Solución de problemas del agente de Windows mediante la herramienta de solución de problemas del agente

Contenido

Introducción

Este documento describe cómo utilizar el script PowerShell integrado de la Herramienta de solución de problemas de agentes para resolver problemas comunes de los agentes de Windows.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

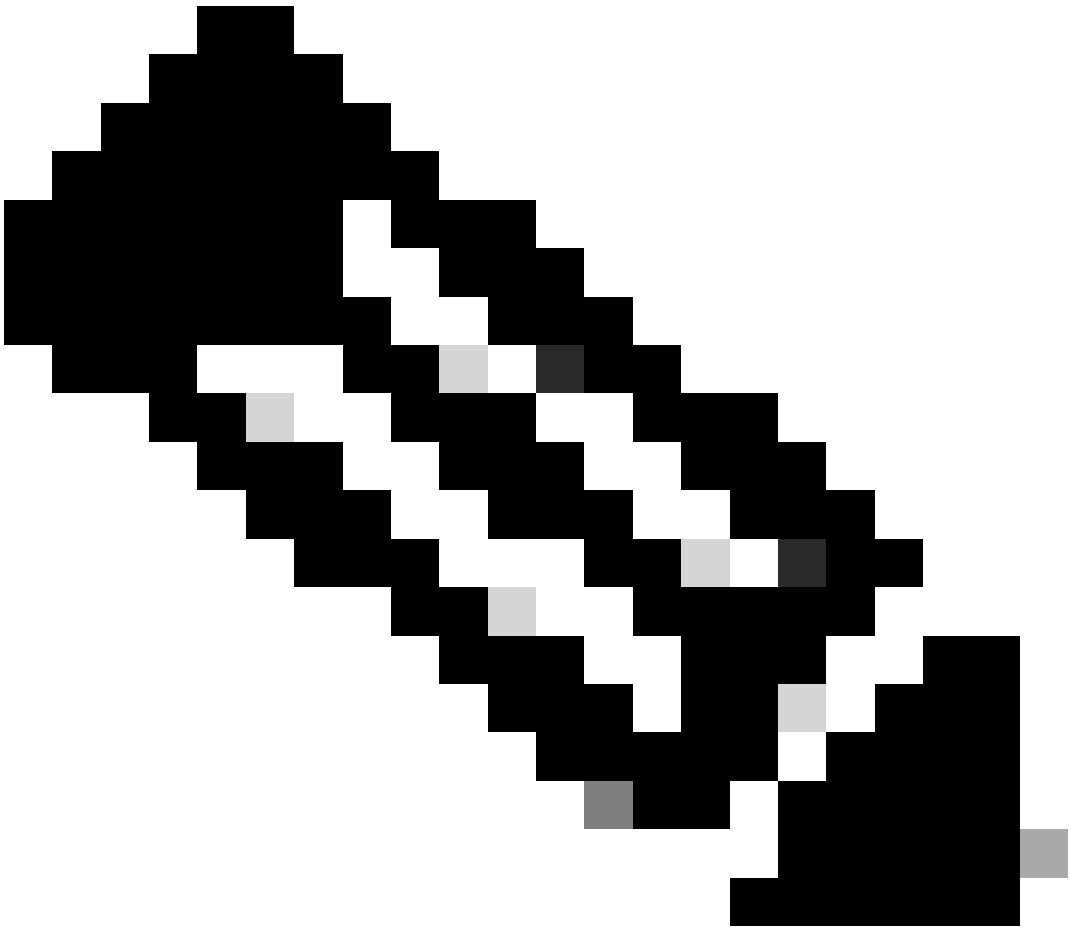
- PowerShell versión 4.0

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en

funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

La secuencia de comandos de la herramienta de solución de problemas de agentes incluye varias opciones que le permiten comprobar el estado general de sus agentes, los problemas conocidos con el registro de agentes, los problemas conocidos con las actualizaciones de agentes, comprobar el estado general de aplicación y recopilar registros para realizar análisis adicionales.



Nota: La Herramienta de resolución de problemas del agente viene empaquetada con el agente a partir de la versión 3.9. Para las versiones anteriores a la 3.9, no se incluye de forma predeterminada. Si utiliza una versión anterior a la 3.9, puede copiar la secuencia de comandos de un equipo con Windows con el agente 3.9 instalado y pegarla en (C:\Program Files\Cisco Tetration) para utilizar la herramienta de solución de problemas.

