

การกำรระบบ Fault Monitoring ของอุปกรณ์ Network
โดยใช้ SNMP trap uu ZABBIX

ZABBIX

+

FORTINET®

presented by **Piraya Phodokmai**

Outline

It's a summary of what we'll discuss today.

01

Introduction

03

Methodology

05

Conclusion and
Recommendation

02

Literature
reviews

04

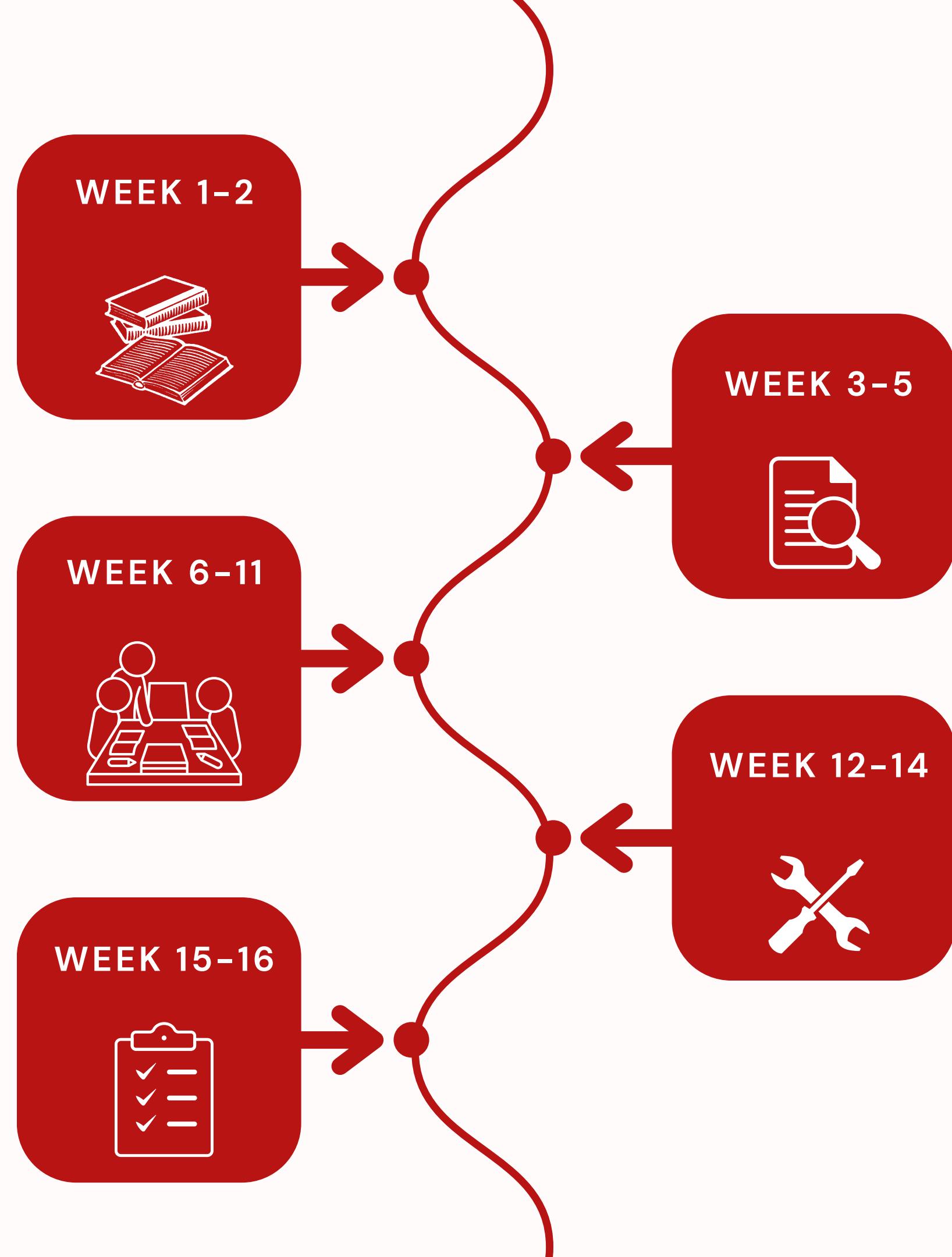
Results

PROJECT TIMELINE

ศึกษาข้อมูลพื้นฐาน
เกี่ยวกับเครือข่ายเน็ตเวิร์ค

ระบบ SNMP Trap
บน ZABBIX

ทดสอบโปรแกรมก่อนใช้งาน



ศึกษาค้นคว้าข้อมูล
เกี่ยวกับการสร้าง
SNMP Trap บน ZABBIX

แก้ไขข้อผิดพลาดต่างๆ
ของโปรแกรม

01



SNMP Walk



SNMP Trap

INTRODUCTION

SNMP Trap มีประโยชน์ในการ
ใช้สำหรับ Monitor อุปกรณ์ Network
มากน้อยเพียงใด?

Objectives

Objective 01

เพื่อศึกษาหลักการทำงานของซอฟต์แวร์ ZABBIX

Objective 02

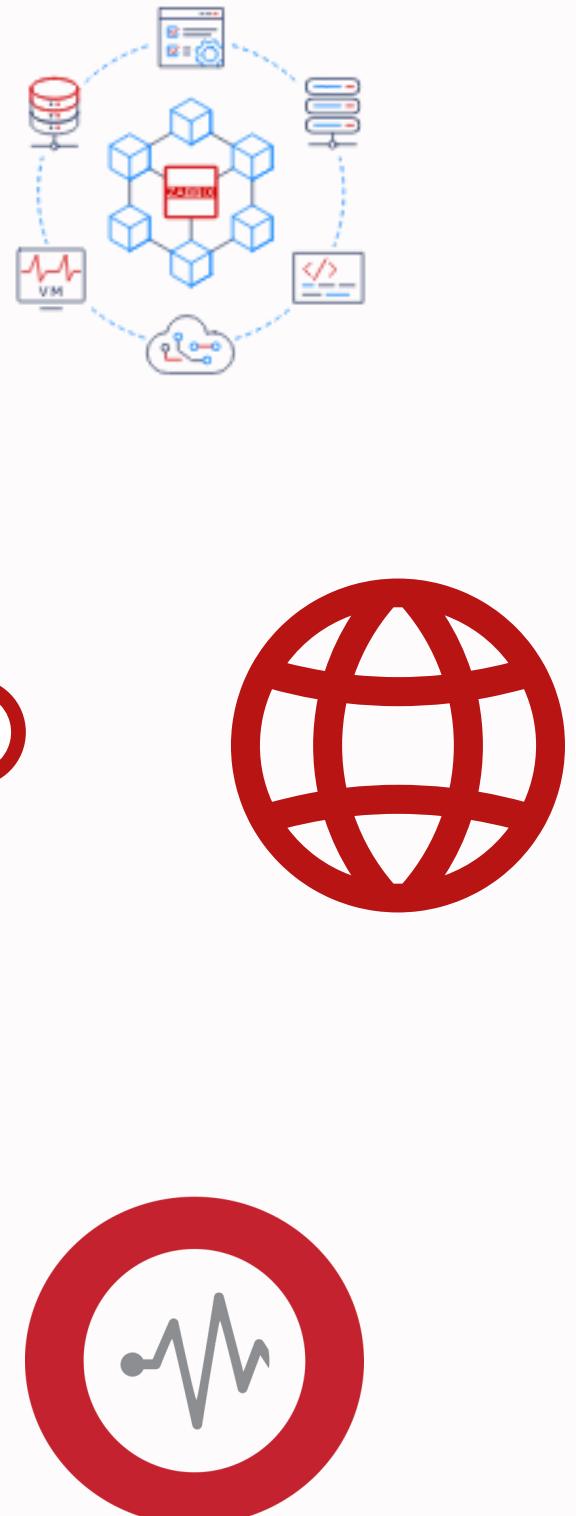
เพื่อศึกษาการทำงานของ SNMP Trap

Objective 03

เพื่อทดสอบระบบการ Monitor อุปกรณ์เน็ตเวิร์คบนซอฟต์แวร์ ZABBIX โดยใช้ วิธี SNMP Trap



