使用代理故障排除工具排除Windows代理故障

目錄

簡介

本文檔介紹如何使用內建的代理故障排除工具PowerShell指令碼解決常見的Windows代理問題。

必要條件

需求

本文件沒有特定需求。

採用元件

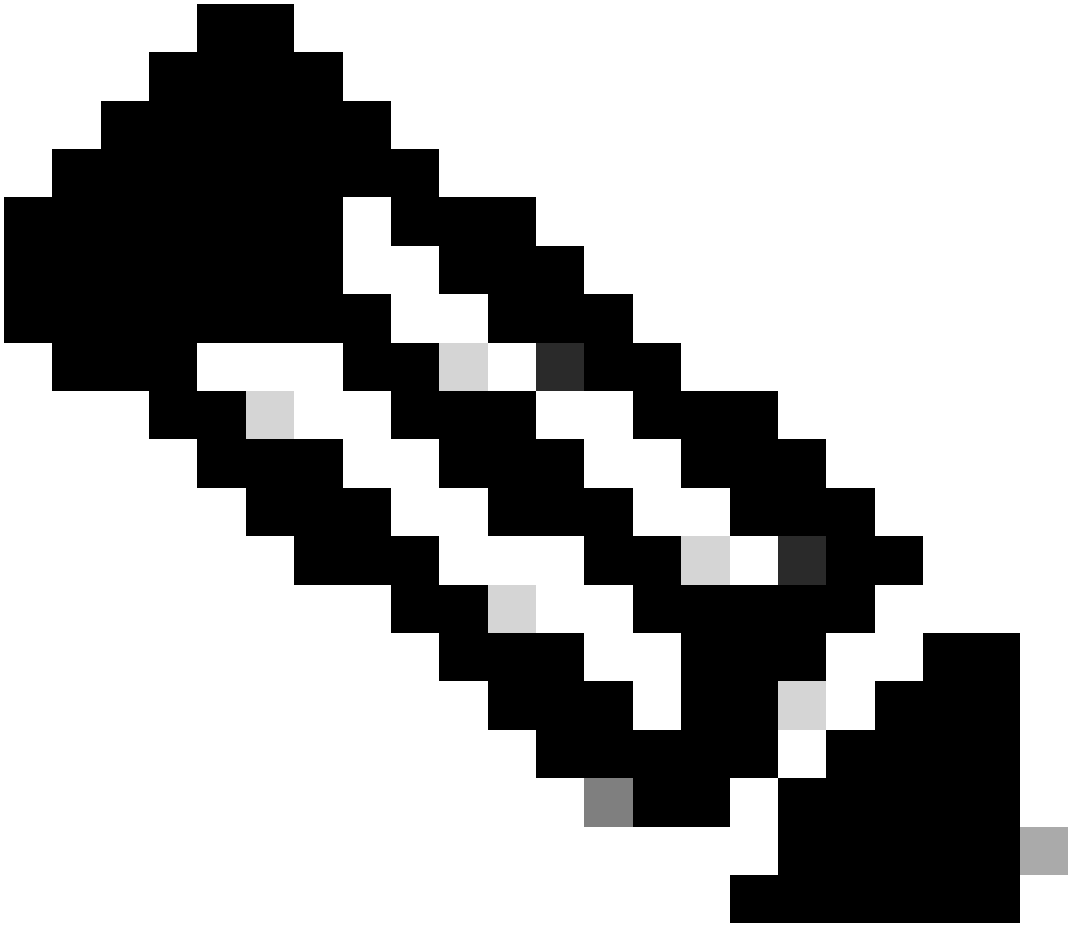
本文中的資訊係根據以下軟體和硬體版本：

- PowerShell版本4.0

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

代理疑難解答工具指令碼附帶多個選項，允許您檢查代理的整體運行狀況、代理註冊方面的已知問題、代理升級方面的已知問題、檢查整體實施運行狀況，以及收集日誌以進行進一步分析。



附註：代理故障排除工具隨3.9版開始的代理一起提供。對於3.9版以前的版本，預設情況下不包括。如果您使用的是3.9之前的版本，您可以從安裝了3.9代理的Windows電腦複製指令碼，然後將其貼上到(C:\Program Files\Cisco Tetration)中，以便使用故障排除工具。

