VIET NAM NATIONAL UNIVERSITY HO CHI MINH CITY

UNIVERSITY OF INFORMATION TECHNOLOGY

-----○○🕮○○-----

PROJECT REPORT

Network and System Management

ZABBIX

LECTURER: MS. TRAN THI DUNG

NT132.N12.ATCL – EN

GROUP 10:

TRUONG THI HOANG HAO - 20520191

TRAN THUY ANH - 20521085

LE QUANG MINH - 20520245

Ho Chi Minh City, January 6th, 2023

I. INTRODUCTION

1.1 OVERVIEW

a. Definition:

Zabbix is an open-source monitoring software that monitors numerous parameters of a network, the health and integrity of servers, virtual machines, and cloud services.

b. What Zabbix offers:

- Zabbix uses a flexible notification mechanism that allows users to configure email-based alerts for virtually any event.
- All Zabbix reports and statistics, as well as configuration parameters, are accessed through a web-based front end.
- Agent-based and agentless monitoring.
- Zabbix is free of cost.
- Zabbix is written and distributed under the GPL General Public License version 2.

1.2 COMPONENTS

- Zabbix Server: Responsible for remote network service testing, information collection, storage, display, alerting, ... so that administrators can best monitor the system.
- Zabbix Proxy: A server used to manage remote branch systems or at different network layers as a temporary metric store when the client sends back to reduce the load on the Zabbix server.
- Zabbix Agent: Set up on the client side to collect information about the server and send it to Zabbix-server or zabbix-proxy
- Web interface: Displays information about the servers being monitored.

1.3 OPERATION

Operations for monitoring Windows:

- Install Zabbix Agent and configure the firewall.
- Create and add the host to the Zabbix server (choose a template, add trigger if needed).
- Wait for the server to receive data about the host.
- Checking the latest data, problems, etc., after a while.

Operations for monitoring Linux:

- Install Zabbix Agent2 and configure the .conf file
- Create and add the host to the Zabbix server (choose template).
- Wait for the server to receive data about the host

Operations for monitoring Website:

- Create a new host which uses a Linux server for monitoring the website
- Create a new web scenario for the host

Mechanism of action:

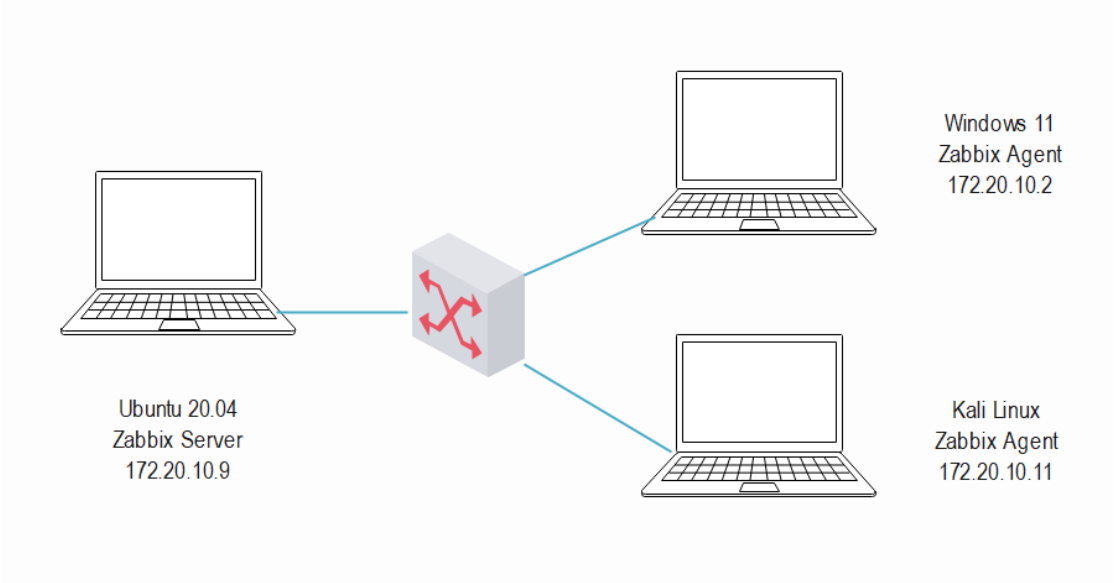
- Zabbix can collect metrics based on Zabbix-agent, SNMP or IPMI then push to the Zabbix server for analysis.
- Zabbix server relies on received metrics to calculate, graph, and alert users based on triggers definition. After the metric is analyzed by the Zabbix server, it will be pushed to store in the Database.
- Zabbix Web is used to display the metrics through the chart for monitoring.

Implement comprehensive monitoring functions:

- Hardware monitoring
- System monitoring
- Network monitoring
- Security monitoring
- Web monitoring
- Log tracking
- Traffic analysis

II. IMPLEMENTATION

2.1 TOPOLOGY



Machine	IP	Package
Ubuntu 20.04	172.20.10.9	Zabbix Server
Windows 11	172.20.10.2	Zabbix Agent
Kali Linux	172.20.10.11	Zabbix Agent

2.2 INSTALLATION

A. Ubuntu 20.04 virtual machine (Server)

- Choose the platform: Zabbix server version 6.2 on Ubuntu 20.04 with MySQL database and Apache web server.
- Install Zabbix repository

  We downloaded the latest Zabbix package, which is 6.2 from their official repo with 'wget' command:

```
wget https://repo.zabbix.com/zabbix/6.2/ubuntu/pool/main/z/zabbix-release/zabbix-release_6.2-2%2Bubuntu20.04_all.deb
```

And then we installed the package with 'dpkg':

```
sudo dpkg -i zabbix-release_6.2-2+ubuntu20.04_all.deb
```

After successfully installed the package, we ran the following command to check for update (upgrade if needed):

```
sudo apt update && sudo apt upgrade
```

- **Install Zabbix server, frontend, agent**

```
sudo apt install zabbix-server-mysql zabbix-frontend-php zabbix-apache-conf zabbix-sql-scripts zabbix-agent
```

- **Create initial database**

Because the Zabbix server needs a database to work correctly, MySQL is one of the databases that are recommended to use with it. We installed mysql-server with this command:

```
sudo apt install mysql-server
```