Pasos Para Ejecutar El Script

Para ejecutar el script de la herramienta de solución de problemas del agente, siga estos pasos:

1. Abra PowerShell como administrador.

2. Acceda al directorio de instalación de CSW (ubicación por defecto: C:\ Program Files \Cisco Tetration).

3. Ejecute el script con este comando:

.\AgentTroubleshootingTool.psl

Lista de parámetros disponibles en esta secuencia de comandos de la herramienta de resolución de problemas del agente

La herramienta de solución de problemas del agente incluye varias opciones que permiten solucionar problemas de distintos aspectos de los agentes.
Estas son las opciones disponibles:

-agentHealth: ejecutar informe de estado del agente
-agentRegistro: buscar problemas en el registro de agentes
-agentUpgrade: buscar problemas con la actualización del agente
-enforceHealth: comprobar si hay problemas con la aplicación
-collectLogs: recopilar registros para depuración
-collectDebugLogs: recopile los registros con loglevel:5 habilitado. Esto incluye los registros recopilados mediante el parámetro -collectLogs también
-todos: ejecutar todos los parámetros excepto -collectDebugLogs

Para utilizar cualquiera de estas opciones, simplemente ejecute el script con el parámetro adecuado.
Por ejemplo, para comprobar el estado de los agentes, ejecute el script con el parámetro -agentHealth:

.\AgentTroubleshootingTool.ps1 -agentHealth

Detalles del parámetro -agentHealth

En el parámetro -agentHealth, está comprobando lo siguiente:

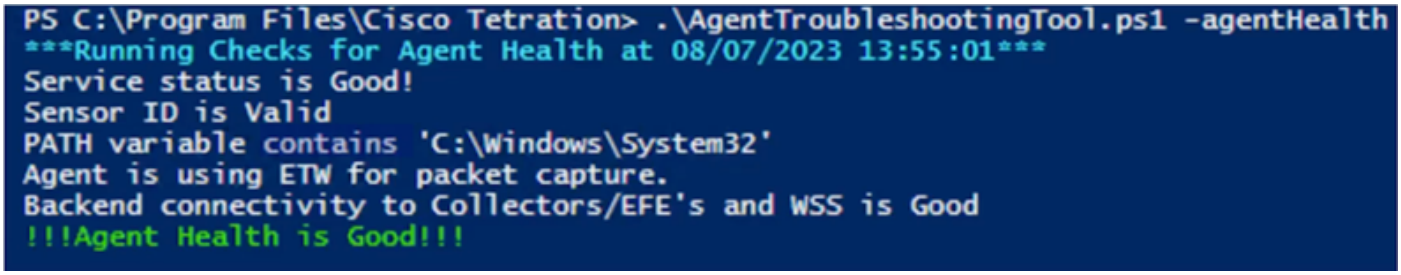
1. Los servicios TestSensor y TestEnforcer se encuentran en estado de ejecución.
2. ID del sensor válido
3. La variable PATH contiene 'C:\ Windows\System32'

4. El agente está utilizando ETW o NPCAP. Si el sistema operativo es 2008R2, está comprobando el estado de NPCAP.

La conectividad de back-end con nuestros recopiladores/EFE y WSS es buena.

Este es un ejemplo de la salida del script cuando se ejecuta el script con -agentHealth parámetro

.\AgentTroubleshootingTool.ps1 -agentHealth



Detalles del parámetro -agentRegistration

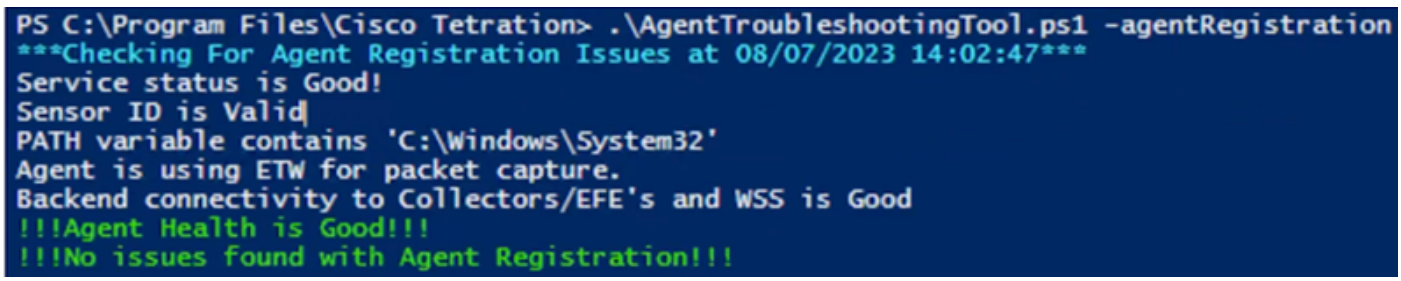
En el parámetro -agentRegistration, está comprobando lo siguiente:

1. Incluye el informe recopilado mediante el parámetro -agentHealth.
2. Los errores de registro se basan en códigos de error, por ejemplo, 401/403, y otros.

