Risoluzione dei problemi relativi a Windows Agent mediante lo strumento di risoluzione dei problemi dell'agente

Sommario

Introduzione

In questo documento viene descritto come utilizzare lo strumento incorporato di risoluzione dei problemi dell'agente PowerShell per risolvere i problemi comuni degli agenti di Windows.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

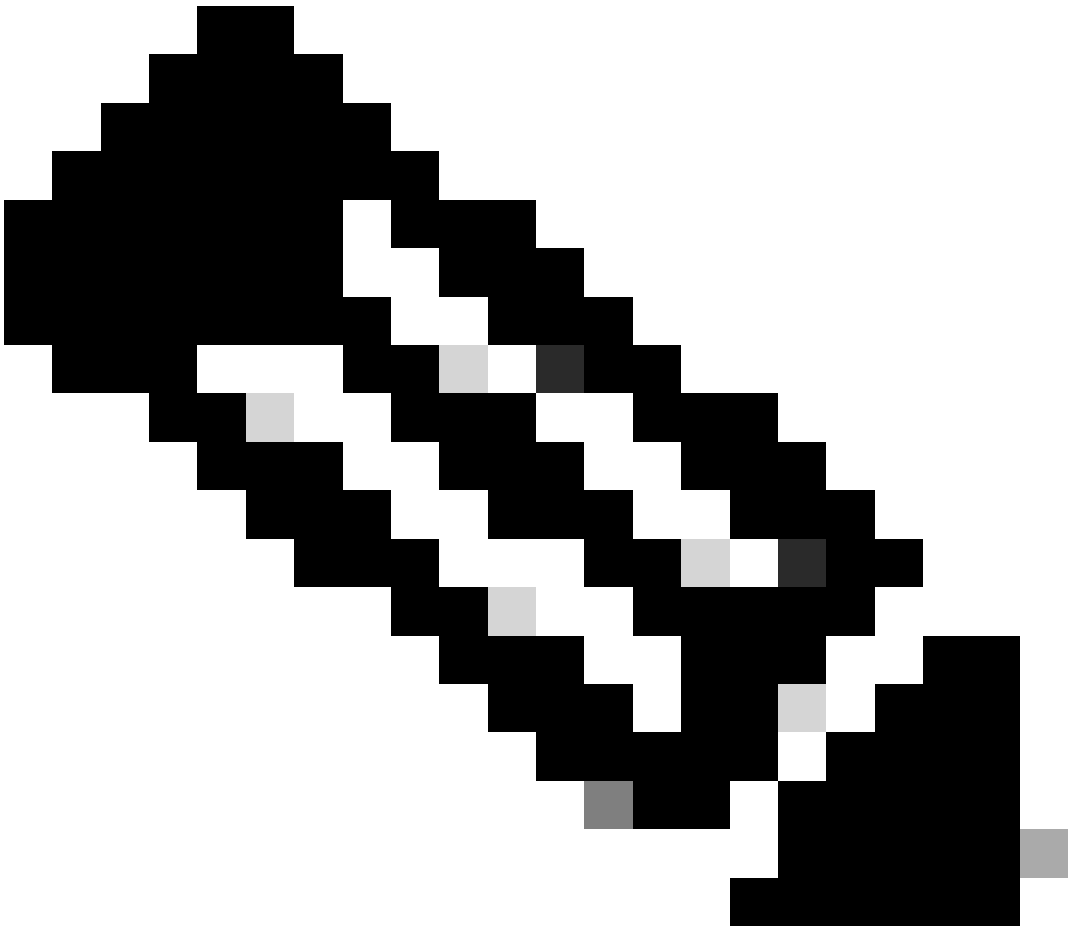
- PowerShell versione 4.0

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata

ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Lo script Agent Troubleshooting Tool viene fornito con diverse opzioni che consentono di controllare lo stato complessivo degli agenti, i problemi noti relativi alla registrazione degli agenti, i problemi noti relativi agli aggiornamenti degli agenti, il controllo dello stato complessivo dell'applicazione e la raccolta dei log per ulteriori analisi.