運行指令碼的步驟

要運行Agent故障排除工具指令碼，請執行以下步驟：

1.以管理員身份開啟PowerShell。

2.導航到CSW安裝目錄(預設位置：C:\ Program Files \Cisco Tetration)。

3.使用以下命令運行指令碼：

.\AgentTroubleshootingTool.psl

此代理疑難解答工具指令碼中可用的引數清單

代理程式故障排除工具附帶多個選項，允許您對代理程式的不同方面進行故障排除。
以下是可用選項：

-agentHealth:運行代理運行狀況報告
-agentRegistration:檢查代理註冊中的問題
-agentUpgrade:檢查代理升級問題
-enforcement健康狀況：檢查執行問題
-collectLog:收集調試日誌
-collectDebugLog:收集已啟用loglevel:5的日誌。這包括使用引數 — collectLogs收集的日誌
-all:運行除 — collectDebugLogs之外的所有引數

要使用這些選項中的任何一個，只需使用適當的引數運行指令碼。
例如，要檢查代理的運行狀況，請使用 — agentHealth引數運行指令碼：

.\AgentTroubleshootingTool.ps1 -agentHealth

引數詳細資訊 — agentHealth

在 — agentHealth引數下，您正在檢查以下內容：

1. 服務TetSensor和TetEnforcer處於運行狀態。
2. 感測器ID有效
3. PATH變數包含「C:\ Windows\System32」
4. 代理正在使用ETW或NPCAP。如果作業系統是2008R2，則您正在檢查NPCAP運行狀況。

與收集器/EFE和WSS的後端連線良好。

以下是使用 — agentHealth運行指令碼時指令碼輸出的示例 參數

.\AgentTroubleshootingTool.ps1 -agentHealth

```
PS C:\Program Files\Cisco Tetration> .\AgentTroubleshootingTool.ps1 -agentHealth
***Running Checks for Agent Health at 08/07/2023 13:55:01***
Service status is Good!
Sensor ID is Valid
PATH variable contains 'C:\Windows\System32'
Agent is using ETW for packet capture.
Backend connectivity to Collectors/EFE's and WSS is Good
!!!Agent Health is Good!!!
```

引數詳細資訊 — agentRegistration

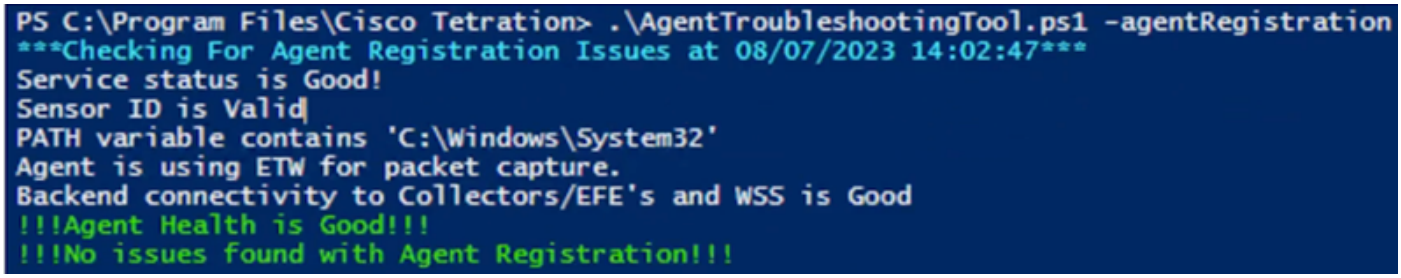
在 — agentRegistration引數下，將檢查以下內容：

1. 它包括使用引數 — agentHealth收集的報告。
2. 註冊錯誤基於錯誤代碼，例如401/403和其他代碼。

如果錯誤地從UI中刪除了代理，還提供一個選項，用於在群集中重新註冊代理。

以下是使用-agentRegistration運行指令碼時的指令碼輸出示例 參數.

