Agent Troubleshooting Toolを使用した、Windowsエージェントの問題のトラブルシューティング

内容

はじめに

このドキュメントでは、組み込みのAgent Troubleshooting Tool(AOT)PowerShellスクリプトを使用して、一般的なWindowsエージェントの問題を解決する方法について説明します。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

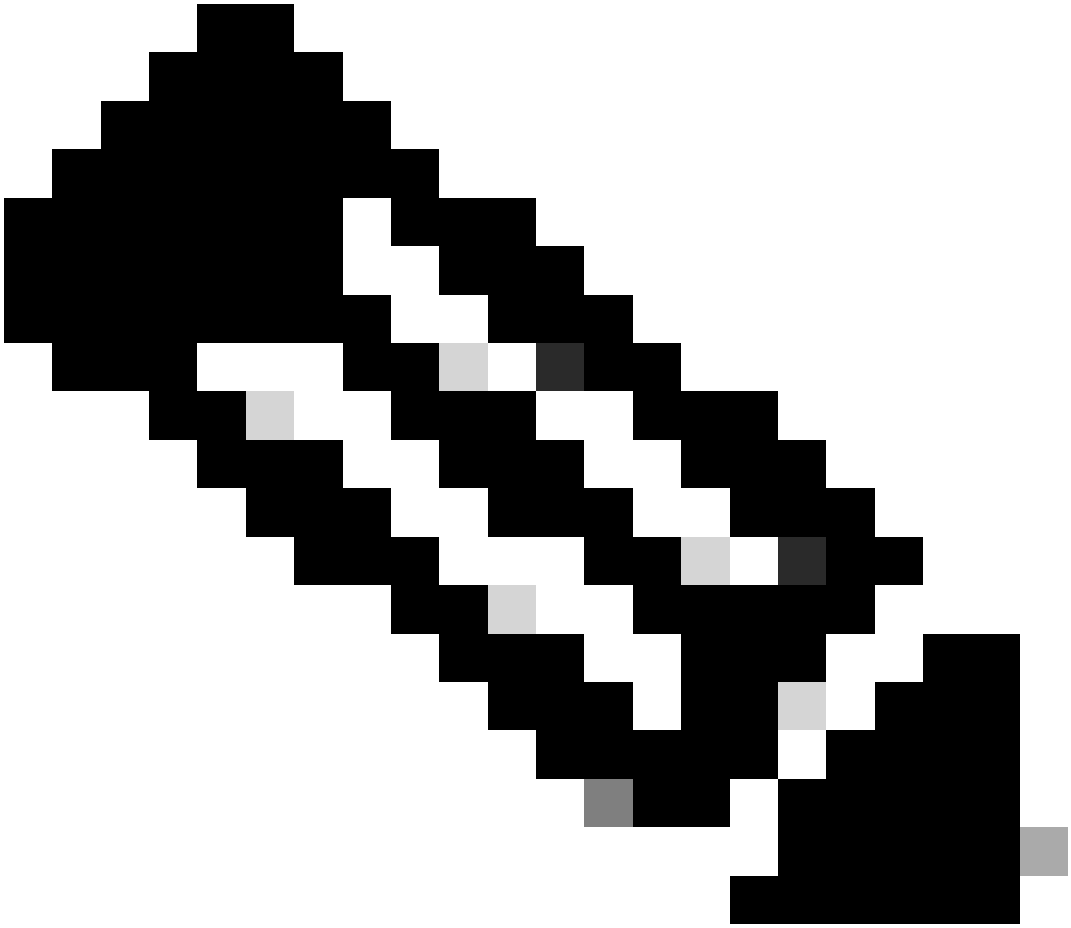
- PowerShellバージョン4.0

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認して

ください。

背景説明

Agent Troubleshooting Toolスクリプトには、エージェントの全体的な健全性、エージェント登録の既知の問題、エージェントのアップグレードの既知の問題、全体的な適用状態の確認、および詳細な分析のためのログ収集を確認できる複数のオプションが用意されています。



