智慧網路監測：Zabbix 網路監控與自動修復系統

專題編號：112-CSIE-S003
執行期限：111 年第 1 學期至 112 年第 1 學期
指導教授：郭忠義
專題參與人員： 107590004　　張哲瑋

一、摘要

本專題旨在研發基於 Zabbix 的高效網路監測及自動修復系統，以提高網路運營的效率和可靠性。此系統支援監測多種關鍵設備，包括 Linux、Cisco Router、Switch 等，並能夠擴展至所有支援 SNMP 協議的網路設備。監測項目包括系統運行時間、CPU 負載、記憶體使用率、磁碟使用情況、網路流量，以及各種重要網絡服務的可用性，並將資訊儲存於 MariaDB。

此外，我們的系統具備強大的告警機制，能夠即時通知運營團隊有關任何異常情況，同時避免了重複性告警的困擾。告警通知方式支援 E-Mail、Teams、Line 等主流通訊軟體。最重要的是，我們實現了自動化修復功能，例如在 DDoS 攻擊發生時，系統能夠自動將流量導向至備用伺服器，以確保網路的可用性和安全性，將有助於組織實現高效的網路管理和故障處理。

關鍵詞：Zabbix、簡易網路管理通訊協定(SNMP)、MariaDB、自動化、高可用性、監控系統。

二、緣由與目的

隨著網路規模的不斷擴大和科技的迅速進步，網路已經成為我們生活中不可或缺的一部分。越來越多的服務和業務透過網際網路來實現，網路已經成為企業運營的核心。然而，在這個高度依賴網路的時代，確保網路的高可用性和持續監控變得至關重要。

同時資訊安全攻擊技術不斷演變，網路面臨各種潛在的威脅。因此需要一個強大且智能的監測和管理系統來應對這些挑戰。本系統的核心目標是整合多種監測功能，同時兼容各種不同型號的網路設備，且能夠即時偵測網路異常並以高效的自動化方式採取行動。

這不僅有助於降低因網路服務異常而造成的業務損失，還能夠提高企業運營效率，減少管理成本，並加強整個網路生態系統的安全性。此系統是為了確保網路能夠持續穩定地支援企業的業務需求而設計，是維護現代企業營運的重要工具。

三、研究報告內容

(一) 研究範圍

1. 監測範圍擴展：將監測範圍擴展至不同操作系統（如 Linux、Windows）、網路設備（如 Cisco 路由器）、以及應用服務（如網頁服務、DNS 服務）。
2. 告警策略優化： 研究更精確的告警策略，以減少虛偽警報並提高告警的準確性。
3. 自動修復功能：進一步發展自動修復機制，以涵蓋更多的異常場景和修復操作。

(二) 使用技術方法

1. Zabbix 監測平台：Zabbix 是一個開源的監測和警報系統，具有卓越的靈活性和可擴展性。它用於實現資訊的收集、網路監測、告警管理和數據視覺化。Zabbix 提供了豐富的模板和插件，可用於不同種類的監測需求，使我們能夠全面監控各種設備和服務。
2. SNMP 協議：簡單網路管理協議（SNMP）是一個標準的網路監測協議，用於從各種網路設備中獲取資訊。我們使用 SNMP 協議來實現從不同設備和服務中的資訊收集，包括系統運行時間、網路流量、CPU 負載、

記憶體使用情況等。

3. MariaDB：MariaDB 是一個高度穩定和可擴展的關聯式資料庫管理系統，用於儲存收集到的監測數據，確保可靠的資料儲存和可擴展性，並支援高效的資料檢索和分析。
4. 自動化腳本：使用自動化腳本來實現自動修復功能，例如使用 shell 編寫自動化腳本，以應對不同類型的網路異常事件。

(三) 架構流程

1. 新增監控設備與建立監控模板： 在系統建置階段，首先要新增監控的設備和服務，同時建立相應的監控模板。包括了監測項目的定義、告警閾值和觸發條件。這一步驟確保了系統能夠有效地監測多種設備和服務。
2. 資訊收集：使用 SNMP 協議從各種設備和服務中收集資訊，這些資訊包含系統運行時間、CPU 負載、記憶體使用、磁碟空間、網路流量等。
3. 資料儲存：監測數據被儲存到 MariaDB 資料庫中，以支援後續的數據分析和查詢。MariaDB 提供了可靠的資料儲存和高效的數據管理功能，確保資料的安全性和可擴展性。
4. 數據呈現：監測數據以視覺化的方式呈現在儀表板上，來創建互動性強、易於理解的監測報告。這使運營團隊能夠即時檢視網路性能和當前狀態。
5. 告警機制：基於收集到的資訊實施強大的告警管理機制，當監測數據超出預定閾值或滿足其他告警條件時，立即觸發告警通知。告警通知可以通過 E-Mail、Teams、Line 等多種通訊工具發送給適當的運營人員，以確保即時響應異常
6. 自動修復：當系統偵測到異常事件時，自動修復機制將被啟動。這一步驟涉及使用 Shell 腳本自動執行修復操作，例如在網路介面流量過高時，自動導流至備用伺服器。這能夠迅速恢復正常運作，降低業務中斷時間。

(四) 實驗結果

1. 監測和告警測試：我們成功設定了監測項目和告警閾值，並模擬了多種異常情況，包括高流量、CPU 過載等。系統能夠迅速偵測到這些異常事件並生成告警通知，通知運營人員採取必要的行動。
2. 自動修復測試：進行了自動修復機制的測試，例如當網路介面流量超過預定閾值時，系統能夠自動導流至備用伺服器。這些測試顯示系統能夠有效地恢復正常運作，降低了業務中斷時間。
3. 數據可視化測試：比較設備資訊並透過儀表板呈現監測數據的視覺化報告。這使運營團隊能夠輕鬆地監視網路性能和異常狀態，並采取適當的措施。

(五) 結論

一個高效的監控系統能提高運營效率，及時偵測問題並迅速解決，減少業務中斷損失。技術挑戰包括大規模設備管理，兼顧安全，以及告警機制的細微調整，需要耗費大量時間。自動化修復機制的設計需要考慮方便性，並根據不同環境和服務進行調整。未來，我們希望這系統能適用於企業環境，融入 AI 技術實現異常預測，並整合 NetFlow 分析，提前預知問題，提高效率和安全性。

參考文獻

[1] Zabbix - Real-time monitoring of IT components and services
https://www.zabbix.com/
[2] THE A TO ZABBIX OF TRAPPING & POLLING
https://netquirks.co.uk/2018/06/19/the-a-to-zabbix-of-trapping-polling/
[3] A Simple Network Management Protocol (SNMP)
https://www.rfc-editor.org/rfc/rfc1157
[4] VRRR Version 3 for IPv4 and IPv6
https://datatracker.ietf.org/doc/html/rfc5798