También se proporciona una opción para volver a registrar el agente con el clúster si se elimina de la interfaz de usuario por error.

A continuación se muestra un ejemplo de la salida del script cuando se ejecuta el script con -agentRegistration parámetro.

.\AgentTroubleshootingTool.ps1 -agentRegistration



Detalles del parámetro -agentUpgrade

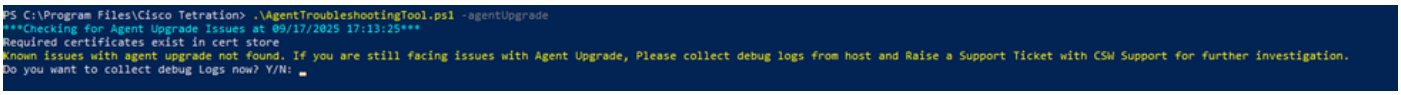
En el parámetro -agentUpgrade, está comprobando lo siguiente:

1. Los certificados necesarios están disponibles en el almacén.
2. La memoria caché MSI está disponible en el directorio C: \ Carpeta \Installer de Windows.

Si no se encuentra ningún problema conocido, pero la actualización del agente sigue fallando, debe proporcionar la opción de recopilar registros de depuración para solucionar más problemas.

A continuación se muestra un ejemplo de la salida del script cuando se ejecuta con -agentUpgrade parámetro

.\AgentTroubleshootingTool.ps1 -agentUpgrade



Detalles del parámetro -enforceHealth

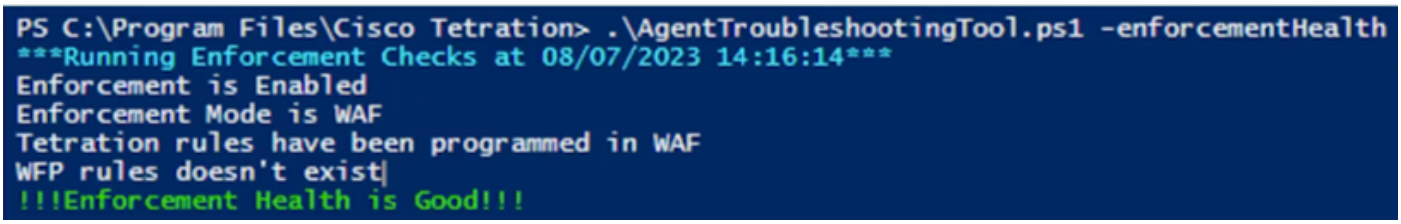
En el parámetro -enforceHealth, está comprobando lo siguiente:

1. La aplicación está habilitada o deshabilitada.
2. Qué modo de aplicación está habilitado.
3. Las reglas de CSW se han programado en WAF o los filtros de WFP se han programado.
4. Los filtros CSW WFP no existen (cuando el modo es WAF).
5. Las reglas WAF de CSW no existen (cuando el modo es WFP).

Los pasos 4 y 5 son para identificar problemas cuando se conmutó el Modo de aplicación.

A continuación se muestra un ejemplo de la salida del script cuando se ejecuta el script con -enforceHealth parámetro.

.\AgentTroubleshootingTool.ps1 -enforceHealth



Detalles del parámetro -collectLogs

La secuencia de comandos recopila los registros con fines de depuración cuando se ejecuta con el parámetro -collectLogs.

Los registros recopilados se pueden guardar en la ruta C:\ Program Files \Cisco Tetration\logs\logs\Troubleshoot_Logs

Este es un ejemplo de la salida del script cuando se ejecuta el script con -collectLogs parámetro.

