## Лабораторна робота №5

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

**Мета**: формування практичних навичок налаштування пасивного моніторингу Windows робочих станцій у системі Nagios 4.х за допомогою агента NCPA (Nagios Cross-Platform Agent), а також організації хостів у тематичні групи для покращення управління та аналізу стану інфраструктури. **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. Крім того, до сервера Serv-G-N-2 налаштовано SSH доступ через NAT Network для VirtualBox Host.



Рис. 5.1. 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++. Налаштовано підключення з хосту NAT Network по протоколу HTTP до систему моніторингу під користувачем nagios.



### Puc. 5.2. Hosts, Host Groups, Service Status Details for Serv-22-40-1.

Встановимо та налаштуємо NCPA на робочій станції WS-G-N-1. Завантажуємо останню стабільну версію агента для Windows 64-bit з офіційного сайту <u>https://www.nagios.org/ncpa/#downloads</u>. На момент написання цього документу це версія 3.1.1.

NCPA Setup	– 🗆 X	NCPA Setup	- 🗆 X	Listener Configuration	- 🗆 X
<u>N</u> agios	Welcome to NCPA Setup	Windows Version - 3.1.1	<u>N</u> agios'	Nagios Cross-Platform Agent (NCPA) Windows Version - 3.1.1	<u>N</u> agios'
	Setup will gude you through the installation of NCPA. It is recommended that you close all other applications before starting Setup. This will make the lookale to uddate relevant system files without having to reboot your computer. Click Next to continue.	License Agreement Nagios Software License Terms and Conditions PLASE READ THIS AGREEMENT CARFULLY BEFORE PURCHASIN SOFTWARE. SP FURCHASING LUSING HAGIOSE DHTERMISSES' SIGUPY YOLA ASSENT TO THIS AGREEMENT, IF YOU ARE ACT AGREEMENT, DIE HAUF OF THE THOTT, JE YOU ARE ACT AGREEMENT, THEN YOU MUST NOT PURCHASE OR LISE INAGIOS S This Software License Terms and Conditions Agreement ("Agreem agreement between Nagios Entreprises" Nagios Software License 1.3	C OR USENIX ONGOIS SOFTWARE, YOU SOFTWARE, YOU OF USER IF ON HIS OF USER IF ON HIS THE TEXES OF THIS OFTWARE. HI's a legal and the purchaser or v	Set General, API and Listener configuration options. General Settings Log Level warring API Configuration Token P@sex/0rd2024 The token used for API access, active checks, and loggin Listener Configuration Bind Port 5693 SSI. Version	g into the web GUL. Iterer Configuration TLSv1_2 V
	Next > Cancel	Nagios Enterprises, LLC	I Agree Cancel	Nagios Enterprises, ILC	Next > Cancel

Рис. 5.3. Інсталяція NCPA v.3.1.1 на робочій станції WS-22-40-1.

Запускаємо завантажений файл ncpa-latest.exe та погоджуємося з ліцензійною угодою.

На третьому екрані показані конфігурації для WEB API доступу. Єдине налаштування, яке тут потрібно, це Token – ключ, який сервер Nagios використовуватиме для автентифікації за допомогою NCPA. Я встановив у якості ключа типову послідовність символів P@ssw0rd2024.

IP-адреса прив'язки 0.0.0.0 означає, що NCPA прослуховуватиме всі адреси Ipv4 на машині Windows. Використовується стандартний порт 5693.

