排程資訊 / 事件日誌

Watchdog 系統的【排程資訊】功能實際上是一種進程管理和監控機制。根據預定的時間表自動執行一系列的程式或腳本，從而實現對系統狀態的持續監控，或是對事件日誌的定期收集。

可以將【排程資訊】視為一種行程表或工作流程，其中包含了一系列的預設任務（例如「行程 1」、「行程 2」、「行程 3」）。
每一個「行程」都對應一個由 Watchdog 提供的程式，這些程式可能是收集事件日誌、硬碟資訊等。而在每個「行程」完成後，系統可以選擇進一步利用 Watchdog 提供的其他程式對產生的結果進行後續處理或篩選。

【排程資訊】的設定可在兩個位置進行。
分別是

- 【偵測名單→排程資訊(Watchdog 本機)】
- 【偵測名單→伺服主機→偵測放大鏡→排程資訊】

選擇何處設定主要取決於希望運行的排程資訊在哪台伺服器上取得資訊並對其做處理。

例如，如果目標是收集特定伺服器（如 192.168.1.1）的事件日誌，就應該在該伺服器上的【偵測放大鏡】選項中設定【排程資訊】。

【排程資訊】有下列主要功能

- 收集記錄
- 由記錄中檢查符合警報條件之字串，發出警報
- 由後製程式處理分析每次收集之記錄 (依功能製作)

壹、 排程資訊設定欄位說明

資訊名稱(英文數字)	使用程式	程式選項或檔案名稱
eveid-462	eveid-4624.bat	
4720	eveid-4720.bat	
4726	eveid-4726.bat	
4723	eveid-4723.bat	
4724	eveid-4724.bat	

【資訊名稱】
可自行定義該資訊名稱，方便查看該行欄位作用與目的，僅可使用小寫英文與數字，若使用大寫會自行轉換成小寫

【使用程式】
定時執行的程式或 sehll script 如 powershell、ls 等，此處多為 Watchdog 系統提供之程式。

Watchdog 系統目前提供的程式如:

- eveid-4625.bat 事件 ID:4625 帳戶無法登入
- eveid-4672.bat 事件 ID:4672 特殊權限已指派給新登入
- eveid-4720.bat 事件 ID:4720 已建立使用者帳戶
- eveid-4726.bat 事件 ID:4726 已刪除使用者帳戶
- eveid-4723.bat 事件 ID:4723 嘗試變更帳戶的密碼
- eveid-4724.bat 事件 ID:4724 嘗試重設帳戶的密碼
- eveid-4732.bat 事件 ID:4732 新增成員至本機群組
- eveid-4733.bat 事件 ID:4733 本機群組中移除成員
- eveid-4756.bat 事件 ID:4756 新增成員至全域群組
- eveid-4757.bat 事件 ID:4757 全域群組中移除成員
- wevelog.bat / 通用型 需在【程式選項或檔案名稱】輸入事件 ID

其他提供之程式如:
指定事件群組名稱但事件 ID 為選項之其他程式 如:

- wevelog-sys.bat (程式內指定 -LogName System)
- wevelog-app.bat (程式內指定 -LogName Application)
- wevelog-sec.bat (程式內指定 -LogName Security)

程式內容 如: wevelog-**app**.bat
Get-EventLog -LogName **Application** -InstanceID %1 -After (Get-Date).AddMinutes(-60) | Format-list

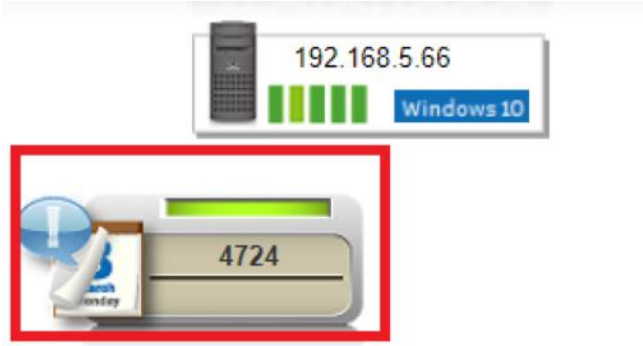
【程式選項或檔案名稱】
定時執行的程式之選項或者本文檔位置(Full Path)

執行時間(分)	長度限制(MB)	保留筆數	警報	後製程式
60	5	55		wdogs_moj_event
60	5	55		wdogs_moj_event
60	5	55		wdogs_moj_event
60	5	55		wdogs_moj_event
60	5	55		wdogs_moj_event

