Troubleshoot Windows Agent Issues Using the Agent Troubleshooting Tool

Contents

Introduction

This document describes how to use the built-in Agent Troubleshooting Tool PowerShell script to resolve common Windows agent issues.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on these software and hardware versions:

- PowerShell version 4.0

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

The Agent Troubleshooting Tool script comes with several options that allow you to check the overall health of your agents, known issues with agent registration, known issues with agent upgrades, check the overall enforcement health, and collect logs for further analysis.

Note: The Agent Troubleshooting Tool comes packaged with the agent beginning in version 3.9. For versions earlier than 3.9, it is not included by default. If you are using a version prior to 3.9, you can copy the script from a Windows machine with the 3.9 agent installed and paste it into (C:\Program Files\Cisco Tetration) to use the troubleshooting tool.

Steps To Run The Script

To run the Agent troubleshooting tool script, follow these steps:

1. Open PowerShell as an administrator.

2. Navigate to the CSW installation directory (default location: C:\ Program Files \Cisco Tetration).

3. Run the script using this command:

```
.\AgentTroubleshootingTool.psl
```

List of Parameters Available in this Agent Troubleshooting Tool Script

The Agent troubleshooting tool comes with several options that allow you to troubleshoot different aspects of your agents.
Here are the available options:

-agentHealth: run agent Health Report
-agentRegistration: check for issues in Agent Registration
-agentUpgrade: check for issues with agent Upgrade
-enforcementHealth: check for issues with Enforcement
-collectLogs: collect Logs for debugging
-collectDebugLogs: collect logs with loglevel:5 enabled. This includes logs collected using the parameter -collectLogs as well
-all: run all parameters except -collectDebugLogs

To use any of these options, simply run the script with the appropriate parameter.
For example, to check the health of your agents, run the script with the -agentHealth parameter:

.\AgentTroubleshootingTool.ps1 -agentHealth

Parameter Details -agentHealth

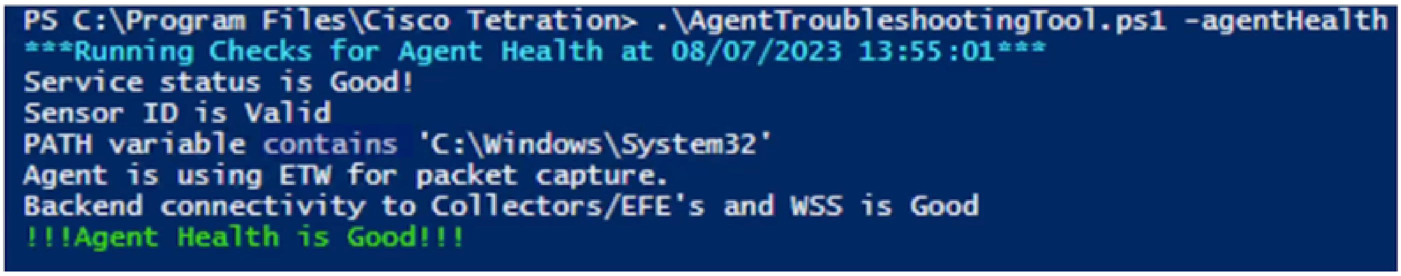
Under the -agentHealth parameter, you are checking these things:

1. Services TetSensor and TetEnforcer are in a running state.
2. Sensor ID is valid
3. PATH variable contains 'C:\ Windows\System32'
4. The agent is using ETW or NPCAP. If the OS is 2008R2, then you are checking NPCAP Health.

Backend connectivity with our collectors/EFEs and WSS is good.

Here is an example of the script output when run the script with the -agentHealth parameter

