

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



台灣之星
3分鐘 · 公開

稍早因為台電設備故障影響
造成了部分區域用戶網路暫時無法使用
目前我們的工程大可在全力搶修中
現在已經陸續恢復通訊..... 顯示更多

T STAR
台灣之星

緊急公告

稍早因台電設備故障影響
造成部份區域用戶
網路暫時無法使用
工程單位目前正全力搶修中

<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
汽車 時尚 體育 3C 評論 玩咖 食譜 地產 專區 TAIPEI TIMES 求職

NEW

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



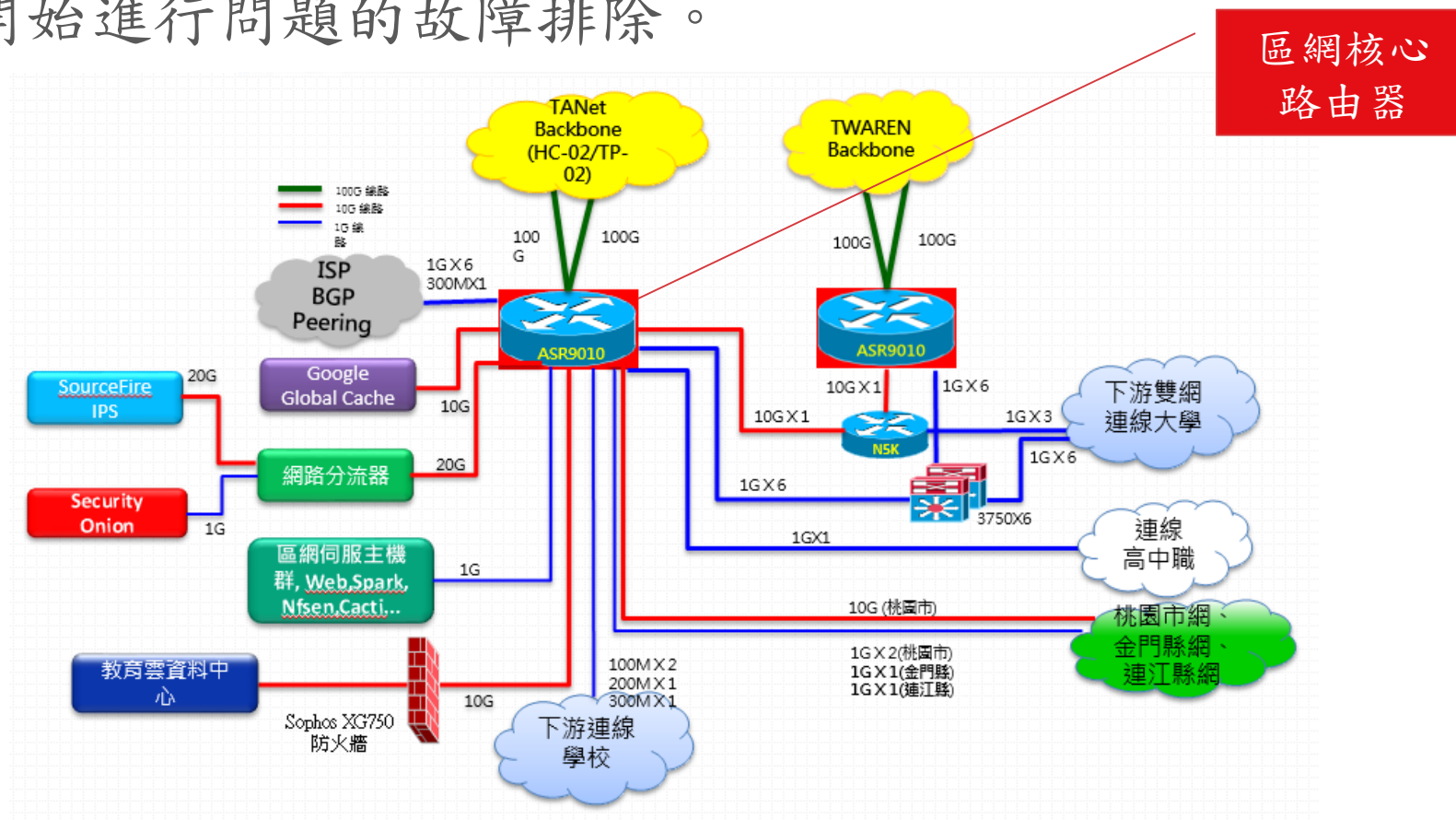
2013/04/02 19:57

〔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



Nagios[®]



