Лабораторна робота №3

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

Мета: налаштувати моніторинг базових параметрів Windows сервера у Nagios 4.X за допомогою агента моніторингу NSClient++.

Інструменти: гіпервізор VirtualBox, модель комп'ютерної мережі.

Завдання до лабораторної роботи

1. Налаштуйте HTTP-доступ для свого VirtualBox Host через NAT до Nagios Serv-G-N-2.
2. Встановіть та налаштуйте на сервері Serv-G-N-1 актуальну версію агента моніторингу NSClient++.
3. Налаштуйте моніторинг основних сервісів (мінімум 10) серверу Serv-G-N-1. Моніторинг серверу Serv-G-N-2 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.

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.

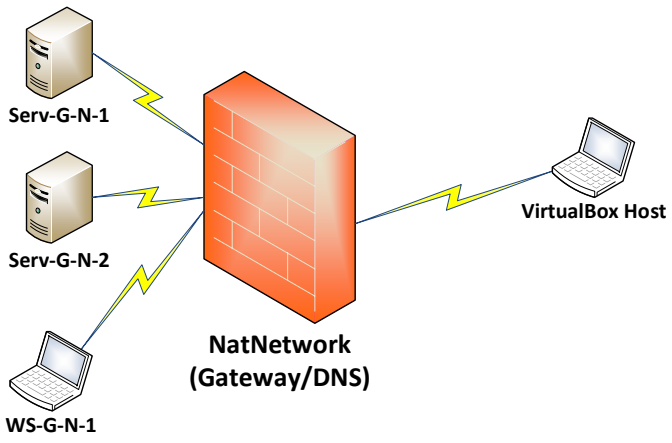

Рис. 3.1. Топологія мережі

На сервері Serv-G-N-2 розгорнуто систему моніторингу на базі Nagios 4.X. Ми підключилися з хосту NAT Network по протоколу HTTP до неї під користувачем nagios

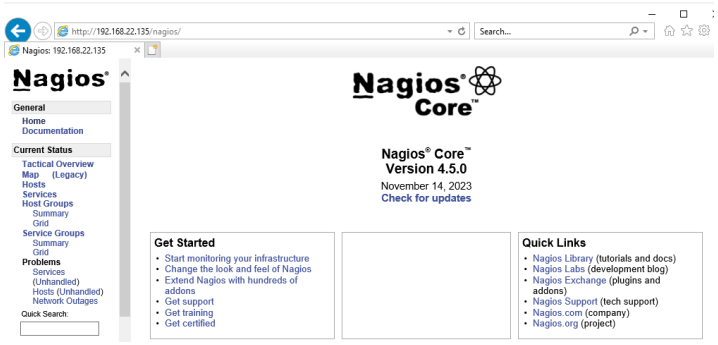

Рис. 3.2. Підключення до Nagios з серверу DC Serv-22-1-1.

Налаштуємо HTTP доступ через NAT Network для VirtualBox Host. У моєму випадку на VirtualBox Host не використовується порт 80, тому Port Forwarding відсутній у налаштування – для підключення через NAT Network використовуємо той же 80 порт. На рис. 3.3 показане таке налаштування NAT Network та підключення до серверу Serv-G-N-2 по IP-адресі та до системи моніторингу Nagios.

