

使用代理故障排除工具排除Windows代理故障

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[运行脚本的步骤](#)

[此代理故障排除工具脚本中可用的参数列表](#)

[参数详细信息 — agentHealth](#)

[参数详细信息 — agentRegistration](#)

[参数详细信息 — agentUpgrade](#)

[参数详细信息 — enforcementHealth](#)

[参数详细信息 — collectLogs](#)

[参数Details-collectDebugLogs](#)

[生成安全工作负载代理日志捆绑包](#)

简介

本文档介绍如何使用内置的代理故障排除工具PowerShell脚本解决常见的Windows代理问题。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

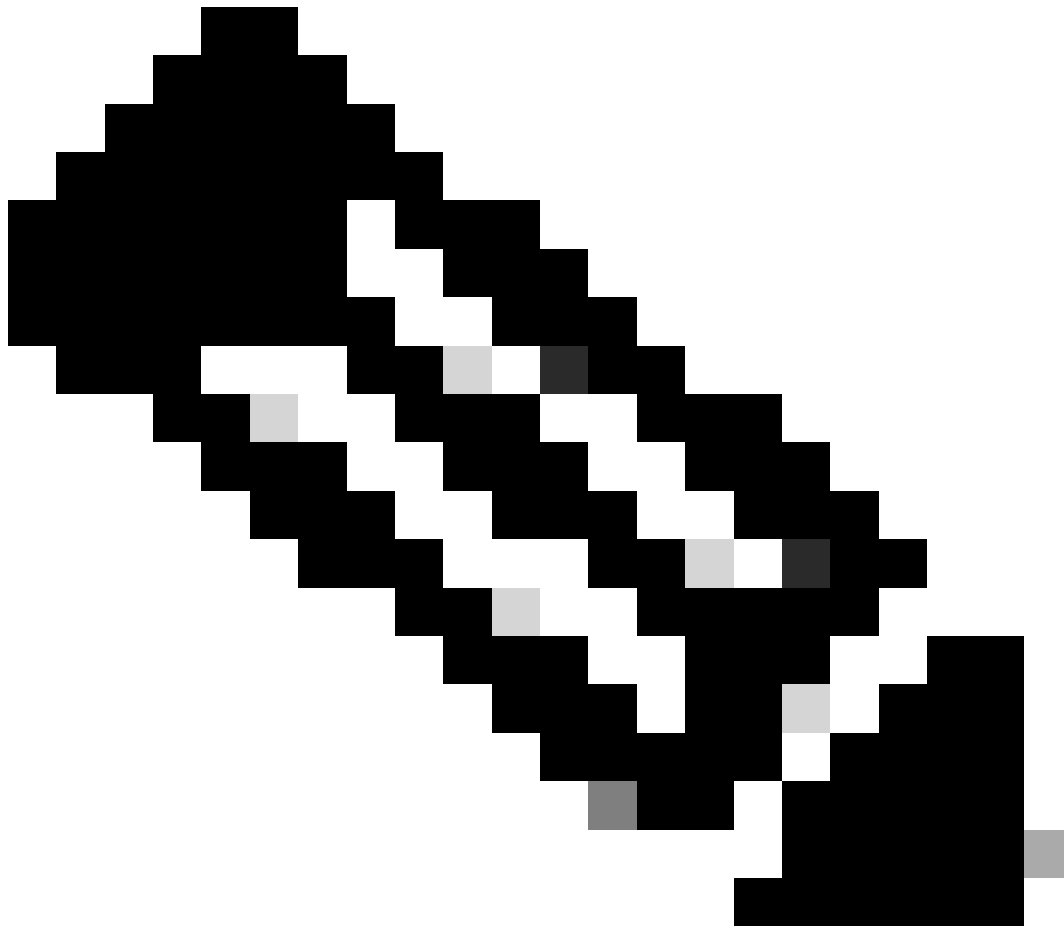
本文档中的信息基于以下软件和硬件版本：

- PowerShell版本4.0

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

代理故障排除工具脚本附带多个选项，通过这些选项，您可以检查代理的整体运行状况、代理注册的已知问题、代理升级的已知问题、检查整体实施运行状况，以及收集日志以进行进一步分析。



注意：从3.9版本开始，代理故障排除工具随代理一起提供。对于3.9之前的版本，默认情况下不包括。如果您使用的是3.9之前的版本，您可以从安装了3.9代理的Windows计算机上复制脚本，然后将其粘贴到(C:\Program Files\Cisco Tetration)中，以使用故障排除工具。

运行脚本的步骤

要运行代理故障排除工具脚本，请执行以下步骤：

- 1.以管理员身份打开PowerShell。
- 2.导航到CSW安装目录(默认位置：C:\Program Files\Cisco Tetration)。
- 3.使用以下命令运行脚本：
`.\AgentTroubleshootingTool.ps1`

