Лабораторна робота №7

Налаштування Nagios моніторингу на базі NRPE (Nagios Remote Plugin Executor).

Мета: формування практичних навичок налаштування та використання протоколу NRPE (Nagios Remote Plugin Executor) для моніторингу серверів Linux у системі Nagios, зокрема конфігурації NRPE на сервері моніторингу та віддаленому Linux-хості, а також додавання специфічних параметрів моніторингу.

Інструменти: гіпервізор VirtualBox, модель комп'ютерної мережі.

Теоретичні відомості

На рис.7.1. наведена модель комп'ютерної мережі, побудована під час виконання попередніх лабораторних робіт. До серверу Serv-G-N-2 налаштовано SSH доступ через NAT Network для VirtualBox Host.

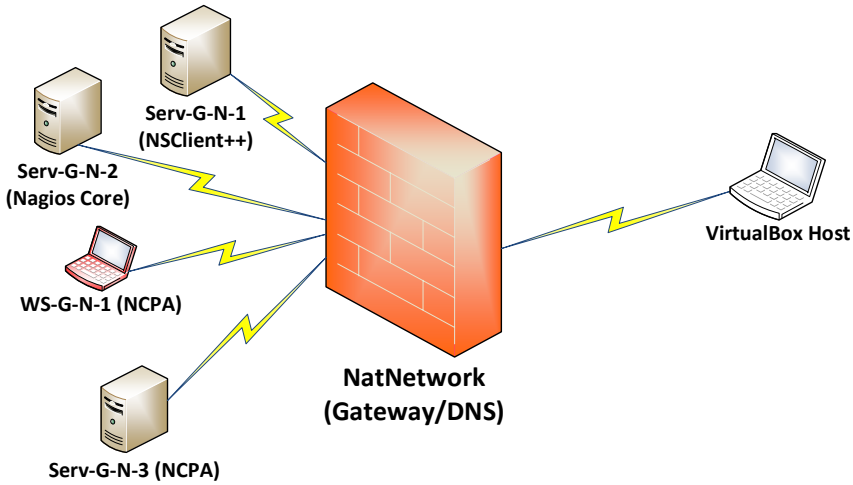


Рис. 7.1. Топологія мережі

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++. Основні сервіси робочої станції WS-G-N-1 та Ubuntu-серверу Serv-G-N-3 відслідковуються за допомогою NCPA. Налаштовано підключення з хосту NAT Network по протоколу HTTP до систему моніторингу під користувачем nagios.

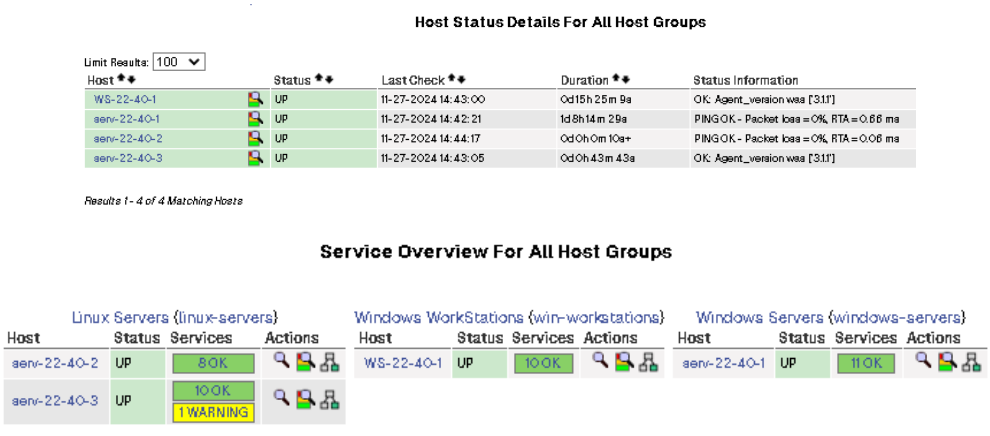


Рис. 7.2. Перегляд груп хостів та хостів у Nagios.

