

Лабораторна робота №6

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

Мета: налаштувати моніторинг базових параметрів Ubuntu та Windows серверів у Nagios 4.X за допомогою NCPA (Nagios Cross-Platform Agent).

Інструменти: гіпервізор VirtualBox, модель комп'ютерної мережі.

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.

Теоретичні відомості

На рис.6.1. 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.

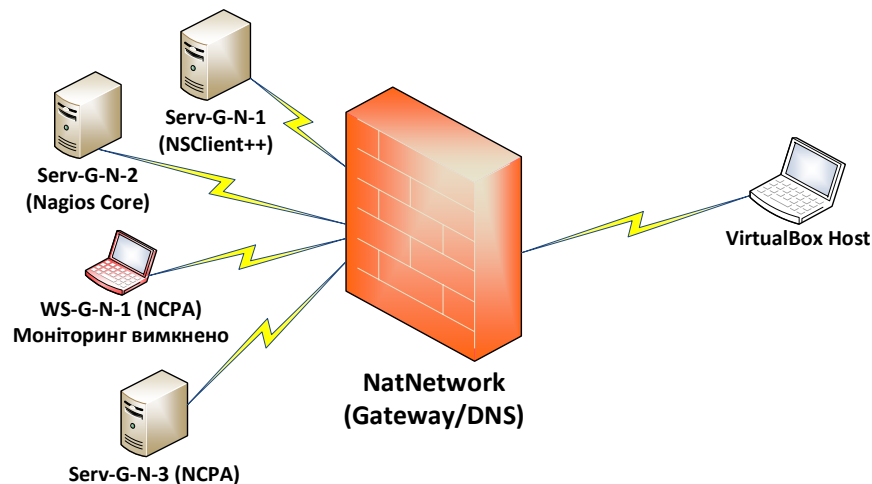


Рис. 6.1. Топологія мережі

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.

Host Status Details For All Host Groups					Service Overview For All Host Groups							
Host	Status	Last Check	Duration	Status Information	Host	Status	Services	Actions	Host	Status	Services	Actions
serv-22-1-1	UP	01-08-2024 20:45:45	3s 27h 25m 12s	PRNG OK - Packet loss = 0%, RTT = 0.79 ms	serv-22-1-2	UP	OK	OK	ws-22-1-1	UP	UNKNOWN	OK
serv-22-1-2	UP	01-08-2024 20:42:25	0s 0h 5m 41s	PRNG OK - Packet loss = 0%, RTT = 0.07 ms	serv-22-1-3	UP	OK	OK	serv-22-1-1	UP	OK	OK
serv-22-1-3	UP	01-08-2024 20:46:19	0s 4h 50m 54s	OK: Agent_version was [3.0.1]								
ws-22-1-1	UP	01-08-2024 20:46:57	0s 0h 5m 9s	OK: Agent_version was [3.0.1]								

Рис. 6.2. 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.

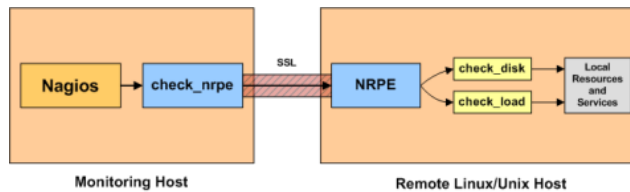


Рис. 6.3. Дизайн Nagios – SSL – NRPE.

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.

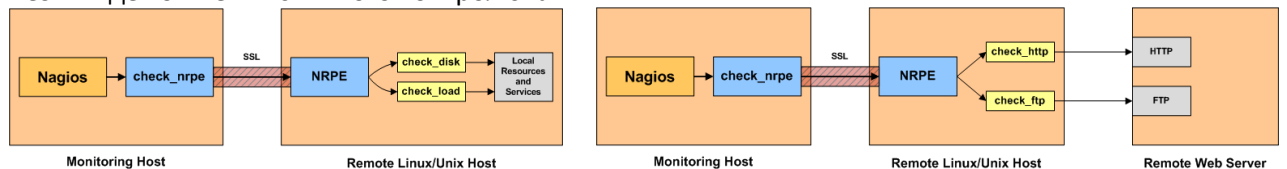


Рис. 6.4. Прямі та непрямі перевірки Nagios – NRPE.