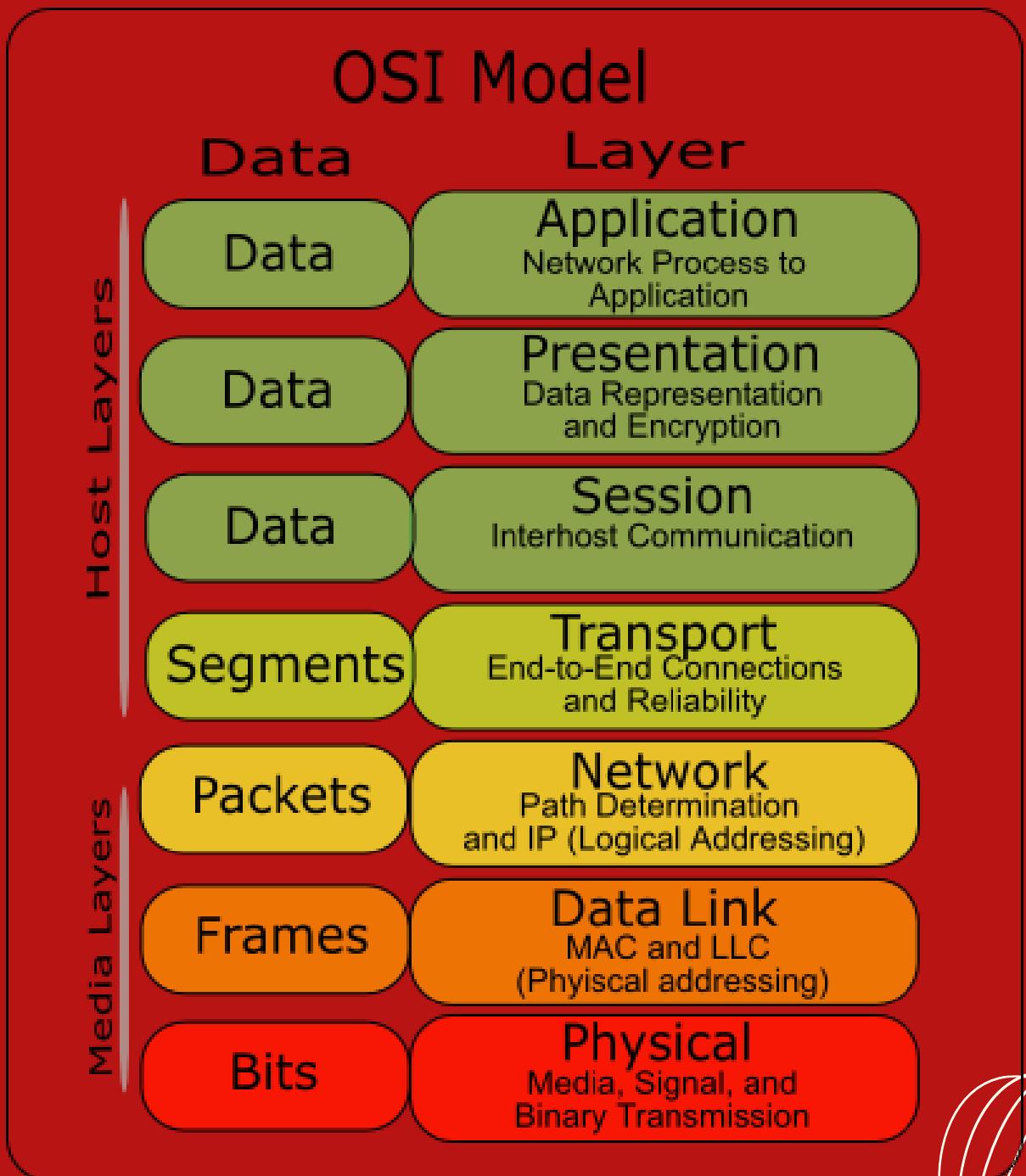
ZABBIX
+
FORTINET®



LITERATURE REVIEWS

OSI 7 LAYER

SNMP ทำงานในระดับ Application Layer ในรูปแบบ Internet Protocol Suit ซึ่ง SNMP agent จะรับคำสั่งผ่านทาง UDP Port 161 โดยตัว manager จะส่งคำสั่งไปยัง Port 161 บนอุปกรณ์ที่ agent จากนั้น agent จะส่งข้อมูลกลับไปยัง manager ตามที่ร้องขอมา ส่วนผู้ที่ manager จะมีการรับ notification หรือที่เรียกว่า Traps (SNMP Traps) ที่ Port 162 โดยผู้ที่ agent จะเป็นคนส่ง notification เมื่อพบสิ่งผิดปกติตามที่ตั้ง rule เอาไว้





Monitoring tool

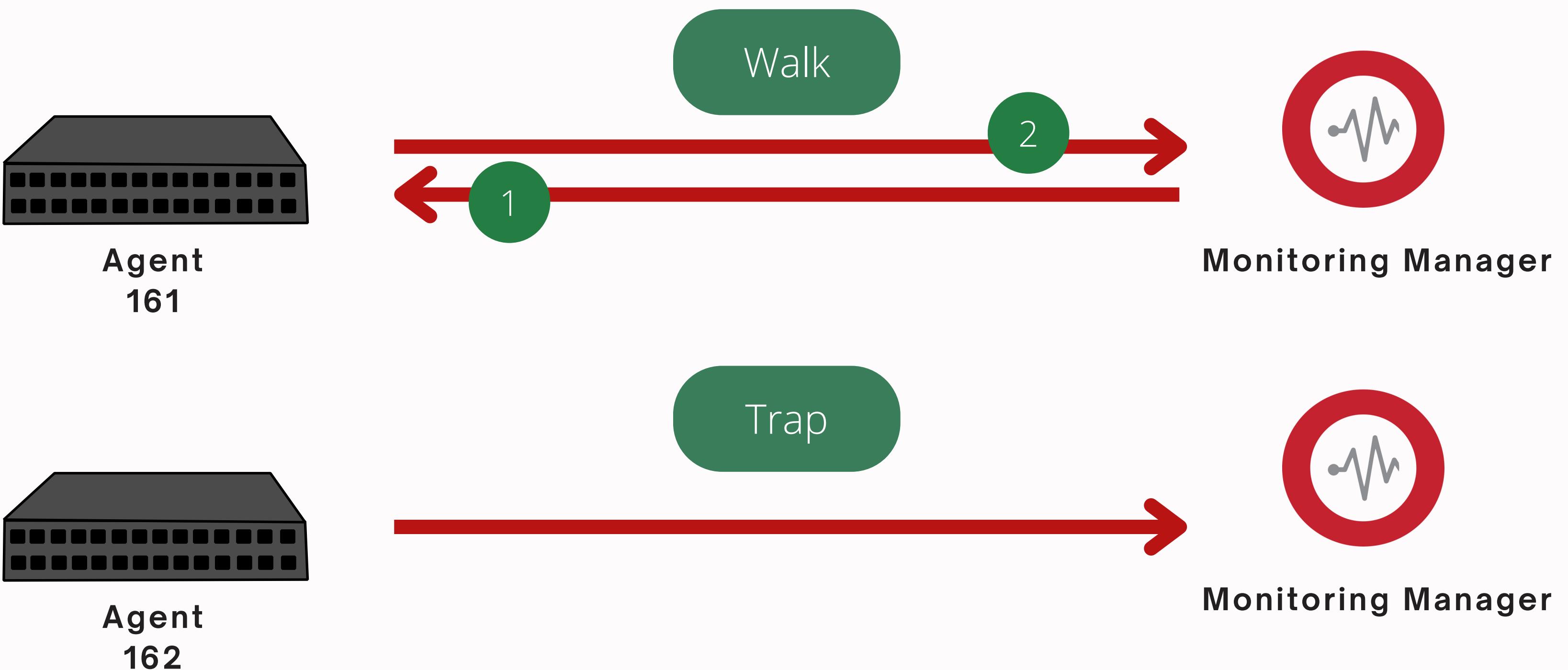
Server



Network
Hardware

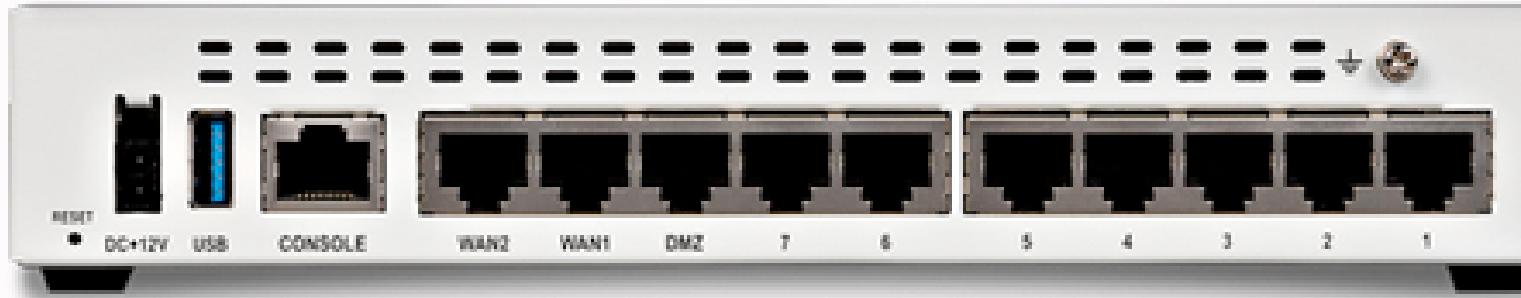


WHAT IS SNMP TRAP?





FortiGate อุปกรณ์ Firewall เด่นเรื่องการจัดการ Network Security
และการจัดการ การใช้งาน Internet ในองค์กร



FortiGate-60E

03

Methodology

01

Virtualization

02

Install ZABBIX

03

Configuration SNMP
Trap uu FortiGate-60E

04

Setting up SNMP Trapper
uu ZABBIX

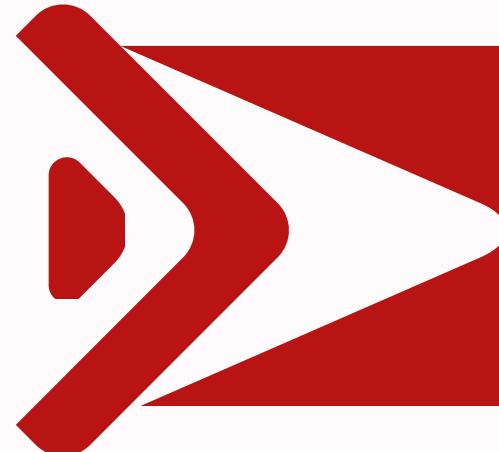
06

สร้าง Trigger

05

Configurations
SNMP Trap uu ZABBIX

01



Virtualization

คือเทคโนโลยีที่สามารถทำให้อุปกรณ์คอมพิวเตอร์หนึ่งเครื่องทำงานได้เหมือนกับมีคอมพิวเตอร์หลายๆเครื่อง เป็นการจำลองการทำงานของเครื่องคอมพิวเตอร์แบบเสมือนและสามารถใช้งานได้จริง



VMware vSphere

VMware vSphere

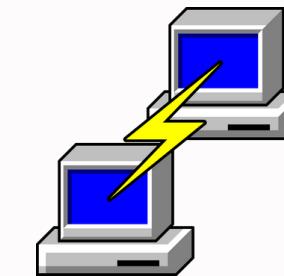
เครื่องเซิร์ฟเวอร์หนึ่งเครื่องใช้ระบบปฏิบัติการมากกว่าหนึ่งตัว เพื่อแบ่งลง OS ได้หลายตัวในการใช้งานที่แตกต่างกัน



