交通部公路總局

建立自動化 IT 資訊維運系統的標準規範

2015/09　Watchdog

● 目錄

一、 十分鐘了解主題

如何建立自動化 IT 資訊維運系統，成立[即時資訊-戰情中心]!?

就是唯有採用[自動化 IT 資訊維運系統]，才能過應付日益龐大複雜的資訊系統與設備，降低 IT 資訊維運的成本而不會淪為看守機器的奴才，讓佔人力 90%的系統檢測工作交由自動化系統檢測機制來完成。

依據墨菲定律(Murphy's Law)的原則(任何有可能會發生的問題，就會發生)，系統必須盡其所能，監控資訊設備內任何有可能會發生異常問題的項目，設定警報臨界點，並即時通知處理，避免事件擴大並讓異常狀態由被動告知轉為主動的預警機制。

＊ 每 100 台伺服器規模，約 150,000 檢測點(node)

超乎想像的海量數據與檢測點，伺服主機(包含實體主機/虛擬主機)，可掌控伺服主機 90%以上的危機因素涵蓋了各層次，

例如：主機硬體層、作業系統層、網路連線層、應用系統層與資訊安全層等。

作業系統層包含如下，

實體主機： IBM AIX、HP-UX、SUN Solaris、SCO UNIX、Linux m與 Microsoft 系列等。

虛擬主機：VMware、Microsoft Hyper-V 與 Sun Virtualbox 等，每台有 30 個以上大項，1000 個以上的監控項目與資訊分析。

交換器(Core Switch/Edge Switch))與路由器(Router)偵測點如下，

依 Switch、VLAN、連接埠拓樸圖、埠速度、MAC、IP、資料流量與負載比、Switch 的 CPU 使用比、記憶體使用比、電源供應器、溫度感測器、風扇狀態、封包流量、廣播封包、錯誤封包、忽略封包、未知封包等，每台有 25 個以上大項，500 個以上的監控項目與資訊分析，每台支援 48 個擴充模組與 1,000 個連接埠。

Netflow，Sflow 網路流量分析，依 IP 與通信埠每小時流量，作次數統計與明細內容，另有網域名稱 IP 所屬國家清單、IP 所屬國家的比例分佈圖等。

還有更多的監控項目，例如：

網路連線、網路安全、轉送機制、特定資訊、應用系統整合、系統與事件日誌整合環境監控系統、資訊設備資產管理、緊急關機等跟資訊設備有關的任何系統。

自動化維運

檢測 -> 警報通知 -> 自動控制命令或人員解除狀況。

7x24 每小時數萬次的定時檢測與資訊收集分析。

建立自動化的系統檢測機制與管理的標準流程(SOP)。

設備資訊整合

串聯所有資訊設備相關的資料關聯整合。

例如：伺服主機、交換器、網路連線效能與設備資產等，進一步提供最新快速的數據與多樣化的圖型介面形成 "資訊戰情中心"的即時資訊監控電視牆。

全方位的檢測與資訊取得

依資訊設備的特性與用途分為主動與被動來檢測與資訊取得，使用百種以上的通信與資料拗定，讓整體資訊設備能完整的受監控。

不停頓的系統交接

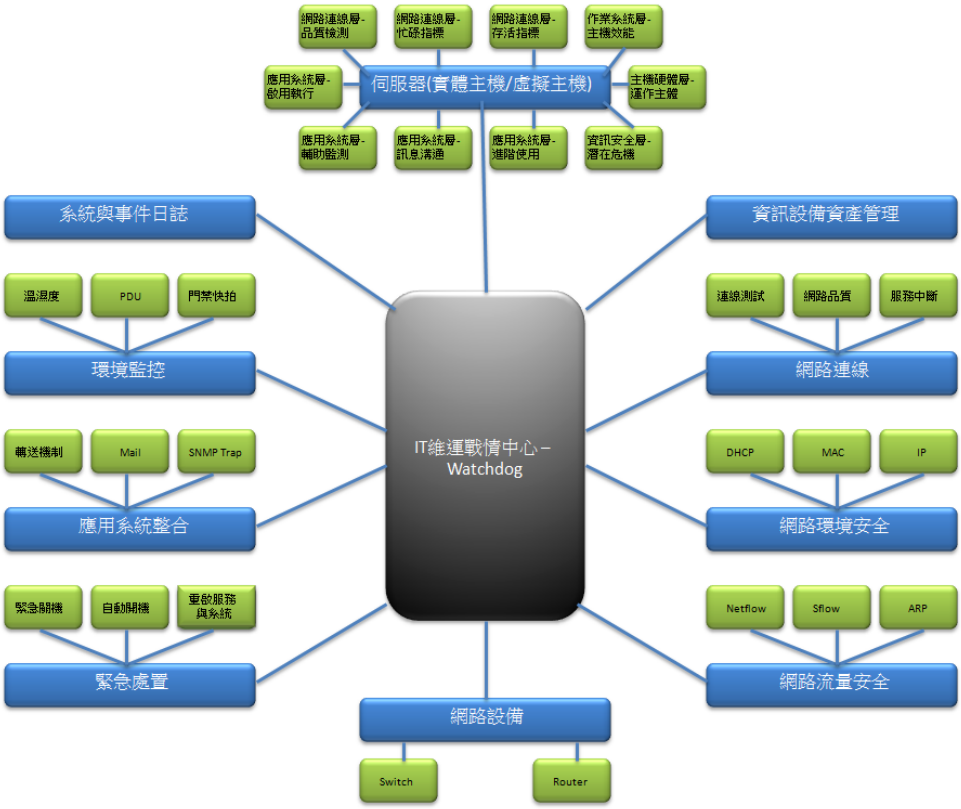
不會因系統人員異動而影響到整體資訊中心的運行控管機制，讓承接人員在短時間內迅速的進入正常運行的作業軌道。

