Solucionar problemas de agentes do Windows usando a ferramenta de solução de problemas do agente

Contents

Introdução

Este documento descreve como usar o script integrado do PowerShell da Agent Troubleshooting Tool para resolver problemas comuns do agente do Windows.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

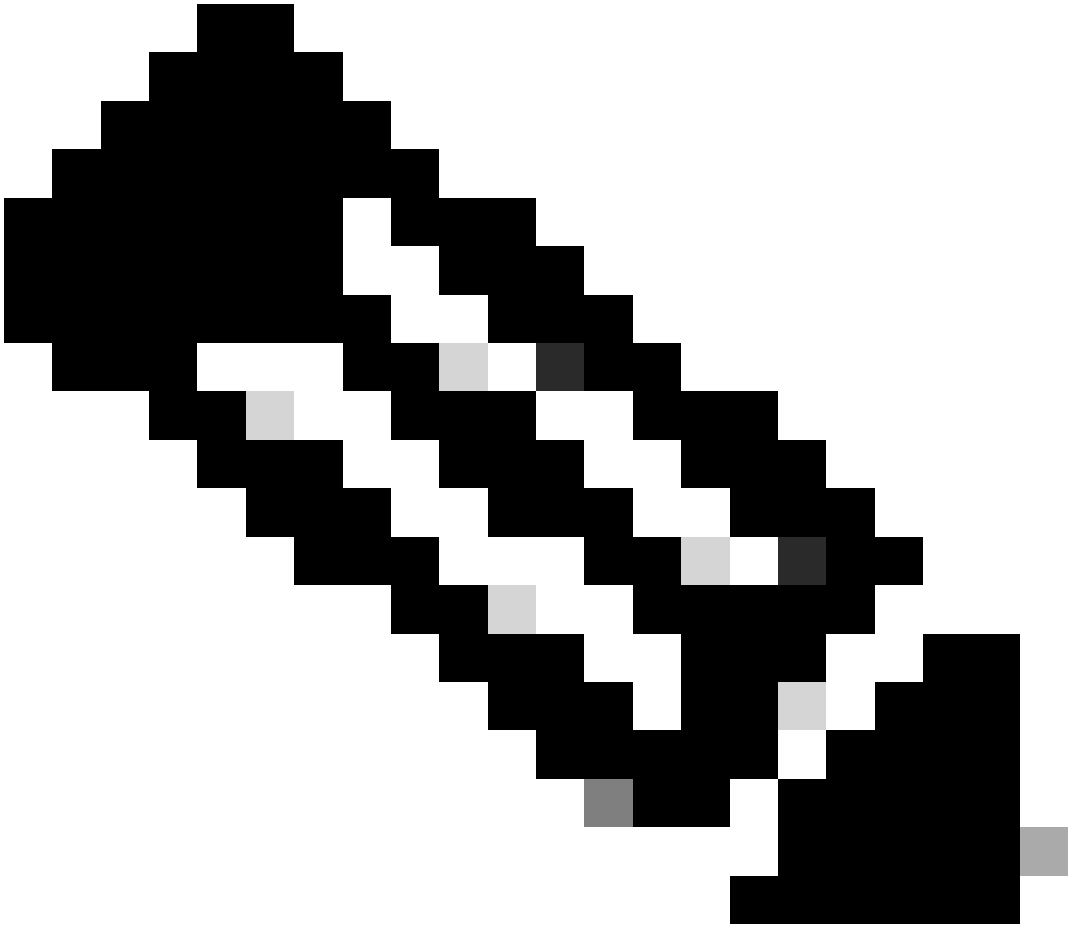
- PowerShell versão 4.0

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto

potencial de qualquer comando.

Informações de Apoio

O script da Ferramenta de solução de problemas do agente vem com várias opções que permitem verificar a integridade geral de seus agentes, problemas conhecidos com o registro do agente, problemas conhecidos com atualizações do agente, verificar a integridade geral da aplicação e coletar logs para análise adicional.



Note: A Agent Troubleshooting Tool é fornecida com o agente que começa na versão 3.9. Para versões anteriores à 3.9, ela não é incluída por padrão. Se estiver usando uma versão anterior à 3.9, você poderá copiar o script de uma máquina Windows com o agente 3.9 instalado e colá-lo em (C:\Program Files\Cisco Tetration) para usar a ferramenta de solução de problemas.