CentOS

CentOS

ระบบปฏิบัติการ Linux สำหรับองค์กรที่เน้นเรื่องความเสถียรและมีการอัปเดตความปลอดภัยระดับสูงทุก 6 เดือน



PuTTY

ใช้ในการสั่งงาน Server ด้วย command line โดยที่ไม่ต้องเดินไปหน้ายังเครื่อง server



Search in all environments

Zabbix-6.4-Project-SNMP-Trainee

ACTIONS

Summary Monitor Configure Permissions Datastores Networks Updates

Powered Off

Guest OS: CentOS 8 (64-bit)
Compatibility: ESXi 6.7 and later (VM version 14)
VMware Tools: Not running, not installed
More info

DNS Name:
IP Addresses:
Host: 10.1.1.19

CPU USAGE: 0 Hz
MEMORY USAGE: 0 B
STORAGE USAGE: 2.13 KB

Launch Web Console
Launch Remote Console

VM Hardware

- > CPU: 4 CPU(s)
- > Memory: 4 GB, 0 GB memory active
- > Hard disk 1: 50 GB
- > Network adapter 1: NOC-Port-Group-Server2 (disconnected)

Notes

Custom Attributes

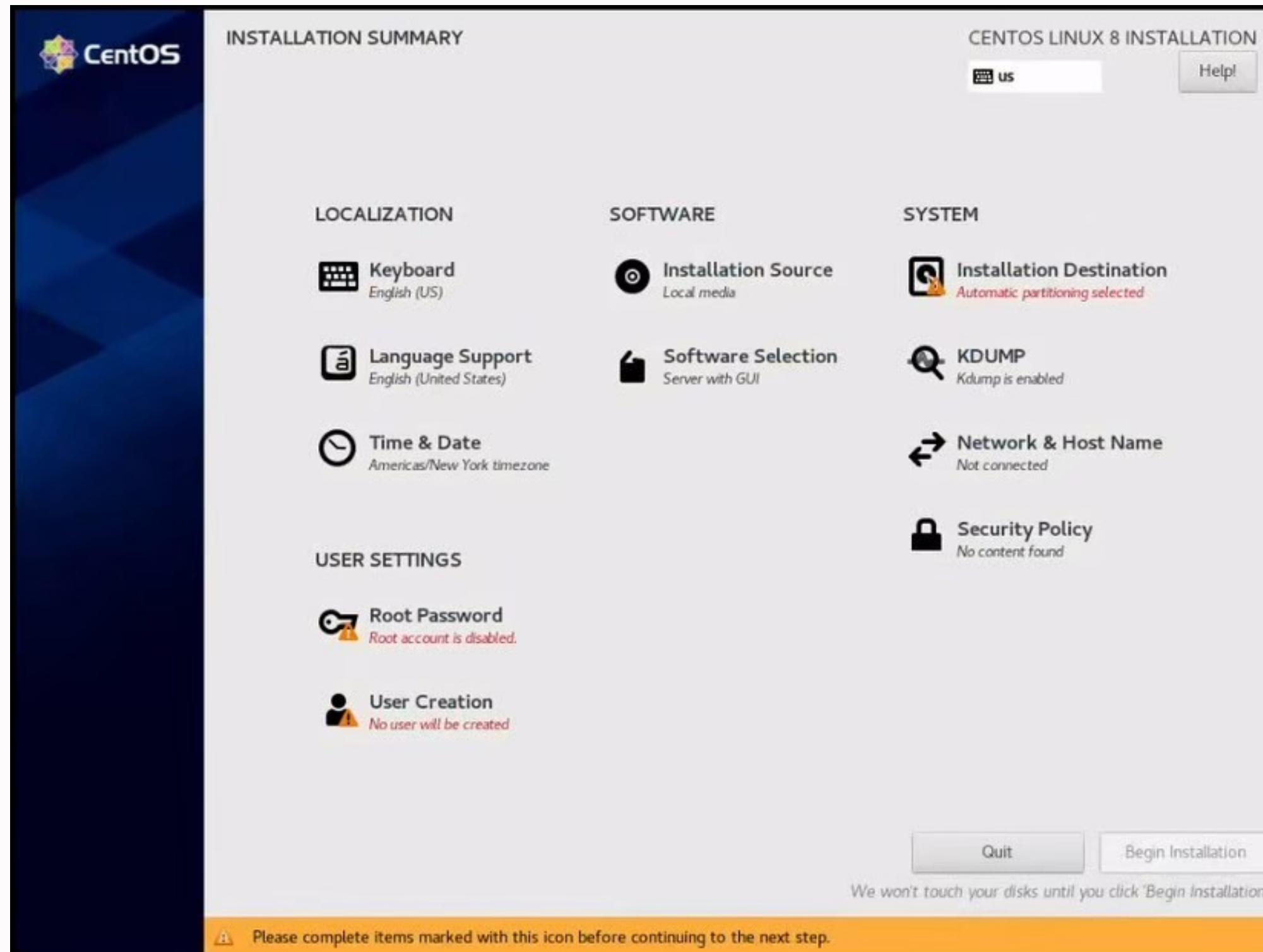
VM Storage Policies

VM Storage Policies

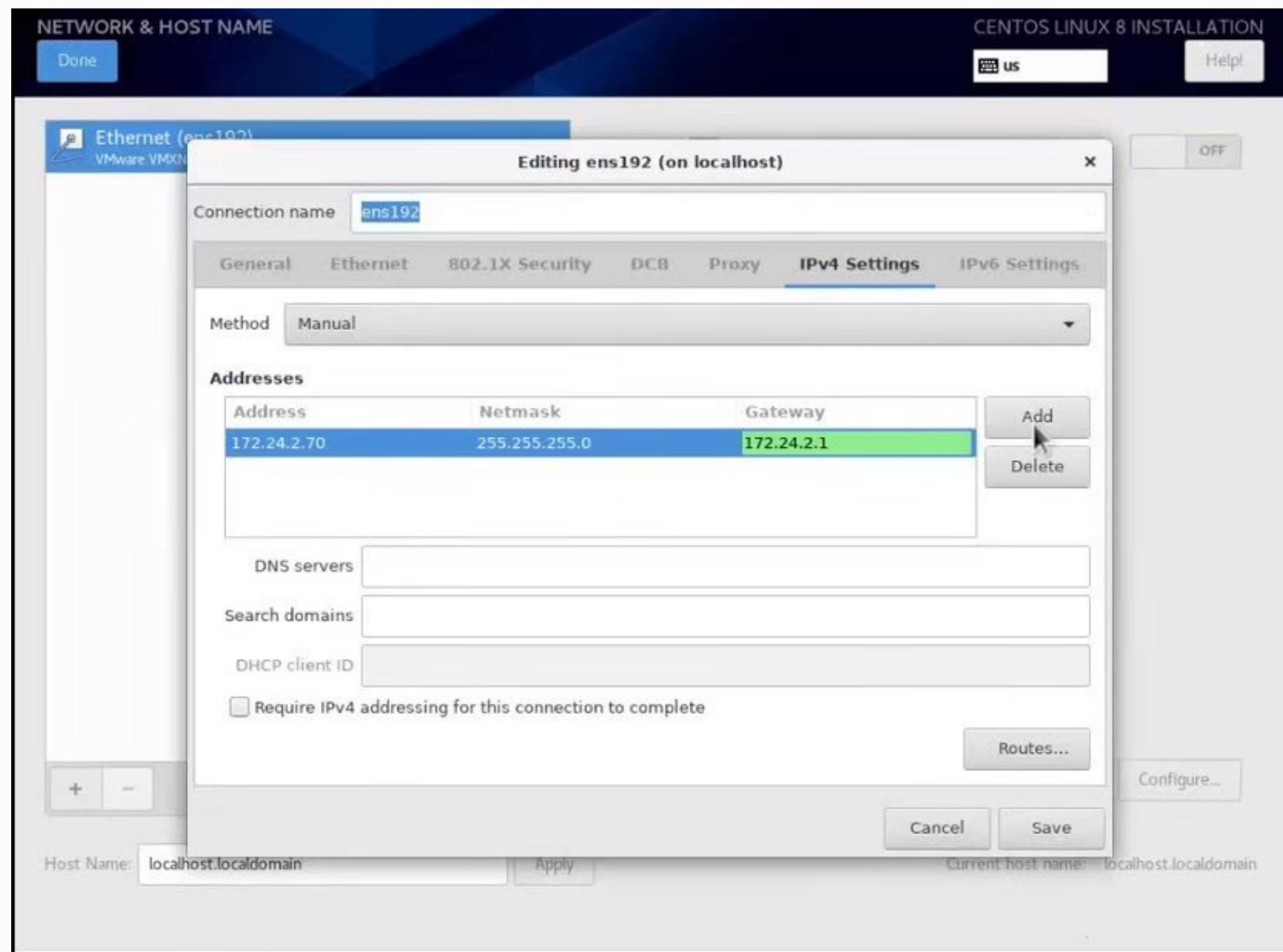
Status	Queued For	Initiator	Start Time	Completion Time	Server

