Лабораторна робота №7

Налаштування Nagios моніторингу Windows 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. Налаштуйте взаємодію NSClient++ на сервері Serv-G-N-1 з NRPE на сервері Serv-G-N-2.
2. Налаштуйте моніторинг основних DC сервісів серверу Serv-G-N-1 за допомогою NRPE.

Звіт має містити:

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

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.

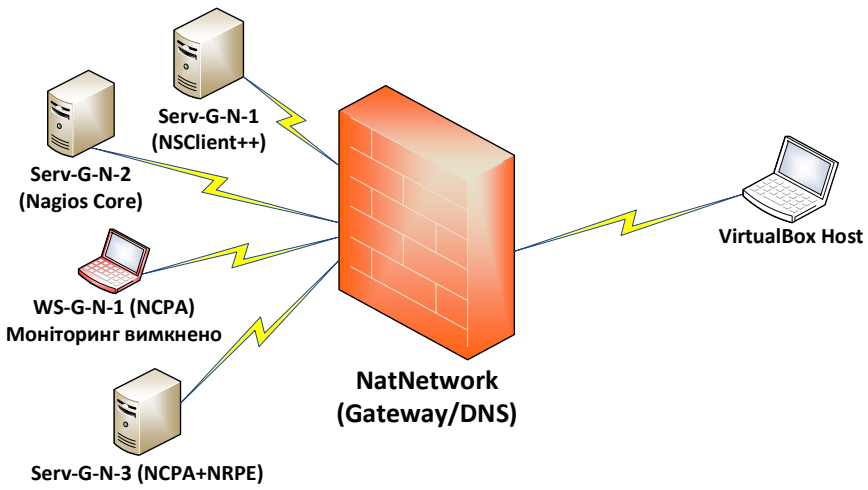


Рис. 7.1. Топологія мережі

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 та NRPE. Налаштовано підключення з хосту NAT Network по протоколу HTTP до систему моніторингу під користувачем nagios.

NRPE розроблений, щоб дозволити запускати плагіни Nagios на віддалених машинах Linux/Unix, але успішно взаємодіє з NSClient++ на Windows.

Windows сервер. Serv-G-N-1.

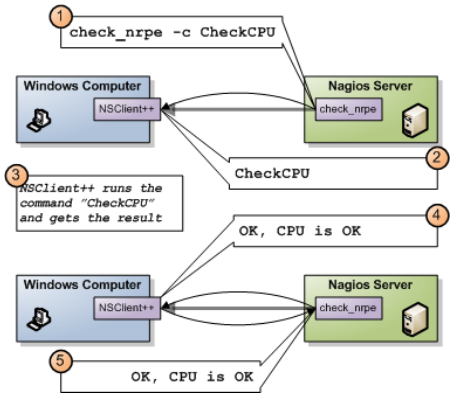


Рис. 7.2. Взаємодія Nagios з NSClient++ на Windows за допомогою check_nrpe.

NRPE працює так само, як SSH або telnet тощо. Він передає команду та очікує на результат. На наведеній вище діаграмі (рис 7.2) відбувається наступне:

1. Nagios виконує check_nrpe з відповідними аргументами.
2. NSClient++ отримує команду для виконання
3. NSClient++ виконає команду та отримає результат у формі,і за бажанням
4. NSClient++ надсилає результат назад до Nagios
5. Nagios отримує результат із check_nrpe (і використовує його, як і будь-який інший плагін)

Отже, по суті, NRPE — це просто транспортний механізм для надсилання результату команди перевірки через мережу.

Сценарій розміщується у каталозі сценаріїв NSClient++. Команда визначається у файлі nsclient.ini та тестується з командного рядка на сервері Nagios:

```
check_winprocess=scripts\check_winprocess.exe $ARG1$
```

Nagios сервер. Serv-G-N-2.

Налаштуємо описаний процес. Сервер Nagios:

/usr/local/nagios/libexec/check_nrpe -H x.x.x.x -c check_winprocess -a '--warn 100 --critical 300' PROCESS OK - 99 process(es)|'processes'=99;100;300

На Nagios сервері (Serv_G_N_2), у каталозі check_nrpe, створюємо DH SSL ключ для «спілкування» NSClient++ з NRPE.

cd /usr/local/nagios/libexec

openssl dhparam -out nrpe_dh_2048.pem 2048

Windows сервер. Serv-G-N-1.