NRPE розроблений, щоб дозволити запускати плагіни Nagios на віддалених машинах Linux/Unix. Основна причина для цього полягає в тому, щоб дозволити Nagios контролювати «локальні» ресурси (наприклад, навантаження ЦП, використання пам'яті тощо) на віддалених машинах. Оскільки ці загальнодоступні ресурси зазвичай не доступні зовнішнім машинам, на віддалених машинах Linux/Unix потрібно встановити такий агент, як NRPE.

Плагіни Nagios можна запускати на віддалених машинах Linux/Unix через SSH. Існує плагін check_by_ssh, який дозволяє це зробити. Використання SSH є більш безпечним, ніж агент NRPE, але воно також накладає більші витрати (ЦП) як на моніторинг, так і на віддалені машини. Це може стати проблемою, коли ви починаєте стежити за сотнями або тисячами машин. Багато адміністраторів Nagios вибирають використання NRPE через менше навантаження.

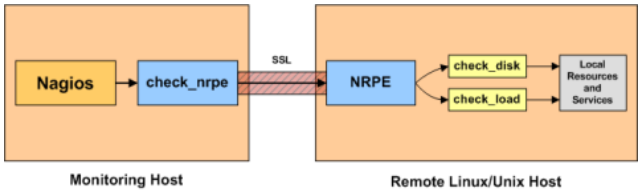


Рис. 7.3. Дизайн Nagios – SSL – NRPE.

NRPE складається з двох частин: плагіна check_nrpe, який знаходиться на Nagios сервері моніторингу та демону NRPE, який працює на віддаленій машині Linux/Unix

Коли Nagios потрібно контролювати ресурс обслуговування віддаленої машини Linux/Unix, Nagios запускає плагін check_nrpe та повідомляє, яку службу потрібно перевірити. check_nrpe зв'язується з демоном NRPE на віддаленому хості через (опціонально) захищене з'єднання SSL.

Демон NRPE запускає відповідний плагін Nagios для перевірки служби чи ресурсу. Результати перевірки служби передаються від демона NRPE назад до плагіна check_nrpe, який потім повертає результати перевірки процесу Nagios

Демон NRPE вимагає, щоб плагіни Nagios були встановлені на віддаленому хості Linux/Unix. Без них демон не міг би нічого контролювати.

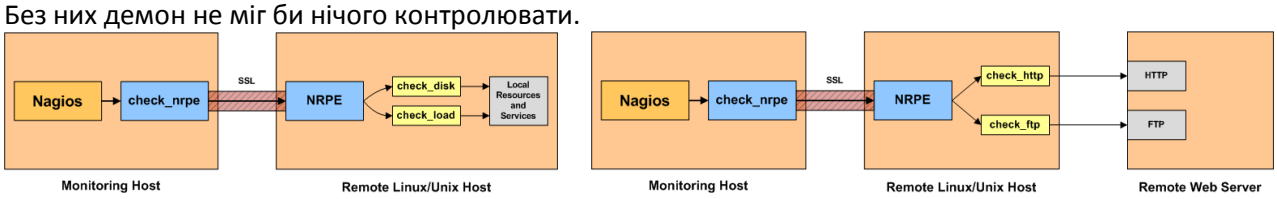


Рис. 7.4. Прямі та непрямі перевірки Nagios – NRPE.

Найбільш простим використанням NRPE є моніторинг «локальних» або «приватних» ресурсів на віддаленій машині Linux/Unix. Сюди входять такі речі, як навантаження ЦП, використання пам'яті, використання підкачки, поточні користувачі, використання диска, стани процесів тощо.

Також можливо використовувати NRPE для опосередкованої перевірки «загальнодоступних» служб і ресурсів віддалених серверів, які можуть бути недоступні безпосередньо з хосту моніторингу. Наприклад, якщо віддалений хост, на якому встановлено демон і плагіни NRPE, може спілкуватися з віддаленим веб-сервером (але хост моніторингу не може). Демон NRPE може бути налаштовано, щоб дозволити опосередковано контролювати віддалений веб-сервер. У цьому випадку демон NRPE по суті діє як проксі.

Nagios сервер. Serv-G-N-2.