More Tasks

ซอฟต์แวร์มอนิเตอร์
ระบบเครือข่าย



ໂຮສຕ້ສໍາຫຼັບເຊີຣົພເວົອຣມອນິເຕອຣ຺້
Linux CentOS 8

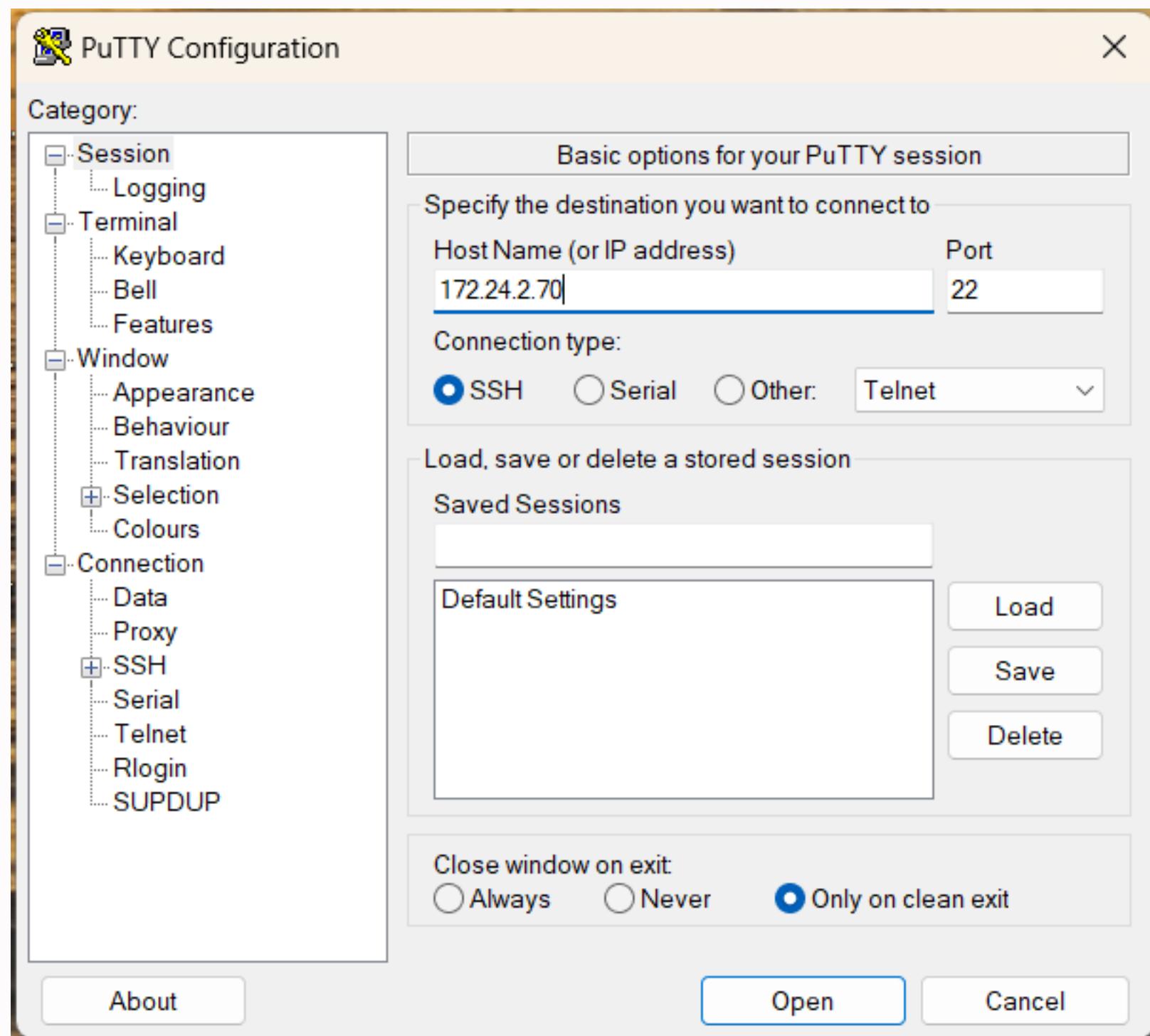


The root account is used for administering the system. Enter a password for the root user.

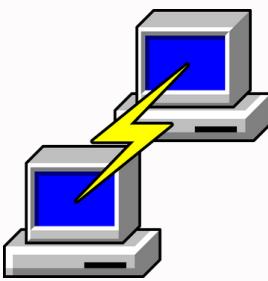
Root Password: Strong

Confirm:

รูปที่ 5.การกำหนดรหัสผ่านผู้ใช้



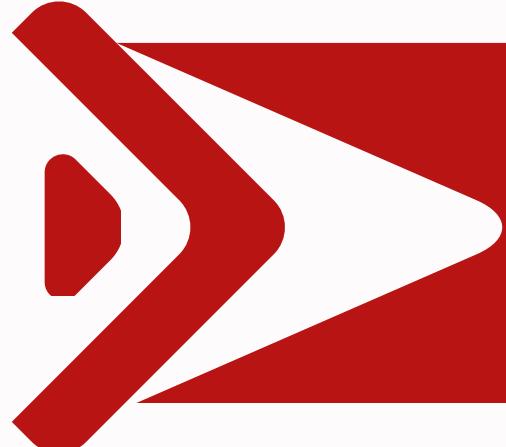
Configuration ของ PuTTY



PuTTY

IP address เป็น IP เดียวกับที่
กำหนดค่าไว้ใน CentOS 8 จากนั้น
ใส่รหัสผ่าน root ที่กำหนดไว้

02



Install ZABBIX >>>www.ZABBIX.com

1

Choose your platform

ZABBIX VERSION	OS DISTRIBUTION	OS VERSION	ZABBIX COMPONENT	DATABASE	WEB SERVER
6.4	Alma Linux	9 Stream	Server, Frontend, Agent	MySQL	Apache
6.0 LTS	CentOS	8 Stream	Proxy	PostgreSQL	Nginx
5.0 LTS	Debian	7	Agent		
4.0 LTS	Debian (arm64)	6	Agent 2		
7.0 PRE-RELEASE	OpenSUSE Leap		Java Gateway		
	Oracle Linux		Web Service		
	Raspberry Pi OS				
	Red Hat Enterprise Linux				
	Rocky Linux				
	SUSE Linux Enterprise Server				
	Ubuntu				
	Ubuntu (arm64)				

Release Notes 6.0

Choose platform ZABBIX

2

Install and configure Zabbix for your platform

a. Install Zabbix repository

```
# rpm -Uvh https://repo.zabbix.com/zabbix/6.0/rhel/8/x86_64/zabbix-release-6.0-4.el8.noarch.rpm  
# dnf clean all
```

b. Install Zabbix server, frontend, agent

```
# dnf install zabbix-server-mysql zabbix-web-mysql zabbix-apache-conf zabbix-sql-scripts zabbix-selinux-policy zabbix-agent
```

c. Create initial database

Documentation

Make sure you have database server up and running.

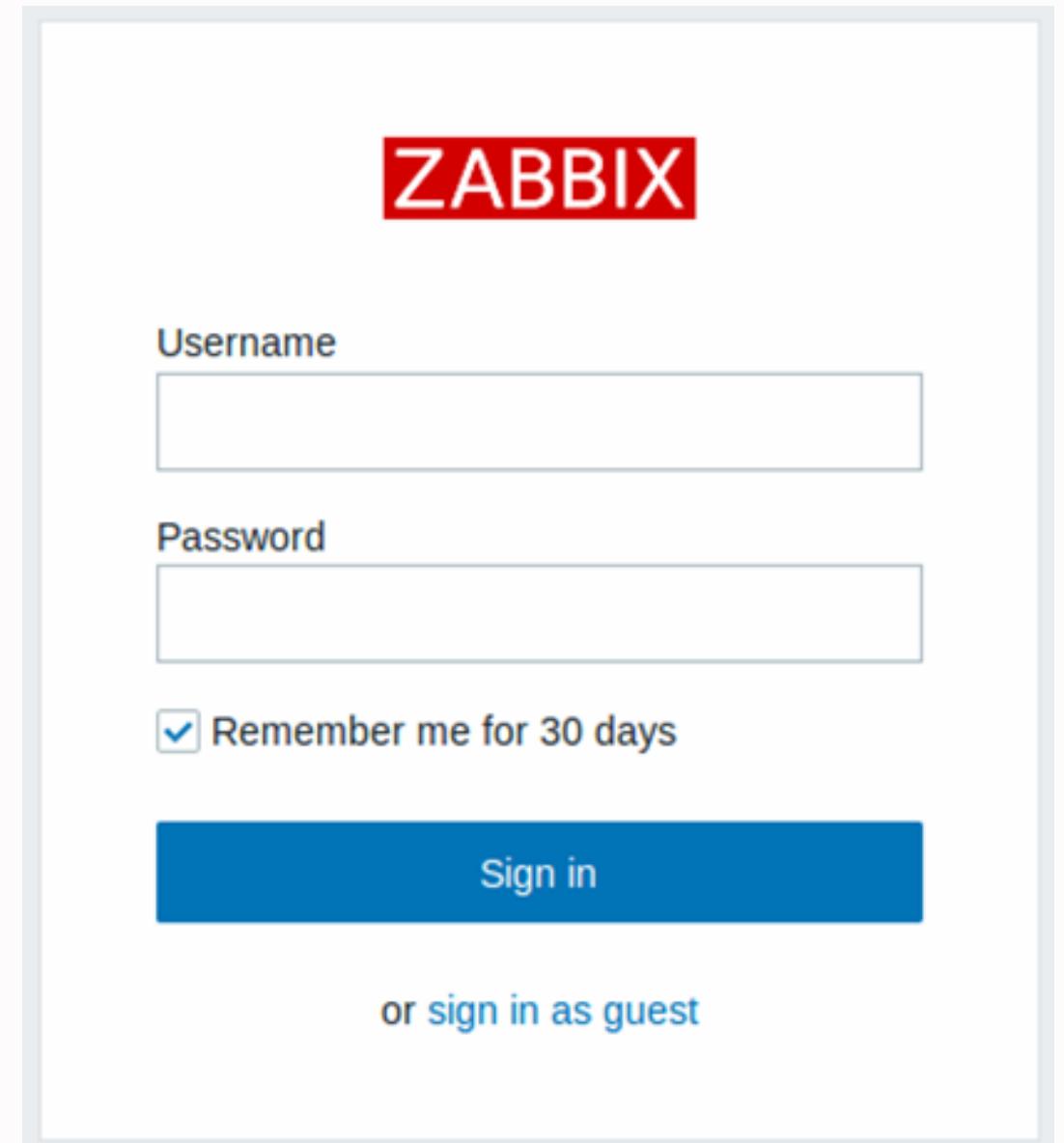
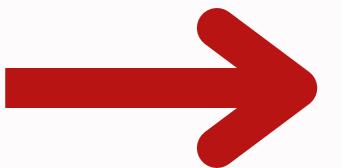
Run the following on your database host.

```
# mysql -uroot -p  
password  
mysql> create database zabbix character set utf8mb4 collate utf8mb4_bin;  
mysql> create user zabbix@localhost identified by 'password';  
mysql> grant all privileges on zabbix.* to zabbix@localhost;  
mysql> set global log_bin_trust_function_creators = 1;  
mysql> quit;
```

