Лабораторна робота №5

Налаштування пасивного моніторингу Windows хосту на базі Nagios Cross-Platform Agent.

Мета: формування практичних навичок налаштування пасивного моніторингу Windows робочих станцій у системі Nagios 4.x за допомогою агента NCPA (Nagios Cross-Platform Agent), а також організації хостів у тематичні групи для покращення управління та аналізу стану інфраструктури.

Інструменти: гіпервізор VirtualBox, модель комп'ютерної мережі.

Теоретичні відомості

На рис.5.1. наведена модель комп'ютерної мережі, побудована під час виконання попередніх лабораторних робіт. Крім того, до сервера Serv-G-N-2 налаштовано SSH доступ через NAT Network для VirtualBox Host.

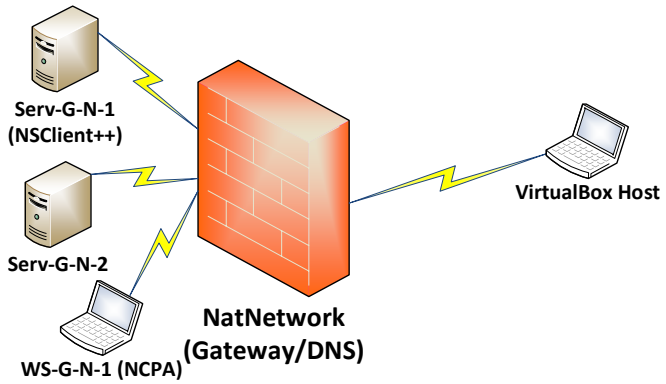
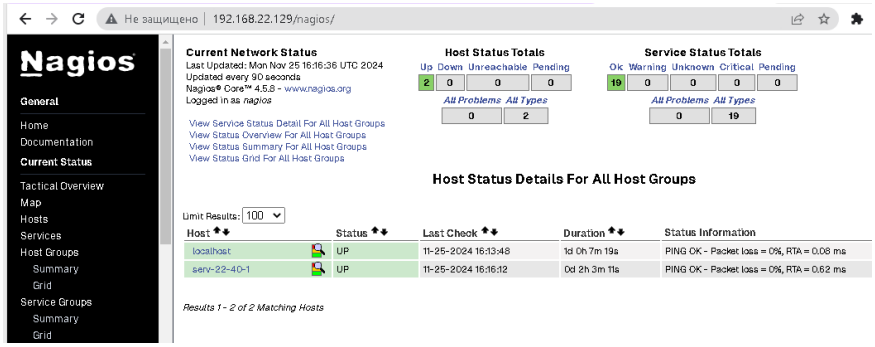


Рис. 5.1. Топологія мережі

На сервері Serv-G-N-2 розгорнуто систему моніторингу на базі Nagios 4.X. Моніторинг основних сервісів серверу Serv-G-N-1 виконується за допомогою NSClient++. Налаштовано підключення з хосту NAT Network по протоколу HTTP до систему моніторингу під користувачем nagios.



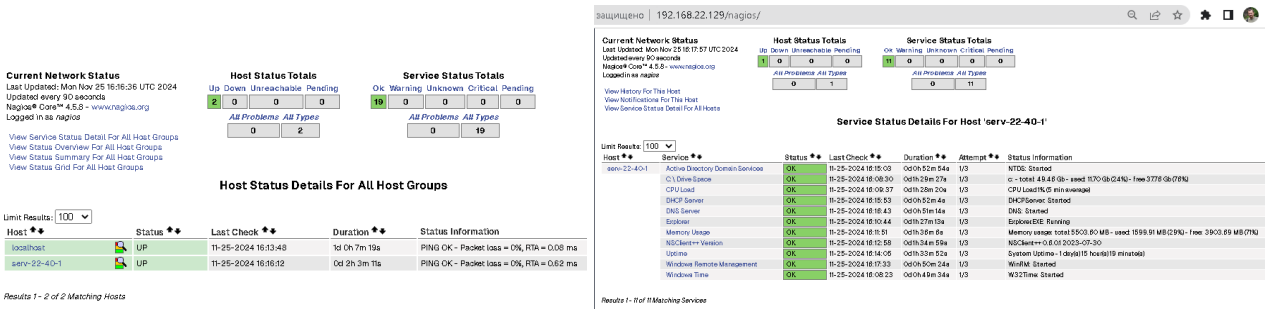


Рис. 5.2. Hosts, Host Groups, Service Status Details for Serv-22-40-1.

Встановимо та налаштуємо NCPA на робочій станції WS-G-N-1. Завантажуємо останню стабільну версію агента для Windows 64-bit з офіційного сайту https://www.nagios.org/ncpa/#downloads . На момент написання цього документу це версія 3.1.1.