Passive Configuration	– 🗆 X	Passive Checks Configuration	- 🗆 X	NCPA Setup	- 🗆 🗙
Nagios Cross-Platform Agent (NCPA) Windows Version - 3.1.1		Nagios Cross-Platform Agent (NCPA) Windows Version - 3.1.1	<u>N</u> agios	Choose Users Choose for which users you want to install NCPA.	<u>N</u> agios
Set configuration for the passive service. This servi to Nagios via NRDP or other protocols in the future. NRDP Configuration	ce handles sending passive check results Advanced Passive Configuration	Passive Check Definitions Configuration will be saved in [etc/ncpa.cfg.d/nrdp.cfg] auto You can leave it blank for no pre-setup checks. To use \ you r	matically when using this form. must escape by doing \\.	Select whether you want to install NCPA only for yourself or t Click Next to continue.	or all users of this computer.
Send passive checks over NRDP           URL         http://192.168-40.135/haglos/           NRDP Token         P@ssn0rd2024           Hostname         [V5-22-40-1]           If no hostname is provided, RCPA will	Check Interval 300 The default check interval in seconds. This is how often the passive checks will be sert.	Filest their - The is to story "pending deed" status in tage 2405TMA4581   MST	ice ^ // // // // // // // // // // // // /	Instal for anyone using this computer     Instal just for me	
Naglos Enterprises, LLC	< Back Next > Cancel	L Nagios Enterprises, LLC	Next > Cancel	Nagios Enterprises, LLC < Back	Next > Cancel

Рис. 5.4. Інсталяція NCPA v.3.1.1 на робочій станції WS-22-40-1.

Екран конфігурації для пасивних перевірок. Встановлюємо прапорець "Send passive checks over NRDP", щоб увімкнути пасивні перевірки та налаштовуємо параметри NRDP:

- URL. URL-адреса хосту Nagios, що приймає результати пасивної перевірки. У моєму випадку <a href="http://192.168.40.135/nagios/">http://192.168.40.135/nagios/</a>
- NRDP Token. Ключ, що використовується під час передачі пасивних перевірок NCPA до Nagios, щоб NRDP прийняв чек. Він може відрізнятися від ключа, що встановлений для API доступу, але враховуючи, що це навчальний стенд, я встановив у якості ключа типову послідовність символів P@ssw0rd2024
- Hostname. Ім'я хоста, якому належать пасивні перевірки на сервері Nagios WS-22-40-1

Продовження інсталяції пасивних перевірок. На екрані запропоновано стандартні пасивні перевірки служб, що будуть виконуватися та надсилатися на сервер Nagios. За потреби їх можна змінити.

NCPA Setup	- 🗆 🗙	NCPA Setup	- 🗆 🗙	NCPA Setup	- 🗆 X
Choose Install Location Choose the folder in which to install NCPA.	<u>N</u> agios'	Installing Please wait while NCPA is being installed.	<u>N</u> agios <sup>°</sup>	<u>N</u> agios	Completing NCPA Setup
Setup will install NCPA in the following folder. To install in a different f select another folder. Click Install to start the installation.	older, dick Browse and	Extract: win32evtlog.pyd 100%			NCPA has been installed on your computer. Click Finish to dose Setup.
		Extract: psutil_windows.pyd 100% Extract: pyexpat.pyd 100% Extract: pswintypes312.dl 100% Extract: select.pyd 100%	^		
Destination Folder CNPzogram Files Naglos NGP2	Browse	Extract: servicemanager.pyd 100% Extract: solite3.dll 100% Extract: unicodedata.pyd 100% Extract: win32abi.pvd 100%			
Space required: 44.0 MB Space available: 39.3 GB		Extract: win32event.pyd 100% Extract: win32evtlog.pyd 100%	~		View NCPA website and documentation
< Back In	stal Cancel	< I	Back Next > Cancel		< Back Finish Cancel

#### Рис. 5.5. Інсталяція NCPA v.3.1.1 на робочій станції WS-22-40-1.

На наступних кроках можливо змінити місце встановлення агенту NCPA та успішно завершити інсталяцію.

Перевіряємо стан служби Nagios Cross-Platform Agent.