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 4.1.0 Release. Завантажуємо інсталяційний пакет

```
cd /tmp
```

```
wget https://github.com/NagiosEnterprises/nrpe/releases/download/nrpe-4.1.0/nrpe-4.1.0.tar.gz
```

Розпаковуємо завантажений архів

```
tar -xzf nrpe-4.1.0.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-4.1.0
```

```
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/
```

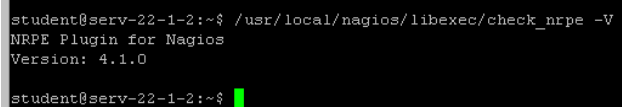
```
sudo make all
```

```
sudo cp /tmp/nrpe-4.1.0/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:



```
student@serv-22-1-2:~$ /usr/local/nagios/libexec/check_nrpe -V
NRPE Plugin for Nagios
Version: 4.1.0
student@serv-22-1-2:~$
```

Рис. 6.5. check_nrpe -V

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-4.1.0/nrpe-4.1.0.tar.gz
```

Розпаковуємо завантажений архів

```
tar -xzf nrpe-4.1.0.tar.gz
```

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

```
cd nrpe-4.1.0
```

```
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
```

Налаштуємо брандмауер. 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,:::1,192.168.22.135
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
```

Для коректної роботи NRPE, необхідно встановити Nagios плагіни на сервер. 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-2.4.8.tar.gz
```

Розпаковка, конфігурація та встановлення:

```
tar -xvzf nagios-plugins-2.4.8.tar.gz
cd nagios-plugins-2.4.8
./configure
make
sudo make install
```

Після цих кроків на сервері 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 192.168.22.137 -c check_users
/usr/local/nagios/libexec/check_nrpe -H 192.168.22.137 -c check_load
/usr/local/nagios/libexec/check_nrpe -H 192.168.22.137 -c check_total_procs
/usr/local/nagios/libexec/check_nrpe -H 192.168.22.137 -c check_zombie_procs
```

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

```
student@serv-22-1-2:~$ /usr/local/nagios/libexec/check_nrpe -H 192.168.22.137 -c check_users
USERS OK - 1 users currently logged in |users=1;5;10;0
student@serv-22-1-2:~$ /usr/local/nagios/libexec/check_nrpe -H 192.168.22.137 -c check_load
OK - load average: 0.00, 0.00, 0.00 |load1=0.000;0.150;0.300;0; load5=0.000;0.100;0.250;0; load15=0.00
0;0.050;0.200;0;
student@serv-22-1-2:~$ /usr/local/nagios/libexec/check_nrpe -H 192.168.22.137 -c check_total_procs
PROCS OK: 107 processes | procs=107;150;200;0;
student@serv-22-1-2:~$ /usr/local/nagios/libexec/check_nrpe -H 192.168.22.137 -c check_zombie_procs
PROCS OK: 0 processes with STATE = Z | procs=0;5;10;0;
student@serv-22-1-2:~$
```

Рис. 6.6. Виклик `check_nrpe` з `Serv-22-1-2` на `Serv-22-1-3`. 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_hdal]=/usr/local/nagios/libexec/check_disk -w 20% -c 10% -p /dev/hdal
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 `google.com`

`/usr/local/nagios/libexec/check_dns -H google.com`

```
student@serv-22-1-3:~$ /usr/local/nagios/libexec/check_dns -H google.com
DNS OK: 0.031 seconds response time. google.com returns 142.251.39.46|time=0.030768s;;0.000000
student@serv-22-1-3:~$ /usr/local/nagios/libexec/check_dns -H falkovsky.net
DNS OK: 0.030 seconds response time. falkovsky.net returns 192.168.22.131|time=0.029540s;;0.000000
student@serv-22-1-3:~$
```

Рис. 6.7. `Serv-22-3`. `check_dns` по двом доменним іменам.

Звичайно можна додати для кожного домену, що нам необхідно перевіряти, свою команду до `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 $ARG1$
```

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 192.168.22.137 -c check_dns -a falkovsky.net`

```
student@serv-22-1-2:~$ /usr/local/nagios/libexec/check_nrpe -H 192.168.22.137 -c check_dns -a falkovsky.net
DNS OK: 0.032 seconds response time. falkovsky.net returns 192.168.22.131|time=0.031616s;;0.000000
student@serv-22-1-2:~$ /usr/local/nagios/libexec/check_nrpe -H 192.168.22.137 -c check_dns -a ztu.edu.ua
DNS OK: 0.029 seconds response time. ztu.edu.ua returns 46.4.92.154|time=0.028954s;;0.000000
student@serv-22-1-2:~$ /usr/local/nagios/libexec/check_nrpe -H 192.168.22.137 -c check_dns -a learn.ztu.edu.ua
DNS OK: 0.039 seconds response time. learn.ztu.edu.ua returns 46.4.92.154|time=0.039419s;;0.000000
student@serv-22-1-2:~$ /usr/local/nagios/libexec/check_nrpe -H 192.168.22.137 -c check_dns -a google.com
DNS OK: 0.037 seconds response time. google.com returns 142.251.39.46|time=0.037009s;;0.000000
student@serv-22-1-2:~$
```

