

Лабораторна робота №12

Налаштування моніторингу Windows-хосту за допомогою розширеного Zabbix Agent 2.

Мета: набути практичних навичок з налаштування моніторингу Windows-хосту за допомогою Zabbix Agent 2, забезпечуючи інтеграцію з сервером моніторингу Zabbix.

Інструменти: гіпервізор VirtualBox, модель комп'ютерної мережі.

Теоретичні відомості

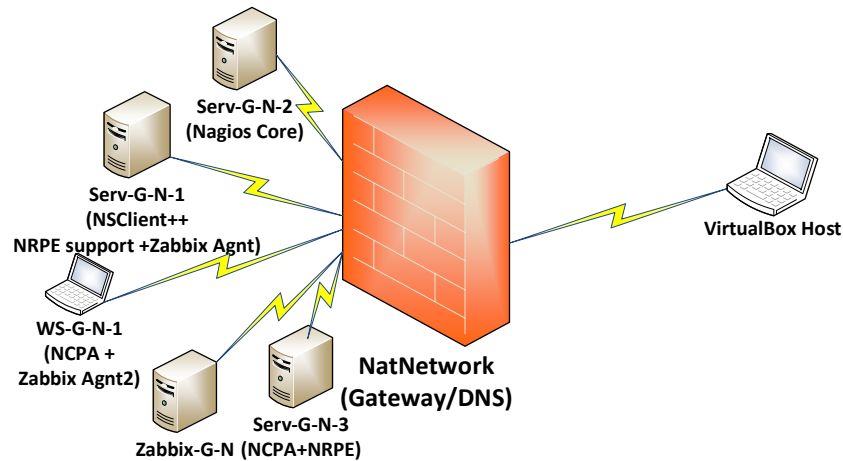


Рис. 12.1. Топологія мережі

На рис. 12.1 наведена модель комп'ютерної мережі, побудована під час виконання попередніх лабораторних робіт. На сервері Serv-G-N-2 розгорнуто систему моніторингу на базі Nagios 4.X. На сервері Zabbix-G-N працює сервер Zabbix з базовими налаштуваннями.

The screenshot shows the Zabbix web interface. The top part displays the 'Hosts' monitoring menu with search filters for Name, Host groups, IP, DNS, Port, and Status. Below this is a table of hosts:

Name	Interface	Availability	Tags	Status	Latest data	Problems	Graphs	Dashboards	Web
Serv-22-40-1	192.168.40.131:10050	OK	class:os target:windows	Enabled	Latest data 137	1	Graphs 12	Dashboards 7	Web
Zabbix-22-40	127.0.0.1:10050	OK	class:os class:windows target:linux	Enabled	Latest data 151	Problems	Graphs 3D	Dashboards 1	Web

The bottom part of the screenshot shows the 'Problems' monitoring menu with search filters for Host groups, Hosts, Triggers, Problem, Severity, Age less than, Show symptoms, Show suppressed problems, and Acknowledgement status. Below this is a table of problems:

Time	Severity	Recovery time	Status	Info	Host	Problem	Duration	Update	Actions	Tags
12:21:01 AM	Warning		PROBLEM		Serv-22-40-1	System time is out of sync (diff with Zabbix server > 60s)	42m 0s	Update		class:os component:system scope:notice

Рис. 12.2. Меню [Monitoring] → [Hosts] у веб-інтерфейсі Zabbix

Налаштування синхронізації часу на сервері Zabbix.

У процесі підключення до системи моніторингу контролера домену (Serv-22-40-1) виявлена проблема синхронізації часу з сервером Zabbix (рис.12.2). Виправити цю проблему безпосередньо через веб-інтерфейс Zabbix неможливо, оскільки вона пов'язана з розсинхронізацією часу на сервері (Serv-22-40-1) та сервері Zabbix-22-40.

Синхронізація часу на сервері Zabbix дуже важлива для коректної роботи системи моніторингу. Є багато методів синхронізації часу. Розглянемо синхронізацію часу на сервері Zabbix з єдиним для нього і контролеру домену NTP сервером. Контролер домену (Serv-G-N-1) зазвичай, виступає NTP-сервером, з якого інші пристрої мережі можуть отримувати точний час.

Переконаємося, що контролер домену налаштований як NTP-сервер. У Windows Server 2019 виконуємо команду PowerShell:

```
w32tm /query /status
```

Це покаже стан служби часу. Якщо вона працює, контролер готовий до синхронізації.

