



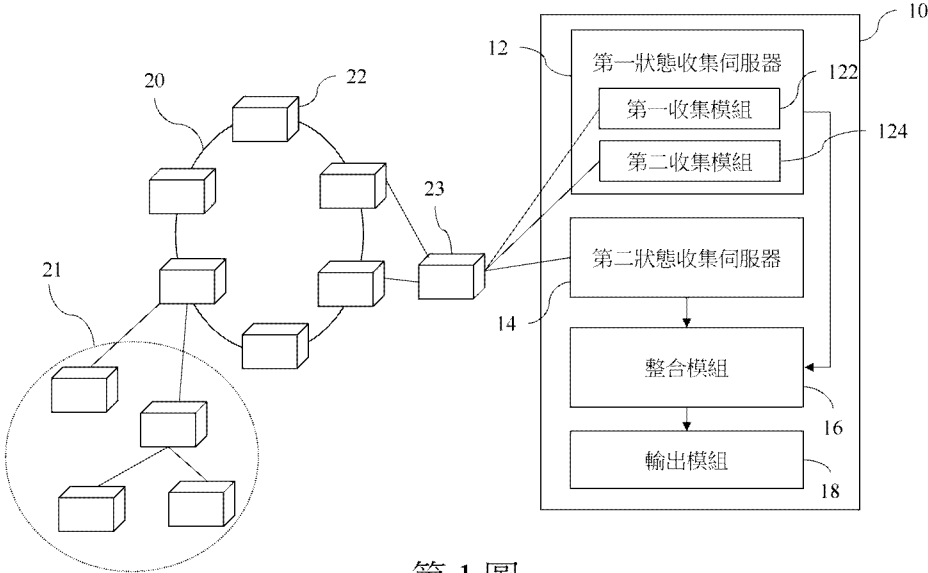
(21)申請案號：113203490 (22)申請日：中華民國 113 (2024) 年 04 月 10 日
(51)Int. Cl.： H04L43/20 (2022.01) H04L43/02 (2022.01)
H04L43/04 (2022.01)
(71)申請人：晉泰科技股份有限公司(中華民國) GENESIS TECHNOLOGY INC. (TW)
新竹市東區光復路二段 289 號 7 樓
(72)新型創作人：林聖源 (TW)；胡翔皓 (TW)
(74)代理人：江日舜
申請專利範圍項數：11 項 圖式數：5 共 20 頁

(54)名稱
乙太網路協定之監控系統

(57)摘要
一種乙太網路協定之監控系統，應用於監控環狀網路中的複數設備，監控系統包括一第一狀態收集伺服器，包括第一收集模組及第二收集模組，此二者分別利用主動和被動方式取得設備的複數設備狀態，第一狀態收集伺服器還包括第一告警通知；一第二狀態收集伺服器，利用 Syslog 服務接收設備的複數 Syslog 資料，並據以產生第二告警通知；一整合模組，設定告警條件，將第一告警通知、第二告警通知與告警條件進行比對，判斷設備是否有一告警事件發生；以及一輸出模組，將告警事件提供給使用者觀看。本創作整合不同通訊協定取得的設備狀態並解析，達到更完善的監控。

指定代表圖：

- 符號簡單說明：
- 10:乙太網路協定之監控系統
 - 12:第一狀態收集伺服器
 - 122:第一收集模組
 - 124:第二收集模組
 - 14:第二狀態收集伺服器
 - 16:整合模組
 - 18:輸出模組
 - 20:環狀網路
 - 21:其它網路設備
 - 22:設備



第 1 圖

M658293

TW M658293 U

23:連接埠裝置



公告本

申請日：
IPC 分類：

M658293

【新型摘要】

【中文新型名稱】 乙太網路協定之監控系統**【中文】**

一種乙太網路協定之監控系統，應用於監控環狀網路中的複數設備，監控系統包括一第一狀態收集伺服器，包括第一收集模組及第二收集模組，此二者分別利用主動和被動方式取得設備的複數設備狀態，第一狀態收集伺服器還包括第一告警通知；一第二狀態收集伺服器，利用Syslog服務接收設備的複數Syslog資料，並據以產生第二告警通知；一整合模組，設定告警條件，將第一告警通知、第二告警通知與告警條件進行比對，判斷設備是否有一告警事件發生；以及一輸出模組，將告警事件提供給使用者觀看。本創作整合不同通訊協定取得的設備狀態並解析，達到更完善的監控。

