VIETNAM NATIONAL UNIVERSITY HO CHI MINH CITY
UNIVERSITY OF INFORMATION TECHNOLOGY
COURSE K15

TRẦN HOÀI RIN - 20521830
LÊ TRỌNG NHÂN – 20521695
LÊ HOÀNG CAO NGUYÊN - 20521672

FINAL REPORT
MONITORING SYSTEM USING NAGIOS CORE AND NAGIOS XI

INFORMATION SECURITY STUDENTS

INSTRUCTOR

TRẦN THỊ DUNG

TP. HỒ CHÍ MINH, 06/01/2023

Table of content

Table of contents

1 INTRODUCTION

1.1 Nagios

Nagios Core

Nagios Core serves as the basic event scheduler, event processor, and alert manager for elements that are monitored

Plugins are standalone extensions to Nagios Core that make it possible to monitor anything and everything with Core.

Nagios XI

Nagios XI is an extended interface of Nagios Core, intended as the enterprise-level version of the monitoring tool. XI acts as monitoring software, configuration manager and toolkit. Nagios XI monitors IT infrastructure components such as applications, OSes, networks and system metrics.

Plug-ins are supported for these infrastructure components to expand on XI's monitoring capabilities. The powerful Nagios Core 4 monitoring engine provides users with the highest degree of monitoring server performance.

1.2 Component

The Nagios server is installed on server (VM1). Then we need two clients use different OS such as Window OS and Linux to monitor.

1.3 Operation

To monitor a machine by Nagios, it requires our team to install NCPA - a single monitoring agent that can be installed on all major operating systems. NCPA allows both active checks via check_ncpa.py and passive checks via NRDP. NCPA comes with a built-in web GUI, documentation, websocket graphing, and is secured with SSL by default.

By default, the agent uses http(s) protocol, port 80 and 443 to move data. Besides, it uses snmp ports 161 and 162 to monitor webisites (161 to send requests and 162 to receive results). Nagios Plugins also uses some common ports like NRPE 5666; NSCA 5667; NCPA 5693; MSSQL 1433; MySQL 3306; OracleDB 1521; Email(SMTP) 25, 465, 587.

One of the core components in NCPA is the Web GUI. Using the Web GUI, we can browse the API, read the docs, view system information, configure, and generate graphs.
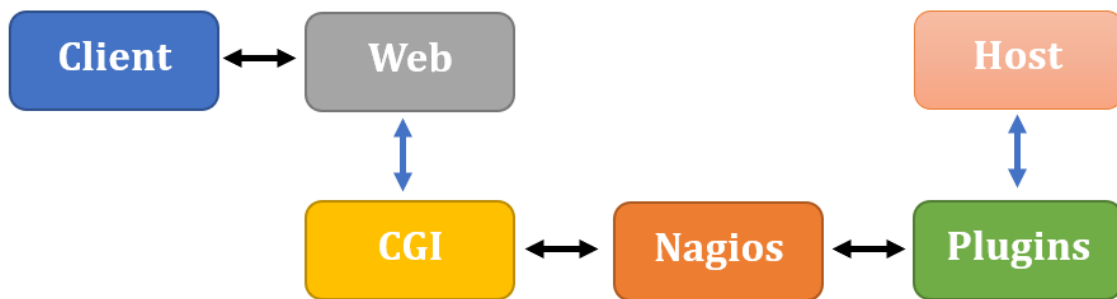
An agent lives on a network element like a Linux server. Nagios reaches out to the agent to check various stats such as drive space, RAM, CPU usage, etc. The agent collects the requested information and responds back to Nagios. Nagios first stores the information for later reports, historical charts, and graphing and then the other action it can take is to generate an alert. With the alert, the stats the agent returns may be representing a drive that's too full or some other state and the generated alert is how we will know about the potential issue.

2   IMPLEMENTATION

2.1   Topology

Nagios Core:
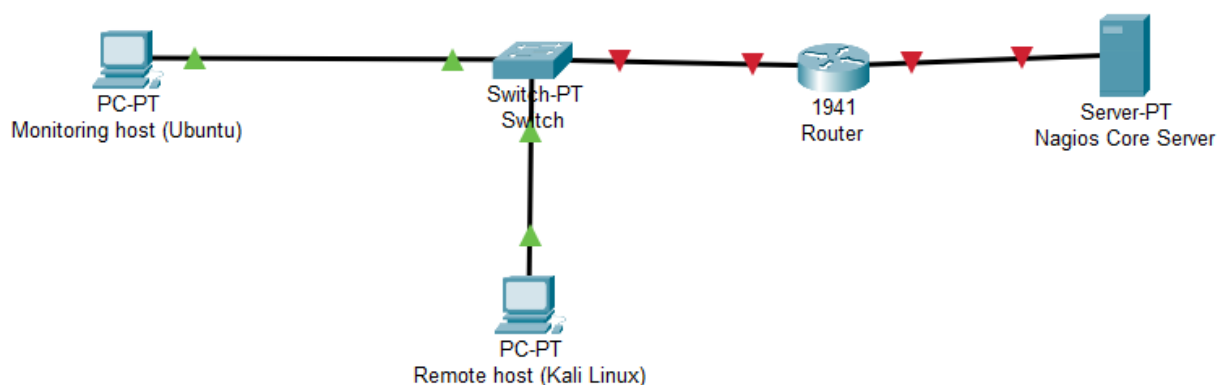
Nagios XI

Name	IP	Netmask
VM1(Nagios Sever)	192.168.91.134	255.255.255.0
VM2(Linux client)	192.168.91.233	255.255.255.0
Laptop (Window client)	192.168.1.7	255.255.255.0
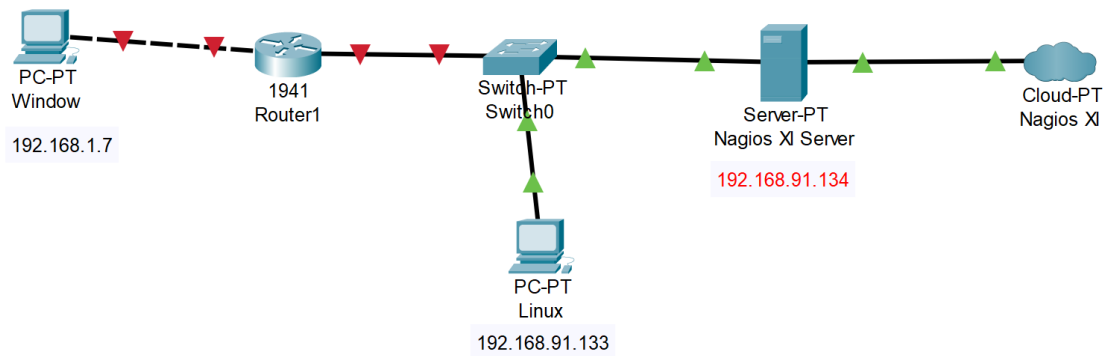
2.2   Installation