.\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!!!
```

Parameter Details -agentRegistration

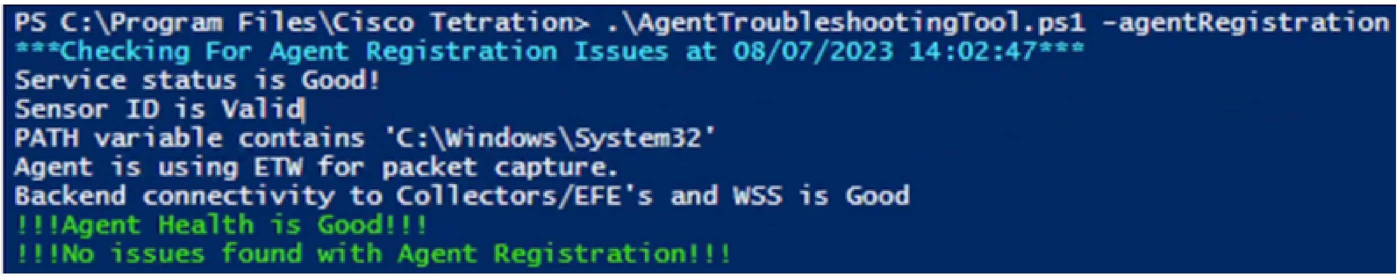
Under the -agentRegistration parameter, you are checking these things:

1. It includes the report collected using the parameter -agentHealth.
2. Registration errors are based on error codes, for example, 401/403, and others.

There is also an option provided to re-register the agent with the cluster if it is deleted from the UI by mistake.

Here is an example of the script output when you run the script with the -agentRegistration parameter.

.\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!!!
```

Parameter Details   -agentUpgrade

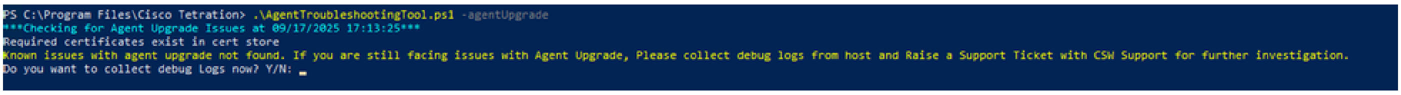
Under the -agentUpgrade parameter, you are checking these things:

1. Required certificates are available in the store.
2. The MSI cache is available under the C: \ Windows \Installer folder.

If no known issues are found, but the agent upgrade is still failing, then you provide the option to collect debug logs for further troubleshooting.

Here is an example of the script output when you run with the -agentUpgrade parameter

.\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:
```

Parameter Details   -enforcementHealth

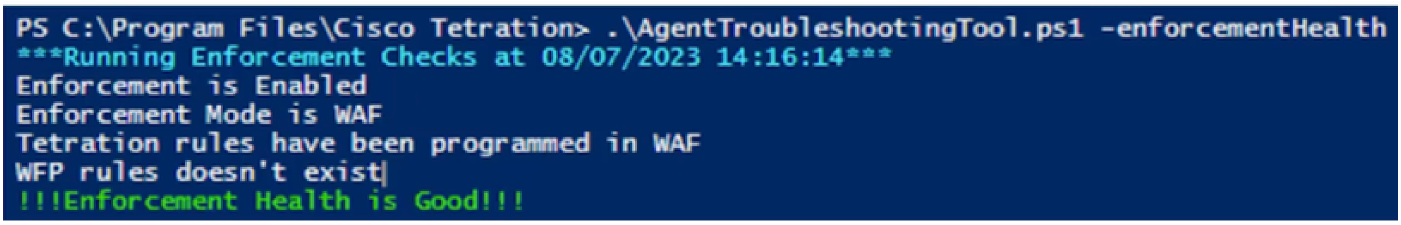
Under the -enforcementHealth parameter, you are checking these things:

1. Enforcement is enabled or disabled.
2. Which Mode of Enforcement is Enabled.
3. CSW rules have been programmed in WAF, or WFP filters have been programmed.
4. CSW WFP filters do not exist (when mode is WAF).
5. CSW WAF rules do not exist (when mode is WFP).

Steps 4 and 5 are to identify issues when Enforcement Mode was switched.

Here is an example of the script output when you run the script with the -enforcementHealth parameter.

.\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!!!
```

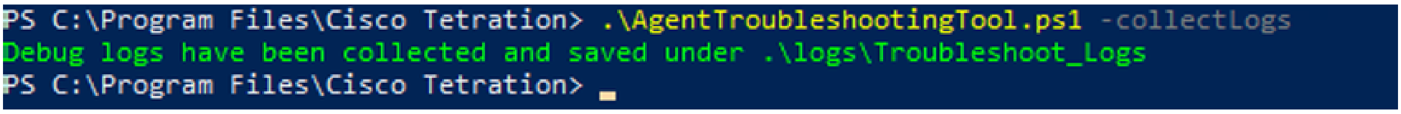
Parameter Details   -collectLogs

The script collects logs for debugging purposes when run with the -collectLogs parameter.