【執行時間】
設定系統每 N 分鐘執行一次排程資訊的程式執行

【長度限制】
限制輸出檔最大容量

【保留筆數】
指的是保留每一欄排程資訊所執行程式之詳細資料最大筆數
如:



【警報】

點擊此處有兩項作用

1. 利用字串進行前面程式輸出結果之篩選
2. 選擇後製程式對前面程式收集之資料進行處理分析

※字串篩選方式請查閱前面章節【網站偵測功能使用】→【第 N 組字串】、【not 排除字串】

【後製程式】

會自動顯於剛剛於【警報】設定的後製程式名稱

➢ 【範例】

若要使用 Windows Server 的事件日誌 InstanceID 取得紀錄

可在排程資訊輸入

資訊名稱	使用程式	程式選項或檔案名稱	執行時間(分)	長度限制(MB)	保留筆數	警報
eveid-4625	c:\rooty\wdogc\shbin\eveid-4625 備註 A	(不須輸入)	10	5	24	(指定後制程式)
eveid-4720	eveid-4720.bat 備註 B	(不須輸入)	10	5	24	(指定後

資訊名稱	使用程式	程式選項或檔案名稱	執行時間(分)	長度限制(MB)	保留筆數	警報
						制程式)
wlog-4624	wevelog.bat	4624 備註 C	10	5	24	(指定後制程式)

※【使用程式】欄位輸入的格式可以是備註 A(全路徑)或者備註 B(無路徑)，擇一即可
※備註 C:【wevelog.bat】為通用程式，若在【程式選項與檔案名稱】輸入 4720 相當於是於【使用程式】輸入【eveid-4720.bat】

於【警報】欄位輸入

後製程式	識別碼	報表名稱
wdogs_sch_event	4625	id4625

系統便會依序執行程式【eveid-4625】→【eveid-4720】→【wlog-4624】
接著再經由後製程式【wdogs_sch_event】處理，產生報表【id4625】

➢ 【實際使用範例】

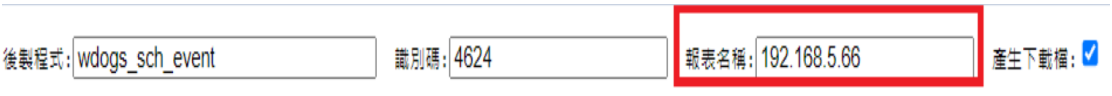
- **【同一 IP，將多個識別碼整合成一張報表】**

在一份報表中，集中呈現某一特定 IP 的多種識別碼（Instance ID）資訊

在設定完要取得的事件 ID 之後

資訊名稱(英文數字)	使用程式
eveid-462	eveid-4624.bat
4720	eveid-4720.bat
4726	eveid-4726.bat
4723	eveid-4723.bat
4724	eveid-4724.bat

在每一個【使用程式】後面的【報表】設定，將所有後製程式的**【報表名稱】設定為同名**，系統則會處理完資料後將其彙整在同一張報表上，建議使用【本機的 IP 名稱】方便在查詢的時候好辨識

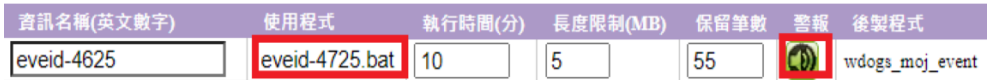


- **【不同 IP，將同一個識別碼整合成一張報表】**

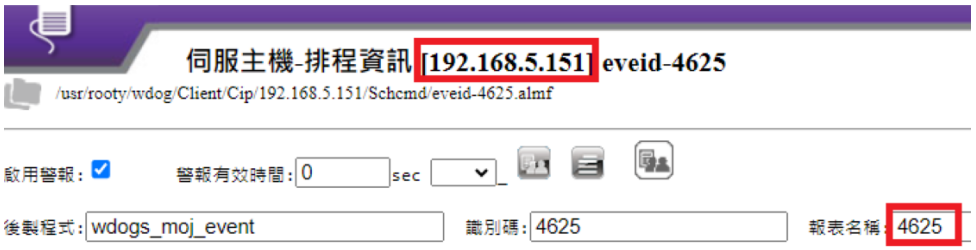
在一份報表中，集中展示特定實例識別碼（Instance ID）下的各種 IP
在設定完要取得的事件 ID 之後

在每一個【使用程式】後面的【警報】設定，
1.選擇後製程式【wdogs_moj_event】
2.將不同主機同欄位的**【報表名稱】設定為同名**，建議使用【事件日誌 ID】方便在查詢的時候好辨識
例如:
要將 192.168.5.151 以及 192.168.5.66 兩台主機之事件 ID4625 整合在一起