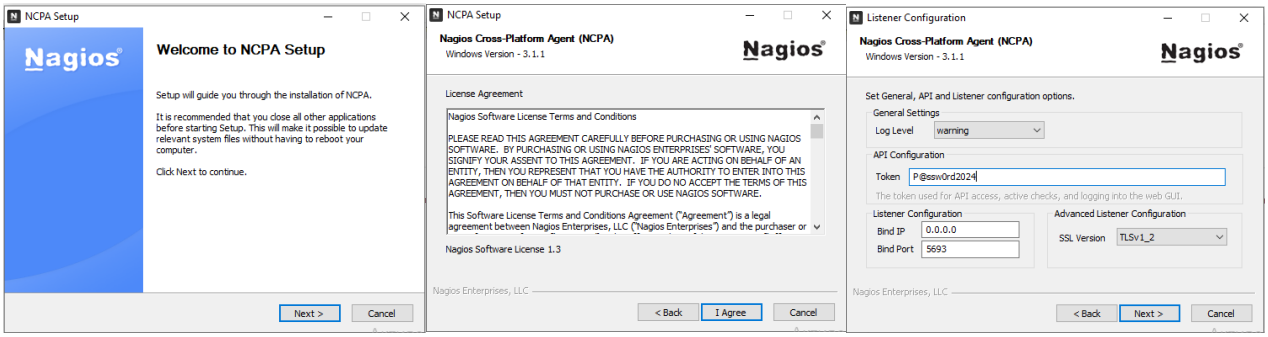


Рис. 5.3. Інсталяція NCPA v.3.1.1 на робочій станції WS-22-40-1.

Запускаємо завантажений файл ncpa-latest.exe та погоджуємося з ліцензійною угодою.

На третьому екрані показані конфігурації для WEB API доступу. Єдине налаштування, яке тут потрібно, це Token – ключ, який сервер Nagios використовуватиме для автентифікації за допомогою NCPA. Я встановив у якості ключа типову послідовність символів P@ssw0rd2024.

IP-адреса прив'язки 0.0.0.0 означає, що NCPA прослуховуватиме всі адреси Ipv4 на машині Windows. Використовується стандартний порт 5693.

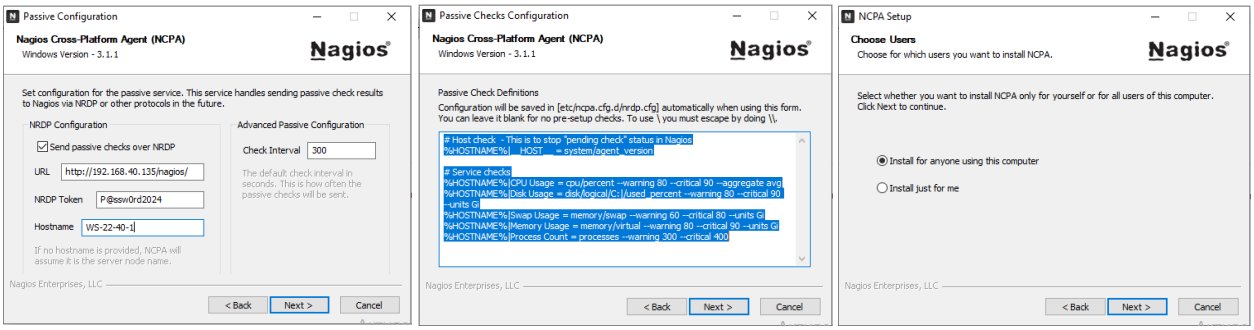


Рис. 5.4. Інсталяція NCPA v.3.1.1 на робочій станції WS-22-40-1.

Екран конфігурації для пасивних перевірок. Встановлюємо прапорець "Send passive checks over NRDP", щоб увімкнути пасивні перевірки та налаштовуємо параметри NRDP:

- **URL**. URL-адреса хосту Nagios, що приймає результати пасивної перевірки. У моєму випадку http://192.168.40.135/nagios/
- **NRDP Token**. Ключ, що використовується під час передачі пасивних перевірок NCPA до Nagios, щоб NRDP прийняв чек. Він може відрізнятися від ключа, що встановлений для API доступу, але враховуючи, що це навчальний стенд, я встановив у якості ключа типову послідовність символів P@ssw0rd2024
- **Hostname**. Ім'я хоста, якому належать пасивні перевірки на сервері Nagios – WS-22-40-1

Продовження інсталяції пасивних перевірок. На екрані запропоновано стандартні пасивні перевірки служб, що будуть виконуватися та надсилатися на сервер Nagios. За потреби їх можна змінити.

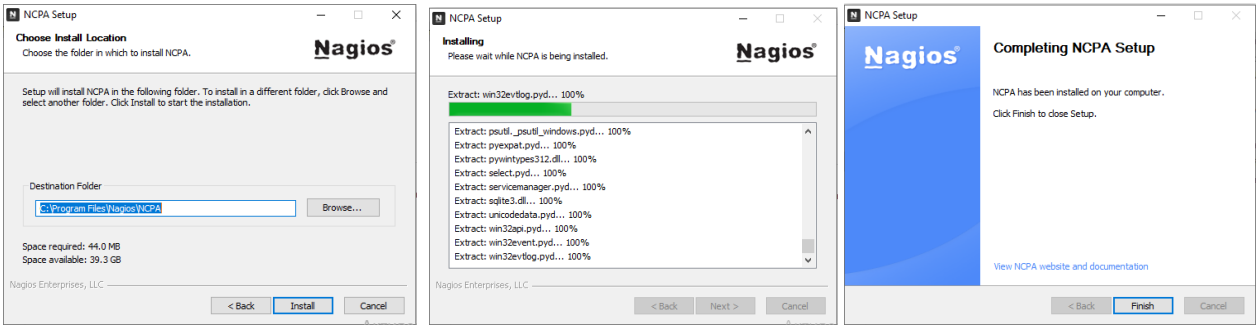


Рис. 5.5. Інсталяція NCPA v.3.1.1 на робочій станції WS-22-40-1.

