開源網路設備監測系統

國立中央大學電算中心

許時準　組長

2022/08/30

大綱

- 前言
- 監測系統的基本概念
- 各種開源監測系統簡介
- 安裝Zabbix系統
- 自動化監測機制
- 系統部署與自動化告警
- Q&A

網路設備重要性

路由器卡片故障！中華電信今早網路大當機

新頭殼newtalk | 閻芝霖 綜合報導

發布 2019.03.12 | 12:01

許多中華用戶發現早上手機突然連不上網，中華電信表示，因為路由器的卡片故障，導致無法連上網。 圖：閻芝霖/攝

https://newtalk.tw/news/view/2019-03-12/218666

電力基礎設備重要性

居隔收不到訊號大崩潰 台電：內湖停電影響台灣之星

2022/05/10 16:14

https://ec.ltn.com.tw/article/breakingnews/3921820

機房設備重要性

自由時報 Liberty Times Net

即時 熱門 政治 社會 生活 健康 國際 地方 蒐奇 影音 財經 娛樂 藝文 NEW
汽車 時尚 體育 3C 評論 玩咖 食譜 地產 專區 TAIPEI TIMES 求職

快訊 漢光開打！ 05:30全台戰機升空警戒、疏散 全面保存戰力

首頁 > 生活

北區無預警斷線 遠傳：機房故障已修復

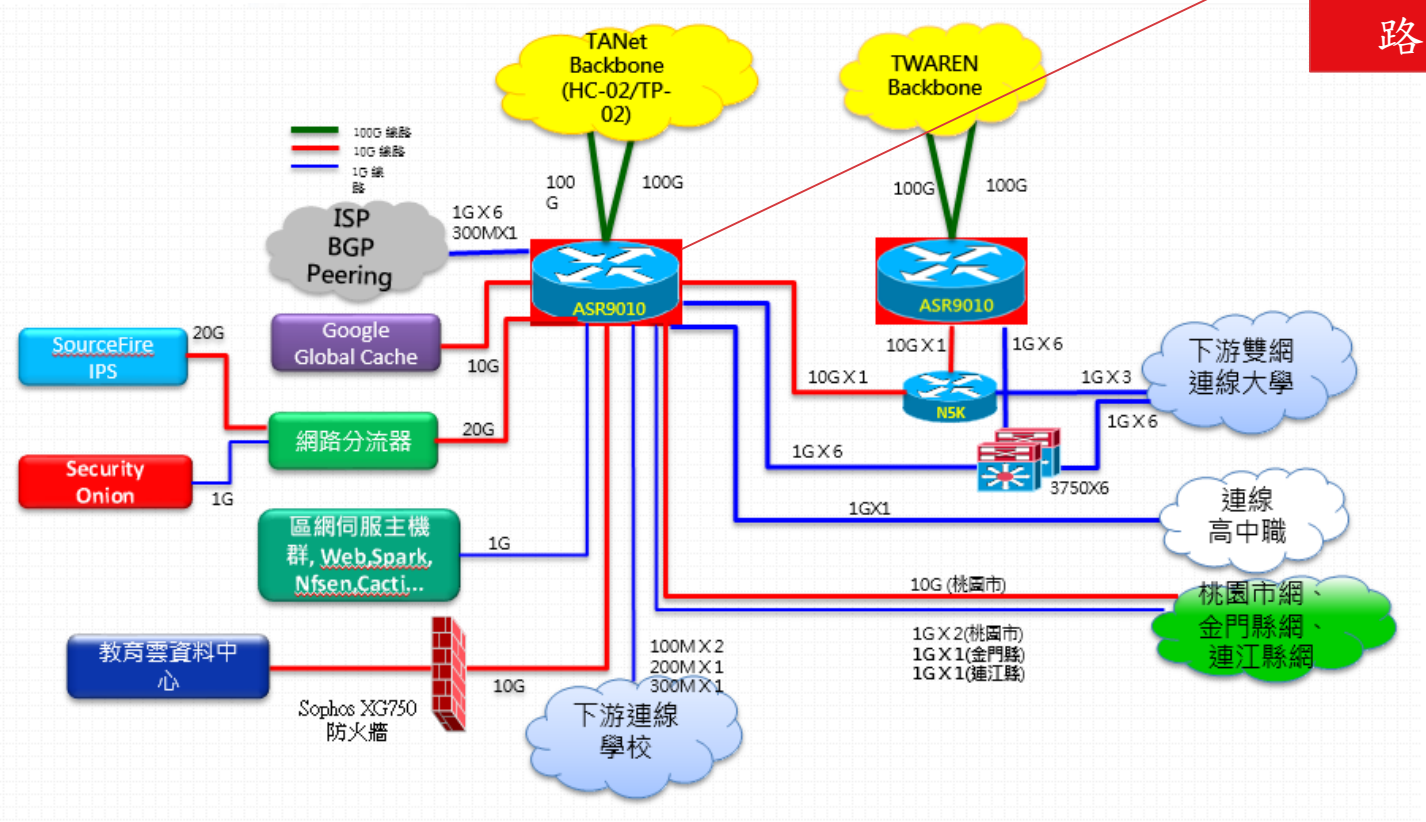
2013/04/02 19:57

〔記者陳炳宏／台北報導〕遠傳電信今天下午傳出大當機事件，包括北區的北市、新北市、桃園、新竹地區許多民眾反應手機無法行動上網與撥接電話，遠傳傍晚表示，因為桃園機房設備故障，影響部分民眾權益，在傍晚6點多時已完成修復，將主動提出賠償。

https://news.ltn.com.tw/news/life/breakingnews/787057

機房網路設備監測

- 即時監看設備的資源與運作狀態是IT人員重要的工作。
- 即時找出問題，而不是等到使用者反映問題，才開始進行問題的故障排除。



監測系統的最重要功能

1. 即時監測系統異常的能力
2. 整合NetFlow 監測及SNMP
3. 即時監測網路流量
4. 即時發送警示訊息

監測系統的資料蒐集模式

1. 第一種為Agent-based模式，在被監測系統上安裝Agent程式。

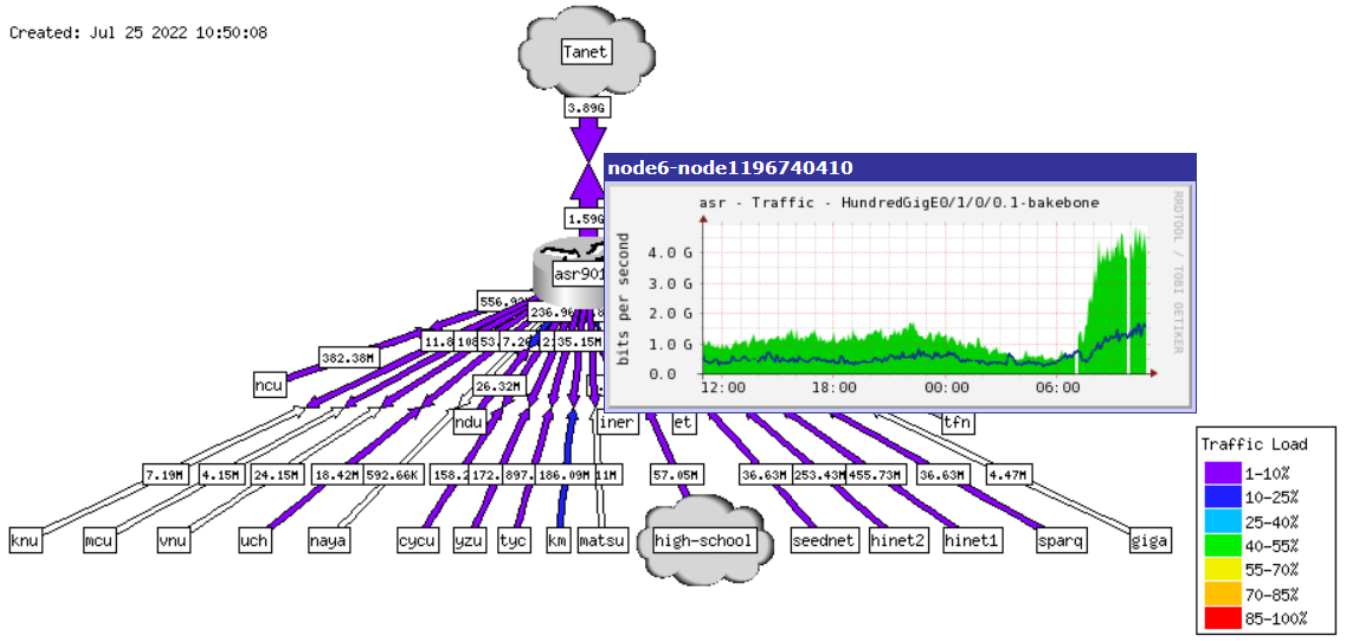
2. 第二種為Agentless模式，利用HTTP、ICMP、SNMP等協定監測，對現有服務架構影響最小。

Monitoring Tools

https://blog.inedo.com/15-best-it-monitoring-tools-and-software

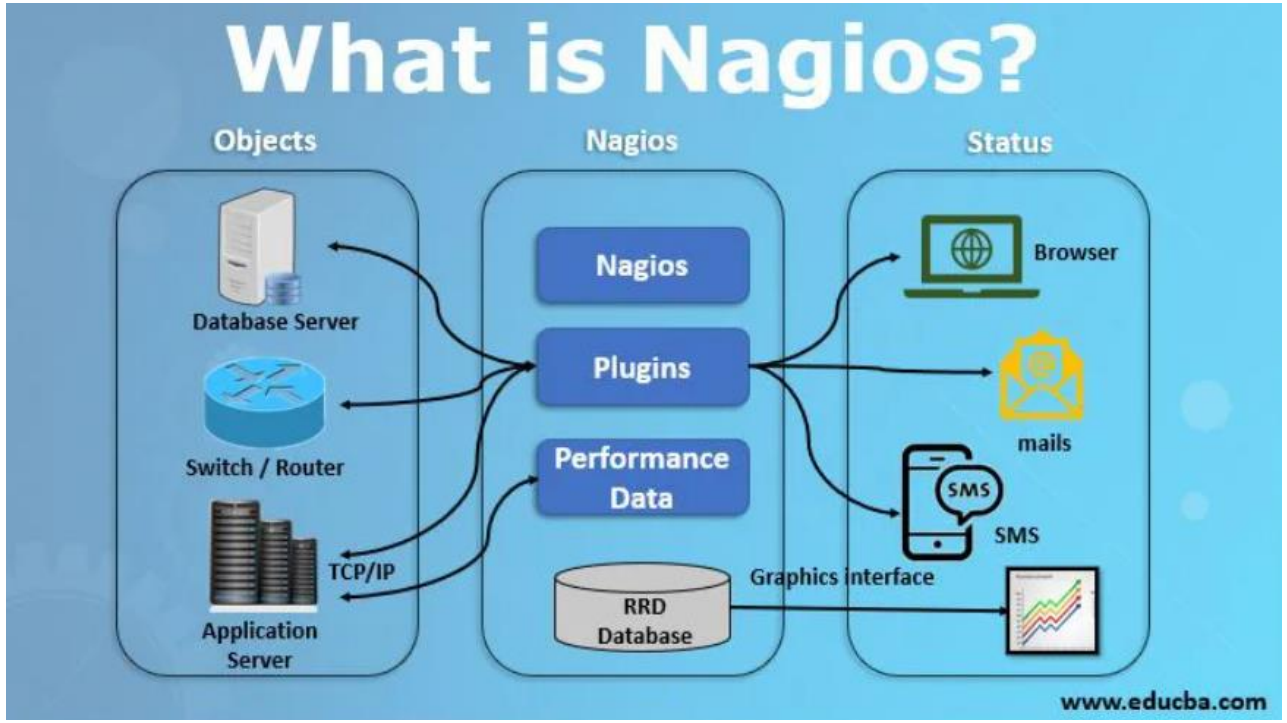
Cacti系統

1. 歷史悠久的網路監測工具，可以安裝在Linux 或 Windows 環境。
2. 主要透過 SNMP 得到各項網路流量資料，可透過 Email 發送警示訊息。
3. 缺點是不像其他市面上的監測系統提供的多樣監測方式



Nagios系統

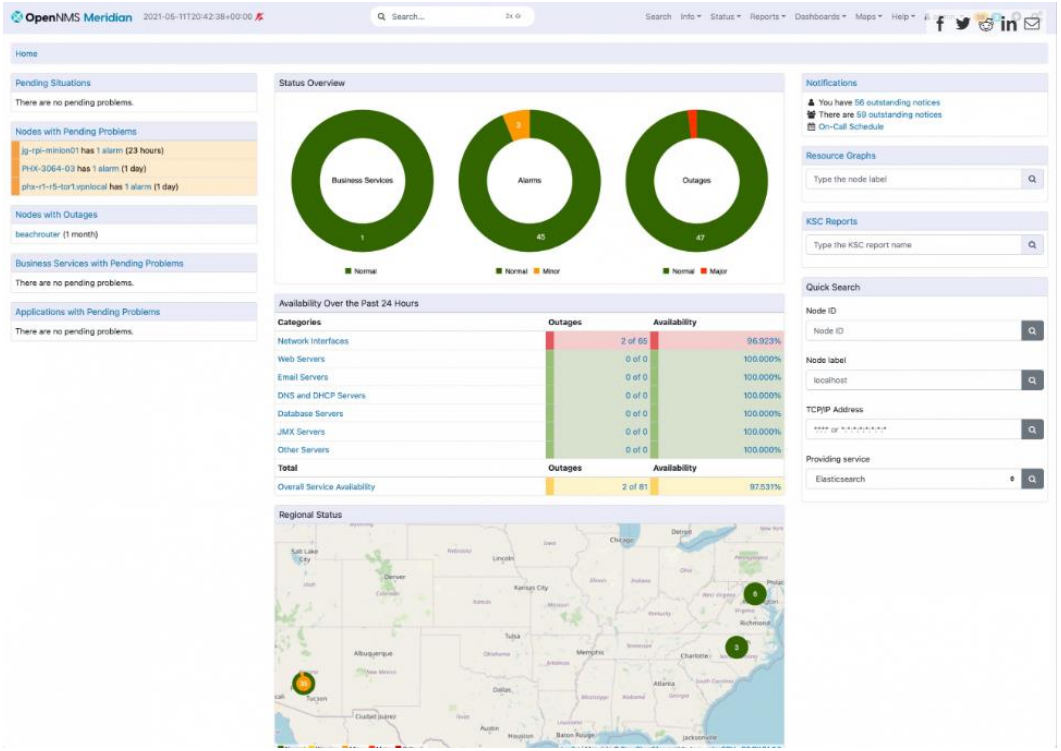
1. 非常受歡迎的監測系統，能監測大部分的協定及網路設備，及安裝NPRE Agent 程式。
2. 缺點是缺乏友善的介面