Nagios Core

Nagios core is needed for both Window and Linux monitor
- Step 1: Install the pre-requisite packages.
  - ➢ sudo apt-get update
  - ➢ sudo apt-get install -y autoconf gcc libc6 make wget unzip apache2 php libapache2-mod-php7.4 libgd-dev
  - ➢ sudo apt-get install openssl libssl-dev
- Step 2: Downloading the Source.
  - ➢ cd /tmp
  - ➢ wget -O nagioscore.tar.gz https://github.com/NagiosEnterprises/nagioscore/archive/nagios-4.4.6.tar.gz
  - ➢ tar xzf nagioscore.tar.gz
- Step 3: Compile.
  - ➢ cd /tmp/nagioscore-nagios-4.4.6/
  - ➢ sudo ./configure --with-httpd-conf=/etc/apache2/sites-enabled
  - ➢ sudo make all
- Step 4: Create user and group.
  - ➢ sudo make install-groups-users
  - ➢ sudo usermod -a -G nagios www-data
- Step 5: Install binaries.
  - ➢ sudo make install
- Step 6: Install service /Daemon.
  - ➢ sudo make install-daemoninit
- Step 7: Install command mode.
  - ➢ sudo make install-commandmode
- Step 8: Install configuration files.
  - ➢ sudo make install-config
- Step 9: Install apache config files.
  - ➢ sudo make install-webconf
  - ➢ sudo a2enmod rewrite
  - ➢ sudo a2enmod cgi

- Step 10: Configure firewall.
  - ➢ sudo ufw allow Apache
  - ➢ sudo ufw reload
- Step 11: Create admin account.
  - ➢ sudo htpasswd -c /usr/local/nagios/etc/htpasswd.users nagiosadmin
- Step 12: Start Apache web server.
  - ➢ sudo systemctl restart apache2.service
- Step 13: Start service /Daemon.
  - ➢ sudo systemctl start nagios.service

2.2.1.1 Monitoring Window OS

- Step 1: Take the newest version of NSClient++ on the official website: https://nsclient.org/

- Step 2: Choose x64

All files:

- Step 3:

- Step 4: Click next
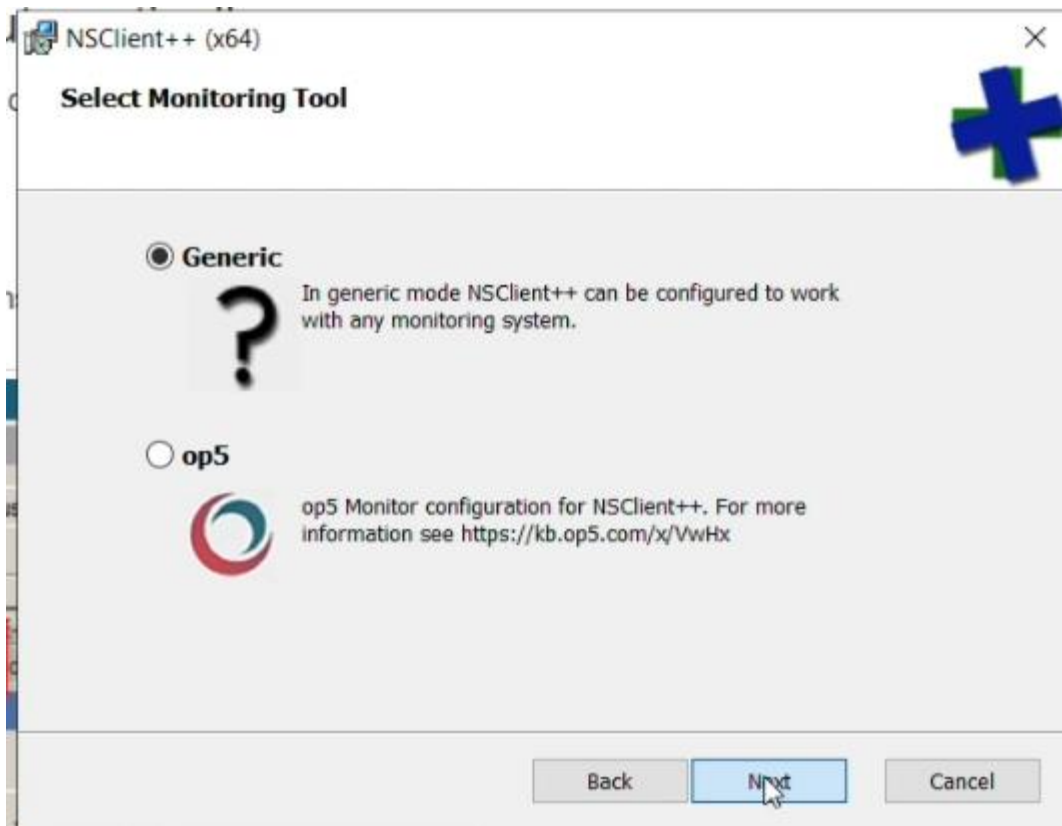
- Step 5: Click Typical
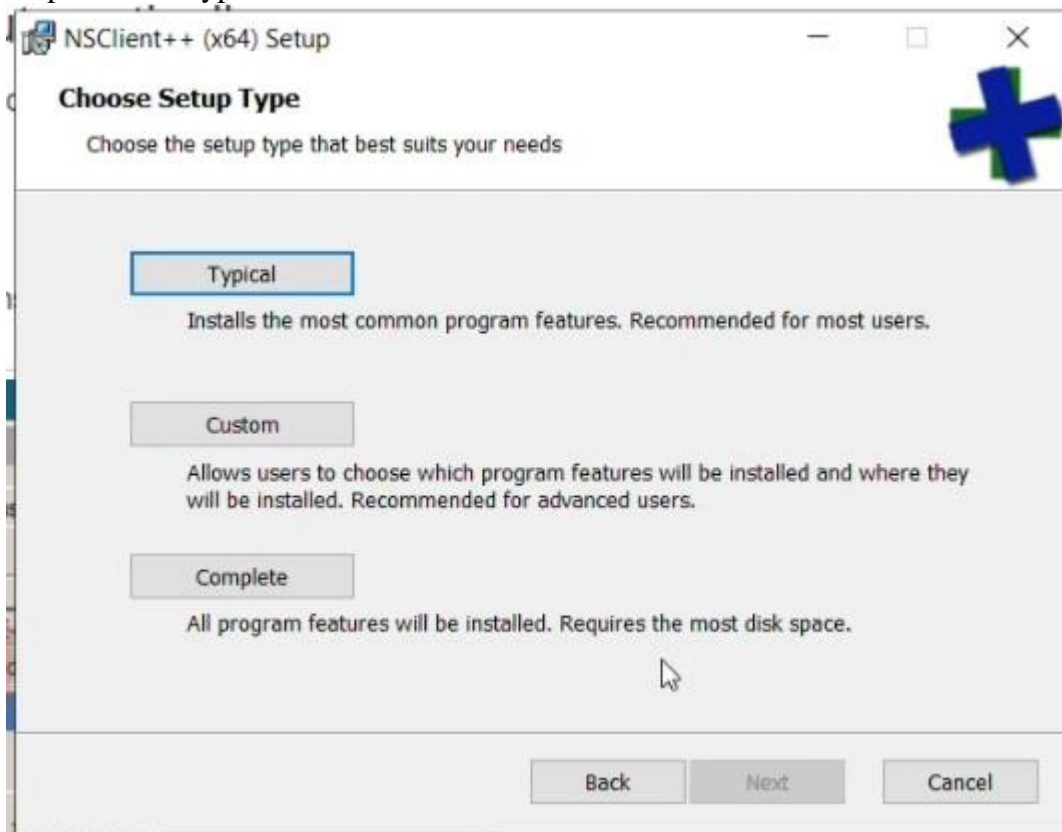
- Step 6:
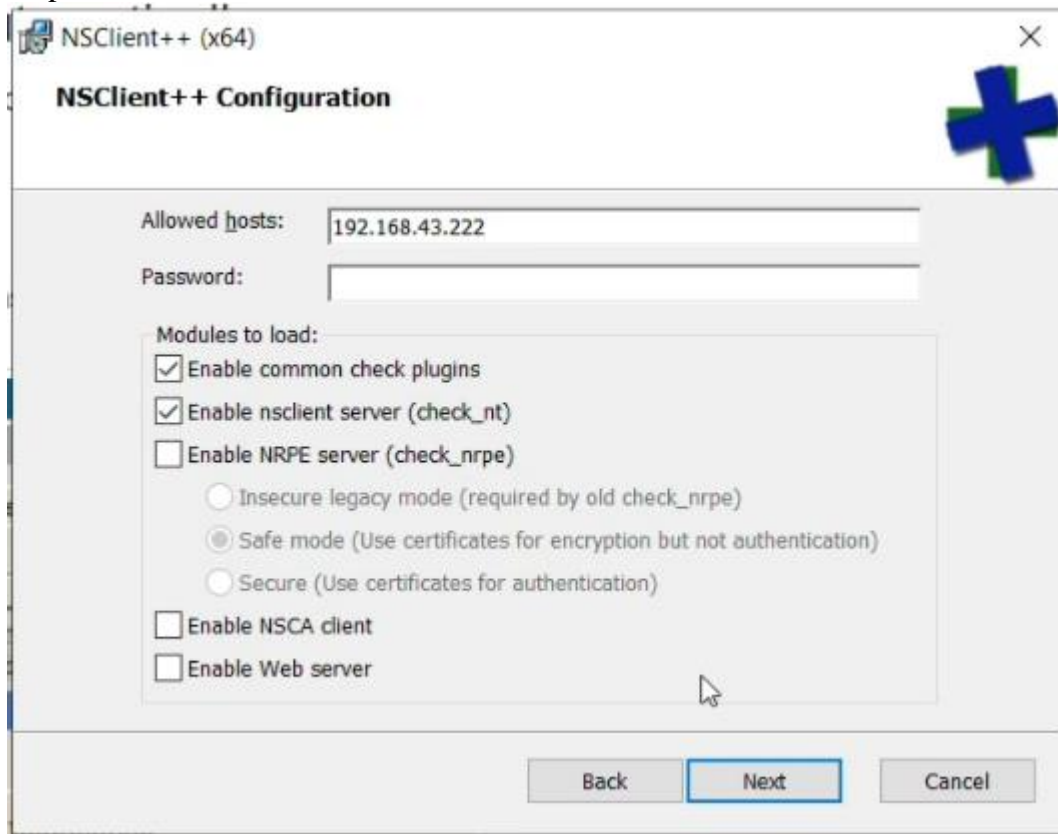
- Step 7: Click Next, Click Install