На наступних кроках можливо змінити місце встановлення агенту NCPA та успішно завершити інсталяцію.

Перевіряємо стан служби Nagios Cross-Platform Agent.

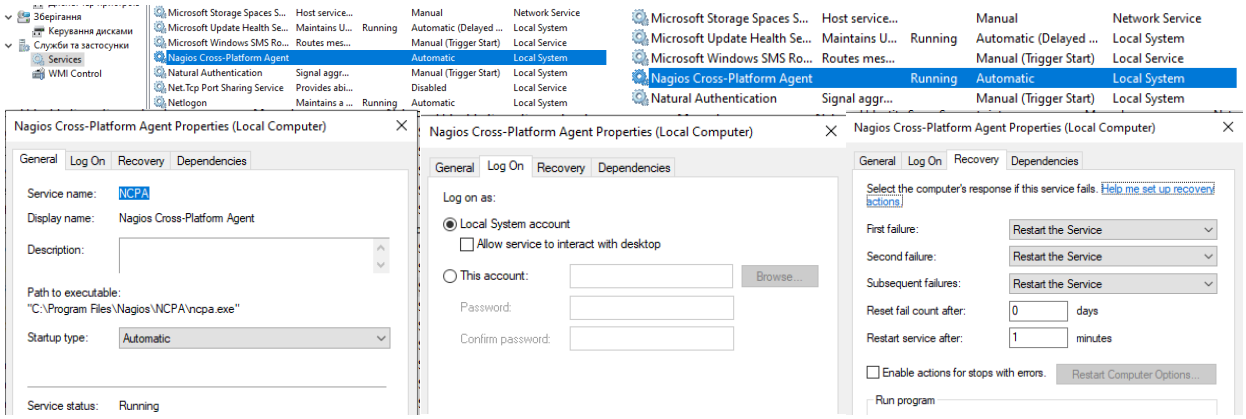


Рис. 5.6. Запуск та налаштування служби NCPA на робочій станції WS-22-40-1.

На рис.5.6 служба NCPA працює, налаштована на автоматичний запуск та змінено дії відновлення служби закладки Recovery на перезапуск сервісу.

Наступний крок перевірки – Windows Defender Firewall. Для роботи NCPA має бути правило, що дозволяє Inbound TCP 5693. Поточна версія NCPA створює ці правила автоматично.

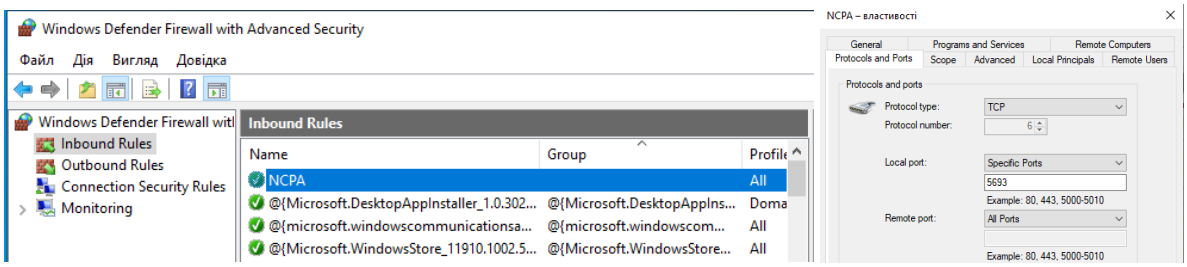


Рис. 5.7. Windows Defender Firewall. Правило NCPA на робочій станції WS-22-40-1.

Остання перевірка – підключаємося до NCPA на станції WS-G-N-1 з серверу Serv-G-N-1. У нашому випадку - https://192.168.40.146:5693.

Можливо підключитися з власного ПК, налаштувавши у NAT Network відповідний Port Forwarding.

