Résolution des problèmes liés à Windows Agent à l'aide de l'outil de dépannage Agent

Table des matières

Introduction

Ce document décrit comment utiliser le script PowerShell de l'outil de dépannage d'agent intégré pour résoudre les problèmes courants des agents Windows.

Conditions préalables

Exigences

Aucune exigence spécifique n'est associée à ce document.

Composants utilisés

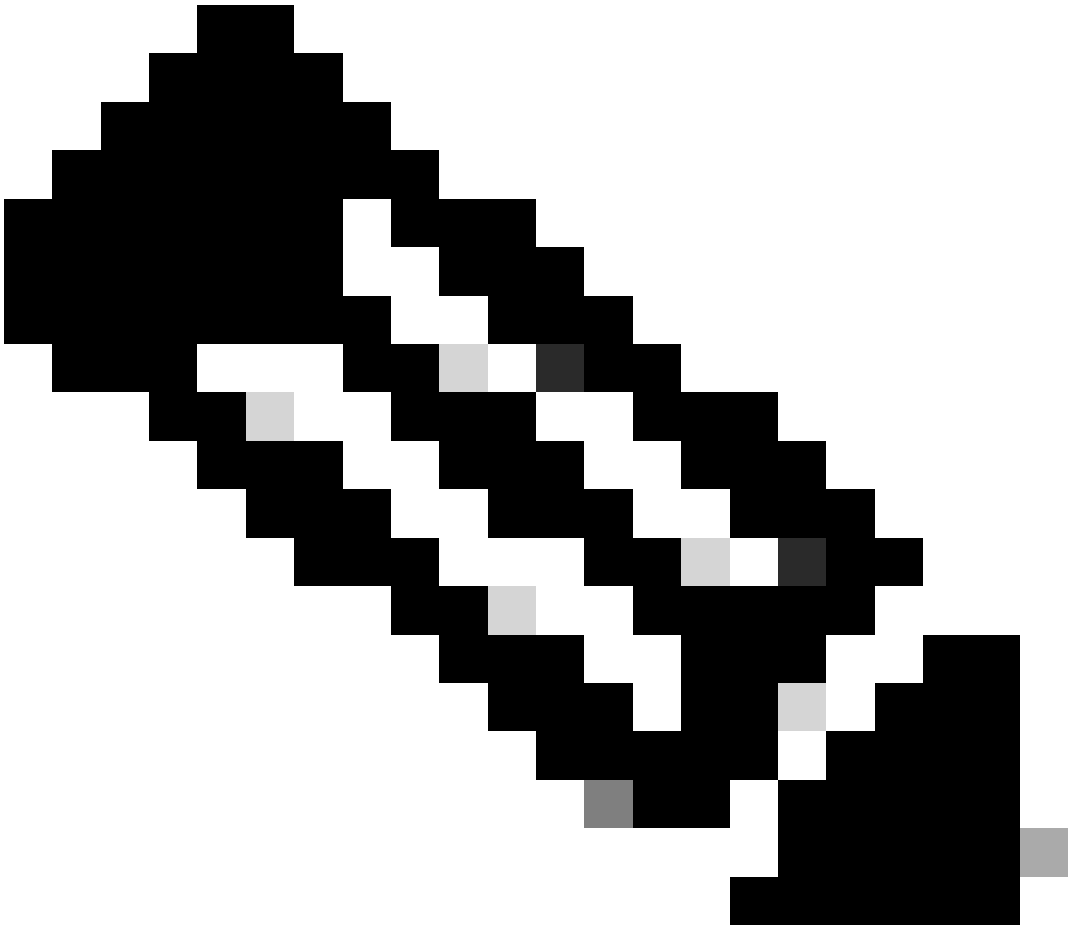
Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- 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. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Informations générales

Le script de l'outil de dépannage de l'agent est fourni avec plusieurs options qui vous permettent de vérifier l'intégrité globale de vos agents, les problèmes connus d'enregistrement des agents, les problèmes connus de mises à niveau des agents, de vérifier l'intégrité globale de l'application et de collecter des journaux pour une analyse plus approfondie.



> Remarque : L'outil de dépannage de l'agent est fourni avec l'agent à partir de la version 3.9. Pour les versions antérieures à la version 3.9, il n'est pas inclus par défaut. Si vous utilisez une version antérieure à la version 3.9, vous pouvez copier le script à partir d'une machine Windows sur laquelle l'agent 3.9 est installé et le coller dans (C:\Program Files\Cisco Tetration) pour utiliser l'outil de dépannage.

