أستكشاف أخطاء وكيل Windows وإصلاحها باستخدام أداة أستكشاف أخطاء البرنامج وإصلاحها

المحتويات

المقدمة

يوضح هذا المستند كيفية إستخدام البرنامج النصي لأداة أستكشاف أخطاء البرامج وإصلاحها PowerShell المدمجة لحل مشكلات البرنامج العميل ل Windows الشائعة.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

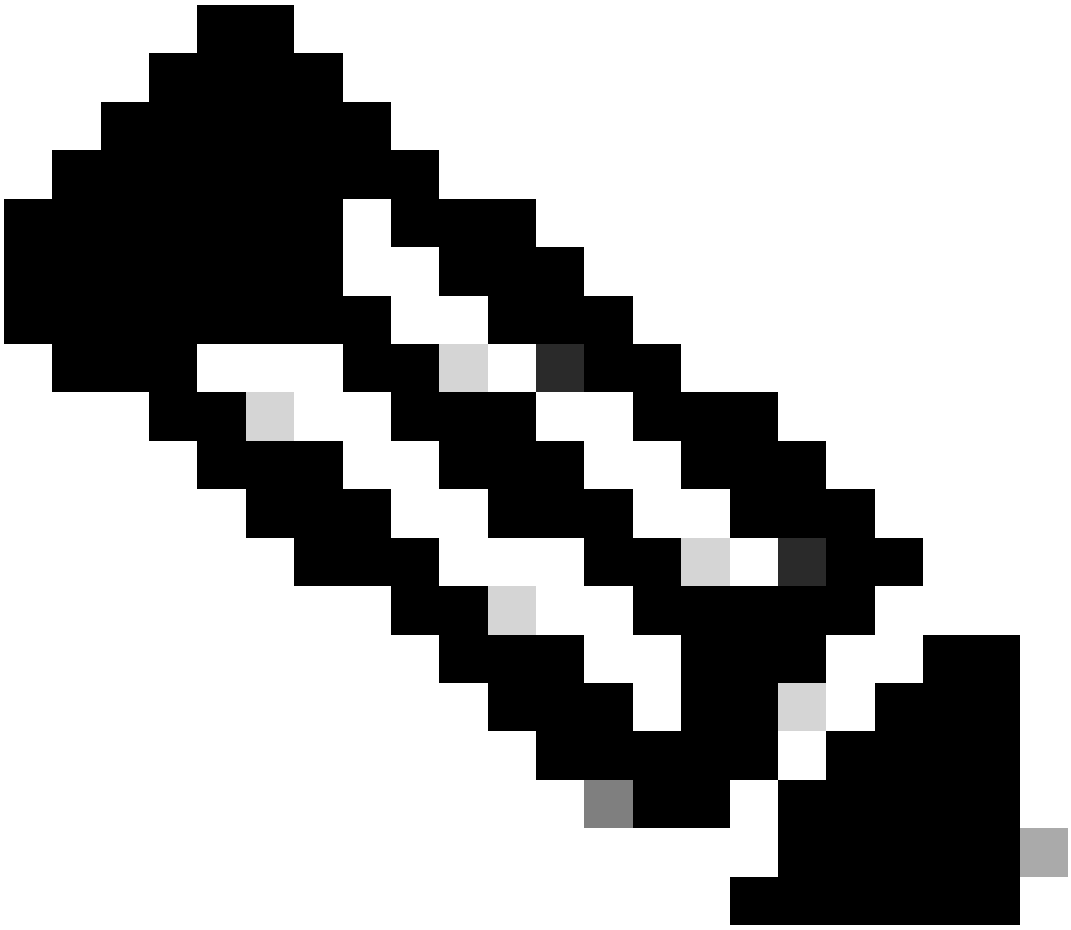
تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- PowerShell، الإصدار 4.0

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

معلومات أساسية

يأتي البرنامج النصي "أداة أستكشاف الأخطاء وإصلاحها للوكيل" مزودا بالعديد من الخيارات التي تتيح لك التحقق من الصحة العامة لوكيلك، والمشكلات المعروفة المتعلقة بتسجيل الوكلاء، والمشكلات المعروفة المتعلقة بترقية الوكلاء، والتحقق من الصحة العامة لعملية التنفيذ، وتجميع السجلات لمزيد من التحليل.