Configure MySQL to secure our database:

```
sudo mysql_secure_installation
```

The password that was set here would be used later on so we need to remember it. Then, we started the mysql server:

```
sudo systemctl start mysql.service
```

Next, run the following command and it would prompt us to type the password that we created before:

```
mysql -uroot -p
```

After that we began creating the database for the Zabbix server.

```
ubuntu@ubuntu-VB:~$ sudo systemctl start mysql.service
ubuntu@ubuntu-VB:~$  mysql -uroot -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 13
Server version: 8.0.31-0ubuntu0.20.04.1 (Ubuntu)

Copyright (c) 2000, 2022, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> create database zabbix character set utf8mb4 collate utf8mb4_bin;
Query OK, 1 row affected (0,02 sec)

mysql> create user zabbix@localhost identified by 'password';
ERROR 1819 (HY000): Your password does not satisfy the current policy requirements
mysql> create user zabbix@localhost identified by 'Z@bbix';
ERROR 1819 (HY000): Your password does not satisfy the current policy requirements
mysql> create user zabbix@localhost identified by 'Z@bbixpw';
ERROR 1819 (HY000): Your password does not satisfy the current policy requirements
mysql> create user zabbix@localhost identified by 'Z@bbixp4ssword';
Query OK, 0 rows affected (0,02 sec)

mysql> grant all privileges on zabbix.* to zabbix@localhost;
Query OK, 0 rows affected (0,02 sec)

mysql>  set global log_bin_trust_function_creators = 1;
Query OK, 0 rows affected (0,00 sec)

mysql> quit;
Bye
```

The password we created in this step is for Zabbix server to use its database. On Zabbix server host import initial schema and data by running the following command (we would be prompted to enter our newly created password):

zcat /usr/share/zabbix-sql-scripts/mysql/server.sql.gz | mysql --default-character-set=utf8mb4 -uzabbix -p zabbix

Waited for a bit then signed in to mysql server again after importing database schema to disable log_bin_trust_function_creators option.

```
# mysql -uroot -p
password
mysql> set global log_bin_trust_function_creators = 0;
mysql> quit;
```

- **Configure the database for Zabbix server**

Next, we went to the /etc/zabbix directory and edited the "zabbix_server.conf" file by adding the following information: DBPassword=password

We replaced the password with the one we created for Zabbix before.

```
DBUser=zabbix

### Option: DBPassword
#       Database password.
#       Comment this line if no password is used.
#
# Mandatory: no
# Default:
DBPassword=Z@bbixp4ssword
```

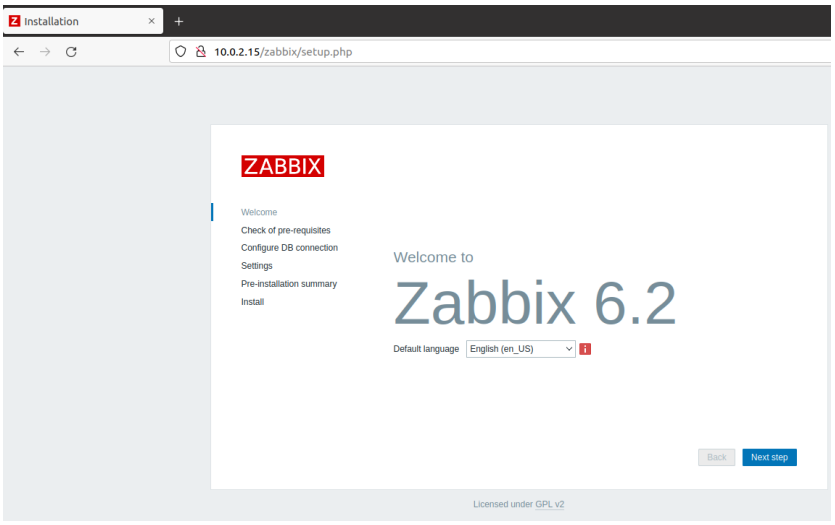
- **Start Zabbix server and agent processes**

Finally, we started the Zabbix server and agent processes and made it start at system boot.

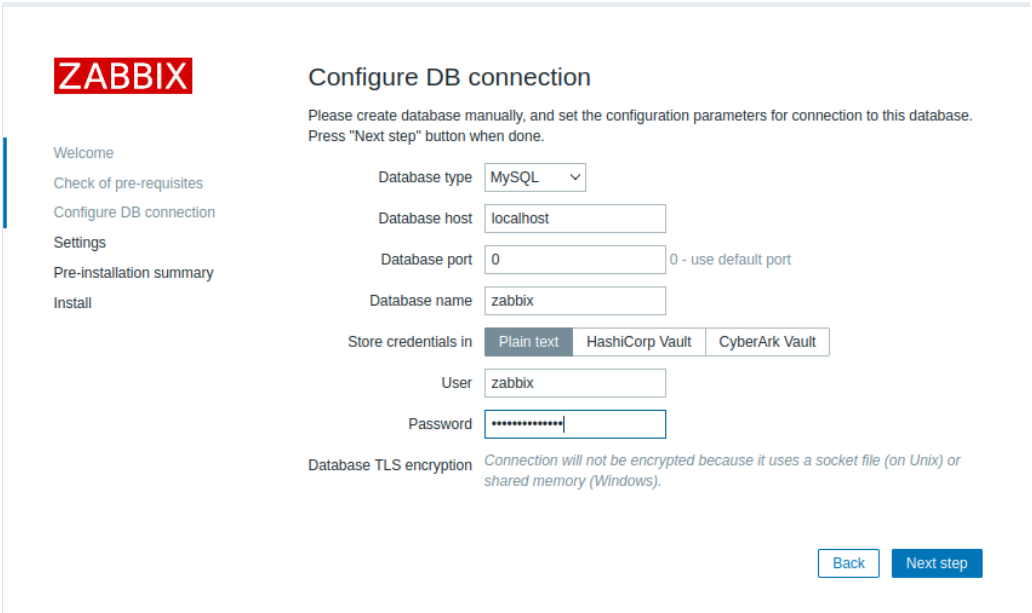
```
# systemctl restart zabbix-server zabbix-agent apache2
# systemctl enable zabbix-server zabbix-agent apache2
```

Checking for the virtual machine's IP address, we had "10.0.2.15".

