Guida all'ottimizzazione delle prestazioni del connettore Mac Secure Endpoint

Sommario

Introduzione

Perché dobbiamo sintonizzarci?

Ogni volta che un file viene creato, spostato, copiato o eseguito su un endpoint Mac, un evento per quel file viene inviato dal sistema operativo al connettore Secure Endpoint Mac. L'evento determina l'analisi del file da parte del connettore. Il processo di analisi in genere prevede l'hashing del file in questione e l'esecuzione attraverso diversi motori di analisi sia sul computer che nel cloud. È importante riconoscere che questo atto di hashing consuma cicli della CPU.

Maggiore è il numero di operazioni ed esecuzioni di file che si verificano su un determinato endpoint, maggiore sarà il numero di cicli della CPU e di risorse di I/O necessarie al connettore per eseguire l'hashing. Al connettore sono state aggiunte diverse funzionalità per ridurre il sovraccarico. Ad esempio, se un file in fase di creazione, spostamento o copia è stato precedentemente analizzato, il connettore utilizzerà un risultato memorizzato nella cache. Tuttavia, nel caso di alcuni eventi, ad esempio le esecuzioni, in cui la protezione è fondamentale, tutti gli eventi vengono sempre analizzati completamente dal connettore. Ciò significa che le applicazioni o i processi che propagano più esecuzioni ripetitive di processi secondari, in particolare in un breve periodo di tempo, possono causare problemi di prestazioni. La ricerca e l'esclusione di applicazioni che eseguono in modo ripetitivo processi secondari a una velocità maggiore di una volta al secondo può ridurre in modo significativo l'utilizzo della CPU e aumentare la durata della batteria dei notebook.

Le operazioni sui file, quali le operazioni di creazione e spostamento, hanno generalmente un impatto minore rispetto all'esecuzione, ma scritture di file eccessive e la creazione di file temporanei possono causare problemi simili. Un'applicazione che scrive frequentemente in un file di log o che genera più file temporanei può causare l'esecuzione di numerosi cicli della CPU da parte di Secure Endpoint con analisi non necessarie e può creare un notevole rumore per il back-end di Secure Endpoint. Distinguere le parti rumorose delle applicazioni legittime è un passo molto importante per mantenere un endpoint produttivo e sicuro.

Lo scopo di questo documento è quello di aiutare a distinguere le operazioni sui file (creazione, spostamento e copia) e le esecuzioni che avranno un effetto negativo sulle prestazioni del daemon e sui cicli di CPU sprecati. L'identificazione di questi percorsi di file e directory consente di creare e gestire i set di esclusione appropriati per l'organizzazione.

Èpossibile aggiungere elenchi di esclusione predefiniti ai criteri gestiti da Cisco per garantire una migliore compatibilità tra il connettore Secure Endpoint e il software antivirus, di sicurezza o di altro tipo. Questi elenchi sono disponibili nella pagina Esclusioni della console come Esclusioni gestite da Cisco.

Tipi di tuning

Sono disponibili tre tipi di opzioni di tuning di esclusione:

1. **Sintonizzazione pre-installazione - questa operazione può essere eseguita prima di installare il connettore Secure Endpoint Mac. In questo modo è possibile individuare con precisione l'applicazione e i percorsi più utilizzati nel computer. Tuttavia, è un processo molto rumoroso e richiede all'utente di fare un po' di analisi e aggregazione da solo.**
2. **Ottimizzazione dello strumento di supporto** - questa operazione può essere eseguita dopo l'installazione del connettore Mac e può essere eseguita su qualsiasi endpoint senza binari aggiuntivi. Offre un aspetto limitato ed è ideale per l'identificazione di applicazioni problematiche.
3. **Procmon Tuning** - questo processo richiede anche l'installazione del connettore, ma richiede anche l'utilizzo del binario Procmon, il nostro strumento di ottimizzazione personalizzato. Si tratta essenzialmente di una versione più sofisticata della funzione di ottimizzazione dello strumento di supporto. Questo metodo richiede la massima configurazione; tuttavia, fornisce i migliori risultati.

1. Tuning pre-installazione

L'ottimizzazione pre-installazione è la forma di ottimizzazione più semplice e viene eseguita principalmente tramite la riga di comando in una sessione di Terminal.

