Лабораторна робота №14

Налаштування SNMP-моніторингу у Nagios.

Мета: набути практичних навичок з налаштування системи моніторингу Nagios Core для збору даних через протокол SNMP у віртуалізованому середовищі.

Інструменти: гіпервізор VirtualBox, модель комп'ютерної мережі.

Теоретичні відомості

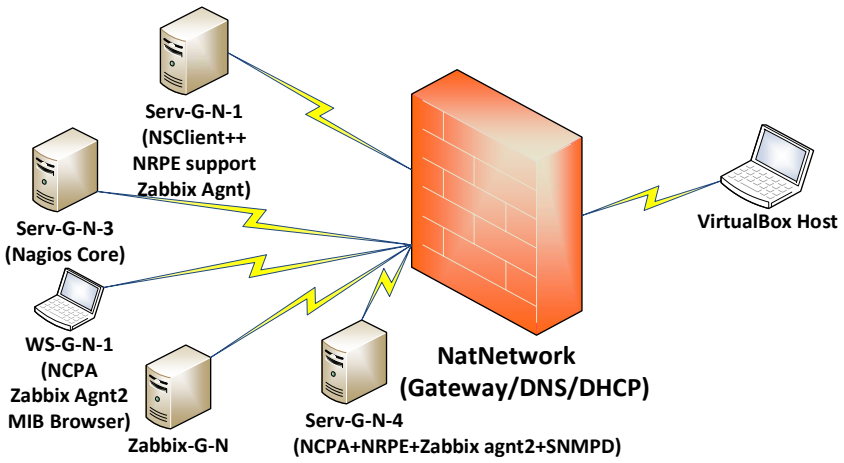

Рис. 14.1. Топологія мережі

На рис. 14.1 наведена модель комп'ютерної мережі, побудована під час виконання попередніх лабораторних робіт. На сервері Serv-G-N-3 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-4. На хості Serv-G-N-4 налаштований сервіс SNMP-серверу.

Інструменти Nagios Core для SNMP-моніторингу.

Nagios Core підтримує моніторинг через SNMP (Simple Network Management Protocol) завдяки використанню спеціальних плагінів. Основні інструменти, які можна використовувати для цього:

- SNMP Plugins (check_snmp) - стандартний плагін check_snmp, який дозволяє виконувати SNMP-запити. Плагін використовується для перевірки доступності OID (Object Identifier) на пристрої, а також для отримання певних метрик (наприклад, завантаженість CPU, використання пам'яті, кількість мережевих підключень тощо).
- Custom SNMP Checks. Використання MIB-файлів (Management Information Base) для читання метрик із пристрою у більш зручному вигляді (наприклад, замість числових OID — зрозумілі назви). Налаштування плагінів для специфічних метрик, які повертаються SNMP-агентом на запит Nagios.
- SNMP Trap Integration. Хоча SNMP Trap є пасивним методом моніторингу, він може використовуватися для отримання повідомлень від пристроїв про критичні події. Для цього потрібно налаштувати демона snmptt (SNMP Trap Translator), який перетворює SNMP Trap у читабельні записи для Nagios.
- Перевірка через сторонні плагіни. Використання плагінів із Nagios Exchange або інших ресурсів для специфічних цілей - моніторинг мережевих пристроїв (світчів, маршрутизаторів), або моніторинг серверів за розширеними метриками (температура, апаратні характеристики).
- Перевірка статусу сервісів через SNMP - моніторинг специфічних сервісів або процесів (наприклад, стан сервісів HTTP, FTP, SSH).

Встановлення плагінів Nagios Core та тестування check_snmp.