<ul> <li>Зберігання</li> <li>Керугання дисками</li> <li>Служби та застосунки</li> <li>Services</li> <li>WMI Control</li> </ul> Nagios Cross-Platform	Microsoft Storage Spaces S Host service     Microsoft Update Health Se Maintains U     Microsoft Update Health Se Maintains U     Microsoft Unders MSR Se     Okater met     Natural Authentication Signal aggi     Natural Authentication Signal aggi     Microsoft Mathematication Signal aggi     Natural Authentication Maintains a     Agent Properties (Local Computer)	Running Running	Manual Automatic (Delayed Manual (Trigger Start) Automatic Manual (Trigger Start) Disabled Automatic Nagios Cross-	Network Service Local System Local Service Local System Local System Local System Platform Agent	Microsoft Storage Spaces S Microsoft Update Health Se Microsoft Windows SMS Ro Nagios Cross-Platform Agent Natural Authentication Properties (Local Computer)	Host se Mainta Routes Signal	ervice ins U Running mes Running aggr lagios Cross-Platforn	Manual Automatic (Delayed Manual (Trigger Start) Automatic Manual (Trigger Start) m Agent Properties (Local G	Network Service Local System Local Service Local System Local System
General Log On Red	covery Dependencies		General Log	On Recovery	Dependencies		General Log On Re	ecovery Dependencies	
Service name: NC	PA		Log on as:				Select the computer's	s response if this service fails.	Help me set up recovervi
Display name: Na	gios Cross-Platform Agent		Local System	stem account			First failure:	Restart the Service	~
Description:		< >	Allow	service to interact	with desktop		Second failure:	Restart the Service	~
Path to executable:			O This acco	ount:	Browse		Subsequent failures:	Restart the Service	~
"C:\Program Files\Nag	gios\NCPA\ncpa.exe"		Password	±			Reset fail count after	0 days	
Startup type: Au	tomatic	$\sim$	Confirm p	assword:			Restart service after:	1 minut	es
							Enable actions for	stops with errors. Restar	t Computer Options
Service status: Ru	nning						Run program		

Рис. 5.6. Запуск та налаштування служби NCPA на робочій станції WS-22-40-1.

На рис.5.6 служба NCPA працює, налаштована на автоматичний запуск та змінено дії відновлення служби закладки Recovery на перезапуск сервісу.

Наступний крок перевірки – Windows Defender Firewall. Для роботи NCPA має бути правило, що дозволяє Inbound TCP 5693. Поточна версія NCPA створює ці правила автоматично.

🔗 Windows Defender Firewall with	h Advanced Security			NCPA – вла Genera	стивості	Programs	and Services Remote	Computers
Файл Дія Вигляд Довідка				Protocols a	nd Ports S	Scope	Advanced Local Principals	Remote Users
				Protocol	s and ports			
				1	Protocol type	e:	TCP	$\sim$
Windows Defender Firewall with	Inbound Rules				Protocol num	nber:	6 🌲	
Cuthound Rules	Name	Group	Profile ^		Local port:		Specific Ports	~
Connection Security Rules	🚱 NCPA		All				5693	-
Monitoring	@{Microsoft.DesktopAppInstaller_1.0.302	@{Microsoft.DesktopAppIns	Doma				Example: 80, 443, 5000-5010	
¢	🔮 @{microsoft.windowscommunicationsa	@{microsoft.windowscom	All		Remote port		All Ports	~
	🔮 @{Microsoft.WindowsStore_11910.1002.5	@{Microsoft.WindowsStore	All				Example: 80, 443, 5000-5010	

Рис. 5.7. Windows Defender Firewall. Правило NCPA на робочій станції WS-22-40-1.

Остання перевірка – підключаємося до NCPA на станції WS-G-N-1 з серверу Serv-G-N-1. У нашому випадку - <u>https://192.168.40.146:5693.</u>

Можливо підключитися з власного ПК, налаштувавши у NAT Network відповідний Port Forwarding.



Рис. 5.8. Налаштування дозволу підключення («довіреного» сайту) до <u>http://192.168.40.146</u> у IE на контролері домену Serv-22-40-1.

