系統日誌-SYSLOG

壹、 系統日誌-SYSLOG 主要功能

【系統日誌】功能專門用於收集和分析伺服主機的操作系統和應用程序的系統日誌。這個功能主要針對 Linux/Unix 系統的標準 SYSLOG 協議。

對於 Windows 環境，由於其事件日誌的原生格式與 SYSLOG 不兼容，所以需要特殊處理以集成到 Watchdog 的日誌收集機制中。一般解決方案是使用如 Nxlog 等專門的日誌轉發和轉換工具。這些工具能夠讀取 Windows 的事件日誌，並將其轉換為 SYSLOG 協議兼容的格式，然後轉發到 Watchdog 系統進行集中分析和監控。

這個功能的設置和使用涉及對不同作業系統的日誌格式和協議的理解，並可能需要結合第三方工具來實現跨平台的日誌集成。

貳、 系統日誌-SYSLOG 功能設定

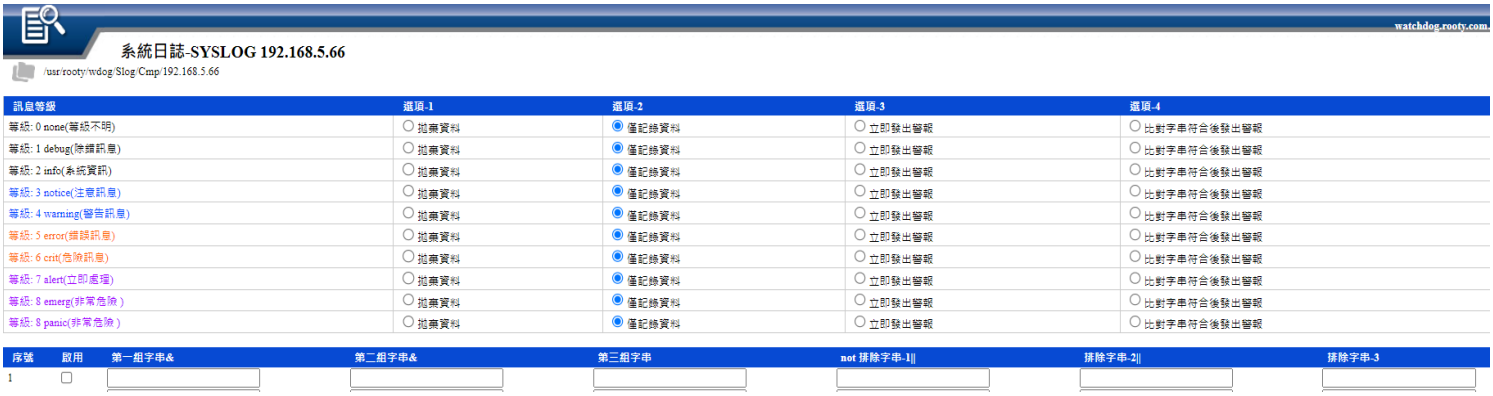
要使用【系統日誌-SYSLOG】功能，涉及兩個主要部分的設定，分別是【Watchdog 系統設定】以及【Client 端日誌轉送設定】

➢ Watchdog 系統設定：

在 Watchdog 系統端，需要進行專門的配置以接收和處理來自客戶端的 SYSLOG 消息。這可以從【偵測名單】→【系統日誌-SYSLOG】來進行設定。在此，您可以定義和管理日誌源、過濾規則、警報條件等，以確保只捕獲和處理感興趣的日誌信息。

進入此配置頁面，僅需輸入 Client 端 IP，由於已經安裝代理程式，系統將自動擷取相關主機資訊。

若有需要進行更進一步的日誌篩選，可以點選【警報條件】



即可進行資料的篩選，若要使用【字串篩選】功能，請參考前面章節【網站偵測】

➢ Client 端日誌轉送設定：

◆ 【Linux SYSLOG 轉送設定】

客戶端的設定是確保適當的系統和應用日誌被轉送到 Watchdog 系統以供分析。這涉及修改特定的日誌轉發配置（例如，Linux 中的/etc/rsyslog.conf 文件），並添加轉發規則以指向 Watchdog 的接收地址和端口。配置可能會因客戶端的作業系統和日誌管理系統的不同而有所不同。