Nota: Agent Troubleshooting Tool viene fornito con l'agente a partire dalla versione 3.9. Per le versioni precedenti alla 3.9, non è incluso per impostazione predefinita. Se si utilizza una versione precedente alla 3.9, è possibile copiare lo script da un computer Windows con l'agente 3.9 installato e incollarlo in (C:\Program Files\Cisco Tetration) per utilizzare lo strumento di risoluzione dei problemi.

Passaggi Per Eseguire Lo Script

Per eseguire lo script dello strumento di risoluzione dei problemi dell'agente, eseguire la procedura seguente:

1. Aprire PowerShell come amministratore.

2. Passare alla directory di installazione di CSW (posizione predefinita: C:\ Program Files \Cisco Tetration).

3. Eseguire lo script utilizzando questo comando:

.\AgentTroubleshootingTool.psl

Elenco dei parametri disponibili nello script dello strumento di risoluzione dei problemi dell'agente

Lo strumento di risoluzione dei problemi dell'agente include diverse opzioni che consentono di risolvere i problemi relativi a diversi aspetti degli agenti.
Le opzioni disponibili sono le seguenti:

-agentHealth: Esegui rapporto di stato agente
-agentRegistration: verifica dei problemi nella registrazione dell'agente
-agentUpgrade: verifica la presenza di problemi con l'aggiornamento dell'agente
-enforcementHealth: verifica la presenza di problemi relativi all'applicazione
-collectLogs: raccogli log per il debug
-collectDebugLogs: raccogliere i log con loglevel:5 abilitato. Sono inclusi anche i log raccolti utilizzando il parametro -collectLogs
-all: eseguire tutti i parametri tranne -collectDebugLogs

Per utilizzare una di queste opzioni, è sufficiente eseguire lo script con il parametro appropriato. Ad esempio, per verificare l'integrità degli agenti, eseguire lo script con il parametro -agentHealth:

.\AgentTroubleshootingTool.ps1 -agentHealth

Dettagli parametro -agentHealth

Nel parametro -agentHealth vengono controllati i seguenti elementi:

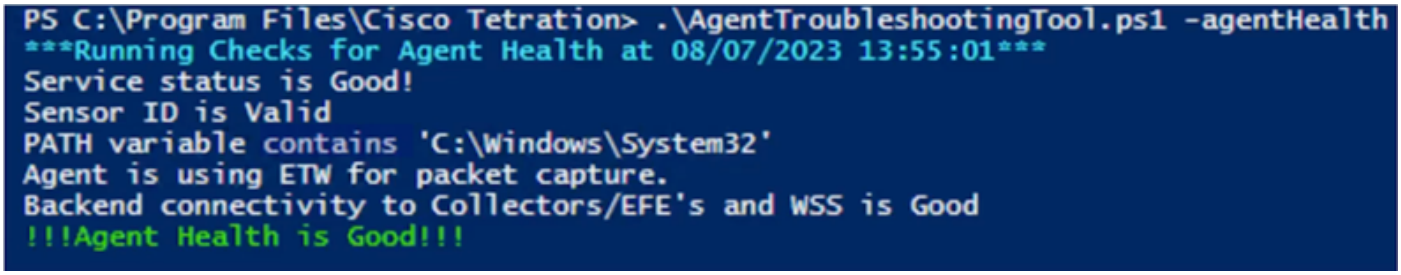
1. I servizi TetSensor e TetEnforcer sono in esecuzione.
2. ID sensore valido
3. La variabile PATH contiene 'C:\ Windows\System32'
4. L'agente utilizza ETW o NPCAP. Se il sistema operativo è 2008R2, si sta verificando lo stato

di integrità di NPCAP.

La connettività back-end con i nostri collector/EFE e WSS è buona.