【指定代表圖】 第(1)圖**【代表圖之符號簡單說明】**

10:乙太網路協定之監控系統

12:第一狀態收集伺服器

122:第一收集模組

124:第二收集模組

14:第二狀態收集伺服器

16:整合模組

18:輸出模組

20:環狀網路

21:其它網路設備

22:設備

23:連接埠裝置

【新型說明書】

【中文新型名稱】 乙太網路協定之監控系統

【技術領域】

【0001】 本創作係有關一種網路監控領域，特別是指一種乙太網路協定之監控系統。

【先前技術】

【0002】 設備之監控仰賴設備回傳其狀態資訊到後端伺服器，維修工程師根據預先設定的條件、關鍵字或數值等判斷設備是否發生異常。有時候條件設的較為寬鬆，設備其實已經發生異常，只是尚未到需要停機的程度，則不會發出告警通知。但在部份情況下，些微異常已經可能導致設備停擺，例如雙料件的設備往往要兩個料件都壞掉才會停機，因此若發生只有一個料件損壞的事件，系統判斷後不會發出告警，但往後當設備出現更嚴重的狀況時容易忽視之前的一個料件的異常事件。

【0003】 此外，目前的監控系統多採用單一通訊協定收集設備狀態資料，但每一種通訊協定收集資料、判斷是否發出告警的方式不同，有可能因為預設偵錯條件的差異而漏失需要告警的設備異常。若能增加監控的精確度，避免設備停機的情況發生，將可避免停機造成的損失。

【0004】 有鑑於此，本創作針對上述習知技術之缺失及未來之需求，提出一種乙太網路協定之監控系統，具體架構及其實施方式將詳述於下：

【新型內容】

【0005】 本創作之主要目的在提供一種乙太網路協定之監控系統，其利用多種不同的通訊協定互相互補以監控環狀網路中的設備狀態，以避免當設備發生微小的異常狀態時被監控系統忽視，例如當設備離線時，被動監控的方式會無法得知設備狀態，從而造成停機維修的困境。

【0006】 本創作之另一目的在提供一種乙太網路協定之監控系統，其係利用SNMP Poller、SNMP Trap結合Syslog同時進行監控。

【0007】 為達上述目的，本創作提供一種乙太網路協定之監控系統，其應用於監控一環狀網路中的複數設備，乙太網路協定之監控系統包括：一第一狀態收集伺服器，包括一第一收集模組及一第二收集模組，第一收集模組及第二收集模組分別利用主動和被動方式取得設備的複數設備狀態，第一狀態收集伺服器還包括至少一第一告警通知；一第二狀態收集伺服器，利用一系統紀錄通訊協定服務接收設備的複數Syslog資料，並據以產生至少一第二告警通知；一整合模組，連接第一狀態收集伺服器及第二狀態收集伺服器，在整合模組中設定一告警條件，將第一告警通知、第二告警通知與告警條件進行比對，判斷設備是否有一告警事件發生；以及一輸出模組，連接整合模組，將告警事件提供給一使用者觀看。

【0008】 依據本創作之實施例，第一狀態收集伺服器係利用簡單網路管理協定進行資料收集與告警。

【0009】 依據本創作之實施例，第一收集模組係設定一偵錯條件，利用簡單網路管理協定對設備進行發現（discover）及輪詢（polling），當設備

狀態中出現符合偵錯條件的事件時，第一收集模組主動從環狀網路中撈取事件並產生第一告警通知。

【0010】 依據本創作之實施例，第一收集模組更包括一輪詢群組（Poller Group），以擴充可收集之設備狀態的設備之數量。

【0011】 依據本創作之實施例，第二收集模組係設定一偵錯條件，且設備利用一簡單網路管理協定陷阱服務（SNMP Trap Service）自動送出一SNMP_Trapped訊息給第二收集模組，由第二收集模組依據偵錯條件對SNMP_Trapped訊息進行解析，並產生一SNMP_Trapped告警通知。

【0012】 依據本創作之實施例，第一狀態收集伺服器更包括一第一資料庫，第一資料庫連接第一收集模組及第二收集模組，用以儲存第一收集模組及第二收集模組所收集之設備狀態及第一告警通知。第一資料庫為基於分散式儲存的資料庫集群。

【0013】 依據本創作之實施例，第二狀態收集伺服器包括一搜尋和數據分析引擎集群，用以對Syslog資料進行解析。

【0014】 依據本創作之實施例，第二狀態收集伺服器包括一第二資料庫，第二資料庫為基於分散式儲存的資料庫集群（MongoDB Cluster），儲存設備的Syslog資料。

