



## Лабораторна робота №13 Налаштування SNMP-моніторингу.

**Мета:** розгорнути та налаштувати SNMP-сервер на базі Ubuntu, забезпечити його інтеграцію з агентами моніторингу та використати SNMP-інструменти для аналізу стану системи.

**Інструменти:** гіпервізор VirtualBox, модель комп'ютерної мережі.

### Теоретичні відомості

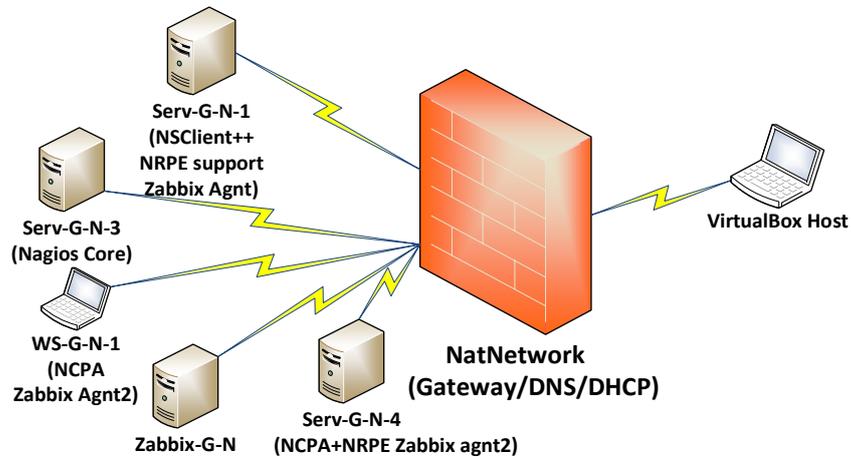


Рис. 13.1. Топологія мережі

На рис. 13.1 наведена модель комп'ютерної мережі, побудована під час виконання попередніх лабораторних робіт. На сервері Serv-G-N-2 розгорнуто систему моніторингу на базі Nagios 4.X. На сервері Zabbix-G-N працює сервер Zabbix з базовими налаштуваннями. В обох моніторингових системах налаштоване спостереження за Serv-G-N-1, WS-G-N-1, Serv-G-N-3.

### Загальні відомості про SNMP (Simple Network Management Protocol)

SNMP – це протокол для моніторингу та управління мережевими пристроями, такими як маршрутизатори, комутатори, сервери, принтери тощо. Основні принципи SNMP-моніторингу:

#### **Архітектура SNMP.**

- Агент (Agent): ПЗ, яке працює на пристрої, що моніториться. Збирає дані пристрою та відповідає на запити.
- Менеджер (Manager): Централізована система, яка опитує агенти, отримує дані та аналізує їх.
- MIB (Management Information Base): БД об'єктів, які можуть бути керовані чи моніторені. Кожен об'єкт описується унікальним ідентифікатором (OID).

#### **Основні операції SNMP**

- Get: Менеджер запитує інформацію в агента.
- Set: Менеджер змінює налаштування на пристрої через агента.
- Trap: Агент самостійно надсилає повідомлення про важливу подію або проблему.
- Walk: Послідовний збір даних з MIB (наприклад, отримання всіх інтерфейсів пристрою).
- Bulk: Оптимізований збір великої кількості даних одним запитом.

#### **Рівні версій SNMP**

- SNMPv1: Початкова версія, базовий набір функцій, слабка безпека.
- SNMPv2c: Додано підтримку "bulk" операцій, але використовується лише «community string» для автентифікації.
- SNMPv3: Додана безпека (шифрування, автентифікація, контроль доступу).

#### **Режими роботи**

- Polling: Менеджер періодично опитує агентів для збору даних.
- Trap-орієнтований: Менеджер отримує тільки події (traps), що надсилаються агентами.

#### **Ключові метрики**

- Статистика інтерфейсів (трафік, помилки, статуси).
- Завантаження процесора та пам'яті.
- Стан дискових накопичувачів.

- Температура, вентилятори, живлення.

SNMP забезпечує ефективний спосіб централізованого контролю мережевих пристроїв і швидкого реагування на події.

### Встановлення SNMP-сервера (snmpd) на Ubuntu Serv-G-N-4

Для забезпечення ефективного вивчення принципів моніторингу SNMP існує широкий вибір безкоштовних інструментів, які можна адаптувати для різних рівнів складності та сценаріїв. Для базових навчальних стендів доцільно використовувати snmpd (Net-SNMP) або MiniSNMPd. Для моделювання складніших мережевих середовищ рекомендовано розгорнути SolarWinds SNMP Simulator або OpenNMS SNMP Mock. У випадках роботи з безпечним протоколом SNMPv3 зручно застосовувати iReasoning або Net-SNMP. А для тестування SNMP-трапів (повідомлень про події) варто скористатися спеціалізованим інструментом SNMPTT.

