Problemen met Windows Agent oplossen met het hulpprogramma voor probleemoplossing van de Agent

Inhoud

Inleiding

In dit document wordt beschreven hoe u het ingebouwde PowerShell-script van het hulpprogramma voor probleemoplossing van de agent kunt gebruiken om veelvoorkomende problemen met de Windows-agent op te lossen.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

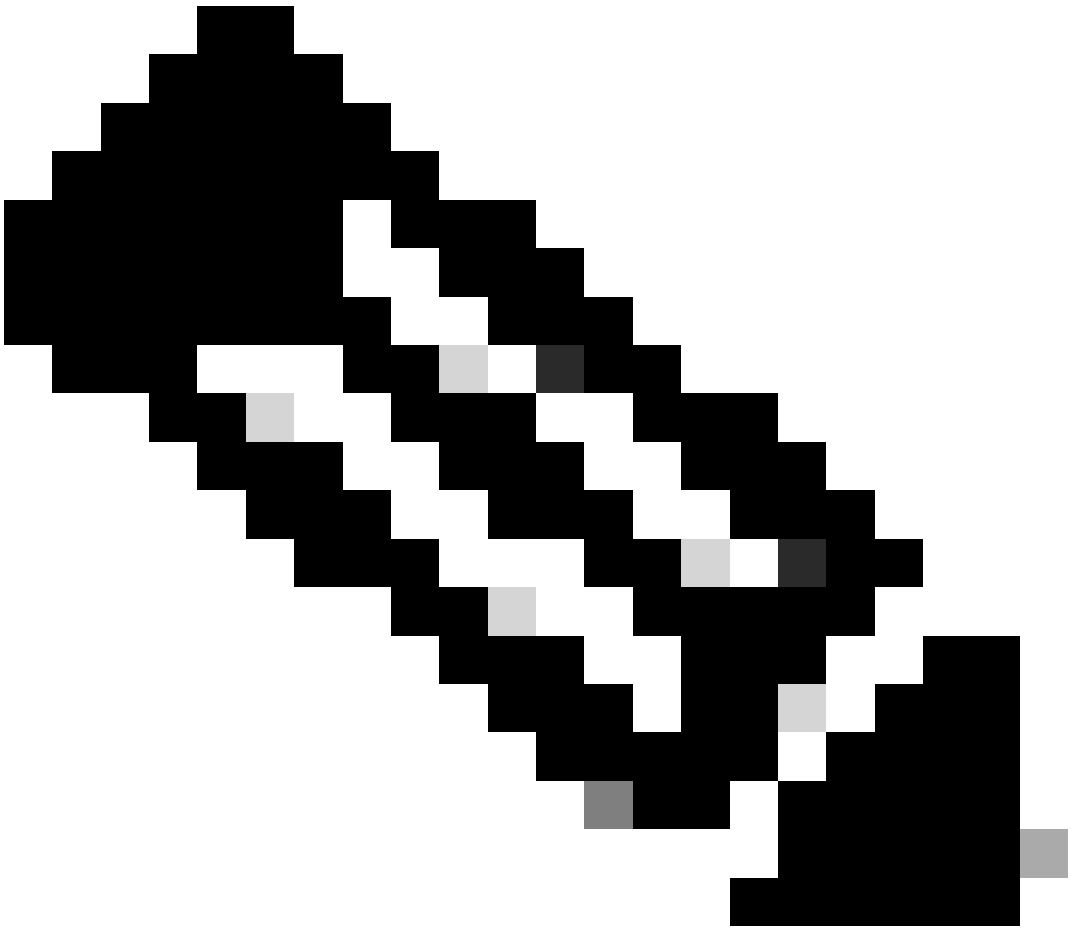
- PowerShell versie 4.0

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een

opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Het script van de Agent-tool voor probleemoplossing wordt geleverd met verschillende opties waarmee u de algehele gezondheid van uw agents kunt controleren, bekende problemen met de registratie van agents, bekende problemen met agent-upgrades, de algehele handhavingsstatus kunt controleren en logboeken kunt verzamelen voor verdere analyse.