【0015】 依據本創作之實施例，輸出模組更顯示第一告警通知、第二告警通知及設備之設備狀態提供給使用者觀看，設備狀態包括設備之即時狀態及歷史狀態。

【0016】 依據本創作之實施例，整合模組更包括一第三資料庫，第三資料庫為Microsoft SQL資料庫。

【0017】 依據本創作之實施例，輸出模組更包括一第四資料庫，第四資料庫為MySQL資料庫。

【圖式簡單說明】

【0018】

第1圖為本創作乙太網路協定之監控系統之方塊圖。

第2圖為本創作乙太網路協定之監控系統之細部方塊圖。

第3圖及第4圖為本創作乙太網路協定之監控系統之示意圖。

第5圖為本創作乙太網路協定之監控系統之另一實施例之示意圖。

【實施方式】

【0019】 下面將結合本創作實施例中的附圖，對本創作實施例中的技術方案進行清楚、完整地描述，顯然，所描述的實施例是本創作一部分實施例，而不是全部的實施例。

【0020】 應當理解，當在本說明書和所附申請專利範圍中使用時，術語「包括」和「包含」指示所描述特徵、整體、步驟、操作、元素和/或元件的存在，但並不排除一個或多個其它特徵、整體、步驟、操作、元素、元件和/或其集合的存在或添加。

【0021】 還應當理解，在此本創作說明書中所使用的術語僅僅是出於描述特定實施例的目的而並不意在限制本創作。如在本創作說明書和所附申請專利範圍中所使用的那樣，除非上下文清楚地指明其它情況，否則單數形式的「一」、「一個」及「該」意在包括複數形式。

【0022】 還應當進一步理解，在本創作說明書和所附申請專利範圍中使用的術語「及/或」是指相關聯列出的項中的一個或多個的任何組合以及所有可能組合，並且包括這些組合。

【0023】 本創作提供一種乙太網路協定之監控系統。請同時參考第1圖，其為本創作乙太網路協定之監控系統10之方塊圖。本創作之乙太網路協定之監控系統10用以監控一環狀網路20中的複數設備22，此環狀網路20係應用彈性乙太網路協定（Resilient Ethernet Protocol, REP），設備22為特定交換器或路由器，只有特定種類的交換器或路由器可建立環狀網路20。其它網路設備21則透過設備22形成的環狀網路20連上網路，這些其它網路設備21可以是無線網路連接器、交換器、路由器等任一種網路設備，且其它網路設備21彼此之間係透過生成樹協定（Spanning Tree Protocol, STP）建立連線。彈性乙太網路協定具有修復時間快、提供不同設備之間網路彈性的優點，極適合工業自動化產業的運用。多台設備22利用彈性乙太網路協定連接成環形拓樸後，通過一連接埠裝置23與本創作所提供的乙太網路協定之監控系統10連接。連接埠裝置23和環狀網路20上的設備22之間係透過生成樹協定（STP）建立連線。本創作的乙太網路協定之監控系統10包括一第一狀態收集伺服器12、一第二狀態收集伺服器14、一整合模組16及一輸出模組18。第一狀態收集伺服器12包括一第一收集模組122及一第二收集模組124，第一收集模組122、第二收集模組124及第二狀態收集伺服器14與連接埠裝置23連接，且第一狀態收集伺服器12及第二狀態收集伺服器14還與整合模組16連接，整合模組16連接輸出模組18。

【0024】 第一狀態收集伺服器12係利用簡單網路管理協定（Simple Network Management Protocol, SNMP）進行資料收集與告警。其中，第一收集模組122係利用主動的方式取得設備22及其它網路設備21的設備狀態，而第二收集模組124則是利用被動方式取得設備22及其它網路設備21的設備狀態。

【0025】 在一實施例中，第一收集模組122為採用簡單網路管理協定的輪詢單元（SNMP Poller），第一收集模組122先設定一偵錯條件，再利用簡單網路管理協定對設備22及其它網路設備21進行發現（discover）及輪詢（polling），當任一設備22及其它網路設備21的設備狀態中出現符合偵錯條件的事件時，第一收集模組122主動從環狀網路20所傳送的設備狀態中撈取出該筆事件，並產生一第一告警通知。在一實施例中，第二收集模組124採用簡單網路管理協定陷阱服務（SNMP Trap Service），其也會設定一偵錯條件，當任一設備22或其它網路設備21利用SNMP Trap送出一SNMP_Trap訊息時，SNMP_Trap訊息通過連接埠裝置23傳送給第二收集模組124。第二收集模組124透過相關的管理資訊庫（Management Information Base, MIB）對該SNMP_Trap訊息進行解析，再與設定的偵錯條件進行比對，並產生一SNMP_Trap告警通知。需注意的是，第一收集模組122及第二收集模組124所設定的偵錯條件可相同或不同，且第一收集模組122主動撈取設備狀態中的異常事件，而第二收集模組124則是被動接收設備發出的SNMP_Trap訊息。