Починаємо з встановлення залежностей стандартного плагіну check_snmp:

sudo apt install -y libsnmp-dev snmp

Встановимо і налаштуємо для SNMP-моніторингу стандартний плагін check_snmp. Його встановлення для поточної на момент написання версії виконується з вихідного коду через компіляцію його вручну. Це передбачає декілька етапів. Для початку перевіримо чи присутній check_snmp у системі командою

/usr/local/nagios/libexec/check_snmp --help

Якщо плагін відсутній у системі, визначаємо поточну версію пакету плагінів (2.4.11) та лінк для його завантаження на офіційних сайтах:
https://www.nagios.org/downloads/nagios-plugins/ або
https://nagios-plugins.org/downloads/ .

Рис. 14.2. Визначення поточної версії плагінів Nagios Core та лінку для завантаження пакету плагінів.

Переходимо у каталог /tmp , завантажуємо та розпаковуємо архів розповсюдження:

cd /tmp
wget https://nagios-plugins.org/download/nagios-plugins-2.4.11.tar.gz
tar -xzf nagios-plugins-2.4.11.tar.gz

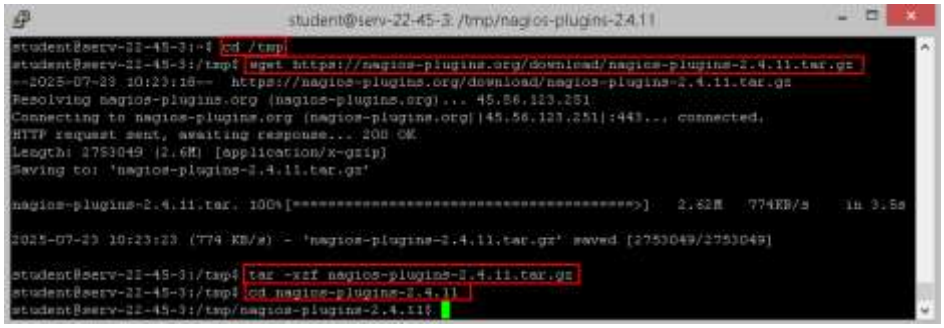

Рис. 14.3. Завантаження та декомпресія пакету плагінів.

Переходимо у каталог із вихідними файлами, готуємо збірку, запускаємо компіляцію та встановлюємо плагіни в системі:

cd nagios-plugins-2.4.11
./configure
make
sudo make install

Після цього всі плагіни з пакету, зокрема check_snmp, будуть встановлені в папку /usr/local/nagios/libexec. Для перевірки роботи плагіну виконуємо команду для перевірки функціональності check_snmp, яка виводить допомогу по використанню плагіну:

/usr/local/nagios/libexec/check_snmp --help

Спробуємо перевірити роботу check_snmp за допомогою тестового SNMP-запиту до Serv-G-N-3:

/usr/local/nagios/libexec/check_snmp -H 192.168.45.132 -C public -o 1.3.6.1.2.1.1.1.0

-H 192.168.45.132 — IP-адреса сервера Serv-22-45-4.
-C public — спільнота SNMP (замініть, якщо виконали інші налаштування).
-o 1.3.6.1.2.1.1.1.0 — OID для отримання опису системи.
Очікуваний результат - відповідь із інформацією про сервер наведений на рис.14.4.

У попередній лабораторній роботі ми дослідили підходи у використанні SNMP-клієнта snmpwalk, що автоматично обробляє усі OID, які є доступними для вказаного кореневого OID. У випадку з check_snmp, необхідно чітко вказати OID до останнього вузла (з індексом). Якщо OID не має індексу або не коректно зазначений, плагін поверне помилку (noSuchName), як на рис.14.4 для складного OID 1.3.6.1.4.1.2021

check_snmp працює як базовий інструмент і, на відміну від snmpwalk, не розуміє складніших запитів, якщо явно не вказано потрібний формат.