Per mac più recente da OS X El Capitan è necessario prima avviare in modalità recovery (comando-r) durante l'avvio e disabilitare la protezione per dtrace:

```
csrutil enable --without dtrace
```

Per verificare quali sono le esecuzioni file più diffuse, eseguire quanto segue:

```
$ sudo newproc.d | perl -pe 'use POSIX strftime; print strftime "[%Y-%m-%d %H:%M:%S] ", localtime'
```

In questo modo vengono generalmente visualizzate le applicazioni che vengono eseguite più volte. Molte applicazioni di provisioning eseguono script o file binari a intervalli brevi per gestire le policy software aziendali. Tutte le applicazioni che vengono eseguite a una velocità superiore a una volta al secondo, o più volte in brevi intervalli, devono essere considerate idonee ad essere escluse.

Per verificare quali operazioni sui file sono più frequenti, eseguire il comando seguente:

```
$ sudo iosnoop | perl -pe 'use POSIX strftime; print strftime "[%Y-%m-%d %H:%M:%S] ", localtime'
```

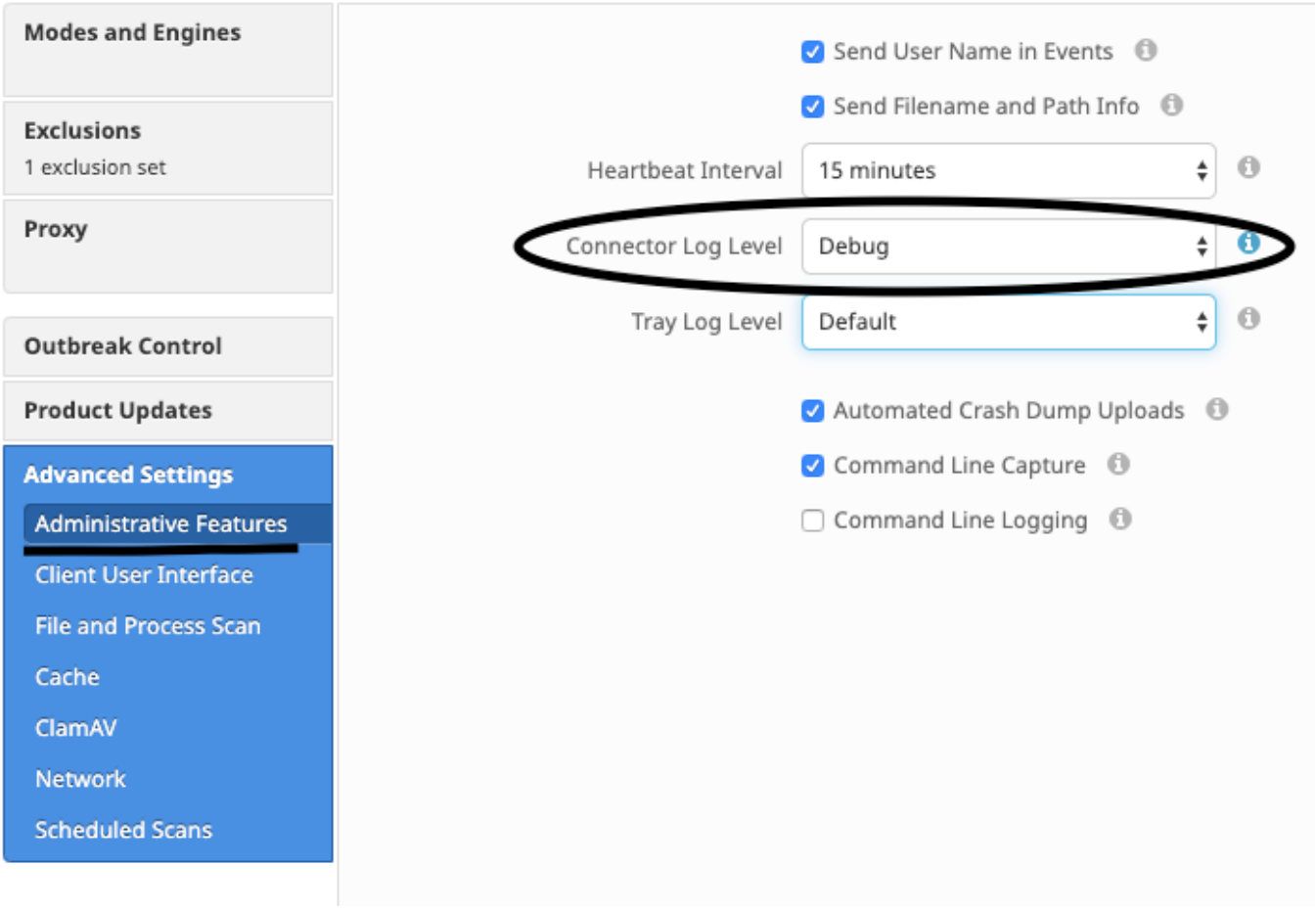
Verranno immediatamente visualizzati i file che vengono scritti più frequentemente. Spesso si tratta di file di log scritti da applicazioni in esecuzione, software di backup che copia i file o applicazioni di posta elettronica che scrivono file temporanei. Inoltre, una buona regola pratica