【0026】 第二狀態收集伺服器14利用一系統紀錄通訊協定服務（System Logging Protocol, Syslog）接收設備22及其它網路設備21的複數Syslog資

料。其中，無論第二狀態收集伺服器14是否有設定偵錯條件或偵錯數值，第二狀態收集伺服器14都可以接收到設備22及其它網路設備21的完整Syslog資料。若第二狀態收集伺服器14有設定偵錯條件或偵錯數值，當有任一設備22或其它網路設備21的Syslog資料與設定之偵錯條件或偵錯數值相符時，第二狀態收集伺服器14會比對出該筆相符的Syslog資料，並產生至少一第二告警通知。

【0027】 整合模組16整合了第一狀態收集伺服器12及第二狀態收集伺服器14所產生的資料，包括第一狀態收集伺服器12取得的設備狀態、第一收集模組122產生的第一告警通知、第二收集模組124接收到的SNMP_Trapping訊息及產生的SNMP_Trapping告警通知、第二狀態收集伺服器14取得的Syslog資料及產生的第二告警通知。整合模組16中設定一告警條件，此告警條件為關鍵字、或關鍵字和數字的結合，並將第一告警通知、第二告警通知與告警條件進行比對。若告警條件和第一告警通知、第二告警通知都相符，代表設備22或其它網路設備21的確有需要維修的告警事件發生，整合模組16會即時將此事件通知給使用者或維修人員。若告警條件僅和第一告警通知或第二告警通知其中一者相符，整合模組16仍會即時將此事件通知給使用者或維修人員，蓋因於本創作同時使用SNMP和Syslog兩種通訊協定的目的就是要讓資料互補，因為Syslog及SNMP_Trapping都是被動的方式等設備22或其它網路設備21丟出訊息，所以本創作透過SNMP polling以主動的方式定期判斷設備22或其它網路設備21是否有異常狀況，避免第二收集模組124和第二狀態收集伺服器14有遺漏沒發現的異常狀況，例如當設備離線時，被動監控的方式會無法得知設備狀態。

【0028】 輸出模組18則用以將告警事件提供給一使用者或維修人員觀看。除了告警事件之外，輸出模組18更顯示第一告警通知、第二告警通知及設備22或其它網路設備21之設備狀態提供給使用者觀看，設備狀態包括設備之即時狀態及歷史狀態。

【0029】 請參考第2圖，其為本創作乙太網路協定之監控系統10之細部方塊圖。第一收集模組122更包括一輪詢群組（Poller Group）123，提供了橫向的效能擴充，因此可應對更大量的設備22及其它網路設備21。第一狀態收集伺服器12更包括一第一資料庫126，其連接第一收集模組122及第二收集模組124，第一資料庫126為基於分散式儲存的資料庫集群（MySQL Cluster），用以儲存第一收集模組122及第二收集模組124所收集之設備狀態、第一告警通知和SNMP_Trap告警通知。第二狀態收集伺服器14包括一搜尋和數據分析引擎集群（Elasticsearch Cluster）142及一第二資料庫144，其中，搜尋和數據分析引擎集群142用以對Syslog資料進行解析，將Syslog資料和偵錯條件進行比對（例如判斷Syslog資料中是否含有error的字眼），若有則發出第二告警通知。第二資料庫144為基於分散式儲存的資料庫集群（MongoDB Cluster），用以儲存設備22及其它網路設備21的Syslog資料，由於搜尋和數據分析引擎集群142及資料庫集群皆為多台主機所組成的集群，因此亦提供了橫向效能擴充的功能以應對大量的設備22及其它網路設備21。整合模組16更包括一第三資料庫162，此第三資料庫162為Microsoft SQL資料庫。輸出模組18更包括一第四資料庫182，此第四資料庫182為MySQL資料庫。第三資料庫162和第四資料庫182皆用以儲存各自所接收到的資料和告警，第三資料庫162還儲存發生符合告警條件的告警事件。