Вміст файлу ключа /usr/local/nagios/libexec/dh_2048.pem зберігаємо на Windows сервері з NSClient++ у файлі C:\Program Files\NSClient++\security\nrpe_dh_2048.pem

Редагуємо файл C:\Program Files\NSClient++\nsclient.ini дозволяючи зовнішні скрипти та додаючи відповідні команди, що описують конфігурацію взаємодії з nrpe

```
[/settings/NRPE/server]
ssl options =
allow arguments = true
allow nasty characters = true
use ssl = 1
port = 5666
extended response = 1
dh = C:\Program Files\NSClient++\security\nrpe_dh_2048.pem
[/modules]
NRPEServer = enabled
CheckSystem=enabled
CheckDisk=enabled
CheckExternalScripts=enabled
CheckEventLog = enabled
CheckHelpers = disabled
CheckNSCP = disabled
NSClientServer = enabled
```

Перезавантажуємо сервіс “NSClient++ Monitoring Agent”, завершуючи налаштування Serv-G-N-1.

Nagios сервер. Serv-G-N-2.

Перевіряємо взаємодію NRPE на Nagios з NSClient++ на Serv-G-N-1. Ключ «-2» додається для ігнорування сумісності версій клієнта та сервера.

/usr/local/nagios/libexec/check_nrpe -H 192.168.22.131 -2

/usr/local/nagios/libexec/check_nrpe -H 192.168.22.131 -2 -c check_drivesize

/usr/local/nagios/libexec/check_nrpe -H 192.168.22.131 -2 -c CheckCPU -a warn=80 crit=90 time=20m time=10s time=4

```
student@serv-22-1-2:/usr/local/nagios/libexec$ /usr/local/nagios/libexec/check_nrpe -H 192.168.22.137
NRPE v4.1.0
student@serv-22-1-2:/usr/local/nagios/libexec$ /usr/local/nagios/libexec/check_nrpe -H 192.168.22.131 -2
I (0.5.2.39 2018-02-04) seem to be doing fine...
student@serv-22-1-2:/usr/local/nagios/libexec$ /usr/local/nagios/libexec/check_nrpe -H 192.168.22.131 -2 -c check_drivesize
CRITICAL D:\: 51.02MB/51.02MB used, Z:\: 276.28GB/315.068GB used|'C:\ used'=11.15491GB;39.56952;44.51571;0;49.46191 'C:\ used
 %'=23%;80;90;0;100 'D:\ used'=51.01953MB;40.81562;45.91757;0;51.01953 'D:\ used %'=100%;80;90;0;100 'Z:\ used'=276.28036GB;2
52.05468;283.56152;0;315.06835 'Z:\ used %'=88%;80;90;0;100
student@serv-22-1-2:/usr/local/nagios/libexec$ /usr/local/nagios/libexec/check_nrpe -H 192.168.22.131 -2 -c CheckCPU -a warn=
80 crit=90 time=20m time=10s time=4
OK: CPU load is ok.|'total 20m'=6%;80;90 'total 10s'=3%;80;90 'total 4'=2%;80;90
student@serv-22-1-2:/usr/local/nagios/libexec$
```

Рис. 7.3. Перевірка відгуку NSClient++ на Serv_22_1_1 на запити NRPE Nagios сервера.

Повторимо основи роботи контролеру домену. Основні служби, які відповідають за роботу DC, це служби Active Directory та DNS:

- **Active Directory Domain Services (AD DS)** є основною службою, яка дозволяє серверу виконувати роль контролера домену. Вона управляє базою даних директорії, реплікацією даних між контролерами домену та забезпечує аутентифікацію та авторизацію користувачів у домені.
- **DNS Server** важлива для роботи Active Directory, оскільки AD використовує DNS для резолюції імен комп'ютерів в IP-адреси та знаходження різних служб у домені.
- **Netlogon** використовується для реєстрації та аутентифікації користувачів у домені та допомагає у виконанні процедур реплікації AD між контролерами домену.
- **Kerberos Key Distribution Center (KDC)** дозволяє забезпечити механізм аутентифікації Kerberos у домені.
- **Intersite Messaging** відповідає за обмін повідомленнями між сайтами AD.