2.2.1.2 Monitoring Linux (Ubuntu 20.x)

INSTALL PLUGINS
- Step 1: Install the prerequisite packages.
  - ➢ sudo apt-get install -y autoconf gcc libc6 libmcrypt-dev make libssl-dev wget bc gawk dc build-essential snmp libnet-snmp-perl gettext
- Step 2: Download the source.
  - ➢ cd /tmp
  - ➢ wget --no-check-certificate -O nagios-plugins.tar.gz https://github.com/nagios-plugins/nagios-plugins/archive/release-2.3.3.tar.gz
  - ➢ tar zxf nagios-plugins.tar.gz
- Step 3: Compile + Install.
  - ➢ cd /tmp/nagios-plugins-release-2.3.3/
  - ➢ sudo ./tools/setup
  - ➢ sudo ./configure
  - ➢ sudo make
  - ➢ sudo make install

INSTALL NRPE
- sudo apt update && apt upgrade
- sudo apt install nagios-nrpe-server nagios-plugins

Nagios XI

- Step 1: Take the newest version of Nagios XI on the official website: https://www.nagios.com/downloads/nagios-xi/microsoft/
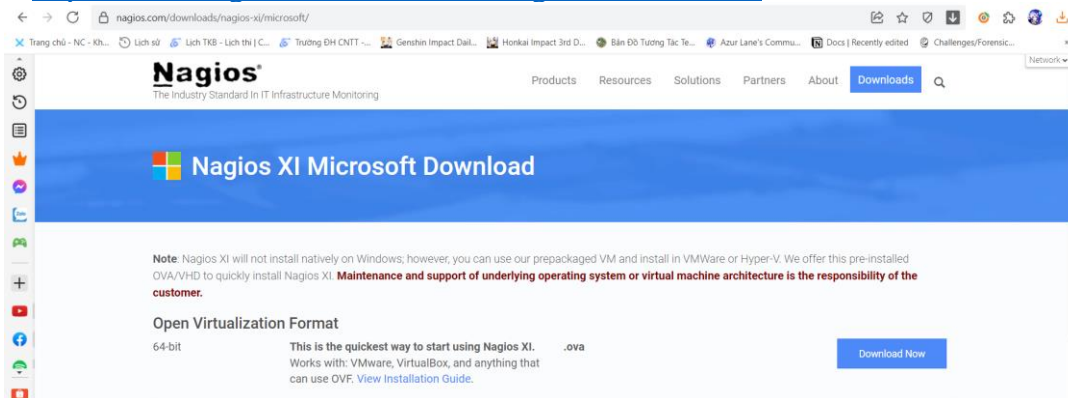
- Step 2: Installing VMware or Virtual Box to install the application.
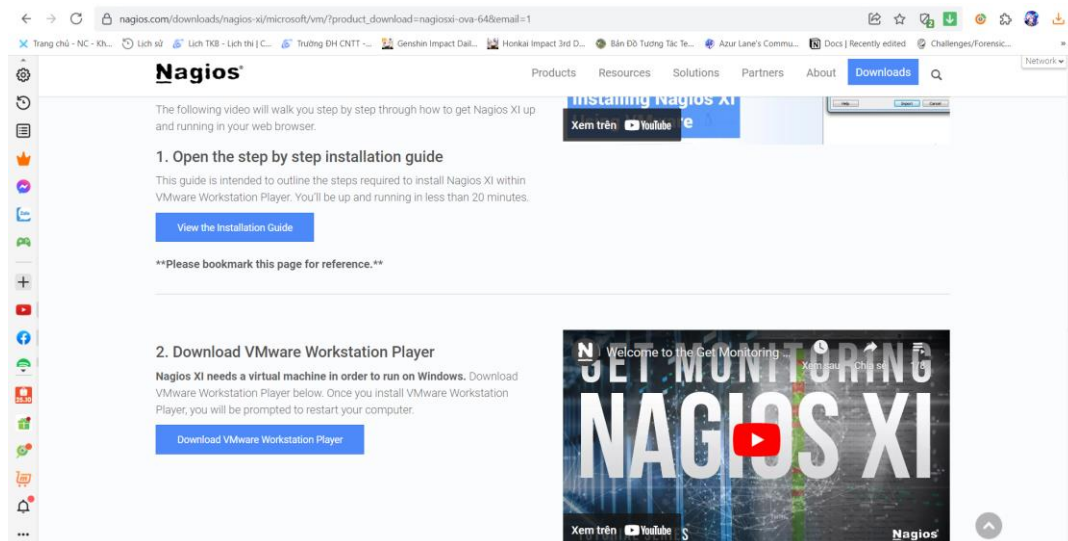
- Step 3: In VMware main board, choose "Open a Virtual Machine" then choose file downloaded from website
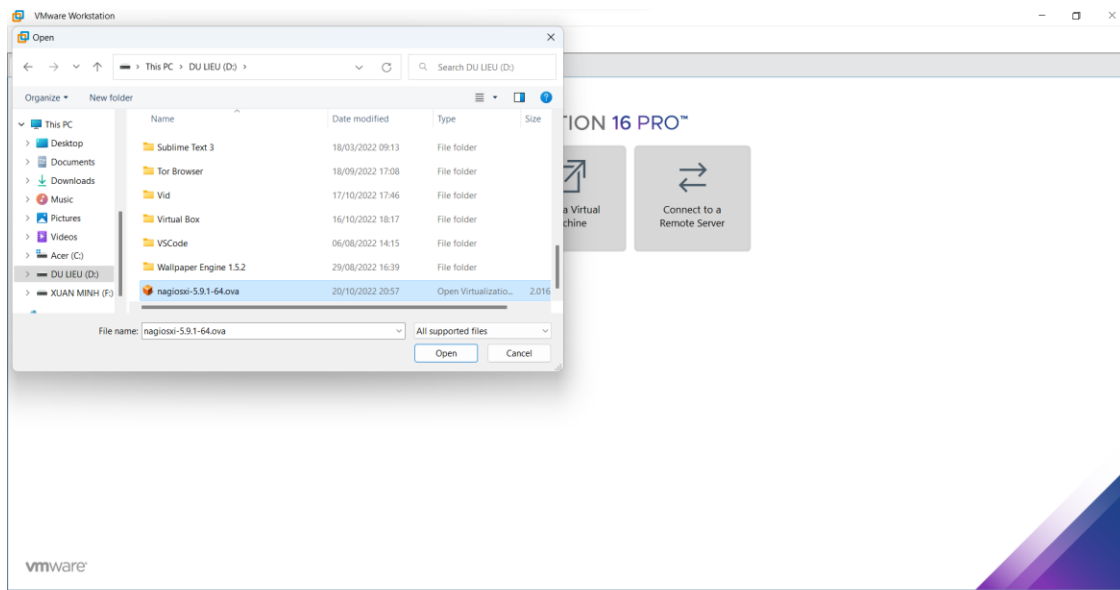
- Step 4: Set name, location for the app then turn on the virtual machine and Nagios XI will be installed automatically
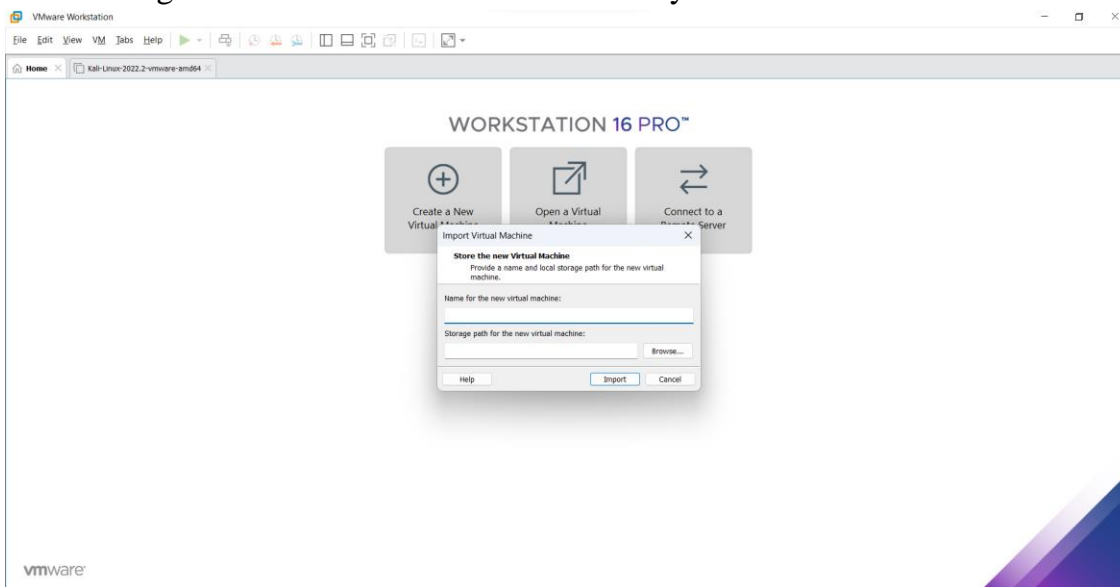
- Step 5: Take the address http://192.168.247.128 and use web browser to access admin panel
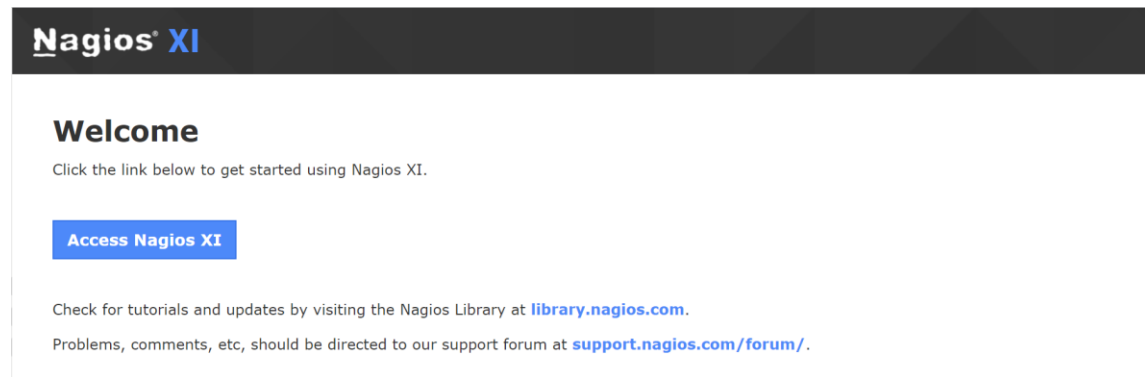
- Step 6: Choose Acces Nagios XI then create account to login:
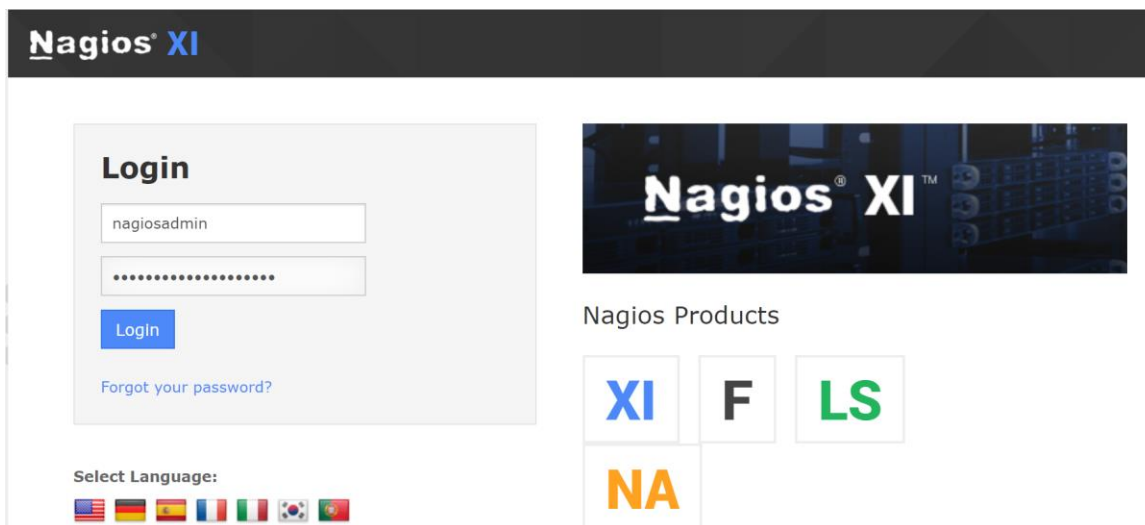
Now we can begin set up to monitor our system
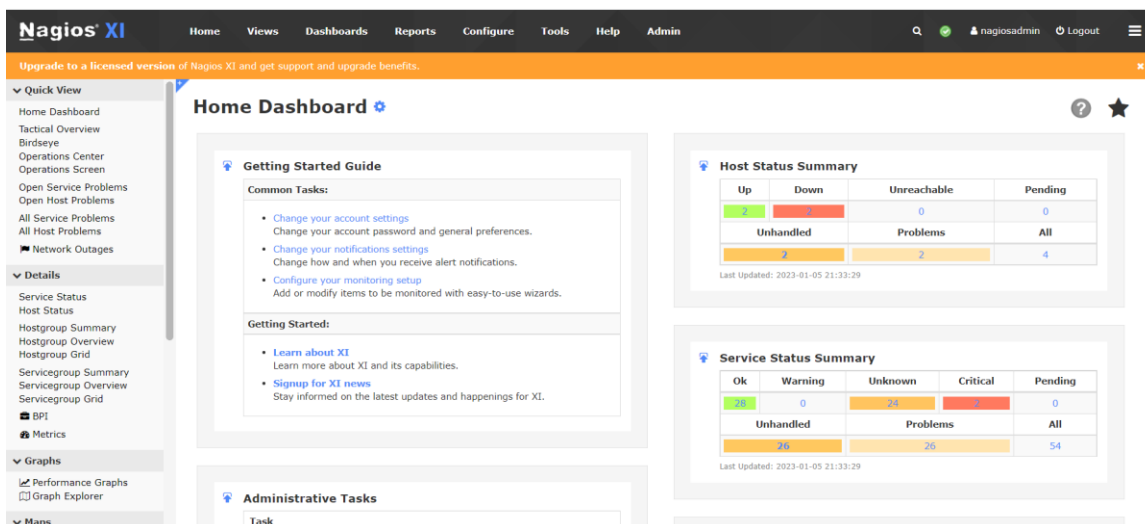
2.3   Configuration