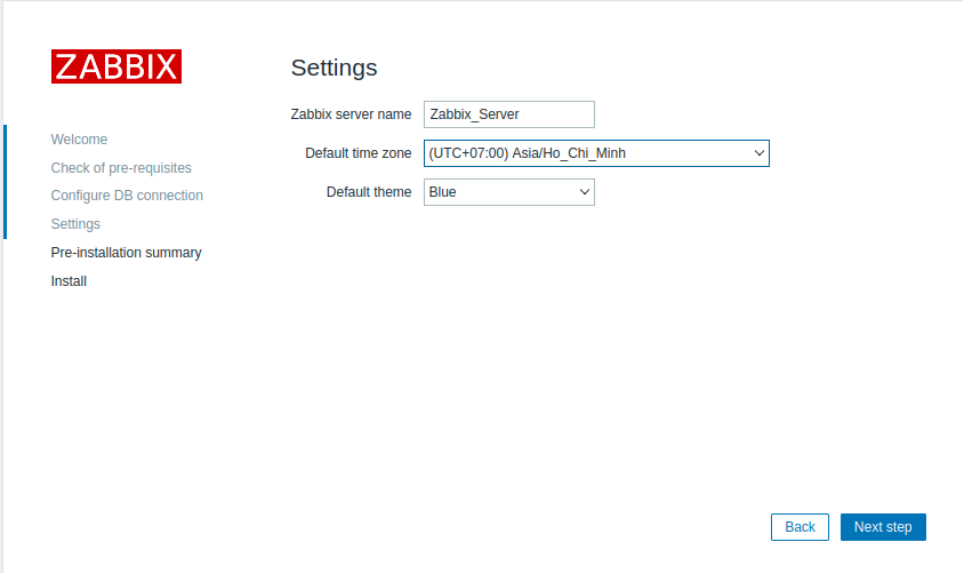
Then, we went to the web browser and configured the frontend for Zabbix at 10.0.2.15/zabbix



Checking all the requirements before installing and to the next page, we entered the database password:



Adding the server's name and changing the time zone:

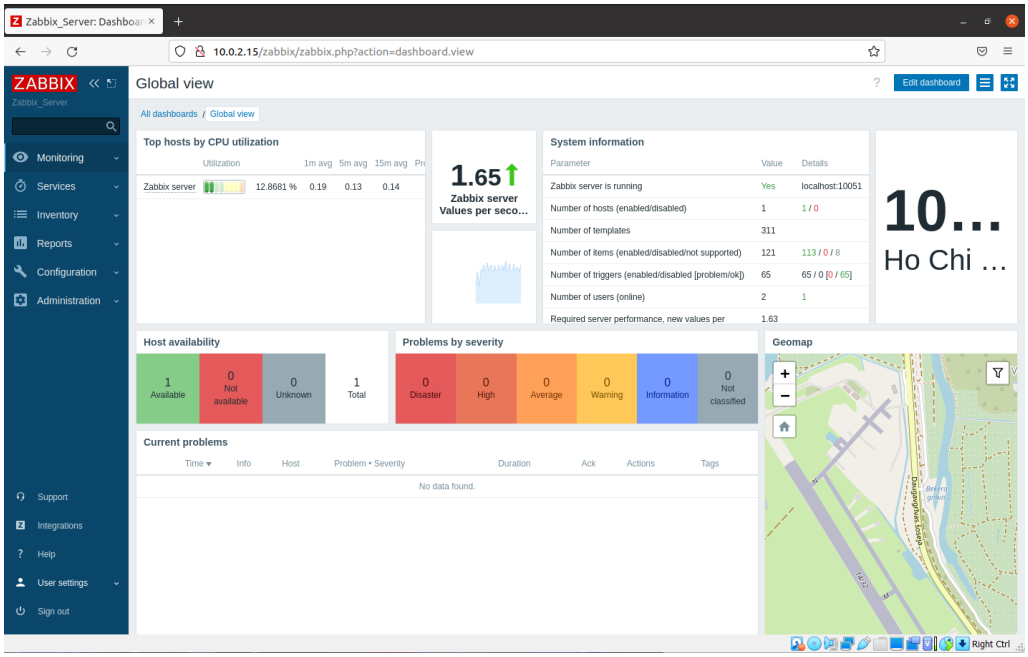


After the previous page, they showed us a summary report for us to check but we could change the setting later by editing the php file. Therefore, we could just click next right away.

After installing Zabbix frontend successfully, we need to edit the /etc/zabbix/web/zabbix.conf.php file to add the Zabbix server's IP and default port.

```
 GNU nano 4.8                    zabbix.conf.php

// Uncomment and set to desired values to override Zabbix hostname/IP and port.
$ZBX_SERVER                     = '10.0.2.15';
$ZBX_SERVER_PORT                = '10051';

$ZBX_SERVER_NAME                = 'Zabbix_Server';
```

Coming back to the login page, we entered "Admin" as username and "zabbix" as password to login as superuser then we would see the following page:



Finally, the installation for the server had been done.

B. Windows (Agent)

- Choose and download the appropriate version for Windows OS: Zabbix agent 6.2 MSI package
- Then open & run the file that had been downloaded

- Accepting the license agreement and jump to the configuration phase B.

C. Kali Linux (Agent2)

- Choose the Agent2 package to install: Zabbix Agent 2 version 6.2 for Debian
- Downloaded then installed Zabbix Agent 2 package:

wget https://repo.zabbix.com/zabbix/6.2/debian/pool/main/z/zabbix-release/zabbix-release_6.2-4%2Bdebian11_all.deb

```
┌──(kali㉿kali)-[~]
└─$ wget https://repo.zabbix.com/zabbix/6.2/debian/pool/main/z/zabbix-release
/zabbix-release_6.2-4%2Bdebian11_all.deb
--2023-01-02 10:49:22--  https://repo.zabbix.com/zabbix/6.2/debian/pool/main/
z/zabbix-release/zabbix-release_6.2-4%2Bdebian11_all.deb
Resolving repo.zabbix.com (repo.zabbix.com)... 178.128.6.101, 2604:a880:2:d0:
:2062:d001
Connecting to repo.zabbix.com (repo.zabbix.com)|178.128.6.101|:443... connect
ed.
HTTP request sent, awaiting response... 200 OK
Length: 3780 (3.7K) [application/octet-stream]
Saving to: 'zabbix-release_6.2-4+debian11_all.deb'

zabbix-release_6.2- 100%[===================>]   3.69K  --.-KB/s    in 0s

2023-01-02 10:49:23 (17.7 MB/s) - 'zabbix-release_6.2-4+debian11_all.deb' sav
ed [3780/3780]
```

dpkg -i zabbix-release_6.2-4+debian11_all.deb

```
┌──(kali㉿kali)-[~]
└─$ sudo dpkg -i zabbix-release_6.2-4+debian11_all.deb
[sudo] password for kali:
Selecting previously unselected package zabbix-release.
(Reading database ... 418249 files and directories currently installed.)
Preparing to unpack zabbix-release_6.2-4+debian11_all.deb ...
Unpacking zabbix-release (1:6.2-4+debian11) ...
Setting up zabbix-release (1:6.2-4+debian11) ...
```

