Beheben von Problemen mit dem Windows-Agent mithilfe des Tools zur Behebung von Agentenproblemen

Inhalt

Einleitung

Voraussetzungen

- Anforderungen
- Verwendete Komponenten

Hintergrundinformationen

Schritte zum Ausführen des Skripts

Liste der verfügbaren Parameter in diesem Tool-Skript zur Behebung von Agentenfehlern

- Parameterdetails -agentHealth
- Parameterdetails -agentRegistration
- Parameterdetails -agentUpgrade
- Parameter-Details -enforcementHealth
- Parameter-Details -collectLogs
- Parameter Details-collectDebugLogs

Protokollpaket des sicheren Workload-Agenten generieren

Einleitung

In diesem Dokument wird beschrieben, wie Sie das integrierte Tool zur Fehlerbehebung für Agenten und das PowerShell-Skript verwenden, um häufige Probleme mit dem Windows-Agent zu beheben.

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

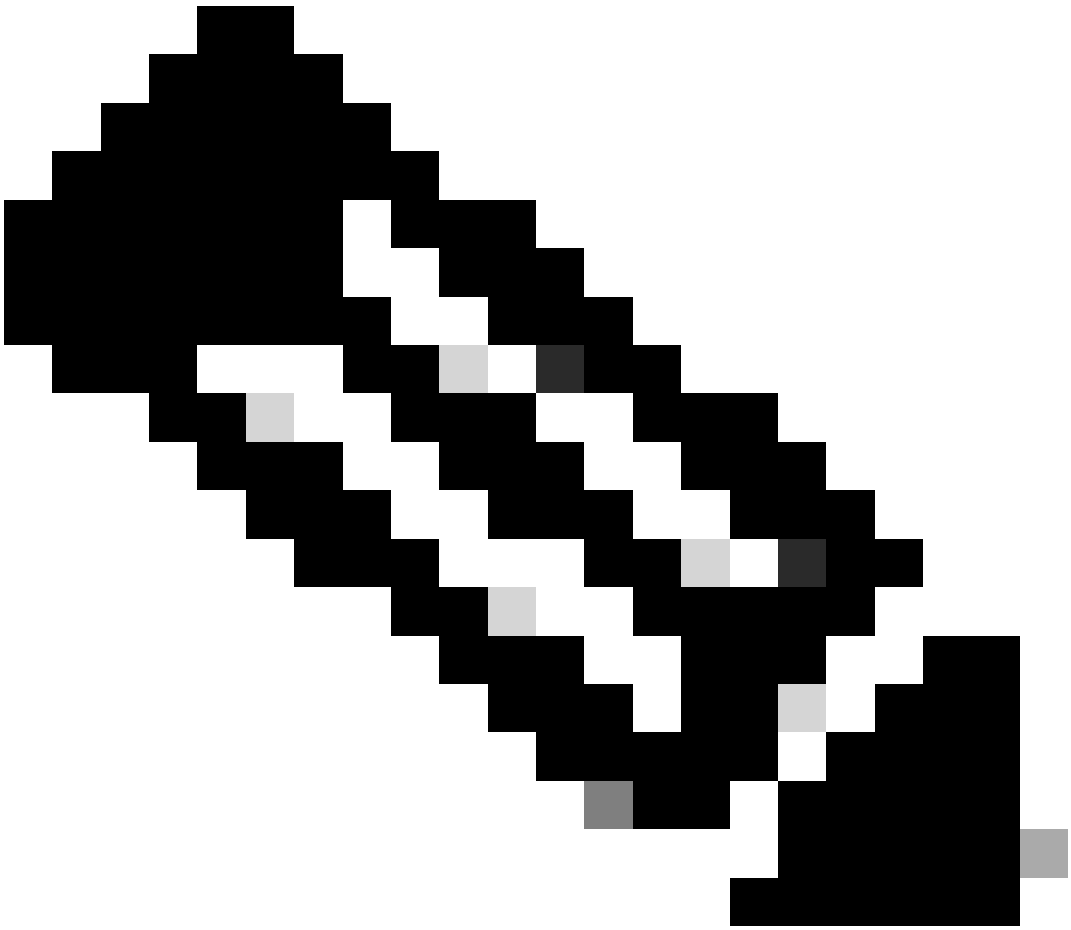
- PowerShell Version 4.0

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten

Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Das Tool-Skript zur Behebung von Agentenfehlern enthält mehrere Optionen, mit denen Sie den Gesamtzustand Ihrer Agenten, bekannte Probleme bei der Agentenregistrierung, bekannte Probleme bei Agent-Upgrades, den Gesamtzustand der Durchsetzung überprüfen und Protokolle für weitere Analysen sammeln können.