← → M https://192.168.40.146.5693/logi	n 👻 😵 Certificate error 🖒	Search	C C PA	ps://192.168.40.146.565 2A × 1	93/gui/ ✔ Checks (	<ul> <li>♥ Ce</li> <li>Live Data</li> </ul>	atificate error C Search	Admin	ှာ - ကြ ⊕ Help	□ × } ☆ 袋 <sup>©</sup> ひ Logout
NCPA			Check St	atistics			NCPA Agent Info	rmation		
		1	Check Re See Live Sta	ts >	Last 30 days	)	NCPA Version Bundled Python	3.1.1 3.12.6 (tags/v Sep 6 2024, 2 v.1940 64 bit	/3.12.6:a4a2 0:11:23) [M (AMD64)]	d2b, SC
	Web GUI Log In						Bundled OpenSSL Bundled zlib Agent Uptime	OpenSSL 3.0. 1.3.1 0:10:36	15 3 Sep 202	:4
		۴					System Informat	ion WS-22-40-1		
							System	Windows 10 10.0.19044		

Рис. 5.9. Web GUI NCPA WS-22-40-1. Налаштування дозволу та підключення на Serv-22-40-1.

На рис. 5.8 та 5.9 показані налаштування «довіреного сайту» у браузері серверу та підключення у ньому до Web GUI. У якості ключа доступу вказується заданий при інсталяції ключ для API доступу, вікно Listener Configuration інсталяції NCPA. «Підгледіти» цей пароль можна переглянувши на хості, де проінстальовано NCPA у файлі \etc\ncpa.cfg. Для підключення через WEB використовується значення community\_string з секції [api]

Переходимо до конфігурування Nagios для взаємодії з NCPA. По аналогії взаємодії з NSClient++, де використовується команда **check\_nt** 

/usr/local/nagios/libexec/check\_nt -H 192.168.40.131 -p 12489 -s P@ssw0rd2024 -v CPULOAD -I 5,80,90

для взаємодії з NCPA використовується команда **check\_ncpa**. Синтаксис дуже схожий:

/usr/local/nagios/libexec/check\_ncpa.py -H 192.168.40.146 -p 5693 -t P@ssw0rd2024 -M cpu/percent -w 80 -c 90 q 'aggregate=avg'

Поточна версія Nagios Core при розгортанні не встановлює цю команду чи її аналоги на сервер. Налаштовуємо взаємодію з NCPA, як описано у <u>Getting Started</u> Завантажуємо скрипт активних перевірок check ncpa.py

#### cd /usr/local/nagios/libexec

### wget https://raw.githubusercontent.com/NagiosEnterprises/ncpa/master/client/check\_ncpa.py

Надаємо файлу скрипта відповідні дозволи для виконання:

chmod +x /usr/local/nagios/libexec/check\_ncpa.py



Puc. 5.10. Serv-22-40-2. Завантаження, зміна рядка повноважень check\_ncpa.py, невдала спроба виконання скрипта і перегляд встановленої версії Phyton.

Помилка при виконанні скрипта /usr/local/nagios/libexec/check\_ncpa.py

/usr/bin/env: 'python': No such file or directory

вказує на відсутність інтерпретатора Python. Скрипт використовує Python для виконання, але на Serv-G-N-2 цей інтерпретатор встановлено під назвою python3, про що говорить перевірка версії Phyton.

Редагуємо перший рядок скрипту check\_ncpa.py на відповідний інтерпретатор Python, змінюючи рядок #!/usr/bin/env python на #!/usr/bin/env python3.



Рис. 5.11. Serv-22-40-2. Редагування назви інтерпретатора Python у скрипті check\_ncpa.py.

Створюємо команду check\_ncpa у конфігураційному файлі для Nagios Core. Зазвичай це файл /usr/local/nagios/etc/objects/commands.cfg

Відкриваємо його для редагування. Файл не порожній — у ньому записано доволі багато команд. Додаємо секцію визначення команди check ncpa:



Наведена секція дозволяє передати більшість аргументів за допомогою \$ARG1\$, роблячи команду динамічнішою.