系統人員回歸到應有的專業

讓系統人員擁有更多的時間做多些需要"思維"與"溝通"的工作，例行工作則由"自動化系統"完成，溝通拗調與進階除錯追蹤(Debug)由"人"來完成，例如：

規劃、安裝設定、系統操作、系統問題決解、進階除錯追蹤(Debug)、跨越不同設備與部門的溝通拗調。

架構圖


網路連線層-品質檢測
網路連線層-忙碌指標
網路連線層-存活指標
作業系統層-主機效能
應用系統層-啟用執行
伺服器(實體主機/虛擬主機)
主機硬體層-運作主體
應用系統層-輔助監測
應用系統層-訊息溝通
應用系統層-進階使用
資訊安全層-潛在危機
系統與事件日誌
資訊設備資產管理
溫濕度
PDU
門禁快拍
連線測試
網路品質
服務中斷
環境監控
網路連線
IT維運戰情中心－Watchdog
轉送機制
Mail
SNMP Trap
DHCP
MAC
IP
應用系統整合
網路環境安全
緊急開機
自動開機
重啟服務與系統
Netflow
Sflow
ARP
緊急處置
網路流量安全
網路設備
Switch
Router

二、 自動化與人工化的 IT 資訊維運有不同的觀念

- 可讓每一位系統人員提升十倍以上的功力與效率。
- 建立預警機制，整合關聯資訊，除錯追蹤(Debug)與大數據分析，24 小時不間斷監控，是自動化與人工化完全不一樣的觀念與做法。
- 直覺式的圖形監控系統，讓所有的維運部門不需經由人員交接溝通，即時就可接手管控。
- 讓異常狀態由被動告知轉為主動式的預警機制。
- 細微與嚴密的監控項目是人工檢測系統無法達成的任務，嚴重的異常狀況發生通常不是常常發生的事件，是偶發或是不常出現與意想不到的狀況，若能預先設立預警通報機制，當事件超過設定之異常臨界值時即時通知，讓系統管理員能夠有時間做預防式處置，不讓其有嚴重事件發生之機會。
- 預先設定"緊急事件處理程序"，當緊急事件發生時就可在短時間內啟用"緊急處理置系統"，例如：斷電、火警的"緊急關機"。

三、 佈署自動化 IT 資訊維運系統的要領

1. 重要的觀念

- 要認知 IT 資訊機房維運管理最大的原則是正確而快速的提供終端使用者資訊服務。
- 依設備用途與特性監測的細項規範與細部資訊佈署。
- 尋找服務目的的存活指標。
- 廣泛的納入任何有危險因素系統運行項目。
- 嚴謹的異常事件告警機制。

- 戰情中心概念的即時資訊。
- 整合設備與系統關聯性資料與架構。
- 跨越部門或設備的除錯追蹤(Debug)機制。
- 統合一貫的管理制度與標準程序。

- 讓操作維運系統是一項科技簡單化的運用。
- 協助接管的資訊管理人員快速掌控設備之設定與應用狀況。
- 協助資訊管理人員專業養成教育。
- 建立自動化維運的標準流程，降低系統人員異動的衝擊力。

2. 存活指標的定義

- 伺服器與作業系統是應用系統的寄宿的殼與生活環境，每一台伺服主機都有其主要的應用目的，了解其主要應用目的才能知道此台伺服主機的監控重點。
- 一台伺服主機的運行不是光從主機效能(一台 CPU 使用率 10%，另一台 CPU 使用率 90%)，就能得知其有無問題。
- 每一個資訊設備的啟用都有其主要用途之項目，為"服務目的"的重要存活指標，當設備的"服務目的"功能喪失後，此設備等於沒有用途，例如：伺服器存活指標

  建立一套伺服主機一定有一項以上的重要"服務目的"與"服務目的"的相關系統

例一： DNS 伺服器但 DNS Service 未啟動，53port 不通 -> DNS 伺服器失效

例二： 網站伺服系統的主要"存活指標"

WEB Service(Apache，IIS、、)，

Java 中介軟體、資料庫應用系統與 DNS 伺服器。

當伺服器 "服務目的"的重要存活指標出問題時，縱然此台伺服主機的其他效能都很健康，但也沒用(如：CPU，Memory，硬碟空間，網路很快)，當然除了主要功能存活指標還有其他運行指標，例如：