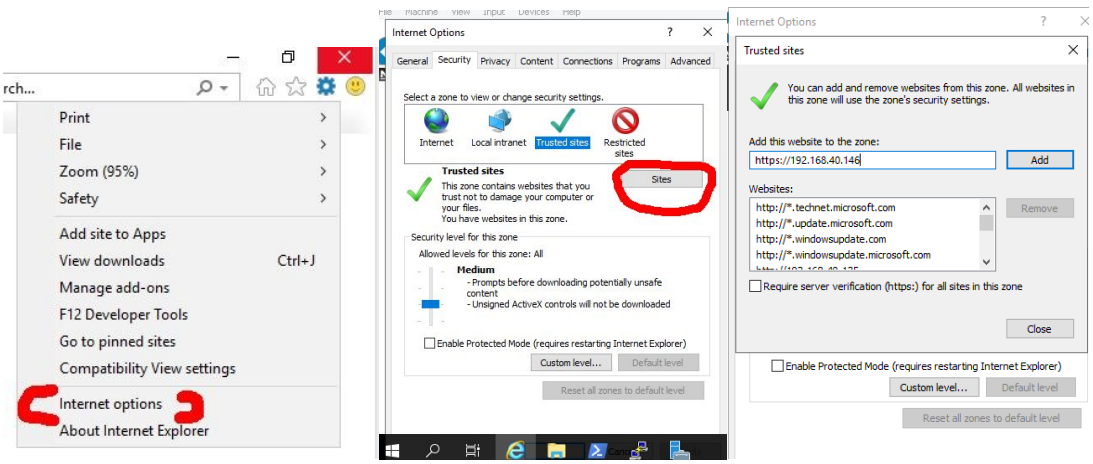


Рис. 5.8. Налаштування дозволу підключення («довіреного» сайту) до http://192.168.40.146 у IE на контролері домену Serv-22-40-1.

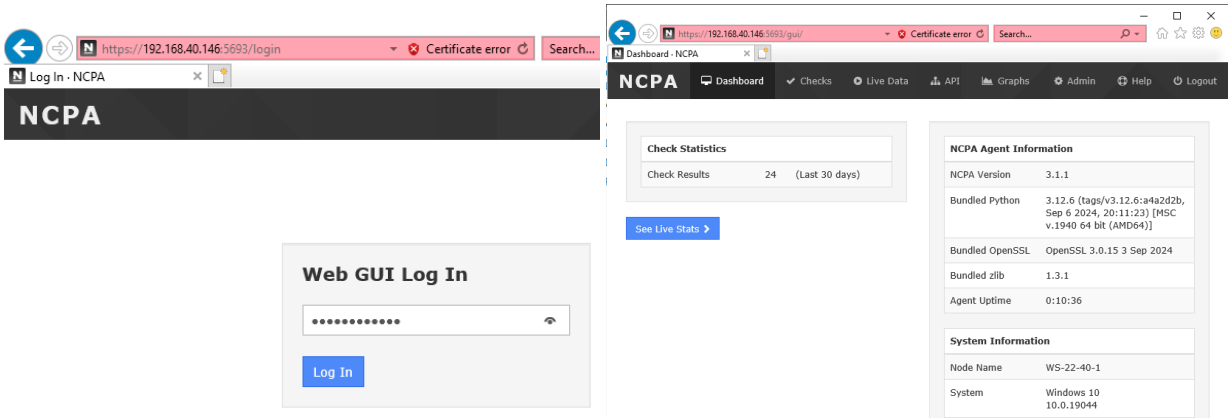


Рис. 5.9. Web GUI NCPA WS-22-40-1. Налаштування дозволу та підключення на Serv-22-40-1.

На рис. 5.8 та 5.9 показані налаштування «довіреного сайту» у браузері серверу та підключення у ньому до Web GUI. У якості ключа доступу вказується заданий при інсталяції ключ для API доступу, вікно Listener Configuration інсталяції NCPA. «Підгледіти» цей пароль можна переглянувши на хості, де проінстальовано NCPA у файлі \etc\ncpa.cfg. Для підключення через WEB використовується значення community_string з секції [api]

Переходимо до конфігурування Nagios для взаємодії з NCPA. По аналогії взаємодії з NSClient++, де використовується команда **check_nt**

/usr/local/nagios/libexec/check_nt -H 192.168.40.131 -p 12489 -s P@ssw0rd2024 -v CPULOAD -l 5,80,90

для взаємодії з NCPA використовується команда **check_ncpa**. Синтаксис дуже схожий:

/usr/local/nagios/libexec/check_ncpa.py -H 192.168.40.146 -p 5693 -t P@ssw0rd2024 -M cpu/percent -w 80 -c 90 -q 'aggregate=avg'

Поточна версія Nagios Core при розгортанні не встановлює цю команду чи її аналоги на сервер.

Налаштовуємо взаємодію з NCPA, як описано у Getting Started

Завантажуємо скрипт активних перевірок check_ncpa.py

cd /usr/local/nagios/libexec

wget https://raw.githubusercontent.com/NagiosEnterprises/ncpa/master/client/check_ncpa.py

Надаємо файлу скрипта відповідні дозволи для виконання:

chmod +x /usr/local/nagios/libexec/check_ncpa.py

```
student@serv-22-40-1:/$
student@serv-22-40-1:/$ cd /usr/local/nagios/libexec
student@serv-22-40-1:/usr/local/nagios/libexec$ sudo wget https://raw.githubusercontent.com/NagiosEnter
prises/ncpa/master/client/check_ncpa.py
--2024-11-26 08:30:28--  https://raw.githubusercontent.com/NagiosEnterprises/ncpa/master/client/check_n
cpa.py
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 185.199.108.133, 185.199.111.133, 18
5.199.110.133, ...
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|185.199.108.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 12200 (12K) [text/plain]
Saving to: 'check_ncpa.py'

check_ncpa.py             100%[=====================================>]  11.91K  --.-KB/s    in 0.001s

2024-11-26 08:30:29 (17.5 MB/s) - 'check_ncpa.py' saved [12200/12200]

student@serv-22-40-1:/usr/local/nagios/libexec$ sudo chmod +x /usr/local/nagios/libexec/check_ncpa.py
student@serv-22-40-1:/usr/local/nagios/libexec$ sudo /usr/local/nagios/libexec/check_ncpa.py
/usr/bin/env: 'python': No such file or directory
student@serv-22-40-1:/usr/local/nagios/libexec$ python3 --version
Python 3.10.12
student@serv-22-40-1:/usr/local/nagios/libexec$
```

Рис. 5.10. Serv-22-40-2. Завантаження, зміна рядка повноважень check_ncpa.py, невдала спроба виконання скрипта і перегляд встановленої версії Phyton.