Étapes D'Exécution Du Script

Pour exécuter le script de l'outil de dépannage de l'agent, procédez comme suit :

1. Ouvrez PowerShell en tant qu'administrateur.

2. Accédez au répertoire d'installation de CSW (emplacement par défaut : C:\ Program Files \Cisco Tetration).

3. Exécutez le script à l'aide de cette commande :

.\AgentTroubleshootingTool.psl

Liste des paramètres disponibles dans ce script de l'outil de dépannage de l'agent

L'outil de dépannage Agent est fourni avec plusieurs options qui vous permettent de dépanner différents aspects de vos agents.
Voici les options disponibles :

-agentHealth : Exécuter le rapport d'intégrité agent
-agentEnregistrement : rechercher les problèmes dans l'enregistrement des agents
-agentUpgrade : rechercher les problèmes de mise à niveau de l'agent
-applicationSanté : vérifier les problèmes d'application
-collectLogs : Collecter les journaux pour le débogage
-collectDebugLogs : collectez les journaux avec loglevel:5 activé. Cela inclut également les journaux collectés à l'aide du paramètre -collectLogs
-tout : exécuter tous les paramètres sauf -collectDebugLogs

Pour utiliser l'une de ces options, exécutez simplement le script avec le paramètre approprié. Par exemple, pour vérifier l'intégrité de vos agents, exécutez le script avec le paramètre -agentHealth :

.\AgentTroubleshootingTool.ps1 -agentHealth

Détails du paramètre -agentHealth

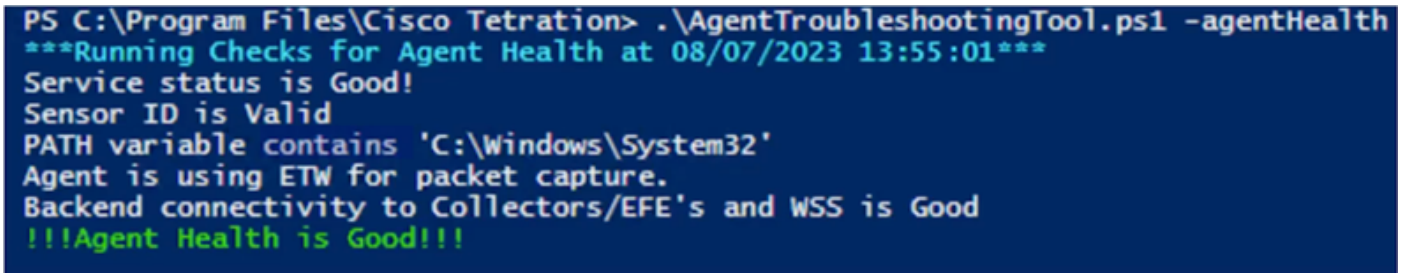
Sous le paramètre -agentHealth, vous vérifiez les éléments suivants :

1. Les services TetSensor et TetEnforcer sont en cours d'exécution.
2. L'ID du capteur est valide
3. La variable PATH contient « C:\ Windows\System32 »
4. L'agent utilise ETW ou NPCAP. Si le système d'exploitation est 2008R2, vous vérifiez l'intégrité de NPCAP.

La connectivité back-end avec nos collecteurs/EFE et WSS est bonne.

Voici un exemple de la sortie du script lors de l'exécution du script avec -agentHealth paramètre

.\AgentTroubleshootingTool.ps1 -agentHealth



Détails du paramètre -agentRegistration

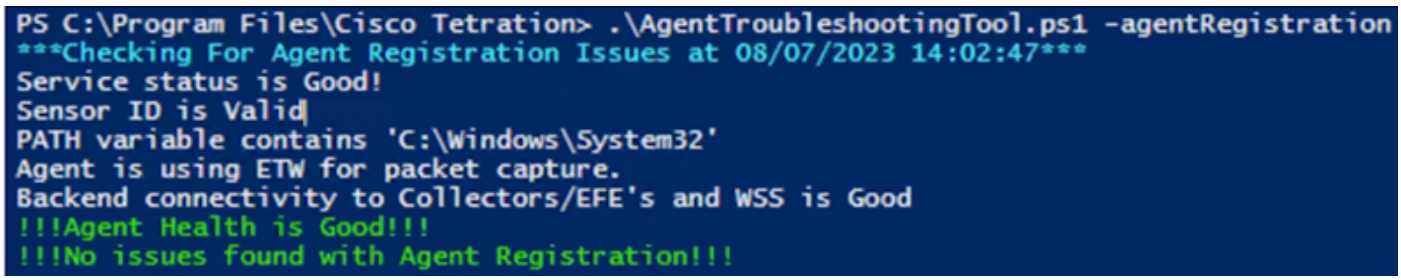
Sous le paramètre -agentRegistration, vous vérifiez les éléments suivants :