Встановимо у якості SNMP-сервера на Ubuntu snmpd та snmp(snmpwalk):

```
sudo apt update
sudo apt install snmpd
sudo apt install snmp
```

Для налаштування SNMP, редагуємо файл конфігурації SNMP демона `/etc/snmp/snmpd.conf`, змінюючи такі параметри для базових налаштувань:

```
sysLocation "Basics of system and network monitoring"
sysContact "kkik_fiv@ztu.edu.ua"
agentAddress udp:161
rocommunity public default -V systemonly
```

Значення `agentAddress udp:161` визначає, що 161 порт відкритий для прослуховування на всіх мережевих інтерфейсах хосту. `rocommunity public default -V systemonly` – правило, що визначає рівень доступу до SNMP, коли до агента звертаються через read-only community (тобто читання, без можливості змін)

Перезапускаємо службу SNMP та перевіряємо, чи вона працює:

```
sudo systemctl restart snmpd
snmpwalk -v 2c -c public localhost
```

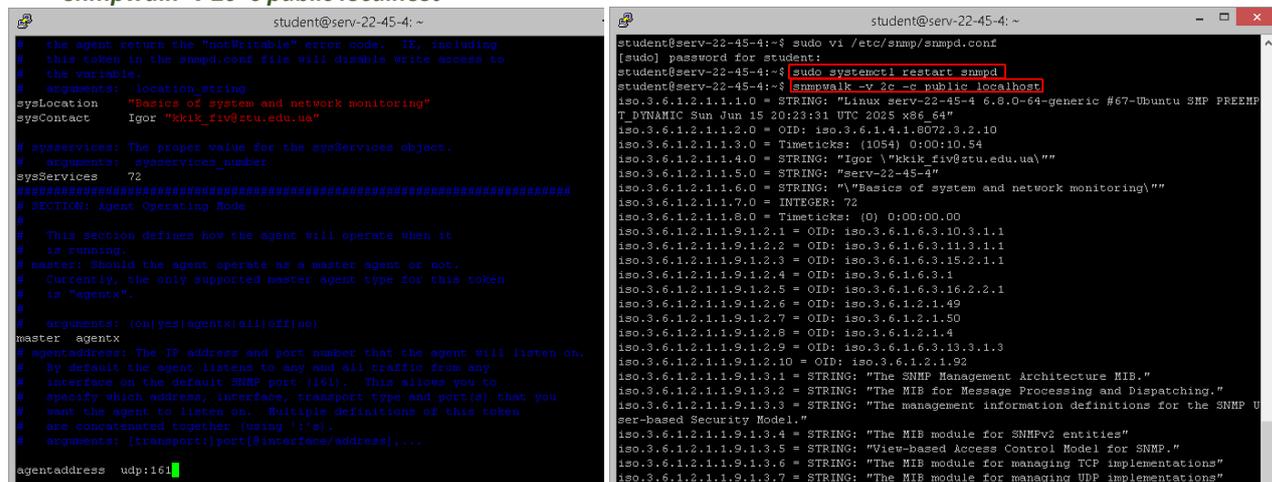


Рис. 13.2. Налаштування SNMPD на сервері Serv-22-45-4

На рис.13.2 показаний процес встановлення, налаштування та перевірки працездатності SNMP-генератора на сервері Serv-G-N-4. Вивід команди snmpwalk є стандартним результатом запиту до SNMP-сервера і показує значення об'єктів, доступних через протокол SNMP.

iso.3.6.1.2.1... —OID (Object Identifier), який ідентифікує конкретний об'єкт в ієрархії MIB (Management Information Base).

= STRING, = INTEGER, = OID — тип значення об'єкта.

Значення справа від = — поточні дані, отримані з сервера.

Відредагуємо файл конфігурації SNMP демона `/etc/snmp/snmpd.conf`, щоб мати можливість отримати інформацію не тільки про системні об'єкти. Замінюємо systemonly на all, щоб мати доступ до всіх об'єктів MIB та коментуємо rocommunity для IPv6:

```
rocommunity public default -V all
#rocommunity6 public default -V systemonly
```



Ми зможемо отримати інформацію не тільки про системні об'єкти, але й про інші компоненти, такі як мережеві інтерфейси, диски тощо.

