Analyze AMP Diagnostic Bundle per CPU elevata

Sommario

Introduzione

In questo documento viene descritto come analizzare un bundle diagnostico da Advanced Malware Protection (AMP) per Endpoints Public Cloud su dispositivi Windows per risolvere i problemi relativi all'utilizzo elevato della CPU.

Contributo di Luis Velazquez e modificato da Yeraldin Sánchez, Cisco TAC Engineers.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Accesso alla console AMP

Componenti usati

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

- AMP for Endpoints Console 5.4.20200204
- Dispositivi del sistema operativo Windows

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.

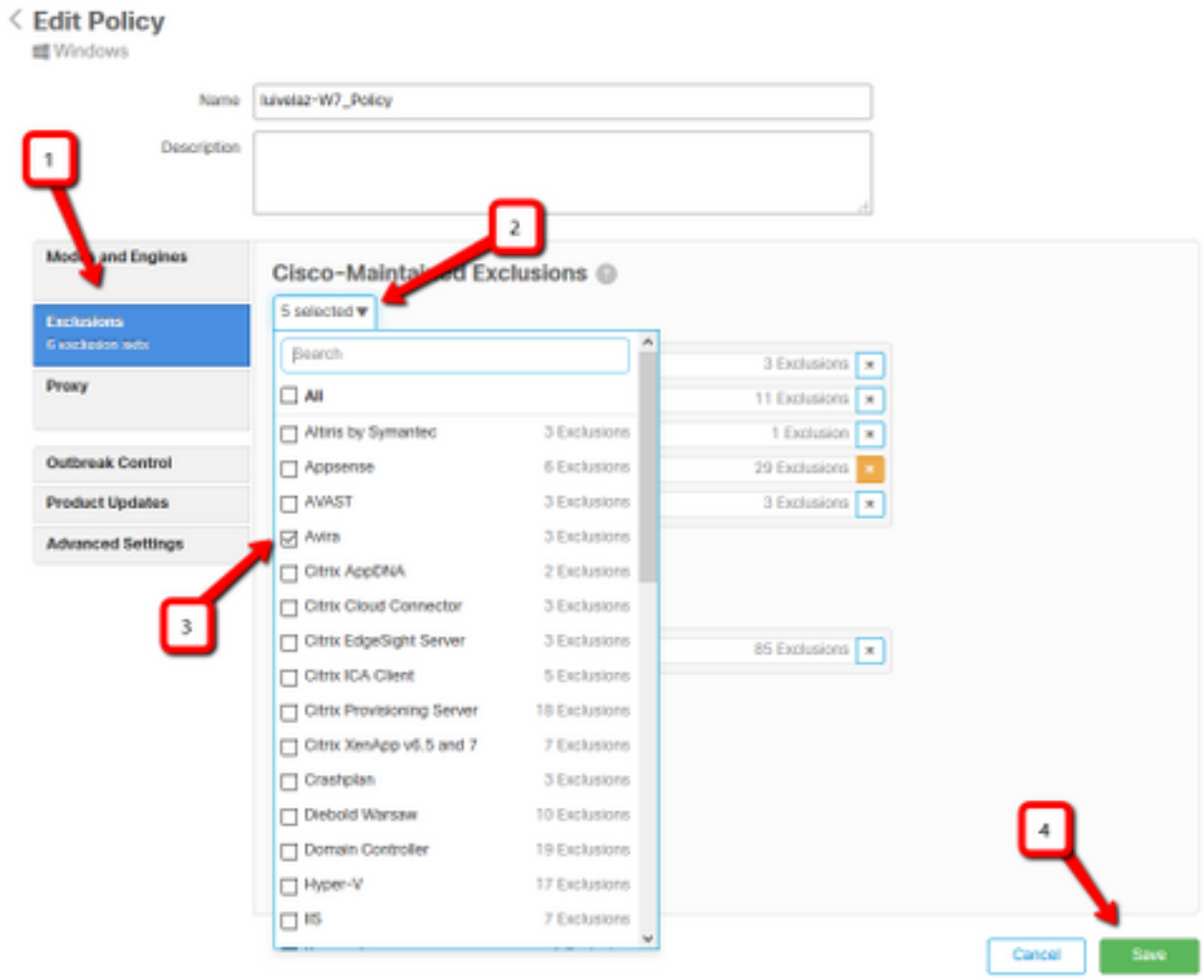
Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

Verificare se nel computer è installato un altro antivirus

Se è installato un altro antivirus, verificare che il processo principale dell'antivirus sia escluso nella configurazione della policy

> **Suggerimento**: Utilizzare le esclusioni gestite da Cisco se il software in uso è incluso nell'elenco, tenere presente che tali esclusioni possono essere aggiunte alle nuove versioni di un'applicazione.
>
> Per visualizzare gli elenchi disponibili nella sezione Esclusioni gestite da Cisco, passare a **Gestione > Criteri > Modifica > Esclusioni > Esclusioni gestite da Cisco.**
> Selezionare quelli necessari all'endpoint in base al software attualmente installato nel computer, quindi salvare il criterio, come mostrato nell'immagine.