Для встановлення Nagios Remote Plugin Executor необхідно отримати лінк актуального релізу пакету на сторінці підтримки https://github.com/NagiosEnterprises/nrpe/releases

На момент написання цього документу це був NRPE Vers 4.1.1 Release. Завантажуємо інсталяційний пакет

```
cd /tmp
wget https://github.com/NagiosEnterprises/nrpe/releases/download/nrpe-4.1.1/nrpe-4.1.1.tar.gz
```

Розпаковуємо завантажений архів

tar -xzvf nrpe-4.1.1.tar.gz

Переходимо в каталог, який був створений під час розпакування, оновлюємо репозиторій, та встановлюємо необхідні для роботи NRPE пакети та виконуємо встановлення NRPE:

cd nrpe-4.1.1

sudo apt-get update

sudo apt-get install -y autoconf automake gcc libc6 libmcrypt-dev make libssl-dev wget openssl

sudo ./configure --enable-command-args --with-ssl-lib=/usr/lib/x86_64-linux-gnu/

sudo make all

sudo cp /tmp/nrpe-4.1.1/src/check_nrpe /usr/local/nagios/libexec/check_nrpe

Виконуємо команду, щоб переконатися, що check_nrpe встановлений:

/usr/local/nagios/libexec/check_nrpe -V

Результат має бути подібний до:

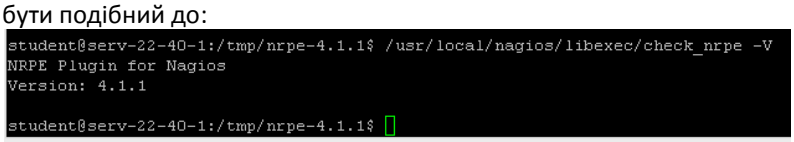


Рис. 7.5. check_nrpe -V на сервері Serv-22-40-2

Додаємо у конфігураційний файл команд ***/usr/local/nagios/etc/objects/commands.cfg*** секцію визначення для встановленої команди

```
# 'check_nrpe' command definition
define command{
        command_name check_nrpe
        command_line $USER1$/check_nrpe -H $HOSTADDRESS$ -c $ARG1$
        }
```

Linux сервер. Serv-G-N-3.

Конфігурування серверної частини завершено, переходимо на Linux-сервер Serv-G-N-3 та повторюємо процедуру встановлення пакету NRPE. Завантажуємо інсталяційний пакет:

cd /tmp

wget https://github.com/NagiosEnterprises/nrpe/releases/download/nrpe-4.1.1/nrpe-4.1.1.tar.gz

Розпаковуємо завантажений архів

tar -xzvf nrpe-4.1.1.tar.gz

Переходимо в каталог, який був створений під час розпакування, оновлюємо репозиторій, та встановлюємо необхідні для роботи NRPE пакети:

cd nrpe-4.1.1

sudo apt-get update

sudo apt-get install -y autoconf automake gcc libc6 libmcrypt-dev make libssl-dev wget openssl

Встановлюємо NRPE:

sudo ./configure --enable-command-args --with-ssl-lib=/usr/lib/x86_64-linux-gnu/

sudo make all

sudo make install

Файли конфігурації.

sudo make install-config

Оновлюємо файл служб /etc/services, що використовується програмами для перекладу зрозумілих людині назв служб у номери портів під час підключення до машини через мережу.

sudo sh -c "echo >> /etc/services"

sudo sh -c "sudo echo '# Nagios services' >> /etc/services"

sudo sh -c "sudo echo 'nrpe 5666/tcp' >> /etc/services"

Це встановлює файли служби або демона.

sudo make install-init

sudo systemctl enable nrpe.service

Якщо на сервері увімкнений брандмауер, налаштовуємо його. Перевірка стану брандмауера:

sudo ufw status.