Додаємо налаштування для моніторингу мережі - доступ до таблиці мережевих інтерфейсів:

```
view all included .1
```

all — дає доступ до всього дерева OID (від кореня .1), що дозволить зібрати дані про трафік, стан інтерфейсів, швидкість тощо.

Додаємо налаштування для моніторингу дискових ресурсів:

```
disk / 10%
disk /var 10%
```

/ — коренева файлова система, 10% — мінімально доступний простір у відсотках (тривога, якщо менше 10%).

Для моніторингу критичних процесів додаємо:

```
proc sshd
proc snmpd
```

sshd, snmpd — приклади процесів, які потрібно перевіряти, якщо ці процеси не працюватимуть, буде сповіщення.

Додаємо налаштування для моніторингу використання пам'яті:

```
load 12 10 5
```

Значення: середнє завантаження CPU за 1, 5 та 15 хвилин. Якщо значення перевищує порогові, буде сповіщення.

Для захисту SNMP-сервера обмежуємо доступ тільки до певних IP-адрес (наприклад, сервера моніторингу):

```
agentAddress udp:161
acl my_networks 192.168.45.128/27
rocommunity public my_networks
```

192.168.45.128/27 — підмережа, якій дозволено доступ.

Зберігаємо внесені зміни конфігурації, перезапускаємо службу SNMP та перевіряємо роботу snmpwalk

```
sudo systemctl restart snmpd
snmpwalk -v 2c -c public localhost
```

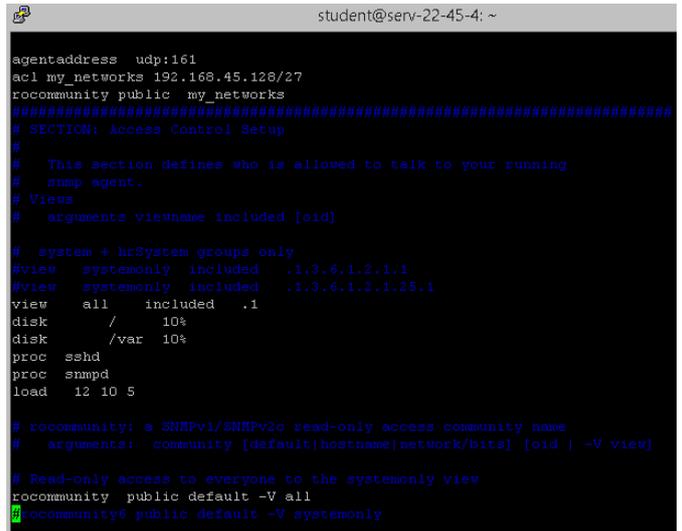


Рис. 13.3. Конфігурація SNMPD на сервері Serv-22-45-4

OID .1.3.6.1.4.1.2021 належить до UCD-SNMP-MIB, яка надає розширену інформацію про системні ресурси, включаючи використання пам'яті, CPU, файлових систем і процесів. У додатку 2 наведено приклади командних рядків snmpwalk для окремих перевірок з використанням OID .1.3.6.1.4.1.2021.

Для моніторингу мережевих інтерфейсів через SNMP використовується IF-MIB. Основний OID для цієї MIB — .1.3.6.1.2.1.2, що містить інформацію про всі інтерфейси. У додатку 3 цього документа наведено основні об'єкти IF-MIB для мережевих інтерфейсів.

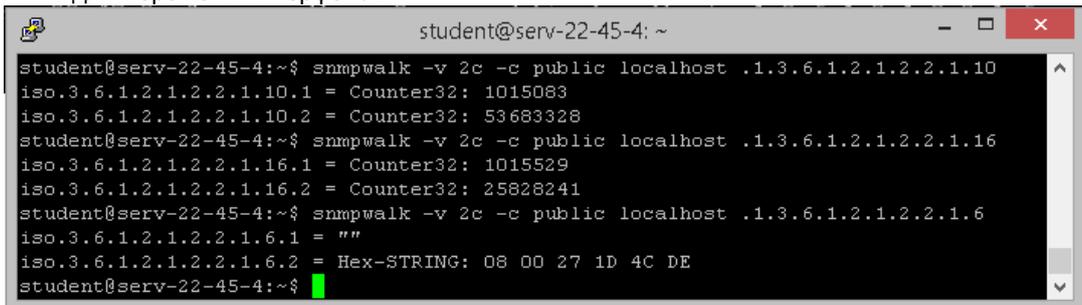


Рис. 13.4. SNMP-статистика на інтерфейсах Serv-22-45-3

- .1.3.6.1.2.1.2.1.10 # прийняті байти,
- .1.3.6.1.2.1.2.1.16 # передані байти,
- .1.3.6.1.2.1.2.1.6 #MAC-адреси.