ملاحظة: تأتي "أداة أستكشاف أخطاء البرنامج وإصلاحها" وقد تم حزمها مع الوكيل الذي تم تضمينها في الإصدار 3.9، بالنسبة للإصدارات الأقدم من الإصدار 3.9. في أدبي، يمكنك نسخ البرنامج النصي بشكل افتراضي. إذا كنت تستخدم إصدارا قبل 3.9، فقط البرنامج النصي 3.9 مثبت على Windows Agent يعمل بنظام التشغيل Windows من (C:\Program Files\Cisco Tetration) في أداة أستكشاف الأخطاء وإصلاحها المستخدام.

خطوات لتشغيل النص التنفيذي

لتشغيل البرنامج النصي لأداة أستكشاف الأخطاء وإصلاحها للوكيل، اتبع الخطوات التالية:

1. افتح PowerShell كمسؤول.

2. انتقل إلى دليل تثبيت CSW (الموقع الافتراضي: C:\ Program Files \Cisco Tetration).

3. قم بتشغيل البرنامج النصي باستخدام هذا الأمر:

.\AgentTroubleshootingTool.psl

قائمة المعلمات المتوفرة في البرنامج النصي لأداة أستكشاف الأخطاء وإصلاحها للوكيل

تحتوي أداة أستكشاف أخطاء البرنامج وإصلاحها على العديد من الخيارات التي تتيح لك أستكشاف الأخطاء وإصلاحها بجوانب مختلفة من البرامج الخاصة بك.
فيما يلي الخيارات المتاحة:

-عوامل الصحة: تشغيل تقرير صحة العامل
-تسجيل الوكيل: التحقق من وجود مشاكل في تسجيل الوكيل
-ترقية الوكيل: التحقق من وجود مشاكل في ترقية الوكيل
- التعزيز الصحي: التحقق من وجود مشاكل تتعلق بالإنفاذ
-collectLog: تجميع السجلات لتصحيح الأخطاء
-collectDebugLog: تجميع السجلات مع تمكين مستوى السجل:5. يتضمن ذلك السجلات التي تم تجميعها باستخدام المعلمة -collectLog أيضا
-الكل: تشغيل كافة المعلمات باستثناء -collectDebugLog

باستخدام أي من هذه الخيارات، بمساعدة قم بتشغيل النص التنفيذي باستخدام المعلمة المناسبة.
على سبيل المثال، للتحقق من صحة وكالئك، قم بتشغيل البرنامج النصي باستخدام المعلمة -agentHealth:

.\AgentTroubleshootingTool.ps1 -agentHealth

تفاصيل المعلمة -agentHealth

تحت المعلمة -agentHealth، تقوم بالتحقق من هذه الأشياء:

1. Services TetSensor و TetEnforcement في حالة تشغيل.
2. معرف المستشعر صالح
3. يحتوي متغير المسار على 'C:\ Windows\System32'
4. يستخدم الوكيل ETW أو NPCAP. إذا كان نظام التشغيل هو 2008R2، فأنت تقوم بالتحقق من صحة NPCAP.

تعد إمكانية الاتصال بالوحدات الخلفية من خلال أدوات التجميع/تقنية EFE و WSS التي نقدمها أمرا جيدا.

هنا مثال على مخرجات النص التنفيذي عند تشغيل النص التنفيذي باستخدام -agentHealth بارامتر

.\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!!!
```

تفاصيل المعلمة -تسجيل العامل

تحت المعلمة -agentRegistration، يتم التحقق من هذه الأشياء:

1. ويتضمن التقرير الذي تم تجميعه باستخدام المعلمة -agentHealth.
2. تستند أخطاء التسجيل إلى رموز الأخطاء، على سبيل المثال، 401/403، وغيرها.

هناك أيضا خيار تم توفيره لإعادة تسجيل العميل مع نظام المجموعة إذا تم حذفه من واجهة المستخدم عن طريق الخطأ.

هنا مثال على مخرجات البرنامج النصي عندما تقوم بتشغيل البرنامج النصي باستخدام -agentRegistration المعلمة.

.\AgentTroubleshootingTool.ps1 -agentRegistration