此代理故障排除工具脚本中可用的参数列表

代理故障排除工具附带多个选项，可用于对代理的不同方面进行故障排除。
以下是可用选项：

- agentHealth:运行代理运行状况报告
- agentRegistration:检查代理注册中的问题
- agentUpgrade:检查代理升级的问题
- enforcementHealth:检查执行问题
- collectLog:收集用于调试的日志
- collectDebugLogs:收集loglevel:5启用的日志。这包括使用参数 — collectLogs收集的日志
- all:运行除 — collectDebugLogs之外的所有参数

要使用这些选项中的任何一个，只需使用适当的参数运行脚本。
例如，要检查代理的运行状况，请运行带有 — agentHealth参数的脚本：

```
.\AgentTroubleshootingTool.ps1 -agentHealth
```

参数详细信息 — agentHealth

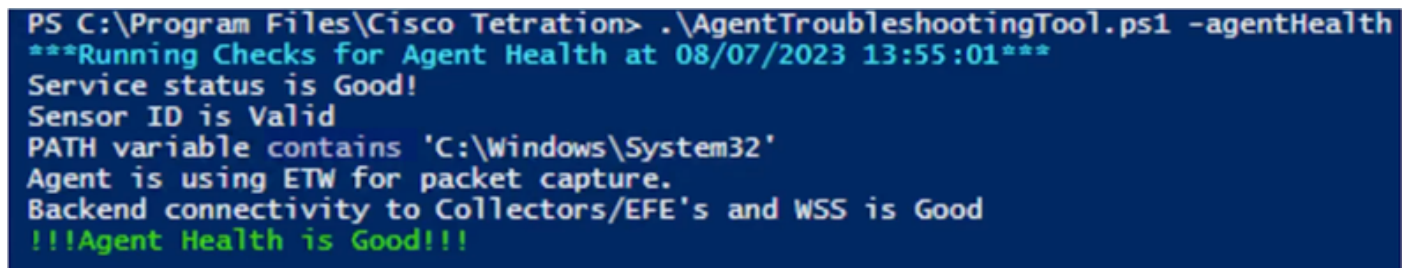
在 — agentHealth参数下，您将检查以下内容：

1. 服务TetSensor和TetEnforcer处于运行状态。
2. 传感器ID有效
3. PATH变量包含“C:\ Windows\System32”
4. 座席正在使用ETW或NPCAP。如果操作系统是2008R2，则您正在检查NPCAP运行状况。

与收集器/EFE和WSS的后端连接良好。

以下是使用 — agentHealth运行脚本时脚本输出的示例 参数

```
.\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!!!
```

参数详细信息 — agentRegistration

在 — agentRegistration参数下，您正在检查以下内容：

1. 它包括使用参数 — agentHealth收集的报告。
2. 注册错误取决于错误代码，例如401/403等。

如果错误地从UI中删除了代理，还提供一个选项，用于在集群中重新注册代理。

以下是使用-agentRegistration运行脚本时的脚本输出示例 参数.

.\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!!!
```

参数详细信息 — agentUpgrade

在 — agentUpgrade参数下，您正在检查以下内容：

1. 所需的证书在存储中可用。
2. MSI缓存在C:\Windows\Installer文件夹。

如果未发现已知问题，但代理升级仍然失败，则您可以选择收集调试日志以进一步排除故障。

以下是使用 — agentUpgrade运行时脚本输出的示例 参数

.\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: _
```

参数详细信息 — enforcementHealth

在 — enforcementHealth参数下，您将检查以下内容：

1. 实施已启用或已禁用。
2. 启用了哪种实施模式。
3. CSW规则已编入WAF，或粮食署过滤器已编入WAF。
4. CSW WFP过滤器不存在（当模式为WAF时）。

5. CSW WAF规则不存在（当模式为WFP时）。

第4步和第5步是确定执行模式切换时的问题。

以下是使用 — enforcementHealth运行脚本时的脚本输出示例 参数。

.\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!!!
```

参数详细信息 — collectLogs

当使用 — collectLogs参数运行时，脚本会收集日志以用于调试目的。

收集的日志可以保存在C:\Program Files\Cisco Tetration\logs\logs\Troubleshoot_Logs路径下

以下是使用 — collectLogs运行脚本时的脚本输出示例 参数。

.\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> █
```