consiste nel considerare qualsiasi elemento con un'estensione del file di registro o del diario come candidato di esclusione appropriato.

2. Strumento di supporto Ottimizzazione

Abilitazione della registrazione di debug

Prima di iniziare l'ottimizzazione dei file di supporto, è necessario attivare la modalità di registrazione debug del daemon del connettore. A tale scopo, utilizzare la console Secure Endpoint, tramite le impostazioni dei criteri del connettore in *Gestione -> Criteri*. Selezionare il criterio, modificarlo e passare alla sezione *Funzioni amministrative* nella barra laterale *Impostazioni avanzate*. Modificare l'impostazione *Connector Log Level* (Livello registro) su **Debug**.



Avanti, salvare i criteri. Una volta salvati i criteri, assicurarsi che sia stata sincronizzataronizzato allaConnettore. Eseguire il comando cConnettore in questa modalità per almeno 15-20 minuti prima di continuare con il resto del tuning.

NOTA: Al termine dell'ottimizzazione, non dimenticare di modificare il *Connector Log Level* ripristino **Predefinito** affinché ilConnettore esecuzioni in sua più efficienti e modalità effettiva.

Esecuzione dello strumento di supporto

Questo metodo prevede l'utilizzo dello strumento di supporto, un'applicazione installata con il connettore Secure Endpoint Mac. È possibile accedervi dalla cartella Applications facendo doppio clic su /Applications->Cisco Secure Endpoint->Support Tool.app. Verrà generato un pacchetto di supporto completo contenente ulteriori file di diagnostica.

Un alternativa, e più veloce, il metodo consiste nell'eseguire riga di comando seguente da a Terminale sessione:

```
sudo/Library/Application Support/Cisco/AMP for Endpoints/SupportTool-x
```

In questo modo si otterrà un file di supporto molto più piccolo contenente solo i file di ottimizzazione rilevanti.

In entrambi i casi, lo strumento di supporto genererà un file zip sul desktop contenente due file di supporto per il tuning: fileops.txt ed excel.txt. fileops.txt contiene un elenco dei file creati e modificati più di frequente nel computer. excel.txt conterrà l'elenco dei file eseguiti con maggiore frequenza. Entrambi gli elenchi sono ordinati in base al numero di scansioni, il che significa che i percorsi digitalizzati con maggiore frequenza vengono visualizzati in cima all'elenco.

Lasciare il connettore in esecuzione in modalità di debug per un periodo di 15-20 minuti, quindi eseguire lo Strumento di supporto. Una buona regola pratica consiste nel fatto che qualsiasi file o percorso con una media di 1000 accessi o più durante tale periodo è un buon candidato da escludere.

Creazione di percorsi, caratteri jolly, nomi e estensioni di file

Per iniziare a utilizzare le regole di esclusione del percorso, è possibile individuare i percorsi di file e cartelle digitalizzati con maggiore frequenza dal file fileops.txt e quindi creare regole di esclusione per tali percorsi. Una volta scaricato il criterio, monitorare il nuovo utilizzo della CPU. L'aggiornamento della regola potrebbe richiedere dai 5 ai 10 minuti prima che l'utilizzo della CPU diminuisca, in quanto il daemon potrebbe impiegare del tempo per recuperare il tempo necessario. Se i problemi persistono, eseguire nuovamente lo strumento per visualizzare i nuovi percorsi osservati.

- Una buona regola pratica consiste nel considerare qualsiasi elemento con un'estensione di file di registro o di diario come candidato di esclusione appropriato.