注：バージョン3.9以降のエージェントには、Agent Troubleshooting Toolが同梱されています。3.9より前のバージョンでは、デフォルトで含まれていません。3.9より前のバージョンを使用している場合は、3.9エージェントがインストールされたWindowsマシンからスクリプトをコピーし、(C:\Program Files\Cisco Tetration)に貼り付けて、トラブルシューティングツールを使用できます。

スクリプトの実行手順

エージェントのトラブルシューティングツールスクリプトを実行するには、次の手順を実行します。

1. 管理者としてPowerShellを開きます。

2. CSWインストールディレクトリ(デフォルトの場所：C:\ Program Files \Cisco Tetration)に移動します。

3. 次のコマンドを使用してスクリプトを実行します。

.\AgentTroubleshootingTool.pslです

このエージェントトラブルシューティングツールスクリプトで使用可能なパラメータのリスト

エージェントのトラブルシューティングツールには、エージェントのさまざまな側面をトラブルシューティングできる複数のオプションが用意されています。
使用可能なオプションは次のとおりです。

-agentHealth：エージェント状態レポートの実行
-agentRegistration：エージェント登録の問題を確認します
-agentUpgrade：エージェントのアップグレードに関する問題を確認します
-enforcementHealth：適用に関する問題を確認します
-collectLogs：デバッグ用にログを収集します
-collectDebugLogs: loglevel:5が有効になっている口グを収集します。これには、パラメータ –collectLogsを使用して収集された口グも含まれます
-all: -collectDebugLogs以外のすべてのパラメータを実行します。

これらのオプションを使用するには、適切なパラメータを指定してスクリプトを実行します。
たとえば、エージェントの状態を確認するには、-agentHealthパラメータを指定してスクリプトを実行します。

.\AgentTroubleshootingTool.ps1 -agentHealth

パラメータの詳細：agentHealth

-agentHealthパラメータの下で、次の項目をチェックします。

1. サービスTetSensorおよびTetEnforcerは実行状態です。
2. センサーIDが有効です
3. PATH変数に'C:\ Windows\System32'が含まれています
4. エージェントがETWまたはNPCAPを使用している。OSが2008R2の場合は、NPCAPの状態を確認します。

シスコのコレクタ/EFEおよびWSSとのバックエンド接続は良好です。

次に、-agentHealthを指定してスクリプトを実行したときのスクリプト出力の例を示します パラメータ

.\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!!!
```

パラメータ詳細：agentRegistration

-agentRegistrationパラメータの下で、次の項目を確認します。

1. これには、パラメータ – agentHealthを使用して収集されたレポートが含まれます。
2. 登録エラーは、エラーコード(401/403など)に基づいています。

誤ってUIから削除したエージェントをクラスタに再登録するオプションもあります。

-agentRegistrationを使用してスクリプトを実行した場合のスクリプト出力の例を次に示します。 パラメータ.

.\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!!!
```

パラメータの詳細：agentUpgrade

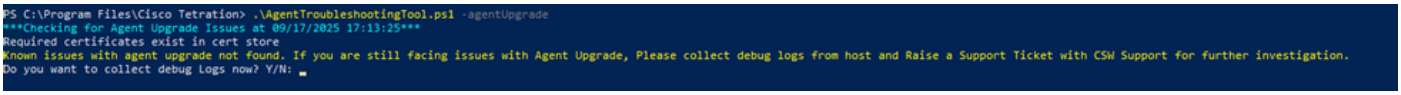
-agentUpgradeパラメータの下で、次の項目を確認します。

1. 必要な証明書がストアで使用できます。
2. MSIキャッシュはC: \ Windows \Installerフォルダにあります。

既知の問題が見つからなくてもエージェントのアップグレードが失敗する場合は、さらにトラブルシューティングを進めるためにデバッグログを収集するオプションを使用できます。