- 系統效能運作指標
- 重要程式指標
- 硬體運作指標

3. 資訊收集的用途與迷思

產生與收集大量的資訊資料是件容易的功能，但這些資料大部份僅會提供事後搜尋與追查訊息的功能，並不是可以收集到大量的資料就是了解系統是處於正常或異常的狀態，更會導至系統人員花費大量的時間來研判解讀資料內容的涵意。

資訊收集的主要目的

- 掌控資訊設備運行或設定的透明度
- 做為異常判定與告警依據的數據或行為
- 做為機器擴充或更新的數據參考值
- 即時資料 - 即時資訊之戰情中心,立即處置
- 短期資料 - 協助效能與狀態比對之判斷，使用時間點做為進階除錯追蹤(Debug)
- 長期資料 - 進階除錯追蹤(Debug)與大數據分析

定義資訊收集的艱難度

- 單一設備的資訊收集-簡單，一行(60 字)的 SNMP 指令可取的 1,000 筆以上的資訊。
- 整合性關聯資訊收集-困難，整合不同設備的關聯性與依賴性，串聯可能相關的資訊項目依據使用者習慣分類統計適當的資訊值，例如：
  - 看伺服器資訊時，也同時知道此伺服器接在那一台 Switch 的連接埠上，此連接埠上的流量，速度等各項資料，設備的存放位置地圖與照片一併出現
  - Switch 每埠的流量比

定義告警機制的嚴謹度

單值的異常告警定義-簡單，
僅依監測系統單一的取得值，例如：CPU 負載上限 80%發出警報，但此伺服器 CPU 負載每 5 分鐘會有一次持續 2 秒 81%，如此告警訊息會產生每 5 分鐘發出一次 ，或每晚 10 點-11 點做備份 CPU 負載 90%

多重定義的異常告警定義-困難，
如上列，定義(A)CPU 負載上限 80%+(B)連續 3 次+(C)每次間隔每 5 分鐘
A+B+C 同時成立才發出告警訊息
定義每晚 10 點-11 點不發出告警訊息

4. 每天都會發生重大事件

每台系統設備每年才會發生一次嚴重事件，看起來是很少的偶發事件，但如有 300 台以上的設備，那等於每天都有嚴重事件發生建立自動化 IT 維運系統不能因為是偶發事件，而不納入監控。

舉個實列：
使用者索取較大量資料時發覺速度很慢，系統人員開始追查：
1、使用者電腦 CPU，Memory，網路卡，硬碟 I/O，防火牆，軟體系統看起來都沒問題
2、資料庫伺服器 CPU，Memory，網路卡，硬碟 I/O，防火牆，軟體系統看起來都沒問題
3、 網路連線與 ping 回應都正常
4、 請網管幫忙看 Switch 設定，網管回應也正常
5、 請資料庫軟體廠商來檢查也很正常
結果花了整天時間，跨越了不同系統領域或部門，結果都是正常，僅能請使用者再試試。

有一天突然好了，原來是網路佈線盤面板(Panel)轉接點接觸不良，造成網路經常自動降速，而小量資料無感...

唯有全面性的監控才能跨越專業領域或部門，進行橫向關聯資訊整合，才能有效的追蹤問題，不讓不同部門或廠商發生互推的狀況， 例如應用組認為是網路的問題等。

四、 建立 IT 維運管理前的準備事項

1. 成立專案

預先規劃任何有可能影響到資訊營運的狀況點，是提升資訊維運妥善率最好的方法，詳細的檢測與收集各類型的資料用於保障正常維運的基本要件。

專案人員

- 原單位資訊管理的負責人
- 維運經理/專案經理(PM)
- 資深系統技術人員(包含：系統，網管，應用)
- 原廠技術人員

定義納入受監控設備的範圍

- 清查納入監控的設備項目，例如：伺服器、Switch
- 受監控設備必須安裝的裝置，例如：IPMI/ILO 的網段與網路線
- 受監控設備必須配合的設定與資訊，例如：Switch SNMP 啟用、Newflow 設定
- 應用系統整合的機制-歸類整合項目
  - 異常訊息轉送
  - 協助數據檢測與分析
  - 協助檢測檔案，時間，程式的狀態

了解資訊中心資源與架構

- 網路架構圖
  - 基礎網路架構圖
  - 網段區域之網路與管制架構圖
  - 網段區域的路由走向
  - 網路設備可支援的功能清單(如：Netflow/Sflow)
- 伺服器佈署的應用
  - 伺服器重要性分類
  - 伺服器重要服務的存活指標點
  - 伺服器服務系統重要支撐項目(如：inode，NAS mount filesystem)
  - 系統設備效能
  - 網路連線應用清單
  - 應用必用的服務清單(如：IIS，Apachee)
  - 重要應用必用的程式
  - 應用程式訊息溝通