Collected logs can be saved under the path C:\ Program Files \Cisco Tetration\logs\logs\Troubleshoot_Logs

Here is an example of the script output when you run the script with the -collectLogs parameter.

.\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> _
```

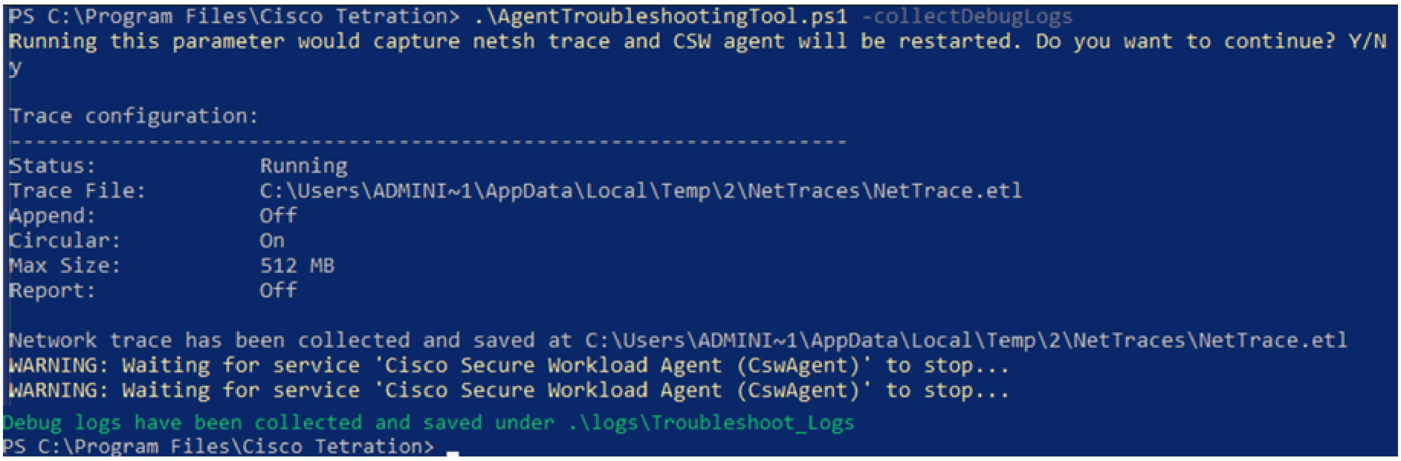
Parameter Details -collectDebugLogs

The script collects logs with loglevel:5 enabled for debugging purposes when you run with the -collectDebugLogs parameter.

Running the script with this parameter would capture the netsh trace, and the CSW agent can be restarted. Collected logs can be saved under the path C:\ Program Files \Cisco Tetration\logs\logs\Troubleshoot_Logs

Here is an example of the script output when you run the script with the -collectDebugLogs parameter.

.\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> _
```

Note: The Agent Troubleshooting Tool displays errors in red color and warnings in yellow color. If you are unable to resolve the common issues flagged by Agent Troubleshooting Tool, please collect debug logs using the Agent Troubleshooting Tool and generate a Secure Workload Agent log bundle and contact Cisco TAC for assistance.