```
PS C:\Program Files\Cisco Tetration> .\AgentTroubleshootingTool.ps1 -agentRegistration
***Checking For Agent Registration Issues at 08/07/2023 14:02:47***
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!!!
!!!No issues found with Agent Registration!!!
```

تفاصيل المعلمة -agentUpgrade

تحت المعلمة -agentUpgrade، يتم التحقق من هذه الأشياء:

1. الشهادات المطلوبة متوفرة في المتجر.

2. تتوفر ذاكرة التخزين المؤقت MSI تحت القيمة C: \ مجلد Windows \Installer.

إذا لم يتم العثور على أي مشاكل معروفة، ولكن لا تزال تقنية العميل معطلة، فعليك توفير الخيار لتجميع سجلات تصحيح الأخطاء لمزيد من أستكشاف الأخطاء وإصلاحها.

هنا مثال على إخراج البرنامج النصي عند التشغيل باستخدام -agentUpgrade باراميتر

.\AgentTroubleshootingTool.ps1 -agentUpgrade

```
PS C:\Program Files\Cisco Tetration> .\AgentTroubleshootingTool.ps1 -agentUpgrade
***Checking for Agent Upgrade Issues at 09/17/2025 17:13:25***
Required certificates exist in cert store
Known issues with agent upgrade not found. If you are still facing issues with Agent Upgrade, Please collect debug logs from host and Raise a Support Ticket with CSW Support for further investigation.
Do you want to collect debug Logs now? Y/N:
```

تفاصيل المعلمة -EnforcementHealth

تحت المعلمة -enforcementHealth، تقوم بالتحقق من هذه الأشياء:

1. تم تمكين التنفيذ أو تعطيله.
2. أي أسلوب من الإنفاذ يكون ممكنا.
3. تمت برمجة قواعد CSW في WAF، أو تمت برمجة عوامل تصفية WFP.
4. عوامل تصفية CSW WFP غير موجودة (عندما يكون الوضع WAF).
5. قواعد CSW WAF غير موجودة (عندما يكون الوضع WFP).

الخطوات 4 و 5 هي لتحديد المشاكل عند تبديل وضع الإنفاذ.

هنا مثال على مخرجات النص التنفيذي عندما تقوم بتشغيل النص التنفيذي مع -enforcementHealth المعلمة.

.\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!!!
```

تفاصيل المعلمة -collectionLog

يقوم البرنامج النصي بتجميع السجلات لأغراض تصحيح الأخطاء عند التشغيل باستخدام المعلمة -collectLog.

يمكن حفظ السجلات المجمعة تحت المسار C:\ Program Files \Cisco Tetration\logs\logs\Troubleshoot_Logs

هنا مثال على مخرجات النص التنفيذي عندما تقوم بتشغيل النص التنفيذي باستخدام -

collectLog المعلمة.

.\AgentTroubleshootingTool.ps1 -collectLog

```
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>
```

تفاصيل المعلمة -collectionDebugLog

يقوم البرنامج النصي بتجميع السجلات باستخدام logLevel:5 الممكنة لأغراض تصحيح الأخطاء عند التشغيل باستخدام المعلمة -collectDebugLog.

سيؤدي تشغيل البرنامج النصي باستخدام هذه المعلمة إلى التقاط تتبع الشبكة، ويمكن إعادة تشغيل عامل CSW.
يمكن حفظ السجلات المجمعة تحت المسار C:\ Program Files \Cisco Tetration\logs\logs\Troubleshoot_Logs