参数详细信息 — collectDebugLogs

当您使用 — collectDebugLogs参数运行时，脚本会收集启用了loglevel:5的日志，以用于调试目的。

使用此参数运行脚本将捕获netsh跟踪，并且可以重新启动CSW代理。

收集的日志可以保存在C:\Program Files\Cisco Tetration\logs\logs\Troubleshoot_Logs路径下

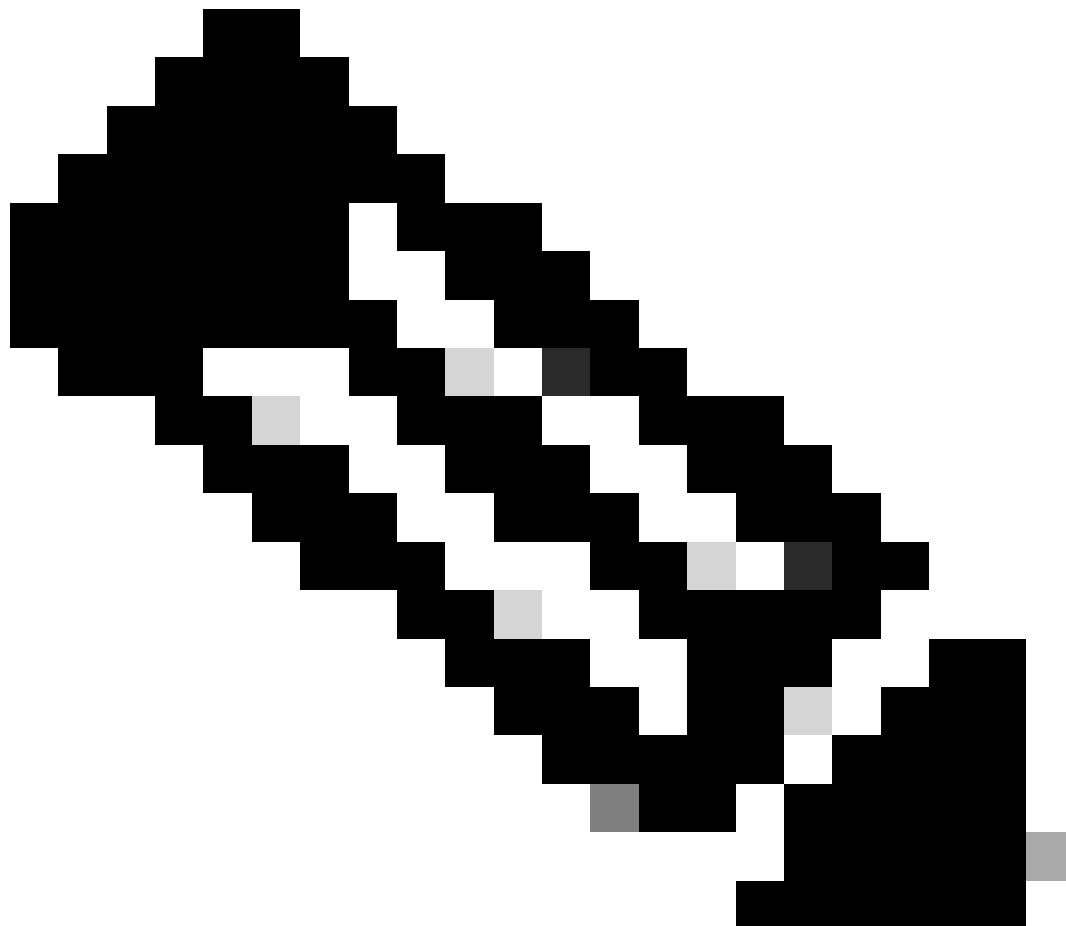
以下是使用 — collectDebugLogs运行脚本时的脚本输出示例 参数。