Рис. 5.12. Додавання секції команди check\_ncpa у файл commands.cfg та перевірка взаємодії з NCPA на станції WS-22-40-1

Кожна зміна конфігурації системи повинна завершуватися перевіркою вірності внесених у конфігурацію змін та перезапуском сервісу Nagios. Перезапуск лише при відсутності помилок 🙂

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

#### sudo service nagios restart

Одразу перевіряємо взаємодію з NCPA, що встановлений на робочій станції WS-G-N-1. Команду check\_ncpa, що описана раніше, замінюємо на ім'я встановленого скрипта check\_ncpa.py:

/usr/local/nagios/libexec/check\_ncpa.py -H 192.168.22.146 -p 5693 -t P@ssw0rd2024 -M cpu/percent -w 80 - c 90 -q 'aggregate=avg'

Редагуємо конфігураційний файл /usr/local/nagios/etc/objects/hostgroups.cfg, де описана група cepвepiв Windows Servers. Додаємо ще одну групу об'єктів моніторингу – робочих станцій Windows, куди включимо робочу станцію WS-G-N-1.

```
define hostgroup {
    hostgroup_name win-workstations
    alias Windows WorkStations
```

У каталозі /usr/local/nagios/etc/objects/workstation створюємо конфігураційний файл для робочої станції /usr/local/nagios/etc/objects/workstation/ws-22-40-1.cfg

de	fine host {	
	host_name	WS-22-40-1
	address	192.168.40.146
	hostgroups	win-workstations
	check_command	check_ncpa!-t 'P@ssw0rd2024' -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
}		
de	fine service {	
	host_name	WS-22-40-1
	service_description	CPU Usage
'aggrega	check_command ate=avg'	check_ncpa!-t 'P@sswOrd2024' -P 5693 -M cpu/percent -w 20 -c 40 -q
	max_check_attempts	5
	check_interval	5
	retry_interval	1
	check_period	24x7
	notification_interval	60
	notification_period	24x7
}		
de	fine service {	
	host_name	WS-22-40-1
	service_description	Memory Usage
	check_command	check_ncpa!-t 'P@ssw0rd2024' -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
}		
de	fine service {	
	host_name	WS-22-40-1
	service_description	Process Count
	check_command	check_ncpa!-t 'P@ssw0rd2024' -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
1		

Це типовий конфігураційний файл для NCPA моніторингу Windows станції — приклад з комплекту поставки NCPA. Щоб переглянути всі доступні параметри моніторингу для цієї станції з консолі серверу моніторингу, використовується команда:

### /usr/local/nagios/libexec/check\_ncpa.py -H 192.168.40.146 -t P@ssw0rd2024 -p 5693 --list

Також можливий перегляд налаштованих параметрів моніторингу через GUI при підключенні до NCPA на станції WS-G-N-1 з серверу Serv-G-N-1.

На рис.5.13 показаний вигляд закладки Checks при підключенні до NCPA робочої станції.

	S	erv-22-40-1 [Ru	nning] - Oracle VM VirtualBox		
e Machine View Input Devices	Help				_
🗧 🔿 🖪 https://192.168.40.146::	5693/gui/checks		▼ Search	• م	• ີ 🗠 🔅 🥲
Checks · NCPA 🛛 🗙 🗋	•				
NCPA 🖵 Dashboard	✓ Checks O Live	Data 🛔 API	i 🔛 Graphs	🌣 Admin 🛛 🕀 H	elp <b>ථ</b> Logout
Checks Status Any	у 💙 Туре	Both 🗸	Executed By Select senders	▼ Filter Search	Q
Page 1 of 7 🛛 Showing 1 - 2	20 of 134 total check reco	rds		1 2 3	4 5 >
Node Endpoint	Check Time	Status	Status Information	Executed By	Туре
processes	11/26/2024 11:54:42	ок	<pre>OK: Process count was 79   'process_count'=79;300;400; 'cpu'=97.699999999999999999;;; 'memory61.38%;;; 'memoryrms'=1.31000000000000005GB;;; 'memory_rss'=1.99000000000001GB;;; Toggle long output</pre>	Internal	Passive
memory/virtual	11/26/2024 11:54:42	ОК	OK: Memory usage was 53.00 % (Available: 1.41 GiB, Total: 3.00 GiB, Free: 1.41 GiB, Used: 1.59 GiB)   'available'=1.41GiB;;; 'total'=3.00GiB;;' percent'=53.00%;80;90; 'free'=1.41GiB;;; 'used'=1.59GiB;;;	Internal	Passive
memory/swap	11/26/2024 11:54:42	ок	OK: Swap usage was 14.30 % (Used: 0.10 GiB, Total: 0.69 GiB, Free: 0.59 GiB)   'used'=0.10GiB;;; 'total'=0.69GiB;;; 'free'=0.59GiB;;;	Internal	Passive
disk/logical/C:  /used_percent	11/26/2024 11:54:42	ОК	OK: Used_percent was 41.70 %   'used_percent'=41.70%;80;90; Act	Internal ivate Windows	Passive
cpu/percent	11/26/2024 11:54:42	OK	OK: Percent was 0.00 %   Go t	Internals to activa	t Passive ows.