Порт 5666 використовується NRPE, і його потрібно відкрити на локальному брандмауері.

sudo mkdir -p /etc/ufw/applications.d

sudo sh -c "echo '[NRPE]' > /etc/ufw/applications.d/nagios"

sudo sh -c "echo 'title=Nagios Remote Plugin Executor' >> /etc/ufw/applications.d/nagios"
sudo sh -c "echo 'description=Allows remote execution of Nagios plugins' >> /etc/ufw/applications.d/nagios"
sudo sh -c "echo 'ports=5666/tcp' >> /etc/ufw/applications.d/nagios"
sudo ufw allow NRPE
sudo ufw reload

Оновлюємо файл конфігурації /usr/local/nagios/etc/nrpe.cfg, де змінюємо два рядки:

```
allowed_hosts=127.0.0.1,::1,192.168.40.135
dont_blame_nrpe=1
```

Allowed hosts – рядок адрес, дозволених для NRPE серверів. Крім локальної адреси додаємо через кому адресу Serv-G-N-2 (Nagios серверу).

dont_blame_nrpe визначає, чи дозволить демон NRPE клієнтам вказувати аргументи для команд, які виконуються.

Наступні команди вносять описані вище зміни конфігурації.

sudo sh -c "sed -i '/^allowed_hosts=/s/$/,192.168.22.135/' /usr/local/nagios/etc/nrpe.cfg"
sudo sh -c "sed -i 's/^dont_blame_nrpe =.*/dont_blame_nrpe=1/g' /usr/local/nagios/etc/nrpe.cfg"

Запускаємо службу / демон:

sudo systemctl start nrpe.service

Перевіряємо, що NRPE слухає запити та відповідає на них.

/usr/local/nagios/libexec/check_nrpe -H 127.0.0.1

Результат має бути подібний до:

NRPE v4.1.0

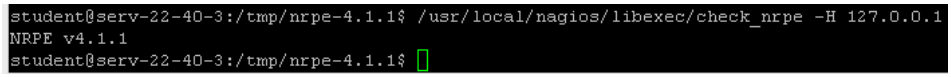


Рис. 7.6. check_nrpe -H 127.0.0.1 на Serv-22-40-3

Для коректної роботи NRPE, необхідно встановити Nagios плагіни на сервер Serv-22-40-3. Плагіни допомагають NRPE виконувати різноманітні перевірки та збирати дані для подальшого відображення в Nagios.

Завантажуємо останню версію Nagios плагінів:

cd /tmp
wget https://nagios-plugins.org/download/nagios-plugins-2.4.9.tar.gz

Розпаковка, конфігурація та встановлення:

tar -xzvf nagios-plugins-2.4.9.tar.gz
cd nagios-plugins-2.4.9
./configure
make
sudo make install

Після цих кроків на сервері Serv-22-40-3 встановлено Nagios плагіни, які можна використовувати для налаштування активних перевірок за допомогою NRPE.

Nagios сервер. Serv-G-N-2.

Переходимо на **Nagios-сервер** та перевіряємо роботу віддаленого виклику процедур перевірок:

/usr/local/nagios/libexec/check_nrpe -H 192.168.40.137 -c check_users
/usr/local/nagios/libexec/check_nrpe -H 192.168.40.137 -c check_load
/usr/local/nagios/libexec/check_nrpe -H 192.168.40.137 -c check_total_procs
/usr/local/nagios/libexec/check_nrpe -H 192.168.40.137 -c check_zombie_procs

Відповідно – завантаження ЦП, кількість підключених користувачів, кількість процесів та кількість «зомбі» процесів.

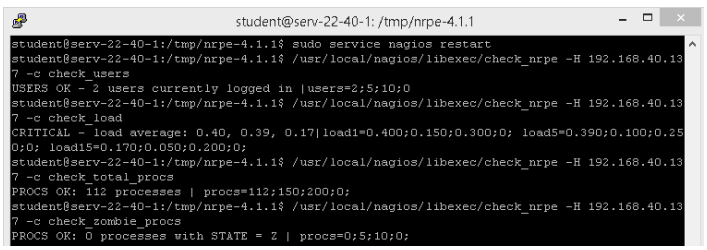


Рис. 7.7. Виклик check_nrpe з Serv-22-40-2 на Serv-22-40-3. Прямі перевірки.

Linux сервер. Serv-G-N-3.