Nagios Core

2.3.1.1 Monitoring Window OS

- Step 1: Open file name nagios.cfg in /user/local/nagios/etc/. Go to line 38 and configuration like this

```
30 cfg_file=/usr/local/nagios/etc/objects/contacts.cfg
31 cfg_file=/usr/local/nagios/etc/objects/timeperiods.
32 cfg_file=/usr/local/nagios/etc/objects/templates.cf
33
34 # Definitions for monitoring the local (Linux) host
35 cfg_file=/usr/local/nagios/etc/objects/localhost.cf
36
37 # Definitions for monitoring a Windows machine
38 cfg_file=/usr/local/nagios/etc/objects/windows.cfg
39
40 # Definitions for monitoring a router/switch
41 #cfg_file=/usr/local/nagios/etc/objects/switch.cfg
42
43 # Definitions for monitoring a network printer
44 #cfg_file=/usr/local/nagios/etc/objects/printer.cfg
45
46
47 # You can also tell Nagios to process all config fi
48 # extension) in a particular directory by using the
49 # directive as shown below:
```

- Step 2: Open file name Windows.cfg in /user/local/nagios/etc/objects/. Go to line 26 and replace window IPaddress into it

```
9
10
11
12 ##############################################################################
13 #
14 # HOST DEFINITIONS
15 #
16 ##############################################################################
17
18 # Define a host for the Windows machine we ll be monitoring
19 # Change the host_name, alias, and address to fit your situation
20
21 define host {
22
23     use                windows-server        ; Inherit default values from a template
24     host_name          winserver             ; The name we re giving to this host
25     alias              My Windows Server     ; A longer name associated with the host
26     address            192.168.43.214        ; IP address of the host
27 }
28
29
30
31 ##############################################################################
32 #
33 # HOST GROUP DEFINITIONS
34 #
35 ##############################################################################
36
```

- Step 3: restart nagios service

```
┌──(kali㊀kali)-[~/Desktop]
└─$ service nagios restart
▯
```

- Step   4: Back to window. Run notepad as Administrator to Edit file C:\ProgramFiles\NSClient++\nsclient.ini

```
[; ........]

; Undocumented key
CheckExternalScripts = disabled

; Undocumented key
CheckHelpers = disabled

; Undocumented key
CheckEventLog = disabled

; Undocumented key
CheckNSCP = disabled

; Undocumented key
CheckDisk = disabled

; Undocumented key
CheckSystem = disabled

; Undocumented key
NSClientServer = enabled
```