ここでは、-agentUpgradeを指定して実行した場合のスクリプト出力の例を示します パラメータ

.\AgentTroubleshootingTool.ps1 -agentUpgrade



パラメータの詳細 – enforcementHealth

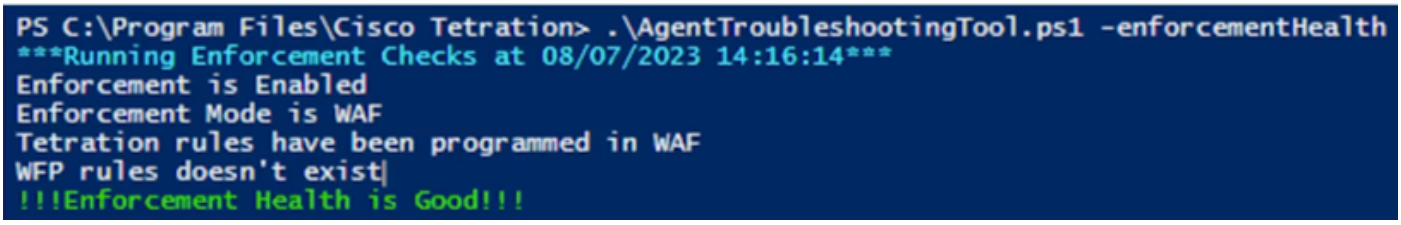
-enforcementHealthパラメータの下で、次の項目を確認します。

1. 強制は有効または無効です。
2. どの適用モードが有効か。
3. CSWルールがWAFでプログラムされているか、またはWFPフィルタがプログラムされています。
4. CSW WFPフィルタが存在しません（モードがWAFの場合）。
5. CSW WAFルールが存在しません（モードがWFPの場合）。

ステップ4と5は、強制モードが切り替わったときの問題を特定することです。

-enforcementHealthを指定してスクリプトを実行したときのスクリプト出力の例を次に示します パラメータ.

.\AgentTroubleshootingTool.ps1 -enforcementHealth



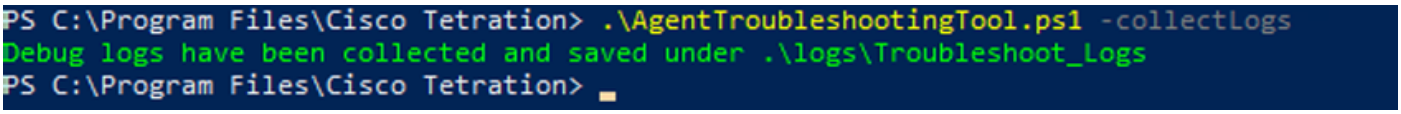
パラメータの詳細：collectLogs

-collectLogsパラメーターを指定して実行すると、デバッグ用にログが収集されます。

収集したログは、パスC:\ Program Files \Cisco Tetration\logs\logs\Troubleshoot_Logsに保存できます。

-collectLogsを指定してスクリプトを実行した場合のスクリプト出力の例を次に示します パラメータ.