Creazione di esclusioni di processo

NOTE: `Process Exclusions on Mac can only be implemented for Mach-O files. Users cannot implement Process Exclusions for file formats such as .sh (Shell Scripts) or .app (Application Bundles).`
Per informazioni sulle procedure consigliate relative alle esclusioni di processo, vedere:Endpoint protetto: Esclusioni dei processi in macOS e Linux

Per prima cosa, un buon pattern di tuning identifica i processi con un elevato volume di esecuzioni da excs.txt, trova il percorso dell'eseguibile e crea un'esclusione per questo percorso. Esistono tuttavia alcuni processi che non devono essere inclusi, tra cui:

- Programmi di utilità generali - Non si consiglia di escludere i programmi di utilità generali (es: usr/bin/grep) senza tenere conto di quanto segue. L'utente può determinare l'applicazione che chiama il processo, ad esempio trovare il processo padre che esegue grep ed escludere il processo padre. Questa operazione deve essere eseguita solo se il processo padre può essere trasformato in una esclusione sicura. Se l'esclusione padre si applica ai figli, verranno escluse anche le chiamate a qualsiasi figlio dal processo padre.È possibile determinare l'utente che esegue il processo. (es: se un processo viene chiamato a un volume elevato dall'utente "root", è possibile escludere il processo, ma solo per l'utente specificato "root", in questo modo l'endpoint sicuro potrà monitorare le esecuzioni di un determinato processo da parte di qualsiasi utente che non sia "root").**NOTA: le esclusioni di processo sono state introdotte nelle versioni 1.11.0 e successive dei connettori. Per questo motivo, i programmi di utilità generale possono essere utilizzati come esclusione di percorso in connettori versione 1.10.2 e successive. Tuttavia, questa pratica è consigliata solo quando è assolutamente necessario un compromesso sulle prestazioni.**

L'individuazione del processo padre è importante per le esclusioni di processo. Una volta individuato il processo principale e/o l'utente del processo, l'utente può creare l'esclusione per un utente specifico e applicare l'esclusione del processo ai processi secondari, che a loro volta escluderanno i processi rumorosi che non possono essere trasformati in esclusioni di processo.

Identifica processo padre

1. Da excel.txt, identificare il processo con volumi elevati (ad esempio: /bin/rm).
2. Aprire ampdaemon.log dal pacchetto di supporto, decomprimere syslog.tar, quindi seguire il percorso /Library/Logs/Cisco/ampdaemon.log

(disponibile solo nel pacchetto di supporto completo, non in un pacchetto di supporto generato con le opzioni predefinite).

3. Cercare ampdaemon.log per il processo da escludere. Trovare la riga di log che mostra l'esecuzione del processo (ad esempio: 19 ago 09:47:29 devs-Mac.local [2537] [fileop]:[info]-[kext_processor.c@938]:[210962]: Daemon Rx: VNODE:EXECUTE X:6210 P:3296 PP:3200 U:502 [/bin/rm]).
4. Identificare il processo padre utilizzando uno dei seguenti metodi: Identificare il percorso del processo padre che può seguire il percorso del processo da escludere (ad esempio: [/bin/rm] [*Percorso processo padre*]).Se il log non include il percorso del processo padre, identificare l'ID del processo padre nella sezione `PP:` della riga di log (ad esempio: PP: 3200).
5. Utilizzando il percorso padre o l'ID del processo padre, ripetere i passaggi 3 e 4 per determinare il padre del processo padre corrente. Continuare il processo fino a quando non è possibile determinare alcun padre o fino a quando l'ID del processo padre non è uguale a 1 (ad esempio: PP:1).
6. Una volta che la struttura del processo è nota, cercare il percorso del programma che copre la maggior parte o tutte le operazioni da escludere e identifica in modo univoco l'applicazione. In questo modo si riduce al minimo la possibilità di escludere involontariamente le operazioni eseguite da un'altra applicazione.

Identifica utente del processo

1. Seguire i passi da 1 a 3 di Identificazione del processo padre dall'alto.
2. Identificare l'utente di un processo utilizzando uno dei seguenti metodi: Trova l'ID utente del processo specificato da `U:` nella riga di registro (ad esempio: U:502).Dalla finestra Terminale eseguire il seguente comando: `dscl . list /Users ID univoco | grep #`, dove # è l'ID utente.L'output dovrebbe essere simile a: `Username 502`, dove `Username` è l'utente del processo specificato.
3. Questo nome utente può essere aggiunto a un'esclusione di processo nella categoria Utente per ridurre l'ambito dell'esclusione, che per alcune esclusioni di processo è importante. **NOTA: se l'utente di un processo è l'utente locale del computer e questa esclusione deve essere applicata a più computer con utenti locali diversi, la categoria Utente deve essere lasciata vuota per consentire l'applicazione dell'esclusione di processo a tutti gli utenti.**