Opmerking: de Agent Troubleshooting Tool wordt geleverd met de agent die begint in versie 3.9. Voor versies ouder dan 3.9 is deze standaard niet inbegrepen. Als u een versie vóór 3.9 gebruikt, kunt u het script kopiëren van een Windows-systeem waarop de 3.9-agent is geïnstalleerd en plakken in (C:\Program Files\Cisco Tetration) om het hulpprogramma voor probleemoplossing te gebruiken.

Stappen om het script uit te voeren

Voer de volgende stappen uit om het script van het hulpprogramma Agent voor probleemoplossing uit te voeren:

1. Open PowerShell als beheerder.

2. Navigeer naar de installatiemap van CSW (standaardlocatie: C:\ Program Files \Cisco Tetration).

3. Voer het script uit met deze opdracht:

.\AgentTroubleshootingTool.psl

Lijst met parameters die beschikbaar zijn in dit agentscript voor probleemoplossing

Het hulpprogramma voor probleemoplossing voor agents wordt geleverd met verschillende opties waarmee u problemen met verschillende aspecten van uw agents kunt oplossen.
Hier zijn de beschikbare opties:

-agentHealth: controlerapport agent uitvoeren
-agentRegistration: controleren op problemen in Agent Registration
-agentUpgrade: controleren op problemen met agent-upgrade
-HandhavingGezondheid: controleren op problemen met handhaving
-collectLogs: verzamel Logs voor foutopsporing
-collectDebugLogs: verzamel logs met logniveau:5 ingeschakeld. Dit omvat ook logs die zijn verzameld met de parameter -collectLogs
-all: alle parameters uitvoeren behalve -collectDebugLogs

Als u een van deze opties wilt gebruiken, voert u het script uit met de juiste parameter.
Als u bijvoorbeeld de status van uw agents wilt controleren, voert u het script uit met de parameter -agentHealth:

.\AgentTroubleshootingTool.ps1 -agentHealth

Parameterdetails -agentHealth

Onder de parameter -agentHealth controleert u deze dingen:

1. Services TetSensor en TetEnforcer bevinden zich in een actieve toestand.
2. Sensor-ID is geldig
3. PATH-variabele bevat 'C:\ Windows\System32'

4. De agent gebruikt ETW of NPCAP. Als het besturingssysteem 2008R2 is, controleert u NPCAP Health.

Backend connectiviteit met onze collectors/EFEs en WSS is goed.

Hier is een voorbeeld van de scriptuitvoer wanneer u het script uitvoert met -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!!!
```

Parametergegevens -agentRegistration

Onder de parameter -agentRegistration controleert u deze dingen:

1. Het bevat het rapport dat is verzameld met behulp van de parameter -agentHealth.
2. Registratiefouten zijn gebaseerd op foutcodes, bijvoorbeeld 401/403, en anderen.

Er is ook een optie voorzien om de agent opnieuw te registreren bij het cluster als deze per ongeluk uit de gebruikersinterface wordt verwijderd.

Hier is een voorbeeld van de scriptuitvoer wanneer u het script uitvoert met de -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!!!
```

Parameterdetails -agentUpgrade

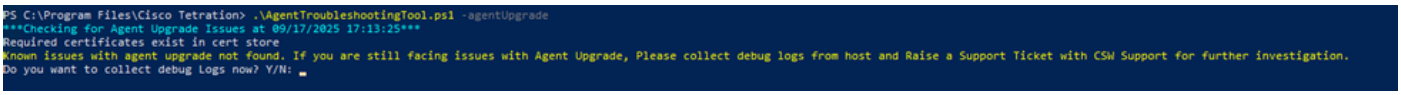
Onder de parameter -agentUpgrade controleert u deze dingen:

1. Vereiste certificaten zijn beschikbaar in de winkel.
2. De MSI-cache is beschikbaar onder de map C: \ Windows \Installer.

Als er geen bekende problemen worden gevonden, maar de agent-upgrade nog steeds mislukt, biedt u de optie om debug-logs te verzamelen voor verdere probleemoplossing.