.\AgentTroubleshootingTool.ps1 -agentRegistration



引數詳細資訊 — agentUpgrade

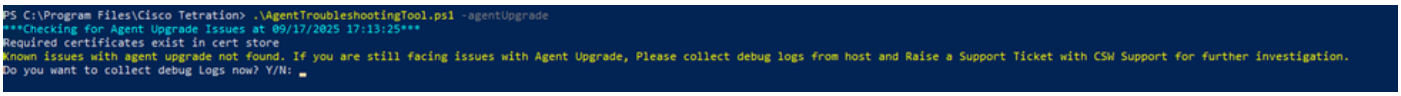
在 — agentUpgrade引數下，您正在檢查以下內容：

1. 商店中提供了所需的證書。
2. MSI快取可在C:\ Windows \Installer資料夾。

如果未發現已知問題，但代理升級仍失敗，則提供收集調試日誌的選項，以便進行進一步的故障排除。

以下是使用 — agentUpgrade運行時指令碼輸出的示例 參數

.\AgentTroubleshootingTool.ps1 -agentUpgrade



引數詳細資訊 — enforcementHealth

在 — enforcementHealth引數下，您正在檢查以下內容：

1. 啟用或禁用實施。
2. 啟用了哪種實施模式。
3. 已將CSW規則編入WAF，或將WFP過濾器編入WAF。

4. CSW WFP篩選器不存在（當模式為WAF時）。
5. CSW WAF規則不存在（當模式為WFP時）。

第4步和第5步是確定在切換實施模式時出現的問題。

以下是使用 — enforcementHealth運行指令碼時的指令碼輸出示例 參數.

.\AgentTroubleshootingTool.ps1 -enforcementHealth

```
PS C:\Program Files\Cisco Tetration> .\AgentTroubleshootingTool.ps1 -enforcementHealth
***Running Enforcement Checks at 08/07/2023 14:16:14***
Enforcement is Enabled
Enforcement Mode is WAF
Tetration rules have been programmed in WAF
WFP rules doesn't exist
!!!Enforcement Health is Good!!!
```

引數詳細資訊 — collectLogs

使用 — collectLogs引數運行時，指令碼會收集日誌以用於調試目的。

收集的日誌可以儲存在路徑C:\ Program Files \Cisco Tetration\logs\logs\Troubleshoot_Logs下

以下是使用 — collectLogs運行指令碼時的指令碼輸出示例 參數.

.\AgentTroubleshootingTool.ps1 -collectLogs

```
PS C:\Program Files\Cisco Tetration> .\AgentTroubleshootingTool.ps1 -collectLogs
Debug logs have been collected and saved under .\logs\Troubleshoot_Logs
PS C:\Program Files\Cisco Tetration>
```

引數詳細資訊 — collectDebugLogs

當您使用 — collectDebugLogs引數運行時，指令碼會收集啟用了loglevel:5的日誌，以用於調試目的。

使用此引數運行指令碼將捕獲netsh跟蹤，並且可以重新啟動CSW代理。
收集的日誌可以儲存在路徑C:\ Program Files \Cisco Tetration\logs\logs\Troubleshoot_Logs下