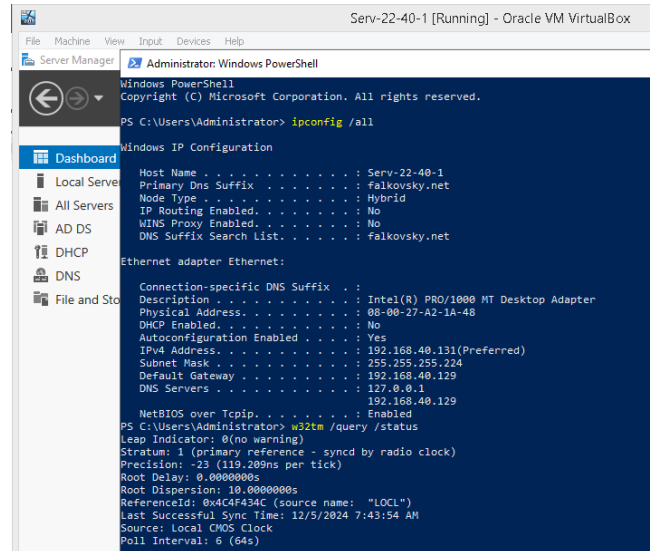


Рис. 12.3. `w32tm /query /status` на контролері домену

Задаємо для служби часу зовнішнє джерело синхронізації `pool.ntp.org` та знову перевіряємо стан служби часу:

```
w32tm /config /manualpeerlist:"pool.ntp.org" /reliable:YES /update
```

```
w32tm /query /status
```

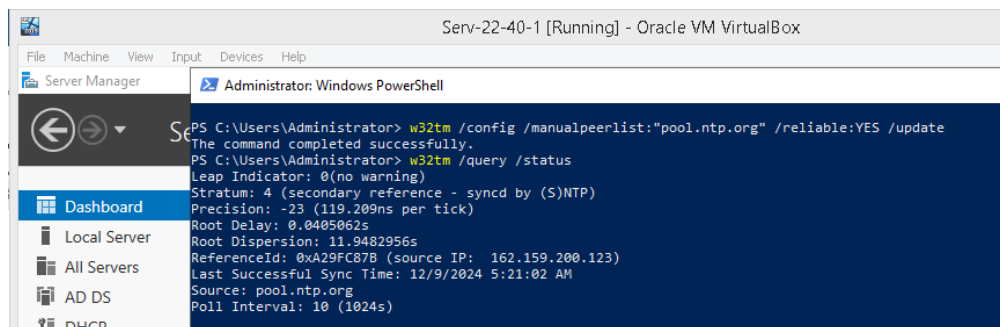


Рис. 12.4. `w32tm /query /status` на контролері після зміни налаштувань.

Якщо служба часу не працює, вмикаємо її та виконуємо примусову синхронізацію часу:

```
w32tm /config /manualpeerlist:" pool.ntp.org " /syncfromflags:manual /reliable:YES /update
```

```
w32tm /resync
```

На сервері Zabbix (Zabbix-G-N) налаштовуємо синхронізацію часу через NTP сервер контролеру домену. Заходимо на сервер Zabbix-G-N через SSH або консоль та перевіряємо зв'язок з контролером домену:

```
ping serv-22-40-1.falkovsky.net
```

Додаємо NTP-сервер до списку:

```
sudo chronyc add server serv-22-40-1.falkovsky.net
```