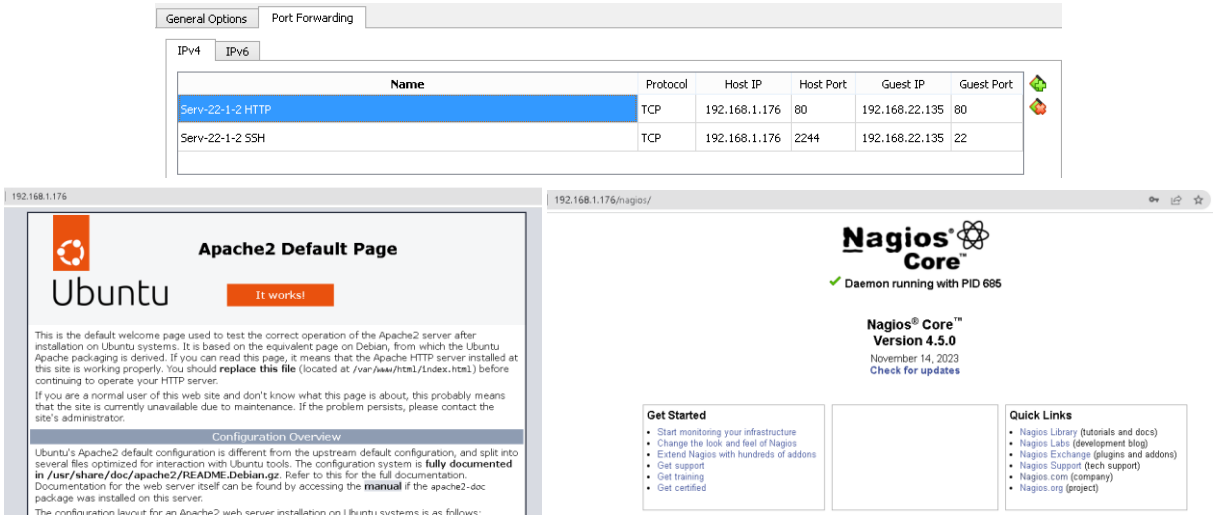

Рис. 3.3. NAT Network. HTTP port settings та підключення з VirtualBox Host по HTTP

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 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

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 - #0.6.0.1.

Завантажуємо та встановлюємо версію, у відповідності до нашої платформи https://github.com/mickem/nscp/releases/download/0.6.0.1/NSCP-0.6.0.1-x64.msi .

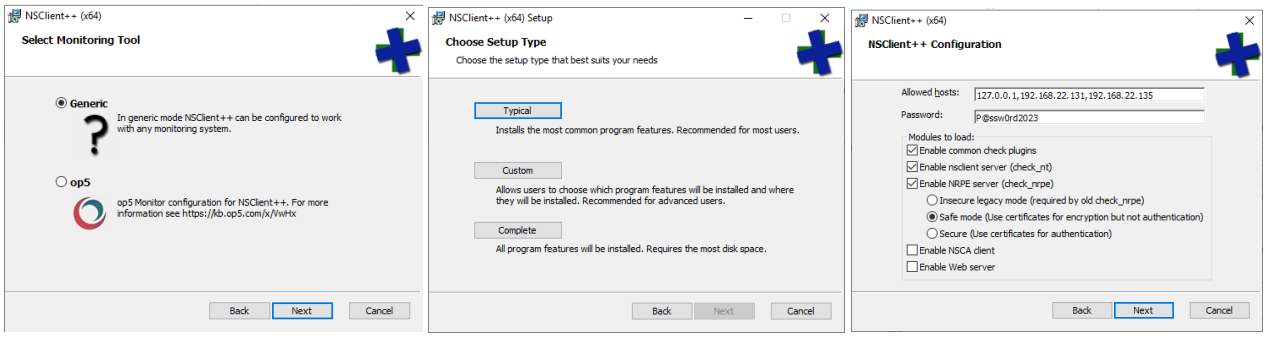

Рис. 3.4. Типова, рекомендована інсталяція NSClient++.

У статті Installing the Windows Agent NSClient++ більш докладно описаний наведений на рис. 3.4 процес інсталяції агента NSClient++.

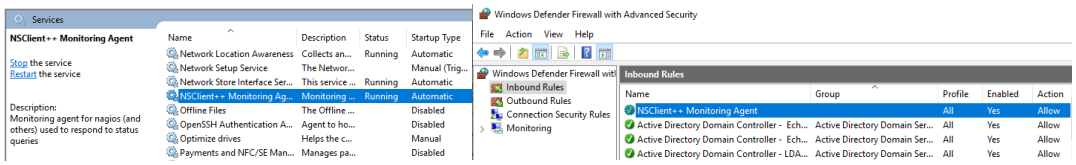

Рис. 3.5. Служба NSClient++ та відповідне правило Windows Firewall.