自動化後檢測點共同的問題

- 需要監控的項目
- 監控項目的異常臨界點
  - 數據類通常會用大於(>)或小於(<)來定義警報發出時機。
  - 字串文字類與訊息類會用比對方式與邏輯(or、and、not)來確認警報發出時機。
- 檢測警報狀況發出的告警效率，嚴謹度與警報敏感度
- 警報發出的管道與通知名單
- 警報發出後的緊急處置方案
- 建立重要關聯整合點(如：封包測試之佈線追蹤)
- 相關資訊建立(如：設備位置，用途，保管人，維護廠商)

2. 依設備與系統不同的層次特性設計監控目標

- 伺服主機(實體主機/虛擬主機)
  - 主機硬體層-運作主體
  - 作業系統層-主機效能
  - 網路連線層-存活指標
  - 網路連線層-忙碌指標
  - 網路連線層-品質檢測
  - 應用系統層-啟用執行
  - 應用系統層-輔助監測
  - 應用系統層-訊息溝通
  - 應用系統層-進階使用
  - 資訊安全層-潛在危機

- 網路設備(交換器/路由器) 網路核心-交換器
  - 流量資訊
  - 狀態資訊
  - 設定資訊
  - 安全檢測
  - 串聯架構

- 中心監控項目-網路連線
- 中心監控項目-轉送機制
- 中心監控項目-特定資訊
- 中心監控項目-應用系統整合
- 中心監控項目-網路安全
- 中心監控項目-系統與事件日誌
- 中心監控項目-協助環境監控
- 中心監控項目-緊急處置

五、 建立 IT 維運管理的監控目標

1. 監控項目-伺服主機

主機硬體層-運作主體

主機板狀態

偵測目的： 即時掌控主機板安全指標數據狀態，保全主機硬體運作正常，使用介面為 IPMI、ILO、IMM 或是 iDRAC 等，例如風扇出問題時會讓主機溫度上升面當機、若是 VMhost 則會影響多台伺服主機。

監測目標： 溫度感測器、風扇轉速、電壓電流等

警報條件： 高於或是低於警報值

即時資訊： 數據或是警報的發佈

資訊收集： 訊息、數據、警報發佈或是解除時間點

緊急處置： 通報或是執行預定程式

警報臨界值： 依設備(要觀察 7 天後才定義警報值)

磁碟陣列

偵測目的： 即時掌控磁碟陣列卡與實體磁碟機之安全指標與設定狀態，可預警式更換磁碟，例如：若是 VMhost 則會影響多台伺服主機。

監測目標：

磁碟陣列卡與記憶體狀態

電池狀態

磁碟陣區

邏輯磁碟區

實體磁碟機

警報條件：

新增或移除

故障

重建

即時資訊：正常/警報發佈

資訊收集：訊息、警報發佈/解除時間點

緊急處置：通報、執行預定程式

警報臨界值：使用預設值

作業系統層-主機效能

CPU 與記憶體

偵測目的： 隨時了解主機使用效能，預警於逐漸影響或突發狀況

監測目標： 使用率

警報條件： 大於使用率+次數+連續時間

即時資訊： 數據/警報發佈

資訊收集： 訊息、數據、警報發佈/解除時間點

緊急處置： 通報、執行預定程式

警報臨界值： 預設 90%

硬碟使用

偵測目的： 定時取得 Filesystem 使用量，確保系統運作正常，預警於逐漸影響或突發狀況

監測目標： 低於(不存在)或高於使用率

警報條件： 大於/小於使用率+次數+連續時間、列表以外的視為非法掛載

即時資訊： 數據/警報發佈

資訊收集： 訊息、數據、警報發佈/解除時間點

緊急處置： 通報、執行預定程式

警報臨界值： 預設 90%

硬碟索引(Unix/Linux inode)

偵測目的： 定時取得 Filesystem inode 使用量，確保系統運作正常，預警於逐漸影響或突發狀況

監測目標： 低於(不存在)或高於使用率

警報條件： 大於/小於使用率+次數+連續時間

即時資訊： 數據/警報發佈

資訊收集： 訊息、數據、警報發佈/解除時間點

緊急處置： 通報、執行預定程式

警報臨界值： 預設 80%

硬碟效能

偵測目的： 定時測試硬碟或 Filesystem 讀寫速度，了解本機 I/O 效能，預警於逐漸影響或突發狀況

監測目標： 低於(不存在)或高於使用率

警報條件： 大於/小於使用率+次數+連續時間

即時資訊： 數據/警報發佈

資訊收集： 訊息、數據、警報發佈/解除時間點

緊急處置： 通報、執行預定程式

警報臨界值： 依設備(要觀察 7 天後才定義警報值)

網路連線層-存活指標

封包測試-代理偵測

偵測目的： 僅限本機與特定主機連線時之網路品質監測，如： 特定專線與主機

監測目標： 漏失率與封包回應時間

警報條件： 大於漏失率或封包回應時間+次數+連續時間

即時資訊： 數據/警報發佈

資訊收集： 訊息、數據、警報發佈/解除時間點

緊急處置： 通報、執行預定程式

警報臨界值： 依設備(要觀察 7 天後才定義警報值)