Оновлюємо час, перевіряємо статус і дивимось чи додався контролер домену до списку NTP-серверів:

```
sudo chronyc makestep
```

```
chronyc tracking
```

```
timedatectl
```

```
chronyc sources
```

```

Zabbix-22-40 [Running] - Oracle VM VirtualBox
root@Zabbix-22-40 ~# sudo systemctl status chronyd
● chronyd.service - NTP client/server
   Loaded: loaded (/usr/lib/systemd/system/chronyd.service; enabled; vendor pre
   Active: active (running) since Sun 2024-12-08 15:31:49 UTC; 16min ago
     Docs: man:chronyd(8)
           man:chrony.conf(5)
   Process: 598 ExecStartPost=/usr/libexec/chrony-helper update-daemon (code=exi
   Process: 571 ExecStart=/usr/sbin/chronyd $OPTIONS (code=exited, status=8/SUCCE
   Main PID: 586 (chronyd)
     Tasks: 1 (limit: 12374)
    Memory: 3.8M
   CGroup: /system.slice/chronyd.service
           └─596 /usr/sbin/chronyd

Dec 08 15:31:48 Zabbix-22-40 systemd[1]: Starting NTP client/server...
Dec 08 15:31:49 Zabbix-22-40 chronyd[586]: chronyd version 4.5 starting (+CMDMD
Dec 08 15:31:49 Zabbix-22-40 chronyd[586]: Loaded 0 symmetric keys
Dec 08 15:31:49 Zabbix-22-40 chronyd[586]: Frequency -26.291 +/- 1.272 ppm read
Dec 08 15:31:49 Zabbix-22-40 chronyd[586]: Using right/UTC timezone to obtain
Dec 08 15:31:49 Zabbix-22-40 systemd[1]: Started NTP client/server.
Dec 08 15:32:22 Zabbix-22-40 chronyd[586]: Selected source 212.127.95.218 (2.al
Dec 08 15:32:22 Zabbix-22-40 chronyd[586]: System clock TAI offset set to 37 se
root@Zabbix-22-40 ~#

root@Zabbix-22-40 ~# ping serv-22-40-1.falkovsky.net
PING serv-22-40-1.falkovsky.net (192.168.40.131) 56(84) bytes of data:
 64 bytes from 192.168.40.131: icmp_seq=1 ttl=128 time=0.483 ms
 64 bytes from 192.168.40.131: icmp_seq=2 ttl=128 time=0.560 ms
 64 bytes from 192.168.40.131: icmp_seq=3 ttl=128 time=0.544 ms
^C
--- serv-22-40-1.falkovsky.net ping statistics ---
 3 packets transmitted, 3 received, 0% packet loss, time 2021ms
 rtt min/avg/max/mdev = 0.483/0.529/0.560/0.033 ms
root@Zabbix-22-40 ~# sudo chronyc add server serv-22-40-1.falkovsky.net
300 OK
root@Zabbix-22-40 ~# sudo chronyc makestep
200 OK
root@Zabbix-22-40 ~# chronyc tracking
Reference ID      : 3EC09F99 (ip153-159.8772.as)
Stratum          : 3
Ref time (UTC)   : Tue Dec 10 07:51:21 2024
System time      : 0.000000000 seconds slow of NTP time
Last offset      : +0.000102562 seconds
RMS offset       : 3565.758156250 seconds
Frequency        : +25.794 ppm slow
Residual freq    : +0.008 ppm
Skew             : 0.198 ppm
Root delay       : 0.009552759 seconds
Root dispersion  : 0.001553099 seconds
Update interval  : 513.2 seconds
Leap status      : Normal
root@Zabbix-22-40 ~#

root@Zabbix-22-40 ~# timedatectl
[root@Zabbix-22-40 ~]# timedatectl
          Local time: Tue 2024-12-10 08:14:49 UTC
          Universal time: Tue 2024-12-10 08:14:49 UTC
             RTC time: Tue 2024-12-10 08:14:50
             Time zone: Etc/UTC (UTC, +0000)
System clock synchronized: yes
              NTP service: n/a
              RTC in local TZ: no
[root@Zabbix-22-40 ~]# chronyc sources
=====
MS Name/IP address             Stratum Poll Reach LastRx Last sample
=====
^* time.cloudflare.com         3    10   377   352   -565us[-565us] +/-  20ms
^* main24.anyplace-hosting.>   2    10   377   948   -2536us[-2639us] +/-  54ms
^* ip153-159.8772.as           2    10   377   468    -64us[-170us] +/- 5846us
^* host-176-36-168-10.b024.>  2    10   377   597  -1160us[-1265us] +/-  44ms
^* 192.168.40.131             3     6   377    49    +40ms[+40ms] +/-  68ms
[root@Zabbix-22-40 ~]#

```

Рис. 12.5. Редагування конфігурації служби chronyc на сервері Zabbix-22-40

```

root@Zabbix-22-40 ~#
# Use public servers from the pool.ntp.org project.
# Please consider joining the pool (http://www.pool.ntp.org/join.html).
pool serv-22-40-1.falkovsky.net iburst
#pool 2.almalinux.pool.ntp.org iburst

# Record the rate at which the system clock gains/loses time.
driftfile /var/lib/chrony/drift

# Allow the system clock to be stepped in the first three updates
# if its offset is larger than 1 second.
makestep 1.0 3

```

Рис. 12.6. Редагування /etc/chrony.conf

У літературі описаний альтернативний, більш складний метод налаштування. Він передбачає редагування файлу конфігурації `/etc/chrony.conf` (рис.12.6) з перезавантаженням служби синхронізації часу:

```
sudo systemctl restart chronyd
```

Синхронізація часу на сервері Zabbix після зміни NTP-серверів може зайняти кілька хвилин.