## Перевірка працездатності агентів моніторингу на сервері Serv-G-N-4

Крім налаштованого SNMP на сервері повинні працювати агенти ncpa та nrpe, призначені для обміну інформацією з Nagios Core. Перевіряємо їх статус:

**sudo service ncpa status**

**sudo service nrpe status**

Якщо якийсь з сервісів не працює, відновлюємо його працездатність за алгоритмом, викладеним у додатку 1 цього документа.

```
student@serv-22-45-4:~$ sudo service ncpa status
ncpa.service - NCPA
   Loaded: loaded (/usr/lib/systemd/system/ncpa.service; enabled; preset: enabled)
   Active: active (running) since Mon 2025-07-21 07:51:53 UTC; 1 day 10h ago
     Docs: https://www.nagios.org/ncpa
   Main PID: 717 (ncpa)
    Tasks: 3 (limit: 1663)
  Memory: 106.9M (peak: 107.2M)
     CPU: 1min 21.919s
   CGroup: /system.slice/ncpa.service
           └─717 /usr/local/ncpa/ncpa -n
             └─883 /usr/local/ncpa/ncpa -n
               └─884 /usr/local/ncpa/ncpa -n

Jul 21 07:51:53 serv-22-45-4 systemd[1]: Started ncpa.service - NCPA.
Jul 21 07:52:32 serv-22-45-4 ncpa[717]: **** Starting NCPA version: 3.1.3
Jul 21 07:52:32 serv-22-45-4 ncpa[717]: **** Starting NCPA version: 3.1.3
student@serv-22-45-4:~$ sudo service nrpe status
nrpe.service - Nagios Remote Plugin Executor
   Loaded: loaded (/usr/lib/systemd/system/nrpe.service; enabled; preset: enabled)
   Active: active (running) since Mon 2025-07-21 07:51:53 UTC; 1 day 10h ago
     Docs: http://www.nagios.org/documentation
   Main PID: 720 (nrpe)
    Tasks: 1 (limit: 1663)
  Memory: 6.0M (peak: 9.8M)
     CPU: 44.231s
   CGroup: /system.slice/nrpe.service
           └─720 /usr/local/nagios/bin/nrpe -c /usr/local/nagios/etc/nrpe.cfg -f

Jul 21 07:51:53 serv-22-45-4 systemd[1]: Started nrpe.service - Nagios Remote Plugin Executor.
Jul 21 07:51:55 serv-22-45-4 nrpe[720]: Starting up daemon
Jul 21 07:51:56 serv-22-45-4 nrpe[720]: Server listening on 0.0.0.0 port 5666.
Jul 21 07:51:56 serv-22-45-4 nrpe[720]: Server listening on :: port 5666.
Jul 21 07:51:56 serv-22-45-4 nrpe[720]: Warning: Daemon is configured to accept command arguments from clients!
Jul 21 07:51:56 serv-22-45-4 nrpe[720]: Listening for connections on port 5666
Jul 21 07:51:56 serv-22-45-4 nrpe[720]: Allowing connections from: 127.0.0.1,::1,192.168.45.136
student@serv-22-45-4:~$
```

Рис. 13.5. Перевірка стану ncpa та nrpe на сервері Serv-22-45-4

Перевіряємо стан Zabbix Agent2 на цьому ж хості:

**sudo systemctl status zabbix-agent2**

```
student@serv-22-45-4:~$ sudo systemctl status zabbix-agent2
zabbix-agent2.service - Zabbix Agent 2
   Loaded: loaded (/usr/lib/systemd/system/zabbix-agent2.service; enabled; preset: enabled)
   Active: active (running) since Tue 2025-07-22 12:38:25 UTC; 6h ago
     Main PID: 6466 (zabbix_agent2)
    Tasks: 12 (limit: 1663)
  Memory: 15.2M (peak: 19.3M)
     CPU: 1min 12.803s
   CGroup: /system.slice/zabbix-agent2.service
           └─6466 /usr/sbin/zabbix_agent2 -c /etc/zabbix/zabbix_agent2.conf

Jul 22 12:38:25 serv-22-45-4 systemd[1]: Started zabbix-agent2.service - Zabbix Agent 2.
Jul 22 12:38:25 serv-22-45-4 zabbix_agent2[6466]: Starting Zabbix Agent 2 (7.4.0rc2)
Jul 22 12:38:25 serv-22-45-4 zabbix_agent2[6466]: Zabbix Agent2 hostname: [serv-22-45-4]
Jul 22 12:38:25 serv-22-45-4 zabbix_agent2[6466]: Press Ctrl+C to exit.
student@serv-22-45-4:~$ ps -e | grep zabbix
6466 ?        00:01:10  zabbix_agent2
student@serv-22-45-4:~$
```

