Лабораторна робота №5

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

Мета: формування навичок налаштування пасивного моніторингу серверів Linux у системі Nagios 4.x за допомогою агента NCPA, оптимізації роботи системи моніторингу шляхом управління хостами та їх інтеграції до тематичних груп хостів.

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. До серверу Serv-G-N-3 налаштовано SSH доступ через NAT Network для VirtualBox Host.

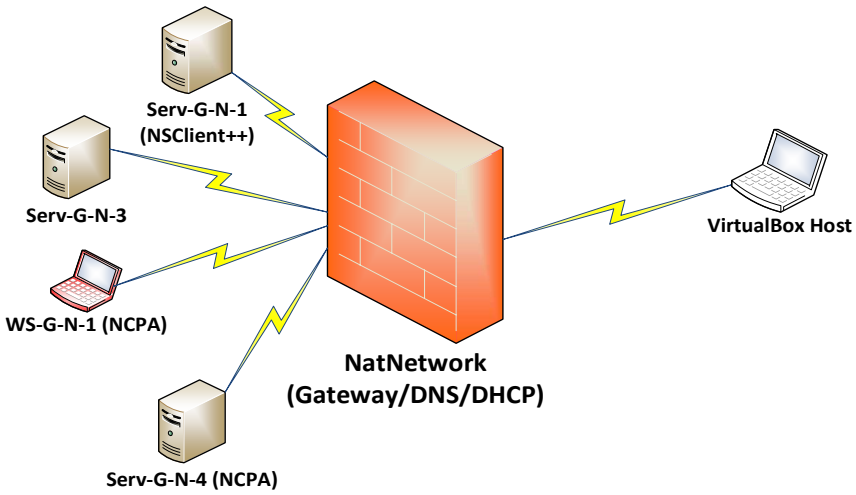

Рис. 5.1. Топологія мережі

На сервері Serv-G-N-3 автоматично, при інсталяції серверу, розгорнуто систему моніторингу на базі Nagios 4.X. Моніторинг основних сервісів серверу Serv-G-N-1 виконується за допомогою NSClient++. Для робочої станції WS-G-N-1 налаштовано моніторинг за допомогою NCPA. Налаштовано підключення з хосту NAT Network по протоколу HTTP до системи моніторингу під користувачем nagios.

Рис. 5.2. Hosts, Host Groups.

Рис. 5.3. Service Status Details for host WS-22-45-1.

Зверніть увагу на «жовтий» статус використання пам'яті на робочій станції WS-22-45-1 (рис.5.2, 5.3). Використані порогові налаштування не підходять для даної робочої станції і тому рекомендовано змінити рядок:

```
check_command          check_ncpa!-t 'P@ssw0rd' -P 5693 -M memory/virtual -w 50 -c 80 -u G
```

Підвищуємо порогові значення Warning з 50 до 80% а Critical з 80 до 90%.

```
check_command          check_ncpa!-t 'P@ssw0rd' -P 5693 -M memory/virtual -w 80 -c 90 -u G
```

Рис. 5.4. Service Status Details for WS-22-45-1 після редагування порогових значень.

Якщо Ваш ПК має менше 16 Gb фізичної пам'яті, для зменшення навантаження на VirtualBox Host, можливо тимчасово відключити робочу станцію WS-G-N-1 та її моніторинг. Для цього перейменовуємо конфігураційний файл робочої станції:

sudo mv /usr/local/nagios/etc/objects/workstation/ws-22-45-1.cfg /usr/local/nagios/etc/objects/workstation/ws-22-45-1.cfg.bkp

Після редагувань файлів конфігурації, перевіряємо відсутність помилок у конфігурації та перезапускаємо сервіс Nagios:

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

sudo service nagios restart

Робоча станція WS-G-N-1 може бути вимкнута.

Створюємо віртуальну машину для розгортання серверу Serv-G-N-4 (рис.5.1.), побудованому на ОС Ubuntu 24.04. Для розгортання серверу імпортується VirtualBox appliance файл Serv-G-N-3.ova.

Після імпорту серверу з appliance його необхідно перейменувати у відповідності до варіанту. Перегляд та перейменування поточного імені серверу:

sudo hostname Serv-G-N-4

hostnamectl

sudo hostnamectl set-hostname New-Name-Server

sudo reboot

Де Serv-G-N-4 – нове ім'я серверу. Після імпорту, або інсталяції сервера необхідно виконати його підключення до відповідної віртуальної мережі, до якої підключені інші хости моделі комп'ютерної мережі. Підключення показано на рис. 5.5.