Hier is een voorbeeld van de scriptuitvoer wanneer u met -agentUpgrade wordt uitgevoerd parameter

.\AgentTroubleshootingTool.ps1 -agentUpgrade



Parameterdetails -enforcementHealth

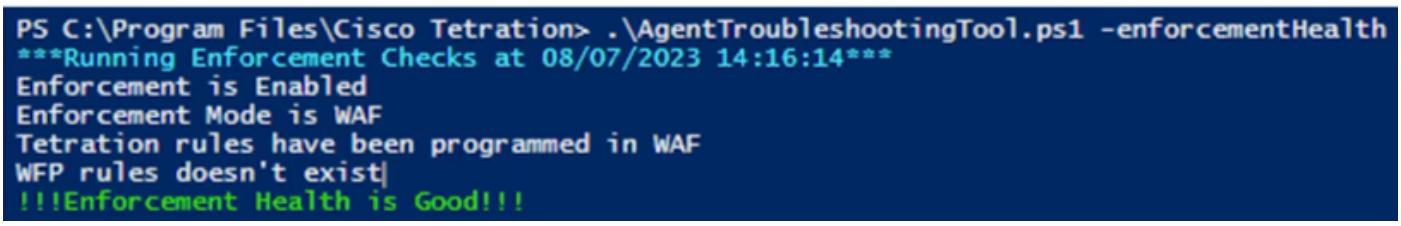
Onder de parameter -enforcementHealth controleert u deze dingen:

1. Handhaving is ingeschakeld of uitgeschakeld.
2. Welke modus voor handhaving is ingeschakeld.
3. CSW-regels zijn geprogrammeerd in WAF of WFP-filters zijn geprogrammeerd.
4. CSW WFP-filters bestaan niet (wanneer de modus WAF is).
5. CSW WAF-regels bestaan niet (wanneer de modus WFP is).

Stap 4 en 5 zijn bedoeld om problemen te identificeren wanneer de handhavingsmodus is ingeschakeld.

Hier is een voorbeeld van de scriptuitvoer wanneer u het script uitvoert met de -enforcementHealth parameter.

.\AgentTroubleshootingTool.ps1 -enforcementHealth



Parameterdetails -collectLogs

Het script verzamelt logs voor debugging doeleinden wanneer uitgevoerd met de -collectLogs parameter.

Verzamelde logs kunnen worden opgeslagen onder het pad C:\ Program Files \Cisco Tetration\logs\logs\Troubleshoot_Logs