Install zabbix platform

```
[root@localhost ~]#  
[root@localhost ~]# systemctl status zabbix-server  
● zabbix-server.service - Zabbix Server  
   Loaded: loaded (/usr/lib/systemd/system/zabbix-server.service; enabled; vendor>  
   Active: active (running) since Sat 2023-08-26 08:36:17 +07; 1 weeks 6 days ago  
     Process: 2402 ExecStart=/usr/sbin/zabbix_server -c $CONFFILE (code=exited, st>  
 Main PID: 2405 (zabbix_server)  
    Tasks: 49 (limit: 23548)  
   Memory: 122.5M  
 CGroup: /system.slice/zabbix-server.service  
         ├─2405 /usr/sbin/zabbix_server -c /etc/zabbix/zabbix_server.conf  
         ├─2425 /usr/sbin/zabbix_server: ha manager  
         ├─2426 /usr/sbin/zabbix_server: service manager #1 [processed 0 even>  
         ├─2427 /usr/sbin/zabbix_server: configuration syncer [synced configu>  
         ├─2483 /usr/sbin/zabbix_server: alert manager #1 [sent 0, failed 0 a>  
         ├─2484 /usr/sbin/zabbix_server: alerter #1 started  
         ├─2485 /usr/sbin/zabbix_server: alerter #2 started  
         ├─2486 /usr/sbin/zabbix_server: alerter #3 started  
         ├─2487 /usr/sbin/zabbix_server: preprocessing manager #1 [queued 0, >  
         ├─2488 /usr/sbin/zabbix_server: preprocessing worker #1 started  
         ├─2489 /usr/sbin/zabbix_server: preprocessing worker #2 started  
         ├─2490 /usr/sbin/zabbix_server: preprocessing worker #3 started  
         ├─2491 /usr/sbin/zabbix_server: lld manager #1 [processed 0 LLD rule>  
         ├─2492 /usr/sbin/zabbix_server: lld worker #1 [processed 1 LLD rules>  
         ├─2493 /usr/sbin/zabbix_server: lld worker #2 [processed 1 LLD rules>
```

172.24.2.70



The image shows the Zabbix web interface login screen. At the top right, the word "ZABBIX" is displayed in its signature red font. Below it is a large red arrow pointing from the terminal output on the left towards the "Sign in" button. The login form consists of two input fields: "Username" and "Password", both currently empty. Below these fields is a checked checkbox labeled "Remember me for 30 days". At the bottom of the form is a large blue "Sign in" button. To the right of the "Sign in" button, the text "or sign in as guest" is visible.

ZABBIX

Username

Password

Remember me for 30 days

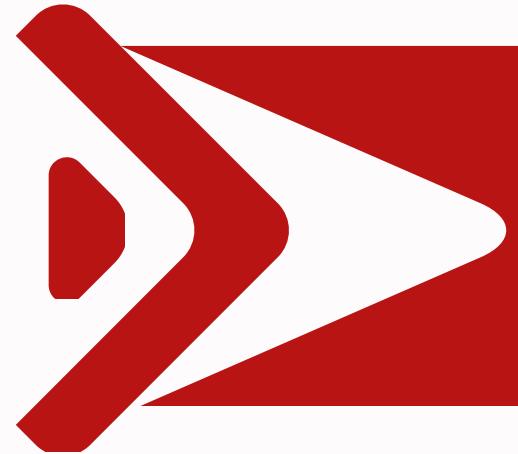
Sign in

or sign in as guest

នូវការស្នើ zabbix server

zabbix log in

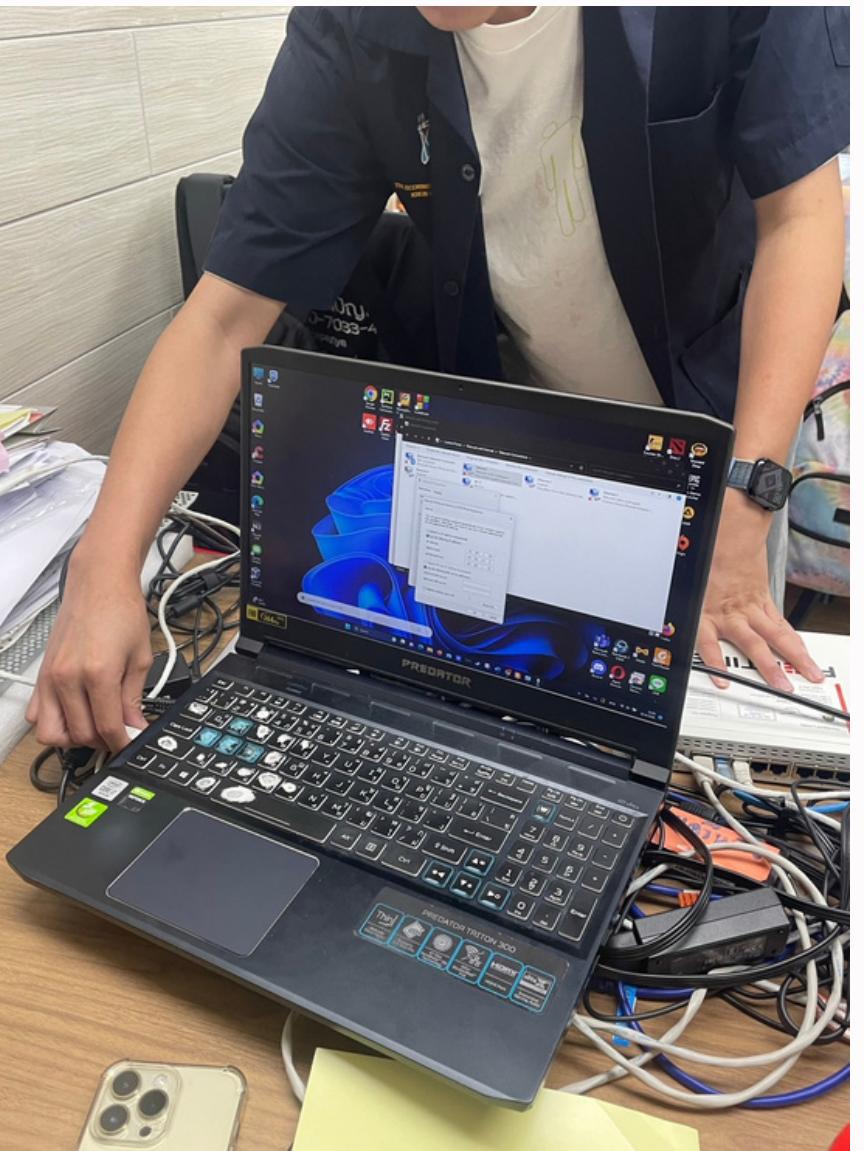
03



Configuration SNMP Trap uu FortiGate-60E

1

เชื่อมต่อ FortiGate-60E เข้ากับคอมพิวเตอร์โดยผ่านสาย wan1



2

ป้อน <http://192.168.1.99> ชื่อเป็นเกตเวย์เริ่มต้นสำหรับเราเตอร์

The screenshot shows a login page for a FortiGate device. At the top, there is a green header bar with a grid icon. Below it, a yellow warning box displays the message "⚠ Your session has expired." In the center, there is a form field containing the text "admin" and another field with several black dots representing a password. At the bottom, a large green "Login" button is visible.

3

Fixed IP ក្នុង Static internet Protocol នៃ Port wan1

Network: 172.24.2.0/24 10101100.00011000.00000010 .00000000 (**Class B**)
Broadcast: 172.24.2.255 10101100.00011000.00000010 .11111111
HostMin: 172.24.2.1 10101100.00011000.00000010 .00000001
HostMax: 172.24.2.254 10101100.00011000.00000010 .11111110
Hosts/Net: 254 (Private Internet)

ការពារចាស់បង្ហាញ IP

Edit Interface

Name	wan1		
Alias			
Type	Physical Interface		
VRF ID	0		
Role	WAN		
Estimated bandwidth	0 kbps Upstream 0 kbps Downstream		
Address			
Addressing mode	Manual <input checked="" type="radio"/> DHCP <input type="radio"/> PPPoE		
IP/Netmask	172.24.2.229/255.255.255.0		
Secondary IP address	<input type="checkbox"/>		
Administrative Access			
IPv4	<input checked="" type="checkbox"/> HTTPS <input checked="" type="checkbox"/> FMG-Access <input type="checkbox"/> FTM	<input checked="" type="checkbox"/> HTTP <small>i</small> <input checked="" type="checkbox"/> SSH <input type="checkbox"/> RADIUS Accounting	<input checked="" type="checkbox"/> PING <input checked="" type="checkbox"/> SNMP <input type="checkbox"/> Security Fabric Connection <small>i</small>