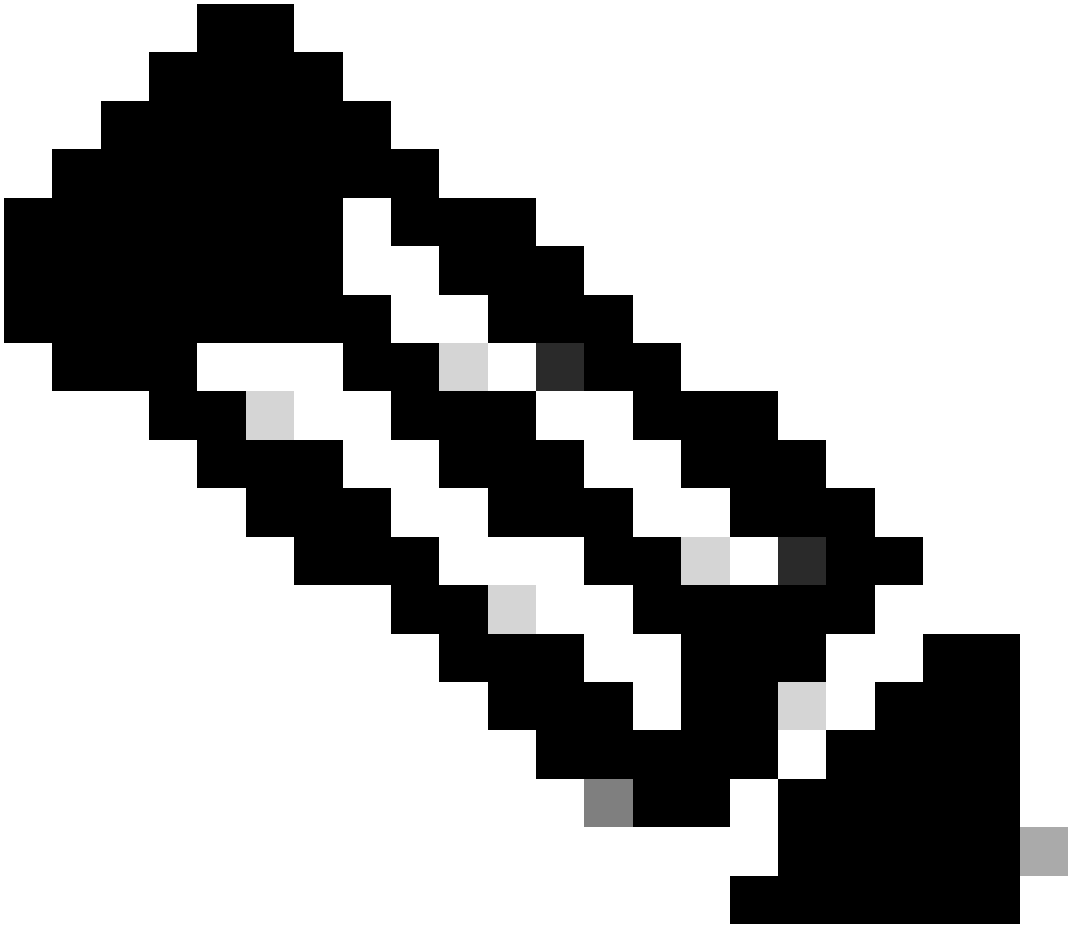
以下是使用 — collectDebugLogs運行指令碼時的指令碼輸出示例 參數.

.\AgentTroubleshootingTool.ps1 -collectDebugLogs

```
PS C:\Program Files\Cisco Tetration> .\AgentTroubleshootingTool.ps1 -collectDebugLogs
Running this parameter would capture netsh trace and CSW agent will be restarted. Do you want to continue? Y/N
y

Trace configuration:
-----------------------------------------------------------------
Status:             Running
Trace File:         C:\Users\ADMINI~1\AppData\Local\Temp\2\NetTraces\NetTrace.etl
Append:             Off
Circular:           On
Max Size:           512 MB
Report:             Off

Network trace has been collected and saved at C:\Users\ADMINI~1\AppData\Local\Temp\2\NetTraces\NetTrace.etl
WARNING: Waiting for service 'Cisco Secure Workload Agent (CswAgent)' to stop...
WARNING: Waiting for service 'Cisco Secure Workload Agent (CswAgent)' to stop...
Debug logs have been collected and saved under .\logs\Troubleshoot_Logs
PS C:\Program Files\Cisco Tetration>
```



附註：Agent Troubleshooting Tool以紅色顯示錯誤，以黃色顯示警告。如果您無法解決代理故障排除工具所標籤的常見問題，請使用代理故障排除工具收集調試日誌，並生成安全工作負載代理日誌捆綁包，然後與Cisco TAC聯絡以獲取幫助。