Поточна версія агента NSClient++ в процесі інсталяції автоматично конфігурує відповідну службу та правило Windows Firewall. Необхідно дещо відредагувати конфігурацію агента. Відкриваємо для редагування файл C:\Program Files\NSClient++\nsclient.ini , шукаємо у ньому ключі CheckEventLog, CheckDisk, CheckSystem та встановлюємо для них значення enabled.

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

Перезавантажуємо службу NSClient++ Monitoring Agent. Конфігурування агента NSClient++ на стороні Windows сервера Serv-G-N-1 завершено. Перевіримо на стороні сервера моніторингу Serv-G-N-2 чи всі налаштування працюють. Для цього виконаємо у ручному режимі команду перевірки зв'язку:

```
student@serv-22-1-2:~$ /usr/local/nagios/libexec/check_nt -H 192.168.22.131 -p 12489 -s P@ssw0rd2023 -v CPULOAD -l 5,80,90
CPU Load 3% (5 min average) |   '5 min avg Load'=3%;80;90;0;100
student@serv-22-1-2:~$
```

Рис. 3.6. Перевірка зв'язку між Nagios(Serv-22-1-2) та NSClient++(Serv-22-1-1).

На рис.3.6 показане виконання команди

/usr/local/nagios/libexec/check_nt -H 192.168.22.131 -p 12489 -s P@ssw0rd2023 -v CPULOAD -l 5,80,90

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 192.168.22.131

Вказує IP-адресу або ім'я хоста (hostname) Windows-сервера, який ви моніторите.

-p 12489

Вказує порт, на якому слухає NSClient++. У цьому випадку, 12489 є стандартним портом для взаємодії з NSClient++.

-s P@ssw0rd2023

Вказує пароль для взаємодії з NSClient++. Цей пароль налаштовується при інсталяції агента на сервері 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-22-1-2:/usr/local/nagios/etc/objects$ sudo mkdir windows
[sudo] password for student:
student@serv-22-1-2:/usr/local/nagios/etc/objects$ sudo mkdir workstation
student@serv-22-1-2:/usr/local/nagios/etc/objects$ sudo mkdir linux
student@serv-22-1-2:/usr/local/nagios/etc/objects$ sudo mkdir network
student@serv-22-1-2:/usr/local/nagios/etc/objects$ sudo mkdir website
student@serv-22-1-2:/usr/local/nagios/etc/objects$ dir
commands.cfg  localhost.cfg  switch.cfg       website      workstation
contacts.cfg  network        templates.cfg    windows
linux         printer.cfg    timeperiods.cfg  windows.cfg
student@serv-22-1-2:/usr/local/nagios/etc/objects$
```

Рис. 3.7. 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:

```
# OBJECT CONFIGURATION FILE(S)
# These are the object configuration files in which you define hosts,
# host groups, contacts, contact groups, services, etc.
# You can split your object definitions across several config files
# if you wish (as shown below), or keep them all in a single config file.

# You can specify individual object config files as shown below:
cfg_file=/usr/local/nagios/etc/objects/commands.cfg
cfg_file=/usr/local/nagios/etc/objects/contacts.cfg
cfg_file=/usr/local/nagios/etc/objects/timeperiods.cfg
cfg_file=/usr/local/nagios/etc/objects/templates.cfg

# Definitions for monitoring the local (Linux) host
cfg_file=/usr/local/nagios/etc/objects/localhost.cfg

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

```
# You can also tell Nagios to process all config files (with a .cfg
# extension) in a particular directory by using the cfg_dir
# directive as shown below:

#cfg_dir=/usr/local/nagios/etc/servers
#cfg_dir=/usr/local/nagios/etc/printers
#cfg_dir=/usr/local/nagios/etc/switches
#cfg_dir=/usr/local/nagios/etc/routers
cfg_dir=/usr/local/nagios/etc/objects/windows
cfg_dir=/usr/local/nagios/etc/objects/workstation
cfg_dir=/usr/local/nagios/etc/objects/linux
cfg_dir=/usr/local/nagios/etc/objects/network
cfg_dir=/usr/local/nagios/etc/objects/website
```

Рис. 3.8. Редагування файлу конфігурації /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-22-1-1.cfg