Розглянемо що ж це за команди та де їх можливо визначити. Відкриваємо файл конфігурації /usr/local/nagios/etc/nrpe.cfg та шукаємо рядки визначення описаних команд:

```
command[check_users]=/usr/local/nagios/libexec/check_users -w 5 -c 10
command[check_load]=/usr/local/nagios/libexec/check_load -r -w .15,.10,.05 -c .30,.25,.20
command[check_hda1]=/usr/local/nagios/libexec/check_disk -w 20% -c 10% -p /dev/hda1
command[check_zombie_procs]=/usr/local/nagios/libexec/check_procs -w 5 -c 10 -s Z
command[check_total_procs]=/usr/local/nagios/libexec/check_procs -w 150 -c 200
```

Спробуємо додати визначення команди. Візьмемо за основу нової команди плагін /usr/local/nagios/libexec/check_dns, який вже встановлено на Serv-G-N-3. Плагін дозволяє перевірити доступність домену. Наприклад перевірка домену ztu.edu.ua

/usr/local/nagios/libexec/check_dns -H ztu.edu.ua

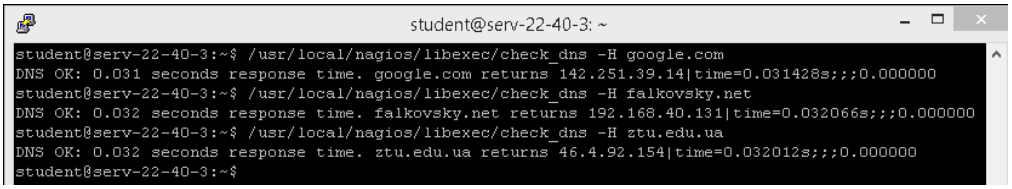
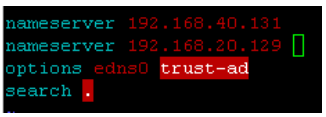


Рис. 7.8. Serv-22-40-3. check_dns по трьом доменним іменам.

Якщо при вірних мережевих налаштуваннях сервер Serv-G-N-3 «не пінгує» домени може знадобитись редагування конфігураційних файлів ***/etc/resolv.conf*** та ***/etc/hosts***. Відкриваємо файл ***/etc/resolv.conf*** для редагування та замінюємо існуючі записи ***nameserver*** записами DNS-серверів, що використовуються у лабораторній роботі:



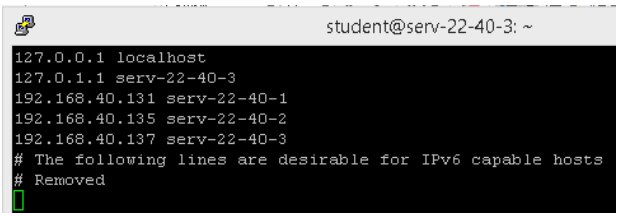
nameserver 192.168.40.131

nameserver 192.168.20.129

Вводимо зміни у файлі ***/etc/resolv.conf*** командою

sudo systemctl restart systemd-resolved

Редагуємо у конфігураційному файлі ***/etc/hosts*** записи серверів:



127.0.0.1 localhost

127.0.1.1 serv-22-40-3

192.168.40.131 serv-22-40-1

192.168.40.135 serv-22-40-2

192.168.40.137 serv-22-40-3

Звичайно можна додати для кожного домену, що нам необхідно перевіряти, окрему команду у файл конфігурації /usr/local/nagios/etc/nrpe.cfg, а можна створити одну, універсальну для будь якого домену. Вона буде виглядати наступним чином:

```
command[check_dns]=/usr/local/nagios/libexec/check_dns -H $ARG1$
```

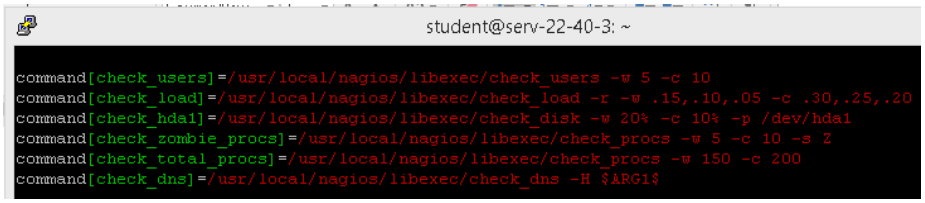


Рис. 7.9. Serv-22-40-3. Додавання check_dns у файл /usr/local/nagios/etc/nrpe.cfg.