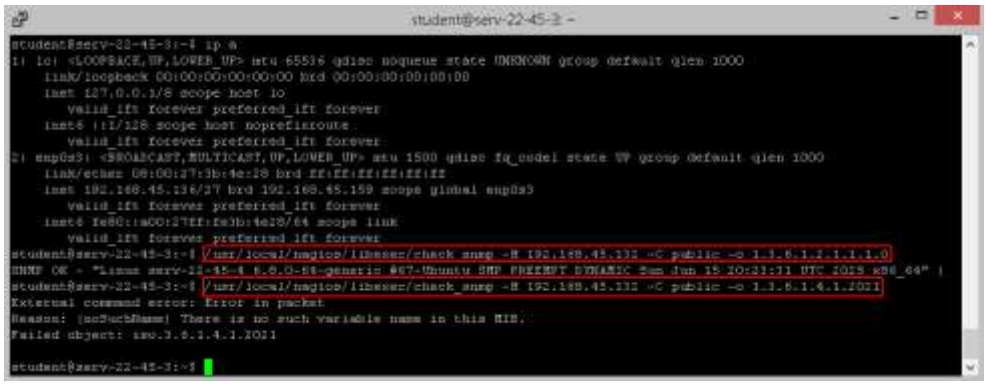

Рис. 14.4. Тестовий запуск плагіну check_snmp на сервері Nagios Core з запитом на сервер Serv-G-N-4

Навіть якщо SNMP-сервер відповідає на snmpwalk, він може повертати відмову (noSuchName) для конкретного OID, якщо дані не доступні для певного OID у запиті безпосередньо, або вказано неправильний контекст (версію, спільноту, хост).

snmpwalk виконує запити до всіх доступних індексів / check_snmp перевіряє лише повні конкретні OID.

Рішення цієї проблеми полягає у попередньому тестуванні OID. Підтвердьте OID із snmpwalk: Виконайте:

snmpwalk -v 2c -c public 192.168.45.132 .1.3.6.1.4.1.2021.9

Переглядаємо отримані у виводі команди OID та впевнюємося, що вони мають індекси (наприклад, .1.3.6.1.4.1.2021.9.1.3.1).

Перевіряємо визначений OID через check_snmp:

/usr/local/nagios/libexec/check_snmp -H 192.168.45.132 -C public -o .1.3.6.1.4.1.2021.9.1.3.1

Для невідомих пристроїв тестування краще виконувати з явним вказуванням версії та параметрів: Виконайте запит із вказаною версією SNMP:

/usr/local/nagios/libexec/check_snmp -H 192.168.45.132 -C public -o .1.3.6.1.4.1.2021.9.1.3.1 -P 2c