.\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>
```

Detalles del parámetro -collectDebugLogs

La secuencia de comandos recopila los registros con el valor loglevel:5 habilitado para la depuración cuando se ejecuta con el parámetro -collectDebugLogs.

Si se ejecuta la secuencia de comandos con este parámetro, se capturará el seguimiento de netsh y se podrá reiniciar el agente CSW.
Los registros recopilados se pueden guardar en la ruta C:\ Program Files \Cisco Tetration\logs\logs\Troubleshoot_Logs

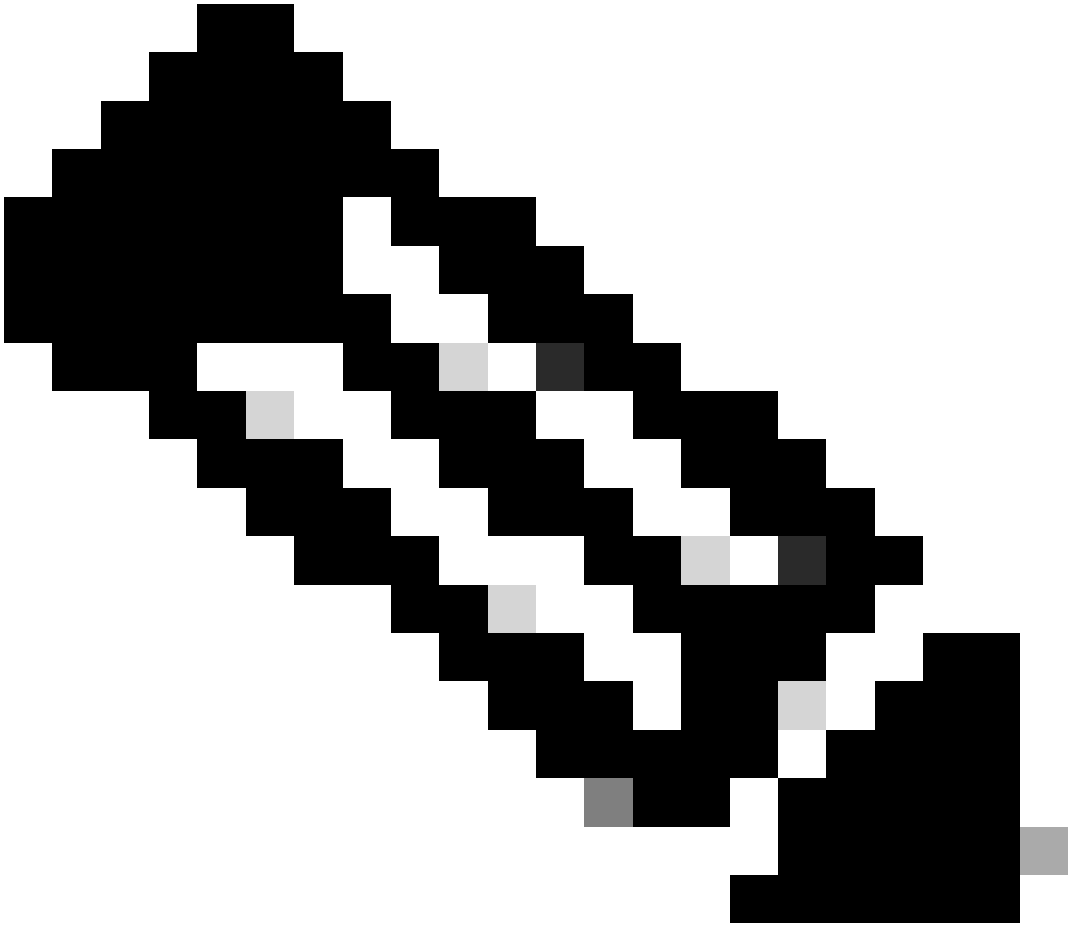
Este es un ejemplo de la salida del script cuando se ejecuta el script con -collectDebugLogs parámetro.

.\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>
```



Nota: La Herramienta de solución de problemas del agente muestra errores en color rojo y advertencias en color amarillo. Si no puede resolver los problemas comunes marcados por la Herramienta de resolución de problemas del agente, recopile los registros de depuración mediante la Herramienta de resolución de problemas del agente y genere un paquete de registro del Agente de carga de trabajo segura y póngase en contacto con el TAC de Cisco para obtener ayuda.

Generar el paquete de registro del agente de carga de trabajo segura

Para recopilar el paquete de registro, el agente de carga de trabajo segura debe estar activo.