Etapas Para Executar O Script

Para executar o script da ferramenta de solução de problemas do agente, siga estas etapas:

1. Abra o PowerShell como administrador.

2. Navegue até o diretório de instalação do CSW (local padrão: C:\ Program Files \Cisco Tetration).

3. Execute o script usando este comando:

.\AgentTroubleshootingTool.psl

Lista de parâmetros disponíveis no script da ferramenta de solução de problemas do agente

A ferramenta de solução de problemas do agente vem com várias opções que permitem solucionar diferentes aspectos dos seus agentes.
Estas são as opções disponíveis:

Integridade do agente: executar Relatório de Integridade do agente
-registro do agente: verifique se há problemas no Registro do agente
-agentUpgrade: verifique se há problemas com a atualização do agente
-aplicaçãoSaúde: verificar problemas com a Imposição
- coletar logs: coletar logs para depuração
-collectDebugLogs: coletar logs com loglevel:5 habilitado. Isso inclui logs coletados usando o parâmetro -collectLogs também
- todos: executar todos os parâmetros, exceto -collectDebugLogs

Para usar qualquer uma dessas opções, basta executar o script com o parâmetro apropriado. Por exemplo, para verificar a integridade dos agentes, execute o script com o parâmetro -agentHealth:

.\AgentTroubleshootingTool.ps1 -agentHealth

Detalhes do parâmetro -agentHealth

No parâmetro -agentHealth, você está verificando estas coisas:

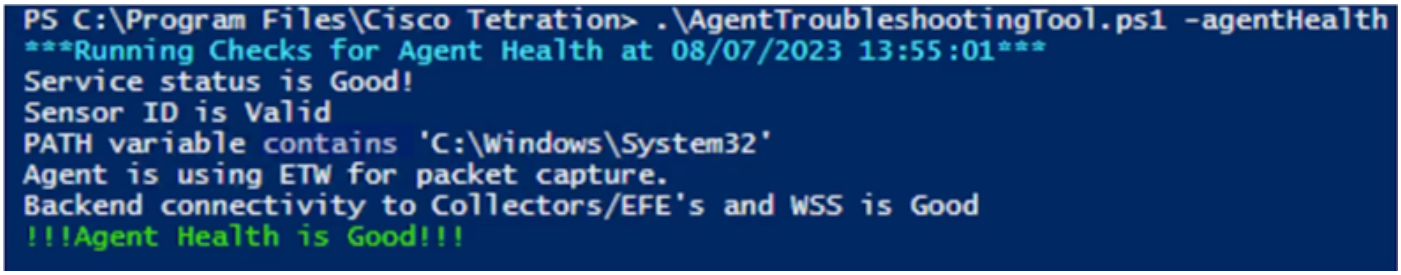
1. Os serviços TestSensor e TestEnforcer estão em um estado de execução.
2. A ID do sensor é válida
3. A variável PATH contém 'C:\ Windows\System32'
4. O agente está usando ETW ou NPCAP. Se o sistema operacional for 2008R2, você estará

verificando a Integridade do NPCAP.

A conectividade de back-end com nossos coletores/EFEs e WSS é boa.

Este é um exemplo da saída do script quando executado com o comando -agentHealth parâmetro

.\AgentTroubleshootingTool.ps1 -agentHealth



Detalhes do parâmetro -agentRegistration

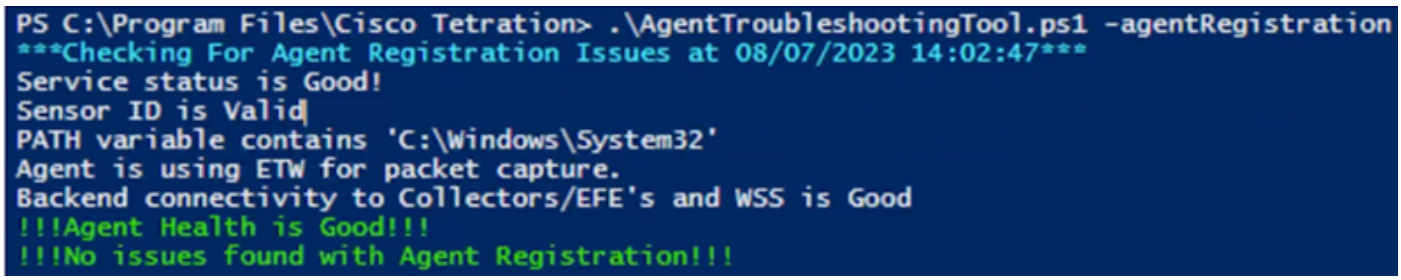
No parâmetro -agentRegistration, você está verificando estas coisas:

1. Ele inclui o relatório coletado usando o parâmetro -agentHealth.
2. Os erros de registro são baseados em códigos de erro, por exemplo, 401/403 e outros.

Há também uma opção fornecida para registrar novamente o agente no cluster se ele for excluído da interface por engano.

Aqui está um exemplo da saída do script quando você executa o script com o comando -agentRegistration parâmetro.

.\AgentTroubleshootingTool.ps1 -agentRegistration



Detalhes do parâmetro -agentUpgrade

No parâmetro -agentUpgrade, você está verificando o seguinte:

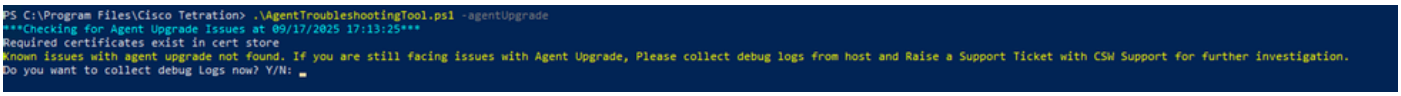
1. Os certificados necessários estão disponíveis no armazenamento.

2. O cache do MSI está disponível na unidade C: \ Windows \Pasta do instalador.

Se nenhum problema conhecido for encontrado, mas a atualização do agente ainda estiver falhando, então você fornecerá a opção de coletar logs de depuração para Troubleshooting adicional.

Aqui está um exemplo da saída do script quando você executa com -agentUpgrade parâmetro

.\AgentTroubleshootingTool.ps1 -agentUpgrade



Detalhes do Parâmetro -enforcementHealth

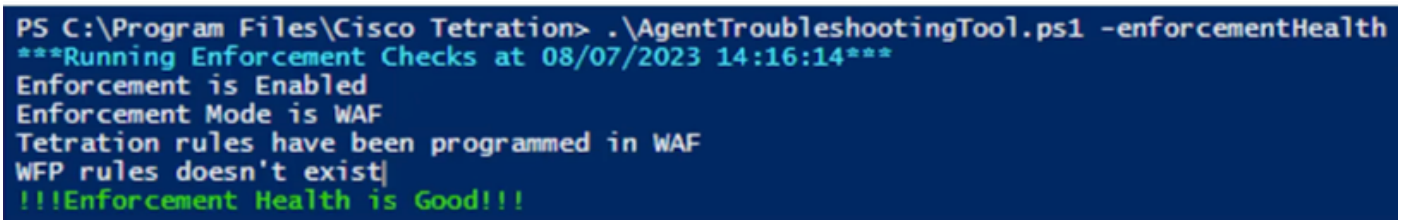
No parâmetro -enforcementHealth, você está verificando estas coisas:

1. A imposição está ativada ou desativada.
2. Que modo de imposição está ativado.
3. As regras do CSW foram programadas no WAF ou os filtros do WFP foram programados.
4. Os filtros WFP do CSW não existem (quando o modo é WAF).
5. As regras WAF do CSW não existem (quando o modo é WFP).

As etapas 4 e 5 são para identificar problemas quando o modo de imposição foi alterado.

Aqui está um exemplo da saída do script quando você executa o script com -enforcementHealth parâmetro.

.\AgentTroubleshootingTool.ps1 -enforcementHealth



Detalhes do parâmetro -collectLogs

O script coleta logs para fins de depuração quando executado com o parâmetro -collectLogs.

Os logs coletados podem ser salvos no caminho C:\ Program Files \Cisco Tetration\logs\logs\Troubleshoot_Logs

Aqui está um exemplo da saída do script quando você executa o script com -

collectLogs parâmetro.