IP 通信埠-代理偵測

偵測目的： 僅限本機與特定主機網路服務程式是否中斷，例如特定專線與主機

監測目標： 網路服務程式中斷(關閉)

警報條件： 關閉狀態+次數+連續時間

即時資訊： 正常/警報發佈

資訊收集： 訊息、警報發佈/解除時間點

緊急處置： 通報、執行預定程式

警報臨界值： 依設備(要觀察 7 天後才定義警報值)

定時檔案-代理偵測

偵測目的： 僅限本機與特定主機系統或主機存活標記，例如特定專線與主機

監測目標： 存活標記(使用字串名稱)

警報條件： 溢時未回報

即時資訊： 正常/警報發佈

資訊收集： 訊息、警報發佈/解除時間點

緊急處置： 通報、執行預定程式

警報臨界值： 依預設值

網路連線層-忙碌指標

網卡流量

偵測目的： 統計分析本機網卡每秒平均收/送封包流量之監測

監測目標： 網路卡

警報條件： 收/送 每秒封包數量最低值或最高值、列表以外的視為非法網卡

即時資訊： 數據/警報發佈

資訊收集： 訊息、數據、警報發佈/解除時間點
緊急處置： 通報、執行預定程式
警報臨界值： 依網路服務特性定義警報值

連線數量
偵測目的： 統計依 Socket Port+本機 IP 連入(ESTABLISHED)的數量
監測目標： 本機 IP+通信埠(Socket Port)
警報條件： 最小與最大連線數量
即時資訊： 數據/警報發佈
資訊收集： 訊息、數據、警報發佈/解除時間點
緊急處置： 通報、執行預定程式
警報臨界值： 依網路服務特性定義警報值

網路連線層-品質檢測
連線測速-接收
偵測目的： 定時檢測二台主機間的網路傳送速度
監測目標： 主機 IP
警報條件： 最低傳送速度與最低回傳速度(KB/sec)
即時資訊： 數據/警報發佈
資訊收集： 訊息、數據、警報發佈/解除時間點
緊急處置： 通報、執行預定程式
警報臨界值： 依網路服務特性定義警報值

連線測速-傳送
偵測目的： 定時檢測二台主機間的網路傳送速度
監測目標： 主機 IP
警報條件： 最低傳送速度與最低回傳速度(KB/sec)
即時資訊： 數據/警報發佈
資訊收集： 訊息、數據、警報發佈/解除時間點
緊急處置： 通報、執行預定程式
警報臨界值： 依網路服務特性定義警報值

應用系統層-啟用執行
執行程式
偵測目的： 定時檢測必須執行之程式數量，用於程式中止未執行或重複執行太多與 LISTEN 服務程式啟用，例如： FTP client 傳送，若卡死則 FTP 程式的數量會增加很多
監測目標： 程式名稱
警報條件： 最低執行數量/最高執行數量

即時資訊： 數據/警報發佈
資訊收集： 訊息、數據、警報發佈/解除時間點
緊急處置： 通報、執行預定程式
警報臨界值： 依程式特性定義警報值

系統服務(Windows service)
偵測目的： 定時檢測系統服務是啟用或停止狀態
監測目標： 系統服務名稱
警報條件： 指定是啟用或停止狀態
即時資訊： 正常/警報發佈
資訊收集： 訊息、警報發佈/解除時間點
緊急處置： 通報、執行預定程式
警報臨界值： 依服務特性定義警報值

應用系統層-輔助監測
檔案數量
偵測目的： 定時檢測資料夾內的檔案數量過少或太多，例如資料傳送暫存區，若檔案數量過多，可能是處理程式已停止運作
監測目標： 資料夾位置名稱
警報條件： 最低或最高檔案數量
即時資訊： 數據/警報發佈
資訊收集： 訊息、數據、警報發佈/解除時間點
緊急處置： 通報、執行預定程式
警報臨界值： 依服務特性定義警報值

檔案偵測
偵測目的： 定時檢測檔案更新時間與使用量，例如若利用檔案來驗證應用程式存活，在一定的時間內應用程式必須更新驗證檔，若溢時未更新表示此應用程式已停止運作
監測目標： 檔案名稱
警報條件： 最高溢時秒或最高低檔案使用量
即時資訊： 數據/警報發佈
資訊收集： 訊息、數據、警報發佈/解除時間點
緊急處置： 通報、執行預定程式
警報臨界值： 依服務特性定義警報值