Рис. 13.6. Перевірка стану Zabbix Agent2 на сервері Serv-22-45-4

Ім'я процесу Zabbix Agent2 для додавання до систем моніторингу перевіряємо командою **ps -e | grep zabbix**

Всі прямі перевірки працездатності сервісів на сервері Serv-22-45-4 виконано.

Зверніть увагу, що одним з завдань даної лабораторної роботи є налаштування SNMP-моніторингу працездатності даних сервісів. У прикладі ми виконали тільки пряму перевірку працездатності агентів моніторингу.

## Практичне застосування SNMP-клієнта з GUI для збору інформації з серверу Serv-G-N-4

Існує кілька безкоштовних GUI-інструментів для Windows x64 для роботи з SNMP на віддалених хостах. Вони дозволяють виконувати snmpwalk, snmpget, переглядати дерева OID, зчитувати та іноді навіть будувати графіки на основі SNMP-даних. Ось порівняння кількох гарних на момент написання цього документа безкоштовних рішень:

Безкоштовні GUI-інструменти для Windows x64 для роботи з SNMP

Інструмент	SNMPv1/v2c/v3	MIB-завантаження	SNMPWalk	Traps	Примітки
iReasoning MIB Browser	✓	✓	✓	✓	Найзручніший GUI
SnmpB	✓	✓	✓	✓	Open Source
ManageEngine MIB Browser	✓	✓	✓	✗	Простий та інтуїтивний
Paessler SNMP Tester	✓	✗	✓	✗	Для швидкої перевірки

Використаємо iReasoning MIB Browser, як найбільш функціональний та простий у налаштуванні, для встановлення на робочу станцію WS-G-N-1. Завантажуємо файл інсталяції setup.exe зі сторінки <https://www.ireasoning.com/downloadmibbrowserfree.php> та виконуємо дії показані на рис. 13.7.