Не забуваємо, що після цих налаштувань необхідно перезавантажити службу nrpe

sudo systemctl restart nrpe

Nagios сервер. Serv-G-N-2.

Переходимо на Nagios та виконуємо виклик налаштованої команди. У команді check_nrpe, аргументи передаються після опції -a, і кожен аргумент розділяється пробілом. check_nrpe для домену falkovsky.net

/usr/local/nagios/libexec/check_nrpe -H 192.168.40.137 -c check_dns -a falkovsky.net

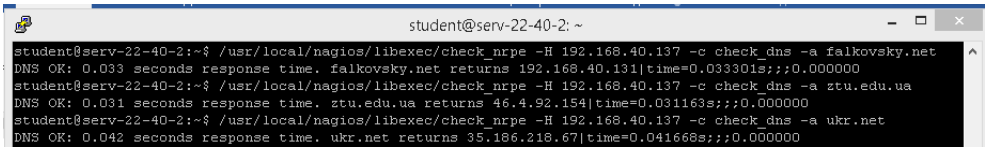


Рис. 7.10. Віддалений виклик check_dns для кількох доменних імен на Serv-22-40-3 з серверу Serv-22-40-2

Додаємо налаштовані команди до конфігураційного файлу сервера /usr/local/nagios/etc/objects/linux/serv-22-40-3.cfg.

```
define service {
    host_name               serv-22-40-3
    use                     generic-service
    service_description     Check users
    check_command           check_nrpe!check_users
    max_check_attempts      5
    check_interval          5
    retry_interval          1
    check_period            24x7
    notification_interval   60
    notification_period     24x7
}
define service {
    host_name               serv-22-40-3
    use                     generic-service
    service_description     Check load CPU
    check_command           check_nrpe!check_load
    max_check_attempts      5
    check_interval          5
    retry_interval          1
    check_period            24x7
    notification_interval   60
    notification_period     24x7
}
define service {
    host_name               serv-22-40-3
    use                     generic-service
    service_description     Check Total procs
    check_command           check_nrpe!check_total_procs
    max_check_attempts      5
    check_interval          5
    retry_interval          1
    check_period            24x7
    notification_interval   60
    notification_period     24x7
}
define service {
    host_name               serv-22-40-3
    use                     generic-service
    service_description     Check Zombie procs
    check_command           check_nrpe!check_zombie_procs
    max_check_attempts      5
    check_interval          5
    retry_interval          1
    check_period            24x7
    notification_interval   60