https://www.educba.com/what-is-nagios/

OpenNMS系統

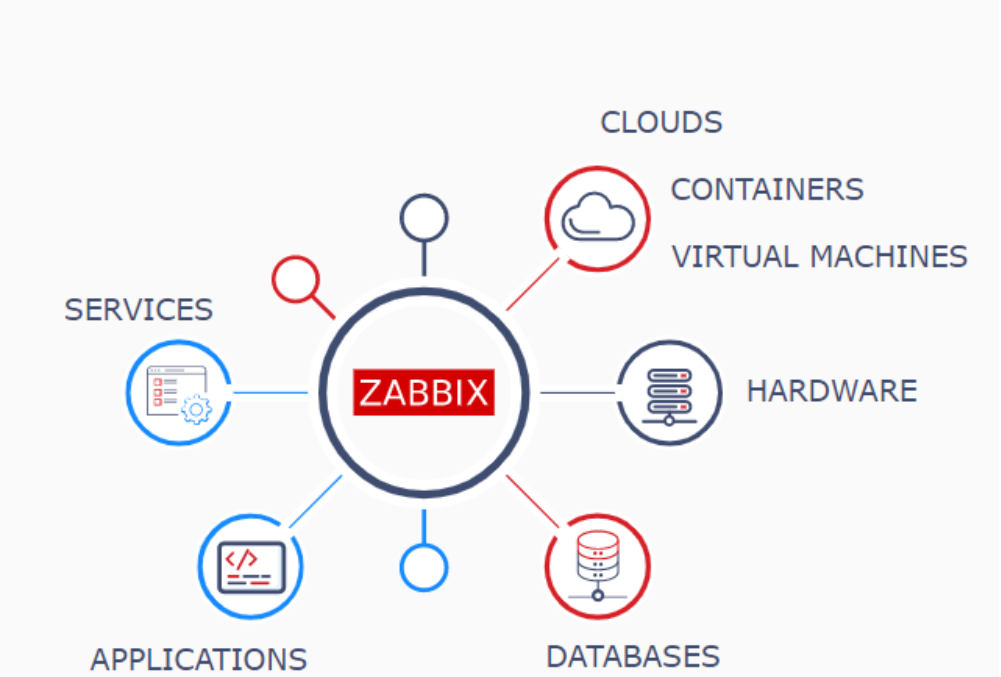
1. OpenNMS 可使用多樣的資料蒐集方式如JMX、WMI、SNMP、NRPE、XML、HTTP、JDBC、 XML、JSON等。
2. 事件導向架構，支援Grafana，有很好的使用者介面和美觀的儀表板和報表。



https://www.opennms.com/

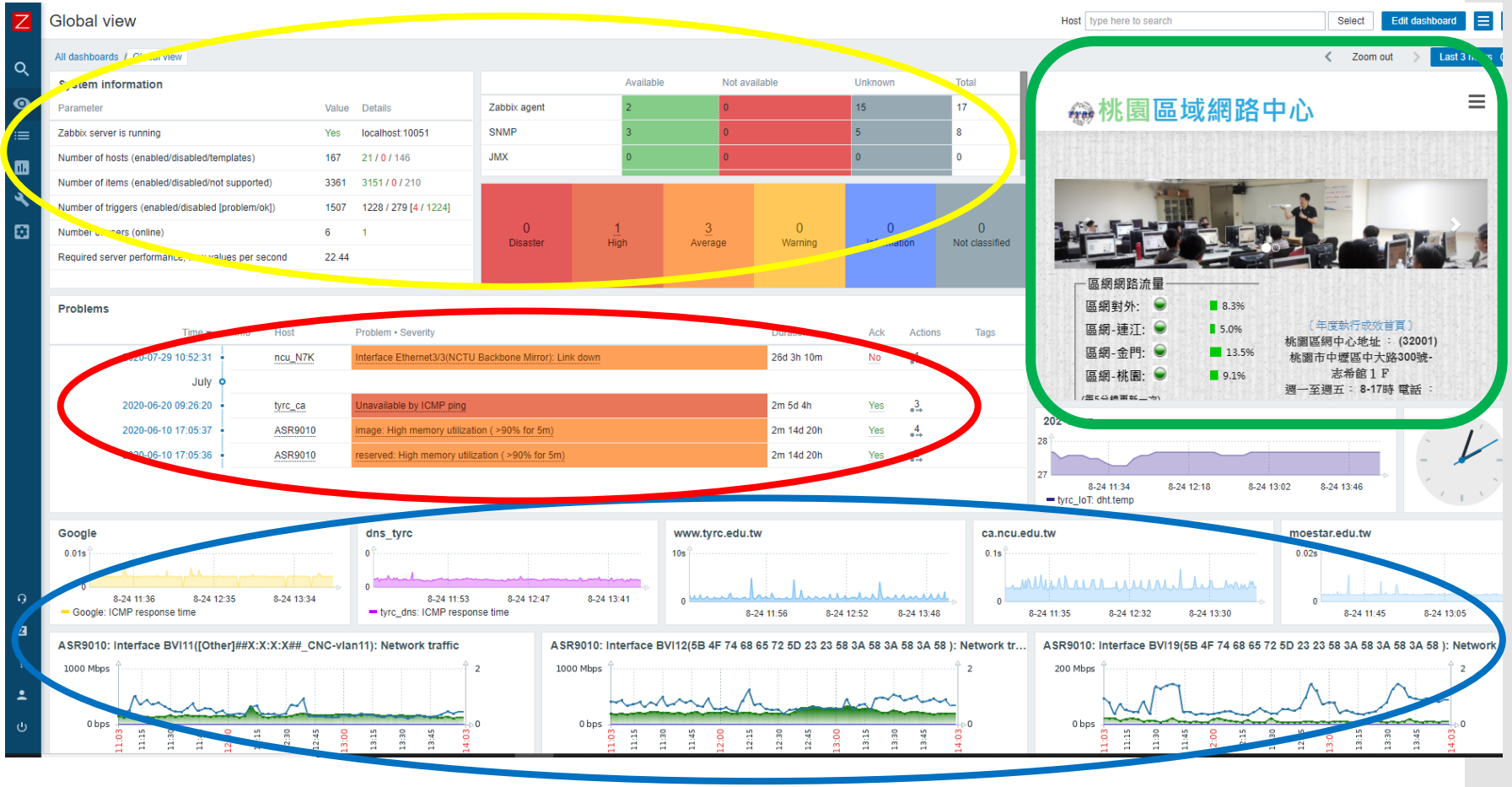
Zabbix監測系統

1. 系統可以監測硬體、資料庫、應用程式與服務、雲端系統。
2. 主要使用SNMP、IPMI、ICMP以及Zabbix Agent程式監測。

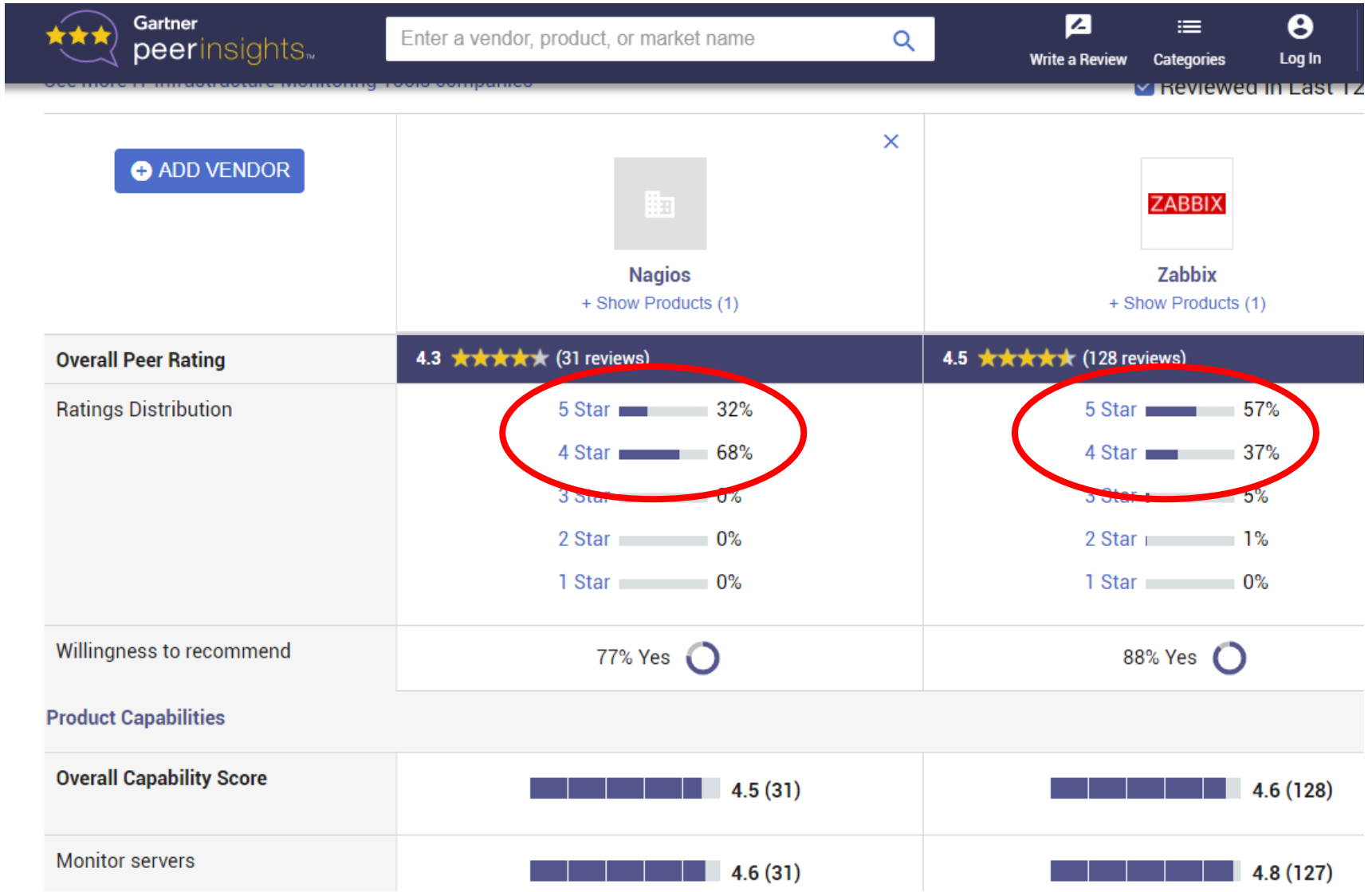


https://www.zabbix.com/features

Zabbix監測系統

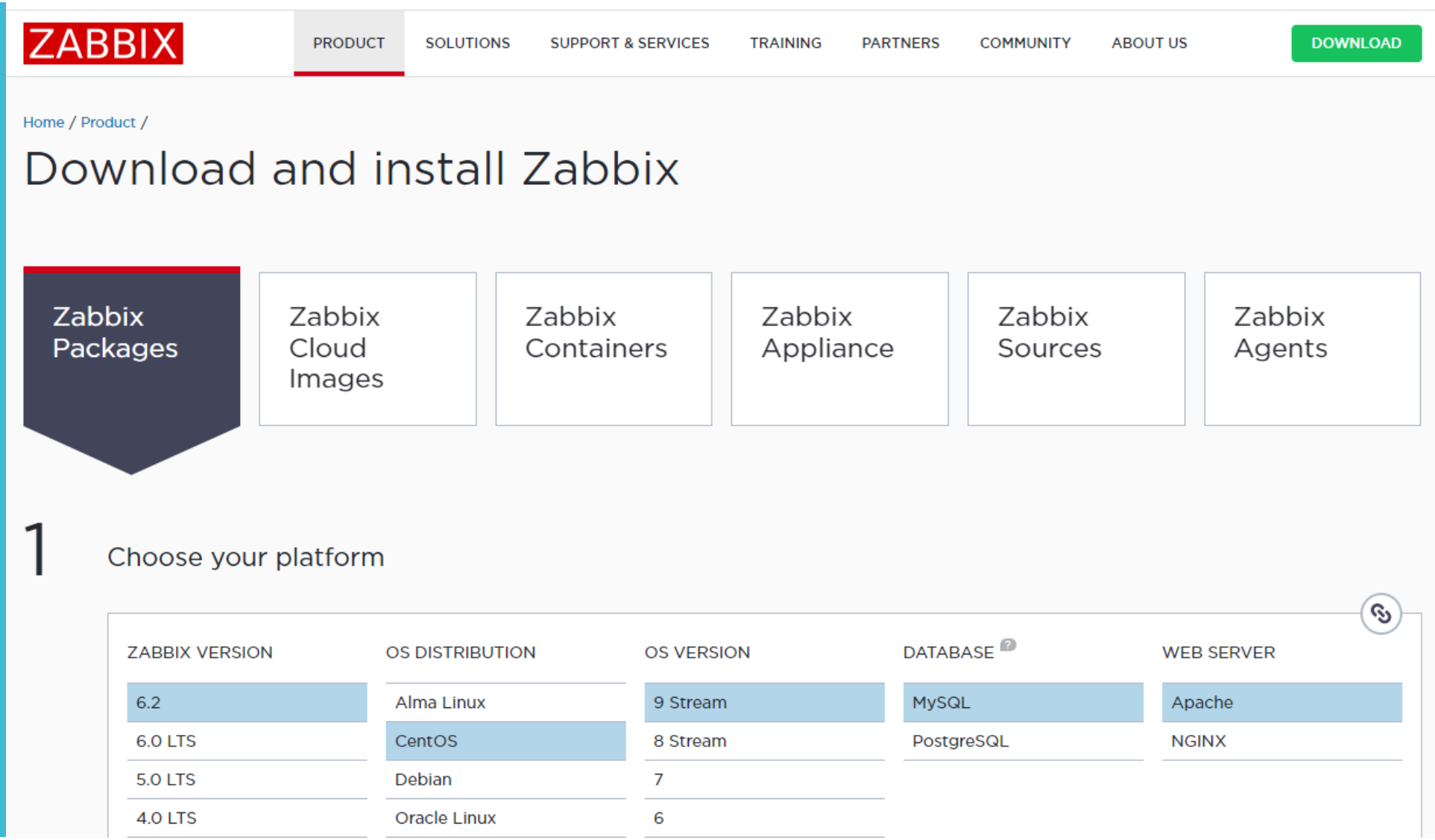

Global view
Host
type here to search
Select
Edit dashboard
All dashboards
System information
Parameter
Value
Details
Zabbix server is running
Yes
localhost:10051
Number of hosts (enabled/disabled/templates)
167
21 / 0 / 146
Number of items (enabled/disabled/not supported)
3361
3151 / 0 / 210
Number of triggers (enabled/disabled [problem/ok])
1507
1228 / 279 [4 / 1224]
Number of users (online)
6
1
Required server performance, new values per second
22.44
Available
Not available
Unknown
Total
Zabbix agent
2
0
15
17
SNMP
3
0
5
8
JMX
0
0
0
0
0 Disaster
1 High
3 Average
0 Warning
0 Information
0 Not classified
Problems
Time
Info
Host
Problem • Severity
Duration
Ack
Actions
Tags
2020-07-29 10:52:31
ncu_N7K
Interface Ethernet3/3(NCTU Backbone Mirror): Link down
26d 3h 10m
No
July
2020-06-20 09:26:20
tyrc_ca
Unavailable by ICMP ping
2m 5d 4h
Yes
2020-06-10 17:05:37
ASR9010
image: High memory utilization (>90% for 5m)
2m 14d 20h
Yes
2020-06-10 17:05:36
ASR9010
reserved: High memory utilization (>90% for 5m)
2m 14d 20h
Yes
Zoom out
桃園區域網路中心
區網網路流量
區網對外:
8.3%
區網-連江:
5.0%
區網-金門:
13.5%
區網-桃園:
9.1%
〔年度執行成效首頁〕
桃園區網中心地址：(32001)
桃園市中壢區中大路300號-
志希館１Ｆ
週一至週五：8-17時 電話：
tyrc_IoT: dht.temp
Google
Google: ICMP response time
dns_tyrc
tyrc_dns: ICMP response time
www.tyrc.edu.tw
ca.ncu.edu.tw
moestar.edu.tw
ASR9010: Interface BVI11([Other]##X:X:X:X##_CNC-vlan11): Network traffic
ASR9010: Interface BVI12(5B 4F 74 68 65 72 5D 23 23 58 3A 58 3A 58 3A 58): Network tr...
ASR9010: Interface BVI19(5B 4F 74 68 65 72 5D 23 23 58 3A 58 3A 58 3A 58): Network
1000 Mbps
0 bps
200 Mbps