 **PAESSLER**

ManageEngine 

 ScienceLogic

 LogicMonitor

solarwinds 

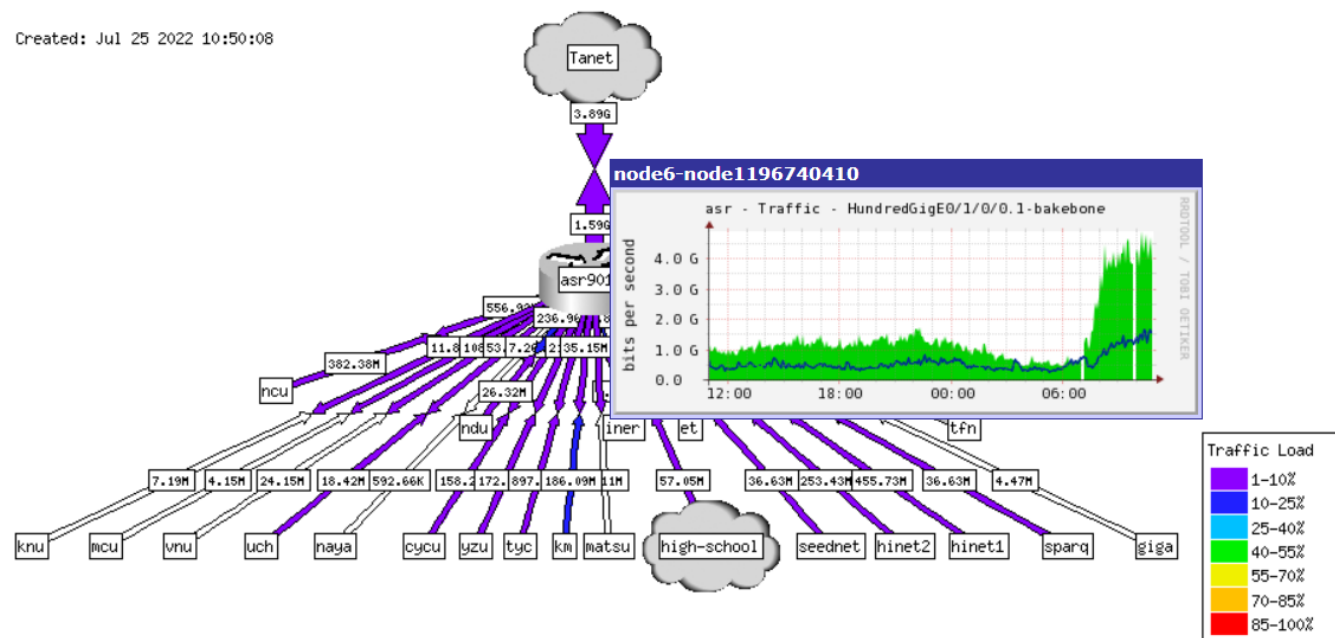
ZABBIX

 **Otter**

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

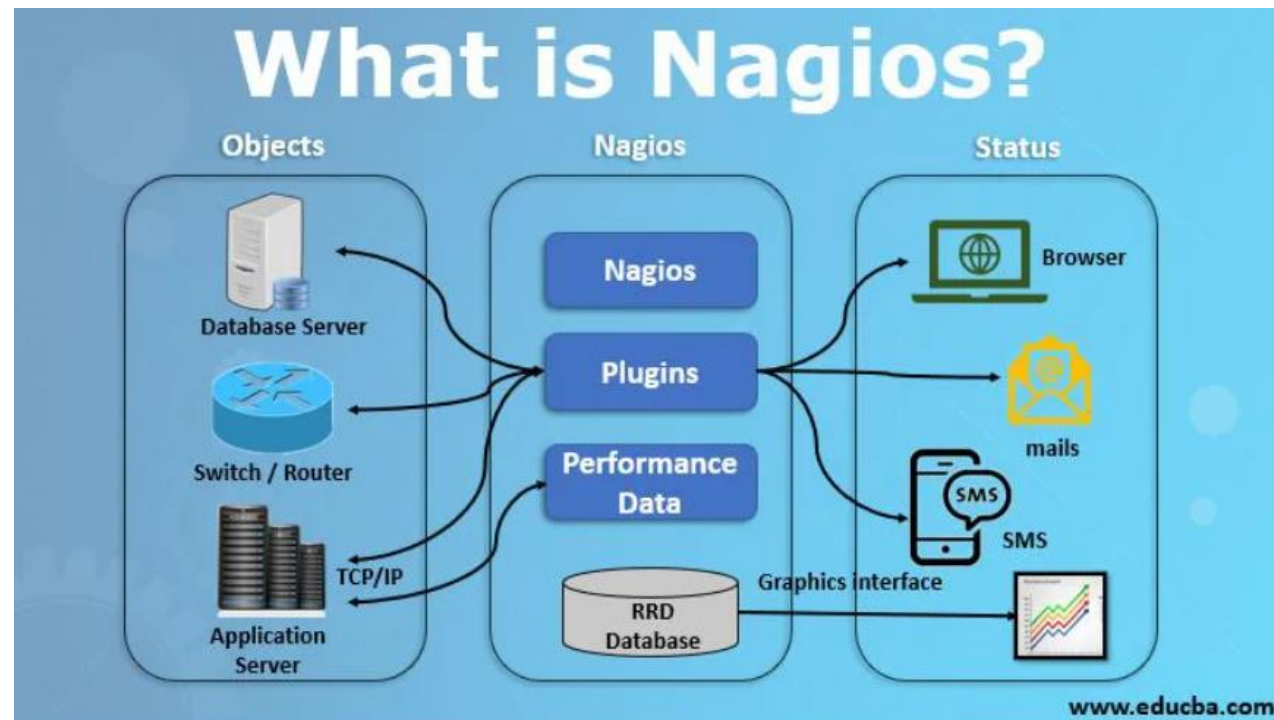
Cacti系統

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

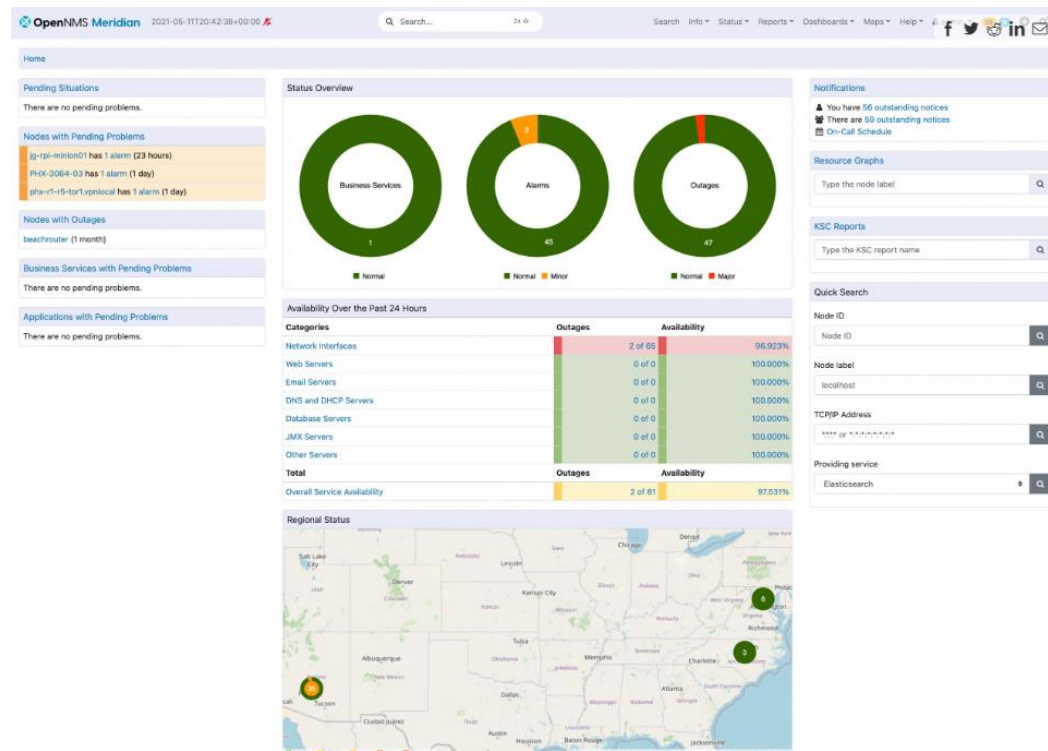
1. 非常受歡迎的監測系統，能監測大部分的協定及網路設備，及安裝NPRE Agent 程式。
2. 缺點是缺乏友善的介面



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

OpenNMS系統

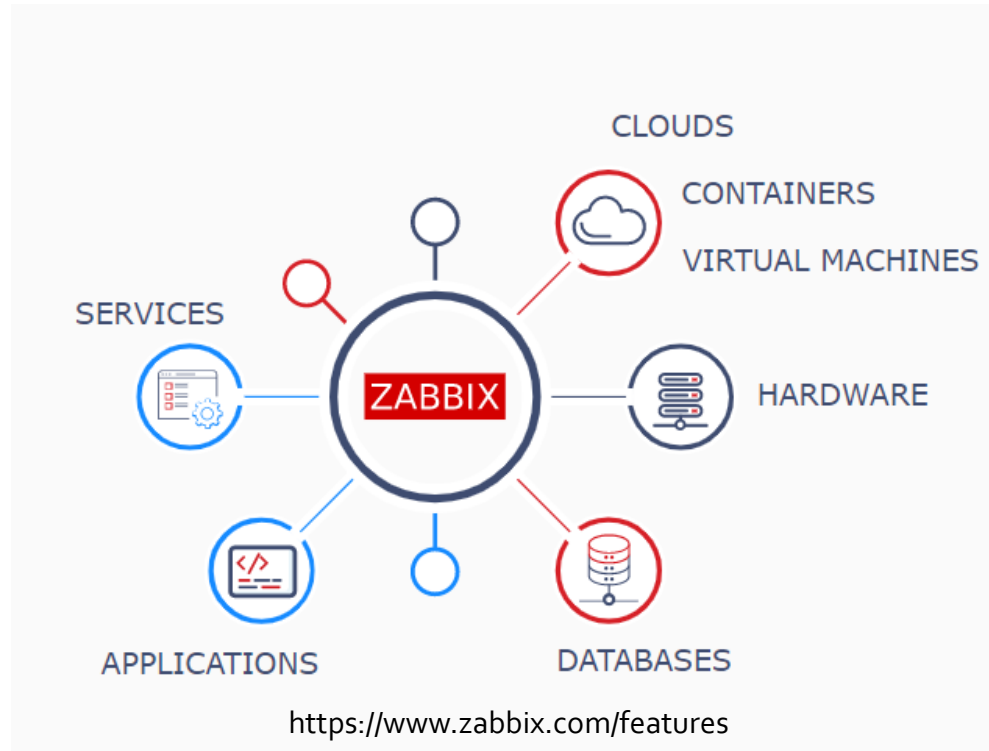
1. OpenNMS 可使用多樣的資料蒐集方式如 JMX、WMI、SNMP、NRPE、XML、HTTP、JDBC、XML、JSON 等。
2. 事件導向架構，支援 Grafana，有很好的使用者介面和美觀的儀表板和報表。