【0030】 使用者利用乙太網路協定之監控系統10進行監控，其監控顯示畫面如第3圖至第5圖所示。第3圖之監控畫面26中顯示發生告警事件的數量，並列出發生告警事件的設備編號。其中，ACS Hub、Core Hub屬於第1圖中的連接埠裝置23，下面顯示的數字為離線設備數量；ZCU97、ZCU98、AP26皆代表由設備22所組成的其中一個環（群組名稱），下面的數字為該環中的設備離線數量。第4圖的監控畫面26表示兩個核心集線器（core hub）和一個Cisco安全控制伺服器（ACS hub），這三台設備皆正常運作中，而第4圖的監控畫面26下方則列出85個設備22的設備狀態（包括UP、Warning或Down）。接著如第5圖所示，其為歷史事件查詢，進一步可在監控畫面26左邊欄位設定查詢條件後，於右邊欄位列出事件處理明細，包括事件等級、事件發生時間、設備IP位置、處理狀態、結案與否等等，便於讓使用者或維修人員一目了然。

【0031】 綜上所述，本創作所提供之乙太網路協定之監控系統，其利用包含SNMP Poller、SNMP Trap和Syslog等多種不同的通訊協定互相互補以監控環狀網路中的設備狀態，以避免當設備發生微小的異常狀態時被監控系統忽視，從而造成停機維修的困境。

【0032】 唯以上所述者，僅為本創作之較佳實施例而已，並非用來限定本創作實施之範圍。故即凡依本創作申請範圍所述之特徵及精神所為之均等變化或修飾，均應包括於本創作之申請專利範圍內。

【符號說明】

【0033】

10:乙太網路協定之監控系統

12:第一狀態收集伺服器

122:第一收集模組

124:第二收集模組

126:第一資料庫

14:第二狀態收集伺服器

142:搜尋和數據分析引擎集群

144:第二資料庫

16:整合模組

162:第三資料庫

18:輸出模組

182:第四資料庫

20:環狀網路

21:其它網路設備

22:設備

23:連接埠裝置

26:監控畫面

【新型申請專利範圍】

【請求項1】 一種乙太網路協定之監控系統，其應用於監控一環狀網路中的複數設備，該乙太網路協定之監控系統包括：

一第一狀態收集伺服器，包括一第一收集模組及一第二收集模組，該第一收集模組及該第二收集模組分別利用主動和被動方式取得該等設備的複數設備狀態，該第一狀態收集伺服器還包括至少一第一告警通知；

一第二狀態收集伺服器，利用一系統紀錄通訊協定（System Logging Protocol, Syslog）服務接收該等設備的複數Syslog資料，並據以產生至少一第二告警通知；

一整合模組，連接該第一狀態收集伺服器及該第二狀態收集伺服器，在該整合模組中設定一告警條件，將該至少一第一告警通知、該至少一第二告警通知與該告警條件進行比對，判斷該等設備是否有一告警事件發生；以及一輸出模組，連接該整合模組，將該告警事件提供給一使用者觀看。

【請求項2】 如請求項1所述之乙太網路協定之監控系統，其中該第一狀態收集伺服器係利用簡單網路管理協定（Simple Network Management Protocol, SNMP）進行資料收集與告警。

【請求項3】 如請求項2所述之乙太網路協定之監控系統，其中該第一收集模組係設定一偵錯條件，利用簡單網路管理協定對該等設備進行發現（discover）及輪詢（polling），當該等設備狀態中出現符合該偵錯條

件的事件時，該第一收集模組主動從該環狀網路中撈取該事件並產生該至少一第一告警通知。

【請求項4】 如請求項2所述之乙太網路協定之監控系統，其中該第一收集模組更包括一輪詢群組（Poller Group），以擴充可收集之該等設備狀態的該等設備之數量。

【請求項5】 如請求項1所述之乙太網路協定之監控系統，其中該第二收集模組係設定一偵錯條件，且該等設備利用一簡單網路管理協定陷阱服務（SNMP Trap Service）自動送出一SNMP_Trap訊息給該第二收集模組，由該第二收集模組依據該偵錯條件對該SNMP_Trap訊息進行解析，並產生一SNMP_Trap告警通知。

【請求項6】 如請求項1所述之乙太網路協定之監控系統，其中該第一狀態收集伺服器更包括一第一資料庫，該第一資料庫連接該第一收集模組及該第二收集模組，用以儲存該第一收集模組及該第二收集模組所收集之該等設備狀態及該至少一第一告警通知，該第一資料庫為基於分散式儲存的資料庫集群（MySQL Cluster）。

【請求項7】 如請求項1所述之乙太網路協定之監控系統，其中該第二狀態收集伺服器包括一搜尋和數據分析引擎集群（Elasticsearch Cluster），用以對該等Syslog資料進行解析。