- Checking for update after installing the package:

sudo apt update

```
┌──(kali㉿kali)-[~]
└─$ sudo apt update
Get:2 https://repo.zabbix.com/zabbix-agent2-plugins/1/debian bullseye InRelea
se [4,927 B]
Get:3 https://repo.zabbix.com/zabbix/6.2/debian bullseye InRelease [4,933 B]
Get:4 https://repo.zabbix.com/zabbix-agent2-plugins/1/debian bullseye/main So
urces [1,001 B]
Get:5 https://repo.zabbix.com/zabbix-agent2-plugins/1/debian bullseye/main am
d64 Packages [621 B]
Get:6 https://repo.zabbix.com/zabbix/6.2/debian bullseye/main Sources [1,234
B]
Get:7 https://repo.zabbix.com/zabbix/6.2/debian bullseye/main amd64 Packages
[5,140 B]
Get:1 http://kali.cs.nctu.edu.tw/kali kali-rolling InRelease [30.6 kB]
Get:8 http://kali.cs.nctu.edu.tw/kali kali-rolling/main i386 Packages [18.8 M
B]
```

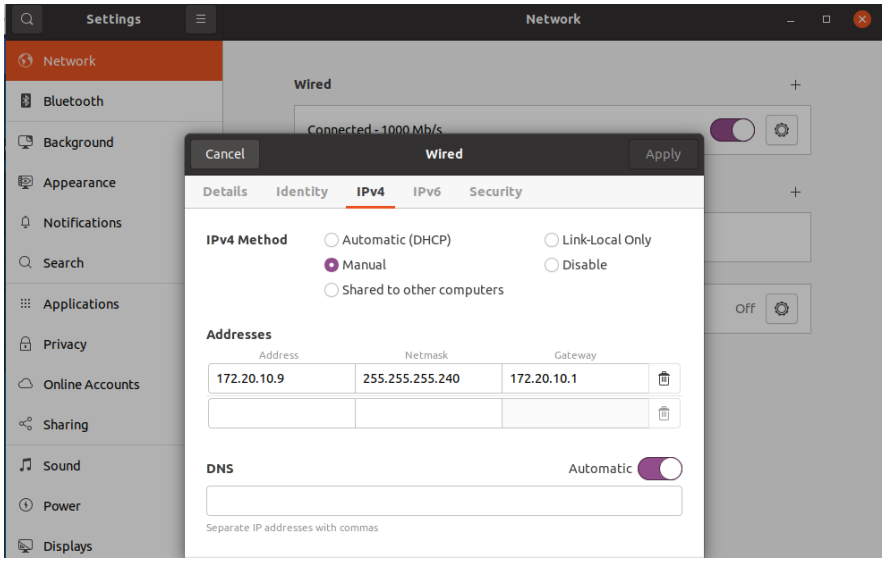
- Installing Zabbix Agent2:

*sudo apt install zabbix-agent2 zabbix-agent2-plugin-**

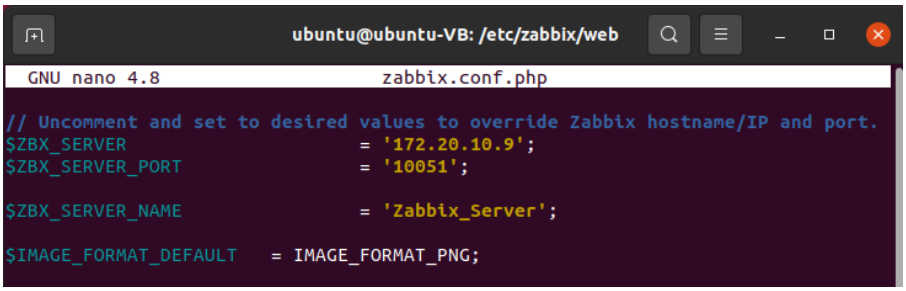
```
┌──(kali㉿kali)-[~]
└─$ sudo apt install zabbix-agent2 zabbix-agent2-plugin-*
[sudo] password for kali:
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
Note, selecting 'zabbix-agent2-plugin-mongodb' for glob 'zabbix-agent2-plugin
-*'
Note, selecting 'zabbix-agent2-plugin-postgresql' for glob 'zabbix-agent2-plu
gin-*'
The following additional packages will be installed:
  libssl1.1
The following NEW packages will be installed:
  libssl1.1 zabbix-agent2 zabbix-agent2-plugin-mongodb
  zabbix-agent2-plugin-postgresql
0 upgraded, 4 newly installed, 0 to remove and 700 not upgraded.
Need to get 11.1 MB of archives.
After this operation, 36.4 MB of additional disk space will be used.
```