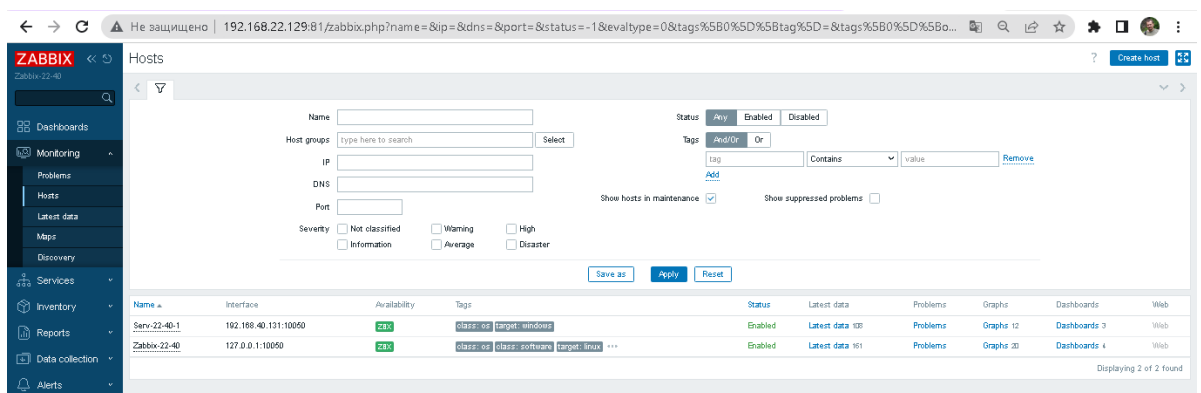


Рис. 12.7. Меню [Monitoring] → [Hosts] у веб-інтерфейсі Zabbix

Налаштування розширеного агентського моніторингу робочої станції Windows у Zabbix.

Завантажуємо Zabbix Agent. На робочій станції Windows WS-G-N-1, де планується встановити агент, переходимо на офіційний сайт [Zabbix Downloads](https://www.zabbix.com).



Рис. 12.8. Вибір операційної системи для агента Zabbix та типу інсталяційного пакету..

Обираємо

Operating System: Windows,

Architecture: x64 (або x86, якщо у вас 32-бітна система ☺),

Zabbix Version: 7.0 (відповідає версії встановленого сервера Zabbix)

та завантажуюмо інсталяційний файл або архів.

Далі описується встановлення агента на Windows сервер чи станцію чи за допомогою msi-пакету /Release 7.06/

На сторінці завантаження присутні два агенти. Обидва агенти Zabbix — це програми для збору даних про систему, але вони мають деякі суттєві відмінності, які варто враховувати залежно від ваших потреб. Zabbix Agent (класичний агент) був використаний для налаштування моніторингу контролеру домену на базі Windows Server 2019. Для моніторингу робочої станції використовуємо Zabbix Agent 2.

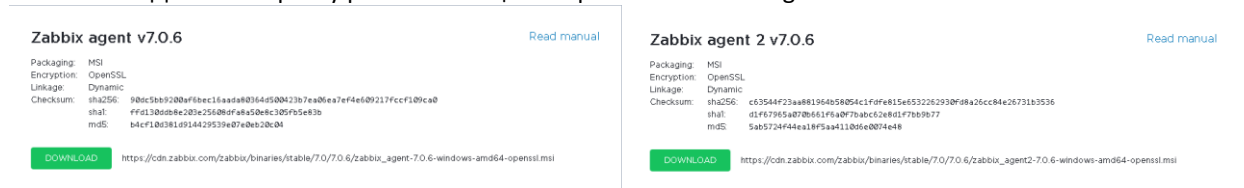


Рис. 12.9. Версії v7.0.6 агентів Zabbix для Windows

Завантажуємо файл інсталяції Zabbix agent 2 v.7.0.6 на робочу станцію WS-G-N-1 та виконуємо встановлення агента.