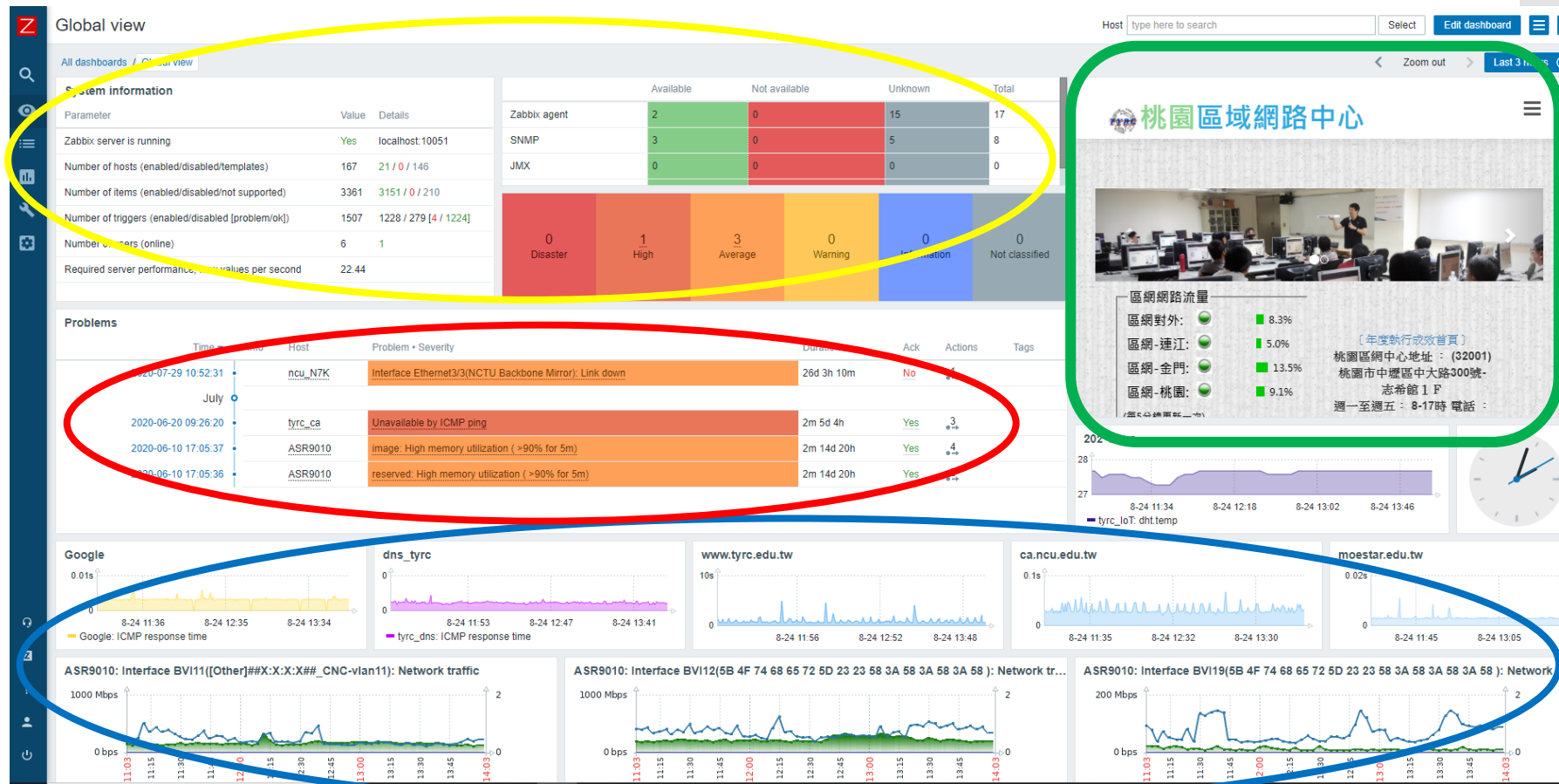
<https://www.opennms.com/>

Zabbix 監測系統

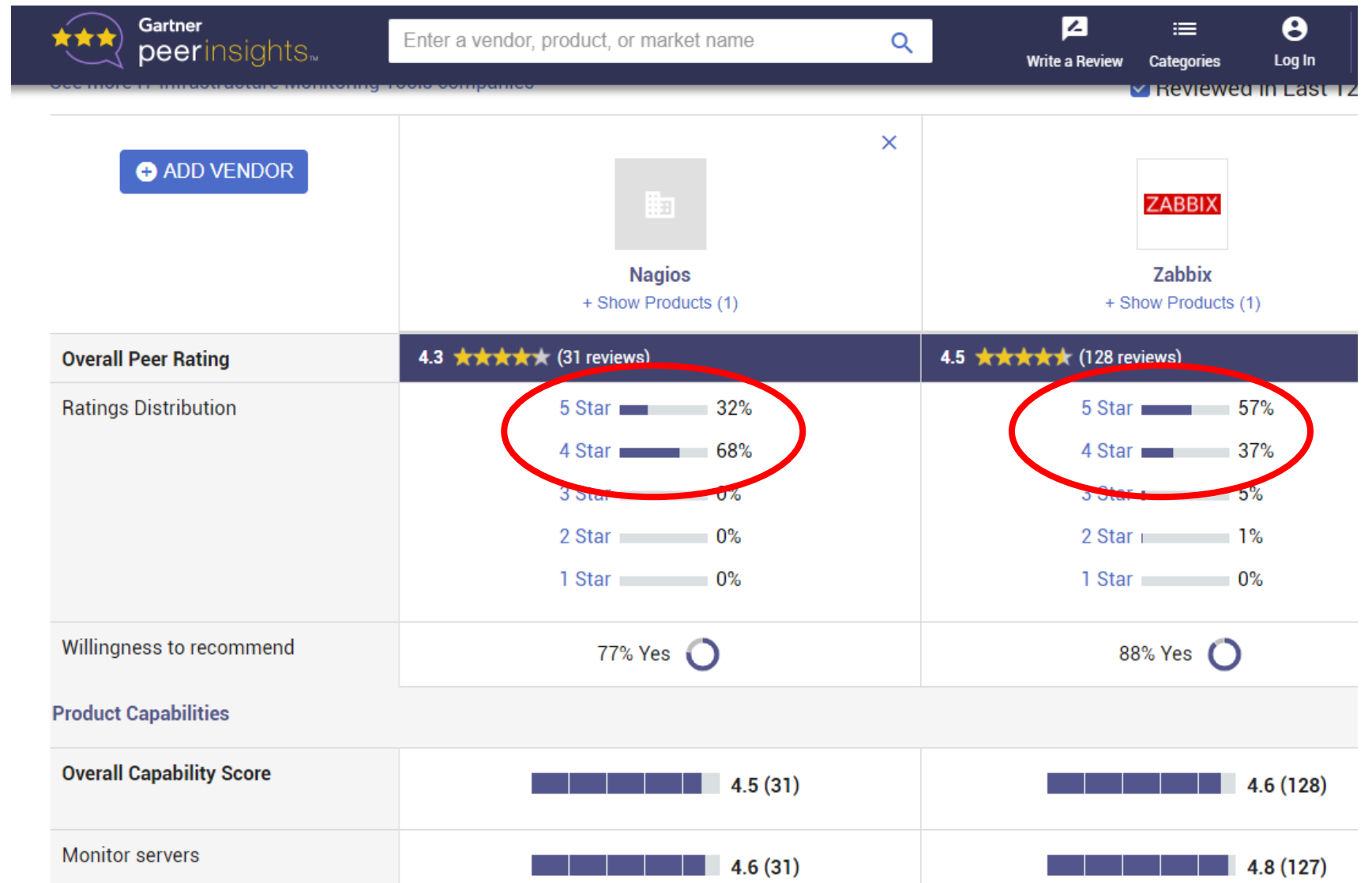
1. 系統可以監測硬體、資料庫、應用程式與服務、雲端系統。
2. 主要使用SNMP、IPMI、ICMP以及Zabbix Agent程式監測。



Zabbix 監測系統



Nagios vs Zabbix



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

Zabbix系統 安裝(1)

Home / Product /

Download and install Zabbix

Zabbix
Packages

Zabbix
Cloud
Images

Zabbix
Containers

Zabbix
Appliance

Zabbix
Sources

Zabbix
Agents

1

Choose your platform

ZABBIX VERSION	OS DISTRIBUTION	OS VERSION	DATABASE ²	WEB SERVER
6.2	Alma Linux	9 Stream	MySQL	Apache
6.0 LTS	CentOS	8 Stream	PostgreSQL	NGINX
5.0 LTS	Debian	7		
4.0 LTS	Oracle Linux	6		

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](#)

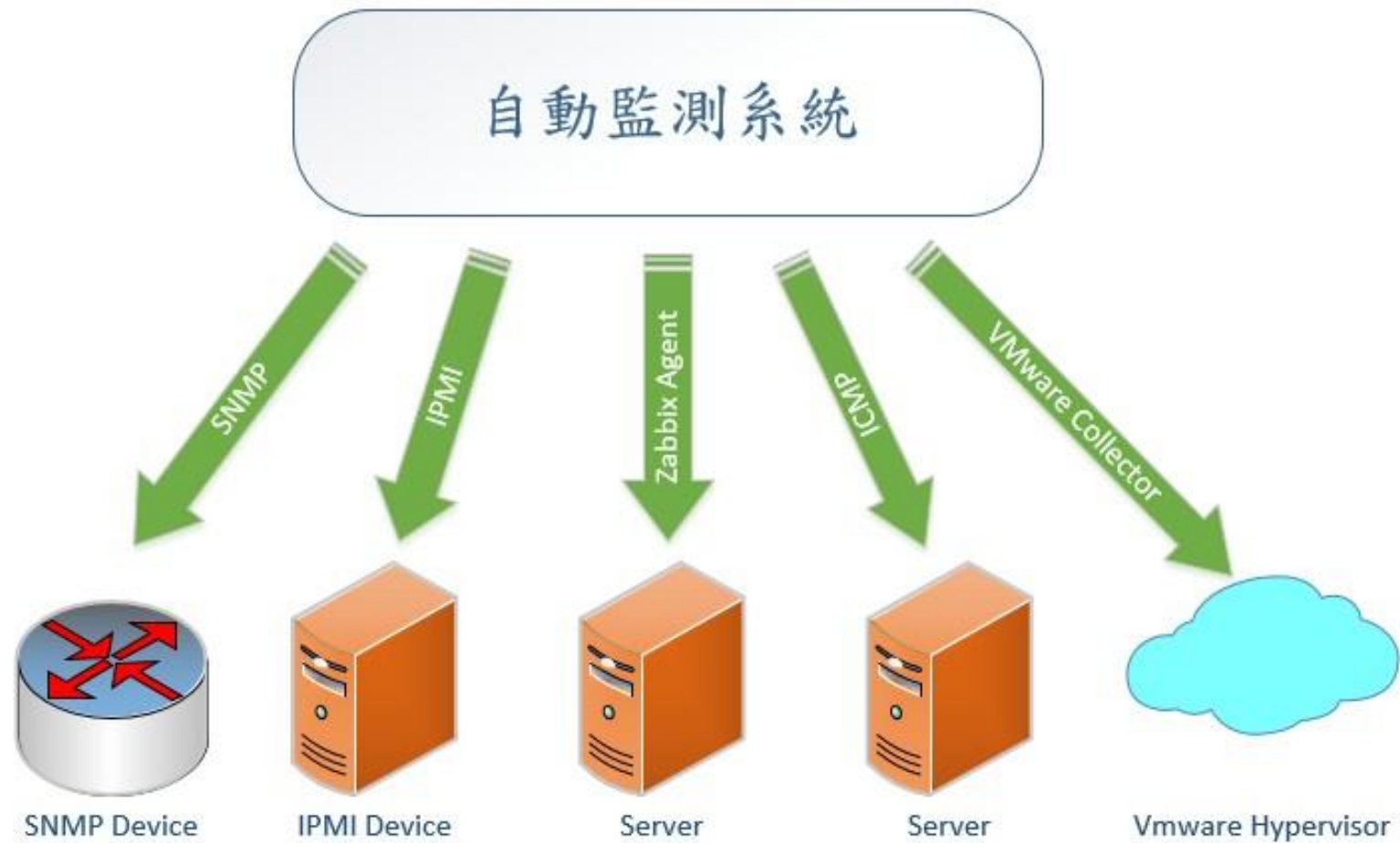
Make sure you have database server up and running.