2.3 CONFIGURATION

A. Set the static IP for Zabbix server

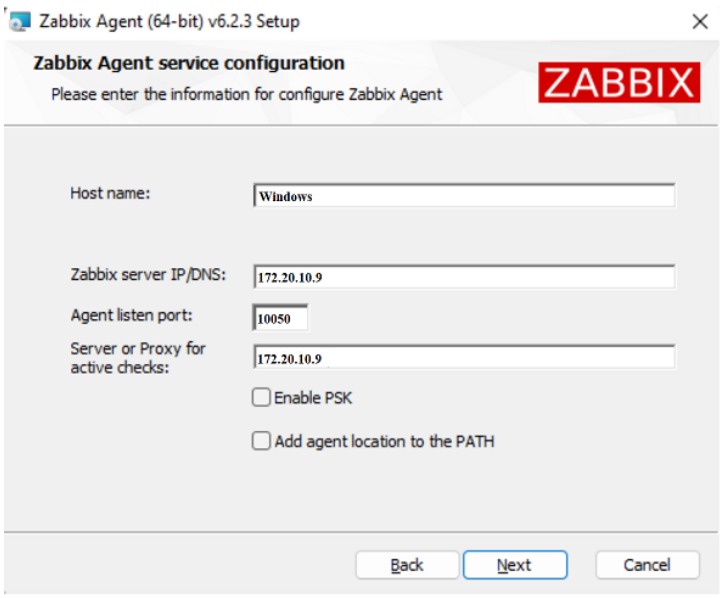


Edit the IP of Zabbix server in /etc/zabbix/web/zabbix.conf.php file



B. Set IP's server for Zabbix Agent on Windows

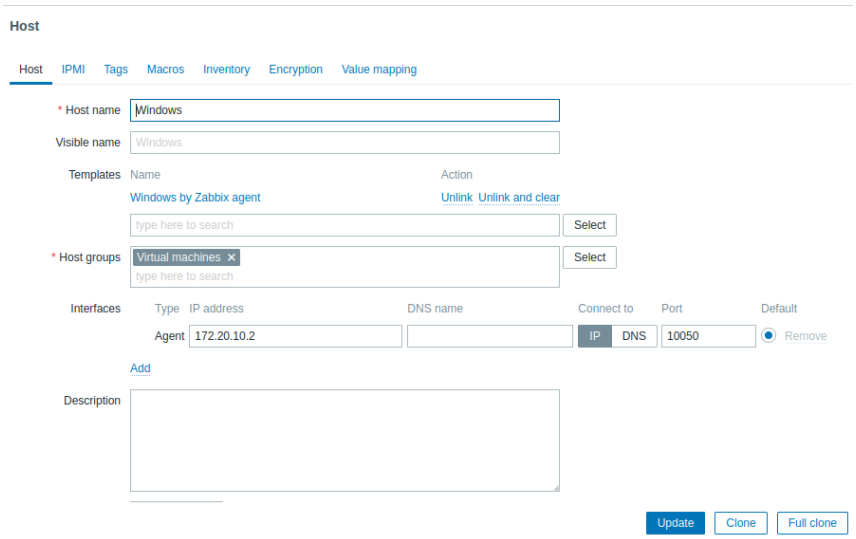
- At first, we ran the Zabbix server and checked the server and agent's IP. Make sure that Zabbix server was running.
- Filling in Zabbix server's IP



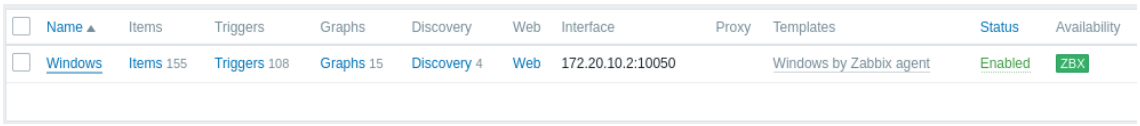
- After this process had been finished, allowing the Zabbix agent to run through the Windows firewall.

C. Add Windows host to Zabbix

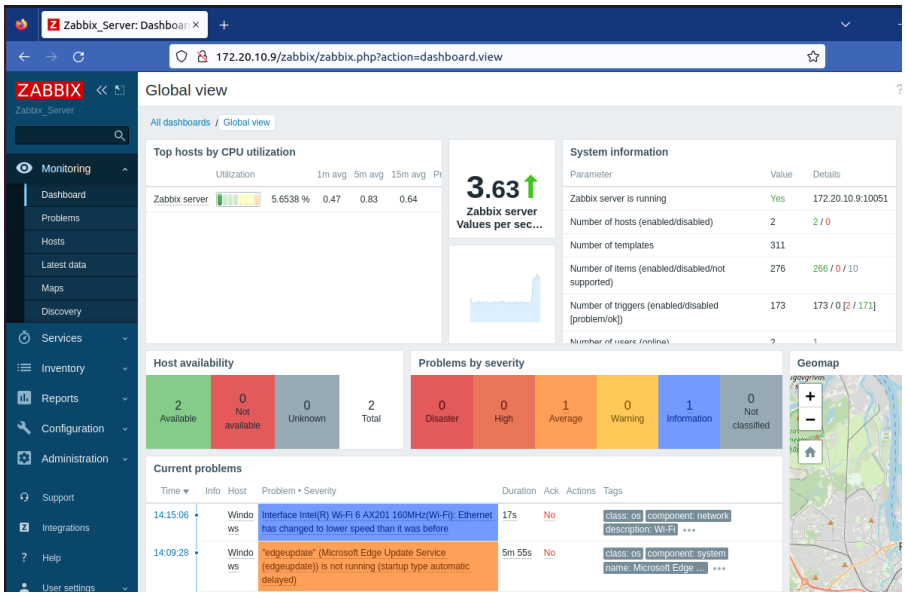
- Creating the host



- Waiting for “Availability” to turn green



- Added successfully with 2 host available



D. Configure Linux's IP

- After installing Zabbix Agent 2 successfully, we need to edit the /etc/zabbix/zabbixagent2.conf file to change the Zabbix server's IP, default Zabbix server's IP and host name.