Nagios vs Zabbix



https://www.gartner.com/reviews/market/it-infrastructure-monitoring-tools/compare/nagios-vs-zabbix

Zabbix系統安裝(1)



https://www.zabbix.com/download

Zabbix系統安裝(2)

ZABBIX

PRODUCT | SOLUTIONS | SUPPORT & SERVICES | TRAINING | PARTNERS | COMMUNITY | ABOUT US | DOWNLOAD

2 Install and configure Zabbix server for your platform

a. Install Zabbix repository

Documentation

```
# wget https://repo.zabbix.com/zabbix/6.2/ubuntu/pool/main/z/zabbix-release/zabbix-release_6.2-1+ubuntu22.04_all.deb
# dpkg -i zabbix-release_6.2-1+ubuntu22.04_all.deb
# apt update
```

b. Install Zabbix server, frontend, agent

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

c. Create initial database

Documentation

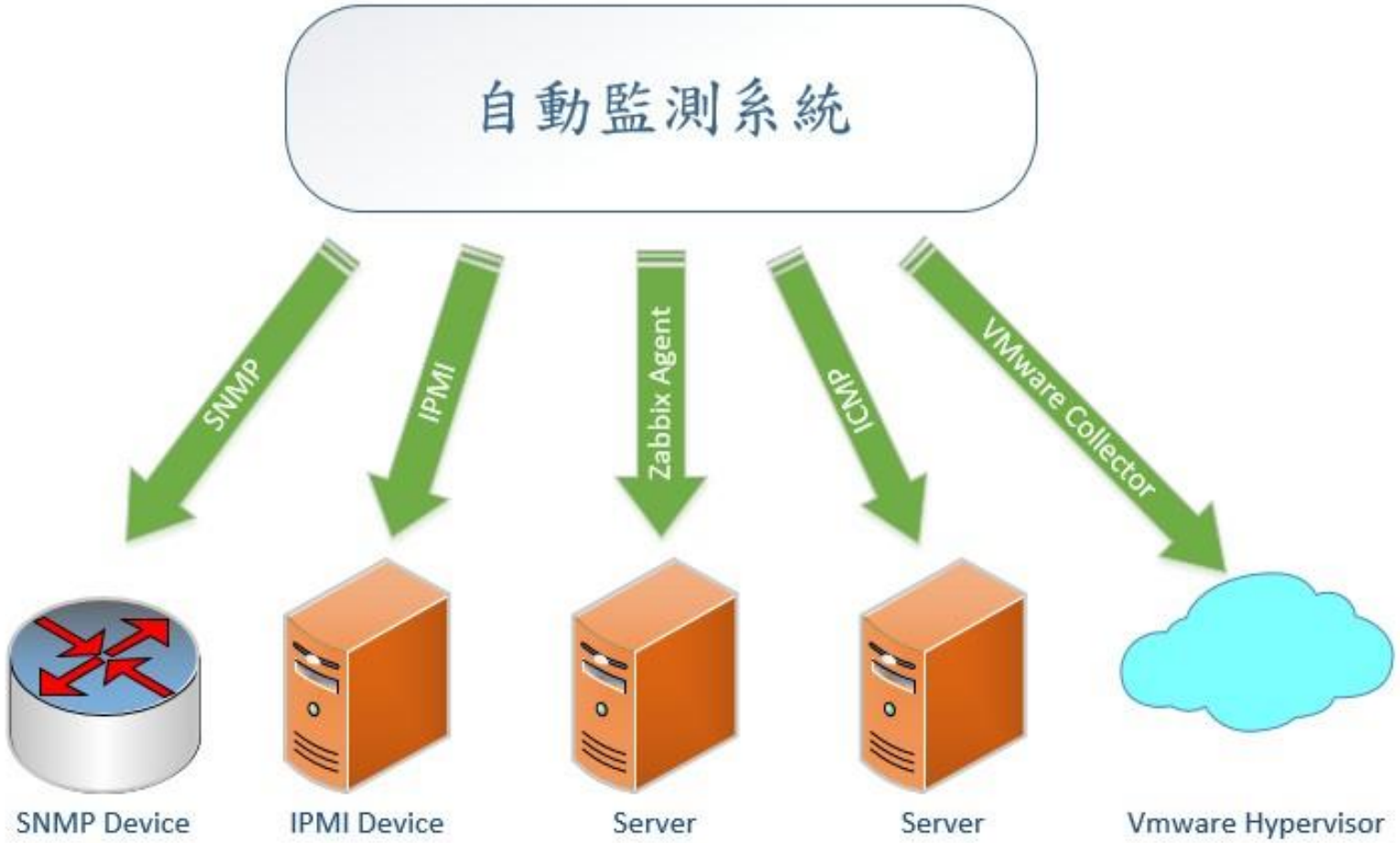
Make sure you have database server up and running.