1. Il inclut le rapport collecté à l'aide du paramètre -agentHealth.
2. Les erreurs d'enregistrement sont basées sur des codes d'erreur, par exemple 401/403 et autres.

Il existe également une option permettant de réenregistrer l'agent avec le cluster s'il est supprimé de l'interface utilisateur par erreur.

Voici un exemple de la sortie du script lorsque vous exécutez le script avec -agentRegistration paramètre.

.\AgentTroubleshootingTool.ps1 -agentRegistration



Détails du paramètre -agentUpgrade

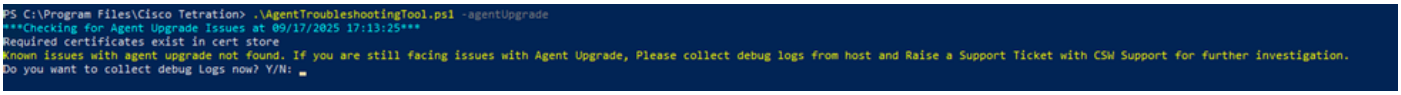
Sous le paramètre -agentUpgrade, vous vérifiez les éléments suivants :

1. Les certificats requis sont disponibles dans le magasin.
2. Le cache MSI est disponible sous le lecteur C: \ Dossier Windows \Installer.

Si aucun problème connu n'est détecté, mais que la mise à niveau de l'agent échoue toujours, vous pouvez collecter des journaux de débogage pour un dépannage plus approfondi.

Voici un exemple de la sortie du script lorsque vous exécutez avec -agentUpgrade paramètre

.\AgentTroubleshootingTool.ps1 -agentUpgrade



Détails du paramètre -enforcementHealth

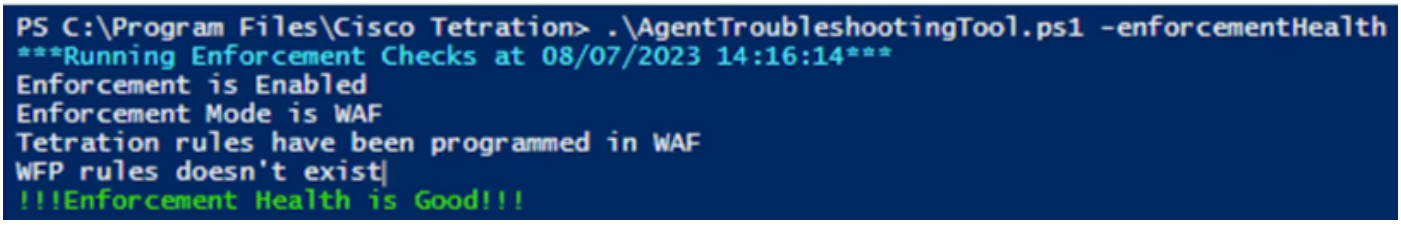
Sous le paramètre -enforcementHealth, vous vérifiez les éléments suivants :

1. L'application est activée ou désactivée.
2. Quel mode d'application est activé ?
3. Les règles CSW ont été programmées dans WAF ou les filtres WFP ont été programmés.
4. Les filtres WFP CSW n'existent pas (lorsque le mode est WAF).
5. Les règles WAF de CSW n'existent pas (lorsque le mode est WFP).

Les étapes 4 et 5 permettent d'identifier les problèmes lors du basculement du mode d'application.

Voici un exemple de la sortie du script lorsque vous exécutez le script avec l'option -enforcementHealth paramètre.

.\AgentTroubleshootingTool.ps1 -enforcementHealth



Détails du paramètre -collectLogs

Le script collecte les journaux à des fins de débogage lorsqu'il est exécuté avec le paramètre -collectLogs.

Les journaux collectés peuvent être enregistrés sous le chemin C:\ Program Files \Cisco Tetration\logs\logs\Troubleshoot_Logs

Voici un exemple de la sortie du script lorsque vous exécutez le script avec -collectLogs paramètre.