Рис. 5.13. Перегляд параметрів моніторингу робочої станції WS-22-40-1 через <u>https://192.168.40.146:5693</u>

На підставі отриманого переліку команд ми можемо обрати необхідні параметри для відображення у системі моніторингу. Виконаємо команду отримання інформації про вільне місце на логічному диску С:

/usr/local/nagios/libexec/check\_ncpa.py -H 192.168.40.146 -t P@ssw0rd2024 -p 5693 -M 'disk/logical/C://free' -w 15: -c 10: -u Gi

-w: встановлює поріг для попередження (warning). Якщо виміряне значення метрики перевищує цей поріг, перевірка видасть статус попередження.

-с: встановлює критичний поріг. Якщо виміряне значення метрики перевищує цей поріг, перевірка видасть статус критичної помилки.

-и: вказує одиниці вимірювання для порогів, заданих ключами -w та -с. G вказує гігабайти.

Довідково, для тренування 🙂, тип файлової системи диска С:

/usr/local/nagios/libexec/check\_ncpa.py -H 192.168.40.146 -t P@ssw0rd2024 -p 5693 -M 'disk/logical/C:|/fstype'

Або, характеристики мережевого інтерфейсу – відправлені пакети:

/usr/local/nagios/libexec/check\_ncpa.py -H 192.168.40.146 -t P@ssw0rd2024 -p 5693 -M 'interface/Ethernet/packets\_sent'

та отримані пакети:

/usr/local/nagios/libexec/check\_ncpa.py -H 192.168.40.146 -t P@ssw0rd2024 -p 5693 -M 'interface/Ethernet/packets\_recv'

Час роботи системи:

/usr/local/nagios/libexec/check\_ncpa.py -H 192.168.40.146 -t P@ssw0rd2024 -p 5693 -M 'system/uptime'

Доповнимо конфігураційний файл /usr/local/nagios/etc/objects/workstation/ws-22-40-1.cfg секціями описаних параметрів.

define service (	
host_name	WS-22-40-1
service_description	Free space on disk C
check_command	check_ncpa!-t 'P@ssw0rd2024' -Р 5693 -М 'disk/logical/C: /free' -w 15: -с 10: -u Gi
max_check_attempts	5
check_interval	5
retry_interval	1
check_period	24x7
notification_interval	60
notification period	24x7