.\AgentTroubleshootingTool.ps1 -collectLogs



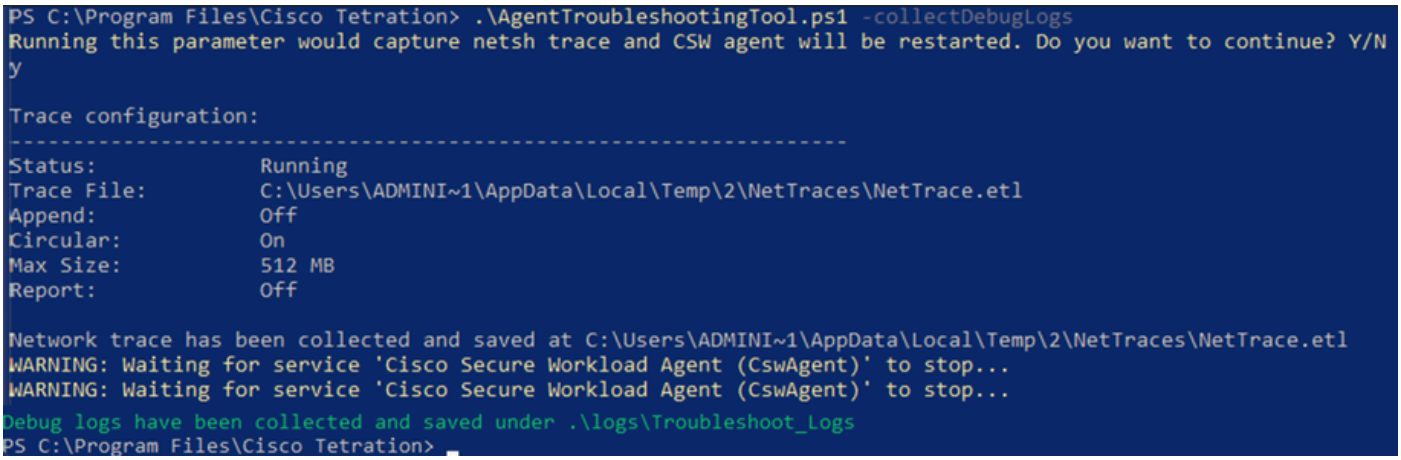
パラメータの詳細：collectDebugLogs

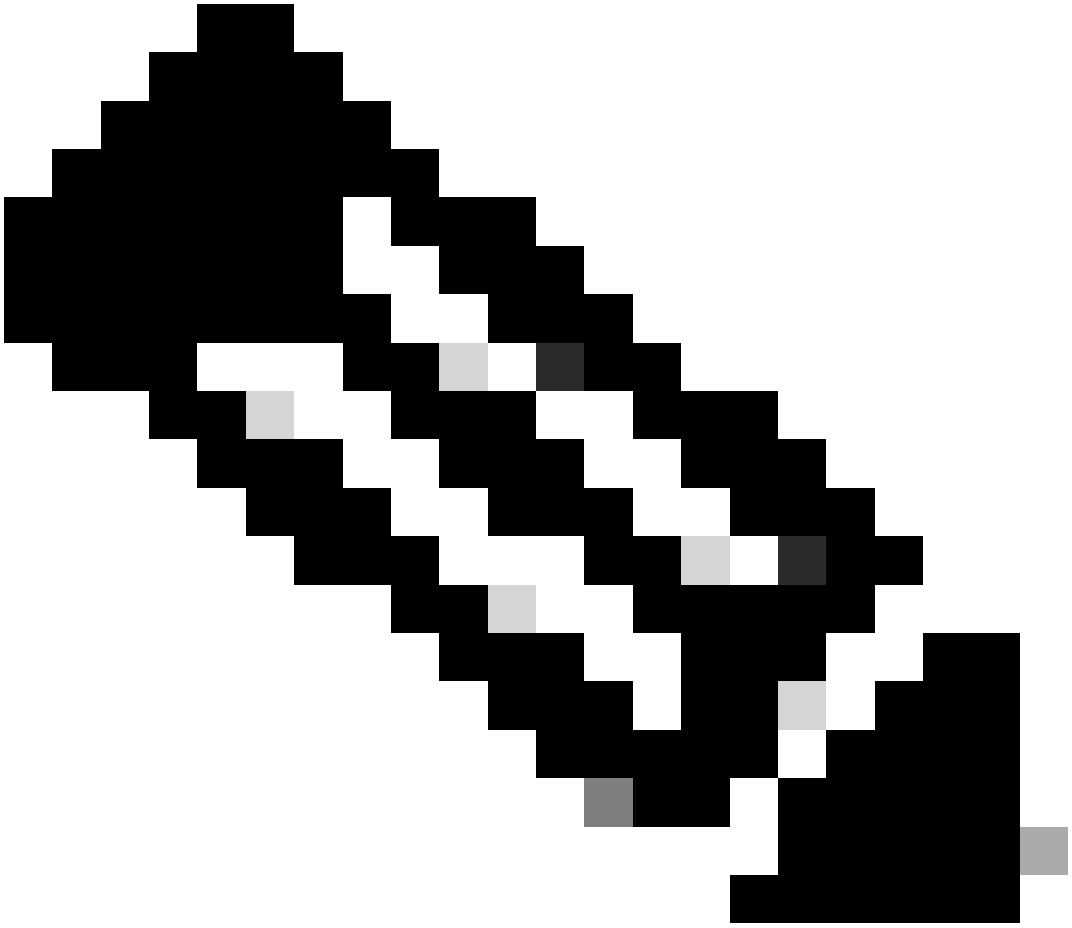
このスクリプトは、-collectDebugLogsパラメータを指定して実行する場合、デバッグ用にloglevel:5を有効にしてログを収集します。