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;
```

Zabbix系統 安裝(2)

自動化監測機制



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

The screenshot displays the iDRAC Enterprise web interface. The top navigation bar includes '仪表板', '系统', '存储', '配置', '维护', and 'iDRAC 设置'. The main heading is 'iDRAC 设置', with sub-tabs for '概览', '连接性', '服务', '用户', '设置', and 'CMC'. Under the '网络' section, there are links for '网络设置', '通用设置', '自动配置', 'IPv4 设置', and 'IPv6 设置'. The 'IPMI 设置' section is expanded, showing three configuration items: '启用 LAN 上的 IPMI' (set to '已启用'), '信道权限级别限制' (set to '管理员'), and '加密密钥*' (set to '000000000'). An '应用' button is located at the bottom right of the settings panel.

以IPMI 監測 (2)

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

The screenshot shows the Zabbix 'Hosts' configuration page for a host named 'tyrc_Dell_blade7'. The host is enabled and has the IPMI monitoring type selected. The configuration includes:

- Host name: tyrc_Dell_blade7
- Visible name: (empty)
- Groups: TYRC_Server
- Interfaces table:

* Interfaces	Type	IP address	DNS name	Connect to	Port
IPMI		172.20		IP	DNS 623

- Step 2: 連結範本

The screenshot shows the 'Templates' tab in the Zabbix 'Hosts' configuration page. It displays the following information:

- Linked templates: Template IPMI Dell PowerEdge M610
- Link new templates: (empty search box)
- Buttons: Update, Clone, Full clone, Delete

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。

ZABBIX

PRODUCT

SOLUTIONS

SUPPORT & SERVICES

TRAINING

PARTNERS

COMMUNITY

ABOUT US



Dell hardware

Dell is computer technology company that develops, sells, repairs, and supports computers and related products and