	}	
	define service {	
	host name	WS-22-40-1
		PhysicalDrive, Read bytes
	check command	check popalet 'P@sswird2024' -P 5693 -M 'disk/physical/PhysicalDrive0/read hutes' -d -u M -w 50 -c
100	check_commund	
	max check attempts	5
	check interval	
	netry interval	
	ietry_intervar	
	check_period	24x7
	notification_interval	60
	notification_period	24x7
	}	
	define service {	
	host name	WS-22-40-1
	_ service description	PhysicalDrive. Write bytes
	check command	check ncpal-t 'P@ssw0rd2024' -P 5693 -M 'disk/physical/PhysicalDrive0/write bytes' -d -u M -w 50 -c
100		
	max check attempts	5
	·	5
	retry interval	7
	-back maniad	-
	check_period	24×1
	notification_interval	60
	notification_period	24x7
	}	
	define service {	
	host_name	WS-22-40-1
	service description	PhysicalDrive. Read time
	check command	- 
	may check attempts	я я
	aback interval	
	check_interval	
	retry_interval	1
	check_period	24x7
	notification_interval	60
	notification_period	24x7
	}	
	define service {	
	host_name	WS-22-40-1
		PhysicalDrive. Write time
		- 
	may check attempts	я я
	aback interval	
	check_interval	
	retry_interval	
	check_period	24x7
	notification_interval	60
	notification_period	24x7
	}	
	define service {	
	host_name	WS-22-40-1
	service_description	Ethernet. Sent bytes
	check_command	check_ncpa!-t 'P@ssw0rd2024' -P 5693 -M 'interface/Ethernet/bytes_sent' -d -u k -w 10 -c 100
	max check attempts	5
	·	5
	rotry interval	7
	, , , , ,	
	Check_period	24x7
	notification_interval	60
	notification_period	24x7
	}	
	define service {	
	host_name	WS-22-40-1
	service_description	Ethernet. Received bytes
	check_command	check_ncpa!-t 'P@ssw0rd2024' -P 5693 -M 'interface/Ethernet/bytes_recv' -d -u k -w 10 -c 100
	max_check attempts	5
	 check interval	5
	retry interval	1
	check period	24x7
	notification intermal	 
	notification_interval	00
	notification_period	24x7
l I	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

Робоча станція WS-G-N-1 працює на динамічній адресації — її IP-адреса змінна у відповідному діапазоні DHCP-серверу. При налаштуванні адресації Nagios-серверу ми налаштували його адресацію з доступом до нашого DNS, тому змінюємо статичну адресацію робочої станції WS-G-N-1 на її ім'я у домені.

Виконаємо перевірку як працює команда **check\_ncpa** з доменним ім'ям (-H ws-G-N-1.surname.net):

/usr/local/nagios/libexec/check\_ncpa.py -H ws-G-N-1.surname.net -p 5693 -t P@ssw0rd2024 -M cpu/percent -w 80 -c 90 -q 'aggregate=avg'

student@serv-22-40-1:/usr/local/nagios/libexec\$ ping falkovsky.net
PING falkovsky.net (192.168.40.131) 56(84) bytes of data.
64 bytes from serv-22-40-1 (192.168.40.131): icmp seq=1 ttl=128 time=0.607 ms
64 bytes from serv-22-40-1 (192.168.40.131): icmp_seq=2 ttl=128 time=0.470 ms
64 bytes from serv-22-40-1 (192.168.40.131): icmp_seq=3 ttl=128 time=0.539 ms
^c
falkovsky.net ping statistics
3 packets transmitted, 3 received, 0% packet loss, time 2047ms
rtt min/avg/max/mdev = 0.470/0.538/0.607/0.055 ms
student@serv-22-40-1:/usr/local/nagios/libexec\$ /usr/local/nagios/libexec/check_ncpa.py -H ws-22-40-1.falkovsky.net
-p 5693 -t P@sswOrd2024 -M cpu/percent -w 80 -c 90 -q 'aggregate=avg'
OK: Percent was 58.80 %   'percent'=58.80%;80;90;
student@serv-22-40-1:/usr/local/nagios/libexec\$

Рис. 5.14. check-ncpa по доменному імені робочої станції ws-22-40-1.falkovsky.net

Редагуємо адресу (значення параметру address) у секції визначення робочої станції відповідного конфігураційного файлу робочої станції /usr/local/nagios/etc/objects/workstation/ws-22-40-1.cfg:

-		
	define host {	
	host_name	WS-22-40-1
	address	ws-22-40-1.falkovsky.net
	hostgroups	win-workstations
	check_command	check_ncpa!-t 'P@ssw0rd2023' -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
	}	

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 зміни у відображенні груп хостів, хостів та їх сервісів після виконаних налаштувань.