Hier is een voorbeeld van de scriptuitvoer wanneer u het script uitvoert met de -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>
```

Parameterdetails -collectDebugLogs

Het script verzamelt logs met logniveau:5 ingeschakeld voor debugging doeleinden wanneer u met de -collectDebugLogs parameter.

Als u het script met deze parameter uitvoert, wordt de netsh-trace vastgelegd en kan de CSW-agent opnieuw worden gestart.
Verzamelde logs kunnen worden opgeslagen onder het pad C:\ Program Files \Cisco Tetration\logs\logs\Troubleshoot_Logs

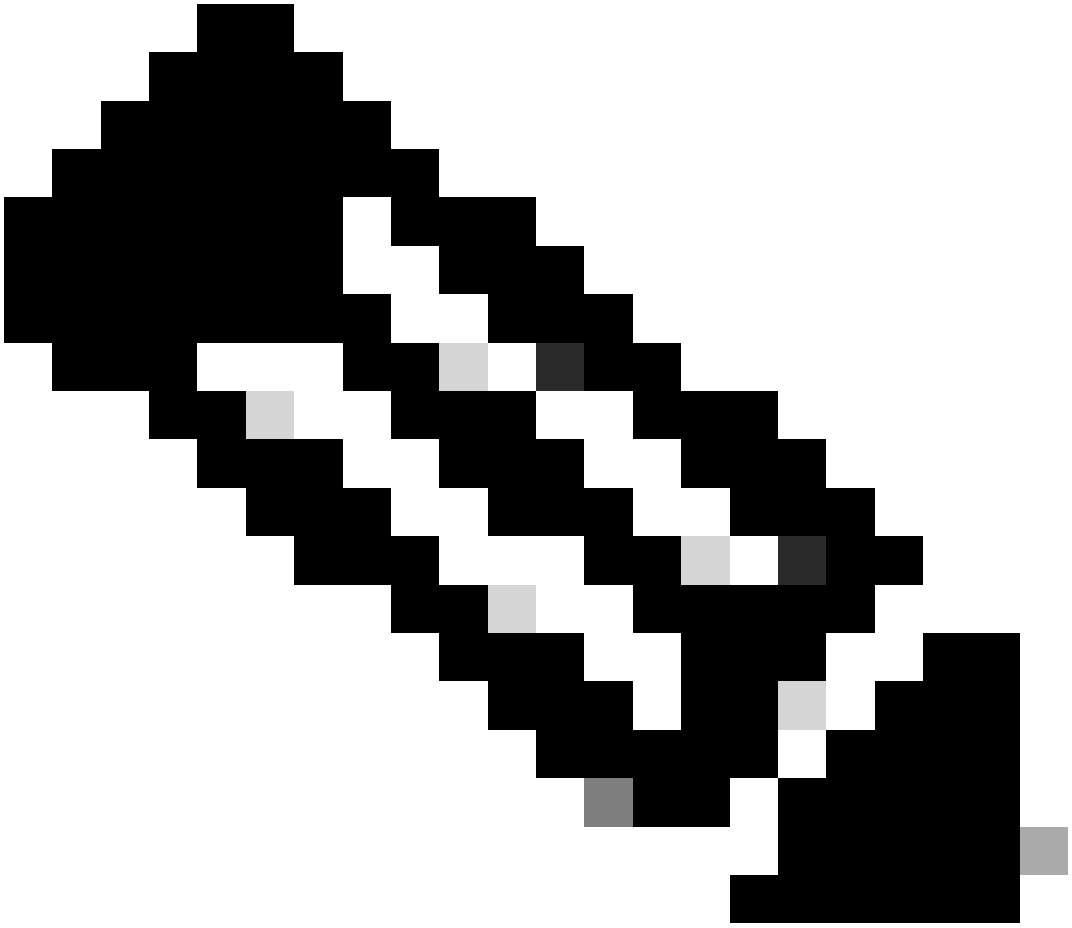
Hier is een voorbeeld van de scriptuitvoer wanneer u het script uitvoert met de -collectDebugLogs parameter.

.\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>
```



Opmerking: met het hulpprogramma Agent voor probleemoplossing worden fouten in rode kleur en waarschuwingen in gele kleur weergegeven. Als u de veelvoorkomende problemen die door Agent Troubleshooting Tool zijn gemarkeerd, niet kunt oplossen, verzamelt u foutopsporingslogboeken met de Agent Troubleshooting Tool en genereert u een logbundel voor de Secure Workload Agent en neemt u contact op met Cisco TAC voor hulp.