Відкриваємо створений файл serv-22-1-1.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-22-1-1* *alias DC-DNS-DHCP falkovsky.net* *address 192.168.22.131* *}*	Визначення об’єкту моніторингу: ім’я серверу, аліас, IP адреса.
# SERVICE DEFINITIONS	Визначення сервісів
define service {	Моніторинг сервісу NSClient++
use generic-service *host_name serv-22-1-1* *service_description NSClient++ Version* *check_command check_nt!CLIENTVERSION -s P@ssw0rd2023* *}*	Зверніть увагу на параметр -s за яким має бути вказаний пароль NSClient++ для цього хоста.
define service {	Моніторинг часу роботи сервера
use generic-service *host_name serv-22-1-1* *service_description Uptime* *check_command check_nt!UPTIME -s P@ssw0rd2023* *}*	
define service {	Моніторинг завантаження ЦП
use generic-service *host_name serv-22-1-1* *service_description CPU Load* *check_command check_nt!CPULOAD!-s P@ssw0rd2023 -l 5,80,90* *}*	Зверніть увагу на положення паролю агенту у командному рядку
define service {	Моніторинг фізичної пам’яті
use generic-service *host_name serv-22-1-1* *service_description Memory Usage* *check_command check_nt!MEMUSE!-s P@ssw0rd2023 -w 80 -c 90* *}*	Зверніть увагу на положення паролю агенту у командному рядку
define service {	Моніторинг системного диску
use generic-service *host_name serv-22-1-1* *service_description C:\ Drive Space* *check_command check_nt!USEDDISKSPACE! -s P@ssw0rd2023 -l c -w 80 -c 90* *}*	Зверніть увагу на положення паролю агенту у командному рядку
define service {	Зразок моніторингу служби на прикладі World Wide Web Publishing Service
use generic-service *host_name serv-22-1-1* *service_description W3SVC* *check_command check_nt!SERVICESTATE!-d SHOWALL -l W3SVC -s P@ssw0rd2023* *}*	
define service {	Зразок моніторингу процесу на прикладі Explorer.exe
use generic-service *host_name serv-22-1-1* *service_description Explorer* *check_command check_nt!PROCSTATE!-d SHOWALL -l Explorer.exe -s P@ssw0rd2023* *}*	

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

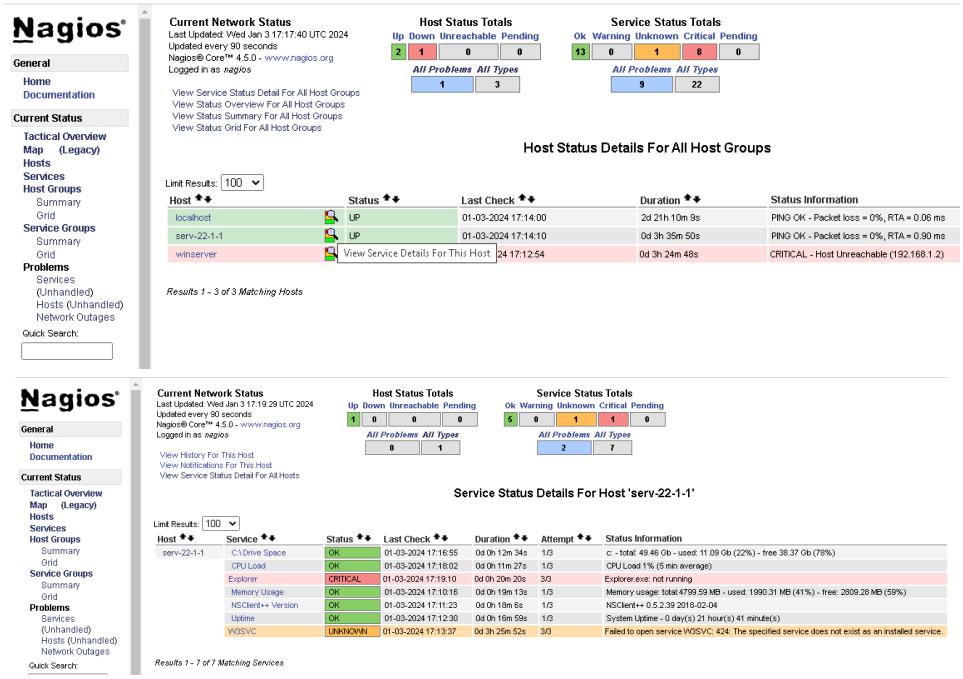

*Рис. 3.9. Перегляд розділу **Hosts** та **View Service Details for** serv-22-1-1*

На рис. 3.9 показаний перегляд отриманої конфігурації – три хости localhost, serv-22-1-1 та winserver. Для шаблону windows.cfg необхідно відключити відображення у створеній конфігурації.