    notification_period     24x7
}
define service {
    host_name               serv-22-40-3
    use                     generic-service
    service_description     Check domain falkovsky.net
    check_command           check_nrpe!check_dns -a falkovsky.net
    max_check_attempts      5
```

```
    check_interval          5
    retry_interval          1
    check_period            24x7
    notification_interval   60
    notification_period     24x7
}
define service {
    host_name               serv-22-40-3
    use                     generic-service
    service_description     Check domain ztu.edu.ua
    check_command           check_nrpe!check_dns -a ztu.edu.ua
    max_check_attempts      5
    check_interval          5
    retry_interval          1
    check_period            24x7
    notification_interval   60
    notification_period     24x7
}
define service {
    host_name               serv-22-40-3
    use                     generic-service
    service_description     Check domain learn.ztu.edu.ua
    check_command           check_nrpe!check_dns -a learn.ztu.edu.ua
    max_check_attempts      5
    check_interval          5
    retry_interval          1
    check_period            24x7
    notification_interval   60
    notification_period     24x7
}
define service {
    host_name               serv-22-40-3
    use                     generic-service
    service_description     Check domain portal.ztu.edu.ua
    check_command           check_nrpe!check_dns -a portal.ztu.edu.ua
    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

Переглядаємо роботу виконаних налаштувань:

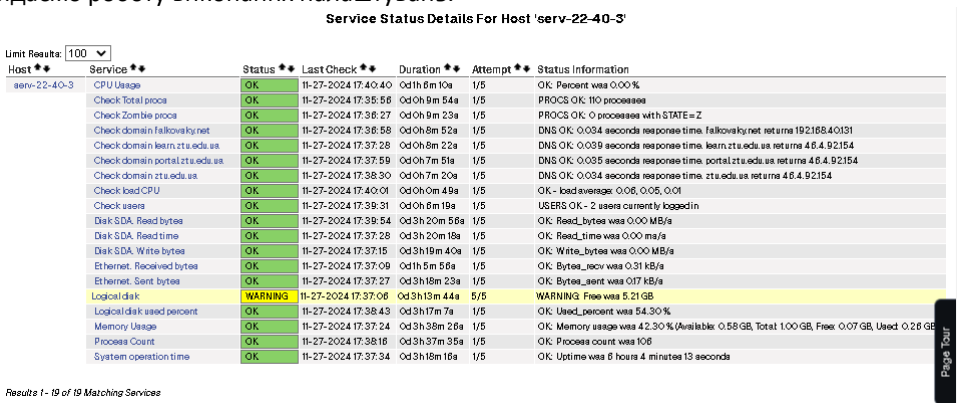


Рис. 7.11. Перегляд сервісів Serv-22-40-3

Змінимо порогові значення Warning та Critical для LogicalDisk:

check_command check_ncpa!-t 'P@ssw0rd2024' -P 5693 -M 'disk/logical/|/free' --warning 10: --critical 5: -u G

на

check_command check_ncpa!-t 'P@ssw0rd2024' -P 5693 -M 'disk/logical/|/free' --warning 4: --critical 2: -u G

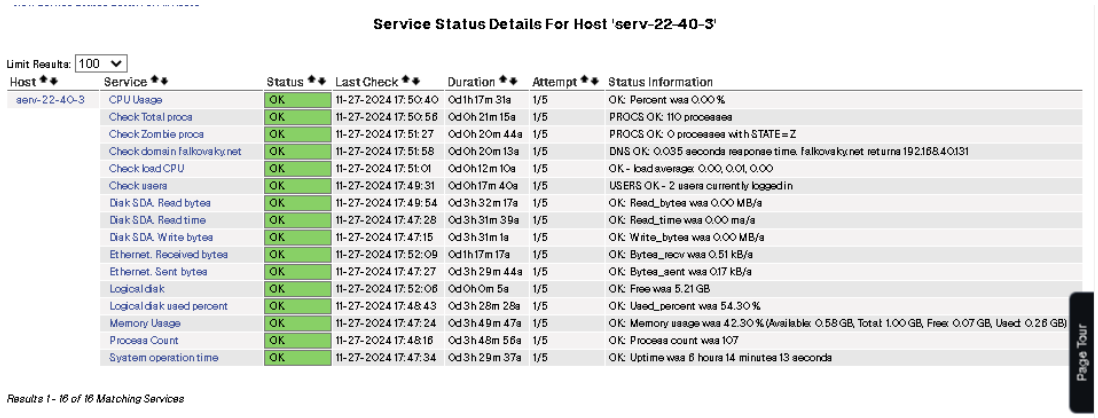
Тимчасово, щоб запобігти можливому ефекту DDoS-атак на доменах ztu.edu.ua, коментами вимикаємо їх налаштований моніторинг, залишаючи лише внутрішній домен.