Anmerkung: Das Agent Troubleshooting Tool wird ab Version 3.9 mit dem Agent ausgeliefert. Bei älteren Versionen als 3.9 ist es nicht standardmäßig enthalten. Wenn Sie eine Version vor 3.9 verwenden, können Sie das Skript von einem Windows-Computer mit installiertem 3.9-Agent kopieren und in (C:\Program Files\Cisco Tetration) einfügen, um das Tool zur Fehlerbehebung zu verwenden.

Schritte zum Ausführen des Skripts

Um das Tool-Skript zur Fehlerbehebung für Agenten auszuführen, gehen Sie wie folgt vor:

1. Öffnen Sie PowerShell als Administrator

2. Navigieren Sie zum CSW-Installationsverzeichnis (Standardspeicherort: C:\ Program Files \Cisco Tetration).

3. Führen Sie das Skript mit dem folgenden Befehl aus:

.\AgentTroubleshootingTool.psl

Liste der verfügbaren Parameter in diesem Tool-Skript zur Behebung von Agentenfehlern

Das Tool zur Fehlerbehebung für Agenten bietet verschiedene Optionen, mit denen Sie verschiedene Aspekte Ihrer Agenten beheben können.
Folgende Optionen stehen zur Verfügung:

-agentGesundheit: Integritätsbericht für Ausführungsagenten
-agentRegistrierung: Prüfung auf Probleme bei der Agent-Registrierung
-agentUpgrade: Prüfung auf Probleme mit Agent-Upgrade
-DurchsetzungGesundheit: Prüfung auf Probleme mit der Durchsetzung
-collectLogs: Protokolle zum Debuggen sammeln
-collectDebugLogs: Protokolle mit aktivierter Protokollebene sammeln:5. Dazu gehören auch Protokolle, die mit dem Parameter -collectLogs erfasst werden.
Alle: Alle Parameter außer -collectDebugLogs ausführen

Um eine dieser Optionen zu verwenden, führen Sie einfach das Skript mit dem entsprechenden Parameter aus.
Führen Sie beispielsweise das Skript mit dem Parameter -agentHealth aus, um die Integrität Ihrer Agenten zu überprüfen:

.\AgentTroubleshootingTool.ps1 -agentHealth

Parameterdetails -agentHealth

Unter dem Parameter -agentHealth überprüfen Sie Folgendes:

1. Dienste TestSensor und TestEnforcer befinden sich im Ausführungszustand.
2. Sensor-ID ist gültig
3. PATH-Variable enthält 'C:\ Windows\System32'

4. Der Agent verwendet ETW oder NPCAP. Wenn das Betriebssystem 2008R2 ist, überprüfen Sie den NPCAP-Zustand.

Die Backend-Konnektivität mit unseren Collectors/EFEs und WSS ist gut.