  Server = 172.20.10.9

  ServerActive = 172.20.10.9

  Hostname = kali

- **Starting Zabbix Agent 2 process:**

  systemctl restart zabbix-agent2

  systemctl enable zabbix-agent2

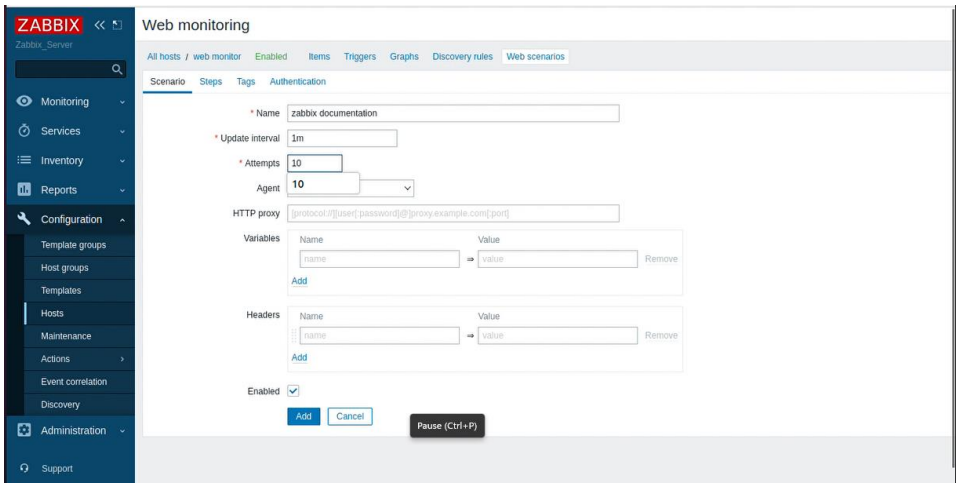
```
┌──(kali㉿kali)-[~]
└─$ systemctl restart zabbix-agent2

┌──(kali㉿kali)-[~]
└─$ systemctl enable zabbix-agent2
Synchronizing state of zabbix-agent2.service with SysV service script with /lib/systemd
/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable zabbix-agent2
```

- Checking if Zabbix Agent 2 is running :

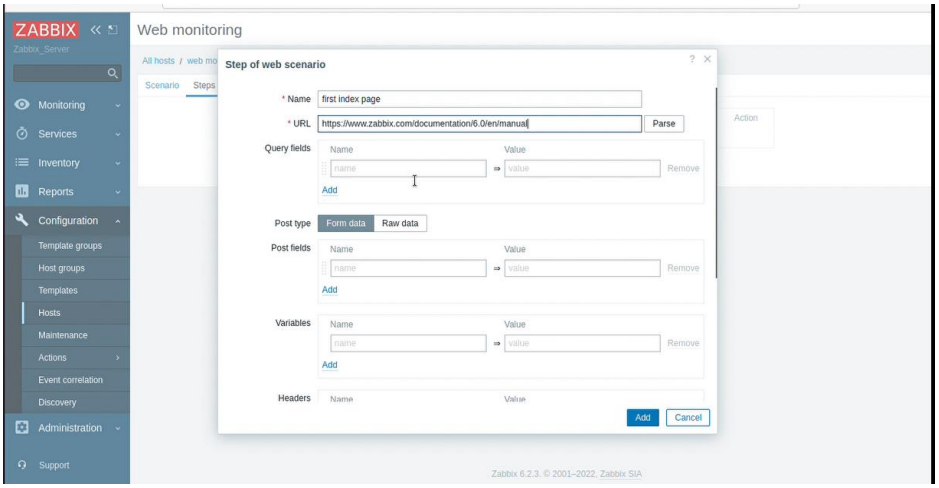
```
┌──(kali㉿kali)-[~]
└─$ sudo netstat -ltnunp
[sudo] password for kali:
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Pro
gram name
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      712/ssh
d: /usr/sbin
tcp6       0      0 :::22                   :::*                    LISTEN      712/ssh
d: /usr/sbin
tcp6       0      0 :::80                   :::*                    LISTEN      803/apa
che2
tcp6       0      0 :::10050                :::*                    LISTEN      2732/za
bbix_agent2
```

E. Configure the web scenario

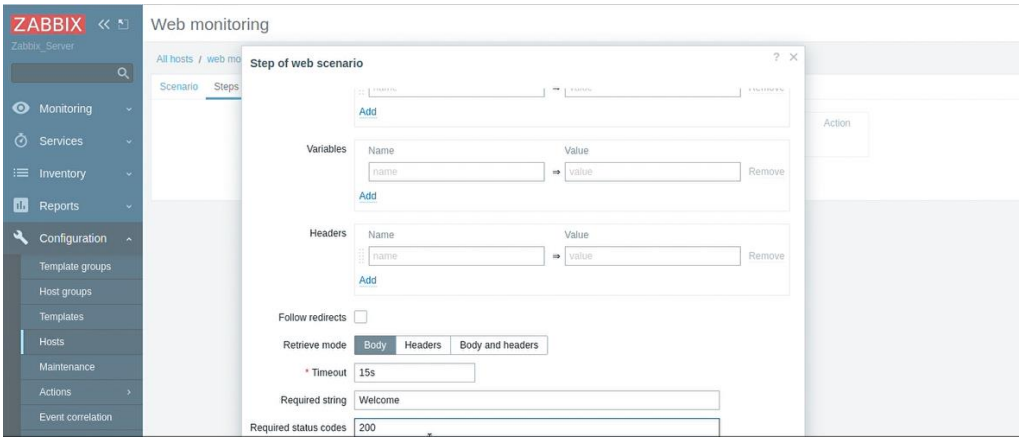
- Creating the host and web scenarios.



- Then, adding a new step to monitor the website. Every step follows an url



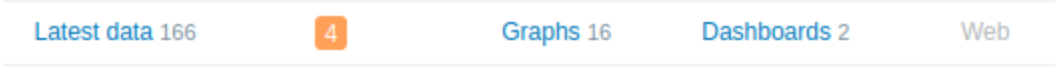
- Using required string and required status code to check if the response packet include that string and its status or not



III. RESULT AND CONCLUSION

A. Windows:

Checking any following data “Monitoring” => “Host” :



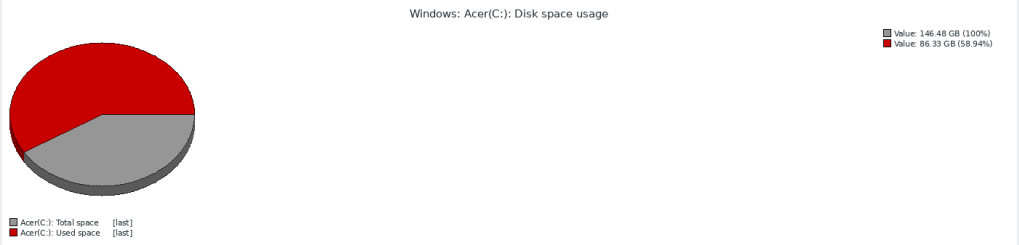
Latest data after a period of time:

Windows	Acer(C:): Used space			component: storage filesystem: C:	Graph
Windows	Cache bytes			component: memory	Graph
Windows	Context switches per second			component: cpu	Graph
Windows	CPU DPC time			component: cpu	Graph
Windows	CPU interrupt time			component: cpu	Graph
Windows	CPU privileged time			component: cpu	Graph
Windows	CPU queue length			component: cpu	Graph
Windows	CPU user time			component: cpu	Graph
Windows	CPU utilization			component: cpu	Graph
Windows	DATA(D:): Space utilization			component: storage filesystem: D:	Graph
Windows	DATA(D:): Total space			component: storage filesystem: D:	Graph
Windows	DATA(D:): Used space			component: storage filesystem: D:	Graph
Windows	Free swap space	5s	666.67 MB	component: memory component: storage	Graph
Windows	Free swap space in %			component: memory component: storage	Graph
Windows	Free system page table entries			component: memory	Graph
Windows	Host name of Zabbix agent running			component: system	History
Windows	Interface Intel(R) Wi-Fi 6 AX201 160MHz(Wi-Fi): Bits received			component: network description: Wi-Fi interface: Intel(R) Wi-...	Graph
Windows	Interface Intel(R) Wi-Fi 6 AX201 160MHz(Wi-Fi): Bits sent			component: network description: Wi-Fi interface: Intel(R) Wi-...	Graph

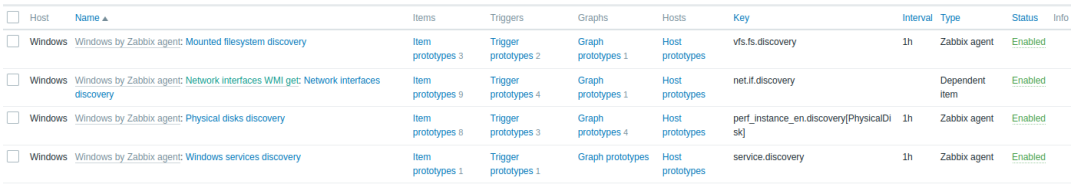
Problems:

Time	Severity	Recovery time	Status	Info	Host	Problem	Duration	Ack	Actions	Tags
13:06:07	Average		PROBLEM		Windows	Zabbix agent is not available (for 3m)	8h 25m 33s	No		class: os component: system scope: availability •••
Today										
2022-11-21 12:07:21	Average		PROBLEM		Windows	"webthreatdefusersvc_44569" (webthreatdefusersvc_44569) is not running (startup type automatic)	2d 9h 24m	No		class: os component: system name: webthreatdefus... •••
2022-11-21 12:07:20	Average		PROBLEM		Windows	"cbdhsvc_44569" (cbdhsvc_44569) is not running (startup type automatic delayed)	2d 9h 24m	No		class: os component: system name: cbdhsvc_44569 •••
2022-11-18 14:09:28	Average		PROBLEM		Windows	"edgeupdate" (Microsoft Edge Update Service (edgeupdate)) is not running (startup type automatic delayed)	5d 7h 22m	No		class: os component: system name: Microsoft Edge ... •••

Graphs of disk space usage for example:



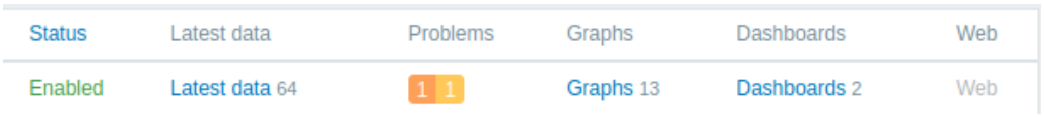
Discovery rules in host configuration that can be modified as need in "Configuration" => "Host" => "Discovery"



Host	Name ▲	Items	Triggers	Graphs	Hosts	Key	Interval	Type	Status	Info
Windows	Windows by Zabbix agent: Mounted filesystem discovery	Item prototypes 3	Trigger prototypes 2	Graph prototypes 1	Host prototypes	vfs.fs.discovery	1h	Zabbix agent	Enabled	
Windows	Windows by Zabbix agent: Network interfaces WMI get: Network interfaces discovery	Item prototypes 9	Trigger prototypes 4	Graph prototypes 1	Host prototypes	net.if.discovery		Dependent item	Enabled	
Windows	Windows by Zabbix agent: Physical disks discovery	Item prototypes 8	Trigger prototypes 3	Graph prototypes 4	Host prototypes	perf_instance_en.discovery[PhysicalDisk]	1h	Zabbix agent	Enabled	
Windows	Windows by Zabbix agent: Windows services discovery	Item prototypes 1	Trigger prototypes 1	Graph prototypes	Host prototypes	service.discovery	1h	Zabbix agent	Enabled	

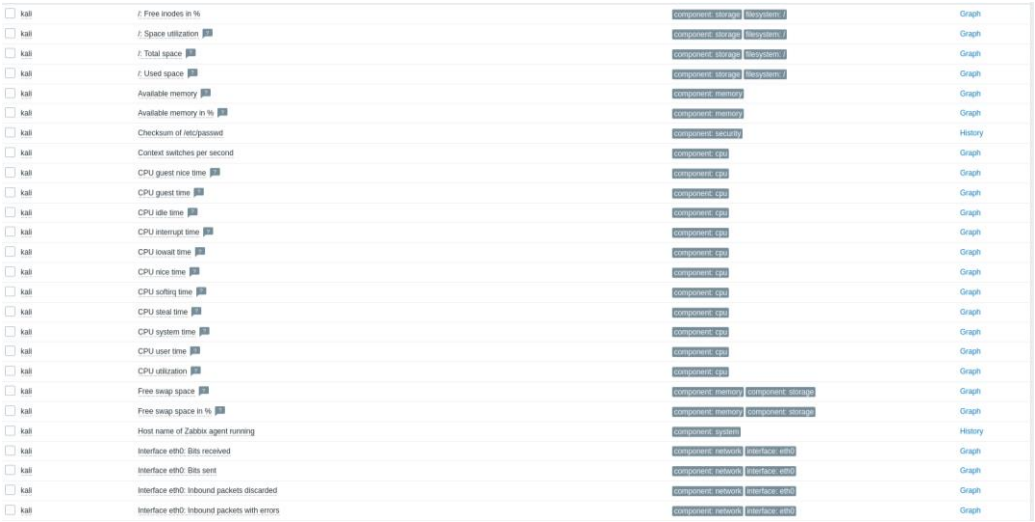
B. Linux:

- Checking any following data: in “Monitoring” => “Host”



