Лабораторна робота №3

Nagios 4.X. Налаштування пасивного моніторингу Windows сервера на базі NSClient++.

Мета: формування навичок налаштування пасивного моніторингу серверів Windows у системі Nagios 4.x за допомогою агента NSClient++, а також конфігурації груп хостів для впорядкування моніторингу в багатосерверному середовищі.

Інструменти: гіпервізор VirtualBox, модель комп'ютерної мережі.

Теоретичні відомості

На рис.3.1. 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.

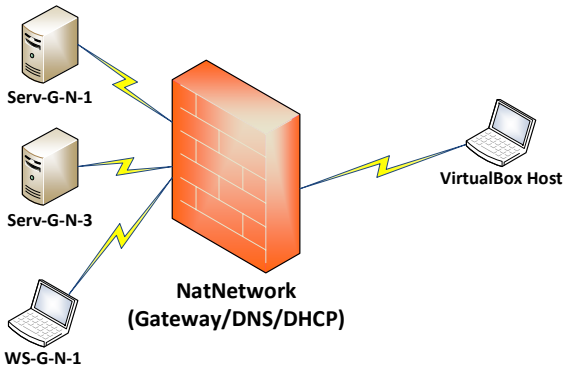

Рис. 3.1. Топологія мережі

На сервері Serv-G-N-3 розгорнуто систему моніторингу на базі Nagios 4.X. Ми підключилися з робочої станції WS-G-N-1 до системи моніторингу по протоколу HTTP під користувачем Nagios.

Налаштуємо HTTP доступ через NAT Network для VirtualBox Host.

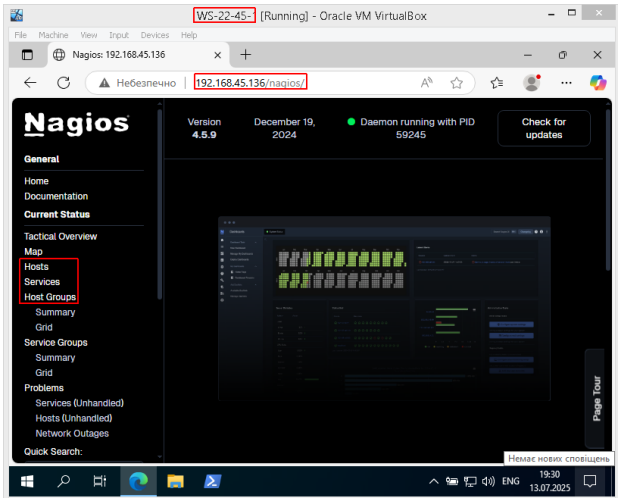

Рис. 3.2. Підключення до Nagios з робочої станції WS-22-45-1.

У більшості випадків пошук адреси для підключення та перевірка «вільних» портів виконується за алгоритмом, що ми використали у одній з попередніх робіт. На VirtualBox Host виконуємо:

ipconfig /all | Select-String -Context 0,10 "VirtualBox Host-Only Ethernet Adapter"
netstat -an | findstr "Знайдена IP-адреса"

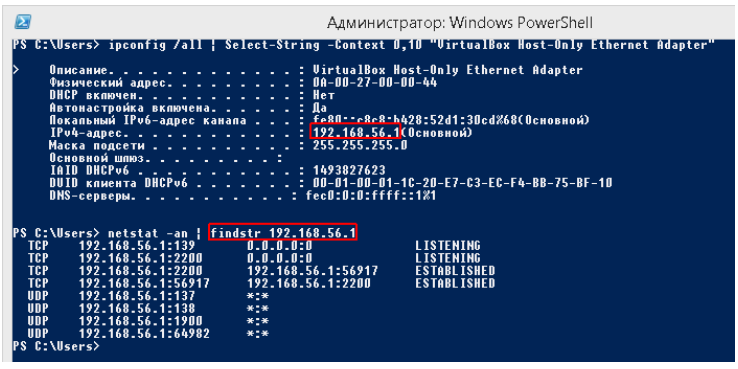

Рис. 3.3. Визначення на хосту VirtualBox Host IP та «вільних» портів

Адреса 192.168.56.1 VirtualBox Host не використовує порт 80. Це спрощує задачу і для підключення через NAT Network до системи моніторингу використовуємо той же 80 порт. На рис. 3.4 показане таке налаштування NAT Network та підключення до серверу Serv-G-N-3 по HTTP (80 порт) до системи моніторингу Nagios. Раніше ми вже налаштували SSH-підключення (22 порт).