應用系統層-訊息溝通
事件警報

偵測目的： 讓各專案的應用程式整合入監控系統，當應用程式必須將緊急事件發佈時可將訊息內容寫入指定之檔案

監測目標： 檔案名稱

警報條件： 檔案成立

即時資訊： 正常/警報發佈

資訊收集： 訊息、警報發佈/解除時間點

緊急處置： 通報、執行預定程式

警報臨界值： 依應用程式定義警報內容

事件數據

偵測目的： 讓各專案的應用程式整合入監控系統，當應用程式必須將數據資料交由此項功能來統計分析與判別正常或發佈警報時，例如：

1.資料庫的 TempDB/TABLE 使用比

2.環控系統收集到的溫濕度數據

監測目標： 檔案名稱內的數據

警報條件： 最低或最高數據值

即時資訊： 數據/警報發佈

資訊收集： 訊息、數據、警報發佈/解除時間點

緊急處置： 通報、執行預定程式

警報臨界值： 依應用程式定義警報值

應用系統層-進階使用

排程資訊

偵測目的： 定時自動執行特定功能之程式，並將產生之結果文字檔回傳

1、保留記錄

2、比對記錄內容符合警報條件

3、將記錄內容交由後製程式處理

監測目標： 使用程式

警報條件： 文字內容

即時資訊： 正常/警報發佈

資訊收集： 訊息、警報發佈/解除時間點

緊急處置： 通報、執行預定程式

警報臨界值： 依應用程式定義警報值

資訊安全層-潛在危機

常駐程式(Unix/Linux)

偵測目的： 檢查作業系統正在執行中的程式是否非指定內

監測目標： 程式名稱

警報條件： 執行中
即時資訊： 正常/警報發佈
資訊收集： 訊息、警報發佈/解除時間點
緊急處置： 通報、執行預定程式
警報臨界值： 執行中

程式比對

偵測目的： 百分百二進位比對指定的程式或檔案與封裝的原始檔是否遭受更改
監測目標： 程式或檔案名稱
警報條件： 比對不同
即時資訊： 正常/警報發佈
資訊收集： 訊息、警報發佈/解除時間點
緊急處置： 通報、執行預定程式
警報臨界值： 比對不同

目錄比對

偵測目的： 百分百二進位比對指定資料夾內的檔案與封裝的原始檔是否遭受更改
監測目標： 程式或檔案名稱
警報條件： 比對不同
即時資訊： 正常/警報發佈
資訊收集： 訊息、警報發佈/解除時間點
緊急處置： 通報、執行預定程式、還原檔案
警報臨界值： 比對不同

系統比對(Windows 系列)

偵測目的： 封存整個作業系統的程式，定時做百分百二進位比對系統內的程式與封裝的原始程式是否遭受更改
監測目標： 整個作業系統的程式
警報條件： 比對不同、新增程式
即時資訊： 正常/警報發佈
資訊收集： 訊息、警報發佈/解除時間點
緊急處置： 通報、執行預定程式
警報臨界值： 比對不同、新增程式

2. 監控項目-虛擬主機

一般性作業系統(如：VirtualBox)，比照伺服主機的監控項目

特殊性作業系統(如： VMware)

磁碟陣列

偵測目的： 即時掌控磁碟陣列卡與實體磁碟機之安全指標與設定狀態、可預警式更換磁碟，例如若是 VMhost 則會影響多台伺服主機

監測目標：

磁碟陣列卡與記憶體狀態、電池狀態

磁碟陣區

邏輯磁碟區

實體磁碟機

警報條件：

新增或移除

故障

重建

即時資訊： 正常/警報發佈

資訊收集： 訊息、警報發佈/解除時間點

緊急處置： 通報、執行預定程式

警報臨界值： 使用預設值

Guest 主機

新增移除 Guest 時發出警報

資訊收集

收集作業系統內的各項資訊

3. 中心監控項目-網路設備

交換器(SWITCH)與路由器(ROUTER)

偵測目的： 詳細的收集可能會影響到"連結設備"，例如伺服主機之效能數據，用於立即發出警訊與查詢關聯架構

監測目標：

SWITCH 設備之 CPU 負載

SWITCH 設備之記憶體使用量

SWITCH 設備之機箱裝置-溫度感測器

SWITCH 設備之機箱裝置-電源供應器

SWITCH 設備之機箱裝置-風扇狀態

SWITCH 設備之 VLAN 分佈與設定

流量檢測(分 進/出/進+出)依三大項分別統計分析

1、依 SWITCH 設備

2、依 VLAN

3、依每一通信埠

通信埠速度

每秒流量負載比

每秒資料封包流量

每秒廣播封包流量

每秒錯誤封包流量

每秒忽略封包流量

每秒未知封包流量

資安檢測

預設合法 MAC，比對非法新增 MAC

使用 CLI

進階使用 CLI 來進行命令執行，如：備份設定檔

串接拓撲圖

展示串接 SWITCH 每一通信埠所連結之關聯設備圖

關聯資訊

自動串接每一通信埠所連結之關聯設備資訊，例如伺服主機的主機資訊

警報條件： 依每一項目

即時資訊： 數據/警報發佈

資訊收集： 訊息、數據、警報發佈/解除時間點

緊急處置： 通報、執行預定程式

警報臨界值： 依設備(要觀察 7 天後才定義警報值)

4. 中心監控項目-網路連線

封包測試

偵測目的： 針對有網路能力的設備進行連線網路品質監測與斷線測試

監測目標： 漏失率與封包回應時間

警報條件： 大於漏失率或封包回應時間+次數+連續時間

即時資訊： 數據/警報發佈

資訊收集： 訊息、數據、警報發佈/解除時間點

緊急處置： 通報、執行預定程式
警報臨界值： 依設備(要觀察 7 天後才定義警報值)