.\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>
```

Détails du paramètre -collectDebugLogs

Le script collecte les journaux avec loglevel : 5 activé à des fins de débogage lorsque vous exécutez avec le paramètre -collectDebugLogs.

L'exécution du script avec ce paramètre capturerait la trace netsh et l'agent CSW pourrait être redémarré.
Les journaux collectés peuvent être enregistrés sous le chemin C:\ Program Files \Cisco Tetration\logs\logs\Troubleshoot_Logs

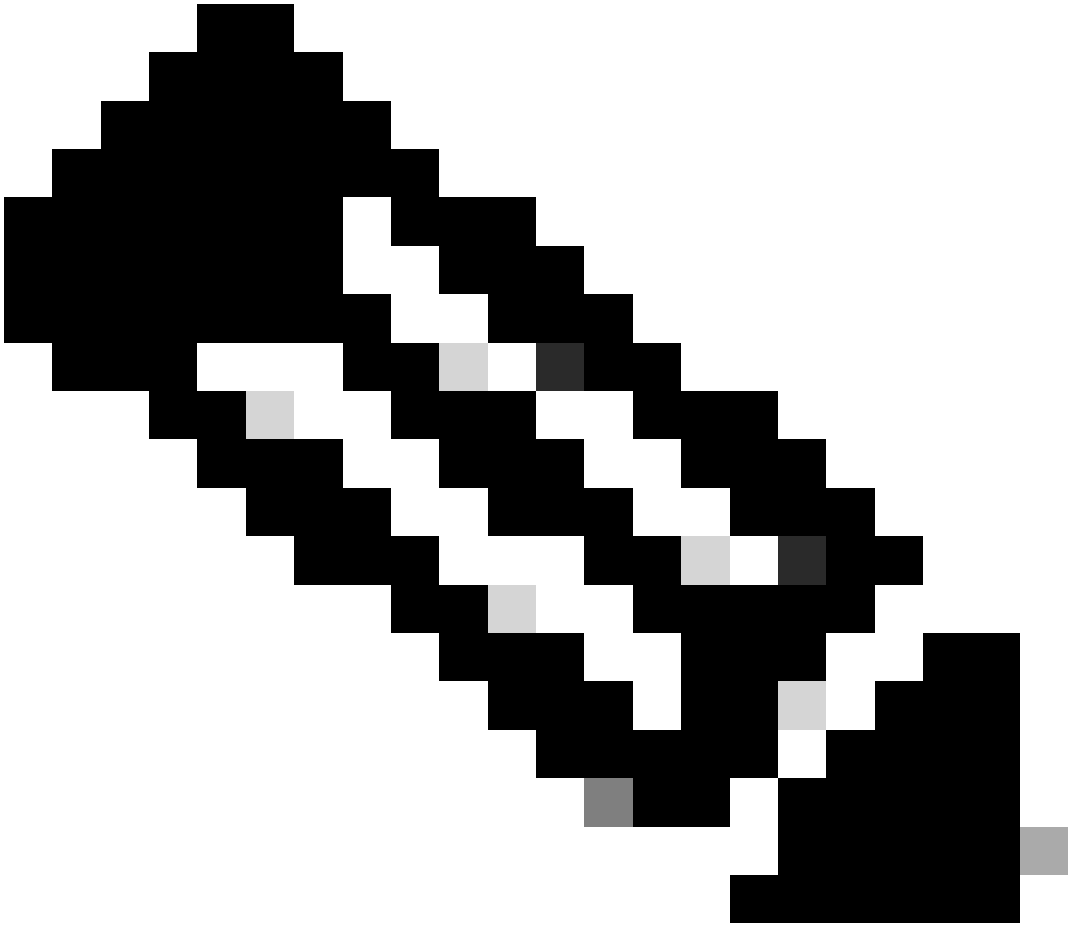
Voici un exemple de la sortie du script lorsque vous exécutez le script avec -collectDebugLogs paramètre.

.\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>
```



Remarque : L'outil de dépannage de l'agent affiche les erreurs en rouge et les avertissements en jaune. Si vous ne parvenez pas à résoudre les problèmes courants signalés par l'outil de dépannage d'agent, collectez les journaux de débogage à l'aide de l'outil de dépannage d'agent, générez un ensemble de journaux d'agent de charge de travail sécurisée et contactez le TAC Cisco pour obtenir de l'aide.