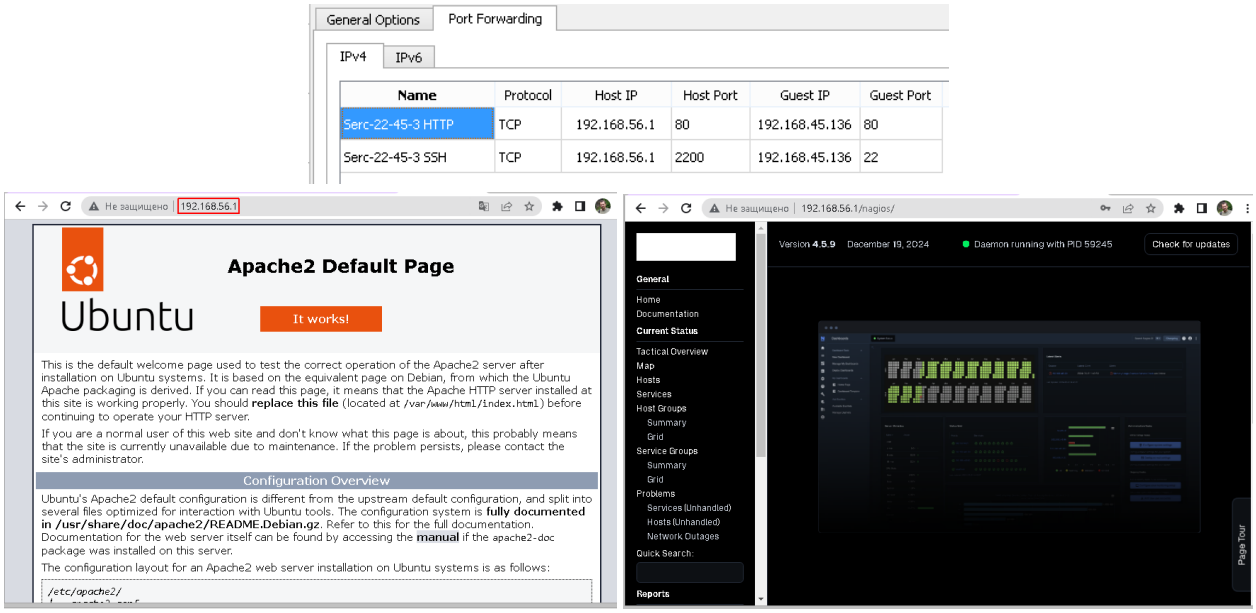

Рис. 3.4. NAT Network. HTTP port forwarding settings та підключення з VirtualBox Host по HTTP

Системи моніторингу, які вимагають встановлення клієнтського програмного забезпечення на хості для ефективного моніторингу, зазвичай використовують агенти. У випадку Nagios є два популярних клієнтських рішення для моніторингу хостів під управлінням ОС Windows:

- **NSClient++**. Агент для моніторингу, який може бути використаний з Nagios. NSClient++ спеціально створений для операційної системи Windows і має підтримку багатьох різних типів моніторингу..
- **NCPA (Nagios Cross-Platform Agent)**. Агент, що може встановлюватися на різних операційних системах, включаючи Windows. Дозволяє надсилати дані про моніторинг Nagios серверу.

Перед розгортанням NSClient++ встановлюємо на сервері Serv-G-N-1 бібліотеки середовища виконання Visual C++ Redistributable з відповідної сторінки. У відповідності до нашої платформи серверу це буде пакет https://aka.ms/vs/17/release/vc_redist.x64.exe. Якщо система безпеки серверу не дозволяє завантажити інсталяційні пакети, завантажте їх на VirtualBox Host та скопіюйте на сервер.

Підключаємо Serv-G-N-1 до системи моніторингу за допомогою агенту NSClient++. На сторінці розповсюдження проекту https://github.com/mickem/nscp/releases актуальна стабільна версія агенту - #0.9.7. Завантажуємо та встановлюємо версію, у відповідності до нашої платформи

https://github.com/mickem/nscp/releases/download/0.9.7/NSCP-0.9.7-x64.msi .