IP 通信埠
偵測目的： 針對有網路服務能力的設備進行 Socket 連線監測確認主機網路服務程式是否中斷、例如： 網站、FTP 伺服器
監測目標： 網路服務程式中斷(關閉)
警報條件： 關閉狀態+次數+連續時間
即時資訊： 正常/警報發佈
資訊收集： 訊息、警報發佈/解除時間點
緊急處置： 通報、執行預定程式
警報臨界值： 依設備(要觀察 7 天後才定義警報值)

定時檔案
偵測目的： 監控主機與特定主機系統或主機執行程式的存活標記
監測目標： 存活標記(使用字串名稱)
警報條件： 溢時未回報
即時資訊： 正常/警報發佈
資訊收集： 訊息、警報發佈/解除時間點
緊急處置： 通報、執行預定程式
警報臨界值： 依預設值

網站偵測
偵測目的： 直接取得網頁資料，用於判斷網站服務是否中斷可檢測網路與 DNS 解析
WEB Server (如：Apachee、IIS)
中介程式(如：Java AP)
後台資料庫
網頁花費時間
監測目標： 網址與網頁參數
警報條件： 網站回應碼
即時資訊： 數據/警報發佈
資訊收集： 訊息、數據、警報發佈/解除時間點
緊急處置： 通報、執行預定程式
警報臨界值： 依預設值

連線測速-接收
偵測目的： 定時檢測二台主機間的網路傳送速度

監測目標： 主機 IP
警報條件： 最低傳送速度與最低回傳速度(KB/sec)
即時資訊： 數據/警報發佈
資訊收集： 訊息、數據、警報發佈/解除時間點
緊急處置： 通報、執行預定程式
警報臨界值： 依網路服務特性定義警報值

連線測速-傳送
偵測目的： 定時檢測二台主機間的網路傳送速度
監測目標： 主機 IP
警報條件： 最低傳送速度與最低回傳速度(KB/sec)
即時資訊： 數據/警報發佈
資訊收集： 訊息、數據、警報發佈/解除時間點
緊急處置： 通報、執行預定程式
警報臨界值： 依網路服務特性定義警報值

5. 中心監控項目-轉送機制

郵件轉送
偵測目的： 整合其他設備的警示訊息，利用郵件方式協助其他設備處理告警事件
監測目標： 郵件信箱帳號
警報條件： 無條件與文字內容篩選條件
即時資訊： 正常/警報發佈
資訊收集： 訊息、警報發佈/解除時間點
緊急處置： 通報、執行預定程式
警報臨界值： 依條件

SNMP TRAP
偵測目的： 整合其他設備的警示訊息，當資訊設備有能力因設備故障或特定訊息而發出 SNMP TRAP 訊息時，例如儲存系統硬碟故障
監測目標： 任何有 SNMP TRAP 功能之設備
警報條件： 無條件與文字內容篩選條件與數據高低條件
即時資訊： 數據/警報發佈
資訊收集： 訊息、數據、警報發佈/解除時間點
緊急處置： 通報、執行預定程式
警報臨界值： 依條件

6. 中心監控項目-特定資訊

SNMP

偵測目的： 指定設備特定的 MIB 與 OID 定時取得文字或數據資料，依據警報條件值判斷為正常或異常

監測目標： 任何有 SNMP 功能之設備

警報條件： 依據文字內容比對警報條件與數據高低條件

即時資訊： 數據/警報發佈

資訊收集： 訊息、數據、警報發佈/解除時間點

緊急處置： 通報、執行預定程式

警報臨界值： 依網路服務特性定義警報值

7. 中心監控項目-應用系統整合

警報閘道

偵測目的： 讓各專案的應用程式整合入監控系統，當應用程式必須將告警或解除警報資料立即交由監控中心發佈時

監測目標： 專案名稱

警報條件： 立即發佈

即時資訊： 正常/警報發佈

資訊收集： 訊息、警報發佈/解除時間點

緊急處置： 通報、執行預定程式

警報臨界值： 依收到訊息

事件數據

偵測目的： 讓特別專屬的應用程式整合入監控系統，當應用程式必須將數據資料交由此項功能來統計分析與判別正常或發佈警報時，例如統計各平均負載伺服器與資料庫主機每台的特定連線數量