Створюємо новий конфігураційний файл /usr/local/nagios/etc/objects/hostgroups.cfg, де буде описана група серверів, шаблоном для якої виступав шаблон /usr/local/nagios/etc/objects/windows.cfg

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

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
```

«Приховуємо» відключений конфігураційний файл шляхом перейменування:

sudo mv /usr/local/nagios/etc/objects/windows.cfg /usr/local/nagios/etc/objects/windows.cfg.tmp

«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

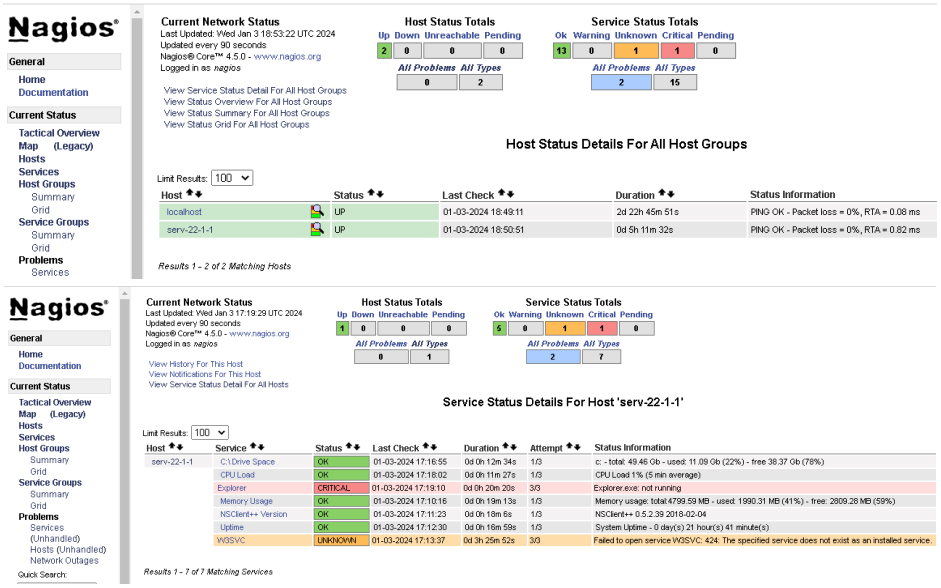

*Рис. 3.10. Перегляд розділу **Hosts** після вимкнення перевірок для шаблону winserver та **View Service Details for serv-22-1-1***

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

На Windows-сервері розгорнуто ряд ролей таких як доменний контролер DC, DNS- та DHCP-сервер. Існує багато служб, які можна моніторити для забезпечення стабільності та ефективності. Підключимо лише кілька з рекомендованих для моніторингу на таких серверах:

- Active Directory Domain Services (NTDS)
- DNS Server
- DHCP Server
- Windows Time (W32Time)
- Windows Remote Management (WinRM)

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.

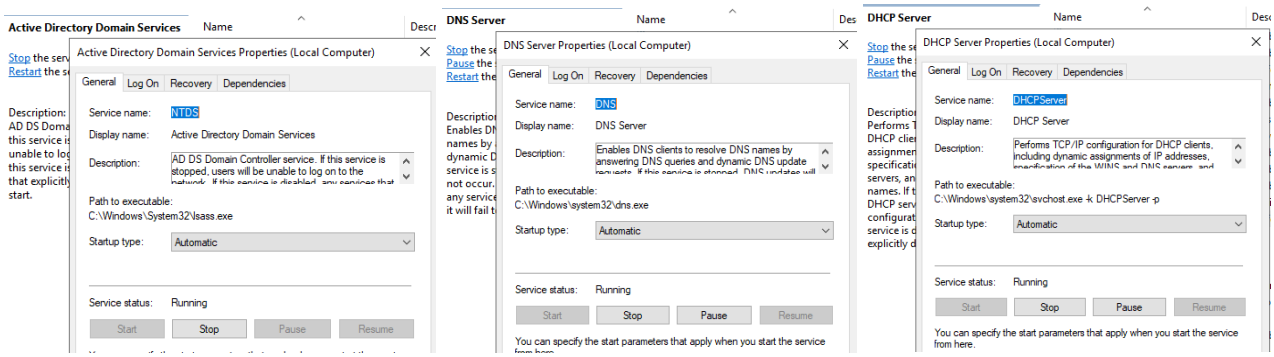

Рис. 3.11. Перегляд назв сервісів на сервері Serv-22-1-1 для налаштування їх моніторингу

Редагуємо конфігураційний файл /usr/local/nagios/etc/objects/windows/serv-22-1-1.cfg замінюючи зразок служби World Wide Web Publishing Service (IIS) на описані вище 5 служб:

```
define service {
    use                     generic-service
    host_name               serv-22-1-1
    service_description     Active Directory Domain Services
    check_command           check_nt!SERVICESTATE!-s P@ssw0rd2023 -d SHOWALL -l NTDS
}
define service {
    use                     generic-service
```

```
    host_name               serv-22-1-1
    service_description     DNS Server
    check_command           check_nt!SERVICESTATE!-s P@ssw0rd2023 -d SHOWALL -l DNS
}
define service {
    use                     generic-service
    host_name               serv-22-1-1
    service_description     DHCP Server
    check_command           check_nt!SERVICESTATE!-s P@ssw0rd2023 -d SHOWALL -l
DHCPServer
}
define service {
    use                     generic-service
    host_name               serv-22-1-1
    service_description     Windows Time
    check_command           check_nt!SERVICESTATE!-s P@ssw0rd2023 -d SHOWALL -l
W32Time
}
define service {
    use                     generic-service
    host_name               serv-22-1-1
    service_description     Windows Remote Management
    check_command           check_nt!SERVICESTATE!-s P@ssw0rd2023 -d SHOWALL -l
WinRM
}
```

Вимикаємо моніторинг запуску Explorer.exe, коментуючи відповідну секцію конфігурації, або просто видаляючи її:

```
#define service {            # Service for monitoring the Explorer.exe process
#    use                     generic-service
#    host_name               serv-22-1-1
#    service_description     Explorer
#    check_command           check_nt!PROCSTATE!-s P@ssw0rd2023 -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

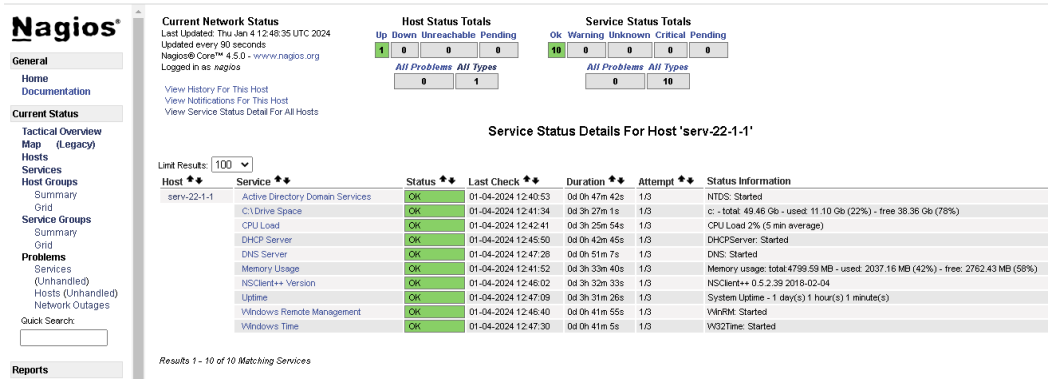

Рис. 3.12. Перегляд налаштованого моніторингу сервісів на сервері Serv-22-1-1

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/