```
#define service {
#    host_name               serv-22-40-3
#    use                     generic-service
#    service_description     Check domain ztu.edu.ua
#    check_command           check_nrpe!check_dns -a ztu.edu.ua
#    max_check_attempts      5
#    check_interval          5
#    retry_interval          1
#    check_period            24x7
#    notification_interval   60
#    notification_period     24x7
#}
#define service {
#    host_name               serv-22-40-3
#    use                     generic-service
#    service_description     Check domain learn.ztu.edu.ua
#    check_command           check_nrpe!check_dns -a learn.tu.edu.ua
#    max_check_attempts      5
#    check_interval          5
#    retry_interval          1
#    check_period            24x7
#    notification_interval   60
#    notification_period     24x7
#}
#define service {
#    host_name               serv-22-1-3
#    use                     generic-service
#    service_description     Check domain portal.ztu.edu.ua
#    check_command           check_nrpe!check_dns -a portal.tu.edu.ua
#    max_check_attempts      5
#    check_interval          5
#    retry_interval          1
#    check_period            24x7
#    notification_interval   60
#    notification_period     24x7
#}
```

Виконуємо перевірку вірності внесених у конфігурацію змін та перезапускаємо сервіс Nagios:

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

sudo service nagios restart



Service Status Details For Host 'serv-22-40-3'

Limit Results: 100

Host	Service	Status	Last Check	Duration	Attempt	Status Information
serv-22-40-3	CPU Usage	OK	11-27-2024 17:50:40	0d 1h 17m 31s	1/5	OK: Percent was 0.00 %
	Check Total procs	OK	11-27-2024 17:50:56	0d 0h 21m 15s	1/5	PROCS OK: 110 processes
	Check Zombie procs	OK	11-27-2024 17:51:27	0d 0h 20m 44s	1/5	PROCS OK: 0 processes with STATE = Z
	Check domain falkovaky.net	OK	11-27-2024 17:51:58	0d 0h 20m 13s	1/5	DNS OK: 0.035 seconds response time. falkovaky.net returns 192.168.40.131
	Check load CPU	OK	11-27-2024 17:51:01	0d 0h 12m 10s	1/5	OK - load average: 0.00, 0.01, 0.00
	Check users	OK	11-27-2024 17:49:31	0d 0h 17m 40s	1/5	USERS OK - 2 users currently logged in
	Disk SDA. Read bytes	OK	11-27-2024 17:49:54	0d 3h 32m 17s	1/5	OK: Read_bytes was 0.00 MB/s
	Disk SDA. Read time	OK	11-27-2024 17:47:28	0d 3h 31m 39s	1/5	OK: Read_time was 0.00 ms/s
	Disk SDA. Write bytes	OK	11-27-2024 17:47:15	0d 3h 31m 1s	1/5	OK: Write_bytes was 0.00 MB/s
	Ethernet. Received bytes	OK	11-27-2024 17:52:09	0d 1h 17m 17s	1/5	OK: Bytes_recv was 0.51 kB/s
	Ethernet. Sent bytes	OK	11-27-2024 17:47:27	0d 3h 29m 44s	1/5	OK: Bytes_sent was 0.17 kB/s
	Logical disk	OK	11-27-2024 17:52:06	0d 0h 0m 5s	1/5	OK: Free was 5.21 GB
	Logical disk used percent	OK	11-27-2024 17:48:43	0d 3h 28m 28s	1/5	OK: Used_percent was 54.30 %
	Memory Usage	OK	11-27-2024 17:47:24	0d 3h 49m 47s	1/5	OK: Memory usage was 42.30 % (Available: 0.58 GB, Total: 1.00 GB, Free: 0.07 GB, Used: 0.26 GB)
	Process Count	OK	11-27-2024 17:48:16	0d 3h 48m 56s	1/5	OK: Process count was 107
	System operation time	OK	11-27-2024 17:47:34	0d 3h 29m 37s	1/5	OK: Uptime was 6 hours 14 minutes 13 seconds

Results 1 - 16 of 16 Matching Services

Page Tour

Рис. 7.12. Перегляд сервісів Serv-22-40-3

Завдання до лабораторної роботи

1. Виконайте налаштування NRPE на Nagios-сервері Serv-G-N-2.
2. Виконайте налаштування NRPE-серверу на лінукс-сервері Serv-G-N-3.
3. Додайте кілька, на Ваш вибір, параметрів NRPE-моніторингу що виконуються на Serv-G-N-3.

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/

- NRPE - How To Install NRPE v4 From Source

https://support.nagios.com/kb/article/nrpe-how-to-install-nrpe-v4-from-source-515.html

- NRPE - How to install NRPE

https://support.nagios.com/kb/article/nrpe-how-to-install-nrpe-8.html

- Index of /downloads/nagiosxi/agents

https://assets.nagios.com/downloads/nagiosxi/agents/

- Exchange Nagios. NRPE - Nagios Remote Plugin Executor

https://exchange.nagios.org/directory/Addons/Monitoring-Agents/NRPE--2D-Nagios-Remote-Plugin-Executor/details

- Using NSClient++ with check_nrpe

https://nsclient.org/docs/howto/nrpe/

- The Nagios Plugins. Category: Operating Systems

https://exchange.nagios.org/directory/Plugins/Operating-Systems