.\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>
```



注意：座席故障排除工具以红色显示错误，以黄色显示警告。如果无法解决代理故障排除工具所标记的常见问题，请使用代理故障排除工具收集调试日志，并生成安全工作负载代理日志捆绑包，然后联系思科TAC以获取帮助。

生成安全工作负载代理日志捆绑包

要收集日志捆绑包，安全工作负载代理必须处于活动状态。

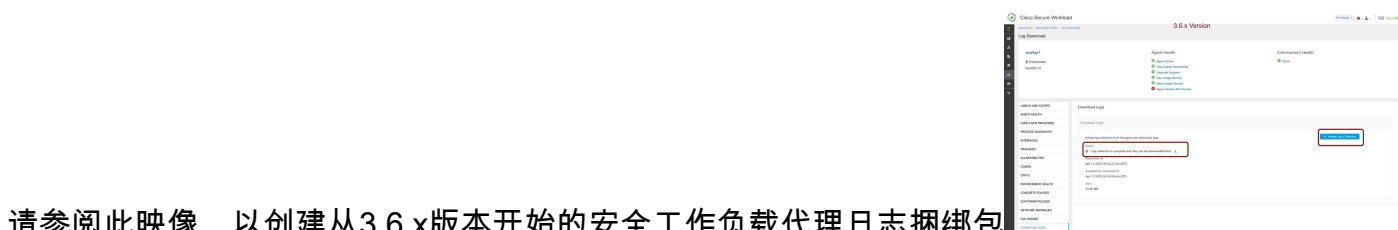
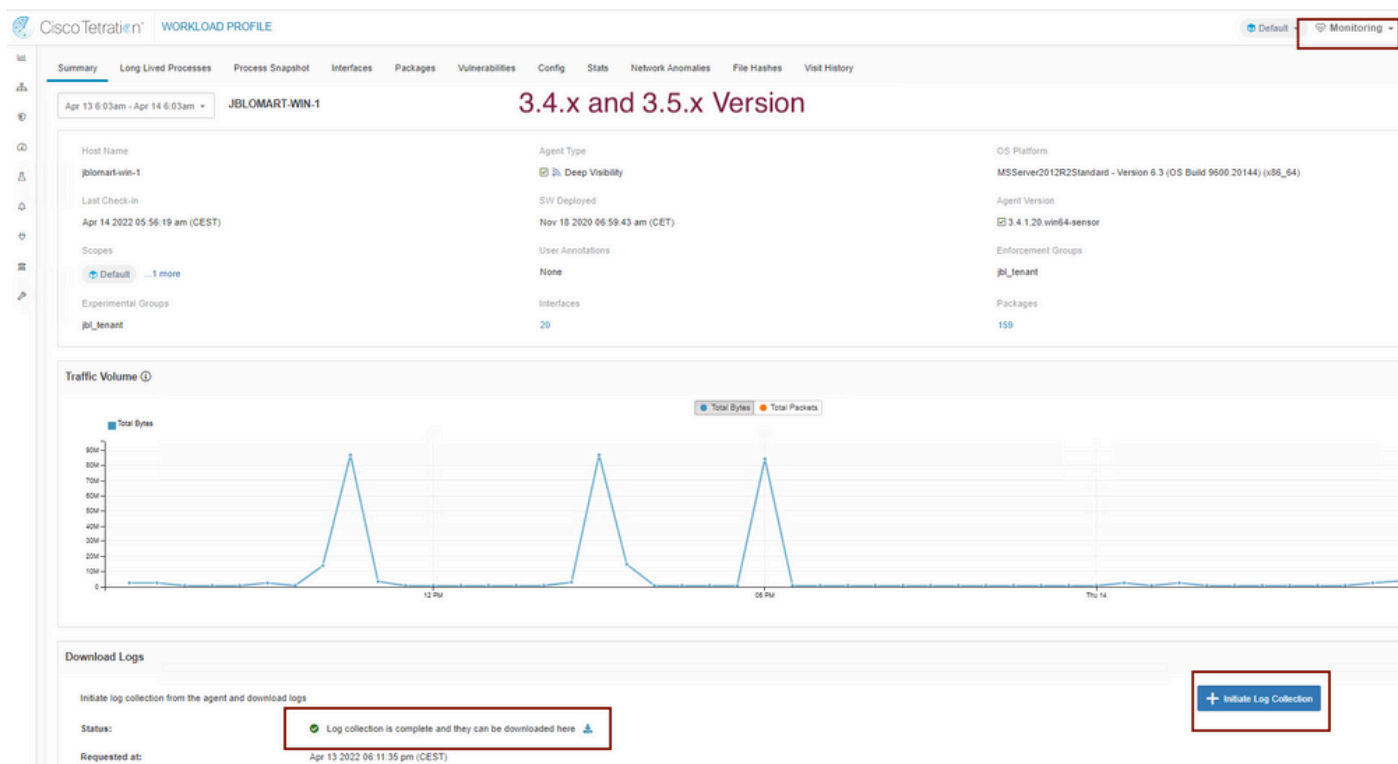
- 对于3.6.x版本，导航至左侧导航面板，选择Manage > Agent，然后单击Agent List。
- 对于3.4.x和3.5.x版本，请从右上角下拉菜单中导航到Monitoring，然后选择Agent List。

使用过滤器选项搜索代理，然后单击代理。该选项将您转到代理的工作负载配置文件。您可以在此处找到有关代理配置的详细信息。

状态，等等。

在工作负载配置文件页面(3.6.x)的左侧导航面板上，选择下载日志 (在3.4.x和3.5.x中，然后点击“摘要”选项卡)。单击Initiate Log Collection从Tetration Agent启动日志收集。完成日志收集可能需要一些时间。日志收集完成后，单击Download以下载日志选项。向下滚动以获取将文件上传到案例编号的选项。

请参阅此映像，为3.4.x和3.5.x版本上运行的代理创建安全工作负载代理日志捆绑包。



请参阅此映像，以创建从3.6.x版本开始的安全工作负载代理日志捆绑包

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。