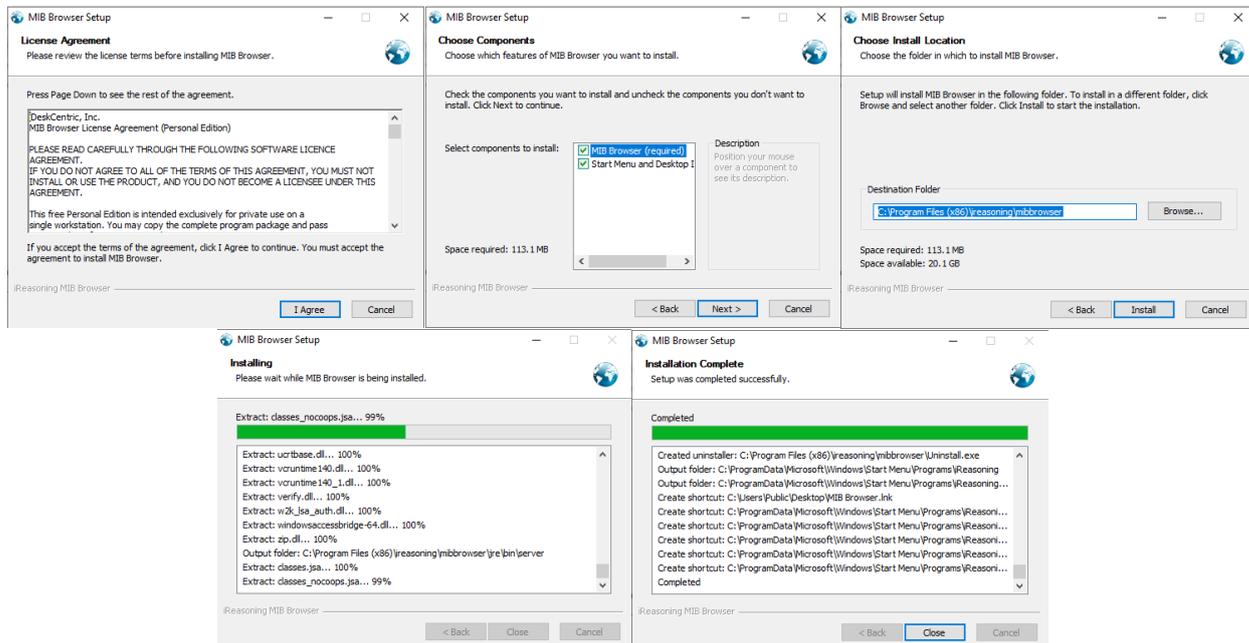


Рис. 13.7. Встановлення iReasoning MIB Browser на WS-22-45-1

Запускаємо встановлений MIB Browser та підключаємося до Serv-G-N-4, на якому попередньо налаштовано службу snmpd, вказуючи у полі Address його адресу. Завантажуємо MIB-модулі (при потребі) або використовуємо вже вбудовані MIB'и клієнта. Виконуємо SNMP-запити типу GET, наприклад, до таких OID:

- .1.3.6.1.2.1.1.0 — системний опис пристрою (sysDescr),
- .1.3.6.1.2.1.2.2 — таблиця мережевих інтерфейсів,
- .1.3.6.1.4.1.2021.9 — інформація про файлові системи (UCD-SNMP-MIB).

Аналізуємо отримані відповіді від SNMP-агента. У разі успішного налаштування буде отримано значення об'єктів MIB, що підтверджує працездатність SNMP-взаємодії.

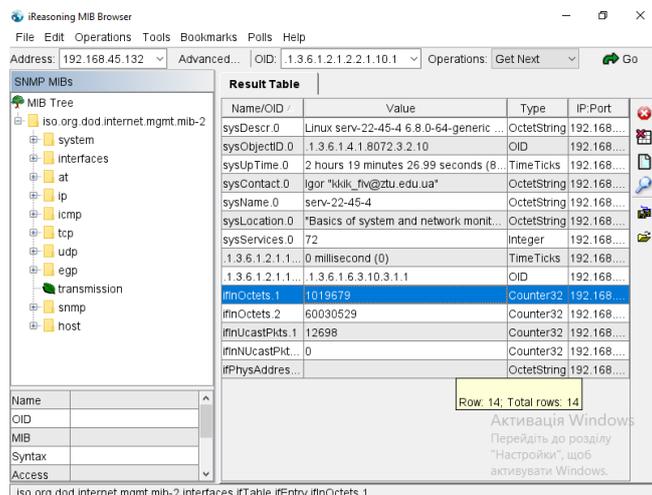


Рис. 13.8. Робота з MIB Browser на WS-22-45-1



### Завдання до лабораторної роботи

1. Встановіть та налаштуйте на сервері Ubuntu (Serv-G-N-4) SNMP-сервер на базі snmpd. Забезпечте службі snmpd доступ до всіх об'єктів MIB.
2. Перевірте працездатність раніше встановлених та налаштованих на сервері Serv-G-N-4 агентів моніторингу ncpa, nrpe, Zabbix Agent2
3. Змініть налаштування snmpd таким чином, щоб можна було додатково відслідковувати стан наступних процесів агентів моніторингу встановлених на сервері (ncpa, nrpe, zabbix-agent2).
4. Використовуючи SNMP-інструмент командного рядка snmpwalk, виконайте моніторинг характеристик серверу Serv-G-N-4 за наступними показниками: використання пам'яті, завантаження процесора, інформація про мережеві інтерфейси, статистика дисків, стан обраних процесів. Інтерпретуйте результати виконання кожної команди. Зробіть висновки щодо стану системи на основі отриманих метрик.
5. Встановіть на робочій станції WS-G-N-1 iReasoning MIB Browser та отримайте кілька базових значень об'єктів MIB з Serv-G-N-4.

### Звіт має містити:

- лістинг використаних команд;
- короткий опис редагування файлів конфігурації;
- скріншоти налаштувань та підключень;
- для кожної snmpwalk-команди наведіть:
  - використаний OID і його опис,
  - отриманий результат,
  - інтерпретацію значень,
- додайте загальний висновок щодо стану системи.

Додаток 1.