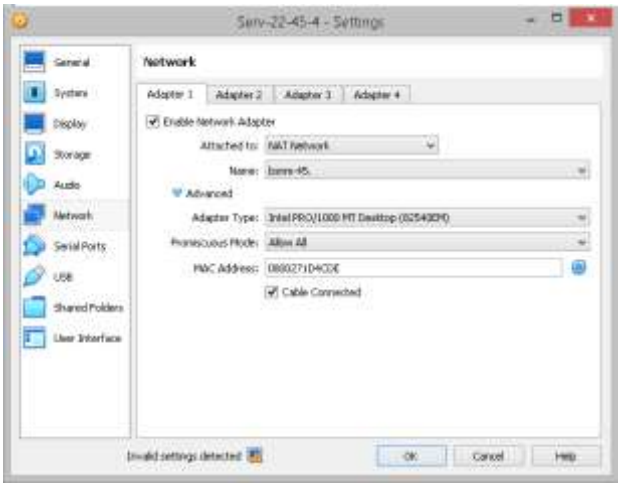

Рис. 5.5. Мережеві налаштування для ВМ Serv-22-45-4 (Ubuntu 22.04) у VirtualBox.

Переглядаємо ім'я серверу та перейменовуємо його:

Hostnamectl

sudo hostnamectl set-hostname New-Name-Server

sudo reboot

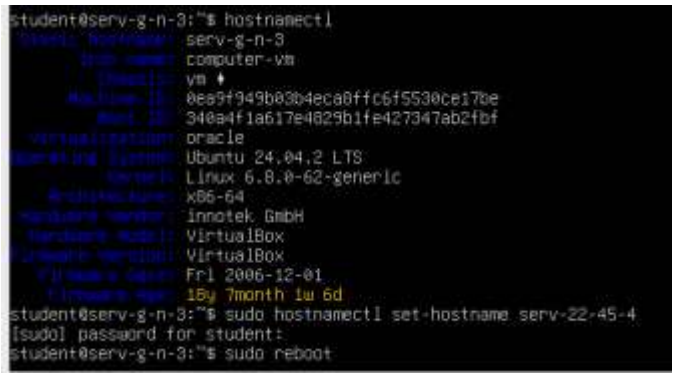

Рис. 5.6. Ім'я серверу Serv-22-45-4.

Serv-G-N-4 сконфігуровано на динамічну адресацію і, можливо, він отримує адресу від DHCP NAT Network. Повторюємо дії, детально описані у методичних вказівках до лабораторної роботи №1.

Змінюємо налаштування динамічної адреси на статичну. Шукаємо назву мережевого інтерфейсу, який необхідно відредагувати

ip a або ***ip link***

sudo dir /etc/netplan

Шукаємо конфігураційні файли Netplan (з розширенням YAML), що зберігаються в каталозі /etc/netplan. Ймовірно, у цьому каталозі є один або декілька файлів YAML. Назва файлу може відрізнятися залежно від налаштувань та версії операційної системи.

sudo dir /etc/netplan

Наприклад, у каталозі знайдено файл 50-cloud-init.yaml. Робимо його копію для редагування:

sudo cp /etc/netplan/50-cloud-init.yaml /etc/netplan/45-natnet.yaml

Відкриваємо для редагування

sudo vi /etc/netplan/45-natnet.yaml

Нижче наведено вміст файлу Netplan до та після редагування.

/etc/netplan/50-cloud-init.yaml --- DHCP	**/etc/netplan/45-natnet.yaml Static 192.168.40.132/27**

`network:`
`  version: 2`
`  ethernets:`
`  enp0s3:`
`  dhcp4: true`
	`network:`
	`  version: 2`
	`  ethernets:`
	`  enp0s3:`
	`  addresses: [192.168.45.132/27]`
	`  gateway4: 192.168.45.129`
	`  nameservers:`
	`  addresses: [192.168.45.129]`

Зберігаємо відредагований Netplan та застосовуємо внесені зміни: ***sudo netplan apply***

Налаштовуємо Port Forwarding для організації SSH доступу до серверу Serv-G-N-4 з фізичної машини – хоста VirtualBox. Налаштування виконується у меню

[Oracle VirtualBox Manager] – [File] – [Tools] – [Network Manager] – [Nat Network] – [Properties] – [Port Forfarding] – [IPv4].