- Step   4: replace "disabled" to "1" then save the file

```
[/modules]

; Undocumented key
CheckExternalScripts = 1

; Undocumented key
CheckHelpers = 1

; Undocumented key
CheckEventLog = 1

; Undocumented key
CheckNSCP = 1

; Undocumented key
CheckDisk = 1

; Undocumented key
CheckSystem = 1

; Undocumented key
NSClientServer = enabled
```

- Result:
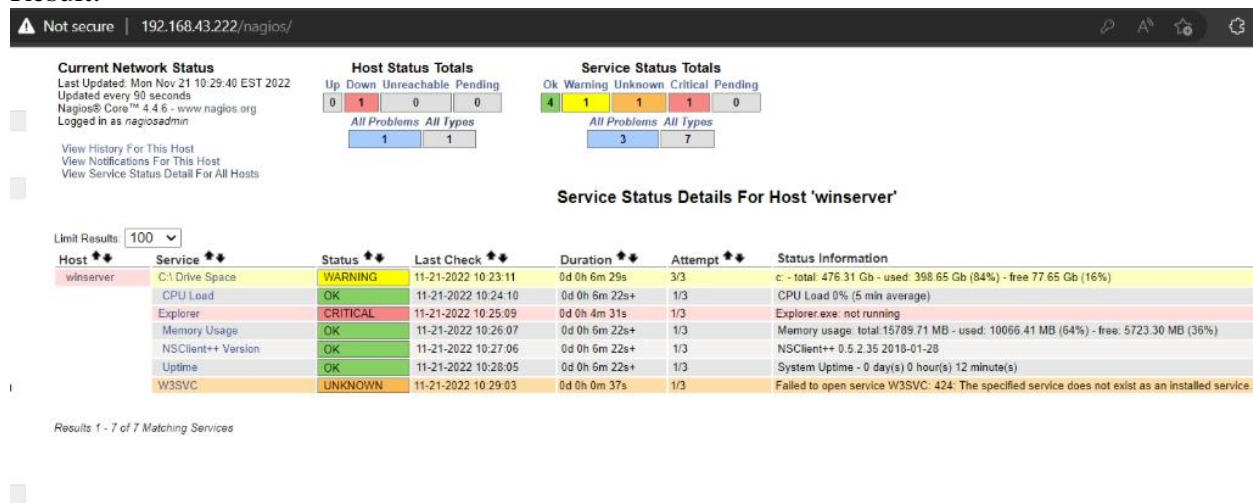
2.3.1.2 Monitoring Linux

CONFIGURE NRPE ON REMOTE HOST
- Step 1: Edit the NRPE configuration file /etc/nagios/nrpe.cfg
  - ➢ sudo nano /etc/nagios/nrpe.cfg
  - ➢ allowed_hosts=127.0.0.1, [IP of monitoring host]
  - ➢ sudo systemctl restart nagios-nrpe-server
- Step 2: Verify connections (on monitoring host)
  - ➢ check_nrpe -H [IP of remote host]

DEFINE HOSTS AND SERVICES ON MONITORING HOST
- Step 1: Define host.
    define host{

15

```
            host_name        host_name
            addressaddress
            max_check_attempts  #
            check_period  timeperiod_name
            contacts            contacts
            contact_groups          contact_groups
            notification_interval  #
            notification_period     timeperiod_name
    }
```
- Step 2: Define service
```
        define service{
            host_name        host_name
            service_description     service_description
            check_command           command_name
            max_check_attempts  #
            check_interval#
            retry_interval  #
            check_period  timeperiod_name
            notification_interval   #
            notification_period     timeperiod_name
            contacts            contacts
            contact_groups          contact_groups
    }
```

Nagios XI

Before beginning to monitor a system, this system need to be installed the Nagios Agent. Our team use NCPA to monitor. We will split this section to three small one to make it easy to follow.

2.3.1.3 Monitoring Window OS
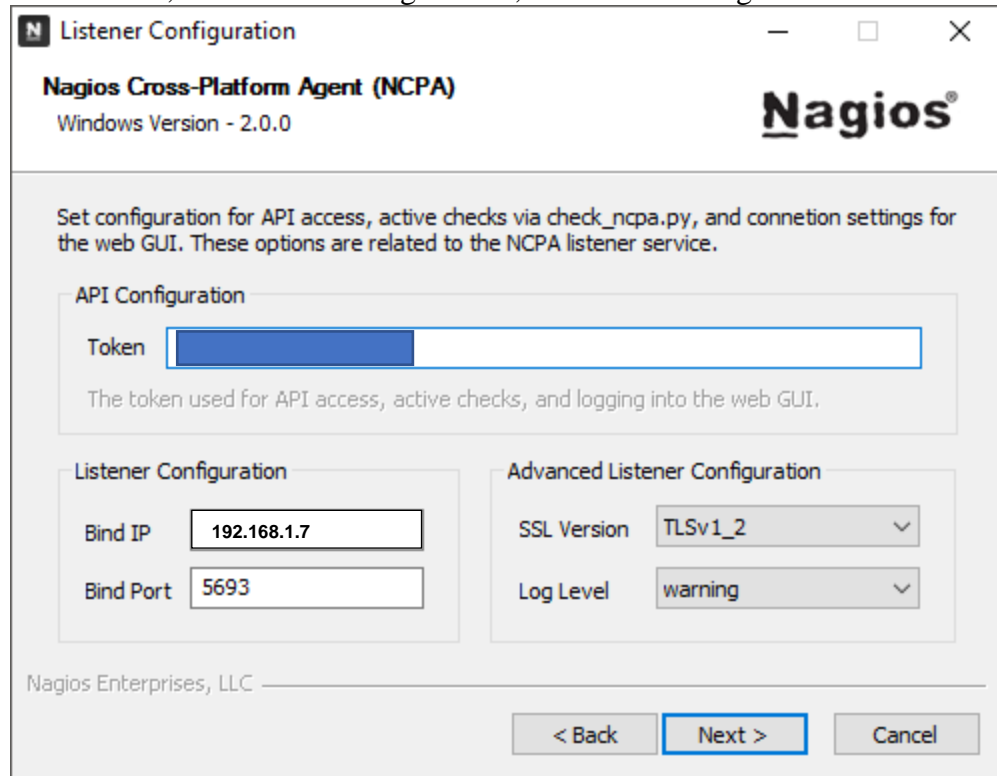
- Step 1: Choose correct version then download and install the agent via https://www.nagios.org/ncpa/
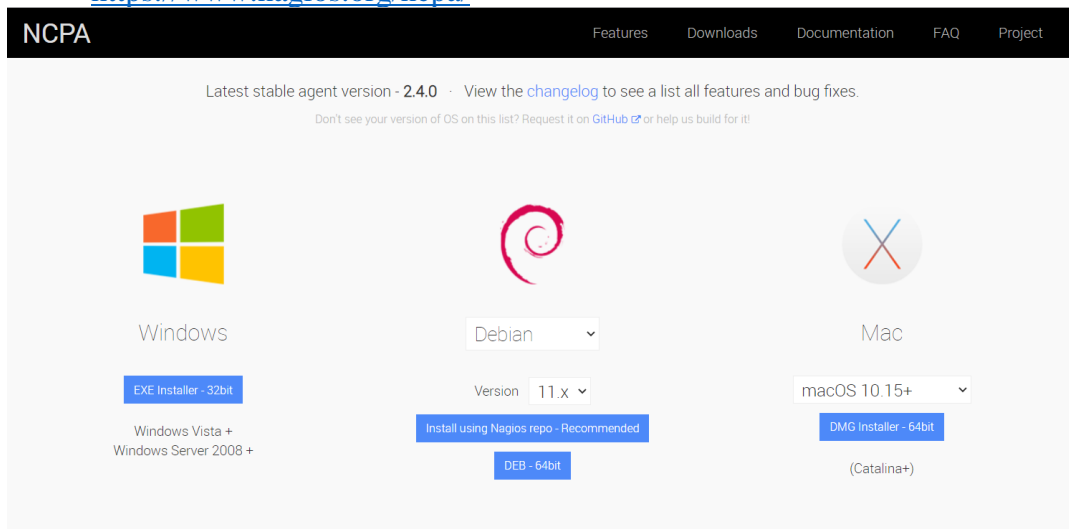
Choose window to get agent for monitoring window. In our group case, we use Kali Linux client so we choose Debian.

