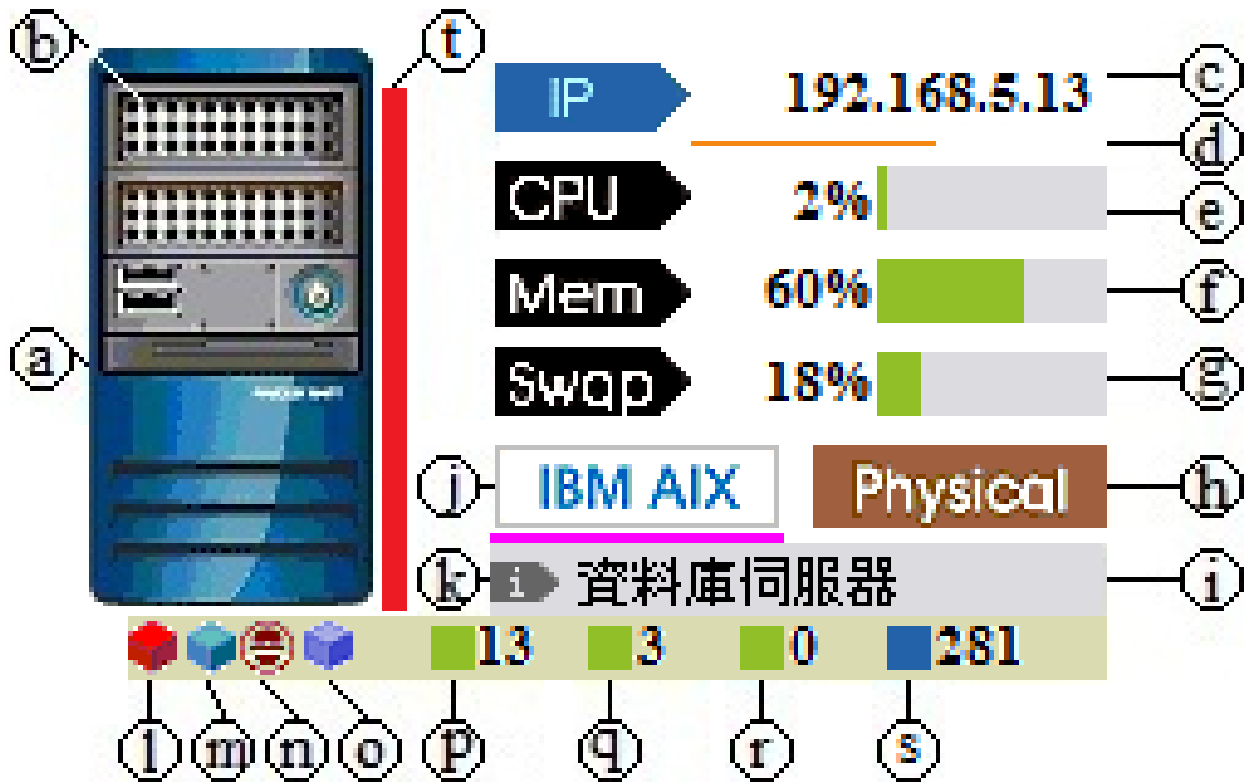


## Watchdog Rooty 伺服器即時資訊狀態圖



戰情中心個別伺服器圖

### ● 伺服主機依重要性區分：A>B>C 級主機

① 伺服主機的圖示：



A 級主機



B 級主機



C 級主機



虛擬主機

### ● 伺服主機的狀態

② 系統狀態的圖示：



正常



警報



暫停



維修



失去連線



重新開機

嚴重警報：

當伺服器的 filesystem, CPU, 實體記憶體, 虛擬記憶體使用比超過 97%以上時發出。



A 級主機



B 級主機



C 級主機



虛擬主機

已通報待處理之警報：

警報發生與通知系統管理員處理中。



A 級主機



B 級主機



C 級主機



虛擬主機

## ● 伺服器 IP 位置

© 伺服器 IP 位置的圖示：



顯示伺服器的 IP 位址

## ● 各項數據的負載量

① Switch 流量與連線狀態圖示：

無-若無色棒表示 Port 線路未連上 Switch 連接埠



藍-已找到本台主機的 Switch 連接埠



橘-本台主機的 Switch 連接埠流量介於 1%-79%(長度依流量比 1-79%)