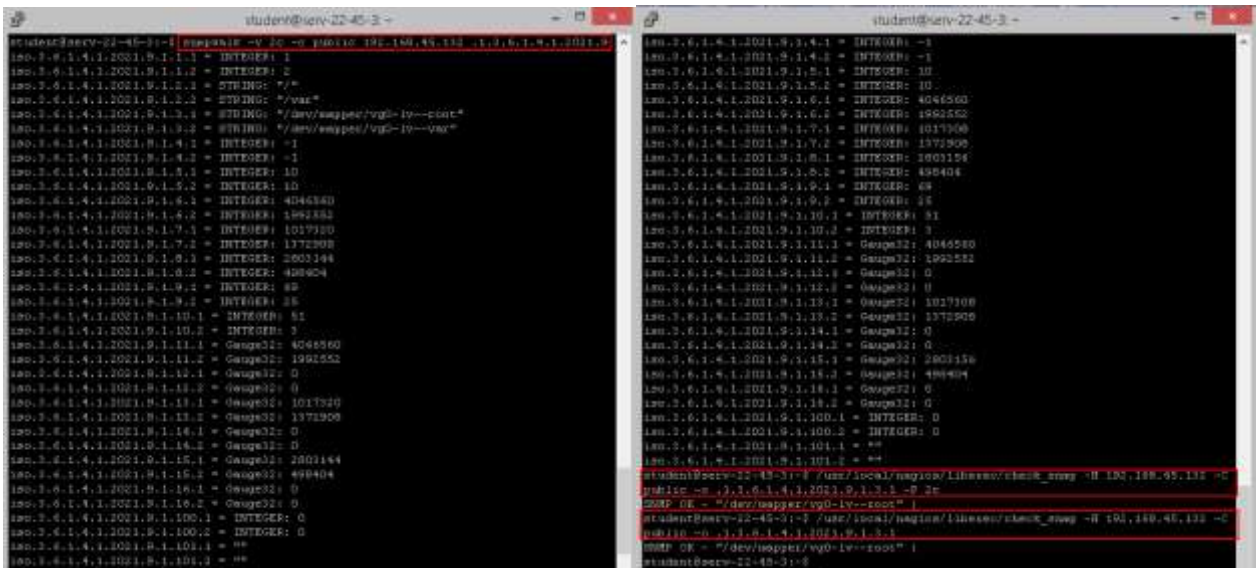

Рис. 14.5. Тестування OID на підтримку check_snmp на сервері Nagios Core Serv-G-N-3

Доцільно розглянути можливість використання таких інструментів, як snmpget та snmptranslate.

snmpget — дозволяє швидко отримати значення конкретного OID без необхідності переглядати великий обсяг даних, як у snmpwalk. Ідеально підходить для точкового тестування OID перед додаванням їх до конфігурації Nagios. Може бути включено як альтернативний інструмент для перевірки роботи SNMP, особливо для OID, що будуть додані до моніторингу.

snmptranslate — дозволяє визначити, що саме означає певний OID, або знайти його описовий текст (наприклад, "System description"). Полегшує роботу з великими деревами OID, роблячи їх зрозумілішими для людей.

snmpget -v 2c -c public 192.168.45.132 1.3.6.1.2.1.2.1.0

snmptranslate 1.3.6.1.2.1.2.1.0

Команда роботи з SNMP-плагіном.

На сервері Nagios Core необхідно визначити, як використовуватиметься плагін check_snmp. Для цього потрібно редагувати запис поточної команди, де використовується тільки $ARG1$, розширивши її для більшої гнучкості. У конфігураційному файлі ***/usr/local/nagios/etc/objects/commands.cfg*** для команди check_snmp.

```
define command{
    command_name    check_snmp
    command_line    $USER1$/check_snmp -H $HOSTADDRESS$ -C $ARG1$ -o $ARG2$ $ARG3$
}
```

$ARG1$ — перший аргумент, який можна використовувати для передачі, наприклад, SNMP community string (-C public).

$ARG2$ — другий аргумент, зазвичай використовується для передачі OID (об'єкта, який моніториться) (-o 1.3.6.1.4.1.2021.9.1.2).

$ARG3$ — третій аргумент, опціональний, для додаткових параметрів, таких як налаштування попереджень чи критичних рівнів (-w <warn> -c <crit>).

Рис. 14.6. commands.cfg – команда check_snmp

Кожна зміна конфігурації системи повинна завершуватися перевіркою вірності внесених у конфігурацію змін та перезапуском сервісу Nagios. Перезапуск лише при відсутності помилок ☺

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

sudo service nagios restart

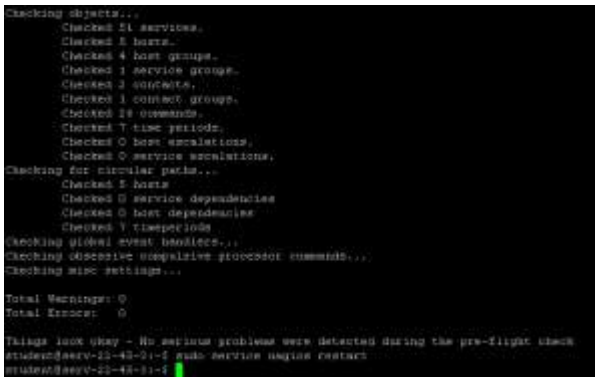

Рис. 14.7. Перевірка відсутності помилок та попереджень у конфігурації Nagios

Рекомендований підхід у роботі з конфігураційними файлами - групування сервісів для одного хосту в одному файлі. Додаємо сервіси файлу конфігурації хосту ***/usr/local/nagios/etc/objects/linux/serv-22-45-4.cfg***