On Window OS, after downloading the file, we run it and begin the listener installation:

Token plays a role like password when we configure. Bind IP is IP address of the client, port is the port to transfer data. We let is default here.

- Step 2: After login to the web server, choose configure then configuration wizard
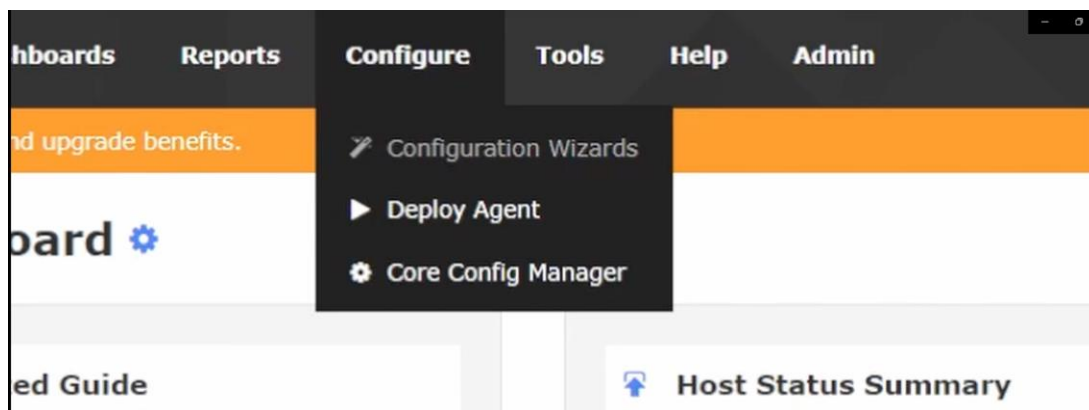
- Step 2: Choose Window then Window Desktop.

- Step 3: Full fill the information and choosing the feature to monitor

Fill IP address, port and token that has been created yet.

Select feature to monitor

- Step 4: Finish the configuration

Configuration Wizard: Windows Desktop - Step 3

Monitoring Settings

Define basic parameters that determine how the host and service(s) should be monitored.

Under normal circumstances:

Monitor the host and service(s) every [5] minutes.

When a potential problem is first detected:

Re-check the host and service(s) every [1] minutes up to [5] times before sending a notification.

[< Back] [Next >] [✔ Finish]

Type the IP address to find client, we can see its information here

Host Status Detail

192.168.1.7

Services

Service Status for this Host   Last updated: 2022-11-20 21:39:22

Service		Status	Duration	Attempt	Last Check	Status Information
Active Telephony Lines		Ok	1h 10m 50s	1/20	2022-11-20 21:28:33	OK: \Telephony\Active Lines was 0.00 Active Lines
Active Terminal Sessions		Ok	1h 9m 29s	1/20	2022-11-20 21:29:33	OK: \Terminal Services\Active Sessions was 1.00 Active Sessions
CPU Usage		Ok	1h 8m 36s	1/20	2022-11-20 21:30:44	OK: Percent was 0.38 %
Disk Usage on C:/		Warning	1h 7m 18s	7/20	2022-11-20 21:31:57	WARNING: Used disk space was 77.90 % (Used: 127.23 GiB, Free: 36.09 GiB, Total: 163.33 GiB)
Disk Usage on D:/		Warning	1h 5m 50s	7/20	2022-11-20 21:33:32	WARNING: Used disk space was 83.00 % (Used: 121.58 GiB, Free: 24.90 GiB, Total: 146.48 GiB)
Disk Usage on F:/		Warning	1h 4m 53s	7/20	2022-11-20 21:34:09	WARNING: Used disk space was 85.60 % (Used: 142.08 GiB, Free: 23.94 GiB, Total: 166.01 GiB)
Ethernet 2 Bandwidth - Inbound		Ok	1h 3m 40s	1/20	2022-11-20 21:35:42	OK: Bytes_recv was 0.00 MB/s
Ethernet 2 Bandwidth - Outbound		Ok	1h 2m 21s	1/20	2022-11-20 21:36:55	OK: Bytes_sent was 0.00 MB/s
Ethernet Bandwidth - Inbound		Ok	1h 1m 20s	1/20	2022-11-20	OK: Bytes_recv was 0.00 MB/s

2.3.1.4   Monitoring Linux

On Linux, it is harder to do this stuff so we will split it to several step.
- Step 1: Install DEB-based Linux using the following command
  sudo dpkg -i ncpa-2.4.0.d10.amd64.deb

```
File  Actions  Edit  View  Help
┌──(kali⊛kali)-[/tmp]
└─$ sudo dpkg -i ncpa-2.4.0.d10.amd64.deb
[sudo] password for kali:
Selecting previously unselected package ncpa.
(Reading database ... 324267 files and directories currently installed.)
Preparing to unpack ncpa-2.4.0.d10.amd64.deb ...
Unpacking ncpa (2.4.0-1) ...
Setting up ncpa (2.4.0-1) ...
Processing triggers for libc-bin (2.36-4) ...
```

- Step 2: By default the token will be set to mytoken so we will change this right away since it allows authentication into the web GUI and access to the API. Access the folder "*/usr/local/ncpa/etc*", open **ncpa.cfg** then change the section **"[api] community_string = <our group token>"**


```
└─$ sudo vim ncpa.config
[sudo] password for kali:

┌──(kali⊛kali)-[/usr/local/ncpa/etc]
└─$ sudo vim ncpa.cfg█
```



```
[api]

#
# The token that will be used to log into the basic
# and to authenticate requests to the API and reque
#
community_string = 123456789█
```

- Step 3: After saving changes, restart the NCPA listener to apply. But in reality, we have to restart the virtual machine to make it change available.
- Step 4: Acording to window configuration, we will skip some step here. Turning to filling information step

Setup NCPA

The agent should be installed before you continue running this wizard.