Available solutions

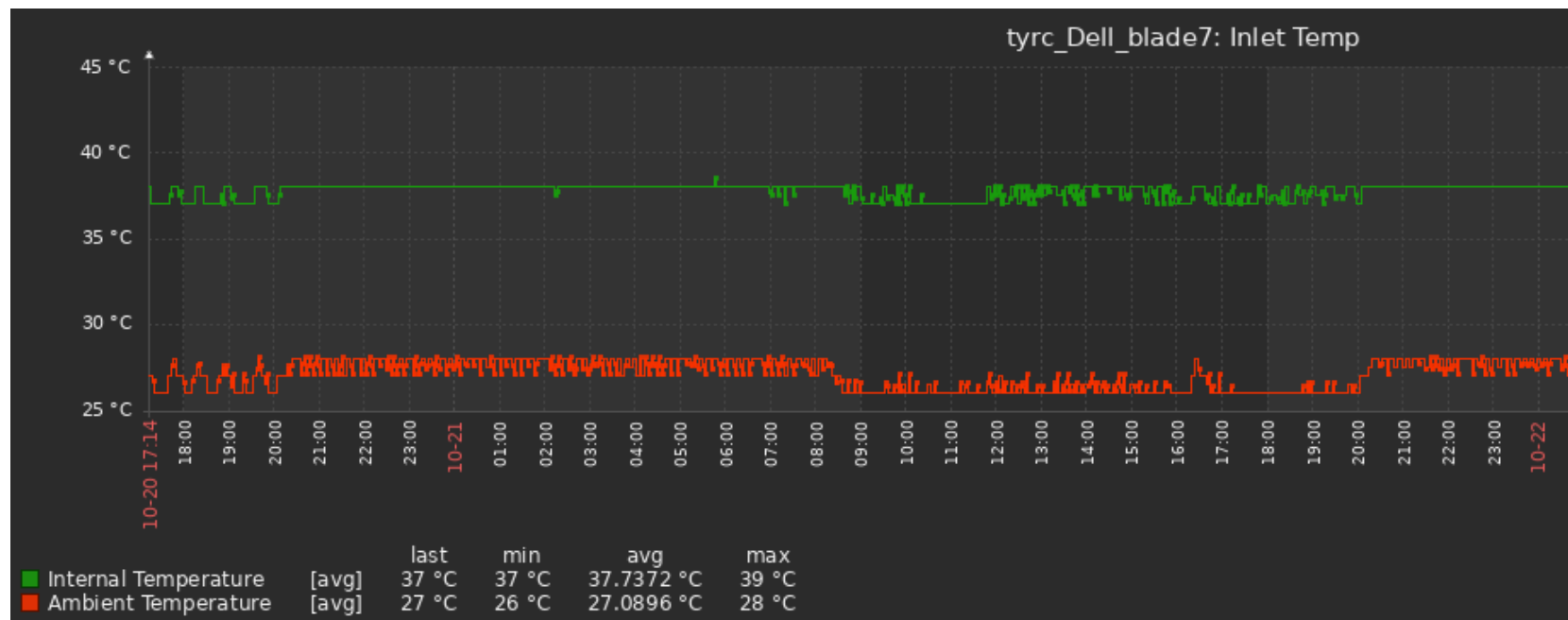
Official Templates

3rd Party Solutions

DELL PowerEdge R700:	DELL PowerEdge R720 by HTTP	DELL PowerEdge R740 by HTTP	DELL PowerEdge R740 SNMP
DELL PowerEdge R800:	DELL PowerEdge R820 by HTTP DELL PowerEdge R840 SNMP	DELL PowerEdge R820 SNMP	DELL PowerEdge R840 by HTTP
General template:	DELL PowerEdge R720 SNMP		

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

The screenshot shows the Zabbix Host configuration page for host ASR9010. The 'Host' tab is selected. The configuration includes:

- Host name: ASR9010
- Visible name: (empty)
- Groups: TYRC_Network, tyr_read_group
- Interfaces table:

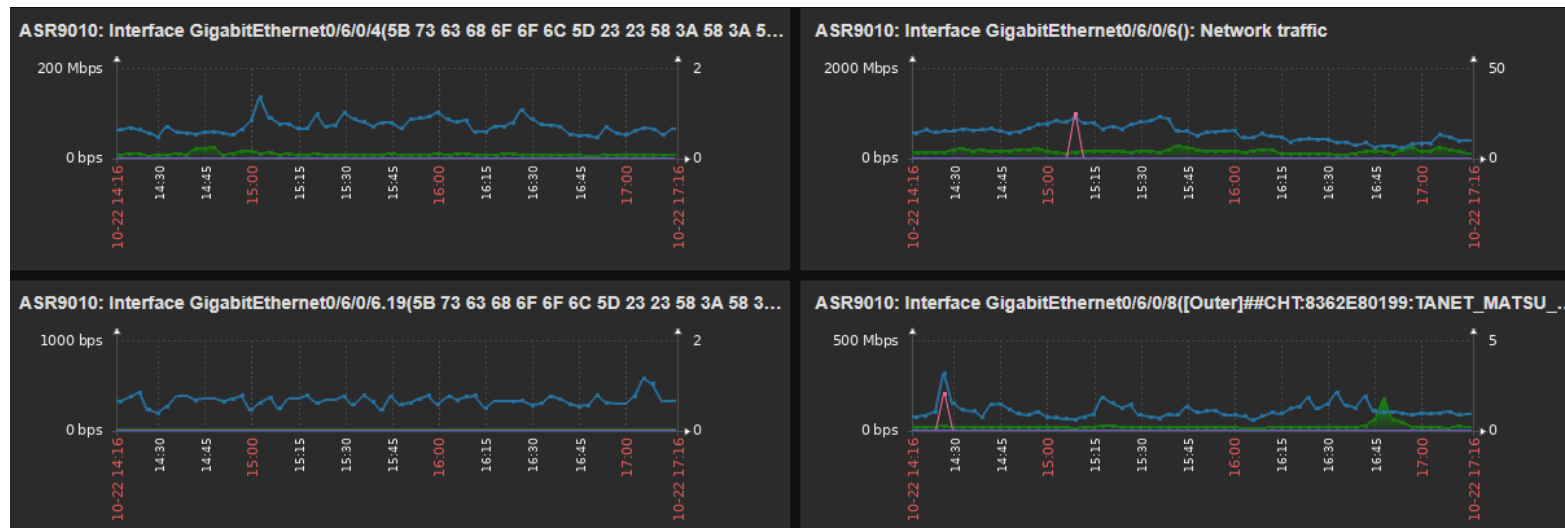
Interfaces	Type	IP address	DNS name	Connect to	Port
SNMP		192.192		IP	161
- SNMP version: SNMPv2
- SNMP community: {\$SNMP_COMMUNITY}
- Use bulk requests:

- Step 2: 連結範本

The screenshot shows the 'Linked templates' section of the Zabbix Host configuration page for host ASR9010. The 'Templates' tab is selected. The table below shows the linked template:

Linked templates	Name	Action
	Template Net Cisco IOS SNMPv2	Unlink U

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)

<input type="checkbox"/> Name ▲	Applications	Items	Triggers	Graphs
<input type="checkbox"/> ASR9010	Applications 169	Items 1572	Triggers 760	Graphs 163

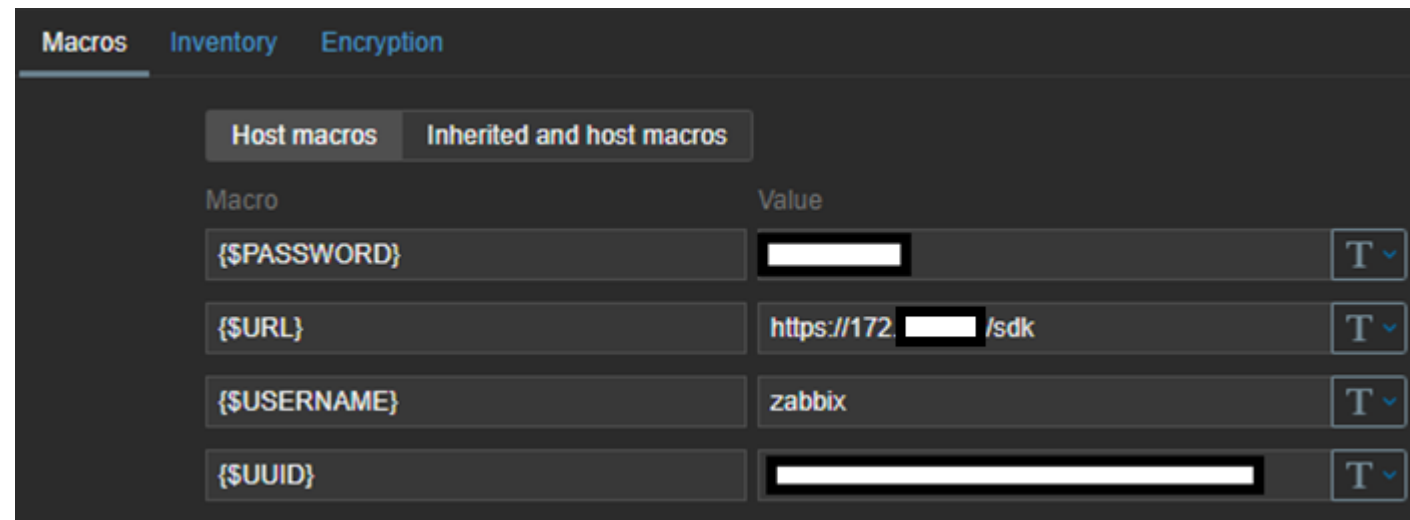
- 系統使用Discovery rules自動找出區網核心路由器169個系統狀態及網路介面
- 合計1572個監測項目以及760個觸發條件。
- 每個網路介面有以下4種觸發條件
 - 介面關閉
 - 高使用率
 - 高錯誤率
 - 介面速率變化

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

Discovery rule Preprocessing LLD macros Filters Overrides

Parent discovery rules Template VM VMware

* Name

Type