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;
```

https://www.zabbix.com/download

自動化監測機制


自動監測系統
SNMP
IPMI
Zabbix Agent
ICMP
VMware Collector
SNMP Device
IPMI Device
Server
Server
Vmware Hypervisor

IPMI

- 智慧型平台管理介面（Intelligent Platform Management Interface）可以透過網路遠端控制溫度、電壓。
- IPMI可以用來監測硬體的狀態，包括主機溫度、風扇轉速、電流感應器等。
- IPMI獨立於作業系統外自行運作，可在受監控的系統關機但有接電源的情況下仍能遠端管理系統。

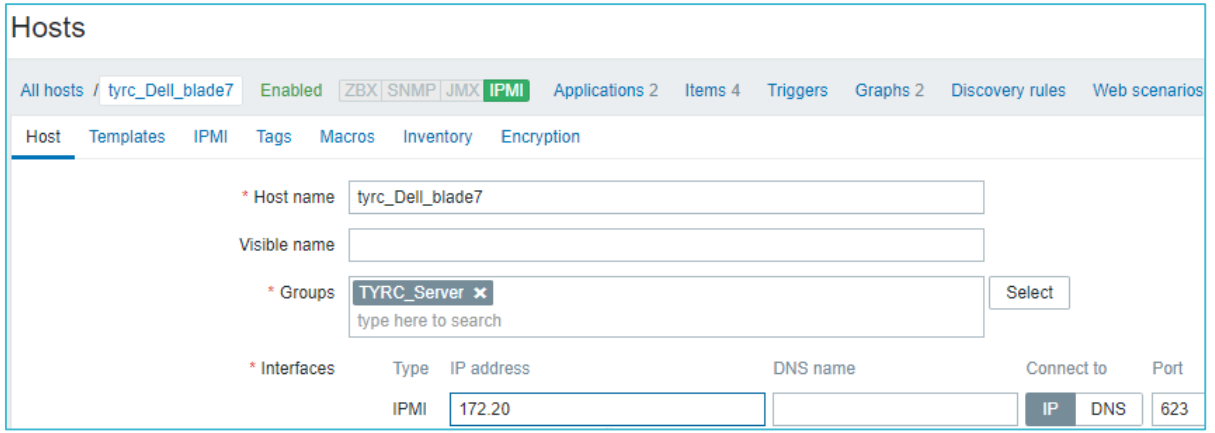
https://zh.wikipedia.org/wiki/IPMI

以IPMI 監測(1)

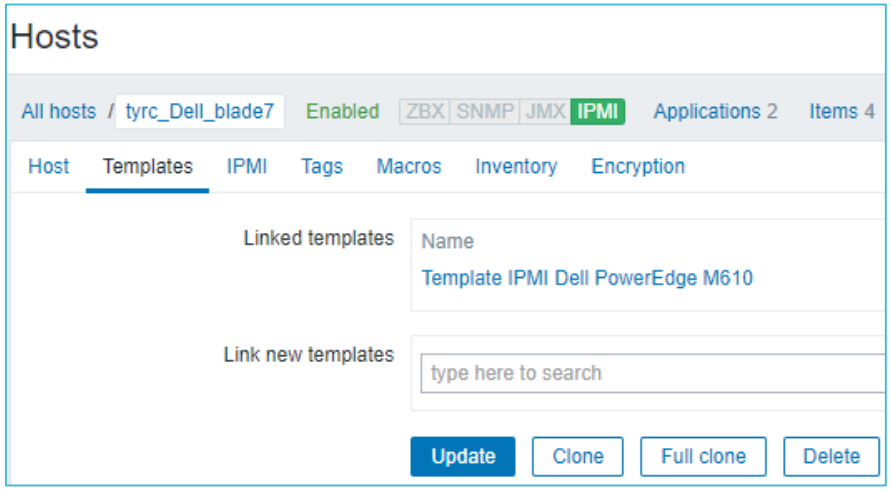
- 刀鋒伺服器設置介面開啟IPMI

以IPMI 監測(2)

- Step 1: Zabbix設定要監控的伺服器IP 及 port 623

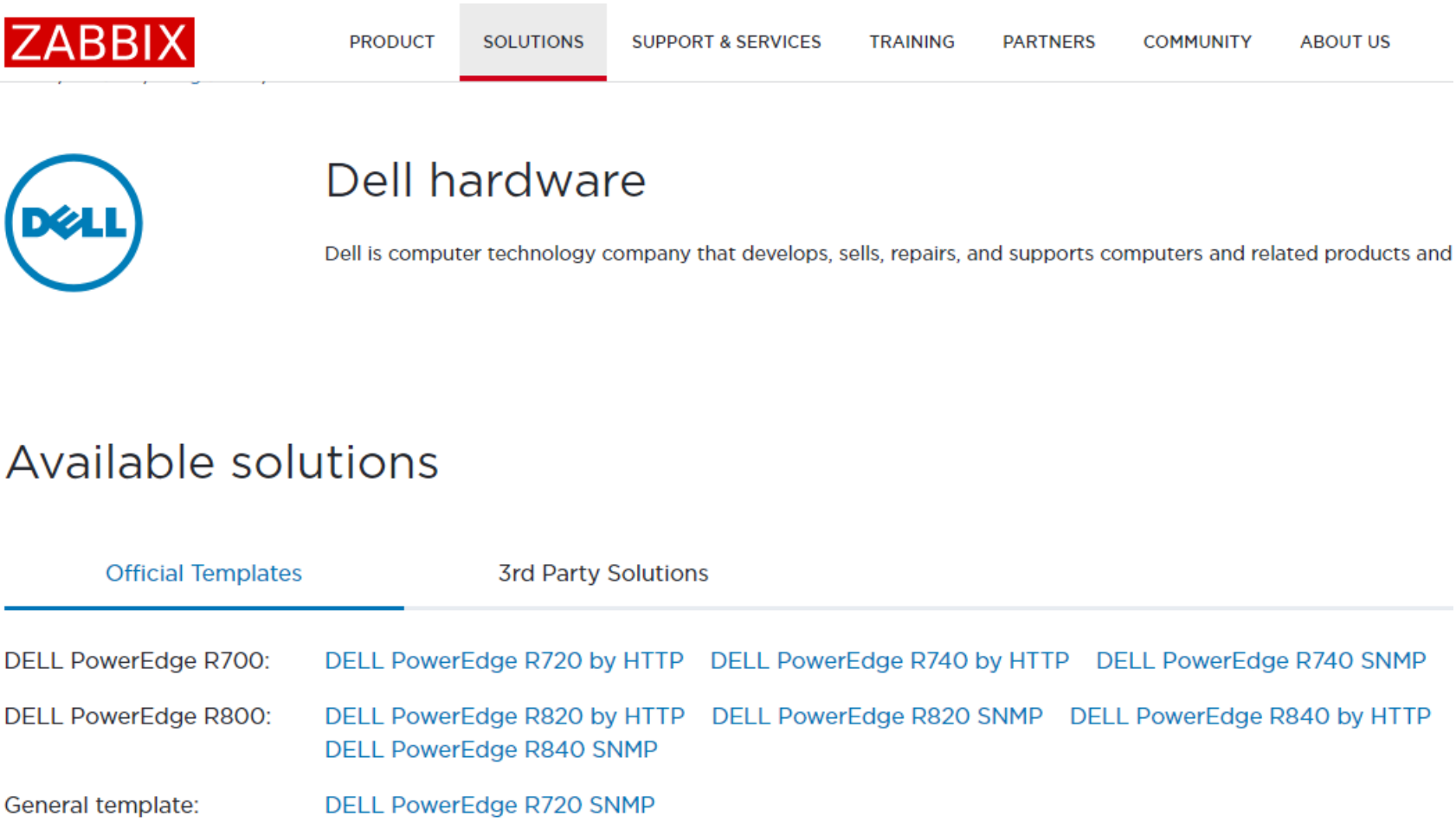


- Step 2: 連結範本



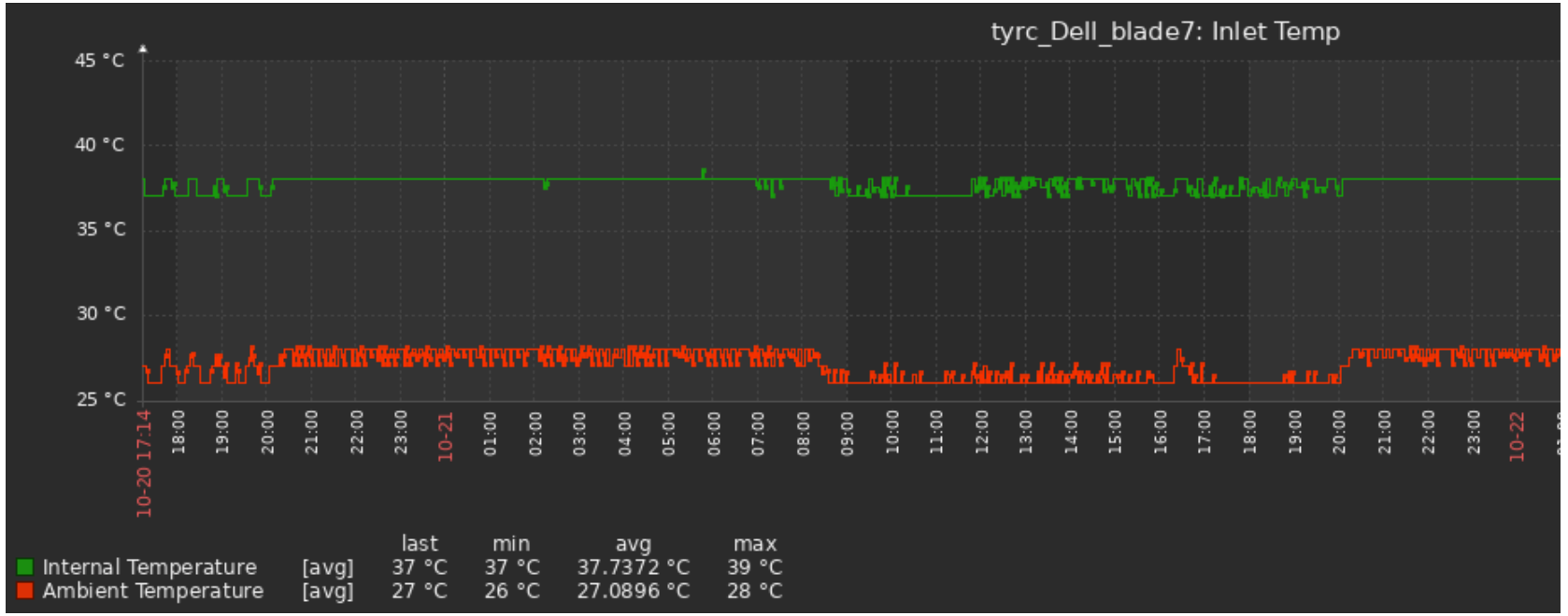
以IPMI 監測(3)

- 如果系統沒有安裝該主機範本，可至Zabbix網站下載官方或第三方範本。



以IPMI 監測(4)

- IPMI可以在缺少作業系統或系統管理軟體下，管理主機及監測硬體的狀態

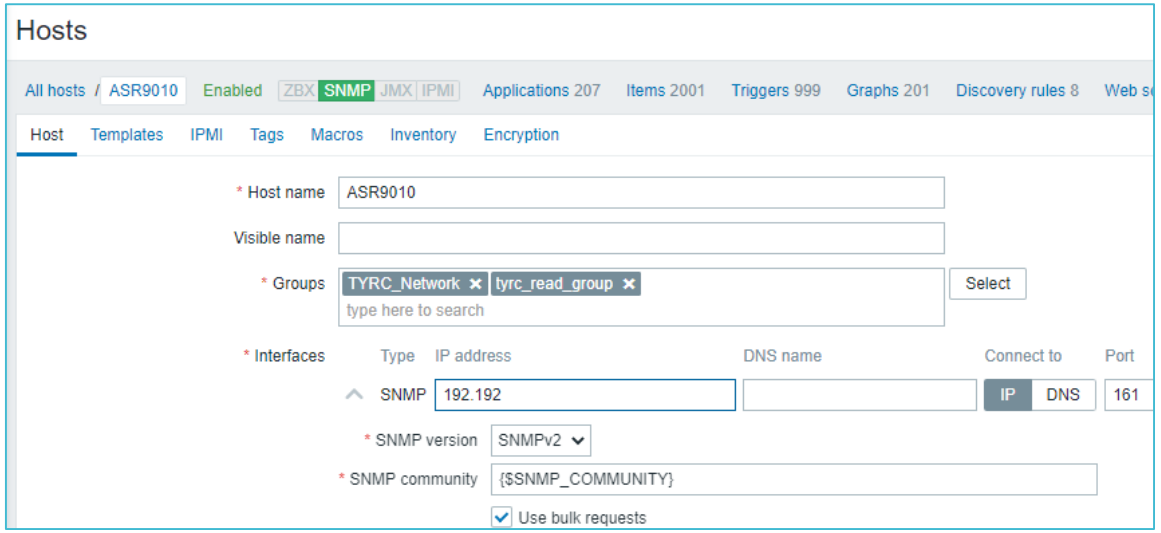


SNMP

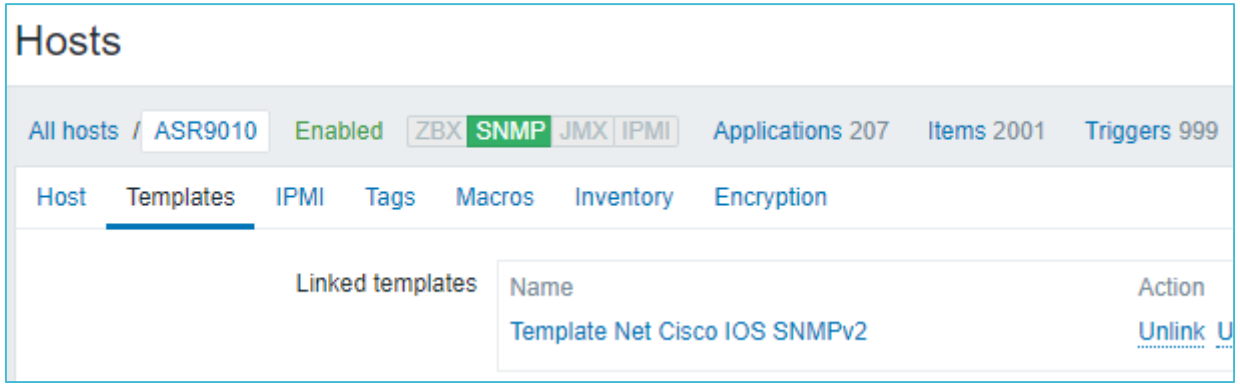
- 多數網路設備如交換器、路由器及UPS都支援SNMP。
- Use bulk requests 以一個request直接存取SNMP MIB多個數值。
- 請設定只允許特定IP可以讀取設備上的SNMP資料

以SNMP監測(1)

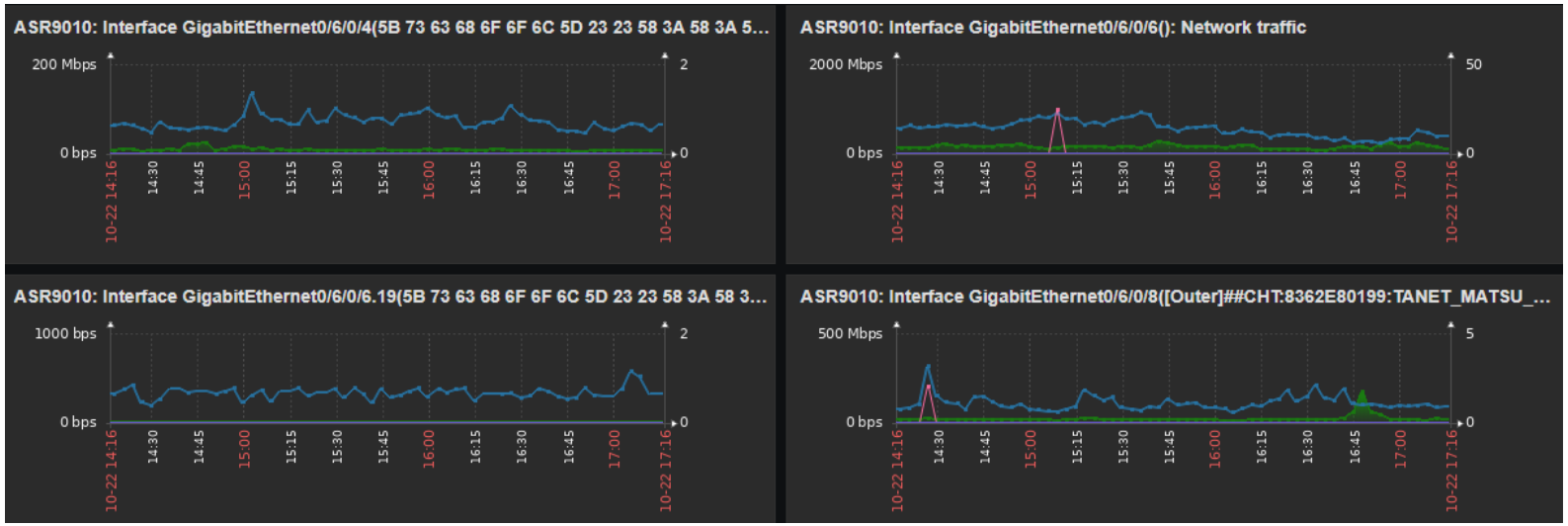
- Step 1: Zabbix設定要監控的伺服器IP 及 port 161



- Step 2: 連結範本

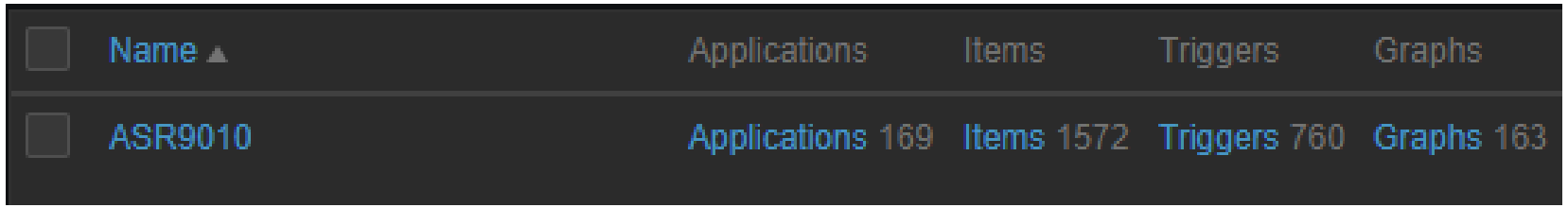


以SNMP監測(2)



- 每個網路介面的監測項目有9個監測項目
  - 接收位元數、傳送位元數
  - 出口錯誤封包數、入口錯誤封包數
  - 出口丟棄封包數、入口丟棄封包數
  - 介面型態
  - 介面網路速度
  - 介面狀態

以SNMP監測(3)



- 系統使用Discovery rules自動找出區網核心路由器169個系統狀態及網路介面
- 合計1572個監測項目以及760個觸發條件。
- 每個網路介面有以下4種觸發條件
  - 介面關閉
  - 高使用率
  - 高錯誤率
  - 介面速率變化

監測雲端Hypervisor(1)

1. 針對雲端虛擬機器例如VMware Hypervisor主要透過SOAP protocol與VMware web 溝通進行監測。

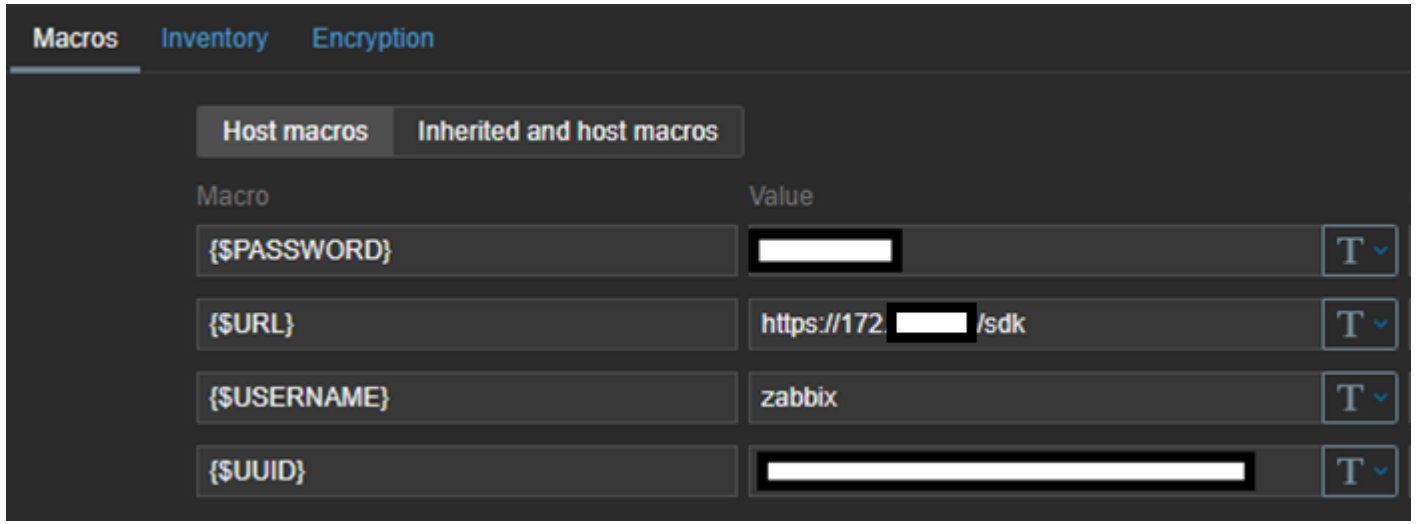
2. 讀取VMware 效能資料包含系統負荷、CPU 使用率、記憶體使用率等統計資料。

3. Hypervisor下的每一個虛擬機器也可以自動帶入，而毋須逐一新增虛擬機器。

監測雲端 Hypervisor(2)

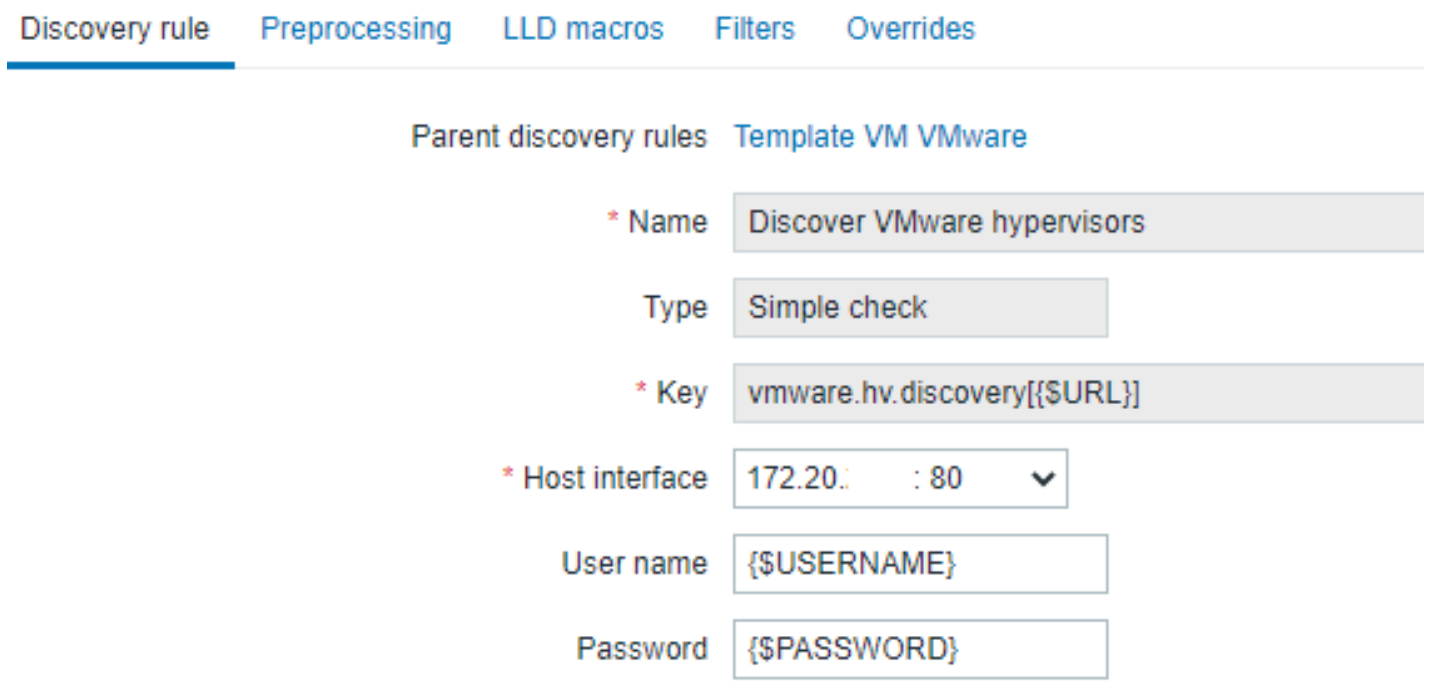
- 設定連結Template VM VMware範本，在系統的Macros定義USERNAME、PASSWORD、URL等參數

- 其中URL指向 Vmware ESXi的 SDK，指向 Vmware 的 https://x.x.x.x/sdk



監測雲端 Hypervisor(3)

- 不需要手動加入Hypervisor下的每一個虛擬機器
- Discovery rules規則自動帶入所有VM



以ICMP監測(1)

1. 對於遠端網路或遠方主機並無讀取SNMP、IPMI或安裝Agent程式的權限，可以利用ICMP監測遠端網路。
2. 使用ICMP，預設是60秒執行一次檢查。
3. 預設檢查項目為ICMP loss、ICMP ping、ICMP response time。

以ICMP監測(2)


Google: ping_loss
60 %
50 %
40 %
30 %
20 %
10 %
0 %
10-20 17:24
18:00
19:00
20:00
21:00
22:00
23:00
10-21
01:00
02:00
03:00
04:00
05:00
06:00
07:00
08:00
09:00
10:00
11:00
12:00
13:00
14:00
15:00
16:00
17:00
18:00
19:00
20:00
21:00
22:00
23:00
10-22
01:00
02:00
03:00
04:00
05:00
last min avg max
ICMP loss [avg] 0 % 0 % 0.9863 % 100 %
Google: ping_response
0.2s
0.15s
0.1s
0.05s
0
10-20 17:24
18:00
19:00
20:00
21:00
22:00
23:00
10-21
01:00
02:00
03:00
04:00
05:00
06:00
07:00
08:00
09:00
10:00
11:00
12:00
13:00
14:00
15:00
16:00
17:00
18:00
19:00
20:00
21:00
22:00
23:00
10-22
01:00
02:00
03:00
04:00
05:00
last min avg max
ICMP response time [avg] 4ms 0 6ms 158ms
Trigger: High ICMP ping response time [> 0.15]

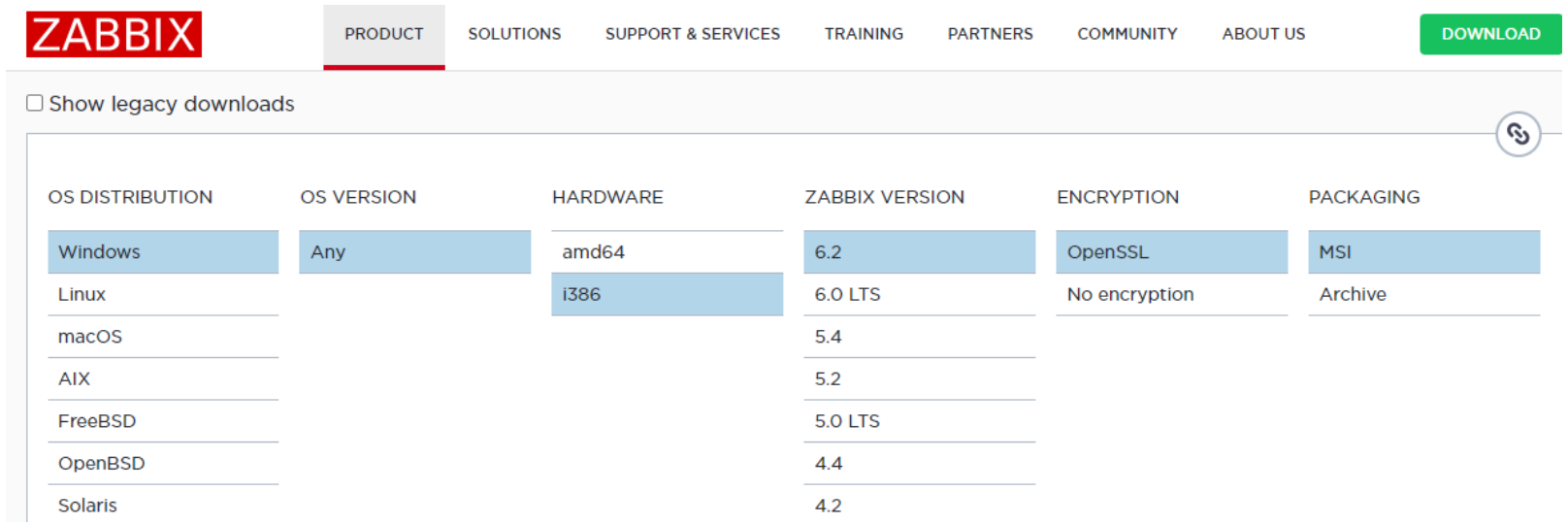
以Agent 程式監測(1)

1. Zabbix Agent 程式，可安裝於如Windows及OpenBSD、Mac OS X、AIX、HP-UX、Solaris、FreeBSD、Linux等作業系統。

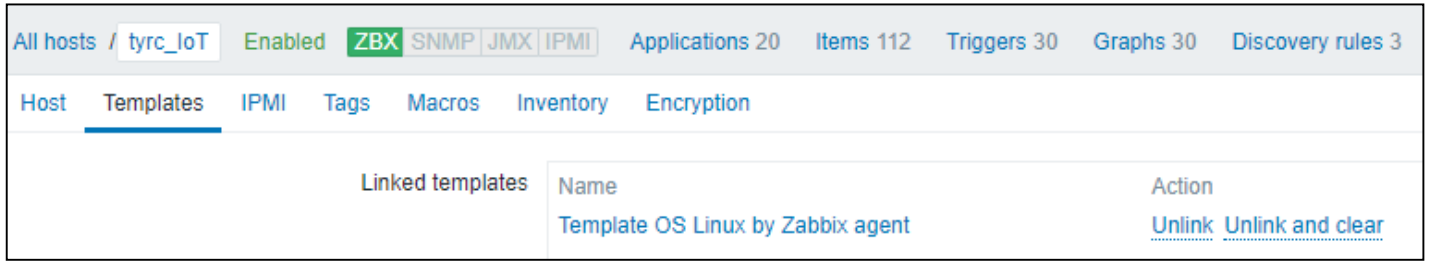
2. Agent 程式可提供更詳細的系統內部狀態，包含系統負荷、CPU 使用率、記憶體使用率、網路使用狀況、硬碟容量等。

以Agent 程式監測(2)

- Step 1:先在被監測主機安裝Zabbix Agent程式

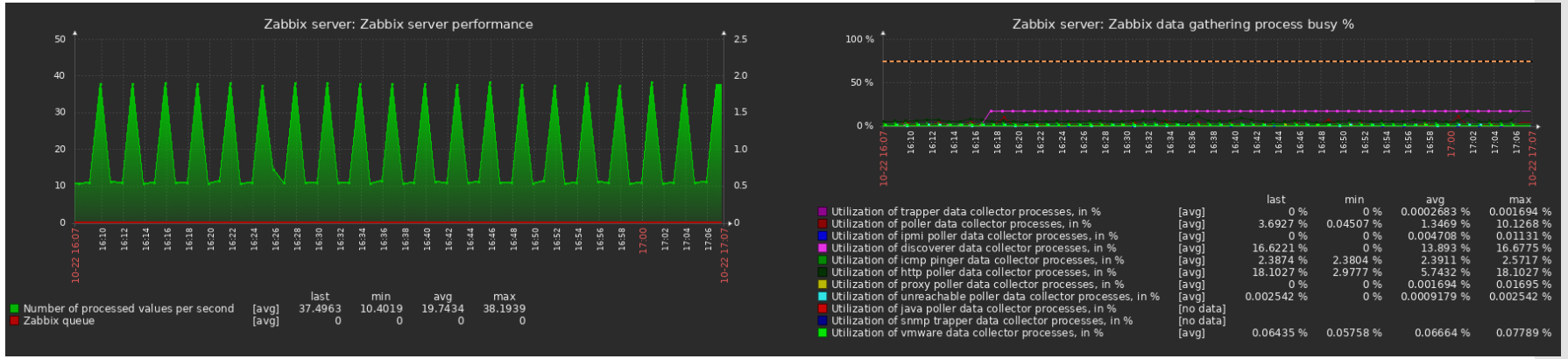


- Step 2:Zabbix 設定主機連結 Template OS by Zabbix agent 範本，即可讀取主機狀態



以Agent 程式監測(3)

- Agent和Server溝通方式有兩種
  - Passive Check －Server 發出要求Agent 資料
  - Active Check －Agent 定期回傳資料給Server
- Agent程式比起由外部偵測可提供更詳細的資料，包含CPU 使用率、記憶體使用率、網路使用狀況、硬碟容量等。

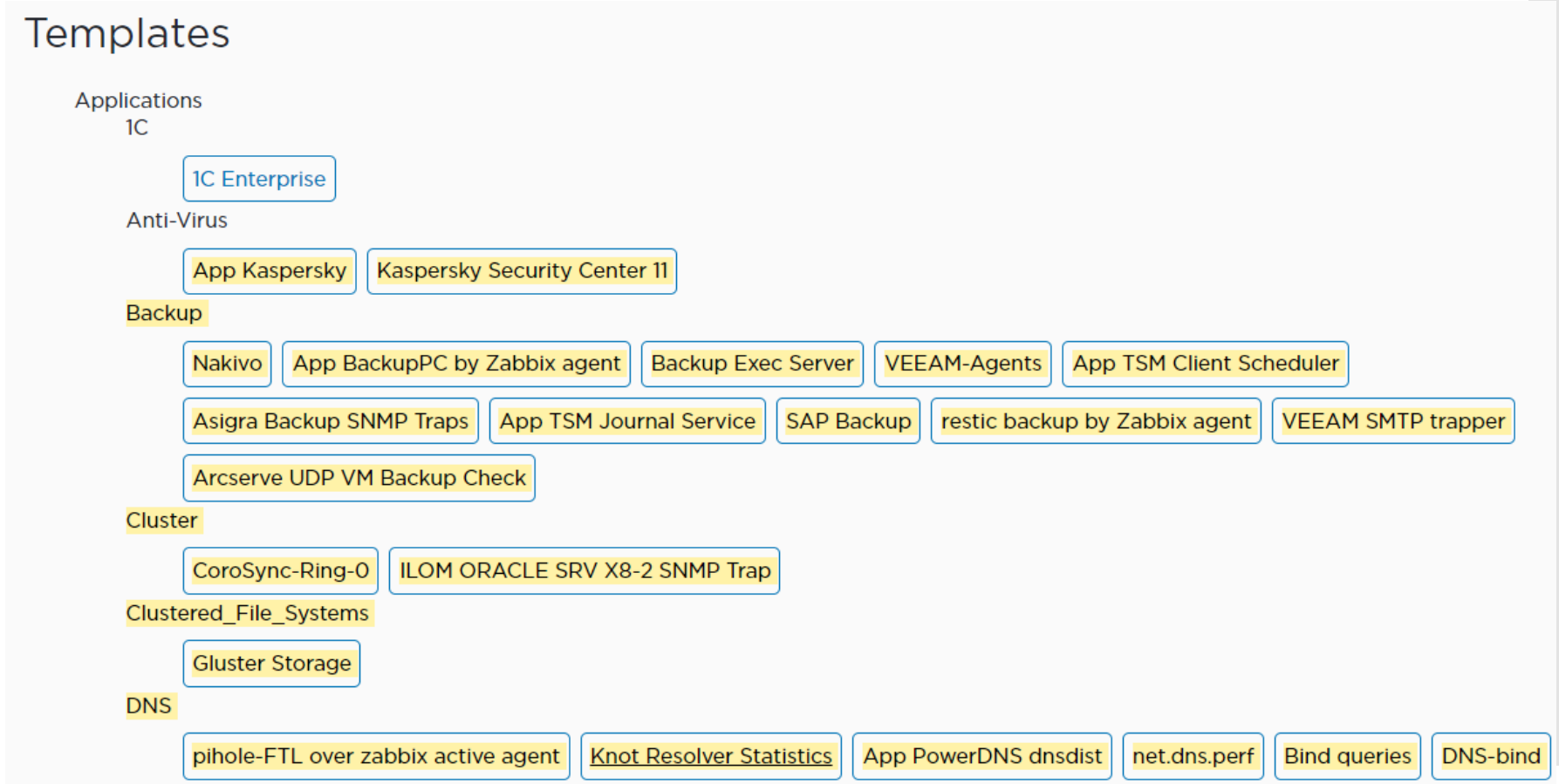


思考一
系統沒有我要的監測資料?

我要監測的設備，透過 SNMP、ICMP、IPMI、Agent程式，都沒有我要的監測資料?

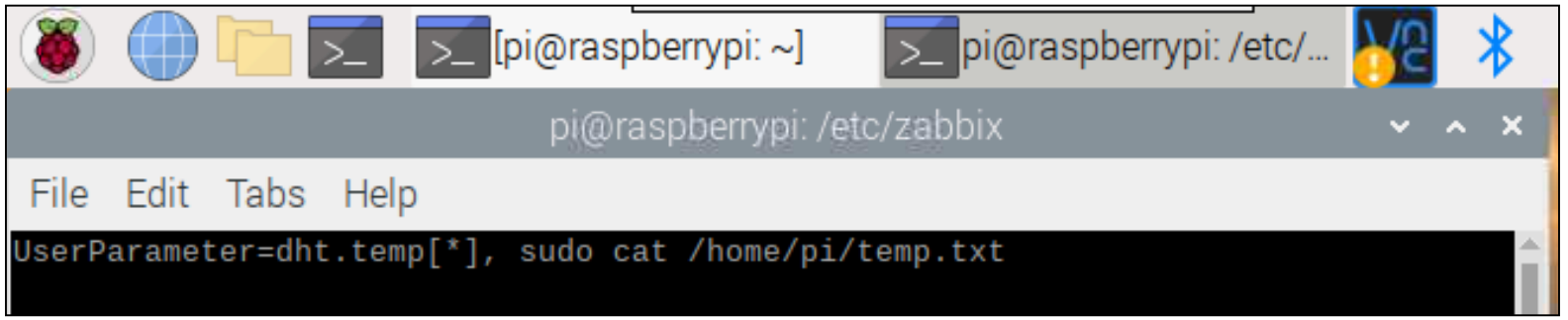
解決方案(1) Zabbix社群

- 下載Zabbix社群範本
- https://share.zabbix.com/

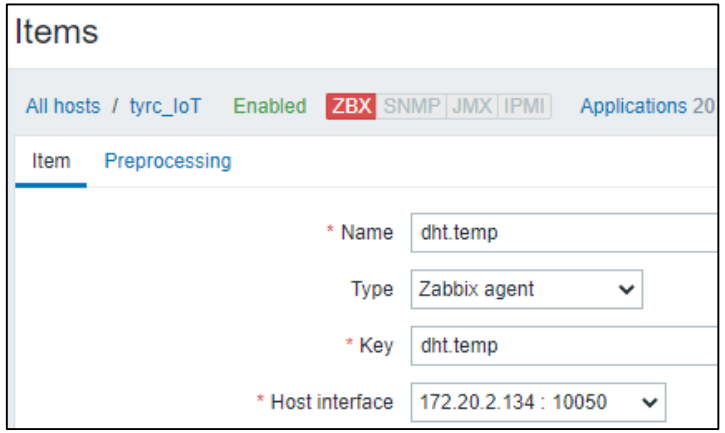


解決方案(2)
自己打造

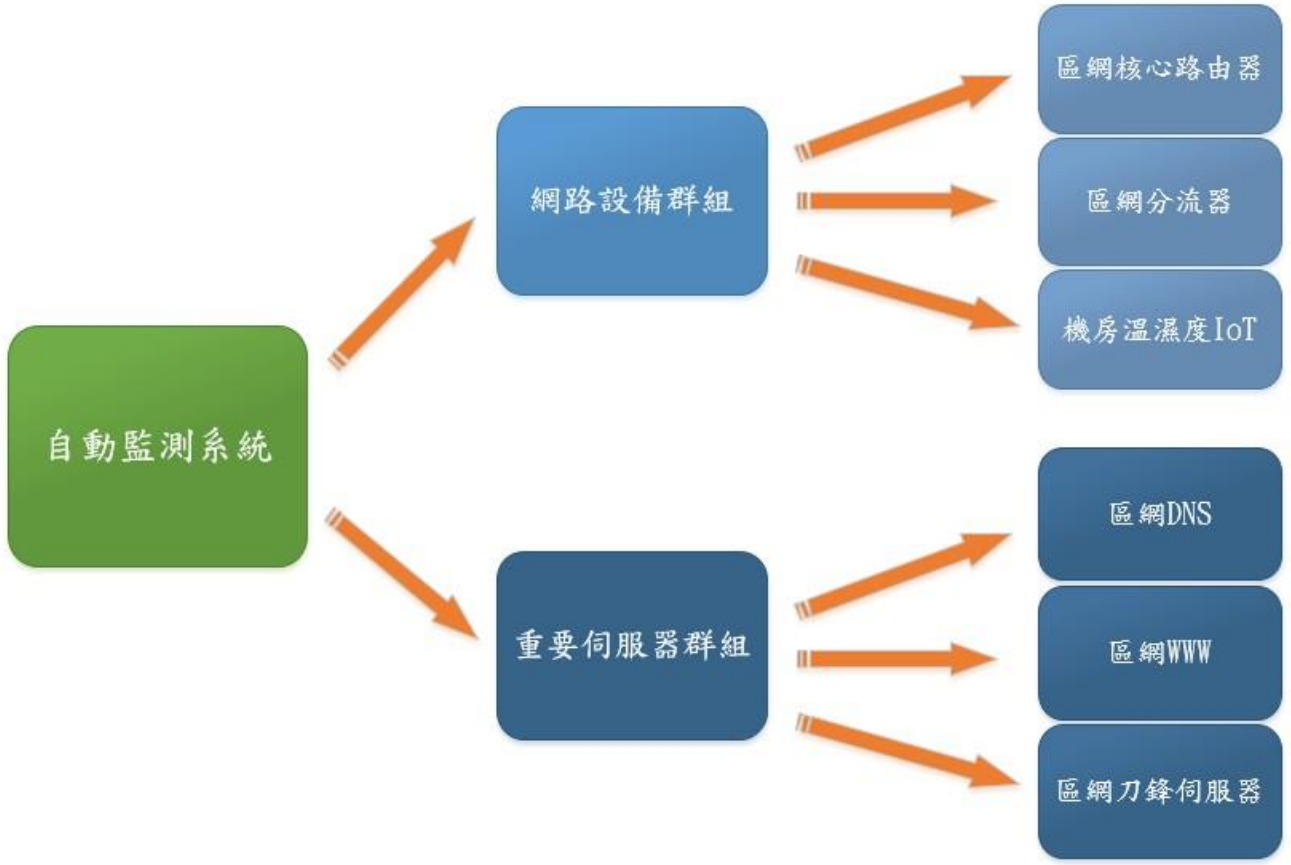
- 例如機房溫溼度監控，可以利用樹莓派實作機房溫溼度監控，樹莓派安裝Zabbix Agent，在 zabbix_agentd.conf設定檔加上使用者定義的回傳值。



- 在Zabbix加上使用者定義的監測Items



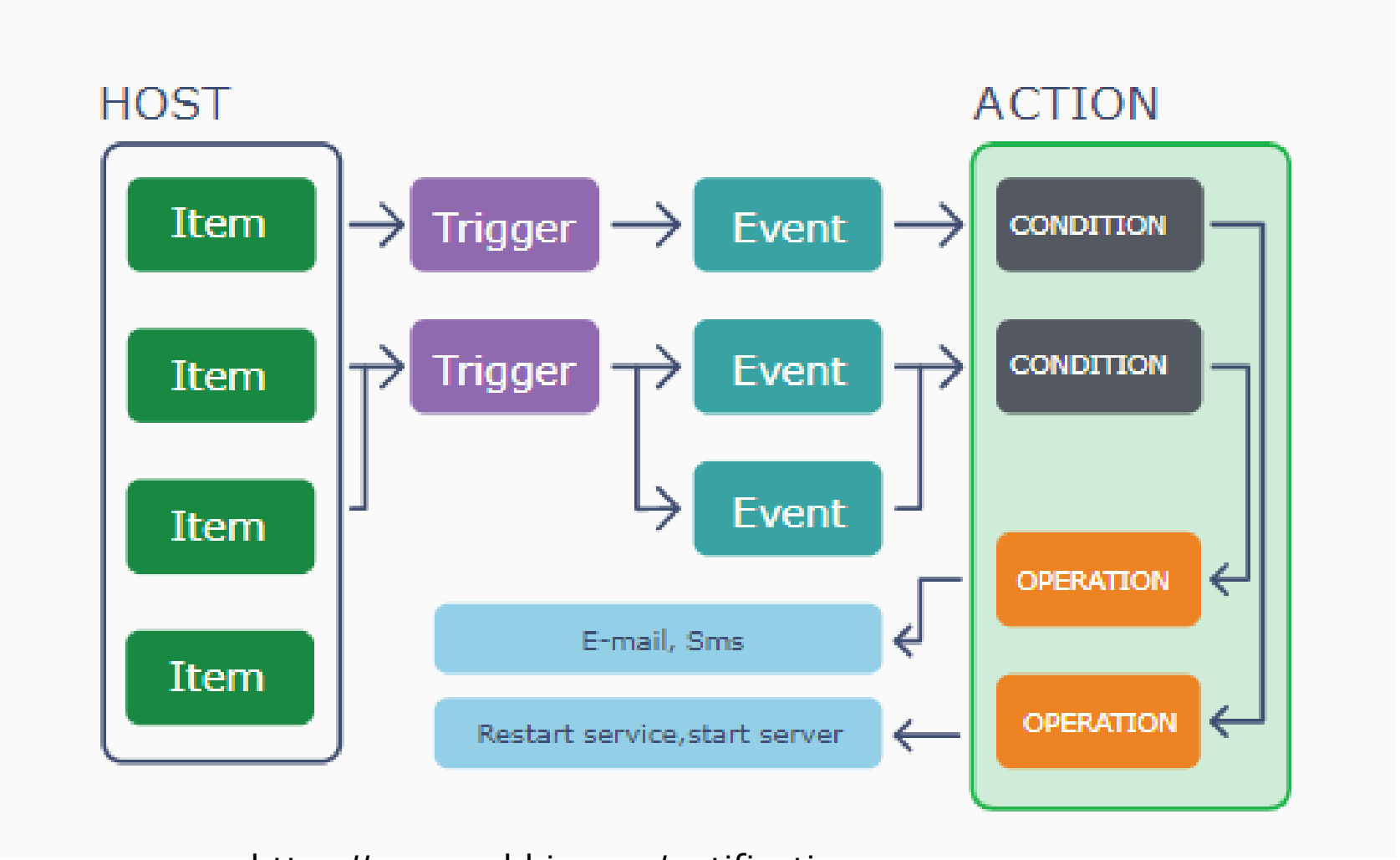
系統部署架構


自動監測系統
網路設備群組
重要伺服器群組
區網核心路由器
區網分流器
機房溫濕度IoT
區網DNS
區網WWW
區網刀鋒伺服器

管理架構

	區網網路設備	區網重要伺服器	校園網路設備	校園重要伺服器
區網管理者群組	Read-write	Read-write	Read	Read
區網使用者群組	Read	Read	Read	Read
校園網管群組	None	None	Read-write	Read-write
校園使用者群組	None	None	Read	Read

事件自動化告警機制(1)



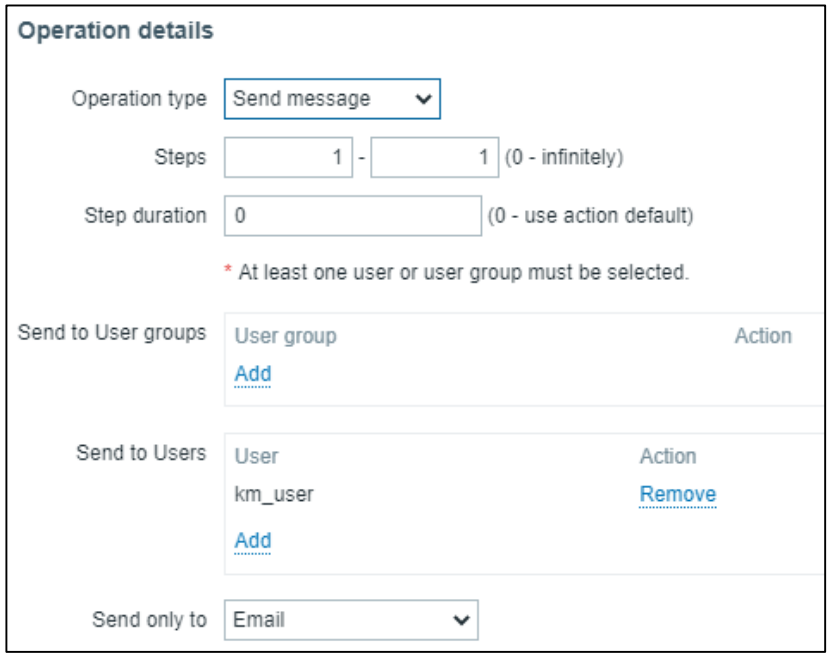
https://www.zabbix.com/notification

事件自動化告警機制(2)

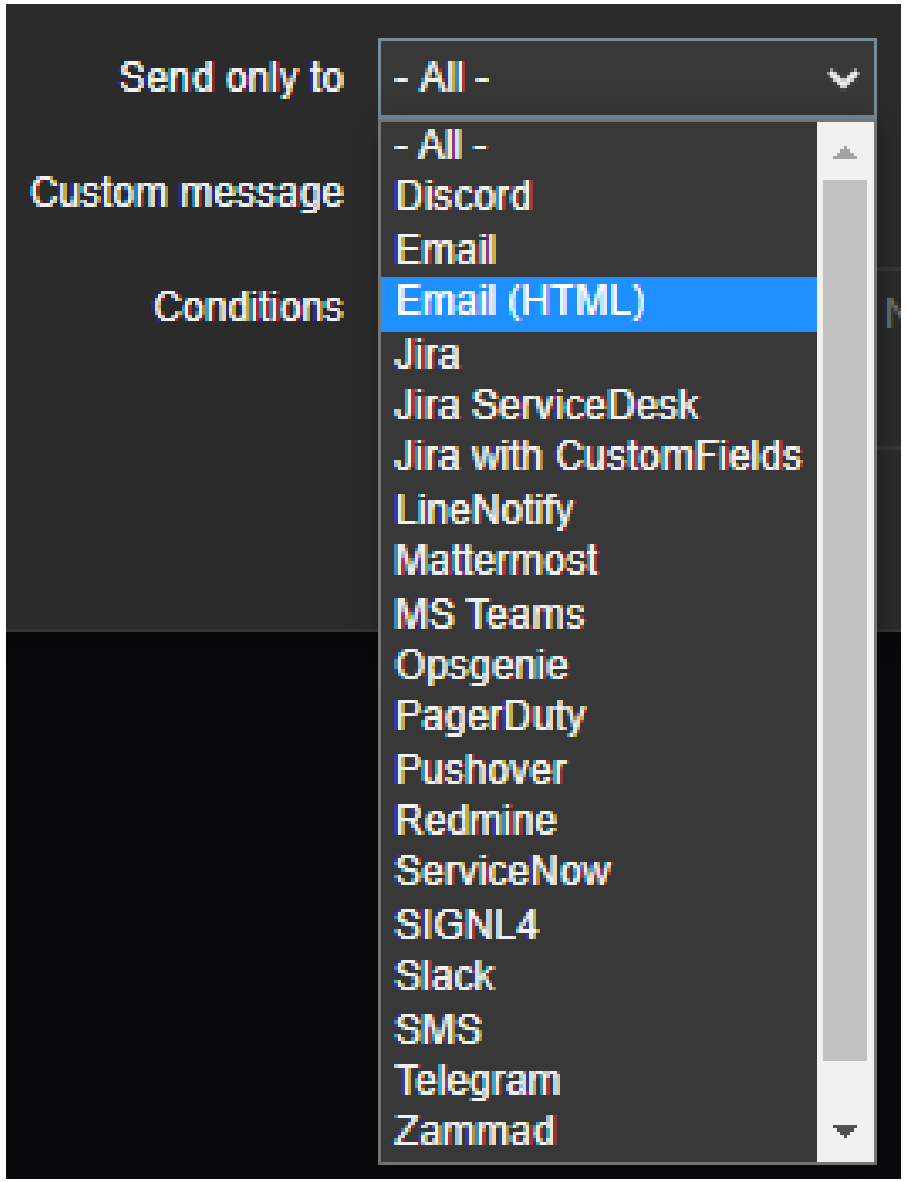
- 將收集到的監測項目數值判斷是否觸發規則。例如判斷某一網路介面是否為Link down?

```
{$IFCONTROL:"GigabitEthernet0/6/0/6.12"}=1
and ({ASR9010:net.if.status[ifOperStatus.184].last()}=2
and {ASR9010:net.if.status[ifOperStatus.184].diff()}=1)
```

- 觸發Trigers 會產生事件，並依照設定自動通知。



事件自動化告警機制(3)

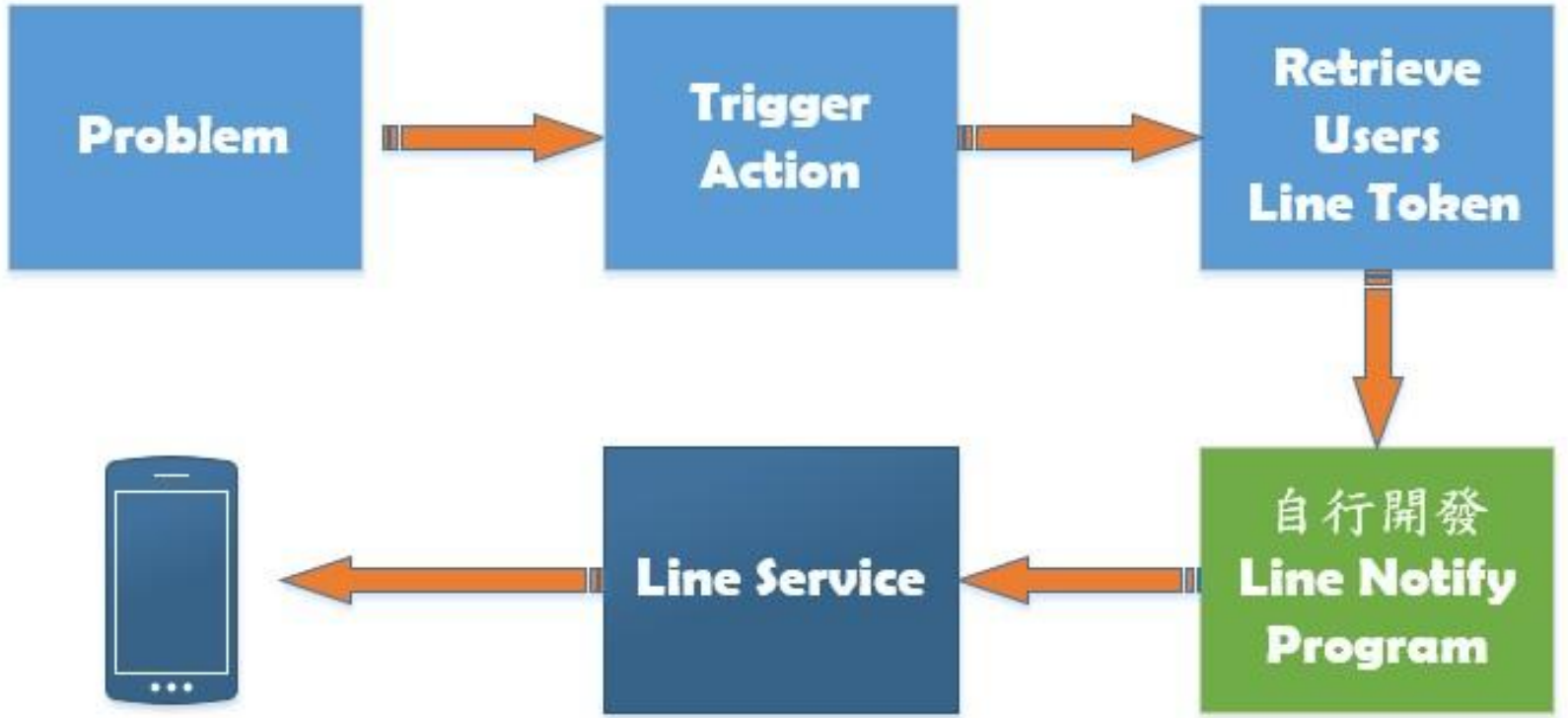

Send only to
- All -
Custom message
Conditions
- All -
Discord
Email
Email (HTML)
Jira
Jira ServiceDesk
Jira with CustomFields
LineNotify
Mattermost
MS Teams
Opsgenie
PagerDuty
Pushover
Redmine
ServiceNow
SIGNL4
Slack
SMS
Telegram
Zammad

思考二
系統沒有我要的告警方式?

1. 系統內建傳送通知的方式，包括Discord、Email、Jira、Mattermost、MS Teams、Opsgenie、PagerDuty、Pushover、Redmine、ServiceNow、SIGNL4、Slack、SMS、Telegram、Zammad、Zendesk等方法。

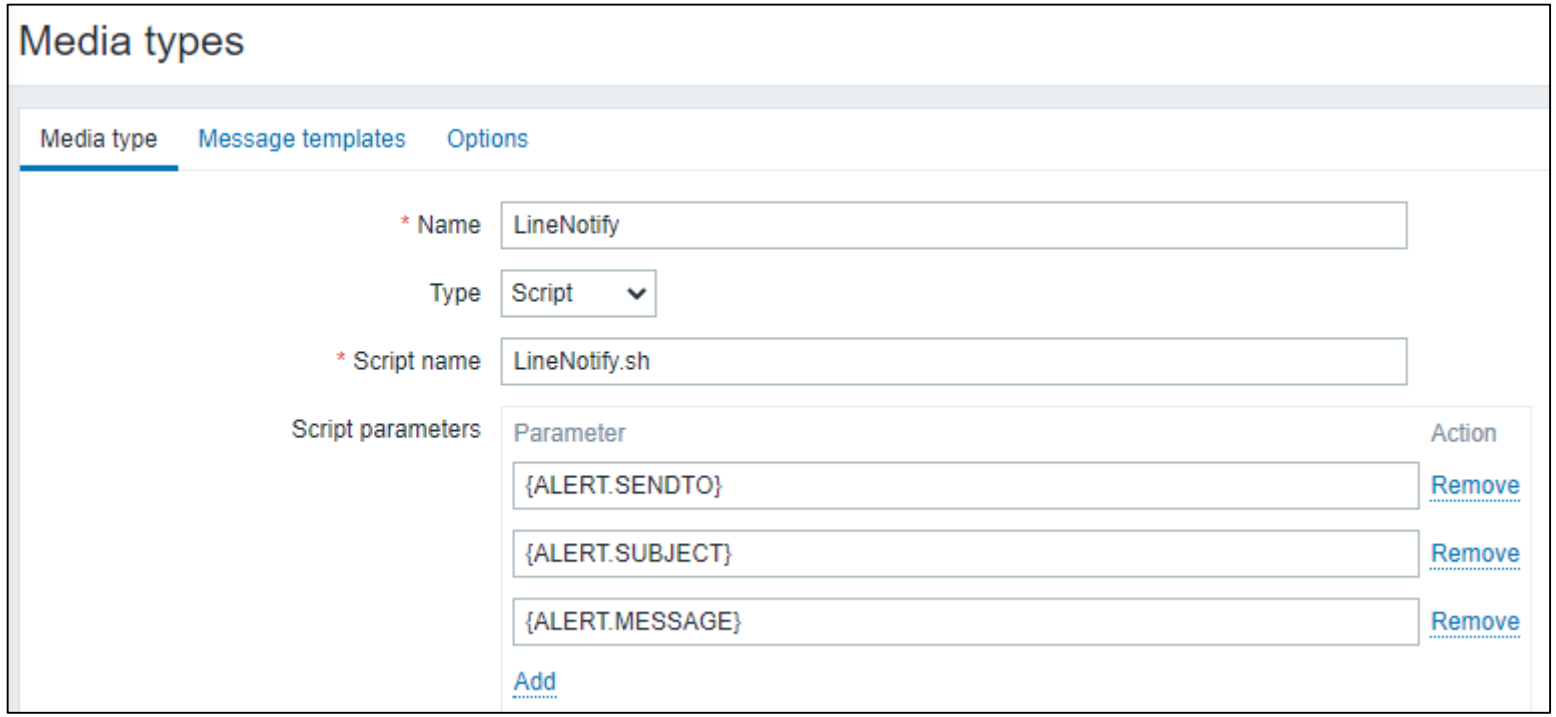
2. 但我想要使用LINE通知。

LINE Notify
程式處理流程

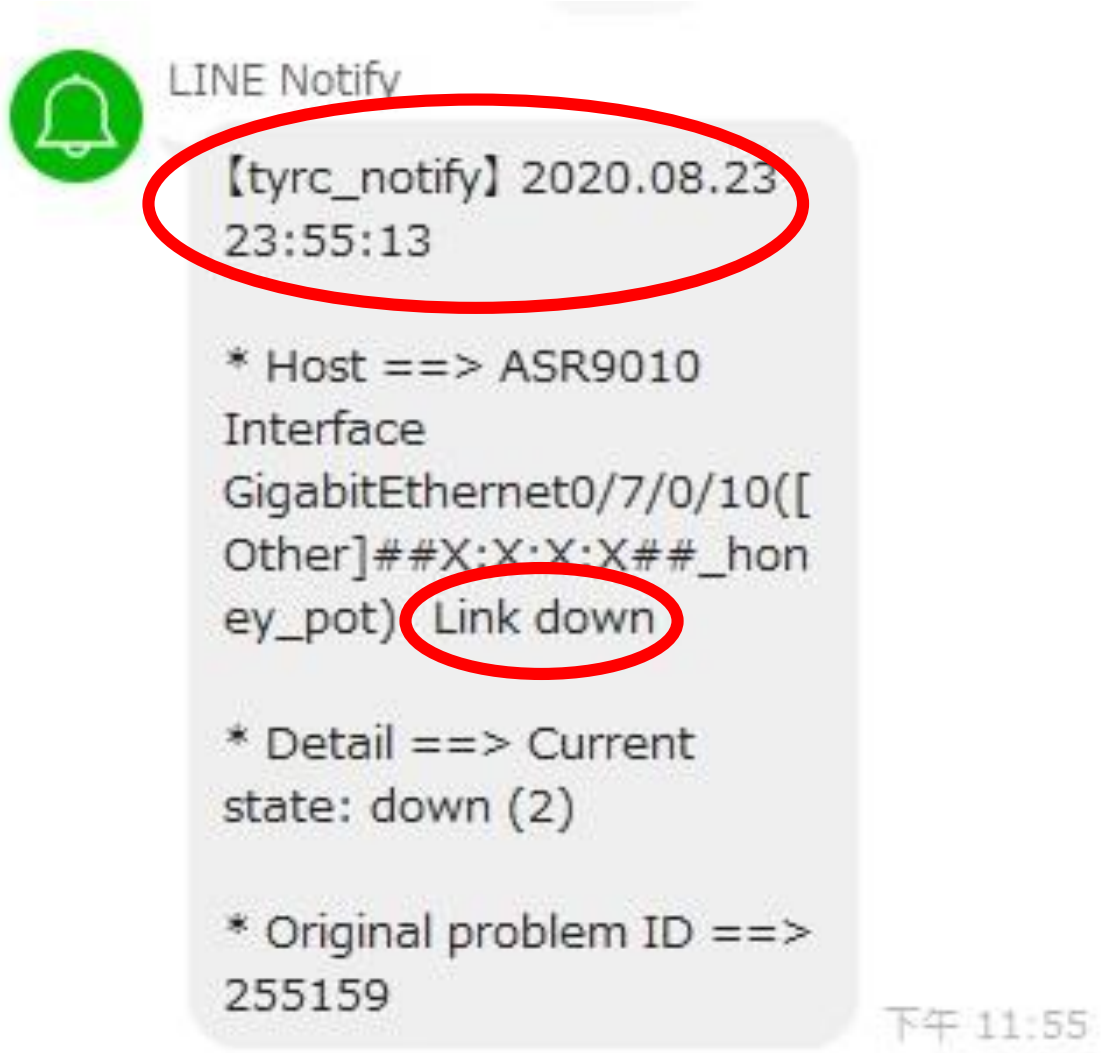


自行開發 LineNotify.sh

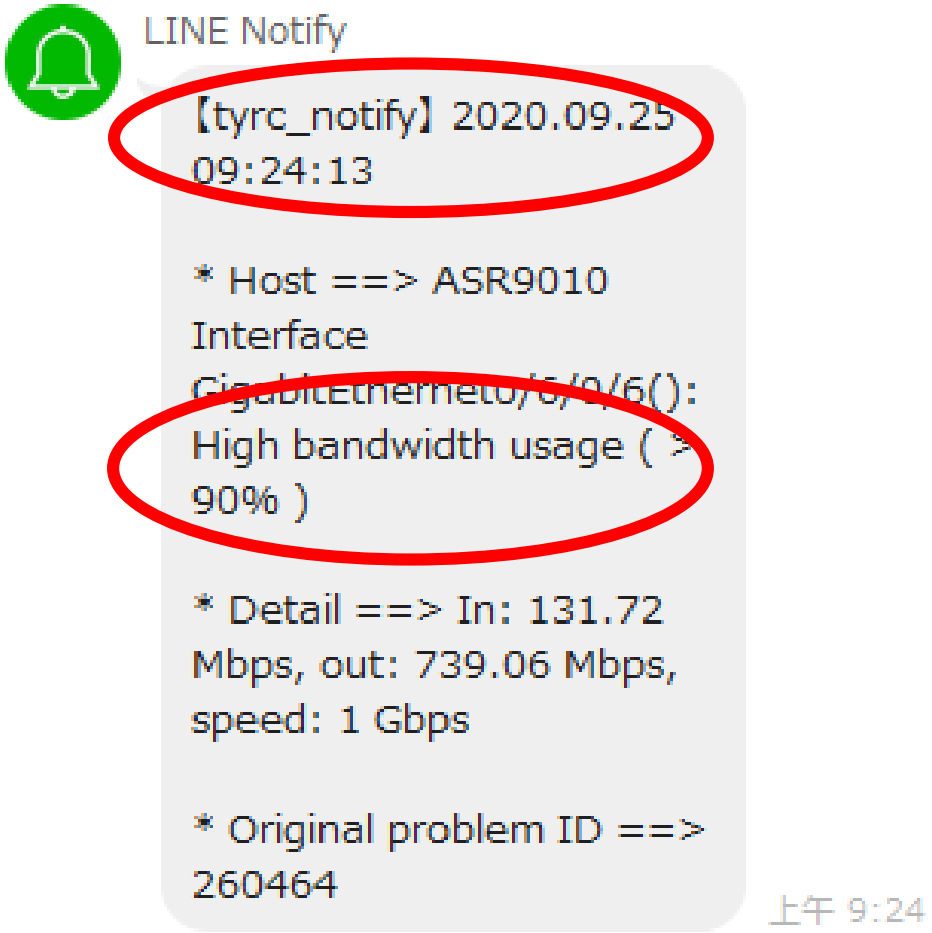
- Step 1:透過LINE Notify產生自己的個人權杖，然後自行開發LineNotify.sh，發送請求到API端點。
- Step 2:在Zabbix新增一個Media types。



即時告警案例(1)連線中斷



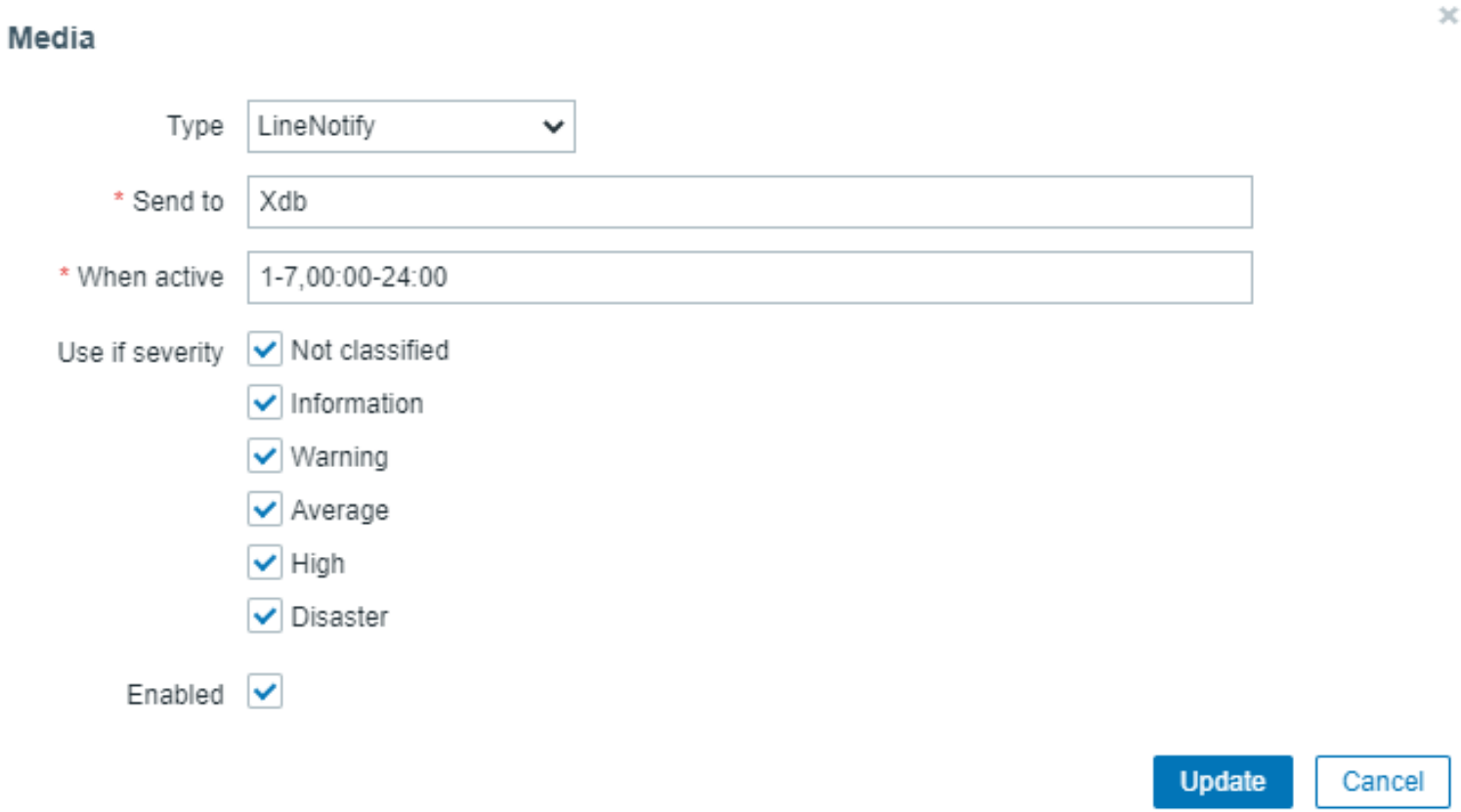
即時告警案例(2)網路壅塞



思考三
用LINE傳送，變成7-11?

用LINE傳送，我變成7-11，不用下班了?

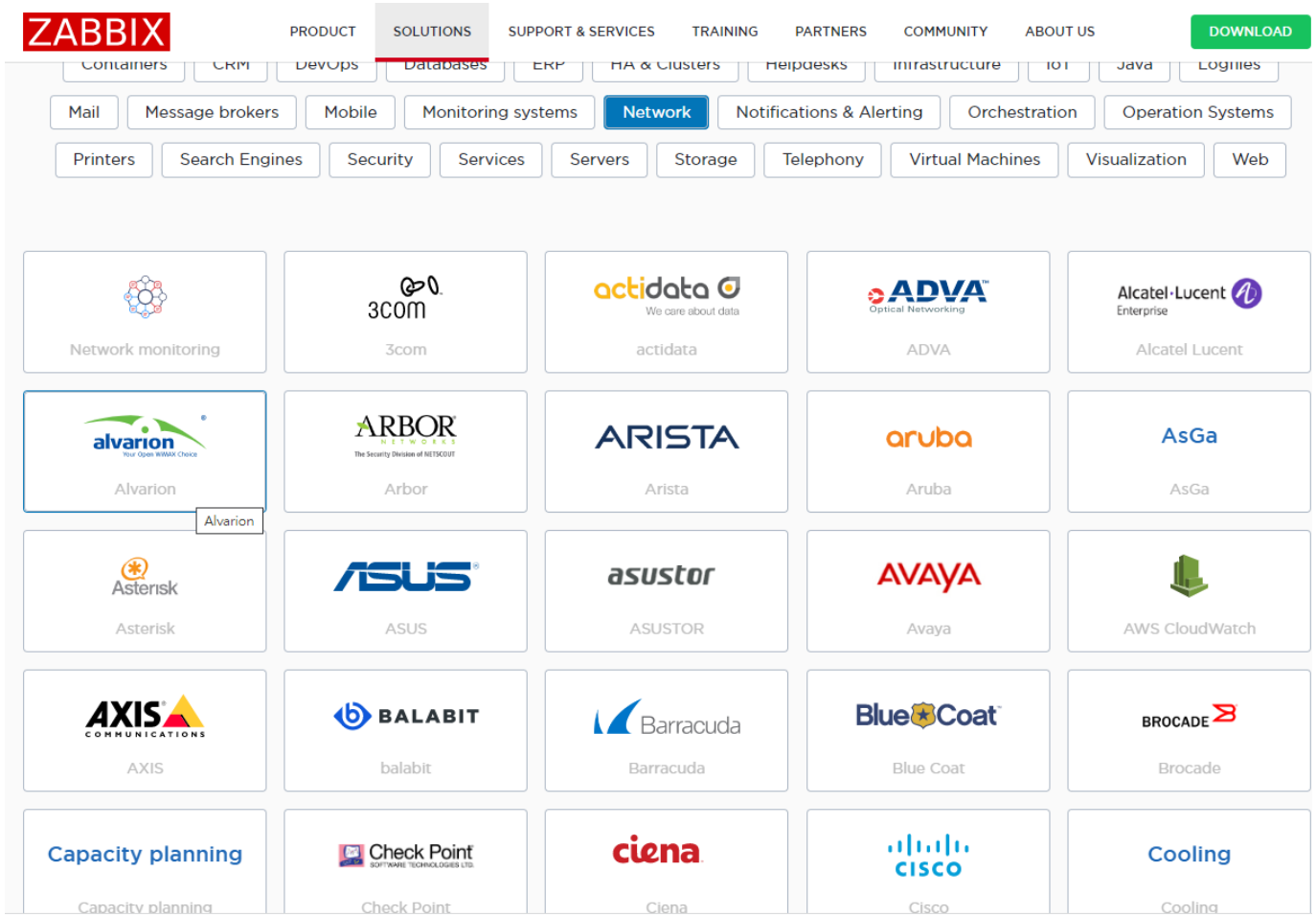
Life is not just about work



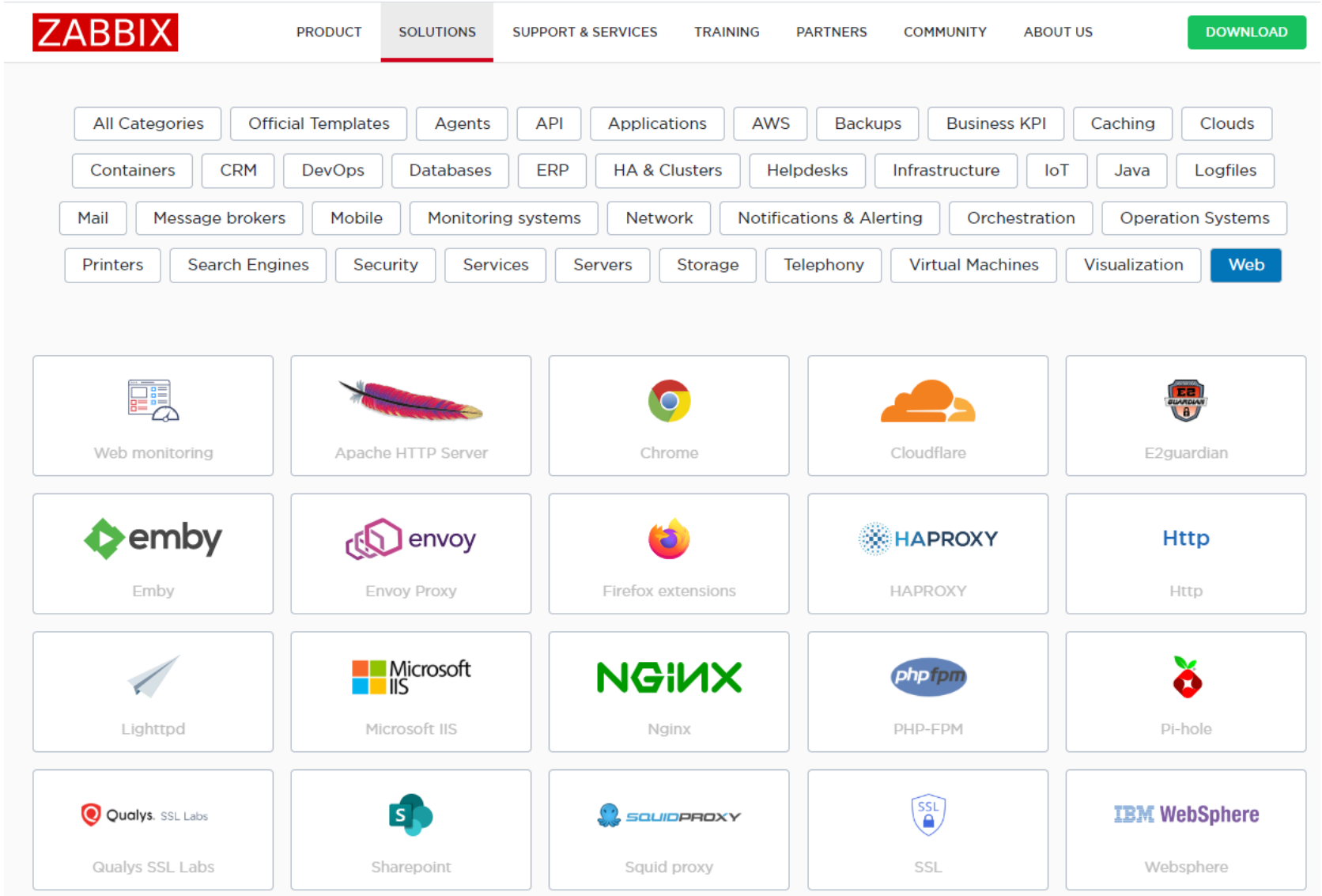
1. d-d,hh:mm-hh:mm
2. 1-5,09:00-17:00

思考四
只能監控硬體設備?

只能監測硬體設備嗎? 軟體系統及應用程式可以監測嗎?



網站監測(1)


ZABBIX
PRODUCT
SOLUTIONS
SUPPORT & SERVICES
TRAINING
PARTNERS
COMMUNITY
ABOUT US
DOWNLOAD
All Categories
Official Templates
Agents
API
Applications
AWS
Backups
Business KPI
Caching
Clouds
Containers
CRM
DevOps
Databases
ERP
HA & Clusters
Helpdesks
Infrastructure
IoT
Java
Logfiles
Mail
Message brokers
Mobile
Monitoring systems
Network
Notifications & Alerting
Orchestration