Зазвичай, ці служби автоматично запускаються під час встановлення ролі контролера домену. У разі проблем з роботою DC рекомендується перевірити статус. Виконаємо ці перевірки для описаних служб:

/usr/local/nagios/libexec/check_nrpe -H 192.168.22.131 -c check_service -a "service=NTDS" "ok=state='running'" "critical=state='stopped'"

/usr/local/nagios/libexec/check_nrpe -H 192.168.22.131 -c check_service -a "service=DNS" "ok=state='running'" "critical=state='stopped'"

/usr/local/nagios/libexec/check_nrpe -H 192.168.22.131 -c check_service -a "service=Netlogon" "ok=state='running'" "critical=state='stopped'"

/usr/local/nagios/libexec/check_nrpe -H 192.168.22.131 -c check_service -a "service=KDC" "ok=state='running'" "critical=state='stopped'"

/usr/local/nagios/libexec/check_nrpe -H 192.168.22.131 -c check_service -a "service=IsmServ" "ok=state='running'" "critical=state='stopped'"

```
student@serv-22-1-2:~$ /usr/local/nagios/libexec/check_nrpe -H 192.168.22.131 -2 -c check_service
-a "service=NTDS" "ok=state='running'" "critical=state='stopped'"
OK: All 1 service(s) are ok.|'NTDS'=4;0;0
student@serv-22-1-2:~$ /usr/local/nagios/libexec/check_nrpe -H 192.168.22.131 -2 -c check_service
-a "service=DNS" "ok=state='running'" "critical=state='stopped'"
OK: All 1 service(s) are ok.|'DNS'=4;0;0
student@serv-22-1-2:~$ /usr/local/nagios/libexec/check_nrpe -H 192.168.22.131 -2 -c check_service
-a "service=Netlogon" "ok=state='running'" "critical=state='stopped'"
OK: All 1 service(s) are ok.|'Netlogon'=4;0;0
student@serv-22-1-2:~$ /usr/local/nagios/libexec/check_nrpe -H 192.168.22.131 -2 -c check_service
-a "service=KDC" "ok=state='running'" "critical=state='stopped'"
OK: All 1 service(s) are ok.|'KDC'=4;0;0
student@serv-22-1-2:~$ /usr/local/nagios/libexec/check_nrpe -H 192.168.22.131 -2 -c check_service
-a "service=IsmServ" "ok=state='running'" "critical=state='stopped'"
OK: All 1 service(s) are ok.|'IsmServ'=4;0;0
student@serv-22-1-2:~$
```

Рис. 7.4. Перевірка служб DC за допомогою NSClient++ за запитами NRPE Nagios сервера.