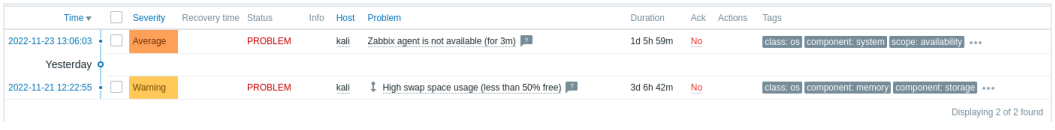
Status	Latest data	Problems	Graphs	Dashboards	Web
Enabled	Latest data 64	1 1	Graphs 13	Dashboards 2	Web

- Latest data after a period of time:



kali	/: Free inodes in %	component: storage filesystem: /	Graph
kali	/: Space utilization	component: storage filesystem: /	Graph
kali	/: Total space	component: storage filesystem: /	Graph
kali	/: Used space	component: storage filesystem: /	Graph
kali	Available memory	component: memory	Graph
kali	Available memory in %	component: memory	Graph
kali	Checksum of /etc/passwd	component: security	History
kali	Context switches per second	component: cpu	Graph
kali	CPU guest nice time	component: cpu	Graph
kali	CPU guest time	component: cpu	Graph
kali	CPU idle time	component: cpu	Graph
kali	CPU interrupt time	component: cpu	Graph
kali	CPU iowait time	component: cpu	Graph
kali	CPU nice time	component: cpu	Graph
kali	CPU softirq time	component: cpu	Graph
kali	CPU steal time	component: cpu	Graph
kali	CPU system time	component: cpu	Graph
kali	CPU user time	component: cpu	Graph
kali	CPU utilization	component: cpu	Graph
kali	Free swap space	component: memory component: storage	Graph
kali	Free swap space in %	component: memory component: storage	Graph
kali	Host name of Zabbix agent running	component: system	History
kali	Interface eth0: Bits received	component: network interface: eth0	Graph
kali	Interface eth0: Bits sent	component: network interface: eth0	Graph
kali	Interface eth0: Inbound packets discarded	component: network interface: eth0	Graph
kali	Interface eth0: Inbound packets with errors	component: network interface: eth0	Graph

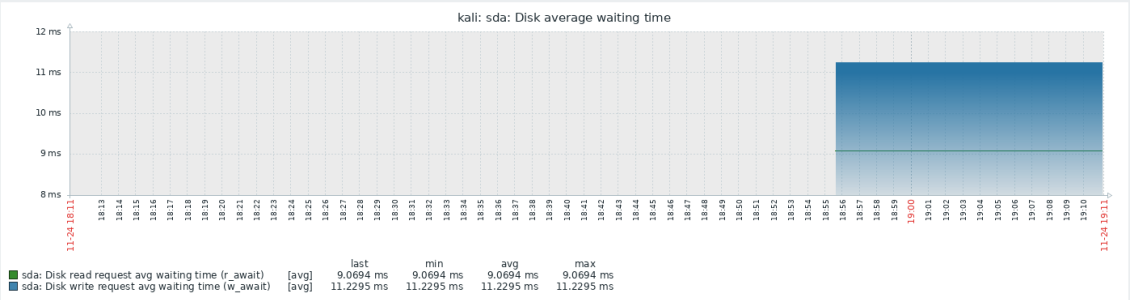
- Problems:



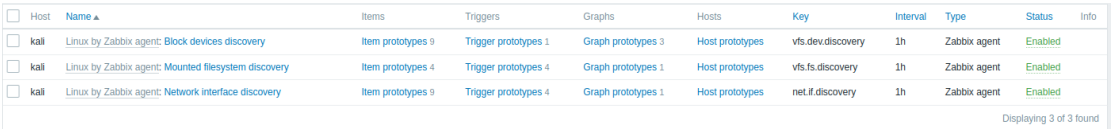
Time ▾	Severity	Recovery time	Status	Info	Host	Problem	Duration	Ack	Actions	Tags
2022-11-23 13:06:03	Average		PROBLEM		kali	Zabbix agent is not available (for 3m)	1d 5h 59m	No		class: os component: system scope: availability •••
Yesterday										
2022-11-21 12:22:55	Warning		PROBLEM		kali	High swap space usage (less than 50% free)	3d 6h 42m	No		class: os component: memory component: storage •••

Displaying 2 of 2 found

- Graphs of disk average waiting time for example:



- Discovery rules in host configuration that can be modified as need in "Configuration" => "Host" => "Discovery":



Host	Name ▲	Items	Triggers	Graphs	Hosts	Key	Interval	Type	Status	Info
kali	Linux by Zabbix agent: Block devices discovery	Item prototypes 9	Trigger prototypes 1	Graph prototypes 3	Host prototypes	vfs.dev.discovery	1h	Zabbix agent	Enabled	
kali	Linux by Zabbix agent: Mounted filesystem discovery	Item prototypes 4	Trigger prototypes 4	Graph prototypes 1	Host prototypes	vfs.fs.discovery	1h	Zabbix agent	Enabled	
kali	Linux by Zabbix agent: Network interface discovery	Item prototypes 9	Trigger prototypes 4	Graph prototypes 1	Host prototypes	net.if.discovery	1h	Zabbix agent	Enabled	

Displaying 3 of 3 found

C. Web:

If running by the right way, after receiving the response from the web server, it will show the download speed, response time, status and response code

Step	Speed	Response time	Response code	Status
first index page	39.69 KBps	390.92ms	200	OK
second index page	62.98 KBps	238.66ms	200	OK
TOTAL		**629.58ms**		OK

D. Conclusion

Zabbix is free, easy to install, configure with pre-built templates and supports a user-friendly web interface.

IV. APPENDIX

1. TASK

Member	Task
Truong Thi Hoang Hao - 20520191	Set up Zabbix Server; Monitor Windows
Tran Thuy Anh - 20521085	Set up Zabbix client; Monitor Linux
Le Quang Minh - 20520245	Set up Zabbix client; Monitor Web

2. SELF-ASSESSMENT

The project has been done smoothly with the cooperation of all of our team members. The only thing that we couldn't implement is that the email alert function. The "less secure app access" option in Gmail has already been removed since May 30th , 2022. So, it's impossible for us to send emails using Gmail account.

3. ANSWER

----------END----------

Thank you!