* Key

* Host interface

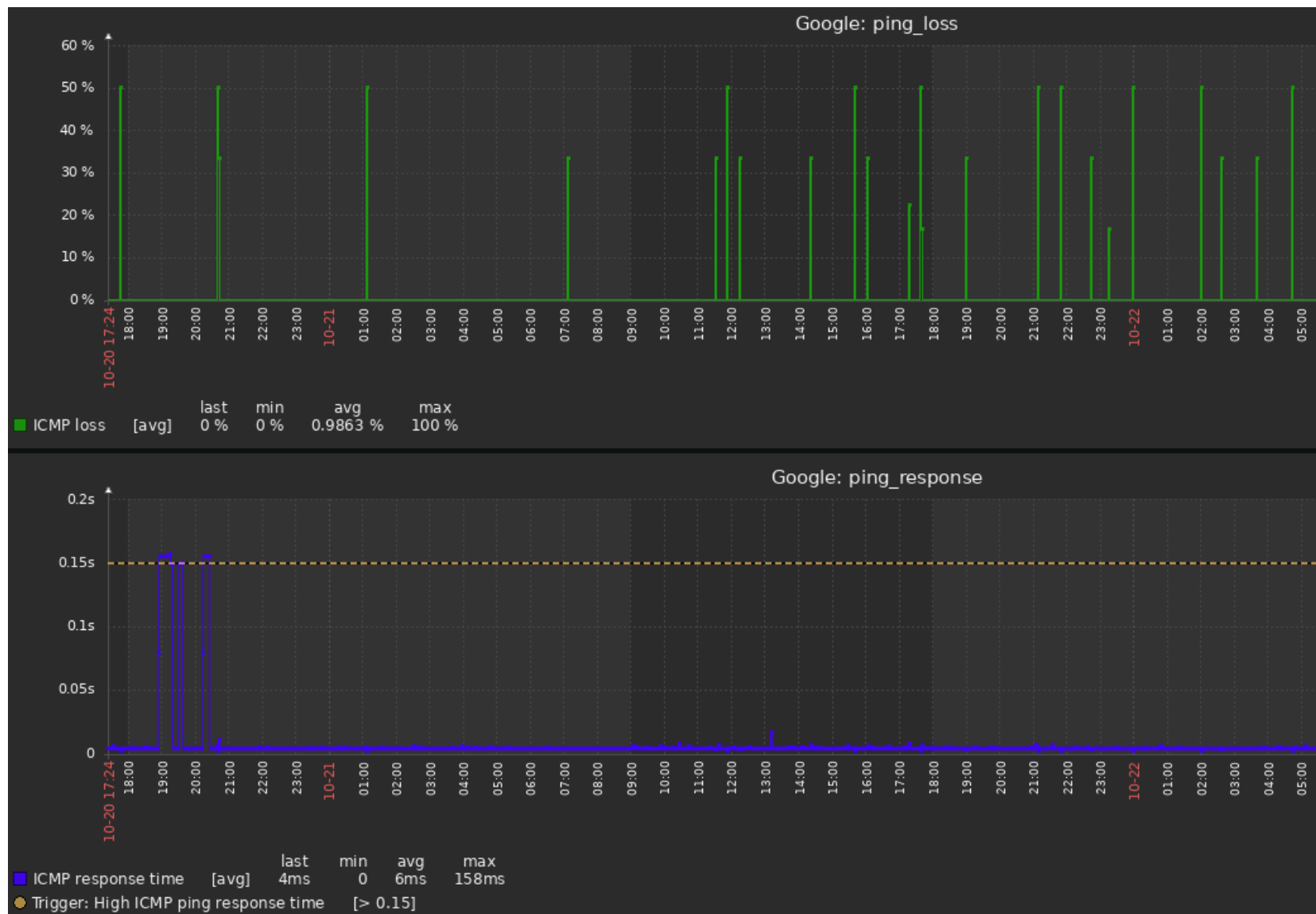
User name

Password

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)



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

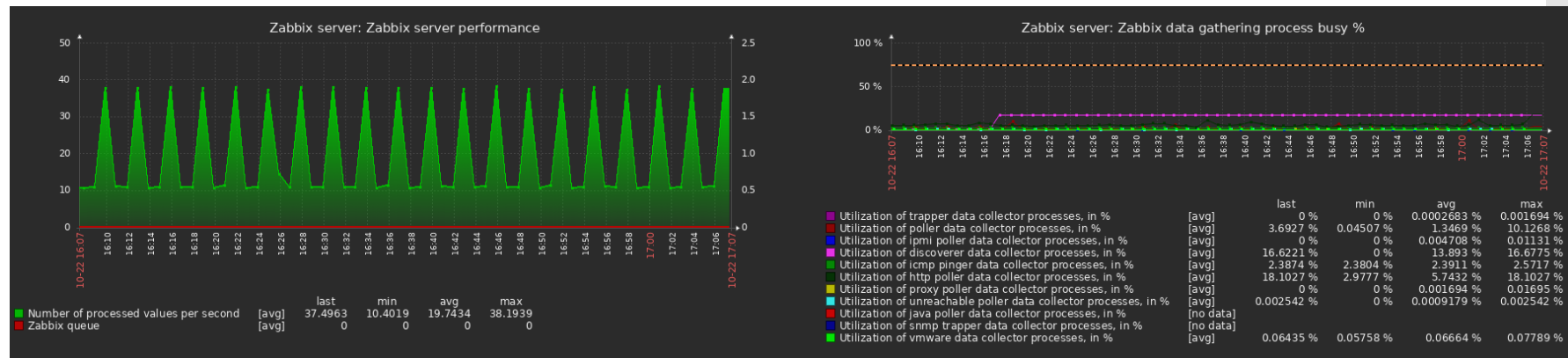
OS DISTRIBUTION	OS VERSION	HARDWARE	ZABBIX VERSION	ENCRYPTION	PACKAGING
Windows	Any	amd64	6.2	OpenSSL	MSI
Linux		i386	6.0 LTS	No encryption	Archive
macOS			5.4		
AIX			5.2		
FreeBSD			5.0 LTS		
OpenBSD			4.4		
Solaris			4.2		

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

Linked templates	Name	Action
	Template OS Linux by Zabbix agent	Unlink Unlink and clear

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/>

Templates

Applications

1C

1C Enterprise

Anti-Virus

App Kaspersky

Kaspersky Security Center 11

Backup

Nakivo

App BackupPC by Zabbix agent

Backup Exec Server

VEEAM-Agents

App TSM Client Scheduler

Asigra Backup SNMP Traps

App TSM Journal Service

SAP Backup

restic backup by Zabbix agent

VEEAM SMTP trapper

Arcserve UDP VM Backup Check

Cluster

CoroSync-Ring-0

ILOM ORACLE SRV X8-2 SNMP Trap

Clustered_File_Systems

Gluster Storage

DNS

pihole-FTL over zabbix active agent

Knot Resolver Statistics

App PowerDNS dnsmist

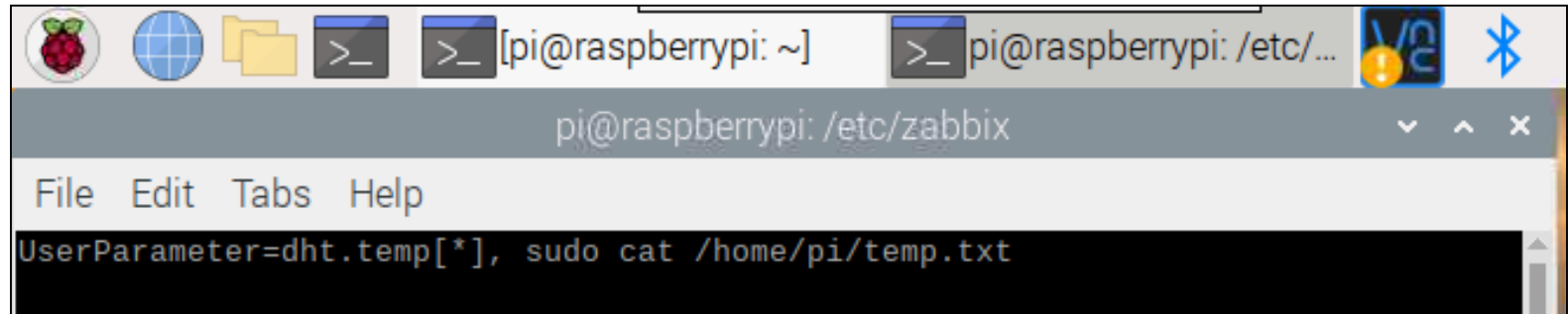
net.dns.perf

Bind queries

DNS-bind

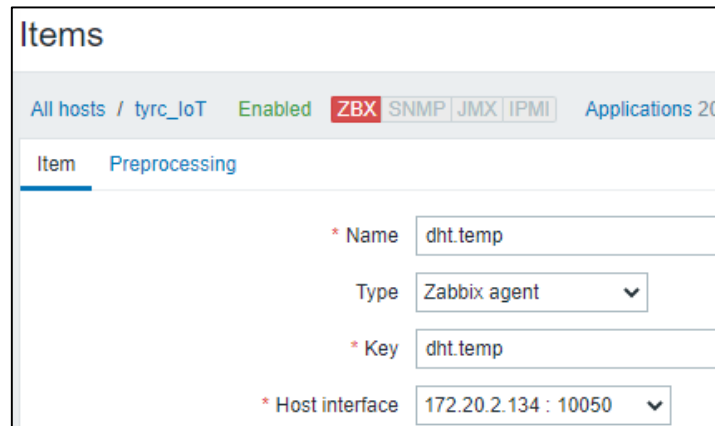
解決方案(2) 自己打造

- 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。



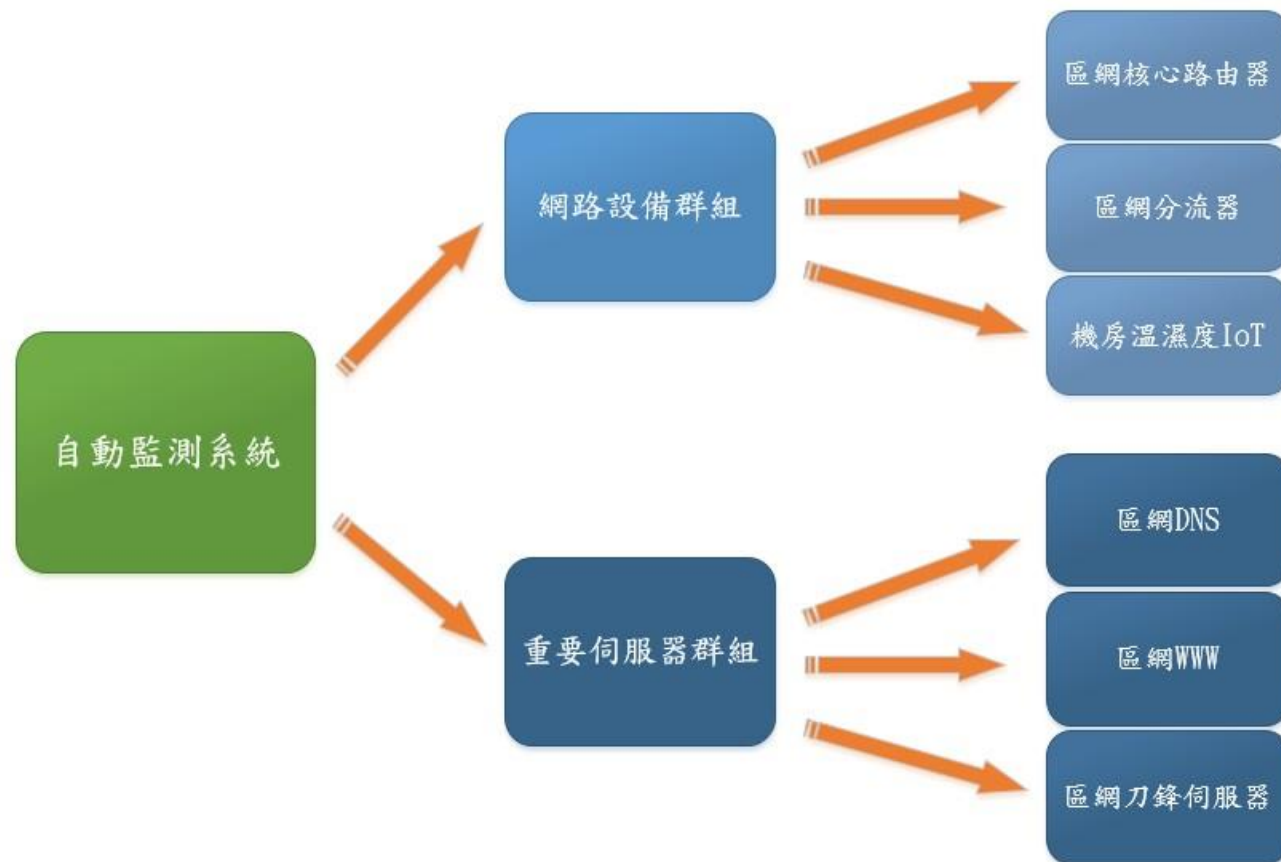
```
pi@raspberrypi: /etc/zabbix
File Edit Tabs Help
UserParameter=dht.temp[*], sudo cat /home/pi/temp.txt
```

- 在Zabbix加上使用者定義的監測Items



Items	
All hosts / tyrc_IoT Enabled ZBX SNMP JMX IPMI Applications 20	
Item	Preprocessing
* Name	dht.temp