.\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>
```

Detalhes do parâmetro -collectDebugLogs

O script coleta logs com loglevel:5 habilitado para fins de depuração quando você executa o parâmetro -collectDebugLogs.

A execução do script com esse parâmetro capturaria o rastreamento do netsh e o agente do CSW poderia ser reiniciado.
Os logs coletados podem ser salvos no caminho C:\ Program Files \Cisco Tetration\logs\logs\Troubleshoot_Logs

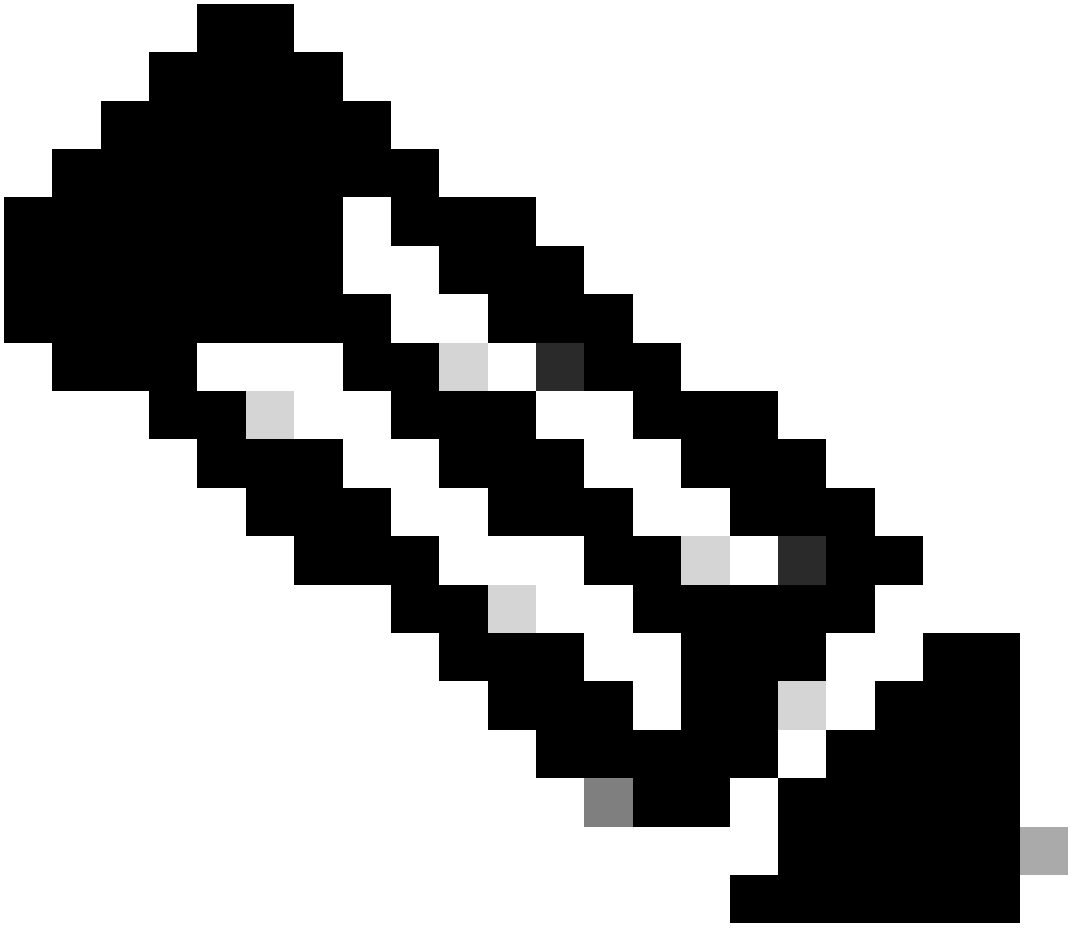
Aqui está um exemplo da saída do script quando você executa o script com -collectDebugLogs parâmetro.

.\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>
```



Note: A Agent Troubleshooting Tool exibe erros em vermelho e avisos em amarelo. Se você não puder resolver os problemas comuns sinalizados pela Ferramenta de solução de problemas do agente, colete os logs de depuração usando a Ferramenta de solução de problemas do agente e gere um pacote de logs do Agente de carga de trabalho segura e entre em contato com o TAC da Cisco para obter assistência.