在 Linux 作業系統中，系統和應用程序的日誌通常由 syslog 協議來管理。若要將這些日誌轉送到特定的主機，必須修改 rsyslog 的配置。

一、**編輯 rsyslog 配置文件**

rsyslog 配置文件通常位於/etc/rsyslog.conf，或者在/etc/rsyslog.d/目錄下的某個文件。

二、**添加轉發規則**

在配置文件的合適位置添加以下行：【*.* @192.168.5.148:514】

這行代表所有設施和優先級的日誌都將通過 UDP 協議傳送 192.168.5.148 的 514 port。

※若要使用 TCP，請先確保 Watchdog 主機的作業系統有開啟 TCP syslog 服務，可以使用指令【netstat -tuln | grep 514】 查看

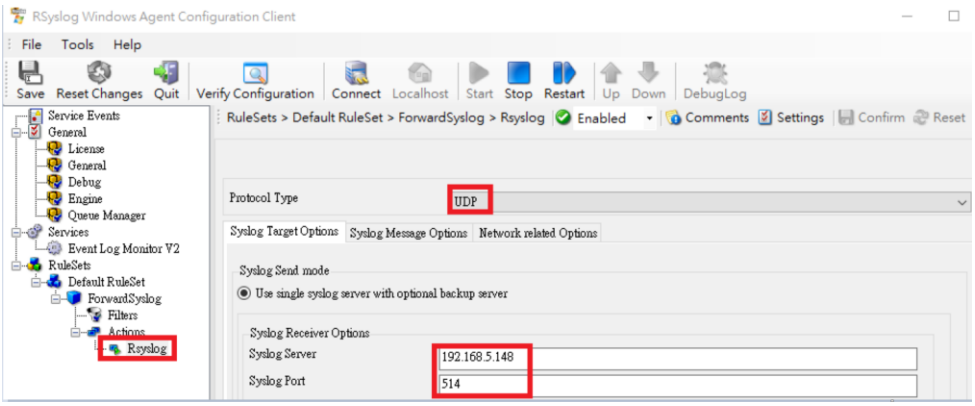
三、**重啟 rsyslog 服務**

輸入指令【 systemctl restart rsyslog】

◆ 【Windows 轉送設定】

由於 Watchdog 系統專為 Linux-Syslog 格式設計，若需整合 Windows 事件日誌，您必須首先在 Windows 環境中將其轉換為 Syslog 標準格式。此轉換可以透過諸如 nxlog 或 Rsyslog 等第三方軟體工具達成。一旦日誌被轉送至 Watchdog 主機，系統將自動解析和分類這些日誌，並將其整合到【偵測狀態】的【系統日誌-SYSLOG】中。

例如:使用 Rsyslog Windows Agent，設定使用 UDP / 514 port，並將日誌轉送到 Watchdog 主機 192.168.5.148 中



Watchdog 主機收到資料後，系統會整合到【偵測狀態】的【系統日誌-SYSLOG】中

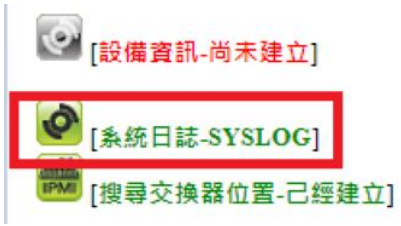
※若要使用 TCP，請先確保 Watchdog 主機的作業系統有開啟 TCP syslog 服務，可以使用指令【netstat -tuln | grep 514】 查看

參、　系統日誌-SYSLOG 狀態查看

若要查看系統日誌，可以從【偵測狀態】→【系統日誌-SYSLOG】查看

選擇要查看系統日誌之主機

選擇【系統日誌-SYSLOG】



接著選擇日期，即可查看收到的系統日誌內容

系統日誌-SYSLOG 192.168.5.81[localhost.localdomain] (20230804)

/home/hrooty/Slog/192.168.5.81/2023/20230804

警報	序號	訊息時間	主機或設備位址	訊息程式	訊息類型	訊息等級	等級說明	訊息內容
	1	2023/08/04 16:25:42	192.168.5.81	sudo	authpriv	info	系統資訊	pam_unix(sudo:session): session closed for user root
	2	2023/08/04 16:25:42	192.168.5.81	sudo	authpriv	info	系統資訊	pam_unix(sudo:session): session closed for user root
	3	2023/08/04 16:26:03	192.168.5.81	polkitd	authpriv	notice	注意訊息	Unregistered Authentication Agent for unix-process:2
	4	2023/08/04 16:26:03	192.168.5.81	polkitd	authpriv	notice	注意訊息	Unregistered Authentication Agent for unix-process:2
	5	2023/08/04 16:26:03	192.168.5.81	systemd	daemon	info	系統資訊	Started System Logging Service.