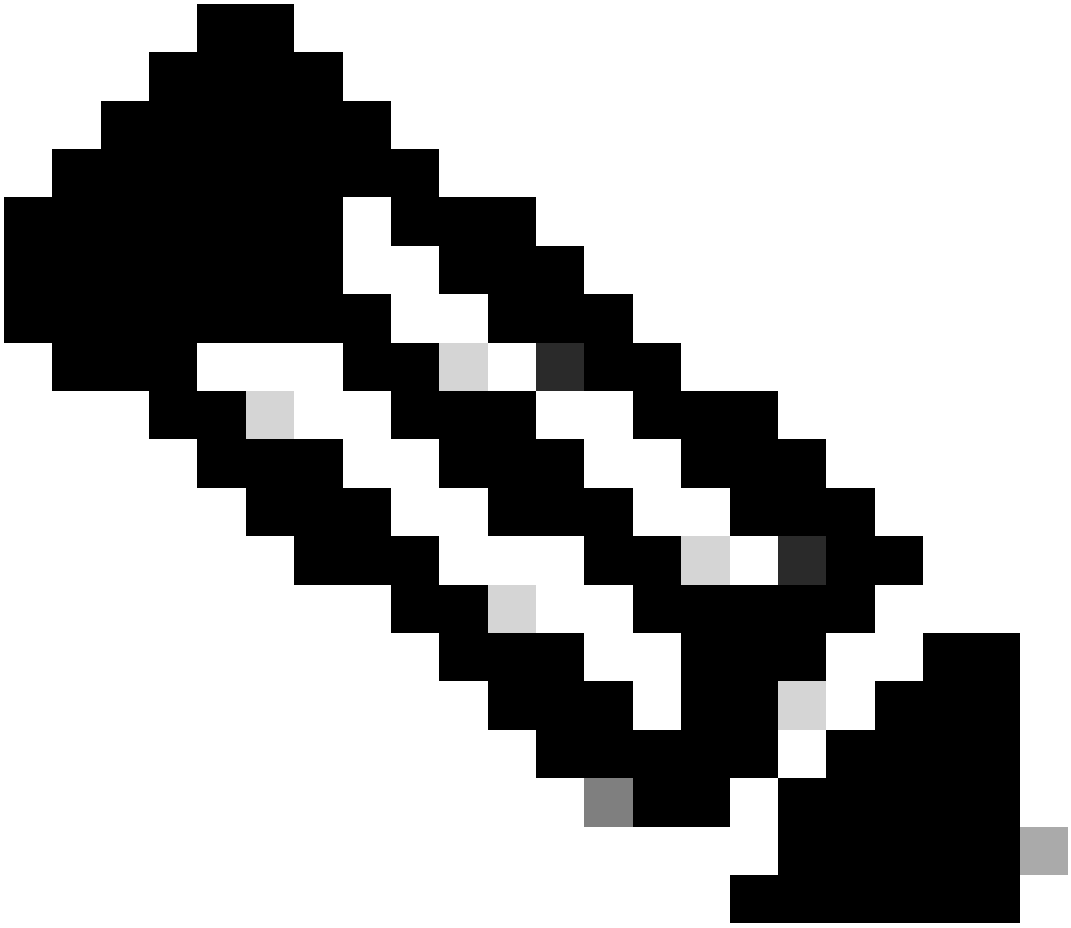
هنا مثال من إخراج البرنامج النصي عندما تقوم بتشغيل البرنامج النصي باستخدام -collectDebugLog المعلمة.

.\AgentTroubleshootingTool.ps1 -collectDebugLog

```
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>
```



ملاحظة: تعرض أداة "أستكشاف أخطاء البرنامج وإصلاحها" الأخطاء باللون الأحمر والتحذيرات باللون الأصفر. إذا لم تكن قادرا على حل المشكلات الشائعة التي تم وضع علامة عليها بواسطة أداة أستكشاف الأخطاء وإصلاحها للوكيل، فالرجاء تجميع سجلات تصحيح الأخطاء باستخدام أداة أستكشاف أخطاء العميل وإصلاحها وإنشاء حزمة سجل وكيل حمل العمل الآمن والاتصال ب Cisco TAC للحصول على مساعدة.