Di seguito è riportato un esempio dell'output dello script quando si esegue lo script con -agentHealth parametro

.\AgentTroubleshootingTool.ps1 -agentHealth



Dettagli parametro -agentRegistration

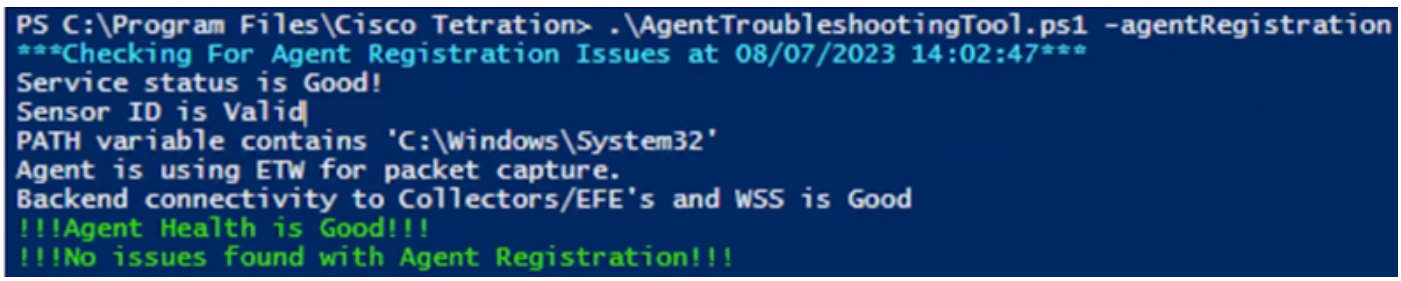
Nel parametro -agentRegistration vengono controllati i seguenti elementi:

1. Include il report raccolto utilizzando il parametro -agentHealth.
2. Gli errori di registrazione si basano sui codici di errore, ad esempio 401/403 e altri.

È inoltre disponibile un'opzione che consente di registrare nuovamente l'agente con il cluster se viene eliminato per errore dall'interfaccia utente.

Di seguito è riportato un esempio dell'output dello script quando si esegue lo script con -agentRegistration parametro.

.\AgentTroubleshootingTool.ps1 -registrazioneAgente



Dettagli parametro -agentUpgrade

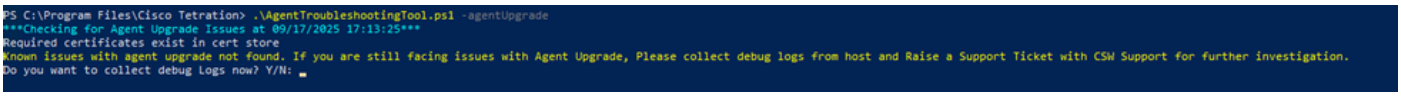
Nel parametro -agentUpgrade è necessario verificare i seguenti elementi:

1. I certificati richiesti sono disponibili nell'archivio.
2. La cache MSI è disponibile sotto la C: \ Cartella \Installer di Windows.

Se non vengono rilevati problemi noti, ma l'aggiornamento dell'agente non riesce, è possibile raccogliere i log di debug per ulteriori operazioni di risoluzione dei problemi.

Di seguito è riportato un esempio dell'output dello script eseguito con -agentUpgrade parametro

.\AgentTroubleshootingTool.ps1 -agentUpgrade



Dettagli parametro -enforcementHealth

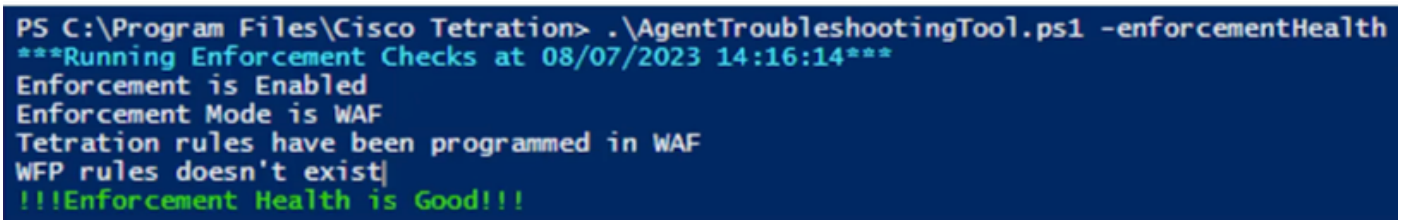
Sotto il parametro -enforcementHealth si verificano i seguenti elementi:

1. L'imposizione è abilitata o disabilitata.
2. Modalità di applicazione attivata.
3. Le regole CSW sono state programmate in WAF oppure i filtri WFP sono stati programmati.
4. I filtri WFP CSW non esistono (quando la modalità è WAF).
5. Le regole WAF CSW non esistono (quando la modalità è WFP).