Hier ist ein Beispiel für die Skriptausgabe, wenn Sie das Skript mit dem Befehl -agentHealth ausführen. 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!!!
```

Parameterdetails -agentRegistration

Unter dem Parameter -agentRegistration überprüfen Sie Folgendes:

1. Er enthält den Bericht, der mit dem Parameter -agentHealth gesammelt wurde.
2. Registrierungsfehler basieren auf Fehlercodes wie 401/403 und anderen.

Es steht auch eine Option zur Verfügung, um den Agenten beim Cluster neu zu registrieren, wenn er versehentlich aus der Benutzeroberfläche gelöscht wird.

Hier ist ein Beispiel für die Skriptausgabe, wenn Sie das Skript mit dem -agentRegistration ausführen. -Parameters.

.\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

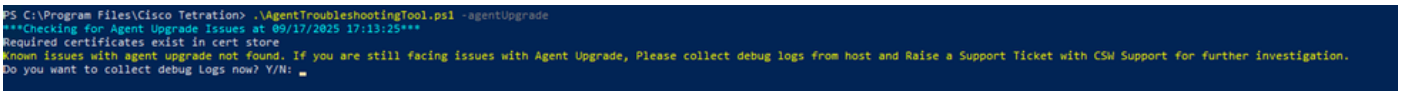
Unter dem Parameter -agentUpgrade überprüfen Sie Folgendes:

1. Erforderliche Zertifikate sind im Speicher verfügbar.
2. Der MSI-Cache ist unter C: \ Windows \Installer.

Wenn keine bekannten Probleme gefunden werden, das Agent-Upgrade jedoch weiterhin fehlschlägt, bieten Sie die Möglichkeit, Debug-Protokolle für die weitere Fehlerbehebung zu sammeln.

Hier ist ein Beispiel für die Skriptausgabe, wenn Sie mit dem -agentUpgrade ausführen. Parameter