このパラメータを使用してスクリプトを実行すると、netshトレースがキャプチャされ、CSWエージェントを再起動できます。
収集したログは、パスC:\ Program Files \Cisco Tetration\logs\logs\Troubleshoot_Logsに保存できます。

-collectDebugLogsを指定してスクリプトを実行した場合のスクリプト出力の例を次に示します パラメータ.

.\AgentTroubleshootingTool.ps1 -collectDebugLogs





注:Agent Troubleshooting Toolでは、エラーが赤色で表示され、警告が黄色で表示されます。Agent Troubleshooting Toolによってフラグが付けられた一般的な問題を解決できない場合は、Agent Troubleshooting Toolを使用してデバッグログを収集し、安全なワークロードエージェントログバンドルを生成して、Cisco TACに連絡してください。

セキュアなワークロードエージェントログバンドルの生成

ログバンドルを収集するには、Secure Workload Agentがアクティブである必要があります。

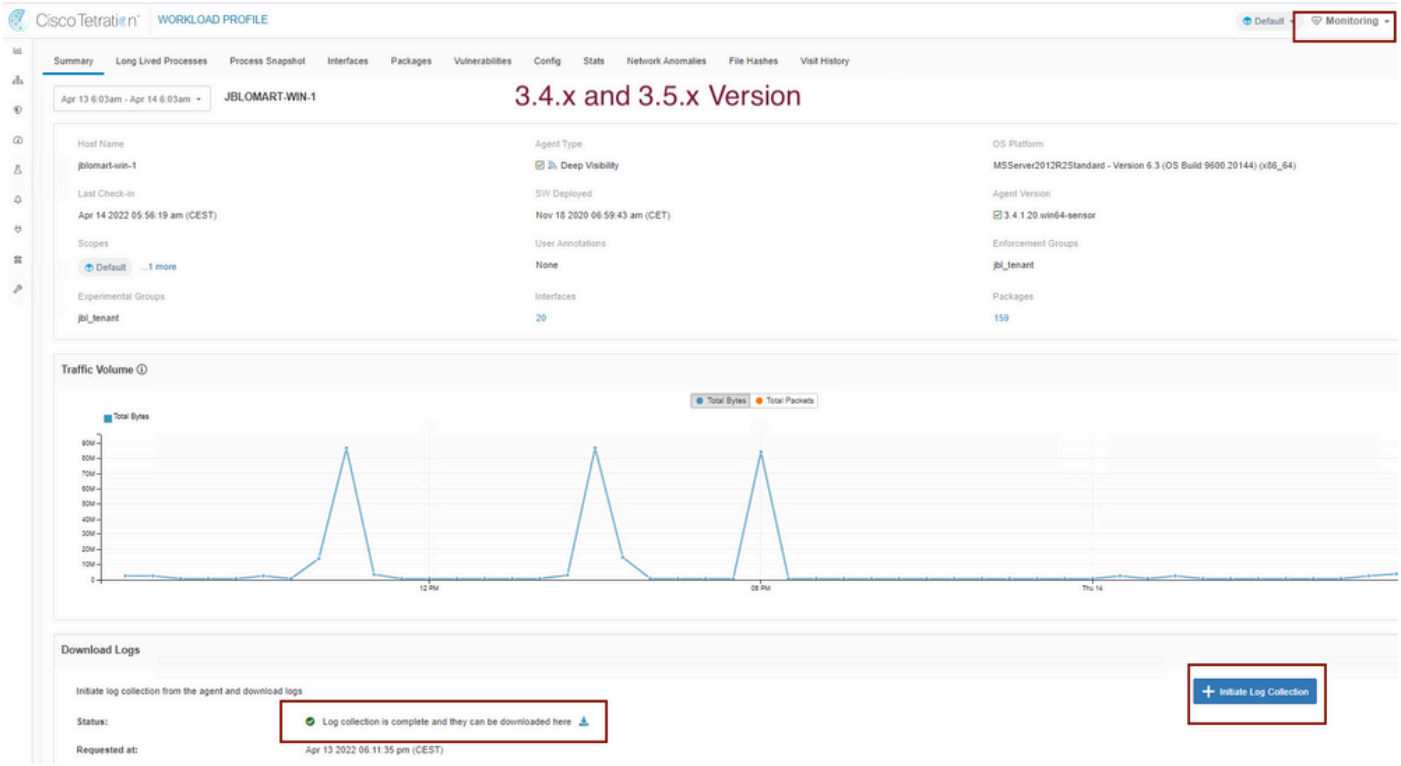
- 3.6.xバージョンの場合は、左側のナビゲーションパネルに移動し、Manage > Agentの順に選択して、Agent Listをクリックします。
- バージョン3.4.xおよび3.5.xの場合、右上のドロップダウンメニューからMonitoringに移動し、Agent Listを選択します。