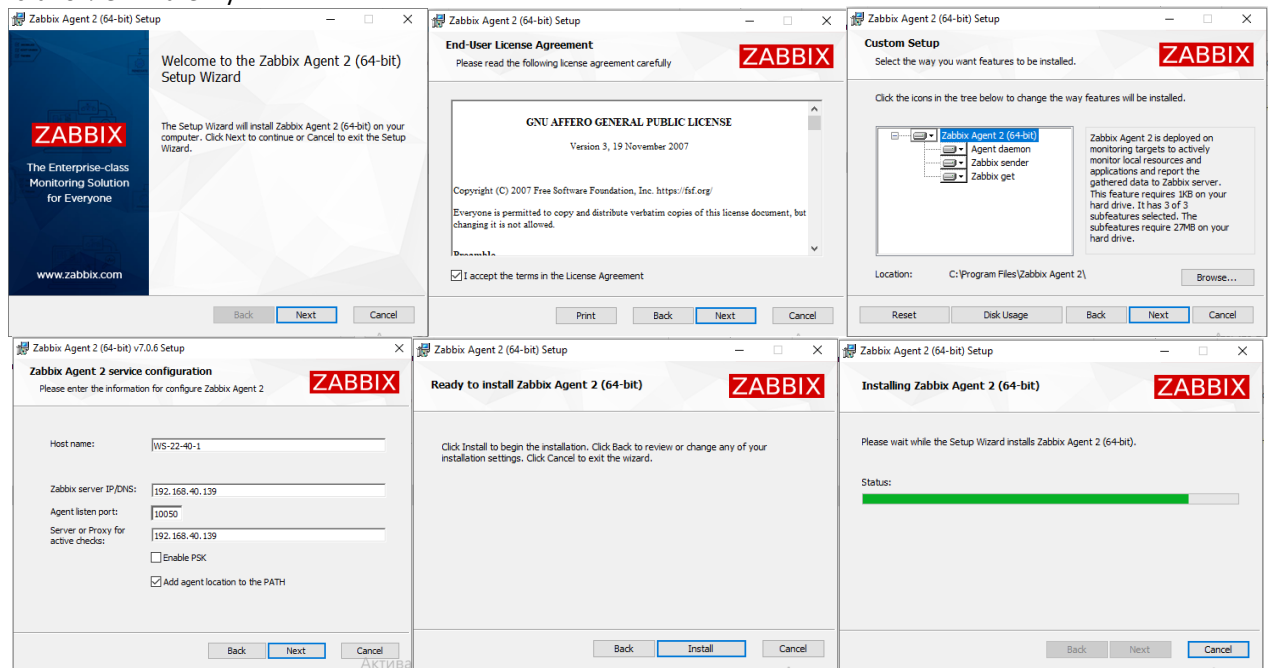


Рис. 12.10. Встановлення Zabbix agent 2 v.7.0.6 для Windows v7.0.6

Для правильного заповнення конфігурації Zabbix Agent (рис.12.9 / малюнок 4) зверніть увагу на такі параметри:

- **Host name.** Ім'я хосту, під яким він буде зареєстрований та відображатися у Zabbix Server. Наприклад: WS-22-40-1.
- **Zabbix server IP/DNS.** Вкажіть IP-адресу або DNS-ім'я сервера Zabbix, з яким агент має з'єднуватися.
- **Agent listen port.** Це порт, на якому агент буде слухати запити. Порт за замовчуванням: 10050.
- **Server or Proxy for active checks.** IP-адреса або DNS-ім'я сервера чи проксі-сервера Zabbix для активних перевірок. Якщо не використовуєте проксі-сервер, вкажіть IP сервера Zabbix.
- **Enable PSK.** Якщо використовуєте шифрування PSK для безпечного з'єднання, поставте галочку та налаштуйте параметри PSK. Якщо PSK не використовується, залиште опцію вимкненою.
- **Add agent location to the PATH.** Додає шлях до агента у змінну середовища PATH, що спрощує доступ до виконуваних файлів агента через командний рядок.