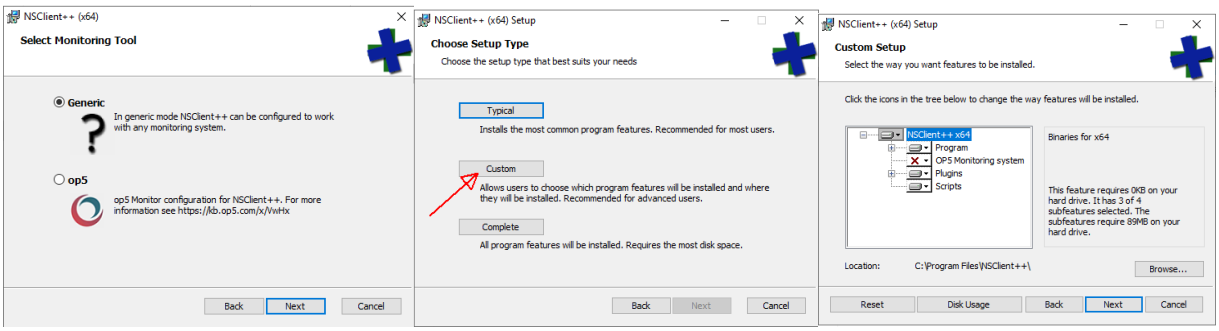

Рис. 3.5. Користувацька, рекомендована інсталяція NSClient++.

Встановлювані елементи залишаємо без змін.

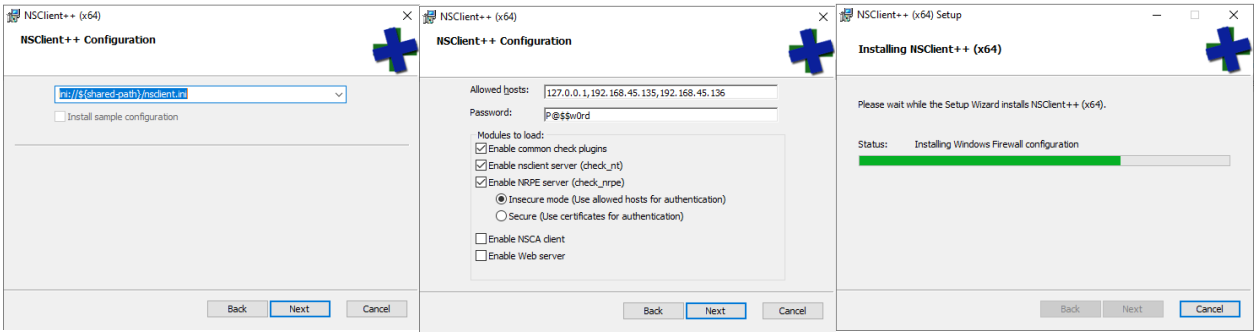

Рис. 3.6. Місце та ім'я файлу ini – без змін. У полі Allowed hosts вказано адреси хостів що будуть отримувати інформацію від клієта (127.0.0.1,192.168.45.135,192.168.45.136). У полі Password вказаний пароль підключення NSClient++. Використовуємо Insecure mode.

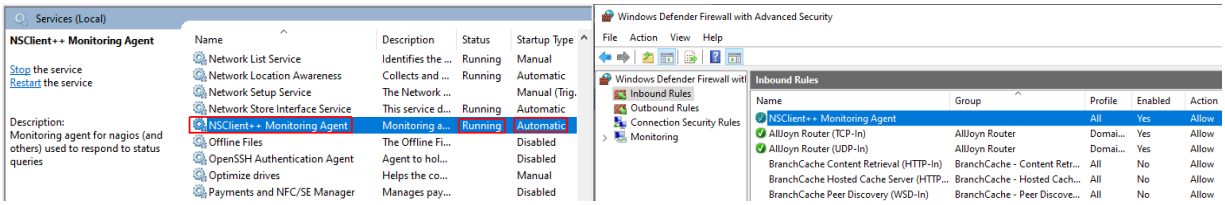

Рис. 3.7. Служба NSClient++ та відповідне правило Windows Firewall.

Поточна версія агента NSClient++ в процесі інсталяції автоматично конфігурує відповідну службу та правило Windows Firewall. Необхідно впевнитись у налаштуваннях конфігурації агента. Відкриваємо для редагування файл C:\Program Files\NSClient++\nsclient.ini , шукаємо у ньому ключі CheckEventLog, CheckDisk, CheckSystem у секції [/modules]. Їх значення повинні бути enabled.

```
[/modules]
CheckEventLog = enabled
CheckDisk = enabled
CheckSystem = enabled
```