Type	Zabbix agent
* Key	dht.temp
* Host interface	172.20.2.134 : 10050

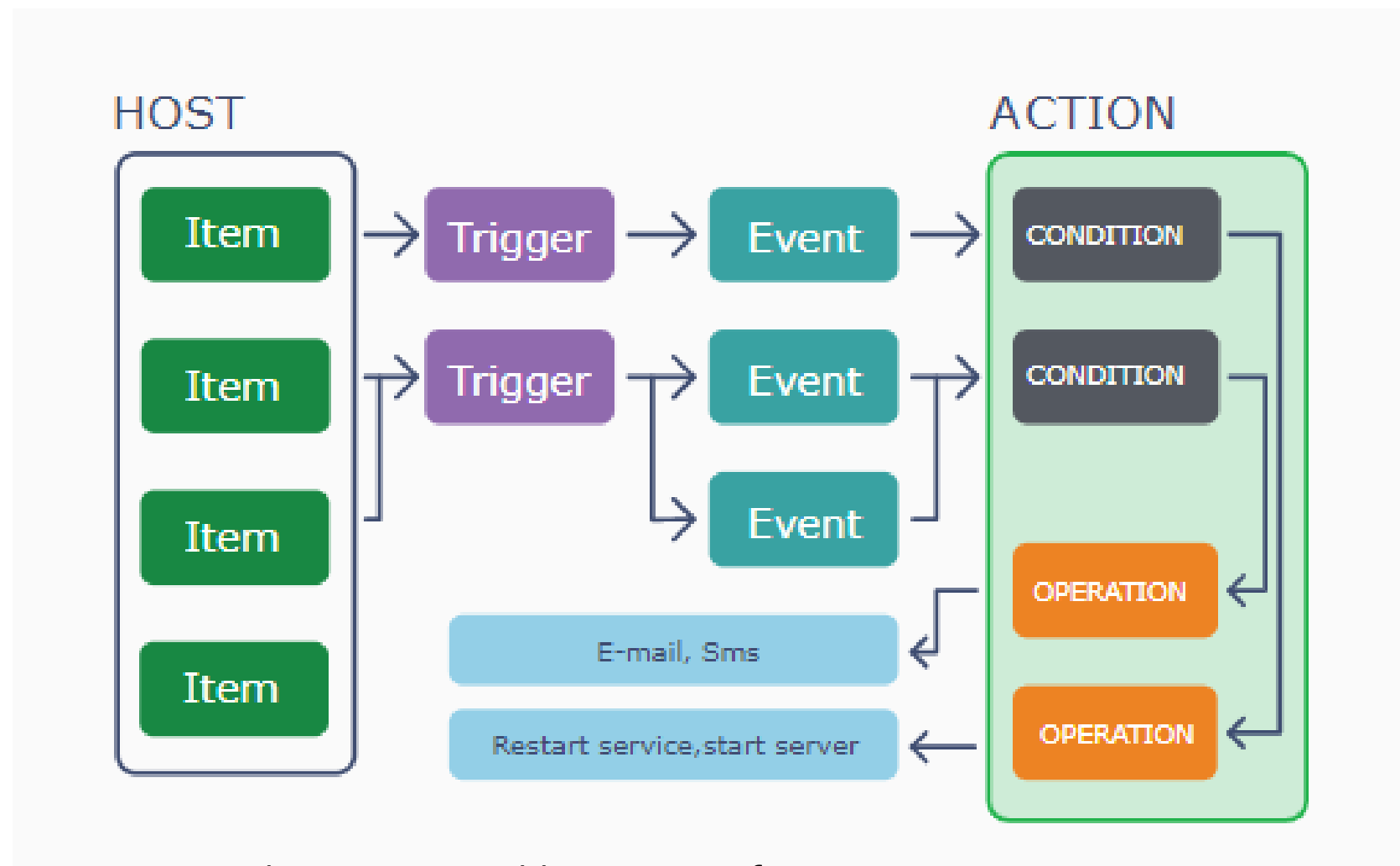
系統部署架構



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Triggers 會產生事件，並依照設定自動通知。

Operation details

Operation type

Steps - (0 - infinitely)

Step duration (0 - use action default)

* At least one user or user group must be selected.

Send to User groups

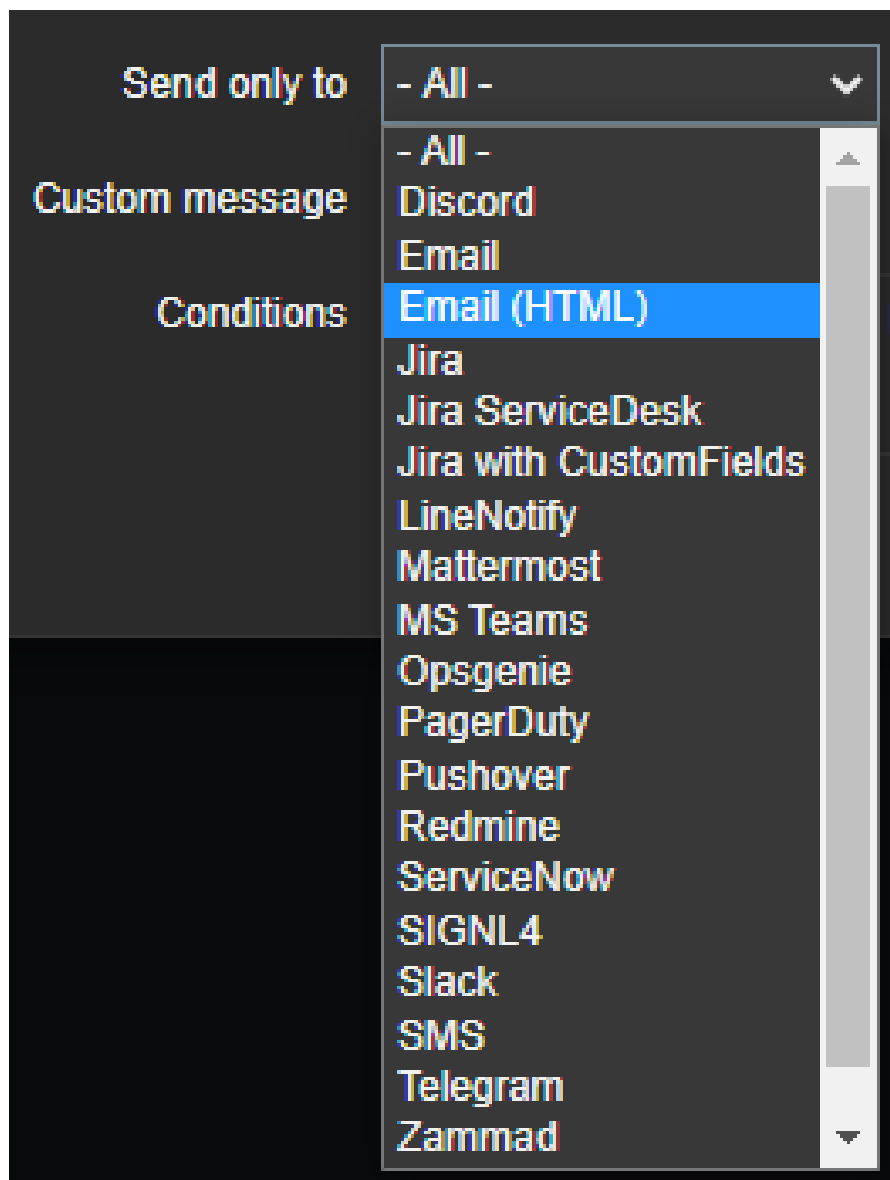
User group	Action
Add	

Send to Users

User	Action
km_user	Remove
Add	

Send only to

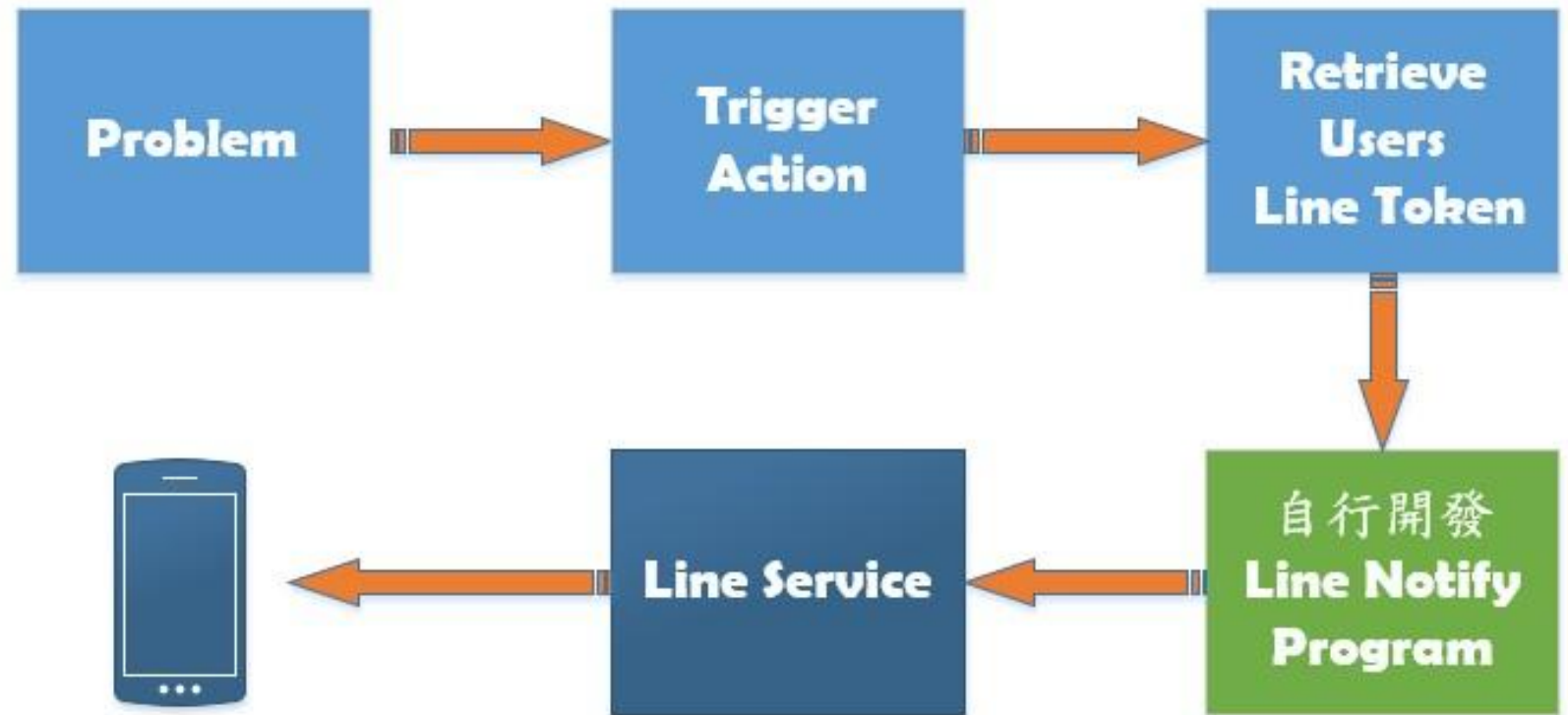
事件自動化告警機制(3)



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。

Media types

Media type Message templates Options

* Name

Type

* Script name

Script parameters

Parameter	Action
<input data-bbox="1302 1001 2204 1043" type="text" value="{ALERT.SENDTO}"/>	Remove
<input data-bbox="1302 1072 2204 1115" type="text" value="{ALERT.SUBJECT}"/>	Remove
<input data-bbox="1302 1143 2204 1186" type="text" value="{ALERT.MESSAGE}"/>	Remove

[Add](#)

即時告警案例 (1) 連線中斷



LINE Notify

【tyrc_notify】 2020.08.23
23:55:13

* Host ==> ASR9010
Interface
GigabitEthernet0/7/0/10([
Other]##X:X.X.X##_hon
ey_pot) Link down

* Detail ==> Current
state: down (2)

* Original problem ID ==>
255159

下午 11:55

即時告警案例 (2) 網路壅塞



LINE Notify

【tyrc_notify】 2020.09.25
09:24:13

* Host ==> ASR9010

Interface

GigabitEthernet0/0/0/6():

High bandwidth usage (> 90%)

* Detail ==> In: 131.72
Mbps, out: 739.06 Mbps,
speed: 1 Gbps

* Original problem ID ==>
260464

上午 9:24

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

Media

Type

* Send to

* When active

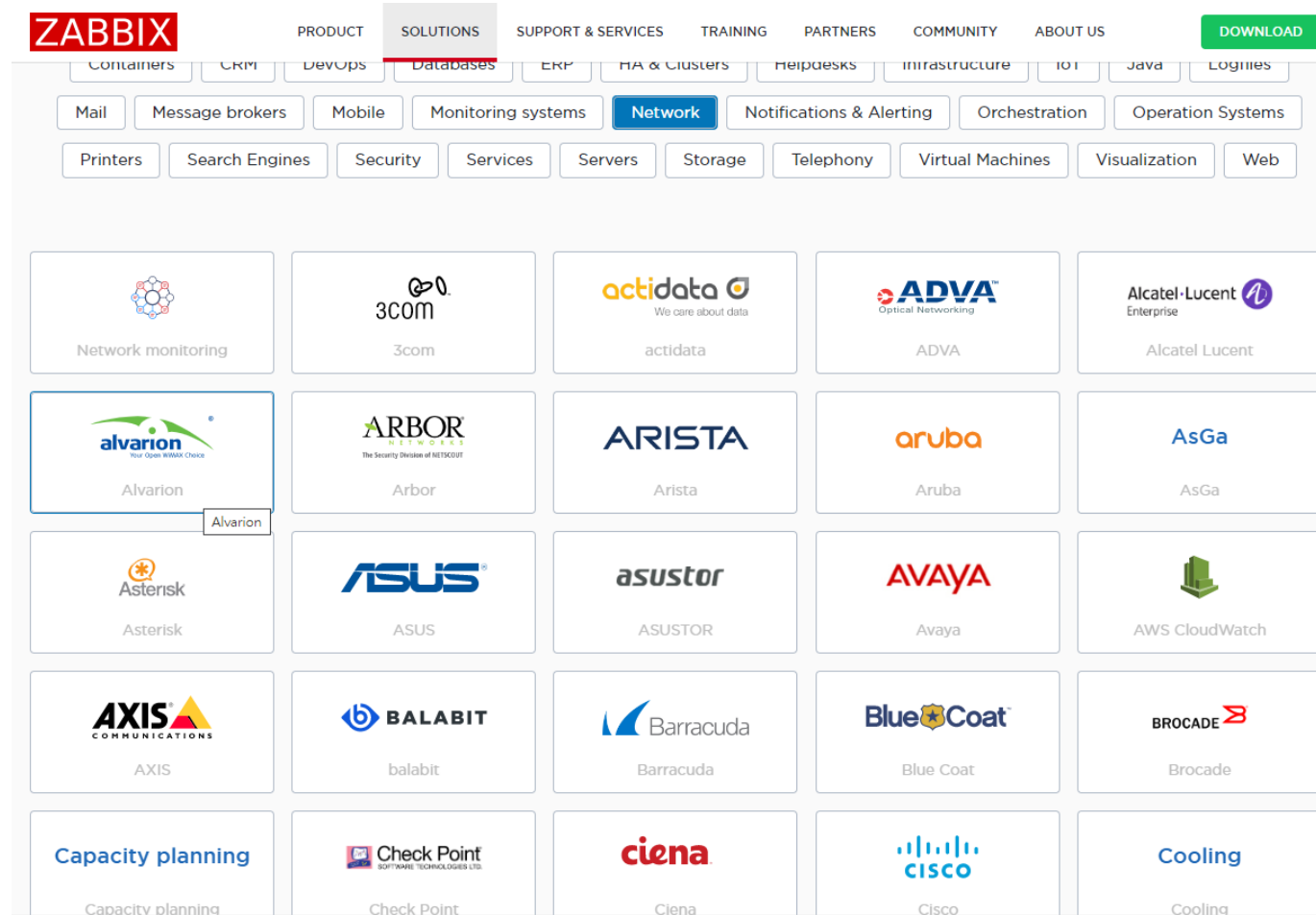
Use if severity Not classified
 Information