Gerar o Pacote de Log do Agente de Carga de Trabalho Segura

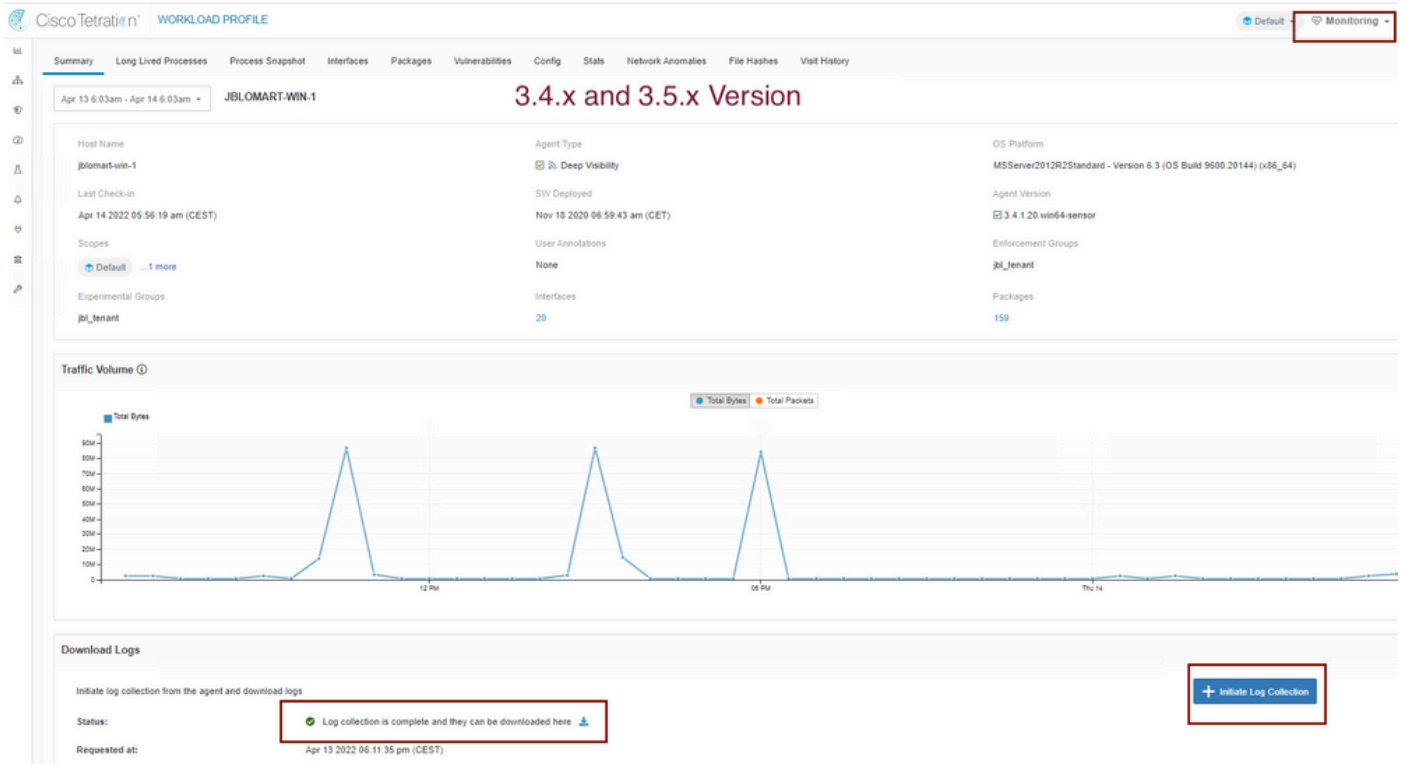
Para coletar o pacote de log, o agente de Carga de Trabalho Segura deve estar ativo.

- Para a versão 3.6.x, navegue para o painel de navegação à esquerda, escolhaGerenciar > Agente e clique emLista de Agentes.
- Para as versões 3.4.x e 3.5.x, navegue paraMonitoramento no menu suspenso superior direito e escolha Lista de Agentes.