Fixed IP នៃ Port wan1

4

Configure FortiGate SNMP v1/v2c

SNMP v1/v2c

Name	Queries	Traps	Hosts	Events	Status
pplus@read	<input checked="" type="checkbox"/> v1 Disable <input checked="" type="checkbox"/> v2 Enable	<input checked="" type="checkbox"/> v1 Disable <input checked="" type="checkbox"/> v2 Enable	0.0.0.0/0 172.24.2.71/32	37	<input checked="" type="checkbox"/> Enable
pplus@J	<input checked="" type="checkbox"/> v1 Disable <input checked="" type="checkbox"/> v2 Enable	<input checked="" type="checkbox"/> v1 Disable <input checked="" type="checkbox"/> v2 Enable	172.24.6.79/32	37	<input checked="" type="checkbox"/> Enable
pplus@zabbix	<input checked="" type="checkbox"/> v1 Disable <input checked="" type="checkbox"/> v2 Enable	<input checked="" type="checkbox"/> v1 Disable <input checked="" type="checkbox"/> v2 Enable	0.0.0.0/0 172.24.2.70/32 172.24.6.59/32	37	<input checked="" type="checkbox"/> Enable

0 Security Rating Issues (3)

Edit SNMP Community

Community Name: pplus@zabbix

Enabled:

Hosts

IP Address:	0.0.0.0.0.0	<input type="button" value="X"/>
Host Type:	Accept queries and send traps	<input type="button" value="▼"/>
IP Address:	172.24.2.70 255.255.255.255	<input type="button" value="X"/>
Host Type:	Accept queries and send traps	<input type="button" value="▼"/>
IP Address:	172.24.6.59 255.255.255.255	<input type="button" value="X"/>
Host Type:	Accept queries and send traps	<input type="button" value="▼"/>

Community Name : pplus@ZABBIX
 IP Address : (ZABBIX IP)
 Host Type : Accept queries and send trap

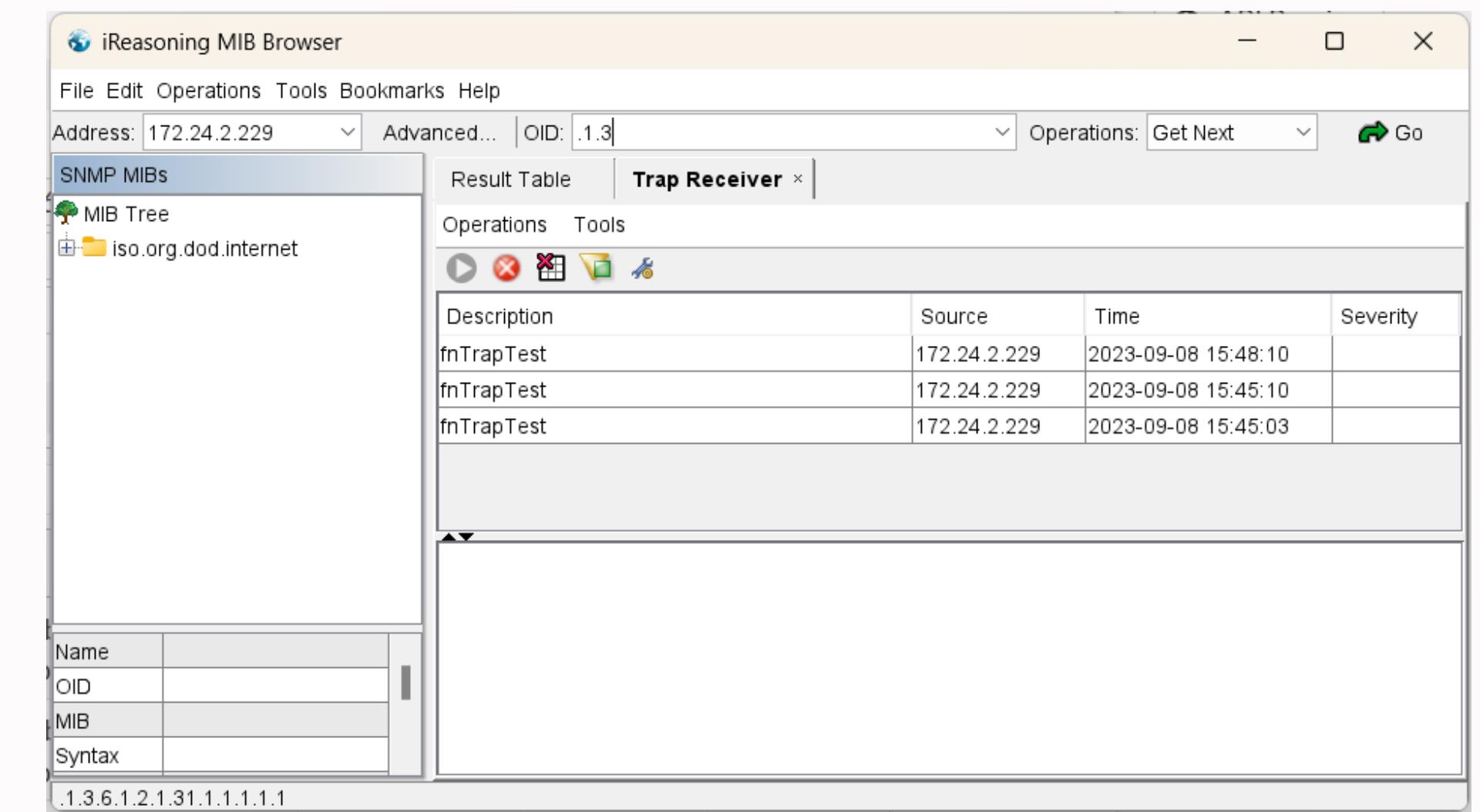
5

ทดสอบการส่ง Trap จาก FortiGate-60E โดยใช้โปรแกรม MIB Browser เป็นตัวรับ

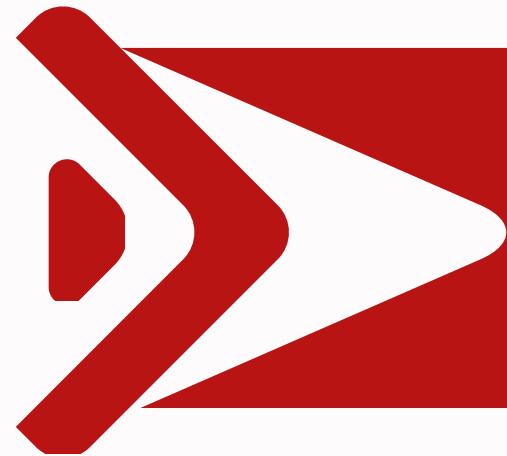
```
CLI Console (1) 🖊️

FortiGate-60E # diagnose snmp trap send
Generating test trap...
Test trap successfully sent to snmp daemon.

FortiGate-60E #
```



04



Setting up SNMP Trapper on ZABBIX

```
root@localhost:~  
# Default:  
#SNMPTrapperFile=/tmp/zabbix_traps.tmp  
  
SNMPTrapperFile=/var/log/snmptrap/snmptrap.log  
  
### Option: StartSNMPTrapper  
#       If 1, SNMP trapper process is started.  
  
#  
# MRGdatory: no  
# Range: 0-1  
# Default:  
StartSNMPTrapper=1  
  
### Option: ListenIP  
#       List of comma delimited IP addresses that the trapper should listen on.  
#       Trapper will listen on all network interfaces if this parameter is missing.  
#  
# Mandatory: no  
# Default:  
# ListenIP=0.0.0.0  
<zabbix/zabbix_server.conf" [readonly] 993L, 26128C      396,1      39%
```

```
root@localhost:~  
[root@localhost ~]# service snmptrapd status  
Redirecting to /bin/systemctl status snmptrapd.service  
● snmptrapd.service - Simple Network Management Protocol (SNMP) Trap Daemon.  
  Loaded: loaded (/usr/lib/systemd/system/snmptrapd.service; enabled; vendor p  
  Active: active (running) since Sat 2023-08-26 08:36:04 +07; 2 weeks 2 days a  
    Main PID: 1530 (snmptrapd)  
      Tasks: 1 (limit: 23548)  
     Memory: 26.0M  
       CGroup: /system.slice/snmptrapd.service  
             └─1530 /usr/sbin/snmptrapd -Lsd -f  
  
Sep 08 15:48:59 localhost.localdomain snmptrapd[1530]: 2023-09-08 15:48:59 <UNK>  
DISMAN-EVENT-MIB::sysUpT  
  
Sep 08 15:48:59 localhost.localdomain snmptrapd[1530]: perl callback function >  
Sep 08 15:50:17 localhost.localdomain snmptrapd[1530]: 2023-09-08 15:50:17 <UNK>  
DISMAN-EVENT-MIB::sysUpT  
Sep 08 15:50:17 localhost.localdomain snmptrapd[1530]: perl callback function >  
Sep 08 15:50:18 localhost.localdomain snmptrapd[1530]: 2023-09-08 15:50:18 <UNK>  
DISMAN-EVENT-MIB::sysUpT  
Sep 08 15:50:18 localhost.localdomain snmptrapd[1530]: perl callback function >  
Sep 08 15:50:29 localhost.localdomain snmptrapd[1530]: 2023-09-08 15:50:29 <UNK>  
DISMAN-EVENT-MIB::sysUpT  
Sep 08 15:50:29 localhost.localdomain snmptrapd[1530]: perl callback function >
```