Додаємо налаштовані команди до конфігураційного файлу сервера

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

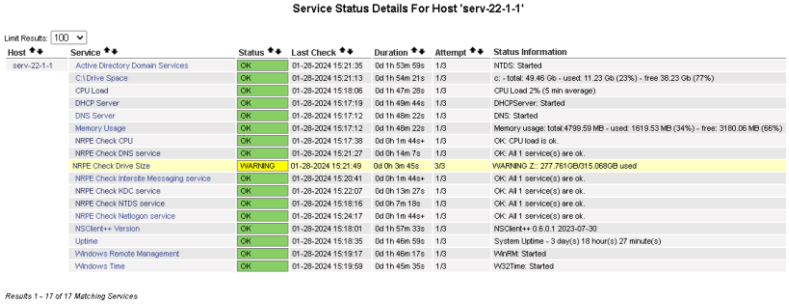
```
    define service {
        use                     generic-service
        host_name               serv-22-1-1
        service_description     NRPE Check Drive Size
        check_command           check_nrpe!check_drivesize
    }
    define service {
        use                     generic-service
        host_name               serv-22-1-1
        service_description     NRPE Check CPU
        check_command           check_nrpe!checkcpu -a warn=80 crit=90 time=20m time=10s time=4
    }
    define service {
        use                     generic-service
        host_name               serv-22-1-1
        service_description     NRPE Check NTDS service
        check_command           check_nrpe!check_service -a "service=NTDS" "ok=state='running'"
"critical=state='stopped'"
    }
    define service {
        use                     generic-service
        host_name               serv-22-1-1
        service_description     NRPE Check DNS service
        check_command           check_nrpe!check_service -a "service=DNS" "ok=state='running'"
"critical=state='stopped'"
    }
    define service {
        use                     generic-service
        host_name               serv-22-1-1
        service_description     NRPE Check KDC service
        check_command           check_nrpe!check_service -a "service=KDC" "ok=state='running'"
"critical=state='stopped'"
    }
    define service {
        use                     generic-service
        host_name               serv-22-1-1
        service_description     NRPE Check Intersite Messaging service
        check_command           check_nrpe!check_service -a "service=IsmServ" "ok=state='running'"
"critical=state='stopped'"
    }
    define service {
        use                     generic-service
        host_name               serv-22-1-1
        service_description     NRPE Check Netlogon service
        check_command           check_nrpe!check_service -a "service=Netlogon" "ok=state='running'"
"critical=state='stopped'"
    }
```

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-22-1-1'

Limit Results: 100

Host	Service	Status	Last Check	Duration	Attempt	Status Information
serv-22-1-1	Active Directory Domain Services	OK	01-28-2024 15:21:35	0d 1h 53m 59s	1/3	NTDS: Started
	C:\ Drive Space	OK	01-28-2024 15:21:13	0d 1h 54m 21s	1/3	c: - total: 49.46 Gb - used: 11.23 Gb (23%) - free 38.23 Gb (77%)
	CPU Load	OK	01-28-2024 15:18:06	0d 1h 47m 28s	1/3	CPU Load 2% (5 min average)
	DHCP Server	OK	01-28-2024 15:17:19	0d 1h 49m 44s	1/3	DHCPServer: Started
	DNS Server	OK	01-28-2024 15:17:12	0d 1h 49m 22s	1/3	DNS: Started
	Memory Usage	OK	01-28-2024 15:17:12	0d 1h 49m 22s	1/3	Memory usage: total:4799.59 MB - used: 1619.53 MB (34%) - free: 3180.06 MB (66%)
	NRPE Check CPU	OK	01-28-2024 15:17:38	0d 0h 1m 44s+	1/3	OK: CPU load is ok.
	NRPE Check DNS service	OK	01-28-2024 15:21:27	0d 0h 14m 7s	1/3	OK: All 1 service(s) are ok.
	NRPE Check Drive Size	WARNING	01-28-2024 15:21:49	0d 0h 3m 45s	3/3	WARNING Z:: 277.761GB/315.068GB used
	NRPE Check Intersite Messaging service	OK	01-28-2024 15:20:41	0d 0h 1m 44s+	1/3	OK: All 1 service(s) are ok.
	NRPE Check KDC service	OK	01-28-2024 15:22:07	0d 0h 1m 27s	1/3	OK: All 1 service(s) are ok.
	NRPE Check NTDS service	OK	01-28-2024 15:18:16	0d 0h 7m 18s	1/3	OK: All 1 service(s) are ok.
	NRPE Check Netlogon service	OK	01-28-2024 15:24:17	0d 0h 1m 44s+	1/3	OK: All 1 service(s) are ok.
	NSClient++ Version	OK	01-28-2024 15:18:01	0d 1h 57m 33s	1/3	NSClient++ 0.6.0.1 2023-07-30
	Uptime	OK	01-28-2024 15:18:35	0d 1h 46m 59s	1/3	System Uptime - 3 day(s) 18 hour(s) 27 minute(s)
	Windows Remote Management	OK	01-28-2024 15:19:17	0d 1h 46m 17s	1/3	WinRM: Started
	Windows Time	OK	01-28-2024 15:19:59	0d 1h 45m 35s	1/3	W32Time: Started

Results 1 - 17 of 17 Matching Services

Рис. 7.5. Перегляд сервісів Serv-22-1-1

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