Назва правила NAT – "Serv-G-N-4 SSH" ,

де G – група,

N – варіант, що Ви виконуєте, протокол – "TCP".

У якості Guest IP задаємо IP-адресу сервера, яку ми отримали за допомогою команди ip a , Port – 22 – порт «за замовчуванням» для SSH доступу. Повторюємо дії, описані у методиці визначення адрес та портів описаній у методичних вказівках до лабораторної роботи №1.

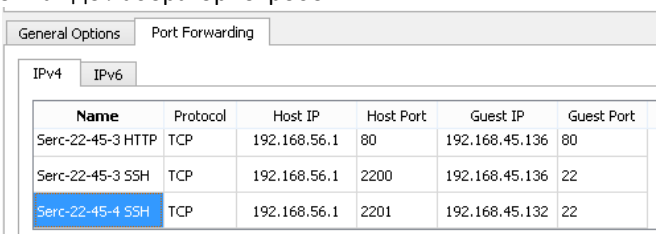

Рис.5.7. Налаштування правила переадресації порту для SSH до серверу Serv-22-45-3[192.16.45.132]. Для переадресації використовується порт 2201.

На рис. 5.7 показане налаштування port forwarding для SSH підключення у NAT Network. У якості порту переадресації для Serv-22-45-3 обрано 2200, для Serv-22-43-4 – порт 2201. Для Serv-22-45-3 організовано доступ по 80 порту (HTTP) до системи моніторингу Nagios.

Підключаємося до Serv-22-45-4 за допомогою Putty. Офіційний сайт інструменту https://www.putty.org/

Можливе використання будь-якого іншого SSH-клієнта на ваш розсуд .

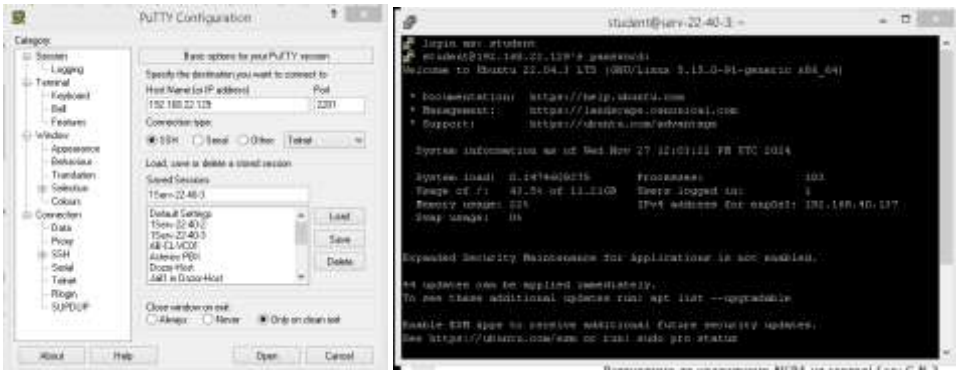

Рис. 5.8. PuTTY SSH до серверу Serv-22-45-4

Встановимо та налаштуємо NCPA на сервері Serv-G-N-4.

Завантажуємо останню стабільну версію агента для DEB Linux 64-bit (Ubuntu 16+) з офіційного сайту https://www.nagios.org/projects/ncpa/#download-ncpa-section. На момент написання цього документу це версія 3.1.3.

Переходимо в тимчасовий каталог (може бути будь-який, наприклад, /tmp)

cd /tmp

Завантажуємо та встановлюємо NCPA

sudo wget https://assets.nagios.com/downloads/ncpa3/ncpa-latest-1.amd64.deb

sudo dpkg -i ./ncpa-latest-1.amd64.deb

Запуск та перевірка роботи служби NCPA:

sudo systemctl start ncpa

sudo systemctl status ncpa

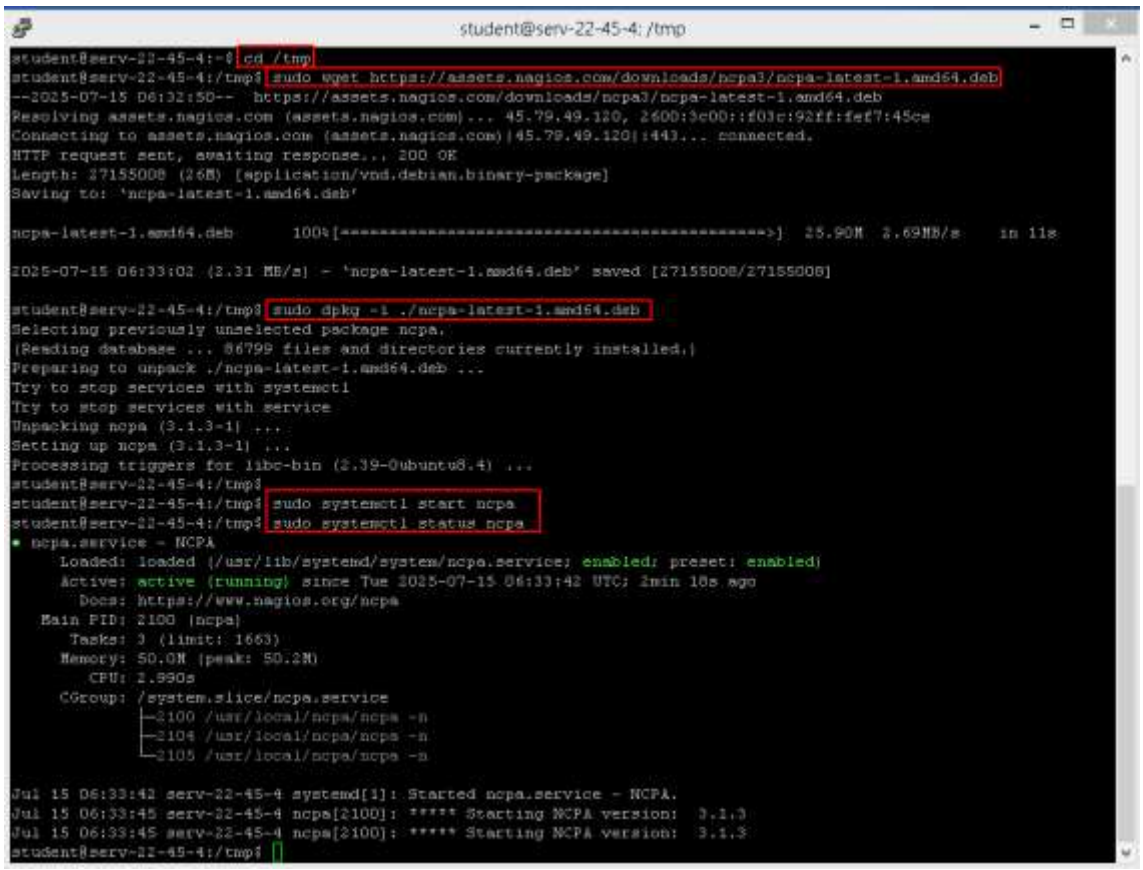

Рис. 5.9. Завантаження, встановлення та запуск NCPA на сервері Serv-22-45-4

Для забезпечення безпеки та автентифікації налаштовуємо Token-и, аналогічно налаштуванням NCPA for Windows. Це робиться редагуванням конфігураційного файлу NCPA, який знаходиться в ***/usr/local/ncpa/etc/ncpa.cfg***. Шукаємо розділ [api] та встановлюємо таємний ключ (Token) для пасивних перевірок.

```
community_string = mytoken                    #було
community_string = P@ssw0rd               #стало
```

А за рядком дозволу WEB API доступу admin_gui_access = 1 встановлюємо Token для HTTP WEB API. Він може відрізнятися від ключа, що встановлений для пасивних перевірок, але враховуючи, що це навчальний стенд, у якості ключа встановлено типову послідовність символів P@ssw0rd

```
admin_password = None                         #було
admin_password = P@ssw0rd                     #стало
```

Зберігаємо зміни та перезапускаємо службу NCPA:

sudo systemctl restart ncpa

Перевірка працездатності NCPA може бути виконана аналогічно перевіркам, що ми виконували для NCPA for Windows. Перевірка, що служба NCPA працює правильно та слухає порт безпосередньо на NCPA:

nc -zv localhost 5693

або з з серверу Nagios

nc -zv 192.168.45.132 5693

перевірка ЦП серверу

/usr/local/nagios/libexec/check_ncpa.py -H 192.168.45.132 -p 5693 -t P@ssw0rd -M cpu/percent -w 80 -c 90 -q 'aggregate=avg'