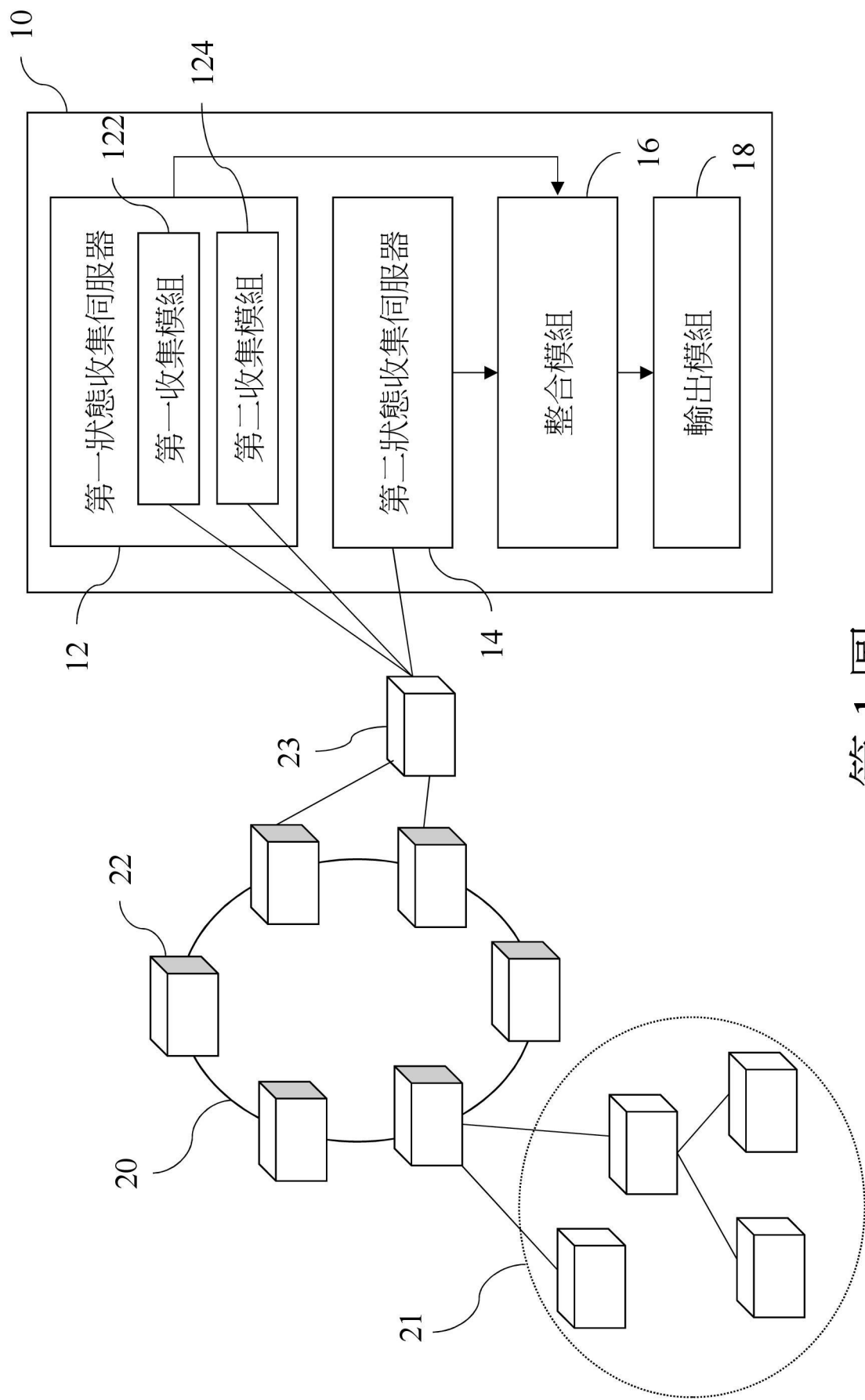
【請求項8】 如請求項1所述之乙太網路協定之監控系統，其中該第二狀態收集伺服器包括一第二資料庫，該第二資料庫為基於分散式儲存的資料庫集群（MongoDB Cluster），儲存該等設備的該等Syslog資料。

【請求項9】 如請求項1所述之乙太網路協定之監控系統，其中該輸出模組更顯示該至少一第一告警通知、該至少一第二告警通知及該等設備之該等設備狀態提供給該使用者觀看，該等設備狀態包括該等設備之即時狀態及歷史狀態。