1

ทำการเพิ่มและแก้ไข ZABBIX server configuration file

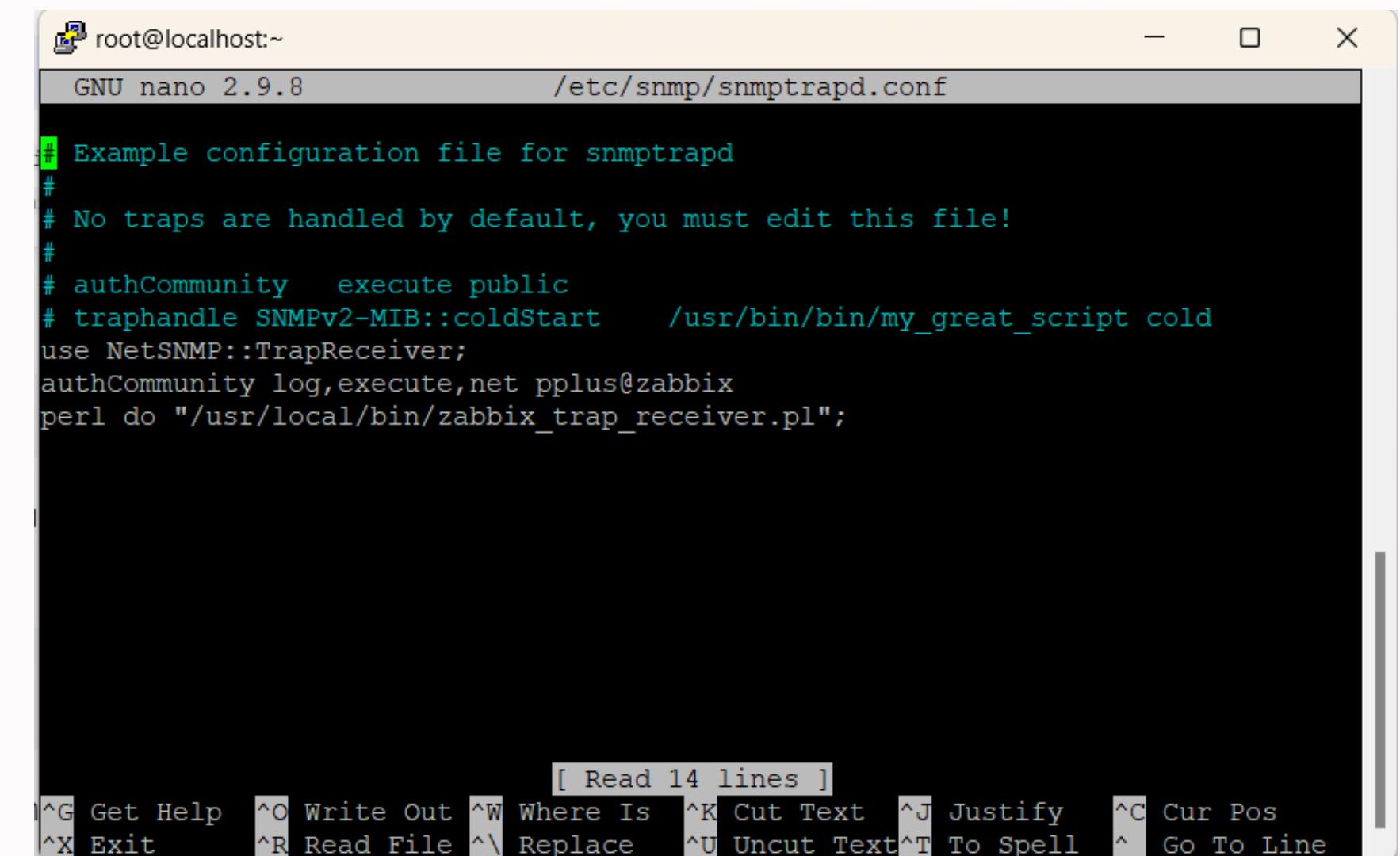
2

ตรวจสอบสถานะของ SNMP Trap

```
[root@localhost ~]# firewall-cmd --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: ens192
  sources:
  services: cockpit dhcpcv6-client http ssh
  ports: 10050/tcp 10051/tcp 22/tcp 162/tcp 162/udp
  protocols:
  forward: no
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
```

3

ทำการตรวจสอบ Port 162



The screenshot shows a terminal window titled "root@localhost:~". The command "nano 2.9.8 /etc/snmp/snmptrapd.conf" is run. The file contains the following configuration:

```
GNU nano 2.9.8          /etc/snmp/snmptrapd.conf
#
# Example configuration file for snmptrapd
#
# No traps are handled by default, you must edit this file!
#
# authCommunity execute public
# trapHandle SNMPv2-MIB::coldStart    /usr/bin/bin/my_great_script cold
use NetSNMP::TrapReceiver;
authCommunity log,execute,net pplus@zabbix
perl do "/usr/local/bin/zabbix_trap_receiver.pl";
```

At the bottom of the terminal, there is a menu bar with the following options: [Read 14 lines], ^G Get Help, ^O Write Out, ^W Where Is, ^K Cut Text, ^J Justify, ^C Cur Pos, ^X Exit, ^R Read File, ^\ Replace, ^U Uncut Text, ^T To Spell, ^L Go To Line.

4

Configuration SNMP Trap

```
### Option: SNMPTrapperFile
#      Temporary file used for passing data from SNMP trap daemon to the server.
#      Must be the same as in zabbix_trap_receiver.pl or SNMPTT configuration file.
#
# Mandatory: no
# Default:
$SNMPTrapperFile=/tmp/zabbix_traps.tmp

$SNMPTrapperFile=/var/log/snmptrap/snmptrap.log

### Option: StartSNMPTrapper
#      If 1, SNMP trapper process is started.
#
# Mandatory: no
# Range: 0-1
# Default:
StartSNMPTrapper=1
```

5

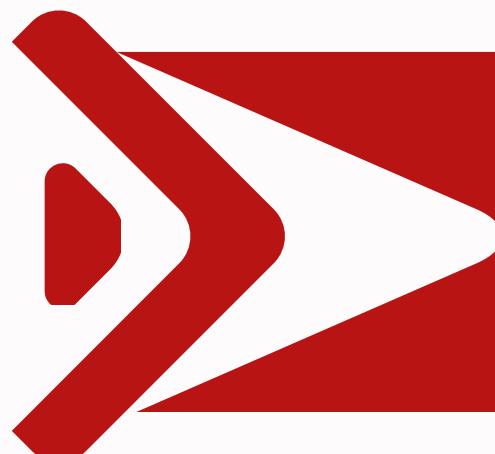
Configuration SNMP Trap receiver

```
[root@localhost ~]# ps ax | grep snmp
 1530 ?        Ss      0:49 /usr/sbin/snmptrapd -Lsd -f
 1532 ?        Ss      9:08 /usr/sbin/snmpd -LS0-6d -f
 2509 ?        S      1:57 /usr/sbin/zabbix_server: snmp trapper [processed da
ta in 0.000036 sec, idle 1 sec]
 931715 pts/0    T      0:00 /bin/systemctl status snmptrapd.service
 931789 pts/0    T      0:00 /bin/systemctl status snmptrapd.service
 932058 pts/0    S+    0:00 grep --color=auto snmp
[root@localhost ~]#
```

6

ตรวจสอบว่า SNMP Trap เชื่อมต่อ กับ ZABBIX Server หรือยัง

05



Configurations SNMP Trap uu ZABBIX

New host

Host IPMI Tags Macros Inventory Encryption Value mapping

* Host name: SNMP Trap

Visible name: SNMP Trap

Templates: type here to search Select

* Groups: Gunk-JJ type here to search Select

Interfaces

Type	IP address	DNS name	Connect to	Port	Default
SNMP	172.24.2.229		IP	162	<input checked="" type="radio"/> Remove
* SNMP version	SNMPv2				
* SNMP community	pplus@zabbix				

Use bulk requests

1

สร้าง Host uu ZABBIX

All hosts / SNMP Trap Enabled SNMP Items Triggers Graphs Discovery rules Web scenarios

Item Tags Preprocessing

* Name: SNMP trap testing
Type: SNMP trap
* Key: snmptrap.fallback
Type of information: Log
* Host interface: 172.24.2.229:161
* History storage period: Do not keep history

2 สร้าง snmptrap.fallback



Test SNMP Trap

3

<input type="checkbox"/> Host	Name ▲	Last check	Last value	C
<input checked="" type="checkbox"/>	SNMP Trap	SNMP trap testing	5s	16:08:48 2023/09/1...



Lasted Data

2023-09-11 09:08:33

```
16:08:32 2023/09/11 PDU INFO:  
    requestid          5062  
    version            1  
    transactionid     1500  
    errorstatus        0  
    notificationtype  TRAP  
    messageid          0  
    receivedfrom       UDP: [172.24.2.229]:162->[172.24.2.70]:162  
    errorindex          0  
    community          pplus@zabbix  
  
VARBinds:  
    DISMAN-EVENT-MIB::sysUpTimeInstance type=67 value=Timeticks: (141559973) 16 days, 9:13:19.73  
    SNMPv2-MIB::snmpTrapOID.0      type=6  value=OID: IF-MIB::linkDown  
    IF-MIB::ifIndex.2              type=2  value=INTEGER: 2  
    IF-MIB::ifAdminStatus.2       type=2  value=INTEGER: 1  
    IF-MIB::ifOperStatus.2        type=2  value=INTEGER: 2  
    SNMPv2-SMI::enterprises.12356.100.1.1.1.0 type=4  value=STRING: "FGT60ETK19006603"  
    SNMPv2-MIB::sysName.0         type=4  value=STRING: "Fortigate-60E"  
    IF-MIB::ifName.2              type=4  value=STRING: "wan2"  
    IF-MIB::ifDescr.2             type=4  value=""
```

linkDown

2023-09-11 09:08:48

```
16:08:47 2023/09/11 PDU INFO:  
    requestid          5070  
    notificationtype  TRAP  
    transactionid     1502  
    errorstatus        0  
    messageid          0  
    version            1  
    community          pplus@zabbix  
    receivedfrom       UDP: [172.24.2.229]:162->[172.24.2.70]:162  
    errorindex          0  
  
VARBinds:  
    DISMAN-EVENT-MIB::sysUpTimeInstance type=67 value=Timeticks: (141561423) 16 days, 9:13:34.23  
    SNMPv2-MIB::snmpTrapOID.0      type=6  value=OID: IF-MIB::linkUp  
    IF-MIB::ifIndex.2              type=2  value=INTEGER: 2  
    IF-MIB::ifAdminStatus.2       type=2  value=INTEGER: 1  
    IF-MIB::ifOperStatus.2        type=2  value=INTEGER: 1  
    SNMPv2-SMI::enterprises.12356.100.1.1.1.0 type=4  value=STRING: "FGT60ETK19006603"  
    SNMPv2-MIB::sysName.0         type=4  value=STRING: "Fortigate-60E"  
    IF-MIB::ifName.2              type=4  value=STRING: "wan2"  
    IF-MIB::ifDescr.2             type=4  value=""
```

linkUp

Trap log file
wan2

4

สร้าง Value mapping



Host						
Host	IPMI	Tags	Macros	Inventory	Encryption	Value mapping 1
Name						Value
Interface status						=1 => Up =2 => Down
						Add