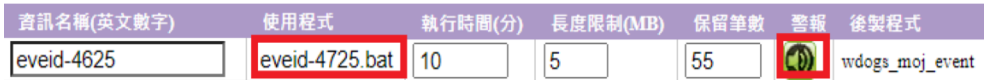
在 192.168.5.151 主機之【排程資訊】，點選【eveid-4725.bat】後方的【警報】



並設定報表名稱為【4625(可自行定義)】



在 192.168.5.66 主機之【排程資訊】，點選【eveid-4725.bat】後方的【警報】



設定報表名稱，報表名稱需與上面設定一致【4625】

系統抓取同樣的報表名稱後，即會整合為一張報表

貳、　查看事件日誌報表

➢ 查看事件日誌報表

接著可於資訊查詢【偵測狀態】→【windows 事件日誌查詢/下載】查看取得之事件日誌

點擊要查看的檔名即可查看內容，內容記錄時間、事件時間、事件識別碼、訊息、帳戶名稱、帳戶網域、工作站名稱、來源網路位址等

➢ 查看識別碼詳細資料

若要查看各別識別碼詳細資料可點擊【偵測狀態】→【伺服器效能與資訊】

接著選擇要查看的 AD server ，並選擇【排程資訊】

選擇要詳細查看的事件識別碼，上面的名稱為排程資訊設定時自定義的【資訊名稱】

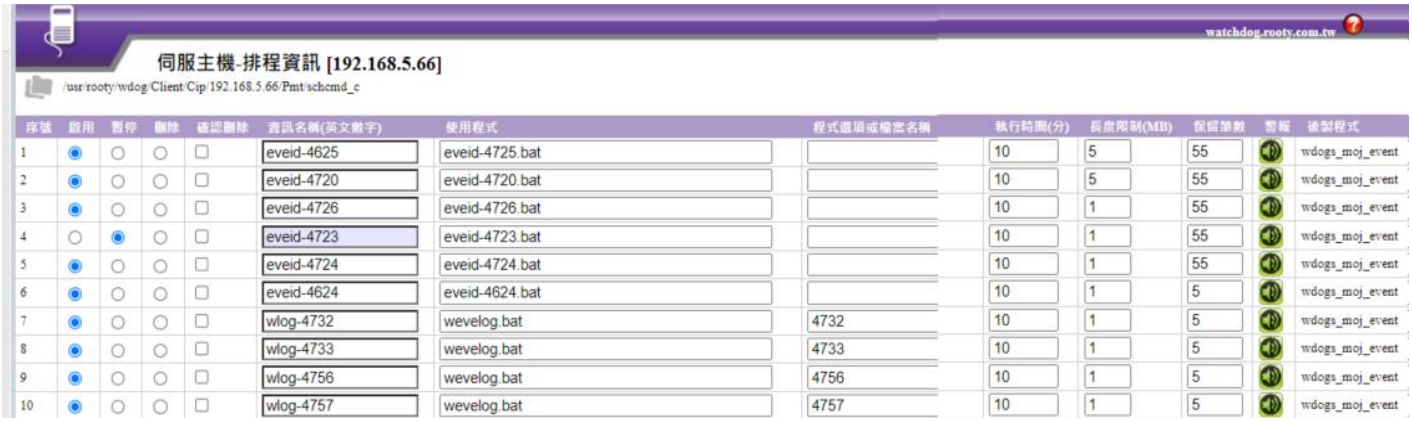
進入要查看詳情的識別碼後，點擊【排程回報-明細紀錄】即可查看

※裡面保存的資料最多筆數為排程資訊設定中的【保留筆數】

參、　大量複製設定檔 / Windows 專用

如果需要在大量的 Windows 伺服器上監控事件日誌，一個有效的方法是使用 Watchdog 系統的插件程式來複製設定檔。可以降低手動設定每一台伺服器的工作量，並確保在所有伺服器上的監控設定的一致性。
首先，在一台選定的 Windows 主機上，建立原始設定檔。
在這個設定檔中須設定所有你希望在所有伺服器上監控的事件日誌。
當原始設定檔準備好後，可以使用 Watchdog 的套件程式來自動地複製這個設定檔到所有其他的 Windows 伺服器。