Identificare se la CPU elevata si verifica quando un'applicazione specifica è in uso

Identificare se il problema si verifica durante l'esecuzione di un'applicazione o di alcune di esse, se si è in grado di replicare il problema aiuta nel processo di identificazione delle potenziali esclusioni.

Raccogli pacchetto diagnostico per analisi

Abilita livello registro di debug

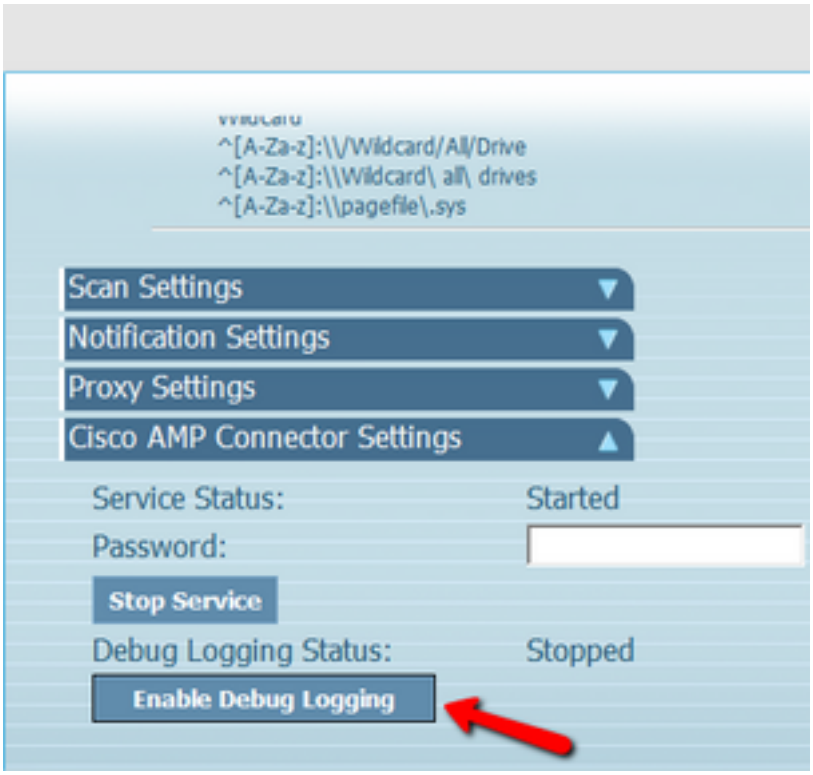
Per raccogliere un pacchetto diagnostico utile, è necessario abilitare il livello del log di debug.

Livello di debug nell'endpoint

Se è possibile replicare il problema e accedere all'endpoint, di seguito è riportata la procedura ottimale per acquisire il bundle di diagnostica:

1. Apri interfaccia utente AMP
2. Passa a **Impostazioni**
3. Scorrere fino alla parte inferiore dell'interfaccia utente di AMP e aprire **Cisco AMP Connector Settings**
4. Fare clic su **Enable Debug Logging**

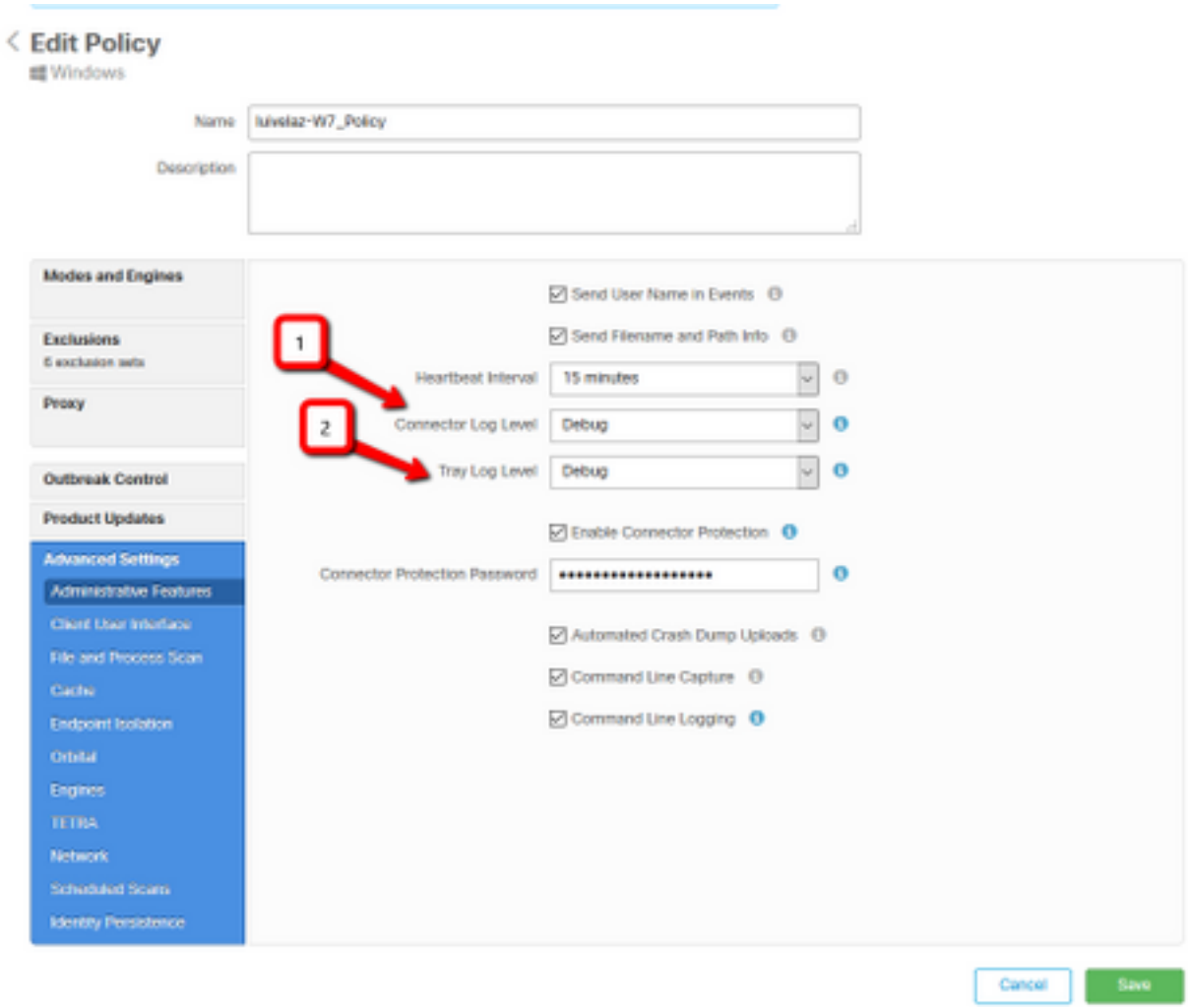
5. **Lo stato della registrazione di debug** deve essere modificato in **Avviato.** Questa procedura abilita il livello di debug fino al successivo heartbeat del criterio, per impostazione predefinita 15 minuti



Livello di debug nel criterio

Se non si dispone dell'accesso all'endpoint o se il problema non può essere riprodotto in modo coerente, è necessario abilitare il livello del registro di debug nel criterio.

Per abilitare il livello di log di debug in base ai criteri, selezionare Gestione > Criteri > Modifica > Impostazioni avanzate > **Livello di log del** connettore e Gestione > Criteri > Modifica > Impostazioni avanzate > Livello di log delle cassette di controllo, quindi selezionare Debug e salvare il criterio, come mostrato nell'immagine.



Attenzione: Se la modalità di debug è abilitata dal criterio, tutti gli endpoint ricevono la modifica.

Nota: Sincronizzare i criteri dell'endpoint per verificare che il livello di debug sia applicato o attendere l'intervallo di heartbeat. Per impostazione predefinita, il valore è 15 minuti.

Riprodurre il problema e raccogliere un pacchetto diagnostico

Quando il livello di debug è configurato, attendere che sul sistema si verifichi lo stato High CPU (CPU elevata) o riprodurre manualmente le condizioni precedentemente identificate, quindi raccogliere il pacchetto di diagnostica.