.\AgentTroubleshootingTool.ps1 -agentUpgrade



Parameter-Details -enforcementHealth

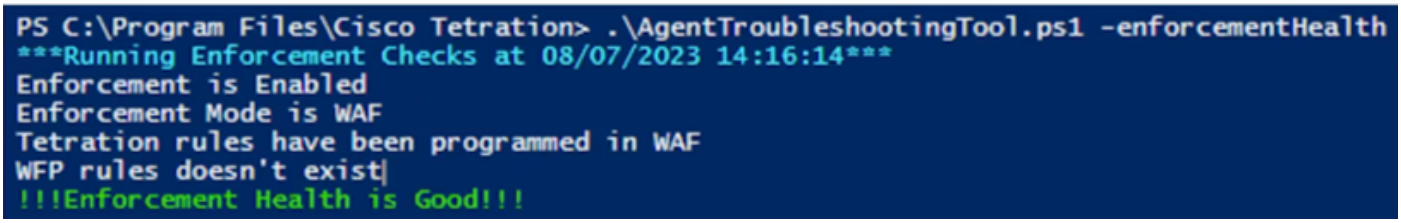
Unter dem Parameter -enforcementHealth überprüfen Sie Folgendes:

1. Die Durchsetzung ist aktiviert oder deaktiviert.
2. Aktivierter Durchsetzungsmodus.
3. CSW-Regeln wurden in WAF programmiert, oder WFP-Filter wurden programmiert.
4. CSW-WFP-Filter sind nicht vorhanden (im WAF-Modus).
5. Es sind keine CSW-WAF-Regeln vorhanden (im WFP-Modus).

Mit den Schritten 4 und 5 werden Probleme beim Umschalten des Erzwingungsmodus identifiziert.

Hier ist ein Beispiel für die Skriptausgabe, wenn Sie das Skript mit dem Befehl -enforcementHealth ausführen. -Parameters.

.\AgentTroubleshootingTool.ps1 -enforcementHealth



Parameter-Details -collectLogs

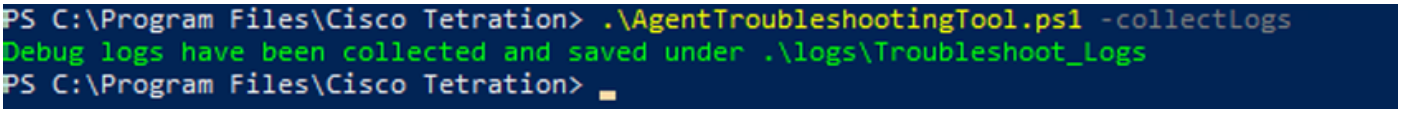
Das Skript sammelt Protokolle für Debugzwecke, wenn es mit dem -collectLogs-Parameter ausgeführt wird.

Die erfassten Protokolle können unter dem Pfad C:\ Program Files \Cisco

Tetration\logs\logs\Troubleshoot_Logs gespeichert werden.

Hier ist ein Beispiel für die Skriptausgabe, wenn Sie das Skript mit dem Befehl -collectLogs ausführen. -Parameters.