生成安全工作負載代理日誌捆綁包

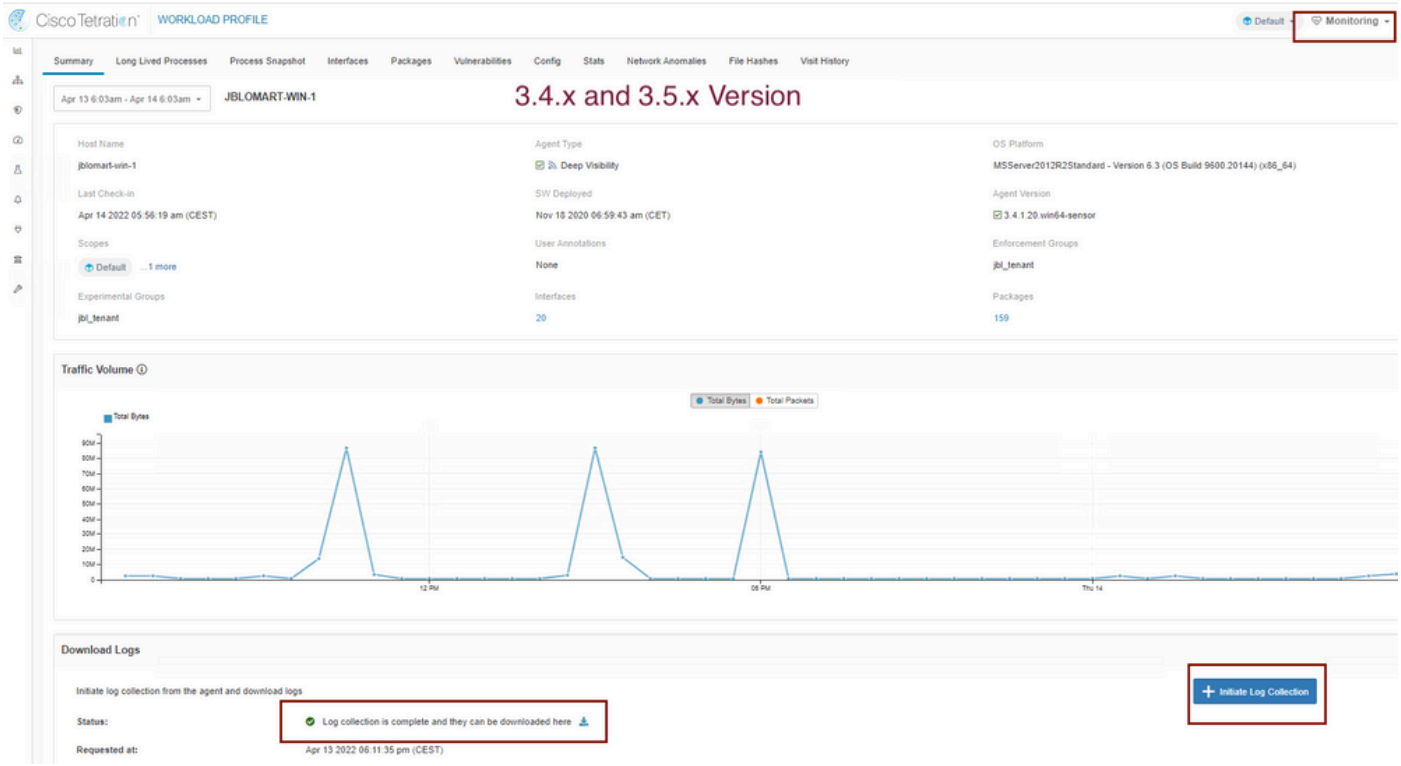
為了收集日誌捆綁，安全工作負載代理必須處於活動狀態。

- 對於3.6.x版本，導航到左側導航面板，選擇Manage > Agent，然後按一下Agent List。
- 對於3.4.x和3.5.x版本，從右上角下拉選單中導航到Monitoring，然後選擇Agent List。

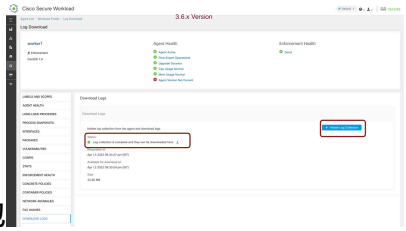
使用過濾器選項搜尋代理，然後按一下代理。該選項會將您轉到代理的工作量配置檔案。您可以在此處找到有關代理配置的詳細資訊，
狀態，等等。

在工作負載配置檔案頁面(3.6.x)的左側導航面板上，選擇Download Logs（在3.4.x和3.5.x中，並遵循摘要頁籤）。 按一下Initiate Log Collection，從Tetration Agent啟動日誌收集。可能需要一段時間才能完成日誌收集。日誌收集完成後，按一下Download選項下載日誌。向下滾動以取得將檔案上傳到案件編號的選項。

請參閱此映像，為在3.4.x和3.5.x版本上運行的代理建立安全工作負載代理日誌捆綁包。



請參閱此映像，以建立從3.6.x版本開始的安全工作負載代理日誌捆綁包



關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。