Per raccogliere il bundle, passare a **C:\Program Files\Cisco\AMP\X.X.X** (dove X.X.X è la versione più recente di AMP installata sul sistema) ed eseguire l'applicazione **ipsupporttool.exe.** questo processo crea un file **.7z** sul desktop denominato **CiscoAMP_Support_Tool_%date%.7z**

Nota: Connector versione 6.2.3 e successive può richiedere un bundle in remoto, passare a **Gestione > Computer**, espandere il record dell'endpoint e utilizzare l'opzione Diagnosi.

Nota: Il pacchetto di diagnostica può anche essere eseguito da un prompt CMD con il comando: **"C:\Program Files\Cisco\AMP\X.X.X\ipsupporttool.exe"**, o **"C:\Program**

Files\Cisco\AMP\X.X.X\ipsupporttool.exe" -o "X:\Folder\I\Can\Get\To", dove X.X.X è la versione AMP più recente installata, è possibile utilizzare il secondo comando per selezionare la cartella di output per il file .7z.

Eseguire l'analisi

Esistono due modi per analizzare un file di diagnostica:

- Diag_Analyzer.exe
- Conteggio.ps1

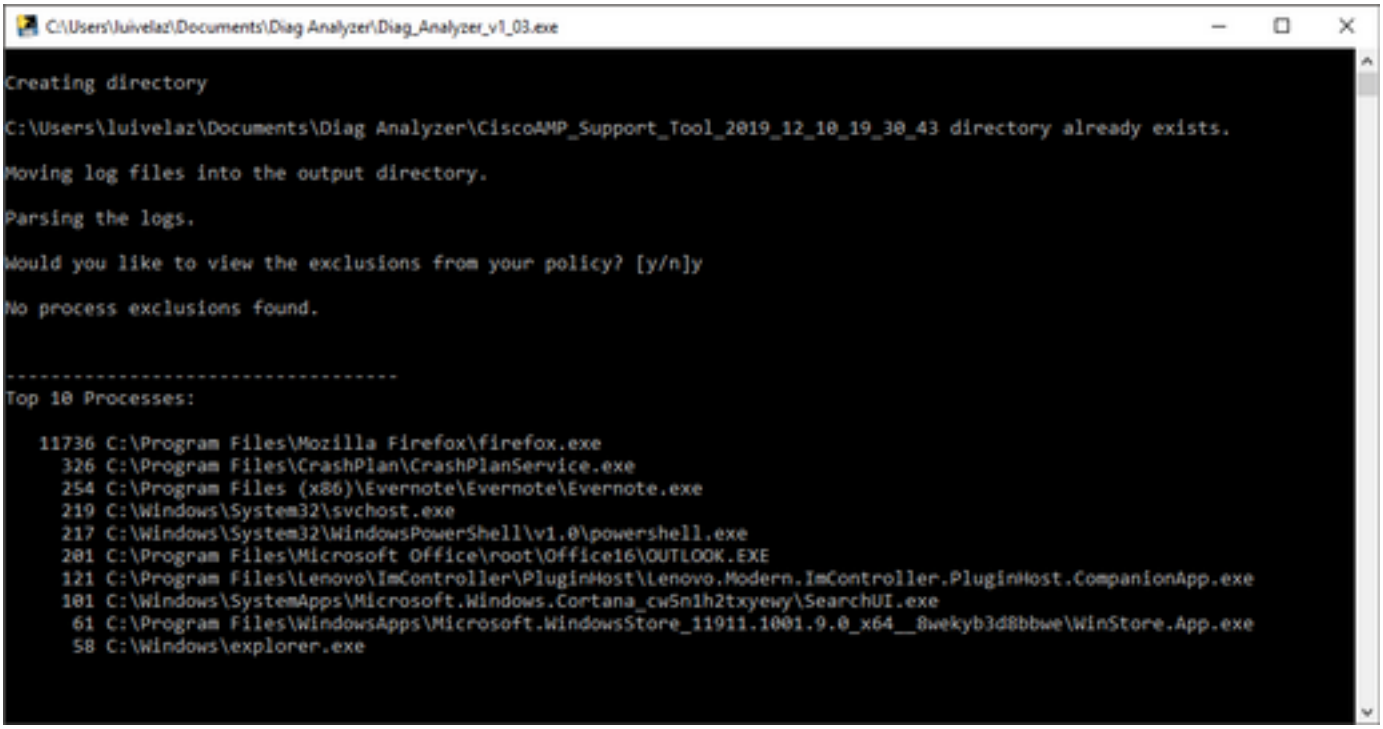
Diag_Analyzer.exe

Passaggio 1. Scaricare l'applicazione qui.

Passaggio 2. Nella pagina GitHub, è presente un file README con ulteriori istruzioni sull'uso.

Passaggio 3. Copiare il file di diagnostica **CiscoAMP_Support_Tool_%date%.7z** nella stessa cartella in cui si trova Diag_Analyzer.exe.

Passaggio 4. Eseguire l'applicazione **Diag_Analyzer.exe**



Passaggio 5. Nel nuovo prompt confermare se si desidera ottenere le esclusioni dal criterio con una **S** o una **N**.

Passaggio 6. Il risultato dello script contiene:

- Primi 10 processi
- Primi 10 file
- Prime 10 estensioni
- Primi 100 percorsi

- Tutti i file

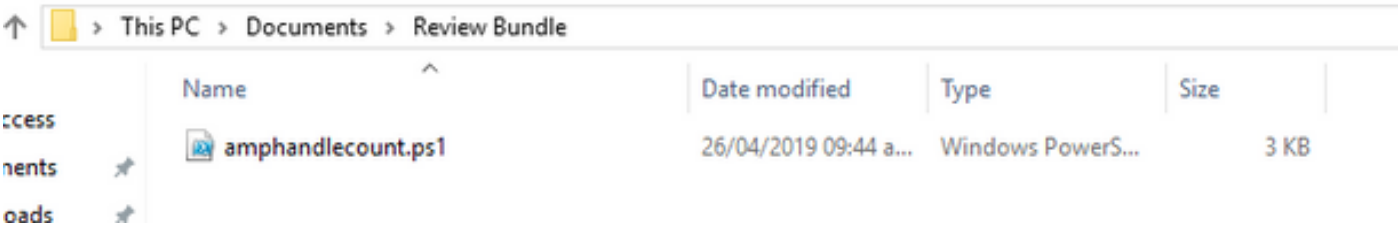
  Nota: Diag_Analyzer.exe verifica i file di diagnostica AMP forniti per sfc.exe.log. quindi, crea una nuova directory con il nome del file di diagnostica e memorizza i file di log al di fuori della .7z, nella directory padre della diagnostica, dopo di che, analizza i log e determina i primi 10 processi, file, estensioni e percorsi, infine, stampa le informazioni sullo schermo e anche su un file {Diagnostic}-summary.txt.

Conteggio.ps1

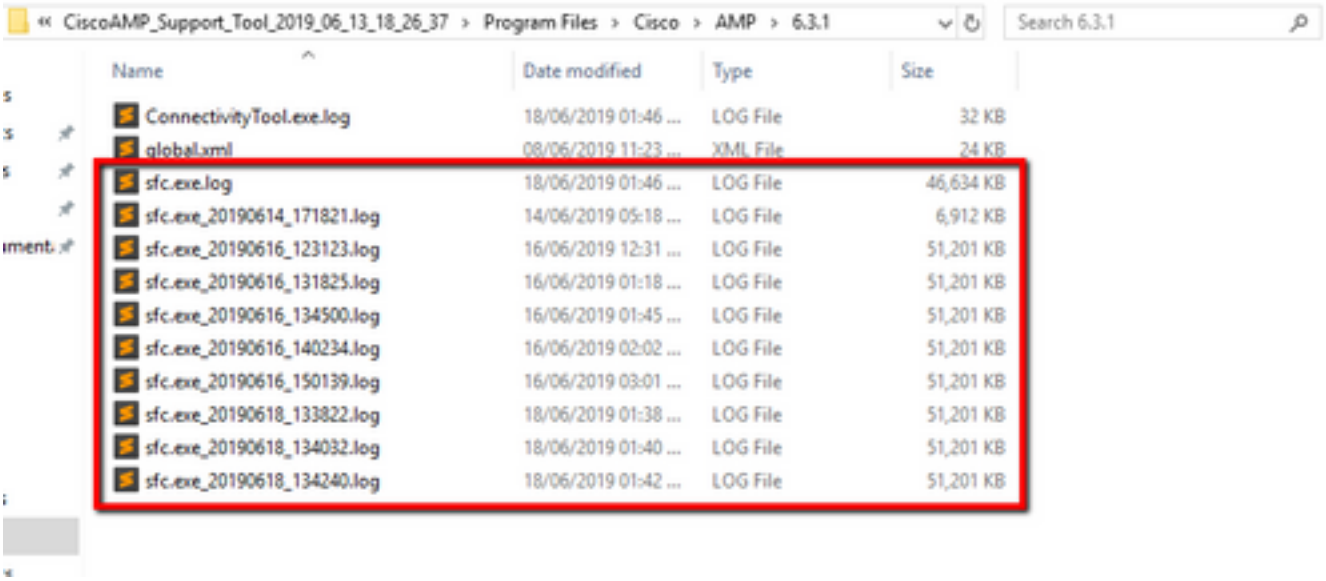
Passaggio 1. Scaricare lo script **amphandlecounts.txt** dalla parte inferiore di questo post della community Review Scanned Files da AMP.

Passaggio 2. Per eseguire lo script in Windows, rinominarlo in **amphandlecount.ps1**.

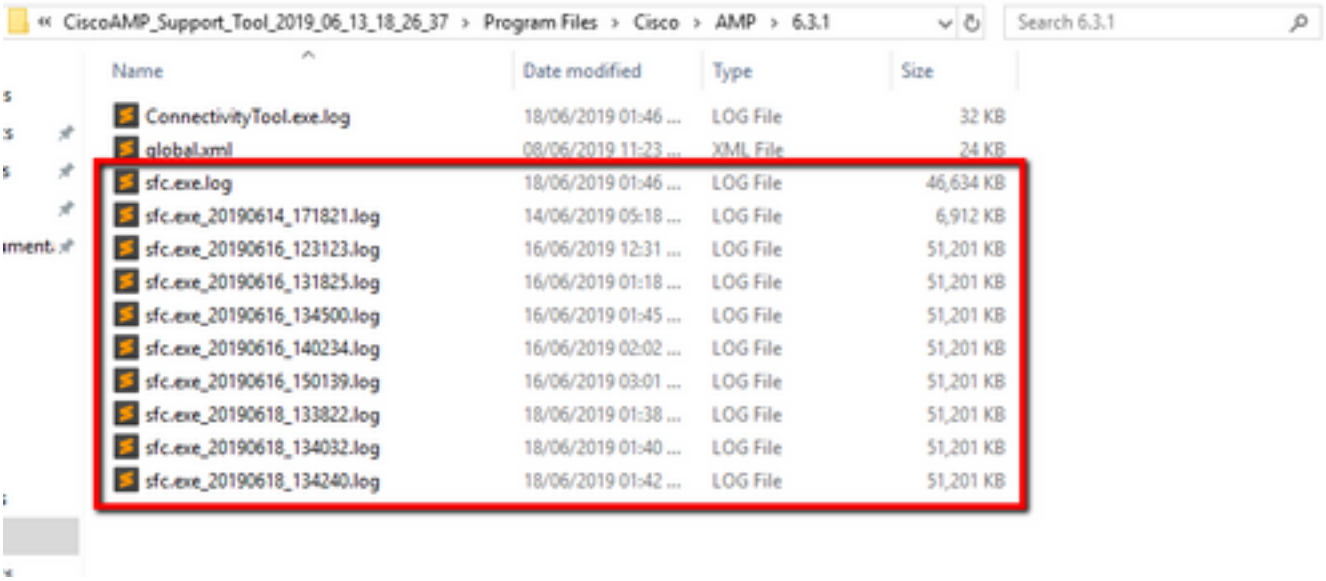
Passaggio 3. Per comodità copiare il file **amphandlecount.ps1** in una cartella propria.



Passaggio 4. Decomprimere il file **CiscoAMP_Support_Tool_%date%.7z** e identificare i file **sfc.log** nel percorso **CiscoAMP_Support_Tool_2019_06_13_18_26_37\Program Files\Cisco\AMP\X.X.X .**



Passaggio 5. Copiare i file **sfc.log** nella cartella **amphandlecount.ps1**.

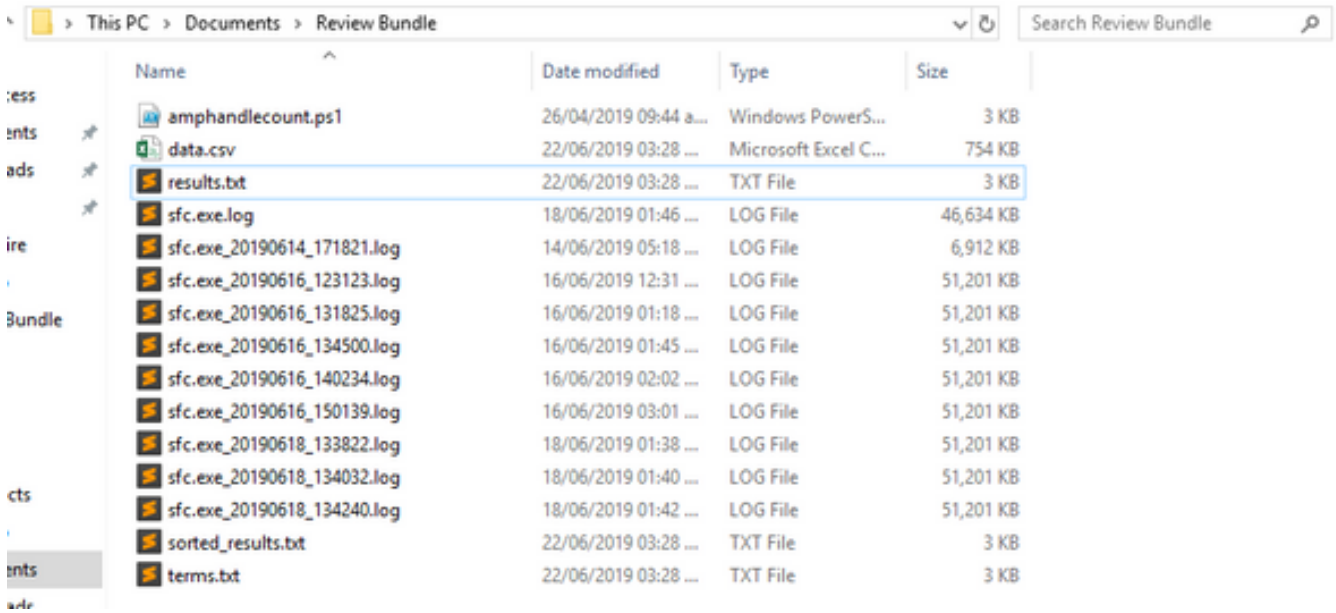


Passaggio 6. Eseguire **amphandlecount.ps1** con PowerShell, quindi viene aperta una finestra e, a seconda dei criteri di esecuzione sull'endpoint, può richiedere l'autorizzazione per l'esecuzione.

> **Suggerimento**: Per modificare i criteri di esecuzione, aprire Windows PowerShell e utilizzare i comandi seguenti:
> Impostare il criterio per consentire l'accesso senza restrizioni all'esecuzione - **Set-ExecutionPolicy -Scope CurrentUser -ExecutionPolicy Unrestricted**
> Impostare il criterio per limitare l'accesso di esecuzione - **Set-ExecutionPolicy -Scope CurrentUser -ExecutionPolicy Restricted**

Passaggio 7. Consentire il completamento di PowerShell (A seconda del numero di file sfc.log presenti nella cartella, il completamento dell'operazione potrebbe richiedere del tempo). Al termine di PowerShell, nella cartella vengono creati quattro file:

- **data.csv**
- **results.txt**
- **sorted_results.txt**
- **terms.txt**



Passaggio 8. I 4 nuovi file contengono il risultato dell'analisi:

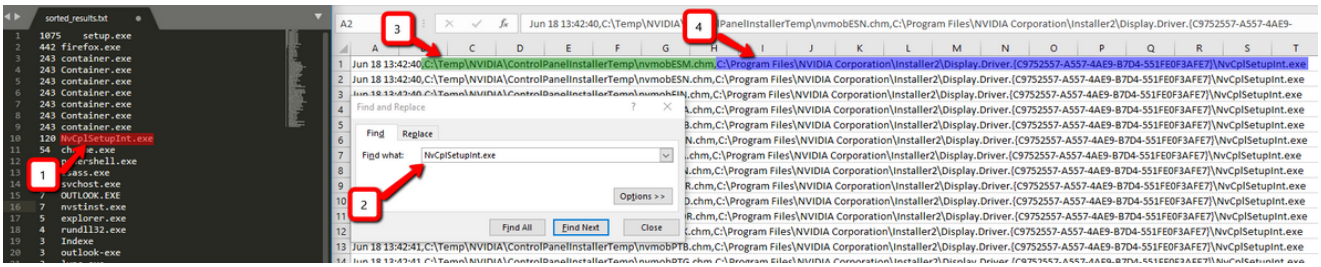
- **data.csv:** contiene il percorso completo dei file analizzati e il processo padre che ha creato/modificato/spostato il file
- **results.txt:** contiene l'elenco dei processi analizzati da AMP
- **sorted_results.txt:** contiene l'elenco dei processi analizzati da AMP con il processo più analizzato
- **term.txt:** contiene il nome dei processi analizzati da AMP

Passaggio 9. Filtrare il nome del processo con conteggi elevati dal file **sorted_results.txt** nel file **data.csv.** È possibile identificare il processo padre con il relativo percorso completo e quindi continuare ad aggiungere un'esclusione al criterio in un elenco personalizzato se il criterio è attendibile.

Processi da cercare:

1. Ctrl + F su "data.csv" e ricerca
2. Percorso del file analizzato da AMP
3. Percorso del processo padre che copia/sposta/modifica il file

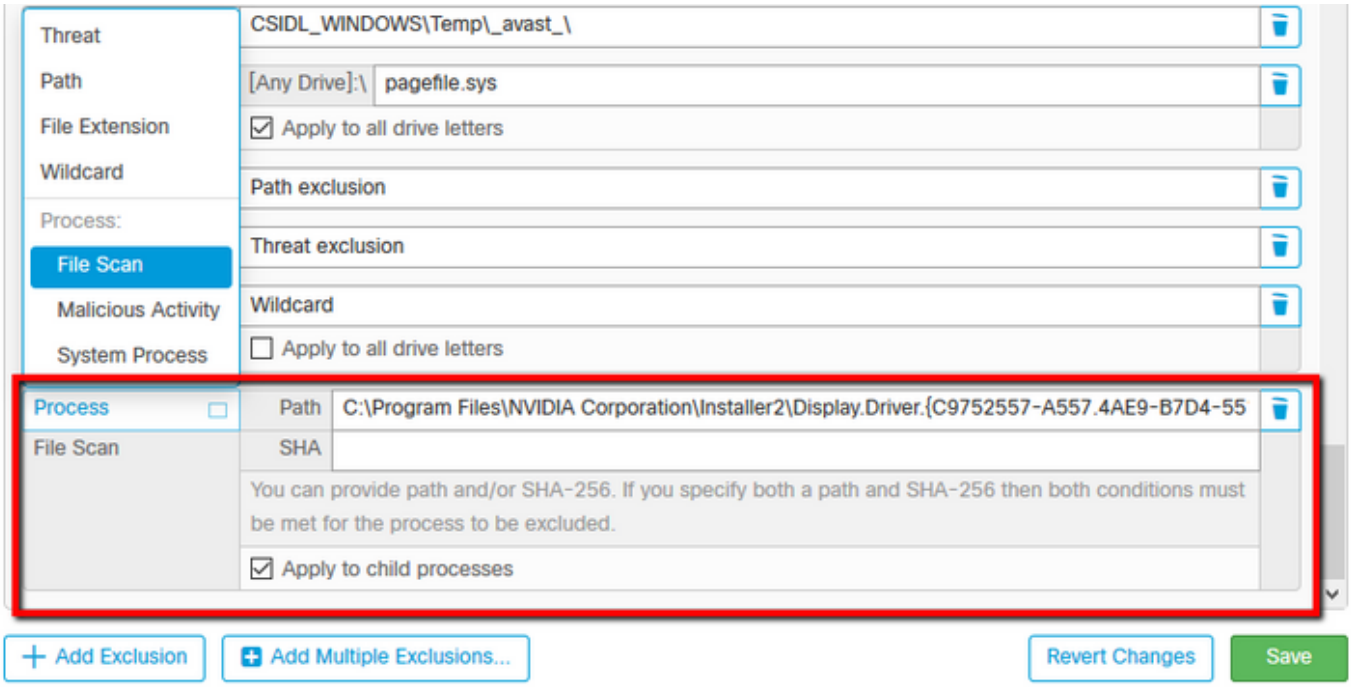
Nota: Nota: Di solito l'esclusione è del tipo "Processo: File Scan" con "Child Processes include" per il processo padre che sta ricevendo le scansioni:



Nota: Qui puoi trovare ulteriori informazioni relative alle best practice per creare esclusioni.

Esclusioni di sintonizzazione

Una volta identificati i processi o i percorsi, è possibile aggiungerli all'elenco di esclusione collegato al criterio applicato sull'endpoint, passare a **Gestione > Esclusioni > Nome esclusione > Modifica,** come mostrato nell'immagine.



Invia il bundle per l'analisi a TAC

ATS TAC può contribuire alla risoluzione di questi scenari; in tal caso, essere pronti a fornire le informazioni successive alla creazione del caso:

- Quando inizia il problema?
- Ci sono dei cambiamenti recenti?
- Il problema si verifica con un'applicazione specifica?Se sì, quale applicazione?
- Sul sistema sono presenti altri programmi antivirus?Se sì, quale antivirus?
- Raccogliere un bundle di debug durante la riproduzione del problema: Procedura per raccogliere un bundle di debug