I passaggi 4 e 5 consentono di identificare i problemi quando è stata attivata la modalità di applicazione.

Di seguito è riportato un esempio dell'output dello script quando si esegue lo script con -enforcementHealth parametro.

.\AgentTroubleshootingTool.ps1 -enforcementHealth



Dettagli parametro -collectLogs

Lo script raccoglie i log per scopi di debug quando viene eseguito con il parametro -collectLogs.

I registri raccolti possono essere salvati nel percorso C:\ Program Files \Cisco Tetration\logs\logs\Troubleshoot_Logs

Di seguito è riportato un esempio dell'output dello script quando si esegue lo script con -collectLogs parametro.

.\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>
```

Dettagli parametro -collectDebugLogs

Lo script raccoglie i log con loglevel:5 abilitato per il debug quando si esegue con il parametro -collectDebugLogs.

L'esecuzione dello script con questo parametro acquisirebbe la traccia netsh e l'agente CSW può essere riavviato.
I registri raccolti possono essere salvati nel percorso C:\ Program Files \Cisco Tetration\logs\logs\Troubleshoot_Logs

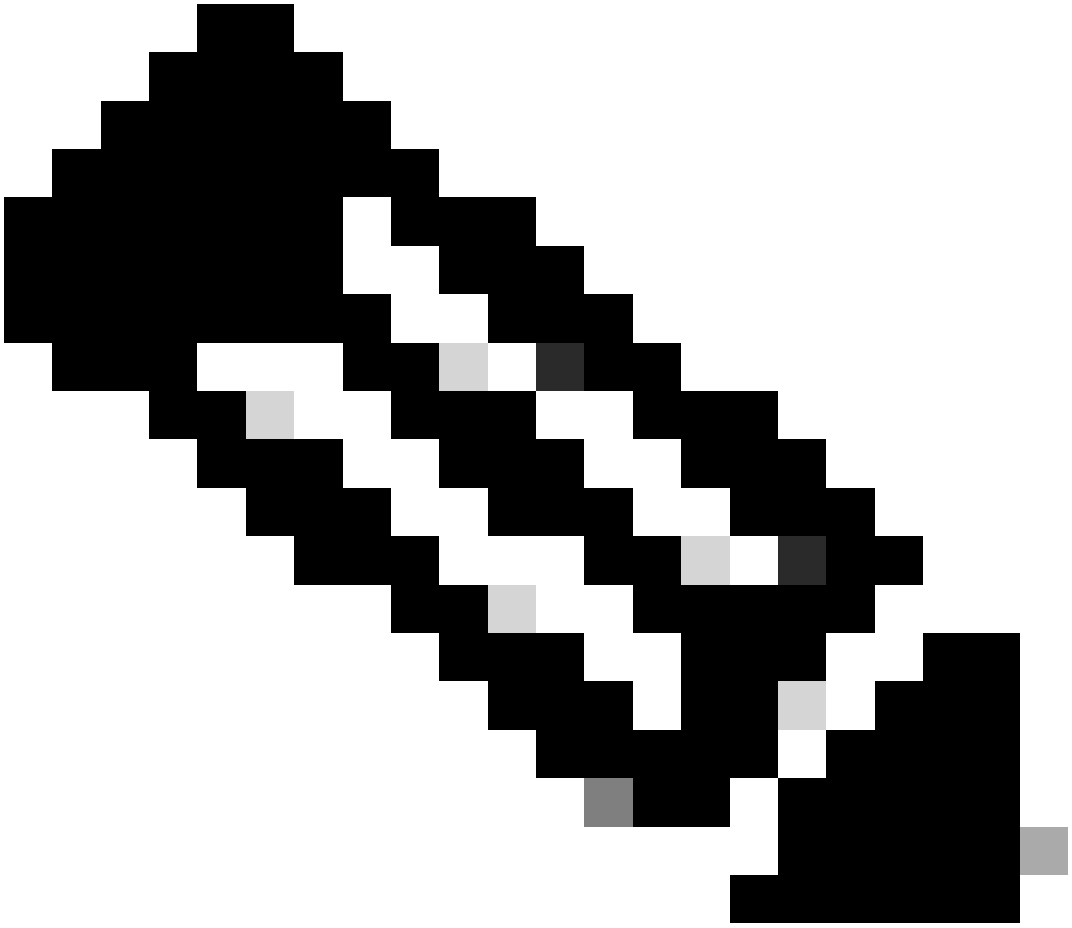
Di seguito è riportato un esempio dell'output dello script quando si esegue lo script con -collectDebugLogs parametro.

.\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>
```