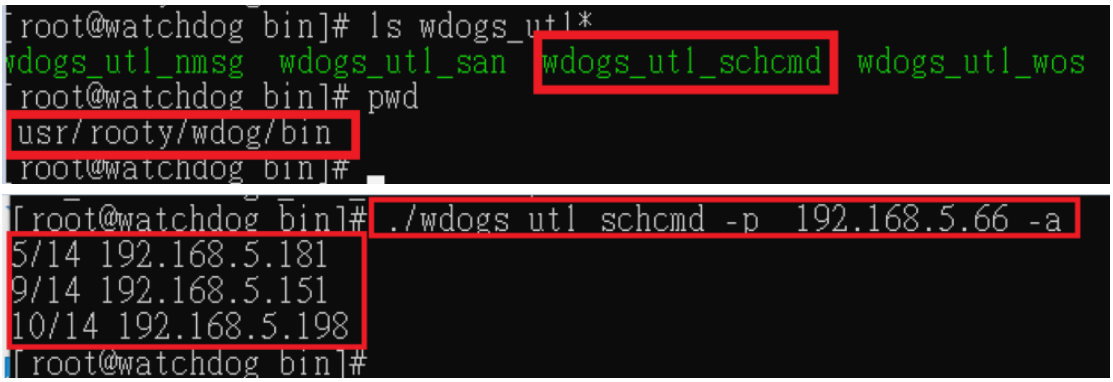
例如：
設定 192.168.5.66 裡的排程資訊【資訊名稱】、【使用程式】、【警報(後製程式)】



序號	啟用	暫停	刪除	確認刪除	資訊名稱(英文數字)	使用程式	程式選項或檔案名稱	執行時間(分)	長度限制(MB)	保留筆數	警報	後製程式
1	◉	○	○	☐	eveid-4625	eveid-4725.bat		10	5	55		wdogs_moj_event
2	◉	○	○	☐	eveid-4720	eveid-4720.bat		10	5	55		wdogs_moj_event
3	◉	○	○	☐	eveid-4726	eveid-4726.bat		10	1	55		wdogs_moj_event
4	○	◉	○	☐	eveid-4723	eveid-4723.bat		10	1	55		wdogs_moj_event
5	◉	○	○	☐	eveid-4724	eveid-4724.bat		10	1	55		wdogs_moj_event
6	◉	○	○	☐	eveid-4624	eveid-4624.bat		10	1	5		wdogs_moj_event
7	◉	○	○	☐	wlog-4732	wevelog.bat	4732	10	1	5		wdogs_moj_event
8	◉	○	○	☐	wlog-4733	wevelog.bat	4733	10	1	5		wdogs_moj_event
9	◉	○	○	☐	wlog-4756	wevelog.bat	4756	10	1	5		wdogs_moj_event
10	◉	○	○	☐	wlog-4757	wevelog.bat	4757	10	1	5		wdogs_moj_event

接著使用 SSH 連進去 Watchdog 本機，並進入/usr/rooty/wdog/bin

執行 Watchdog 本機裡面的 wdogs_utl_schcmd 程式
如:
./wdogs_utl_schcmd –p 192.168.5.66 –a
(輸入剛設定好排程資訊的主機 IP，並加上參數【-a】代表複製到全部的 Windows)



底下的 192.168.5.181、192.168.5.151、192.168.5.198 則是顯示設定檔被複製成功的 Windows 主機

※以上方法僅適用於第一次套用設定，若有新增 Windows 主機欲使用同樣排程資訊之設定檔，切勿在輸入一次指令【./wdogs_utl_schcmd –p 192.168.5.66 –a】，否則有可能會造成系統混亂

若有新增 Windows 主機欲使用同樣排程資訊設定檔

可以使用指令

【./wdogs_utl_schcmd –p 192.168.5.66 –d 192.168.5.198】

192.168.5.66 是原始設定檔的主機 IP，192.168.5.198 則是你想要複製過去設定檔的新主機 IP

※抓取不到資料

如果在 Windows 伺服器的【排程資訊】中找不到對應的事件 ID 的資料（即顯示為空白），或遲遲未產生【Windows 事件日誌】報表，這可能是因為某些設定錯誤或不一致所導致。
在這種情況下，首先需要做的就是檢查【使用程式】和【程式選項或檔案名稱】的設定是否正確。

例如，如果【使用程式】中輸入的是【eveid-4624.bat】，而在【警報】的【識別碼】中輸入的是【4625】，則系統會無法找到對應的事件，因為它們不一致。在這種情況下，你需要確保這兩個設定是一致的。

另外，即使你的伺服器尚未產生該事件 ID，你在【排程回報-明細紀錄】中仍然應該可以看到對應的搜尋結果，而不應該顯示為空白。如果你看到的是空白，這可能表示你的監控設定存在問題，需要優先檢查並修正。
如: