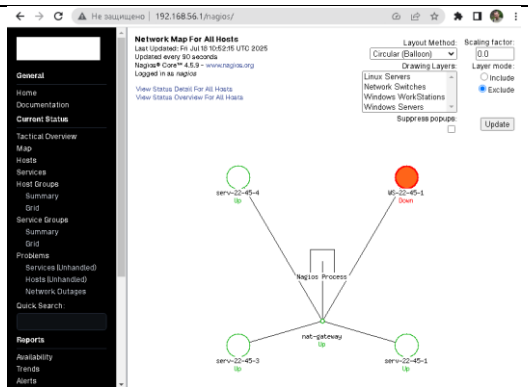


Рис. 9.3. Карта топології мережі після налаштування параметру parents хостів. Map (Legacy)

Створення конфігураційного файлу для груп сервісів

Створюємо новий файл */usr/local/nagios/etc/objects/servicegroup.cfg*. У цьому файлі виконується визначення різних груп сервісів та прив'язка до них конкретних сервісів. Це налаштування виконується для відображення пункту меню Service Groups . Файл повинен мати вміст типу:

```
define servicegroup{
    servicegroup_name       cpuload
    alias                   CPU Load
    members                 serv-22-45-1,CPU Load, serv-22-45-3,Current Load, serv-22-45-4,CPU Usage, WS-22-45-1,CPU Usage
}
```

У цьому прикладі створена група сервісів: "CPU Load" для виведення навантаження на CPU. Група має аліас та список членів. Так само можливо налаштувати будь яку аналогічну групу сервісів. Наприклад об’єднати сервіси, що відповідають за роботу ключових служб контролерів домену, або дані моніторингу пропускної здатності мережі.

Підключаємо конфігураційний файл до Nagios - додаємо новий рядок у конфігураційний файл Nagios */usr/local/nagios/etc/nagios.cfg*, щоб вказати Nagios, що він має завантажити цей файл:

```
cfg_file=/usr/local/nagios/etc/objects/servicegroup.cfg
```

Виконуємо перевірку вірності внесених у конфігурацію змін та перезапускаємо сервіс Nagios:

sudo /usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg

sudo service nagios restart

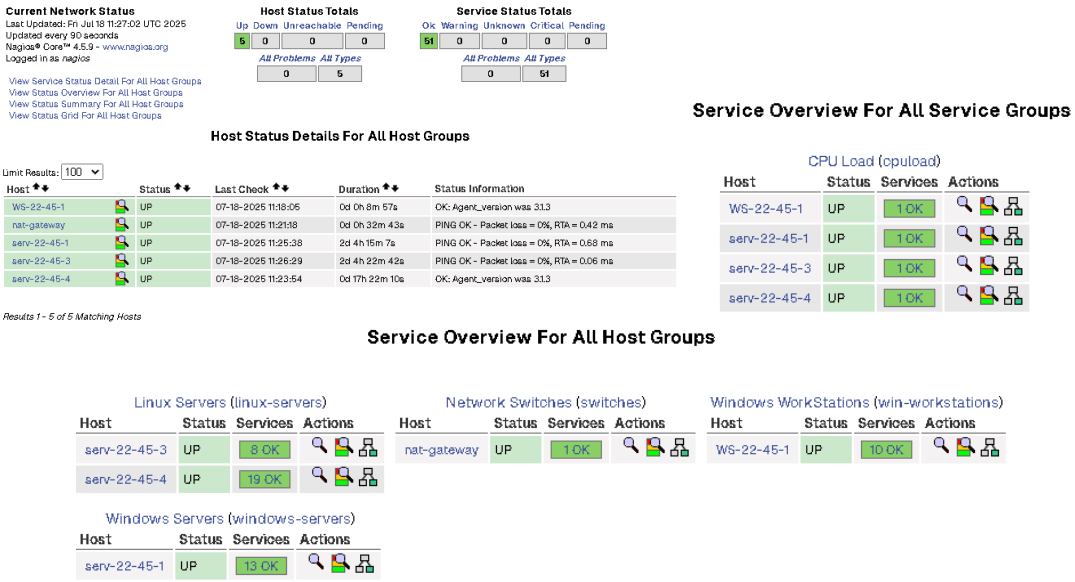


Рис. 9.4. Налаштована група сервісів CPU Load, статуси хостів та групи хостів.

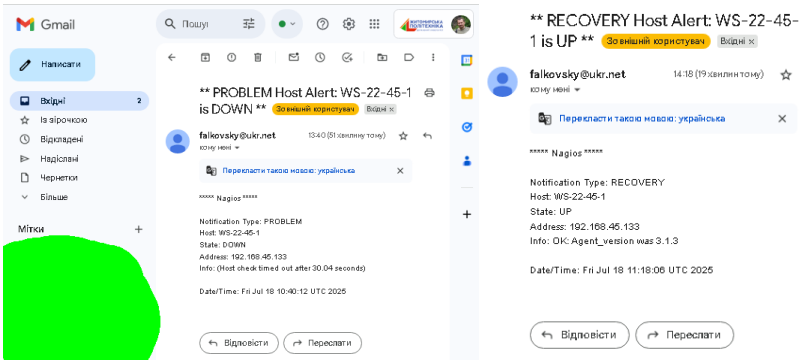


Рис. 9.5. Отримані поштові повідомлення про вимкнення/увімкнення робочої станції.