إنشاء حزمة سجل وكيل حمل العمل الآمن

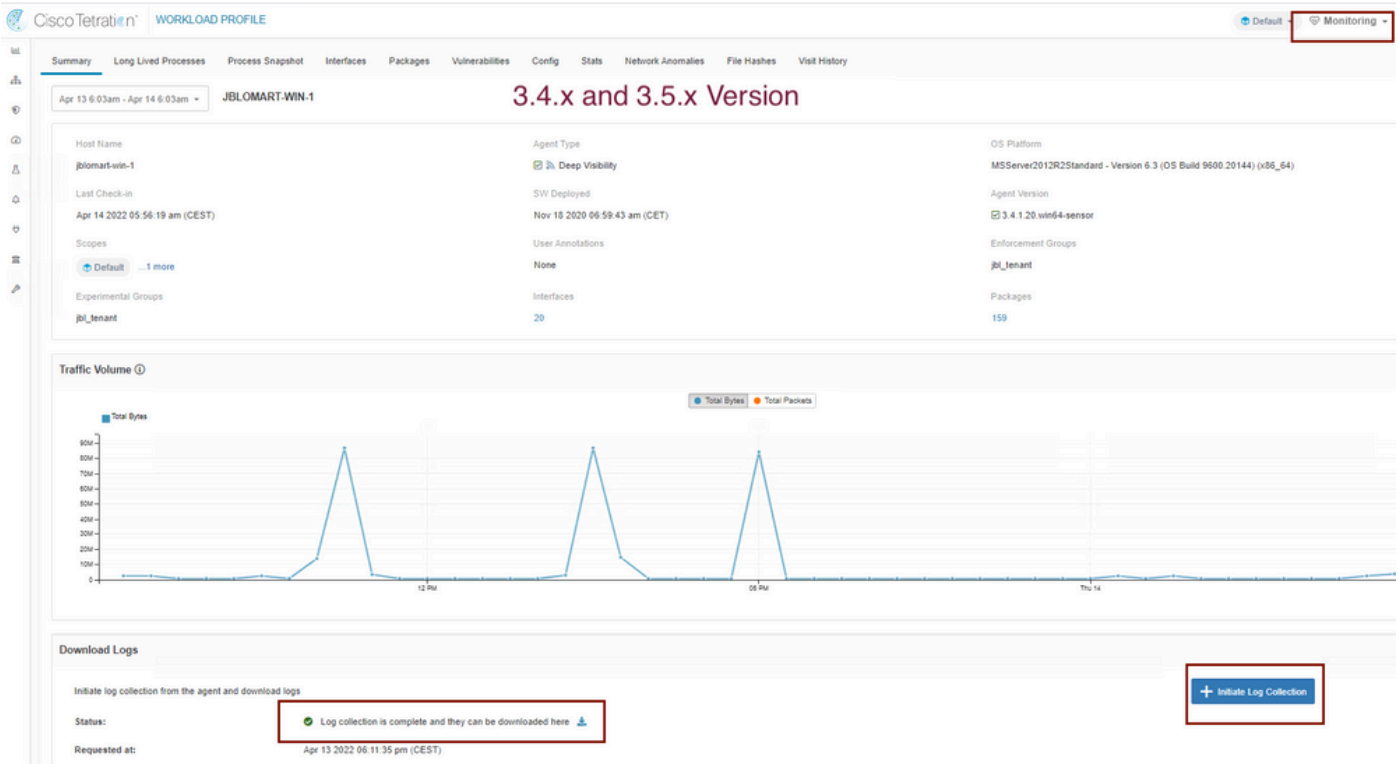
لتجميع حزمة السجل، يجب أن يكون عامل حمل العمل الآمن نشطا.

- بالنسبة لإصدار 3.6.x، انتقل إلى لوحة التصفح اليسرى، واختارManage > Agent، وانقر فوق قائمة العوامل.
- بالنسبة لإصدارات 3.4.x و 3.5.x، انتقل إلىMonitoring من القائمة المنسدلة العليا اليمنى واختر قائمة العوامل.

أستخدم خيار عامل التصفية للبحث عن العامل، وانقر فوق العامل. ينقلك إلى ملف تعريف عبء العمل للعامل. هنا يمكنك العثور على تفاصيل حول تكوين الوكيل، الحالة ، وهكذا.

في لوحة التصفح من الجانب الأيسر لصفحة ملف تعريف حمل العمل (3.6.x)، أختر سجلات التنزيل (في 3.4.x و 3.5.x واتبع علامة التبويب الملخص). انقر فوق بدء تجميع السجلات لبدء تجميع السجلات من وكيل المصادقة. قد يستغرق إكمال مجموعة السجلات بعض الوقت. بمجرد اكتمال مجموعة السجلات، انقر فوق الخيار تنزيل لتنزيل السجلات. قم بالتمرير إلى أسفل للحصول على خيار لتحميل الملف إلى رقم الحالة.

ارجع إلى هذه الصورة لإنشاء حزمة سجل وكيل حمل العمل الآمن للوكلاء الذين يعملون على إصدارات 3.4.x و 3.5.x.



ارجع إلى هذه الصورة لإنشاء حزمة سجل وكيل حمل العمل الآمن بدءا من إصدار 3.6.x 

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).