 Warning
 Average
 High
 Disaster

Enabled

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)

The screenshot displays the Zabbix website's 'SOLUTIONS' page. At the top, the Zabbix logo is on the left, and navigation links for 'PRODUCT', 'SOLUTIONS', 'SUPPORT & SERVICES', 'TRAINING', 'PARTNERS', 'COMMUNITY', and 'ABOUT US' are in the center. A green 'DOWNLOAD' button is on the right. Below the navigation is a grid of category buttons, with 'Web' highlighted in blue. The main content area features a 4x5 grid of solution cards, each with an icon and a title. The cards include: 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, and WebSphere.

Category	Solution
Web	Web monitoring
Web	Apache HTTP Server
Web	Chrome
Web	Cloudflare
Web	E2guardian
Web	Emby
Web	Envoy Proxy
Web	Firefox extensions
Web	HAPROXY
Web	Http
Web	Lighttpd
Web	Microsoft IIS
Web	Nginx
Web	PHP-FPM
Web	Pi-hole
Web	Qualys SSL Labs
Web	Sharepoint
Web	Squid proxy
Web	SSL
Web	WebSphere

Triggers

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

網站監測(2)

網站被駭?

聯合新聞網

即時 要聞 選舉 娛樂 運動 全球 社會 地方 產經 股市 房市 生活 健康 橘世代 **文教** 評論 兩岸 數位

快訊 >>> 羽球/BWF積分排名「解封」 小戴8月世錦賽後即將重返球后 12:04

udn / 文教 / 大學研究所

聽新聞 0:00 / 0:00

台大教務處網站被駭「只有一個中國」 校方：正在處理中

2022-08-07 22:26 中央社 / 台北7日電

+ 台灣大學



The screenshot shows a webpage with a red header featuring the slogan "世界上只有一個中國" (There is only one China in the world). Below the header, there are navigation links and a search bar. A prominent banner at the bottom of the page reads "偉哉台大資安" (Great is the security of NTU). The page also contains a list of university events and a footer with contact information.

<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