Помилка при виконанні скрипта ***/usr/local/nagios/libexec/check_ncpa.py***

/usr/bin/env: 'python': No such file or directory

вказує на відсутність інтерпретатора Python. Скрипт використовує Python для виконання, але на Serv-G-N-2 цей інтерпретатор встановлено під назвою python3, про що говорить перевірка версії Phyton.

Редагуємо перший рядок скрипту check_ncpa.py на відповідний інтерпретатор Python, змінюючи рядок **#!/usr/bin/env python** на **#!/usr/bin/env python3**.

```
student@serv-22-40-1:/usr/local/nagios/libexec$ python3 --version
Python 3.10.12
student@serv-22-40-1:/usr/local/nagios/libexec$ sudo vi /usr/local/nagios/libexec/check_ncpa.py
student@serv-22-40-1:/usr/local/nagios/libexec$ /usr/local/nagios/libexec/check_ncpa.py
Usage: check_ncpa.py [options]

Options:
  -h, --help            show this help message and exit
  -H HOSTNAME, --hostname=HOSTNAME
                        The hostname to be connected to.
  -M METRIC, --metric=METRIC
                        The metric to check, this is defined on client system.
                        This would also be the plugin name in the plugins
                        directory. Do not attach arguments to it, use the -a
                        directive for that. DO NOT INCLUDE the api/
                        instruction.
  -P PORT, --port=PORT  Port to use to connect to the client. [Default: 5693]
  -w WARNING, --warning=WARNING
                        Warning value to be passed for the check.
  -c CRITICAL, --critical=CRITICAL
                        Critical value to be passed for the check.
```

Рис. 5.11. Serv-22-40-2. Редагування назви інтерпретатора Python у скрипті check_ncpa.py.

Створюємо команду check_ncpa у конфігураційному файлі для Nagios Core. Зазвичай це файл **/usr/local/nagios/etc/objects/commands.cfg**

Відкриваємо його для редагування. Файл не порожній – у ньому записано доволі багато команд. Додаємо секцію визначення команди check_ncpa:

```
define command {
    command_name    check_ncpa
    command_line    $USER1$/check_ncpa.py -H $HOSTADDRESS$ $ARG1$
}
```

Наведена секція дозволяє передати більшість аргументів за допомогою $ARG1$, роблячи команду динамічнішою.

```
define command {
    command_name    check_nt
    command_line    $USER1$/check_nt -H $HOSTADDRESS$ -p 12489 -v $ARG1$ $ARG2$
}

define command {
    command_name    check_ncpa
    command_line    $USER1$/check_ncpa.py -H $HOSTADDRESS$ $ARG1$
}

##############################################################################
student@serv-22-40-1:/usr/local/nagios/libexec$ sudo vi /usr/local/nagios/etc/objects/commands.cfg
[sudo] password for student:
student@serv-22-40-1:/usr/local/nagios/libexec$ /usr/local/nagios/libexec/check_ncpa.py -H 192.168.40.146
-p 5693 -t P@ssw0rd2024 -M cpu/percent -w 80 -c 90 -q 'aggregate=avg'
OK: Percent was 11.40 % | 'percent'=11.40%;80;90;
student@serv-22-40-1:/usr/local/nagios/libexec$
```

Рис. 5.12. Додавання секції команди check_ncpa у файл commands.cfg та перевірка взаємодії з NCPA на станції WS-22-40-1

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

Одразу перевіряємо взаємодію з NCPA, що встановлений на робочій станції WS-G-N-1. Команду check_ncpa, що описана раніше, замінюємо на ім’я встановленого скрипта check_ncpa.py:

/usr/local/nagios/libexec/check_ncpa.py -H 192.168.22.146 -p 5693 -t P@ssw0rd2024 -M cpu/percent -w 80 -c 90 -q 'aggregate=avg'

Редагуємо конфігураційний файл ***/usr/local/nagios/etc/objects/hostgroups.cfg***, де описана група серверів Windows Servers. Додаємо ще одну групу об’єктів моніторингу – робочих станцій Windows, куди включимо робочу станцію WS-G-N-1.

```
define hostgroup {
    hostgroup_name  win-workstations
    alias           Windows WorkStations
}
```