Item Tags Preprocessing

* Name: Link status trap for wan2

Type: SNMP trap

* Key: snmptrap[ifOperStatus.2]

Type of information: Character

* Host interface: 172.24.2.229:161

* History storage period: Do not keep history

Storage period: 90d

Value mapping: Interface status

Populates host inventory field: -None-

5

สร้าง Item Port Interface ที่มีบนอุปกรณ์

Regular Expression



Tags Preprocessing 1

Preprocessing steps	Name	Parameters
1: Regular expression	(IF-MIB::linkDown IF-MIB::linkUp) (\"wan2\")	\1

Add

Type of information Character

Update Clone Execute now Test Clear history and trends Delete Cancel

REGULAR EXPRESSION 2 matches (307 steps, 3.7ms) / gm

```
! / (IF-MIB::linkDown|IF-MIB::linkUp)|("wan2") /
```

TEST STRING

```
requestid*****5078
**version*****
**errorstatus*****
**notificationtype*****TRAP
**transactionid*****1504
**messageid*****
**receivedfrom*****UDP:[172.24.2.229]:162->[172.24.2.70]:162
**errorindex*****
**community*****pplus@zabbix
VARBINDS:
**DISMAN-EVENT-MIB::sysUpTimeInstance?type=67"value=Timeticks:(156575829)*18
days,*2:55:58.29
**SNMPv2-MIB::snmpTrapOID.0*****type=6"value=OID:IF-MIB::linkDown
**IF-MIB::ifIndex.2*****type=2"value=INTEGER:2
**IF-MIB::ifAdminStatus.2*****type=2"value=INTEGER:1
**IF-MIB::ifOperStatus.2*****type=2"value=INTEGER:2
**SNMPv2-SMI::enterprises.12356.100.1.1.0?type=4"value=STRING:
"FGT60ETK19006603"
**SNMPv2-MIB::sysName.0*****type=4"value=STRING:"FortiGate-60E"
**IF-MIB::ifName.2*****type=4"value=STRING:"wan2"
**IF-MIB::ifDescr.2*****type=4"value=""
```

EXPLANATION

```
/ (IF-MIB::linkDown|IF-MIB::linkUp)|("wan2") /
  1st Alternative (IF-MIB::linkDown|IF-MIB::linkUp)
    1st Capturing Group
      IF-MIB::linkDown
        IF-MIB::linkDown matches the characters IF-
          MIB::linkDown literally (case sensitive)
      2nd Alternative IF-MIB::linkUp
```

MATCH INFORMATION

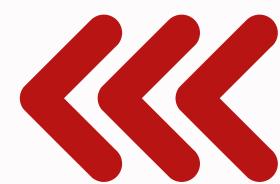
Match 1	531-547	IF-MIB::linkDown
Group 1	531-547	IF-MIB::linkDown
Match 2	933-939	"wan2"
Group 2	933-939	"wan2"

QUICK REFERENCE

- All Tokens
- Common Tok... ✓
- General Tokens
- Anchors
- Meta Sequences

A single character of: a, b o... [a]
A character except: a, b o... [^a]
A character in the range: a-z [a-z]
A character not in the ran... [^a-z]
A character in the rang... [a-zA-Z]
Any single character

Regular Expression Test



Preprocessing Replace



Preprocessing 3

Preprocessing steps	Name	Parameters
1: Regular expression	(IF-MIB::linkDown IF-MIB::linkUp) (\"wan2\")	\1
2: Replace	IF-MIB::linkDown	2
3: Replace	IF-MIB::linkUp	1

Add

Type of information Character

Update Clone Execute now Test Clear history and trends Delete Cancel

Item Tags Preprocessing 3

Preprocessing steps	Name	Parameters
1:	Regular expression	(IF-MIB::linkDown IF-MIB::linkUp) (^ \n)\1
2:	Replace	IF-MIB::linkDown
3:	Replace	IF-MIB::linkUp

Add

Type of information Character

Update Clone Execute now Test Clear history and trends Delete Cancel



<input type="checkbox"/> Host	Name ▲	Last check	Last value	
<input checked="" type="checkbox"/>	SNMP Trap	Link status trap for wan2	6s	Down (2)
<input checked="" type="checkbox"/>	SNMP Trap	SNMP trap testing	5s	13:21:46 2023/09/1...

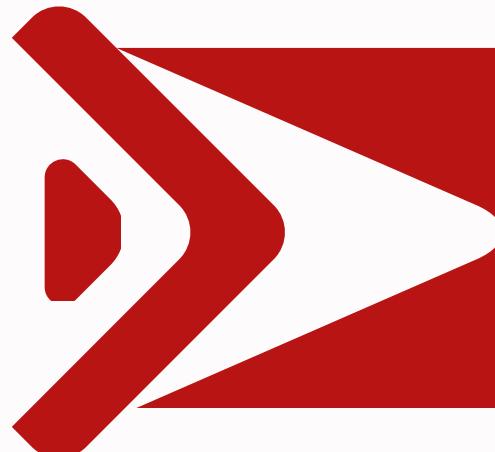
8

Test



<input type="checkbox"/> Host	Name ▲	Last check	Last value	
<input checked="" type="checkbox"/>	SNMP Trap	Link status trap for wan2	5s	Up (1)
<input checked="" type="checkbox"/>	SNMP Trap	SNMP trap testing	4s	13:22:30 2023/09/1...

06



สร้าง Trigger เพื่อแจ้ง Alarm

Trigger Tags Dependencies

* Name: Link status trap for dmz

Event name: Link status trap for dmz

Operational data:

Severity: Average

* Expression: last (/SNMP Trap/snmptrap[ifOperStatus.3])=2

Add

Expression constructor

สร้าง Trigger ของ Port ที่ต้องการ

04

RESULTS

ดึงสายแลนที่ Port dmz

Time ▾	<input type="checkbox"/> Severity	Recovery time	Status	Info	Host	Problem	Duration	Ack
04:17:40	<input type="checkbox"/> Average		PROBLEM		SNMP Trap	Link status trap for dmz	1s	No

เสียบสายแลนที่ Port dmz

Time ▾	<input type="checkbox"/> Severity	Recovery time	Status	Info	Host	Problem	Duration	Ack
04:17:40	<input type="checkbox"/> Average	04:18:06	RESOLVED		SNMP Trap	Link status trap for dmz	26s	No

จากการดึงสายแลนที่ Port wan2 และ dmz แล้วพบว่ามี Alarm แจ้งเตือนเข้ามาพร้อมกับแจ้งว่าเกิดปัญหาขึ้นที่ Port ใดและเมื่อเสียบสายแลนกลับเข้าไปที่ Port ดังกล่าวพบว่าปัญหาที่ได้รับแจ้ง Alarm เมื่อสักครู่ได้รับการ Resolved

Host	Name	Problems	Ok
SNMP Trap	Link status trap for dmz	0.0726%	99.9274%
SNMP Trap	Link status trap for wan2	0.0802%	99.9198%



dmz



wan2

จากกราฟจะพบว่าในระยะเวลา 30 ที่ผ่านมา Port wan2 เกิด linkDown 0.0726% ที่ Port dmz เกิด linkDown 0.0802% และทั้งสอง Port ได้รับการแก้ไขเรียบร้อย

CONCLUSION AND RECOMMENDATION

Conclusion

- จากการการทำระบบ Fault Monitoring ของอุปกรณ์เน็ตเวิร์ค โดยใช้ SNMP trap บน ZABBIX นี้ ผลลัพธ์จากการทดสอบผ่านอุปกรณ์ FortiGate-60E ตามมาตรฐานของบริษัท เมื่อตัวอุปกรณ์เกิดการ failure จะสามารถแจ้ง Alarm ได้เอง โดยไม่จำเป็นต้องให้ผู้ดูแล Manager ส่งคำสั่งไปหา Agent เพื่อเอาชุดข้อมูล ซึ่งจาก การทดสอบสรุปได้ว่า ระบบการ Monitor อุปกรณ์เน็ตเวิร์คบนซอฟต์แวร์ ZABBIX โดยใช้วิธีการ SNMP Trap นี้มีประสิทธิภาพในการ Monitor อุปกรณ์เน็ตเวิร์ค

CONCLUSION AND RECOMMENDATION

Recommendation

- ข้อจำกัดที่เกิดจากการ Monitor อุปกรณ์เน็ตเวิร์คหลายตัวพร้อมกันโดยใช้ SNMP Trap ที่มีการใช้ Template เดียวกันนั้นอาจจะไม่สามารถทำได้เนื่องจากเมื่อเป็น อุปกรณ์คละแบบอาจจะมี Interface ที่ต่างกัน ทำให้ไม่สามารถใช้การตรวจจับ ข้อมูลโดยใช้ Regular Expression เดียวกันได้ ดังนั้นจึงจำเป็นต้องทำการ พัฒนาการตรวจจับข้อมูลในรูปแบบอื่นๆ เช่น JavaScript



Thank You

QUESTION?