Після завершення встановлення агента, перевіряємо стан служби «Zabbix Agent» та чи створилось відповідне агенту правило на Windows Defender Firewall:

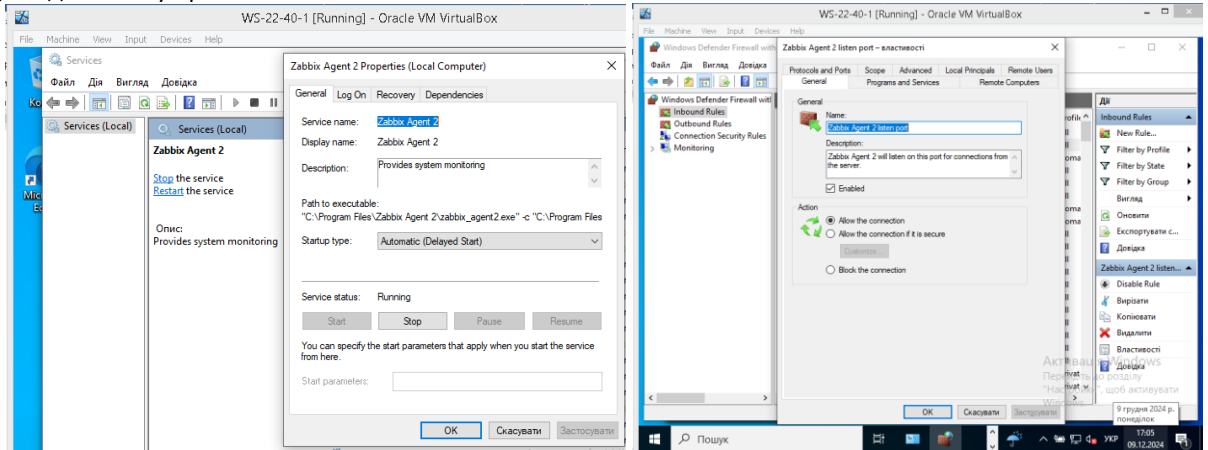


Рис. 12.11. Сервіс та правило Firewall «Zabbix Agent» на WS-22-40-1

На цьому конфігурування серверу WS-G-N-1 завершено.

Заходимо у веб-інтерфейс Zabbix (<http://192.168.40.139>), переходимо у лівому меню до [Data collection] → [Hosts.]. Натискаємо кнопку Create host у верхньому правому куті для додавання нового хосту.

Вводимо ім'я хосту, додаємо інтерфейс із типом Agent, прив'язуємо шаблон (наприклад, Template OS Windows by Zabbix agent active) та зберігаємо налаштування.