.\AgentTroubleshootingTool.ps1 -collectLogs



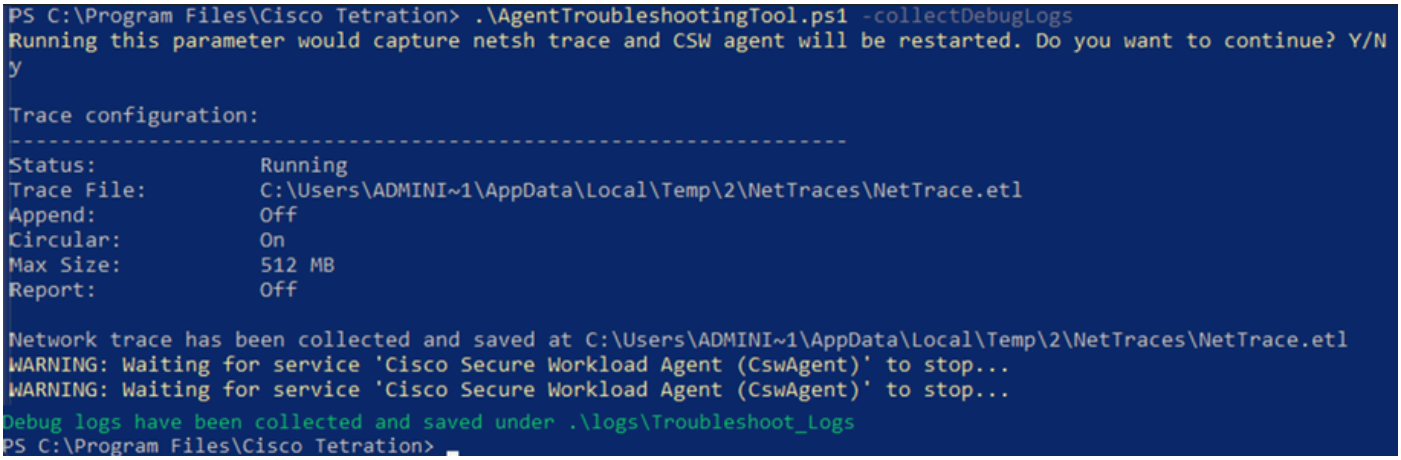
Parameterdetails - collectDebugLogs

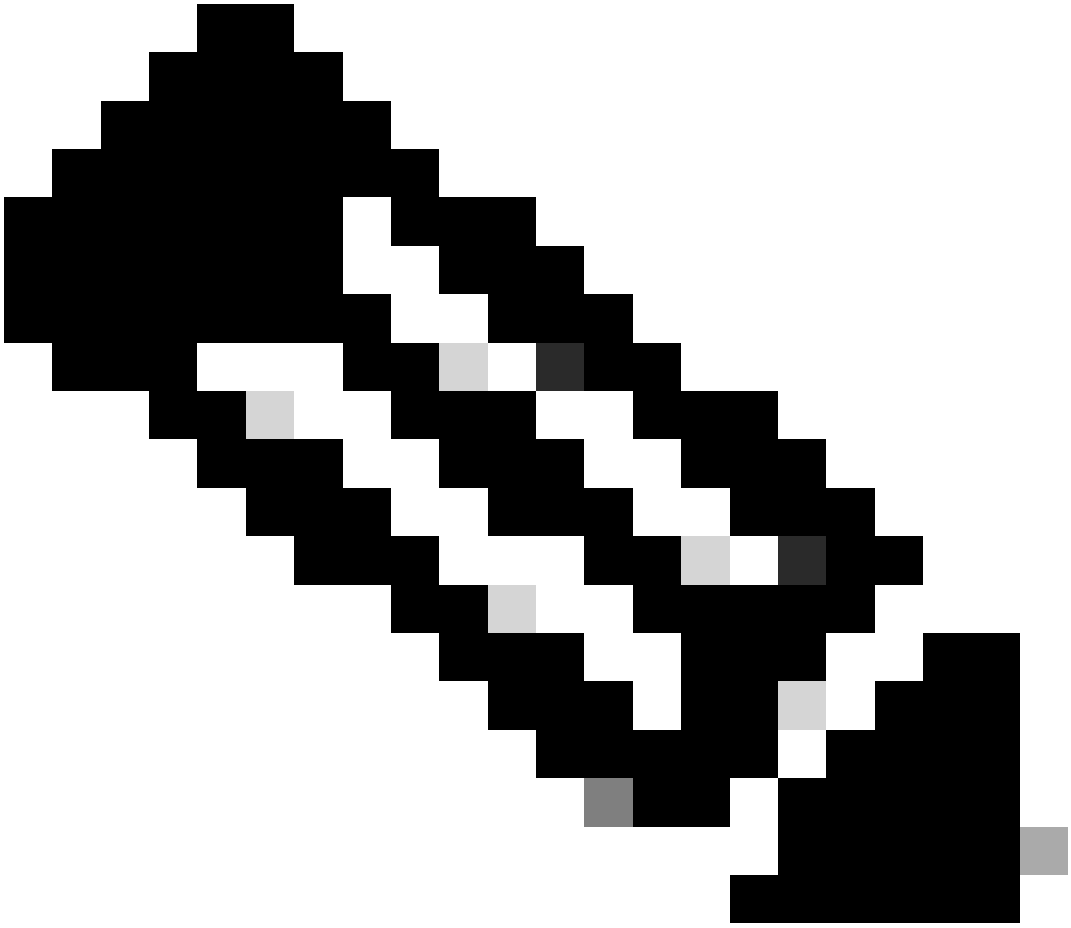
Das Skript sammelt Protokolle mit aktivierter Protokollstufe:5 für Debugzwecke, wenn Sie den -collectDebugLogs-Parameter verwenden.

Wenn Sie das Skript mit diesem Parameter ausführen, wird die netsh-Ablaufverfolgung erfasst, und der CSW-Agent kann neu gestartet werden.
Die erfassten Protokolle können unter dem Pfad C:\ Program Files \Cisco Tetration\logs\logs\Troubleshoot_Logs gespeichert werden.

Hier ist ein Beispiel für die Skriptausgabe, wenn Sie das Skript mit dem Befehl -collectDebugLogs ausführen. -Parameters.

.\AgentTroubleshootingTool.ps1 -collectDebugLogs





Anmerkung: Das Agent Troubleshooting Tool zeigt Fehler in roter und Warnungen in gelber Farbe an. Wenn Sie nicht in der Lage sind, die vom Agent Troubleshooting Tool gekennzeichneten häufigen Probleme zu beheben, sammeln Sie mithilfe des Agent Troubleshooting Tool Debugging-Protokolle, erstellen Sie ein Secure Workload Agent-Protokollpaket, und wenden Sie sich an Cisco TAC, um Unterstützung zu erhalten.

Protokollpaket des sicheren Workload-Agenten generieren