`define service{`
`  use  generic-service`
`  host_name  serv-22-45-4`
`  service_description  SNMP. Eth0. Network Inbound Bytes`
`  check_command  check_snmp!public!1.3.6.1.2.1.2.2.1.10.2`
`}`
	Прийняті байти на інтерфейсі

`define service{`
`  use  generic-service`
`  host_name  serv-22-45-4`
`  service_description  SNMP. Eth0. Network Outbound Bytes`
`  check_command  check_snmp!public!1.3.6.1.2.1.2.2.1.16.2`
`}`
	Передані байти на інтерфейсі

`define service{`
`  use  generic-service`
`  host_name  serv-22-45-4`
`  service_description  SNMP. Eth0. Inbound Packet Errors`
`  check_command  check_snmp!public!1.3.6.1.2.1.2.2.1.14.2`
`}`
	Кількість помилок у вхідних пакетах

`define service{`
`  use  generic-service`
`  host_name  serv-22-45-4`
`  service_description  SNMP. Eth0. Outbound Packet Errors`
`  check_command  check_snmp!public!1.3.6.1.2.1.2.2.1.20.2`
`}`
	Кількість помилок у вихідних пакетах

`define service{`
`  use  generic-service`
`  host_name  serv-22-45-4`
`  service_description  SNMP. CPU Load. 5 min average`
`  check_command  check_snmp!public!1.3.6.1.4.1.2021.10.1.3.2`
`}`
	Завантаження CPU за 5 хвилин

Перевіряємо вірність внесених у конфігурацію змін та перезапускаємо сервіс Nagios. Перезапуск лише при відсутності помилок ☺

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

sudo service nagios restart

Рис. 14.8. Перегляд налаштованих сервісів у GUI Nagios

Завдання до лабораторної роботи

1. Завантажте з офіційних сайтів та встановіть на сервері Nagios Core (Serv-G-N-3) актуальну версію пакету плагінів.
2. Налаштуйте на сервері плагін check_snmp для моніторингу довільного пристрою, відповідно до вимог мережі, з урахуванням SNMP-версії та спільного рядка (community string), щоб забезпечити правильну роботу.
3. Використовуючи команди snmpwalk та check_snmp на сервері Serv-G-N-3, отримайте 5-6 OID з сервера Serv-G-N-4, які відповідають важливим для моніторингу метрикам, таким як використання пам'яті, завантаження процесора, мережевий трафік тощо. Переконайтесь, що ці OID підтримуються плагіном check_snmp. Зверніть увагу, що у майбутніх завданнях будуть використовуватись наступні мережеві OID: прийняті та передані байти на інтерфейсі, кількість помилок у вхідних пакетах та кількість помилок у вихідних пакетах.
4. Додайте моніторинг сервісів, що відповідають визначеним у попередньому завданні OID, до Nagios-конфігурації сервера Serv-G-N-4. Для назви кожного check_snmp сервісу додайте помітку SNMP у конфігурацію.

Звіт має містити:

- лістинг використаних команд;
- короткий опис редагування файлів конфігурації;
- скріншоти налаштувань та підключень;

Додаток 1.

Приклади командних рядків snmpwalk для окремих перевірок.

Таблиця 14.1.

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

Додаток 2.

Основні об'єкти IF-MIB для інтерфейсів.

Таблиця 14.2.

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 широкомовних 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 широкомовних 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	ifHCOutOctets	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
- Using Nagios check_snmp plugin to get snmp info from router.
https://support.nagios.com/forum/viewtopic.php?t=32742
- check_snmp with multi OID and conditional?
https://support.nagios.com/forum/viewtopic.php?t=48862