Générer l'offre groupée de journaux de Secure Workload Agent

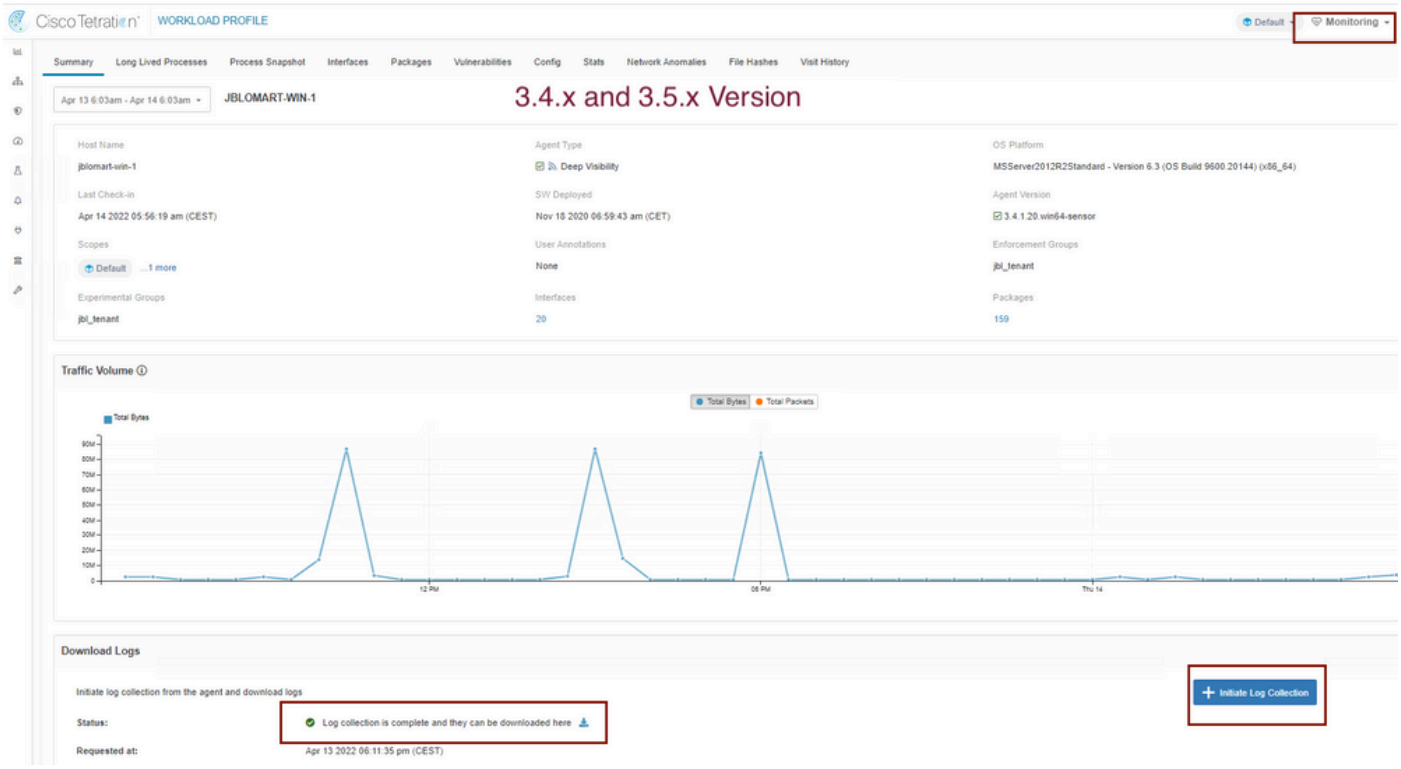
Pour collecter le lot de journaux, l'agent de charge globale sécurisée doit être actif.

- Pour la version 3.6.x, naviguez jusqu'au panneau de navigation gauche, choisissezManage > Agent, et cliquez sur Agent List.
- Pour les versions 3.4.x et 3.5.x, accédez à Surveillance dans le menu déroulant en haut à droite et choisissez Liste d'agents.