Рис. 5.10. Перегляд відгуку NCPA серверу Serv-22-45-4 з Serv-22-45-3

Відредагуємо на сервері *Serv-22-45-3* конфігураційні файли для вірного відображення групи серверів Linux. У файлі груп хостів ***/usr/local/nagios/etc/objects/hostgroups.cfg*** додаємо секцію Linux Servers:

```
define hostgroup {
    hostgroup_name  linux-servers
    alias           Linux Servers
}
```

У файлі конфігурації локального серверу ***/usr/local/nagios/etc/objects/localhost.cfg*** «прибираємо» відповідну секцію, додаємо «належність» до групи хостів та виправляємо ім'я та аліас імені хосту на реальне (у всіх секціях конфігурації):

```
#define hostgroup {
#    hostgroup_name          linux-servers          ; The name of the hostgroup
#    alias                   Linux Servers          ; Long name of the group
#    members                 localhost              ; Comma separated list of hosts that belong to this group
#}
define host {
use                     linux-server
hostgroups              linux-servers
host_name               serv-22-45-3
alias                   Serv-22-45-3
address                 127.0.0.1
 }
```

У головному конфігураційному файлі /usr/local/nagios/etc/nagios.cfg прибираємо з переліку конфігураційних файлів файл локального хосту:

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

Переносимо конфігураційний файл локального хосту до каталога, зарезервованого для групи хостів Linux Servers

sudo mv /usr/local/nagios/etc/objects/localhost.cfg /usr/local/nagios/etc/objects/linux/localhost.cfg

«Звична», але обов'язкова 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

Створюємо типовий конфігураційний файл для нового серверу Serv-G-N-3 з групи хостів Linux Servers у відповідному, зарезервованому каталозі: **/usr/local/nagios/etc/objects/linux/serv-22-45-4.cfg**

```
define host {
    host_name               serv-22-45-4
    address                 192.168.45.132
    use                     linux-server
    hostgroups              linux-servers
    check_command           check_ncpa!-t 'P@ssw0rd' -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               serv-22-45-4
    use                     generic-service
    service_description     CPU Usage
    check_command         check_ncpa!-t 'P@ssw0rd' -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               serv-22-45-4
    use                     generic-service
    service_description     Memory Usage
    check_command           check_ncpa!-t 'P@ssw0rd' -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               serv-22-45-4
    use                     generic-service
    service_description     Process Count
    check_command           check_ncpa!-t 'P@ssw0rd' -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
}
```

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

Перегляд всіх доступних параметрів моніторингу для цього серверу з серверу Nagios:

/usr/local/nagios/libexec/check_ncpa.py -H 192.168.40.132 -t P@ssw0rd -p 5693 –list

Додаємо кілька важливих параметрів моніторингу для серверу Serv-G-N-4 у файл конфігурації:

```
define service {
    host_name               serv-22-45-4
   service_description     Ethernet. Sent bytes
   check_command           check_ncpa!-t 'P@ssw0rd' -P 5693 -M interface/enp0s3/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               serv-22-45-4
   service_description     Ethernet. Received bytes
   check_command          check_ncpa!-t 'P@ssw0rd' -P 5693 -M interface/enp0s3/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
}
define service {
    host_name               serv-22-45-4
    service_description     System operation time
    check_command           check_ncpa!-t 'P@ssw0rd' -P 5693 -M 'system/uptime'
    max_check_attempts      5
    check_interval          5
    retry_interval          1
    check_period            24x7
    notification_interval   60
    notification_period     24x7
```

```
}
      define service {
          host_name                serv-22-45-4
          use                      generic-service
          service_description      Logical disk
          check_command         check_ncpa!-t 'P@ssw0rd' -P 5693 -M 'disk/logical/|/free' --warning 10: --critical 5: -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                serv-22-45-4
          use                      generic-service
          service_description      Logical disk used percent
         check_command          check_ncpa!-t 'P@ssw0rd' -P 5693 -M 'disk/logical/|/used_percent' --warning 90 --critical 95
          max_check_attempts       5
          check_interval           5
          retry_interval           1
          check_period             24x7
          notification_interval    60
          notification_period      24x7
      }
define service {
    host_name                serv-22-45-4
    use                      generic-service
    service_description      Disk SDA. Read bytes
    check_command            check_ncpa!-t 'P@ssw0rd' -P 5693 -M 'disk/physical/sda/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                serv-22-45-4
    use                      generic-service
    service_description      Disk SDA. Write bytes
    check_command            check_ncpa!-t 'P@ssw0rd' -P 5693 -M 'disk/physical/sda/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                serv-22-45-4
    use                      generic-service
    service_description      Disk SDA. Read time
    check_command            check_ncpa!-t 'P@ssw0rd' -P 5693 -M 'disk/physical/sda/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
}
```