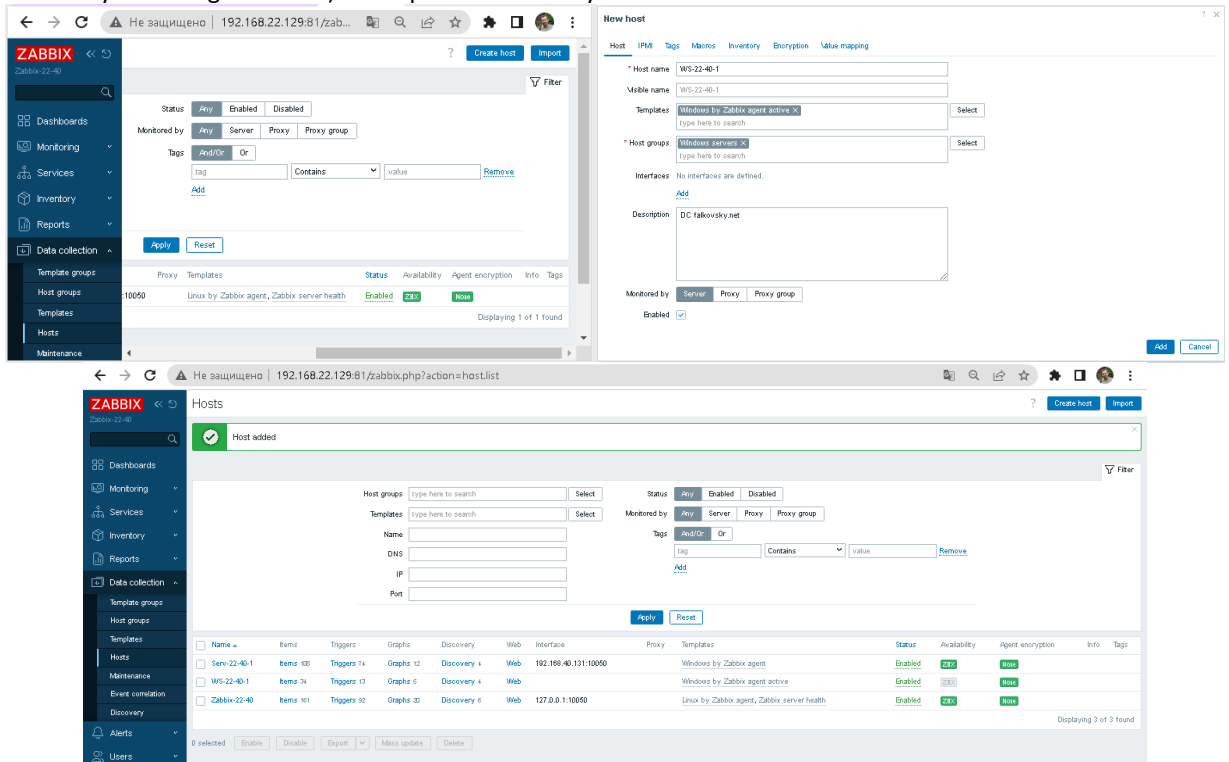


Рис. 12.12. Додавання хосту у веб-інтерфейс Zabbix

При додаванні хосту ми не вказували IPv4 адресу робочої станції, що має динамічну адресацію, але встановлення на робочу станцію Zabbix agent 2 та налаштування Template хосту у "Windows by Zabbix agent active" дозволило вирішити цю проблему. Інше рішення такого питання - доступ до хосту через DNS або за іншими налаштуваннями (наприклад, через записи у файлі hosts).

Переглянемо результати виконаних налаштувань. Меню [Data collection] → [Hosts] або меню [Monitoring] → [Hosts]. Загальний статус хоста: зелена іконка сигналізує, що хост доступний і дані отримуються, червона іконка вказує на проблему з підключенням.

У меню [Monitoring] → [Hosts] для кожного хосту є кілька підменю: Dashboard, Problems, Graphs, Items та інші. На рис.12.12 система моніторингу виявила проблему запуску служби NCPA. Виправимо цю проблему одразу у налаштуваннях служби.