- Download the latest version of NCPA for the system you would like to monitor
- Follow the installation instructions (PDF version) and configure the token for the agent

Connect to NCPA

Address: 192.168.91.133

The IP address or FQDNS name used to connect to NCPA.

Port: 5693

Port used to connect to NCPA. Defaults to port 5693.

☑ Do not verify SSL certificate

Token: ●●●●●●●●● 👁

Authentication token used to connect to NCPA.

System: Debian ⌄

Used to set the icon for the host.

The Linux client we use is Kali Linux so at the "System" tag, we choose Debian. IP and token is the same as what we do with window.

- Step 5: Choose features to monitor

Specify the metrics you'd like to monitor on the NCPA Agent.

Ping
Monitors the server with an ICMP ping. Useful for watching network latency and general uptime.

Total Processes
Monitors the total number of processes running on the server.

⚠ 150   ❗ 250

Current Process Count

199

CPU Usage
Check the CPU usage of the system.

⚠ 20 % ❗ 40 %

☑ Show average CPU usage instead of per cpu core

Current CPU Usage

1   %

User Count
Check the number of users currently logged into the system.

⚠ 2 # ❗ 4 #

Current User Count

1

Memory Metrics

Default units to use for memory metric ouput: Gi ∨

Main Memory Usage
Monitor memory usage as percentage of memory used.

⚠ 50 % ❗ 80 %

Current Memory Usage

45.6   %

- Step 6: Finish the set up

Configuration Wizard: Linux Server - Step 3

Monitoring Settings

Define basic parameters that determine how the host and service(s) should be monitored.

Under normal circumstances:

Monitor the host and service(s) every 5 minutes.

When a potential problem is first detected:

Re-check the host and service(s) every 1 minutes up to 5 times before sending a notification.

‹ Back   Next ›   ✔ Finish

Find the client and we can see all of its information

Host Status Detail

192.168.91.133

Services

🏠 | 📄 Services | 📊 | ➕ | ⚙️ | 📈 | 🗒️ | 📶

Service Status for this Host   Last updated: 2022-11-20 21:39:45

Service	Status		Duration	Attempt	Last Check	Status Information
CPU Usage	⚡	Unknown	11m 20s	5/5	2022-11-20 21:38:25	UNKNOWN: An error occured connecting to API. (Connection error: '[Errno 113] No route to host')
Disk Usage on /	⚡	Unknown	10m 20s	5/5	2022-11-20 21:39:27	UNKNOWN: An error occured connecting to API. (Connection error: '[Errno 113] No route to host')
Disk Usage on /run/credentials/systemd-sysusers.service	⚡	Unknown	12m 55s	5/5	2022-11-20 21:36:48	UNKNOWN: An error occured connecting to API. (Connection error: '[Errno 113] No route to host')
Disk Usage on /sys/fs/bpf	⚡	Unknown	13m 14s	5/5	2022-11-20 21:36:25	UNKNOWN: An error occured connecting to API. (Connection error: '[Errno 113] No route to host')
Disk Usage on /sys/fs/cgroup	⚡	Unknown	12m 42s	5/5	2022-11-20 21:37:03	UNKNOWN: An error occured connecting to API. (Connection error: '[Errno 113] No route to host')
Memory Usage	⚡	Unknown	13m 55s	5/5	2022-11-20 21:35:55	UNKNOWN: An error occured connecting to API. (Connection error: '[Errno 113] No route to host')
Ping	⚡	Critical	12m 31s	5/5	2022-11-20 21:37:14	CRITICAL - 192.168.91.133: Host unreachable @ 192.168.91.134. rta nan, lost 100%
Swap Usage	⚡	Unknown	12m 20s	5/5	2022-11-20 21:37:25	UNKNOWN: An error occured connecting to API. (Connection error: '[Errno 113] No route to host')
Total Processes	⚡	Unknown	13m 35s	5/5	2022-11-20 21:36:08	UNKNOWN: An error occured connecting to API. (Connection error: '[Errno 113] No route to host')
User Count	⚡	Unknown	12m 12s	5/5	2022-11-20 21:37:33	UNKNOWN: An error occured connecting to API. (Connection error: '[Errno 113] No route to host')
eth0 Bandwidth - Inbound	⚡	Unknown	12m 5s	5/5	2022-11-20 21:37:40	UNKNOWN: An error occured connecting to API. (Connection error: '[Errno 113] No route to host')
eth0 Bandwidth - Outbound	⚡	Unknown	11m 57s	5/5	2022-11-20 21:37:48	UNKNOWN: An error occured connecting to API. (Connection error: '[Errno 113] No route to host')

2.3.1.5 Monitoring Website

Website is a special situation, it does not require any agent to monitor so we can do the configuration easily.

- Step 1: Choose configuration then configuration tool, choose website

- Step 2: Type the website we want to monitor here

- Step 3: Choose services to monitor

- Step 4: Finish configuration

Check via the web server

Host Status Detail

www.nagios.com

Service Status for this Host

Service	Status	Duration	Attempt	Last Check
SSL Certificate	Ok	N/A	1/5	
DNS IP Match	Ok	N/A	1/5	
DNS Resolution	Ok	N/A	1/5	
HTTP	Ok	N/A	1/5	
Ping	Ok	N/A	1/5	

3 RESULT AND CONCLUSION

Mission \ Member	Trần Hoài Rin	Lê Trọng Nhân	Lê Hoàng Cao Nguyên
Nagios XI (Window + Linux)	✓		
Nagios Core (Window)		✓	
Nagios Core (Linux)			✓
Slide	✓		
Report	✓	✓	✓
Presentation	✓	✓	✓

Skill \ Point	4	3	2	1	
Report (1 point)	✓				
Presentation (1 point)		✓			
Theory (2 point)	✓				
Demonstration (5 point)	✓				
Total /9	8	0.75			8.75

4 ANSWER QUESTIONS

4.1 Advantage and disadvantage of two versions of Nagios

Nagios Core

Advantage:

26

- Useful plugins for any infrastructure monitoring situation via 3rd-party manufacturers.

- Monitors a variety of standard metrics.

- Easy-to-use GUI

Disadvantages:

- No functionality to configure directly via a web interface. Changes in configuration have to be made by editing configuration files from scratch.

- Configuration is quite challenging for users with low technical knowledge.

Nagios XI

Advantage:
- Having UI makes Nagios XI friendly with user and easy to make up with.
- All tools and funtions has been already installed.

Disadvantage:
- To make use of all of XI's functions, it requires payment.

4.2 Nagios XI affordability?

With the quantity of 100 machines in the topology, there are 2 options to choose from:
- Standard Edition: $1995
- Enterprise Edition: $3495

4.3 Can Nagios be deployed on MacOS?

Nagios is designed to run on Linux operating system and it can monitor Unix machines (like MacOS) using Nagios XI with the help of MacOS/X agent.