Nota: Agent Troubleshooting Tool visualizza gli errori in rosso e le avvertenze in giallo. Se non è possibile risolvere i problemi comuni contrassegnati dallo strumento di risoluzione dei problemi dell'agente, raccogliere i log di debug utilizzando lo strumento di risoluzione dei problemi dell'agente e generare un bundle di log dell'agente del carico di lavoro sicuro e contattare Cisco TAC per assistenza.

Genera il pacchetto di log dell'agente del carico di lavoro protetto

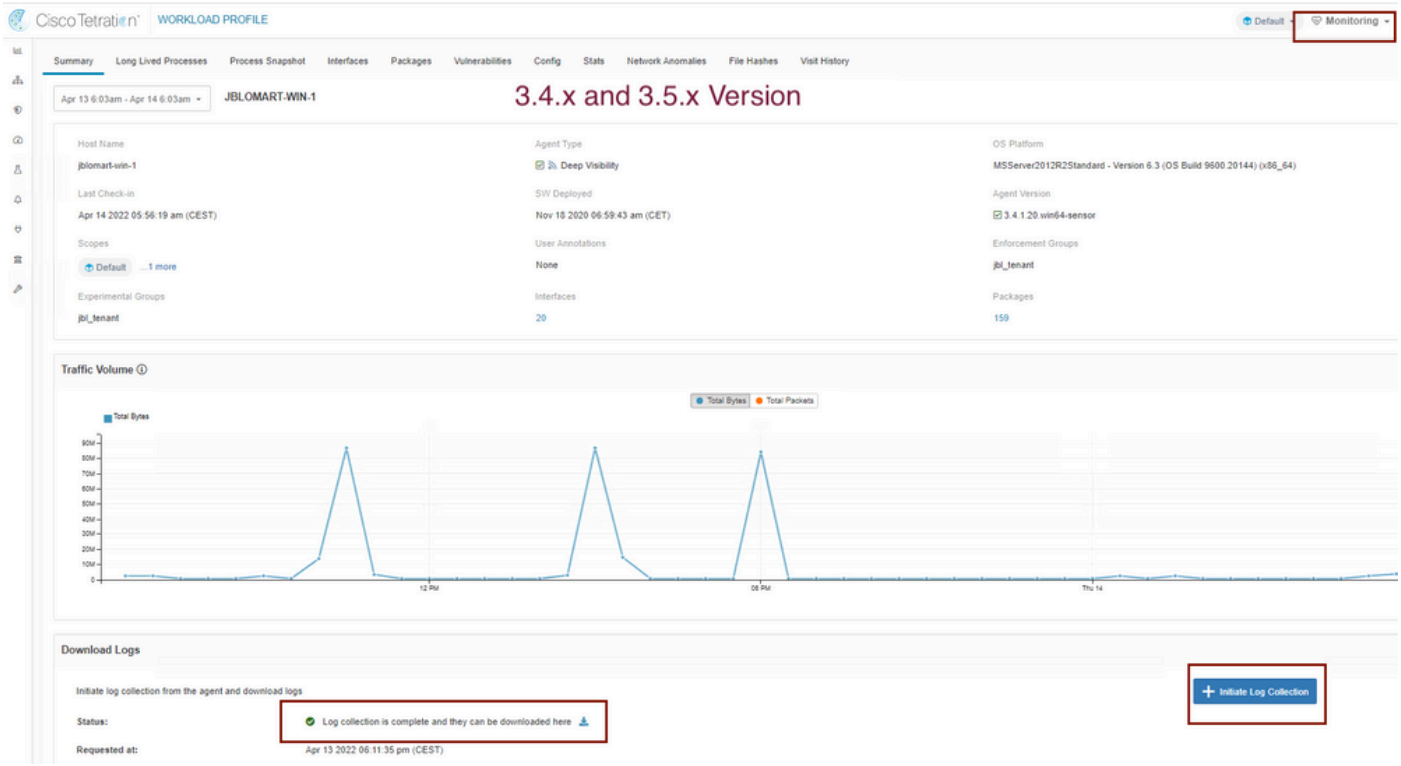
Per raccogliere il bundle del log, è necessario che l'agente Secure Workload sia attivo.