У каталозі /usr/local/nagios/etc/objects/workstation створюємо конфігураційний файл для робочої станції **/usr/local/nagios/etc/objects/workstation/ws-22-40-1.cfg**

```
define host {
    host_name               WS-22-40-1
    address                 192.168.40.146
    hostgroups              win-workstations
    check_command           check_ncpa!-t 'P@ssw0rd2024' -P 5693 -M system/agent_version
    max_check_attempts      5
    check_interval          5
    retry_interval          1
    check_period            24x7
    notification_interval   60
    notification_period     24x7
    notifications_enabled   1
}
define service {
    host_name               WS-22-40-1
    service_description     CPU Usage
    check_command                   check_ncpa!-t 'P@ssw0rd2024' -P 5693 -M cpu/percent -w 20 -c 40 -q
'aggregate=avg'
    max_check_attempts      5
    check_interval          5
    retry_interval          1
    check_period            24x7
    notification_interval   60
    notification_period     24x7
}
define service {
    host_name               WS-22-40-1
    service_description     Memory Usage
    check_command           check_ncpa!-t 'P@ssw0rd2024' -P 5693 -M memory/virtual -w 50 -c 80 -u G
    max_check_attempts      5
    check_interval          5
    retry_interval          1
    check_period            24x7
    notification_interval   60
    notification_period     24x7
}
define service {
    host_name               WS-22-40-1
    service_description     Process Count
    check_command           check_ncpa!-t 'P@ssw0rd2024' -P 5693 -M processes -w 150 -c 200
    max_check_attempts      5
    check_interval          5
    retry_interval          1
    check_period            24x7
    notification_interval   60
    notification_period     24x7
}
```

Це типовий конфігураційний файл для NCPA моніторингу Windows станції – приклад з комплекту поставки NCPA. Щоб переглянути всі доступні параметри моніторингу для цієї станції з консолі серверу моніторингу, використовується команда:

/usr/local/nagios/libexec/check_ncpa.py -H 192.168.40.146 -t P@ssw0rd2024 -p 5693 --list

Також можливий перегляд налаштованих параметрів моніторингу через GUI при підключенні до NCPA на станції WS-G-N-1 з серверу Serv-G-N-1.

На рис.5.13 показаний вигляд закладки Checks при підключенні до NCPA робочої станції.

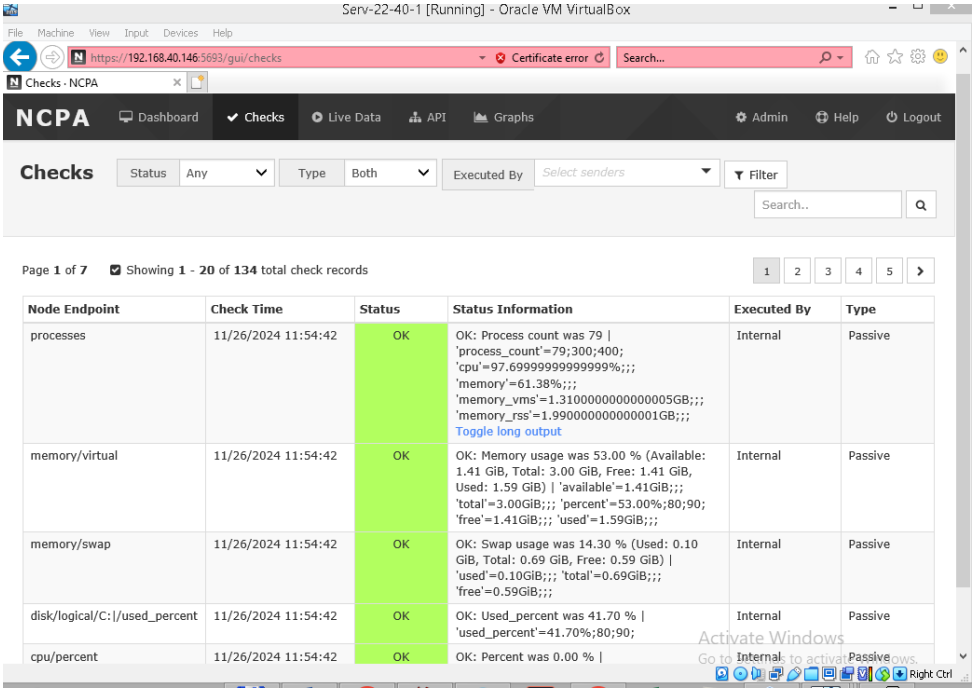


Рис. 5.13. Перегляд параметрів моніторингу робочої станції WS-22-40-1 через https://192.168.40.146:5693

На підставі отриманого переліку команд ми можемо обрати необхідні параметри для відображення у системі моніторингу. Виконаємо команду отримання інформації про вільне місце на логічному диску C:

/usr/local/nagios/libexec/check_ncpa.py -H 192.168.40.146 -t P@ssw0rd2024 -p 5693 -M 'disk/logical/C:|/free' -w 15: -c 10: -u Gi

-w: встановлює поріг для попередження (warning). Якщо виміряне значення метрики перевищує цей поріг, перевірка видасть статус попередження.

-c: встановлює критичний поріг. Якщо виміряне значення метрики перевищує цей поріг, перевірка видасть статус критичної помилки.

-u: вказує одиниці вимірювання для порогів, заданих ключами -w та -c. G вказує гігабайти.