За будь яким редагуванням конфігураційного файлу nsclient.ini повинно бути перезавантаження служби NSClient++ Monitoring Agent. Конфігурування агента NSClient++ на стороні Windows сервера Serv-G-N-1 завершено. Перевіримо на стороні сервера моніторингу Serv-G-N-3 чи всі налаштування працюють. Для цього виконаємо у ручному режимі команду перевірки зв'язку:

```
student@serv-22-45-3:/tmp$ /usr/local/nagios/libexec/check_nt -H 192.168.45.135 -p 12489 -s P@sswOrd -v CPULOAD -l 5,80,90
NSClient - ERROR: Invalid password.
student@serv-22-45-3:/tmp$ /usr/local/nagios/libexec/check_nt -H 192.168.45.135 -p 12489 -s P@sswOrd -v CPULOAD -l 5,80,90
CPU Load 0% (5 min average) |   '5 min avg Load'=0%;80;90;0;100
student@serv-22-45-3:/tmp$
```

Рис. 3.8. Перевірка зв'язку між Nagios(Serv-22-45-3) та NSClient++(Serv-22-45-1).

На рис.3.8 показане виконання команд

/usr/local/nagios/libexec/check_nt -H 192.168.45.135 -p 12489 -s P@$$w0rd -v CPULOAD -l 5,80,90
/usr/local/nagios/libexec/check_nt -H 192.168.45.135 -p 12489 -s P@ssw0rd -v CPULOAD -l 5,80,90

У першій команді в паролі доступу використовувались символи $$, які для передачі з сервера на сервер необхідно «екранувати». Для спрощення пароль було змінено у файлі C:\Program Files\NSClient++\nsclient.ini, служба NSClient++ Monitoring Agent перезавантажена після змін.

Команда /usr/local/nagios/libexec/check_nt використовується для моніторингу параметрів на віддалених Windows-серверах за допомогою NSClient++. У даному випадку, ми використовуємо команду для отримання інформації про завантаження ЦП.

-H 192.168.45.135	Вказує IP-адресу або ім'я хоста (hostname) Windows-серверу, що моніториться.
-p 12489	Вказує порт, на якому «слухає» NSClient++. У цьому випадку, 12489 є стандартним портом для взаємодії з NSClient++.
-s P@ssw0rd	Вказує пароль для взаємодії з NSClient++. Цей пароль налаштовується при інсталяції агента на сервері (рис.3.7) та може бути змінений у файлі nsclient.ini, що ми вже редагували.
-v CPULOAD	Вказує параметр, що перевіряється. У цьому випадку, це CPULOAD (завантаження процесора).

-l 5,80,90 Вказує параметри для порівняння зі значенням CPULOAD. Вказано, що буде генеруватися критичний стан, якщо завантаження ЦП перевищує 90% протягом 5 хвилин. Нормальний стан - якщо завантаження ЦП менше 80%.

Результат виглядає так:

CPU Load 0% (5 min average) | '5 min avg Load'=0%;80;90;0;100

показує, що завантаження ЦП за 5 хвилин становить 0%, що знаходиться в межах вказаних порогових значень (80% і 90%). У цей момент моніторингу відсутня проблема з завантаженням ЦП.

Налаштування клієнтської частини моніторингу для Windows сервера завершено.

Переходимо до налаштувань безпосередньо у системі моніторингу. На розгорнутій системі, у каталозі /usr/local/nagios/etc/objects є кілька конфігураційних файлів:

- **commands.cfg**. Відповідає за визначення команд, які використовуються для виконання перевірок. Визначає, як має бути виконана перевірка (наприклад, яку команду виконати на віддаленому сервері).
- **localhost.cfg**. Містить конфігурацію для моніторингу локального хоста (сервера, на якому встановлений Nagios).
- **switch.cfg**. Містить конфігурацію для моніторингу комутаторів (мережевого обладнання).
- **timeperiods.cfg**. Відповідає за визначення періодів часу, коли моніторинг активний або вимкнений.
- **contacts.cfg**. Містить конфігурацію для визначення контактів - осіб, які отримають повідомлення про проблеми.
- **printer.cfg**. Може містити конфігурацію для моніторингу принтерів.
- **templates.cfg**. Визначає шаблони, які можна використовувати для спрощення конфігурації. Шаблони дозволяють вам визначити спільні властивості для груп хостів або сервісів.
- **windows.cfg**. Містить зразок конфігурації для моніторингу Windows-серверів.

Кожен файл виконує конкретну роль у конфігурації Nagios. Вони можуть бути використані окремо або разом для організації конфігурації за різними аспектами системи.