Operation Systems
Printers
Search Engines
Security
Services
Servers
Storage
Telephony
Virtual Machines
Visualization
Web
Web monitoring
Apache HTTP Server
Chrome
Cloudflare
E2guardian
Emby
Envoy Proxy
Firefox extensions
HAPROXY
Http
Lighttpd
Microsoft IIS
Nginx
PHP-FPM
Pi-hole
Qualys SSL Labs
Sharepoint
Squid proxy
SSL
Websphere

網站監測(2)

Triggers

Name	Description	Expression	Severity	Dependencies and additional info
Apache: Service is down	-	`last(/Apache by Zabbix agent/net.tcp.service[http,"{$APACHE.STATUS.HOST}","{$APACHE.STATUS.PORT}"])=0`	AVERAGE	Manual close: YES **Depends on:** - Apache: Process is not running
Apache: Service response time is too high	-	`min(/Apache by Zabbix agent/net.tcp.service.perf[http,"{$APACHE.STATUS.HOST}","{$APACHE.STATUS.PORT}"],5m)>{$APACHE.RESPONSE_TIME.MAX.WARN}`	WARNING	Manual close: YES **Depends on:** - Apache: Process is not running - Apache: Service is down
Apache: has been restarted	Uptime is less than 10 minutes.	`last(/Apache by Zabbix agent/apache.uptime)<10m`	INFO	Manual close: YES
Apache: Version has changed	Apache version has changed. Ack to close.	`last(/Apache by Zabbix agent/apache.version,#1)<>last(/Apache by Zabbix agent/apache.version,#2) and length(last(/Apache by Zabbix agent/apache.version))>0`	INFO	Manual close: YES
Apache: Process is not running	-	`last(/Apache by Zabbix agent/proc.num["{$APACHE.PROCESS_NAME}"])=0`	HIGH	

網站被駭?

https://udn.com/news/story/6928/6519901

如何判斷網站被駭?

1. 網站檔案修改時間被異動?
2. 網站檔案大小不同?
3. 網站檔案內容變動?
4. 如何判斷是正常使用者更新網頁?還是駭客?

結論

- 網路設備監測系統隨時監測核心路由器、交換器、機房溫溼度監測、實體及虛擬伺服器、應用系統的服務。
- 充分掌握網路及重要系統設備的妥善率，提供網管人員即時的警示訊息，得以迅速排除問題。
- 透過系統自動監測，可以及早發現可能有潛在的問題點。

Q&A