Довідково, для тренування ☺, тип файлової системи диска C:

/usr/local/nagios/libexec/check_ncpa.py -H 192.168.40.146 -t P@ssw0rd2024 -p 5693 -M 'disk/logical/C:|/fstype'

Або, характеристики мережевого інтерфейсу – відправлені пакети:

/usr/local/nagios/libexec/check_ncpa.py -H 192.168.40.146 -t P@ssw0rd2024 -p 5693 -M 'interface/Ethernet/packets_sent'

та отримані пакети:

/usr/local/nagios/libexec/check_ncpa.py -H 192.168.40.146 -t P@ssw0rd2024 -p 5693 -M 'interface/Ethernet/packets_recv'

Час роботи системи:

/usr/local/nagios/libexec/check_ncpa.py -H 192.168.40.146 -t P@ssw0rd2024 -p 5693 -M 'system/uptime'

Доповнимо конфігураційний файл **/usr/local/nagios/etc/objects/workstation/ws-22-40-1.cfg** секціями описаних параметрів.

```
define service {
    host_name               WS-22-40-1
    service_description     Free space on disk C
    check_command           check_ncpa!-t 'P@ssw0rd2024' -P 5693 -M 'disk/logical/C:|/free' -w 15: -c 10: -u Gi
    max_check_attempts      5
    check_interval          5
    retry_interval          1
    check_period            24x7
    notification_interval   60
    notification_period     24x7
```

```
}
define service {
    host_name               WS-22-40-1
   service_description      PhysicalDrive. Read bytes
   check_command            check_ncpa!-t 'P@ssw0rd2024' -P 5693 -M 'disk/physical/PhysicalDrive0/read_bytes' -d -u M -w 50 -c
100
    max_check_attempts      5
    check_interval          5
    retry_interval          1
    check_period            24x7
    notification_interval   60
    notification_period     24x7
}
define service {
    host_name               WS-22-40-1
   service_description      PhysicalDrive. Write bytes
   check_command            check_ncpa!-t 'P@ssw0rd2024' -P 5693 -M 'disk/physical/PhysicalDrive0/write_bytes' -d -u M -w 50 -c
100
    max_check_attempts      5
    check_interval          5
    retry_interval          1
    check_period            24x7
    notification_interval   60
    notification_period     24x7
}
define service {
    host_name               WS-22-40-1
   service_description      PhysicalDrive. Read time
   check_command            check_ncpa!-t 'P@ssw0rd2024' -P 5693 -M 'disk/physical/PhysicalDrive0/read_time' -d -w 50 -c 100
    max_check_attempts      5
    check_interval          5
    retry_interval          1
    check_period            24x7
    notification_interval   60
    notification_period     24x7
}
define service {
    host_name               WS-22-40-1
   service_description      PhysicalDrive. Write time
   check_command            check_ncpa!-t 'P@ssw0rd2024' -P 5693 -M 'disk/physical/PhysicalDrive0/write_time' -d -w 50 -c 100
    max_check_attempts      5
    check_interval          5
    retry_interval          1
    check_period            24x7
    notification_interval   60
    notification_period     24x7
}
define service {
    host_name               WS-22-40-1
   service_description      Ethernet. Sent bytes
   check_command            check_ncpa!-t 'P@ssw0rd2024' -P 5693 -M 'interface/Ethernet/bytes_sent' -d -u k -w 10 -c 100
    max_check_attempts      5
    check_interval          5
    retry_interval          1
    check_period            24x7
    notification_interval   60
    notification_period     24x7
}
define service {
    host_name               WS-22-40-1
   service_description      Ethernet. Received bytes
   check_command            check_ncpa!-t 'P@ssw0rd2024' -P 5693 -M 'interface/Ethernet/bytes_recv' -d -u k -w 10 -c 100
    max_check_attempts      5
    check_interval          5
    retry_interval          1
    check_period            24x7
    notification_interval   60
    notification_period     24x7
}
```

Перевірка вірності внесених у конфігурацію змін та перезапуск сервісу Nagios:

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

sudo service nagios restart

Робоча станція WS-G-N-1 працює на динамічній адресації – її IP-адреса змінна у відповідному діапазоні DHCP-серверу. При налаштуванні адресації Nagios-серверу ми налаштували його адресацію з доступом до нашого DNS, тому змінюємо статичну адресацію робочої станції WS-G-N-1 на її ім'я у домені.

Виконаємо перевірку як працює команда **check_ncpa** з доменним ім'ям (-H ws-G-N-1.surname.net):

/usr/local/nagios/libexec/check_ncpa.py -H ws-G-N-1.surname.net -p 5693 -t P@ssw0rd2024 -M cpu/percent -w 80 -c 90 -q 'aggregate=avg'

```
student@serv-22-40-1:/usr/local/nagios/libexec$ ping falkovsky.net
PING falkovsky.net (192.168.40.131) 56(84) bytes of data.
64 bytes from serv-22-40-1 (192.168.40.131): icmp_seq=1 ttl=128 time=0.607 ms
64 bytes from serv-22-40-1 (192.168.40.131): icmp_seq=2 ttl=128 time=0.470 ms
64 bytes from serv-22-40-1 (192.168.40.131): icmp_seq=3 ttl=128 time=0.539 ms
^C
--- falkovsky.net ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2047ms
rtt min/avg/max/mdev = 0.470/0.538/0.607/0.055 ms
student@serv-22-40-1:/usr/local/nagios/libexec$ /usr/local/nagios/libexec/check_ncpa.py -H ws-22-40-1.falkovsky.net
 -p 5693 -t P@sswOrd2024 -M cpu/percent -w 80 -c 90 -q 'aggregate=avg'
OK: Percent was 58.80 % | 'percent'=58.80%;80;90;
student@serv-22-40-1:/usr/local/nagios/libexec$
```