Щодо того, який з них є "шаблоном" і "конфігураційним", це може залежати від самої конфігурації та ваших вимог. Файли templates.cfg зазвичай містять шаблони для використання у конфігурації хостів та сервісів, спрощуючи процес конфігурування для схожих об'єктів моніторингу. Файли, які містять конфігурацію конкретних об'єктів (наприклад, localhost.cfg, switch.cfg, windows.cfg), визначають параметри самого об'єкта моніторингу. Зрозуміло, що найзручнішою та найбільш гнучкою конфігурацією буде та, я якій для кожного об’єкту (хоста, елемента мережевого обладнання, сайту і т.і.) моніторингу створюється свій файл конфігурації, а об’єкти розділені на групи, приналежність до яких визначається певними міркуваннями.

Для нашої моделі комп’ютерної мережі найбільш логічним буде поділ об’єктів на Windows-сервери, Linux-сервери, мережеве обладнання, WEB-сайти. Створюємо відповідні підкаталоги для кожної з перелічених груп об’єктів моніторингу: windows, linux, workstation, network, website.

```
student@serv-22-45-3:/usr/local/nagios/etc/objects$ dir
commands.cfg  contacts.cfg  localhost.cfg  printer.cfg  switch.cfg  templates.cfg  timeperiods.cfg  windows.cfg
student@serv-22-45-3:/usr/local/nagios/etc/objects$ sudo mkdir linux
[sudo] password for student:
student@serv-22-45-3:/usr/local/nagios/etc/objects$ sudo mkdir workstation
student@serv-22-45-3:/usr/local/nagios/etc/objects$ sudo mkdir network
student@serv-22-45-3:/usr/local/nagios/etc/objects$ sudo mkdir website
student@serv-22-45-3:/usr/local/nagios/etc/objects$ dir
commands.cfg  linux          network      switch.cfg     timeperiods.cfg  windows.cfg
contacts.cfg  localhost.cfg  printer.cfg  templates.cfg  website          workstation
student@serv-22-45-3:/usr/local/nagios/etc/objects$
```

Рис. 3.9. Створення каталогів для файлів конфігурації об’єктів моніторингу.

Редагуємо файл конфігурації /usr/local/nagios/etc/nagios.cfg.

Знімаємо коментар для конфігураційного файлу windows.cfg

(*# Definitions for monitoring a Windows machine*)

та додаємо створені каталоги груп об’єктів моніторингу (рис.3.10).

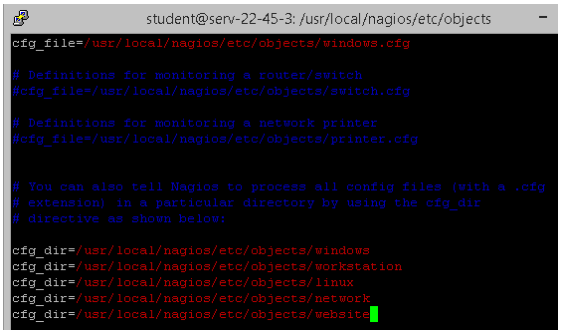

Рис. 3.10. Редагування /usr/local/nagios/etc/nagios.cfg

Створюємо типовий файл конфігурації моніторингу об'єкту типу сервер Windows у відповідному каталозі ***/usr/local/nagios/etc/objects/windows***. Для цього копіюємо зразок конфігураційного файлу:

sudo cp /usr/local/nagios/etc/objects/windows.cfg /usr/local/nagios/etc/objects/windows/serv-22-45-1.cfg

Відкриваємо створений файл ***serv-22-45-1.cfg*** для редагування та вносимо до нього зміни у відповідності до зразка, наведеного у таблиці 3.1.

Таблиця 3.1

Конфігураційний файл	Опис секцій

`define host {`
`  use  windows-server`
`  host_name  serv-22-45-1`
`  alias  Windows Server Falkovsky`
`  address  192.168.45.135`
`}`
	Визначення об'єкту моніторингу: ім'я серверу, аліас, IP адреса.

`# SERVICE DEFINITIONS`
`define service {`
`  use  generic-service`
`  host_name  serv-22-45-1`
`  service_description  NSClient++ Version`
`  check_command  check_nt!CLIENTVERSION -s P@ssw0rd`
`}`
	Визначення сервісів
	Моніторинг сервісу NSClient++
	Зверніть увагу на параметр -s за яким має бути вказаний пароль NSClient++ для цього хоста.