Доступ через GUI при підключенні до NCPA на сервері Serv-G-N-4 з серверу Serv-G-N-1, або робочої станції WS-G-N-1 що показаний на рис.5.11.

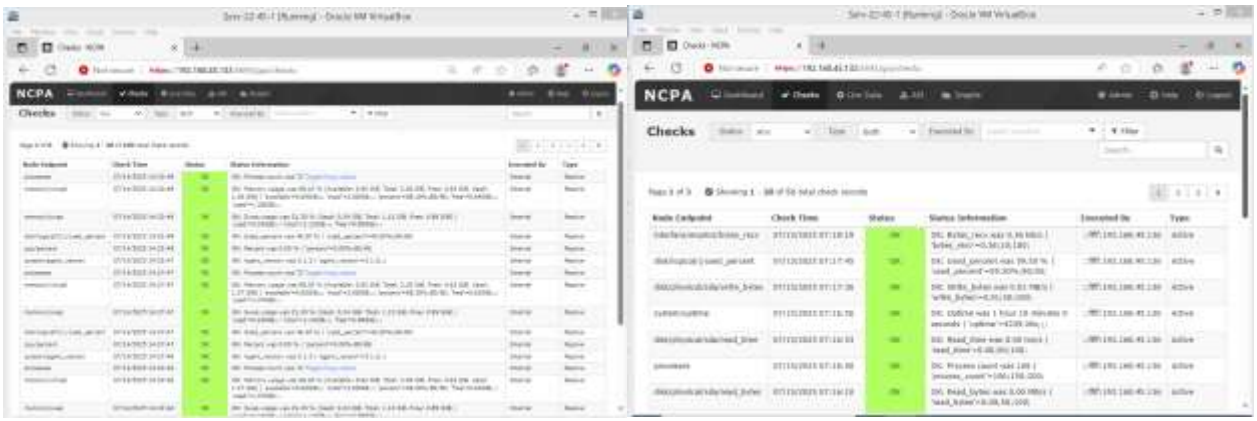

Рис. 5.11. Перегляд параметрів моніторингу Linux серверу Serv-22-45-4 через https://192.168.45.132:5693 та робочої станції WS-22-45-1 через https://192.168.45.133:5693 з Serv-22-40-1

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

Рис. 5.12. Перегляд виконаних налаштувань Service Status Details for host Serv-22-45-4

Змінюємо порогові значення для сервісу disk/logical/|/free. 1,59 Гб для ВМ такого типу достатньо ☺. На рис.5.12 показані зміни статусу цього сервісу.

Рис. 5.13. Перегляд налаштованих хостів та їх груп у Nagios.

Завдання до лабораторної роботи

1. Для зменшення навантаження на VirtualBox Host тимчасово відключіть робочу станцію WS-G-N-1 та її моніторинг.
2. Проінсталюйте або імпортуйте з appliance ВМ Ubuntu 22.04 Serv-G-N-4 та підключіть її до моделі комп'ютерної мережі (рис.5.1)
3. Встановіть та налаштуйте на Serv-G-N-4 актуальну версію агента моніторингу NCPA. У звіті обов'язково наведіть скрін HTTP-підключення до NCPA серверу.
4. Сконфігуруйте групи хостів Nagios для включення до групи Linux Servers локального хосту Nagios (Serv-G-N-3) та серверу Serv-G-N-4.
5. Налаштуйте моніторинг основних сервісів (мінімум 8) серверу Serv-G-N-4. У звіті обов'язково наведіть скріни закладок Hosts та View Service Details for Serv-G-N-4.

Звіт має містити:

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

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 запускалася 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

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