Рис. 5.14. check-ncpa по доменному імені робочої станції ws-22-40-1.falkovsky.net

Редагуємо адресу (значення параметру address) у секції визначення робочої станції відповідного конфігураційного файлу робочої станції **/usr/local/nagios/etc/objects/workstation/ws-22-40-1.cfg:**

```
define host {
    host_name               WS-22-40-1
   address                  ws-22-40-1.falkovsky.net
   hostgroups               win-workstations
    check_command           check_ncpa!-t 'P@ssw0rd2023' -P 5693 -M system/agent_version
    max_check_attempts      5
    check_interval          5
    retry_interval          1
    check_period            24x7
    notification_interval   60
    notification_period     24x7
    notifications_enabled   1
}
```

Перевірка вірності внесених у конфігурацію змін та перезапуск сервісу Nagios:

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

sudo service nagios restart

Переглядаємо зміни у відображенні груп хостів, хостів та їх сервісів після виконаних налаштувань.

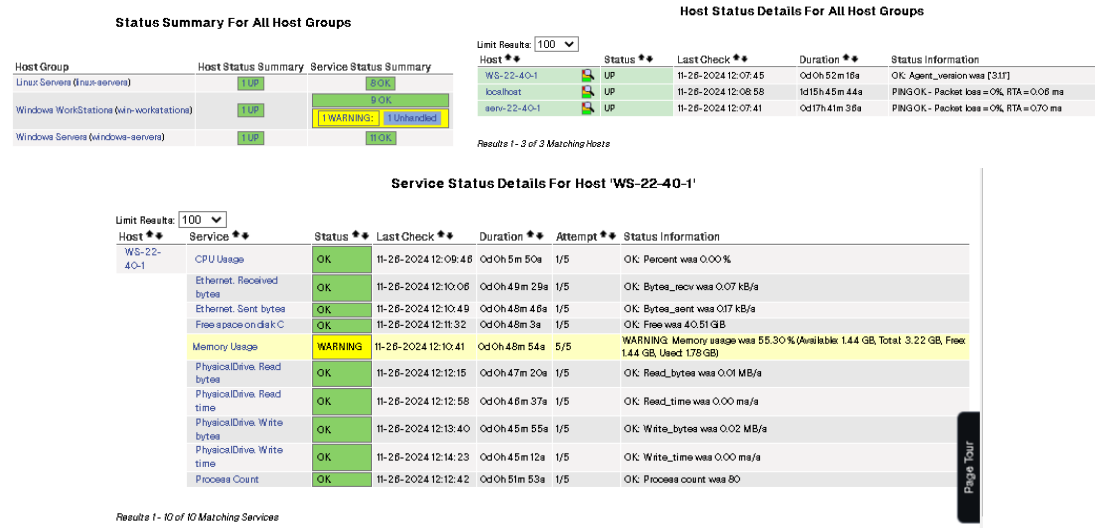


Рис. 5.15. Перегляд виконаних налаштувань:
Host Group Summary, Host Status, Service Status Details for host WS-22-1-1

Зверніть увагу на «жовтий» статус використання пам'яті на робочій станції WS-22-40-1 (рис.5.15.).

Завдання до лабораторної роботи

1. Встановіть та налаштуйте на робочій станції WS-G-N-1 актуальну версію агента моніторингу NCPA. У звіті обов'язково наведіть скрін закладки checks HTTP-підключення до NCPA WS-G-N-1.
2. Налаштуйте моніторинг основних сервісів (мінімум 10) робочої станції WS-G-N-1. У звіті обов'язково наведіть скріни закладок Hosts та View Service Details for WS-G-N-1.
3. Відредагуйте конфігурацію Nagios таким чином, щоб у системі було три активних групи хостів: Windows Servers, Windows Workstations та Linux Servers. Закладка Host Groups Nagios.

Звіт має містити:

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

Корисні посилання

- Nagios Add-Ons Projects
https://www.nagios.org/downloads/nagios-core-addons/

- NCPA. Downloads latest stable agent
https://www.nagios.org/ncpa/#downloads

- Installing NCPA
https://nagiosenterprises.my.site.com/support/s/article/Installing-NCPA-9f1de62f#Installing_NCPA_On_Windows

- NCPA. Getting Started
https://www.nagios.org/ncpa/getting-started.php

- Download check_ncpa.py
https://raw.githubusercontent.com/NagiosEnterprises/ncpa/master/client/check_ncpa.py

- Nagios Plugins Downloads
https://nagios-plugins.org/downloads/

- GitHub. NagiosEnterprises/ncpa
https://github.com/NagiosEnterprises/ncpa

- GitHub. NagiosEnterprises/ncpa/"free disk space"
https://github.com/NagiosEnterprises/ncpa/issues/857

- Nagios Support Knowledgebase. Network Interface Checks
https://support.nagios.com/kb/article/network-interface-checks-781.html