`define service {`
`  use  generic-service`
`  host_name  serv-22-45-1`
`  service_description  Uptime`
`  check_command  check_nt!UPTIME -s P@ssw0rd`
`}`
	Моніторинг часу роботи сервера

`define service {`
`  use  generic-service`
`  host_name  serv-22-45-1`
`  service_description  CPU Load`
`  check_command  check_nt!CPULOAD!-s P@ssw0rd -l 5,80,90`
`}`
	Моніторинг завантаження ЦП
	Зверніть увагу на положення паролю агенту у командному рядку

`define service {`
`  use  generic-service`
`  host_name  serv-22-45-1`
`  service_description  Memory Usage`
`  check_command  check_nt!MEMUSE!-s P@ssw0rd -w 80 -c 90`
`}`
	Моніторинг фізичної пам'яті
	Зверніть увагу на положення паролю агенту у командному рядку

`define service {`
`  use  generic-service`
`  host_name  serv-22-45-1`
`  service_description  C:\ Drive Space`
`  check_command  check_nt!USEDDISKSPACE! -s P@ssw0rd -l c -w 80 -c 90`
`}`
	Моніторинг системного диску
	Зверніть увагу на положення паролю агенту у командному рядку

`define service {`
`  use  generic-service`
`  host_name  serv-22-45-1`
`  service_description  Explorer`
`  check_command  check_nt!PROCSTATE!-d SHOWALL -l Explorer.exe -s P@ssw0rd`
`}`
	Зразок моніторингу процесу на прикладі Explorer.exe

Відкриваємо для редагування файл визначення зразку-шаблону для моніторингу Windows хостів ***/usr/local/nagios/etc/objects/windows.cfg*** та очищаємо його, залишивши єдину секцію визначення групи хостів. Це необхідно зробити для відключення відображення зразка хосту на ім'я ***windows*** у створеній конфігурації:

```
define hostgroup {
    hostgroup_name          windows-servers         ; The name of the hostgroup
    alias                   Windows Servers        ; Long name of the group
}
```

Після завершення редагування будь якого файлу шаблону чи конфігурації обов'язково виконуємо загальну перевірку конфігурації системи:

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

Для введення у дію виконаних змін конфігурації необхідно перезавантажити сервіси Apache та Nagios :

sudo service apache2 restart
sudo service nagios restart

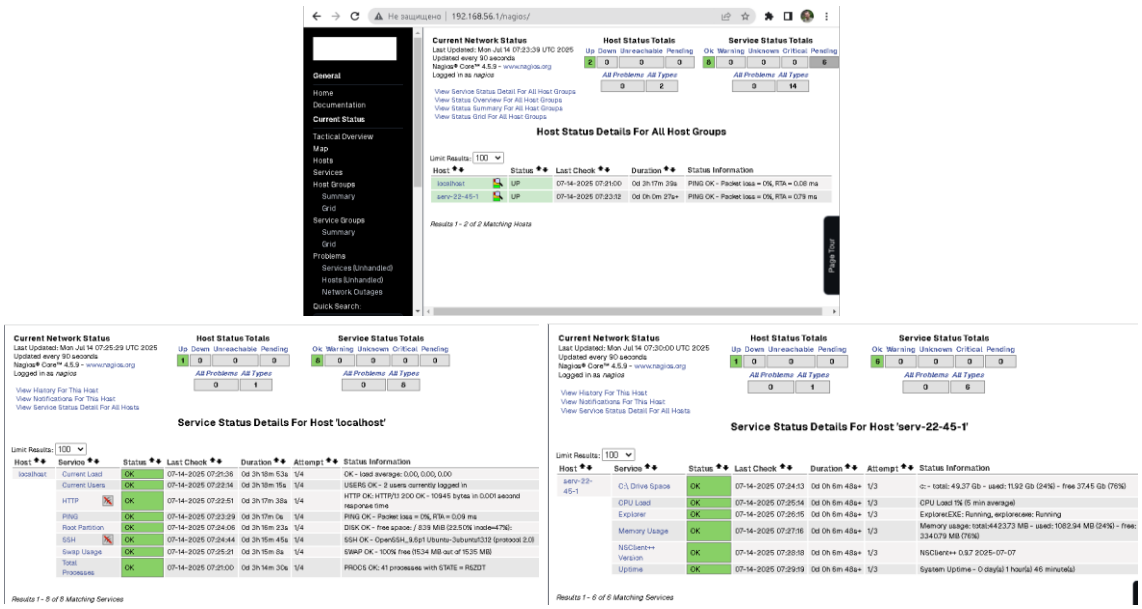

*Рис. 3.11. Перегляд розділу **Hosts** та **View Service Details for** serv-22-45-1*

На рис. 3.11 показаний перегляд отриманої конфігурації – два хости localhost та serv-22-45-1.