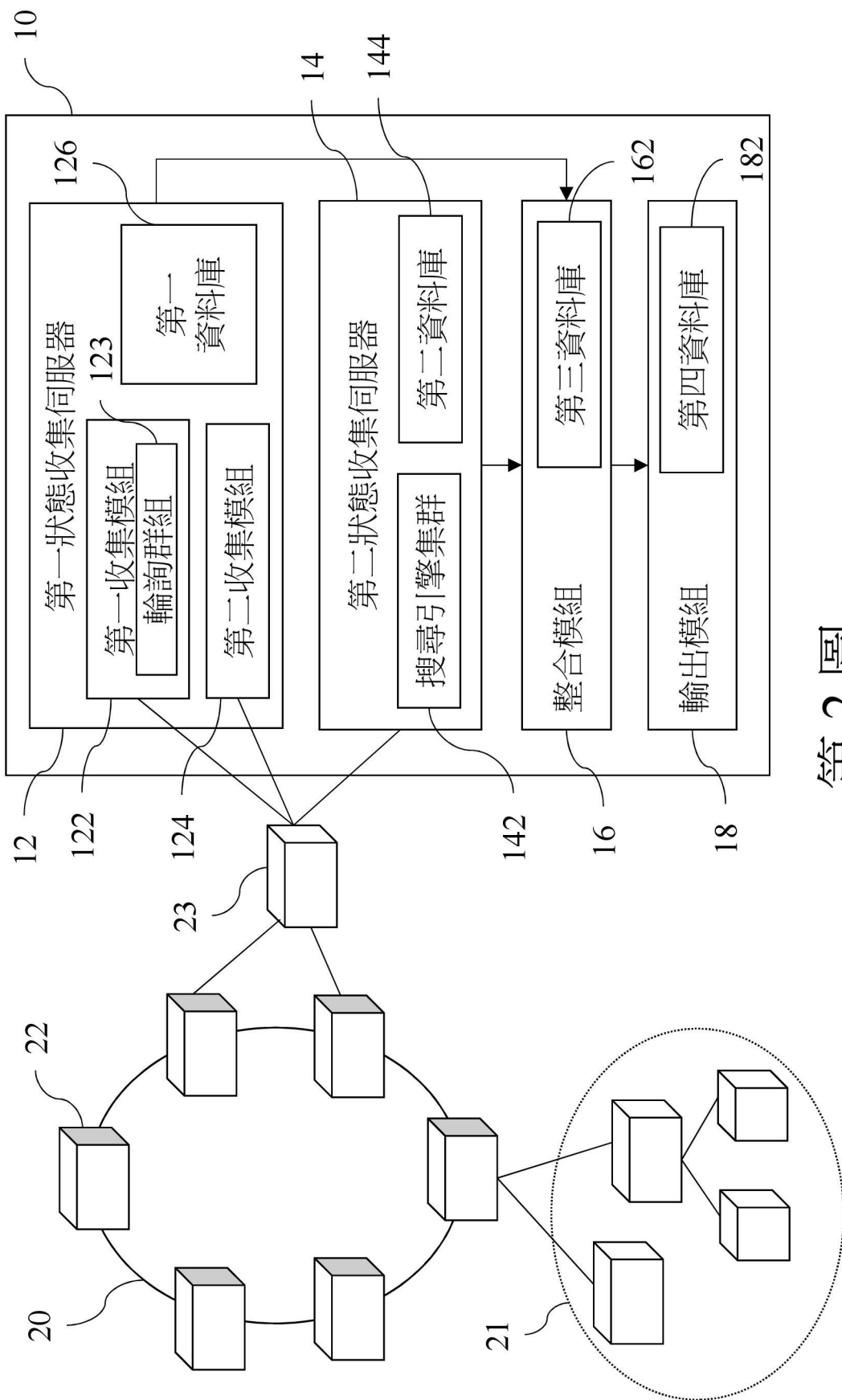
【請求項10】 如請求項1所述之乙太網路協定之監控系統，其中該整合模組更包括一第三資料庫，該第三資料庫為Microsoft SQL資料庫。

【請求項11】 如請求項1所述之乙太網路協定之監控系統，其中該輸出模組更包括一第四資料庫，該第四資料庫為MySQL資料庫。

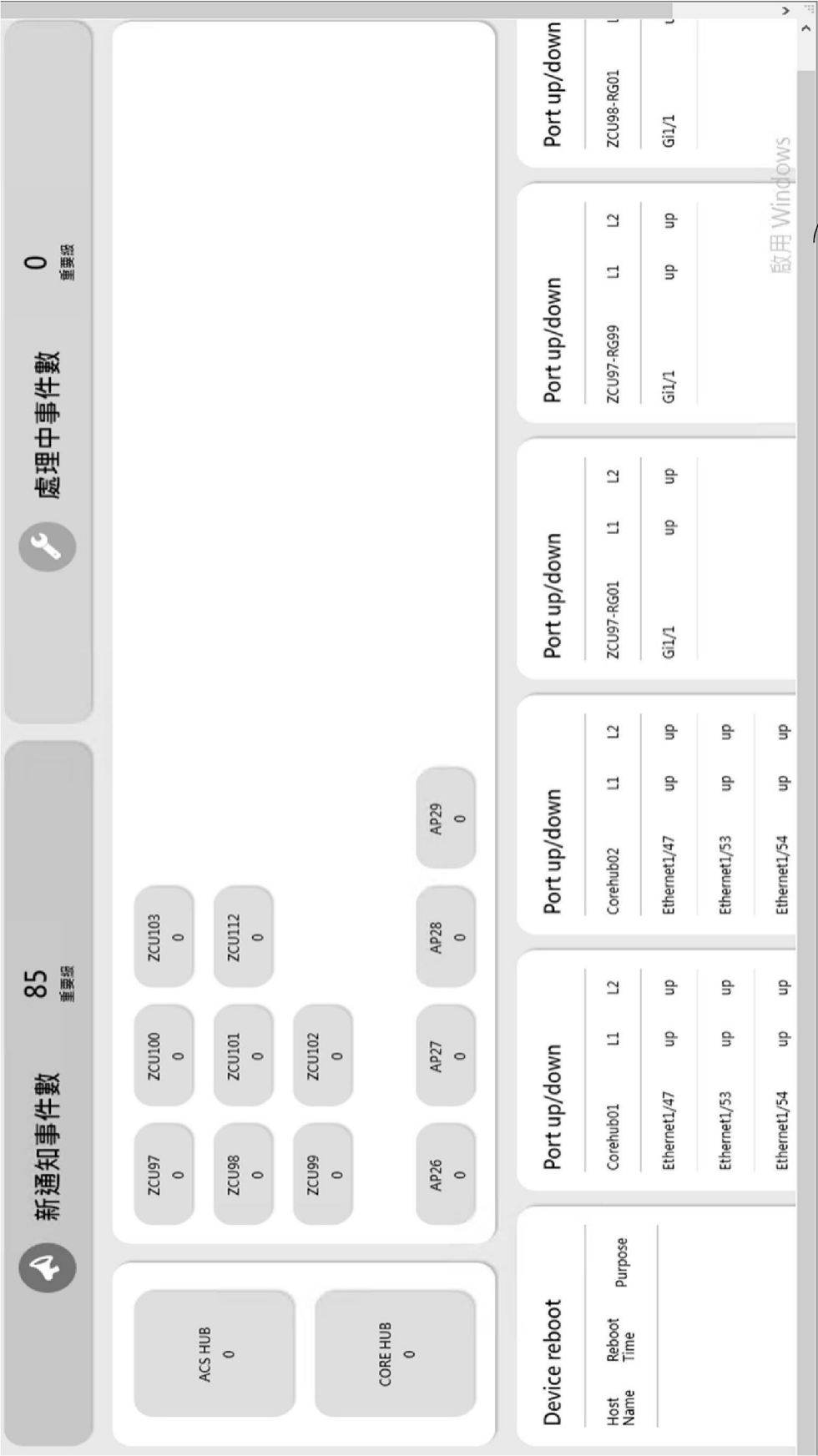
【新型圖式】



第 1 圖



第 2 圖



第 3 圖 26



三 歷史事件查詢

設定查詢條件

服務狀態

未結束

事件時間

起始日

截止日

事件等級

☒ Critical ☒ Major

☒ Minor ☐ Warning

☐ Info

查詢

事件處理明細

批次確認

批次結束

輸入關鍵字搜尋

事件等級	事件時間 Case ID	Hostname IP	服務需求	處理狀態	確認	結果	詳細內容
☐ Critical	2023/11/30 20:15 GS23110033	corhub01 172.28.1.251	進入全域模式	進行中	確認	結果	
☐ Critical	2023/11/30 11:18 GS23110032	corhub01 172.28.1.251	進入全域模式	進行中	確認	結果	
☐ Major	2023/11/22 12:20 GS23110031	ha-73102 172.28.97.103	進入全域模式	進行中	確認	結果	
☐ Major	2023/11/07 17:54 GS23110030	zcu97-rg99 172.28.113.50	進入全域模式	進行中	確認	結果	
☐ Major	2023/11/07 17:49 GS23110029	hz-73052 172.28.113.53	進入全域模式	進行中	確認	結果	
☐ Major	2023/11/07 17:43 GS23110028	hz-73030 172.28.113.31	進入全域模式	進行中	確認	結果	
☐ Major	2023/11/07 17:43 GS23110027	hz-73003 172.28.113.2	進入全域模式	進行中	確認	結果	

第5圖