フィルタオプションを使用してエージェントを検索し、agentをクリックします。 エージェント

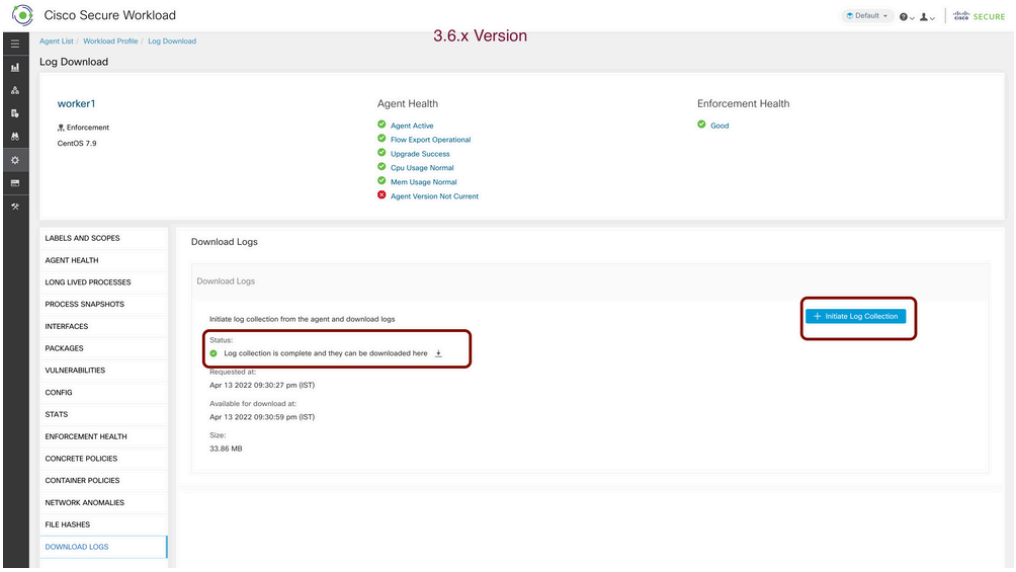
の作業負荷プロファイルが表示されます。ここでは、エージェント設定の詳細を確認できます。ステータスなど。

ワークロードプロファイルページ(3.6.x)の左側のナビゲーションパネルで、Download Logs を選択します（3.4.xおよび3.5.xで、summaryタブに従います）。 Initiate Log Collectionをクリックして、Tetration Agentからのログ収集を開始します。ログ収集が完了するまでに時間がかかる場合があります。ログの収集が完了したら、次のダウンロードオプションをクリックしてログをダウンロードします。スクロールダウンして、ケース番号にファイルをアップロードするオプションを表示します。

バージョン3.4.xおよび3.5.xで稼働するエージェント用のセキュアなワークロードエージェントログバンドルを作成するには、次のイメージを参照してください。



3.6.xバージョン以降のセキュアワークロードエージェントログバンドルを作成するには、次のイメージを参照してください



翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。