Рис. 6.8. `check_dns` для кількох доменних імен на `Serv-22-1-2`

Додаємо налаштовані команди до конфігураційного файлу сервера `/usr/local/nagios/etc/objects/linux/serv-22-1-3.cfg`.

```
define service {
    host_name          serv-22-1-3
    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-22-1-3
    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-22-1-3
    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-22-1-3
    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-22-1-3
    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-22-1-3
    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-22-1-3
    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-22-1-3
    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:

Service Status Details For Host 'serv-22-1-3'

Host	Service	Status	Last Check	Duration	Attempt	Status Information
serv-22-1-3	CPU Usage	OK	01-28-2024 05:39:25	0d 20h 2m 2s	1/5	OK: Percent was 6.00 %
	Check Total procs	OK	01-28-2024 05:36:58	0d 0h 23m 27s	1/5	PROCS OK: 109 processes
	Check Zombie procs	OK	01-28-2024 05:37:30	0d 0h 22m 55s	1/5	PROCS OK: 0 processes with STATE = Z
	Check domain falkovsky.net	OK	01-28-2024 05:38:02	0d 0h 22m 23s	1/5	DNS OK: 0.031 seconds response time. falkovsky.net returns 192.168.22.131
	Check domain learn.ztu.edu.ua	OK	01-28-2024 05:35:38	0d 0h 9m 47s	1/5	DNS OK: 0.038 seconds response time. learn.ztu.edu.ua returns 46.4.92.154
	Check domain portal.ztu.edu.ua	OK	01-28-2024 05:36:49	0d 0h 8m 36s	1/5	DNS OK: 0.034 seconds response time. portal.ztu.edu.ua returns 46.4.92.154
	Check domain ztu.edu.ua	OK	01-28-2024 05:37:07	0d 0h 18m 18s	1/5	DNS OK: 0.029 seconds response time. ztu.edu.ua returns 46.4.92.154
	Check load CPU	OK	01-28-2024 05:38:34	0d 0h 21m 51s	1/5	OK - load average: 0.01, 0.02, 0.00
	Check users	OK	01-28-2024 05:38:05	0d 0h 27m 20s	1/5	USERS OK - 1 users currently logged in
	Disk SDA_ Read bytes	OK	01-28-2024 05:38:53	1d 9h 1m 32s	1/5	OK: Read_bytes was 0.00 MB/s
	Disk SDA_ Read time	OK	01-28-2024 05:38:47	0d 5h 2m 38s	1/5	OK: Read_time was 0.37 ms/s
	Disk SDA_ Write bytes	OK	01-28-2024 05:39:43	3d 0h 21m 43s	1/5	OK: Write_bytes was 0.01 MB/s
	Disk SDA_ Write time	OK	01-28-2024 05:37:53	0d 5h 3m 32s	1/5	OK: Write_time was 2.76 ms/s
	Enp0s3_ Received bytes	OK	01-28-2024 05:38:32	0d 5h 2m 53s	1/5	OK: Bytes_recv was 0.23 kB/s
	Enp0s3_ Sent bytes	OK	01-28-2024 05:39:43	3d 0h 21m 43s	1/5	OK: Bytes_sent was 0.17 kB/s
	Logical disk	OK	01-28-2024 05:37:39	8d 13h 28m 38s	1/5	OK: Free was 4.94 GB
	Logical disk used percent	OK	01-28-2024 05:37:42	3d 0h 17m 43s	1/5	OK: Used_percent was 56.70 %
	Memory Usage	OK	01-28-2024 05:39:25	8d 18h 1m 2s	1/5	OK: Memory usage was 36.20 % (Available: 0.64 GB, Total: 1.00 GB, Free: 0.11 GB, Used: 0.20 GB)
	Process Count	OK	01-28-2024 05:35:52	8d 18h 0m 13s	1/5	OK: Process count was 106
	System operation time	OK	01-28-2024 05:39:04	1d 9h 1m 22s	1/5	OK: Uptime was 8 days 21 hours 4 minutes 19 seconds

Results 1 - 20 of 20 Matching Services

Рис. 6.9. Перегляд сервісів Serv-22-1-3

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

```

#define service {
#   host_name          serv-22-1-3
#   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-22-1-3
#   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
```

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>