監測目標： 檔案名稱內的數據

警報條件： 最低或最高數據值

警報條件： 檔案成立

即時資訊： 數據/警報發佈

資訊收集： 訊息、數據、警報發佈/解除時間點

緊急處置： 通報、執行預定程式

警報臨界值： 依應用程式定義警報值

8. 中心監控項目-網路環境安全

DHCP 伺服器

偵測目的： 內部網路內流竄著各類型的通信協定，有些僅會浪費網路資源，但有些則會造成嚴重影響，例如不當的 DHCP 伺服器

監測目標：

合法 DHCP 伺服器以外的 DHCP 伺服器

非法 DHCP 伺服器檢查

DHCP 伺服器溢放 IP 檢查

IP 衝突危機檢查

警報條件： 合法以外的 IP 與 MAC

即時資訊： 正常/警報發佈

資訊收集： 訊息、警報發佈/解除時間點

緊急處置： 通報、執行預定程式

警報臨界值： 依應用定義警報值

IP 與 MAC 控管

偵測目的： 降低 IP 衝突的危機，非法私接設備

監測目標：

MAC 綁 IP 名單

合法 MAC 名單

訪客臨時名單

IP 衝突危機檢查

警報條件： 合法 IP 與 MAC 以外的設備

即時資訊： 正常/警報發佈

資訊收集： 訊息、警報發佈/解除時間點

緊急處置： 通報、執行預定程式

警報臨界值： 依應用定義警報值

9. 中心監控項目-網路流量安全

Netflow/Sflow 流量

偵測目的： 即時掌控網路資料流向，提供每筆資料詳細資訊資料內容包含網路拹定的各種重要資訊，例如來源 IP、來源拹定通信埠、來源 MAC、通信拹定 (ICMP、IGMP、TCP、UDP、ARP)、目的 IP、目的拹定通信埠與目的 MAC 資料流量

依據資料源可分析統計下列資訊

網內進或出、網外進或出的

每小時封包(Packet)統計量

每小時流量(Bytes)統計量

每小時次數統計量

每天總計量

依 TCP 通信埠統計

依 UDP 通信埠統計

網域名稱 IP 所屬國家清單

IP 所屬國家的比例分佈圖

監測目標： 任何由 Netflow/Sflow 捕捉到的網路流量

警報條件： 每小時統計量

即時資訊： 數據/警報發佈

資訊收集： 訊息、數據、警報發佈/解除時間點

緊急處置： 通報、執行預定程式

警報臨界值： 依應用定義警報值

ARP 要求與回應

偵測目的： 即時掌控內網中 ARP 流動數量，即時讓系統人員更能了解網路中的 ARP 流動量是否正常，依每一 IP 設備統計

每小時要求量統計

每小時回應量統計

每天總計量統計

監測目標： 任何內網中發出 ARP 要求與回應之 IP

警報條件： 每小時統計量

即時資訊： 數據/警報發佈

資訊收集： 訊息、數據、警報發佈/解除時間點

緊急處置： 通報、執行預定程式

警報臨界值： 依應用定義警報值

10. 中心監控項目-系統與事件日誌

系統與事件日誌

偵測目的： 即時收集系統日誌或事件日誌

1、 應付準則

2、 利用等級分類或訊息內容篩檢而發出警報

3、 事後追查問題

監測目標： 指定系統日誌或事件日誌的主機與設備

警報條件： 設定等級分類或訊息內容篩檢而發出警報

即時資訊： 正常/警報發佈

資訊收集： 訊息、警報發佈/解除時間點

緊急處置： 通報、執行預定程式

警報臨界值： 依應用定義警報值

11. 中心監控項目-協助環境監控

不斷電系統-UPS

偵測目的： 大部份資訊機房都配有 UPS，防止突然斷電之危機，而且都會由環控系統監控，UPS 會配備網卡並支援 SNMP，但將重要的電力來源設備納入雙重且整合的性監測，將會是多一層保障

監測目標：

市電輸入電壓

輸入頻率

輸出電壓

輸出負載

電池剩餘容量

警報條件： 最低或最高數據值

即時資訊： 數據/警報發佈

資訊收集： 訊息、數據、警報發佈/解除時間點

緊急處置： 通報、執行預定程式

警報臨界值： 依系統定義警報值

溫度與濕度感測器

偵測目的： 機房溫度與濕度是由環控系統來監控，但如果再要新增數組溫度與濕度感測器或再將重要的設備納入雙重且整合的監測，將會是多一層保障

監測目標：

溫度感測器

濕度感測器

警報條件： 最低或最高數據值

即時資訊： 數據/警報發佈
資訊收集： 訊息、數據、警報發佈/解除時間點
緊急處置： 通報、執行預定程式
警報臨界值： 依系統定義警報值

網路攝影機

偵測目的： 即時快拍，存檔記錄容量小，存放時間長隨時可查詢照片，例如人員進出重要地點時立即拍攝

監測目標：

紅外線感測器
門禁感測器

警報條件： 觸動/開啟
即時資訊： 數據/警報發佈
資訊收集： 警報時間點
緊急處置： 通報、執行預定程式
警報臨界值： 觸動/開啟

12. 中心監控項目-緊急處置

緊急關機

當市電中斷時，UPS 如果品質還很好時，會有 20-30 分鐘的時間進行緊急關機，但是要使用多重方式來執行 "緊急關機"動作，例如：

虛擬按鍵(由瀏覽器操作)
實體按鍵來進行全面關機是一個快速又安全的方法

實施"緊急關機"必須要有嚴密的控管機制與步驟

要考慮系統之間的依賴性與順序
依不同重要等級依序關機
依不同性質的伺服主機使用不同的方法關機、例如實體主機/虛擬主機(VMware)/儲存系統(Storage)
建立執行控管機制
要考慮執行的方法與位置、例如機房火災人員無法進入