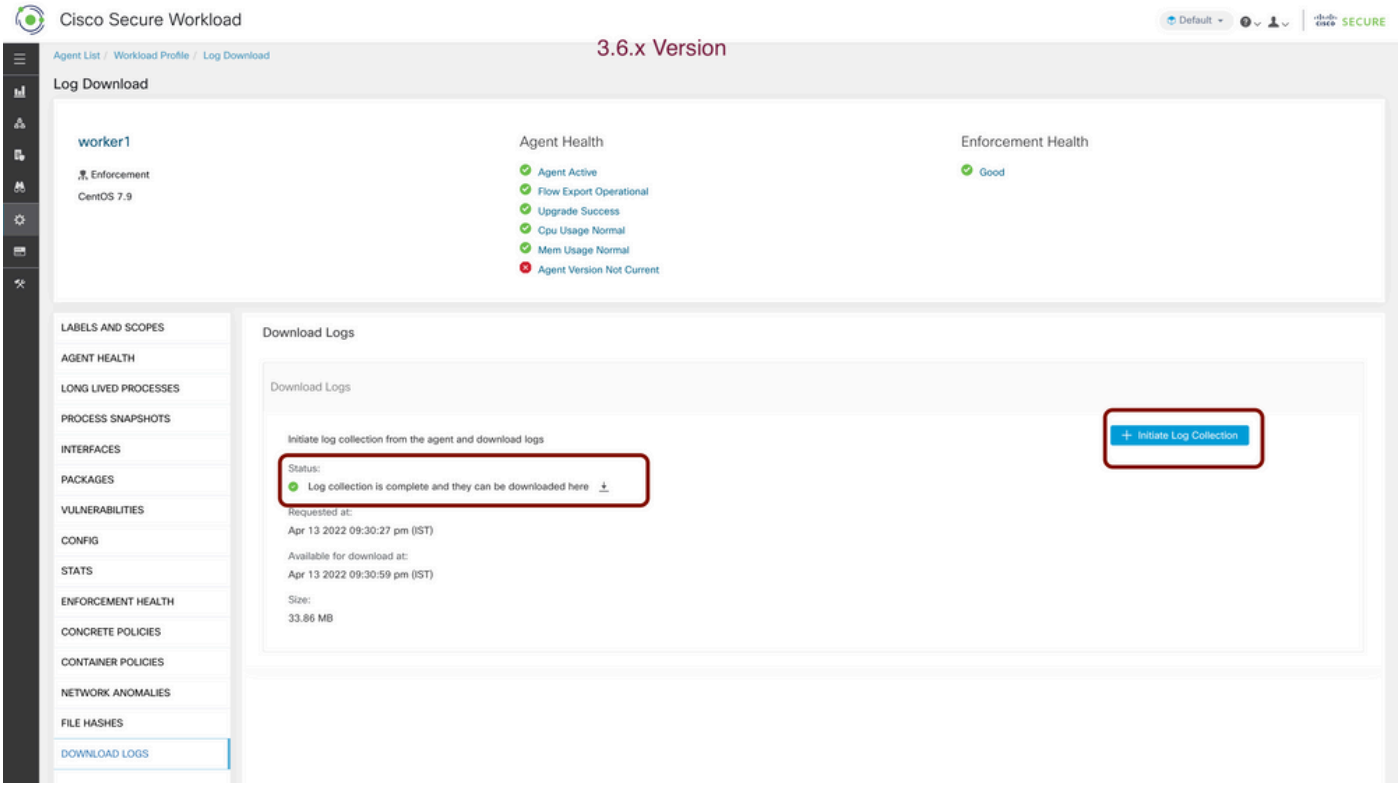
Utilize a opção de filtro para procurar o agente e clique no agente. Isso o levará ao perfil de carga de trabalho do agente. Aqui você pode encontrar detalhes sobre a configuração do agente, e assim por diante.

No painel de navegação do lado esquerdo da página de perfil de carga de trabalho (3.6.x), escolha Download Logs (no 3.4.x e no 3.5.x e siga a guia summary). Clique em Initiate Log Collection para iniciar a coleta de logs no Tetration Agent. Pode demorar um pouco para concluir a coleta de logs. Quando a coleta de logs estiver concluída, clique na opçãoDownload herepara fazer o download dos logs. Role para baixo para obter uma opção para carregar o arquivo para o número do caso.

Consulte esta imagem para criar o Pacote de Logs do Secure Workload Agent para agentes em execução nas versões 3.4.x e 3.5.x.



Consulte esta imagem para criar o Pacote de Log do Secure Workload Agent a partir da versão 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

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.