Status Sum	mary For All Host	Groups			Host Status Deta	uls For All Host	Groups
lingt Group	Uppt Status Summary	On a final Ottoburg Community	Limit Results: 100 ∨ Host ★	Status **	Last Check **	Duration **	Status Information
Host Group	Host status summary	service status summary	WS-22-40-1 🌇 🥵	UP	11-26-2024 12:07:45	Od Oh 52 m 16a	OK: Agent_version was [3.17]
China Contona (mast and tota)	TOP	DOK	localhost 🔒	UP	11-26-2024 12:08:58	1d15h45m44a	PINGOK - Packet loss = 0%, RTA = 0.06 ms
Windows WorkStations (win-workstations)	1 UP	1)WARNING: 110shandled	serv-22-40-1 🏻 🔒	UP	11-26-2024 12:07:41	Od 17h 41m 36a	PING OK - Packet loss = 0%, RTA = 0.70 ms
Windows Servers (windows-servers)	1 UP	110K	Results 1 - 3 of 3 Matching Ho	sts			
		Service St	atus Details For Hos	st 'WS-22-4	10-1'		

lost *+	Service **	Status 🏞	Last Check 🏞	Duration 🏞 🕈	Attempt **	Status Information
WS-22- 40-1	CPU Usage	ок	11-26-2024 12:09:46	Od Oh 5 m 5Oa	1/5	OK: Percent was 0.00 %
	Ethernet, Received bytes	ок	11-26-2024 12:10:06	Od Oh 49 m 29a	1/5	OK: Bytes_recv was 0.07 kB/a
	Ethernet, Sent bytes	OK	11-26-2024 12:10:49	Od Oh 48m 46a	1/5	OK: Bytes_sent was 0.17 kB/s
	Free space on disk C	OK	11-26-2024 12:11:32	Od Oh 48m 3a	1/5	OK: Free was 40.51 GiB
	Memory Usage	WARNING	11-26-2024 12:10:41	Od Oh 48m 54a	5/5	WARNING Memory usage was 55.30 % (Available: 1.44 GB, Totat 3.22 GB, Fre 1.44 GB, Used: 178 GB)
	PhysicalDrive. Read bytes	ок	11-26-2024 12:12:15	Od Oh 47m 20s	1/5	OK: Read_bytes was 0.01 MB/s
	PhysicalDrive. Read time	ок	11-26-2024 12:12:58	Od Oh 46 m 37a	1/5	OK: Read_time was 0.00 ms/s
	PhysicalDrive Write bytes	ок	11-26-2024 12:13:40	Od Oh 45 m 55a	1/5	OK: Write_bytes was 0.02 MB/s
	PhysicalDrive Write time	ок	11-26-2024 12:14:23	Od Oh 45 m 12a	1/5	OK: Write_time was 0.00 ms/s
	Process Count	OK	11-26-2024 12:12:42	Od Oh 51m 53a	1/5	OK: Process count was 80

Рис. 5.15. Перегляд виконаних налаштувань:

Host Group Summary, Host Status, Service Status Details for host WS-22-1-1

Зверніть увагу на «жовтий» статус використання пам'яті на робочій станції WS-22-40-1 (рис.5.15.).

## Завдання до лабораторної роботи

- 1. Встановіть та налаштуйте на робочій станції WS-G-N-1 актуальну версію агента моніторингу NCPA. У звіті обов'язково наведіть скрін закладки checks HTTP-підключення до NCPA WS-G-N-1.
- 2. Налаштуйте моніторинг основних сервісів (мінімум 10) робочої станції WS-G-N-1. У звіті обов'язково наведіть скріни закладок Hosts та View Service Details for WS-G-N-1.
- 3. Відредагуйте конфігурацію Nagios таким чином, щоб у системі було три активних групи хостів: Windows Servers, Windows Workstations та Linux Servers. Закладка Host Groups Nagios.

## Звіт має містити:

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

# 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" <u>https://github.com/NagiosEnterprises/ncpa/issues/857</u>

Nagios Support Knowledgebase. Network Interface Checks
 <a href="https://support.nagios.com/kb/article/network-interface-checks-781.html">https://support.nagios.com/kb/article/network-interface-checks-781.html</a>