### Виправлення помилки з запуском клієнта Nagios на Ubuntu.

Виправлення помилки з роботою ncpa. Перевіряємо статус служби клієнта.

```
sudo service ncpa status
```

Вимикаємо автозапуск служби NCPA, щоб вона не запускала під час перезавантаження системи.

```
sudo systemctl disable ncpa
```

```
sudo reboot
```

```
sudo service ncpa status
```

Змінюємо права доступу до файлу процесу ncpa.pid, щоб дозволити його видалення та видаляємо.

```
sudo chmod 777 /usr/local/ncpa/var/run/ncpa.pid
```

```
sudo rm /usr/local/ncpa/var/run/ncpa.pid
```

Перезапускаємо службу та відновлюємо її автозапуск.

```
sudo service ncpa restart
```

```
sudo systemctl enable ncpa
```

Це універсальний алгоритм відновлення та працює також з nrpe. Файл процесу nrpe-клієнта знаходиться по шляху /usr/local/nagios/var/nrpe.pid



### Приклади командних рядків snmpwalk для окремих перевірок.

Таблиця 13.2.

<i>snmpwalk -v 2c -c public localhost .1.3.6.1.4.1.2021</i>	Моніторинг ресурсів системи, включаючи використання пам'яті, CPU, файлових систем і процесів.
Приклади для перевірки дисків	
<i>snmpwalk -v 2c -c public localhost .1.3.6.1.4.1.2021.9</i>	Перевірка дисків.
<i>snmpwalk -v 2c -c public localhost .1.3.6.1.4.1.2021.9.1.2</i>	Ім'я файлової системи.
<i>snmpwalk -v 2c -c public localhost .1.3.6.1.4.1.2021.9.1.3</i>	Тип файлової системи.
<i>snmpwalk -v 2c -c public localhost .1.3.6.1.4.1.2021.9.1.6</i>	Загальний обсяг диску (KB).
<i>snmpwalk -v 2c -c public localhost .1.3.6.1.4.1.2021.9.1.7</i>	Обсяг використаного місця (KB).
<i>snmpwalk -v 2c -c public localhost .1.3.6.1.4.1.2021.9.1.8</i>	Вільний обсяг диску (KB).
Приклади для перевірки процесів	
<i>snmpwalk -v 2c -c public localhost .1.3.6.1.4.1.2021.2</i>	Перевірка процесів
<i>snmpwalk -v 2c -c public localhost .1.3.6.1.4.1.2021.2.1.2</i>	Перевірка процесу 1. Назва процесу.
<i>snmpwalk -v 2c -c public localhost .1.3.6.1.4.1.2021.2.1.5</i>	Перевірка процесу 1. Статус процесу.
Приклади для перевірки завантаження CPU	
<i>snmpwalk -v 2c -c public localhost .1.3.6.1.4.1.2021.10</i>	Перевірка завантаження CPU.
<i>snmpwalk -v 2c -c public localhost .1.3.6.1.4.1.2021.10.1.3.1</i>	Перевірка завантаження CPU за 1 хв
<i>snmpwalk -v 2c -c public localhost .1.3.6.1.4.1.2021.10.1.3.2</i>	Перевірка завантаження CPU за 5 хв
<i>snmpwalk -v 2c -c public localhost .1.3.6.1.4.1.2021.10.1.3.3</i>	Перевірка завантаження CPU за 15 хв
Приклади для перевірки використання пам'яті	
<i>snmpwalk -v 2c -c public localhost .1.3.6.1.4.1.2021.4</i>	Інформація про використання пам'яті (KB)
<i>snmpwalk -v 2c -c public localhost .1.3.6.1.4.1.2021.4.3</i>	Сумарна фізична пам'ять (Total Swap Memory).
<i>snmpwalk -v 2c -c public localhost .1.3.6.1.4.1.2021.4.4</i>	Сумарна RAM пам'ять.
<i>snmpwalk -v 2c -c public localhost .1.3.6.1.4.1.2021.4.5</i>	Вільна фізична пам'ять (Free Swap Memory).
<i>snmpwalk -v 2c -c public localhost .1.3.6.1.4.1.2021.4.6</i>	Вільна RAM пам'ять (Free RAM).
<i>snmpwalk -v 2c -c public localhost .1.3.6.1.4.1.2021.4.13</i>	Сумарна буферна пам'ять (Buffer Memory).
<i>snmpwalk -v 2c -c public localhost .1.3.6.1.4.1.2021.4.14</i>	Сумарна пам'ять у кеші (Cached Memory).
<i>snmpwalk -v 2c -c public localhost .1.3.6.1.4.1.2021.4.15</i>	Сумарна доступна пам'ять (Shared Memory).
<i>snmpwalk -v 2c -c public localhost .1.3.6.1.4.1.2021.4.5.0</i>	Загальний обсяг пам'яті (memTotalReal) (KB).
<i>snmpwalk -v 2c -c public localhost .1.3.6.1.4.1.2021.4.6.0</i>	Вільна пам'ять (memAvailReal) (KB).
<i>snmpwalk -v 2c -c public localhost .1.3.6.1.4.1.2021.4.11.0</i>	Використана пам'ять (memTotalReal - memAvailReal) (KB).
<i>snmpwalk -v 2c -c public localhost .1.3.6.1.4.1.2021.4.3.0</i>	Загальний розмір swap (KB).
<i>snmpwalk -v 2c -c public localhost .1.3.6.1.4.1.2021.4.4.0</i>	Вільний swap (KB).