紅-本台主機的 Switch 連接埠流量介於 80%-100%(長度依流量比 80-100%)

Ⓒ CPU 負載量的圖示：



色棒顯示以下顏色時



綠→正常, 未超出警報臨界值



黃→正常, 未超出警報臨界值, 但已超出 90%使用值



紅→異常, 超出警報臨界值

Ⓓ Memory 負載量的圖示：



色棒顯示以下顏色時



綠→正常, 未超出警報臨界值



黃→正常, 未超出警報臨界值, 但已超出 90%使用值



紅→異常, 超出警報臨界值

Ⓔ 虛擬記憶體負載量的圖示：



色棒顯示以下顏色時



綠→正常, 未超出警報臨界值



黃→正常, 未超出警報臨界值, 但已超出 90%使用值



紅→異常, 超出警報臨界值

## ● 伺服主機類型

Ⓘ 實體主機, 虛擬主機, 或無資料的圖示：



## ● 伺服主機名稱或別名

Ⓛ 伺服主機名稱或別名的圖示：







## ● 伺服器主機的作業系統

① 作業系統的圖示：









封包測試狀態圖示：

-  紅-封包測試結果超過警戒值
-  桃-封包測試結果有漏失(loss)但未設定警戒值, 長度會隨漏失百分比改變
-  綠-封包測試結果漏失(loss)的百分比為 0
-  灰-封包測試功能暫停, 或無法取得偵測值



## ● RAID 磁碟陣列

Ⓚ RAID 磁碟陣列的圖示：



-  灰 → 無或未建立磁碟陣列資訊
-  綠 → 已建立磁碟陣列監控
-  紫 → 已建立磁碟陣列命令, 但未取得資料
-  藍 → 已建立磁碟陣列命令, 已取得資料, 但未加入監控
-  黃 → 已搜尋到磁碟陣列資料, 但並未設定
-  黑/橘 → 標記本機無磁碟陣列

## ● 系統服務狀態的圖示



① 資料庫系統的圖示：

-  無資料庫(DB) 服務系統, 例如: MSsql, Mysql
-  有資料庫(DB) 服務系統, 例如: MSsql, Mysql

Ⓜ 郵件系統的圖示：

-  無郵件(Mail) 服務系統, 例如: MS Exchange, SmtP
-  有郵件(Mail) 服務系統, 例如: MS Exchange, SmtP

① 網站系統的圖示：

-  無網站(WEB) 服務系統, 例如: IIS, Apache
-  有網站(WEB) 服務系統, 例如: IIS, Apache

ⓐ 帳戶系統的圖示：

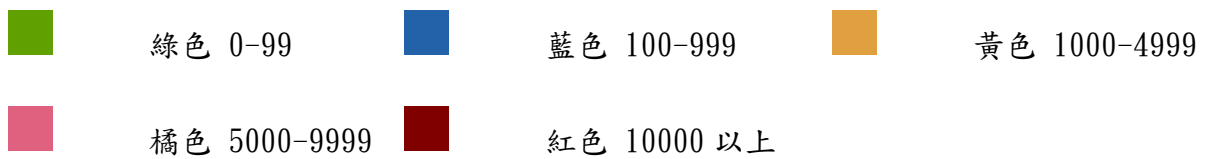
-  無 AD/DC 或 Ldap 的服務系統
-  有 AD/DC 或 Ldap 的服務系統

## ●TCP 連線狀態

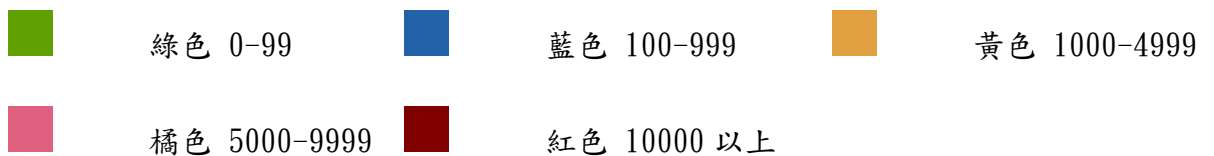
① TCP LISTEN 的數量:



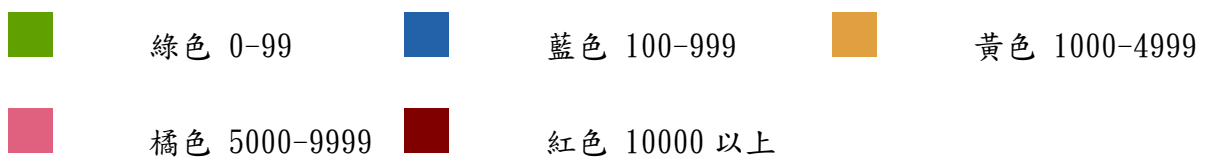
② TCP ESTABLISHED 進的數量:



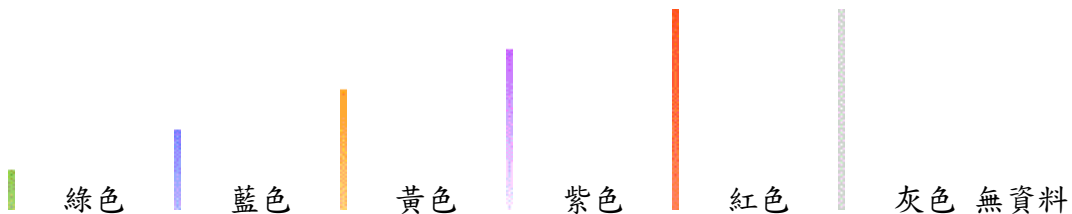
③ TCP ESTABLISHED 出的數量:



④ TCP TIME\_WAIT 等待斷線的數量:



⑤ 處理程序(process)的數量:



Linux/Unix 作業系統的處理程序數量:

綠色: 1~299

藍色: 300~999

黃色：1000~4999  
 紫色：5000~9999  
 紅色：10000~  
 灰色：沒有取得資料

Windows作業系統的處理程序數量：

綠色：1~99  
 藍色：100~299  
 黃色：300~499  
 紫色：500~999  
 紅色：1000~  
 灰色：沒有取得資料



監控項目圖

## 主機資訊：



提供即時的系統資訊，是對伺服器主機進行系統診療和效能判斷的依據，  
 仍需根據個別主機或處理程序數量判定。

這些資訊包括：主機資訊，作業系統，網路路由，網卡資訊，網路設定，

TCP/UDP/ARP 之網路狀態，處理程序數量，執行程式，工作排程等等。

#### 處理程序數量分析：

透過即時分析每一支正在運行程式的歷史紀錄，協助系統人員做初步的效能判斷和除錯(debug)。

#### 處理程序數量分析(圖表)：

將處理程序數量依類別分類並用圖形表示，便於分析比較和除錯。例如將處理程序數量分為非法執行程式，非法執行 DLL 程式，危險等級，非法 TCP-LISTEN 埠等等。

## 以上功能又分為硬體層，作業系統層，應用系統層

硬體層， 例如 IPMI, ILO, 磁碟陣列等

作業系統層(OS)，例如 CPU, Memory 等

應用系統層(AP)，例如執行程式，事件警報，事件數據等

## 監控項目警示顏色說明：



灰-無任何監控項目



綠-所有監控項目正常



藍-所有監控項目暫停



橘-監控項目異常未發警報



紅-監控項目異常已發警報

## ● 偵測類功能：



封包測試



定時檔案



IP 通信埠



硬碟使用



CPU 與記憶體



硬碟效能



磁碟陣列



網卡 流量



連線數量



程式比對



目錄比對



執行程式



檔案數量



檔案偵測



事件警報



事件數據



排程資訊



連線測速-接收



連線測速-傳送



常驻程式(Unix/Linux 功能) 硬碟索引(Unix/Linux 功能)







系統比對



系統服務

系統比對(MS/Windows 功能) 系統服務(MS/Windows 功能)

## ● 資訊類功能：



代理程式

代理程式



外網連線

外網連線



重要記事

重要記事



處理程序

處理程序數量



處理程序拓樸圖

處理程序數量拓樸圖



偵測項目拓樸圖

偵測項目拓樸圖



歸屬主機拓樸圖

歸屬主機拓樸圖



TCP連線拓樸圖

TCP 連線拓樸圖



TCP連線分析圖

TCP 連線分析圖



封包測試

封包測試



開機記錄

開機記錄

## ● 關聯類功能：



IPMI

IPMI



交換器

交換器



系統記錄

系統記錄



UPS



網站連結



設備資訊