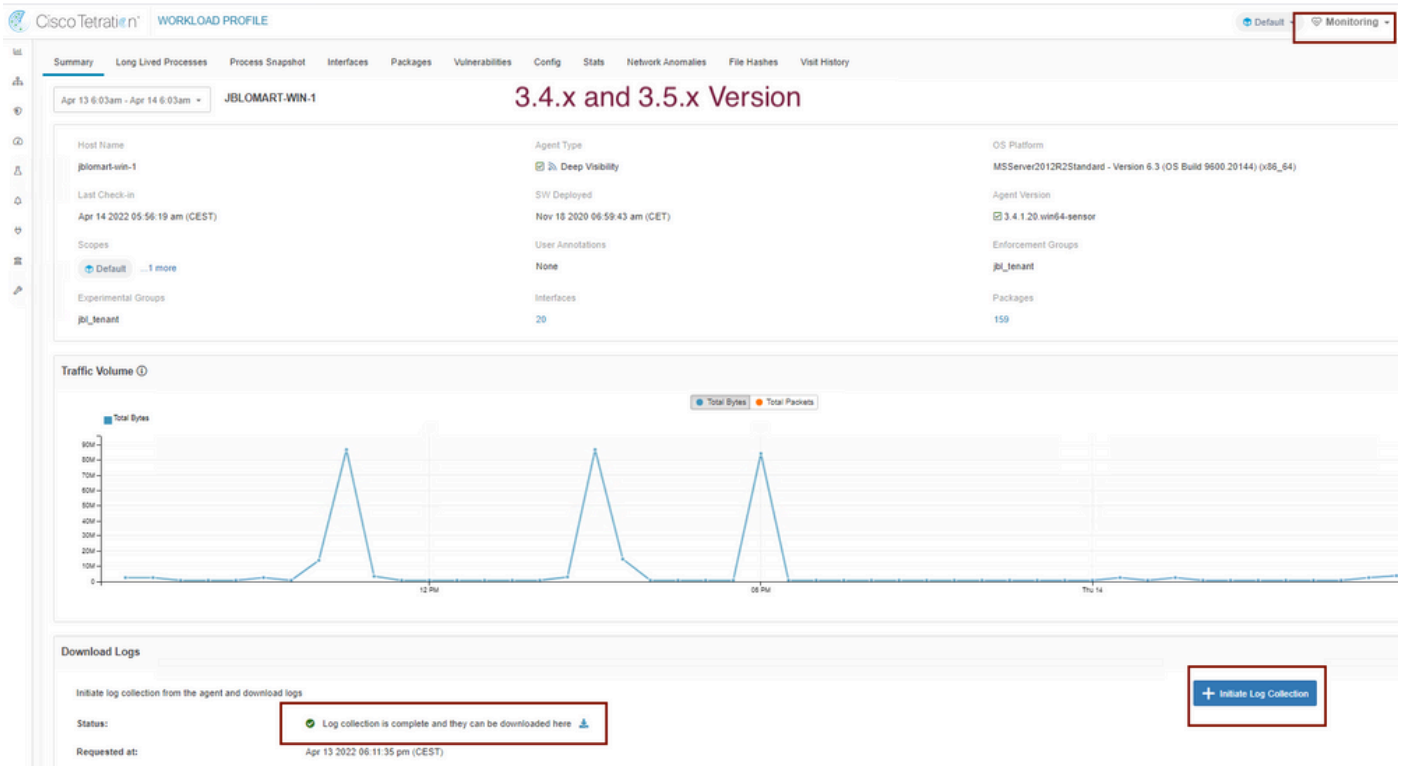
- Para la versión 3.6.x, desplácese al panel de navegación izquierdo, elija Administrar > Agente, y haga clic en Lista de agentes.

- Para las versiones 3.4.x y 3.5.x, vaya aSupervisión desde el menú desplegable superior derecho y elija Lista de agentes.

Utilice la opción de filtro para buscar el agente y haga clic en elagente. Le lleva al perfil de carga de trabajo del agente. Aquí puede encontrar información sobre la configuración del agente, estado, etc.

En el panel de navegación del lado izquierdo de la página del perfil de carga de trabajo (3.6.x), elija Descargar registros (en 3.4.x y 3.5.x y siga la ficha de resumen). Haga clic en Iniciar Recopilación de Registros para iniciar la recopilación de registros desde el Agente de Tetración. Puede llevar un tiempo completar la recopilación de registros. Una vez completada la recopilación de registros, haga clic en la opciónDescargar aquí para descargar los registros. Desplácese hacia abajo para obtener una opción para cargar el archivo en el número de caso.

Consulte esta imagen para crear el Secure Workload Agent Log Bundle para los agentes que se ejecutan en las versiones 3.4.x y 3.5.x.



Consulte esta imagen para crear el Secure Workload Agent Log Bundle a partir de la versión 3.6.x

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).