Перевіряємо налаштовану систему моніторингу Nagios Core. Переходимо у веб-інтерфейс, переглядаємо статуси хостів і сервісів, оцінюємо спрацьовування тригерів. Після симуляції відмов (наприклад, вимкнення хостів) перевіряємо отримані поштові повідомлення на вказані адреси. Успішне надсилання свідчить про правильну інтеграцію Nagios із SMTP-сервером (Postfix + ukr.net/gmail).

Завдання до лабораторної роботи

1. Налаштуйте отримання поштових повідомлень про критичні події «Вимкнення серверу чи станції». У звіт включіть скрін отриманого повідомлення.
2. Налаштуйте базовий моніторинг мережевого шлюза NAT Network та додайте його як «батьківський» пристрій до конфігурацій хостів. У звіт включіть оновлений вигляд Map (Legacy) сайту Nagios.
3. Створіть довільну групу сервісів. Наприклад «навантаження CPU хостів». У звіт включіть відповідний скрін.

Звіт має містити:

- лістинг використаних команд;
- скріншоти отриманих результатів моніторингу у Nagios 4;
- короткий опис редагування файлів конфігурації Nagios 4.

Додаток 9.1.

Інструкція: Postfix + ukr.net (SMTP relay)

Ukr.net вимагає IMAP пароль додатку (не основний пароль облікового запису!). Налаштування протоколу та генерація паролю описані тут.

1. Вмикаємо автентифікацію та TLS у Postfix:

   sudo postconf -e "relayhost = [smtp.ukr.net]:465"
   sudo postconf -e "smtp_sasl_auth_enable = yes"
   sudo postconf -e "smtp_sasl_password_maps = hash:/etc/postfix/sasl_passwd"
   sudo postconf -e "smtp_sasl_security_options = noanonymous"
   sudo postconf -e "smtp_tls_wrappermode = yes"
   sudo postconf -e "smtp_tls_security_level = encrypt"
   sudo postconf -e "smtp_generic_maps = hash:/etc/postfix/generic"

2. Створюємо файл паролів у форматі smtp-сервер логін:пароль

echo "[smtp.ukr.net]:465 yourname@ukr.net:ваш_пароль_додатку" | sudo tee /etc/postfix/sasl_passwd

3. Створюємо файл заміни адреси відправника у форматі системна_адреса smtp-адреса

   echo "student@serv-22-45-3 yourname@ukr.net" | sudo tee /etc/postfix/generic

4. Компілюємо файли до .db:

   sudo postmap /etc/postfix/sasl_passwd
   sudo postmap /etc/postfix/generic

5. Змінюємо права доступу на файли:

   sudo chown root:root /etc/postfix/sasl_passwd /etc/postfix/generic
   sudo chmod 600 /etc/postfix/sasl_passwd /etc/postfix/generic

6. Перезапуск та перевірка стану Postfix:

   sudo systemctl restart postfix
   systemctl status postfix

Додаток 9.2.

Інструкція: Postfix + gmail.com (SMTP relay)

Gmail вимагає пароль додатку (не основний пароль облікового запису!). Налаштування протоколу та генерація паролю описані тут та ось тут ☺.

1. Основні налаштування:

```
sudo postconf -e "relayhost = [smtp.gmail.com]:587"
sudo postconf -e "smtp_sasl_auth_enable = yes"
sudo postconf -e "smtp_sasl_password_maps = hash:/etc/postfix/sasl_passwd"
sudo postconf -e "smtp_sasl_security_options = noanonymous"
sudo postconf -e "smtp_use_tls = yes"
sudo postconf -e "smtp_tls_security_level = encrypt"
sudo postconf -e "smtp_generic_maps = hash:/etc/postfix/generic"
```

2. Файл авторизації:

```
echo "[smtp.gmail.com]:587 yourname@gmail.com:пароль_додатку" | sudo tee /etc/postfix/sasl_passwd
```

3. Файл підстановки адреси:

```
echo "student@serv-22-45-3 yourname@gmail.com" | sudo tee /etc/postfix/generic
```

4. Компіляція та захист:

```
sudo postmap /etc/postfix/sasl_passwd
sudo postmap /etc/postfix/generic
sudo chown root:root /etc/postfix/sasl_passwd /etc/postfix/generic
sudo chmod 600 /etc/postfix/sasl_passwd /etc/postfix/generic
```

5. Змінюємо права доступу на файли:

```
sudo chown root:root /etc/postfix/sasl_passwd /etc/postfix/generic
sudo chmod 600 /etc/postfix/sasl_passwd /etc/postfix/generic
```

6. Перезапуск та перевірка стану Postfix:

```
sudo systemctl restart postfix
systemctl status postfix
```

Корисні посилання

- Як підключити зовнішню програму до скриньки Ukr.net
https://wiki.ukr.net/ManageIMAPAccess

- Access your Ukr.net Account from an Email Program using IMAP
https://www.getmailspring.com/setup/access-ukr-net-via-imap-smtp

- Google.com > Administration > SNMP Configuration
https://www.google.com/support/enterprise/static/gsa/docs/admin/74/admin_console_help/admin_snmp.html

- Google developer. IMAP, POP, and SMTP
https://developers.google.com/workspace/gmail/imap/imap-smtp

- How to Install and Use SendEmail on Linux
https://tecadmin.net/how-to-install-sendemail-in-linux/

- NagiosQL - Nagios configuration tool Files
https://sourceforge.net/projects/nagiosql/files/nagiosql/