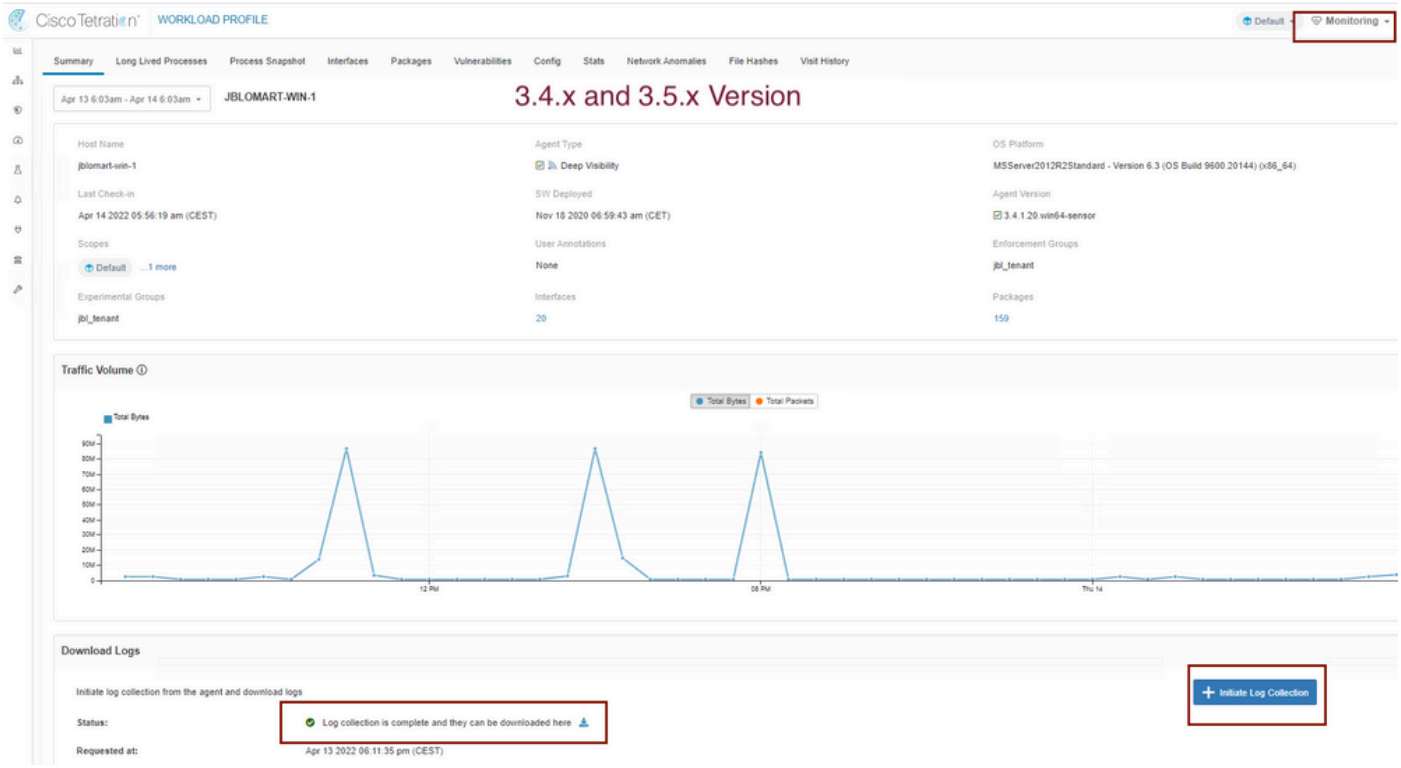
Um das Protokollpaket zu sammeln, muss der Secure Workload-Agent aktiv sein.

- Navigieren Sie für die Version 3.6.x zum linken Navigationsbereich, wählen Sie Verwalten > Agent, und klicken Sie auf Agentenliste.
- Navigieren Sie für die Versionen 3.4.x und 3.5.x aus dem Dropdown-Menü oben rechts zu Überwachung, und wählen Sie Agentenliste aus.

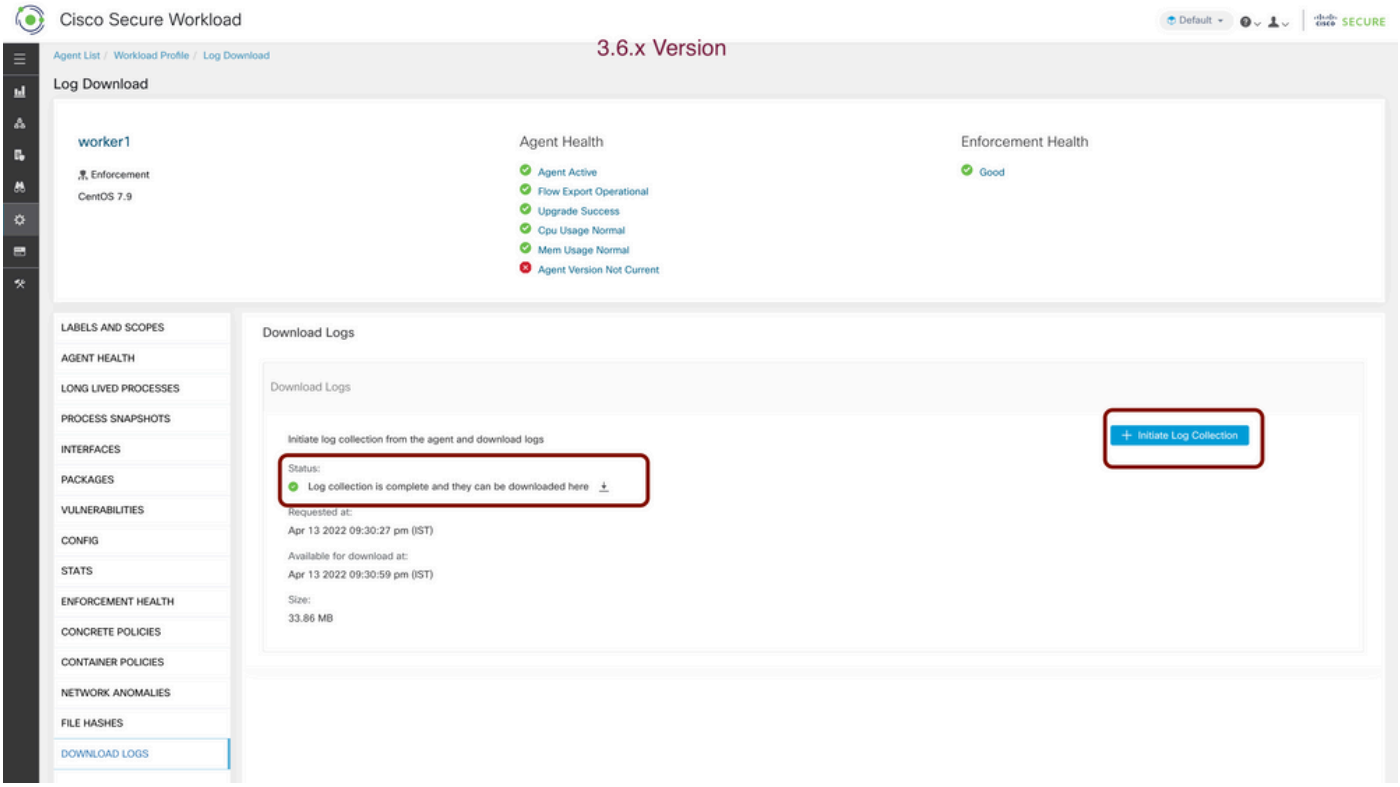
Verwenden Sie die Filteroption, um nach dem Agenten zu suchen, und klicken Sie auf den Agenten. Dadurch gelangen Sie zum Workload-Profil des Agenten. Hier finden Sie Details zur Agentenkonfiguration,
Status usw.

Wählen Sie im linken Navigationsbereich der Workload-Profilseite (3.6.x) die Option Download Logs (Protokolle herunterladen) (in den Versionen 3.4.x und 3.5.x, und folgen Sie der Registerkarte "Zusammenfassung"). Klicken Sie auf Protokollsammlung initiieren, um die Protokollsammlung vom Tetration Agent zu initiieren. Es kann eine Weile dauern, bis die Protokollsammlung abgeschlossen ist. Wenn die Protokollsammlung abgeschlossen ist, klicken Sie auf die Option Download here (Herunterladen), um die Protokolle herunterzuladen. Scrollen Sie nach unten, um eine Option zum Hochladen der Datei auf die Ticketnummer anzuzeigen.