Generate the Secure Workload Agent Log Bundle

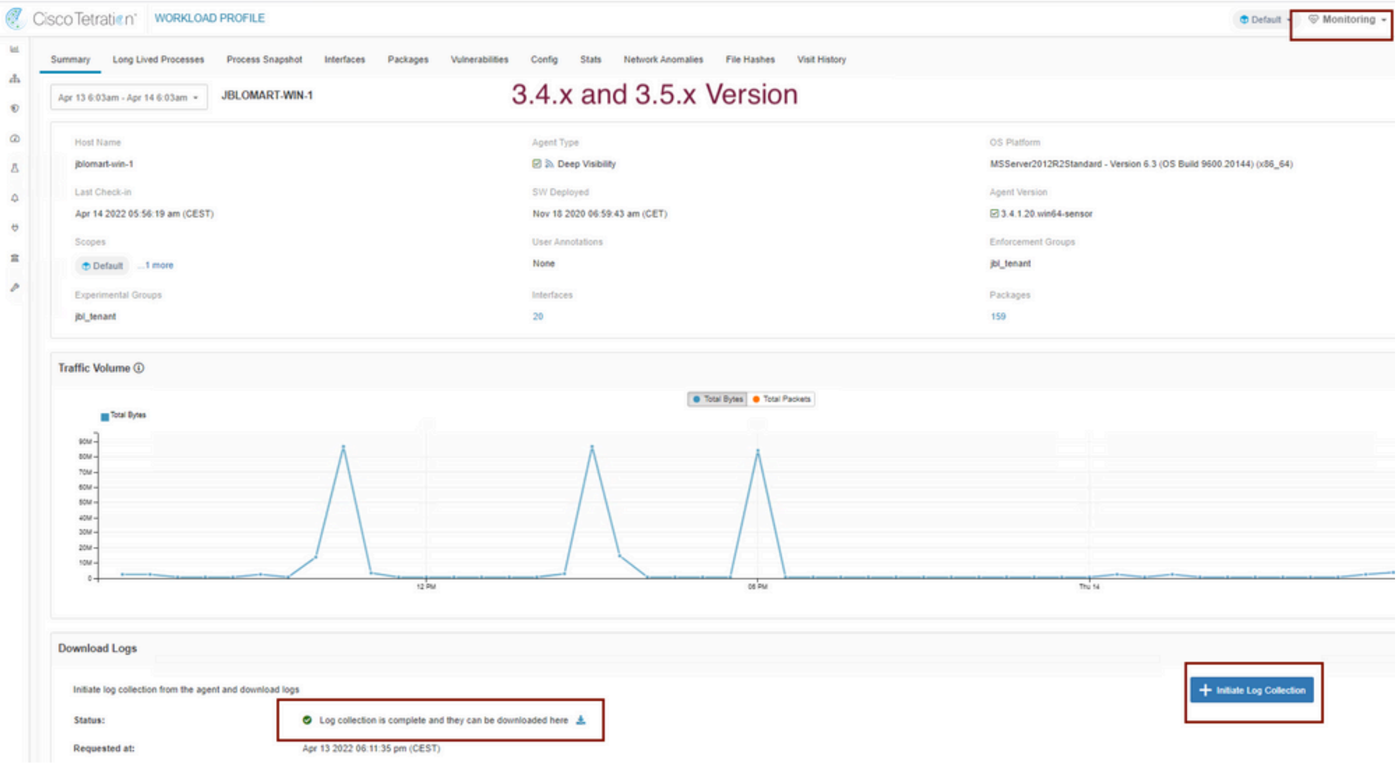
In order to collect the log bundle, the Secure Workload agent must be active.

- For the 3.6.x version, navigate to the **left navigation** panel, choose**Manage > Agent**, and click**Agent List**.
- For the 3.4.x and 3.5.x versions, navigate to**Monitoring from** the **top right drop-down** menu and choose **Agent List**.

Utilize the filter option to search for the agent, and click the**agent**. It takes you to the workload profile of the agent. Here you can find details about the agent configuration, status, and so on.

At the **left side navigation** panel of the workload profile page (3.6.x), choose **Download Logs** (in the 3.4.x and 3.5.x and follow the summary tab). Click **Initiate Log Collection** to initiate the log collection from the Tetration Agent. It can take a while to complete the log collection. Once the log collection is complete, click the**Download here**option to download the logs. Scroll down to get an option to upload the file to the case number.

Refer to this image to create the Secure Workload Agent Log Bundle for agents running on 3.4.x and 3.5.x versions.



JBLOMART-WIN-1

Host Name: jblomart-win-1

Agent Type: ☑ Deep Visibility

OS Platform: MSServer2012R2Standard - Version 6.3 (OS Build 9600.20144) (x86_64)

Last Check-in: Apr 14 2022 05:56:19 am (CEST)

SW Deployed: Nov 18 2020 06:59:43 am (CET)

Agent Version: ☑ 3.4.1.20.win64-sensor

Scopes: Default ...1 more

User Annotations: None

Enforcement Groups: jbl_tenant

Experimental Groups: jbl_tenant

Interfaces: 20

Packages: 159

Initiate log collection from the agent and download logs

Status: Log collection is complete and they can be downloaded here

Requested at: Apr 13 2022 06:11:35 pm (CEST)

Refer to this image to create the Secure Workload Agent Log Bundle starting from 3.6.x version