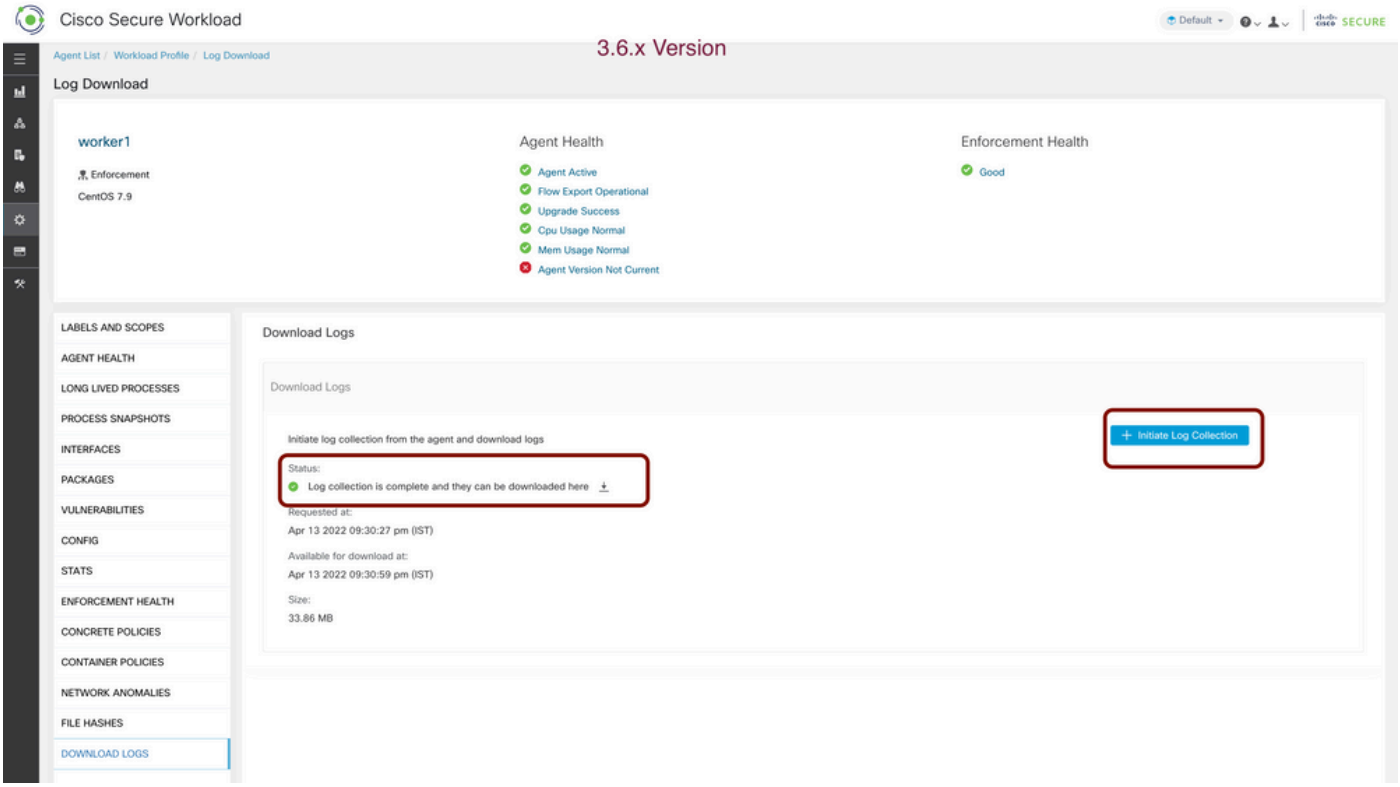
Utilisez l'option de filtre pour rechercher l'agent, puis cliquez sur l'agent. Elle vous amène au profil de charge globale de l'agent. Vous trouverez ici des informations détaillées sur la configuration de l'agent,
état, etc.

Dans le volet de navigation latéral gauche de la page de profil de charge de travail (3.6.x), choisissez Download Logs (dans les versions 3.4.x et 3.5.x et suivez l'onglet de résumé). Cliquez sur Initiate Log Collection pour lancer la collecte de journaux à partir de l'agent de tétration. La collecte du journal peut prendre un certain temps. Une fois la collecte des journaux terminée, cliquez sur l'option Télécharger ici pour télécharger les journaux. Faites défiler la page vers le bas pour obtenir une option permettant de télécharger le fichier vers le numéro de dossier.

Reportez-vous à cette image pour créer l'offre groupée de journaux d'agent de charge globale sécurisée pour les agents s'exécutant sur les versions 3.4.x et 3.5.x.



Reportez-vous à cette image pour créer l'ensemble de journaux de l'agent de charge globale sécurisée à partir de la version 3.6.x


Cisco Secure Workload
3.6.x Version
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

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.