- Per la versione 3.6.x, spostarsi nel pannello di navigazione a sinistra, scegliereGestisci > Agente, quindi fare clic su Elenco agenti.
- Per le versioni 3.4.x e 3.5.x, passare a Monitoraggio dal menu a discesa in alto a destra e scegliere Elenco agenti.

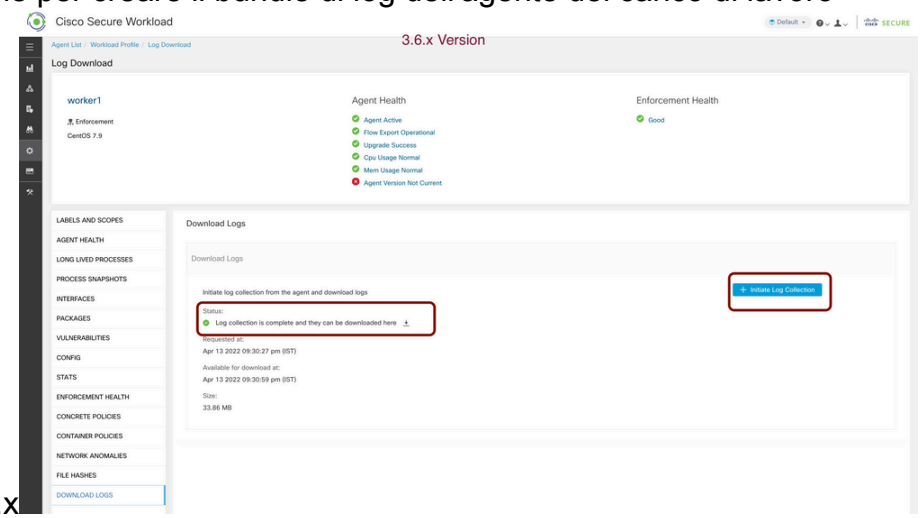
Utilizzare l'opzione di filtro per cercare l'agente e fare clic sull'agente. Viene visualizzato il profilo del carico di lavoro dell'agente. Qui è possibile trovare i dettagli sulla configurazione dell'agente, e così via.

Nel pannello di navigazione a sinistra della pagina del profilo del carico di lavoro (3.6.x), scegliere Download log (nelle versioni 3.4.x e 3.5.x e seguire la scheda di riepilogo). Fare clic su Avvia raccolta log per avviare la raccolta di log dall'agente Tetration. Il completamento della raccolta dei log può richiedere del tempo. Una volta completata la raccolta dei log, fare clic sull'opzione Download (Scarica qui) per scaricare i log. Scorrere verso il basso per ottenere un'opzione per caricare il file nella richiesta numero.

Fare riferimento a questa immagine per creare il pacchetto di log dell'agente del carico di lavoro sicuro per gli agenti in esecuzione sulle versioni 3.4.x e 3.5.x.



Fare riferimento a questa immagine per creare il bundle di log dell'agente del carico di lavoro sicuro a partire dalla versione 3.6.x



Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).