### Основні об'єкти IF-MIB для інтерфейсів.

Таблиця 13.3.

OID	Назва	Опис
.1.3.6.1.2.1.2.1.0	ifNumber	Кількість інтерфейсів у системі.
.1.3.6.1.2.1.2.2.1.1	ifIndex	Індекс інтерфейсу (унікальний для кожного).
.1.3.6.1.2.1.2.2.1.2	ifDescr	Опис інтерфейсу (наприклад, eth0, lo).
.1.3.6.1.2.1.2.2.1.3	ifType	Тип інтерфейсу (Ethernet, Loopback, etc.).
.1.3.6.1.2.1.2.2.1.4	ifMTU	Розмір MTU інтерфейсу.
.1.3.6.1.2.1.2.2.1.5	ifSpeed	Швидкість інтерфейсу (в бітах/сек).
.1.3.6.1.2.1.2.2.1.6	ifPhysAddress	MAC-адреса інтерфейсу.
.1.3.6.1.2.1.2.2.1.7	ifAdminStatus	Адміністративний статус (включений/виключений).
.1.3.6.1.2.1.2.2.1.8	ifOperStatus	Оперативний статус (активний/неактивний).
.1.3.6.1.2.1.2.2.1.9	ifLastChange	Час останньої зміни стану інтерфейсу.
.1.3.6.1.2.1.2.2.1.10	ifInOctets	Прийняті байти на інтерфейсі.
.1.3.6.1.2.1.2.2.1.11	ifInUcastPkts	Кількість прийнятих одноадресних пакетів.
.1.3.6.1.2.1.2.2.1.12	ifInNUcastPkts	Кількість прийнятих багатоадресних або ширококомовних пакетів.
.1.3.6.1.2.1.2.2.1.13	ifInDiscards	Кількість відкинутих вхідних пакетів.
.1.3.6.1.2.1.2.2.1.14	ifInErrors	Кількість помилок у вхідних пакетах.
.1.3.6.1.2.1.2.2.1.15	ifInUnknownProtos	Кількість пакетів із невідомими протоколами.
.1.3.6.1.2.1.2.2.1.16	ifOutOctets	Передані байти на інтерфейсі.
.1.3.6.1.2.1.2.2.1.17	ifOutUcastPkts	Кількість переданих одноадресних пакетів.
.1.3.6.1.2.1.2.2.1.18	ifOutNUcastPkts	Кількість переданих багатоадресних або ширококомовних пакетів.
.1.3.6.1.2.1.2.2.1.19	ifOutDiscards	Кількість відкинутих вихідних пакетів.
.1.3.6.1.2.1.2.2.1.20	ifOutErrors	Кількість помилок у вихідних пакетах.
.1.3.6.1.2.1.2.2.1.21	ifOutQLen	Довжина черги вихідних пакетів (у пакетах).
.1.3.6.1.2.1.31.1.1.1.1	ifName	Повна назва інтерфейсу (часто більш детальна, ніж ifDescr).
.1.3.6.1.2.1.31.1.1.1.15	ifHighSpeed	Швидкість інтерфейсу у Мбіт/сек (підтримує великі значення).
.1.3.6.1.2.1.31.1.1.1.18	ifAlias	Опис інтерфейсу (може бути визначений адміністратором).
.1.3.6.1.2.1.31.1.1.1.6	ifHCInOctets	Прийняті байти (64-бітовий лічильник для великих значень).
.1.3.6.1.2.1.31.1.1.1.10	ifHCOctets	Передані байти (64-бітовий лічильник для великих значень).

#### Корисні посилання

- How To Install and Configure an SNMP Daemon and Client on Ubuntu.

<http://surl.li/uejoxx>

- Linux snmpwalk: An Overview of SNMP and the snmpwalk Utility.

<http://surl.li/hobszl>

- Nagios. SNMP Monitoring.

<http://surl.li/ypfjoe>