De logbundel van de Secure Workload Agent genereren

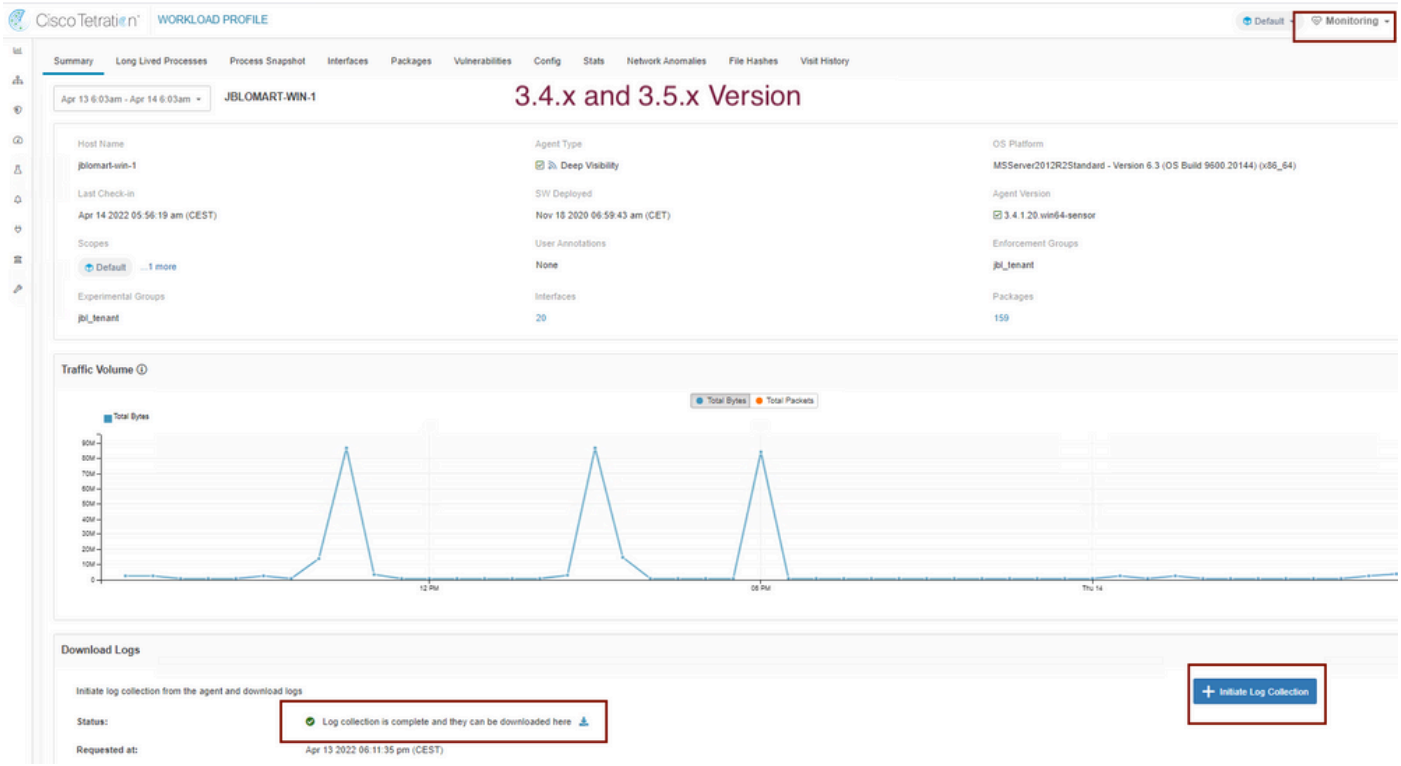
Om de logbundel te verzamelen, moet de agent voor de veilige werklast actief zijn.

- Voor de 3.6.x-versie navigeert u naar het linkernavigatiedeelvenster, kiest u Beheren > Agent en klikt u op Agentlijst.
- Navigeer voor de versies 3.4.x en 3.5.x naar Monitoring in het vervolgkeuzemenu rechtsboven en kies Agentenlijst.

Gebruik de filteroptie om naar de agent te zoeken en klik op de agent. Het brengt u naar het werklastprofiel van de agent. Hier vindt u informatie over de configuratie van de agent, status, enzovoort.

Kies in het linkernavigatiepaneel van de pagina Werklastprofiel (3.6.x) de optie Logbestanden downloaden (in de 3.4.x en 3.5.x en volg het tabblad Overzicht). Klik op Logboekverzameling starten om de logboekverzameling vanuit de Tetration Agent te starten. Het kan enige tijd duren voordat de logboekverzameling is voltooid. Zodra de logboekverzameling is voltooid, klikt u op de optie Hier downloaden om de logboeken te downloaden. Scroll naar beneden om een optie te krijgen om het bestand naar het zaaknummer te uploaden.

Raadpleeg dit image om de Secure Workload Agent-logbundel te maken voor agents die op 3.4.x- en 3.5.x-versies worden uitgevoerd.



Raadpleeg dit image om de Secure Workload Agent-logbundel te maken vanaf versie 3.6.x 

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.