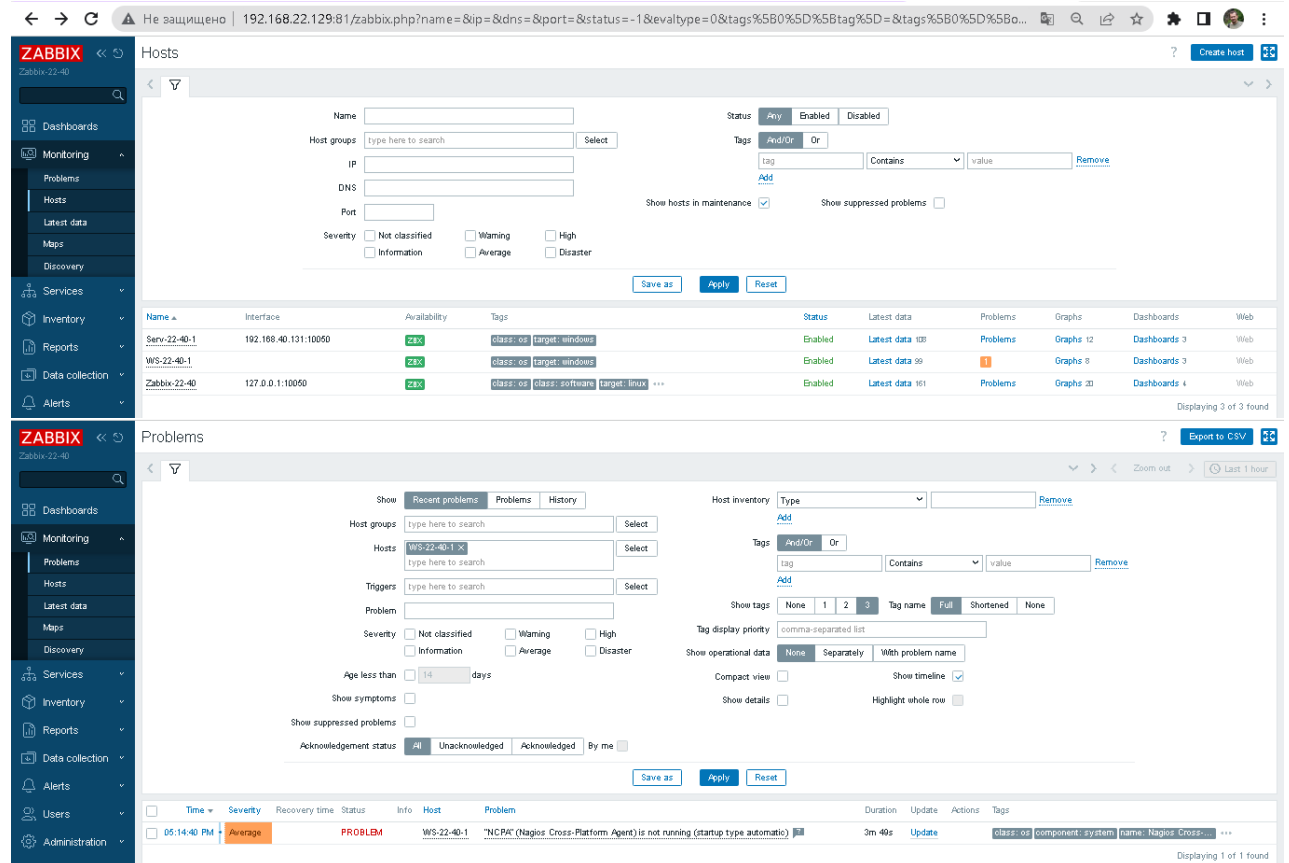


Рис. 12.13. Меню [Monitoring] → [Hosts] у веб-інтерфейсі Zabbix

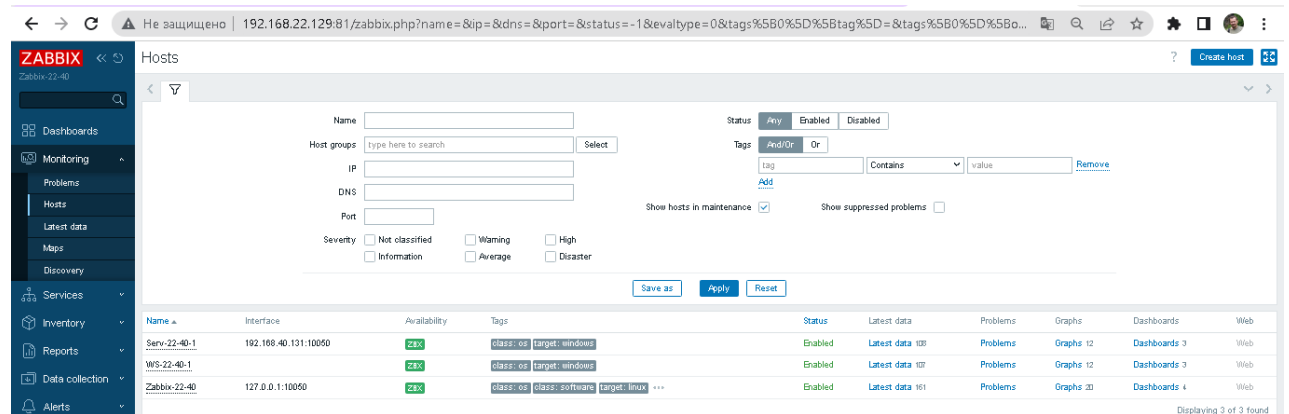


Рис. 12.14. Меню [Monitoring] → [Hosts] у веб-інтерфейсі Zabbix. Проблеми відсутні.

Завдання до лабораторної роботи

1. Виконайте налаштування синхронізації часу серверів Serv-G-N-1 та Zabbix-G-N з DC NTP.
2. Встановіть та налаштуйте на робочій станції WS-G-N-1 оновлений Agent 2 Zabbix без використання шифрування PSK та зміни портів для моніторингу.
3. Додайте робочу станцію WS-G-N-1 до переліку хостів сервера Zabbix-G-N
4. Перегляньте дані моніторингу у веб-інтерфейсі Zabbix. Чи існують у даний момент якісь проблеми?

Звіт має містити:

- лістинг використаних команд;
- короткий опис редагування файлів конфігурації;
- скріншоти налаштувань та підключень.

Корисні посилання

- How to Set NTP Server on Windows Server?
<https://operavps.com/docs/set-ntp-server-on-windows-server/>
- How to Set the Timezone and Configure NTP on Windows Server
<https://docs.vultr.com/how-to-set-the-timezone-and-configure-ntp-on-windows-server>
- RedHat. Chapter 18. Configuring NTP Using the chrony Suite.
<http://surl.li/ryqiaq>
- chronyd. Manual Page.
<https://chrony-project.org/doc/4.6/chronyd.html>
- Zabbix Manual.
<https://www.zabbix.com/documentation/current/en/manual>
- Zabbix Download Agents.
https://www.zabbix.com/download_agents