Verwenden Sie dieses Image, um das Secure Workload Agent-Protokollpaket für Agents zu erstellen, die unter den Versionen 3.4.x und 3.5.x ausgeführt werden.



Verwenden Sie dieses Image, um das Secure Workload Agent-Protokollpaket ab Version 3.6.x zu erstellen.


Cisco Secure Workload
3.6.x Version
Default
SECURE
Agent List / Workload Profile / Log Download
Log Download
worker1
Enforcement
CentOS 7.9
Agent Health
Agent Active
Flow Export Operational
Upgrade Success
Cpu Usage Normal
Mem Usage Normal
Agent Version Not Current
Enforcement Health
Good
LABELS AND SCOPES
AGENT HEALTH
LONG LIVED PROCESSES
PROCESS SNAPSHOTS
INTERFACES
PACKAGES
VULNERABILITIES
CONFIG
STATS
ENFORCEMENT HEALTH
CONCRETE POLICIES
CONTAINER POLICIES
NETWORK ANOMALIES
FILE HASHES
DOWNLOAD LOGS
Download Logs
Download Logs
Initiate log collection from the agent and download logs
Initiate Log Collection
Status:
Log collection is complete and they can be downloaded here
Requested at:
Apr 13 2022 09:30:27 pm (IST)
Available for download at:
Apr 13 2022 09:30:59 pm (IST)
Size:
33.86 MB

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.