Перейменуємо конфігураційний файл ***/usr/local/nagios/etc/objects/windows.cfg*** у файл опису груп хостів ***/usr/local/nagios/etc/objects/hostgroups.cfg***. Шаблоном опису групи Windows Servers у файлі вже існує:

```
define hostgroup {
   hostgroup_name  windows-servers
   alias           Windows Servers
}
```

```
student@serv-22-45-3:/usr/local/nagios/etc/objects$ dir
commands.cfg     linux          printer.cfg     timeperiods.cfg  workstation
contacts.cfg     localhost.cfg  switch.cfg      website
hostgroups.cfg   network        templates.cfg   windows
student@serv-22-45-3:/usr/local/nagios/etc/objects$
```

Рис. 3.12. Створення файлу опису груп хостів /usr/local/nagios/etc/objects/hostgroups.cfg

Відкриваємо для редагування файл /usr/local/nagios/etc/nagios.cfg. Додаємо параметр cfg_file для новоствореної конфігурації hostgroups.cfg та коментуємо ***windows.cfg***:

```
cfg_file=/usr/local/nagios/etc/objects/hostgroups.cfg
# Definitions for monitoring a Windows machine
#cfg_file=/usr/local/nagios/etc/objects/windows.cfg
```

«Звична операція» – 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
```

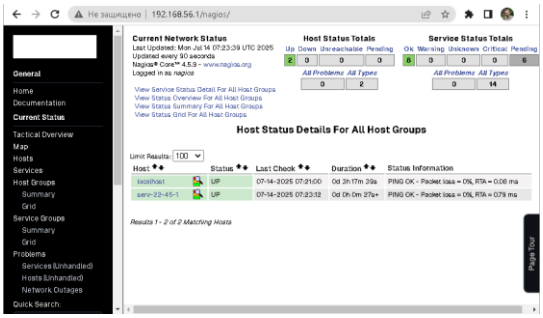

*Рис. 3.13. Перегляд розділу **Hosts** після перебудови конфігурації групи хостів Windows Servers*

Перегляд сервісів для налаштованого Serv-22-45-1 може показати помилки, а саме відсутність моніторингу служби World Wide Web Publishing Service та моніторингу процесу Explorer.exe. Ці сервіси включені з шаблону як зразки.

Щодо служби World Wide Web Publishing Service (IIS), її моніторинг дійсно може бути корисним, але у нашому випадку відповідний стек служб не розгортався. Однак враховуйте специфіку вашого середовища та потреб вашої організації при виборі служб для моніторингу.

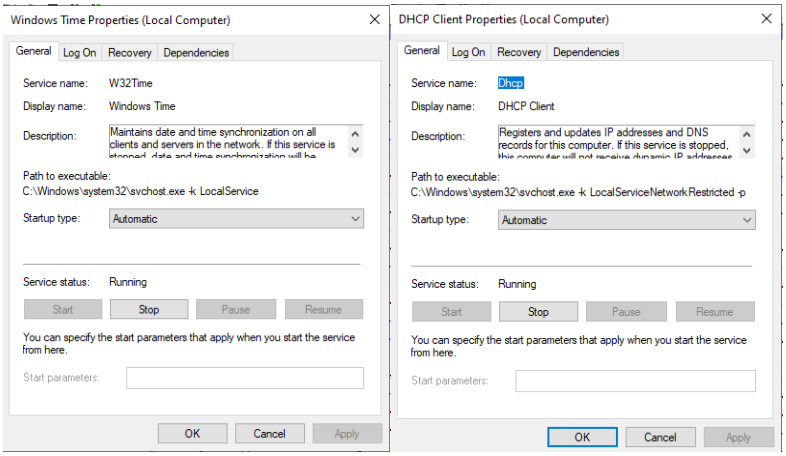

Рис. 3.14 Перегляд назв сервісів на сервері Serv-22-45-1 для налаштування їх моніторингу

Редагуємо конфігураційний файл ***/usr/local/nagios/etc/objects/windows/serv-22-45-1.cfg*** додаючи показані на рис. 3.14 служби:

```
define service {
    use                     generic-service
    host_name               serv-22-45-1
    service_description     Data Sharing Service
    check_command           check_nt!SERVICESTATE!-s P@ssw0rd -d SHOWALL -l DsSvc
}
define service {
    use                     generic-service
    host_name               serv-22-45-1
    service_description     DHCP Client
    check_command           check_nt!SERVICESTATE!-s P@ssw0rd -d SHOWALL -l Dhcp
}
```

Якщо нам знадобиться вимкнути моніторинг сервісу чи додатку, нижче наведено зразок вимикання моніторингу запуску Explorer.exe, коментуванням відповідної секції конфігурації:

```
#define service {            # Service for monitoring the Explorer.exe process
#    use                     generic-service
#    host_name               serv-22-45-1
#    service_description     Explorer
#    check_command           check_nt!PROCSTATE!-s P@ssw0rd -d SHOWALL -l explorer.exe
#}
```

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

Рис. 3.15. Перегляд налаштованого моніторингу сервісів Serv-22-45-1 та вміст Host Groups Nagios

Завдання до лабораторної роботи

1. Налаштуйте HTTP-доступ для свого VirtualBox Host через NAT до Nagios Serv-G-N-3.
2. Встановіть та налаштуйте на сервері Serv-G-N-1 актуальну версію агента моніторингу NSClient++.
3. Налаштуйте моніторинг основних сервісів (мінімум 2) серверу Serv-G-N-1. Моніторинг серверу Serv-G-N-3 залишаємо без змін. У звіті обов'язково наведіть скріни закладок Hosts та View Service Details for Serv-G-N-1.
4. Відредагуйте конфігурацію Nagios таким чином, щоб у системі було дві активних групи хостів: Windows-server та Linux-server. Закладка Host Groups Nagios.

Звіт має містити:

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

Додаток 1.

Перелік базових командних рядків check_nt для роботи з NSClient

У додатку наведено повні командні рядки, що використані у вигляді команд при побудові конфігурації хосту з NSClient++.

В прикладах -s використано пароль NSClient++ P@ssw0rd

Після -H - IP-хосту, де встановлено NSClient++ 192.168.45.135

/usr/local/nagios/libexec/check_nt -H 192.168.45.135 -p 12489 -s P@ssw0rd -v CPULOAD -l 5,80,90
CPU Load 34% (5 min average) | '5 min avg Load'=34%;80;90;0;100

/usr/local/nagios/libexec/check_nt -H 192.168.45.135 -p 12489 -s P@ssw0rd -v CLIENTVERSION
NSClient++ 0.6.0.1 2023-07-30

/usr/local/nagios/libexec/check_nt -H 192.168.45.135 -p 12489 -s P@ssw0rd -v UPTIME
System Uptime - 0 day(s) 0 hour(s) 8 minute(s) |uptime=8

/usr/local/nagios/libexec/check_nt -H 192.168.45.135 -p 12489 -s P@ssw0rd -v MEMUSE -w 80 -c 90
Memory usage: total:4799.59 MB - used: 1405.62 MB (29%) - free: 3393.97 MB (71%) | 'Memory usage'=1405.62MB;3839.67;4319.63;0.00;4799.59

/usr/local/nagios/libexec/check_nt -H 192.168.45.135 -p 12489 -s P@ssw0rd -v USEDDISKSPACE -l c -w 80 -c 90
c:\ - total: 49.46 Gb - used: 11.51 Gb (23%) - free 37.96 Gb (77%) | 'c:\ Used Space'=11.51Gb;39.57;44.52;0.00;49.46

/usr/local/nagios/libexec/check_nt -H 192.168.45.135 -p 12489 -s P@ssw0rd -v SERVICESTATE -l Dhcp

OK: All 1 service(s) are ok.

Корисні посилання

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

- GitHub. NSClient. NagiosExange
https://exchange.nagios.org/directory/Addons/Monitoring-Agents/NSClient++/details

- GitHub. NSClient. Version history. Download page
https://github.com/mickem/nscp/releases

- Installing the Windows Agent NSClient++
https://nagiosenterprises.my.site.com/support/s/article/Installing-the-Windows-Agent-NSClient-0b485593

- How to Install NSClient Nagios Monitoring Agent on Windows System
https://kifarunix.com/how-to-install-nsclient-nagios-monitoring-agent-on-windows-system/

- Installing NSClient++
https://nsclient.org/docs/installing/

- How to Monitor and Configure a Windows Server Using Nagios
https://webhostinggeeks.com/howto/how-to-monitor-and-configure-a-windows-server-using-nagios/